Acronis

# Acronis® vmProtect® 9

## User Guide

## Copyright Statement

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Third party code may be provided with the Software and/or Service. The license terms for such third-parties are detailed in the license.txt file located in the root installation directory. You can always find the latest up-to-date list of the third party code and the associated license terms used with the Software and/or Service at http://kb.acronis.com/content/7696

## Acronis patented technologies

Technologies used in this product are covered by the following patents: U.S. Patent # 7,047,380; U.S. Patent # 7,246,211; U.S. Patent # 7,318,135; U.S. Patent # 7,366,859; U.S. Patent # 7,636,824; U.S. Patent # 7,831,789; U.S. Patent # 7,886,120; U.S. Patent # 7,934,064; U.S. Patent # 7,949,635; U.S. Patent # 7,979,690; U.S. Patent # 8,069,320; U.S. Patent # 8,073,815; U.S. Patent # 8,074,035.

# Table of contents

# 1 Introducing Acronis vmProtect 9

Acronis believes that virtualization and transition to the cloud are not only a better way of doing computing, but also allow for achieving less downtimes and faster recoveries while reducing costs. Unfortunately, most of backup and recovery solutions are designed for physical systems and are either not good enough for virtual environments or do not allow for all of the benefits and savings that virtualization could potentially give.

Acronis is firmly committed to helping its customers and channel partners get most of virtualization, and intend to set a new standard of backup and recovery in virtualized environments through:

- Reducing IT operating and maintenance costs to help business performance by providing technology that is easy to use and easy to implement.
- Minimizing overhead and getting most benefits from VMware vSphere environments by providing a backup and recovery solution specially designed for virtualized environments.
- Minimize risk of data loss by storing backups offsite in Acronis Cloud Storage.

# 2 Acronis vmProtect 9 Overview

Acronis vmProtect 9 is a comprehensive backup and recovery solution designed for VMware vSphere™ environments. It enables organizations to perform an agent-less backup of entire ESX(i) virtual machines with the ability to recover entire machines or individual files and folders.

## 2.1 Acronis vmProtect 9 Features

Using Acronis award-winning imaging technology, Acronis vmProtect 9 creates an exact image (backup) of the virtual machine, including guest operating system, configuration files and applications, resource pool/vApp properties and datastore settings. It then provides you with the ability to recover this backup to either the original ESX(i) host or to a new one. The ability to start a virtual machine directly from a backup without performing an actual restore, making the VM operational in a few seconds after a failure, is one of the key new features.

Other new features include:

- An option to choose between virtual appliance or Windows-based installation.
- Web-based easy-to-use user interface.
- LAN-free backup with direct access to shared storage.
- Instantly run a VM from a backup on an existing ESX(i) host for quick recovery.
- New enhanced always incremental storage format for backups.
- Simultaneously back up several virtual machines.
- Support for vApp/resource pool settings backup/restore.
- Change Block Tracking (CBT) support.
- Disaster Recovery Plan.
- Centralized Dashboard.

Main advantages of using Acronis vmProtect 9 are:

1. **Ease-of-use.** Acronis vmProtect 9 can be deployed either as virtual appliance or installed on a Windows machine and is managed via brand new web-based interface. Given Acronis experience in designing intuitive GUIs and focused target on VMware – the interface allows starting right away without a need to investigate or read documentation, and avoids dangerous mistakes or misconfiguration.
2. **More functionality.** In addition to standard backup and restore features, vmProtect 9 includes unique functionality, such as: running virtual machine directly from backup; unlimited number of P2V conversions; backup to cloud-based Acronis Cloud Storage; industry-standard 256-bit encryption to protect backups.
3. **Low Total Cost of Ownership (TCO).** vmProtect 9 is priced per CPU, and a list prices are quite low. Virtual Appliance does not require a dedicated machine or Windows license to operate, plus a reliable and intuitive solution saves administrator's time and management cost.
4. **Safe investments by working with established vendor.**

# 3 How Acronis vmProtect 9 Works

## 3.1 Virtual machines backup and restore

As with a physical machine, your virtual machine (or several VMs as a whole virtual infrastructure) should also be protected. Once you have installed Acronis vmProtect 9 agent, you can:

- Back up a virtual machine or multiple virtual machines residing on the server without having to install additional software on each virtual machine.
- Recover a virtual machine to the same or another virtual machine residing on the same server or on another virtualization server. The virtual machine configuration stored in a virtual machine backup and the virtual disks data will be restored to a new virtual machine.

A virtual machine can be online (running), offline (stopped), suspended, or switched between the three states during backup.

A virtual machine has to be offline (stopped) during the recovery to this machine. The machine will be automatically stopped before recovery. You can opt for manual stopping of machines.

The detailed information can be found in the “Creating a backup of virtual machines” (p. 30) and “Restoring a backup of virtual machines” sections (p. 54).

## 3.2 Backup archive structure

Acronis vmProtect 9 allows you to create the backup of virtual machines by using one of the two backup archive schemes: Multiple files backup scheme (Legacy mode) or Single file backup scheme (Always Incremental mode).

In Acronis vmProtect 9, the Single file backup scheme is set as the default.

### 3.2.1 Multiple files backup scheme (Legacy mode)

With this scheme, the data for each backup is stored in a separate archive file (.tib extension). A full backup is created at the first launch. The following backups are performed according to the incremental method.

Set up the backup retention rules and specify the appropriate settings. The outdated backups, i.e. backups older than the designated number of days (defined by the retention rules) are deleted dynamically in compliance with the following procedure:

Note that it is not possible to delete a backup which has dependencies. For example, if you have a full backup plus a set of incremental backups, you cannot simply delete the full backup. If you do, the incremental backups will not be recoverable. The backups which become subject to deletion (according to the retention rules) will not be deleted until all the dependent backups also become deletable. This limitation can be overcome by utilizing the Always Incremental backup mode.

### 3.2.2 Single file backup scheme (Always Incremental mode)

Usually, backups are kept only for a certain time period (retention time) or there is a policy to keep only the last X backups in the backup chain. Backup archives are managed on a daily, weekly, etc. basis. The main limitation of the Legacy mode backup archive is that you cannot delete a random backup from the backup chain since it may have dependencies on it from subsequent backups. This is where Always Incremental backup archive can help.

Always Incremental mode uses a new generation archive format which may contain several backups from a number of virtual machines. After the first full backup, all other backups are saved to this archive in incremental mode. Physically all data is located inside one file as opposed to the Legacy archive format where each backup is stored in a separate .tib file. Therefore, unlike the Legacy mode archive, it is possible to delete a random backup from Always Incremental archive even if it has dependencies.

When a certain backup expires due to the pre-defined retention rules (for example to “delete the backups if they are older than 2 days”), the backup algorithm just marks these outdated backup blocks as “free” ones.

The blocks of expired backups with dependencies (which are needed to restore the newer backups) are not marked as “free” to ensure the archive consistency. Everyday, the archive should contain data that is not older than two days in order to restore the backup (retention time). This is the basic rule of the Always Incremental archive. All excessive data in the archive is marked for deletion, i.e. as “free” space. The initial archive still occupies the same space on the storage as before, however all newer backups will be written to the “free” blocks first, and only if all the “free” blocks are filled, the total size of the archive will be increased.

This approach allows keeping the archive size as small as possible and prevents it from excessive growing. Also, the implementation of this backup scheme significantly saves time and resources for managing the backups inside the archive because the “free” blocks marking is almost an instant operation. Thus, the limitations of the Legacy archive mode are no longer true for Always Incremental archive.

The Always Incremental archive total size includes the size of the “used” blocks and the size of the “free” blocks. Usually, the size of the Always Incremental archive does not grow indefinitely and stays within the total size of the backups you want to keep.

# 4 Installation of Acronis vmProtect 9

## 4.1 Requirements

### 4.1.1 Supported operating systems

Acronis vmProtect 9 supports the following operating systems:

- Windows XP Professional SP2 (x64), SP3 (x86).
- Windows Server 2003/2003 R2 - the Standard, Enterprise, Small Business Server editions (x86, x64).
- Windows Vista - all editions (x86, x64).
- Windows 7 - all editions (x86, x64).
- Windows 8.
- Windows Server 2008 - the Standard, Enterprise, Foundation editions (x86, x64).
- Windows Small Business Server 2008.
- Windows Server 2008 R2 - the Standard, Enterprise, Datacenter, Foundation editions.
- Windows Small Business Server 2011.
- Windows Server 2012.

### 4.1.2 System requirements

The components installed in Windows:

| Edition name | Memory (above the OS and running applications) | Disk space required during installation or update | Disk space occupied by the component(s) |
|---|---|---|---|
| vmProtect 9 | 80 MB | 1 GB | 500 MB |

To perform each task (Backup, Restore, RunVM, Validate, etc.) the Agent needs about 100Mb of memory. Acronis vmProtect 9 could perform parallel tasks (such as parallel backup tasks, etc) of up to 5 tasks at a time. If more than 5 tasks are run simultaneously, the Agent will process only the first 5 tasks, while the other tasks will remain in the queue with the “waiting” status.

Also, note that Acronis vmProtect 9 reserves and always uses the following system TCP ports: 111 (sunrpc), 9000 (WCS), 764 (nfs_server), 9876 (Remote Agent Service), and UDP port: 2049 (nfs).

Here is a list of supported environments for Acronis vmProtect 9:

- VMware vSphere (Virtual Infrastructure).
- Server types: ESX and ESXi.
- Versions: 4.0*, 4.1, 5.0, 5.1.
- Editions/Licenses.
  - VMware vSphere Standard (Hot-add backup mode is supported on vSphere 5.0+ only).
  - VMware vSphere Advanced.
  - VMware vSphere Enterprise.
  - VMware vSphere Enterprise Plus.

- VMware vSphere Essentials (Hot-add backup mode is supported on vSphere 5.0+ only).
- VMware vSphere Essentials Plus (Hot-add backup mode is supported on vSphere 5.0+ only).

VMware vSphere Hypervisor (Free ESXi) is NOT supported.

(*) ESX(i) version 4.0 environment is supported with exceptions, for example, Exchange Server Backup Extraction (p. 63) and ESXi configuration backup (p. 75) features are not supported.

Supported versions of Microsoft Exchange: MS Exchange Server 2003 SP2+, MS Exchange Server 2007, MS Exchange Server 2010, MS Exchange Server 2013 (backup and restore of databases ONLY). Extracting MS Exchange databases located on Windows dynamic disks (LDM) is NOT supported.

Supported versions of Microsoft SQL: MS SQL Server 2005, MS SQL Server 2008, MS SQL Server 2012.

Supported versions of Microsoft SharePoint: MS Windows SharePoint Services 3.0 SP2, MS Office SharePoint Server 2007 SP2, MS SharePoint Foundation 2010 SP1, MS SharePoint Server 2010 SP1, MS SharePoint 2013 Technical Preview.

Acronis vmProtect 9 supports the following file systems for the backed up virtual machines: NTFS/FAT16/FAT32/ext2/ext3/ext4/ReFS. For other VM file systems sector level backup mode is used, which means that granular recovery from such archives is not possible (only entire VMs can be restored). An example of unsupported file systems are Linux LVM volumes (or Windows Dynamic Disks). They are backed up in sector-by-sector mode.

Please, note, that the following environments for the backup/restore operations are NOT supported:

- RDM disks (Raw Device Mapping).
- Fault tolerance VMs.

Also, independent virtual drives CANNOT be backed up when the virtual machine is turned on. Please, power off such VMs before their back up.

For the smooth operation of the Acronis vmProtect 9 Web Console, you should have one of the following versions of your web browser:

- Mozilla Firefox 3.6 or higher.
- Internet Explorer 7.0 or higher.
- Opera 10.0 or higher.
- Safari 5.0 or higher.
- Google Chrome 10.0 or higher.

For proper Web Console operation with IE 8, please, check your internet settings. **Tools** -> **Internet Options** -> **Security** tab -> **Internet** -> **Security level** shoud not be set to “High”. Level of privacy at the **Privacy** tab should be set to “Medium High” or lower.

For proper Web Console operation with IE 9, please, check your internet settings. **Tools** -> **Internet Options** -> **Advanced** -> **“Do not save encrypted pages to disk”** option must be cleared. Otherwise the **File Recovery** feature will not function properly.

## 4.1.3 How to install VMware Tools

Acronis vmProtect 9 requires the installation of VMware Tools inside the virtual machines that you plan to back up. This is necessary to support proper quiescence of the file system (utilize VSS support) and to enable files/folders exclusions capability. To install the VMware Tools:

- Run the VMware Infrastructure/vSphere Client.
- Connect to the ESX(i) server.
- Select the virtual machine and run the guest operating system.
- Right click the virtual machine and select **Guest** -> **Install/Upgrade VMware Tools**.
- Follow the onscreen instructions.

Note that the **Run VM from backup** feature requires VMkernel networking to be configured on the ESX(i) server. This can be done in vSphere client by going to **Configuration** -> **Networking** and adding VMkernel connection type to the vSwitch properties.

## 4.1.4 Privileges for VM backup and recovery

Once Acronis vmProtect 9 Agent is installed on a Windows machine or deployed to an ESX(i) host, the first thing you do is the configuration of ESX(i) hosts/vCenter which will be managed by this Agent. The scope of available operations depends on the privileges a user (that you have specified while adding a ESX(i) host/vCenter in vmProtect 9 Agent web console: **Configure** -> **ESX(i) Hosts**) 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(i) virtual machines and, additionally, for virtual appliance deployment.

