Department of Veterans Affairs
Mental Health – Suicide Prevention
Suicide Prevention Package
Suicide Prevention Package Patch YS*5.01*130

January 6, 2020

Version 2.0

Deployment, Installation, Back-Out, and Rollback Guide for YS*5.01*130

Submitted as CLIN 0001AX

Contract VA118-16-D-1007, Task Order VA11817F10070006

Revision History

Date	Version	Description	Author
January 2020	2.0	Updated sections 7 and 8 with VistA installer info. Updated proxy setup to remove IP specific information	Booz Allen Hamilton
December 2019	1.9	Install guide updated to match the patch tracking message. Created section 4.6 and updated image in section 4.7	Booz Allen Hamilton
October 2019	1.8	YS*5.01*130 updates, updated POC information	Booz Allen Hamilton
July 2019	1.7	YS*5.01*130 updates	Booz Allen Hamilton
May 2019	1.6	YS*5.01*130 updates	Booz Allen Hamilton
February 2019	1.5	YS*5.01*139 updates	Booz Allen Hamilton
December 2018	1.4	YS*5.01*137 updates	Booz Allen Hamilton
September 2018	1.3	YS*5.01*136 updates	Booz Allen Hamilton
August 2018	1.2	YS*5.01*134 updates	Booz Allen Hamilton
July 2018	1.1	YS*5.01*134 updates	Booz Allen Hamilton
March 2018	1.0	Initial Version	Booz Allen Hamilton

Artifact Rationale

This document describes the Deployment, Installation, Back-out, and Rollback Guide (DIBO&RG) for new products going into the Veterans Affairs (VA) Enterprise. The plan includes information about system support, issue tracking, escalation processes, and roles and responsibilities involved in all those activities. Its purpose is to provide clients, stakeholders, and support personnel with a smooth transition to the new product or software, and should be structured appropriately, to reflect particulars of these procedures at a single or at multiple locations.

Per the Veteran-focused Integrated Process (VIP) Guide, the DIBO&RG is required to be completed prior to Critical Decision Point #2 (CD #2), with the expectation that it will be updated throughout the lifecycle of the project for each build, as needed.

Table of Contents

1 Introduction

This document describes how to deploy and install the patch YS*5.01*130 of the Mental Health package, 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 in this document.

1.1 Purpose

The purpose of this plan is to provide a single, common document that describes how, when, where, and to whom Mental Health patch YS*5.01*130 will be deployed and installed, as well as how it is to be backed out and rolled back, if necessary. The plan also identifies resources, communications plan, and rollout schedule. Specific instructions for installation, back-out, and rollback are included in this document

1.2 Dependencies

Minimum requirements:

Application Name	Minimum Version Needed
CPRS	31
Clinical Reminders	2.0
Kernel	8.0
RPC Broker	1.1
PIMS	5.3
VA FileMan	22.2
Mailman	8.0

It is assumed that this patch is being installed into a fully patched Veterans Health Information System and Technology Architecture (VistA) system. Patch YS*5.01*130 must also be installed.

Current versions of the Comprehensive Suicide Risk Evaluation, 24 Hr Triage, and Safety Plan CPRS form templates must be installed through the Reminder Exchange utility.

1.3 Constraints

There are no constraints beyond the installation into an up-to-date VistA system.

2 Roles and Responsibilities

The following describes the roles and responsibilities associated with the testing and release of YS*5.01*130. This is a VistA patch that will be deployed via the normal Mailman route.

Table 1: Deployment, Installation, Back-out, and Rollback Roles and Responsibilities

Team	Phase / Role	Tasks	Project Phase (See Schedule)
Project Manager	Deployment	Determine and document the roles and responsibilities of those involved in the deployment.	Design
Software Quality Assurance (SQA), Test Sites	Deployment	Test for operational readiness	Test

Team	Phase / Role	Tasks	Project Phase (See Schedule)
Project Manager, Release Manager	Deployment	Execute deployment	Release
Individual VistA Sites	Installation	Plan and schedule installation	Release
Release Manager	Back-out	Confirm availability of back-out instructions and back-out strategy (what are the criteria that trigger a back-out)	Release
Sustainment Team	Post Deployment	Hardware, Software and System Support	Sustain

3 Deployment

The deployment is planned as a simultaneous (National Release) rollout. Once approval has been given to nationally release, YS*5.01*130 will be available for installation and deployment at all sites.

Scheduling of test installs, testing and production deployment will be at the site's discretion. It is anticipated there will be a 30-day compliance period.

3.1 Timeline

The deployment and installation are scheduled to run during July 2019 as depicted in the Master Deployment Schedule in the Suicide Prevention Program (SPP) Project Management Plan.

3.2 Site Readiness Assessment

This section discusses the locations that will receive the YS*5.01*130 deployment.

Deployment Topology (Targeted Architecture)

MHA Update (YS*5.01*130) will be deployed to each VistA instance. This includes local sites as well as regional data centers. The executable and associated files will also be deployed to client workstations. For the web application portion, it is deployed in the Microsoft Azure cloud environment.

Site Information (Locations, Deployment Recipients)

The initial deployment will be to Initial Operating Capability (IOC) sites for verification of functionality. Once testing is completed and approval is given for national release, MHA Update (YS*5.01*130) will be deployed to all VistA systems.

The Production IOC testing sites are:

- Milwaukee Veterans Affairs Medical Center (VAMC)
- Orlando VAMC

Site Preparation

Other than a fully patched VistA system, there is no other preparation required.

3.3 Resources

Facility Specifics (optional)

N/A

Hardware

IPad, Kiosk

Software

N/A

Communications

When MHA Update (YS*5.01*130) is released, the released-patch notification will be sent from the National Patch Module to all personnel who have subscribed to notifications for the Mental Health package.

4 Vista and MHA Installation

4.1 Pre-installation and System Requirements

MHA Web Patient Entry (YS*5.01*130) assumes a fully-patched VistA system.

4.2 Platform Installation and Preparation

There are both VistA and Windows client components that must be installed for MHA Web Patient Entry. The VistA portion is distributed as a PackMan message. The Windows client executable is distributed in a zip file.

The time to deploy the GUI updates to Windows clients will vary depending on the method the site uses for running the MHA executable (network share, Citrix, etc.). There are no conflicting changes on the VistA server, so the current Windows executable (version 1.0.3.75) may continue to operate until the upgrade to this updated Windows executable (version 1.0.3.80) is accomplished.

4.3 Download and Extract Files

The MHA Web Patient Entry (YS*5.01*130) Windows client is being released as a host file.

The preferred method is to retrieve files from download.vista.med.va.gov.

This transmits the files from the first available server. Sites may also elect to retrieve files directly from a specific server.

Sites may retrieve the software and/or documentation using Secure File Transfer Protocol (SFTP) from the ANONYMOUS.SOFTWARE directory at: REDACTED

Documentation can also be found on the VA Software Documentation Library at:

http://www.va.gov/vdl/

MHA Web Patient Entry file

Files to be downloaded	File Contents	Download Format
YS_501_130.ZIP	MHA executable	Binary

4.4 Access Requirements and Skills Needed for the Installation

Installation of MHA Web Patient Entry (YS*5.01*130) requires the following:

- Programmer access to the VistA instance and the ability to install a KIDS build.
- Citrix Access Gateway (CAG) installs – access/ability to upload to the CAG.
- Network Share installs – access/ability to upload executable files to the network share location.
- Individual workstation installs – access/ability to push executable and supporting files to required work stations.

4.5 Installation Procedure

YS*5.01*130 KIDS Installation

This patch can be loaded with users in the system, but it is recommended that it be installed when user activity is low. Installation time will be less than 5 minutes.

1. Choose the PackMan message containing this patch and invoke the INSTALL/CHECK MESSAGE PackMan option.

2. Start up the Kernel Installation and Distribution System Menu [XPD MAIN]:

```
    Edits and Distribution ...
    Utilities ...
    Installation ...

  Select Kernel Installation & Distribution System Option: Installation
    1    Load a Distribution
    2    Verify Checksums in Transport Global
    3    Print Transport Global
    4    Compare Transport Global to Current System
    5    Backup a Transport Global
    6    Install Package(s)
         Restart Install of Package(s)
         Unload a Distribution
```

3. From this menu, you may elect to use the following options (when prompted for the INSTALL NAME, enter YS*5.01*130):

a. Backup a Transport Global - This option will create a backup message of any routines exported with this patch. It will not backup any other changes such as DD's or templates.
b. Compare Transport Global to Current System - This option will allow you to view all changes that will be made when this patch is installed. It compares all components of this patch (routines, DD's, templates, etc.).
c. Verify Checksums in Transport Global - This option will allow you to ensure the integrity of the routines that are in the transport global.

4. Use the Install Package(s) option and select the package: YS*5.01*130.

a. When prompted "Want KIDS to Rebuild Menu Trees Upon Completion of Install? NO//", answer NO.
b. When prompted "Want KIDS to INHIBIT LOGONs during the install? NO//", answer NO.
c. When prompted "Want to DISABLE Scheduled Options and Menu Options and Protocols? NO//", answer NO.

YS*5.01*130 GUI Installation

The ZIP file contains the updated MHA GUI executable file. Download the ZIP file and extract the file.

The following methods of installation are available. Sites' choice of which method(s) to use will depend upon Regional/VISN policies, Local Area Network (LAN) performance or other local circumstances. User requirements, physical location and methods of connection to the VA network may warrant more than one of the options below to be used.

- **Network (shared) installation:**

  This method is typically the simplest to maintain, providing the local network infrastructure is robust enough to handle the additional traffic caused by users running the MHA GUI executable (YS_MHA.exe) across the LAN.

  The MHA executable (YS_MHA.exe) is copied to a network shared location.

  Since MHA is launched from the CPRS toolbar, CPRS must know where to find it on the network drive (see Section 4.5.3 below). Use the parameter, ”ORWT TOOLS MENU”, to enter the network location of YS_MHA.exe.

  Note: MHA no longer uses the file, YS_MHA_AUX.dll, so it is not necessary to update the YS MHA_AUX DLL LOCATION parameter.

- **Citrix installation:**

  The MHA executable (YS_MHA.exe) and supporting files are installed and run from a remote workstation, and the user views the remote workstation’s screen on their local workstation.

  For the local site users, this method is on a similar level to the Network (shared) installation above. The users' workstations require only an appropriate shortcut (and the necessary Citrix Access Group (CAG) infrastructure).

  Note: For issues with CAG, please contact your local or national help desk.

  For the Citrix Farm administrator, this method involves installations on the host in a similar manner to the manual installation method outlined below.

- **Manual install:**

This method is used primarily for advanced users and at testing locations.

Note: You may need to have a user with Administrator rights complete this step.

The following steps will update an existing installation of MHA, if one exists on the workstation. These steps use the default file locations.

1. Locate the YS_501_130.ZIP file and unzip it.
2. Copy the unzipped YS_MHA.exe to C:\Program Files x86)\Vista\YS\MHA\.

If desired, you may use different directories than those specified above, but you must also update the ORWT TOOLS MENU parameters to reflect the file location.

- **SCCM install:**
  An SCCM package is available for deployment to workstations at a site. To deploy via SCCM, request that the "Mental Health Assistant " program be deployed.

Setting Connector Proxy User

To create a connector proxy user:

1. You must hold the Kernel XUMGR key.
2. Add a new connector proxy user by using the Foundations menu on your M system and choosing the Enter/Edit Connector Proxy User option.
3. The account requires no additional information from what is prompted for by the option.
4. Leave the connector proxy user's Primary Menu empty.
5. The IP and port of VistaLink listener on IOC cloud is mentioned below:

Example	IP#	PORT# / TCP
Milwaukee	XXXXX	XXXX /TCP

6. Securely communicate the access code and verify code for the connector proxy user to the following personal:

REDACTED

- **Do not enter divisions for a connector proxy user**
- **Do not enter a primary menu**
- **Do not also use the connector proxy user as a test "end-user"**
- **Utilize the user only as a connector proxy user**

Setting MHA on the CPRS Tools Menu

This procedure configures VistA so that "Mental Health Assistant" appears as a choice on a user's Tools menu on the CPRS desktop software. Unlike previous versions of MHA, where this was optional, Version 3 of VistA MHA MUST be started from the CPRS Tools Menu. Selecting this choice from the CPRS Tools menu will offer the user full MHA3 functionality, based on a user's access permissions in VistA.

The basic steps for setting up VistA MHA3 on the Tools menu are no different from doing it for other applications. The main difference lies in how the Name=Command entry is formatted. The following text capture is taken from the CPRS Setup documentation, to serve as an example of how to perform this step for MHA3:

Example: Setting up VistA MHA3 on the CPRS Tools menu, GUI Parameters [ORW PARAM GUI]

```
Select GUI Parameters Option: tm GUI<ENTER> Tool Menu Items

CPRS GUI Tools Menu may be set for the following: <ENTER>

1 User USR [choose from NEW PERSON]

2 Location LOC [choose from HOSPITAL LOCATION]

3 Division DIV [REGION 5]

4 System SYS [OEX.ISC-SLC.VA.GOV]

Enter selection: 1<ENTER> User NEW PERSON

Select NEW PERSON NAME: MHPROVIDER,ONE <ENTER>------------- Setting CPRS GUI Tools Menu
for User: MHPROVIDER,ONE----------

Sequence: ? <ENTER>

Enter the sequence in which this menu item should appear.

Select Sequence: 2

Are you adding 2 as a new Sequence? Yes//<ENTER> YES

Sequence: 2// <Enter>

Name=Command: Mental Health Assistant=”C:\Program Files (x86)\Vista\YS\MHA3\YS_MHA.exe”
s=%SRV p=%PORT c=%DFN u=%DUZ m=%MREF
```

From the previous example, adjust according to your own system’s settings, such as directory path, New Person Name and other parameters—consult the CPRS Setup Guide for the meaning of these parameters. The pertinent portion of the example is the “Name=Command:” field. This field should be entered in a single line—no line-breaks allowed, including all the % parameters that follow the filename and path to the MHA3 executable file.

The path shown represents a typical path used during a default installation. If your path is different, adjust accordingly. **ALL five parameters must be included as shown above, in the precise order in which they are found in the example.** Here is what the Name=Command line should look like:

Mental Health Assistant=”C:\Program Files (x86)\Vista\YS\MHA3\YS_MHA.exe” s=%SRV p=%PORT c=%DFN u=%DUZ m=%MREF

Sequence number 2 is shown in the example, but, if you have other entries in the Tools Menu, then the next free sequence number will do just fine. (Sometimes when cutting and pasting, unseen control characters can be included in the text and will cause the command line to malfunction.)

After this step is completed, a new choice will appear in the user's CPRS Tools Menu labeled "Mental Health Assistant". Clicking on this menu entry will start MHA3 with a selected patient synchronized to the one currently selected in CPRS.

Refer to the Computerized Patient Record System (CPRS) Setup Guide for more information about this procedure.

