



## Automated Backups Guide

Document Version: **2017-08-03**

Copyright © 2017 Network Development Group, Inc.  
[www.netdevgroup.com](http://www.netdevgroup.com)

NETLAB Academy Edition, NETLAB Professional Edition, and NETLAB+ are registered trademarks of Network Development Group, Inc.

VMware is a registered trademark of VMware, Inc. Cisco, IOS, Cisco IOS, Networking Academy, CCNA, and CCNP are registered trademarks of Cisco Systems, Inc. EMC<sup>2</sup> is a registered trademark of EMC Corporation.

## 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.

 Datacenter & Cloud Infrastructure	
VMware vCloud Suite	<a href="#">Download Product</a>   <a href="#">Drivers &amp; Tools</a>
VMware vSphere with Operations Management	<a href="#">Download Product</a>   <a href="#">Drivers &amp; Tools</a>   <a href="#">Get Training</a>
VMware vSphere	<a href="#">Download Product</a>   <a href="#">Drivers &amp; Tools</a>   <a href="#">Download Trial</a>   <a href="#">Get Training</a>
VMware vSAN	<a href="#">Download Product</a>   <a href="#">Drivers &amp; Tools</a>   <a href="#">Download Trial</a>   <a href="#">Get Training</a>
VMware vSphere Data Protection Advanced	<a href="#">Download Product</a>   <a href="#">Drivers &amp; Tools</a>   <a href="#">Get Training</a>
VMware vSphere Storage Appliance	<a href="#">Download Product</a>   <a href="#">Drivers &amp; Tools</a>
VMware vSphere Hypervisor (ESXi)	<a href="#">Download Product</a>   <a href="#">Drivers &amp; Tools</a>   <a href="#">Get Training</a>
VMware vCloud Director	<a href="#">Download Product</a>   <a href="#">Drivers &amp; Tools</a>   <a href="#">Get Training</a>


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*.

Product/Details	
<b>VMware vSphere Data Protection - Upgrade ISO</b> File size: 5.048 GB File type: iso  <a href="#">Read More</a>	<a href="#">Download Now</a>  <a href="#">Download Manager</a>
<b>VMware vSphere Data Protection</b> File size: 5.494 GB File type: ova  <a href="#">Read More</a>	<a href="#">Download Now</a>  <a href="#">Download Manager</a>

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.







You either are not entitled or do not have permissions to download this product. Check with your My VMware Super User, Procurement Contact or Administrator.

If you recently purchased this product through VMware Store or through a third-party, try downloading later.

[Download Trial](#)

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)**.

### Download Packages

	Download the hypervisor (vSphere ESXi Installable)
	Download VMware vCenter Server - Choose only one of the options based on which type of vCenter you want to run.
	Download VMware vRealize Operations and vRealize Log Insight
	Download additional components (optional)

(<sup>1</sup>)Click for information about using MD5 checksums, SHA-1 checksums and SHA-256 checksums.

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

Download additional components (optional)

Optional packages

The following packages are all optional for the usage and deployment of vSphere.

---

**VMware vSphere Replication 6.1.11 Appliance - \*.iso disk image**  
2016-11-10 | 6.1.11 | 1.144 GB | iso

Manually Download

**MD5SUM(\*)**: 5127873868b9df9c5a1264c4b6bb8c41  
**SHA1SUM(\*)**: 48a9bb0ecc281ea8e8228665412b64f5a20e6828  
**SHA256SUM(\*)**: c964785df65890c62b526ec317c0ea2ffac60ca347a4d5343f4fb7b204efff11

---

**VMware vSphere Data Protection**  
2015-09-10 | 6.1 | 5.233 GB | .ova

Manually Download

OVA file for VMware vSphere Data Protection.  
Right-click the '.ova' link to download and save the file locally with the .ova extension. Use the VMware vSphere Web Client to import this .ova file to your setup

**MD5SUM(\*)**: 9cd6055b45428ecc9f9e279ca5756a35  
**SHA1SUM(\*)**: 3ae7b3710253c0a4471e2f69f4af8b22b6625ab1

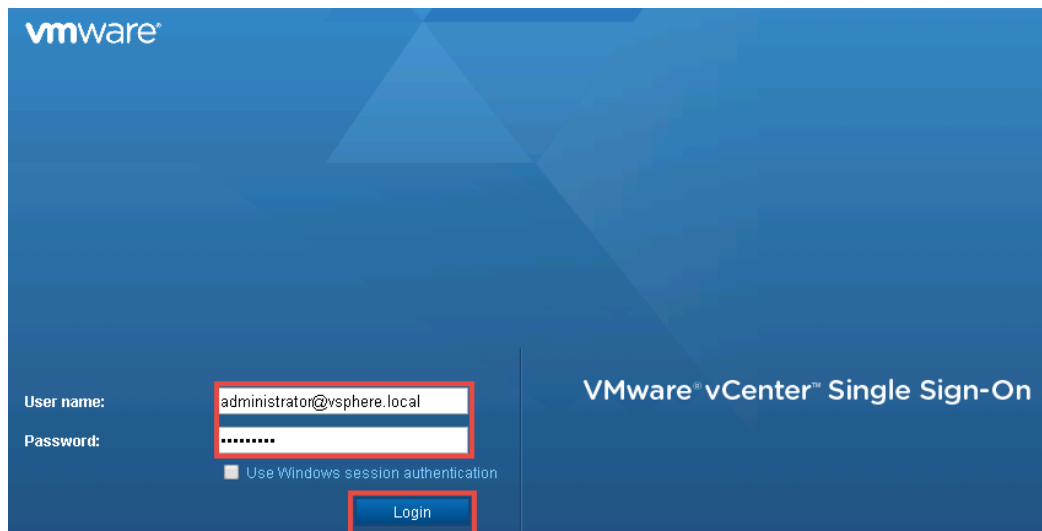
- The download should now begin.

## 2.2 Deploying vSphere Data Protection

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

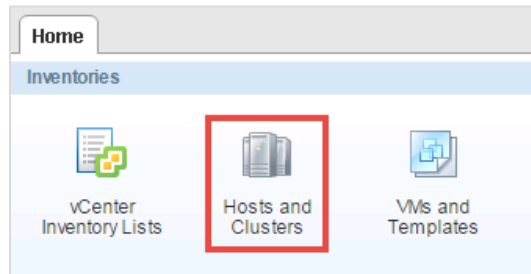
For additional guidance on deploying *VDP*, reference to pages **29-30**, from the [VMware vSphere Data Protection Administration Guide](#).

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

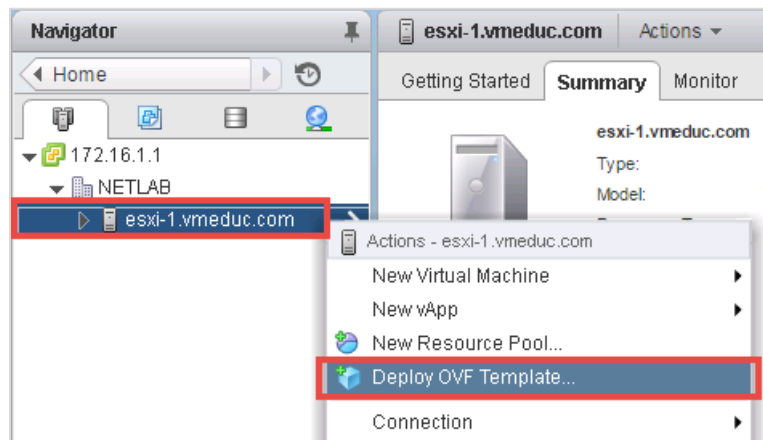


Before proceeding any further, verify that *VMware Client Integration Plug-in* is installed and running on the web browser being used for the *Web Client*. It can be confirmed if the plugin is installed by seeing whether or not the “*Download Client Integration Plugin*” message appears on the bottom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

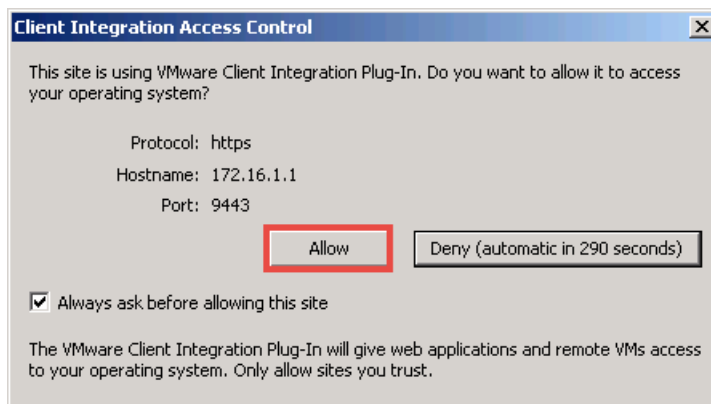
2. Once logged in, on the *Home* tab, click on the **Hosts and Clusters** icon.



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

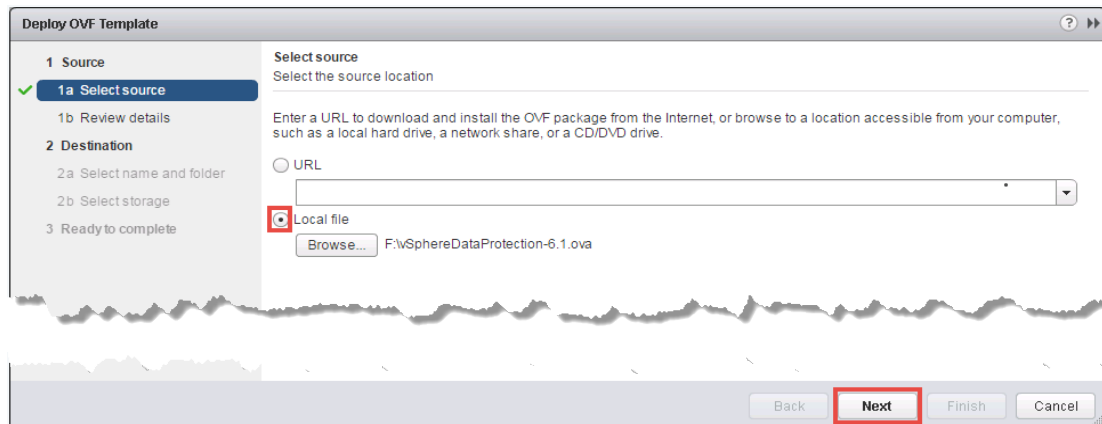


4. Once the *Deploy OVF Template* wizard appears, notice that a *Client Integration Access Control* window may appear. Click **Allow** (or anything similar - browser dependent) to initiate access for the plugin utility.

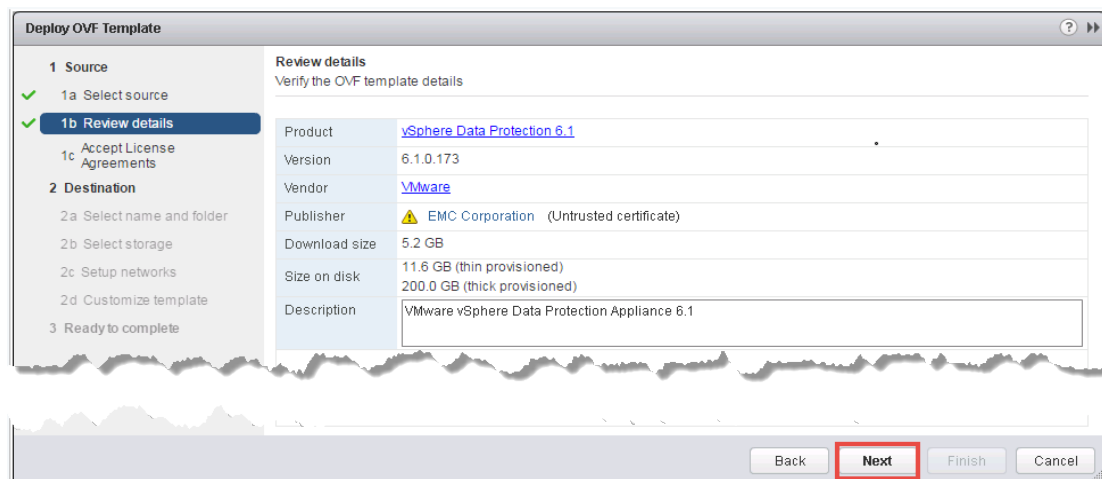




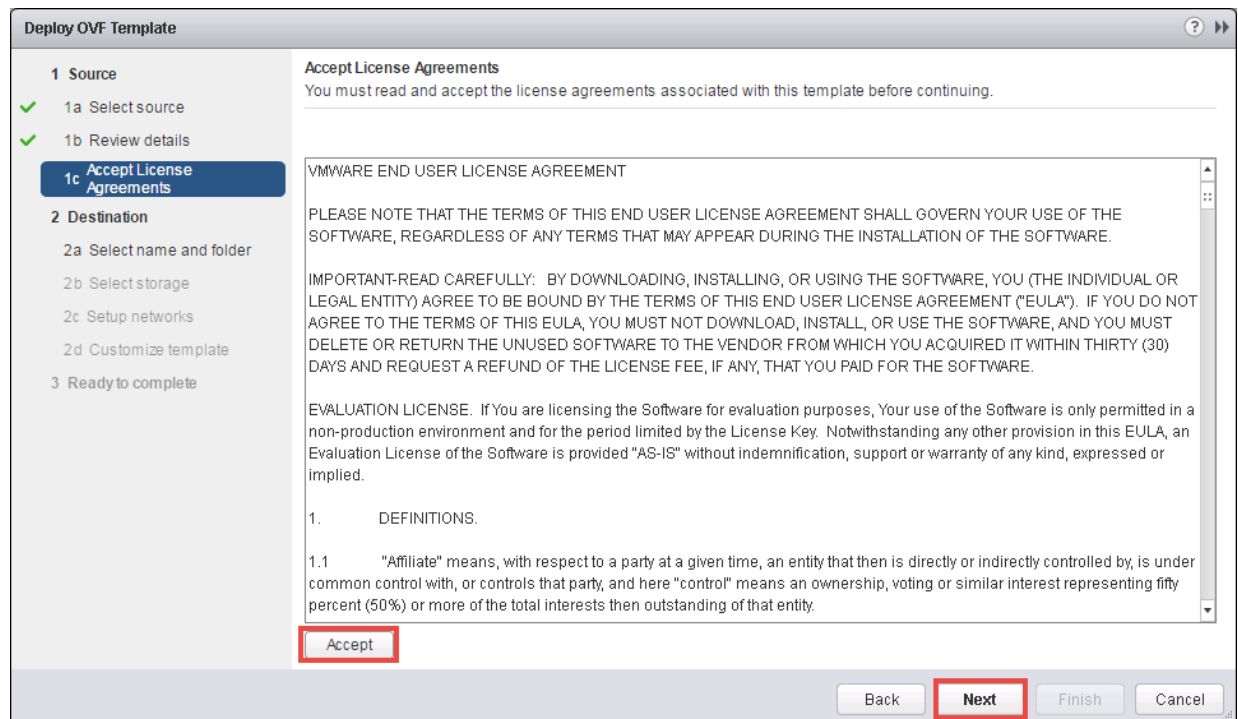
5. In the *Deploy OVF Template* window, in the *Select source* page, choose either **URL** or **Local file**, depending on where the *vSphereDataProtection-x.x.ovf* file is stored. For this example, the OVA is stored locally on the client machine. Click **Next**.



