NetVault®: Backup
User's Guide

for the
VaultDR System Plugins

VaultDR Offline Plugin ver. 5.1 (VaultOS)

VaultDR Online Plugin for Windows ver. 3.0

VaultDR Online Plugin for Linux ver. 3.0

VaultDR Server ver. 2.4

VOG-101-5.1-EN-01 10/30/08

Copyrights

BakBone Software

9540 Towne Centre Drive, Suite 100 ◆ San Diego, California 92121 ◆ 866.484.2663

BakBone®

Table of Contents

Chapter 5: The VaultDR Online Plugin for Linux 83

Appendix A: Troubleshooting/Support 117

SECTION 1:

Introduction & Overview

Chapter 1:
INTRODUCTION

1.0.0 VaultDR System of Plugins – An Overview

The **VaultDR System** is a Disaster Recovery (DR) solution capable of recovering an entire disk — including the operating system, applications, system settings, partition information, and data. NetVault: Backup's **VaultDR System** is comprised of three components that provide the ability to create a DR image of a Client machine on Windows and Linux-based platforms.

The **VaultDR System** is comprised of two key components, or plugins, each of which provides its own form of disaster recovery backup, and a third component that serves as a basic operating system that is used to prepare a target DR Client for backup/restore. The sections that follow serve as a brief description of each of these components:

1.0.1 VaultDR Offline Plugin

The **VaultDR Offline Plugin** implements a **block-by-block** backup and restore technique to fully recover a system. This **block-by-block** operation takes the target system offline and makes it unavailable. This is done to either:

- **Backup** – An ***Offline Backup*** fully backs up all aspects of a target system (O/S, applications, system settings, etc.). This is ideal for new systems that have been configured for use.
- **Restore** – An ***Offline Restore*** recovers a machine that has no functional operating system to a previously configured state.

1.0.2 VaultDR Online Plugin

The **VaultDR Online Plugin** makes it possible to backup a full system ***while it remains online and active***. When a recovery is required, the **VaultDR Offline Plugin** operating system (VaultOS) is used to boot the target DR client to allow for a complete recovery of data (i.e., an ***Offline Restore*** is required).

1.0.3 VaultDR Server

The **VaultDR Server** resides on the NetVault: Backup Server and enables backup and recovery of a target client's data via the **VaultDR Offline Plugin** or the **VaultDR Online Plugin**.

1.0.4 VaultOS Operating System

The **VaultDR Offline Plugin** includes a component known as **VaultOS**. The **VaultOS** operating system is a minimal operating system that is used to boot a target disaster recovery client system to prepare it for either backup or restore (depending on the **VaultDR System Plugin** in use). This minimal operating system will start up the target client, load all applicable device drivers, and leave its hard drive in a state suitable for either backup or restore.

Important: Each version of the **VaultDR Offline Plugin** and **VaultDR Online Plugin** offers its own, specific form of the **VaultOS** operating system (e.g., the **VaultDR Online Plugin for Linux** operating systems uses its own form of **VaultOS**). Complete details on the setup and use of this component are covered in the relevant chapter of this guide.

Important: VaultDR Server version 2.3 and later requires **VaultOS** version 5.x to perform backups.

1.1.0 About this Guide

The set up and use of the **VaultDR Offline Plugin** and the **VaultDR Online Plugin** varies based on the operating system running on the target Disaster Recovery Client. This guide is broken down into individual sections for each plugin; each section is broken down into individual chapters that cover the use of the given plugin in a specific operating system environment.

- **Section 1: Introduction and Overview –** This section contains overview information for the VaultDR System Plugins and details regarding their use.
- **Section 2: The VaultDR Offline Plugin** – This section discusses the **VaultDR Offline Plugin**, also known as **VaultOS**. It includes installation, configuration, backup and restore instructions for the **VaultDR Server** and **VaultOS**.
- **Section 3: The VaultDR Online Plugin** – This section is broken down into the following individual chapters:
  - *The VaultDR Online Plugin for Windows* – This chapter covers the version of the VaultDR Online Plugin designed for use in Microsoft Windows operating system environments.
  - *The VaultDR Online Plugin for Linux* – This chapter covers the version of the VaultDR Online Plugin designed for use in Linux operating system environments.

In addition, an appendix is included that offers basic troubleshooting information as well as contact information for BakBone Technical Support (*Troubleshooting/Support* on page 117).

1.1.1 Target Audience

System administration experience is recommended when using the **VaultDR Offline Plugin** or **VaultDR Online Plugin**. Although it is not necessary to have this level of experience to perform routine backups with either plugin, the initial configuration of each plugin, the configuration of a target Client and the restore procedure will require administrator knowledge.

1.1.2 Recommended Additional Reading

It is recommended that the following documentation be readily available for reference when setting up using any of the **VaultDR System Plugins**:

- ***The NetVault: Backup Administrator's Guide –*** This guide describes features available in NetVault: Backup that can be used in conjunction with this family of plugins (i.e., functionality that is not unique to the **VaultDR System Plugins**). This document can be downloaded from the **Product Documentation** page of BakBone Software's web site:

  http://www.bakbone.com/documentation

1.2.0 Open Source Code Availability

The **VaultOS** component software used with the VaultDR System Plugins was created using open source, Linux kernel source code. To obtain a copy of this open source code, make a written request to:

BakBone Software, Inc.

Attn: Product Management

9540 Towne Centre Drive, Suite 100

San Diego, CA 92121

Chapter 2: VaultDR System Deployment Overview

2.0.0 VaultDR Deployment Scenarios

This chapter details deployment scenarios for the following VaultDR products:

- VaultDR Offline Plugin for Intel x86 Clients
- VaultDR Online Plugin for Windows Clients
- VaultDR Online Plugin for Linux Clients

2.1.0 VaultDR Offline Plugin for Intel x86 Clients with Windows NetVault: Backup Server

This scenario is deployed when the user wants to perform offline or cold backups of Intel x86 Clients and has a Windows NetVault: Backup Server deployed.

The VaultDR Server for Windows component is installed on the Windows NetVault: Backup Server and the VaultDR Offline Plugin for Intel x86 Clients, VaultOS, is installed on each Intel x86 Client you wish to protect with offline or cold backups.

In this scenario, VaultOS is used to perform the backup and recovery of the Intel x86 Clients.

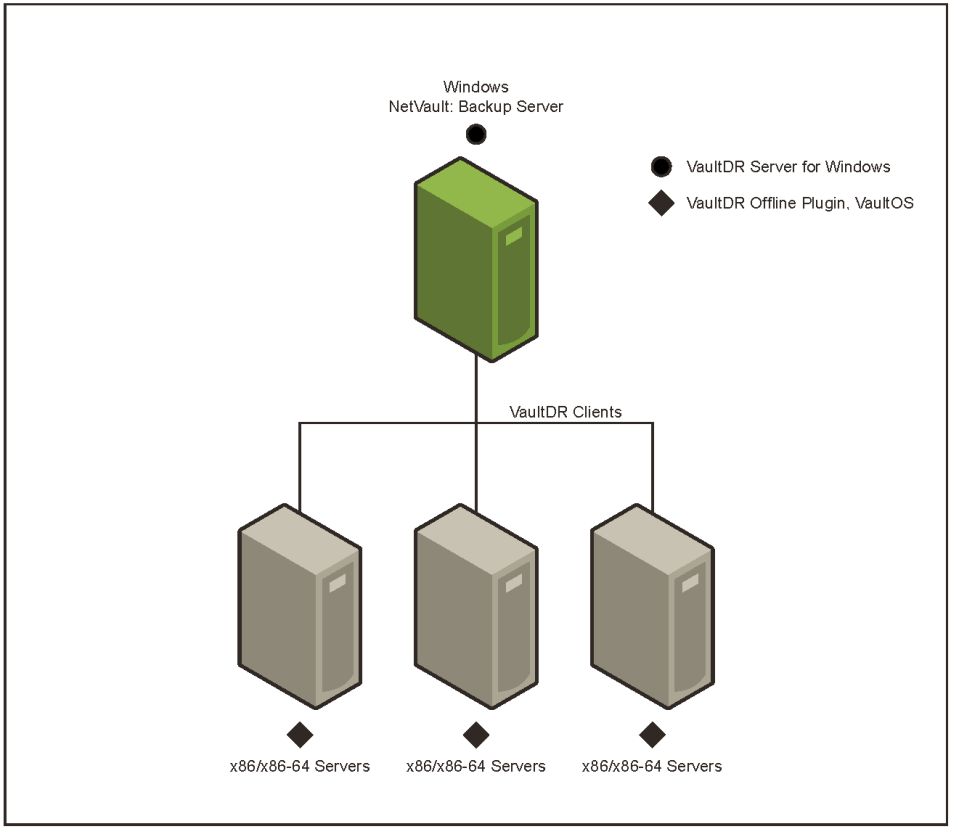


Figure 2-1: *VaultDR Offline Plugin for Intel x86 Clients with Windows Server*

Refer to *The VaultDR Offline Plugin for Intel x86 Clients* on page 25 for more information.

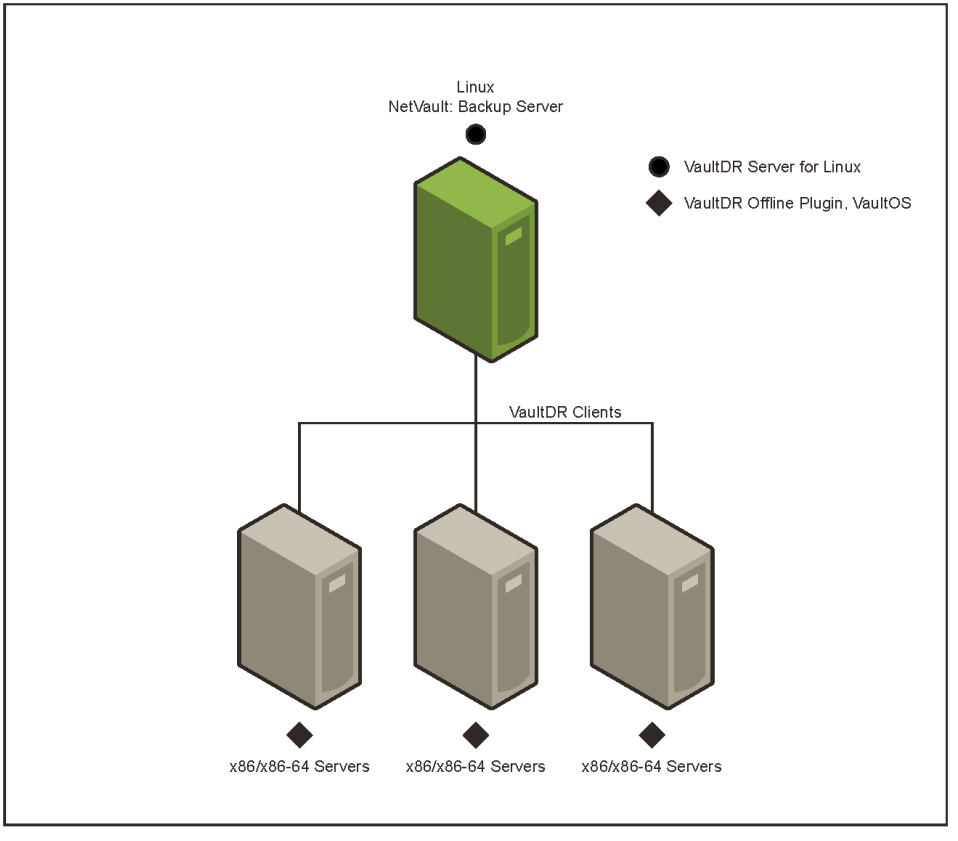
2.2.0 VaultDR Offline Plugin for Intel x86 Clients with Linux NetVault: Backup Server

This scenario is deployed when the user wants to perform offline or cold backups of Intel x86 Clients and has a Linux NetVault: Backup Server deployed.

The VaultDR Server for Linux component is installed on the Linux NetVault: Backup Server and the VaultDR Offline Plugin for Intel x86 Clients, VaultOS, is installed on each Intel x86 Client you wish to protect with offline or cold backups.

In this scenario, VaultOS is used to perform the backup and recovery of the Intel x86 Clients.

Figure 2-2: *VaultDR Offline Plugin for Intel x86 Clients with Linux Server*



Refer to *The VaultDR Offline Plugin for Intel x86 Clients* on page 25 for more information.

2.3.0 VaultDR Online for Windows Plugin with Windows NetVault: Backup Server

This scenario is deployed when the user wants to perform online or hot backups of Windows Clients and has a Windows NetVault: Backup Server deployed.

The VaultDR Server for Windows component is installed on the Windows NetVault: Backup Server and the VaultDR Online Plugin for Windows is installed on each Windows Client you wish to protect with online or hot backups.

In this scenario, VaultOS is used to perform the recovery of the Windows Clients.

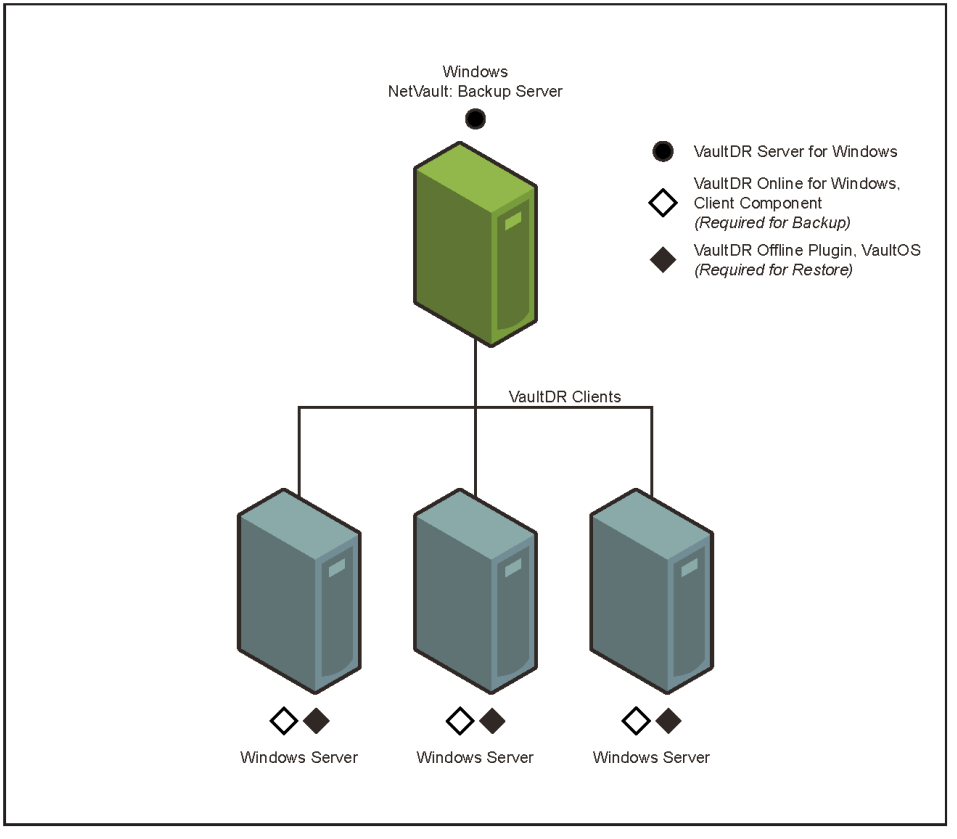


Figure 2-3: *VaultDR Online Plugin for Windows Clients with Windows Server*

Refer to *The VaultDR Online Plugin for Windows* on page 55 for more information

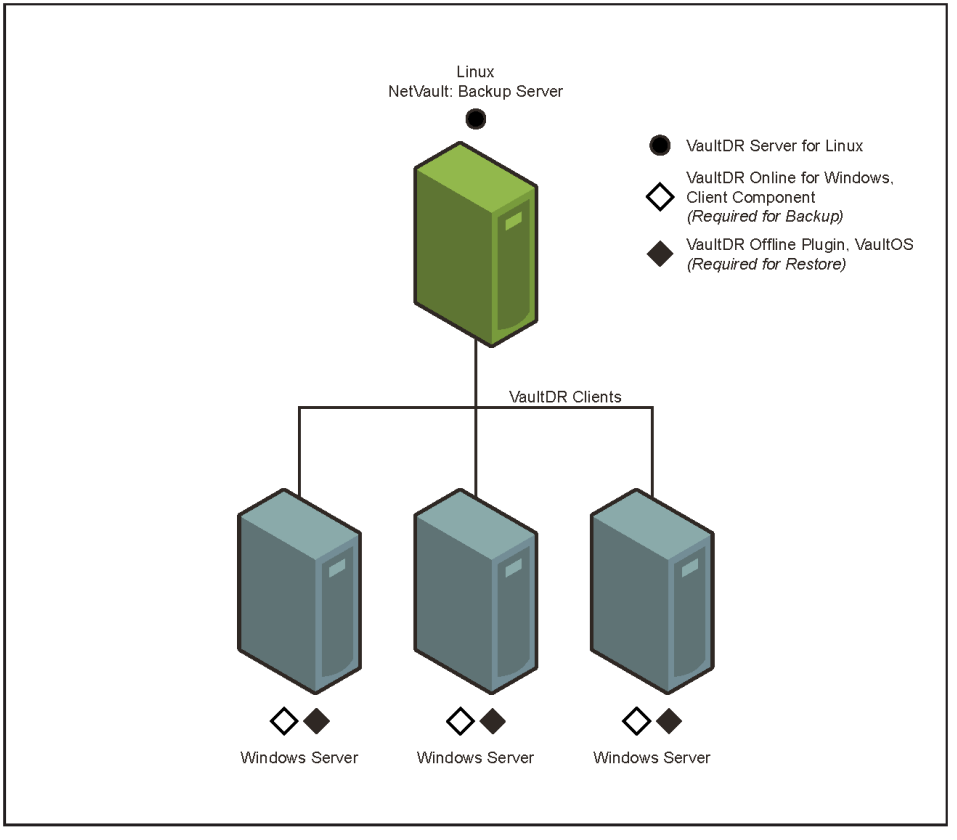
2.4.0 VaultDR Online for Windows Plugin with Linux NetVault: Backup Server

This scenario is deployed when the user wants to perform online or hot backups of Windows Clients and has a Linux NetVault: Backup Server deployed.

The VaultDR Server for Linux component is installed on the Linux NetVault: Backup Server and the VaultDR Online Plugin for Windows is installed on each Windows Client you wish to protect with online or hot backups.

In this scenario, VaultOS is used to perform the recovery of the Windows Clients.

Figure 2-4: *VaultDR Online Plugin for Windows Clients with Linux Server*



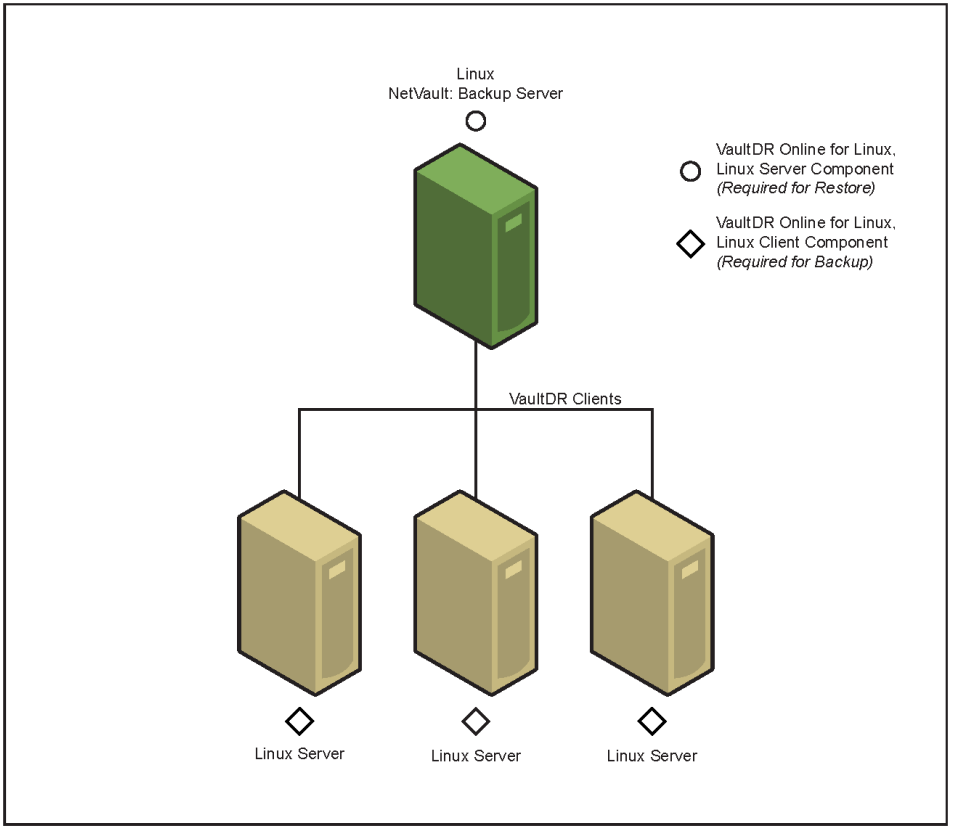
Refer to *The VaultDR Online Plugin for Windows* on page 55 for more information.

2.5.0 VaultDR Online for Linux Plugin with Linux NetVault: Backup Server

This scenario is deployed when the user wants to perform online or hot backups of Linux Clients and has a Linux NetVault: Backup Server deployed.

The VaultDR Online for Linux, Linux Server Component is installed on the Linux NetVault: Backup Server and the VaultDR Online Plugin for Linux, Linux Client Component is installed on each Linux Client you wish to protect with online or hot backups.

Figure 2-5: *VaultDR Online Plugin for Linux Clients with Linux Server*



Refer to *The VaultDR Online Plugin for Linux* on page 83 for more information.

2.6.0 VaultDR Online for Linux Plugin with Windows NetVault: Backup Server

This scenario is deployed when the user wants to perform online or hot backups of Linux Clients and has a Windows NetVault: Backup Server deployed.

The VaultDR Online for Linux, Windows Server Component is installed on the Windows NetVault: Backup Server and the VaultDR Online Plugin for Linux, Linux Client Component is installed on each Linux Client you wish to protect with online or hot backups.

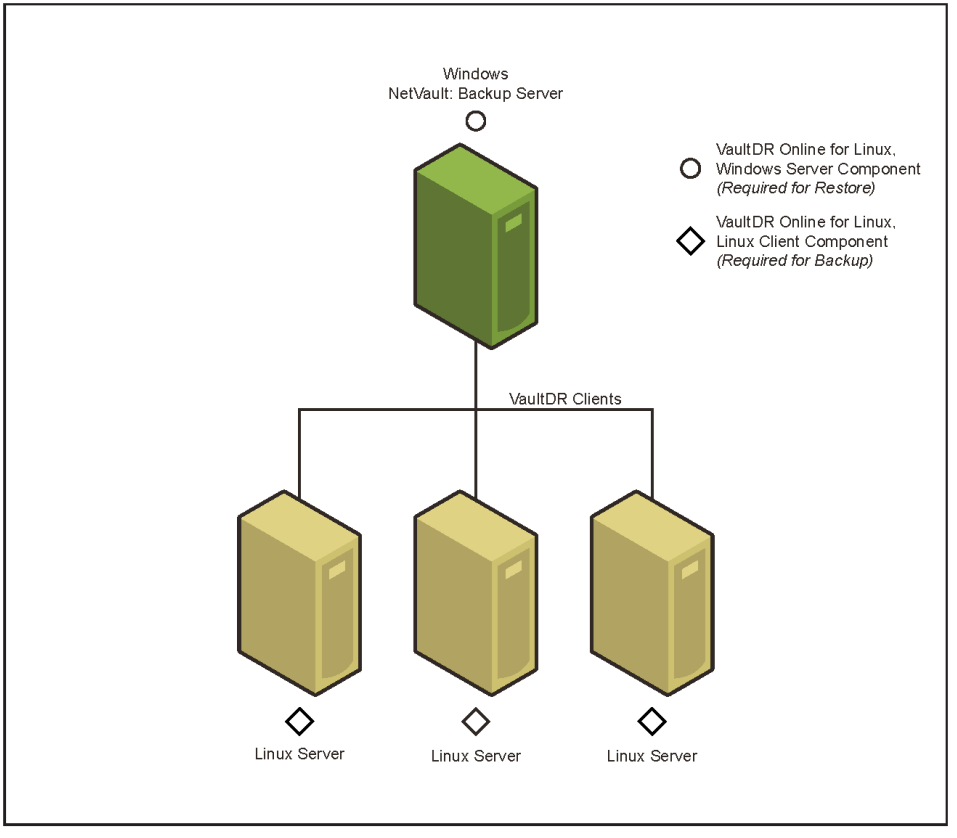


Figure 2-6: *VaultDR Online Plugin for Linux Clients with Windows Server*

Refer to *The VaultDR Online Plugin for Linux* on page 83 for more information.

2.7.0 VaultDR Online for Windows Plugin and VaultDR Online for Linux Plugin with Linux NetVault: Backup Server

This scenario is deployed when the user wants to perform online or hot backups of both Linux and Windows Clients and has a Windows NetVault: Backup Server deployed.

The VaultDR Online for Linux, Windows Server Component is installed on the Windows NetVault: Backup Server and the VaultDR Online Plugin for Linux, Linux Client Component is installed on each Linux Client you wish to protect with online or hot backups.

Additionally, the VaultDR Server for Linux component is installed on the Linux NetVault: Backup Server and the VaultDR Online Plugin for Windows is installed on each Windows Client you wish to protect with online or hot backups.

In this scenario, VaultOS is used to perform the recovery of the Windows Clients.

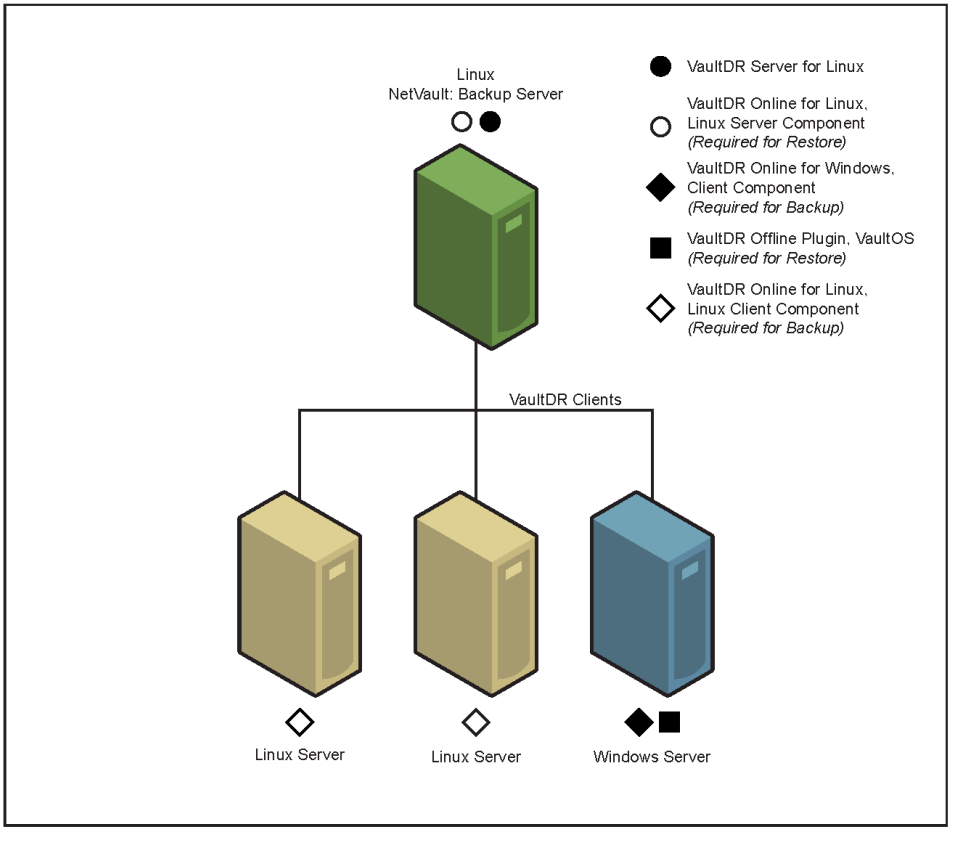


Figure 2-7: *Online Plugin for Windows and Online Plugin for Linux with Linux Server*

Refer to *The VaultDR Online Plugin for Windows* on page 55 and *The VaultDR Online Plugin for Linux* on page 83 for more information.

