Automated Backups Guide

Document Version: 2017-08-03

Contents

Introduction 2
1 Prerequisites 3
1.1 Pre-installation Configuration 3
2 Implementing Automated Backups 4
2.1 Acquiring the vSphere Data Protection OVA 4
2.2 Deploying vSphere Data Protection 6
2.3 Configuring vSphere Data Protection 13
2.4 Configuring Backup Window on vSphere Data Protection 20
2.5 Creating a Backup Job 23
2.6 Restoring a Backup 28
3 Additional Configuration Best Practices 31
3.1 Configuring the Email Notifications and Reports 31
4 Common Alarms 32
4.1 Maintenance Services are not Running 32

Introduction

This is the *NETLAB+ Automated Backups Guide,* for the virtual edition of NETLAB+.

NETLAB+ is a remote access solution that allows academic institutions to deliver a hands-on IT training experience with a wide variety of curriculum content options. The training environment that NETLAB+ provides enables learners to schedule and complete lab exercises for information technology courses. NETLAB+ is a versatile solution for facilitating IT training in a variety of disciplines including networking, virtualization, storage and cyber security.

It is imperative that you establish a plan for making backups of your NETLAB+ virtual appliance on a regular basis to protect against data loss and disaster recovery preparedness. You are also strongly advised to perform a backup before any software update and prior to adding additional content to your NETLAB+ system.

It is the responsibility of the customer to maintain backups of their NETLAB+ VE system.

To ensure that backups are performed regularly, consider implementing an automated method of creating backups. Taking the time to set up a robust, automated backup process helps protect the investment your organization has made in your NETLAB+ VE system. The material in this guide provides guidance on implementing automated backups of your NETLAB+ VE system, using VMware vSphere Data Protection (VDP).

1 Prerequisites

This section will help outline what is required before configuring a backup job.

1.1 Pre-installation Configuration

Mechanisms that need to be in place, before the *vSphere Data Protection* (*VDP*) installation:

- **vCenter Licensing:** The *vCenter* needs to be licensed prior to deploying the *vSphere Data Protection* appliance.
- **DNS Configuration**: A *DNS* server must be in place to support both forward and reverse lookup on the *VDP* and the *vCenter*.
- **NTP Configuration**: The *VDP* appliance receives the correct time through *vSphere*, so *NTP* must be configured properly on all *vSphere Hosts* and *vCenter Servers*.

2 Implementing Automated Backups

This section assumes that a working infrastructure is already in place. The *NETLAB+ VE* system should already be configured to match the infrastructure and vice versa.

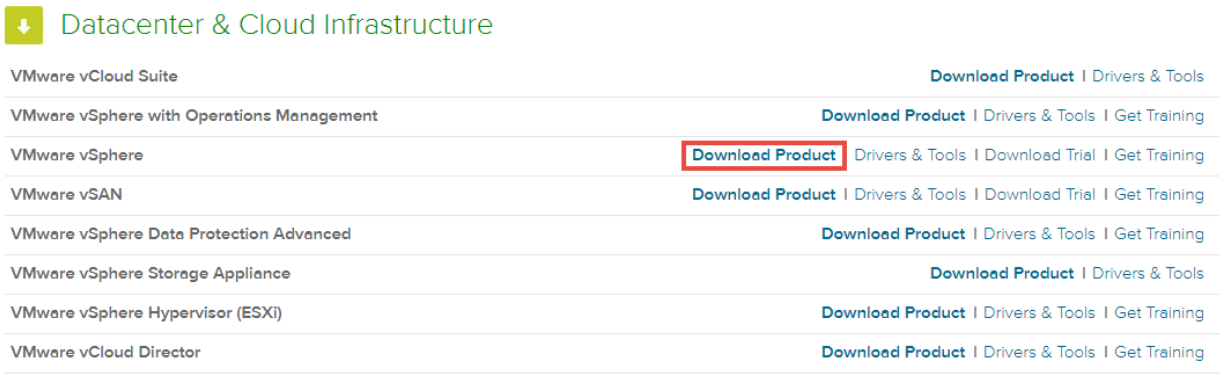
The proposed automated backup solution requires the use of *vSphere Data Protection*. This is a backup and recovery solution from *VMware*. It has been configured to be fully integrated with existing *VMware vCenter Server* appliances and *VMware vSphere Web Client*. This backup solution has the ability to provide disk-based backups of virtual machines as well as applications.

More features of the *VDP* appliance can be found in the *VMware vSphere Data Protection Technical Overview* guide.

2.1 Acquiring the vSphere Data Protection OVA

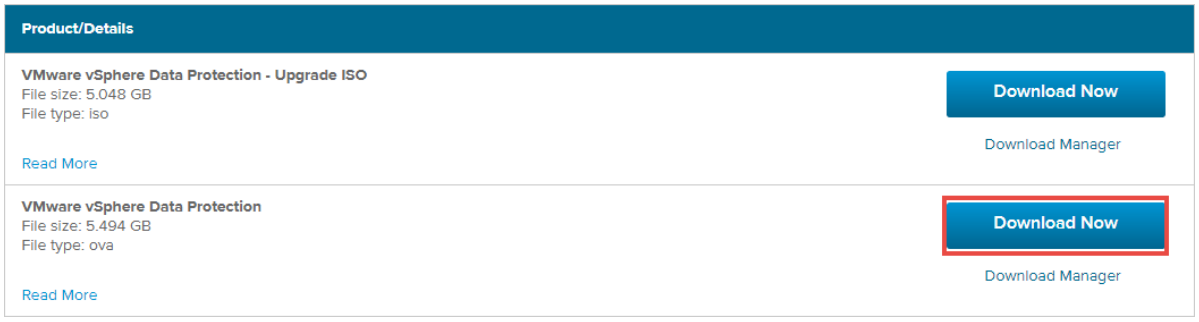
The *vSphere Data Protection* OVA is required to install the *VDP* application in a given *VMware Infrastructure*. This section will describe how to download the *VDP* appliance from VMware.

1. Using a web browser, preferably on an administrative machine, navigate to http://my.vmware.com/en/web/vmware/downloads. This will bring you to the *All Downloads* page supported by *VMware*. Login to *My VMware*.
2. Underneath *Datacenter & Cloud Infrastructure*, click on **Download Product** for the *VMware vSphere* product.



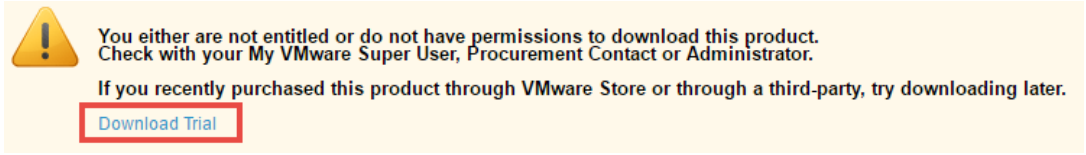
3. On the *Download VMware vSphere* page, scroll down and determine the type of licensing used for your *VMware vSphere*. Once identified, click on the **Go to Downloads** link for the *VMware vSphere Data Protection 6.x.x* product.

4. On the *Download VMware vSphere Data Protection 6.x.x* page, click on the **Download Now** button for *VMware vSphere Data Protection*.

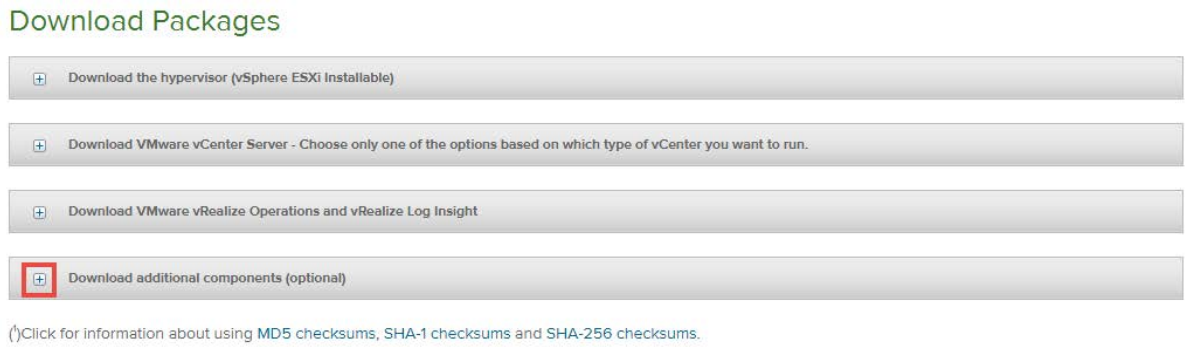


If not logged in already, the webpage will prompt for a login. Continue with the login.

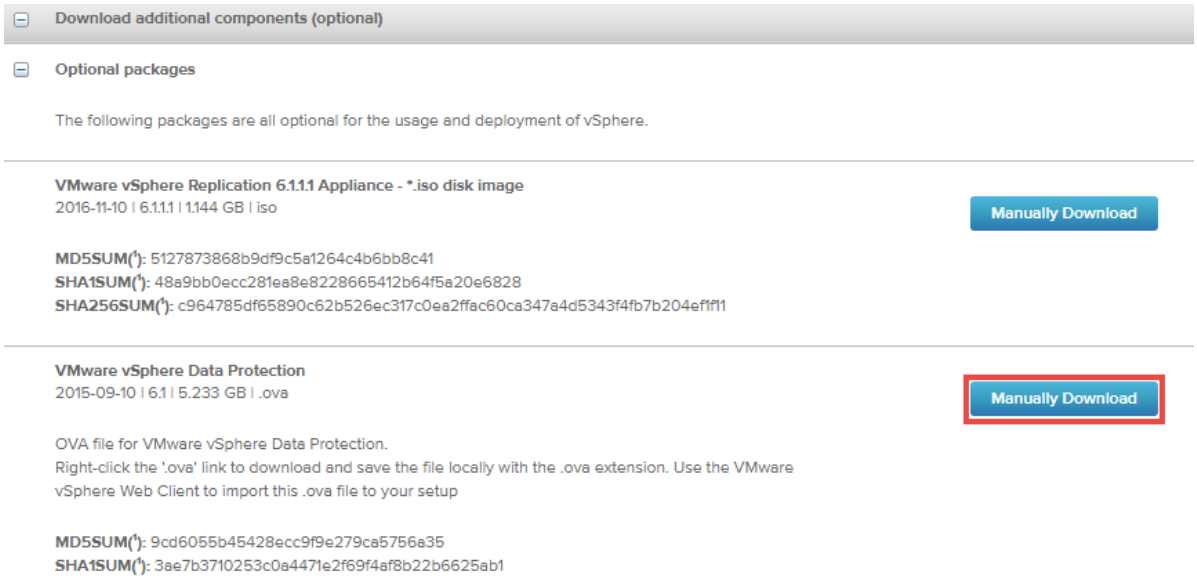
5. The download should begin, if it does not, proceed to the next step.
6. If a message appears stating that you do not have permissions to download the product, click on the **Download Trial** link exposed below the message.



7. The page will redirect to a page called *Product Evaluation Center for VMware vSphere and vSphere with Operations Management*. Scroll down towards the *Download Packages* table and expand **Download additional components (optional)**.



8. Once the list is expanded, click on the **Manually Download** button for *VMware vSphere Data Protection*.



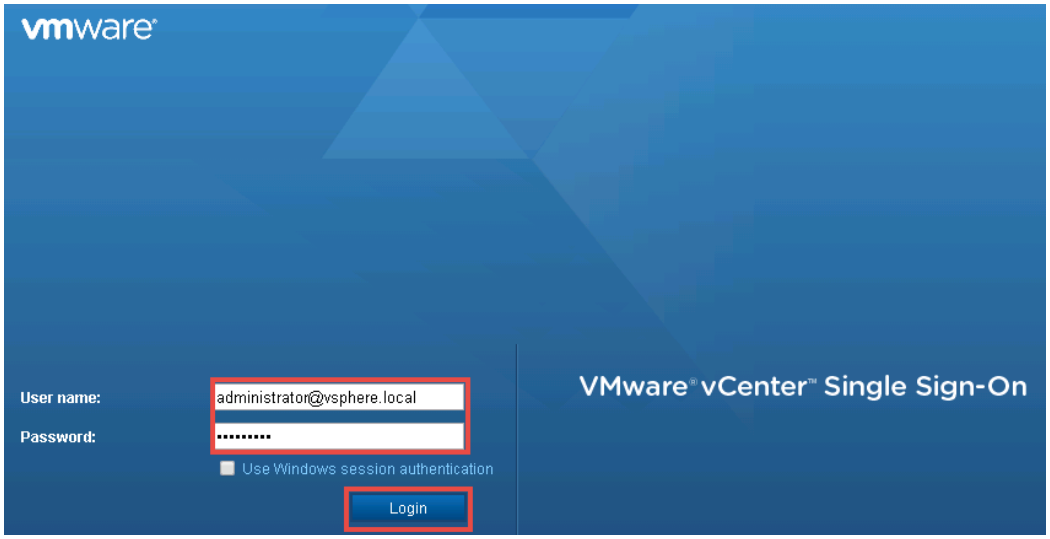
9. The download should now begin.

2.2 Deploying vSphere Data Protection

This section describes how to deploy the *VDP* appliance from an *OVA* file.

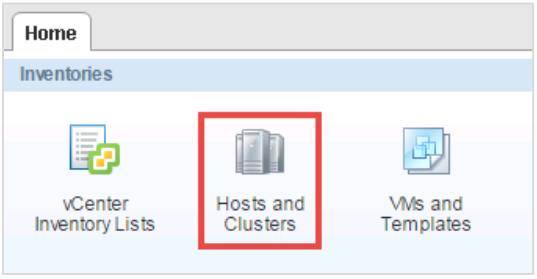
For additional guidance on deploying *VDP*, reference to pages **29-30**, from the *VMware vSphere Data Protection Administration Guide*.

1. Navigate to the **VMware Web Client** and login as *administrator*.

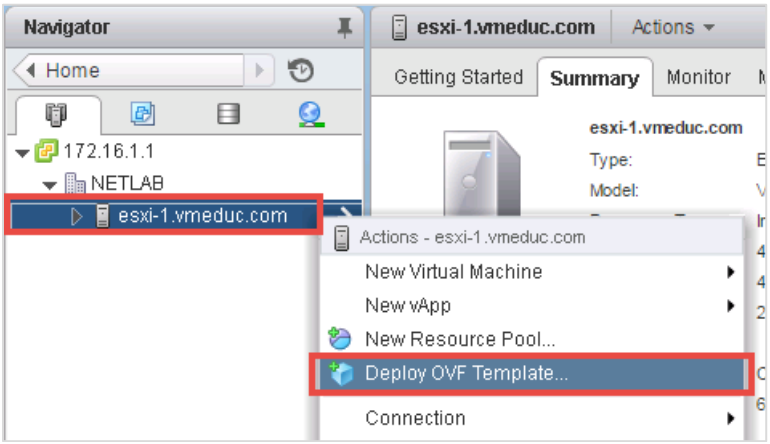


Before proceeding any further, verify that *VMware Client Integration Plug-in* is installed and running on the web browser being used for the *Web Client*. It can be confirmed if the plugin is installed by seeing whether or not the "*Download Client Integration Plugin*" message appears on the bottom of the *Web Client* login screen. If present, the plugin is not installed.

