Metasploit OVF Template

Deploying to VMware ESX and ESXi Servers

Last Updated 3/15/12

RAPID7

TABLE OF CONTENTS

About This Guide

Deploying the Metasploit OVF

Setting up the Virtual Machine

About This Guide

This guide provides instructions for you to set up a Metasploit OVF virtual machine on a VMware ESX or ESXi server. The following sections describe the audience, organization, and conventions used within this guide.

Target Audience

This guide is for IT and security professionals who use Metasploit Pro as a penetration testing solution.

Organization

This guide includes the following chapters:

- About this Guide
- Setting Up the Metasploit AMI for Amazon EC2

Document Conventions

The following table describes the conventions and formats that this guide uses:

Convention	Description
Command	Indicates buttons, UI controls, and fields. For example, "**Click Projects > New Project**."
Code	Indicates command line, code, or file directories. For example, "Enter the following: `chmod +x Desktop/metasploit-3.7.1-linux-x64-installer`."
Title	Indicates the title of a document or chapter name. For example, "For more information, see the *Metasploit Pro Installation Guide*."
Note	Indicates there is additional information about the topic.

Support

You can visit the Customer Center or e-mail the Rapid7 support team to submit questions and receive support for Metasploit Pro and Metasploit Express. To log in to the Customer Center, use the e-mail and password provided by Rapid7.

The following table describes the methods you can use to contact the Rapid7 support team.

Support Method	Contact Information
Customer Center	http://www.rapid7.com/customers/customer-login.jsp
E-mail	support@rapid7.com

There is not an official support team dedicated to the Metasploit Framework or Metasploit Community. If you are a Metasploit Community or Framework user, you can visit the Metasploit Community for support.

Required Credentials

The following table describes the credentials that you need to deploy the Metasploit OVF template and to access Metasploit Pro:

Account	Credentials
`Ubuntu VM`	`ubuntu:metasploit [password must be changed after the first log in]`
`Metasploit Pro`	`admin:[password provided after installation]`

Deploying the Metasploit OVF

OVF, or Open Virtualization Format, is an XML file that contains a virtual machine and a preconfigured template for the virtual machine. You can deploy an OVF template to create a virtual machine that contains the software that you want to run.

The Metasploit OVF template contains an Ubuntu system with an instance of Metasploit Pro. You can deploy the Metasploit OVF template on VMware ESX Server or ESXi Server. To deploy the Metasploit OVF, you can use a VMware infrastructure client, such as vSphere Client, on a system other than the one that hosts the ESX or ESXi Server.

Before You Begin

The following sections describe the requirements, resources, and applications that are necessary before you can deploy the OVF template.

Requirements

Before you can download and deploy the Metasploit OVF template, you must meet the following requirements:

- Have a VMware infrastructure client, such as vSphere client, installed on your system.
- Be familiar with Ubuntu and Metasploit Pro.

Resources

The following resources provide additional information to help you set up and the Metasploit OVF VM:

- VMWare Help
- Metasploit Community Site

Supported Applications

The Metasploit VM contains the following systems and applications:

- Ubuntu 10.04 LTS
- Metasploit Pro

Downloading the Metasploit OVF Zip

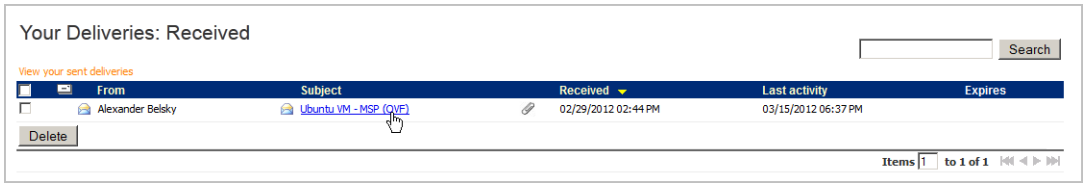
To obtain the Metasploit OVF VM, you must contact Rapid7 support to obtain the download link for the Metasploit OVF application package. The Rapid7 support team will e-mail you an FTP link to the OVF zip file.