### Privileges on vCenter Server or ESX(i) host

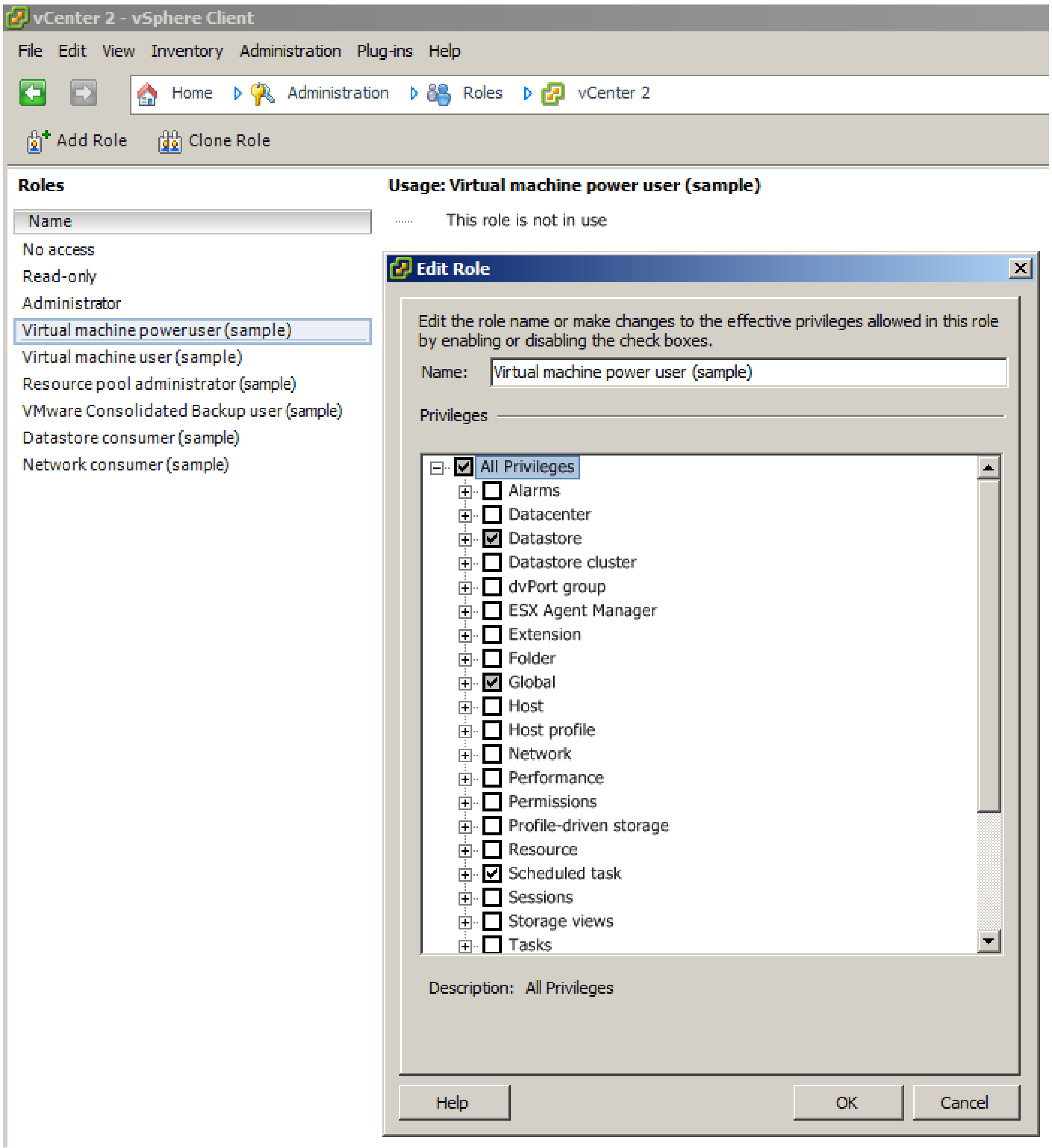
Outlined in the below table are the privileges a vCenter Server user must have to perform operations on all the vCenter hosts and clusters.

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

The roles privileges can be configured via the vSphere Client connected to a ESX(i) host/vCenter from **Administration** -> **Roles**. After that you can assign the specific user for connection to vCenter with particular role from **Permissions** tab, as shown in the pictures below.



vCenter 2 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home ▷ Administration ▷ Roles ▷ vCenter 2
Add Role
Clone Role

**Roles**

Name
- No access
- Read-only
- Administrator
- Virtual machine power user (sample)
- Virtual machine user (sample)
- Resource pool administrator (sample)
- VMware Consolidated Backup user (sample)
- Datastore consumer (sample)
- Network consumer (sample)

**Usage: Virtual machine power user (sample)**

This role is not in use

**Edit Role**

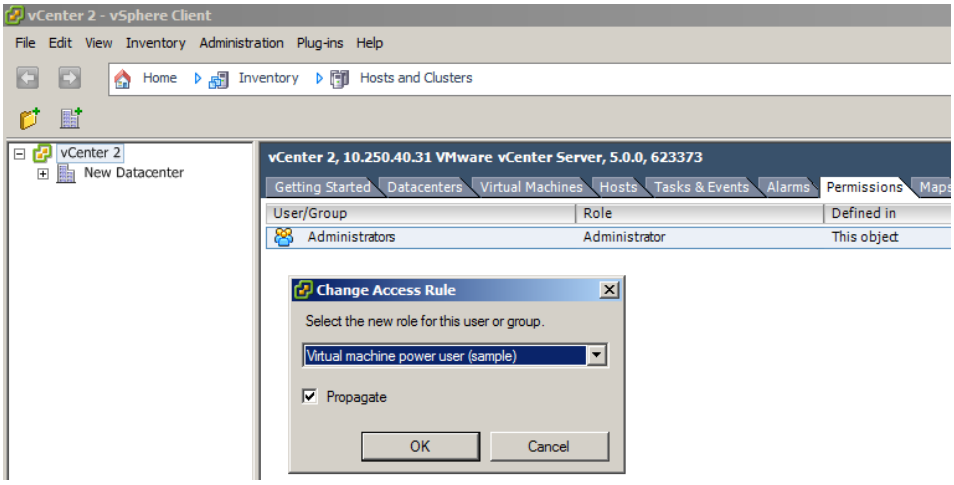
Edit the role name or make changes to the effective privileges allowed in this role by enabling or disabling the check boxes.

Name: Virtual machine power user (sample)

Privileges

- ☑ All Privileges
  - □ Alarms
  - □ Datacenter
  - ☑ Datastore
  - □ Datastore cluster
  - □ dvPort group
  - □ ESX Agent Manager
  - □ Extension
  - □ Folder
  - ☑ Global
  - □ Host
  - □ Host profile
  - □ Network
  - □ Performance
  - □ Permissions
  - □ Profile-driven storage
  - □ Resource
  - ☑ Scheduled task
  - □ Sessions
  - □ Storage views
  - □ Tasks

Description: All Privileges



vCenter 2 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home ▷ Inventory ▷ Hosts and Clusters
vCenter 2
New Datacenter
Getting Started
Datacenters
Virtual Machines
Hosts
Tasks & Events
Alarms
Permissions
Maps

vCenter 2, 10.250.40.31 VMware vCenter Server, 5.0.0, 623373

| User/Group | Role | Defined in |
|---|---|---|
| Administrators | Administrator | This object |

**Change Access Rule**

Select the new role for this user or group.

Virtual machine power user (sample)

☑ Propagate

## 4.2 Installation options

The very first thing you have to do is to install Acronis vmProtect 9 software, configure your ESX(i) host connection settings and set up your access credentials to Acronis vmProtect 9 web console.

When you run your Acronis vmProtect 9 installation package, the installation menu appears. Acronis vmProtect 9 has three main installation options:

- **Install Acronis vmProtect 9 as Virtual Appliance on an ESX(i) host**.
- **Install Acronis vmProtect 9 as Windows Agent**.
- **Extract installation files**.

**The first option** allows you to install the software on a remote ESX(i) host (see Installing Acronis vmProtect 9 as Virtual Appliance on an ESX(i) Host (p. 17)).

**The second option** allows you to install Acronis vmProtect 9 software on your local PC (see Installing Acronis vmProtect 9 as Windows Agent (p. 18)).

**The third option** allows you to extract the installation files (see Extracting installation files (p. 20)) and perform either Acronis vmProtect 9 remote deployment or local installation manually with the help of standard installation tools. You can always choose this option, if you would need to manage or troubleshoot your Virtual Appliance / Windows Agent installation without the default installer, or if you would need to install only a certain component without carrying out the full installation procedure.

There are several reasons why Acronis vmProtect 9 Virtual Appliance deployment to an ESX(i) host is preferable over Acronis vmProtect 9 Windows Agent installation. These reasons are:

1. Your backups will be LAN-free without additional setup effort (you don't have to connect the FC/iSCSI storage to the Windows machine where you run the Agent).
2. The hotadd method used by Virtual Appliance (attaching virtual drives to Virtual Appliance during backup) is usually fastest possible to get access to the VM data for reading.
3. Virtual Appliance is free from possible software compatibility issues (such as 3rd party NFS servers or other services which may block the ports).
4. It is easier to maintain Virtual Appliance and you don't have to have a dedicated Windows machine for it. Surely it is a better choice if your infrastructure is fully virtualized.
5. Virtual Appliance is easier and faster to install.

The disadvantage of Virtual Appliance is that the backup will consume CPU and memory resources from the ESX(i) host, which may be a problem for highly loaded environments. In this case, if you have a physical computer available to be used as a console for managing all vmProtect 9 functionality, you can choose to install the vmProtect 9 Windows Agent locally.

### 4.2.1 Installing Acronis vmProtect 9 as Virtual Appliance on an ESX(i) host

Acronis vmProtect 9 software could be installed directly on an ESX(i) host. The process of remote installation of Acronis vmProtect 9 Virtual Appliance to an ESX(i) host is called deployment. The software for running all necessary Acronis services will be installed on a separate small virtual machine under a specially customized OS (small Linux distribution).

1. First, read the Acronis vmProtect 9 license agreement, select the acceptance check box and then click **Next**.
2. Specify the desired ESX(i) server or vCenter access credentials: IP address or hostname, your user name and access password. When you click **Next**, the installer will automatically check the connection and go through the authorization procedure.
3. Then the installer will check for previous versions of Acronis vmProtect 9 or any other Acronis software on the specified ESX(i) server. If you already have the Acronis Virtual Appliance set up there and it is outdated, then the installer would prompt you to update it to the latest version or create the new Virtual Appliance.
4. Set your Appliance (VM) name, choose the ESX(i) host and datastore as a target for deploying the Acronis vmProtect 9 software. You can change the Appliance name or keep the default one. The Appliance name should be unique within the ESX(i) host. If you set the vCenter and its credentials on the previous installation step, you have to choose one of the ESX(i) hosts contained in that vCenter from the respective drop-down list. Otherwise, there will be no choice and you will see your direct ESX(i) host.

   Then, select the datastore on that specific ESX(i). If the space on that datastore is not enough for installation, you will get the warning suggesting that you free up some space on the selected datastore or choose another one. There can be only one unique Virtual Appliance with the specified name on the specified datastore. If the Appliance name already exists there, you will have to change either your Appliance name or the datastore.

   If you specify the vCenter on this step, you can select to **Enable vCenter integration** with the respective check box.

   You can optionally select the **Automatically start up the Virtual Appliance after ESXi host reboot** check box.
5. Provide the information on the network settings for your Virtual Appliance. This step contains standard network settings like IP address, subnet mask, default gateway, DNS server settings, etc. You can also let the appliance acquire the network settings automatically, which is the default option.
6. The next step prompts you to accept or ignore your participation in the Acronis Customer Experience Program.
7. After going through all the required steps of the installation wizard, you will finally see the summary information of the deployment operations to be performed – components to be installed, required space, account information and chosen destination (host and datastore).

   Then the Acronis vmProtect 9 installer deploys the Virtual Appliance software. You will see the progress bar with the current installation step indicated. After the deployment is finished successfully, the appliance is started automatically. Please, wait until the whole process is completed and everything is checked. This may take several minutes.

If the installation process finished successfully and all Acronis vmProtect 9 components were successfully deployed, you will get the “Deployment has been completed” page. Here, select the check box if you wish to run the Acronis vmProtect 9 Web Console (it will be opened in the default

Internet browser) to connect to your newly deployed Acronis vmProtect 9 Virtual Appliance. Then click **Close**. The default login:password for the Acronis vmProtect 9 Web Console is admin:root. NOTE: it is highly recommended to change the password after first login at **Configure** -> **Agent Password** page (for more information refer to Managing Agent Password section (p. 105)). With default credentials the login is performed automatically. If you've changed the Agent Password configuration, then you'll get the default login screen upon connection to the Web Console.

