Collaborative Terminology Tooling & Data Management   
(CTT & DM)

Tooling and Server Development

Deployment and Installation Guide



November 2016

Department of Veterans Affairs

Office of Information and Technology (OI&T)

**Revision History**

| Date | Version | Description | Author |
| --- | --- | --- | --- |
|  | 1.0 | Delivery to VA | ManTech Mission Solutions & Services |
| 10/31/2016 | 0.3 | Updated Document to Address TW Comments | C. Cuestas, ManTech Mission Solutions & Services |
| 10/28/2016 | 0.2 | Technical Writer Review – Draft Edits | B. Stanley, ManTech Mission Solutions & Services |
| 10/27/2016 | 0.1 | Initial Draft | C. Cuestas, ManTech Mission Solutions & Services |

Table of Contents

[1 Introduction 1](#_Toc468265155)

[1.1 Purpose 1](#_Toc468265156)

[1.2 Dependencies 1](#_Toc468265157)

[1.3 Constraints 2](#_Toc468265158)

[1.4 Roles and Responsibilities 2](#_Toc468265159)

[*2* Deployment 3](#_Toc468265160)

[2.1 Timeline 3](#_Toc468265161)

[2.2 Site Readiness Assessment 3](#_Toc468265162)

[2.2.1 Deployment Topology (Targeted Architecture) 4](#_Toc468265163)

[2.2.2 Site Preparation 5](#_Toc468265164)

[2.3 Resources 5](#_Toc468265165)

[2.3.1 Facility Specifics 5](#_Toc468265166)

[2.3.2 Hardware 5](#_Toc468265167)

[2.3.3 Software 5](#_Toc468265168)

[2.3.4 Communications 6](#_Toc468265169)

[3 Installation 6](#_Toc468265170)

[3.1 Pre-installation and System Requirements 6](#_Toc468265171)

[3.2 Platform Installation and Preparation 6](#_Toc468265172)

[*3.3* Download and Extract Files 6](#_Toc468265173)

[3.4 Database Creation 6](#_Toc468265174)

[3.5 Installation Scripts 6](#_Toc468265175)

[3.6 Cron Scripts 6](#_Toc468265176)

[3.7 Access Requirements and Skills Needed for the Installation 7](#_Toc468265177)

[3.8 Installation Procedure 7](#_Toc468265178)

[3.8.1 JAVA 7](#_Toc468265179)

[3.8.2 SSL CertsToJDK 7](#_Toc468265180)

[3.8.3 CSR and Certificate 8](#_Toc468265181)

[3.8.4 TOMCAT 9](#_Toc468265182)

[3.8.5 GitBlit 10](#_Toc468265183)

[3.8.6 Prisme 11](#_Toc468265184)

[3.8.7 Jenkins 11](#_Toc468265185)

[3.8.8 Maven 12](#_Toc468265186)

[3.8.9 Nexus 12](#_Toc468265187)

[3.8.10 Komet 13](#_Toc468265188)

[3.8.11 Single Sign On – Internal 15](#_Toc468265189)

[3.9 Installation Verification Procedure 16](#_Toc468265190)

[3.10 System Configuration 16](#_Toc468265191)

[3.11 Database Tuning 17](#_Toc468265192)

[4 Back-Out Procedure 17](#_Toc468265193)

[4.1 Back-Out Strategy 17](#_Toc468265194)

[4.2 Back-Out Considerations 17](#_Toc468265195)

[4.2.1 Load Testing 17](#_Toc468265196)

[4.2.2 User Acceptance Testing 17](#_Toc468265197)

[4.3 Back-Out Criteria 17](#_Toc468265198)

[4.4 Back-Out Risks 17](#_Toc468265199)

[4.5 Authority for Back-Out 17](#_Toc468265200)

[4.6 Back-Out Procedure 17](#_Toc468265201)

[4.7 Back-out Verification Procedure 18](#_Toc468265202)

[5 Rollback Procedure 18](#_Toc468265203)

[5.1 Rollback Considerations 18](#_Toc468265204)

[5.2 Rollback Criteria 18](#_Toc468265205)

[5.3 Rollback Risks 18](#_Toc468265206)

[5.4 Authority for Rollback 18](#_Toc468265207)

[5.5 Rollback Procedure 18](#_Toc468265208)

[5.6 Rollback Verification Procedure 18](#_Toc468265209)

# Introduction

This document describes how to deploy and install the CTT & DM system as well as how to back-out the product and rollback to a previous version or data set. This document is a companion to the project charter and management plan for this effort. The scope of the ETS project is to develop new product that provides the capability to create and edit VHAT and other terminology map sets for consumption by other VA services. The technology stack provides the capability to:

* Develop an integrated web-accessible Terminology Management Platform (TMP) that supports terminology development, maintenance, and distribution across VA. The platform will be built on existing open source tools and frameworks such as the International Health Terminology Standards Development Organization (IHTSDO) workbench and Informatics Architecture Acceleration (ISAAC) editor.
* Deploy the TMP (ETS tooling and server solution) in various environments including production and pre-production.
* Provide operations and maintenance support for TMP development and deployment.
* Provide support for production operations, production performance improvements, and portal framework.
* Create and deploy patches to VistA systems to integrate authoritative terminology content into VistA in a native format.
* Enable computability of VA health and benefits services clinical data through semantic interoperability to exchange clinical data between VA (VHA, VBA, NCA), DoD, and approved non-VA entities. (Clinical data will be natively coded and mapped to national standards and terminologies.)

## Purpose

The purpose of this plan is to provide a single, common document describing how, when, where, and to whom the CTT & DM system will be deployed and installed as well as how it is to be backed out and rolled back if necessary. The plan also identifies the resources, communications plan, and rollout schedule. Specific instructions for installation, back-out, and rollback are included in this document.

## Dependencies

* The CTT&DM tool requires a series of open source technologies to run underneath it. These technologies are: Tomcat, Apache Webserver, SSL, Jenkins, GitBlit, Nexus and Maven.
* An assigned Systems Administrator will install the required software. PRISME and KOMET may be installed after the required software installation is complete.
* This document is part of the deliverables package.

## Constraints

Servers in Pre Prod and Prod at AITC have the following configuration:

* 16GB of RAM
* 64GB x 1 🡪 HD1– OS
* 472GB x 1 🡪 HD2 - data
* 4 x CPUs

## Roles and Responsibilities

The list below identifies the individuals responsible for the system’s deployment, configuration, and administration.

Table : Deployment, Installation, Back-out, and Rollback Roles

| **Name** | **Team** | **Role** |
| --- | --- | --- |
| Esigie Aguele | ManTech | Program Manager |
| Dan Armbrust | ManTech | Lead Engineer/Developer |
| Claudio Cuestas | ManTech | Sr. Systems Administrator |
| Derrick Allen | VA Team | Project Manager |
| Victor Ramirez | VA Team | Sr. Systems Administrator |

The list below identifies specific responsibilities of each team member.

Table : Deployment, Installation, Back-out, and Rollback Responsibilities

| ID | Team | Phase / Role | Tasks | Project Phase (See Schedule) |
| --- | --- | --- | --- | --- |
|  | Claudio Cuestas (ManTech) and Victor Ramirez (VA Team) | Deployment | Plan and schedule deployment (including orchestration with vendors) |  |
|  | Claudio Cuestas (ManTech) and Victor Ramirez (VA Team) | Deployment | Determine and document the roles and responsibilities of those involved in the deployment. |  |
|  | Claudio Cuestas (ManTech) and Victor Ramirez (VA Team) | Deployment | Deploy and configure procedure and provide installation package. |  |
|  | Claudio Cuestas (ManTech) |  | Oversee and assist during the installation in pre-prod and prod. |  |
|  | Claudio Cuestas (ManTech) and Victor Ramirez (VA Team) | Deployment | Test for operational readiness |  |
|  | Victor Ramirez (VA Team) | Deployment | Execute deployment |  |
|  | Victor Ramirez (VA Team) | Installation | Plan and schedule installation |  |
|  | Victor Ramirez (VA Team) | Installation | Ensure authority to operate and that certificate authority security documentation is in place |  |
|  | Victor Ramirez (VA Team) | Installation | Validate through facility POC to ensure that IT equipment has been accepted using asset inventory processes |  |
|  | Derrick Allen (VA Team) | Installations | Coordinate training |  |
|  | N/A | Back-out | Confirm availability of back-out instructions and back-out strategy (what are the criteria that trigger a back-out) |  |
|  | Derrick Allen (VA Team) | Post Deployment | Hardware, Software and System Support |  |

Once the approval process and certifications are complete, the Project and Program Managers will indicate the starting deployment time.

# Deployment

This application deployment is dependent on a series of open source services/packages that must be installed, configured and running.

We detailed this process below in section 3.8.

## Timeline

TBD

## Site Readiness Assessment

* The application will be deployed on servers hosted at the AITC Datacenter in the pre-production and production environments.

The applications will be installed across multiple servers in these two environments.

