**Patient Centered Management Module (PCMM)**

**Deployment, Installation, Back-Out, and Rollback Guide (DIBRG)**



**December 2022**

**Version 1.0**

**Department of Veterans Affairs**

**Office of Information and Technology**

**Revision History**

| **Date** | **Version** | **Author** | **Description** |
| --- | --- | --- | --- |
| 12/30/2022 | 1.0 | REDACTED | Baseline Version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**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 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 as needed throughout the life cycle of the project for each build.

**Table of Contents**

[1 Introduction 7](#_Toc123293380)

[1.1 Purpose 7](#_Toc123293381)

[1.2 Dependencies 7](#_Toc123293382)

[1.3 Constraints 8](#_Toc123293383)

[2 Roles and Responsibilities 9](#_Toc123293384)

[3 Deployment 10](#_Toc123293385)

[3.1 Site Readiness Assessment 10](#_Toc123293386)

[3.2 Deployment Topology (Targeted Architecture) 10](#_Toc123293387)

[3.3 Resources 10](#_Toc123293388)

[3.3.1 Hardware 10](#_Toc123293389)

[3.3.2 Software 11](#_Toc123293390)

[3.3.3 Communications 12](#_Toc123293391)

[3.4 Deployment/Installation/Back-Out Checklist 12](#_Toc123293392)

[4 Installation 13](#_Toc123293393)

[4.1 Pre-installation and System Requirements 13](#_Toc123293394)

[4.1.1 Update Configuration Files 13](#_Toc123293395)

[4.1.2 Copy the ear Files to the Servers 14](#_Toc123293396)

[4.1.3 Import the LDAP Certificates to the Trust Stores 14](#_Toc123293397)

[4.2 Installation Procedure 14](#_Toc123293398)

[4.2.1 Stop Apache and Mirth Connect Services 14](#_Toc123293399)

[4.2.2 Add Startup Parameters to Managed Servers 14](#_Toc123293400)

[4.2.3 Stop the Managed Servers and Delete the Old Build 15](#_Toc123293401)

[4.2.4 SQL Database Changes 15](#_Toc123293402)

[4.2.5 Delete Files from Managed Server Folders 15](#_Toc123293403)

[4.2.6 Modify LDAP Parameters in ciss.properties File 15](#_Toc123293404)

[4.2.7 Deploy the Latest Build 16](#_Toc123293405)

[4.2.8 Start Apache and Mirth Connect Services 16](#_Toc123293406)

[4.3 Installation Verification Procedure 16](#_Toc123293407)

[4.4 System Configuration 16](#_Toc123293408)

[4.5 Database Tuning 16](#_Toc123293409)

[5 Back-Out 16](#_Toc123293410)

[5.1 Back-Out Procedures 16](#_Toc123293411)

[5.1.1 Database 16](#_Toc123293412)

[5.1.2 Application EAR Files 16](#_Toc123293413)

[5.2 Authority for Back-Out 17](#_Toc123293414)

[6 Rollback Procedure 17](#_Toc123293415)

[6.1 Rollback Considerations 17](#_Toc123293416)

[6.2 Rollback Criteria 17](#_Toc123293417)

[6.3 Rollback Risks 17](#_Toc123293418)

[6.4 Authority for Rollback 18](#_Toc123293419)

[6.5 Rollback Procedure 18](#_Toc123293420)

[6.6 Rollback Verification Procedure 18](#_Toc123293421)

[7 Risk and Mitigation Plan 18](#_Toc123293422)

[Appendix A: Acronyms and Abbreviations 19](#_Toc123293423)

**List of Tables**

[Table 1 – PCMM Application Dependencies 7](#_Toc86697501)

[Table 2 – Deployment, Installation, Back-Out, and Rollback Roles and Responsibilities 9](#_Toc86697502)

[Table 4 – Hardware Specifications 11](#_Toc86697503)

[Table 5 – Software Specifications 11](#_Toc86697504)

[Table 6 – Deployment/Installation/Back-Out Checklist 12](#_Toc86697505)

[Table 7 – Acronyms and Abbreviations 27](#_Toc86697506)

**List of Figures**

[Figure 1 – Deployment Topology (Targeted Architecture) 10](#_Toc86697507)

# Introduction

This document describes how to deploy and install the Patient Centered Management Module (PCMM) release WEBP\*1.0\*27 and how to back out and roll back to a previous version or dataset.