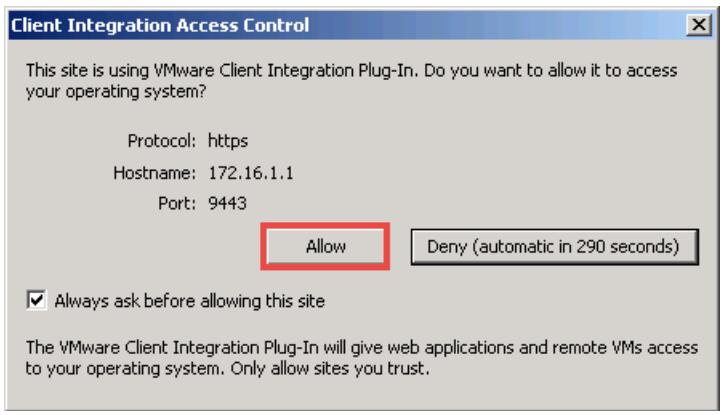
2. Once logged in, on the *Home* tab, click on the **Hosts and Clusters** icon.



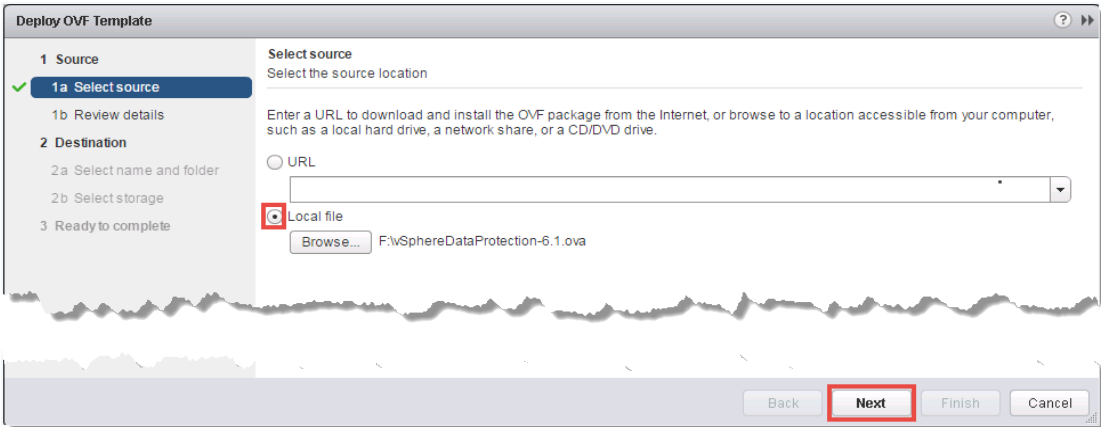
3. In the *Navigator* pane, right-click on the desired **ESXi host** and select **Deploy OVF Template**.



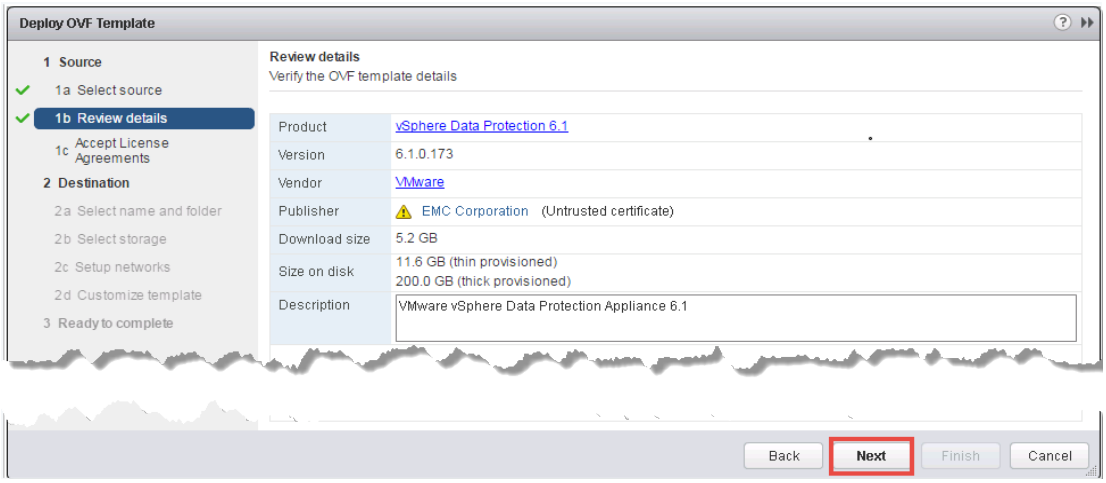
4. Once the *Deploy OVF Template* wizard appears, notice that a *Client Integration Access Control* window may appear. Click **Allow** (or anything similar - browser dependent) to initiate access for the plugin utility.



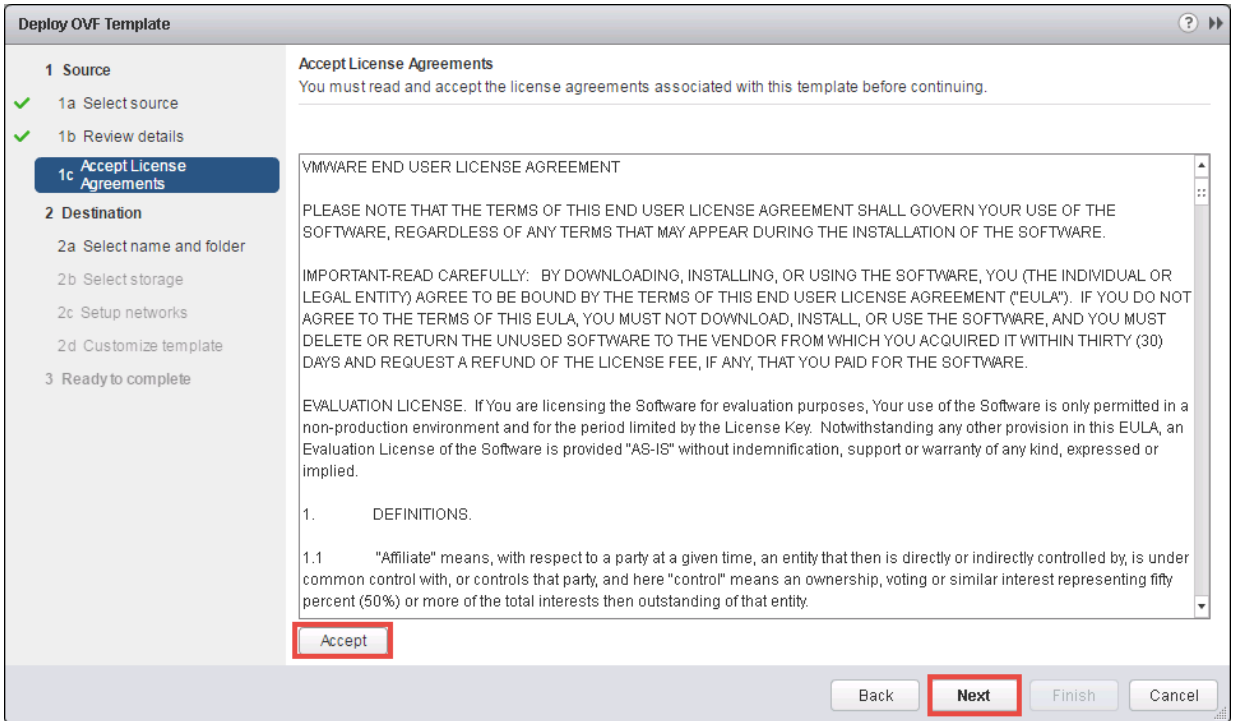
5. In the *Deploy OVF Template* window, in the *Select source* page, choose either **URL** or **Local file**, depending on where the *vSphereDataProtection-x.x.ova* file is stored. For this example, the OVA is stored locally on the client machine. Click **Next**.



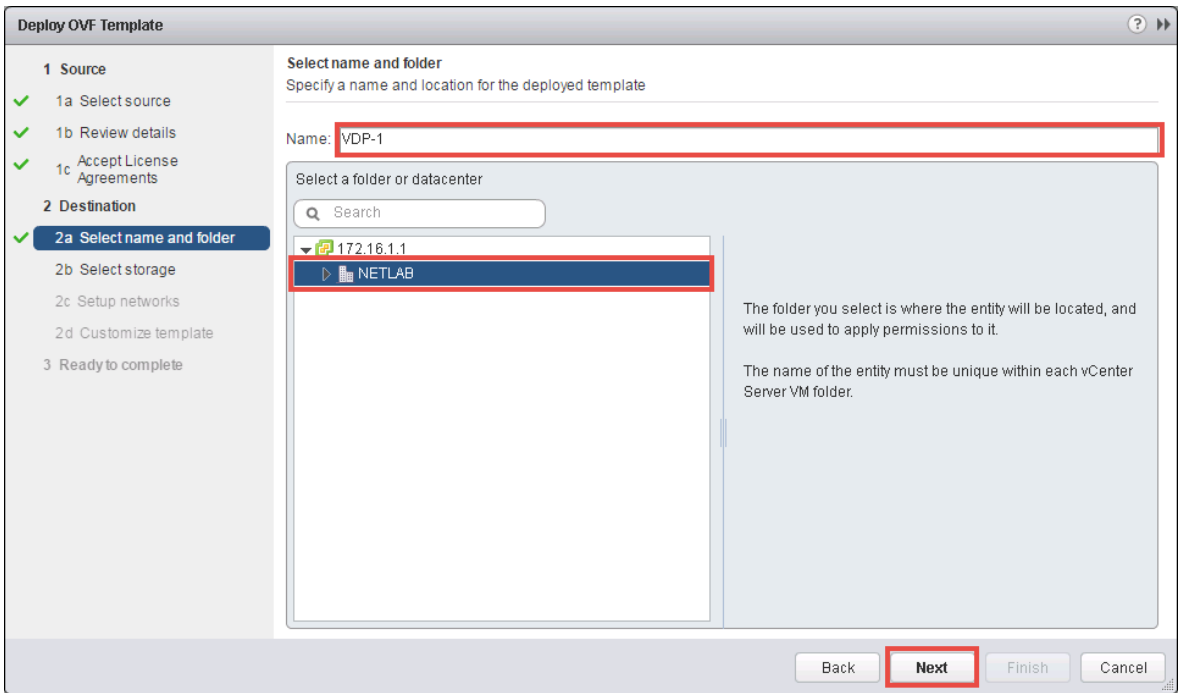
6. On the *Review details* page, verify the OVF template details and click **Next**.



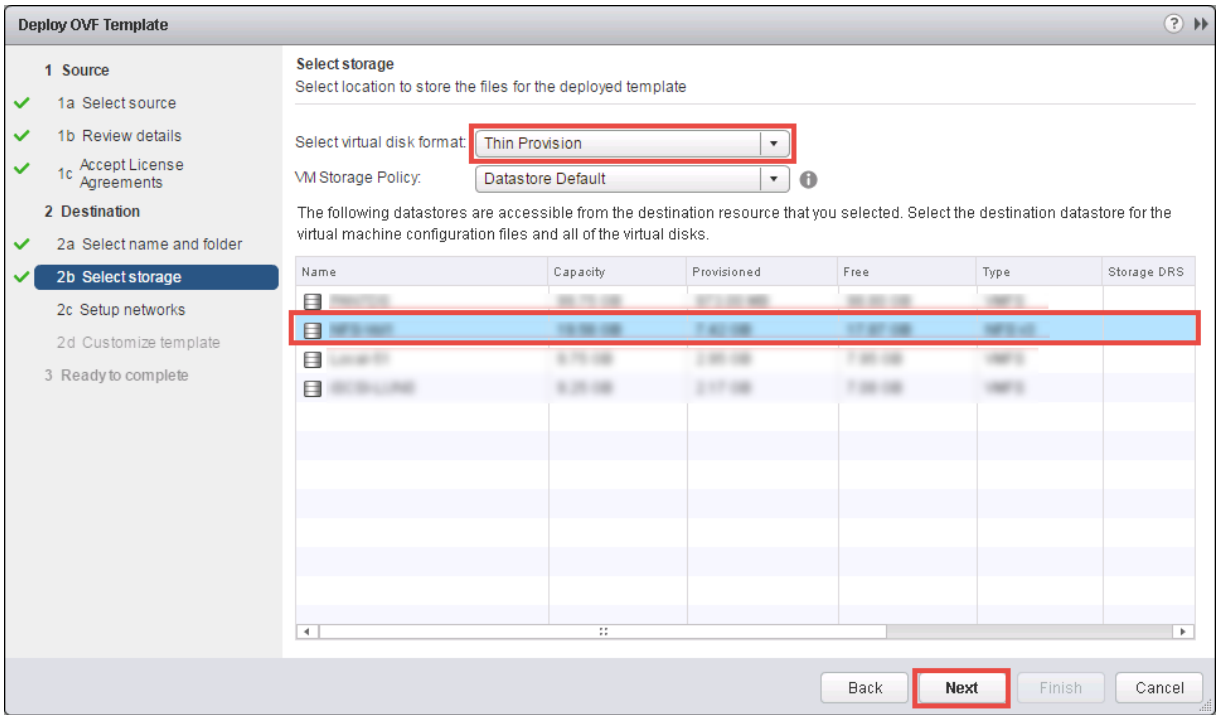
7. On the *Accept License Agreements* page, read and **Accept** the license agreements. When finished, click **Next**.