4.6 Post-Installation Instructions

After the KIDS build for YS*5.01*130 is installed, the existing MHA executable (1.0.3.75) and the new MHA executable (1.0.3.80) will both still function. A simultaneous update of the Windows executable is not required. This provides the option of having some users continue with the existing executable while others (perhaps those with access to iPads or kiosks) use the new executable. Adding another MHA item to the CPRS Tools menu can accomplish this. These are the basic steps:

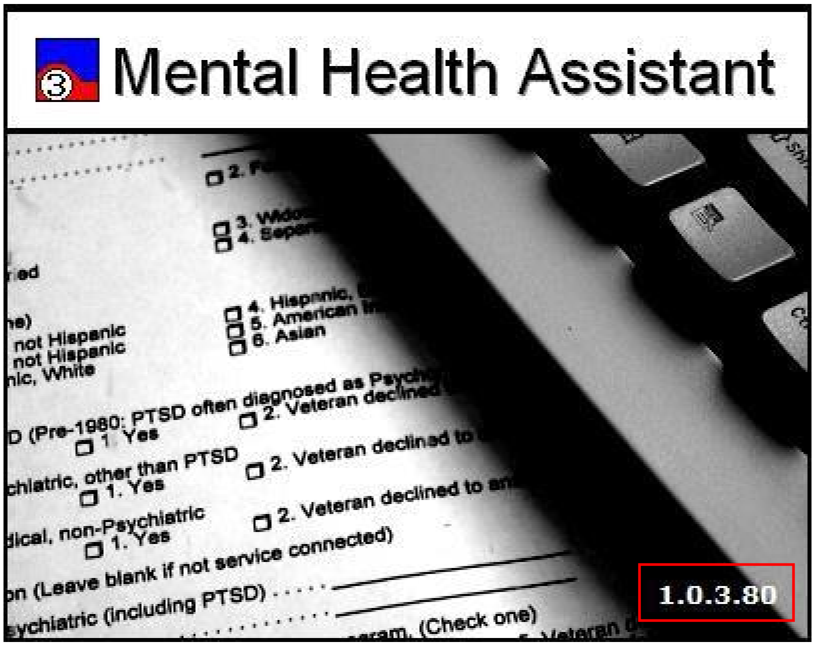
- Rename the new "YS_MHA.exe" to something like "YS_MHA_130.exe" and place it in the directory where you currently have YS_MHA.exe.
- Edit the parameter, ORWT TOOLS MENU, and add a temporary item named something like "MHA Patient Entry" that invokes the executable that you just renamed. (See Setting MHA on the CPRS Tools Menu).
- When you are ready for all users to use the new executable, simply delete the YS_MHA.exe file and rename "YS_MHA_130.exe" to "YS_MHA.exe". Don't forget to remove the temporary item from the ORWT TOOLS MENU.

If your site's workstations are all Windows 10 and you are not using "Secure Desktop" with MHA anymore, you can just move to the new YS_MHA.exe immediately, without adding a new item to the CPRS Tools menu.

4.7 Installation Verification Procedure

To verify that everything is installed properly, do the following:

- Launch CPRS.
- From the CPRS menu, select Tools, then Mental Health Assistant.
- As MHA starts you should see the splash screen with version 1.0.3.80 displayed in the lower right corner.



4.8 System Configuration

N/A

4.9 Database Tuning

N/A

5 Vista and MHA Back-Out Procedure

5.1 Back-Out Strategy

It is possible to partially back-out the installation of YS*5.01*130. This would involve restoring instrument specifications to their previous state and then restoring the saved routines. The back-out of changes to the data dictionary would require a patch to a patch.

5.2 Back-Out Considerations

Please contact VistA support and the development team before attempting a back-out. The back-out procedure will still leave some changes in place. In addition, the installation of subsequent patches may be problematic if YS*5.01*130 is not installed.

5.3 Back-Out Criteria

A back-out should only be considered if there is a patient safety issue, if MHA no longer functions, or if there is some other catastrophic failure.

5.4 Back-Out Risks

The risks vary depending on what is causing the failure of the system. The main risk is that the Mental Health package would be left in an unknown configured state.

5.5 Authority for Back-Out

The VistA system manager determines if a back-out of YS*5.01*130 should be considered.

5.6 Back-Out Procedure

If you wish to restore newly installed instruments to their previous state, you must do that before any other back-out steps. See the instructions for restoring the previous instrument state in the Rollback Procedure section to do this.

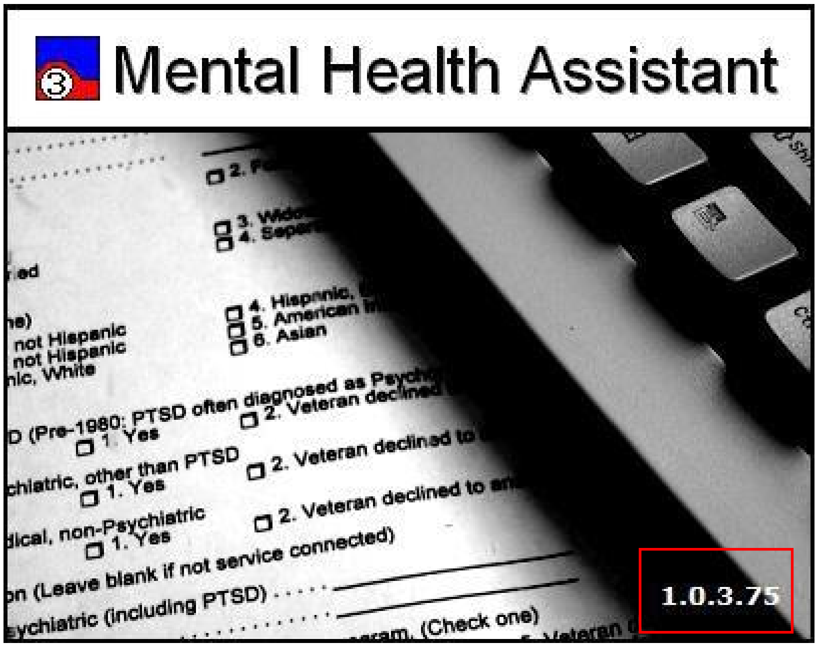
To back-out routines, you must have already selected the “Backup a Transport Global” option during the installation process. To restore the previous routines:

1. Choose the PackMan message containing the backup you created during installation.
2. Invoke the INSTALL/CHECK MESSAGE PackMan option.
3. Select Kernel Installation & Distribution System Option: Installation
4. Use the Install Package(s) option to install the previously saved routines.

If you need to back-out data dictionary modifications, remove protocols, options, or templates, you will need to contact the development team for a patch.

5.7 Back-out Verification Procedure

A successful back-out may be verified by running MHA and seeing a splash screen with the highlighted version number:



MHA should prompt for access/verify instead of PIV PIN and run successfully.

Verification of the back-out procedure would be the resolution of the problem that caused the need for the back-out.

6 Vista and MHA Rollback Procedure

6.1 Rollback Considerations

YS*5.01*130 adds new and updates existing mental health instruments. It is possible to roll back these changes within one week of the installation.

6.2 Rollback Criteria

A rollback might be considered if the behavior of mental health instruments appears to be adversely affected after installation of YS*5.01*130. The VistA support and product development team should be contacted to determine if there is an alternative fix short of a rollback.

6.3 Rollback Risks

A rollback could adversely impact future installations of mental health instruments and cause problems with scoring existing mental health instruments.

6.4 Authority for Rollback

The VistA system manager determines if a rollback of mental health instruments distributed by YS*5.01*130 should be considered.

6.5 Rollback Procedure

These steps assume that there is a compelling reason to rollback specific instruments to their previous state.

For instruments that have been inactivated by YS*5.01*130 that need to be made active again:

- Using FileMan, edit the OPERATIONAL field (#10) and the LAST EDIT DATE field (#18) in the MH TESTS AND SURVEYS file (601.71). Select the instrument that requires re-activation.
- Change the value of the OPERATIONAL field from “Dropped” back to “Yes”
- Change the value of the LAST EDIT DATE field to ‘NOW’.

Should it be required to move instruments back to being scored in YS_MHA_AUX DLL, contact the Mental Health development team for a routine that can find the appropriate records and make the replacement.

Optionally, if you want to see how many records will be restored, choose “Trial Install” then select the number of the backup you wish to restore.

When you are ready to restore an instrument, choose “Install Exchange Entry” then select the number of the backup you want to restore.

6.6 Rollback Verification Procedure

Verify the restore by checking to see that the instrument behaves as it did prior to the install.

7 MHA Web Installation

*This step will not be done by the VistA installer

7.1 Prerequisite

Users should have access to the VA government Azure subscription. An active zero account is required to access the Azure dashboard. A GFE laptop or desktop with elevated privileges and an active VA VPN connection are necessary. The following software is also required:

1) Reflections Workspace
2) WinSCP
3) GitBash

This guide assumes no existing production virtual machines exist.

7.2 SSH Key

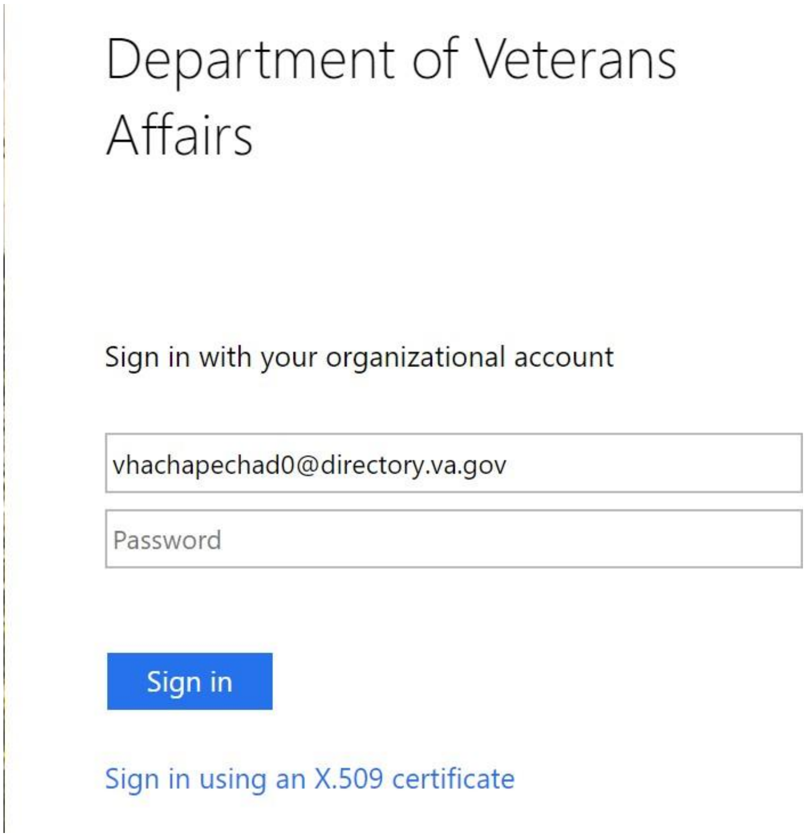
Using GitBash(Windows) or a bash terminal(Linux/Mac), create an SSH key pair that is used to SSH into Linux without using a password. Open a Git Bash terminal (Windows) or bash shell (Linux/Mac) and use ssh_keygen to create an SSH key pair.

```
$ ssh-keygen -t rsa -b 2048
```

This command generates public and private keys with the default name of id_rsa in the ~/.ssh directory. Save this file for later.

7.3 Create a VM

Sign in to the Azure portal available here.



Department of Veterans Affairs

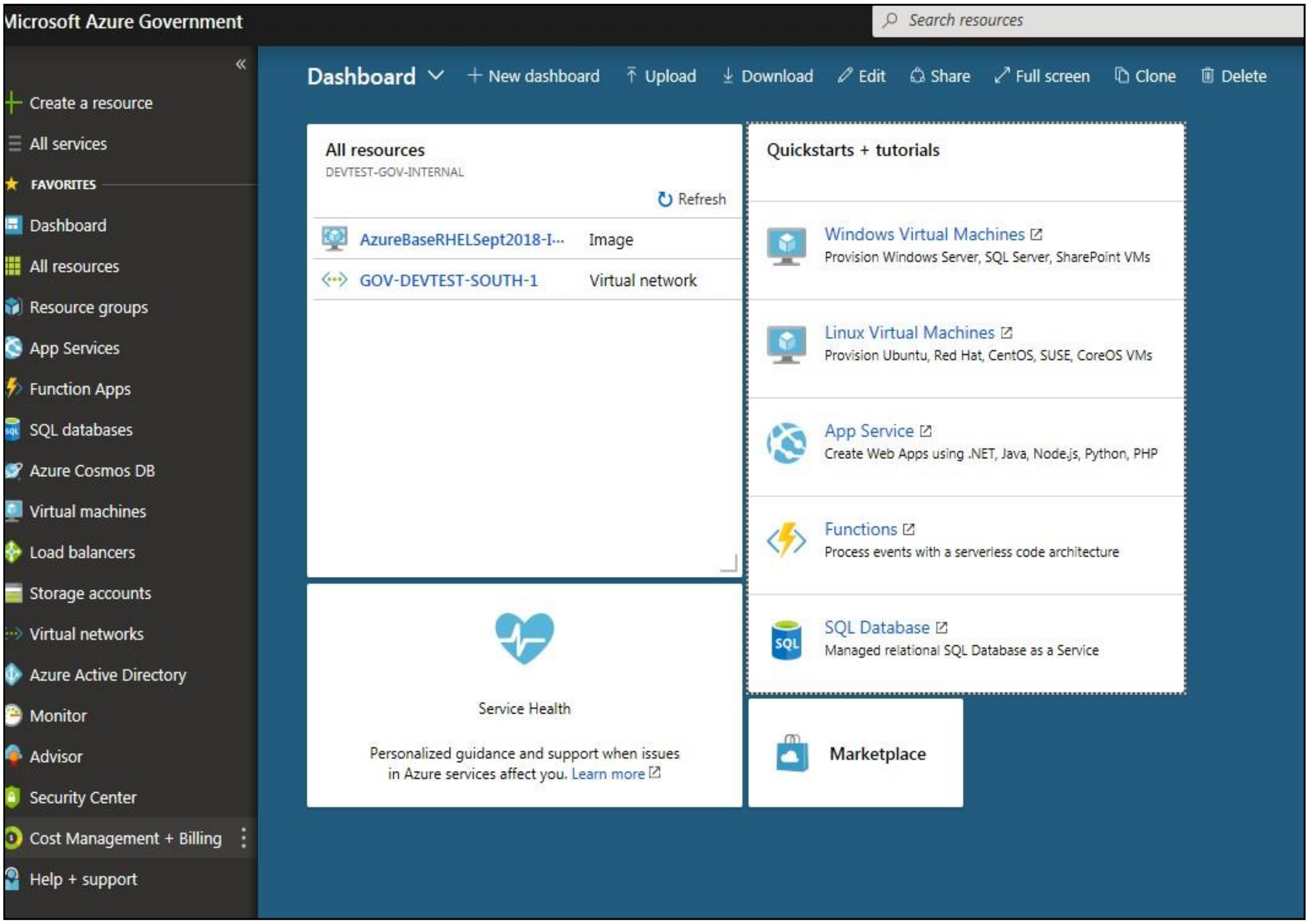
Sign in with your organizational account