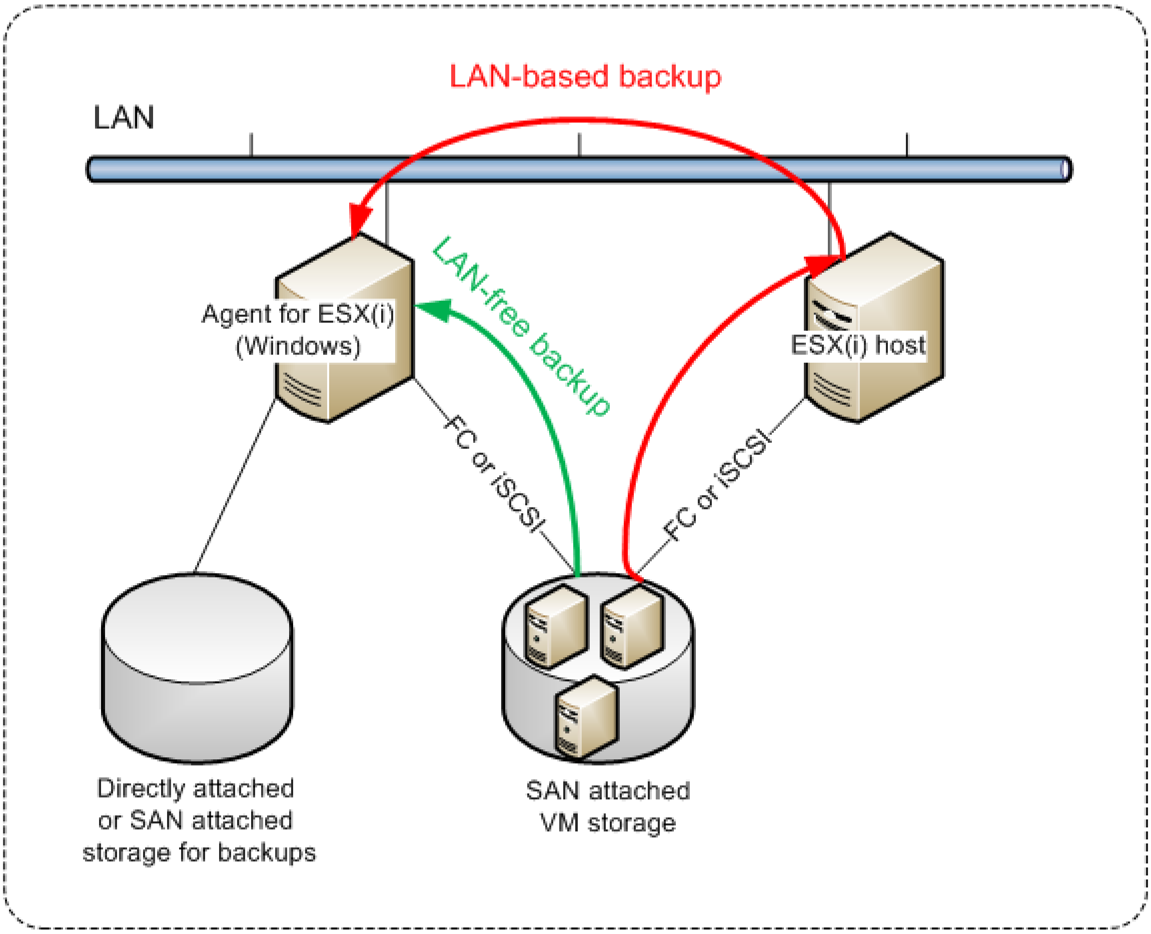
If there is any problem, the Virtual Appliance (parts of it which have already been deployed during the installation) will be removed from ESX(i) automatically. You will get the "**Failed to install vmProtect 9 components**" page. Here, you can see the summary information on the installed and failed to install components. **Show log** link opens up a pop-up with the detailed information, and **Troubleshoot** link opens the online page with the particular error description on the Acronis Knowledge Base website at http://kb.acronis.com. If you still cannot find the answer on how to solve this problem, please, contact the Acronis support team (p. 110).

### 4.2.2 Installing Acronis vmProtect 9 as Windows Agent

If your production ESX(i) hosts are so heavily loaded that running the virtual appliances is not desirable, consider installing Acronis vmProtect 9 Windows Agent on a physical machine outside the ESX(i) 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.



Acronis vmProtect 9 Windows Agent can be installed on any machine that runs Windows and meets the system requirements. Here is a brief description of the steps you need to go through in order to complete your Windows Agent installation.

1. First, read the Acronis vmProtect 9 license agreement, select the acceptance check box and then click **Next**.
2. Specify credentials for the Acronis services. The Acronis Managed Machine Service component (responsible for the core functionality of Acronis vmProtect 9) runs as a service. Specify the account under which the component's service will run after the installation (this account will be automatically granted with “Log on as service” permissions on the machine). Here you should provide the credentials of any Windows user which has “**Log on locally**” permissions on the machine with the Agent installed. Typically, this can be any user account from “**Administrators**”, “**Power Users**” or “**Users**” group. Set the HTTPs port, e.g. the default 9877 port. For access to Acronis web console page after Acronis vmProtect 9 Agent is installed, open your web browser and enter “https://myserver:port” in the browser address bar.

   **Note that in order to successfully connect to your installed Agent through the browser (web console), the name of your local PC where Acronis vmProtect 9 is installed should not contain an underscore (_) symbol. You should provide the credentials of any user with Administrator privileges on the machine.**

3. Select the way you want your components to be installed, i.e. specify the location where to install the software. The default destination for installing Acronis vmProtect 9 is the C:\Program Files\Acronis or C:\Program Files (x86)\Acronis folder. You can change the destination by typing in a new folder name or selecting it by browsing. If the folder does not exist, it will be automatically created in the process of installation. The **Disk usage** button shows the available disk space for the different volumes on your PC and helps you to choose the target disk for installation. If there is not enough free space on the selected volume, you'll be prompted to free up the required space or select another volume. Upon specifying the desired destination, click **Next.**
4. Please, read the information about the Acronis Customer Experience Program, choose if you want to participate in it or not, and then click **Next**. The main purpose of ACEP is to help us collect user statistics in order to improve our software functionality, customer service and customer experience.
5. After going through all the required installation wizard steps, you will finally see the summary information of the install operations to be performed, components to be installed, required space, account information and chosen destination.
6. Click **Install** to start the process. You will see the Acronis vmProtect 9 installation progress bar. During installation, Windows Firewall may prompt you to unblock TCP/IP ports. This is required for the appliance to operate properly. To unblock, in the opened Windows Firewall dialog box click the **Unblock** button. Please, wait until the installation is finished. It may take several minutes.

If the installation process finished successfully and all Acronis vmProtect 9 components were successfully installed, you will get the "Installation has completed" page. Here select the check box if you wish to run Acronis vmProtect 9 Web Console and click **Close**.

If the installation process fails and all or some of the Acronis vmProtect 9 components for any reason could not be successfully installed, you will get the "Failed to install vmProtect 9 components" page. Here you can see the summary information on the installed and failed to install components. **Show log** link opens up a pop-up window with the detailed information, and **Troubleshoot** link opens the online page with the particular error description on the Acronis Knowledge Base website at http://kb.acronis.com. If you still cannot find the answer how to solve this problem, please contact the Acronis support team (p. 110).

## 4.2.3 Extracting installation files

Acronis vmProtect 9 installation package provides you with the option to extract the installation files on your PC to be executed manually and to be installed by the standard tools.

Click the **Extract installation files** of the Acronis vmProtect 9 installation main menu. Select the desired components to be saved as separate installation files on your PC:

- AcronisESXAppliance.ovf and two .vmdk files – installation files for Acronis Virtual Appliance.
- vmProtectAgent.msi – the main installation file for Acronis vmProtect 9 Windows Agent.
- vmProtectExchangeBackupAgent.msi – installation file for Acronis vmProtect 9 Exchange Backup Agent. This Agent might be installed inside the guest OS where User Account Control (UAC) is enabled. It is meant to overcome the UAC limitations to allow the vmProtect 9 Exchange Backup options. Upon installation the **Acronis vmProtect 9 Exchange Backup Agent** service provides the communication channel with Acronis vmProtect 9 Agent.

Specify the location you want to extract your files to, and then click **Extract**. The **Disk usage** button shows the available space for the different volumes on your PC and helps you to choose the destination disk for the files extraction.

Close the dialog when the extraction process is completed.

### 4.2.4 Configuring ESX(i) host connection settings

For detailed information on setting and configuring your ESX(i) host connection credentials, please refer to Managing ESX(i) hosts (p. 99) section.

### 4.2.5 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.

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. The maximum supported locally attached storage size is 2TB.

   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 task expand the **Local Folders** item and choose the locally attached storage drive, for example D:\.

The same procedure applies to File recovery and other operations with the backups.

## 4.3 Uninstalling Acronis vmProtect 9

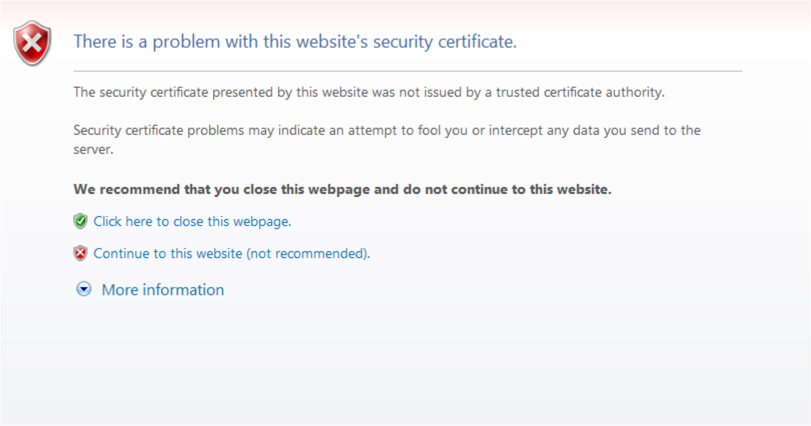
To uninstall Acronis vmProtect 9 Windows Agent, use the default **Add or Remove Programs** tool of Windows.

To uninstall Acronis vmProtect 9 Virtual Appliance, you have to manually remove the VM with the virtual appliance from the ESX(i) host with your VMware vSphere client.

# 5 Getting started

Once you installed the Acronis vmProtect 9 or deployed your Acronis vmProtect 9 Virtual Appliance, you can run the Acronis vmProtect 9 Web Console. The Web Console will be opened in the default Internet browser.

Note that the Acronis vmProtect 9 web server (installed on the Agent side) which provides the user interface uses self-signed certificates. As a result, you may receive the “There is a problem with this website’s security certificate” error message when connecting to Acronis Agent via your Internet Browser. To avoid this message, you should add this self-signed certificate to the list of trusted certificates. The exact instructions depend on the type of Internet browser you are using. You can refer to your browser’s help for further information.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

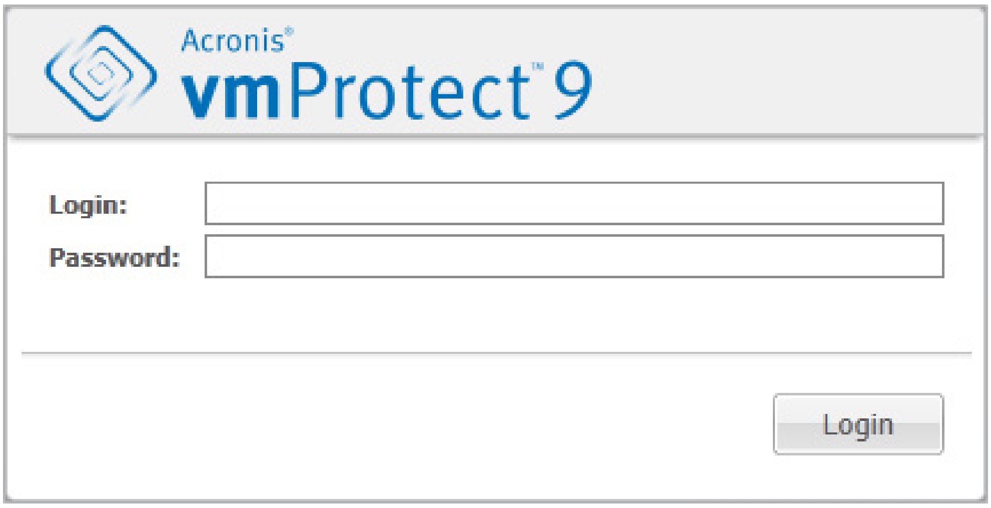
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

**We recommend that you close this webpage and do not continue to this website.**

Click here to close this webpage.
Continue to this website (not recommended).
More information

Certificate error message

Once the Web Console opens in the Internet browser, you will get a login screen where you need to provide user credentials for Acronis vmProtect 9. In case of Virtual Appliance-based installation, the default login:password is **admin:root**. In case of Windows Agent-based installation, you should provide the credentials of any Windows user who has “**Administrator**” privileges on the machine with the Agent installed. The user should also be granted with “**Log on locally**”, “**Access this computer from the network**” and “**Log on as a batch job**” privileges. These privileges can be checked from **Start** -> **Run** -> **secpolmsc** -> **Security Settings** -> **Local Policies** -> **User Rights Assignment**.



Login page

After logging in the Acronis vmProtect 9 you will see a welcome screen with the Dashbord's Quick Start. The three buttons of this section will give you a hint of what to start with:

- First of all, to be able to perform the first backup task of a Virtual Machines, you have to go to the ESX(i) Host section (p. 99) and specify the IP address / hostname and credentials for the vCenter or individual ESX(i) host where these machines are running.
- Setting up an ESX(i) host will not bind the licenses to it automatically. Therefore, you have to follow to the Licenses page (p. 96) to set up your licenses.
- After setting up your ESX(i) hosts and licenses, you can run the New backup task wizard (p. 30), which will guide you through all the steps of the backup process.

## 5.1 Dashboard Management

After installing and running Acronis vmProtect 9 (i.e. connecting to Acronis vmProtect 9 component via web-based console), the default dashboard screen appears. Initially the dashboard contains 2 sections: the **Quick Start** section and the **Virtual Machines** section, which presents general information about your vCenter, ESX(i) hosts, the number of machines managed on the ESX(i) hosts and the number of mounted virtual machines. The **Dashboard** view will be changed from the initial (**Quick Start**) view after there is a backup task created. As a result of this change, the **Quick Start** section will disappear and the additional sections (described below) will be added.

The main workspace area of the Acronis vmProtect 9 dashboard shows an overview of all currently running tasks or the last finished task details if there are no running tasks. The dashboard is designed to be the most user-friendly environment for presenting summary information about the current status of your backup, restore and other tasks. It does so by using color-coding for successful and failed tasks. As the dashboard outlines all actions you can perform with Acronis vmProtect 9, it presents a very useful tool for a quick operational decision making.

You can switch to the dashboard by clicking the main Acronis vmProtect 9 logo in the top left corner, or by clicking the **Home** button in the main menu. Any group on the dashboard, except **Alerts**, can be hidden into a tray with the respective minimize icon.

### Tasks

The **Tasks** section presents summary information about the current tasks that are running or about the last completed task when there are no tasks running. The progress bar shows the completed percentage of the backup/restore tasks, task name, starting time, remaining time and current speed. From the dashboard **Tasks** block, you can directly open the task log, stop the task or switch to the **Tasks** (**View** -> **Tasks**) page.

### Task Statistics

The **Task Statistics** section shows summary information about the backup/restore tasks executions. The information on a diagram is presented visually for quick and easy perception and analysis. The successful tasks are marked green. The failed tasks are marked red. The tasks finished with warnings are marked yellow. You can see the tasks percentages and get the detailed statistics for a certain date by pointing at the respective diagram. Also you can change the statistics view by clicking **Hourly**, **Daily** or **Weekly**.

