Contents

CONTACTING VEEAM SOFTWARE ............................................................................................................................. 4
GETTING STARTED .................................................................................................................................................... 5
SYSTEM REQUIREMENTS .......................................................................................................................................... 7
BACKUP INFRASTRUCTURE SETUP ........................................................................................................................... 8
  INSIGHT INTO VEEAM BACKUP & REPLICATION INFRASTRUCTURE ................................................................. 9
  INSTALLING VEEAM BACKUP & REPLICATION ................................................................................................. 12
  CONNECTING VIRTUAL INFRASTRUCTURE SERVERS .......................................................................................... 16
  CONFIGURING BACKUP PROXY ............................................................................................................................ 21
  CONFIGURING BACKUP REPOSITORY .................................................................................................................. 26
DATA PROTECTION AND DISASTER RECOVERY TASKS ......................................................................................... 33
  PERFORMING BACKUP ............................................................................................................................................. 35
  BACKING UP AND RESTORING MICROSOFT SQL SERVER DATABASES ............................................................ 53
  PERFORMING FULL VM RESTORE ........................................................................................................................... 60
  RESTORING GUEST OS FILES ................................................................................................................................. 64
    Scenario 1. Restoring VM Guest OS Files (FAT, NTFS, ReFS) ............................................................................. 65
    Scenario 2. Restoring VM Guest Files (Linux, Unix and so on) ....................................................................... 69
  RESTORING VM FILES ........................................................................................................................................... 74
  CREATING BACKUP COPY ....................................................................................................................................... 78
  PERFORMING REPLICA............................................................................................................................................ 84
  FAILING OVER A VM REPLICA ............................................................................................................................... 101
  UNDOING FAILOVER .............................................................................................................................................. 104
  FAILING BACK TO THE PRIMARY VM ..................................................................................................................... 106
  COMMITTING FAILBACK ....................................................................................................................................... 109
DISTRIBUTED BACKUP INFRASTRUCTURE MANAGEMENT .............................................................................. 111
  INSTALLING AND CONFIGURING VEEAM BACKUP ENTERPRISE MANAGER ................................................... 112
  SEARCHING FOR GUEST OS FILES AND PERFORMING 1-C Click RESTORE ..................................................... 119
  PERFORMING SELF-RESTORE OF VM GUEST OS FILES .................................................................................. 122
  CLONING AND EDITING JOBS ............................................................................................................................... 127
  RESTORING DATA FROM ENCRYPTED BACKUP FILE WITHOUT PASSWORD .................................................... 129
Contacting Veeam Software

At Veeam Software we value the feedback from our customers. It is important not only to help you quickly with your technical issues, but it is our mission to listen to your input, and build products that incorporate your suggestions.

Customer Support

Should you have a technical concern, suggestion or question, please visit our Customer Center Portal at www.veeam.com/support.html to open a case, search our knowledge base, reference documentation, manage your license or obtain the latest product release.

Company Contacts

For the most up to date information about company contacts and offices location, please visit www.veeam.com/contacts.html.

Online Support

If you have any questions about Veeam products, you can use the following resources:

- Full documentation set: www.veeam.com/documentation-guides-datasheets.html
- Community forum at forums.veeam.com
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 re-invents data protection for VMware vSphere and Microsoft Hyper-V virtual environments. Veeam Backup & Replication supports the entire virtual infrastructure with industry leading features such as 2-in-1 backup and replication, streamlined VM recovery and instant file-level recovery, built-in compression and deduplication, scalability, centralized management and many more.

About This Guide

This guide will help you become familiar with Veeam Backup & Replication and evaluate its capabilities. It explains the primary features of Veeam Backup & Replication and will help you begin using the product, regardless of your previous experience with the product.

Intended Audience

The document is intended for IT professionals who are looking to deploy Veeam Backup & Replication to protect their Microsoft Hyper-V virtual environment. This guide will be of interest to novices to the product and to Microsoft Hyper-V administrators, consultants and analysts who have used previous versions of Veeam Backup & Replication and want to evaluate new features.

Document Structure

The guide provides a set of self-guided evaluation exercises that you should follow to familiarize yourself with Veeam Backup & Replication. Each evaluation exercise provides a short feature overview, an evaluation case, an evaluation procedure, and guidelines for validation of the exercise results.

The guide is comprised of four major parts:

- **Reference Environment**: This section describes requirements to a test lab that you need to provision to successfully perform evaluation tasks.
- **Backup Infrastructure Setup**: This section describes Veeam Backup & Replication installation and deployment steps that must be completed before you can start evaluating the product.
- **Data Protection and Disaster Recovery**: This section describes evaluation cases covering the most typical data protection and disaster recovery tasks that you can perform with Veeam Backup & Replication.
- **Distributed Backup Infrastructure Management**: This section describes how you can manage a distributed backup infrastructure using Veeam Backup Enterprise Manager.
Help and Support

This guide provides a high-level overview of Veeam Backup & Replication primary features and should be regarded as a supplement to existing technical documentation. The complete set of documentation can be found on the Veeam Technical Documentation page.

For technical support and assistance, use the following resources:

- Veeam Community Forums
- Customer Support Portal
System Requirements

To learn about system requirements, required ports and other, see Release Notes.
Backup Infrastructure Setup

This section describes Veeam Backup & Replication installation and deployment steps that you need to complete before you can start evaluating the product.
Insight into Veeam Backup & Replication Infrastructure

Veeam Backup & Replication infrastructure comprises a set of components needed to perform data protection and disaster recovery tasks. The backup infrastructure that we will use for evaluation includes the following components:

- **Veeam backup server**: a physical or virtual machine running Veeam Backup & Replication. The Veeam backup server performs the role of the main management component: it is the configuration and control center of the backup infrastructure.

- **Virtual infrastructure servers**: Hyper-V hosts used as the source and the target for backup and replication.

- **Backup proxy (onhost or offhost)**: a 'data mover' component that retrieves VM data from the source storage, processes it and transfers to the destination.

- **Backup repository**: a location used to store backup files and auxiliary replica files.

To perform evaluation exercises, you can use a simple deployment scenario or a distributed deployment scenario (recommended). The choice depends on your test lab environment. If you have a very small test lab and there is no possibility to allocate dedicated servers that will perform the roles of an offhost backup proxy and backup repository, you can use a simple deployment scenario to evaluate the product. However, whenever possible, it is recommended that you use a distributed deployment scenario. This will help you gain insight into the architecture of the backup infrastructure, evaluate its benefits and increase your experience in deploying backup infrastructure components.
Simple Deployment

In a simple deployment scenario, you will need three components:

- Veeam backup server
- Source Hyper-V host
- Target Hyper-V host (used for a replication scenario)

The Veeam backup server performs two roles:

- It is the ‘control center’ of the backup infrastructure, coordinating job performance and other administrative activities.
- It is the default backup repository: all backups and auxiliary replica files are stored on the Veeam backup server, in the Backup folder on the volume with the greatest amount of free disk space.

The source Hyper-V host also performs two roles:

- It is the host on which VMs you want to back up or replicate are located.
- It is the default backup proxy. When you perform backup or replication, VM data is processed directly on the source Hyper-V host and then moved to the target. All services necessary for backup proxy functioning are installed on the source Hyper-V host.

Distributed Deployment

In the distributed deployment scenario, roles of backup infrastructure component are assigned to dedicated servers. The backup infrastructure includes the following components:

- Veeam backup server
- Offhost backup proxy
- Backup repository
- Source and target Hyper-V hosts

The distributed deployment scenario enables efficient data transfer and use of resources in the backup infrastructure. During backup and replication, VM data is retrieved from the source storage and processed on a dedicated server (offhost backup proxy). Processed VM data is then transferred to the dedicated backup repository in the backup scenario or to the target Hyper-V host in the replication scenario.

This type of backup, with VM processing offloaded to the offhost backup proxy, is known as offhost backup. Offhost backup does not impose any load on production Hyper-V hosts: all resource-intensive backup operations are performed on the offhost backup proxy and the source Hyper-V host remains unaffected.

Depending on your production environment and the backup and replication scenarios you plan to use, the distributed backup infrastructure may include multiple dedicated offhost backup proxies and backup repositories controlled by a single Veeam backup server. However, to evaluate the product, it is sufficient to deploy one offhost backup proxy and one backup repository locally in your test lab.
## Exercise List

To deploy Veeam backup infrastructure, perform the following exercises.

<table>
<thead>
<tr>
<th>Exercise</th>
<th>Description</th>
<th>Time Estimates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Veeam Backup &amp; Replication</td>
<td>Install Veeam Backup &amp; Replication on a physical or virtual machine.</td>
<td>5-10 minutes</td>
</tr>
<tr>
<td>Connect virtual infrastructure servers</td>
<td>In the Veeam Backup &amp; Replication console, connect hosts that you want to use as the source and the target for backup and replication.</td>
<td>5-7 minutes</td>
</tr>
<tr>
<td>Configure a backup proxy</td>
<td>In the Veeam Backup &amp; Replication console, connect a server that you want to use as a backup proxy, and assign the role of the backup proxy to it. This exercise must be performed only if you decide to follow the distributed deployment scenario.</td>
<td>5-7 minutes</td>
</tr>
<tr>
<td>Configure a backup repository</td>
<td>In the Veeam Backup &amp; Replication console, connect a server or that you want to use as a backup repository, and assign the role of a backup repository to it. This exercise must be performed only if you decide to follow the distributed deployment scenario.</td>
<td>5-7 minutes</td>
</tr>
</tbody>
</table>
Installing Veeam Backup & Replication

Install Veeam Backup & Replication on a Microsoft Windows machine, either physical or virtual.

Evaluation Case

In this exercise, you will install Veeam Backup & Replication. By installing Veeam Backup & Replication, you configure a Veeam backup server — the core component in the backup infrastructure that controls all other components.

Prerequisites

- The machine where you plan to install Veeam Backup & Replication must meet system requirements to a Veeam backup server.
- You must have Local Administrator permissions on the machine where Veeam Backup & Replication will be installed.
- You must have a valid trial license or full paid license for Veeam Backup & Replication.
Procedure

To install Veeam Backup & Replication:


2. Mount the installation image using disk image emulation software, or burn the downloaded ISO image file to a blank CD/DVD. If you are installing Veeam Backup & Replication on a virtual machine, use built-in tools of the virtualization management software to mount the installation image to the virtual machine.

3. Run the Setup.exe file from the ISO.

4. On the splash screen, click the Install tile on the left to launch the Veeam Backup & Replication setup wizard.

Alternatively, you can click the Veeam Backup & Replication tile on the right.
5. At the License Agreement step of the wizard, select I accept the terms in the license agreement.

6. At the Provide License step of the wizard, specify the path to the license file. You must obtain the license file after you download the product from the web site.

7. At the Program Features step of the wizard, keep the default settings.
8. At the **System Configuration Check** step of the wizard, install missing software components and enable missing features, if any.

![System Configuration Check](image)

9. At the **Default Configuration** step of the wizard, specify if you want to use default installation settings or specify installation settings on your own. In the latter case, the setup wizard will include additional steps for configuring the necessary settings.

If you have chosen to specify custom installation settings, pass through the next wizard steps and specify the required settings manually. If you have chosen to use default installations settings, click **Install** to begin installation.

![Default Configuration](image)

10. When the installation process completes, click **Finish** to close the wizard.

**Validation**

Select **Programs > Veeam > Veeam Backup & Replication** from the **Start** menu to make sure that Veeam Backup & Replication has been installed successfully.
Connecting Virtual Infrastructure Servers

In the Veeam Backup & Replication console, connect virtual infrastructure servers to the backup server.

You can connect standalone Hyper-V hosts, Hyper-V clusters or SCVMM servers. If a Hyper-V host is a part of a cluster or SCVMM hierarchy, it is recommended to connect a cluster to Veeam Backup & Replication, not a host itself.

Evaluation Case

In this exercise, you will connect Hyper-V hosts that you plan to use as the source and the target for backup and replication.