* The new application is Collaborative Terminology Tooling and Data Management software.
* The application will be installed and deployed on the following server in AITC.  
  The server list below:
  + DNS

### Deployment Topology (Targeted Architecture)

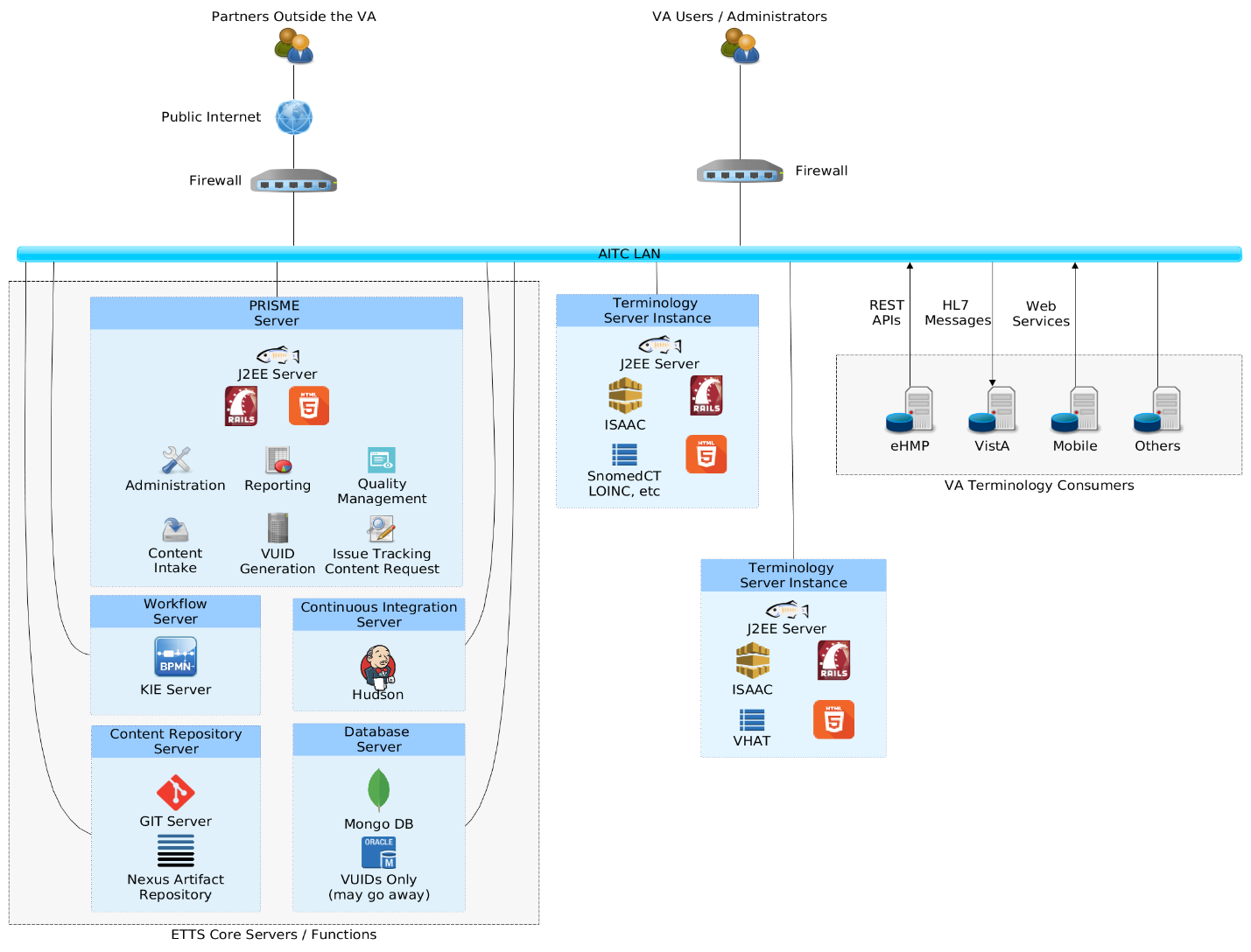


Figure : Deployment Topology

The deployment location is pre-production and production servers at AITC

### Site Preparation

N/A

## Resources

### Facility Specifics

N/A

### Hardware

The following table describes hardware specifications required at each site prior to deployment.

Table : Hardware specifications

| Required Hardware | Model | Version | Configuration | Manufacturer | Other |
| --- | --- | --- | --- | --- | --- |
| Server |  | CentOS6.8 | 16GB RAM, 1x HD 64GB and 1 x HD 472GB, 4 x CPUs |  |  |
| Server |  | CentOS6.8 | 16GB RAM, 1x HD 64GB and 1 x HD 2100GB, 4 x CPUs |  |  |

Please see the Roles and Responsibilities table in Section 1.4 for details about who is responsible for preparing the site to meet these hardware specifications.

