RIL-TMS
Production Operational Guide

Document Version 1.1.3
Updated - 12th October 2018

Version History

Version	**Date**	**Author**	**Changes**
1.0	01/27/2017	Rajesh B S	First version
1.0.2	02/20/2017	Rajesh B S	Review of TMS Application Installation
1.0.3	03/30/2017	Rajesh B S	Tomcat Configuration Changes
1.0.5	04/15/2017	Rajesh B S	Tomcat logrotate and Startup scripts
1.0.6	29/04/2017	Rajesh B S	Tomcat and Application Configuration Changes
1.0.8	11/05/2017	Rajesh B S	Simplification of the setup
1.0.9	11/01/2018	Kumar Swamy	Reviewed the document
1.0.10	07/06/2018	Sauri N	Updated the Application properties
1.1	04/10/2018	Sauri N	Modified for Production Setup
1.1.1	11/10/2018	Sauri N	Addition Parameters of the Production
1.1.2	12/10/2018	Rudra H	Reviewed on the Application Properties
1.1.3	21/02/2019	Sauri N	Updated the changes requested by InfoSec Team

girmiti software™

Girmiti Software Private Limited
SLV PLAZA, ARVIND AVENUE
KUNDALAHALLI,
MARATHAHALLI BANGALORE 560037

Table of Content

1. Introduction

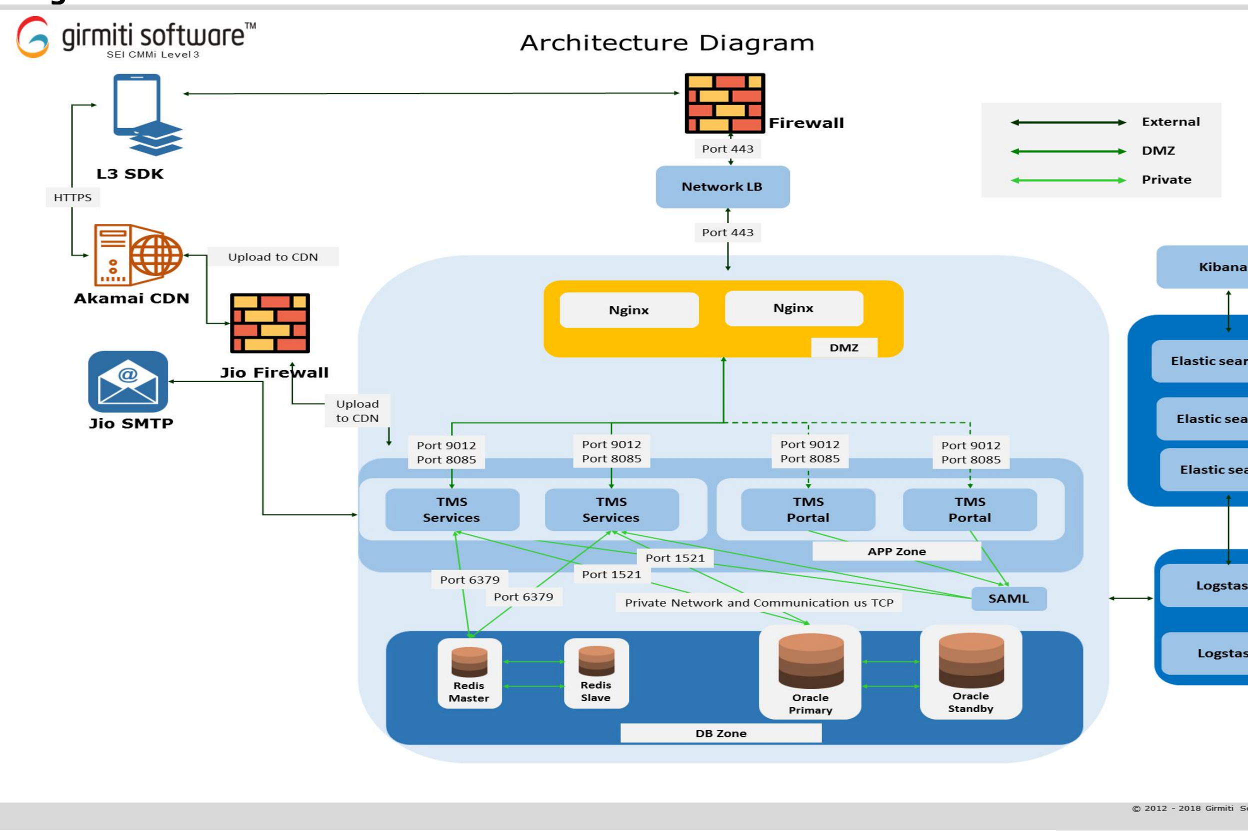
This document covers the RJIL TMS Production Setup

2. Purpose

The purpose is the cover each configuration items to complete the production setup.

3. Production

3.1. Architecture Diagram



This diagram below is the production infrastructure design approved by the RJIL Team, specifically accepted by InfoSec Team, Product Team of RJIL.

