Acronis Backup & Recovery 11 Virtual Edition

Update 0

Backing Up Virtual Machines

Table of contents

1 Introduction

This document contains information that is specific for backup and recovery of virtual machines with Acronis Backup & Recovery 11 Virtual Edition.

For detailed information about the functionality provided by Acronis Backup & Recovery 11, please refer to the product help system, Web Help or guides for Acronis Backup & Recovery 11 Advanced Editions.

2 Supported virtualization platforms

The following table summarizes how various virtualization platforms are supported by Acronis Backup & Recovery 11.

Platform	Backup at a hypervisor level (p. 6)	Backup from inside a guest OS (p. 8)
VMware		
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 Microsoft Hyper-V Server 2008 R2	+	+
Microsoft Virtual PC 2005, 2007		+
Microsoft Virtual Server 2005		+
Citrix		
Citrix XenServer 4.1.5, 5.5, 5.6		+
Red Hat and Linux		
Red Hat Enterprise Virtualization (RHEV)		+
Kernel-Based Virtual machines (KVM)		+
Parallels		
Parallels Workstation		+
Parallels Server 4 Bare Metal		+

* 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 & Recovery 11 Agent for VMware vSphere ESX(i) or Acronis Backup & Recovery 11 Agent for Hyper-V. These agents require a license for Acronis Backup & Recovery 11 Virtual Edition to work.

Agents

Agent for VMware vSphere ESX(i) is delivered in two versions:

- Agent for ESX(i) (Virtual Appliance) can be imported or deployed to a VMware ESX(i) Server.
- For off-loaded backup, Agent for ESX(i) (Windows) can be installed on a machine running Windows.

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

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.

  A virtual machine can be running, stopped, suspended, or switch between the three states during backup.
- **Disk-level recovery**

  Recovery of entire machines or 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.
- **Cluster support**

  Backup and recovery of clustered virtual machines.
- **VMware vMotion/Microsoft Migration support** (p. 22)

  Uninterrupted backup during migration of the backed up machine. A backup plan is executed no matter which host the machine is running on.
- **Simultaneous backups of virtual machines** (p. 33)

  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 to handle one or multiple ESX(i) servers** (p. 16)

  Applies to VMware vSphere only

  Protect your virtual environment with as many agents as you want, from one agent for all hosts to one agent for each machine. The management server evenly distributes virtual machines among the agents. Or, you can bind the agents (p. 20) with the machines manually.
- **Off-load backup with Agent for VMware vSphere ESX(i) (Windows)** (p. 13)

Applies to VMware vSphere only

A Windows version of Agent for ESX(i) enables you to off-load backups from a ESX(i) host.

- **Automatic agent deployment** (p. 19)

  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. 18)

  Applies to VMware vSphere only

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

Limitations

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

- VMware vSphere does not support snapshots of fault tolerant virtual machines, independent disks, and Raw Device Mapping (RDM) disks in physical compatibility mode.
- 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. 8). Using this method, you can also:

- Perform a file-level backup and recovery.
- Execute pre/post backup or pre/post data capture commands within the guest operating system.
- Back up volumes created using Logical Volume Manager (LVM) on virtual machines running Linux.

For more details, please see the following sections:

- Backing up fault tolerant machines (p. 22)
- Backing up independent disks and RDMs (p. 23)
- Backing up pass-through disks (p. 29)

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 & Recovery 11 Agent for Windows or Acronis Backup & Recovery 11 Agent for Linux.

Agents

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.

Functionality

Backup from inside the guest OS includes all the Acronis Backup & Recovery 11 functionality available for physical machines. In particular, conversion to a virtual machine.

Conversion to a virtual machine

Wherever Agent for Windows is installed, it can convert a disk-level backup to a virtual machine of any of the following types: VMware Workstation, Microsoft Virtual PC, Parallels Workstation or Citrix XenServer Open Virtual Appliance (OVA). The virtual machine files will be saved to the destination you specify.