When you click on the download link provided in the e-mail, the Rapid7 FTP site displays. Log in to the Rapid7 FTP site to download the file. If you do not have a Rapid7 account, you must create one. Visit the Rapid7 User Registration page to create an account.

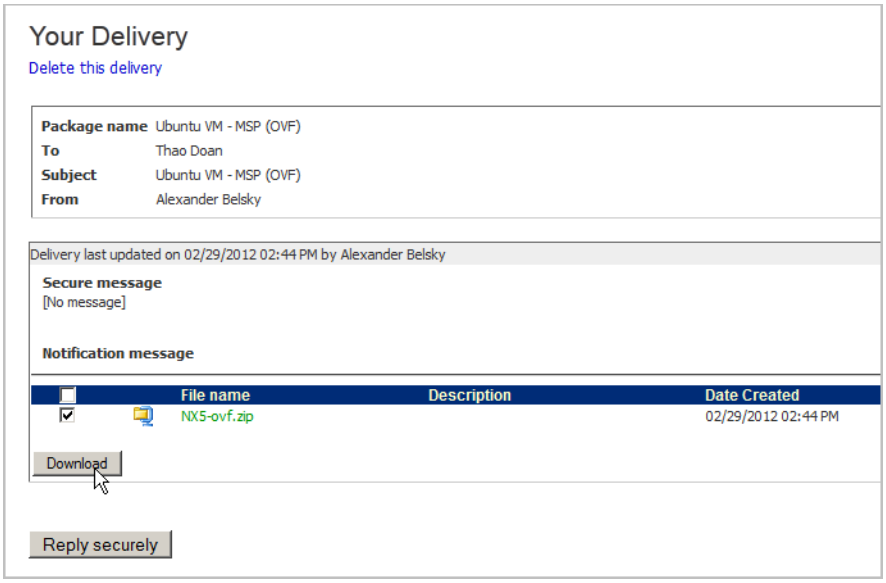
After you log in to the Rapid7 FTP site, follow these steps to download the Metasploit OVF zip:

1. Click the **Received** link.

2. The next page displays the deliveries that are available for you to download. Locate the delivery with the subject line “Ubuntu VM - MSP (OVF).”
3. Click the subject line. The delivery page displays with the OVF zip provided as an attachment.



4. Select the OVF zip file and click **Download**.



The zip file is approximately 1 GB. Download times may vary based on your network connection.

Validating the File

To ensure that the downloaded zip file is not corrupt, you may want to verify that the ISO image that you downloaded matches the ISO image on the FTP site. To do this, you need to perform a SHA1 check.

Windows

To verify the SHA1 hash, you need to download the sha1sum.exe program. Use the following link to download the sha1sum program: http://updates.metasploit.com/data/sha1sum.exe (signature).

Download and save the sha1sum program to the folder that contains the Metasploit OVM zip file.

After you download the sha1sum program, open the command line terminal. Enter the file path to the sha1sum program followed by the path to the Metasploit OVF zip file. Then, press **Enter**.

```
c:\> c:\users\username\Desktop\SHA\sha1sum.exe
c:\users\username\Desktop\SHA\metasploit_latest_ovf.zip
708573fffd188567322e13e192a2721c68ddff
```

Check the hash value with the SHA1 value from the FTP server.

