**Department of Veterans Affairs**

**Patient-Centered Management Module   
Re-host/Re-Engineering (PCMMR)**

**Production Operations Manual**

VA logo

**August 2014**

**Document Version 1.8**

Department of Veterans Affairs

Office of Information & Technology

Product Development

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 08/11/2014 | 1.8 | Technical edit. | Kate Hula |
| 6/03/2014 | 1.7 | Review and update to current configuration | Noel Morrison |
| 1/17/2013 | 1.6 | Technical Edit | Brian Lynch |
| 1/15/2013 | 1.5 | Additional content in section 7.4 | Noel Morrison |
| 11/16/2012 | 1.4 | Technical Edit | Brian Lynch |
| 11/16/2012 | 1.3 | Additional details added | Jan Joubert |
| 11/14/2012 | 1.2 | Additional details added | Noel Morrison |
| 11/8/2012 | 1.1 | Technical Edit | Brian Lynch |
| 10/10/2012 | 1.0 | Initial document | Noel Morrison |

**Table of Contents**

[1. Introduction 1](#_Toc396141385)

[1.1 Summary 1](#_Toc396141386)

[1.2 Purpose 1](#_Toc396141387)

[1.3 Scope 1](#_Toc396141388)

[1.4 Related Documents and Agreements 1](#_Toc396141389)

[1.4.1 Memorandum of Understanding (MOU) 1](#_Toc396141390)

[1.4.2 Service Level Agreement (SLA) 2](#_Toc396141391)

[1.4.3 Service Level Requirements (SLR) 2](#_Toc396141392)

[1.4.4 Operational Level Agreement (OLA) 2](#_Toc396141393)

[1.4.5 Operations and Maintenance Plan (O&M) 2](#_Toc396141394)

[1.4.6 Underpinning Contract 2](#_Toc396141395)

[1.5 Section Summary 3](#_Toc396141396)

[2. System Business and Operational Description 3](#_Toc396141397)

[2.1 Operational Priority and Service Level 4](#_Toc396141398)

[2.2 Logical System Description 4](#_Toc396141399)

[2.3 Physical System Description 4](#_Toc396141400)

[2.4 Software Description 6](#_Toc396141401)

[2.4.1 Background Processes 7](#_Toc396141402)

[2.4.2 Job Schedules – (Reference Background Processes) 7](#_Toc396141403)

[2.5 Dependent Systems 8](#_Toc396141404)

[2.5.1 MVI (HL7v2, HL7v3 configuration) 8](#_Toc396141405)

[2.5.2 VistA 8](#_Toc396141406)

[2.5.3 VistALink 8](#_Toc396141407)

[3. Installation Operations 8](#_Toc396141408)

[3.1 Install SQL Server Procedures 8](#_Toc396141409)

[*3.1.1* *Use Microsoft’s Best practices for SQL Server install.* 8](#_Toc396141410)

[3.2 Install Weblogic Procedures 8](#_Toc396141411)

[3.2.1 Install Java JDK Procedures 8](#_Toc396141412)

[3.2.2 Install Weblogic Portal software Procedures 9](#_Toc396141413)

[3.2.3 Create domains directory, and set permissions 11](#_Toc396141414)

[3.2.4 Copy the latest domain files 11](#_Toc396141415)

[4. Routine Operations 11](#_Toc396141416)

[4.1 Administrative Procedures 11](#_Toc396141417)

[4.1.1 System Start-up 11](#_Toc396141418)

[4.1.2 System Shut-down 13](#_Toc396141419)

[4.1.3 Back-up and Restore 16](#_Toc396141420)

[4.2 Security / Identity Management 17](#_Toc396141421)

[4.2.1 Identity Management 17](#_Toc396141422)

[4.2.2 Access control 17](#_Toc396141423)

[4.3 User Notifications 18](#_Toc396141424)

[4.4 System Monitoring, Reporting, and Tools 18](#_Toc396141425)

[4.4.1 Availability Monitoring 18](#_Toc396141426)

[4.4.2 Performance/Capacity Monitoring 20](#_Toc396141427)

[4.4.3 Critical Metrics 20](#_Toc396141428)

[4.5 Routine Updates, Extracts and Purges 20](#_Toc396141429)

[4.6 Scheduled Maintenance 21](#_Toc396141430)

[4.7 Capacity Planning 21](#_Toc396141431)

[5. Exception Handling 21](#_Toc396141432)

[5.1 Routine Errors 21](#_Toc396141433)

[5.1.1 Security 21](#_Toc396141434)

[5.1.2 Time-outs 22](#_Toc396141435)

[5.1.3 Concurrency 22](#_Toc396141436)

[5.2 Significant Errors 22](#_Toc396141437)

[5.2.1 Application Error Logs 22](#_Toc396141438)

[5.2.2 Application Error Codes and Descriptions 22](#_Toc396141439)

[5.2.3 Infrastructure Errors 22](#_Toc396141440)

[5.3 Dependent System(s) 24](#_Toc396141441)

[5.4 Trouble Shooting 24](#_Toc396141442)

[5.5 System Recovery 24](#_Toc396141443)

[5.5.1 Restart after Non-Scheduled System Interruption 24](#_Toc396141444)

[5.5.2 Restart after Database Restore 24](#_Toc396141445)

[6. Continuity of Operations 24](#_Toc396141446)

[7. Disaster Recovery 24](#_Toc396141447)

[7.1 Required: 24](#_Toc396141448)

[7.2 Assumptions: 24](#_Toc396141449)

[7.3 WebLogic Server (CRRC): 24](#_Toc396141450)

[7.4 Database server (CRRC): 25](#_Toc396141451)

[7.5 Database server (Hines): 26](#_Toc396141452)

[7.6 WebLogic server (HITC): 26](#_Toc396141453)

[7.7 Checking the Load Balancer (CRRC): 26](#_Toc396141454)

[8. Back-Out Procedures 28](#_Toc396141455)

[8.1 Database 28](#_Toc396141456)

[8.2 Weblogic 28](#_Toc396141457)

[8.3 Vista Patches 28](#_Toc396141458)

[9. System Support 28](#_Toc396141459)

[9.1 Support Structure 28](#_Toc396141460)

[9.1.1 Support Hierarchy 28](#_Toc396141461)

[9.1.2 Division of Responsibilities 29](#_Toc396141462)

[9.2 Support Procedures 29](#_Toc396141463)

# Introduction

## Summary

A Production Operations Manual (POM) defines the specific technical and operational processes that must be carried out on a daily, weekly, monthly, or yearly basis. A POM is an application/system-specific document containing detailed topology, dependencies, monitoring specifics, maintenance windows, and etc. Additionally, it contains the system’s scheduled events (regular production jobs, performance reporting, or maintenance windows, etc). The POM provides Field Operations staff the necessary instructions to operate and support production computer systems.

The production support for the Production System is divided or shared between the Enterprise Operations & Infrastructure (EOI) and Product Development within the Office of Information & Technology (OI&T), and Corporate Data Center Operations (CDCO).

## Purpose

The purpose of this document is to:

* Be used as a reference manual for the daily operation and maintenance of Patient-Centered Management Module Re-Engineering (PCMMR).
* Assist support personnel on the resolution of system issues.
* Assist in the capacity, maintenance, and upgrade planning of PCMMR.

