Pharmacy Product System – National (PPS-N)

Troubleshooting Guide

Version 1.1.02

August 2015

Department of Veterans Affairs
Office of Information and Technology (OIT)
Product Development

Revision History

Date	Version	Change Reference	Author
May 2015	1.1.02	Updated date and version number to 1.1.02.	Enterprise Application Maintenance
August 2014	1.1.01	Updated version number to 1.1.01. And made some formatting changes.	Enterprise Application Maintenance
November 2013	1.0.01	Updated version number to 1.0.01.	Enterprise Application Maintenance
January 2013	1.0	Clerical Modifications made based on NRR review comments.	SwRI
November 2012	1.0	Updated to include a section detailing the steps necessary when getting the test to production error.	SwRI
August 2012	1.0	Updated to include Lyn Teague's comments. Including updating footers, and an acronym list and rewording some sections to make them less ambiguous.	SwRI
July 2012	1.0	Updated for National Release	SwRI
June 2012	1.0	Addition of Browser Troubleshooting	SwRI
March 2012	1.0	Initial Draft	SwRI

(This page included for two-sided copying.)

Table of Contents

1 Introduction

1.1 Summary

The Pharmacy Product System (PPS) – National (PPS-N) Troubleshooting Guide is written to be a supplement to any Operations Manual that is provided for the support staff, whether it be Field Operations, HealtheVet Maintenance (after the product is in production), or the development team that needs to initially support the product.

1.2 Purpose

The purpose of this document is to list the error messages that any user may come across in the application. Some of the messages require that support staff be notified, and these are noted.

1.3 Scope

This scope of this document is limited to the PPS-N application. Any references to external systems is only for describing an interface and how the interface and that system affects the operation of PPS-N, or as a tool that may be used as part of system monitoring or the support and issue resolution system.

1.4 Acronyms

The following is a list of acronyms for this document.

Acronym	Definition
ANR	Automated Notification Reporting.
API	Application Programming Interface
CDCO	Corporate Data Center Operations
CRUD	Create Read Update Delete
DBA	Database Administrator
NDF-MS	National Drug File – Management System
EPL	Enterprise Product List
FDB	First Databank
FDB-MedKnowledge Framework	First Databank – MedKnowledge Framework

Acronym	Definition
FSS	Federal Supply Schedule
HSD&D	Health Systems Design and Development
ITC	Information Technology Center
JDBC	Java DataBase Connectivity
JDK	Java Development Kit
JSP	Java Server Pages
KAAJEE	Kernel Authorization and Authentication for Java Enterprise Edition
NDF	National Drug File
PPS-N	Pharmacy Product System - National
PRE	Pharmacy Re-Engineering
PREP	Pre-Production
SAN	Storage Area Network
SDS	Standard Data Service
SLA	Service Level Agreement
STK	Software Toolkit
STS	Standards and Terminology Service
VA	Veterans Affairs
VETS	Veterans Enterprise Terminology Service
VHA	Veterans Health Affairs
Vista	Veterans Health Information Systems and Technology Architecture

2 System Business and Operational Description

The PPS-N application allows national VA personnel to more easily, quickly and safely manage the VA National Formulary which directs which products (such as medications and supplies) are to be purchased and used by the VA hospital system. This in turn fulfils the overall Pharmacy Enterprise Product Systems objectives of facilitating the improvement of pharmacy operations and patient safety for the VHA.

The PPS-N application supports a platform-independent browser based interface that allows PPS-N users to keep the application's database (known as the Enterprise Product List or EPL) up to date. PPS-N performs the following major business functions:

- Add/edit/approve medication and supply information
- Manage the national formulary list
- Synchronize the Enterprise Product List (EPL) data with the legacy National Drug File – Management System (NDF-MS) data
- Create national drug reports
- Process First DataBank (FDB) additions and updates
- Search FDB for drug information.
- Interfaces with the Veterans Enterprise Terminology Service (VETS) system (for Standard Med Route information)
- Interfaces with the Federal Supply Schedule (FSS) system (for pricing data)

The Pharmacy Benefits Management group (PBM) is the primary business owner of the application. They are responsible for overseeing customized changes that are necessary for overriding data table updates supplied weekly by First Data Bank.

2.1 Operational Priority and Service Level

The Service Level of the system and the availability of the system are described in the Rough Order of Magnitude (ROM) it provides information to set up and support the PRE PPS-N application at ITC-Austin TX and NDF VistA environments at Albany NY. No formal SLA is available for the PPS-N application.

2.2 Logical System Description

The logical view describes the architecturally significant parts of the design model. The object oriented decomposition of the PPS-N application can be logically divided into three primary tiers: Presentation Tier, Business Logic Tier, and Data Persistence Tier. Each tier has its own design and implementation framework, and defined points of interaction with the other respective tiers.

2.2.1 Presentation Tier Overview

The presentation tier represents the GUI screens that allow the user to interact with the application, and the logic initiated by user interaction to execute screen functionality. Presentation Tier uses well known Model-View-Controller (MVC) design pattern implemented by the Spring MVC framework using Sun Microsystems JSP pages as the "View" portion of MVC. The MVC framework is used to manage the display screens and to dispatch and delegate requests initiated by the user to a business rule processing

business logic tier. The design of the MVC framework as it is used in the PPS-N application leverages an object hierarchy with commonly shared base classes.

2.2.2 Business Logic Tier Overview

The business logic tier is responsible for receiving business rule processing requests from the presentation tier, or other parts of the business logic tier. It is composed of services implemented as Spring beans. Transactional integrity is ensured by using Spring managed transactions.

The main services implemented deal with creation/modification/deletion of customization requests, workflow, queries and custom update generation.

The services encapsulate the business rules governing the creation/modification/deletion of customization requests and their workflow. The services are also responsible for interfacing and abstracting the data persistence tier from the rest of the application logic.

2.2.3 Data Persistence Tier Overview

The data persistence tier is designed and implemented with the open source Hibernate framework. The Hibernate framework is an object oriented abstraction for database CRUD operations (please see the Hibernate website for further information).

The data persistence tier interfaces with three logical Oracle databases. The first is the PPS-N database ("National EPL") containing the tables and database objects necessary for the PPS-N application to perform its various functions. The second is the FDB-DIF database, which is the source of various drug information utilized by PPS-N data migrations. The third is the FSS database, which is another data source utilized by PPS-N data migrations. The relevant tables in each of these databases have representative domain model objects and data access objects (DAOs) in the data persistence design. Additionally, PPS-N interacts with two other database systems, NDFMS (via a VistaLink API) and FSS (via a JDBC Connection).