This document further details the criteria for determining if a back-out is necessary, the authority for making that decision, the order in which installed components will be backed out, the risks and criteria for a rollback, and the authority for acceptance or rejection of the risks.

## Purpose

The purpose of this document is to provide a single, common plan that defines how the VA PCMM implementation will be deployed and installed, including how it is to be backed out and rolled back, if necessary.

The plan also identifies resources, a communications plan, and rollout schedule. Specific instructions for installation, back-out, and rollback are included in this document.

## Dependencies

The PCMM application is dependent on the following systems, applications, and services:

Table 1 – PCMM Application Dependencies

| **Dependency** | **Type** | **Dependency Type** | **PCMM Use** |
| --- | --- | --- | --- |
| Cerner Millennium | System | System | Cerner EHR solutions share a single design, which eases information sharing across care teams and venues. Care teams across the continuum use the system to document and access critical patient data, streamline workflows, and help with patient safety for active-duty service members, dependents, and Veterans. |
| Cerner OPENLink | Service | Data/Information | The Cerner interface engine providing extensive data transformation, message routing, and communications-protocol bridging. |
| VA SSH File Transfer Protocol (SFTP) Site | Service | Data/Information | The SFTP Site will be set up by the OEHRM group to allow for file transfers between VA and Cerner for various data-migration and syndication activities, including transfer of the patient, staff, and encounter files discussed in this document. |
| Corporate Data Warehouse (CDW) | Service | Data/Information | CDW is an internal data service that interacts with and queries CDW-cached data. Data will be a scheduled task to load CDW into the PCMM environment. CDW data will reside within PCMM for lookup and reference within the PCMM decision logic. The data will have their own designated datastore due to being relational data. |
| Clinical Information Support System (CISS) | System | System | PCMM utilizes the Clinical Information Support System (CISS) framework as part of its implementation but does not share a CISS portal with any other application or partner systems outside of PCMM functionality |
| VistA | System | System | Synchronizes CPRS header information from VistA for PCP assignment status or Mental Health Treatment Coordinator (MHTC) assignment. |
| Master Patient Index (MPI) | System | System | Registers a patient from MPI broadcast messages and updates patient traits from MPI. |

## Constraints

The PCMM project team, software, and test servers will adhere to the following directives, policies, procedures, standards, and guidelines:

* Veteran-focused Integration Process (VIP)
* Section 508 Information Technology (IT) accessibility standards governed under 29 U.S.C 794d
* Health Insurance Portability and Accountability Act (HIPAA)
* VA DIRECTIVE 6508 – Privacy Impact Assessments
* VA Directive 6500 – Information Security Program
* One (1) VA Technical Reference Model (TRM)
* VA Standards & Conventions Committee (SACC) Codes Standards and Conventions
* PCMM will pass any Web Application Security Assessment (WASA) scans.
* PCMM will not have any critical or high issues identified by a Fortify scan.

# Roles and Responsibilities

The following table identifies the interface’s deployment, installation, back-out, and rollback roles and responsibilities.

Table 2 – Deployment, Installation, Back-Out, and Rollback Roles and Responsibilities

|  |  |  |  |
| --- | --- | --- | --- |
| **Team** | **Contact** | **Phase / Role** | **Tasks** |
| REDACTED | REDACTED | Build and Deployment in Local Dev | Plan and schedule deployment in local environment. |
| REDACTED | REDACTED | Deployment in Software Quality Assurance (SQA)/User Acceptance Testing (UAT) in Department of Veterans Affairs (VA) | Support in configuration and access to production and SQA environments |
| REDACTED | REDACTED | Production System Administrator | Production deployment |
| REDACTED | REDACTED | Project Manager | Plan and coordination of installation |
| REDACTED | REDACTED | Installation | Validate through facility point of contact (POC) to ensure that IT equipment has been accepted using asset inventory processes. |
| REDACTED | REDACTED | Back-out | Confirm availability of back-out instructions and back-out strategy. (What are the criteria that trigger a back-out?) |
| REDACTED | REDACTED | Post Deployment | Hardware, software, and system support |

# Deployment

The deployment is planned as an iterative rollout.