The hardware has already been procured and running on the network.

### Software

The following table describes software specifications required at each site prior to deployment.

Table : Software specifications

| Required Software | Make | Version | Configuration | Manufacturer | Other |
| --- | --- | --- | --- | --- | --- |
| Tomcat | Apache | 8.0.33 |  |  |  |
| WebServer | Apache | 2.2.15 |  |  |  |
| JDK | Oracle | 8.9.1 |  |  |  |
| Gitblit |  |  |  |  |  |
| Jenkins | Hudson | 2.19.1 |  |  |  |
| Maven | Apache | 3.3.9 |  |  |  |
| Nexus | Sonatype | 2.14.0 |  |  |  |
| SSL Certs | VA Provider |  |  |  |  |

Please see the Roles and Responsibilities table in Section 1.4 above for details about who is responsible for preparing the site to meet these software specifications.

### Communications

For inquiries related to deployment, configuration, management, and error handling of these applications, contact Dan Armbrust at [PII](mailto:PII) and/or Claudio Cuestas <PII>

#### Deployment/Installation/Back-Out Checklist

N/A

# Installation

## Pre-installation and System Requirements

All the hardware is in place at AITC and ready to receive the installation.

## Platform Installation and Preparation

All the hardware is in place at AITC and ready to receive the installation.

## Download and Extract Files

Our deployment package includes all necessary software.

## Database Creation

The Oracle databases and accounts have already been created and are ready for use.

## Installation Scripts

See section 4.8 for details.

## Cron Scripts

N/A

## Access Requirements and Skills Needed for the Installation

The Systems Administrator executing the deployment will have elevated access to each system in pre-production and production systems.

## Installation Procedure

Use this document to install and configure the following services:

* Java
* SSL Certificate
* Tomcat Server
* GitBlit
* Maven
* Jenkins
* Nexus
* Prisme
* Komet
* Single Sign On

The provided serverSetup.zip file contains a “cert” directory with all of the Internal, Intermediate and Root SSL Certificates.

There is also an “installers” directory where you can find Java, Tomcat, Maven, GitBlit and other scripts that will help during the installation process.

### JAVA

From the root directory “ / ” unzip the provided serverSetup.tar.gz file containing the Java RPM, set the appropriate permissions and install it.

Assuming that the serverSetup.tar.gz file has been placed in servers /tmp directory.

cd /

tar –zxvf /tmp/serverSetup.tar.gz

As root run the following:

/app/installers/installjava.sh

### SSL CertsToJDK

This will install the CA Root and Intermediate Certificates to the JDK version just installed in the previous step.

As root run the following:

/app/installers/installsslcert.sh

You will be asked the following question three times, one for each certificate:

“Trust this certificate?”

Respond “yes”

### CSR and Certificate

This step requires the use of **keytool** and **openssl** to generate the CSR and the certificate chain required for SSL to be properly set up.

-Generate a CSR (Certificate Signing Request)

Update the CN (Common Name, which is the Fully Qualified Server Name) to have the right hostname.

cd /app/certs/

openssl req -new -newkey rsa:2048 -nodes -keyout **server.key** -out server.csr -subj "DNSDNS/emailAddress=PII"

#### View the CSR

The openssl tool will allow us to view the contents of the CSR.

Once Generated, the contents of the CSR should look like the following:

openssl req -text -noout -verify -in **server.csr**

verify OK

Certificate Request:

Data:

Version: 0 (0x0)

Subject: C=US, ST=TX, L=Austin, O=VA, OU=STS, CN=DNS/emailAddress=PII

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

#### CSR Submission

Please submit the CSR **server.key** via the following URLs:

http://DNS/

https://DNS

#### Create Certificate Chain

When fulfilled, put the certificate into a **server.crt** file.

ensure that your .crt file starts with

-----BEGIN CERTIFICATE-----

and ends with

-----END CERTIFICATE-----

Now we export the certificate from the **server.crt** file you recently created and the keystore file that was used to generate the CSR **server.key** into a new pkcs12 file called **server.p12** together with the VA’s Internal Certficate named **VA-Internal-E5-ICA1-v1.crt**

openssl pkcs12 -export -in **server.crt** -inkey **server.key** **-out server.p12** -name tomcat -CAfile **VA-Internal-E5-ICA1-v1.crt** -caname root

(password - tomcat)