Prerequisites

- You must decide which hosts you want to use as source and target for backup and replication.
- The Veeam backup server must have access to all hosts you plan to use for backup and replication.
- On every connected Hyper-V host, Veeam Backup & Replication deploys a set of components: Veeam Installer Service, Veeam Data Mover and Hyper-V Integration Service. Make sure that File and Printer Sharing is enabled in the network connection settings of the host. Otherwise, these components will not be installed.
- If you plan to add SCVMM, make sure that SCVMM Admin UI is installed on the Veeam backup server. Otherwise, you will not be able to add SCVMM servers to Veeam Backup & Replication.
- Make sure that all necessary ports are open.
Procedure

To connect Hyper-V hosts, failover cluster or SCVMM:

1. Run Veeam Backup & Replication: from the **Start** menu, select **Programs > Veeam > Veeam Backup & Replication**.

2. In the authentication window, click **Connect**.

3. In the inventory pane of the **Backup Infrastructure** view, right-click the **Managed servers** node and select **Add Server**.
4. In the Add Server window, click Microsoft Hyper-V to launch the New Hyper-V Server wizard.

5. At the Name step of the wizard, specify a DNS name or IP address of the server.
6. At the **Type** step of the wizard, choose the server type: **Microsoft System Center Virtual Machine Manager (SCVMM)**, **Microsoft Hyper-V cluster** or **Microsoft Hyper-V server (standalone)**.

7. At the **Credentials** step of the wizard, specify credentials for the user account with administrator permissions to the added server: click **Add** on the right of the **Credentials** field and specify the user name and password to connect to the added server. Credentials must be specified in the **DOMAIN \USERNAME** format. Click **OK**.

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

9. Repeat the procedure for all virtual infrastructure servers that you want to add.
Validation

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, click the **Managed servers** node.
3. Make sure that the added server is available in the working area.
Configuring Backup Proxy

The offhost backup proxy is a backup infrastructure component that you must configure if you want to perform offhost backup. The role of the offhost backup proxy can be assigned to a physical or virtual machine that meets system requirements. On this machine, Veeam Backup & Replication installs a data mover component responsible for data processing and transfer.

During offhost backup, Veeam Backup & Replication triggers a snapshot of a volume on which VMs are located. After that, the snapshot is split from the source Hyper-V host and mounted to the offhost backup proxy. This is made possible due to VSS transportable shadow copies. The transportable shadow copy technology allows you to create a snapshot of a data volume on one server and mount it to another server within the same SAN subsystem. The mount operation is performed at the SAN layer, so your network resources are not impacted. The operation takes only a couple of minutes regardless of the snapshot size.

After the snapshot is mounted, the data mover running on the offhost backup proxy accesses the mounted snapshot, retrieves VM data from it, processes it and transfers data to the destination. As a result, VM processing is offloaded to the offhost backup proxy and the load on the source Hyper-V host is reduced.

Evaluation Case

In this exercise, you will configure an offhost backup proxy. Configuration of a backup proxy is performed in two stages:

1. In the Veeam Backup & Replication console, add a server that will perform the role of an offhost backup proxy.
2. Assign the role of an offhost backup proxy to the added server.

Prerequisites

- You must have a dedicated physical or virtual Microsoft Windows machine that meets system requirements to an offhost backup proxy. Note that the version of the Hyper-V host and offhost backup proxy must be the same.
- The source Hyper-V host and the offhost backup proxy must be connected through a SAN configuration to the shared storage.
- The offhost backup proxy must have access to the Veeam backup server and backup repository for backup and restore scenarios, and to the target host for a replication scenario.
- A VSS hardware provider that supports transportable shadow copies must be installed and properly configured on the offhost backup proxy and Hyper-V host. The VSS hardware provider is usually distributed as a part of client components supplied by the storage vendor. Typically, when configuring a VSS hardware provider, you need to specify a server controlling the LUN and disk array credentials to provide access to the array. To learn about specifics of the VSS hardware provider configuration, contact your SAN vendor.
- If you plan to perform offhost backup for a Hyper-V cluster with CSV, make sure you deploy an offhost backup proxy on a host that is not a part of a Hyper-V cluster. Otherwise the cluster will fail during backup or replication.
- Make sure that all necessary ports are open.
Procedure

To configure an offhost backup proxy:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, right-click the **Managed servers** node and select **Add Server**.
3. In the **Add Server** window, click **Microsoft Windows** to launch the **New Windows Server** wizard.
4. At the **Name** step of the wizard, specify a DNS name or IP address of a Microsoft Windows server.

5. At the **Credentials** step of the wizard, specify credentials for the user account with Administrator permissions to the added server: click **Add** on the right of the **Credentials** field and specify the user name and password to connect to the added server. Credentials must be specified in the `DOMAIN\USERNAME` format for domain accounts or `HOST\USER` format for local accounts. Click **OK**. If you have specified credentials before, you can simply select them from the **Credentials** list.

6. Follow next steps of the wizard. At the last step of the wizard, click **Finish** to add the server.
Next, assign the role of a backup proxy to the added server.

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

2. In the inventory pane, right-click the **Backup Proxies** node and select **Add Hyper-V Offhost Backup Proxy**.

3. At the **Server** step of the wizard, in the **Choose server** list select the Microsoft Windows server that you have added.

4. In the **Connected volumes** field, leave the **Automatic detection** option selected. Veeam Backup & Replication will automatically detect all volumes to which the configured offhost backup proxy has access.

5. Follow next steps of the wizard. At the last step of the wizard, click **Finish** to finalize configuration of the offhost backup proxy.
Validation

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, click the **Backup Proxies** node.
3. Make sure that the added offhost backup proxy is available in the working area.

![Backup Infrastructure View](image_url)
Configuring Backup Repository

Backup repository is a location to which created backup files and auxiliary replica files are stored. You can use the following types of backup repositories:

- Microsoft Windows-based server with local or directly attached storage
- Linux-based server with local, directly attached or mounted NFS storage
- CIFS share
- Deduplication storage appliance*

* This guide describes backup repository configuration on Microsoft Windows, Linux servers and SMB shares. To learn about using deduplication storage appliances with Veeam Backup & Replication, see Veeam Backup & Replication User Guide at www.veeam.com/documentation-guides-datasheets.html.

Evaluation Case

In this exercise, you will configure a backup repository in which backup files and auxiliary replica files will be stored.

Prerequisites

- You must have a Microsoft Windows server with a local or directly attached storage, Linux-based server with a local, directly attached or mounted NFS storage, CIFS share or deduplicating storage appliance that will perform the role of a backup repository.
- If a Microsoft Windows- or Linux-based server is used as a backup repository, these servers must have access to the Veeam backup server and the server that will perform a role of the offhost backup proxy (this can be a dedicated offhost backup proxy or source Hyper-V host performing the role of the default backup proxy). In case of a CIFS share, make sure that you have an account with the Full Control permissions on the share to be able to connect to it.
- Make sure that all necessary ports are open.
Procedure

To configure a backup repository:

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

2. If you plan to use a Microsoft Windows-based or Linux-based server as a backup repository, right-click the **Managed servers** node in the inventory pane and select **Add Server**.

If you plan to use a CIFS share as a backup repository, you do not need to add a server. Go to the procedure describing how to assign the backup repository role.
3. In the **Add Server** window, select the server type: **Microsoft Windows** or **Linux**.

![Add Server Window](image)

3. Select the type of server you want to register with backup infrastructure. All registered servers can be found under the Managed servers node on the Infrastructure tab.

   - **VMware vSphere**: Adds vCenter Server (recommended), or standalone vSphere Hypervisor (ESXi/ESX).
   - **VMware vCloud Director**: Adds VMware vCloud Director 5.5 or later server.
   - **Microsoft Hyper-V**: Adds SCVMM server, Hyper-V cluster, or standalone host (2008 R2 or later).
   - **Microsoft SMB3**: Adds SMB3 server cluster, or standalone SMB3 server.
   - **Microsoft Windows**: Adds Microsoft Windows server (Windows 2008 or later).
   - **Linux**: Adds Linux server (must have SSH and Perl).

![New Windows Server Window](image)

4. At the **Name** step of the wizard, specify a DNS name or IP address of the Microsoft Windows- or Linux-based server that you want to use as a backup repository.

![New Windows Server Window](image)
5. At the **Credentials** step of the wizard, enter credentials for the user account with administrator access permissions to the added server: click **Add** on the right of the **Credentials** field and specify the user name and password to connect to the added server.

If you have specified credentials before, you can simply select them from the **Credentials** list.

6. Follow the next steps of the wizard. At the last step of the wizard, click **Finish** to add the server.

Next, assign the role of a backup repository:

1. Right-click the **Backup Repositories** node in the inventory pane and select **Add Backup Repository** to launch the **New Backup Repository** wizard.
2. At the **Name** step of the wizard, specify a name for the added backup repository.

![New Backup Repository](image1)

3. At the **Type** step of the wizard, select the type of backup repository: **Microsoft Windows server**, **Linux server** or **Shared folder**.

![New Backup Repository](image2)
4. For a Microsoft Windows- or Linux-based repository, select the server that you have added. For a CIFS share, specify a UNC path to the shared folder that will be used as a backup repository and enter credentials of an account with administrative privileges on the share.

5. At the Repository step of the wizard, specify a path to the folder to which backups and auxiliary replica files will be stored. Click Populate to see how much space is available on the backup repository.

6. Follow next steps of the wizard. At the last step of the wizard, click Finish. After you configure a new backup repository, Veeam Backup & Replication will display a window suggesting you to change the configuration backup location to the newly created repository. Click No to leave the default settings.
Validation

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, click the **Backup Repositories** node.
3. Make sure that the added backup repository is available in the working area.
Data Protection and Disaster Recovery Tasks

This section describes a set of exercises that you can perform to get familiar with the product functionality. Each exercise covers one of the most typical data protection or disaster recovery tasks and allows you to evaluate primary features of Veeam Backup & Replication.

Exercise List

To evaluate the key possibilities of Veeam Backup & Replication, perform the following exercises.

<table>
<thead>
<tr>
<th>Exercise</th>
<th>Description</th>
<th>Time Estimates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performing backup</td>
<td>Configure a backup job.</td>
<td>5-10 minutes</td>
</tr>
<tr>
<td></td>
<td>Run the backup job to create a full image-level backup.</td>
<td>Varies*</td>
</tr>
<tr>
<td></td>
<td>Run the backup job again to create an incremental backup.</td>
<td>Varies*</td>
</tr>
<tr>
<td>Backing up and restoring Microsoft SQL Server databases</td>
<td>Back up a virtualized Microsoft SQL Server and restore a database to a specific transaction.</td>
<td>Varies*</td>
</tr>
<tr>
<td>Restoring a full VM</td>
<td>Restore a full VM from the image-level backup.</td>
<td>Varies*</td>
</tr>
<tr>
<td>Restoring guest OS files</td>
<td>Restore specific guest OS files from the created image-level backup.</td>
<td>5-7 minutes</td>
</tr>
<tr>
<td>Restoring VM files</td>
<td>Restore a VM configuration file (XML) from the image-level backup.</td>
<td>5-7 minutes</td>
</tr>
<tr>
<td>Creating a backup copy</td>
<td>Create a copy of a backup file and store it on the secondary backup repository.</td>
<td>Varies*</td>
</tr>
<tr>
<td>Performing replication</td>
<td>Configure a replication job.</td>
<td>5-10 minutes</td>
</tr>
<tr>
<td></td>
<td>Run the replication job to create a VM replica on the target host.</td>
<td>Varies*</td>
</tr>
<tr>
<td></td>
<td>Run the replication job once again to create a restore point for a VM replica.</td>
<td>Varies*</td>
</tr>
<tr>
<td>Activity</td>
<td>Description</td>
<td>Time</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>--------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Failing over a VM replica</td>
<td>Fail over to the VM replica from the original VM.</td>
<td>3-5 minutes</td>
</tr>
<tr>
<td>Failing back to a primary VM</td>
<td>Fail back to the original VM from the VM replica.</td>
<td>Varies*</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 Backup

Veeam Backup & Replication backs up VMs at the image level. It retrieves VM data from the source storage, compresses and deduplicates it and writes to the backup repository in Veeam’s proprietary format. You can use the image-level backup for all types of data restore scenarios: restore a full VM, VM files, and separate guest OS files from the same backup file.

To perform backup, Veeam Backup & Replication leverages VSS capabilities and Hyper-V VSS components. Veeam Backup & Replication acts as a VSS requestor: it communicates with the VSS framework and triggers a checkpoint of a VM. After the checkpoint is created, Veeam Backup & Replication accesses the checkpoint to retrieve VM data.

