JBoss Tomcat Environment Build Standards_V1

JBoss WebServer New Environment Build Standards Draft

Important Information:
This is a controlled document and all content is required and must be compliant with disaster recovery guidelines for offline availability. Do not alter, remove or add any sections to this document. Do not embed documents within this document. Document approval requires that all applicable sections be completed. If a section does not apply, simply enter "Not Applicable".

Table of Contents

Apache Build for Tomcat

Objective:

This document contains information about build standards and naming conventions used when building out a Tomcat environment. It is useful to have this document readily available while working through all of the other steps involved in the build out.

Audience:

This document is intend to use by Middleware engineers (who has good understanding about Redhat Tomcat, Apache, AppDynamics etc., Other middleware products) in order to build the environment based on SAA/TAD.

Revision History:

05/11/2017	BK	Initial Version
05/15/2017	Sandy/David/Brad	Review
06/20/2017	Christopher	Review
06/21/2017	Christopher/Jan/Brent/Caleb	Review
06/22/2017	Sandy	Review
06/22/2017	Caleb	Review

Product List:

Jboss WebServer 3.x - AppServer
Jboss WebServer 3.x – HTTP Server
AppDynamics - Monitoring
Jenkins and Ansible - DevOps

Prerequisites

Supported/Licensed products will be installed and configured according to instructions within Middleware Technical Architecture Document. Alterations to standard Middleware shared environments will be discussed and implemented according to business needs and requirements. The standard Middleware shared environment discussed in this document offers a stable and supportable environment.
Pre-requisites that will need to be defined prior to build the environment includes are the following:

- Operating system and Platform:
- File system structure:
- Application requirements:
- Application account(s):
- Support roles:
- Monitoring
- Security
- Network
- Database
- Disaster Recovery
- MQ
- WebSeal
- JDK Version

Assumptions

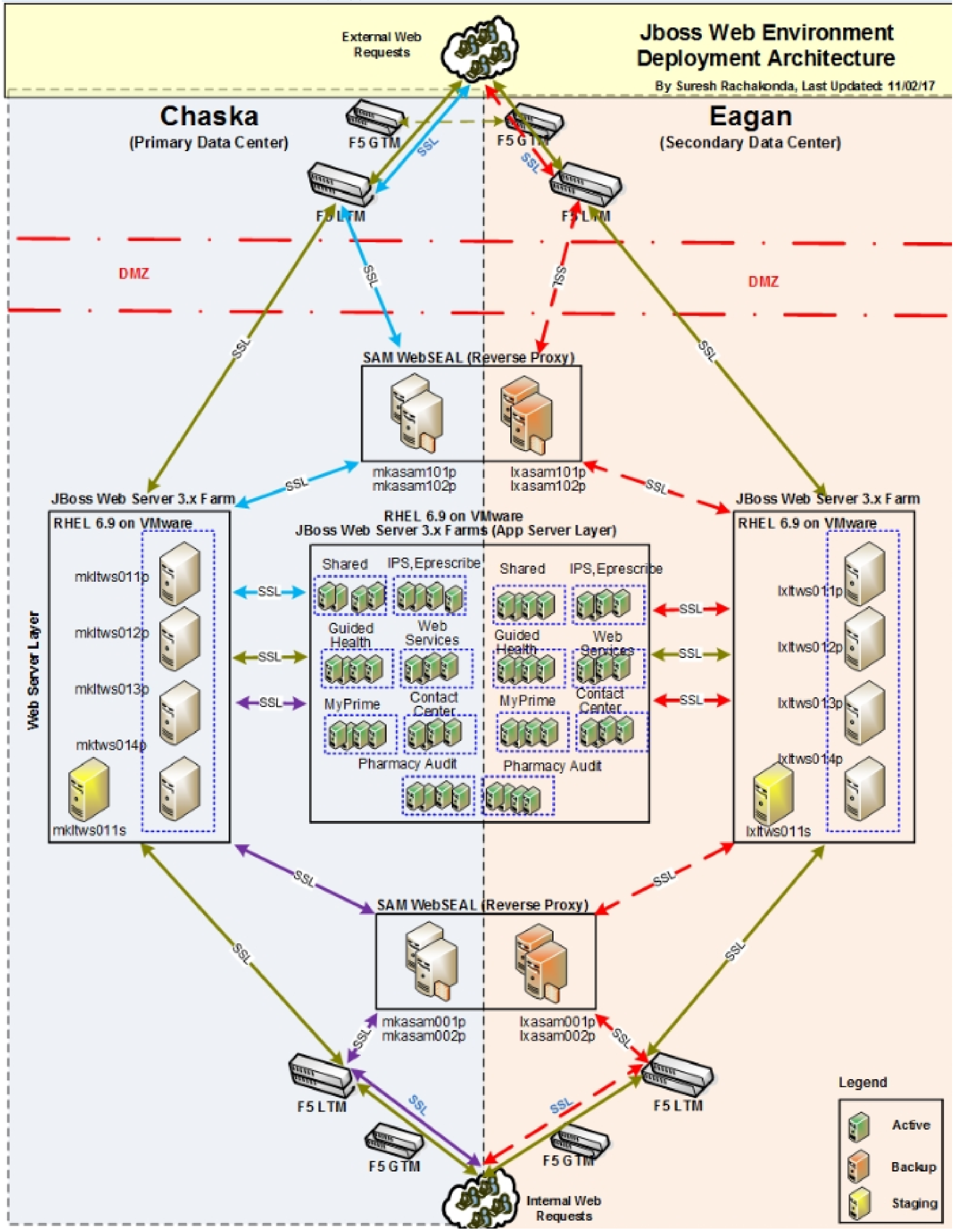
- Basic understanding of Jboss WebServer 3.x, AppDynamics, DevOps, RHEL, JDK and other Middleware tools.
- Ability to view scripts and log files.