## Scope

The scope of this document is limited to CISS/PCMMR. Any references to external systems are only for describing an interface and how the interface and the external system affects the operation of CISS/PCMMR or as a tool that may be used as part of system monitoring or the support and issue resolution system.

## Related Documents and Agreements

The Department of Veterans Affairs (VA) Service Level Management Board (SLMB) has developed a memorandum that standardizes terminology and definitions for key documents used for implementation, operation, and monitoring of services provided by OI&T. The primary documents are Memorandum of Understanding (MOU), Service Level Agreement (SLA), Service Level Requirements (SLR), Operational Level Agreement (OLA), Operations and Maintenance (O&M). The purpose and relationships of these documents are summarized below.

### Memorandum of Understanding (MOU)

The Memorandum of Understanding (MOU), a written agreement between an OI&T service provider and customer(s), documents the services that each party will provide for a program or service. The MOU is the foundation document upon which the SLA, O&M Plan, and others are built. The MOU is a strategic document, whereas the SLA, O&M, and POM are more functional and tactical documents.

The MOU serves as the signatory document that invokes the SLA. The SLA/SLRs are referenced in the appendix of the MOU, allowing them to be managed or modified without renegotiating the entire MOU.

### Service Level Agreement (SLA)

A Service Level Agreement (SLA) is a consolidated mutual agreement between a service provider and customer(s) that documents and describes agreed levels of performance and availability. The SLA describes Service Level Targets (SLTs), key performance indicators, a monitoring approach, and a process for managing the service levels. In the VA, all SLAs are approved, negotiated, and governed through the Service Level Management Board (SLMB).

### Service Level Requirements (SLR)

In the VA, Service Level Requirements (SLRs) are a list of basic performance measurement requirements. A SLR is proposed by the customer and negotiated with OI&T to reach a good faith agreement on the acceptable level of service and the metrics to monitor the service. The SLR is a service-specific breakdown (usually in a table) in an SLA appendix with a unique name and number.

After the SLR is negotiated, it results in an agreed Service Level Target (SLT) with metrics, measurement techniques, and assumptions. The SLA and SLTs are a combined document.

### Operational Level Agreement (OLA)

An Operational Level Agreement (OLA) is an agreement between two or more OI&T entities that documents agreed service levels for general performance or critical services. An OLA is very similar to a SLA except that it is internal to OI&T functional units. An OLA defines specific key performance indicators and related metrics to measure success criteria. OLA metrics should form the foundation upon which SLA metrics can be derived for customer-facing services.

### Operations and Maintenance Plan (O&M)

The Operations and Maintenance (O&M) Plan defines the operational support tasks and activities that each of the Office of Information & Technology (OI&T) functional areas are required to provide in the delivery and support of a production enterprise system. The O&M Plan defines specific roles and responsibilities of OI&T functional support teams to avoid confusion over which party is responsible for specific areas of process, tasks, or actions. The O&M plan supports the specific service levels for each activity as defined in the Service Level Agreement (SLA), describes how performance is measured, and identifies the responsible entities for each activity.

All key functions are assigned to one or more responsible parties and activities are clearly defined in order to maintain and support the applications and system components throughout its life cycle. These roles and responsibilities are displayed in a tabular RACI format at the end of each section of the plan to further define **R**esponsibility, **A**ccountability, **C**onsultation, and **I**nformation roles.

### Underpinning Contract

An Underpinning Contract is an agreement between an information technology service provider and a third party, including vendors, that provides goods or services that support delivery of an IT service to a customer. It is developed either by the Program Office or OI&T, depending on ownership of the budget/funds

## Section Summary

|  |  |
| --- | --- |
| Section | Summary |
| 1. Introduction | This section describes the scope and purpose of the document, along with other relevant documents. |
| 2. System Business and Operational Description | This section provides the reader with a description of the system. It describes what the system does in the context of the VA. |
| 3. Installation | This section describes the installation of the required components. |
| 4. Routine Operations | This section describes what is required of an operator/administrator or other non-business user to maintain the system at an operational and accessible state. |
| 5. Exception Handling | This section gives an overview of how system problems are handled. It should describe the general expectations of how the administrator and other operations personnel should respond and handle system problems. |
| 6. Continuity of Operations | This section describes the processes or procedures that operations personnel need to execute in order to fulfill their responsibility in the systems Continuity of Operations plan (COOP). |
| 7. Disaster Recovery | This section describes the processes or procedures that operations personnel need to execute in order to fulfill their responsibility in the systems Disaster Recovery (DR) plan. |
| 8. System Support | This section describes the VHA system support structure and how to use it to resolve system problems. |

# System Business and Operational Description

The Clinical Information Support System (CISS) project is a Health*e*Vet initiative from the Veterans Program portfolio. It is a Web-based portal application that provides a central interface for users to access information and applications necessary for their roles. The applications accessed through CISS are called partner systems. The initial CISS partner system is the Patient-Centered Management Module Re-Engineering (PCMMR), a Web-based application that assists VA facilities in implementing and monitoring patient and staff assignments in both primary care and non-primary care teams.

While implementing the CISS framework and the PCMMR application, the PCMMR project team follows an agile software methodology to support rapid programming and short six-month releases to production. For more information please view the Agile Software Development Methodology and other documents available on the [CISS TSPR page](http://DNS       .med.DNS   /warboard/anotebk.asp?proj=1256&Type=Active):

[http://DNS .med.DNS /warboard/anotebk.asp?proj=1256&Type=Active](http://DNS       .med.DNS   /warboard/anotebk.asp?proj=1256&Type=Active)

This document contains instructions to help System Operators install, administer, and troubleshoot the delivered software. System Operators are defined as IT staff at the data centers where CISS and PCMMR are deployed.

## Operational Priority and Service Level

The CISS/PCMM project is a 24x7 system.

## Logical System Description

Intranet access to the application is achieved from the customers’ web browsers to a URL address associated with the Load Balancer’s Virtual IP (VIP). Connectivity is directed to the CISS application servers. With the exception of requesting the web-based content-sensitive help, all other traffic is redirected to the WebLogic application Java Virtual Machine (JVM)s and their configured server ports. The CISS login portal web page interacts with the VA Lightweight Directory Access Protocol (LDAP) service to determine access to the portal and any partner applications. Once access is gained and the PCMMR partner application button is accessible, the PCMMR application may be launched. PCMMR application saves data into a local database and certain functions require interactions between the VistA systems of the chosen site.

## Physical System Description

The CISS servers consist of three virtual servers/machines (VM), consisting of two applications servers, and one database server. Redundancies are achieved through multiple methods: replication of data at the OS and application levels.

The architectural design of each of the three groups consists of different redundancies:

* The database servers are to be clustered at the OS level and at the database application level. The database servers are connected to a NetApp Data Storage, for additional storage, redundancy, and availability.
* The two application servers are not clustered at the Operating System (OS) level, but are clustered at the application level. OS-level implemented synchronization and application clustering maintain the redundancies.

The current systems implemented are 16 GB Memory per VM. Microsoft Windows 2012 Standard and Red Hat Enterprise Linux 6.x are the operating systems of the systems. All systems are attached to sites Gigabit network. Three of the VM’s reside at Martinsburg, WV (CRRC), production site. Four other servers are located at Hines, IL. The Hines site is considered the Disaster Recovery (DR) site.

