Pharmacy Reengineering (PRE) Inbound ePrescribing 4.0

Deployment, Installation, Rollback, and Back-Out Guide

January 2021

Department of Veterans Affairs

Office of Information and Technology (OI&T)

Revision History

Date	Version	Description	Author
01/28/2021	4.0	Updates for changes with 4.0.5.012 reference: pg4 3.1, pg5 3.2.1, pg7 3.2.3, pg9 4.1, pg19 4.2, pg39 4.8	Technatomy
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

Date	Version	Description	Author
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 to have the ability to transfer prescriptions electronically between pharmacies, both VA to VA, as well as VA to non-VA (ideally). Once received, these prescriptions will then be fed into the existing Veterans Health Information Systems and Technology Architecture (VistA) Outpatient Pharmacy (OP) for processing and dispensing.

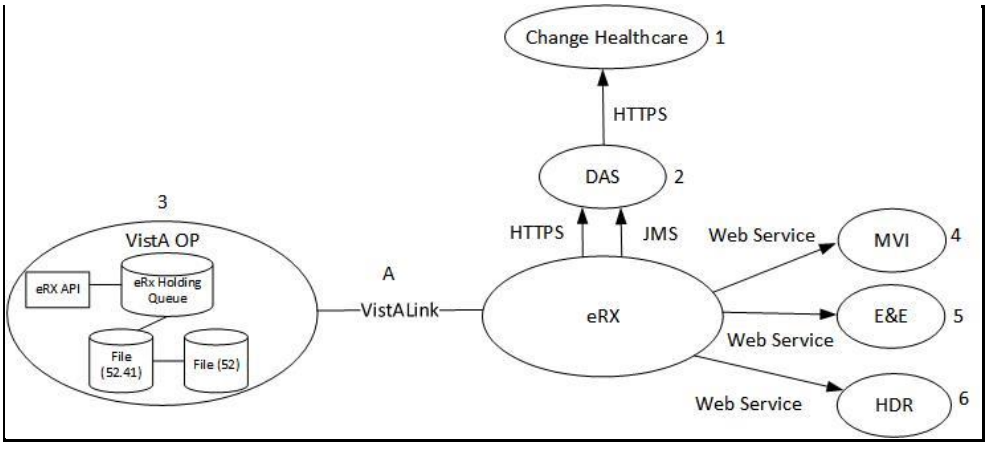
1.1 Purpose

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

1.2 Dependencies

Figure 2 depicts the Inbound 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

ID	Team	Phase / Role	Tasks	Project Phase (See Schedule)
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 (what are the criteria that trigger a back-out).	Deployment
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 - NewRx and Cancel Rx Request/Response	09/23/19-12/20/19
VIP Build 2 - RxRenewal Request/Response	12/23/19-04/10/20
VIP Build 3 - RxChange / Rational Migration	03/23/20-06/12/20
VIP Build 4 - RxChange / Rational Migration	06/15/20-09/04/20
VIP Build 5 - Regression Testing, Bug fixes, Certification Test	09/08/20-10/16/20
IOC Preparation and Testing	10/19/20-12/10/20

3.2 Site Readiness Assessment

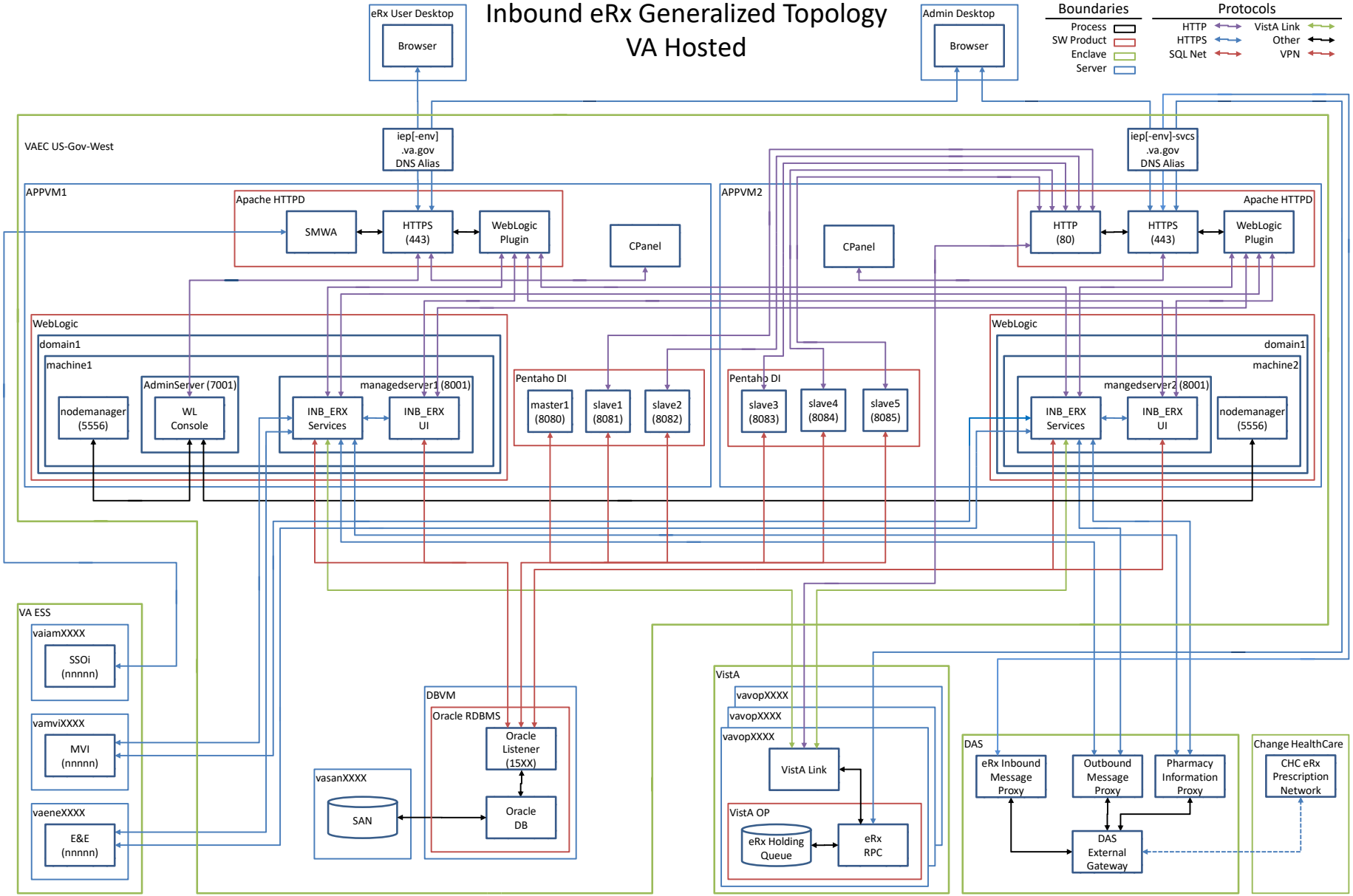
This section discusses the locations that will receive the PRE Inbound eRx application deployment. Topology determinations are made by Enterprise Systems Engineering (ESE) and vetted by Field Operations (FO), National Data Center Program (NDCP), and AITC during the design phase as appropriate. Field 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 October of 2020. IOC sites are:

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

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	12.2.1.4	Clustered	Oracle	
Oracle Database	Database	19.0.0.0.0	Standalone (not synchronized across data centers)	Oracle	
Pentaho Data Integration	Data Integration Tool	9.0.0.0	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.4.0\deployments

3.3.4 Communications

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

- Communication between the development team and AITC will occur via email and conference calls scheduled through Microsoft Lync.
- Notification of scheduled maintenance periods that require the service to be offline or that may degrade system performance will be disseminated to the business user community a minimum of 48 hours prior to the scheduled event.
- Notification to VA users for unscheduled system outages or other events that impact the response time will be distributed within 30 minutes of the occurrence.
- Notification will be distributed to VA users regarding technical help desk support for obtaining assistance with receiving and processing inbound eRxs, and sending and receiving eRx transfers.

3.3.4.1 Deployment/Installation/Back-Out Checklist

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

Table 5: Deployment/Installation/Back-Out Checklist

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

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

RAM (GB)	Space (GB)	CPUs	OS	VM Description/Use/DNS Required
16	300	4	RHEL 7	DEV1 DB Server running Oracle
16	300	4	RHEL 7	DEV2 DB Server running Oracle
16	300	4	RHEL 7	SQA1 DB Server running Oracle
16	300	4	RHEL 7	DEV1 AP Server running Apache/WebLogic
16	300	4	RHEL 7	DEV2 AP Server running Apache/WebLogic
16	300	4	RHEL 7	DEV3 DB Server running Oracle/AP Server running Apache/WebLogic
16	300	4	RHEL 7	DEV3 AP Server running Apache/WebLogic
16	300	4	RHEL 7	SQA1 AP Server running Apache/WebLogic
16	300	4	RHEL 7	SQA1 AP Server running Apache/WebLogic

Table 7: Staging Detailed VM Requirements

RAM (GB)	Space (GB)	CPUs	OS	VM Description/Use/DNS Required
16	800	4	RHEL 7	STAG1/STAG2 DB Server running Oracle
16	300	4	RHEL 7	STAG1 Application Server running Apache/WebLogic
16	300	4	RHEL 7	STAG1 Application Server running Apache/WebLogic
16	300	4	RHEL 7	STAG2 Application Server running Apache/WebLogic
16	300	4	RHEL 7	STAG2 Application Server running Apache/WebLogic

Table 8: Pre-Production Detailed VM Requirements

RAM (GB)	Space (GB)	CPUs	OS	VM Description/Use/DNS Required
16	1300	4	RHEL 7	PREP1 DB Server running Oracle
16	1300	4	RHEL 7	PREP2 DB Server running Oracle
16	300	4	RHEL 7	PREP1 Application Server running Apache/WebLogic
16	300	4	RHEL 7	PREP1 Application Server running Apache/WebLogic
16	300	4	RHEL 7	PREP2 Application Server running Apache/WebLogic
16	300	4	RHEL 7	PREP2 Application Server running Apache/WebLogic

Table 9: Production Detailed VM Requirements

RAM (GB)	Space (GB)	CPUs	OS	VM Description/Use/DNS Required
16	1300	4	RHEL 7	PROD1 DB Server running Oracle
16	1300	4	RHEL 7	PROD2 DB Server running Oracle
16	300	4	RHEL 7	PROD1 Application Server running Apache/WebLogic
16	300	4	RHEL 7	PROD1 Application Server running Apache/WebLogic
16	300	4	RHEL 7	PROD2 Application Server running Apache/WebLogic
16	300	4	RHEL 7	PROD2 Application Server running Apache/WebLogic

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
DEV3	/u01/oracle	$ORACLE_BASE/wlserver	$ORACLE_BASE/user_projects/domains/iep-dev3
SQA1	/u01/app/Oracle_Home	$ORACLE_BASE/wlserver	$ORACLE_BASE/user_projects/domains/erxdomain1
STAG1	/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
PREP1	/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
PROD1	/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: Environment Variables (Continued)

ENV	JAVA_HOME		
DEV1	/u01/app/java/latest	N/A	N/A
DEV2	/u01/app/java/latest	N/A	N/A
DEV3	/u01/oracle/java/latest	N/A	N/A
SQA1	/u01/app/java/latest	N/A	N/A
STAG1	/u01/app/java/latest	N/A	N/A
STAG2	/u01/app/java/latest	N/A	N/A
PREP1	/u01/app/java/latest	N/A	N/A
PREP2	/u01/app/java/latest	N/A	N/A
PROD1	/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

The following table lists the symbolic names that should be substituted throughout this document as system administrators are completing the installation steps.

Table 12: 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
DEV3	vaausapperx803.aac.va.gov	vaausapperx803	vaausapperx804.aac.va.gov	vaausapperx804	iep-dev3
SQA1	vaauserxappsqa1.aac.va.gov	vaauserxappdev1	vaauserxappdev2.aac.va.gov	vaauserxappdev2	erxdomain1
STAG1	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
PREP1	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
PROD1	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 13: 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
DEV3	dev2	Dev3	8001	vaausapperx803.aac.va.gov	vaausapperx803	vaauserxdbsdev1.aac.va.gov	ERXD1	1549
SQA1	sqa1	Sqa1	8001	vaauserxappsqa2.aac.va.gov	vaauserxappsqa2	vaauserxdbssqa1.aac.va.gov	ERXS1	1549
STAG1	stag1	Stag1	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
PREP1	prep1	Prep1	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
PROD1	prod1	Prod1	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 14: Symbolic Names by Environment (cont)

ENV	mserver1	mserver2	cluster	machine1	machine2
DEV1	erx1	erx2	dev1	Machine1	Machine2
DEV2	erx1	erx2	dev1	Machine1	Machine2
DEV3	ManagedServer001	ManagedServer002	Cluster001	Machine1	Machine2
SQA1	erx1	erx2	dev1	Machine1	Machine2
STAG2	ManagedServer001	ManagedServer002	Cluster001	Machine1	Machine2
STAG1	ManagedServer001	ManagedServer002	Cluster001	Machine1	Machine2
PREP2	ManagedServer001	ManagedServer002	Cluster001	Machine1	Machine2
PREP1	ManagedServer001	ManagedServer002	Cluster001	Machine1	Machine2
PROD2	ManagedServer001	ManagedServer002	Cluster001	Machine1	Machine2
PROD1	ManagedServer001	ManagedServer002	Cluster001	Machine1	Machine2

Table 15: 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"
DEV3	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"

Table 16: Symbolic Names by Environment (cont)

ENV	iam_hco	iam_policy_entries
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"
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 17: 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 18: Symbolic Names for sensitive items

Symbolic Name
keystore_passphrase
privatekey_passphrase
weblogic_password

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 X Windows on VM1 and VM2

1. Install the Linux X Window libraries (the following must be performed by a system administrator):
   ```
   $ dzdo 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 dzdo su to another account, first modify the .Xauthority file
6. As your normal Linux login account:
   ```
   $ cp ~/.Xauthority /tmp
   ```
7. After you dzdo su to another user, copy the .Xauthority file:
   ```
   $ cp /tmp/.Xauthority ~
   ```

4.2.2 Setup Administration Accounts on VM1 and VM2

1. Verify the /etc/sudoers file has "#includedir /etc/sudoers.d" entry near the end of the file, if not, perform the following:
   ```
   $ dzdo chmod u+w /etc/sudoers
   $ dzdo vi /etc/sudoers
   ```
   Add #includedir /etc/sudoers.d near the end of the file, exit the vi editor.
   ```
   $ dzdo chmod u+w /etc/sudoers
   ```
2. Modify the Linux weblogic account .bash_profile, replace the PATH= and export PATH with the following near the end of the file:
   ```
   export JAVA_HOME=[ORACLE_BASE]/java/latest
   export PATH=${JAVA_HOME}/bin:${PATH}:${HOME}/bin
   ```
3. Create the oracle software directory if it doesn't exist (the following must be performed by a system administrator):
   ```
   $ dzdo chmod 755 /u01
   $ dzdo mkdir -p /u01/oracle
   $ dzdo chown weblogic:weblogic /u01/oracle
   $ dzdo chmod 755 /u01/oracle
   ```
4. Create the Linux kettle user and group (the following must be performed by a system administrator):
   ```
   $ dzdo groupadd -g 7600 kettle
   $ dzdo useradd -g kettle
   $ dzdo usermod -a -G weblogic kettle (weblogic group already exists in LDAP)
   ```

5. Create the app software directory if it doesn't exist (the following must be performed by a system administrator):

```
$ dzdo chmod 755 /u01
$ dzdo mkdir -p /u01/app
$ dzdo chown weblogic:weblogic /u01/app
$ dzdo chmod 755 /u01/app
```

6. Create the pentaho software directory if it doesn't exist (the following must be performed by a system administrator):

```
$ dzdo mkdir -p /u01/app/pentaho
$ dzdo chown kettle:kettle /u01/app/pentaho
$ dzdo chmod 755 /u01/app/pentaho
```

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

```
umask 0022
```

8. Modify the Linux kettle account .bash_profile, replace the PATH= and export PATH with the following near the end of the file:

```
export JAVA_HOME=[ORACLE_BASE]/java/latest
export PATH=${JAVA_HOME}/bin:${PATH}:${HOME}/bin
```

9. Create the Linux kettle sudoer file (the following must be performed by a system administrator):

```
$ dzdo vi /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
```

10. Create the Linux apache sudoer file (the following must be performed by a system administrator):

```
$ dzdo vi /etc/sudoers.d/apache
apache ALL=(kettle:kettle) NOPASSWD:/u01/app/cpanel/bin/carte_slave_util.sh
```

4.2.3 Install Java on VM1 and VM2

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

```
$ dzdo su - weblogic
```

2. Create downloads directory if it doesn't exist (the following must be performed by a system administrator):

```
$ dzdo mkdir -p /u01/downloads
$ dzdo chown weblogic:weblogic /u01/downloads
$ dzdo chmod 777 /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
$ chmod 755 /u01/app/java
```

5. Unpack the Oracle JDK 1.8 archive in the downloads directory:

```
$ cd /u01/app/java
$ gzip -cd < /u01/downloads/jdk-8u[xxx]-linux-x64.tar.gz | tar xvf -
```

6. Create symbolic link for latest Java installation:

```
$ ln -s jdk1.8.0_[xxx] latest
```

7. Open permissions to permit access to all users:

```
$ find jdk1.8.0_[xxx] -type d -exec chmod g+rx,o+rx {} \;
$ find jdk1.8.0_[xxx] -type f -exec chmod g+r,o+r {} \;
exit
```

8. Return back in your normal Linux login account.

```
$ exit
```

4.2.4 Apache Installation on VM1 and VM2

Perform the following steps on VM1 and VM2:

1. EO SA installs standard Apache 2.2 RHEL6 RPM, as your normal Linux login account verify as follows:

```
$ dzdo rpm -q -a | grep httpd
httpd-tools-2.4.6-95.el7.x86_64
httpd-2.4.6-95.el7.x86_64
```

2. Install the Linux NSS package (the following must be performed by a system administrator):

```
$ dzdo yum install mod_nss.x86_64
```

3. Modify the httpd startup configuration (the following must be performed by a system administrator):

```
$ dzdo systemctl enable httpd # for RHEL 7 systems
```

4.2.5 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:

```
$ dzdo vi /etc/httpd/conf/httpd.conf
```

2. Modify Listen parameter in /etc/http/conf/httpd.conf:

```
Listen 80
```

3. Modify <Directory /> section in /etc/http/conf/httpd.conf:

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

4. Modify <Directory "/var/www/html"> section in /etc/http/conf/httpd.conf:

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

5. Modify < IfModule alias_module> section in /etc/http/conf/httpd.conf:

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

6. Modify <Directory "/var/www/cgi-bin"> section in /etc/http/conf/httpd.conf:

```
<Directory "/var/www/cgi-bin">
    AllowOverride None
    Options None
    Order allow,deny
    Allow from all
</Directory>
```

7. Add Header Edit entries to bottom of /etc/http/conf/httpd.conf

```
# Set security options for cookies (to prevent cross-site scripting [XSS] attacks)
  Header edit Set-Cookie "(?i)^((?:(?!;\s?HttpOnly).)+)$" "$1; HttpOnly"
  Header edit Set-Cookie "(?i)^((?:(?!;\s?secure).)+)$" "$1; Secure"
# Prevent clickjacking attacks
  Header always append X-Frame-Options DENY
```

8. Disable SSL:

```
$ dzdo mv /etc/httpd/conf.d/ssl.conf /etc/httpd/conf.d/ssl.conf_orig
$ dzdo touch /etc/httpd/conf.d/ssl.conf
$ dzdo chmod 644 /etc/httpd/conf.d/ssl.conf
```

9. Modify the httpd startup configuration (the following must be performed by a system administrator):

```
$ dzdo systemctl enable httpd
```

10. Start Apache:

```
$ dzdo systemctl start httpd
```

4.2.6 Certificate Configuration

1. Generate a permanent certificate using Venafi:
   Nickname: ***[vm1_fqdn]***
   Description: ***[ERX|IEP] [ENV]***
   SAN's: ***[vm1_fqdn], [vm1_fqdn]***
2. Generate a ***[vm1_fqdn]*** pkcs12 certificate store:

```
$ openssl pkcs12 -export -name [vm1_fqdn] -in [vm1_fqdn].crt -inkey [vm1_fqdn].key -out
[vm1_fqdn].p12
Enter Export Password: ####
Verifying - Enter Export Password: ####
```

3. Generate a ***[vm2_fqdn]*** pkcs12 certificate store:

```
$ openssl pkcs12 -export -name [vm2_fqdn] -in [vm1_fqdn].crt -inkey [vm1_fqdn].key -out
[vm2_fqdn].p12
Enter Export Password: ####
Verifying - Enter Export Password: ####
```

4. Generate ***[vm1_fqdn]*** java keystore:

```
$ keytool -importkeystore -deststorepass ######## -destkeypass ######## -destkeystore
[vm1_fqdn].jks -srckeystore [vm1_fqdn].p12 -srcstoretype PKCS12 -srcstorepass #### -alias
[vm1_fqdn]
```

5. Import VA-Internal-S2-RCA1-v1.pem Certificate into ***[vm1_fqdn]*** java keystore:

```
$ keytool -import -alias VA-Internal-S2-RCA1-v1 -file VA-Internal-S2-RCA1-v1.pem -
keystore [proxy_fqdn].jks
Enter keystore password: ########
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

6. Import VA-Internal-S2-ICA4-v1.pem Certificate into ***[vm1_fqdn]*** java keystore:

```
$ keytool -import -alias VA-Internal-S2-ICA1-v1 -file VA-Internal-S2-ICA1-v1.pem -
keystore [proxy_fqdn].jks
Enter keystore password: ########
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

4.2.7 Create NSS certificate database on VM1

1. Create a new NSS certificate database:

```
$ dzdo mv /etc/httpd/alias /etc/httpd/alias_orig
$ dzdo mkdir /etc/httpd/alias
$ dzdo chmod 755 /etc/httpd/alias
$ dzdo certutil -N -d sql:/etc/httpd/alias
Enter new password: ####
Re-enter password: ####
```

2. Add server permanent certificate:

```
$ dzdo pk12util -i [proxy_fqdn].p12 -d sql:/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:

```
$ dzdo certutil -A -d sql:/etc/httpd/alias -i VA-Internal-S2-RCA1-v1.pem -t CT,, \
    -n VA-Internal-S2-RCA1-v1
$ dzdo certutil -A -d sql:/etc/httpd/alias -i /u01/tmp/va_internal_s2_ica4.pem -t CT,, \
    -n va_internal_s2_ica4
$ dzdo certutil -A -d sql:/etc/httpd/alias -i /u01/tmp/va_internal_s2_rca1.pem -t CT,, \
    -n va_internal_s2_rca1
```

4. Modify certificate database permissions:

```
$ dzdo chmod g+rx,o+rx /etc/httpd/alias
$ dzdo chmod -R g+r,o+r /etc/httpd/alias/*
```

5. Verify installed certificates:

```
$ certutil -L -d sql:/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:

```
$ dzdo chmod g+r,o+r /etc/httpd/conf/password.conf
```

8. Start HTTPD server

```
$ dzdo systemctl start httpd
```

4.2.8 Create NSS certificate database on VM2

1. Create a new NSS certificate database:

```
$ dzdo mv /etc/httpd/alias /etc/httpd/alias_orig
$ dzdo mkdir /etc/httpd/alias
$ dzdo cp /etc/httpd/alias_orig/pkcs11.txt /etc/httpd/alias
$ dzdo certutil -N -d sql:/etc/httpd/alias
Enter new password: ####
Re-enter password: ####
```

2. Add server permanent certificate:

```
$ dzdo pk12util -i [vm2_fqdn].p12 -d sql:/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:

```
$ dzdo certutil -A -d sql:/etc/httpd/alias -i VA-Internal-S2-RCA1-v1.pem -t CT,, \
    -n VA-Internal-S2-RCA1-v1
$ dzdo certutil -A -d sql:/etc/httpd/alias -i /u01/tmp/va_internal_s2_ica4.pem -t CT,, \
    -n va_internal_s2_ica4
$ dzdo certutil -A -d sql:/etc/httpd/alias -i /u01/tmp/va_internal_s2_rca1.pem -t CT,, \
    -n va_internal_s2_rca1
```

4. Modify certificate database permissions:

```
$ dzdo chmod g+rx,o+rx /etc/httpd/alias
$ dzdo chmod -R g+r,o+r /etc/httpd/alias/*
```

5. Verify installed certificates:

```
$ certutil -L -d sql:/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:

```
$ dzdo chmod g+r,o+r /etc/httpd/conf/password.conf
```

8. Start HTTPD server

```
$ dzdo systemctl start httpd
```

4.2.9 NSS Configuration on VM1 and VM2

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.

```
$ cd /etc/httpd/conf.d
$ dzdo cp nss.conf nss.conf_orig
$ dzdo mv ssl.conf ssl.conf_orig
$ dzdo touch ssl.conf
$ dzdo chmod 644 ssl.conf
```

2. Modify NSS configuration:

```
$ dzdo cp /etc/httpd/conf.d/nss.conf /etc/httpd/conf.d/nss.conf_orig
$ dzdo 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. Modify NSSCertificateDatabase parameter:

```
#NSSCertificateDatabase /etc/httpd/alias
NSSCertificateDatabase sql:/etc/httpd/alias
```

   j. Save the nss.conf file.

3. Start HTTPD server

```
$ dzdo systemctl restart httpd
```

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

4.2.10 NSS Configuration on VM2

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.

```
$ cd /etc/httpd/conf.d
$ dzdo mv ssl.conf ssl.conf_orig
$ dzdo touch ssl.conf
$ dzdo chmod 644 ssl.conf
```

2. Modify NSS configuration:

```
$ dzdo 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 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. Modify NSSCertificateDatabase parameter:

```
#NSSCertificateDatabase /etc/httpd/alias
NSSCertificateDatabase sql:/etc/httpd/alias
```

   j. Save the nss.conf file.

3. Start HTTPD server

```
$ dzdo systemctl restart httpd
```

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

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

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

1. As your normal Linux login account, dzdo su to the weblogic account:
```
$ dzdo su - weblogic
```
2. Create downloads directory if it doesn't exist (the following must be performed by a system administrator):
```
$ dzdo mkdir -p /u01/downloads
$ dzdo chown weblogic:weblogic /u01/downloads
$ dzdo chmod 777 /u01/downloads
```
3. Download Oracle WLS Plugin 12.2.1.3 archive (v44415-01) to the downloads directory:

   Download from AITC IEP eRx Downloads directory
4. Unzip the Oracle WLS Plugin 12.2.1.3 archive to in the downloads directory:
```
$ unzip fmw_12.2.1.3.0_wlsplugins_Disk1_1of1.zip WLSPlugins12c-12.2.1.3.0.zip
$ unzip WLSPlugins12c-12.2.1.3.0.zip \
    WLSPlugin12.2.1.3.0-Apache2.2-Apache2.4-Linux_x86_64-12.2.1.3.0.zip
$ mkdir WLSPlugin12.2.1.3.0-Apache2.2-Apache2.4-Linux_x86_64-12.2.1.3.0
$ unzip WLSPlugin12.2.1.3.0-Apache2.2-Apache2.4-Linux_x86_64-12.2.1.3.0 \
    -d WLSPlugin12.2.1.3.0-Apache2.2-Apache2.4-Linux_x86_64-12.2.1.3.0
$ chmod -R g+rx,o+rx WLSPlugin12.2.1.3.0-Apache2.2-Apache2.4-Linux_x86_64-12.2.1.3.0
$ exit
```
5. You should be back in your normal Linux login account.
6. Copy the Apache Plug-in for WebLogic libraries to the HTTPD modules directory (the following must be performed by a system administrator):
```
$ dzdo cp -r /u01/downloads/WLSPlugin12.2.1.3.0-Apache2.2-Apache2.4-Linux_x86_64-
12.2.1.3.0 /etc/httpd/modules/WLSPlugin
$ dzdo find /etc/httpd/modules/WLSPlugin -type d -exec chmod g+rx,o+rx {} \;
$ dzdo find /etc/httpd/modules/WLSPlugin -type f -exec chmod g+r,o+r {} \;
```
7. Modify the /etc/sysconfig/httpd file (the following must be performed by a system administrator):
```
$ dzdo vi /etc/sysconfig/httpd
```
   Add the following to the end of the file:
```
# Update LD_LIBRARY_PATH to include Weblogic Plugin
LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/etc/httpd/modules/WLSPlugin/lib
```

4.2.12 Install Centrify for Apache on VM1 and VM2

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

1. Create downloads directory if it doesn't exist (the following must be performed by a system administrator):

```
$ dzdo mkdir -p /u01/downloads
$ dzdo chown weblogic:weblogic /u01/downloads
$ dzdo chmod 777 /u01/downloads
```

2. As your normal Linux login account, dzdo su to the weblogic account:

```
$ dzdo su - weblogic
```

3. Download the Centrify for Apache package (centrify-apache-4.4.4-rhel3-x86_64.tgz) to the downloads directory from AITC IEP eRx Downloads directory
4. Unzip Centrify for Apache package to in the downloads directory:

```
$ cd /u01/downloads
$ mkdir centrify-apache-4.4.4-rhel3-x86_64
$ tar xvzf centrify-apache-4.4.4-rhel3-x86_64.tgz -C centrify-apache-4.4.4-rhel3-x86_64
$ chmod o+rx centrify-apache-4.4.4-rhel3-x86_64
$ chmod o+r centrify-apache-4.4.4-rhel3-x86_64/*
$ exit
```

5. You should be back in your normal Linux login account.
6. Install the Centrify for Apache package (the following must be performed by a system administrator):

```
$ dzdo rpm -Uvh /u01/downloads/centrify-apache-4.4.4-rhel3-x86_64/centrifydc-apache-
4.4.4-rhel3-x86_64.rpm
```

4.2.13 Install IEP CPanel on VM1 and VM2

1. On VM1, create downloads directory if it doesn't exist (the following must be performed by a system administrator):

```
$ dzdo mkdir -p /u01/downloads
$ dzdo chown weblogic:weblogic /u01/downloads
$ dzdo chmod 777 /u01/downloads
```

2. Download the eRx/IEP Configurator (erx_iep_ x.x.x.xxx_configur_yyyymmdd _hhmmss.sh) to the downloads directory.
3. As your normal Linux login account, dzdo execute the eRx/IEP Configurator (erx_iep_ x.x.x.xxx_configur_yyyymmdd _hhmmss.sh) (the following must be performed by a system administrator):

```
$ dzdo /u01/downloads/erx_iep_ x.x.x.xxx_configur_yyyymmdd _hhmmss.sh
```

4. Select options 1 and 2, then Exit (x).
5. Repeat steps 1 through 4 on VM2
6. Check the CPanel, pull up the following URL's in a Browser:

```
$ https://[vm1_fqdn]/cpanel
$ https://[vm2_fqdn]/cpanel
```

4.2.14 Install Apache SSOi Web Agent on VM1

1. Create downloads directory if it doesn't exist (the following must be performed by a system administrator):

```
$ dzdo mkdir -p /u01/downloads
$ dzdo chown weblogic:weblogic /u01/downloads
$ dzdo chmod 777 /u01/downloads
```

2. As your normal Linux login account, dzdo su to the weblogic account:

```
$ dzdo su - weblogic
```

3. 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

4. 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
```

5. You should be back in your normal Linux login account.
6. Start Xming or other X Server on your Windows Desktop/Laptop. Connect to the server using Putty. The DISPLAY environment variable should be set.
7. Execute the CA SiteMinder Apache Web Agent installer (the following must be performed by a system administrator):

```
$ dzdo /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>
```

4.2.15 Configure Apache SSOi Web Agent on VM1

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

```
$ dzdo 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.

4.2.16 Post Configure Edits for Apache SSOi Web Agent on VM1

1. As your normal Linux login account, dzdo su to the root account:

```
$ dzdo 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 webagent files

```
# chmod 666 /u01/app/CA/webagent/config/SmConf.conf
# chmod 777 /u01/app/CA/webagent/log
```

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.

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

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

dzdo systemctl edit httpd.service

This will open a text file to edit. Drop in the following:

[Service]
ExecStart=
ExecReload=

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

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

Do a reload:
dzdo systemctl daemon-reload

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

Cheers!

