Pharmacy Reengineering (PRE)

Inbound ePrescribing (IEP) 3.1

Pentaho 8.2

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

February 2020

Department of Veterans Affairs (VA)

Office of Information and Technology (OIT)

Revision History

Date	Version	Description	Author
02/26/2020	2.7	PSO*7.0*589 Maintenance Patch Release: • Updated WebLogic Installation section • Updated Pentaho Installation section • Updated VistA Back-Out and Rollback sections • Updated Title page, Revision History, and Footers • Updated formatting for consistency throughout	Liberty C. Barthauer, PM J. Smith, TW
06/06/2019	2.6	Updates for changes with 3.1.0.005 reference: pg: 117, 127, and 132 Updated Title page to month of June	Technatomy
05/07/2019	2.5	Updates for changes with 3.1.0.004 reference: pg 127, 132, 145, 146, and 150 Updated Title page to month of March	Technatomy
03/11/2019	2.4	Updates for changes with 3.1.0.003 reference: pg 127, 132, 145, 146, and 150 Updated Title page to month of February	Technatomy
10/29/2018	2.3	Update Title page to month of November	Technatomy
10/24/2018	2.2	Updates for changes with 3.0.5.008 reference: pg 132	Technatomy
09/21/2018	2.1	Updated to address VIP RA Comments Sections: 5.6.1, 5.7.1, 6.5.2, 6.5.2.1	Technatomy
09/19/2018	2.0	Updates for changes with 3.0.5.005.	Technatomy
07/26/2017	0.93	Updates for changes with 2.0.4.057.	Technatomy
07/20/2017	0.92	Updates for changes with 2.0.4.057.	Technatomy
06/27/2017	0.91	Updates for changes with 2.0.4.054.	Technatomy
05/22/2017	0.8	Updates for changes with 2.0.4.048.	Technatomy
05/10/2017	0.7	Updates for changes with 2.0.3.047.	Technatomy
04/25/2017	0.6	Updates with corrected information for Staging, PreProd and Production.	Technatomy
04/12/2017	0.5	Updates with corrected information for Staging, PreProd and Production.	Technatomy
02/15/2017	0.4	Updates with corrected information for Staging, PreProd and Production. New sections for SSOi.	Technatomy
02/07/2017	0.3	Multiple updates with new steps introduced throughout Build 1, cleanup for Staging, PreProd and Production.	Technatomy
11/10/2016	0.2	Sprint Update – Added draft steps for rolling back Weblogic; added the VistA Patch #; added a placeholder for backing out the database.	Technatomy
10/27/2016	0.1	Initial Draft (Template Version 2.2 March 2016)	Technatomy

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

Table of Figures

List of Tables

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 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.

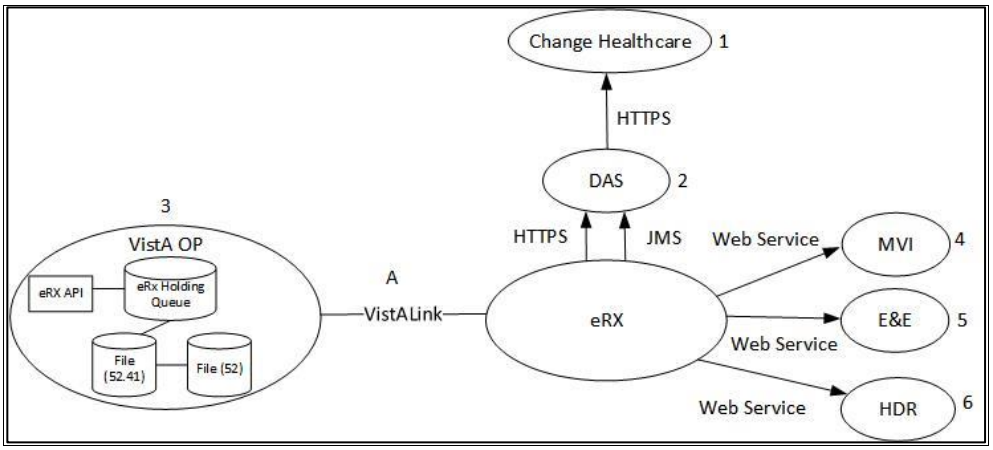
1.1 Purpose

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 1 depicts the Inbound eR_x 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 eR_x 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 HL7and 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.

Table 1: Deployment, Installation, Back-out, and Rollback Roles and Responsibilities

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
7	Regional PM/FIS/OPP PM/ Nat'l Education & Training	Installations	Coordinate training.	Deployment
8	FO, EO, NDCP or Product Development (depending upon project ownership)	Back-out	Confirm availability of back-out instructions and back-out strategy	Deployment

ID	Team	Phase / Role	Tasks	Project Phase (See Schedule)
			(what are the criteria that trigger a back-out).	
9	FO, EO, NDCP or Product Development (depending upon project ownership)	Post Deployment	Hardware, Software and System Support.	Maintenance

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 2: Deployment Timeline

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

3.2 Site Readiness Assessment

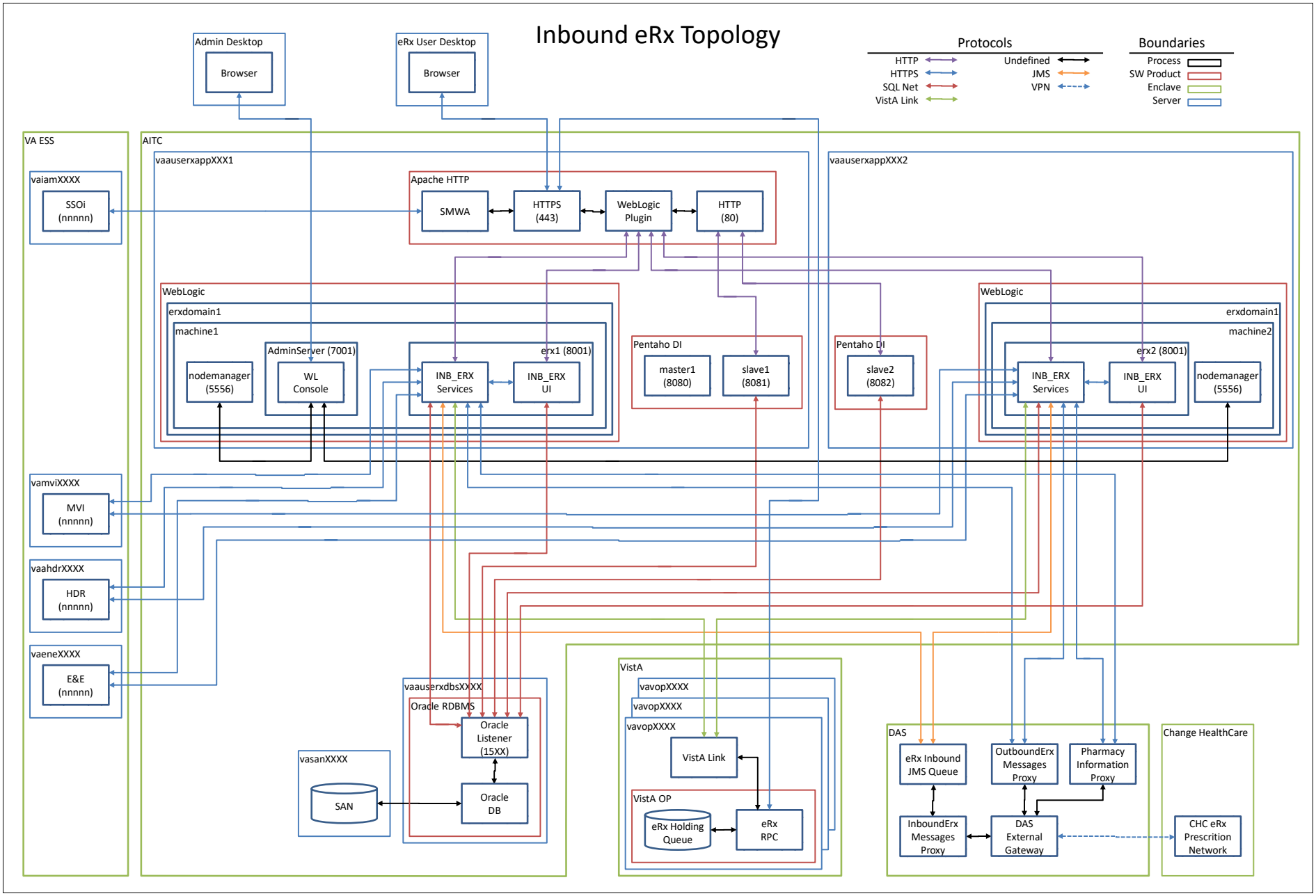
This section discusses the locations that will receive the PRE Inbound eRx application deployment. Topology determinations are made by Enterprise Systems Engineering (ESE) and vetted by Field Operations (FO), National Data Center Program (NDCP), and AITC during the design phase as appropriate. Field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



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 3: Site Preparation

Site/Other	Problem/Change Needed	Features to Adapt/Modify to New Product	Actions/Steps	Owner
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 4: Software Specifications

Required Software	Make	Version	Configuration	Manufacturer	Other
WebLogic Application Server	Application Server	12.1.3c	Clustered	Oracle	
Oracle Database	Database	11.2.0g	Standalone (not synchronized across data centers)	Oracle	
Pentaho Data Integration	Data Integration Tool	8.2	Standalone	Pentaho (a Hitachi Group Company)	

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 is an example of the coordination effort and can be used to document the day/time/individual when each activity (deploy, install, back-out) is completed for Inbound eRx.

Table 5: Deployment/Installation/Back-Out Checklist

Activity	Day	Time	Individual who completed task
Deploy			
Install			
Back-Out			

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 6: Development/SQA Detailed VM Requirements

VM	RAM (GB)	Space (GB)	CPUs	OS	VM Description/Use/DNS Required
1	16	300	4	RHEL 6	DEV 1 DB Server running Oracle
2	16	300	4	RHEL 6	DEV 2 DB Server running Oracle
3	16	300	4	RHEL 6	SQA 1 DB Server running Oracle
4	16	300	4	RHEL 6	SQA 2 DB Server running Oracle
5	16	300	4	RHEL 6	DEV1 AP Server running Apache/WebLogic
6	16	300	4	RHEL 6	DEV 2 AP Server running Apache/WebLogic
7	16	300	4	RHEL 6	SQA 1 AP Server running Apache/WebLogic
8	16	300	4	RHEL 6	SQA 2 AP Server running Apache/WebLogic
Total	128	2400	32	8	

Table 7: Staging Detailed VM Requirements

VM	RAM (GB)	Space (GB)	CPUs	OS	VM Description/Use/DNS Required
1	16	800	4	RHEL 7	STAGING DB Server running Oracle
2	16	300	4	RHEL 7	STAGING Application Server running Apache/WebLogic

VM	RAM (GB)	Space (GB)	CPUs	OS	VM Description/Use/DNS Required
3	16	300	4	RHEL 7	STAGING Application Server running Apache/WebLogic
Total	48	1400	16	3	

Table 8: Pre-Production Detailed VM Requirements

VM	RAM (GB)	Space (GB)	CPUs	OS	VM Description/Use/DNS Required
1	16	1300	4	RHEL 6	PRE-PRODUCTION DB Server running Oracle
2	16	300	4	RHEL 6	PRE-PRODUCTION Application Server running Apache/WebLogic
3	16	300	4	RHEL 6	PRE-PRODUCTION Application Server running Apache/WebLogic
Total	48	1900	12	3	

Table 9: Production Detailed VM Requirements

VM	RAM (GB)	Space (GB)	CPUs	OS	VM Description/Use/DNS Required
1	16	1300	4	RHEL 6	PRODUCTION DB Server running Oracle
2	16	300	4	RHEL 6	PRODUCTION Application Server running Apache/WebLogic
3	16	300	4	RHEL 6	PRODUCTION Application Server running Apache/WebLogic
Total	48	1900	12	3	

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 10: Environment Variables

ENV	ORACLE_BASE	WLS_HOME	DOMAIN_HOME
DEV1	/u01/app/Oracle_Home	$ORACLE_BASE/wlserver	$ORACLE_BASE/user_projects/domains/erxdomain1
DEV2	/u01/app/Oracle_Home	$ORACLE_BASE/wlserver	$ORACLE_BASE/user_projects/domains/erxdomain2
SQA1	/u01/app/Oracle_Home	$ORACLE_BASE/wlserver	$ORACLE_BASE/user_projects/domains/erxdomain1
STAG	/u01/oracle	$ORACLE_BASE/wlserver	$ORACLE_BASE/user_projects/domains/iep-stage
STAG2	/u01/oracle	$ORACLE_BASE/wlserver	$ORACLE_BASE/user_projects/domains/iep-stage2
PREP	/u01/oracle	$ORACLE_BASE/wlserver	$ORACLE_BASE/user_projects/domains/iep-preprod
PREP2	/u01/oracle	$ORACLE_BASE/wlserver	$ORACLE_BASE/user_projects/domains/ iep-preprod2
PROD	/u01/oracle	$ORACLE_BASE/wlserver	$ORACLE_BASE/user_projects/domains/iep-prod
PROD2	/u01/oracle	$ORACLE_BASE/wlserver	$ORACLE_BASE/user_projects/domains/iep-prod2

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

ENV	vm1_fqdn	vm1_name	vm2_fqdn	vm2_name	domain
DEV1	vaauserxappdev1.aac.va.gov	vaauserxappdev1	vaauserxappdev2.aac.va.gov	vaauserxappdev2	erxdomain1
DEV2	vaauserxappdev2.aac.va.gov	vaauserxappdev2	vaauserxappdev1.aac.va.gov	vaauserxappdev1	erxdomain2
SQA1	vaauserxappsqa1.aac.va.gov	vaauserxappdev1	vaauserxappdev2.aac.va.gov	vaauserxappdev2	erxdomain1
STAG	vaausappiep402.aac.va.gov	vaausappiep402	vaausappiep403.aac.va.gov	vaausappiep403	iep-stage
STAG2	vaausappiep621.aac.va.gov	vaausappiep621	vaausappiep622.aac.va.gov	Vaausappiep622	iep-stage2
PREP	vaausappiep404.aac.va.gov	vaausappiep404	vaausappiep405.aac.va.gov	vaausappiep405	iep-preprod
PREP2	vaausappiep421.aac.va.gov	vaausappiep421	vaausappiep422.aac.va.gov	vaausappiep422	iep-preprod2
PROD	vaausappiep201.aac.va.gov	vaausappiep201	vaausappiep202.aac.va.gov	vaausappiep202	iep-prod
PROD2	vaausappiep221.aac.va.gov	vaausappiep221	vaausappiep222.aac.va.gov	vaausappiep222	iep-prod2

Table 12: Symbolic Names by Environment (cont.)

ENV	env	Env	erx_port	proxy_fqdn	proxy_name	db_fqdn	db_name	db_port
DEV1	dev1	Dev1	8001	vaauserxappdev1.aac.va.gov	vaauserxappdev1	vaauserxdbsdev1.aac.va.gov	ERXD1	1549
DEV2	dev2	Dev2	8003	vaauserxappdev2.aac.va.gov	vaauserxappdev2	vaauserxdbsdev2.aac.va.gov	ERXD2	1550
SQA1	sqa1	Sqa1	8001	Vaauserxappsqa2.aac.va.gov	vaauserxappsqa2	vaauserxdbssqa1.aac.va.gov	ERXS1	1549
STAG	stag	Stag	8001	vaausappiep402.aac.va.gov	vaausappiep403	vaausdbsiep400.aac.va.gov	IEPQA	1647
STAG2	stag2	Stag2	8001	vaausappiep622.aac.va.gov	vaausappiep622	vaausdbsiep400.aac.va.gov	IEPQA2	1648
PREP	prep	Prep	8001	vaausappiep404.aac.va.gov	vaausappiep404	vaausdbsiep401.aac.va.gov	IEPY	1647
PREP2	prep2	Prep2	8001	vaausappiep422.aac.va.gov	vaausappiep422	vaausdbsiep420.aac.va.gov	IEPY2	1647
PROD	prod	Prod2	8001	vaausappiep201.aac.va.gov	vaausappiep201	vaausdbsiep200.aac.va.gov	IEPP	1647
PROD2	prod2	Prod2	8001	vaausappiep221.aac.va.gov	vaausappiep221	vaausdbsiep220.aac.va.gov	IEPP2	1647

Table 13: Symbolic Names by Environment (cont.)

ENV	mserver1	mserver2	cluster
DEV1	erx1	erx2	dev1
DEV2	erx1	erx2	dev1
SQA1	erx1	erx2	dev1
STAG2	ManagedServer001	ManagedServer002	Cluster001
STAG	ManagedServer001	ManagedServer002	Cluster001
PREP2	ManagedServer001	ManagedServer002	Cluster001
PREP	ManagedServer001	ManagedServer002	Cluster001
PROD2	ManagedServer001	ManagedServer002	Cluster001
PROD	ManagedServer001	ManagedServer002	Cluster001

Table 14: Symbolic Names by Environment (cont.)

ENV	iam_hco	iam_policy_entries
DEV1	INTHCO	policyserver="smp1.int.iam.va.gov,44441,44442,44443" policyserver="smp2.int.iam.va.gov,44441,44442,44443" policyserver="smp3.int.iam.va.gov,44441,44442,44443" policyserver="smp4.int.iam.va.gov,44441,44442,44443"
DEV2	INTHCO	policyserver="smp1.int.iam.va.gov,44441,44442,44443" policyserver="smp2.int.iam.va.gov,44441,44442,44443" policyserver="smp3.int.iam.va.gov,44441,44442,44443" policyserver="smp4.int.iam.va.gov,44441,44442,44443"
SQA1	SQAHCO	policyserver="smp1.sqa.iam.va.gov,44441,44442,44443" policyserver="smp2.sqa.iam.va.gov,44441,44442,44443" policyserver="smp3.sqa.iam.va.gov,44441,44442,44443" policyserver="smp4.sqa.iam.va.gov,44441,44442,44443"
STAG	PREPRODHCO	policyserver="smp1.preprod.iam.va.gov,44441,44442,44443" policyserver="smp2.preprod.iam.va.gov,44441,44442,44443" policyserver="smp3.preprod.iam.va.gov,44441,44442,44443" policyserver="smp4.preprod.iam.va.gov,44441,44442,44443" policyserver="smp5.preprod.iam.va.gov,44441,44442,44443" policyserver="smp6.preprod.iam.va.gov,44441,44442,44443" policyserver="smp7.preprod.iam.va.gov,44441,44442,44443" policyserver="smp8.preprod.iam.va.gov,44441,44442,44443"
STAG2	PREPRODHCO	policyserver="smp1.preprod.iam.va.gov,44441,44442,44443" policyserver="smp2.preprod.iam.va.gov,44441,44442,44443" policyserver="smp3.preprod.iam.va.gov,44441,44442,44443" policyserver="smp4.preprod.iam.va.gov,44441,44442,44443" policyserver="smp5.preprod.iam.va.gov,44441,44442,44443" policyserver="smp6.preprod.iam.va.gov,44441,44442,44443" policyserver="smp7.preprod.iam.va.gov,44441,44442,44443" policyserver="smp8.preprod.iam.va.gov,44441,44442,44443"

Table 15: Symbolic Names by Environment (cont.)

ENV	iam_hco	iam_policy_entries
PREP	PREPRODHCO	policyserver="smp1.preprod.iam.va.gov,44441,44442,44443" policyserver="smp2.preprod.iam.va.gov,44441,44442,44443" policyserver="smp3.preprod.iam.va.gov,44441,44442,44443" policyserver="smp4.preprod.iam.va.gov,44441,44442,44443" policyserver="smp5.preprod.iam.va.gov,44441,44442,44443" policyserver="smp6.preprod.iam.va.gov,44441,44442,44443" policyserver="smp7.preprod.iam.va.gov,44441,44442,44443" policyserver="smp8.preprod.iam.va.gov,44441,44442,44443"
PREP2	PREPRODHCO	policyserver="smp1.preprod.iam.va.gov,44441,44442,44443" policyserver="smp2.preprod.iam.va.gov,44441,44442,44443" policyserver="smp3.preprod.iam.va.gov,44441,44442,44443" policyserver="smp4.preprod.iam.va.gov,44441,44442,44443" policyserver="smp5.preprod.iam.va.gov,44441,44442,44443" policyserver="smp6.preprod.iam.va.gov,44441,44442,44443" policyserver="smp7.preprod.iam.va.gov,44441,44442,44443" policyserver="smp8.preprod.iam.va.gov,44441,44442,44443"

Table 16: Symbolic Names by Environment (cont.)

ENV	iam_hco	iam_policy_entries
PROD	PRODHCO	policyserver="smp1.prod.iam.va.gov,44441,44442,44443" policyserver="smp2.prod.iam.va.gov,44441,44442,44443" policyserver="smp3.prod.iam.va.gov,44441,44442,44443" policyserver="smp4.prod.iam.va.gov,44441,44442,44443" policyserver="smp5.prod.iam.va.gov,44441,44442,44443" policyserver="smp6.prod.iam.va.gov,44441,44442,44443" policyserver="smp7.prod.iam.va.gov,44441,44442,44443" policyserver="smp8.prod.iam.va.gov,44441,44442,44443"
PROD2	PRODHCO	policyserver="smp1.prod.iam.va.gov,44441,44442,44443" policyserver="smp2.prod.iam.va.gov,44441,44442,44443" policyserver="smp3.prod.iam.va.gov,44441,44442,44443" policyserver="smp4.prod.iam.va.gov,44441,44442,44443" policyserver="smp5.prod.iam.va.gov,44441,44442,44443" policyserver="smp6.prod.iam.va.gov,44441,44442,44443" policyserver="smp7.prod.iam.va.gov,44441,44442,44443" policyserver="smp8.prod.iam.va.gov,44441,44442,44443"

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 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 17: Symbolic Names for sensitive items

Symbolic Name			
keystore_passphrase			
privatekey_passphrase			
weblogic_password			

The following are the properties that define the SSL security settings for WebLogic. These properties must be set respective to each environment.

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

Ensure the environment variables are set as follows:

```
$ 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
Cmnd_Alias WLS_SU=/bin/su - weblogic, /bin/su - weblogic2, /bin/su - weblogic3, /bin/su -
aacesrpprod, /bin/su - aacxpologger, /bin/su - introsvr
```

```
Cmnd_Alias WLS_CMD=/bin/ls, /bin/du, /bin/grep, /bin/cat, /sbin/chkconfig --list,
/sbin/service wls stop, /sbin/service wls start
Cmnd_Alias LSOF_CMD=/usr/sbin/lsof
WLS     ALL=(ALL) WLS_CMD
WLS     ALL=(ALL) WLS_SU
WLS     ALL=(ALL) LSOF_CMD
%weblogic        ALL=(ALL)       WLS_CMD
%weblogic        ALL=(ALL)       WLS_SU
%weblogic        ALL=(ALL)       LSOF_CMD
<ctrl>d
```

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
Cmnd_Alias KETTLE_SU=/bin/su - kettle
Cmnd_Alias KETTLE_CMD=/bin/ls, /bin/du, /bin/grep, /bin/cat, /sbin/chkconfig --list,
/usr/sbin/lsof
%kettle        ALL=(ALL)       KETTLE_CMD
%kettle        ALL=(ALL)       KETTLE_SU
<ctrl>d
```

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
<ctrl>d
```

4.2.4 Install Java

1. Log into Linux and 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 to your Linux 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, login to Linux and verify the following:
   ```
   $ 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/httpd/conf.d/pentaho.conf:

```
$ sudo vi /etc/httpd/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>
<Location /slave5/>
  ProxyPass http://[vm2_fqdn]:8085/
  ProxyPassReverse http://[vm2_fqdn]:8085/
  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:
distinguished_name = req_distinguished_name
[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
 [ req_attributes ]
challengePassword              = xxxxxxxxxx
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. Log into Linux and 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:

```
$ cat > va_intermediate_ca2_s2_cert.pem
```

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
```
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
```
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
```
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
```
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
```
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
```
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
```
26. Paste the vaww.esrpre-prod.aac.va.gov.pem content from Appendix 8.1.12
```
<ctrl>d
```
27. Create the das-test.va.gov.pem certificate in the “certificates” directory:
```
$ cat > vaww.esrstage1a.aac.va.gov.pem
```
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
```
30. Paste the das-sqa.va.gov.pem content from Appendix 8.1.14.
```
<ctrl>d
```
31. Create the das.va.gov.pem certificate in the “certificates” directory:
```
$ cat > das.va.gov.pem
```
32. Paste the das.va.gov.pem content from Appendix 8.1.15.
```
<ctrl>d
```

33. Create a certificate request configuration file:

```
$ 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 ]
subjectAltName=@alt_names

[ alt_names ]
DNS.1=[proxy_fqdn]
DNS.2=[vm2_fqdn]
<ctrl>d
```

34. Generate a permanent certificate signing request:

```
$ openssl req -out [proxy_fqdn]_csr_[yyyymmdd].txt -newkey rsa:2048 -keyout
[proxy_fqdn]_key.txt -new -sha256 -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:

```
$ cat > /u01/certificates/[proxy_fqdn]_cert.pem
```

37. Paste permanent certificate content.

```
<ctrl>d
```

38. Generate a ***[proxy_fqdn]*** pkcs12 certificate store:

```
$ 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:

```
$ keytool -importkeystore -deststorepass ######## -destkeypass ######## -destkeystore
[proxy_fqdn].jks -srckeystore [proxy_fqdn].p12 -srcstoretype PKCS12 -srcstorepass #### -
alias [proxy_fqdn]
```

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

```
$ 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:

```
$ 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 -file
betrusted_production_ssp_ca_a1_cert.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.esrstage1a.aac.va.gov.pem Certificate into ***[proxy_fqdn]*** java keystore:

```
$ keytool -import -alias vaww.esrstage1a.aac.va.gov -file vaww.esrstage1a.aac.va.gov.pem
-keystore [proxy_fqdn].jks
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.esrspre-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
Enter new password: ####
Re-enter password: ####
```

2. Add server permanent certificate:

```
$ sudo pk12util -i [proxy_fqdn].p12 -d /etc/httpd/alias -n [proxy_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.

4.2.9 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
   #TransferLog /etc/httpd/logs/access_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
#TransferLog /etc/httpd/logs/access_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.

4.2.12 Install Apache Plug-in for WebLogic on VM1 and VM2

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

1. Log into Linux and 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
```

4.2.13 Configure Apache Plug-in for WebLogic on VM1

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

1. Log into Linux and 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
  WLProxySSL 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 Configure Apache Plug-in for WebLogic on VM2

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

1. Log into Linux and 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
  WLProxySSL 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.

4.2.15 Create IEP CPanel on VM1 and VM2

1. Log into Linux and 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 Deploymentss 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
```

4.2.16 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. Log into Linux and 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+rx 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
      : /u01/app/CA/webagent
```
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
PRESS <ENTER> TO CONTINUE: <ENTER>
```
14. Confirm exit from installer:
```
PRESS <ENTER> TO EXIT THE INSTALLER: <ENTER>
```

4.2.17 Configure Apache SSOi Web Agent on VM1

1. Log into Linux and sudo su to the root account (the following must be performed by a system administrator):

```
$ sudo su -
```

2. Change directory to the agent home and "source" the Siteminder environment:

```
# cd /u01/app/CA/webagent
# . ./ca_wa_env.sh
```

3. Change to install config info directory and launch the configuration wizard:

```
# cd install_config_info
# ./ca-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

```
Policy Server IP Address
------------------------

Enter the IP Address of the Policy Server where you are registering this host.

Policy Server IP Address (Default: ): [iam_policy]
```

11. In the FIPS Mode Settings, select 3 then press Enter

```
FIPS Mode Setting
-----------------

  ->1- FIPS Compatibility Mode
    2- FIPS Migration Mode
    3- FIPS Only Mode
```

```
ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:: 3
```

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)
--------------------

    1- [] Apache 2.2.15

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
  ->2- No

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 doesnt
   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.

4.2.18 Post Configure Edits for Apache SSOi Web Agent on VM1

1. Log into Linux and 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 verbocity

    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 neer the bottom to be:

```
components:  WebAgent
data: Date, Time, Pid, Function, TransactionID, User, Message
```

13. Modify sysctl for Apache on RHEL 7.

    Open a text file for sysctl properties:

    dzdo systemctl edit httpd.service

    Insert 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.

    Reload the deamon:

dzdo systemctl daemon-reload

httpd should come up with a normal start command.
If a “file not found” error occurs, file “ca_wa_env.sh” may be in a different location.
These files can get installed in different locations across different systems.
If this is the case, execute a find command:

dzdo find / -name ‘ca_wa_env.sh’

If ‘ca_wa_env.sh’ is not found, search for “set-apache-env.sh”.

dzdo find / -name ‘set-apache-env.sh’
Update override.conf with the correct path.

Reload the deamon:
dzdo systemctl daemon-reload

Verify system is functioning correctly.

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

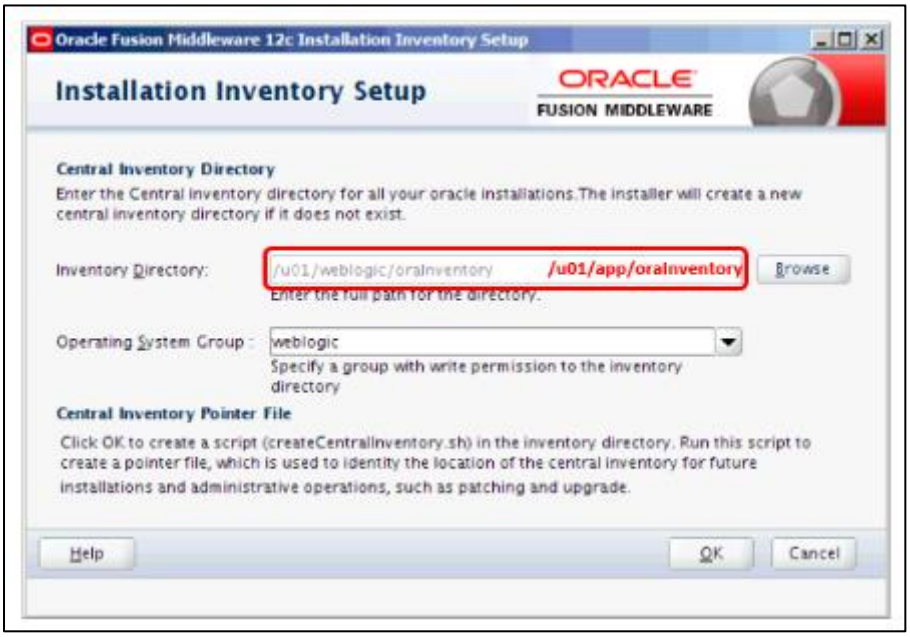
The following subsections describe the steps to install the WebLogic application server. Most activities are to be performed by the WebLogic Administrator.