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

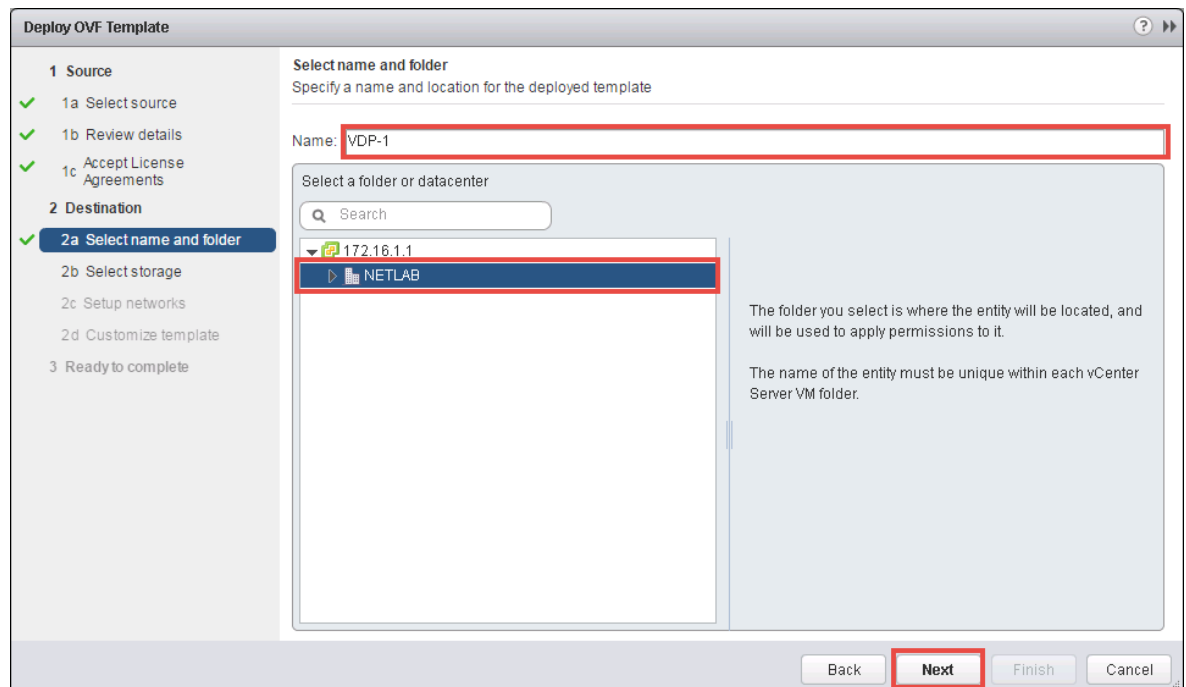


7. On the *Accept License Agreements* page, read and **Accept** the license agreements. When finished, click **Next**.



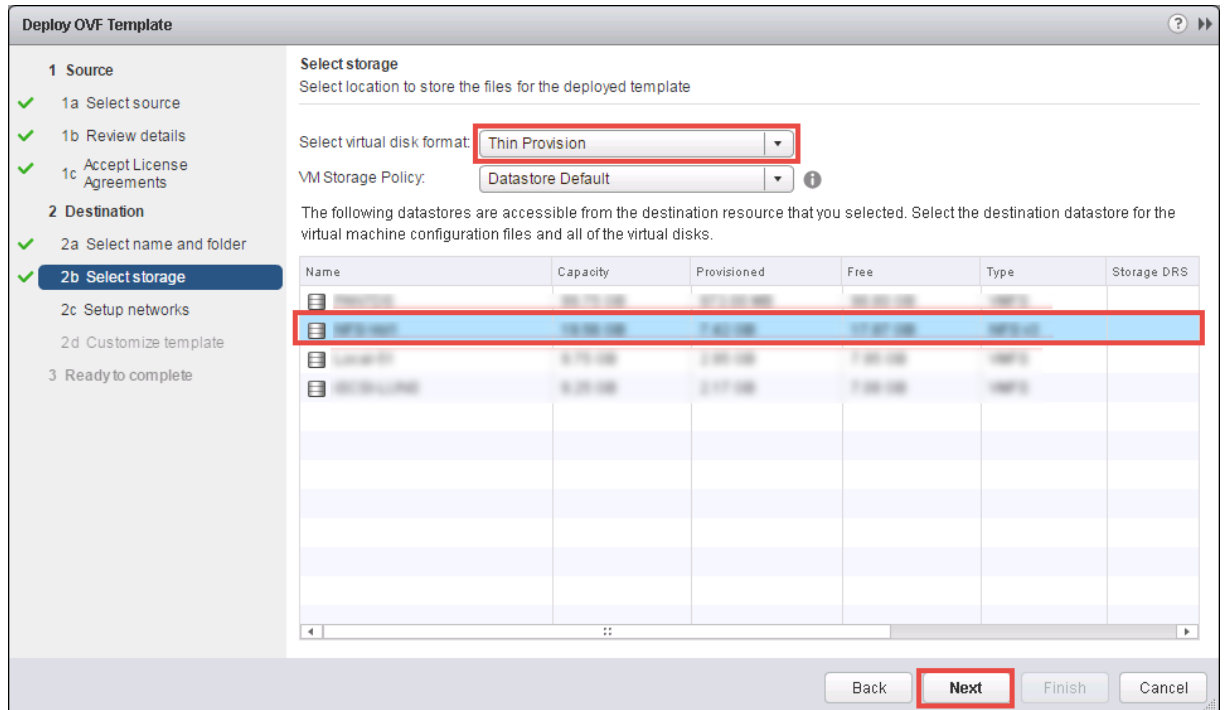
The screenshot shows the 'Deploy OVF Template' wizard at the 'Accept License Agreements' step. The left sidebar shows the progress: 1 Source (1a Select source, 1b Review details, 1c Accept License Agreements), 2 Destination (2a Select name and folder, 2b Select storage, 2c Setup networks, 2d Customize template), and 3 Ready to complete. The main area displays the 'VMWARE END USER LICENSE AGREEMENT' text. At the bottom, the 'Accept' button is highlighted with a red box, and the 'Next' button in the footer is also highlighted with a red box.

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**.



The screenshot shows the 'Deploy OVF Template' wizard at the 'Select name and folder' step. The left sidebar shows the progress: 1 Source (1a Select source, 1b Review details, 1c Accept License Agreements), 2 Destination (2a Select name and folder, 2b Select storage, 2c Setup networks, 2d Customize template), and 3 Ready to complete. The main area has a 'Name' text field containing 'VDP-1' and a 'Select a folder or datacenter' list box with 'NETLAB' selected. The 'Next' button in the footer is highlighted with a red box.

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**.



**Deploy OVF Template**

**1 Source**

- 1a Select source
- 1b Review details
- 1c Accept License Agreements

**2 Destination**

- 2a Select name and folder
- 2b Select storage**
- 2c Setup networks
- 2d Customize template
- 3 Ready to complete

**Select storage**  
Select location to store the files for the deployed template

Select virtual disk format: **Thin Provision**

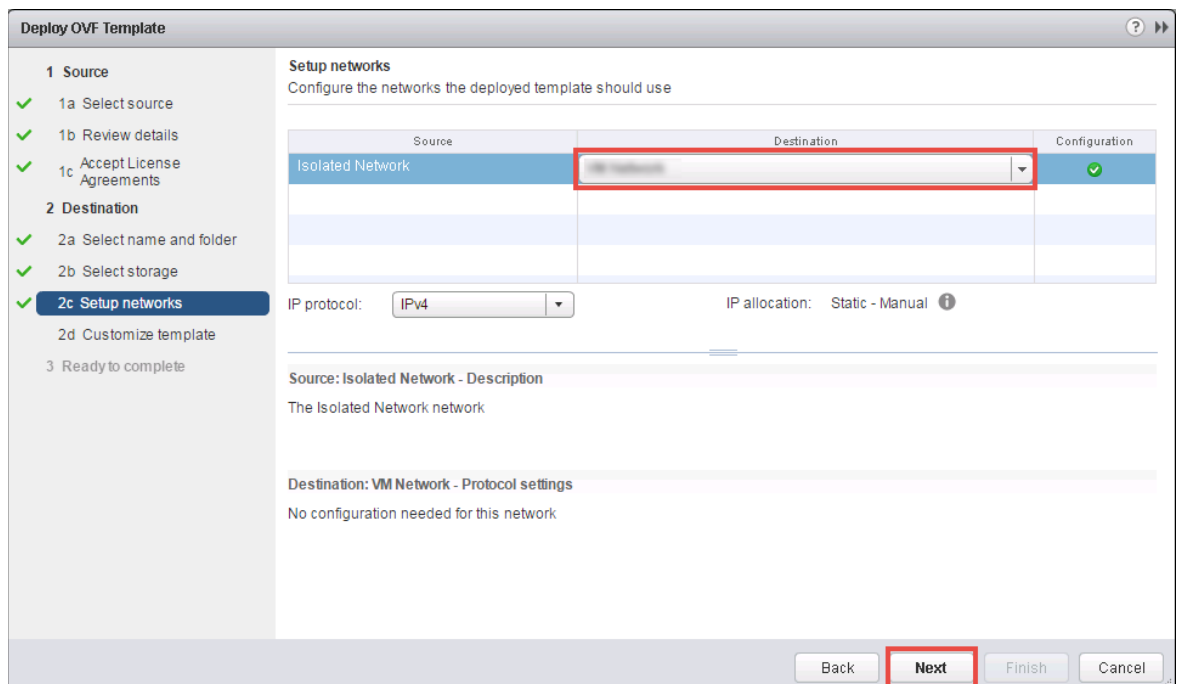
VM Storage Policy: **Datastore Default**

The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Provisioned	Free	Type	Storage DRS
datastore1	10.00 GB	0.00 GB	10.00 GB	VMFS	
datastore2	10.00 GB	0.00 GB	10.00 GB	VMFS	
datastore3	10.00 GB	0.00 GB	10.00 GB	VMFS	
datastore4	10.00 GB	0.00 GB	10.00 GB	VMFS	

Back **Next** Finish Cancel

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



**Deploy OVF Template**

**1 Source**

- 1a Select source
- 1b Review details
- 1c Accept License Agreements

**2 Destination**

- 2a Select name and folder
- 2b Select storage
- 2c Setup networks**
- 2d Customize template
- 3 Ready to complete

**Setup networks**  
Configure the networks the deployed template should use

Source	Destination	Configuration
Isolated Network	VM Network	✓

IP protocol: **IPv4** IP allocation: Static - Manual

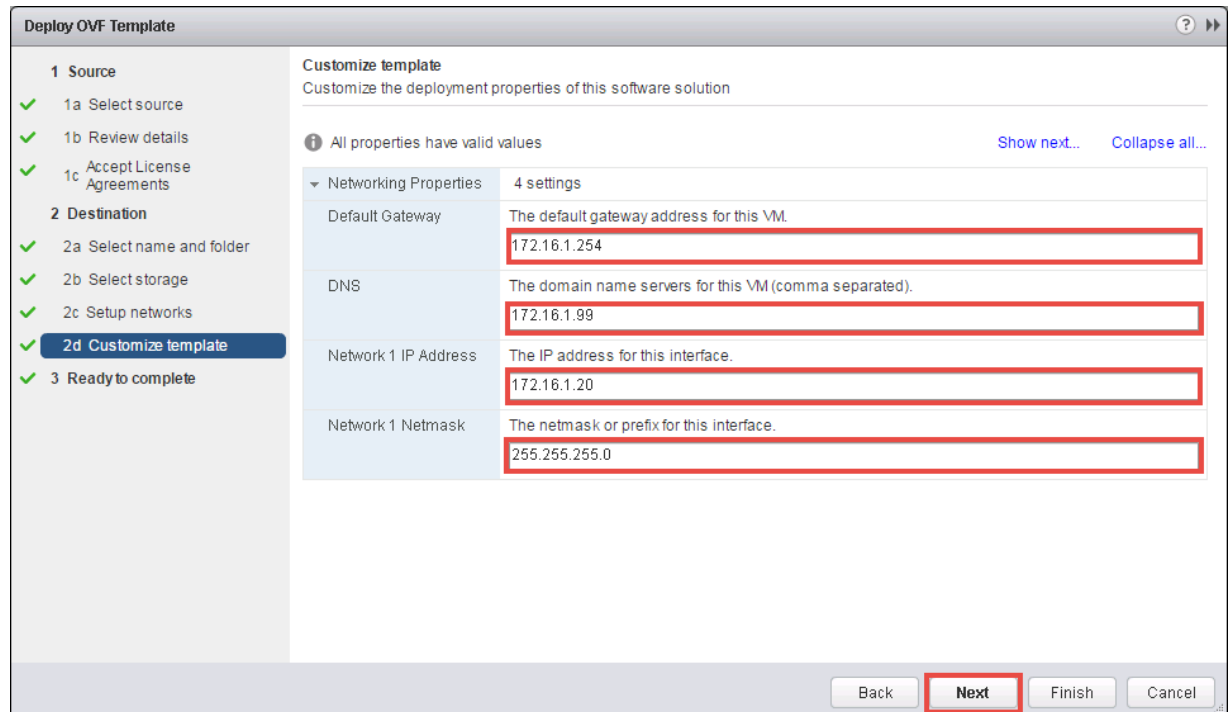
**Source: Isolated Network - Description**  
The Isolated Network network

**Destination: VM Network - Protocol settings**  
No configuration needed for this network

Back **Next** Finish Cancel

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.