The main difference between the two data centers is that the Hines, IL has the additional MS Windows server as the MS SQL Server “Witness” server. The “Witness” server monitors the Martinsburg and Hines database servers, and delegates which server is the Primary and the other as the Stand-by nodes.



**Weblogic Database**

**PCMM Database**

**F5 LTM Load Balancer**

**w/ failover pair**

**Database VM**

**Weblogic VM**

**F5 GTM Load Balancer**

***PCMM Domain***

***ATTENDED Cluster***

***CISS, CISS Usermanagement,* PCMM**

***UNATTENDED Cluster***

***PCMM\_unattended***

PCMM SQL Database Mirroring

Primary Data Center

Secondary Data Center



## Software Description

The Operating Systems:

* Microsoft Windows 2012 Standard Edition x\_64 Bit
* Red Hat Enterprise Linux 6 x64 Bit

The Applications:

* BEA / Oracle WebLogic 10.3.6
* Microsoft SQL Server 2012
* Apache 2.2.15
* VistALink 1.6

File system sizes differentiate between the Servers Functions:

* Windows servers database servers:
  + - Local Drives
* C: 60 GB OS Drive
* E: 300 GB Database Files
* F: 150 GB Temp Database Files
* H: 200 GB Backup Files
* I: 200 GB Database Log Files
* RHEL Application server
  + - /dev/mapper/rootvg-root 1.0 G /
    - /dev/mapper/rootvg-opt 4.0G /opt
    - /dev/mapper/rootvg-var 4.0G /var
    - /dev/mapper/rootvg-tmp 4.0G /tmp
    - /dev/mapper/rootvg-usr 4.0G /usr
    - /dev/mapper/rootvg-home 2.0G /home
    - /dev/cciss/c0d0p1 251M /boot
    - tmpfs 7.9G /dev/shm
    - /dev/mapper/rootvg-u01 20.0G /u01

There are numerous scripts involved in monitoring and synchronizing of servers systems.

### Background Processes

The Microsoft SQL Server runs a Daily Maintenance Plan: Maintenance Cleanup on Local server connections to remove database backup files.

* Clean up history on Local server connection History type: Backup, Job, Maintenance Plan.
* Backup Database on Local server connection: CISS, Model Databases - Transaction Logs.
* Check Database integrity on Local server connection: CISS\_PROD, CISS\_distributor, master, model, msdb.
* Update Statistics on Local server connection: CISS\_PROD, CISS\_distributor, master, model, msdb.
* Backup Database on Local server connection: CISS\_PROD, CISS\_distributor, master, model, msdb.
* Reorganize index on Local server connection: CISS\_PROD Tables.

The SQL backups are stored on the mapped H: SAN attached drive. The database servers have an OS-level backup that runs at 5:00 A.M. daily. The DOS batch script does a checksum of the last backups, XCOPY of the files to the DR servers, and purges any files that are over five days.

The Linux servers, application, and web servers each have the following scheduled jobs:

(i.e., Scripts/Process still pending)

* Unattended Server
  + (part of PCMMR but separate from web application it runs all the background tasks) Runtime PropertiesProperty files are used to accommodate the universal build of the application artifact to be deployed to any environment, to read those variables saved in the properties files.

### Job Schedules – (Reference Background Processes)

No scripts specific to PCMMR at this time.

## Dependent Systems

Systems on which CISS/PCMMR are dependent:

### MVI (HL7v2, HL7v3 configuration)

* *Describe Detailed Configuration here*

### VistA

* Patch must be installed before PCMMR can be turned on.
* Proxy user must be setup and established

### VistALink

* VistAlink uses 2 library files and a XML file, and for each VistA connection a deployable directory of files corresponding to each station ID.
* The XML file has detail connection information for each station: IP/DNS, port, access, & verify codes for the VistAlink proxy user.

# Installation Operations

**Note:** Assumption is that this is a new install

## Install SQL Server Procedures

### *Use Microsoft’s Best practices for SQL Server install.*

## Install Weblogic Procedures

### Install Java JDK Procedures

#### Download the VA & project approved SDK from another server or directly from the Oracle/Java website: <http://www.oracle.com/technetwork/java/javase/downloads/index.html>

##### Select the “Previous Releases” link and select from the Correct OS and OS Bit Version. Download the .bin, not the RPM file. Example Below is **Linux Java 1.6 Build 31 x64**

##### Either upload the file from your local download or copy the download link, do a wget or curl command on the Linux server, and place the file in the /usr/java directory.

Curl Example: ( as root )

curl -o /usr/java/jdk-7u60-linux-x64.bin 'http://blah.com?download=blah'

##### Change permissions

##### chmod 555 /usr/java/jdk-7u60-linux-x64.bin;

##### Change to java directory:

##### cd /usr/java/;

##### Execute binary:

##### ./jdk-7u60-linux-x64.bin;

##### Fix the Symbolic/Soft links:

##### rm –rf default latest;

##### ln –s /usr/java/latest default; ln –s /u01/java/jdk1.7.0\_60 latest;

### Install Weblogic Portal software Procedures

#### Run installer as root:

#### NOTE: Yellow highlighted text = Text to type, [ENTER] = Press the Enter/Return Key

Aqua highlighted text = Visual assisted break in the Text Based UI/Readability

##### java –d64 –jar portal103\_generic.jar.zip;

Unable to instantiate GUI, defaulting to console mode.

Extracting 0%........................................................................................100%

<-------------- Oracle Installer - Oracle WebLogic Portal 10.3.6 ------------->

Welcome:

--------

This installer will guide you through the installation of Oracle WebLogic

Portal 10.3.6. Type "Next" or enter to proceed to the next prompt. If you want to change data entered previously, type "Previous". You may quit the installer at any time by typing "Exit".

Enter [Exit][Next]> [ENTER]

<-------------- Oracle Installer - Oracle WebLogic Portal 10.3.6 ------------->

Choose Middleware Home Directory:

---------------------------------

"Middleware Home" = [Enter new value or use default

"/root/Oracle/Middleware"]

Enter new Middleware Home OR [Exit][Previous][Next]> /u01/app/bea [ENTER]

<-------------- Oracle Installer - Oracle WebLogic Portal 10.3.6 ------------->

Choose Middleware Home Directory:

---------------------------------

"Middleware Home" = [/u01/app/bea]

Use above value or select another option:

1 - Enter new Middleware Home

2 - Change to default [/root/Oracle/Middleware]

Enter option number to select OR [Exit][Previous][Next]> [ENTER]

<-------------- Oracle Installer - Oracle WebLogic Portal 10.3.6 ------------->

Choose Products and Components:

-------------------------------

Release 10.3.6.0

|\_\_\_\_\_WebLogic Server [1] x

| |\_\_\_\_\_Core Application Server [1.1] x

| |\_\_\_\_\_Administration Console [1.2] x

| |\_\_\_\_\_Configuration Wizard and Upgrade Framework [1.3] x

| |\_\_\_\_\_Web 2.0 HTTP Pub-Sub Server [1.4] x

| |\_\_\_\_\_WebLogic SCA [1.5] x

| |\_\_\_\_\_WebLogic JDBC Drivers [1.6] x

| |\_\_\_\_\_Third Party JDBC Drivers [1.7] x

| |\_\_\_\_\_WebLogic Server Clients [1.8] x

| |\_\_\_\_\_WebLogic Web Server Plugins [1.9] x

| |\_\_\_\_\_UDDI and Xquery Support [1.10] x

| |\_\_\_\_\_Server Examples [1.11]

|\_\_\_\_\_WebLogic Portal [Installed] x

|\_\_\_\_\_Portal Server [2.1] x

|\_\_\_\_\_Workshop Portal Extension [Installed]

|\_\_\_\_\_Portal Examples [2.3]

\*Estimated size of installation: 847.3 MB

Enter number exactly as it appears in brackets to toggle selection OR [Exit][Previous][Next]> [ENTER]

<-------------- Oracle Installer - Oracle WebLogic Portal 10.3.6 ------------->

JDK Selection (Any \* indicates Oracle Supplied VM):

---------------------------------------------------

JDK(s) chosen for use with this product installation will be installed. Supported defaults if not deselected will be used in script string-substitution.