- Understanding of Build and deployment process.
- Understanding of Prime Environments and Architecture

Architecture

We group the Tomcat applications among the Tomcat VM servers. We will be using Jboss webserver 3.x on Tomcat VM Servers in case of application layer and web layer.
Applications run on each data center in higher environments.

Out of Scope (not related to any customization configuration)
This tomcat container is not intended for any applications which need full Java JEE Container



Environment

Naming Standards

File System Name	Description
/opt/jboss	JBoss Tomcat FS
/opt/AppDynamics/	
	AppDynamics monitoring tools Agent install FS
/opt/jboss/logs	JWS Logs FS

Tomcat VM server name standard

In case of Eagan Data Center Tomcat VM name is lxltct**<env> and Chaska Data center Tomcat VM name is ckltct**<env>
The tomcat VM server number starts from 011 and refer below example for test tomcat env
lxltct011t
lxltct012t
lxltct013t
lxltct014t
lxltct015t
lxltct016t
lxltct017t
lxltct018t
lxltct019t
lxltct020t
lxltct021t
lxltct022t
lxltct023t
lxltct024t
The following are standards for determining how to name new components in the application container environment. The java service would be running on jboss service id
Application ID
Application IDs are the root naming element for all of the Tomcat application server components. They are arranged as follows:
<descriptor><instance number>
Where:

- *descriptor* is a short name for the application, preferably under 14 characters (i.e. "pharmacyworks", "msatools")
- "instance number" is a number starting at 01 that is incremented by 1 for each new instance for that application that is created in the same environment

Base Install Location:
/opt/jboss/
<Application ID>/(e.g. pharmacyworks01)
java/
jre1.8.0 -> jre1.8.0_*<xx>/*
jre1.8.0_*<xx>/*
Binary /opt/jboss/jws31/tomcat<version>/bin
Container /opt/jboss/jws31/applications/*<Application ID>*
If newer JWS version is used in future ie' jws3.2, the jws32 directory should be used under /opt/jboss