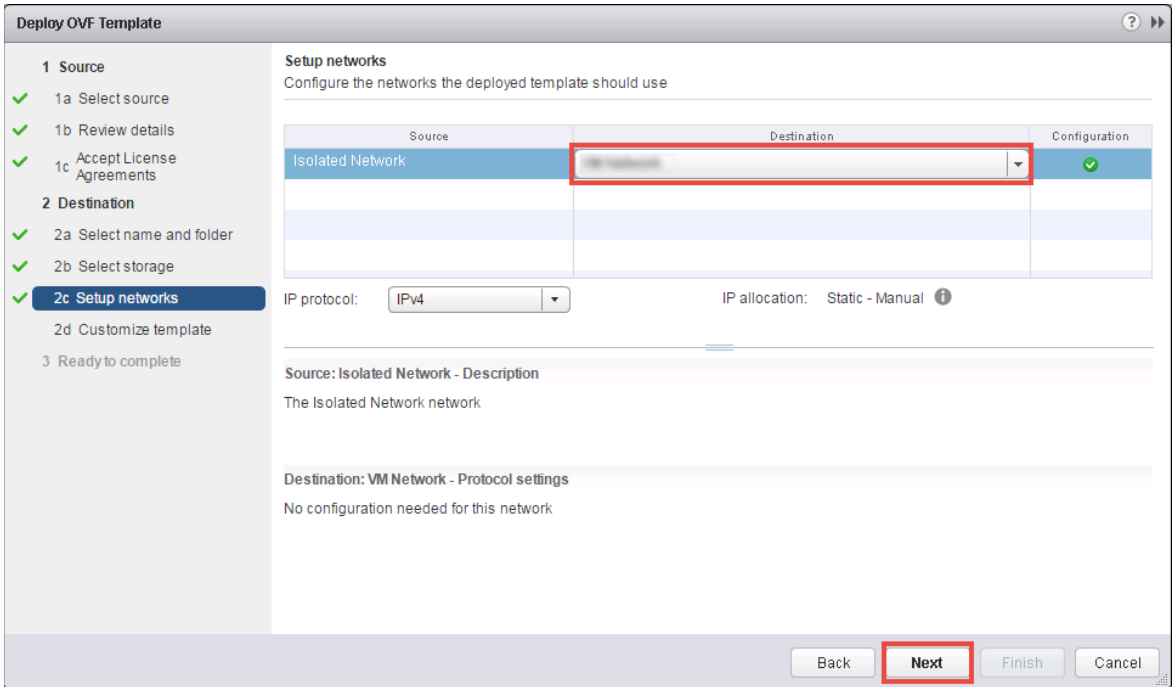
8. On the *Select name and folder* page, type the name for the *vSphere Data Protection* appliance in the **Name** text field. Select the appropriate **datacenter** object and click **Next**.



9. On the *Select storage* page, select **Thin Provision** in the drop-down menu for *Select virtual disk format*. Then choose which **datastore** to store the appliance on, ensuring that enough space is present. Click **Next**.

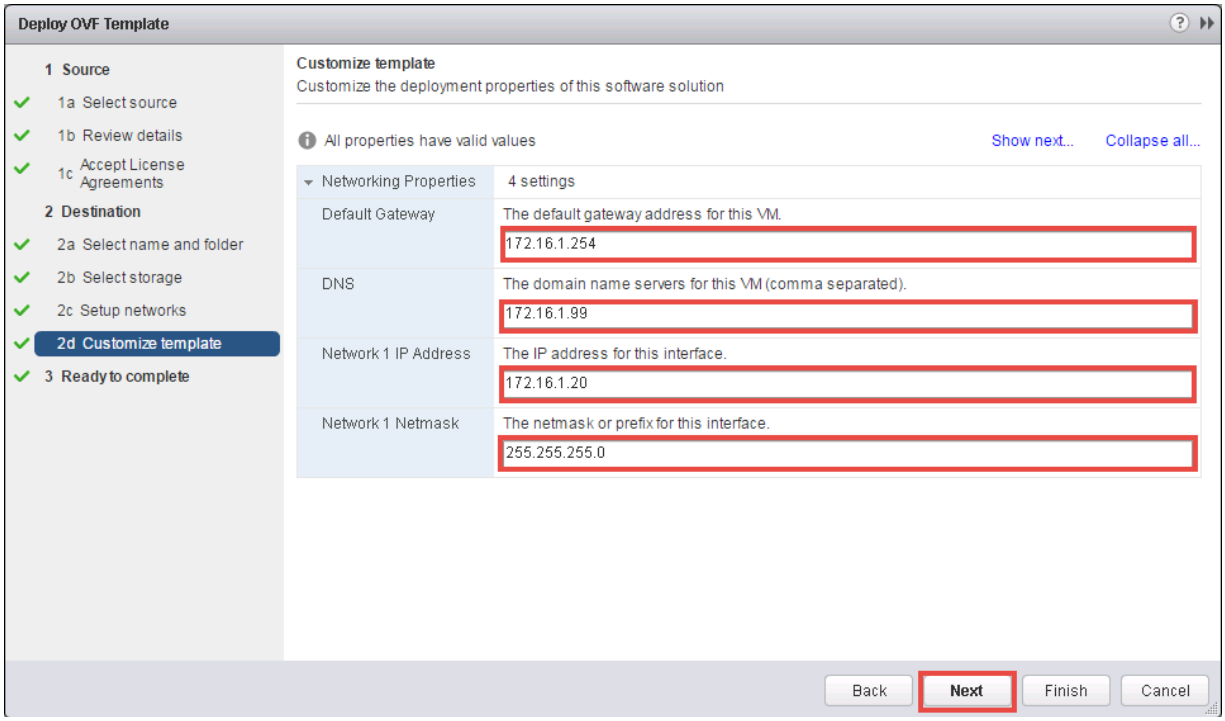


10. On the *Setup networks* page, choose the **management network** for your infrastructure and click **Next**.

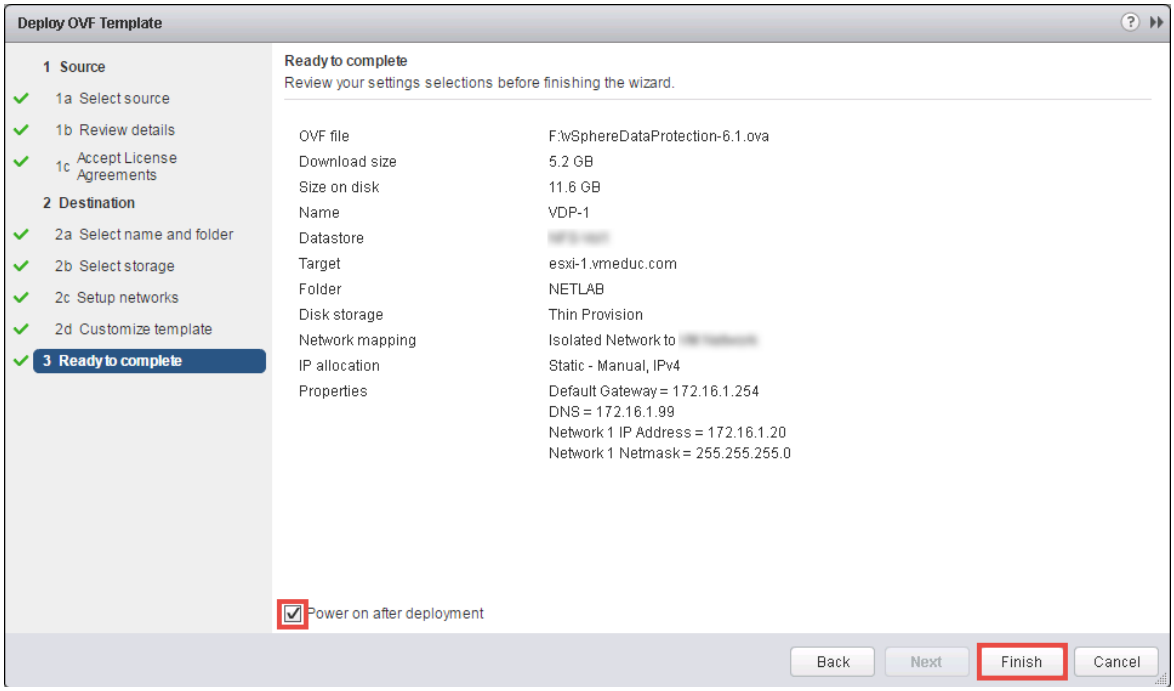


11. On the *Customize template* page, fill in the fields for **Default Gateway**, **DNS**, **Network 1 IP address**, and **Network 1 Netmask**. Click **Next**.

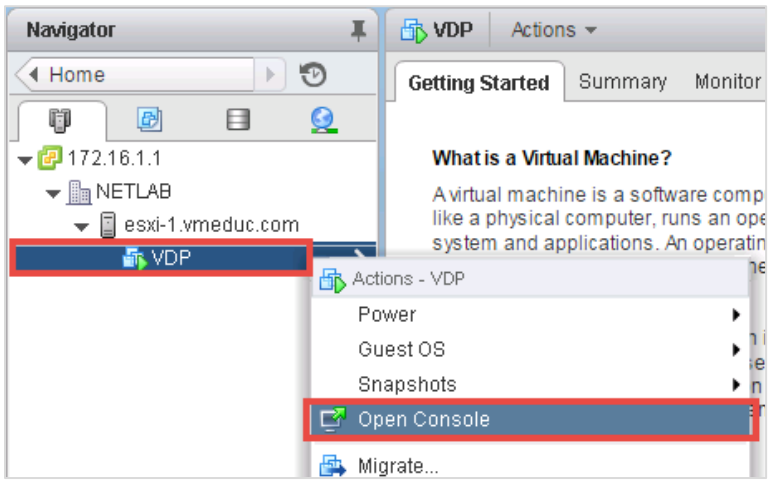
The *VDP* appliance does not support *DHCP*. An assigned static IP address will be required.



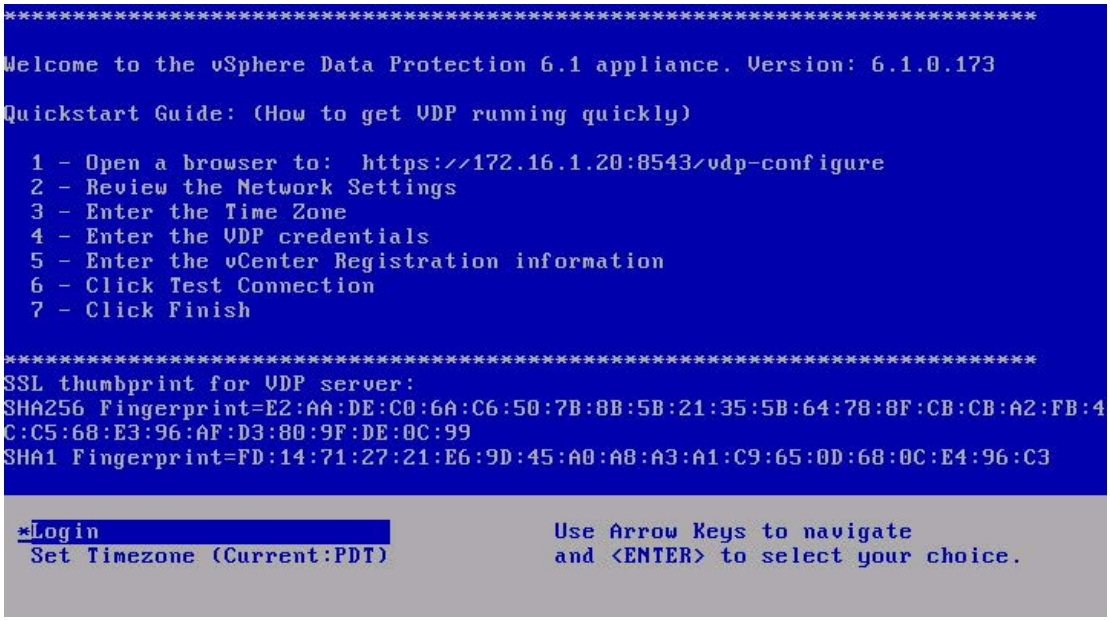
12. On the *Ready to complete* page, review the configurations, check the box for **Power on after deployment** and click **Finish**.



13. Monitor the deployment progress in the *Recent Tasks* pane. Once finished, right-click on the **vSphere Data Protection** VM in the *Navigator* pane and select **Open Console**.



14. Verify that the *vSphere Data Protection* VM has finished its boot-up process before proceeding to the next step. A blue welcome screen will signal that the boot-up is complete.



2.3 Configuring vSphere Data Protection

This section will provide guidance on how to configure the *VDP* appliance so that it can be added to *vCenter*.

For additional guidance on deploying *VDP*, reference to pages **30-32**, from the *VMware vSphere Data Protection Administration Guide*.

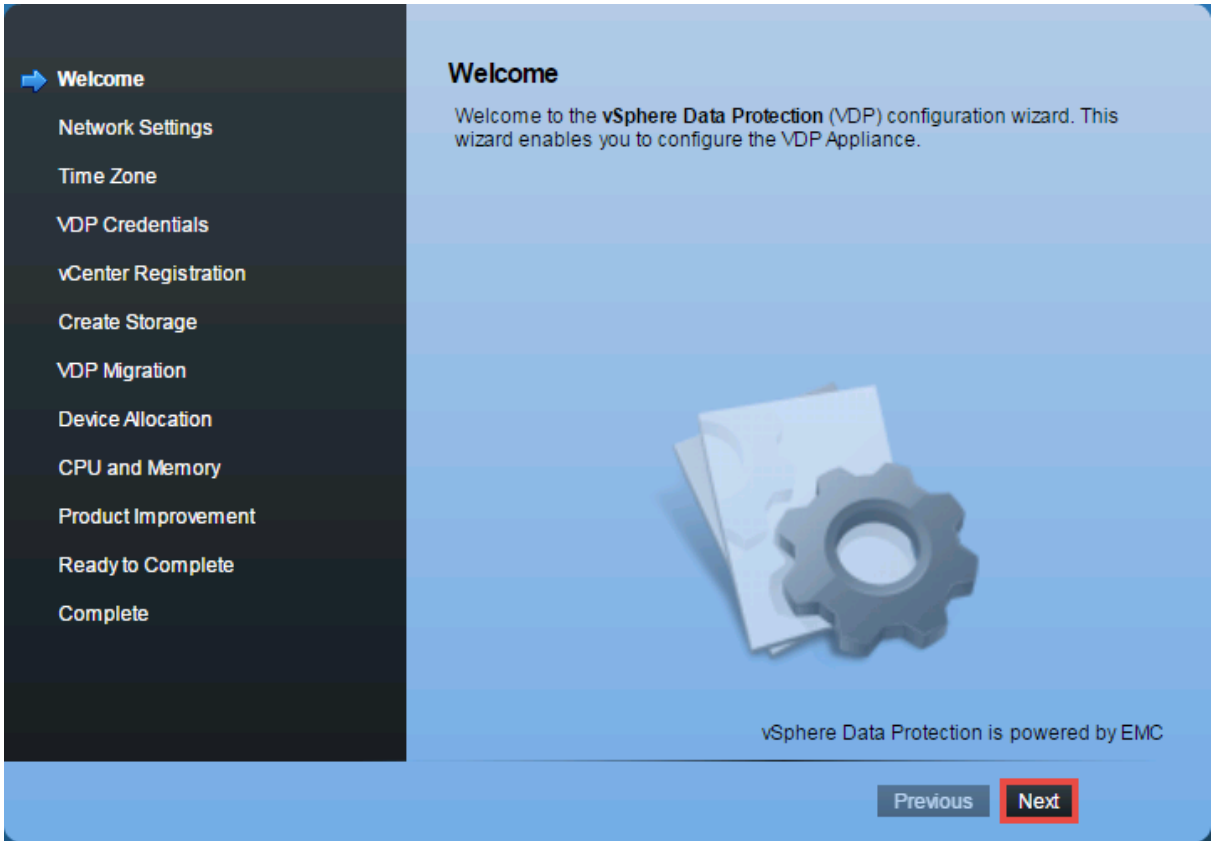
1. Using the client machine, open a **new tab** in the web browser and enter **`https://YOUR_VDP_IP:8543/vdp-configure`** into the address field and press the **Enter** key.

