Acronis

Acronis Backup Advanced 11.7 Update 1

APPLIES TO THE FOLLOWING PRODUCTS

Advanced for VMware / Hyper-V / RHEV / Citrix XenServer / Oracle VM

BACKING UP VIRTUAL MACHINES

Copyright Statement

Acronis patented technologies

Technologies, used in this product, are covered and protected by one or more U.S. Patent Numbers: 7,047,380; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121 and patent pending applications.

Table of contents

1 About this document

This document contains information that is specific for backup and recovery of virtual machines with Acronis Backup.

For the most comprehensive information about the functionality provided by Acronis Backup, please refer to

Acronis Backup Help

Web Help: http://www.acronis.com/en-us/support/documentation/AcronisBackup_11.7/

Built-in context-sensitive Help available in Acronis Backup Management Console by clicking the question-mark button .

For the purpose of convenience, this information is also presented in other sources. Use the ones that correspond to your preferences.

Installation information

Installation Help available in your setup program by clicking **View Installation Help**.

Installation Guide for Acronis Backup Advanced:
http://www.acronis.com/en-us/download/docs/aba11.7/installguide

Information about the core functionality provided by Acronis Backup

User Guide for Acronis Backup Advanced:
http://www.acronis.com/en-us/download/docs/aba11.7/userguide

Command-line interface

Command-Line Reference: http://www.acronis.com/en-us/download/docs/ab11.7/cmdlineref

2 Supported virtualization platforms

The following table summarizes how various virtualization platforms are supported by Acronis Backup.

Platform	Backup at a hypervisor level (p. 7)	Backup from inside a guest OS (p. 34)
VMware		
VMware vSphere versions: 5.0, 5.1, 5.5, and 6.0 **VMware vSphere editions:** VMware vSphere Essentials VMware vSphere Essentials Plus VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	+	+
VMware vSphere Hypervisor (Free ESXi)**		+
VMware Server (VMware Virtual server) VMware Workstation VMware ACE VMware Player		+
Microsoft		
Windows Server 2008 (x64) with Hyper-V Windows Server 2008 R2 with Hyper-V Microsoft Hyper-V Server 2008/2008 R2 Windows Server 2012/2012 R2 with Hyper-V Microsoft Hyper-V Server 2012/2012 R2 Windows 8, 8.1 (x64) with Hyper-V Windows 10 with Hyper-V Windows Server 2016 with Hyper-V Microsoft Hyper-V Server 2016	+	+
Microsoft Virtual PC 2004 and 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
Citrix		
Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, and 6.5		Only fully virtualized (aka HVM) guests

Platform	Backup at a hypervisor level (p. 7)	Backup from inside a guest OS (p. 34)
Red Hat and Linux		
Red Hat Enterprise Virtualization (RHEV) 2.2, 3.0, 3.1, 3.2, 3.3, 3.4, 3.5, and 3.6		+
Kernel-based Virtual Machines (KVM)		+
Parallels		
Parallels Workstation		+
Parallels Server 4 Bare Metal		+
Oracle		
Oracle VM Server 3.0 and 3.3		+
Oracle VM VirtualBox 4.x		+

* The Standard edition does not support Hot-add so backups may run slower.

** Backup at a hypervisor level is not supported for vSphere Hypervisor because this product restricts access to Remote Command Line Interface (RCLI) to read-only mode. The agent works during the vSphere Hypervisor evaluation period while no serial key is entered. Once you enter a serial key, the agent stops functioning.

3 Backup at a hypervisor level

Backup at a hypervisor level (also known as agent-less backup) means the ability to back up and recover virtual machines without installing agents into the guest systems. This functionality becomes available by using Acronis Backup Agent for VMware or Acronis Backup Agent for Hyper-V.

Agent for VMware can be imported or deployed to a VMware ESX(i) host as a virtual appliance.

Agent for VMware requires either of the following licenses to work:

- Acronis Backup Advanced for VMware
- Acronis Backup Advanced Universal License

Agent for Hyper-V needs to be installed directly on a Hyper-V host.

Agent for Hyper-V requires either of the following licenses to work:

- Acronis Backup Advanced for Hyper-V
- Acronis Backup Advanced Universal License

3.1 Features and capabilities

Backup at a hypervisor level includes the following main features and capabilities.

- **Disk-level backup**

  Backup of entire machines or individual disks or volumes.

  During backup, a virtual machine can be running, stopped, suspended, or switching between the three states.
- **Disk-level recovery**

  Recovery of entire machines, individual disks or volumes to a new or existing virtual machine.

  A virtual machine has to be stopped during the recovery to this machine. By default, the software stops the machine automatically.
- **File-level recovery** (p. 30)

  Recovery of individual files and folders to a network share, FTP or SFTP server.
- **Cluster support**

  Backup and recovery of clustered virtual machines.
- **Support for VMware vMotion (p. 19)/Microsoft Migration**

  A backup plan is executed no matter which host the machine is running on.
- **Simultaneous backups of virtual machines** (p. 32)

  An agent can simultaneously back up as many as 10 virtual machines. The exact number is defined by the user.
- **Incremental conversion to a virtual machine**

  An agent can convert a disk-level backup to a virtual machine of the corresponding type: VMware ESX(i) or Microsoft Hyper-V. Conversion of an incremental backup updates the machine instead of creating it from scratch.
- **Flexible configuration of the agents** (p. 14)

  Applies to VMware vSphere only

Protect your virtual environment with as many agents as you want, from one agent for each host to one agent for each machine. The management server evenly distributes virtual machines among the agents running within each host. Or, you can bind the agents (p. 17) with the machines manually.

- **Automatic agent deployment** (p. 16)

  Applies to VMware vSphere only

  Just include virtual machines in a backup plan. The agents will be deployed and configured in the background if you allowed this when configuring integration with the vCenter Server.

- **Backup to a locally attached storage** (p. 15)

  Applies to VMware vSphere only

  Add a dedicated virtual disk to Agent for VMware (Virtual Appliance) and do backups directly to this storage, omitting LAN.

- New **Changed Block Tracking (CBT)** (p. 18) developed by Acronis

  Perform faster incremental and differential backups of ESX(i) virtual machines without using VMware CBT.

- **Support for UEFI-based virtual machines**

  Back up and recover virtual machines that use Unified Extensible Firmware Interface (UEFI). Convert a UEFI-based physical machine to a virtual machine that uses the same boot firmware.

- **Support for VM templates** (p. 21)

  Back up and recover virtual machine templates in the same way as normal ESX(i) virtual machines.

3.2 Limitations

Sometimes, backup at a hypervisor level is not possible because of virtualization product or Acronis Backup limitations.

- Agent for VMware cannot back up fault tolerant virtual machines.
- Agent for VMware cannot back up Raw Device Mapping (RDM) disks in physical compatibility mode and independent disks.
- Microsoft Hyper-V does not provide control over pass-through disks to a host system. As a result, the Microsoft Software Shadow Copy provider cannot provide Agent for Hyper-V with snapshots of pass-through disks.

To overcome these limitations, use backup from inside a guest OS (p. 34). Using this method, you can also:

- Execute pre/post backup or pre/post data capture commands within the guest operating system.
- Back up individual files and folders of a virtual machine.
- Recover files to a virtual machine's file system.
- Back up a guest system stored on a logical volume to be able to recover the machine to a different platform.
- Use the backup and recovery options that are not effective for backup at a hypervisor level (p. 33).

For more details, please see the following sections:

- Backing up independent disks and RDMs (p. 20)
- Backing up pass-through disks (p. 26)

- Backing up fault tolerant machines (p. 20)
- Backing up Linux logical volumes and MD devices (p. 29)

3.3 What does a virtual machine backup store?

Backing up an entire virtual machine, its disks or volumes, results in a standard disk backup. A backup created at a hypervisor level also stores the virtual machine configuration. This configuration will be suggested by default when recovering the backup content to a new virtual machine.

You can recover disks and volumes from a virtual machine backup to a physical machine. Similarly, you can recover disks or volumes from a physical machine backup to a new or existing virtual machine. Hence, physical to virtual and virtual to physical machine migration becomes available.

With Agent for Windows or Agent for Linux, you can mount volumes from a virtual machine backup and recover individual files from it.

3.4 Working in VMware vSphere

3.4.1 Getting started with Agent for VMware

This section describes how to start backing up ESX(i) virtual machines.

3.4.1.1 Prerequisites

Ensure that:

- You have a vCenter Server that manages one or more ESX(i) hosts.
- VMware Tools is installed on every virtual machine you want to back up. See installation instructions later in this section.
- You have an appropriate number of Acronis Backup Advanced licenses (p. 7). Each ESX(i) host whose virtual machines you want to back up requires a separate license. For a vSphere cluster, you need as many licenses as there are hosts in the cluster.

  To use the product in the trial mode, you do not need licenses.
- You have a machine running Windows that will act as the management server. This machine must be always turned on and available across the network. For system requirements, see the installation documentation.
- You downloaded the setup program of Acronis Backup Advanced.

To install VMware Tools

1. In VMware Infrastructure/vSphere Client, log on to the vCenter Server.
2. Select the virtual machine and run the guest operating system.
3. Right-click the virtual machine and select **Guest** > **Install/Upgrade VMware Tools**.
4. Follow the onscreen instructions.

3.4.1.2 Installation

In this step, you will install the management server. This will enable backing up the virtual machines of the vCenter Server.

1. On the machine that will act as the management server, log on as an administrator and start the setup program.

2. Click **Install Acronis Backup**.
3. Accept the terms of the license agreement.
4. Select the **Centrally monitor and configure the backing up of physical and virtual machines** check box.
5. Type all your license keys or import them from a text file.
6. Click **Install**.

3.4.1.3 Integration with the vCenter Server

In this step, you will integrate the management server with your vCenter Server. Integration enables the management server to automatically deploy agents to ESX(i) hosts.

1. Start the management console, by clicking **Acronis Backup** on the desktop.
2. Click **Connect to a management server**. In **Machine**, type the name of the current machine.
3. In the **Navigation** pane, right-click **Virtual machines**, and then click **Configure VMware vCenter integration**.
4. Specify the name or IP address of the vCenter Server, and the user name and password of a vCenter Server administrator.

   Note: *If you want to specify a non-administrative user account, make sure that the account has the appropriate privileges (p. 21).*
5. Select the **Automatically deploy Agent for VMware (Virtual Appliance)** check box.
6. Click **OK**.

Result:

- The **All virtual machines** view shows all virtual machines of the vCenter Server.
- The virtual machines are shown as grayed out because Agent for VMware has not been deployed yet. The agent will be deployed automatically after you select the virtual machines for backing up.

3.4.1.4 Creating a centralized vault

In this step, you will create a centralized vault available across the network. This will enable easy access to the backups.

1. In your network, choose a machine where you want to store the backed-up data. It can be the machine where you installed the management server.
2. On the machine where you installed the management server, click **Acronis Backup** on the desktop.
3. Click **Connect to a management server**. In **Machine**, type the name of the current machine.
4. On the **Actions** menu, click **Create centralized vault**.
5. In **Name**, type the name of the vault.
6. In **Type**, select **Unmanaged**.
7. Click **Path** and then specify the path to the network share where the backups will be stored. Click **OK**. When prompted, provide access credentials for the shared folder.
8. Click **OK**. You can see the vault name in the **Navigation** tree under **Vaults > Centralized**. Click the vault name to check its free space and contents.

3.4.1.5 Backup and recovery

Backup

In this step, you will back up one or more virtual machines to the centralized vault you created.

1. In the welcome screen, click **Back up now**.
2. Click **Items to back up**. In **Data to back up**, select **Virtual machines**.
3. Select the virtual machines that you want to back up.
4. Click **Location**, expand **Vaults**, and then specify the vault you have created.
5. Click **OK** to start backing up the virtual machines.

Result:

- Agent for VMware (Virtual Appliance) is deployed on each host or cluster whose machines you selected to back up.
- The machines are backed up to the centralized vault you specified.

Recovery

In this step, you will recover the disks of a backed-up virtual machine to an existing virtual machine on the vCenter Server.