Application Properties Files

Application Properties files used for deployments should be under:
~~/opt/jboss/*<Application ID>*/properties/~~
Proposal
~~*/opt/jboss/appProperties/<Application ID>/properties/*~~
/opt/jboss/jws31/*properties/<Application ID>/*

The Secure Properties files should be under
Proposal
~~*/opt/jboss/appProperties/<Application ID>/secureproperties/*~~
/opt/jboss/jws31/*secureproperties/<Application ID>/*

The tomcat application and container logs
All Application and container logs will be going to /opt/jboss/logs/<Application ID>/

~~Library files(IBM MQ and Database etc.,)~~Libraries would be bundled in application during build /deployment?

~~/opt/jboss/jws31~~{-}/lib/mqlib/<version>/ ------~~-Directory for MQ library files~~
~~/opt/jboss/jws31/lib/dblib/iseriesdb2/<version>/ ----- Directory for ISeriesDB2 Driver files~~
~~/opt/jboss/jws31/lib/dblib/pseriesdb2/<version>/~~--- ~~Directory for PSeriesDB2 Driver files~~
~~/opt/jboss/jws31/lib/dblib/mssql/<version>/ ----- Directory for Microsoft SQL Driver files~~
~~/opt/jboss/jws31~~{-}/lib/dblib/oracle/<version>/ ----~~-Directory for Oracle Driver files~~

1. **a.** **Application NAS Mounts**Should scripts be managed as ansible deployed packages instead of a common mount point?

Default server mounts that should exist on Middleware systems

~~/nas/depot~~ Redhat Satellite/Nexus is repository for binaries ?

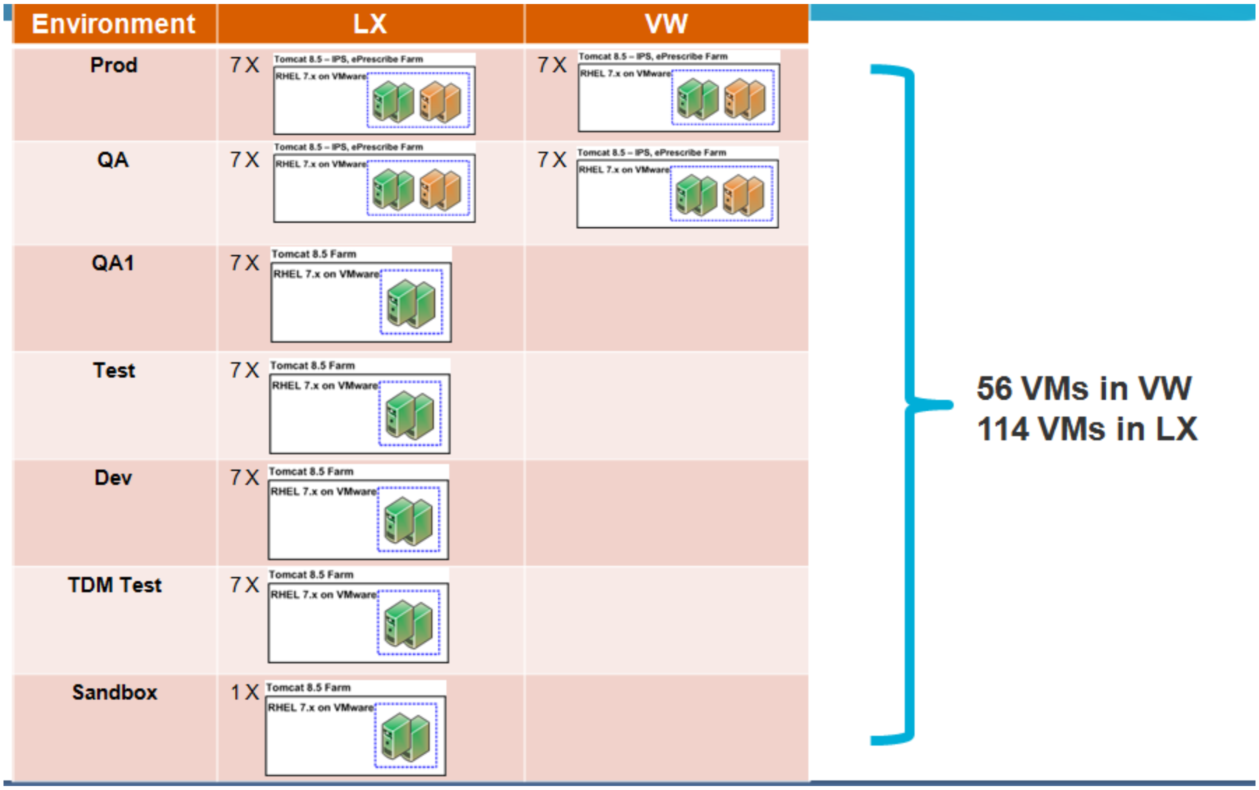
/nas/serveradmin for netcool client ?

