

PAX Portfolio Manager Installation Guide

V 1.53.00



**PPM Installation Guide**

**Version: V1.53.00\_20201015**

**Document No: PPM-Installation-Guide**

**Status: ［］Draft ［★］Release ［ ］Modify**

**Copyright © 2009-2020 PAX Technology, Inc. All rights reserved**

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or de-compilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purposes.

**Security Notice: No part of this publication may be copied, distributed, stored in a retrieval system, translated into any human or computer language, transmitted, in any form or by any means, without the prior written consent of PAX Technology, Inc.**

PAX is a registered trademark of PAX Technology and/or its affiliates. Other names may be trademarks of their respective owners.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Comment | Author |
| 2019/3/28 | V1.03.00 | Release | Elliott Zhang |
| 2020/5/28 | V1.52.00 | Release | Ada Jiang / Liming |
| 2020/10/12 | V1.53.00 | Section 4.5.3 added security configuration for penetration testing | Ada Jiang |

Content

[1 Summary 1](#_Toc4705343)

[1.1 Purpose 1](#_Toc4705344)

[1.2 Audience 1](#_Toc4705345)

[1.3 Terms 1](#_Toc4705346)

[1.4 Conventions 2](#_Toc4705347)

[2 Environment 3](#_Toc4705348)

[2.1 Hardware 3](#_Toc4705349)

[2.2 Software 3](#_Toc4705350)

[2.2.1 Software Requirements 3](#_Toc4705351)

[2.2.2 PPM Software Components List 4](#_Toc4705352)

[3 Preinstallation Tasks 5](#_Toc4705353)

[3.1 Logging in to the Server as root 5](#_Toc4705354)

[3.2 Create a dedicated email account 6](#_Toc4705355)

[3.3 Subscribe Amazon SNS (OPTIONAL) 7](#_Toc4705356)

[4 Installation 7](#_Toc4705357)

[4.1 Get Installation Packages 7](#_Toc4705358)

[4.2 Configure Hosts 8](#_Toc4705359)

[4.3 Configure Firewall 8](#_Toc4705360)

[4.4 Install 9](#_Toc4705361)

[4.4.1 Install DB 9](#_Toc4705362)

[4.4.1 Install PPM Bundle (Master) 10](#_Toc4705363)

[4.5 Configure 11](#_Toc4705364)

[4.5.1 PPM Config File - tms.properties 11](#_Toc4705365)

[4.5.1 FastDFS Connection - fastdfs.yml 17](#_Toc4705366)

[4.6 Start & Stop PPM 17](#_Toc4705367)

[5 Install PPM Cluster (Redundant) – Optional 18](#_Toc4705368)

[5.1 Introduction 18](#_Toc4705369)

[5.2 Install Master 19](#_Toc4705370)

[5.3 Install Slave 19](#_Toc4705371)

[5.4 Configure Cluster 20](#_Toc4705372)

[5.4.1 PPM Config File - tms.properties 20](#_Toc4705373)

[5.4.2 FastDFS Connection - fastdfs.yml 21](#_Toc4705374)

[5.4.3 FastDFS Storage - storage.conf 22](#_Toc4705375)

[5.4.4 Nginx Proxy - nginx.conf 23](#_Toc4705376)

[5.5 Start & Stop PPM Cluster 24](#_Toc4705377)

[6 Configuration Table 25](#_Toc4705378)

[References 25](#_Toc4705379)

[Appendix 1 26](#_Toc4705380)

[FAQ 26](#_Toc4705381)

# Summary

## Purpose

The document guides how to install PAX Portfolio Manager.

## Audience

The document suits for installer, operator of PAX Portfolio Manager.

## Terms

Table 1 Terms

|  |  |
| --- | --- |
| Terms | Explanation |
| PPM | PAX Portfolio Manager |
| POS | Point of Sale |
| TERMINAL SN | Machine Serial Number of terminal device |

## Conventions

|  |  |
| --- | --- |
|  | 【Used for marking prompt information 】 |

|  |  |
| --- | --- |
|  | 【Used for reminding the audience to pay attention to some information which may lead to exception or mistake 】 |

|  |  |
| --- | --- |
|  | 【Used for warning the audience to be careful about some information which may lead to serious error or damage 】 |

# Environment

## Hardware

|  |  |
| --- | --- |
| PPM　SERVER | DB SERVER |
| Processor: Intel(R) Xeon(R) CPU E5-2603 v3 (2GHz, 6 core) or above  Memory: DDR4 16G or above  Hard Disk: 500GB or above | Processor: Intel(R) Xeon(R) CPU E5-2603 v3 (2GHz, 6 core) or above  Memory: DDR4 16G or above  Hard Disk: 1TB or above |

## Software

### Software Requirements

|  |  |
| --- | --- |
| PPM　SERVER | WEB Browser |
| RedHat (CentOS) Linux 7.5 or above 64bit operating system  openssl 1.02 or above  Python2.7 or above | <Suggest to update your browser to the latest version>  IE 10.0 or above  Safari 6.0 or above  FireFox 53 or above  Chrome 57 or above |