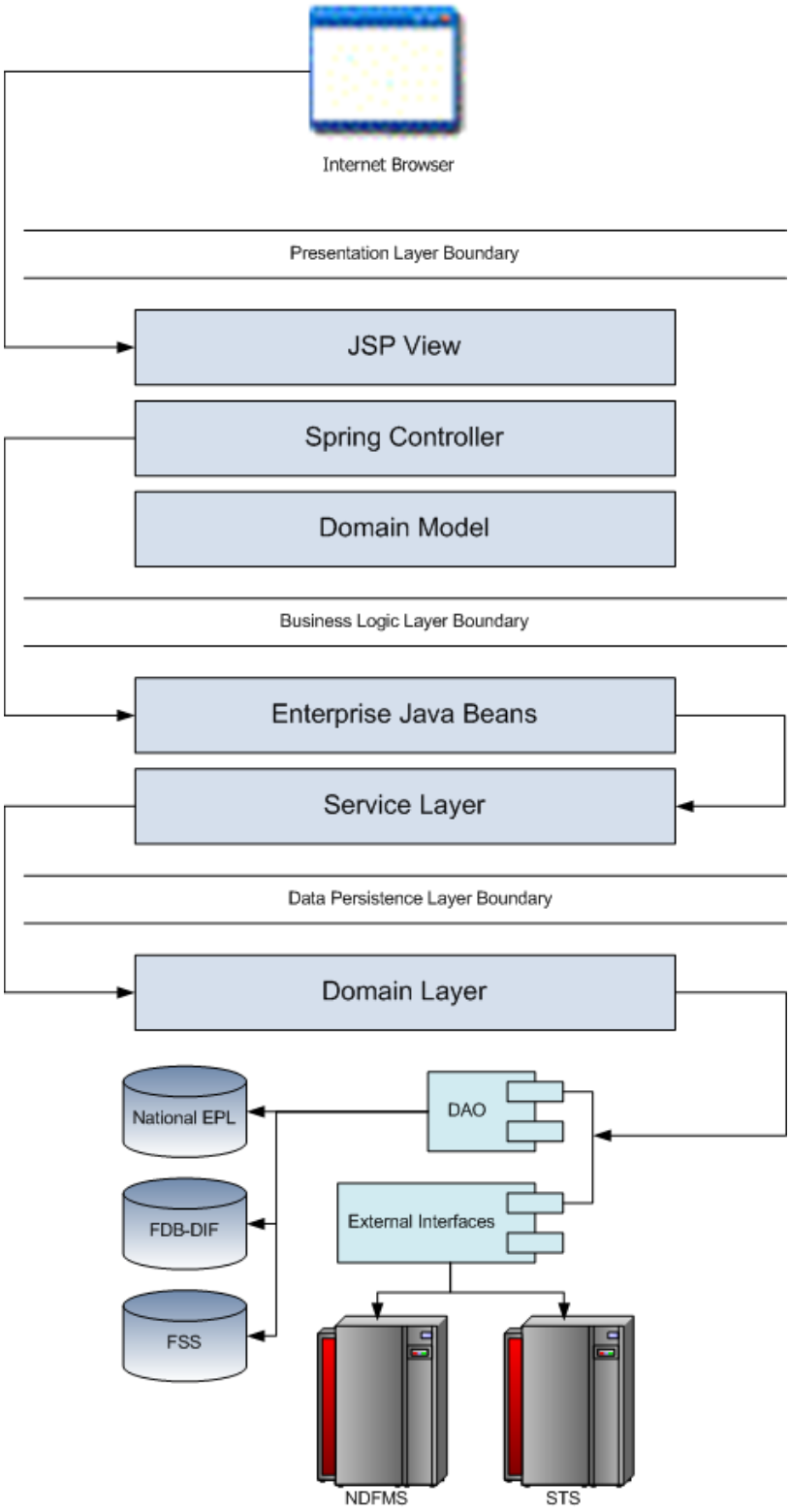

Figure 2-1. Logical System Overview

2.2.4 PPS-N Logical System Components

The logical system description defines the PPS-N system components. The Logical System components are defined in the PPS-N Software Design Document.

2.3 Physical System Description

PPS-N is a national deployment at the Austin Information Technology Center (AITC). There is no disaster recovery site at AITC. The PPS-N application's components are deployed on two servers: an application server (WebLogic) and a database server (Oracle). The characteristics of these servers are described in more detail below.

WebLogic application server:

Parameter	Value
Central Processing Unit	2 CPU, x86 architecture (Intel x86 or equivalent), 2 GHz or faster
RAM	8 GB
Available Hard Disk Space	70 GB
RAID Configuration	RAID 1
Operating System	Red Hat Linux – Enterprise Edition Version 5.0
Mouse	Generic
Video Resolution	640 x 480 pixels
Network Interface	dual Gigabit or higher
Software	BEA WebLogic 10.3

Oracle database server:

Parameter	Value
Central Processing Unit	4 CPU, i386 architecture (Intel 386 or equivalent), 2 GHz or faster
RAM	16 GB
Available Hard Disk Space	150 GB
RAID Configuration	RAID 1
Operating System	Red Hat Linux v 5.0
Mouse	Generic
Video Resolution	640 x 480 pixels
Network Interface	dual Gigabit or higher
Fiber Channel Interface	dual Host Bus Adapters
Database	Oracle 11g

PPS-N is deployed at the national level as a single application server node connected to a database server.

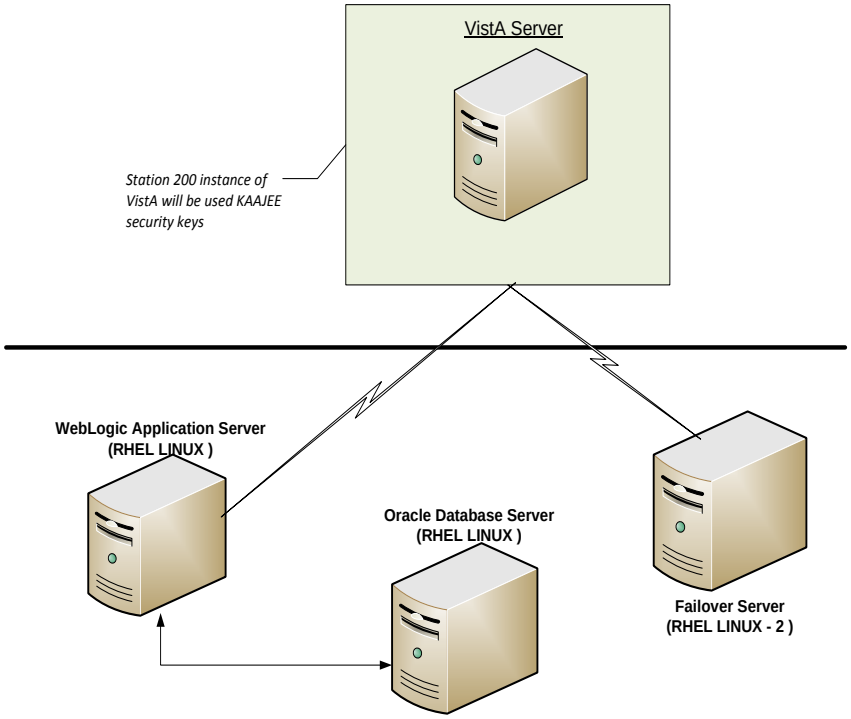

Figure 2-2. PPS-N Deployment

2.4 Software Description

The PPS-N application conforms to the requirements of the VA in determining the use of third party tools. Please refer to the Health*e*Vet-VistA Application Architecture Planning TRM Tools list for the approved VA programming APIs and libraries and the VA Web Operations Developer's Guide.