2.8.0 VaultDR Online for Windows Plugin and VaultDR Online for Linux Plugin with Windows NetVault: Backup Server

This scenario is deployed when the user wants to perform online or hot backups of both Linux and Windows Clients and has a Windows NetVault: Backup Server deployed.

The VaultDR Online for Linux, Windows Server Component is installed on the Windows NetVault: Backup Server and the VaultDR Online Plugin for Linux, Linux Client Component is installed on each Linux Client you wish to protect with online or hot backups.

Additionally, the VaultDR Server for Windows component is installed on the Windows NetVault: Backup Server and the VaultDR Online Plugin for Windows is installed on each Windows Client you wish to protect with online or hot backups.

In this scenario, VaultOS is used to perform the recovery of the Windows Clients.

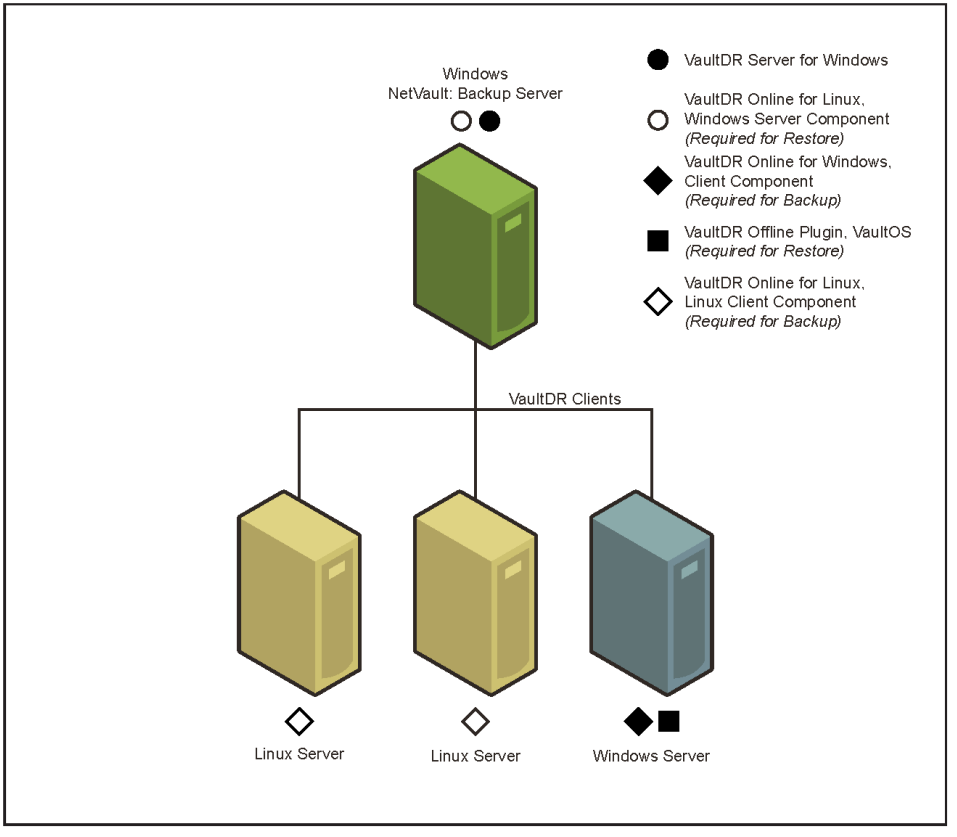


Figure 2-8: *Online Plugin for Windows and Online Plugin for Linux with Windows Server*

Refer to *The VaultDR Online Plugin for Windows* on page 55 and *The VaultDR Online Plugin for Linux* on page 83 for more information.

SECTION 2:

The VaultDR Offline Plugin

Chapter 3:

The VaultDR Offline Plugin for Intel x86 Clients

3.0.0 About VaultDR Server

The **VaultDR Server** resides on the NetVault: Backup Server and enables backup and recovery of a target client's data via the **VaultDR Offline Plugin**.

3.0.1 VaultDR Server Environment Overview

The processes required to successfully set up and use the **VaultDR Server** must be followed in a specific order. The table below offers a rough outline of how to establish a **VaultDR Server** environment.

The VaultDR Server Environment Setup
Components Required:
■ **VaultDR Server** ■ **VaultOS Operating System**
Installation
Install the **VaultDR Server** on the *NetVault: Backup Server*.
Configuration
Configure the **VaultDR Server**: 1. Create a **VaultOS Boot System** (e.g., to a writable CD-ROM). 2. Add the target VaultDR Clients to the **VaultDR Server** on the NetVault: Backup Server.
Backup
Perform an offline backup of the desired Client machine. 1. Boot the target VaultDR Client system with **VaultOS**. 2. From the NetVault: Backup Server, administer backup of Client by selecting data to be backed up (e.g., partitions, drives, volumes, etc.).
Restore
Perform an offline restore to the target VaultDR Client 1. Boot the target VaultDR Client system with **VaultOS**. 2. From the NetVault: Backup Server, administer restores to the target VaultDR Client by selecting data included in the DR backup.

3.1.0 Installation

This section covers all of the steps required to successfully install (and upgrade) the **VaultDR Server**.

3.1.1 Pre-Installation Considerations and Requirements

Prior to installing (or upgrading) the **VaultDR Server**, the following points must be reviewed, and applicable actions must be taken:

- **VaultDR Server Component Compatibility** – In order for the **VaultDR Server** to function properly, all of its associated components ***must be the proper version*** (i.e., version "X" of the **VaultDR Server** will only work with its appropriate version of **VaultOS**). Refer to the *Release Notes* provided with the binary installation file for complete compatibility information.
- **Existing VaultDR Server Backups (upgrades ONLY)** – It is important to note that backups performed with earlier versions of this plugin may not be compatible with the newest release of the plugin. Prior to performing an upgrade to the newest version, consult the *Release Notes* for complete compatibility information.

Before installing the **VaultDR Server**, make sure that the following requirements have been met:

- The ***Server*** version of the NetVault: Backup software must be installed on at least one machine.
- The VaultDR Client machine (the target of the backup/restore) must have a supported Intel x86-based operating system installed.

3.1.2 Installation Procedure

The NetVault: Backup **VaultDR Server** must be installed on a NetVault: Backup Server. It is installed and removed via the NetVault Client **Management** window. To install this plugin, follow the procedure below.

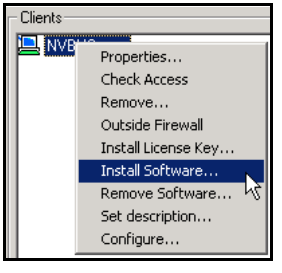


Figure 3-1: *The Install Software option*

1. From the machine acting as the NetVault: Backup Server, open the NetVault **Client Management** window by clicking the **Client Management** button on the NetVault: Backup GUI (or select **Client Management** from the **Administration** pull-down menu).
2. Right-click on the desired machine (the NetVault: Backup Server) in the **Clients** frame and select **Install Software** from the pop-up menu.
3. Navigate to the location of the **".npk"** installation file (e.g., the NetVault: Backup APM Installation CD or the directory where the file was downloaded).

Select the file (e.g., **drc*xxxx*.npk**) and click **Open** and the installation process will begin.

Note: Based on the operating system in use and the location of this file, the directory path for it may vary, but the file required for installation of this plugin should be entitled **"drc*xxxx*.npk"** (where "***xxxx***" represents the software platform and version number).

Important: If using the NetVault: Backup APM Installation CD to install a plugin to a Linux-based operating system, it may first be necessary to mount the CD-ROM drive in order to access the disk. See the relevant operating system's documentation for instructions on how to accomplish this. This also applies to accessing files for other procedures required for installation of the **VaultDR System** plugins.

4. Once the installation has completed, a successful installation message will appear in the **Install Software** dialog. This completes the process, and the plugin is now ready for use.

3.1.3 Removing the VaultDR Server

Follow the procedure below to remove the **VaultDR Server**:

1. Access the **Client Management** window of NetVault: Backup.
2. Right-click on the NetVault: Backup Server or the appropriate NetVault Client in the **Clients** list to reveal the pop-up menu and select **Remove Software**.

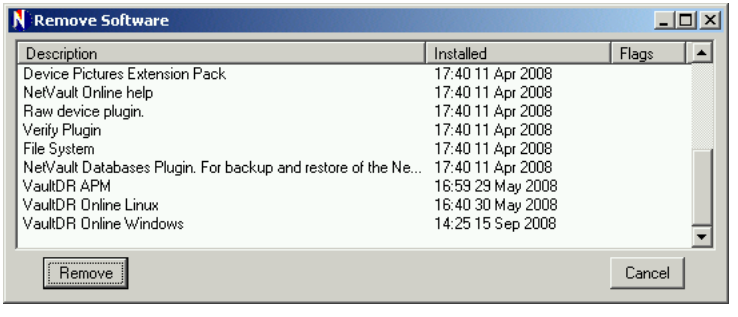


Figure 3-2: *The Remove Software dialog*

3. Select the desired Plugin for removal (e.g., Select the desired Plugin for removal (e.g., **VaultDR APM** or **VaultDR Online APM**) from the displayed list and click the **Remove** button.
4. A dialog will appear asking for confirmation. Click **OK** to proceed (or **Cancel** to abort). Clicking **OK** results in the removal of the software, and a confirmation message will appear. Click **OK** to close this dialog and return to the **Client Management** window.

3.2.0 Configuration

The second phase of setting up the **VaultDR Server** involves environment configuration. This configuration process can be broken down into two basic steps:

- **Phase 1: Creating a VaultOS Boot System**
- **Phase 2: Configuring the Plugin on the NetVault: Backup Server**

The sections that follow fully illustrate the procedures that must be followed to complete both of these steps.

3.2.1 Phase 1: Creating a VaultOS Boot System

Prior to using the **VaultDR Server**, it is necessary to create a **VaultOS Boot System.** This minimal operating system loads to a target machine's memory, rather than to its hard drive. This leaves the hard drive(s) inactive (offline) and in a suitable state for backup or restore. The **VaultOS** operating system is created on a writable CD. You can also boot from a LiveCD with the VaultOS binaries on a separate device, such as a USB stick. This is described in *Creating a Rescue Device for Use with a LiveCD* on page 30.

3.2.1.a Creating a Bootable VaultOS CD

The **VaultDR Server** allows you to create a bootable CD-ROM that can be used to prepare a Client machine for the restore process.

Requirements

The following items are required for this procedure:

- Installation ISO image (obtained via download).
- A writable CD-ROM drive
- A blank CD-ROM
- CD generation software

Creation Procedure

Note: It is recommended that all applications running on the machine performing this operation be shut down before starting this procedure.

1. Download VaultOS from the BakBone website via the following link:

   http://www.bakbone.com/downloads

2. Follow the instructions on the **Download Software** page to download the VaultOS component for your operating system.
3. Note the name and location of this file (e.g., "C:\downloads\vaultos_x86_v*xxx*.iso" where *xxx* represents the software version number).

4. Insert a blank CD-ROM in the writable drive.
5. Create a new CD with CD generation software using the VaultOS ".**iso**" file. For details on this procedure, see the relevant documentation for the CD generation software in use.

3.2.1.b Creating a Rescue Device for Use with a LiveCD

A LiveCD is an operating system that boots from a CD without the necessity of installing to a hard drive. This allows you to initiate disaster recovery without the operating system on disk. VaultDR supports booting from a LiveCD with VaultOS on a separate device, such as a USB stick (RescueUSB) or another CD (RescueCD). For a list of supported operating system LiveCDs, refer to the *NetVault: Backup VaultDR Offline Plugin Supported Platforms* document on the BakBone website:

http://www.bakbone.com/documentation

Important: The LiveCD must mount the loop-back device in order to perform backup and restore with VaultDR.

Requirements

The following items are required to create a RescueCD or RescueUSB device:

- The "**drdaemon**" and "**vaultdr_client.sh**" files (obtained via download)
- A USB port and a USB device with enough space to hold the "**drdaemon**" and "**vaultdr_client.sh**" files (1MB is sufficient)

  OR
- A writable CD-ROM drive and a blank CD

Note: You will need two CD-ROM drives on the target system in order to use a RescueCD with a LiveCD.

Creation Procedure

1. Download VaultOS from the BakBone website via the following link:

   http://www.bakbone.com/downloads
2. Note the name and location of this file (e.g. "/home/vaultos_x86_v*xxx*.zip" where *xxx* represents the software version number).
3. Extract "**drdaemon**" and "**vaultdr_client.sh**" from the ".zip" file and copy them to your blank media (e.g. a USB stick or CD-R disc).

For instructions on booting from a LiveCD, refer to *Booting the VaultDR Client from a LiveCD* on page 36.

3.2.2 Phase 2: Configuring the VaultDR Server

Before performing a backup with the **VaultDR Server**, the plugin must be configured on the NetVault: Backup Server. The section that follows details this process.

3.2.2.a Adding a VaultDR Client to the VaultDR Server

In order to properly access a VaultDR Client machine for backup and restore, you must add it to the **VaultDR Server**. Follow the steps below to accomplish this.

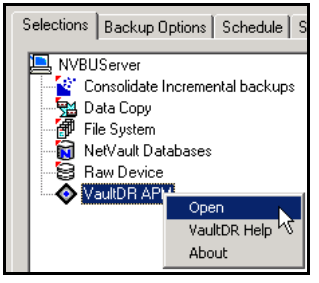


Figure 3-3: Opening the VaultDR Server on the NetVault: Backup Server

1. Access the **Backup** window via the **Backup** button or the command toolbar in the NetVault: Backup GUI (or select **Backup** from the **Operations** pull-down menu).
2. In the Selections tab of the Backup window, locate the machine acting as the NetVault: Backup Server (i.e., the machine with the **VaultDR Server** installed) and open it by double-clicking on it.
3. Locate the **VaultDR Server** in the list of available APM/plugins revealed (labeled as **"VaultDR APM"**) and open it by double-clicking on it (or right-click on it and select **Open** from the pop-up menu).
4. With the first launching of the plugin, the **Open** command will reveal the **Add VaultDR Client** dialog. The following fields must be input in order to add a **VaultDR Client**:

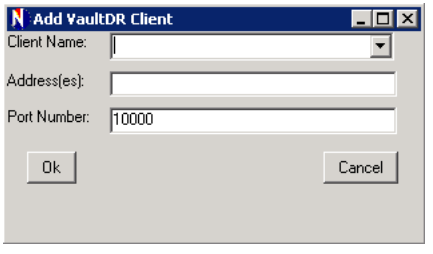


Figure 3-4: The Add VaultDR Client dialog

- **Name –** The name of the desired Client. NetVault: Backup will scan the network, looking for any available systems that can be added as a VaultDR Client, and reveal them for selection from this drop-down menu.
- **Address(es) –** A comma-separated list of addresses that can either be IP addresses or resolvable network names (e.g., 10.55.55.1, Server_1, 10.55.55.2, etc.) that refer to the machine to be added.
- **Port Number** – The port used to invoke **drdaemon** (e.g., 15555). The default value is 10000.

Important: If you specify a port number other than the default 10000, you will have to manually enter the new port number when you boot the VaultDR Client. For details, see step 17 on page 41.

Adding Additional VaultDR Clients

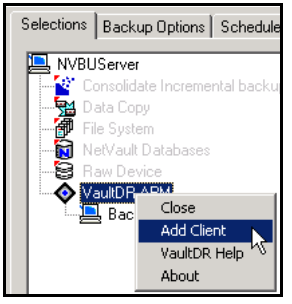


Figure 3-5: *The **Add Client** option*

Once an initial **VaultDR Client** has been added to the NetVault: Backup Server, it is necessary to use the procedure detailed below to add additional Clients.

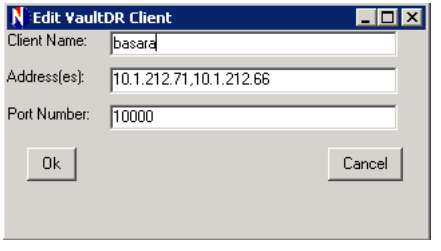
1. Launch the **Backup** window and double-click on the NetVault: Backup Server (with the **VaultDR Server** installed on it) to open it.
2. Double-click on the **VaultDR Server** to open it.
3. Right-click on the plugin and select **Add Client** from the pop-up menu. The **Add VaultDR Client** dialog launches.
4. Input values in the fields of the dialog as explained above in **Step 4** of the section *Adding VaultDR Clients to the NetVault: Backup Server (**VaultDR Server** ONLY)*.
5. Repeat these steps as required until all **VaultDR Clients** have been added.

Editing an Existing VaultDR Client

With a **VaultDR Client** added to the NetVault: Backup Server, the settings made during the original addition process can be edited, if necessary. To accomplish this, follow the steps outlined below.

1. From the **Selections** tab, with the **VaultDR APM** icon open to reveal the desired client, right-click on it to access its associated pop-up menu and select **Edit Client**.
2. The **Edit Client** dialog appears, containing the following fields:

Figure 3-6: *The Edit VaultDR Client dialog*



- **VaultDR Client Name** – This field contains the previously set name for the selected client. Change this value as desired. If changed, this is how this VaultDR Client will be revealed in NetVault: Backup.
- **IP Address** – This field will contain the IP address originally set for this client. It is possible to change this value completely, or add additional addresses, each separated with a comma.
- **Port Number** – The port used to invoke **drdaemon** (e.g., 15555). The default value is 10000.

Important: If you specify a port number other than the default 10000, you will have to manually enter the new port number when you boot the VaultDR Client. For details, see step 17 on page 41.

3. With the desired new values input, click **OK** to close this dialog and commit the changes.

Removing an Existing VaultDR Client

If it is necessary to remove a previously added **VaultDR Client** from the NetVault: Backup Server, follow the steps outlined below:

1. From the **Selections** tab, with the **VaultDR APM** icon open to reveal the desired **VaultDR Client**, right-click on it to access its associated pop-up menu and select **Remove Client**.
2. A dialog will launch asking for confirmation of the removal command. Click **Yes** to remove it (or **No** to abort).

3.2.2.b The 'About' Dialog

Also available from this pop-up menu is the **About** option. This option can be accessed in order to view version information for the currently installed plugin (e.g., **VaultDR** or **VaultDR Online**). To access this option, right-click on the plugin and select **About** from the pop-up menu. Click **OK** to close the **About** dialog and return to the **Backup** window.

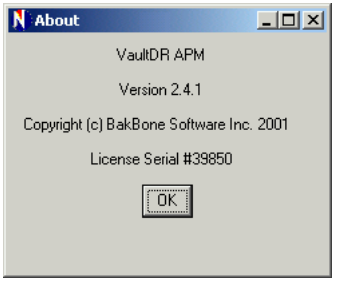


*Figure 3-7: The **About** dialog*

3.3.0 Booting a VaultDR Client with VaultOS

To use the **VaultDR Server** to backup or restore a target VaultDR Client, you must first take the system offline and boot it with the required components. This is accomplished by booting the Client machine with the **VaultOS Boot System** (the media created in the processes explained in the section, *Phase 1: Creating a VaultOS Boot System* on page 29). Rather than installing software to the Client's hard drive, this boot system will load a minimal operating system to the VaultDR Client's memory, leaving the hard drive completely inactive (offline) and in a suitable state for either backup or restore.

3.3.1 Booting with VaultOS

This process entails the configuration of network equipment installed on the target VaultDR Client (i.e., loading driver software for the system's NIC/SCSI card to memory in order to use the device and access the system).

The overall boot process with **VaultOS** can be broken down into two phases:

- **Phase 1: Gather VaultDR Client Network Information**
- **Phase 2: Boot the VaultDR Client with VaultOS Media**

Important: Before beginning this procedure, it is necessary to verify the boot order of the target VaultDR Client. The machine's ***CD-ROM Drive*** must be the first source of a boot for this process to work.

3.3.1.a Gather VaultDR Client Network Information

In this first phase of the process, you must gather specific network-related information from the VaultDR Client for use in the boot process (e.g., NIC and SCSI interface values). This includes the following values:

- **IP Address**
- **Network Mask**
- **Gateway**

Important: If the target VaultDR Client is configured with multiple NIC/SCSI devices for access, it is recommended that you gather the above information for ***each device***. The **VaultOS** boot process will recognize ***all*** of these device and request that you configure each of them individually, with this information (but only one of the devices actually needs to be successfully configured for use).

The sections that follow offer example procedures that can be used to obtain these required values, based on the operating system in place on the target VaultDR Client.

Linux VaultDR Client

1. Log in locally to the Linux VaultDR Client and initiate a Terminal Session.
2. Type the following command at the prompt:

   ifconfig

3. In the content that is revealed, locate and record the **IP Address** and the **Network Mask** values.

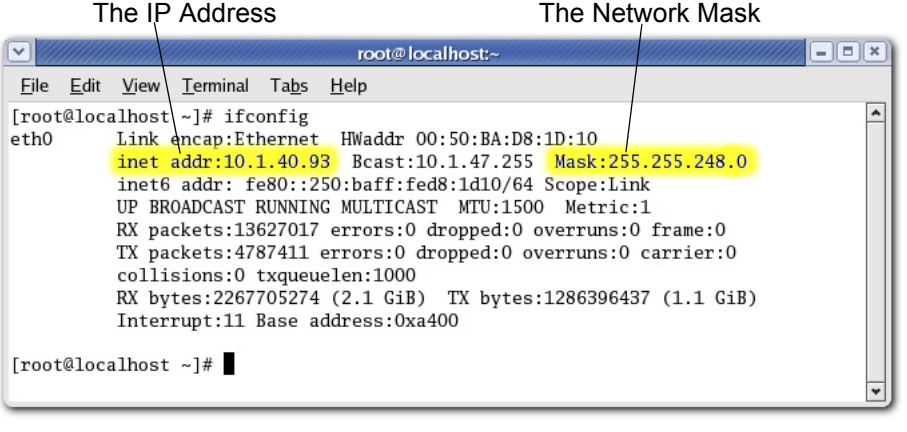


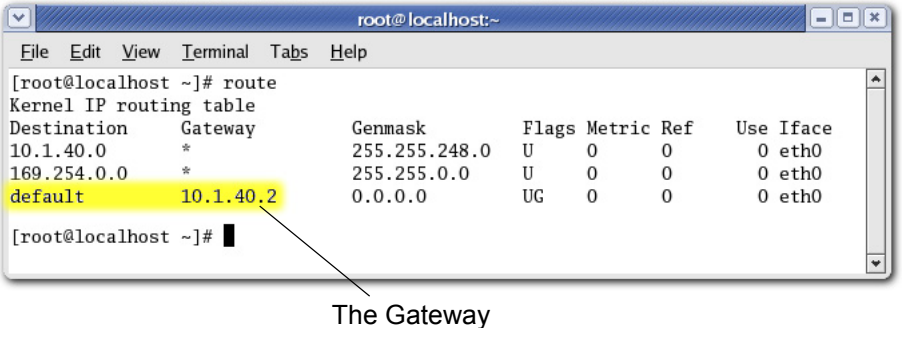
Figure 3-8: *The result of the* ***ifconfig*** *command, with the "IP address" and "Network Mask" values noted*

4. At the prompt, input the following command:

   route

5. In the content that is revealed, locate and record the **Gateway** value (when the command is issued, this value will be revealed as the **"default"** value).

Figure 3-9: *The result of the **route** command, with the "Gateway" value noted*



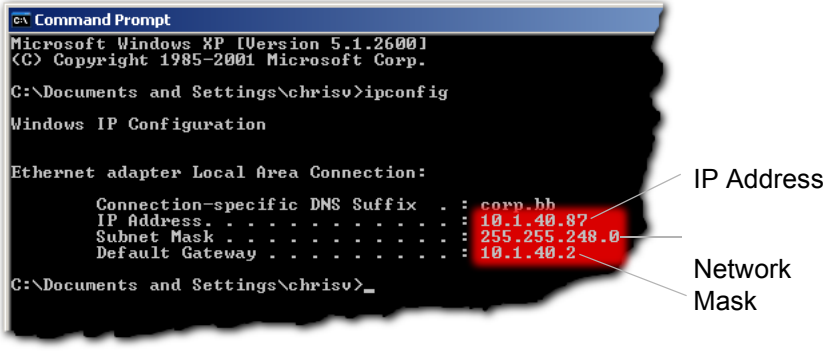
Windows VaultDR Client

1. Log in locally to the Windows VaultDR Client and launch a Command Prompt session.
2. Type the following command at the prompt:

   ipconfig

3. In the content that is revealed, locate and record the **IP Address**, **Subnet Mask** (**Network Mask)** and **Default Gateway** values.

Figure 3-10: *The results of the **ipconfig** command, with the required values noted*



With all relevant networking information noted, it is now possible to boot the target VaultDR Client. Follow the steps outlined in *Booting the VaultDR Client from a LiveCD* below if you are booting from a LiveCD. Otherwise, proceed to *Booting the VaultDR Client with VaultOS* on page 38.

3.3.1.b Booting the VaultDR Client from a LiveCD

If you are booting the VaultDR Client from a LiveCD, perform the following procedure. If you are booting the VaultDR Client from a standard VaultOS CD, proceed to *Booting the VaultDR Client with VaultOS* on page 38.

Requirements

The following items are required for this procedure:

- A LiveCD containing the desired operating system

Important: The LiveCD must mount the loop-back device in order to perform backup and restore with NetVault.

- A Rescue device (see *Creating a Rescue Device for Use with a LiveCD* on page 30)
- A USB port (for a RescueUSB device) or a secondary CD-ROM drive (for a RescueCD) on the target system.

Note: If you are using a RescueCD, you will need two CD-ROM drives on the target system — one for the LiveCD and one for the RescueCD.

1. Insert the LiveCD in the CD-ROM drive on the target system and reboot.
2. After the operating system launches, plug in the USB stick or load the RescueCD.
3. In most cases, the LiveCD will automatically mount the USB/CD drive and show an icon on the desktop.
   a. Use the “mount -l” command to find the path where the device is mounted.

      Example:

      ```
      # mount -l
      ...
      /dev/sdb1 on /media/disk type ext2 (rw,nosuid,nodev)
      ```

4. If the LiveCD does not automatically mount the USB drive, you must mount it manually as shown in the following sub-steps.

Note: Follow the same procedure to use a RescueCD by mounting a CD instead of a USB device.

   a. Perform the command, “ls -l /dev/disk/by-id/usb*” to find the USB devices on the system.

Example:

```
# ls -l /dev/disk/by-id/usb*
root 9 2007-09-26 8:16 /dev/disk/by-id/usb-JetFl -> ../../sdb
root 10 2007-09-26 8:16 /dev/disk/by-id/usb-JetFl-part1_-> ../../sdb1
root 10 2007-09-26 8:16 /dev/disk/by-id/usb-JetFl-part2 -> ../../sdb2
```

b. Always mount the first partition on the device.