   IP addresses will vary, depending on the infrastructure.

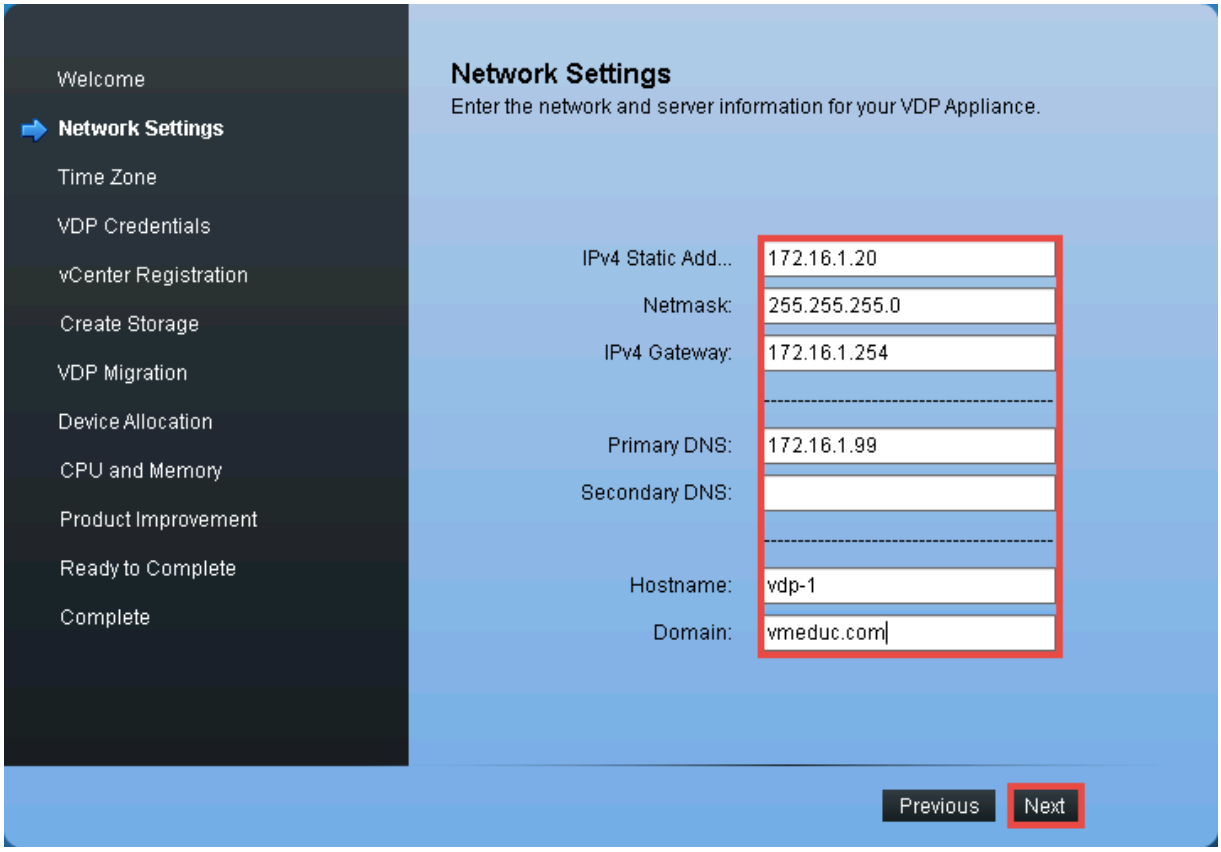
2. Once the web page redirects, notice an SSL certificate warning may appear. Depending on the web browser, proceed to the destination, ignoring the warnings.

3. On the *vSphere Protection Configuration Utility* login page, login using the default credentials; **`root`** as the *username* and **`changeme`** as the default *password*.

4. Once redirected, notice the welcome page for the *VDP* configuration wizard. Click **Next** to continue.



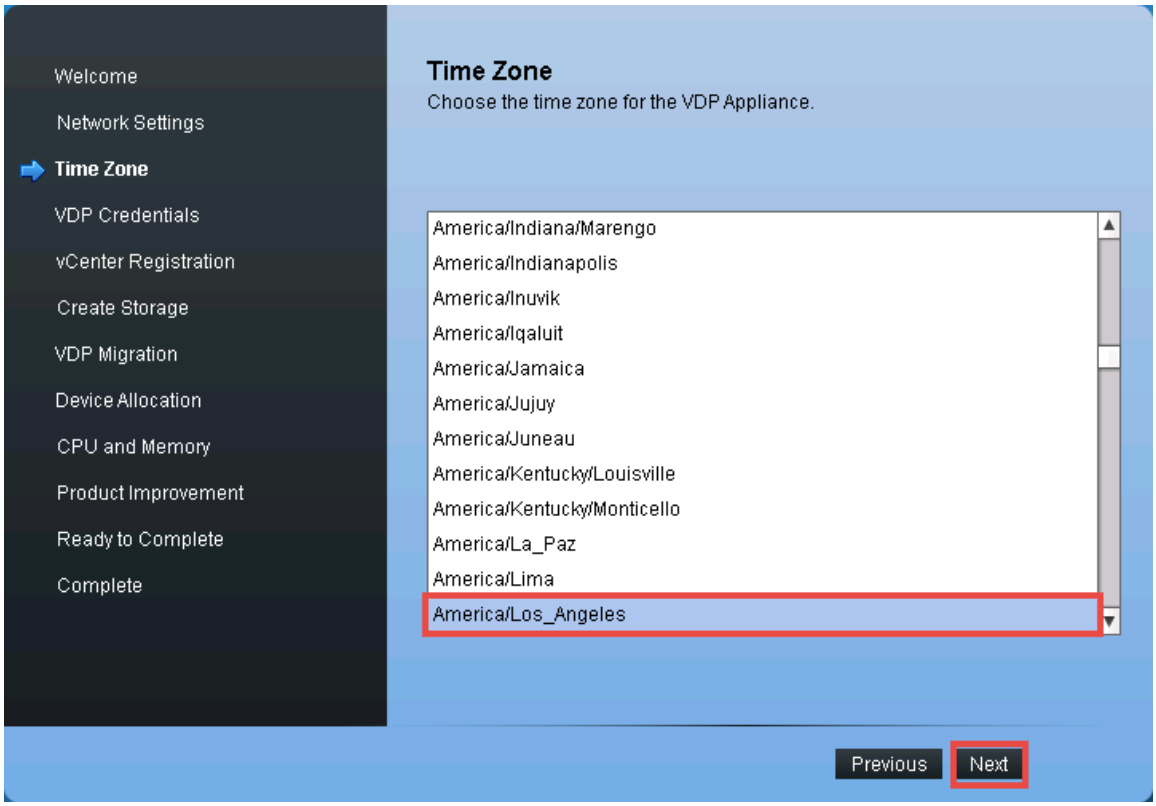
5. On the *Network Settings* page, enter the information pertinent to your *VMware* infrastructure. Click **Next**.



It is important to have *DNS* configured prior to initial *VDP* setup. A reverse *DNS* lookup (*PTR* record) needs to be configured on the local DNS, otherwise an error message will appear (see below):

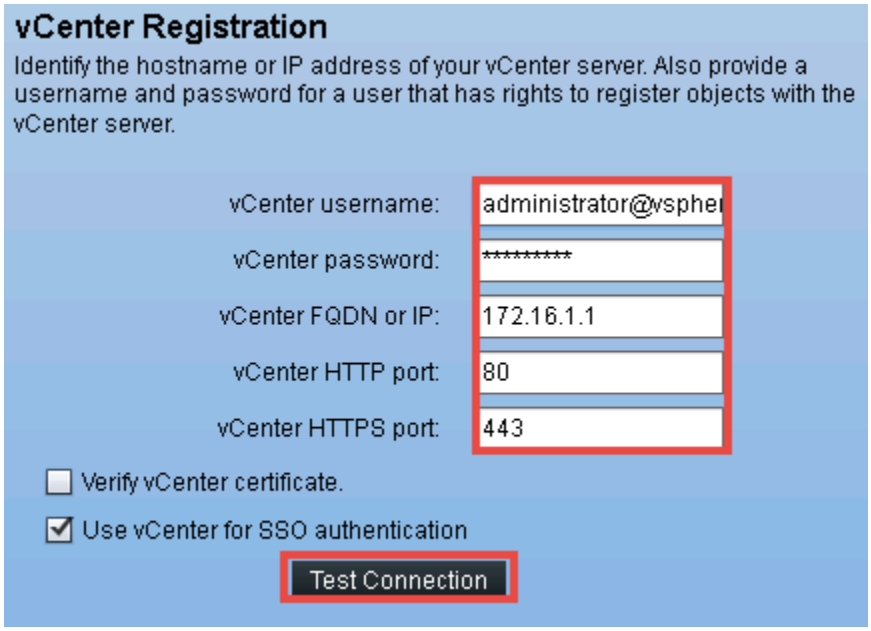
For more information on *DNS* configuration, see **page 23**, *DNS Configuration*, in the following *VMware* guide: *vSphere Data Protection Administration Guide*.

6. On the *Time Zone* page, choose your local time zone and click **Next**.



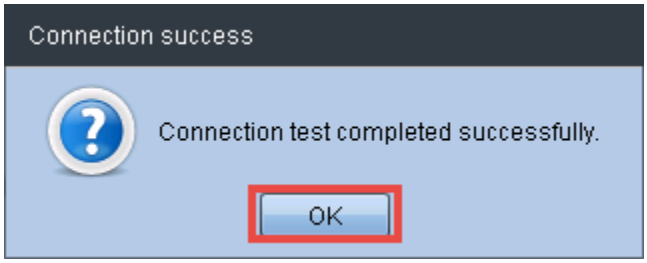
7. On the *VDP Credentials* page, enter a new password for the *vSphere Data Protection* appliance. Click **Next**.

8. On the *vCenter Registration* page, enter the *vCenter* information in the appropriate fields. Once the fields are populated, click **Test Connection**.



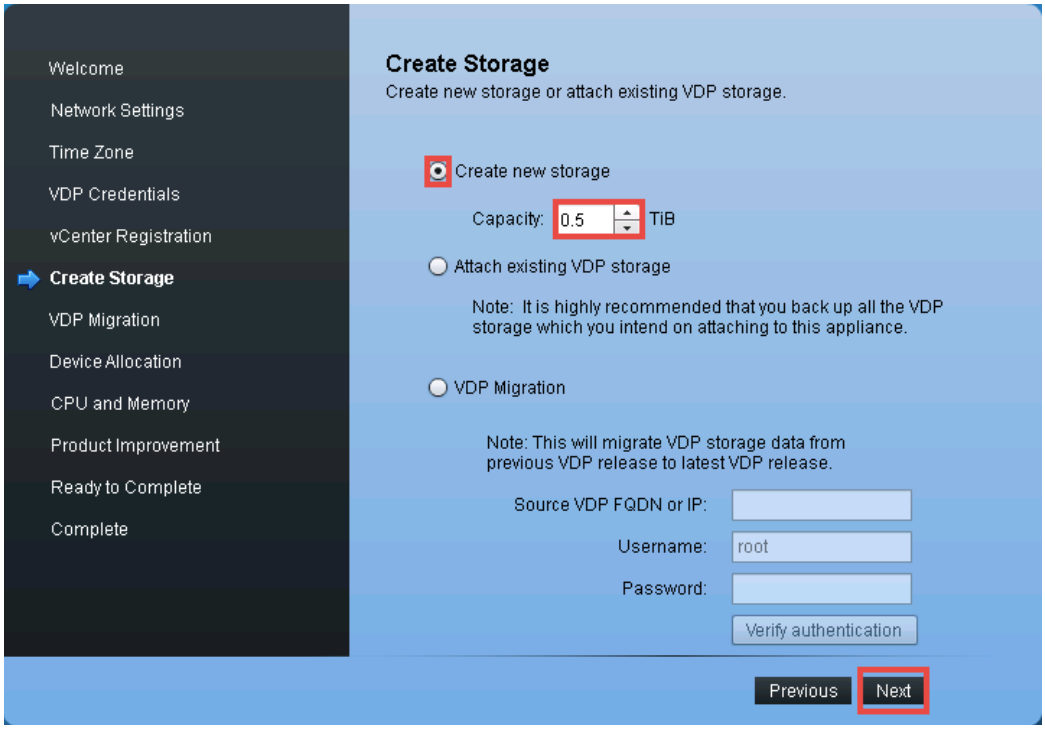
The default port for *HTTP* is *80*. The default port for *HTTPS* is *443*. If different ports are used, the ports must be opened in */etc/firewall.base* followed by a restart of the *avfirewall* service.

