Table of Contents

Getting Started ......................................................... 4
  About VMware Data Recovery ........................................ 4
  About This Guide ..................................................... 4
  Intended Audience .................................................... 4
  Assumptions .......................................................... 4
  Reference Setup Environment ....................................... 4
    vCenter Server ..................................................... 5
    ESX Hosts ........................................................ 5
    Networking ........................................................ 5
    Storage ............................................................ 5
    Virtual Machines ................................................ 5
What Will Be Covered ................................................ 6
VMware Data Recovery Evaluation Worksheet .................. 7
Help and Support During Evaluation ................................ 8
  VMware Data Recovery resources ................................ 8
  VMware vSphere and VMware vCenter resources .............. 8
VMware Contact Information ........................................ 8
Providing Feedback .................................................. 9
Backup ................................................................. 9
  Perform Initial Backup ................................................. 9
    Background Knowledge .............................................. 9
    Use Case – Perform Initial Backup .............................. 10
    Getting Started ................................................... 10
    Install the Client Plug-In ........................................ 10
    Install the Backup Appliance .................................. 10
    Steps to Perform Initial Backup ................................ 13
  Manually Trigger a Virtual Machine Backup .................. 15
    Use Case – Manually Trigger a Virtual Machine Backup .. 15
    Getting Started ................................................... 15
    Steps to Manually Trigger a Virtual Machine Backup .... 15
Restore ............................................................... 16
  Virtual Machine Restore Rehearsal ............................... 16
    Background Knowledge ............................................. 16
    Use Case – Virtual Machine Restore Rehearsal .............. 16
    Getting Started ................................................... 16
    Steps to Perform a Virtual Machine Restore Rehearsal .... 16
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Machine Restore</td>
<td>17</td>
</tr>
<tr>
<td>Background Knowledge</td>
<td>17</td>
</tr>
<tr>
<td>Use Case – Virtual Machine Restore</td>
<td>17</td>
</tr>
<tr>
<td>Getting Started</td>
<td>17</td>
</tr>
<tr>
<td>Steps to Perform a Virtual Machine Restore</td>
<td>17</td>
</tr>
<tr>
<td>File-Level Restore</td>
<td>18</td>
</tr>
<tr>
<td>Background Knowledge</td>
<td>18</td>
</tr>
<tr>
<td>Use Case – File-Level Restore</td>
<td>19</td>
</tr>
<tr>
<td>Getting Started</td>
<td>19</td>
</tr>
<tr>
<td>Steps to Perform a File-Level Restore</td>
<td>19</td>
</tr>
<tr>
<td><strong>Administration</strong></td>
<td>20</td>
</tr>
<tr>
<td>Extend a Destination Store</td>
<td>20</td>
</tr>
<tr>
<td>Background Knowledge</td>
<td>20</td>
</tr>
<tr>
<td>Use Case – Extend a Destination Store</td>
<td>21</td>
</tr>
<tr>
<td>Getting Started</td>
<td>21</td>
</tr>
<tr>
<td>Steps to Extend a Destination Store</td>
<td>21</td>
</tr>
<tr>
<td><strong>Notification</strong></td>
<td>22</td>
</tr>
<tr>
<td>Background Knowledge</td>
<td>22</td>
</tr>
<tr>
<td>Use Case – Notification Alerting</td>
<td>22</td>
</tr>
<tr>
<td>Getting Started</td>
<td>23</td>
</tr>
<tr>
<td>Steps to Configure an Email alert</td>
<td>23</td>
</tr>
<tr>
<td><strong>Maintenance Window</strong></td>
<td>24</td>
</tr>
<tr>
<td>Background Knowledge</td>
<td>24</td>
</tr>
<tr>
<td>Use Case – Maintenance Window</td>
<td>24</td>
</tr>
<tr>
<td>Getting Started</td>
<td>24</td>
</tr>
<tr>
<td>Steps to Configure the Maintenance Window</td>
<td>25</td>
</tr>
<tr>
<td><strong>Conclusion</strong></td>
<td>26</td>
</tr>
</tbody>
</table>
Getting Started

About VMware Data Recovery

VMware® Data Recovery (vDR) enables quick, simple and complete data protection for virtual machines. It is a disk-based backup and recovery solution. vDR is fully integrated with VMware vCenter™ Server to enable centralized and efficient management of backup jobs. It incorporates capabilities such as block-based data deduplication and performs only incremental backups after the first full backup is completed, to maximize storage efficiency. As a result of deduplication and the use of incremental backups, vDR significantly reduces the space requirements of the destination disk on which the backup data is stored.