In Veeam Backup & Replication, backup is job-driven: to perform backup, you need to configure a backup job. A backup job defines when, what, how and where to back up. One backup job can be used to process one or several VMs.

Veeam Backup & Replication performs both full and incremental backup. During the first run of a backup job, Veeam Backup & Replication creates a full VM backup (VBK). All subsequent job cycles produce incremental backups:

- VIB if forward incremental or forever forward incremental backup is used.
- VRB if reversed incremental backup is used.

The number of increments kept on disk depends on retention policy settings.

Evaluation Case

In this exercise, you will create backup of VM(s). You will configure a backup job and run it twice to create full and incremental backups.

It is recommended that you create a backup job for at least two VMs: one Microsoft Windows-based VM and one running OS other than Microsoft Windows, for example, Linux, Unix, BSD and so on. This will let you follow the two guest OS recovery scenarios afterwards: restoring guest OS files from a Windows-based VM and restoring guest OS files with multi-OS restore wizard.

Prerequisites

- All backup infrastructure components that will take part in the backup process must be added to the Veeam Backup & Replication console. These include Hyper-V host on which VM(s) reside, SCVMM or Hyper-V cluster. If you plan to use a distributed architecture scenario, you should also have an offhost proxy and a backup repository.

- [Optional] To receive an e-mail notification when a backup job completes, specify global email notification settings. To do that, select General Options from the main menu of Veeam Backup & Replication and specify necessary settings on the E-mail Settings tab.

- [Optional] To evaluate the application-aware image processing feature and the file indexing feature, make sure that at least one of backed up VMs runs Microsoft Windows 2003 SP1 or later.
Procedure

To perform backup of VMs, perform the following steps.

Step 1. Create a backup job

1. Open the Home view.

2. On the Home tab, click the Backup Job button and select Microsoft Hyper-V to launch the New Backup Job wizard.

3. At the Name step of the wizard, specify a name for the created backup job.
Step 2. Add VMs to the backup job

You can back up individual VMs or VM containers: Hyper-V hosts, clusters, SCVMM and so on. Jobs with VM containers are dynamic in nature: if a new VM is added to the container after the backup job is created, the job is automatically updated to include the new VM.

1. At the **Virtual Machines** step of the wizard, click **Add**.

2. To quickly find a VM or VM container, specify the name of the object that you want to find in the search field and click the **Start search** button on the right. Select a VM or VM container in the displayed list and click **Add**.
Step 3. Exclude VMs and VM disks

If you create a backup job for a VM container, you can exclude specific VMs or VM containers from the backup job. You can also select which VM disks to back up.

1. At the Virtual Machines step of the wizard, click Exclusions.

2. Use the VMs tab to exclude VMs or VM container from a backup job. Click Add and select VMs and VM containers that must be excluded. To quickly find a VM or container, enter the name of the object you want to find in the search field and click the Start search button on the right.

3. Click the Disks tab. Select a VM and click Edit to select disks that must be backed up. This functionality is useful, for example, if you want to back up only VM system drives.

4. To exclude disks of a VM added as part of a container, click Add on the right to include the VM in the list as a standalone instance.

5. Click OK.

6. Click Recalculate to see the total size of selected objects.
Step 4. Define the VM backup order

If you have included a number of VMs or VM containers in the backup job, you can specify the order in which VMs must be processed. This will help you make sure that the most important VMs in the job are processed first — for example, if you must fit into the backup window and you are unsure how much time VM processing will take.

1. At the **Virtual Machines** step of the wizard, select the added VM in the list.

2. Use the **Up** and **Down** buttons on the right to move the VM higher or lower in the list. The higher is VM in the list, the higher its priority. If you added a VM container as a single instance, VMs inside the container will be processed at random.
Step 5. Select a backup proxy and backup repository

If you use a distributed deployment scenario, you must point the created job to the backup proxy that will process VM data and to the backup repository to which VM backups must be stored.

1. At the **Storage** step of the wizard, click the **Choose** button next to the **Backup proxy** field. Make sure that the **Off-host backup** option is selected in the **Backup Proxy** window. Veeam Backup & Replication will offload the backup processing from the source Hyper-V host to the backup proxy and thus reduce the load on the production host.

2. Make sure that the **Failover to on-host backup mode if no suitable off-host proxies available** check box is selected. If the off-host backup proxy is not available or is not properly configured, Veeam Backup & Replication will use the on-host backup method to process VMs.

3. From the **Backup repository** list, select the backup repository that you have configured. Backup files created by the job will be written to this backup repository.

4. Define the number of restore points that must be kept. By default, Veeam Backup & Replication keeps 14 restore points.
Step 6. Specify advanced backup settings

At the **Storage** step of the wizard, click **Advanced** to specify additional backup settings.

1. On the **Backup** tab, you can select the mode in which you want to perform backup: forever forward incremental, forward incremental or reverse incremental.
   - The forever forward incremental backup method produces a backup chain that consists of the first full backup and a set of forward incremental backups following it. To use this backup method, select **Incremental** and do not enable active full and/or synthetic full backup.
   - The forward incremental backup method produces a backup chain that consists of the first full backup and a set of forward incremental backups following it. Additionally, the forward incremental backup chain contains synthetic full and/or active full backups that 'split' the backup chain into shorter series. To use this backup method, select **Incremental** and enable active full and/or synthetic full backup.
   - The reverse incremental backup method produces a backup chain that consists of the last full backup and a set of reverse incremental backups preceding it. To use this backup method, select **Reverse incremental**.

2. If you have selected to use forward incremental backup, select **Enable synthetic fulls** and specify a day on which a new full backup file must be created. This option is useful if your corporate policies require you to periodically create full backups. To create a synthetic full backup, Veeam Backup & Replication uses full and incremental backup files that already reside on the backup repository (instead of retrieving VM data from the production storage). Synthetic full backups do not impact the virtual infrastructure or primary storage.

3. With synthetic backup scheduled, you will have a number of full backups on disk — a full backup created at the first run of the backup job and those create according to the synthetic backup schedule. To save the disk space, you can select the **Transform previous full backup chains into rollbacks** check box. In this case, Veeam Backup & Replication will transform all previous full backup chains to a reversed incremental backup sequence. This option allows you to keep only one full backup image on disk and so reduce the amount of space required to store backups.
4. Open the **Storage** tab. Leave the **Enable inline data deduplication** check box selected. Veeam Backup & Replication deduplicates identical blocks of data when backing up multiple VMs in one job and eliminates empty space on logical disks of VMs. Use of deduplication dramatically reduces storage costs: you can reduce the backup size up to 90% when backing up VMs created from the same template.

5. Make sure the **Exclude swap file blocks** check box is selected. Swap files are dynamic and change intensively between runs of a backup job. Veeam Backup & Replication will identify data blocks of the Microsoft Windows pagefile in the VM guest OS and exclude them from processing, which will result in increased performance and smaller increments.

6. To reduce the size of a backup file, Veeam Backup & Replication offers 5 compression levels: **None, Dedupe-friendly, Optimal, High** and **Extreme**, that provide different compression ratios to meet the needs of your environment. For this evaluation exercise, make sure that the **Optimal** compression level is selected in the **Compression level** list.

7. Veeam Backup & Replication lets you encrypt backup files and restore data from encrypted backups even if you have lost a password. To enable backup file encryption, select the **Enable backup file encryption** check box and click **Add** on the right to specify the necessary password.

Veeam Backup & Replication lets you decrypt backup files even if you have lost or forgotten the password. To learn more, see the **Restoring Data from Encrypted Backup File Without Password** scenario.
8. Open the **Notifications** tab. Select the **Send email notifications to the following recipients** check box. When the job completes, you will receive a notification with details on the job performance. You will be able to receive e-mail notifications only if you specify global e-mail settings. To specify e-mail settings, select **General Options** from the main menu.

![Advanced Settings](image)

**NOTE:**

Make sure that you specify your email address once: either in the **To** field in general notification settings or in job notification settings. If you specify both, you will receive two identical notifications when the job is completed.

9. Open the **Hyper-V** tab.

10. If you back up a non VSS-aware VM (for example, Linux-based VMs), select the **Enable Hyper-V guest quiescence** check box.

Make sure that the **Take crash consistent backup instead of suspending VM** check box is selected. Veeam Backup & Replication will use the crash-consistent method instead of offline backup and will not bring the VM offline.
11. Make sure that the **Use changed block tracking data** check box is selected. In this case, Veeam Backup & Replication employs its proprietary changed block tracking technology. Instead of scanning the VM image to know which data blocks have changed since the previous job run, Veeam Backup & Replication queries the CBT driver to get the list of changed blocks. Use of CBT increases the speed and efficiency of block-level incremental backups. For example, if only 5% of a VM changed since the last backup, incremental backup will be performed 20 times faster.
Step 7. Specify additional guest OS processing options

At the **Guest Processing** step of the wizard, you can enable additional options for VM guest OS processing:

- Application-aware image processing, which will ensure proper restore of VSS-aware applications. To back up running VMs with VSS-aware applications, Veeam Backup & Replication uses application-aware image processing based on Microsoft VSS. Jobs with application-aware image processing produce transactionally consistent backups, that, unlike crash consistent backups, ensure proper recovery of virtualized applications without any data loss.

- Guest OS file indexing, which will enable you to search for guest OS files in backed up VMs and restore files in 1 click. With this option selected, Veeam Backup & Replication creates a catalog (or index) of VM guest OS files. To learn about the 1-click restore scenario, see the **Searching for Guest OS Files and Performing 1-Click Restore** section.

To enable application-aware image processing and indexing:

1. At the **Guest Processing** step of the wizard, select the **Enable application-aware processing** check box.

2. Select the **Enable guest file system indexing** check box.

3. Specify credentials for the user account with Local Administrator permissions on all VMs included into the job: click **Add** on the right of the **Credentials** field and specify the user name and password. If you have specified credentials before, you can simply select them from the **Credentials** list. OS credentials are required to install, start and remove Veeam’s runtime process that coordinates indexing and VSS activities inside the VM.
By default, the specified guest OS credentials are used for all VMs processed by the backup job. If you back up several VMs that use different guest OS credentials, click **Credentials**. Select a VM in the list and click **Set User > Standard credentials/ Linux credentials**. Then specify guest OS credentials with Local Administrator permissions for this VM. Repeat the procedure for all VMs in the job.

4. To specify advanced options for VSS processing, click **Applications**. Select a VM in the list and click **Edit**.

5. On the **General** tab, select the **Try application processing, but ignore failures** option to continue the backup job even if VSS errors occur. If application-aware image processing fails during the job, Veeam Backup & Replication will create a crash-consistent backup.

6. Make sure that the **Process transaction logs with this job** option is selected to correctly handle transaction logs after the backup job is completed. In this case, if the backup job finishes successfully, Veeam Backup & Replication will truncate transaction logs so that they do not overflow storage space. If together with Veeam Backup & Replication you use a third-party backup tool that maintains consistency of transaction logs, select the **Perform copy only** option to prevent possible conflicts.
**NOTE:**
If you add a virtualized Microsoft SQL Server to the backup job, you can configure the job to copy transaction logs. To learn more, see Backing up and Restoring Microsoft SQL Server Databases.

7. Click **Indexing**, select the necessary VM in the list and click **Edit** > **Windows indexing** or **Linux indexing**. Select **Index everything** to perform indexing of the entire guest file system.
Step 8. Specify job scheduling settings

A backup job can be run manually, or scheduled to run periodically. To schedule a backup job:

1. At the Schedule step of the wizard, select the Run the job automatically check box. If you do not select this check box, the job will be saved and you will have to run it manually.

2. Select the schedule type: daily, monthly, periodically or continuously. You can also chain the jobs so that they run one after another.

3. Make sure the Retry failed VM processing check box is selected. During the retry cycle, only VMs that failed during the main backup cycle will be processed.

4. Select the Terminate job if it exceeds allowed backup window check box and click Window. Define the backup window for your environment. In case the created job overlaps the specified window, it will be automatically terminated not to produce additional overhead on your virtual environment.

5. Click Apply.
Step 9. Review job settings and start the job

1. Review the summary of backup job settings.

2. Select the **Run the job when I click Finish** check box and click **Finish**. The job will start.
Step 10. Monitor job performance in real time

When the job is running, you can view job statistics in the real-time mode. Job statistics provide detailed data on the job: job progress, duration, processing rate, performance bottlenecks, the amount of data processed, read and transferred and other details of the job performance. Beside general job statistics, you can view detailed data for each VM or VM container processed by the job.