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

14. Restart Apache and check the logs for connection or errors.

```
# exit
$ dzdo service httpd stop
$ dzdo 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 on VM1 and VM2

1. Start Xming or other X Server on your Windows Desktop/Laptop. Connect to the server using Putty. The DISPLAY environment variable should be set.
2. As your normal Linux login account, copy your .Xauthority file to /tmp:
```
$ cp ~/.Xauthority /tmp
$ chmod 644 /tmp/.Xauthority
$ echo $DISPLAY
```
3. As your normal Linux login account, dzdo su to the weblogic account:
```
$ dzdo su - weblogic
```
4. Copy the .Xauthority file from your normal Linux account to the current account:
```
$ cp ~yourusername/.Xauthority .
$export DISPLAY=[value from step 2]
```
5. Create downloads directory if it doesn't exist (the following must be performed by a system administrator):
```
$ dzdo mkdir -p /u01/downloads
$ dzdo chown weblogic:weblogic /u01/downloads
$ dzdo chmod 777 /u01/downloads
```
6. Download Oracle WLS 12.2.1.4 installer to the downloads directory:

Download from AITC IEP eRx Downloads directory

7. Unzip the Oracle WLS 12.1.3 installer to the downloads directory:
   ```
   $ unzip fmw_12.2.1.4.0_wls_Disk1_1of1.zip fmw_12.2.1.4.0_wls.jar
   ```
8. Run the Oracle WLS 12.1.3 installer:
   ```
   $ java -jar fmw_12.2.1.4.0_wls.jar
   ```
9. Enter "y" to accept prerequisite checks.
10. Enter "/u01/oracle/oraInventory".
11. Click **OK**.

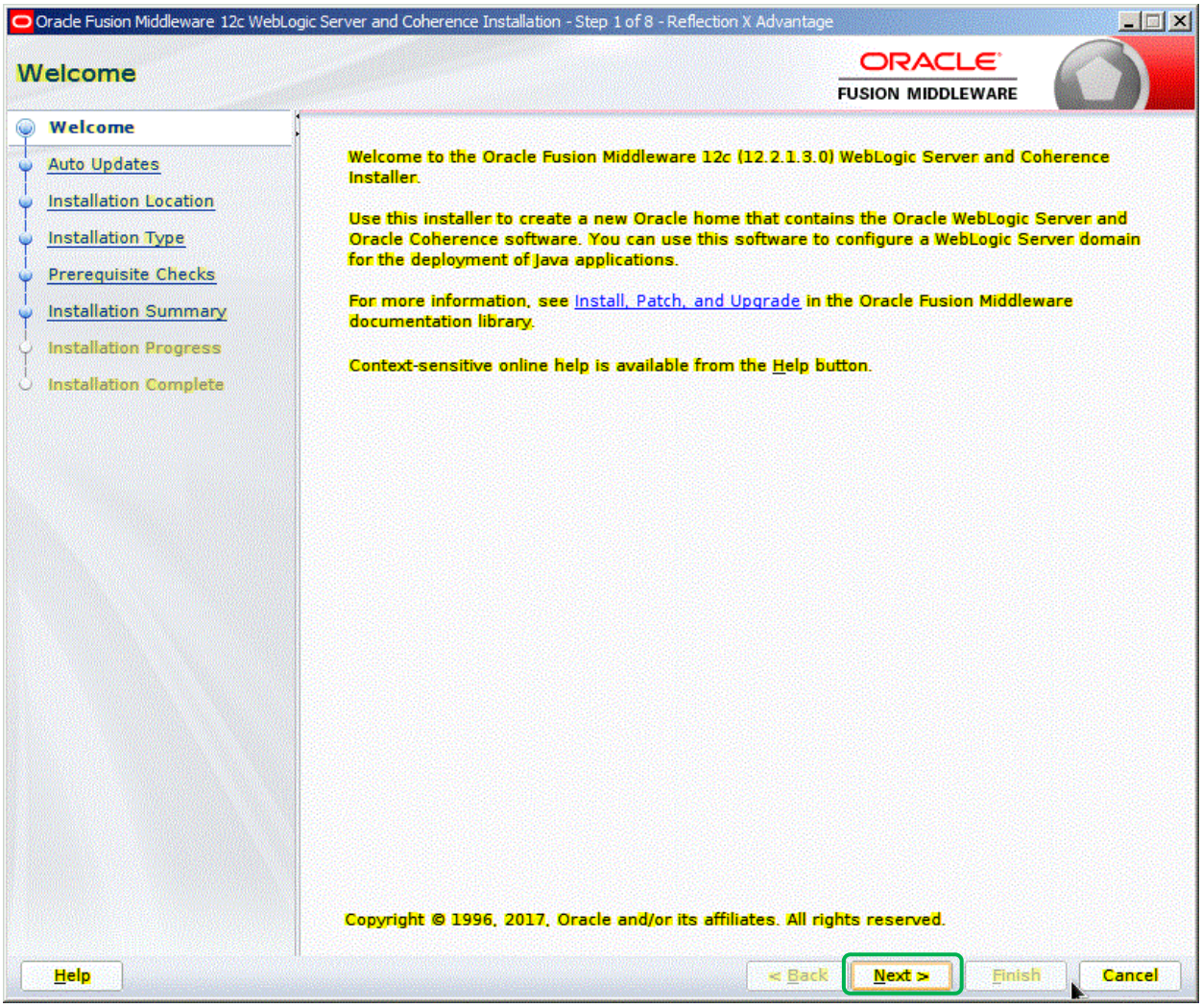
Figure 3: Install WebLogic – Oracle Fusion Middleware Installation Inventory Setup

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

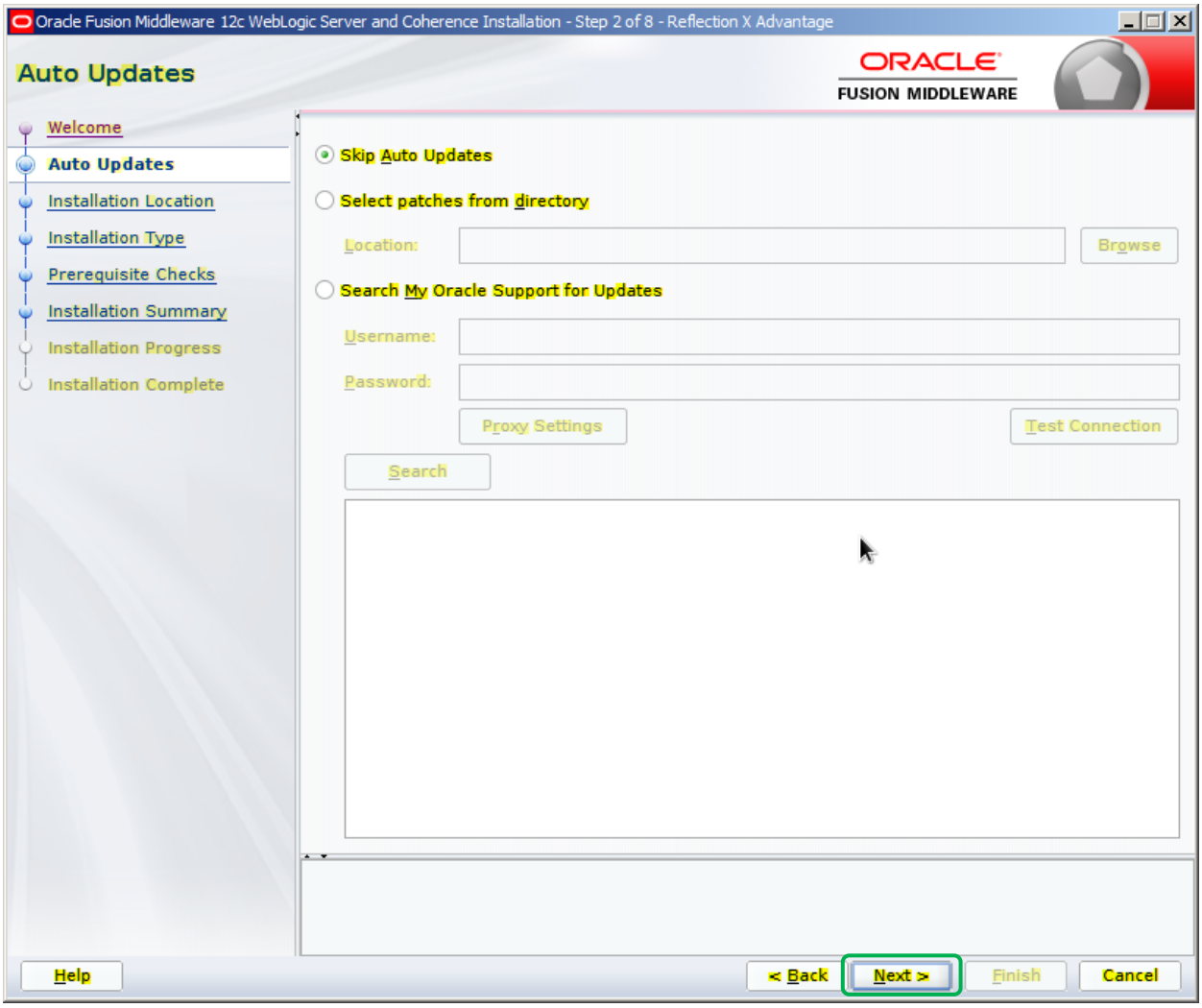
Figure 4: Install WebLogic – Oracle Universal Installer Dialog Box

13. Once the installer comes up, click **Next**.

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

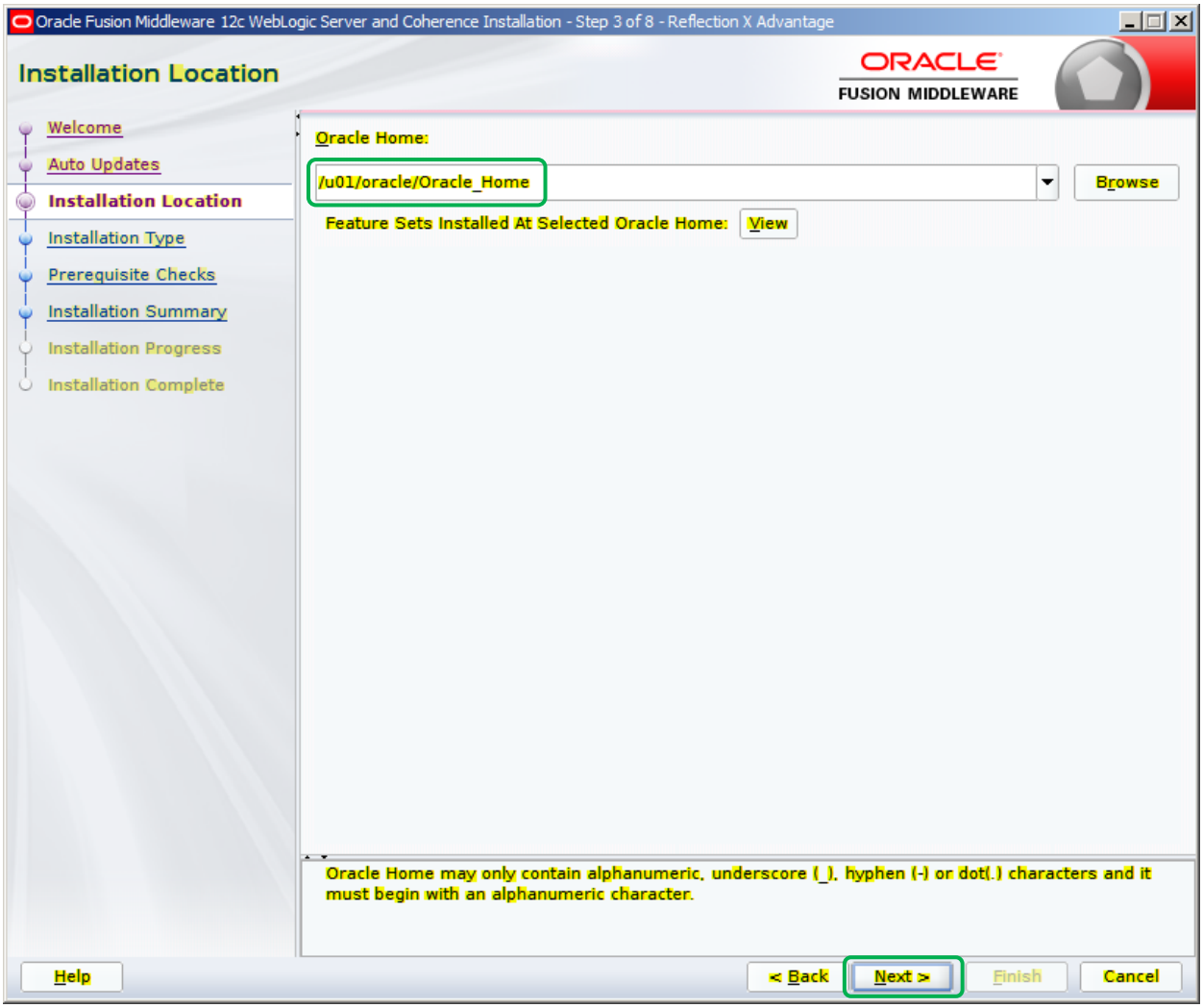


14. Click Next:



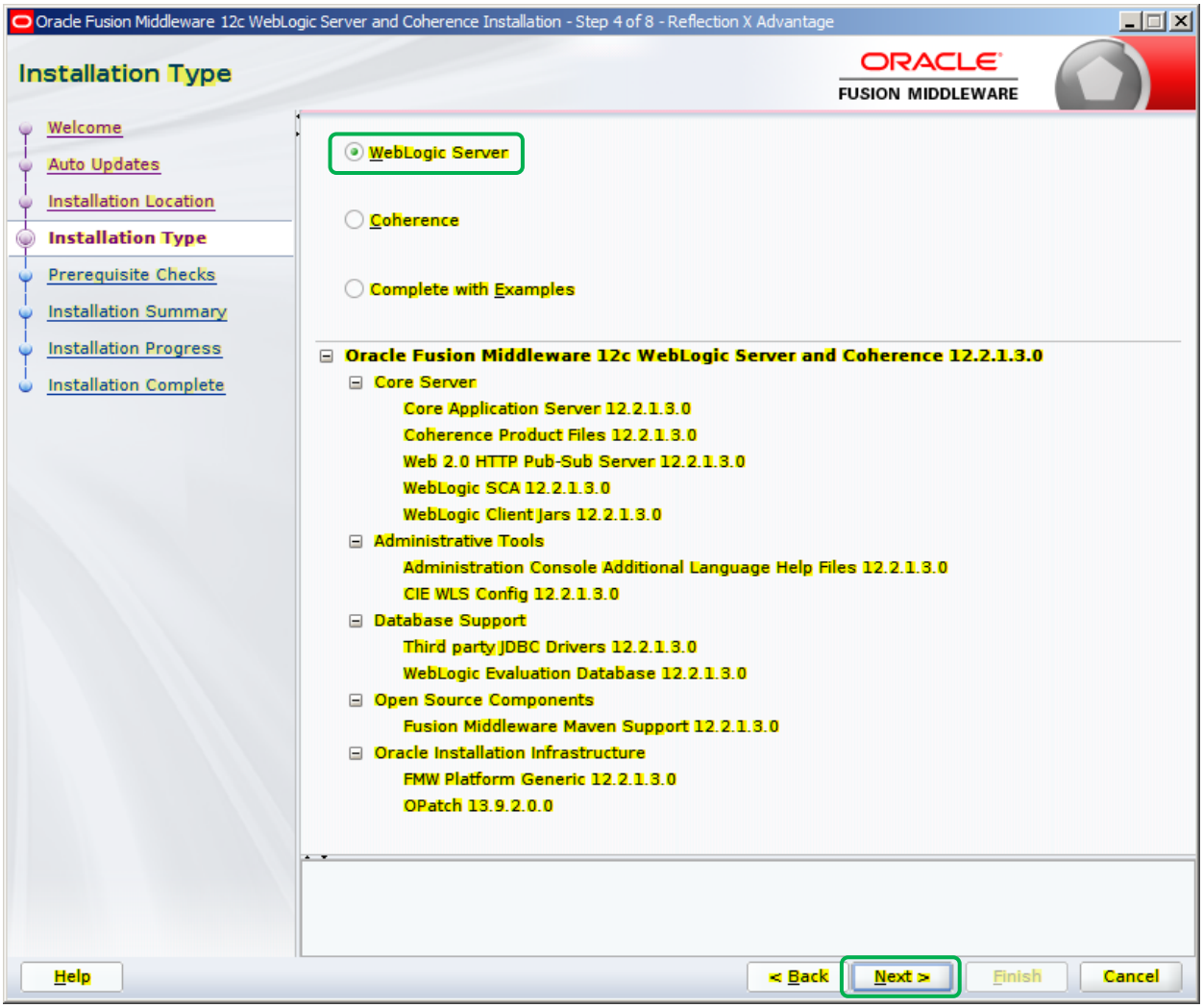
15. Enter *Oracle Home*: "***[ORACLE_BASE]***".
16. Click **Next**.

Figure 6: Install WebLogic – Installation Location



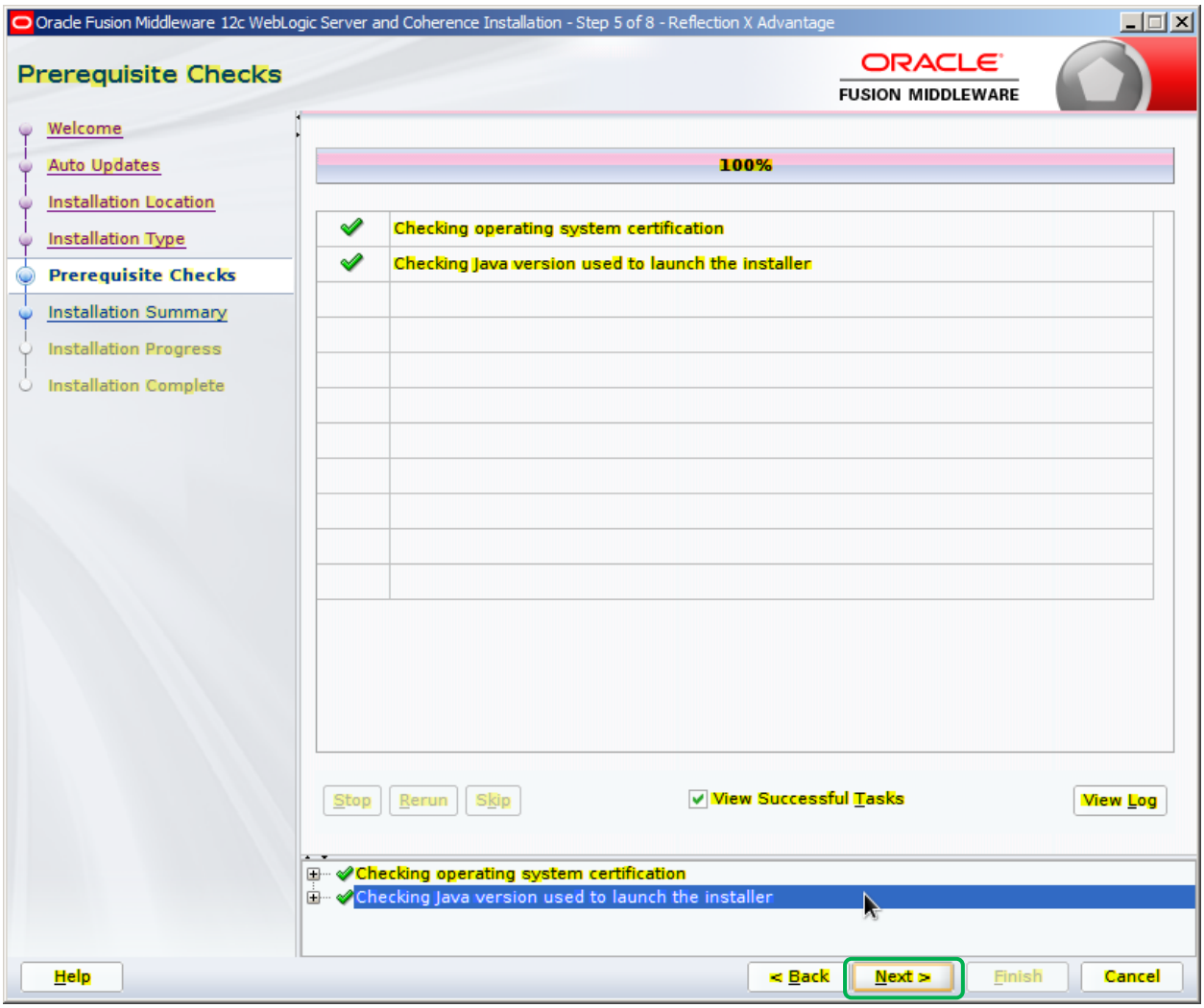
17. For *Installation Type*, select the *WebLogic Server* radio button.
18. Click **Next**.

Figure 7: Install WebLogic – Installation Type



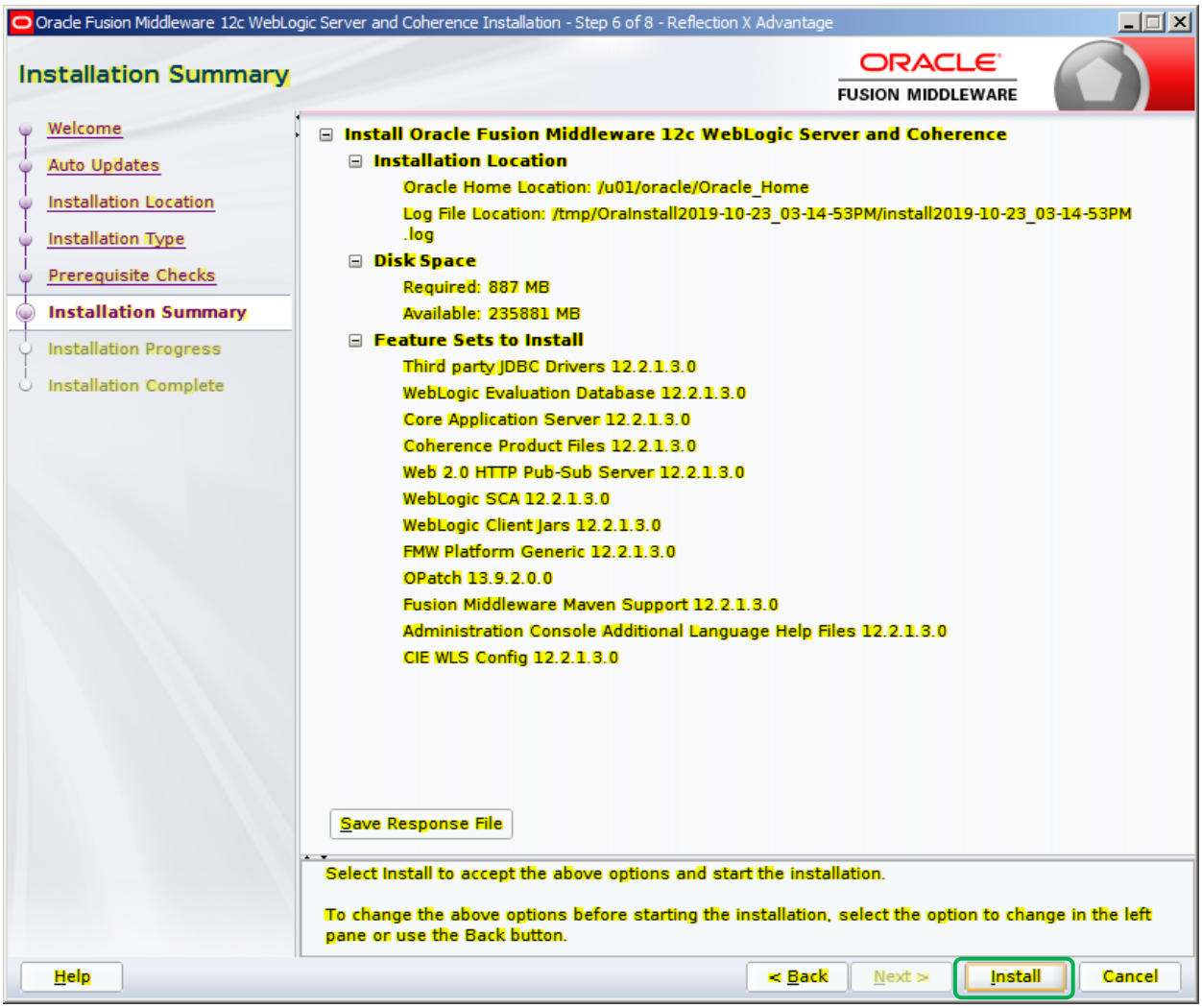
19. Click **Next** again on the **Prerequisite Checks** screen.

Figure 8: Install WebLogic – Prerequisite Checks



20. On the *Installation Summary* screen, click **Install**.

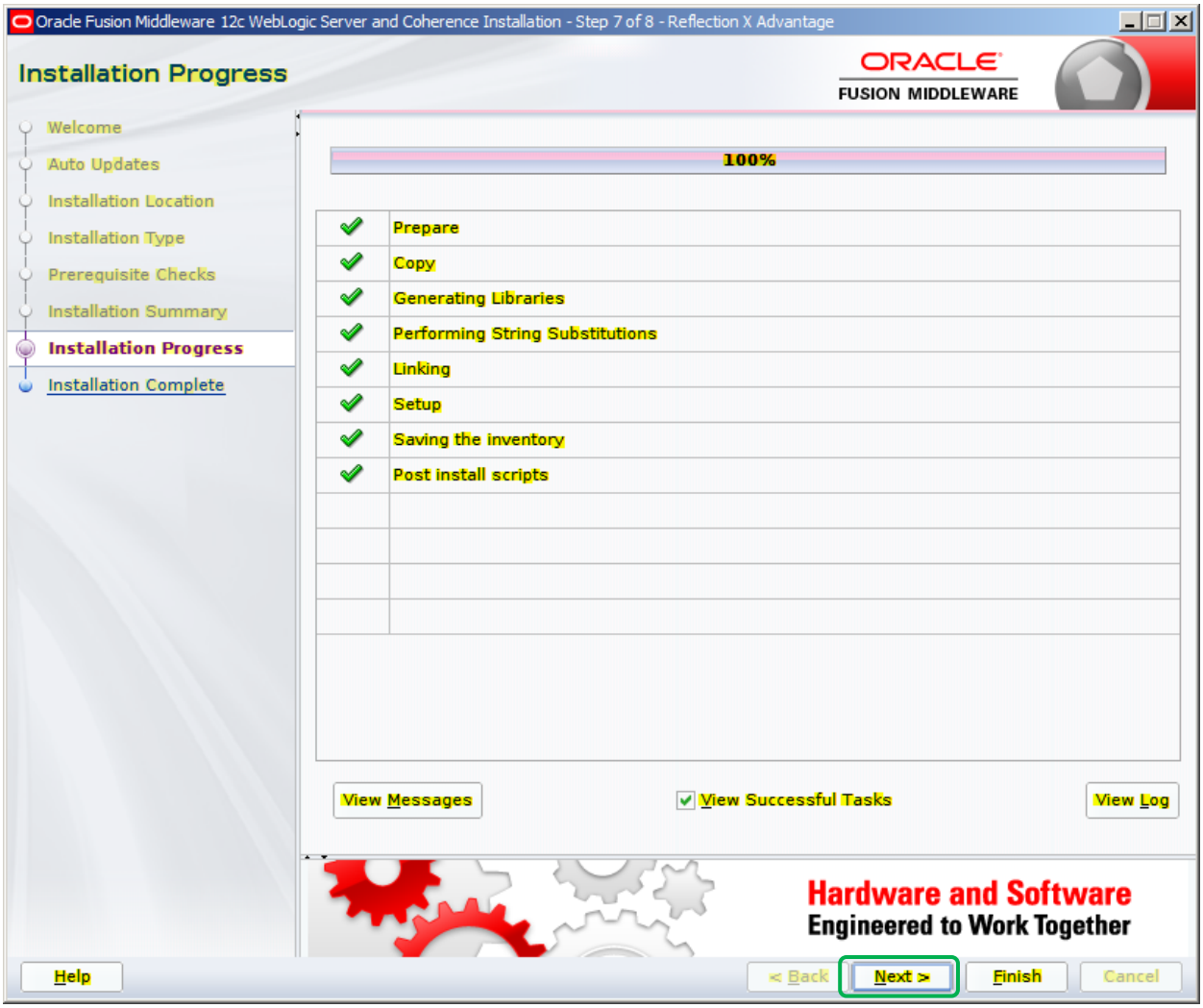
Figure 9: Install WebLogic – Installation Summary Screen



21. Wait while the installation progresses.

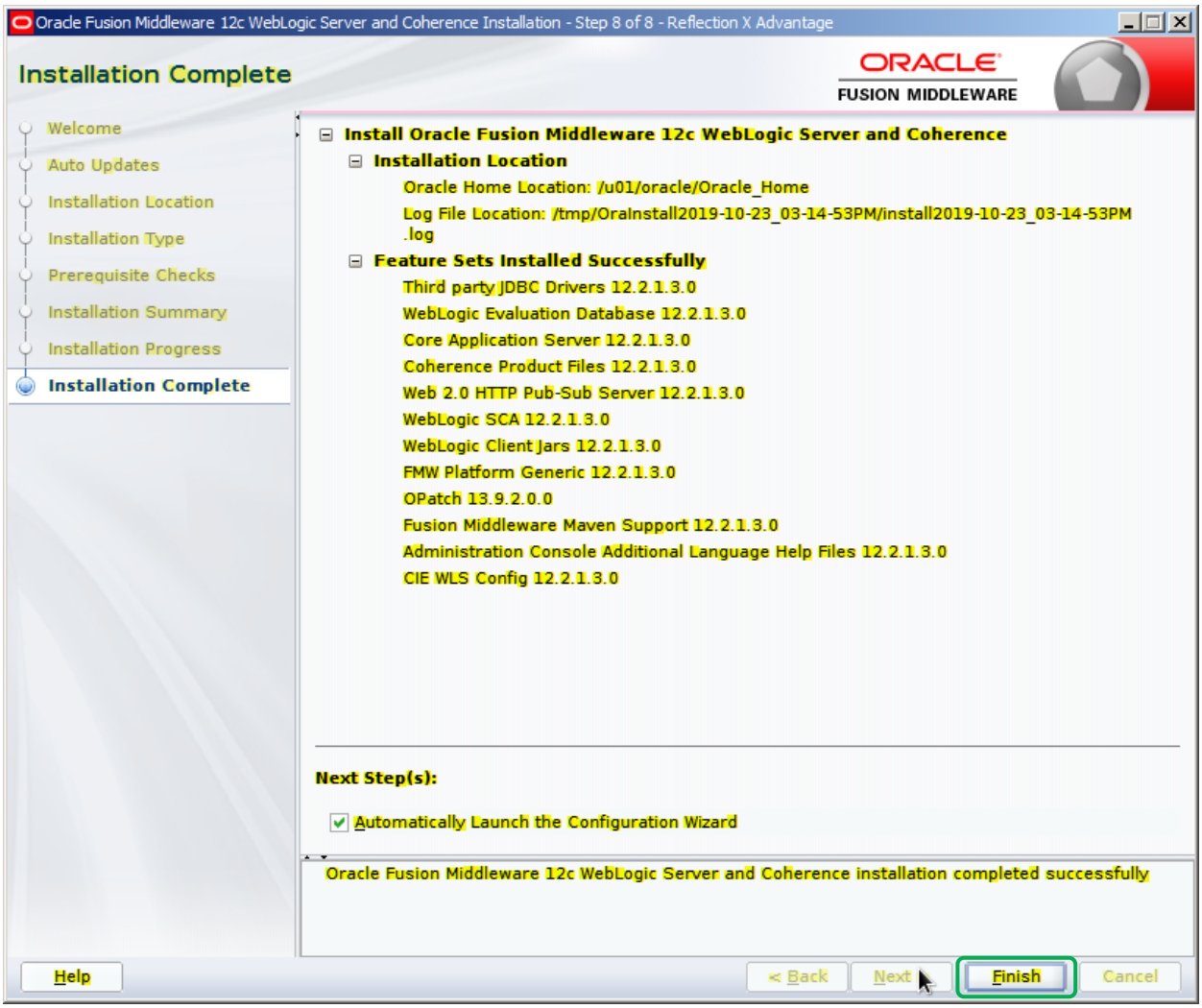
22. Once the installation is complete, the following screen will display.
23. Click **Next**.

Figure 10: Install WebLogic – Installation Progress Screen



24. On VM1, leave *Automatically Launch the Configuration Wizard* checked, on VM2 uncheck it.
25. Click **Finish**.

Figure 11: Install WebLogic – Installation Complete

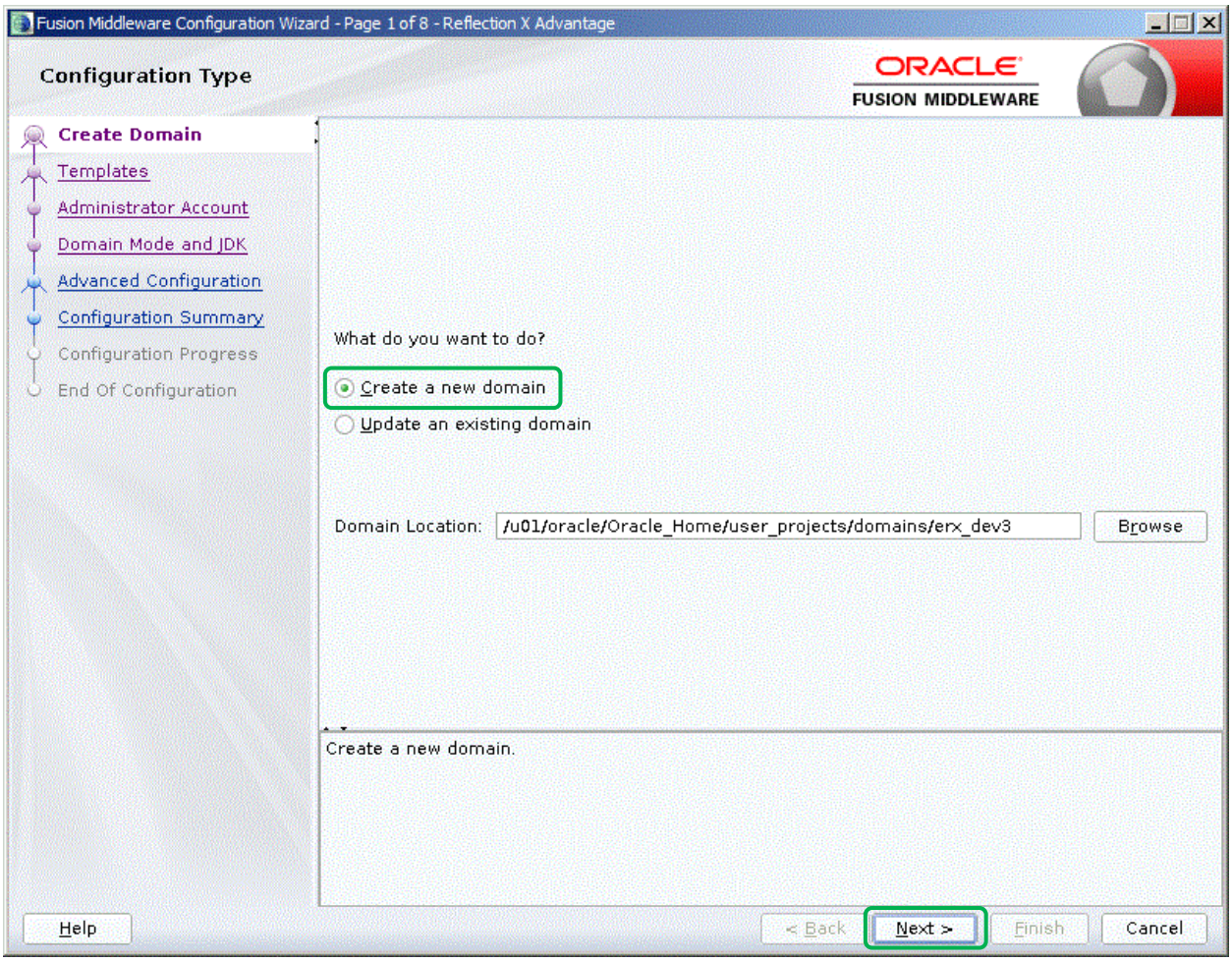


26. On VM2, skip the remaining steps in this section.
27. On VM1, the Oracle **Configuration Wizard** splash screen will appear for a few moments.

Figure 12: Install WebLogic – Oracle Configuration Wizard Splash Screen

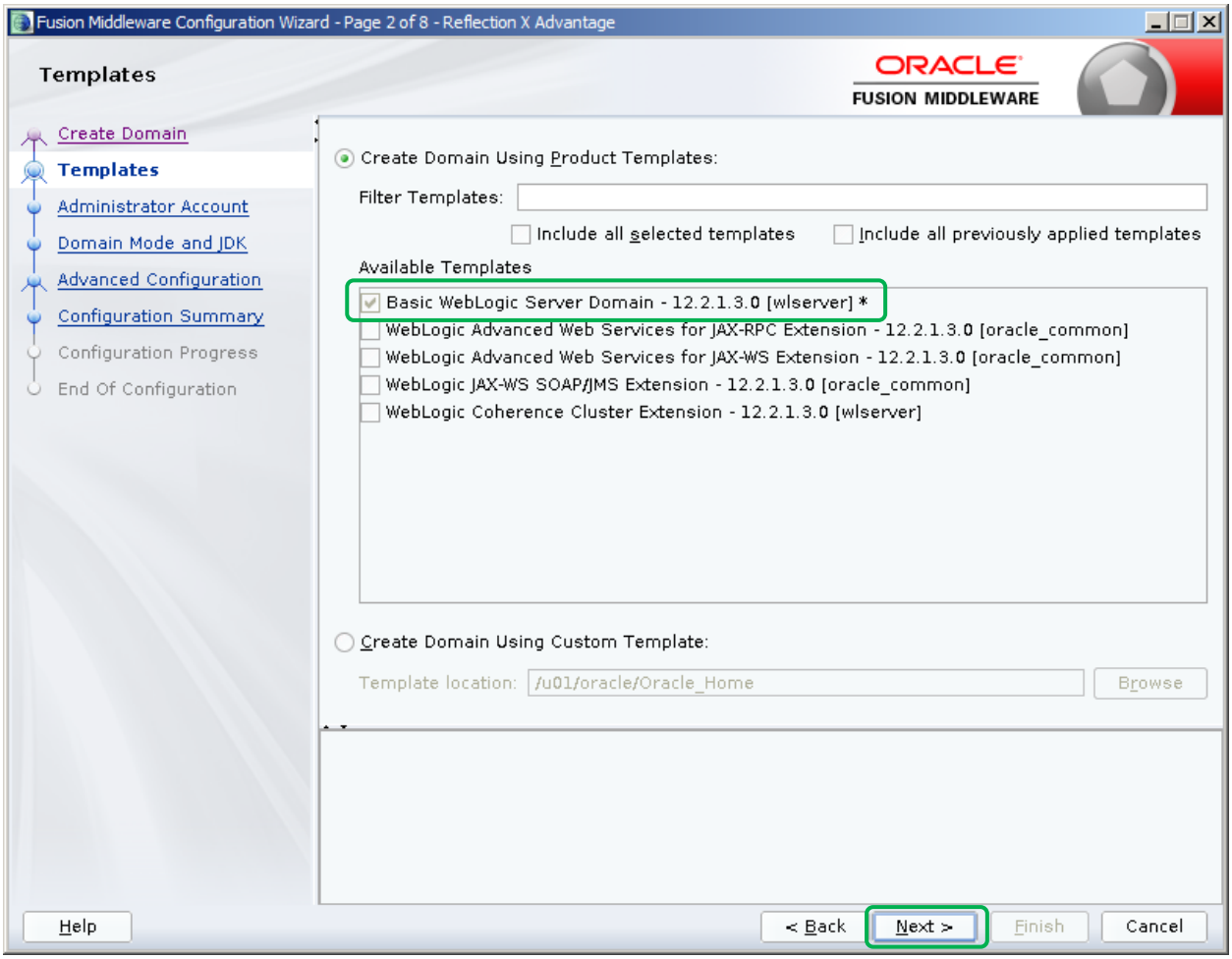
28. On the **Configuration Type** screen, select *Create a new domain*.
29. Enter the following in the *Domain Location*:
    [ORACLE_BASE]`/Oracle_Home/user_projects/domains/`***[domain]***
30. Click **Next**.

Figure 13: Install WebLogic – Create New Domain



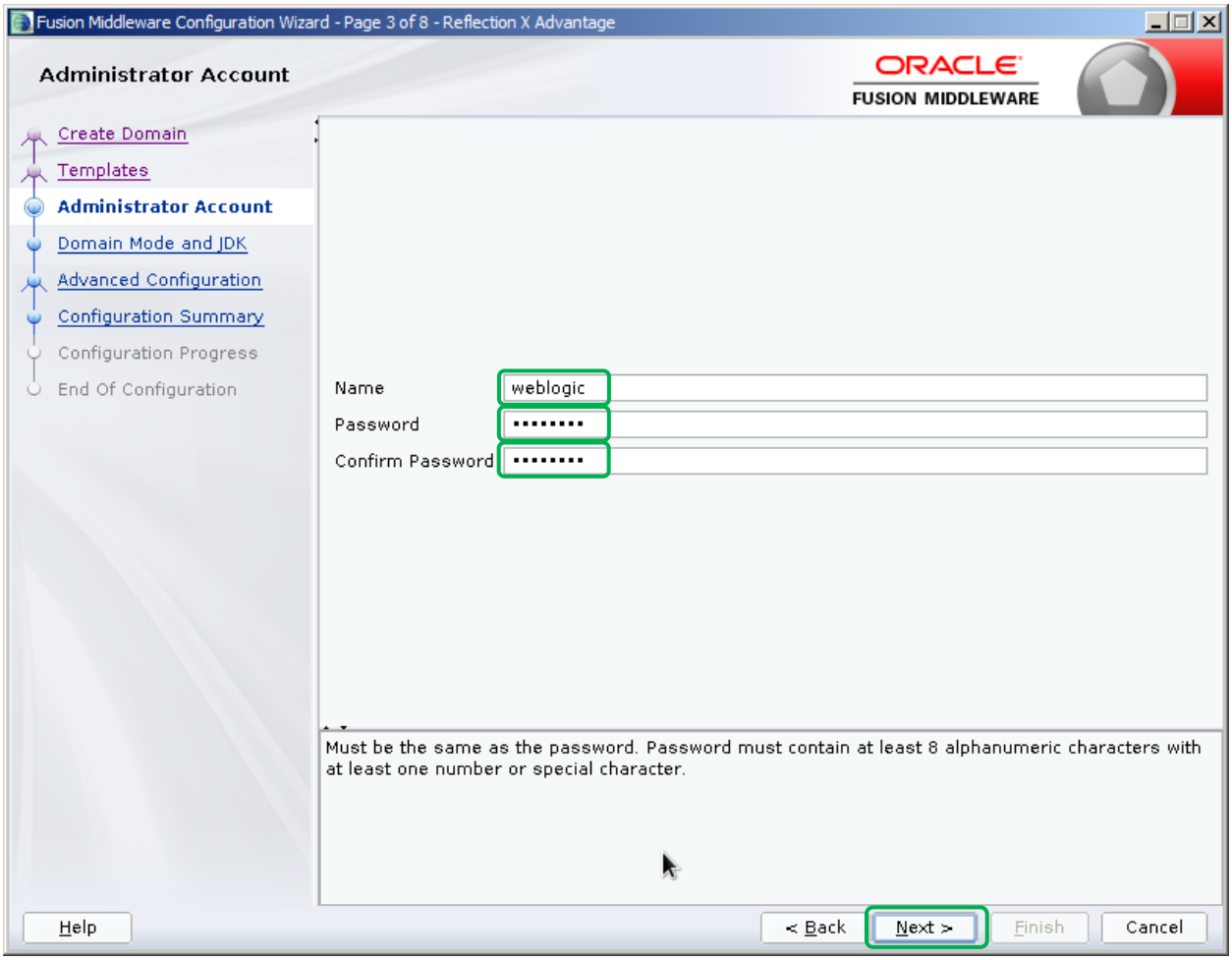
31. On the **Templates** screen, select the *Create Domain using Product Templates* radio button.
32. Under *Available Templates*, select "Basic WebLogic Server Domain".
33. Click **Next**.

Figure 14: Install WebLogic – Templates Screen



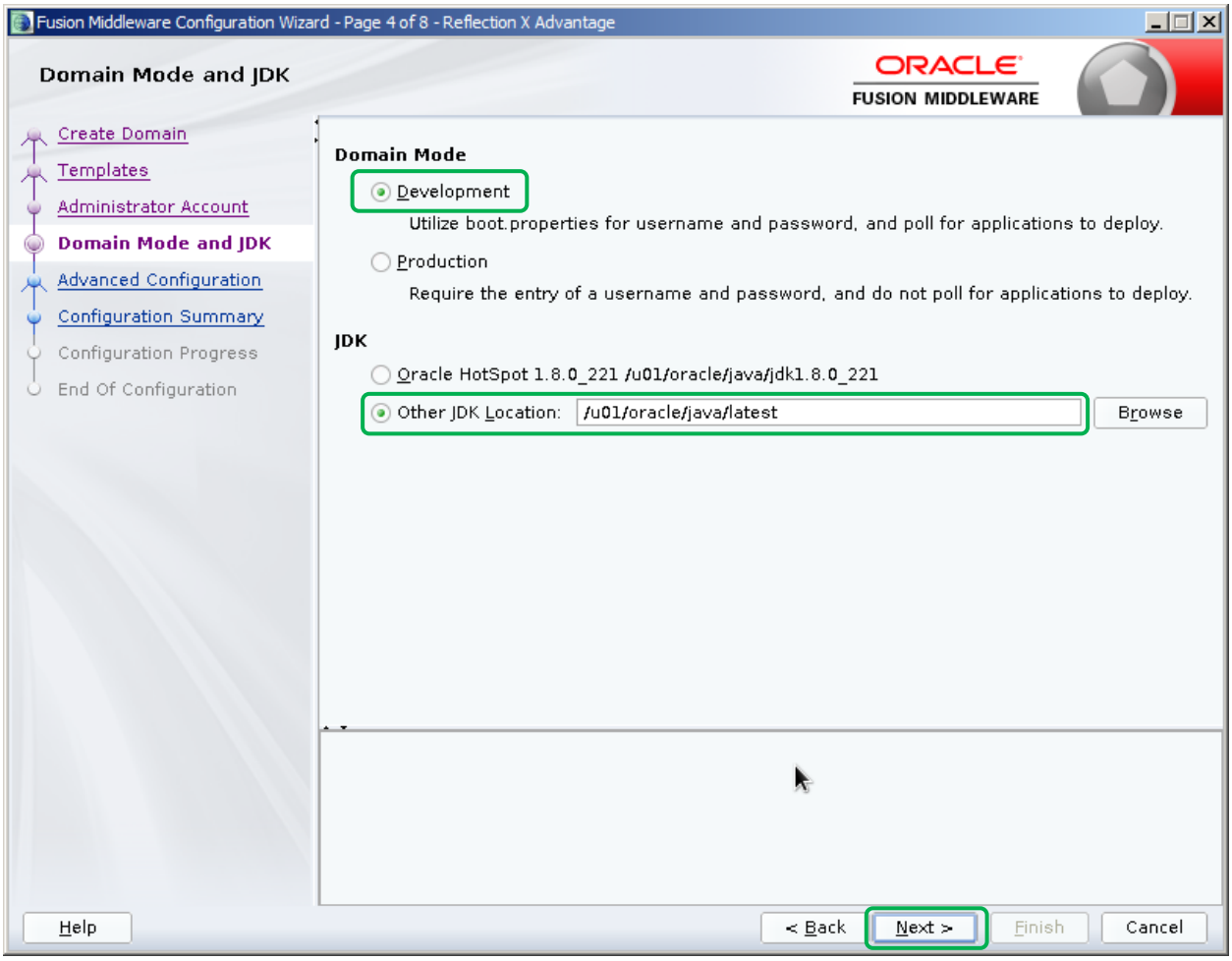
34. On the **Administrator Account** screen, enter *Name*: "weblogic"
35. Enter *Password*: "#########"
36. Enter *Confirm Password*: "#########"
37. Click **Next**.

Figure 15: Install WebLogic – Administrator Account Screen



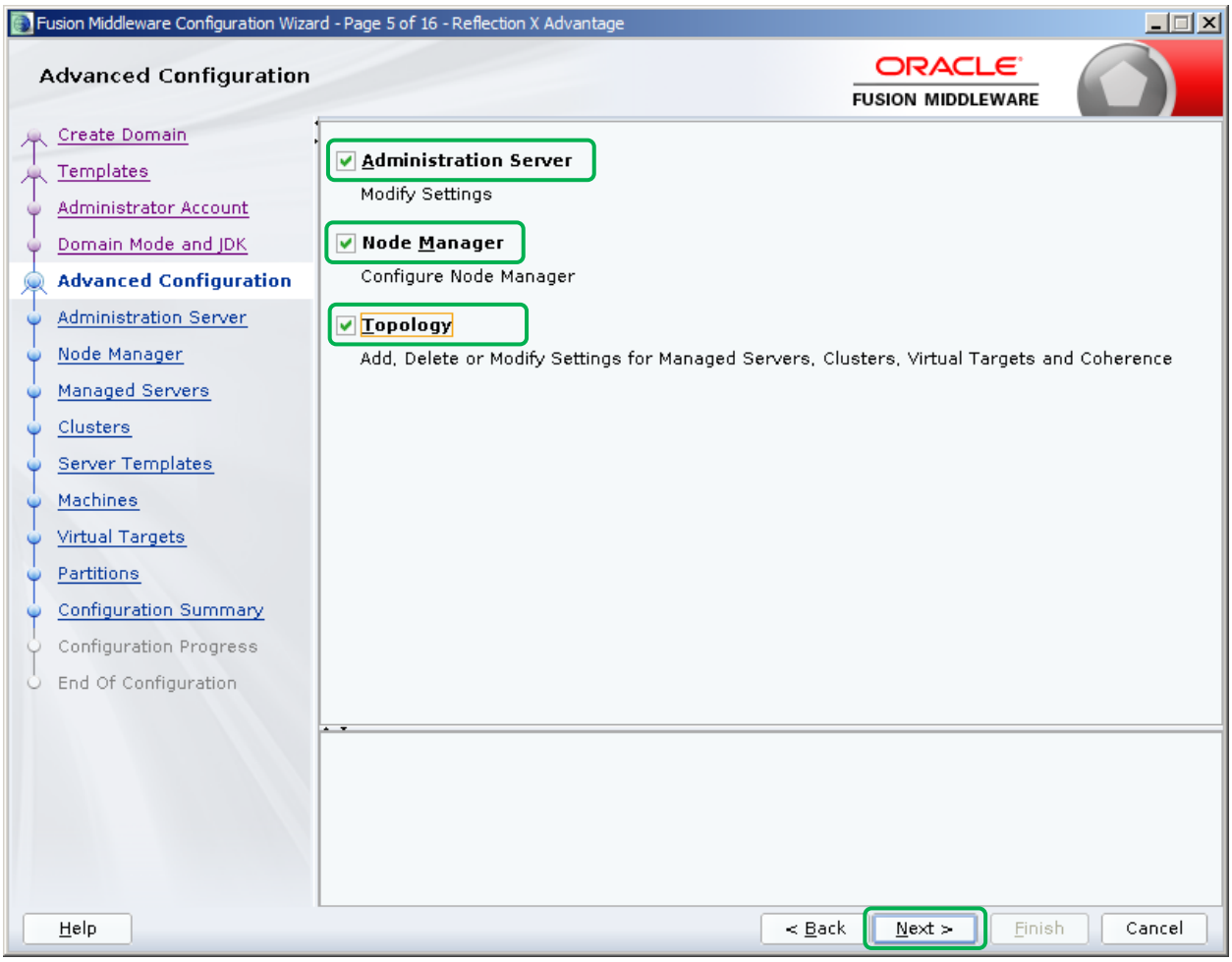
38. On the **Domain Mode and JDK** screen, select the *Development* radio button for the *Domain Mode*.