### PPM Software Components List

|  |  |
| --- | --- |
| SOFTWARE | VERSION |
| Tomcat | 8.5.11 |
| JDK | 1.8 |
| MySQL | Community Server 5.7   * Only InnoDB storage engine is supported * Must be configured to use UTF8 charset |
| Oracle | 11g   * Must be configured to use a UTF8-family charset (see NLS\_CHARACTERSET) * Increase max connections to 1000 |
| FastDFS | 5.08 |
| Redis | 3.2.8 |
| Nginx | nginx/1.10.1 |

# Preinstallation Tasks

## Logging in to the Server as root

To log in to the **PPM/DB Server** as **root**, complete the following procedures.

|  |  |
| --- | --- |
| Item | Description |
| Operation System Requirements | Make sure that version of Linux is RHEL7 or above, enter the following command:  # cat /etc/redhat-release  # cat /proc/version |
| System Architecture | To check system architecture, enter the following command:  # uname -m  Verify that the processor architecture matches the PPM installation package that you want to install. |
| Memory Requirements | 16G RAM or above (recommended)  To check the RAM size, enter the following command:  # cat /proc/meminfo |
| Disk Space Requirements | DB server: 1TB or above (recommended)  PPM server: 500G or above (recommended)  To check the amount of free disk space available, enter the following command:  # df -h |
| CPU Requirements | Intel(R) Xeon(R) CPU E5-2603 v3 or above (recommended)  Enter the following command to display the CPU information:  # cat /proc/cpuinfo |
| Network Port Requirements | PPM need to use several tcp ports. To determine those tcp ports are not being used, enter the following command:   |  |  | | --- | --- | | Component | Port | | MySQL | # netstat -anp | grep 3306 | | FDFS Tracker Server | # netstat -anp | grep 22122 | | FDFS Storage Server | # netstat -anp | grep 23000 | | Redis Server | # netstat -anp | grep 6379 | | Redis Sentinel: | # netstat -anp | grep 26379 | | Tomcat Server | # netstat -anp | grep 8080 | | PXRetailer Message Server | # netstat -anp | grep 8089 | | Nginx Proxy for Tomcat Server | # netstat -anp | grep 10443 | | Nginx Proxy for PXRetailer Message Server | # netstat -anp | grep 10080 | |

## Create a dedicated email account

PPM needs an email account with SMTP access to be used solely for outgoing alert messages and password reset messages.

## Subscribe Amazon SNS (OPTIONAL)

Amazon Simple Notification Service (SNS) are required for outgoing SMS messages to work.

To use the AWS SNS, you will need an AWS account and AWS credentials.

To create a new AWS account, see [Sign Up for AWS and Create an IAM User](http://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/signup-create-iam-user.html).

# Installation

## Get Installation Packages

Get the right PPM installation packages.

|  |  |
| --- | --- |
| Package Type | Description |
| PPM\_Installation\_Package\_[version]\_linux64.tar.gz | PPM installation package. |
| PPM\_SQL\_Script\_[version].zip | PPM SQL script package |

## Configure Hosts

The host and IP will be specified during install process.

## Configure Firewall

|  |  |
| --- | --- |
|  | When attaching server to a publicly accessible interface, ensure that you have implemented proper authentication and firewall restrictions to protect the server. |

Login PPM/DB server machine as root, configure firewall to allow internal access between components.

|  |  |
| --- | --- |
| Configure Firewall | |
| MySQL Server | Configure firewall to allow MySQL Server access:  $ firewall-cmd --permanent --add-port=3306/tcp  $ firewall-cmd --reload |
| Oracle | If you are using oracle database, please make sure PPM Server can access the oracle instance remotely. |
| FDFS Tracker | Configure firewall to allow FastDFS Tracker access:  $ firewall-cmd --permanent --add-port=22122/tcp  $ firewall-cmd --reload |
| FDFS Storage | Configure firewall to allow FastDFS Storage access:  $ firewall-cmd --permanent --add-port=23000/tcp  $ firewall-cmd --reload |
| Redis Server | Configure firewall to allow Redis Server access:  $ firewall-cmd --permanent --add-port=6379/tcp  $ firewall-cmd --reload |
| Redis Sentinel | Configure firewall to allow Redis Sentinel access:  $ firewall-cmd --permanent --add-port=26379/tcp  $ firewall-cmd --reload |
| Tomcat Server | Configure firewall to allow Tomcat Server access:  $ firewall-cmd --permanent --add-port=8080/tcp  $ firewall-cmd --reload |
| PXRetailer Message Server | Configure firewall to allow PXRetailer Messager Server access:  $ firewall-cmd --permanent --add-port=8089/tcp  $ firewall-cmd --reload |
| Nginx Proxy for Tomcat Server | Configure firewall to allow port 10443:  $ firewall-cmd --permanent --add-port=10443/tcp  $ firewall-cmd --reload |
| Nginx Proxy for PXRetailer Message Server | Configure firewall to allow port 10089:  $ firewall-cmd --permanent --add-port=10089/tcp  $ firewall-cmd --reload |