5 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.

6 Working in VMware vSphere

6.1 Getting started with Agent for ESX(i)

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

6.1.1 Prerequisites

Make sure that:

- You have a vCenter Server that manages one or more ESX(i) hosts.
- VMware Tools are installed on every virtual machine you want to back up. See installation instructions later in this section.
- You have one or more licenses for Acronis Backup & Recovery 11 Virtual Edition. Each ESX(i) host whose virtual machines you want to back up requires a separate license. You can purchase full license keys or obtain trial license keys.
- 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 & Recovery 11.

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.

6.1.2 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 & Recovery 11**.
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**.

6.1.3 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 & Recovery 11** 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. 24).*
5. Select the **Automatically deploy Agent for ESX(i) (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 ESX(i) has not been deployed yet. The agent will be deployed automatically after you select the virtual machines for backing up.

6.1.4 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 & Recovery 11** 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.

6.1.5 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 **Create backup plan**.
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 ESX(i) (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.

6.2 Installation of Agent for ESX(i)

Agent for ESX(i) enables backup and recovery of ESX(i) virtual machines without installing agents into the guest systems.

The agent is delivered in two versions:

- Agent for ESX(i) (Virtual Appliance) can be imported or deployed to a VMware ESX(i) host.
- For off-loaded backup, Agent for ESX(i) (Windows) can be installed on a machine running Windows.

Preparation

We highly recommend that you install Acronis Backup & Recovery 11 Management Server prior to the Agent for ESX(i) installation. During the agent installation, specify the management server each time you are asked to register the agent or prompted for a license server (unless you chose to use a separately installed license server).

Agent for ESX(i) (Virtual Appliance)

There are three methods of installing **Agent for ESX(i) (Virtual Appliance)**:

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

  Use this method for troubleshooting purposes or if you cannot install Acronis Backup & Recovery 11 Management Server for some reason.
- Deployment (p. 15) from Acronis Backup & Recovery 11 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 ESX(i)**. Refer to the context help for further instructions.

- Automatic deployment from Acronis Backup & Recovery 11 Management Server.