1. Open the Home view.
2. Select the Jobs node in the inventory pane.
3. Double-click the job in the working area and click Show Details. Now you can track the job performance as the job runs.
4. Select the name of a specific VM or a VM container to view detailed statistics for this specific object only. Note that Veeam Backup & Replication processes all VMs and VM containers in the job in parallel.

5. Wait for the job to complete. Note that the job must complete with the Success or at least the Warning status. If the job completes with the Failed status, the backup file will not be created and you will not be able to perform restore operations.
Step 11. Perform incremental backup

To perform incremental backup of a VM, do the following:

1. Open the **Home** view.
2. Select the **Jobs** node in the inventory pane.
3. Right-click the job in the working area and select **Start**. Wait for the job to complete. Note that the job must complete with the **Success** or at least the **Warning** status.
Validation

After a backup job completes, the resulting backup file is stored to the backup repository that you have selected as a backup target. Veeam Backup & Replication creates a full backup file, VBK, during the first run of a backup job. During every next job run, it copies changes that were made to the VM since the last backup, whether full or incremental.

Depending on the backup mode you selected, Veeam Backup & Replication handles incremental changes differently:

- If you use the incremental backup mode (forever forward incremental or forward incremental), Veeam Backup & Replication saves incremental changes to the VIB file next to the VBK file on the backup repository.
- If you use the reversed incremental backup mode, Veeam Backup & Replication injects copied changes to the full backup file and saves replaced blocks of data as a reversed increment file, VRB, next to the VBK file on the backup repository.

Additionally, next to backup files, Veeam Backup & Replication creates a backup metadata file, VBM, that contains information on the backup job, VMs in the backup, number and structure of backup files, restore points and so on. This metadata file facilitates import of backups and mapping of backup jobs to existing backups.

To check backup results:
1. Open the **Files** view.
2. In the inventory pane, expand the backup repository file tree.
3. Open the target folder on the backup repository. In this folder, find the subfolder with the backup job name and open it. Make sure that it contains a VBK, VIB/VRB and VBM files.
4. Open the **Home** view.
5. Select the **Jobs** node in the inventory pane. Double-click the backup job in the working area. Check the job results.
6. If you have chosen to receive an e-mail message once the job is completed, open your email client and check the **Inbox** folder. Make sure that you have two incoming e-mails with job results: one for the full backup and one for the incremental backup.
Backing up and Restoring Microsoft SQL Server Databases

To protect a virtualized Microsoft SQL Server, you can configure a backup job that will create image-level VM backups and, in addition, copy database transaction logs. Image-level backups will capture the VM state at specific points in time. Transaction logs will keep records of all transactions performed against protected databases since the moment of the last backup. If a Microsoft SQL Server VM fails, you can recover the VM from the necessary restore point and then apply transaction logs to get databases on the Microsoft SQL Server to the required state between backups.

To configure a backup job that copies transaction logs, you must create a regular backup job and specify advanced settings for transaction logs shipping. In these settings, you define:

- How often you want to back up transaction logs
- How transaction logs must be shipped to the destination
- How long transaction logs must be retained

With these settings enabled, Veeam Backup & Replication actually creates two jobs linked with each other:

- A regular backup job responsible for creating image-level backups
- An auxiliary job responsible for shipping database transaction logs

The regular backup job runs by the defined job schedule. It creates image-level backups and saves them on the backup repository. After the image-level backup has been successfully created, Veeam Backup & Replication truncates transaction logs on the virtualized Microsoft SQL Server.

The auxiliary backup job runs continuously. The job copies transaction logs accumulated between VM restore points at scheduled intervals, for example, every 15 minutes. As a result, on the backup repository you will have a chain of restore points and a set of transaction logs that cover intervals between these restore points.

Veeam Backup & Replication ships transaction logs to the backup repository and saves them in files of VLB format next to VM image-level backups. To ship transaction logs from the virtualized Microsoft SQL Server to the backup repository, Veeam Backup & Replication uses log shipping servers — Microsoft Windows machines added to the backup infrastructure. You can select explicitly what log shipping servers you want to use, or let Veeam Backup & Replication assign log shipping servers automatically.

For restore operations, Veeam Backup & Replication offers a special tool — Veeam Explorer for Microsoft SQL Server. Veeam Explorer for Microsoft SQL Server is integrated with Veeam Backup & Replication. The explorer is installed automatically when you deploy Veeam Backup & Replication.

Veeam Explorer for Microsoft SQL Server supports a number of restore scenarios:

- You can restore a database to a specific point in time or to a specific transaction.
- You can restore a database to a specific point in time or transaction and export it to the necessary location.
Evaluation Case

In this exercise, you will back up a Microsoft SQL VM and restore a database on the Microsoft SQL Server to a specific transaction using the created backup. To do this, you will perform the following actions:

1. Configure a backup job that will create a Microsoft SQL VM backup and copy transaction logs.
2. Use the created VM image-level backup and transaction logs to recover a database on the Microsoft SQL Server to a specific transaction with Veeam Explorer for Microsoft SQL Server.

It is strongly recommended that you use a non-production Microsoft SQL Server with a sample database for this exercise.

Prerequisites

Make sure that the *Full* or *Bulk-logged* recovery model is enabled for the database on the Microsoft SQL Server that you plan to back up. If the recovery model is set to *Simple*, Veeam Backup & Replication will not detect and process transaction logs.
Procedure

Step 1. Configure the backup job for a Microsoft SQL VM

1. In Veeam Backup & Replication, configure a backup job that processes a Microsoft SQL Server VM. For details, see the Performing Backup exercise.

2. At the Guest Processing step of the New Backup Job wizard, select the Enable application-aware processing check box. In the Guest OS credentials section, specify a user account to connect to the VM guest OS. The user account must have the sysadmin privileges on the Microsoft SQL Server. In the opposite case, Veeam Explorer for Microsoft SQL Server will fail to automatically identify Microsoft SQL databases in the created VM backup.

3. Click Applications.

4. Select the Microsoft SQL Server VM in the list and click Edit.

5. In the Transaction logs section, make sure that the Process transaction logs with this job option is selected.

6. Open the SQL tab.

7. Select the Backup logs periodically option.

8. In the Backup logs every <N> minutes field, specify how often you want to ship transaction logs from the Microsoft SQL Server VM to the backup repository. By default, Veeam Backup & Replication ships transaction logs every 15 minutes.

9. In the Retain log backups section, specify the retention policy for transaction logs. You can store them for a specific number of days or until a preceding image-level backup is removed from the backup chain.
10. In the **Log shipping servers** section, leave the **Automatic selection** option selected. Veeam Backup & Replication will automatically identify the least loaded Microsoft Windows server in your backup infrastructure and use this server to ship transaction logs to the backup repository.

11. At the **Schedule** step of the wizard, define scheduling settings for the job. If you do not specify that the job must run automatically by the defined schedule, the backup job will be unable to ship transaction logs to the backup repository.

12. Finish working with the wizard and run the job to produce an image-level backup of the Microsoft SQL Server VM.

13. When you create a backup job that processes a Microsoft SQL Server VM and enable transaction log shipping, Veeam Backup & Replication creates two jobs: one processing the Microsoft SQL Server VM and the other one shipping transaction logs. In the inventory pane of the **Home** view, expand the **Last 24 hours** node to see the created jobs.
14. After the image-level backup has been created, perform some transaction on the database on the Microsoft SQL Server VM that you have backed up. For example, if you use a test database, you can manually run a simple Microsoft SQL script to insert a record into the database or drop a record.

15. Wait for the period of time that you have defined in the **Backup logs every <N> minutes** field. After this period has expired, Veeam Backup & Replication will ship transaction logs and store them in a file of VLB format on the target backup repository, next to the image-level backup of the Microsoft SQL Server VM.
Step 2. Recover a database to a specific transaction

1. Open the **Home** view.

2. In the inventory pane, click the **Backups** node.

3. In the working area, expand the backup job processing the Microsoft SQL Server VM, right-click the Microsoft SQL Server VM and select **Restore application items > Microsoft SQL Server databases**.

4. Pass through the steps of the **Microsoft SQL Server Database Restore** wizard: select a restore point and specify a restore reason. At the last step of the wizard, click **Finish** to start the recovery process. Veeam Backup & Replication will automatically mount the Microsoft SQL Server VM file system to the Veeam backup server, locate the Microsoft SQL database and attach it to a staging Microsoft SQL Server — Microsoft SQL Server on which the Veeam Backup & Replication database is deployed. After that, Veeam Backup & Replication will automatically open the database in Veeam Explorer for Microsoft SQL Server.
5. In the left pane of Veeam Explorer for Microsoft SQL Server, right-click the necessary database and select **Restore point-in-time state to <Microsoft SQL Server\Instance Name>**.

6. Veeam Backup & Replication will launch the Restore wizard. At the **Specify restore point** step of the wizard, select **Restore to a specific point in time**. Use the slider below to define the exact point in time to which you want to restore the database.

7. Select the **Perform restore to the specific transaction** check box and click **Next**.

8. At the **Fine-tune the restore point** step of the wizard, select a transaction to which you want to restore the database and click **Restore**.

9. Veeam Backup & Replication will start restoring database to the selected transaction. When the restore process is complete, Veeam Explorer for Microsoft SQL Server will display a popup message to notify you of the restore operation results.

**Validation**

Check the state of the restored database on the Microsoft SQL Server VM and make sure it has been restored to the necessary state.
Performing Full VM Restore

If a production VM has failed, you can restore it from the backup with full VM recovery. You can restore a single VM or a multiple VMs at once, both to the original location or to a new location. VM(s) can be recovered to the latest state or any valid point in time.

When Veeam Backup & Replication creates a backup of a VM, it additionally stores information about the initial VM location to the backup file. As all initial VM settings are available, restore of a VM to the original location is extremely fast: you can do it basically in one click. Restore to the original location mitigates the risk of operator's errors: you do not have to provide any VM data during the restore process, so the chance to specify wrong settings is minimal.

Evaluation Case

In this exercise, you will restore a VM from the backup to its original location and power it on on the Hyper-V host.

Prerequisites

- You can restore a VM from any backup that has been successfully run at least once. Open the Home view, select the Backups node in the inventory pane. Then expand the backup job and verify that there is at least one restore point available for the VM.

**NOTE:**

When you restore a VM to the original location, Veeam Backup & Replication automatically deletes the initial VM. For safety's sake, make sure that you use a non-production VM for this exercise.
Procedure

To restore a full VM to its original location, perform the following steps:

1. Open the **Home** view.

2. In the inventory pane, select the **Backups > Disk** node. Expand the backup job in the working area, right-click the necessary VM in the corresponding backup job and select **Restore entire VM**.

3. At the **Virtual Machines** step of the wizard, select the VM in the list, click **Point** on the right and choose the necessary restore point. If you select an incremental restore point, Veeam Backup & Replication will automatically restore data blocks from the full backup file and the chain of incremental backup files.

4. At the **Restore mode** step of the wizard, select **Restore to the original location**.
5. Select **Quick rollback**. Veeam Backup & Replication will perform incremental VM restore — retrieve from the backup file only those data blocks that have changes since the selected restore point was created and write these data blocks to the source volume. This option lets you significantly speed up the restore process.

<table>
<thead>
<tr>
<th>Full VM Restore Wizard</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtual Machines</strong></td>
</tr>
<tr>
<td><strong>Restore Mode</strong></td>
</tr>
<tr>
<td>- Restore to the original location</td>
</tr>
<tr>
<td>Quick rollback (restore changed blocks only)</td>
</tr>
<tr>
<td>Reason</td>
</tr>
<tr>
<td>Summary</td>
</tr>
</tbody>
</table>

6. At the **Reason** step of the wizard, specify the reason for restoring the VM.

<table>
<thead>
<tr>
<th>Full VM Restore Wizard</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtual Machines</strong></td>
</tr>
<tr>
<td><strong>Restore Mode</strong></td>
</tr>
<tr>
<td>Reason</td>
</tr>
<tr>
<td>Summary</td>
</tr>
</tbody>
</table>

7. At the last step of the wizard, select the **Power on VM after restoring** check box. Then click **Finish**.
Validation

Open the Hyper-V Manager and make sure that the restored VM is running on the original host.
Restoring Guest OS Files

Together with full VM restore, Veeam Backup & Replication offers Instant File-Level Restore (IFLR) that lets you recover guest OS files and folders from the backup. IFLR does not require you to perform a specific file-level backup. Restore of guest OS files, as well as all other restore options, is available from the same image-level VM backup. Neither should you extract the VM image from the backup prior to restore: VM guest OS files can be recovered on-the-fly, directly from a regular backup or from a VM replica. This makes the restore process extremely fast and does not require you to provision additional storage resources.