39. For *JDK*, select the *Other JDK Location* radio button, and specify ***{JAVA_HOME}***.
40. Click **Next**.

Figure 16: Install WebLogic - Domain Mode and JDK



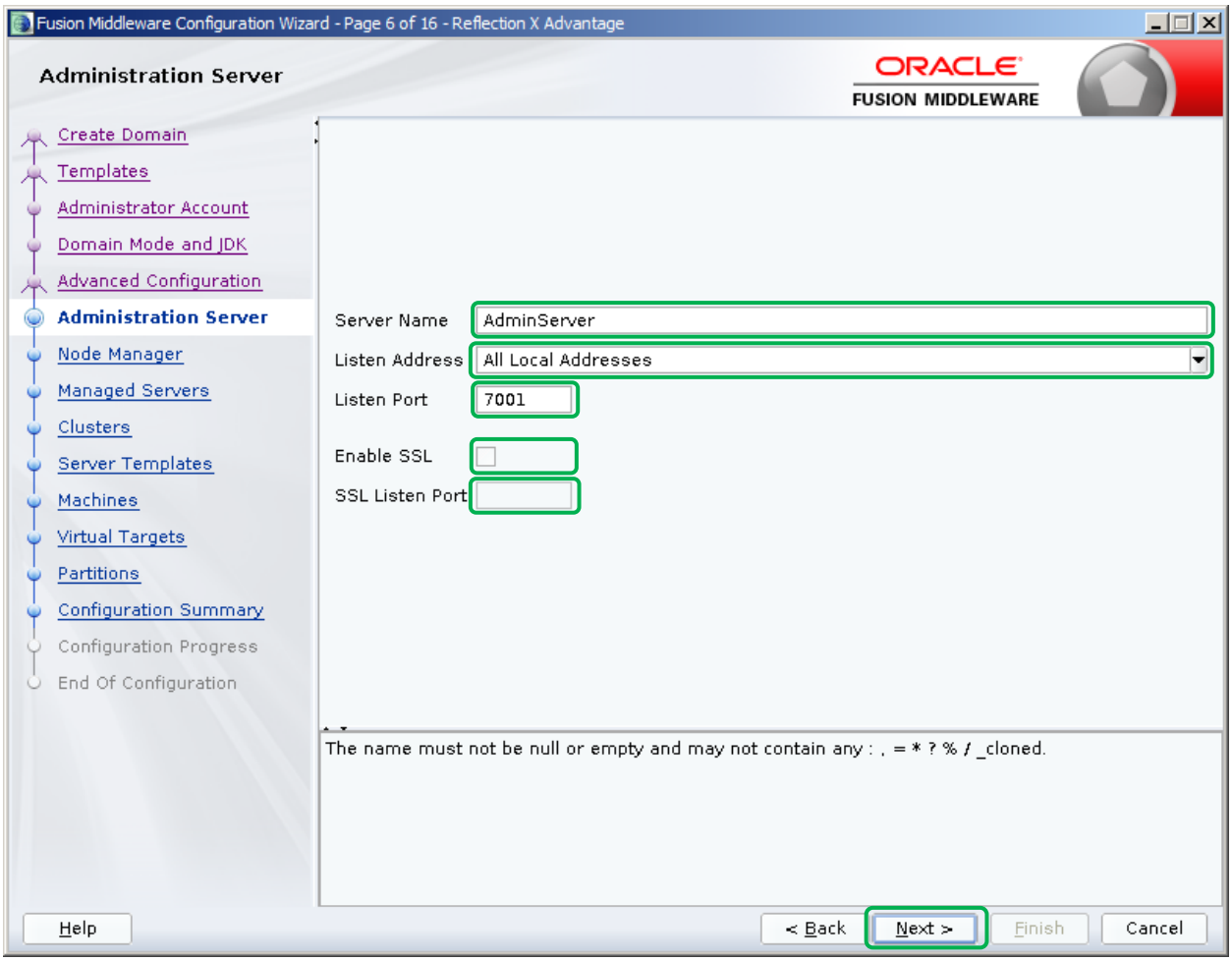
41. On the **Advanced Configuration** screen, check *Administration Server*, *Node Manager*, and *Managed Servers, Clusters and Coherence*.
42. Click **Next**.

Figure 17: Install WebLogic– Advanced Configuration



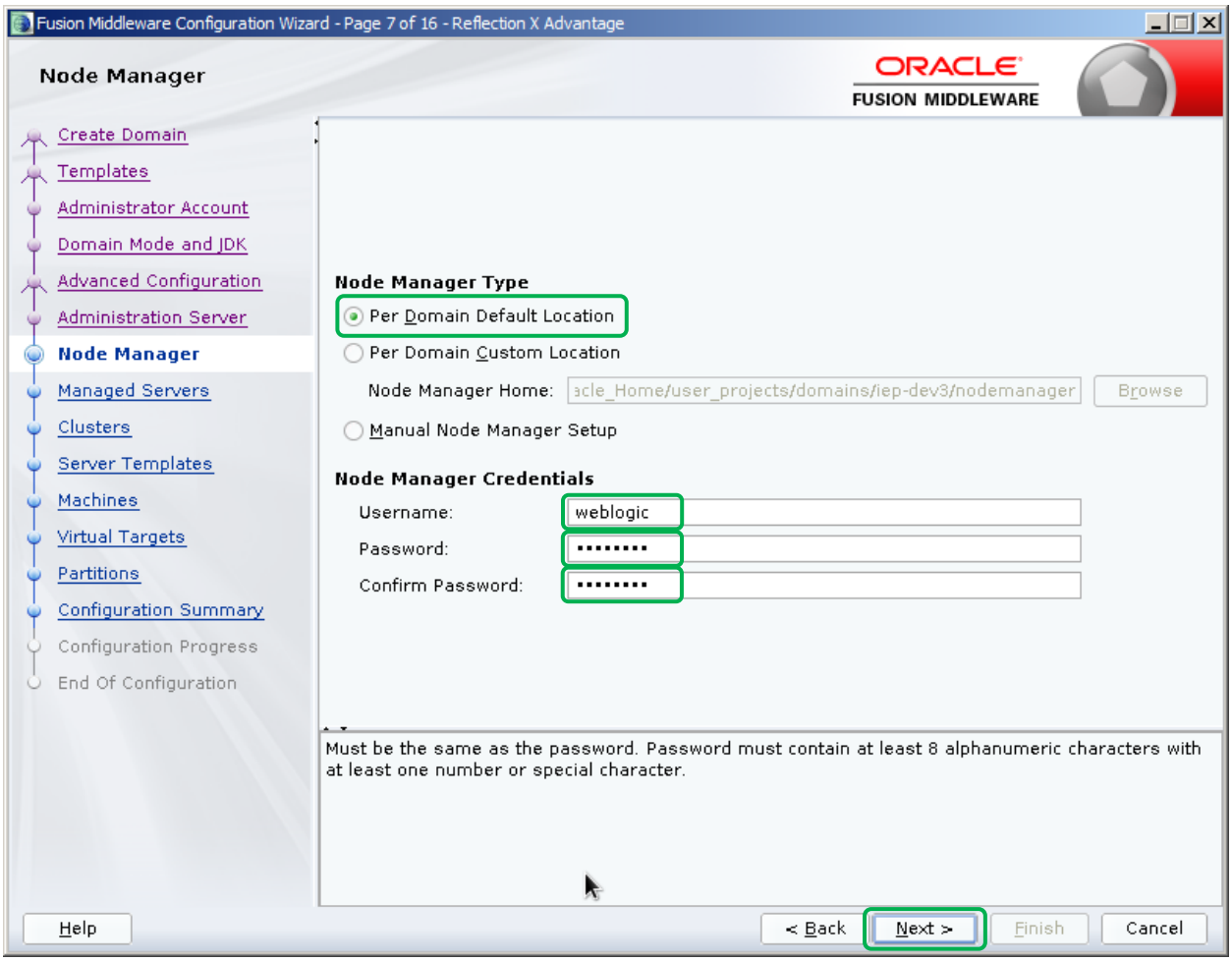
43. On the **Administration Server** screen, enter *Server Name*: "AdminServer"
44. Enter *Listen Address*: "All Local Addresses"
45. Enter *Listen Port*: "7001"
46. Uncheck the check box for *Enable SSL*.
47. Leave the *SSL Listen Port* field blank.
48. Click **Next**.

Figure 18: Install WebLogic – Administration Server Screen



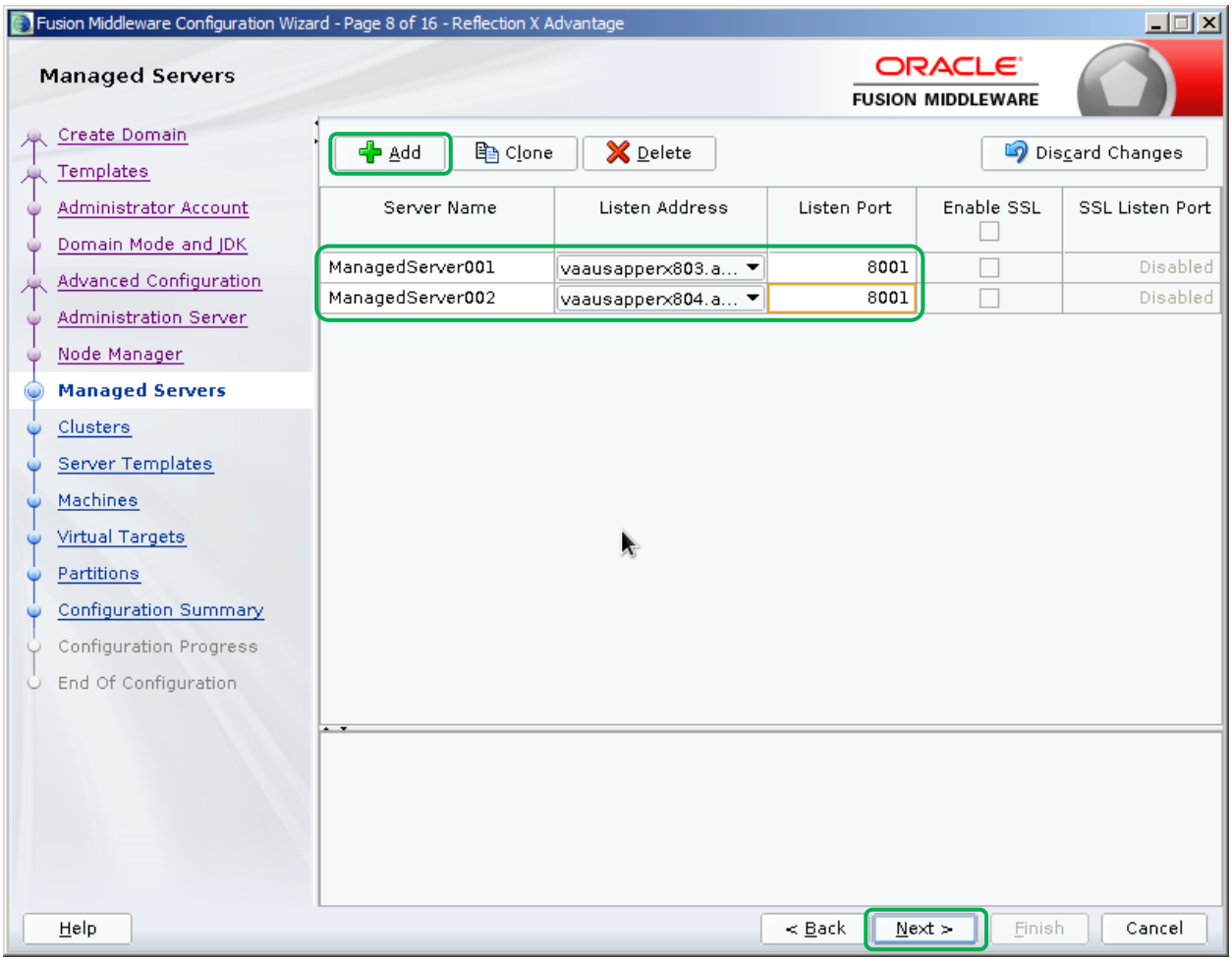
49. On the **Node Manager** screen, select the *Per Domain Default Location* radio button.
50. Enter *Username*: "weblogic"
51. Enter *Password*: "########"
52. Enter *Confirm Password*: "########"
53. Click **Next**.

Figure 19: Install WebLogic – Node Manager



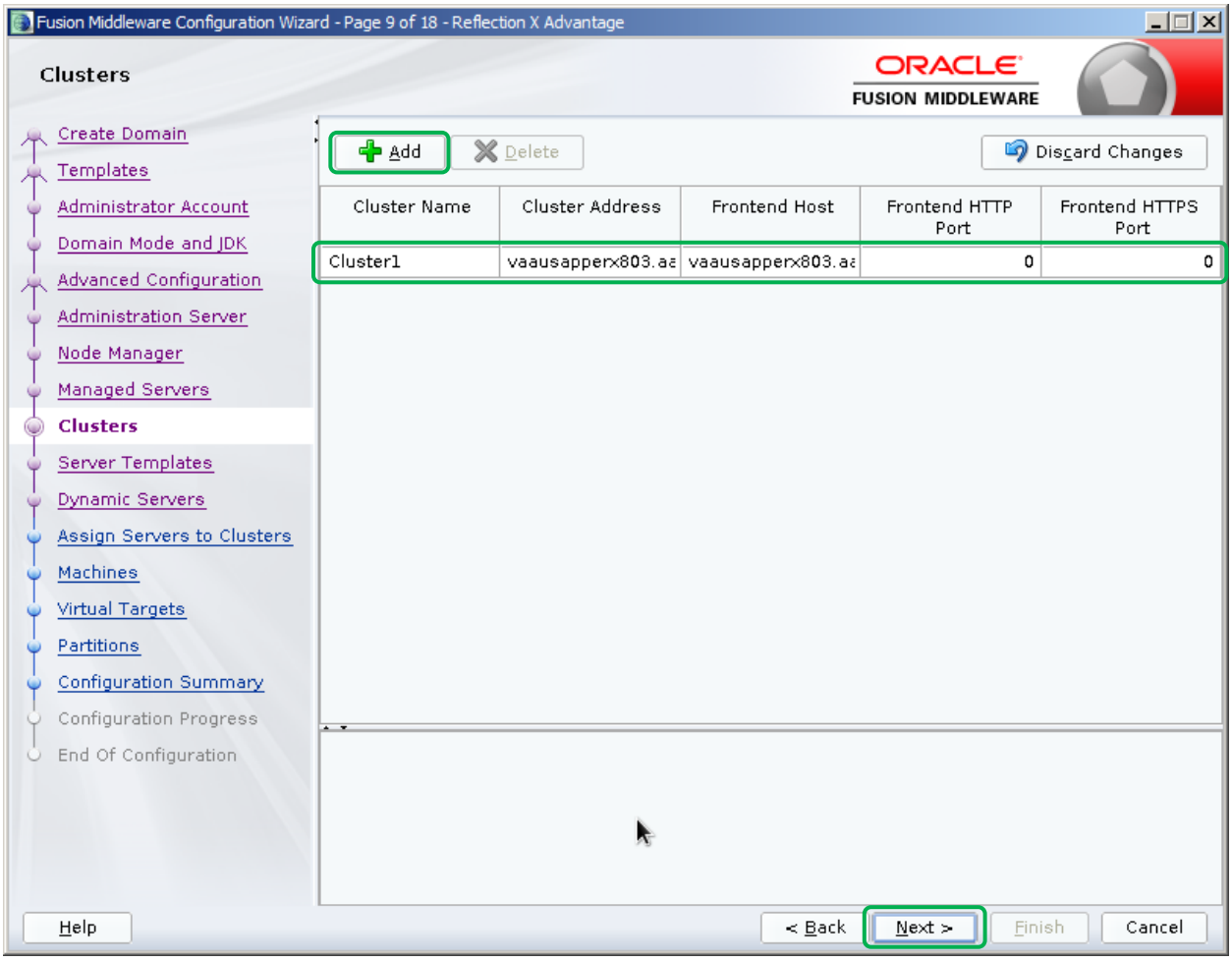
54. On the **Managed Servers** screen, click **Add**.
55. Enter the *Server Name*: ***[mserver1]***
56. Enter the *Listen Address*: ***[vm1_fqdn]***
57. Enter *Listen Port*: "8001"
58. Leave *Enable SSL* unchecked.
59. Leave *SSL Listen Port* empty (Disabled).
60. Click **Add**.
61. Enter *Server Name*: ***[mserver2]***
62. Enter *Listen Address*: ***[vm2_fqdn]***
63. Enter Listen Port: "8001"
64. Leave *Enable SSL* unchecked.
65. Leave *SSL Listen Port* empty (Disabled).
66. Click **Next**.

Figure 20: Install WebLogic – Managed Servers

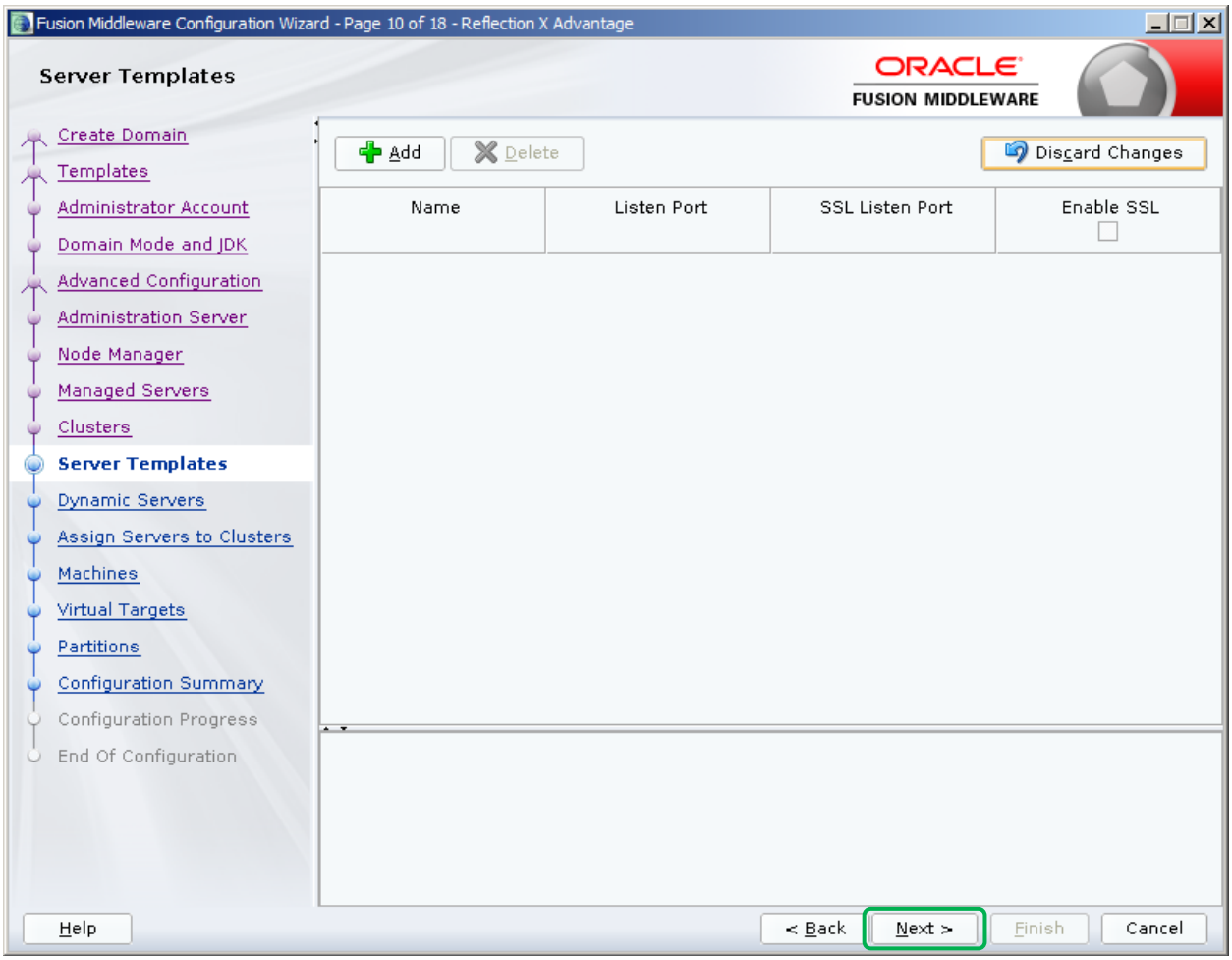


67. On the **Clusters** screen, click **Add**.
68. Enter *Cluster Name*: "***[cluster]***"
69. Enter *Cluster Address*: "***[vm1_fqdn]***:***[erx_port]***,***[vm2_fqdn***]:***[erx_port]***"
70. Enter *Frontend Host*: "***[proxy_fqdn]***"
71. Enter *Frontend HTTP Port*: "80"
72. Enter *Frontend HTTPS*: "443"
73. Click **Next**.

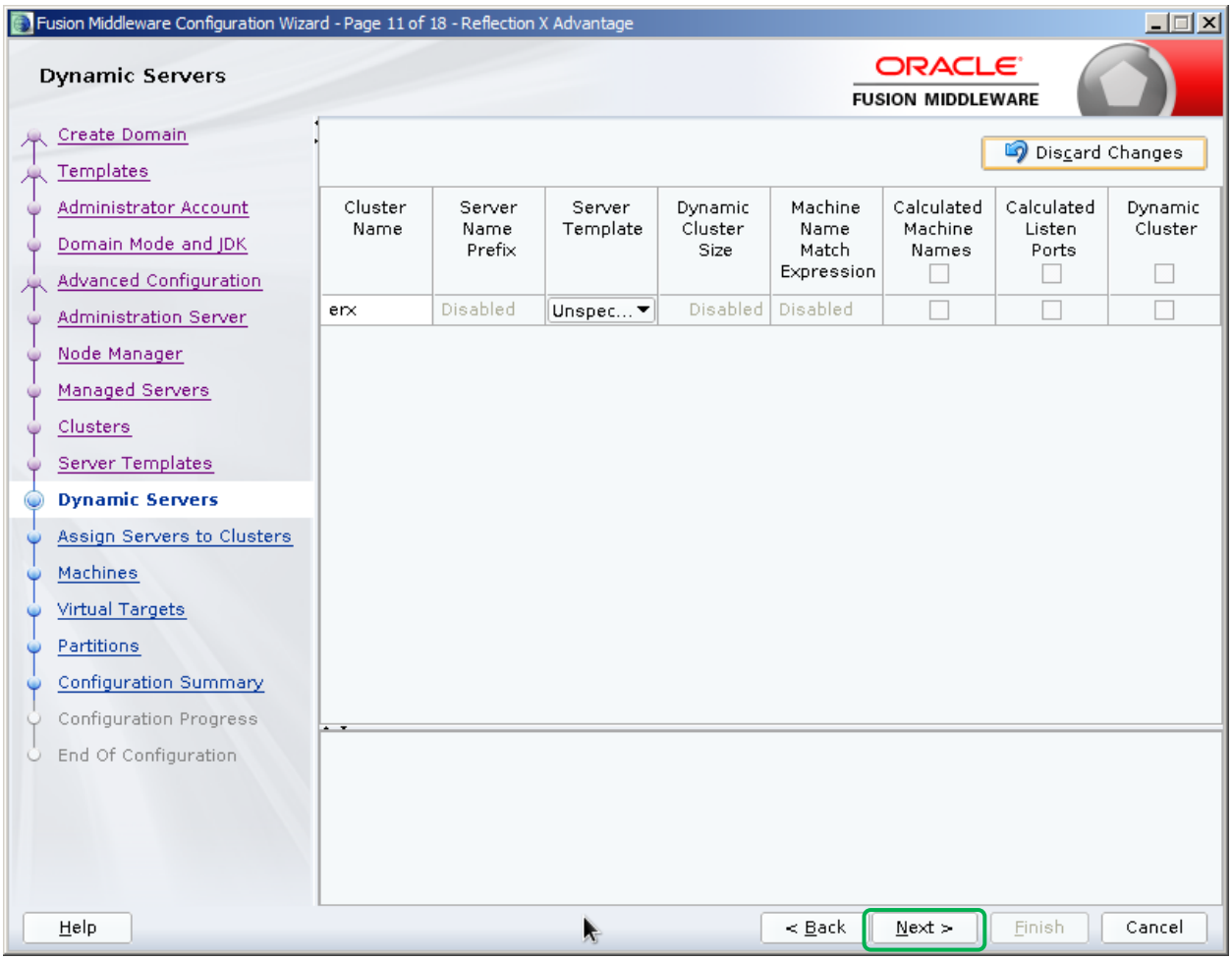
Figure 21: Install WebLogic – Clusters



74. Click **Next**.

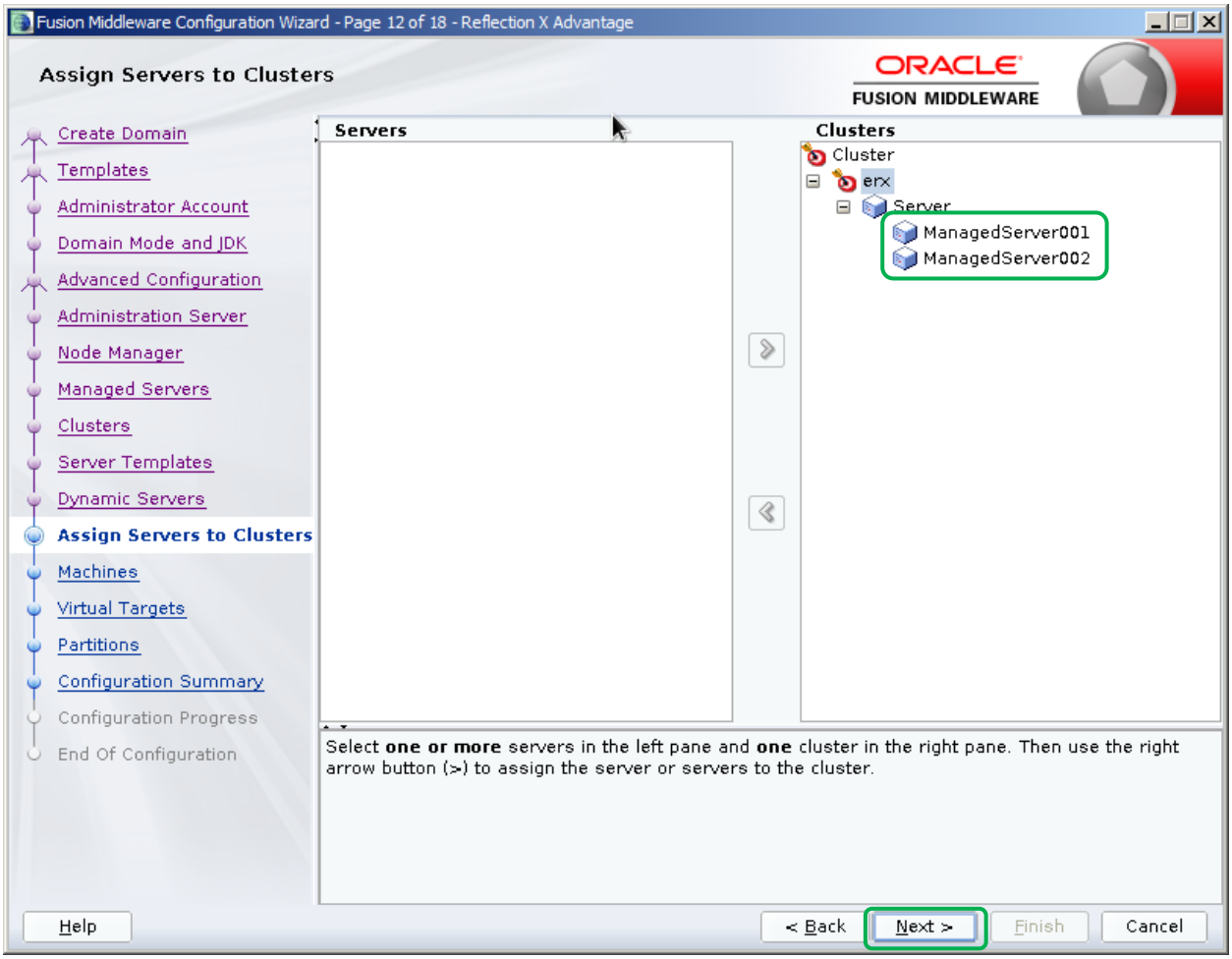


75. Click **Next**.



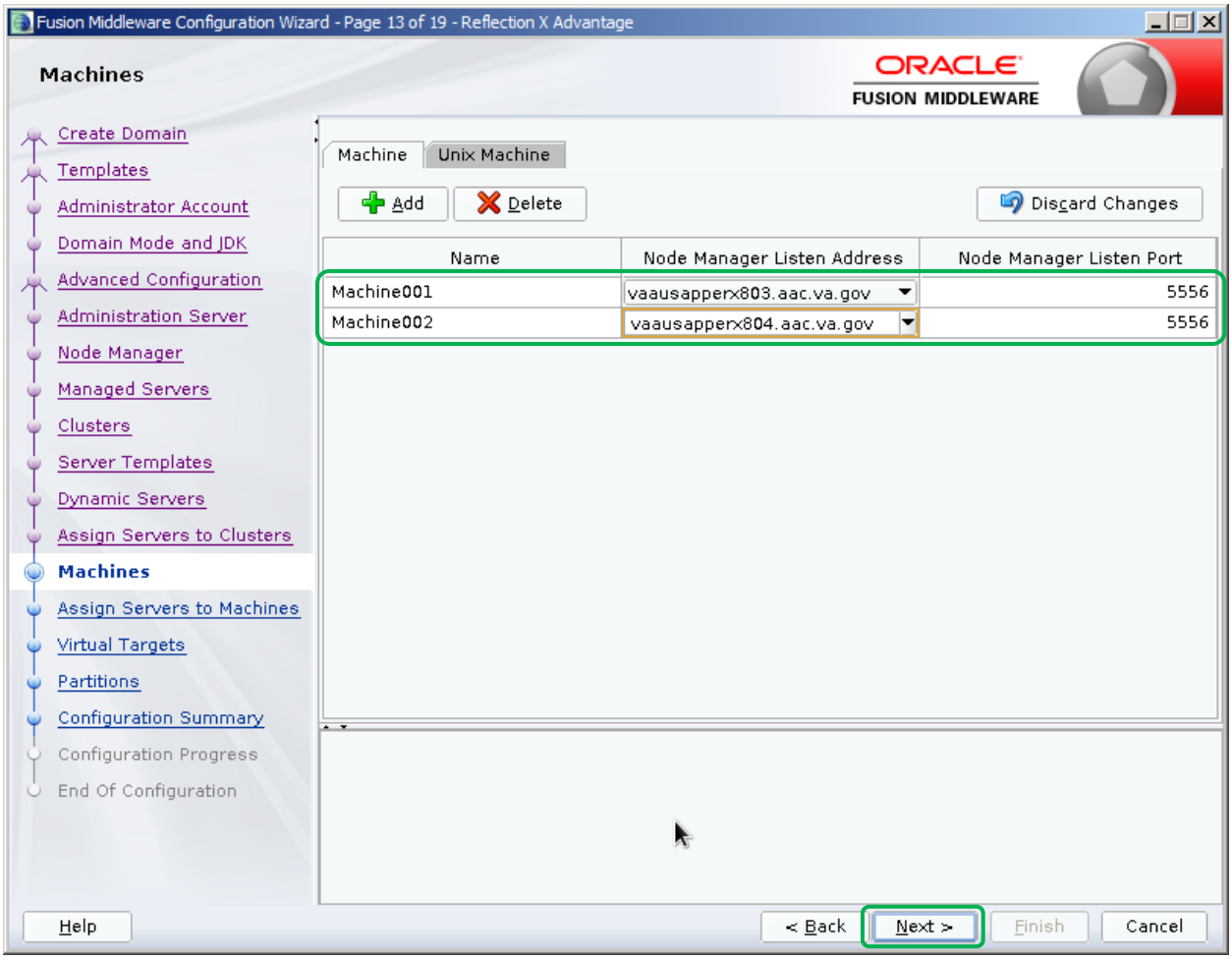
76. Assign ***[mserver1]*** and ***[mserver2]*** managed servers to the ***[cluster]*** cluster.
77. Click **Next**.

Figure 22: Install WebLogic – Assign Servers to Clusters



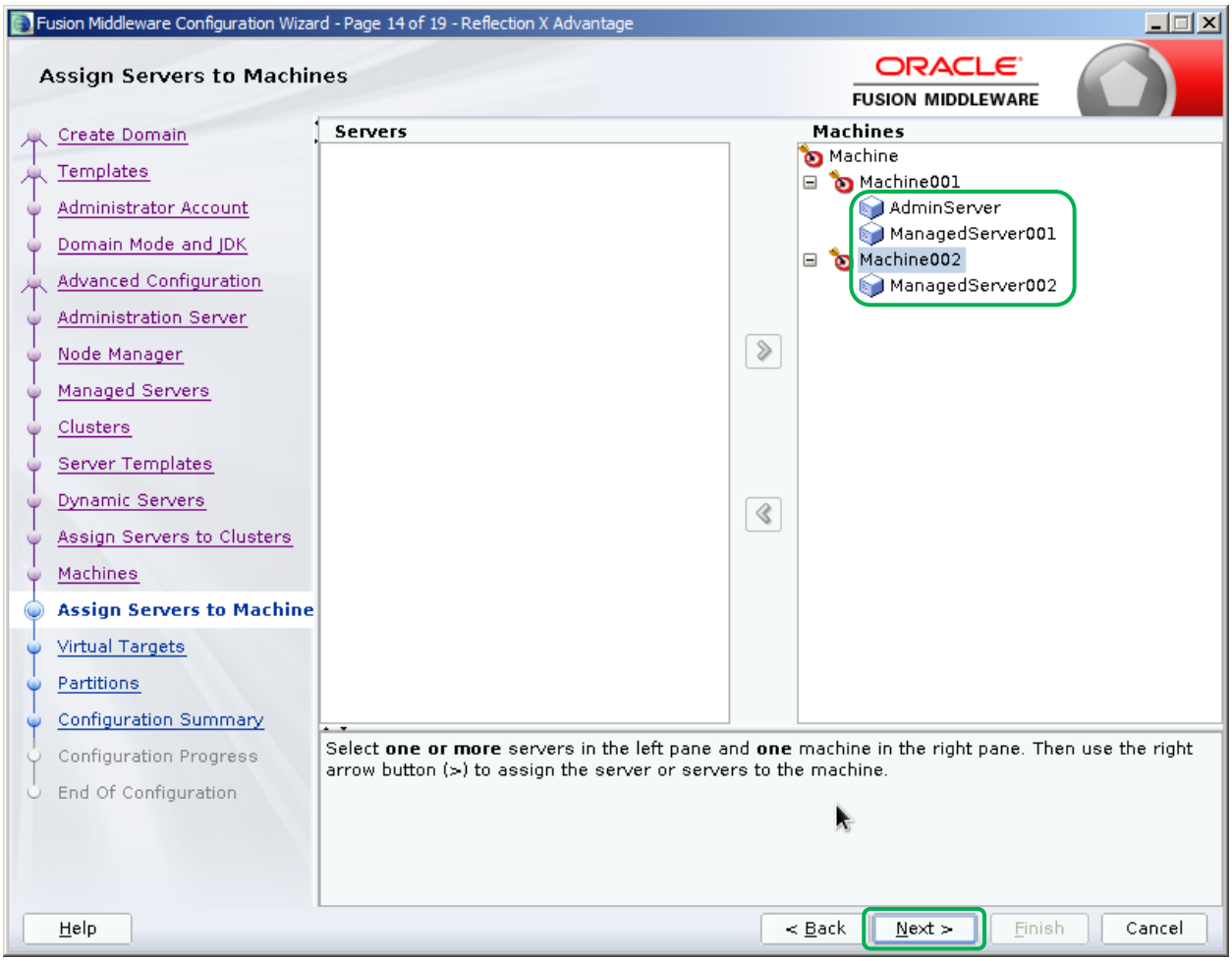
78. Click **Add**.
79. Enter *Name*: "***[machine1]***"
80. Enter *Node Manager Listen Address*: "***[vm1_fqdn]***"
81. Enter *Node Manager Listen Port*: "5556"
82. Enter *Name*: "***[machine2]***"
83. Enter *Node Manager Listen Address*: "***[vm2_fqdn]***"
84. Enter *Node Manager Listen Port*: "5556"
85. Click **Next**.

Figure 23: Install WebLogic – Machines

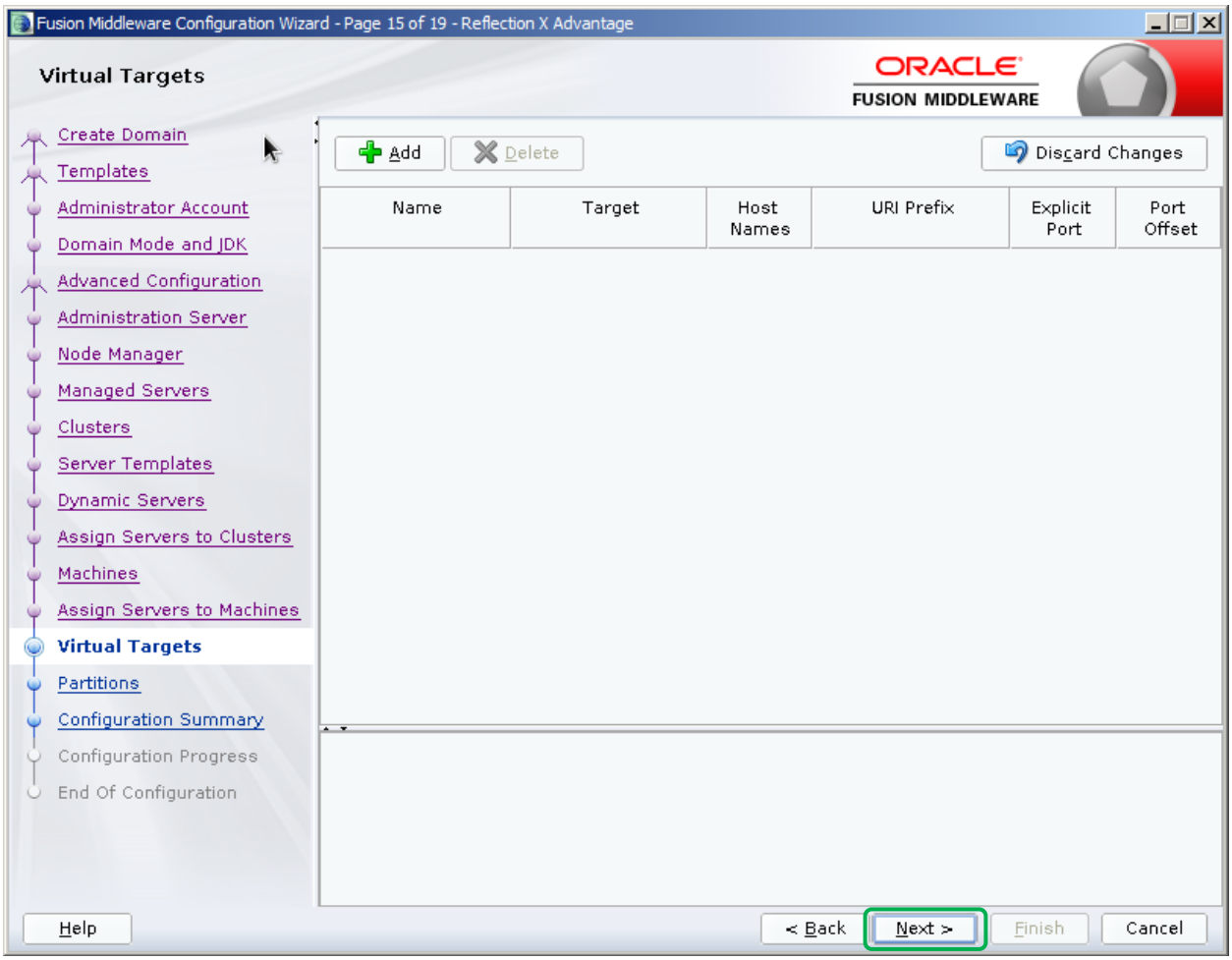


86. On the **Assign Servers to Machines** screen, add "AdminServer" on *Servers* panel to "***[machine1]***" on *Machines* panel.
87. Add "***[mserver1]***" on *Servers* panel to "***[machine1]***" on *Machines* panel.
88. Add "***[mserver2]***" on *Servers* panel to "***[machine2]***" on *Machines* panel.
89. Click **Next**.

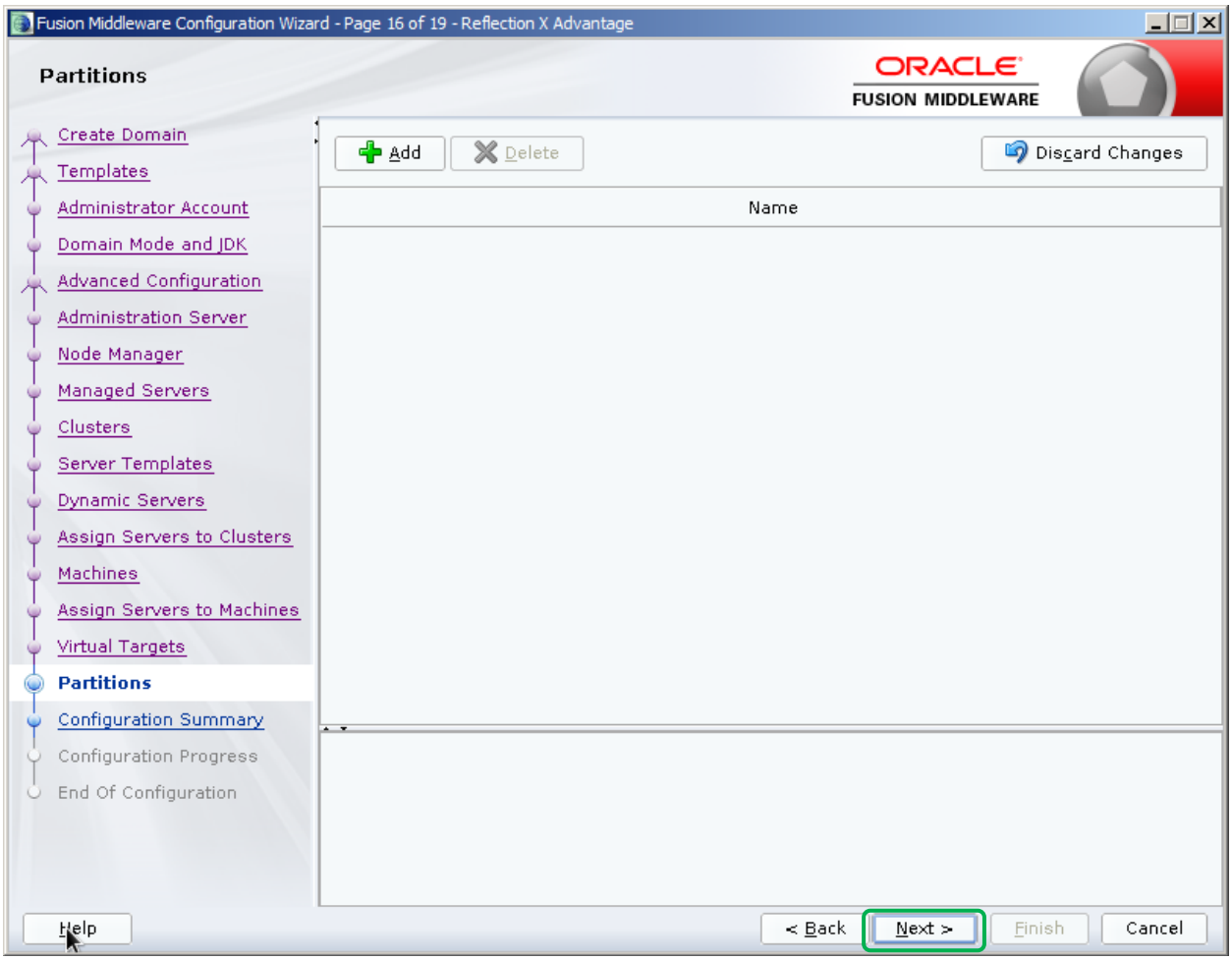
Figure 24: Install WebLogic – Assign Servers to Machines



90. Click **Next**.

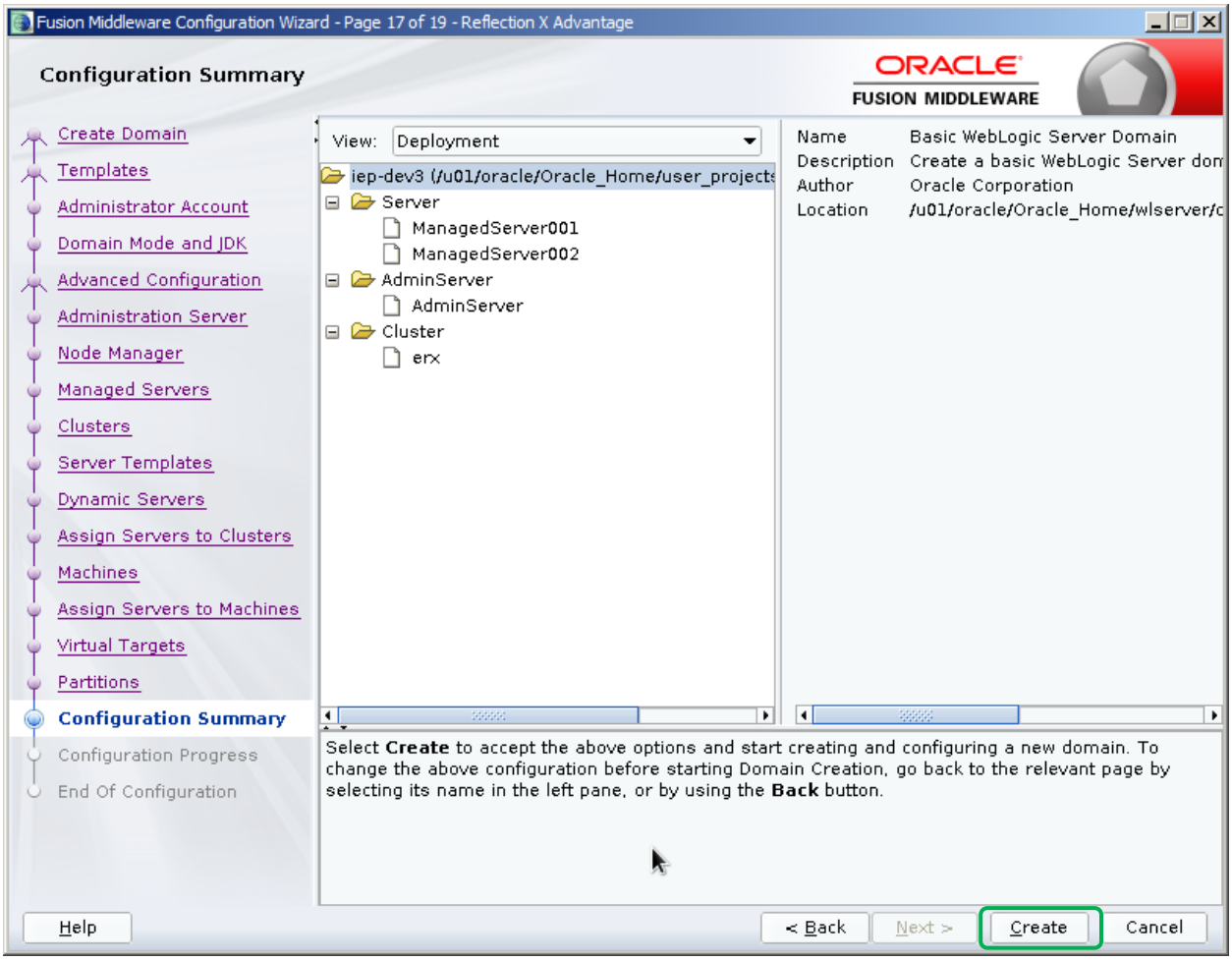


91. Click **Next**.



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

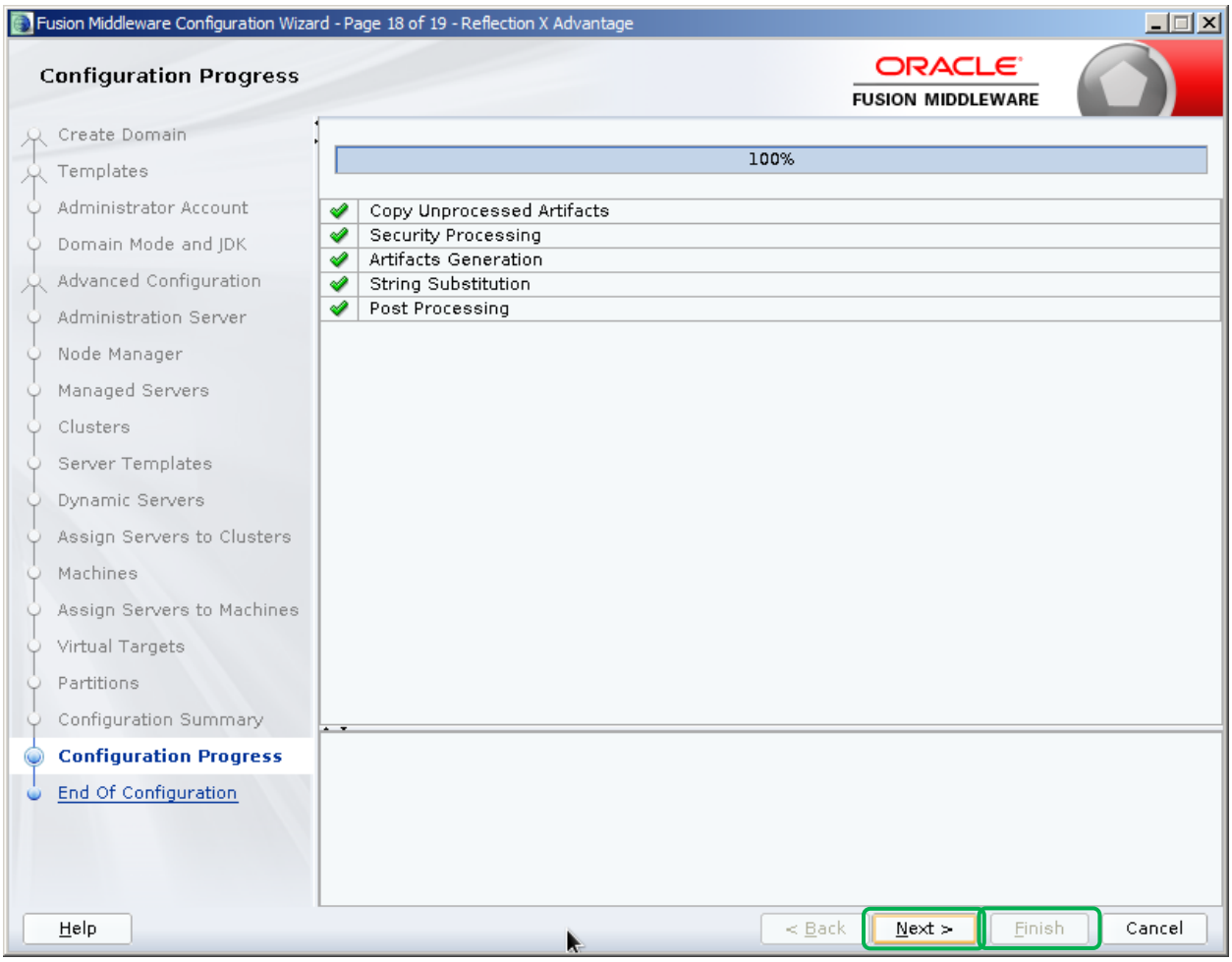
Figure 25: Install WebLogic – Configuration Summary Screen



93. Once the configuration is complete, click **Next**.

94. If the configuration is successful, the **Configuration Success** screen will display as illustrated in the figure below.
95. Click **Finish**.

Figure 26: Install WebLogic - Configuration Success



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

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

97. 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="${SAVE_JAVA_OPTIONS}"
JAVA_OPTIONS="${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.ls -

4.8.1.9 Disable basic authentication on VM1

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