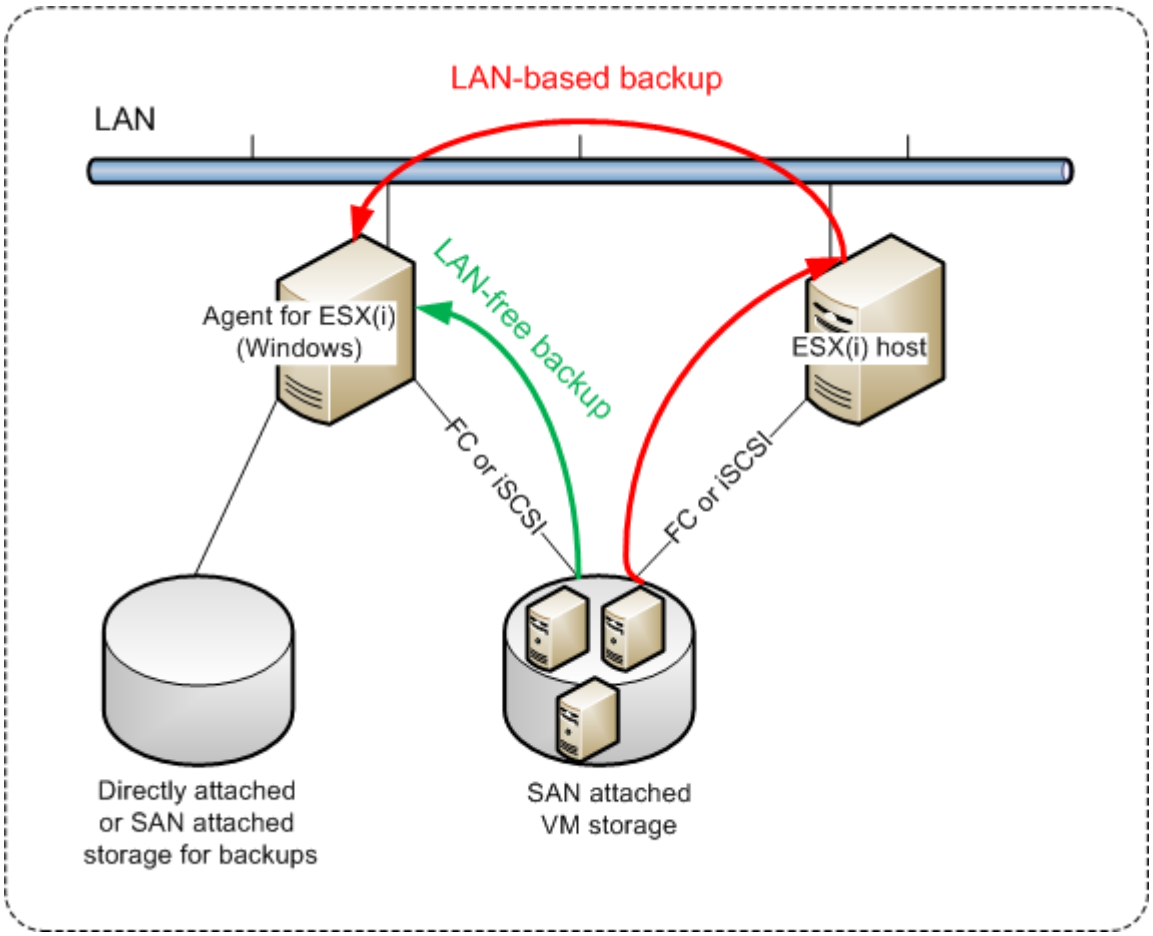
  This is the easiest method. It is recommended in most cases. Connect the console to the management server. In the **Navigation** tree, right click **Virtual machines**, and then click **Configure VMware vCenter integration**. Specify the vCenter Server, and then enable **Automatic deployment**. Any time 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.

Agent for ESX(i) (Windows)

If your production ESX(i) hosts are so heavily loaded that running the virtual appliances is not desirable, consider installing **Agent for ESX(i) (Windows)** on a physical machine outside the ESX infrastructure.

If your ESX(i) uses a SAN attached storage, install the agent on a machine connected to the same SAN. The agent will back up the virtual machines directly from the storage rather than via the ESX(i) host and LAN. This capability is called a LAN-free backup.

The diagram below illustrates a LAN-based and a LAN-free backup. LAN-free access to virtual machines is available if you have a fibre channel (FC) or iSCSI Storage Area Network. To completely eliminate transferring the backed up data via LAN, store the backups on a local disk of the agent's machine or on a SAN attached storage.



Agent for ESX(i) (Windows) can be installed on any machine that runs Windows and meets the system requirements. Follow the instructions described in the "Interactive installation in advanced editions" section.

During installation, specify the vCenter Server or ESX(i) Server whose virtual machines the agent will back up.

You will be able to set or change this setting at a later time. To access this setting after the agent has been installed, connect the console to the machine with the agent and select from the top menu **Options > Machine options > Agent for VMware vSphere ESX(i) (Windows)**.

Providing licenses

None of the installation methods results in consuming a license. The licenses will be required later. Once you configure the first backup of virtual machines, one license will be assigned to each ESX(i) Server that hosts a machine selected for backup.

If you have *n* ESX(i) servers, it is recommended that you purchase *n* Virtual Edition licenses and import them to the license server or to the management server before configuring the first backup. If you are planning to add more virtualization servers to your environment, upload a few more licenses in advance. This will ensure uninterrupted operation of your backup plans even if machines included in it migrate to a new server.

6.3 Operations with agents

This section explains how to deploy, update or remove Agent for ESX(i) (Virtual Appliance) using Acronis Backup & Recovery 11 Management Server.