1|Add Local Jdk

2|/usr/java/jdk1.6.0\_31[x]

\*Estimated size of installation: 847.3 MB

Enter 1 to add or >= 2 to toggle selection OR [Exit][Previous][Next]> [ENTER]

<-------------- Oracle Installer - Oracle WebLogic Portal 10.3.6 ------------->

JDK Selection (Any \* indicates Oracle Supplied VM):

---------------------------------------------------

JDK(s) chosen for use with this product installation will be installed. Supported defaults if not deselected will be used in script string-substitution.

\*Confirmation required

\*-------------------------

\*WebLogic Server 10.3.6.0 will use uncertified JVM: Sun 1.6.0\_31

\*

\*Please consult documentation for appropriate JDK

\*Choose "Yes" to continue with the settings.

->1|Yes

2|No

Enter 1 for "Yes" or 2 for "No" OR [Exit][Previous][Next]> [ENTER]

<-------------- Oracle Installer - Oracle WebLogic Portal 10.3.6 ------------->

Choose Product Installation Directories:

----------------------------------------

Middleware Home Directory: [/drive/u01/app/bea]

Product Installation Directories:

1|WebLogic Server: [/drive/u01/app/bea/wlserver\_10.3]

2|WebLogic Portal: [/drive/u01/app/bea/wlportal\_10.3]

Enter index number to select OR [Exit][Previous][Next]> [ENTER]

<-------------- Oracle Installer - Oracle WebLogic Portal 10.3.6 ------------->

The following Products and JDKs will be installed:

--------------------------------------------------

WebLogic Portal 10.3.6.0

|\_\_\_\_\_WebLogic Server

| |\_\_\_\_\_Core Application Server

| |\_\_\_\_\_Administration Console

| |\_\_\_\_\_Configuration Wizard and Upgrade Framework

| |\_\_\_\_\_Web 2.0 HTTP Pub-Sub Server

| |\_\_\_\_\_WebLogic SCA

| |\_\_\_\_\_WebLogic JDBC Drivers

| |\_\_\_\_\_Third Party JDBC Drivers

| |\_\_\_\_\_WebLogic Server Clients

| |\_\_\_\_\_WebLogic Web Server Plugins

| |\_\_\_\_\_UDDI and Xquery Support

|\_\_\_\_\_WebLogic Portal

|\_\_\_\_\_Portal Server

\*Estimated size of installation: 847.3 MB

Enter [Exit][Previous][Next]> [ENTER]

<-------------- Oracle Installer - Oracle WebLogic Portal 10.3.6 ------------->

Installing files..

0% 25% 50% 75% 100%

[------------|------------|------------|------------]

[\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*]

Performing String Substitutions...

<-------------- Oracle Installer - Oracle WebLogic Portal 10.3.6 ------------->

Installing Patches...

0% 25% 50% 75% 100%

[------------|------------|------------|------------]

[\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*]

Creating Domains...

<-------------- Oracle Installer - Oracle WebLogic Portal 10.3.6 ------------->

Installation Complete

Congratulations! Installation is complete.

Press [Enter] to continue or type [Exit]> [ENTER]

<-------------- Oracle Installer - Oracle WebLogic Portal 10.3.6 ------------->

Clean up process in progress ...

### Create domains directory, and set permissions

( as root )

mkdir –p /u01/domains/common\_jars/connectors/;

mkdir –p /u01/domains/PCMM\_Domain/;

chown -R wlp\_user:wlp\_user /u01/domains/;

chown -R wlp\_user:wlp\_user /u01/app/bea/;

cd ;

mv bea .bea;

ln -s /u01/app/bea bea;

ln -s /u01/domains/ ;

ln -s /u01/app/bea/wlserver\_10.3/ weblogic;

ln -s /u01/app/bea/wlserver\_10.3/common/nodemanager/ ;

### Copy the latest domain files

Copy the files from approved repository, adjust the config files for the environment, severname, Database connections

# Routine Operations

Using Linux bash scripts to extract data from the different servers and systems, the data is gathered, parsed, and output in csv, xml, flat file, or direct to email. The systems administrator will monitor the WebLogic JVM - Java Virtual Machine Memory, File System usages, VistALink Adaptor connectivity via Dashboards, Consoles, or received emails. The systems administrator will also deploy the new artifacts during planned outages, stop and start the WebLogic managed servers, and monitor system backups. Routine OS patches, updates will be performed via mechanisms standard to the OS.

The database administrator will monitor database growth, replication, and backups. The database administrator will perform updates, upgrades, and maintenance to the database or database engine.

## Administrative Procedures

### System Start-up

#### Windows Database Server

* Once the server is powered on, the SQLServer database instance for CISS will automatically start. To verify service is running, open the Windows Services, locate the following:
  + SQL Server (PROD\_SQLSERVER)
  + SQL Server Agent (PROD\_SQLSERVER)
  + SQL Server Browser
  + SQL Server FullText Search (PROD\_SQLSERVER)
  + SQL Server Integration Services
  + SQL Server VSS Writer
* Log into SQL Server Management Studio to confirm SQL server database is up and running, and that you can connect to the database.
* The 5:00 A.M. backup is an OS-level scheduled task.

#### Linux Application server:

* Once the server is powered on, the WebLogic CISS Domain Node manager must be started.
  + Sudo to the weblogic user:

sudo su – wlp\_user ;

* + Start the nodemanager and background the process:

startnodemanager.sh ciss.properties

* + Allow the nodemanager to start, check by verifying the port 5556 is listening, and run the lsof command:

/usr/sbin/lsof -Pni |grep wlp\_user | grep LISTEN ;

* To start the WebLogic PCMM Domain, Node manager must be started.
  + Sudo to the weblogic user:

sudo su – wlp\_user ;

* Start the WebLogic PCMMR Domain Administrative Console:
  + bash PCMM\_Domain/startWeblogic.sh &
  + Watch for the following text in the output sent to the screen.
    - <Server state changed to STARTING>
    - <Server started in RUNNING mode>
  + Verify the Admin sever started by either the following methods:
  + Run the getstatus.sh script:
    - cd ~;
    - getstatus.sh pcmm.properties ;
    - Run the lsof command Looking for the Admin server port 5300:

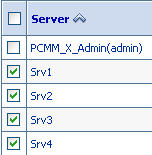
/usr/sbin/lsof -Pni |grep 5300;