### Virtual Machines

The **Virtual Machines** section shows the hosts and clusters (vCenter) names and gives the total number of VMs running on the managed ESX(i) host(s) as well as the number of mounted virtual machines (*see the Mounted VMs (p. 92) section*).

### Locations

The **Locations** section shows the total statistics for your backup locations status. It shows the Total backups number, information about the Occupied space, space Occupied by others, and Free space (both in megabytes/gigabytes and percentages). Occupied space is the space occupied by Acronis backups. Occupied by others is the space occupied by the data which is not a backup archive. The Free space statistics is available only for locations which support the retrieval of its value (for example there will be no such field for FTP locations). Also, from the **Locations** section you can switch directly to the **Recovery Points** view by clicking the link below.

# 5.2 Using Web Console

## 5.2.1 Ribbon tabs

The ribbon menu on the top of the screen allows for managing of the software and performing all of the operational functions. The basic Acronis vmProtect 9 functions available through the top menu are described in the following sections below.

There are 3 main tabs in the Acronis vmProtect 9 ribbon menu: **Actions** tab, **View** tab and **Configure** tab. The fourth additional Acronis tab appears dynamically depending on the current user-selected **View** or **Configure** operation.

### Dashboard view

The **Home** button which always appears on the ribbon bar leads to the **Dashboard** view. The Dashboard configuration is described in the “Dashboard management” section (p. 23).

### 1) Actions tab

The first **Actions** tab contains the basic functions of Acronis vmProtect 9 and allows for starting of the following basic tasks.

#### a. Backup task

This is the **Backup** button which runs the **New Backup Task** wizard. The wizard settings are described in the “Backup” section (p. 30).

#### b. Replication task

This is the **Replication** button which runs the **New Replication Task** wizard. The wizard settings are described in the “New Replication Task” section (p. 45).

#### c. Recovery tasks

This is the drop-down menu with Restore tasks. The **Entire VM** button runs the **New Restore Task** wizard. The **Files and Folders** button runs the **File recovery** wizard. **Microsoft Exchange server**, **Microsoft SQL server** and **Microsoft SharePoint Server Data** buttons run the respective extract wizards. The wizards and their settings are described in the “Recovery” section (p. 54).

### d. Run VM from backup task

This is the **Run VM from backup** button which activates the run VM from backup task wizard. The wizard settings are described in the “Running VM from backup” section (p. 70).

### e. Validation task

This is the **Validate** button which starts the new validation task. The task is described in the “Validating backup” section (p. 90).

### f. ESXi Configuration Backup task

This is the **ESXi Configuration Backup** button which runs the **New ESXi Backup Task** wizard. The wizard settings are described in the “Bare Metal Recovery of ESX(i) Hosts” section (p. 75).

## 2) View tab

The second **View** tab contains the basic data views of Acronis vmProtect 9 and allows quick navigation and switching between these basic views.

### a. Tasks view

This is the link to the **Tasks** view. The Tasks management is described in the “Managing tasks” section (p. 81).

### b. Recovery Points view

This is the link to the **Recovery Points** view. The Recovery Points management is described in the “Managing recovery points” section (p. 85).

### c. Replicas view

This is the link to the **Replicas** view. The Replicated VM management is described in the “Managing replicated VMs” section (p. 48).

### d. Mounted VM(s) view

This is the link to **Mounted VM(s)** view. The Mounted virtual machines management is described in the “Managing mounted VMs” section (p. 92).

### e. Show Logs view

This is the link to the **Show Logs** view. The Logs management is described in the “Managing logs” section (p. 93).

## 3) Configure tab

The third **Configure** tab contains the basic tools for Acronis vmProtect 9 configuration and allows you to specify the default settings for the basic backup/restore operations as well as other settings.

### a. ESX(i) Hosts

This is the link to the **ESX(i) hosts** management page. Managing ESX(i) hosts is described in the “Managing ESX(i) hosts” section (p. 99).

### b. Licenses

This is the link to the **Licenses** management page. Managing licenses is described in the "Managing licenses" section (p. 96).

### c. Settings

The **Agent Settings** page contains **Acronis Cloud backup subscription** settings, **Acronis Cloud backup proxy** settings, **Agent Password** settings and **Export/Import** configuration settings.

Also there are two buttons with the default **Backup settings** and **Restore settings** on the **Configure** tab. Click the **Backup settings** or **Restore settings** button to open the backup/restore settings page where you can set up the defaults for all the backup/restore tasks. These backup/restore settings, as well as other settings, are described in detail in the "Managing settings" section (p. 103).

### 4) vmProtect 9 dynamic tab

This is the dynamic tab which appears in the ribbon and changes depending on the currenty selected action of the **View** tab. This dynamic tab shows the buttons which are specific to the current **View** tab actions.

### a. View -> Recovery Points

When the **Recovery Points** view is selected, the **Recovery Points** tab appears in the ribbon menu. The **Recovery Points** management page is described in the "Managing recovery points" section (p. 85).

### b. View -> Replicas

When the **Replicas** view is selected, the **Replicas** tab appears in the ribbon menu. The **Replicas** management page is described in the "Managing replicas" section (p. 45).

### c. View -> Mounted VM(s)

When the **Mounted VM(s)** view is selected, the **Mounted VM(s)** tab appears in the ribbon menu. The **Mounted VM(s)** page is described in the "Managing mounted VMs" section (p. 92).

### d. View -> Show Logs

When the **Show Logs** view is selected, the **Logs** tab appears in the ribbon menu. The **Logs** management page is described in the "Managing logs" section (p. 93).

## 5.2.2 Logout link

In the top right corner of Acronis vmProtect 9 you can see your current user name and the **Logout** button to exit the program or reenter it with another user name.

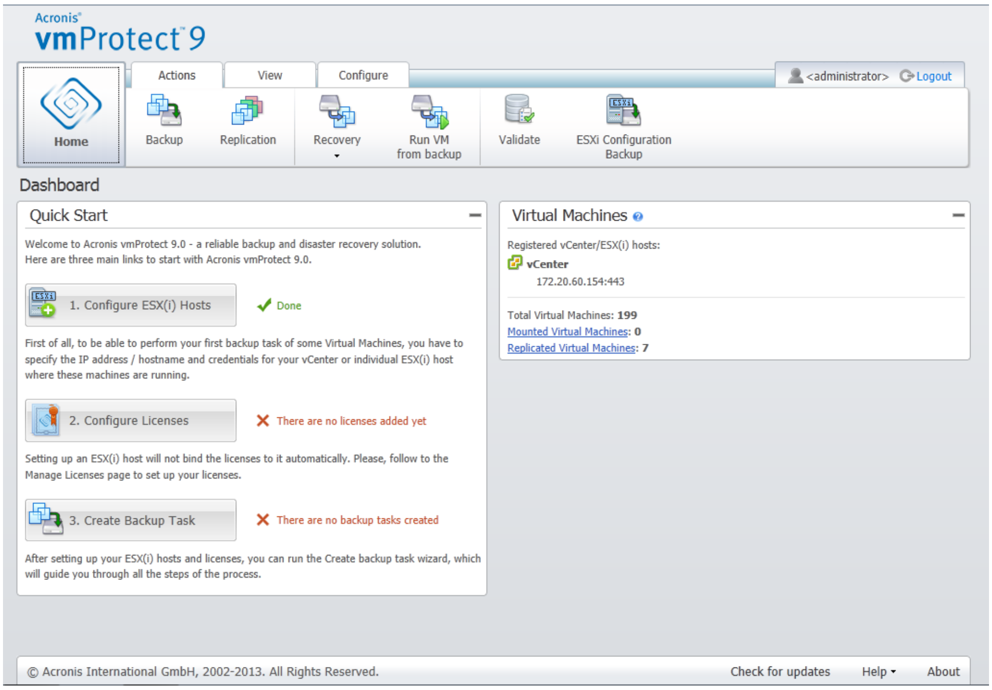
# 6 vCenter Integration

The main tool for managing the vSphere virtual infrastructure is the VMware vSphere client. Although the VMware vSphere client does not provide native backup/restore functionality, it's not always convenient to run another tool to manage these important operations. Acronis vmProtect 9 introduces vCenter integration which allows for basic backup and restore functionality directly from the VMware vSphere client without having to run Acronis vmProtect 9 Web interface. The vCenter integration affects only thick VMware vSphere Client, i.e. you won't get Acronis vmProtect functionality in the VMware vSphere Web Client.

Integration with vCenter is only possible if there is a vCenter registered in Acronis vmProtect 9 Agent. Without a registered vCenter, such integration is not possible. Also, integration is automatically disabled when a vCenter is removed from the vmProtect 9 Agent configuration.

Acronis vmProtect 9 integration with vCenter can be manually enabled and disabled from both vmProtect 9 Web interface and vCenter plug-in manager. In order to enable vCenter integration, go to the **Configure** -> **ESX(i) Hosts** and select the **Enable vCenter Integration** check box when adding a new vCenter, or click the **Enable vCenter Integration** button. To disable the function, click **Disable vCenter Integration**. The Acronis vmProtect 9 login screen shows the IP address of the Agent where integration was enabled.

The integration is available under **Inventory** -> **Solutions and Applications** -> **Acronis vmProtect 9.0** for vSphere clients connected to vCenter.



Dashboard

Quick Start

Welcome to Acronis vmProtect 9.0 - a reliable backup and disaster recovery solution.
Here are three main links to start with Acronis vmProtect 9.0.

1. Configure ESX(i) Hosts ✓ Done

First of all, to be able to perform your first backup task of some Virtual Machines, you have to specify the IP address / hostname and credentials for your vCenter or individual ESX(i) host where these machines are running.

2. Configure Licenses ✗ There are no licenses added yet

Setting up an ESX(i) host will not bind the licenses to it automatically. Please, follow to the Manage Licenses page to set up your licenses.

3. Create Backup Task ✗ There are no backup tasks created

After setting up your ESX(i) hosts and licenses, you can run the Create backup task wizard, which will guide you through all the steps of the process.

Virtual Machines

Registered vCenter/ESX(i) hosts:
vCenter
172.20.60.154:443

Total Virtual Machines: 199
Mounted Virtual Machines: 0
Replicated Virtual Machines: 7

© Acronis International GmbH, 2002-2013. All Rights Reserved.

## How vCenter integration works

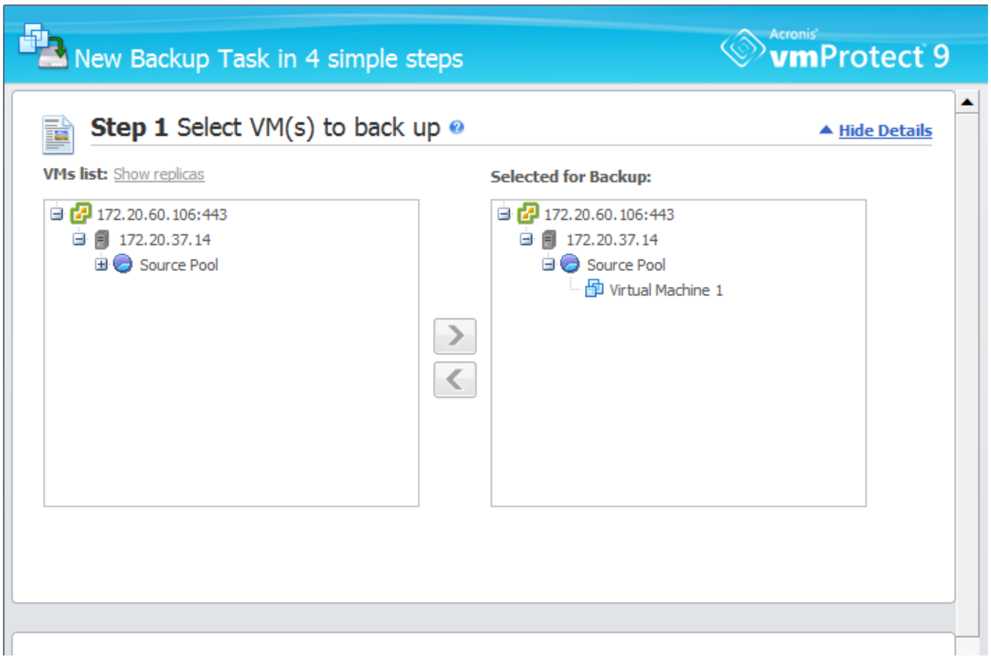
vCenter integration allows you to create backup, restore, replication, etc. tasks and view their progress directly within the VMware vSphere interface.

Select any Virtual Machine, vApp/Resource Pool or ESX(i) host/Cluster in the VMware vSphere tree list. Right-click on the selected item to open the context menu. The context menu contains the

**Acronis vmProtect 9 Backup** and **Acronis vmProtect 9 Restore** options. Choosing one of these options results in opening the Acronis pop-up and activating the backup/restore wizard which will help you create the backup/restore task and implement it right away.