3.2. Hardware Servers

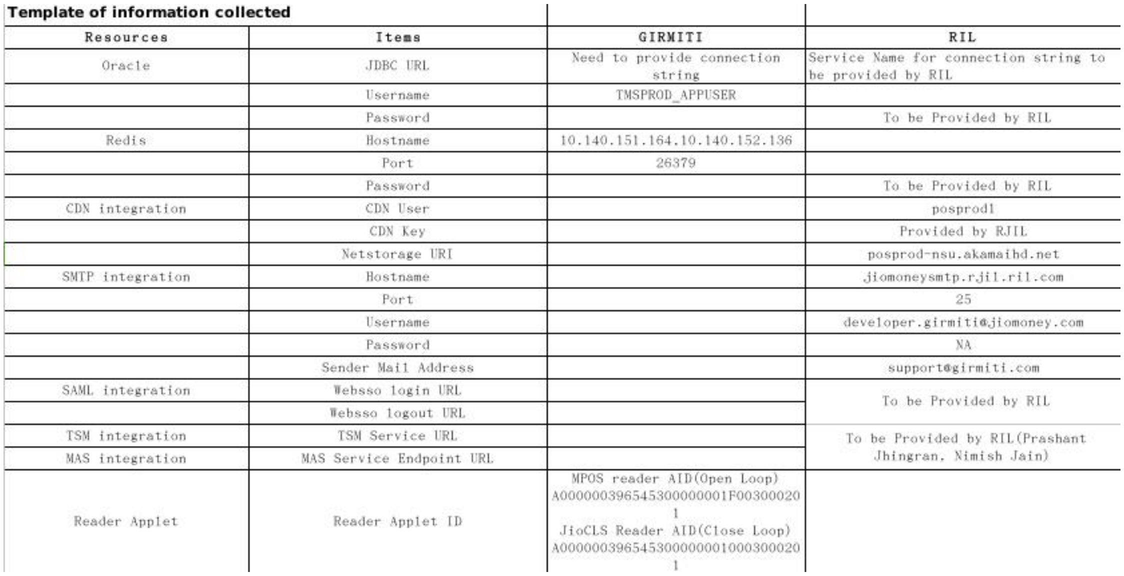
Production Server provided by the RIL for TMS application installation and Configurations.

Services	vCPU	RAM	Storage	IPs
TMS-Girmiti - TMS - Portal1	2	8	400 GB	10.140.132.114
TMS-Girmiti - TMS - Portal2	2	8	400 GB	10.140.150.108
TMS-Girmiti - TMS - Service1	8	21	500 GB	10.140.132.115
TMS-Girmiti - TMS - Service2	8	19	500GB	10.140.150.109
TMS-Girmiti - Redis1	8	16	500 GB	10.140.151.164
TMS-Girmiti - Redis2	8	16	500 GB	10.140.152.136
TMS-Girmiti - Oracle 1	16	32	1.500 TB	10.140.133.81
TMS-Girmiti- Oracle 2	16	32	1.500 TB	10.140.133.87
TMS-Girmiti - NGinx LB1	2	8	400 GB	10.140.129.150
TMS-Girmiti - NGinx LB2	2	8	400 GB	10.140.129.151
TMS-Girmiti - Logstash1				10.140.151.166
TMS-Girmiti - Logstash2				10.140.152.137
TMS-Girmiti - Elastic search				10.140.151.163
TMS-Girmiti - Elastic search 2				10.140.151.165
TMS-Girmiti - Elastic search 3				10.140.152.138
TMS-Girmiti - Kibana				10.140.144.156

3.3. Firewall Ports and Network Flow

Table below helps to open the ports on each zone and shows the network flow between all the zone

3.4. Checklists



Template of information collected

Resources	Items	GIRMITI	RIL
Oracle	JDBC URL	Need to provide connection string	Service Name for connection string to be provided by RIL
	Username	TMSPROD_APPUSER	
	Password		To be Provided by RIL
Redis	Hostname	10.140.151.164.10.140.152.136	
	Port	26379	
	Password		To be Provided by RIL
CDN integration	CDN User		posprod1
	CDN Key		Provided by RJIL
	Netstorage URI		posprod-nsu.akamaihd.net
SMTP integration	Hostname		jiomoneysmtp.rjil.ril.com
	Port		25
	Username		developer.girmiti@jiomoney.com
	Password		NA
	Sender Mail Address		support@girmiti.com
SAML integration	Websso login URL		To be Provided by RIL
	Websso logout URL		
TSM integration	TSM Service URL		To be Provided by RIL(Prashant Jhingran, Nimish Jain)
MAS integration	MAS Service Endpoint URL		
Reader Applet	Reader Applet ID	MPOS reader AID(Open Loop) A000000396545300000001F003000201 JioCLS Reader AID(Close Loop) A0000003965453000000010003000201	

Contact Details

- Prashanth
- Miten
- Arun
- Elango
- Rajesh S
- Rudra
- Imtiyaz
- Rajesh B S
- Kumarswamy

3.5. Application Server Installation

Installation of Software servers components on the relevant server.

```
tar -zxvhf jdk-8u162-linux-x64.tar
tar -zxvhf apache-tomcat-8.5.27.tar.gz
yum install redis-3.2.10-2.el7.x86_64.rpm
yum install nginx-1.12.2-1.el7_4.ngx.x86_64.rpm
yum install nginx-module-perl-1.12.1-1.el7.ngx.x86_64
yum install nginx-module-xslt-1.12.1-1.el7.ngx.x86_64
yum install nginx-module-geoip-1.12.1-1.el7.ngx.x86_64
```

Kernel parameters of the servers

1) Check the default settings on the servers

```
sudo cat /proc/sys/net/ipv4/tcp_keepalive_time
sudo cat /proc/sys/net/ipv4/tcp_keepalive_intvl
sudo cat /proc/sys/net/ipv4/tcp_keepalive_probes
sudo cat /proc/sys/net/ipv4/tcp_retries2
sudo cat /proc/sys/net/ipv4/tcp_retries1
```

```
sudo cat /proc/sys/net/ipv4/tcp_keepalive_time
7200
sudo cat /proc/sys/net/ipv4/tcp_keepalive_intvl
75
sudo cat /proc/sys/net/ipv4/tcp_keepalive_probes
9
sudo cat /proc/sys/net/ipv4/tcp_retries2
15
```