Linux

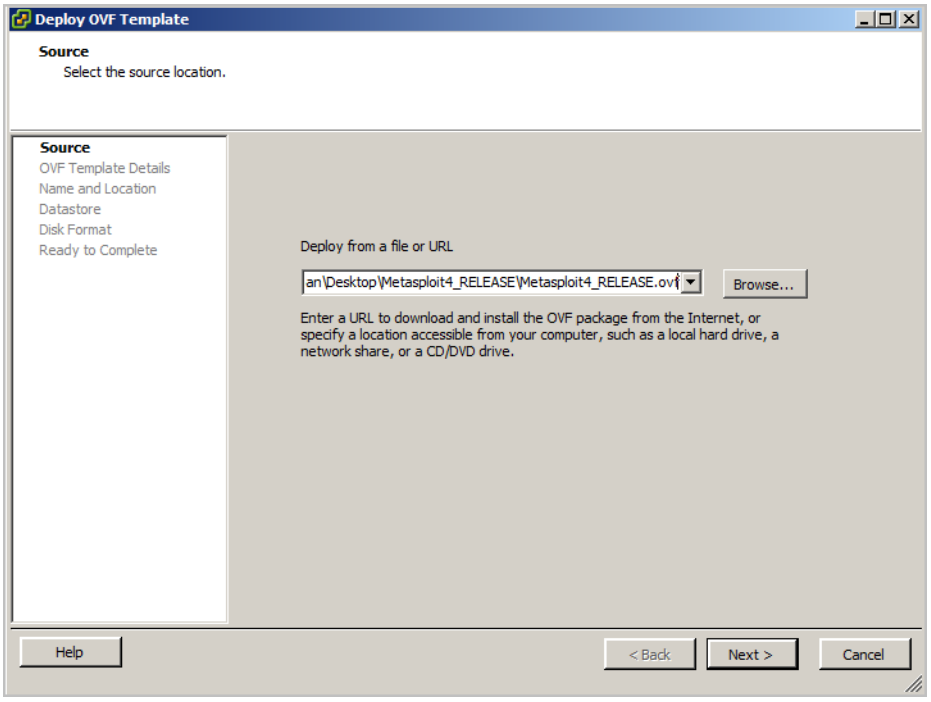
To verify the SHA1 hash, type the following command at the command line to calculate the SHA1 hash for the Metasploit OVM zip file: `sha1sum /path/to/file`. Replace `/path/to/file` with the full path to the Metasploit OVM zip file.

```
user@computer-name:~$ sha1sum NX5-ovf.zip
708573fffd188567322e13e192a2721c68ddff Metasploit_latest_ovf.zip
```

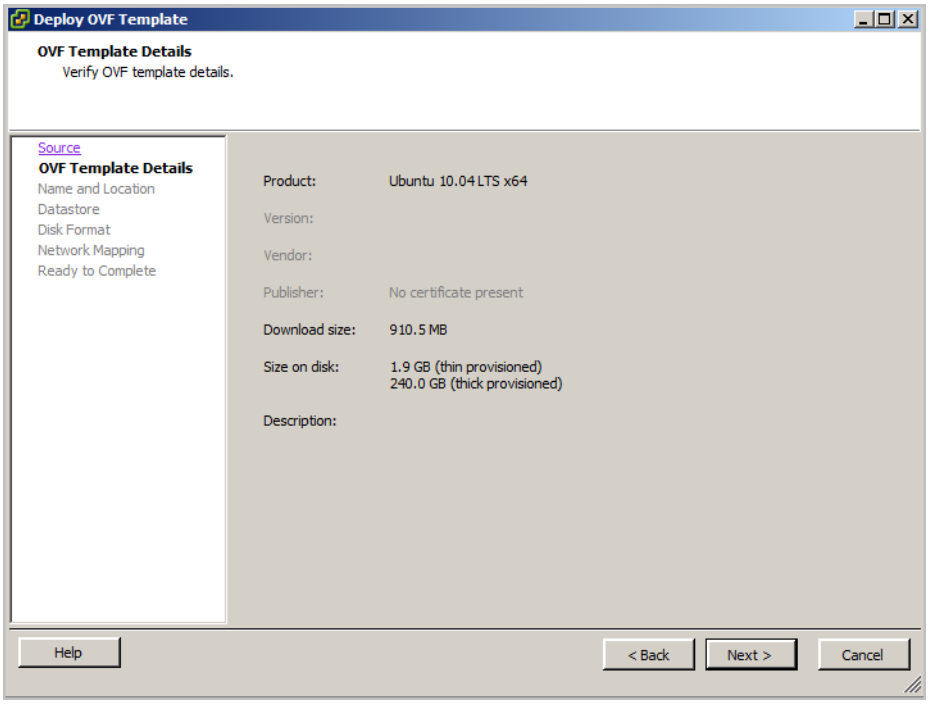
Deploying the Metasploit OVF to VMware ESX and ESXi Servers

The following instructions describe how to deploy an OVF template with vSphere Client.