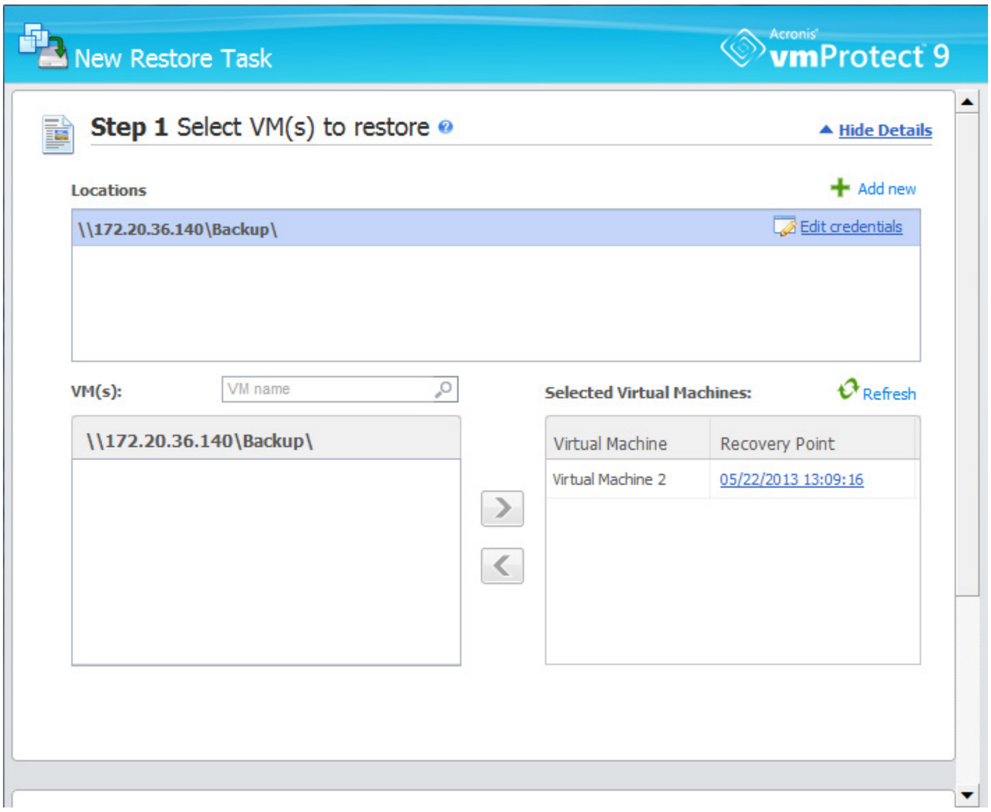
The appearance of the backup/restore wizards (including backup/restore settings) in VMware vSphere interface is exactly the same as in the Acronis vmProtect 9.

The standard **New Backup Task** wizard consists of 4 steps which are explained in detail in the Creating a backup of Virtual Machines (p. 30) section. The first step of the wizard in VMware vSphere **Acronis backup** pop-up will be pre-filled with the VM you right-clicked on; however, you can change the default selection.



vCenter Integration, New Backup Task, step 1

The standard **New Restore Task** wizard consists of 3 steps which are explained in detail in the Restoring a Backup of Virtual Machines (p. 54) section. The first step of the wizard in VMware vSphere **Acronis restore** pop-up will be pre-filled with the VM you right-clicked on. The latest available recovery point in the first discovered **Recent Location** will be selected.



Locations: \\172.20.36.140\Backup\

VM(s): \\172.20.36.140\Backup\

Selected Virtual Machines:

| Virtual Machine | Recovery Point |
|---|---|
| Virtual Machine 2 | 05/22/2013 13:09:16 |

vCenter Integration, New Restore Task, step 1

Note that it's not possible to operate with folders in the **VMs and Templates** view of vSphere client. In this case you will get Acronis context menu items only for Virtual Machines.

Note that vCenter integration is managed by a particular vmProtect 9 Agent. Therefore if the Agent is inaccessible from vCenter side, the functionality available from context menus will not work properly.

## VMware vSphere and Acronis vmProtect 9 synchronization

With VCenter integration enabled, all operations performed in the VMware vSphere client are mirrored in the main Acronis vmProtect 9 interface. These synchronized operations are: new tasks and the tasks' progress. The **Recent Tasks** section shows the progress of backup/restore/etc. tasks executed through the context menu in the VMware vSphere client. Also, when backing up to or restoring from a new location via the context menu option in the VMware vSphere client, the recent locations in vmProtect 9 are also updated.

Similarly, all backup/restore/etc. tasks performed by Acronis vmProtect 9 are registered as **Tasks** in VMware vSphere client.

# 7 Backup

Click **Create Backup Task** in the dashboard's **Quick start** or **Backup** in the **Actions** tab of the main menu to create a new backup task. The **New Backup Task** wizard opens in the main workspace area and asks you to provide the required information and make all necessary settings for the new create backup task. The wizard consists of the four consecutive steps which appear in the same area:

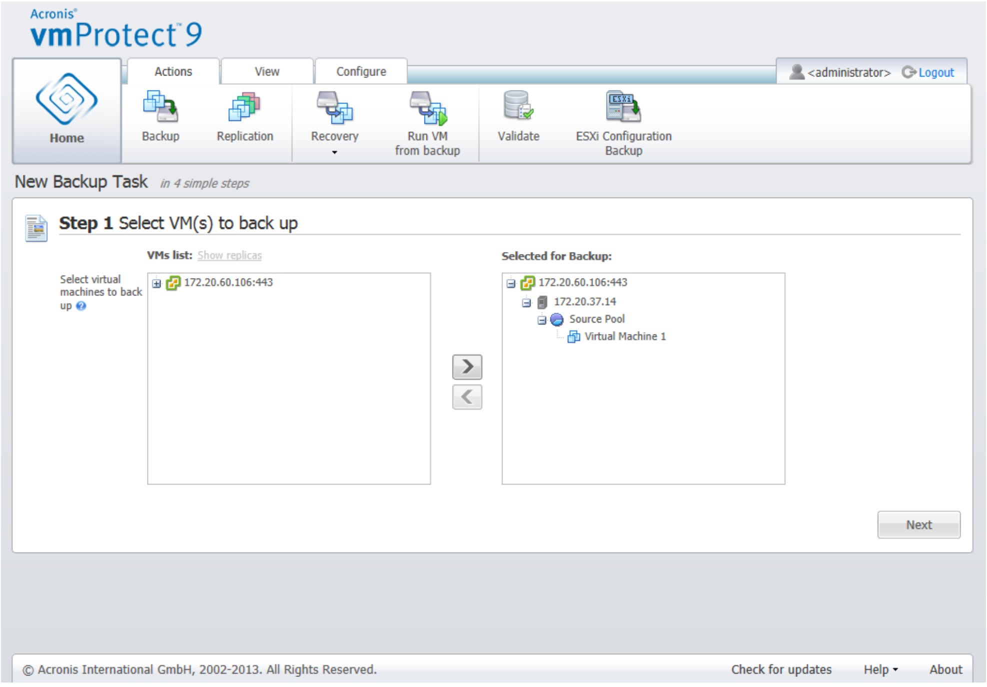
- Select VM(s) to backup.
- When to backup.
- Where to backup.
- How to backup.

These four steps of the wizard and their possible options are described below.

## 7.1 Select VM(s) to back up

In the first step, you should select the virtual machines (or vApps) which you want to back up. The left side shows all your ESX(i) host(s)/vCenter managed by Acronis vmProtect 9 Agent with the list of their virtual machines. If you don't see the exact virtual machine to back up that you are looking for in this list, make sure that you have added the corresponding ESX(i) host from the **Configure** -> **ESX(i) Hosts** page.

Select the virtual machines (or vApps) by moving the machines from the left side of the butterfly control to the right one, via the **>** and **<** buttons. The list on the right shows all the virtual machines selected for backup. The **>** button is used to add the VM to the backup list, and the **<** button is used to remove the VM from this list. You can also select the VM by double-clicking it.



**Step 1** Select VM(s) to back up

Select virtual machines to back up

VMs list: Show replicas
- 172.20.60.106:443

Selected for Backup:
- 172.20.60.106:443
  - 172.20.37.14
    - Source Pool
      - Virtual Machine 1

New Backup Task wizard, Step 1 "Select VM(s) to back up"

You can back up dynamic groups of the machines by selecting the upper level unit (e.g. ESX(i) host or VMs folder) in the tree and moving it to the right list with the same **>** button. As a result, all the machines running within this group will be automatically included in the backup list. Moreover, any new machines created in this group will be backed up automatically by the current backup task.

You can also back up replica VMs (see the Replication section (p. 45)). For that click the **show replicas** button above the VMs list and select the replica VM for backup. Note that it's not recommended to perform replication to and backup from replica VM at the same time. Be careful while setting up the schedules.

After you make the selection of VM(s) to back up, click **Next** to finish the first step and continue further on.

## 7.2 When to back up

In the second step of Create backup task wizard, you should define the schedule of backing up your virtual machines data. There are two options available – scheduling your backup, and creating a single time backup task ("Do not schedule, run on demand"). By default the schedule is to create backups daily at 12:00. Here you can change the default value or select "Do not schedule, run on demand" which means that the backup task will not be executed on schedule. It will be started either right after the backup task creation or can be run manually from the **Tasks** view.

Set your scheduling of how often to back up the data. Acronis vmProtect 9 allows for weekly scheduling and functions in Windows and Linux operating systems.

In the **Schedule** area, select the appropriate parameter as follows: Every: <...> week(s) on: <...>. Specify a certain number of weeks and the days of the week you want the task to be run. For example, with the Every **2** week(s) on **Mon** setting, the task will be performed on Monday of every other week.

In the **During the day execute the task...** area, select one of the following: Once at: <...> or Every: <...> From: <...> Until: <...>.

For the **Once at: <...>** choice, set up the time at which the task will be run once.

For the **Every: <...> From: <...> Until: <...>** choice, set up how many times the task will be run during the specified time interval. For example, setting the task schedule to Every 1 hour From 10:00:00 AM until 10:00:00 PM allows the task to be run 12 times from 10 AM to 10 PM during one day.

Let's see some of the scheduling examples.

### "One day in the week" schedule

This is a widely used backup schedule. If we need to run the Backup task every Friday at 10 PM, the parameters are set up as follows:

1. Every: **1** week(s) on: **Fri**.
2. Once at: **10:00:00 PM**.

### "Workdays" schedule

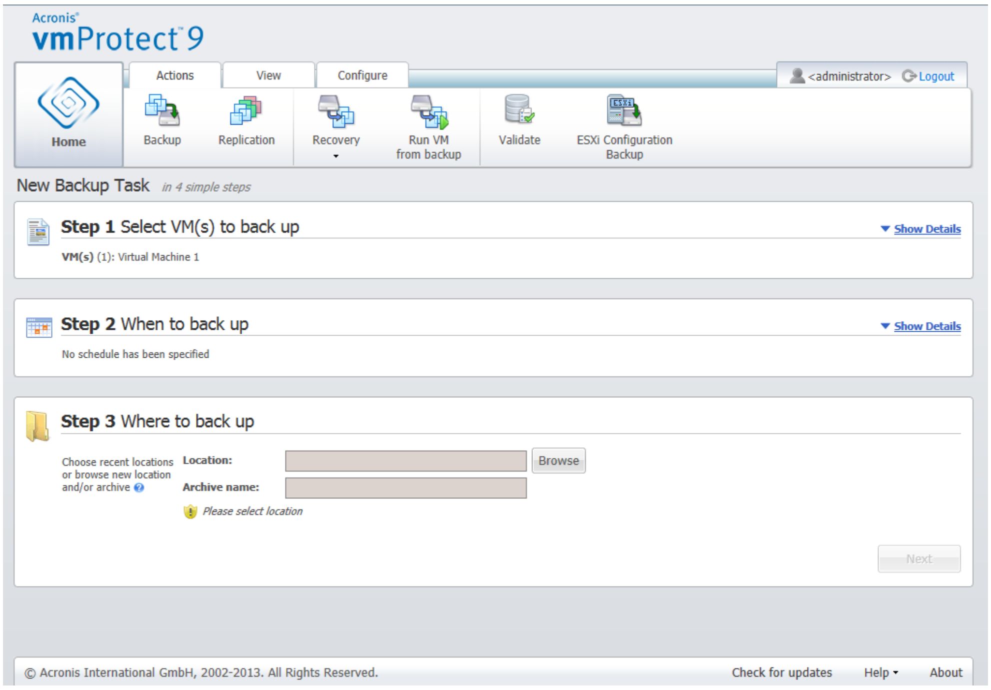
Run the task every week on workdays: from Monday to Friday. During a workday, the task starts only once at 9 PM. The schedule's parameters are thus set up as follows:

1. Every: **1** week(s) on: **<Workdays>**. Selecting the **Workdays** check box automatically selects the corresponding check boxes (**Mon, Tue, Wed, Thu**, and **Fri**), and leaves the remaining two unchanged.
2. Once at: **09:00:00 PM**.

After setting up your backup schedule of “When to back up”, click **Next** to go to the last step of the wizard.

## 7.3 Where to back up

In the third step, you should define the location for your backup archive. Select a location by clicking on the **Browse** button. You will see a pop-up window with the browsing options where you can define or change the path and set the archive name. From the list of recent locations, you can either select one of the locations that was previously used or set up a new one.



New Backup Task *in 4 simple steps*

**Step 1** Select VM(s) to back up

VM(s) (1): Virtual Machine 1

**Step 2** When to back up

No schedule has been specified

**Step 3** Where to back up

Choose recent locations or browse new location and/or archive

**Location:**

**Archive name:**

*Please select location*

New Backup Task wizard, Step 3 “Where to back up”

The **Archive name** field shows the name of the archive selected in the **Browse** pop-up.

The left side of the **Browse** pop-up shows the list of:

- Cloud backup storages.
- Recent Locations.
- Local folders.
- Network folders.
- FTP servers.
- SFTP servers.

If your vmProtect 9 Agent has no licenses added, the only possible choice for a backup destination is Acronis Cloud Backup Storage.

Choose one of the backup location types from the browse tree on the left side. If the chosen location requires authentication (Cloud backup storage, Network folders or FTP/SFTP servers), you will initially see a dialogue for submitting your credentials in the right pane. After successfully logging in, this pane shows the contents of the selected location, i.e. the archives inside this location.

*Note that Acronis vmProtect 9 Cloud backup storage might be unavailable in your region. For more information, visit http://www.acronis.eu/my/backup-recovery-online/ .*

Also, please, note that within the Acronis Cloud backup storage application-aware backups, the backup validation and run VM from backup operations are not possible.

Note that to successfully backup to an FTP/SFTP server, you need to have the deletion rights assigned to the respective file and folder on that server.

Instead of browsing for the location in the tree, you can manually enter the path in the corresponding **Location** field below and click on the **Go** button to explore this location. In this case, you will see the same authentication dialogue in the right pane where you are asked to enter your login and password.

Enter your archive name value in the corresponding **Archive name** field below. Note that it is not recommended to have more than one backup task writing data to the same archive. The retention rules applied to the archive by different backup tasks may cause an unpredictable outcome.

Select the archive type for the new backup. Acronis vmProtect 9 can save your backup data by using one of the two basic types of archives – Standard archive (Legacy mode) or Always Incremental archive. “Always Incremental” archive type is not supported on FTP/sFTP/Acronis Cloud Storage locations.