```
$ cd $DOMAIN_HOME/config/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.jar"
export PRE_CLASSPATH
```

Enter :wq to save the file and exit vi.

4.8.1.11 Create Startup/Shutdown Scripts on VM1

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

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

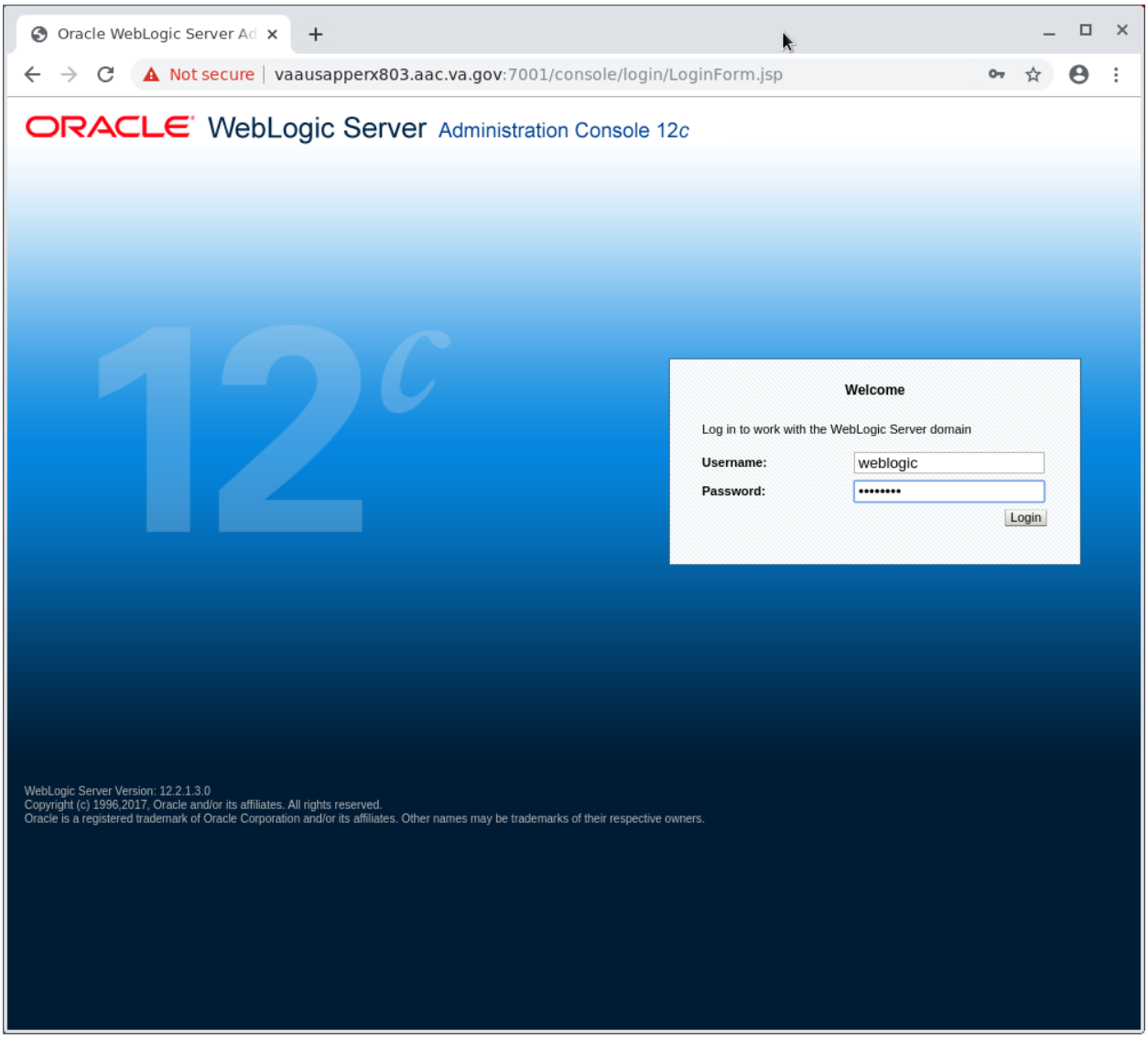
4.8.1.12 Start up Weblogic Admin Console on VM1

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

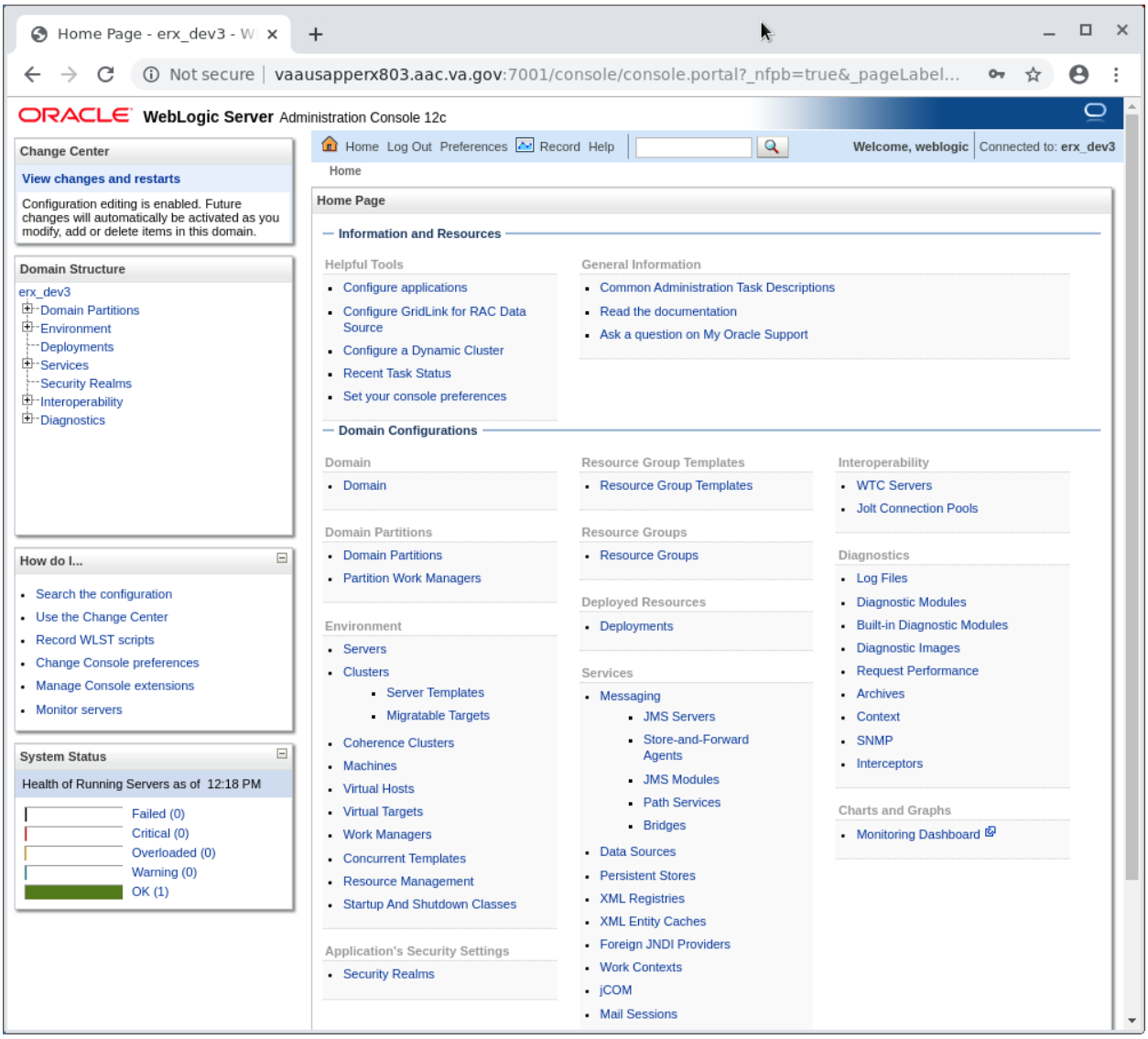
1. As your normal Linux login account, dzdo su to the weblogic account:
   ```
   $ dzdo su - weblogic
   ```
2. On VM1, start node manager:
   ```
   $ ./startNodemanager_[domain].sh
   ```
3. On VM1, start AdminServer:
   ```
   $ ./startWebLogic_[domain].sh
   ```

4.8.1.13 Log into Weblogic Admin Console on VM1

1. Start a Web Browser from the Linux command prompt:
   ```
   $ /opt/google/chrome/chrome --window-size=1000,900 &
   ```
2. Access the non-secure Weblogic Admin Console URL:
   ```
   http://[vm1_fqdn]:7001/console/ > DEV3: http://vaausapperx803.aac.va.gov:7001/console/
   ```
3. Log into the Weblogic console with the Weblogic admin username and password:



4. The WebLogic Admin Console Home Page :

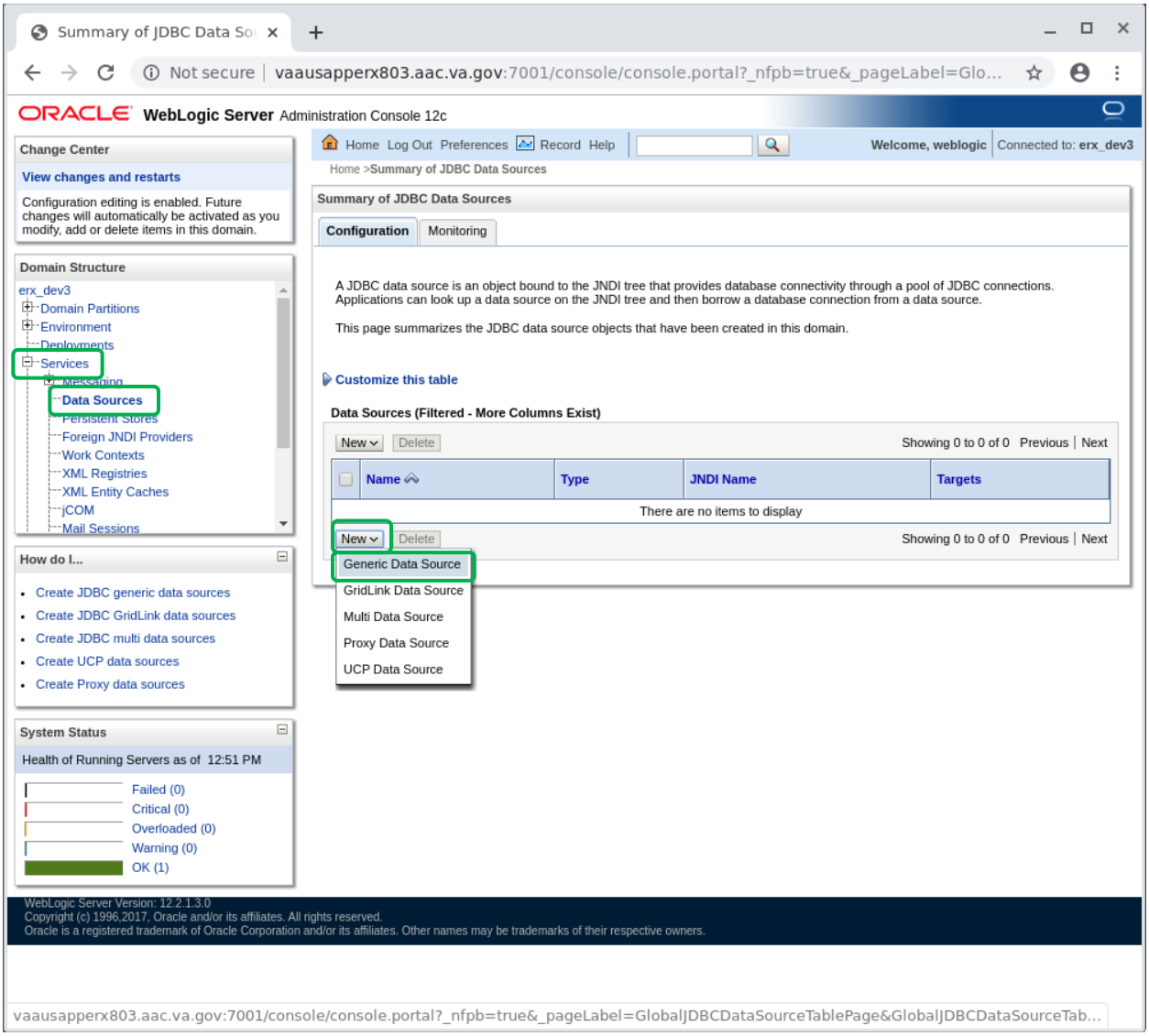


4.8.1.14 Create Inbound eRx Datasource

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

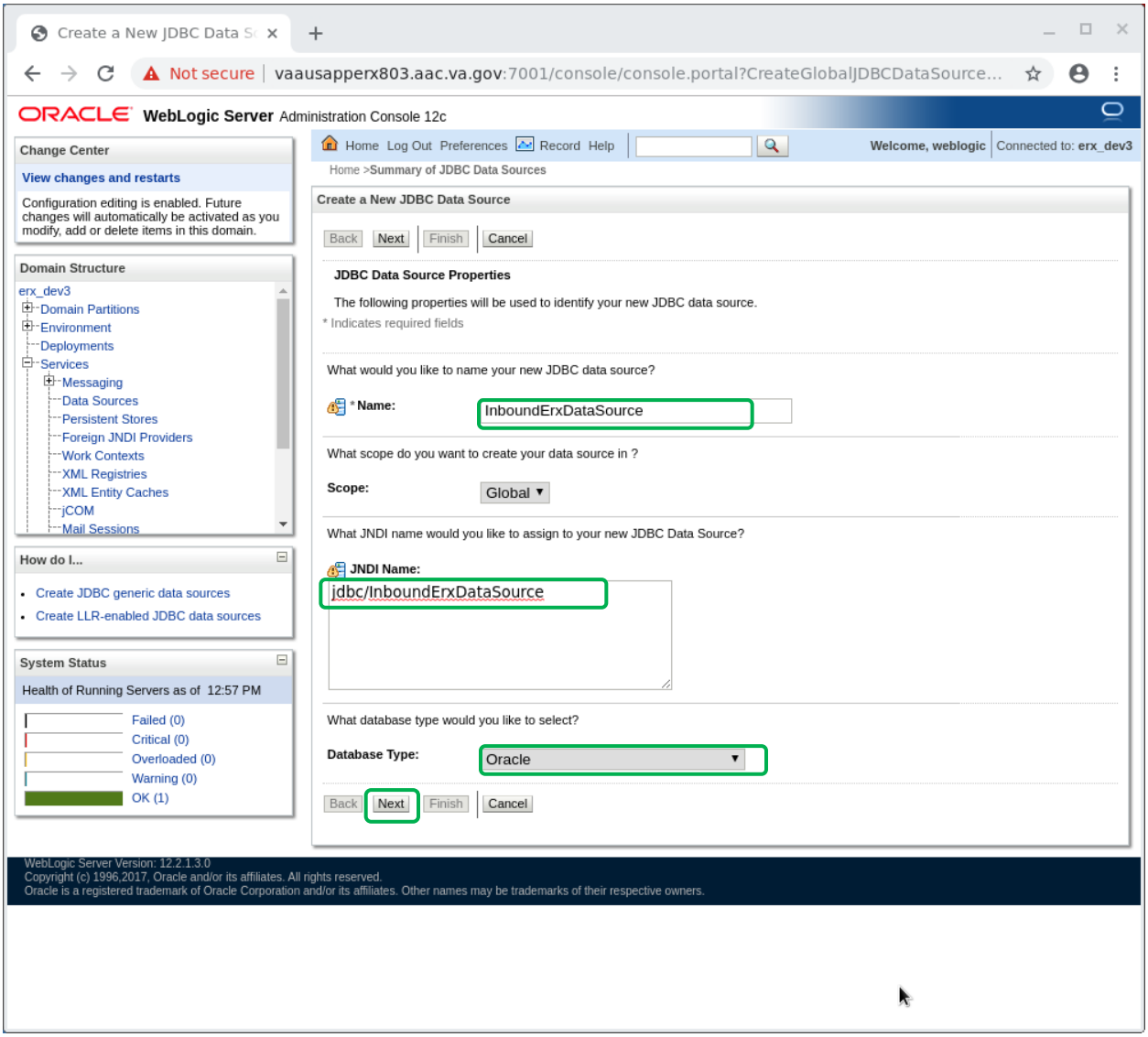
1. Navigate to *Services* > *Data Sources*.
2. From the *Data Sources* page, click **New**.

Figure 27: Create Inbound eRx Datasource – Datasources



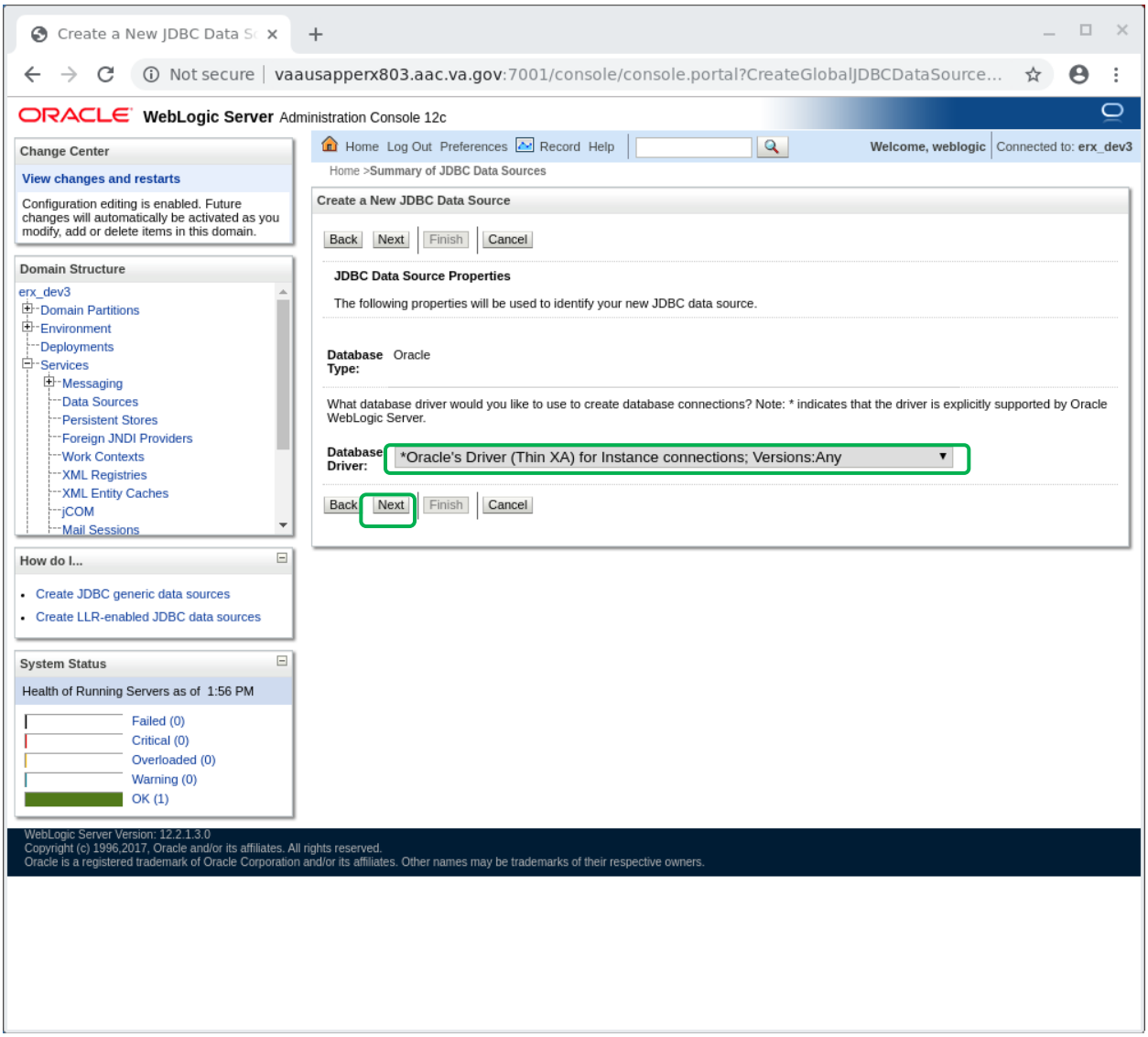
3. Enter *Name*: “InboundErxDataSource”
4. Enter *JNDI Name*: “jdbc/InboundErxDataSource”
5. Select *Database Type*: “Oracle”
6. Click **Next**.

Figure 28: Create Inbound eRx Datasource – Datasource Properties



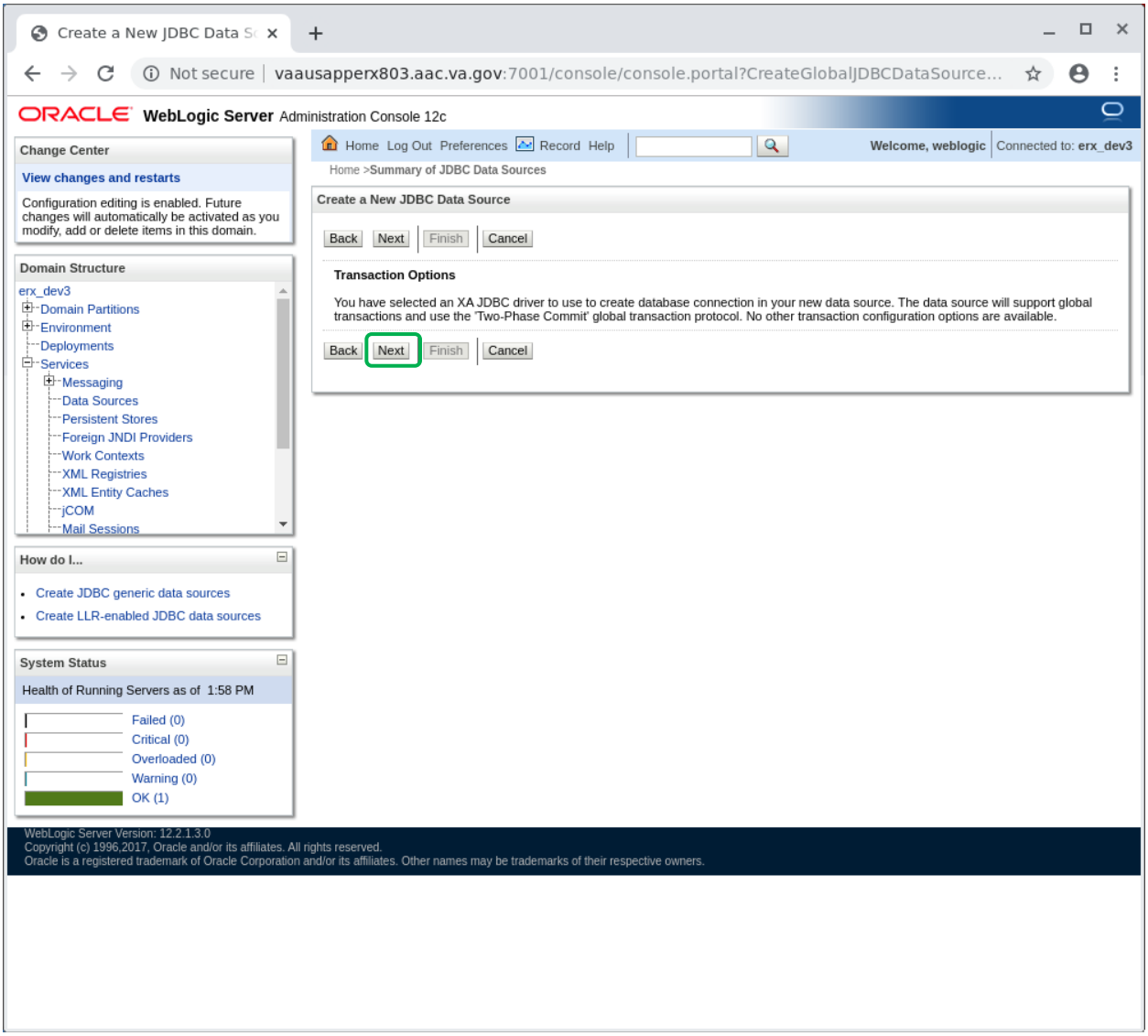
7. Select *Database Driver*: "Oracle's Driver (Thin XA) for Instance connections; Versions: Any"
8. Click Next.

Figure 29: Create Inbound eRx Datasource – Database Driver



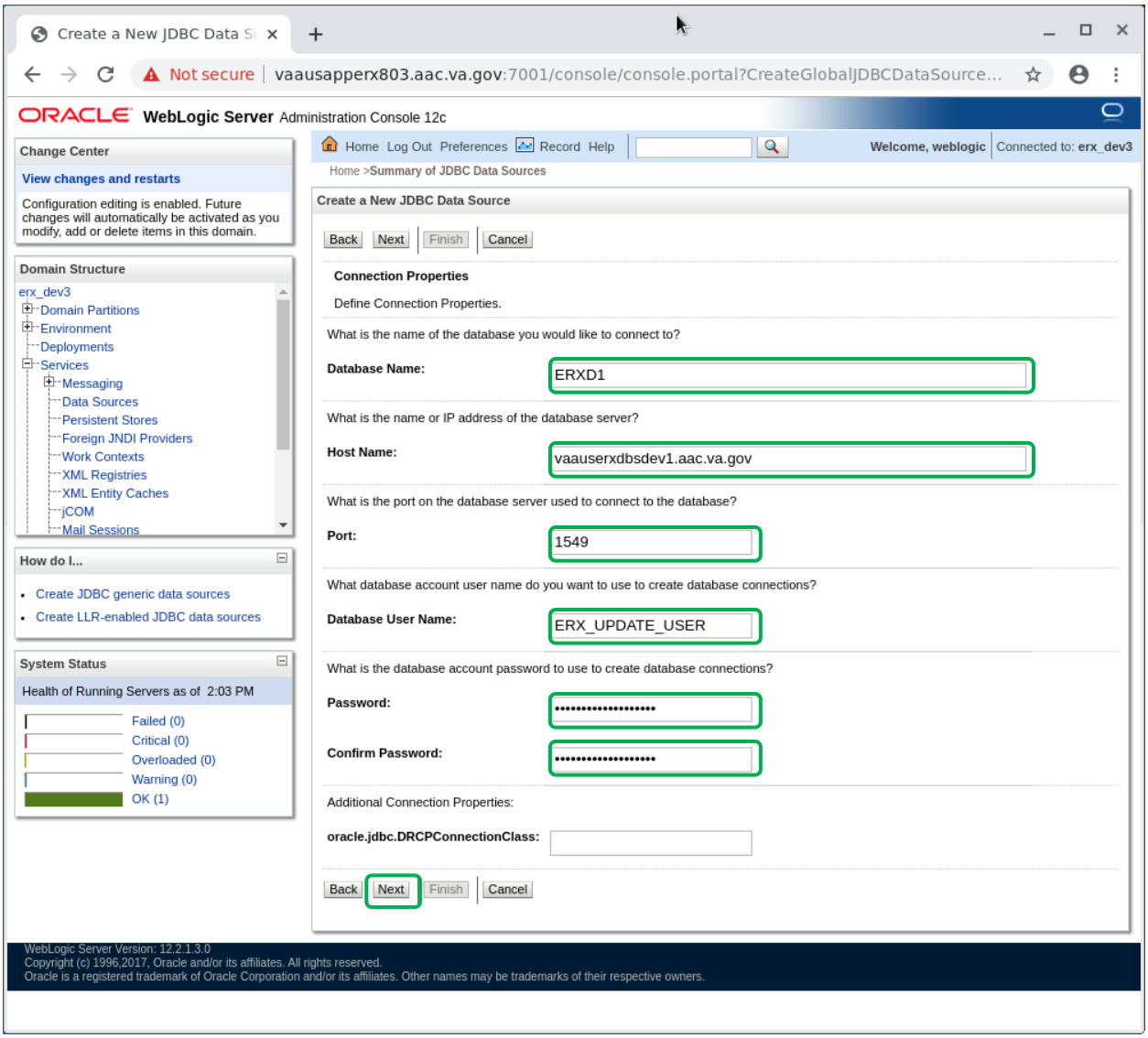
9. Click **Next**.

Figure 30: Create Inbound eRx Datasource – Transaction Properties



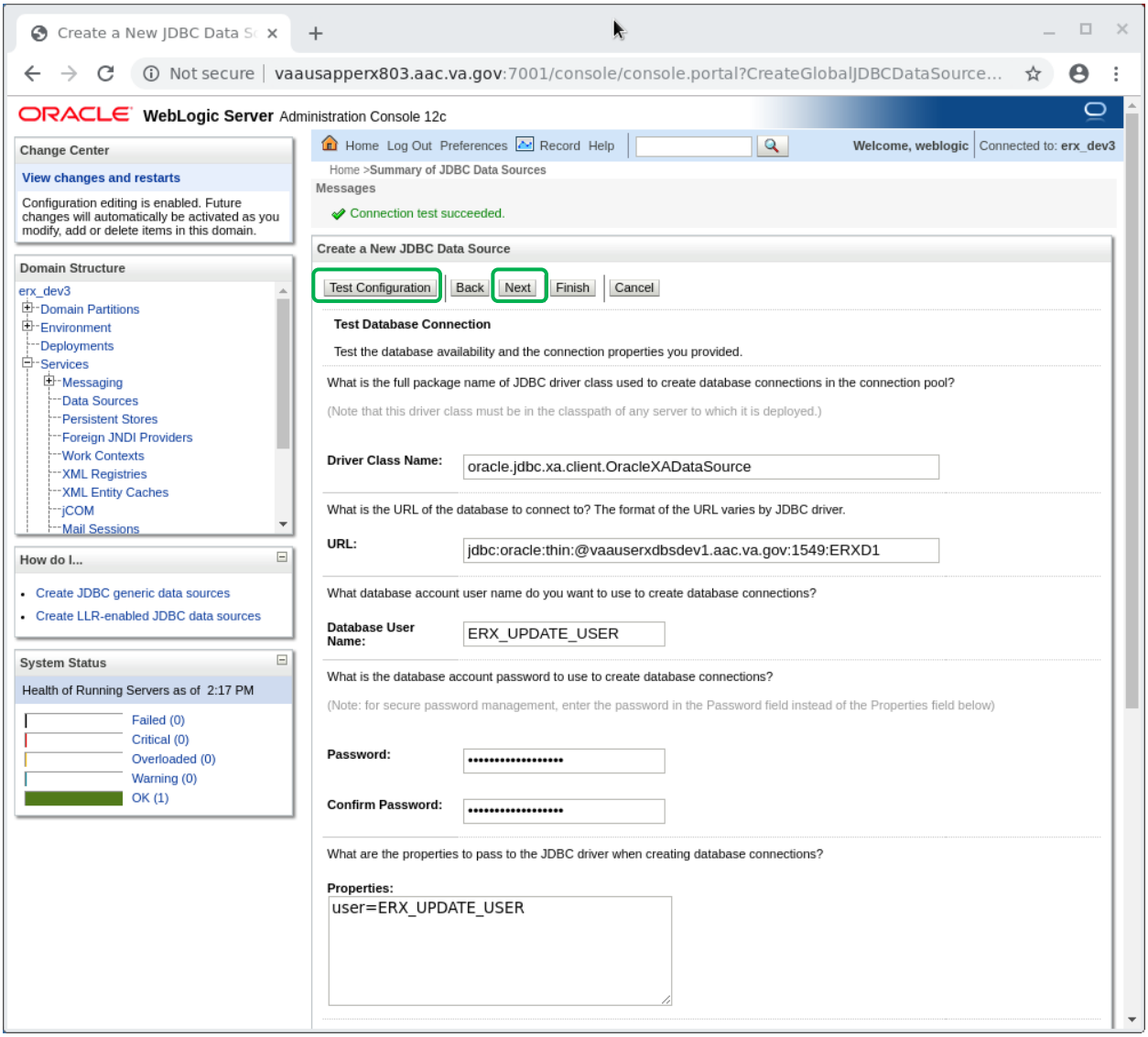
10. Enter *Database Name*: "***[DB_NAME]***"
11. Enter *Host Name*: "***[DB_FQDN]***"
12. Enter *JNDI Name*: "jdbc/InboundErxDataSource"
13. Enter *Port*: "***[DB_PORT]***"
14. Enter *Password*: "***[DB_PASSWORD]***"
15. Enter *Confirm Password*: "***[DB_PASSWORD]***"

Figure 31: Create Inbound eRx Datasource – Connection Properties



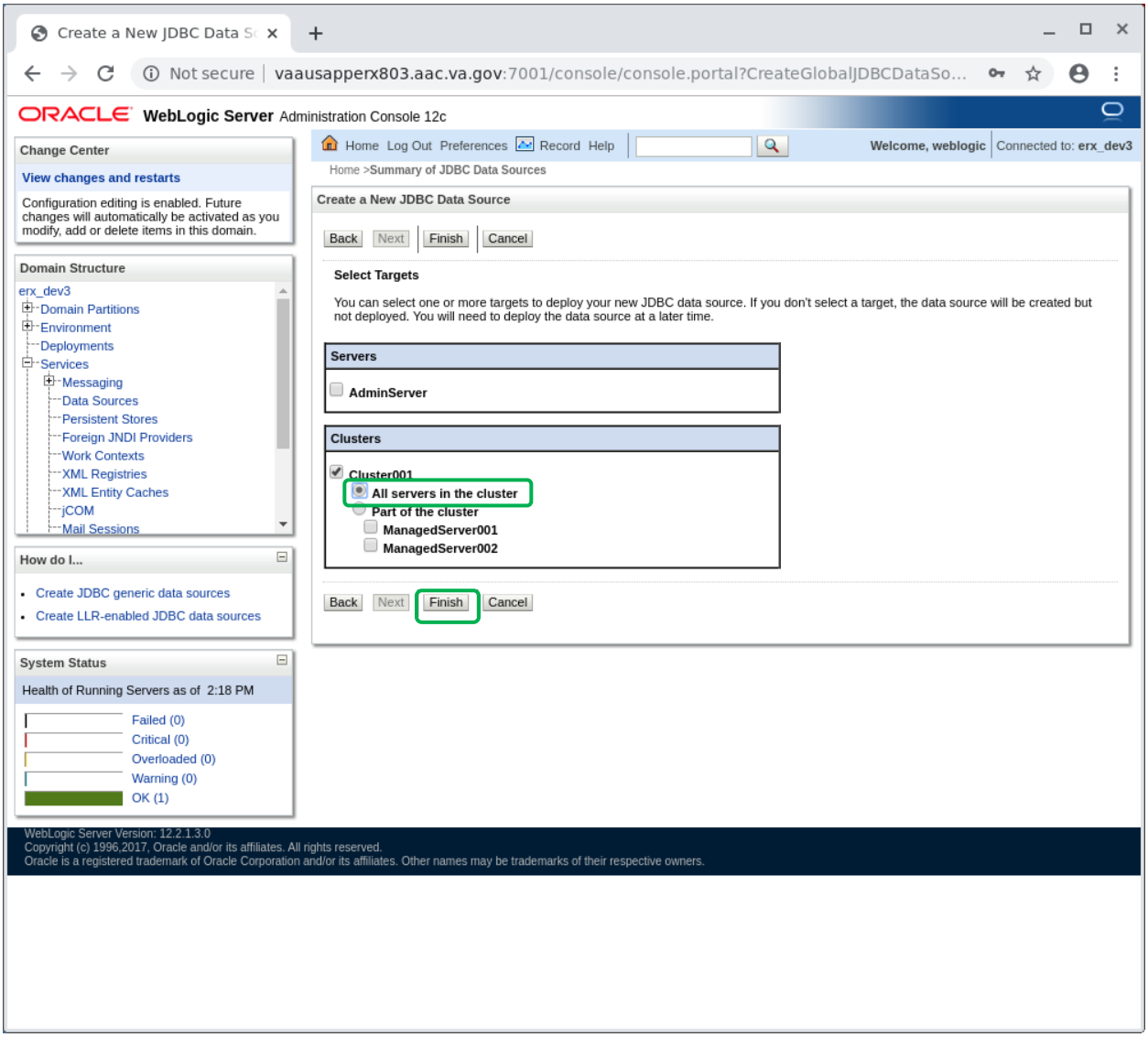
16. Click the “Test Configuration” button
17. If test is not successful, Click “Back” button and correct settings, otherwise click “Next”

Figure 32: Create Inbound eRx Datasource – Test Connection



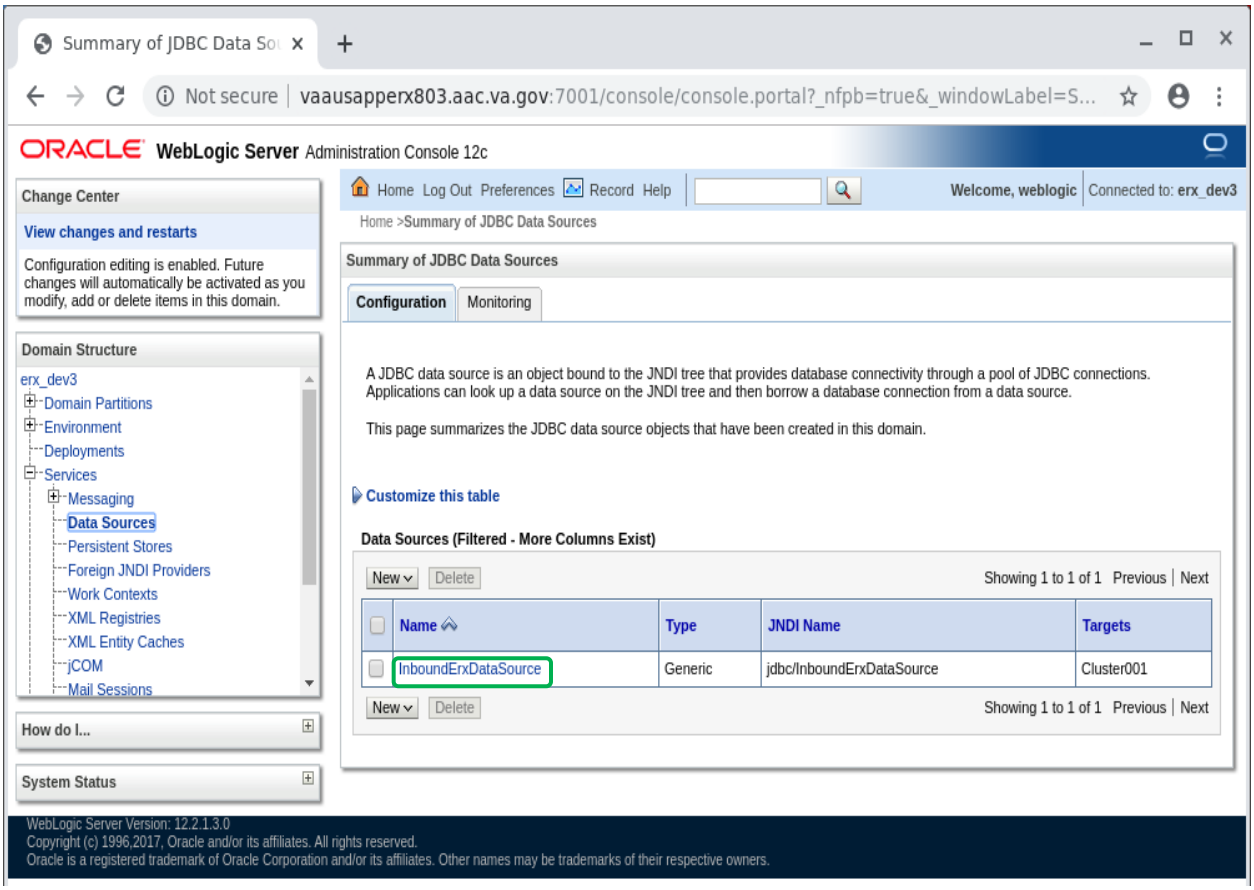
18. Select “All servers in the cluster”
19. Click “Finish” button.

Figure 33: Create Inbound eRx Datasource – Select Targets/Finish



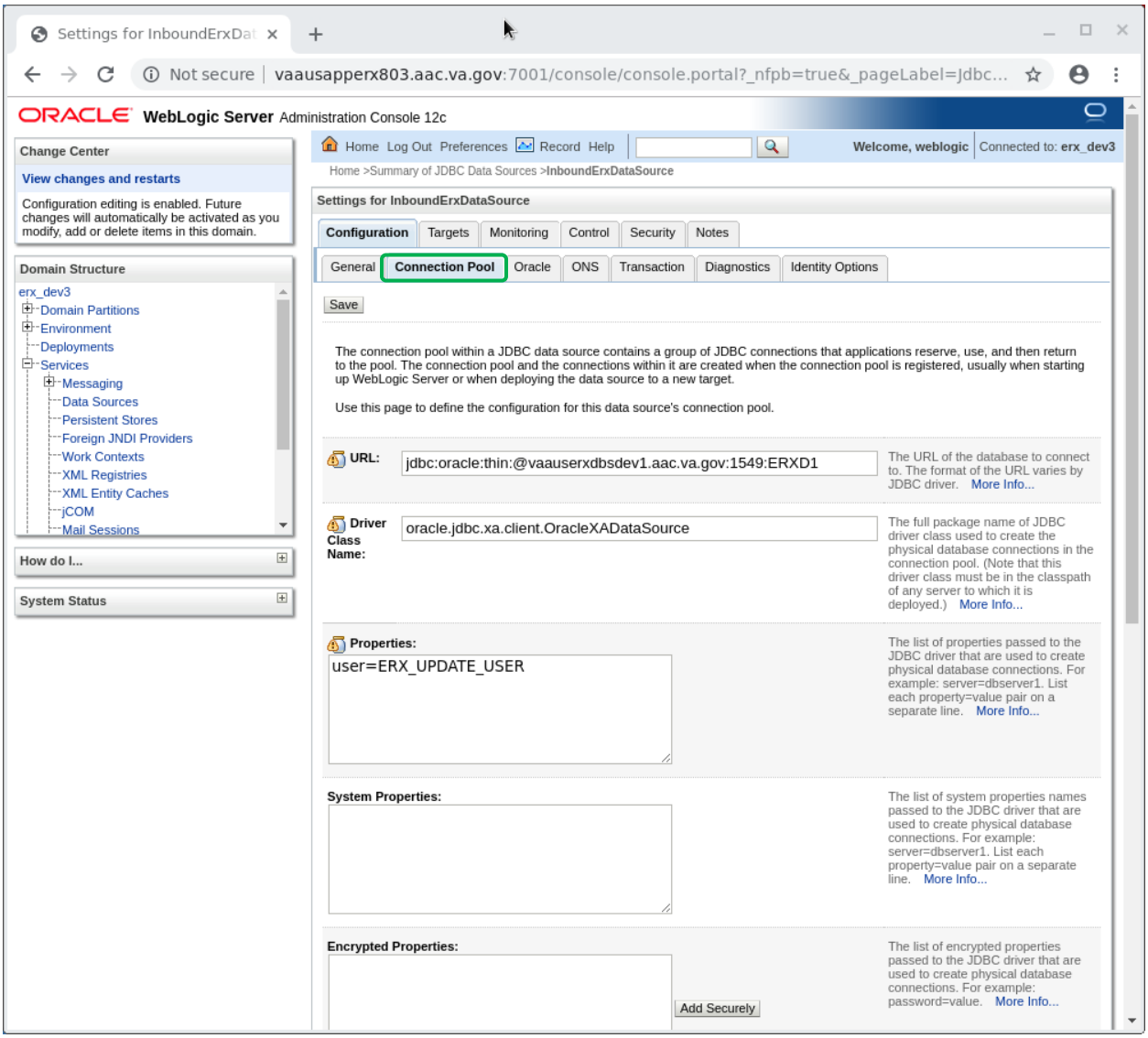
20. Select “InboundErxDataSource” hyperlink

Figure 34: Create Inbound eRx Datasource – Modify New Datasource



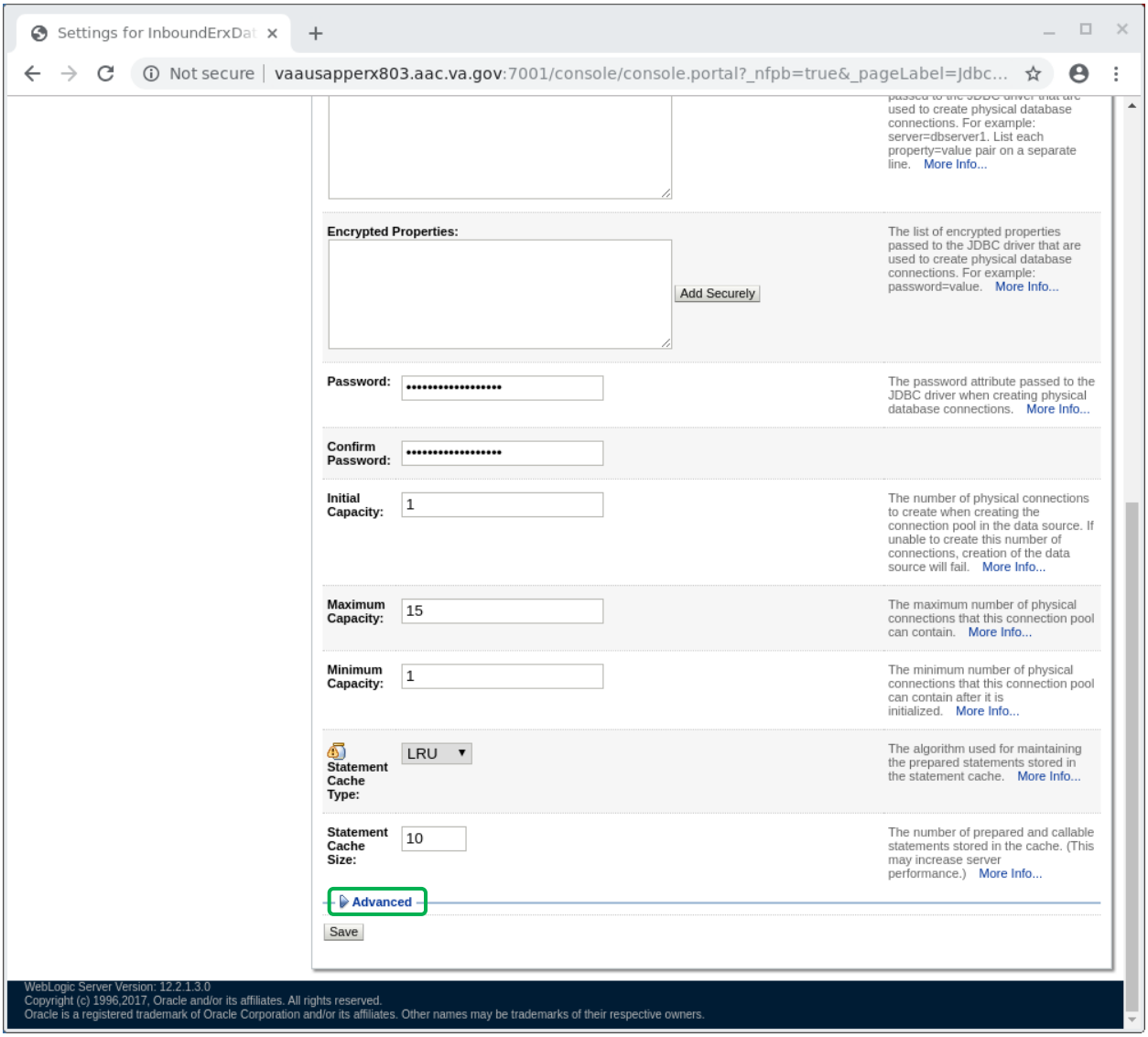
21. Select “Connection Pool” tab

Figure 35: Inbound eRx Datasource –Connection Pool Properties



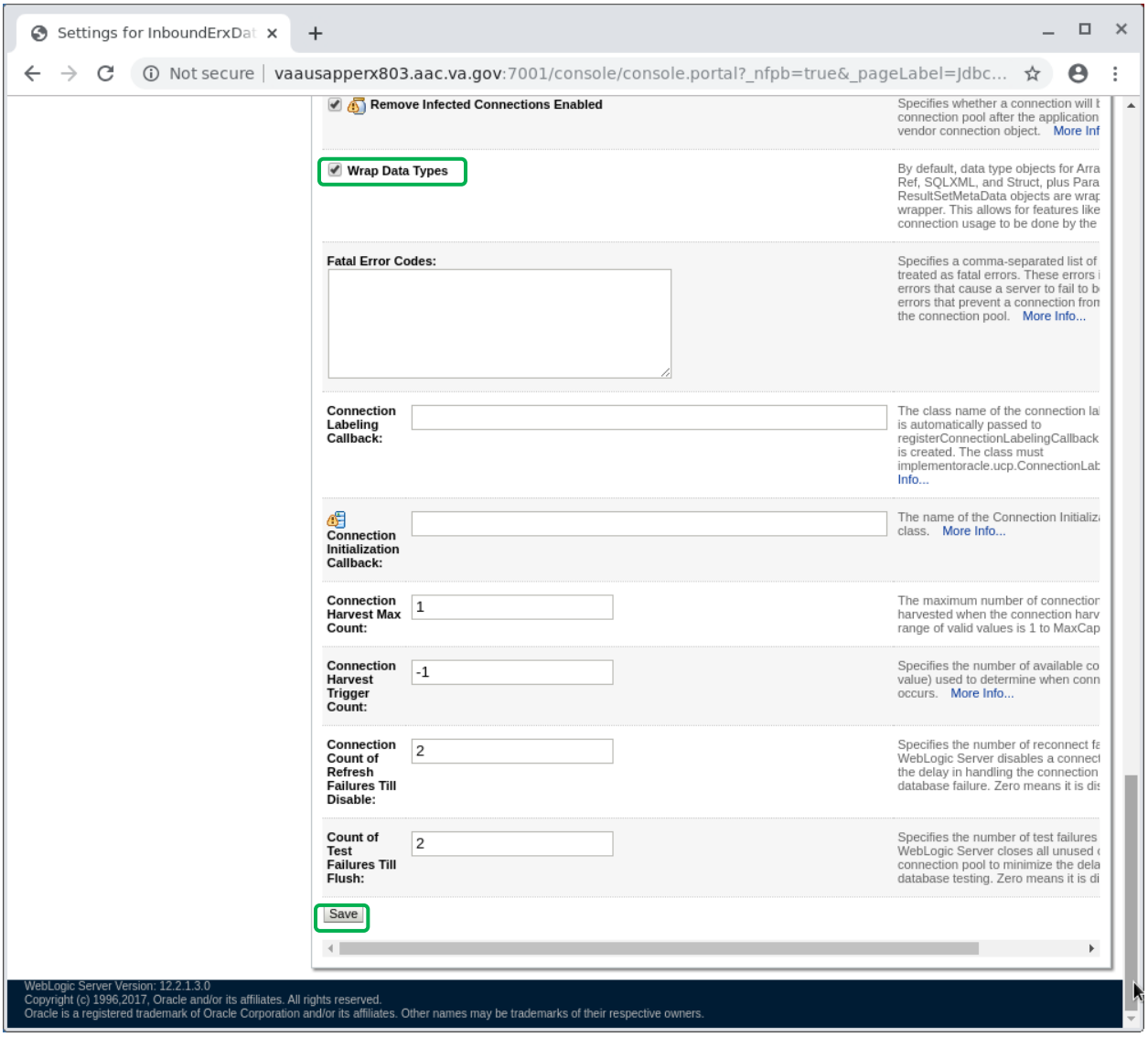
22. Scroll to the bottom of the “Connection Pool” page
23. Select “Advanced” hyperlink to expand the advanced properties

Figure 36: Inbound eRx Datasource –Connection Pool Advanced Properties



24. Scroll to the bottom of the of the "Advanced Connection Pool" page
25. Unckeck the "Wrap Data Types" property
26. Click the "Save" button

Figure 37: Inbound eRx Datasource – Wrap Data Type Property

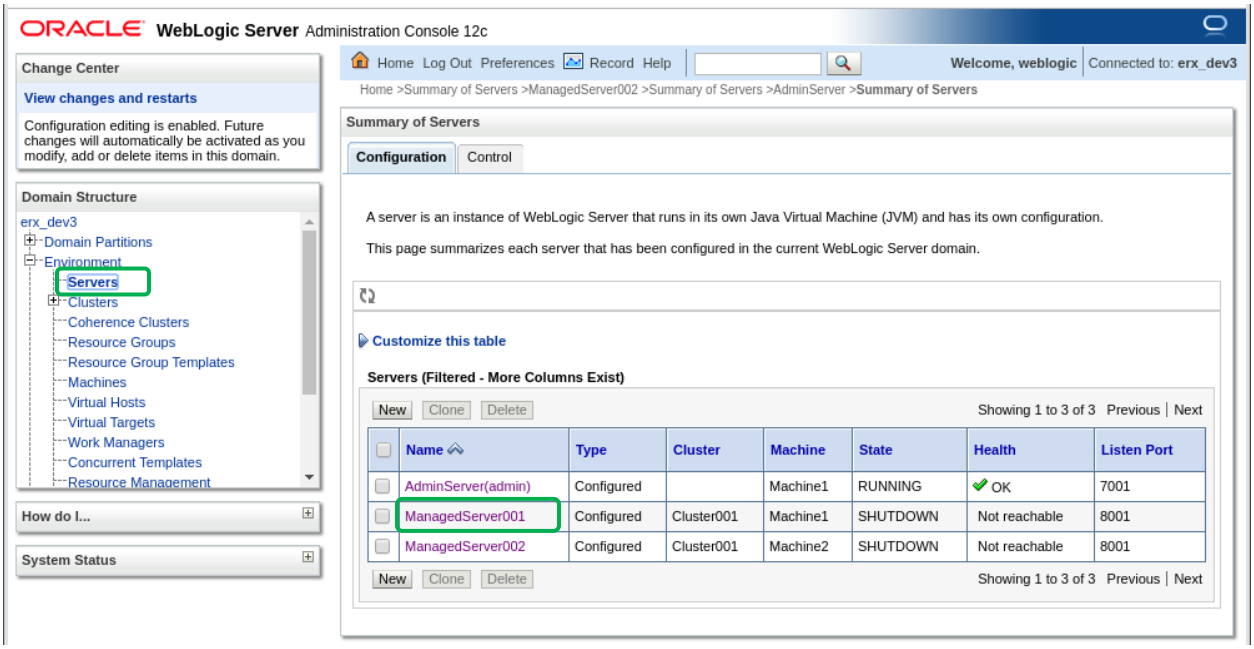


4.8.1.15 Configure Identity/Trust Store File on Managed Servers

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

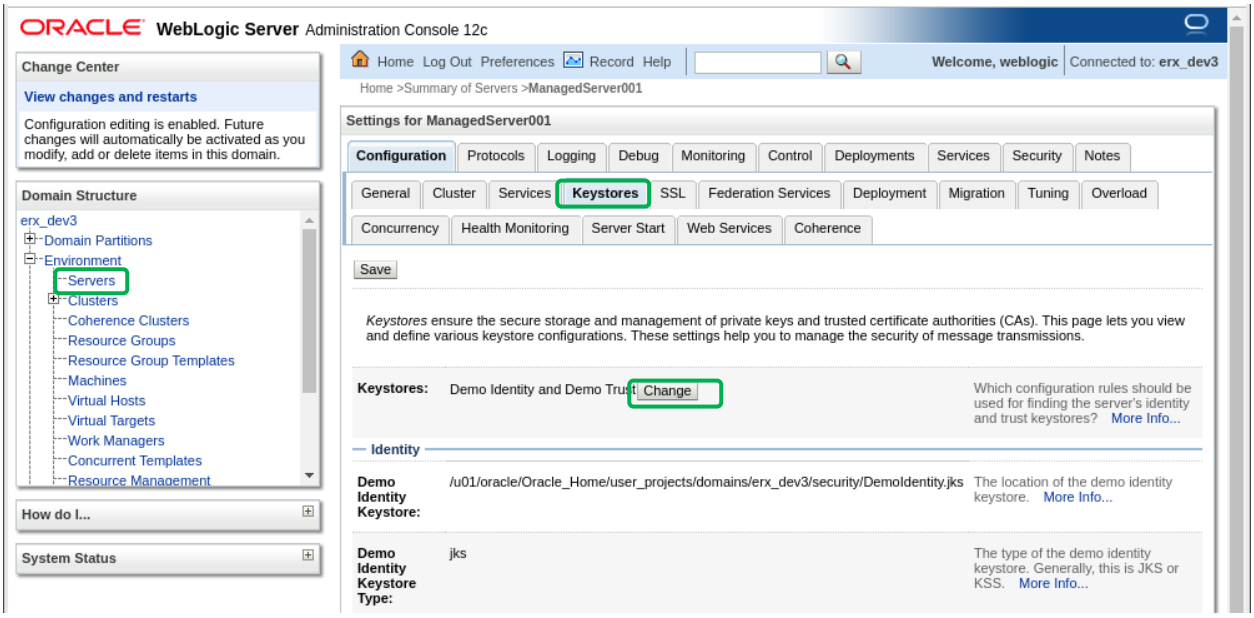
1. Under **Domain Structure**, navigate to **Environment > Servers**.
2. Click on the "***[mserver1]***" link to access the server configuration page.

Figure 38: Configure Identity/Trust Store File – Access Server Configuration Page



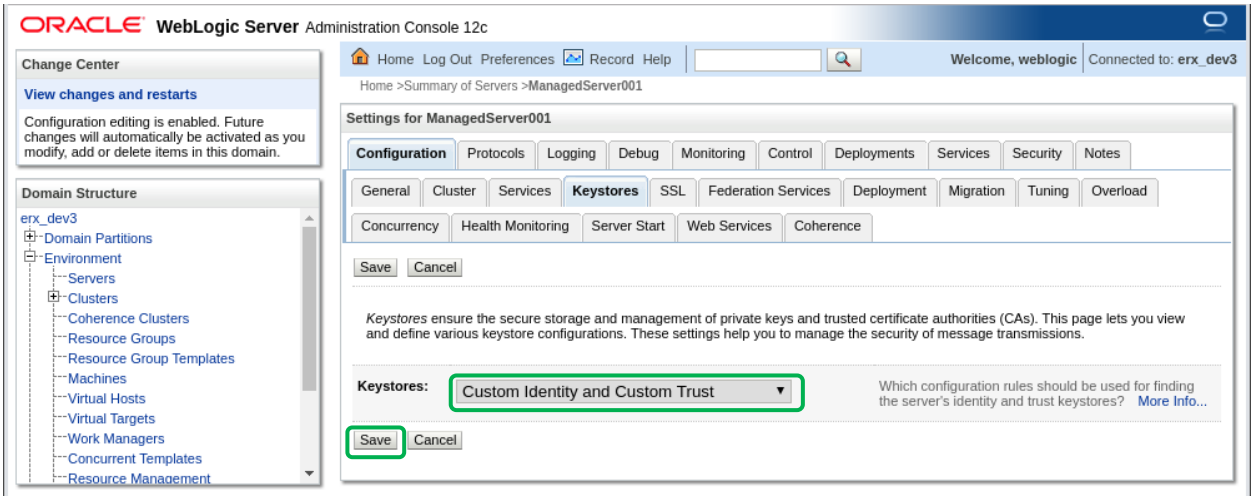
3. Under **Configuration** > **Keystores**, click **Change**.

Figure 39: Configure Identity/Trust Store File – Change Keystores



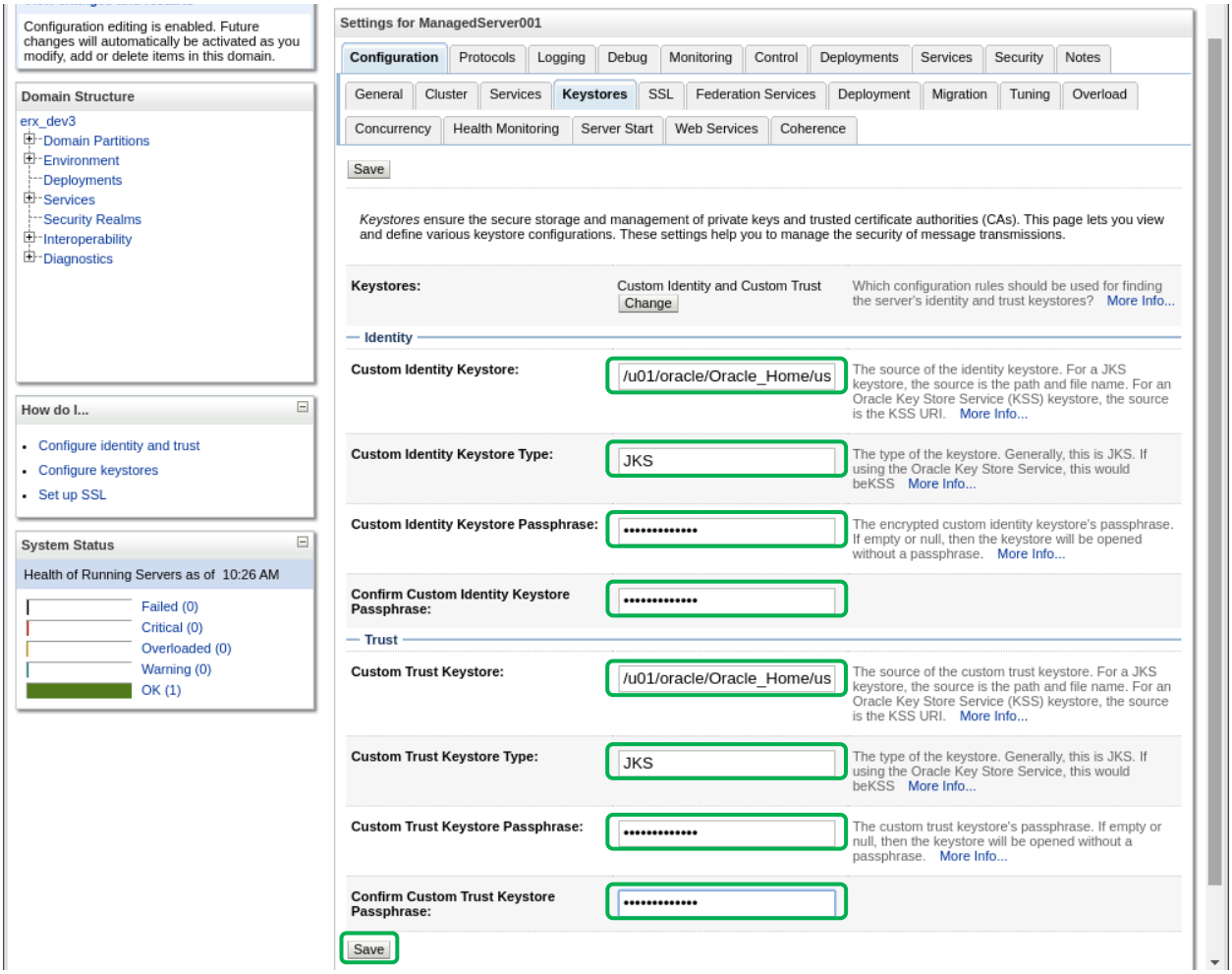
4. For *Keystores*, select "Custom Identity and Custom Trust".
5. Click **Save**.

Figure 40: Configure Identity/Trust Store File – Keystores – Select Custom Identify and Custom Trust



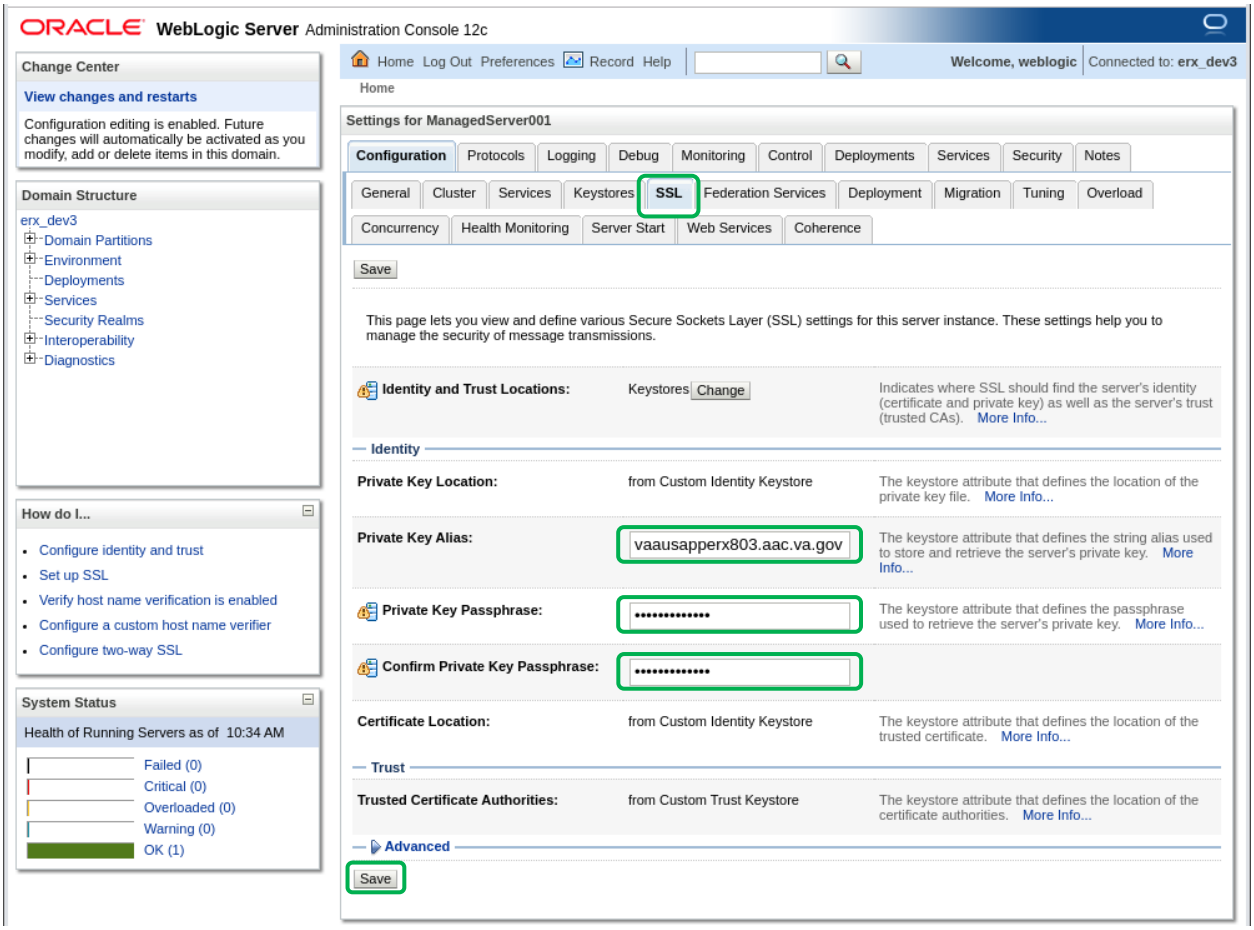
6. Modify the setting under the **Keystores** tab as illustrated in the figure below. The *Custom Identity Keystore* and *Custom Trust Keystore* use the same file path to the keystore file copied to the Domain "security" directory: (***[DOMAIN_HOME]***/security/***[proxy_fqdn]***.jks).

Figure 41: Configure Identity/Trust Store File – Modify Keystore Settings



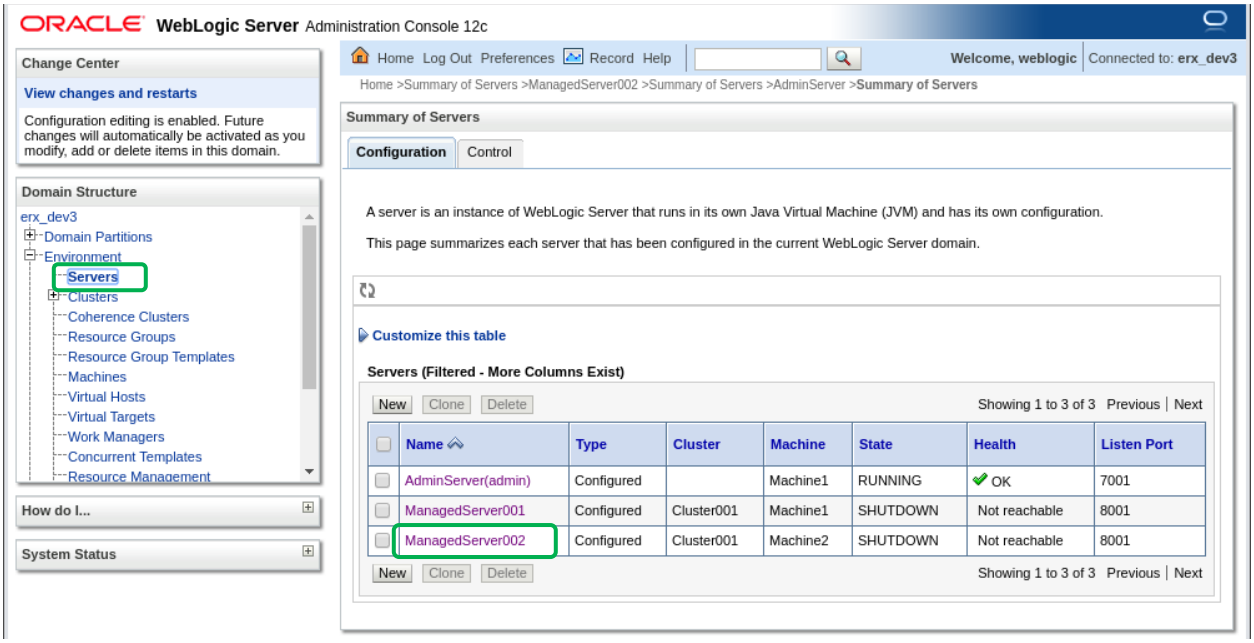
7. Modify the setting under the **SSL** tab as illustrated in the figure below. For the *Private Key Alias*, enter "***[proxy_fqdn]***".
8. Enter and confirm the *Private Key Passphrase*.
9. Click **Save**.

Figure 42: Configure Identity/Trust Store File – Modify SSL Settings



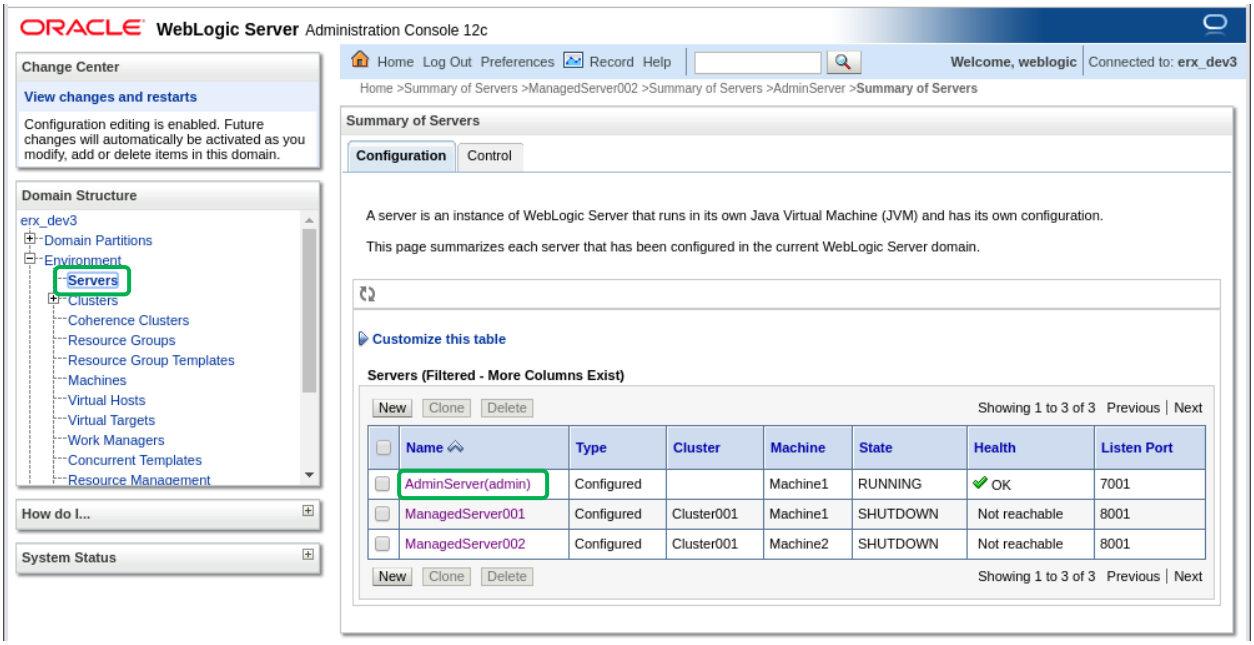
10. Navigate to *Servers*, and then click on the "erx2" link to access the server configuration page in the **Administration Console**.
11. Repeat the Keystore configuration steps for "erx2" as described earlier in this section for "erx1".

Figure 43: Configure Identity/Trust Store File – Managed Server 2 Configuration



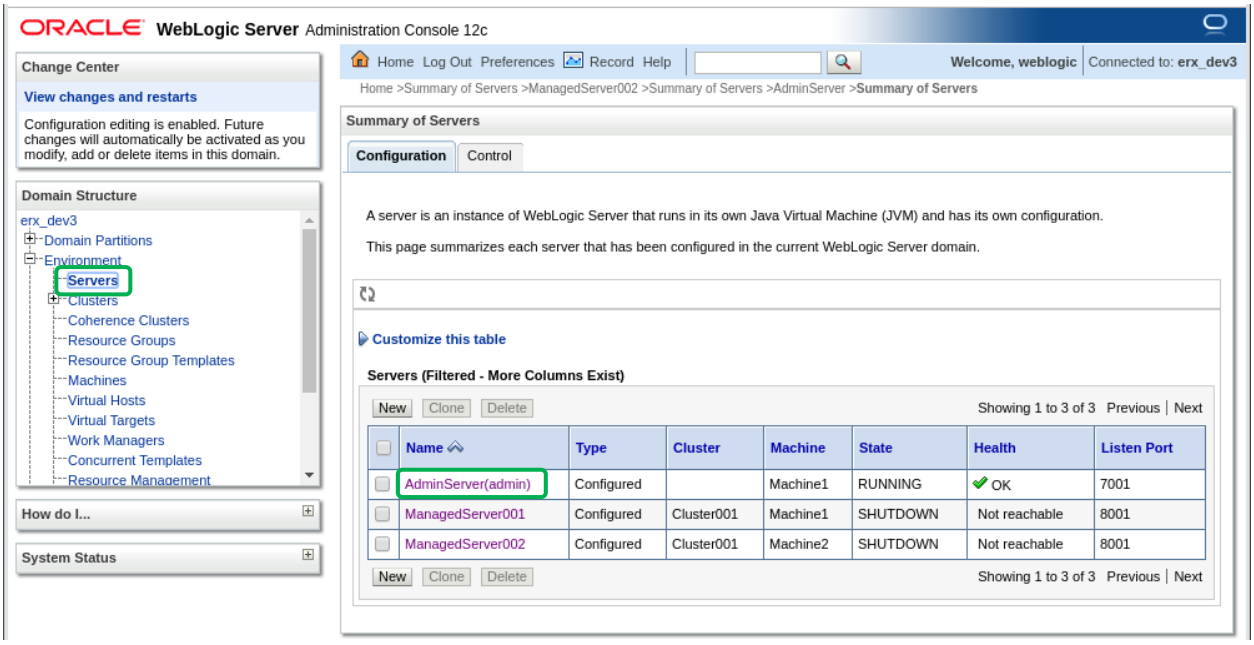
12. Navigate to *Servers*, and then click on the "AdminServer(admin)" hyperlink to access the server configuration page.
13. Repeat the Keystore configuration steps for "AdminServer(admin)" as described earlier in this section for "erx1".

Figure 44: Configure Identity/Trust Store File – Admin Server Configuration



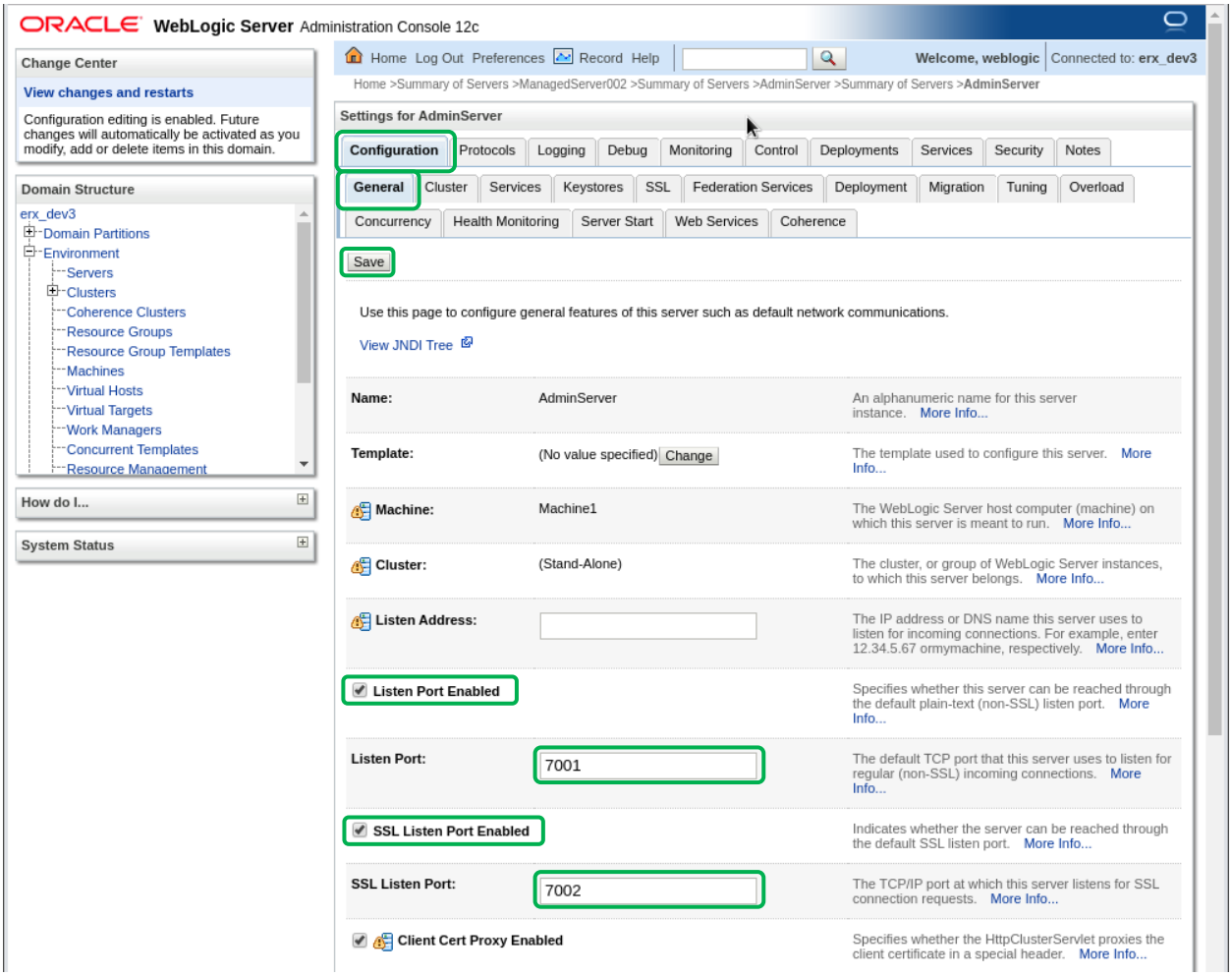
14. Navigate to *Servers*, and then click on the "AdminServer(admin)" hyperlink to access the server configuration page.

Figure 45: Configure Identity/Trust Store File – Admin Server Configuration



15. Under “Configuration” > “general” tabs:
    Check “Listen Port Enabled”
    Enter “Listen Port”: 7001
    Check “SSL Port Enabled”
    Enter “SSL Listen Port”: 7002
    Click “Save” button.

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



4.8.1.16 Pack Domain on VM1

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

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

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

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

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

6. Copy the resulting jar file to VM2 under:

```
/u01/templates
```

4.8.1.17 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
```

4.8.1.18 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
```

4.8.1.19 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 the "$ORACLE_BASE/domain-registry.xml" file contains an entry like the following. If it doesn't, add it manually.
```
<domain location="[DOMAIN_HOME]"/>
```
5. Check the "$DOMAIN_HOME/nodemanager/nodemanager.domains" file contains an entry like the following. If it doesn't, add it manually.
```
erxdomain1=[DOMAIN_HOME]
```
6. If the node manager is not already started on this server, start it now.
```
$ nohup $DOMAIN_HOME/bin/startNodeManager.sh &
```

4.8.1.20 Check Node Manager on Each WebLogic Machine

This section outlines the steps for checking that the node manager is reachable on each WebLogic machine.

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

4.8.1.21 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.

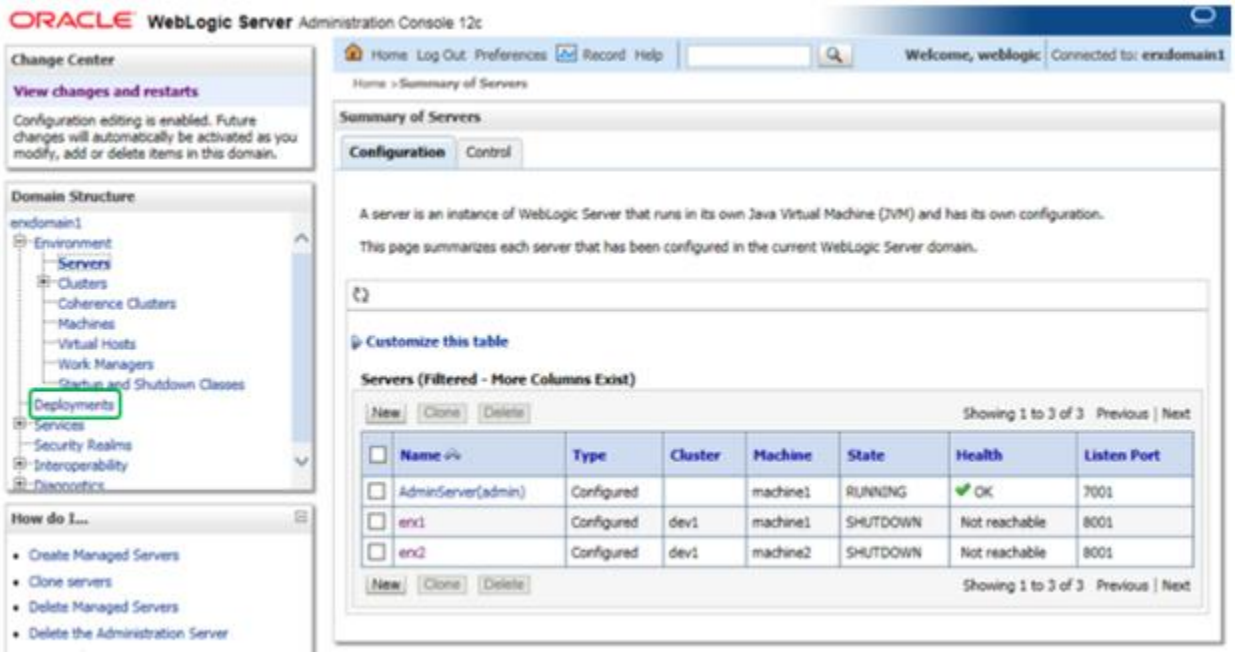
4.8.1.22 Deploy Test Application

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 47: Deploy Test Application: Deployments Page

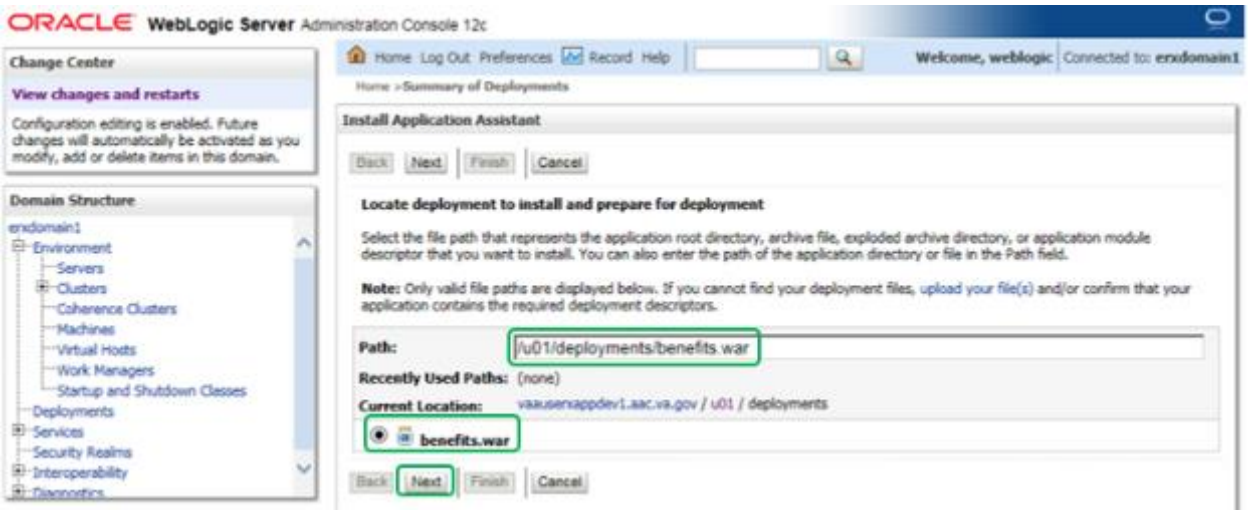


5. From the *Deployments* page, click **Install**.

Figure 48: Deploy Test Application – Install

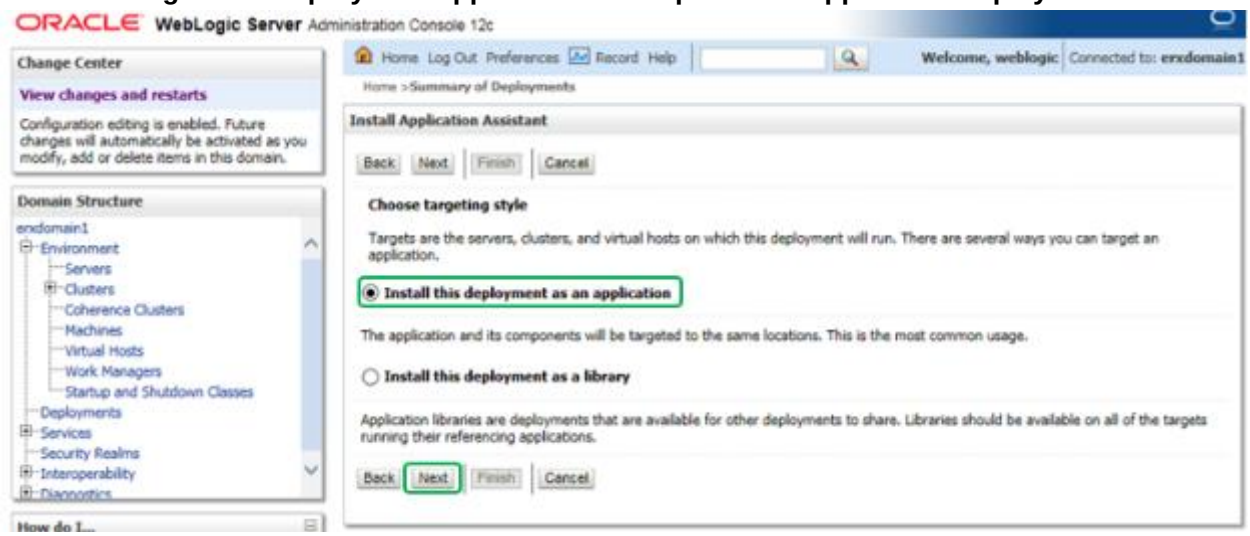
6. Install a new deployment of the test application using the WAR file as indicated in the figure below.
7. Click **Next**.

Figure 49: Deploy Test Application – WAR File



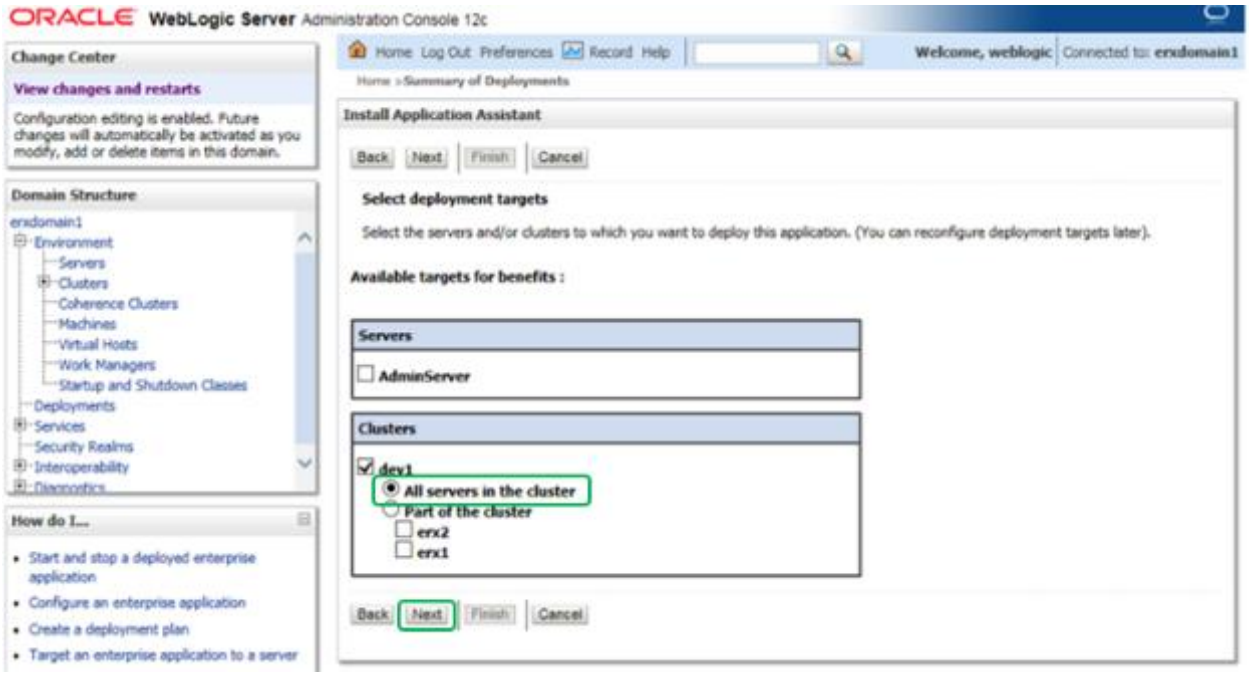
8. Accept the defaults for an application deployment. (The *Install this deployment as an application radio butto*n is marked.)
9. Click **Next**.

Figure 50: Deploy Test Application – Accept Default Application Deployment



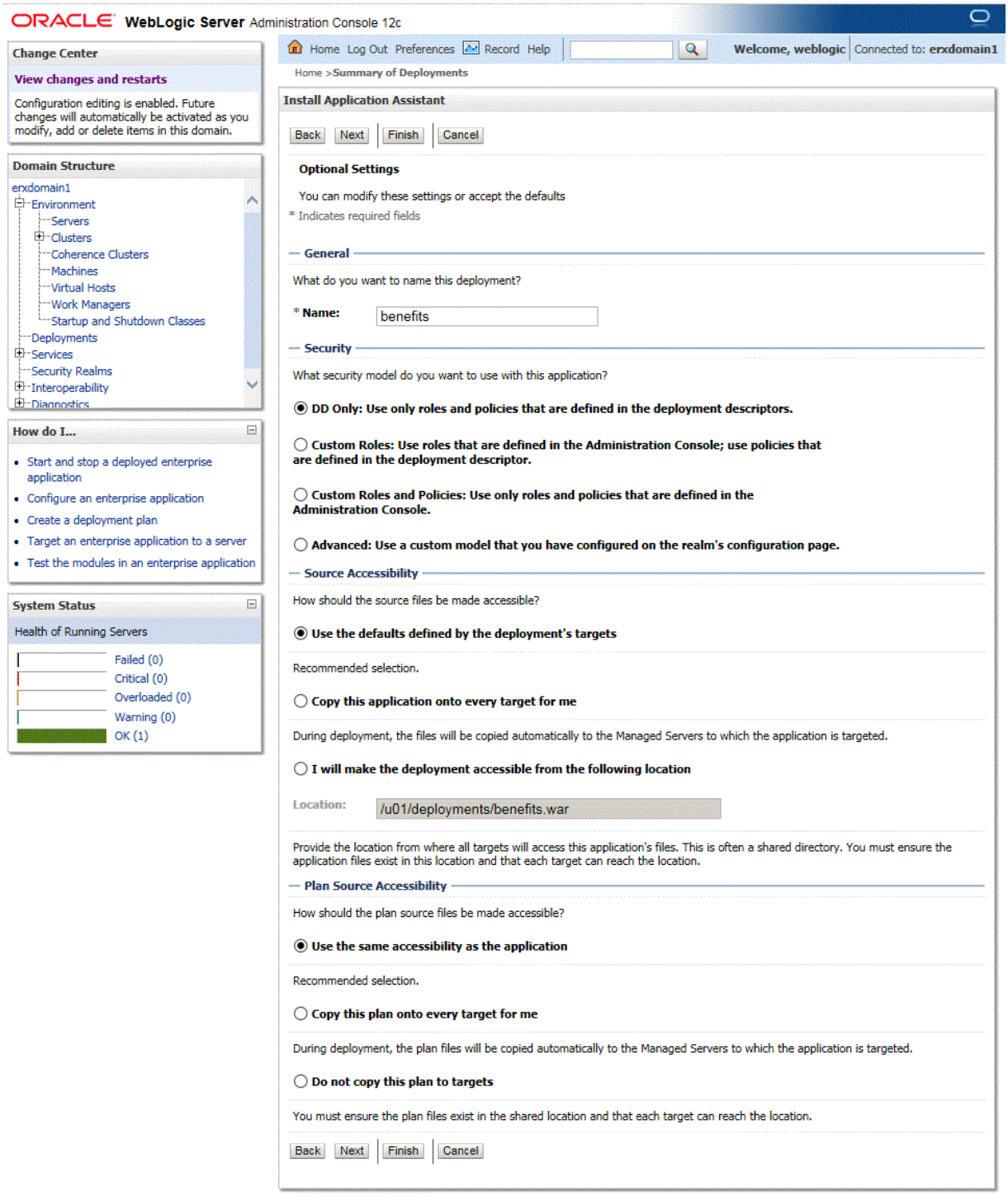
10. Select the *All servers in the cluster* option under the "erx" cluster as the target for the deployment.
11. Click **Next**.

Figure 51: Deploy Test Application – Select Deployment Target



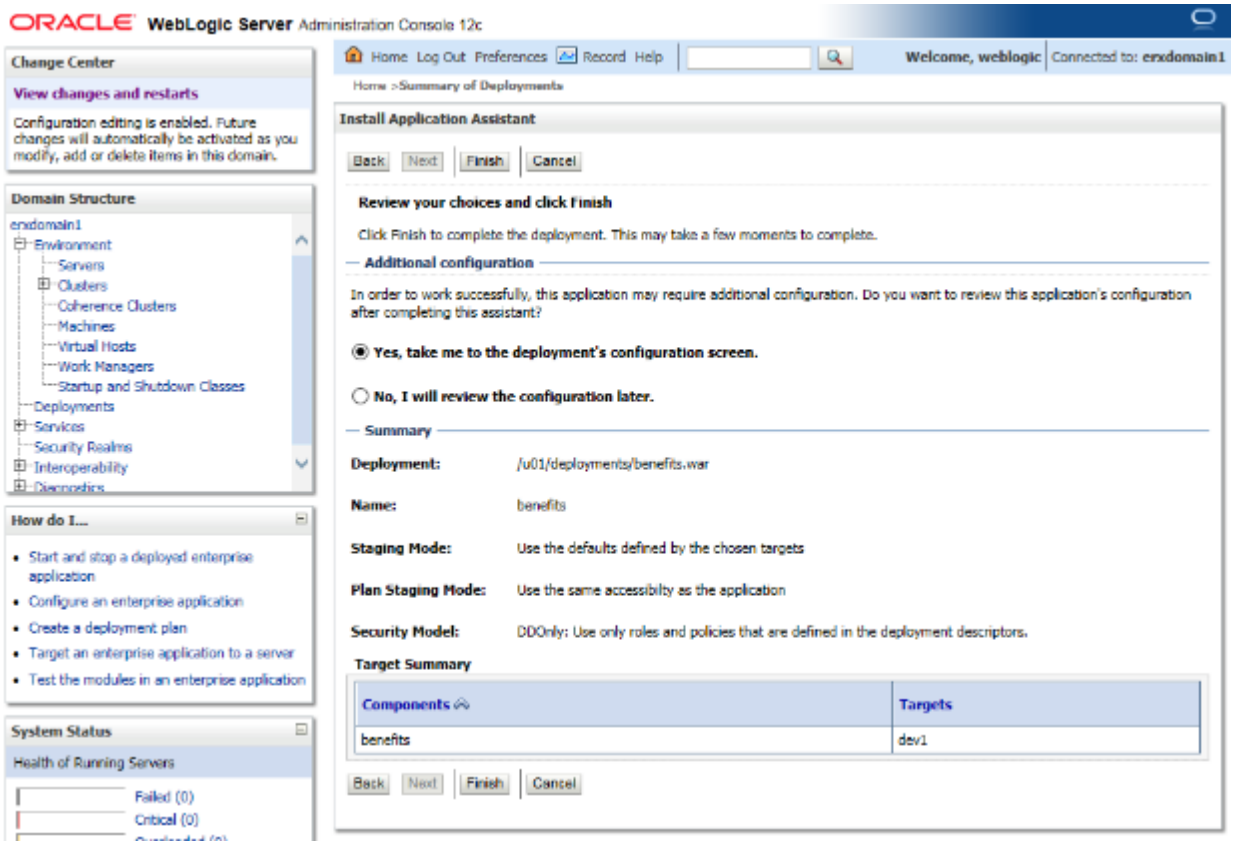
12. All of the values should appear as illustrated in the figure below.
13. Click **Next**.

Figure 52: Deploy Test Application – Verify Deployment Settings



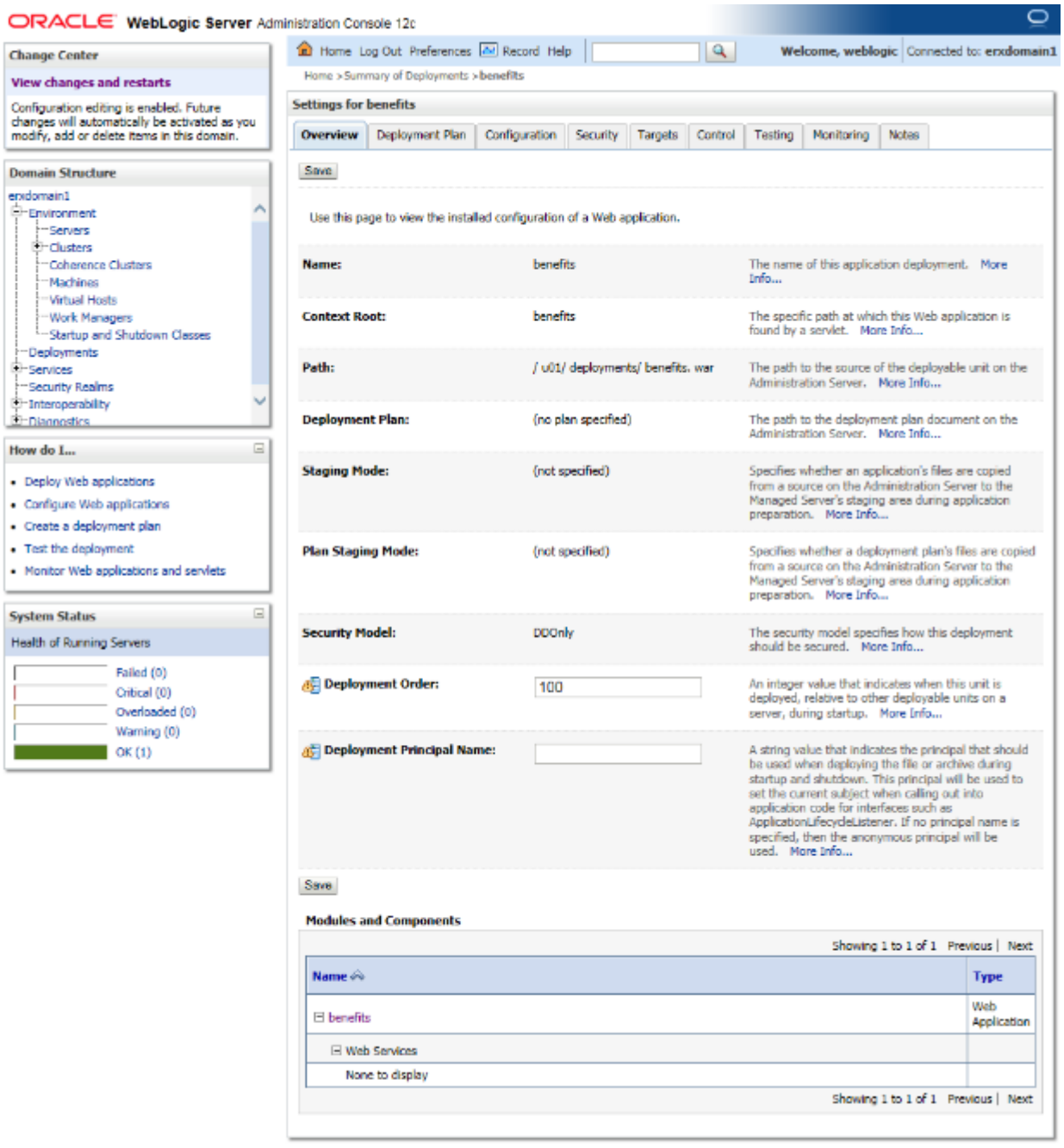
14. Verify that all of the values appear as illustrated in the figure below.
15. Click **Finish**.

Figure 53: Deploy Test Application – Verify Deployment Settings (Finish)



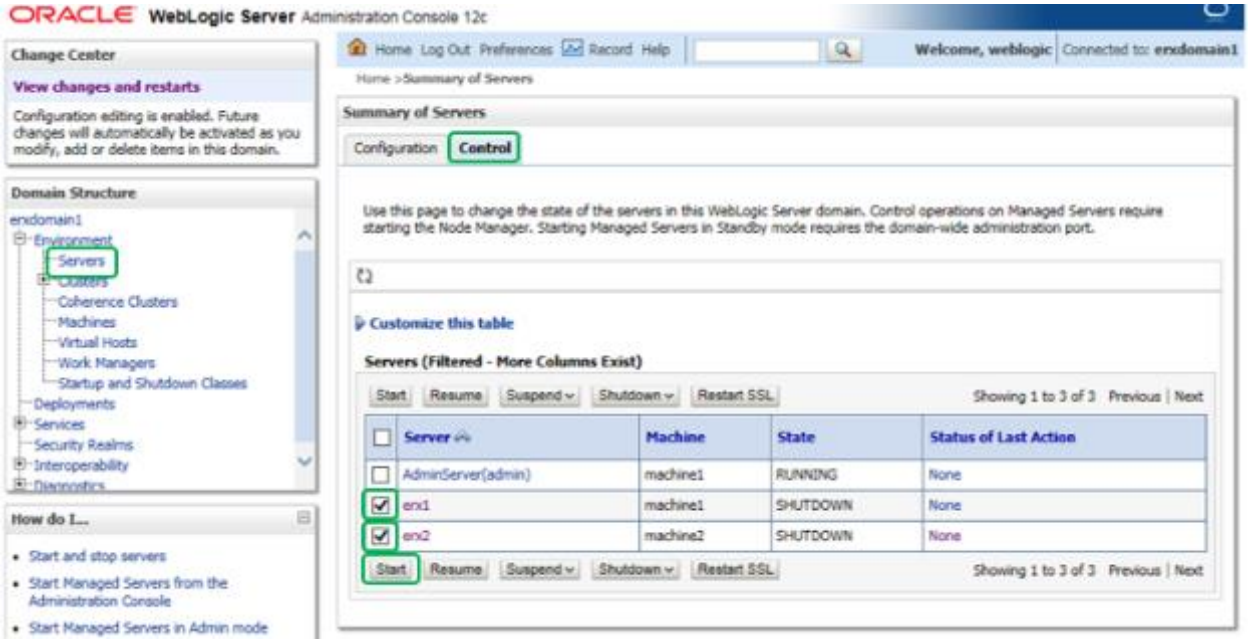
16. The **Overview** tab should appear as illustrated in the figure below.

Figure 54: Deploy Test Application – Verify "benefits" Settings



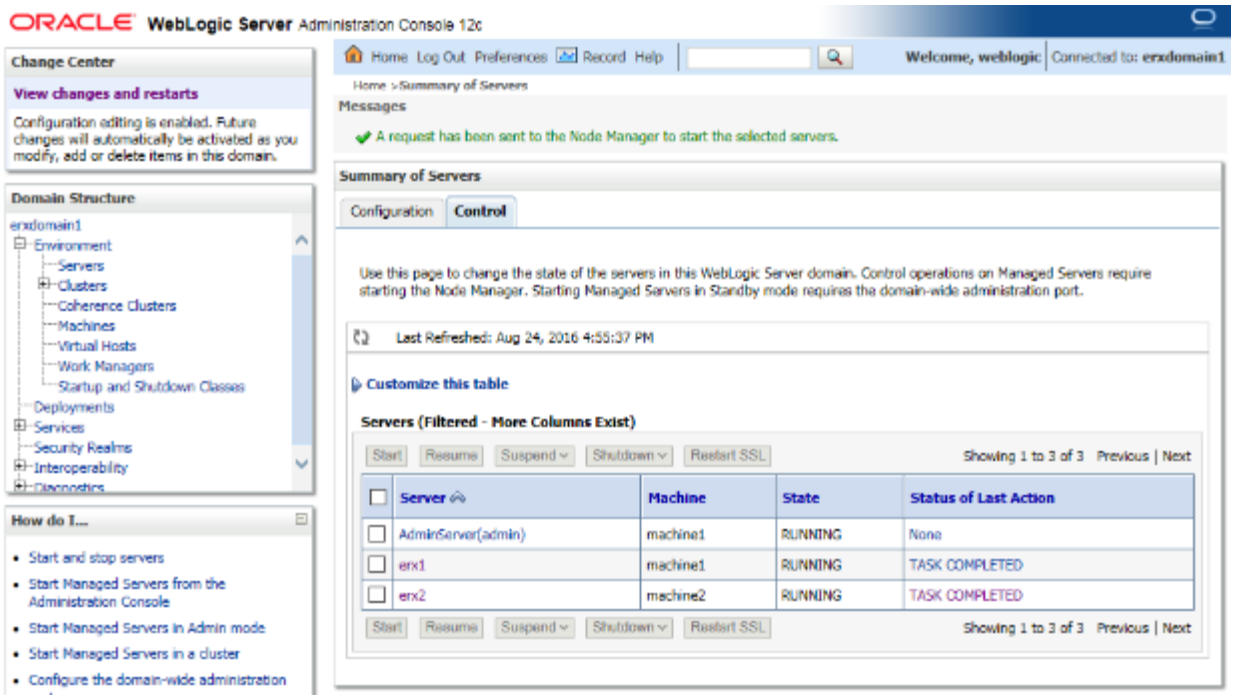
17. Navigate to the **Servers** page in the WebLogic console.
18. Select the **Control** tab.
19. Select "erx1" and "erx2" servers.
20. Click **Start**.

Figure 55: Deploy Test Application – Summary of Servers Table



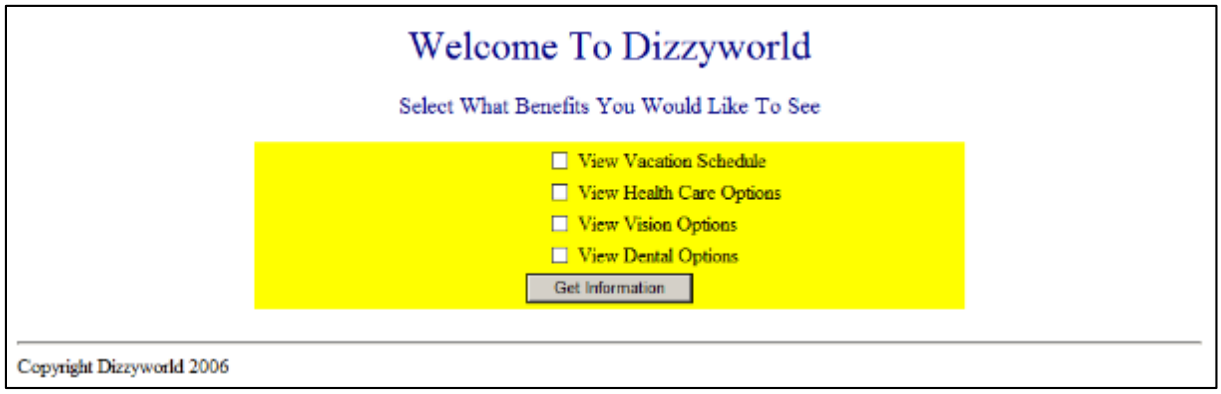
21. After a couple minutes, the state on the servers will change to "RUNNING".

Figure 56: Deploy Test Application – Servers Running



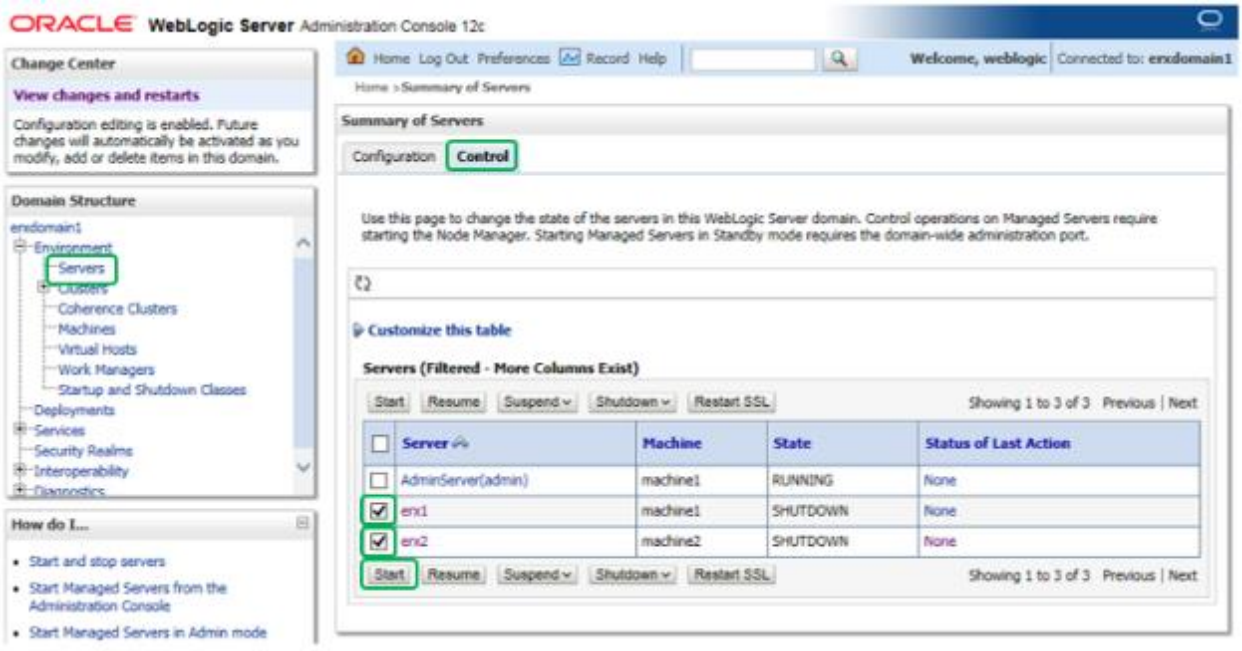
22. Open a web browser to http://***[vm1_fqdn]***/benefits/.
23. The Dizzyworld Benefits application will display.

Figure 57: 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. Click **Shutdown**.

Figure 58: Deploy Test Application – Shutdown Servers



4.8.1.23 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.

4.8.1.24 Install VistALink on VM1 and VM2

This section outlines the steps for installing VistALink.

1. As your normal Linux login account, dzdo su to the weblogic account:
   ```
   $ dzdo su - weblogic
   ```
2. Create downloads directory if it doesn't exist (the following must be performed by a system administrator):
   ```
   $ dzdo mkdir -p /u01/downloads
   $ dzdo chown weblogic:weblogic /u01/downloads
   $ dzdo chmod 777 /u01/downloads
   ```
3. Download vljConnector-1.5.0.028.jar, vljFoundationsLib-1.6.0.28.jar, log4j-1.2.17.jar to the downloads directory:

   Download from AITC IEP eRx Downloads directory
4. Create configureVistalink.sh
   ```
   $ cd $DOMAIN_HOME
   $ cat > bin/configureVistaLink.sh
   #!/bin/sh

   # ------------ VistaLink Edits --------------

   USERSTAGING=${DOMAIN_HOME}/vistalink
   export USERSTAGING
   echo "."
   echo "User Staging Area: ${USERSTAGING}"
   echo "."

   # Vistalink Classpath...

   VLJCLASSPATH=${USERSTAGING}/resource_adapters
   export VLJCLASSPATH

   echo "Vistalink Staging Area: $VLJCLASSPATH"

   CLASSPATH=${CLASSPATH}${CLASSPATHSEP}${USERSTAGING}
   export CLASSPATH
   CLASSPATH=${CLASSPATH}${CLASSPATHSEP}${VLJCLASSPATH}
   export CLASSPATH
   # ------------ End VistaLink Edits --------------
   <CTRL D>
   $chmod 755 bin/configureVistaLink.sh
   ```
5. Modify configureVistaLink.sh (**Production environment only**):
   ```
   $ vi $DOMAIN_HOME/bin/configureVistaLink.sh
   ```
   Add the following line to the bottom of the file:
   ```
   export JAVA_OPTIONS="${JAVA_OPTIONS} -Dgov.va.med.environment.production=true"
   ```

6. Modify the Domain Startup script (startWebLogic.sh):

```
$ vi $DOMAIN_HOME/bin/startWeblogic.sh
```

Modify JAVA_OPTIONS about 1/3 of the way down the file as shown:

```
#JAVA_OPTIONS="${SAVE_JAVA_OPTIONS}
JAVA_OPTIONS="${SAVE_JAVA_OPTIONS}
 -Dweblogic.security.SSL.minimumProtocolVersion=TLSv1.1"
```

Add call to configureVistalink.sh after the setDomainEnv.sh call as shown:

```
. ${DOMAIN_HOME}/bin/setDomainEnv.sh $*
. ${DOMAIN_HOME}/bin/configureVistaLink.sh $*
```

7. Modify the nodemanager.properties file:

```
$ vi $DOMAIN_HOME/nodemanager/nodemanager.properties
```

Ensure StartScriptEnabled=true:

```
StartScriptEnabled=true
```

4.8.1.25 Configure VistALink on VM1 and VM2

1. Create downloads directory if it doesn't exist (the following must be performed by a system administrator):
```
$ dzdo mkdir -p /u01/downloads
$ dzdo chown weblogic:weblogic /u01/downloads
$ dzdo chmod 777 /u01/downloads
```
2. Download the eRx/IEP Configurator (erx_iep_ x.x.x.xxx_configur_yyyymmdd _hhmmss.sh) to the downloads directory.
3. As your normal Linux login account, dzdo execute the eRx/IEP Configurator (erx_iep_ x.x.x.xxx_configur_yyyymmdd _hhmmss.sh) (the following must be performed by a system administrator):
```
$ dzdo /u01/downloads/erx_iep_ x.x.x.xxx_configur_yyyymmdd _hhmmss.sh
```
4. Select option 3, 4 and 5 then Exit (x).

4.8.1.26 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:

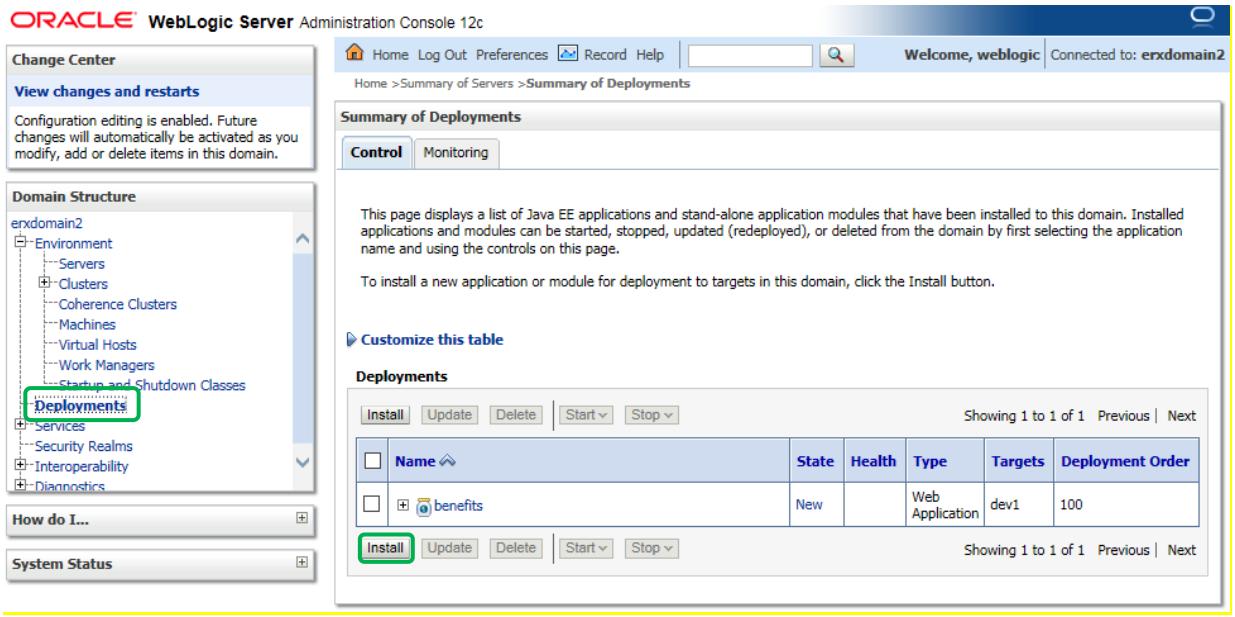
1. Stop the new domain on the VM1.
```
$ $DOMAIN_HOME/bin/stopWebLogic.sh
```
2. On VM1 stop the node manager.
```
$ $DOMAIN_HOME/bin/stopNodeManager.sh
```
3. On VM1, start the node manager.
```
$ DOMAIN_HOME/bin/stopNodeManager.sh
```
4. On VM2 stop the node manager.
```
$ $DOMAIN_HOME/bin/stopNodeManager.sh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

4.8.1.27 Deploy VistALink Libraries

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

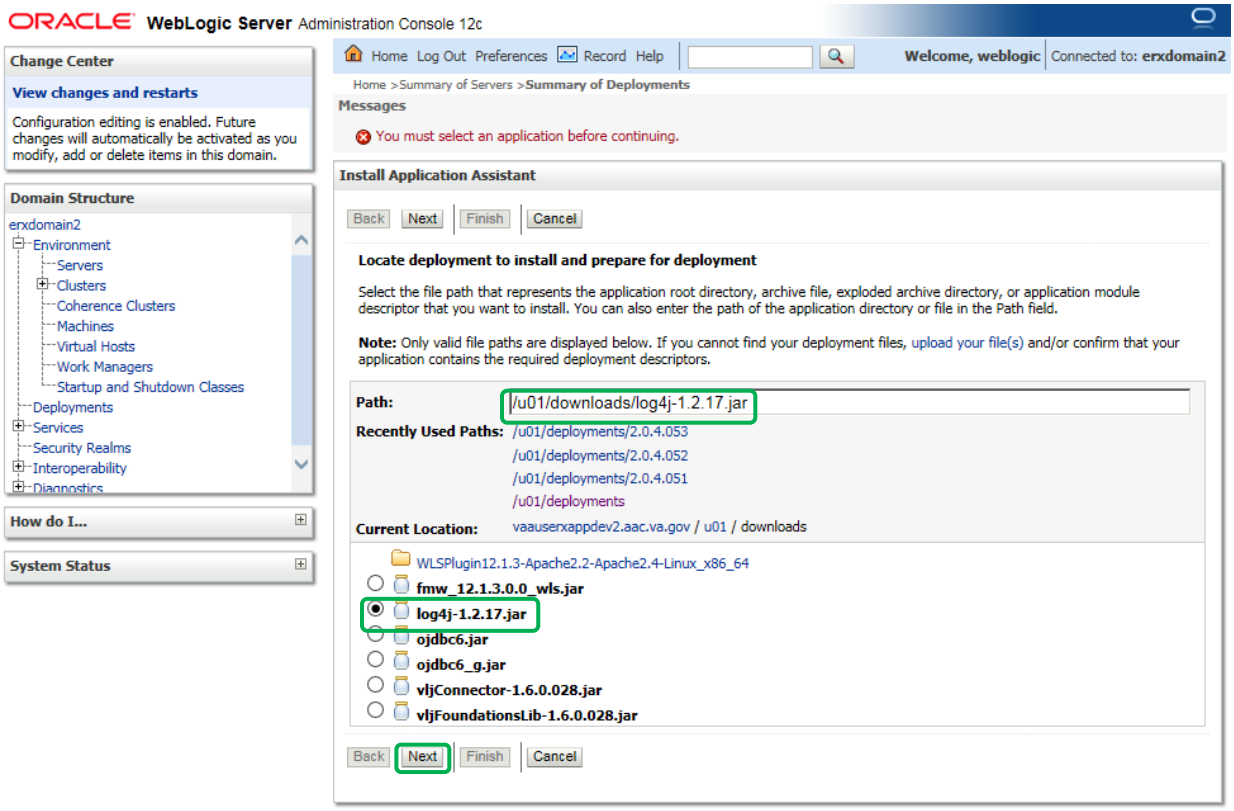
1. Navigate to the *Deployments* page.
2. From the *Deployment*s screen, click **Install**.