* Start the WebLogic CISS managed servers using 1 of 2 methods:
  + Command Line:
    - cd ~;
    - startcluster.sh pcmm.properties ;
    - startcluster.sh pcmm\_unattnd.properties ;
    - getstatus.sh pcmm.properties ;
    - getstatus.sh pcmm\_unattnd.properties ;
    - appstatus.sh pcmm.properties;
  + Via the Admin console:

Log into the Admin console using the host name and admin port for the URL:

Example: http:// DNS apppcmm91.pcmm.cc.med.DNS :5300/console

* + - Select the Control tab
    - Select the Check box next to the managed servers ( Srv1, Srv2, … )



* + - Click the ‘Start’ button, located above the list of managed servers:



**Note:** Start time takes roughly 15 minutes.

* + - Press F5 to refresh or click the button with the curved circular arrows, to check the Status
* Verify all Mount Points are Connected:
  + As the Root User:

mount –a;

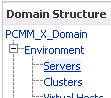
### System Shut-down

The best solution to bringing the servers offline is as follows:

* Either via command line or console, stop the WebLogic managed servers
  + Login to the WebLogic PCMM Domain Admin node server via ssh
    - sudo su - wlp\_user ;
    - cd ~;
    - stopcluster.sh pcmm.properties ;
    - stopcluster.sh pcmm\_unattnd.properties ;
    - getstatus.sh pcmm.properties ;
    - ps -ef | grep 'PCMM\_[Aa]dmin' | \

awk '{print $1}' | xargs –i kill {};

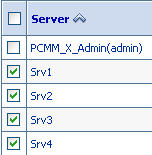
* + Or login to the WebLogic Admin console
    - Navigate to the Summery of Servers



* + - Select the ‘Control’ Tab.



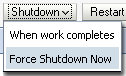
* + - Select all applicable manage servers check boxes.



* + - Click the ‘Shutdown’ menu button.



* + - Select ‘Force Shutdown Now’ from the drop-down selection.



* + - Select the ‘Yes’ button to shutdown the managed servers selected.



* + If Admin servers was not selected, repeat three previous steps to shut down the WebLogic Admin server.
* Shut down the Linux server OS.
  + Both application and web server can be shut down
    - Sudo to the Root user.
      * sudo su – root ;

WARNING: running the next command will HALT the server, unless the ILO access has been configured or there is a physical person to power on the server: (Virtual Machines this is not a concern)

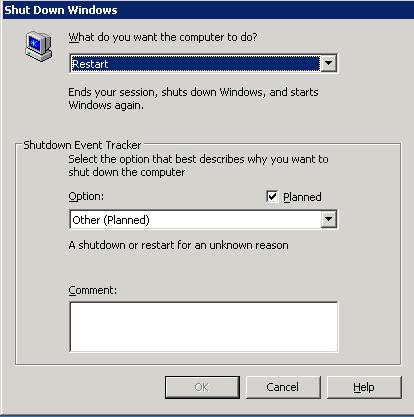
shutdown –h now.

* Shut down Windows server OS
  + The SQLServer Database engine and any other processes will be brought down normally thru the system services.
  + Shut down Windows server.
  + Click the **Start** button.



WARNING: running the next set of screen will HALT the server, unless the ILO access has been configured or there is a physical person to power on the server.

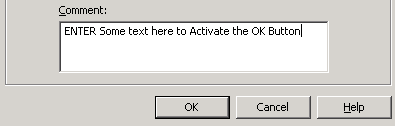
* + Change the drop-down box from **Restart** to **Shut down**:



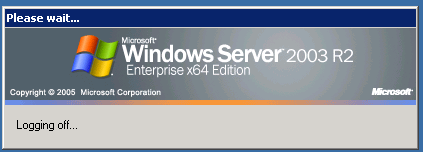
to

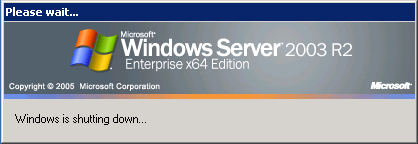


* + Enter some Reason or Comment for shutting down the server.



* + Click **OK**.





### Back-up and Restore

The production database is the only instance in the CISS/OHRS/PCMM environment where an official backup is being handled. The SQL Server database has its own mechanism for database backup and restore:

* Database backup procedures: (see Section 3.1.3.1)
* Database restore procedures: (see Section 3.1.3.2)
* Describe Database Backup/Mirroring

*Described in this section.*

#### Back-up Procedures

* + - * Database
* The Database Administrator can elaborate. The internal backup schedule backs up the Transactional log and all databases, each exported to their own separate directories and corresponding database names.
* Two nightly backups are performed
* 9:00 p.m. -- mostly for the previous day’s transactions
* 4:00 a.m.
  + - * SAN Device
* Every evening a full back up is run at 6:00 P.M. and the following drives (e.g., G:\ , H:\ ) are being backed up to tape (mentioned in the section Storage and Rotation).

#### Restore Procedures

* + - * SAN Device
* Daily Linear Tape-Open (LTO) tapes are stored locally at the site.
* An official request must be made to the EMC staff to restore data from tape and an alternate location must be established to restore the file(s).
  + - * Database
* A full database backup is performed each morning at 4:00 a.m. immediately followed by a Transaction Log backup. The same process is repeated at 9:00 p.m. The backup files are stored on a drive that is distinct from the database files. The database files are archived on to the disaster recovery server, and the storage area network engineers perform server level backups that send the files to a secure off-site facility. The backup and recovery policy used for the CISS\_PROD database is through SQL Server Maintenance Plan backups. Recovery is achieved by using SQL Server Enterprise manager, selecting “Restore Database” under database tasks and selecting the latest backup and transaction log file.

#### Back-up Testing

Not applicable

#### Storage and Rotation

* + - * Use EMC Networker 7.6 as the backup application/system to back up all hosts in Capitol Region Readiness Center, Martinsburg (CRRC), West Virginia, and Hines (HITC), Illinois data centers to tape.
      * Both CRRC and HITC also use new tape libraries as tape backup systems. Each of these new tape library units provide Linear Tape-Open (LTO)-4 tape drive systems to backup data to tape (LTO-4 tapes will support 800GB native/1600GB compressed of data).
      * Backups are performed daily/nightly via the network for most systems.
      * Times in which backups are performed are based on the requirements and input of the corresponding project owner, Database Administrator (DBA), application owners, etc.
      * Type of backups performed are weekly full and daily incremental.
      * EMC staff performs a monthly backup which is retained per VA long-term retention policies.
      * Tape rotation: all short-term retention tape backups (90 days or less) rotate based on the need and when tapes have expired.
      * All short-term retention tape backups are temporarily stored in a secure location onsite (once the tapes have been ejected from the tape library) until they have expired and can be recycled/reused.
      * All long-term retention tape backups are stored at a secure offsite facility (Iron Mountain). They will usually do one scheduled pick up per week – tapes are shipped offsite on a routine basis using this system.
      * Retention is based solely on the requirements of the specific project – the standard for the retention of all backup data is 90 days, and then the tapes are recycled. Monthly backups are retained for two years (at Iron Mountain) under the current standard VA retention policy (mentioned above).

## Security / Identity Management

CISS/PCMM has many levels of security, starting at the OS layer, to the application portal, database, CISS, and PCMM applications. Each section below will have different methods or levels of complexity.