Then we import the **server.p12** file into a new keystore file called **server.keystore**

This **server.keystore** file will be used to configure apache and tomcat to support SSL.

keytool -importkeystore -deststorepass tomcat -destkeystore **server.keystore** -srckeystore **server.p12** -srcstoretype PKCS12 -srcstorepass tomcat -alias tomcat

Place the server.keystore file in the “/app/certs” directory and set the appropriate permissions.

sudo chown root /app/certs/server.keystore

sudo chmod 700 /app/certs/server.keystore

To view the contents of the keystore file: keytool –list –v –keystore server.keystore

### TOMCAT

From the root directory “/app“ unzip the provided tomcat file as part of the original serverSetup.zip file. Become root on the server, unzip the tomcat file and run the “finishTomcatSetup.sh” script to install and configure tomcat.

sudo su -

cd /app

yum –y install unzip

unzip installers/apache-tomcat-8.0.33.zip

./installers/finishTomcatSetup.sh

#### Configure SSL in Tomcat

Verify that the 8080 connector for SSL is in place.

in the file /app/apache-tomcat-8.0.33/conf/server.xml”

<Connector port="8080" protocol="org.apache.coyote.http11.Http11NioProtocol"

maxThreads="150" SSLEnabled="true" scheme="https" secure="true"

clientAuth="false" sslProtocol="TLS"

keystoreFile="/app/certs/server.keystore" keystorePass="tomcat"

maxPostSize="209715200"/>

<!-- Define an AJP 1.3 Connector on port 8009 -->

<Connector port="8009" protocol="AJP/1.3" redirectPort="8080" />

### GitBlit

#### Deploy and Configure

Run /app/installer/installgit.sh to create the directory and set up proper ownership. It will also deploy the application in Tomcat

Define new Git data directory in context.xml

edit /app/apache-tomcat-8.0.33/conf/context.xml - add: (towards end of file inside the Context tags)

<Environment name="baseFolder" type="java.lang.String" value="/app/gitData" override="false" />

#### Install Tomcat’s startup script

cp /app/etc/init.d/tomcat” to “/etc/init.d/”

The server running Tomcat must be able to run it with an Xmx of 14GB

This can be tuned in /etc/init.d/tomcat

#### Bring up Tomcat

/etc/init.d/tomcat start

Tail the logs to check Tomcat coming up and to spot any possible issues

tail –f /app/apache-tomcat-8.0.33/logs/catalina.out

Finally,

Edit /app/gitData/defaults.properties – add the following at the end of the file:

web.enableRpcServlet=true

web.enableRpcManagement=true

web.enableRpcAdministration=true

Restart Tomcat /etc/init.d/tomcat restart

Login to gitblit with admin/admin - create a new account and delete default account

Replace the “ServerName” with the actual fully qualified hostname.

https://hostname.domainname:8080/git/

Remember the new admin account you created (for later configuration)

Create the following Repositories:

With Access Policy: “Restrict Push (Named)

[contentConfigurations](https://vaausdbsctt700.aac.va.gov:8080/git/summary/contentConfigurations.git)

editChangesets

### Prisme

#### Deploy and Configure

Execute the following:

/app/installers/installprisme.sh

cd /app/prismeData

make sure the server\_config.yml and oracle\_database.yml files are present.

Rename the file accordingly:

PreProd

mv /app/prismeData/oracle\_database.yml-PRE/app/prismeData/oracle\_database.yml

mv /app/prismeData/server\_config.yml-PRE /app/prismeData/server\_config.ymlmv /app/prismeData/oracle\_database.yml-PROD /app/prismeData/oracle\_database.yml

mv /app/prismeData/server\_config.yml-PROD /app/prismeData/server\_config.yml

Start Tomcat

sudo /etc/init.d/tomcat start

### Jenkins

#### Install and Configure

We are going to install the Jenkins repo first and install the RPM via yum.

As Root run the following:

/app/installers/installjenkins.sh

If a ssh key is needed, this is the manual process of generating one.

############################

# sudo -u jenkins ssh-keygen

That will generate the key for you here:

/var/lib/jenkins/.ssh/id\_rsa.pub

##############################

/etc/init.d/Jenkins start

Replace the “ServerName” with the actual fully qualified hostname.

Go to <https://ServerName:8080/jenkins>

Log In with the following credentials devtest/devtesthardtoguess

Go to Configure / look for Jenkins Location and change the Jenkins URL to :

https://ServerName:8080/jenkins

Replace the “ServerName” with the actual fully qualified hostname.