Veeam Backup & Replication provides three options for guest OS files recovery:

- Recovery from Windows-based file systems (FAT, NTFS and ReFS)
- Recovery from most commonly used file systems (including Linux, Unix, BSD and so on) with the multi-OS restore wizard
- Universal File-Level Recovery* for any OS or file system through leveraging the Instant VM Recovery technology. To learn about the Instant VM Recovery scenario, see Veeam Backup & Replication User Guide.

You can recover VM guest OS files to the latest state or any valid point in time.

Evaluation Case

In this exercise, you will recover guest OS files and folders from the image-level VM backup and save them to the Veeam backup server.

The exercise covers two evaluation scenarios:

- **Scenario 1.** Recovering guest OS files from the backup of a Windows-based VM.
- **Scenario 2.** Recovering guest OS files from the backup of a Linux-based VM or other non-Windows VM with the help of the multi-OS recovery wizard.
Scenario 1. Restoring VM Guest OS Files (FAT, NTFS, ReFS)

When you recover guest OS files from Windows-based VMs, Veeam Backup & Replication mounts the content of a backup file directly to the Veeam backup server and displays the file tree in the built-in file browser. You can copy the files you need and save them locally or anywhere on the network. You can even point applications to restored files and work with these files as usual.

Prerequisites

- You can restore VM guest OS files from any backup that has been successfully run at least once. Open the Home view, select the Backups node in the inventory pane. Then expand the backup job and check if there is at least one restore point available for the VM.
- Windows file restore mode supports Microsoft Windows file systems only (FAT, NTFS and ReFS). To restore files from VMs running other file systems, use the multi-OS file restore wizard.
- You cannot restore files from a VM if it is currently being backed up or replicated.

Procedure

To restore guest OS files from a Microsoft Windows VM:

1. Open the Home view.
2. In the inventory pane, select the Backups > Disk node. Expand the backup job in the working area, right-click a necessary VM in the corresponding backup job and choose Restore guest files > Microsoft Windows.
3. At the **Restore Point** step of the wizard, select the necessary restore point.

![Image of Restore Point step]

4. At the **Reason** step of the wizard, specify the reason for future reference.

![Image of Reason step]

5. At the last step of the wizard, click **Finish**.
6. Veeam Backup & Replication will display the Backup Browser window with the file system tree of the VM. Right-click the necessary file or folder, select Copy To and browse to the C:\Restored in the Choose folder field.

7. Close the Backup Browser.
Validation

1. Rescan the file hierarchy on the backup server.
   
   Open the **Backup Infrastructure** view. In the inventory pane, select **Managed Servers**. In the list of managed servers, right-click the backup server and choose **Rescan**. Wait for the rescan task to complete and close the window with rescan results.

2. Check restored files on the backup server.
   
   Open the **Files** view. In the inventory pane, expand the file tree under the backup server. Select the **C:\Restored** folder and make sure that the restored files or folders are available there.
Scenario 2. Restoring VM Guest Files (Linux, Unix and so on)

While most of backup tools offer file-level recovery for a very small number of file systems, typically, Windows and rarely Linux, Veeam’s multi-OS restore wizard allows you to recover guest OS files from the most commonly used file systems such as Linux, Unix, BSD, MacOS and many others.

For file-level recovery, Veeam Backup & Replication uses a special FLR helper — a small virtual appliance based on the stripped-down Linux kernel. When you perform file-level restore, Veeam Backup & Replication automatically starts the appliance and mounts VM disks to the FLR appliance as virtual hard drives. Virtual disks are mounted directly from backup files, without prior extraction of the backup content, which makes the restore process much faster in comparison with competitive solutions. You can then copy individual files and folders from VM disks to your local machine drive or a network share.

Prerequisites

- You can restore VM guest files from any backup that has been successfully run at least once. Open the Home view, select the Backups node in the inventory pane. Then expand the backup job and check if there is at least one restore point available for the VM.

- Encrypted LVM volumes are not supported.

Procedure

To restore guest OS files from the backup of a Linux-based VM or other non-Windows VM:

1. Open the Home view.

2. In the inventory pane, select the Backups > Disk node. Expand the backup job in the working area, right-click the necessary VM in the corresponding backup job and choose Restore guest files > Linux and other.
3. At the **Restore Point** step of the wizard, select the necessary restore point.

4. At the **Reason** step of the wizard, specify the reason for future reference.
5. At the last step of the wizard, click **Customize** to specify settings for the FLR appliance. Select Hyper-V host and the network on which the FLR appliance will run.

![FLR Appliance Configuration](image)

6. At the last step of the wizard, click **Finish**. Note that the FLR appliance usually takes 20 seconds or less to boot.

7. Veeam Backup & Replication will display the Backup Browser with the file system tree of the VM. Right-click a file or folder, select **Copy To** to open the **Select Destination** window. In the **Server** field, choose a server to which you want to restore files. In the **Path to folder** field, specify a destination folder.

8. If you are restoring files to the original Linux host, select the **Preserve permissions and ownership** check box so that all user access permissions for the file are preserved in the restored copy.
9. Click **Restore**.
Validation

1. Rescan the file hierarchy on the backup server.
   
   Open the **Backup Infrastructure** view. In the inventory pane, select **Managed Servers**. In the list of managed servers, right-click the server to which you restored files, and choose **Rescan**. Wait for the rescan task to complete and close the window with rescan results.

2. Check restored files on the backup server.
   
   Open the **Files** view. In the inventory pane, expand the file tree under the backup server. Select the destination folder and make sure that the restored files or folders are available there.
Restoring VM Files

Veeam Backup & Replication allows you to restore specific VM files: VHD/VHDX, XML and others. The latter recovery scenario can be used, for example, if one of your VM files is missing or is corrupted and you need to bring it back. With Veeam Backup & Replication, you can restore the required VM file directly from the image-level backup, without prior de-staging of the VM image from the backup file.

VM files can be recovered to the latest state or to any valid point in time; you can bring them to the original location or to a new location.

Evaluation Case

In this exercise, you will recover a VM configuration file, XML, and store to the C:\Restored folder on the Veeam backup server.

Prerequisites

You can restore VM files from any backup that has been successfully run at least once. Open the Home view, select the Backups node in the inventory pane. Then expand the backup job and check if there is at least one restore point available for the VM.

Procedure

To restore a VM configuration file, do the following:

1. Open the Home view.
2. In the inventory pane, select the Backups > Disk node. Expand the backup job in the working area, right-click a necessary VM in the corresponding backup job and choose Restore VM files.
3. At the **Restore Point** step of the wizard, select the necessary restore point. If you select an incremental restore point, Veeam Backup & Replication will automatically restore data blocks from the full backup file and the chain of incremental backup files.

4. At the **Restore Destination** step of the wizard, specify a folder to which VM files must be restored.
   a. In the **Destination** list, choose the backup server.
   b. In the **Path to folder** field, specify a path to the folder to which VM files must be restored, for example: `C:\Restored`.
   c. In the **VM files to restore** section, select a check box next to the XML file.
5. At the **Reason** step of the wizard, specify the reason for future reference and click **Next**.

![Hyper-V Restore Wizard](image)

6. At the last step of the wizard, click **Finish** to restore the VM file.
Validation

1. Rescan the file hierarchy on the backup server.

   Open the Backup Infrastructure view. In the inventory pane, select Managed Servers. In the list of managed servers, right-click the backup server and choose Rescan. Wait for the rescan task to complete and close the window with rescan results.

2. Check restored files on the backup server.

   Open the Files view. In the inventory pane, expand the file tree under the backup server. Select C:\Restored folder and make sure that the restored VMX file is available there.
Creating Backup Copy

According to the 3-2-1 backup rule, you must adhere to the following requirements when building your backup plan:

- You must have at least three copies of data in different locations: production data, backup and its copy.
- You must use two different types of media to store your data, for example, disk storage and tape.
- You must keep at least one copy of your data offsite, for example, in the cloud or in the remote site.

With the backup copying capability in Veeam Backup & Replication, you can create several instances of the same backup file and copy them to secondary backup repositories that perform the role of the long-term storage. Secondary backup repositories can be located in the same site as the source one or can be created offsite. The backup copy file has the same format as the primary backup so you can restore necessary data directly from it in case a disaster strikes.

During the backup copying process, Veeam Backup & Replication does not simply copy a backup file from one backup repository to another. Instead, Veeam Backup & Replication retrieves data blocks necessary to create a restore point as of the latest point in time and copies this data to the target backup repository. The backup chain produced on the target backup repository is forever forward incremental: the first restore point in the chain is a full backup and all subsequent restore points are incremental backups.

The backup copy process is job-driven. When you create a backup copy job, you define what backup file you want to copy, the target repository for storing the copy, retention policy and other settings for the copying process. The backup copy job supports the GFS retention scheme, allowing you to design a long-term archiving plan.

Unlike the backup job that typically runs on a specific schedule, the backup copy job runs continuously, in cycles. By default, a new backup copy cycle begins every day; however, you can specify any time interval needed. At the beginning of every backup copy interval, Veeam Backup & Replication checks the source backup repository: if a new restore point has been added to the primary backup chain, Veeam Backup & Replication automatically copies it to the target backup repository. After that, the backup copy job is put on hold until a new backup copy interval begins and a new point appears on the source backup repository.

Evaluation Case

In this exercise, you will create a copy of the backup file that has been created in the Performing Backup exercise with the evaluation backup job. The backup file will be copied from the source backup repository and written to the target backup repository (default backup repository).

Prerequisites

- The source and target backup repositories that will take part in the backup copy process must be added to the Veeam Backup & Replication console.
- You must have a backup that has been successfully run at least once. Open the Home view, select the Backups node in the inventory pane. Then expand the backup job and check if there exist VM backups that you can copy.
Procedure

To create a copy of the backup file:

1. Open the **Home** view.

2. On the **Home** tab, click the **Backup Copy** button and select **Microsoft Hyper-V backup** to launch the **New Backup Copy Job** wizard.

3. At the **Job** step of the wizard, specify a name for the created backup copy job.
4. **In the Copy every field**, specify a synchronization time interval, or the length for the backup copy cycle. At the beginning of every synchronization interval, Veeam Backup & Replication checks the source backup repository. If a new restore point has appeared, Veeam Backup & Replication copies this restore point to the target backup repository.

5. **At the Virtual Machines step of the wizard**, click **Add** and select **From jobs**. In the list of jobs, select the backup job that is used to create the backup you want to copy. Veeam Backup & Replication will monitor the source backup repository on which the backup job stores the resulting backup file. If Veeam Backup & Replication detects a new restore point on the source backup repository at the beginning of a new synchronization interval, Veeam Backup & Replication will automatically trigger a new backup copy cycle and copy a new restore point to the target backup repository.
6. At the **Target** step of the wizard, select the target backup repository from the **Backup repository** list.

7. In the **Restore points to keep** field, specify the number of restore points you want to retain. By default, Veeam Backup & Replication keeps 7 restore points on the target backup repository.

8. During the backup copying process, backup data can be transferred directly, from the source backup repository to the target backup repository, or through a pair of WAN accelerators. The latter scenario is recommended for copying backups offsite or over slow network connections. To learn more about WAN acceleration, see [Veeam Backup & Replication User Guide](#).

In this exercise, both backup repositories are located onsite: for this reason, you will use the **Direct** data transfer path. Leave the **Direct** option selected.
9. At the **Schedule** step of the wizard, define the period of time when the backup copy job is allowed to transport data over the network. The backup copy window can be helpful if you do not want the backup copy job to produce unwanted overhead for the production environment or do not want the job to overlap the production hours.