## Install

### Install DB

#### MySQL

If MySQL is adopted, follow the following steps to install MySQL database.

|  |  |
| --- | --- |
|  | For production, you must deploy DB on another independent server. Don’t put DB together with PPM Web Server.  MySQL has a dependency on the libaio library. Data directory initialization and subsequent server startup steps will fail if this library is not installed locally. If necessary, install it using the appropriate package:  $ manager.yum install libaio |

|  |  |
| --- | --- |
| Install MySQL | |
| 1) | Login DB server machine as root. |
| 2) | Copy PPM Installation package to the machine. |
| 3) | Unpack PPM Installation package:  $tar -xzvf [PPM Installation Package] -C /opt  “[PPM Installation Package]” refers to the PPM installation package name. |
| 4) | Install MySQL:  $ cd /opt/pax/support\_scripts  $ ./install.sh -i mysql |

#### Oracle

If Oracle is adopted, using PPM SQL script package to initialize the database.

|  |  |
| --- | --- |
| Init Oracle Database | |
| 1) | Login DB server machine. |
| 2) | If the oracle database has not been installed, please install oracle database software and create a database instance for PPM |
| 3) | Create a database user for PPM |
| 4) | Initialize tables for PPM   1. Copy PPM SQL script package to Oracle HOME directory 2. Then unzip SQL script package   $ unzip [SQL Script Package]  “[SQL Script Package]” should be replaced with the PPM SQL script package name.   1. Create tables and initialize tables   $ cd ppm\_oracle  $ sqlplus [PPM database user]/[PPM database password]@[ oracle database name]  SQL> spool paxppm.log;  SQL> set define off;  SQL> @ create\_tms.sql;  SQL> @ init\_tms.sql;  SQL> @ country.sql;  SQL> @ permission.sql;  SQL> @ tables\_oracle.sql;  SQL> spool off;  SQL>exit; |

### Install PPM Bundle (Master)

|  |  |
| --- | --- |
| Install PPM Bundle | |
| 1) | Login PPM Server machine as root. |
| 2) | Copy PPM Installation package to the machine. |
| 3) | Unpack PPM Installation package:  $tar -xzvf [PPM Installation Package] -C /opt  “[PPM Installation Package]” refers to the PPM installation package name. |
| 4) | Install PPM master:  $ cd /opt/pax/support\_scripts  $ ./install.sh -i master  It should install all the components except mysql. |

## Configure

### PPM Config File - tms.properties

Login PPM Server machine as root, edit PPM configuration file:

$ vi /opt/pax/ppm/main/conf/tms.properties

|  |  |
| --- | --- |
| /opt/pax/ppm/main/conf/tms.properties | |
| Server URLs | Configure the host of PPM Server  #############CAS SSO AUTHENTICATION #############  cas.server.prefix=https://192.168.6.175:10443/cas  tms.server.prefix=https://192.168.6.175:10443/tms  Note: 192.168.6.175 is the host of the PPM Server, and please replace it with actual server IP address. |
| Database | Configure database connection  ############DATABASE ###############  #----- MySQL 5.7 or greater (default)  database.user=paxppm  database.password=\*\*\*\*\*\* #(Note: replace it with actual passport for db user ‘paxppm’  database.url=jdbc:mysql://localhost:3306/pax\_ppm?useUnicode=true&characterEncoding=UTF-8&useCursorFetch=true&useSSL=false&useLegacyDatetimeCode=false&serverTimezone=UTC  database.driverClass=com.mysql.jdbc.Driver  database.validationQuery=select 1  hibernate.dialect=org.hibernate.dialect.MySQLInnoDBDialect  quartz.config=classpath:ppm\_quartz\_clustering.properties  #----- Oracle 11g/12c  #database.user=pax\_ppm  #database.password=\*\*\*\*\*\* #(Note: replace it with actual passport for db user ‘paxppm’  #database.url=jdbc:oracle:thin:@192.168.6.157:1521:prdbps01  #database.driverClass=oracle.jdbc.OracleDriver  #database.validationQuery=select 0 from dual  #hibernate.dialect=org.hibernate.dialect.Oracle10gDialect  #quartz.config=classpath:ppm\_quartz\_clustering\_oracle.properties  Note:  If you are using oracle database  a) Either MySQL or Oracle was used, please comment the other. Only one database configuration shall be enabled here.  b) “prdbps01” should be replaced with [Oracle\_SID];  c) “192.168.6.157:1521” should be replaced with Oracle Service IP and port |
| Redis | Configure Redis connection  ############### REDIS###############  spring.redis.sentinel.nodes=ppm-redis-master:26379  # cluster config  # spring.redis.sentinel.nodes=192.168.6.175:26379,192.168.6.176:26379  Note:  If you’re deploying a cluster server, please use the following configuration:  spring.redis.sentinel.nodes=192.168.6.175:26379,192.168.6.176:26379  “192.168.6.175” and “192.168.6.176” should be replaced with PPM Server IP addresses. |
| Email | Configure email server  ############### EMAIL ###############  email.host=smtp.163.com  email.port=465  email.user=\*\*\*\*\*\*  email.password=\*\*\*\*\*\*  email.from=\*\*\*\*\*\*  email.name=PAX Technical Support  Example：  Here is an example of using office365  email.host=smtp.office365.com  email.port=587  email.user=TMS@pax.us  email.password=\*\*\*\*\*\*  email.from=TMS@pax.us  email.name=PAX Technical Support |
| PXRetailer Message Server | Configure PXRetailer Message Server  #############PXRetailer MESSAGE SERVER##############  # Defines how many times terminal will try to download a package before giving up.  pxretailer.downloadRetryAttempts=3  pxretailer.syncToServerTime=false  pxretailer.terminalTimeSynInterval=7200000  pxretailer.chsDelay=300  pxretailer.hmsDelay=300  pxretailer.adsDelay=5  # Set terminal status offline when the server did not receive heart beat message  # from terminal for the last maxHeartBeatInterval milliseconds  pxretailer.maxHeartBeatInterval=600000 |
| PXDesigner | Configure PXDesigner parameters  #################PXDesigner ################  # For security reasons, PPM web service only can be called from local address.  # You can set the pxdesigner server ip to allow PXDesigner to access PPM web service instance remotely.  pxdesigner.server.ip=  # for example: pxdesigner.server.ip=192.168.98.52,192.168.98.5  # After successful authentication, CAS will redirect the user to the specified URL  pxdesigner.login.callbackUrl= |
| Amazon SNS | Configure Amazon SNS  ###########Amazon SNS #############  sms.amazon.service.enable=false  # Creates a new profile credentials provider that returns the AWS security credentials for the  # specified profiles configuration file and profile name.  sms.amazon.profilesConfigFile=classpath:amazon-sns-credentials  sms.amazon.profileName=PaxAlertMonitor  sms.amazon.disableCertChecking=true |
| LDAP | Configure LDAP server  ########## LDAP AUTHENTICATION#########  tms.ldap.enabled=falsetms.ldap.url=ldap://192.168.6.201:389  # baseDN to search on  tms.ldap.baseDn=cn=Users,dc=pax,dc=com  # search filter to execute; e.g. (mail={user})  # e.g. tms.ldap.searchFilter=sAMAccountName={user}  # tms.ldap.searchFilter=%s@ldaptive.org  tms.ldap.searchFilter=sAMAccountName={user}  # If your directory does not allow anonymous access to the attribute used for DN resolution then you can configure a BindConnectionInitializer  # manager/administrator DN  tms.ldap.managerDn=cn=administrator,cn=Users,dc=pax,dc=com  # manager/administrator password  tms.ldap.managerPassword=Pax123qwe  # whether to throw an exception if multiple entries are found with the search filter  tms.ldap.allowMultipleDns=false  # whether a subtree search should be performed; by default a onelevel search is used  tms.ldap.subtreeSearch=true |
| User Management | Configure parameters  ############### USER MANAGEMENT ###############  # Users set to suspend after x times of password verification failure (Default = 6).  tms.user.lockUserAccountAfterFailedLoginTimes=6  # Users set to suspend after x days of inactivity (Default = 30).  tms.user.inactiveUser.lock.days=30  tms.user.inactiveUser.lock.warningDays=7  # Users deleted after x days of inactivity (Default = 90).  tms.user.inactiveUser.delete.days=90  # User password is required to be changed every x days (Default=28 days).  tms.user.passwordExpiration.days=28  tms.user.passwordExpiration.warningDays=7  # The past x number of passwords, where x = configurable, passwords cannot be used. (Default=13)  tms.user.oldPassword.preserveNumber=13  tms.user.useGlobalSetting=true  tms.user.password.encode.staticSalt=pax  tms.user.forgetPasswordUrl=${tms.server.prefix}/user/forgetMyPassword  tms.user.resetPasswordUrl=${tms.server.prefix}/user/resetMyPassword |
| System Cleaner | Configure parameters  ############# SYSTEM CLEANER ##########  # delete audit log after a specified retention time frame  # Unit: Month  tms.auditLogRetentionTime=13  # delete user log after a specified retention time frame  # Unit: Month  tms.userLogRetentionTime=13  # delete log files after a specified retention time frame  # Unit: Month  tms.logFileRetentionTime=3  tms.logFileDirs=/opt/pax/ppm/main/logs,/opt/pax/ppm/main/tomcat-ins/logs  # delete terminal event log after a specified retention time frame  # Unit: Month  tms.terminalEventLogRetentionTime=13  # delete group event log after a specified retention time frame  # Unit: Month  tms.groupEventLogRetentionTime=13  # delete terminal usage data after a specified retention time frame  # Unit: Month  tms.terminalUsageDataRetentionTime=13  # delete unused package after a specified retention time frame  # Unit: Month  tms.unusedPackageRetentionTime=13 |