9. Once the connection is confirmed, click **OK,** followed by clicking **Next**.

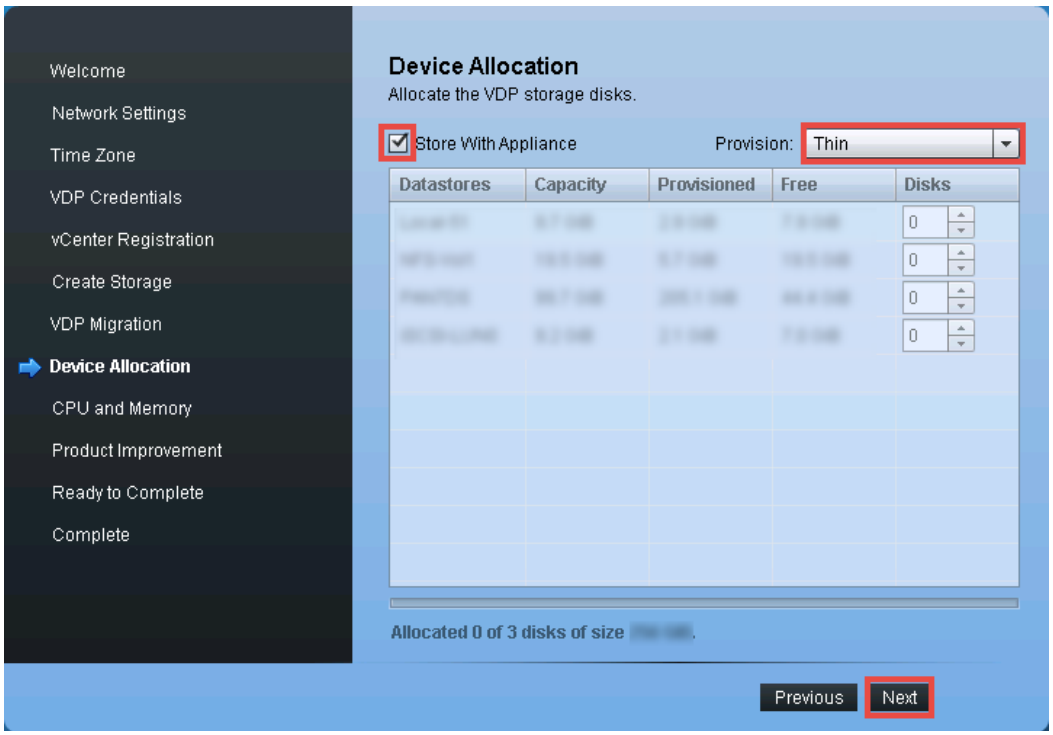


10. On the *Create Storage* page, select the bubble for **Create new storage** and create a capacity for **0.5TB**. Click **Next**.

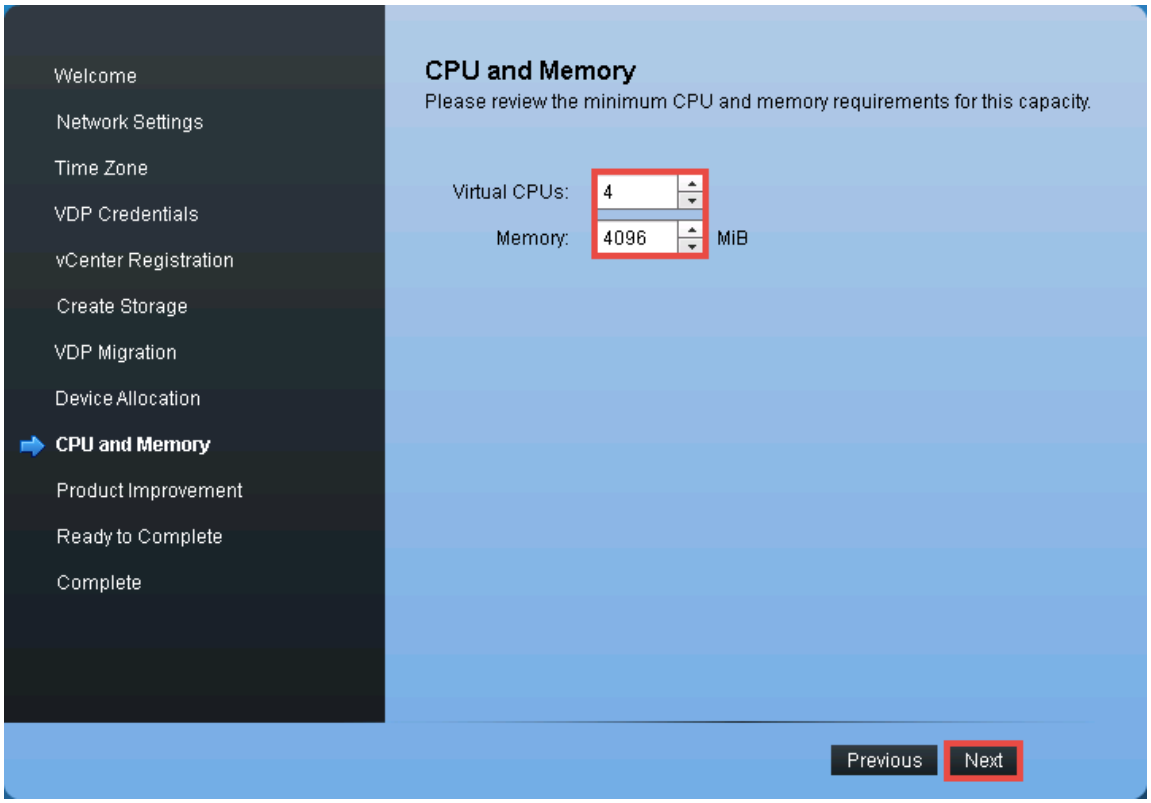
For additional guidance on VDP best practices for storage capacity, reference to pages **27-28**, from the *VMware vSphere Data Protection Administration Guide*.



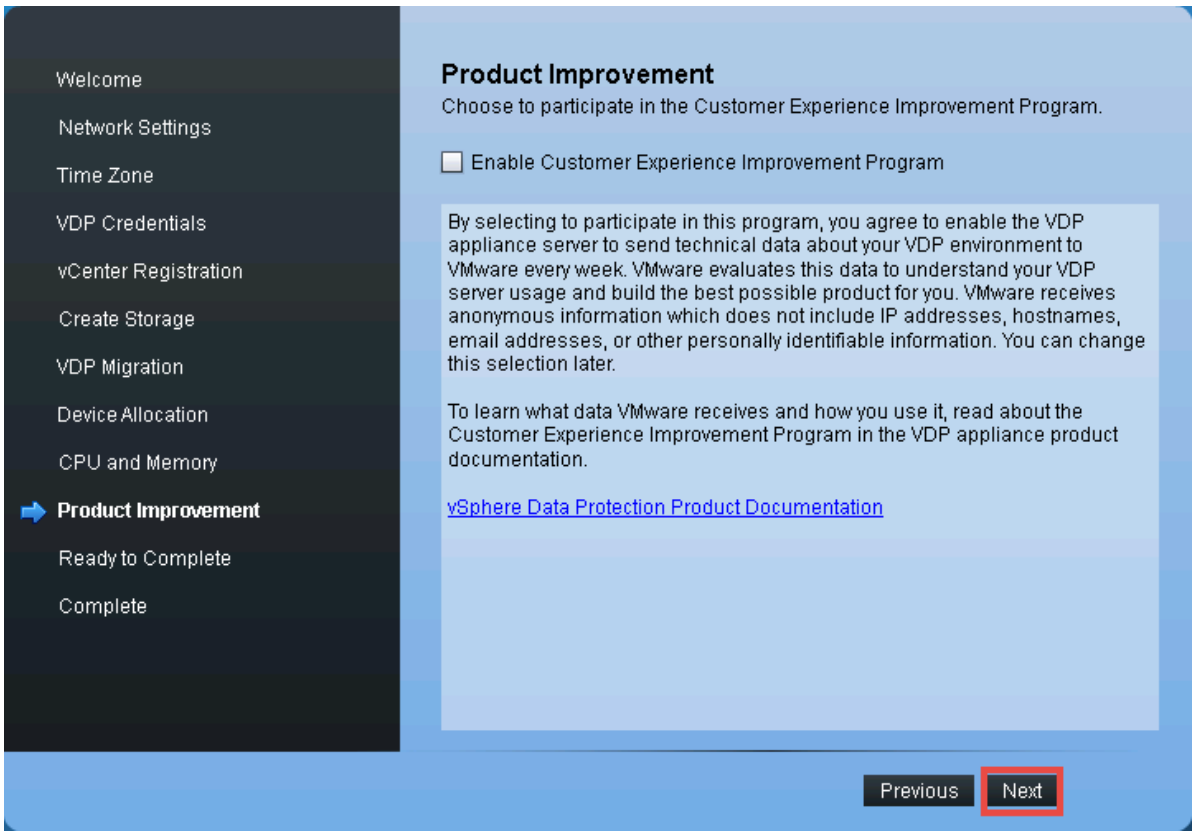
11. On the *Device Allocation* page, select **Thin** for the *Provision* type and check the box for **Store With Appliance**. Click **Next**.



12. On the *CPU Allocation* page, leave the **defaults** and click **Next**.

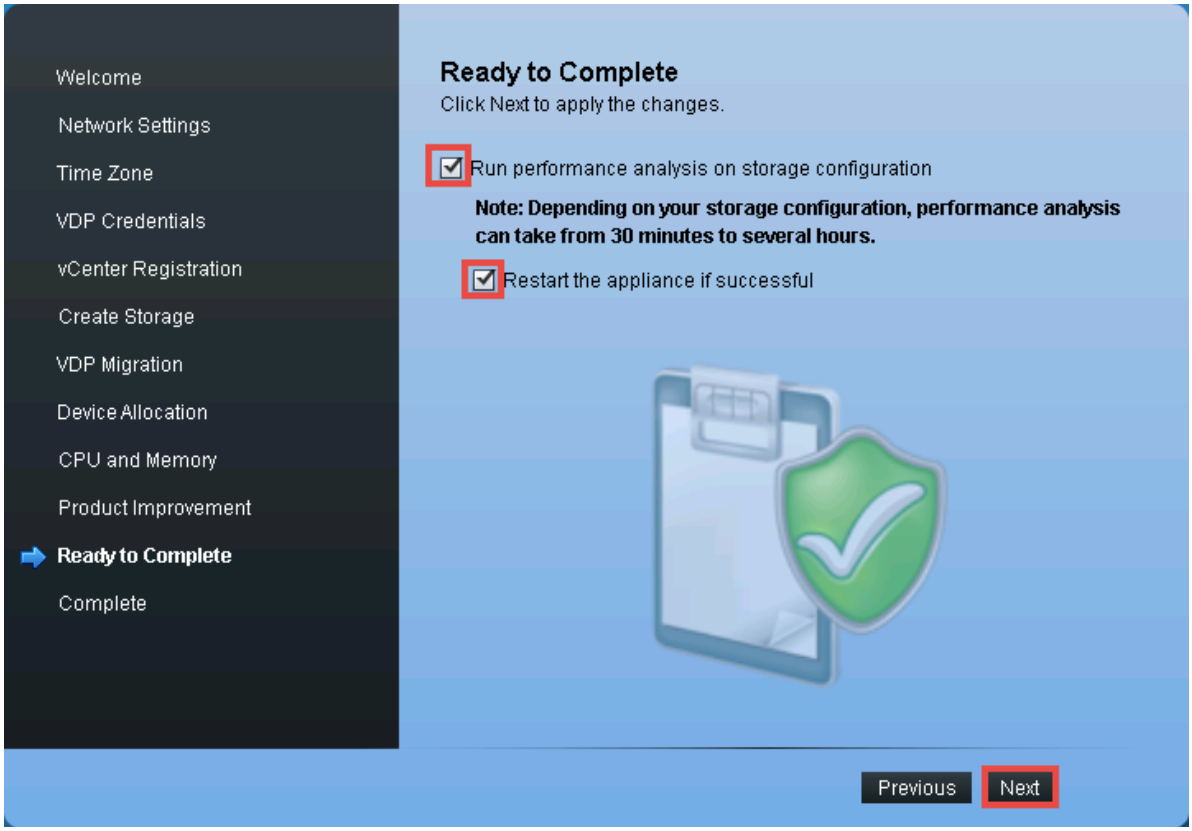


13. On the *Product Improvement* page, if desired, check the box **for Enable Customer Experience Improvement Program**. Click **Next**.



14. On the *Ready to Complete* page, if desired, check the box for **Run performance analysis on storage configuration** and **Restart the appliance if successful** to test storage performance compatibility. Click **Next** to continue.

The test performs write, read, and seek performance tests on the disks.



15. Once the storage check finalizes without any errors, the appliance will restart. Wait until the appliance fully reboots to access it again.

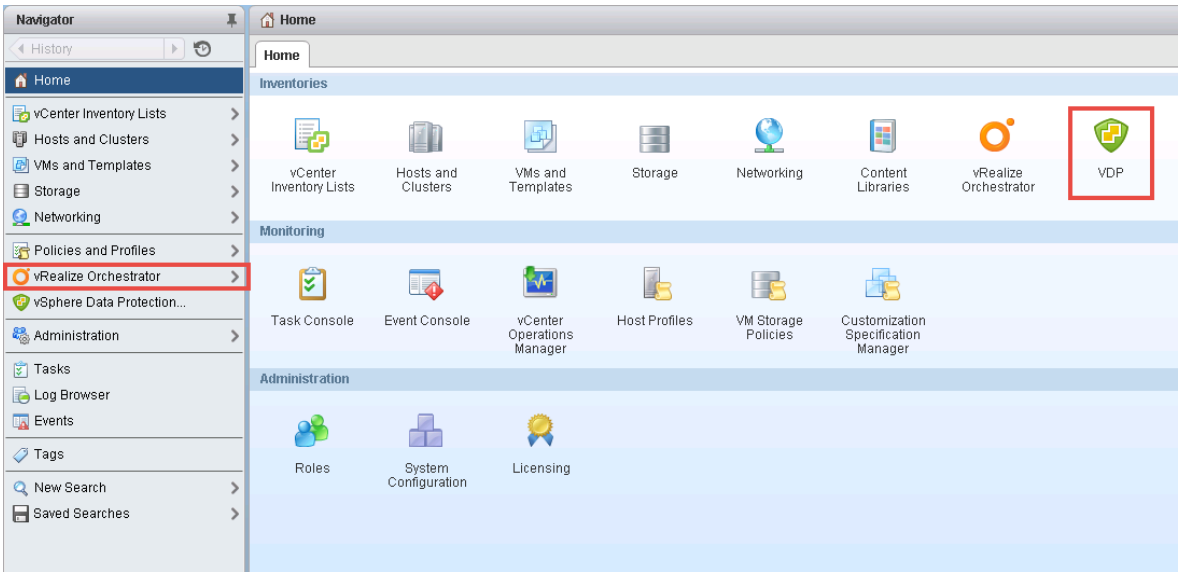
For additional guidance on minimum storage performance benchmarks, reference to page **71**, from the *VMware vSphere Data Protection Administration Guide*.

2.4 Configuring Backup Window on vSphere Data Protection

This section will cover how to change the amount of time available for processing backup requests.

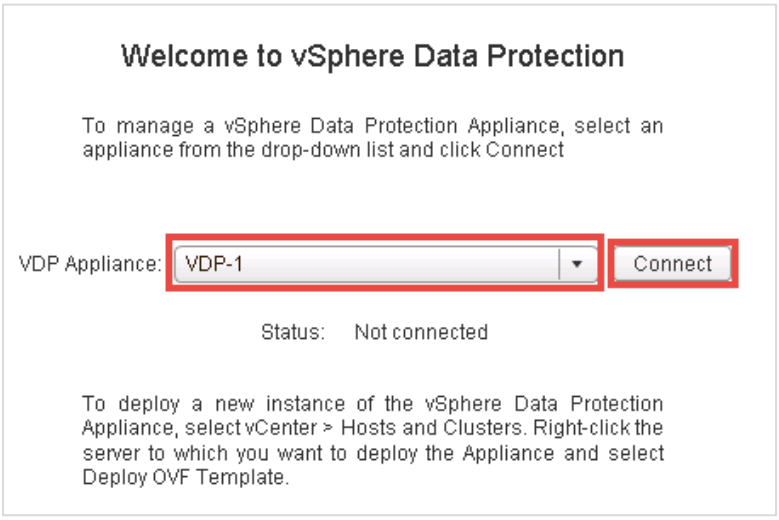
For additional guidance on editing the backup window, reference to pages **54-55**, from the *VMware vSphere Data Protection Administration Guide*.