10. Click **Apply**.

11. At the last step of the wizard, select the **Enable the job when I click Finish** check box and click **Finish**. The job will start running in the continuous mode.

12. To monitor the job performance, click the **Backup Copy** node under **Jobs** in the inventory pane. Double-click the created backup copy job in the working area: now you can monitor the job performance in the real-time mode.
Validation

1. Open the **Files** view.
2. Expand the file tree of the target backup repository.
3. Find a subfolder with the backup copy job name and make sure a full backup file is available in it.
Performing Replication

With Veeam Backup & Replication, you can not only back up, but also replicate your VMs. When you replicate a VM, Veeam Backup & Replication creates an exact copy of a production VM in the native Microsoft Hyper-V format on a spare Hyper-V host and maintains this copy in sync with the original VM.

Replication provides the best RTOs as you actually have a copy of a VM in a ready-to-start state. If the primary VM goes down for some reason, you can immediately fail over to the VM replica and restore critical services with minimum downtime. For this reason, replication is most commonly used for VMs running tier 1 applications.

Replication is a job-driven process. During the first run of a replication job, Veeam Backup & Replication copies the whole VM image and registers a replicated VM on the target Hyper-V host. During next cycles of a job, Veeam Backup & Replication copies only incremental changes and creates restore points for a VM replica so you can recover your VM to the necessary state. Every restore point is in fact a Microsoft Hyper-V checkpoint. When you perform incremental replication, data blocks that have changed since the last replication cycle are written to the checkpoint differential disk. The number of restore points in the chain depends on your retention policy settings.

To provide extremely fast incremental replication, Veeam Backup & Replication uses its proprietary changed block tracking technology. With changed block tracking, you can replicate much faster and can schedule replication jobs as often as every few minutes. So you get near-CDP at only a fraction of the cost of traditional CDP solutions.

With Veeam Backup & Replication, you can perform both onsite replication for HA and offsite replication for DR scenarios. For replication over WAN or slow links, Veeam Backup & Replication provides a number of means to optimize data transmission: it performs inline deduplication and compresses replica traffic. You can also configure network throttling rules to prevent replication jobs from consuming the entire bandwidth of your environment and perform replica seeding.

Evaluation Case

In this exercise, you will create a replica of a VM on the target host, and create one restore point next to a full VM replica.

Please note that this guide describes replication to a local target host located in the same network. To learn about replicating offsite, see Veeam Backup & Replication User Guide.

Prerequisites

- All backup infrastructure components that will take part in the replication process must be added to the Veeam Backup & Replication console. These include a source and target Hyper-V hosts. If you plan to use a distributed deployment scenario, you must also have an offhost backup proxy.
- [Optional] To receive an e-mail notification when a replication job completes, specify global e-mail notification settings. To do that, select General Options from the main menu of Veeam Backup & Replication and specify necessary settings on the E-mail Settings tab.
- [Optional] To evaluate the application-aware image processing feature, make sure that at least one of replicated VMs runs Microsoft Windows 2003 SP1 or later.
Procedure

To replicate a VM, perform the following steps.

Step 1. Create a replication job

1. Open the **Home** view.

2. On the **Home** tab, click the **Replication Job** button and select **Microsoft Hyper-V** to launch the **New Replication Job** wizard.

3. At the **Name** step of the wizard, specify a name for the created replication job.
Step 2. Add VMs to the replication job

You can replicate individual VMs or VM containers: Hyper-V hosts, clusters, SCVMM and so on. Jobs with VM containers are dynamic in nature: if a new VM is added to the container after the replication job is created, the job is automatically updated to include the new VM.

1. At the **Virtual Machines** step of the wizard, click **Add**.

2. To quickly find a VM or VM container, specify the name of the object that you want to find in the search field and click the **Start search** button on the right. Select a VM or VM container in the displayed list and click **Add**.
Step 3. Exclude VMs and VM disks

If you create a replication job for a VM container, you can exclude specific VMs or VM containers from the replication job. You can also select which VM disks to replicate.

1. At the **Virtual Machines** step of the wizard, click **Exclusions**.

2. On the **VMs** tab, click **Add**. Select VMs that must be excluded. To quickly find a VM or VM container, enter the name of the object you want to find in the search field and click the **Start search** button on the right.

3. On the **Disks** tab, select a VM and click **Edit** to select disks that must be replicated. This functionality is useful, for example, if you only want to replicate VM system drives.

   If you want to exclude disks of a VM added as part of a container, click **Add VM** on the right to include the VM in the list as a standalone instance.

4. Click **OK**.

5. Click **Recalculate** to see the total size of replicated objects.
Step 4. Define the VM replication order

If you have included a number of VMs or VM containers in the replication job, you can specify the order in which VMs must be processed. This will help you make sure that the most important VMs in the job are processed first, for example, if you must fit into the backup window and you are not sure how much time VM processing will take.

1. At the **Virtual Machines** step of the wizard, click the added VM in the list.

2. Use the **Up** and **Down** buttons on the right to move the VM higher or lower in the list. The higher is the VM in the list, the higher its priority. If you added a VM container as a single instance, VMs inside the container will be processed at random.
Step 5. Select replica destination

At the **Destination** step of the wizard, specify the target for a replicated VM.

1. Click **Choose** next to the **Host** or **Cluster** field and select a host on which the VM replica must be registered.

2. Click **Choose** next to the **Path** field and specify a path to a location where VM replica files should be stored.
Step 6. Specify general settings for the replication job

You must point the replication job to a backup repository. The backup repository stores replica metadata (checksums of read data blocks) required to streamline incremental passes of the job.

1. At the **Job Settings** step of the wizard, in the **Repository for replica metadata** list, select the backup repository that you have configured.
   
   A metadata file created by the job will be stored to this backup repository.

2. In the **Replica name suffix** field, specify a suffix to append to the name of the replica. Veeam Backup & Replication will use the name of the primary VM with the suffix for the name of the replica VM.

3. Select the maximum number of restore points that you want to keep on disk. By default, Veeam Backup & Replication keeps 14 restore points.

![New Replication Job wizard](image-url)
Step 7. Specify advanced replica settings

At the **Job Settings** step of the wizard, click **Advanced** to specify additional settings for the replication job.

1. On the **Traffic** tab, make sure the **Exclude swap file blocks** check box is selected.

   Swap files are dynamic and change intensively between runs of a replication job. With this option selected, Veeam Backup & Replication will identify data blocks of the Microsoft Windows pagefile in the guest OS and exclude them from processing, which will result in increased performance and a smaller size of increments.

2. During replication, Veeam Backup & Replication compresses VM data to reduce load on the network. Veeam Backup & Replication offers 5 compression levels that provide different compression ratios to meet the needs of your environment: **None**, **Dedupe-friendly**, **Optimal**, **High** and **Extreme**.
3. Open the **Notifications** tab. Select the **Send email notifications to the following recipients** check box and specify the e-mail address.

When the job completes, you will receive an e-mail notification with details on job performance. Note that you will be able to receive an e-mail notification only if you specify global e-mail settings. To specify e-mail settings, select **General Options** from the main menu.

**NOTE:**

Make sure that you specify your e-mail address once: either in the **To** field in general notification settings, or in job notification settings. If you specify both, you will receive two identical notifications when the job is completed.
4. Open the Hyper-V tab.

5. If you replicate a non VSS-aware VM, for example, a Linux-based VM, select the Enable Hyper-V guest quiescence check box.

6. Make sure that the Take crash consistent backup instead of suspending VM check box is selected. Veeam Backup & Replication will use the crash-consistent method instead of offline backup and will not bring the VM offline.

7. Make sure that the Use changed block tracking data check box is selected. In this case, Veeam Backup & Replication employs its proprietary changed block tracking technology. Instead of scanning the VM image to know which data blocks have changed since the previous job run, Veeam Backup & Replication queries the CBT driver to get the list of changed blocks. Use of CBT increases the speed and efficiency of block-level incremental replication. For example, if only 5% of a VM changed since the last replication cycle, incremental replication will be performed 20 times faster.
Step 8. Specify replication data path

At the Data Transfer step of the wizard, you must select backup infrastructure components that will be used for the replication process and choose a path for VM data transfer.

1. Click Choose next to the Source proxy field. Make sure that the Off-host backup option is selected in the Backup Proxy window. Veeam Backup & Replication will offload the replication processing from the source Hyper-V host to the offhost backup proxy you have configured and thus reduce the load on the production host.

2. Make sure that the Failover to onhost backup mode if no suitable backup proxies are available check box is selected. If the offhost backup proxy is not available or is not properly configured, Veeam Backup & Replication will use the onhost backup method to process VMs.

3. During the replication process, VM data can be transferred directly thorugh backup proxy(ies) to the target datastore or via a pair of WAN accelerators. The latter scenario is recommended for replicating VM offsite or over slow network connections. To learn more about WAN acceleration, see Veeam Backup & Replication User Guide.

In this exercise, source and target hosts are located onsite. For this reason, leave the Direct option selected.
Step 9. Specify additional guest OS processing options

To replicate VMs running VSS-aware applications, Veeam Backup & Replication uses application-aware image processing based on Microsoft VSS. Jobs with application-aware image processing produce transactionally consistent replicas, that, unlike crash consistent replicas, ensure proper recovery of virtualized applications without any data loss.

To enable application-aware image processing:

1. At the Guest Processing step of the wizard, select the Enable application-aware processing check box.

2. Specify guest OS credentials with Local Administrator privileges on all VMs included in the job. OS credentials are required to install, start and remove a runtime process that coordinates VSS activities inside the VM.

3. By default, the specified guest OS credentials are used for all VMs processed by the replication job. If you replicate several VMs that use different guest OS credentials, click Credentials. Select a VM in the list and click Set User. Then specify guest OS credentials with administrator privileges for this specific VM. Repeat the procedure for all VMs in the job.

4. To specify advanced options for VSS processing, click Applications. Select a VM in the list and click Edit.
5. On the **General** tab, select **Try application processing, but ignore failures** to continue the replication job even if VSS errors occur. If VSS processing fails during the job, Veeam Backup & Replication will create a crash-consistent VM replica.

6. Make sure that the **Process transaction logs with this job** option is selected to correctly handle transaction logs after the replication job is complete. In this case, if the replication job finishes successfully, Veeam Backup & Replication will truncate transaction logs so that they do not overflow storage space. If you use a third-party backup tool that maintains the consistency of transaction logs, select the **Perform copy only** option to prevent possible conflicts.
Step 10. Specify job scheduling settings

A replication job can be run manually, or scheduled to run periodically. To schedule a replication job:

1. At the **Schedule** step of the wizard, select the **Run the job automatically** check box. If you do not select this check box, the job will be saved and you will have to run it manually.

2. Select the schedule type: daily, monthly, periodically or continuously. You can also chain the jobs so that they run one after another.

3. Select the **Retry failed VM processing** check box. During the retry cycle, only VMs that have failed during the main replication cycle will be processed.

4. Select the **Terminate job if it exceeds allowed backup window** check box and click **Window**. Define the backup window for your environment. In case the created job overlaps the specified window, it will be automatically terminated not to produce additional overhead on the virtual environment.

5. Click **Apply**.

![New Replication Job](image)
Step 11. Review job settings and start the job

1. Review the summary of replication job settings.

2. Select the **Run the job when I click Finish** check box and click **Finish**. The job will start.
Step 12. Monitor job performance in real time

When a replication job is running, you can view job statistics in the real-time mode. Job statistics provide detailed data on the job: job progress, duration, processing rate, performance bottlenecks, the amount of data processed, read and transferred, and other details of the job performance.

In addition to general job statistics, you can view detailed data for each VM or VM container processed by the job.

1. Open the **Home** view.
2. In the inventory pane, select **Jobs > Replication**.
3. Double-click the job in the working area and click **Show Details**. Now you can track the job performance as the job runs.
4. Select the name of a specific VM or a VM container to view detailed statistics for this specific object only.
5. Wait for the job to complete. Note that the job must complete with the **Success** or at least the **Warning** status. If the job completes with the **Failed** status, the VM replica will not be created, and you will not be able to perform failover and failback operations.
Step 13. Perform incremental replication

To perform incremental replication of a VM, do the following:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs > Replication**.
3. Right-click the job in the list and select **Start**. Wait for the job to complete. Note that the job must complete with the **Success** or at least the **Warning** status.