## Site Readiness Assessment

The PCMM application will exist within the VA Enterprise Cloud (VAEC) for SQA, ETS, INT, and production environments. The PCMM development team will maintain a local DEV environment to be used for sprint development and testing processes.

## Deployment Topology (Targeted Architecture)

The figure below details the PCMM Deployment Topology (Targeted Architecture).

REDACTED

Figure 1 – Deployment Topology (Targeted Architecture)

## Resources

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

### Hardware

PCMM is an enterprise application hosted at the VA Austin Information Technology Center (AITC).

The PCMM servers consist of eight virtual servers (VM), consisting of three application servers to accommodate end-user work, two application servers to support web service calls, and two database servers and one file share server to act as a quorum witness to the database cluster. Redundancies are achieved through replication of data at both the OS and application levels.

The architectural design of each group consists of different redundancies:

* The database servers are clustered at the Operating System (OS) level and database-application level. They are connected to a NetApp Data Storage to provide additional storage, redundancy, and availability.
* The application servers are not clustered at the OS level, but at the application level in two clusters: attended and unattended. Currently, the attended cluster contains one WL server and the unattended cluster contains two WL servers. OS-level implemented synchronization and application clustering maintain the redundancies.

Table 4 – Hardware Specifications

|  |  |  |  |
| --- | --- | --- | --- |
| **Required Hardware** | **Quantity** | **Version** | **Configuration** |
| Application Server | 3 | Linux-RHEL7.3 | Attended Linux application server with WebLogic and Apache Web Server |
| Application Server | 2 | Linux-RHEL7.3 | Unattended application server with WebLogic |
| Database Server | 2 | Linux-RHEL7.3 | Windows database server for PCMM-Web application |
| File Share Server | 1 | Linux-RHEL7.3 | Windows File Share Server |

### Software

The following table describes software specifications required prior to deployment. If there are site-dependent differences, those difference will need to be provided.

Table 5 – Software Specifications

| **Required Software** | **Manufacturer** | **Version** | **Configuration** |
| --- | --- | --- | --- |
| Oracle WebLogic Server | Oracle | 12.2.1.4.0 | Standard |
| Java™ SE Development Kit 7 | Oracle | jdk1.8.0\_341 (or higher) | Standard |
| Microsoft SQL Server | Microsoft | 2019 (or higher) | Standard |
| Microsoft SQL Server Management Studio (SMS) | Microsoft | 2019 (or higher) | Standard |
| Apache | Apache | 3.0.5 (or higher) | Standard |
| jTDS driver | SourceForge | jtds-1.3.1.jar | Standard |
| VistALink | VistA | 1.6 | Standard |
| Mirth Connect | MirthCorp | 3.10 (or higher) | Standard |
| Python | Python | 3.6.8 | Standard |

### Communications

* Notifications 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 scheduled events.
* Notifications to VA users for unscheduled system outages or other events that impact response times will be distributed within 30 minutes of an occurrence.
* Notifications to VA users for unexpected system outages or other events that impact the response time will be distributed to users as soon as possible
* Notifications will be distributed to VA users regarding technical help-desk support for obtaining assistance with receiving and processing.