vhachapechad0@directory.va.gov

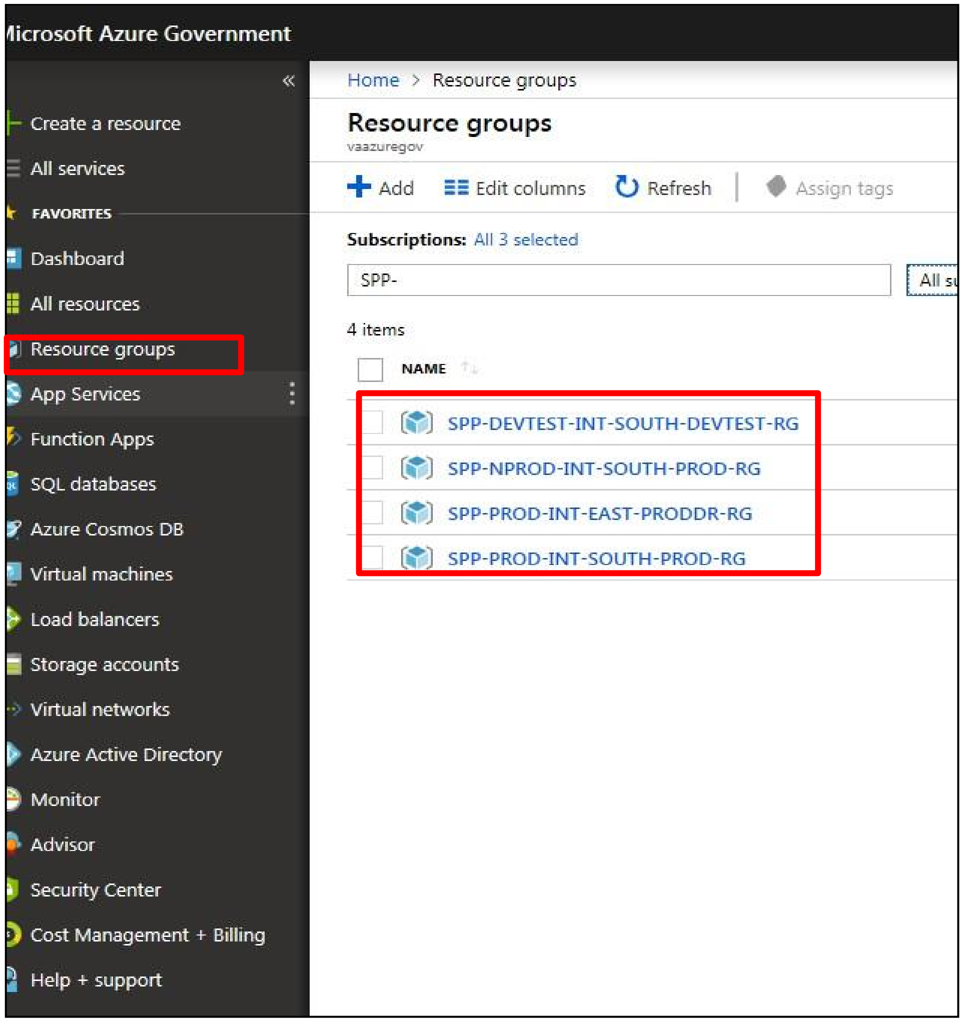
Select “Sign in using an X.509 certificate”

The system would respond with a list of certificates. Select the valid certificate for your zero token and enter your PIN.

On successful authentication, the user is navigated to Azure portal as shown below:



Click Resource groups in the left panel of the Azure portal, the portal shows available resource groups as shown below:



Resource groups
vaazuregov

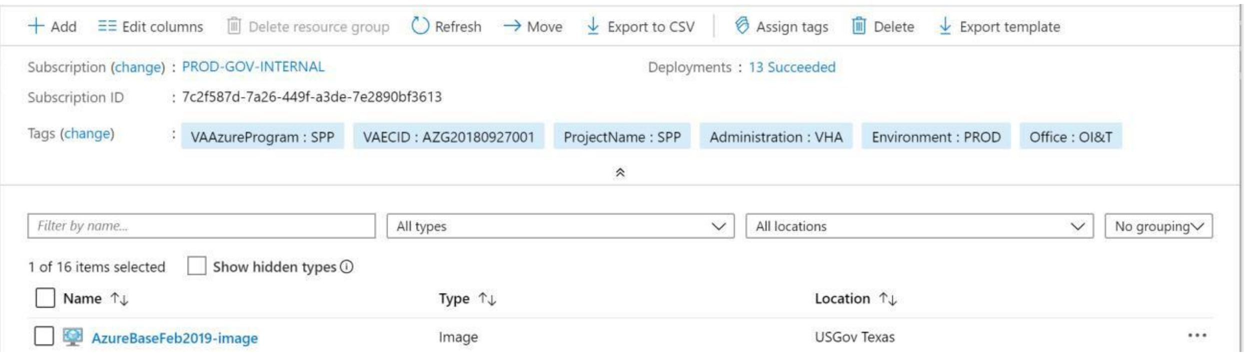
Subscriptions: All 3 selected

SPP-

4 items

NAME
SPP-DEVTEST-INT-SOUTH-DEVTEST-RG
SPP-NPROD-INT-SOUTH-PROD-RG
SPP-PROD-INT-EAST-PRODDR-RG
SPP-PROD-INT-SOUTH-PROD-RG

We are creating virtual machines for production, select the SPP-PROD-INT-SOUTH-PROD-RG resource group.

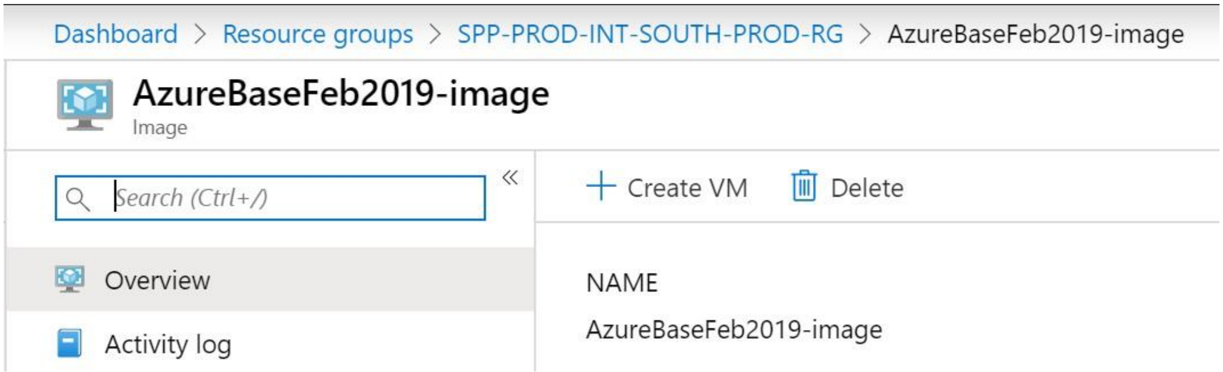


Subscription (change) : PROD-GOV-INTERNAL
Deployments : 13 Succeeded
Subscription ID : 7c2f587d-7a26-449f-a3de-7e2890bf3613
Tags (change) : VAAzureProgram : SPP | VAECID : AZG20180927001 | ProjectName : SPP | Administration : VHA | Environment : PROD | Office : OI&T

1 of 16 items selected   □ Show hidden types

Name	Type	Location
AzureBaseFeb2019-image	Image	USGov Texas

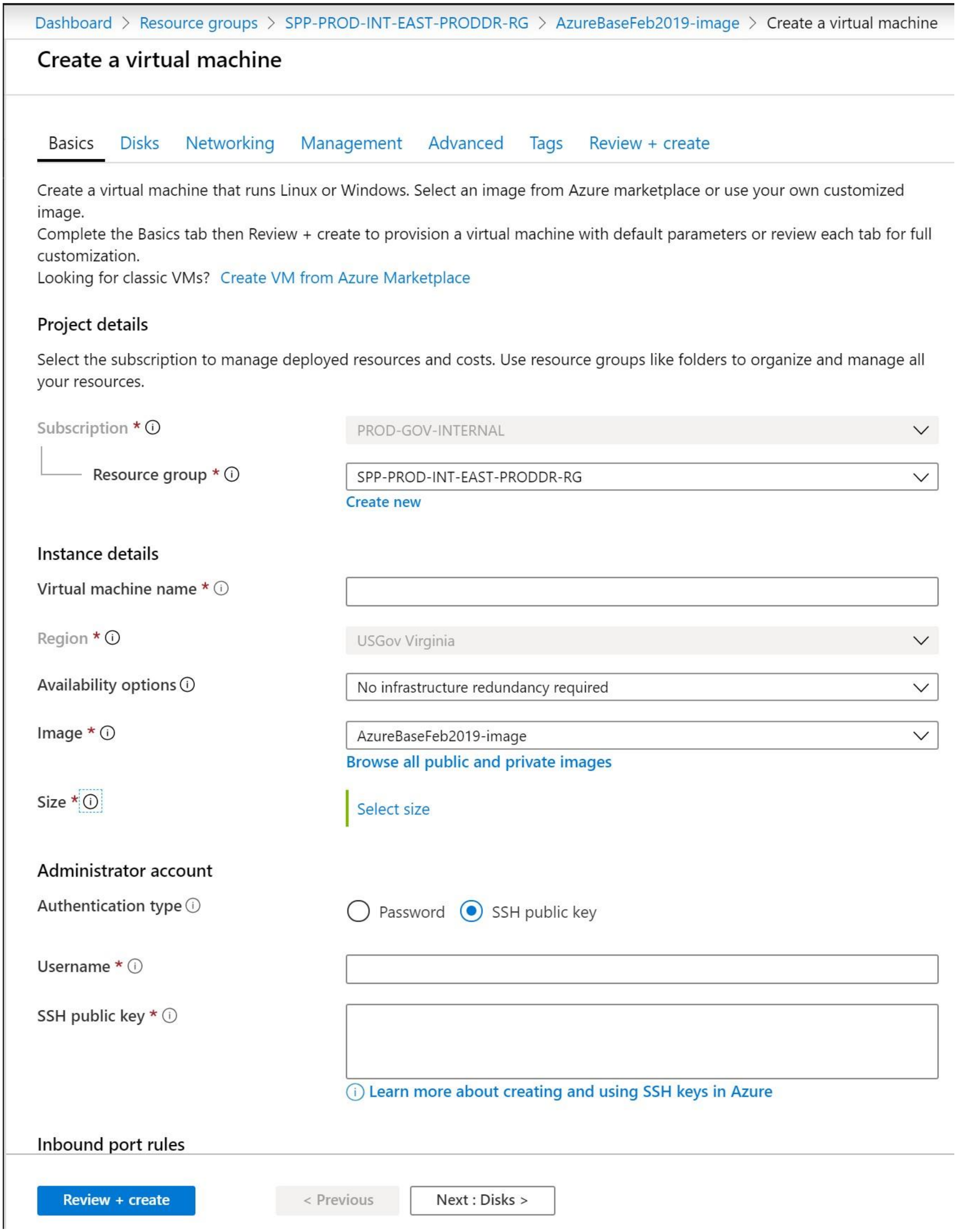
In the list of resources, select the AzureBaseFeb2019-image.


Dashboard > Resource groups > SPP-PROD-INT-SOUTH-PROD-RG > AzureBaseFeb2019-image
AzureBaseFeb2019-image
Image
Search (Ctrl+/)
Overview
Activity log
+ Create VM
Delete

NAME

AzureBaseFeb2019-image

Click “Create VM” at the top of the portal



Dashboard > Resource groups > SPP-PROD-INT-EAST-PRODDR-RG > AzureBaseFeb2019-image > Create a virtual machine

Create a virtual machine

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image.
Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.
Looking for classic VMs? Create VM from Azure Marketplace

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ PROD-GOV-INTERNAL

Resource group * ⓘ SPP-PROD-INT-EAST-PRODDR-RG

Create new

Instance details

Virtual machine name * ⓘ

Region * ⓘ USGov Virginia

Availability options ⓘ No infrastructure redundancy required

Image * ⓘ AzureBaseFeb2019-image

Browse all public and private images

Size * ⓘ Select size

Administrator account

Authentication type ⓘ ○ Password ● SSH public key

Username * ⓘ

SSH public key * ⓘ

ⓘ Learn more about creating and using SSH keys in Azure

Inbound port rules

Enter details as shown:

Resource group: Leave the default selected.

Virtual Machine Name: Enter the name of the virtual machine (eg. vac21appspp200)

Size: Find and select "Standard F8s"

Administration type: Since we are creating administrative account, select SSH public key, type your user name, then paste your public key into the text box. Remove any leading or trailing white space in your public key.

User Name: sppAdmin

SSH Key: Copy and paste the public part of the SSH key here.

Press Next : Disks

Leave Premium SSD selected.

Select Next : Networking

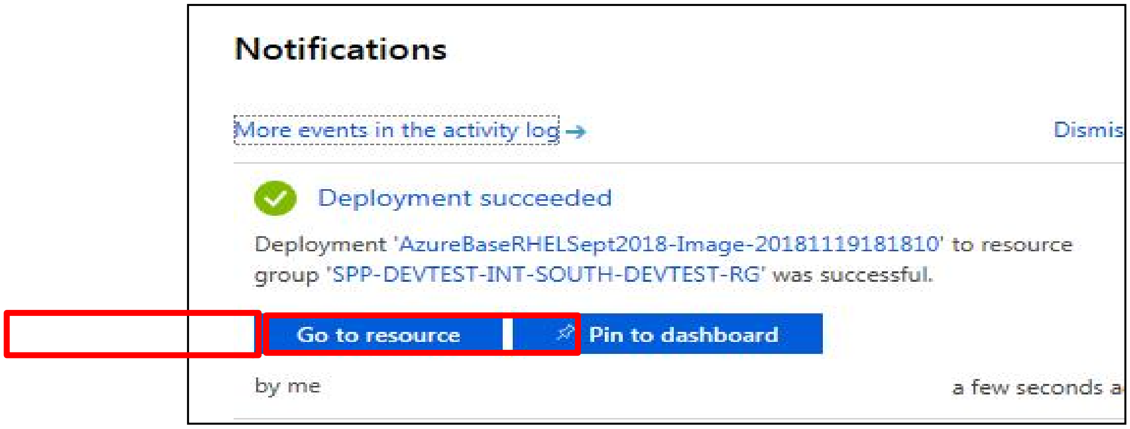
Select default virtual network and any available subnet for this resource group.

Since VM is not accessible from public network, select None for Public IP address.

Select "Allow selected ports and select all options from the list (HTTP, HTTPS, SSH, RDP)

Press Review + Create

Click Create button. It will take a few minutes for VM to be deployed. Once deployed, the following screen will display the notifications box in the right column.