1. To access the *VDP* appliance, log into the *vCenter* using the *Web Client*. On the **Home** tab, notice a **VDP** icon is present. Click on the icon to access the VDP control interface.

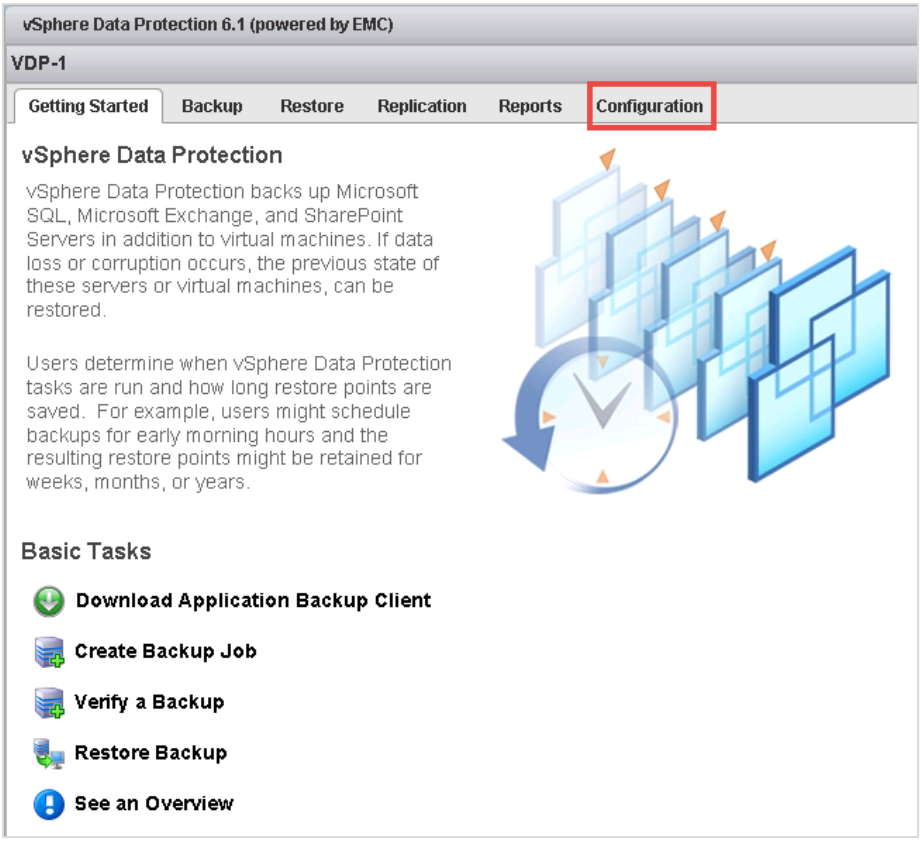


There is also a new entry in the *Navigator* pane, *vSphere Data Protection*. Clicking this will also access the same *VDP* controls.

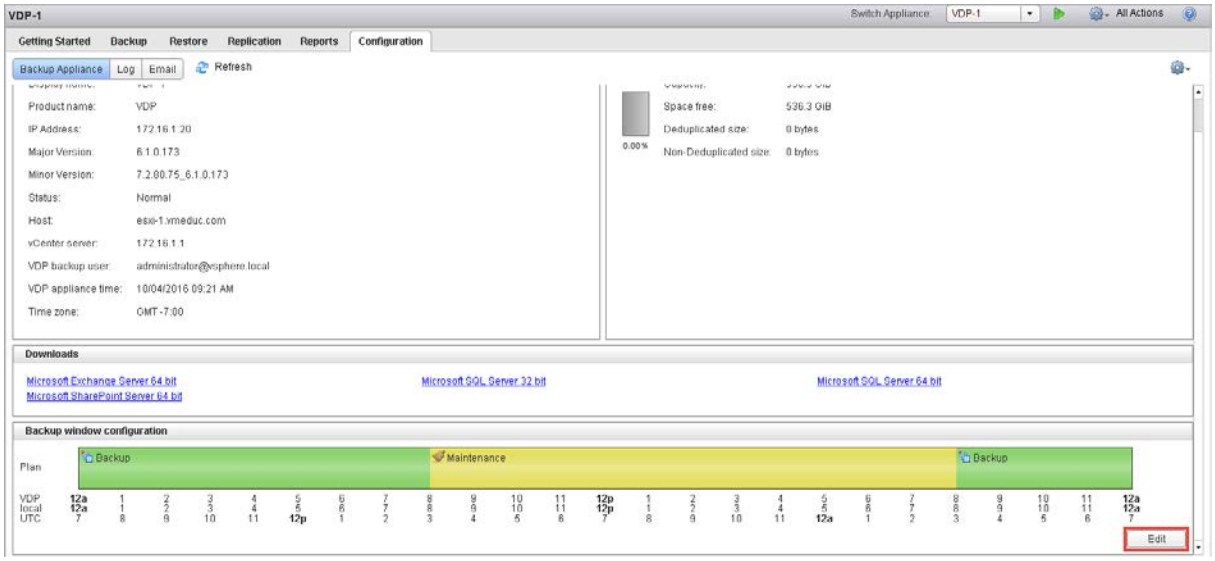
2. On the *Welcome to vSphere Data Protection* screen, select the newly deployed **VDP** appliance from the drop-down menu and click **Connect**.



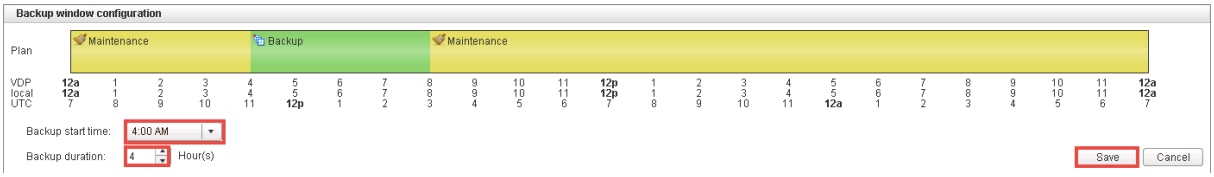
3. Once the *VDP* appliance control interface appears, click on the **Configuration** tab.



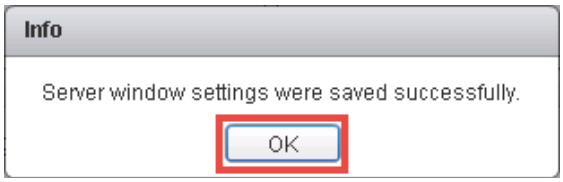
4. On the *Configuration* tab, scroll down to the **Backup window configuration** pane. Notice that the backup window by default is set to begin at 8 P.M. local time and is set to end at 8 A.M. local time. This leaves a 12-hour backup window by default. Click on the **Edit** button.



5. Notice the *Backup start time* and *Backup duration* configuration options appear. Configure the backup window times that work best for your policies. For this example, a backup window from 4 A.M. to 8 A.M local time is configured. Once finished, click **Save**.



6. A pop-up window appears, signaling a successful configuration. Click **OK**.

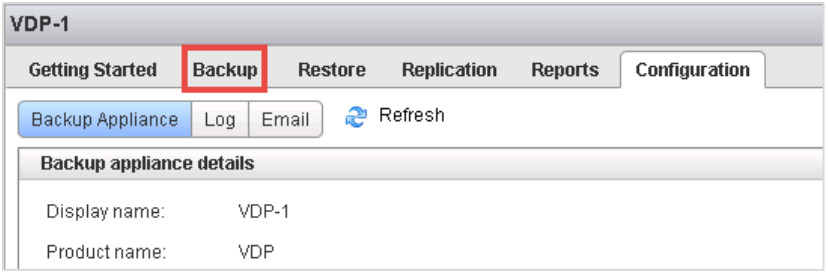


2.5 Creating a Backup Job

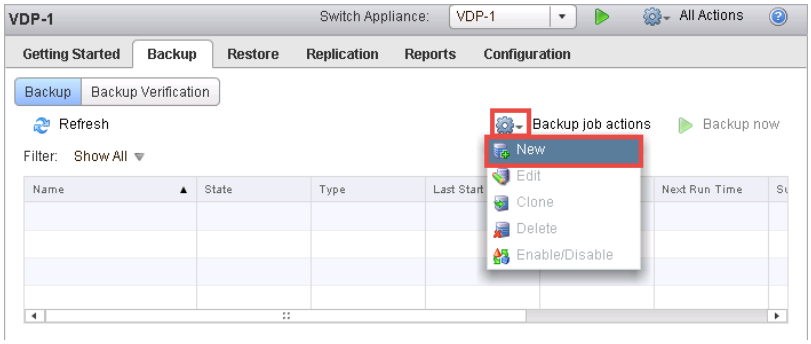
This section will cover on how to create a full image backup job for the *NETLAB+ VE* system.

For additional guidance on creating full image backup jobs, reference to pages **114-115**, from the *VMware vSphere Data Protection Administration Guide*.

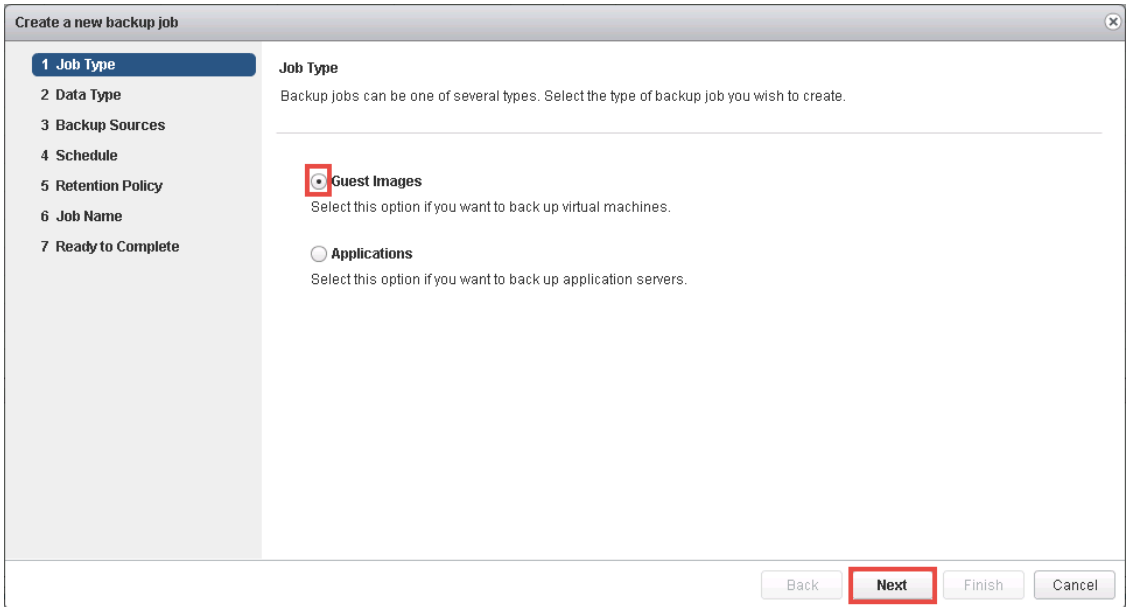
1. Click on the **Backup** tab to start the creation of a backup job.



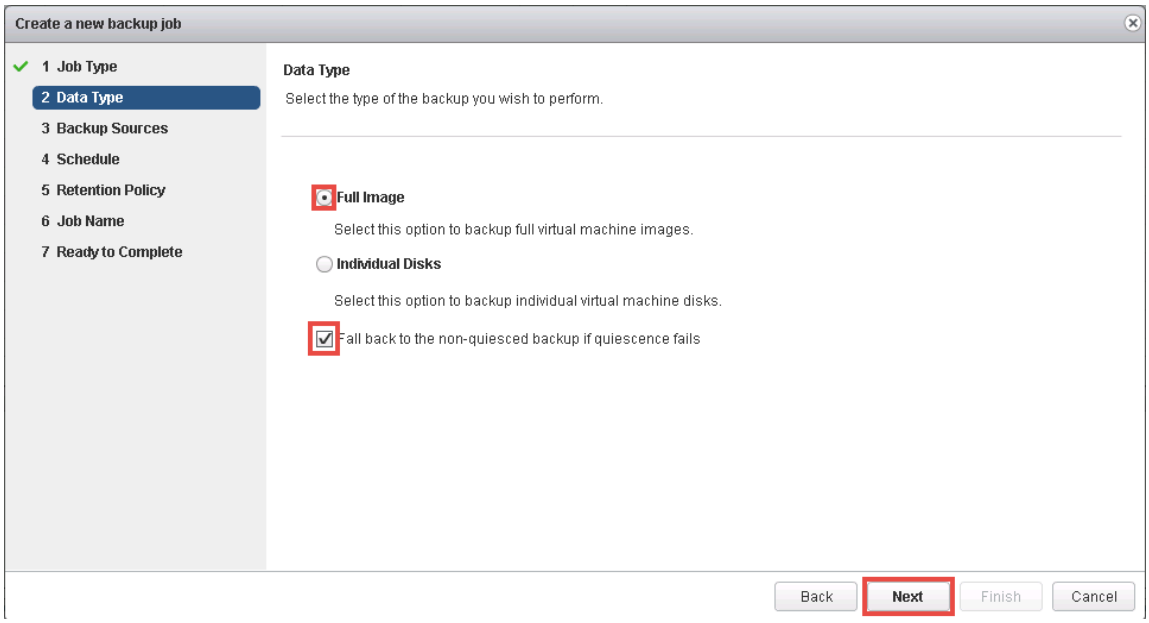
2. While viewing the *Backup* tab, click on **Backup job actions** and select **New**.