## Deployment/Installation/Back-Out Checklist

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

Table 6 – Deployment/Installation/Back-Out Checklist

| **#** | **Activity** | **Responsible Party** | **Start Time** | **Duration** |
| --- | --- | --- | --- | --- |
| 1 | PRE01 – Add new parameters to pcmm.properties and ciss.properties files on REDACTED. | REDACTED |  | 20 min |
| 2 | PRE02 – Create folder in /u01/app/BUILDS and copy the new build ear files to servers REDACTED. | REDACTED |  | 45 min |
| 3 | PRE03 – Import the LDAP certificates into the trust store on every app server | REDACTED |  | 90 min |
|  | **Production Deployment 9:00 PM Eastern** |  |  |  |
|  | 1 REDACTED – Stop Mirth Connect, Apache | REDACTED |  | 5 min |
|  | 2 All managed servers – In the WebLogic console, add the new startup parameters to all of the managed servers. | REDACTED |  | 10 min |
|  | 3 All servers – Stop the WebLogic managed servers | REDACTED |  | 10 min |
|  | 4 REDACTED – Delete the old pcmmr and pcmmr\_unattended deployments | REDACTED |  | 5 min |
|  | 5 REDACTED – Delete the old pcmmr deployment | REDACTED |  | 5 min |
|  | 6 All servers – Delete the cache, tmp, and stage folders from each managed server folder | REDACTED |  | 10 min |
|  | 7 All servers – Modify the ldap parameters in ciss.properties to use secure LDAP | REDACTED |  | 10 min |
|  | 8 REDACTED – Deploy the new pcmmr and pcmmr\_unattended ear files. | REDACTED |  | 10 min |
|  | 9 REDACTED – Start the WebLogic managed servers | REDACTED |  | 5 min |
|  | 10 REDACTED– Deploy the new pcmmr ear file | REDACTED |  | 10 min |
|  | 11 REDACTED – Start the WebLogic managed server | REDACTED |  | 5 min |
|  | 12 REDACTED– Start Apache, Mirth Connect, and SmartApp | REDACTED |  | 5 min |
|  | Smoke test (logon, SmartApp, search in Cerner for staff/patient, search in Vista) | REDACTED |  | 20 min |
|  | Test web services | REDACTED |  | 10 min |
|  | User validation – batch reassign or unassign multiple patients to or from a team; test CPRS pop-up window | REDACTED |  |  |

# Installation

## Pre-installation and System Requirements

### Update Configuration Files

**pcmm.properties**

Make a copy of the existing pcmm.properties file and then add the following parameters to file on every app server:

persistence.query.timeout=600000

persistence.lock.timeout=600000

scheduledJobs.patientAutoInactivation.encounterBackdateOverlap=3

**ciss.properties**

Make a copy of the existing ciss.properties file and then add the following parameters to file on every app server:

setSSLEnvFromProps=false

### Copy the ear Files to the Servers

Follow the existing naming convention and create a folder in /u01/app/BUILDS on REDACTED.

Example: /u01/app/BUILDS/2022.12.08\_0935-1. 27. 02

Copy pcmmr.ear and pcmmr\_unattended\_ear-1.0-27-02.ear to REDACTED, and pcmmr.ear to REDACTED.

### Import the LDAP Certificates to the Trust Stores

Import the server certificates for all of the VA LDAP servers into the trust store on each application server. There are a total of 23 certificates to import. Copy the certificates to REDACTED on each server. Use this example to import the certificates:

REDACTED

## Installation Procedure

### Stop Apache and Mirth Connect Services

Stop the Apache and Mirth Connect services on REDACTED:

dzdo service mcservice stop

dzdo service httpd stop

Verify the services are stopped:

dzdo service mcservice status

dzdo service httpd status

### Add Startup Parameters to Managed Servers

In the WebLogic console on REDACTED, go to each managed server, and select the Configuration – Server Start tab. Paste the following at the end of the values in the Arguments section:

- REDACTED

Note: Enter the correct password; adjust store name for the web services servers.

### Stop the Managed Servers and Delete the Old Build

In the WebLogic console on REDACTED, stop each managed server. Delete the previous deployments of pcmmr and pcmmr\_unattended.

### SQL Database Changes

SQL database changes are not applicable for this installation.

### Delete Files from Managed Server Folders

On each server, delete cache, stage, and tmp from the managed server folder.

Example:

cd /u01/app/oracle/user\_projects/domains/PCMM\_Domain/servers/ REDACTED

rm –rf ./cache/

rm –rf ./stage/

rm –rf ./tmp/

### Modify LDAP Parameters in ciss.properties File

On each server, make a copy of the existing ciss.properties file and modify the LDAP parameters to use secure LDAP.

Change the following lines:

ldapReadServerUrl1=REDACTED

ldapReadServerUrl2=REDACTED

ldapWriteServerUrl1=REDACTED

ldapWriteServerUrl2=REDACTED

To

ldapReadServerUrl1= REDACTED

ldapReadServerUrl2= REDACTED

ldapWriteServerUrl1= REDACTED

ldapWriteServerUrl2= REDACTED

### Deploy the Latest Build

In the WebLogic console deploy the new pcmmr.ear file on REDACTED. Deploy pcmmr\_unattended\_ear on REDACTED.

Target pcmmr to the AttendedCluster. Target pcmmr\_unattended to the UnattendedCluster.

The deployment order should be set to 95 for pcmmr and pcmmr\_unattended.

Start the deployments and then start the managed servers.