Click Apply and Save

### Maven

#### Install and Configure

**Maven must be installed on the same server as Jenkins.**

Become root on the server, and run the following:

/app/installers/installmaven.sh

Edit /app/jenkinsMavenSettings.xml file and add the servername and credentials for nexus.

### Nexus

#### Install and Configure

As Root run the following:

/app/installers/installnexus.sh

Add the following into “/app/nexus-2.14.0-01/bin/jsw/conf/wrapper.conf”

vi /app/nexus-2.14.0-01/bin/jsw/conf/wrapper.conf

wrapper.app.parameter.3=./conf/jetty-https.xml

wrapper.app.parameter.4=./conf/jetty-http-redirect-to-https.xml

To set up SSL, use the existing keystore “server.keystore” but rename it accordingly and set ownership.

cp /app/certs/server.keystore /app/certs/nexus.keystore

chown nexus /app/certs/nexus.keystore

chgrp nexus /app/certs/nexus.keystore

Set the SSL port in “/app/nexus-2.14.0-01/conf/nexus.properties”

vi /app/nexus-2.14.0-01/conf/nexus.properties

application-port-ssl=8443

Configure “jetty-https.xml” to specify keystore

change /app/nexus-2.13.0-01/conf/jetty-https.xml to like this:

<Set name="keyStore">/app/certs/nexus.keystore</Set>

<Set name="trustStore">/app/certs/nexus.keystore</Set>

<Set name="keyStorePassword">tomcat</Set>

<Set name="keyManagerPassword">tomcat</Set>

<Set name="trustStorePassword">tomcat</Set>

Start Nexus, log in and configure via the GUI.

/etc/init.d/nexus start

Go to https://YourServerName:8080/nexus/

login (admin/admin123), update permissions, disable unneeded repositories

Create "termdata" release repo

disable apache snapshots, disable / delete 3rd party, disable m1 shadow

update 'public' group to match repos

### Komet

Komet is installed 100% via the Prisme UI.

Log in to prisme http://YourHostName:8080/

Once in, Click on “App Deployer”

Select the application type “Komet Tooling Deployment” and click “Next”

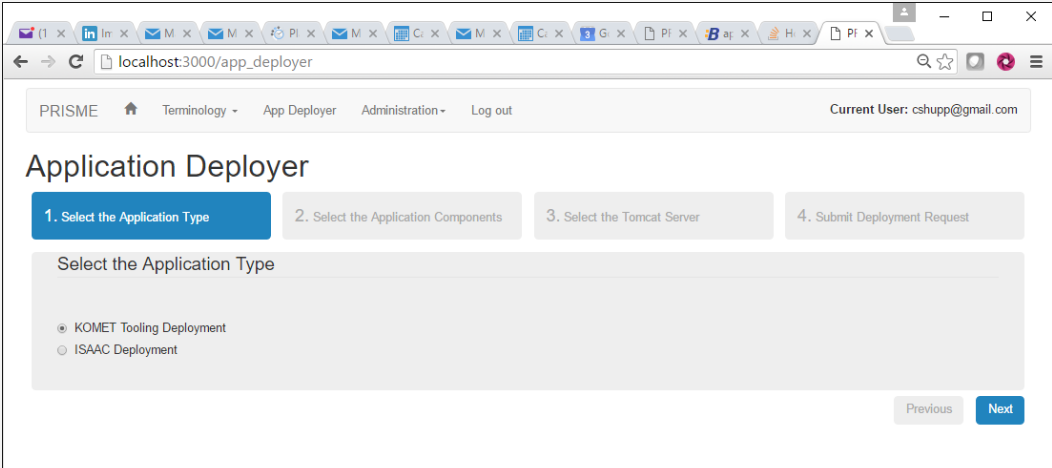


Figure : Application Deployer Application Type Screen

Then, select the application component(s) “Tomcat Application Server: Isaac-rest” and click “Next”