### FastDFS Connection - fastdfs.yml

Login PPM Server machine as root, edit FastDFS configuration file:

$ vi /opt/pax/ppm/main/conf/fastdfs.yml

|  |  |
| --- | --- |
| /opt/pax/ppm/main/conf/fastdfs.yml | |
| FastDFS | Configure FastDFS  # =======================  # The distributed file system FDFS configuration  # ========================  fdfs:  trackerList: #support multiple trackers  - ppm-fdfs-tracker:22122  Note:  If you’re deploying a cluster server, use the following configuration:  fdfs:  trackerList: #support multiple trackers  - 192.168.6.175:22122  - 192.168.6.176:22122  “192.168.6.175” and “192.168.6.176” should be replaced with PPM Server IP addresses. |

### Nginx Config File – nginx.conf

Login PPM Server machine as root, edit PPM configuration file:

$ vi /opt/pax/ppm/nginx/conf/nginx.conf

|  |  |
| --- | --- |
| /opt/pax/ppm/nginx /conf/nginx.conf | |
| Global Setting | Configure the maximum size of the uploaded file:  client\_max\_body\_size 1024M;  Config buffer size：  fastcgi\_buffer\_size 64k;  fastcgi\_buffers 4 64k;  fastcgi\_busy\_buffers\_size 128k;  fastcgi\_temp\_file\_write\_size 128k;  Blocking nginx version information in response headers  server\_tokens off; |
| Tomcat Setting | Config Tomcat:  # upstream (Load balancing server settings): This command is mainly used for load balancing, setting up a series of back-end servers  #upstream ppm-tomcat {  # ip\_hash;  # server 192.168.6.175:8080;  # server 192.168.6.176:8080;  #}  # server command is mainly used to specify the host and port.  # ppm-tomcat is the load-balancing server name. The following configuration indicates that nginx proxy to 8080 through 10443. If you want to configure load balancing, add the server and configure the load balancing scheduling algorithm (The default is polling).  upstream ppm-tomcat {  server 127.0.0.1:8080;  }  # CA digital certificates configured for HTTPS  ssl\_certificate certs/ppm.crt;  # Configure the server private key for https  ssl\_certificate\_key certs/ppm.key;  location / {  # This ppm-tomcat must match the name of upstream  proxy\_pass <http://ppm-tomcat>;  # If you need to modify the "Location" and "Refresh" fields in the response header from the proxy server, you can use the proxy\_redirect command to set  proxy\_redirect http:// https://;  # proxy\_set\_heade allows the request header sent to the proxy server to be redefined or some fields to be added.  proxy\_set\_header Host $host:$server\_port;  proxy\_set\_header X-real-ip $remote\_addr;  proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;  # Requests and responses timeout setting:  proxy\_connect\_timeout 300;  proxy\_send\_timeout 300;  proxy\_read\_timeout 300;  If you want to restrict use of SwaggerUI, configure it as follows:  Delete or off underscores\_in\_headers on;  Or close port  Update proxy\_set\_header Host $host:$server\_port; to proxy\_set\_header Host $host;  Additional security configuration for penetration testing：  To prevent users from maliciously modifying the Host field in the HTTP Header, the following checks are added to nginx.conf to verify the validity of the Host field.  if ($host != '0.0.0.0') {  return 403;  }  Note: '$host' can only use IP or domain name, you must modify it after installation.  Using Swagger-UI exposes JQuery version information, the following configuration will disable Swagger-UI.  if ($uri = '/tms/swagger-ui.html') {  return 403;  }  Prohibit methods other than GET,POST,PUT, such as OPTIONS.  if ($request\_method !~\* GET|POST|PUT) {  return 403;  } |
| PxRetailer Setting | The steps to configure one-way authentication for HTTPS are as follows：  #### Begining of PxRetailer ####  #upstream ppm-pxretailer {  # server 192.168.6.175:8089 weight=1;  # server 192.168.6.176:8089 weight=1;  #}  upstream ppm-pxretailer {  server localhost:8089 weight=1;  }  server {  #Support https  listen 10089 ssl;  server\_name localhost;  #Configure CA certificate and server private key  ssl\_certificate certs/server.crt;  ssl\_certificate\_key certs/server.key;    ## If two-way authentication is required, add ssl\_client\_certificate and ssl\_verify\_client configurations:  ## ssl\_client\_certificate certs/ca.crt;  ## ssl\_verify\_client on;  ssl\_session\_cache shared:SSL:1m;  ssl\_session\_timeout 5m;  ssl\_ciphers HIGH:!aNULL:!MD5;  ssl\_prefer\_server\_ciphers on;    location / {  proxy\_pass http://ppm-pxretailer;  proxy\_set\_header Host $host;  proxy\_set\_header X-real-ip $remote\_addr;  proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;  }  }  #### Ending of the PxRetailer ####  If you want to support two-way authentication of pxretailer, add the following two statements under pxretailer:  p.s This is just the configuration of PPM  # The root certificate public key, which is used to authenticate each client  ssl\_client\_certificate /data/sslKey/root-cert.cer;  # Open client certificate verification  ssl\_verify\_client on;  For certificate generation of one-way authentication or two-way authentication, please refer to the following:  CA private key:    Please use this CA certificate to generate other certificates.  Generate the server-side private key  1. Generate a server private keys: server.key  openssl genrsa -out server.key 4096  2. Generate a server-side digital certificate request: server.csr  openssl req -new -key server.key -out server.csr  #Country Name, State or Province Name, Locality Name, Organizational Name(I filled in the Choosefine Ltd), Common Name must be filled in. Others can be left blank。  ##Notes: If you are accessing it with an IP address, then 'Common Name' can be accessed by entering IP. If using domain name access, then 'Common Name' must be the domain name!  3. Issuing the server's digital certificate with the CA private key: server.crt  openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt -days 9999  Generate the client-side private key  1. Generate client private keys and certificates: client.key  openssl genrsa -out client.key 4096  2. Generate a client-side digital certificate request: client.csr  openssl req -new -key client.key -out client.csr  ##Notes: The information entered here needs to be consistent with what was entered when server.csr was generated.  3. Issuing the client's digital certificate with the CA private key: client.crt  openssl x509 -req -in client.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out client.crt -days 9999  4. Generate client p12 format root certificate  openssl pkcs12 -export -clcerts -in client.crt -inkey client.key -out client.p12 |