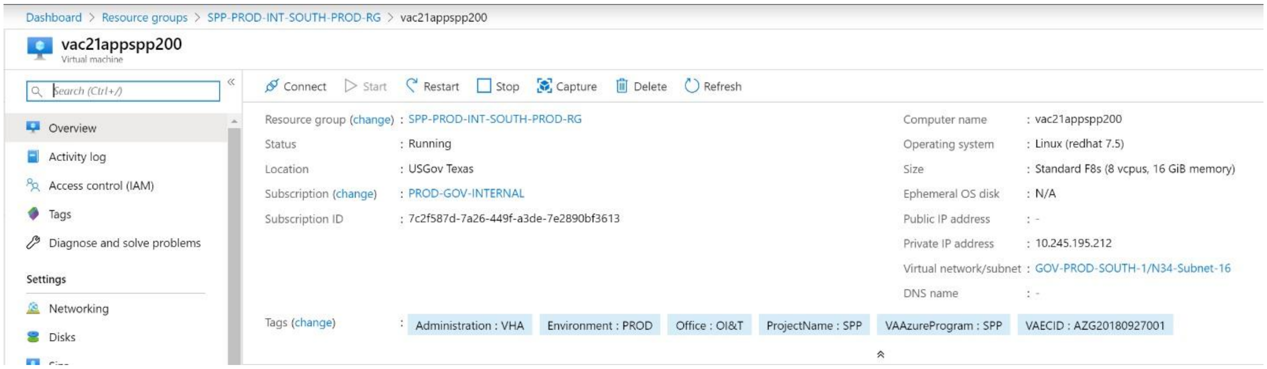
Notifications

Deployment succeeded

Deployment 'AzureBaseRHELSept2018-Image-20181119181810' to resource group 'SPP-DEVTEST-INT-SOUTH-DEVTEST-RG' was successful.

Push Pin to dashboard button, all resources created are displayed in the resource group.

Push Go to resource button and the following screen is displayed.



vac21appspp200
Virtual machine

Resource group (change) : SPP-PROD-INT-SOUTH-PROD-RG
Status : Running
Location : USGov Texas
Subscription (change) : PROD-GOV-INTERNAL
Subscription ID : 7c2f587d-7a26-449f-a3de-7e2890bf3613

Computer name : vac21appspp200
Operating system : Linux (redhat 7.5)
Size : Standard F8s (8 vcpus, 16 GiB memory)
Ephemeral OS disk : N/A
Public IP address : -
Private IP address : 10.245.195.212
Virtual network/subnet : GOV-PROD-SOUTH-1/N34-Subnet-16
DNS name : -

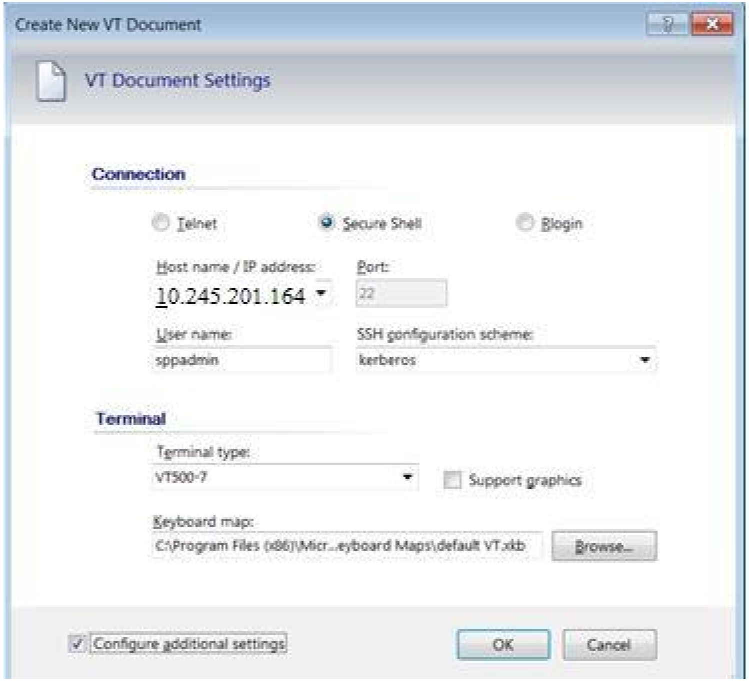
Tags (change) : Administration : VHA Environment : PROD Office : OI&T ProjectName : SPP VAAzureProgram : SPP VAECID : AZG20180927001

7.4 Connect to the virtual machine

Configure Reflections to Connect to Cloud

Configure a session to connect to a cloud server and Configure Reflections Security to generate publick key.

1. Open up MicroFocus Reflections
2. Go to File, New VT Terminal
3. Click on Secure Shell for the Connection
4. Enter the IP address, (10.245.195.212) (This is an example. Please check the IP's of the virtual machines across resource groups)
5. Enter sppprodadmin for the user name and Kerberos for the ssh configuration scheme.
6. Check the Configure additional settings checkbox



Connection

○ Telnet ● Secure Shell ○ Rlogin

Host name / IP address: 10.245.201.164

Port: 22

User name: sppadmin

SSH configuration scheme: kerberos

Terminal

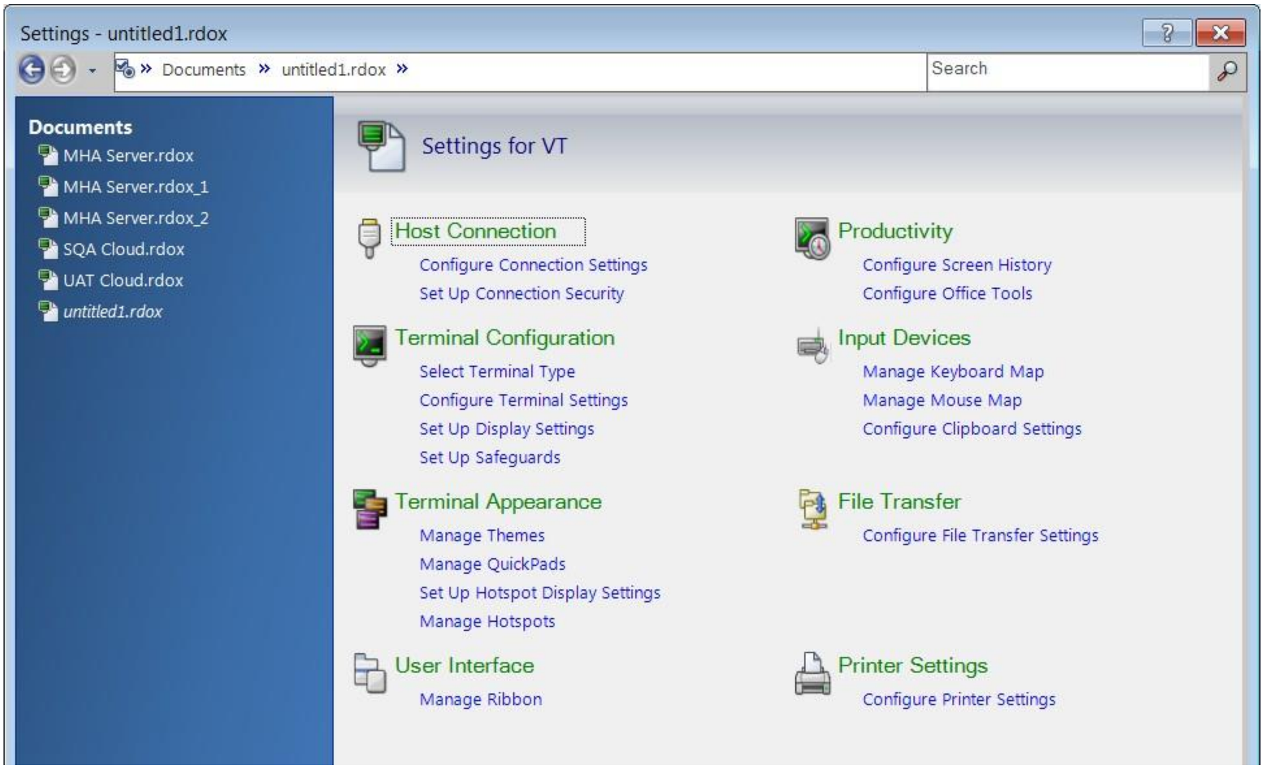
Terminal type: VT500-7

□ Support graphics

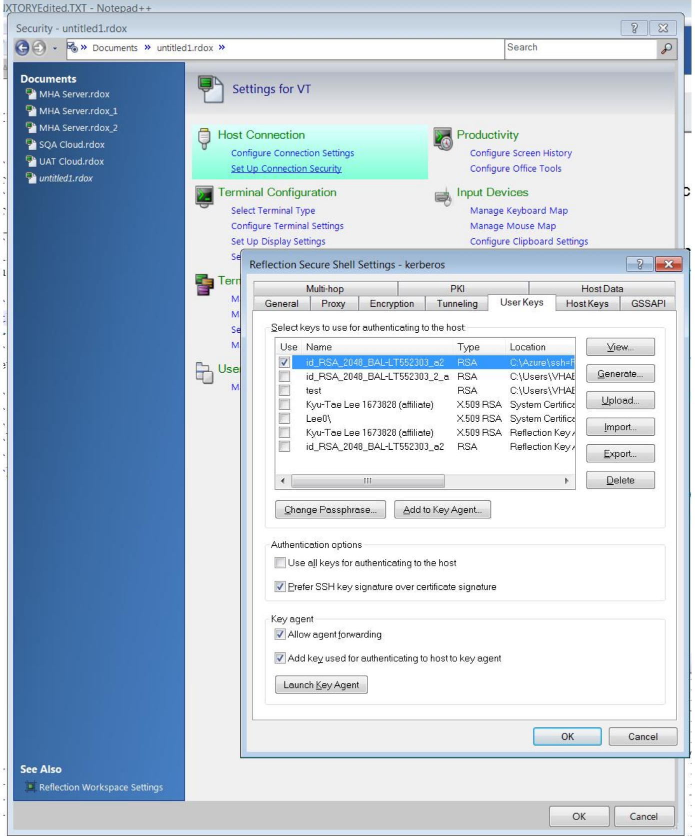
Keyboard map: C:\Program Files (x86)\Micr...eyboard Maps\default VT.xkb

☑ Configure additional settings

7. Click OK
8. Click on Set Up Connection Security



9. Click on the User Keys tab



Select keys to use for authenticating to the host:

Use	Name	Type	Location
☑	id_RSA_2048_BAL-LT552303_a2	RSA	C:\Azure\ssh=F
□	id_RSA_2048_BAL-LT552303_2_a	RSA	C:\Users\VHAE
□	test	RSA	C:\Users\VHAE
□	Kyu-Tae Lee 1673828 (affiliate)	X.509 RSA	System Certifica
□	Lee0\	X.509 RSA	System Certifica
□	Kyu-Tae Lee 1673828 (affiliate)	X.509 RSA	Reflection Key /
□	id_RSA_2048_BAL-LT552303_a2	RSA	Reflection Key /

Authentication options

□ Use all keys for authenticating to the host

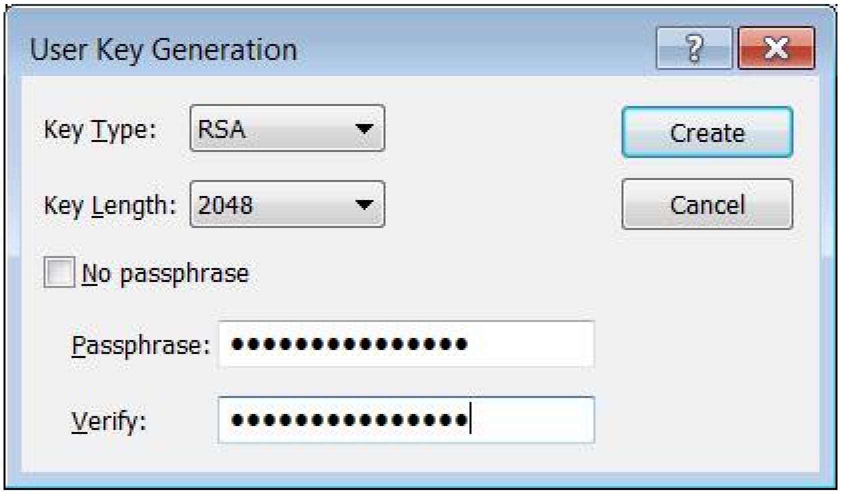
☑ Prefer SSH key signature over certificate signature

Key agent

☑ Allow agent forwarding

☑ Add key used for authenticating to host to key agent

10. Click on Generate
11. Keep the Key Type as RSA and Key Length as 2048
12. Enter a passphrase that you will remember and click Create.



User Key Generation

Key Type: RSA

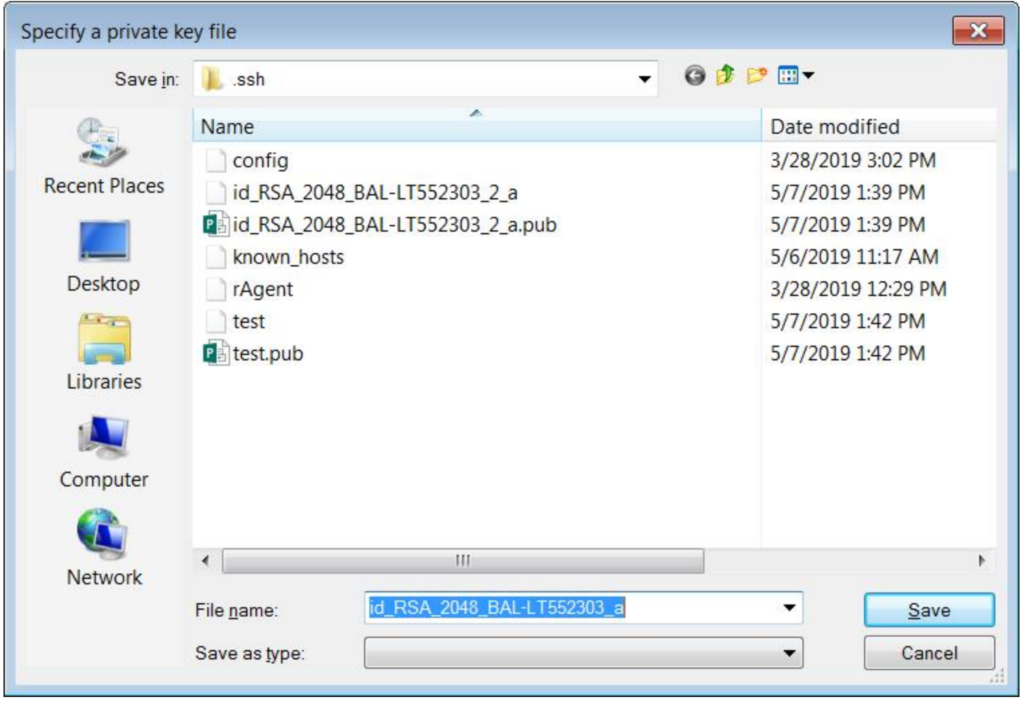
Key Length: 2048

☐ No passphrase

Passphrase: ●●●●●●●●●●●●●●●●

Verify: ●●●●●●●●●●●●●●●●

13. Leave the key name and location default and click Save



Specify a private key file

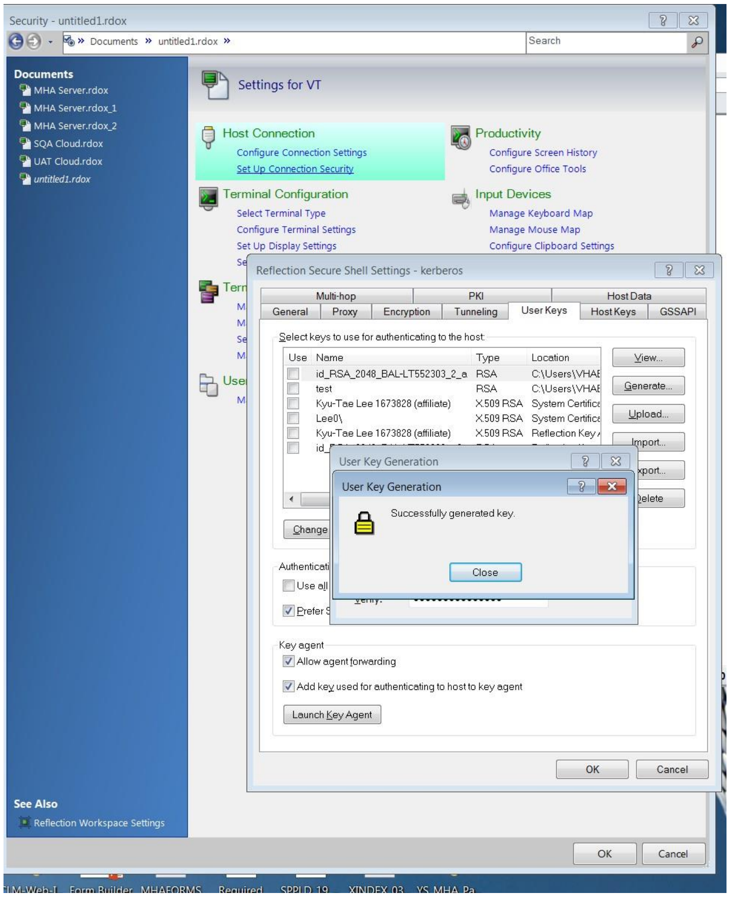
Save in: .ssh

Name	Date modified
config	3/28/2019 3:02 PM
id_RSA_2048_BAL-LT552303_2_a	5/7/2019 1:39 PM
id_RSA_2048_BAL-LT552303_2_a.pub	5/7/2019 1:39 PM
known_hosts	5/6/2019 11:17 AM
rAgent	3/28/2019 12:29 PM
test	5/7/2019 1:42 PM
test.pub	5/7/2019 1:42 PM