6.3.1 Deploying Agent for ESX(i) (Virtual Appliance)

If your host or cluster 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 ESX(i)**.
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. 24) 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 ESX(i)**.

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

6.3.2 Updating Agent for ESX(i) (Virtual Appliance)

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

To update Agent for ESX(i)

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

When upgrading from Acronis Backup & Recovery 10 to Acronis Backup & Recovery 11, you must also specify the agent's host.

6.3.3 Removing Agent for ESX(i) (Virtual Appliance)

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

If other agents are connected to the same vCenter Server or ESX(i), 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 ESX(i)

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

6.4 Flexible configuration of the agents

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

The below distribution algorithm works for both virtual appliances and agents installed in Windows. 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.

However, when choosing an agent for a machine, the management server tries to optimize the overall system performance. In particular, the management server considers the agent and the virtual machine location. An agent hosted on the same host is preferred. If there is no agent on the same host, an agent from the same cluster is preferred.

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 cluster, 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 cluster. 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 ESX(i) binding**.

Manual binding

The **Agent for ESX(i) binding** (p. 20) 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. 19) section.

- **1 agent for entire vSphere** - Enable vCenter integration (disable automatic deployment of virtual appliances). Deploy an agent to the host you prefer or install an agent on a Windows machine. Connect the agent to vCenter Server.
- **1 agent per host or cluster** - 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 or cluster** - Enable vCenter integration (automatic deployment of virtual appliances may be enabled or disabled). Deploy the required number of agents to the

hosts you prefer and/or install the required number of agents on Windows machines. 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.

6.5 Using a locally attached storage

You can attach an additional disk to an Agent for ESX(i) (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 when a single virtual appliance manages the entire virtual environment residing in a SAN attached storage.

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 vSphere, and one or more of them use locally attached storages, you need to manually bind (p. 20) 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 ESX(i) (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.

6.6 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.

6.6.1 VMware vCenter integration

This option enables communication between Acronis Backup & Recovery 11 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 is available in all Acronis Backup & Recovery 11 advanced editions; a license for Virtual Edition is not required. No software installation is required on the vCenter Server.

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 & Recovery 11 in the vCenter Server inventory.
- Automatically deploy agents to the ESX(i) hosts managed by the vCenter Server.

  An agent is deployed in the background to each host or cluster whose virtual machines you include in a backup plan.

  Note. *Automatic deployment requires licenses for Acronis Backup & Recovery 11 Virtual Edition. Each host or cluster will take one license from the license server.*

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. 24) 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 ESX(i) (Virtual Appliance)** check box.
5. Click **OK**.

To enable automatic deployment of Agent for ESX(i) (Virtual Appliance)

1. Enable integration with the vCenter Server as described above.

2. Click **Automatic deployment**.
3. Select the **Automatically deploy Agent for ESX(i) (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. 24) 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 ESX(i) (Virtual Appliance)

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

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

6.6.2 Agent for ESX(i) binding

This option is effective if more than one Agent for ESX(i) serve the virtual machines of a vCenter Server.

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. 16).

The **Agent for ESX(i) 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 ESX(i) 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

- The option comes in handy if you want a particular (very large) machine to be backed up by Agent for ESX(i) (Windows) via a fibre channel while other machines are backed up by virtual appliances.
- It is necessary to use this option if one or more of the agents have locally attached storages (p. 18).
- Let's assume you want to back up 20 virtual machines using 3 Agents for ESX(i). 5 machines of 20 need to be backed up to Acronis Online Backup Storage.

  Allocate one of the agents for online backups and assign the subscription to this agent. Then, bind each of the 5 machines with this agent. The remaining 15 machines will be distributed among the 3 agents.

  As a result, you need only one subscription for the Acronis Backup & Recovery Online service. If the machines were distributed automatically, you would need to buy 3 subscriptions, one subscription per agent.