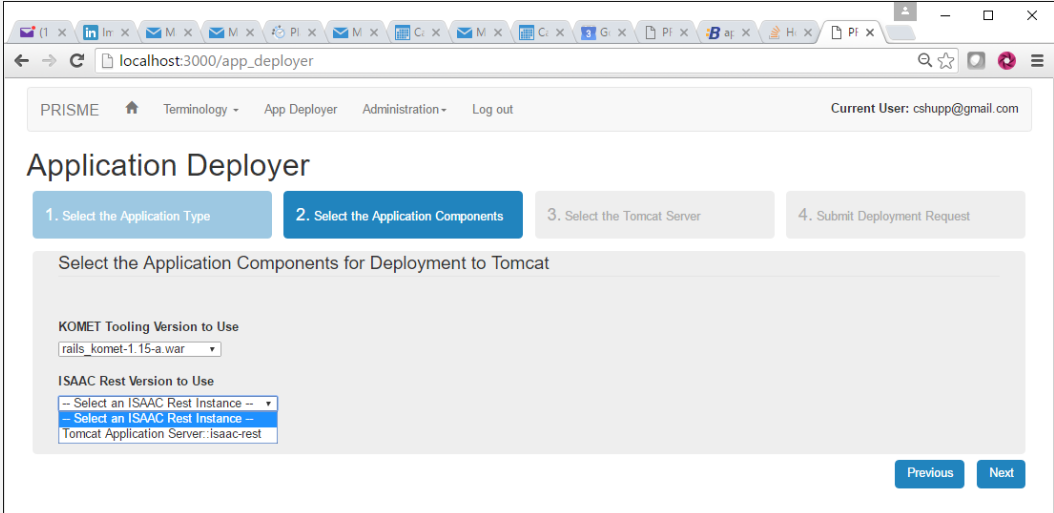


Figure : Application Components for Deployment to Tomcat

Then, select the tomcat server “Tomcat localhost” and click “Next”

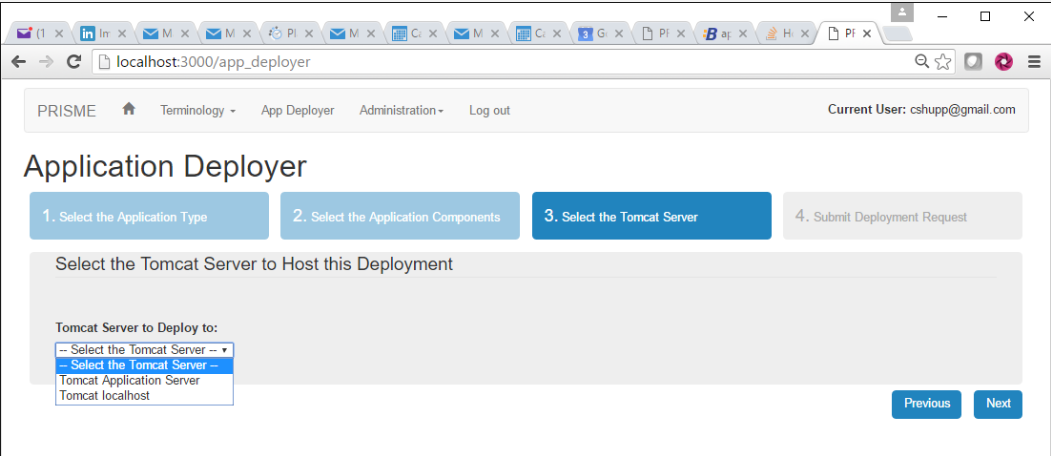


Figure : Application Deployer Tomcat Host Server

Lastly, review and submit the “Deployment Request” and click “Finish”