About This Guide

This guide supports a self-directed, hands-on evaluation of VMware Data Recovery by IT professionals who are looking to deploy vDR in their VMware vSphere® environment to protect their virtual machines.

Intended Audience

This guide covers evaluation cases that are suitable for IT professionals who want to evaluate the vDR data protection and restore features.

Assumptions

To successfully use this guide, the following is assumed:

• VMware ESX®/VMware ESXi™ Server version 4.1 or later has been installed on the physical servers designated for this evaluation.
• VMware vCenter Server version 4.1 or later and the VMware vSphere® Client™ have been installed in the environment to manage the ESX server hosts.
• Sufficient storage has been allocated and configured to store the virtual machines and the destination stores.
• Virtual machines have been preconfigured and installed with proper guest operating systems and VMware Tools.
• VMware Data Recovery appliance has been downloaded and imported into the vSphere environment.
• VMware Data Recovery plug-in has been installed on the vSphere Client.
• Proper evaluation licenses have been obtained and installed.

For detailed information regarding installation, configuration, administration and usage of VMware vSphere and VMware Data Recovery, refer to the online documentation:

VMware vSphere: http://www.vmware.com/support/pubs/vs_pubs.html
VMware Data Recovery: http://www.vmware.com/support/pubs/vdr_pubs.html

Reference Setup Environment

Evaluators must provision the necessary hardware for the exercises included in this guide. This section provides details on a sample environment that was used for this VMware Data Recovery evaluation in the lab.
The following diagrams illustrate the lab setup:

Figure 1. ESX Cluster and Virtual Machines in Reference Setup Environment
Note: The arrow is pointing at the appliance.

**vCenter Server**
One vCenter Server was deployed, managing the ESX hosts.

**ESX Hosts**
Two ESX hosts were configured in a cluster.

**Networking**
There was a Microsoft Active Directory and a domain name server (DNS) in the lab. The DNS is configured to resolve the host name of the vDR appliance. It is recommended that forward and reverse lookups are configured properly on the DNS server for the vDR appliance.

**Storage**
A 511.75GB Fibre Channel SAN was shared by the ESX servers.

**Virtual Machines**
Two virtual machines running Windows Server 2008 R2, one running Windows Server 2003, and one running Linux were used. Each virtual machine had a 10GB hard disk.
What Will Be Covered

This guide will walk through the full cycle of virtual machine protection and restoration using VMware Data Recovery. The following are among the major vDR features that will be exercised in this evaluation:

1. Perform an initial backup.
2. Manually trigger a backup run outside of the backup window.
3. Extend the size of a destination store.
4. Perform a virtual machine restore rehearsal.
5. Perform a real virtual machine restore.
6. Perform a file-level restore.
7. Configure email reporting.
8. Configure a maintenance period.

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>FEATURES</th>
<th>WHAT WILL BE COVERED</th>
<th>TIME ESTIMATES</th>
</tr>
</thead>
</table>
| Backup           | Virtual machine protection        | Perform initial backup.  
1. Create a backup job.  
2. Bring the protected virtual machines to compliance. | 15 minutes     |
| Backup           | Virtual machine protection        | Manually trigger a backup.  
1. Select virtual machines to back up and trigger the backup. | 15 minutes     |
| Backup           | Virtual machine protection        | Extend a destination store.  
1. Increase the size of the destination store in virtual machine settings of the vDR appliance.  
2. Reboot the vDR appliance.  
3. Reconnect to the vDR appliance in the vDR plug-in interface.  
4. Unmount, extend and mount the destination store.  
5. Perform an integrity check on the destination store. | 15 minutes     |
| Restore          | Virtual machine restore rehearsal | Perform a restore rehearsal.  
1. Select the virtual machine to restore, its restore point and destination store.  
2. Verify the data restored.  
3. Delete the virtual machine created during the rehearsal. | 15 minutes     |
| Restore          | Virtual machine level restore     | Perform a real restore.  
1. Select the virtual machine to restore, its restore point and a destination store.  
2. Verify the data restored. | 15 minutes     |
| Restore          | File-level restore                | Perform a file-level restore.  
1. Set up a file-level restore agent.  
2. Use the file-level restore agent CLI to restore a file. | 15 minutes     |
| Administration   | Email alerting                    | Configure email alerting.  
1. Configure the alert.  
2. Trigger the job. | 15 minutes     |
| Administration   | Maintenance window                | Configure the maintenance period.  
1. Configure a maintenance period.  
2. Configure a copy period. | 15 minutes     |