Example:

```
# mount /dev/sdb1 /mnt/usb
```

5. Run "vaultdr_client.sh".

Example:

```
# cd /mnt/usb
# sh vaultdr_client.sh
```

The preceding command launches **drdaemon**.

Important: Some LiveCDs automatically mount all partitions for devices, which can lead to restore failure if the file system is mounted prior to a backup or restore job. If you boot with a LiveCD, make sure the file system is unmounted before performing a backup or restore.

Important: Some LiveCDs automatically use the swap partition for swap operations, which can lead to restore failure if the swap partition is used prior to a backup or restore job. If you boot with a LiveCD, make sure the LiveCD does not use the swap partition before performing a backup or restore.

6. If you configured VaultDR to use a port other than the default "10000" as shown in *The Add VaultDR Client dialog* on page 31 (or *The Edit VaultDR Client dialog* on page 32), you must exit from the **VaultDR Daemon** dialog and enter the new port number manually.
   a. To exit the **VaultDR Daemon** dialog, press **<Ctrl-C>**.
   b. At the command prompt, type the following command and press **Enter**:

```
drdaemon -p port_number
```

where *port_number* is the port you specified in *The Add VaultDR Client dialog* on page 31 (or *The Edit VaultDR Client dialog* on page 32).

Note: If you wish to relaunch **VaultDR Daemon** from the command prompt without changing the port number, type "**drdaemon**" and press **Enter**.

3.3.1.c Booting the VaultDR Client with VaultOS

Follow the steps below to boot from a standard VaultOS CD. If you are booting from a LiveCD, refer to *Booting the VaultDR Client from a LiveCD* on page 36.

1. Power down the VaultDR Client and insert the **VaultOS** CD.
2. Upon reboot, there will be a 60 second delay after the boot prompt appears. Press **Enter** to start the sequence immediately.

   A series of dialogs will launch as various applications are loaded to system memory.

Note: The initial load sequence may take several minutes, during which time the screen may appear blank.

Important: This process will only successfully continue if **VaultOS** can locate the appropriate NIC/SCSI driver components for the networking hardware available on the VaultDR Client. If no drivers can be found, you must manually load device drivers for the VaultDR Client.

3. The **Setup Networking** dialog launches first. Highlight the **Yes** button (using either the **Arrow** keys or the **Tab** key) and press **Enter** to begin.

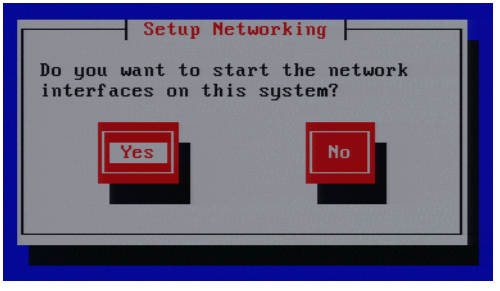


*Figure 3-11: The **Setup Networking** dialog*

   The **Network Configuration** dialog appears for all NIC/SCSI devices on the VaultDR Client machine.
4. If multiple NIC cards are present in the client machine, the following dialog appears. Highlight the NIC card to be configured and select **Edit**.

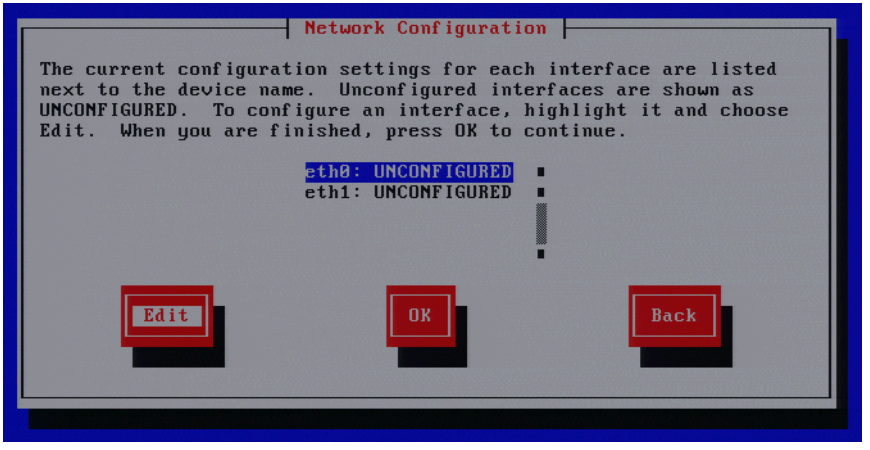


Figure 3-12: *The Network Configuration dialog*

5. If only one NIC card is present in the client machine, the following dialog appears. Select **Yes** to configure the network interface.

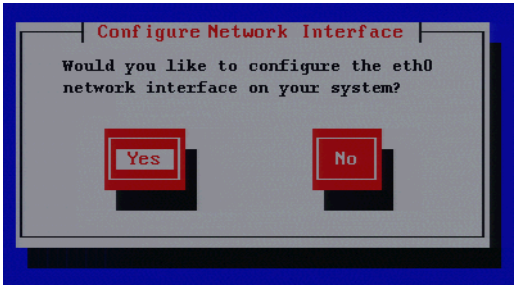


Figure 3-13: *The Configure Network Interface dialog*

6. The **Network Configuration for <Device Name>** dialog appears for the selected device. Press the **Spacebar** to enable **IPv4 support**. Use the **Tab** key to highlight the **OK** button and press **Enter** to continue.

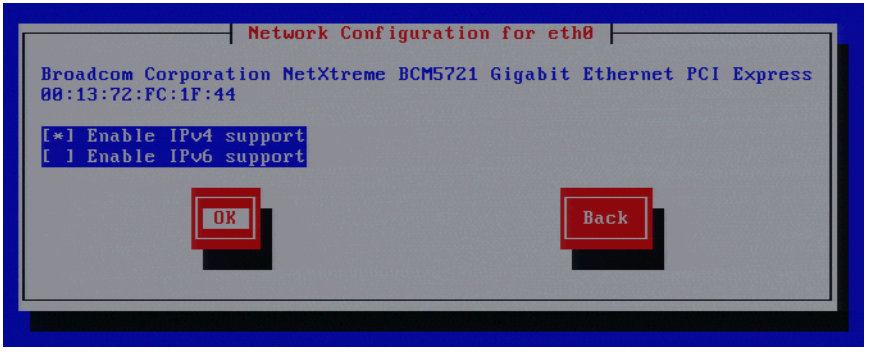
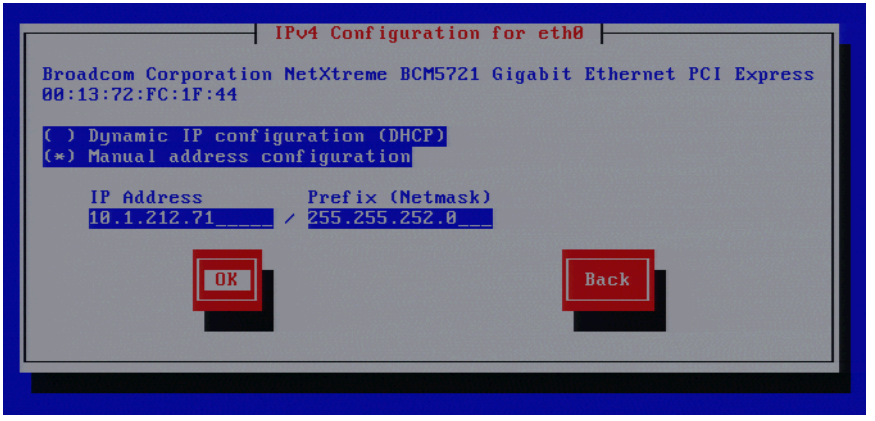


Figure 3-14: *The Network Configuration for eth0 dialog*

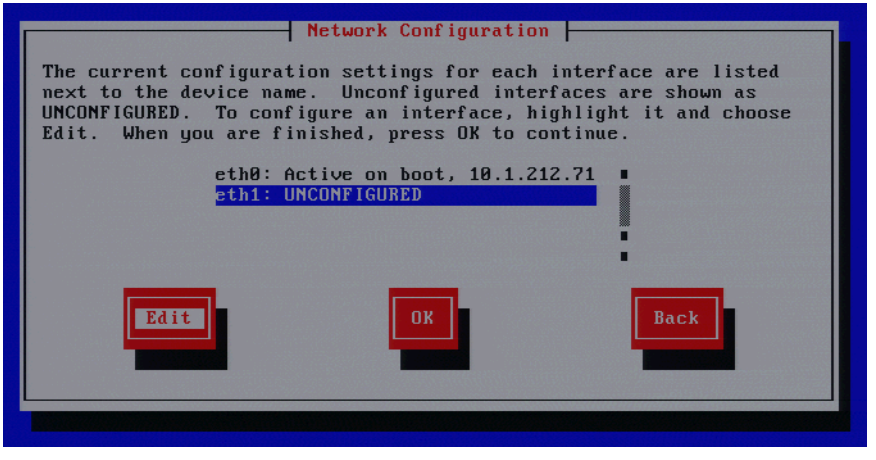
7. Use the **Tab** key to highlight **Manual address configuration** and press the **Spacebar** to enable the Manual address configuration.
8. Press the **Tab** key to place the cursor in the **IP Address** field, and input this value (as recorded during *Gather VaultDR Client Network Information* on page 34).

Figure 3-15: *The IPv4 Configuration for eth0 dialog*



9. Press the **Tab** key again to access the **Netmask** field and input the appropriate **Network Mask** (as recorded during *Gather VaultDR Client Network Information* on page 34).
10. Use the **Tab** key to highlight the **OK** button and press **Enter** to continue.
11. If an additional NIC/SCSI card exists on the target VaultDR Client, select the appropriate device from the **Network Configuration** dialog. Repeat **Steps 4–9** to configure the device for use.

Figure 3-16: *The Network Configuration dialog*



Important: If you do not wish to configure additional NIC/SCSI devices, this process can be skipped. However, you must ensure that the device is unconfigured.

12. Use the **Tab** key to highlight the **OK** button and press **Enter** to continue.
13. The **Miscellaneous Network Settings** dialog is launched. Use the **Tab** key to highlight the first field **"Gateway"** and input the appropriate value (as recorded during *Gather VaultDR Client Network Information* on page 34).

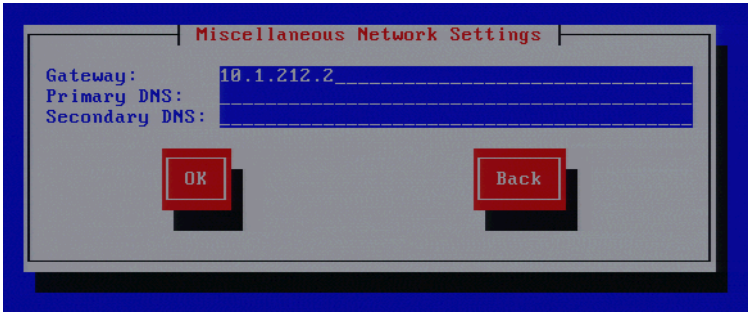


Figure 3-17: *The Miscellaneous Network Settings dialog*

14. Use the **Tab** key to skip through the two **DNS-related** fields and highlight the **OK** button. Press **Enter** to continue.
15. The **Network Interfaces** dialog appears. Select the **OK** button.

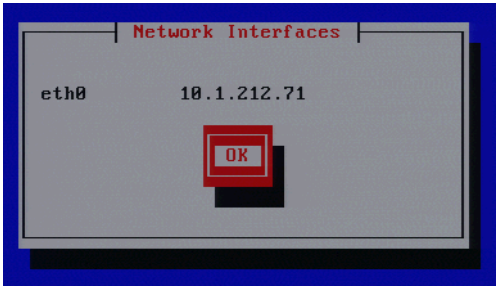


Figure 3-18: *The **Network Interfaces** dialog*

16. After clicking **OK**, the **VaultDR Daemon** dialog will launch automatically, awaiting commands from the NetVault: Backup Server. The Client is now prepared for backup or restore.

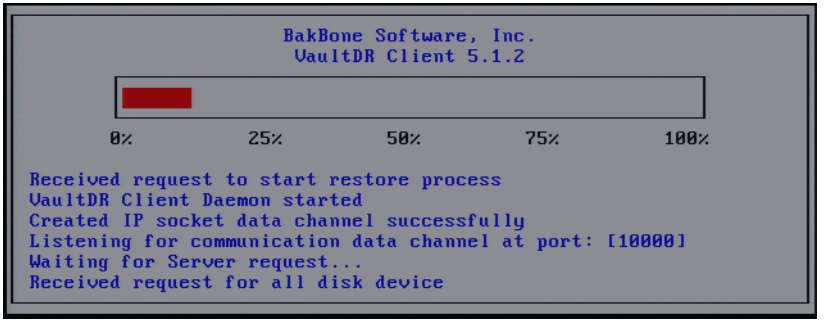


Figure 3-19: *The **VaultDR Daemon** dialog*

17. If you configured VaultDR to use a port other than the default "10000" as shown in *The Add VaultDR Client dialog* on page 31 (or *The Edit VaultDR Client dialog* on page 32), you must exit from the **VaultDR Daemon** dialog and enter the new port number manually.

a. To exit the **VaultDR Daemon** dialog, press **<Ctrl-C>**.
b. At the command prompt, type the following command and press **Enter**:

```
drdaemon -p port_number
```

where *port_number* is the port you specified in *The Add VaultDR Client dialog* on page 31 (or *The Edit VaultDR Client dialog* on page 32).

Note: If you wish to relaunch **VaultDR Daemon** from the command prompt without changing the port number, type "**drdaemon**" and press **Enter**.

3.4.0 Backing Up Data

The **VaultDR Server** makes it possible to backup full systems. In addition, the plugin provides granular backup capabilities allowing for the selection of individual items for a backup. This includes the following items:

- **Operating System**
- **Applications**
- **Specific User Information**
- **Disk Partitions** – All (or individual) partitions can be selected for backup.
- **Mounted Volumes (Linux/UNIX)** – All of which are backed up as individual partitions.

Note: The **Master Boot Record (MBR)** and the **Partition Table** items will be backed up automatically when a partition (all or individual) is backed up using the **VaultDR Server**. Therefore, these items are not available to select for a backup.

3.4.1 Phase 1: Prerequisites

Prior to initiating a backup with the **VaultDR Server**, review the following sub-sections for details on prerequisites that must be met.

3.4.1.a Step 1: Boot the VaultDR Client with VaultOS

It is first necessary to boot the target VaultDR Client with the **VaultOS** operating system to prepare it for the backup. Review all of the steps covered in the section, *Booting with VaultOS* on page 33 to accomplish this.

3.4.1.b Step 2: Verify Disk Geometry and Device Size

Prior to performing a backup of any portion of a VaultDR Client's hard drive, it is recommended that the **Disk Size** as well as the **Disk Geometry** of the selected drive be noted. When restoring previously backed up data, if these items are not taken into account, a restore could fail.

Example of How to Note the Drive Disk Size and Disk Geometry

A Client drive is divided into three partitions. The primary partition is 10 gigabytes (GB), the first logical partition is 7 GB and the second is 3 GB. A backup of the first logical partition is performed with the **VaultDR Server**. Upon restore of the system after a hard drive crash, if the first logical partition was restored, it would need to be restored to the proper partition (i.e., the first logical partition), or the restore would fail.

The above information, including the **Disk Size** and **Disk Geometry** of a selected Client, can be determined via the NetVault: Backup Server as follows:

1. With the VaultDR Client booted using **VaultOS** (as outlined in the section, *Booting a VaultDR Client with VaultOS* on page 33), access the NetVault: Backup Server and launch the NetVault: Backup GUI.
2. Access the **Backup** window and double-click on the NetVault: Backup Server to open it (i.e., the system containing the **VaultDR Server**).
3. Open the **VaultDR Server** by double-clicking on it.
4. Select the appropriate VaultDR Client displayed under the plugin and double-click on it to reveal the disk(s) contained within.
5. To determine the **Disk Geometry**, right-click on the desired disk and select **Disk Geometry** from the pop-up menu.
6. The **Display Device Geometry** dialog will display listing details about the partition structure of the selected disk.

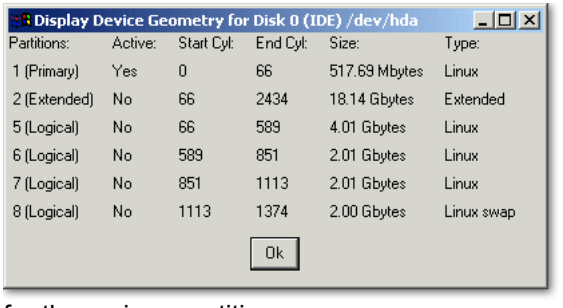
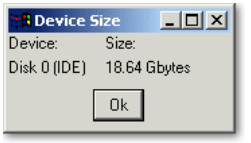


*Figure 3-20: The **Display Device Geometry** dialog*

   - **Partitions** – Each individual partition is listed here by number and the partition type.
   - **Active** – Displays the current activity state of the partition ("Yes" or "No").
   - **Start Cyl** – Displays the origination point (cylinder) for the various partitions.
   - **End Cyl** – Displays the partition's end point (cylinder).
   - **Size** – Displays the size of each partition.
   - **Type** – Displays the type of partition.
7. With sufficient information noted, click **OK** to close this dialog.
8. To determine the overall size of a disk, right-click on the desired disk in the **Backup** window and select **Disk Size** from the pop-up menu.

*Figure 3-21: The **Device Size** dialog*



9. The **Device Size** dialog will display listing specific details about the size of the selected disk.
   - **Device** – The number and type of the disk.
   - **Size** – The size of the selected disk.
10. After noting this information, click **OK** to close this dialog.

3.4.2 Phase 2: Backup Procedure

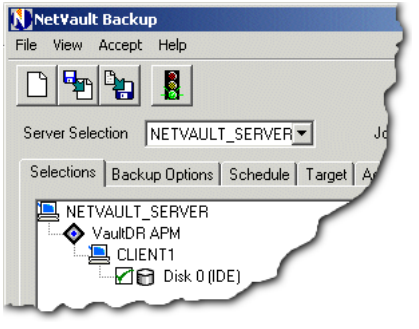
Follow the steps listed below to perform a **VaultDR** backup:

1. With the VaultDR Client booted with **VaultOS**, access the NetVault: Backup Server, and launch the NetVault: Backup GUI.the **Backup** window from the NetVault: Backup GUI.

Important: The **VaultDR Client** machine must be booted with the **VaultOS** software prior to each operation of the **VaultDR Server** (backup or restore). If this procedure is not completed properly, the **VaultDR Client** will be inaccessible from the NetVault: Backup Server. See the section, *Booting a VaultDR Client with VaultOS* on page 33 for details on this process.

2. Access the **Backup** window by clicking on the **Backup** button in either command toolbar or by selecting **Backup** from the **Operations** pull-down menu).
3. Locate the NetVault: Backup Server in the **Selections** tab (i.e., the system containing the **VaultDR Server**) and double-click on it to open it.
4. Locate the **VaultDR Server** in the list revealed (displayed as **"VaultDR APM"**) and open it by double-clicking on it. The hard disk(s) located on the Client system will be revealed. In order to select the entire disk for a backup, click the checkbox to the left of the disk title.

*Figure 3-22: The **Selections** tab of the **NetVault Backup** window*



5. Disk(s) can be opened by double-clicking on the disk. Individual partitions will be displayed and made available for selection. NetVault: Backup provides data on each type of partition, including the size, status and type. This information is displayed to the right of each partition, in parentheses.
   - **Primary Partition** – Each hard disk can contain up to four different *true partitions*. They are referred to as the primary partitions, and can be individually selected for backup.

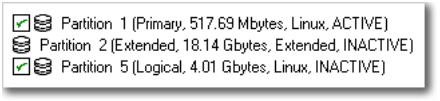


Figure 3-23: *The three types of partitions as revealed in the Backup window*

- **Extended Partition** – This is the space on the hard disk ***not allocated*** to the primary partition(s). This type of partition ***cannot*** be selected for a backup. In order to add it, the ***entire*** drive must be selected.
- **Logical Partition** – Logical partitions allow multiple system images to run in one machine. This can be multiple instances of the same operating system or different operating systems. Logical partitions can be individually selected for a backup.

Important: The Linux kernel supports only 15 partitions per SCSI disk and 63 partitions per IDE disk. Because of this limitation, VaultOS detects only 15 partitions per SCSI disk and 63 partitions per IDE disk, regardless of the target operating system. If you exceed the maximum supported partitions, an error message will appear on the NetVault: Backup Server.

6. Select items as desired for a backup. Selected items are marked by a green check, items not selected are blank, and omitted items contain a red cross.

Figure 3-24: *Examples of items selected and omitted for backup*

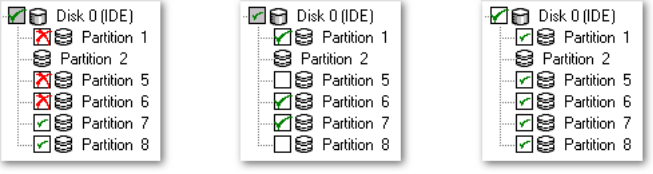
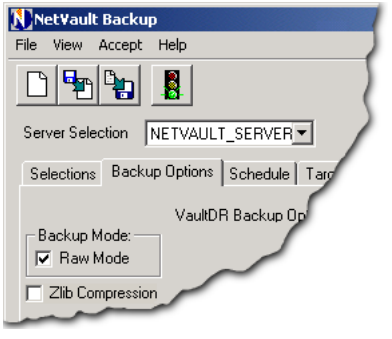


Figure 3-25: *The **Raw Mode** option selected from the **Backup Options** tab*

7. Select the **Backup Options** tab to reveal the following available options. You can select either **Raw Mode**, **Zlib Compression**, or both.



   - **Raw Mode** – When selected, all partition information for a selected hard drive will be ignored, and a "bit-by-bit" backup of the entire disk image will be performed. This bit-by-bit form of data transfer will occur during the restore of this backup as well, thereby eliminating the need to format the target drive.
   - **Zlib Compression** – Select this option to compress data on the VaultDR Client prior to transfer during backup. This will reduce overall network traffic during data transfer and also require less media space to accommodate the VaultDR backup. This option is particularly useful for partitions that contain a large amount of unused space, that would otherwise need 1:1 space on the backup medium.

Important: When **Raw Mode** is selected, not only will the media in use be backed up, but the entire partition as well (e.g., if 6 GB are in use on a 30 GB partition, 30 GB of media will be used to backup the partition). The **Raw Mode** option should only be used when a complete hard drive is selected for a **VaultDR Server** backup (i.e., not an individual partition).

Important: Dynamic disks must be backed up via **Raw Mode** to maintain partition information.

8. The remaining tabs (e.g., **Schedule**, **Target** and **Advanced Options**) contain additional options that can be set as desired. The options available in these tabs are not unique to the **VaultDR Server**. For more information on these tabs, see the *NetVault®: Backup Administrator's Guide*.
9. Input an appropriate title for the job in the **Job Title** box. It is recommended that a detailed name be used to allow for easy identification of the job at the time of restore.

Figure 3-26: *Inputting a Job Title and submitting a backup job*

10. Begin the job by clicking on the **Submit** button.
11. The GUI on the NetVault: Backup Server can be used to monitor the job in regards to its progress and job log entries (via the **Job Management** and **NetVault: Backup Logs** dialogs, respectively. For complete details on the use of these dialogs in the NetVault: Backup GUI, see the *NetVault®: Backup Administrator's Guide*).

3.5.0 Restoring Data

This section offers instructions for the recovery of a **VaultDR Server** backup.

3.5.1 Phase 1: Prerequisites

A DR restore procedure is a delicate operation, and prior to setting up and running one, the prerequisites covered in the following sections must be met:

3.5.1.a Step 1: Ensure that Device File Names Match

The target device name on the VaultDR Client (e.g., Disk 0 (IDE)) ***must be the same*** as it was at the time of backup.

Important: When relocating a DR backup, ensure that the hard disk installed on the new relocation target has the same name as the hard disk that existed in the original target machine.

3.5.1.b Step 2: Boot the VaultDR Client with VaultOS

It is first necessary to boot the target VaultDR Client with the **VaultOS** operating system to prepare it for the restore of a DR image. Perform the steps covered in the section, *Booting a VaultDR Client with VaultOS* on page 33 to accomplish this.

3.5.1.c Step 3: Gather Noted Device Size and Disk Geometry Information

This information should have been noted prior to the backup (see the section, *Step 2: Verify Disk Geometry and Device Size* on page 42). Have this information handy to complete the restore properly.

3.5.1.d Step 4: Verify Access to the Target VaultDR Client

The VaultDR Client machine that is to serve as a target for the restore must be accessible to the **VaultDR Server**. The section that follows outlines the required steps for this verification.

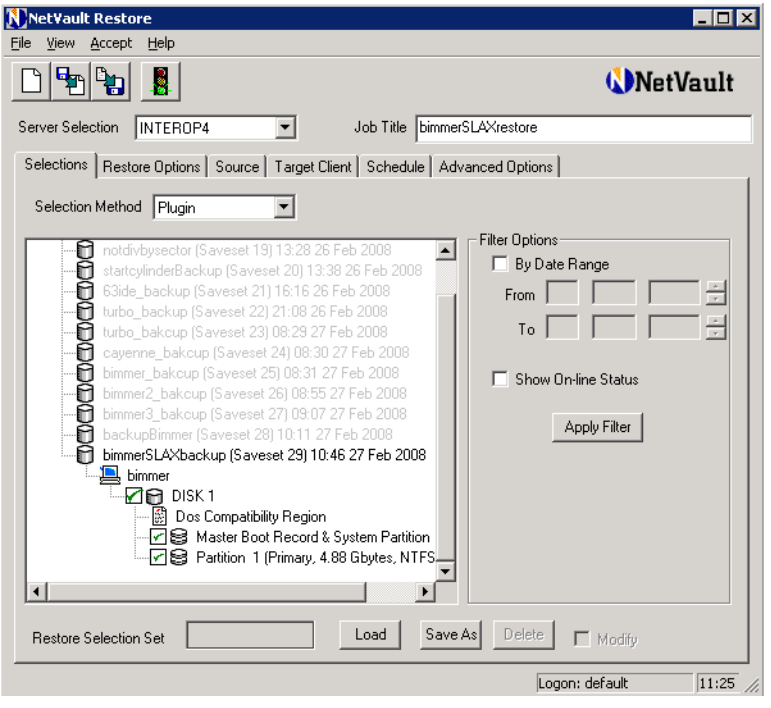
1. With the VaultDR Client booted with **VaultOS**, access the NetVault: Backup Server and launch the NetVault: Backup GUI.
2. Access the **Backup** window to verify that the desired Client machine has been added as a **VaultDR Client**. To do this, follow the procedure below:
   a. Open the **VaultDR Server** to reveal any previously added Clients.
   b. Browse the list for the desired **VaultDR Client**. To verify settings for a specific **VaultDR Client**, right-click on the Client name and select **Edit** from the pop-up menu.
   c. The **Edit VaultDR Client** dialog launches. Verify that the data is correct or change it as required.
   d. If the **VaultDR Client** is added properly, continue on to the next section, *Phase 2: Restore Procedure*; otherwise, proceed to the following step.
3. Add the desired **VaultDR Client**. For detailed instructions on this process, see the section *Adding a VaultDR Client to the VaultDR Server* on page 31. Once completed, close the **Backup** window of the **VaultDR Server** and continue on to the *Restore Procedure* section that follows.