4.8.1.1 Install WebLogic

1. Log into Linux and sudo to the weblogic account as follows:
   ```
   $ 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. Log into Linux and modify your .Xauthority permissions:
   ```
   $ chmod 755 ~
   $ chmod 644 ~/.Xauthority
   ```
6. Log into Linux and 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".

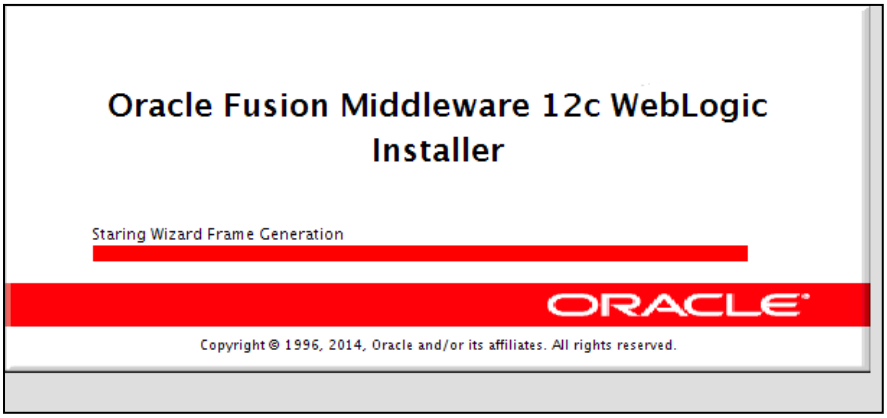
14. Select **OK**.

Figure 3: Install WebLogic – Oracle Fusion Middleware Installation Inventory Setup



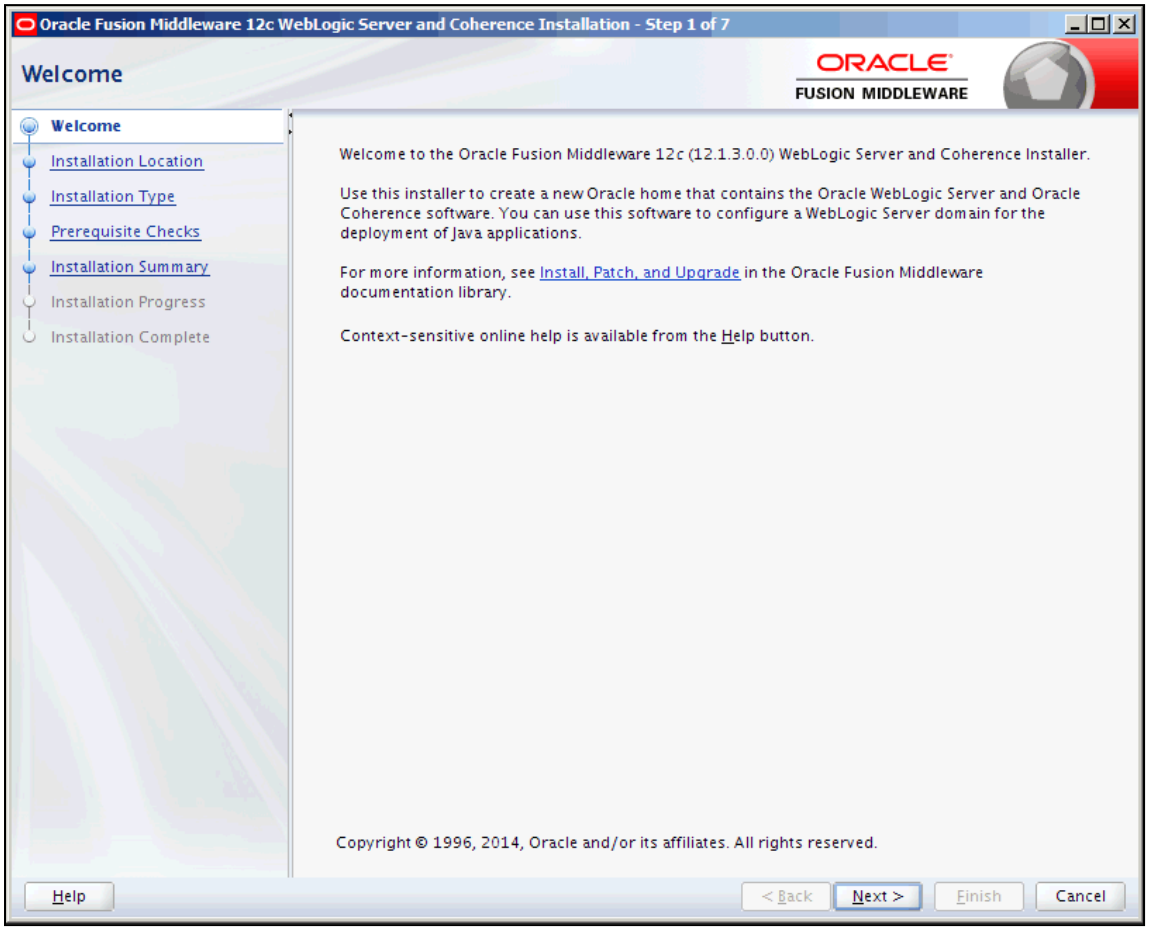
15. The Oracle Universal Installer will appear for a few moments.

Figure 4: Install WebLogic – Oracle Universal Installer Dialog Box



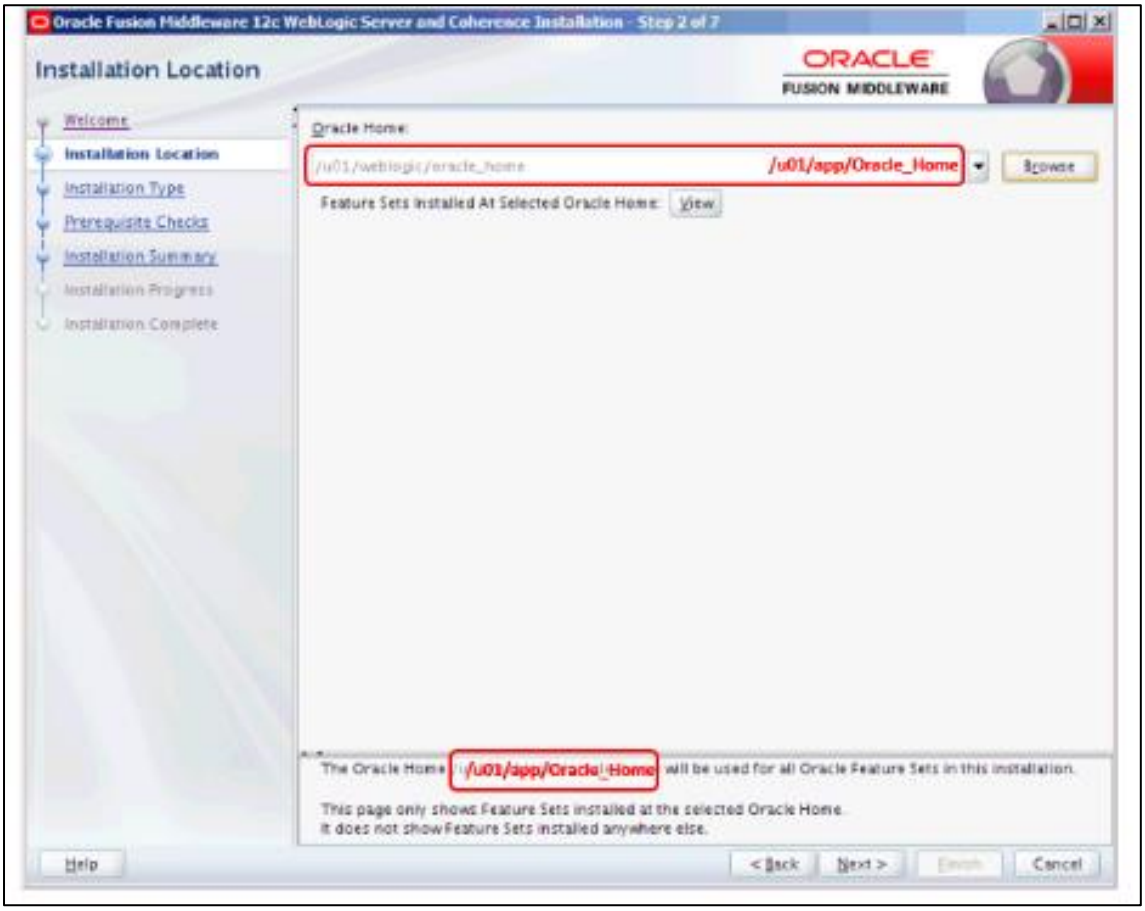
16. Once the installer is complete, select **Next**.

Figure 5: Install WebLogic – Oracle Fusion Middleware WebLogic Server and Coherence Installer



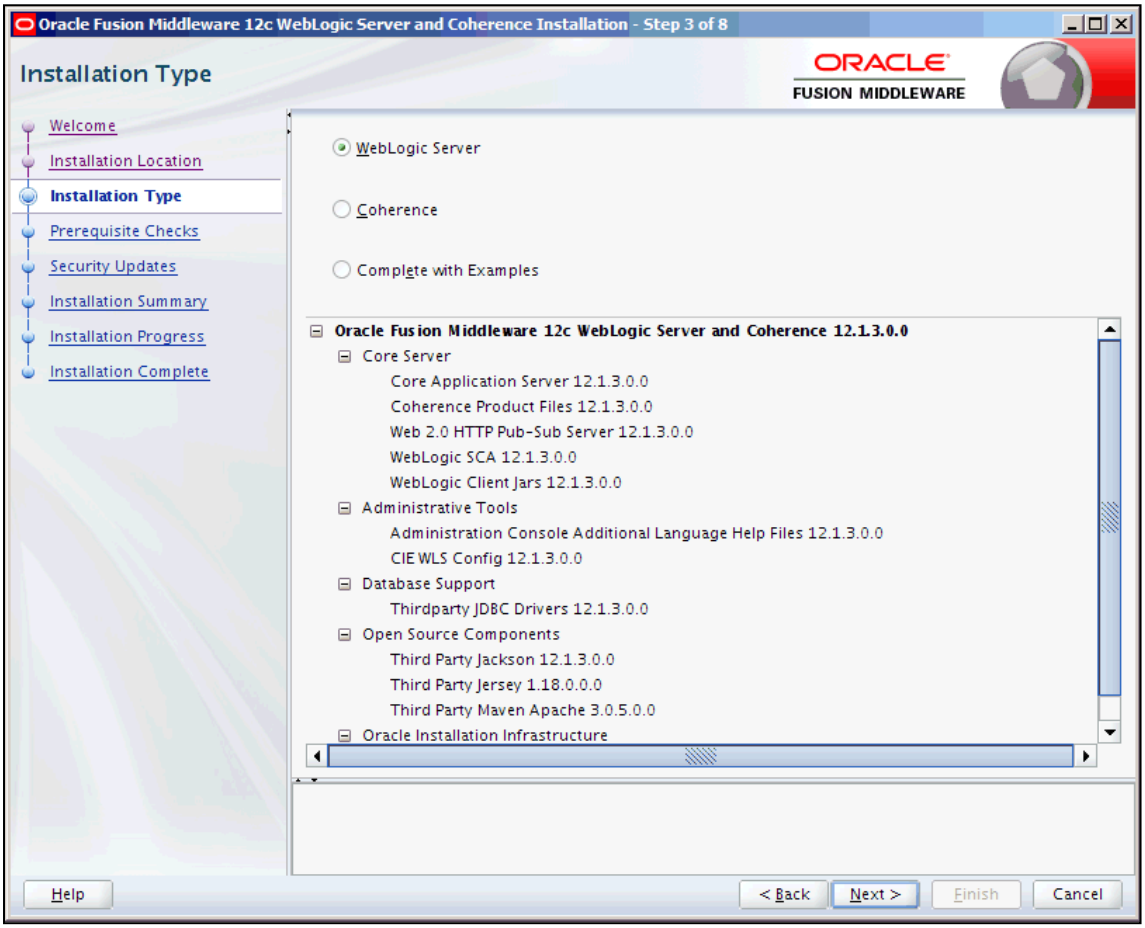
17. Enter *Oracle Home*: "***[ORACLE_BASE]***".
18. Select **Next**.

Figure 6: Install WebLogic – Installation Location



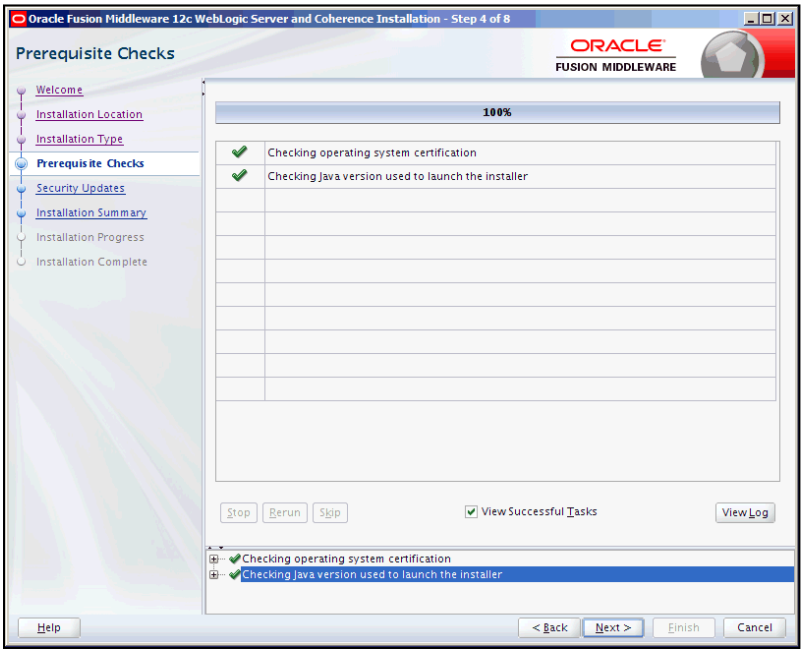
19. For *Installation Type*, select the *WebLogic Server* radio button.
20. Select **Next**.

Figure 7: Install WebLogic – Installation Type



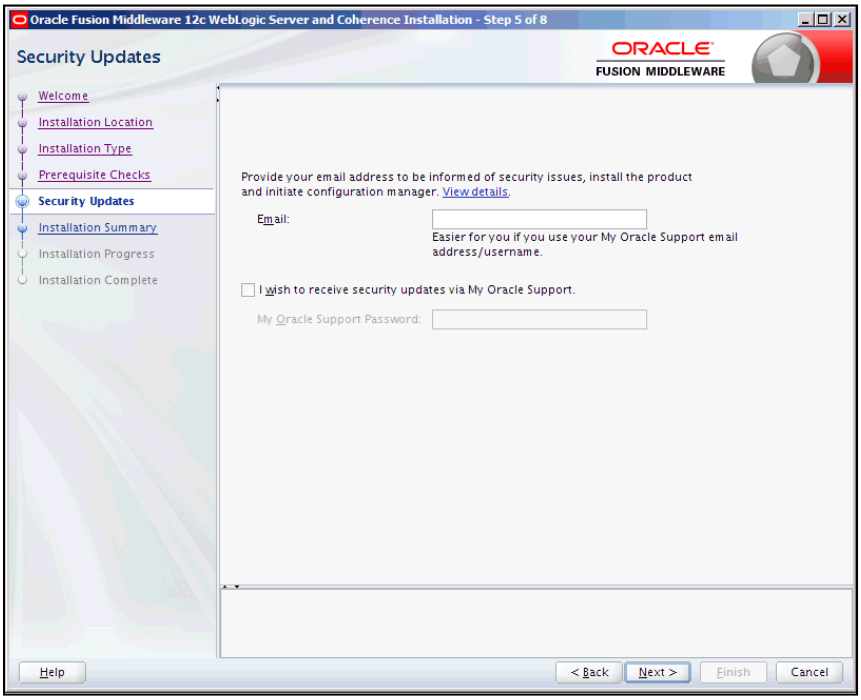
21. Select **Next** again on the **Prerequisite Checks** screen.

Figure 8: Install WebLogic – Prerequisite Checks



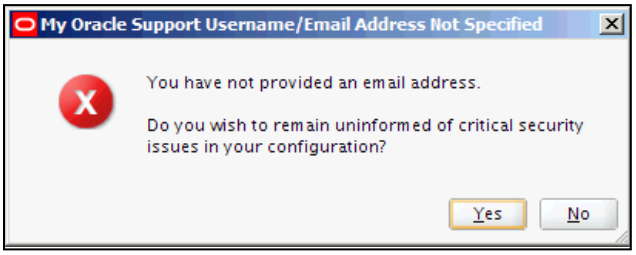
22. On the Security Updates screen, leave the *Email* field blank.
23. Uncheck "I wish to receive security updates via My Oracle Support".
24. Select **Next**.

Figure 9: Install WebLogic – Security Updates Screen



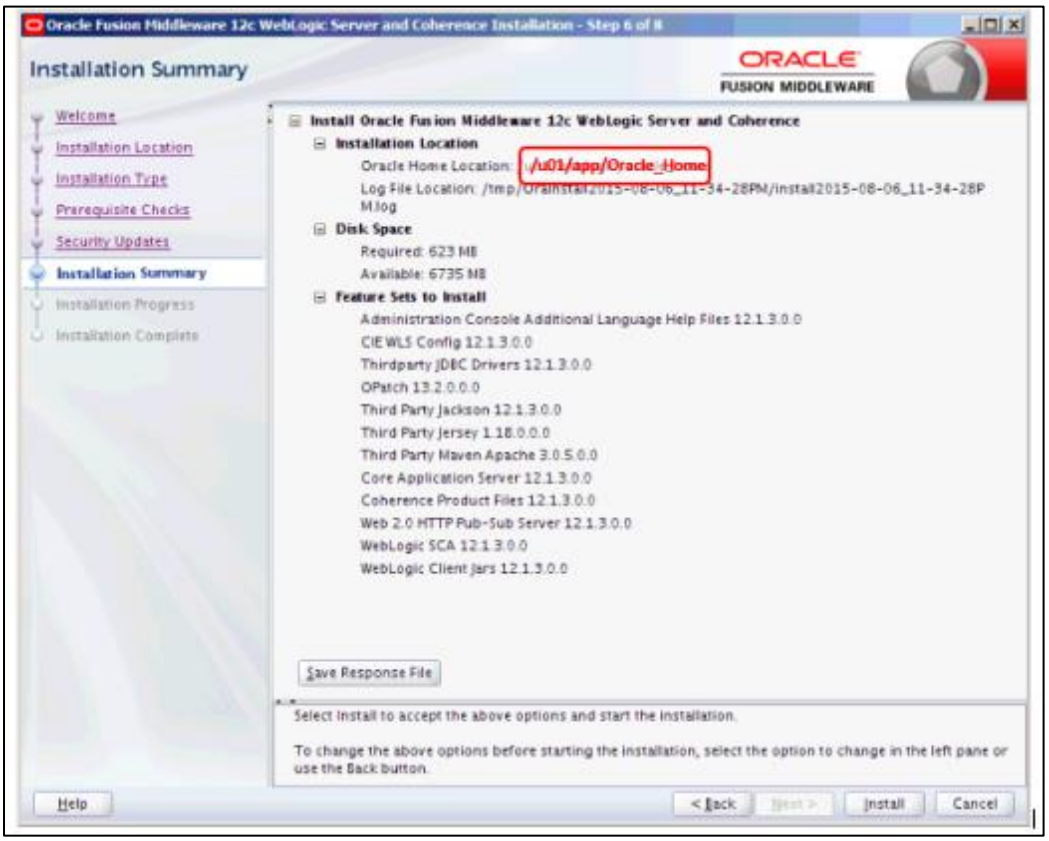
25. Select **Yes** to acknowledge not receiving critical security issues notifications.

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



26. On the *Installation Summary* screen, select **Install**.

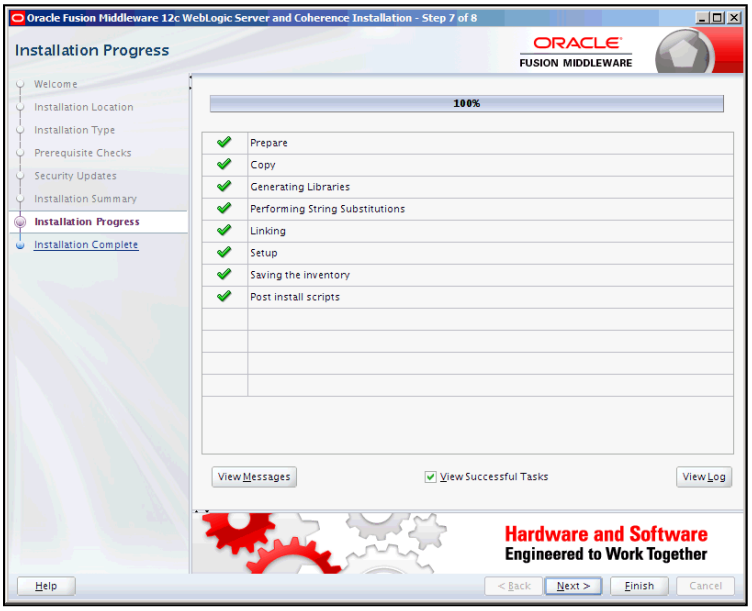
Figure 11: Install WebLogic – Installation Summary Screen



27. Wait while the installation progresses.

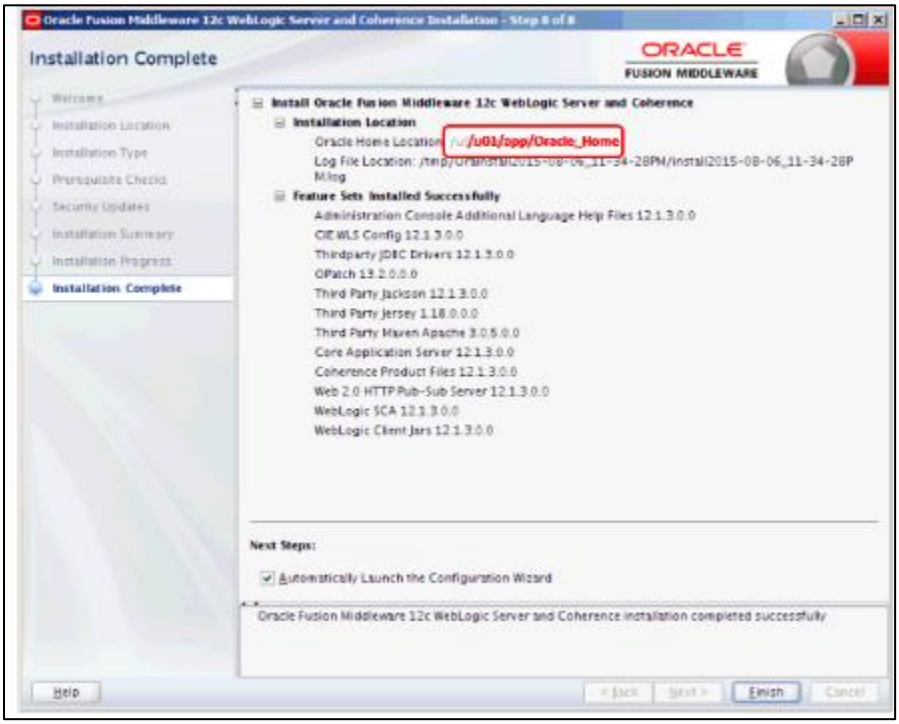
28. Once the installation is complete, the following screen will display.
29. Select **Next**.

Figure 12: Install WebLogic – Installation Progress Screen



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

Figure 13: Install WebLogic – Installation Complete



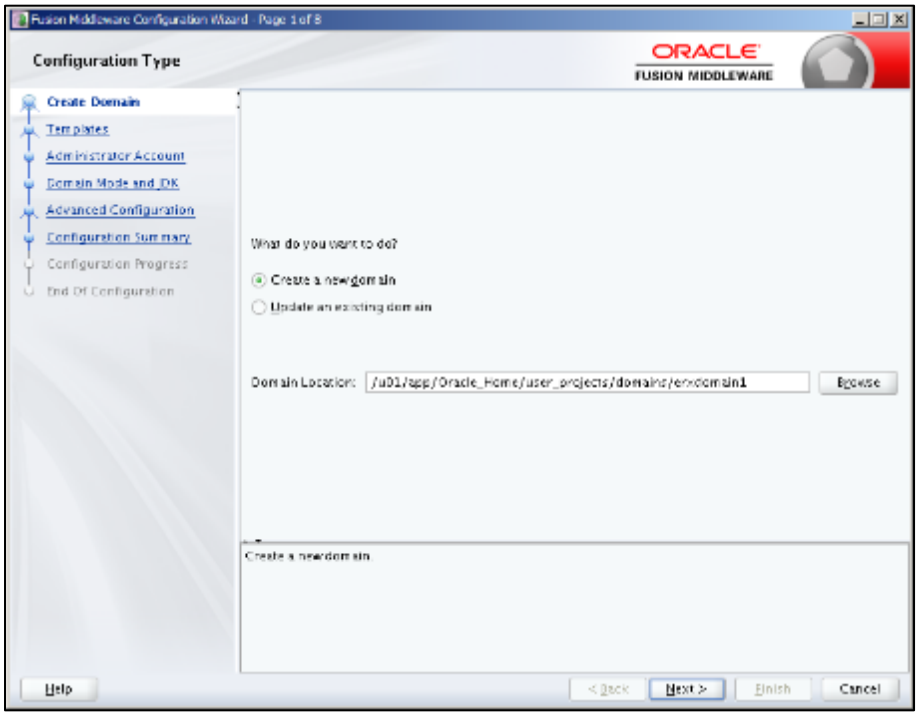
32. The Oracle **Configuration Wizard** splash screen will appear for a few moments.

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*:

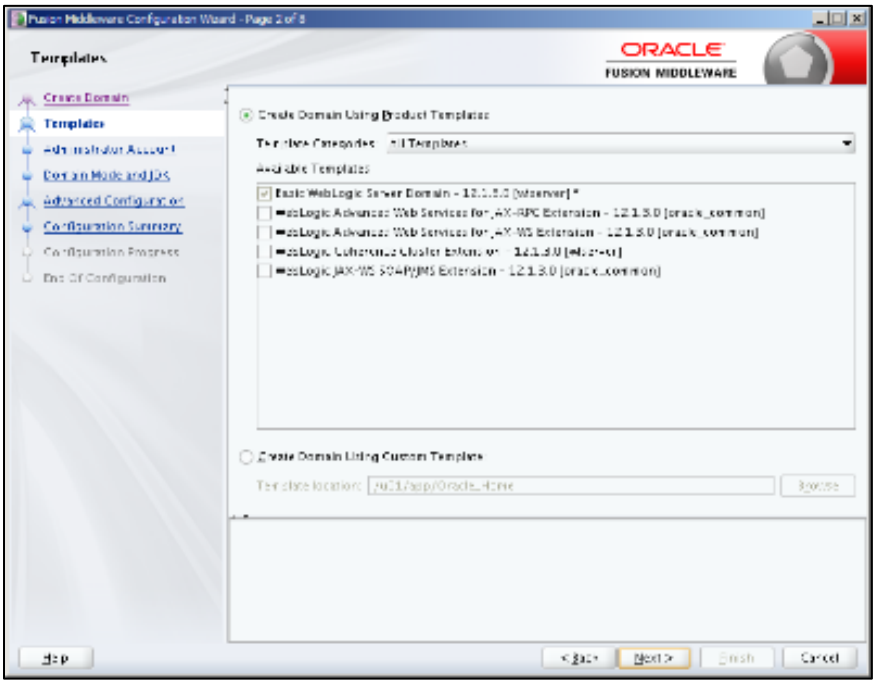
    [ORACLE_BASE]`/user_projects/domains/`***[domain]***
35. Select **Next**.

Figure 15: Install WebLogic – Create New Domain



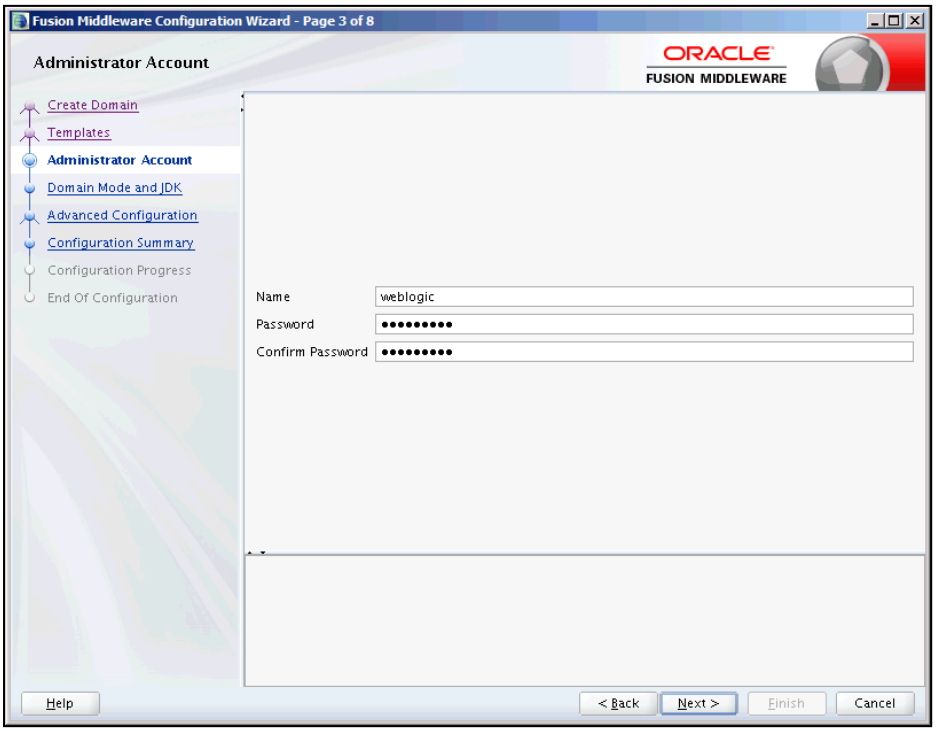
36. On the **Templates** screen, select the *Create Domain using Product Templates* radio button.
37. Under *Available Templates*, select “Basic WebLogic Server Domain”.
38. Select **Next**.

Figure 16: Install WebLogic – Templates Screen



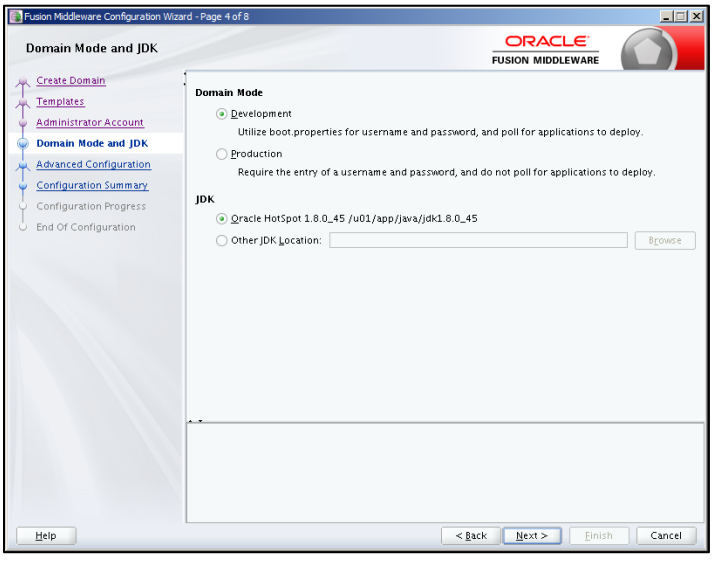
39. On the **Administrator Account** screen, enter *Name*: “weblogic”
40. Enter *Password*: “xxxxxxxx”
41. Enter *Confirm Password*: “xxxxxxxx”
42. Select **Next**.

Figure 17: Install WebLogic – Administrator Account Screen



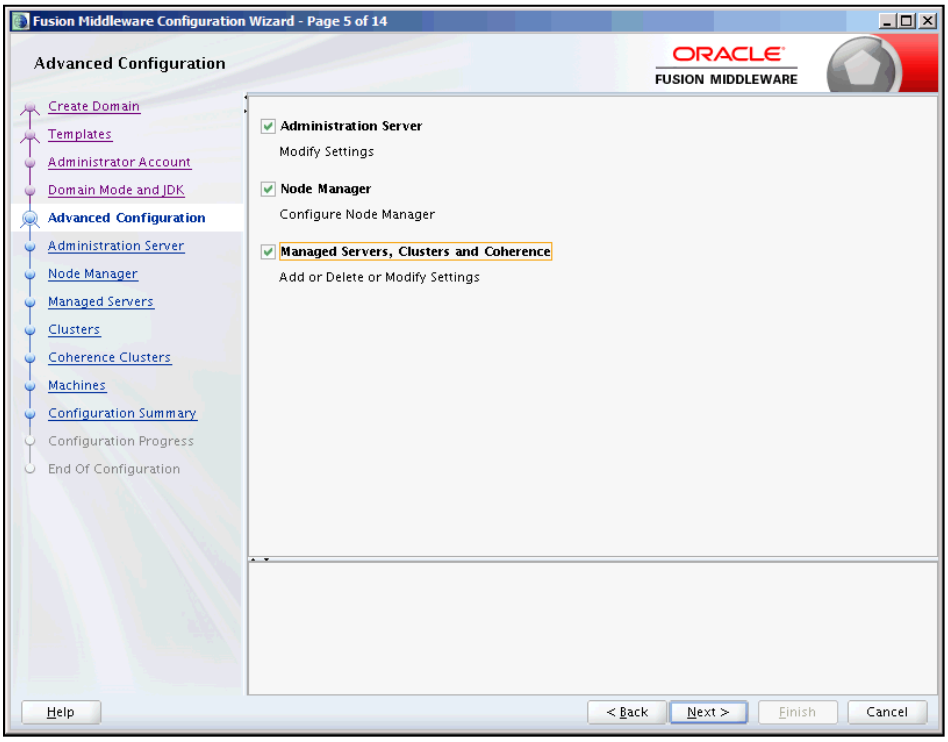
43. On the **Domain Mode and JDK** screen, select the *Development* radio button for the *Domain Mode*.
44. For *JDK*, select the *Oracle HotSpot 1.8.0_xxx* radio button.
45. Select **Next**.

Figure 18: Install WebLogic - Domain Mode and JDK



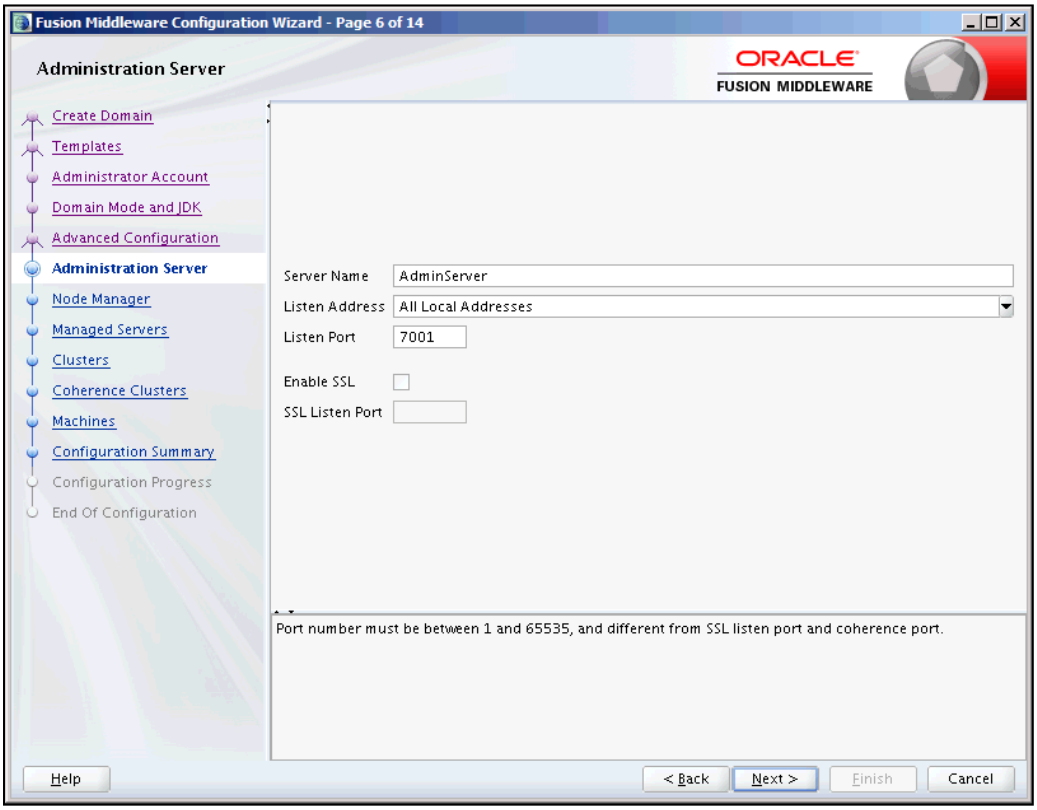
46. On the **Advanced Configuration** screen, check *Administration Server, Node Manager*, and *Managed Servers, Clusters and Coherence*.
47. Select **Next**.

Figure 19: Install WebLogic– Advanced Configuration



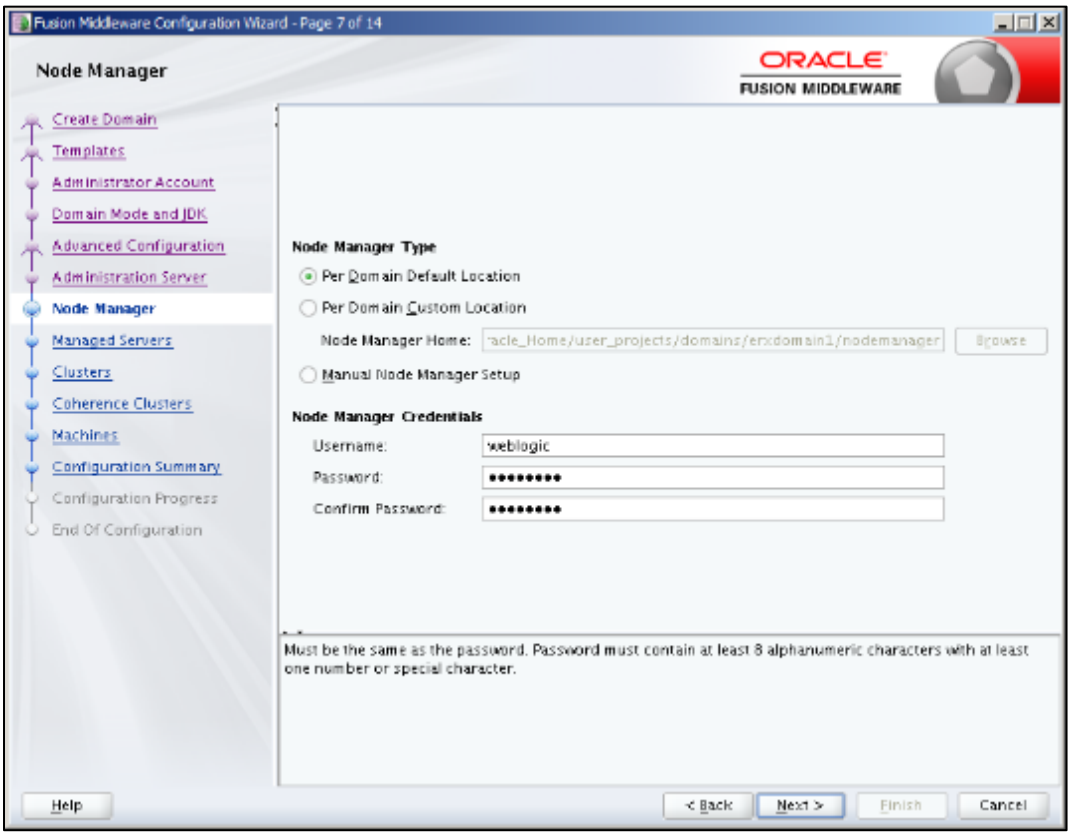
48. On the **Administration Server** screen, enter *Server Name*: “AdminServer”
49. Enter *Listen Address*: “All Local Addresses”
50. Enter *Listen Port*: “7001”
51. Uncheck the check box for *Enable SSL*.
52. Leave the *SSL Listen Port* field blank.
53. Select **Next**.

Figure 20: Install WebLogic – Administration Server Screen



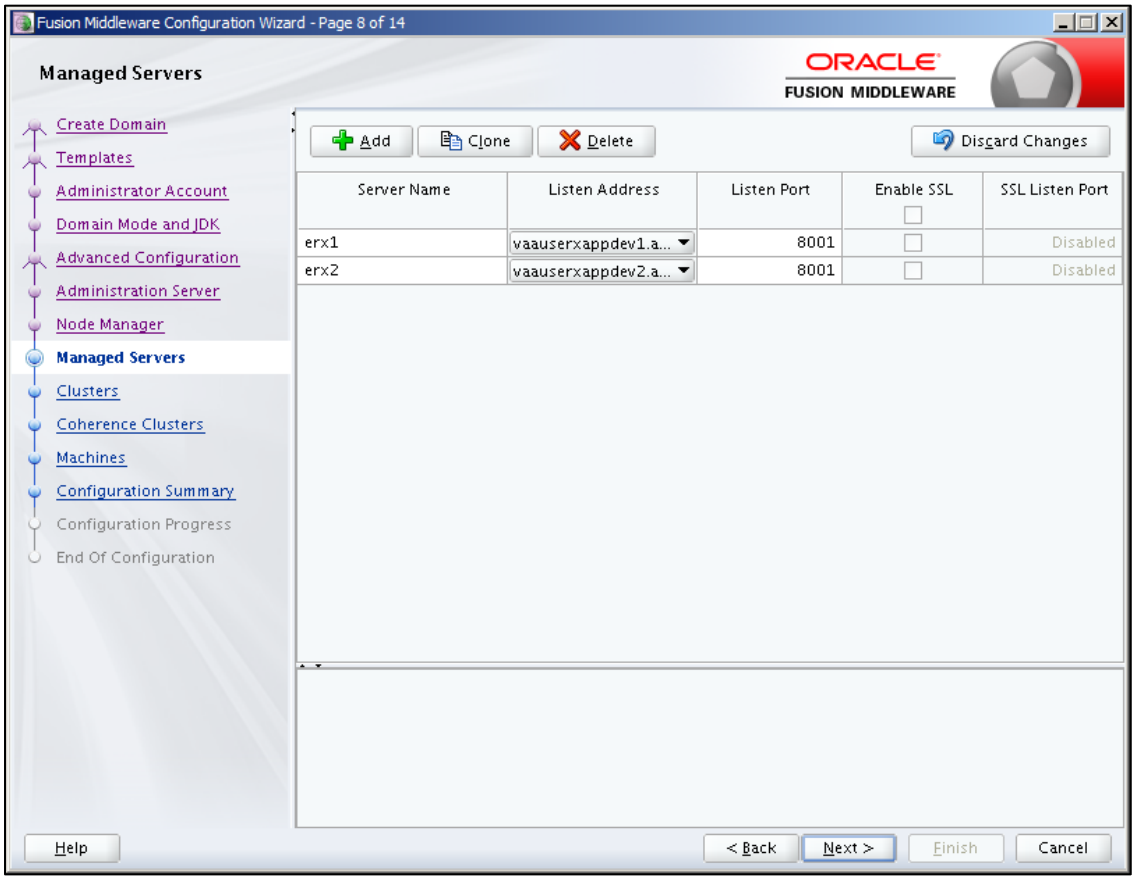
54. On the **Node Manager** screen, select the *Per Domain Default Location* radio button.
55. Enter *Username*: “weblogic”
56. Enter *Password*: “xxxxxxxx”
57. Enter *Confirm Password*: “xxxxxxxx”
58. Select **Next**.

Figure 21: Install WebLogic – Node Manager



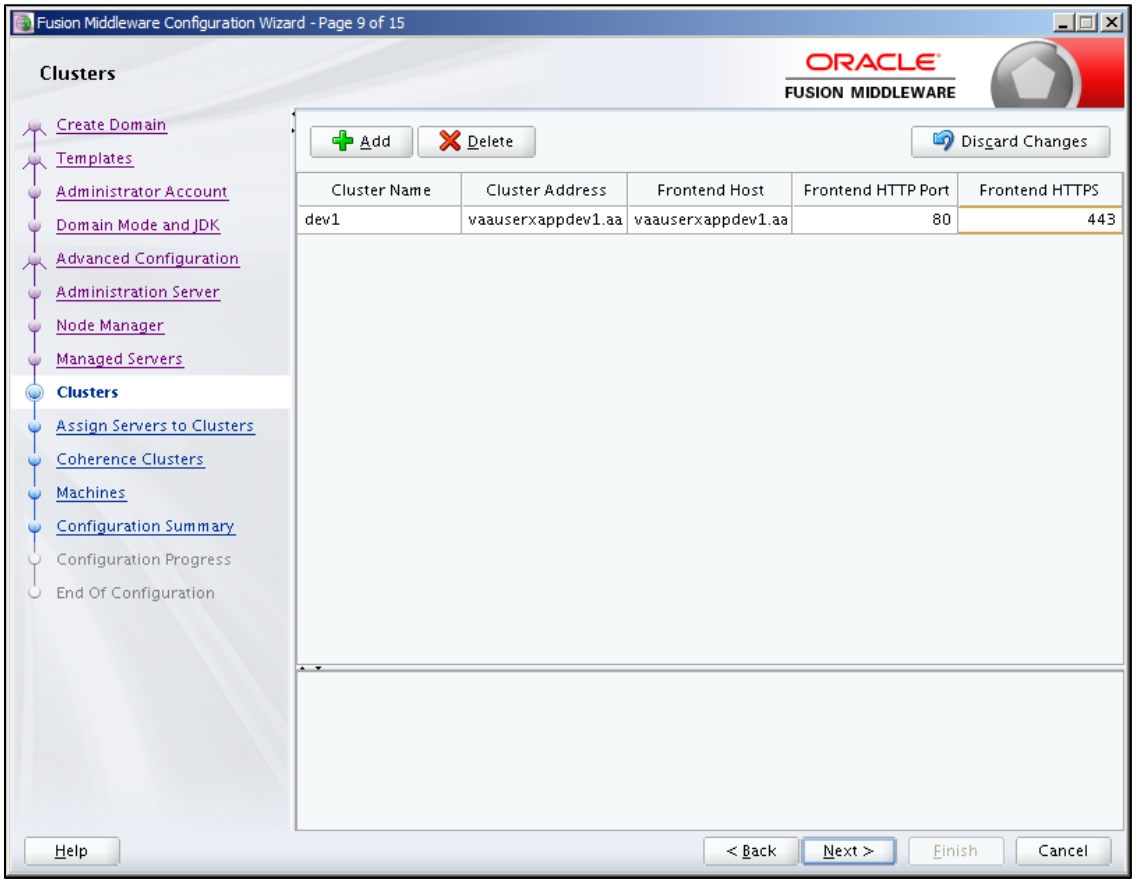
59. On the **Managed Servers** screen, select **Add**.
60. Enter the *Server Name*: “erx1”
61. Enter the *Listen Address*: ***[vm1_fqdn]***
62. Enter *Listen Port*: “8001”
63. Leave *Enable SSL* unchecked.
64. Leave *SSL Listen Port* empty (Disabled).
65. Select **Add**.
66. Enter *Server Name*: “erx2”
67. Enter *Listen Address*: ***[vm2_fqdn]***
68. Enter Listen Port: “8001”
69. Leave *Enable SSL* unchecked.
70. Leave *SSL Listen Port* empty (Disabled).
71. Select **Next**.

Figure 22: Install WebLogic – Managed Servers



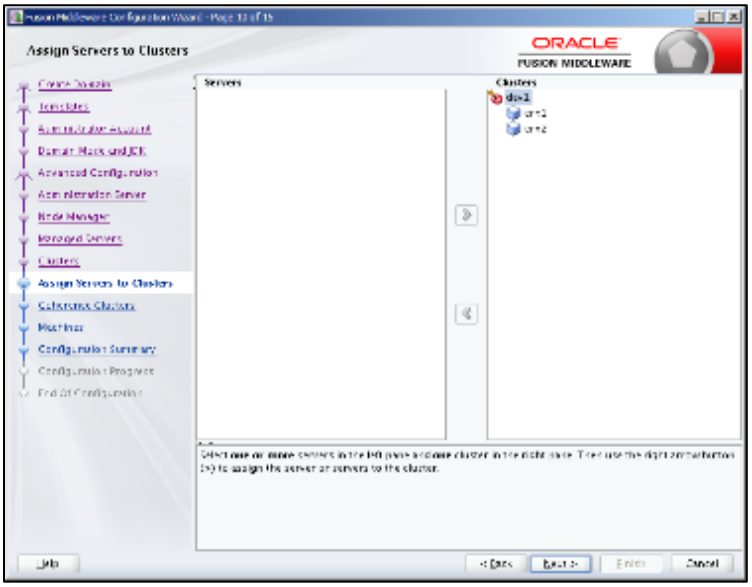
72. On the **Clusters** screen, select **Add**.
73. Enter *Cluster Name*: “erx”
74. Enter *Cluster Address*: “***[vm1_fqdn]***:***[erx_port]***, ***[vm2_fqdn***]:***[erx_port]***”
75. Enter *Frontend Host*: “***[proxy_fqdn]***”
76. Enter *Frontend HTTP Port*: “80”
77. Enter *Frontend HTTPS*: “443”
78. Select **Next**.

Figure 23: Install WebLogic – Clusters



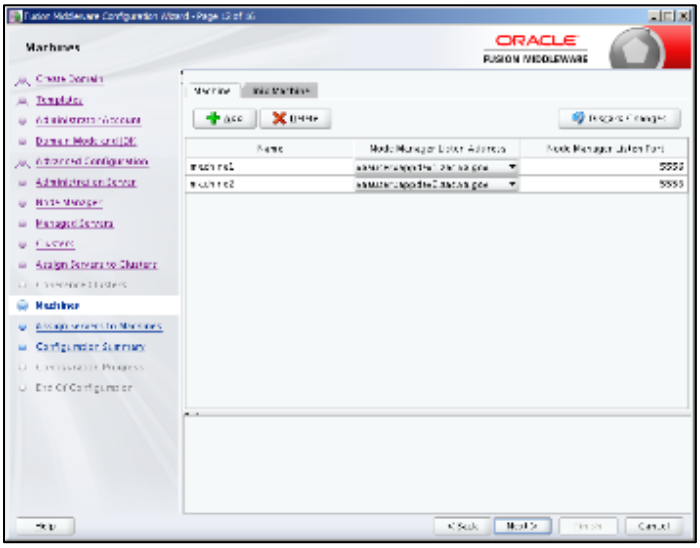
79. Assign “erx1” and “erx2” servers to the “erx” cluster.
80. Select **Next**.

Figure 24: Install WebLogic – Assign Servers to Clusters



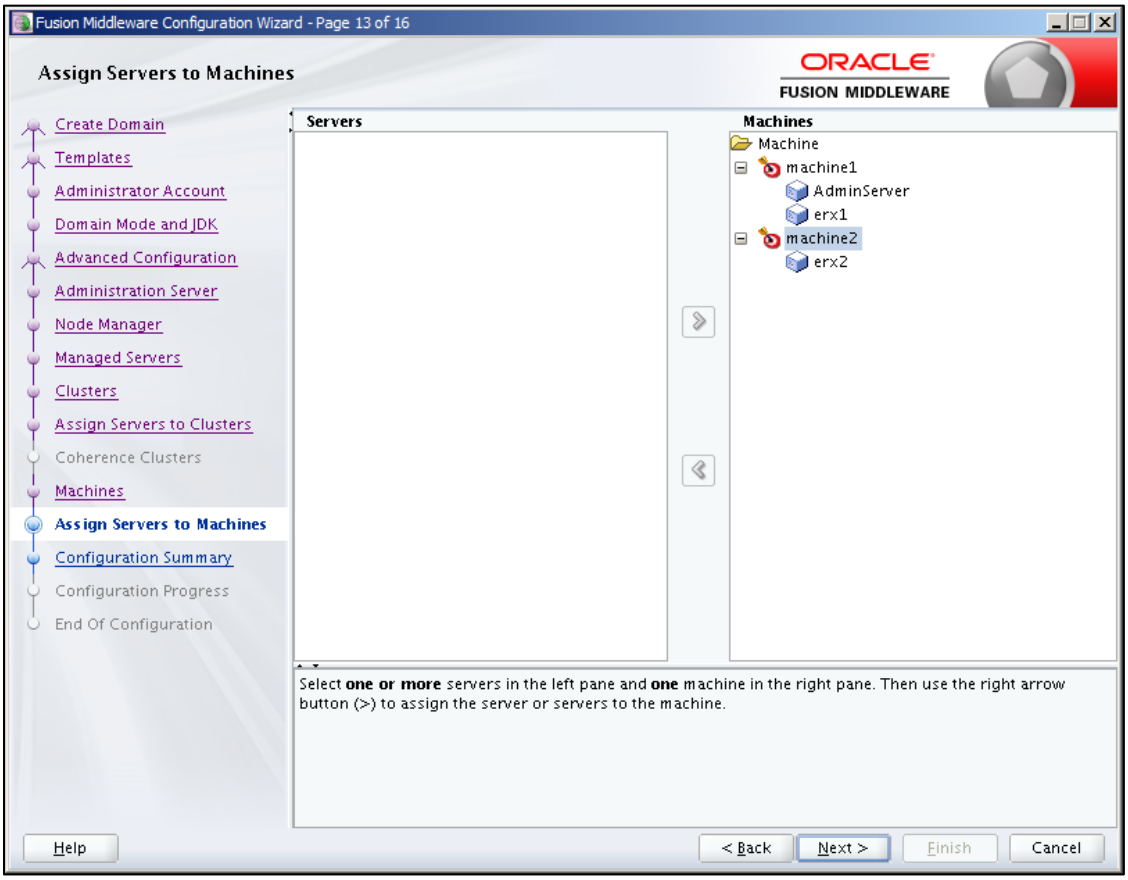
81. Select **Add**.
82. Enter *Name*: “machine1”
83. Enter *Node Manager Listen Address*: “***[vm1_fqdn]***”
84. Enter *Node Manager Listen Port*: “5556”
85. Enter *Name*: “machine2”
86. Enter *Node Manager Listen Address*: “***[vm1_fqdn]***”
87. Enter *Node Manager Listen Port*: “5556”
88. Select **Next**.

Figure 25: Install WebLogic – Machines



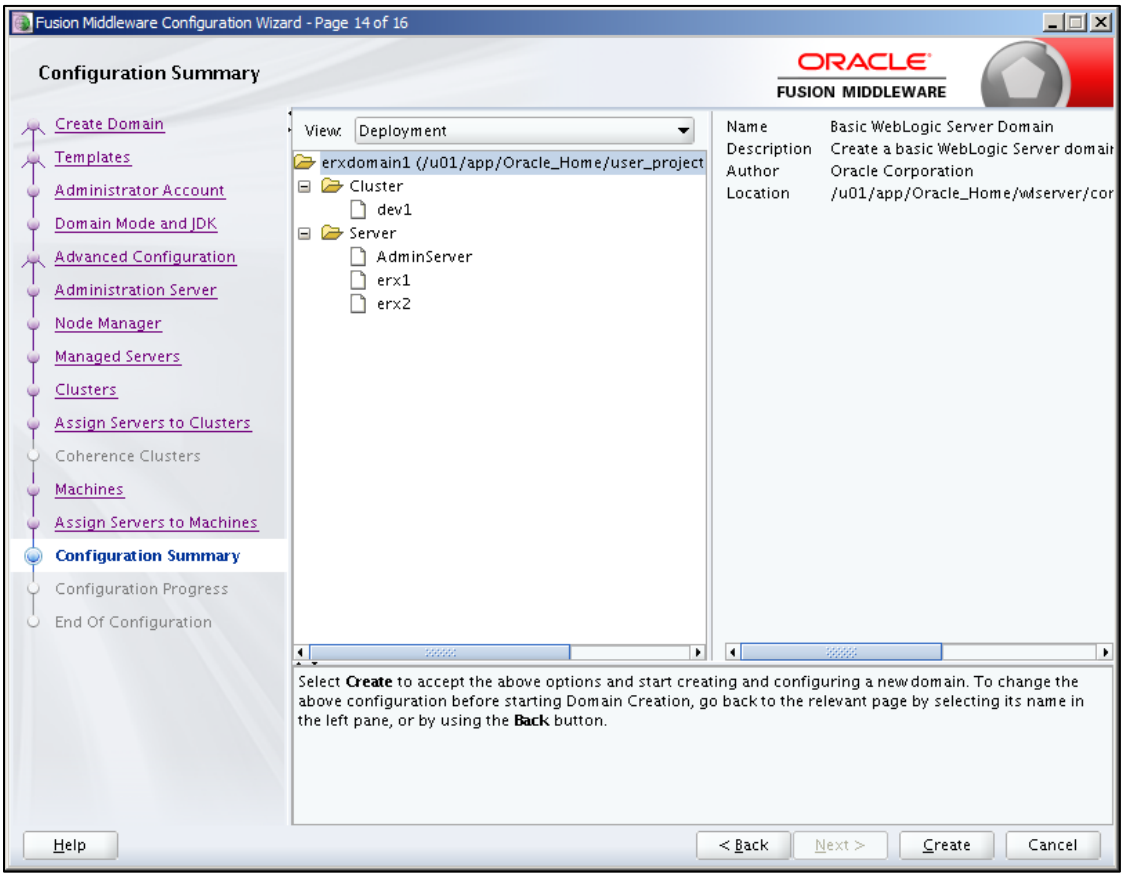
89. On the **Assign Servers to Machines** screen, add “AdminServer” on *Servers* panel to “machine1” on *Machines* panel.
90. Add “erx1” on *Servers* panel to “machine1” on *Machines* panel.
91. Add “erx2” on *Servers* panel to “machine2” on *Machines* panel.
92. Select **Next**.

Figure 26: Install WebLogic – Assign Servers to Machines



93. On the **Configuration Summary** screen, select **Create** to accept the options and start creating and configuring the new domain.

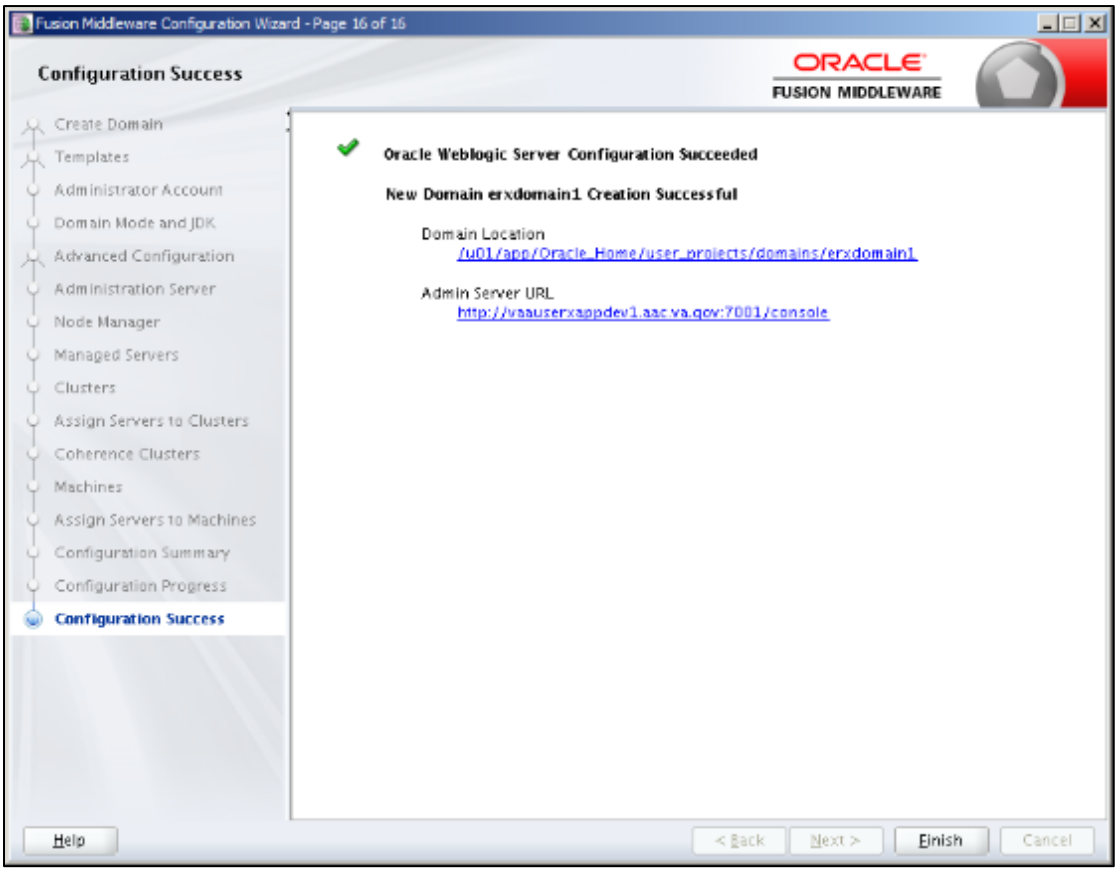
Figure 27: Install WebLogic – Configuration Summary Screen



94. Once the configuration is complete, select **Next**.

95. If the configuration is successful, the **Configuration Success** screen will display as illustrated in the figure below.
96. Select **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 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]
CustomIdentityKeyStoreType=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]/module
s/com.oracle.weblogic.jpa21support_1.0.0.0_2-1.jar
export PRE_CLASSPATH
```

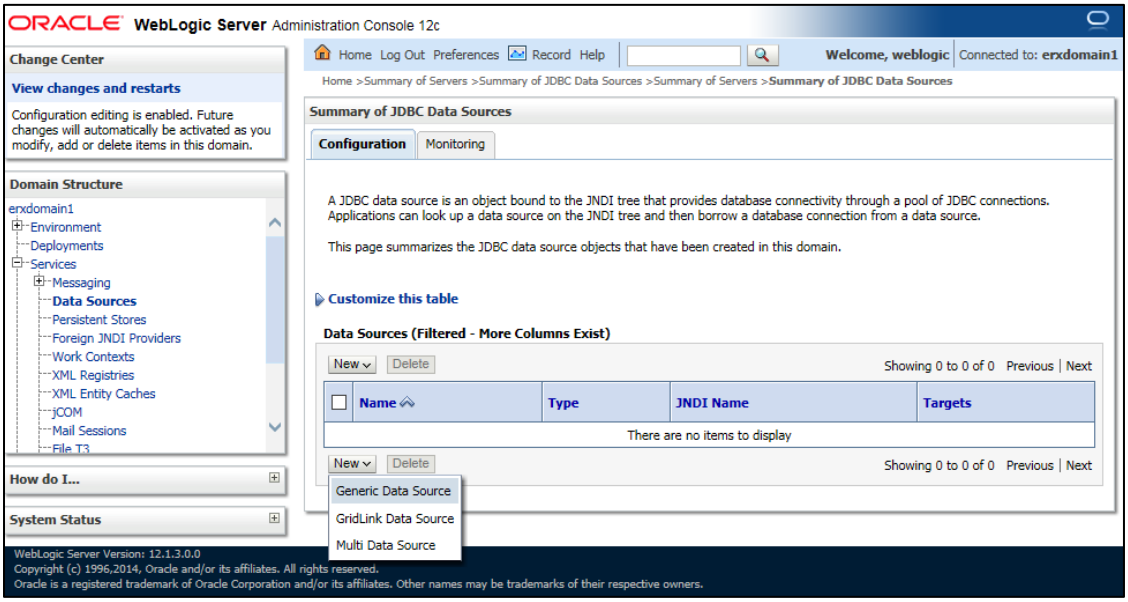
Enter :wq to save the file and exit vi.

4.8.1.11 Create Inbound eRx Datasource

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

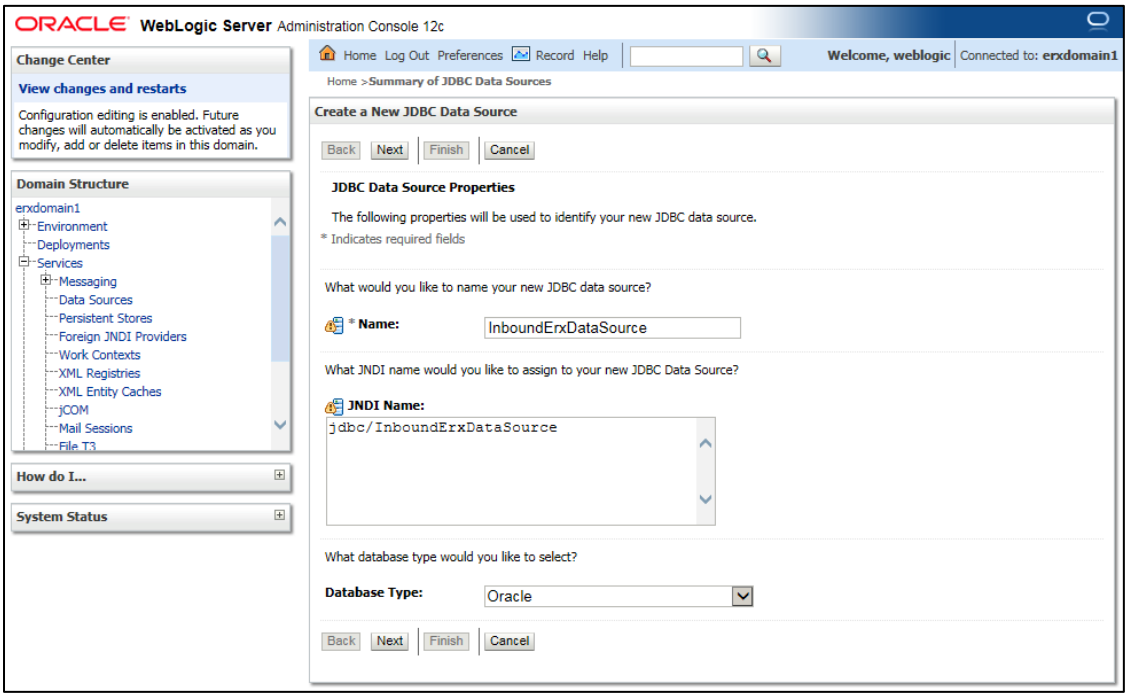
1. Navigate to *Services*, then to *Data Sources*.
2. From the *Data Source*s page, select **New**.

Figure 29: Create Inbound eRx Datasource – Datasources



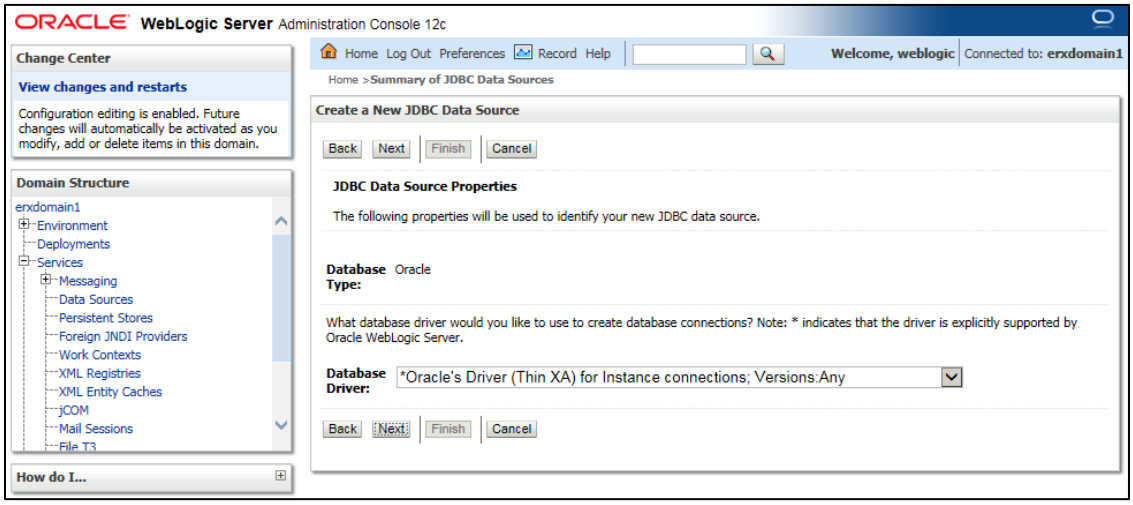
3. Enter *Name*: **InboundErxDataSource**
4. Enter *JNDI Name*: **jdbc/InboundErxDataSource**
5. Select *Database Type*: **Oracle**
6. Select **Next**.

Figure 30: Create Inbound eRx Datasource – Datasource Properties



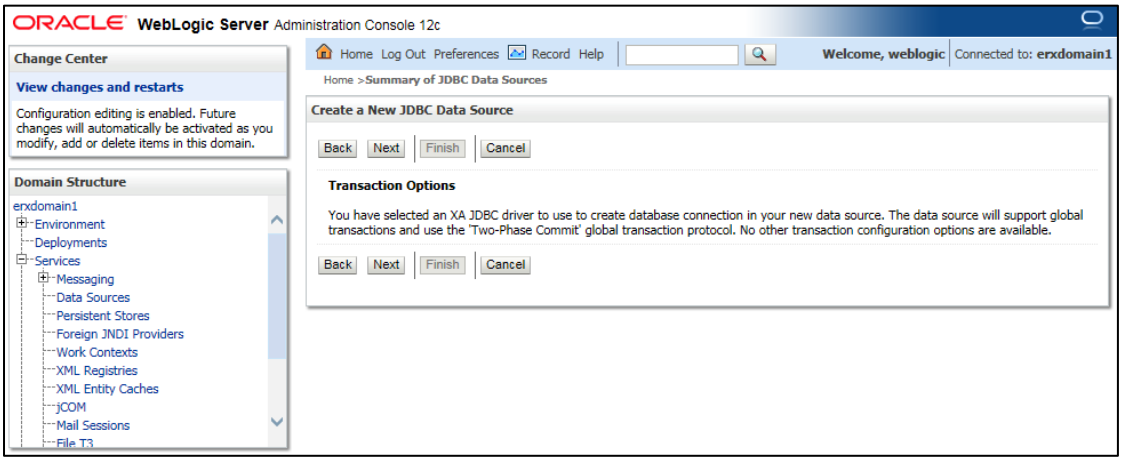
7. Select *Database Driver*: **Oracle's Driver (Thin XA) for Instance connections; Versions: Any**
8. Select Next.

Figure 31: Create Inbound eRx Datasource – Database Driver



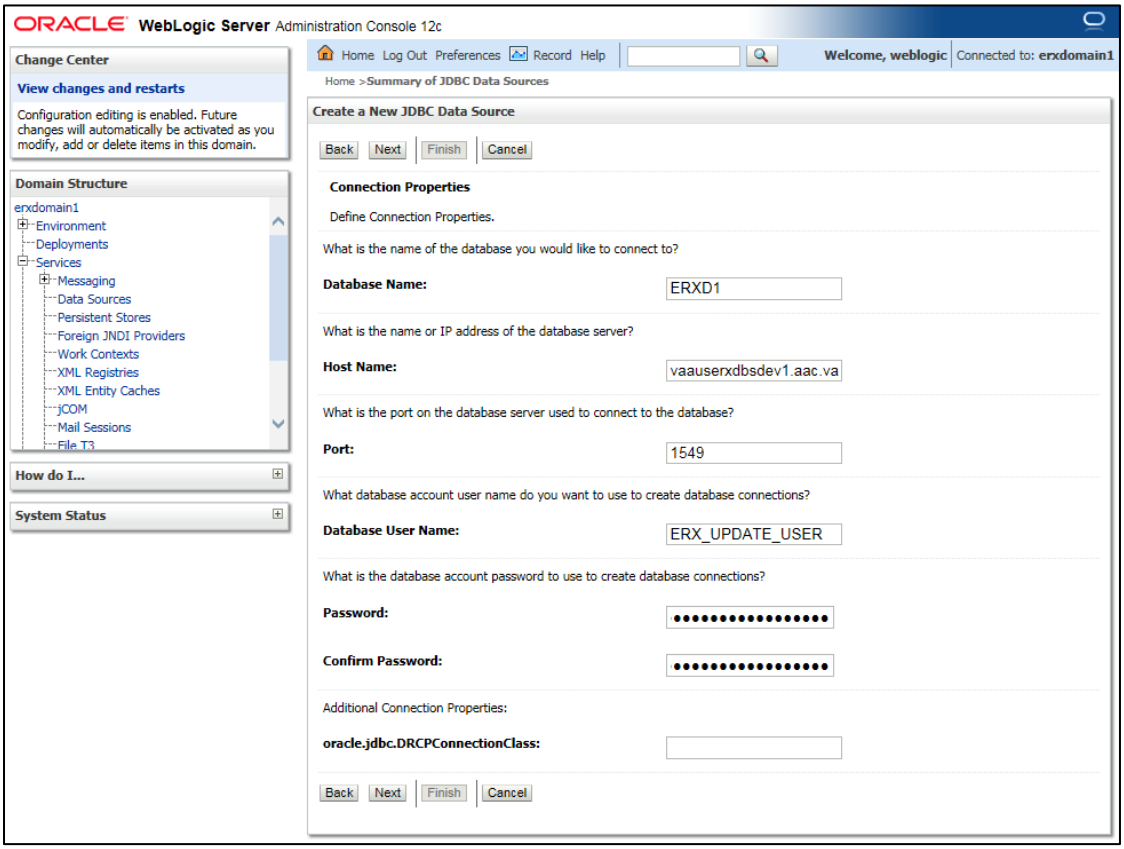
9. Select **Next**.