Select the **Save each backup in separate files** option for the Legacy archive (*please, refer to “Multiple files backup scheme (Legacy mode)” section* (p. 9)). Or select the **Save all backups in one file (recommended)** option. This means that the archive will have the new enhanced “Always Incremental” format (*please, refer to “Single file backup scheme (Always Incremental)” section* (p. 10)).

In case of editing your existing backup task or selecting an existing archive for the backup location, this setting is not shown.

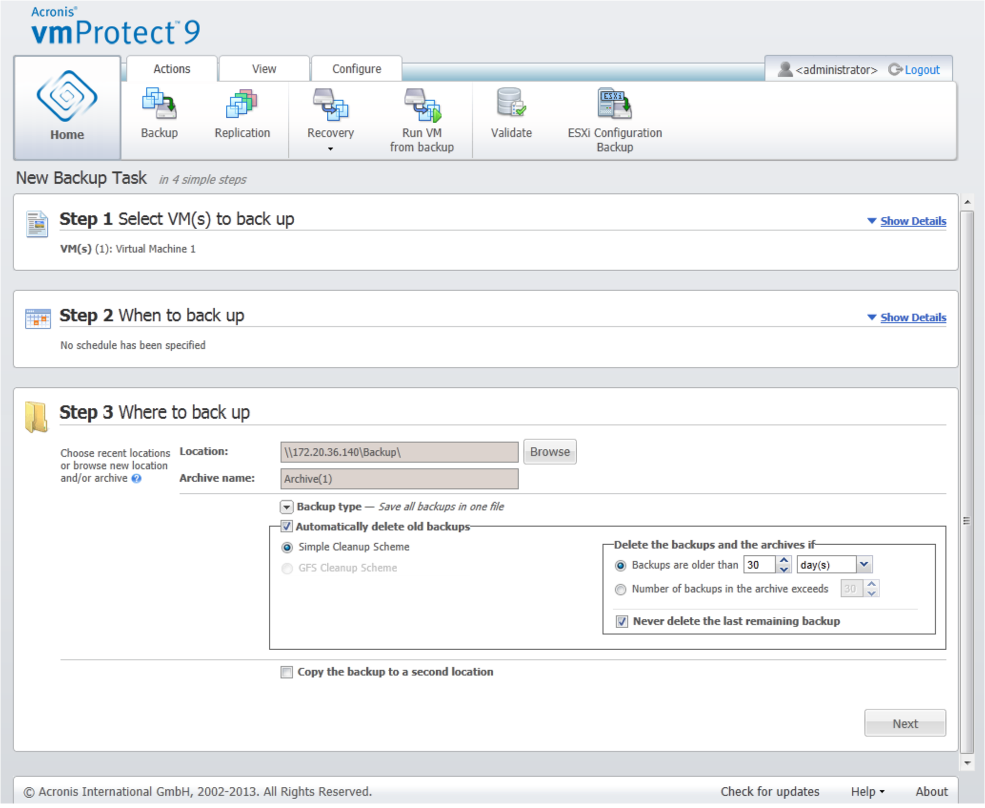
Select the **Automatically delete old backups** check box to define the retention rules for backup management inside the archive. The availability of the options depends on the schedule setup in the previous step (*section “When to Backup”*) and on the selected archive format. For example, the Grandfather-Father-Son (GFS) cleanup scheme will not be available for the unscheduled backup task. Create full backups every: <...> choice will not be available for the “Save all backups in one file” option (as full backups don’t make sense for the Always Incremental archive format). What follows is a description of each retention rule.

### 1. Not specified

If the retention rules are not specified, then no programmed backups management will be performed, i.e. all the backups will be stored inside the archive indefinitely.

### 2. Simple cleanup scheme

The selection of the simple cleanup scheme allows you to keep a certain number of backups inside the archive or keep the backups for a certain time period.



New Backup Task *in 4 simple steps*

**Step 1** Select VM(s) to back up

VM(s) (1): Virtual Machine 1

**Step 2** When to back up

No schedule has been specified

**Step 3** Where to back up

Choose recent locations or browse new location and/or archive

Location: \\172.20.36.140\Backup\

Archive name: Archive(1)

Backup type — *Save all backups in one file*

☑ Automatically delete old backups

● Simple Cleanup Scheme

○ GFS Cleanup Scheme

Delete the backups and the archives if

● Backups are older than 30 day(s)

○ Number of backups in the archive exceeds 30

☑ Never delete the last remaining backup

□ Copy the backup to a second location

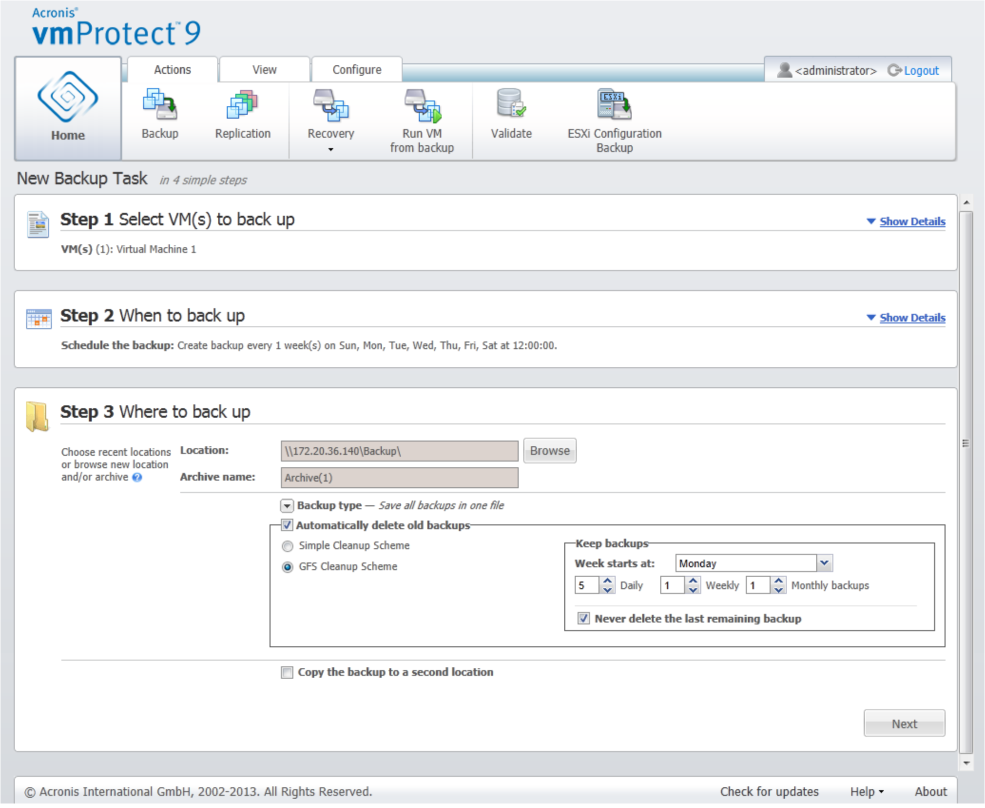
© Acronis International GmbH, 2002-2013. All Rights Reserved.

Create Backup wizard, Step 3 “Where to back up”, Simple cleanup scheme, delete the outdated backups

The second option allows you to clean up the archive if the number of backups exceeds <…>. Again, if you set this number at 1, then for the Always Incremental archive mode there will be a synthetic full backup created, i.e. an incremental backup which will remove the unnecessary old recovery point contents after the backup is finished. If the retention number of archives is greater than 1, then the cleanup is performed according to the Always Incremental archive mode (*refer to section “Single file backup scheme (Always Incremental)” (p. 10) of this User Manual for further information*).

## 3. GFS cleanup scheme

This is a common “Grandfather-Father-Son” cleanup scheme which allows you to keep a certain number of daily, weekly and monthly backups. Indicate how many daily, weekly and monthly backups you need to keep. All backups made within one day are considered to be “daily” ones and will be all deleted when that date is expired. The same rule applies to “weekly” backups.



New Backup Task *in 4 simple steps*

**Step 1** Select VM(s) to back up

**VM(s)** (1): Virtual Machine 1

**Step 2** When to back up

**Schedule the backup:** Create backup every 1 week(s) on Sun, Mon, Tue, Wed, Thu, Fri, Sat at 12:00:00.

**Step 3** Where to back up

Choose recent locations or browse new location and/or archive

**Location:** \\172.20.36.140\Backup\

**Archive name:** Archive(1)

**Backup type** — *Save all backups in one file*

☑ **Automatically delete old backups**

○ Simple Cleanup Scheme

● GFS Cleanup Scheme

**Keep backups**

**Week starts at:** Monday

5 Daily 1 Weekly 1 Monthly backups

☑ **Never delete the last remaining backup**

☐ **Copy the backup to a second location**

© Acronis International GmbH, 2002-2013. All Rights Reserved.

Create Backup wizard, Step 3 “Where to back up”, GFS cleanup scheme

Note that retention rules are applied **only before** the backup task execution. The reason for this is that with the Always Incremental archive there is no need to remove recovery points after the backup because it does not free disk space. If after performing the backup there are new excessive recovery points which have to be deleted according to the set up retention rules, they will be removed only before next backup. For example, if you set up the retention rules to **Delete the backups and the archives if** your **Backups are older than** 3 days or **Number of backups in the archive exceeds** 3, there will actually be up to 4 backups stored in the archive, and not 3.

Note that at least **one backup** will always remain intact inside the archive even if this backup becomes subject to deletion according to the specified retention rules. This design ensures that you always have at least one backup available for recovery in the archive. This will be true until you clear the **Never delete the last remaining backup** check box (selected by default) which defines the behavior of the program when there is only one valid recovery point left and it becomes subject to deletion. This may be the case, for example, when you have applied a backup task to a group of virtual machines and one of the machines has been deleted from the ESX(i) host, making it no longer possible to be backed up. At some point (according to the specified retention rules), all the backups of this deleted VM will become subject to deletion. Accordingly, the **Never delete the last remaining backup** check box will prevent or force the deletion of the last remaining backup.

You can protect your VM environment by storing your backups in several different locations. By default, the backup task saves all backup archives to a single storage. But you can configure the task to copy the created backups to another archive storage on the second location.

Select **Copy the backup to a second location** check box.

The following settings allow you to configure the backup copying options. Select the second location where you would also like to store your backups and the **archive name**. Click Browse and select from the available list of locations.

From the **When to copy** drop down list select if you would like to copy the backup to the second location immediately after each backup is created. Or you can indicate the specific days for performing your backup copy, other than the backup schedule days. In this case you can also choose to **copy all missed recovery points** or **copy last created recovery points only**.

The **Copy last created recovery points** option might be useful when the first location selected is sometimes unreachable. In case the **Copy all missed recovery points** option is selected and the retention rules for the first storage are executed on the main location, then the software deletes the recovery points that should be removed by these rules, even if these recovery points were not copied to the second location. So when the retention rules are executed it is not checked if the recovery points were already copied to the second storage or not.

By default, the backup type and the clean up rules for the copied backups are the same as the respective primary backup settings. Meanwhile, you can choose to specify different settings, for example, employ a different backup type, or change the retention rules options.

After you’ve selected “Where to back up”, click on **Next** to finish this step and proceed to the next one.

## 7.4 How to back up

On the fourth step you should define the preferences of your new backup task.

### 7.4.1 Application-Aware Backup Settings

Prior to running **Microsoft Exchange Server Items**, **Microsoft SQL Server Databases**, **Microsoft SharePoint Server Data** or **Microsoft Active Directory** recovery you have to configure your backups to become “Application-aware”. From the VMs list on the left select the specific VM(s) running MS Exchange Server, MS SQL Server, MS SharePoint Server, MS Active Directory, provide its/their **Domain Administrator Credentials**. You can add several VMs running applications.

Optionally you can choose to **Automatically truncate the transaction logs after backup**.

Note that for enabling the Application-aware backup, you have to provide guest OS login credentials for the selected VM(s) running MS Exchange server, MS SQL Server, MS SharePoint Server, MS Active Directory. This means that you have to specify a user with domain administrator privileges. User Account Control (UAC) technology introduced in Windows Server 2008 operating system is not natively supported by Acronis vmProtect 9 since the product accesses the VMs data in agent-less mode. So, if UAC is enabled for the user you specify, we would suggest the following possible solutions (either one is acceptable):

1. Disable UAC for the specified user. The UAC can be enabled/disabled via a domain group policy, for example.

2. Specify a different user for which UAC is disabled. For example you can use a built-in domain administrator account which has UAC disabled by default.
3. Install a small (up to 30Mb) “Acronis Backup Agent” inside the VM. For that: run Acronis vmProtect 9 installation package, choose **Extract Components** option from the menu, extract Acronis Backup Agent .msi component and install the Agent onto the server where UAC is enabled. Then, you can employ any domain user with domain administrator privileges independently from UAC state.

Note that while vmProtect 9 is not a cluster-aware software, it is still possible to perform Application-aware backups of Exchange cluster nodes (Exchange 2003 SP2+ versions are supported). During the backup Acronis vmProtect 9 can back up the Exchange databases available for the specific VM (node of Exchange cluster) at the given moment of time. While there are many different types of Exchange cluster (SCC, CCR, DAG) which all have their own specifics, the main thing you should ensure is that the Exchange databases data is actually accessible from the VM you are backing up with “Application-aware” option. The same approach applies to transaction logs truncation option – they will be truncated for the accessible databases only.

For example, it does not matter which node of Exchange 2010 DAG cluster you are backing up, since in this case each node can host active databases and passive databases (i.e. replicas of databases from other nodes), and all these databases will be properly backed up as they are accessible from any node. Note that the logs will be truncated for both active and passive databases in this case.

The exception from this rule is SCC cluster where database is located on shared storage and therefore is inaccessible for vStorage API used to get access to the VM data. SCC clusters are NOT supported.

If you are planning to extract the Exchange database from the backup and perform recovery to the point of failure, which implies replacing the database with the backup copy and rolling up the transactions logs on top of it, then you should make sure to extract the very latest version of the database, so that the existing transaction logs can be applied to this copy. If any of the transactions logs are missing in the chain then their roll up will not be possible.