1. In the **Navigation** tree, expand **Vaults** > **Centralized** and then select the vault where you saved the archives. If prompted, provide access credentials for the vault.
2. In the **Data view** tab, in **Show**, select **Disks**.
3. Select the virtual machine that you want to recover. Under **Versions**, select a recovery point. By default, the latest recovery point is selected.

   Details. Instead of recovering the entire virtual machine, you can recover individual disks of it.
4. Click **Recover**.
5. Under **Where to recover**, in **Recover to**, select **Existing virtual machine**.
6. Click **Select**, and then select an existing virtual machine, either the same one you have backed up (recommended for getting started), or a different one.

   Details. The agent will automatically stop this virtual machine before starting the recovery to it. The machine must be powered off during the recovery for the recovery task to succeed.
7. If required, do the following for every disk found in the backup:
   a. Click **Recover 'Disk N' to:** and choose the destination disk from the disks of the existing machine.
   b. In **NT signature**, leave the default setting: **Select automatically**.
8. Click **OK** to immediately start the recovery.

3.4.2 Installation of Agent for VMware

Agent for VMware enables backup and recovery of ESX(i) virtual machines without installing agents into the guest systems. The agent is delivered as a virtual appliance.

Preparation

We highly recommend that you install Acronis Backup Management Server prior to the Agent for VMware installation.

Installation

There are three methods of installing **Agent for VMware**:

- Importing to a ESX(i) host as an OVF template.

  Use this method for troubleshooting purposes or if you cannot install Acronis Backup Management Server for some reason.
- Deployment (p. 13) from Acronis Backup Management Server to a specified host or cluster.

  Connect the console to the management server. In the **Navigation** tree, right click **Virtual machines**, then click **Deploy Agent for VMware**. Refer to the context help for further instructions.
- Automatic deployment from Acronis Backup Management Server.

  This is the easiest method. It is recommended in most cases. Connect the console to the management server. In the **Navigation** tree, right click **Virtual machines**, and then click **Configure VMware vCenter integration**. Specify the vCenter Server, and then enable **Automatic deployment**. Any time a virtual machine is selected for backup but the agent is not installed on its host, the Virtual Appliance will be automatically deployed on the host when the backup starts.

Providing licenses

Agent for VMware requires either of the following licenses to work:

- Acronis Backup Advanced for VMware
- Acronis Backup Advanced Universal License

The installation of the agent does not require a license. However, you must specify a license server when installing the management server, or when connecting the console to the agent (if the agent was imported manually). Once the agent starts backing up a virtual machine, the agent checks whether the virtual machine's host has a license. If it does not have one, the agent takes a free license from the specified license server and assigns it to the host. If the host is included in a cluster, licenses will be assigned to all of the clustered hosts. Therefore, you need one license for each clustered ESX(i). This ensures the uninterrupted operation of your backup plans when virtual machines are moved around the cluster.

3.4.3 Operations with agents

This section explains how to deploy, update or remove Agent for VMware (Virtual Appliance) using Acronis Backup Management Server.

3.4.3.1 Prerequisites

To perform operations described in this section, Acronis Backup Management Server uses a number of TCP ports:

- Ports **443** and **902** are used to access the vCenter Server and ESX(i) hosts.
- Port **9876** is used to access Agent for VMware (Virtual Appliance).

If the management server uses a custom firewall, ensure that this firewall allows outgoing connections to these ports. Windows Firewall is configured automatically by Acronis Backup.

If the traffic from the management server to the vCenter Server, the ESX(i) hosts, or the agents goes through a router or a similar network device, ensure that the device does not block this traffic.

No special configuration is required on the vCenter Server or the ESX(i) hosts.

3.4.3.2 Deploying Agent for VMware (Virtual Appliance)

If your host contains a big number of virtual machines, you may want to deploy one or more agents in addition to the automatically deployed one. The instructions below will also help you deploy the agent to a stand-alone ESX(i) host that is not managed by vCenter Server.

To deploy an additional virtual appliance

1. Connect the management console to the management server.
2. In the **Navigation** tree, right click the group that has the same name as the vCenter Server. When deploying an agent to a stand-alone host, right click **Virtual machines**.
3. Click **Deploy Agent for VMware**.
4. Select the hosts or clusters to which you want to deploy the agent, or check the **Select all** check box. When deploying an agent to a stand-alone host, enter the host name or IP address and administrator credentials.
5. [Optional] If necessary, modify the **VA name**, **Datastore** and **Network interface** settings suggested for each agent by default.

   [Optional] You may also want to modify the credentials that the agent will use to access the vCenter Server or ESX(i). Keep in mind that centralized backup and recovery tasks will run under this account by default. This means that the account must have the necessary privileges (p. 21) on the vCenter Server. Otherwise, you will need to specify credentials for the account with the necessary privileges in every centralized backup plan or recovery task.

   [Optional] You may want to manually set the agent network settings, including the IP address. To do so, click **Network configuration**. By default, the agent obtains the network settings from the DHCP server, provided that this server is present in your network.

   Tip: *You will be able to change the network settings after the agent is deployed. To do so, select the virtual appliance in VMware vSphere inventory and go to the virtual appliance console. Under* ***Agent options****, click the* ***Change*** *link next to the name of the network interface, such as eth0.*
6. Click **Deploy Agent for VMware**.

Result: Once a new agent is deployed, the management server redistributes the virtual machines among the agents.

3.4.3.3 Updating Agent for VMware (Virtual Appliance)

You can update Agent for VMware (Virtual Appliance) using the management server GUI.

To update Agent for VMware

1. In the **Virtual machines** view, on the toolbar, click **Update Agent for VMware**.
2. Select the agents to update.
3. Click **Update Agent for VMware**.

When upgrading from Acronis Backup & Recovery 10 to Acronis Backup, you need to additionally specify the agent's host.

3.4.3.4 Removing Agent for VMware (Virtual Appliance)

You can remove Agent for VMware (Virtual Appliance) using the management server GUI.

If other agents are connected to the same ESX(i) host, they will undertake the backups of the machines assigned to the removed agent. If there are no such agents, the machines will become unprotected.

To remove Agent for VMware

1. In the **Virtual machines** view, on the toolbar, click **Remove Agent for VMware**.
2. Select the agents to remove.
3. Click **Remove Agent for VMware**.

3.4.4 Flexible configuration of the agents

This section gives you an overview of how the management server organizes the operation of multiple agents running within a VMware vCenter host.

All agents must be registered on the management server. All agents must be connected to vCenter Server.

Distribution algorithm

The management server evenly distributes the virtual machines between the agents. By evenly, we mean that each agent manages an equal number of machines. The amount of storage space occupied by a virtual machine is not counted.

Once a virtual machine is assigned to an agent, all centralized backups of this machine will be delegated to this agent.

Redistribution

Redistribution takes place each time the established balance breaks, or, more precisely, when a load imbalance among the agents reaches 20 percent. This may happen when a machine or an agent is added or removed, or a machine migrates to a different host, or if you manually bind a machine to an agent. If this happens, the management server redistributes the machines using the same algorithm.

For example, you realize that you need more agents to help with throughput and deploy an additional virtual appliance to the host. The management server will assign the most appropriate machines to the new agent and update the centralized backup plans on the involved agents. The old agents' load will reduce.

When you remove an agent from the management server, the machines assigned to the agent are distributed among the remaining agents. However, this will not happen if an agent gets corrupted or is deleted bypassing the management server. Redistribution will start only after you remove such agent from the management server.

Viewing the distribution result

You can view the result of the automatic distribution in the **Agent** column available for each virtual machine on the management server. Also, it is displayed in the management server options. To access this window, select **Options** > **Management server options** from the top menu, and then select **Agent for VMware binding**.

Manual binding

The **Agent for VMware binding** (p. 17) option lets you exclude a virtual machine from this distribution process by specifying the agent that must always back up this machine. The management server will continue maintaining the overall balance, but it is allowed to pass the machine to a different agent only if the original agent is removed.

Tips on setup

Below are brief instructions on how to set up some of the available configurations. For detailed information about integration with vCenter see the "VMware vCenter integration" (p. 16) section.

- **1 agent per host** - default (achieved by automatic deployment). Enable vCenter integration (do not disable automatic deployment of virtual appliances). Alternatively, you can deploy or install the agents manually and connect them to vCenter Server.
- **more than 1 agent per host** - Enable vCenter integration (automatic deployment of virtual appliances may be enabled or disabled). Deploy the required number of agents to the hosts (at least one agent per host). Connect the agents to vCenter Server.

Make sure that all agents are registered on the management server. If you deploy virtual appliances from an OVF template, you need to add them to the management server manually.

In any case you can bind one or more virtual machines to the agents manually.

Do not create local backup plans on agents if you want to make the best of the automatic distribution.

3.4.5 Using a locally attached storage

You can attach an additional disk to Agent for VMware (Virtual Appliance) so the agent can back up to this locally attached storage. Such backup is normally faster than backup via LAN and it does not consume the network bandwidth. We recommend using this method if you have only one ESX(i) host in your environment.

Data backed up to a locally attached storage does not appear in the centralized catalog. To access a backup stored in a locally attached storage, connect the console directly to the agent.

Using a locally attached storage presumes that the agent always backs up the same machines. If multiple agents work within the host, and one or more of them use locally attached storages, you need to manually bind (p. 17) each agent to all machines it has to back up. Otherwise, if the machines are redistributed among the agents by the management server, a machine's backups may be dispersed over multiple storages.

You can add the storage to an already working agent or when importing the agent from an OVF template.

To attach a storage to an already working agent

1. In VMware vSphere inventory, right click the Agent for VMware (Virtual Appliance).
2. Add the disk by editing the settings of the virtual machine. The disk size must be at least 10 GB.

   Be careful when adding an already existing disk. Once the storage is created, all data previously contained on this disk will be lost.
3. Go to the virtual appliance console. The **Create storage** link is available at the bottom of the screen. If it is not, click **Refresh**.
4. Click the **Create storage** link, select the disk and specify a label for it.

   Details. The label length is limited to 16 characters due to file system restrictions.

To select a locally attached storage as a backup destination

When creating a backup plan, in **Where to back up** > **Location** do one of the following, depending on where the console is connected:

- When connected to the management server – Select **Store each machine's archive in the specified folder on the machine with agent**. Then type the letter corresponding to the locally attached storage, for example, D:\.
- When connected directly to the agent – Type the letter corresponding to the locally attached storage, for example, D:\.

To recover a machine from a locally attached storage

Connect the console directly to the agent where the storage is attached. Click **Recover**. In **What to recover** > **Select data**, select the locally attached storage. Complete the recovery settings as described in the "Creating a recovery task" section.

3.4.6 Configuring ESX(i)-related options

This section describes the ESX(i)-related options that you can configure on the management server and on a managed machine.

3.4.6.1 VMware vCenter integration

This option enables communication between Acronis Backup Management Server and VMware vCenter Server. To access this option, connect the console to the management server and then select **Options** > **Management server options** from the top menu.

Integration provides the capability to:

- View virtual machines managed by the VMware vCenter in the management server GUI.

  The **VMs and Templates** inventory view appears under **Navigation** > **Virtual machines**.
- View the backup status of these machines in the vCenter Server.

  This information appears in the virtual machine summary (**Summary** > **Annotations**) or on the **Virtual Machines** tab for every host, datacenter, folder or entire vCenter Server.
- Automatically register virtual machines created by Acronis Backup in the vCenter Server inventory.
- Automatically deploy agents to the ESX(i) hosts managed by the vCenter Server.

  After you create a backup plan, an agent is deployed to each host whose virtual machines are included in the backup plan.

To enable integration of the management server with a vCenter Server

1. Click **VMware vCenter integration**.
2. Select the **Enable integration with the following vCenter Server** check box.
3. Specify the vCenter Server's IP address or name and provide access credentials for the server.

   This account will be used for deploying agents from the management server. This means the account must have the necessary privileges (p. 21) for deploying virtual appliances on the vCenter Server. We also recommend that the account have the necessary privileges for backup and recovery, because the agents will use this account to connect to the vCenter Server by default.
4. [Optionally] Select the **Automatically deploy Agent for VMware (Virtual Appliance)** check box.
5. Click **OK**.