Add in rc.local

```
sudo echo "6" > /proc/sys/net/ipv4/tcp_keepalive_time
sudo echo "1" > /proc/sys/net/ipv4/tcp_keepalive_intvl
sudo echo "10" > /proc/sys/net/ipv4/tcp_keepalive_probes
sudo echo "3" > /proc/sys/net/ipv4/tcp_retries2
sudo echo "0" > /proc/sys/net/ipv4/tcp_retries1
```

Make these parameters permanent by adding the below to sysctl.conf so these are applied even after the reboot.

```
sudo vi /etc/sysctl.conf
net.ipv4.tcp_keepalive_time = 6
net.ipv4.tcp_keepalive_intvl = 1
net.ipv4.tcp_keepalive_probes = 10
net.ipv4.tcp_retries2 = 3
net.ipv4.tcp_retries1 = 0
```

runtime

```
sudo sysctl -w net.ipv4.tcp_retries1=0
sudo sysctl -w net.ipv4.tcp_retries2=3
sudo sysctl -w net.ipv4.tcp_keepalive_probes=10
sudo sysctl -w net.ipv4.tcp_keepalive_intvl=1
sudo sysctl -w net.ipv4.tcp_keepalive_time=6
```

edit /etc/sysctl.conf and add below content to end of file for kernel parameters to persist on reboot

```
net.ipv4.tcp_keepalive_time = 6
net.ipv4.tcp_keepalive_intvl = 1
net.ipv4.tcp_keepalive_probes = 10
net.ipv4.tcp_retries2 = 3
```

3.5.1. nGinx

nGinx Version nginx-1.12.2-2 to be installed

##nginx Server setup

To set up the yum repository , create the file named /etc/yum.repos.d/nginx.repo with the following contents:

```
[nginx]
name=nginx repo
baseurl=http://nginx.org/packages/RHEL/7.3/$basearch/
gpgcheck=0
enabled=1
```

```
sudo yum update
sudo yum install nginx
cd /etc/nginx/conf.d
sudo firewall-cmd --reload
sudo firewall-cmd --add-service=http --permanent
sudo service nginx restart
```

Update the Configuration file as below.

vi/etc/nginx/nginx.conf

```
user  nginx;
worker_processes  2;
error_log  /var/log/nginx/error.log warn;
pid        /var/run/nginx.pid;

events {
    worker_connections  1024;
}

http {
    include       /etc/nginx/mime.types;
    default_type  application/octet-stream;

    log_format  main  '$remote_addr - $remote_user [$time_local]
"$request" '
                      '$status $body_bytes_sent "$http_referer" '
                      '"$http_user_agent" "$http_x_forwarded_for"';

    access_log  /var/log/nginx/access.log  main;
    sendfile        on;
    #tcp_nopush     on;

    keepalive_timeout  60;
# Display nginx Version number in error or http header may result in hacker to search for known vulnerability.
# Therefore, the version number should be removed for every http response.
server_tokens off;

    #gzip  on;
          # set client body size to 2M #
          client_max_body_size 2G;

    include /etc/nginx/conf.d/*.conf;
}
```

Add the backends Tomcat configuration

```
Vi /etc/conf.d/tms_lb.conf
```

```
upstream tms-portal-backend {
    ip_hash;
    server  10.140.132.114:9012;
    server  10.140.132.114:8085;
    server  10.140.150.108:9012;
    server  10.140.150.108:8085;
    }

Upstream tms-service-backend {
     server 10.140.132.115:9012;
     server  10.140.150.109:9012;
     server  10.140.132.115:8085;
     server  10.140.150.109:8085;
}
server {
   listen 8080;
        server_name localhost;

   # Return a 302 redirect to the /webapp/ directory when user
    # requests '/'
    location = / {
        return 302 /chatak-tms/;
    }
   location /chatak-tms-services/ {
        proxy_set_header   X-Real-IP $remote_addr;
        proxy_set_header   Host      $http_host;
        proxy_http_version 1.1;
        proxy_set_header Connection "";
  proxy_connect_timeout 159s;
  proxy_send_timeout   600;
  proxy_read_timeout   600;
      proxy_pass http://tms_portal_backend;

   }

   location /chatak-tms/ {
        proxy_set_header   X-Real-IP $remote_addr;
        proxy_set_header   Host      $http_host;
        proxy_http_version 1.1;
        proxy_set_header Connection "";
        proxy_connect_timeout 159s;
        proxy_send_timeout   600;
        proxy_read_timeout   600;
        proxy_pass http://tms_service_backend;
        allow 10.77.245.96/27;
        allow 10.77.59.96/27;
        deny all;
   }
   location /manager1/ {
      proxy_pass http://10.140.132.114:9012/manager/;
   }
   location /manager2/ {
      proxy_pass http://10.140.150.108:9012/manager/;
   }
location /manager3/ {
      proxy_pass http://10.140.132.115:8085/manager/;
   }
   location /manager4/ {
      proxy_pass http://10.140.150.109:8085/manager/;
   }
}
```