The three-tiered architecture consisting of an Internet browser based graphical user interface accessing a Spring-based web application/presentation tier, a J2EE based business logic service processing layer, and a Hibernate based data access tier conforms to the design recommended by the HSD&D Core Specifications for Rehosting Initiatives and generally acceptable J2EE implementation recommendations.

PPS-N is a J2EE application, conforming to version 1.4 of the specification. It is deployed on WebLogic v10.3 and uses JDK v1.6.0_16. It makes use of the following third party frameworks: Spring 3.0.5, Hibernate 3.6.1 and Log4j 1.2.15. The presentation tier also makes use of the JavaScript library Prototype 1.6.0. As mandated by the VA, PPS-N employs KAAJEE 1.1.0 for user authentication and authorization. KAAJEE, in turn, uses SDS 17.0 and VistALink 1.6.

The software components for the PPS-N are:

Component Name	Vendor	Version	License	Configuration
Operating System	Redhat			Standard
National Database	Oracle			See PPS-N Installation Guide.
Programming Language	Sun/Oracle	6	Sun Binary Code License	Standard
WebLogic	Oracle	10.3.2		See PPS-N Installation Guide.
Drug Information Framework	First Databank	3.1		See PPS-N Installation Guide

2.4.1 Background Processes

There are several background processes that run on the PPS-N production servers:

- At 7am each morning, a job runs to alert DBAs to service accounts with passwords that will expire in the next 15 days.
- Also at 7am, a job runs to purge trace files, log files older than a set parameter.
- At 5am, a daily job runs to move audit logs that need to be kept longer to a more permanent location.
- At 6am, a job runs to move old alert logs to a backup directory and start a new log for each day to make troubleshooting and maintenance easier and to free up space for customer data.
- Every night at 11pm, a job runs to gather statistics on each table which are used by the Oracle optimizer to choose data access paths for peak performance.
- A weekly job runs on Sunday to monitor space usage and allow database and system administrators to do capacity planning. A weekly job runs on Thursdays to verify/monitor privileges held by users for security and DBA review.

System Monitoring jobs that monitor the database and application servers are described in Section 3.4.

2.4.2 Job Schedules

A Quartz Scheduler schedules the nightly update processes that execute at a configured time once per day. Whether successful or unsuccessful, the process will execute again on the following day.

There are five scheduled jobs that are scheduled through the Quartz scheduler:

- FDB-DIF Add: Checks the FDB-DIF for any new packaged drugs that have been added since the last time the job ran.
- FDB-DIF Update: Checks the FDB-DFI for any updated drugs that have been updated since the last time the job ran.
- STS Update: Checks the VETS web service API to see if any changes have been made to the Standard Medication Routes since the last time the job ran.
- FSS Update: Checks the Federal Supply Schedule database to see if any pricing information has been updated since the last time the job ran.

- Proposed Inactivation Process: Checks to see if any drugs have reached their proposed inactivation date and processes any that have.

2.5 Dependent Systems

PPS-N depends on VistA for user authentication and authorization since the Application depends upon the use of KAAJEE which employs VistALink to authenticate users with VistA. In addition, it also needs an SDS instance to provide institution information. KAAJEE uses an Oracle database to temporarily store user information.

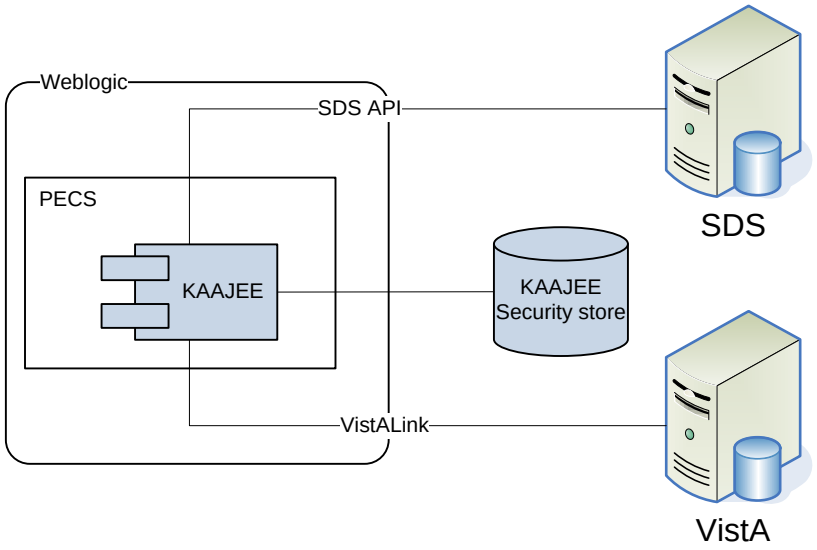

Figure 2-3. Dependent System

The system automation dependencies are:

Dependency Name	Location	Function	Interface Method
VistA	VA Internal	VistA access to PPS-N	WEB
KAAJEE		Security	

(This page included for two-sided copying.)

3 Routine Operations

The PPS-N requires Oracle support of the FDB DIF and Developer tables by a data base administrator. The understanding of Linux and WebLogic is also required.

3.1 Administrative Procedures

3.1.1 System Start-up

The servers are brought online by applying appropriate power and pressing the power button. Once the operating system is loaded and the server is accessible, the DBA is advised and will bring the database online. Once the database is online, the application admin is advised and will bring the application online.

If the server is up and the database is down, the script on the database server, vapredbs1, in the directory /u01/oracle/admin/PREP/scripts, is a startup script which can be run by the Oracle Unix user to start up any database on the server. It is called from that directory as ./startup_db.ksh <database_name>, i.e., ./startup_db.ksh PREP.

WebLogic as pre and post steps.

PRE Pre-Production	
WebLogic Install Directory	/u01/app/bea
Domain Directory	/u01/app /bea/user_projects/domains/ pps
Admin Server Startup Script	/u01/app /bea/user_projects/domains/pps-preprod/startWebLogic.sh
Node Manager Startup Script	/u01/app /bea/wlserver_10.3/server/bin/startNodeManager.sh
Managed Server Startup	From Admin Console: pps_ms1

PRE Production	
WebLogic Install Directory	/u01/app /bea
Domain Directory	/u01/app /bea/user_projects/domains/pps-prod
Admin Server Startup Script	/u01/app/bea/user_projects/domains/pecs-prod/startWebLogic.sh
Node Manager Startup Script	/u01/app /bea/wlserver_10.3/server/bin/startNodeManager.sh
Managed Server Startup	From Admin Console: pps_ms1

1. Login to server as your user and become the WebLogic user:

   i.e.***: sudo su - weblogic***

2. See the previous table to identify the script you wish to run for starting the Admin Server or a Node Manager. When running a script, preface all startup scripts with the ***nohup*** command and place in the background.

   i.e.: Starting the Admin Server
   cd /u01/app/bea/user_projects/domains/pps-*
   nohup ./startWebLogic.sh &

i.e.: Starting a Node Manager
cd /u01/app/bea/wlserver_10.3/server/bin
nohup ./startNodeManager.sh &

Login to the WebLogic GUI Admin console with your LAN ID. If this does not work, check the Password Vault for the environment and use the specified account. Start the requested Managed Servers.

