© 2013 Veeam Software.
All rights reserved. All trademarks are the property of their respective owners.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means, without written permission from Veeam Software Inc (Veeam). The information contained in this document represents the current view of Veeam on the issue discussed as of the date of publication and is subject to change without notice. Veeam shall not be liable for technical or editorial errors or omissions contained herein. Veeam makes no warranties, express or implied, in this document. Veeam may have patents, patent applications, trademark, copyright, or other intellectual property rights covering the subject matter of this document. All other trademarks mentioned herein are the property of their respective owners. Except as expressly provided in any written license agreement from Veeam, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Important! Please read the End User Software License Agreement before using the accompanying software program(s). Using any part of the software indicates that you accept the terms of the End User Software License Agreement.
CONTENTS

GETTING STARTED ........................................................................................................... 4
WHAT IS VPOWER ............................................................................................................. 6
REFERENCE ENVIRONMENT ............................................................................................. 7
   BACKUP INFRASTRUCTURE SETUP ............................................................................................ 7
   vPOWER SETTINGS .................................................................................................................. 7
      Email Settings ..................................................................................................................... 11
   SAMPLE TEST LAB ................................................................................................................ 12
VPOWER CAPABILITIES .................................................................................................... 13
   PERFORMING INSTANT VM RECOVERY .................................................................................. 14
   PERFORMING SUREBACKUP RECOVERY VERIFICATION ....................................................... 20
      Step 1: Create a Virtual Lab ................................................................................................ 21
      Step 2: Create an Application Group ............................................................................... 32
      Step 3: Create and Run a SureBackup Job ........................................................................ 37
   PERFORMING UNIVERSAL APPLICATION-ITEM RECOVERY .................................................. 46
   USING ON-DEMAND SANDBOX .......................................................................................... 54
   PERFORMING UNIVERSAL FILE-LEVEL RECOVERY .............................................................. 61
GETTING STARTED

About Veeam Backup & Replication

Veeam® Backup & Replication™ is a data protection and disaster recovery solution for virtual environments of any size and complexity. Veeam Backup & Replication provides fast, flexible and reliable recovery of virtualized applications and data. It unifies backup and replication in a single solution, increases the value of backup and reinvents data protection for VMware vSphere and Microsoft Hyper-V virtual environments. Veeam Backup & Replication supports your entire virtual infrastructure with industry leading features such as 2-in-1 backup and replication, instant file-level recovery and streamlined VM recovery, scalability, built-in deduplication, centralized management and many more.

About This Guide

This guide will help you become familiar with vPower — the breakthrough technology in Veeam Backup & Replication that lets you run a virtual machine (VM) directly from a compressed and deduplicated backup file located on regular backup storage.

It is highly recommended that you go through the Veeam Backup & Replication Evaluator’s Guide for VMware at http://www.veeam.com/documentation-guides-datasheets.html before you start working with this guide. Otherwise some concepts may be new and complicated to you.

Intended Audience

The document is intended for IT professionals who are looking to deploy Veeam Backup & Replication to protect their VMware virtual environment. This guide will be of interest to VMware administrators, consultants and analysts who want to evaluate vPower capabilities in Veeam Backup & Replication.

Document Structure

The guide provides a set of self-guided evaluation exercises that you should follow to familiarize yourself with vPower. Every evaluation exercise contains a short feature overview, an evaluation case and evaluation procedure as well as comments on validation of the exercise results.

The guide is comprised of three major parts:

- **What is vPower.** This section provides a general description of the vPower technology and features enabled by it.

- **Reference Environment.** This section describes requirements for a test lab that you need to provision to successfully perform evaluation tasks.

- **vPower Capabilities.** This section describes evaluation cases covering the most typical data protection and disaster recovery tasks that you can perform to evaluate the vPower technology.
Help and Support

This guide provides a high-level overview of the vPower technology and should be regarded as a supplement to existing technical documentation. You can find the complete set of documentation on the Resources web page at http://www.veeam.com/documentation-guides-datasheets.html.

For technical support and assistance, use the following resources:

- Customer Center: cp.veeam.com. Should you have a technical concern, suggestion or question, please visit our Customer Center Portal to open a case, search our knowledge base, reference documentation, manage your license or obtain the latest product release.
WHAT IS VPOWER

vPower is Veeam’s breakthrough technology that lets you run a VM directly from a compressed and deduplicated backup file residing on a regular disk-based backup storage. With vPower, Veeam overcomes limitation of traditional backup and takes data protection to the new level.

The key construct of vPower is vPower NFS server, Veeam’s proprietary technology. From the technical point of view, vPower NFS is a Windows service that runs on a Windows-based machine and enables this machine to act as an NFS server.

On the vPower NFS server Veeam Backup & Replication creates a special directory — vPower NFS datastore. When you start a VM from the backup, Veeam Backup & Replication “publishes” the VMDK files of VMs from the backup on the vPower NFS datastore. Technically, Veeam Backup & Replication emulates the presence of VMDK files on the vPower NFS datastore: the VMDK files themselves are still located in the backup file on the repository.

The vPower NFS datastore is then mounted to the ESX(i) host. As a result, the ESX(i) host can “see” backed up VM images via the vPower NFS datastore and work with them as with regular VMDK files: the emulated VMDK files function as pointers to the real VMDK files in the backup.

Backed up VMs presented to ESX(i) hosts always remain in the read-only state. This way, Veeam Backup & Replication guarantees there are no unexpected modifications to the content of the backup file. All changes made to VMs while they are running are stored to specific cache, or redo logs. The redo logs can be stored to the vPower NFS datastore or re-directed to any datastore in your environment, depending on the use case scenario. After you finish working with VMs started from backups, the redo logs are cleared.

vPower enables the following advanced capabilities:

- **Instant VM Recovery**: you can start a VM from the backup file in a couple of seconds.
- **SureBackup® recovery verification**: you can verify every VM in every backup for recoverability by testing the state of a VM, OS and applications running inside the VM.
- **U-AIR® (Universal Application-Item Recovery)**: you can recover application items from any virtualized application.
- **On-demand sandbox**: you can start one VM or a group of VMs in the isolated virtual lab, aside from your production environment, and use them for testing, troubleshooting, applying patches and so on.
- **Instant File-Level Restore (IFLR)**: you can recover guest OS files and folders from any file system.
REFERENCE ENVIRONMENT

To successfully use this guide and evaluate vPower capabilities, you need to provision the environment, a test lab, that you will use to follow evaluation scenarios.

Backup Infrastructure Setup

For this guide, you need to deploy the backup infrastructure as described in the Veeam Backup & Replication Evaluator’s Guide for VMware at www.veeam.com/vmware-esx-backup/resources.html. Please make sure that all components in your backup infrastructure meet the requirements specified in the Reference Environment section and that you have carefully followed all exercises from the Backup Infrastructure Setup section of Veeam Backup & Replication Evaluator’s Guide for VMware.

You can use a simple deployment or a distributed deployment for the backup infrastructure. In a nutshell, you should have the following components in your backup infrastructure:

- Veeam Backup server
- ESX(i) host(s) added to the Veeam Backup & Replication console
- Backup proxy (default or dedicated)
- Backup repository (default or dedicated)

To evaluate vPower capabilities, you additionally need to set up vPower-specific settings for some of the backup infrastructure components. Check the vPower Settings section and configure your backup infrastructure as described in the section.