To enable automatic deployment of Agent for VMware (Virtual Appliance)

1. Enable integration with the vCenter Server as described above.
2. Click **Automatic deployment**.

3. Select the **Automatically deploy Agent for VMware (Virtual Appliance)** check box.
4. Specify the credentials that the automatically deployed agents will use to connect to the vCenter Server.

   Centralized backup and recovery tasks will run under this account by default. This means the account should have the necessary privileges (p. 21) on the vCenter Server. Otherwise, you will need to specify credentials for the account with the necessary privileges in every centralized backup plan or recovery task.
5. Click **OK**.

To disable integration of the management server with a vCenter Server

1. Click **VMware vCenter integration**.
2. Clear the **Enable integration with the following vCenter Server** check box.
3. Click **OK**.

   Result. Automatic deployment of the agent is also disabled. The virtual machines managed by the already existing agents remain on the management server. The backup plans that back up these machines continue functioning.

To disable automatic deployment of Agent for VMware (Virtual Appliance)

1. Click **Automatic deployment**.
2. Clear the **Automatically deploy Agent for VMware (Virtual Appliance)** check box.
3. Click **OK**.

   Result. Automatic deployment of the agent is disabled. Integration with the vCenter Server is preserved.

3.4.6.2 Agent for VMware binding

This option is effective if more than one Agent for VMware are running within a VMware vCenter host.

To access this option, connect the console to the management server and then select **Options** > **Management server options** from the top menu.

The management server evenly distributes the machines between the agents. This balance may break when a machine or an agent is added or removed. If this happens, the management server redistributes the machines and updates the centralized backup plans accordingly. You can view the result of this distribution in the **Agent** column available for each virtual machine on the management server. For more information about automatic distribution see "Flexible configuration of the agents" (p. 14).

The **Agent for VMware binding** option lets you exclude a virtual machine from this distribution process by specifying the agent that must always back up this machine. The management server will continue maintaining the overall balance, but it is allowed to pass the machine to a different agent only if the original agent is removed.

To configure the **Agent for VMware binding** option, associate (bind) a virtual machine with one of the agents.

To bind a machine with an agent:

1. Select the agent. The software shows the virtual machines currently managed by the agent. Machines available for automatic distribution are grayed out.
2. Click **Bind with virtual machine**. This opens a window that shows the full list of machines the agent can access.

3. Select one or more machines, and click **OK**.

   Result. The list of the virtual machines currently managed by the agent is updated. Machines bound to the agent are displayed in black color. They are no longer available for automatic distribution.

To unbind a machine from an agent:

1. Select the agent. The software shows the virtual machines currently managed by the agent. Machines available for automatic distribution are grayed out. Machines bound to the agent are displayed in black color.
2. Click **Unbind virtual machine**. This opens a window that shows the list of machines bound with the agent.
3. Select one or more machines, and click **OK**.

   Result. The list of the virtual machines currently managed by the agent is updated. The unbound machines become grayed out. If a machine disappears from the list, it means that the machine was assigned to a different agent as a result of automatic distribution.

Usage examples

- It is necessary to use this option if one or more of the agents have locally attached storages (p. 15).
- Let's assume you want to back up 20 virtual machines using three Agents for VMware. Five machines out of 20 need to be backed up to Acronis Cloud Storage.

  Allocate one of the agents for cloud backups. Then, bind each of the five machines with this agent. The remaining 15 machines will be distributed among the three agents.

  As a result, the cloud backups of a virtual machine will be sent to a single archive. Without the binding, each agent will create its own archive in the cloud storage, starting from a full backup. So, backups of one machine will be distributed among up to three archives.

3.4.6.3 Changed Block Tracking (CBT)

This option applies only to Agent for VMware.

This option determines whether to use Changed Block Tracking (CBT) when performing an incremental or differential backup of an ESX(i) virtual machine.

To access this option, connect the console to the management server or to Agent for VMware. Then, select **Options > Default backup options** or **Options > Default backup and recovery options > Default backup options**, respectively. The default setting will be used unless you override it with a different setting in the backup plan.

How it works

The Changed Block Tracking mechanism tracks changes to the contents of virtual disks.

Changed Block Tracking was originally introduced in VMware ESX(i) 4.0. Starting with Acronis Backup 11.5 Update 5, there is an Acronis proprietary implementation of the CBT mechanism, which is unrelated to the VMware implementation. Acronis CBT does not use or change the virtual machine configuration settings related to VMware CBT (**ctkEnabled**, **scsi#:#.ctkEnabled**, and **ctkDisallowed**).

Without using CBT, Agent for VMware reads the virtual machine's file system to determine which blocks have changed. When using CBT, the agent obtains the list of changed blocks from the ESX(i) host. The agent only needs access to the file system to determine which of these blocks must be included in the backup. This leads to faster backups and reduces the load on the storage during a backup.

CBT is most effective for large amounts of data that changes little between backups. In particular, databases often consist of large files with relatively small daily changes.

Available settings

The preset is: **Use CBT**

- **Use CBT**

  Acronis Backup uses CBT for each virtual machine that is included in the backup plan.
- **Do not use CBT**

  Acronis Backup does not use CBT.

3.4.7 Support for VM migration

This section informs you about what to expect when migrating virtual machines within a datacenter, by using the vCenter Server migration options.

vMotion

vMotion moves a virtual machine's state and configuration to another host while the machine's disks remain in the same location on shared storage.

- vMotion of Agent for VMware (Virtual Appliance) is not supported and is disabled.
- vMotion of a virtual machine is disabled during a backup. Backups will continue to run after the migration, but will be managed by the agent on the target host. If there is no Agent for VMware on the target host, a new agent will be deployed.

Storage vMotion

Storage vMotion moves virtual machine disks from one datastore to another.

- Storage vMotion of Agent for VMware (Virtual Appliance) is not supported and is disabled.
- Storage vMotion of a virtual machine is disabled during a backup. Backups will continue to run after the migration.

3.4.8 Support for datastore clusters and Storage DRS

Datastore clusters and Storage Distributed Resource Scheduler (Storage DRS, SDRS) are new features in VMware vSphere 5.

A datastore cluster is a collection of datastores. The Storage DRS feature provides load balancing for a datastore cluster in terms of storage space and I/O traffic. Storage DRS uses storage vMotion to distribute the virtual disks among the datastores included in the datastore cluster.

Storage vMotion of a virtual machine is disabled during a backup. If a backup starts while storage vMotion is in progress, storage vMotion fails. To avoid this, you can set up the **SDRS Scheduling** option for the datastore cluster so that the automation level changes to **Manual** for the duration of your backup window. For more information about compatibility with Storage VMotion, see the "Support for VM migration" (p. 19) section.

When setting up a destination for a recovery to a new virtual machine or for a regular conversion to a virtual machine, you can select either a datastore cluster or one of its datastores, depending on whether SDRS is enabled:

- Datastore clusters with enabled Storage DRS are shown with this icon:  .

- Datastore clusters with disabled Storage DRS are not shown. Instead, their individual datastores are shown in the form *DatastoreClusterName*/*DatastoreName*.

3.4.9 Backing up fault tolerant machines

Agent for VMware does not back up virtual machines with the VMware Fault Tolerance feature enabled, and you cannot select them for backup under **Virtual machines**. If you include a group containing a fault tolerant machine in a backup plan, this machine will be automatically excluded.

To back up a fault tolerant virtual machine, do one of the following:

- **Turn off VMware Fault Tolerance, then turn it on after performing the backup.**

  Note that you should "turn off" rather than "disable" it. You can turn Fault Tolerance off and on when required using vSphere scripts. Normally this works, but unnecessary actions (such as removing or creating the secondary virtual machine) take time and resources. Also, the machine reliability is reduced during the backup.
- **Install Agent for Windows or Agent for Linux in the guest operating system.**

  An Acronis Backup Advanced license (p. 7) assigned to the host enables you to install agents in an unlimited number of guest systems.

  For more information about how to install the agent, see the installation documentation.

  After you install the agent and add the machine to the management server, the machine appears under **Machines with agents** in the **All machines with agents** group. When creating a backup plan, select the machine here rather than under **Virtual machines**. Or, you can connect the console to the machine directly as to a physical machine.

3.4.10 Backing up independent disks and RDMs

Agent for VMware cannot back up Raw Device Mapping (RDM) disks in physical compatibility mode or independent disks. The agent skips these disks and adds warnings to the log. You can avoid the warnings by excluding independent disks and RDMs in physical compatibility mode from the backup plan.

If you want to back up these disks, install Agent for Windows or Agent for Linux in the guest operating system.

An Acronis Backup Advanced license (p. 7) assigned to the host enables you to install agents in an unlimited number of guest systems.

For more information about how to install the agent, see the installation documentation.

After you install the agent and add the machine to the management server, the machine appears under **Machines with agents** in the **All machines with agents** group. When creating a backup plan, select the machine here rather than under **Virtual machines**. Or, you can connect the console to the machine directly as to a physical machine.

You might want to use a different backup strategy for independent disks or RDMs in physical compatibility mode. For example, if these disks contain frequently changing databases, you can back them up more often than the operating system, or use different settings for them. In this case, create a separate backup plan for these disks.

3.4.11 Backing up virtual machine templates

A virtual machine template (or simply a template) is a set of files and parameters that represents a complete virtual machine. Templates are typically used to create multiple similar virtual machines.

Virtual machine templates appear in the **All virtual machines** group on the management server along with other virtual machines.

In terms of backup and recovery, a virtual machine template acts as a normal virtual machine. You can back up its disks, recover its disks and files, add it to static or dynamic groups, and perform other operations described in this document.

Virtual machine templates are unrelated to OVF templates that are used to deploy Agent for VMware (Virtual Appliance).

3.4.12 Privileges for VM backup and recovery

Once Agent for VMware is deployed to a vCenter's host, any user of the vCenter Server can connect a management console to the agent. The scope of available operations depends on the privileges a user has on the vCenter Server. Only those actions are available that the user has permission to perform. The below tables contain the privileges required for backup and recovery of ESX virtual machines and, additionally, for virtual appliance deployment.

If the agent was deployed directly to an ESX(i) host or manually imported to the host, and you want the vCenter users to be able to connect to the agent and the below privileges to take effect, connect the agent to the vCenter Server rather than to the ESX(i) host. To change the connection, access the virtual appliance GUI using the vSphere Client and specify access credentials for the vCenter Server in the **ESX(i)/vCenter** setting.

Privileges on vCenter Server or ESX(i) host

Outlined in the below table are the privileges a vCenter Server user must have to perform operations on all the vCenter hosts and clusters.

To enable a user to operate on a specific ESX host only, assign the user the same privileges on the host.

		Operation				
Object	**Privilege**	**Back up a VM**	**Back up a VM's disk**	**Recover to a new VM**	**Recover to an existing VM**	**VA deployment**
Datastore	**Allocate space**	+	+	+	+	+
	Browse datastore					+
	Configure datastore					+
	Low level file operations					+
Global	**Licenses**	+	+	+	+	
	Disable methods	+	+			
	Enable methods	+	+			

		Operation				
Object	**Privilege**	**Back up a VM**	**Back up a VM's disk**	**Recover to a new VM**	**Recover to an existing VM**	**VA deployment**
Host > Configuration	**VM autostart configuration**					+
	System management	+	+			
Host > Inventory	**Modify cluster**					+
Host > Local operations	**Create VM**					+
	Delete VM					+
	Reconfigure VM	+	+			+
Network	**Assign network**			+	+	+
Resource	**Assign VM to resource pool**			+	+	+
vApp	**Import**					+
Virtual machine > Configuration	**Add existing disk**	+	+	+		
	Add new disk	+	+	+	+	+
	Add or remove device			+		+
	Advanced	+	+	+		+
	Change CPU count			+		
	Disk lease					
	Memory			+		
	Remove disk	+	+	+	+	
	Rename			+		
	Settings				+	
Virtual machine > Interaction	**Configure CD media**			+		
	Console interaction					+
	Guest operating system management by VIX API					+

		Operation				
Object	**Privilege**	**Back up a VM**	**Back up a VM's disk**	**Recover to a new VM**	**Recover to an existing VM**	**VA deployment**
	Power off				+	+
	Power on			+	+	+
Virtual machine > Inventory	**Create from existing**				+	
	Create new			+	+	+
	Move					+
	Remove			+	+	+
Virtual machine > Provisioning	**Allow disk access**	+	+	+	+	
	Allow virtual machine download	+	+	+		
Virtual machine > State	**Create snapshot**		+		+	+ (VA update)
	Remove snapshot		+		+	+ (VA update)

3.5 Working in Microsoft Hyper-V

3.5.1 Getting started with Agent for Hyper-V

This section describes how to start backing up Hyper-V virtual machines.