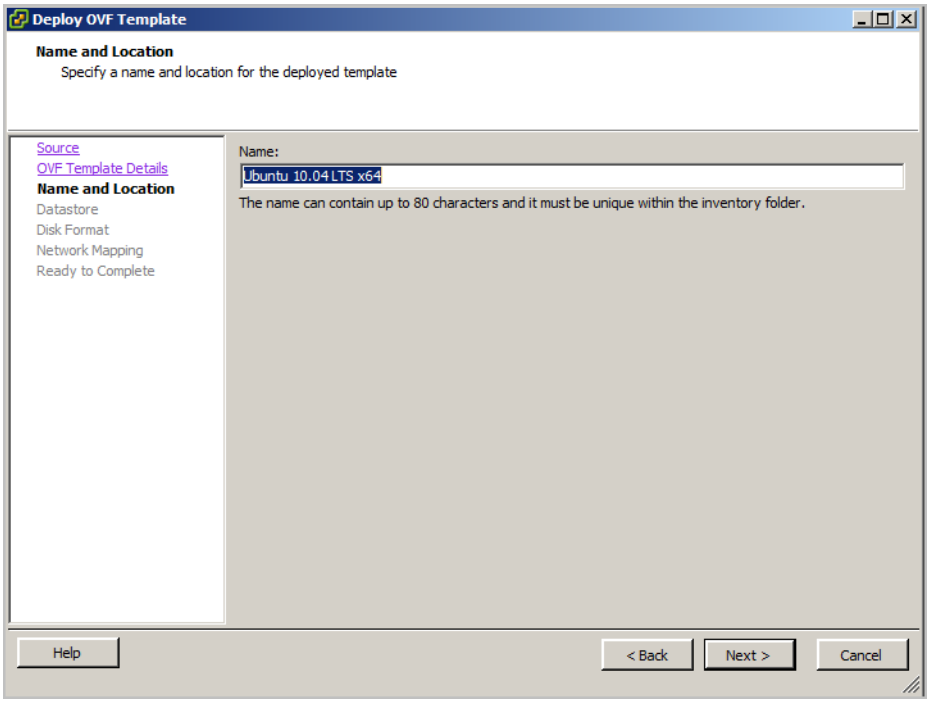
1. Download the Metasploit OVF application package.
2. Unzip the file.
3. Open and log in to vSphere Client.
4. Select **File > Deploy OVF Template**. The **Deploy OVF Template Wizard** appears.
5. Browse to the location of the OVF file and select it.



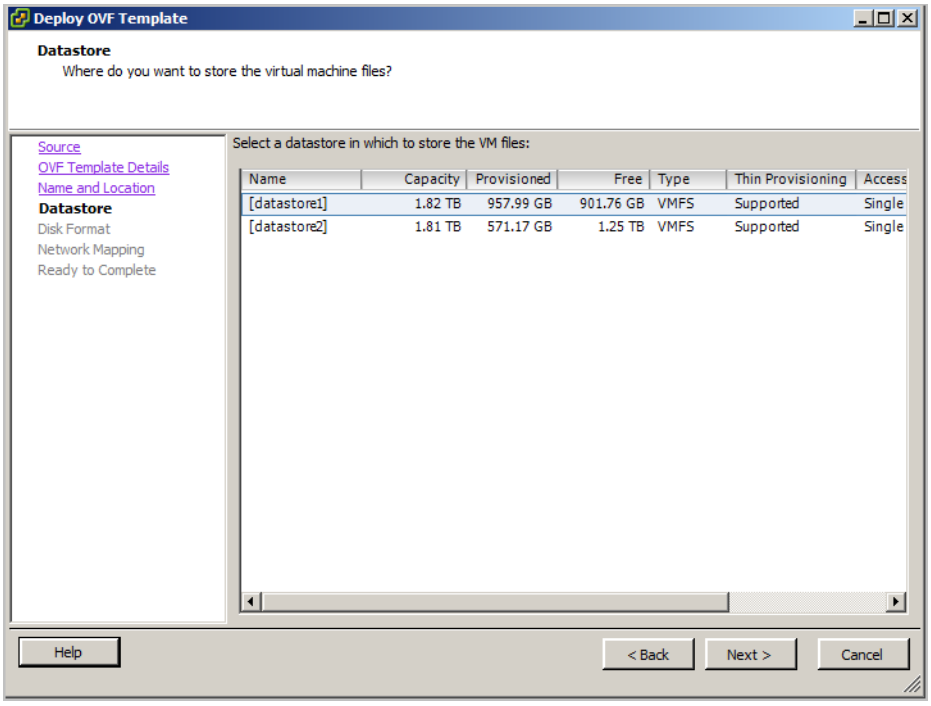
6. Click **Next**. The OVF template details display.