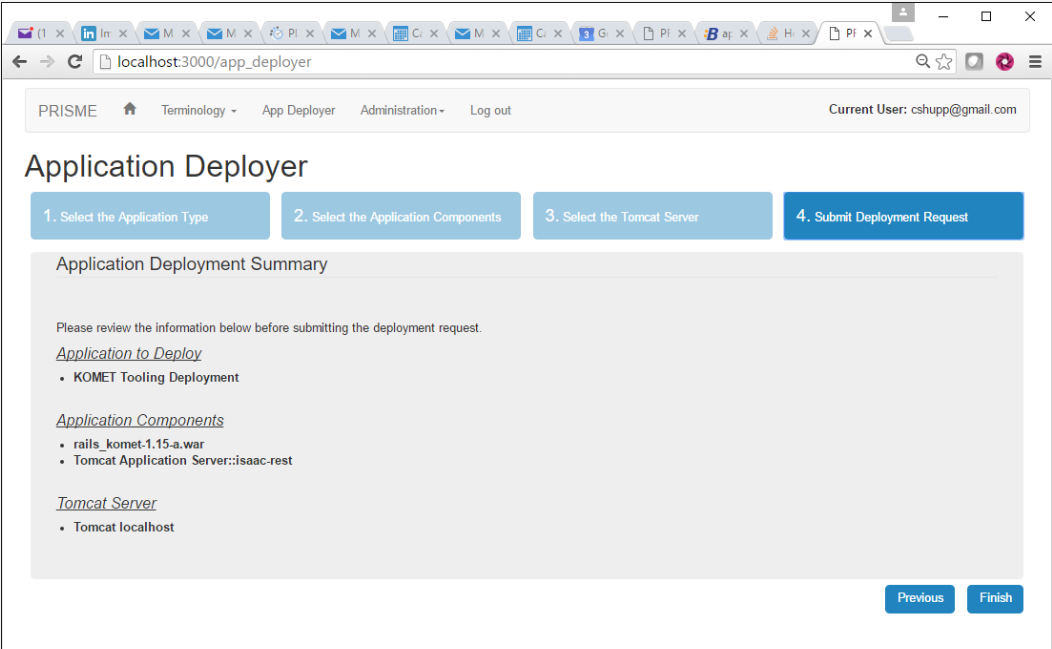


Figure : Application Deployment Summary

### Single Sign On – Internal

There are 2 main components for SSOi:

Siteminder webagent and Apache webserver.

Apache is already installed on servers in pre-prod and prod.

If it is not installed, please run as root:

yum –y install httpd

Once httpd is installed, the siteminder for SSOi webagent must be sourced in the Apache start up script.

vi /etc/init.d/httpd

# Source function library.

. /app/CA/webagent/ca\_wa\_env.sh

Run the following command to extract and copy all the necessary files.

This will also set the proper file permissions and ownership

app/installers/installssoi.sh

Copy the correct ssl.conf file to /etc/httpd/conf.d

cp app/installers/apache\_extensions/ssl.conf-PRE /etc/httpd/conf.d/ssl.conf

cp app/installers/apache\_extensions/ssl.conf-PROD /etc/httpd/conf.d/ssl.conf

There will be updated ssl.conf files for both PreProd and Prod containing the ability to deploy multiple instances of isaac-rest as well as komet in a single tomcat server.

With this changes we have also updated the server\_config.yml file that was initially installed as per in section 3.8.6.1 of this manual.

**Install SSOi webagent**

Refer To siteminder webagent installation document

## Installation Verification Procedure

To verify the installation access each system URL

*Replace the “ServerName” with the actual fully qualified hostname.*

Tomcat

[DNS](https://DNS)

[DNS](https://DNS)

<https://DNS>

Git

[DNS](https://DNS)

[DNS](https://DNS)

[DNS](https://DNS)

## System Configuration

System configuration is detailed in the installation section. No added configuration needed.

## Database Tuning

N/A

# Back-Out Procedure

The operation is not currently working on legacy applications. A manual back-up process for creating and editing terminology is available. As a result, the back-out strategy for CTT\_DM Release 2 (R2) is to turn off the application if necessary to address issues. A back out procedure will be provided for Release 3.

## Back-Out Strategy

The AITC will follow established communications procedures and turn off the application if necessary.

## Back-Out Considerations

In the absence of legacy application, all “Go/No-Go” decisions regarding deployment and installation in production will be made during final functionality testing in pre-production.

### Load Testing

TBD. This information is expected by November 30, 2016.

### User Acceptance Testing

TBD. This information is expected by December 09, 2016.

## Back-Out Criteria

Back-out criteria would include a critical data error discovered under approval by the COR and VA PM.

## Back-Out Risks

Slower operations in processing terminology updates has been identified as a back-out risk.

## Authority for Back-Out

Alan Arnold, COR, is the back-out authority for this project.

## Back-Out Procedure

Currently the back-out procedure is to turn the system off. A back-out procedure will be provided with Release 3.

## Back-out Verification Procedure

In the event of a back-out, the team will verify the presence of an application landing page informing that the system is not currently available.

# Rollback Procedure

N/A

## Rollback Considerations

N/A

## Rollback Criteria

N/A

## Rollback Risks

N/A

## Authority for Rollback

N/A

## Rollback Procedure

N/A

## Rollback Verification Procedure

N/A

Template Revision History

| Date | Version | Description | Author |
| --- | --- | --- | --- |
| March 2016 | 2.2 | Changed the title from Installation, Back-Out, and Rollback Guide to Deployment and Installation Guide, with the understanding that Back-Out and Rollback belong with Installation. | VIP Team |
| February 2016 | 2.1 | Changed title from Installation, Back-Out, and Rollback Plan to Installation, Back-Out, and Rollback Guide as recommended by OI&T Documentation Standards Committee | OI&T Documentation Standards Committee |
| December 2015 | 2.0 | The OI&T Documentation Standards Committee merged the existing *“Installation, Back-Out, Rollback Plan”* template with the content requirements in the OI&T End-user Documentation Standards for a more comprehensive Installation Plan. | OI&T Documentation Standards Committee |
| February 2015 | 1.0 | Initial Draft | Lifecycle and Release Management |