3.1.2 System Shut-down

The application is first taken offline by the application admin and advises the team. The DBA takes the database offline and advises the team. The System Administrator will run "ps -ef" to identify any hung WebLogic or Oracle processes prior to shutdown/reboot of the servers.

If the server is up and the database is up but needs to come down for maintenance on the database or server, the script on the database server, vapredbs1, in the directory, /u01/oracle/admin/PREP/scripts, is a shutdown_ script which can be run by the Oracle Unix user to shut down any database on the server. It is called from that directory as ./shutdown_db.ksh <database_name>, i.e., ./shutdown_db.ksh PREP.

a. Login to the WebLogic GUI Admin console with your LAN ID. If this does not work, check the Password Vault for the environment and use the specified account.

   Select all the servers including Admin server and shut them down.

b. Login to server as your user and become the WebLogic user:

   i.e.: ***sudo su – weblogic***
   kill <nodemanager PID>

c. Verify if all the servers are stopped.

   i.e. ***ps –ef | grep java***, should not display any WebLogic instances.

3.1.3 Back-up & Restore

In this section, a high-level description of the systems back-up and restore strategy is elaborated.

3.1.3.1 Back-up Procedures

All servers are backed up under the AITC Enterprise Backup solution.

The PRE server backup policy is as follows:

- Differentials run Mon-Thurs – three-week retention.
- Full backup run on Fridays – three-month retention

```
host vapredbs1-b: vapredbs1-

================================================================================
Running Command: bpcoverage -c vapredbs1-b -coverage -no_cov_header


CLIENT: vapredbs1-b

  Mount Point        Device          Backed Up By Policy  Notes
  -----------        ------          -------------------  -----
  /             /dev/mapper/rootvg-root PRE_prd_sys
  /             /dev/mapper/rootvg-root *PRE_prd_ays
  /boot           /dev/sda1        PRE_prd_sys
  /boot           /dev/sda1        *PRE_prd_ays
```

```
  /dev/pts         devpts                        UNCOVERED
  /home           /dev/mapper/rootvg-home PRE_prd_sys
  /home           /dev/mapper/rootvg-home *PRE_prd_ays
  /opt           /dev/mapper/rootvg-opt  PRE_prd_sys
  /opt           /dev/mapper/rootvg-opt *PRE_prd_ays
  /proc/sys/fs/binfmt_misc none                          UNCOVERED
  /sys           sysfs                      UNCOVERED
  /u01           /dev/mapper/rootvg-u01  PRE_prd_sys
  /u01           /dev/mapper/rootvg-u01 *PRE_prd_ays
  /u02           /dev/mapper/VG01-u02              UNCOVERED
  /u03           /dev/mapper/VG01-u03              UNCOVERED
  /u04           /dev/mapper/VG01-u04              UNCOVERED
  /u05           /dev/mapper/VG01-u05              UNCOVERED
  /u06           /dev/mapper/VG01-u06              UNCOVERED
  /u07           /dev/mapper/VG01-u07              UNCOVERED
  /usr           /dev/mapper/rootvg-usr  PRE_prd_sys
  /usr           /dev/mapper/rootvg-usr *PRE_prd_ays
  /var           /dev/mapper/rootvg-var  PRE_prd_sys
  /var           /dev/mapper/rootvg-var *PRE_prd_ays

    Working on vapredbs1 now!

===============================================================================
Checking status of latest backup run:

-------------------------------------------------------------------------------
Backups from last 24 hours:

/net/work/bpjobs/bpjobs.linux.bsh: kill: (8134) - No such pid
STATUS CLIENT    POLICY      SCHED   SERVER   TIME COMPLETED
 0  vapredbs1-b  RMAN       PRE_1mo  vaaacbck7-b 07/11/2010 05:05:44

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Running Command: ping -s vapreapp1-b 56 3

----vapreapp1-b PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/2

===============================================================================
Running Command: bpclntcmd -hn vapreapp1-b

host vapreapp1-b: vapreapp1-b

===============================================================================
Running Command: bpcoverage -c vapreapp1-b -coverage -no_cov_header

CLIENT: vapreapp1-b

  Mount Point        Device          Backed Up By Policy  Notes
  -----------        ------          -------------------  -----
  /             /dev/mapper/rootvg-root PRE_prd_sys
  /             /dev/mapper/rootvg-root *PRE_prd_ays
  /boot           /dev/sda1         PRE_prd_sys
  /boot           /dev/sda1        *PRE_prd_ays
  /dev/pts         devpts                        UNCOVERED
  /home           /dev/mapper/rootvg-home PRE_prd_sys
  /home           /dev/mapper/rootvg-home *PRE_prd_ays
  /opt           /dev/mapper/rootvg-opt  PRE_prd_sys
  /opt           /dev/mapper/rootvg-opt *PRE_prd_ays
  /proc/sys/fs/binfmt_misc none                          UNCOVERED
  /sys           sysfs                      UNCOVERED
  /u01           /dev/mapper/rootvg-u01  PRE_prd_sys
  /u01           /dev/mapper/rootvg-u01 *PRE_prd_ays
  /usr           /dev/mapper/rootvg-usr  PRE_prd_sys
  /usr           /dev/mapper/rootvg-usr *PRE_prd_ays
  /var           /dev/mapper/rootvg-var  PRE_prd_sys
  /var           /dev/mapper/rootvg-var *PRE_prd_ays
```

The database server, vapredbs1, is backed up for a system backup each weekend to tape and the tapes are retained for a month.

Oracle Recovery Manager software is used to perform full backups of the PREP database each Tuesday and Saturday mornings. The tapes are retained offsite for 1 month. Recovery Manager is also used to backup archive logs and the database control file to tape daily, and are also retained offsite for a month. The full database backups run for about 40-45 minutes. The archive log backups are shorter, about 25-30 minutes.

3.1.3.2 Restore Procedures

Recover disk layout and OS version:

1. Refer to one of the following for a filesystem layout:
    a. cfg2html reports
    b. Filesystem report stored in /opt/ops/hosts.reports/<hostname>.fs.txt on vaaacmul11.aac.va.gov
    c. Restore /opt/ops/<hostname>.fs.txt to /tmp/ on vaaacmul11.aac.va.gov
2. Refer to one of the following to determine which RedHat version to install:
    a. cfg2html reports
    b. Cfg2html output stored in /opt/cfg2html on vaaacmul11.aac.va.gov
    c. RedHat release report stored in /opt/ops/hosts.reports/<hostname>.release.txt on vaaacmul11.aac.va.gov
    d. Restore /etc/redhat-release to /tmp/ on vaaacmul11.aac.va.gov

Build server using STK image server

a. STK image server

Install Netbackup client

a. NetBackup Client setup document

Rebuild user accounts:

1. Request the NetBackup administrator to restore following files:
    a. /home
    b. /etc/passwd
    c. /etc/shadow
    d. /etc/group
    e. /etc/gshadow
2. Run ***pwck*** to verify password files
3. Run ***grpck*** to verify group file

Restore customized configuration files and user directories:

1. Request the NetBackup administrator to restore following files/directories:
    - /etc/snmp/snmpd/conf
    - /etc/at.allow
    - /etc/at.deny
    - /etc/cron.allow
    - /etc/cron.deny
    - /etc/hosts
    - /etc/sudoers
    - /etc/security/limits.conf
    - /etc/yum.conf
    - /etc/aliases

- /etc/hosts.allow
- /etc/hosts.deny
- /etc/httpd
- /etc/sysctl.conf
- /etc/syslog.conf
- /opt/ops/acct
- /opt/ops/bin
- /etc/cron.daily/passwd_age
- /etc/cron.monthly/SecurityCheck
- /usr/local/bin
- /usr/local/nagios
- /etc/logrotate.d
- /etc/logrotate.conf
- /etc/ntp
- /etc/ntp.conf
- /etc/multipath.conf
- /u0x
- /var/spool/cron

2. Restart the following services:

    - snmpd
    - sendmail
    - httpd
    - syslog
    - nptd
    - multipathd

Install 3rd Party software

Once the server, vapredbs1 is restored from tape, including /etc, /var and /u01 with the Oracle software having been restored from tape, the database can be restored using Recovery Manager. The script to do this should have been restored to the /u01/oracle/admin/PREP/rman directory and is called rman_restore_db_from_tape.ksh. It must be run as the Oracle Unix user with the latest full backup of the database in the tape device and the database name as a parameter.

3.1.3.3 Back-up Testing

At the discretion of the Program Manager, random files can be selected to be restored to an alternate location.

Currently, there is no restore testing. The DBA team has requested an extra server to user for this purpose and will implement testing procedures when this server is purchased by AITC.

3.1.3.4 Storage and Rotation

Full Backups are performed on Sundays and kept for a month. This means that at any time, we should have 4 full backup tapes available for each server. Tapes are normally dispatched offsite on Mondays.

Differentials are run for the remainder of the week to capture daily changes and are sent offsite on Mondays.

These are the files that we backup on vapredbs1:

- /
- /boot
- /home
- /opt
- /usr
- /var
- /u01

Schedule:

- Diff Mon-Thurs 3 week retention
- Full Fri 3 months retention

3.2 Security / Identity Management

Security used is - KAAJEE.

KAAJEE document webpage: http://www4.va.gov/vdl/application.asp?appid=151

Document used from this page is the Installation Guide & Release Notes 1.0.1 (WebLogic 8.1)

The PPS-N application is only accessible by users signed directly into the VA network, or by users signed into the VA network via the RESCUE client. User authentication into the VA network is a precondition of PPS-N application access. Application authentication and authorization will be controlled by the VA KAAJEE security API.

In order to log into the application, each user must have a valid VistA account, at a local or national facility, since KAAJEE delegates user authentication to VistA. At the application's login screen, users will be prompted for their access and verify codes, and will be allowed to select the VistA instance which issued their credentials.

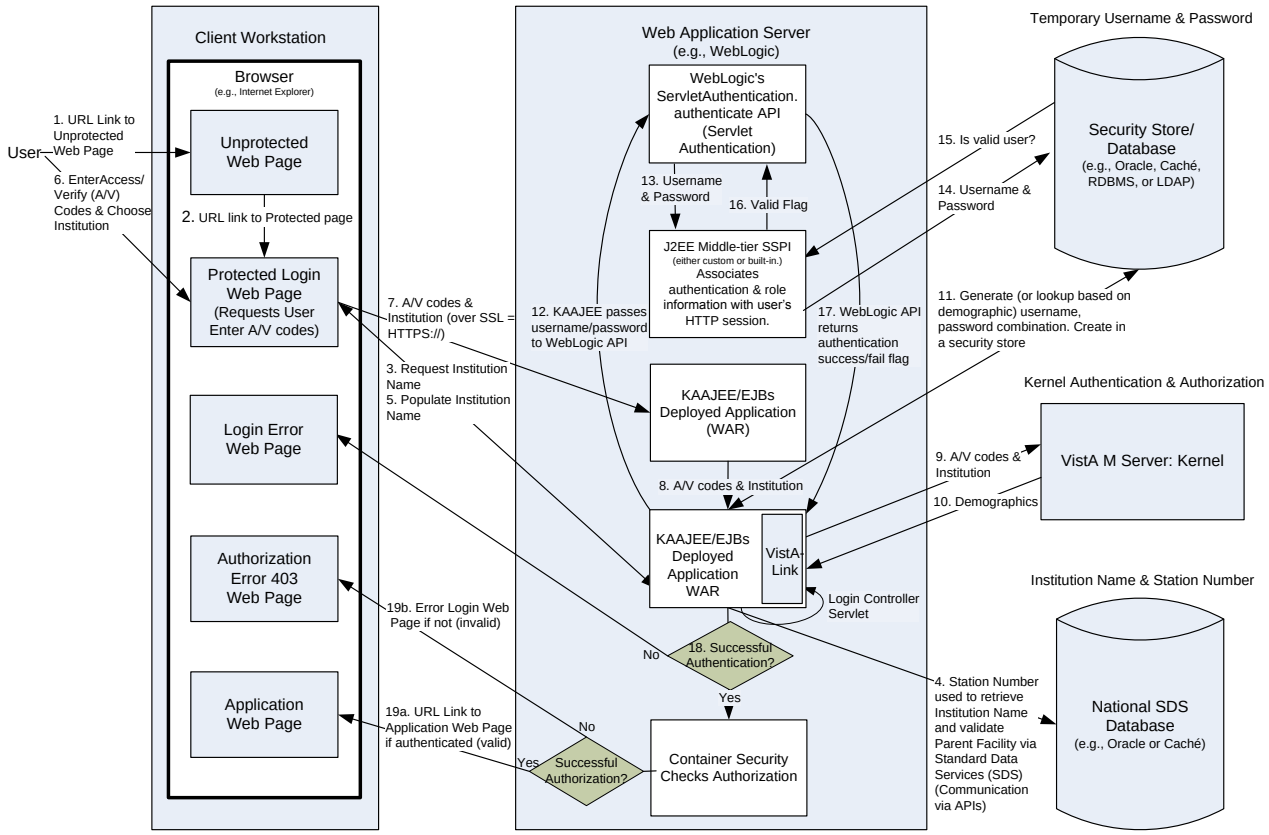

Figure 3-1. KAAJEE Application Overview

3.2.1 Identity Management

AITC utilizes VA Form 9957 for the creation, modification, and deletion of accounts. The request is approved by the Program Manager or his or designated representative. The 9957 request also identifies the servers and the level of access to be granted.

Users are verified for access to PPS-N by the current VA VistA system. New users must be created in VistA to have access to PPS-N and the PREP database using form 9957 which must be completed by a functional group manager and sent to security to review. Once it is reviewed and approved by security, it is sent to the AITC group who administers VistA to add the user. VistA administrators are in a separate group within AITC from the database and system administrators.

Security reviews of the application and database are performed after each upgrade and after quarterly security database patches are applied to verify access is limited to approve users. Any issues found at the application level, VistA level, or Database level must be remediated within a week to 30 days depending on the level of the issue.

