This procedure is used to setup an Amazon Web Service (AWS) Elastic Compute Cloud (EC2) Windows instance that is configured to run the META application. It is assumed that the reader has an account on <https://meta-arrow.signin.aws.amazon.com/console>. It also assumes that a Linux instance has been setup per the META Cloud Linux Procedure and is currently running.

**Setup security group: Open up Instance TCP ports for connection**

In the EC2 tab of the AWS site, select the Security Groups link located in the left pane.

You can create a new security group by pressing the create security button and

Complete the procedure by filling in the name, description. Keep the default for the VPC, which is “no VPC”.

Select the Default security group or the new security group that was created earlier. The details should display below

Select the Inbound tab

Enter a Custom TCP Rule for port 22 (SSH), 80 (HTTP), 5900, 5901 (VNC), 3389(RDP). For each port, enter the port number in the Port Range field, leave the Source as 0.0.0.0/0 for each and select Add Rule.

After entering the TCP rules, select Apply Rule Changes.

**Create an EC2 Instance**

In the EC2 tab of the AWS site, select the Instances link located in the left pane

Select the Launch Instance button

Microsoft Windows Server 2008 R2 Base (AMI Id: ami-1cbd4475)

Microsoft Windows 2008 R2 SP1 Datacenter edition and 64-bit architecture.

Root Device Size: 35 GB.

In the Instance Type drop down, select Large (m1.large), then select Continue

In the Availability Zone, select Zone: us-east-1c and then select Continue.

In the next window (Advanced Instance Options), select Continue

In the next window (Add tags to your instance), select Continue

The next window is Key Pairs window. If you haven’t created a Key Pair in the past, you either need to create one or choose an existing one from the drop down list and get the actual key file from someone else.

To create a Key Pair, select the associated radio button

Enter a key name (e.g., your username)

Select Create and Download your key

Store the resulting key file (e.g., username.pem) to known location (e.g., c:\keys\meta)

In the next window (Security Groups), select default groups or the new security group, and select create.

In the next window (Review Settings), select Launch

**Create and attach an EBS volume (i.e. hard drive space) to Instance**

In the EC2 tab of the AWS site, select the Volumes link located in the left pane

Select the Create Volume button in the EBS Volumes pane

In the Create Volume window, enter a Size: 80 GB and Availability Zone: us-east-1c

Select Yes, Create. The new volume should show in the list of volumes

Right-click on the new volume and select Attach Volume

In the Attach Volume window select the Instance ID of the instance that you want to connect to

Enter a “xvdf” for the device and continue.

**Retrieve initial Administrator password**

Ensure that the instance key (e.g., c:\keys\meta\username.pem) is available on your laptop

In the EC2 tab of the AWS site, select the Instances link located in the left pane

Right-click on the Windows instance and select to retrieve the windows password

Follow directions for browsing to and copying in contents of the key file

Record the username and password in a safe place

**create key pair.**

Ensure that the instance key (e.g., c:\keys\meta\username.pem) is available on your laptop

In the EC2 tab of the AWS site, select the key pairs link located in the left pane.

Add a new key pair by pressing the “create key pair” button.

Follow the direction to save the <keypair name>.pem file to your client laptop.

Record the username and password in a safe place

The password generation may sometimes take over 30 minutes. Wait at least 15 minutes, before retrieving the windows password.

Right-click on the Windows instance and select to retrieve the windows password

**Remote login to Windows instance from Linux instance and setup accounts**

*Note: outgoing Remote Desktop Protocol (RDP) connections are not allowed from the BAE network. This procedure works around this restriction by using the Linux instance to RDP to the Windows instance. Once an SSH daemon is established on the Windows instance, an RDP connection from the BAE network can be established over an SSH tunnel.*

Establish a VNC connection to the Linux instance and login as <username>. *Note, details for this step are provided in the META Cloud Linux Procedure in Section Configure VNC.*

Remote login to the Windows instance using the command rdesktop –g 80% <Windows instance> (e.g., rdesktop –g 80% ec2-184-72-153-142.compute-1.amazonaws.com)

Login as Administrator using the retrieved password

Select the Start menu, and then in the Search Programs field, enter “user accounts”

Select Change password, and then change the retrieved Administrator password to something meaningful

In a similar fashion, select Manage another account, select Create a new account, and then create a new user account with password

Goto the system properties from the control panel and select the Remote tab

Make sure allow connections from computer running any version of RD is selected and then

Press the select users button.

Press the add button and enter the name of the <user>.

Press the check names button, which will find the qualified name of the user.

Press OK.