Figure 59: Deploy VistA Link Libraries – Deployments



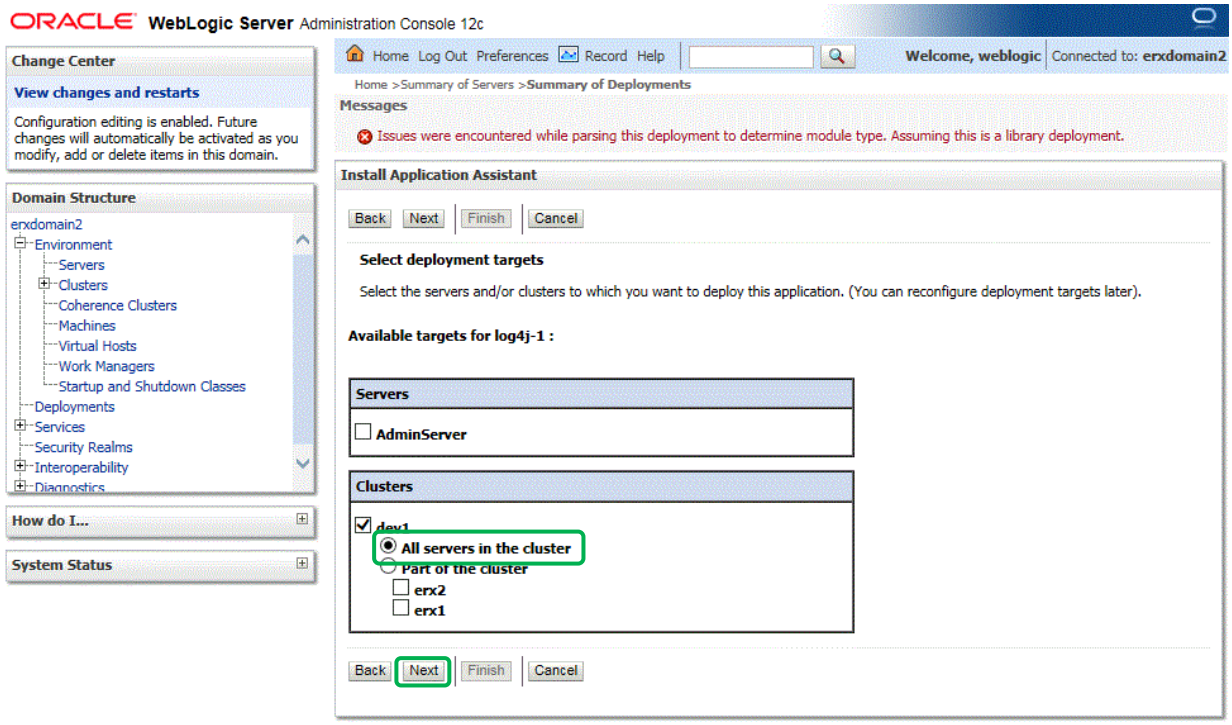
3. Enter *Path*: "/u01/downloads"
4. Install a new deployment of "log4j-1.2.17.jar" by selecting the jar file as indicated, and then click **Next**.

Figure 60: Deploy VistA Link Libraries – Select log4j Library to deploy



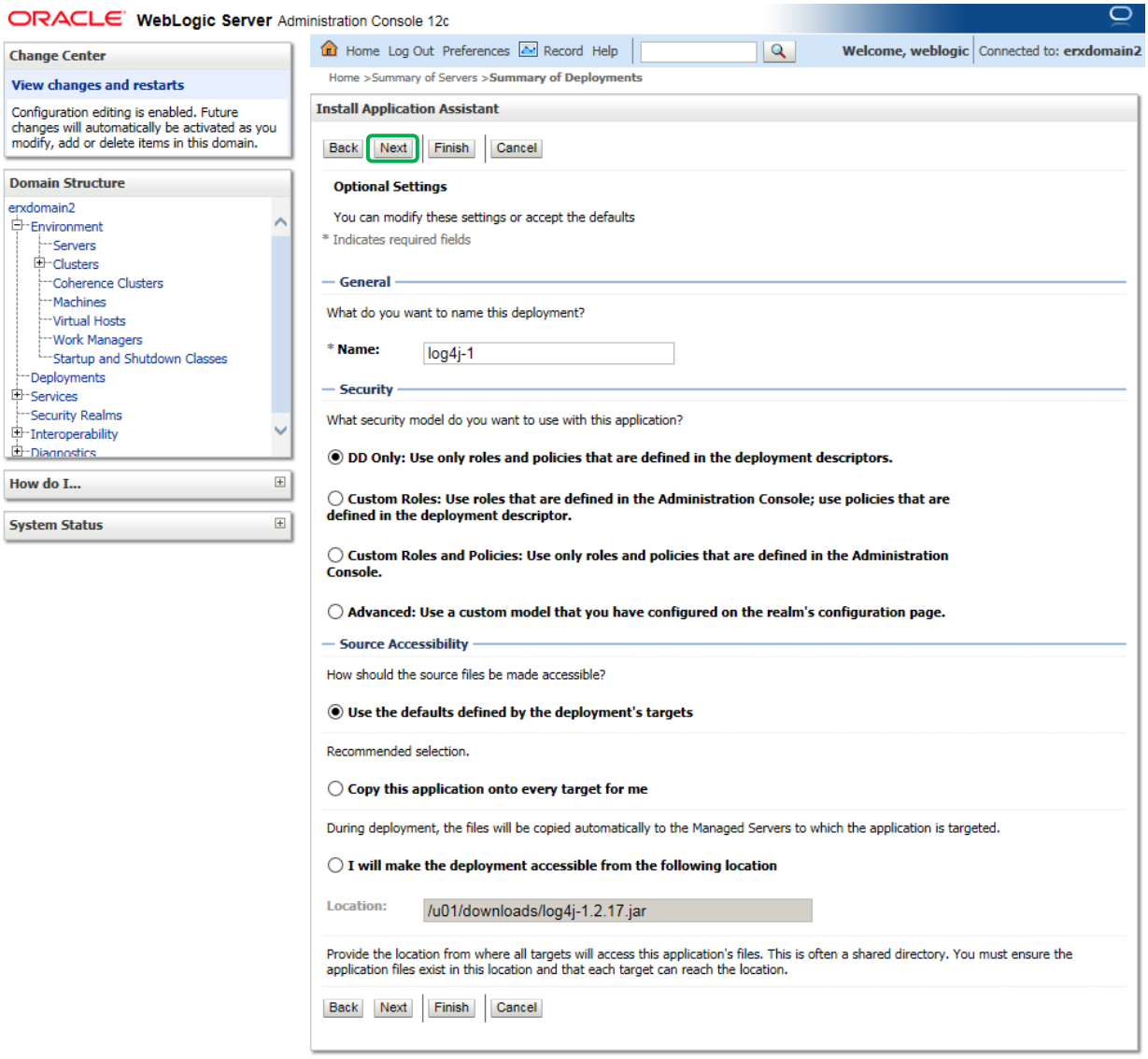
5. Select *All servers in the cluster* as the target for the deployment, and then click **Next**.

Figure 61: Deploy VistA Link Libraries – Select Deployment Targets



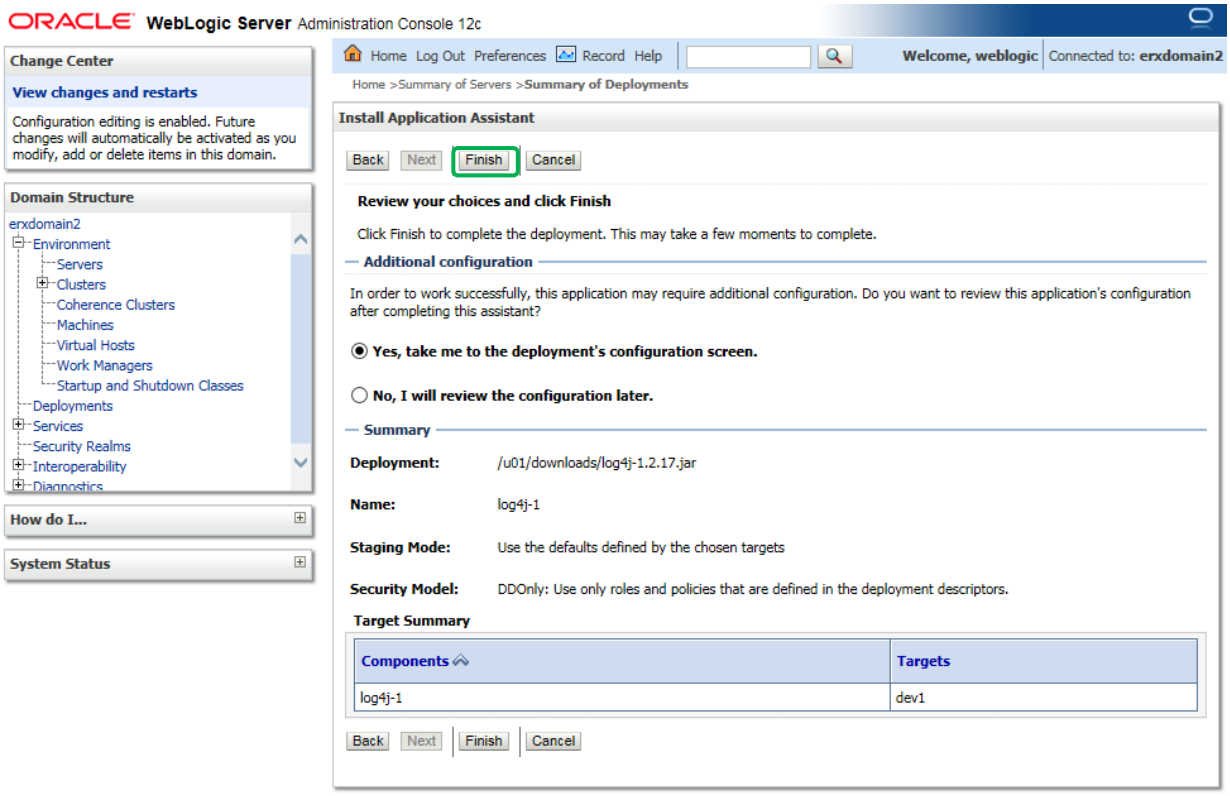
6. All of the values should appear as illustrated in the figure below.
7. Click **Next**.

Figure 62: Deploy VistA Link Libraries – Summary of Deployments Verification 1



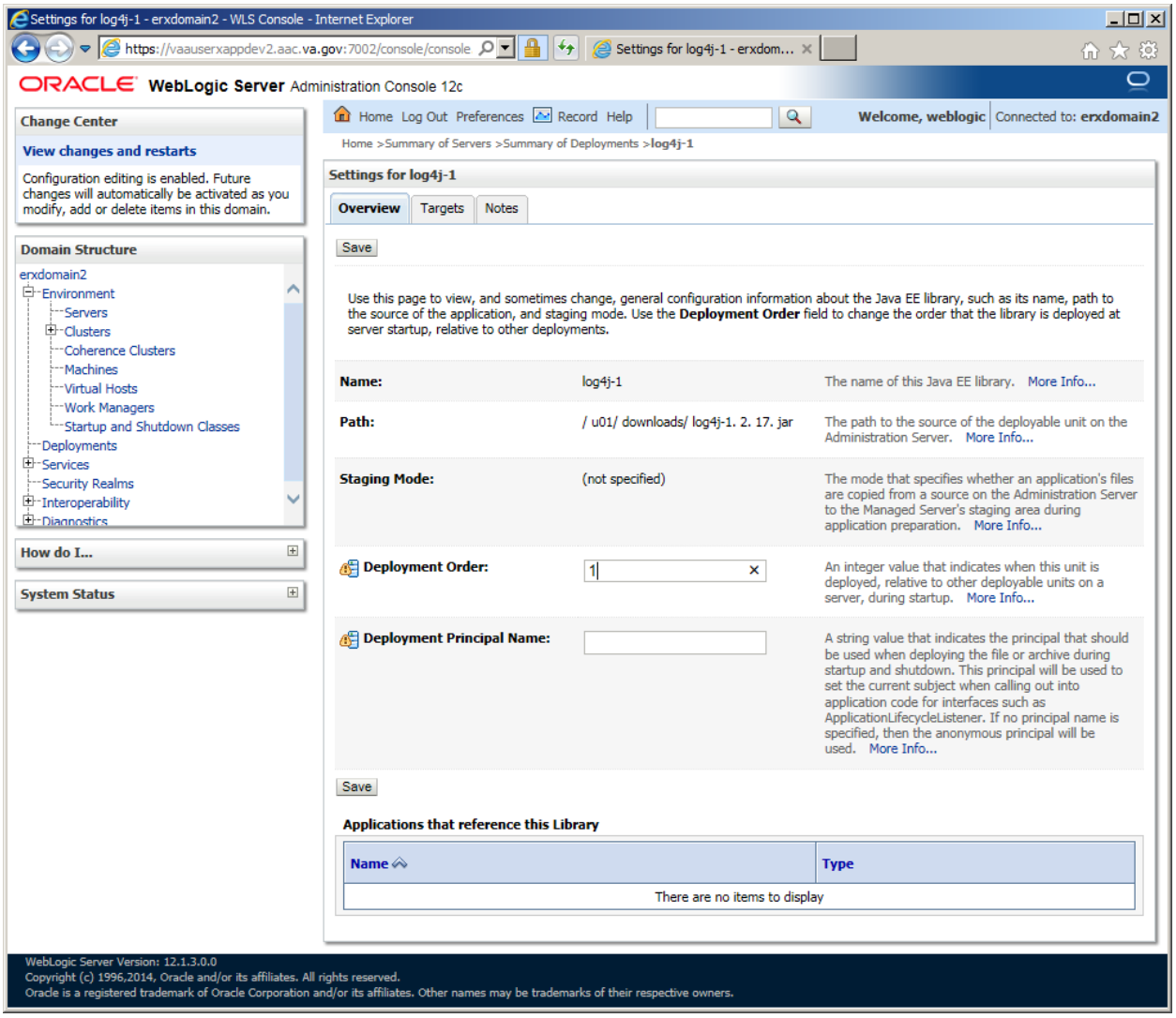
8. Verify that all of the values appear as illustrated in the figure below.
9. Click **Finish**.

Figure 63: Deploy VistA Link Libraries – Summary of Deployments Verification 2



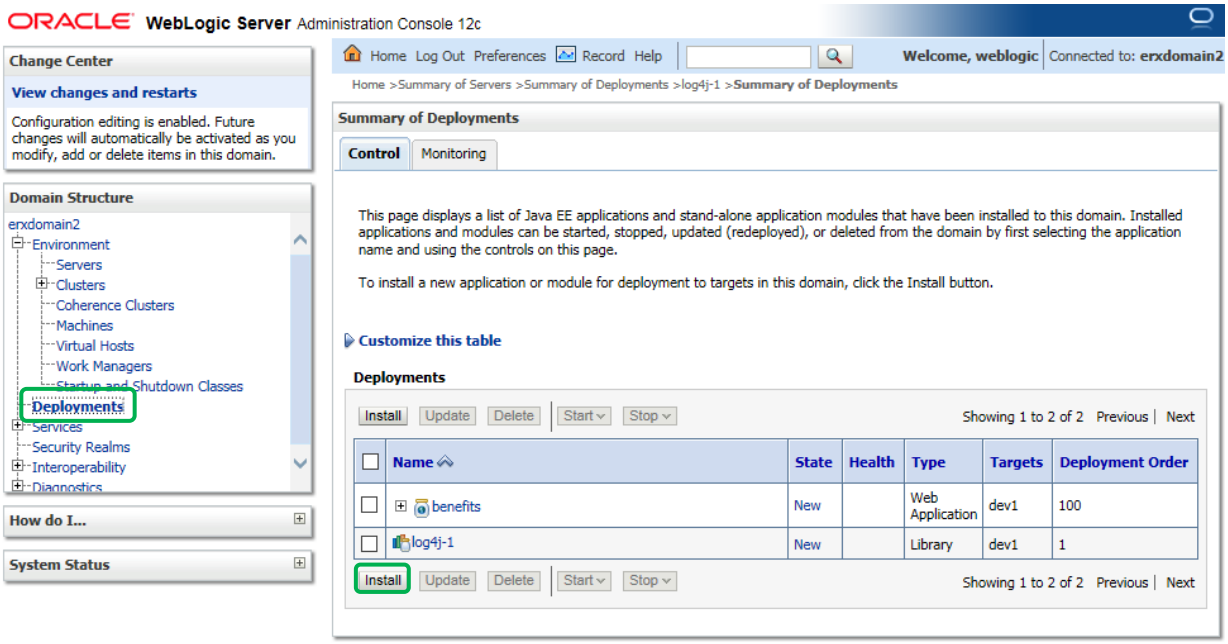
10. The **Deployment Configuration** screen should appear as illustrated in the below figure.
11. Enter *Deployment Order*: "1".
12. Click **Save**.

Figure 64: Deploy VistA Link Libraries – Deployment Configuration Screen



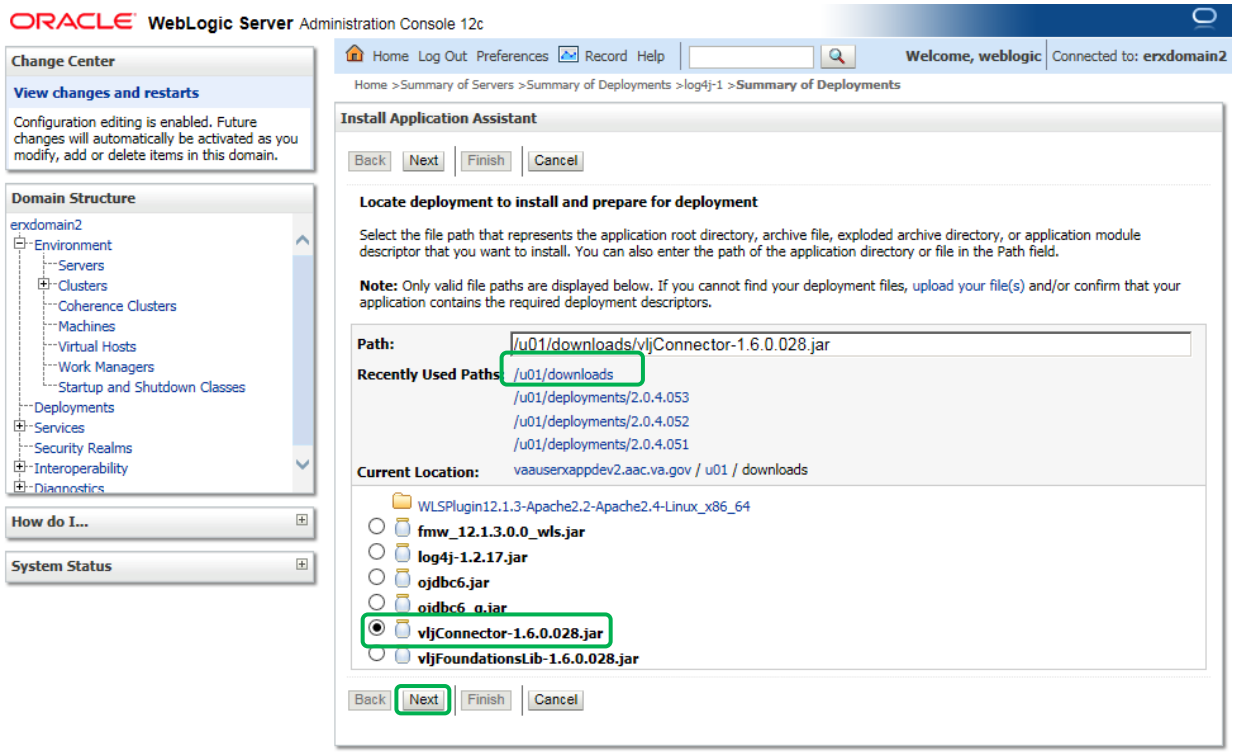
13. Navigate to the *Deployments* page.
14. From the *Deployments* screen, click **Install**.

Figure 65: Deploy VistA Link Libraries – Deployments



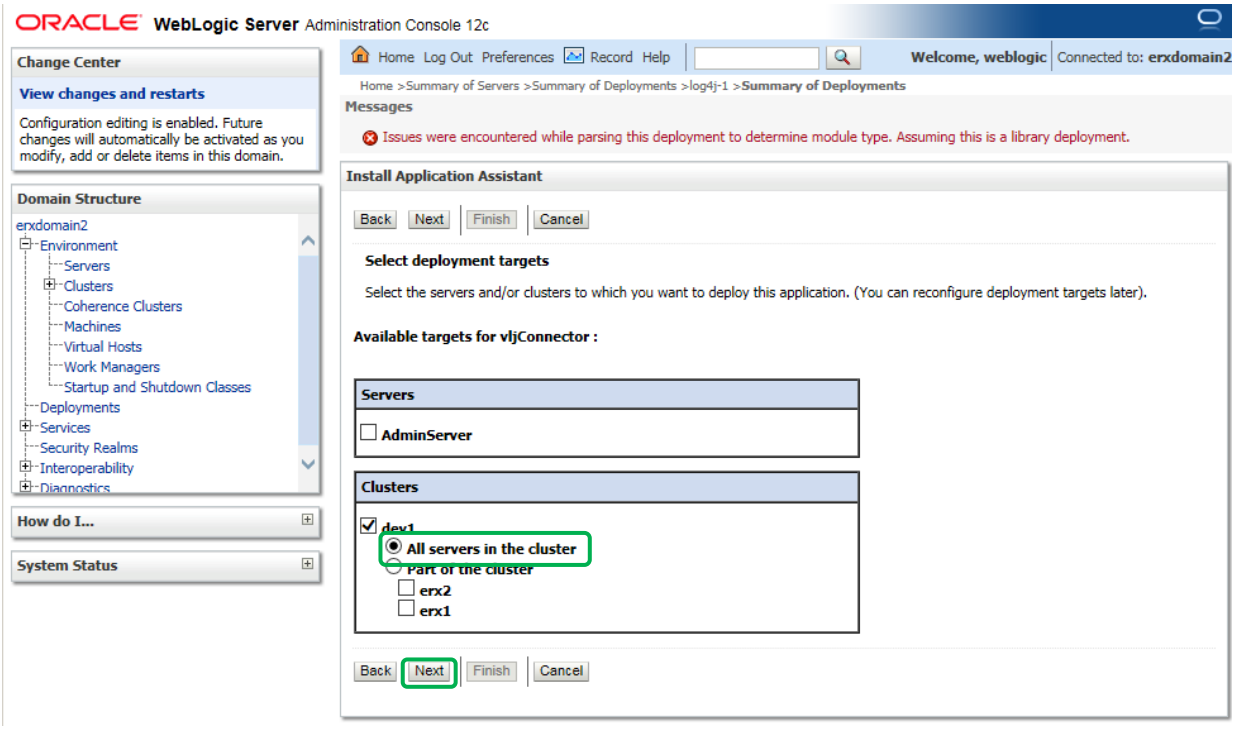
15. Enter *Path*: "/u01/downloads"
16. Install a new deployment of "vljConnector-1.6.0.028.jar" by selecting the jar file as indicated, and then click **Next**.

Figure 66: Deploy VistA Link Libraries – Select vljConnector-1.6.0.028.jar Library to deploy



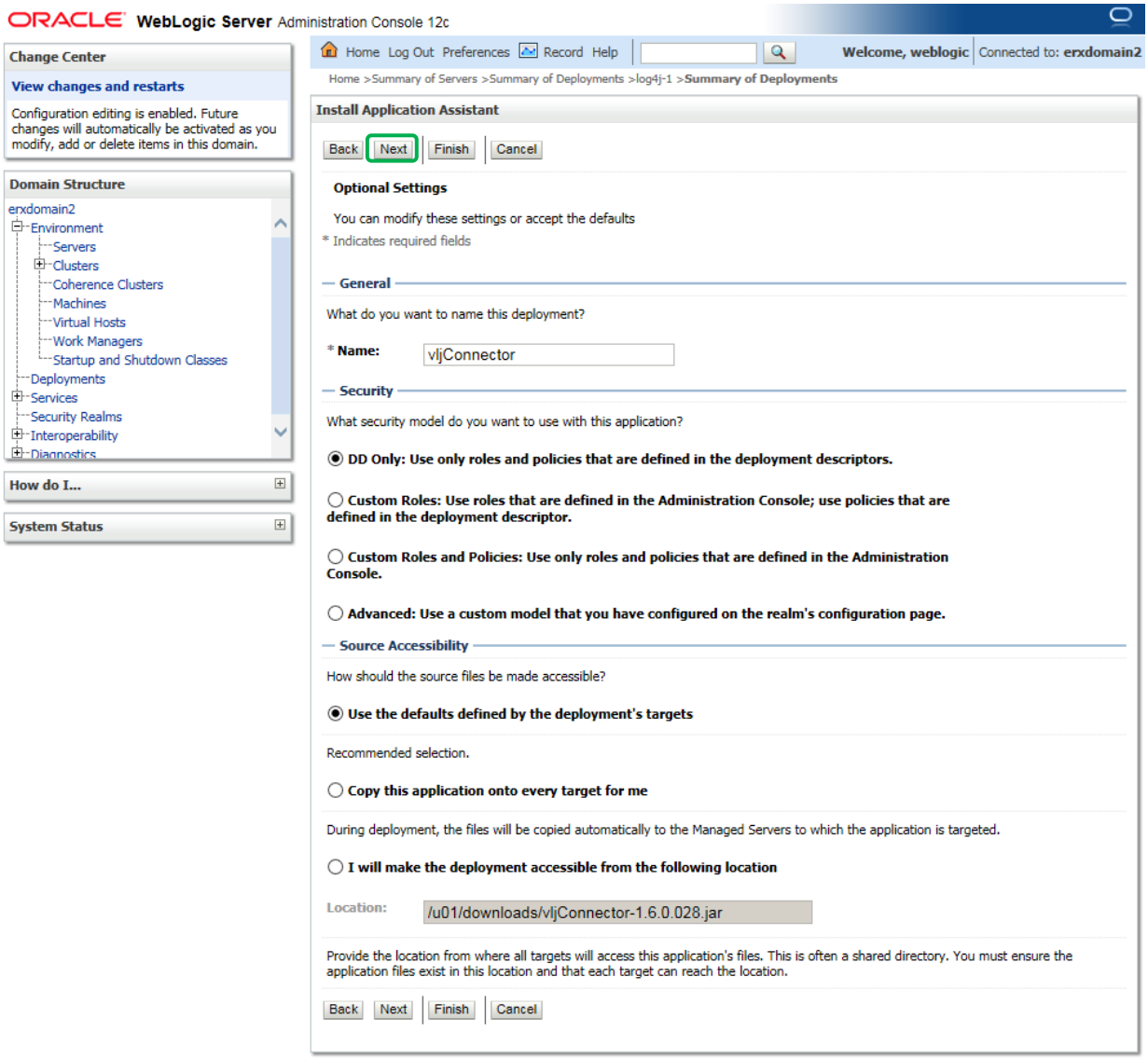
17. Select *All servers in the cluster* as the target for the deployment, and then click **Next**.

Figure 67: Deploy VistA Link Libraries – Select Deployment Targets



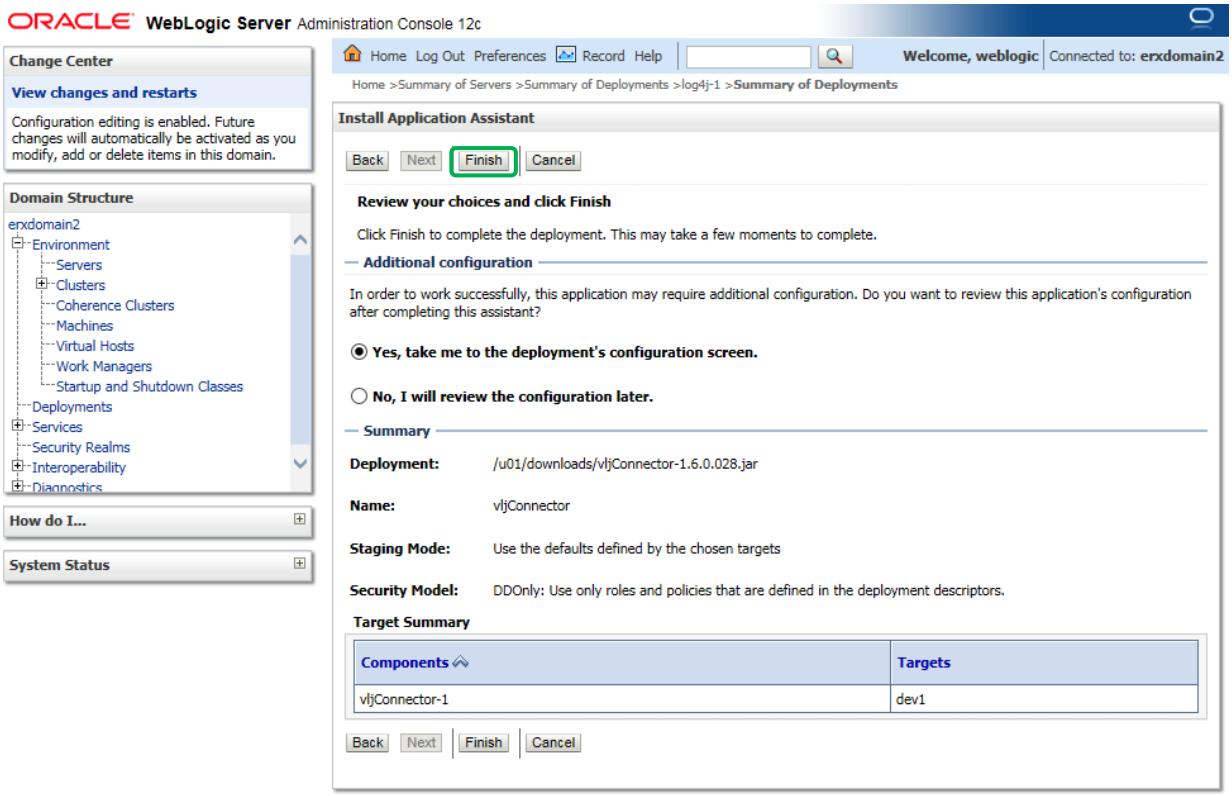
18. All of the values should appear as illustrated in the figure below.
19. Click **Next**.

Figure 68: Deploy VistA Link Libraries – Summary of Deployments Verification 1



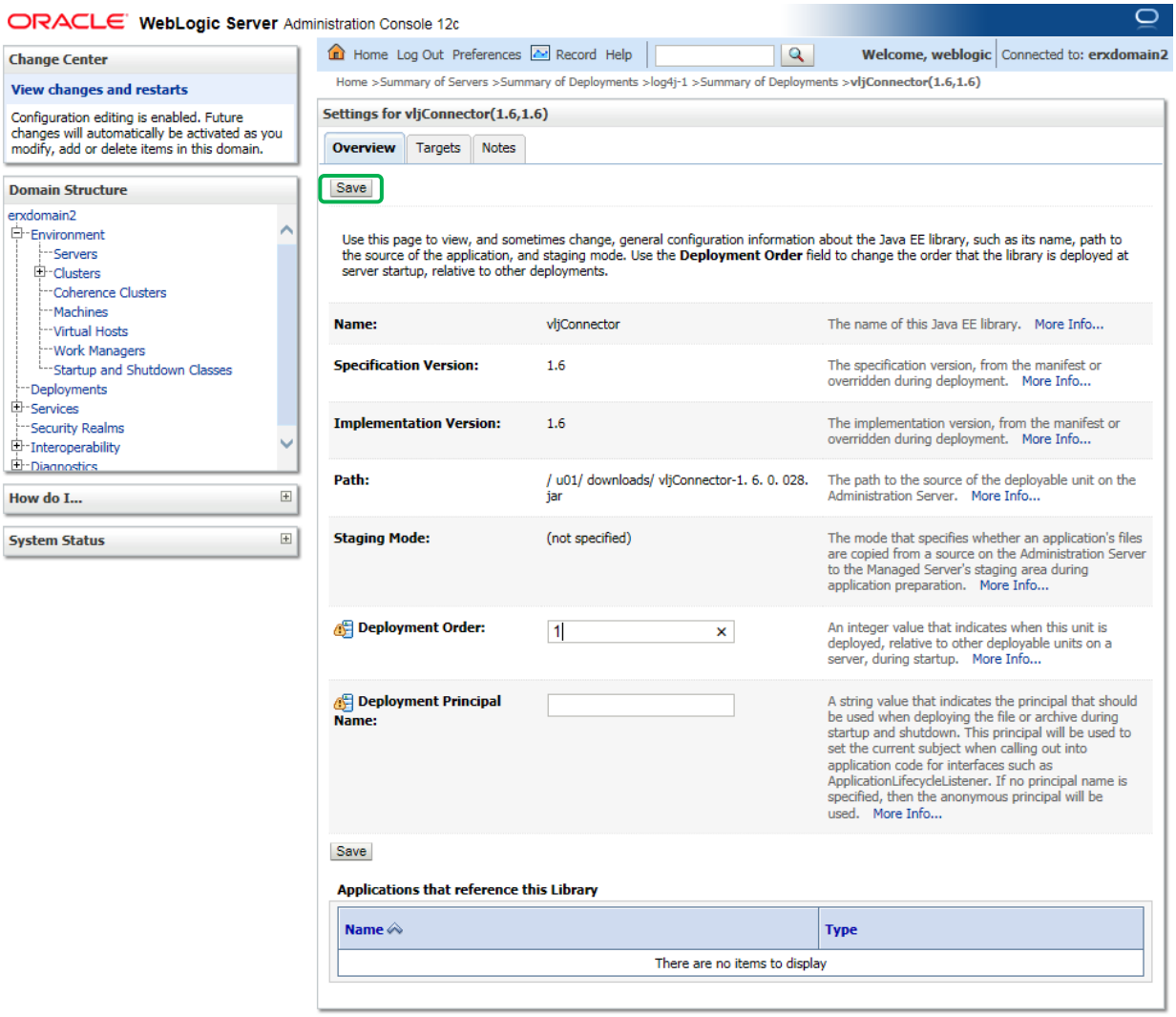
20. Verify that all of the values appear as illustrated in the figure below.
21. Click **Finish**.

Figure 69: Deploy VistA Link Libraries – Summary of Deployments Verification 2



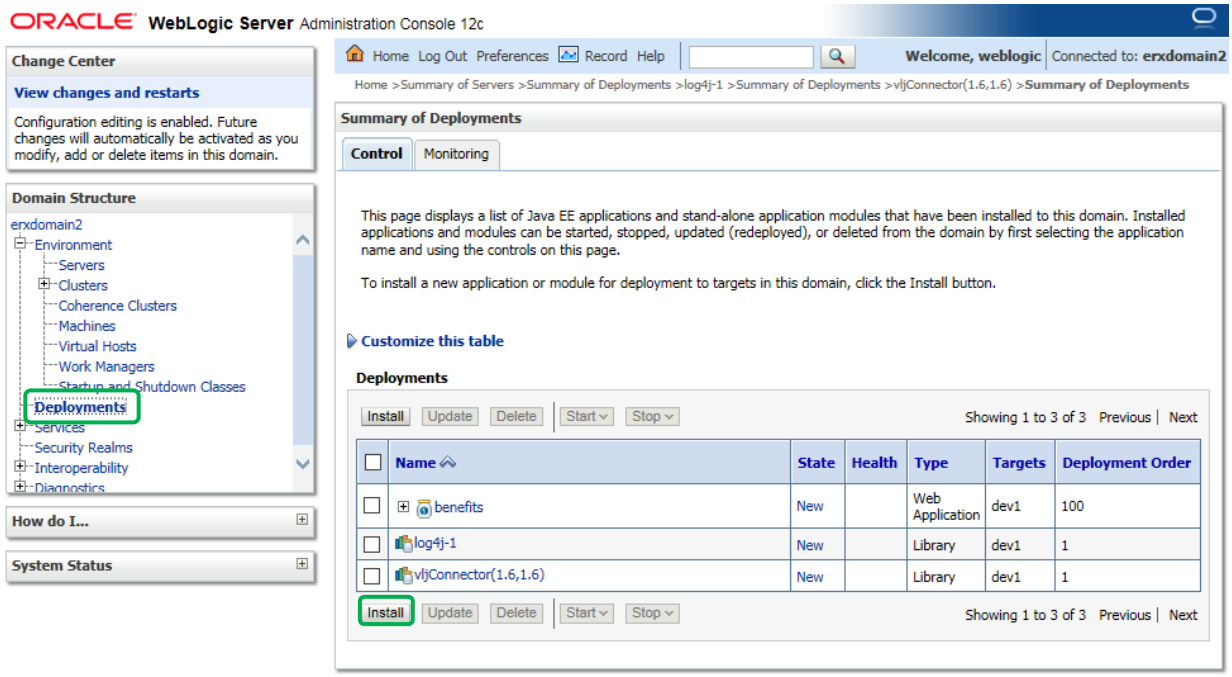
22. The **Deployment Configuration** screen should appear as illustrated in the below figure.
23. Enter *Deployment Order*: "1".
24. Click **Save**.

Figure 70: Deploy VistA Link Libraries – Deployment Configuration Screen



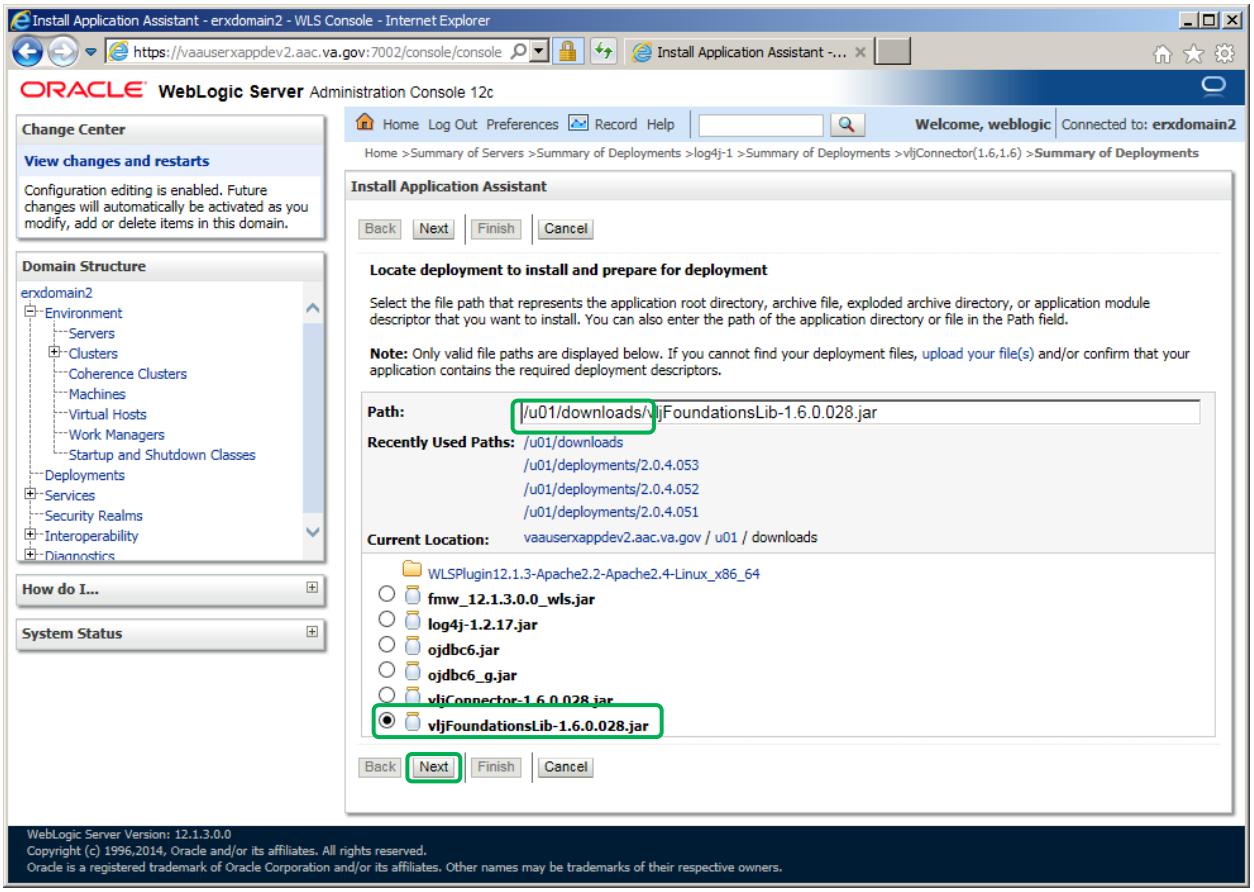
25. Navigate to the *Deployments* page.
26. From the *Deployments* screen, click **Install**.

Figure 71: Deploy VistA Link Libraries – Deployments



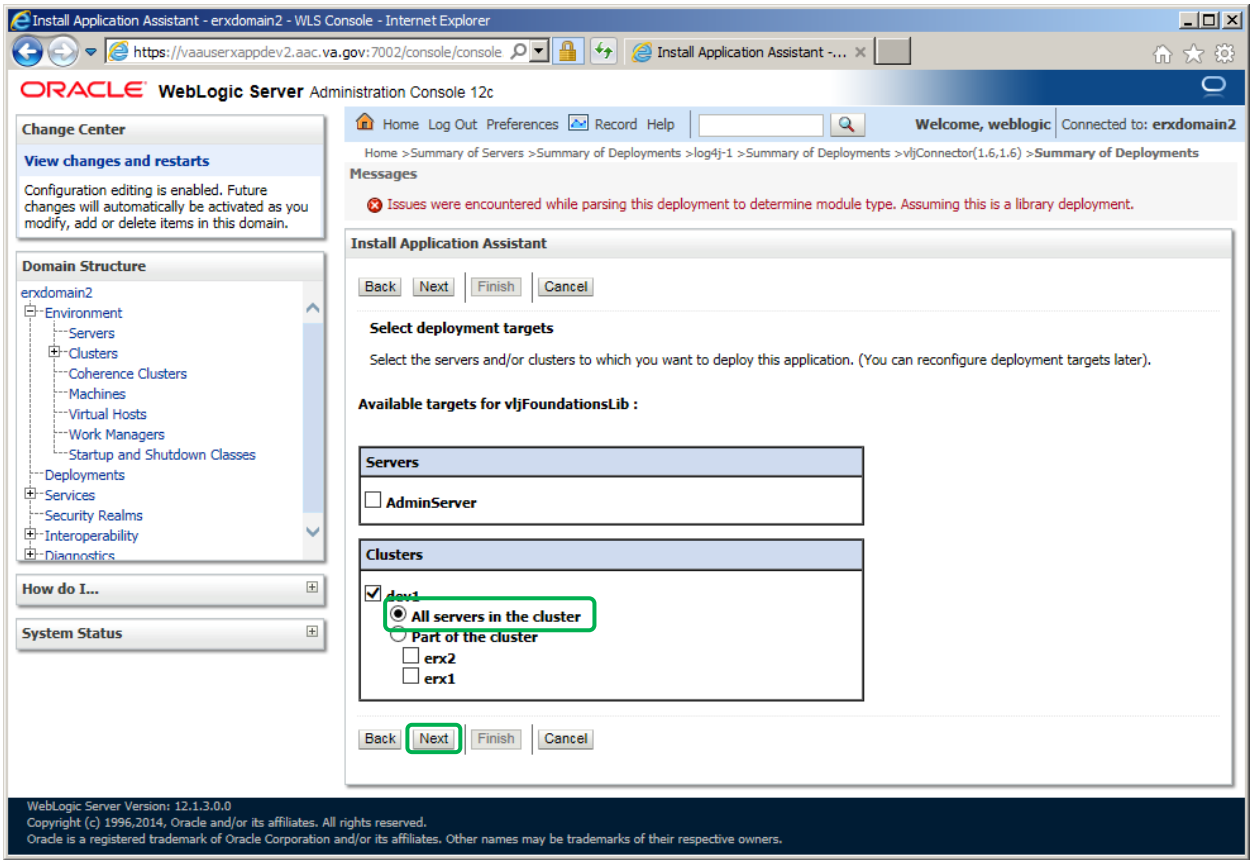
27. Enter *Path*: "/u01/downloads"
28. Install a new deployment of "log4j-1.2.17.jar" by selecting the jar file as indicated, and then click **Next**.

Figure 72: Deploy VistA Link Libraries – Select log4j Library to deploy



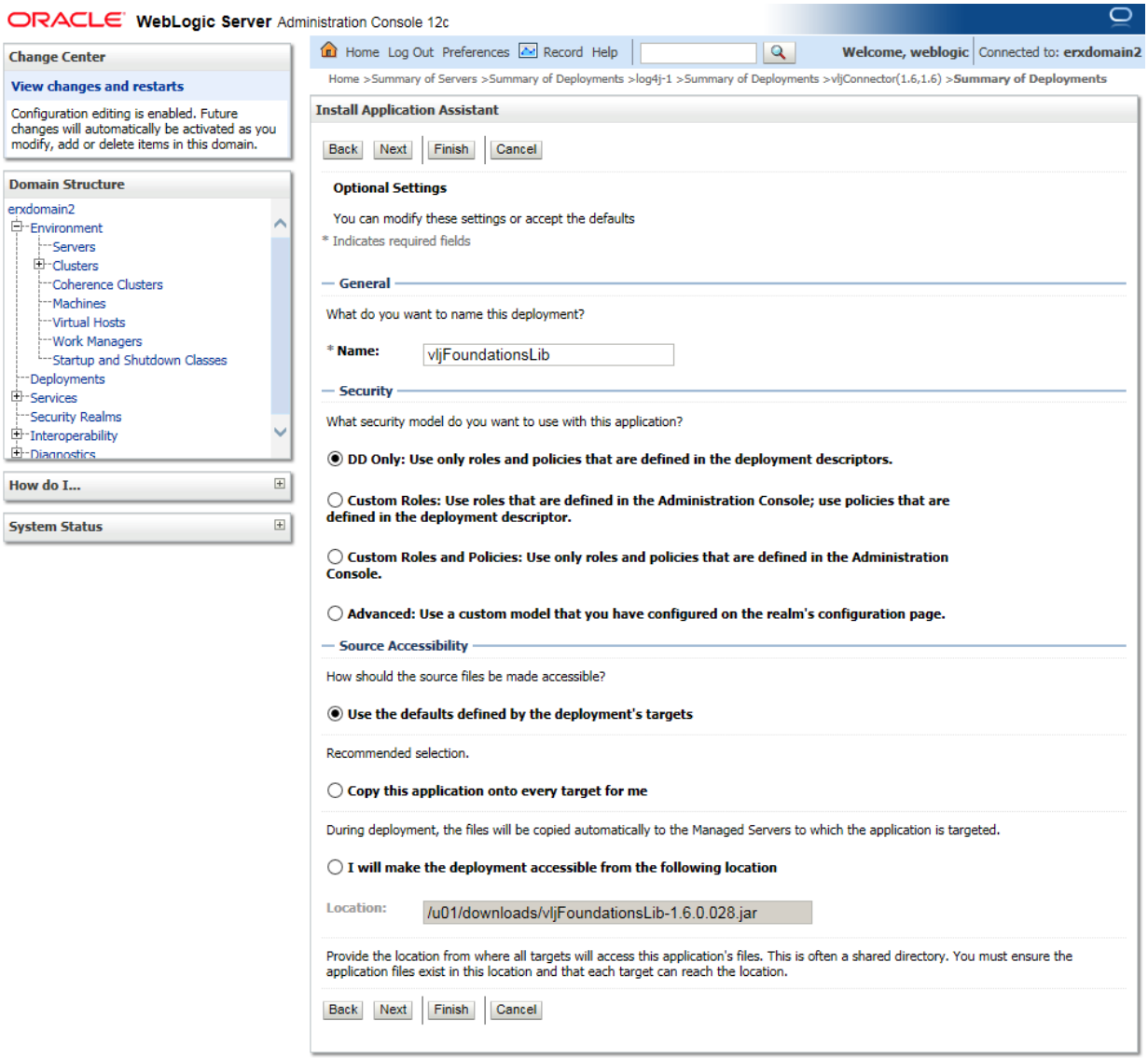
29. Select *All servers in the cluster* as the target for the deployment, and then click **Next**.

Figure 73: Deploy VistA Link Libraries – Select Deployment Targets



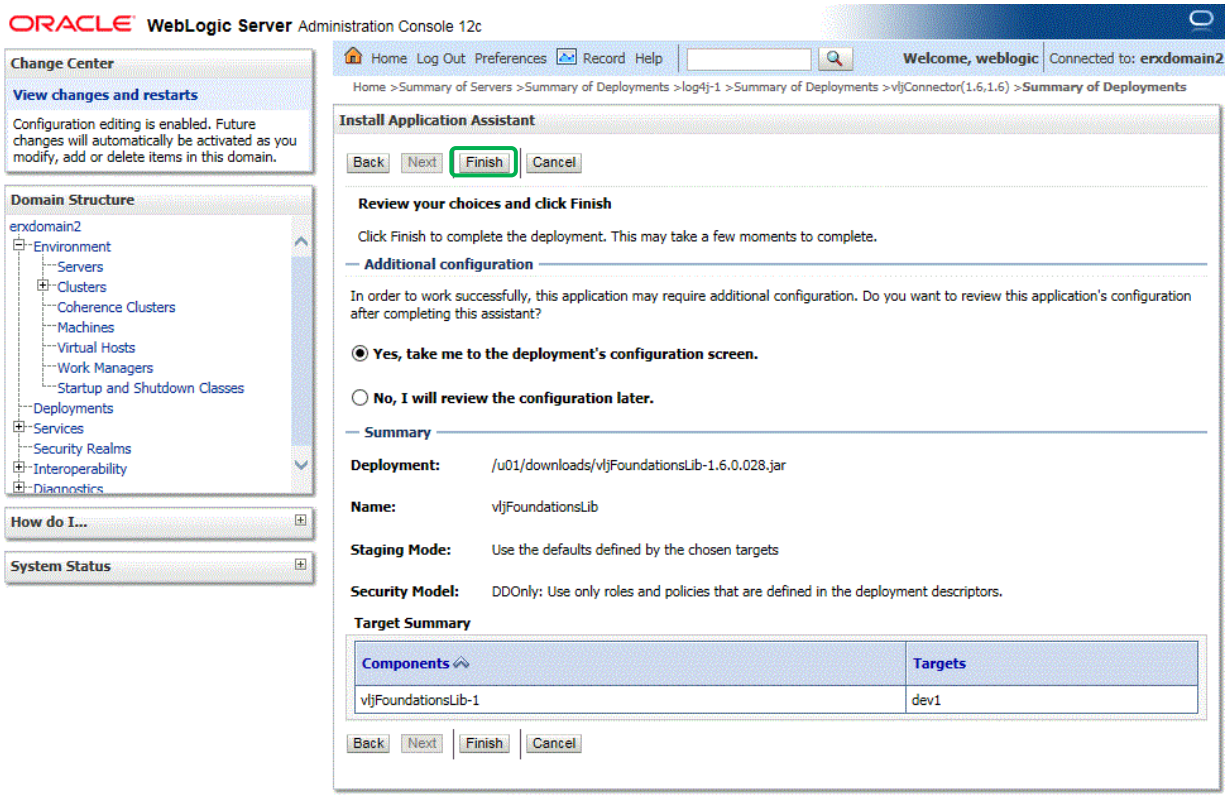
30. All of the values should appear as illustrated in the figure below.
31. Click **Next**.