1. The time estimates are dependent on the virtual machine’s having only one virtual disk of 10GB. If your virtual machine has a larger disk or more than one disk, you must allocate more time accordingly.
VMware Data Recovery Evaluation Worksheet

Use the following worksheet to organize the evaluation process.

<table>
<thead>
<tr>
<th>HARDWARE CHECKLIST</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Servers</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SOFTWARE CHECKLIST</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware ESX Server</td>
<td></td>
</tr>
<tr>
<td>VMware vCenter Server</td>
<td></td>
</tr>
<tr>
<td>VMware vSphere Client</td>
<td></td>
</tr>
<tr>
<td>VMware vSphere Client</td>
<td></td>
</tr>
<tr>
<td>VMware Data Recovery Plug-In</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VIRTUAL APPLIANCE CHECKLIST</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Data Recovery Appliance</td>
<td></td>
</tr>
</tbody>
</table>

After successfully installing the VMware vSphere and VMware Data Recovery software components, proceed to perform the evaluation of VMware Data Recovery. For each scenario, use the corresponding checklist below to ensure that the proper sequence is followed.

<table>
<thead>
<tr>
<th>BACKUP</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform initial backup</td>
<td></td>
</tr>
<tr>
<td>Manually trigger backup job</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RESTORE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual machine restore rehearsal</td>
<td></td>
</tr>
<tr>
<td>Virtual machine restore</td>
<td></td>
</tr>
<tr>
<td>File-level restore</td>
<td></td>
</tr>
</tbody>
</table>
Help and Support During Evaluation

This guide provides an overview of the steps required to ensure a successful evaluation of VMware Data Recovery. It is not meant to be a substitute for product documentation. Refer to the online product documentation for vDR for more detailed information (see the following for links). You can also consult the online VMware knowledge base if you have any additional questions. If you require further assistance, contact a VMware sales representative or channel partner.

VMware Data Recovery resources
- Product resources:  
  http://www.vmware.com/products/data-recovery/resources.html
- Product community:  
- VMware Data Recovery administrator’s guide:  

VMware vSphere and VMware vCenter resources
- Product documentation:  
  http://www.vmware.com/support/pubs/
- Online support:  
  http://www.vmware.com/support/
- Support offerings:  
  http://www.vmware.com/support/services
- Education services:  
  http://mylearn1.vmware.com/mgrreg/index.cfm
- Support knowledge base:  
  http://kb.vmware.com

VMware Contact Information

For additional information or to purchase VMware vSphere and VMware Data Recovery, the VMware global network of solutions providers is ready to assist. If you would like to contact VMware directly, you can reach a sales representative at 1-877-4VMWARE (650-475-5000 outside North America) or email sales@vmware.com. When emailing, include the state, country and company name from which you are inquiring. You can also visit http://www.vmware.com/vmwarestore/.
Providing Feedback

Your feedback is appreciated on the material included in this guide. In particular, any guidance on the following topics would be extremely helpful:

• How useful was the information in this guide?
• What other specific topics would you like to see covered?
• Overall, how would you rate this guide?

Send your feedback to the following address: tmdocfeedback@vmware.com, with “VMware Data Recovery Evaluation Guide” in the subject line. Thank you for your help in making this guide a valuable resource.