File name: id_RSA_2048_BAL-LT552303_a

Save as type:

14. You should see a successful key generated:



Select keys to use for authenticating to the host:

Use	Name	Type	Location
□	id_RSA_2048_BAL-LT552303_2_a	RSA	C:\Users\VHAE
□	test	RSA	C:\Users\VHAE
□	Kyu-Tae Lee 1673828 (affiliate)	X.509 RSA	System Certifica
□	Lee0\	X.509 RSA	System Certifica
□	Kyu-Tae Lee 1673828 (affiliate)	X.509 RSA	Reflection Key A
□	id_		

Successfully generated key.

Authenticati

□ Use all

☑ Prefer S

Key agent

☑ Allow agent forwarding

☑ Add key used for authenticating to host to key agent

15. Click Close
16. This key will be used for authentication.

WinSCP: It’s a popular free open source SFTP client, FTP client SFTP and FTP client for Windows, a powerful file manager that will improve your productivity.

Add the private key to the cloud server for authentication. Please contact the administrator for private -key.ppk

Download and install from https://winscp.net/eng/download.php

What is SSH private and public key:

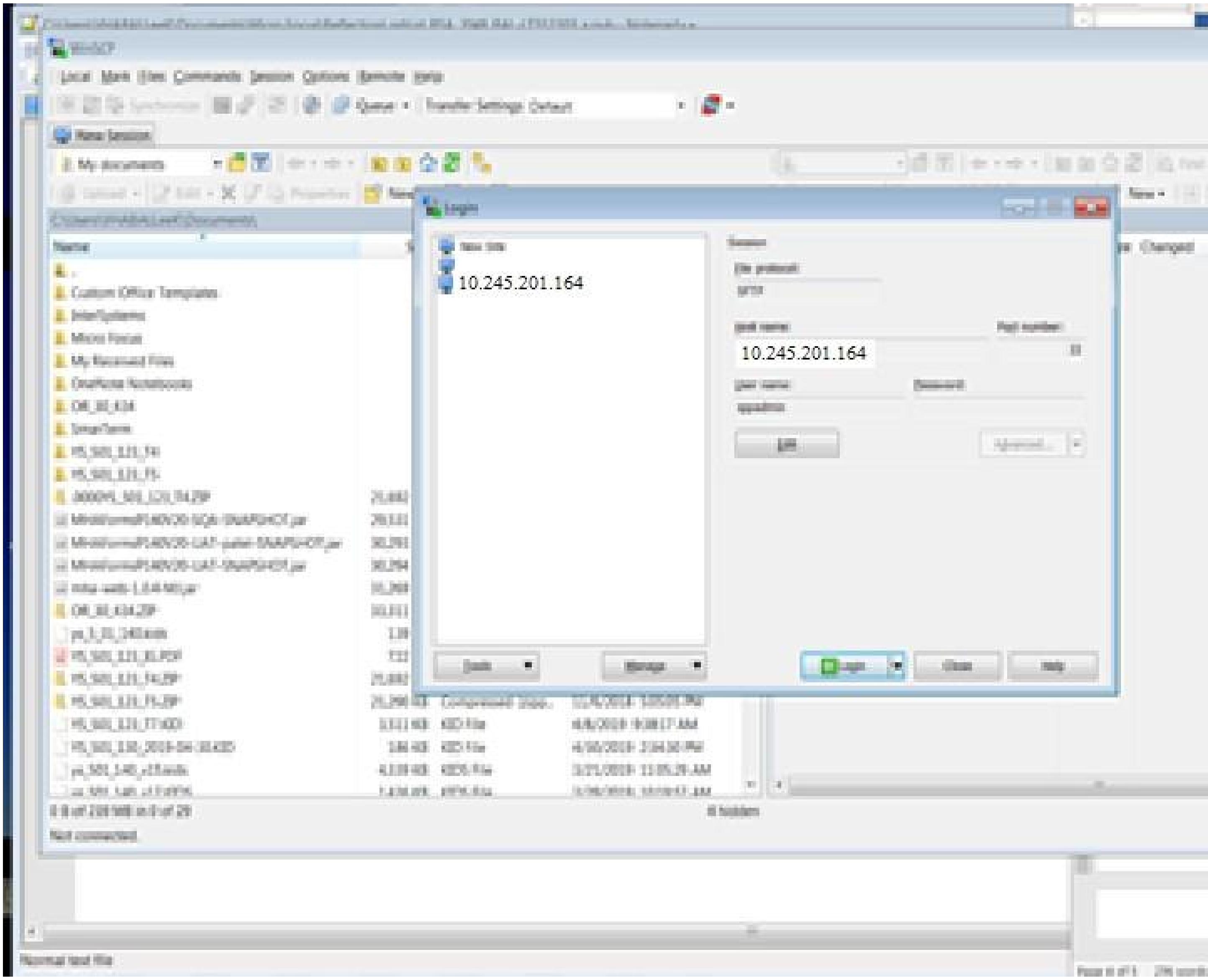
Password authentication is the default method most SSH (Secure Shell) clients use to authenticate with remote servers, but it suffers from potential security vulnerabilities.

An alternative to password authentication is public key authentication, in which we generate and store on your computer a pai r of cryptographic keys and then configure our server to recognize and accept your keys.

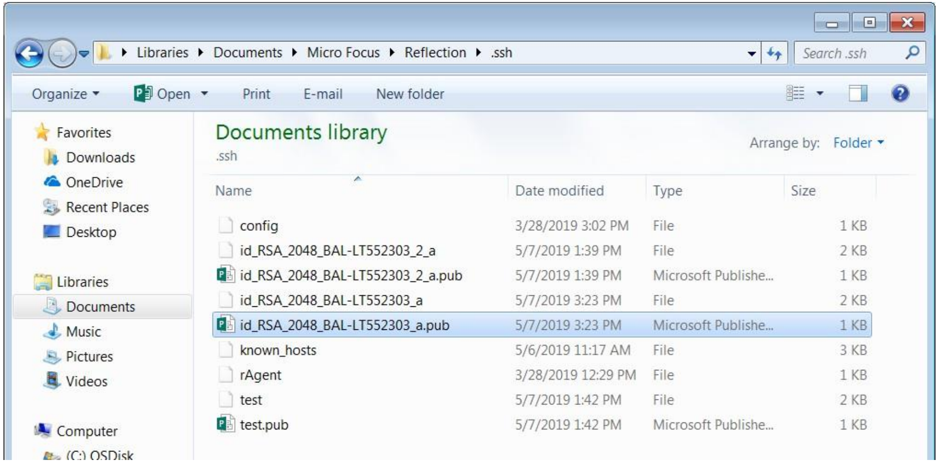
Because a password isn’t required at login, we are able to able to log in to servers from within scripts or automation tools that we need to run unattended. SSH public-key authentication relies on asymmetric

cryptographic algorithms that generate a pair of separate keys (a key pair), one "private" and the other "public". You keep the private key a secret and store it on the computer you use to connect to the remote system

1. Create FTP connection to the cloud. This tool enables to move Jar file to the virtual machine. Click New Site, the following window will open. Enter the IP address of the virtual machine. Leave port default value

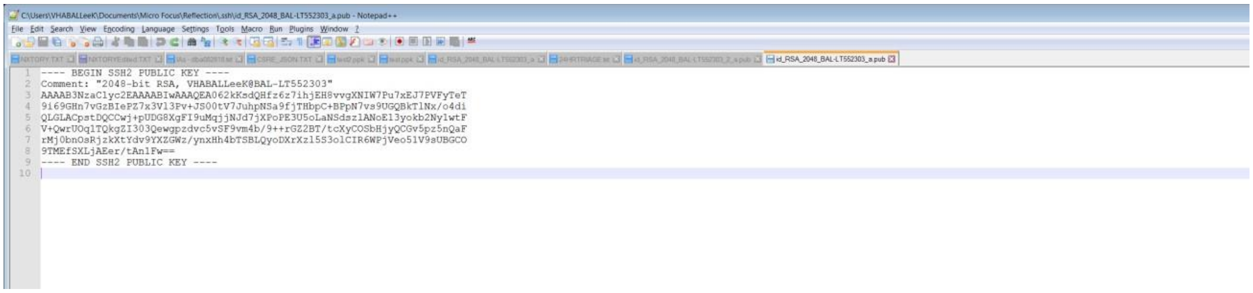


2. Find the key you just created. It will be in the folder: C:\Users\{username}\Documents\Micro Focus\Reflection\.ssh
3. Open the file using a text editor that is the version WITH the .pub extension. (Note – Use the "Open With" option and choose your text editor)

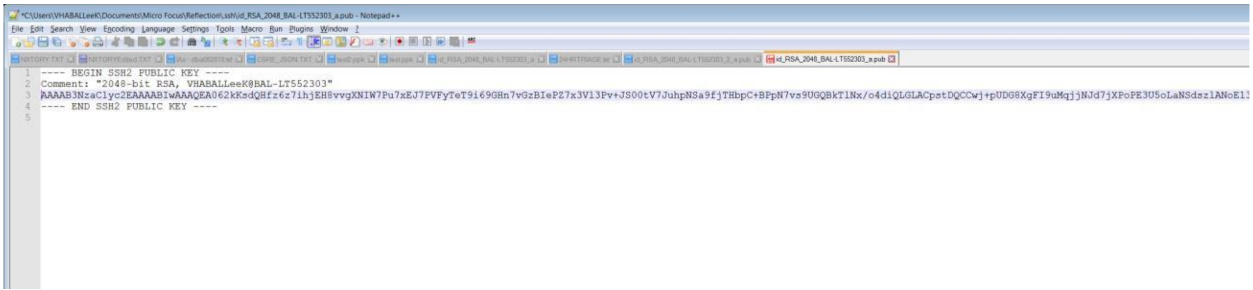


Name	Date modified	Type	Size
config	3/28/2019 3:02 PM	File	1 KB
id_RSA_2048_BAL-LT552303_2_a	5/7/2019 1:39 PM	File	2 KB
id_RSA_2048_BAL-LT552303_2_a.pub	5/7/2019 1:39 PM	Microsoft Publishe...	1 KB
id_RSA_2048_BAL-LT552303_a	5/7/2019 3:23 PM	File	2 KB
id_RSA_2048_BAL-LT552303_a.pub	5/7/2019 3:23 PM	Microsoft Publishe...	1 KB
known_hosts	5/6/2019 11:17 AM	File	3 KB
rAgent	3/28/2019 12:29 PM	File	1 KB
test	5/7/2019 1:42 PM	File	2 KB
test.pub	5/7/2019 1:42 PM	Microsoft Publishe...	1 KB

4. Using the text editor, CAREFULLY put all the hexadecimal characters on one line.

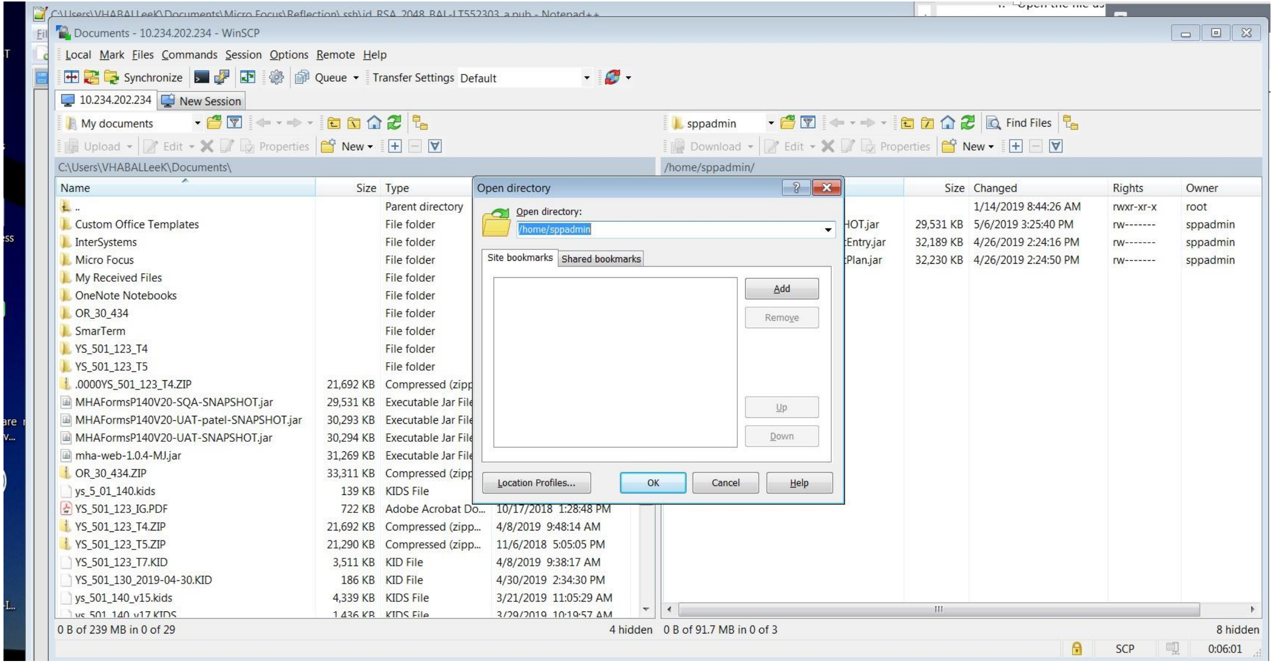

C:\Users\VHABALLeeK\Documents\Micro Focus\Reflection\.ssh\id_RSA_2048_BAL-LT552303_a.pub - Notepad++