Figure 74: Deploy VistA Link Libraries – Summary of Deployments Verification 1



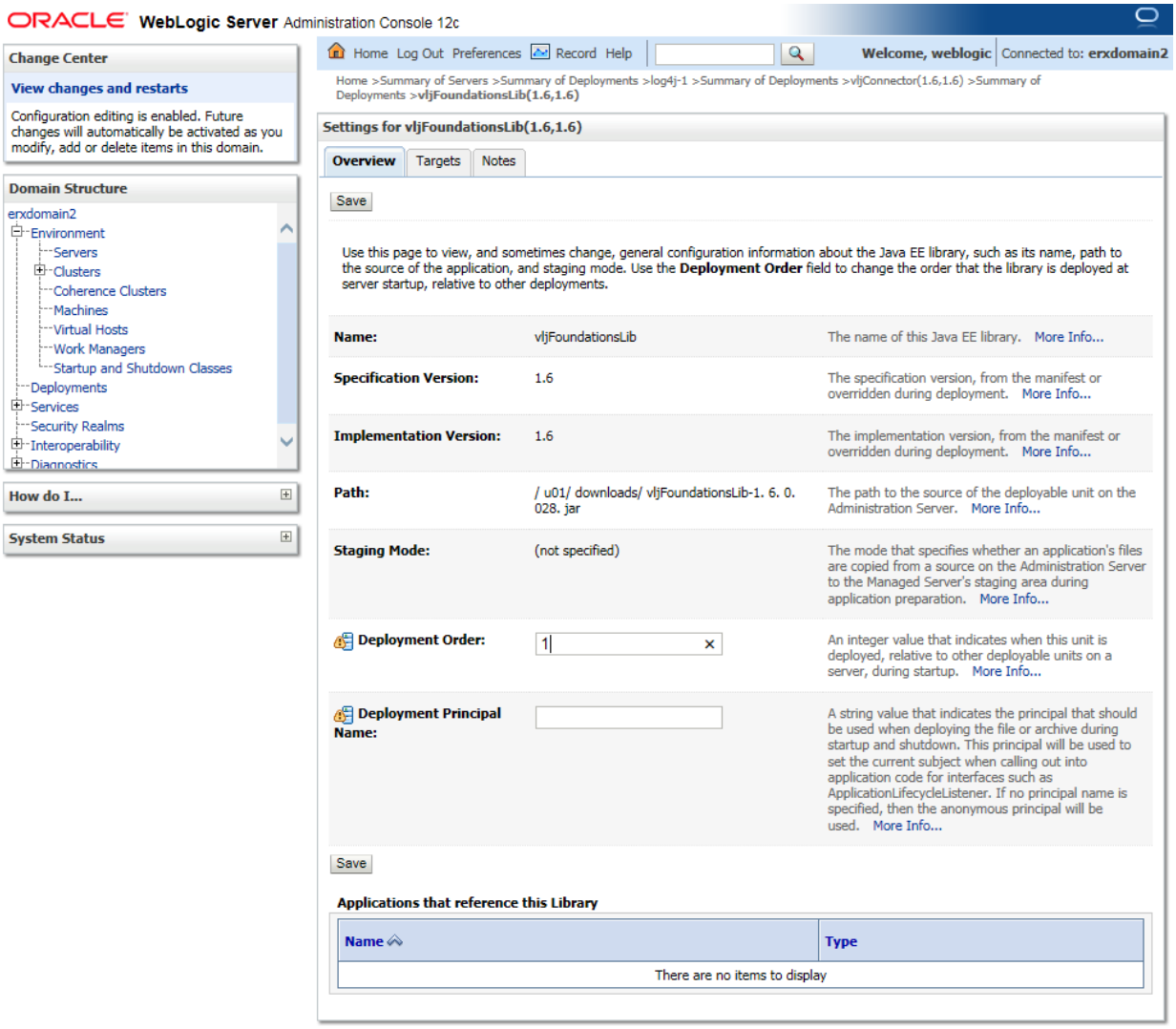
32. Verify that all of the values appear as illustrated in the figure below.
33. Click **Finish**.

Figure 75: Deploy VistA Link Libraries – Summary of Deployments Verification 2



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

Figure 76: Deploy VistA Link Libraries – Deployment Configuration Screen

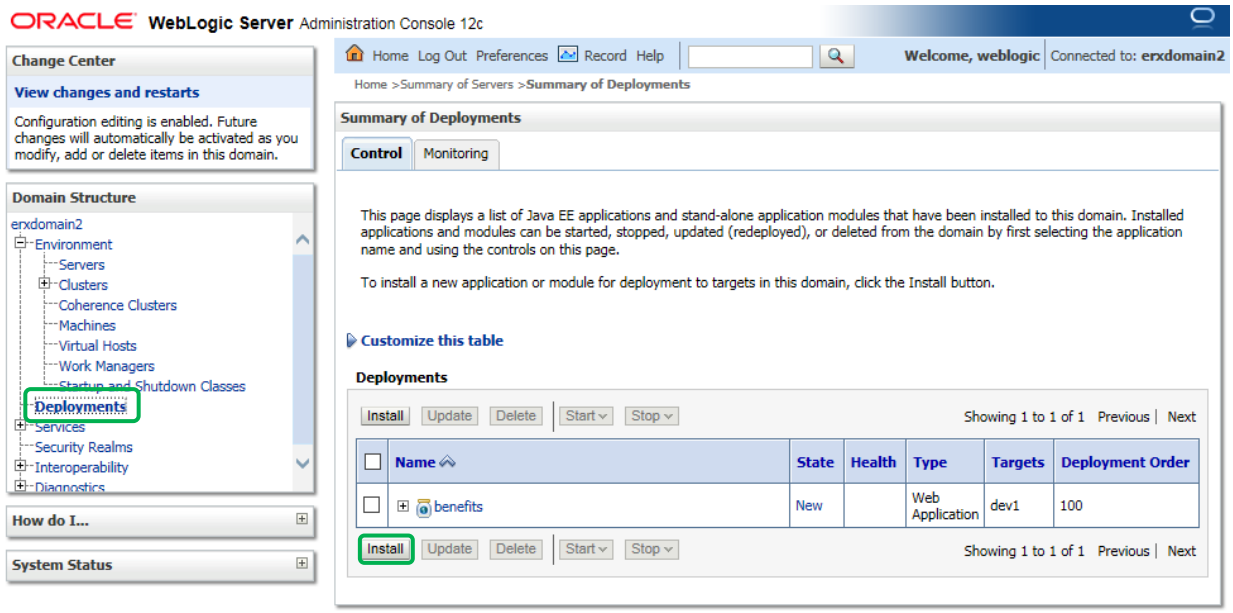


4.8.1.28 Deploy VistALink Adapters

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

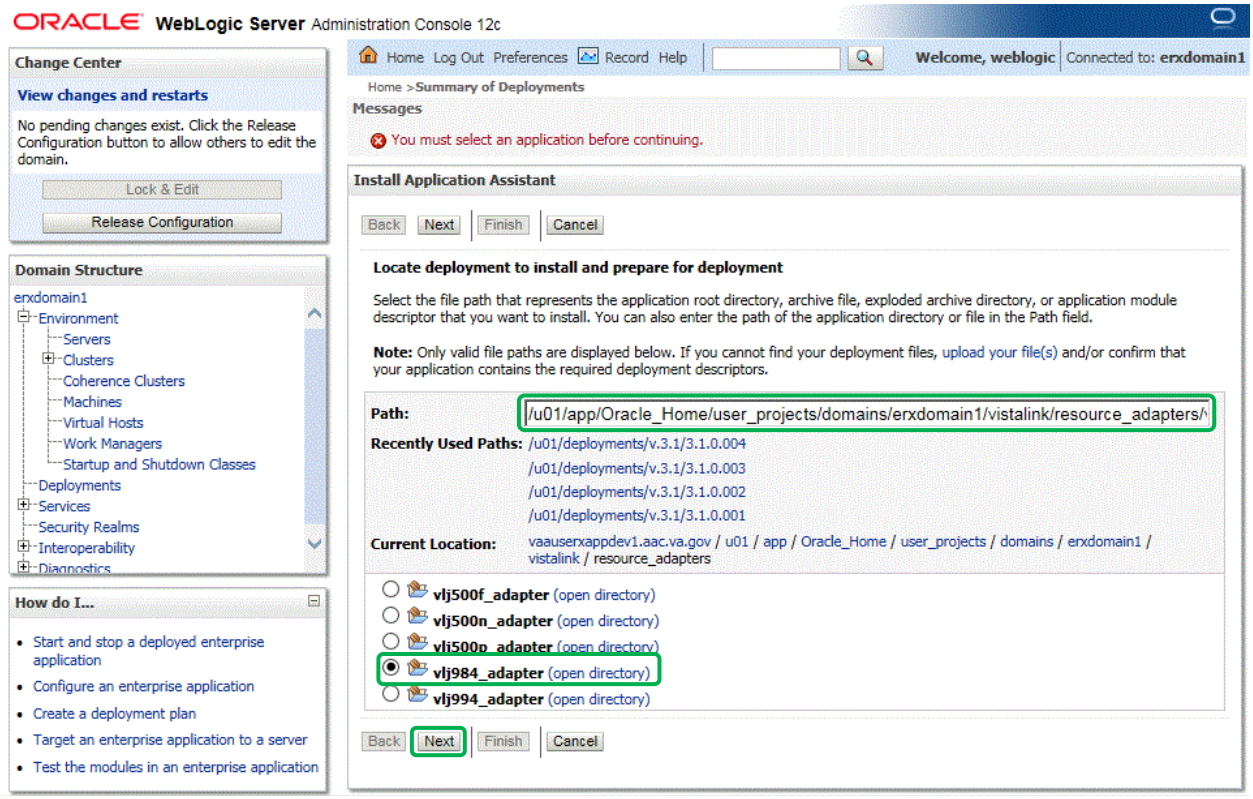
1. Create downloads directory if it doesn't exist (the following must be performed by a system administrator):
```
$ dzdo mkdir -p /u01/downloads
$ dzdo chown weblogic:weblogic /u01/downloads
$ dzdo chmod 777 /u01/downloads
```
2. Download the eRx/IEP Configurator (erx_iep_ x.x.x.xxx_configur_yyyymmdd _hhmmss.sh) to the downloads directory.
3. As your normal Linux login account, dzdo execute the eRx/IEP Configurator (erx_iep_ x.x.x.xxx_configur_yyyymmdd _hhmmss.sh) (the following must be performed by a system administrator):
```
$ dzdo /u01/downloads/erx_iep_ x.x.x.xxx_configur_yyyymmdd _hhmmss.sh
```
4. Select option 3 and 5 then Exit (x).
5. The WebLogic Administrator stops the VM1 managed server, per section: **Error! R eference source not found.**, step **Error! Reference source not found.**
6. The System Administrator executes the eRx/IEP Configurator script containing adapter configuration on VM1, menu options 1, 2 and 3.
7. The WebLogic Administrator will start the VM1 managed server, per section 7.1.2.
8. The WebLogic Administrator stops the VM2 managed server, per section: **Error! R eference source not found.**, step **Error! Reference source not found.**
9. The System Administrator executes the eRx/IEP Configurator script containing adapter configuration on VM2, menu options 1, 2 and 3.
10. The WebLogic Administrator will start the VM2 managed server, per section 7.1.2.
11. The WebLogic navigates to the *Deployment*s screen, click **Install**.

Figure 77: Deploy VistALink Adapter – Deployments



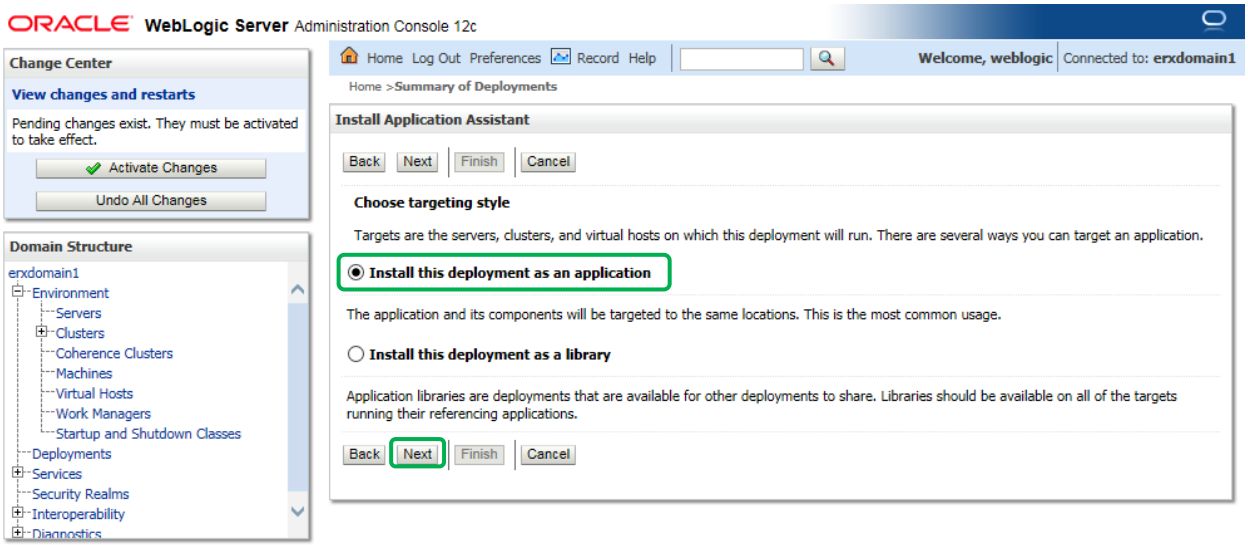
1. Enter *Path*: "***[DOMAIN_HOME]***/vistalink/resource_adapters", press enter.
2. Select the desired vljXXX_adapter to be installed, and then click **Next**.

Figure 78: Deploy VistALink Adapter – Select vljxxx_apapter to install



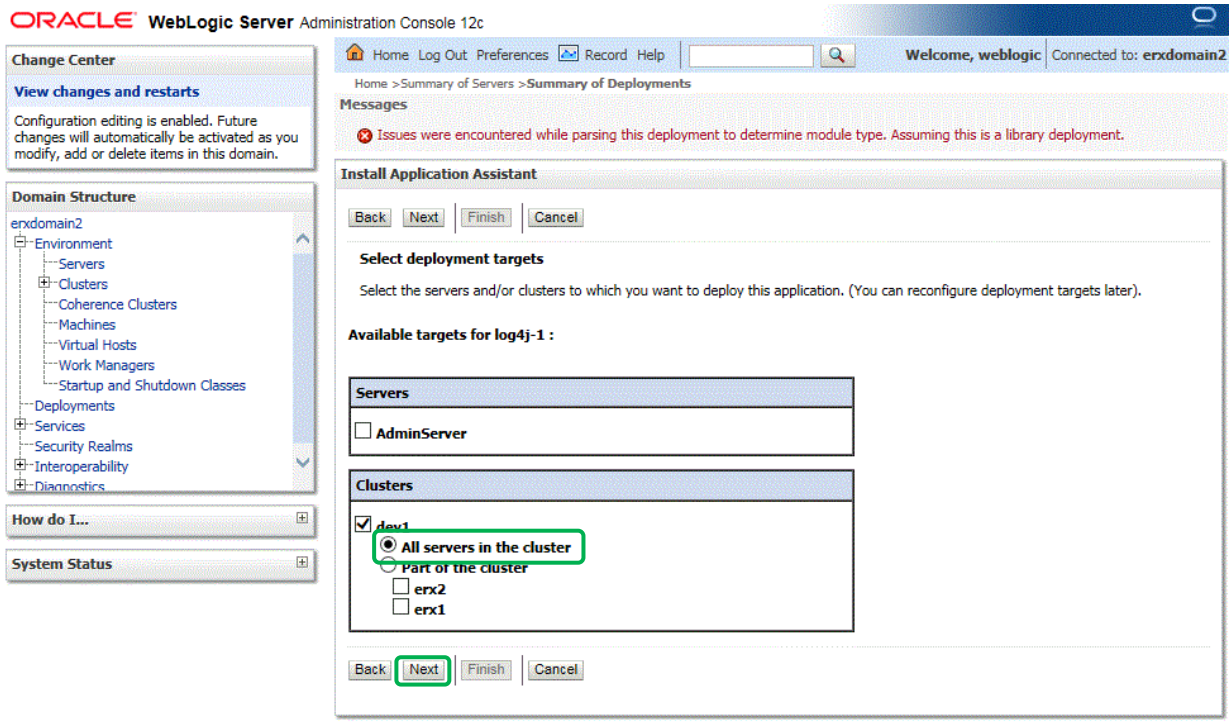
3. Select *Install this deployment as an application* as the target for the deployment, and then click **Next**.

Figure 79: Deploy VistALink Adapter – Select Deployment Type



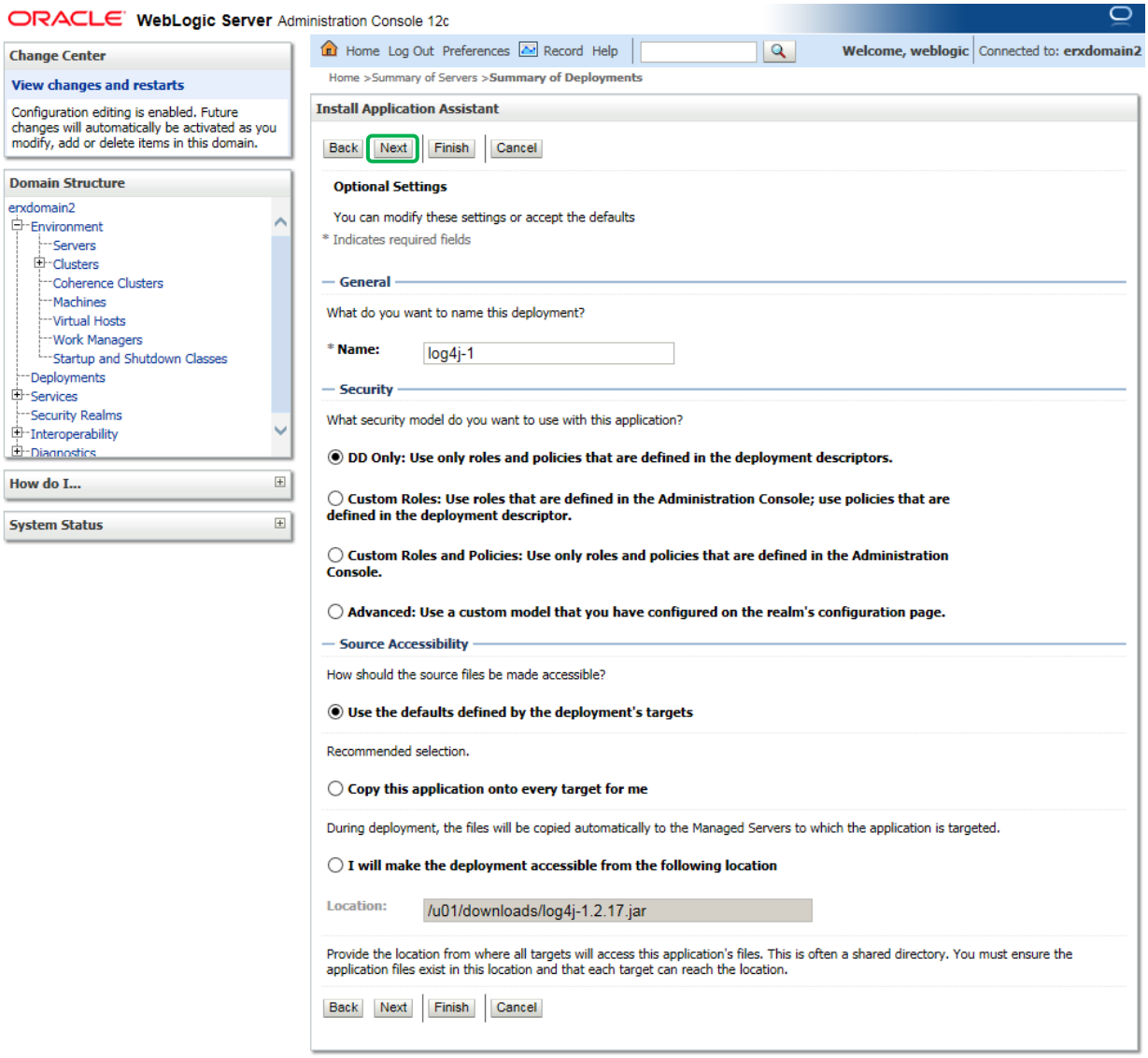
4. Select *All servers in the cluster* as the target for the deployment, and then click **Next**.

Figure 80: Deploy VistALink Adapter – Select Deployment Targets



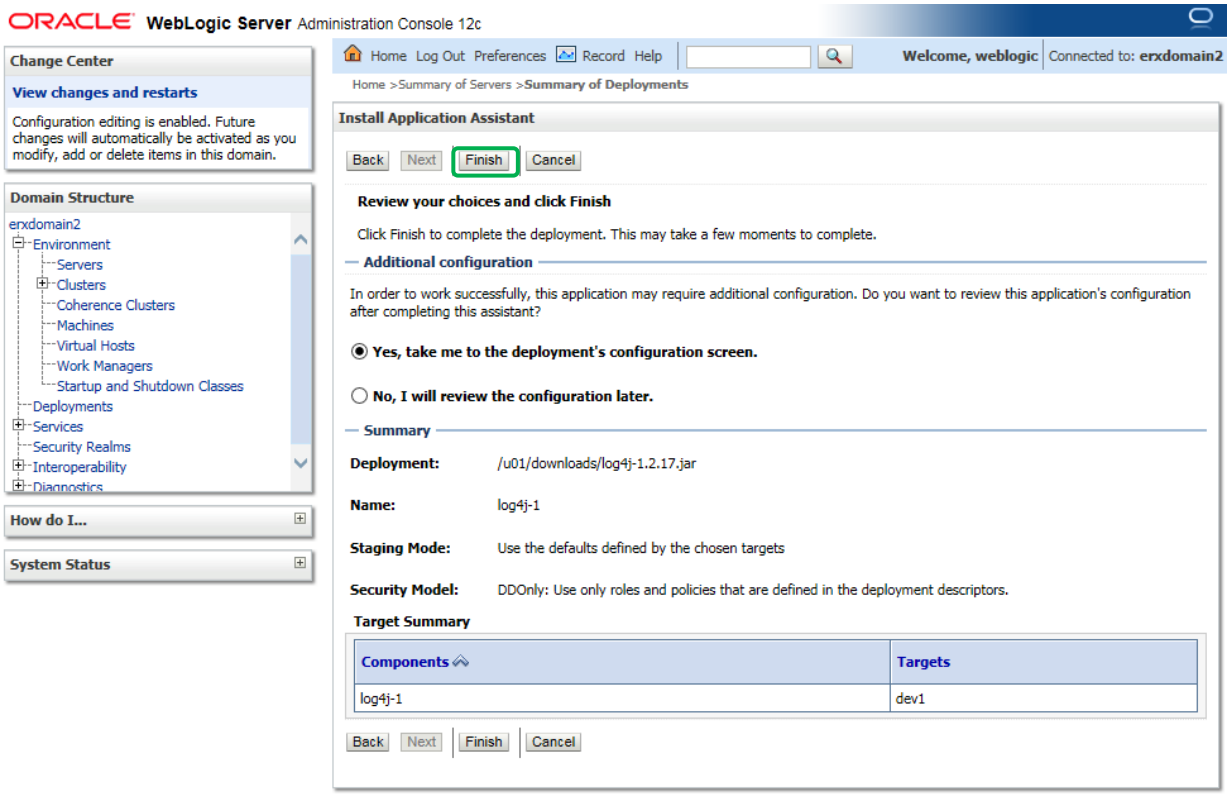
5. All of the values should appear as illustrated in the figure below.
6. Click **Next**.

Figure 81: Deploy VistALink Adapter – Adapter Optional Settings



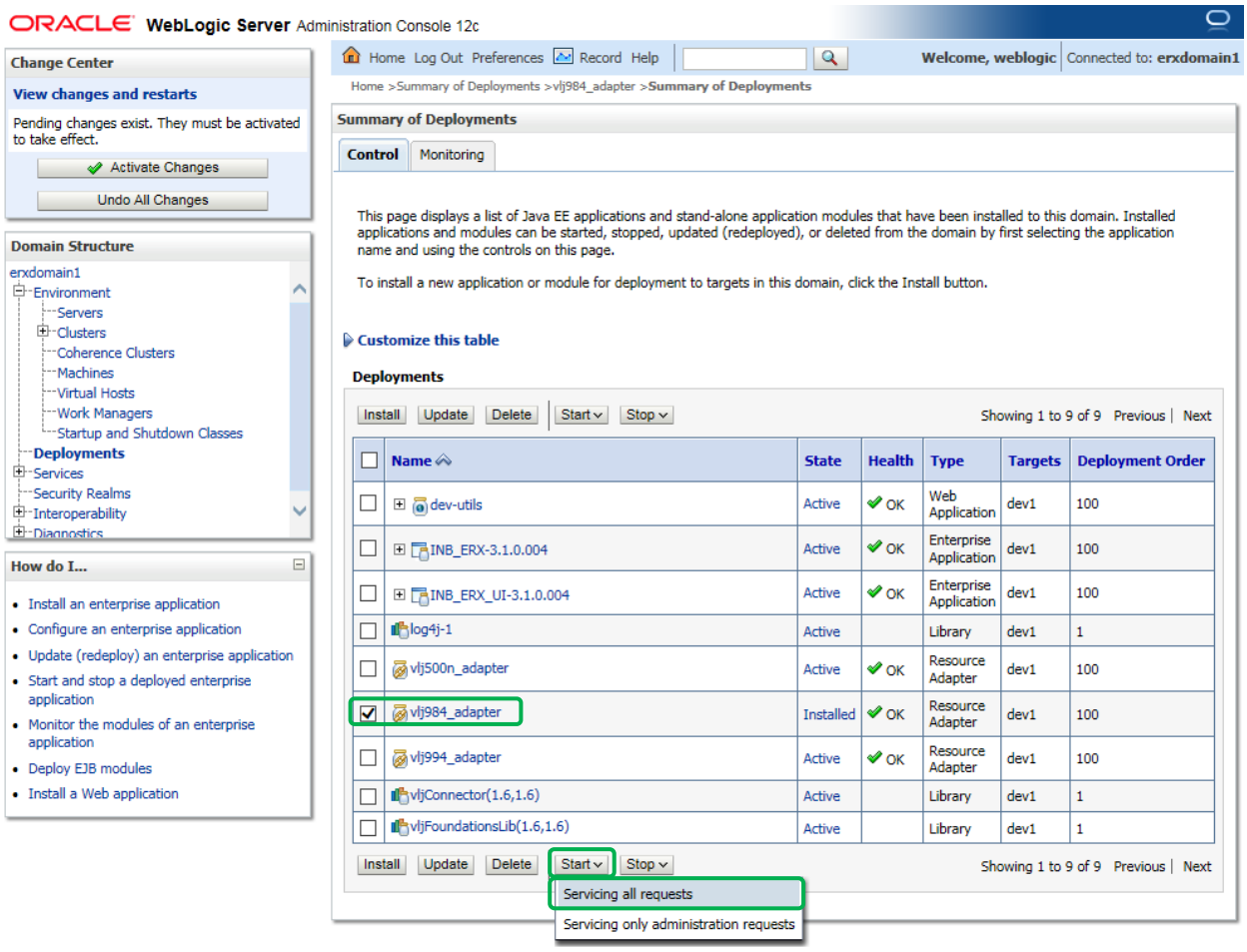
7. Verify that all of the values appear as illustrated in the figure below.
8. Click **Finish**.

Figure 82: Deploy VistALink Adapter – Finish Adapter Installation



9. Navigate to Deployments, select the vljXXX_adapter, click Start > Servicing all Requests.

Figure 83: Deploy VistALink Adapter – 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.

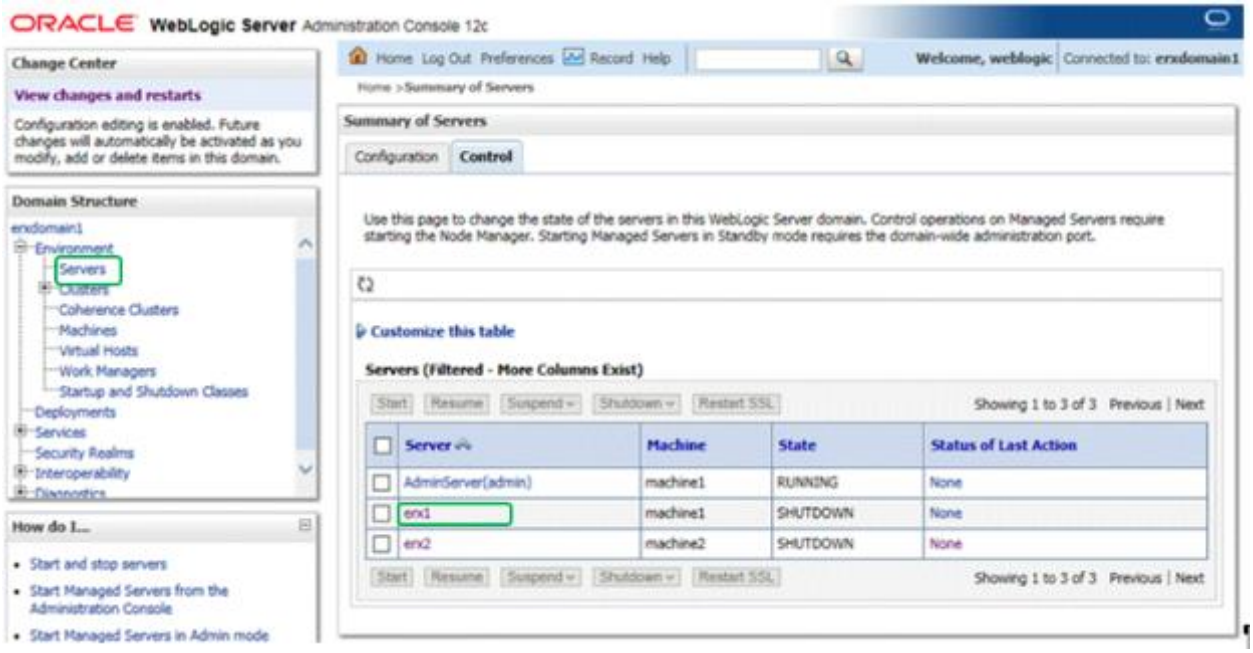
4.8.2.1 Install Inbound eRx Application

1. Create downloads directory if it doesn't exist (the following must be performed by a system administrator):
```
$ dzdo mkdir -p /u01/downloads
$ dzdo chown weblogic:weblogic /u01/downloads
$ dzdo chmod 777 /u01/downloads
```
2. Download the eRx/IEP Configurator (erx_iep_ x.x.x.xxx_deploy_yyyymmdd _hhmmss.sh) to the downloads directory.
3. As your normal Linux login account, dzdo execute the eRx/IEP Configurator (erx_iep_ x.x.x.xxx_deploy_yyyymmdd _hhmmss.sh) (the following must be performed by a system administrator):
```
$ dzdo /u01/downloads/erx_iep_ x.x.x.xxx_configur_yyyymmdd _hhmmss.sh
```
4. Select option 3, 5 and 6 then Exit (x).
5. Shut down WebLogic (refer to Sections 4.8.2.3 and 4.8.2.4).
6. As your normal Linux login account, dzdo su to the weblogic account:
```
$ dzdo su - weblogic
```
7. Create the downloads directory if it doesn't exist:
```
$ mkdir -p /u01/downloads
```
8. Download Inbound eRx application to the downloads directory.

   Download from AITC IEP eRx Downloads directory
9. Create the deployments directory if it doesn't exist:
```
$ mkdir -p /u01/deployments
```
10. Copy the application EAR to the deployments directory:

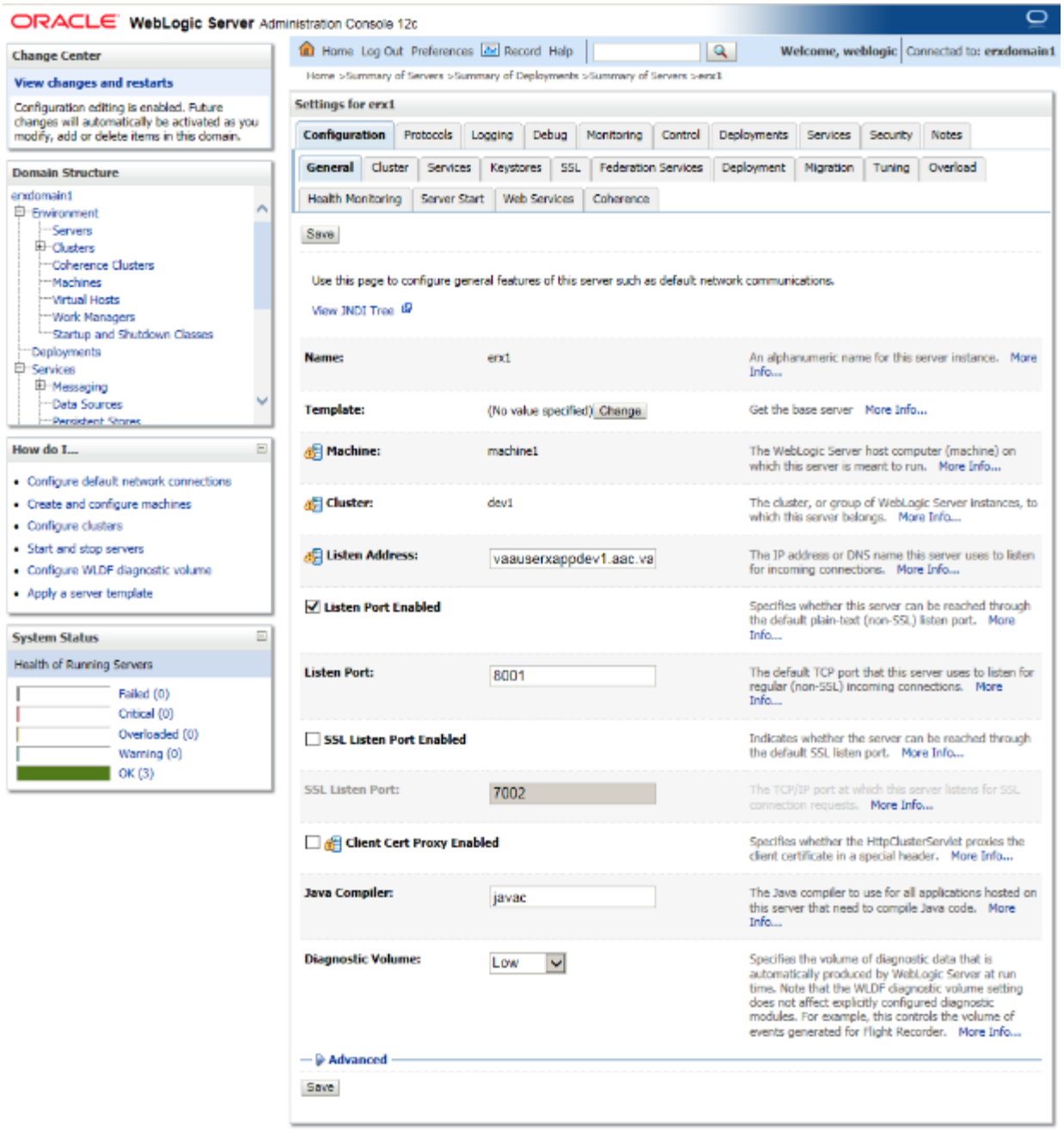
    Download from AITC IEP eRx Downloads directory
11. Access the WebLogic Admin Console by directing a browser to: https://***[vm1_fqdn]***:7002/console/ and log in with the "weblogic" account.
12. Navigate to the **Servers** page.
13. From the **Administration Console** > **Servers** page, click the "erx1" link to configure the server.

Figure 84: Install Inbound eRx Application – Configure Servers



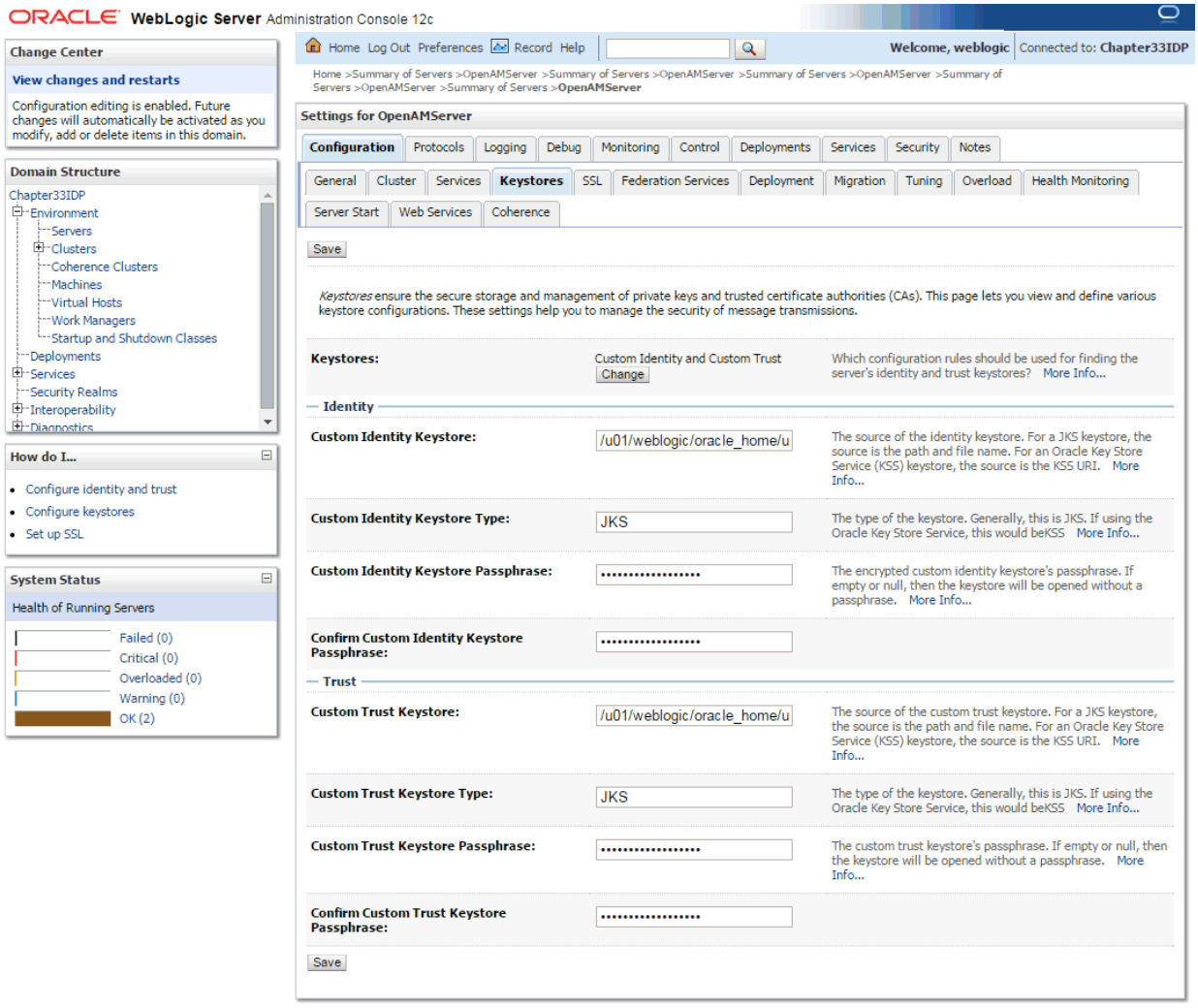
14. The server configuration screen should appear as shown in the figure below.
15. Inspect the settings under the **General** tab. The *Listen Address* should be ***[vm1_fqdn]***. The non-secure listening port (*Listen Port Enabled*) should be enabled and set to port "8001" (*Listen Port*). The secure 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 85: Install Inbound eRx Application – Verify Server Settings



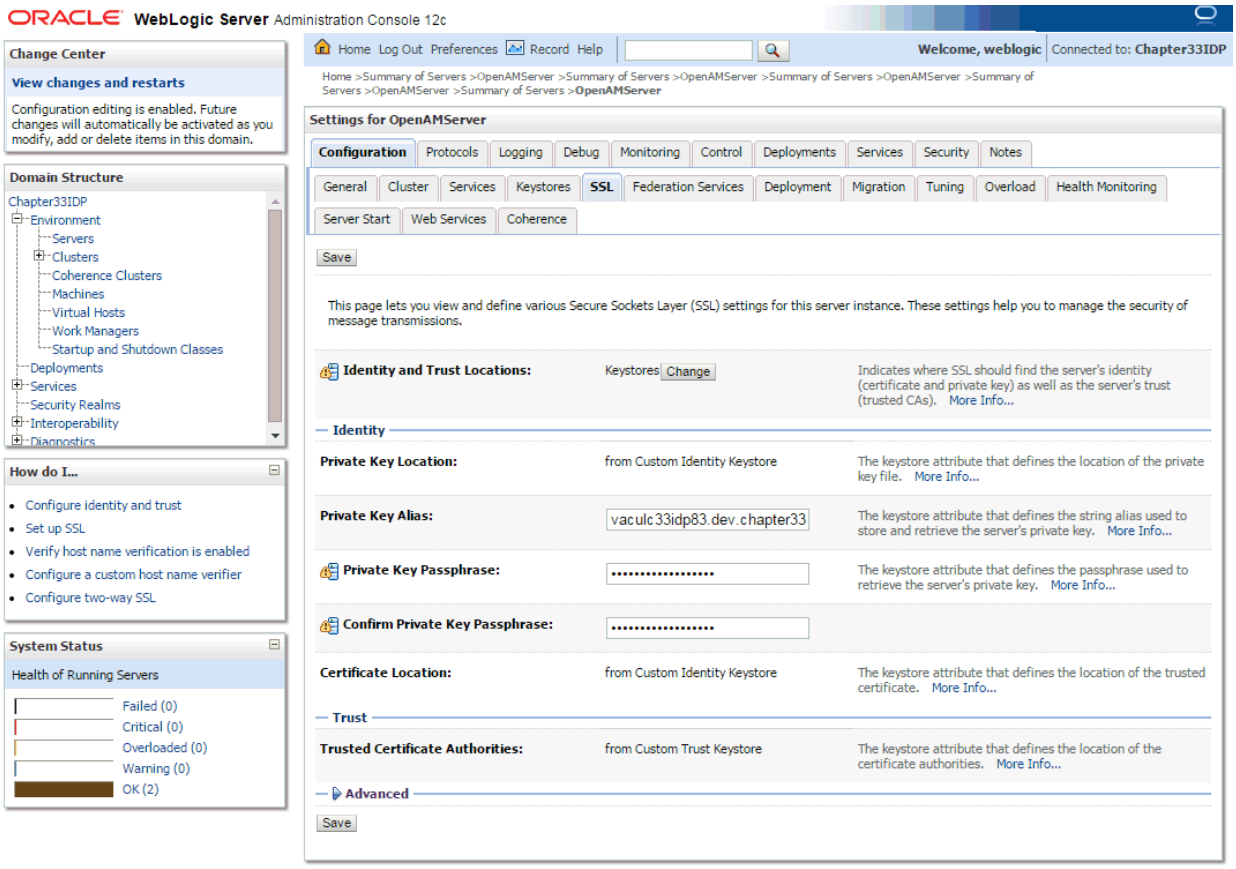
16. Review the setting under the **Keystores** tab as illustrated in the figure below. Verify the *Keystores* option is set to "Custom Identity and Custom Trust", and that the fields under the *Identity* and *Trust* sections are filled with the same corresponding values.

Figure 86: Install Inbound eRx Application – Verify General & Keystore Settings



17. Verify the settings under the **SSL** tab. The *Private Key Alias* should be the Fully Qualified Domain Name of the server, and the *Passphrase* is ########.

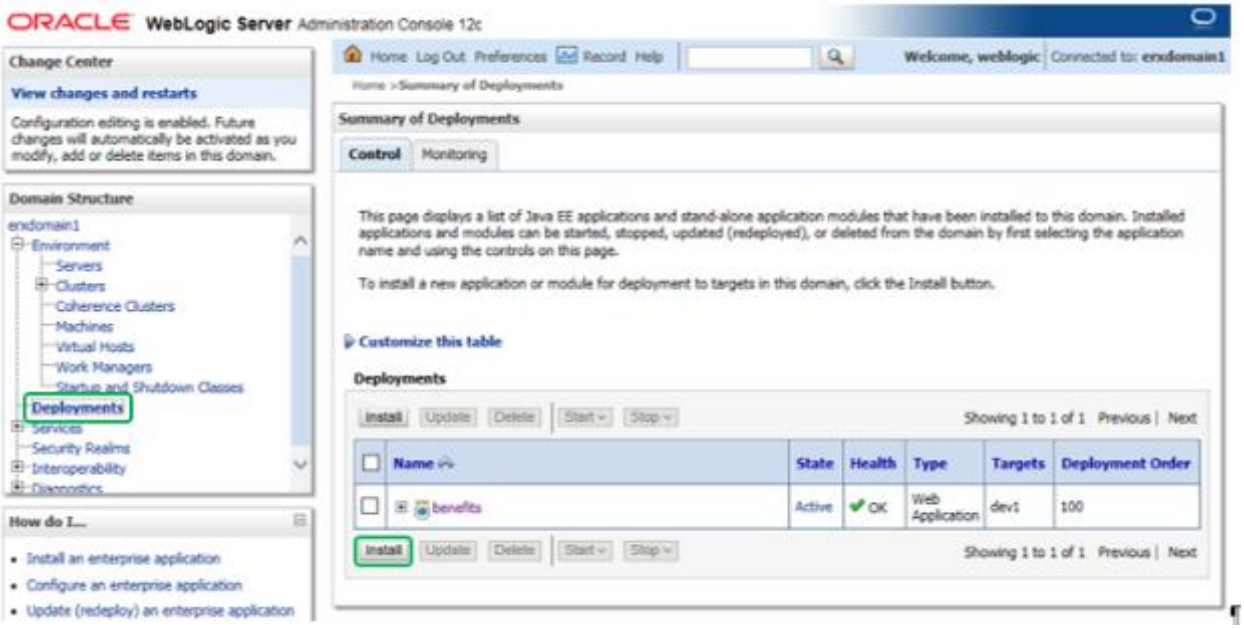
Figure 87: Install Inbound eRx Application – Verify SSL Settings



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

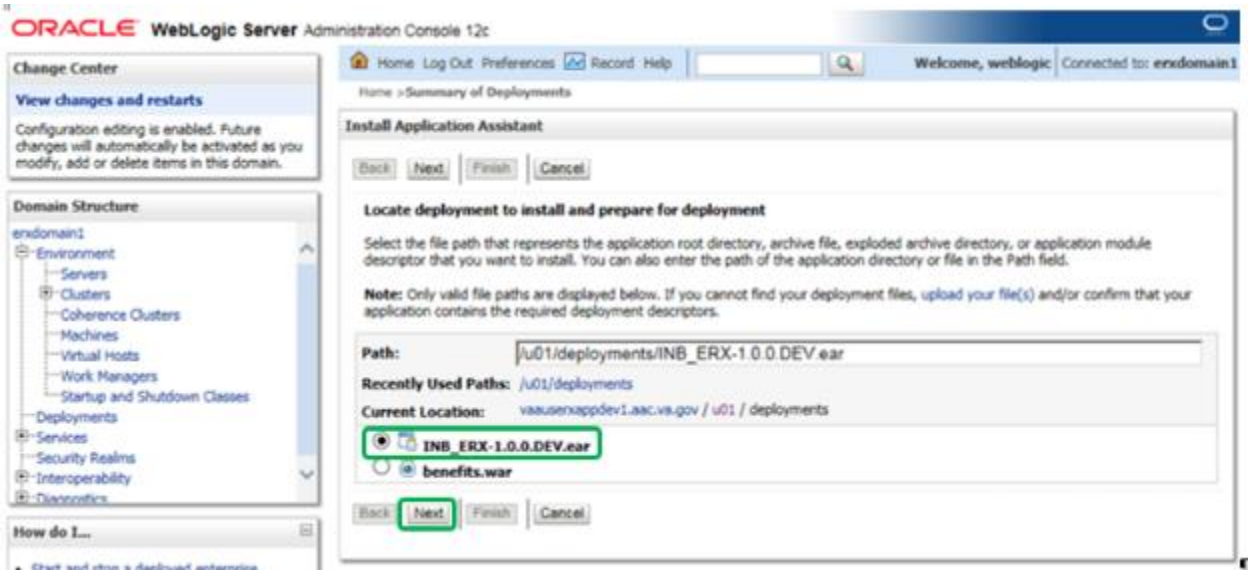
19. Navigate to the **Deployments** page.
20. From the **Deployments** page, click **Install**.

Figure 88: Install Inbound eRx Application – Summary of Deployments



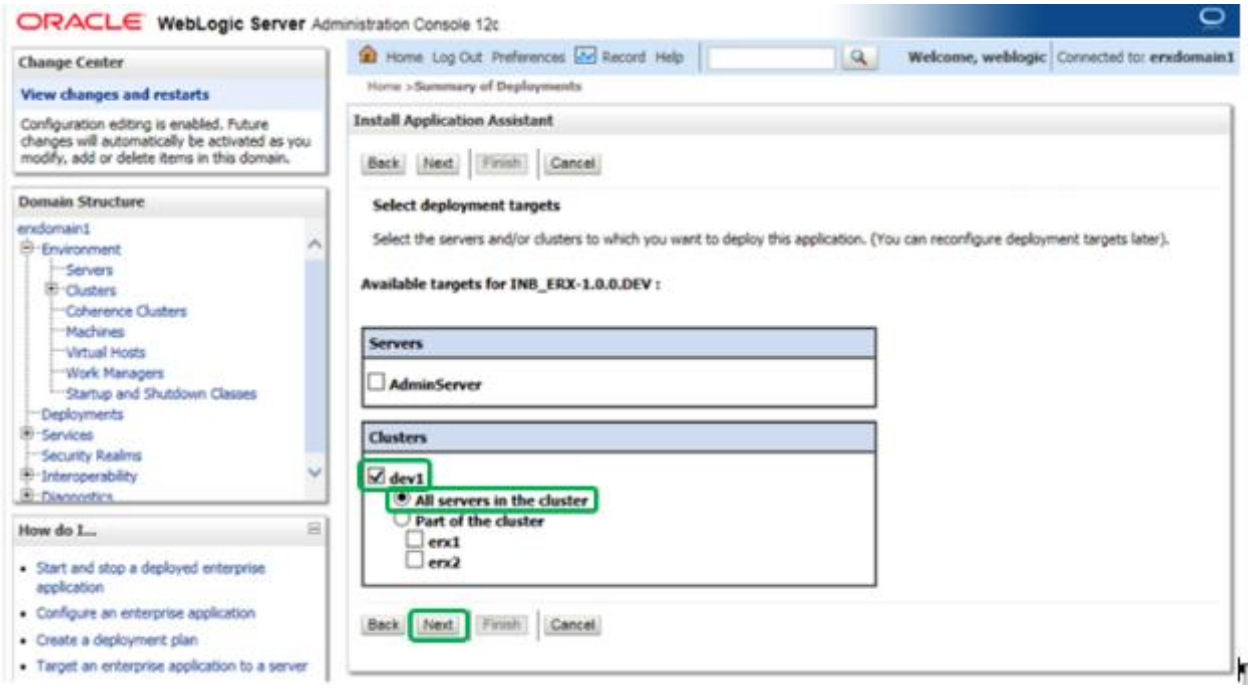
21. Install a new deployment of INB_ ERX-3.1.0.005.ear using the WAR file as indicated in the figure below.
22. Click **Next**.

Figure 89: Install Inbound eRx Application – Install New Deployment of INB_ERX



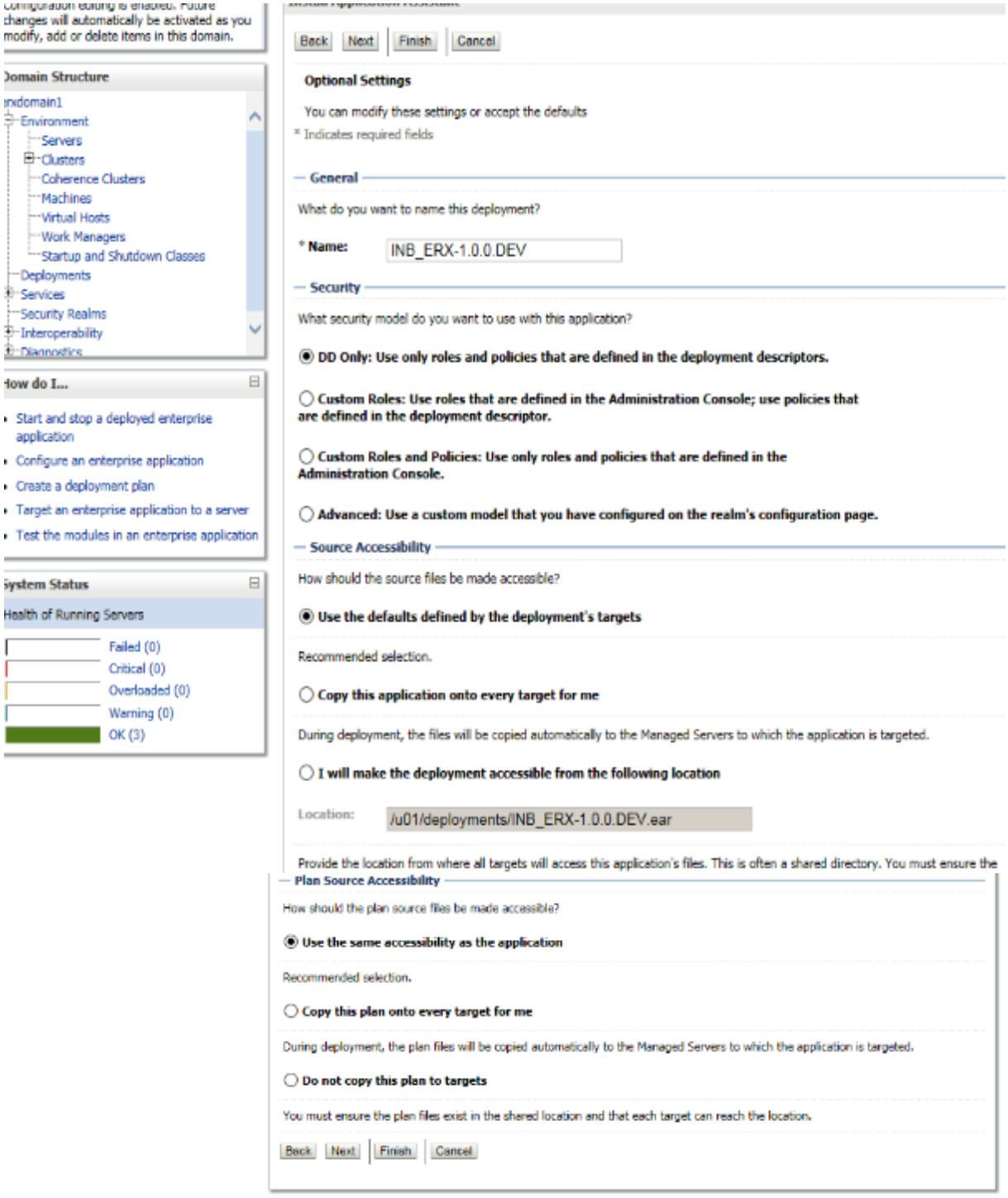
23. Accept the defaults for an application deployment.
24. Click **Next**.
25. Select the cluster and "All servers in the cluster" as the target for the deployment.
26. Click **Next**.