Logout of Instance and verify ability to login to user account as <user>

**Format the EBS volume**

*Note: it seems that the volume is usable without following these steps. But the AWS website says to do it and it doesn’t hurt anything.*

Remote login to the Windows instance as Administrator

Select the Start menu, and then select Run

Enter diskmgmt.msc

In the Disk Management window, right-click on D: and select Format

**Configure Internet Explorer (IE)**

*Note: the initial security settings for IE on the Instance are very restrictive, requiring constant manual intervention; this section loosens them to the level that exists on the client’s computer*

On client computer, startup IE, and then navigate to Tools->Internet Options -> Security -> Custom level

Remote login to the Windows instance as the user, startup IE, and navigate to Tools->Internet Options -> Security -> Custom level

Change the settings of IE on the remote computer to match those on the client computer

**Download Cygwin**

Remote login to the Windows instance as the user

Start IE and navigate to [www.cygwin.com](http://www.cygwin.com)

Select the Cygwin DLL link (e.g., Cygwin DLL 1.7.9-1)

Save it to D:\, and then run it

Select Download from internet

Set Root directory to D:\cygwin

Set local package directory (e.g., D:\cygwinLocalPackage)

Select “http://gatech.edu” as the download site

Select to install everything except games and X11. Double check that the desired components are set to “Install” by expanding each and verifying its subcomponents are set to “Install”

The installation will take an hour or two

**Configure SSH Daemon**

Remote login to the Windows instance as the Administrator

Create system environmental variable CYGWIN with value ntsec tty

Append ;d:\cygwin\bin to the system PATH variable

Open Cygwin shell windows as Administrator (i.e., right-click and select Run as administrator)

Enter the following commands:

chmod +r /etc/passwd

chmod u+w /etc/passwd

chmod +r /etc/group

chmod u+w /etc/group

chmod 755 /var

touch /var/log/sshd.log

chmod 664 /var/log/sshd.log

Enter the command ssh-host-config

Enter Yes to each Yes/No question

When prompted for the value of CYGWIN, enter ntsec tty

When prompted for a different server name than cyg\_server, answer Yes, and then enter sshd. Reenter this name when prompted to do so.

Set the password for sshd to something familiar (e.g., Meta1$)

Enter the command cyglsa-config

Enter Yes to each Yes/No question

The Windows instance will automatically reboot

Remote login to the Windows instance as the Administrator

Open Cygwin shell windows as Administrator (i.e., right-click and select Run as administrator)

Open the file /usr/bin/rebaseall in an editor. Locate line 110 which should begin with the text “sed –e ‘cygwin1\.dll$/d’”.

Insert “-e ‘\=/sys-root/mingw/bin=d’ ” between “sed “ and “-e”. then save the changed file

Enter the command ash

Enter the command /usr/bin/rebaseall

Set password for sshd account to something familiar (e.g., Meta1$) using the command passwd sshd

From the Start menu, enter services in the Search programs and in the Services window, locate the CYGWIN sshd service and double click it to open its properties

Under the Log On tab, select Local System account. Leave the checkbox blank

Under the General tab, press Start to begin the service. It should start without error

Make sure that every account has a password. This is necessary for sshd to work

If you are still unable to start the sshd and if the following error is observed:

if the “/var/empty must be owned by root and not ….”

in the /var/sshd.log,

Change ownership of /var/empty with

chown SYSTEM empty

return to the services and start the CYGWIN sshd

Enter the following commands to synchronize the Windows user accounts with Cygwin

mkpasswd –cl > /etc/passwd

mkgroup –l > /etc/group

Verify local connection to cygwin by opening up a Cygwin shell on the Windows instance and entering the command ssh <username>@127.0.0.1 or ssh localhost. In either case, the Cygwin hippo should display

**Configure the Firewall to allow external SSH and HTTP connections**

Remote login to the Windows instance as the Administrator

From the Start menu, enter Firewall in the Search programs and files field, and then select Windows Firewall w/ Advanced Security

Right-click on the Inbound Rules and select New Rule

Select Port, and then Next

Enter 22 for Specific local ports, and then Next

Select Allow the connection, and then Next.

Leave all selections checked and give a name for this rule(for example sshd-port-22) . Press Finish.

The new rule should show up at the top of the list, active and ready.

Repeat the above steps to setup an inbound rule for ports 80 and 8080.

**Configure SSH and RDP connections on Client computer**

In a Cygwin window on your laptop, cd to /home/<username>/.ssh

Create or edit the config file under .ssh

Add the following lines to the config file. The Public DNS is provided in the EC2 Instance details (e.g., ec2-50-17-74-76.compute-1.amazonaws.com). The LocalForward line allows for Remote Desktop connection. The RemoteForward allows for access to the Magic Draw license server.