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "2048-bit RSA, VHABALLeeK@BAL-LT552303"
AAAAB3NzaC1yc2EAAAABIwAAAQEA062kKsdQHfz6z7ihjEH8vvgXNIW7Pu7xEJ7PVFyTeT
9i69GHn7vGzBIePZ7x3V13Pv+JS00tV7JuhpNSa9fjTHbpC+BPpN7vs9UGQBkTlNx/o4di
QLGLACpstDQCCwj+pUDG8XgFI9uMqjjNJd7jXPoPE3U5oLaNSdsz1ANoE13yokb2Ny1wtF
V+QwrUOq1TQkgZI303Qewgpzdvc5vSF9vm4b/9++rGZ2BT/tcXyCOSbHjyQCGv5pz5nQaF
rMj0bnOsRjzkXtYdv9YXZGWz/ynxHh4bTSBLQyoDXrXz15S3olCIR6WPjVeo51V9sUBGCO
9TMEfSXLjAEer/tAnlFw==
---- END SSH2 PUBLIC KEY ----
```


*C:\Users\VHABALLeeK\Documents\Micro Focus\Reflection\.ssh\id_RSA_2048_BAL-LT552303_a.pub - Notepad++

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "2048-bit RSA, VHABALLeeK@BAL-LT552303"
AAAAB3NzaC1yc2EAAAABIwAAAQEA062kKsdQHfz6z7ihjEH8vvgXNIW7Pu7xEJ7PVFyTeT9i69GHn7vGzBIePZ7x3V13Pv+JS00tV7JuhpNSa9fjTHbpC+BPpN7vs9UGQBkTlNx/o4diQLGLACpstDQCCwj+pUDG8XgFI9uMqjjNJd7jXPoPE3U5oLaNSdsz1ANoE13
---- END SSH2 PUBLIC KEY ----
```

5. Copy the string into your buffer.
6. Connect to the cloud server using WinSCP. Your default directory will be /home/sppadmin.
7. Change directory to the hidden subfolder .ssh by clicking on the blue /home/sppadmin/ bar.


Documents - 10.234.202.234 - WinSCP

Open directory:
/home/sppadmin

C:\Users\VHABALLeeK\Documents\

Name	Size	Type	Changed
..		Parent directory	
Custom Office Templates		File folder	
InterSystems		File folder	
Micro Focus		File folder	
My Received Files		File folder	
OneNote Notebooks		File folder	
OR_30_434		File folder	
SmarTerm		File folder	
YS_501_123_T4		File folder	
YS_501_123_T5		File folder	
.0000YS_501_123_T4.ZIP	21,692 KB	Compressed (zipp	
MHAFormsP140V20-SQA-SNAPSHOT.jar	29,531 KB	Executable Jar File	
MHAFormsP140V20-UAT-patel-SNAPSHOT.jar	30,293 KB	Executable Jar File	
MHAFormsP140V20-UAT-SNAPSHOT.jar	30,294 KB	Executable Jar File	
mha-web-1.0.4-MJ.jar	31,269 KB	Executable Jar File	
OR_30_434.ZIP	33,311 KB	Compressed (zipp	
ys_5_01_140.kids	139 KB	KIDS File	
YS_501_123_IG.PDF	722 KB	Adobe Acrobat Do...	10/17/2018 1:28:48 PM
YS_501_123_T4.ZIP	21,692 KB	Compressed (zipp...	4/8/2019 9:48:14 AM
YS_501_123_T5.ZIP	21,290 KB	Compressed (zipp...	11/6/2018 5:05:05 PM
YS_501_123_T7.KID	3,511 KB	KID File	4/8/2019 9:38:17 AM
YS_501_130_2019-04-30.KID	186 KB	KID File	4/30/2019 2:34:30 PM
ys_501_140_v15.kids	4,339 KB	KIDS File	3/21/2019 11:05:29 AM
ys_501_140_v17.KIDS	1,436 KB	KIDS File	3/29/2019 10:19:57 AM

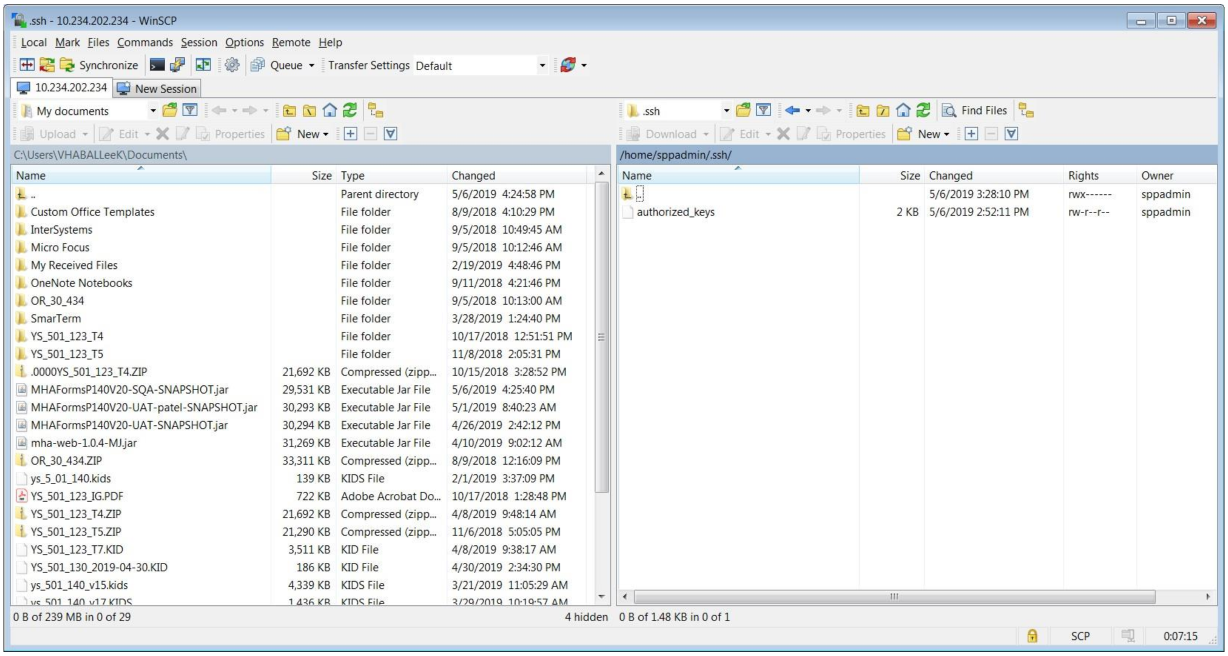
0 B of 239 MB in 0 of 29 — 4 hidden

/home/sppadmin/

Name	Size	Changed	Rights	Owner
		1/14/2019 8:44:26 AM	rwxr-xr-x	root
HOT.jar	29,531 KB	5/6/2019 3:25:40 PM	rw-------	sppadmin
Entry.jar	32,189 KB	4/26/2019 2:24:16 PM	rw-------	sppadmin
Plan.jar	32,230 KB	4/26/2019 2:24:50 PM	rw-------	sppadmin

0 B of 91.7 MB in 0 of 3 — 8 hidden

8. Add to the end of the directory string /.ssh



.ssh - 10.234.202.234 - WinSCP
Local Mark Files Commands Session Options Remote Help
Synchronize Queue Transfer Settings Default
10.234.202.234 New Session
My documents
Upload Edit Properties New
.ssh
Find Files
Download Edit Properties New

C:\Users\VHABALLeeK\Documents\

Name	Size	Type	Changed
..		Parent directory	5/6/2019 4:24:58 PM
Custom Office Templates		File folder	8/9/2018 4:10:29 PM
InterSystems		File folder	9/5/2018 10:49:45 AM
Micro Focus		File folder	9/5/2018 10:12:46 AM
My Received Files		File folder	2/19/2019 4:48:46 PM
OneNote Notebooks		File folder	9/11/2018 4:21:46 PM
OR_30_434		File folder	9/5/2018 10:13:00 AM
SmarTerm		File folder	3/28/2019 1:24:40 PM
YS_501_123_T4		File folder	10/17/2018 12:51:51 PM
YS_501_123_T5		File folder	11/8/2018 2:05:31 PM
.0000YS_501_123_T4.ZIP	21,692 KB	Compressed (zipp...	10/15/2018 3:28:52 PM
MHAFormsP140V20-SQA-SNAPSHOT.jar	29,531 KB	Executable Jar File	5/6/2019 4:25:40 PM
MHAFormsP140V20-UAT-patel-SNAPSHOT.jar	30,293 KB	Executable Jar File	5/1/2019 8:40:23 AM
MHAFormsP140V20-UAT-SNAPSHOT.jar	30,294 KB	Executable Jar File	4/26/2019 2:42:12 PM
mha-web-1.0.4-MJ.jar	31,269 KB	Executable Jar File	4/10/2019 9:02:12 AM
OR_30_434.ZIP	33,311 KB	Compressed (zipp...	8/9/2018 12:16:09 PM
ys_5_01_140.kids	139 KB	KIDS File	2/1/2019 3:37:09 PM
YS_501_123_IG.PDF	722 KB	Adobe Acrobat Do...	10/17/2018 1:28:48 PM
YS_501_123_T4.ZIP	21,692 KB	Compressed (zipp...	4/8/2019 9:48:14 AM
YS_501_123_T5.ZIP	21,290 KB	Compressed (zipp...	11/6/2018 5:05:05 PM
YS_501_123_T7.KID	3,511 KB	KID File	4/8/2019 9:38:17 AM
YS_501_130_2019-04-30.KID	186 KB	KID File	4/30/2019 2:34:30 PM
ys_501_140_v15.kids	4,339 KB	KIDS File	3/21/2019 11:05:29 AM
ys_501_140_v17.KIDS	1,436 KB	KIDS File	3/29/2019 10:19:57 AM

0 B of 239 MB in 0 of 29 4 hidden

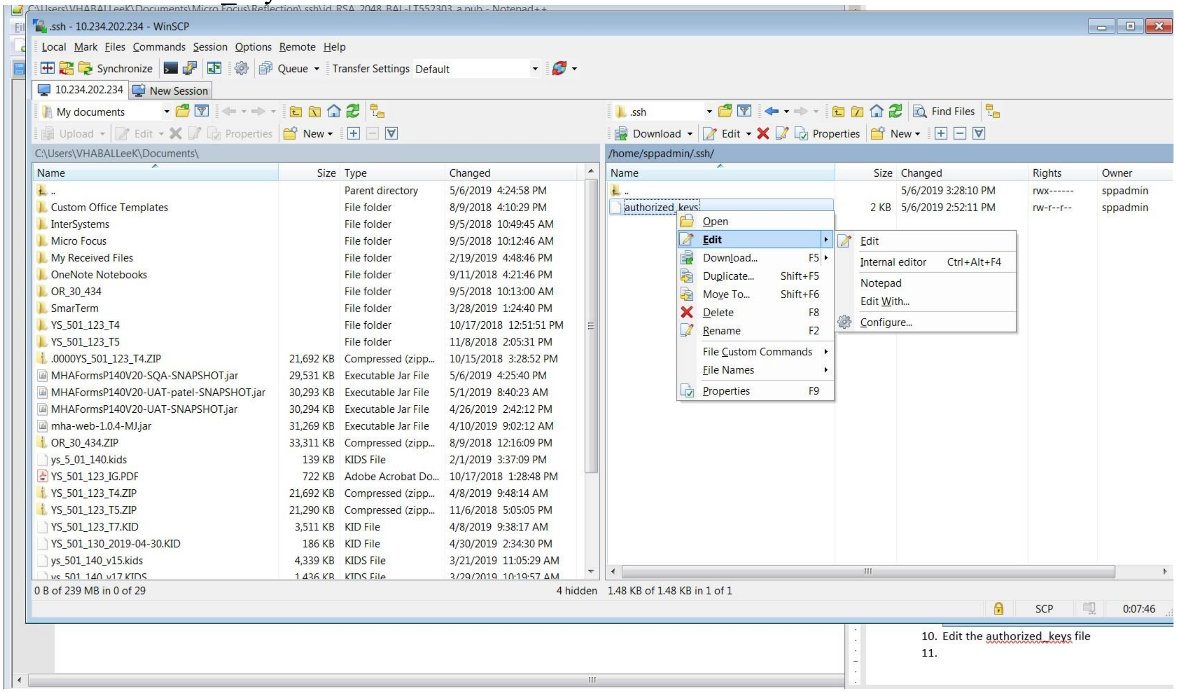
/home/sppadmin/.ssh/

Name	Size	Changed	Rights	Owner
..		5/6/2019 3:28:10 PM	rwx------	sppadmin
authorized_keys	2 KB	5/6/2019 2:52:11 PM	rw-r--r--	sppadmin

0 B of 1.48 KB in 0 of 1

SCP 0:07:15

9. Edit the authorized_keys file



C:\Users\VHABALLeeK\Documents\Micro Focus\Reflection\.ssh\id_RSA_2048_BAL-LT552303_a.pub - Notepad++

.ssh - 10.234.202.234 - WinSCP
Local Mark Files Commands Session Options Remote Help
Synchronize Queue Transfer Settings Default
10.234.202.234 New Session
My documents
Upload Edit Properties New
.ssh
Find Files
Download Edit Properties New
Open
Edit
Download... F5
Duplicate... Shift+F5
Move To... Shift+F6
Delete F8
Rename F2
File Custom Commands
File Names
Properties F9
Edit
Internal editor Ctrl+Alt+F4
Notepad
Edit With...
Configure...