3.5.2. Apache Tomcat

Latest Tomcat Apache version 8.5.34 to be installed from the Apache Tomcat Server Website https://tomcat.apache.org/
- Tomcat 8.5.33 or 8.5.34

```
http://mirrors.estointernet.in/apache/tomcat/tomcat-8/v8.5.34/bin/apache-tomcat-8.5.34.tar.gz

## AppServer Setup
#Run the Script for creation of tomcat user with permission (CIS
benchmark)
## This file purposefully copy to root folder so it does get executed
from user



#Deployment Paths:
mkdir -p /app/tools/tms                -      TMS parent folder
mkdir -p /app/tools/tms/java/jdk1.8.0_162       - Java Home
mkdir -p /app/tools/tms/resources  -      TMS config parent folder
mkdir -p /app/tools/tms/resources/properties     -      application
configuration file
mkdir -p /app/tools/tms/resources/certs          -      client certs
mkdir -p /app/tools/tms/jvm1/      -      Application Server (Tomcat)

useradd -U -d /opt/appservers -M -s /sbin/nologin tomcat
chown -R tomcat:tomcat /opt/appservers/

# Installation of servers
tar -zxvhf jdk-8u162-linux-x64.tar
tar -zxvhf apache-tomcat-8.5.27.tar.gz

[root@Server1 ~]# cat /root/cis_tc_script.sh
chmod 755 /App/tools/tms/jvm1/webapps
chmod g-w,o-rwx /App/tools/tms/jvm1/conf
chmod o-rwx /App/tools/tms/jvm1/logs
chmod o-rwx /App/tools/tms/jvm1/temp
chmod g-w,o-rwx /App/tools/tms/jvm1/bin
chmod g-w,o-rwx /App/tools/tms/jvm1/webapps
chmod 0770 /App/tools/tms/jvm1/conf/catalina.policy
chmod g-w,o-rwx /App/tools/tms/jvm1/conf/catalina.properties
chmod g-w,o-rwx /App/tools/tms/jvm1/conf/context.xml
chmod g-w,o-rwx /App/tools/tms/jvm1/conf/logging.properties
chmod g-w,o-rwx /App/tools/tms/jvm1/conf/server.xml
chmod g-w,o-rwx /App/tools/tms/jvm1/conf/tomcat-users.xml
chmod g-w,o-rwx /App/tools/tms/jvm1/conf/web.xml
chown -R tomcat:tomcat /App/tools/
cd /App/tools/tms/jvm1/lib
mkdir -p org/apache/catalina/util
echo "server.info=Apache Tomcat Version 8.5.x" >
org/apache/catalina/util/ServerInfo.properties
```

```
rm -rf work/* logs/* temp/* webapps/host-manager webapps/ROOT webapps/examples webapps/docs
mkdir -p /App/tools/tms/jvm1/webapps/ROOT/WEB-INF
echo "I am here!" > /App/tools/tms/jvm1/webapps/ROOT/index.html
```

Edit conf/tomcat-users.xml

```
<role rolename="manager-gui"/>
<role rolename="manager-script"/>
<role rolename="manager-jmx"/>
<role rolename="manager-status"/>
<role rolename="admin-gui"/>
<role rolename="admin-script"/>

<user username="DeployTMS"
password="s098uv98sadouihghsrp9vhsuincfsdjf" roles="manager-gui,manager-script,manager-jmx,manager-status,admin-gui,admin-script"/>
```

A default Tomcat installation includes the Manager. To add an instance of the Manager web application Context to a new host install the manager.xml context configuration file in the $CATALINA_BASE/conf/[enginename]/[hostname] folder. Here is an example:

Edit tomcat/conf/context.xml -
Make sure the Path is change appropriately suite the installation.

```
<Environment name="java/chatakTmsSysConfig" override="false"
type="java.lang.String"
value="file:///App/tools/tms/resources/properties/chatak-tms.properties"/>
```

(Change the Context appropriate to your deployment location)

```
#Deployment Paths:
/App/tools/tms                    -       TMS parent folder
/App/tools/tms/java/jdk1.8.0_162  - Java Home
/App/tools/tms/resources    -       TMS config parent folder
/App/tools/tms/resources/properties       -       application configuration file
```

```
/App/tools/tms/resources/certs        -      client certs
/App/tools/tms/jvm1/      -      Application Server (Tomcat)
```

#Add the tomcat service to System Control Manager (systemd Service)

```
[root@Server1 ~]# cat /etc/systemd/system/tms-jvm1.service
[Unit]
Description=TMS Service
After=network.target
After=systemd-user-sessions.service
After=network-online.target

[Service]
Type=forking
User=tomcat
Group=tomcat
WorkingDirectory=/App/tools/tms/jvm1
ExecStart=/App/tools/tms/jvm1/bin/startup.sh
ExecStop=/App/tools/tms/jvm1/bin/shutdown.sh
TimeoutSec=300
Restart=on-failure
RestartSec=30
StartLimitInterval=350
StartLimitBurst=10

[Install]
WantedBy=multi-user.target

[root@Server1 ~]# systemctl daemon-reload
[root@Server1 ~]# systemctl enabled tms-jvm1
[root@Server1 ~]# systemctl start tms-jvm1
```

#To check Tomcat started

[root@Server1 ~]# systemctl status tms-jvm1 -l (if you see green in the output and started - it is health)

#Deployment and Application Configuration

find the logs folder for application logs - /app/tools/tms/jvm1/logs/
chatak-tms.log ---> for web logs
chatak-tms-service ---> for service logs

##Application is already in the info Mode which is default.
To enable it to debug mode ---> goto webapps/chatak-tms/WEB-INF/classes/log4j.properties --> then change the level to Debug

##To start the tomcat in debug mode.
systemctl disable tms-jvm1

```
systemctl stop tms-jvm1
goto --> /App/tools/tms/jvm1/bin/catalina.sh debug
togo back to normal mode ---> close the debug console --> systemctl enable tms-jvm1 --> systemctl start tms-jvm1
```

```
##Deploy the files to webapps folder and restart the tomcat
copy the package (.war) files to /App/tools/tms/jvm1/webapps
systemctl restart tms-jvm1
```

All JVMs should have below parameters in startup.sh

TMS Services JVM Parameters should be as below.