**Deploy OVF Template**

**1 Source**

- 1a Select source
- 1b Review details
- 1c Accept License Agreements

**2 Destination**

- 2a Select name and folder
- 2b Select storage
- 2c Setup networks
- 2d Customize template**

**3 Ready to complete**

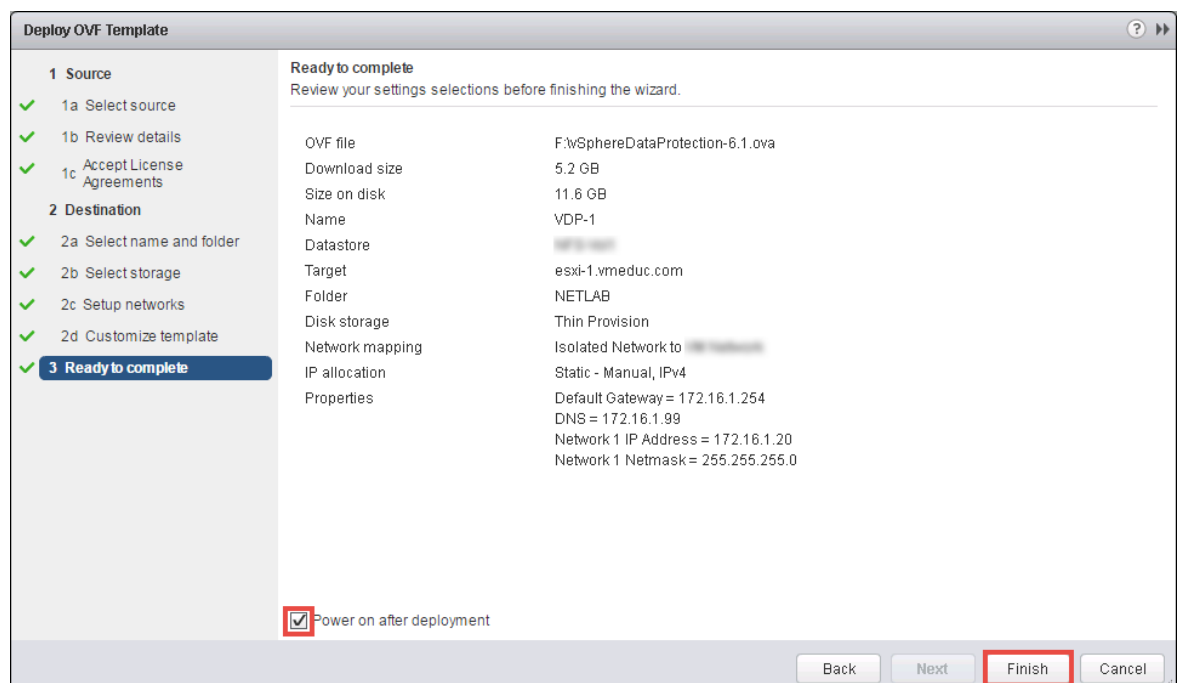
**Customize template**  
Customize the deployment properties of this software solution

**All properties have valid values** [Show next...](#) [Collapse all...](#)

Networking Properties	4 settings
Default Gateway	The default gateway address for this VM. 172.16.1.254
DNS	The domain name servers for this VM (comma separated). 172.16.1.99
Network 1 IP Address	The IP address for this interface. 172.16.1.20
Network 1 Netmask	The netmask or prefix for this interface. 255.255.255.0

Back **Next** Finish Cancel

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



**Deploy OVF Template**

**1 Source**

- 1a Select source
- 1b Review details
- 1c Accept License Agreements

**2 Destination**

- 2a Select name and folder
- 2b Select storage
- 2c Setup networks
- 2d Customize template
- 3 Ready to complete**

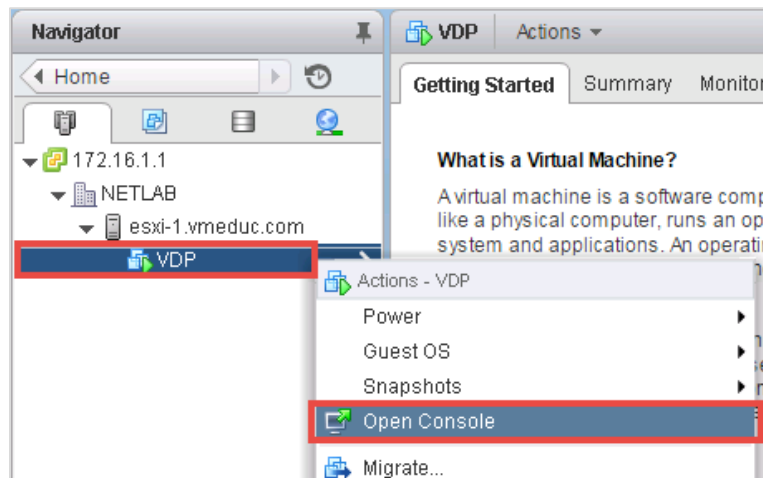
**Ready to complete**  
Review your settings selections before finishing the wizard.

OVF file	F:\wSphereDataProtection-6.1.ova
Download size	5.2 GB
Size on disk	11.6 GB
Name	VDP-1
Datastore	esxi-1.vmeduc.com
Target	esxi-1.vmeduc.com
Folder	NETLAB
Disk storage	Thin Provision
Network mapping	Isolated Network to
IP allocation	Static - Manual, IPv4
Properties	Default Gateway = 172.16.1.254 DNS = 172.16.1.99 Network 1 IP Address = 172.16.1.20 Network 1 Netmask = 255.255.255.0

☒ Power on after deployment

Back Next **Finish** Cancel

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.

```

*****
Welcome to the vSphere Data Protection 6.1 appliance. Version: 6.1.0.173

Quickstart Guide: (How to get VDP running quickly)

 1 - Open a browser to: https://172.16.1.20:8543/vdp-configure
 2 - Review the Network Settings
 3 - Enter the Time Zone
 4 - Enter the VDP credentials
 5 - Enter the vCenter Registration information
 6 - Click Test Connection
 7 - Click Finish

*****
SSL thumbprint for VDP server:
SHA256 Fingerprint=E2:AA:DE:C0:6A:C6:50:7B:8B:5B:21:35:5B:64:78:8F:CB:CB:A2:FB:4
C:C5:68:E3:96:AF:D3:80:9F:DE:0C:99
SHA1 Fingerprint=FD:14:71:27:21:E6:9D:45:A0:A8:A3:A1:C9:65:0D:68:0C:E4:96:C3

*****
*Login
Set Timezone (Current:PDT)

Use Arrow Keys to navigate
and <ENTER> to select your choice.

```

## 2.3 Configuring vSphere Data Protection

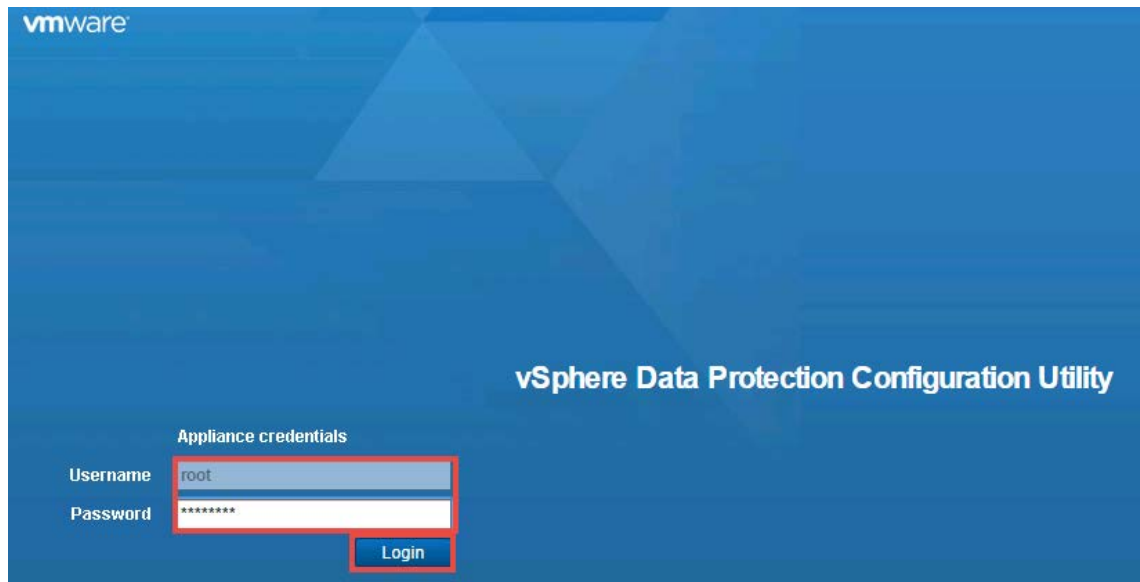
This section will provide guidance on how to configure the *VDP* appliance so that it can be added to *vCenter*.

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

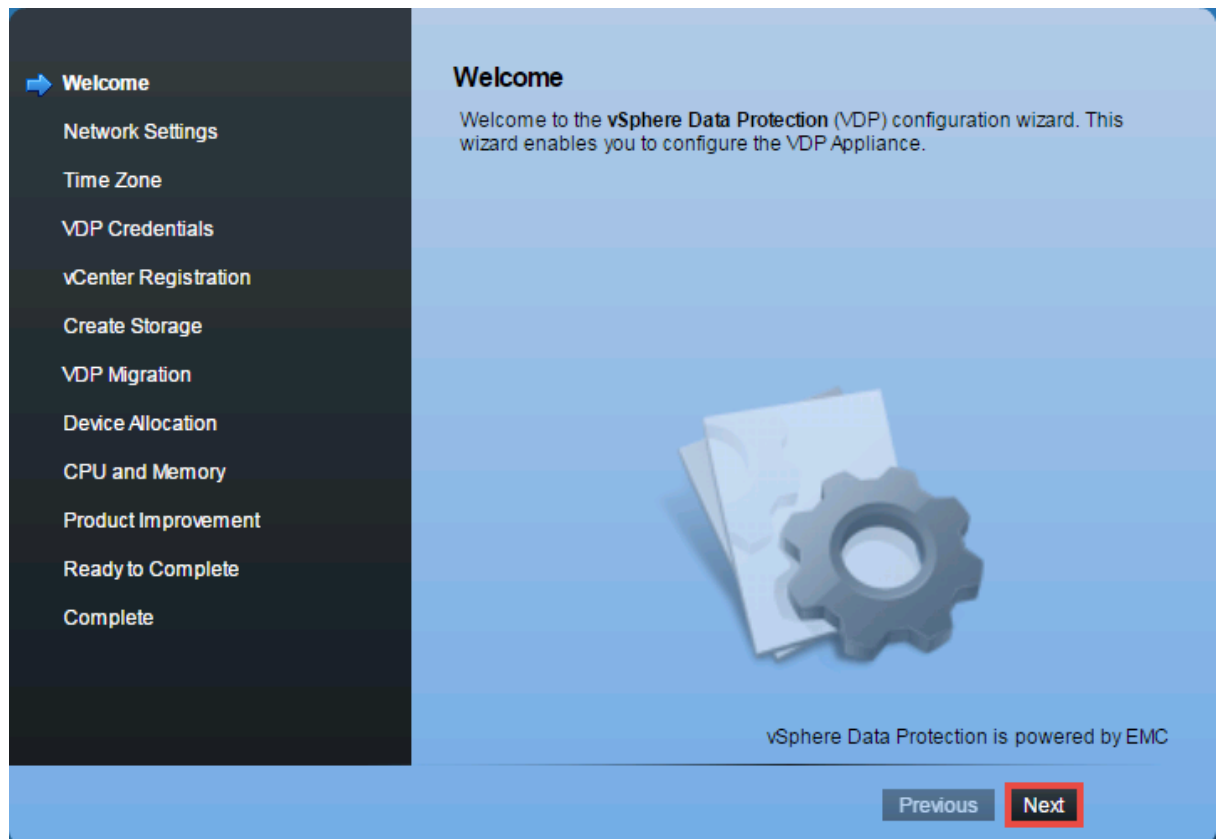
1. Using the client machine, open a **new tab** in the web browser and enter `https://YOUR_VDP_IP:8543/vdp-configure` into the address field and press the **Enter** key.

IP addresses will vary, depending on the infrastructure.

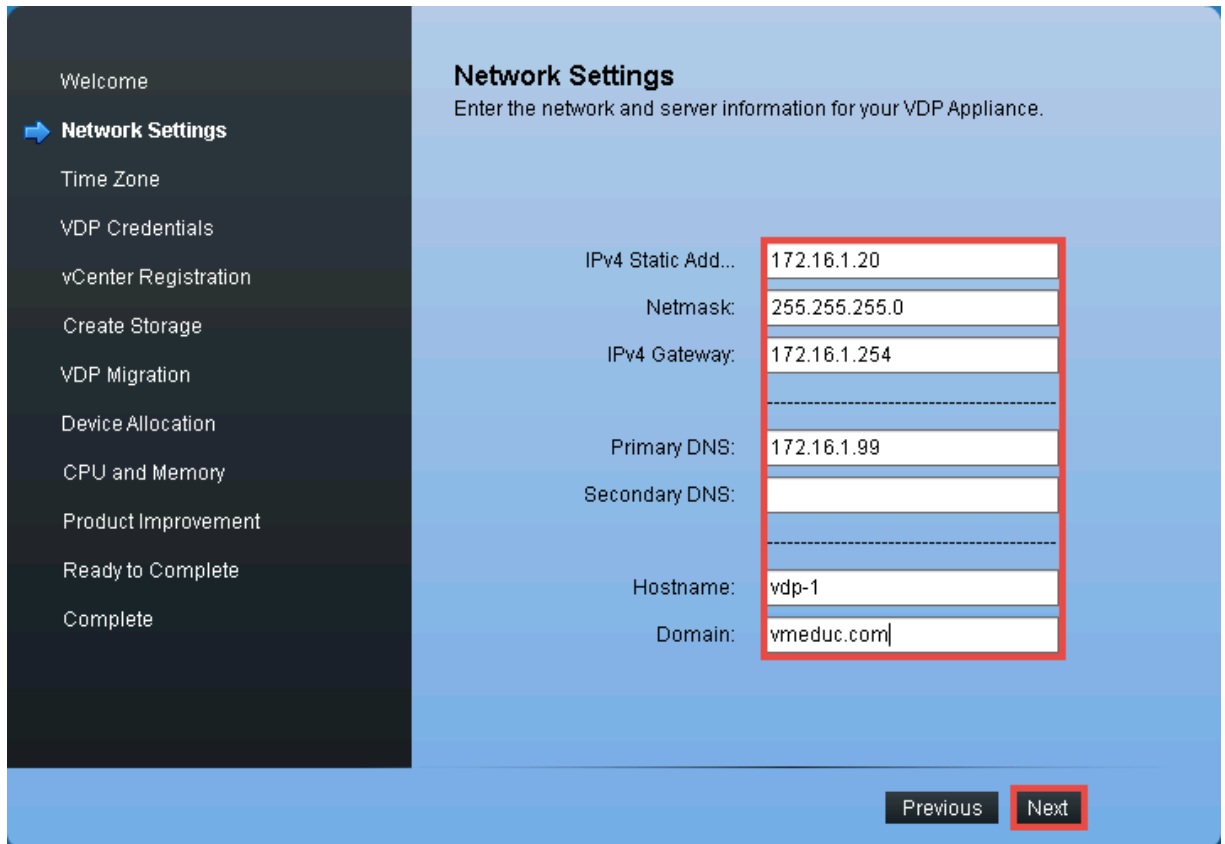
2. Once the web page redirects, notice an SSL certificate warning may appear. Depending on the web browser, proceed to the destination, ignoring the warnings.
3. On the *vSphere Protection Configuration Utility* login page, login using the default credentials; `root` as the *username* and `changeme` as the default *password*.