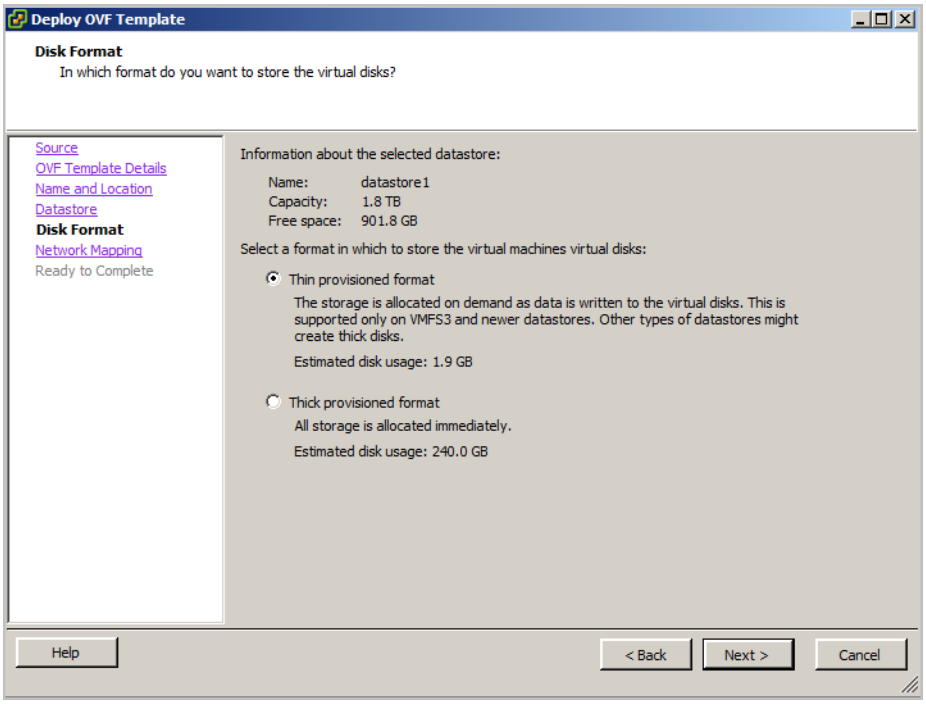
7. Verify the details, and then click **Next**.
8. On the **Name and Location** screen, you can change the name of the virtual machine.