You can also configure general email settings to receive email notifications with job results during evaluation.

vPower Settings

Before you proceed to evaluating vPower capabilities, make sure that you have configured the following settings required by the vPower functionality.

- Select a Windows-based server to function as a vPower NFS server and deploy the vPower NFS server on it.
- Select an ESX(i) host on which the virtual lab will be created. The virtual lab is required for SureBackup Recovery Verification, U-AIR and On-Demand Sandbox scenarios.
- Make sure that ports used by the vPower NFS service are open.
- (Optional) Make sure that VMs you plan to use have VMware Tools installed.
vPower NFS Server

The vPower NFS server is the core vPower component required for all evaluation exercises described in this guide. You can use one of the following scenarios for deploying the vPower NFS server (starting from the most efficient):

- If you use a dedicated Windows-based repository to store backup files, it is recommended that you deploy the vPower NFS server directly on this backup repository. In this case, the vPower NFS service will have a direct connection to the backups stored on this backup repository, which will help optimize the vPower performance.
- If you use the default backup repository on the Veeam Backup server, deploy the vPower NFS server on the Veeam Backup server.
- If you use a Linux-based repository or a CIFS share for storing backups, deploy the vPower NFS server on the Veeam Backup server or any Windows-based machine in your environment (either physical or virtual).

Important! It is strongly recommended that you enable the vPower NFS server on the Windows machine that is located in the same network as the ESX(i) host on which the virtual lab is created. Otherwise, you will need to manually change the routing settings on the ESX(i) host. To learn more, see the Recovery Verification section in the Veeam Backup & Replication User Guide for VMware at www.veeam.com/vmware-esx-backup/resources.html.

To deploy the vPower NFS server, follow the next steps:

1. Make sure that the Windows-based machine on which you plan to deploy the vPower NFS server is added to the Veeam Backup & Replication console.
2. In Veeam Backup & Replication, open the Backup Infrastructure view.
3. Select Backup Repositories in the inventory pane.
4. In the working area, right-click the repository to which you plan to store backups and select Properties.
5. Move on to the vPower NFS step of the wizard.
6. Make sure that the Enable vPower NFS server check box is selected.
7. From the list below, select the Windows-based server on which the vPower NFS server will be enabled.

8. Specify the folder for the vPower NFS datastore. You should have at least 10 GB of free disk space available in this folder. Note that you cannot create the vPower NFS datastore in a folder that you have mapped to the drive letter.

9. Finish working with the wizard.

**ESX(i) Host for the Virtual Lab**

VMs run from backups are started in the virtual lab – a fenced-off environment that is created using available resources of your virtual environment. The virtual lab can be created on an ESX(i) host where VM you want to back up reside or any other ESX(i) host in your environment. The ESX(i) host on which you plan to deploy a virtual lab must have the VMkernel port group that can communicate with vPower NFS server. VMkernel port groups are available on ESXi hosts by default. ESX hosts, however, do not have VMkernel port groups by default. If you decide to use an ESX host for the virtual lab, you will have to add the VMkernel port group onto it to be able to connect to the vPower NFS server.

To learn about adding a VMkernel port group onto an ESX host, see http://www.youtube.com/watch?v=YCzldd6wcU.

Make sure that you can ping the VMkernel IP from the vPower NFS server and/or ping the vPower NFS server from the ESX host. To ping the vPower NFS server from the ESX host, use the `vmkping` utility on the ESX host. `vmkping` is similar to the ping tool; the only difference is that ICMP packets are sent via the VMkernel interface rather than the service console interface.

To learn more, see http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1003728.
Ports

Make sure that the following ports are open:

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veeam Backup server</td>
<td>Windows server</td>
<td>TCP</td>
<td>6161</td>
<td>Default port used by the Veeam vPower NFS Service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP</td>
<td>111, 2049+, 1058+</td>
<td>Standard NFS ports*</td>
</tr>
</tbody>
</table>

*If ports 2049 and 1058 are occupied, the succeeding port numbers will be used.

If the default ports are occupied, you can use other ports. To edit port numbers:

1. In Veeam Backup & Replication, open the Backup Infrastructure view.
2. Select Backup Repositories in the inventory pane.
3. In the working area, right-click the repository where the backup files reside and select Properties.
4. Move on to the vPower NFS step of the wizard.
5. Click Ports and edit port values as needed.

VMs

To perform all tests during SureBackup recovery verification, make sure the VMs that you plan to use have VMware Tools installed. Otherwise, the heartbeat test will not be performed and the SureBackup job will complete with the Warning status.
Email Settings

To receive email notifications with the SureBackup job results, configure main email settings in Veeam Backup & Replication:

1. In Veeam Backup & Replication, select **Options** from the main menu.
2. On the **Email Settings** tab, specify the SMTP settings as needed.

![Image of Email Settings configuration window]
Sample Test Lab

For this evaluator's guide, test lab with the following configuration is used:

- Veeam Backup server is deployed in a virtual machine on the ESXi host.
- Backup proxy is deployed in a virtual machine with the HotAdd access to backed up VMs.
- Backup repository is a physical Windows-based VM with a locally attached storage. The vPower NFS server is enabled on the backup repository. The backup repository (vPower NFS server) is located in the same network as the ESX(i) host on which the virtual lab is created.
- VMs are located on two ESXi hosts. One ESXi host is used as a location for a virtual lab.
- VMs are located in two different networks: 172.16.x.x, and 192.168.x.x. Using VMs from different networks will let you configure advanced networking settings for the virtual lab and fully evaluate the virtual lab capabilities. However, you can use VMs that belong to the same network as well.

For this evaluator's guide, the following VMs are used:

- Virtualized Exchange server used for Instant Recovery and SureBackup recovery verification
- Virtualized Domain Controller used for SureBackup recovery verification and U-AIR
- Virtualized DNS server used for U-AIR
- Virtualized file server used for on-demand sandbox
- Two VMs running Novell Netware OS used for IFLR

The picture above illustrates one of variants of a distributed deployment scenario. For evaluation of vPower capabilities, you can use a simpler configuration. However, you need to make sure that your test lab meets requirements listed in the Backup Infrastructure Setup section in the Veeam Backup & Replication Evaluator’s Guide for VMware Environments at www.veeam.com/vmware-esx-backup/resources.html. Additionally, make sure that you have configured all settings listed in the vPower Settings section of this guide.
VPOWER CAPABILITIES

This section describes a set of exercises that you can perform to get to know the vPower functionality.