Figure 32: Create Inbound eRx Datasource – Transaction Properties



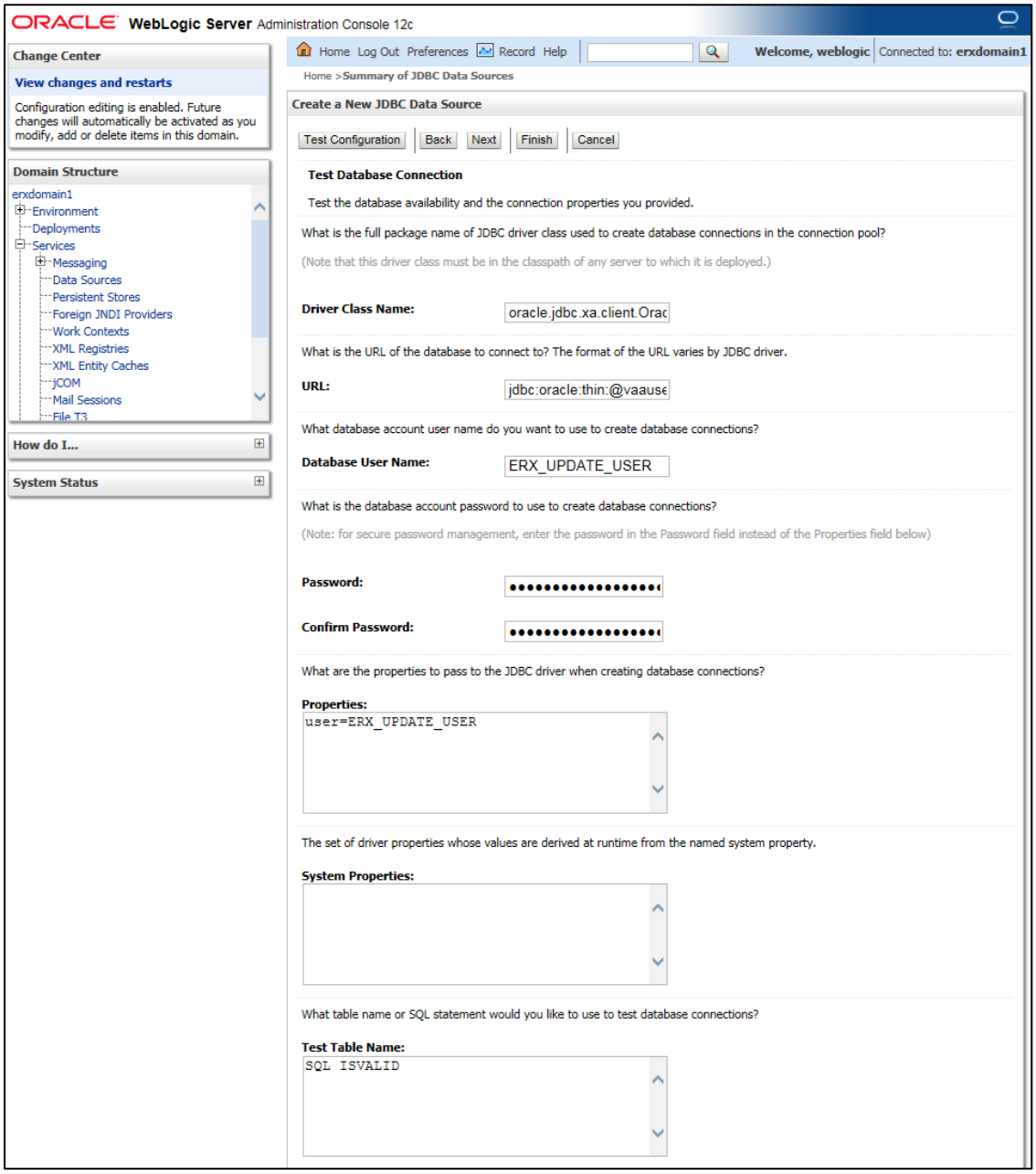
10. Enter *Database Name*: **[DB_NAME]**
11. Enter *Host Name*: **[DB_FQDN]**
12. Enter *JNDI Name*: **jdbc/InboundErxDataSource**
13. Enter *Port*: **[DB_PORT]**
14. Enter *Password*: **[DB_PASSWORD]**
15. Enter *Confirm Password*: **[DB_PASSWORD]**

Figure 33: Create Inbound eRx Datasource – Connection Properties



16. Select **Test Configuration**.
17. If test is not successful, select **Back** and correct settings, otherwise select **Next**.

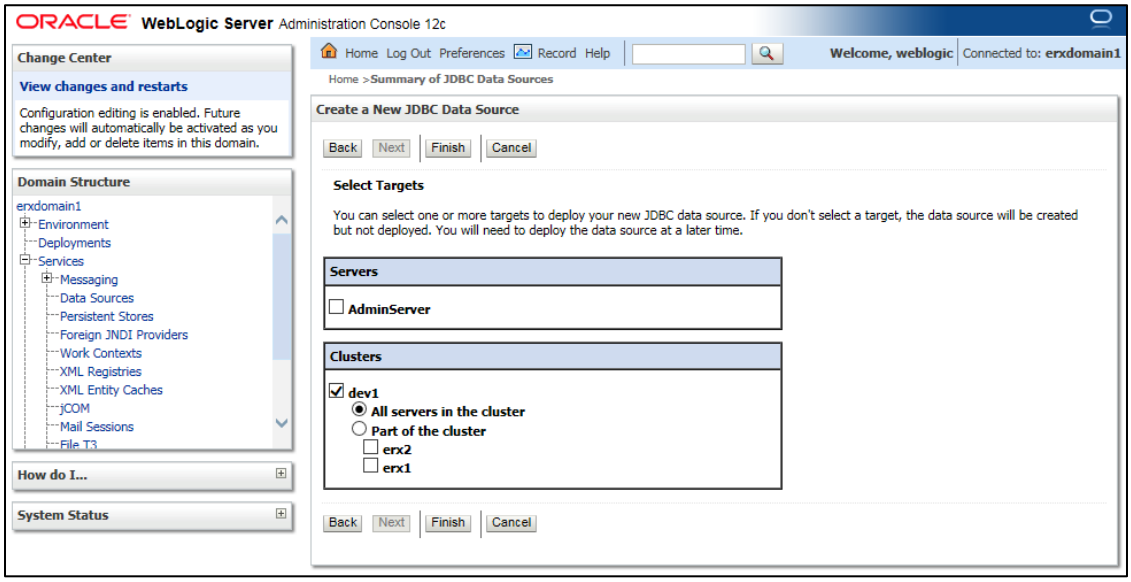
Figure 34: Create Inbound eRx Datasource – Test Connection



18. Select **All servers in the cluster**.

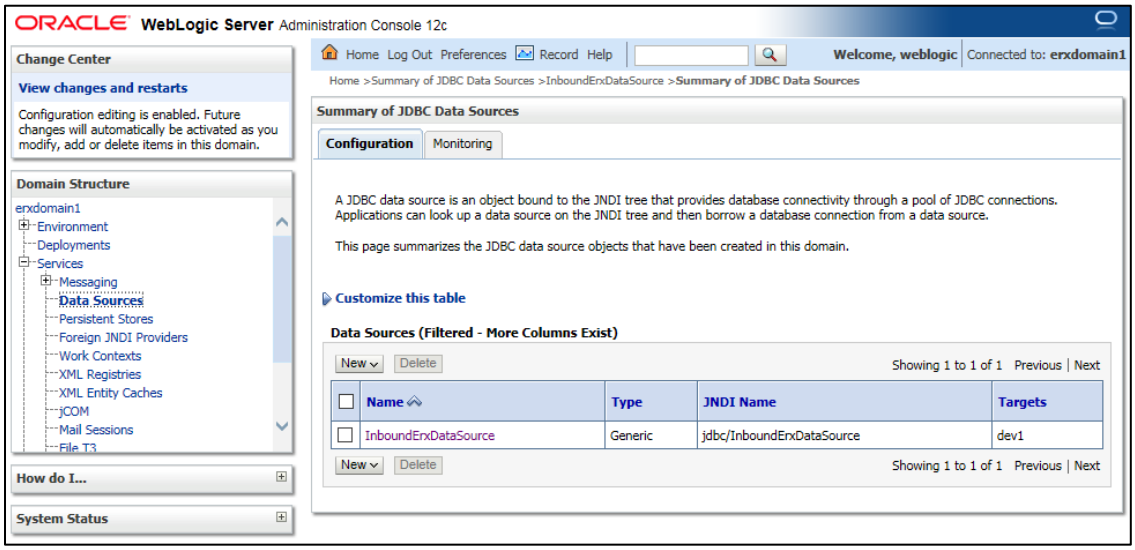
19. Select **Finish**.

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



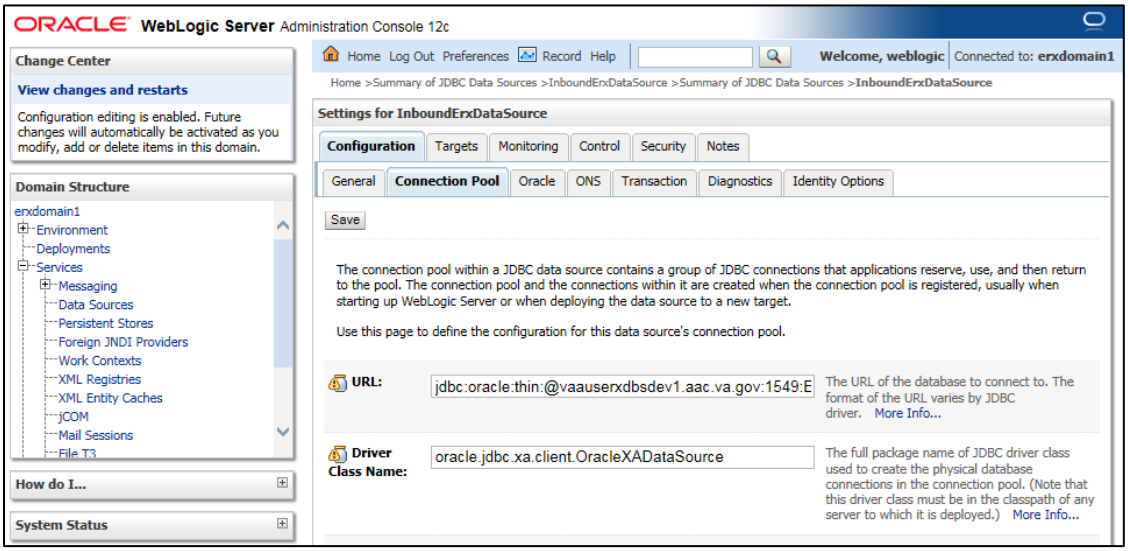
20. Select **InboundErxDataSource** hyperlink.

Figure 36: Create Inbound eRx Datasource – Modify New Datasource



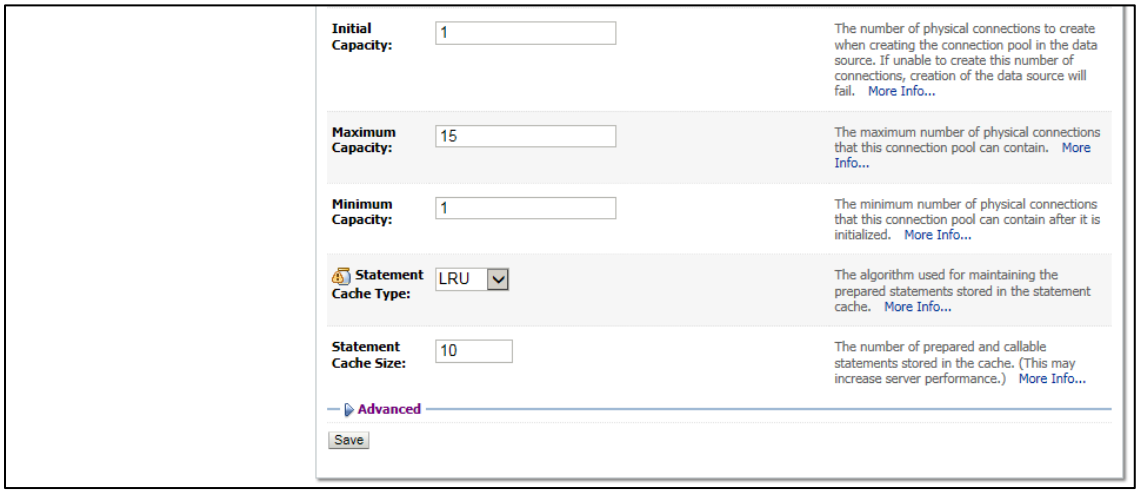
21. Select the **Connection Pool** tab.

Figure 37: Inbound eRx Datasource –Connection Pool Properties



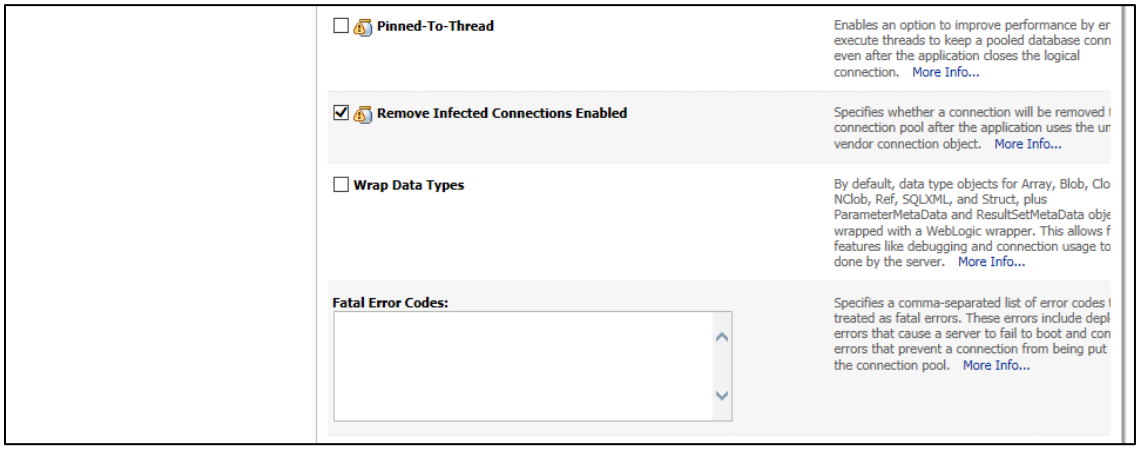
22. Scroll to the bottom of the **Connection Pool** page.
23. Select the **Advanced** hyperlink to expand the advanced properties.

Figure 38: Inbound eRx Datasource –Connection Pool Advanced Properties



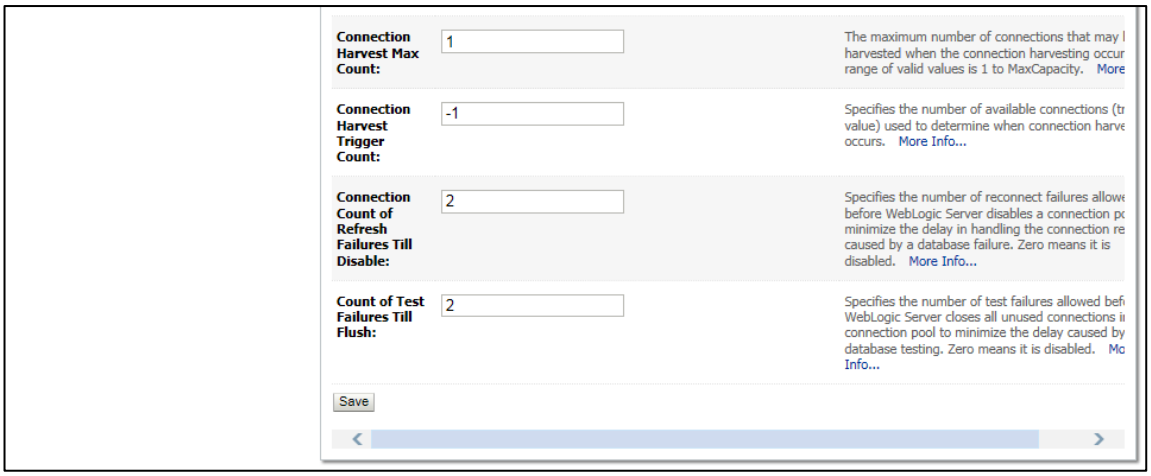
24. Scroll down and uncheck the **Wrap Data Types** property.

Figure 39: Inbound eRx Datasource – Wrap Data Type Property



25. Scroll to the bottom of the of the **Advanced Connection Pool** page.
26. Select **Save**.

Figure 40: Inbound eRx Datasource – Save Properties

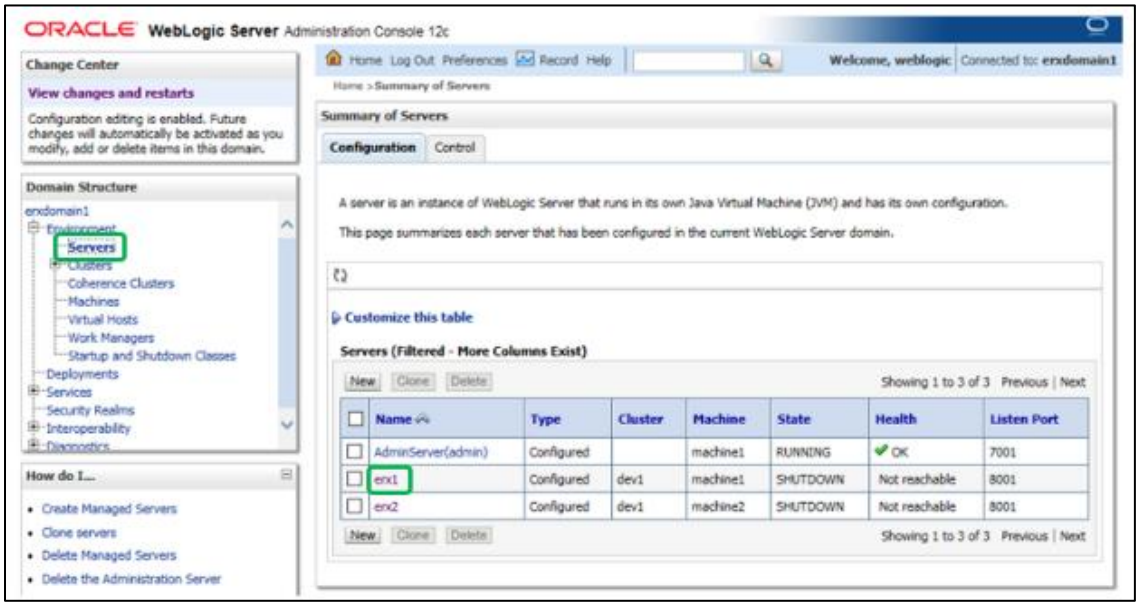


4.8.1.12 Configure Identity/Trust Store File on Managed Servers

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

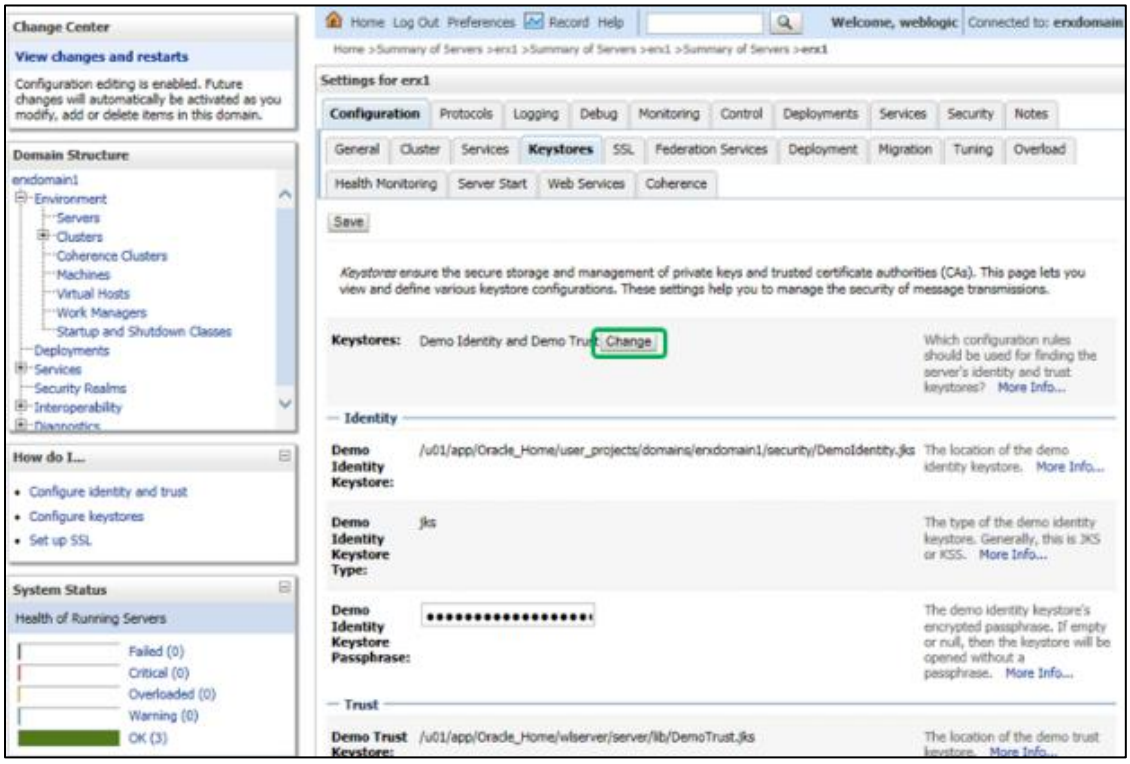
1. Under **Domain Structure**, navigate to **Servers**.
2. Select the **erx1** link to access the server configuration page in the **Administration Console**.

Figure 41: Configure Identity/Trust Store File – Access Server Configuration Page



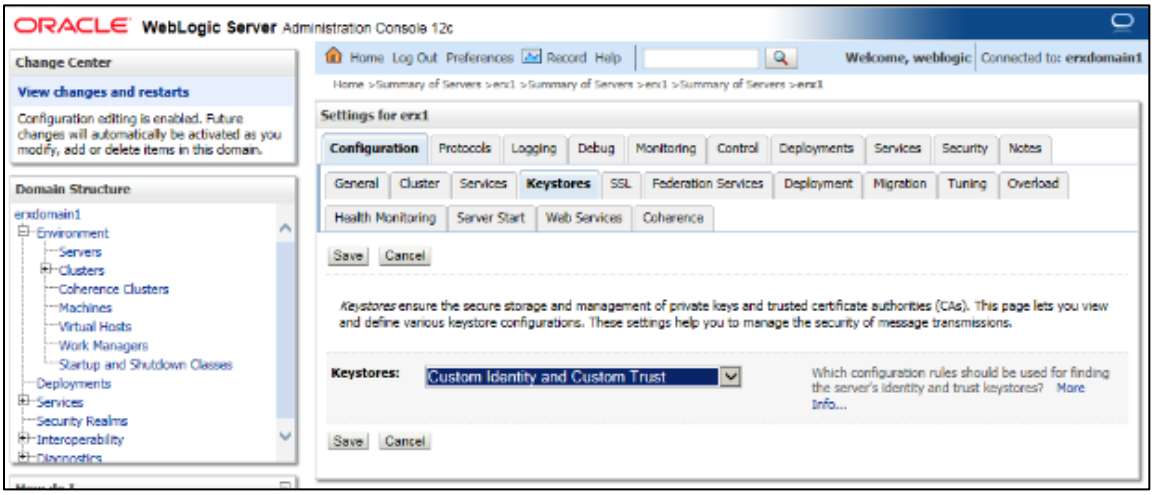
3. Under **Configuration** > **Keystores**, select **Change**.

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



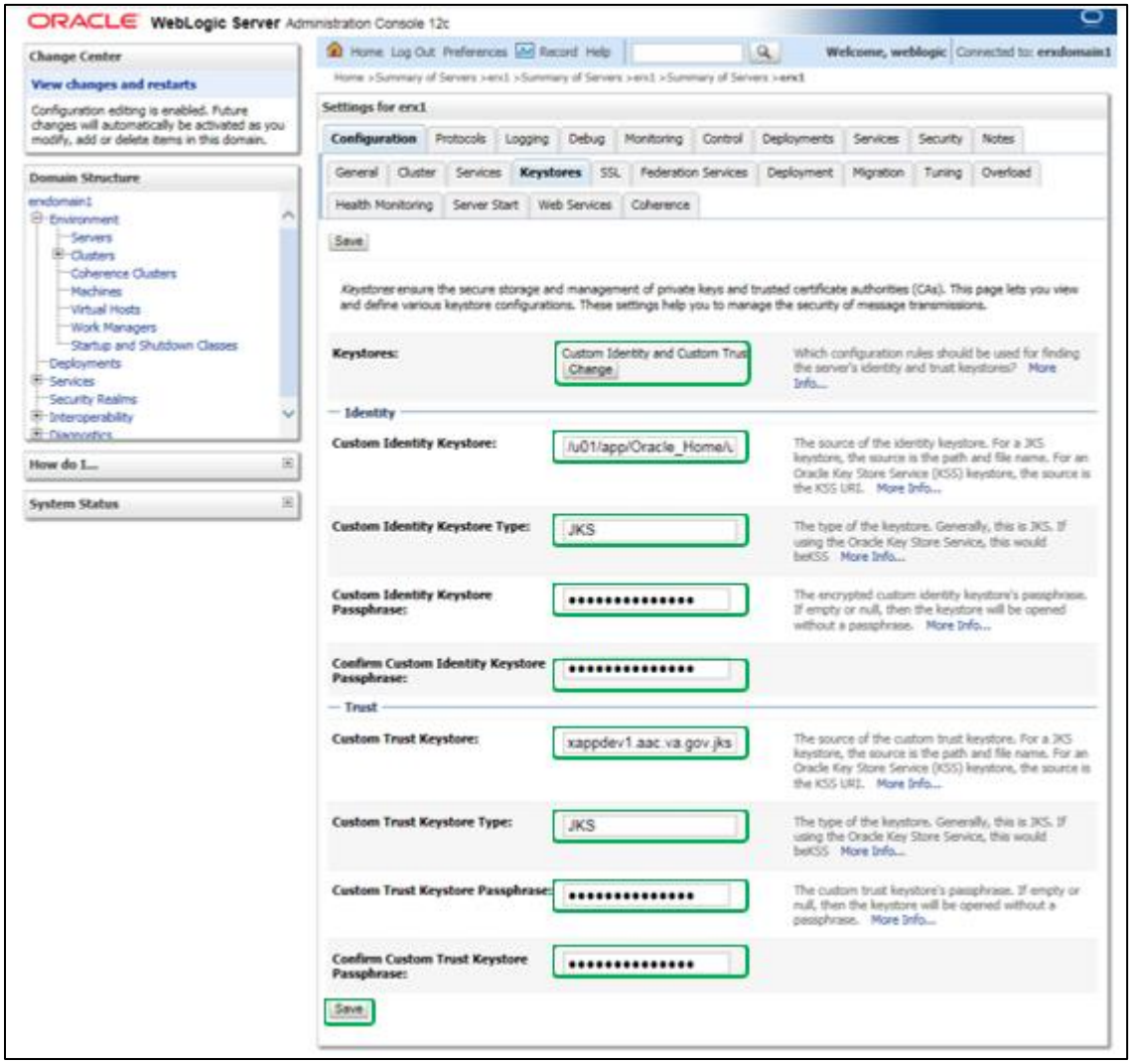
4. For *Keystores*, select **Custom Identity and Custom Trust**.
5. Select **Save**.

Figure 43: Configure Identity/Trust Store File – Keystores – Select Custom Identify and Custom Trust



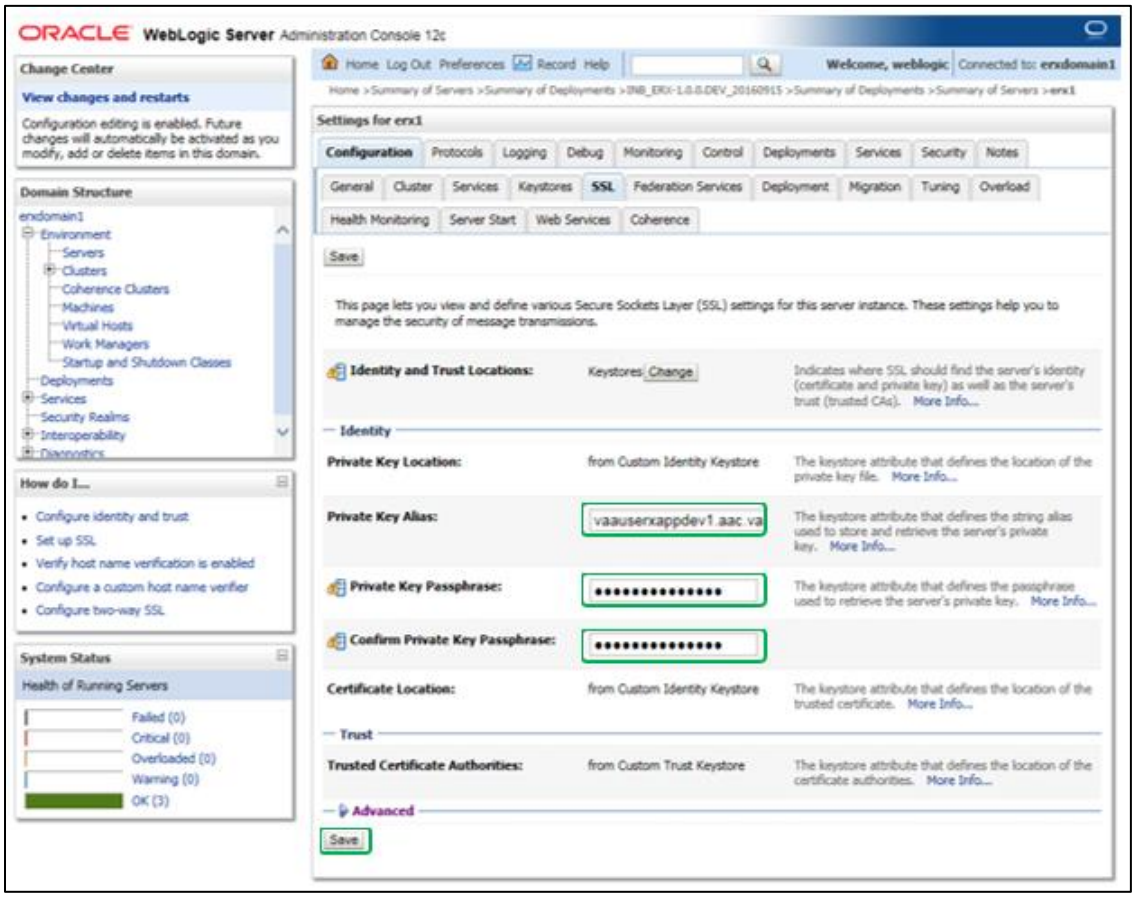
6. Modify the setting under the **Keystores** tab as illustrated in the figure below. The *Custom Identity Keystore* and *Custom Trust Keystore* use the same file path to the keystore file copied to the Domain "security" directory: (***[DOMAIN_HOME]***/security/***[proxy_fqdn]***.jks).

Figure 44: Configure Identity/Trust Store File – Modify Keystore Settings



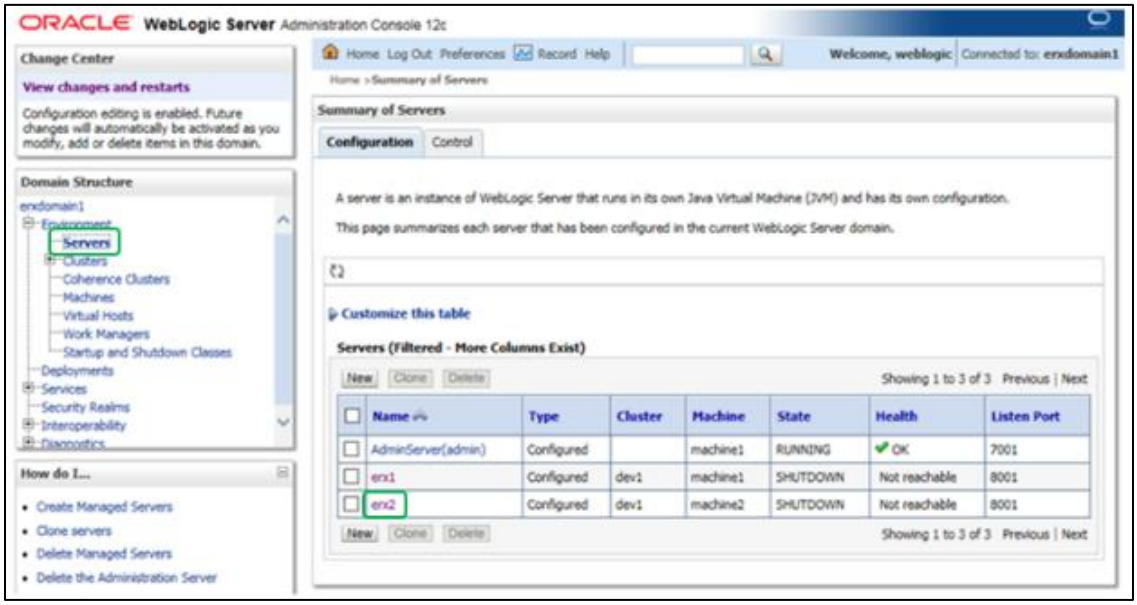
7. Modify the setting under the **SSL** tab as illustrated in the figure below. For the *Private Key Alias*, enter **[proxy_fqdn]**.
8. Enter and confirm the *Private Key Passphrase*.
9. Select **Save**.

Figure 45: Configure Identity/Trust Store File – Modify SSL Settings



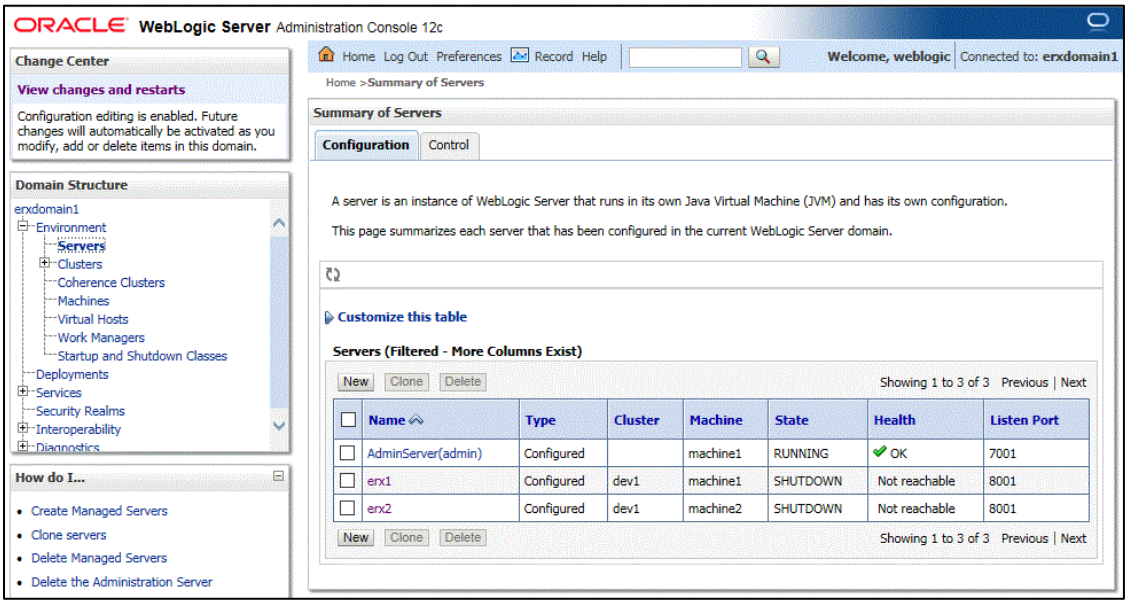
10. Navigate to *Servers*, and then select the **erx2** link to access the server configuration page in the **Administration Console**.
11. Repeat the Keystore configuration steps for **erx2** as described earlier in this section for **erx1**.

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



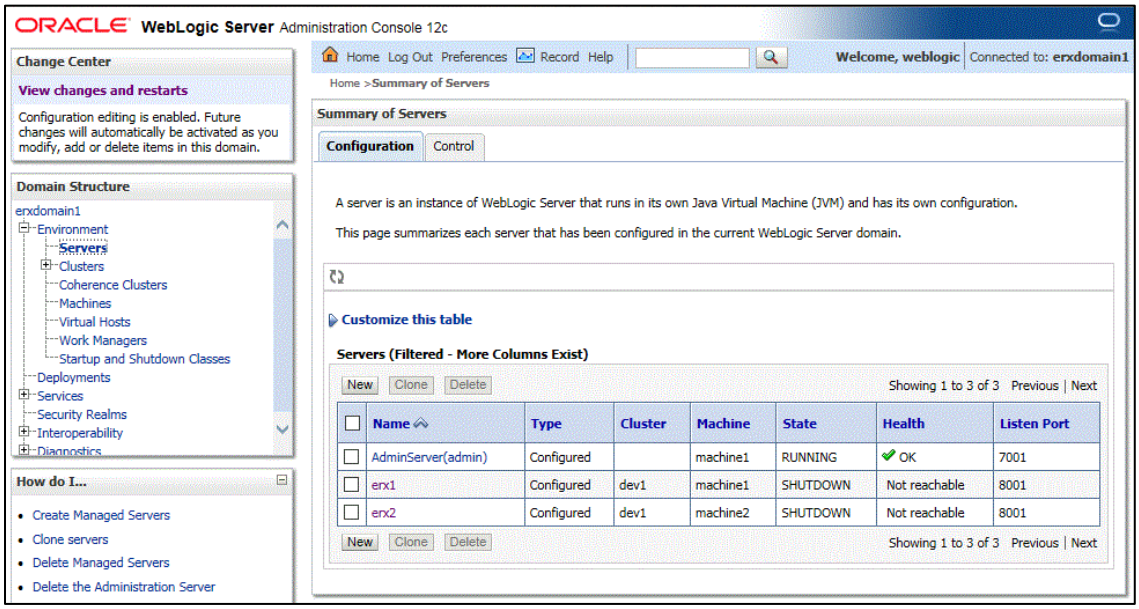
12. Navigate to *Servers*, and then select the **AdminServer(admin)** hyperlink to access the server configuration page.
13. Repeat the Keystore configuration steps for **AdminServer(admin)** as described earlier in this section for **erx1**.

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



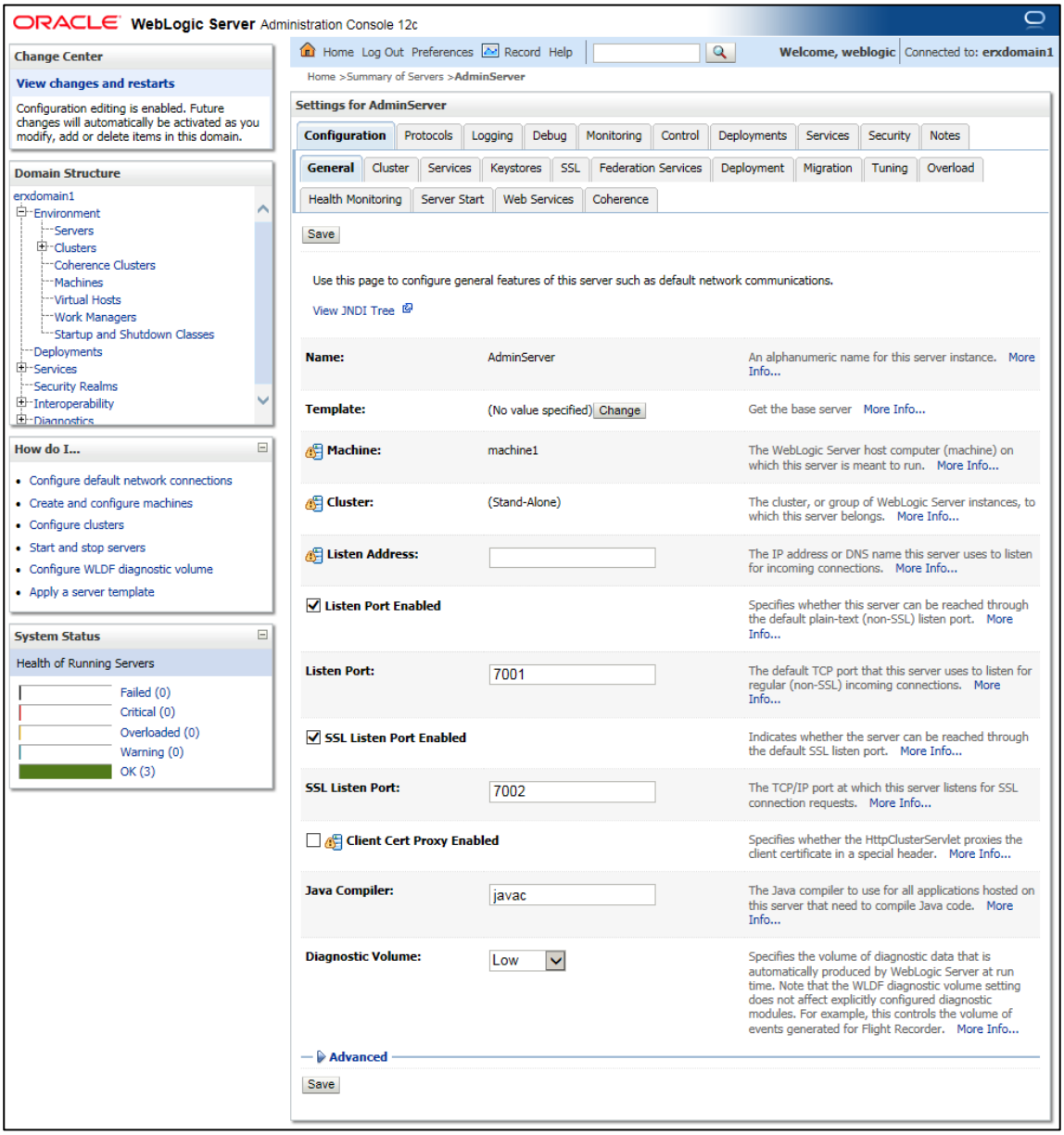
14. Navigate to *Servers*, and then select the **AdminServer(admin)** hyperlink to access the server configuration page.

Figure 48: Configure Identity/Trust Store File – Admin Server Configuration



15. Under **Configuration** and **General** tabs:
    a. Check **Listen Port Enabled**
    b. Enter *Listen Port:* **7001**
    c. Check **SSL Port Enabled**
    d. Enter *SSL Listen Port:* **7002**
    e. Select **Save**.

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. 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 -
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.

```
> connect('weblogic', '########', 't3s://[vm1_fqdn]:7002')
> nmEnroll('[DOMAIN_HOME]', '[DOMAIN_HOME]/nodemanager')
> disconnect()
> exit()
```

4. Check that the "$ORACLE_BASE/domain-registry.xml" file contains an entry like the following. If it doesn't, add it manually.

```
<domain location="[DOMAIN_HOME]"/>
```