### Identity Management

* + - * OS:

Users are identified by their roles in the project, by the VA and contracting staff. Roles and permissions are determined by the Systems Admin and Database Admin, and are communicated to the team.

* + - * WebLogic:

Users request access to the WebLogic application from the Systems Administrator. The SA determines access needs, and reviews alternate means of access to assist the user’s request. If console access is required, READ-ONLY/MONITOR user access is given to the request, unless more access is necessary.

* + - * Portal:

Users request access from their local occupation administrative staff and the request is communicated to the VA PM for approval. The VA PM will grant the user access using LDAP to associate the users VA ID with the CISS/PCMM LDAP organizational unit (OU).

* + - * PCMM application:

User portal access establishes the user’s roles and privileges and options usability within the PCMM application.

### Access control

* + - * OS:
* Users are identified by their role in the project or dependency, and granted the minimum access to achieve their task or role.
* Using their VA-issued log in as their account,
  + - The account is created with details of the person’s name and title.
    - Specific rights are given to the user’s log in, and any additional sudo (Linux) rights and privileges are configured.
    - (Linux) The amount of time the user requires access determines their account expiration.(min 1 day )
      * WebLogic:

User is added via the Console

* + - Password and roles assigned.
      * Portal:

All users can access the portal using their VA user ID and password.

* + - * PCMM:
* Only the USER ID associated with the CISS portal will be granted to the PCMM button to access the PCMM application.
* Each person is granted a role or set of roles in the PCMM application, and depending on the role, each person has access to different aspects to the PCMM application and permission to execute different tasks within the application.

## User Notifications

The Systems or Database Administrator informs the project team of a request for an outage window. The project team requests, via daily meetings and/or email, from the VA systems Owner (VA PM), permission for a scheduled outage window. The VA PM notifies the User Community of the Outage and its implications.

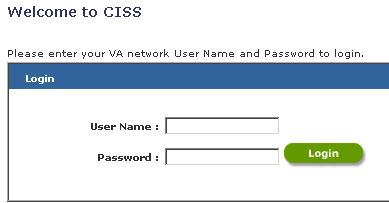
## System Monitoring, Reporting, and Tools

* + - * OS
* The Linux servers have standard monitoring scripts that send emails to the root user. Those standard scripts, in conjunction to Multi Traffic Router Graph (MRTG), and some custom scripts inform the Systems and Database Administrators of any issues or pending issues. (These are being re-worked, re-configured.)
* No tool can monitor every aspect, so custom scripts are created to run against Windows, Linux SNMP, and the WebLogic Scripting Tool (WLST).
* MRTG and/or custom charts are used for its ability to chart any numerical data and has other underlying abilities.
* Using PHP, WLST, MRTG, custom scripts, and system-generated emails, the Systems Administrator has a wealth of options and avenues in monitoring the systems.
  + - * Database Administration :
* The Microsoft SQLServer has some internal Reporting and Monitoring capabilities.
* Emails are sent to the Systems Admin and Database Admin for the nightly backups.
* The Replication manager tool within the Enterprise Studio is used in order to monitor the performance of replication between the CISS-PCMM server and DR servers.
  + - * SSRS (PCMMR’s reporting tool):

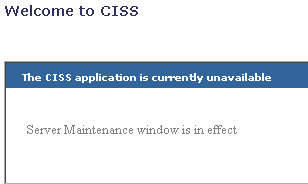
### Availability Monitoring

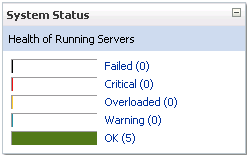
Availability of the CISS/OHRS/PCMM application:

* + - * Launch a browser to the application URL:
* The traffic will pass through the Load Balancer to the WebLogic servers.
* Web Help traffic passes through the Load Balancer to the Apache servers, and is redirected via iRule on the Load balancers.
* The load balancer will validate the connectivity to the WebLogic-managed server located on the Application server.
  + - If the application is available, the network traffic is passed to the WebLogic-managed server.

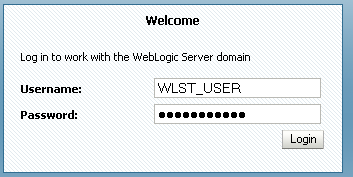


* + - If the application is not available, the traffic is re-directed to a static Error/Maintenance webpage.

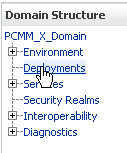


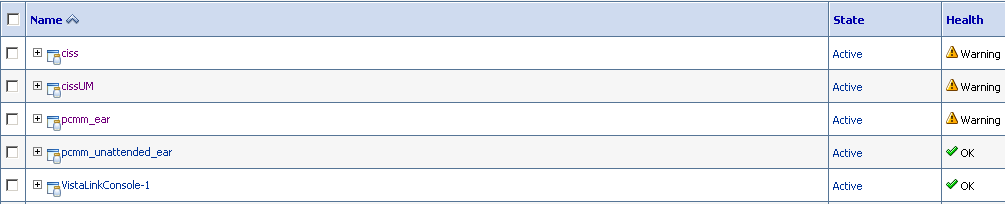


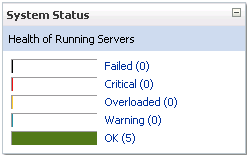
* + - * WebLogic PCMM Domain Administration Console
  + Log into the Admin console:



* + Navigate to the Deployments page.



* + Review the Deployed Applications for any potential Issues, Warning:
  + Review the Health of the Running Managed servers:



### Performance/Capacity Monitoring

* + - * Using the MRTG application, systems can be monitored for performance and capacity using the data captured. MRTG charts assist the DBA and SA in their overall analysts of the capacity and recommendations accordingly.
* Server network bandwidth, speed, usage.
* WebLogic: Java Virtual Memory (JVM) heap sizes, and usage
* File System: size, usage, Input/output
* System uptime, system or IO wait, usage
  + - * Data can be analyzed actively, on demand, or post event. Each is made available via different means.

### Critical Metrics

* + - * Additional Metrics need to be identified for future monitoring
      * Hard disk drive (HDD) usage
      * Network usage
      * Input / Output (I/O) to the HDD
      * WebLogic can monitor JMS messaging and the Console can show problems. The need for monitoring has been very minimal; and no further action has been requested.

## Routine Updates, Extracts and Purges

* + - * Database
* DBA to expand on updates , extracts, and any purges
* SDS update
* An email is sent to all projects that officially use the SDS database.
* A manual update is done by the Database Administrator and requires the PCMM application to be recycled. This allows clean connections to the updated data.
* Database extracts are performed periodically for use in the PROD Mirror and SQA testing Databases. DBA to expand.

## Scheduled Maintenance

Every month, all OS patches and WebLogic updates are performed using Development Lifecycle procedures, scheduling outages with the team and customer.

## Capacity Planning

Twice a year the SA, DBA, and project team will review the capacity and performance of the previous year, noting any potential areas of interest, and making any recommendations and adjustments. From this meeting, a plan of action will be scheduled and any outage requests sent to the VA PM.

# Exception Handling

## Routine Errors

Like most systems, may generate a small set of errors that may be considered “routine.” These errors are routine in the sense that they have minimal impact on the user and do not compromise the operational state of the system. Most of the errors are transient in nature and only require the user to retry an operation. The following sub-sections describe these errors, their causes, and what, if any, response an operator needs to take.