Exercise List

To evaluate the product capabilities enabled by vPower, perform the following exercises:

<table>
<thead>
<tr>
<th>Exercise</th>
<th>Description</th>
<th>Time Estimates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performing Instant VM Recovery</td>
<td>Immediately restore a VM by running it directly from an image-level backup.</td>
<td>1-2 minutes</td>
</tr>
<tr>
<td>Performing SureBackup Recovery Verification</td>
<td>Verify recoverability of a backup file (by the example of a Microsoft Exchange server).</td>
<td>Varies*</td>
</tr>
<tr>
<td>Performing Universal Application-Item Recovery (U-AIR)</td>
<td>Restore application objects directly from an image-level backup (by the example of the Active Directory U-AIR wizard).</td>
<td>3-5 minutes</td>
</tr>
<tr>
<td>Using On-Demand Sandbox</td>
<td>Create an isolated virtual lab and start there a VM from an image-level backup.</td>
<td>3-5 minutes</td>
</tr>
<tr>
<td>Performing universal file-level recovery</td>
<td>Restore files and folders from a VM guest OS (by the example of Novell NetWare VM).</td>
<td>3-5 minutes</td>
</tr>
</tbody>
</table>

* The actual time required to perform this exercise depends on your test lab configuration, the hardware and software being used and the size of processed VMs.
Performing Instant VM Recovery

Insight into Instant VM Recovery

With Instant VM Recovery, you can restore a VM from a backup in a couple of seconds. Instant VM Recovery lets you run a VM directly from a compressed and deduplicated backup file located on a regular backup storage. You can use Instant VM Recovery to restore a failed VM to the production environment or start a VM from the backup and use it for testing.

Instant VM Recovery uses a regular image-level backup created with Veeam Backup & Replication. You can start the VM from the latest backup or from any necessary restore point.

When you perform Instant VM Recovery, Veeam Backup & Replication mounts the VM image from the archived backup to the selected ESX(i) host. The backup file itself remains in read-only state. All changes that you make to the VM while it is running are written to redo logs. These redo logs can be stored to the vPower NFS datastore or redirected to any datastore in your environment.

Instant VM Recovery provides the best RTO and the highest SLA for VMs. You can think of Instant VM Recovery as of having a “spare tire” for a failed VM. Because you do not have to extract VM data from the backup and copy it to the production storage, the restore process is extremely fast. It virtually equals the time needed to start the VM and varies from several seconds to a couple of minutes.

Evaluation Case

In this exercise, you will run a VM directly from a backup file and start it on an ESX(i) host. The VM will be registered under its initial name with the _restored suffix appended. The redo logs will be stored on the default NFS storage.

After you validate that the VM is successfully started, you can migrate the VM to production or terminate the Instant VM Recovery session.

Prerequisites

- Make sure that you have at least 10 GB of free disk space on the vPower NFS datastore to store redo logs for the restored VM. By default, the redo logs are written to the C:\ProgramData\Veeam\Backup\NfsDatastore folder on the vPower NFS server.
- Make sure that the original VM is powered off. If you restore the VM to the same network where the original VM runs, there may be conflict between the original VM and the restored VM.
Procedure

1. Create a backup of the necessary VM as described in Veeam Backup & Replication Evaluator’s Guide for VMware at www.veeam.com/vmware-esx-backup/resources.html. To check if the backup has been successfully created, open the Backup & Replication view, select the Backups node in the inventory pane and expand the backup job to verify that there is at least one restore point available for the VM.

2. Open the Backup & Replication view.

3. In the inventory pane, select the Backups node.

4. In the working area, expand the necessary backup job. Right-click the VM in the job and select Instant VM recovery.

5. At the Restore point step, select the point to which you want to restore the VM.

![Instant Recovery](image-url)
6. At the **Restore Mode** step, select **Restore to a new location, or with different settings**.

![Restore Mode](image)

- **Virtual Machine**
  - **Restore Point**
- **Restore Mode**
  - **Restore to the original location**
    - Quickly restore restore of selected VMs to the original location, and with the original name and settings. This option minimizes the chance of user input error.
  - **Restore to a new location, or with different settings**
    - Customize restored VM location, and change its settings. The wizard will automatically populate all contexts with the original VM settings as the default settings.

![Destination](image)

- **Destination**
  - **Host**
  - **VM folder**
- **Restored VM name**
  - **Restored VM name**
- **Resource pool**
  - **Production**
  - **Sales**
  - **Test**

7. At the **Destination** step, select the ESX(i) host on which the VM should be registered. In the **Resource pool** box, select the resource pool to which the restored VM should belong.

8. In the **Restored VM name** field, add the `_restored` suffix to the VM name.
9. At the **Datastore** step, leave the **Redirect virtual disk updates** check box not selected. This will let you use Storage vMotion to migrate the VM to production after the VM is recovered from the backup.

![Instant Recovery dialog box](image)

10. At the **Ready to Apply** step, select the **Connect VM to network** and **Power on VM automatically** check boxes.

![Instant Recovery dialog box](image)

11. Click **Finish** to start Instant VM Recovery.
Validation

1. Open vSphere Client and make sure that the restored VM is started on the ESX(i) host you selected.

2. In Veeam Backup & Replication, open **Backup & Replication** view, select the **Instant Recovery** node in the inventory pane and make sure that the Instant VM Recovery session is available in the working area.

3. Open the vPower NFS datastore: by default, C:\ProgramData\Veeam\Backup\NfsDatastore folder on the vPower NFS server, and check if emulated VM files and redo logs (cache file) are available there.
Finalizing Instant VM Recovery

After Instant VM Recovery is successfully completed, you can do one of the following:

- **Migrate the VM to production.** You can use this scenario if you have recovered a failed VM to the production ESX(i) host and want to permanently move the VM files to the production storage.

- **Terminate the Instant VM Recovery session.** You can use this scenario if you have recovered a VM for testing purposes and want to power it off after testing is completed.

**Migrating the VM to production**

For VM migration, you can use VMware Storage vMotion, replicate or copy a VM to production with Veeam Backup & Replication or use Veeam’s Quick Migration. When you migrate the VM to the production, you move the VM contents from the backup file to the production storage. The VM data is pulled from the backup and consolidated with changes made to the VM (redo logs). As a result, you get the VM in the latest state in your production environment.

To migrate the restored VM with Quick Migration:

1. Open the **Backup & Replication** view in Veeam Backup & Replication.
2. In the inventory pane, select **Instant Recovery**.
3. In the working area, right-click the name of the recovered VM and select **Migrate to production**.
4. The **Quick Migration** wizard will be launched. Follow the wizard steps to move the VM to your production environment. To learn more about quick migration, see the Veeam Backup & Replication User Guide at [www.veeam.com/vmware-esx-backup/resources.html](http://www.veeam.com/vmware-esx-backup/resources.html).

After quick migration is complete, terminate the Instant VM Recovery session as described below.

**Terminating the Instant VM Recovery session**

When you terminate the Instant VM recovery session, the VM is unpublished from the ESX(i) host and redo logs are cleared from the vPower NFS datastore.

To terminate the current Instant VM Recovery session:

1. Open the **Backup & Replication** view in Veeam Backup & Replication.
2. In the inventory pane, select **Instant Recovery**.
3. In the working area, right-click the name of the recovered VM and select **Stop publishing**.
Performing SureBackup Recovery Verification

Insight into SureBackup

SureBackup is Veeam’s concept that lets you test your backups for recoverability. Traditional backup tools simply verify integrity of backup files. In practice, however, such backups do not necessarily work.

In contrast to traditional backup tools, Veeam Backup & Replication performs “live” verification of a VM in the backup file. It boots the VM from the backup, starts applications running inside this VM and checks if these applications work well.