5. Check that 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 has not been started already 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 select the *Machines* node.
3. In the right-hand pane, select on the first WebLogic machine (machine1).
4. Select the **Monitoring** tab. Be patient. This may take some time the first time it's done.
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
```

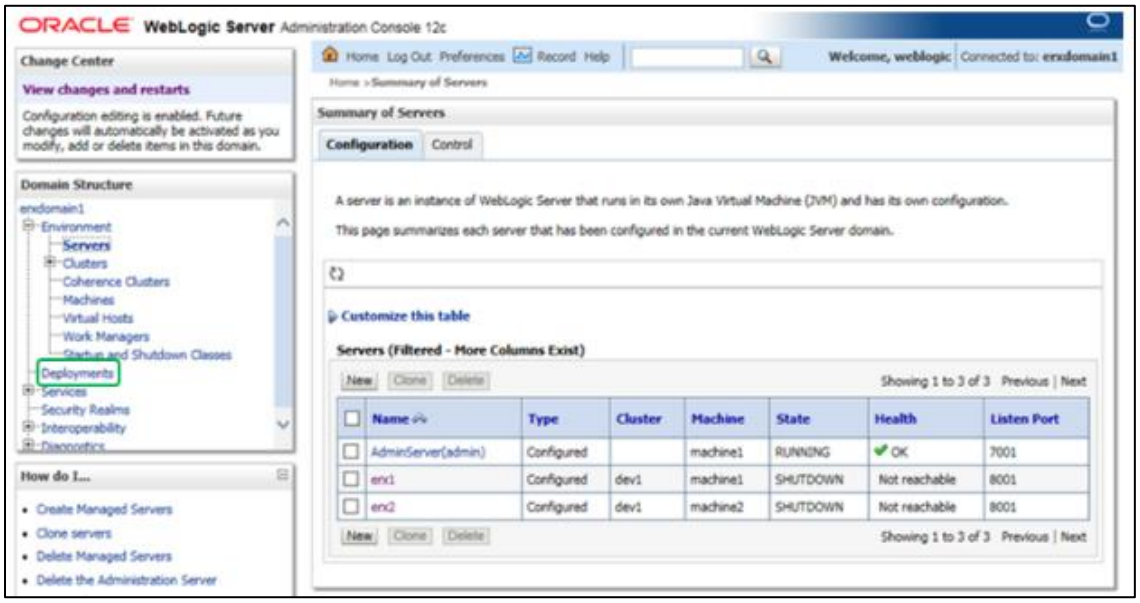
NOTE: The above username and password will be encoded/encrypted after the first shutdown/startup cycle.

4.8.1.19 Deploy Test Application

This section outlines the steps for deploying the test application.

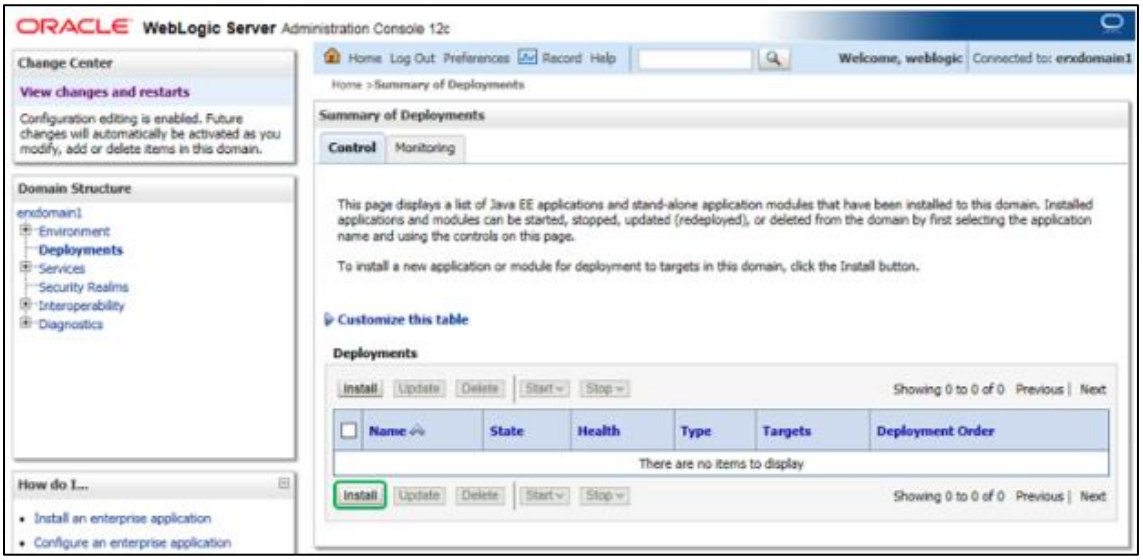
1. Start the node manager on all servers.
2. Create the deployments directory if it doesn't exist:
   ```
   $ mkdir -p /u01/deployments
   ```
3. Copy test application to the deployments directory:
   ```
   $ cp /u01/downloads/benefits.war /u01/deployments
   ```
4. Navigate to the *Deployments* page.

Figure 50: Deploy Test Application: Deployments Page



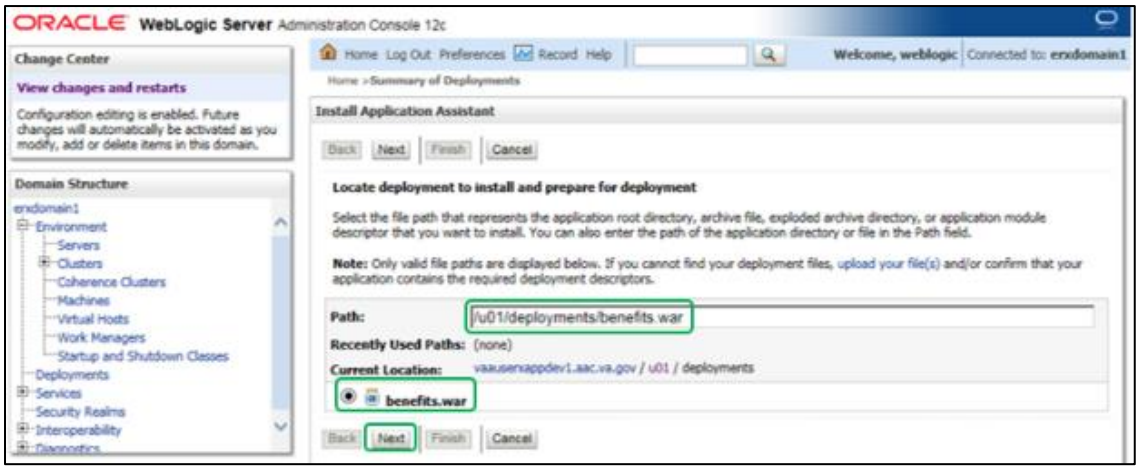
5. From the *Deployments* page, select **Install**.

Figure 51: Deploy Test Application – Install



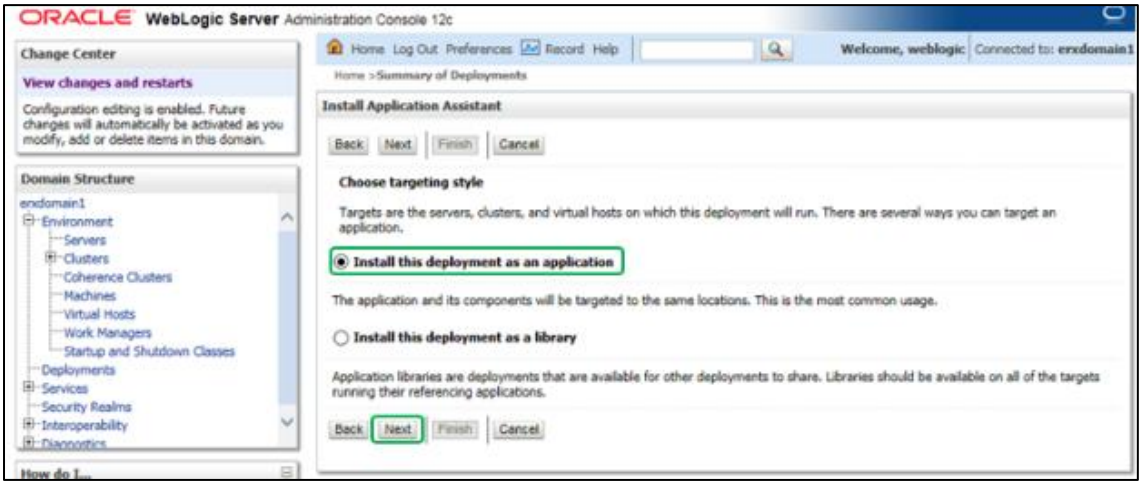
6. Install a new deployment of the test application using the WAR file as indicated in the figure below.
7. Select **Next**.

Figure 52: Deploy Test Application – WAR File



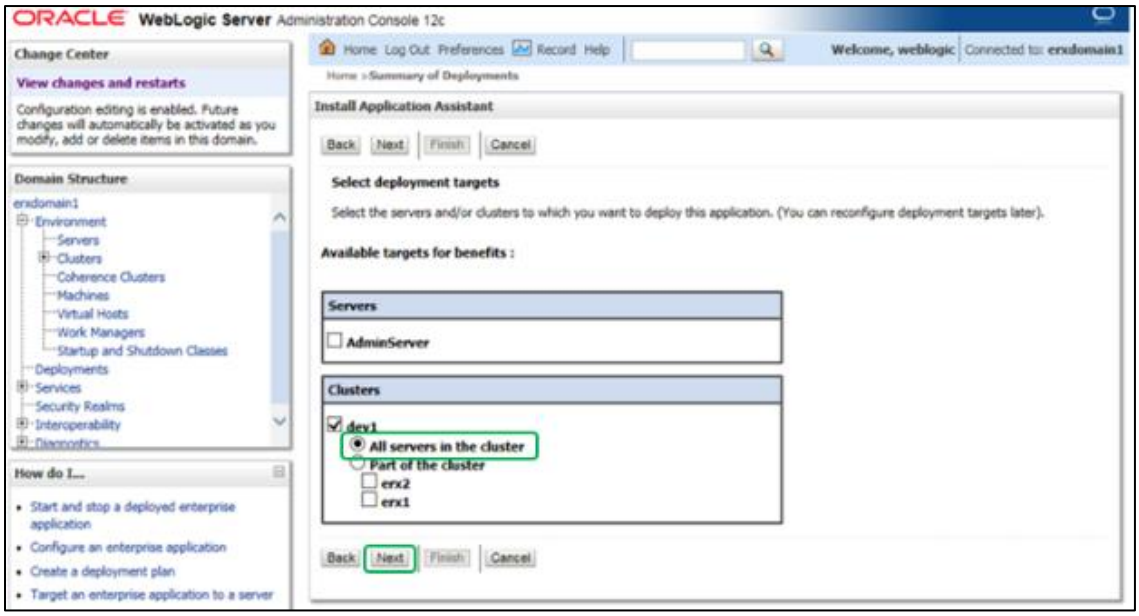
8. Accept the defaults for an application deployment. (The *Install this deployment as an application* radio button is marked.)
9. Select **Next**.

Figure 53: Deploy Test Application – Accept Default Application Deployment



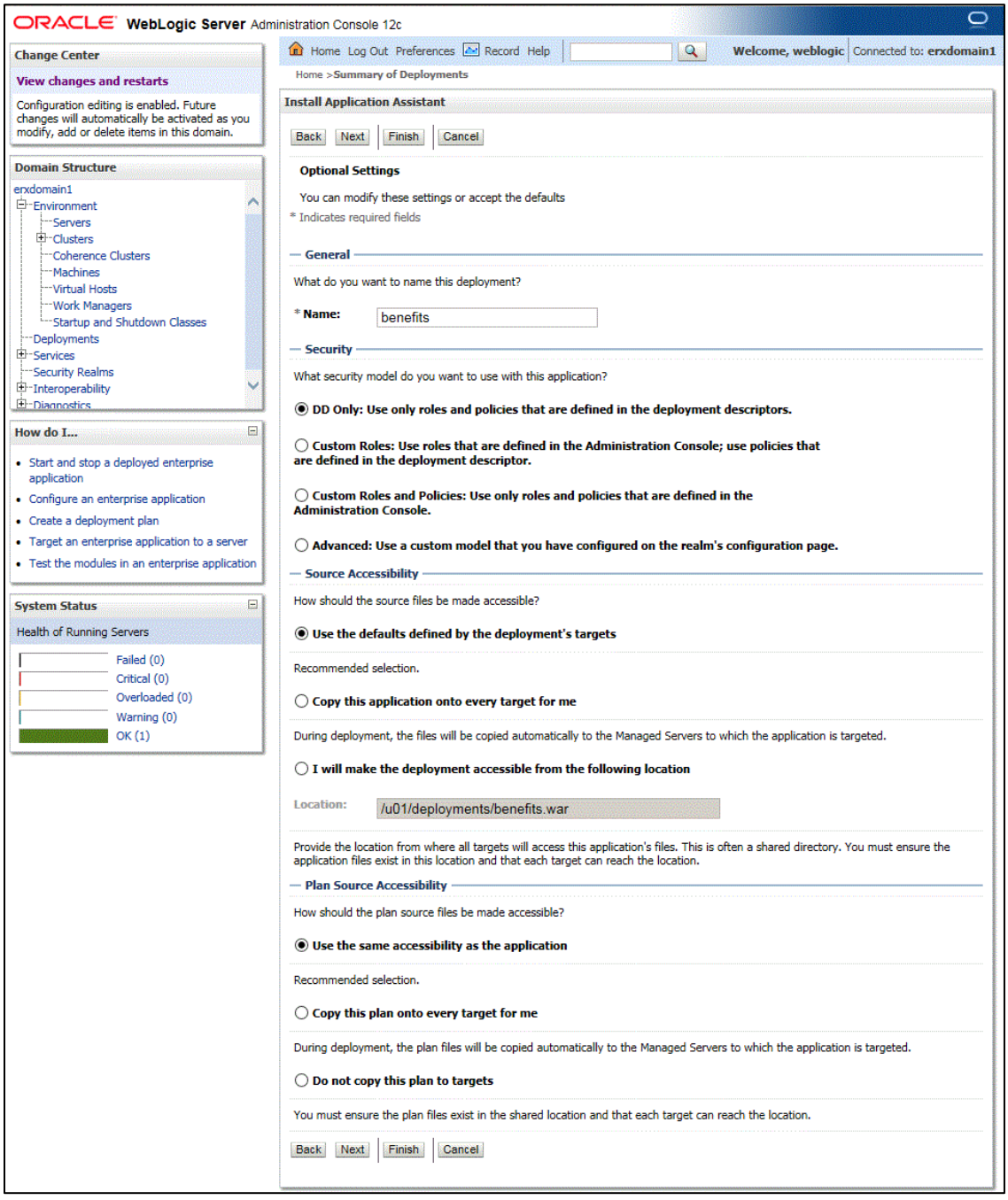
10. Select the **All servers in the cluster** option under the “erx” cluster as the target for the deployment.
11. Select **Next**.

Figure 54: Deploy Test Application – Select Deployment Target



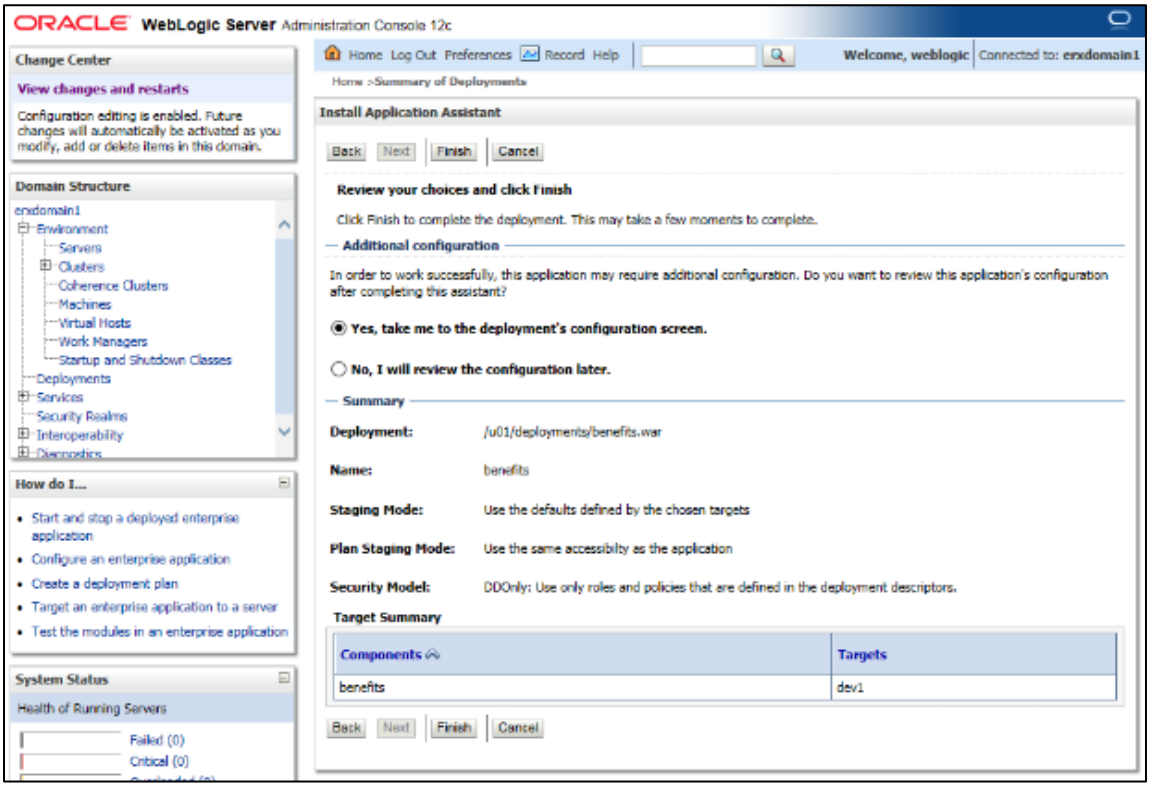
12. All of the values should appear as illustrated in the figure below.
13. Select **Next**.

Figure 55: Deploy Test Application – Verify Deployment Settings



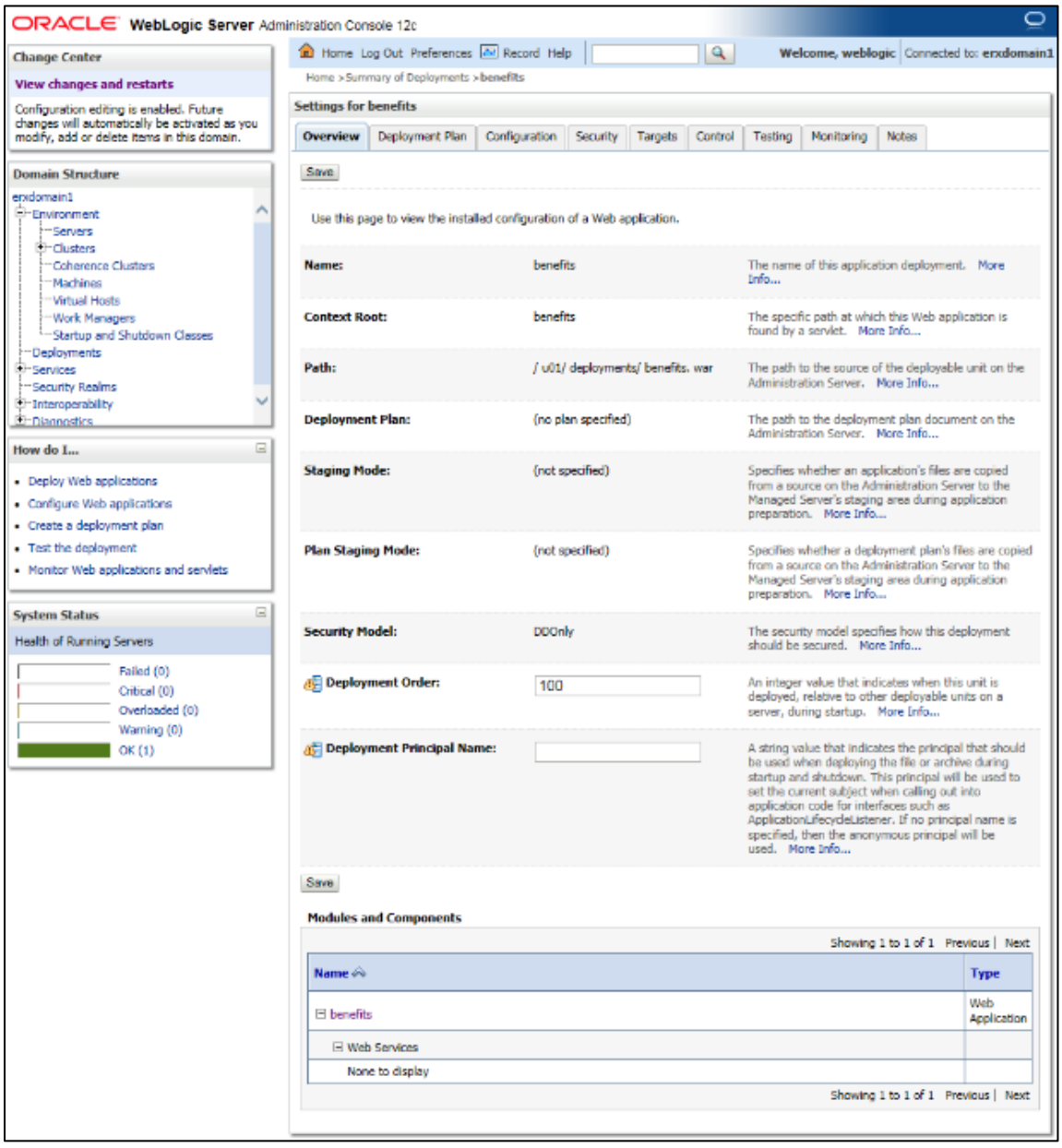
14. Verify that all of the values appear as illustrated in the figure below.
15. Select **Finish**.

Figure 56: Deploy Test Application – Verify Deployment Settings (Finish)



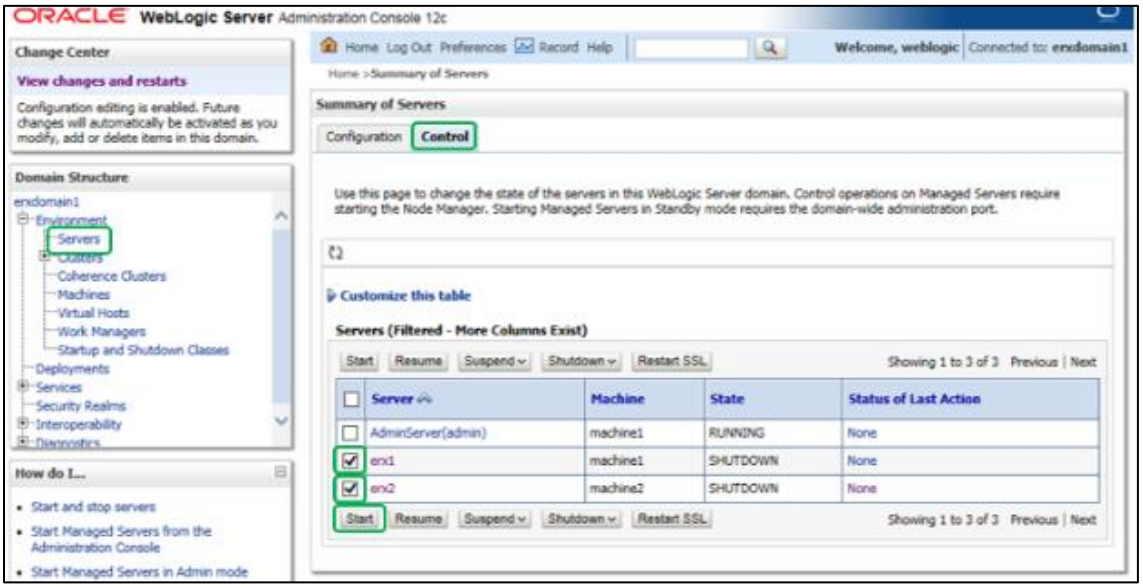
16. The **Overview** tab should appear as illustrated in the figure below.

Figure 57: Deploy Test Application – Verify "benefits" Settings



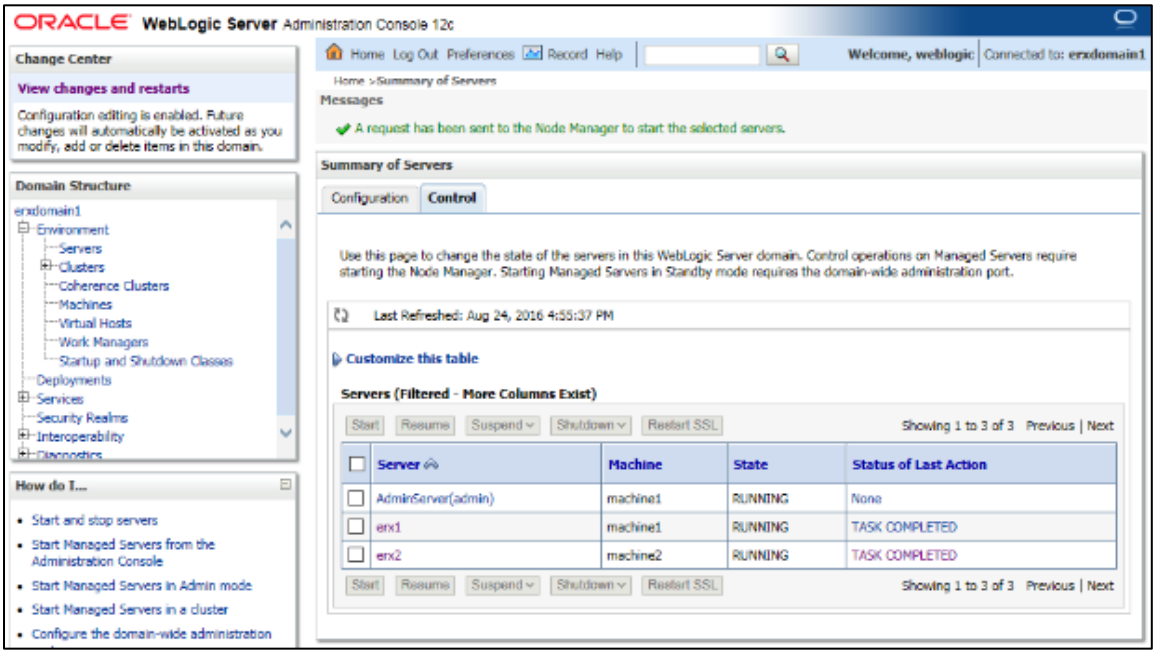
17. Navigate to the **Servers** page in the WebLogic console.
18. Select the **Control** tab.
19. Select **erx1** and **erx2** servers.
20. Select **Start**.

Figure 58: Deploy Test Application – Summary of Servers Table



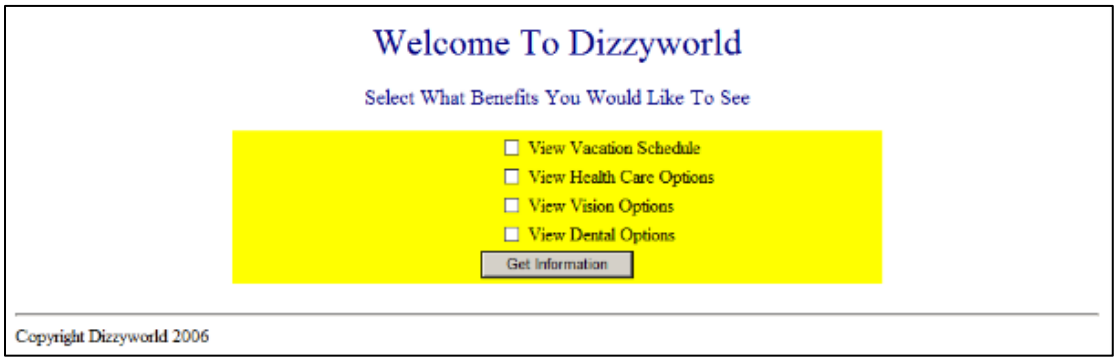
21. After a couple minutes, the state on the servers will change to **RUNNING**.

Figure 59: Deploy Test Application – Servers Running



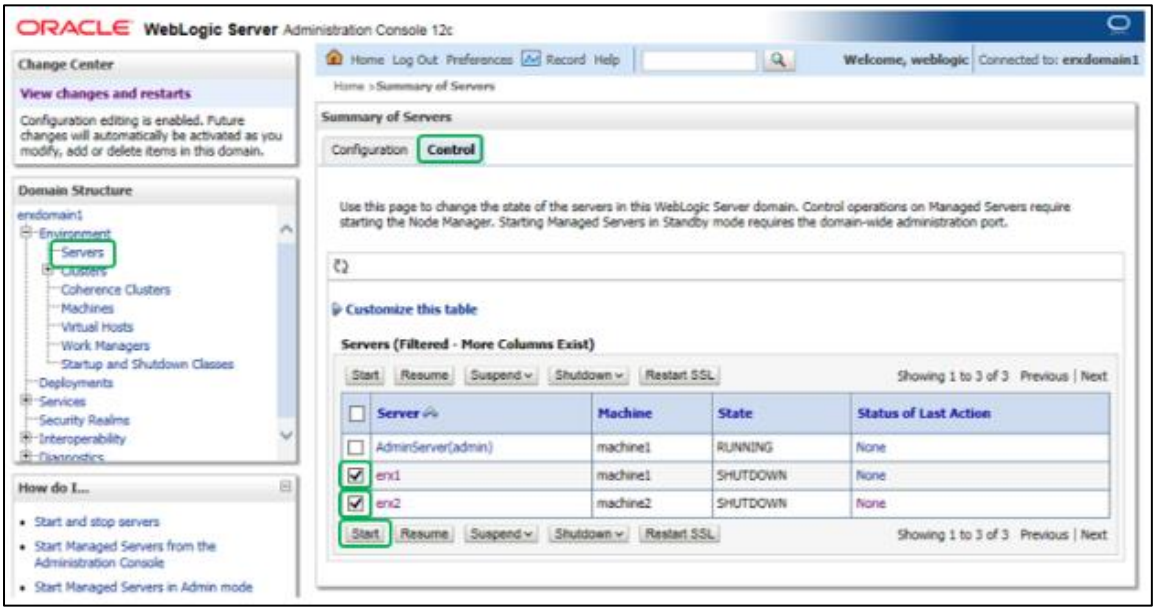
22. Open a web browser to **http://*[vm1_fqdn]*/benefits/**.
23. The Dizzyworld Benefits application will display.

Figure 60: Deploy Test Application – Open Dizzyworld Benefits Application



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. Select **Shutdown**.

Figure 61: Deploy Test Application – Shutdown Servers



4.8.1.20 Configure JPA for Domain on VM2

On VM2, 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]/module
s/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. Log into Linux and sudo su to the weblogic account:
   ```
   $ sudo su - weblogic
   ```
2. Create a 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
    ```

4.8.1.22 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. Log into Linux and 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:

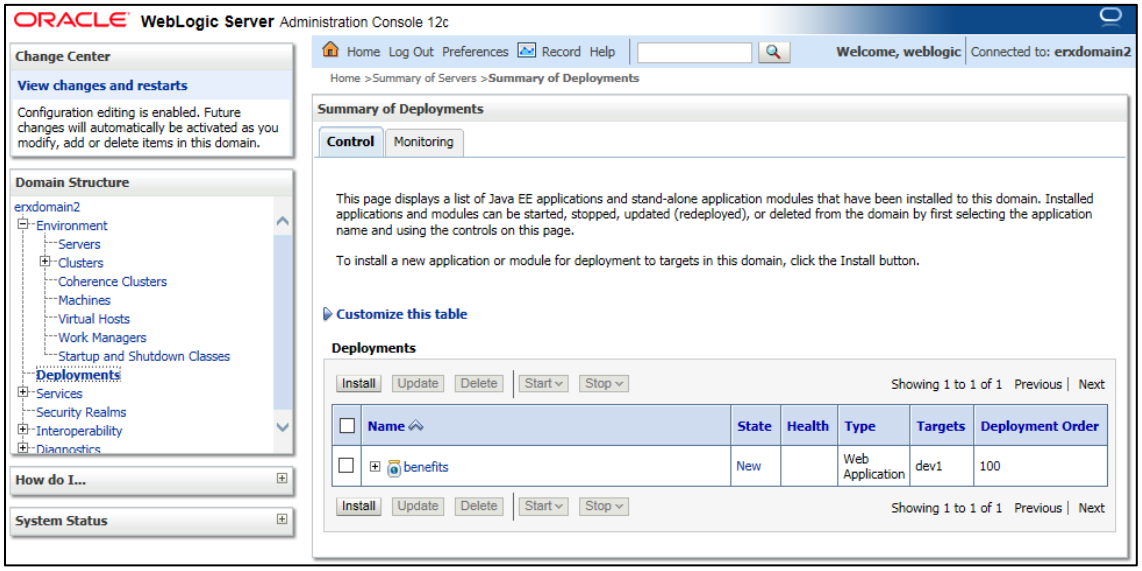
1. Stop the new domain on the VM1.
   ```
   $ $DOMAIN_HOME/bin/stopWebLogic.sh
   ```
2. On VM1 stop the node manager.
   ```
   $ $DOMAIN_HOME/bin/stopNodeManager.sh
   ```
3. On VM1, start the node manager.
   ```
   $ DOMAIN_HOME/bin/stopNodeManager.sh
   ```
4. On VM2 stop the node manager.
   ```
   $ $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:

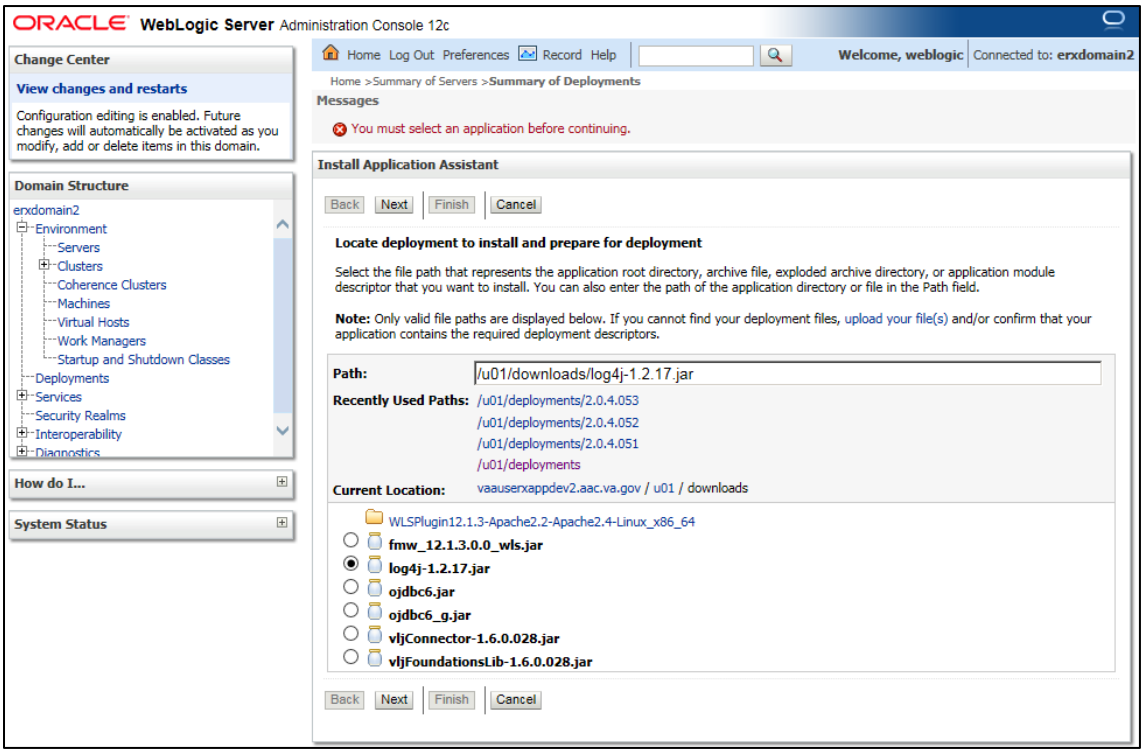
1. Navigate to the *Deployments* page.
2. From the *Deployment*s screen, select **Install**.

Figure 62: Deploy VistA Link Connector – Deployments



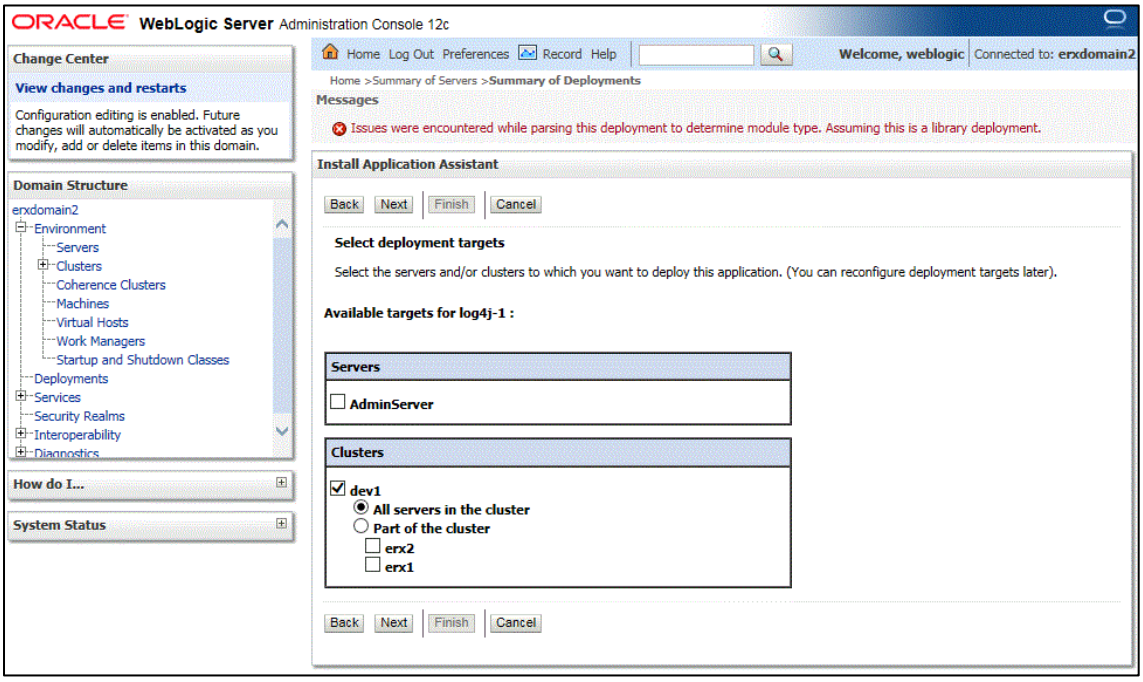
3. Enter *Path*: **/u01/downloads**
4. Install a new deployment of **log4j-1.2.17.jar** by selecting the jar file as indicated, and then select **Next**.

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



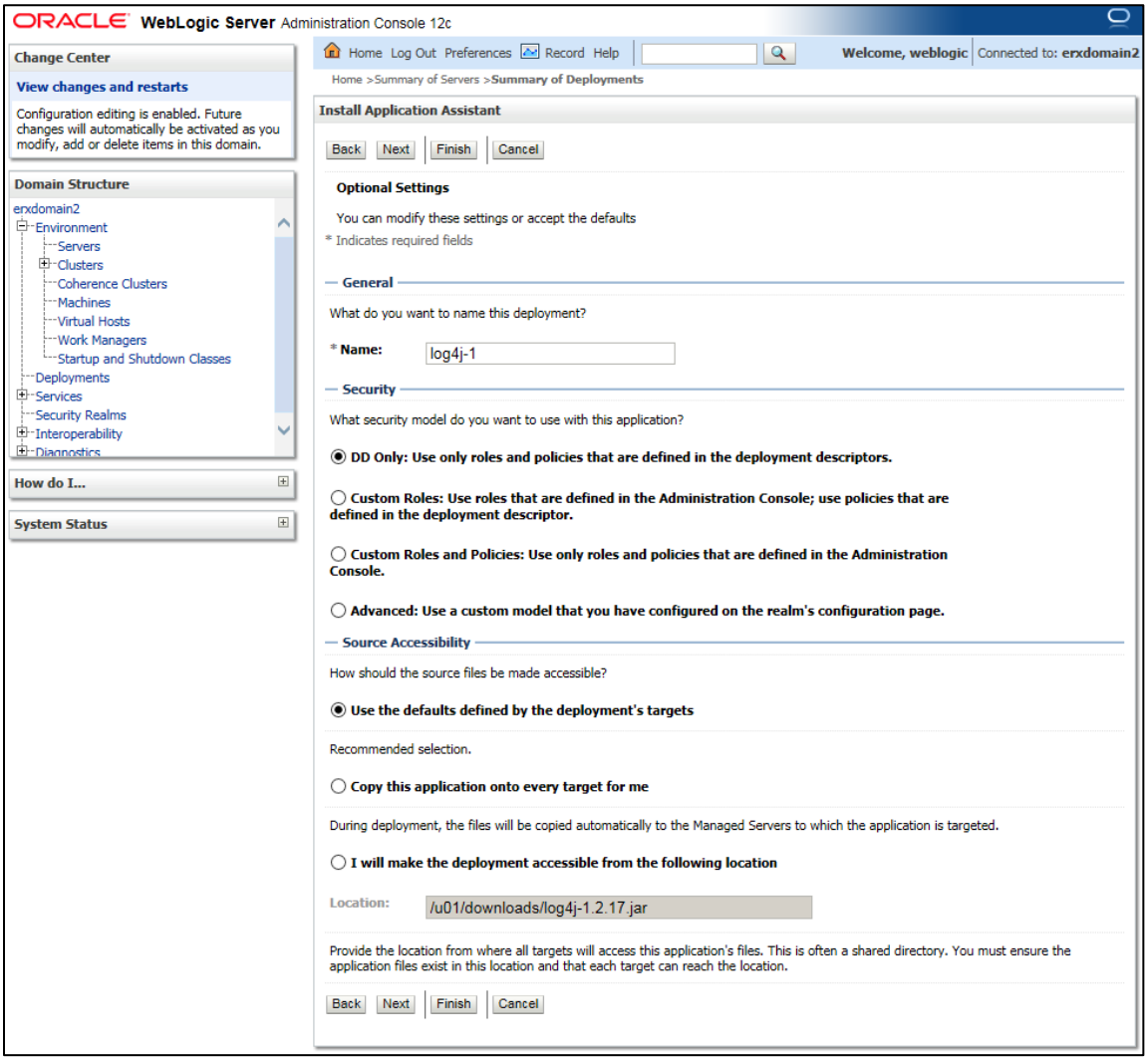
5. Select **All servers in the cluster** as the target for the deployment, and then select **Next**.

Figure 64: Deploy VistA Link Connector – Select Deployment Targets



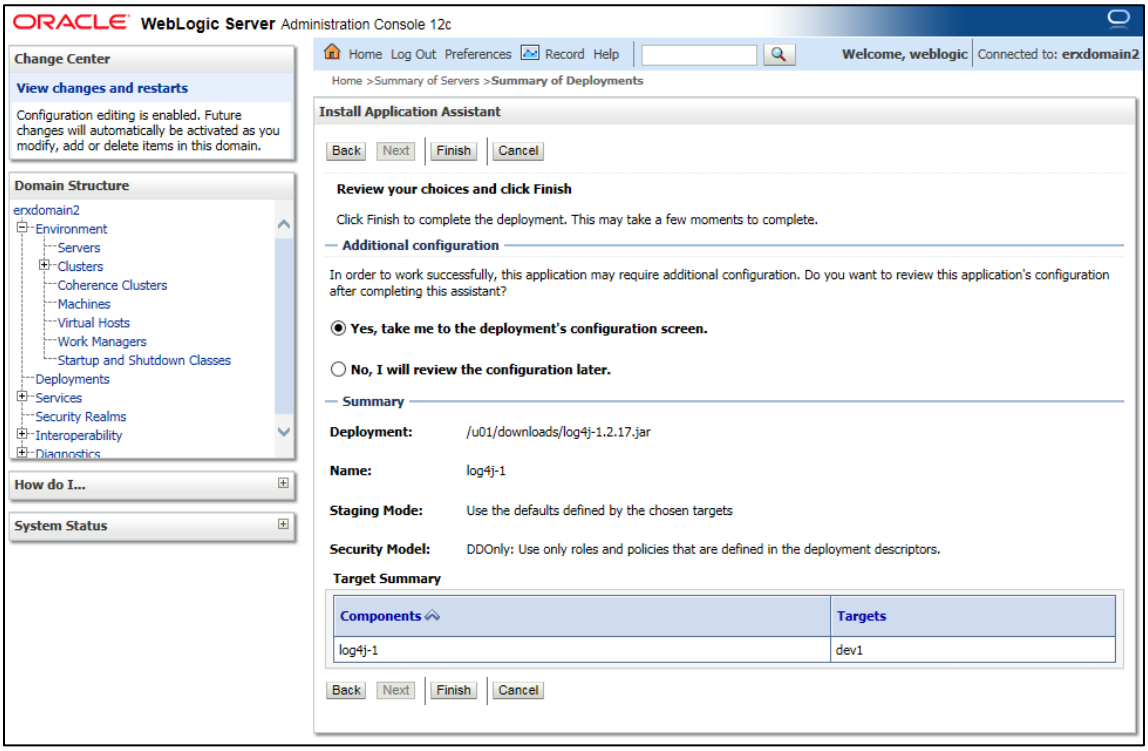
6. All of the values should appear as illustrated in the figure below.
7. Select **Next**.

Figure 65: Deploy VistA Link Connector – Summary of Deployments Verification 1



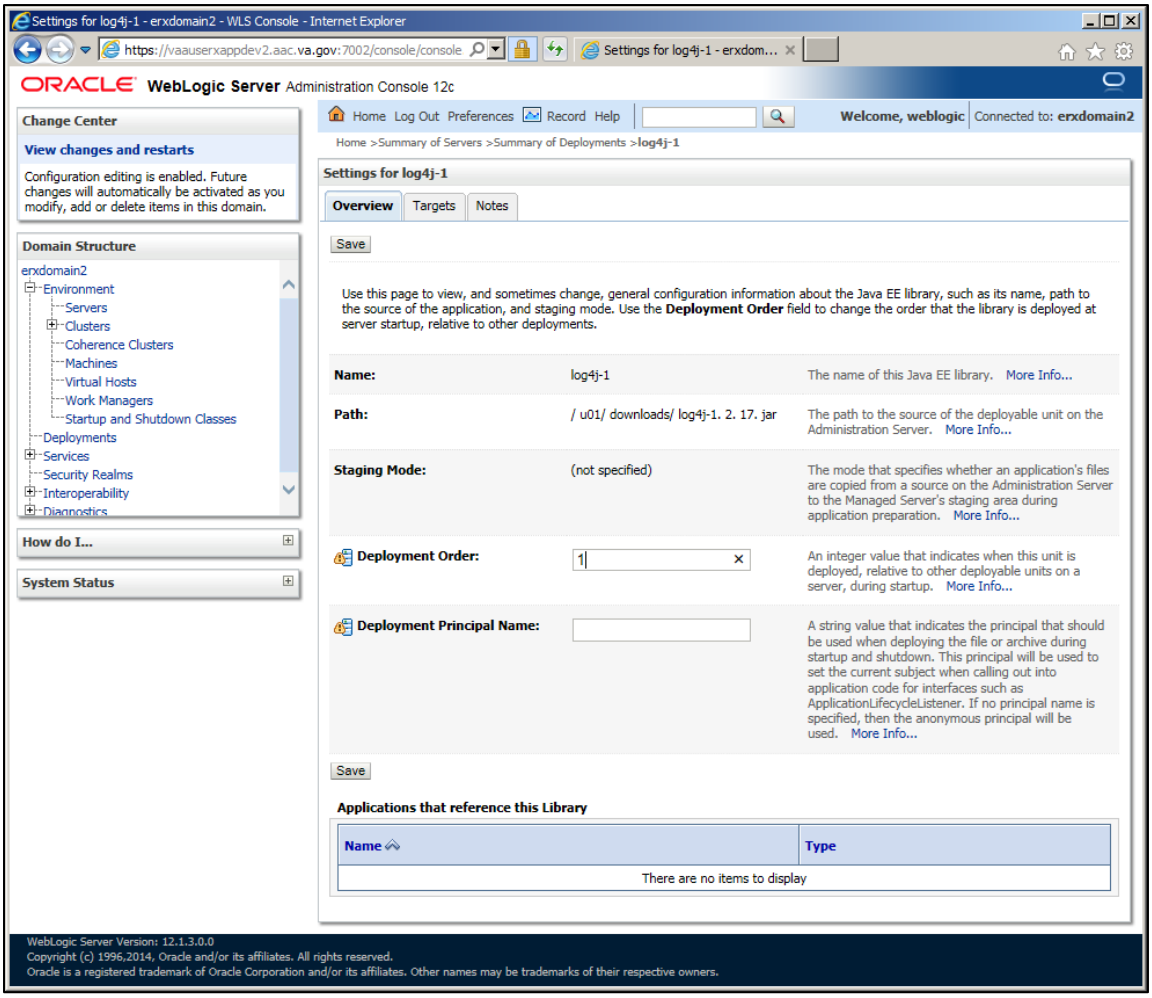
8. Verify that all of the values appear as illustrated in the figure below.
9. Select **Finish**.

Figure 66: Deploy VistA Link Connector – Summary of Deployments Verification 2



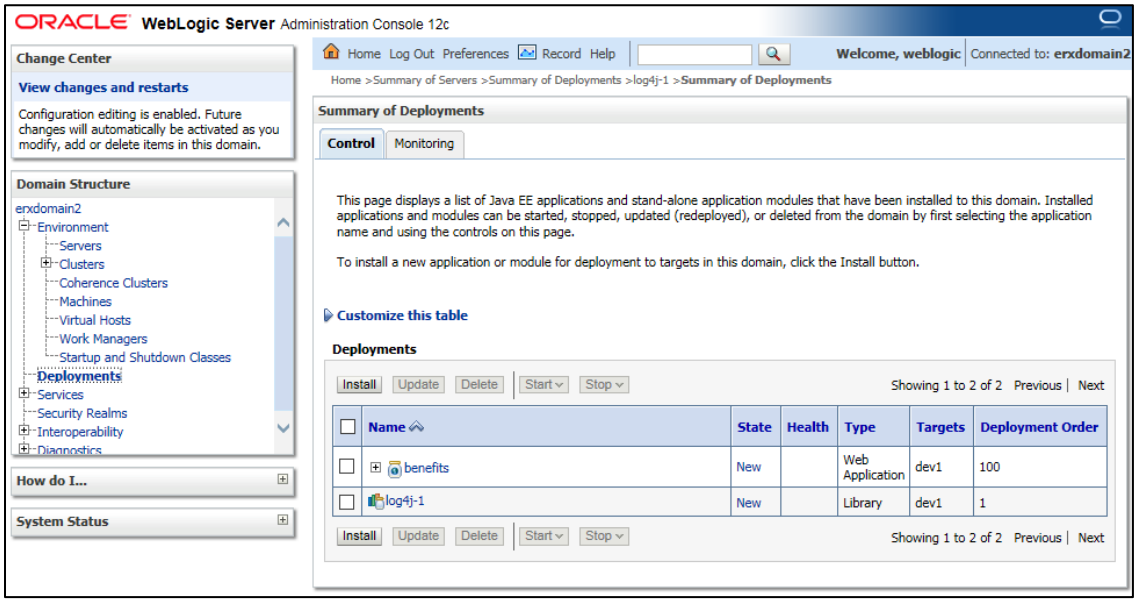
10. The **Deployment Configuration** screen should appear as illustrated in the below figure.
11. Enter *Deployment Order*: **1**
12. Select **Save**.

Figure 67: Deploy VistA Link Connector – Deployment Configuration Screen



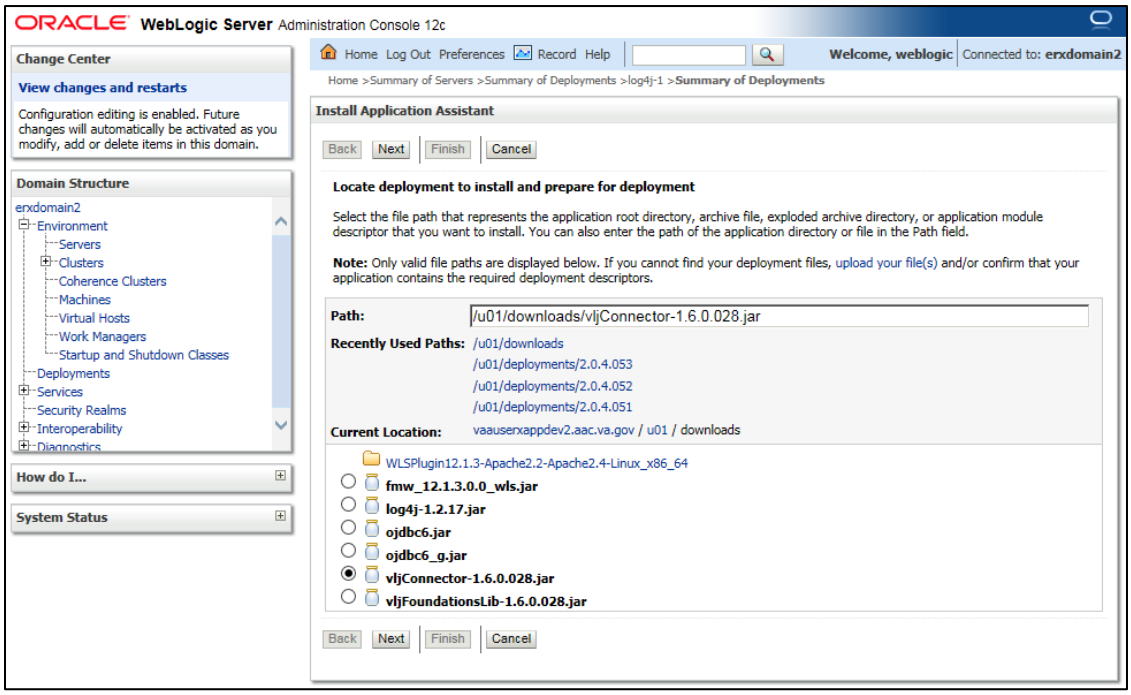
13. Navigate to the *Deployments* page.
14. From the *Deployment*s screen, select **Install**.

Figure 68: Deploy VistA Link Connector – Deployments



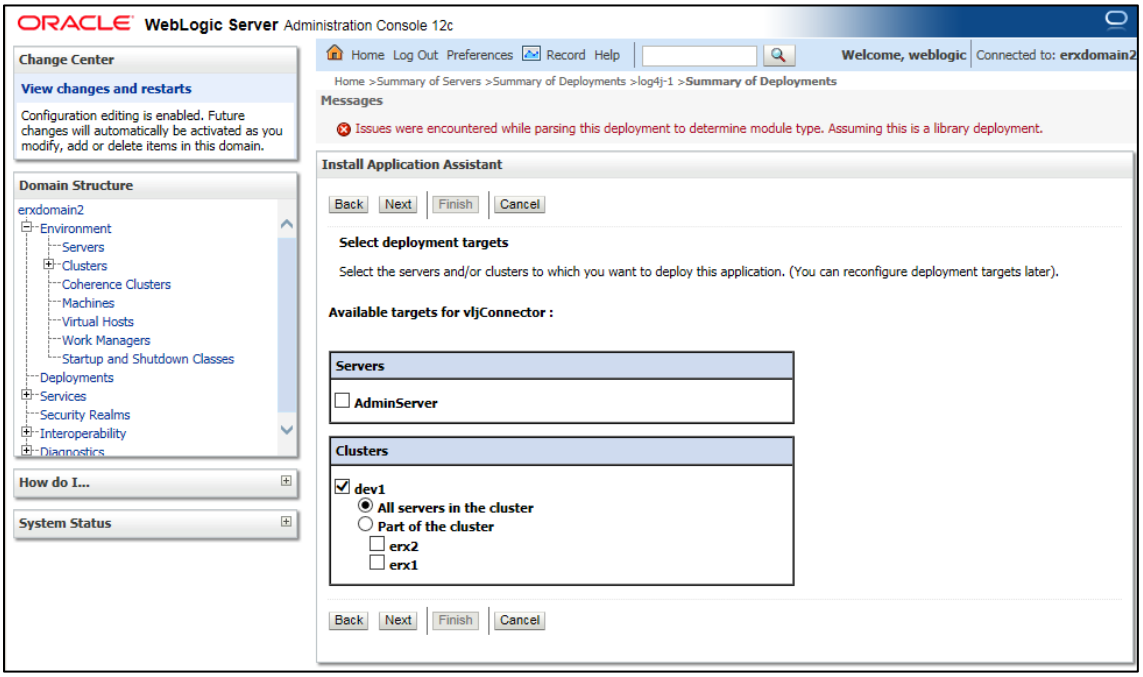
15. Enter *Path*: **/u01/downloads**
16. Install a new deployment of **vljConnector-1.6.0.028.jar** by selecting the jar file as indicated, and then select **Next**.

Figure 69: Deploy VistA Link Connector – Select vljConnector-1.6.0.028.jar Library to deploy



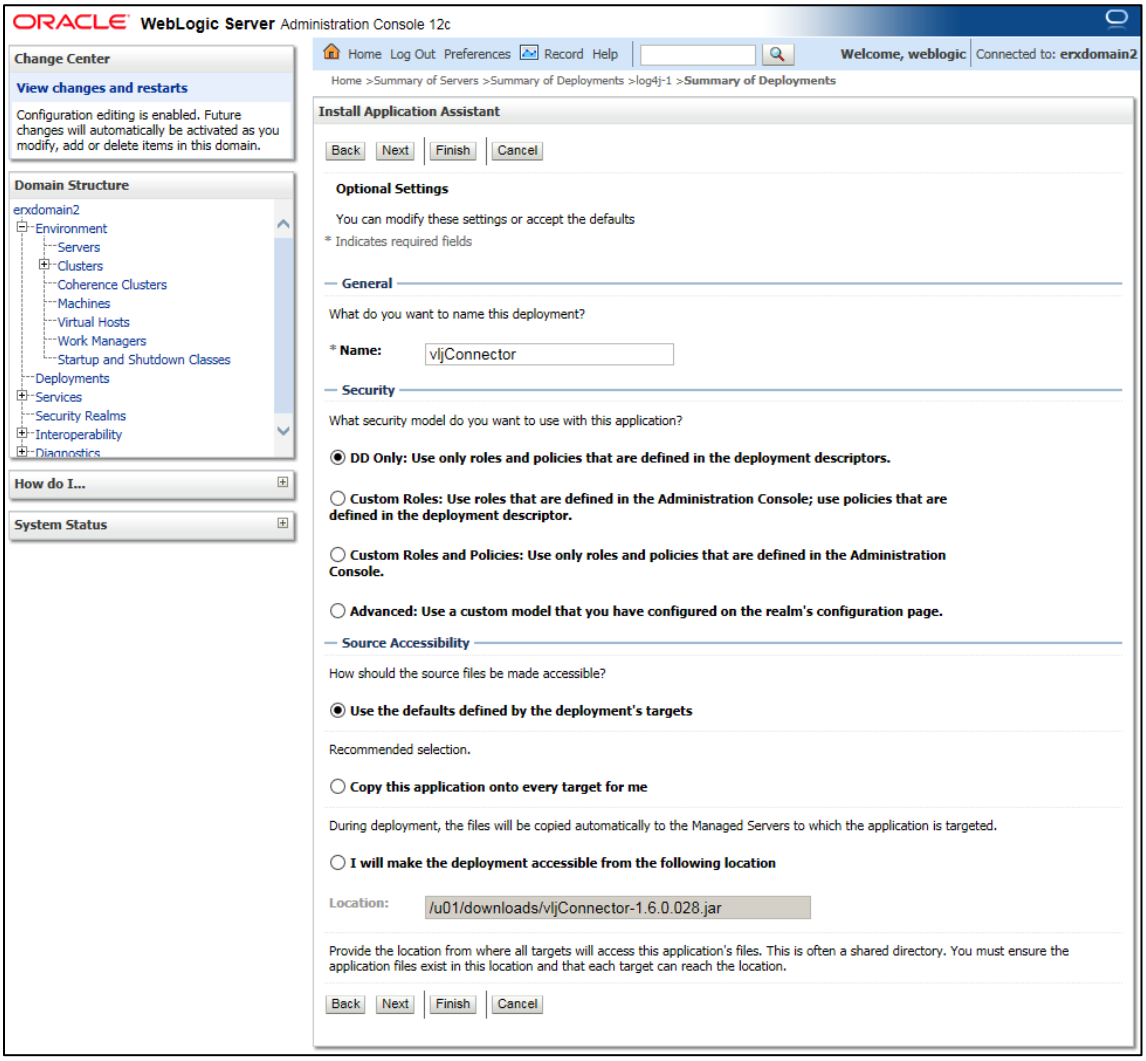
17. Select **All servers in the cluster** as the target for the deployment, and then select **Next**.