*NOTE: The backup of VM(s) with Active Directory should not be older than the “tombstone lifetime” setting (60 days by default). Otherwise, the domain controller within the VM(s) restored from such an outdated archive will be inconsistent. For more information, please, refer to http://support.microsoft.com/kb/216993/en-us.*

### 7.4.2 Backup validation

If you would like to check the newly created backup for consistency (perform the backup validation), select the **Validate after backup** check box (*for further information on Backup validation, please refer to section “Validating backups”* (p. 90)).

If you have configured your backup task to copy the backups to a second location, here you can choose to validate your backups in the second location or not.

### 7.4.3 Other settings

Click **More options** to open the pop-up with the additional settings. These options are described in the “Options” section (p. 38).

### 7.4.4 Completing the Create backup task wizard

To complete the New backup task wizard, you should define the task name. Note that [ ] { } ; , . symbols are not allowed for the task name.

When you click on the **Save** button, all the parameters of your set up backup task will be saved and you will see the created task in the **Tasks** view. Clicking on the **Save & Run** button will result in saving the task and running it right away.

## 7.5 Options

Clicking on the **More options** in the last step of the **New Backup Task** wizard opens up a pop-up with the settings. If no changes were made to the settings, they will retain their respective default values for your current backup task. Note that if later on you change certain settings and save them as default, it will not affect the tasks created with the default settings (they will retain the settings which were default at the moment of the task creation).

This section below describes all the settings one by one.

### 7.5.1 Archive Protection

The default value for the **Archive protection** parameter is “Disabled”. This option is not available when editing the existing task or when creating a new task specifying the existing archive.

In order to protect your archive from unauthorized access, select the **Set password for the archive** check box, then type your password in the **Enter the password** field; and, finally re-type it in the **Confirm the password** field. Note that the password is case-sensitive.

The created archive can be protected either with just a password or enhanced with the Advanced Encryption Standard (AES) 128/192/256-bit key encryption algorithm. Ia you select **Do not encrypt**, your archive will be protected with the password only. If you would like to use the encryption, select one of the following: AES 128, AES 192 or AES 256.

The AES cryptographic algorithm operates in the Cipher-block chaining (CBC) mode and uses a randomly generated key with a user-defined size of 128, 192 or 256 bits. The larger the key size, the longer it will take for the program to encrypt the archive and the more secure your data will be.

### 7.5.2 Source Files Exclusion

With the source files exclusion rules you can define which data will be skipped from the source data during the backup process and thus be excluded from the list of backed up items. These can be files or folders defined by a path set up for exclusion.

This option is effective for the backup of virtual machines which contain volumes of NTFS and FAT file systems only. Specifically, it works with all switched off VMs (with FAT and NTFS file systems) and for switched on VMs with OS version windows server 2003 and higher. Besides, the option requires VMware tools running on the target VM.

Use the following parameters to specify which files and folders to exclude.

### Exclude files matching the following criteria

Select this check box to skip files and folders with names matching any of the listed criteria (called file masks). Use the **Add**, **Edit**, **Remove** and **Remove All** buttons to create and manage the list of file masks.

You can use one or more wildcard characters "*" and "?" in a file mask.

To exclude a folder specified by a path containing the drive letter, add a backslash ("\") to the folder name in the criterion, for example: C:\Finance\.

For example, you can set the **Source files exclusion** to **Exclude files matching the following criteria**: *.tmp, *.~, *.bak.

You can exclude the whole volume of the backed up VM by specifying exclusions in the following format: C:\* or D:\* . Note that the drive letters specified in the exclusions settings may not correspond the drive letters defined in the guest OS. For example, you have Windows 2008 guest OS which has system reserved partition (without a drive letter assigned). Then to exclude the files from the C: drive you have to specify D:\* in the exclusions settings in Acronis vmProtect 9.

Another example. Suppose the source system has the following partitions:

- System Reserved
- C: (Local Disk)
- D: (CD-ROM)
- E: (Local Disk)
- K: (Local Disk)

In Acronis vmProtect 9 these volumes will be enumerated in alphabetical order starting from the "system reserved" partition and skipping CD-ROM(s):

- C: (System Reserved)
- D: (C: (Local Disk))
- E: (E: (Local Disk))
- F: (K: (Local Disk))

Therefore in order to exclude the K: drive you should specify F:\* in the exclusions settings in Acronis vmProtect 9.

Tip: you can check the volume letters enumeration via the File Recovery feature (where you browse through the files/folders tree inside an existing recovery point).

## 7.5.3 Compression Level

The **Compression level** option defines the level of compression applied to the data being backed up. The default setting for this option is **Normal**.

The optimal data compression level depends on the type of data being backed up. For example, even maximum compression will not significantly reduce the archive size if it already contains fairly compressed files, such as .jpg, .pdf or .mp3. However, such formats as .doc or .xls could be significantly further compressed.

Select one of the following compression levels:

- **None**. The data will be copied "as is", without any compression. The resulting backup size will be maximal.
- **Normal**. This compression level is recommended in most cases.
- **High**. The resulting backup size will typically be less than for the **Normal** level.
- **Maximum**. This is the highest degree of the data compression. But the time for performing backup task will be maximal. You may want to select maximum compression when backing up to removable media to reduce the number of required volumes.

### 7.5.4 Error Handling

These options enable you to specify how to handle errors that might occur during backup.

When a recoverable error occurs, the program re-attempts to perform the failed operation. You can set the time interval and the number of attempts. The task finishes as soon as the operation succeeds OR the specified number of attempts is reached.

There are separate settings for network errors (**Re-attempt the data transmission if network error occurs**) and VM backup errors (**Re-attempt the failed VM processing**). The both options are enabled by default with the following settings: **Number of attempts** – 5, and **Interval between attempts** – 30 seconds.

For example, with the default network error settings if the backup destination on the network becomes unavailable or not accessible, the program will attempt to reach the destination every 30 seconds, but no more than 5 times. The attempts will be stopped as soon as the connection is resumed or if the specified number of attempts is reached.

With the default backup error settings the failed VM backup processing is automatically restarted 30 seconds after the failure and after 5 such attempts the program proceeds to the next VM backup.

### 7.5.5 Disaster Recovery Plan

The disaster recovery scenario implies that sometimes there are different technical persons managing backup and recovery procedures. Thus the person who performs the recovery may not know the details of where the images are located, which machines they belong to, etc. Acronis vmProtect 9 allows you to create a **Disaster Recovery Plan (DRP)** that contains simple step-by-step instructions on how to recover data from backup archive in case of system failure. The **Disaster Recovery Plan** can be sent by e-mail to specified users or saved to specific location/folder.

**Disaster Recovery Plan** is generated by Acronis Agent and sent after the first backup. A new **Disaster Recovery Plan** is sent if the backup task is modified or if there are significant changes to the backup contents.

The default value for the **Disaster Recovery Plan** parameter is "Disabled".

You can enable the **Disaster Recovery Plan** in the **Default Backup Settings** for all backup tasks. Go to **Configure** -> **Backup settings** and click **Disaster Recovery Plan**. You can also set up DRP for any individual backup task at the step 4 of the **New backup task** wizard. Click **More options** and go to the **Disaster Recovery Plan** section.

Select **Send disaster recovery plans** check box to enable the DRP. Configure the DRP options as follows:

- Enter the destination e-mail address in the **E-mail addresses** field. You can enter several e-mail addresses separated by semicolons.
- Enter the e-mail **subject**. The default subject line is **Acronis vmProtect 9 Notification from Acronis Appliance**.
- Enter the outgoing mail server (SMTP) in the **SMTP Server** field.
- Set the **port** of the outgoing mail server. By default the port is set to 25.
- If your SMTP server requires authentication, enter **User name** and **Password** in the appropriate fields.
- Enter the e-mail sender's name in the **From** field.
- If necessary, select **Use encryption** and choose the encryption type - SSL or TLS.
- You can click **Send test e-mail message** to check if the **Disaster Recovery Plan** is sent correctly with the specified settings.

Select **Upload disaster recovery plans to the following location** check box if you would like to keep the DRP copy and **Browse** the location.

## 7.5.6 Notifications

### 1) E-mail notifications

This option sets up e-mail notifications about the basic events during your backup task, such as successful completion, backup failure or need for user interaction. The default setting for this option is Disabled.

Select the **Send e-mail notifications** check box to enable notifications.

Under **Send e-mail notifications** check box select the desired settings as follows:

- **When backup completes successfully** – to send a notification when the backup task has completed successfully.
- **When backup fails** – to send a notification when the backup task has failed.
- **Add full log to the notification** – to receive the full log.

Type one or several e-mail addresses where notifications will be sent. Addresses are entered in the **E-mail addresses** field separated by semicolons.

Indicate the desired **Subject** for your notification messages.

**SMTP server** – enter the name of the outgoing mail SMTP server.

**Port** – set the port of the SMTP server (the default port value is set to 25).

**User name** – enter your username.

**Password** – enter your password.

**From** – type the e-mail address of the user from whom the message will be sent. If you leave this field empty, messages will be sent as if they are from the destination address.

**Use encryption** – you can opt for the encrypted connection to the mail server and choose SSL or TLS encryption types.

Click **Send test e-mail message** to make sure all your settings are correct.

## 2) SNMP notifications

This option defines whether the agent(s) operating on the managed machine have to send the logs of the backup operation events to the specified Simple Network Management Protocol (SNMP) managers. You can choose the types of events to be sent. The default setting for this option is: Disabled**.**

Select whether to send the backup operation events log messages to machines running SNMP management applications, please, choose one of the following:

- **Do not send SNMP notifications** – to disable sending the events log of the backup operations to SNMP managers.
- **Send SNMP notifications individually for backup operation events** – to send the events log of the backup operations to the specified SNMP managers.
  **Type of events to send** – choose the types of events to be sent: Information, Warnings or Errors.
  **Server name or it's IP** – type the name or IP address of the host running the SNMP management application where the notifications will be sent to.
  **Community** – type the name of the SNMP community to which both the host running the SNMP management application and the sending machine belong. The typical community is **public**.
  Click **Send test message** to make sure all your settings are correct.

## SNMP objects

Acronis vmProtect 9 provides the following Simple Network Management Protocol (SNMP) objects to SNMP management applications:

- Type of event

  Object identifier (OID): 1.3.6.1.4.1.24769.100.200.1.0

  Syntax: OctetString

  The value may be “Information”, “Warning”, “Error” and “Unknown”. “Unknown” is sent only in the test message.
- Text description of the event

  Object identifier (OID): 1.3.6.1.4.1.24769.100.200.2.0

  Syntax: OctetString

  The value contains the text description of the event (it looks identical to messages published by Acronis vmProtect 9 in its log).

**Example of varbind values:**

1.3.6.1.4.1.24769.100.200.1.0:Information

1.3.6.1.4.1.24769.100.200.2.0:I0064000B

### Supported operations

Acronis vmProtect 9 **supports only TRAP operations**. It is not possible to manage Acronis vmProtect 9 using GET- and SET- requests. This means that you need to use an SNMP Trap receiver to receive TRAP-messages.

### More information

http://kb.acronis.com/content/11851

### About the test message

When configuring SNMP notifications, you can send a test message to check if your settings are correct.

The parameters of the test message are as follows:

- Type of event
  OID: 1.3.6.1.4.1.24769.100.200.1.0
  Value: "Unknown"
- Text description of the event
  OID: 1.3.6.1.4.1.24769.100.200.2.0
  Value: "?00000000"

## 7.5.7 Additional Settings

### 1) Deduplication

This option defines whether to enable or disable the deduplication for the archive created by the backup task. The default setting for Deduplication is: Enabled.

Deduplication is performed on the archive level. This means that only the data which is saved to this archive will be deduplicated. In other words, if there are 2 archives saved into the same location with deduplication enabled, the duplicated data which may be present in both of these archives will not be deduplicated.

### 2) CBT backup

This option defines whether to utilize the Changed Block Tracking feature of VMware for the virtual machines supporting it. The default setting for CBT backup is: Enabled.

CBT backup keeps track of all the changed blocks inside the virtual machine. This significantly reduces the time for creating backups. The time is reduced because Acronis vmProtect 9 does not need to check which blocks have changed since the last backup. It gets this information from the VMware API.

### 3) Use FTP in active mode

It is possible to use FTP active mode for FTP authentication and data transfer. The default setting for Use FTP in active mode is: Disabled.

Enable this option if your FTP server supports active mode and you want this mode to be used for file transfers.

After you finished with all the settings, click **OK** to close the pop-up and apply them for the current backup task only.

## 7.6 Managing created backup task

When editing an existing backup task you will see all the sections (steps) of the backup wizard you completed while creating your backup task. All four steps of the wizard will appear on the screen at once. Note that when editing an existing backup task you cannot modify the archive type (**Always Incremental** or **Legacy Mode**). (*For further information, please, refer to “Managing Tasks” section* (p. 81)).