Backup

Perform Initial Backup

<table>
<thead>
<tr>
<th>Backup</th>
<th>Virtual machine protection</th>
<th>Perform an initial backup. 1. Create a backup job. 2. Bring the protected virtual machines to compliance.</th>
<th>15 minutes</th>
</tr>
</thead>
</table>

Background Knowledge

To back up virtual machines, a backup job must be created. A backup job captures the following attributes and policies:

1. The virtual machines to backup.
2. The destination store to store the protected virtual machines.
3. The backup window (that is, a time slot in a day) in which the backup job can run.
4. The retention policy used for determining which virtual machine backups are preserved over a period of time.

Each virtual machine can be protected by only one backup job. Each backup job can be associated with only one destination store. A backup job is run once a day during the backup window that is scheduled.

At most, two destination stores can be attached to a vDR appliance. Each destination store can be, at most, 1TB. In each destination store, vDR reserves 10GB of space for internal usage. VMware highly recommends allocating at least 50GB for destination stores, to leave enough space for backup data.

VMware recommends using virtual disks (VMDKs) for destination stores because the performance characteristics are well understood and consistent. CIFS, on the other hand, gives varying performance characteristics across CIFS providers. In many cases, lab statistics show that virtual disks yield better performance than network-based destination stores.

If a virtual machine has changes that have not been backed up, it is “out of compliance.” When a backup job is first created, the virtual machines are “out of compliance” because they have not been protected at all. Manually trigger the Backup Now option, or wait until the backup job runs in the next backup window, to complete a backup and bring the system into compliance with the protection policy.

vDR performs data deduplication for backed-up data within and across virtual machines. For example, virtual machines with the same operating system (OS) will have only one copy of common OS data stored in the destination stores.
Use Case – Perform Initial Backup
To start protecting virtual machines, create a backup job. After creating this backup job, bring the virtual machines to compliance by triggering the Backup Now function. Typically the initial protection takes longer than subsequent backups because the initial protection backs up the whole virtual machine. To start the upload immediately, trigger the Bring to Compliance function.

Getting Started
Before proceeding, ensure that the VMware Data Recovery plug-in has been properly installed and that the backup appliance has been properly imported and configured.

Getting Started
Before proceeding, ensure that the VMware Data Recovery plug-in has been properly installed and that the backup appliance has been properly imported and configured.

![VMware Data Recovery Installation Files](image)

**Figure 3. VMware Data Recovery Installation Files**
Note: As seen after downloading the ISO.

Install the Client Plug-In
**Prerequisites**
VMware Data Recovery plug-in connects to the backup appliance using TCP port 22024. If there is a firewall between the vSphere Client and the vDR appliance, TCP port 22024 must be open before the vDR appliance can be managed with the vSphere Client.

Linked Mode for vSphere vCenter is not supported with the vDR plug-in. However, if Linked Mode is required, ensure that when starting the vSphere client, it is connecting to the vCenter instance that has the vDR appliance on which work will be done.

**Procedure**
1. Run the plug-in installer `VMwareDataRecoveryPlugin.msi` on the vSphere Client machine.
2. Follow the prompts of the installation wizard.
3. Start the vSphere Client, and log in to a vCenter Server.
4. Select **Plugins > Manage Plugins** and make sure that the VMware Data Recovery plug-in is enabled.
5. The client plug-in can now be used to manage VMware Data Recovery. If the VMware Data Recovery plug-in does not appear in the vSphere Client, restart the client.

Install the Backup Appliance
**Procedure**
1. From the vSphere Client, select **File > Deploy OVF Template**.
2. Select **Deploy from file**, and then browse to the folder `VMwareDataRecovery-ovf-x86_64\` and select `VMwareDataRecovery.ovf`.
3. Review the OVF file details.
4. Select a location for the backup appliance in the vSphere inventory. You can optionally rename the backup appliance.
5. Select the host or cluster to which the backup appliance will be deployed.
6. Select a datastore to store the virtual machine files for the vDR virtual appliance.
7. Review the deployment settings and click Finish. The backup appliance is now deployed into your environment.

**vDR appliance configuration involves:**

**I. Network settings**

To configure the network settings:

1. In the vSphere Client, select Home > Inventory > Hosts and Clusters.
2. Select the VMware Data Recovery appliance.
3. Launch the console for VMware Data Recovery appliance.
4. In the console, select Configure Network.
5. Enter the following configuration:
   a. IP address
   b. Netmask
   c. Gateway
   d. DNS Server 1
   e. DNS Server 2
   f. Proxy server
   g. Proxy port

**Figure 4. vDR Console After Network Configuration**

**II. Destination store addition and formatting**

For this exercise, a destination store with at least 50GB of free space is required.