Veeam Backup & Replication uses a regular image-based backup for SureBackup recovery verification. You can verify a VM from the latest backup or from any necessary restore point. Veeam Backup & Replication performs the following tests against the verified VM:

- **Heartbeat test**: Veeam Backup & Replication starts the VM and waits for a heartbeat signal from VMware Tools installed inside the VM.
- **Ping test**: Veeam Backup & Replication checks if the started VM can respond to ping requests from the Veeam Backup server.
- **Application test**: Veeam Backup & Replication waits for applications to start inside the VM and runs a script that checks application-specific network ports. For example, to verify Active Directory, Veeam Backup & Replication probes port 389 for a response. You can run pre-defined scripts to verify applications or use your own custom scripts.

For SureBackup recovery verification, Veeam leverages vPower and virtual lab technologies. To verify a VM, Veeam Backup & Replication starts it directly from the compressed and deduplicated backup file in the isolated virtual lab. During verification, VM backups remain in the read-only state. All changes made to the VMs are written to redo logs that are stored on a selected datastore in your environment.

If the verified VM runs an independent application, it can be started in the virtual lab alone. If the verified VM is dependent on other services and applications, it is started in the virtual lab together with other VMs running applications and services necessary for the VM functioning. For example, if you want to verify an Exchange VM, you also need to start the Domain Controller and DNS VMs in the virtual lab to make sure that Exchange is working in a proper way.

The recovery verification process is job-based and fully automated. You can create a SureBackup job and schedule it to run regularly right after the backup is created. This way, you can verify every VM in every backup and guarantee all your backups work well.

**Evaluation Case**

In this exercise, you will verify a Microsoft Exchange VM*. To perform recovery verification, you will complete three steps:

- **Step 1**: Create a virtual lab in which testing will be performed.
- **Step 2**: Create an application group containing all VMs on which the Microsoft Exchange VM is dependent.
- **Step 3**: Create a SureBackup job. When you run a SureBackup job, Veeam Backup & Replication will automatically start the virtual lab, run VMs from the application group in the virtual lab and verify the started VMs.

* You can use this exercise to verify any VM in your virtual environment. Just make sure that you add to the application group all VMs on which the verified VM is dependent.
Step 1: Create a Virtual Lab

A virtual lab is an isolated environment that Veeam Backup & Replication uses for recovery verification, application-item recovery and so on.

The networking scheme of the virtual lab resembles the networking scheme of your production environment. Technically, in the virtual lab you have a copy of your production environment fenced off from the outer world. For example, if VMs in your production environment are connected to two networks, the virtual lab will also have two networks. The networks in the virtual lab are mapped to those in the production environment.

When you create a virtual lab, Veeam Backup & Replication automatically adds a number of new instances on the ESX(i) host where the virtual lab resides:

- A new resource pool
- A new VM folder
- A new vSwitch

The vSwitch is only used by the VMs started in the virtual lab: there is no routing outside the virtual lab to other networks.

To let you access VMs running in the virtual lab from the production network, Veeam Backup & Replication uses a special proxy appliance. The proxy appliance is a Linux-based auxiliary VM created in the virtual lab. The proxy appliance is connected to both the production network and to the isolated network and so has visibility of the production environment and the virtual lab. In essence, the proxy appliance acts as a gateway between the two networks, routing requests from the outside to the VMs in the virtual lab.

VMs in the virtual lab are started with the same IP addresses as in the production network. This lets VMs in the virtual lab function just as if they run in the production environment.

To let the traffic into the virtual lab, Veeam Backup & Replication uses masquerade IP addressing. Every VM in the virtual lab has a masquerade IP address, along with the IP address from the production network. The masquerade IP address is similar to the IP address in the production network: for example, if the IP address of a VM is 172.16.1.13, the masquerade IP address may be 172.18.1.13.
The masquerade IP address can be thought of as an entry point to the VM in the virtual lab from the production side. When you want to access a specific VM in the virtual lab, Veeam Backup & Replication addresses it by its masquerade IP address.

At the moment you start a virtual lab, Veeam Backup & Replication creates a static route in the routing table on the Veeam Backup server. This static route designates the masquerade network traffic to the proxy appliance. The proxy appliance here acts as a NAT device: it resolves the masquerade IP address, replaces it with “real” IP address of a VM in the production network and then directs the request to the necessary VM in the virtual lab. The static route is non-persistent: when you power off the virtual lab, the route is removed from the routing table on the Veeam Backup server.

For example, your Microsoft Exchange server has IP address 172.16.10.13 in the production network. If you run this Microsoft Exchange VM from the backup in the virtual lab, the Microsoft Exchange VM in the virtual lab is assigned a masquerade IP address, for example, 172.18.10.13. Correspondingly, from the production side, the Microsoft Exchange VM running in the virtual lab has IP address 172.18.10.13.

According to this routing table, when you try to access the Microsoft Exchange VM in the virtual lab by IP address 172.18.10.13, Veeam Backup & Replication first sends the request to the proxy appliance (in the picture below, the proxy appliance has IP address 172.16.11.142). The proxy appliance resolves the IP address, replaces it with “real” IP address of the Microsoft Exchange VM in the virtual lab, 172.16.10.13, and routes the request to the Microsoft Exchange VM in the virtual lab.

![Interface List](image)

**Note** If you want to access the VM in the virtual lab manually, for example, to perform some testing, make sure that routing is properly set up on your machine. In case you access the VM in the virtual lab from the Veeam Backup & Replication console, you do not need to perform any additional configuration: Veeam Backup & Replication automatically updates the routing table on the Veeam Backup server. In case you want to access the VM in the virtual lab from some other machine, you need to manually add a corresponding route to the routing table on that machine.

In this exercise, you will create a virtual lab in which the Microsoft Exchange VM will be verified. The Microsoft Exchange VM will be started together with the Domain Controller that additionally performs the role of Global Catalog. The Microsoft Exchange server and the Domain Controller are located in two different networks. For this reason, the virtual lab will also have two networks that will be mapped to corresponding networks in the production environment.*

*If all of your VMs are located in the same network, when following this exercise, choose the basic networking scheme at the Networking step of the New Virtual Lab wizard. Veeam Backup & Replication will then
automatically set up all necessary network settings for your virtual lab and you will not have to specify them manually.

**Prerequisites**

- Make sure that you have a valid trial or Enterprise license for Veeam Backup & Replication installed. If you have a Standard license, you will not be able to perform SureBackup recovery verification.
- The ESX(i) host on which you plan to deploy a virtual lab must have a VMkernel interface. Otherwise mounting of the vPower NFS datastore on the ESX(i) host will fail. To learn more, see the vPower Settings section.
- Make sure that ports used by the NFS service are open on the ESX(i) host. To learn more, see the vPower Settings section.

**Procedure**

1. In Veeam Backup & Replication, open the **Backup Infrastructure** view.
2. Right-click the **Virtual Labs** node under **SureBackup** in the inventory tree and select **Add Virtual Lab**.
3. Specify a name for the virtual lab.
4. At the **Host** step of the wizard, select an ESX(i) host on which the virtual lab should be created.
5. At the **Datastore** step of the wizard, choose a datastore to which redo logs of VMs started in the virtual lab should be written.