JVM 1 :

```
export CATALINA_OPTS="$CATALINA_OPTS -Dfile.encoding=UTF-8 -Xms1024m -Xmx8192m -Xmn4195m -XX:ParallelGCThreads=4 -XX:-HeapDumpOnOutOfMemoryError -XX:+UseG1GC -Xloggc:/tmp/gc_tms_1.txt
```

JVM 2::

```
export CATALINA_OPTS="$CATALINA_OPTS -Dfile.encoding=UTF-8 -Xms1024m -Xmx7168m -Xmn4300m -XX:ParallelGCThreads=4 -XX:-HeapDumpOnOutOfMemoryError -XX:+UseG1GC -Xloggc:/tmp/gc_tms_2.txt
```

Portal JVM Parameters should be as per below.

JVM 1 :

```
export CATALINA_OPTS="$CATALINA_OPTS -Dfile.encoding=UTF-8 -Xms512m -Xmn2048m -XX:ParallelGCThreads=4 -XX:-HeapDumpOnOutOfMemoryError -XX:+UseG1GC -Xloggc:/tmp/gc_tms_1.txt
```

JVM 2 :

```
export CATALINA_OPTS="$CATALINA_OPTS -Dfile.encoding=UTF-8 -Xms512m -Xmn2048m -XX:ParallelGCThreads=4 -XX:-HeapDumpOnOutOfMemoryError -XX:+UseG1GC -Xloggc:/tmp/gc_tms_2.txt
```

Create a logrotate tomcat file with below content and copy the file to /App/logrotate.d folder on each instance. Find the catalina.out file path of each tomcat instance and modify the script as per that instance and restart cron services. Repeat the below steps for all the JVM’s.

```
# rotate log files daily (override with -f option)
daily
# don't keep any backlogs
rotate 0
# truncate log instead of removing it and making a new file
copytruncate
```

```
# Keep catalina.out unless it gets too big - could be used for debugging startup
/App/tools/tms/jvm1/logs/catalina.out {
  compress
  missingok
}
```

- Perform a test rotation: logrotate --force /App/logrotate.d/tms.rotate
- Archiving of WebApps and Resources and Logs -
- Make a copy of new deployment by pushing the log files to to Remote storage.
- Specifically on the LifeCycle, is part of the decission for Audit purpose. LifeCycle can be, a sync to Remote storage in gz format and schedule storage of the 6 months log and Archive of Yearly files.

  No changes required on the script unless CATALINA_HOME directory is changed during the deployment for each application.

On the Server.xml Modify the application tomcat

Service-JVM1

```
<Server shutdown="SHUTDOWN" port="8005">

<Connector port="9012" maxSwallowSize="2147483648"
maxPostSize="2147483648" maxThreads="500" redirectPort="8443"
connectionTimeout="2000000" protocol="HTTP/1.1"/>
```

Disable by commenting the below line.

```
<Listener className="org.apache.catalina.core.AprLifecycleListener"
SSLEngine="on"/>
```

Service-JVM2

```
<Server shutdown="SHUTDOWN" port="8006">

<Connector port="8085" maxSwallowSize="2147483648"
maxPostSize="2147483648" maxThreads="500" redirectPort="8443"
connectionTimeout="2000000" protocol="HTTP/1.1"/>
```

Disable by commenting the below line.

```
<Listener className="org.apache.catalina.core.AprLifecycleListener"
SSLEngine="on"/>
```

Portal-JVM1

```
<Server shutdown="SHUTDOWN" port="8005">

<Connector port=”9012" maxSwallowSize="2147483648"
maxPostSize="2147483648" maxThreads="500" redirectPort="8443"
connectionTimeout="2000000" protocol="HTTP/1.1"/>
```

Disable by commenting the below line.

```
<Listener className="org.apache.catalina.core.AprLifecycleListener"
SSLEngine="on"/>
```

On the web.xml Modify the application tomcat

Change the Listings to false

```
<init-param>
        <param-name>listings</param-name>
        <param-value>false</param-value>
</init-param>
```

Cross check the session and allign with nGinx Session timeout

```
<session-config>
        <session-timeout>60</session-timeout>
</session-config>
```

For TMS Apk Upload size

```
<multipart-config>
        <!-- 50MB max →
        <max-file-size>419430400</max-file-size>
        <max-request-size>419430400</max-request-size>
        <file-size-threshold>0</file-size-threshold>
</multipart-config>
```

REPEAT ABOVE STEPS FOR JVM2 SETUP ON THE SAME SERVER
REPEAT ABOVE STEPS FOR ALL JVM1/JVM2 OF PORTAL SERVER

Note: The Application would run in tomcat user only and not in root user.

3.5.3. Redis Server and Redis Sentinel Setup

Redis Master Configuration
Redis Master & Slave will run on port 6379

```
#vi /etc/redis.conf
```

```
protected-mode no
port 6379
pidfile /var/run/redis.pid
logfile /var/log/redis/redis.log
```

```
dir /var/lib/redis
appendonly yes
```

Redis Master Sentinel Configuration
Redis Master and Slave Sentinel will run on Port 26379

```
#vi /etc/redis-sentinel.conf
sentinel monitor TMS-REDIS2 10.140.151.164 6379 1
sentinel down-after-milliseconds TMS-REDIS2 5000
sentinel failover-timeout TMS-REDIS2 10000
logfile "/var/log/redis/sentinel.log"
sentinel known-slave TMS-REDIS2 10.140.152.136 6379
```