Figure 90: Install Inbound eRx Application – Select INB_ERX Deployment Targets



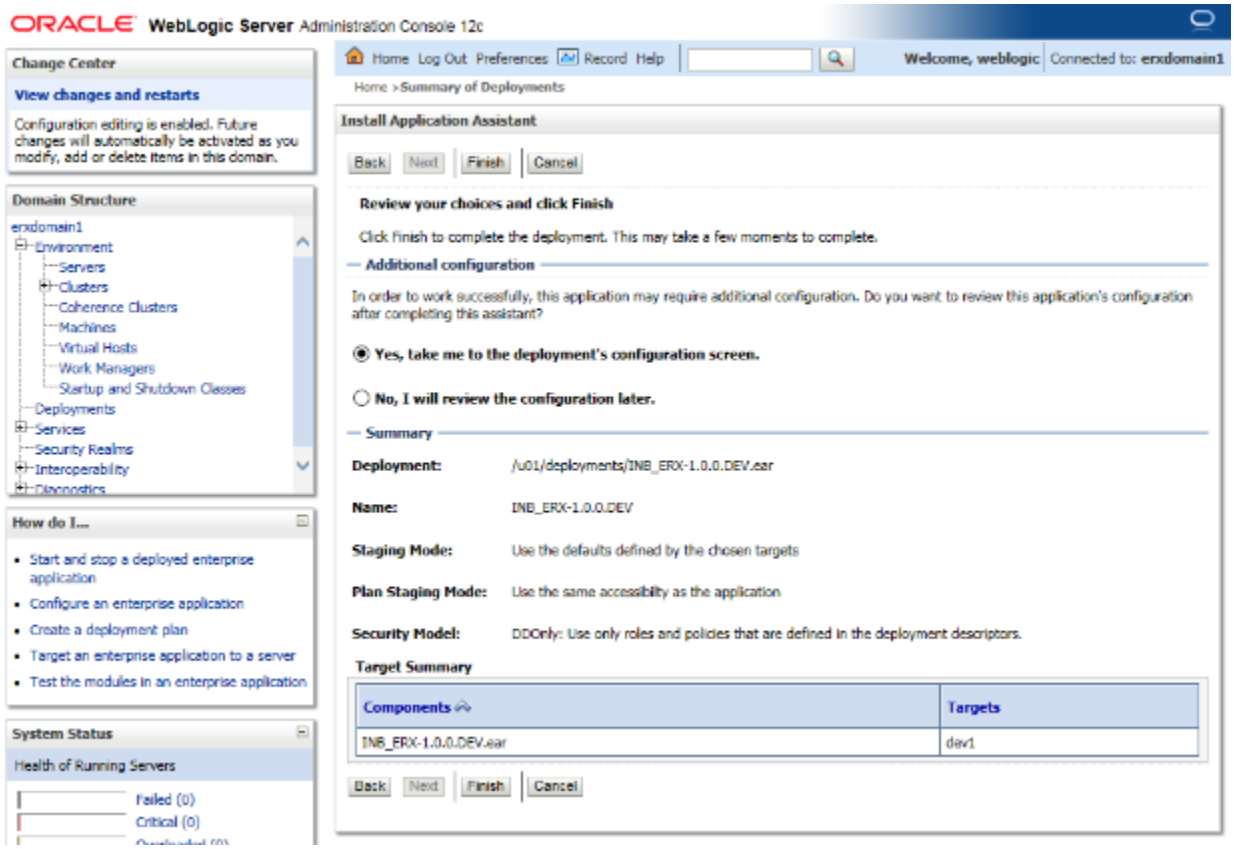
27. All of the values should appear as illustrated in the figure below.
28. Click **Next**.

Figure 91: Install Inbound eRx Application – Verify INB_ERX Deployment Settings



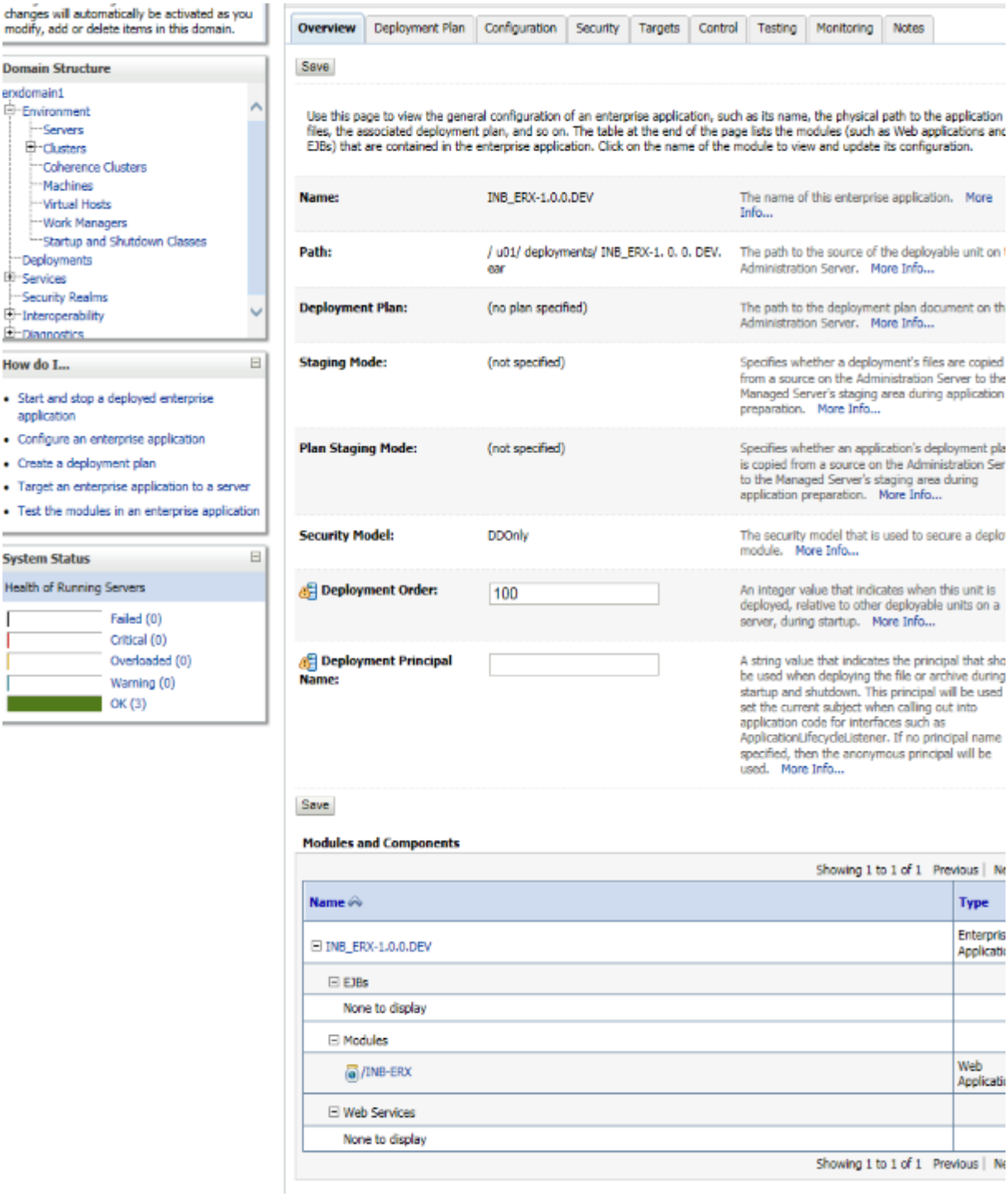
29. All of the values should appear as illustrated in the figure below.
30. Click **Finish**.

Figure 92: Install Inbound eRx Application – Verify INB_ERX Deployment Settings (Finish)



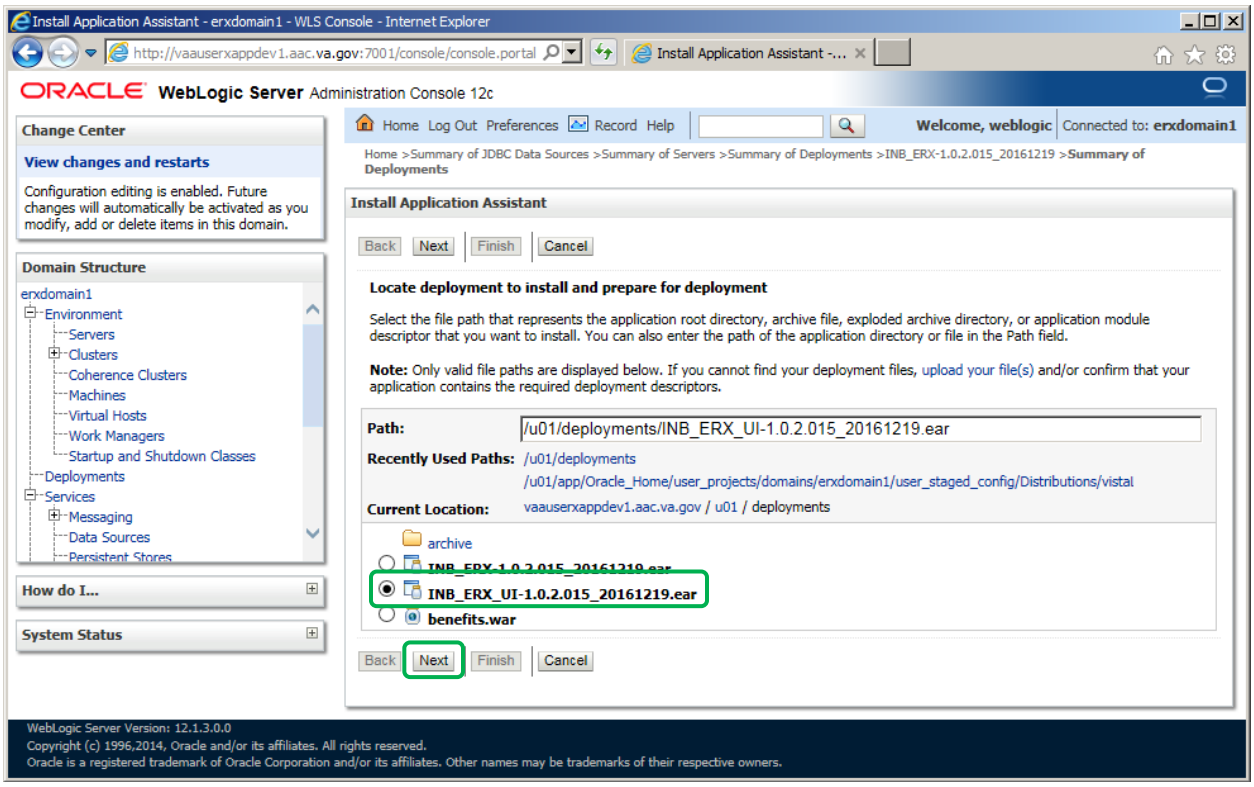
31. The **Overview** tab should appear as illustrated in the figure below.

Figure 93: Install Inbound eRx Application – Verify INB_ERX Deployment Configuration Settings



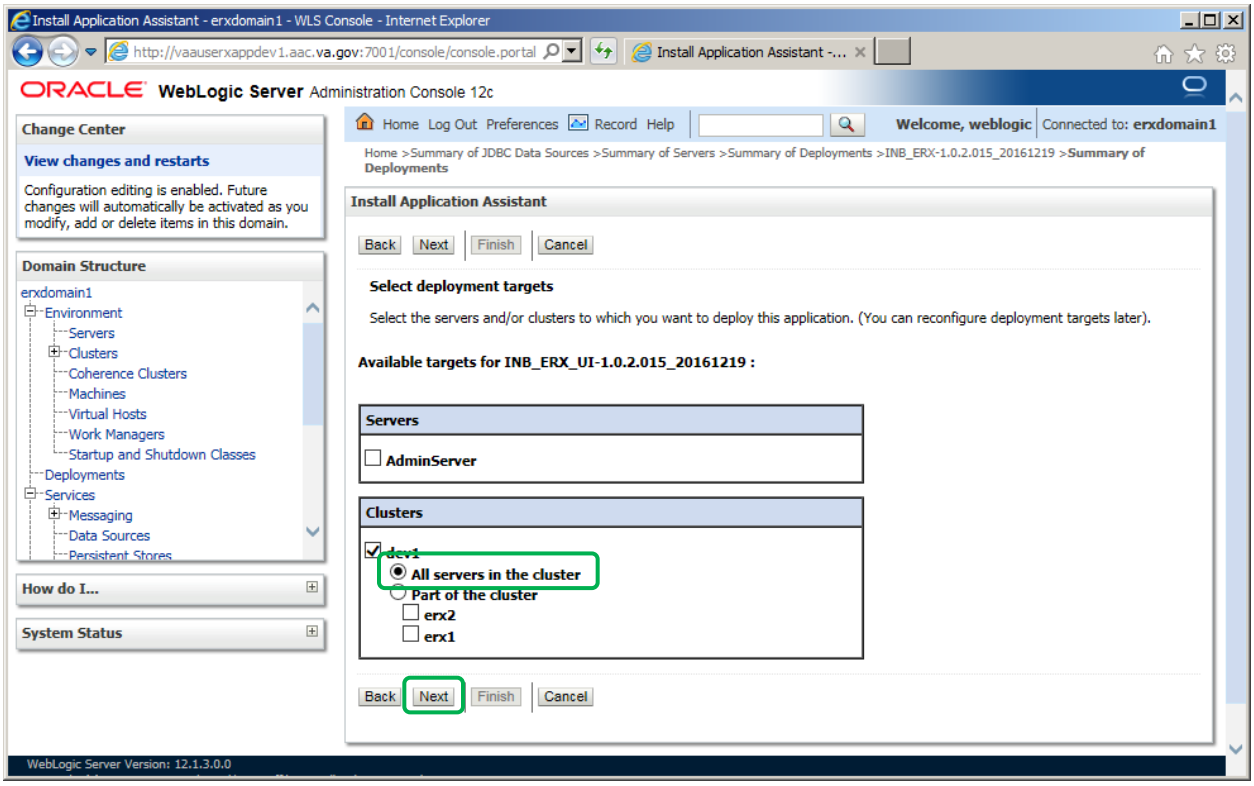
32. Navigate to the **Deployments** page.
33. From the **Deployments** page, click **Install**.
34. Install a new deployment of INB_ERX_UI-4.0.5.012.ear, select the appropriate EAR file.
35. Click **Next**.

Figure 94: Install Inbound eRx Application – Install New Deployment of INB_ERX_UI



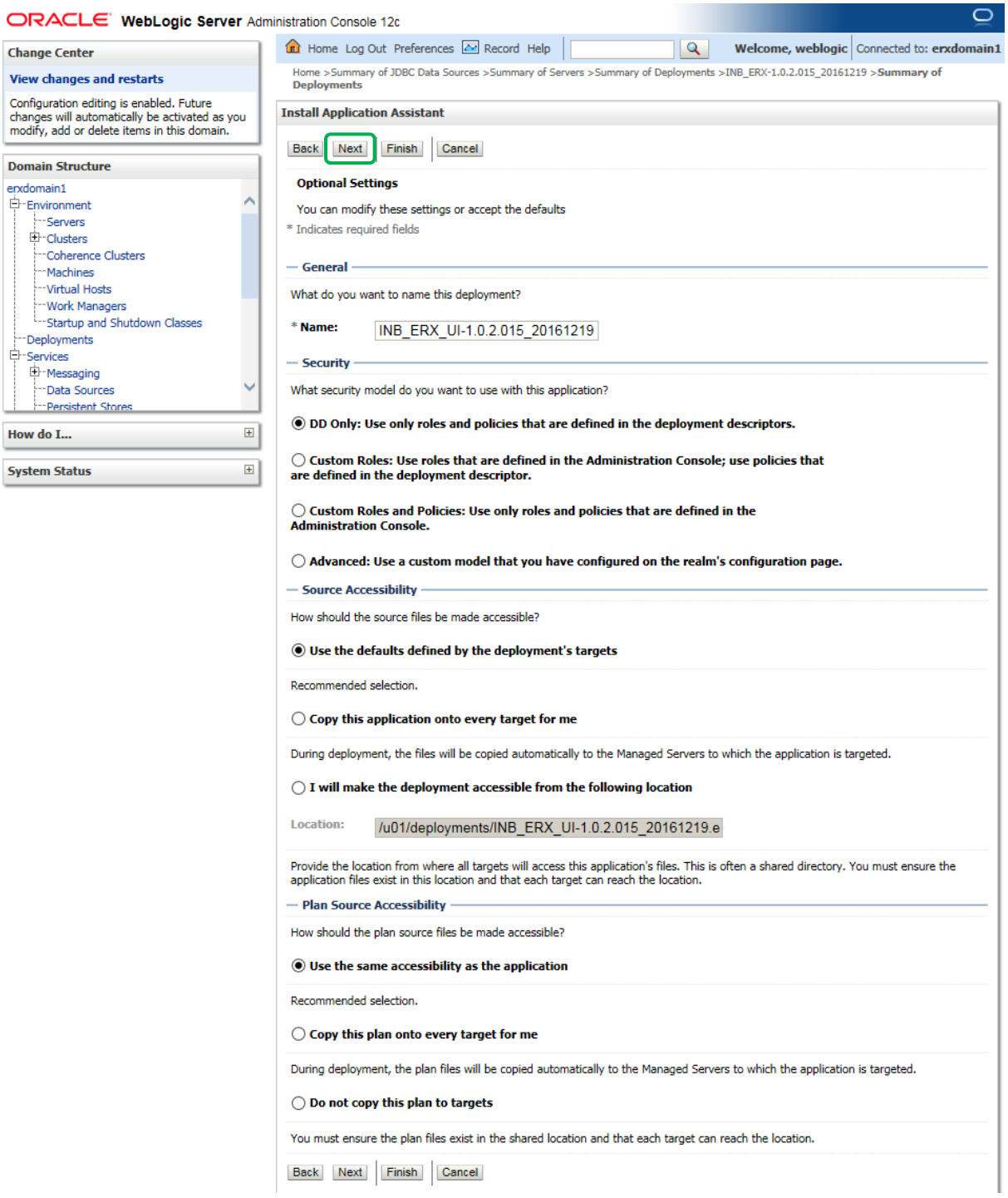
36. Accept the defaults for an application deployment.
37. Click **Next**.
38. Select the cluster and "All servers in the cluster" as the target for the deployment.
39. Click **Next**.

Figure 95: Install Inbound eRx Application – Select INB_ERX_UI Deployment Targets



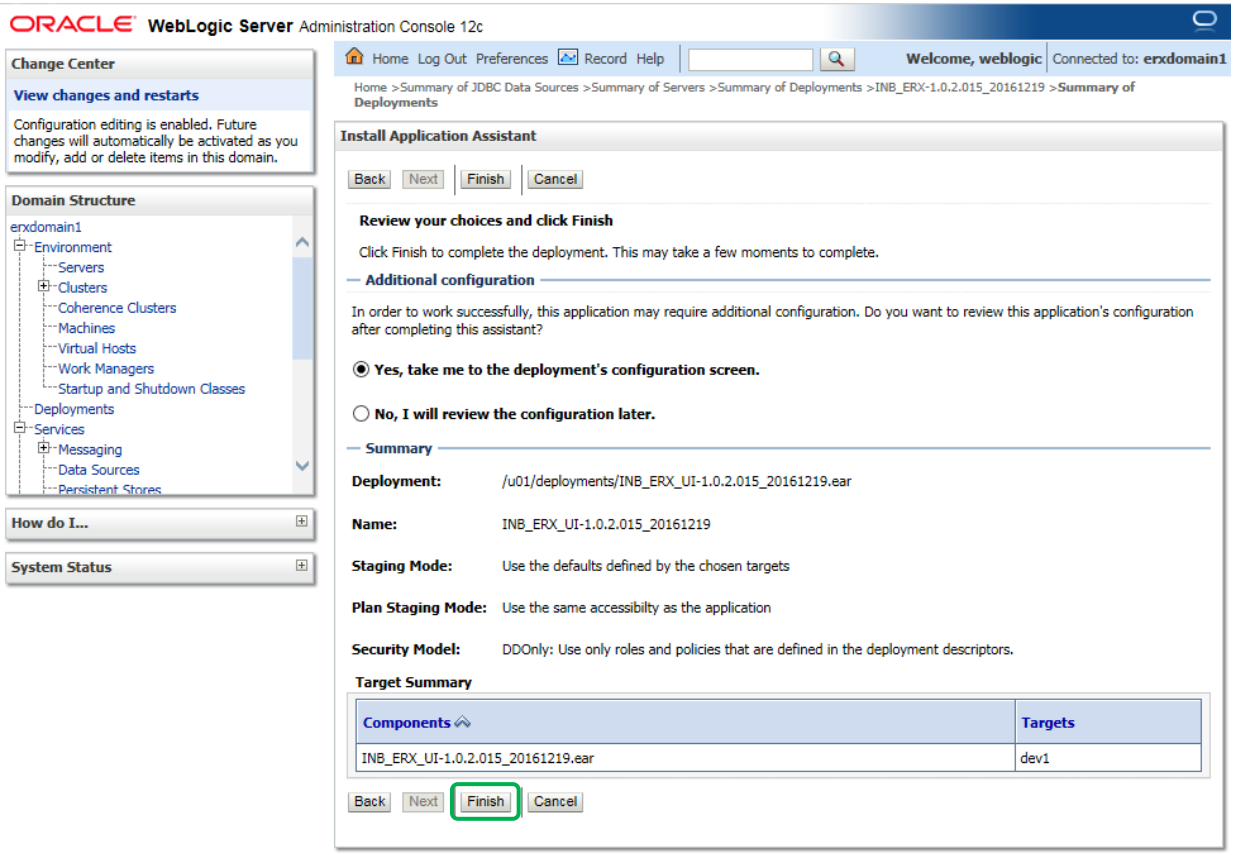
40. All of the values should appear as illustrated in the figure below.
41. Click **Next**.

Figure 96: Install Inbound eRx Application – Verify INB_ERX_UI Deployment Settings



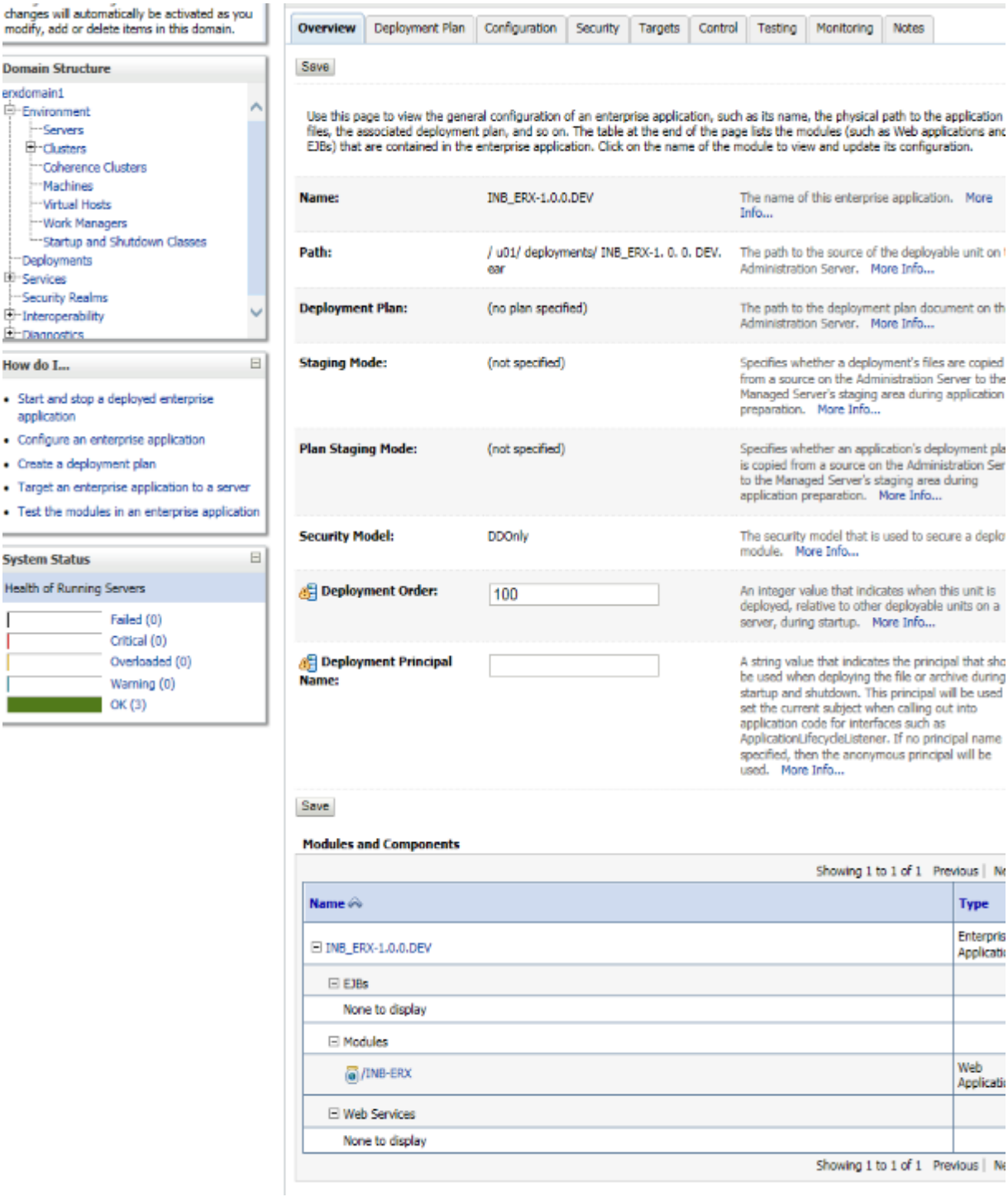
42. All of the values should appear as illustrated in the figure below.
43. Click **Finish**.

Figure 97: Install Inbound eRx Application – Verify INB_ERX_UI Deployment Settings (Finish)



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

Figure 98: Install Inbound eRx Application – Verify INB_ERX_UI Deployment Configuration Settings



45. Navigate to the **Servers** page in the WebLogic console.
46. Select the **Control** tab.
47. Select "erx1" and "erx2", and then click **Start**.

Figure 99: Install Inbound eRx Application – Start erx Servers

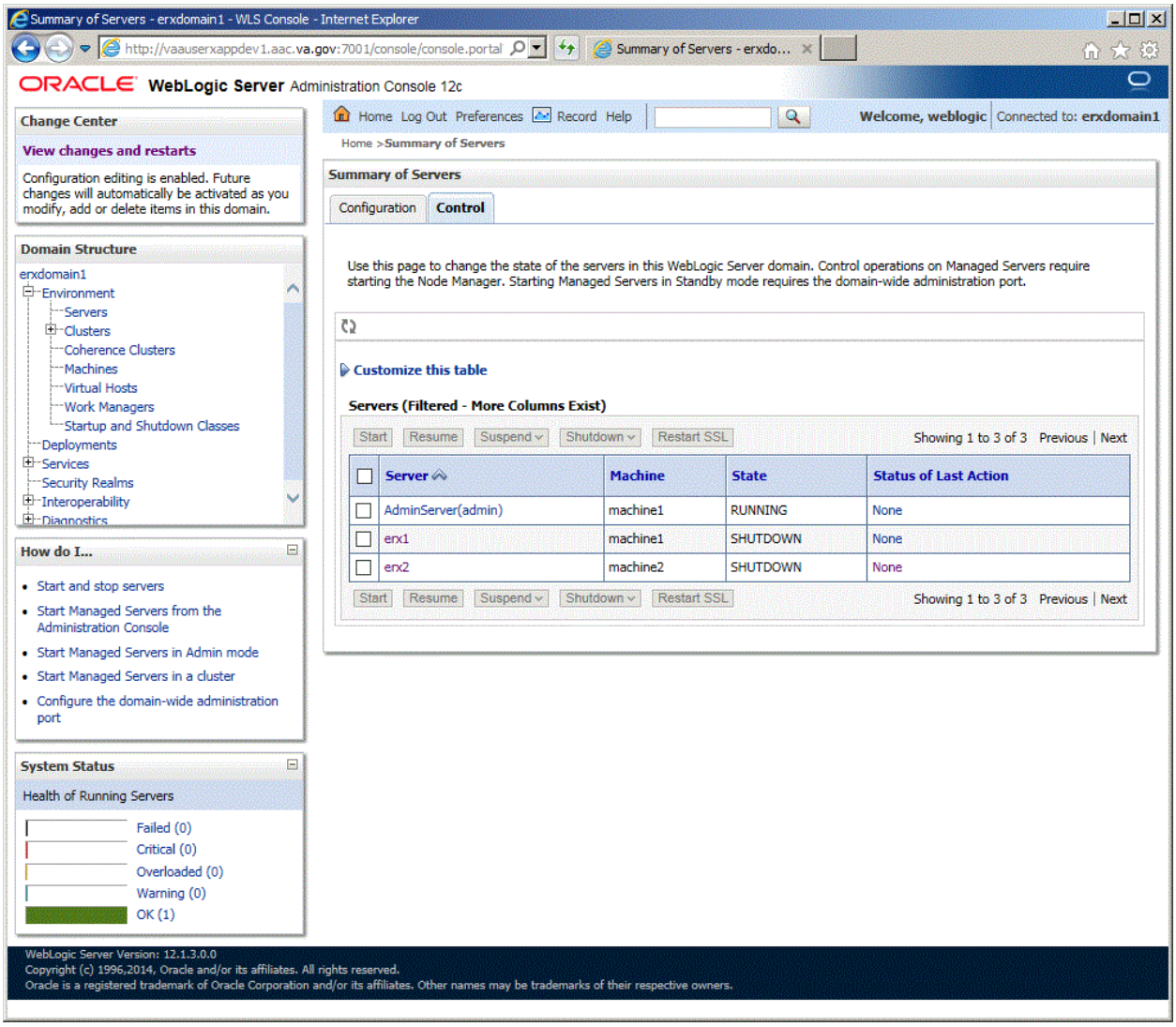
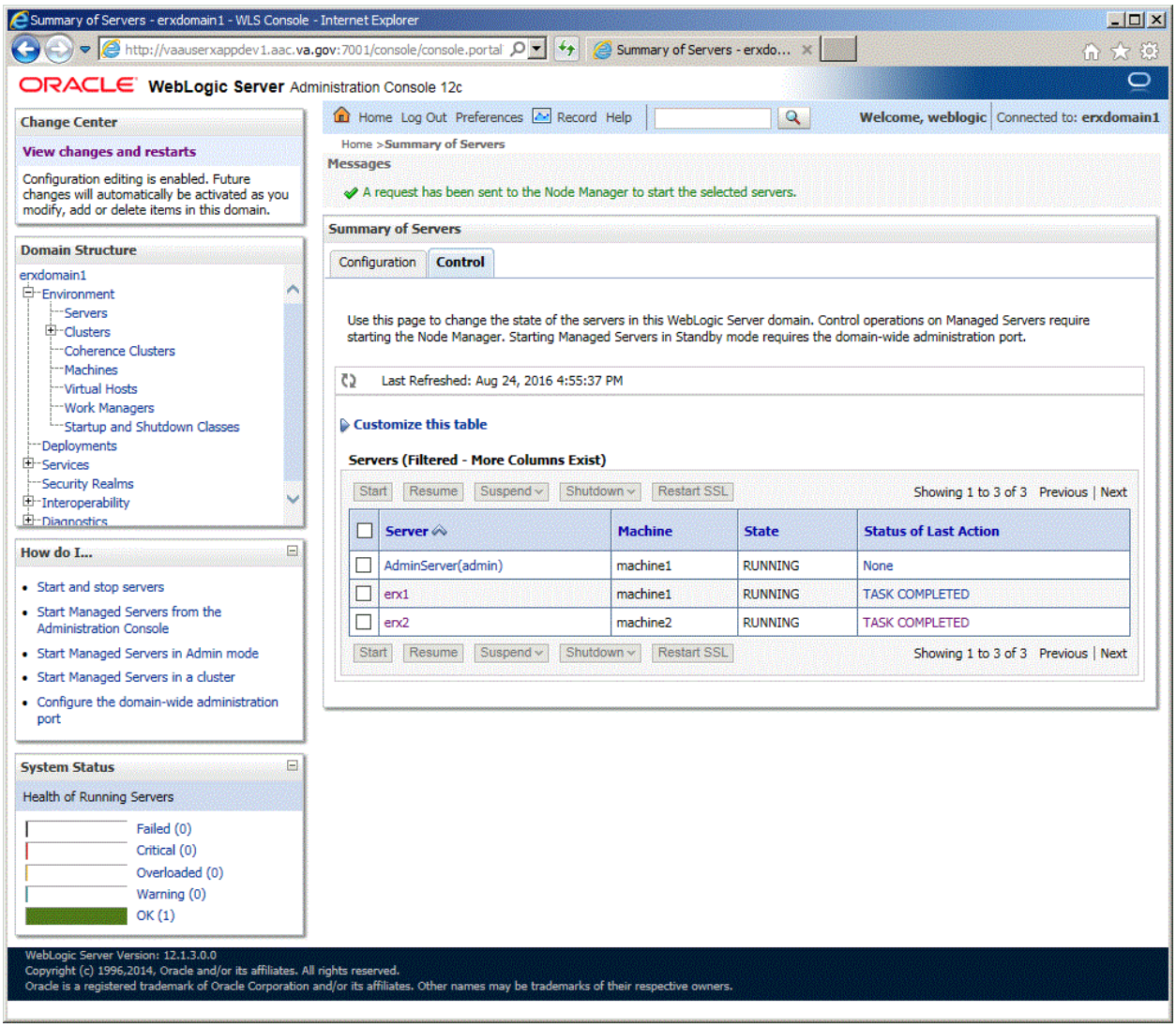


Figure 100: Install Inbound eRx Application – erx Servers Running



4.8.2.2 Create Startup/Shutdown Scripts

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

48. As your normal Linux login account, dzdo su to the weblogic account:

```
$ dzdo su - weblogic
```

49. Create startup scripts with the following commands:

```
$ cat > startNodemanager_[domain].sh
tmp_domain_home="[DOMAIN_HOME]"
cp ${tmp_domain_home}/nodemanager/nodemanager.log
${tmp_domain_home}/nodemanager/nodemanager_old.log
cat /dev/null > ${tmp_domain_home}/nodemanager/nodemanager.log
nohup ${tmp_domain_home}/bin/startNodeManager.sh 2>&1>
${tmp_domain_home}/nodemanager/nm.out &
<ctrl>d

$ cat > startWebLogic_[domain].sh
tmp_domain_home="[DOMAIN_HOME]"
cp ${tmp_domain_home}/servers/AdminServer/logs/AdminServer.log
${tmp_domain_home}/servers/AdminServer/logs/AdminServer_old.log
cat /dev/null > ${tmp_domain_home}/servers/AdminServer/logs/AdminServer.log
```

```
nohup ${tmp_domain_home}/bin/startWebLogic.sh 2>&1>
${tmp_domain_home}/servers/AdminServer/logs/AdminServer.out &
<ctrl>d

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

$ cat > stopWebLogic_[domain].sh
tmp_domain_home="[DOMAIN_HOME]"
${tmp_domain_home}/bin/stopWebLogic.sh
<ctrl>d
```

4.8.2.3 Shut Down Domain

The section provides the steps for shutting down the domain:

1. On VM1, as your normal Linux login account, dzdo su to the weblogic account:
   ```
   $ dzdo 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, as your normal Linux login account, dzdo su to the weblogic account:
   ```
   $ dzdo su - weblogic
   ```
2. Shut down Nodemanager with the following command:
   ```
   $ ./stopNodemanager_[domain].sh
   ```
3. On VM2, as your normal Linux login account, dzdo su to the weblogic account:
   ```
   $ dzdo 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 on VM1 and VM2

Perform the following steps on both VM1 and VM2:

1. Create downloads directory if it doesn't exist (the following must be performed by a system administrator):
```
$ dzdo mkdir -p /u01/downloads
$ dzdo chown weblogic:weblogic /u01/downloads
$ dzdo chmod 777 /u01/downloads
```
2. 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
3. Download the eRx/IEP Installer (erx_iep_ x.x.x.xxx_install_yyyymmdd _hhmmss.sh) to the downloads directory.
4. As your normal Linux login account, execute the eRx/IEP Installerr (erx_iep_ x.x.x.xxx_install_yyyymmdd _hhmmss.sh) exist (the following must be performed by a system administrator):
```
$ dzdo /u01/downloads/erx_iep_ x.x.x.xxx_install_yyyymmdd _hhmmss.sh
```
5. Select option 18, then Exit (x).
6. Download the eRx/IEP Configurator (erx_iep_ x.x.x.xxx_configur_yyyymmdd _hhmmss.sh) to the downloads directory.
7. As your normal Linux login account, execute the eRx/IEP Configurator (erx_iep_ x.x.x.xxx_configur_yyyymmdd _hhmmss.sh) exist (the following must be performed by a system administrator):
```
$ dzdo /u01/downloads/erx_iep_ x.x.x.xxx_configur_yyyymmdd _hhmmss.sh
```
8. Select option 4, then Exit (x).

4.8.3.2 Pentaho Repository Definition Import on VM1

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

1. Create downloads directory if it doesn't exist (the following must be performed by a system administrator):
```
$ dzdo mkdir -p /u01/downloads
$ dzdo chown weblogic:weblogic /u01/downloads
$ dzdo chmod 777 /u01/downloads
```
2. Download the eRx/IEP Deployer (erx_iep_ x.x.x.xxx_deploy_yyyymmdd _hhmmss.sh) to the downloads directory.
3. As your normal Linux login account, execute the eRx/IEP Installerr (erx_iep_ x.x.x.xxx_deploy_yyyymmdd _hhmmss.sh) exist (the following must be performed by a system administrator):
```
$ dzdo /u01/downloads/erx_iep_ x.x.x.xxx_deploy_yyyymmdd _hhmmss.sh
```
4. Select options 6 and 7, then Exit (x).

4.9 Installation Verification Procedure

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

4.10 System Configuration

This section is not applicable to the Inbound eRx project.

4.11 Database Tuning

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

5. Back-Out Procedure

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

The Inbound eRx system will provide data protection measures, such as back-up intervals and redundancy that is consistent with systems categorized as mission critical (12 hour restoration, 2 hour recover point objective). This section outlines the backout strategy, considerations, testing, criteria for backout, risks, authority to approve and the procedures to perform a backout for Inbound eRx.

5.1 Back-Out Strategy

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

5.2 Back-Out Considerations

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

5.2.1 Load Testing

This section is not applicable to the Inbound eRx project.

5.2.2 User Acceptance Testing

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

5.3 Back-Out Criteria

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

5.4 Back-Out Risks

There are no known risks related to a back-out.

5.5 Authority for Back-Out

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

5.6 Back-Out Procedure

This section outlines the backout procedure for Inbound ePrescribing application

5.6.1 Back-Out of Database

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

5.6.1.1 Restore backup files from tape

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

5.6.1.2 Mount the instance

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

5.6.1.3 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; }

5.6.1.4 Open the database and reset logs

1. RMAN> alter database open resetlogs;

5.6.2 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.

5.6.2.1 Remove New Release

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

5.6.2.2 Deploy Back-out Release

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

1. Use the WebLogic console that was started at the beginning of the roll-back process.
2. Within the **Domain Structure** panel in the left column of the WebLogic console, click the Deployments node.
3. Verify that application is in **Lock & Edit** mode. **Lock & Edit** mode is indicated by the "greyed-out" **Lock & Edit** selection button.
4. Click the **Install** button in the **Deployments** panel in the right column of the WebLogic console.
5. WebLogic will now display the panel **Install Application Assistant** in the right column of the console, where the location of the Inbound eRx deployment will be found.
    a. If the rolled-back Inbound eRx deployment has already been transferred to the Deployment Machine, navigate to the deployment file location using the links and file structure displayed within the **Location** panel within the Install Application Assistant in the right column of the console. Choose the ear file associated with the rolled-back release.

b. If the rolled-back Inbound eRx deployment has not been transferred to the Deployment Machine:

i. Click on the upload your file(s) link in the **Install Application Assistant** panel in the right section of the console.

ii. Click the **Deployment Archive Browse** to see the Choose file dialogue used to select the Deployment Archive.

iii. Click **Next** in the Upload a Deployment to the admin server panel in the right column of the WebLogic console to return to the Locate deployment to install and prepare for deployment panel within the Install Application Assistant.

6. Once the rolled-back Inbound eRx deployment is located and selected, click **Next.**
7. WebLogic will now display the panel Choose targeting style within the Install Application Assistant in the right column of the console. Leave the default value selected, install this deployment as an application, and click **Next**.
8. Within the **Install Application Assistant** in the right column of the console, WebLogic will now display the panel Select deployment targets, where the Deployment Server will be selected as the target in the next step.
9. For the **Target**, select the **Deployment Server**.
10. Click **Next**.
11. Within the **Install Application Assistant**, WebLogic will now display the panel **Optional Settings** in the right column of the console, where the name of the deployment and the copy behavior are chosen.
12. Enter the **Name** for the deployment. Use: : INB_ERX-4.0.5.012
13. Verify that the following default option for Security is selected:

    DD Only: Use only roles and policies that are defined in the deployment descriptors.
14. Verify that the following default option for Source accessibility is selected:

    Use the defaults defined by the deployment's targets.
15. Click **Next**.
16. Within the **Install Application Assistant,** in the right column of the console WebLogic, will now display the panel **Review your choices and click Finish**, which summarizes the steps completed above.
17. Verify that the values match those entered in Steps 6 through 17 and click **Finish**.
18. WebLogic will now display the panel **Settings for Inbound eRx**, in the right column of the console, where the values previously entered are available as well as a setting to change the deployment order.
19. Leave all the values as defaulted by WebLogic and click **Save**.
20. Within the **Change Center** panel in the left column of the WebLogic console, click **Activate Changes**.
21. Within the **Domain Structure** panel in the left column of the WebLogic console, click the Deployments node.

22. WebLogic will now display the panel **Summary of Deployments** in the right column of the console, where all deployments for the WebLogic domain are listed.
23. Select the previously deployed INB_ERX-4.0.5.012 deployment, click **Start**, and then select **Servicing all requests** from the drop-down list box.
24. WebLogic will now display the panel **Start Application Assistant** in the right column of the console for confirmation to start servicing requests.
25. Click **Yes** in the **Start Application Assistant** panel in the right column of the WebLogic console.
26. WebLogic now returns to the **Summary of Deployments** panel in the right column of the console.
27. Verify that the State of the INB_ERX-4.0.5.012 deployment is "Active".

5.7 Back-out Verification Procedure

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

6. Rollback Procedure

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

6.1 Rollback Considerations

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

6.2 Rollback Criteria

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 is the Inbound eRx IPT, the VA PM, and other relevant stakeholders, where applicable.

6.5 Rollback Procedure

6.5.1 Rollback of Database

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

6.5.1.1 Restore backup files from tape

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

6.5.1.2 Mount the instance

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

6.5.1.3 Restore and recover the datafiles

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

6.5.1.4 Open the database and reset logs

32. RMAN> alter database open resetlogs;

6.5.2 Rollback WebLogic

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

6.5.2.1 Remove New Release

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

8. WebLogic now returns to the **Summary of Deployments** panel in the right column of the console.
9. Verify that the State of the Inbound eRx deployment is "Prepared".
10. Select the previously deployed Inbound eRx deployment, and then click **Delete**.
11. WebLogic will now display the panel **Delete Application Assistant** in the right column of the console for confirmation to start servicing requests.
12. Click **Yes** in the **Delete Application Assistant** panel in the right column of the WebLogic console.
13. WebLogic now returns to the Summary of Deployments panel in the right column of the console.
14. Verify that the Inbound eRx deployment is deleted and no longer present.

6.5.2.2 Deploy Rolled-Back Release

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

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

7. WebLogic will now display the panel Choose targeting style within the Install Application Assistant in the right column of the console. Leave the default value selected, install this deployment as an application, and click **Next**.
8. Within the **Install Application Assistant** in the right column of the console, WebLogic will now display the panel Select deployment targets, where the Deployment Server will be selected as the target in the next step.
9. For the **Target**, select the **Deployment Server**.
10. Click **Next**.
11. Within the **Install Application Assistant**, WebLogic will now display the panel **Optional Settings** in the right column of the console, where the name of the deployment and the copy behavior are chosen.
12. Enter the **Name** for the deployment. Use: : INB_ERX-4.0.5.012
13. Verify that the following default option for Security is selected:

    DD Only: Use only roles and policies that are defined in the deployment descriptors.
14. Verify that the following default option for Source accessibility is selected:

    Use the defaults defined by the deployment's targets.
15. Click **Next**.
16. Within the **Install Application Assistant,** in the right column of the console WebLogic, will now display the panel **Review your choices and click Finish**, which summarizes the steps completed above.
17. Verify that the values match those entered in Steps 6 through 17 and click **Finish**.
18. WebLogic will now display the panel **Settings for Inbound eRx**, in the right column of the console, where the values previously entered are available as well as a setting to change the deployment order.
19. Leave all the values as defaulted by WebLogic and click **Save**.
20. Within the **Change Center** panel in the left column of the WebLogic console, click **Activate Changes**.
21. Within the **Domain Structure** panel in the left column of the WebLogic console, click the Deployments node.
22. WebLogic will now display the panel **Summary of Deployments** in the right column of the console, where all deployments for the WebLogic domain are listed.
23. Select the previously deployed INB_ERX-4.0.5.012 deployment, click **Start**, and then select **Servicing all requests** from the drop-down list box.
24. WebLogic will now display the panel **Start Application Assistant** in the right column of the console for confirmation to start servicing requests.
25. Click **Yes** in the **Start Application Assistant** panel in the right column of the WebLogic console.
26. WebLogic now returns to the **Summary of Deployments** panel in the right column of the console.
27. Verify that the State of the INB_ERX-4.0.5.012 deployment is “Active”.

6.5.3 Rollback VistA Patch

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

6.6 Rollback Verification Procedure

6.6.1.1 Validation of Roll Back Procedure

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

7. Operational Procedures

This section outlines server startup and shutdown procedures.

7.1 Startup Procedures

7.1.1 Start Weblogic Node Managers and Admin Console

1. At your normal Linux login account, dzdo su to the weblogic account:
   ```
   $ dzdo 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. As your normal Linux login account, dzdo su to the kettle account:
   ```
   $ dzdo su - kettle
   ```
2. On VM1, start ***[ENV]*** Master Slave:
   ```
   $ ./startCarte[Env]Master1.sh
   ```
3. From the CPanel (https://***[proxy_fqdn]***/cpanel), wait for the ***[ENV]*** Master Slave to start up by watching: https://***[proxy_fqdn]***/master1/kettle/status/
4. On VM 1, start ***[ENV]*** Dynamic Slave1:
   ```
   $ ./startCarte[Env]Slave1.sh
   ```
5. On VM 1, start ***[ENV]*** Dynamic Slave2:
   ```
   $ ./startCarte[Env]Slave2.sh
   ```
6. On VM 2, start ***[ENV]*** Dynamic Slave3:
   ```
   $ ./startCarte[Env]Slave3.sh
   ```
7. On VM 2, start ***[ENV]*** Dynamic Slave4:
   ```
   $ ./startCarte[Env]Slave4.sh
   ```
8. From the CPanel (https://***[proxy_fqdn]***/cpanel), wait for the ***[ENV]*** Slave1 to start up by watching: https://***[proxy_fqdn]***/slave1/kettle/status/
9. From the CPanel (https://***[proxy_fqdn]***/cpanel), wait for the ***[ENV]*** Slave2 to start up by watching: https://***[proxy_fqdn]***/slave2/kettle/status/
10. From the CPanel (https://***[proxy_fqdn]***/cpanel), wait for the ***[ENV]*** Slave3 to start up by watching: https://***[proxy_fqdn]***/slave3/kettle/status/
11. From the CPanel (https://***[proxy_fqdn]***/cpanel), wait for the ***[ENV]*** Slave4 to start up by watching: https://***[proxy_fqdn]***/slave4/kettle/status/
12. From the CPanel (https://***[proxy_fqdn]***/cpanel), check that all 4 dynamic slaves have registered with the master: https://***[proxy_fqdn]***/slave1/kettle/getSlaves/
13. From the CPanel (https://***[proxy_fqdn]***/cpanel), start the message processing jobs:
    https://***[proxy_fqdn]***/slave1/kettle/runJob/?job=inbound_main/InboundMessageProcessing_JOB
    https://***[proxy_fqdn]***/slave2/kettle/runJob/?job=inbound_main/InboundMessageProcessingRetry_JOB
    https://***[proxy_fqdn]***/slave3/kettle/runJob/?job=inbound_vista_delivery/InboundDeliverToVista_JOB
    https://***[proxy_fqdn]***/slave4/kettle/runJob/?job=outbound_main/OutboundMessageProcessing_JOB
14. From the CPanel (https://***[proxy_fqdn]***/cpanel), check the InboundMessageProcessing_JOB status: https://***[proxy_fqdn]***/slave1/kettle/status, click on the InboundMessageProcessing_JOB hyperlink and check the job status page.

15. From the CPanel (https://***[proxy_fqdn]***/cpanel), check the InboundMessageProcessingRetry_JOB status: https://***[proxy_fqdn]***/slave2/kettle/status, click on the InboundMessageProcessingRetry_JOB hyperlink and check the job status page.
16. From the CPanel (https://***[proxy_fqdn]***/cpanel), check the InboundDeliverToVista _JOB status: https://***[proxy_fqdn]***/slave3/kettle/status, click on the InboundDeliverToVista _JOB hyperlink and check the job status page.
17. From the CPanel (https://***[proxy_fqdn]***/cpanel), check the OutboundMessageProcessing _JOB status: https://***[proxy_fqdn]***/slave4/kettle/status, click on the OutboundMessageProcessing hyperlink and check the job status page.

7.2 Shut Down Procedures

7.2.1 Pentaho Services Shutdown

1. As your normal Linux login account, dzdo su to the kettle account:
   ```
   $ dzdo 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
   ```
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. As your normal Linux login account, dzdo su to the weblogic account:
   ```
   $ dzdo 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:
6. $ ./stopNodemanager_***[domain]***.sh