Host admin

User administrator

HostName <Instance’s Public DNS>

LocalForward 3390 localhost:3389

RemoteForward 10000 boundry.alphatech.com:11011

Host user

User <user account’s username>

HostName <Instance’s Public DNS>

LocalForward 3390 localhost:3389

RemoteForward 10000 boundry.alphatech.com:11011

Windows 7 clients fails to remote desktop over the port 3390. Use the following configuration

Host admin

User administrator

HostName <Instance’s Public DNS>

LocalForward 5029 localhost:3389

RemoteForward 10000 boundry.alphatech.com:11011

Host user

User <user account’s username>

HostName <Instance’s Public DNS>

LocalForward 5029 localhost:3389

RemoteForward 10000 boundry.alphatech.com:11011

Navigate to key folder (e.g., cd /cygdrive/c/keys/meta)

Verify ability to connect via ssh as Administrator and User using the config file (e.g., ssh -i <key name>.pem admin and ssh -i <key name>.pem user)

Disconnect existing ssh connections and then connect via ssh as Administrator

On the client computer, select Start->All Programs->Accessories->Communications->Remote Desktop Connection

In the Remote Desktop Connection window, select the Display tab and click on the slider. Set the dimensions equal to the Client computers display dimensions. *Note, the Full Screen setting doesn’t always give a full screen, sometimes the dimensions have to match*

In the General tab, enter localhost:3390(windows xp) or 5029(windows 7) for Computer, and then select Connect. A remote desktop window to the Windows instance should display

Login as Administrator, select Start, right-click Computer, and select Manage

In the Server Manager window, navigate to Configuration->Local Users and Groups->Groups

Double-click the Remote Desktop Users group and add the user account to the group

Logoff the Windows instance

Disconnect existing ssh connections and then reconnect to the user account

Verify that a connection can be established again via Remote Desktop. *Note, this verifies that the a Remote Desktop connection works over a ssh connection established with the user account*

Note: Windows 7 clients will see windows security box pop up. Enter the password to authenticate the username. If an error is encountered while validating the remote windows instance, press yes to continue with the connection.

**Install development tools**

The tools are available for download from the Meta Deployment shared folder on Karl Fischer’s laptop gldlkwf1. You can map a local drive to gldlkwf1\Meta Deployment for easy access. All tools but Magic Draw (MD) can alternatively be downloaded from the Web. To copy a file from a client computer to the Instance (or back), you can use Secure Copy (SCP). To do so, it is convenient to navigate to the keys directory (e.g., cd /cygdrive/c/keys/meta). The syntax for the command will be as follows:

scp –i <key file>.pem <source file path> <username>@<Instance Public DNS>:<destination file path> (e.g., scp –i meta.pem hello.txt root@ec2-50-17-171-124.comput-1.amazonaws.com:/home/kwf)

Copy the development tool installation packages, identified below, to the Instance using the scp command

Use Remote Desktop to log into the Instance as Administrator

Install the following development tools using the actions specified for each tool.

jdk-6u22-windows-x64.exe – double-click and follow installation directions to install in default location

clisp-2.44-win32-mingw-big-install.exe – double-click and follow installation directions to install in default location

apache-maven-3.0.3.zip – unzip to c:\Program Files

apache-ant-1.8.2.zip - unzip to c:\Program Files

MD\_UML\_170\_sp1\_win64.exe - double-click and follow installation directions to install in default location. In the Shortcuts installation window, select Create icon for all users. After installation, right-click the installation folder and select properties. In the Security tab, select Users, select Edit, and then grant Full control permissions. *Note, users need this access to add plug-ins.*

Startup Magic Draw UML via the desktop Start menu button. Select to look for updates and install any Magic Draw service packs. Exit out of the program and then restart it. Got to the Help menu and select Resource/Plugin Manager, and then select to install any SysML service packs. Exit out of the program to ensure updates are in place for next time

springsource-tool-suite-2.6.1.RELEASE-e3.6.2-win32-x86\_64-installer.exe -double-click and follow installation directions to install in default location. After installation, right-click the installation folder and select properties. In the Security tab, select Users, select Edit, and then grant Full control permissions. *Note, users need this access to store meta data*

TortoiseSVN-1.6.15.21042-x64-svn-1.6.16.msi -double-click and follow installation directions to install in default location

Use Internet Explorer to find and download the latest version of FireFox, and then install it