3.5.2 Phase 2: Restore Procedure

1. From the NetVault: Backup Server, access the **Restore** window from the NetVault: Backup GUI (by clicking on the **Restore** button or by selecting **Restore** from the **Operations** pull-down menu).
2. In the **Selections** tab of the **Restore** window, **VaultDR Server** backups are displayed from the NetVault: Backup Server. Locate this system in the list and double-click on it in order to open it.

3. Locate the **VaultDR Server** (displayed as **"VaultDR APM"**) and double-click on it to open it. The backup saveset(s) from previous backup(s) completed with this plugin will be revealed. Double-click on the desired saveset in order to open it.
4. The previously backed up Client machine will be displayed. Double-click on it to open it and reveal the disk(s) that were backed up.
5. The individual disk(s) that were backed up will be displayed. To restore the entire disk, click in the box to the left of the appropriate disk title to select it.

Figure 3-27: *The* ***Selections*** *tab on the* ***NetVault Restore*** *dialog*



6. It is also possible to expand a disk to view its contents. Double-click on the desired disk to open it. With a disk open, individual items can be selected for restore if desired.

   Note: The **Dos Compatibility Region** is the first 32k – 512 bytes from start of the disk that immediately follows the Master Boot Record (MBR). VaultDR backs up this region to support GRUB Stage 1.5. However, this region will always be backed up and restored regardless of the existence of GRUB Stage 1.5. This option is non-selectable.

   Selectable items for a restore consist of the following:

   - **Master Boot Record and System Partition**
   - **Individual Partitions**

7. Select the **Restore Options** tab to access the following:

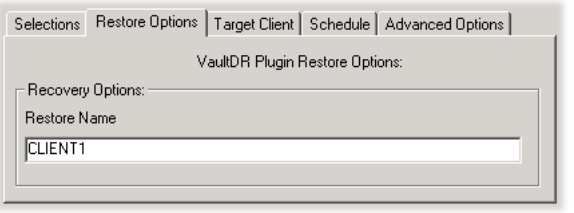


*Figure 3-28: The **Restore Name** field on the **Restore Options** tab*

   - **Recovery Options Frame** – This frame contains the **Restore Name** field. By default, the value in this field is NetVault: Backup's name for the VaultDR Client that this backup was originally performed from (based on the backup saveset selected from the **Selections** tab of the **Restore** window). This name is associated with a specific IP address that was previously configured. If this value is left at its default setting, selected data will be restored to the machine that was originally backed up. This field can be used if it is necessary to relocate restored data to a Standby VaultDR Client (for complete details on this procedure and its use of this option, see the section *Recovery to a Standby VaultDR Client* on page 50).
8. The remaining tab selections in the **Restore** window (e.g., **Schedule**, **Advanced Options** and **Target Client**) offer additional options that can be set as desired. The options available are not specific to the **VaultDR System Plugins**. For more information on these options, see the *NetVault®: Backup Administrator's Guide*.
9. Input an appropriate title for the job in the **Job Title** box.
10. Begin the job by clicking on the **Submit** button.

The following issues apply when restoring a **VaultDR Offline Plugin** backup to a disk other than its original disk. Disregard this note when restoring a **VaultDR Offline Plugin** backup to its original disk.

- If selecting individual partitions for a restore, it is also necessary to select the **Master Boot Record and System Partition** item. Failure to do so will result in a failed restore.
- When performing a restore of a **VaultDR Server** backup, options available in the **Target Client** tab should be left at their default settings. If a target other than the intended is selected from this tab the restore will fail.

3.5.3 Recovery to a Standby VaultDR Client

In the event of a hardware failure in a specific Client machine, it is possible to restore a previous **VaultDR Backup** to another, pre-configured VaultDR Client, or **"Standby"**. Follow the procedure below to accomplish this.

Before performing the recovery procedure, consider the following important points:

- This procedure will only work when restoring backups performed with the standard **VaultDR Server**.
- The target **VaultDR Client** (the **"Standby"**) for this operation must be pre-configured using the procedure described in the section *Adding a VaultDR Client to the VaultDR Server* on page 31.
- When attempting this operation, there must be sufficient disk space on the **Standby** machine, otherwise the operation will fail. For more information, see *Step 2: Verify Disk Geometry and Device Size* on page 42.
- With this process, it is recommended that the new target machine have ***at least a similar*** hardware configuration to that of the originally backed up machine (in regards to the NIC and SCSI cards used). If the hardware in use differs too much from the original, driver software conflicts may occur, resulting in a failed restore.
- Values input in the **Restore Name** field in the **Restore Options** tab are case-sensitive. Ensure that the exact NetVault: Backup name of the machine to be relocated to is input in this field, otherwise the restore will fail.
- Relocations of this type ***must be*** restored to the same partition they were backed up from. For example, if a VaultDR backup was taken of a system's **"C:\"** partition on a Windows-based system, the restore must be performed to the relocation target's **"C:\"** partition as well. It is not possible to restore to a different partition.

3.5.3.a Recovery Procedure

1. From the **Selections** tab of the **Restore** window, access the relevant VaultDR backup saveset(s) and select the desired items for a restore.
2. From the **Restore** window, select the disk to be relocated.
3. Right-click on a disk item and select **Rename** from the pop-up menu.

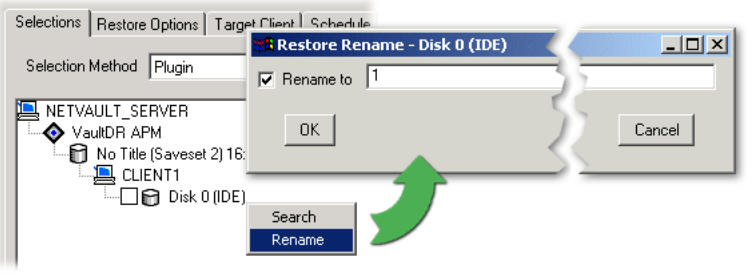


Figure 3-29: *Selecting the **Rename** option to access the **Restore Rename** dialog*

4. The **Restore Rename** dialog appears. Click the checkbox to the left of the **Rename to** field in order to activate it and input the Disk Number for the disk to be restored. (E.g., Input 0 for the system disk 1, 1 for the system disk 2 and so on. Note that evaluation of the SCSI disks is done before the IDE disks. So a system with two SCSI disks and two IDE disks would have the numbering 0 – SCSI 1, 1 – SCSI 2, 2 – IDE 1, 3 – IDE 2.)
5. Repeat **Steps 3** and **4** above for each disk that is to be relocated.
6. Select the **Restore Options** tab.
   - **Restore Name** – Input the name of the pre-configured VaultDR Client that is to serve as the standby machine in this field.
7. Continue with the restore (as explained previously in the section *Phase 2: Restore Procedure* on page 47) and submit the job.

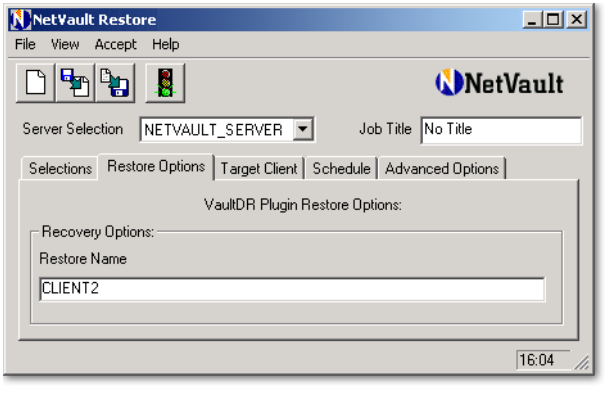


Figure 3-30: *The **Recovery Options** frame of the **Restore Options** tab*

SECTION 3:

The VaultDR Online Plugin

Chapter 4:

THE VAULTDR ONLINE PLUGIN FOR WINDOWS

4.0.0 About the VaultDR Online Plugin for Windows

The **VaultDR Online Plugin for Windows** operating systems (hereinafter referred to as the **VaultDR Online Plugin**) is a Disaster Recovery (DR) solution that allows you to fully backup and restore an entire hard disk on a target client, including the operating system, applications, system settings, partition information, and data.

- **Backup** – The backup process allows you to target a Windows-based system, and perform a full and complete backup of its contents while the system remains ***online and available*** to users.
- **Recovery** – The recovery process requires that you utilize the VaultOS boot utility provided with the plugin, to take the protected Windows-based system ***offline***, which allows for complete access to its hard disk for restore operations.

Important: This plugin works in conjunction with the **VaultDR Server**. Prior to conducting a backup with the **VaultDR Online Plugin**, you must install the **VaultDR Server** and verify connectivity between target VaultDR Client(s) and the NetVault: Backup Server where VaultDR Server is installed. In addition, the VaultDR Server is required to perform all restores of **VaultDR Online Plugin** backups.

4.0.1 VaultDR Online Plugin Environment Overview

The processes required to successfully set up and use the **VaultDR Online Plugin** must be followed in a specific order. The table below offers a rough outline of how to establish a **VaultDR Online Plugin** environment.

The VaultDR Online Plugin for Windows Environment Setup

Components Required:

VaultDR Server

- **VaultDR Online Plugin**
- **VaultOS Operating System**

Installation

1. Install the **VaultDR Server** on the ***NetVault: Backup Server***.
2. Add Client machine(s) to be backed up by the **VaultDR Online Plugin** to the NetVault: Backup Server (i.e., via the **Client Management** window in the NetVault: Backup GUI).
3. Install the **VaultDR Online Plugin** on any NetVault Client machine requiring ***active*** Disaster Recovery backups (e.g., the Clients added in Step 2 above, but not the NetVault: Backup Server itself).

Configure the VaultDR Server

1. Create a **VaultOS Boot System** (e.g., to a writable CD-ROM)
2. Add the target VaultDR Clients to the **VaultDR Server** on the NetVault: Backup Server.

Verify Access to the VaultDR Server

You must verify that all target VaultDR Clients are accessible to the **VaultDR Server**. Failure to do so may result in an inability to perform a restore.

- Boot the target VaultDR Client system with **VaultOS**.
- From the NetVault: Backup Server, access the **VaultDR Server** to ensure that the target VaultDR Client is accessible to the **VaultDR Server**.

Perform Online Backups with the VaultDR Online Plugin

From the NetVault: Backup Server, perform online backups as required, of each VaultDR Client using the **VaultDR Online Plugin** (e.g., O/S, applications, system settings, etc.).

Recovery

Perform an *offline* restore to the target VaultDR Client

1. Boot the target VaultDR Client system with **VaultOS**.
2. From the NetVault: Backup Server, administer restores to the target VaultDR Client by selecting data included in the VaultDR Online Plugin backup(s).

4.1.0 Installation

Before installing the **VaultDR Online Plugin**, you must install the **VaultDR Server**. This section covers all of the steps required to install the **VaultDR Server** and the **VaultDR Online Plugin**.

4.1.1 Installing the VaultDR Server

Before installing the **VaultDR Server**, make sure that the following requirements have been met:

- The ***Server*** version of the NetVault: Backup software must be installed on at least one machine.
- The VaultDR Client machine (the target of the backup/restore) must have a supported Windows operating system installed.

Important: In order for the **VaultDR Server** to function properly, all of its associated components must be the proper version (i.e., version "X" of the **VaultDR Server** will only work with its appropriate version of **VaultOS**). Refer to the *NetVault: Backup Supported APMs and Plugins* document on the BakBone website for details.

4.1.1.a Installation Procedure

The NetVault: Backup **VaultDR Server** must be installed on a NetVault: Backup Server. It is installed and removed via the NetVault Client **Management** window. To install this plugin, follow the procedure below.

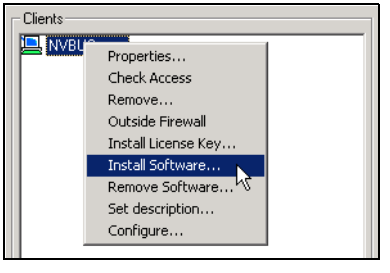


Figure 4-1: *The **Install Software** option*

1. From the machine acting as the NetVault: Backup Server, open the NetVault **Client Management** window by clicking the **Client Management** button on the NetVault: Backup GUI (or select **Client Management** from the **Administration** pull-down menu).
2. Right-click on the desired machine (the NetVault: Backup Server) in the **Clients** frame and select **Install Software** from the pop-up menu.
3. Navigate to the location of the **".npk"** installation file (e.g., the NetVault: Backup APM Installation CD or the directory where the file was downloaded). Select the file (e.g., **drc*xxxx*.npk**) and click **Open** and the installation process will begin.

Note: Based on the operating system in use and the location of this file, the directory path for it may vary, but the file required for installation of this plugin should be entitled **"drc*xxxx*.npk"** (where "***xxxx***" represents the software platform and version number).

Important: If using the NetVault: Backup APM Installation CD to install a plugin to a UNIX-based operating system, it may first be necessary to mount the CD-ROM drive in order to access the disk. See the relevant operating system's documentation for instructions on how to accomplish this. This also applies to accessing files for other procedures required for installation of the **VaultDR System** plugins.

4. Once the installation has completed, a successful installation message will appear in the **Install Software** dialog. This completes the process, and the plugin is now ready for use.

4.1.2 Adding VaultDR Online Plugin Clients

Once the **VaultDR Server** successfully installed on the NetVault: Backup Server, the next step is to add the client machines that are to be backed up using the **VaultDR Online Plugin**. This is accomplished via the **Client Management** window of the NetVault: Backup GUI on the NetVault: Backup Server. For complete details on the use of this window to add Clients to the NetVault: Backup Server, see the *NetVault®: Backup Administrator's Guide*.

With the desired Clients added, the **VaultDR Online Plugin** can be installed remotely from the NetVault: Backup Server.

4.1.3 Installing the VaultDR Online Plugin for Windows

The **VaultDR Online Plugin** must be installed on each NetVault Client from which **VaultDR Online** functionality is desired (i.e., if attempting to conduct a **VaultDR Online** backup of a remote NetVault Client, this plugin software ***must be*** installed on that Client).

4.1.3.a Step 1: Prerequisites

Before installing the **VaultDR Online Plugin**, make sure that the following requirements have been met:

- At least the ***Client*** version of the NetVault: Backup software must be installed.
- The Client machine (the target of the backup/restore) must be running a supported Windows platform. For details on the Windows platforms supported by the VaultDR Online Plugin, refer to the *NetVault: Backup Supported APMs and Plugins* document on the BakBone website:

  http://www.bakbone.com/documentation

- Approximately 10–20% of the hard disk drive's space must remain free and available for use.
- The **VaultDR Server** must be installed on the NetVault: Backup Server.
- The system to serve as the VaultDR Client must have been added to the NetVault: Backup Server via the **Client Management** window (as explained in *Adding VaultDR Online Plugin Clients* on page 59).

4.1.3.b Step 2: VaultDR Online Plugin Installation Procedure

The **VaultDR Online Plugin** must be installed on the Client machine that is to be protected. To install this plugin, perform the following steps.

1. From the machine acting as the NetVault: Backup Server, open the **Client Management** window by clicking the **Client Management** button on the NetVault: Backup GUI (or select **Client Management** from the **Administration** pull-down menu).
2. Locate the desired Client in the list displayed in the **Clients** frame (i.e., one of the Clients added in *Adding VaultDR Online Plugin Clients* on page 59). Right-click on that Client and select **Install Software** from the pop-up menu.
3. Navigate to the location of the **".npk"** installation file (e.g., the NetVault: Backup APM Installation CD or the directory housing the binary installation file). Select the file (e.g., **drw*xxxx*.npk**) and click **Open** and the installation process will begin.
4. Once the installation has completed, a successful installation message will appear in the **Install Software** dialog.

Important: All versions of the VaultDR Online Plugin for Windows now support VSS, except Windows 2000. If you are running VaultDR Online Plugin for Windows on a Windows 2000 system, you must install the **NetVault: Backup Open File Manager (OFM) Plugin** separately. For details, refer to the *NetVault®: Backup User's Guide for the Open File Manager Plugin*.

It is important to note the following:

- The most recently installed version of either the VaultDR Online Plugin for Windows or the OFM Plugin determines the version of the components in use by both during backup operations. Therefore, if you are running the OFM Plugin, it is recommended that *both* plugins be updated to the most recent version available in order to avoid any potential conflicts.

4.1.4 Upgrading VaultDR Online Plugin for Windows

The steps required to upgrade VaultDR Online Plugin for Windows vary depending on the version of Windows running on the target client. Follow the procedure below for the given version of Windows.

4.1.4.a Upgrading VaultDR Online Plugin on Windows 2000

VaultDR Online Plugin for Windows 2000 uses the Open File Manager (OFM) Plugin. If you have a previous version of the VaultDR Online Plugin installed, the OFM driver is already present.

To upgrade VaultDR Online Plugin on Windows 2000, perform the following steps:

1. Uninstall the previous version of VaultDR Online Plugin for Windows. For details on uninstalling the VaultDR Online Plugin, refer to *Removing the VaultDR Server and Online Plugins* on page 62.
2. Install VaultDR Online Plugin for Windows 3.x. For details on installing the Online Plugin, refer to *Installing the VaultDR Online Plugin for Windows* on page 59.

Note: The previous OFM driver will remain on the machine and will be listed under **Backup Options**.

Important: VaultDR Online Plugin for Windows v3.x uses OFM for Windows 2000 only. The v3.x plugin does not include OFM. If you install VaultDR Online Plugin for Windows v3.x on a Windows 2000 machine, the OFM Plugin must be installed separately.

4.1.4.b Upgrading VaultDR Online Plugin on Windows 2003 and Later

To upgrade VaultDR Online Plugin on Windows 2003 and above, perform the following steps:

1. Uninstall the previous version of VaultDR Online Plugin for Windows. For details on uninstalling the VaultDR Online Plugin, refer to *Removing the VaultDR Server and Online Plugins* on page 62.
2. Install VaultDR Online Plugin for Windows. For details on installing the Online Plugin, refer to *Installing the VaultDR Online Plugin for Windows* on page 59.

Note: When upgrading from VaultDR Online Plugin 2.3 or earlier, the OFM driver will remain on the machine but it will not be used or listed under **Backup Options**. VSS is the only supported driver for Windows 2003 and later.

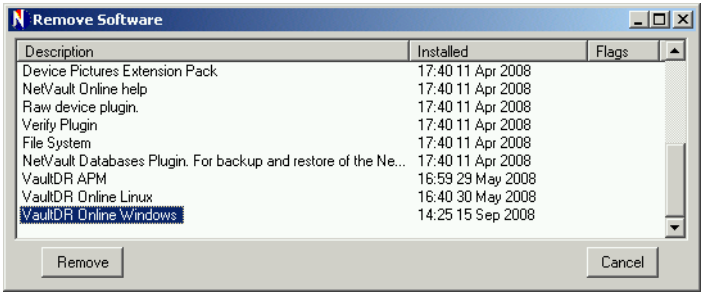
Important: Backup jobs created in previous versions of VaultDR Online Plugin for Windows are incompatible with VaultDR Online Plugin for Windows 3.0. After upgrading to version 3.0, the user must recreate old backup jobs.

4.1.5 Removing the VaultDR Server and Online Plugins

Follow the procedure below to remove the online or offline Plugin.

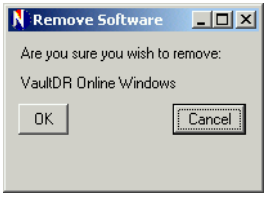
1. Access the **Client Management** window of NetVault: Backup.
2. Right-click on the NetVault: Backup Server or the appropriate NetVault Client in the **Clients** list to reveal the pop-up menu and select **Remove Software**.

Figure 4-2: *The **Remove Software** dialog*



3. Select the desired Plugin for removal (e.g., **VaultDR Online Windows**) from the displayed list and click the **Remove** button.
4. A dialog will appear asking for confirmation. Click **OK** to proceed (or **Cancel** to abort). Clicking **OK** results in the removal of the software, and a confirmation message will appear. Click **OK** to close this dialog and return to the **Client Management** window.

Figure 4-3: *The **Remove Software** confirmation dialog*



4.1.5.a Post-Removal Procedure (Windows 2000 ONLY)

Once the **VaultDR Online Plugin** has been removed, various components that were installed to the current system still exist. These files can be removed as desired using the manual process detailed in the steps below:

1. With the NetVault: Backup GUI closed, navigate to the directory:

   ...\netvault\util

2. In this directory, locate the file entitled **setuplv.exe** and double-click on it to run it.
3. A command prompt window will launch, offering the user the following commands:
   - **(I)nstall**
   - (**U)ninstall**
   - **(C)ancel**
4. At the prompt input **"U"** (for **(U)ninstall**) and press **Enter**.
5. The uninstallation process will now run and the command prompt window will automatically close upon completion.

Important: NetVault: Backup's **Open File Manager (OFM) Plugin** for Windows operating systems shares use of the components that are installed by the **Setuplv.exe** file with the **VaultDR Online Plugin**. If both OFM and VaultDR Online Plugin for Windows are installed on the same machine and the **VaultDR Online Plugin** is removed, these components ***must remain*** in order to continue using the **OFM Plugin**.

4.2.0 Configuration

The second phase of setting up the **VaultDR Server** involves environment configuration. This configuration process can be broken down into two basic steps:

- **Phase 1: Creating a VaultOS Boot System**
- **Phase 2: Configuring VaultDR Server on the NetVault: Backup Server**

The sections that follow fully illustrate the procedures that must be followed to complete both of these steps.

Note: The only configurations required apply to the use of the **VaultDR Server**. There are no configuration requirements necessary with the **VaultDR Online Plugin** (and there are no configuration options available).

4.2.1 Phase 1: Creating a VaultOS Boot System

The initial backup requirement with the **VaultDR Server**, as well as all restore operations require the use of the VaultOS Boot System to boot the target VaultDR Client. This minimal operating system loads to a target machine's memory, rather than to its hard drive. This leaves the hard drive(s) inactive (offline) and in a suitable state for backup or restore.

The **VaultOS** operating system is created on a writable CD. The following section documents the creation procedure.

4.2.1.a Installing VaultOS on a Writable CD

The **VaultDR Server** allows you to create a bootable CD-ROM that can be used to prepare a Client machine for the restore process. This procedure can be performed on any machine that meets the requirements listed below.

Requirements

The following items are required for this procedure:

- **Installation ISO Image** (i.e., either from the NetVault: Backup APM Installation CD or obtained via download).
- **A writable CD-ROM Drive**
- **A blank CD-ROM**
- **CD Generation Software**

Creation Procedure (All O/S Platforms)

Important: It is recommended that all applications running on the machine performing this operation be shut down before starting this procedure.

1. Based on installation type (i.e., from an installation CD or from a downloaded file), navigate to the following directory:

   ...\<Operating System>\vaultdr\vaultos

2. Locate the CD image file entitled **vaultos_x86_v*xxx*.iso** where ***xxx*** indicates the VaultOS software version. If using an installation CD, copy it to the machine's local hard drive. Otherwise, simply note the directory path to this file.
3. Insert a blank CD-ROM in the writable drive.
4. Create a new CD with the CD generation software using the **vaultos_x86_v*xxx*.iso** file. For details on this procedure, see the relevant documentation for the CD generation software in use.

4.2.2 Phase 2: Configuring the VaultDR Server

Before performing the required initial backup with the **VaultDR Server**, it must be configured on the NetVault: Backup Server.

4.2.2.a Adding a VaultDR Client to the VaultDR Server

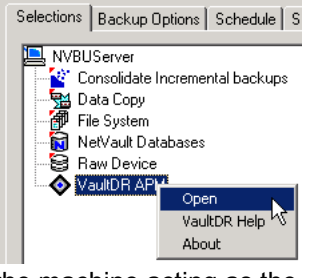


Figure 4-4: *Opening the VaultDR Server on the NetVault: Backup Server*

In order to properly access a VaultDR Client machine for backup and restore, you must add it to the **VaultDR Server**. Follow the steps below to accomplish this.

1. Access the **Backup** window by clicking on either of the **Backup** button in the either of the command toolbars available in the NetVault: Backup GUI (or select **Backup** from the **Operations** pull-down menu).
2. In the Selections tab of the Backup window, locate the machine acting as the NetVault: Backup Server (i.e., the machine with the **VaultDR Server** installed) and open it by double-clicking on it.
3. Locate the **VaultDR Server** in the list of available APM/plugins revealed (i.e., labeled as the **"VaultDR APM"**) and open it by double-clicking on it (or right-click on it and select **Open** from the pop-up menu).
4. With the first launching of the plugin, the **Open** command will reveal the **Add VaultDR Client** dialog. The following fields must be input in order to add a **VaultDR Client**:

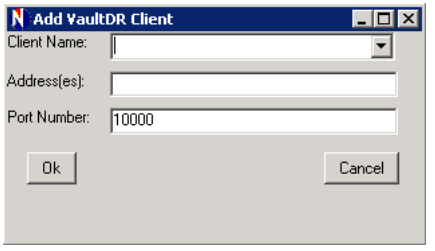


*Figure 4-5: The **Add VaultDR Client** dialog*

- **Name –** The name of the desired VaultDR Client. NetVault will scan the network looking for any available systems that can be added as a VaultDR Client, and reveal them for selection from this drop-down menu.

Important: The Client **Name** must be the VaultDR client name exactly as it appears on the VaultDR client machine. If the **Name** is not exactly the same, Restore jobs may fail.

- **Address(es) –** A comma-separated list of addresses that can either be IP addresses or resolvable network names (e.g., 10.55.55.1, Server_1, 10.55.55.2, etc.) that refer to the machine to be added.
- **Port Number** – The port used to invoke **drdaemon** (e.g., 15555). The default value is 10000.

Important: If you specify a port number other than the default 10000, you will have to manually enter the new port number when you boot the VaultDR Client. For details, see step 17 on page 72.

Adding Additional VaultDR Clients

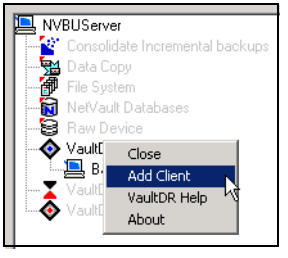


*Figure 4-6: Right-click to access the **Add Client** command.*

Once an initial **VaultDR Client** has been added to the NetVault: Backup Server, it is necessary to use the procedure detailed below to add additional Clients.

1. Launch the **Backup** window and double-click on the NetVault: Backup Server (with the **VaultDR Server** installed on it) to open it.
2. Double-click on the **VaultDR Server** to open it.
3. Right-click on the plugin and select **Add Client** from the pop-up menu. The **Add VaultDR Client** dialog launches.
4. Input values in the fields of the dialog as explained above in **Step 4** of the section *Adding VaultDR Clients to the NetVault: Backup Server (***VaultDR Server** *ONLY)*.
5. Repeat these steps as required until all **VaultDR Clients** have been added.

Editing an Existing VaultDR Client

With a **VaultDR Client** added to the NetVault: Backup Server, the settings made during the original addition process can be edited, if necessary. To accomplish this, follow the steps outlined below:

1. From the **Selections** tab, with the **VaultDR APM** icon open to reveal the desired client, right-click on it to access its associated pop-up menu and select **Edit Client**.
2. The **Edit Client** dialog appears, containing the following fields:
   - **VaultDR Client Name** – This field contains the previously set name for the selected client. Change this value as desired. If changed, this is how this VaultDR Client will be revealed in NetVault: Backup.
   - **IP Address** – This field will contain the IP address originally set for this client. It is possible to change this value completely, or add additional addresses, each separated with a comma.
   - **Port Number** – The port used to invoke **drdaemon** (e.g., 15555). The default value is 10000.

Important: If you specify a port number other than the default 10000, you will have to manually enter the new port number when you boot the VaultDR Client. For details, see step 17 on page 72.