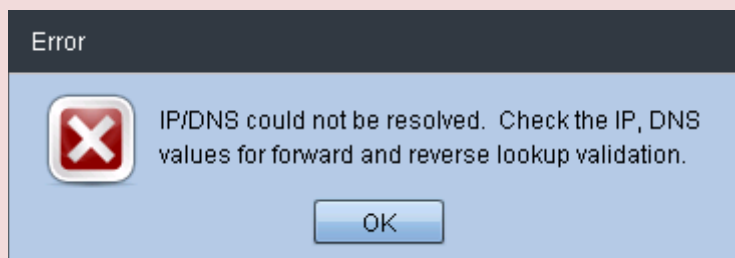
4. Once redirected, notice the welcome page for the *VDP* configuration wizard. Click **Next** to continue.



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



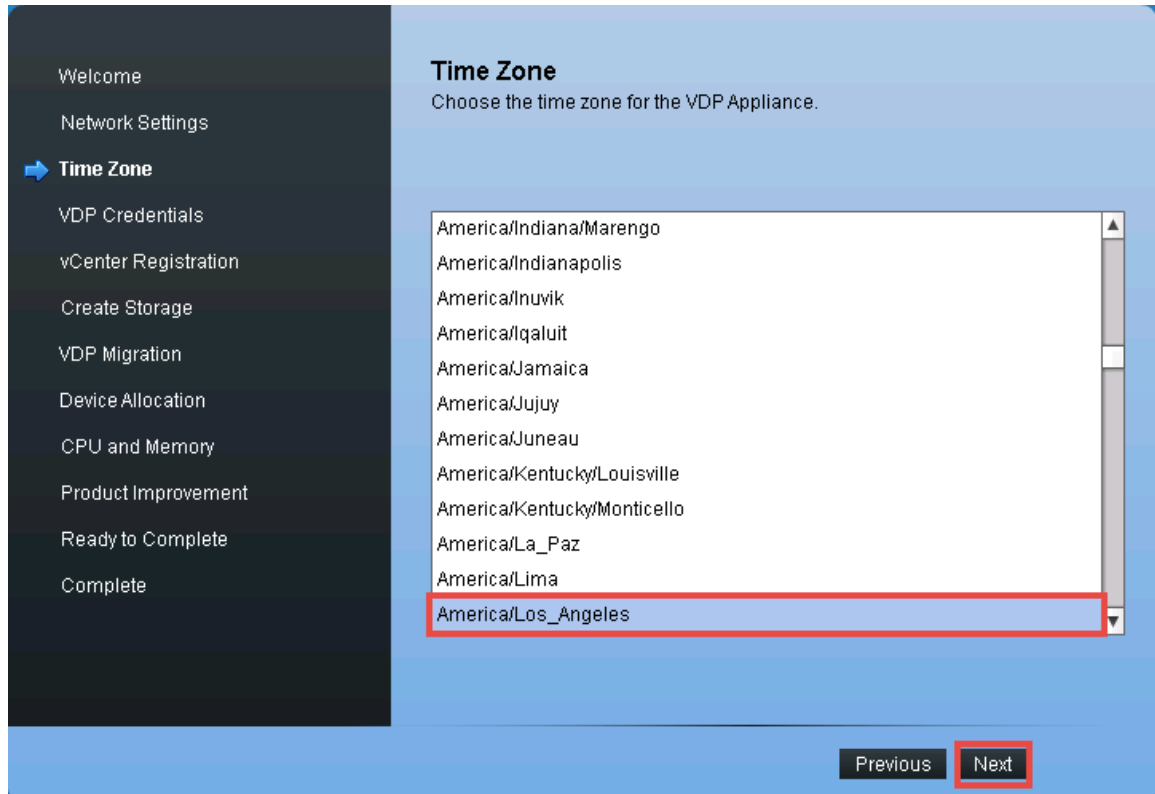
It is important to have *DNS* configured prior to initial *VDP* setup. A reverse *DNS* lookup (*PTR* record) needs to be configured on the local *DNS*, otherwise an error message will appear (see below):



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**.




**Time Zone**  
Choose the time zone for the VDP Appliance.

- America/Indiana/Marengo
- America/Indianapolis
- America/Inuvik
- America/Iqaluit
- America/Jamaica
- America/Jujuy
- America/Juneau
- America/Kentucky/Louisville
- America/Kentucky/Monticello
- America/La\_Paz
- America/Lima
- America/Los\_Angeles**

Previous **Next**

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



**VDP Credentials**  
Enter a password for the VDP Appliance.

**Four character classes:**  
Upper case letters A-Z  
Lower case letters a-z  
Numbers 0-9  
Special characters (Examples: ~!@#,.)

**Passwords criteria:**

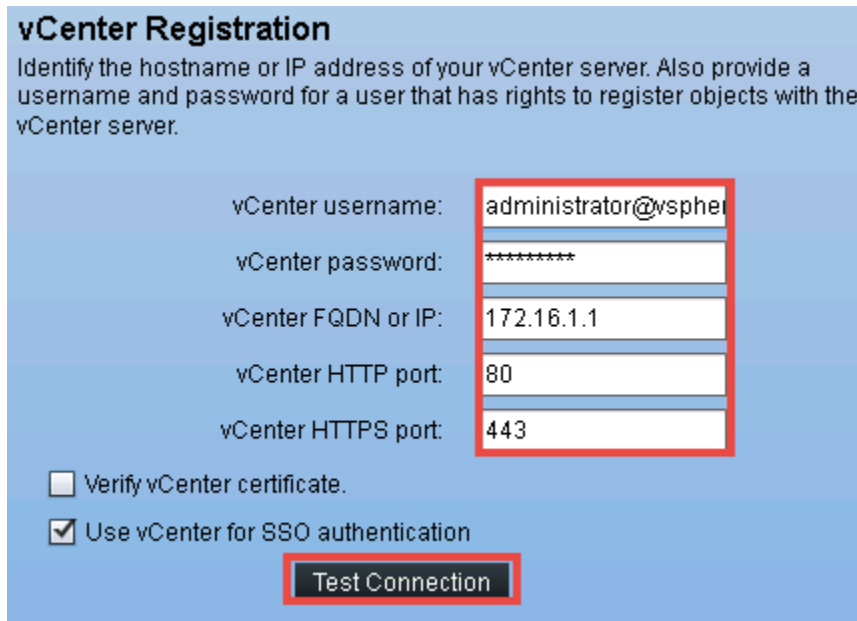
- ✓ All four character classes, at least 6 characters long
- Three character classes, at least 7 characters long
- One or two character classes, at least 8 characters long
- (NOTE: Initial character in uppercase and Final character as numeral are not included in the character class count.)

New password:

Verify password:  ✓

Previous **Next**

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



**vCenter Registration**

Identify the hostname or IP address of your vCenter server. Also provide a username and password for a user that has rights to register objects with the vCenter server.

vCenter username:	administrator@vsphere
vCenter password:	*****
vCenter FQDN or IP:	172.16.1.1
vCenter HTTP port:	80
vCenter HTTPS port:	443

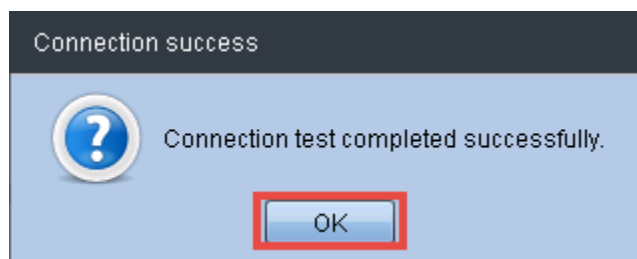
☐ Verify vCenter certificate.

☒ Use vCenter for SSO authentication

**Test Connection**

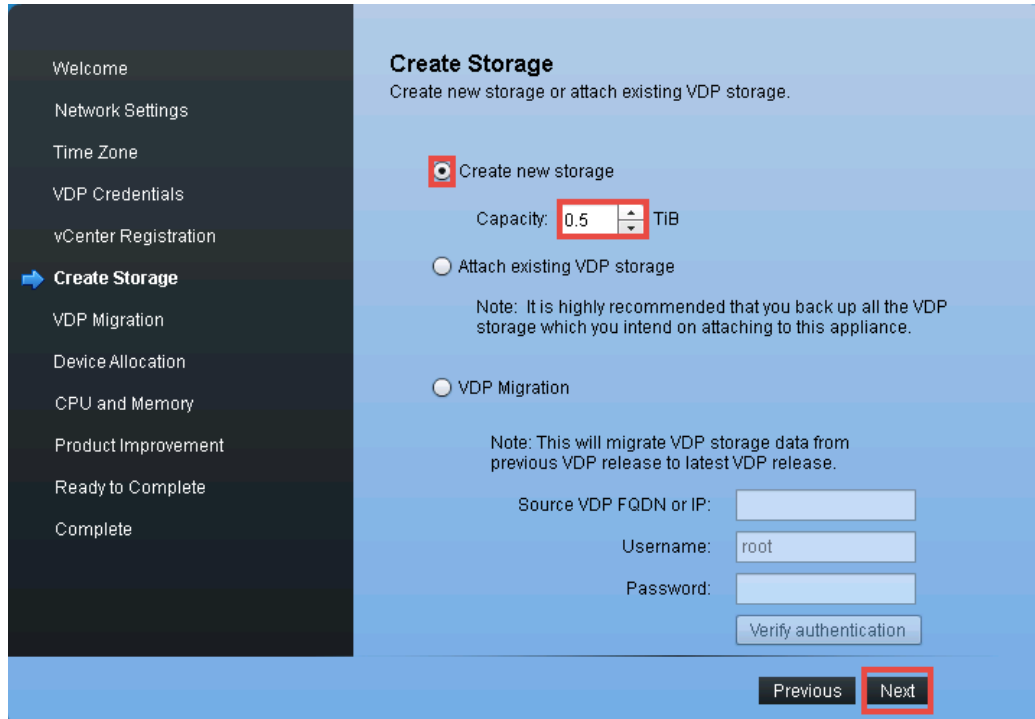
The default port for *HTTP* is *80*. The default port for *HTTPS* is *443*. If different ports are used, the ports must be opened in */etc/firewall.base* followed by a restart of the *avfirewall* service.

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

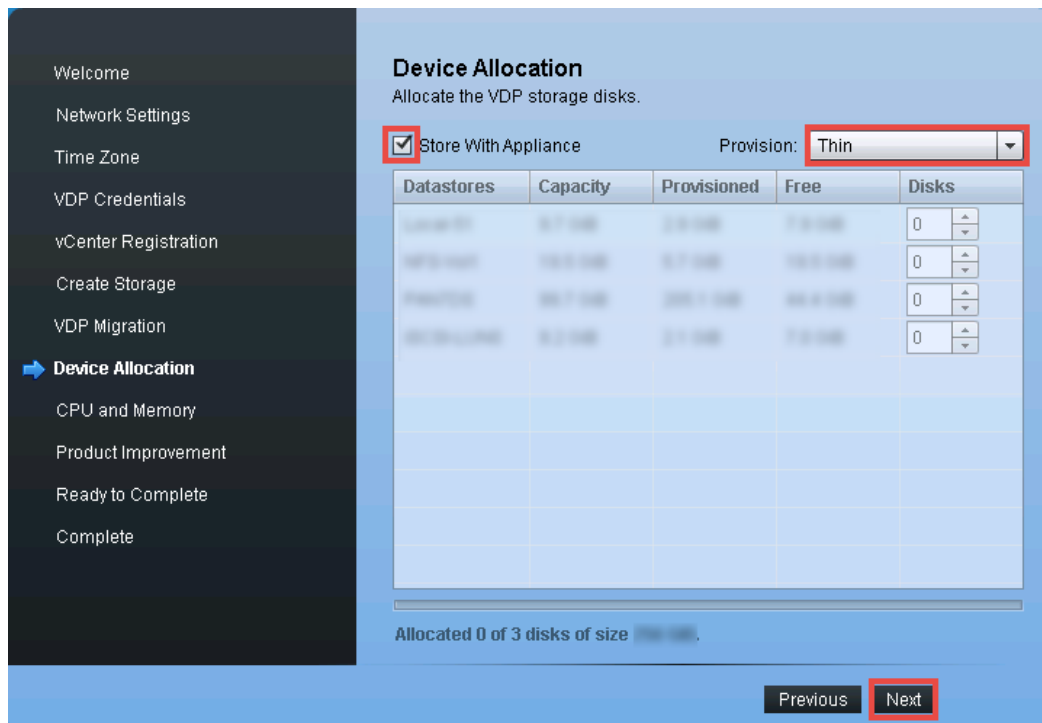


10. On the *Create Storage* page, select the bubble for **Create new storage** and create a capacity for **0.5TB**. Click **Next**.