6. At the **Proxy** step of the wizard, leave the default proxy settings selected. In the **Production network connection** section, make sure that the correct production network is selected.
7. At the **Networking** step of the wizard, select **Advanced**. This type of networking is recommended if VMs you plan to start in the virtual lab are located in different networks. If all of your VMs are located in the same network, select **Basic** and finish working with the wizard. Veeam Backup & Replication will configure all network settings of the virtual lab automatically.

![Networking Step](image)

8. At the **Isolated Networks** step of the wizard, you should specify what isolated networks should be created in the virtual lab and map these networks to corresponding production networks. To add an isolated network to the virtual lab, click **Add**.

9. Click **Browse**. Select the necessary network in the production environment. This production network will be mapped to the isolated network you are creating.
10. In the **Isolated network** field, specify a name for the network created in the virtual lab. By default, Veeam Backup & Replication sets the virtual lab name to the *Lab name + network name* value.

11. At the **Network Settings** step of the wizard, you should define main settings for isolated networks in the virtual lab.
The proxy appliance connects to isolated networks in the virtual lab using vNIC adapters. For every isolated network in the virtual lab, you need to add one vNIC adapter onto the proxy appliance.

To add a vNIC adapter, click **Add**. From the network list at the top, select the network for which you are adding the adapter.

12. In the **IP address** field, specify the IP address that the proxy appliance will have in the isolated network. In the **Mask** field, define the network mask.

The IP address of the proxy appliance in the virtual lab is typically the same as the IP address of the default gateway in the production network. To get the IP address of the default gateway and the network mask of the production network, start the command prompt on any machine connected to the corresponding production network and type `ipconfig`: 

```
Connection-specific DNS Suffix : veeam.lab
IP Address : 172.36.11.38
Subnet Mask : 255.255.0.0
Default Gateway : 172.36.0.1
```
13. After you specify the IP address for the proxy appliance and the network mask, Veeam Backup & Replication will automatically generate a masquerade network IP address for the network in the virtual lab. You can adjust this IP address if necessary. Note that the IP address for the masquerade network should be unique in your environment.

14. Select the **Enable DHCP service on this adaptor** check box and click **OK**.

15. Repeat the procedure for all isolated networks that you have created. In this exercise, we have added two vNIC adapters: the first one to communicate with the VM Network in which the Microsoft Exchange VM will be started and the second one to communicate with the VM Network2 in which the Domain Controller VM will be started.
16. Select the **Route network traffic between vNICs** check box to enable communication between the two isolated networks in the virtual lab.

17. Follow the next steps of the wizard without changing default settings. At the last step, click **Finish**.

**Validation**

To check if the virtual lab has been successfully created:

1. Open the **Backup Infrastructure** view.
2. Select the **Virtual Labs** node under **SureBackup** in the inventory pane and make sure that the virtual lab is available in the working area.
3. Open vSphere Client and make sure that a new resource pool with the proxy appliance is available on the selected ESX(i) host.
4. Open the networking settings of the ESX(i) host on which the virtual lab has been created: in vSphere Client, select the ESX(i) host in the inventory tree, click the **Configuration** tab and select **Networking** under **Hardware**.

Make sure that a new vSwitch has been added to the ESX(i) host and that the proxy appliance is connected to all networks that you have created.
Step 2: Create an Application Group

An application group contains VMs on which the verified VM is dependent. These are VMs that enable full functionality of the verified VM.

During a SureBackup job, Veeam Backup & Replication starts in the virtual lab VMs from the application group in the required order and performs necessary tests against them. This way, Veeam Backup & Replication creates the necessary environment to start the verified VM. Only after all VMs from the application group are started and tested, the verified VM itself is started in the virtual lab.

For example, if you want to verify a SharePoint VM, you first need to start in the virtual lab the Domain Controller and the SQL server on which SharePoint is dependent. Subsequently, the application group for SharePoint verification will contain the Domain Controller and the SQL server VMs.

In this exercise, the application group will contain only one VM — the Domain Controller with the role of Global Catalog used by the Microsoft Exchange VM.

Prerequisites

- Make sure that all applications and services on which the verified VM is dependent are virtualized in your environment. For this exercise, you should have a virtualized Domain Controller. The Domain Controller should additionally have a role of the Global Catalog.
- For the heartbeat test to pass successfully, make sure that VMware Tools are installed in all VMs you plan to add to the application group.
- Create backups of all VMs you plan to include into the application group as described in Veeam Backup & Replication Evaluator’s Guide for VMware: www.veeam.com/vmware-esx-backup/resources.html. To check if the backups have been successfully created, open the Backup & Replication view, select the Backups node in the inventory pane and expand the backup job to verify that there is at least one restore point available for the VM.

Procedure

1. In Veeam Backup & Replication, open the Backup Infrastructure view.
2. Right-click the Application Groups node under SureBackup in the inventory tree and select Add Application Group.
3. Specify a name for the application group.
4. At the **Virtual Machines** step of the wizard, click **Add VMs > From Backups**. To quickly find the VM, use the search field at the bottom of the window.

5. Select the VM and click **Add**.
6. From the VM list, select the added VM and click **Edit**.

7. On the **Roles** tab, select check boxes next to the roles that the VM performs: **Domain Controller** and **Global Catalog**.

8. Click the **Startup Options** tab. Check the settings in the **Memory** and **Startup time** sections. Note that if the application running in the VM takes much time to start, you may need to increase the startup time.

9. Make sure that the **VMware Tools heartbeat is present** and **VM responds to ping on any network adaptor** check boxes are selected. Otherwise, the heartbeat and ping tests will not be performed against the VM.
10. Click the **Test Scripts** tab. When you select a VM role, Veeam Backup & Replication automatically assigns a predefined script that will be run to verify that the application inside the VM is working normally.

In this exercise, Veeam Backup & Replication will run a predefined script that will probe standard ports of the Domain Controller and Global Catalog: 389 and 3268.

11. If you verify a VM that has some other role not listed on the **Role** tab, click **Add**. In the **Test Script** window, select **Use the following test script**.

12. In the **Name field**, specify a name for the script.
13. In the **Path** field, define the path to the executable script file that should be run.
   
   - If you have your own custom script to verify the application, define the path to it.
   - If you do not have a custom script, you can use Veeam's standard script that probes the application communication ports. The script located in the installation folder of Veeam Backup & Replication: by default, `$Program Files\Veeam\Backup and Replication\Veeam.Backup.ConnectionTester.exe`. Specify this path in the **Path** field. In the **Arguments** field, specify the IP address of the tested VM (you can specify in explicitly or use the `%vm_ip%` variable) and the port that you want to probe.

14. Repeat steps 5-13 for all VMs that you have added to the application group.

15. Follow the next steps of the wizard. At the last step, click **Finish**.

**Validation**

To check if the application group has been successfully created:

1. Open the **Backup Infrastructure** view.

2. Select the **Application Groups** node under **SureBackup** in the inventory pane and make sure that the application group is available in the working area.
Step 3: Create and Run a SureBackup Job

In this exercise, you will configure a SureBackup job and run it. When you start the SureBackup job, Veeam Backup & Replication will start the virtual lab, run there VMs from the application group and test them; then Veeam Backup & Replication will start the verified VM and test it.