6.6.3 Agent for VMware vSphere ESX(i) (Windows)

This option is effective only for Windows machines on which Acronis Backup & Recovery 11 Agent for VMware vSphere ESX(i) (Windows) is installed. To access this option, connect the console to the machine and then select **Options > Machine options** from the top menu.

This option defines the vCenter Server or ESX(i) host whose virtual machines the agent will back up.

We recommend specifying the vCenter Server rather than an individual host so the agent can access any virtual machine managed by the vCenter Server.

If you have specified the server when installing the agent, this option is already configured. Otherwise, specify the name or IP address of the server and the credentials that the agent will use to connect to it.

Centralized backup and recovery tasks will run under this account by default. This means the account should have the necessary privileges (p. 24) 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.

6.7 Support for VM migration

This section informs what you can expect when migrating virtual machines within a datacenter using vCenter Server migration options. Performance considerations apply to both "hot" and "cold" migration.

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 is fully supported for both Agent for ESX(i) (Virtual Appliance) and the virtual machines being backed up by the agent. Migration of either the virtual appliance or a machine can take place during backup.

Storage VMotion

Storage VMotion moves a virtual machine disks from one datastore to another. Migration of Agent for ESX(i) (Virtual Appliance) with Storage VMotion is possible unless a backup or recovery is in progress. During migration, the agent postpones any backup that has to start. It starts the backup after the migration has been completed.

Migration of a virtual machine with Storage VMotion during backup is possible, but the backup may fail or succeed with warnings. The agent will not be able to delete the snapshot taken before migration because the machine is gone. To avoid this situation, do not migrate a virtual machine until its backup is completed.

Performance considerations

It is critical to understand that backup performance degrades when Agent for ESX(i) (Virtual Appliance) does not have direct access to the storage where the backed up disks are. In this case, the agent cannot attach the disks. Instead, it obtains data from these disks through LAN. This process is much slower than obtaining data from directly attached disks.

So the best practice is that Agent for ESX(i) (Virtual Appliance) be hosted on a host for which all shared storages of the cluster are accessible. In this case, backup performance remains optimal, wherever (within the shared storages) a virtual machine or the virtual appliance migrates. Once a machine migrates to a local storage of a different host, its backups will run slower.

6.8 Backing up fault tolerant machines

VMware vSphere does not support snapshots of virtual machines with the VMware Fault Tolerance feature enabled. Therefore, Agent for ESX(i) does not back up these machines 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; otherwise, a snapshot will not be created. 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 & Recovery 11 Virtual Edition license 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.

6.9 Backing up independent disks and RDMs

VMware vSphere does not provide snapshots of independent disks or of Raw Device Mapping (RDM) disks in physical compatibility mode. Therefore, Agent for ESX(i) cannot back up such disks when the virtual machine is online or suspended. 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.

When a virtual machine is offline (powered off), Agent for ESX(i) can access the independent disks and RDMs in physical compatibility mode via ESX(i). Then, the agent can copy the information from them in a consistent state. As a result, the agent is able to back up all of the disks regardless of their mode.

The following table shows the role which the state of a virtual machine plays on whether Agent for ESX(i) can back up a disk.

VM disk modes	ESX(i) 3 machine state			ESX(i) 4 machine state		
	Online	Suspended	Offline	Online	Suspended	Offline
Basic virtual	+	+	+	+	+	+
Independent persistent	–	–	+	–	–	+
Independent nonpersistent	–	–	+	–	–	+
RDM in physical compatibility mode	–	–	+	–	–	+
RDM in virtual compatibility mode (basic virtual)	+	+	+	+	+	+
RDM in virtual compatibility mode (independent persistent)	–	–	+	–	–	+
RDM in virtual compatibility mode (independent nonpersistent)	–	–	+	–	–	+

If you want to always back up independent disks and RDMs in physical compatibility mode, do one of the following:

- **If, according to your business process, a machine with such disks goes offline regularly, schedule its backup for these hours.**

  Please make sure that the backup is completed within the "offline" hours. VMware vSphere will not be able to power on the machine while the backup is in progress. This is because the independent disks and RDMs in physical compatibility mode are locked by Agent for ESX(i) during backup.