9. On the **Datastore** screen, select where you want to store the virtual machine files.

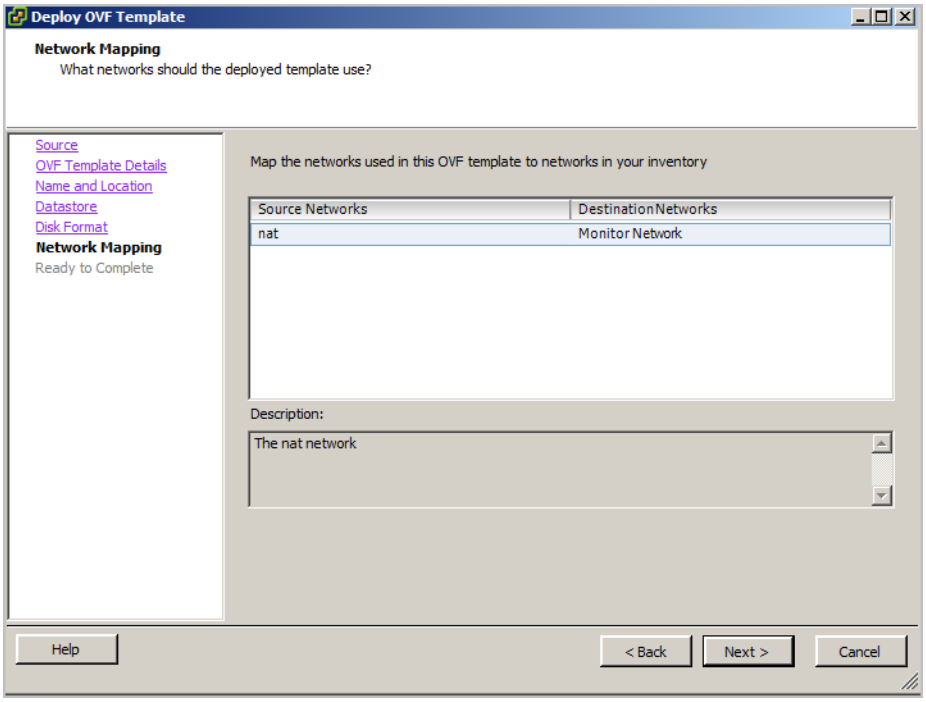


10. On the **Disk Format** screen, select the format that you want to use to store the virtual disks. You can choose between thin and thick. The thin provisioned format is recommended.

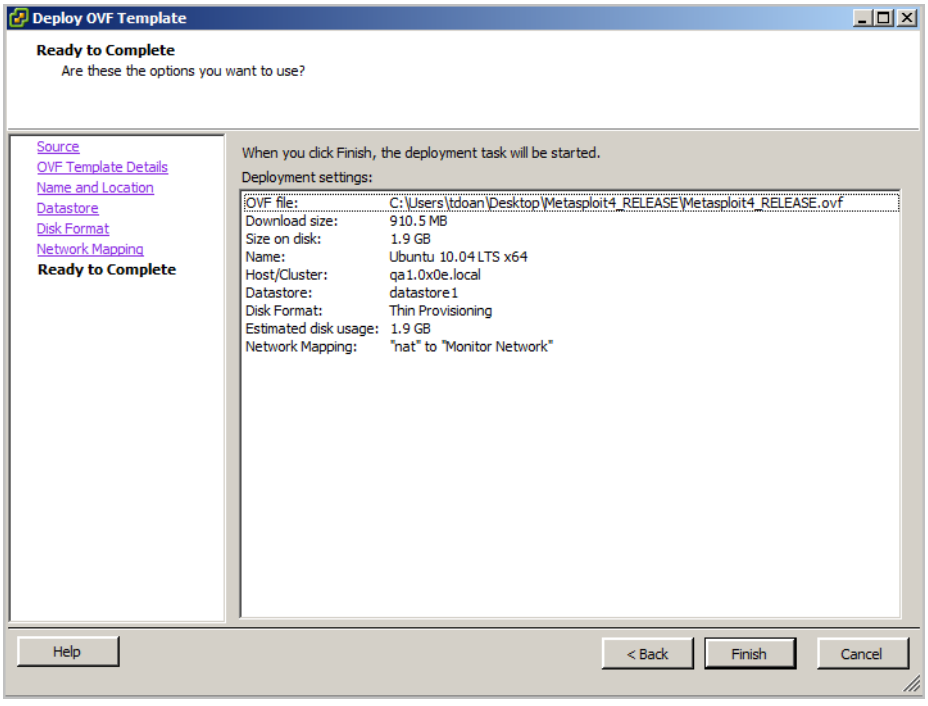


11. On the **Network Mapping** screen, map the networks in the OVF template to the

networks in your inventory.



12. On the **Ready to Complete** page, review the deployment details and click **Finish**. Deployment may take a few minutes.



13. After the deployment is complete, you need to open the deployed image and set up the virtual machine.

Setting up the Virtual Machine

After you deploy the Metasploit OVF template, you need to install and set up Metasploit Pro. When you launch the virtual machine, the command line terminal appears and prompts you to log in. You must provide the necessary credentials so that the Metasploit Pro set up script can run the installer.