Prerequisites

- For the heartbeat test to pass successfully, make sure that VMware Tools are installed in the verified VM.
- Create a backup of the verified VM as described in Evaluator’s Guide for VMware at www.veeam.com/vmware-esx-backup/resources.html. To check if the backup has been successfully created, open the Backup & Replication view, select the Backups node in the inventory pane and expand the backup job to verify that there is at least one restore point available for the VM.

Note that Veeam Backup & Replication verifies all VMs in the backup job you select for testing. For time economy, it is recommended that you include in the backup job only those VM(s) you want to verify.

- (Optional) To receive an email notification when a SureBackup job is completed, specify global email notification settings. To learn more, see the Email Settings section.

Procedure

1. In Veeam Backup & Replication, open the Backup & Replication view.
2. On the Home tab, click the SureBackup Job button.
3. Specify a name for the SureBackup job.

![New SureBackup Job](image)
4. At the **Virtual Lab** step of the wizard, select the virtual lab that you have configured.
5. At the **Application Group** step of the wizard, select the application group that you have created.

6. At the **Backup job** step of the wizard, select the **Link backup jobs** check box.

7. Click **Add** and select the backup job with the VM you want to verify.
8. Select the added backup job in the list and click **Edit**.

9. In the **Verification Options** window, select the check box next to the role that the verified VM performs: **Mail Server**.

![Verification Options window]

16. Click the **Startup Options** tab. Check the settings in the **Memory** and **Startup time** sections. Note that if the application running in the VM takes much time to start, you may need to increase the startup time.

17. Make sure that the **VMware Tools heartbeat is present** and **VM responds to ping on any network adaptor** check boxes are selected. Otherwise, the heartbeat and ping tests will not be performed against the VM.

![Startup Options tab]

18. Click the **Test Scripts** tab. When you select a server role, Veeam Backup & Replication automatically assigns a predefined script that should be run to verify if the application inside the VM is working normally.
In this exercise, Veeam Backup & Replication will run a predefined script that will probe standard port of the mail server for SMTP communication: 25.

19. If you verify a VM that has some other role not listed on the Role tab, click Add. In the Test Script window, select Use the following script.

20. In the Name field, specify the script name.
21. In the **Path** field, define the path to the executable script file that should be run.
   - If you have your own custom script to verify the application, define the path to it.
   - If you do not have a custom script, you can use Veeam’s standard script that probes the application communication ports. The script located in the installation folder of Veeam Backup & Replication: by default, `C:\Program Files\Veeam\Backup and Replication\Veeam.Backup.ConnectionTester.exe`. Specify this path in the **Path** field. In the **Arguments** field, specify the IP address of the tested VM (you can specify in explicitly or use the `%vm_ip%` variable) and the port that you want to probe.

22. If you have defined general SMTP settings, Veeam Backup & Replication will send an email notification to the specified email address when the job completes. If you want to send notifications to additional email addresses, at the **Settings** step of the wizard, select the **Send email notifications to the following recipients** check box and specify these email addresses in the field below.

To learn more, see the Email Settings section.

23. At the **Schedule** step of the wizard, select the **Run the job automatically** check box and define the time at which the job should run. If you do not select this check box, you will have to run the job manually.

24. Typically, a SureBackup job should run after the linked backup job completes: in this case, the SureBackup job will verify the created backup. However, in some cases, the linked backup job may not complete until the SureBackup job starts. If Veeam Backup & Replication finds out that the backup job is still running, the SureBackup job will fail to start.
To overcome this situation, select the **If some linked backup jobs are still running, wait up to** check box and specify the time period in the field on the right. In this case, if the linked backup job is still running, Veeam Backup & Replication will wait for the defined period of time and check the backup job after the period elapses. If the linked backup job is finished within the specified period, the SureBackup job will start. If the backup job is still running, the SureBackup job will not be started.

25. **At the last step of the wizard, select the Run the job once I click Finish check box.**

26. **Click Finish. The job will start.**

Veeam Backup & Replication will first power on the virtual appliance in the virtual lab, then start and verify VMs from the application group. After the VMs from the application group are tested, Veeam Backup & Replication will start the verified VM in the virtual lab and perform all necessary tests against it.
27. To view the real-time statistics for the running job, open the **Backup & Replication** view, select the **Jobs** node in the inventory pane and double-click the created job in the working area.

28. To view detailed information on a specific VM, select it in the list.
Validation

1. In Veeam Backup & Replication, open the **Backup & Replication** view and select **Jobs** in the inventory pane. Check the SureBackup job in the working area and make sure it has completed with the **Success** status.

2. Double-click the SureBackup job in the working area to see detailed information.

3. If you have selected to run a custom script, make sure it has returned 0; this means the script has passed without any errors.

4. If you have configured Veeam Backup & Replication to send an email notification after the SureBackup job completes, open the **Inbox** folder in your email client and make sure that you have an incoming email with details on the SureBackup job.
Performing Universal Application-Item Recovery

Insight into U-AIR

With U-AIR, you can recover application items such as Active Directory objects, emails and database records directly from backups. U-AIR does not require you to create special backups or use additional tools: you can recover application items directly from regular image-level backups created in Veeam Backup & Replication.

In many respects, the U-AIR process is similar to the SureBackup recovery verification. To let you perform application-item recovery, Veeam Backup & Replication runs a SureBackup job. The SureBackup job powers on an isolated virtual lab and starts the VM from which you want to recover items in this virtual lab. The VM is started in bundle with other VMs on which it is dependent so that the target application can function as usual. All VMs are started directly from compressed and deduplicated backup files that reside on the backup storage.

Therefore, to be able to recover application items from a backup with U-AIR, you should have:

- A pre-configured virtual lab in which VMs will be started.
- A pre-configured application group. The application group should include the VM from which you want to recover application items and all VMs on which this VM is dependent.
- A pre-configured SureBackup job with the virtual lab and application group linked to it.

To make the recovery process smooth and easy, Veeam provides a set of U-AIR wizards:

- Microsoft Active Directory U-AIR wizard
- Microsoft Exchange U-AIR wizard
- Microsoft SQL U-AIR wizard
- Universal U-AIR wizard

Recovery of items from Microsoft Active Directory, Microsoft Exchange and Microsoft SQL is wizard-driven: to recover necessary application items, you need to go through the wizard.

To recover items from other virtualized applications, you should use the Universal U-AIR wizard. The Universal U-AIR wizard powers on the virtual lab and runs there the VM with the necessary application. After that, you can log on to the started VM and restore items you need using native management tools for the application.

Evaluation Case

In this exercise, you will recover a deleted account from the backup of the Domain Controller. The Domain Controller will be started together with the DNS server to enable full application functionality.

Note

The U-AIR procedure has two workflow scenarios: typical U-AIR workflow and a simplified U-AIR workflow. In this guide, you will follow the simplified workflow scenario. To learn about the typical workflow scenario, see the product documentation at www.veeam.com/vmware-esx-backup/resources.html.

To recover application items from the backup, you will complete two steps:

1. Set up the environment for U-AIR. To run the Domain Controller and DNS server in the isolated environment, you will re-use the virtual lab, application group and SureBackup job that you have configured in the previous exercise.

2. Recover application items from the backup. You will start the Active Directory U-AIR wizard and recover the deleted account with it.