3. With the desired new values input, click **OK** to close this dialog and commit the changes.

Removing an Existing VaultDR Client

If it is necessary to remove a previously added **VaultDR Client** from the NetVault: Backup Server, follow the steps outlined below:

1. From the **Selections** tab, with the **VaultDR APM** icon open to reveal the desired **VaultDR Client**, right-click on it to access its associated pop-up menu and select **Remove Client**.
2. A dialog will launch asking for confirmation of the removal command. Click **Yes** to remove it (or **No** to abort).

4.2.2.b The 'About' Pop-up Menu Item

Also available from the pop-up menu for both the **VaultDR Server** and **VaultDR Online Plugin** is the **About** command. This command can be accessed in order to give version information for the currently installed plugin. To access this command, right-click on the plugin and select **About** from the pop-up menu. Click **OK** to close it and return to the **Backup** window.

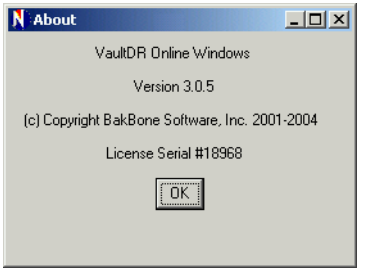


Figure 4-7: *The **About** dialog*

4.3.0 Booting a VaultDR Client with VaultOS

When performing backups using the **VaultDR Online Plugin**, a target VaultDR Client can be active and currently in use by an end user (i.e., ***online***). However, various operations associated with the **VaultDR Online Plugin** require that the target VaultDR Client be taken ***offline*** and made completely accessible to the NetVault: Backup Server. This includes the following two operations:

- **Verifying Access to the VaultDR Server**
- **All Restore Operations**

To bring a target DR system to this offline state, the **VaultOS** operating system is used to load a minimal operating system to a target VaultDR Client's memory. The **VaultOS** boot process entails the configuration of network equipment installed on the target VaultDR Client (i.e., loading driver software for the system's NIC/SCSI card to memory in order to use the device and access the system). This boot process varies based on the version of **VaultOS** in use:

4.3.1 Booting with VaultOS

This process entails the configuration of network equipment installed on the target VaultDR Client (i.e., loading driver software for the system's NIC/SCSI card to memory in order to use the device and access the system).

The overall boot process with **VaultOS** can be broken down into two phases:

- **Phase 1: Gather VaultDR Client Network Information**
- **Phase 2: Boot the VaultDR Client with VaultOS**

Important: Before beginning this procedure, it is necessary to verify the boot order of the target VaultDR Client. The machine's ***CD-ROM Drive*** must be the first source of a boot for this process to work.

4.3.1.a Phase 1: Gather VaultDR Client Network Information

In this first phase of the process, you must gather specific network-related information from the VaultDR Client for use in the boot process (e.g., NIC and SCSI interface values). This includes the following values:

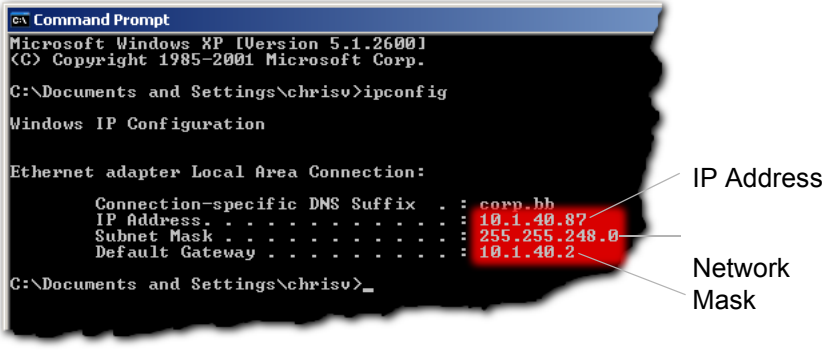
- **IP Address**
- **Network Mask**
- **Gateway**

Important: If the target VaultDR Client is configured with multiple NIC/SCSI devices for access, it is recommended that you gather the above information for ***each device***. The **VaultOS** boot process will recognize ***all*** of these device and request that you configure each of them individually, with this information (but only one of the devices actually needs to be successfully configured for use).

The steps that follow can be used to obtain all of these network values:

1. Log in locally to the Windows VaultDR Client and launch a Command Prompt session.
2. At the prompt, type the following command at the prompt:

   ```
   ipconfig
   ```
3. In the content that is revealed, locate and record the **IP Address**, **Subnet Mask** (**Network Mask)** and **Default Gateway** values.



4.3.1.b Phase 2: Booting the VaultDR Client with VaultOS

With all relevant networking information noted, it is now possible to boot the target VaultDR Client. Follow the steps below to accomplish this.

1. Power down the VaultDR Client and insert the **VaultOS** CD.
2. Upon reboot, there will be a 60 second delay after the boot prompt appears. Press **Enter** to start the sequence immediately.

   A series of dialogs will launch as various applications are loaded to system memory.

Note: The initial load sequence may take several minutes, during which time the screen may appear blank.

Important: This process will only successfully continue if **VaultOS** can locate the appropriate NIC/SCSI driver components for the networking hardware available on the VaultDR Client. If no drivers can be found, you must manually load device drivers for the VaultDR Client.

3. The **Setup Networking** dialog launches first. Highlight the **Yes** button (using either the **Arrow** keys or the **Tab** key) and press **Enter** to begin.

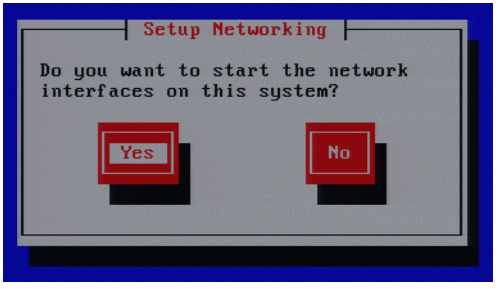


Figure 4-8: *The **Setup Networking** dialog*

The **Network Configuration** dialog appears for all NIC/SCSI devices on the VaultDR Client machine.

4. If multiple NIC cards are present in the client machine, the following dialog appears. Highlight the NIC card to be configured and select **Edit**.

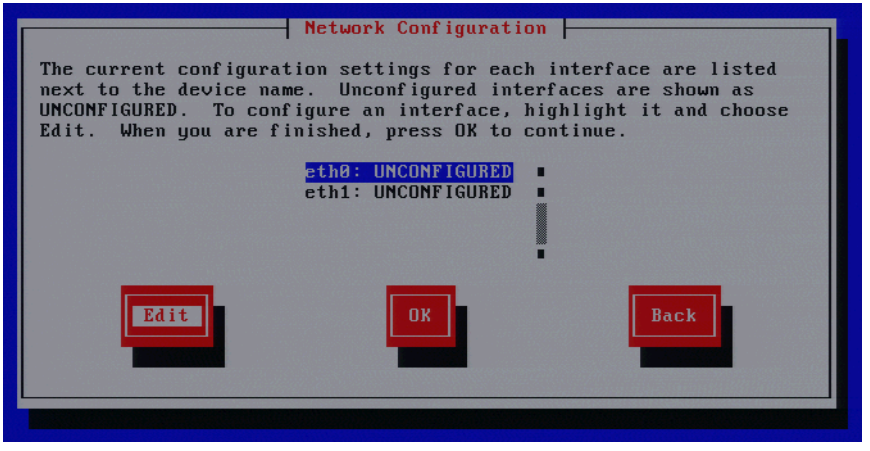


Figure 4-9: *The Network Configuration dialog*

5. If only one NIC card is present in the client machine, the following dialog appears. Select **Yes** to configure the network interface.

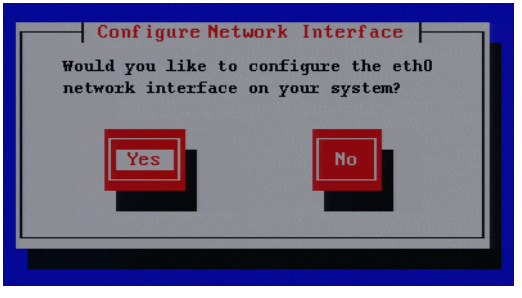


Figure 4-10: *The Configure Network Interface dialog*

6. The **Network Configuration for <Device Name>** dialog appears for the selected device. Press the **Spacebar** to enable **IPv4 support**. Use the **Tab** key to highlight the **OK** button and press **Enter** to continue.

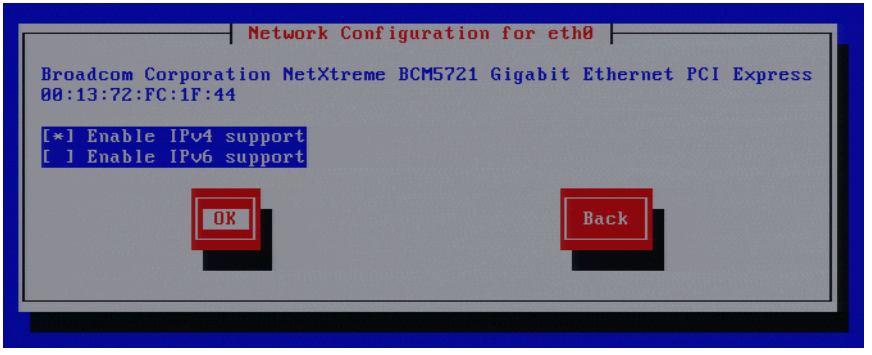


Figure 4-11: *The Network Configuration for eth0 dialog*

7. Use the **Tab** key to highlight **Manual address configuration** and press the **Spacebar** to enable the Manual address configuration.
8. Press the **Tab** key to place the cursor in the **IP Address** field, and input this value (as recorded during *Phase 1: Gather VaultDR Client Network Information* on page 67).

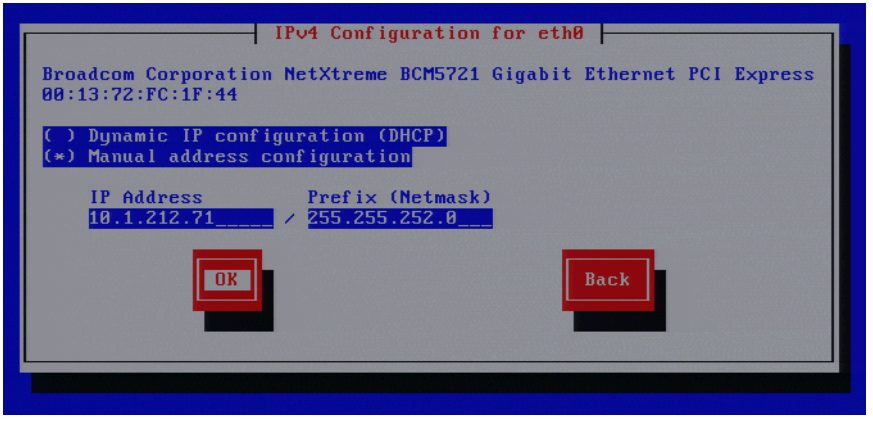
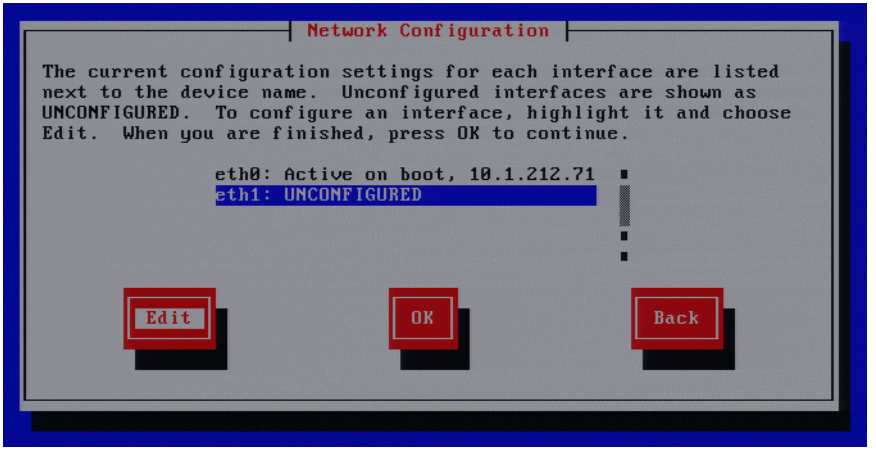


Figure 4-12: *The IPv4 Configuration for eth0 dialog*

9. Press the **Tab** key again to access the **Netmask** field and input the appropriate **Network Mask** (as recorded during *Phase 1: Gather VaultDR Client Network Information* on page 67).
10. Use the **Tab** key to highlight the **OK** button and press **Enter** to continue.
11. If an additional NIC/SCSI card exists on the target VaultDR Client, select the appropriate device from the **Network Configuration** dialog. Repeat **Steps 4–9** to configure the device for use.

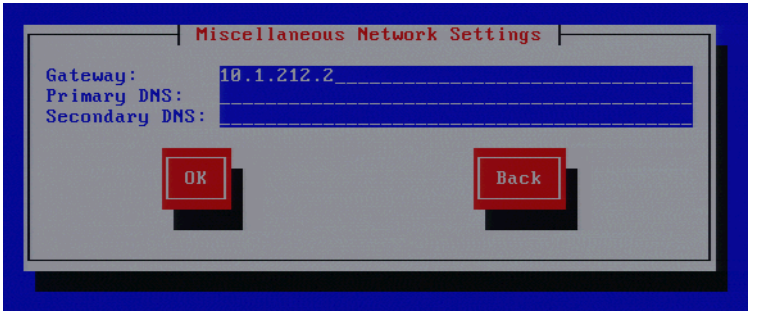
Figure 4-13: The Network Configuration dialog



Important: If you do not wish to configure additional NIC/SCSI devices, this process can be skipped. However, you must ensure that the device is unconfigured.

12. Use the **Tab** key to highlight the **OK** button and press **Enter** to continue.
13. The **Miscellaneous Network Settings** dialog is launched. Use the **Tab** key to highlight the first field **"Gateway"** and input the appropriate value (as recorded during *Phase 1: Gather VaultDR Client Network Information* on page 67).

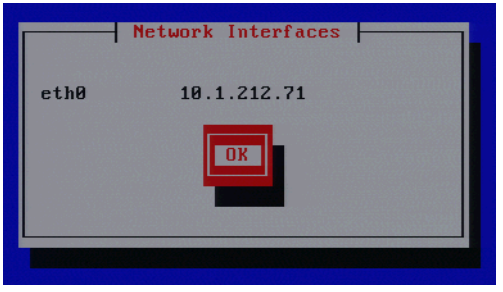
Figure 4-14: The Miscellaneous Network Settings dialog



14. Use the **Tab** key to skip through the two **DNS-related** fields and highlight the **OK** button. Press **Enter** to continue.

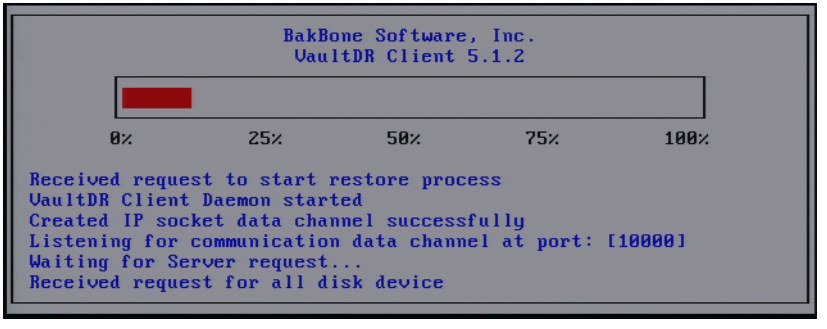
15. The **Network Interfaces** dialog appears. Select the **OK** button.

Figure 4-15: *The **Network Interfaces** dialog*



16. After clicking **OK**, the **VaultDR Daemon** dialog will launch automatically, awaiting commands from the NetVault: Backup Server. The Client is now prepared for backup or restore.

Figure 4-16: *The **VaultDR Daemon** dialog*



17. If you configured VaultDR to use a port other than the default “10000” as shown in *The Add VaultDR Client dialog* on page 65, you must exit from the **VaultDR Daemon** dialog and enter the new port number manually.
    a. To exit the **VaultDR Daemon** dialog, press **<Ctrl-C>**.
    b. At the command prompt, type the following command and press **Enter**:

    ```
    drdaemon -p port_number
    ```

    where *port_number* is the port you specified.

Note: If you wish to relaunch **VaultDR Daemon** from the command prompt without changing the port number, type “**drdaemon**” and press **Enter**.

4.4.0 Backing Up Data

Backups of a target VaultDR Client are broken down into a two part-process:

- **Phase 1: Prerequisites**
- **Phase 2: Backup with the VaultDR Online Plugin**

The sections that follow illustrate all of the steps used to perform both phases of the **VaultDR Online Plugin** backup process.

4.4.1 Phase 1: Prerequisites

This section documents any prerequisite procedures that must be followed, prior to performing a backup with the **VaultDR Online Plugin**.

The following limitations apply to backups performed with the VaultDR Online Plugin for Windows:

- The **VaultDR Online Plugin** only supports 15 partitions on Windows SCSI based installs and 63 partitions on IDE devices. Backup attempts on such machines using VaultDR Online Plugin will result in non-recoverable images.
- Backup of Dynamic Disks is not supported.
- If the space allocated for shadow copies on the volume is insufficient, the oldest persistent shadow copy may be lost when you perform a backup. For information about shadow copies and how they are implemented, refer to the MSDN Library page here:

  http://msdn.microsoft.com/en-us/library/bb968832(VS.85).aspx

  For instructions on allocating space for shadow copies, see the following TechNet article:

  http://technet.microsoft.com/en-us/library/cc786104.aspx

4.4.1.a Step 1: Verify Access to the VaultDR Server

Prior to using the **VaultDR Online Plugin** to perform active backups of a target VaultDR Client, you must first verify that the VaultDR Client is bootable with VaultOS, and that it is accessible to the **VaultDR Server**. This procedure is performed to ensure that the target VaultDR Client will be accessible at restore time. Note the following:

- Failure to perform this verification process, may result in the inability to restore backups taken with the **VaultDR Online Plugin**.
- This procedure only needs to be performed ***once*** for a target VaultDR Client, unless its networking hardware is changed at a later date. If this is the case, you will need to perform these procedures again.
- This procedure must be performed for each VaultDR Client that is to be backed up with the **VaultDR Online Plugin**.

Part 1: Boot the VaultDR Client with VaultOS

It is first necessary to boot the target VaultDR Client with the **VaultOS** operating system to prepare it for the backup. Review all of the steps covered in the section, *Booting a VaultDR Client with VaultOS* on page 67 to accomplish this.

Part 2: Verify Access to the VaultDR Client

1. After you have booted the VaultDR Client using VaultOS (as outlined in the section, *Booting a VaultDR Client with VaultOS* on page 67), access the NetVault: Backup Server and launch the NetVault: Backup GUI.
2. Access the **Backup** window and double-click on the NetVault: Backup Server to open it (i.e., the system containing the **VaultDR Server**).
3. Open the **VaultDR Server** by double-clicking on it.
4. Locate the appropriate VaultDR Client displayed under the plugin and double-click on it to open it. One of two results will occur:
   - **System Disk(s) will be Revealed** – If selectable disks are revealed, you have verified that the VaultDR Client is accessible.
   - **An Error Message is Revealed** – If a dialog displays stating **"Failed to connect to client"**, the VaultDR Client is not accessible. This can be for any number of reasons. The most common reason is that the networking hardware was not properly configured during boot of the VaultDR Client with **VaultOS**. Reboot the target VaultDR Client with VaultOS, using instructions illustrated in the section, *Booting a VaultDR Client with VaultOS* on page 67, and ensure that the proper network-related values are used.

4.4.1.b Step 2: Verify Disk Geometry and Device Size

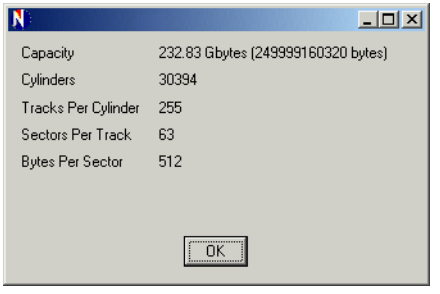
The **VaultDR Online Plugin** makes it possible to view the disk geometry and partition information of a selected system. It is recommended that these items be noted before a system is backed up with the **VaultDR Online Plugin**. When restoring previously backed up data, if this is not taken into account, a restore could fail. Dialog boxes containing this information can be accessed as follows:

Accessing the Disk Geometry Dialog Box

1. From the NetVault: Backup Server, launch NetVault: Backup and access the **Backup** window.
2. In the **Backup** window, double-click on the Client (containing the **VaultDR Online Plugin**) in order to open it.
3. Open the **VaultDR Online Plugin** by double-clicking on it.
4. Select the appropriate Client displayed under the plugin and double-click on it to reveal the disk(s) contained within.

5. To determine the disk geometry of a specific disk, right-click on it and select **Disk Geometry** from the pop-up menu. This dialog will show size and quantity for various items pertaining to the selected disk:
   - **Capacity**
   - **Cylinders**
   - **Tracks Per Cylinder**
   - **Sectors Per Track**
   - **Bytes Per Sector**
6. With sufficient information noted, click **OK** to close this dialog.

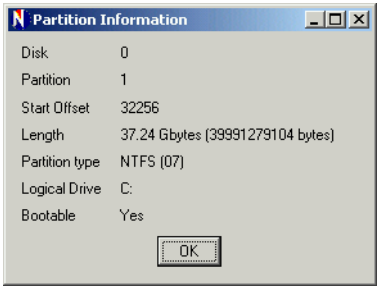
*Figure 4-17: The **Disk Geometry** dialog*



Accessing the Partition Information Dialog Box

1. Follow **Steps 1–4**, as described in the section *Accessing the Disk Geometry Dialog Box, above*.
2. With the disk(s) revealed, double-click on a selected disk to open it (or right-click on it and select **Open** from the pop-up menu).
3. Detailed information can be gathered about a displayed partition by right-clicking on it and selecting **Partition Info** from the pop-up menu. From the dialog that launches, various items of information can be gathered:
   - **Disk Number**
   - **Partition Number**
   - **Start Offset Point**
   - **Length of the Selected Partition**
   - **Partition Type**
   - **Logical Drive Label** (e.g., **"C:"**, **"D:"**)
   - **Boot Status** (e.g., **"Yes"** or **"No"**, indicating whether it is possible to boot from this partition or not)
4. With sufficient information noted, click **OK** to close this dialog.

*Figure 4-18: The **Partition Information** dialog*



4.4.2 Phase 2: Backup with the VaultDR Online Plugin

As noted in previous sections, the **VaultDR Online Plugin** makes it possible to backup full systems as well as individual partitions contained within that system, while they remain online and active.

Note the following important points:

- Attempts to perform a VaultDR Online Plugin backup of a system whose hard disk is full or nearly full, may fail. The plugin requires a portion of the local system's hard disk to synchronize data. If enough free space is not available for this synchronization of data, the backup will fail.
- On Windows 2003 clients and later, two backup snapshots cannot be taken at the same time (e.g., if you launch simultaneous backups on two clients from the same server). Shadow copy creation is serialized. This is a known limitation of Volume Shadow Copy Service (VSS).
- The **Master Boot Record** (MBR) and the **Partition Table** items are backed up automatically when a partition (all or individual) is backed up with this plugin.

The sections below detail the processes necessary to complete a successful backup with the **VaultDR Online Plugin**.

1. From the NetVault: Backup Server, access the **Backup** window from the NetVault: Backup GUI (via the **Backup** button or by selecting the **Backup** command from the **Operations** pull-down menu).
2. From the **Backup** window, double-click on the desired Client to be backed up (e.g., the Client machine on which the **VaultDR Online Plugin** is installed).
3. Open the **VaultDR Online Plugin** by double-clicking on it. The hard disk(s) located on the Client system will be revealed. In order to select the entire disk for a backup, click the box to the left of the disk title.
4. A disk can be opened by double-clicking on it. Individual partitions will be displayed and made available for selection. Various information in regards to each partition will be displayed (e.g., the partition number; the drive letter assigned — C:, D:; and the file system — NTFS, HPFS, etc.).
5. Select desired items for a backup. Selected items will contain a green check, deselected items will be blank, and omitted items will contain a red cross.

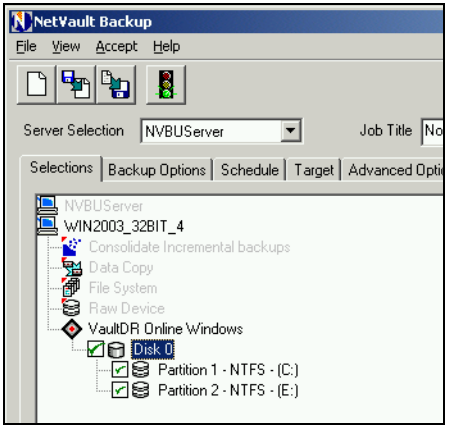


Figure 4-19: *The VaultDR Online Plugin opened with items selected for a backup*

6. Select the **Backup Options** tab to set these options as required. This tab contains the Backup Options parameters, which are described below.
   - **Windows 2000 Only** – On Windows 2000 clients, the following Backup Options are available:

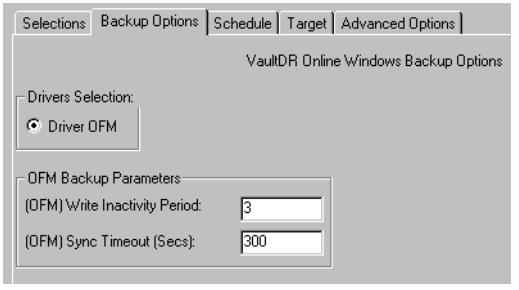


*Figure 4-20: The **Backup Options** tab for Windows 2000 Clients*

- **Driver OFM** – The Open File Manager Plugin (OFM) is the only available backup driver for Windows 2000 clients. No other driver can be used. The **Driver OFM** radio button is selected by default.
- **(OFM) Write Inactivity Period** – In order for this plugin to safely allow for the backup of open files, it uses the **Write Inactivity Period** to determine when the system is in a safe state. This period is set to 3 seconds by default. The **VaultDR Online Plugin** will wait until it sees no write activity for the specified time before determining if it is safe to begin the backup of the system. The Plugin will continually attempt to establish this **Write Inactivity Period** until the time set as the **Sync Timeout (Secs)** has elapsed.

Important: The **VaultDR Online Plugin** uses a default setting of three seconds for the **Write Inactivity Period**. Note that this parameter can be set to less than three seconds, but a minimum of three seconds is recommended.

- **(OFM) Sync Timeout (Secs)** – The **VaultDR Online Plugin** uses this setting to determine when to stop synchronizing the system. If, for example, the **Sync Timeout** is set to 300 seconds (five minutes), the **VaultDR Online Plugin** will try for 300 seconds to find a time during which the **Write Inactivity Period** requirement is met. Note that this may take much longer than 300 seconds. The **Sync Timeout** will vary depending on the DISK I/O load on a volume.

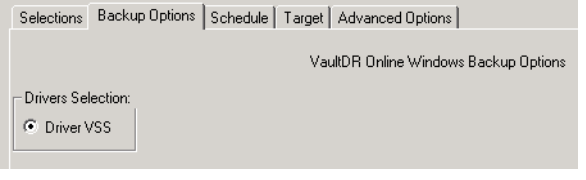


*Figure 4-21: The **Backup Options** tab for Windows 2003 and Later*

- **Windows 2003 and Later** – Windows 2003 and later clients use Volume Shadow Copy Service (VSS), a service that coordinates various components to create consistent shadow copies of one or more volumes. It is the only available backup driver for Windows 2003 and above. There are no user configurable backup options available with VSS. The VSS radio button is selected by default.