Validation

To check replication results:

1. Open the Hyper-V Manager and make sure that a VM replica has been created.
2. In Veeam Backup & Replication, open the **Files** view.
3. In the inventory pane, expand file tree of the target Hyper-V host. Make sure that the **Replicas** folder has been created on the target storage and that this folder contains files of a VM replica.
4. Open the **History** view and select the **Jobs** node in the inventory pane. Double-click the replication job in the list. Check the properties of the created replica.
5. If you have configured to receive an e-mail message once the job completes, open your e-mail client and check the **Inbox** folder. Make sure that you have two e-mail messages with job results — one for the full replication, and another one for the incremental replication.
Failing Over a VM Replica

If a primary VM in the production site becomes unavailable, you can quickly restore services by failing over to its replica. When you perform failover, the VM replica takes over the role of the original VM: you switch from the production VM to its replica and shift your processes from the production host to a secondary host. As a result, you have your VM up and running within a couple of minutes, and your users can access services and applications they need with minimal disruption.

In Veeam Backup & Replication, you can fail over to the latest state of a replica or to any of its valid restore points.

Failover itself is an intermediate step that needs to be finalized. Depending on a disaster recovery scenario, you can do one of the following:

- **Perform permanent failover.** When you perform permanent failover, you 'commit failover'. That is, you permanently switch from the original VM to a VM replica and use this replica as the original VM. This scenario is acceptable if the original VM and a VM replica are located in the same site and are nearly equal in terms of resources. In this case, your users will not experience any latency in ongoing operations.

- **Perform failback.** When you perform failback, you 'return' from a VM replica to the original VM after the problem in the production site is eliminated. All changes that took place while the VM replica was running are transferred to the original VM. You can follow this scenario if your VM replica is located in a DR site and is running on a lower tier host and storage: that is, it is not intended for continuous operations.

- **Undo failover.** When you undo failover, you switch back to the original VM and work with it in the normal operation mode. All changes made to the VM replica are discarded. You can follow this scenario if you plan to perform some testing and troubleshooting of your VM replica and do not want to affect your production environment in any way.

Veeam Backup & Replication supports failover and failback operations for one VM and for a number of VMs. This way, if you have a problem with Hyper-V host, you can restore its work with minimum downtime.

**Evaluation Case**

In this exercise, you will fail over from the original VM to the VM replica you created in the previous exercise, and undo failover to get back to the production VM.

When you fail over from a running original VM to a VM replica, Veeam Backup & Replication does not power off the original VM, it simply powers on the VM replica.

**Prerequisites**

The failover option can be used with any VM replica that was successfully created at least once. Open the **Home** view, and select the **Replicas** node in the inventory pane. Check if there is at least one restore point available for the replicated VM.
Procedure
To fail over to a VM replica:

1. Open the **Home** view.
2. In the inventory pane, select the **Replicas** node.
3. Right-click the replicated VM and select **Failover Now** to launch the **Hyper-V Failover Wizard**.
4. If you want to fail over to a specific restore point, at the **Virtual Machines** step of the wizard, select the VM in the list, click **Point** and choose the restore point to which you want to fail over.
5. At the **Reason** step of the wizard, specify the reason for future reference.
6. At the last step of the wizard, click **Finish** to fail over to a VM replica.
Validation

1. Open the **Home** view.
2. Select the **Replicas** node in the inventory pane.
3. Make sure that the replicated VM is in the **Failover** state.
4. Open the Hyper-V Manager and make sure that the VM replica is powered on.
Undoing Failover

When you undo failover, Veeam Backup & Replication reverts the VM replica to its pre-failover state, powers it off, and deletes all changes that have taken place since the VM replica was powered on. You can use the production VM and perform its replication as usual.

Procedure

To undo failover:

1. Open the Home view.
2. Select the Replicas node in the inventory pane.
3. Right-click the VM and select Undo Failover.
4. In the displayed dialog box, click Yes.
Validation

1. Open the **Home** view.

2. Select the **Replicas** node in the inventory pane.

3. Make sure that the replicated VM is in the **Ready** state.

4. Open the Hyper-V Manager and make sure that the VM replica is powered off.
Failing Back to the Primary VM

If you want to resume operation of a production VM, you can fail back to it from a VM replica. When you perform failback, you get back from the VM replica to the original VM, shift your processes from the secondary host to the production host and return to the normal operation mode.

When you perform failback, Veeam Backup & Replication triggers a failback protective checkpoint of a VM replica. This checkpoint acts as a restore point and saves the pre-failback state of a replica to which you can return afterwards. Veeam Backup & Replication synchronizes the original VM with the VM replica to make sure you get back to the most recent state of a VM. The original VM is then powered on; all replication activities are put on hold.

You can fail back to the VM in the original location or in the new location:

- If you have managed to restore operation of the source host, you can fail back to the original VM on the source host.
- If the source host is not available, you can restore the original VM to a new location and fail back to it. You can also fail back to an entirely new location without restoring the original VM beforehand: in this case, VM replica files will be simply transferred to the necessary destination.

In Veeam Backup & Replication, failback itself is an intermediate action that needs to be finalized. Depending on a disaster recovery scenario, you can do one of the following:

- **Commit failback.** When you commit failback, you finalize recovery of the original VM in the production site. The original VM in the production site or at a new location becomes the primary VM, a VM replica is returned to the normal state and Veeam Backup & Replication resumes replication activities.

- **Undo failback.** If the production VM is not working as expected, you can undo failback and get back to a VM replica. In this case, the VM replica returns to the Failover state.

**Evaluation Case**

In this exercise, you will fail back from a VM replica to the primary VM on the source host, and then commit failback.

**Prerequisites**

You can perform failback for a VM replica in the Failover state. To put the VM replica to this state, make sure you have performed the Failing Over VM Replica exercise. If you have already undone failover, repeat the Failing Over VM Replica exercise for your VM.
Procedure

To fail back to the production VM:

1. Open the **Home** view.
2. In the inventory pane, select the **Replicas** node.
3. Right-click the VM and select **Failback to production** to launch the **Failback Wizard**.

   ![Failback Wizard screenshot](image)

4. At the **Replicas** step of the wizard, click **Next**.
5. At the **Destination** step of the wizard, select **Failback to the original VM**.

6. At the last step of the wizard, select the **Power on VM after restoring** check box and click **Finish**.
Validation

1. Open the **Home** view.
2. In the inventory pane, select the **Replicas** node.
3. Make sure that the replicated VM is in the **Failback** state.
Committing Failback

When you commit failback, you confirm that you want to get back to the production VM. Veeam Backup & Replication resumes replication activities for the VM to which you failed back.

The failback protective checkpoint that saves the pre-failback state of a VM replica is not deleted — Veeam Backup & Replication uses this checkpoint as an additional restore point for VM replica. With the pre-failback checkpoint, Veeam Backup & Replication needs to transfer less changes and therefore puts less load on the network when replication activities are resumed.

Procedure

1. Open the **Home** view.
2. In the inventory pane, select the **Replicas** node.
3. Right-click the VM and select **Commit Failback**.
4. In the displayed dialog box, click **Yes**.
Validation

1. Open the **Home** view.

2. In the inventory pane, select the **Replicas** node.

3. Make sure that the replicated VM is in the **Ready** state.
Distributed Backup Infrastructure Management

For large geographically dispersed virtual environments with multiple Veeam backup servers, it is recommended to use Veeam Backup Enterprise Manager.

Veeam Backup Enterprise Manager is an optional component in the backup infrastructure that federates Veeam backup servers and offers a consolidated view of these servers through a web console. You can centrally control and manage jobs configured on different Veeam backup servers through a single pane of glass, edit and clone jobs, monitor jobs state and get reporting data across all backup servers. Veeam Backup Enterprise Manager also enables you to search for Windows guest OS files in all current and archived backups across your backup infrastructure and restore these files in 1 click.

This section describes a set of exercises that you should perform to learn how to manage a distributed backup infrastructure using Veeam Backup Enterprise Manager.

Exercise List

To evaluate the key features of Veeam Backup Enterprise Manager, perform the following exercises:

<table>
<thead>
<tr>
<th>Exercise</th>
<th>Description</th>
<th>Time Estimates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing and configuring Veeam Backup Enterprise Manager</td>
<td>Install Veeam Backup &amp; Replication on a physical or virtual machine. Add the Veeam backup server to Veeam Backup Enterprise Manager and collect data from the added Veeam backup server.</td>
<td>5-7 minutes</td>
</tr>
<tr>
<td>Searching for guest OS files and restoring them in 1 click</td>
<td>Find a guest OS file in a backup of a Windows-based VM and restore this file directly from Veeam Backup Enterprise Manager to the original VM in 1 click.</td>
<td>1-2 minutes</td>
</tr>
<tr>
<td>Configuring self-service restore</td>
<td>Delegate the file-level restore task to another team member.</td>
<td>2-5 minutes</td>
</tr>
<tr>
<td>Cloning and editing jobs</td>
<td>Clone a created backup job, save it under a new name and edit its settings directly in Veeam Backup Enterprise Manager.</td>
<td>3-5 minutes</td>
</tr>
<tr>
<td>Restoring data from encrypted backups without a password</td>
<td>Create an encrypted backup file and unlock it without a password.</td>
<td>5-7 minutes</td>
</tr>
</tbody>
</table>
Installing and Configuring Veeam Backup Enterprise Manager

Evaluation Case

In this exercise, you will install Veeam Backup Enterprise Manager, connect the Veeam backup server to it and collect data from the connected Veeam backup server. In the production environment, Veeam Backup Enterprise Manager typically federates a number of Veeam backup servers. For evaluation purposes, you can connect one Veeam backup server to Veeam Backup Enterprise Manager.

Prerequisites

- The machine on which you plan to install Veeam Backup Enterprise Manager must meet the system requirements.
- You must have at least one instance of the Veeam backup server installed. On the Veeam backup server, you must have at least one backup or replication job that has been successfully performed.
- If you plan to install Veeam Backup Enterprise Manager on the same machine where the Veeam backup server runs, you must disable all backup and replication jobs and close the Veeam Backup & Replication console.
- Make sure that all necessary ports are open.
Procedure

To install Veeam Backup Enterprise Manager, do the following:

2. Mount the installation image using disk image emulation software, or burn the downloaded ISO image file to a blank CD/DVD or. If you are installing Veeam Backup & Replication on a virtual machine, use built-in tools of the virtualization management software to mount the installation image to the virtual machine.
3. Run the Setup.exe file from the ISO.
4. On the splash screen, click the Veeam Backup Enterprise Manager tile on the right to launch the Veeam Backup Enterprise Manager Setup wizard.

5. At the License Agreement step of the wizard, select I accept the terms in the license agreement.
6. At the **Provide License** step of the wizard, specify the path to the license file you obtained after you downloaded the product from the web site.

   If you are installing Veeam Backup Enterprise Manager on the backup server, you can proceed without providing a license file. In this case, Veeam Backup Enterprise Manager will use the license that is already installed on the backup server.

![Provide License step](image1)

7. At the **Program Features** step of the wizard, leave default settings.

![Program Features step](image2)

8. At the **System Configuration Check** step of the wizard, install missing software components and enable missing features, if any.

![System Configuration Check step](image3)
9. At the **Default Configuration** step of the wizard, specify if you want to use default installations settings or specify installation settings on your own. In the latter case, the setup wizard will include additional steps for configuring the necessary settings.

If you have chosen to specify custom installation settings, pass through the next wizard steps and specify the required settings manually. If you have chosen to use default installations settings, click **Install** to begin installation.

10. When the installation process completes, click **Finish** to close the wizard.

Once the installation process completes, connect the Veeam backup server to Veeam Backup Enterprise Manager.

1. Start Veeam Backup Enterprise Manager by choosing **Programs > Veeam > Veeam Backup Enterprise Manager**.

   To access Veeam Backup Enterprise Manager remotely, use the following address:

   https://enterprise_manager_server_name:9443

2. If you access Veeam Backup Enterprise Manager remotely, specify credentials of a user with Local Administrator rights or the user who installed Veeam Backup Enterprise Manager and click **Login**.
3. Click **Configuration** at the top right corner of the window.

4. In the **Backup Servers** configuration section, click **Add**.

5. In the **Backup Server Settings** window, specify a DNS name or the IP address of the Veeam backup server you want to connect.