3.5.1.1 Prerequisites

Ensure that:

- You have a machine running Windows with the Hyper-V role enabled.
- Hyper-V Integration Services are installed on every virtual machine you want to back up. See installation instructions later in this section.
- You have an appropriate number of Acronis Backup Advanced licenses (p. 7). You need one license per Hyper-V host. If you have a Hyper-V cluster (also called a failover cluster), obtain licenses for each node of the cluster.

  To use the product in the trial mode, you do not need licenses.
- You have a machine running Windows that will act as the management server. This machine must be always turned on and available across the network. For the system requirements, see the installation documentation.
- You downloaded the setup program of Acronis Backup Advanced.

To install the Hyper-V Integration Services

1. Run the guest operating system.
2. Select **Action** > **Insert Integration Services Setup Disk.**
3. The server connects the ISO image of the setup disk to the machine. Follow the onscreen instructions.

3.5.1.2 Installation

Installing the management server

In this step, you will install the management server. This will enable backing up the virtual machines of the Hyper-V host or cluster.

1. On the machine that will act as the management server, log on as an administrator and start the setup program.
2. Click **Install Acronis Backup**. Accept the terms of the license agreement.
3. Select the **Centrally monitor and configure the backing up of physical and virtual machines** check box.
4. Type all your license keys or import them from a text file.
5. Click **Install**.

Installing the agent for Hyper-V

In this step, you will install Acronis Backup Agent for Hyper-V on a Hyper-V host.

Perform the following procedure on the Hyper-V host. If you have a Hyper-V cluster, perform this procedure on each node of the cluster.

1. Log on to the Hyper-V host as an administrator and start the setup program.
2. Click **Install Acronis Backup**. Accept the terms of the license agreement.
3. Select the **Back up this machine's data** check box, and then ensure that the **Hyper-V Virtual Machines** check box is selected on the next page.
4. Select **I purchased a license or a subscription**.
5. Select the **Use the following license server** check box, and then enter the name or IP address of the machine where you installed the management server.

   Details. The license server is integrated with the management server.
6. Ensure that the proper license is selected, and then click **Next**.
7. If prompted for the Acronis Managed Machine Service (agent) account, specify an account of a domain user who has administrative privileges on all nodes of your Hyper-V cluster.
8. Click **Register now**. Specify the name or IP address of the machine where you installed the management server. Provide the user name and password of an administrator on that machine.
9. Specify whether the Hyper-V host will participate in the Acronis Customer Experience Program (CEP).
10. Click **Install**.

3.5.1.3 Creating a centralized vault

In this step, you will create a centralized vault available across the network. This will enable easy access to the backups.

1. In your network, choose a machine where you want to store the backed-up data. It can be the machine where you installed the management server.

2. On the machine where you installed the management server, click **Acronis Backup** on the desktop.
3. Click **Connect to a management server**. In **Machine**, type the name of the current machine.
4. On the **Actions** menu, click **Create centralized vault**.
5. In **Name**, type the name of the vault.
6. In **Type**, select **Unmanaged**.
7. Click **Path** and then specify the path to the network share where the backups will be stored. Click **OK**. When prompted, provide access credentials for the shared folder.
8. Click **OK**. You can see the vault name in the **Navigation** tree under **Vaults > Centralized**. Click the vault name to check its free space and contents.

3.5.1.4 Backup and recovery

Backup

In this step, you will back up one or more virtual machines to the centralized vault you created.

1. In the welcome screen, click **Back up now**.
2. Click **Items to back up**. In **Data to back up**, select **Virtual machines**.
3. Select the virtual machines that you want to back up.
4. Click **Location**, expand **Vaults**, and then specify the vault you have created.
5. Click **OK** to start backing up the virtual machines.

Recovery

In this step, you will recover the disks of a backed-up virtual machine to an existing virtual machine on the Hyper-V host.

1. In the **Navigation** tree, expand **Vaults** > **Centralized** and then select the vault where you saved the archives. If prompted, provide access credentials for the vault.
2. In the **Data view** tab, in **Show**, select **Disks**.
3. Select the virtual machine that you want to recover. Under Versions, select a recovery point. By default, the latest recovery point is selected.

   Details. Instead of recovering the entire virtual machine, you can recover individual disks of it.
4. Click **Recover**.
5. Under **Where to recover**, in **Recover to**, select **Existing virtual machine**.
6. Click **Browse**, and then select the Hyper-V host to which you want to recover the virtual machine.
7. Click **Select**, and then select an existing virtual machine, either the same one you have backed up (recommended for getting started), or a different one.

   Details. By default, the agent will automatically stop this virtual machine before starting the recovery to it. The machine must be powered off during the recovery for the recovery task to succeed.
8. If required, do the following for every disk found in the backup:
   a. Click **Recover 'Disk N' to:** and choose the destination disk from the disks of the existing machine.
   b. In **NT signature**, leave the default setting: **Select automatically**.
9. Click **OK** to immediately start the recovery.

3.5.2 Backing up clustered Hyper-V machines

In a Hyper-V cluster, virtual machines may migrate between cluster nodes. Follow these recommendations to set up a correct backup of clustered Hyper-V machines:

1. A machine must be available for backup no matter what node it migrates to. To ensure that a backup plan can access a machine on any node, run the plan under a domain user account that has administrative privileges on each of the cluster nodes.

   We recommend that you specify such an account for the agent service during the Agent for Hyper-V installation. Otherwise, you will need to specify credentials for such account in every centralized backup plan or recovery task.
2. Install Agent for Hyper-V on each node of the cluster.
3. Register all of the agents on the management server, either during installation or later.
4. Back up clustered machines by using the management server, rather than by connecting directly to a cluster node.
5. When creating a centralized backup plan, select a clustered machine under the cluster, rather than under a cluster node. This way, the backup plan will still apply to the machine after it moves to a different node.

High Availability of a recovered machine

When recovering backed-up disks to a *new* Hyper-V virtual machine, you can choose whether to make the machine highly available. In the **VM/VS Selection** window, after clicking **Create a new virtual machine on the server**, you need to specify the target Hyper-V host. If you select the target host under the cluster, the resulting virtual machine will be highly available. If you select the same host outside the cluster, the machine will not be highly available.

When you recover backed-up disks to an *existing* Hyper-V virtual machine, the machine's High Availability property remains as is.

When you do a *conversion* to a Hyper-V virtual machine within a backup plan, the resulting machine is not highly available. It is considered as a spare machine and is normally powered off. If you need to use the machine in the production environment, you can configure it for High Availability from the **Failover Cluster Management** snap-in.

3.5.3 Backing up pass-through disks

Microsoft Hyper-V does not provide control over pass-through disks to the host operating system. As a result, the Microsoft Software Shadow Copy provider cannot provide Agent for Hyper-V with snapshots of pass-through disks. During backup, the agent skips these disks and adds warnings to the log. You can avoid the warnings by excluding pass-through disks from the backup plan.

If you want to back up pass-through disks, install Agent for Windows or Agent for Linux in the guest operating system. An Acronis Backup Advanced license (p. 7) assigned to the host enables you to install agents in an unlimited number of guest systems. For more information about how to install the agent, see the installation documentation.

After you install Agent for Windows or Agent for Linux and add the machine to the management server, the machine appears under **Machines with agents** in the **All machines with agents** group. When creating a backup plan, select the machine here rather than under **Virtual machines**. Or, you can connect the console to the machine directly as is done with a physical machine.

You might want to use a different backup strategy for pass-through disks. For example, if these disks contain frequently changing databases, you can back them up more often than the operating system, or use different settings for them. In this case, create a separate backup plan for these disks.

3.5.4 Backing up and recovering a Hyper-V host

For disaster recovery purposes, you can perform a disk-level backup of the entire Hyper-V host. This will back up the operating system and all virtual machines that are stored on the host's local disks.

To back up the host, you need to **install Agent for Windows** on it. In Microsoft Hyper-V Server 2008/2008 R2, we recommend installing Agent for Windows remotely. If Agent for Hyper-V is already installed on the host, no additional license will be taken by Agent for Windows.

Alternatively, you can back up the host by using a bootable media.

Usage examples

Example 1. Backing up a stand-alone host

Consider the following scenario:

- You want to back up a host whose virtual machines are stored locally, such as on local disks or on logical unit number (LUN) devices.
- You do not need to recover individual virtual machines from the backup.

In this scenario, install Agent for Windows, and then create and run a backup plan to back up the entire host.

Backup

When setting up a backup for a host, make sure that:

- You selected to use the **Volume Shadow Copy Service (VSS)** backup option. In **Snapshot provider**, select **Software - System provider**. This ensures that the virtual machines are backed up in a consistent state.
- You installed Hyper-V Integration Services (p. 23) in the guest operating systems. This ensures that VSS does not put running virtual machines into a saved state (does not pause them) when taking the snapshot.

Recovery

Use the bootable media to recover the host to the same or dissimilar hardware.

After recovering the host to **the same hardware in the same configuration,** you can resume working with the virtual machines right away.

After recovering the host to a machine with a **different set or placement of network adapters,** you need to reassign the virtual network adapters of the virtual machines to the physical adapters of the host.

The most recent operating systems remain bootable when recovered to dissimilar hardware, or the VMware or Hyper-V platforms. If a recovered operating system does not boot, use the Acronis Universal Restore tool to update the drivers and modules that are critical for the operating system startup. For details, see the Acronis Universal Restore page at http://www.acronis.com/en-us/aur/.

Example 2. Backing up a cluster node before installing software updates

Consider the following scenario:

- You have a Hyper-V cluster with two or more nodes that use Cluster Shared Volumes (CSV) for storing virtual machines.
- You want to regularly back up virtual machines of the cluster.
- You want to back up cluster nodes before installing software updates on them.

In this scenario, install both Agent for Hyper-V and Agent for Windows on each node of the cluster. Register the nodes on the management server.

Set up disk-level backups for both nodes, by creating a centralized backup plan. You can exclude virtual machines from the backup, by excluding the CSV where the machines are stored from the CSV owner backup. Volumes that correspond to CSV do not have letters, so you can easily recognize them.

Before installing the software updates, back up the nodes. Install the software updates on one node at a time. If installing the updates has caused problems with the operating system, turn off the node. The remaining nodes will take over the virtual machines that ran on the node. Use the bootable media to recover the node. Once the node is operational again, the virtual machines will migrate back to it.

To back up the virtual machines themselves, create a separate backup plan. For details, see "Backing up clustered Hyper-V machines" (p. 26).

3.5.5 Support for Hyper-V 3.0

This section describes how Acronis Backup supports new features introduced in Hyper-V 3.0. This version of Hyper-V appears in Windows Server 2012.

VHDX format

The VHDX format appeared in Hyper-V 3.0 as a new version of the virtual hard disk (VHD) format. The VHDX format supports a maximum disk size of 64 TB, compared with the maximum size of 2 TB for VHD. The VHDX format also supports disks with a physical and/or logical sector size of 4 KB.

Agent for Hyper-V can back up and recover virtual machines whose disks have the VHDX format. When recovering a virtual machine from a Hyper-V host of an earlier version to a Hyper-V 3.0 host, the agent converts the machine's disks to the VHDX format.