Redis Slave Configuration

```
#vi /etc/redis.conf
bind *
protected-mode no
port 6379
pidfile /var/run/redis.pid
logfile /var/log/redis/redis.log
dir /var/lib/redis
slaveof 10.140.151.164 6379
appendonly yes
```

Redis Slave Sentinel Configuration

```
sentinel monitor TMS-REDIS2 10.140.151.164 6379 1
sentinel down-after-milliseconds TMS-REDIS2 5000
sentinel failover-timeout TMS-REDIS2 10000
logfile "/var/log/redis/sentinel.log"
```

To check status of Redis on Redis 1

```
#systemctl status redis
● redis.service - Redis persistent key-value database
   Loaded: loaded (/usr/lib/systemd/system/redis.service; disabled; vendor preset:
disabled)
  Drop-In: /etc/systemd/system/redis.service.d
           └─limit.conf
   Active: active (running) since Fri 2018-10-05 21:51:10 IST; 2s ago
 Main PID: 32228 (redis-server)
   Memory: 1.0M
   CGroup: /system.slice/redis.service
           └─32228 /usr/bin/redis-server *:6379
```

To check the status of Redis Sentinel on Redis 1

```
#systemctl status redis-sentinel
● redis-sentinel.service - Redis Sentinel
   Loaded: loaded (/usr/lib/systemd/system/redis-sentinel.service; enabled; vendor
preset: disabled)
  Drop-In: /etc/systemd/system/redis-sentinel.service.d
           └─limit.conf
   Active: active (running) since Fri 2018-10-05 19:24:40 IST; 2h 57min ago
  Process: 28208 ExecStop=/usr/libexec/redis-shutdown redis-sentinel (code=exited, status=0/SUCCESS)
 Main PID: 28241 (redis-sentinel)
   Memory: 1.4M
   CGroup: /system.slice/redis-sentinel.service
           └─28241 /usr/bin/redis-sentinel *:26379 [sentinel]

Oct 05 19:24:40 girmiti systemd[1]: Starting Redis Sentinel...
Oct 05 19:24:40 girmiti systemd[1]: Started Redis Sentinel.
```

To check status of the configuration done use the below command

```
#redis-cli -h 10.140.151.164  -p 6379
> info
# Clients
connected_clients:3
client_longest_output_list:0
client_biggest_input_buf:0
blocked_clients:0

# Replication
role:master
connected_slaves:1
slave0:ip=10.140.152.136,port=6379,state=online,offset=1,lag=0
master_repl_offset:1
repl_backlog_active:1
repl_backlog_size:1048576
repl_backlog_first_byte_offset:2
repl_backlog_histlen:0
```

We can implement the same with Sentinel as given below

```
#redis-cli -h 10.140.151.164 -p 26379
# Server
redis_version:3.2.12
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:3dc3425a3049d2ef
redis_mode:sentinel
os:Linux 3.10.0-693.11.1.el7.x86_64 x86_64
arch_bits:64
multiplexing_api:epoll
gcc_version:4.8.5
process_id:28241
run_id:e4bb594d6fb3e1c359852958e23c4ce0b3c70d3b
tcp_port:26379
uptime_in_seconds:11104
uptime_in_days:0
hz:11
lru_clock:12032128
executable:/usr/bin/redis-sentinel
config_file:/etc/redis-sentinel.conf
```

```
# Sentinel
sentinel_masters:2
sentinel_tilt:0
sentinel_running_scripts:0
sentinel_scripts_queue_length:0
sentinel_simulate_failure_flags:0
master0:name=TMS-REDIS2
status=ok,address=10.140.152.136:6379,slaves=1,sentinels=2
master1:name=TMS-REDIS2,status=ok,address=19
```

Redis Init Script

```
[Unit]
Description=Redis persistent key-value database
After=network.target

[Service]
ExecStart=/usr/bin/redis-server /etc/redis.conf --supervised systemd
ExecStop=/usr/libexec/redis-shutdown redis
Type=notify
User=redis
Group=redis
RuntimeDirectory=redis
RuntimeDirectoryMode=0755

[Install]
WantedBy=multi-user.target
```

Redis Sentinel Init Script

```
[Unit]
Description=Redis Sentinel
After=network.target


[Service]
ExecStart=/usr/bin/redis-sentinel /etc/redis-sentinel.conf --supervised systemd
ExecStop=/usr/libexec/redis-shutdown redis-sentinel
Type=notify
User=redis
Group=redis
RuntimeDirectory=redis
RuntimeDirectoryMode=0755

[Install]
WantedBy=multi-user.target
```

Note:
Permissions for redis configuration file should be **redis:root**
Permissions for redis-sentinel configuration file should be **redis:redis**
The working directory for both the Redis should be the same i.e **/var/lib/redis**

To test the redis performance use the below command

```
#redis-benchmark -h 10.140.152.136  -p 26379 -q -n 1000 -c 1000 -P 10000
PING_INLINE: 217.01 requests per second
PING_BULK: 503.52 requests per second
SET: 123.76 requests per second
GET: 152.93 requests per second
INCR: 138.54 requests per second
LPUSH: 123.66 requests per second
RPUSH: 133.92 requests per second
LPOP: 123.50 requests per second
RPOP: 136.17 requests per second
SADD: 129.92 requests per second
HSET: 100.85 requests per second
SPOP: 118.48 requests per second
LPUSH (needed to benchmark LRANGE): 157.46 requests per second
LRANGE_100 (first 100 elements): 131.42 requests per second
LRANGE_300 (first 300 elements): 112.26 requests per second
LRANGE_500 (first 450 elements): 134.01 requests per second
LRANGE_600 (first 600 elements): 115.63 requests per second
MSET (10 keys): 6.90 requests per second
```

3.5.4. Oracle Standalone Server Setup

JIO take care of this installation at their team end.