While the occasional occurrence of these errors may be routine, getting a large number of an individual error over a short period of time is an indication of a more serious problem. In that case, the error needs to be treated as an exceptional condition.

### Security

Error:

“Reverse mapping checking getaddrinfo for xxxx-lt.vha.med.DNS failed - POSSIBLE BREAK-IN ATTEMPT!”

This error is normal because of the slowness of the VPN DNS updates.

A user connects via VPN into the VA network and the DNS system should be updated with the connecting Workstation/Laptop hostname are associated with the IP address. The DNS is slow to propagate the changes across the VA network. When the Linux server does a reverse lookup of the requesting IP, the discrepancy of Hostnames occurs.

### Time-outs

* Each user has a 15-minute inactive timer on the Linux servers. Once the time has expired, their current session is logged out.
* VistAlink Adapters have timeouts, while attempting to connect to the configured Port and IP for the associated Station ID.

### Concurrency

Not applicable

## Significant Errors

Significant errors can be defined as errors or conditions that affect the system stability, availability, performance, or otherwise make the system unavailable to its user base. The following sub-sections contain information to aid administrators, operators, and other support personnel in the resolution of errors, conditions, or other issues.

* Apache, SSH, OS, WebLogic -Database Connection, JVM sizes, and deployable artifact problems.

### Application Error Logs

* + - * Apache
* All Apache logs are written to the directory /var/log/httpd/, unless specially identified in the Apache configuration files.
  + - * Security / SSH
* /var/log/secure
  + - * General Messages
* /var/log/messages
  + - * Application Messages
* {DOMAIN Home}/logs
  + - * WebLogic Managed servers
* {DOMAIN Home}/servers/{MANAGED server}/logs/

### Application Error Codes and Descriptions

Not applicable

### Infrastructure Errors

#### Database

One error situation with SQL Server databases, which is encountered sometimes in situations where a DBA has not been continuously hands-on monitoring the database, occurs when the size of the Transaction Log file grows so large that there is a danger of running out of disk space. This is a serious issue. Normally, the size of the database files needs to be monitored such that this situation will not occur.

The correct way to control the growth of the Transaction Log file is to regularly perform a full database backup and IMMEDIATELY follow it with a Transaction Log backup. This process may even be back-to-back repeated one time; this should shrink the size of the Transaction Log.

Note however, in a replicated scenario like CISS, if the replication queue is broken, then the transaction log grows in size, and it does not shrink even with the backup. In this case, the replication needs to be restored first so that the queues get flushed.

A rarely encountered but serious error situation happens if the SQL Server database were to ever go into suspect status. In this situation, the only way to recover would be to have the latest database and transaction log files available, and run the following steps one at a time:

* EXEC sp\_resetstatus 'CISS\_PROD';
* ALTER DATABASE CISS\_PROD SET EMERGENCY;
* DBCC checkdb('CISS\_PROD');
* ALTER DATABASE CISS\_PROD SET SINGLE\_USER WITH ROLLBACK IMMEDIATE;
* DBCC CheckDB ('CISS\_PROD', REPAIR\_ALLOW\_DATA\_LOSS);
* ALTER DATABASE CISS\_PROD SET MULTI\_USER;

#### Web Server

Most errors are syntax errors after modifying the configuration files; check syntax and verify against another Apache configuration file.

#### Application Server

* + - * VistAlink errors:
* Root cause exception:gov.va.med.vistalink.security.m.SecurityTooManyInvalidLoginAttemptsFaultException:Fault Code: 'Server'; Fault String: 'Logon Failed'; Fault Actor: '';Code: '183005'; Type: ''; Message: 'Logon failure: 'Device/IP address is locked due to too many invalid signon attempts.'' ">
* ResourceAllocationException thrown by resource adapter on call to ManagedConnectionFactory.createManagedConnection(): "gov.va.med.vistalink.adapter.cci.VistaLinkResourceException: Cannot create VistaSocketConnection; Root cause exception: gov.va.med.net.VistaSocketException: Cannot create TCP/IP socket.; Root cause exception: java.net.ConnectException: Connection refused ">

#### Network

Network failures are reported in numerous locations: the DMESG system, /var/log/messages, the application logs, and the WebLogic-managed server’s logs. The nature of the problem determines where the error will be reported.

#### Authentication & Authorization

Errors of authentication could be reported in the associated logs.

* Linux

The /var/log/secure files will report any issues connecting and authenticating the user.

* WebLogic Administration console

{DOMAIN Home}/servers/{Admin server}/logs/{Admin server}.log

## Dependent System(s)

Not applicable.

## Trouble Shooting

Not applicable

## System Recovery

The following sub-sections define the process and procedures necessary to restore the system to a fully operational state after a service interruption. Each of the sub-sections starts at a specific system state and ends up with a fully operational system.

### Restart after Non-Scheduled System Interruption

* Use Section 3.1.1 for the actual details.
* Verify database servers are started, and database is running.
* Verify web server is started, and Apache is running.
* Verify the application server is started, start weblogic admin application server, start managed servers.

### Restart after Database Restore

Follow Section 7 - Disaster Recovery.

# Continuity of Operations

Not applicable

# Disaster Recovery

DR is a manual process.

## Required:

Access to CRRC and IHTA via the following servers:

* WebLogic Admin servers ( DNS apppcmm81.cc.med.DNS :5100, DNS apppcmm81.cc.med.DNS :5300 )
* SQL Database server (DNS dbspcmm81.vha.med.DNS , )

## Assumptions:

* Production environment, passwords, SQL server DBA skills, RHEL / MS Windows 2012 SA skills, proper user level permissions, all servers are running at proper/normal runtime levels.
* These procedures assume that the fail-over is planned and all sites are operational. They do not discuss returning to normal operations, which could be done by executing the same procedures with HITC as the initial site and CRRC as the destination.
* If the primary data center is down, you will need to rely on the replicated database at the DR site.

## WebLogic Server (CRRC):

*Check with other CISS partners before stopping CISS*

* Log into the node of the WebLogic application server.
* Check the Status of the WebLogic system:
* Command Line:
  + - Sudo to the wlp\_user user:
* sudo su – wlp\_user ;
  + - Run the following:
    - cd ~;
    - getstatus.sh pcmm.properties;
    - getstatus.sh pcmm\_un\*.properties;
* Shut down the managed servers
* Command Line:
  + - Sudo to the wlp\_user user:
* sudo su – wlp\_user ;

Run the following:

* + - cd ~;
    - stopcluster.sh pcmm.properties;
    - stopcluster.sh pcmm\_un\*.properties;