Identity Management is done through VistALink. We will have one connection configured for each VistA site and the user management is done at each local VistA site.

Authorization is handled through the use of specific VistA security keys. Additionally, PPS-N does not assign individual permissions to users. Instead, it defines a number of roles for its users (requestor, approver, release manager, and administrator) and associates a set of permissions with each of them. However, new users' roles must be approved by an administrator. These roles are mapped to security keys as follows.

PPS-N Role	VistA Security Key
PPS National Viewer	PSS_PPSN_VIEWER
PPS National Second Approver	PSS_PPSN_SECOND_APPROVER
PPS National Manager	PSS_PPSN_MANAGER
PPS National Supervisor	PSS_PPSN_SUPERVISOR
PPS National Migrator	PPS_PPSN_MIGRATOR

Depending on the permissions needed by a user, the appropriate role is determined and the corresponding key assigned to their account. The user provisioning process is part of the VistA system and is thus not documented here. Password changes, account activation/inactivation etc. must be performed through VistA. Refer to the appropriate documentation for details on user account management.

3.2.2 Access Control

A password aging script is used to identify accounts for which passwords have not been changed with 90 days. Accounts are automatically locked if they are not changed at the end of the 90 day period. Accounts are removed after 180 days and a new VA Form 9957 will need to be submitted if the user still requires access. Passwords cannot be changed within the first 7 days.

Passwords must meet the VA security policy including being at least 8 characters long with alpha, numeric, special characters, and mixed case, and must be changed every 90 days. User IDs are only granted to VA employees who have already been granted VA Network IDs.

WebLogic console admin username and passwords are saved in the Password Vault and it is accessible only by WebLogic admin group.

Temporary or read only access can be provided to development or operational teams through the WebLogic security realms if required.

The purpose of this screen is to provide an authorized user access to the system. The user must enter their valid, assigned/designated Access Code and Verify Code using this screen. The Access Codes and Verify Codes are stored in, and validated against the VistA Link system via the KAAJEE interface. The system will validate or authenticate the data entered by the user and, if it is valid, allow the user access to the PPS-N application. The maintenance of the user account and password information is part of the VistA system and is thus not documented here. Refer to VistA documentation for details on the user account maintenance.

If the response from the authentication request is successful via the KAAJEE API, KAAJEE will return a user profile object which will be used by the application to determine the user's role(s) and permissions. On successful login, the system transfers (navigates) the user to the Home page of the application.

It should be noted that the authentication mechanism used by the KAAJEE API is “Form” based authentication. This type of authentication is configured in and enforced by the application server. A login form page is specified within the application configuration deployment descriptor which tells the application server what page within the application is to be used for authentication. When a request for login is received by the application server, the server knows to display this form. If a user session times out and the user subsequently requests an application link or resource, the application server will forward requests to the page specified as the login form first.

Within the PPS-N application, if the user session times out the application server will forward the user to the login page. Once logged in, the user will be redirected to the application home page.

A user's role will determine the screens and operations that will be accessible. The following table lists a set of permissions that each of the roles will be able to accomplish.

X – indicates edit capabilities

R – indicates read only capabilities

Blank indicates the user does not have this privilege. This will be implemented either as grayed out buttons/links on the page or by elements not being visible on the page. This decision on whether to gray out the item or make in non-visible will be a usability decision.

Permission	Viewer	2nd Approver	Manager	Supervisor	Migrator
View Migration Tab					X
All Migration Permissions					X
View Home Page	R	R	R	X	R
Manage PPS Tab					
Simple Search	X	X	X	X	X
Advanced Search	X	X	X	X	X
Create System Templates				X	
Delete other user's search templates				X	
Manage personal Search template	X	X	X	X	X
Edit Item – Submit Change Request	X	X	X	X	X
Edit Item – Submit Change			X	X	
Add Item			X	X	
Requests	X	X	X	X	X
Approve Requests Marked for PPS Second Approver		X	X	X	
Approve Requests not marked for PPS Second Approver			X	X	
Saved Work In Progress	R	X	X	X	R
Delete other user's saved				X	

works in progress					
PPS Data Elements	X	X	X	X	X
Edit Domain Item			X	X	
Add Domain Item			X	X	
PPS Data Requests	X	X	X	X	X
Reports	X	X	X	X	X
COTS Services					
PMI	X	X	X	X	X
FDB Search	X	X	X	X	X
Manage COTS VA Mappings	R	R	X	X	R
Add Item from FDB Search			X	X	
New FDB Items Tab	R	R	X	X	R
Modified FDB Items Tab	R	R	X	X	R
Manage Application					
System Information	X	X	X	X	X
Manager External Systems (FSS and STS, Override VistA Synch	R	R	X	X	R
User Preferences	X	X	X	X	X
Migration					X

3.3 User Notifications

User standard CDCO procedures for ANR, etc.

Notification Steps	
Step 1	Send out email to:

AITC Personnel	PRE Personnel
Robert Thomas-Cano	Pavani Mukthipudi
Mary Esther Veloria	Anitha Alluri

<table>
<tr><td></td><td>a. Subject: Per CO or ANR xxxxx AITC will bring down <ENV> to perform maintenance at hh:mm AM/PM CST
b. Email line1: Per CO or ANR xxxxx AITC will bring down <ENV> to perform scheduled maintenance at hh:mm AM/PM CST
c. Email line2: AITC will send out notice once the <ENV> is back online and ready for smoke test.</td></tr>
<tr><td>Step 2</td><td>Login to the WebLogic GUI Admin console with your LAN ID, if this does not work, check the Password Vault for the environment and use the specified account.

Shutdown the requested Managed Servers or Clusters as listed in the Change Order or Service Request.</td></tr>
<tr><td>Step 3</td><td>Verify maintenance/deployment completed

Start the requested Managed Servers or Clusters as listed in the Change Order or Service Request.</td></tr>
<tr><td>Step 4</td><td>Send out email to:

<table><tr><th>AITC Personnel</th><th>OED Personnel</th></tr><tr><td>Robert Thomas-Cano</td><td>Pavani Mukthipudi</td></tr><tr><td>Mary Esther Veloria</td><td>Anitha Alluri</td></tr></table>a. Subject: Per CO or ANR xxxxx AITC has successfully completed <ENV> maintenance at {time} CST

b. Email line1: Per CO or ANR xxxxx AITC has successfully completed <ENV> maintenance at {time} CST
c. Email line2: <ENV> is back online and ready for smoke test.
d. Email line3: Please update this thread with test results and any outstanding issues.</td></tr>
</table>

System downtime due to application or system software upgrades will be planned with AITC. Users will be notified by PRE using the appropriate mailing lists. The notice will be provided at least two hours in advance. Notification will also be provided when the application becomes available again.

3.4 System Monitoring, Reporting, & Tools

Oracle Enterprise Manager and Grid Control are used to monitor availability and performance of the PPS-N database on the vaausppsdbs1 server. Standard AITC thresholds are set for space monitoring, availability of the database, and network connectivity. Database administrators are alerted immediately if the monitoring tool detects a problem. In addition, if connectivity to the database fails, an incident ticket is created in the User Service Desk software and relayed to AITC management and the primary and secondary database administrator for the project.