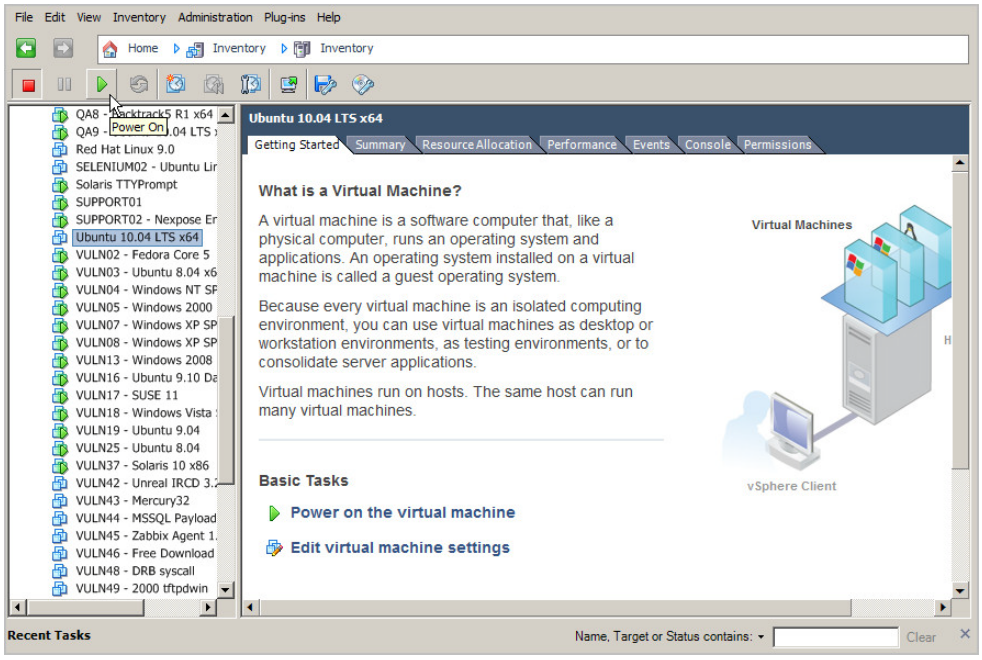
After the installation completes, the system displays the account information and address that you can use to log in to Metasploit Pro. The first time you log in to Metasploit Pro, you must provide a license key to activate the system. Contact Rapid7 Support for a license key.

The VM does not contain a graphical user interface; however, you can access Metasploit Pro through a web GUI. The default Metasploit address is `https://[VM IP addres]:3790`.

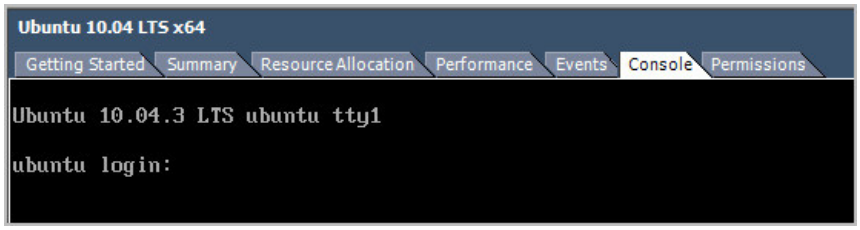
Installing Metasploit Pro

Use the following steps to launch the deployed virtual machine and install Metasploit Pro.