To add a destination store:

1. In vSphere Client, select Inventory > VMs and Templates.
2. In the inventory, right-click the vDR appliance virtual machine and select Edit Settings.
3. In the Hardware tab, click Add.
4. Select Hard Disk and click Next.
5. Select Create a new virtual disk and click Next.
6. Specify the disk size (e.g., 50GB) and other options. Click Next.
7. Specify the advanced options for the virtual disk and click Next.
8. Click Finish to create the disk.

To format a destination store:
1. In the vSphere Client, select Home > Solutions and Applications > VMware Data Recovery.
2. Connect to vDR appliance if not yet done.
3. Go to the Configuration tab.
4. Click Destinations.
5. Select the disk that was just added (e.g., /dev/sdb).
6. Click Format...

Virtual Hardware Upgrade
vDR has the capability to perform Changed Block Tracking if the protected virtual machine has VMware Virtual Hardware version 7 or later, as opposed to version 4. To attain better performance, it is recommended that all virtual machines be upgraded from Virtual Hardware version 4 to version 7 or later. Be aware that you must upgrade VMware Tools before you upgrade Virtual Hardware. VMware vCenter™ Update Manager can do this most easily. You can find more information in the vSphere documentation.
Figure 7. Virtual Machine with VMware Virtual Hardware Version 4

Steps to Perform Initial Backup
To create a backup job:
1. In the vSphere Client, select Home > Solutions and Applications > VMware Data Recovery.
2. You might be prompted with a configuration wizard that will finish with a prompt to start a backup. If you are not prompted, change to the Backup tab, and select New to start the new job wizard.
3. Name the backup job.
4. On the Virtual Machines page, select individual virtual machines or containers that comprise virtual machines to be backed up. Click Next.

Figure 8. Select Virtual Machines to Back Up

5. On the Destination page, select the destination store for this backup job.

Figure 9. Select Destination Store for Backup Job
6. On the **Backup Window** page, accept the default times or specify alternate backup windows. Click **Next**.

![Select Backup Window for Backup Job](image)

Figure 10. Select Backup Window for Backup Job

7. On the **Retention Policy** page, accept the default retention policy or specify an alternate retention policy. Click **Next**.

![Select Retention Policy for Backup Job](image)

Figure 11. Select Retention Policy for Backup Job

8. On the **Ready to Complete** page, review the summary information for the backup job. Click **Next**.

To bring the virtual machines to compliance:

1. In the vSphere Client, select **Home > Solutions and Applications > VMware Data Recovery**.
2. Go to the **Backup** tab.
3. Select the **Backup Job** to bring to compliance.
4. Right-click the **Backup Job**.
5. Select Backup **Now\All Sources**.
Manually Trigger a Virtual Machine Backup

| Backup       | Virtual machine protection | Manually trigger a backup. 1. Select virtual machines to back up and trigger the backup. | 15 minutes |

Use Case – Manually Trigger a Virtual Machine Backup

If there is important data in a virtual machine that must be backed up immediately, before the backup window opens, a virtual machine backup can be manually triggered.

Getting Started

Ensure that a backup job has been created, as discussed earlier.

Steps to Manually Trigger a Virtual Machine Backup

To manually trigger a virtual machine backup:

1. In the vSphere Client, select Home > Solutions and Applications > VMware Data Recovery.
2. Select the virtual machine to back up.
3. Right-click the virtual machine and select Backup Now.
### Restore

#### Virtual Machine Restore Rehearsal

| Restore | Virtual machine restore rehearsal | Perform a restore rehearsal. 1. Select the virtual machine to restore, its restore point and a destination store. 2. Verify the data restored. 3. Delete the virtual machine created during the rehearsal. | 15 minutes |

**Background Knowledge**

VMware Data Recovery provides the capability to rehearse a virtual machine restore without actually restoring “in place.” When performing a virtual machine restore rehearsal, vDR restores all the necessary data for a virtual machine without the network. In this fashion, the restored virtual machine is not “online.” Users can log on to the virtual machine to verify that files have been properly backed up and can be restored.