Figure 70: Deploy VistA Link Connector – Select Deployment Targets



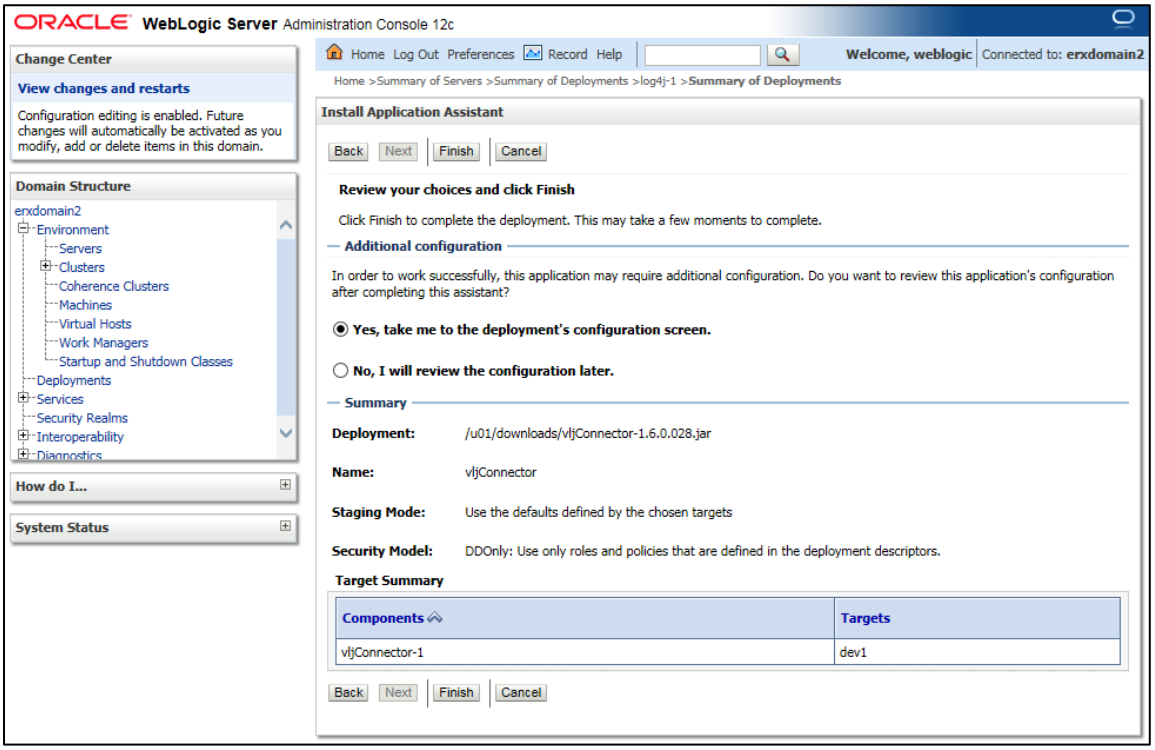
18. All of the values should appear as illustrated in the figure below.
19. Select **Next**.

Figure 71: Deploy VistA Link Connector – Summary of Deployments Verification 1



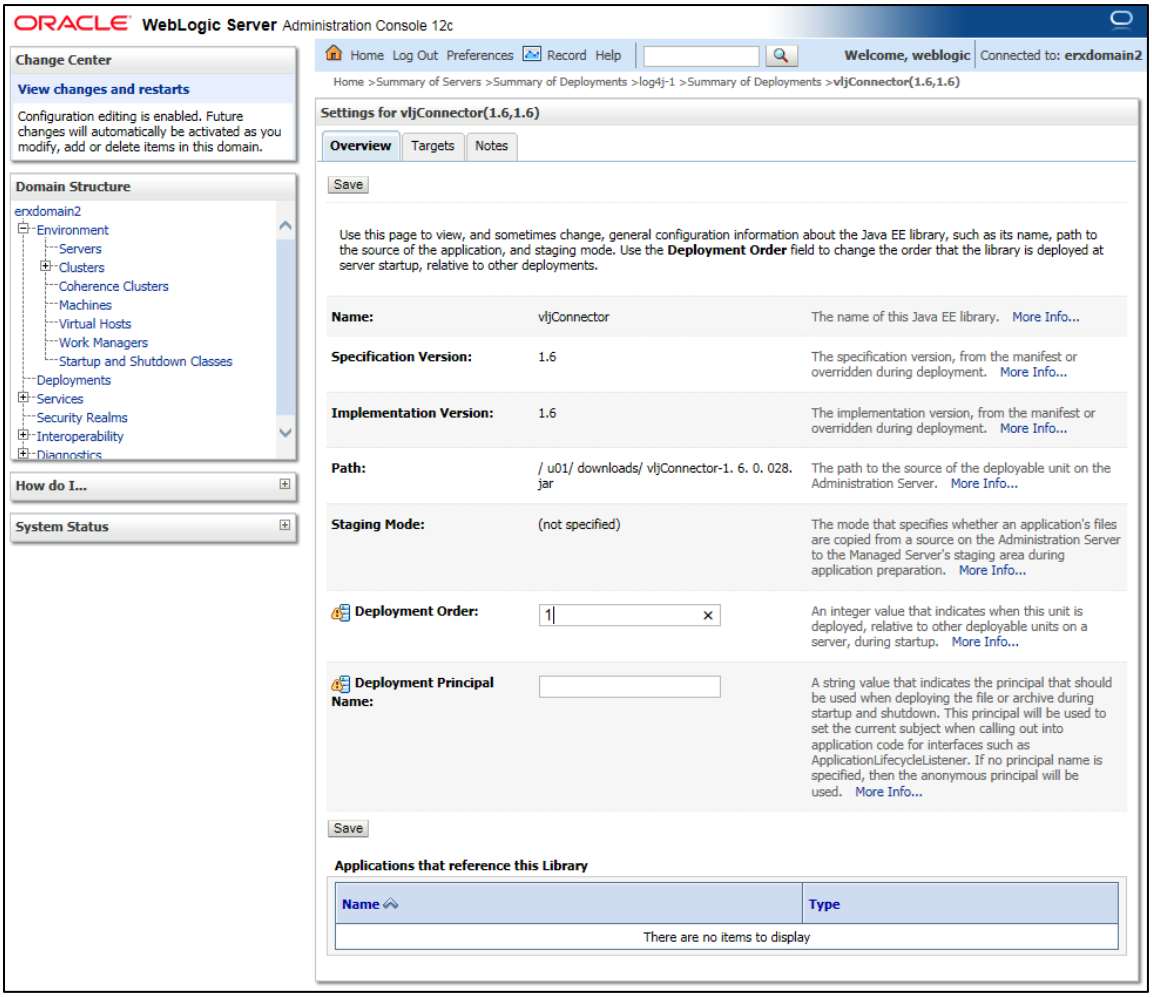
20. Verify that all of the values appear as illustrated in the figure below.
21. Select **Finish**.

Figure 72: Deploy VistA Link Connector – Summary of Deployments Verification 2



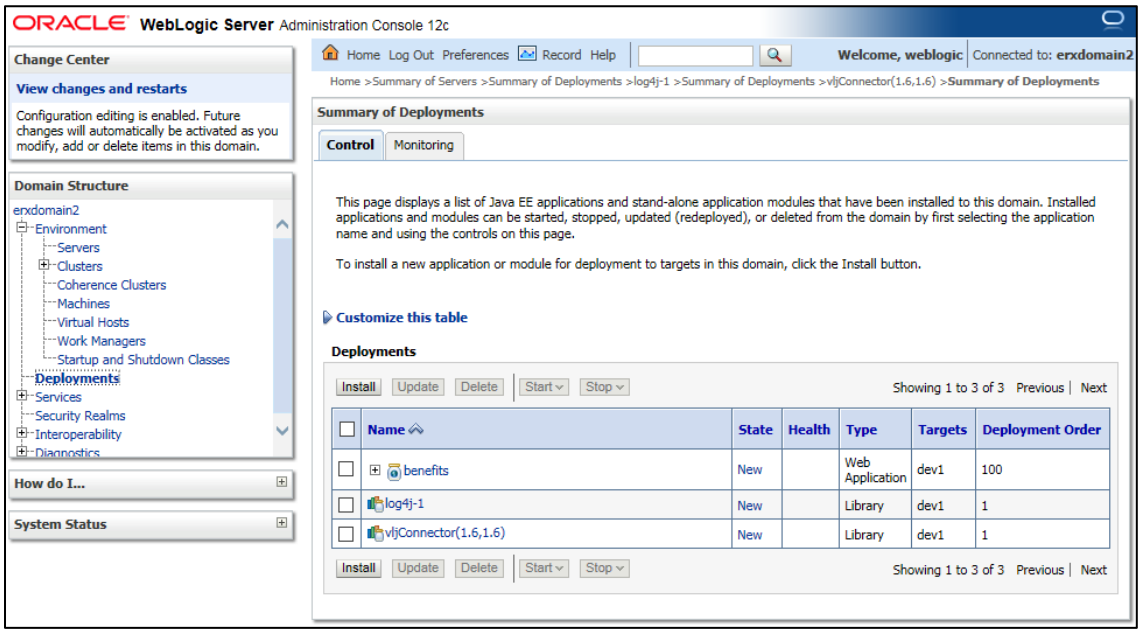
22. The **Deployment Configuration** screen should appear as illustrated in the below figure.
23. Enter *Deployment Order*: **1**
24. Select **Save**.

Figure 73: Deploy VistA Link Connector – Deployment Configuration Screen



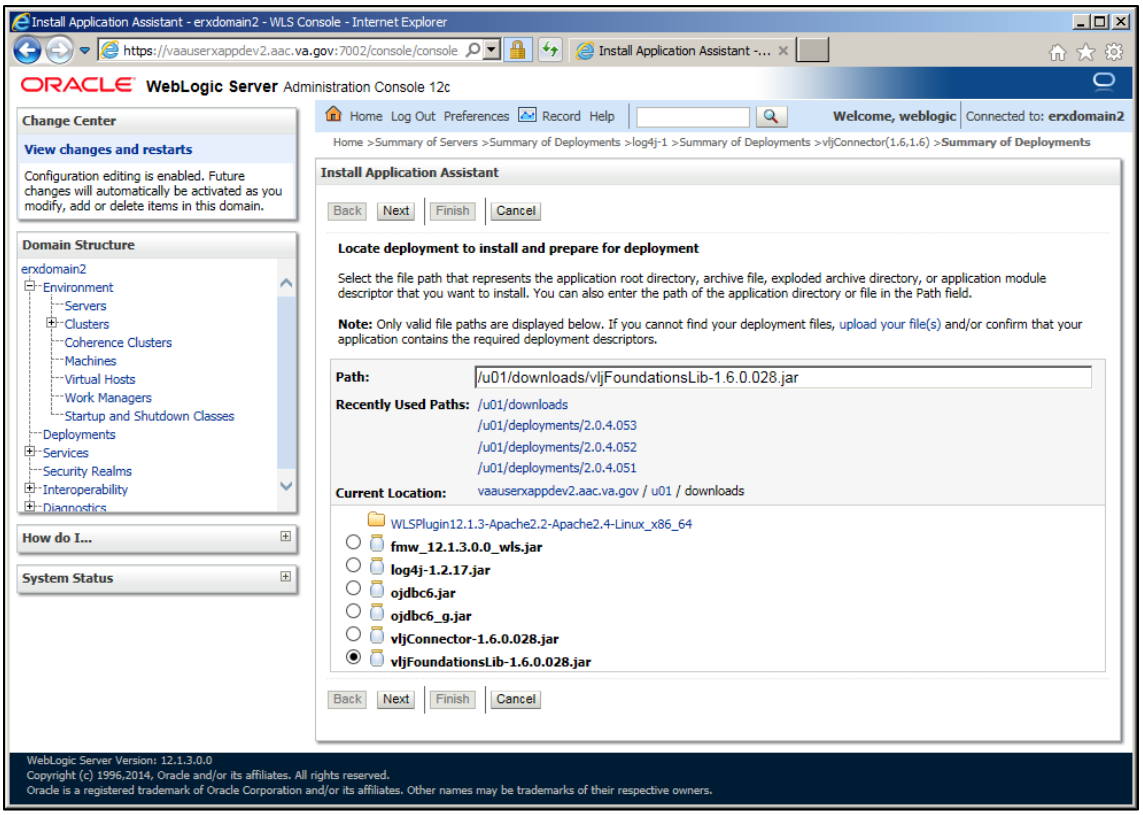
25. Navigate to the *Deployments* page.
26. From the *Deployment*s screen, select **Install**.

Figure 74: Deploy VistA Link Connector – Deployments



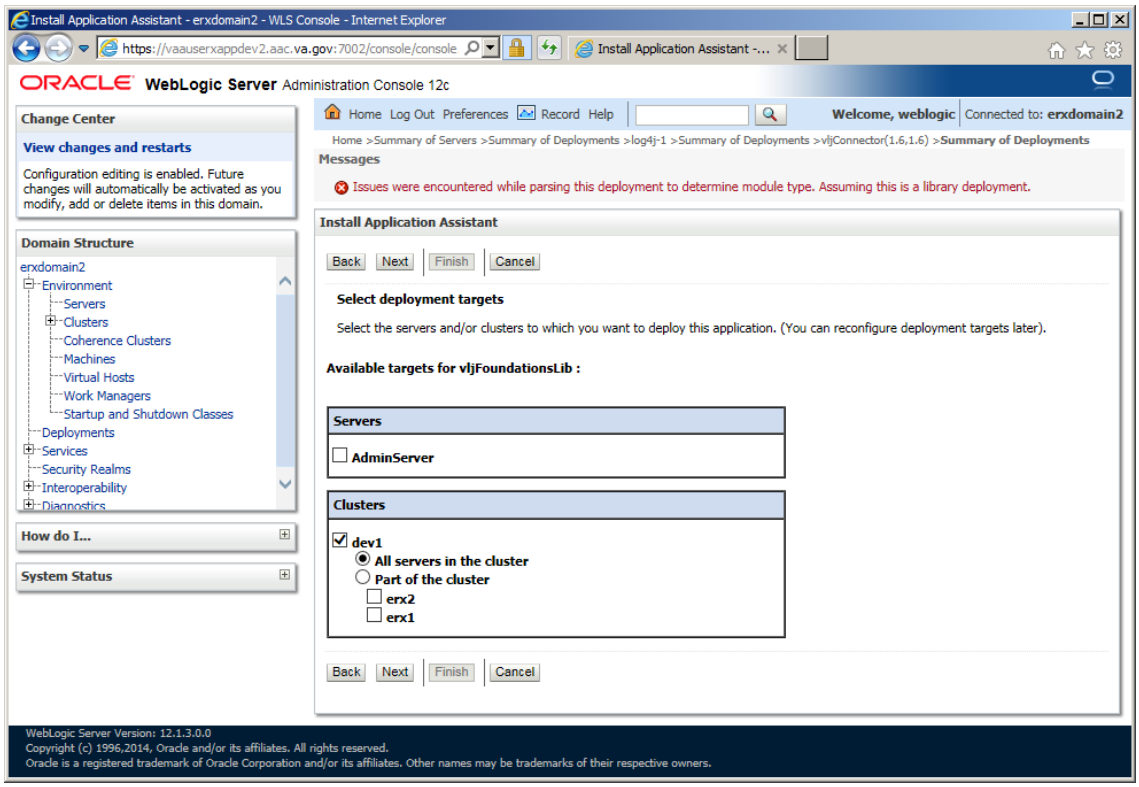
27. Enter *Path*: **/u01/downloads**
28. Install a new deployment of **vljFoundationsLib-1.6.0.028.jar** by selecting the jar file as indicated, and then select **Next**.

Figure 75: Deploy VistA Link Connector – Select vljFoundationsLib to deploy



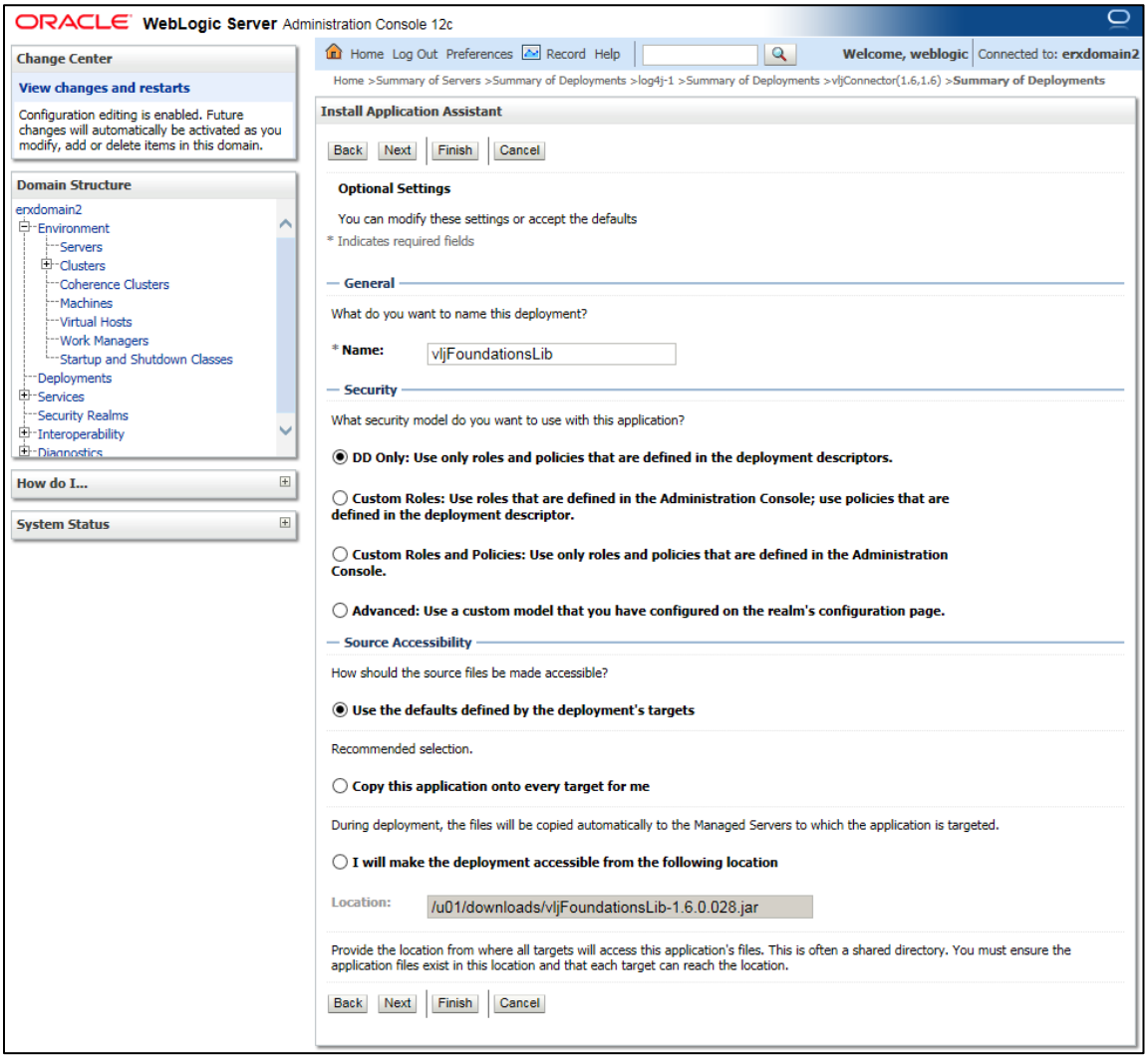
29. Select **All servers in the cluster** as the target for the deployment, and then select **Next**.

Figure 76: Deploy VistA Link Connector – Select Deployment Targets



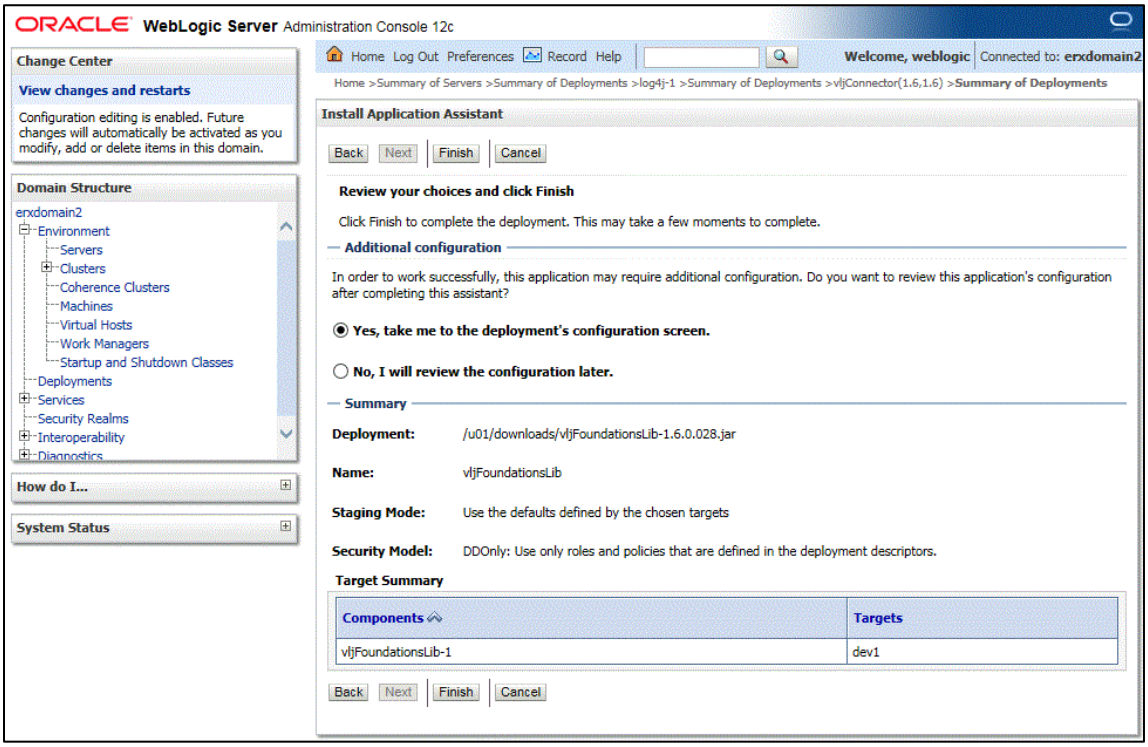
30. All of the values should appear as illustrated in the figure below.
31. Select **Next**.

Figure 77: Deploy VistA Link Connector – Summary of Deployments Verification 1



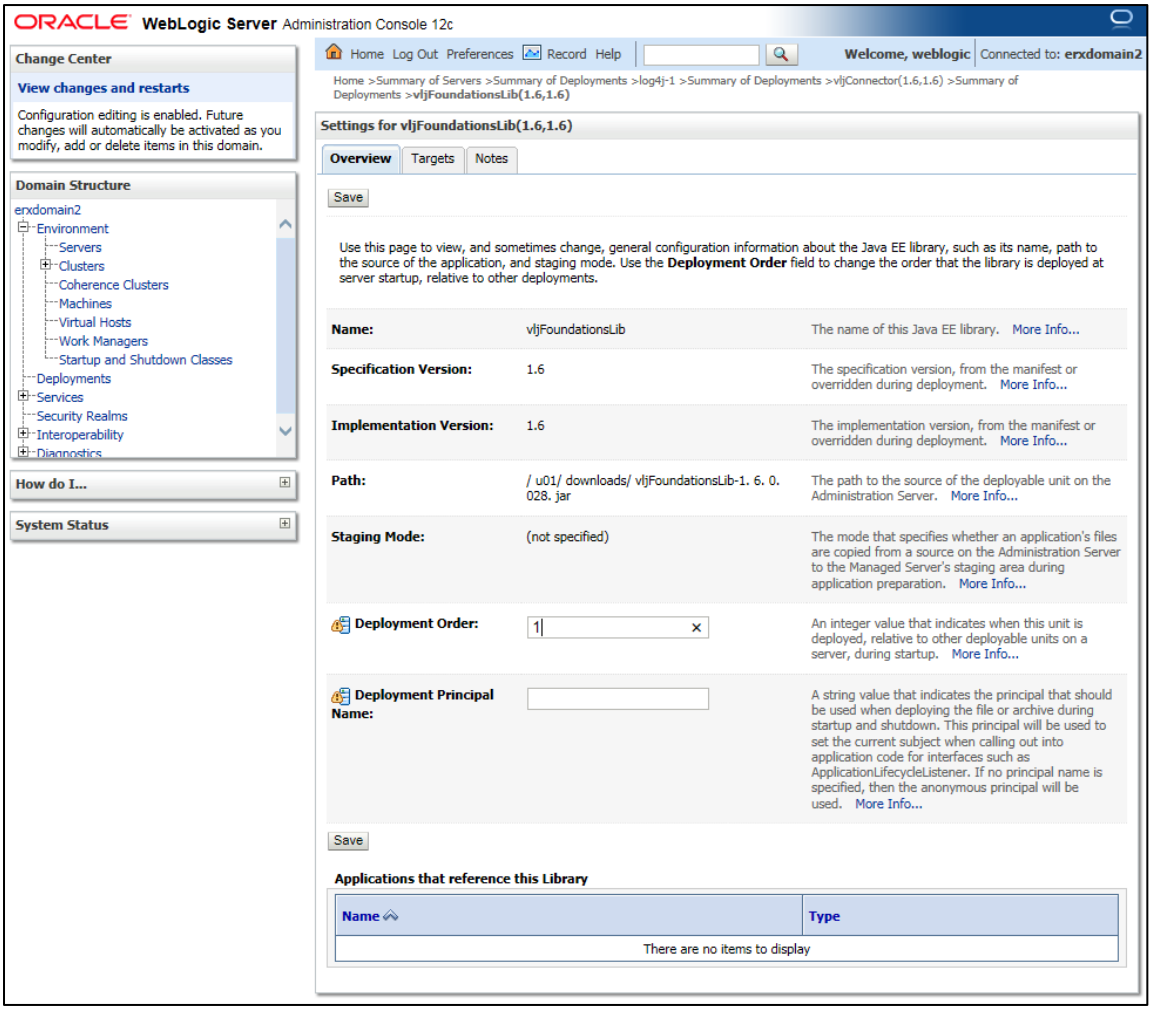
32. Verify that all of the values appear as illustrated in the figure below.
33. Select **Finish**.

Figure 78: Deploy VistA Link Connector – Summary of Deployments Verification 2



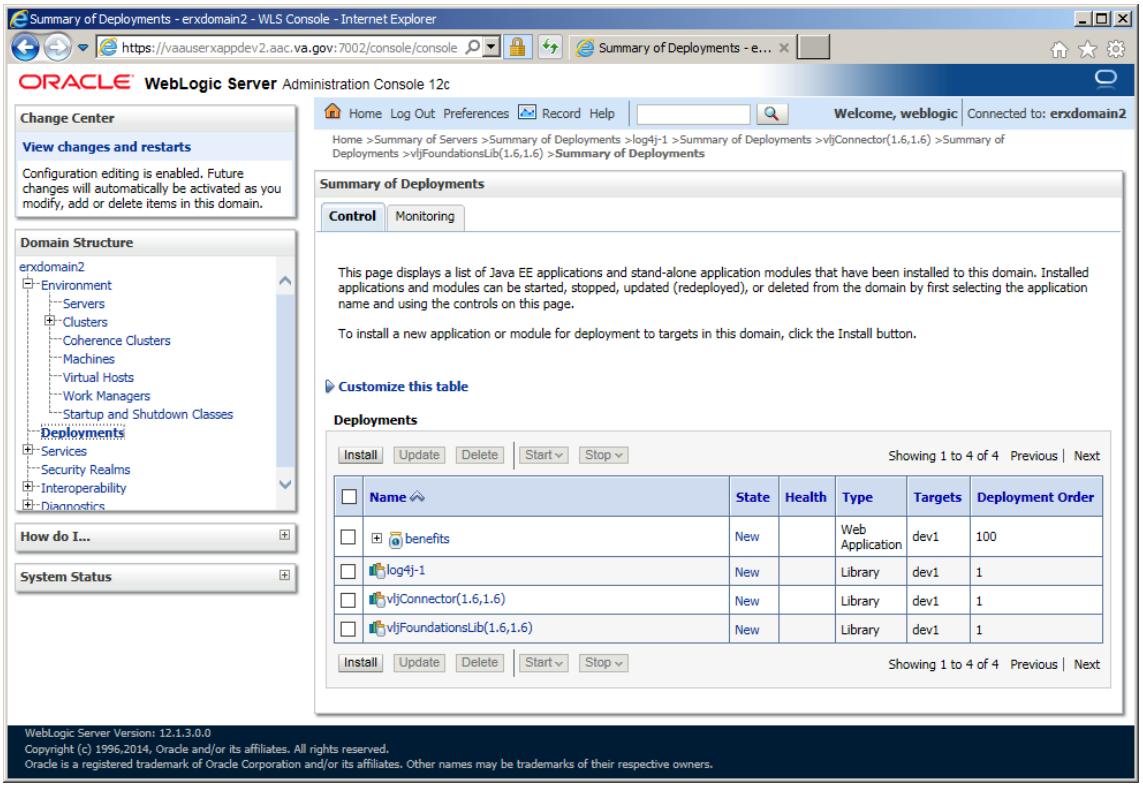
34. The **Deployment Configuration** screen should appear as illustrated in the below figure.
35. Enter *Deployment Order*: **1**
36. Select **Save**.

Figure 79: Deploy VistA Link Connector – Deployment Configuration Screen



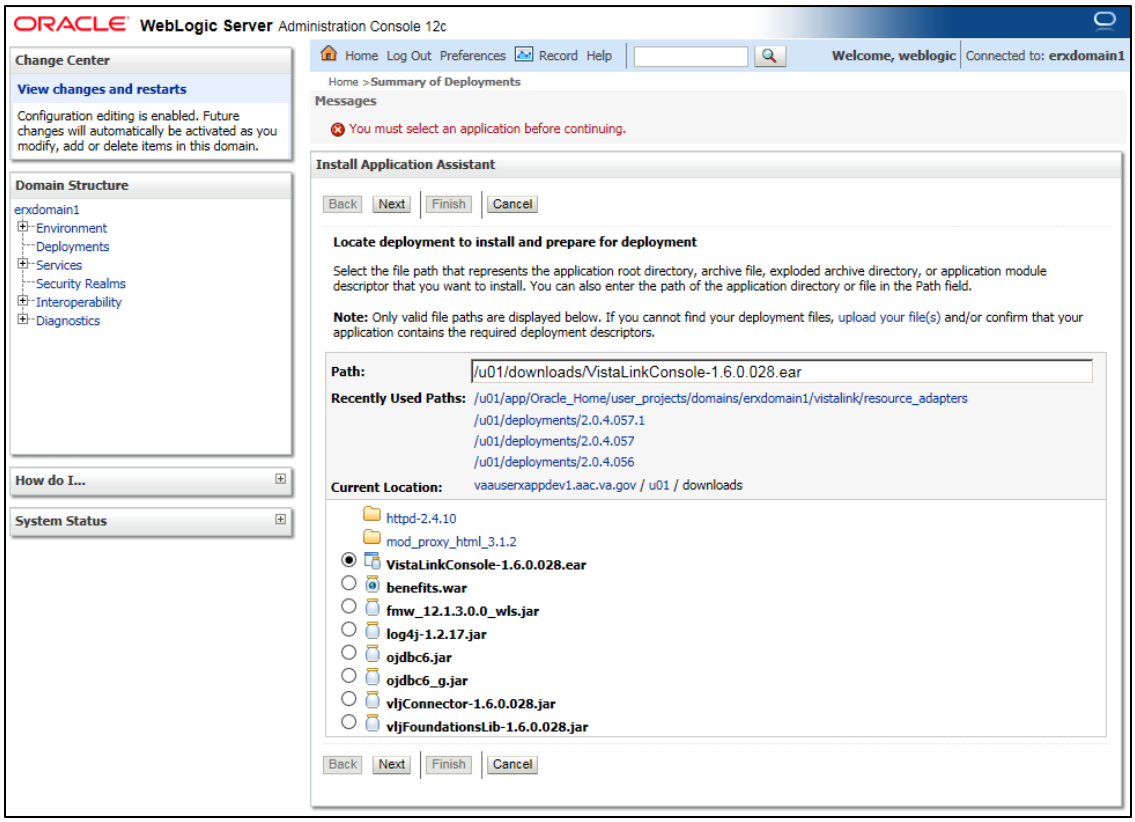
37. Navigate to the *Deployments* page.
38. From the *Deployment*s screen, select **Install**.

Figure 80: Deploy VistA Link Connector – Deployments



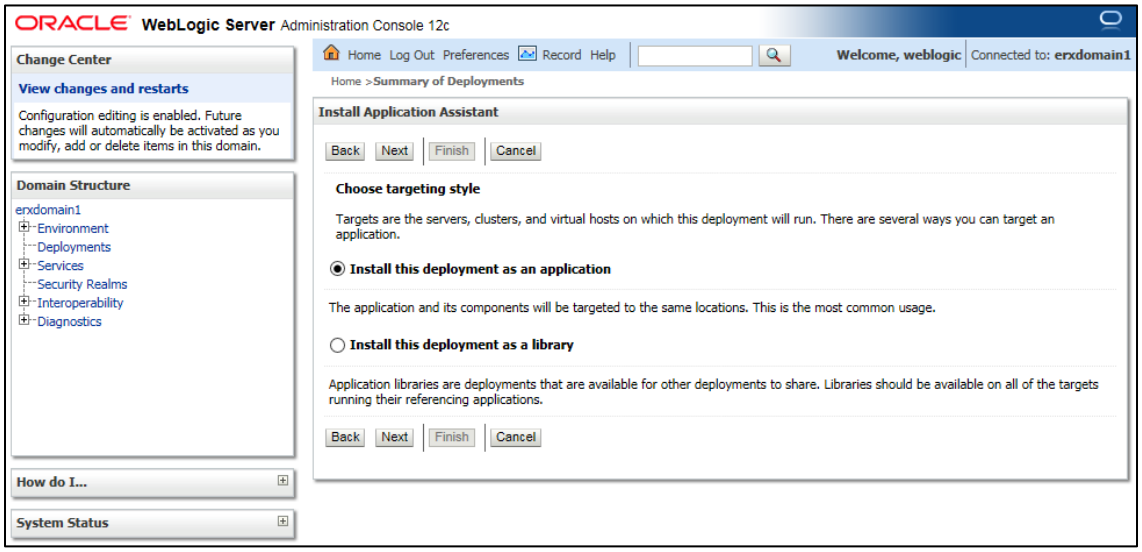
39. Enter *Path*: **/u01/downloads**
40. Install a new deployment of **VistaLinkConsole-1.6.0.0.28.ear** by selecting file as indicated, and then select **Next**.

Figure 81: Deploy VistA Link Connector – Select VistaLinkConsole to deploy



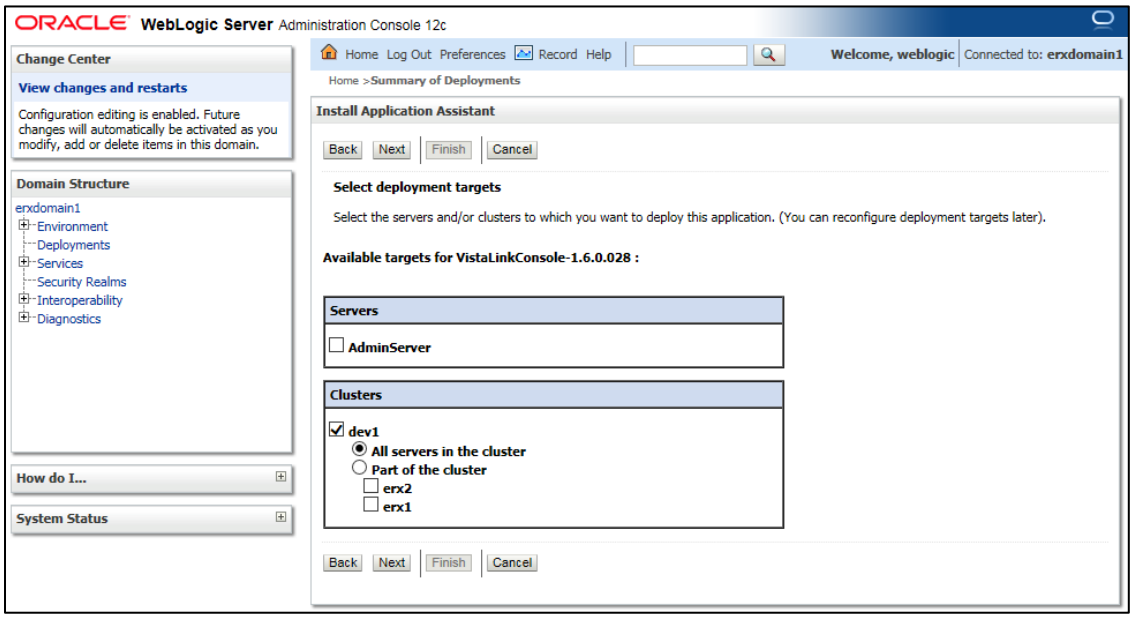
41. Select **All servers in the cluster** as the target for the deployment, and then select **Next**.

Figure 82: Deploy VistA Link Connector – Select Deployment Targets



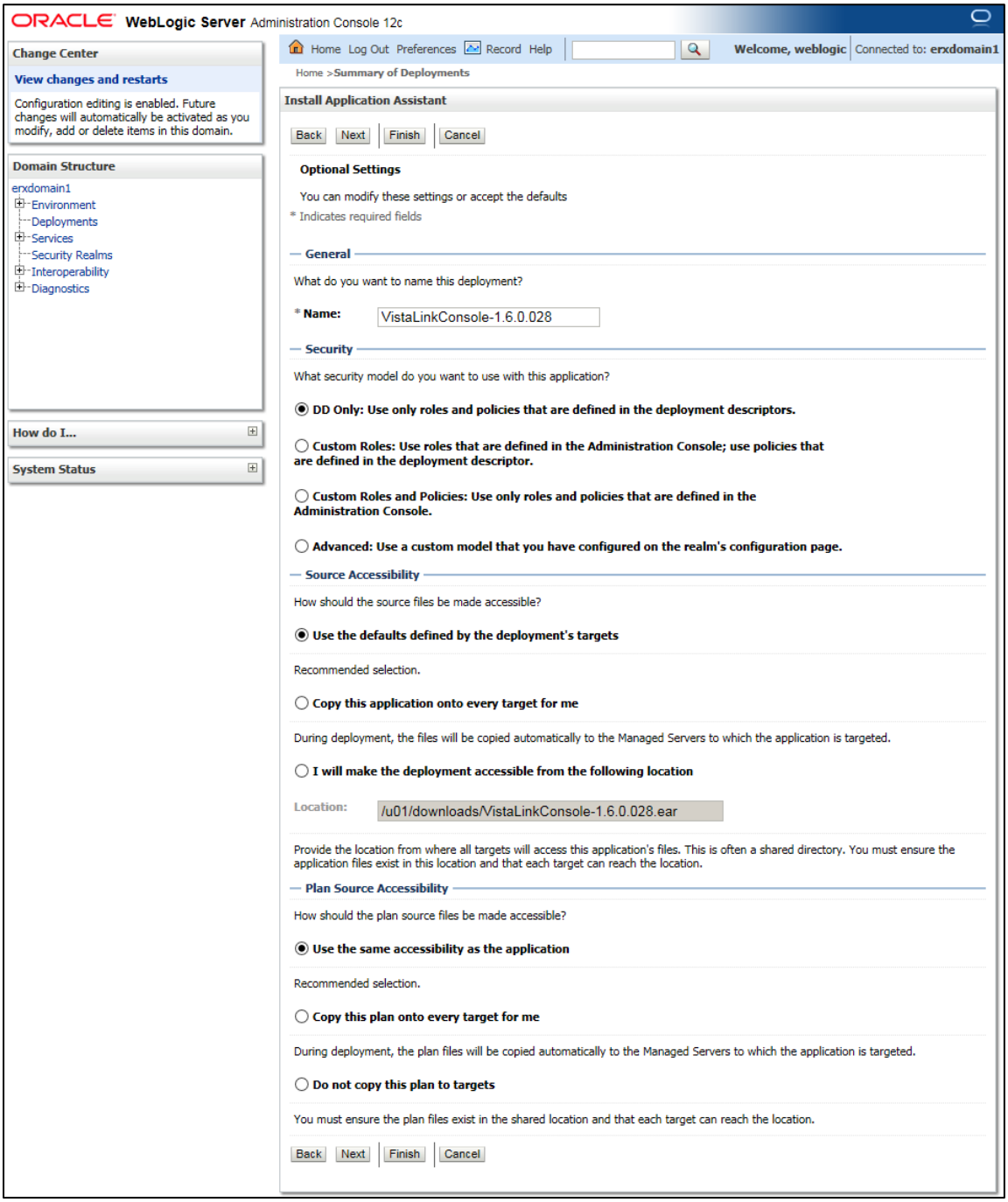
42. Select **All servers in the cluster** as the target for the deployment, and then select **Next**.

Figure 83: Deploy VistA Link Connector – Select Deployment Targets



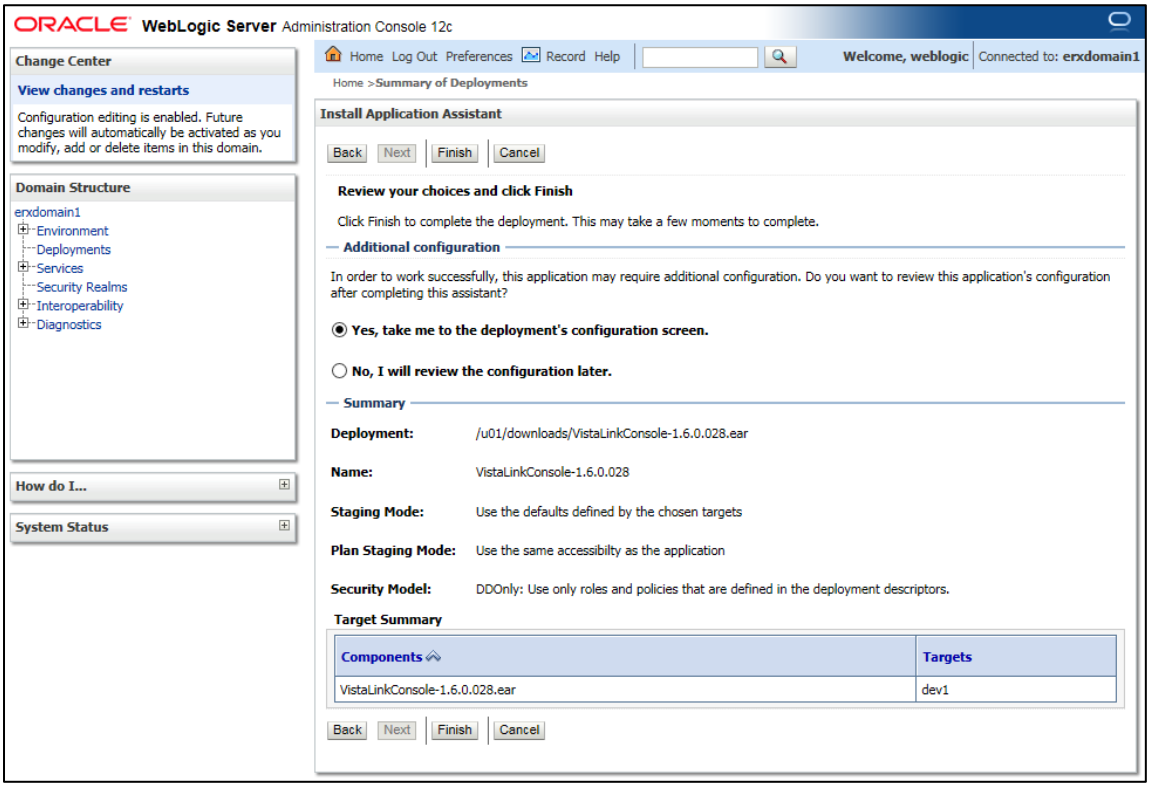
43. All of the values should appear as illustrated in the figure below.
44. Select **Next**.

Figure 84: Deploy VistA Link Connector – Summary of Deployments Verification 1



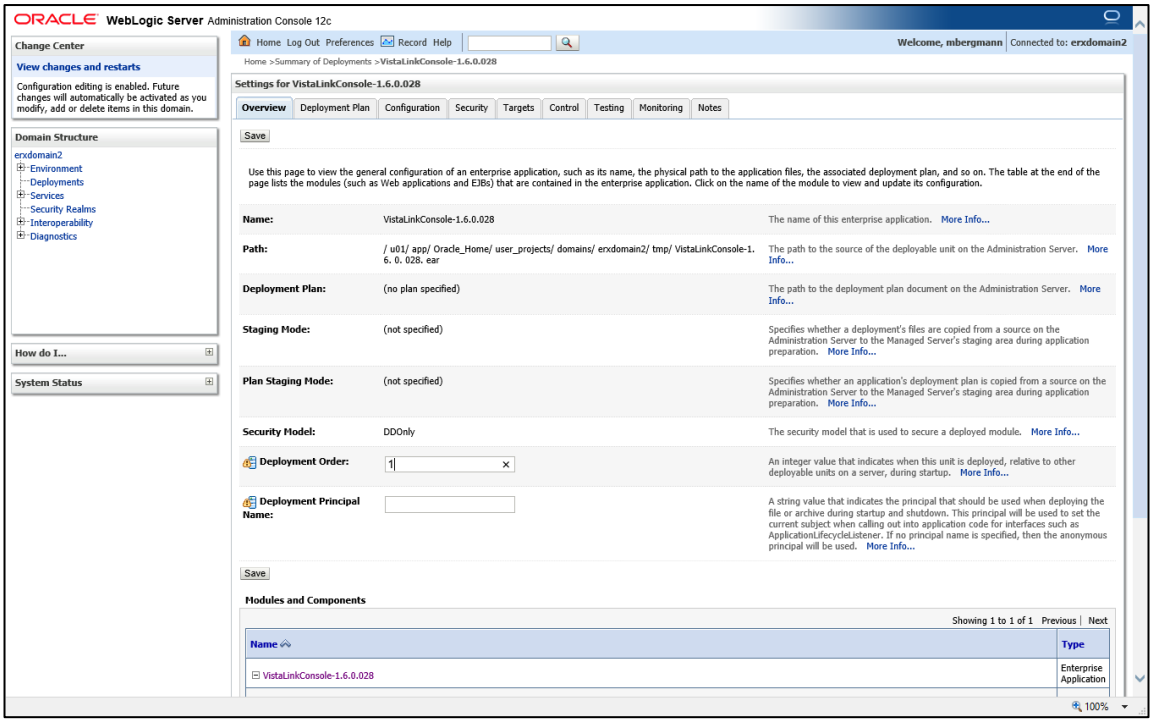
45. Verify that all of the values appear as illustrated in the figure below.
46. Select **Finish**.

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. Select **Save**.

Figure 86: Deploy VistA Link Connector – Deployment Configuration Screen

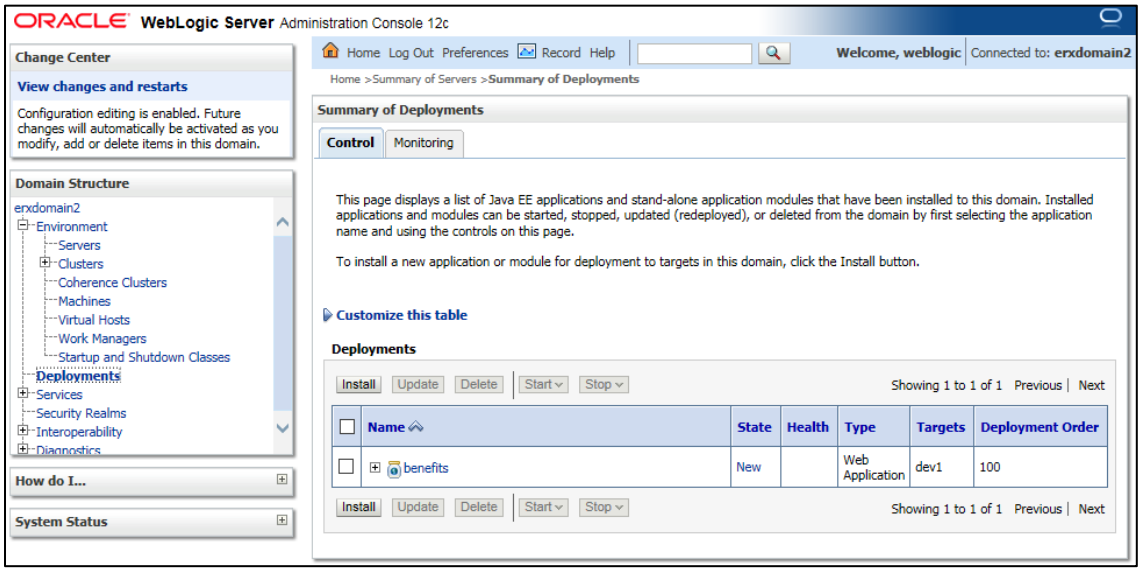


4.8.1.27 Deploy VistALink Adapters

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

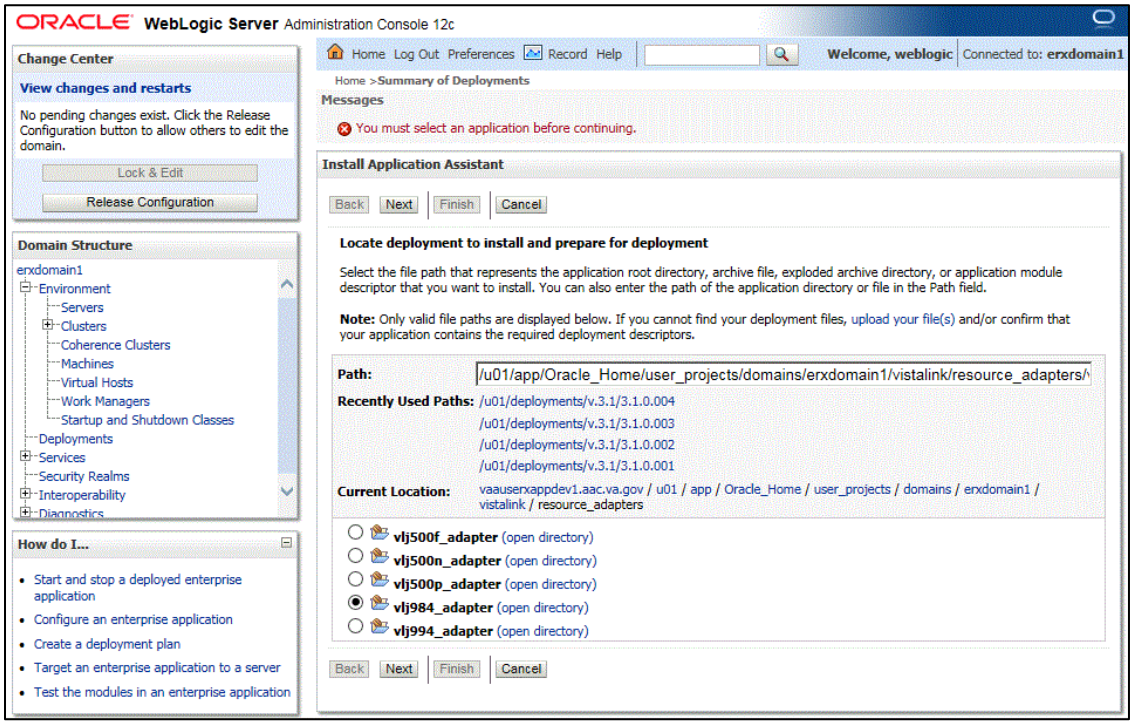
1. The WebLogic Administrator stops the VM1 managed server, per section: 7.2.2, step **Error! Reference source not found.**
2. The System Administrator executes the eRx/IEP Configurator script containing adapter configuration on VM1, menu options 1, 2 and 3.
3. The WebLogic Administrator will start the VM1 managed server, per section 7.1.2.
4. The WebLogic Administrator stops the VM2 managed server, per section: 7.2.2, step **Error! Reference source not found.**
5. The System Administrator executes the eRx/IEP Configurator script containing adapter configuration on VM2, menu options 1, 2 and 3.
6. The WebLogic Administrator will start the VM2 managed server, per section 7.1.2.
7. The WebLogic navigates to the *Deployment*s screen and selects **Install**.