### Start Apache and Mirth Connect Services

Start the Apache and Mirth Connect services on REDACTED:

dzdo service httpd start

dzdo service mcservice start

Verify the services are stopped:

dzdo service httpd status

dzdo service mcservice status

## Installation Verification Procedure

## System Configuration

System configuration changes are not applicable for this installation.

## Database Tuning

Database adjustments are not applicable for this installation.

# Back-Out

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

## Back-Out Procedures

### Database

SQL database changes are not applicable for this installation.

### Application EAR Files

Stop the Mirth Connect and Apache services.

Stop the WebLogic managed servers.

Delete the new pcmmr and pcmmr\_unattended deployments.

Remove the newly added startup arguments for all of the managed servers.

Replace the modified ciss.properties and pcmm.properties files with the copies made prior to the deployment.

Deploy the previous ear files.

Start the WebLogic managed servers.

Start the Apache and Mirth Connect services.

## Authority for Back-Out

Based on authority provided by the business sponsor and VA OIT IT program manager, PCMM can be backed out in accordance with their approval.

# Rollback Procedure

Rollback pertains to data associated with this PCMM interface.

## Rollback Considerations

It is necessary to determine if a wholesale rollback of the data associated with the PCMM interface is needed or if a better course of action would be correcting the data through a new version of the patch (if prior to a national release) or through a subsequent patch aimed at specific areas modified or affected by the original patch (after a national release). A wholesale rollback of the data associated with this patch still will require uninstalling Python and removing the cron jobs on the PCMM Web Services Server.

## Rollback Criteria

The decision to perform a wholesale rollback for this installation will be made by the business sponsor(s) and VA OIT IT program manager. Criteria will be determined based on separate and unique factors and evaluated upon post-installation use of the product.

## Rollback Risks

There are no risks identified to perform a wholesale rollback of Python and the cron jobs from the PCMM Web Services Server. There is no impact to the build or databases for this installation.

## Authority for Rollback

Based on authority provided by the business sponsor and VA OIT IT program manager, PCMM can be rolled back in accordance with their approval.

## Rollback Procedure

The rollback procedure steps are documented in Section 5.1 for the application and infrastructure. The back-out instructions are the same as those for the rollback of the application.

## Rollback Verification Procedure

Verify that all above data components have been removed from the system as described in the previous section.

# Risk and Mitigation Plan

The PCMM project team maintains a Program Risk Registry. Refer to this for all risks and mitigation plans for the PCMM project, including PCMM Web and VistA integration and the rest of the VA partner interfaces (Cerner Millennium, Cerner OpenLink, VA SFTP Site, and VA CDW).

1. Acronyms and Abbreviations

Table 7 – Acronyms and Abbreviations

| **Acronym / Abbreviation** | **Definition** |
| --- | --- |
| AWS | Amazon Web Services |
| COTS | Commercial off-the-Shelf |
| CDW | Corporate Data Warehouse |
| CISS | Clinical Information Support System |
| CPU | Central Processing Unit |
| DAS | Data Access Service |
| DB | Database |
| DDL | Data Definition Language |
| ETL | Extract - Transform – Load |
| ETS | Enterprise Testing Service |
| EHR | Electronic Health Record |
| EHRM | Electronic Health Record Modernization |
| GovCloud | Government Cloud |
| HIE | Health Information Exchange |
| HL7 | Health Level 7 |
| HIPAA | Health Insurance Portability and Accountability Act |
| IAM | Identity and Access Management |
| IOC | Initial Operating Capability |
| IT | Information Technology |
| PCMM | Patient Centered Management Module |
| PITC | Philadelphia Information Technology Center |
| OIT | Office of Information and Technology |
| OEHRM | Office of Electronic Health Record Modernization |
| QA | Quality Assurance |
| SaaS | Software as a Service |
| SACC | Standards & Conventions Committee |
| SFTP | SSH File Transfer Protocol |
| TRM | Technical Reference Model |
| UAT | User Acceptance Testing |
| VA | U.S. Department of Veterans Affairs |
| VAMC | Veterans Affairs Medical Center |
| VIP | Veteran-focused Integration Process |
| VISN | Veterans Integrated Service Network |
| VistA | Veterans Information Systems and Technology Architecture |
| VM | Virtual Machine |
| WASA | Web Application Security Assessment |