When recovering a virtual machine with VHDX disks to a Hyper-V host of an earlier version, the agent converts the disks to the VHD format. The agent tries to make the resulting disk meet the requirements of the VHD format. For example, if the source VHDX disk is greater than 2 TB, the agent attempts to reduce the resulting VHD disk size to 2 TB.

Dynamic Memory

Dynamic Memory adjusts the original amount of the virtual machine's memory depending on the machine's actual memory needs. Agent for Hyper-V can back up and recover virtual machines that use the Dynamic Memory feature. However, the agent does not save the Dynamic Memory settings for these machines.

When recovering a machine to a new virtual machine, the agent sets up the original amount of memory for it. The Dynamic Memory feature for the recovered machine will be turned off.

Private VLANs

Private virtual local area networks (private VLANs, PVLANs) enable you to isolate groups of virtual machines on a host as if each group were on a separate physical network. This feature of Hyper-V 3.0

is useful when hosting virtual machines of more than one organization, to prevent any communication between machines that belong to different organizations.

When backing up a Hyper-V 3.0 virtual machine, Agent for Hyper-V backs up the machine's PVLAN settings. The agent recovers these settings when recovering the machine to a new or existing machine on *the same host.*

When recovering the machine to a *different host,* the agent clears the PVLAN settings for the recovered machine.

Virtual Fibre Channel HBAs

Virtual Fibre Channel host bus adapters (HBAs) enable each virtual machine to access a Fibre Channel storage as if the machine had an individual Fibre Channel connection. For example, you can configure a virtual machine to access only a specific logical unit number (LUN) of a Storage Area Network (SAN), rather than all of the LUNs available to the Hyper-V host.

Although Agent for Hyper-V can back up virtual machines that have HBAs, it cannot back up the contents of the storage itself. If you have to back up this storage directly from the virtual machine, install Agent for Windows into the guest operating system.

3.6 Backing up Linux logical volumes and MD devices

Acronis Backup can back up virtual machines that have logical volumes (also known as LVM volumes) or MD devices (also known as Linux Software RAID).

You can choose between backing up these machines at a hypervisor level (by using Agent for VMware or Agent for Hyper-V) or by installing Agent for Linux inside the guest operating system.

Backing up at a hypervisor level

This is your natural choice if you back up entire machines and recover them onto the same platform (ESX(i) or Hyper-V). You do not need to install multiple agents or create bootable media in this case.

Since Agent for VMware or Agent for Hyper-V cannot access the file system of a logical volume or MD device, they back up the underlying disks or partitions sector-by-sector. Non-LVM volumes are backed up in the normal mode, by backing up their file systems. All backed up data can be recovered back to the original place without any problem.

Limitations

Sector-by-sector backup of logical volumes results in the following limitations:

- If the root directory is located on a logical volume, the system may fail to boot after recovery to hardware or to a different platform (ESX(i) or Hyper-V). Please be aware of this, since recent Linux distributions, such as Fedora or RHEL, place the root directory on a logical volume by default. Use the Acronis Universal Restore tool to make the recovered system bootable.
- When creating a backup plan, you cannot select a logical volume or MD device. Select either the entire machine or all of the partitions that make up the volume group or device.
- File backup and file recovery from a disk-level backup are not possible for files located on logical volumes and MD devices.
- Resizing of a logical volume during recovery is not possible.

The common limitation of hypervisor-level backup is that you cannot execute pre/post backup or pre/post data capture commands within the guest operating system.

Installing the agent into the guest system

For advanced operations, install Agent for Linux in the guest system and back up the logical volumes/MD devices as the ones of a physical machine. By doing this, you will overcome almost all of the above limitations.

Using Linux-based bootable media, you will be able to recover logical volumes/MD devices "as is". However, the Acronis Universal Restore tool is still required for virtual-to-physical and virtual-to-virtual machine conversion. For more information about backing up logical volumes and MD devices on physical machines, see the Acronis Backup Advanced User Guide.

3.7 File-level recovery

Agents for VMware and Agent for Hyper-V can recover files from a file backup or from a disk backup of a physical or virtual machine.

Depending on the agent that performs the recovery, you can recover files to the following locations:

- **A local folder** on the machine where the agent is installed. This location is not available for Agent for VMware (Virtual Appliance).
- **A network share**
- **An FTP or SFTP server**

To recover files by using the management server

1. Connect the console to the management server.
2. If the backup is stored in a managed vault, click **Data catalog**. Otherwise, click the respective centralized unmanaged vault and then click the **Data view** tab.
3. Select the files and the point in time to recover them to. We recommend selecting the files as follows:
   a. Select **Show > Folders/files**.
   b. Select the files and the point in time.
   c. Click **Recover**.

   Details. If the backup is stored in a centralized unmanaged vault, the files may initially not appear in **Data view**. The reason is that Agent for VMware (Virtual Appliance) does not catalog data to the file level when backing up to such vaults. If you cannot find a file in **Data view**, use **Archive view**:
   - Click the **Archive view** tab, expand the archive, right-click the backup, and then click **Recover**. In **Backup contents**, select **Files** and then select the files to recover.

   Alternatively, update the catalog by clicking **Catalog now**, and then use **Data view** again. Updating the catalog may be time-consuming.
4. Under **Where to recover**, select Agent for VMware (Virtual Appliance) or Agent for Hyper-V that will perform the recovery.

   Tip. Alternatively, you can select a machine where Agent for Windows or Agent for Linux is installed. This way, you can recover the files directly onto that machine.
5. Proceed with creating the recovery task.

Using a similar procedure, you can recover files when the console is directly connected to an agent. Use either **Data view** or **Archive view** when connected to Agent for Hyper-V. When connected to Agent for VMware (Virtual Appliance), the **Data view** tab is available only for managed vaults and a locally attached storage (p. 15).

Recovering files to a virtual machine

To recover files directly into a virtual machine, use either of the following methods:

- **Recover the files to a system network share** of the virtual machine. For example, the **\\MyVM\c$** network share corresponds to the C volume of the **MyVM** virtual machine. This method applies only to virtual machines running Windows. You must specify the credentials of an administrator on the virtual machine.
- Install Agent for Windows or Agent for Linux **inside the guest operating system** and then recover the files by using this agent.

Or you may recover the files to a network share in your network, and then move them to the virtual machine or access them from the virtual machine.

3.8 Virtual machines on a management server

Availability of virtual machines

Virtual machines are displayed as available when the agent is available for the management server and the machines are available for the agent. The list of virtual machines is refreshed dynamically every time the management server synchronizes with the agents.

When the virtualization server or the virtual appliance becomes unavailable or is withdrawn, the virtual machines are grayed out.

When virtual machines become unavailable for the agent (this happens when machines are removed from the virtualization server inventory, deleted from the disk, or the server's storage is down or disconnected), the machines disappear from the **All virtual machines** groups and other groups they are included in. Tasks that back up these virtual machines will fail with an appropriate log record; as a result, the backup plan will have the **Error** status.

The online or offline state of a virtual machine does not affect its backup since virtual machines can be backed up in both states.

Backup plans for virtual machines

Virtual machines can be included in a backup plan that backs up disks and volumes.

What happens when a group of virtual machines is included in a backup plan

Each machine will be backed up to a separate archive. The default archive name will include the virtual machine name. It is advisable to keep the default archive naming so that you can easily find each machine's backups in the storage vault.

The backups can run concurrently even if executed by the same agent. You can set the number (p. 32) of virtual machines for the agent to simultaneously back up. The maximum value is 10.

Grouping of virtual machines

The **Virtual machines** section of the navigation tree contains one built-in group called **All virtual machines**. You cannot modify this group manually, delete or move it. You can include this group in a backup plan that backs up disks and volumes.

You can create both static and dynamic groups of virtual machines. Any virtual machine that is currently available can be added to a static group. You cannot create groups that contain both physical and virtual machines.

The membership criteria for dynamic groups of virtual machines are as follows:

- **Virtualization server type**

Using this criterion, you can create a dynamic group of virtual machines hosted on all registered Hyper-V or ESX(i) servers. Any machine added to the servers will appear in this group. Any machine deleted from the servers will disappear from this group.

- **All VMs backed up by agent**

Using this criterion, you can create a dynamic group of virtual machines managed by the specified agent.

- **Operating system**

Using this criterion, you can create a dynamic group of virtual machines running the specified operating system.

3.9 VM-specific backup and recovery options

When you create a backup plan or recovery task, these options appear in the **Plan parameters** or **Task parameters** section. You can either use a default option, or override the default option with the custom value that will be specific for this plan only.

To view and change the default options, connect the console to the management server or to the machine with the agent, and then select **Options** > **Default backup and recovery options** from the top menu.

3.9.1 Simultaneous VM backup

This option is effective when backing up virtual machines with Agent for VMware or Agent for Hyper-V.

This option is not effective when the backup destination is Acronis Cloud Storage.

This option defines how many virtual machines an agent can back up simultaneously when executing the given backup plan.

The preset is: **2**.

If, according to the backup plan, an agent has to start backing up multiple machines at once, it will choose two machines. (To optimize the backup performance, the agent tries to match machines stored on different storages.) Once any of the two backups is completed, the agent chooses the third machine and so on.

You can change the number of virtual machines for an agent to simultaneously back up. The maximum value is 10.

To prohibit simultaneous backup, clear the **Back up virtual machines simultaneously** check box. The backups will be queued by the agents.

Tips on usage

Remember that you can make a different setting for each agent, depending on its host load, available transports (LAN, SAN, Hot-add) and other factors. To do so, connect the console to the agent and select **Options** > **Default backup and recovery options** > **Simultaneous VM backup**. These settings will be used unless you override them with the common setting set in the backup plan.

By default, Agent for VMware (Virtual Appliance) uses 2 virtual processors. If you observe that CPU usage during backup approaches 100%, increase the number of virtual processors in the virtual appliance settings. This may significantly increase simultaneous backup performance. Power off the virtual appliance, click **Edit settings…**, choose **Hardware** > **CPUs** and select the desired number of processors.

3.9.2 VM power management

These options are effective for virtual machines residing on the virtualization servers.

These options are available only if any Acronis agent for virtual machines is installed on the virtualization server.

Power off target virtual machines when starting recovery

The preset is: **On**.

Recovery to an existing virtual machine is not possible if the machine is online, and so the machine is powered off automatically as soon as the recovery task starts. Users will be disconnected from the machine and any unsaved data will be lost.

Clear the check box for this option if you prefer to power off virtual machines manually before the recovery.

Power on the target virtual machine when recovery is completed

The preset is: **Off**.

After a machine is recovered from a backup to another machine, there is a chance the existing machine's replica will appear on the network. To be on the safe side, power on the recovered virtual machine manually, after you take the necessary precautions.

Select the check box for this option if automatic powering on of the virtual machine is required.

3.10 Limitations for backup and recovery options

The following backup options are effective for backup inside the guest system but not for backup at a hypervisor level:

- **Fast incremental/differential backup**
- **File-level backup snapshot**
- **File-level security**
- **LVM snapshotting**
- **Media components**
- **Multi-volume snapshot**
- **Pre/Post data capture commands**
- **Volume Shadow Copy Service**

The **Pre/Post commands** options, both for backup and for recovery, are effective only for Agent for Hyper-V. The commands that you specify in these options run on the machine with the agent and not on the virtual machines being backed up or recovered.

4 Backup from inside a guest OS

Backup from inside a guest OS assumes backing up and recovering virtual machines similarly to physical machines. This functionality becomes available by using Acronis Backup Agent for Windows or Acronis Backup Agent for Linux.

For online backup and recovery, install Agent for Windows or Agent for Linux in the corresponding guest system. You can use bootable media to do off-line ("cold") backups and "bare metal" recovery to an empty virtual machine. Installing the software, backing up, and recovery are the same as with a physical machine.

4.1 Working with Red Hat Enterprise Virtualization

This section describes in brief how to use Acronis Backup in Red Hat Enterprise Virtualization environments. It also guides you through P2V and V2V migrations that can be performed with Acronis Backup.