- **Install Agent for Windows or Agent for Linux in the guest operating system.**

  An Acronis Backup & Recovery 11 Virtual Edition license 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.

6.10 Privileges for VM backup and recovery

Once Agent for ESX(i) is deployed to a vCenter's host or cluster, 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/ESXi 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/ESXi 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/ESXi 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. In addition, the **Global** > **Licenses** privilege is required to be able to back up virtual machines of a specific ESX 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					+
	Low level file operations					+
Global	**Licenses**	+ (required on ESX host only)	+ (required on ESX host only)	+	+	

Network	**Assign network**			+	+	+
Resource	**Assign VM to resource pool**			+	+	+
Virtual machine > Configuration	**Add existing disk**	+	+	+		
	Add new disk			+	+	+
	Add or remove device			+		+
	Change CPU count			+		
	Memory			+		
	Remove disk	+	+	+	+	
	Rename			+		
	Settings				+	
Virtual machine > Interaction	**Configure CD media**			+		
	Console interaction					+
	Power off				+	+
	Power on			+	+	+
Virtual machine > Inventory	**Create from existing**			+	+	
	Create new			+	+	+
	Remove			+	+	+
Virtual machine > Provisioning	**Allow disk access**			+	+	
Virtual machine > State	**Create snapshot**	+	+		+	+
	Remove snapshot	+	+		+	+

Privileges for a folder

To enable a user to operate within a specific vCenter folder, assign the user the following privileges on the folder.

		Operation		
Object	**Privilege**	**Back up a VM**	**Back up a VM's disk**	**Recover to an existing VM**
Datastore	**Allocate space**			+
Global	**Licenses**	+	+	+
Network	**Assign network**			+
Resource	**Assign VM to resource pool**			+
Virtual machine > Configuration	**Add existing disk**	+	+	
	Add new disk			+
	Remove disk	+	+	+
	Settings			+
Virtual machine > Interaction	**Power off**			+
	Power on			+
Virtual machine > Inventory	**Create from existing**			+
	Create new			+
	Remove			+
Virtual machine > Provisioning	**Allow disk access**			+
Virtual machine > State	**Create snapshot**	+	+	+
	Remove snapshot	+	+	+

7 Working in Microsoft Hyper-V

7.1 Getting started with Agent for Hyper-V

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

7.1.1 Prerequisites

Make sure that:

- You have a machine running Windows 2008/2008 R2 (x64) with Hyper-V.
- You installed Hyper-V Integration Services in the guest operating systems.
- You have one or more licenses for Acronis Backup & Recovery 11 Virtual Edition. 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. You can purchase full license keys or obtain trial license keys.
- 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 & Recovery 11.

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.

7.1.2 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 & Recovery 11**. 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 & Recovery 11 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 & Recovery 11**. Accept the terms of the license agreement.
3. Select the **Back up this machine's data** check box.
4. Click **Take license keys from license server**. In **IP/name**, specify the name or IP address of the machine where you installed the management server.

   Details. The license server is integrated with the management server.
5. Make sure that the check box with the license is selected, and then click **Next**.
6. 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.
7. 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.
8. Specify whether the Hyper-V host will participate in the Acronis Customer Experience Program (CEP).
9. Click **Install**.

7.1.3 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 & Recovery 11** 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.

7.1.4 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 **Create backup plan**.
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.

7.2 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.

7.3 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 & Recovery 11 Virtual Edition license 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.

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. 33) 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.

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.

9.1 Simultaneous VM backup

This option is effective when backing up virtual machines with Agent for VMware vSphere ESX(i) or Agent for Hyper-V.

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 ESX(i) (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.

If the backup speed is still insufficient, consider installing Agent for ESX(i) (Windows) (p. 13) on a separate physical machine. The agent can share the load with the virtual appliances or undertake backup of all the machines.

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.