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

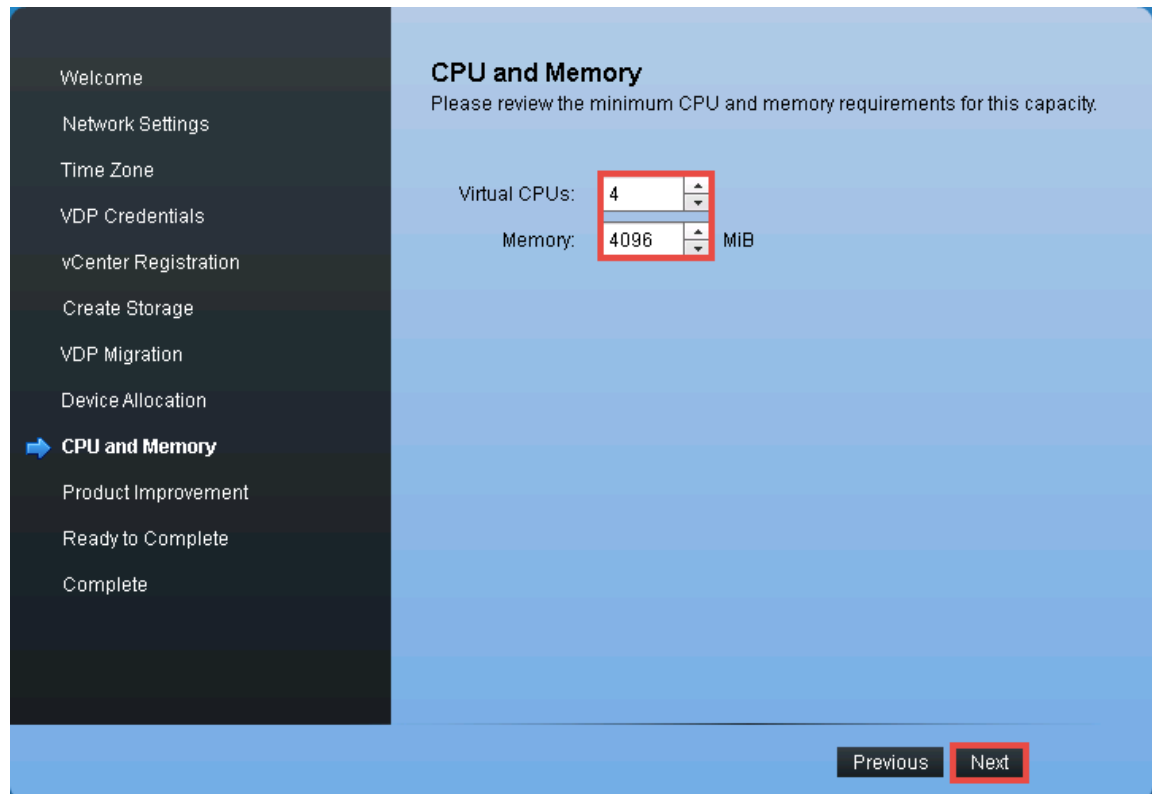


11. On the *Device Allocation* page, select **Thin** for the *Provision* type and check the box for **Store With Appliance**. Click **Next**.



Datastores	Capacity	Provisioned	Free	Disks
Local Disk	512 GB	512 GB	512 GB	0
SSD Storage	512 GB	512 GB	512 GB	0
Flash Storage	512 GB	512 GB	512 GB	0
SSD Storage	512 GB	512 GB	512 GB	0

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



Welcome

Network Settings

Time Zone

VDP Credentials

vCenter Registration

Create Storage

VDP Migration

Device Allocation

➔ **CPU and Memory**

Product Improvement

Ready to Complete

Complete

### CPU and Memory

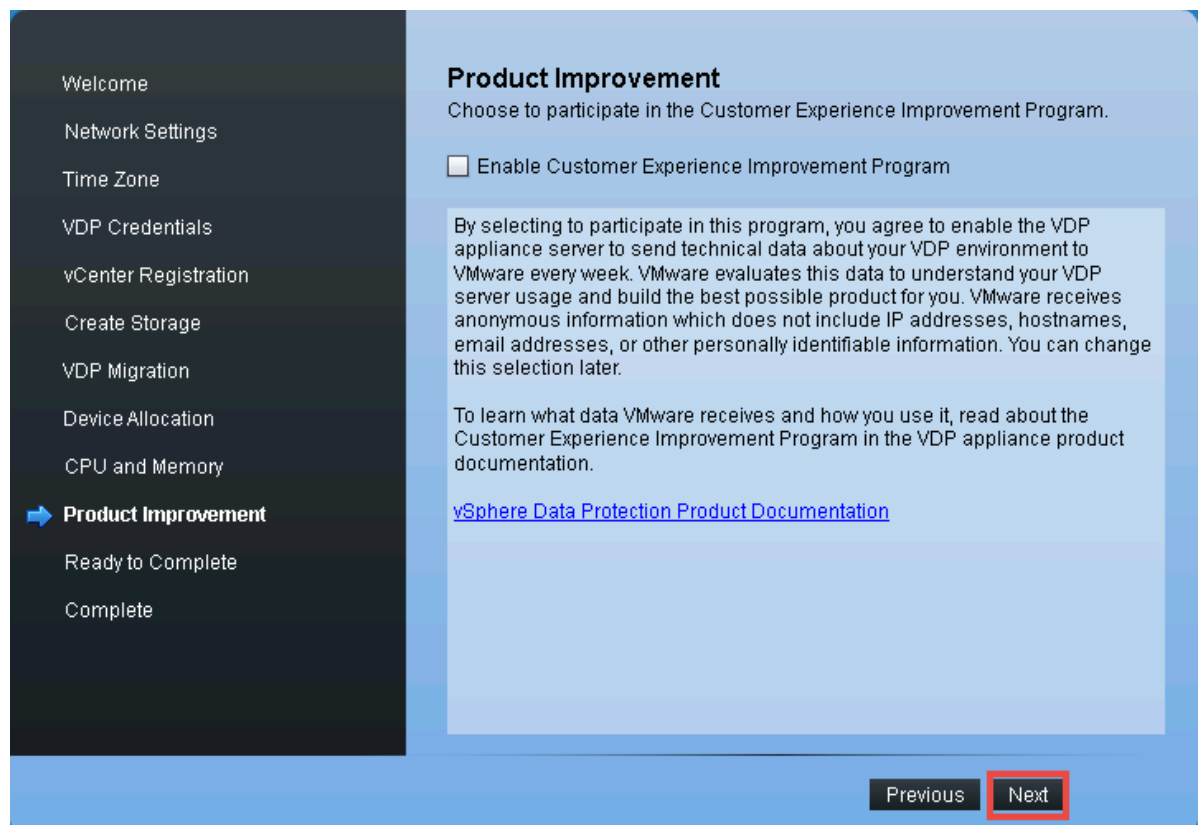
Please review the minimum CPU and memory requirements for this capacity.

Virtual CPUs: 4

Memory: 4096 MIB

Previous Next

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



Welcome

Network Settings

Time Zone

VDP Credentials

vCenter Registration

Create Storage

VDP Migration

Device Allocation

CPU and Memory

➔ **Product Improvement**

Ready to Complete

Complete

### Product Improvement

Choose to participate in the Customer Experience Improvement Program.

☐ Enable Customer Experience Improvement Program

By selecting to participate in this program, you agree to enable the VDP appliance server to send technical data about your VDP environment to VMware every week. VMware evaluates this data to understand your VDP server usage and build the best possible product for you. VMware receives anonymous information which does not include IP addresses, hostnames, email addresses, or other personally identifiable information. You can change this selection later.

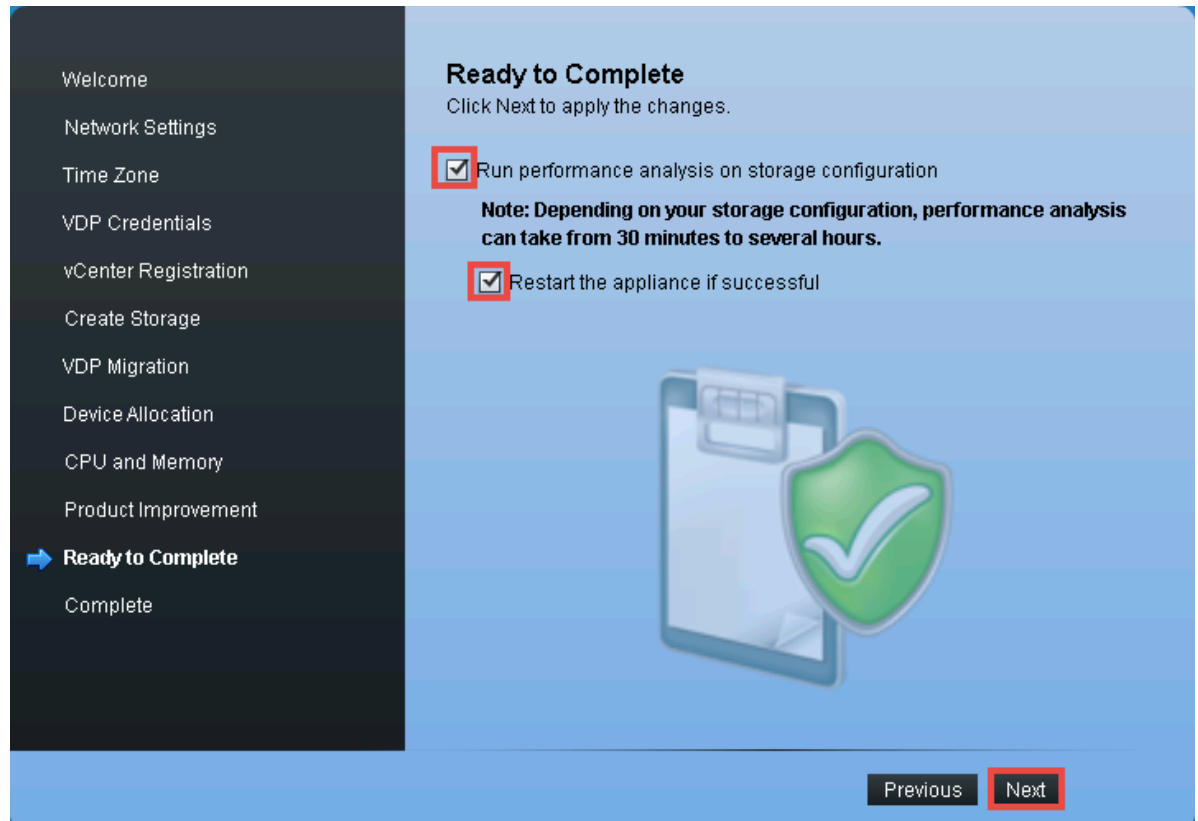
To learn what data VMware receives and how you use it, read about the Customer Experience Improvement Program in the VDP appliance product documentation.

[vSphere Data Protection Product Documentation](#)

Previous 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.

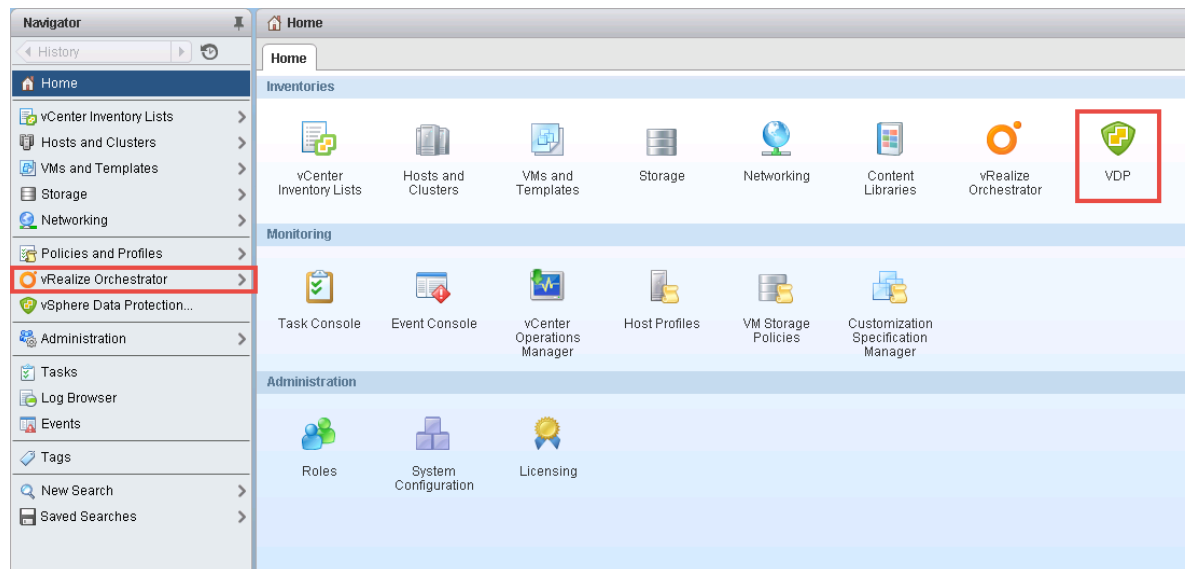
For additional guidance on minimum storage performance benchmarks, reference to page **71**, from the [VMware vSphere Data Protection Administration Guide](#).

## 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.

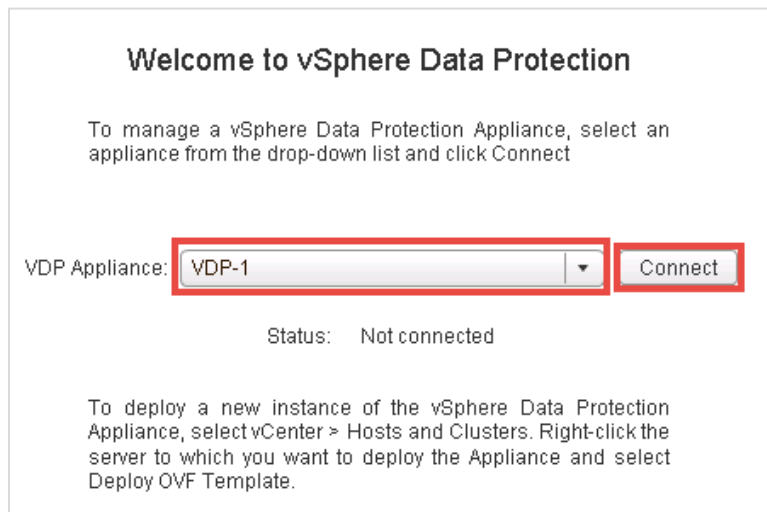
For additional guidance on editing the backup window, reference to pages **54-55**, from the [VMware vSphere Data Protection Administration Guide](#).