**Use Case – Virtual Machine Restore Rehearsal**

Using this feature to perform virtual machine restore rehearsal, IT administrators can periodically verify that the data has been properly backed up and can be restored. This periodic verification can be built into the data protection process so IT administrators can be certain that the virtual machines can be restored properly. Many of the data protection offerings from competitors do not provide this capability to customers.

**Getting Started**

There must be at least one restore point available for the virtual machine that is targeted for restore. Without a restore point, there is no valid backup data from which to restore. To create a restore point, either wait for an associated backup job to finish running during the backup window or manually trigger a backup run.

**Steps to Perform a Virtual Machine Restore Rehearsal**

To perform a virtual machine restore rehearsal:

1. In the vSphere Client, select **Home > Solutions and Applications > VMware Data Recovery**.
2. Right-click a virtual machine to perform restore rehearsal upon. Select **Restore Rehearsal from Last Backup**.
3. The virtual machine restore wizard appears, displaying the source selection followed by **Destinations** selection. Make sure to select the destination from the drop-down list.
4. Click **Restore** to complete the restore rehearsal.
Virtual Machine Restore

| Restore | Virtual machine level restore | Perform a real restore. 1. Select the virtual machine to restore, its restore point and a destination store. 2. Verify the data restored. | 15 minutes |

Background Knowledge

VMware Data Recovery can be used to restore virtual machines to the state captured by the restore points. If the virtual machine uses VMware Virtual Hardware version 7 or higher, vDR uses a technique called Changed Block Tracking to find out which blocks create a differential from the current system and recovers only those blocks.

Use Case – Virtual Machine Restore

In the case of data corruption, it is crucial to be able to restore the protected virtual machines for business continuity. IT administrators can use the restore capability in vDR to restore the virtual machines to a desired state.

Getting Started

There must be at least one restore point available for the virtual machine that is targeted for restore. Without a restore point, there is no valid backup data from which to restore. To create a restore point, either wait for an associated backup job to finish running during the backup window or manually trigger a backup run.

Steps to Perform a Virtual Machine Restore

1. In the vSphere Client, select Home > Solutions and Applications > VMware Data Recovery.
2. Enter the virtual machine name or IP address of the vDR backup appliance. Click Connect.
3. Click the Restore tab. Click the Restore link to launch the virtual machine restore wizard. The virtual machine restore wizard will appear.
Figure 15. Perform a Virtual Machine Restore

4. On the **Source Selection** page, specify a source from which to restore virtual machines. Click **Next**.

![Source Selection](image1)

Figure 16. Select Source (i.e., Restore Point) to Restore From

5. On the **Destination Selection** page, specify how restored machines will be configured. Click **Next**.

![Destination Selection](image2)

Figure 17. Select Virtual Machine to Restore To

6. On the **Ready to Complete** page, review the configuration. Click **Restore**.

### File-Level Restore

| Restore | File-level restore | Perform a file-level restore.  
|---------|--------------------|--------------------------------------------------|----------|
|         |                    | 1. Set up a file-level restore agent.  
|         |                    | 2. Use the file-level restore agent CLI to restore a file.  

**Background Knowledge**

Beyond restoration of a full virtual machine, VMware Data Recovery provides a capability called File-Level Restore (FLR) for restoration of needed files without the requirement to restore the entire virtual machine.
Use Case – File-Level Restore

In a scenario in which it is necessary to recover one or more files from a virtual machine, IT administrators can restore those lost files without restoring the whole virtual machine using vDR. File-Level Restore is desirable because the virtual machine is still functional, it might have drifted since the last backup, and it might have files that do not yet exist in the captured restore points. FLR provides another level of flexibility for data restore.

Getting Started

There must be at least one restore point available for the virtual machine that is targeted for restore. Without a restore point, there is no valid backup data from which to restore. To create a restore point, either wait for an associated backup job to finish running during the backup window or manually trigger a backup run.

To ensure that FLR is properly installed, copy the vdrFileRestore.exe to a location of choice on the virtual machine with the files to be restored. All files required for FLR to function as expected are contained within the vdrFileRestore.exe, which should be copied to c:\FLR. After FLR is started, there is help available from within the tool.