Logging Standards

Samba shares or logging tools will be used for both Application and tomcat container logs.
Application logs –
Container logs –

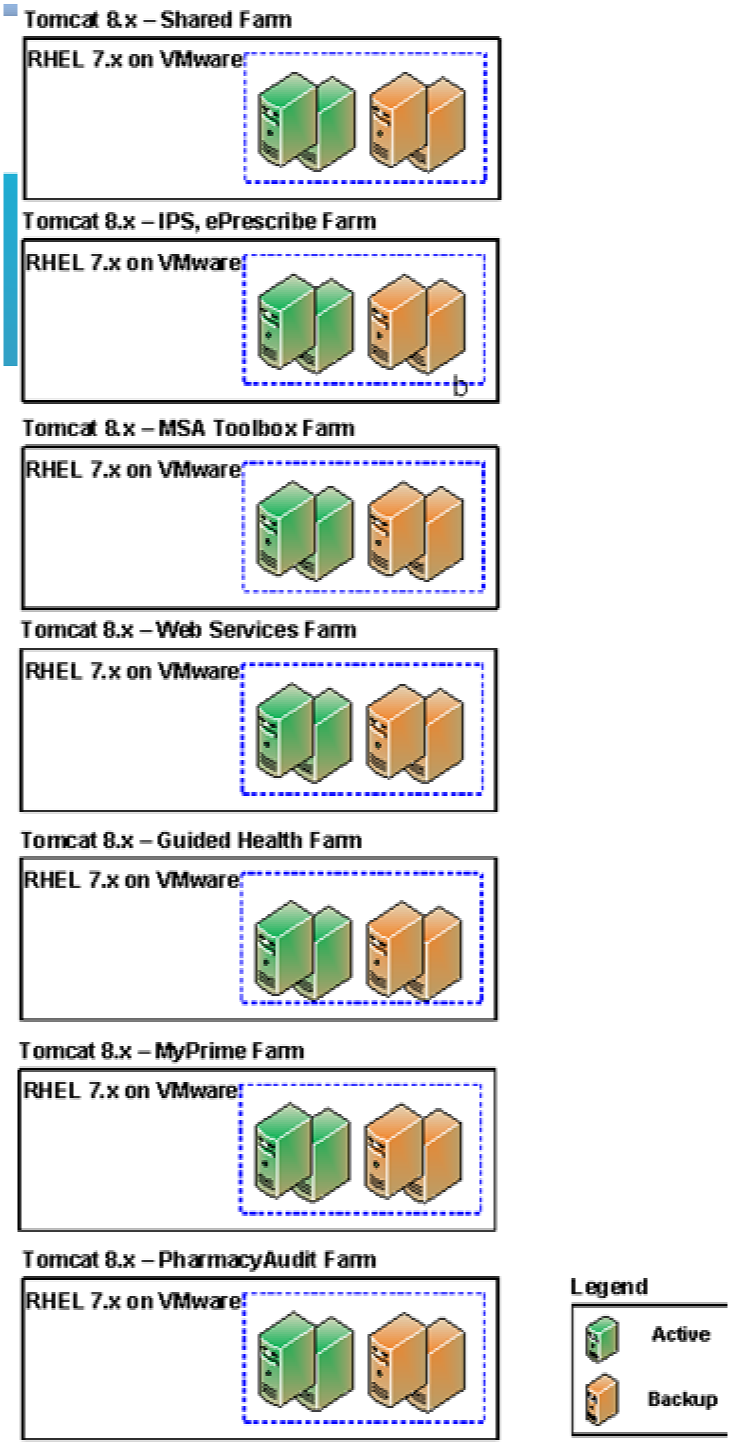
1. **a.** Ports

We got following application groups among Tomcat VM servers.



Environment	LX	VW
Prod	7 X Tomcat 8.5 – IPS, ePrescribe Farm RHEL 7.x on VMware	7 X Tomcat 8.5 – IPS, ePrescribe Farm RHEL 7.x on VMware
QA	7 X Tomcat 8.5 – IPS, ePrescribe Farm RHEL 7.x on VMware	7 X Tomcat 8.5 – IPS, ePrescribe Farm RHEL 7.x on VMware
QA1	7 X Tomcat 8.5 Farm RHEL 7.x on VMware	
Test	7 X Tomcat 8.5 Farm RHEL 7.x on VMware	