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.

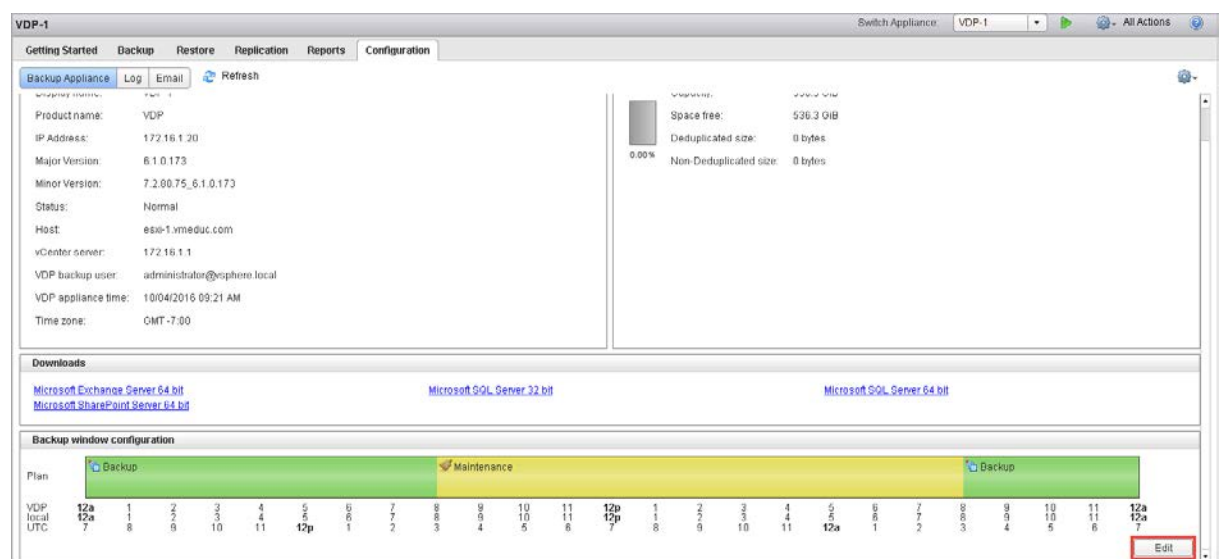
2. On the *Welcome to vSphere Data Protection* screen, select the newly deployed VDP appliance from the drop-down menu and click **Connect**.



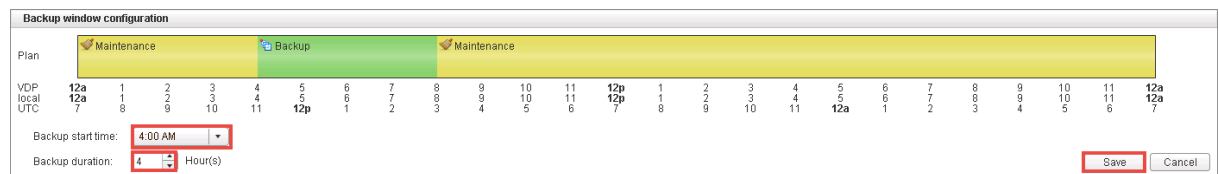
- Once the VDP appliance control interface appears, click on the **Configuration** tab.



- 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.



- 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**.



Backup window configuration

Plan: Maintenance Backup Maintenance

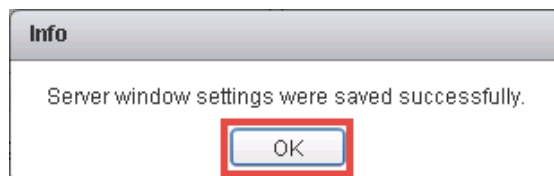
VDP local UTC: 12a 1 2 3 4 5 6 7 8 9 10 11 12p 1 2 3 4 5 6 7 8 9 10 11 12a

Backup start time: 4:00 AM

Backup duration: 4 Hour(s)

Save Cancel

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

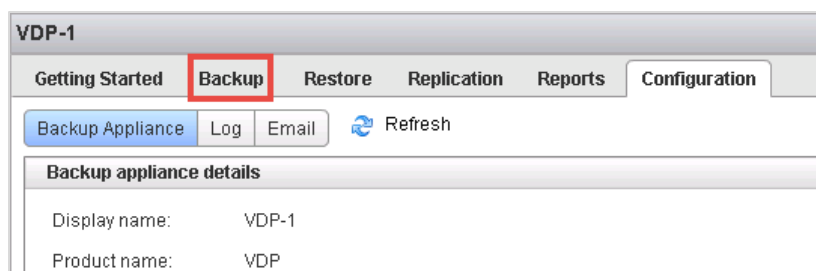


## 2.5 Creating a Backup Job

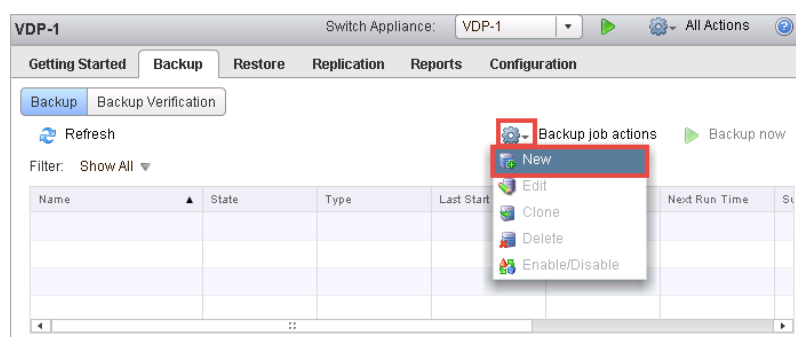
This section will cover on how to create a full image backup job for the *NETLAB+ VE* system.

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

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

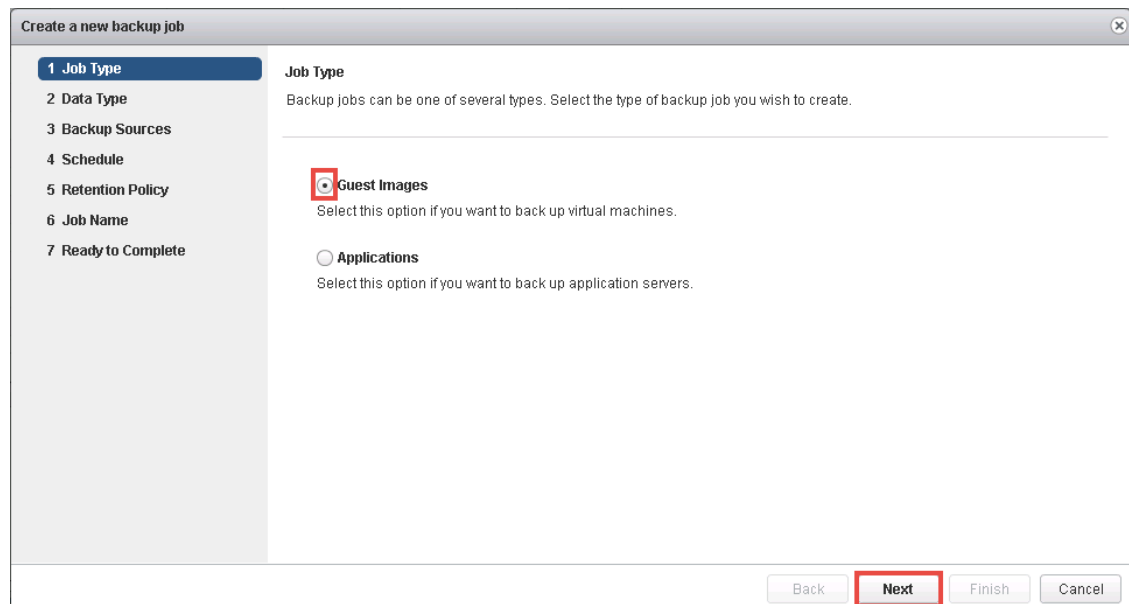


- While viewing the *Backup* tab, click on **Backup job actions** and select **New**.



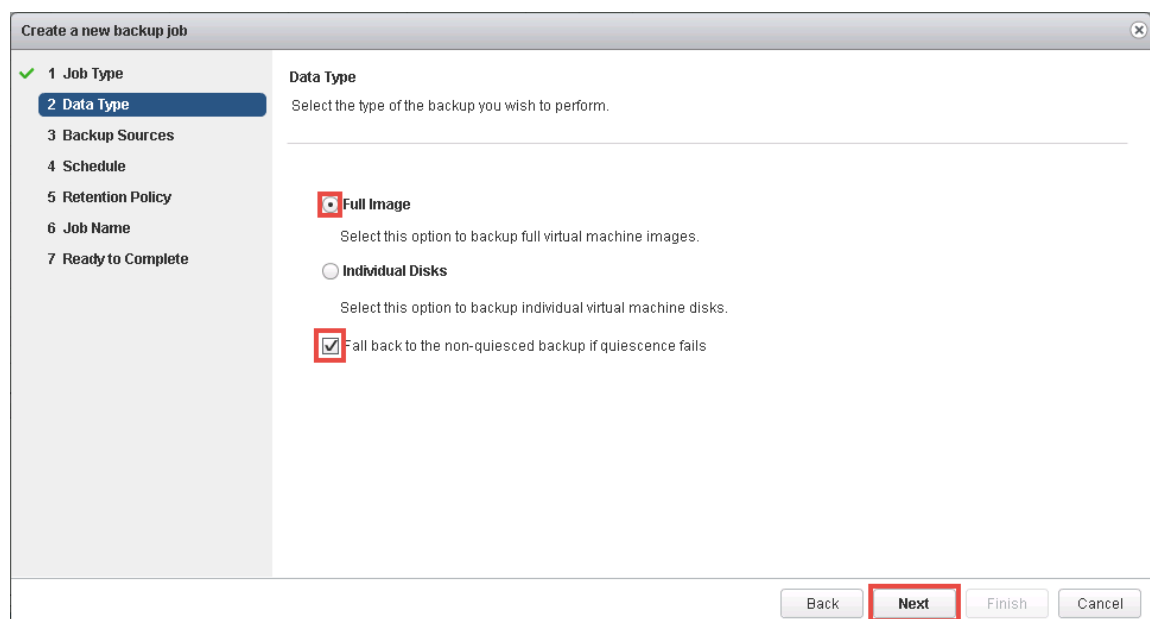


3. Notice that the *Create a new backup job* wizard appears. On the *Job Type* page, select **Guest Images** and click **Next**.



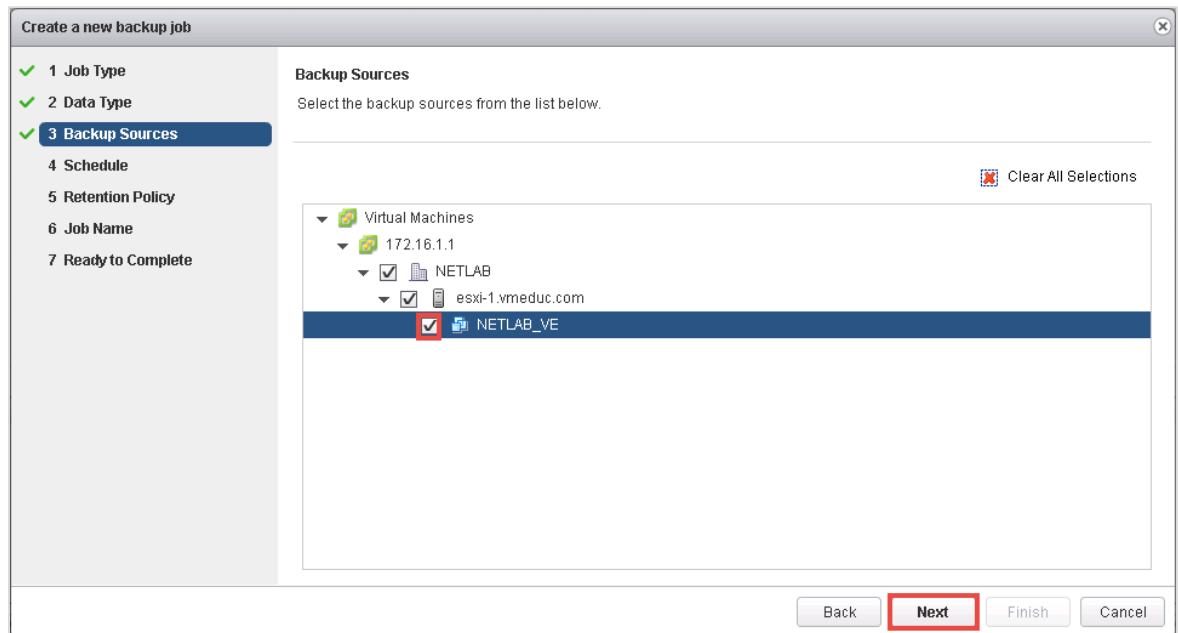
The screenshot shows the 'Create a new backup job' wizard window. On the left, a sidebar lists the steps: 1 Job Type (selected), 2 Data Type, 3 Backup Sources, 4 Schedule, 5 Retention Policy, 6 Job Name, and 7 Ready to Complete. The main area is titled 'Job Type' and contains the text: 'Backup jobs can be one of several types. Select the type of backup job you wish to create.' There are two radio button options: 'Guest Images' (selected and highlighted with a red box) and 'Applications'. Below 'Guest Images' is the text: 'Select this option if you want to back up virtual machines.' Below 'Applications' is the text: 'Select this option if you want to back up application servers.' At the bottom right, there are four buttons: 'Back', 'Next' (highlighted with a red box), 'Finish', and 'Cancel'.