6. Provide a name and password of the user account with Local Administrator rights on the added Veeam backup server.

7. Click **OK**.

   Veeam Backup Enterprise Manager will automatically start collecting data about all backup and replication jobs from connected Veeam backup server.
8. To receive consolidated e-mail notifications about the status and summary of all jobs performed in the backup infrastructure, in the configuration menu click **Notifications** and specify e-mail notification settings.
Validation

1. At the top left corner of the window, click **Home** to get back to the main view of Veeam Backup Enterprise Manager.

2. Click the **Last 24 hours** and **Last 7 days** tabs in Veeam Backup Enterprise Manager and make sure that these tabs provide information about backup and replication jobs performed on the Veeam backup server you have connected.

3. If you have configured e-mail notification settings, open your email client and check the **Inbox** folder. Make sure that you have an incoming email about all performed jobs.
Searching for Guest OS Files and Performing 1-Click Restore

Veeam Backup Enterprise Manager allows you to search for Microsoft Windows and Linux guest files in backed up VMs. This can be useful, for example, if you need a file that has been deleted on the VM and you want to restore it from a backup. Once you find the file, you can immediately restore the file directly from Veeam Backup Enterprise Manager with 1 click. The file can be restored to its original location or saved to a local machine.

Evaluation Case

In this exercise, you will delete a file on the original VM, search for it in the backed up VM image and restore it to its original location.

Prerequisites

- Make sure that you have successfully created a backup of a Microsoft Windows or Linux VM with the guest file indexing option enabled.
- Make sure that you have successfully connected the Veeam backup server to Veeam Backup Enterprise Manager and collected data from it.
Procedure

To find and restore a guest OS file, do the following:

1. Delete a file you want to restore on the original VM.
2. In the main view of Veeam Backup Enterprise Manager, click the Files tab.
3. In the Type in VM name field, specify the name of a backed up VM whose file system you want to browse.
4. In the Restore point field, select a restore point from which you want to restore the deleted file.
5. Click the Mount Backup link and wait for Veeam Backup & Replication to mount the content of the backup file to the Veeam backup server.

After the backup is mounted, you can browse guest OS files from the backup.

You can find the necessary guest OS files using the search functionality. In the Search field on the right, type in the name of the necessary file and click the search icon.
6. Right-click the necessary file in the list and select **Restore > Overwrite**.

7. Click **Yes** to confirm the operation.

**Validation**

Open the original VM and make sure that the found file has been successfully restored.
Performing Self-Restore of VM Guest OS Files

You can delegate a task of restoring guest OS files of Windows-based VMs to users having administrator rights on these VMs, for example, to application owners. Delegated file-level restore simplifies the data restore process. Users do not have to wait for backup administrators to recover deleted or modified files and folders.

For delegated file-level restore, Veeam Backup & Replication offers the Veeam Self Service File Restore portal. Authorized users can log on to the portal, browse the content of VM backups and restore the necessary VM guest OS files and folders to the original location or download restored files to the local computer. The restore process does not require any intervention from the backup administrator side: users can perform search and restore operations on their own, just like the administrator working with Veeam Backup Enterprise Manager.

Only authorized users can browse and restore files in the Veeam Self Service File Restore portal. To be able to see the content of VM backups, the user must be added to the Local Administrators group in the VM guest OS. When the user logs on to the portal, the portal displays only those VMs and restore points that the user is permitted to access. Other VMs are not visible to the user.

Evaluation Case

In this exercise, you will perform self-service restore of VM guest OS files from the backup file using the Veeam Self Service File Restore portal.

Prerequisites

- Make sure that the Veeam backup server is connected to Veeam Backup Enterprise Manager.
- Make sure that the Enterprise Plus license is installed on the Veeam Backup Enterprise Manager server. You can use a valid trial license or paid license.
- Make sure that the user account under which you plan to perform self-service restore belongs to a trusted domain or the same domain as the Veeam Backup Enterprise Manager server. Users from untrusted domains cannot use the Veeam Self Service File Restore portal.
Procedure

To restore VM guest OS files using the Veeam Self Service File Restore portal:

1. Log on to the VM whose guest OS files you plan to restore. Make sure that the user account under which you plan to perform self-service restore is added to the local Administrators group on this VM.

2. In Veeam Backup & Replication, configure a backup job that processes this VM. At the Guest Processing step of the New Backup Job wizard, select the Enable guest file system indexing check box and specify a user account for file indexing.

For details, see the Performing Backup exercise.
3. Run the backup job to produce a backup file.

4. Log on to Veeam Backup Enterprise Manager using the Administrator account.

5. Open the Configuration view.

6. In the Backup Servers section, click Start Collecting to collect the latest data about the performed backup job from the Veeam backup server. To check if data has been collected, click Sessions on the left and make sure that the data collection session has completed with the Success status.

7. Sign out from Veeam Backup Enterprise Manager.
8. Together with Veeam Backup Enterprise Manager, the Veeam Backup & Replication setup deploys the Veeam Self Service File Restore portal. To open the portal web console, choose Programs > Veeam > Veeam Self Service File Restore.

To access Veeam Self Service File Restore portal remotely, use the following address:
https://enterprise_manager_server:9443/selfrestore

9. Log on to the Veeam Self Service File Restore portal under the user account that you plan to use to restore VM guest OS files.

10. The portal will display only one tab — Files, with the file tree of the VM guest OS file system. You can choose the necessary VM and a restore point from which you want to restore data.

11. Find the necessary file or folder using the Browse or Search tab on the left, right-click it and select the necessary restore option from the list.
Validation

Open the file or folder restore location and make sure that the file or folder has been successfully restored.
Cloning and Editing Jobs

Veeam Backup Enterprise Manager lets you clone jobs configured on Veeam backup servers. When you clone a job, you create an exact copy of any backup or replication job available in the job list. Configuration details of a created job copy are written to the same Microsoft SQL database where details of the original job are stored. You can work with the created job both in Veeam Backup Enterprise Manager and in the Veeam Backup & Replication console on the Veeam backup server.

The recommended practice is to configure a set of job templates in advance, using the Veeam Backup & Replication console on every managed Veeam backup server. Administrators working Veeam Backup Enterprise Manager can then use these templates for cloning and further editing.

Evaluation Case

In this exercise, you will create a copy of the backup job and edit its settings.

Prerequisites

- Make sure that you have at least one backup job that has been successfully performed on the Veeam backup server.
- Make sure that you have successfully connected the Veeam backup server to Veeam Backup Enterprise Manager and collected data from it.

Procedure

To clone a job, do the following:

1. In Veeam Backup Enterprise Manager, click the Jobs tab.
2. Select the necessary job in the list, click Job at the top of the list and choose Clone.
3. Select the cloned job in the list. The job has the same name as the original job, and has the _cloneN suffix.
4. On the toolbar, click **Job** and select **Edit**.
5. Go through the steps of the wizard and edit the job settings as required.

### Validation

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Select the **Jobs** node in the inventory pane.
3. Make sure that the cloned job is available in the working area.
Restoring Data from Encrypted Backup File Without Password

You can create encrypted backups that are protected with a password.

When you restore data from an encrypted backup on the same backup server, you do not have to specify a password. When you import an encrypted backup on another backup server and restore VM data from it, Veeam Backup & Replication requires a password to unlock the backup content.

In most backup products, if you do not have a password, the backup content will remain locked, and the backup will be of no use. Veeam Backup & Replication lets you decrypt encrypted backups even if you do not have a password, for example:

- The password is lost.
- The user who knows the password has left your organization or does not want to provide the password.
- A third-party organization requires you to decrypt the backup, for example, by a court decree.

To restore data without a password, you must make sure that the backup infrastructure meets the following requirements:

- The backup server that was used for backup encryption and the backup server that will be used for backup decryption must be connected to Veeam Backup Enterprise Manager.
- The backup server and Veeam Backup Enterprise Manager server must have an Enterprise or higher license installed.

In this case, Veeam Backup & Replication will engage an additional master key — Enterprise Manager key, in the encryption process. The Enterprise Manager key consists of two components: public key and private key. The public key is passed to all backup servers that are connected to Veeam Backup Enterprise Manager. The private key is kept only on the Veeam Backup Enterprise Manager server; it is used to decrypt a backup when the password is not available.

To decrypt a backup, you can specify the password or create a request to Veeam Backup Enterprise Manager. An administrator working with Veeam Backup Enterprise Manager will process the request with the Password Recovery wizard — the wizard will apply the private key matching the public key that was used for backup encryption. As a result, you will be able to access backup data in the Veeam Backup & Replication console.

Evaluation Case

In this exercise, you will create an encrypted backup and restore data from it without a password. To do this, you will perform the following steps:

1. Create an encrypted backup with a backup job.
2. To emulate a situation of data decryption on another Veeam backup server, remove the created backup from the Veeam Backup & Replication console and re-import the created backup back to the Veeam Backup & Replication console.
3. Decrypt the backup file without a password.

Prerequisites

- Make sure that the Veeam backup server is connected to Veeam Backup Enterprise Manager.
- Make sure that Enterprise or Enterprise Plus license is installed on the Veeam backup server. You can use a valid trial license or paid license.
Procedure

To create an encrypted backup and restore data from it without a password, perform the following steps.

Step 1. Create an encrypted backup

1. In Veeam Backup & Replication, open the **Home** view.
2. Open properties of a backup job that you have configured in the **Performing Backup** exercise.
3. Pass to the **Storage** step of the wizard and click **Advanced**.
4. In the **Advanced Settings** window, open the **Storage** tab.

5. In the **Encryption** section, select the **Enable backup file encryption** check box and click **Add** on the right.
6. In the **Password** field, specify a password that you want to use for the backup file encryption. To view the specified password, click and hold the eye icon on the right of the field.

7. In the **Hint** field, specify a hint for the password.

8. Make sure that the **Loss protection enabled** label is displayed under the **Password** field. In the opposite case, you will not be able to restore data from the encrypted backup without a password.

9. Save the new job settings and run the backup job once again to produce an encrypted backup file.

10. When you enable encryption for an already existing backup job, Veeam Backup & Replication restarts the backup chain — it produces a new full backup. To make sure that the encrypted backup has been created, open the target folder on the backup repository, find a subfolder with the backup job name and make sure that a new VBK file is added to the backup chain.
Step 2. Remove the backup from configuration and re-import it

1. In Veeam Backup & Replication, open the **Home** view.
2. In the inventory pane, select **Backups > Disk**.
3. In the working area, right-click the backup job and select **Remove from configuration**.
   
   Veeam Backup & Replication will remove records about the created backup and encryption keys from the Veeam Backup & Replication database. The actual backup files will remain on the backup repository.

4. On the **Home** tab of the ribbon, click **Import Backup**.
5. From the **Computer** list in the **Import Backup** window, select a backup repository where backup files are located.

6. In the **Backup file** field, specify a path to the VBM backup file on the backup repository.

7. Click **OK**. Veeam Backup & Replication will import the backup and place it under the **Backups > Encrypted** node.

8. Additionally, Veeam Backup & Replication will display a warning that the backup file you import is encrypted. Click **OK** in the message window to close it.
Step 3. Decrypt the backup file without a password

1. In the inventory pane, click the Disk (Encrypted) node under Backups.

2. In the working area, right-click the imported job and select Specify password.

3. In the Specify Password window, click the I have lost the password link. Veeam Backup & Replication will launch the Encryption Key Restore wizard.

4. In the Encryption Key Restore wizard, click Copy to clipboard to copy the displayed request for data decryption.
5. Log in to Veeam Backup Enterprise Manager as Administrator.
6. In the top right corner of the window, click **Configuration**.
7. On the left, click **Key Management**.
8. At the top of the view, click **Password Recovery**.
9. In the **Challenge Request** window, paste the copied text of the request.

10. Pass through the next steps of the wizard. At the **Response** step of the wizard, copy the displayed text to the clipboard.
11. Get back to the Veeam Backup & Replication console; in the **Encryption Key Restore** wizard, click **Next**.

12. At the **Response** step of the wizard, paste the copied response to the text field, click **Next** and click **Finish**. Veeam Backup & Replication will decrypt the backup file and move the imported backup to the **Backups > Disk (imported)** node.
Validation

1. Open the **Home** view.
2. Select the **Disk (imported)** node in the inventory pane.
3. Make sure that the imported backup is available in the working area.