You can use this exercise to restore application items from the backup of any VM. Just make sure that you add to the application group the VM from which you want to recover application items and all VMs on which this VM is dependent.
**Prerequisites**

- Make sure that you have a valid trial or Enterprise license for Veeam Backup & Replication installed. If you have a Standard license, you will not be able to use U-AIR.
- Download the necessary U-AIR wizard from www.veeam.com/downloads and install it on the Veeam Backup & Replication server. Note that you should have a user account at the Veeam’s website to be able to download the wizard. When installing the U-AIR wizard, select to skip Enterprise Manager configuration.
- Make sure that you have a virtual lab configured as described in the Performing SureBackup Recovery Verification section.
- Make sure that you have an application group configured as described in the Performing SureBackup Recovery Verification section.
- Make sure that you have a SureBackup job configured as described in the Performing SureBackup Recovery Verification section.
- Make sure that all applications you plan to use for U-AIR are virtualized. These include the application from which you want to recover items (Active Directory) and applications and services on which this primary application is dependent (DNS).
- Create backups of the Domain Controller and DNS VMs as described in Veeam Backup & Replication Evaluator's Guide for VMware at www.veeam.com/vmware-esx-backup/resources.html. To check if the backup has been successfully created, open the Backup & Replication view, select the Backups node in the inventory pane and expand the backup job to verify that there is at least one restore point available for the VM.

**Procedure**

Before you start working with the U-AIR wizard, you need to set up the environment in which the VM with the necessary application will be started.

1. Check the settings of the virtual lab you have configured for SureBackup recovery verification: open the Backup Infrastructure view, select the Virtual Labs node in the inventory pane, right-click the virtual lab in the working area and select Properties.
   
   You may need to adjust the network settings of the virtual lab. For example, if your virtual lab is using basic networking settings and the VMs you want to start in the virtual lab are connected to different networks, you will need to re-configure the virtual lab and define advanced networking settings. To learn more, see the Create a Virtual Lab section.

2. Save changes and finish working with the wizard.

3. Edit settings of the application groups you have configured for SureBackup recovery verification: open the Backup Infrastructure view, select the Application Groups node in the inventory pane, right-click the application group in the working area and select Properties.

   For U-AIR, the application group should contain:
   
   - VM from which you want to restore items: Domain Controller
   - All VMs on which the restored VM is dependent: DNS server

   Move on to the Virtual Machines step of the wizard and click Add to add the necessary VMs to the application group. Then assign corresponding roles to them as described in the Create an Application Group section.
4. Save changes and finish working with the wizard.

5. Edit settings of the SureBackup job you have configured for SureBackup recovery verification: open the Backup & Replication view, select the SureBackup node in the inventory pane, right-click the SureBackup job in the working area and select Edit.

6. Move on to the Application Group step of the wizard.

7. Select the Keep the application group running once the job completes check box. This will let you work with VMs from the application group after verification of VMs is completed.
8. Move on to the **Backup Jobs** step of the wizard.

9. Clear the **Link backup jobs** check box. For U-AIR, you will only need to start VMs from the application group; you do not need to start VMs from any backup jobs.

10. Save changes and finish working with the wizard.

After you have configured the environment for application-item recovery, you can start the recovery itself.

**Important!** It is strongly recommended that you use test VMs for this exercise. If you use a production Domain Controller, you can create a test account that you will use for this evaluation exercise. This will ensure that your production data stays intact if any problem occurs.

1. Log on to Active Directory in the production environment and delete some object, for example, the user account. You will restore this account from the backup to the production Domain Controller using U-AIR.
2. In Veeam Backup & Replication, open the **Backup & Replication** view and select **SureBackup** under the **Jobs** node in the inventory tree. Right-click the SureBackup job in the working area and select **Start**.

3. Double-click the started SureBackup job to view the realtime statistics. Wait for DNS server and Domain Controller to be started and successfully tested.

4. In the session window, right-click the Domain Controller VM from which you want to recover items and select the corresponding command: **Active Directory item recovery**.
5. The **Microsoft Active Directory U-AIR** wizard will be launched. Veeam Backup & Replication will automatically define the IP address of the Domain Controller running in the production environment and the IP address of the Domain Controller inside the virtual lab. Typically, these IP addresses coincide.
6. Specify the username and password to connect to the Domain Controller in the production environment and to the Domain Controller in the virtual lab.

7. At the **AD Object** step of the wizard, select the account you want to restore. All deleted AD objects have the *(DELETED)* suffix appended to them.

8. At the **Review** step of the wizard, make sure that the **Enable users** check box is selected. This will let you automatically enable the user account right after it is restored to the production Domain Controller.

9. Finish working with the wizard to complete the application item recovery.
Validation

Log on to Active Directory in the production and make sure that the account has been successfully restored to it.

Finalizing U-AIR Process

After you have successfully recovered application items to the production environment, you can power off the virtual lab:

1. In Veeam Backup & Replication, open the **Backup & Replication** view and select **SureBackup** under the **Jobs** node in the inventory tree.

2. Right-click the SureBackup job that you have started to power on the virtual lab for U-AIR and select **Stop**.

Veeam Backup & Replication will power off all VMs in the virtual lab and the virtual lab itself.
Using On-Demand Sandbox

In addition to other capabilities, vPower lets you create and use an on-demand sandbox. The on-demand sandbox is an isolated virtual environment where you can run one or more VMs from backups. You can use the sandbox to troubleshoot problems with VMs, test software patches, upgrades, install new software and so on.

The on-demand sandbox is fully fenced off from the production environment so you can work with VMs in it without any harm to production VMs. VMs in the sandbox are run directly from backups that remain in the read-only state. All changes made to VMs in the sandbox are written to redo logs that are deleted after you finish working with the sandbox and power it off.

You can start VMs from the most recent backup in the sandbox or use any previous restore point of a VM.

To create an on-demand sandbox, you should have:

- A pre-configured virtual lab in which VMs will be started.
- A pre-configured application group. The application group should include all VMs that you want to test. This can be one VM or a group of VMs that work together.
- A pre-configured SureBackup job with the virtual lab and application group linked to it.

Evaluation Case

In this exercise, you will create an on-demand sandbox and start a file server VM in it. To run the file server in the sandbox, you will re-use the virtual lab, application group and SureBackup job that you have configured in the Performing SureBackup Recovery Verification exercise.

Prerequisites

- Make sure that you have a valid trial or Enterprise license for Veeam Backup & Replication installed. If you have a Standard license, you will not be able to create an on-demand sandbox.
- Make sure that you have a virtual lab configured as described in the Performing SureBackup Recovery Verification section.
- Make sure that you have an application group configured as described in the Performing SureBackup Recovery Verification section.
- Make sure that you have a SureBackup job configured as described in the Performing SureBackup Recovery Verification section.
- Create a backup of the VM(s) that you want to start in the sandbox as described in Veeam Backup & Replication Evaluator’s Guide for VMware at www.veeam.com/vmware-esx-backup/resources.html. To check if the backup has been successfully created, open the Backup & Replication view, select the Backups node in the inventory pane and expand the backup job to verify that there is at least one restore point available for the VM.
- (Optional) Make sure that the remote desktop connection is enabled on all VMs you want to start in the sandbox. This will let you log on to VMs in the sandbox using the remote desktop connection.
Procedure

1. Check the settings of the virtual lab you have configured for SureBackup recovery verification: in Veeam Backup & Replication, open the Backup Infrastructure view, select the Virtual Labs node in the inventory pane, right-click the virtual lab in the working area and select Properties.