Dev	7 X Tomcat 8.5 Farm RHEL 7.x on VMware	
TDM Test	7 X Tomcat 8.5 Farm RHEL 7.x on VMware	
Sandbox	1 X Tomcat 8.5 Farm RHEL 7.x on VMware	

56 VMs in VW
114 VMs in LX

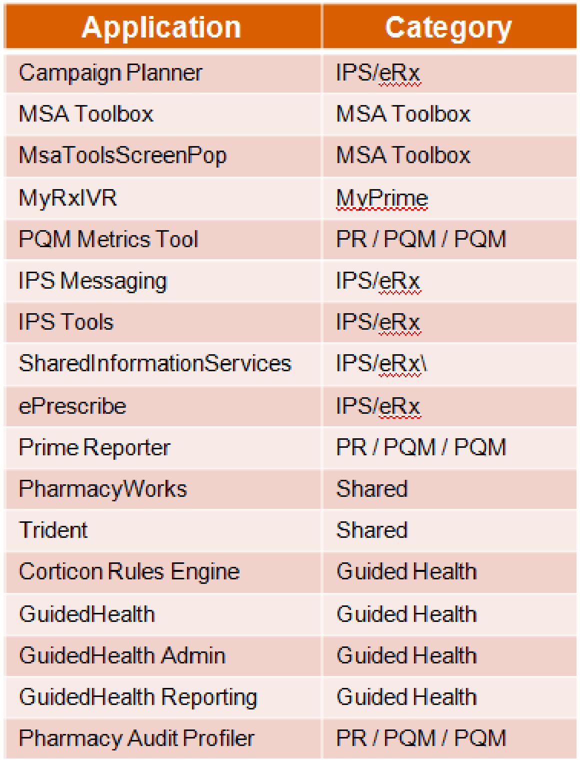


Tomcat 8.x – Shared Farm
RHEL 7.x on VMware
Tomcat 8.x – IPS, ePrescribe Farm
RHEL 7.x on VMware
Tomcat 8.x – MSA Toolbox Farm
RHEL 7.x on VMware
Tomcat 8.x – Web Services Farm
RHEL 7.x on VMware
Tomcat 8.x – Guided Health Farm
RHEL 7.x on VMware
Tomcat 8.x – MyPrime Farm
RHEL 7.x on VMware
Tomcat 8.x – PharmacyAudit Farm
RHEL 7.x on VMware
Legend
Active
Backup