7. The remaining tab selections (e.g., **Schedule**, **Target** and **Advanced Options**) offer additional options that can be set as desired. The options available in these tabs are not specific to the **VaultDR Online Plugin**. For more information, refer to the relevant chapters of the *NetVault®: Backup Administrator's Guide*.

8. Enter a name for the job in the **Job Title** box. It is highly recommended that a name be assigned that will differentiate this job from any others performed with this plugin. This will allow for easier recognition of the job during restore.
9. Submit the backup job by clicking the **Submit** button on the command toolbar.
10. The GUI on the NetVault: Backup Server can be used to monitor the job in regards to its progress and job log entries (i.e., via the **Job Management** and **NetVault: Backup Logs** dialogs, respectively. For complete details on the use of these dialogs in the NetVault: Backup GUI, see the *NetVault®: Backup Administrator's Guide*).

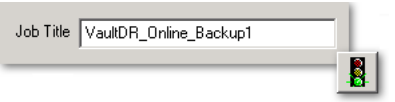


Figure 4-22: *The **Job Title** box*

4.5.0 Restoring Data

The restore of data backed up with the **VaultDR Online Plugin** is handled by the **VaultDR Server** (i.e., backups performed using the **VaultDR Online Plugin** are revealed beneath the **VaultDR Server** node — **"VaultDR APM"** — in the **Selections** window of the NetVault: Backup GUI).

The sections that follow illustrate all of the procedures required to perform a restore of a **VaultDR Online Plugin** backup.

4.5.1 Phase 1: Prerequisites

The restore procedure for a **VaultDR Online Plugin** backup is a delicate operation. Prior to setting up and running a restore, the prerequisites covered in the following sections must be met.

Before continuing to **Step 1** below, note the following limitations:

Bitlocker Volumes

Volumes that are encrypted using Bitlocker on Windows 2008 clients lose encryption upon restore. If you are using Bitlocker, you must re-enable encryption when you restore the machine.

Shadow Copies

Windows uses VSS persistent snapshots to implement shadow copies in Windows 2003/2008. When restored, these shadow copies are not properly recognized by Windows. They can become orphaned and consume disk space.

Microsoft does not recommend backing up shadow copies. However, the VaultDR Online Plugin performs backups at the block level so there is no way to prevent the backup of snapshot files. You must manually delete the snapshot files and re-enable shadow copies on the recovered volume.

For instructions on deleting shadow copies, see the following TechNet article:

http://technet.microsoft.com/en-us/library/cc776119.aspx

For instructions on enabling shadow copies, see the following TechNet article:

http://technet.microsoft.com/en-us/library/cc776483.aspx

In addition, BakBone recommends limiting the amount of space allocated to shadow copies to 300 Mb. This will delete the cache files. Alternatively, disable shadow copies.

For further information on Microsoft's recommended best practices for shadow copies, see the following TechNet article:

http://technet.microsoft.com/en-us/library/cc753975.aspx

Windows Disk Management

Windows 2008 automatically assigns drive letters to new-found partitions following a restore. Windows 2003 does not automatically assign drive letters to new-found partitions. This behavior can be controlled via the **diskpart.exe** command. For further information, refer to the TechNet article located here:

http://technet.microsoft.com/en-us/library/cc773140.aspx

4.5.1.a Step 1: Ensure that Device File Names Match

The target device name on the VaultDR Client (e.g., **"Disk 0 (IDE)"**) ***must be the same*** as it was at the time of backup.

4.5.1.b Step 2: Boot the VaultDR Client with VaultOS

It is first necessary to boot the target VaultDR Client with the VaultOS operating system to prepare it for the restore of a DR image. Perform the steps covered in the section, *Booting a VaultDR Client with VaultOS* on page 67 to accomplish this.

4.5.1.c Step 3: Gather Noted Device Size and Disk Geometry Information

Have the information noted in *Step 2: Verify Disk Geometry and Device Size* on page 74 handy to complete the restore. This helps ensure that you backup the correct data.

4.5.1.d Step 4: Verify Access to the Target VaultDR Client

The VaultDR Client machine that is to serve as a target for the restore must be accessible to the **VaultDR Server**. The section that follows outlines the required steps for this verification.

Note: Although it is not a requirement, BakBone recommends that the target machine for the restore have the same hardware configuration as the original machine.

---

1. With the VaultDR Client booted with **VaultOS**, access the NetVault: Backup Server and launch the NetVault: Backup GUI.
2. Access the ***Backup*** window to verify that the desired Client machine has been added as a **VaultDR Client**. To do this, follow the procedure below:
   a. Open the **VaultDR Server** to reveal any previously added Clients.
   b. Browse the list for the desired **VaultDR Client**. To verify settings for a specific **VaultDR Client**, right-click on the Client name and select **Edit** from the pop-up menu.
   c. The **Edit VaultDR Client** dialog launches. Verify that the data is correct or change it as required.
   d. If the **VaultDR Client** is added properly, continue on to the next section, *Phase 2: Restore Procedure*; otherwise, proceed to the following step.
3. Add the desired **VaultDR Client**. For detailed instructions on this process, see the section *Adding a VaultDR Client to the VaultDR Server* on page 64. Once completed, close the **Backup** window of the **VaultDR Server** and continue on to the *Restore Procedure* section that follows.

4.5.2 Phase 2: Restore Procedure

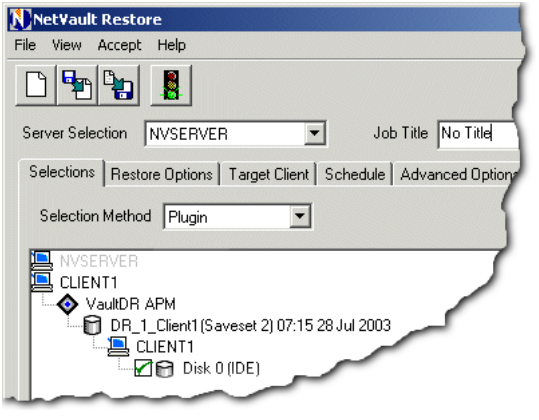


Figure 4-23: *The **Selections** tab of the **Restore** window*

Restoring a **VaultDR Online Plugin** backup is accomplished by performing the following steps.

1. With the VaultDR Client booted with **VaultOS**, access the NetVault: Backup Server and launch the NetVault: Backup GUI.
2. From the NetVault: Backup Server, access the **Restore** window from the NetVault: Backup GUI (by clicking on the **Restore** button or by selecting **Restore** from the **Operations** pull-down menu).
3. In the **Selections** tab of the **Restore** window, completed **VaultDR Online Plugin** backups are displayed from the ***NetVault Client*** that was actually backed up. Locate the desired Client and double-click on it to open it.
4. Restores of **VaultDR Online Plugin** backups are handled by the **VaultDR Server**. Therefore, these backups are revealed beneath the **VaultDR Server** node (i.e., labeled as **"VaultDR APM"**). Locate this node and double-click on it to open it. The backup saveset(s) from previous backup(s) completed with this plugin will be revealed. Double-click on the desired saveset to open it.

5. The backed up VaultDR Client machine will be displayed. Double-click on it to open it and reveal the disk(s) that were backed up.
6. Locate each desired disk, and click in the box to its left to select it for a restore.
7. It is also possible to expand each disk to view its contents. Double-click on the desired disk to open it. With a disk open, individual items can be selected for restore if desired. Selectable items for a restore consist of:
   - **Master Boot Record and System Partition**
   - **Individual Partitions**
8. Select the **Restore Options** tab to access the following:
   - **Recovery Options Frame** – This frame contains the **Restore Name** field. The default value in this field will be the actual system name for the Client machine that was backed up. In order to perform a restore correctly, input the ***NetVault: Backup machine name of the target VaultDR Client***.

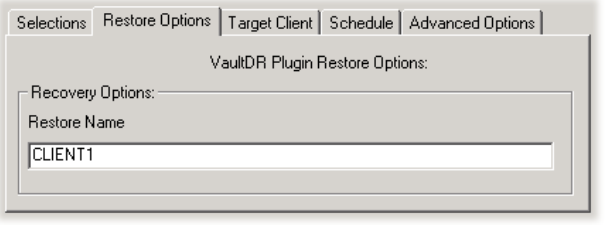


Figure 4-24: *The **Restore Name** field as seen in the **Restore Options** tab*

9. Restores of **VaultDR Online Plugin** backups ***must be*** routed through the NetVault: Backup Server (to utilize the **VaultDR Server** components installed there). Therefore, the **Target Client** tab must be selected. In the dialog that appears, select the NetVault: Backup Server from the list of displayed machines, as the intended target. This setting will work in tandem with the **Restore Name** option set in the **Restore Options** tab to route the restore properly.

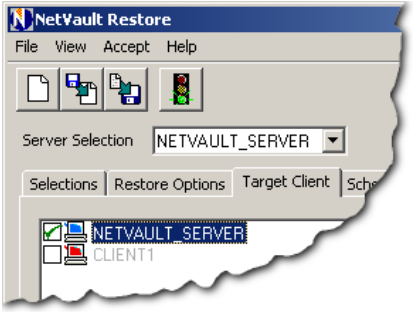


Figure 4-25: *The **Target Client** tab with the NetVault: Backup Server selected*

10. The remaining tab selections in the **Restore** window (e.g., **Schedule** and **Advanced Options**) offer additional options that can be set as desired. The options available are not specific to the **VaultDR System Plugins**. For more information on these options, see the *NetVault®: Backup Administrator's Guide*.
11. Input an appropriate title for the job in the **Job Title** box and begin the job by clicking on the **Submit** button.

Important: When inputting a name in the **Restore Name** field of the **Restore Options** tab, ensure that the value used is the ***NetVault: Backup machine name*** for the target machine, taking case sensitivity into account. The NetVault: Backup machine name can be found in the **NetVault Client Management** window.

Note: As mentioned earlier, it is necessary to route a restore of this type through the NetVault: Backup Server to utilize its locally installed **VaultDR Server** components. This will write all restored data to the machine named in the **Restore Name** field, ***not*** to the NetVault: Backup Server.

Chapter 5:

The VaultDR Online Plugin for Linux

5.0.0 The VaultDR Online Plugin for Linux – An Overview

The **VaultDR Online Plugin for Linux** operating systems is a **Disaster Recovery (DR)** solution capable of backing up and recovering an entire disk including the operating system, applications, system settings, partition information, and data. This version of the plugin makes it possible to backup a full Linux system while it ***remains online and active*** (e.g., perform an ***"online backup"***), thereby allowing system administrators to conduct DR backups while eliminating system down-time for users.

Once the plugin is properly installed and configured, a DR image of a live system can be taken and saved for future recovery in the event of a system failure. During the creation of this DR image, the **VaultDR Online Plugin for Linux** can automatically include ***all*** information pertaining to the networking hardware in use by the target Linux VaultDR Client machine (i.e., driver information files). These files are then compiled into a separate CD creation file (i.e., **".iso"** file format) that can be saved along with the DR image. At the time of recovery, this file is then recovered and used to create a bootable CD-ROM, complete with the necessary driver files that were taken from the Linux VaultDR Client. Using this CD, the Linux VaultDR Client can be successfully booted to a state that will allow for the recovery of the DR image.

5.0.1 Operating Systems Supported with this Plugin

As the title of this plugin states, it supports DR operations for Intel (x86)-based operating systems, including the following:

- **Linux (*ONLY*)**

5.1.0 Installation

This section covers the installation procedures required to successfully install the **VaultDR Online Plugin for Linux** operating systems for use with NetVault: Backup.

5.1.1 Installation Prerequisites

Certain prerequisites must be met before a system administrator can successfully install this plugin. Ensure that all of the following points have been accounted for:

- **VaultDR Online Plugin for Linux Obtained** – via download from BakBone Software's web site or the NetVault: Backup APM installation CD.
- **Separate NetVault: Backup Server Established** – A machine that will not serve as a Linux VaultDR Client must be set up with the ***Server*** version of NetVault: Backup installed and it must have network connectivity to all desired Linux VaultDR Clients.

Important: NetVault: Backup requires that the **VaultDR Online Plugin for Linux** be installed on ***both*** the NetVault: Backup Server ***and*** each desired NetVault: Backup Client. Installation of the plugin is required on the Client machine during backup and on the Server machine during restore. If the NetVault: Backup Server is running an operating system other than Linux, ensure that the correct version of this plugin is available for installation on this O/S. For example, if the NetVault: Backup Server is running Microsoft Windows 2000, the Windows 2000 version of the **VaultDR Online Plugin for Linux** is required for installation on the NetVault: Backup Server, while the Linux-based version of the plugin would be required for installation on all target VaultDR Clients. If both the NetVault: Backup Server and the desired VaultDR Clients are running Linux, only a single version of the plugin is required.

- **Uninstall Previous Version of VaultDR Online Plugin –** If a previous version of the plugin is installed, it must be completely removed before proceeding with the installation. See *Removing the VaultDR Online Plugin for Linux* on page 89 for details.
- **Client Machine Memory Requirement** – All machines that are to serve as VaultDR Clients must have ***at least 128 MB of RAM*** installed.
- **Linux VaultDR Client Machine(s) Configured as NetVault: Backup Client(s)** – All machines that are to serve as Linux VaultDR Clients must have ***at least*** the Client version of NetVault: Backup installed, and each must be successfully added to the NetVault: Backup Server as NetVault: Backup Clients via the **Client Management** window of the NetVault: Backup GUI.

Note: For complete instructions on the processes outlined in the points above (i.e., installing the Server/Client version of NetVault: Backup and adding a machine to the NetVault: Backup Server to serve as a NetVault: Backup Client), see the *NetVault®: Backup Administrator's Guide*.

- **100 MB Free Space on All Target Machines for Plugin Installation** – All machines that the plugin is to be installed on must have 100 MB of free space to accommodate a third party DR boot utility application that is used by this plugin to perform backups and restores.
- **Additional Free Hard Disk Space on Target VaultDR Clients** – This plugin utilizes existing free space on a target VaultDR Client's hard disk to synchronize the backup of currently online files. If a target VaultDR Client's hard disk is full (or nearly full), attempts to perform an online backup may fail.
- **The "mkisofs" Utility Installed and Available on all Linux VaultDR Clients** – NetVault: Backup requires that this component be installed to allow for the creation of ".iso" CD creation files from any potential Linux VaultDR Clients. This component may not be automatically available with all installations of Linux.

The following command can be issued from a terminal session launched from most versions of Linux in order to verify that this component is installed:

rpm -qa | grep mkisofs

In the event that the component ***does not exist*** on an intended Linux VaultDR Client, it can be obtained and installed as follows:

a. Access the following web site:

http://www.rpmfind.net/

b. In the search field present at the top of the page, input **"mkisofs"** and click **Search**.

c. In the list of available files for download, locate the entry specific to the version of Linux running on the intended VaultDR Client and download this file.

d. With this file available on the VaultDR Client (i.e., via copying the file or direct download), open a terminal session and navigate to the location of the file.

e. Input the following command to initiate the installation, and follow the install prompts as they appear:

rpm -i <*installation_file_name*>

- **The "SYSLINUX" Package Installed (SUSE Linux 9.0, ONLY)** – This version of the **VaultDR Online for Linux Plugin** uses a specific boot loader application for the creation of the bootable CD-ROM that is required for the restore procedure. Default installations of SUSE Linux 9.0 do not offer support for this boot loader application. Therefore, the SYSLINUX package must be installed on all VaultDR Client systems running SUSE Linux 9.0. At the time of this publication, this component could be found for download at the following link:

http://syslinux.zytor.com

- **The "vim-6.3.84-2.i586.rpm" Package Installed (SUSE Linux 10, ONLY)** – Backups of SUSE Linux 10 VaultDR Clients will fail, unless this package is installed. At the time of this publication, this package could be obtained from the following link:

http://rpm.pbone.net/index.php3/stat/17/dept/4/idg/Productivity_Editors_Vi

Important: NetVault: Backup's **Encryption Plugin** functionality is not supported for use with this plugin. Ensure that this functionality is ***disabled*** before installing/using the **VaultDR APM**. For details on uninstalling the Encryption Plugin, refer to the *NetVault®: Backup Administrator's Guide*.

5.1.2 Installation Procedure

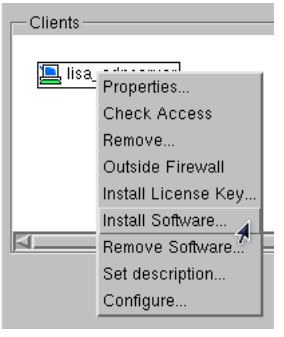
Use the steps below to successfully install the **VaultDR Online Plugin for Linux**.

5.1.2.a Phase 1: Installation on the NetVault: Backup Server

1. From the machine acting as the NetVault: Backup Server, open the NetVault: Backup **Client Management** window by clicking either of the **Client Management** buttons in the NetVault: Backup GUI (or by selecting the **Client Management** command from the **Administration** pull-down menu).

Figure 5-1: The Install Software option

2. In the **Clients** frame, right-click on the machine acting as the NetVault: Backup Server and select the **Install Software** command from the pop-up menu.

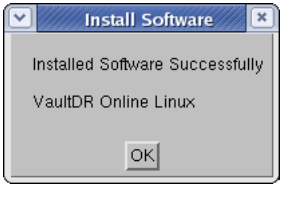


3. In the dialog that appears, navigate to the location of the **".npk"** installation file (i.e., the NetVault: Backup APM installation CD or the directory to which the file was downloaded from BakBone Software's web site) and click on it to select it. In the event that the O/S running on the NetVault: Backup Server is something other than Linux, ensure that the installation file selected is the file ***specific to the O/S in use on the NetVault: Backup Server*** (e.g., if the O/S running on the NetVault: Backup Server were Windows 2000, ***two*** versions of the plugin would be required and it would be necessary to target the Windows 2000 **".npk"** file for installation on the NetVault: Backup Server). With the file selected, click **Open** to begin the installation process.

Important: In the event that the NetVault: Backup Server is running an O/S other than Linux, it is highly recommended that the *NetVault: Backup End User Release Notes* document for each O/S-related version of this plugin be reviewed. This will allow the user to correctly identify by name exactly which plugin installation file is required at each phase of the installation. Based on the operating system in use and the location of this file, the directory path for it may vary, but the file required for installation of this plugin should be entitled **"dr*xxxxx*.npk"** (where **"*xxxx*"** represents various O/S software platforms and the plugin version number).

*Figure 5-2: The **Install Software** confirmation dialog*

4. Once the installation has completed, a successful installation message will appear in the **Install Software** dialog. With this, the plugin has been successfully installed on the NetVault: Backup Server.



5.1.2.b Phase 2: Installation on Each Linux VaultDR Client

1. While still in the **Client Management** window, locate the first of the desired Linux VaultDR Client machines (i.e., the Linux-based Clients previously added to the NetVault: Backup Server as NetVault: Backup Clients).
2. Right-click on this Client and select the **Install Software** command from the pop-up menu.
3. Navigate to the location of the ***Linux-based version*** of the **VaultDR Online Plugin for Linux** installation (**".npk"**) file.
4. Click on the file to select it and click **Open** to initiate the installation process.
5. Upon successful installation of the plugin, a confirmation dialog will display stating such.
6. Repeat **Steps 1–5** for each remaining NetVault: Backup Client that is to be targeted for a Linux-based DR backup.

5.1.2.c Storix Installation

Installation of this plugin on the NetVault: Backup Server and each Linux Client will also create two additional directories on the machine:

- **/storix**
- **/opt/storix**

These directories contain Storix SBAdmin — a third party DR boot utility application that is used by this plugin to perform backups and restores. The data contained within these directories is required by this plugin. Removal of these directories will result in the inability to use the plugin.

When you install the VaultDR Online Plugin for Linux, two additional Storix directories are created – the **Storix Bin** directory and the **Storix Temp** directory. The **Storix Bin** directory is where the Storix software is installed. It is located in "/opt/storix/bin" by default. The **Storix Temp** directory contains the "linuxboot.iso" file after a successful backup. It is located in "/storix/temp" by default. The directory locations can be changed via the NetVault Configurator from the **VaultDR Online Linux** sub-tab on the **Plugin Options** tab.

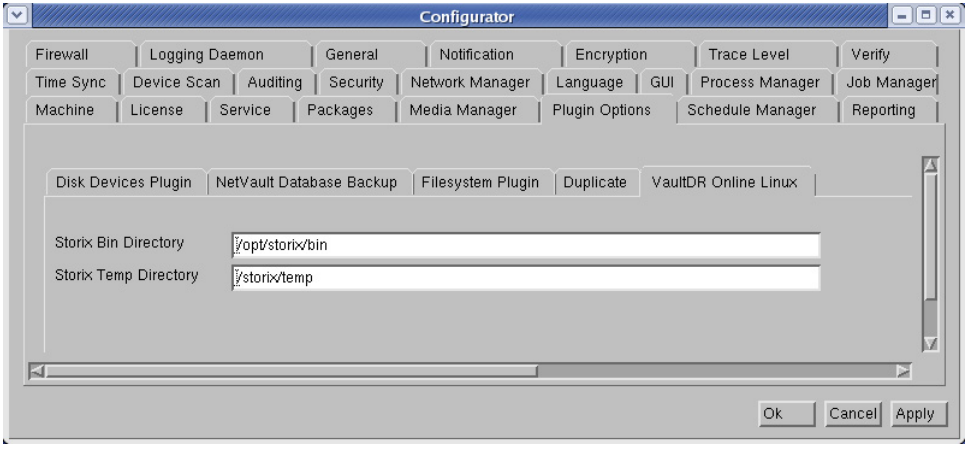


Figure 5-3: *The **Plugin Options** tab in NetVault Configurator*

If you change the location of either or both of the Storix directories, prior to performing a DR backup via the NetVault: Backup GUI, you must configure the new directory path(s).

For example, if you change the **Storix Temp** directory to "/storix/temp222", perform the following steps.

1. On the Linux Client, create the directory where the Boot Image should reside:

   mkdir /storix/temp222

2. Launch NetVault Configurator.
3. Select the **Plugin Options** tab and the **VaultDR Online Linux** sub-tab.
4. Modify the path/name in the **Storix Temp Directory** field. This path/name must be exactly as in step 1.
5. Click **Apply**, then click **Ok**.

5.1.3 Removing the VaultDR Online Plugin for Linux

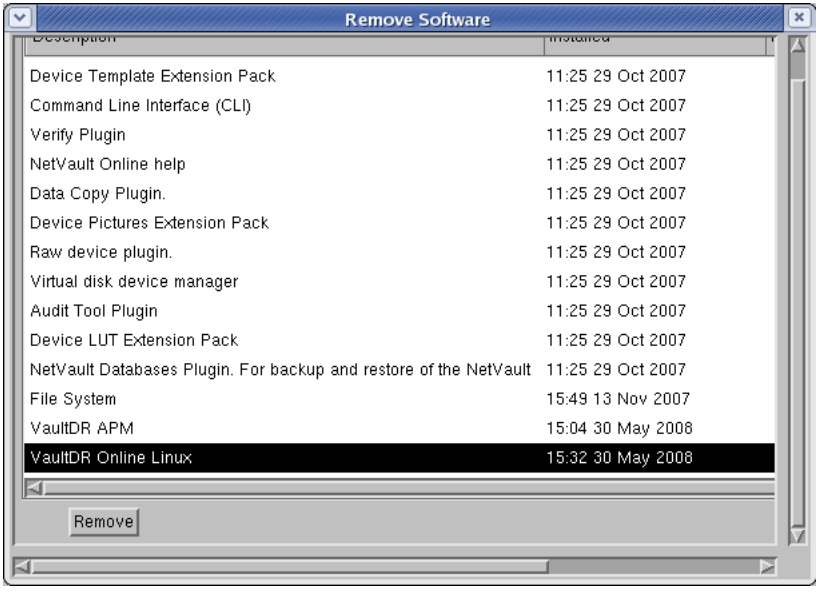
Follow the procedure below to remove this plugin from a target machine.

Important: If you are upgrading the VaultDR Online Plugin from a previous version, you must completely remove the plugin and all associated data. To do so, follow the steps below. If you are removing the plugin from a Linux client, you must also perform the procedure detailed in *Removal of Associated Sub-directories* on page 90.

1. Access the **Client Management** window of NetVault: Backup.
2. Right-click on the desired machine in the displayed list of the **Clients** (i.e., the NetVault: Backup Server or a NetVault: Backup Client with the **VaultDR Online Plugin for Linux** installed). In the pop-up menu that is revealed, select the **Remove Software** command.

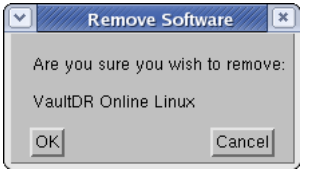
3. In the **Remove Software** dialog that appears, select the desired plugin for removal (e.g., **VaultDR Online Linux)** from the displayed list and click **Remove**.

Figure 5-4: *The **Remove Software** dialog*



4. A dialog will appear asking for confirmation. Click **OK** to proceed (or **Cancel** to abort). Clicking **OK** will result in the removal of the software, and a confirmation message will appear. Click **OK** to close this dialog and return to the **Client Management** window.

Figure 5-5: *The **Remove Software** confirmation dialog*



5.1.3.a Removal of Associated Sub-directories

As outlined in a note in the section *Phase 2: Installation on Each Linux VaultDR Client* on page 88, the installation of this plugin on a Linux VaultDR Client creates additional sub-directories that are required for use by this plugin. The uninstallation process outlined above does not automatically remove these additional **"storix"** directories and other related data. To completely remove all associated directories and files, follow the steps outlined below:

1. From the machine containing the installation of this plugin, navigate to the "/opt/storix/bin" directory:

   cd /opt/storix/bin

2. At the command prompt, issue the following command to remove the remaining directories:

   ./stuninstall

3. You will be prompted to remove user configuration and history files. Respond "**y**" to each prompt.

   The following box shows the screen output for the procedure above.

```
# cd /opt/storix/bin
# ./stuninstall

This program will remove Storix System Backup
Adminsitrator software from the system. You may choose to
keep the user configuration files in the
/storix directory will not be removed in case you decide
to reinstall this or another version at a later time.

Do you wish to also remove the user configuration and
history files in the data (/storix) directory (y/n)? y

Are you sure you want to remove the software (y/n)? y
Removing system startup configuration ...
Removing program files ...
Removing user data and history files ...

Storix System Backup Administrator has been removed.
```

4. Remove the "/usr/netvault/util/linux" directory via the following command:

   rm -irf /usr/netvault/util/linux

5. Remove the README files via the following command:

   rm -irf /usr/netvault/util/RE*

6. Respond "**y**" to the prompts.
7. Remove the "/usr/netvault/util/stinstall" directory via the following command:

   rm -irf /usr/netvault/util/stinstall

8. Respond "**y**" to the prompt.

5.2.0 Generating a DR Image

Important: Attempts to perform a **VaultDR Online Plugin for Linux** backup of a system whose hard disk is full or nearly full, may fail. The plugin requires a portion of the local system's hard disk to synchronize data. If enough free space is not available for this synchronization of data, the backup will fail.

If the user changed the default **Storix Temp** directory as described in *Storix Installation* on page 88, ensure that the new **Storix Temp** directory exists before continuing.

5.2.1 The Backup Dialog

This section outlines the use of the NetVault: Backup GUI's **Backup** dialog from the NetVault: Backup Server in order to create a DR image of a Linux Client.