4.1.1 Overview of the RHEV platform

Red Hat Enterprise Virtualization (RHEV) is a virtualization solution based on Red Hat Enterprise Linux. Its advanced functionalities allow enterprises to centrally manage their virtual environments while reducing the cost and complexity of large deployments.

Components

The RHEV platform consists of the following components:

- Red Hat Enterprise Virtualization Manager which allows system administrators to view and manage virtual machines via a single graphical user interface.
- Hosts running Red Hat Enterprise Virtualization Hypervisor or Red Hat Enterprise Linux where virtual machines are hosted.

Interfaces

The Red Hat Enterprise Virtualization Manager includes an Administration Portal and a User Portal.

- The Administration Portal is designed for setting up, configuring, and managing the Red Hat Enterprise Virtualization environment.
- The User Portal allows users to start, stop, reboot, and connect to virtual machines.

Storage domains

The RHEV platform uses the following storage domain types:

- **Data domains** store virtual disks, templates and snapshots. A data domain cannot be shared across different data centers. A data domain can be organized by using NFS, SAN (iSCSI/FCP-connected storages), or a local storage of a virtualization host.
- **ISO domains** store ISO files used to install and boot operating systems and applications for the virtual machines. An ISO domain can be shared across different data centers. An ISO domain can only be organized by using NFS.
- **An export domain** is used to copy or move images between data centers and RHEV Manager installations. An export domain can be moved between data centers. However, it can only be

active in one data center at a time. An export domain can use NFS or SAN (iSCSI/FCP-connected storages).

4.1.2 How Acronis Backup works with RHEV

Acronis Backup can back up and recover virtual machines running in the Red Hat Enterprise Virtualization environment. Backup and recovery become available by installing Agent for Linux or Agent for Windows into the guest systems. This means that Acronis Backup will treat the virtual machines as physical ones and provide the full scope of functionality it provides for physical machines. This also means that operations are not possible on the machines that are powered off.

Backup and recovery (p. 36)

Using Acronis Backup Management Server, you can:

- Centrally deploy the agents onto the virtual machines managed by your RHEV Manager.
- Create and deploy centralized backup plans which the agents will execute.
- Monitor how successfully the backup plans are executed.
- Recover disks, volumes, files or entire machines to their original location or to a different machine.
- View alerts, logs, reports, current activities and more.

In addition, you can directly manage each individual machine by connecting Acronis Backup Management Console to it.

P2V and V2V migration (p. 41)

Acronis Backup provides several migration methods for you to easily migrate physical machines to the RHEV environment. The methods differ in complexity and flexibility. They cover all possible scenarios of migration. These methods can also be used to migrate a virtual machine from a different virtualization platform to the RHEV platform.

Licensing

You need a license for each host running at least one machine that needs backing up. Taking into account that machines migrate within a cluster, you need one license for each clustered host. An Acronis Backup Advanced for RHEV license enables backing up an unlimited number of virtual machines which run on the same host and an unlimited number of migrations to that host.

To install the product in the trial mode, you do not need a license key. In the trial mode, you can back up the hosted machines during a limited time period and perform three migrations to the host.

Supported versions of RHEV

- Red Hat Enterprise Virtualization Manager: versions 2.2, 3.0, 3.1, 3.2.
- Red Hat Enterprise Virtualization Hypervisor, Red Hat Enterprise Linux: versions 5.5 and higher.

Supported guest OS

Acronis Backup supports all the virtualized guest operating systems supported by RHEV.

- Red Hat Enterprise Linux 3 (32-bit and 64-bit)
- Red Hat Enterprise Linux 4 (32-bit and 64-bit)
- Red Hat Enterprise Linux 5 (32-bit and 64-bit)
- Red Hat Enterprise Linux 6 (32-bit and 64-bit)

- Windows XP Service Pack 3 and newer (32-bit only)
- Windows 7 (32-bit and 64-bit)
- Windows 8/8.1 (32-bit and 64-bit)
- Windows Server 2003 Service Pack 2 and newer (32-bit and 64-bit)
- Windows Server 2008 (32-bit and 64-bit)
- Windows Server 2008 R2 (64-bit only)
- Windows Server 2012/2012 R2

4.1.3 Backup and recovery of RHEV virtual machines

This section contains step-by-step instructions enabling you to quickly set up centralized backups of virtual machines and to see what recovery is like. These steps may be sufficient for protecting a basic RHEV environment. Nevertheless, you can use the full scope of the Acronis Backup functionality described in the product Help, Installation Guide, User Guide for Acronis Backup Advanced, and Command-Line Reference.

4.1.3.1 Prerequisites

Make sure that:

- You have the RHEV infrastructure deployed.
- You know the name or IP address of the RHEV Manager server and the credentials to access the server.
- You know the administrative user name and password for each of the guest systems you want to back up.
- You have a machine running Windows that will act as the management server. This machine must be always turned on and available across the network.
- You downloaded the setup program of Acronis Backup Advanced.
- You have the Acronis Backup Advanced license keys (Universal or for RHEV) in a TXT or EML file. You need a license for each host running at least one machine that needs backing up. Taking into account that machines migrate within a cluster, you need one license for each clustered host. For multiple license keys, the text format is one line for one key.

4.1.3.2 Installing Acronis Backup Management Server

1. On the machine that will act as the management server, log on as an administrator and start the Acronis Backup setup program.
2. Click **Install Acronis Backup**. Accept the terms of the license agreement.
3. Select the **Centrally monitor and configure the backing up of physical and virtual machines** check box.
4. Type all your license keys or import them from a text file.
5. Click **Install**.

4.1.3.3 Adding RHEV machines to Acronis Backup Management Server

In this step, you will add machines from the RHEV environment to Acronis Backup Management Server. Acronis Backup agents will be automatically installed on these machines.

Alternatively, you can install the agents on each machine manually as described in the "Hot imaging..." (p. 46) section. After the agents are installed, add the machines to the management server.

To use the following procedure, you need:

- Red Hat Enterprise Virtualization Manager version 3.x. If your Manager version is 2.2, install the agents manually or use other installation methods described in the installation documentation.
- Guest tools installed on every machine you want to add.

Preparation of RHEV machines running Linux

1. For successful installation of Acronis Backup Agent for Linux, you may need to manually install the following Linux packages: **gcc**, **make**, and **kernel-devel**. For details, see the "Preparation" section in "Installation of Agent for Linux" (p. 46).
2. Make sure that TCP port 22 is opened and that the SSH daemon is running on each virtual machine you want to add. After the remote installation is complete, you can close the port and stop the SSH daemon.
3. Open TCP port 9876 on each virtual machine you want to add. Acronis Backup uses this port for communication between the components; therefore, it must remain open for both incoming and outgoing requests.
4. By default, the management server takes the installation packages from the folder **%CommonProgramFiles%\Acronis\RemoteInstaller**<product build number>. To be able to remotely install Agent for Linux, download the agent installation files (.i686 or .x86_64) from the Acronis website and put them into this folder on the management server.

Preparation of RHEV machines running Windows

1. For successful installation on a remote machine running Windows XP, the option **Control panel > Folder options > View > Use simple file sharing** must be *disabled* on that machine.

   For successful installation on a remote machine running Windows Vista or later, the option **Control panel > Folder options > View > Use Sharing Wizard** must be *disabled* on that machine.
2. For successful installation on a remote machine that is *not* a member of an Active Directory domain, User Account Control (UAC) must be *disabled*.
3. File and Printer Sharing must be *enabled* on the remote machine. To access this option:
   - On a machine running Windows XP with Service Pack 2 or Windows 2003 Server: go to **Control panel > Windows Firewall > Exceptions > File and Printer Sharing**.
   - On a machine running Windows Vista, Windows Server 2008, Windows 7, or later: go to **Control panel > Windows Firewall > Network and Sharing Center > Change advanced sharing settings**.
4. Acronis Backup uses TCP ports 445 and 25001 for remote installation. Also, it uses TCP port 9876 for remote installation and for communication between the components.

   Port 445 is automatically opened when you enable File and Printer Sharing. Ports 9876 and 25001 are automatically opened through Windows Firewall. If you use a different firewall, make sure that these three ports are open (added to exceptions) for both incoming and outgoing requests.

   After the remote installation is complete, you can remove ports 445 and 25001 from exceptions. Port 25001 is automatically closed through Windows Firewall. Port 9876 needs to remain open.

Connecting to the management server

1. Double-click the **Acronis Backup** icon on the desktop to start the management console.
2. Connect the console to the management server: Click **Connect to a management server**.

a. Enter the server name or IP address.
b. If prompted for credentials, specify the user name and password.

Adding machines from RHEV environment

1. On the **Actions** menu, click **Add multiple machines**.
2. Click **From Red Hat Enterprise Virtualization environment**. Specify the name or IP address of the RHEV Manager server and credentials of the account with the rights to access this machine. When entering the name of an Active Directory user account, be sure to also specify the domain name (DOMAIN\Username or Username@domain).
3. In the opened window:
   a. Specify the machines you want to add to the management server:
      - Click **Add** to specify the selected machine.
      - Click **Add all** to specify all virtual machines included into the selected data center or cluster.

      Details. You can add only the machines that are currently powered on. To search for a machine, you can type its exact name or use wildcards in the search box.
   b. The software automatically retrieves IP addresses of the specified machines from the RHEV Manager. If a machine has several IP addresses, you can select the value from the drop-down list. If the **IP address** box is empty, enter the IP address manually.

      Details. The IP address may be not available if, for example, guest tools are not installed in the guest OS.
   c. Provide the credentials of the user with administrative privileges for each machine. If there is a universal administrator account on the network, enter the account credentials for one machine, and set the option to apply it to all the machines that you specified.
   d. Click **OK**.

Installing agents

Acronis Backup detects on which of the selected machines its agents are not installed. If there is at least one machine without an agent, do the following:

1. Agent for Windows and/or Agent for Linux is selected for installation by default. Click **Next**.
2. Click **Use licenses from the following license server**. In the opened window:
   a. Specify the name or IP address of the management server and administrative credentials.
   b. [Optional] If you need to specify additional licenses, click **Add license** and type the license keys or import them from a text file. Click **OK**.
   c. Click **Next**.
3. Leave the default installation options for the agent.
4. Specify whether the machines will participate in Acronis Customer Experience Program (CEP).

   Details. Acronis Customer Experience Program applies only to machines running Windows.
5. The summary window displays a list of machines where the components will be installed. Click **Proceed** to start the installation.

Once the installation starts, the program displays the operation progress and names of the machines where the agent is being installed.

Managing the machines

For further work with the machines you added, select **Machines with agents** from the **Navigation** tree.

4.1.3.4 Creating a bootable media

In this step, you will install Acronis Media Builder and create a bootable media ISO. The ISO file is required when you recover (p. 48) an entire virtual machine. Also, you can back up a virtual machine using the ISO, if you do not want to install the backup software in the guest system.

Installing Acronis Media Builder

First, you need to install Acronis Media Builder on one of the machines running Linux. The machine must have Linux desktop GUI installed.

Download the Acronis Media Builder installation file and save it on the selected machine. Then, go to the directory where the installation file is located and run the following commands:

- If the machine is running a 32-bit operating system,

```
chmod 755 AcronisBackup*
./AcronisBackupAdvancedMediaBuilderL_11.7_.i686 -a
```

- If the machine is running a 64-bit operating system,

```
chmod 755 AcronisBackup*
./AcronisBackupAdvancedMediaBuilderL64_11.7_.x86_64 -a
```

Creating a bootable media

To create a bootable media:

1. Run Acronis Media Builder by using the following command:

```
sudo mediabuilder
```

2. Follow the on-screen instructions. For detailed information, refer to the built-in Help. It is available in every program window by pressing F1.
3. In the **Select the media output** window, select **ISO image**. Then select a directory on the RHEV ISO domain and specify the ISO file name. The default name is AcronisMedia.iso. Or, you can enter the directory path manually; for example, nfs://10.200.200.10/opt/iso:/{ISO DOMAIN UUID}/images/11111111-1111-1111-1111-111111111111.