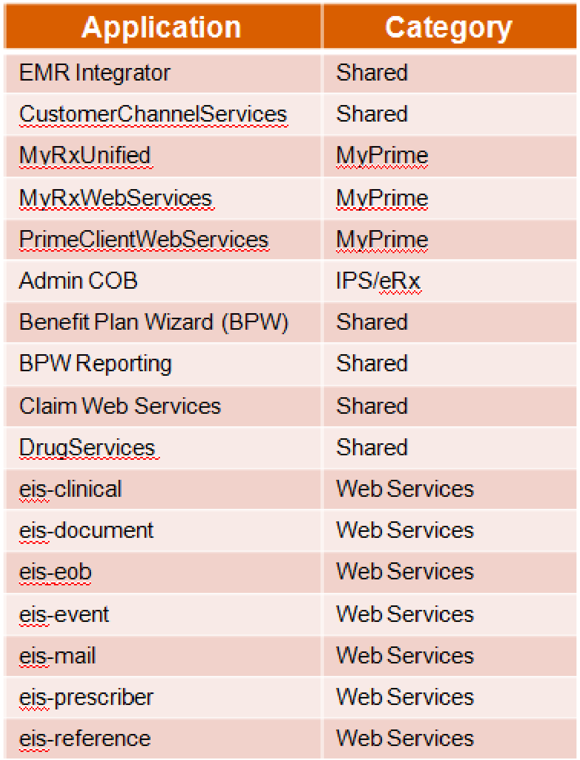
In case of Prod, Application grouping Vs Tomcat VM Servers as follows

Environment	Farm Name	ServerNames	
		Chaska Data Center	Eagan Data Center
Prod	Shared	mkltct011p	lxltct011p
		mkltct012p	lxltct012p
		mkltct013p	lxltct013p
		mkltct014p	lxltct014p
	IPS,Eprescribe	mkltct015p	lxltct015p
		mkltct016p	lxltct016p
		mkltct017p	lxltct017p

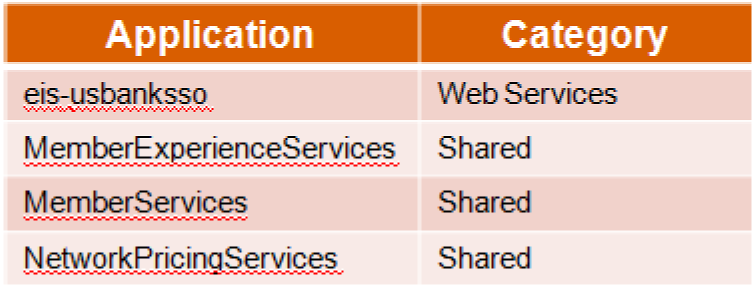
		mkltct018p	lxltct018p
	Contact Center	mkltct019p	lxltct019p
		mkltct020p	lxltct020p
		mkltct021p	lxltct021p
		mkltct022p	lxltct022p
	WebServices	mkltct023p	lxltct023p
		mkltct024p	lxltct024p
		mkltct025p	lxltct025p
		mkltct026p	lxltct026p
	Guided Health	mkltct027p	lxltct027p
		mkltct028p	lxltct028p
		mkltct029p	lxltct029p
		mkltct030p	lxltct030p
	MyPrime	mkltct031p	lxltct031p
		mkltct032p	lxltct032p
		mkltct033p	lxltct033p
		mkltct034p	lxltct034p
	PharmacyAudit	mkltct035p	lxltct035p
		mkltct036p	lxltct036p
		mkltct037p	lxltct037p
		mkltct038p	lxltct038p



Application	Category
Campaign Planner	IPS/eRx
MSA Toolbox	MSA Toolbox
MsaToolsScreenPop	MSA Toolbox
MyRxIVR	MyPrime
PQM Metrics Tool	PR / PQM / PQM
IPS Messaging	IPS/eRx
IPS Tools	IPS/eRx
SharedInformationServices	IPS/eRx\
ePrescribe	IPS/eRx
Prime Reporter	PR / PQM / PQM
PharmacyWorks	Shared
Trident	Shared
Corticon Rules Engine	Guided Health
GuidedHealth	Guided Health
GuidedHealth Admin	Guided Health
GuidedHealth Reporting	Guided Health
Pharmacy Audit Profiler	PR / PQM / PQM