C:\Users\VHABALLeeK\Documents\

Name	Size	Type	Changed
..		Parent directory	5/6/2019 4:24:58 PM
Custom Office Templates		File folder	8/9/2018 4:10:29 PM
InterSystems		File folder	9/5/2018 10:49:45 AM
Micro Focus		File folder	9/5/2018 10:12:46 AM
My Received Files		File folder	2/19/2019 4:48:46 PM
OneNote Notebooks		File folder	9/11/2018 4:21:46 PM
OR_30_434		File folder	9/5/2018 10:13:00 AM
SmarTerm		File folder	3/28/2019 1:24:40 PM
YS_501_123_T4		File folder	10/17/2018 12:51:51 PM
YS_501_123_T5		File folder	11/8/2018 2:05:31 PM
.0000YS_501_123_T4.ZIP	21,692 KB	Compressed (zipp...	10/15/2018 3:28:52 PM
MHAFormsP140V20-SQA-SNAPSHOT.jar	29,531 KB	Executable Jar File	5/6/2019 4:25:40 PM
MHAFormsP140V20-UAT-patel-SNAPSHOT.jar	30,293 KB	Executable Jar File	5/1/2019 8:40:23 AM
MHAFormsP140V20-UAT-SNAPSHOT.jar	30,294 KB	Executable Jar File	4/26/2019 2:42:12 PM
mha-web-1.0.4-MJ.jar	31,269 KB	Executable Jar File	4/10/2019 9:02:12 AM
OR_30_434.ZIP	33,311 KB	Compressed (zipp...	8/9/2018 12:16:09 PM
ys_5_01_140.kids	139 KB	KIDS File	2/1/2019 3:37:09 PM
YS_501_123_IG.PDF	722 KB	Adobe Acrobat Do...	10/17/2018 1:28:48 PM
YS_501_123_T4.ZIP	21,692 KB	Compressed (zipp...	4/8/2019 9:48:14 AM
YS_501_123_T5.ZIP	21,290 KB	Compressed (zipp...	11/6/2018 5:05:05 PM
YS_501_123_T7.KID	3,511 KB	KID File	4/8/2019 9:38:17 AM
YS_501_130_2019-04-30.KID	186 KB	KID File	4/30/2019 2:34:30 PM
ys_501_140_v15.kids	4,339 KB	KIDS File	3/21/2019 11:05:29 AM
ys_501_140_v17.KIDS	1,436 KB	KIDS File	3/29/2019 10:19:57 AM

0 B of 239 MB in 0 of 29 4 hidden

/home/sppadmin/.ssh/

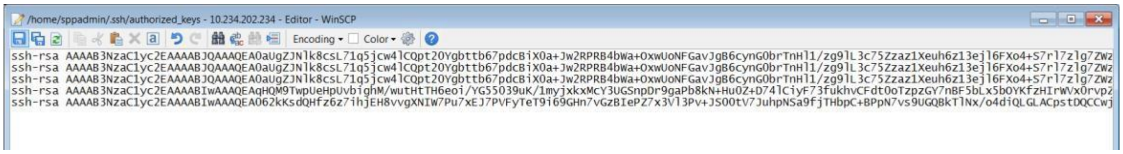
Name	Size	Changed	Rights	Owner
..		5/6/2019 3:28:10 PM	rwx------	sppadmin
authorized_keys	2 KB	5/6/2019 2:52:11 PM	rw-r--r--	sppadmin

1.48 KB of 1.48 KB in 1 of 1

SCP 0:07:46

10. Edit the authorized_keys file
11.

10. Add on to the end of the file:
    a. Type in ssh-rsa
    b. Paste in your string
    c. Press the Save icon

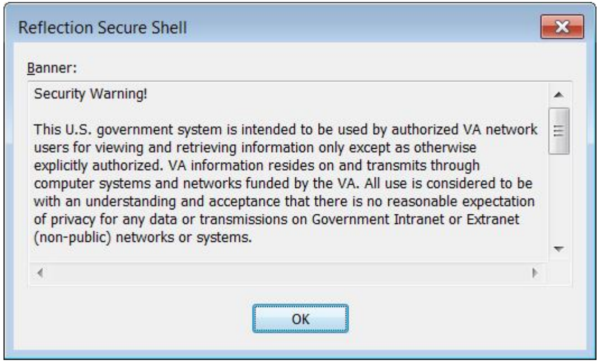


/home/sppadmin/.ssh/authorized_keys - 10.234.202.234 - Editor - WinSCP
Encoding
Color

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEA0aUgZJNlk8csL71q5jcw4lCQpt20Ygbttb67pdcBiX0a+Jw2RPRB4bWa+OxwUoNFGavJgB6cynG0brTnHl1/zg9lL3c75Zzaz1Xeuh6z13ejl6FXo4+S7rl7zlg7ZWz
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEA0aUgZJNlk8csL71q5jcw4lCQpt20Ygbttb67pdcBiX0a+Jw2RPRB4bWa+OxwUoNFGavJgB6cynG0brTnHl1/zg9lL3c75Zzaz1Xeuh6z13ejl6FXo4+S7rl7zlg7ZWz
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEA0aUgZJNlk8csL71q5jcw4lCQpt20Ygbttb67pdcBiX0a+Jw2RPRB4bWa+OxwUoNFGavJgB6cynG0brTnHl1/zg9lL3c75Zzaz1Xeuh6z13ejl6FXo4+S7rl7zlg7ZWz
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAqHQM9TwpUeHpUvbighM/wutHtTH6eoi/YG55039uK/1myjxkxMcY3UGSnpDr9gaPb8kN+Hu0Z+D74lCiyF73fukhvCFdt0oTzpzGY7nBF5bLx5bOYKfzHIrWVx0rvpZ
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA062kKsdQHfz6z7ihjEH8vvgXNIW7Pu7xEJ7PVFyTeT9i69GHn7vGzBIePZ7x3Vl3Pv+JS00tV7JuhpNSa9fjTHbpC+BPpN7vs9UGQBkTlNx/o4diQLGLACpstDQCCwj
```

11. Close WinSCP
12. Connect to the cloud server
    1. Go to Reflections

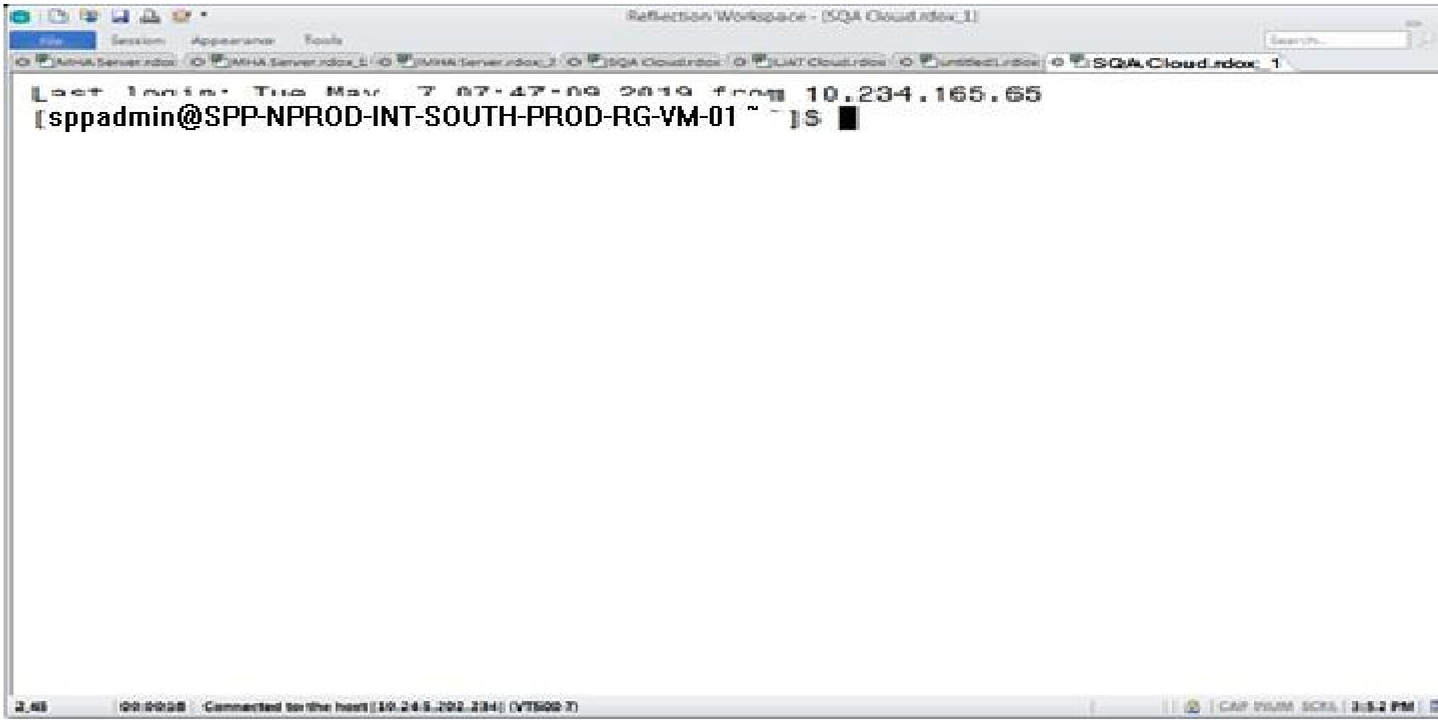
2. Use the connection you configured to the cloud server.
3. A Reflections Secure Shell popup should appear. Click OK



Security Warning!

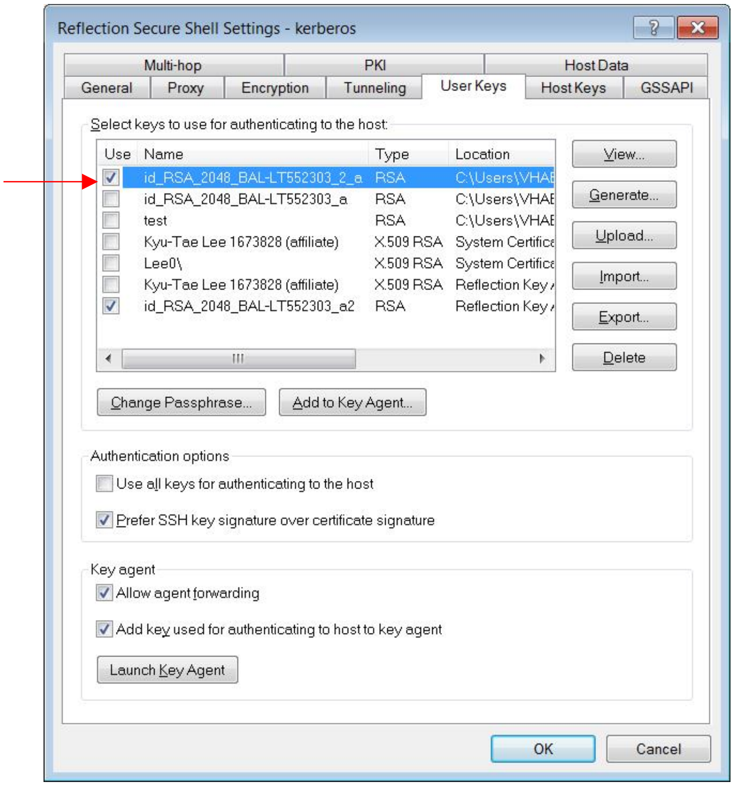
This U.S. government system is intended to be used by authorized VA network users for viewing and retrieving information only except as otherwise explicitly authorized. VA information resides on and transmits through computer systems and networks funded by the VA. All use is considered to be with an understanding and acceptance that there is no reasonable expectation of privacy for any data or transmissions on Government Intranet or Extranet (non-public) networks or systems.

4. You should then be logged in


Reflection Workspace - [SQA Cloud.rdox_1]
File
Session
Appearance
Tools
SQA Cloud.rdox_1
Connected to the host [10.245.202.234] (VT500 7)
CAP NUM SCRL

```
Last login: Tue May  7 07:47:09 2019 from 10.234.165.65
[sppadmin@SPP-NPROD-INT-SOUTH-PROD-RG-VM-01 ~ ]$
```

5. If it prompts for a password, then the key configuration is incorrect. Make sure that in your connection settings that your new key is checked:



Select keys to use for authenticating to the host:

Use	Name	Type	Location
☑	id_RSA_2048_BAL-LT552303_2_a	RSA	C:\Users\VHAE
□	id_RSA_2048_BAL-LT552303_a	RSA	C:\Users\VHAE
□	test	RSA	C:\Users\VHAE
□	Kyu-Tae Lee 1673828 (affiliate)	X.509 RSA	System Certifica
□	Lee0\	X.509 RSA	System Certifica
□	Kyu-Tae Lee 1673828 (affiliate)	X.509 RSA	Reflection Key A
☑	id_RSA_2048_BAL-LT552303_a2	RSA	Reflection Key A

Authentication options

□ Use all keys for authenticating to the host

☑ Prefer SSH key signature over certificate signature

Key agent

☑ Allow agent forwarding

☑ Add key used for authenticating to host to key agent

Please contact the administrator for private-key.ppk

7.5 Software Installation

Connect to the cloud server as shown above (13)

1. **Login as root user**:
   $ sudo su –

2. **Update the server**

```
yum update -y  --exclude=BESAgent  --exclude=CentrifyDC  --exclude=CentrifyDC-curl  --
exclude=CentrifyDC-openldap  --exclude=CentrifyDC-openssh--exclude=CentrifyDC-
openssl >/tmp/yum-out 2>&1 &
```

3. **Install GCC**

```
# yum install -y gcc-c++  make
Loaded plugins: product-id, rhnplugin, search-disabled-repos, subscription-:manager
This system is not registered with RHN Classic or Red Hat Satellite.
You can use rhn_register to register.
Red Hat Satellite or RHN Classic support will be disabled.
rhel-7-server-rpms                                   | 3.5 kB     00:00
(1/3): rhel-7-server-rpms/7Server/x86_64/group          | 856 kB  00:01
(2/3): rhel-7-server-rpms/7Server/x86_64/updateinfo     | 3.1 MB  00:01
(3/3): rhel-7-server-rpms/7Server/x86_64/primary_db     | 52 MB 00:02
Package 1:make-3.82-23.el7.x86_64 already installed and latest version
Resolving Dependencies
--> Running transaction check
```

```
---> Package gcc-c++.x86_64 0:4.8.5-36.el7 will be installed
--> Processing Dependency: gcc = 4.8.5-36.el7 for package: gcc-c++-4.8.5-36.el7.
x86_64
--> Processing Dependency: libstdc++ = 4.8.5-36.el7 for package: gcc-c++-4.8.5-3
6.el7.x86_64
--> Processing Dependency: libstdc++-devel = 4.8.5-36.el7 for package: gcc-c++-4
.8.5-36.el7.x86_64
--> Processing Dependency: libmpc.so.3()(64bit) for package: gcc-c++-4.8.5-36.el
7.x86_64
--> Processing Dependency: libmpfr.so.4()(64bit) for package: gcc-c++-4.8.5-36.e
l7.x86_64
--> Running transaction check
---> Package gcc.x86_64 0:4.8.5-36.el7 will be installed
--> Processing Dependency: cpp = 4.8.5-36.el7 for package: gcc-4.8.5-36.el7.x86_
64
--> Processing Dependency: libgomp = 4.8.5-36.el7 for package: gcc-4.8.5-36.el7.
x86_64
--> Processing Dependency: glibc-devel >= 2.2.90-12 for package: gcc-4.8.5-36.el
7.x86_64
--> Processing Dependency: libgcc >= 4.8.5-36.el7 for package: gcc-4.8.5-36.el7.
x86_64
---> Package libmpc.x86_64 0:1.0.1-3.el7 will be installed
---> Package libstdc++.x86_64 0:4.8.5-28.el7_5.1 will be updated
---> Package libstdc++.x86_64 0:4.8.5-36.el7 will be an update
---> Package libstdc++-devel.x86_64 0:4.8.5-36.el7 will be installed
---> Package mpfr.x86_64 0:3.1.1-4.el7 will be installed
--> Running transaction check
---> Package cpp.x86_64 0:4.8.5-36.el7 will be installed
---> Package glibc-devel.x86_64 0:2.17-260.el7 will be installed
--> Processing Dependency: glibc = 2.17-260.el7 for package: glibc-devel-2.17-26
0.el7.x86_64
--> Processing Dependency: glibc-headers = 2.17-260.el7 for package: glibc-devel
-2.17-260.el7.x86_64
--> Processing Dependency: glibc-headers for package: glibc-devel-2.17-260.el7.x
86_64
---> Package libgcc.x86_64 0:4.8.5-28.el7_5.1 will be updated
---> Package libgcc.x86_64 0:4.8.5-36.el7 will be an update
---> Package libgomp.x86_64 0:4.8.5-28.el7_5.1 will be updated
---> Package libgomp.x86_64 0:4.8.5-36.el7 will be an update
--> Running transaction check
---> Package glibc.x86_64 0:2.17-222.el7 will be updated
--> Processing Dependency: glibc = 2.17-222.el7 for package: glibc-common-2.17-2
22.el7.x86_64
---> Package glibc.x86_64 0:2.17-260.el7 will be an update
---> Package glibc-headers.x86_64 0:2.17-260.el7 will be installed
--> Processing Dependency: kernel-headers >= 2.2.1 for package: glibc-headers-2.
17-260.el7.x86_64
--> Processing Dependency: kernel-headers for package: glibc-headers-2.17-260.el
7.x86_64