1. In vSphere Client, select the deployed virtual machine from the virtual machine list and click **Power On**.



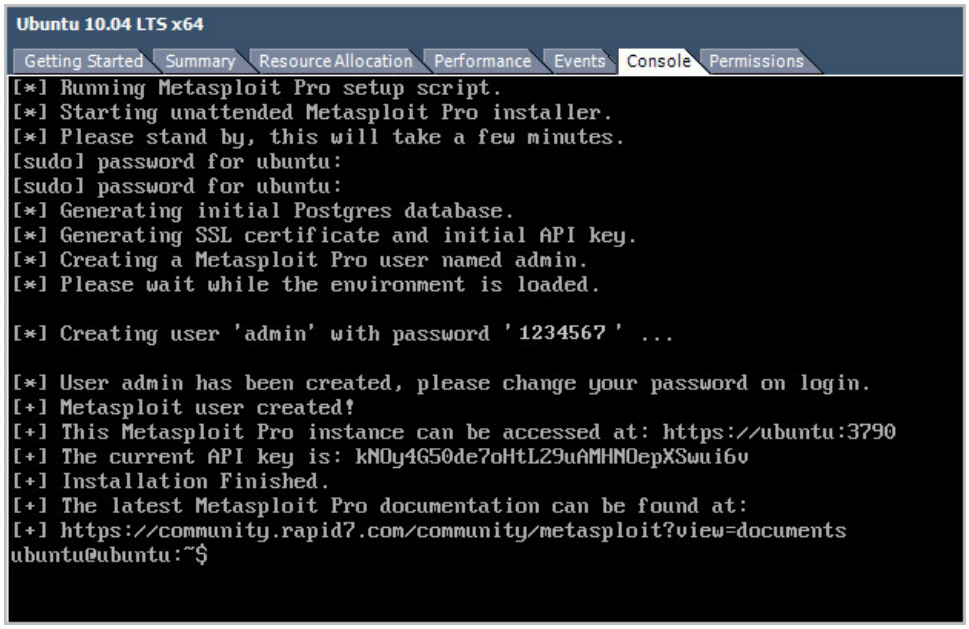
2. Click the **Console** tab.
3. When the Ubuntu login appears, use the following credentials to log in to the Metasploit VM for the first time: `ubuntu:metasploit`.



4. The next prompt asks you to change the password for the VM. Enter the current password (metasploit) to proceed.
5. Enter the new password that you want to use for the VM. Then, re-enter the password again.

6. The installation begins and can take a few minutes to complete. After the installation completes, the system displays the user name and password for Metasploit Pro. You must copy this information so that you can use it to log in to Metasploit Pro later. You can change the user name and password after you log in the first time.

   The following image shows that the user name and password is `admin:1234567` and the local address for the Metasploit Pro instance is `https://ubuntu:3790`.



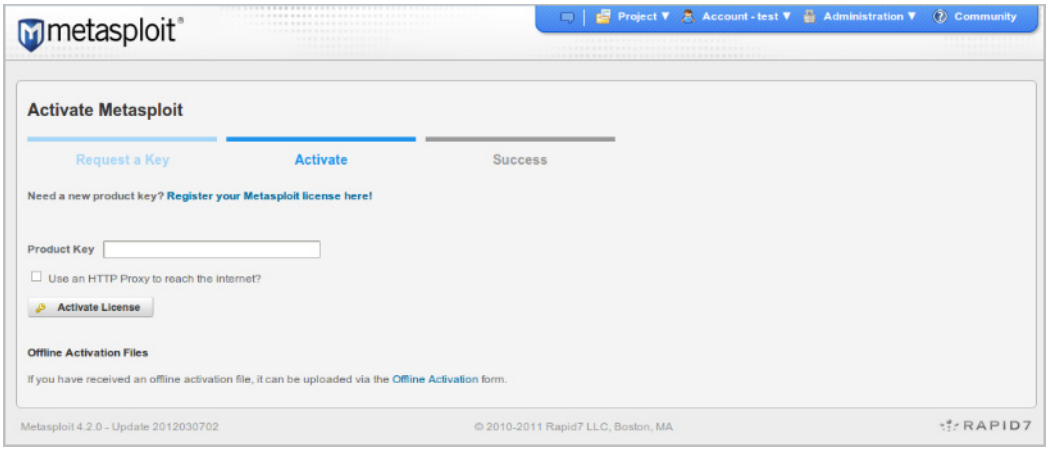
Activating Metasploit

1. Open a web browser on your local machine.
2. Browse to `https://[VM IP address]:3790`.

   Note: To find the IP address for the VM, run `ifconfig` on the VM.

3. When the Activation page appears, enter the product key and click **Activate License**.

   Note: Contact support@rapid7.com to obtain a product license key.



After you activate Metasploit, you should change your password. To change your password, select **Account > User Settings**.

Now, you are ready to use the Metasploit VM. Please visit the Metasploit documentation for more information on how to use the Metasploit products.