   Alternatively, you can save the ISO on a network share and then import it to the ISO domain using the ISO uploader utility.

4.1.3.5 Backing up RHEV machines

In this step, you will create an unmanaged centralized vault and set up a centralized backup plan for multiple machines.

An unmanaged vault is just a shortcut to a shared folder on the network. In general, it is recommended that you install a storage node and create a managed vault on the node to be able to use data deduplication and the centralized data catalog.

Creating a centralized vault

1. Create a shared folder on the network.
2. Start the management console.
3. Connect the console to the management server.
4. In the **Navigation** tree, click **Vaults**, and then click **Create**.
5. Specify the name of the new vault. Optionally, type the comments on the vault.
6. Click **Path**. In the **Path** field, type the folder path. Or, you can select this folder in the tree. Click **OK** to confirm your selection. If prompted, provide access credentials for the location.

7. Click **OK** to create the vault.

Backing up the machines

1. In the management console, click **Create backup plan**.
2. Under **What to back up**, click **Items to back up**.
3. Expand the **Management Server** node, expand the **Machines with agents** node, and then expand the **All Machines** node.
4. Select the check boxes next to the machines you want to back up. Click **OK** to confirm your selection.
5. Under **Where to back up**, click **Location**. In the opened window, expand the **Centralized** node, and then select the vault you have created. Click **OK** to confirm your selection. If prompted, provide access credentials for the vault.
6. Under **How to back up**, in **Backup scheme** box, specify **Manual start**.
7. Click **OK** to create the backup plan.
8. You will be taken to the **Backup plans and tasks** view, where you can see the backup plan you just created. Select this plan and click **Run**.

   Details. Later, you can manually run the same backup plan again.

4.1.3.6 Recovering RHEV machines

You can recover RHEV machines using one of the following methods:

- **Recovering to a machine running the operating system**

  Use this method if the Acronis agent is running on the machine and you need to recover the lost data (a data disk, a data volume, or an individual file) or add the backed-up data from another machine.

  To recover the operating system itself, the Acronis agent will need to boot the machine into the bootable environment. If the machine is running Linux, make sure that, in addition to Agent for Linux, you have installed Acronis Backup Bootable Components & Media Builder for Linux.

- **Recovering to a machine booted with bootable media**

  Use this method when you need to recover the operating system that has crashed or is infected with malware. Installation of the bootable components is not required in this case because the components will be loaded from the media to the machine's RAM.

To recover to a machine running the operating system

1. Start the management console.
2. Connect the console to the management server or directly to the target machine.
3. Click **Recover**.
4. Under **What to recover**, click **Select data**. In the opened window:
   a. Select **Data path** box.
   b. Click **Browse**.
   c. In the opened window, expand the **Centralized** node, select the vault where your backup is stored and press **Enter**. If prompted, specify the user name and password to access the vault location.
   d. On the **Data view** tab, in the **Show** box, select **Machines/disks/volumes** to browse and search for entire disks and volumes in disk-level backups.

      Details. You should select **Folders/files** in the **Show** box when you want to recover individual files or folders.

e. Select the check boxes for the data disks you want to recover.

f. Select the date of the backup version you want to recover. By default, the latest version is selected.

g. Click **OK**.

5. Make sure that under **Where to recover**, in **Recover to**, the **Physical machine** option is selected. As a result:
   - If the console is connected to the management server, the data will be recovered to the original machine by default. To select a different target machine, click **Browse**. Make sure that the target machine has enough disks with sizes at least as big as the original disks.
   - If the console is connected directly to the target machine, the data will be recovered to that machine.
6. [Optional] Acronis Backup maps the selected disks to the target disks automatically. If you are not satisfied with the mapping result, you can re-map the disks manually:
   a. Unmap the disks in the reverse order; that is, the last mapped disk should be unmapped first.
   b. Select the destination disk for each of the source disks.
7. Under **When to recover**, specify **Now** to perform the recovery immediately.
8. Click **OK** to start the recovery.

   Details. You will see the operation progress.

To recover to a machine booted with bootable media

For the detailed description of the procedure, see "Recovery to an existing virtual machine booted with bootable media" (p. 48).

4.1.4 Migrating a physical machine to a virtual machine

4.1.4.1 Considerations before migration

Migration of a physical machine to a RHEV environment is performed in two steps. First, you create an image of the machine in a .tib file on an intermediate storage. Next, you deploy this image to a new or existing RHEV virtual machine. Acronis Backup can create a new, fully configured virtual machine directly in a RHEV export domain. You only need to import it to the required data center.

A machine image is also referred to as a "backup" because it is created using the backup software.

When choosing the migration method, take into account the following considerations.

Choose intermediate storage

Decide where you will save the image. With the default level of data compression, the required storage space is around 70% of the amount of data to be migrated. Consider an SMB (CIFS) or NFS network share or a fixed disk of the machine being migrated. External devices, such as USB drives, are also supported.

Migrate an entire machine or exclude some of the disks?

If there is a storage connected to the machine using iSCSI HBA, exclude it from the image. You will be able to add this storage to the resulting virtual machine using iSCSI software initiator after the migration completes.

A Fibre Channel-connected storage cannot be added to a RHEV virtual machine. If you need the storage on the resulting virtual machine, let it be included in the image. The storage will be converted to a virtual disk. Otherwise, exclude the storage from the image.

Imaging method: hot or cold?

The image can be taken under the operating system (hot imaging) or under bootable media (cold imaging). Take into account the following considerations.

- **Is the server reboot/downtime acceptable?**

  During cold imaging, the imaged machine will be off-line and will not provide the necessary services.

- **Do you need Acronis software on the resulting machine?**

  Hot imaging requires installation of an Acronis agent on the physical machine. The agent will be present in the migrated system as well. If you are planning to back it up using Acronis Backup, having the agent already installed is a plus. If adding software to the system is not acceptable, use cold imaging.

- **Do you need migration on a schedule?**

  A migration that uses hot imaging can be scheduled. This comes in handy for updating the virtual "standby" server. Cold migration is performed interactively.

- **Is it critical that the latest changes to the original system will be missing in the migrated system?**

  Once the hot imaging starts, Acronis Backup takes a snapshot of the physical machine. Then, it compresses the snapshot data and saves it to the location you specify. During this process, changes to the original system may occur. The changes will not be transferred to the migrated system because they are not present in the snapshot. If you decommission the physical machine or return it to a lessor, the changes will be lost. To avoid the data loss, use cold imaging.

Deployment method: convert or recover?

Acronis Backup can deploy the image automatically as soon as it is created. This method is called "conversion to a virtual machine". The resulting virtual machine will be similar to the original machine. If you configure the deployment as a separate operation (recovery), you will be able to change the machine configuration: add/remove/resize disks, and set the virtual machine memory.

Resizing the disks during recovery makes good sense because the newly created disks always have the Raw format. They will needlessly occupy a lot of space if the data size is much less than the disk size. The alternative way to save space is recovery to a previously created virtual machine with the optimal disk sizes.

Let Acronis create a virtual machine or do it yourself?

Take into account the following considerations.

- **Recreate logical volumes or convert them to basic ones?**

  A machine created by Acronis always has basic volumes. If logical volumes or MD devices are present in the image, they will be converted to basic ones. The same applies to dynamic volumes used in Windows systems. The operating system remains bootable, since Acronis properly updates GRUB and standard Windows loaders. Custom boot loaders may require manual reactivation.

  The original LVM structure can be reproduced only if you create the RHEV virtual machine in advance and boot it using bootable media. Then, either perform recovery with the enabled **Apply RAID/LVM** option, or create the LVM structure manually and then perform recovery with the disabled option.

  There is no option to recreate dynamic volumes during recovery. If you need dynamic volumes on the resulting machine, create the volume group using the disk management functionality of the bootable media. Then, perform recovery over these volumes.

- **Are you ready to provide necessary drivers for Universal Restore?**

  When Acronis creates a virtual machine on its own and deploys an image to it, the necessary drivers are installed automatically because the software knows what drivers or modules are required for the machine. When you create a machine and boot it using bootable media, Acronis treats it as a physical machine. This is why you need to explicitly apply Universal Restore and specify the path to the necessary drivers. The ISO of the floppy disk with the drivers can be found in the RHEV ISO domain. Its default name is virtio*.iso.

4.1.4.2 Migration methods

Based on the considerations described in the previous section, we suggest the following methods of migration. Choose the one that best suits your needs.

Cold imaging + recovery to a new machine

This is the simplest method. It fits most cases and does not require software installation. It allows you to modify basic settings of the virtual machine, including disk size.

Step-by-step instructions (p. 43)

Hot imaging + conversion to a virtual machine

This is a simple method. It requires software installation unless the machine is already protected with an Acronis agent. The virtual machine settings cannot be modified on the fly. The method is useful in the "stand-by server" scenario when you create a spare virtual machine and update it from time to time. Also, you can easily back it up using Acronis Backup because the virtual machine contains an Acronis agent.

Step-by-step instructions (p. 47)

Hot imaging + recovery to a new machine

This is a combination of the previous two methods. It is useful for migrating a machine already protected with an Acronis agent. It allows you to modify basic settings of the virtual machine, including disk size.

Step-by-step instructions can be combined from the ones of the previous two methods.

Recovery to an existing virtual machine booted with bootable media

This is the most advanced and flexible method. This is the only way to reproduce LVMs or software RAID on the resulting virtual machine. With this method, you can use all the functionality available at a physical machine recovery and create whatever volume layout you wish. The imaging method can be either cold or hot. It does not influence the recovery.

Step-by-step instructions (p. 48)

4.1.4.3 Cold imaging + recovery to a new machine

Preparation

Configuring an NFS export domain

1. Make sure that an NFS export domain is attached to the data center where you want to save the virtual machine.

2. For RHEV Manager to be able to import the resulting virtual machine to the data center, the virtual machine files must have the same owner (**vdsm:kvm**) as the NFS export directory.

   This can be achieved by adding the following NFS export settings:

   - Map all users to the anonymous account.
   - Set the user ID of the anonymous account to **36** (**vdsm**).
   - Set the group ID of the anonymous account to **36** (**kvm**).

   With these settings, files written to the directory by any user will be owned by **vdsm:kvm**. After the migration is finished, you may revert the NFS export settings to the original values.

   Example. In Linux, NFS exports are controlled by the **/etc/exports** configuration file. In this file, the line corresponding to the export directory can look as follows:

   ```
   /opt/export *(rw,sync,all_squash,anonuid=36,anongid=36)
   ```

   where **/opt/export** is the export path; **all_squash** maps all user IDs and group IDs to the anonymous account; **anonuid** and **anongid** explicitly set the user ID and group ID of the anonymous account to the specified values.

Getting bootable media

If you have installed Acronis Backup in the *trial* mode, do the following:

- Download the ISO of "**Migration to RHEV media**" from the Acronis website. Burn the ISO to a CD or DVD by using a third-party tool.

If you have installed Acronis Backup in the *full* mode, do either of the following:

- Download the ISO of either "**Migration to RHEV media**" or regular "**Bootable media**" from the Acronis website. Burn the ISO to a CD or DVD by using a third-party tool.

  OR

- Create the regular bootable media by using Acronis Media Builder.

Booting the machine

1. Boot the physical machine using the bootable media.
2. In the boot menu, click **Acronis Backup** or **Migration to RHEV** (depending on the media you have).
3. [Optional] Click **Configure network...** to check the network settings and to change them if necessary. These settings are used as long as the machine is booted from the media.
4. Click **Manage this machine locally**.
5. On the **Tools** menu, click **Change volume representation**. If the machine's operating system is Linux, make sure that the media is in the "Linux-style volume representation" mode. If the machine's operating system is Windows, make sure that the media is in the "Windows-style volume representation" mode.

Imaging

1. Click **Back up now**.
2. By default, all disks of the machine are selected for imaging. If you need to exclude a disk or volume, under **What to back up**, click **Items to back up** and clear the check box near the disk or volume. For more details about the exclusion, see "Considerations before migration" (p. 41).