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



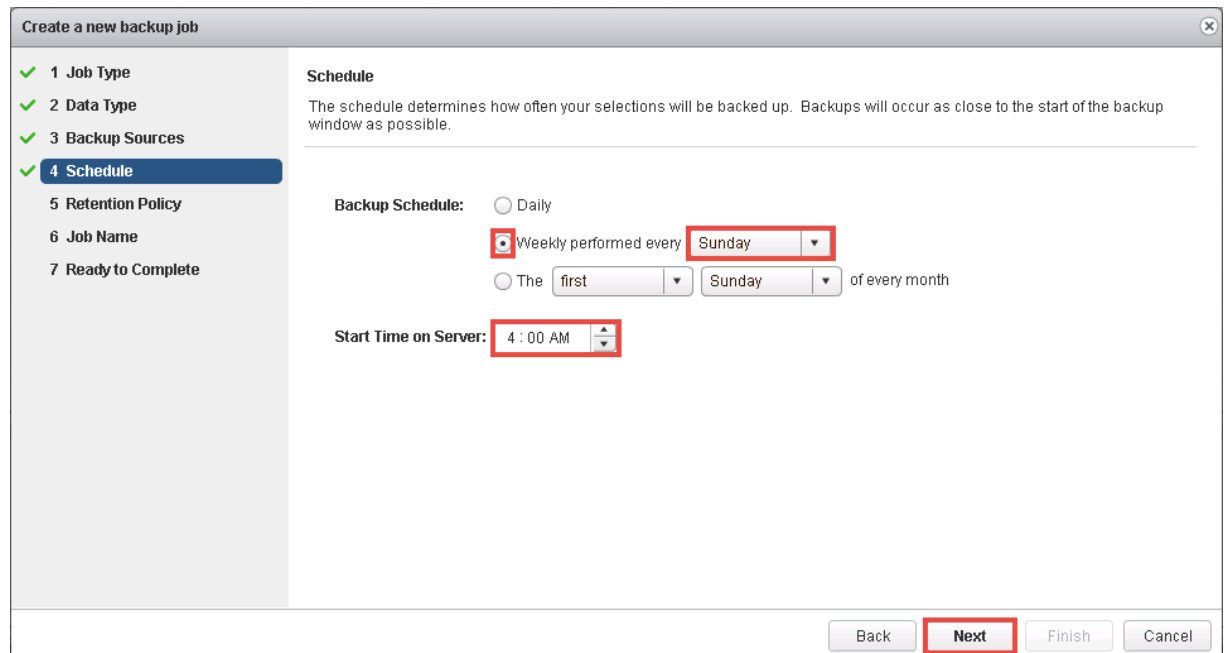
The screenshot shows the 'Create a new backup job' wizard window, now on the 'Data Type' page. The sidebar shows '1 Job Type' with a green checkmark and '2 Data Type' selected. The main area is titled 'Data Type' and contains the text: 'Select the type of the backup you wish to perform.' There are three radio button options: 'Full Image' (selected and highlighted with a red box), 'Individual Disks', and 'Fall back to the non-quieted backup if quiescence fails' (checked with a checkbox and highlighted with a red box). Below 'Full Image' is the text: 'Select this option to backup full virtual machine images.' Below 'Individual Disks' is the text: 'Select this option to backup individual virtual machine disks.' Below the checked checkbox is the text: 'Fall back to the non-quieted backup if quiescence fails'. At the bottom right, there are four buttons: 'Back', 'Next' (highlighted with a red box), 'Finish', and 'Cancel'.

- 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**.



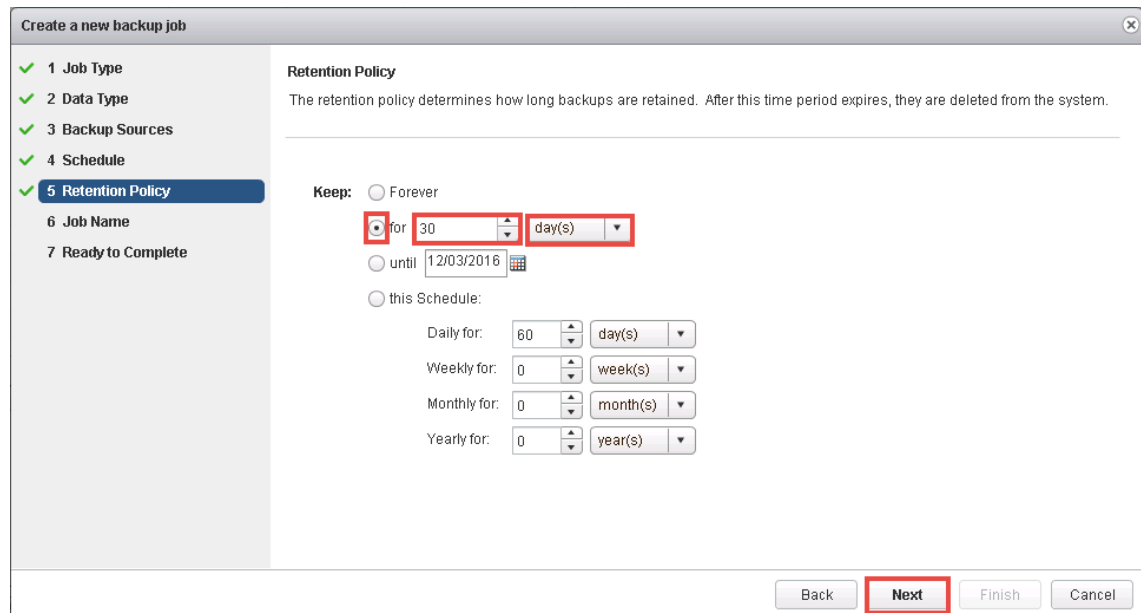
The screenshot shows the 'Create a new backup job' dialog box, specifically the 'Backup Sources' tab. On the left, a sidebar lists seven steps: 1 Job Type, 2 Data Type, 3 Backup Sources (highlighted), 4 Schedule, 5 Retention Policy, 6 Job Name, and 7 Ready to Complete. The main area is titled 'Backup Sources' and contains the instruction 'Select the backup sources from the list below.' Below this is a tree view showing a hierarchy: 'Virtual Machines' expanded to '172.16.1.1', which is expanded to 'NETLAB' and 'esxi-1.vmeduc.com'. Under 'NETLAB', the item 'NETLAB\_VE' is selected with a checkmark. A 'Clear All Selections' button is in the top right. At the bottom, there are four buttons: 'Back', 'Next' (highlighted with a red box), 'Finish', and 'Cancel'.

- 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.



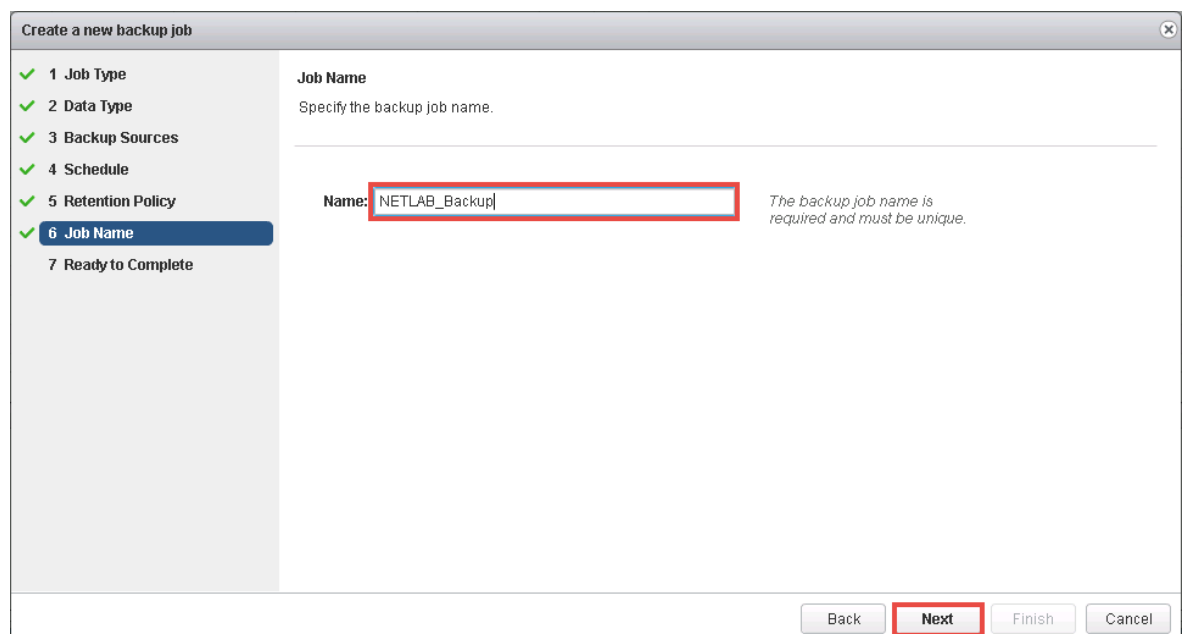
The screenshot shows the 'Create a new backup job' dialog box, specifically the 'Schedule' tab. The sidebar on the left is the same as the previous screenshot, but '4 Schedule' is now highlighted. The main area is titled 'Schedule' and contains the instruction 'The schedule determines how often your selections will be backed up. Backups will occur as close to the start of the backup window as possible.' Below this, the 'Backup Schedule' section has two radio buttons: 'Daily' (unselected) and 'Weekly performed every' (selected). The 'Weekly performed every' option has a dropdown menu set to 'Sunday'. Below this, there is another set of dropdowns: 'The first' followed by 'Sunday' and 'of every month'. The 'Start Time on Server' is set to '4:00 AM' in a time picker. At the bottom, there are four buttons: 'Back', 'Next' (highlighted with a red box), 'Finish', and 'Cancel'.

- 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.



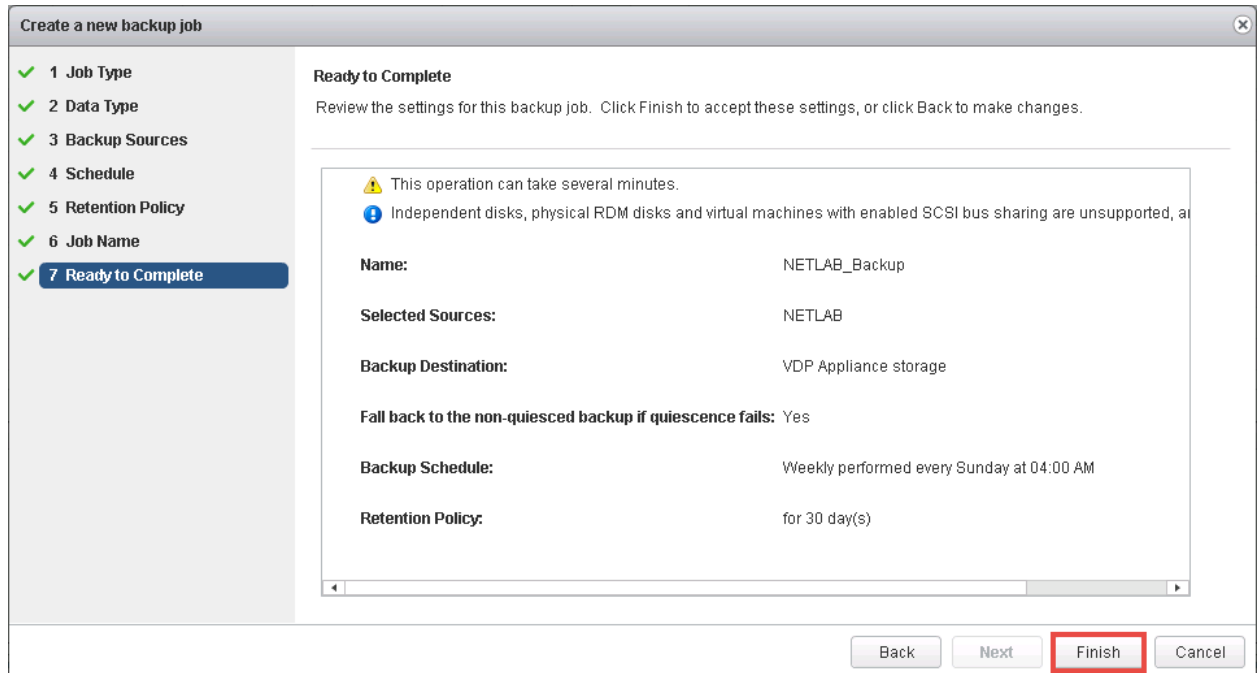
The screenshot shows the 'Create a new backup job' dialog box, specifically the 'Retention Policy' step. On the left, a sidebar lists steps 1 through 7, with '5 Retention Policy' selected. The main area is titled 'Retention Policy' and contains the text: 'The retention policy determines how long backups are retained. After this time period expires, they are deleted from the system.' Below this, there are three radio button options: 'Forever', 'for 30 day(s)', and 'until 12/03/2016'. The 'for 30 day(s)' option is selected and highlighted with a red box. Below these options, there are four groups of settings for 'this Schedule': 'Daily for: 60 day(s)', 'Weekly for: 0 week(s)', 'Monthly for: 0 month(s)', and 'Yearly for: 0 year(s)'. At the bottom right, there are four buttons: 'Back', 'Next' (highlighted with a red box), 'Finish', and 'Cancel'.

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



The screenshot shows the 'Create a new backup job' dialog box, specifically the 'Job Name' step. On the left, the sidebar lists steps 1 through 7, with '6 Job Name' selected. The main area is titled 'Job Name' and contains the text: 'Specify the backup job name.' Below this, there is a text input field labeled 'Name:' containing the text 'NETLAB\_Backup'. To the right of the input field, there is a note: 'The backup job name is required and must be unique.' At the bottom right, there are four buttons: 'Back', 'Next' (highlighted with a red box), 'Finish', and 'Cancel'.

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



**Create a new backup job**

Ready to Complete

Review the settings for this backup job. Click Finish to accept these settings, or click Back to make changes.

⚠ This operation can take several minutes.  
 ⓘ Independent disks, physical RDM disks and virtual machines with enabled SCSI bus sharing are unsupported, and...