Figure 87: Deploy VistA Link Connector – Deployments



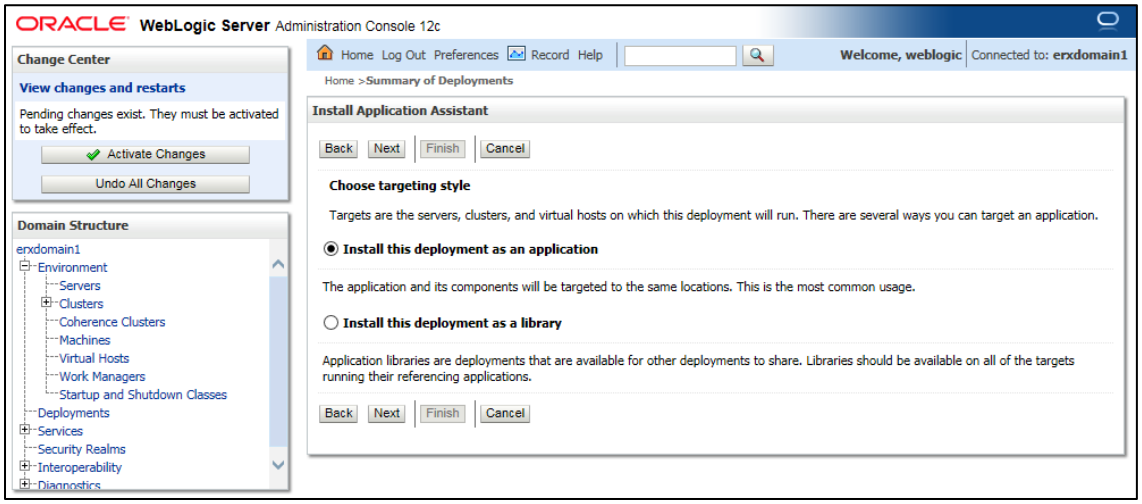
8. Enter *Path*: **[DOMAIN_HOME]**/vistalink/resource_adapters, .
9. Select the desired vljXXX_adapter to be installed, and then select **Next**.

Figure 88: Deploy VistA Link Connector – Select vljxxx_apapter to install



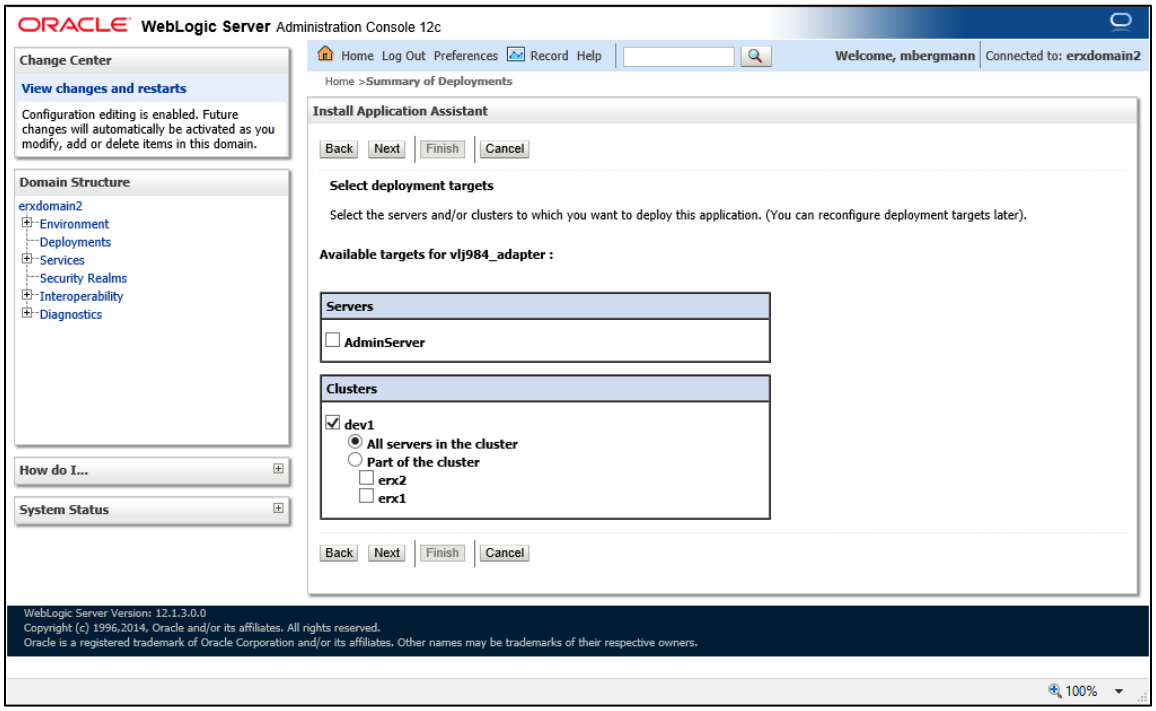
10. Select **Install this deployment as an application** as the target for the deployment, and then select **Next**.

Figure 89: Deploy VistA Link Connector – Select Deployment Type



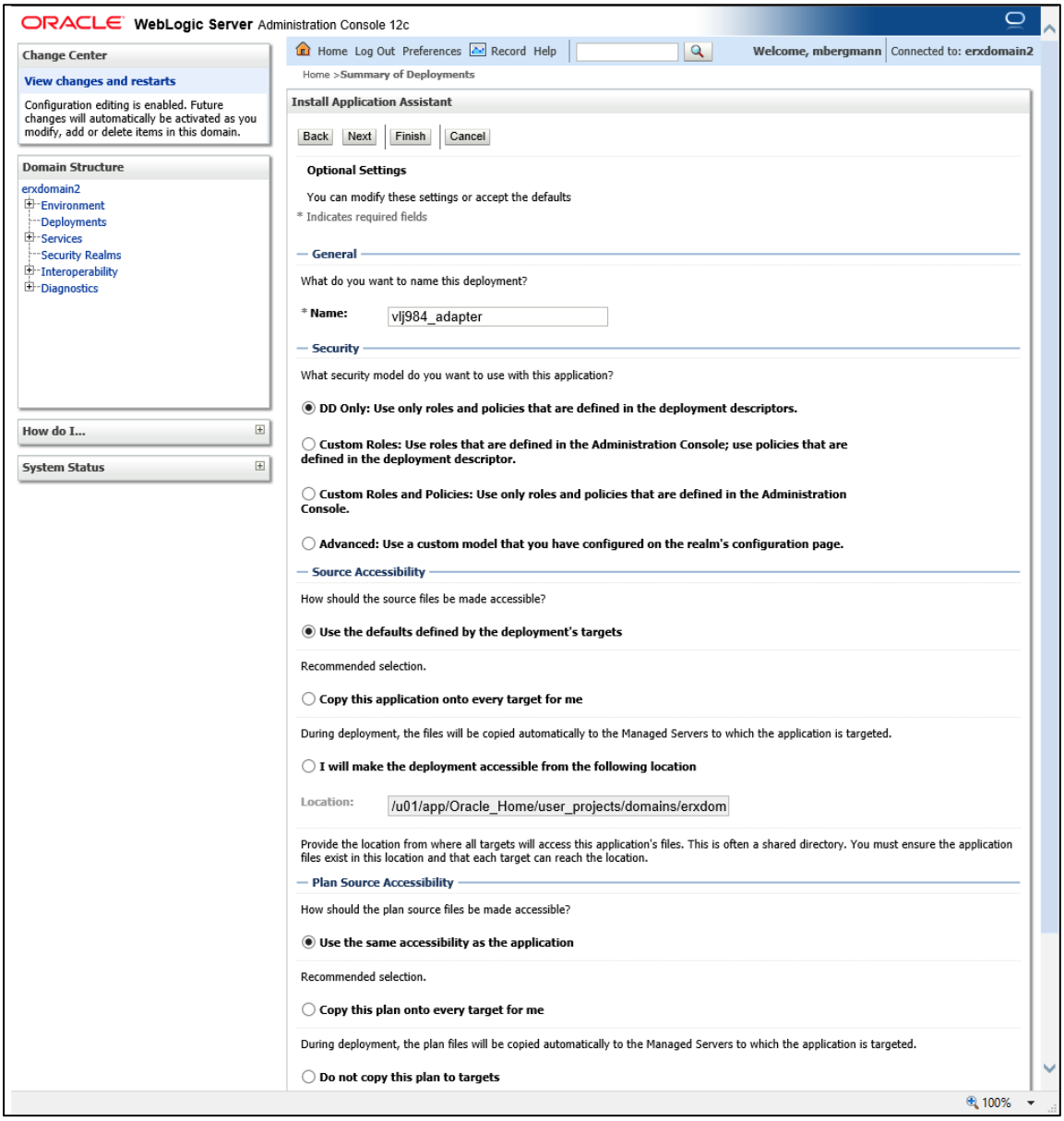
11. Select **All servers in the cluster** as the target for the deployment, and then select **Next**.

Figure 90: Deploy VistA Link Connector – Select Deployment Targets



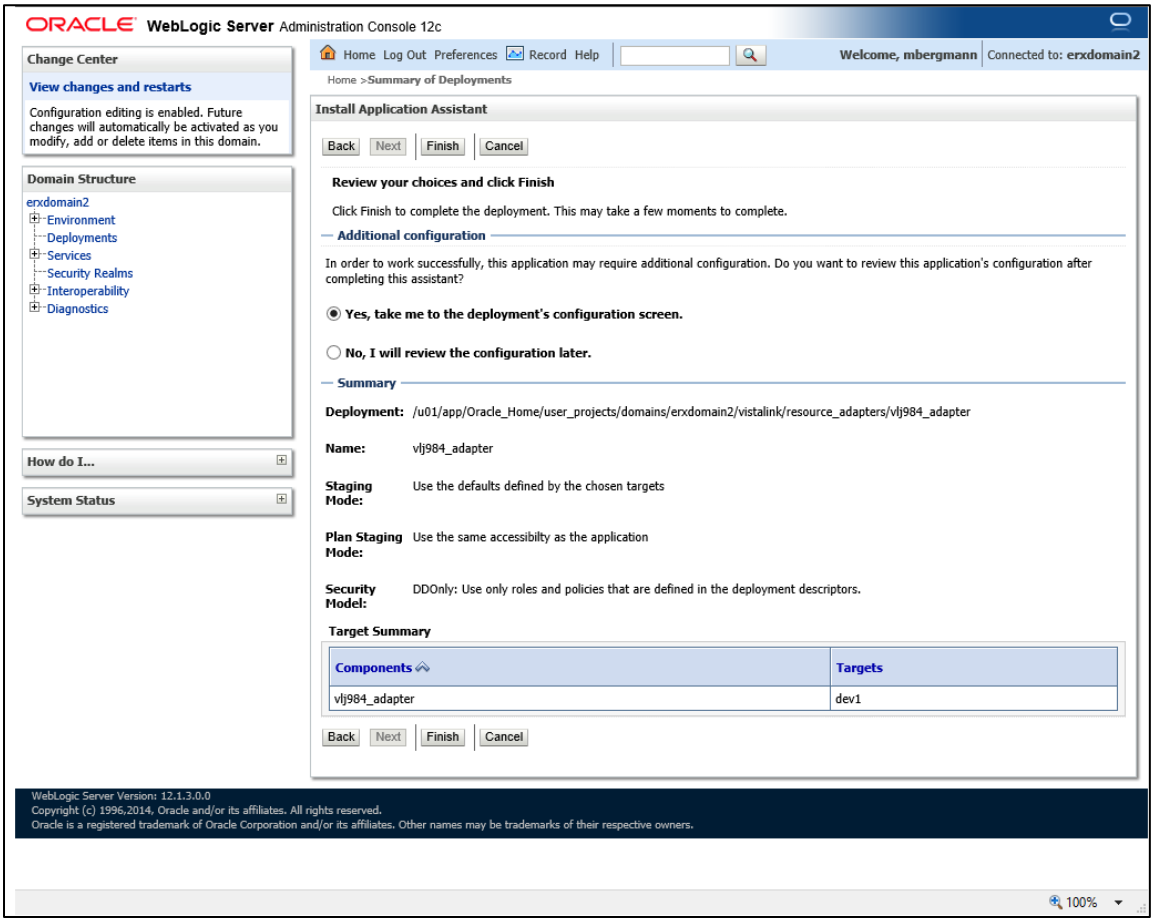
12. All of the values should appear as illustrated in the figure below.
13. Select **Next**.

Figure 91: Deploy VistA Link Connector – Adapter Optional Settings



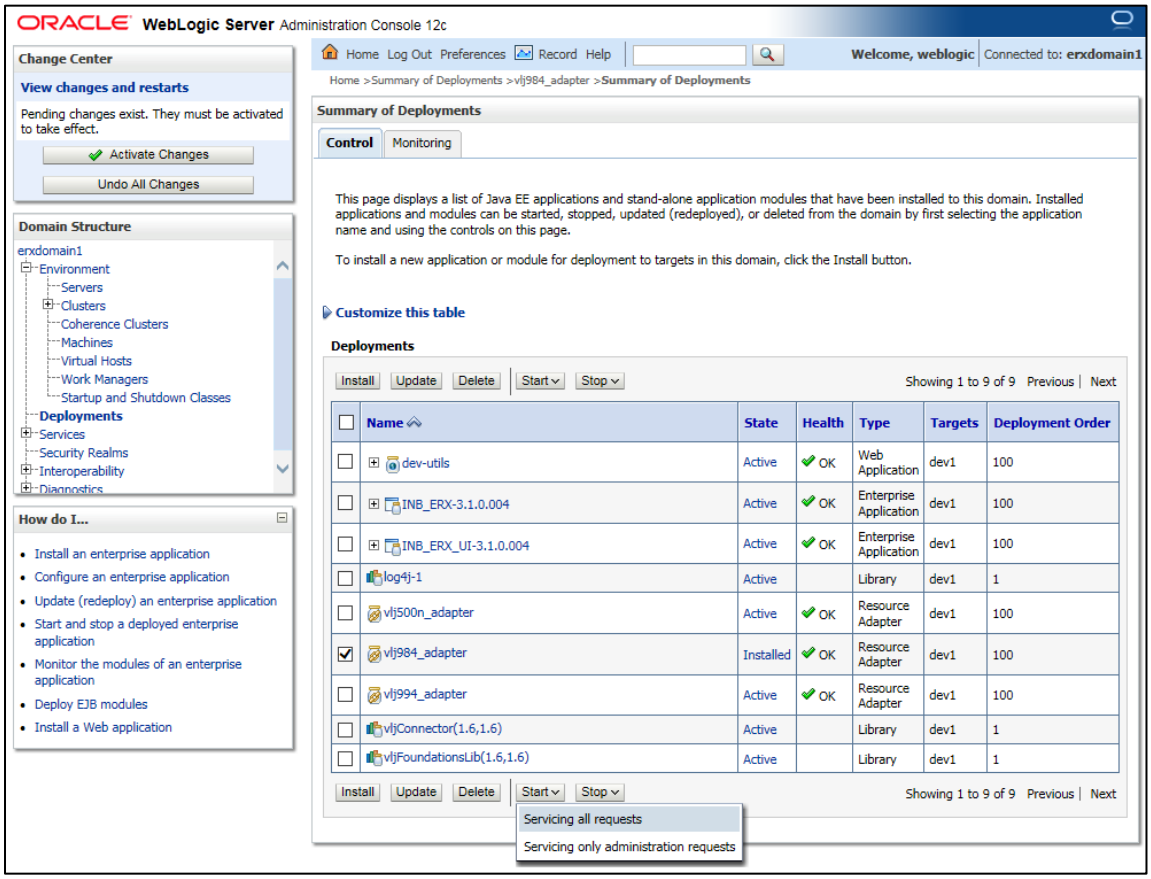
14. Verify that all of the values appear as illustrated in the figure below.
15. Select **Finish**.

Figure 92: Deploy VistA Link Connector – Finish Adapter Installation



16. Navigate to Deployments, select the **vljXXX_adapter**, select Start > Servicing all Requests.

Figure 93: Deploy VistA Link Connector – Start Resource Adapter



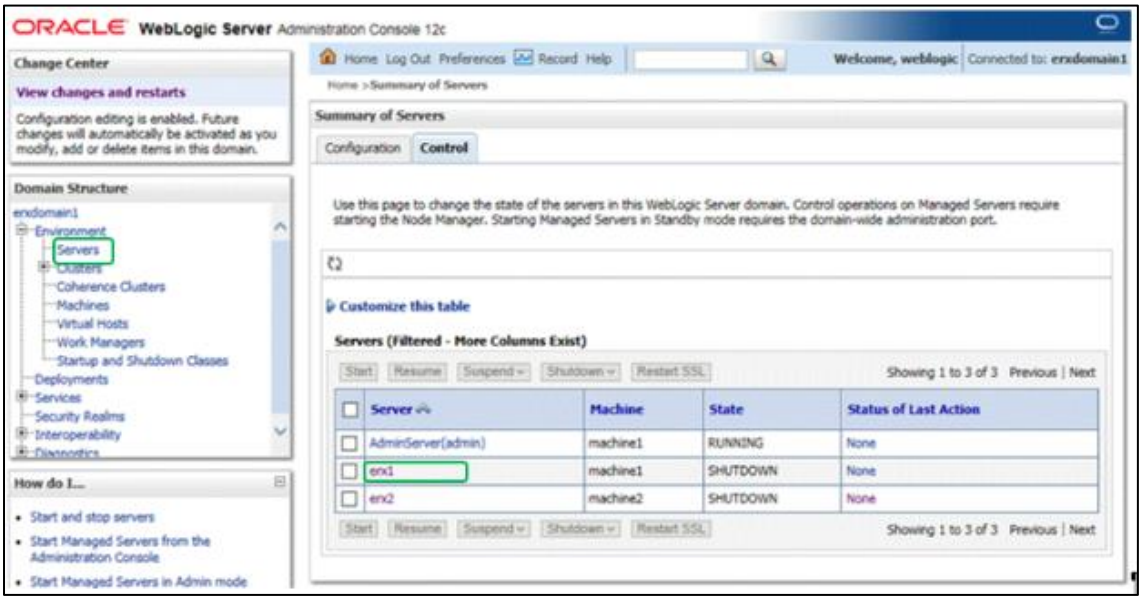
4.8.2 Inbound eRx Application Installation

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

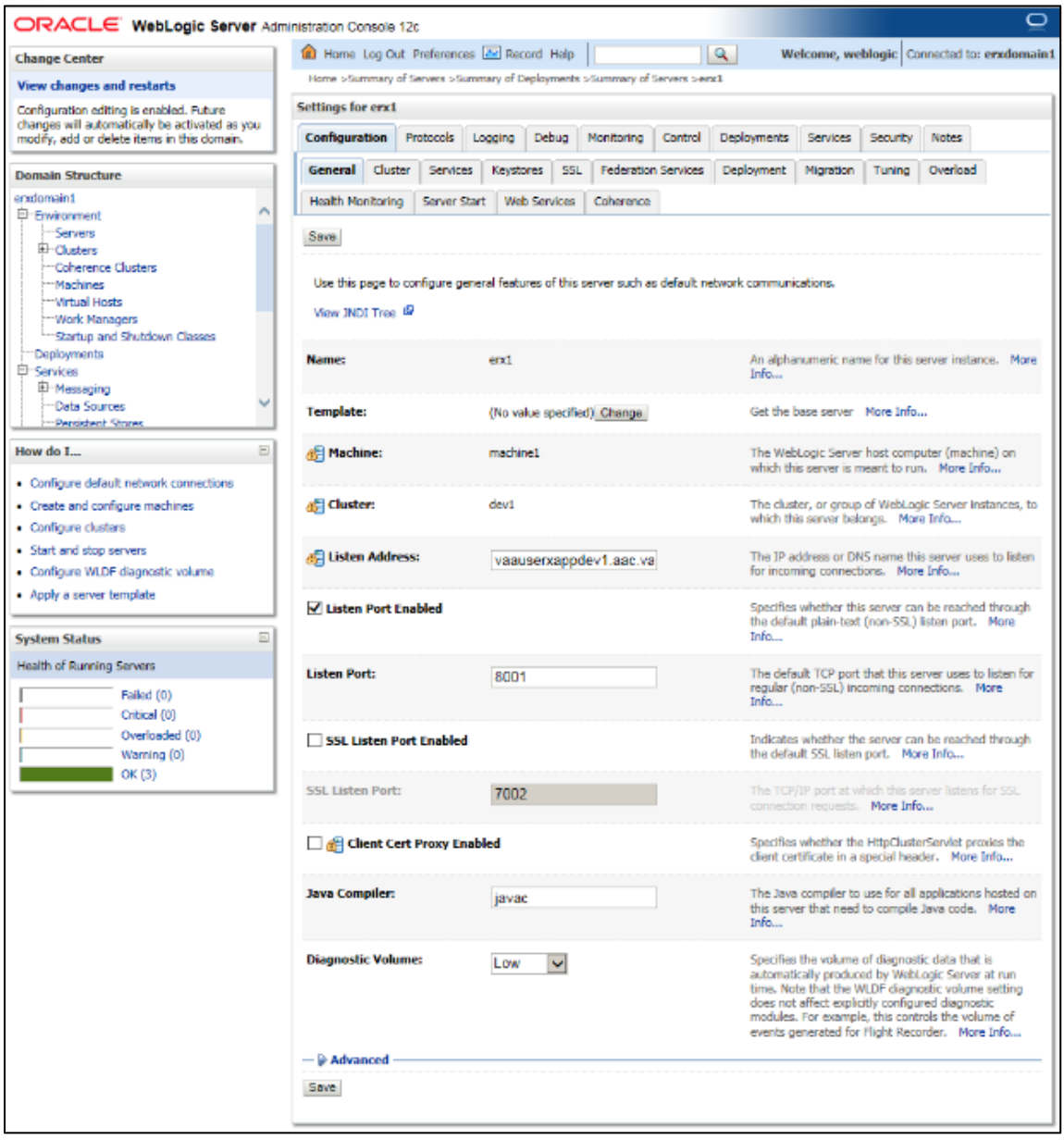
1. Shut down WebLogic (refer to Sections 4.8.2.3 and 4.8.2.4).
2. Log into Linux and sudo su to the weblogic account:
   ```
   $ sudo su - weblogic
   ```
3. Create the downloads directory if it doesn't exist:
   ```
   $ mkdir -p /u01/downloads
   ```
4. Download Inbound eRx application to the downloads 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, select the **erx1** link to configure the server.

Figure 94: Install Inbound eRx Application – Configure Servers



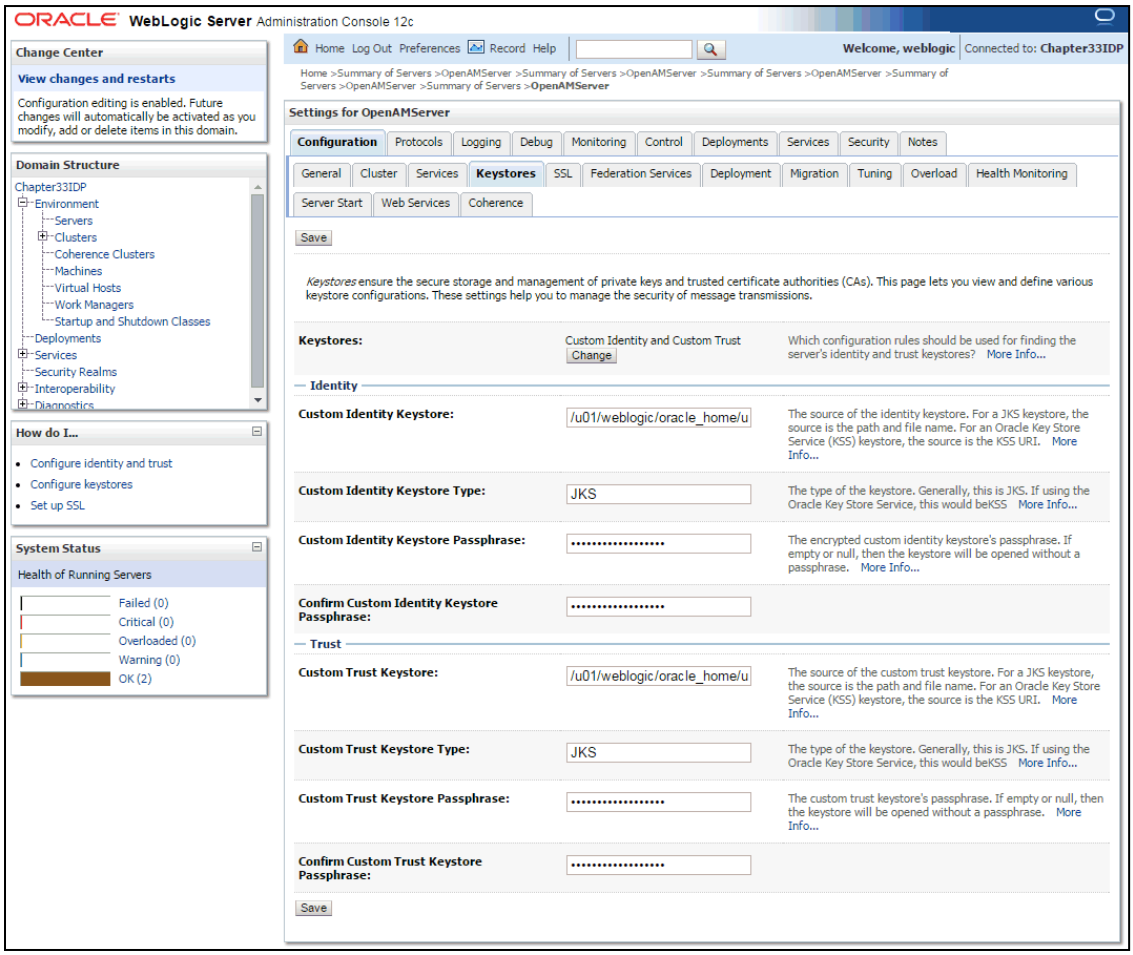
10. The server configuration screen should appear as shown in the figure below.
11. Inspect the settings under the **General** tab. The *Listen Address* should be ***[vm1_fqdn]***. The non-secure listening port (*Listen Port Enabled*) should be enabled and set to port **8001** (*Listen Port*). The secure 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 95: Install Inbound eRx Application – Verify Server Settings



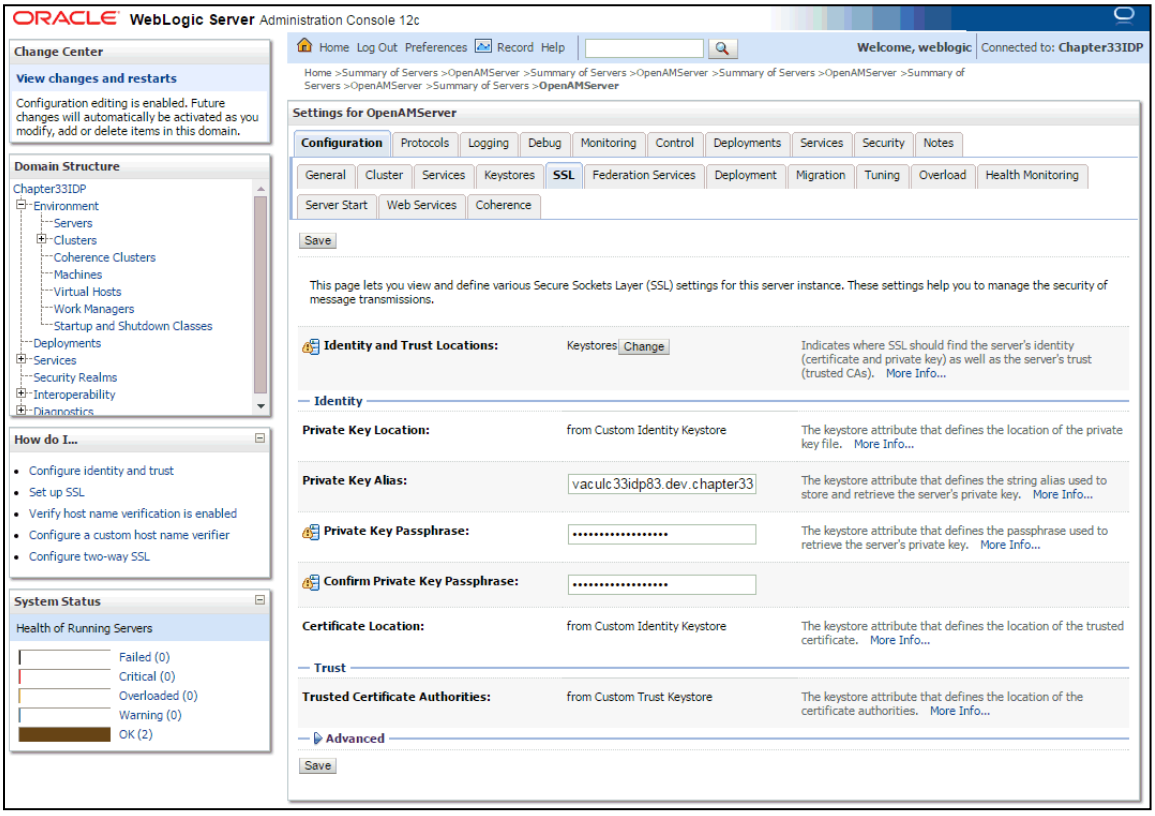
12. Review the setting under the **Keystores** tab as illustrated in the figure below. Verify the *Keystores* option is set to **Custom Identity and Custom Trust**, and that the fields under the *Identity* and *Trust* sections are filled with the same corresponding values.

Figure 96: 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 xxxxxxxx.

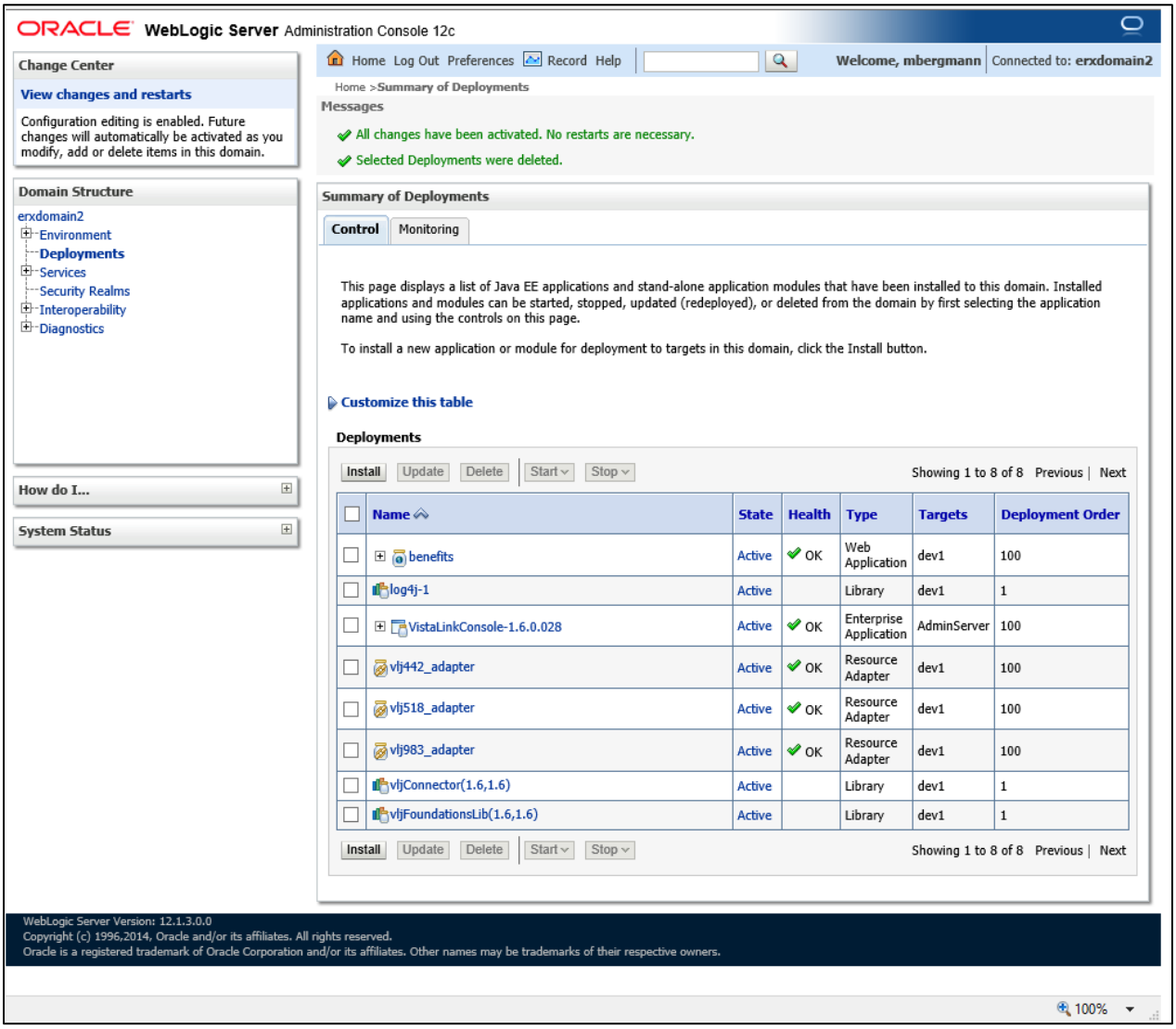
Figure 97: Install Inbound eRx Application – Verify SSL Settings



14. Repeat the previous three steps for the **erx2** managed server to verify the *General Configuration*, *Keystores*, and *SSL* settings.

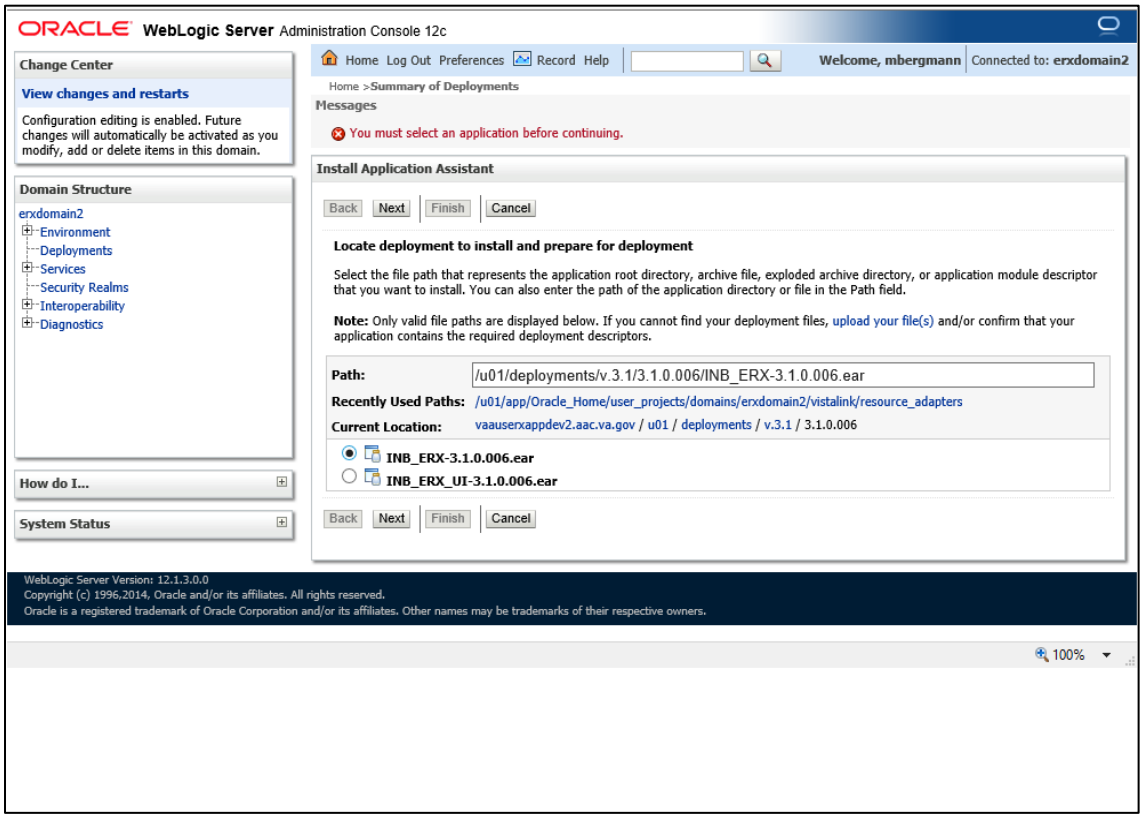
15. Navigate to the **Deployments** page.
16. From the **Deployments** page, select **Install**.

Figure 98: Install Inbound eRx Application – Summary of Deployments



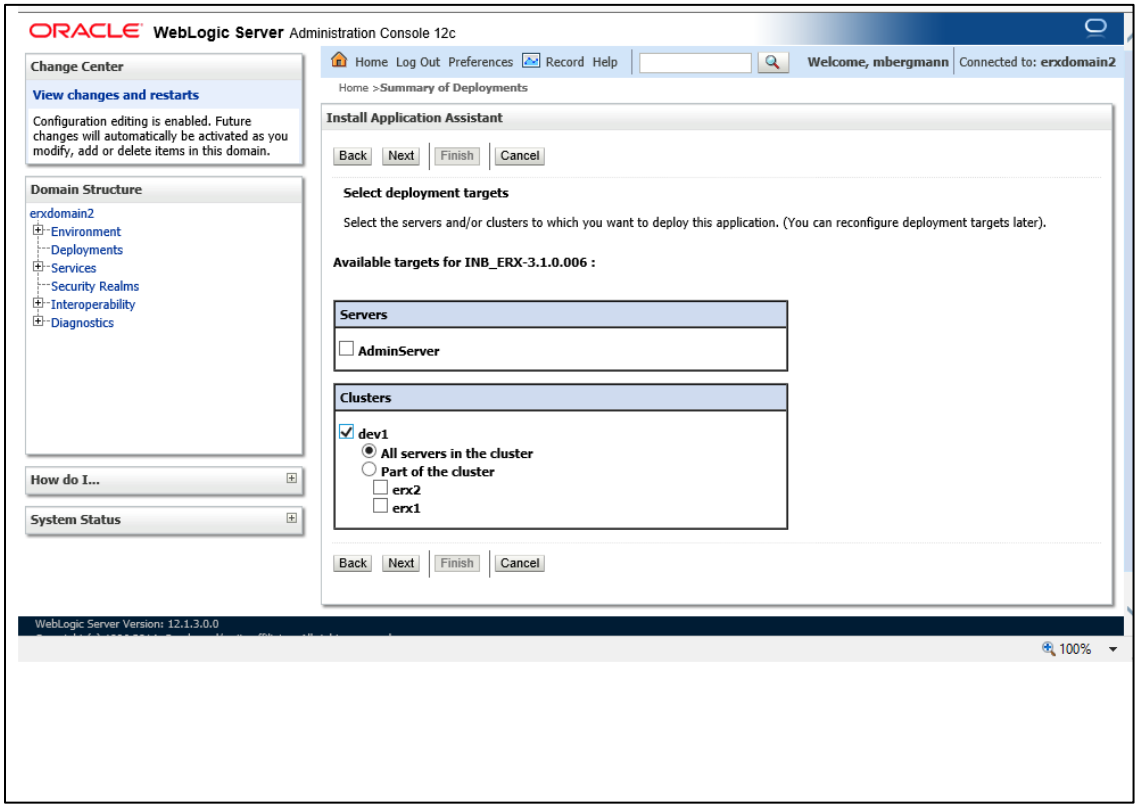
17. Install a new deployment of **INB_ ERX-3.1.0.006.ear** using the .ear file as indicated in the figure below.
18. select **Next**.

Figure 99: Install Inbound eRx Application – Install New Deployment of INB_ERX



19. Accept the defaults for an application deployment.
20. Select **Next**.
21. Select the cluster and **All servers in the cluster** as the target for the deployment.
22. Select **Next**.

Figure 100: Install Inbound eRx Application – Select INB_ERX Deployment Targets



23. All of the values should appear as illustrated in the figure below.
24. Select **Next**.

Figure 101: Install Inbound eRx Application – Verify INB_ERX Deployment Settings

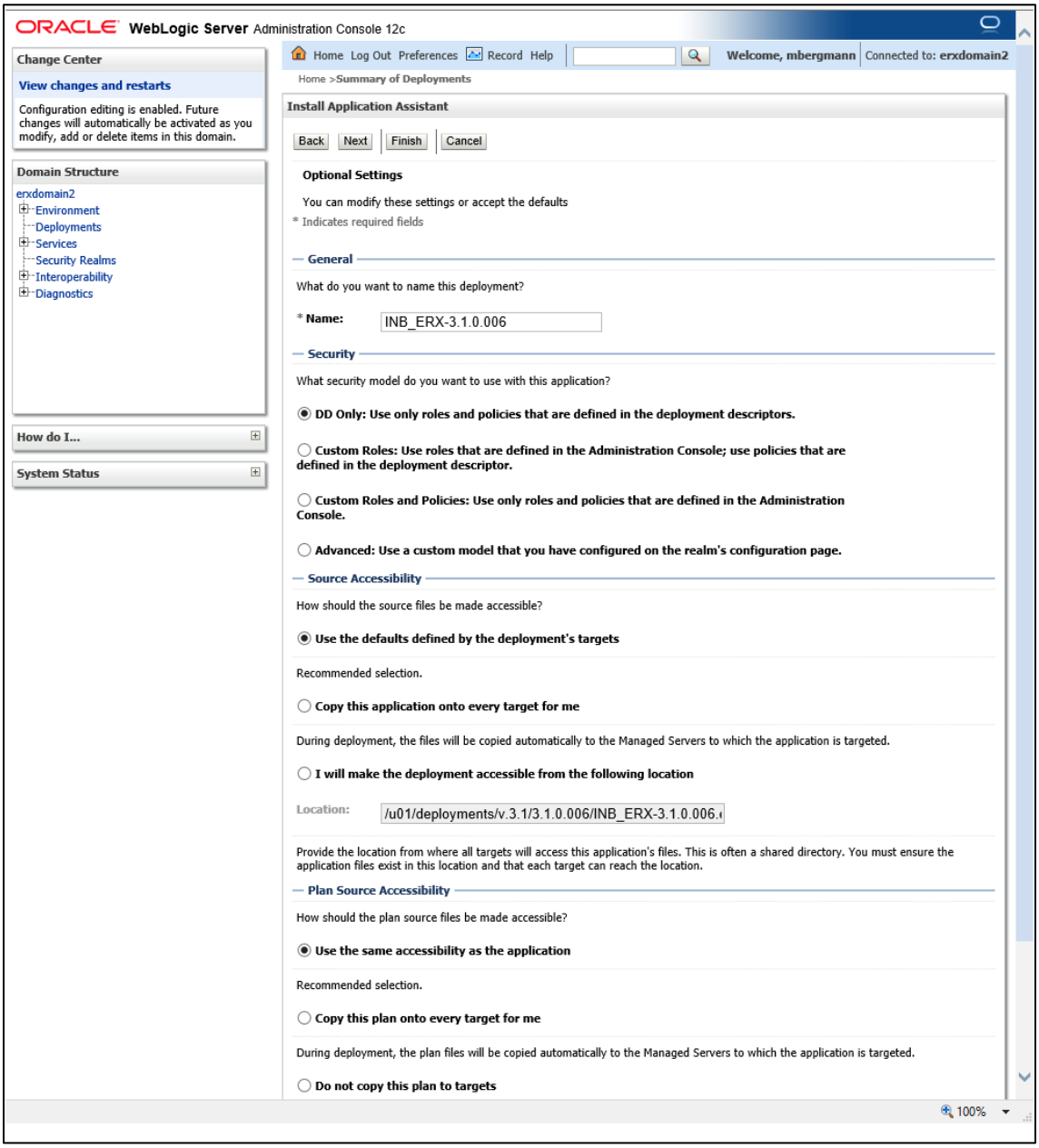
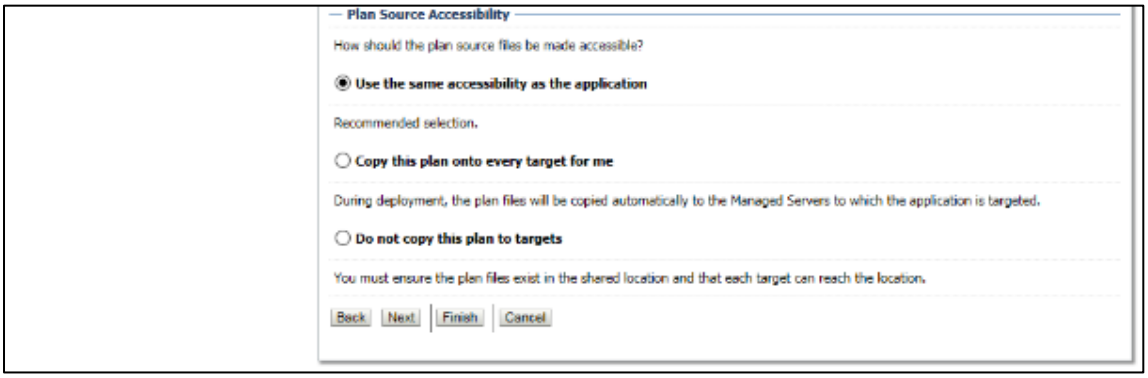
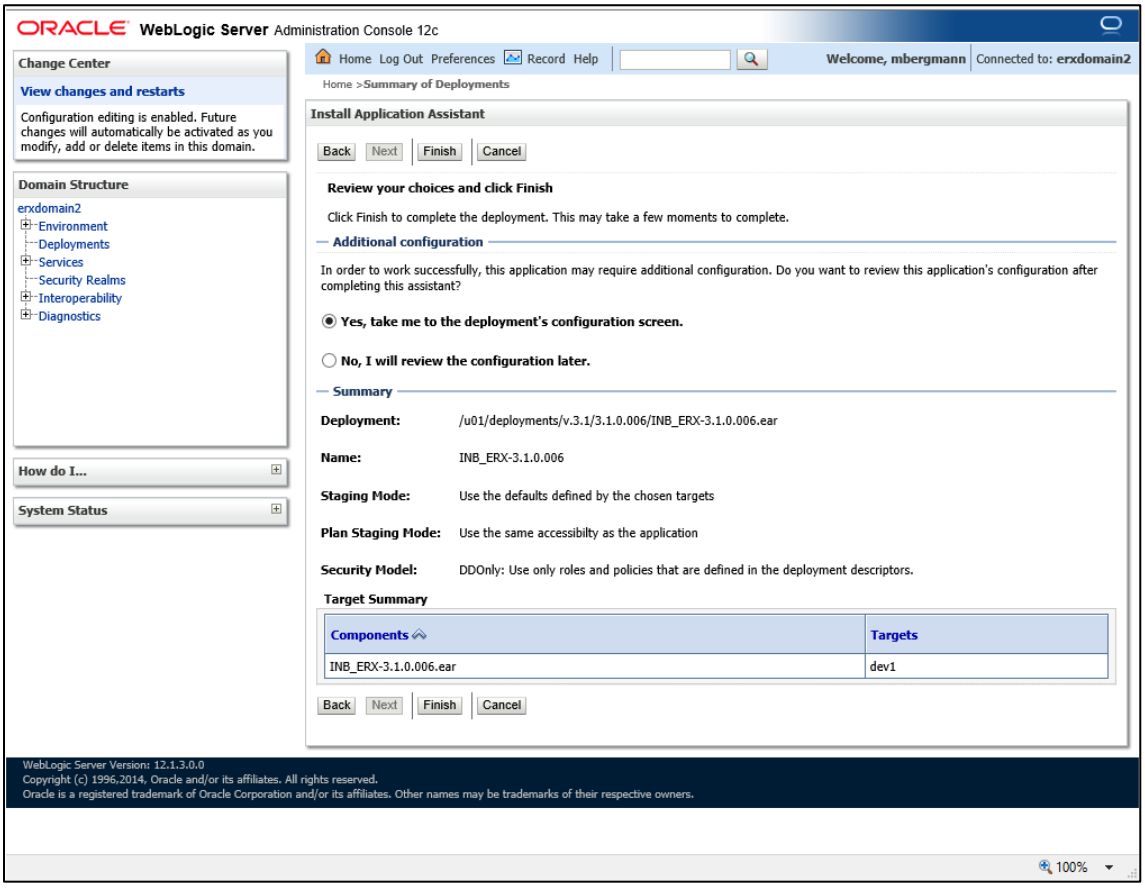


Figure 102: Install Inbound eRx Application – Verify INB_ERX Deployment Continued



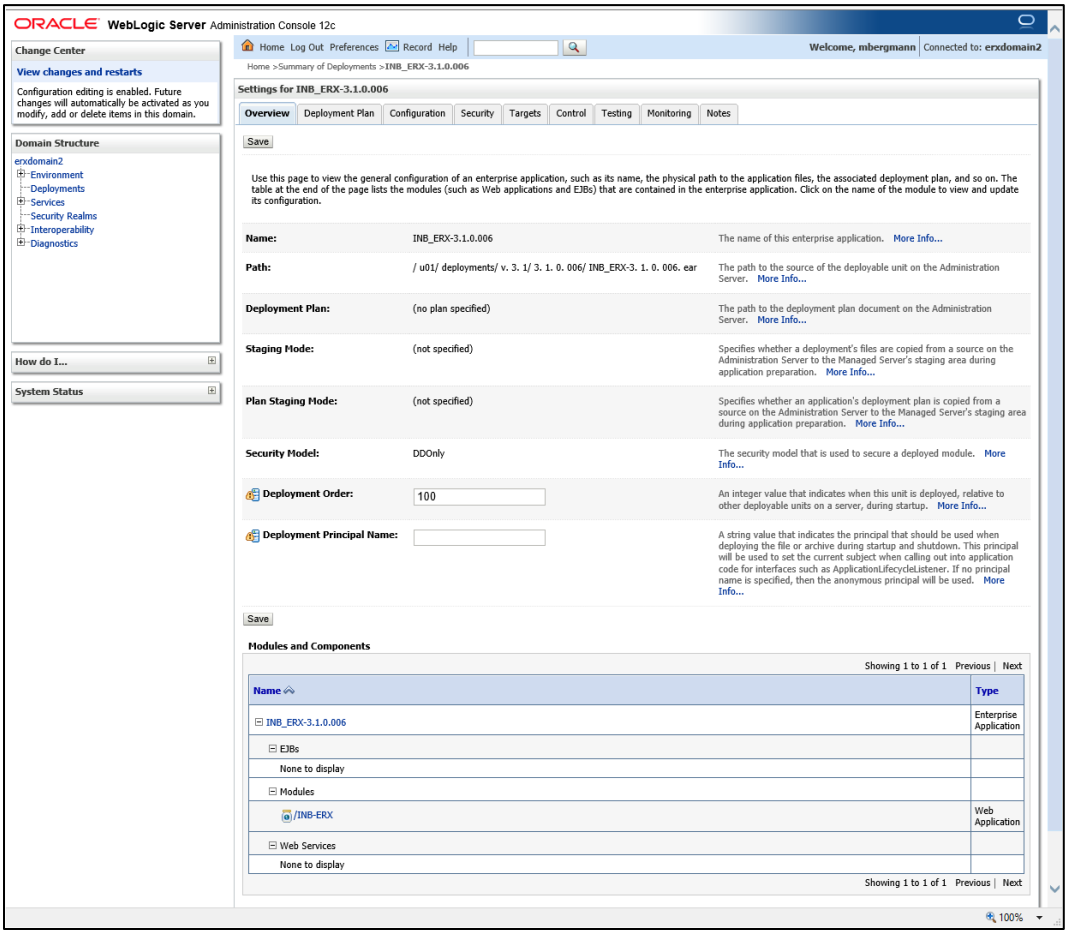
25. All of the values should appear as illustrated in the figure below.
26. Select **Finish**.