Add the following system environmental variables

MDUML\_HOME = C:\Program Files\MagicDraw UML

JAVA\_HOME = C:\Program Files\Java\jdk1.6.0\_22

M2\_HOME = C:\Program Files\apache-maven-3.0.3

ANT\_HOME = C:\Program Files\apache-ant-1.8.2

Update the PATH system environmental variable as follows

PATH = %JAVA\_HOME%\bin;%M2\_HOME%\bin;%ANT\_HOME%\bin;<existing PATH>

Reboot the instance to ensure the environmental variables are set

Use Remote Desktop to log into the Instance as a user

Open a Command window

Enter the command java –version and verify the correct version of Java is referenced

Enter the command mvn –version and verify the correct version of Maven is referenced

Enter the command ant –version and verify the correct version of Ant is referenced

**Configure and Run ARRoW Menu and Magic Draw**

Use Remote Desktop to log into the Instance as a user

Navigate to d:\

Checkout the META trunk to d:\trunk using Tortoise (via Explorer) or SVN (via Cygwin command) using the URL: svn+ssh://<username>@cvsext.ait.na.baesystems.com/proj/meta/svn/trunk. *Note, the checkout takes a couple hours*

Navigate to trunk/arrow-mvn-init

Enter mvn install

Navigate to trunk/ArrowManualArtifacts

Enter mvn install

Navigate to trunk/arrow-mvn-all

Enter mvn install

Navigate to trunk/mdplugin

Enter mvn install

Navigate to trunk/ArrowWebServices

Enter mvn tomcat:run to run on port 8080. If you want to run on port 80, add the parameter “-Dmaven.tomcat.port=80”

Start the FireFox web browser

Enter the address <http://localhost/ArrowWebServices/index.html>

The ARRoW menu window should display

Startup Magic Draw UML via the desktop Start menu button

Follow Magic Draw directions to connect to the server

**Configure and Component Model Library (CML)**

Establish a SSH connection to the instance and login as <username>. Then login via Remote Desktop

Navigate to D:\trunk\Component ModelLibrary\CMLServer

Unzip artifactory-2.3.3.2 so that it shows up under CMLServer

Copy artifactory.config.orig.xml to …\CMLServer \artifactory-2.3.3.1\etc\artifactory.config.xml

Copy jetty.xml to …\CMLServer \artifactory-2.3.3.1\etc \jetty.xml

Create directory …\CMLServer \artifactory-2.3.3.1\logs

Start Artifactory using …\CMLServer\start.bat

Open a Cygwin shell on the instance and navigate to /cygdrive/d/trunk/models/Armor

Enter mvn –gs cml\_settings.xml deploy

Start the FireFox web browser

Enter the address <http://localhost:8888/artifactory/webapp/browserepo.html>

The Artifactory browser should display and the user should be able to locate the Armor artifact

**Create an Elastic IP address and associate it with an instance**

In the EC2 tab of the AWS site, select the Elastic IPs link located in the left pane

Select the Allocate New Address button. The Allocate New Address pop-up window should display with EC2 selected in the drop-down menu

Select Yes, Allocate. A new IP address line item will display in the main window

*Note, the following steps require that an EC2 instance is running*

Right-click the new line item and select Associate. The Associate Address pop-up window should display

Select an instance from the Select an instance drop-down menu, and then select Yes, Associate. The newly associated instance ID should display in the IP address line item

**Create an Amazon Machine Image (AMI)**

*Note, the following steps require that an EC2 instance exists. I’m not sure if it needs to be running*

In the EC2 tab of the AWS site, select the Instances link located in the left pane.

Right-click the desired instance and select Create Image (EBS AMI). The Create Image window should display

Give the image a meaningful name (e.g., linux-karl) and optional description, and then select Create This Image

The image creation process takes several minutes. The instance is stopped, snapshots of the disk volumes are created, and then the instance is restarted

In the EC2 tab of the AWS site, select the AMIs link located in the left panel. A line item for the new image should be displayed

To start an instance from the new AMI, right-click the AMI and select Launch Instance

*Note, it’s very important to keep track of the items associated with an AMI and instance so that they are not accidentally deleted. For sanity’s sake, it may be worth keeping a record of the the items associated with a given instance and AMI including: AMI ID, Security Group ID, Snapshot IDs, and Volume IDs. An example follows:*

*AMI ID: ami-8d9457e4, Security group: sg-a94073c0,*

*Snapshots: snap-32851a52 35 GiB, snap-36851a56 80 GiB*

*Volumes: vol-a29c19c8 35 GiB, vol a09c19ca 80 GiB*