‘

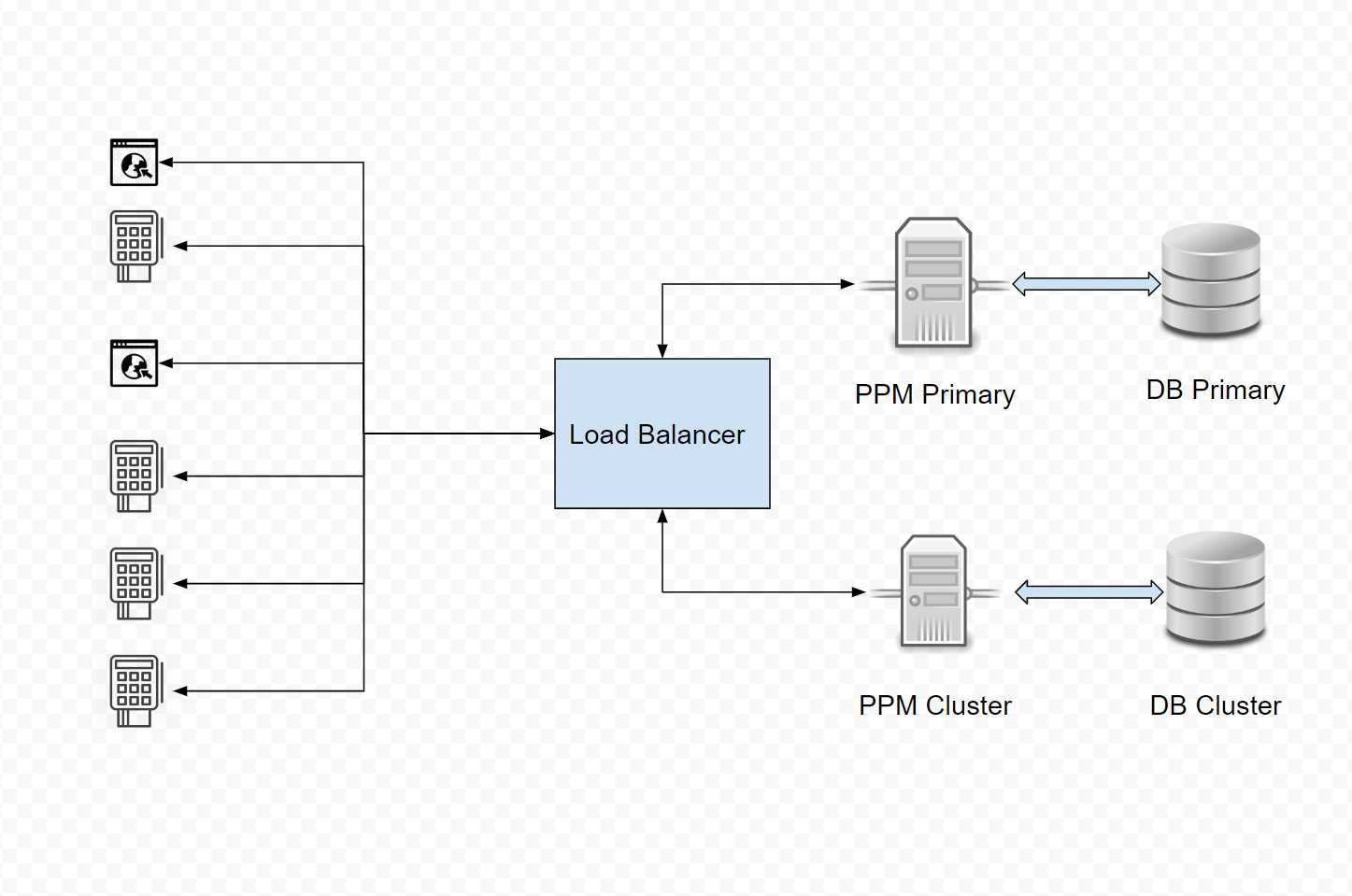
## Start & Stop PPM

|  |  |
| --- | --- |
| Start & Stop PPM | |
| 1) | Login server machine as PPM. Make sure your DB is config right and connectable |
| 2) | Start PPM  $ cd /opt/pax/ppm/bin  $ sudo ./start\_all.sh |
| 3) | After start PPM successfully, enter URL: <https://[host]:10443/tms> in browser, then you can successfully visit TMS website. The initial user name and password is: admin/pax123456  PXRetailer Message Server IP and Port: [host]:10089 |
| 4) | Stop PPM  $ cd /opt/pax/ppm/bin  $ sudo ./stop\_all.sh |

# Install PPM Cluster (Redundant) – Optional

## Introduction

PPM supports a redundant deployment, which enables a clustered server instance to take over the service immediately in case its primary server’s running failure.



## Install Master

See the section: [Install PPM Bundle (Master)](#_Install_PPM_(Master))

## Install Slave

|  |  |
| --- | --- |
| Install Slave | |
| 1) | Login PPM Slave Server machine as root. |
| 2) | Get PPM installation package |
| 3) | Unpack PPM Installation package:  $tar -xzvf [PPM Installation Package] -C /opt  “[PPM Installation Package]” should be replaced with the PPM installation package name. |
| 4) | Install PPM master:  $ cd /opt/pax/support\_scripts  $ ./install.sh -i slave  It should install all the components except mysql. |

## Configure Cluster

### PPM Config File - tms.properties

Login **PPM Master Server and PPM Slave Server** machine as root, edit PPM configuration file:

$ vi /opt/pax/ppm/main/conf/tms.properties

|  |  |
| --- | --- |
| /opt/pax/ppm/main/conf/tms.properties | |
| Server URLs | Configure the host of **PPM Master Server**:  #############CAS SSO AUTHENTICATION #############  cas.server.prefix=https://192.168.6.175:10443/cas  tms.server.prefix=https://192.168.6.175:10443/tms  Note: 192.168.6.175 is the host of the **PPM Master Server**, and you should replace it with the actual value. |