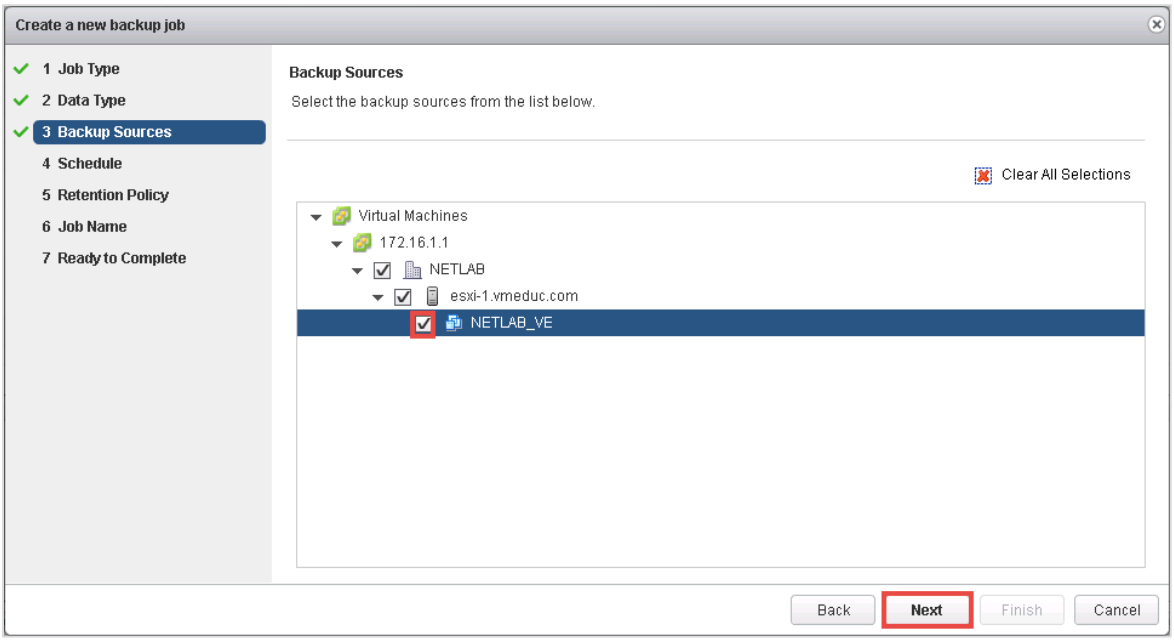
3. Notice that the *Create a new backup job* wizard appears. On the *Job Type* page, select **Guest Images** and click **Next**.



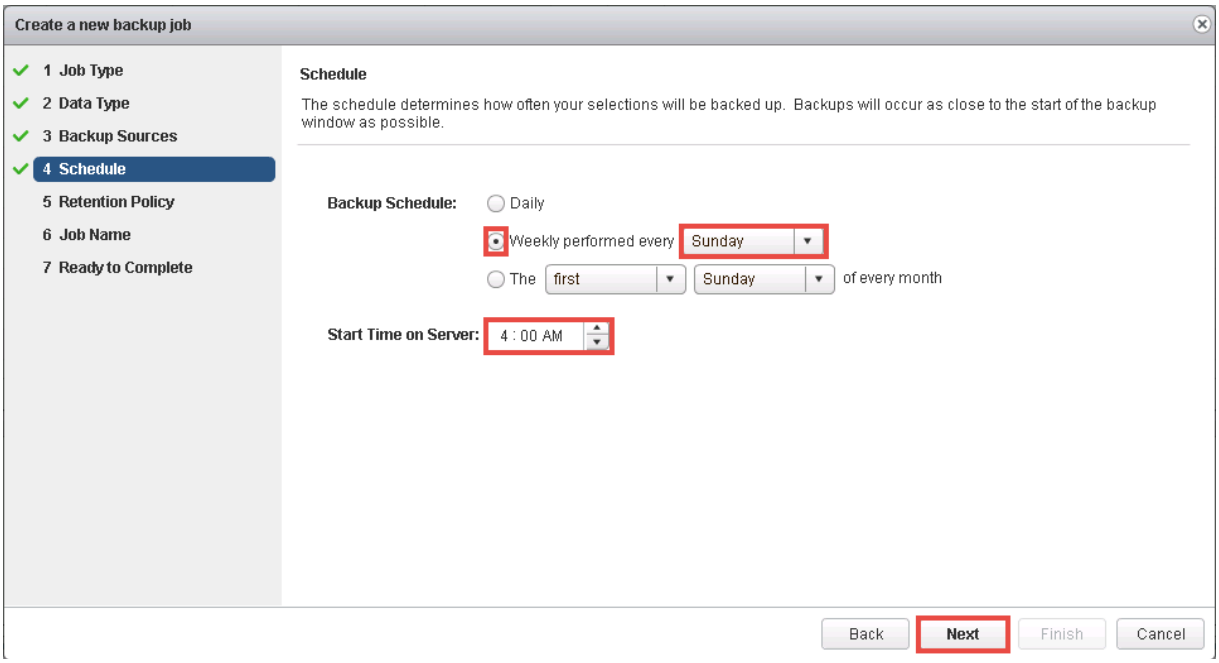
4. On the *Data Type* page, select **Full Image** and leave the box checked for **Fall back to the non-quiesced backup if quiescence fails**. Click **Next**.



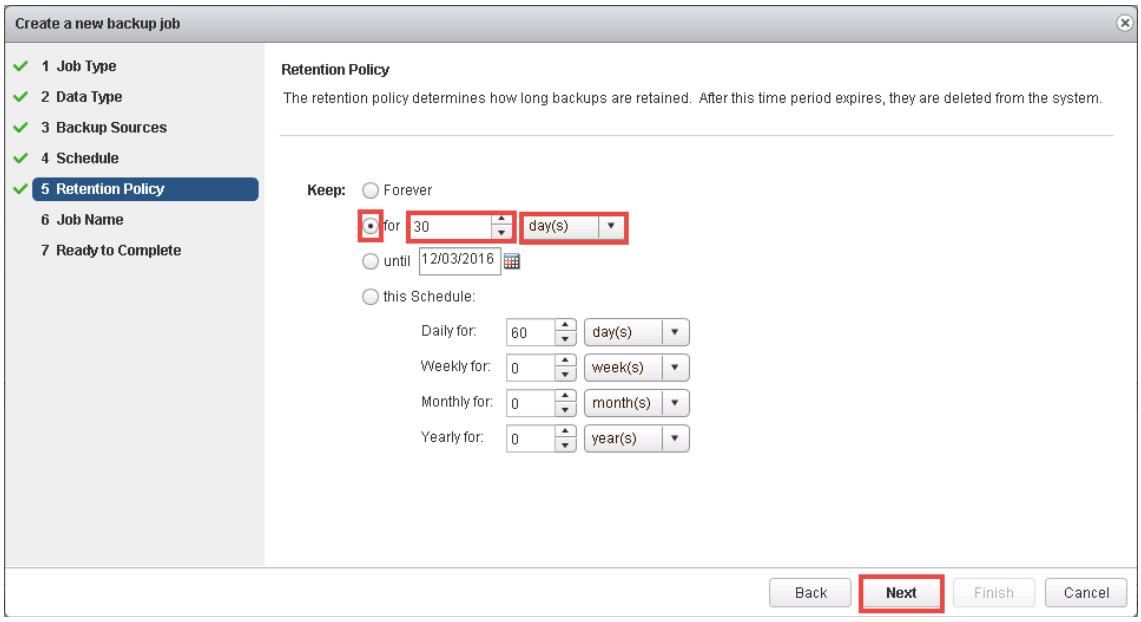
5. On the *Backup Sources* page, expand the list for **Virtual Machines** until the **NETLAB+ VE** virtual machine appears. Check the box for it. Click **Next**.



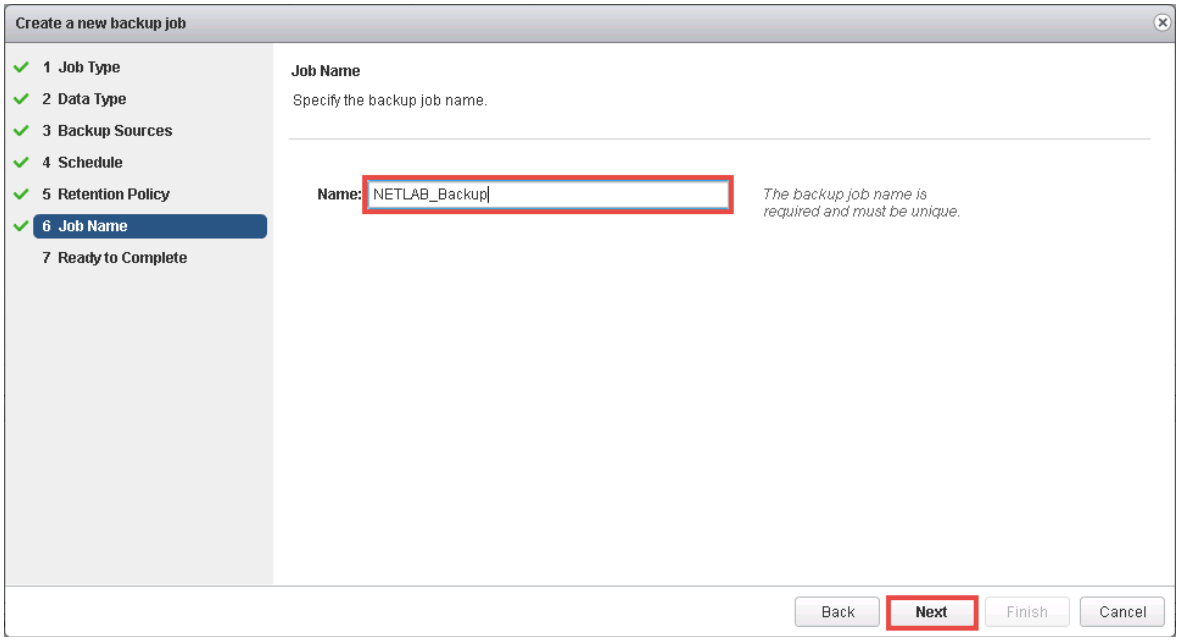
6. On the *Schedule* page, determine the frequency of how often you'd like to make full backups of the *NETLAB+ VE* virtual machine. For this example, a backup schedule of **Weekly** performed every **Sunday** at **4 A.M.** local time is configured.



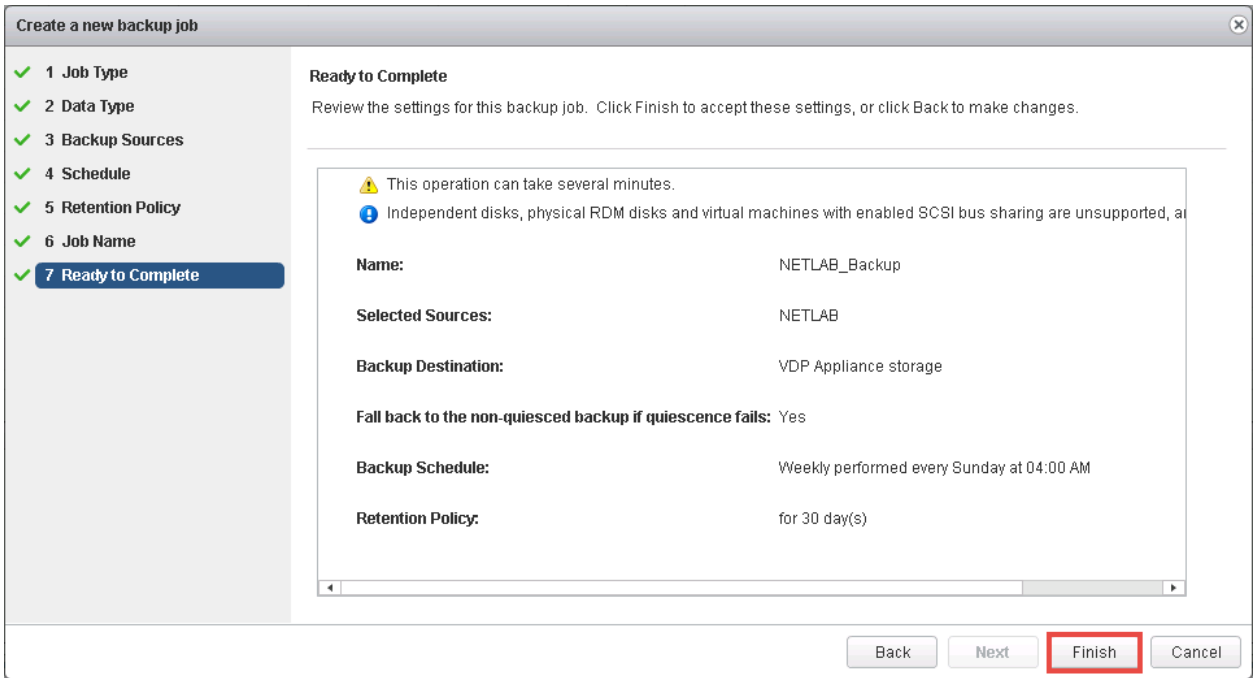
7. On the *Retention Policy* page, determine the policy for which you wish to retain the number of backups made for the *NETLAB+ VE* virtual machine. For this example, the retention policy is set so that each full backup created is retained for **30 days** from the moment it was created by the backup job. Click **Next** to continue.



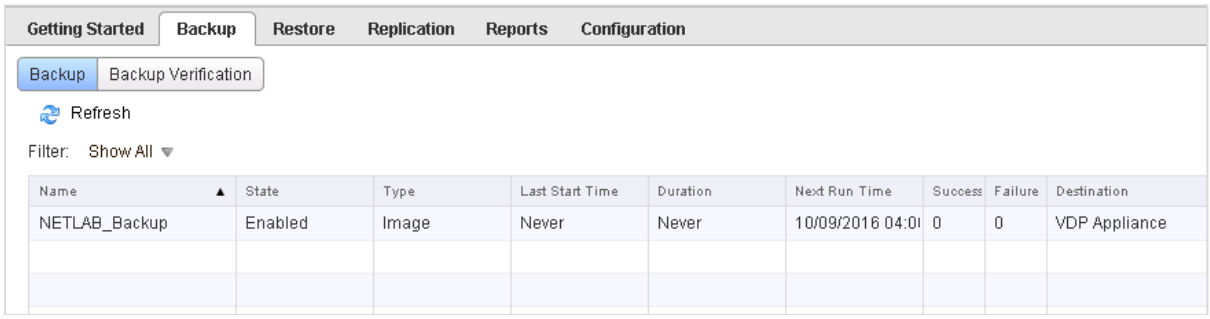
8. On the *Job Name* page, enter **NETLAB+_Backup** into the *Name* field. Click **Next**.