Steps to Perform a File-Level Restore

To perform a file-level restore:

1. Log on to the virtual machine to which files will be restored.

2. Open a command prompt. For example, in a Windows XP virtual machine, click Start > Run, enter cmd, and click OK. Change the directory to the location to which vdrFileRestore.exe was copied, such as c:\FLR.

3. Use the vdrFileRestore.exe to specify the fully qualified domain name (FQDN) for the VMware Data Recovery backup appliance that manages the restore points that contain the files to be restored. For example, to see all available restore points on the appliance named vdrc.thewhites.ca, enter: C:\FLR\vdrFileRestore.exe -a vdrc.thewhites.ca.

After selecting the Login button, this command might return output such as the following:

![Figure 18. Opening Screen with File-Level Restore](image)

4. Using the GUI, select the date of the chosen restore point and let it expand.
5. Select the correlate disk on the date from which files will be recovered. Click the Mount button. The following illustrates what this should look like.

![Figure 19. Mounting a Disk](image)

6. The contents of the disks for the selected restore point can now be browsed. Files can be copied to the virtual machine currently running, as preferred, and to the preferred location.

7. When any required restoration tasks are complete for any used mounted disk image, use the Unmount button to close the connection that `vdrFileRestore` has established with the restore point. All disks will be unmounted and closed, and `vdrFileRestore.exe` will clean up any remaining files it has created for its own functioning when the tool is closed.

### Administration

#### Extend a Destination Store

| Backup | Virtual machine protection | Extend a destination store.  
1. Increase the size of the destination store in the virtual machine settings of the vDR appliance.  
2. Reboot the vDR appliance.  
3. Reconnect to the vDR appliance in the vDR plug-in interface.  
4. Unmount, Extend and Mount the destination store.  
5. Perform an Integrity Check on the destination store. | 15 minutes |
|---------|--------------------------|--------------------------------------------------|

**Background Knowledge**

If there is concern about overprovisioning the size of the destination store, provision just enough space and, using the vDR capability, extend them as needed.

Statistics gathered from lab testing indicate that space requirements will plateau (i.e., remain more or less the same) after some time as long as there are no further additions of new protected virtual machines. Eventually, the amount of space freed by exercising the retention policy will balance the amount of new data added to the destination store during backups.
In this release, vDR requires that to extend a destination store, it first must be unmounted, then extended in the storage configuration tab of the vSphere Client, then extended in the vDR plug-in interface, and then remounted.

Destination datastores should grow by increments (e.g., 10 percent of the original size) each increase, because that increment might be all that is required to accommodate all further backups. VMware does not support contracting destination stores.

**Use Case – Extend a Destination Store**

If storage requirements for a destination store grow, the destination store can be extended until it reaches 1TB.

After extending the destination store, verify the data integrity of the extended destination store by manually running an integrity check.

**Getting Started**

Ensure that a vDR appliance has been properly configured with a destination store, which will then be extended.

**Steps to Extend a Destination Store**

1. In the vSphere Client, select **Inventory > VMs and Templates**.
2. In the inventory, right-click the vDR appliance virtual machine and select **Edit Settings**.
3. Select the hard disk that must be extended (e.g., hard disk 2).
4. Change the **Provisioned Size** to 60GB.
5. Click **OK**.

![Figure 20. Change the Provisioned Size of a Destination Store from 50GB to 60GB](image)

6. Reboot the vDR appliance.
7. In the vSphere Client, select **Home > Solutions and Applications > VMware Data Recovery**.
8. Connect to the vDR appliance.
9. Go to the **Configuration** tab.
10. Select **Destinations**.
11. Select the destination store that was extended in step 4.
12. Click **Unmount**.
13. Click **Extend**.

![Figure 21. Extend a Destination Store After Changing the Size in Virtual Machine Settings](image)
14. Click **Mount**.

![Mount an Extended Destination Store](image)

**Figure 22.** Mount an Extended Destination Store

15. Click **Integrity Check...**

16. Click **Yes**.

![Perform a Manual Integrity Check](image)

**Figure 23.** Perform a Manual Integrity Check

vDR runs a daily automated incremental integrity check and a full check of the entire deduplication store once a week. If damaged restore points are found during the integrity check, the deduplication store is locked. As a result, no backups can be performed until the issues reported by the integrity check are fixed. Damaged restore points must be deleted. In addition, an automated incremental integrity check will run only in the maintenance window. The manual integrity check will run whenever it is started. Refer to the [vDR Administrator’s Guide](http://www.vmware.com/pdf/vdr_20_admin.pdf) for more details.