| Database | Configure database connection  ############DATABASE ###############  #----- MySQL 5.7 or greater (default)  database.user=paxppm  database.password=\*\*\*\*\*\* #(Note: replace it with actual passport for db user ‘paxppm’  database.url=jdbc:mysql://localhost:3306/pax\_ppm?useUnicode=true&characterEncoding=UTF-8&useCursorFetch=true&useSSL=false&useLegacyDatetimeCode=false&serverTimezone=UTC  database.driverClass=com.mysql.jdbc.Driver  database.validationQuery=select 1  hibernate.dialect=org.hibernate.dialect.MySQLInnoDBDialect  quartz.config=classpath:ppm\_quartz\_clustering.properties  #----- Oracle 11g/12c  #database.user=pax\_ppm  #database.password=\*\*\*\*\*\* #(Note: replace it with actual passport for db user ‘paxppm’  #database.url=jdbc:oracle:thin:@192.168.6.157:1521:prdbps01  #database.driverClass=oracle.jdbc.OracleDriver  #database.validationQuery=select 0 from dual  #hibernate.dialect=org.hibernate.dialect.Oracle10gDialect  #quartz.config=classpath:ppm\_quartz\_clustering\_oracle.properties  Note:  If you are using oracle database  a) Either MySQL or Oracle was used, please comment the other. Only one database configuration shall be enabled here.  b) “prdbps01” should be replaced with [Oracle\_SID];  c) “192.168.6.157:1521” should be replaced with Oracle Service IP and port |
| Redis | Configure Redis connection:  ############### REDIS###############  spring.redis.sentinel.nodes=ppm-redis-master:26379  # cluster config  # spring.redis.sentinel.nodes=192.168.6.175:26379,192.168.6.176:26379  Note:  If you deploy a cluster, use the following configuration:  spring.redis.sentinel.nodes=192.168.6.175:26379,192.168.6.176:26379  “192.168.6.175” and “192.168.6.176” should be replaced with PPM Server IP addresses. |

For other configuration items, see the section: [Configure – tms.properties](#_tms.properties)