   Details. In addition, you can use the **Show exclusions** control to exclude files. Do not try to use this control to exclude disks. It works at a file level.
3. Under **Where to back up**, click **Location**. In the opened window:

a. Specify the location where to save the image. For more details about the location, see "Considerations before migration" (p. 41).
b. [Optional, but recommended] In the **Name** box, type the image name. It could be the name of the machine being imaged. The name cannot end with a number.
c. Click **OK**.

4. [Optional] Under **Parameters**, in **Backup options**, you can set other parameters of the imaging such as compression or network bandwidth usage.
5. Click **OK** to start the imaging.

   Details. You will see the operation progress.
6. After the operation is completed, click **Close** in the progress window.

   Details. To view the operation log, select **Navigation** > **Log** from the menu**.**

Recovery

1. Click **Recover**.
2. Under **What to recover**, click **Select data**. In the opened window:
   a. In the **Data path** box, enter the path to the image location and press **Enter**. If prompted, specify the user name and password to access the location.
   b. In the **Archive view** tab, expand the archive you have created in the "Imaging" step and select the image. Normally, it is named like "Backup #1".
   c. Select the check boxes for all of the MBRs and volumes.
   d. Click **OK**.
3. Under **Where to recover**, in **Recover to**, select **New virtual machine**.
4. Click **Browse**, select **Save the virtual machine as a set of files**, and then select **Red Hat Enterprise Virtualization** in the tree. Click **OK** to confirm your selection.
5. Click **Storage**, click **Browse**, and then do the following:
   - If the media is in the Linux-style volume representation mode, expand the **NFS folders** node, and then select the path to the RHEV export domain. Or, you can enter the NFS path manually; for example, nfs://10.200.200.10/opt/export:/{EXPORT DOMAIN UUID}.
   - If the media is in the Windows-style volume representation mode, expand the **Network folders** node, expand the **NFS** workgroup, and then select the path to the RHEV export domain. Or, you can enter the path manually; for example, \\10.200.200.10\opt\export\{EXPORT DOMAIN UUID}.

   Click **OK** to confirm your selection.
6. Click **Virtual machine settings**. In the opened window:
   a. [Optional] Change the number and size of the virtual machine's disks, memory, virtual machine name and/or the number of processors.

      Details. Resizing the disks makes good sense because the newly created disks always have the Raw format. They will needlessly occupy a lot of space if the data size is much less than the disk size. On the other hand, make sure that you do not set the disk size too low. The disks must have enough free space for the growing data and for the operating system to work.
   b. Click **OK**.
7. The destination disk for each of the source MBRs and volumes is selected automatically. You can change the destination if required.
8. [Optional] Under **Task**, in **Recovery options**, you can set other parameters of the recovery.

9. Click **OK** to start the recovery.

   Details. You will see the operation details.
10. Click the **Progress** tab to see the operation progress.
11. After the operation is completed, click **Close** in the progress window.
12. Import (p. 50) the machine to the required data center using RHEV Manager.

4.1.4.4 Hot imaging + conversion to a virtual machine

Installation of Agent for Linux

This section describes how to install Acronis Backup Agent for Linux and Management Console on a machine running Red Hat Enterprise Linux.

Preparation

Installing Agent for Linux requires that the following Linux packages be present on the machine: **gcc**, **make**, and **kernel-devel**. Acronis Backup installer will download and install them automatically using your Red Hat subscription.

You need to install the packages manually if:

- The machine does not have an active Red Hat subscription or Internet connection.
- The installer cannot find the **kernel-devel** and **gcc** version corresponding to the kernel version. If the available **kernel-devel** is more recent than your kernel, you need to either update the kernel or install the matching **kernel-devel** version manually.
- You have the required packages on the local network and do not want to spend time for automatic search and downloading.

To install the packages manually, run the following command as the root user:

```
rpm -ivh PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
```

Ensure that the **kernel-devel** version is the same as the kernel version. Ensure that the **gcc** version is the same as the one with which the kernel was compiled.

Installation in a 32-bit operating system

To install Agent for Linux and Management Console in a 32-bit operating system, go to the directory where the installation files are located and run the following commands:

```
chmod 755 AcronisBackup*
./AcronisBackupAdvancedAgentL_11.7_.i686 -a -l <license key>
./AcronisBackupAdvancedMConsoleL_11.7_.i686 -a
```

Installation in a 64-bit operating system

To install Agent for Linux and Management Console in a 64-bit operating system, go to the directory where the installation files are located and run the following commands:

```
chmod 755 AcronisBackup*
./AcronisBackupAdvancedAgentL64_11.7_.x86_64 -a -l <license key>
./AcronisBackupAdvancedMConsoleL64_11.7_.x86_64 -a
```

Installation of Agent for Windows

The following procedure describes how to install Acronis Backup Agent for Windows and Management Console on a machine running Windows. To do so:

1. Log on as an administrator and run the Acronis Backup Advanced setup program.
2. Click **Install Acronis Backup**.
3. Accept the terms of the license agreement, and then click **Next**.
4. Select the **Back up this machine's data** check box, and then click **Next**.
5. Click **I purchased a license or a subscription**, and then click **Next**.
6. Type your license key or import it from a text file, and then click **OK**. Click **Next**.
7. Ensure that the proper license is selected, and then click **Next**.
8. In the next window, leave the default setting: **I will register the component(s) later**. Click **Next**.
9. Specify whether the machine will participate in the Acronis Customer Experience Program (CEP). Click **Next**.
10. Click **Install** to proceed with installation.
11. On successful installation, click **Finish** to close the wizard window.

Hot imaging + conversion to a virtual machine

1. Configure an NFS export domain as described in the "Preparation" (p. 43) section.
2. Double-click the **Acronis Backup** icon on the desktop.

   If the machine is running Linux, you must be logged on as the root user. If you are logged on as a non-root user, run the following command:

   ```
   sudo acronis_console
   ```
3. Click **Manage this machine**.
4. Click **Create backup plan**.
5. By default, all disks of the machine are selected for imaging. If you need to exclude a disk, under **What to back up**, click **Items to back up** and clear the check box near the disk. For more details about the exclusion, see "Considerations before migration" (p. 41).

   Details. In addition, you can use the **Show exclusions** control to exclude files. Do not try to use this control to exclude disks. It works at a file level.
6. Under **Where to back up**, click **Location**. In the opened window:
   a. Specify the location where to save the image. For more details about the location, see "Considerations before migration" (p. 41).
   b. [Optional, but recommended] In the **Name** box, enter the image name. It could be the name of the machine being imaged.
   c. Click **OK**.
7. In **Backup scheme**, select **Manual start**.
8. Click **Show backup type, validation, convert to virtual machine**.
9. In **Convert to virtual machine**, select **Convert**.
10. By default, the current machine will perform the conversion. If you have selected a network share as the image location, you can click **Browse** and select another machine with the agent. Specify the credentials to access the machine.
11. Click **VM type**, select **Save as files of the VM type that I select to the folder that I specify**, and then select **Red Hat Enterprise Virtualization** in the tree. Click **OK** to confirm your selection.
12. Click **Storage**, and then do the following, depending on the machine's operating system:

- If the machine is running **RHEL**, expand the **NFS folders** node, and then select the path to the RHEV export domain. Or, you can enter the NFS path manually; for example, nfs://10.200.200.10/opt/export:/{EXPORT DOMAIN UUID}.
- If the machine is running **Windows**, select any convenient storage such as a local or network folder.

Click **OK** to confirm your selection.

13. [Optional] Under **Plan parameters**, in **Backup options**, you can set other parameters of the imaging, such as compression or network bandwidth usage.
14. Click **OK** to create the backup plan.
15. You will be taken to the **Backup plans and tasks** view, where you can see the backup plan you just created. Select this plan and click **Run**.
16. If the machine is running Windows: once the operation is completed, copy the created virtual machine to the RHEV export domain by using the operating system tools or third-party software.
17. Import (p. 50) the machine to the required data center using RHEV Manager.

4.1.4.5 Recovery to an existing virtual machine booted with bootable media

Preparation

1. If you do not have an image (a .tib file) of the machine you want to migrate, create it in either of the following ways:
   - Perform the "Preparation (p. 43)" and "Imaging (p. 44)" stages of the cold imaging (p. 43) procedure.
   - Perform steps 1-5 and 11-12 of the hot imaging (p. 47) procedure.
2. If you do not have the ISO of "**Migration to RHEV media**", download it from the Acronis website.
3. Save the ISO on the RHEV ISO domain.
4. Prepare a RHEV virtual machine to perform the recovery to. If necessary, create it using the Red Hat Enterprise Virtualization Manager.
5. If the source machine has logical volumes, decide whether you want the target virtual machine to have logical volumes as well.
   - If you want to reproduce the original LVM structure, make sure the target virtual machine has enough disks with sizes at least as big as the original disks. The volume structure will be created automatically if you choose the **Apply RAID/LVM** option.
   - If you want to obtain a different logical volume structure, you will need to create it manually. Make sure that the total size of the machine's disks is greater than the amount of data you are going to recover. The disks must have enough free space for the growing data and for the operating system to work.

Booting the machine

1. Boot the target machine by using the "**Migration to RHEV media**" ISO.
2. In the boot menu, click **Acronis Backup**.
3. [Optional] Click **Configure network...** to check the network settings and to change them if necessary.
4. Click **Manage this machine locally**.

[Optional] Creating the logical volumes

If you chose to create the logical volume structure manually, do the following:

1. On the **Actions** menu, click **Start shell**. Alternatively, you can press CTRL+ALT+F2.
2. Create the volume structure by using the `lvm` utility.
3. Press ALT+F1 to return to the graphical interface.

Selecting the image

1. Click **Recover**.
2. Under **What to recover**, click **Select data**. In the opened window:
   a. In the **Data path** box, enter the path to the image location and press **Enter**. If prompted, specify the user name and password to access the location.
   b. In the **Archive view** tab, expand the archive that contains the image, and select the image. Normally, it is named like "Backup #1".
   c. In **Backup contents**, select **Volumes**.
   d. Select the check boxes for all of the volumes and MBRs.
   e. Click **OK**.

[Optional] Applying RAID/LVM

If you chose to reproduce the original LVM structure, click **Apply RAID/LVM** and confirm the expected result that appears in a pop-up window. Otherwise, skip this step.

Mapping volumes

If you created the logical volume structure manually, specify where to place each of the volumes being recovered. Otherwise, the software automatically maps volumes from the image to the target machine disks. MBRs and boot volumes are always mapped automatically.

To map an MBR or a volume:

   a. Click **Required** next to it, and select the desired destination.
   b. If you need to resize a volume or change other volume properties, click **Properties** next to the volume. Make the necessary changes and click **OK**.

To change the mapping or size of a volume, you need to clear the mapping of the subsequent volumes. To clear the mapping of an MBR or a volume, click **Clear** next to it. To clear the mapping of all of the MBRs and volumes at once, click **Clear all**.

Starting the recovery

Click **OK** to start the recovery.

Applying Universal Restore

Universal Restore ensures that the operating system can boot on the new hardware.

1. Once the recovery is completed, boot the machine into **Acronis Universal Restore**.
2. Under **Universal Restore for Linux**/**Universal Restore for Windows**, select **Use**.
3. If the system being recovered is Windows, provide the RHEV drivers for it:
   a. In the RHEV Manager, right-click the virtual machine being recovered to, select **Change CD**, and select the ISO of the floppy disk with the drivers. This ISO can be found in the RHEV ISO domain. Its default name is virtio*.iso.
   b. On the machine, under **Automatic driver search**, click **Add folder**, expand the **Local folders** node, select the CD drive, and then click **OK**.

4.1.4.6 Importing a virtual machine to a data center

To import a machine from the export domain to the data center where the export domain is attached:

1. Go to the Red Hat Enterprise Virtualization Manager Web console.
2. In the upper row of tabs, click **Storage**.
3. Select the export domain to which the machine was added.
4. In the lower row of tabs, click **VM Import**.
5. Select the required virtual machine, and click **Import**.
6. Select the **Destination Cluster** and **Destination Storage** of the data center.
7. Click **OK** to start the import.