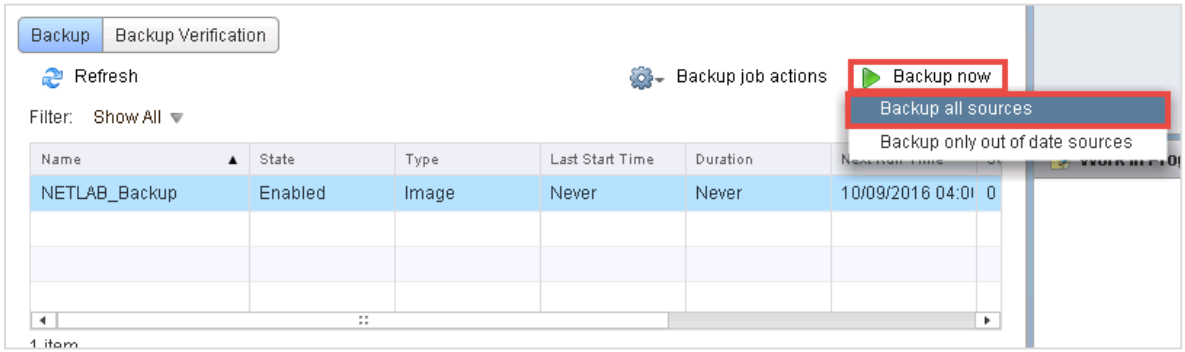
9. On the *Ready to Complete* page, review the configurations and click **Finish**.



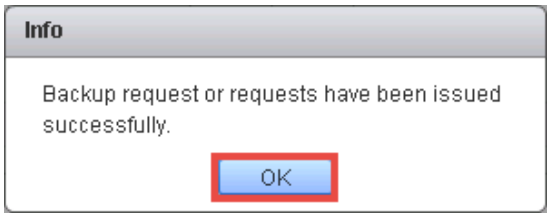
10. Notice the backup job now appears in the table on the *Backup* tab.



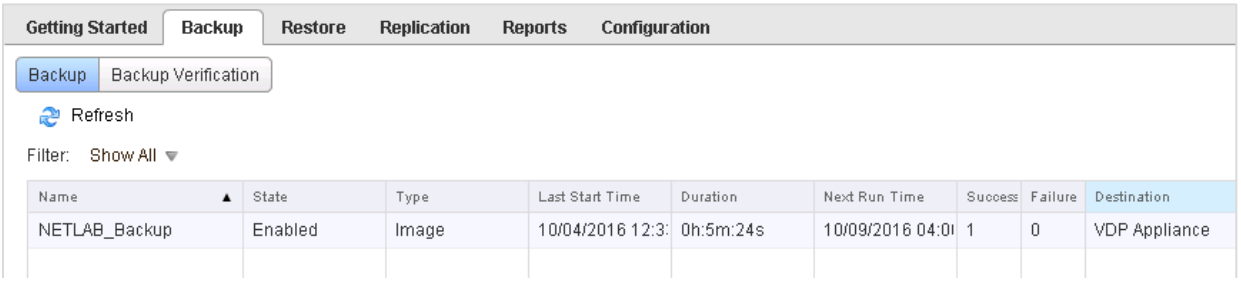
11. Run a test backup by clicking on **Backup now** followed by selecting **Backup all sources**.



12. Click **OK** in the dialog window to continue.



13. Monitor the progress of the backup in the *Recent Tasks* pane. Once completed, refresh the screen and notice a successful backup job.



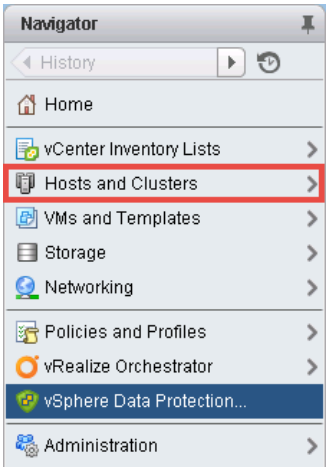
2.6 Restoring a Backup

This section will help guide through the steps on how to restore a *NETLAB+ VE* backup created from a backup job.

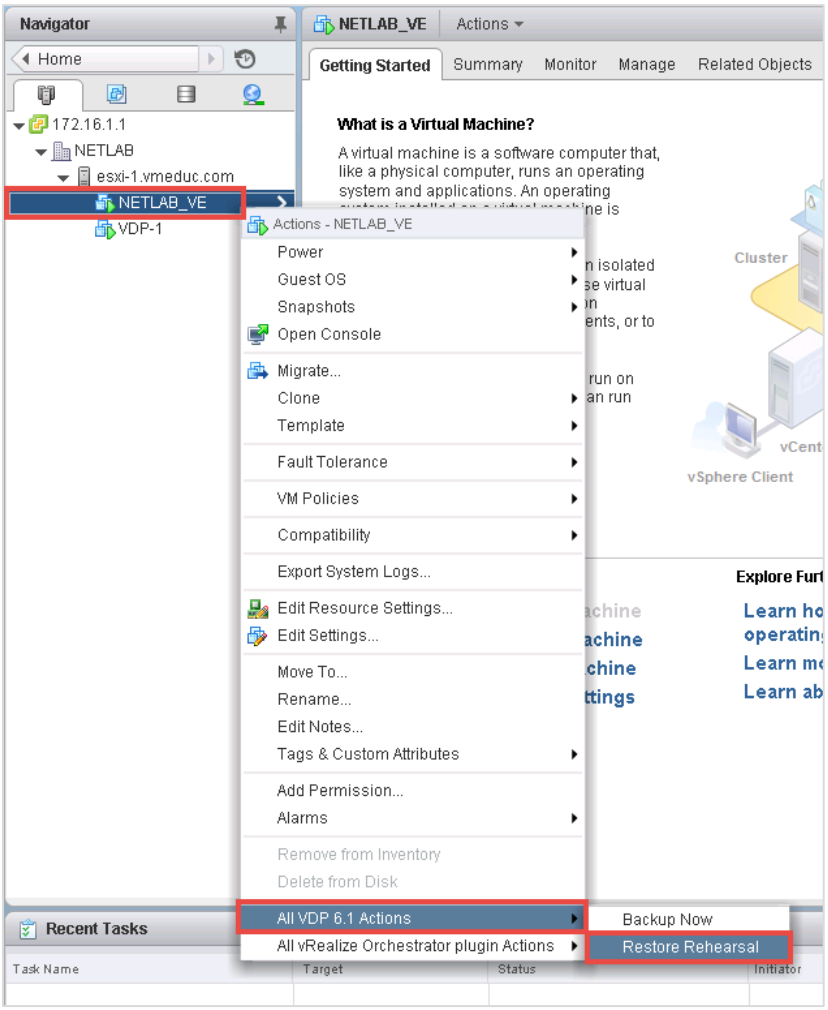
After restoring a backup of NETLAB+ VE, it will be necessary to reactivate your NETLAB+ VE system by entering your license key. After completing the steps below, see the *Manage License* section of the *NETLAB+ VE Administrator Guide* for details.

For additional guidance on restoring a backup, reference to pages **130-135**, from the*VMware vSphere Data Protection Administration Guide*.

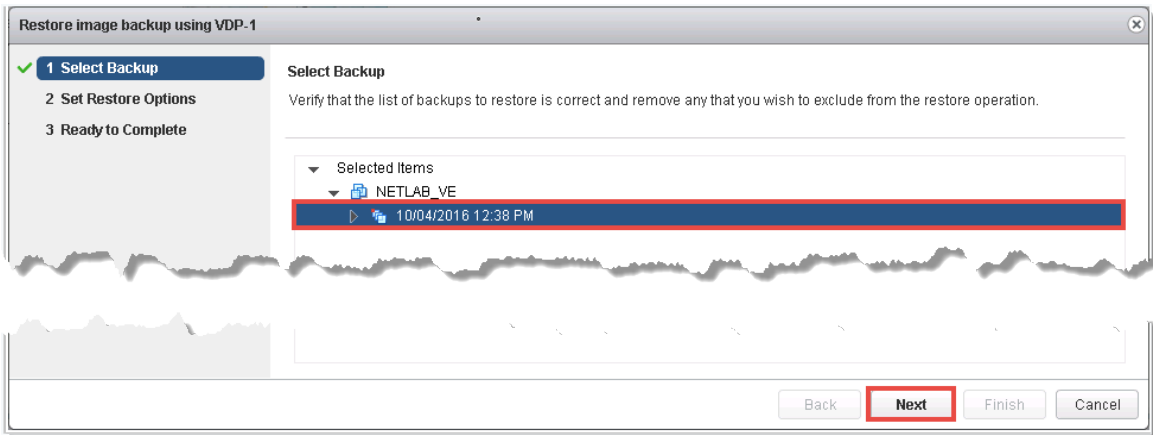
1. To restore a virtual machine from a backup job, navigate to **Hosts and Clusters** from the *Navigator* pane.



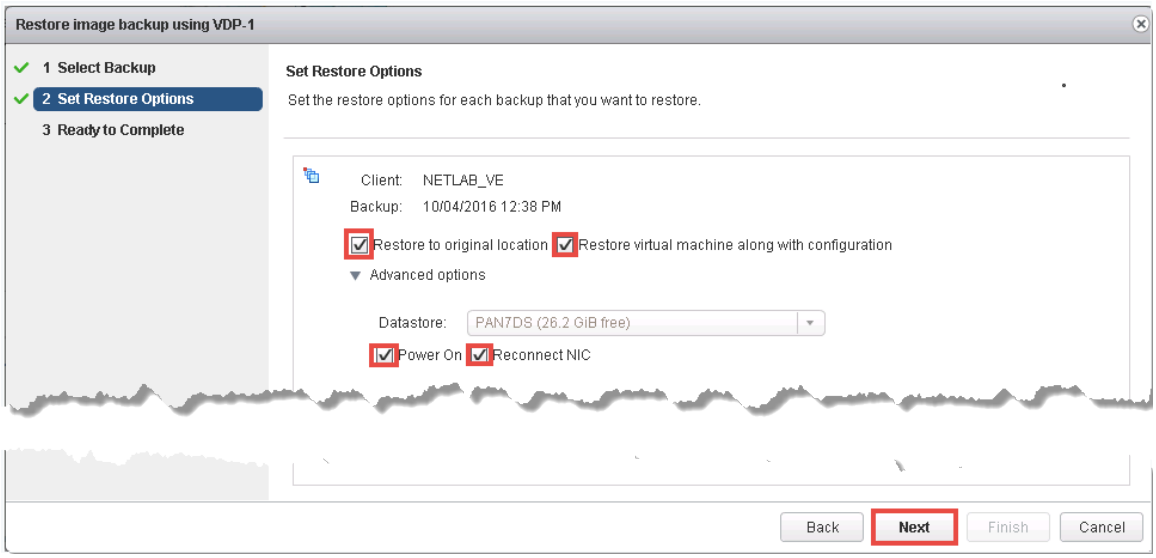
2. Expand the list in the *Navigator* pane and right-click on the **NETLAB+ VE** virtual machine, selecting **All VDP Actions > Restore Rehearsal**.



3. Notice a *Restore image backup using VDP* wizard appears. On the *Select Backup* page, choose **any desired backup** that you wish to restore from and click **Next**.

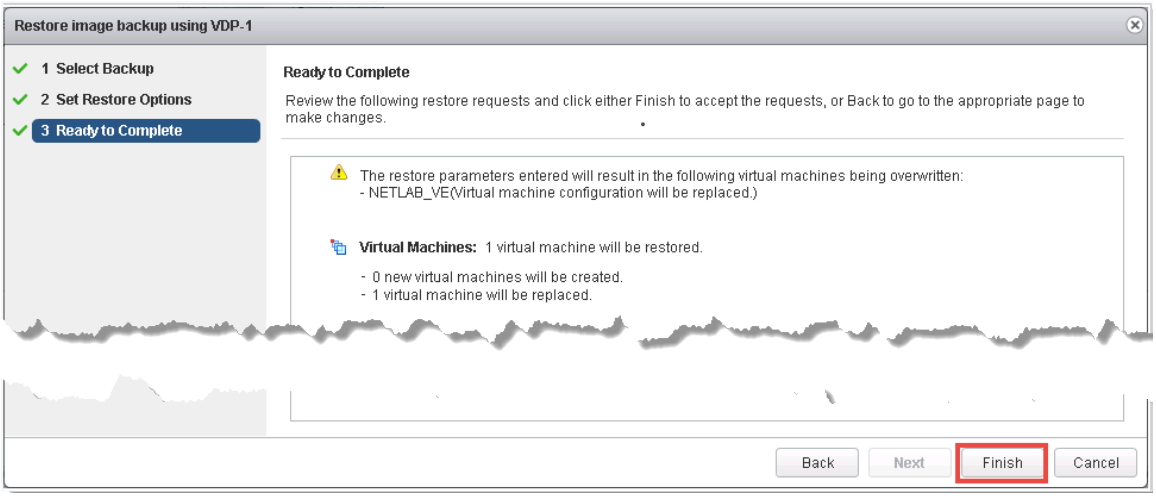


4. On the *Set Restore Options* page, check the boxes for **Restore to original location** and **Restore virtual machine along with configuration**. Expand the **Advanced options**, placing a check for **Power On** and **Reconnect NIC**. Click **Next**.



Choosing these settings will restore and replace the current NETLAB+ VE virtual machine that is in production. Because of this, click **Cancel** and make sure to **power off** the **NETLAB+ VE** virtual machine. If it is not powered off, the restore request will result in an error stating that it cannot be fulfilled due to the VM being powered on.

5. On the *Ready to Complete* page, review the restore request and click **Finish**.



6. Once the restore request initiates, notice the progress in the *Recent Tasks* pane to completion.
7. It will be necessary to reactivate your NETLAB+ VE system by entering your license key. Please refer to the *Manage License* section of the *NETLAB+ VE Administrator Guide* for details.

3 Additional Configuration Best Practices

This section will provide links to the *vSphere Data Protection Administration Guide* for best practices on optional configurations for the *VDP* appliance. These are not required to run backups but may prove useful to the administrator.

3.1 Configuring the Email Notifications and Reports

For guidance on configuring email notifications and reporting, reference to pages **55-56**, from the *VMware vSphere Data Protection Administration Guide*.

4 Common Alarms

This section will provide tips on fixing common alarms that may surface when initially deploying the *VDP* appliance.

For identifying alarm definitions pertinent to the *VDP* appliance, reference to page **59**, from the *VMware vSphere Data Protection Administration Guide*.

4.1 Maintenance Services are not Running

If a "VDP: Maintenance services are not working" alarm appears, the steps outlined below will help manually start the maintenance services on the VDP appliance.

1. Either **SSH** or **directly console** into the *vSphere Data Protection* system.
2. Once direct access is initiated, log into the system using **root** as the *username* and the password in which was configured on the system.
3. Using the shell, enter the command below to view the status of the maintenance windows scheduler.

```
dpnctl status
```

4. Start the maintenance windows by entering the command below.

```
dpnctl start maint
```

5. Confirm the status of the maintenance windows scheduler to make sure it is now enabled. Enter the command below.

```
dpnctl status
```