Figure 103: Install Inbound eRx Application – Verify INB_ERX Deployment Settings (Finish)



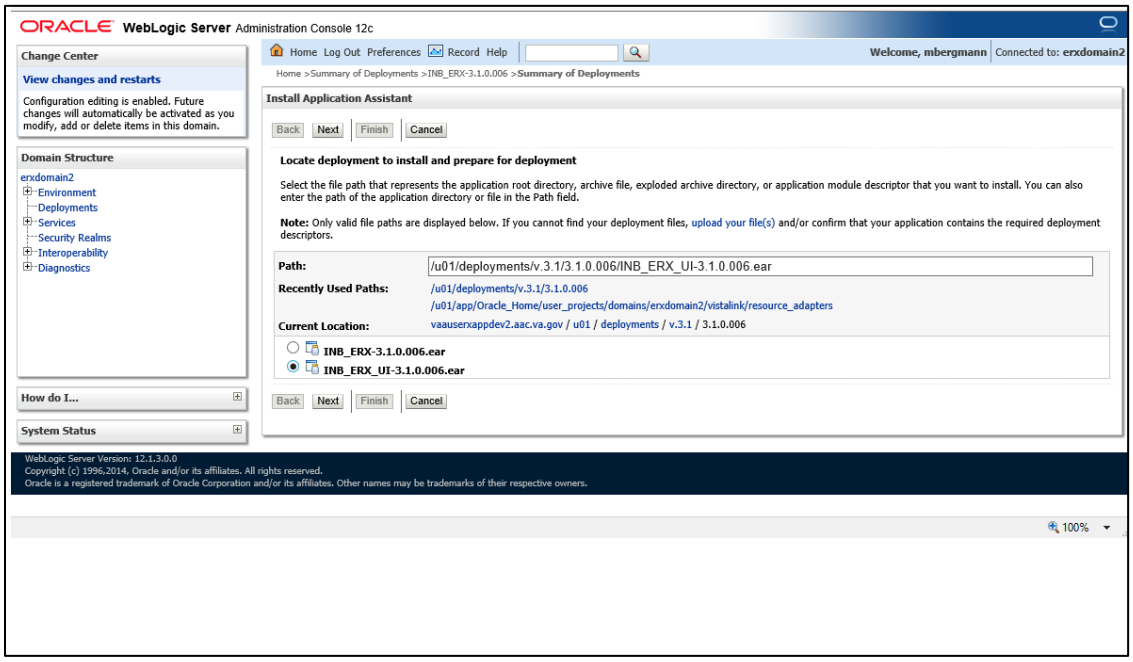
27. The **Overview** tab should appear as illustrated in the figure below.

Figure 104: Install Inbound eRx Application – Verify INB_ERX Deployment Configuration Settings



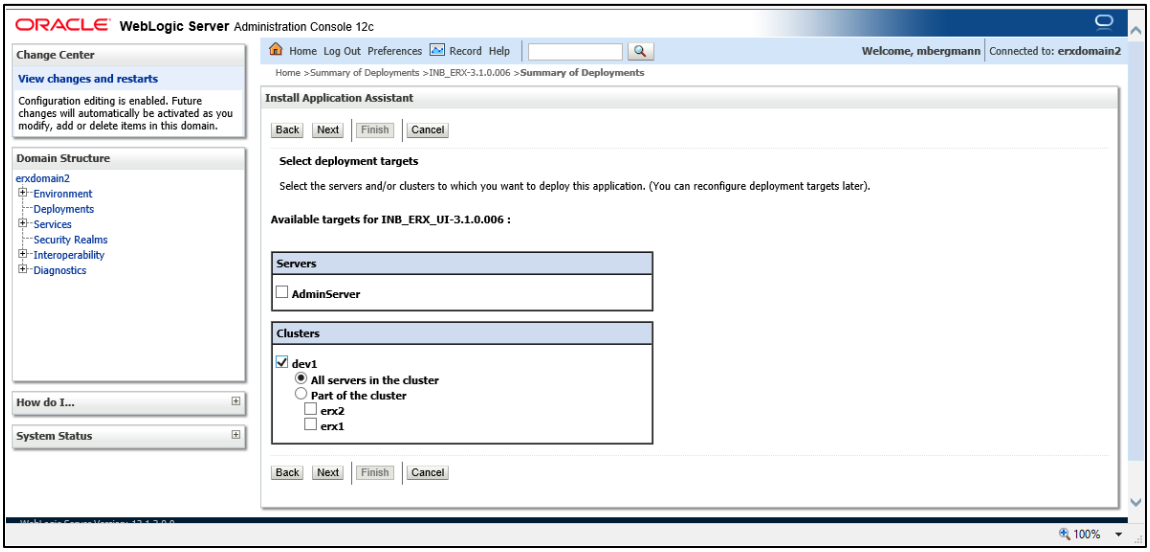
28. Navigate to the **Deployments** page.
29. From the **Deployments** page, select **Install**.
30. Install a new deployment of **INB_ERX_UI-3.1.0.006.ear**, select the appropriate EAR file.
31. Select **Next**.

Figure 105: Install Inbound eRx Application – Install New Deployment of INB_ERX_UI



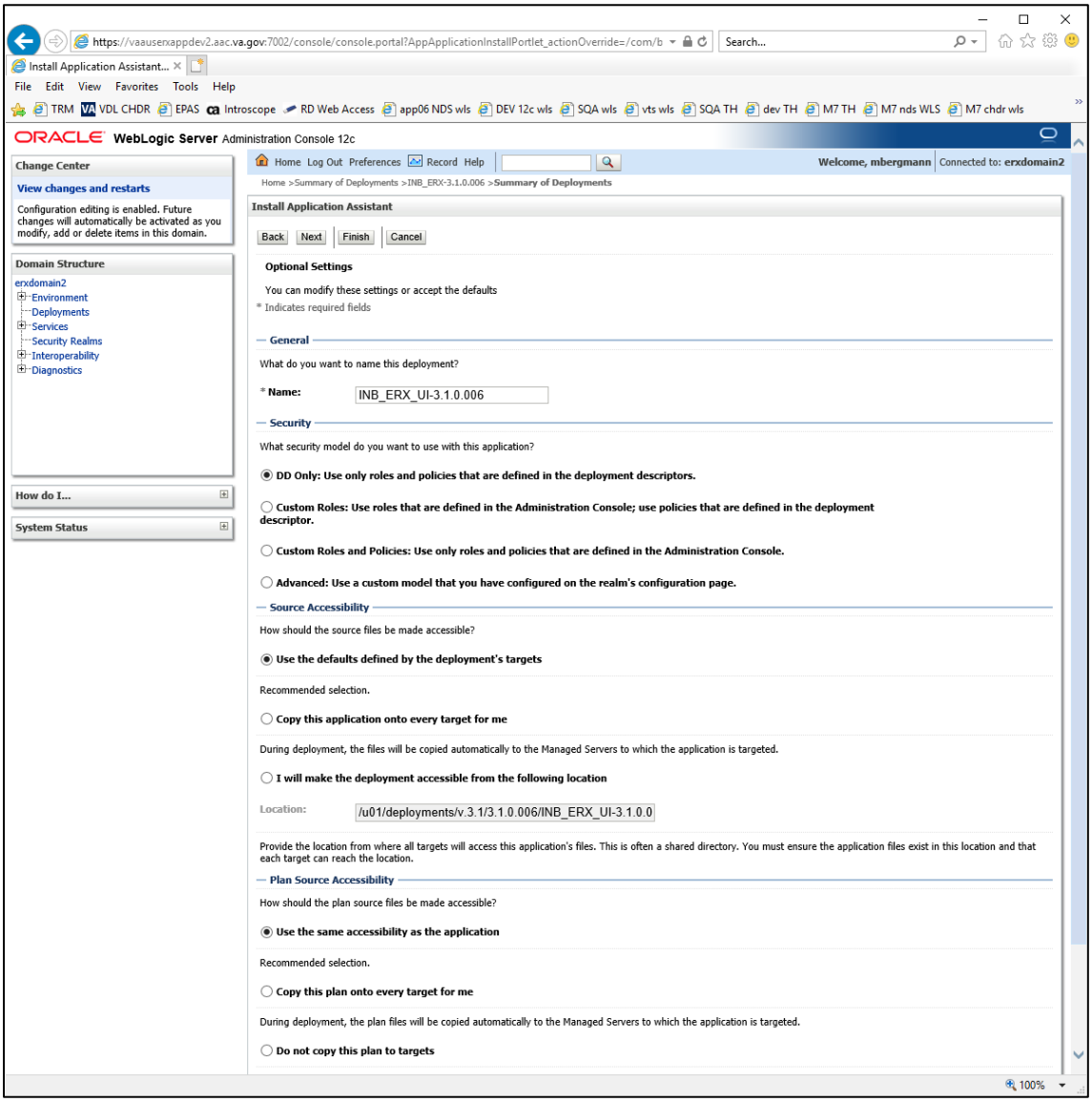
32. Accept the defaults for an application deployment.
33. Select **Next**.
34. Select the cluster and **All servers in the cluster** as the target for the deployment.
35. Select **Next**.

Figure 106: Install Inbound eRx Application – Select INB_ERX_UI Deployment Targets



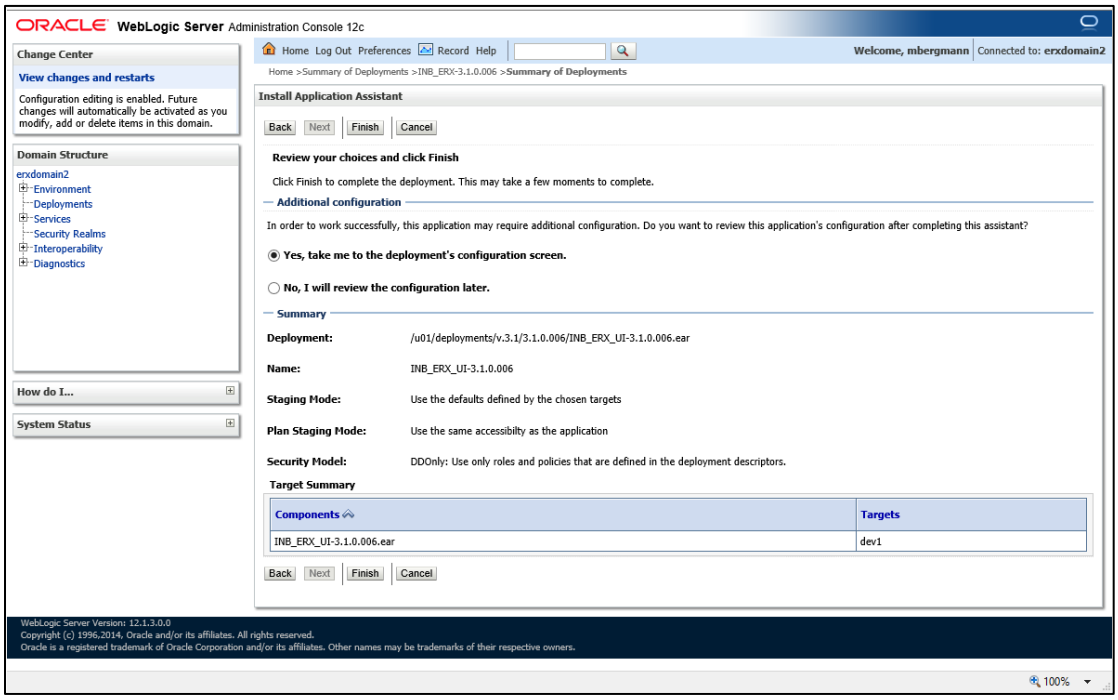
36. All of the values should appear as illustrated in the figure below.
37. Select **Next**.

Figure 107: Install Inbound eRx Application – Verify INB_ERX_UI Deployment Settings



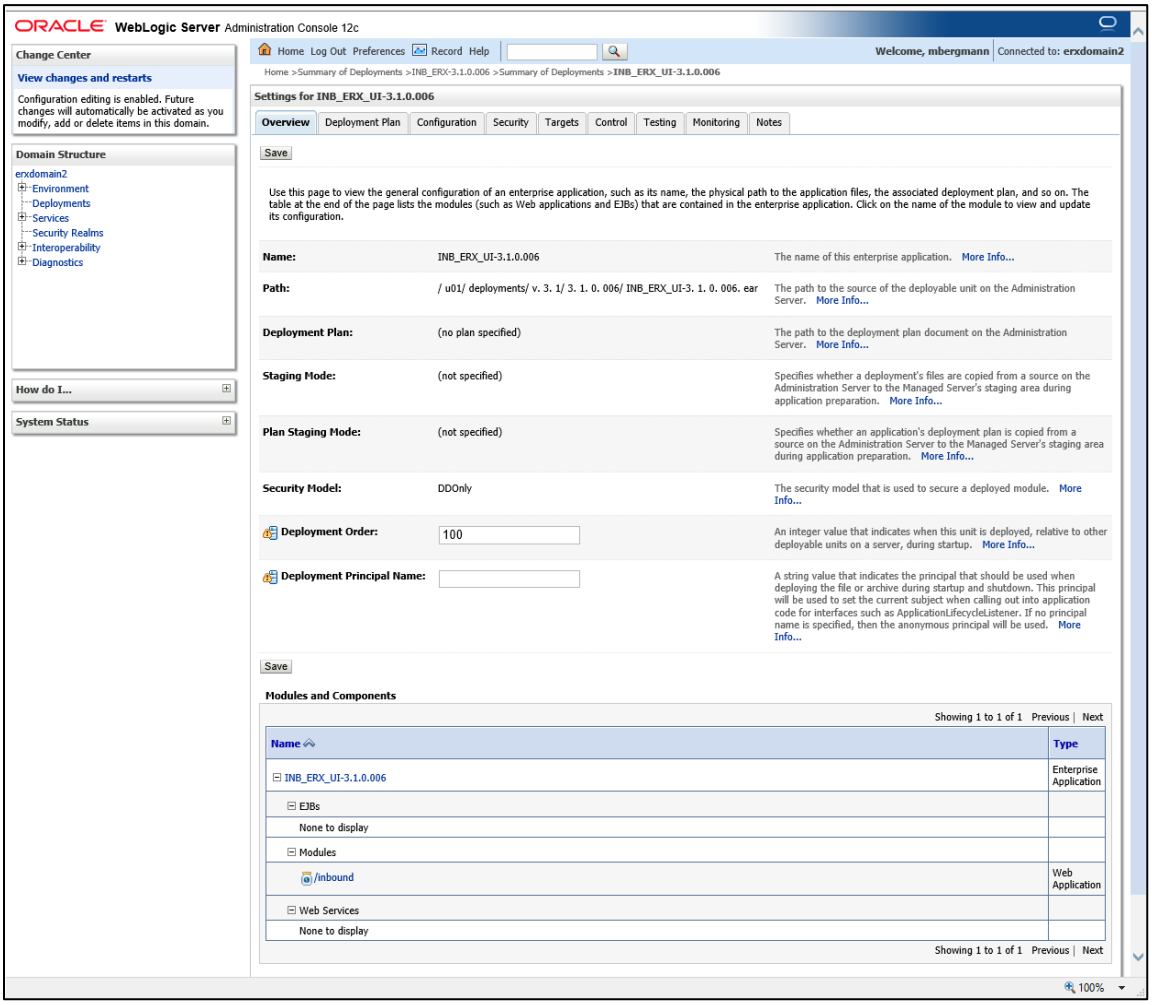
38. All of the values should appear as illustrated in the figure below.
39. Select **Finish**.

Figure 108: Install Inbound eRx Application – Verify INB_ERX_UI Deployment Settings (Finish)



40. The **Overview** tab should appear as illustrated in the figure below.

Figure 109: 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 select **Start**.

Figure 110: Install Inbound eRx Application – Start erx Servers

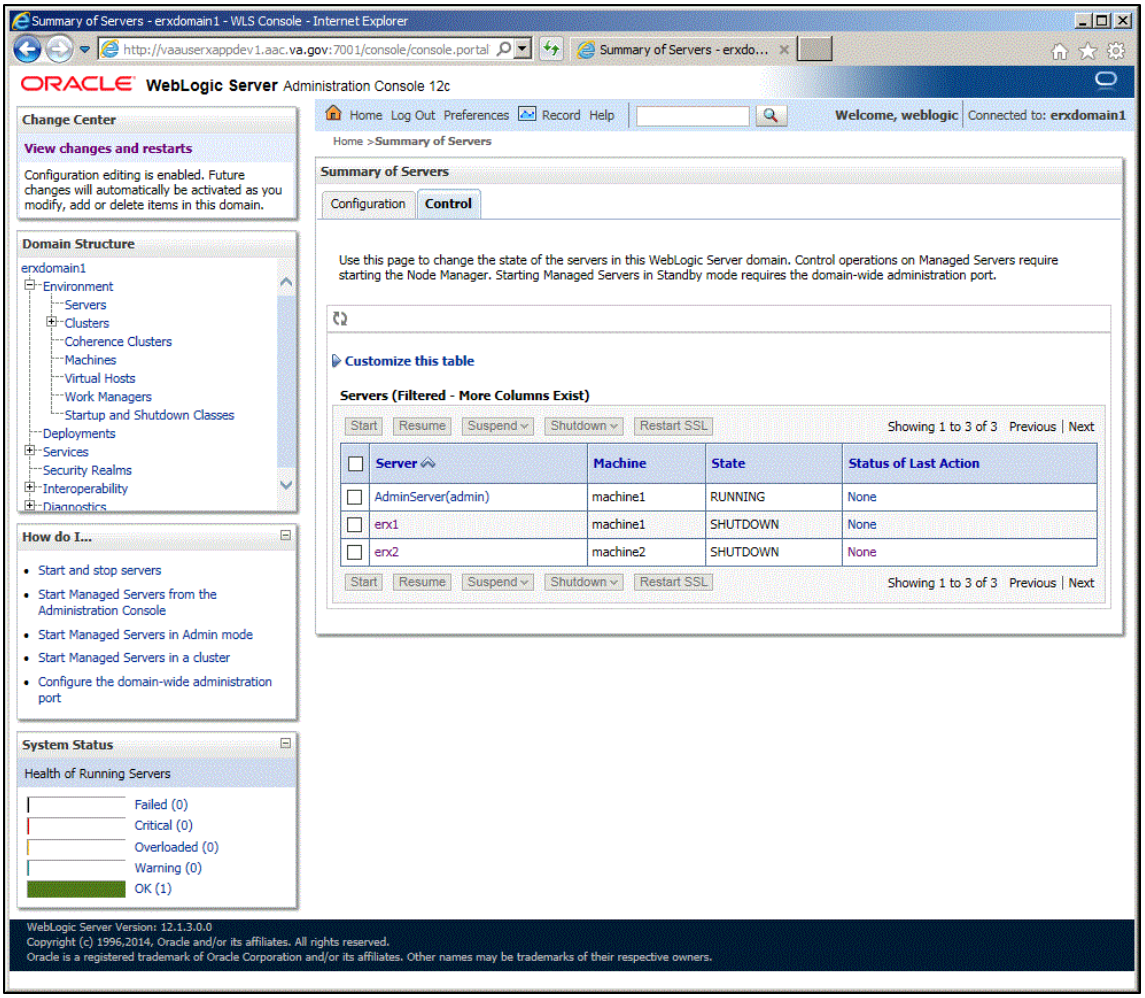
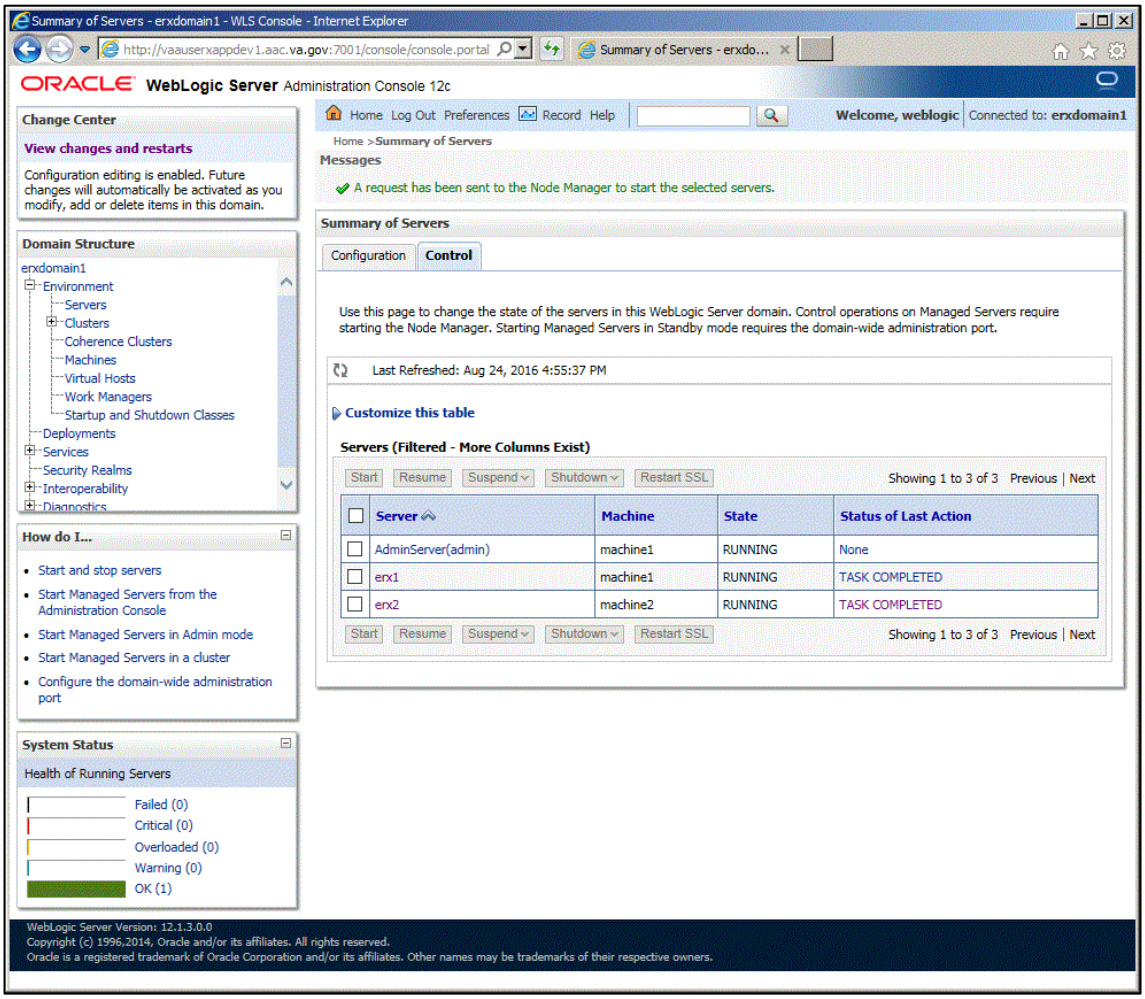


Figure 111: Install Inbound eRx Application – erx Servers Running



4.8.2.2 Create Startup/Shutdown Scripts

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

1. Log into Linux and 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, log into Linux login and 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 Nodemanagers

This sections outlines the steps for shutting down the nodemanagers:

1. On VM1, Log into Linux and sudo su to the weblogic account:
   ```
   $ sudo su - weblogic
   ```
2. Shut down Nodemanager with the following command:
   ```
   $ ./stopNodemanager_[domain].sh
   ```
3. On VM2, Log into Linux and 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. Log into Linux and sudo su to the kettle account:
   ```
   $ sudo su - kettle
   ```
2. Create downloads directory if it doesn't exist:
   ```
   $ mkdir -p /u01/downloads
   ```
3. Download Pentaho Data Integration Community Edition 8.2 archive (pdi-ce-8.2.0.0-342.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:
   ```
   $ mkdir -p /u01/app/pentaho
   ```
6. On VM1, unzip the Pentaho Data Integration Community Edition 8.2 archive to the pentaho master1 installation directory:
   ```
   $ cd /u01/app/pentaho
   $ unzip /u01/downloads/pdi-ce-8.2.0.0-342.zip
   $ mv data-integration pdi-[env]master1
   ```
7. On VM1, unzip the Pentaho Data Integration Community Edition 8.2 archive to the pentaho slave1 installation directory:
   ```
   $ cd /u01/app/pentaho
   $ unzip /u01/downloads/pdi-ce-8.2.0.0-342.zip
   $ mv data-integration pdi-[env]slave1
   ```
8. On VM1, unzip the Pentaho Data Integration Community Edition 8.2 archive to the pentaho slave2 installation directory:
   ```
   $ cd /u01/app/pentaho
   $ unzip /u01/downloads/pdi-ce-8.2.0.0-342.zip
   $ mv data-integration pdi-[env]slave2
   ```
9. On VM2, unzip the Pentaho Data Integration Community Edition 8.2 archive to the pentaho slave3 installation directory:
   ```
   $ cd /u01/app/pentaho
   $ unzip /u01/downloads/pdi-ce-8.2.0.0-342.zip
   $ mv data-integration pdi-[env]slave3
   ```
10. On VM2, unzip the Pentaho Data Integration Community Edition 8.2 archive to the pentaho slave4 installation directory:
    ```
    $ cd /u01/app/pentaho
    $ unzip /u01/downloads/pdi-ce-8.2.0.0-342.zip
    $ mv data-integration pdi-[env]slave4
    ```
11. On VM2, unzip the Pentaho Data Integration Community Edition 8.2 archive to the pentaho slave5 installation directory:
    ```
    $ cd /u01/app/pentaho
    $ unzip /u01/downloads/pdi-ce-8.2.0.0-342.zip
    $ mv data-integration pdi-[env]slave5
    ```

12. On VM1, unzip the environment specific configuration archive to the pentaho master1 installation directory:

```
$ cd /u01/app/pentaho/pdi-[env]master1
$ unzip /u01/downloads/pdi-[env]_cfg_[yyyymmdd].zip
```

13. 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
```

14. 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
```

15. 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
```

16. 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
```

17. On VM2, unzip the environment specific configuration archive to the pentaho slave5 installation directory:

```
$ cd /u01/app/pentaho/pdi-[env]slave5
$ unzip /u01/downloads/pdi-[env]_cfg_[yyyymmdd].zip
```

18. 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 >
${KETTLE_HOME}/logs/[env]slave1-8082_${datestamp}.out 2>&1 &
<ctlr>d
$ chmod 755 ~/startCarte[Env]Slave2.sh
```

19. On the Master VM, create slave3, slave4 and slave5 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]slavefx3-8083.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-[env]slave4
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]slave4-8084.xml >
${KETTLE_HOME}/logs/[env]slave4-8084_${datestamp}.out 2>&1 &
<ctlr>d
$ chmod 755 ~/startCarte[Env]Slave4.sh

$ cat > ~/startCarte[Env]Slave5.sh
unset DISPLAY
export KETTLE_HOME=/u01/app/pentaho/pdi-[env]slave5
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]slave5-8085.xml >
${KETTLE_HOME}/logs/[env]slave5-8085_${datestamp}.out 2>&1 &
<ctlr>d
$ chmod 755 ~/startCarte[Env]Slave5.sh
```

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

```
$ cd ~
$ cat > ~/updateRepo[Env].sh
unset DISPLAY
export KETTLE_HOME=/u01/app/pentaho/pdi-[env]master1
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
${KETTLE_HOME}/logs/updateRepoDev1_${datestamp}.out 2>&1

${KETTLE_HOME}/import.sh -rep="[ENV] Repo" -user=admin -pass=admin -dir=/ -replace=Y -
norules=Y -file=${KETTLE_HOME}/erx_repo/inbound_vista_delivery.xml | tee -a
${KETTLE_HOME}/logs/updateRepoDev1_${datestamp}.out 2>&1

${KETTLE_HOME}/import.sh -rep="[ENV] Repo" -user=admin -pass=admin -dir=/ -replace=Y -
norules=Y -file=${KETTLE_HOME}/erx_repo/outbound_main.xml | tee -a
${KETTLE_HOME}/logs/updateRepoDev1_${datestamp}.out 2>&1
<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. Log into Linux and 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. Log into Linux and 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=vaauserxappdev2.aac.va.gov
nexus-context-path=/nexus/
```

11. Modify ~nexusol/.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:
```
INSTALL4J_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
#
ProxyPass /nexus/ http://vaauserxappdev2.aac.va.gov:8061/nexus/
ProxyPassReverse /nexus/ http://vaauserxappdev2.aac.va.gov:8061/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

Not applicable to patch PSO*7.0*589.

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 known operational state of the software and appropriate platform settings.

The Inbound eRx system will provide data protection measures, such as back-up intervals and redundancies that are consistent with systems categorized as mission critical (12 hour restoration, 2 hour recover point objectives). 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.

5.6 Back-Out Procedure

This section outlines the backout procedure for the following:

- Pentaho 8.2 upgrade patch PSO*7.0*589
- WebLogic

5.6.1 Back-Out of VistA Patch

Not applicable for patch PSO*7.0*589.

5.6.2 Back-Out of Database

This section outlines the steps for backing out Database changes on the 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 procedures are 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, select the **Deployments** node.
3. Within the **Change Center** panel in the left column of the WebLogic console, select **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, select **Stop**, and then select **Force Stop Now** from the drop-down list.
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. Select **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 select **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. Select **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 has been deleted and is 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, select 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. Select **Install** 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 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. Select the **upload your file(s)** link in the **Install Application Assistant** panel in the right section of the console.
        ii. Select the **Deployment Archive Browse** to see the **Choose file** dialogue used to select the Deployment Archive.
        iii. Select **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, select **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 select **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. Select **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-3.1.0.005**
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. Select **Next**.
16. Within the **Install Application Assistant,** in the right column of the console WebLogic, the panel **Review your choices and click Finish** will now be displayed, which summarizes the steps completed above.
17. Verify that the values match those entered in Steps 6 through 17 and select **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 select **Save**.
20. Within the **Change Center** panel in the left column of the WebLogic console, select **Activate Changes**.
21. Within the **Domain Structure** panel in the left column of the WebLogic console, select 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-3.1.0.005 deployment, select **Start**, and then select **Servicing all requests** from the drop-down list.
24. WebLogic will now display the panel **Start Application Assistant** in the right column of the console for confirmation to start servicing requests.
25. Select **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-3.1.0.005 deployment is **Active**.

5.7 Back-out Verification Procedure

For verifying the 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 PSO*7.0*551.

Depending on the approach taken for the back-out, the verification steps will vary. 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

Rollback 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 Rollback.

6.4 Authority for Rollback

The POCs with the authority to order the Rollback are the Inbound eRx IPT, the VA PM, and other relevant stakeholders.

6.5 Rollback Procedure

6.5.1 Rollback of Database

This section outlines the steps for rollback of Database changes on the 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 procedures are 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, select the **Deployments** node.
3. Within the **Change Center** panel in the left column of the WebLogic console, select **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, select **Stop**, and then select **Force Stop Now** from the drop-down list.
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. Select **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 select **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. Select **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, select the **Deployments** node.

3. Verify that the application is in **Lock & Edit** mode. **Lock & Edit** mode is indicated by the "greyed-out" **Lock & Edit** selection button.
4. Select 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, which is within the **Install Application Assistant** panel 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. Select on the **upload your file(s)** link in the **Install Application Assistant** panel in the right section of the console.
        ii. Select the **Deployment Archive Browse** to see the **Choose file** dialogue used to select the Deployment Archive.
        iii. Select **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, select **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 select **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. Select **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-3.1.0.005**
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. Select **Next**.

16. Within the **Install Application Assistant,** in the right column of the console WebLogic, the panel **Review your choices and click Finish** will now be displayed, which summarizes the steps completed above.
17. Verify that the values match those entered in Steps 6 through 17 and select **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 select **Save**.
20. Within the **Change Center** panel in the left column of the WebLogic console, select **Activate Changes**.
21. Within the **Domain Structure** panel in the left column of the WebLogic console, select 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-3.1.0.005** deployment, select **Start**, and then select **Servicing all requests** from the drop-down list.
24. WebLogic will now display the panel **Start Application Assistant** in the right column of the console for confirmation to start servicing requests.
25. Select **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-3.1.0.005** 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 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 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. Log into Linux and 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:
   ```
   $ ./startWebLogic_[domain].sh
   ```
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. Log into Linux and 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. On VM 2, start ***[ENV]*** Dynamic Slave5:
   ```
   $ ./startCarte[Env]Slave5.sh
   ```
9. From the CPanel (https://***[proxy_fqdn]***/cpanel), wait for the ***[ENV]*** Slave1 to start up by watching: https://***[proxy_fqdn]***/slave1/kettle/status/
10. From the CPanel (https://***[proxy_fqdn]***/cpanel), wait for the ***[ENV]*** Slave2 to start up by watching: https://***[proxy_fqdn]***/slave2/kettle/status/
11. From the CPanel (https://***[proxy_fqdn]***/cpanel), wait for the ***[ENV]*** Slave3 to start up by watching: https://***[proxy_fqdn]***/slave3/kettle/status/
12. From the CPanel (https://***[proxy_fqdn]***/cpanel), wait for the ***[ENV]*** Slave4 to start up by watching: https://***[proxy_fqdn]***/slave4/kettle/status/
13. From the CPanel (https://***[proxy_fqdn]***/cpanel), wait for the ***[ENV]*** Slave5 to start up by watching: https://***[proxy_fqdn]***/slave5/kettle/status/
14. From the CPanel (https://***[proxy_fqdn]***/cpanel), check that all 5 dynamic slaves have registered with the master: https://***[proxy_fqdn]***/slave1/kettle/getSlaves/
15. 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

    https://***[proxy_fqdn]***/slave5/kettle/runJob/?job=inbound_vista_delivery/InboundDeliverToVistaMbM_JOB
16. From the CPanel (https://***[proxy_fqdn]***/cpanel), check the InboundMessageProcessing_JOB status: https://***[proxy_fqdn]***/slave1/kettle/status, select the **InboundMessageProcessing_JOB** hyperlink and check the job status page.
17. From the CPanel (https://***[proxy_fqdn]***/cpanel), check the InboundMessageProcessingRetry_JOB status: https://***[proxy_fqdn]***/slave2/kettle/status, select the **InboundMessageProcessingRetry_JOB** hyperlink and check the job status page.
18. From the CPanel (https://***[proxy_fqdn]***/cpanel), check the InboundDeliverToVista _JOB status: https://***[proxy_fqdn]***/slave3/kettle/status, select the **InboundDeliverToVista _JOB** hyperlink and check the job status page.
19. From the CPanel (https://***[proxy_fqdn]***/cpanel), check the OutboundMessageProcessing _JOB status: https://***[proxy_fqdn]***/slave4/kettle/status, select the **OutboundMessageProcessing** hyperlink and check the job status page.

20. From the CPanel (https://***[proxy_fqdn]***/cpanel), check the InboundDeliverToVistaMbM_JOB status: https://***[proxy_fqdn]***/slave5/kettle/status, select the **InboundDeliverToVistaMbM_JOB** hyperlink and check the job status page.

7.2 Shut Down Procedures

7.2.1 Pentaho Services Shutdown

1. Log into Linux and sudo su to the kettle account:

```
$ sudo su - kettle
```

2. As kettle on VM2:

```
$ /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
$ /u01/app/pentaho/pdi-[env]slave5/carte.sh [vm2_fqdn] 8085 -s -u cluster -p cluster
```

3. As kettle on VM1:

```
$ /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. Log into Linux and sudo su to the weblogic account:

```
$ 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:

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

4. On VM1, as weblogic:

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

5. On VM2, as weblogic:

```
$ ./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
MRMwEQYKCZImiZPyLGQBGRYDZ292MRIwEAYKCZImiZPyLGQBGRYCdmExHDAaBgNV
BAMTE1ZBIEludGVybmFsIFJvb3QgQ0EwHhcNMDUxMjIyMTY0NDM1WhcNMjUxMjIy
MTY1MzE5WjBHMRMwEQYKCZImiZPyLGQBGRYDZ292MRIwEAYKCZImiZPyLGQBGRYC
dmExHDAaBgNVBAMTE1ZBIEludGVybmFsIFJvb3QgQ0EwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQDVafeLiz6lsJVkI1+suHKtVyCZAyyjSHhuDcIxonjg
EVk3mRUYZW3QPVuvS2m3NjKujJw9eL4FwGNnou+CUEdTvpAMoIo9Xhcm3uzR1Gq+
Gn6f9ichJYrttNkQo+JXPqgzEsNqUEFBRuQymmK7kZODAPnzN9VMlGjDGejDGCD5
fxyJyhkurwNWmVjUl8D3E6mMWM/1OyinGmTC6i4FQiJpVW5IauZDS0ceJhr2BSEW
BuH8W6mAQ9ZdXkiUBZm4/AUVw6QayK9kHTpFHoYhli1pJ12iDLn1a+NJdzNJiz7U
URdrW0LBSBApDXijKsAMmcyXMvk4ULONR9BewoCQRVrBAgMBAAGjZjBkMBMGCSsG
AQQBgjcUAgQGHgQAQwBBMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0G
A1UdDgQWBBTjZG2vNo8cUIHkMxOg9OHayccdzzAQBgkrBgEEAYI3FQEEAwIBADAN
BgkqhkiG9w0BAQUFAAOCAQEAox6+zBW1kK1py0UarVb6G+cphwcPi/Gt4OzS58Aq
BiZ9j36GWzdD/LtbbG3J7Lj/gE9sFqTV8cxe9sES22TxHhcA5eSF3tOg6xWMzi9S
npRvQGSHvyYLhQ5KbJPTW3w1t2WGmxlDRCXI0cvXONuPEWN2Y15vBbv7T2kA63M0
oieYDKb6BMCzj3VBHF5WuoXXXXcJBUEPWjtJffZ88kqFkHt1DKqjdBqZIp9r56pd
4PujhowXBOdViWFJcK2wIMlNvHSkjzB1uXzTkssdMUg8CiZPpkDHMui0PhPo3ZOH
hiEE/Cj5hryyeF+iwSwQX6YkH2stk53By1ctdC/N8Egudg==
-----END CERTIFICATE-----
```

8.1.2 va_internal_subordinate_ca_cert.txt

```
-----BEGIN CERTIFICATE-----
MIIF2zCCBMOgAwIBAgIHPQAAAAAW2TANBgkqhkiG9w0BAQUFADBHMRMwEQYKCZIm
iZPyLGQBGRYDZ292MRIwEAYKCZImiZPyLGQBGRYCdmExHDAaBgNVBAMTE1ZBIElu
dGVybmFsIFJvb3QgQ0EwHhcNMTMwODE1MDA0NzA4WhcNMjMwODEzMDA0NzA4WjBQ
MRMwEQYKCZImiZPyLGQBGRYDZ292MRIwEAYKCZImiZPyLGQBGRYCdmExJTAjBgNV
BAMTHFZBIEludGVybmFsIFN1Ym9yZGluYXRlIENBIDEwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQC8gdm7W2s9uaWucxI+miZR0P/6U2psmLn+kht6Rmdd
maar842z5/iSPHhnhPCr6Gc69YZovnJK/hjM1uxsvluu6OCFgYRGKYfAO2XaXCju
lyXmjoq09TGXJIpkCHpjNBWL8BtcgGmbbZt7WWILbvbONcscaewQ0hXOWsy7P+E2
maxhtxbg/tVmSlE6anLXCMThFuRRy2B9ps/osh8WgW91PP9Jd0YwpFCSIsU2PN1i
9gvPr8GQD+5yQPsg4ya/QFDBWyccM2eDFLXL8Tx0nJKoTSWwcT7ETjpJYFT7aqva
w36Ws62KSUy/QXTWGcEIipRePlum88/7yI27av6hdpzpAgMBAAGjggLBMIICvTAP
BgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTeJbRYCv2TJ9qNPR86dkt3UtlbEzAL
BgNVHQ8EBAMCAYYwEAYJKwYBBAGCNxUBBAMCAQIwIwYJKwYBBAGCNxUCBBYEFEWp
QVzWUmQmIUEwpoAI9JTK0qHLMDwGCSsGAQQBgjcVBwQvMC0GJSsGAQQBgjcVCIHI
wzOB+fAGgaWfDYTggQiFwqpLBpr2G4H2/kACAWQCAQIwHwYDVR0jBBgwFoAU42Rt
rzaPHFCB5DMToPTh2snHHc8wgdgGA1UdHwSB0DCBzTCByqCBx6CBxIYwaHR0cDov
L2NybC5wa2kudmEuZ292L3BraS9jcmwvVkFJbnRlcm5hbFJvb3QuY3JshoGPbGRh
cDovL2xkYXAucGtpLnZhLmdvdi9DTj1WQUludGVybmFsUm9vdCxDTj1DRFAsQ049
UEtJLENOPVNlcnZpY2VzLERDPVZBLERDPUdPVj9jZXJ0aWZpY2F0ZVJldm9jYXRp
b25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnQwggEL
BggrBgEFBQcBAQSB/jCB+zCBkgYIKwYBBQUHMAKGgYVsZGFwOi8vbGRhcC5wa2ku
dmEuZ292L0NOPVZBSW50ZXJuYWxSb290LENOPUFJQSxDTj1QS0ksQ049U2Vydmlj
ZXMsREM9VkEsREM9R09WP2NBQ2VydGlmaWNhdGU/YmFzZT9vYmplY3RDbGFzcz1j
ZXJ0aWZpY2F0aW9uQXV0aG9yaXR5MCMGCCsGAQUFBzABhhdodHRwOi8vb2NzcC5w
a2kudmEuZ292LzA/BggrBgEFBQcwAoYzaHR0cDovL2FpYS5wa2kudmEuZ292L1BL
SS9BSUEvVkEvVkFJbnRlcm5hbFJvb3QuY2VyMA0GCSqGSIb3DQEBBQUAA4IBAQAJ
5Tw4vho1QAuiebJ3zFow3esXmqyjRWeHhbszbNzsYop1szqelsFP0h69IYuVKVC5
eHzlCxZ6zF0dFgFOkDf65BKoIyQ4W9942rRzr8eKDiyFdb2dGqP1uS7VtcyX6kI4
BmhW5P8G6wRrD6Az7G3WUMpHZYtoaE8udOk86lZk9P7h7PlnElzH7inr307F/KjL
kc9m/RRdktv9nG2c3cEMa74lfCxiQpI2/gWTXKJJKy5younKbEUtu4o3qXHji21V
/D02OIOvcs7RYsiZuTKoKjO3/uQli85QKifnzpWyLfto0ucFIi9W9q2yuWPU6wIT
eaQRaJrinDddHRgSBqN4
-----END CERTIFICATE-----
```

8.1.3 va_root_ca_s2_cert.pem

```
-----BEGIN CERTIFICATE-----
MIIDhzCCAm+gAwIBAgIQKNXLQBAcYqRGJ+LYwX8c6TANBgkqhkiG9w0BAQsFADBK
MRMwEQYKCZImiZPyLGQBGRYDZ292MRIwEAYKCZImiZPyLGQBGRYCdmExHzAdBgNV
BAMTFlZBLUludGVybmFsLVMyLVJDQTEtdjEwHhcNMTYxMDI2MTYxMzIwWhcNMzYx
MDI2MTYyMjU5WjBKMRMwEQYKCZImiZPyLGQBGRYDZ292MRIwEAYKCZImiZPyLGQB
GRYCdmExHzAdBgNVBAMTFlZBLUludGVybmFsLVMyLVJDQTEtdjEwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQC7qJL6b5hzXU7o+lHgX32ods7AgOGinzA4
f9JfuzlrFp+ZvVrRgXwZLkKGfjyNQIIY6uI9fG8dwNLrBa0vWYoKwMJ4pbEjl+gy
1UDOrh3e3fPd68L3m+sUx0K/z+ZSiNkhK1MOP0wFQtYmtCDc7b5zy5NApGBCJAJB
QcdrVH8MCxC0IZEpxsTjuSDpcea09eD4nYAeBUVzg+N9K9esWF+SLZxsCnFgMuL/
ikS093wsaoFyBe0H0wH7GDNmV/Zxlxy3krzGqszfGRmxb4pXkbqvrOGzju2RZoRx
lYKYnB4brDR4BGW984fiiJq1ofbwCK4ql7nhSi71TEnxRfltCaPrAgMBAAGjaTBn
MBMGCSsGAQQBgjcUAgQGHgQAQwBBMAsGA1UdDwQEAwIBhjASBgNVHRMBAf8ECDAG
AQH/AgEBMB0GA1UdDgQWBBQBLYthZhuM0ODTTD5O7FsZsBHGYTAQBgkrBgEEAYI3
FQEEAwIBADANBgkqhkiG9w0BAQsFAAOCAQEAaE16FdPpLptzZA1sdGREaSfDP46j
e2m7Nelz2CDdT/goRS5q1+uxQpaUvH08Lxw9Nr6Chr018K1uHYMgLuFybflm5P0R
B/XKKJATszamkMUYRSGeSf1uXKNz4dqXu2yv9BvxyY2qdGJUpEyOmcuZwq/Zh1qv
1Aoq67ZeBt0R0ZnJmLiMQ7ywd2kQ8MtWlx2tcN0nZmtPOb3WkrvG2sgFZN064gP2
YVlKp9RaENjNwYNVyyTbq8CofUIYV2OfSbsI1GR3CQSqPO5CUJ/ScdWuWJVfhWLt
l1H5l12CCqk+7vaTBtK+QjBliAayTFyonUocbD5VBxB4DvlCMk7uATrhNw==
-----END CERTIFICATE-----
```

8.1.4 va_internal_ca1_s2_cert.pem

```
-----BEGIN CERTIFICATE-----
MIIEoDCCA4igAwIBAgITFAAAAARskyEu6lBaeQAAAAAABDANBgkqhkiG9w0BAQsF
ADBKMRMwEQYKCZImiZPyLGQBGRYDZ292MRIwEAYKCZImiZPyLGQBGRYCdmExHzAd
BgNVBAMTFlZBLUludGVybmFsLVMyLVJDQTEtdjEwHhcNMTYxMDI3MTY0MTA3WhcN
MjYxMDI1MTY0MTA3WjBKMRMwEQYKCZImiZPyLGQBGRYDZ292MRIwEAYKCZImiZPy
LGQBGRYCdmExHzAdBgNVBAMTFlZBLUludGVybmFsLVMyLUlDQTEtdjEwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC4bY+wR9CKBb6rxoRajhPAFJIPdwHe
bp3Kzy5CxlPmQMk6ANqX3WWqM/qSebBHCNYvdqSgXMSdVXu0loCIhqBLvccwmxdc
4rJD6Vydh3WEv74LayMIIrzl06QLcj+6GnVmWm5/+FbEF9SynICY2RhmO8roLp1o
UnaNiC3Pruy97ZLHN/OE8Z7FMWIHHB/GQHwX/1P05p0yv/8WsojctrW8S3d56VlH
u4W4ilKZMoTxDR2JFpn6q22J4DjVG8ouOSyJQmXMFR+HcmVPAaJbAF1L0w0BOrlF
3W9w4RFo/PWdEm+SopGiTFeMMaPXG377FlEhWuX/I0yXtQT9zXt4rTTVAgMBAAGj
ggF9MIIBeTAQBgkrBgEEAYI3FQEEAwIBADAdBgNVHQ4EFgQUG23f6z3l4g3vFrHQ
3l9YGlbL5OwwPAYJKwYBBAGCNxUHBC8wLQYlKwYBBAGCNxUIgcjDM4H58AaBpZ8N
hOCBCIXCqksGg+96htu7FwIBZAIBEjALBgNVHQ8EBAMCAYYwEgYDVR0TAQH/BAgw
BgEB/wIBADAfBgNVHSMEGDAWgBQBLYthZhuM0ODTTD5O7FsZsBHGYTBJBgNVHR8E
QjBAMD6gPKA6hjhodHRwOi8vY3JsLnBraS52YS5nb3YvcGtpL2NybC9WQS1JbnRl
cm5hbC1TMi1SQ0ExLXYxLmNybDB7BggrBgEFBQcBAQRvMG0wRwYIKwYBBQUHMAKG
O2h0dHA6Ly9haWEucGtpLnZhLmdvdi9wa2kvYWlhL1ZBL1ZBLUludGVybmFsLVMy
LVJDQTEtdjEuY2VyMCIGCCsGAQUFBzABhhZodHRwOi8vb2NzcC5wa2kudmEuZ292
MA0GCSqGSIb3DQEBCwUAA4IBAQCA/ZQYzX1u6rB0xITkVY5K8zPAjosvD6ynkr0B
uCH+qOj3edjVQENg1JRVK89HqBQNMspbTUsZz2TEVKNH5xWtY0jp6vJm1DYDUqSu
bEMe3CeJpkeD9S8JZV/P4P9swPkK2ziptOlskqqnmcK7ZrJbevb4GPvQ+wCUf2r8
t3ybYK5B1fyuX4L+h/GVdQWInS3Nt8hvyDyMeW7y7rC+6I0IJRLlaO9OtbbNZfIn
VR6NHQUatOvdb9HVwJKvPvpeF0PYtScUXus+mZrV6RXKtYrFEbUX9jcrVlq2ML2H
A92Pm2HzYILqvw/D2WQOCqZSKfpYr7jgekcGMBriisBlBq4D
-----END CERTIFICATE-----
```

8.1.5 va_internal_ca2_s2_cert.pem

```
-----BEGIN CERTIFICATE-----
MIIEoDCCA4igAwIBAgITFAAAAAOX9+lYJSJG4QAAAAAAAzANBgkqhkiG9w0BAQsF
ADBKMRMwEQYKCZImiZPyLGQBGRYDZ292MRIwEAYKCZImiZPyLGQBGRYCdmExHzAd
BgNVBAMTFlZBLUludGVybmFsLVMyLVJDQTEtdjEwHhcNMTYxMDI2MTgzNDM4WhcN
MjYxMDI0MTgzNDM4WjBKMRMwEQYKCZImiZPyLGQBGRYDZ292MRIwEAYKCZImiZPy
LGQBGRYCdmExHzAdBgNVBAMTFlZBLUludGVybmFsLVMyLUlDQTItdjEwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC9UaJu7b6BP9ffk9eZyAjCoLZHAQXD
QWiVrR1D1rkowF7cwSeoyPQ5yoMrH9TLQEb/GRVaL5UeHHw9bqbnXvMOgGuV1O64
vu42RDUEKofout/34LpBN9DC2JCsocNMVtwyoFuGJBYAeygZDNaLuI53tpzw74pa
WKoiD5pXtOoJkuARs2vMHD3kuzNeBdXFWo/l45gnZFpxmJo/Dr3wGzDDiO7h53S/
VVAaOXdPISVm1sieKtoLEinyy9qbkxdC7k1MdMJuYnRF92aZY+gezvpVqW7F1T8z
pT35wqbxbE1oqRAMlMEb7D5M19Kp/bWOfZ/zhWH6Y6lA91q4FsTsXxe1AgMBAAGj
ggF9MIIBeTAQBgkrBgEEAYI3FQEEAwIBADAdBgNVHQ4EFgQU71TwDfev76TpwXsl
gO+9o6wnA7cwPAYJKwYBBAGCNxUHBC8wLQYlKwYBBAGCNxUIgcjDM4H58AaBpZ8N
hOCBCIXCqksGg+96htu7FwIBZAIBEjALBgNVHQ8EBAMCAYYwEgYDVR0TAQH/BAgw
BgEB/wIBADAfBgNVHSMEGDAWgBQBLYthZhuM0ODTTD5O7FsZsBHGYTBJBgNVHR8E
QjBAMD6gPKA6hjhodHRwOi8vY3JsLnBraS52YS5nb3YvcGtpL2NybC9WQS1JbnRl
cm5hbC1TMi1SQ0ExLXYxLmNybDB7BggrBgEFBQcBAQRvMG0wRwYIKwYBBQUHMAKG
O2h0dHA6Ly9haWEucGtpLnZhLmdvdi9wa2kvYWlhL1ZBL1ZBLUludGVybmFsLVMy
LVJDQTEtdjEuY2VyMCIGCCsGAQUFBzABhhZodHRwOi8vb2NzcC5wa2kudmEuZ292
MA0GCSqGSIb3DQEBCwUAA4IBAQCX2482Kh858YMc2aYMek32bSZoMRRCKgNEwBBH
DwXpNu0zDjaxrvIPi+foEk/MvTn7PMSqcPYnuRw3IPCJ1uD00S/kUMMXJm3ON3l4
L4nmZz4BrhyZsYOyYHQJoE4KT2/Diw28XFJYH6FtDZnA105s3xnilg7NatBvBX0K
WayJ1ETJkp2aPlon9u+Tq/YE++Y0ek3MCozimRW/iWxzq2cd2UfNRyt2fJugAiJ2
S3AJbCWb5KTZi1ip9tRiHyXDxxcJ+N9FSQgZ1e/B62m9Xouh6VCTi3alCRY1MXSG
2+yUvBNmGIB0+tacbQAyXYEPAVHrE5B+VLs/7jrHDR5ap2ln
-----END CERTIFICATE-----
```

8.1.6 betrusted_production_ssp_ca_a1_cert.txt