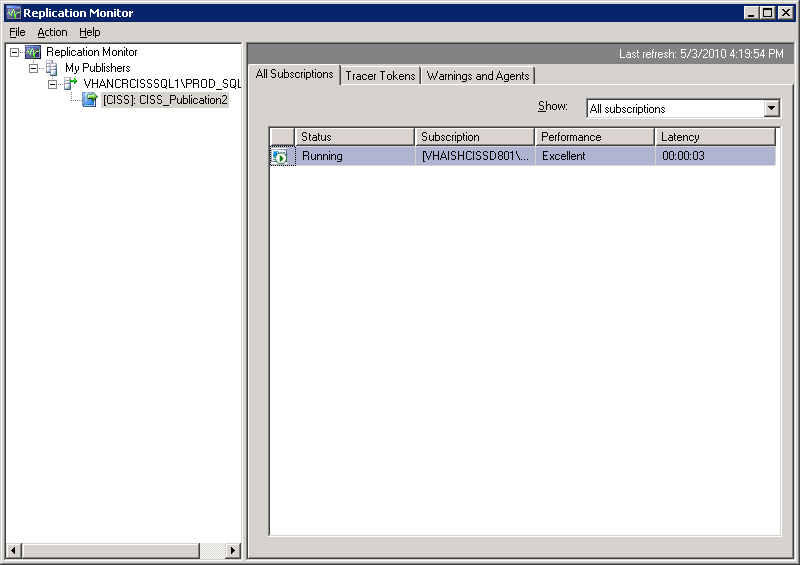
**If servers will not stop/die, kill the PID of the Managed servers**

* + - * ps –ef | grep [Ss]rv | awk '{print $2}' \

| xargs –i\ kill -9 {}

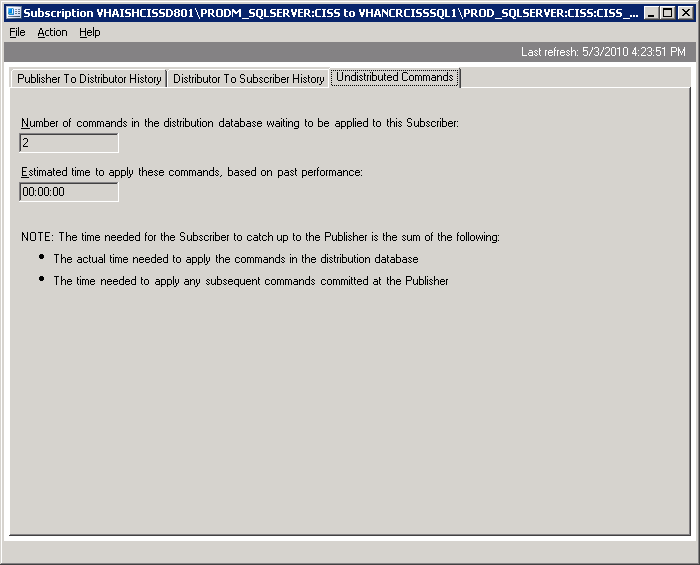
## Database server (CRRC):

* Log into the Primary Windows SQL server machine.
* Make sure that DB is running and that there are no transactions happening.
  + Start -> All Programs -> Microsoft SQL Server 2012 -> SQL Server Management Studio using the SYSTEM user.
  + Right click Replication -> Launch Replication Monitor



* + Double-click the Subscription name in the right-side window.
  + Click on **Undistributed Commands** – the number of commands waiting should be zero.

If it is not zero, press F5 to refresh screen until it is zero.



* Stop replication by running script Dropreplication.sql stored in the Clear Case stream Dev\_CISS\_Data\_mgt in the CISS\_db\Production Maintenance\Replication vobs.
* Make sure the application is disconnected from the database and make a backup of the CISS\_PROD database.
  + GZIP the Database backup and XCOPY to Hines.

## Database server (Hines):

* Log into the Primary Windows SQL server machine.
* Make sure that DB is running and that there are no transactions happening.
  + Unzip/WinRAR - the CRRC Backup.
  + Restore the CRRC backup to CISS\_PROD database.
  + Confirm Users can connect to the Database.

## WebLogic server (HITC):

* Log into the node of the WebLogic application server.
  + Once given the “GO” from the DBA
* Start the weblogic managed servers:
  + Command Line:
    - Sudo to the wlp\_user user
    - sudo su – wlp\_user ;
    - Start ALL the Managed servers
    - startcluster.sh pcmm\_unattnd.properties;
    - startcluster.sh pcmm.properties;
* Verify that the WebLogic is running:

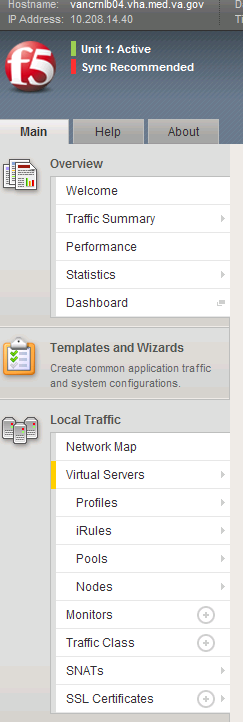
[http://vaww-dr.ciss.med.DNS /](http://vaww-dr.ciss.med.DNS   /)

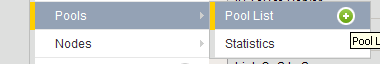
**Note:** this link is only valid after following the instructions above.

* Have testers smoke test the system

## Checking the Load Balancer (CRRC):

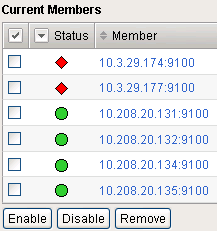
* Log into https://IP /tmui/login.jsp. ( You Must have an Account on the Load Balancer )



* Select Local Traffic >> Pools >> Pool List
* 
* Enter “\*CISS\*” in the Search Box at the Top of the List
* Select CISS\_Production Pool
* Select Members Tab



* + Weblogic Servers that are Active will be represented in Green Circles.
  + The Black Diamond is an inactivated node.The Red Diamond is an inactive node.



* The Load Balancer should balance the LOAD to the Active servers (e.g., Hines or FW-Martinsburg)
  + Enter “\*CISS\*” in the Search Box at the Top of the List.

# Back-Out Procedures

## Database

Restore backup before initial database updates.

## Weblogic

* During initial setup, shut down WebLogic domain JVM’s.
* Update release, simple removal of updated artifacts, restore previous artifacts, and restart domain.

## Vista Patches

Once a patch has been applied to theVista system there is no back-out procedure.

# System Support

An understanding of how System Name is supported by various organizations within the VA is important to operators and administrators of the system. In the event that you are unable to resolve an issue, then it is necessary to understand how to obtain support through OI&T’s system support organizations. The following sections describe the support structure and provide procedures on how to obtain support.

The information in these sub-sections is a summary of parts of the CISS/PCMM O&M plan. This document is available in ClearCase and should be used if additional information is required.

## Support Structure

This section describes the systems support structure as seen from the perspective of operations personnel. The first section defines the support hierarchy through which a support request may navigate. The second section defines the responsibilities for each level of support.

### Support Hierarchy

* Network

An email or phone call must be made to the VA National Service Desk for the NSOC staff to investigate.

* Servers Hardware

After a system administrator has evaluated the problem regarding hardware or beyond his abilities to fix or repair, the Hardware Vendor – HP, needs to be contacted and their staff will require additional information to troubleshoot the problem.

* Operating systems

Each vendor (Microsoft and Red Hat) has a designated VA representative and that person should be contacted initially to help escalate the issues to the vendor’s support systems.

* WebLogic

Must have a Oracle Support ID and Login to contact Oracle support. There is a POC in the VA who manages the Oracle Support Identifiers.

* SQLServer

Please follow up with the Microsoft Representative.

### Division of Responsibilities

* Support Tier 1: National Service Desk
* Support Tier 2 : CISS/PCMM Project Staff, Primary Analysis
* Support Tier 3: SA, DBA, Developers

## Support Procedures

Not applicable