System monitoring is done through the following:

1. WebLogic console
2. VistA link console
3. Introscope
4. CEM
5. Xpolog

3.4.1 Availability Monitoring

1. WebLogic console (URL: http://<machine>:7001/console) has the entire WebLogic environment configuration.
   a. We can monitor the admin server, node manager and managed servers running states, and control managed servers start and stop activity.
   b. Manager servers health and performance, application deployment state, database connection pools, and JMS can also be monitored from here.
2. VistALink console (URL: http://<machine>:7001/vlconsole/welcome/login.jsp) has the VistA sites connection information.
   It gives the ability to add, edit, update, and check the status of each connection configured.
3. Introscope: Monitoring tool. One agent per machine is deployed and it can provide in detail monitoring of all the WebLogic components from that environment. And monitoring alerts and notifications can be generated using this tool.

3.4.2 Performance/Capacity Monitoring

Patrol is utilized by AITC to capture Performance and Capacity activities.

It can monitor the http traffic coming from internet cloud to AITC.

3.5 Routine Updates, Extracts and Purges

Each night data is exported from the PREP production database, and imported into the pre-production database, and to the Software Quality Assurance and Pharmacy Benefits Management database so testers can work with updated data.

3.6 Scheduled Maintenance

Currently, there is no scheduled maintenance window for PRE. This will be needed in the future so AITC has a window to do server patching, etc.

Any normal changes that are initiated by the PRE team will come in a Request for Change form to the AITC Build Manager. These requests will be submitted by 12:00pm CST on Friday for a Monday implementation in the Pre-Production environment. Production requests must be received by 12:00pm on Tuesday for implementation on Wednesday. Emergency change requests will be implemented as soon as possible.

3.7 Capacity Planning

3.7.1 Initial Capacity Plan

The initial Capacity Planning for Storage was done by PRE and EIE team as per the Application requirement. Subsequently, it was decided in concurrence with AITC Architect to add Host Bus Adaptor cards to the Servers, so as PRE Servers have access to SAN Storage. The SAN storage will be used to expand the storage capacity for future use as needed.

4 Browser Issues and Settings

This section presents a possible list if issues that may be attributed to browser settings or other configuration values that must be addressed by the end user.

4.1 IE9 Developer Tools Settings

Internet Explorer 9 (IE9) allows users to modify the browsers settings, which in turn affects the browser's interaction with the PPSN application.

A user may view and change the browser settings via the Developer Tools interface that [typically] comes with IE9.

The Developer Tools interface may be accessed from within IE by following either of the following steps:

- Press the **F12** key on the keyboard
- Go to the **Tools** menu, towards the bottom of the menu is **F12 Developer Tools**, click on this

The Developer Tools interface will either appear within the browser window, typically in the bottom portion of the window; or as a separate window. Please note that if it shows up as the former, it may look like a menu bar appears at the bottom of the window. This menu bar provides access to the browser settings.

4.1.1 Required Settings

- Internet Explorer 9 allows the user to change its `Browser Mode`. **Ensure that this value is: `IE9`**.
- Document Mode is usually set by the page loaded. Unfortunately, the end user may override this, and this can cause "buggy" behavior. **Ensure that this value is `IE9 standards`**.

4.1.2 Troubleshooting Some Typical Problems

This section details some typical problems that may be encountered due to the browser and must be addressed by the end user.

4.1.2.1 User Search Preferences

The `Search Preferences` page under the `User Preferences` menu has been observed to act "buggy" if the settings in section 4.1.1 are not adhered to.

Behavior: The saving of the selected fields or movement of a field for a search template does not perform in the expected manner.

Fix:

1. Ensure the required settings in section 4.1.1 are adhered to.
2. On the Developer Tools menu, click on `Cache` menu, click `Clear browser cache…`
3. Navigate to any other page within PPSN.
4. Navigate back to the `Search Preferences` page.
5. Repeat the modification(s) to the search template that was attempted earlier.

(This page included for two-sided copying.)

5 Exception Handling

This section presents a list of possible exceptions/errors that may occur during normal operation.

5.1 Routine Errors

The system validates form field values per business rule and data integrity constraints before the form is submitted for processing. If values do not pass user interface validation, the user is redirected back to the wizard form and a message is displayed informing the user of the corrections needed. Please see Alternative Flows in the Software Design Document for data validation errors.

The system receives the value after form validation, and applies the appropriate business rules (if any) to the value. Examples of a business rule validation may include bounds checking, or any interdependencies that may exist between two data values. Please see Alternative Flows in the Software Design Document for data validation errors.

Like most systems, PPS-N may generate a small set of error 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. While the occasional occurrence of these errors may be routine, getting a large number of an individual errors 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.

5.1.1 Security

Security is addressed at design tiers respective of the security requirement. Security authentication and authorization is provided by the KAAJEE security API, and is abstracted by the services layer of the application.

The PPS-N subsystem does not provide or enforce a security model. However, the system does access other system interfaces which may encounter security violations when accessed. The following known security errors may occur:

1. **Access to STS denied**: The configured STS web logic account is unreachable. This could be because the web server changed hosts or ports.
2. **Access to FSS denied**: The configured FSS JDBC connection is refused. This is most likely the result of a password expiring. The JDBC connection may need to be updated.
3. **Access to FDB-DIF denied**: The configured FDB-DIF JDBC connection is refused. This is most likely the result of a password expiring. The JDBC connection may need to be updated.
4. **Access to "temporary" directory denied**: The WebLogic process does not have sufficient permission to write to the operating system defined temporary directory (e.g., "/tmp"). To resolve this, the WebLogic process should be granted write access to the temporary directory.

5.1.2 Time-outs

Time out may occur when accessing third party Database. Sometimes queries are dependent upon the availability of the database or run out of time if a large results query is requested.

The following process has a known potential timeout in the PPS subsystem:

Hibernate query: A hibernate query will wait for the amount of time configured in the JDBC connection. A large number of timeouts may indicate insufficient system resources or the timeout value may be set to low.

5.1.3 Concurrency

No information at this time.

5.2 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.

5.2.1 Application Error Logs

PPS-N uses the Apache Log4j framework for logging. Log files are accessible to authorized users through the web-based Xpolog tool.

Logs location - /u01/app/bea/user_projetcs/domains/pecs-<Env>/ VistALink_Folder/logs/

Maxfilesize=10000KB

Max. backed up files are 10.

Growth rate is capped at 100MB

5.2.2 VistALink Error

Error Creating User

If a PPS-N user is logging onto the system and gets the following error: "**Error processing login credentials: Error creating user in the KaajeeManageableAuthenticator database"** it is most likely because the connection between the PPS-N web logic server and the SDS server has lost connectivity. This connectivity is not automatically re-established by the VistALink software so the web logic server may need to be restarted to re-establish the connection.