Application	Category
EMR Integrator	Shared
CustomerChannelServices	Shared
MyRxUnified	MyPrime
MyRxWebServices	MyPrime
PrimeClientWebServices	MyPrime
Admin COB	IPS/eRx
Benefit Plan Wizard (BPW)	Shared
BPW Reporting	Shared
Claim Web Services	Shared
DrugServices	Shared
eis-clinical	Web Services
eis-document	Web Services
eis-eob	Web Services
eis-event	Web Services
eis-mail	Web Services
eis-prescriber	Web Services
eis-reference	Web Services



Application	Category
eis-usbanksso	Web Services
MemberExperienceServices	Shared
MemberServices	Shared
NetworkPricingServices	Shared

Each Tomcat farm will have a range of 200 ports assigned to it. Of the 200 ports the following port ranges will be defined for use by tomcat instance in each farm:
100 – 109 for use by first Tomcat Instance
Port 100 will be assigned to Server Port
Port 101 will be assigned to non SSL HTTP Connector
Port 102 will be assigned to SSL HTTP Connector
Port 103-109 will be assigned to application if it needs any additional port
100 – 109 <Application ID descriptor>01 (first instance of Tomcat Container on a Tomcat VM)
110 – 119 <Application ID descriptor>02 (second instance of Tomcat Container on a Tomcat VM)
120 – 129 <Application ID descriptor>03 (third instance of Tomcat Container on a Tomcat VM)
The port ranges will start at 10,000 and increment by 200 for each tomcat farm after the first.
Example for the first tomcat farm:
10000 – 10009 <Application ID descriptor>01 (first instance of Tomcat Container on a Tomcat VM)
10010 – 10019 <Application ID descriptor>02 (second instance of Tomcat Container on a Tomcat VM)
10020 – 10029 <Application ID descriptor>03 (third instance of Tomcat Container on a Tomcat VM)
The second tomcat farm would be the same as above but ports would start at 10200.
Revise description of port reservations.Use confluence or wiki to maintain ports info for each farm and applications.

1. a. Certifications

Internal CA should issue host based cert and middleware should automate cert renewal
We keep certificates in below keystore files:

Keystore - /opt/jboss/jws31/keystores/keystore
TrustStore - /opt/jboss/jws31/keystores/truststore
We should use SHA2 cert
~~Common Keystore~~
~~Keystore - /opt/tomcat/keystore/.keystore~~
~~TrustStore - /opt/tomcat/keystore/.truststore~~
The application certs should goto cacerts in Java path as we donot keep truststore entry in setenv.sh file due to security reasons.

1. a. Security

The application should be using dedicated service account at LDAP side and use same in tomcat side if application needs LDAP for role based authentication.The appdev should request for service account at LDAP side if they do not have one already. We should not use middleware LDAP service account at tomcat side for any of tomcat applications.
LDAP must be configured with ssl port(636) and ldap cert needs to be added into truststore
We should use below SHA2 LDAP F5 vip
usmnd01-sldap.primetherapeutics.com – Chaska –This F5 vip is only for Chaska
usmnd02-sldap.primetherapeutics.com – Lexington- This F5 vip is only for Lexington
prime-sldap.primetherapeutics.com – This F5 vip is common for Chaska and Lexington
The LDAP SHA2 certs are available in below path
J:\Technology\Documentation\Middleware\WAS 8.5\Planning Documentation\LDAPSHA2Cert

1. a. File System Security and JBoss role managementInsert reference to Security document.

1. a. Monitoring

Current Monitoring standards for an application will be implemented with each tomcat container being instrumented with the Monitoring client within the container config file.
The AppDynamics agent will be installed by using Jenkins to orchestrate ansible scripts and tomcat service account should be a member of the appdynamics gateway group and team group.