--> Running transaction check
```

```
---> Package glibc-common.x86_64 0:2.17-222.el7 will be updated
---> Package glibc-common.x86_64 0:2.17-260.el7 will be an update
---> Package kernel-headers.x86_64 0:3.10.0-957.el7 will be installed
--> Finished Dependency Resolution
--> Finding unneeded leftover dependencies
Found and removing 0 unneeded dependencies
Dependencies Resolved
==================================================================
==========
 Package          Arch      Version          Repository           Size
==================================================================
==========
Installing:
 gcc-c++          x86_64    4.8.5-36.el7      rhel-7-server-rpms    7.2 M
Installing for dependencies:
 cpp             x86_64    4.8.5-36.el7     rhel-7-server-rpms    6.0 M
 gcc             x86_64    4.8.5-36.el7     rhel-7-server-rpms     16 M
 glibc-devel       x86_64    2.17-260.el7     rhel-7-server-rpms    1.1 M
 glibc-headers      x86_64    2.17-260.el7      rhel-7-server-rpms    683 k
 kernel-headers    x86_64    3.10.0-957.el7   rhel-7-server-rpms    8.0 M
libmpc            x86_64    1.0.1-3.el7      rhel-7-server-rpms     51 k
libstdc++-devel   x86_64    4.8.5-36.el7     rhel-7-server-rpms1.5 M
mpfr             x86_64    3.1.1-4.el7      rhel-7-server-rpms    203 k
Updating for dependencies:
 glibc            x86_64    2.17-260.el7     rhel-7-server-rpms    3.6 M
glibc-common      x86_64    2.17-260.el7     rhel-7-server-rpms     11 M
libgcc           x86_64    4.8.5-36.el7     rhel-7-server-rpms    102 k
libgomp           x86_64    4.8.5-36.el7     rhel-7-server-rpms    157 k
libstdc++         x86_64    4.8.5-36.el7     rhel-7-server-rpms    304 k
Transaction
Summary==========================================================
===============
Install 1 Package (+8 Dependent packages)
Upgrade          ( 5 Dependent packages)
Total download size: 56 M
Downloading packages:
Delta RPMs disabled because /usr/bin/applydeltarpm not installed.
(1/14): cpp-4.8.5-36.el7.x86_64.rpm                  | 6.0 MB   00:01
(2/14): gcc-4.8.5-36.el7.x86_64.rpm                  |  16 MB   00:01
…………
 (14/14): mpfr-3.1.1-4.el7.x86_64.rpm                 | 203 kB  00:00
------------------------------------------
Total                              8.5 MB/s | 56 MB 00:06
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Updating   : libgcc-4.8.5-36.el7.x86_64                     1/19
  Updating   : glibc-2.17-260.el7.x86_64                      2/19
```

```
……………. Installing : glibc-headers-2.17-260.el7.x86_64
[######################################   ] 19/19
```

4. **Install Node.js**

   a. Install Node.js YUM repository

   ```
   # yum install -y gcc-c++  make
   # curl -sL https://rpm.nodesource.com/setup_8.x | sudo -E bash –
   ```

   b. Install Node.js

   ```
   # sudo yum install -y nodejs
   ```

   c. Check Node.js and NPM version

   ```
   # node -v
    => v8.15.0
   #npm -v
   =>6.4.1
   ```

5. **Install Yarn package management**

   ```
   # curl -sL https://dl.yarnpkg.com/rpm/yarn.repo | sudo tee /etc/yum.repos.d/yarn.repo


   # yum install yarn
   ```

6. **Docker**

   Docker is free and open-source software. It automates the deployment of any application as a lightweight, portable, self-sufficient container that will run virtually anywhere. Typically, you develop software on your laptop/desktop. You can build a container with your app, and it can test run on your computer. It will scale in cloud, VM, and more.

   A. **Install Docker**

      a.
      ```
      # yum remove docker docker-common docker-selinux docker-engine-selinux docker-engine docker-ce
      ```

      b.
      ```
      # yum install -y yum-utils device-mapper-persistent-data lvm2
          # yum-config-manager --add-repo
      ```

      c. vi /etc/yum/pluginconf.d/search-disabled-repos.conf modify notify_only=0

      d.
      ```
      # yum install docker-ce  --skip-broken
      ```

   B. **Start Docker**

      ```
      systemctl start docker.service
      ```

   C. **Docker Status**

   ```
   #systemctl status docker.service
   => //? docker.service - Docker Application Container Engine
   // Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; vendor preset: disabled)
   // Active: active (running) since Wed 2018-11-21 13:43:34 CST; 26s ago
   //     Docs: https://docs.docker.com
   ```

```
// Main PID: 80981 (dockerd)
//    Tasks: 27
// Memory: 51.7M
// CGroup: /system.slice/docker.service
//          +-80981 /usr/bin/dockerd -H unix://
//          +-81007 containerd --config /var/run/docker/containerd/containerd....
Nov 21 13:43:33 SPP-NPROD-INT-SOUTH-PROD-RGdockerd[80981]: time="2018-11-
21T13:...
Nov 21 13:43:33 SPP-NPROD-INT-SOUTH-PROD-RGdockerd[80981]: time="2018-11-
21T13:...
Nov 21 13:43:33 SPP-NPROD-INT-SOUTH-PROD-RGdockerd[80981]: time="2018-11-
21T13:...
Nov 21 13:43:33 SPP-NPROD-INT-SOUTH-PROD-RGdockerd[80981]: time="2018-11-
21T13:...
Nov 21 13:43:33 SPP-NPROD-INT-SOUTH-PROD-RGdockerd[80981]: time="2018-11-
21T13:...
Nov 21 13:43:34 SPP-NPROD-INT-SOUTH-PROD-RG dockerd[80981]: time="2018-11-
21T13:...
Nov 21 13:43:34 SPP-NPROD-INT-SOUTH-PROD-RGdockerd[80981]: time="2018-11-
21T13:...
Nov 21 13:43:34 SPP-NPROD-INT-SOUTH-PROD-RGdockerd[80981]: time="2018-11-
21T13:...
Nov 21 13:43:34 SPP-NPROD-INT-SOUTH-PROD-RGdockerd[80981]: time="2018-11-
21T13:...
Nov 21 13:43:34 SPP-NPROD-INT-SOUTH-PROD-RGsystemd[1]: Started Docker
Applicati...
Hint: Some lines were ellipsized, use -l to show in full.
```

D. Stop Docker

```
# systemctl stop docker.service
```

E. Restart Docker

```
# systemctl restart docker.service
```

7.5 Deploy Production Jar to the cloud (IOC/Production)

1. Rename <Jar file> to patientEntry<env>.jar for Patient Entry and staffEntry<env>.jar for Staff Entry aka Patient Plan
2. Move Production Jar file (patientEntry<env>.jar / staffEntry<env>.jar) to /home/sppadmin location in VM as explained above using WINSCP
3. Login as sudo: # sudo su <Password>. Please contact administrator for password.
4. Navigate to /workspace/virtualization/encryptedPassword. Vim settings.env file and change the value for jasypt.encryptor.password
   jasypt.encryptor.password=<value>, save the file.
5. Run the Production Jar in docker

   Navigate to /workspace/virtualization/<application>/<env>

   ```
   # cp /home/sppadmin/<Jar File> .
   ```

Patient Entry:

```
##Navigate to /workspace/ virtualization/patient-entry

cd /workspace/ virtualization//patient-entry

cp /home/sppadmin/ patientEntry<env>.jar .

##Create docker image file:

 docker build -t patiententry --build-arg jar-file=patientEntry<env>.jar . --no-cache

## Run Docker container
docker run -dit -p<proper_port>:8443 --env-
file=/workspace/virtualization/encryptedPassword/settings.env -v
"$(pwd)":/src –name=patiententry --cpus=3 --memory=6144m --memory-swap=7168m
--restart always patiententry

docker ps
```

You will see status like:

```
CONTAINER ID      IMAGE           COMMAND              CREATED         STATUS
PORTS                 NAMES

ff4de5a3ef25      patiententry                  "/bin/sh -c 'java -j…"          4 days ago        Up 4 days
          0.0.0.0:8082->8443/tcp   patiententry
```

Staff Entry (Patient Plan):

```
##Navigate to /workspace/ virtualization//patient-plan

cd /workspace/ virtualization//patient-plan

cp /home/sppadmin/ staffEntryIOC.jar.

## Create docker image file:

 docker build -t staffentry --build-arg jar-file=staffEntry.jar . --no-cache

## Run Docker Container
docker run -dit -p<proper_port>:8443 --env-
file=/workspace/virtualization/encryptedPassword/settings.env -v
"$(pwd)":/src –name=staffentry --cpus=3 --memory=6144m --memory-swap=7168m -
-restart always staffentry

docker ps
```

You will see status like:

```
CONTAINER ID      IMAGE           COMMAND              CREATED         STATUS
PORTS                   NAMES

31be835a4f61      staffentry   "/bin/sh -c 'java -j…"             4 days ago            Up 4 days
          0.0.0.0:8083->8443/tcp    staffentry
```

8. Build Web Application

*This step will not be done by the VistA installer

8.1 Preparing the Application for Production

The project leverages the Maven to build the application. The project is structured in multiple modules with the mha-web-parent project being where the application is built from.

7.4 Prerequisite

The git client is installed, the user has Github access to the EPMO organization, and the user has pulled down the spp_mha_web project.

7.5 Building the Application

The application is built from the mha-web/mha-web-parent directly. For a production ready application, use the command *mvn clean install -PbuildAll -DskipTests*. This will build all the jars with production flags for the UI so that the code is minimized and additional logging is disabled. Three jars are built by this command, mha-patient-web-<version>-SNAPSHOT.jar, mha-clinician-web-<version>-SNAPSHOT.jar, and mha-admin-web-<version>-SNAPSHOT.jar.

7.6 Properties and Data Configuration

Properties files are a way of controlling what settings are active at a given time. Our properties files control the following behavior:

- Server Port
- Server key-store & trust-store settings (files, passwords, protocols and settings)
- MySQL database connection settings
- Logging settings
- JWT Secret
- Password encryption secret

Properties files reside in the mha-web/mha-env-config project. Each properties file is a duplicate of the others with settings specific to the environment of the folder it resides in. For IOC/Production, the template file in the ioc folder should be used and filled in according to that environment. **Keys and passwords should never be shared between development and production environments.**

The local properties file used for local development is packaged in the jar. Placing an environment specific properties file on the classpath of the jar will override those settings. In this way we can use the same jar for all environments without rebuilding the jar.

7.7 Encrypted Passwords

Passwords can be encrypted/decrypted with a library called jasypt. For IOC/Production environments, generate a random 256bit key using the Jasypt library or any online tool. Then use the key with the EncodePassword.java file in /mha-web/mha-model/src/test/java/com/va/med/mha/model/security to encrypt the passwords. Copy and paste the encrypted passwords into the properties file. Encrypt the passwords for any datasources. The password for the keystore cannot be encrypted.

To encrypt a value use the following command:

```
java -cp ~/.m2/repository/org/jasypt/jasypt/1.9.3/jasypt-1.9.3.jar
org.jasypt.intf.cli.JasyptPBEStringEncryptionCLI input='<password_to_encrypt>' password=<encryption_key>
```

Take the outputted value and put it inside ENC() tags in the properties file. Make sure the encryption key you use in the command and the encryption key you have on your path are the same.

Also create a key for the system variable called jasypt.encryptor.password. This can be accomplished a few different ways. The easiest is to add the value to the system path via an environment variable. You can also set the variable on the terminal or script that you start the application in. Finally you can pass it as an argument in the command to start the application. To generate an encryption key, use a site like randomkeygen.com to generate a 256-bit key, preferably on a different machine. Copy the value generated and set it on the path in the desired way. For our cloud environments, this goes in the /workspace/virtualization/encryptedPassword/settings.env file that is used with the docker command to start the container.

7.8 Keystores

Create keystore with Certificate for IOC/Production. A different password should be used for Dev/IOC/Production environments. Put the name of the keystore along with the password in the properties file.

7.9 Enabling Strong Encryption

In order for encryption to work, support must potentially be added to the JRE. The JRE by default only ships with relatively weak encryption support to meet export control laws. Unlimited strength encryption must be added for the encryption set up below to work. Policy files to enable unlimited strength encryption can be downloaded here. Copy these files to the <JDK/JRE install directory>/jre/lib/security/policy/unlimited folder.

Note: As of Java 8 Update 161, unlimited strength encryption is enabled by default.

7.10 Encrypting/Decrypting Passwords

The application now uses encrypted passwords in order to protect access to the database. This requires some configuration in order to work. We use the Jasypt library to encrypt and decrypt the passwords outside and inside the application. The current unencrypted passwords are in the Resources directory. If these unencrypted passwords are every changed, they must be re-encrypted and replaced in the respective properties file in /mha-web/src/main/resources/ folder.

To set up the encryption, you must have the encryption key on the path for the application. This can be accomplished a few different ways. The easiest is to add the value to the system path via an environment variable. You can also set the variable on the terminal or script that you start the application in. Finally you can pass it as an argument in the command to start the application. To generate an encryption key, use a site like randomkeygen.com to generate a 256-bit key, preferably on a different machine. Copy the value generated and set it on the path in the desired way.

Then to encrypt a value use the following command:

```
java -cp ~/.m2/repository/org/jasypt/jasypt/1.9.3/jasypt-1.9.3.jar
org.jasypt.intf.cli.JasyptPBEStringEncryptionCLI input='<password_to_encrypt>' password=<encryption_key>
```

Take the outputted value and put it inside ENC() tags in the properties file. Make sure the encryption key you use in the command and the encryption key you have on your path are the same.

Note: *Once the production Jar file is created, we are ready deploy in the cloud. Please navigate to 7.5 of Cloud Setup*.

7.11 JWT Secret

A new secret key needs to be generated for dev, pre-prod, and production environments. This is a random 64 character string that can be generated manually or using an online generator.