Test Production Mismatch

If a PPS-N user is logging onto the system and gets the following error: "**Error processing login credentials: Could not get a connection from connector pool for institution '521'.; Root cause exception: gov.va.med.vistalink.adapter.cci.VistaLinkResourceException: Can not perform setup; Root cause exception: gov.va.med.vistalink.security.m.SecurityProductionMismatchException: Fault Code: 'Server'; Fault String: 'Production-Test Mismatch'; Fault Actor: ''; Code: '183007'; Type: ''; Message: 'A production/test mismatch was detected between the client (true) and the server (false).'"** it is most likely because the NDF server has been reset to a 'TEST' server. A NDF manger will need to run the command D ASK^XUPROD and answer the questions asked as shown below:

```
USRISCSVR:NDF>D ASK^XUPROD

This is currently a TEST account.

Only answer YES if this is the full time Production Account.
```

```
Answer No for all other accounts.
Is this a Production Account? No// YES
Are you sure you want to change from a TEST account
to a PRODUCTION account? No// YES
This is now a PRODUCTION account.
USRISCSVR:NDF>
I SET IT TO PRODUCTION
```

(This page included for two-sided copying.)

6 Application Error Messages

While navigating through the PPS-N system, the user may encounter two types of errors; System Errors and Validation Errors. System Errors are unplanned errors which are unexpected in normal system operation, and Validation Errors are both expected and commonly occurring in normal system operation.

6.1 Error Messages

This section describes the different kinds of errors a user could encounter while navigating through the PPS-N system in greater detail.

6.1.1 Validation Errors

The most common error the user should encounter is a Validation Error. The user will encounter a Validation Error if she enters a value into an input on a webpage which is not expected by the system. In this case, the system has tried to execute an action, and that action has thrown an expected error based on the users malformed input. This error is thrown and handled at the Service Layer, passed back up to the Presentation Layer and then displayed to the user on the webpage where they entered the malformed input. The error message is displayed is user readable and highlighted on the page to inform the user she needs to correct her input before the operation she was trying to perform can proceed.

The following example describes how a user would encounter a Validation Error. The user is updating her user preferences and is changing the default number of rows displayed in results tables. This input is expecting integers from 10-100. She accidently enters 11a in the input and submits the form. As the system is expecting an integer, it does not update her preferences but instead returns with an error informing her input must only contain whole numbers and numeric digits.

6.1.2 System Errors

System Errors are unplanned errors which occur during system operation. These unplanned errors include Java errors (e.g. null pointer exceptions), database exceptions (e.g. connection errors), and any other error unexpected error the system might encounter. When an unexpected error occurs the system will display the following message to the user, “A System Error has occurred and has been logged. Please contact the system administrator.” The system will store the error containing all of the stack trace information in a log on the server, so the administrator may investigate what caused the error.

(This page included for two-sided copying.)

7 Infrastructure Errors

VHA IT systems rely on various infrastructure components. These components will have been defined in the Logical and Physical Descriptions section of this document. Most, if not all of these infrastructure components generate their own set of errors. Each Component has its own sub-section and describes how errors are reported. The sub-sections are typical list of components and are meant to be modified for each individual system.

The sub sections are not meant to replicate existing documentation on the infrastructure component. If documentation is available online then a link to the documentation is appropriate. Each sub-section should contain implementation specific details such and Database names, server names, paths to log files, etc.

PRE Team will work with AITC resources to resolve the Infrastructure errors. AITC will be responsible for System, Network, Database and PRE will provide the support as SME and on PPS-N application.

7.1 Database

Oracle monitoring tools monitor several aspects of the PPS-N databases and alert database administrators via email and create service desk tickets for conditions such as “disk full errors or tablespace full”, archive log directory full, database down, connectivity to database down, etc.

In addition, as with all Oracle databases, errors within the database are recorded in the Oracle alert log for the database and trace files are created that will allow DBAs to review any errors. Any such errors are emailed to the database administrators daily.

7.2 Web Server

At this Time the PPS-N application does not implement a Web server front end, or the WebLogic/Apache Plug-in is not being utilized officially. Apache writes output to Logs Located on the Linux web server, to the directory /var/log/httpd/, unless changed in the httpd.conf configuration file. Access to these usually requires Super User or Root access.

7.3 Application Server

The PPS-N application and WebLogic log in conjunction assist in the Troubleshooting of the App or the WebLogic portal. PPS-N Logs are located in the

> ${DOMAIN_HOME}/PPS-NLogs directory, consisting of the Following Files: ct_prod.log, hibernate.log, server.log, spring.log, and struts.log.

Assistance from PPS-N Java Developers may be required to parse the Logs files to determine any issues.

The WebLogic application server logs reside in the

> ${DOMAIN_HOME}/servers/${Each_Managed_Server_name}/logs/.

There are 2 primary log files to review:

- ${Each_Managed_Server_name}.log
- ${Each_Managed_Server_name}.out.

The WebLogic administrator should be able to parse these files. Assistance from PPS-N Java Developers may be required if out to the scope of the WebLogic Administration skill set.

7.4 Network

Using Orion, a Solar Winds monitoring tool, AITC Service Desk and/or network engineers monitor the layer 2 and layer 3 network switches. If an alarm is generated by Orion, AITC Service Desk will create a service ticket, and then attempt to triage the problem. AITC Service Desk, which operates 24x7, will notify the appropriate personnel. Appropriate personnel will triage the issue and work on the resolution of the issue.

7.5 Authentication and Authorization

Authentication and authorization errors can be reported if KAAJEE encounters errors. The most common causes would be problems with the KAAJEE user store connection or the dependent systems: SDS or one of the VistA instances. In either case, appropriate errors will be logged, indicating the cause.

7.6 Dependent System(s)

The dependent systems are those used for authentication and authorization. See Section 2.5, Dependent Systems, for a discussion of errors.

8 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.

PPS-N is designated as Routine Support for disaster recovery. This level of support will acquire replacement processing capacity after an AITC disaster declaration. The recovery time objective (RTO) is that it will be operational when the AITC resumes regular processing services or no later than 30 days after a disaster declaration. Data will be restored from the last backup (recovery point objective (RPO)).

System backups of the vapredbs1 server are performed on the following basis:

- Full backups are performed on Sundays and kept for one month. This means that at any time, there should be four full backup tapes available for each server.
- Tapes are normally dispatched offsite on Mondays.
- Differentials are run for the remainder of the week to capture daily changes.
- Differential results are sent offsite on Mondays.
- Oracle Recovery Manager is the application used to perform full backups of the PREP database every Tuesday and Saturday morning. The tapes are retained offsite for one month. Recovery Manager is also used to back up archive logs and the control file database to tape daily and these are also retained offsite for a month. The full database backups run for about 40-45 minutes. The archive log backups are shorter, which run about 25-30 minutes.

This section provides procedures for recovering the application at the alternate site, while Section 5.0 describes other efforts that are directed to repair damage to the original system and capabilities. Backup procedures are also defined in this section.

Procedures are outlined for each team required to complete the recovery. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

The Team Leader or designee will provide hourly recovery status updates to the Austin Service Desk (ASD).

8.1 Restart after Non-Scheduled System Interruption

This section's instructions are identical to those found in Section 3.1, Administrative Procedures.

Software is recovered from images stored on the SAN. The same recovery procedures listed in ACP 4.1 should be followed for a return to original site restoration. An alternate site would need comparable equipment installed and would need to be able to boot from SAN for successful execution of this plan.

(This page included for two-sided copying.)