```
-----BEGIN CERTIFICATE-----
MIIG6DCCBdCgAwIBAgICAZowDQYJKoZIhvcNAQELBQAwWTELMAkGA1UEBhMCVVMxGDAWBgNVBAoT
D1UuUy4gR292ZXJubWVudDENMAsGA1UECxMERlBLSTEhMB8GA1UEAxMYRmVkZXJhbCBDb21tb24g
UG9saWN5IENBMB4XDTEwMTIwOTE5NTUyNFoXDTIwMTIwOTE5NDkwNFowgYgxCzAJBgNVBAYTAlVT
MRkwFwYDVQQKExBCZXRydXN0ZWQgVVMgSW5jMQwwCgYDVQQLEwNTU1AxJzAlBgNVBAsTHkJldHJ1
c3RlZCBQcm9kdWN0aW9uIFNTUCBDQSBBMTEnMCUGA1UEAxMeQmV0cnVzdGVkIFByb2R1Y3Rpb24g
U1NQIENBIEExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAn2gPTEBKtvo7JnaOXE7F
YHlPYO5qXCVjbqe9LediLo3efZgsmFEK4otlL6lUC9PJAuIteeriLkOv9+momu08xX1FyJdYAWm/
moYRLVUMiCuDgJVLpw7FgmQh7FBBAW7IHeBvCYzUU4Ozh9VdYuxKkcA5sz9HgFL7RUyblMAPel79
JBpOdLvYEgBA+O25/VVLyeqD2wCQhkWkEIsWFDG1i6FjdVK/i1ot4kUj8nHS/o9uiIebYK+8lPg0
lK0jHhIzoxeTGDx9wiVmkZ/A3FRtramMEPQQaL2d//kY4tImmXW541hAn9SWy9Ur523tOxDpsNE1
VaN+7RU4Yt4Cxf6XrwIDAQABo4IDiDCCA4QwDwYDVR0TAQH/BAUwAwEB/zBPBgNVHSAESDBGMAwG
CmCGSAFlAwIBAwYwDAYKYIZIAWUDAgEDBzAMBgpghkgBZQMCAQMIMAwGCmCGSAFlAwIBAw0wDAYK
YIZIAWUDAgEDETCB6QYIKwYBBQUHAQEEgdwwgdkwPwYIKwYBBQUHMAKGM2h0dHA6Ly9odHRwLmZw
a2kuZ292L2ZjcGNhL2NhQ2VydHNJc3N1ZWRUb2ZjcGNhLnA3YzCBlQYIKwYBBQUHMAKGgYhsZGFw
Oi8vbGRhcC5mcGtpLmdvdi9jbj1GZWRlcmFsJTIwQ29tbW9uJTIwUG9saWN5JTIwQ0Esb3U9RlBL
SSxvPVUuUy4lMjBHb3Zlcm5tZW50LGM9VVM/Y0FDZXJ0aWZpY2F0ZTtiaW5hcnksY3Jvc3NDZXJ0
aWZpY2F0ZVBhaXI7YmluYXJ5MIIBJwYIKwYBBQUHAQsEggEZMIIBFTA+BggrBgEFBQcwBYYyaHR0
cDovL3NpYTEuc3NwLXN0cm9uZy1pZC5uZXQvQ0EvU1NQLUNBLUExLVNJQS5wN2MwgdIGCCsGAQUF
BzAFhoHFbGRhcDovL2RpcjEuc3NwLXN0cm9uZy1pZC5uZXQvY249QmV0cnVzdGVkJTIwUHJvZHVj
dGlvbiUyMFNTUCUyMENBJTIwQTEsb3U9QmV0cnVzdGVkJTIwUHJvZHVjdGlvbiUyMFNTUCUyMENB
JTIwQTEsb3U9U1NQLG89QmV0cnVzdGVkJTIwVVMlMjBJbmMsYz1VUz9jQUNlcnRpZmljYXRlO2Jp
bmFyeSxjcm9zc0NlcnRpZmljYXRlUGFpcjtiaW5hcnkwDgYDVR0PAQH/BAQDAgHGMB8GA1UdIwQY
MBaAFK0MenVc5fOYxHmYDqwo/Zf05wL8MIG4BgNVHR8EgbAwga0wKqAooCaGJGh0dHA6Ly9odHRw
LmZwa2kuZ292L2ZjcGNhL2ZjcGNhLmNybDB/oH2ge4Z5bGRhcDovL2xkYXAuZnBraS5nb3YvY24l
M2RGZWRlcmFsJTIwQ29tbW9uJTIwUG9saWN5JTIwQ0Esb3U1M2RGUEtJLG8lM2RVLlMuJTIwR292
ZXJubWVudCxjJTNkVVM/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdDAdBgNVHQ4EFgQUu6TpuYML
MnIaIQ6qz0UdtxYjyA0wDQYJKoZIhvcNAQELBQADggEBAK+kk+1bsJuVspfA+lt3cJ9l8AIi8Ra4
rECJ2NqVdR9K4QdfNOmg0zAW2ybpvJ3ZD8y7vVzkzdkXwJsGMZMLKYK93d4I/TjsMyZMQFSWo9fV
Txn9El9ivIdzO+R27tYK8LIKhKSO0Q1I6kytzeXiWTwpXHH0YSUFpLNOr30gZUsuoWhpg/sb7VfQ
s+T2fNzXRRw3mqwbqQcx3WfdfLmfwCZC4gcirw1N0Sfo2GqgIc1/OzEL93tJh20SXPwJLkF2WN4k
HUmR1MQE0X8yQ+WYt6gl51qWKNXoQMm+TT2W3Y8tEOQGXd+nlCHiwKQyrPCLlL+EmFqyIN+lltvm
AxH6k1M=
-----END CERTIFICATE-----
```

8.1.7 federal_common_policy_ca_cert.txt

```
-----BEGIN CERTIFICATE-----
MIIEYDCCA0igAwIBAgICATAwDQYJKoZIhvcNAQELBQAwWTELMAkGA1UEBhMCVVMxGDAWBgNVBAoT
D1UuUy4gR292ZXJubWVudDENMAsGA1UECxMERlBLSTEhMB8GA1UEAxMYRmVkZXJhbCBDb21tb24g
UG9saWN5IENBMB4XDTEwMTIwMTE2NDUyN1oXDTMwMTIwMTE2NDUyN1owWTELMAkGA1UEBhMCVVMx
GDAWBgNVBAoTD1UuUy4gR292ZXJubWVudDENMAsGA1UECxMERlBLSTEhMB8GA1UEAxMYRmVkZXJh
bCBDb21tb24gUG9saWN5IENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2HX7NRY0
WkG/Wq9cMAQUHK14RLXqJup1YcfNNnn4fNi9KVFmWSHjeavUeL6wLbCh1bI1FiPQzB6+Duir3MPJ
1hLXp3JoGDG4FyKyPn66CG3G/dFYLGmgA/Aqo/Y/ISU937cyxY4nsyOl4FKzXZbpsLjFxZ+7xaBu
gkC7xScFNknWJidpDDSPzyd6KgqjQV+NHQOGgxXgVcHFmCye7Bpy3EjBPvmE0oSCwRvDdDa3ucc2
Mnr4MrbQNq4iGDGMUHMhnv6DOzCIJOPpwX7e7ZjHH5IQip9bYi+dpLzVhW86/clTpyBLqtsgqyFO
HQ1O5piF5asRR12dP8QjwOMUBm7+nQIDAQABo4IBMDCCASwwDwYDVR0TAQH/BAUwAwEB/zCB6QYI
KwYBBQUHAQsEgdwwgdkwPwYIKwYBBQUHMAWGM2h0dHA6Ly9odHRwLmZwa2kuZ292L2ZjcGNhL2Nh
Q2VydHNJc3N1ZWRCeWZjcGNhLnA3YzCBlQYIKwYBBQUHMAWGgYhsZGFwOi8vbGRhcC5mcGtpLmdv
di9jbj1GZWRlcmFsJTIwQ29tbW9uJTIwUG9saWN5JTIwQ0Esb3U9RlBLSSxvPVUuUy4lMjBHb3Zl
cm5tZW50LGM9VVM/Y0FDZXJ0aWZpY2F0ZTtiaW5hcnksY3Jvc3NDZXJ0aWZpY2F0ZVBhaXI7Ymlu
YXJ5MA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUrQx6dVzl85jEeZgOrCj9l/TnAvwwDQYJKoZI
hvcNAQELBQADggEBAI9z2uF/gLGH9uwsz9GEYx728Yi3mvIRte9UrYpuGDco71wb5O9Qt2wmGCMi
TR0mRyDpCZzicGJxqxHPkYnos/UqoEfAFMtOQsHdDA4b8Idb7OV316rgVNdF9IU+7LQd3nyKf1tN
nJaK0KIyn9psMQz4pO9+c+iR3Ah6cFqgr2KBWfgAdKLI3VTKQVZHvenAT+0g3eOlCd+uKML80cgX
2BLHb94u6b2akfI8WpQukSKAiaGMWMyDeiYZdQKlDn0KJnNR6obLB6jI/WNaNZvSr79PMUjBhHDb
NXuaGQ/lj/RqDG8z2esccKIN47lQA2EC/0rskqTcLe4qNJMHtyznGI8=
-----END CERTIFICATE-----
```

8.1.8 veterans_affairs_device_ca_b2_cert.txt


```
-----BEGIN CERTIFICATE-----
MIIHVTCCBj2gAwIBAgICHGAwDQYJKoZIhvcNAQEFBQAwgYgxCzAJBgNVBAYTAlVTMRkwFwYDVQQK
ExBCZXRydXN0ZWQgVVMgSW5jMQwwCgYDVQQLEwNTU1AxJzAlBgNVBAsTHkJldHJ1c3RlZCBQcm9k
dWN0aW9uIFNTUCBDQSBBMTEnMCUGA1UEAxMeQmV0cnVzdGVkIFByb2R1Y3Rpb24gU1NQIENBIEEx
MB4XDTA4MDgwNzE1MjQwMFoXDTE4MDgwNzE1MjI0NlowcjETMBEGCgmSJomT8ixkARkWA2dvdjES
MBAGCgmSJomT8ixkARkWAnZhMREwDwYDVQQLEwhTZXJ2aWNlczEMMAoGA1UECxMDUEtJMSYwJAYD
VQQDEx1WZXRlcmFucyBBZmZhaXJzIERldmljZSBDQSBCMjCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBALTxrfB9i65LBlPlCvdruZNIsSG3WY0JxNQfIxTBZqsOneWFnR2wElFzhkxvjQRx
vQAfqz1gBum5cMl+7BmoFF9ueRP5uQGF++f+2leQ7HE+5cqw9DlQ4wBtlE/zRrcOPqhQ9Usybq44
XCLneNvQ56nGyw/KxgyqgycUqojDIqWOIdQ/e12jSxa5qCmrzdLsEFpx9kVuWz8Wvn4K5VWOV/Pb
EMhvOmdxpXwEBwUALqhGbTBeq52N0UG1wgoJJRii0uR5T+bK8QJ+NF7vzmnReWudTFhV3av9WZhu
7banQGcS66HBc1h22FlYDefq2yEHpgmPOBvv8EC+3I1DnNh519cCAwEAAaOCA9wwggPYMA8GA1Ud
EwEB/wQFMAMBAf8wTwYDVR0gBEgwRjAMBgpghkgBZQMCAQMGMAwGCmCGSAFlAwIBAwcwDAYKYIZI
AWUDAgEDCDAMBgpghkgBZQMCAQMNMAwGCmCGSAFlAwIBAxEwggE+BggrBgEFBQcBAQSCATAwggEs
MDoGCCsGAQUFBzAChi5odHRwOi8vYWlhMS5zc3Atc3Ryb25nLWlkLm5ldC9DQS9TU1AtQ0EtQTEu
cDdjMIG2BggrBgEFBQcwAoaBqWxkYXA6Ly9kaXIxLnNzcC1zdHJvbmctaWQubmV0L2NuPUJldHJ1
c3RlZCUyMFByb2R1Y3Rpb24lMjBTU1AlMjBDQSUyMEExLG91PUJldHJ1c3RlZCUyMFByb2R1Y3Rp
b24lMjBTU1AlMjBDQSUyMEExLG91PVNTUCxvPUJldHJ1c3RlZCUyMFVTJTIwSW5jLGM9VVM/Y0FD
ZXJ0aWZpY2F0ZTtiaW5hcnkwNQYIKwYBBQUHMAGGKWh0dHA6Ly9vY3NwMS5zc3Atc3Ryb25nLWlk
Lm5ldC9TU1AtQ0EtQTEvMIHXBggrBgEFBQcBCwSByjCBxzA7BggrBgEFBQcwA4YvaHR0cDovL2Fp
YTEuc3NwLXN0cm9uZy1pZC5uZXQvQ0EvVkFkZXZpY2VDQS5wN2MwgYcGCCsGAQUFBzADhntsZGFw
Oi8vZGlyMS5zc3Atc3Ryb25nLWlkLm5ldC9jbj1WZXRlcmFucyUyMEFmZmFpcnMlMjBEZXZpY2Ul
MjBDQSUyMEIyLG91PVBLSSxvdT1TZXJ2aWNlcyxkYz12YSxkYz1nb3Y/Y0FDZXJ0aWZpY2F0ZTti
aW5hcnkwDgYDVR0PAQH/BAQDAgHGMB8GA1UdIwQYMBaAFLuk6bmDCzJyGiEOqs9FHbcWI8gNMIIB
BgYDVR0fBIH+MIH7MDWgM6Axhi9odHRwOi8vY2RwMS5zc3Atc3Ryb25nLWlkLm5ldC9DRFAvU1NQ
LUNBLUExLmNybDCBwaCBvqCBu4aBuGxkYXA6Ly9kaXIxLnNzcC1zdHJvbmctaWQubmV0L2NuJTNk
QmV0cnVzdGVkJTIwUHJvZHVjdGlvbiUyMFNTUCUyMENBJTIwQTEsb3UlM2RCZXRydXN0ZWQlMjBQ
cm9kdWN0aW9uJTIwU1NQJTIwQ0ElMjBBMSxvdSUzZFNTUCxvJTNkQmV0cnVzdGVkJTIwVVMlMjBJ
bmMsYyUzZFVTP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3QwHQYDVR0OBBYEFIGUNZ4qqHdgI2bs
Kp1uz7Z1GVBdMA0GCSqGSIb3DQEBBQUAA4IBAQBTnvlRJn0nM90ddSlQ6dX4nEB6LU7UEjESjgbt
blNx0IPcw+muXo4NYExTLIRJrlkOI/MSaITk0UAnSALFfLPom36SdSQ9rjxKEkqO+4/FCcScH7wE
Crw5k1AfRdsqR5cgDJlfj+sPMCYpMX0vydIiUwkpoqGKQVA0V8AI9/Z1VpmpuvWc8kogqfs+Hly6
lg3JsJ2jiLFkSO+sbwN9ZqOQTOQgFPFbScZJKV1g8jTEo0YoX/w+nSHjK5EMJwIz6yo1J8wvmjcN
1VlS3hkjxrOOqSf0/I+nz2hgybR/nkft3zk1zKeH4NPmug0F48mGSRsnkHzksGE8iSaCPkz3snJQ
-----END CERTIFICATE-----
```

8.1.9 vaww.esrdev.aac.va.gov_cert.txt


```
-----BEGIN CERTIFICATE-----
MIIHizCCBnOgAwIBAgIDBTdaMA0GCSqGSIb3DQEBCwUAMHIxEzARBgoJkiaJk/IsZAEZFgNnb3Yx
EjAQBgoJkiaJk/IsZAEZFgJ2YTERMA8GA1UECxMIU2VydmljZXMxDDAKBgNVBAsTA1BLSTEmMCQG
A1UEAxMdVmV0ZXJhbnMgQWZmYWlycyBEZXZpY2UgQ0EgQjIwHhcNMTUwOTE0MTcxNDI3WhcNMTgw
ODA3MTUyMjQ2WjBcMRMwEQYKCZImiZPyLGQBGRYDZ292MRIwEAYKCZImiZPyLGQBGRYCdmExEDAO
BgNVBAsTB2RldmljZXMxHzAdBgNVBAMTFnZhd3cuZXNyZGV2LmFhYy52YS5nb3YwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQCkYcAL0+9HukeVKIzrs0gKOhDskClbu0oOJDGjc0t72mOz
2rgj4+79J6AExovcy7nYiAsGYEmFMhwmDl3v3+aLk8E7P8xf5KFENycYhuxBI61llO0CISs7Wk2h
prkGHR0HkTyxuuUknwzhQ+9qm3CqMGDVhXqNuEwWQoJ3us22drK4NBrZn+dMTeTlKHSo9QeoICWc
bqoueoKWlOFl7UlnAaCGrABMoncEO+b9QDZB5i83IxMuZFlhwve6JHsOXKe0t3H8WbKy9M3+kOtc
xMTMOVesj7p+3mqDn/ckozRyDkMHc0SZs3jSpRr43IYIpDU4R2SOxgVq0O1f7/J+WIHrAgMBAAGj
ggQ+MIIEOjCB7AYDVR0RBIHkMIHhghZ2YXd3LmVzcmRldi5hYWMudmEuZ292ghh2YXd3LmVzcmRl
djMwLmFhYy52YS5nb3aCGHZhd3cuZXNyZGV2MzEuYWFjLnZhLmdvdoIYdmF3dy5lc3JkZXY0MC5h
YWMudmEuZ292ghV2aGFlc3J3ZWIzLmFhYy52YS5nb3aCF3Zhd3cuZXNyZGV2MS5hYWMudmEuZ292
ghd2YXd3LmVzcmRldjIuYWFjLnZhLmdvdoIXdmF3dy5lc3JkZXYzLmFhYy52YS5nb3aCF3Zhd3cu
ZXNyZGV2NC5hYWMudmEuZ292MBcGA1UdIAQQMA4wDAYKYIZIAWUDAgEDCDCCATAGCCsGAQUFBwEB
BIIBIjCCAR4wOwYIKwYBBQUHMAKGL2h0dHA6Ly9haWExLnNzcC1zdHJvbmctaWQubmV0L0NBL1ZB
ZGV2aWNlQ0EucDdjMIGABggrBgEFBQcwAoZ0bGRhcDovL2RpcjEuc3NwLXN0cm9uZy1pZC5uZXQv
Y249VmV0ZXJhbnMlMjBBZmZhaXJzJTIwRGV2aWNlJTIwQ0ElMjBCMixvdT1QS0ksb3U9U2Vydmlj
ZXMsZGM9dmEsZGM9Z292P2NBQ2VydGlmaWNhdGUwIwYIKwYBBQUHMAGGF2h0dHA6Ly9vY3NwLnBr
aS52YS5nb3YvMDcGCCsGAQUFBzABhitodHRwOi8vb2NzcDEuc3NwLXN0cm9uZy1pZC5uZXQvVkEt
U1NQLUNBLUIyMA4GA1UdDwEB/wQEAwIFoDAnBgNVHSUEIDAeBggrBgEFBQcDAQYIKwYBBQUHAwIG
CGCGSAFlAwYHMB8GA1UdIwQYMBaAFIGUNZ4qqHdgI2bsKp1uz7Z1GVBdMIIBgQYDVR0fBIIBeDCC
AXQwMKAuoCyGKmh0dHA6Ly9jcmwucGtpLnZhLmdvdi9QS0kvQ1JML3ZhZGV2aWNlLmNybDB0oHKg
cIZubGRhcDovL2xkYXAucGtpLnZhLmdvdi9jbiUzZFNTUEIyQUUsY24lM2RDRFAsY24lM2RQS0ks
Y24lM2RTZXJ2aWNlcyxkYyUzZHZhLGRjJTNkZ292P2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Qw
NKAyoDCGLmh0dHA6Ly9jZHAxLnNzcC1zdHJvbmctaWQubmV0L0NEUC92YWRldmljZS5jcmwwgZOg
gZCggY2GgYpsZGFwOi8vZGlyMS5zc3Atc3Ryb25nLWlkLm5ldC9jbiUzZFZldGVyYW5zJTIwQWZm
YWlycyUyMERldmljZSUyMENBJTIwQjIsb3UlM2RQS0ksb3UlM2RTZXJ2aWNlcyxkYyUzZHZhLGRj
JTNkZ292P2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3QwHQYDVR0OBBYEFFauWBgfqlovaoQ/3SJE
igCTXVyhMA0GCSqGSIb3DQEBCwUAA4IBAQAYuPXvhL4/ElzooFV5fAbwm822Vz7U49ZF/JSEBQqG
QBhmwbFCu7wklIu40Efkzj2nSfAeGzijfh1eaTiLC1q+wpqh5ezl3kzBJNAUTmPlJZQfVGHX0rFQ
AvOqFs5YNakKkthHnbQAWvJ1n1Bje1on6YFu3L5eeJDwdO2CBUboK/fc/m8Nxe47UTsoRG1uin6Y
8P9QglpJT6HqSHQsqanLkncU3wTh2vyJUtfMuJq0nBDvBg3PCxtoU2/wqkdFY+UEKHTjYXXkxPuX
NVHQ6sdQNq3y584edm9phxMW2rmbxEN0oN7oQWUPBEACrtrK84MxM1w6WTShl6YMV/dQz8ho
-----END CERTIFICATE-----
```

8.1.10 vaww.esrstage1a.aac.va.gov.pem

```
-----BEGIN CERTIFICATE-----
MIIFiDCCBHCgAwIBAgIHPQAAAAC3pjANBgkqhkiG9w0BAQsFADBKMRMwEQYKCZIm
iZPyLGQBGRYDZ292MRIwEAYKCZImiZPyLGQBGRYCdmExHzAdBgNVBAMTFlZBLUlu
dGVybmFsLVMyLUlDQTEtdjEwHhcNMTcwMzE0MjA1NjQ3WhcNMjAwMzEzMjA1NjQ3
WjCBwDELMAkGA1UEBhMCVVMxDjAMBgNVBAgTBVRleGFzMQ8wDQYDVQQHEwZBdXN0
aW4xKjAoBgNVBAoTIVVTIERlcGFydG1lbnQgb2YgVmV0ZXJhbnMgQWZmYWlyczEN
MAsGA1UECxMEQUlUQzEjMCEGA1UEAxMadmF3dy5lc3JzdGFnZTFhLmFhYy52YS5n
b3YxMDAuBgkqhkiG9w0BCQEWIWNkY293ZWJsb2dpY2FkbWluaXN0cmF0b3JzQHZh
LmdvdjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPvu747uobthNU4I
8GOjiQ2R3WY2F+LWYznx+6xaPSUyaawXZ8heBNngo5CbkyWhQPpuDBAjpUjiYX9Q
9AMlLhJppZEi8NmBLFkojISALEl/+3LM8NhFnA1wNCrMSjDY2HL688X277VKjgcJ
qFnF8KdldeGh9fpDnWXDWITHhO2HzYojKu415jb+GicjzB/rI+RoYftY6MDQpLcu
ltVv9SXrnDLkebe+3fKOhmrecvUhFwdYClx1V5o55iDipZlLSxAAw0RHho8wXxBm
7J7c5SN150YV5Dsido6Ui4Rroe2ewiizQsVKNe9MOsw2agIUsx+LhIY49S/s/Nzl
hcYs2qUCAwEAAaOCAfowggH2MAsGA1UdDwQEAwIFoDBYBgNVHREEUTBPghp2YXd3
LmVzcnN0YWdlMWEuYWFjLnZhLmdvdoIadmF3dy5lc3JzdGFnZTFhLmFhYy52YS5n
b3aCFXZoYWVzcndlYjYuYWFjLnZhLmdvdjAdBgNVHQ4EFgQUnkF4Y5jfPVwdOyv/
XYljZLS7r/YwHwYDVR0jBBgwFoAUG23f6z3l4g3vFrHQ3l9YGlbL5OwwSQYDVR0f
BEIwQDA+oDygOoY4aHR0cDovL2NybC5wa2kudmEuZ292L3BraS9jcmwvVkEtSW50
ZXJuYWwtUzItSUNBMS12MS5jcmwwewYIKwYBBQUHAQEEbzBtMEcGCCsGAQUFBzAC
hjtodHRwOi8vYWlhLnBraS52YS5nb3YvcGtpL2FpYS92YS9WQS1JbnRlcm5hbC1T
Mi1JQ0ExLXYxLmNlcjAiBggrBgEFBQcwAYYWaHR0cDovL29jc3AucGtpLnZhLmdv
djA9BgkrBgEEAYI3FQcEMDAuBiYrBgEEAYI3FQiByMMzgfnwBoGlnw2E4IEIhcKq
SwaDgp9ggeCLUgIBZAIBEjAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwEw
JwYJKwYBBAGCNxUKBBowGDAKBggrBgEFBQcDAjAKBggrBgEFBQcDATANBgkqhkiG
9w0BAQsFAAOCAQEAhm1jRtWAEQStJz2uPw8piDho8Iit3dz2j2/Zy0bmhbg7e1Fg
jg4xR2qv4CpNuNinxgMhsrlXV7roxY9UVK3CkmT6Js5DFuR0yQ9u4WsdM0NxxvEa
Keh3hPwBRelcSKbMefn071CObMLz9qSf9gMQ34vhlKzmVxftn5FBK8LNE/a6uoDv
FxovRmOAa/qMGMZdMZEmb144+hAngFbFmwXkOFDQOlDBG8SAYfklUNfBw92u+3jV
UApxi9bvnulp8UyHsG9QEa+fs49v1qhp4UGiY7CWLhnZbaHNLoYhpioVSruPnMa+
a4vuHW2QSxKVTY+2P3gJpXoUlSLoAJJtKi2njw==
-----END CERTIFICATE-----
```

8.1.11 vaww.esrstage1b.aac.va.gov.pem

```
-----BEGIN CERTIFICATE-----
MIIFiDCCBHCgAwIBAgIHPQAAAAC3pzANBgkqhkiG9w0BAQsFADBKMRMwEQYKCZIm
iZPyLGQBGRYDZ292MRIwEAYKCZImiZPyLGQBGRYCdmExHzAdBgNVBAMTFlZBLUlu
dGVybmFsLVMyLUlDQTEtdjEwHhcNMTcwMzE0MjEwNzA5WhcNMjAwMzEzMjEwNzA5
WjCBwDELMAkGA1UEBhMCVVMxDjAMBgNVBAgTBVRleGFzMQ8wDQYDVQQHEwZBdXN0
aW4xKjAoBgNVBAoTIVVTIERlcGFydG1lbnQgb2YgVmV0ZXJhbnMgQWZmYWlyczEN
MAsGA1UECxMEQUlUQzEjMCEGA1UEAxMadmF3dy5lc3JzdGFnZTFiLmFhYy52YS5n
b3YxMDAuBgkqhkiG9w0BCQEWIWNkY293ZWJsb2dpY2FkbWluaXN0cmF0b3JzQHZh
LmdvdjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOKj1U0RxzhQg8ij
tPGY1wH7q5TDfsSvQUoPBbgOF53MYR8VotqM0JViggyP4G/TmYJ/HMvaP/2K1tS5
60hHGIPMg01Xa9ZbxhR6u8rp/A7QiX96jkWzHuuP4OEijW9j23xGcfx3lLaeL4HF
amhrYnIDpYBPkgqltVNLHBQiNJE/FcReCpbhHrHFJyr0L+dmkjQWC/CL44qtsIeo
dM67p87NswOKcaiRsbVw+CosJFZH6WGKgTFDuYyn9ZNpPeBRBUmdS770SCAKukGY
1WIFBXm1AjckGjVUoE9f5N0D8tSPrfyxnxpSIOHcCtkYLwujl4oGj0Iuee9qisn5
jkYVulcCAwEAAaOCAfowggH2MAsGA1UdDwQEAwIFoDBYBgNVHREEUTBPghp2YXd3
LmVzcnN0YWdlMWIuYWFjLnZhLmdvdoIadmF3dy5lc3JzdGFnZTFiLmFhYy52YS5n
b3aCFXZoYWVzcndlYjQuYWFjLnZhLmdvdjAdBgNVHQ4EFgQU61ixAn4MoiuQ4n41
gmSf+uKn4TUwHwYDVR0jBBgwFoAUG23f6z3l4g3vFrHQ3l9YGlbL5OwwSQYDVR0f
BEIwQDA+oDygOoY4aHR0cDovL2NybC5wa2kudmEuZ292L3BraS9jcmwvVkEtSW50
ZXJuYWwtUzItSUNBMS12MS5jcmwwewYIKwYBBQUHAQEEbzBtMEcGCCsGAQUFBzAC
hjtodHRwOi8vYWlhLnBraS52YS5nb3YvcGtpL2FpYS92YS9WQS1JbnRlcm5hbC1T
Mi1JQ0ExLXYxLmNlcjAiBggrBgEFBQcwAYYWaHR0cDovL29jc3AucGtpLnZhLmdv
djA9BgkrBgEEAYI3FQcEMDAuBiYrBgEEAYI3FQiByMMzgfnwBoGlnw2E4IEIhcKq
SwaDgp9ggeCLUgIBZAIBEjAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwEw
JwYJKwYBBAGCNxUKBBowGDAKBggrBgEFBQcDAjAKBggrBgEFBQcDATANBgkqhkiG
9w0BAQsFAAOCAQEAFNLz/wWJSdzIVUGd4bzXTAXktnnP1IanNIrLbW3qNoWyi1ft
4uNL6E5LFsDTMohvwjOGHaphdJmAp9HD4ZJlTWXblXNXe2yPa6jCKspJVc2j42ls
fws0ZxOUeelS/XQZWNjs6qbEOOsJ4PtwOb1Myq/1V1tTWAOTZu3snjH1pVyHmHZ6
35i4mHmZJtHmEVlDg3DzrTvw0ejzgnq3MpvN25Np+Msi0uyLT8qcUjhWgrJS2Aw5
2qyA2n9vfQTcmg5U6eSyzJl4gCoG5xhZaHAmTW4FySAwmcqKyjM4hkySTSKKLqSZ
5Q65eFKajsUIW+jXD63HuiweHP8vrzl/4M1Vkg==
-----END CERTIFICATE-----
```

8.1.12 vaww.esrpre-prod.aac.va.gov.pem

```
-----BEGIN CERTIFICATE-----
MIIFojCCBIqgAwIBAgIHPQAAAADC6jANBgkqhkiG9w0BAQsFADBKMRMwEQYKCZIm
iZPyLGQBGRYDZ292MRIwEAYKCZImiZPyLGQBGRYCdmExHzAdBgNVBAMTFlZBLUlu
dGVybmFsLVMyLUlDQTEtdjEwHhcNMTcwNDA0MTEzMzAxWhcNMjAwNDAzMTEzMzAx
WjCBwTELMAkGA1UEBhMCVVMxDjAMBgNVBAgTBVRleGFzMQ8wDQYDVQQHEwZBdXN0
aW4xKjAoBgNVBAoTIVVTIERlcGFydG1lbnQgb2YgVmV0ZXJhbnMgQWZmYWlyczEN
MAsGA1UECxMEQUlUQzEkMCIGA1UEAxMbdmF3dy5lc3JwcmUtcHJvZC5hYWMudmEu
Z292MTAwLgYJKoZIhvcNAQkBFiFjZGNvd2VibG9naWNhZG1pbmlzdHJhdG9yc0B2
YS5nb3YwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDSSFJ9AnbkaLXB
J7ngjAHzGnkTQM8eKl3k7iYUKLYjhmH9ZuIiYQQEVqh1bsM+YlvdFXLjc1Vg7P10
ntkSG/QBz6VDhd8RkeOjEkLmT4/88VZnlbGRAApaVp3UM6dy5r9fkN0yRgoUBVqS
hPaj0m2Z6UQkKz589eS0lCCWSWzl5K6dFDFvIqmmb0yyfvZ8+lP7BqbI7cOsJAhx
5sDzBKAR3JVsGM+7f5oX/euIyuRagrBcbQPrG6Moc5owEkH6t1s2+m6BiVHENIBn
sGHaIWhq+b1zsQ9vwYjc/9bGHJ7D928la/LRPErsWKL2uSqQcHA7PfJm8wLpkO5Y
+/O7iyNVAgMBAAGjggITMIICDzALBgNVHQ8EBAMCBaAwcQYDVR0RBGowaIIbdmF3
dy5lc3JwcmUtcHJvZC5hYWMudmEuZ292ght2YXd3LmVzcnByZS1wcm9kLmFhYy52
YS5nb3aCFXZoYWVzcndlYjcuYWFjLnZhLmdvdoIVdmhhZXNyd2ViOC5hYWMudmEu
Z292MB0GA1UdDgQWBBQJAFTUt3mxMbBdr/ODTQUQMY2WBjAfBgNVHSMEGDAWgBQb
bd/rPeXiDe8WsdDeX1gaVsvk7DBJBgNVHR8EQjBAMD6gPKA6hjhodHRwOi8vY3Js
LnBraS52YS5nb3YvcGtpL2NybC9WQS1JbnRlcm5hbC1TMi1JQ0ExLXYxLmNybDB7
BggrBgEFBQcBAQRvMG0wRwYIKwYBBQUHMAKGO2h0dHA6Ly9haWEucGtpLnZhLmdv
di9wa2kvYWlhL3ZhL1ZBLUludGVybmFsLVMyLUlDQTEtdjEuY2VyMCIGCCsGAQUF
BzABhhZodHRwOi8vb2NzcC5wa2kudmEuZ292MD0GCSsGAQQBgjcVBwQwMC4GJisG
AQQBgjcVCIHIwzOB+fAGgaWfDYTggQiFwqpLBoOCn2CB4ItSAgFkAgESMB0GA1Ud
JQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDATAnBgkrBgEEAYI3FQoEGjAYMAoGCCsG
AQUFBwMCMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUAA4IBAQAgJ6f4AoV7lndB
myYN1S76+rZGccqOoHKSF074o06os8b8qcRSctJOIRxzWME8wiy55PHS5nkhn0wm
oWna2P6Efec2FQ8ZURsbi8IefwUX7ISWJ99+6C+lL6VrCH1hEQOPXTRdbQm8H3dR
cvhlHNQ3MtXuswI3sFvBqmYFsXsOtRwiRzFuiT7K4v5kW3Kkre5bsjSLBXq1VFjT
PTVMIcH3QgP6hbjfgJtQoHfDoQPFSa6DjbGvja4Y+rQMqiBC1VN1ZLG44VqsDlyC
u5AO830gi/ilgf30Iyv1Jl/mXJT1LdAUZjG5dPtwT4/Jx3KqJ7cDWdy54ddD1RJb
IyXeTQaF
-----END CERTIFICATE-----
```

8.1.13 das-test.va.gov.pem

```
-----BEGIN CERTIFICATE-----
MIIG7TCCBdWgAwIBAgIDBZSiMA0GCSqGSIb3DQEBCwUAMHIxEzARBgoJkiaJk/Is
ZAEZFgNnb3YxEjAQBgoJkiaJk/IsZAEZFgJ2YTERMA8GA1UECxMIU2VydmljZXMx
DDAKBgNVBAsTA1BLSTEmMCQGA1UEAxMdVmV0ZXJhbnMgQWZmYWlycyBEZXZpY2Ug
Q0EgQjIwHhcNMTYwNjEwMTMxOTUwWhcNMTgwODA3MTUyMjQ2WjBVMRMwEQYKCZIm
iZPyLGQBGRYDZ292MRIwEAYKCZImiZPyLGQBGRYCdmExEDAOBgNVBAsTB2Rldmlj
ZXMxGDAWBgNVBAMTD2Rhcy10ZXN0LnZhLmdvdjCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAKJg1wPGT7WrI1FYJ5HkivoJKwR3nulq6n9hD3m+ENXlRbDP
HOrTxOXg2YpSK/ORRdVBN4OXD+NVaVyv4XyWzG2ZIF06wGX9ooGTU2EA/MMKh3ts
XDWTBOIEGjDQ3CUnCZ2J3FF+SSBYtRFRI1CqYt/77kC4GafjDsFy6MfiXdis9O6R
RSaXPCFdF7qRqq3Lx8Qr1sP5rYj4f95HRGKqn4X/5S1z5Us8O+ZReWALUAMtAWr6
ZZ5B8CYhcSxPsvPw7wNl5IYjKGe9/DaXeszHKF7tW3VPOg6/g8gSVsOBVlVayUWx
IjzeXen1DWpusmLkD7a9aVeB1E1+W0amYXmGEUMCAwEAAaOCA6cwggOjMFYGA1Ud
EQRPME2CD2Rhcy10ZXN0LnZhLmdvdoIcdmFhdXNkYXNhcHBpbnQwMDIuYWFjLnZh
LmdvdoIcdmFhdXNkYXNhcHBpbnQwMDMuYWFjLnZhLmdvdjAXBgNVHSAEEDAOMAwG
CmCGSAFlAwIBAwgwggEwBggrBgEFBQcBAQSCASIwggEeMDsGCCsGAQUFBzAChi9o
dHRwOi8vYWlhMS5zc3Atc3Ryb25nLWlkLm5ldC9DQS9WQWRldmljZUNBLnA3YzCB
gAYIKwYBBQUHMAKGdGxkYXA6Ly9kaXIxLnNzcC1zdHJvbmctaWQubmV0L2NuPVZl
dGVyYW5zJTIwQWZmYWlycyUyMERldmljZSUyMENBJTIwQjIsb3U9UEtJLG91PVNl
cnZpY2VzLGRjPXZhLGRjPWdvdj9jQUNlcnRpZmljYXRlMCMGCCsGAQUFBzABhhdo
dHRwOi8vb2NzcC5wa2kudmEuZ292LzA3BggrBgEFBQcwAYYraHR0cDovL29jc3Ax
LnNzcC1zdHJvbmctaWQubmV0L1ZBLVNTUC1DQS1CMjAOBgNVHQ8BAf8EBAMCBaAw
JwYDVR0lBCAwHgYIKwYBBQUHAwEGCCsGAQUFBwMCBghghkgBZQMGBzAfBgNVHSME
GDAWgBSBlDWeKqh3YCNm7Cqdbs+2dRlQXTCCAYEGA1UdHwSCAXgwggF0MDCgLqAs
hipodHRwOi8vY3JsLnBraS52YS5nb3YvUEtJL0NSTC92YWRldmljZS5jcmwwdKBy
oHCGbmxkYXA6Ly9sZGFwLnBraS52YS5nb3YvY24lM2RTU1BCMkFFLGNuJTNkQ0RQ
LGNuJTNkUEtJLGNuJTNkU2VydmljZXMsZGMlM2R2YSxkYyUzZGdvdj9jZXJ0aWZp
Y2F0ZVJldm9jYXRpb25MaXN0MDSgMqAwhi5odHRwOi8vY2RwMS5zc3Atc3Ryb25n
LWlkLm5ldC9DRFAvdmFkZXZpY2UuY3JsMIGToIGQoIGNhoGKbGRhcDovL2RpcjEu
c3NwLXN0cm9uZy1pZC5uZXQvY24lM2RWZXRlcmFucyUyMEFmZmFpcnMlMjBEZXZp
Y2UlMjBDQSUyMEIyLG91JTNkUEtJLG91JTNkU2VydmljZXMsZGMlM2R2YSxkYyUz
ZGdvdj9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0MB0GA1UdDgQWBBRJxg3+eZpU
APnLc56q/SjzkLYrFzANBgkqhkiG9w0BAQsFAAOCAQEAYW2JnS8JhfoGH0DTQrYr
bw8ZXEjGW/jwG1rVzsRNRt3ncBLdj2Zis0QjDo9mArG5s/xHpa35aQZjUGQAgv/t
wZ3jl1lH0jZIAch6tn7YRzhpqA7u5ozf8eUTpuAeJtVFeIo9RUR871DWWYpWPMw7
D4LGcLB4HpLfBb/4BMXQnM1cyCsXYSkXDQHl+xPzUUQkJpi7JRdoMLPxZ2r9ewJf
dDbn8FEnxmNkI15G7qCmaW2cmfitnsJ8hoZC+rLL7B3+0/kzZL3O2yzX2WXmUWzk
Z3Mf3C9K+LOWsrTwVUOkiVJL6xrbI6j2dOGpgShDnn7d5+ftgHsXi3GdbEHYx2Ah
4w==
-----END CERTIFICATE-----
```

8.1.14 das-sqa.va.gov.pem

```
-----BEGIN CERTIFICATE-----
MIIG7DCCBdSgAwIBAgIDBbrgMA0GCSqGSIb3DQEBCwUAMHIxEzARBgoJkiaJk/Is
ZAEZFgNnb3YxEjAQBgoJkiaJk/IsZAEZFgJ2YTERMA8GA1UECxMIU2VydmljZXMx
DDAKBgNVBAsTA1BLSTEmMCQGA1UEAxMdVmV0ZXJhbnMgQWZmYWlycyBEZXZpY2Ug
Q0EgQjIwHhcNMTYwODI2MTY0NzE3WhcNMTgwODA3MTUyMjQ2WjBUMRMwEQYKCZIm
iZPyLGQBGRYDZ292MRIwEAYKCZImiZPyLGQBGRYCdmExEDAOBgNVBAsTB2Rldmlj
ZXMxFzAVBgNVBAMTDmRhcy1zcWEudmEuZ292MIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAqRt193fnTlYYwqxiC6XMCcOOsJorP1Wop43czuqGH0P3Z2uj
f5ubSi8jfvqQGhuWVJ6mjAxJQevjpuFddu3GGWMVvofa96wA852qdMcXtj8z9exH
L1rN86o+8CkU7yj9iFsasSWf0a0CLK3jz+GiGakmtztnoZoXc2T+e3NaJhASIdjU
IZH5hVB4qi4PgmCW6rL7SAOetcCtMtaAFS0DK8s+VLxSeAzDjvybAc6jXgUXDYNK
Dr3HtWDy3AKz3kOkva4ipDnxrcNKPJN01EM+RKMy7s23BjmBq3EHnB+4fT6t62DL
OJhKqQ7jqJCBLoNeEHnth7+i3VVL0N4eEqPxoQIDAQABo4IDpzCCA6MwVgYDVR0R
BE8wTYIOZGFzLXNxYS52YS5nb3aCHHZhYXVzZGFzYXBwc3FhMDAxLmFhYy52YS5n
b3aCHXZhYXVzZGFzYXBwc3FhMDAyLmFhYy52YS5nb3YgMBcGA1UdIAQQMA4wDAYK
YIZIAWUDAgEDCDCCATAGCCsGAQUFBwEBBIIBIjCCAR4wOwYIKwYBBQUHMAKGL2h0
dHA6Ly9haWExLnNzcC1zdHJvbmctaWQubmV0L0NBL1ZBZGV2aWNlQ0EucDdjMIGA
BggrBgEFBQcwAoZ0bGRhcDovL2RpcjEuc3NwLXN0cm9uZy1pZC5uZXQvY249VmV0
ZXJhbnMlMjBBZmZhaXJzJTIwRGV2aWNlJTIwQ0ElMjBCMixvdT1QS0ksb3U9U2Vy
dmljZXMsZGM9dmEsZGM9Z292P2NBQ2VydGlmaWNhdGUwIwYIKwYBBQUHMAGGF2h0
dHA6Ly9vY3NwLnBraS52YS5nb3YvMDcGCCsGAQUFBzABhitodHRwOi8vb2NzcDEu
c3NwLXN0cm9uZy1pZC5uZXQvVkEtU1NQLUNBLUIyMA4GA1UdDwEB/wQEAwIFoDAn
BgNVHSUEIDAeBggrBgEFBQcDAQYIKwYBBQUHAwIGCGCGSAFlAwYHMB8GA1UdIwQY
MBaAFIGUNZ4qqHdgI2bsKp1uz7Z1GVBdMIIBgQYDVR0fBIIBeDCCAXQwMKAuoCyG
Kmh0dHA6Ly9jcmwucGtpLnZhLmdvdi9QS0kvQ1JML3ZhZGV2aWNlLmNybDB0oHKg
cIZubGRhcDovL2xkYXAucGtpLnZhLmdvdi9jbiUzZFNTUEIyQUUsY24lM2RDRFAs
Y24lM2RQS0ksY24lM2RTZXJ2aWNlcyxkYyUzZHZhLGRjJTNkZ292P2NlcnRpZmlj
YXRlUmV2b2NhdGlvbkxpc3QwNKAyoDCGLmh0dHA6Ly9jZHAxLnNzcC1zdHJvbmct
aWQubmV0L0NEUC92YWRldmljZS5jcmwwgZOggZCggY2GgYpsZGFwOi8vZGlyMS5z
c3Atc3Ryb25nLWlkLm5ldC9jbiUzZFZldGVyYW5zJTIwQWZmYWlycyUyMERldmlj
ZSUyMENBJTIwQjIsb3UlM2RQS0ksb3UlM2RTZXJ2aWNlcyxkYyUzZHZhLGRjJTNk
Z292P2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3QwHQYDVR0OBBYEFM46SuxQAM8n
ayR/hlJgt/b0caNbMA0GCSqGSIb3DQEBCwUAA4IBAQAOz+ie4OlLRty9CTpt7qtm
CCg8O5Msj5PDTm2QM2nX+VRiwV3cMldgsoK0gr9SKvjx+8sArMQLkzC21XavuwVh
Qn42mKm1XJvk3kbJx7Na0tg+8etepzHv1tfORJ1taCt1NTPIU8IBAxZWsYh81218
k8u7/KtnsK6zqiBRaNloovMl20CDxeWnFRzSLrTV91Z5V+gr1KlEIS3WkiHO7d+n
wqYnZB4fA0mjJ83Mrt8IxiTZTP8Qn1LoyPR/vfoqOUamxRBWlIo4wTvEvN6+9hJ3
GQhfO9E/l7v5lvgh7Wor58X+iRIBvj04PyU9PB8/ZYTst/t5IoucbMCir77ZEk0B
-----END CERTIFICATE-----
```

8.1.15 das.va.gov.pem

```
-----BEGIN CERTIFICATE-----
MIIHezCCBmOgAwIBAgIDBfJ1MA0GCSqGSIb3DQEBCwUAMHIxEzARBgoJkiaJk/Is
ZAEZFgNnb3YxEjAQBgoJkiaJk/IsZAEZFgJ2YTERMA8GA1UECxMIU2VydmljZXMx
DDAKBgNVBAsTA1BLSTEmMCQGA1UEAxMdVmV0ZXJhbnMgQWZmYWlycyBEZXZpY2Ug
Q0EgQjIwHhcNMTcwMTA2MTk1MTE1WhcNMTgwODA3MTUyMjQ2WjBQMRMwEQYKCZIm
iZPyLGQBGRYDZ292MRIwEAYKCZImiZPyLGQBGRYCdmExEDAOBgNVBAsTB2Rldmlj
ZXMxEzARBgNVBAMTCmRhcy52YS5nb3YwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDZSc8gGHDms81rMeAffccObXAmUPpiG49PECDwNnIkPu6oSd3xEUuZ
9AWR7S+tR8zyzca2G8GaJj0OQxgT2C4vz2mniuNTnEkA1sTf2eNbMN7kcEo6SJJX
P+GUEmpszqxVIoi0nzvOiEfkfVfhu5rxI5fWUdNxYj7DErCMTiQtn1GAvEittYK5
pZJSvGuth+VHGYD3u6Oz1L1Gx+2z0DZYUJriB9nX0JzTAAPFr9maxac5qMwAwbNz
3bcpu1mYOaYkMHFEiUB6qLs8VoQli/rUlg6dDAK0amtu+dvNYA4q2g+HMoOXRrXj
yzuT+lOAMc8rzjBCJuJiAX4hJanLV7KnAgMBAAGjggQ6MIIENjCB6AYDVR0RBIHg
MIHdggpkYXMudmEuZ292ghx2YWF1c2Rhc2FwcHJwZDAwMS5hYWMudmEuZ292ghx2
YWF1c2Rhc2FwcHByZDAwMi5hYWMudmEuZ292ghx2YWF1c2Rhc2FwcHByZDAwMy5h
YWMudmEuZ292ghx2YWF1c2Rhc2FwcHByZDAwNC5hYWMudmEuZ292ghx2YWF1c2Rh
c2FwcHByZDAwNS5hYWMudmEuZ292ghx2YWF1c2Rhc2FwcHByZDAwNi5hYWMudmEu
Z292ght2YWF1c2Rhc2FwcHByZDQzLmFhYy52YS5nb3YwFwYDVR0gBBAwDjAMBgpg
hkgBZQMCAQMIMIIBMAYIKwYBBQUHAQEEggEiMIIBHjA7BggrBgEFBQcwAoYvaHR0
cDovL2FpYTEuc3NwLXN0cm9uZy1pZC5uZXQvQ0EvVkFkZXZpY2VDQS5wN2MwgYAG
CCsGAQUFBzAChnRsZGFwOi8vZGlyMS5zc3Atc3Ryb25nLWlkLm5ldC9jbj1WZXRl
cmFucyUyMEFmZmFpcnMlMjBEZXZpY2UlMjBDQSUyMEIyLG91PVBLSSxvdT1TZXJ2
aWNlcyxkYz12YSxkYz1nb3Y/Y0FDZXJ0aWZpY2F0ZTAjBggrBgEFBQcwAYYXaHR0
cDovL29jc3AucGtpLnZhLmdvdi8wNwYIKwYBBQUHMAGGK2h0dHA6Ly9vY3NwMS5z
c3Atc3Ryb25nLWlkLm5ldC9WQS1TU1AtQ0EtQjIwDgYDVR0PAQH/BAQDAgWgMCcG
A1UdJQQgMB4GCCsGAQUFBwMBBggrBgEFBQcDAgYIYIZIAWUDBgcwHwYDVR0jBBgw
FoAUgZQ1niqod2AjZuwqnW7PtnUZUF0wggGBBgNVHR8EggF4MIIBdDAwoC6gLIYq
aHR0cDovL2NybC5wa2kudmEuZ292L1BLSS9DUkwvdmFkZXZpY2UuY3JsMHSgcqBw
hm5sZGFwOi8vbGRhcC5wa2kudmEuZ292L2NuJTNkU1NQQjBRSxjbiUzZENEUCxj
biUzZFBLSSxjbiUzZFNlcnZpY2VzLGRjJTNkdmEsZGMlM2Rnb3Y/Y2VydGlmaWNh
dGVSZXZvY2F0aW9uTGlzdDA0oDKgMIYuaHR0cDovL2NkcDEuc3NwLXN0cm9uZy1p
ZC5uZXQvQ0RQL3ZhZGV2aWNlLmNybDCBk6CBkKCBjYaBimxkYXA6Ly9kaXIxLnNz
cC1zdHJvbmctaWQubmV0L2NuJTNkVmV0ZXJhbnMlMjBBZmZhaXJzJTIwRGV2aWNl
JTIwQ0ElMjBCMixvdSUzZFBLSSxvdSUzZFNlcnZpY2VzLGRjJTNkdmEsZGMlM2Rn
b3Y/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdDAdBgNVHQ4EFgQUvaLuziprIjqH
vyKPGlFwBP6elTwwDQYJKoZIhvcNAQELBQADggEBACOKYWvcihUGT0M9q/dw2FeN
jHzc9ghlsLxDOH1z5zpUfo7vCN5XvckRtPJBxAgPfBma+Cvm4MvJ09Cz6XTKkfZL
joqRm1dg9n61+bIEiX2wgwDT8yBYQRC+eoM6UdoSN7hk60xxZnvahJAdGEStwl2+
FdtejxfiRJr0kA9he/Yrl1EJ2NmWK1YWG6UPzGa1rT4H/OQGTItdxr1VIAff75Ub
089I4vVubkSLAgiwd5xpQnS27uj3OgQUjvJvSwU59/cdMoAw+XLNBlgXVcB3eplK
3SbuZJIJRbhg8HZn4D6aX/g+g0ZPjATMZWBPNLpgPYX/dW5rYjhbs5d5rXUikgc=
-----END CERTIFICATE-----
```