### FastDFS Connection - fastdfs.yml

Login **PPM Master Server and PPM Slave Server** machine as root, edit FastDFS configuration file:

$ vi /opt/pax/ppm/main/conf/fastdfs.yml

|  |  |
| --- | --- |
| /opt/pax/ppm/main/conf/fastdfs.yml | |
| FastDFS | Configure FastDFS:  # =======================  # The distributed file system FDFS configuration  # ========================  fdfs:  trackerList: #support multiple trackers  - ppm-fdfs-tracker:22122  Note:  If you deploy a cluster, use the following configuration:  fdfs:  trackerList: #support multiple trackers  - 192.168.6.175:22122  - 192.168.6.176:22122  “192.168.6.175” and “192.168.6.176” should be replaced with PPM Server IP addresses. |

### FastDFS Storage - storage.conf

Login **PPM Master Server and PPM Slave Server** machine as root, edit FastDFS Storage configuration file:

$ vi /opt/pax/ppm/fdfs\_ppm/conf/storage.conf

|  |  |
| --- | --- |
| /opt/pax/ppm/fdfs\_ppm/conf/storage.conf | |
| FastDFS Storage | Configure FastDFS Storage:  # tracker\_server can ocur more than once, and tracker\_server format is  # "host:port", host can be hostname or ip address  tracker\_server=ppm-fdfs-tracker:22122  # cluster config  # tracker\_server=192.168.6.176:22122  # tracker\_server=192.168.6.175:22122  Note:  If you deploy a cluster   1. delete the following configuration:   tracker\_server=ppm-fdfs-tracker:22122  2) use the following configuration:  # cluster config  tracker\_server=192.168.6.176:22122  tracker\_server=192.168.6.175:22122  “192.168.6.175” and “192.168.6.176” should be replaced with PPM Server IP addresses. |

### Nginx Proxy - nginx.conf

Login **PPM Master Server and PPM Slave Server** machine as root, edit Nginx Proxy for Tomcat Server and PXRetailer Message Server:

$ vi /opt/pax/ppm/nginx/conf/nginx.conf

|  |  |
| --- | --- |
| /opt/pax/ppm/nginx/conf/nginx.conf | |
| Nginx Proxy for Tomcat Server | Configure Nginx Proxy for Tomcat Server:  #### Begining of Tomcat ####  #upstream ppm-tomcat {  # ip\_hash;  # server 192.168.6.175:8080;  # server 192.168.6.176:8080;  #}  upstream ppm-tomcat {  server 127.0.0.1:8080;  }  Note:  If you deploy a cluster   1. delete the following configuration:   upstream ppm-tomcat {  server 127.0.0.1:8080;  }  2) use the following configuration:  upstream ppm-tomcat {  ip\_hash;  server 192.168.6.175:8080;  server 192.168.6.176:8080;  }  “192.168.6.175” and “192.168.6.176” should be replaced with PPM Server IP addresses. |
| Nginx Proxy for PXRetailer Message Server | Configure Nginx Proxy for Tomcat Server:  #### Begining of PxRetailer ####  #upstream ppm-pxretailer {  # server 192.168.6.175:8089 weight=1;  # server 192.168.6.176:8089 weight=1;  #}  upstream ppm-pxretailer {  server localhost:8089 weight=1;  }  Note:  If you deploy a cluster   1. delete the following configuration:   upstream ppm-pxretailer {  server localhost:8089 weight=1;  }  2) use the following configuration:  upstream ppm-pxretailer {  server 192.168.6.175:8089 weight=1;  server 192.168.6.176:8089 weight=1;  }  “192.168.6.175” and “192.168.6.176” should be replaced with PPM Server IP addresses. |

## Start & Stop PPM Cluster

1. Start **PPM Master Server**, see [Start & Stop PPM](#_Start_&_Stop)
2. Start **PPM Slave Server**, see [Start & Stop PPM](#_Start_&_Stop)

# Configuration Table

|  |  |
| --- | --- |
| Component | Configuration |
| MySQL | Database: pax\_ppm  Users:  root / PaxPPM\_123@pax  paxppm / PaxPPM\_123@hz |
| Redis Server | Port: 6379 |
| Redis Sentinel | Port: 26379 |
| FDFS Tracker | Port: 22122 |
| FDFS Storage | Port: 23000 |
| Tomcat Server | Port: 8080 |
| PXRetailer Message Server | Port: 8089 |
| Nginx Proxy for Tomcat Server | Port: 10443 |
| Nginx Proxy for PXRetailer Message Server | Port: 10089 |

References

1. FastDFS - GitHub: <https://github.com/happyfish100/fastdfs>
2. Redis - Official Site: <https://redis.io/>
3. Apache Tomcat - Official Site: <http://tomcat.apache.org/>
4. Nginx - Official Site: <http://nginx.org/>
5. MySQL- Offical Site: <https://www.mysql.com/>

Appendix 1

FAQ

**PAX Portfolio Manager Installation Guide**