3.5.5. Security

3.5.5.1. CIS Security Checks

3.5.5.1.1. OS and Tomcat

- Cross Check on the Productions Servers for latest patches, CIS Hardening Scripts are executed and Kernel parameters at sysctl.conf, Ulimit and NTP. At least the referral script are executed - https://github.com/mattdoesinfosec/cis-audit-scripts/blob/master/cis_redhat7_check_formatted_public.sh
- Tomcat Harderning is as part of the Tomcat installations, it covers X-Frame-Options – to prevent clickjacking attack, X-XSS-Protection – to avoid cross-site scripting attack, X-Content-Type-Options – block content type sniffing, HSTS – add strict transport security, Domain name on Tomcat default virtual Host tag, Remove the tomcat version number in ServerInfo.properties

3.5.5.2. Enable Tomcat Security

Tomcat Configration covers the security. Any addition configuration made to be updated here.

3.5.5.3. Enable TLS Certificates

As per the discussion on 11/10/2018, TLS Termination will be on Network Load Balancers.

3.5.5.4. Enable nGinx Security

No SSL Security such as HSTS is not included in nGinx as SSL is not configured in this nGinx.

3.5.6. Benchmark Test

Testing commands are covered in the above sections.

Benchmark Results:

```
[jioappadm@NVMBD2AAG170V02 ~]$ ab -k -c 10 -n 10
https://tmsprod1.pos.jio.com/chatak-tms-services/
This is ApacheBench, Version 2.3 <$Revision: 1430300 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/

Benchmarking tmsprod1.pos.jio.com (be patient).....done


Server Software:        nginx
Server Hostname:        tmsprod1.pos.jio.com
Server Port:            443
SSL/TLS Protocol:       TLSv1.2,AES256-SHA,2048,256

Document Path:          /chatak-tms-services/
Document Length:        382 bytes

Concurrency Level:      10
Time taken for tests:   0.033 seconds
Complete requests:      10
Failed requests:        0
Write errors:           0
Keep-Alive requests:    10
Total transferred:      9470 bytes
HTML transferred:       3820 bytes
Requests per second:    307.45 [#/sec] (mean)
Time per request:       32.526 [ms] (mean)
Time per request:       3.253 [ms] (mean, across all concurrent requests)
Transfer rate:          284.33 [Kbytes/sec] received

Connection Times (ms)
              min  mean[+/-sd] median   max
Connect:        0    8   3.1      9      11
Processing:     4    7   2.2      7      12
Waiting:        4    7   2.2      7      12
Total:         12   15   2.3     16      19

Percentage of the requests served within a certain time (ms)
  50%     16
  66%     16
  75%     16
  80%     17
  90%     19
  95%     19
  98%     19
  99%     19
 100%     19 (longest request)
```

3.6. Application Deployment and Configuration

3.6.1. TMS (mPOS / TPOS) Deployment

Application Packages Updates are delivered in archive compressed format as shown in above table. Replace the WAR file into per application tomcat $CATALINA_HOME\webapps directory and delete the application's unpacked directory, and then restart Tomcat.

3.6.2. CDN Configuration

As per the environment at RIL, the CDN connectivity has been granted via RIL's properitery Proxy.

To make sure the Application is using the provided proxy of RIL, we need to provide the below configuration in bashrc

```
#.bashrc
# Source global definitions
   if [ -f /etc/bashrc ]; then
            . /etc/bashrc
    fi
https_proxy=https://jiomoneyproxy.rjil.ril.com:8080
```

The below line no_proxy is used so that other domains or IPs which doesn't require proxy can be bypassed

```
no_proxy="tmsprod1.pos.jio.com|49.204.88.100|sitohs.jio.com|websms.way2mint.com|sitbill.rpay.co.in|jiomoneysmtp.rjil.ril.com|jio-wes-poc.otlabs.fr|downloadprod1.pos.jiophone.net|localhost|127.0.0.1|10.*.*.*|NVMBD2ACQ90V03"
```

3.6.3. TMS Application Properties Configuration

Application resources path for each application properties are maintained under the resources folder.

Look for the below properties and add the appropreiate values. Refer the lines mark Orange.