**Notification**

<table>
<thead>
<tr>
<th>Notification</th>
<th>Configure email alerting</th>
<th>Perform a file-level restore. 1. Set up. 2. Test. 3. Trigger a job.</th>
<th>15 minutes</th>
</tr>
</thead>
</table>

**Background Knowledge**

It is useful to see a daily email containing the status of backups and the destination store.

**Use Case – Notification Alerting**

Generally it is not necessary to use vDR to check whether or not jobs have completed. Sometimes it is important to check, because a destination store might be nearly full or something might have occurred that should be known. An example would be an instance of additional machines unexpectedly being backed up due to their having been added to the same resource pool as one that vDR already protects. Instead of checking each morning using the vDR plug-in, a notification email that summarizes vDR activities can be sent automatically. This informational email can be used to determine whether further investigation of the backup state is required.
Getting Started

You will need to know the electronic mail server name or IP that you wish to direct your email through, as well as the destination address for mailed reports.

Steps to Configure an Email alert

To configure the destination server and email address, use the following steps:

1. In the vSphere Client, select Home > Solutions and Applications > VMware Data Recovery.
2. Enter the virtual machine name or IP address of the backup appliance. Click Connect.
3. Click the Configuration tab. Click the Email link to work with the settings.
4. Use the Properties button to access the configure screen.
5. Now complete the configuration as seen in the following figure.

6. Use the Send test email link to make sure email can be sent and received successfully.
7. The specified To: address will now receive a daily summary of backup and destination activities, as seen in the following example.
Configure maintenance window that doesn’t overlap with the backup policies.
1. Confirm backup policies.
2. Configure maintenance time.
3. Confirm your window of no activity.

Background Knowledge
There are two categories of activities that might be running at the destination. If any of these activities are running, you should not attempt to copy the destinations to other locations such as tape or offsite virtual infrastructure. These two categories are 1) backups/restores and 2) appliance maintenance activities such as Integrity Check and Reclaim operations. It is very advantageous to have the ability to copy the destination offsite. To make it safe to do so, set a backup schedule and an offset maintenance window so there is a period of time with no activities. At that time, it would be safe to make a copy of your destination.

Use Case – Maintenance Window
It is necessary to know when it is safe to copy a destination to another location. This might be for redundancy purposes or to ensure a clean backup copy of the data. This requires a maintenance window that is offset from the backup window, to guarantee a period of time during which no activities are accessing the data on the destination.

Getting Started
You must have a vDR destination store that is properly configured, as well as a backup policy. You must then configure a time range for all backup activities. With this configured, there will now be a time frame to create a maintenance window that doesn’t conflict with these activities. See the following figure, which shows a backup job backup window.
Steps to Configure the Maintenance Window

To configure the maintenance window, use the following steps:

1. In the vSphere Client, select **Home > Solutions and Applications > VMware Data Recovery**.
2. Enter the virtual machine name or IP address of the backup appliance. Click **Connect**.
3. Click the **Configuration** tab.
4. Select the **Destinations** option from the left side of the screen.
5. Highlight the destination that you want to create a maintenance window.
6. Now select the **Maintenance Schedule** option.
7. After the **Maintenance Schedule** option is selected, you can configure the maintenance window.
8. If the default backup window is used, you can use the default maintenance schedule, which is seen in the following figure.
9. This will provide a time frame from 7 a.m. to 9 a.m. for copying the destination to another location where there will be no activity.
Conclusion

VMware Data Recovery is an effective data protection tool for small and medium businesses. It enables quick, simple and complete data protection for virtual machines, incorporating capabilities such as block-based data deduplication and performing only incremental backups after the first full backup, to maximize storage efficiency. This guide provides you with step-by-step instructions on how to perform backup and restore operations using vDR. These operations are straightforward and easy to perform. After going through the evaluation exercises in this guide, you should be able to make the right choice to implement your data protection solutions in your virtual datacenter.