1. From the NetVault: Backup Server, access the **Backup** dialog from the NetVault: Backup GUI (by clicking either **Backup** button or by selecting the **Backup** command from the **Operations** pull-down menu).
2. From the **Backup** dialog, locate the NetVault: Backup Client that is to serve as a target for a DR backup (i.e., a machine containing an installation of the **VaultDR Online Plugin for Linux**). Double-click on this Client to open it and reveal a list of APMs/plugins installed there.
3. Locate the **VaultDR Online Plugin for Linux** (i.e., labelled as **"VaultDR Online Linux"** in the **Selections** tab) and open it by double-clicking on it. An icon representing the VaultDR Client displays.
4. From this level of the selection tree, it is possible to select the entire Linux Client for inclusion in a DR backup, or it can be double-clicked to open it and reveal its individual selectable DR components. Two items will appear as selectable for the Linux VaultDR Client machine:

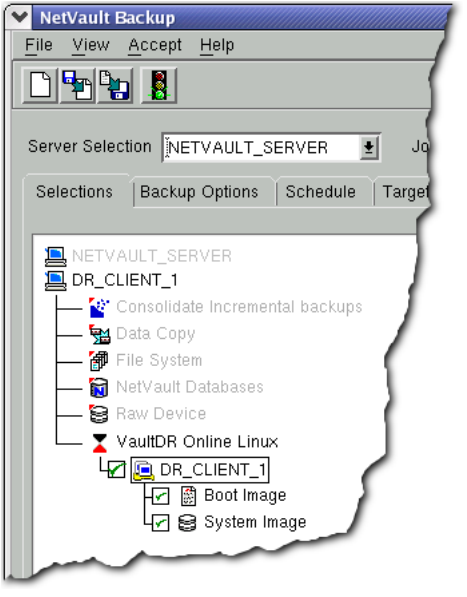


Figure 5-6: *The* ***Selections*** *tab of the* ***NetVault Backup*** *dialog*

   - **Boot Image** – Select this item in order to have the plugin scan the Linux VaultDR Client machine and incorporate required system information (i.e., NIC card driver files) as well as various operating system data files into a CD creation file (entitled **"linuxboot.iso"**). This file can be restored to the NetVault: Backup Server where it would be used to create a bootable CD-ROM. This CD-ROM is then used to boot the same Linux VaultDR Client the **Boot Image** data was taken from in order to prepare it for the recovery of its backed up **System Image** information.
   - **System Image** – Select this item in order to perform a DR backup of the entire Client system. This will include all system information for the Linux VaultDR Client, including all partition and **Disk Boot Record** information.

     Note the following important points:

- When backing up the **System Image**, you must also backup the **Boot Image** or the backup will fail. Check both boxes under the Linux VaultDR Client machine.
- The **Boot Image** must be selected for backup at least once from a Linux VaultDR Client. The **"linuxboot.iso"** file that is created is required during the recovery process and failure to take at least one backup of this item will result in the inability to recover the **System Image** information taken from a specific Linux VaultDR Client.
- The **Boot Images** data backup incorporates driver information files from the "**/lib/modules**" directory on the Client machine. Before backing up this data ensure that proper device information files for all the devices used by the target Client are available in the "**/lib/modules**" directory.

  Note that:

  - The boot CD will be unable to load devices for which proper device driver files are not available in the **Boot Images** backup.
  - The boot CD will load only those devices for which the device drivers are supported by the third party DR boot utility application used by the **VaultDR Online Plugin for Linux**.
- The **VaultDR Online for Linux Plugin** does not support the backup of Access Control Lists (ACLs) and attribute information. When a backup of a target Linux system is performed these details will not be included. Once the restore of this backup is performed, any ACLs/attributes must be manually recreated.

- The remaining tab selections (e.g., **Schedule**, **Target** and **Advanced Options**) contain additional options that can be set as desired. The options available in these tabs are not unique to the **VaultDR Online Plugin for Linux** (for more information on these tabs and the options available within, see the *NetVault®: Backup Administrator's Guide*).
- Input a suitable name for the job in the **Job Title** field. It is recommended that a detailed name be used to allow for easy identification of the job at the time of recovery. Launch the job by clicking on the **Submit** button.

5.2.2 The 'About' Pop-up Menu Item

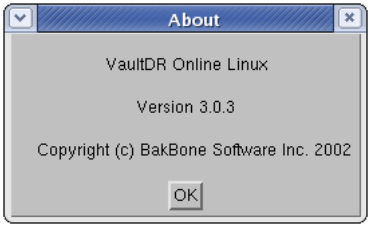


*Figure 5-7: The **About** dialog*

From the **Selections** tab of the **Backup** window, right-clicking on the **VaultDR Online Linux** node, followed by selecting **About** from the pop-up menu will reveal the **About** dialog. This dialog contains version information for the currently installed version of **VaultDR Online Plugin for Linux**. To close this dialog and return to the **Selections** tab, click **OK**.

5.3.0 Creating the Required Bootable CD-ROM

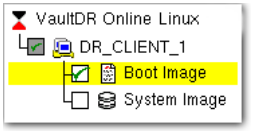


Figure 5-8: *The Boot Image item for a Linux VaultDR Client selected for inclusion in a DR image*

With a successful DR image taken, the next phase of the DR procedure is the creation of a CD-ROM that contains the proper O/S and device driver files for the target VaultDR Client, in order to boot this machine when a recovery is required. This required data is included in a DR image when the **Boot Image** item is selected for inclusion in a backup of a target VaultDR Client. As outlined in earlier sections, when the **Boot Image** item is included, a CD-creation file, entitled **"linuxboot.iso"** is created and saved on ***both*** the target VaultDR Client itself and on the piece of media targeted by the backup. This allows an administrator to select from various different methods to create this CD-ROM. Any number of methods can be used to access this data and create this required CD. The following sections cover two example methods that can be used to successfully accomplish this.

Important: ***Both*** of the following CD creation methods require that the aforementioned **Boot Image** item for a Linux VaultDR Client be previously backed up in ***at least*** one DR image. Failure to backup this information will result in the inability to create this required CD, and it will not be possible to properly boot the target Linux Client for a recovery.

5.3.1 Method 1: Create the CD and Save it for Future Use

Performed prior to the need for a recovery, this method allows the administrator to create this required CD from the **"linuxboot.iso"** file that was saved ***locally*** on the target VaultDR Client, and then store this CD for later use. Follow the steps outlined below to create the CD using this method:

5.3.1.a Prerequisites

The following items are required in order to create the CD:

- **Writable CD-ROM Drive** (available locally on the target VaultDR Client)
- **One Blank, Writable CD**
- **CD Generation Software** (installed locally on the target VaultDR Client)

5.3.1.b Creation Procedure

1. From the target VaultDR Client, insert a blank, writable CD into the drive.
2. Launch the CD generation software and access the **"linuxboot.iso"** file. This file will reside in the directory named in the **Boot Images Directory** field of the **Backup Options** tab for this particular backup job (e.g., the default value is **"/storix/temp"**). So, if this value was not changed prior to backup, the file will be located in this directory.

3. Using this file, create the CD using the utilities within the CD generation software.

Important: As CD generation softwares vary, no instruction is given here on how to launch or administer their use. See the relevant software's documentation for complete instructions on generating a CD using an **".iso"** CD creation file.

4. With the CD completed, remove it from the drive and label it appropriately so that it can be easily referenced for future use (e.g., assign a label corresponding to something specific about the target VaultDR Client, such as its O/S-assigned name).

5.3.2 Method 2: Create the CD-ROM at the Time of Recovery

With this method, an administrator can create this required CD using data recovered from the actual DR image backup, at the point in time that a recovery is required. Follow the steps outlined below to create the CD using this method:

5.3.2.a Prerequisites

The following items are required in order to create the CD:

- **Writable CD-ROM Drive** (available locally on the target VaultDR Client)
- **One Blank, Writable CD**
- **CD Generation Software** (installed locally on the target VaultDR Client)

5.3.2.b Creation Procedure

1. It is first necessary to recover the **Boot Image** data taken from the backup of the target Linux VaultDR Client. From the NetVault: Backup Server, access the **Restore** window (i.e., via either the large or small command toolbar buttons in the GUI or the **Restore** command accessed from the **Operations** pull-down menu).
2. From the **Selections** tab, locate the NetVault: Backup Client that was configured as the Linux VaultDR Client in question and double-click on it to open it and reveal the APMs/plugins used to backup data on this machine.
3. Double-click on the **VaultDR Online Linux** icon to open it and reveal the backup savesets created with this plugin.
4. Access the backup saveset that contains a backup of the **Boot Image** data for the target VaultDR Client by double-clicking on it. The NetVault: Backup Client will appear in the tree, double-click on it to reveal the data included in the DR image. Locate the **"linuxboot.iso"** item and select it for recovery.

Important: Only include the **"linuxboot.iso"** item in this recovery job. Any other items selected for recovery during this procedure will not be successfully restored.

5. Select the **Target Client** tab. In the list of displayed Clients, select the NetVault: Backup Server as the target for the restore.
6. Leave all other options available in the remaining tabs of the **Restore** window at their default settings (i.e., the **Restore Options**, **Schedule** and **Advanced Options** tabs).
7. Input a suitable name for the job in the **Job Title** field (e.g., something labelling it as the recovery of the **"linuxboot.iso"** data) and submit the job.
8. The file will be recovered to the following subdirectory of the NetVault: Backup installation directory, on the NetVault: Backup Server (where **"..."** represents the path to NetVault: Backup's installation directory):

   .../netvault/tmp

Important: Recovery of the **Boot Image** information, regardless of the Linux VaultDR Client it was performed from, will create a CD creation file entitled **"linuxboot.iso"** in the above-named directory. If **Boot Image** information is recovered from an additional Linux VaultDR Client using the above procedure, its **"linuxboot.iso"** file will be restored and ***overwrite*** any file of the same name currently residing in this directory, and ***no warning will be issued***. Therefore, it is recommended that this entire process be followed through to completion for a single Linux VaultDR Client, ***before*** attempting to recover backed up **Boot Image** information from an additional Linux VaultDR Client.

9. Insert a blank, writable CD into a CD-ROM writer that is accessible to the NetVault: Backup Server.
10. Launch the CD generation software and access the **"linuxboot.iso"** file. This file will reside in the directory named in step 8 above. Create the CD using the necessary utilities within the CD generation software.

Note: As CD generation softwares vary, no instruction is given here on how to launch or administer their use. See the relevant software's documentation for complete instructions on generating a CD using an **".iso"** CD creation file.

11. With the CD completed, remove it from the drive and label it appropriately. For example, assign a label corresponding to something specific about the target VaultDR Client, such as its O/S-assigned name.

Important: Provided the hardware configuration in the target Linux VaultDR Client ***does not change***, this CD can be saved for future use in booting the Client for the recovery of future DR images recorded with this plugin. If however, new networking hardware is implemented or the device driver files in the Client machine change any time, the **Boot Image** data for the Client will need to be backed up again and this procedure will need to be repeated to create a new CD.

Important: The Boot CD will be unable to load devices for which proper driver files are not incorporated in the **Boot Image** backup. We recommend the boot media be tested on the target Linux VaultDR Client for successful loading of all the devices during boot up process.

5.4.0 Recovering a DR Image

The steps required to successfully recover a DR image performed with the **VaultDR Online Plugin for Linux** vary based on how the data was originally managed during backup. The overall process can be roughly broken down into the following steps:

- **Phase 1: Pre-Recovery Considerations**
- **Phase 2: Set Up and Launch the Recovery in NetVault: Backup**
- **Phase 3: Boot the Target VaultDR Client with the Appropriate O/S and Drivers**
- **Phase 4: Monitor Restore Job Progress and Finalize a Recovery**

The following sections of the document cover the processes required to successfully complete each of the steps above.

Important: VaultDR Online Plugin for Linux version 3.0 cannot be used to restore data that was backed up using a previous version of the **VaultDR Online Plugin**. In order to recover pre-3.0 data, you must use the same version of the **VaultDR Online Plugin for Linux** that was used to back it up.

Note: The **VaultDR Online Plugin for Linux** can only process one restore at a time.

5.4.1 Phase 1: Pre-Recovery Considerations

Before launching a recovery of a **VaultDR Online Plugin for Linux** backup, it is recommended that you take the following points into consideration.

- **The Recovery Process will Add/Modify Various Existing Files** – During the restore process, the following list of files will be added/modified:
  - **/etc/hosts**
  - **/etc/fstab**
  - **/etc/modules.conf**
  - **/etc/lilo.conf**
  - **/etc/sysconfig/network**
  - **/etc/sysconfig/network-script/ifcfg-eth* (where * is a numerical value)**
  - **/etc/sysconfig/network-script/ifcfg-lo**

- **/boot/initrd-storix-*device_name*.img**

To preserve the existing state of these files, the following procedure can be followed.

Note: This process is not required. It is only intended to offer a procedure to maintain the existing state of the named files after a **VaultDR Online Plugin for Linux** recovery (i.e., the recovery will still complete successfully if this procedure is not followed).

1. From the machine acting as the NetVault: Backup Server, access the **Backup** window and conduct a standard **File System Plugin** backup of the following files:
   - **/etc/hosts**
   - **/etc/fstab**
   - **/etc/modules.conf**
   - **/etc/lilo.conf**
   - **/etc/sysconfig/network**
   - **/etc/sysconfig/network-script/ifcfg-eth***
   - **/etc/sysconfig/network-script/ifcfg-lo**

Important: It is not necessary to backup the "**/boot/initrd-storix-*device_name*.img**" file. This file should be left alone so that it will be properly modified during the recovery process.

Note: For complete instructions on the use of the **File System Plugin**, see the *NetVault®: Backup Administrator's Guide*.

2. Perform the recovery of the **VaultDR Online Plugin for Linux** backup as outlined in the sections that follow.
3. Restore the **File System Plugin** backup of these files after the DR recovery has completed.

- **Accommodating for Raw Format Disks on a Target VaultDR Client** – As noted in an earlier section of this guide, the **VaultDR Online Plugin for Linux *does not*** support the backup of Raw format disks. However, the utility used to boot a target VaultDR Client for the recovery will initialize these disks even though they were not backed up, and there is potential for data loss. Prior to initiating a recovery, note the partition structure of the target VaultDR Client and ensure that you follow the steps outlined in the section, *Boot Procedure: Accommodating for Raw Disks* on page 108 in order to preserve any Raw format disks that may exist.

Important: When performing a system restore, Storix SBAdmin creates the partition table starting at sector 1. The user can specify the size of the partitions and the number of sectors, but they cannot specify the partition offset.

5.4.2 Phase 2: Set Up and Launch the Recovery in NetVault: Backup

As noted above, it is first necessary to set up a recovery job for a Linux VaultDR Client from the NetVault: Backup GUI on the NetVault: Backup Server. It is also necessary to actually launch this job, before attempting to boot the Linux VaultDR Client with the created CD. Perform the following steps to set up and launch a DR recovery job.

1. From the NetVault: Backup Server, access the **Restore** window (i.e., via either the large or small command toolbar buttons in the GUI or the **Restore** command accessed from the **Operations** pull-down menu).
2. From the **Selections** tab, locate the NetVault: Backup Client that was configured as the Linux VaultDR Client in question and double-click on it to open it. The APMs/plugins used to successfully backup data on this machine will display.
3. Double-click on the **VaultDR Online Linux** icon to open it and reveal the backup savesets created with this plugin.
4. Locate the desired backup saveset, identified by its title (i.e., the name given to the DR image in the **Job Title** field at the time of backup) and double-click on it to open it.
5. The Linux VaultDR Client displays. From this level of the tree, the DR image can be selected in its entirety, or it can be double-clicked to open it and reveal its individual contents. In order for the restore to work properly all data items must be selected (the browse functionality is only intended to allow you to view the contents of the backup saveset — not select individual items for the recovery).

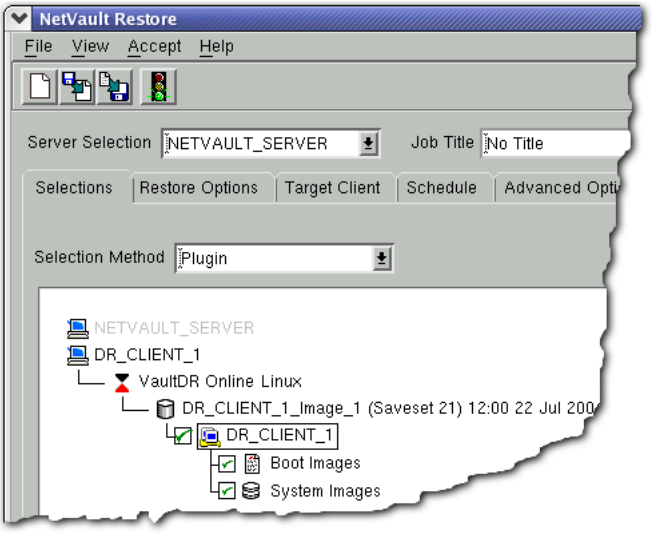


Figure 5-9: A Linux VaultDR Client's backup saveset

Note the following:

- If the entire contents of a backup saveset are not selected for the restore, the recovery will fail once it is launched.
- If a disk is comprised of ***four*** primary partitions, the ***fourth*** partition will be automatically converted to an ***extended logical*** partition during the recovery. Having a fourth primary partition inhibits the ability to add more partitions to the disk at a later time. By converting the fourth partition to a logical one, this allows you to use additional space on a hard disk to create future partitions (e.g., in the event that the recovery is being performed to disk that is larger than the original). There is ***no*** data loss associated with this behavior. You will be alerted to this fact during the boot process in a dialog of the **System Installation for Linux** (see the section, *Phase 3: Boot the Target VaultDR Client with the Appropriate O/S and Drivers* on page 101 for details on this process).

6. Select the **Restore Options** tab to reveal the following fields:
   - **Client Hostname** – This field contains the NetVault name of the Linux VaultDR Client that was the target of the DR backup. The value in this field only

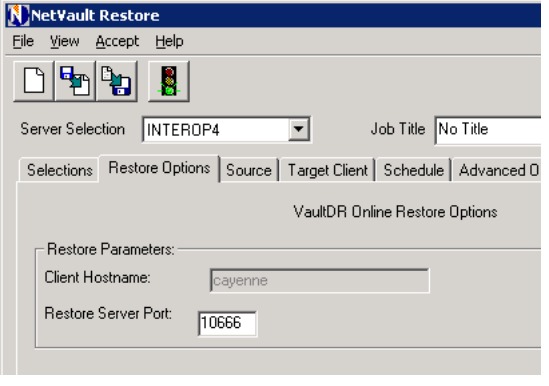
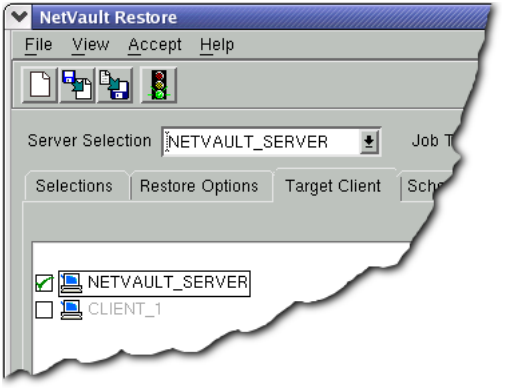


*Figure 5-10: The **Restore Options** tab*

serves as a reference and cannot be changed (it will remain greyed-out and unavailable).

- **Restore Server Port** – This field allows users to choose the port for incoming connections on the server. The default value is 10666.

*Figure 5-11: The **Target Client** tab*



7. Restores must be routed through the NetVault: Backup Server to use the necessary components installed there. Therefore, the **Target Client** tab must be selected. In the dialog that appears, select the NetVault: Backup Server from the list of displayed machines, as the intended target. This setting will work in tandem with the value revealed in the **Client Hostname** field of the **Restore Options** tab to route the restore properly.
8. The remaining tab selections (e.g., **Schedule** and **Advanced Options**) contain additional options that can be set as desired. The options available in these tabs are not unique to the **VaultDR Online Plugin for Linux**. For information on these tabs and the options available within, see *Chapter 5: The Restore Window* of the *NetVault®: Backup Administrator's Guide*.
9. Input an appropriate name for the job in the **Job Title** field and launch the job by clicking on the **Submit** button.

Note: With the completion of the process above, the job will be added to the NetVault: Backup job queue, but unlike a traditional NetVault: Backup restore job, it will not actually begin running. The steps covered in the following section, *Phase 3: Boot the Target VaultDR Client with the Appropriate O/S and Drivers* ***must be*** successfully performed before the job will actually begin.

5.4.3 Phase 3: Boot the Target VaultDR Client with the Appropriate O/S and Drivers

The following sections detail the procedures to be used to successfully boot a target Linux Client machine to recover a DR image backup.

5.4.3.a Step 1: Boot Prerequisites

Ensure the following have taken place before attempting to boot the VaultDR Client:

- **Bootable CD Created** – A VaultDR Online Boot CD must have been previously created for the target Linux Client, using the procedures outlined in *Creating the Required Bootable CD-ROM* on page 94.
- **CD-ROM Drive Set as Primary Boot Source on Target VaultDR Client** – The Linux machine serving as the VaultDR Client must have its CD-ROM drive set up as the primary boot source in order to have the machine boot from CD (e.g., by accessing the system's BIOS application and setting the Drive as the primary boot source).
- **NetVault: Backup Server/Client Information Gathered** – After booting the target Linux Client with the created boot CD, it is necessary to configure the machine using various information, including the following:
  - **NetVault: Backup Server IP Address**
  - **Linux VaultDR Client IP Address**
  - **Gateway Address** (if applicable)
  - **Subnet Mask**
- **Communication Port Free for Use** – The communication port ***must be*** free and accessible to the **VaultDR Online Plugin for Linux**. If the default port 10666 is not available, you must reconfigure the communication port before proceeding. For details, see *Reconfiguring the Communication Port* on page 102.

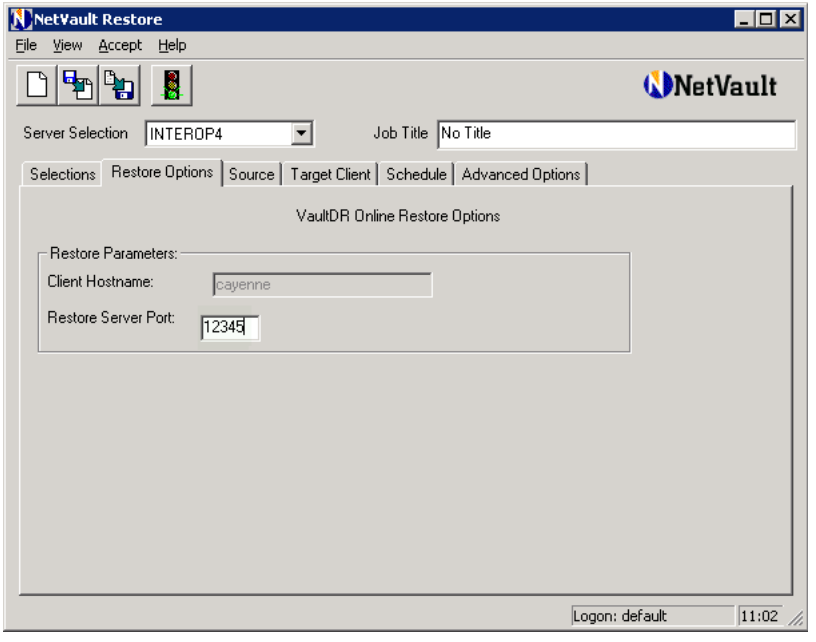
Note: In most circumstances, the 10666 port will be available for use. Circumstances under which it may not be available include if a system administrator had specifically assigned it for use to another application or if you have a firewall setup on another port.

5.4.3.b Reconfiguring the Communication Port

The VaultDR Online Plugin for Linux listens on port 10666 by default. If you have a firewall configured, you may need to change the communication port in order to perform a recovery. Let us assume, for example, that you wish to change the communication port to 12345. Perform the following steps:

1. Open the firewall for port 12345. This allows communication between the VaultDR Client to be restored and the NetVault: Backup Server.
2. Launch NetVault: Backup on the VaultDR Server.
3. Access the **NetVault Restore** dialog via the **Restore** button or the command toolbar in the NetVault: Backup GUI (or select **Restore** from the **Operations** menu).
4. Select the **Restore Options** tab.
5. Input "12345" in the **Restore Server Port** field.

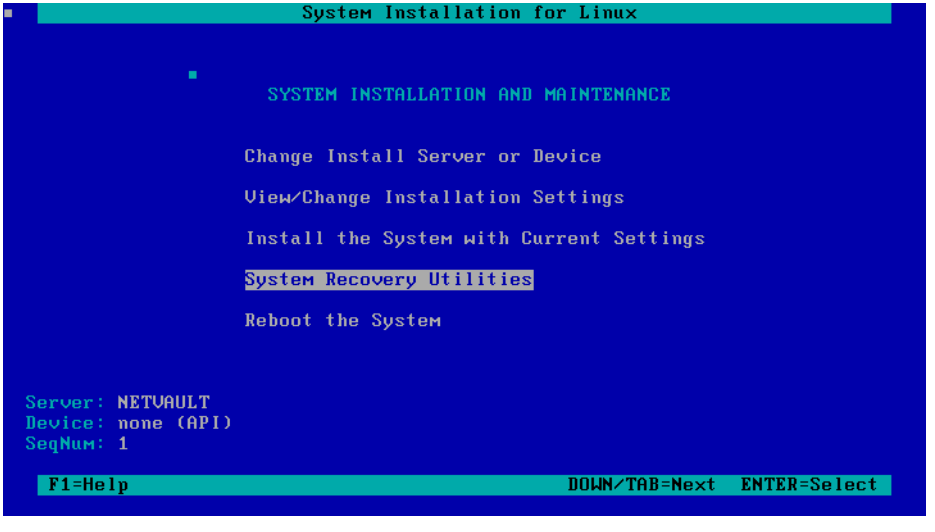
*Figure 5-12: The **Restore Options** tab*



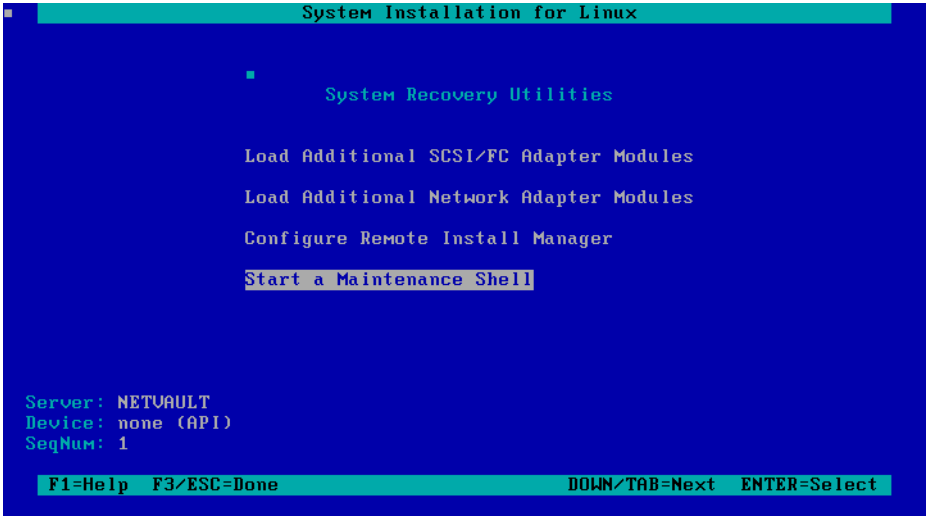
6. Click the **Submit** button.

After setting the port number on the VaultDR Server, you must make the following changes on the VaultDR Client:

1. Boot from the CD, as described in *Step 2: Boot Procedure* on page 104. The **System Installation for Linux** application launches and the following menu appears.