**Name:** NETLAB\_Backup

**Selected Sources:** NETLAB

**Backup Destination:** VDP Appliance storage

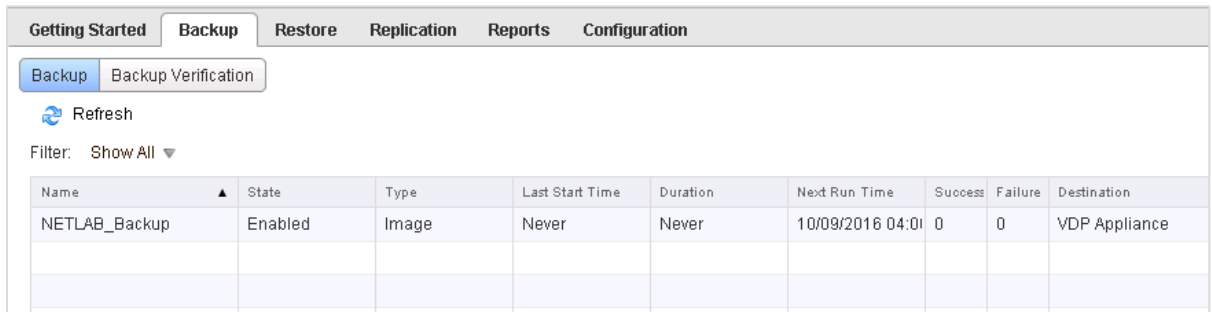
**Fall back to the non-quieted backup if quiescence fails:** Yes

**Backup Schedule:** Weekly performed every Sunday at 04:00 AM

**Retention Policy:** for 30 day(s)

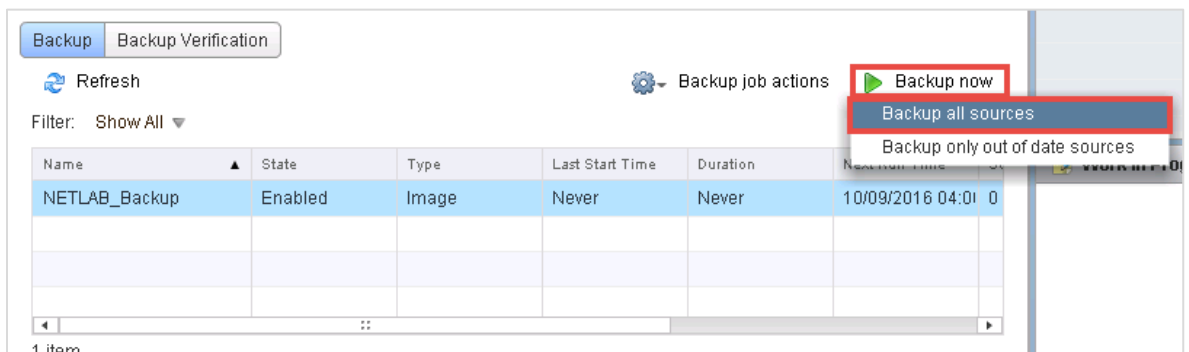
Back Next **Finish** Cancel

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



Name	State	Type	Last Start Time	Duration	Next Run Time	Success	Failure	Destination
NETLAB_Backup	Enabled	Image	Never	Never	10/09/2016 04:00	0	0	VDP Appliance

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



Backup Backup Verification

Refresh

Filter: Show All ▼

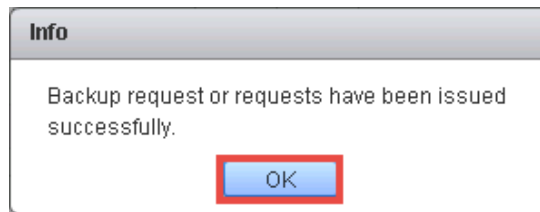
Backup job actions

- Backup now
- Backup all sources
- Backup only out of date sources

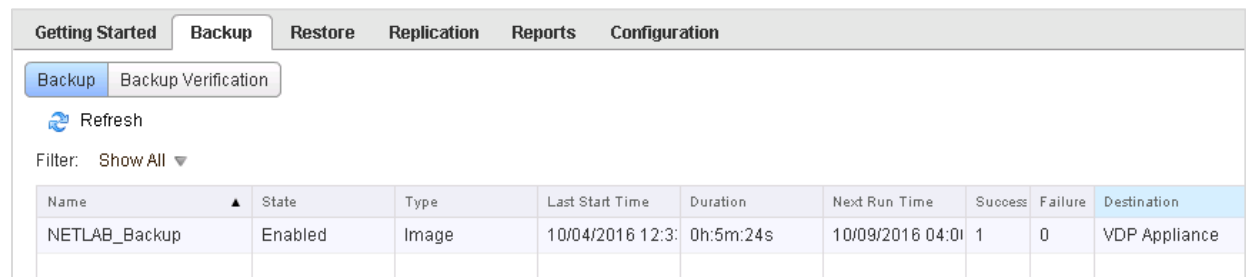
Name	State	Type	Last Start Time	Duration	Next Run Time	Success	Failure	Destination
NETLAB_Backup	Enabled	Image	Never	Never	10/09/2016 04:00	0	0	VDP Appliance

1 item

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



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



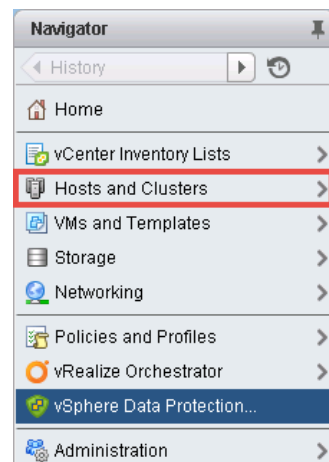
## 2.6 Restoring a Backup

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

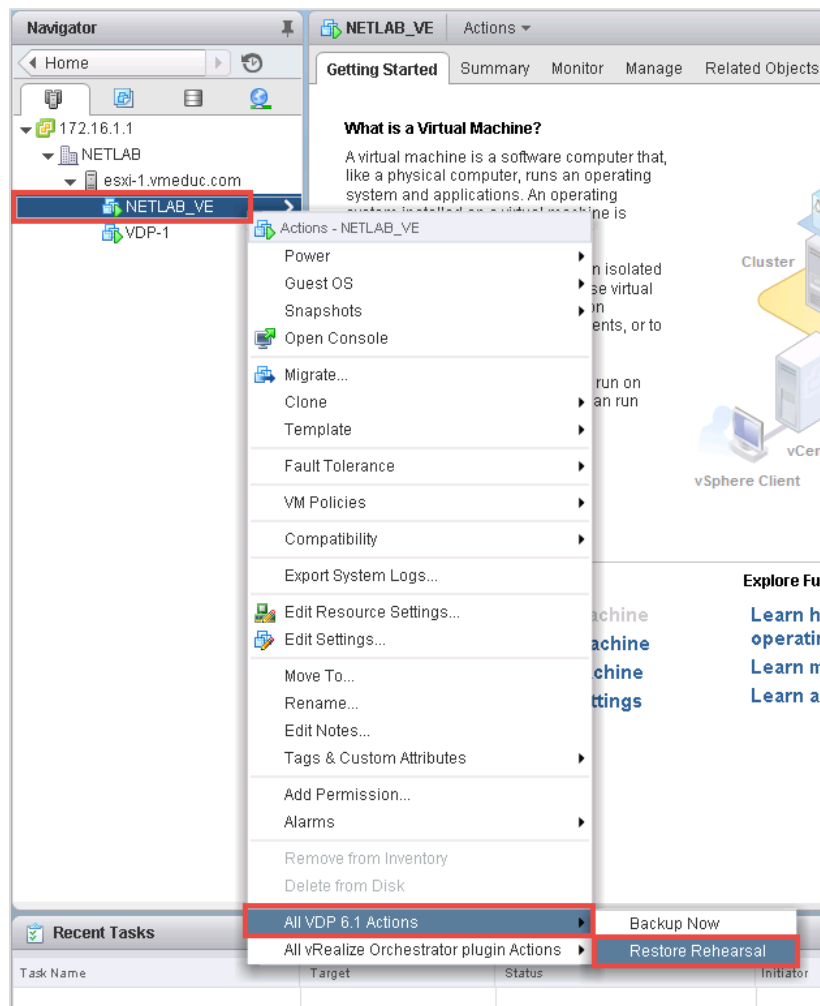
After restoring a backup of *NETLAB+ VE*, it will be necessary to reactivate your *NETLAB+ VE* system by entering your license key. After completing the steps below, see the *Manage License* section of the *NETLAB+ VE Administrator Guide* for details.

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

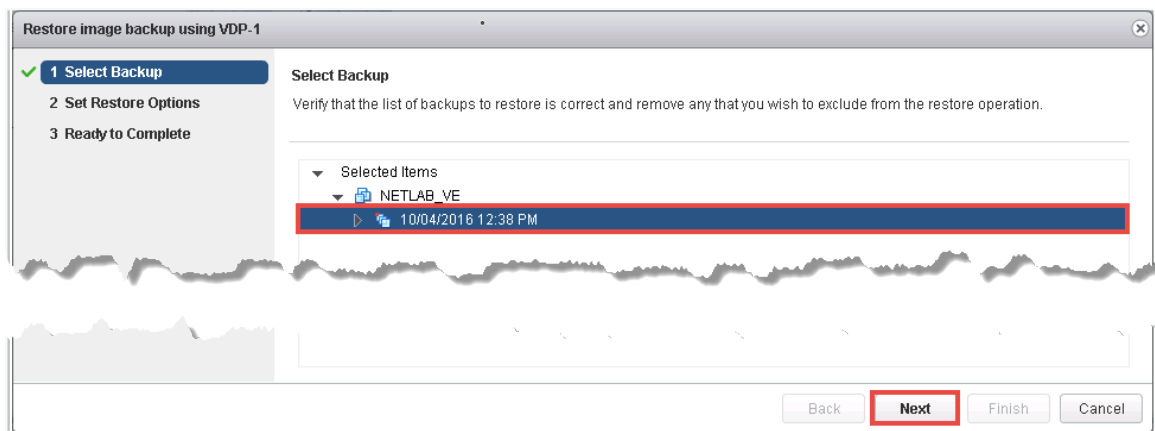
- To restore a virtual machine from a backup job, navigate to **Hosts and Clusters** from the *Navigator* pane.



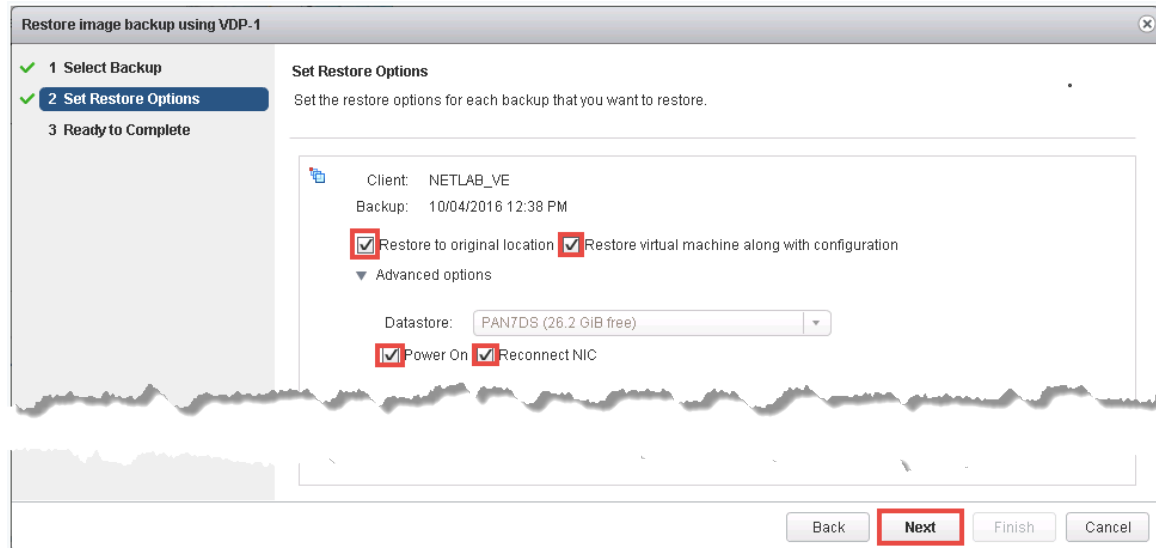
- Expand the list in the *Navigator* pane and right-click on the **NETLAB+ VE** virtual machine, selecting **All VDP Actions > Restore Rehearsal**.



- 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**.

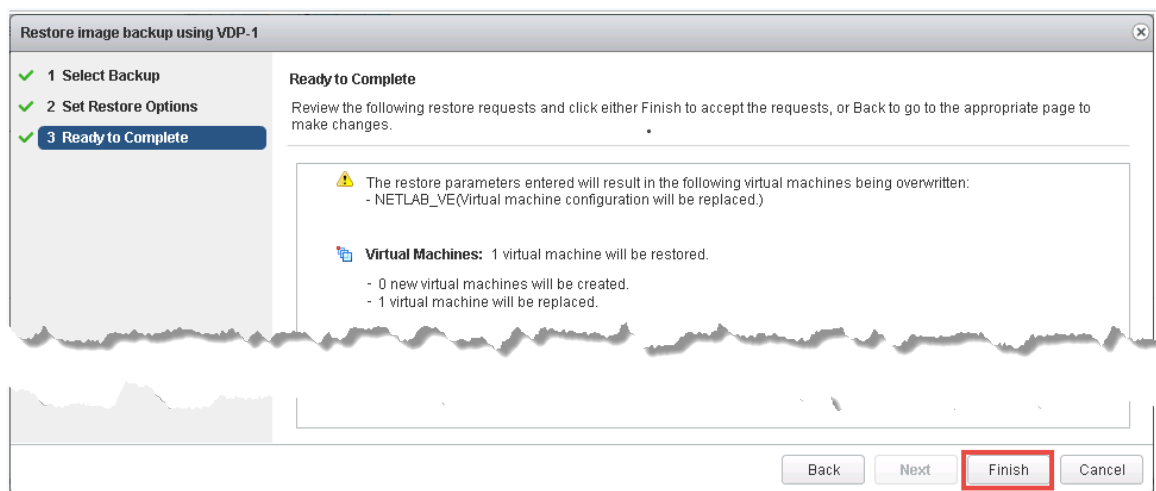


- On the *Set Restore Options* page, check the boxes for **Restore to original location** and **Restore virtual machine along with configuration**. Expand the **Advanced options**, placing a check for **Power On** and **Reconnect NIC**. Click **Next**.



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.

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



- Once the restore request initiates, notice the progress in the *Recent Tasks* pane to completion.
- 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
```