Edit the file /App/tools/tms/resources/chatak-tms.properties

```
mail.smtp.starttls.enable=true
mail.smtp.ssl.trust=false
mail.smtp.quitwait=true
mail.smtp.auth=true
mail.smtp.host=jiomoneysmtp.rjil.ril.com
mail.smtp.port=25
mail.smtp.protocol=smtp
prepaid.user.email.token.expiry.time=2880
prepaid.from.email.id=developer.girmiti@jiomoney.com
prepaid.email.username=developer.girmiti@jiomoney.com
prepaid.email.password=
tms.otp.retry.count=4

# Email configuration settings ends here
#########################################################
#########################################################
#
scheduler.session.release.reminder.cron=0/10 * * * * ?
scheduler.session.release.scheduler.pool.size=10
scheduler.session.release.reminder.pool.size=10
scheduler.payout.reminder.cron=0 0 21 * * ?

#########################################################
#########################################################
#Redis Configuraion
#########################################################
#########################################################
redis.sentinelMasterName=TMS-REDIS2
redis.master.sentinel.host=10.140.151.164
redis.slave.sentinel.host=10.140.152.136
redis.master.sentinelport=26379
redis.slave.sentinelport=26379
redis.maxTotal=300
redis.maxIdle=25
redis.maxWaitMillis=30000
redis.minIdle=15
#########################################################
###################################
# OAuth2 Token Configuration
#########################################################
###################################
cw.mifare.oauth2.token.validity.seconds=1800

############## OAUTH configurations Start. username and password must be
changed to PRODUCTION
chatak.oauth.refresh.service.url=/secure/oauth/token?grant_type=refresh_token&refresh_t
oken=
chatak.wallet.oauth.service.url=/secure/oauth/token?grant_type=password&username=Cha
takWalletUser&password=ChatakWalletPass
chatak.wallet.client.id=ChatakWalletUser
chatak.wallet.client.secret=ChatakWalletPass
chatak.wallet.oauth.basic.auth.username=ChatakWalletBasicAuth
chatak.wallet.oauth.basic.auth.password=ChatakWallet@Secure
chatak.wallet.param.user.type=userType
chatak.wallet.user.type=CWS

#########################################################
#########################################################
#
# MPOS Service Configuration
mpos.service.endpoint.url=https://prodmoneyprofilemgmt.rjil.ril.com:10061/Services/Merc
hantInquiry_v1_0/OperationsEndpoint
mpos.service.mock.flag=false

#########################################################
#########################################################
#
# TSM Service Configuration
tsm.service.wallet.provider.id=NXP

#TSM Service Call
tsm.service.url=https://10.140.129.141:8080/v1/wallets/
tsm.service.notification.url=https://tmsprod1.pos.jio.com/chatak-tms-
services/tms/walletService/notification

#########################################################
#########################################################
#
# Reader Applet Id
reader.applet.id=A00000039654530000001F003000201
applet.keyVersion=90
applet.sequence.counter=1

# Application Version
nxp.tms.admin.deployed.version = Version3.5

# TMS MasterKeyManagement Configuration
tms.service.masterkey.max.device.counter=999900
tms.service.masterkey.max.device.version=FF

# Time expiration
tms.email.link.expiration.time.hours=48
tms.user.auto.unlock.time.hours=24

# HeartBeat Frequency
tms.heartBeat.frequency.value.seconds=86400

# OTP Retry count 0 to 4
tms.otp.retry.count=4

#Application Apk Store Path
chatak.tms.application.update.url.path=https://downloadprod1.pos.jiophone.net/apk/
chatak.tms.firmware.update.url.path=https://downloadprod1.pos.jiophone.net/firmware/
chatak.tms.l3sdk.update.url.path=https://downloadprod1.pos.jiophone.net/l3sdkApk/
chatak.tms.cap.update.url.path=https://downloadprod1.pos.jiophone.net/cap/
#Tomcat installation directory for CDN upload API.
#chatak.tms.tomcat.install.apk.directory=/webapps/Updates/apk/
#chatak.tms.tomcat.install.firmware.directory=/webapps/Updates/firmware/
#chatak.tms.tomcat.install.apk=/apk
#chatak.tms.tomcat.install.firmware=/firmware

chatak.tms.tomcat.install.apk.directory =/webapps/Updates/apk/
chatak.tms.tomcat.install.firmware.directory =/webapps/Updates/firmware/
chatak.tms.tomcat.install.l3sdk.directory =/webapps/Updates/l3sdkApk/
chatak.tms.tomcat.install.cap.directory =/webapps/Updates/cap/
chatak.tms.tomcat.install.apk=/apk
chatak.tms.tomcat.install.firmware=/firmware
chatak.tms.tomcat.install.l3sdk=/l3sdkApk
chatak.tms.tomcat.install.cap=/cap

#CDN Configuration
chatak.tms.cdn.user=posprod1
chatak.tms.cdn.key=jxbi2kPGwvbgXu3rRAiaU+zujJU2OKvpfWf7rGgEUUC4mutsL+m9Uj0W6
IZx/cFg
chatak.tms.cdn.netstorageURI=posprod-nsu.akamaihd.net/735191/girmiti
```

3.6.4. Troubleshoot

The below should be configured in catalina.sh so that always Application recognizes the Proxy:

```
JAVA_OPTS="$JAVA_OPTS -Djava.net.useSystemProxies=true -Dhttps.proxyPort=8080 -Dhttps.proxyHost=jiomoneyproxy.rjil.ril.com"
```

The below line should be configured in catalina.sh in case the DB connections have not been released and receiving connection reset error:

```
JAVA_OPTS="$JAVA_OPTS-
Djava.security.egd=file:/dev/../dev/urandom"
```

3.6.5. TMS Database Configuration

Once the Oracle 12c Database credentials received from JIO. On TMS Plaform Applications properties below changes to be made.

<jdbc configuration details here>

3.7. Application Test

3.7.1. Manual Test

3.7.2. Performance Test

3.8. Automation

3.8.1. Script to deployment

- Need to know the tool to which scripts has to created.
- Considering the Application deployment using playbook of ansible.
- Pre-requisites are defined above.
- The deployment will use the tomcat manager with credentials to deploy the files to all tomcat application
- Tomcat_check health check will help nGinx to identify the tomcat health route the traffic to active tomcat in the backend

3.9. High Availability Configurations and testing

3.9.1. nGinx Load Balancer with application servers

nGinx configuration above covers the the configuration parameters, the HA test result sets to update here

3.9.2. Redis Server sentinel with master/slave servers

Redis Server sentinel and Redis Server configuration with parameters are coverd above. HA test results sets to be update here.

3.9.3. Oracle Master with single slave servers

<jdbc setup and configure details here>

3.10. Centralized Log Management and Monitoring

<Log location and Logs snippet to be added here, so JIo can add them to the elastic search agent to stream the log data to ELK to visulize>

4. Reference

- https://tomcat.apache.org/download-80.cgi
- https://github.com/mattdoesinfosec/cis-audit-scripts/blob/master/cis_redhat7_check_formatted_public.sh