1. a. Startup Script

The tomcat base rc.d/init.d script should be linked to specific run level directories on Tomcat VM node. Hence java processes come up automatically when Tomcat VM Server gets rebooted as part of scheduled or unscheduled outage.
Middleware startup should be kept in /opt/jboss/Prime/init.d/

1. a. Maintenance ScriptsWould maintence scripts be candidates for implementation as an ansible script?

Have scripts to archive container, application logs and clear old logs which are 45 days old in backup log folder on each tomcat VM node. The container logs should be rotated in daily basis by using script.
The heap dump and core dump files which are 5 days old should be cleaned if we see any
Additional maintenance script should be added if any
List of Maintenance scripts are

- stopAllservers
- startAllServers
- stop/startindividualServers
- notificationonexpiringcertsinTruststore
- backupconfig- needed ?
- Archive logs and clear old logs
- Detect Headdump and Coredump
- synchronizeStaticContent
- listenerPortsWatchdog
- medispanImageCopier(Weekly Medispan Image Updates)

1. a. CyberArkInsert reference to security standards.

CyberArk is the third party tool to store service account used within Prime Therapeutics. Security standards for handling of service accounts should be followed.

1. a. AutomationThis section could be impacted by discussion from [CJL4].

Build Automation:
The new tomcat instance will build through Jenkins and Ansible tower build & deploy tool.
Operations and Maintenance Automation: (Need discussion on this area)
Currently using scripts for start/stop/patching …etc
Application Build & Deploy:
Jenkins will be used for application deployment. Nexus will be used as repository to keep binaries.

1. a. Reverse Proxy Hardening

IP whitelisting at Webserver side
TAI intercepter config and Setup

1. a. PCI Remediation

Secure HTTP cookies
Disable sslv3 TSL1.0

1. a. Forum Sentry

Research mutual authentication configuration for outbound calls to forum Sentry

1. a. Dynamic outbound call for webservice calls

1. a. Performance Tuning

Web container Threadpool,dataSource connection pool,JMS connection pool tune-up,heap size etc.,
Webcontainer setting change if any

1. a. Ulimit Settings

Keep number of files count as 65000 and nproc count as 10000 at starting point. We will increase them based on load test result if needed.
Apache Build for Tomcat

Prerequisites

Make sure we got correct apache libraries on a webserver VM

Naming Standards

File System Name	Description
/opt/httpd/logs/	Apache access and Error logs
/opt/AppDynamics	AppDynamics agent install
/opt	Apache install FS

Apache WebServer Installation

The Jboss webserver should be installed based on instructions from Redhat vendor by using Jenkins and Ansible tower. We will be using Jboss webserver 3.x on Tomcat VM Servers in case of web layer. The httpd service uses user id **apache** and root user hands over httpd process to apache user id once httpd service starts with root user. We should switch user to apache user id if needed.

WebServer Server Config File	/opt/httpd/conf/httpd.confShould we have a conf file in conf.d for each Application ID descriptor or each Application ID? or
WebServer DocumentRoot path	/var/www/html/*<Application ID>*

Httpd Configuration File

It should be using NameVirtualhost and virtual host section should be created for each application url with RewriteCondition,documentroot,log file names.

Some virtualhost section should be having SSLEnable and SSLClientAuth entries depends upon application setup which requires SSL.

we should keep SSLCiperSpec entries in the required virtual host section of application url based on PCI remediation.

Maintenance script

We should discuss the script (ansible vs shell script) and automation framework (Jenkins?).

Have scripts to take backup and upload webserver logs on each webserver. The apache webservers should be having scripts for system down, system up and recycle tomcat apache webserver to handle RxClaim and ISeries switch etc.,

Traffic routing for application deployment

Archiving webserver logs

Purging logs older than 45 days

System down,system up page setup

Recycle apache service