2. From the **System Installation and Maintenance** dialog, select **System Recovery Utility** and press **Enter**.
3. Select **Start a Maintenance Shell** and press **Enter**. This will open a maintenance shell prompt.



4. From the maintenance shell, execute the following commands:

```
maint> echo "ServerPort=12345" > /tmp/nvdrx.cfg
maint> exit
```

5. Proceed with the boot procedure, as described in *Step 2: Boot Procedure* on page 104.

5.4.3.c Step 2: Boot Procedure

Follow the steps outlined below in order to successfully boot the Linux VaultDR Client:

Important: If the target Linux VaultDR Client is comprised of any Raw format disks, a specific boot procedure must be followed in order to preserve any data that currently exists on those disks (i.e., because the does not support the backup and restore of Raw format disks). See the process outlined in the section, *Boot Procedure: Accommodating for Raw Disks* on page 108.

1. Insert the created CD into the CD-ROM drive on the target Linux VaultDR Client and reboot the machine.
2. The boot process will begin as necessary files are loaded from the CD to system memory. This procedure can take several minutes, based on the hardware configuration of the target Linux VaultDR Client.

3. Upon successful boot off of the CD, the **System Installation for Linux** application launches and the following initial screen appears:

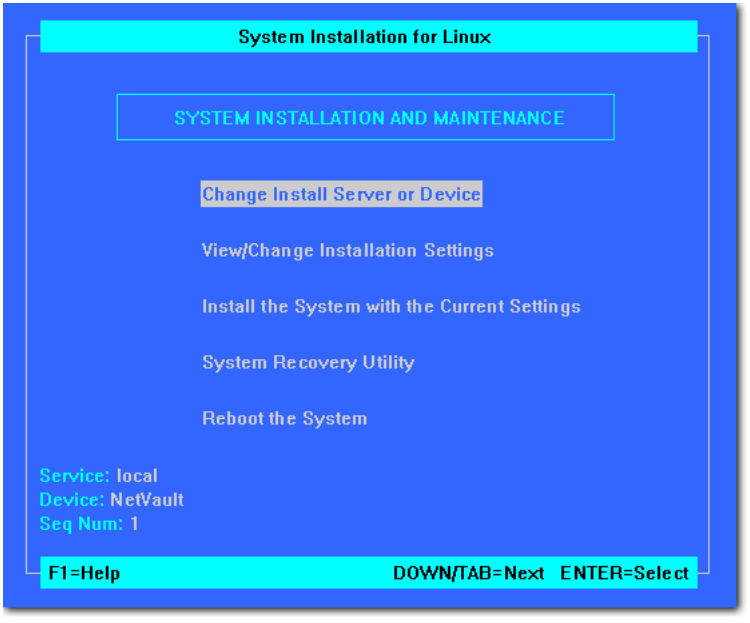


Figure 5-13: *The initial screen of the System Installation for Linux application*

Note: The **System Installation for Linux** application offers several utilities that can be used to customize a DR recovery. However, the use of all of these utilities is not covered in this guide. Only the tools required to perform a standard recovery operation are covered here.

Important: While it is strongly recommended that only the utilities required to perform a standard DR recovery be used with this plugin (as covered in this guide), the **System Installation for Linux** application contains a built-in help system that offers brief instructions on its use. This help system can be accessed on a per screen basis through the use of the **F1** key.

4. If necessary, use the arrow keys to navigate to the **Change Install Server or Device** option (default selection) and hit the **Enter** key to select it.
5. In the **Set Install Device or Server** dialog that appears next, use the arrow keys to navigate to the **Set or Change Network Configuration** option located below the **For NETWORK Installation** heading and hit the **Enter** key to select this option.

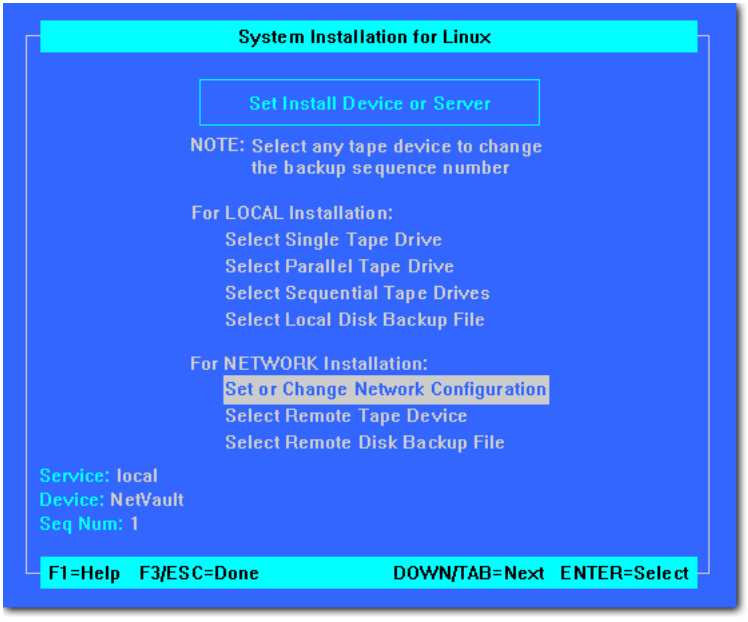


Figure 5-14: *Selecting the Set or Change Network Configuration option from the Set Install Device or Server dialog*

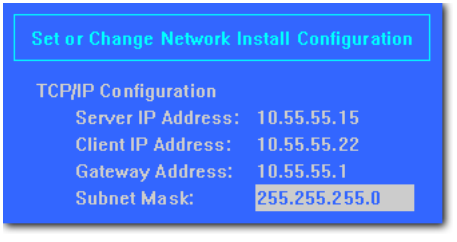


Figure 5-15: *Values input as required in the four fields for the TCP/IP Configuration settings*

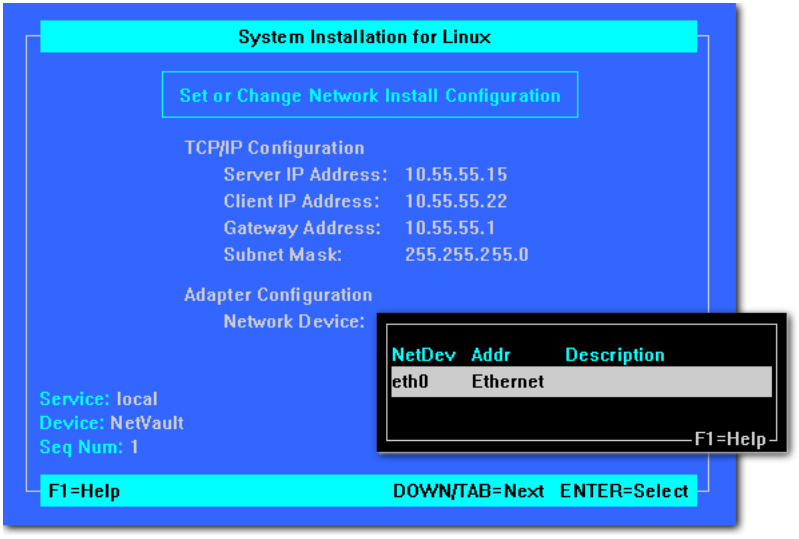
6. In the **Set or Change Network Install Configuration** dialog that launches, input the following information under the **TCP/IP Configuration** heading, using the arrow keys to navigate between the four fields:
   - **Server IP Address** – The IP address assigned to the NetVault: Backup Server that was used to launch the job in the previous section.
   - **Client IP Address** – The IP address assigned to the machine serving as the Linux VaultDR Client.
   - **Gateway Address** – The gateway address in use by the network (if applicable).

Important: Use of the **Gateway** field is optional. If VaultDR Server and Client are in the same network segment, ensure that this field ***remains blank***. Only include a gateway value if Server and Client exist in a ***different*** segment.

   - **Subnet Mask** – The Subnet Mask value in use by the network.
7. With the previous four values successfully input, use the arrow keys to navigate to the **Network Device** field, below the **Adapter Configuration** heading. The available commands listed in the bar at the bottom of this dialog

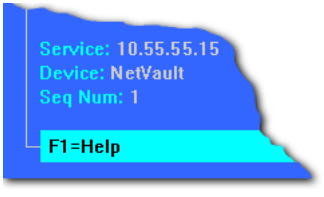
will be updated to reveal the **"F4=List"** option. Hit the **F4** key to display a list of network interface cards (NIC) available in the Linux Client.

Figure 5-16: With TCP/IP Configuration settings made, the Network Device selection dialog is accessed to select a NIC to be used by navigating to the Network Device field with the arrow keys followed by hitting the F4 key



8. In the sub-window that launches, use the arrow keys to navigate to the NIC to be used and hit the **Enter** key to select it. The **Network Device** field will be updated to reveal this selected NIC. Hit either the **F3** or **Esc** keys to confirm all settings and exit out of this dialog.
9. Back in the **Set Install Device or Server** dialog, no additional settings are required. Hit either the **F3** or **Esc** keys to exit out of this dialog.
10. Returning to the **System Installation and Maintenance** dialog of this application, the informational fields at the bottom left will be updated to reveal the values input (i.e., the Service field will be updated to reveal the IP address input for the NetVault: Backup Server).

Figure 5-17: Setup information updated to reveal the NetVault: Backup Server's IP address in the Service field



11. Use the arrow keys to navigate to the **Install the System with Current Settings** option, and hit the **Enter** key to initiate the job. If all settings were properly input, the process will continue, otherwise a red dialog will launch stating that the job could not be initiated.

Important: In order for this process to successfully launch, the desired recovery job must have already been set up and launched from the NetVault: Backup Server (as outlined in the section *Phase 2: Set Up and Launch the Recovery in NetVault: Backup* on page 99).

Figure 5-18: *The warning dialog issued as a recovery job is started*

12. Before actual job launch, the frame in this dialog will be updated with a message stating that the selected disks will be erased and overwritten on the Linux VaultDR Client if the operation is continued. Hit the **Y** key to confirm and start the recovery (or hit **N** to abort the job and return to the set up application).

5.4.3.d Boot Procedure: Accommodating for Raw Disks

Multiple sections of this guide have noted that the **VaultDR Online Plugin for Linux** does not support the backup and restore of Raw format disks. However, once the standard boot process discussed in the previous section is fully followed, any Raw format disks will be automatically initialized, and the restore of data will launch. As an end result, any data that exists on these raw format disks ***will be lost***. Use the steps outlined below to properly boot a target Linux VaultDR Client that contains any Raw format disks in order to omit them from the restore:

Warning: This procedure ***must be*** followed in order to ensure that data items on any existing raw formatted disks is preserved. BakBone Software cannot be held liable if this procedure is not followed to boot a machine containing raw disks and data is lost.

Important: The process described in the section, *Phase 2: Set Up and Launch the Recovery in NetVault: Backup* on page 99 must be followed before attempting this configuration. If the DR backup job has not been initially queued up to run, it will not be possible to complete this process (i.e., this configuration must be performed after the job has been launched in the NetVault: Backup GUI).

1. Perform **Steps 1–9**, as illustrated in the section, *Step 2: Boot Procedure* on page 104. Do not complete the process (i.e., ***do not*** perform **Steps 10–12**)
2. After returning to the **System Installation and Maintenance** dialog, use the arrow keys to navigate to the **View/Change Installation Settings** option and press the **Enter** key to continue. Various dialogs will appear as the backup job information is read from the NetVault: Backup Server. This process may take several minutes to complete.

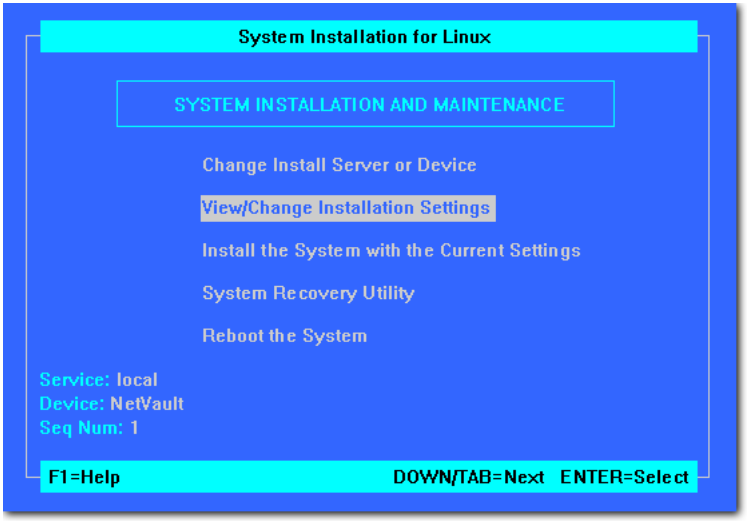


Figure 5-19: *Selecting the View/Change Installation Settings from the initial screen*

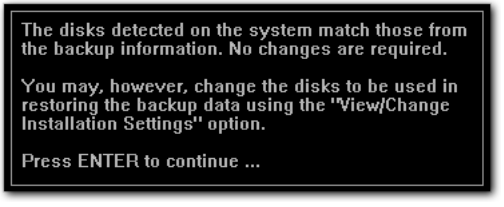


Figure 5-20: *The warning dialog that will appear at this stage of the process*

3. A frame may appear in this dialog stating that the disks on the system match the current configuration. To continue with the set up and close this dialog, press the **Enter** key.
4. The **Change Installation Settings Menu** dialog will appear. Press **Enter** to select the default option, **Select Disks to Use for Installation**.

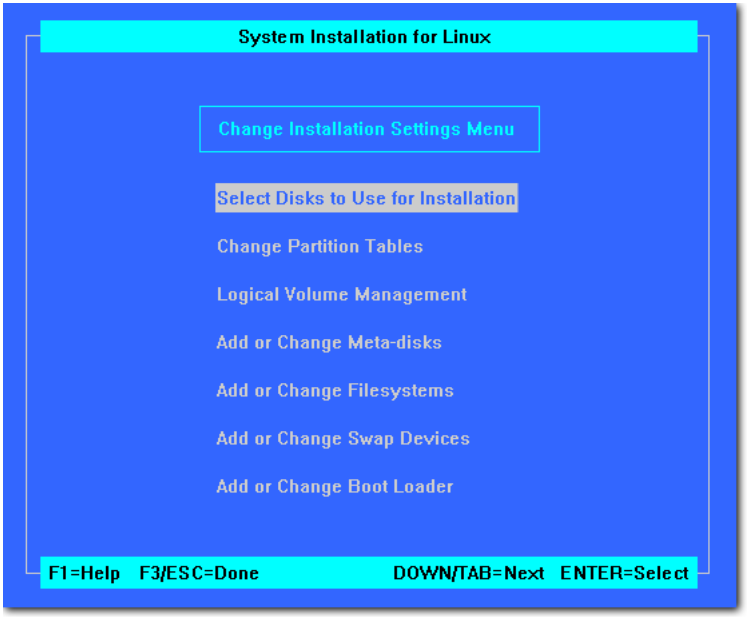


Figure 5-21: *From the Change Installation Settings Menu, select the Select Disks to Use for Installation option*

5. The dialog will update with a frame containing a list of disks that are currently available on the target system. Using the **Arrow** keys, select the disk that is to be left out of the restore (i.e., the Raw partition formatted disk) and press **Enter** to select it.

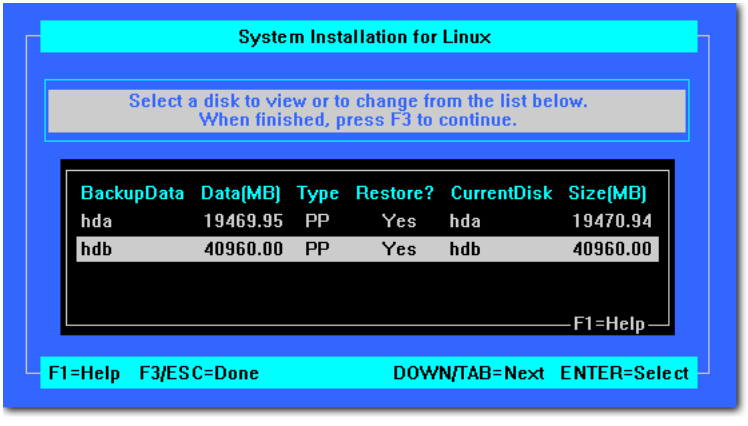


Figure 5-22: *In this example the disk "hdb" is selected from the list to be omitted from the recovery*

6. With the desired disk selected, the frame will update to contain a list of available options. Using the **Arrow** keys highlight the **DO NOT RESTORE the Disk Backup Data** option and press **Enter**.

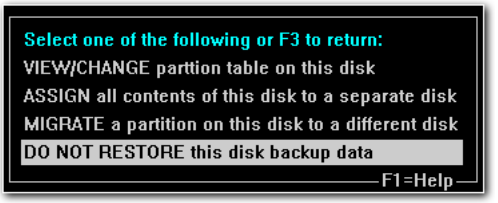


Figure 5-23: Select the DO NOT RESTORE This Disk Backup Data option from the list of options

Important: Prior to selecting the **DO NOT RESTORE This Disk Backup Data** option for a drive, ensure that the selected drive is the one that is to be omitted. Once the drive has been omitted from the restore, it cannot be re-added (i.e., the only way to change the configuration is to reboot the Linux VaultDR Client, and restart this entire process).

7. The frame in the dialog will be updated to contain a message stating that by selecting this disk, it will not be recovered. Press the **"Y"** key to confirm (or "N" to abort the process and return to the previous screen). With the omit command confirmed, the frame in the dialog will reveal the list of disks on the target system, and the disk that is to be omitted from the recovery will be labelled as **"---------AVAILABLE---------"**.

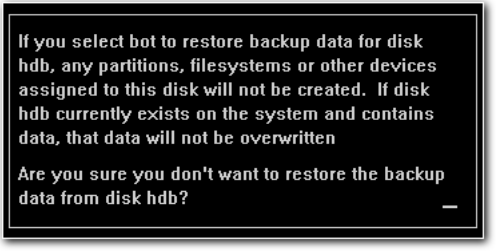


Figure 5-24: By pressing the "Y" key when this message is displayed, the disk "hdb" will be omitted from the recovery

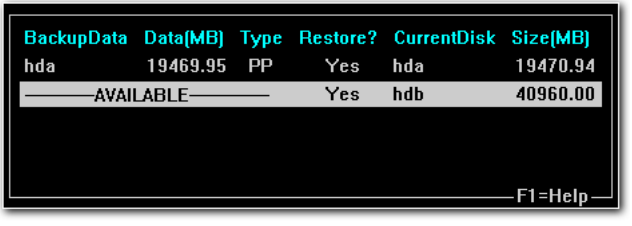


Figure 5-25: With the process complete, the disk "hdb" is omitted from the recovery and marked as "AVAILABLE" in the list of disks

8. If additional disks are to be omitted, repeat **Steps 5–7** to omit them.
9. With the desired disk(s) omitted from the recovery, press **Esc** or **F3** ***twice*** to return to the **System Installation and Maintenance** dialog of this application. The informational fields at the bottom left will be updated to reveal the values input (i.e., the **Service** field will be updated to reveal the IP address input for the NetVault: Backup Server).

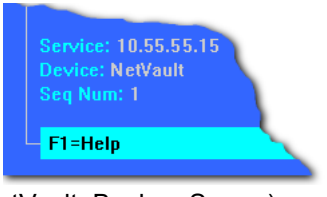


Figure 5-26: Setup information updated to reveal the NetVault: Backup Server's IP address in the Service field

10. Use the arrow keys to navigate to the **Install the System with Current Settings** option, and press **Enter** to initiate the job. If all settings were

properly input, the process will continue, otherwise a red dialog will launch stating that the job could not be initiated.

11. Before actual job launch, the frame will be updated with a message stating that the selected disks will be erased and overwritten on the Linux VaultDR Client if the operation is continued. Only those disks that were ***not omitted*** will display in this frame. Hit the **Y** key to confirm and start the recovery (or hit **N** to abort the job and return to the set up application).

Figure 5-27: *The final frame reveals only the disk "hda", since the remaining disk was omitted from the recovery*

5.4.4 Phase 4: Monitor Job Progress and Finalize a Recovery

From the NetVault: Backup Server, it is possible to monitor the progress of any job via the **Job Management** dialog. While it is not necessary to monitor a job's progress, it is recommended that this be done when performing a recovery of a VaultDR Client. Once the recovery of a Linux VaultDR Client has completed, it is necessary to perform a last task to bring it back online. By monitoring the recovery job, a user will be alerted to the completion of a job and this final task can be performed.

Note: This section offers an example of the use of the **Job Management** dialog of the NetVault: Backup GUI for the sole purpose of monitoring the progress of a Linux DR recovery operation in order to finalize the job. The tools made available in this dialog are not exclusive to the **VaultDR Online Plugin for Linux** and complete information on their use can be found in *Chapter 10: The Job Management Window* of the *NetVault®: Backup Administrator's Guide*.

1. With the recovery job running, access the **Job Management** dialog from the GUI on the NetVault: Backup Server (i.e., by clicking either of the **Job Management** command toolbar buttons or by selecting the **Job Management** command from the **Operations** pull-down menu, in the main window of the GUI).
2. In the list of jobs displayed here, locate the Linux DR recovery job in progress and right-click on it. In the pop-up menu that appears, select the **Monitor Job** command.

Important: In addition to the **Monitor Job** command located in this pop-up menu, the **Abort Job** command can be accessed to stop the job. If this command is used to stop a recovery job, NetVault: Backup ***will*** stop the actual transfer of data. However, the **System Installation for Linux** application currently running on the Linux VaultDR Client will stall and its commands, while still accessible will ***not*** be usable. A full reboot of the Linux VaultDR Client must be performed with the CD inserted in the drive in order to reactivate the application for use.

3. The **Job Monitor - <Job Title>** dialog will launch. Various information pertaining to the currently running recovery job will be displayed, including the plugin in use and data transfer rate values. The **Status** field in the **Job Information** frame at the top of this dialog will display the current status of the job (e.g., **Waiting for Media**, **Reading from Media**, etc.). As the recovery finishes, data transfer values will stop and this field will be updated with **"Restore Complete"**. The job has now completed and this dialog can be closed.

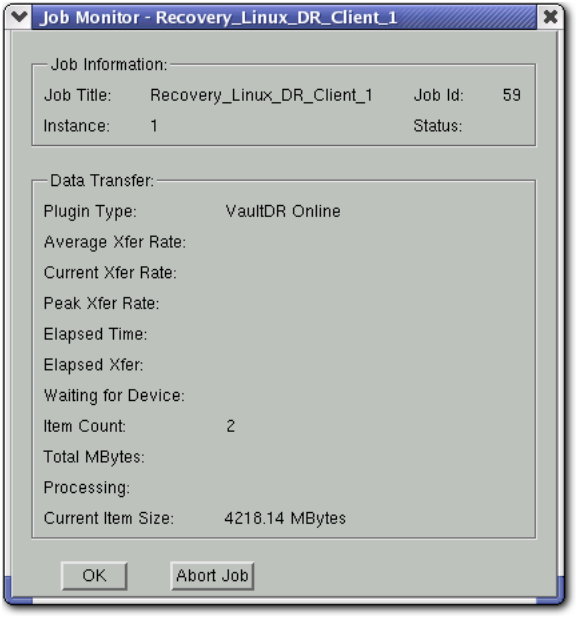


Figure 5-28: The Job Monitor dialog accessed from a selected job in the Job Management window

4. To complete the recovery process, locally access the Linux VaultDR Client machine and reboot it via the **Reboot the System** command in the **System Installation for Linux** application, or by manually shutting down the system. Upon restart of the machine, eject the CD from the drive before the boot process begins.
5. The Linux VaultDR Client will boot and its file system should be recovered to the point in time the DR image was taken.

5.4.5 Post-Restore Notes/Procedures

After a the restore process completes on a target Linux Client, the following points will apply to that machine:

- **The "hosts" file for the Target will be Modified** – A restore will modify the target VaultDR Client machine's entry in its **"../etc/hosts"** file (e.g., after recovery, the host name ***will not*** appear along with the IP address and the

alias for this Client in the **"…/etc/hosts"** file). The machine will still be accessible via its IP address, but for it to be accessible via its host name, this file must be edited to incorporate the appropriate host name information. See the relevant Linux documentation for information on this "hosts" file and how it should be edited to include the proper host name for the target Linux machine.

- **Perform a Restore of the Modified Files Backup (if Applicable)** – With the recovery completed, you can now restore the files backed up in the **File System Plugin** backup described in the section, *Phase 1: Pre-Recovery Considerations* on page 97. This will restore these files to their state before the DR recovery.
- **Change to Boot Loader Application** – If running a version of the Linux boot loader utility other than **"GRUB"**, be aware that after a DR image is recovered on a target Linux Client, the boot loader utility will be replaced with the **"GRUB"** version of this application.
- **Change in the Start-end Sector Location for a DR Restore** – After a recovery of a DR image, the start-end sector for a restored partition may be different from its original backed-up location. The partition size will remain the same size, but no unallocated space will be created after the Master Boot Record. Therefore, some boot loaders (e.g., GRUB) will not be usable, because they require this additional, unallocated space. This is the case because the LILO version of the boot loader utility that is automatically established after a recovery (as explained in the previous point) does not require this unallocated space.
- **Change to Swap Partition** – During a recovery, the VaultDR for Linux module implicitly modifies the "/etc/fstab" file entry for the swap partition.

  Example:

  For example, before the restore, "fstab" contains the following entry for the swap device:

```
LABEL=SWAP-sda2     swap     swap     defaults     0 0
```

  After the restore, the original swap entry is commented out and a new entry is added:

```
# Updated by Storix System Installation
#LABEL=SWAP-sda2     swap     swap     defaults     0 0
/dev/sda2           swap     swap     defaults     0 0
```

  The swap partition is enabled automatically, but the label for the swap partition is removed.

SECTION 4:

Appendix

Appendix A:
TROUBLESHOOTING/SUPPORT

A.0.0 Troubleshooting

The following table describes commonly encountered problems and possible solutions.

Symptom	Reason	Solution
Backup Completed with Warnings	Once this status is revealed for backup, check the NetVault Log entries for the job to see if they display one or both of the following messages: ■ **"Failed to add backup record"** ■ **"Failed to write index of backup to the database"** These messages indicate that the selected data was actually backed up, but the job's index information was not properly added by NetVault to its database. Without this index information, the data cannot be properly restored.	Method 1: Access the **Device Management** window of the NetVault GUI and perform a scan of the media targeted by the job (i.e., by right-clicking on a the target media and selecting the **Scan** command from the pop-up menu). NetVault stores index information for backup jobs in two locations: in the NetVault Database and on the media targeted by the backup. By performing this scan, the index information will be added to the NetVault Database. To verify this, open the **Restore** window and locate the specific job. If it can be browsed and a restore job set up, the scan process has corrected the problem. Method 2: If the previous method failed, it will be necessary to re-run the backup job.

A.1.0 Technical Support

BakBone Software is dedicated to providing friendly, expert advice to NetVault customers. Our highly trained professionals are available to answer your questions, offer solutions to your problems and generally help you make the most of your NetVault purchase. Log on to our web site for more information.

http://www.bakbone.com/supportportal

A.1.1 Documentation Updates

For late-breaking documentation updates, refer to the BakBone Software Knowledge Base. BakBone's Knowledge Base articles for VaultDR System Plugins can be found at the following links:

- VaultDR Offline Plugin v5.1:

  http://kb.bakbone.com/4096
- VaultDR Online Plugin for Windows Clients v3.0:

  http://kb.bakbone.com/3905
- VaultDR Online Plugin for Linux Clients v3.0:

  http://kb.bakbone.com/3813
- VaultDR Server v2.4:

  http://kb.bakbone.com/4100