You may need to adjust the network settings of the virtual lab. For example, if your virtual lab is using basic networking settings and the VMs you want to start in the sandbox are located in different networks, you will need to re-configure the virtual lab and define advanced networking settings. To learn more, see the Create a Virtual Lab section.

2. Save changes and finish working with the wizard.

3. Edit settings of the application groups you have created for SureBackup recovery verification: open the Infrastructure view, select the Application Groups node in the inventory pane, right-click the application group in the working area and select Properties.

4. To be able to start VMs in the sandbox, you need to include them into the application group. For this exercise, the application group will contain only one VM: a virtualized file server.

Move on to the Virtual Machines step of the wizard and click Add to add the necessary VMs.

5. Save changes and finish working with the wizard.

6. Edit settings of the SureBackup job you have configured for SureBackup recovery verification: open the Backup & Replication view, select the SureBackup node in the inventory pane, right-click the SureBackup job in the working area and select Edit.
7. Move on the Application Group step of the wizard. Make sure that the Keep the application group running once the job completes check box is selected. This will let you work with VMs from the application group after the verification of VMs is completed.

8. Move on to the Backup Jobs step of the wizard. Make sure that the Link backup jobs check box is not selected.

9. Save changes and finish working with the wizard.
10. In Veeam Backup & Replication, open the **Backup & Replication** view and select **SureBackup** under the **Jobs** node in the inventory tree. Right-click the SureBackup job in the working area and select **Start**.

11. If you want to run VMs not from the latest backup but from some other restore point, right-click the SureBackup job in the working area and select **Start**. In the displayed window, select the date on which the necessary restore point was created. Click **OK**.

12. Double-click the started SureBackup job to view the realtime statistics. Wait for the VM to be started and successfully tested.

13. After the VM is powered on, you can log on to the VM console and work with it as usual. There are several ways to log on to the VM console.

   - Click the link with the VM name in the SureBackup session window. The VM console will be opened.
Log on to the VM console using the remote desktop connection. Note that you should use the VM masquerade IP to connect to the VM.

To get the VM masquerade IP, open the properties of the virtual lab and move on to the Ready to Apply step of the wizard. Check the Masquerade IP value in the Network settings section:

![Edit Virtual Lab screenshot](image)

In this example, the masquerade network IP is 172.18.x.x. The IP address of the file server in the production network is 172.16.11.152. Subsequently, you should access the file server started in the virtual lab using IP address 172.18.11.152:

![Remote Desktop Connection screenshot](image)

You can also log on to the VM console using vSphere Client: in the inventory tree of vSphere Client, select the VM started in the virtual lab and click the Console tab.
Stopping VMs in the Sandbox

After you have finished working with VMs in the sandbox, you can power off the virtual lab:

1. In Veeam Backup & Replication, open the Backup & Replication view and select SureBackup under the Jobs node in the inventory tree.
2. Right-click the SureBackup job that you have started to create a virtual lab for U-AIR and select Stop.

Veeam Backup & Replication will power off all VMs in the virtual lab and the virtual lab itself.
Performing Universal File-Level Recovery

Insight into Universal File-Level Recovery

Veeam Backup & Replication provides two wizards for instant file-level recovery (IFLR):

- Built-in wizard for file-level recovery from FAT/NTFS file systems
- Multi-OS wizard for file-level recovery from 15 most popular file systems such as Linux, Unix and FreeBSD

To restore files and folders from file systems not covered by these two wizards, you can leverage the vPower technology. vPower extends Veeam’s IFLR and lets you immediately restore files from any file system supported by VMware.

To recover files with vPower, you first need to restore a VM with Instant VM Recovery and then mount the disks of the restored VM to the VM that runs the same file system. Alternatively, you can mount the VM disks to a Windows-based VM and then use specialized tools such as PortLock Drive Explorer to browse for files and folders on the restored disks.

Evaluation Case

In this exercise, you will restore files from a VM running Novell NetWare. The exercise includes two steps:

1. You will perform Instant VM Recovery to publish the VM from a compressed and deduplicated backup file. The VM will be restored but not powered on.

2. You will mount the disk of the restored VM to another VM running Novell NetWare. The disk will be attached as a new local drive and you will be able to search for necessary files from the VM console as usual.

Prerequisites

- Make sure that you have two VMs running Novell NetWare in your test lab. The first VM will be backed up and you will use the created backup for file-level recovery. The other VM will be used as a basis for disk mounting: disks of the instantly recovered VM will be mounted to it.

- Make sure that you have at least 10 GB of free disk space on the vPower NFS datastore to which redo logs created during Instant VM Recovery will be written. By default, the redo logs are written to the C:\ProgramData\Veeam\Backup\NfsDatastore folder on the vPower NFS server.
Procedure

1. Create a backup of the VM running Novell Netware as described in Veeam Backup & Replication Evaluator’s Guide for VMware at www.veeam.com/vmware-esx-backup/resources.html. To check if the backup has been successfully created, open the **Backup & Replication** view, select the **Backups** node in the inventory pane and expand the backup job to verify that there is at least one restore point available for the VM.

2. Perform Instant VM Recovery: follow the steps of the Performing Instant VM Recovery exercise. Note that you only need to publish the VM to an ESX(i) host from the backup; you do not need to power it on. For this reason, at the **Ready to Apply** step of the **Instant VM Recovery** wizard, do not select the **Power on VM automatically** check box.
3. Finish working with the Instant VM Recovery wizard. To check if the VM has been successfully published, open vSphere Client and make sure that the restored VM is available but not powered on.

Now you can attach the virtual disk of the restored VM to the other VM running Novell Netware:

1. In vSphere Client, right-click the second VM running Novell Netware and select Edit Settings.
2. On the **Hardware** tab, click **Add** and choose to add a new hard disk.

3. At the **Select Disk** step of the wizard, choose **Use an existing virtual disk**.
4. At the **Select Existing Disk** step, browse to the Veeam's vPower NFS datastore. The vPower NFS datastore is located on your Veeam Backup server, on the backup repository with VM backups or on any other Windows-based server you selected to use as the vPower NFS server.

5. On the vPower NFS datastore, find a folder with the name of the instantly restored VM. This folder contains emulated VM files; the actual VM files are located in the backup stored on the backup repository.

6. Open the folder and choose the VM disk you want to mount to the target VM.
7. The disk should be added to the target VM as a new drive. At the **Advanced Options** step of the wizard, select the virtual device node that is not yet occupied.

8. Proceed with the wizard and finalize disk mount. Please note that you may need to reset the Novell Netware server on the target VM to see the mounted disk.

Now you can browse to files and folders as usually.
Validation

Open the console of the target Novell Netware VM and make sure that the disk has been successfully attached to the VM and you can search for necessary files.

**Before disk mount:**

**After disk mount:**

**Finalizing Universal Instant File-Level Recovery**

After file-level recovery is finished, do the following:

1. Remove the disk from the target VM using vSphere Client.
2. Terminate the Instant VM Recovery session as described in the Performing Instant VM Recovery section.