# 8 Replication

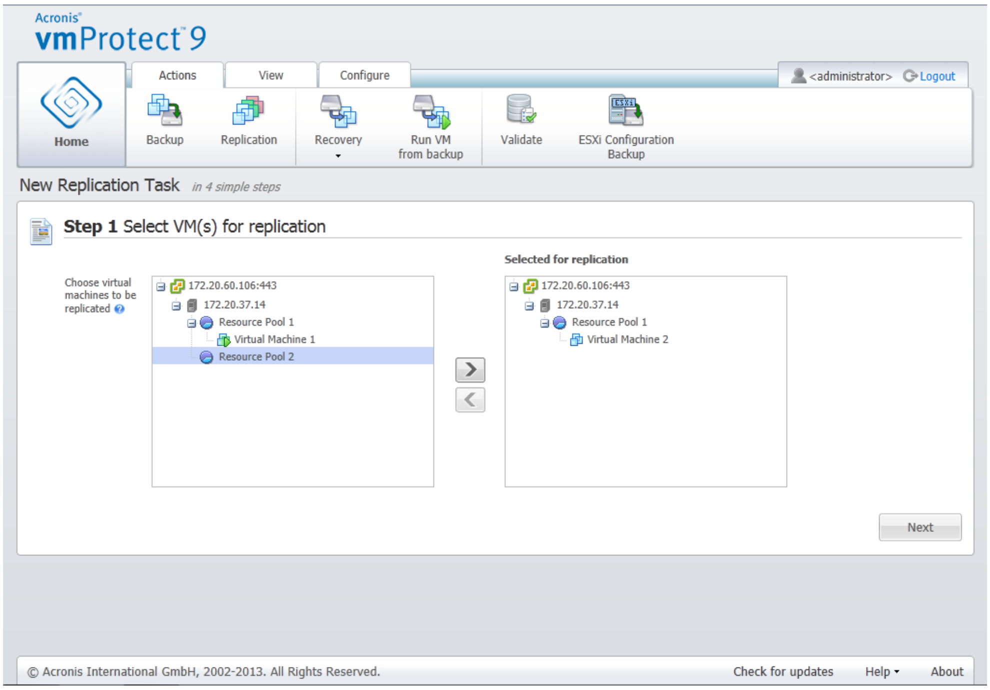
## 8.1 New Replication Task

The replication feature provides you with the ability to clone your critical VMs and to be able to start your critical service fast in case of failure. To run the **New Replication Task**, click **Actions** -> **Replication**.

### 8.1.1 Select VM(s) for Replication

In the first step of the **New Replication Task** wizard you should select the virtual machine(s) you want to replicate. The left side shows all of the ESX(i) hosts/vCenter you have which are managed by Acronis vmProtect 9 Agent and a list of their virtual machines. If you don't see the exact virtual machine to be replicated in this list, make sure that you have added the corresponding ESX(i) host from the **Configure** -> **ESX(i) Hosts** page.

Select the virtual machine(s) by moving the machines from the left side of the butterfly control to the right side by using the **>** and **<** buttons. The list on the right shows the virtual machines selected for replication. The **>** button is used to add the VM to the selected list, and the **<** button is used to remove the VM from this list. You can also select the VM by double-clicking it.



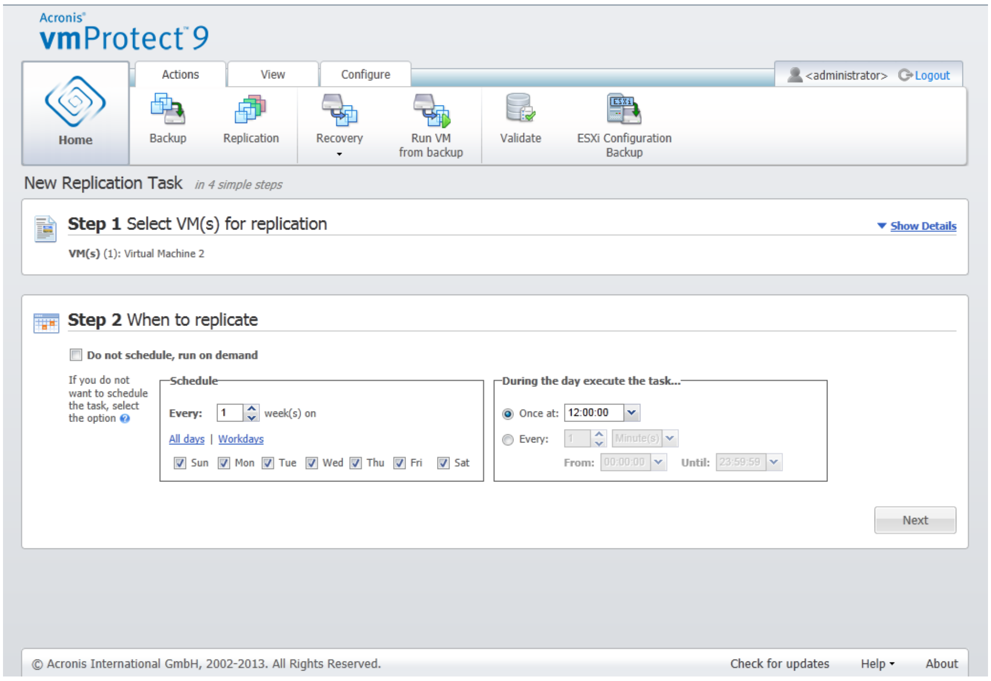
New Replication Task, step 1 "Select VM(s) for replication"

You can back up dynamic groups of the machines by selecting the upper level unit (e.g. ESX(i) host or VMs folder) in the tree and moving it to the right list with the same **>** button. As a result, all the machines running within this group will be automatically included in the backup list. Moreover, any new machines created in this group will be replicated automatically by the current replication task.

You have to select at least one VM for replication. After you make your selection, click **Next** to finish the first step and continue further on.

## 8.1.2 When to Replicate

In the second step of the **New Replication Task** wizard, you should define the schedule of replicating your virtual machines. There are two options available – creating a single time replication task ("Do not schedule, run on demand") and weekly scheduling. By default the schedule is to create replicas daily at 12:00. In this step, you can change the default value or select "Do not schedule, run on demand" which means that the replication task will not be executed on schedule. It will be started either right after creating your replication task or can be run manually from the **Tasks** view.



New Replication Task *in 4 simple steps*

**Step 1** Select VM(s) for replication

**VM(s)** (1): Virtual Machine 2

**Step 2** When to replicate

☐ **Do not schedule, run on demand**

If you do not want to schedule the task, select the option

Schedule

Every: 1 week(s) on

All days | Workdays

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

During the day execute the task...

● Once at: 12:00:00

○ Every: 1 Minute(s)

From: 00:00:00 Until: 23:59:59

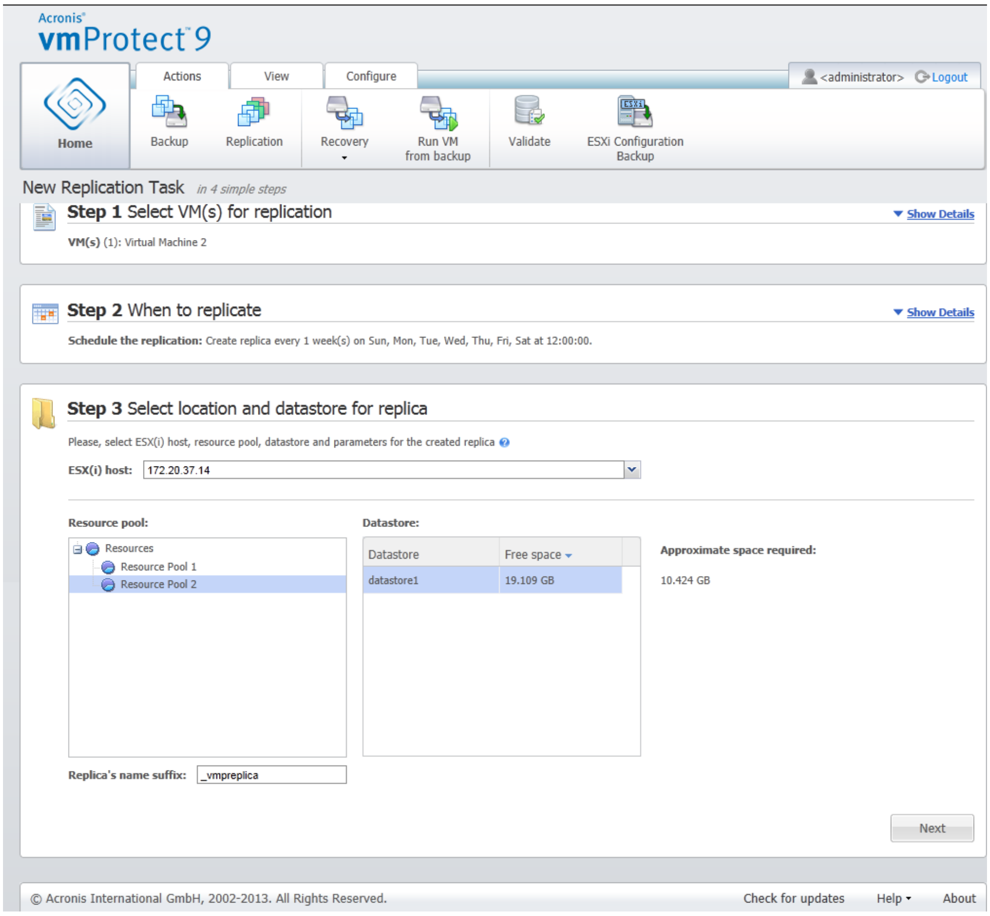
New Replication Task, step 2 "When to replicate"

Replication task scheduling is the same as backup task scheduling. Detailed information on scheduling options as well as scheduling examples can be found in "When to back up" section (p. 31).

After setting up your replication task schedule, click **Next** to go to the next step of the wizard.

## 8.1.3 Select location and datastore for replica

In the third step of the **New Replication Task** wizard you should define the location and datastore for VM replicas. Here, you have to first define the **ESX(i) Host** by selecting one from the drop-down list. Then, select the **Resource Pool** on the destination ESX(i) Host and destination **datastore**.



New Replication Task *in 4 simple steps*

**Step 1** Select VM(s) for replication

**VM(s)** (1): Virtual Machine 2

**Step 2** When to replicate

**Schedule the replication:** Create replica every 1 week(s) on Sun, Mon, Tue, Wed, Thu, Fri, Sat at 12:00:00.

**Step 3** Select location and datastore for replica

Please, select ESX(i) host, resource pool, datastore and parameters for the created replica

**ESX(i) host:** 172.20.37.14

**Resource pool:**

- Resources
  - Resource Pool 1
  - Resource Pool 2

**Datastore:**

| Datastore | Free space |
|---|---|
| datastore1 | 19.109 GB |

**Approximate space required:**

10.424 GB

**Replica's name suffix:** _vmpreplica

© Acronis International GmbH, 2002-2013. All Rights Reserved.

New Replication Task, step 3 “Select location and datastore for replica”

Define the **Replica name's Suffix** to be used when creating the VM replica. The default replica name is “%Machine_Name%_vmpreplica”, where “%Machine_name%” is the original VM name which is being replicated, and “_vmpreplica” is the **Replica name's Suffix**. If a VM with such a name already exists, you'll get a warning prompting you to change the name suffix.

Upon making the selection, click **Next** to proceed to the next step.

## 8.1.4 Replication task options

In the fourth step of the **New Replication Task** wizard you should define your replication task name. Note that [ ] { } ; , . symbols are not allowed for the task name.

For replication task preferences click **More options...**. The following options are available.

### **1)** E-mail notifications**.**

### **2)** SNMP notifications**.**

For details see the Notifications section (p. 41).

### **3)** CBT replication**.**

This option in the **Additional settings** section defines whether to utilize the Changed Block Tracking (CBT) feature of VMware for the virtual machines supporting it. The default setting for CBT replication is: Enabled.

CBT replication keeps track of all the changed blocks inside the virtual machine. This significantly reduces the time for replication. The time is reduced because Acronis vmProtect 9 does not need to check which blocks have changed since the last backup. It gets this information from the VMware API.

**4)** Provisioning mode**.**

Specify the provisioning mode that will be used on the target VM replicas. The modes are **thin provisioning/thick provisioning/flat provisioning/As an original**. The default mode is **Thin provisioning**. Flat provisioning mode is used for ESXi version 5.0+.

When you click on the **Save** button, all your task parameters will be saved and you will see the created task in the **Tasks** view. Clicking on the **Save & Run** button will save the task and run it right away.

# 8.2 Managing replicated VMs

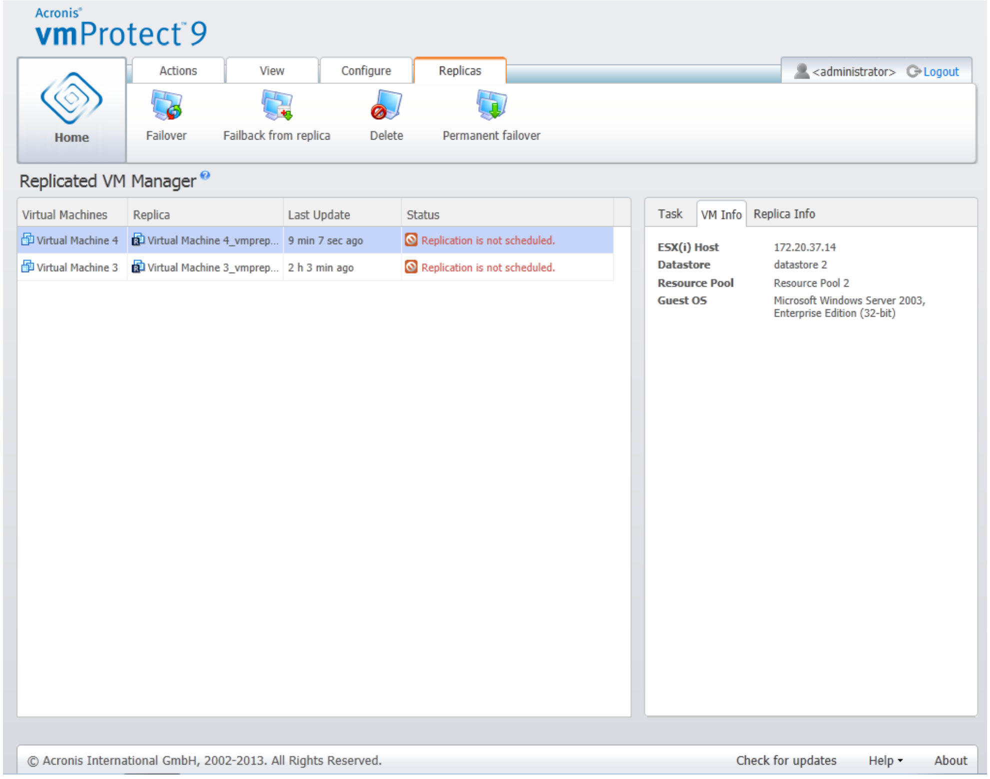
## 8.2.1 Replicated VM Manager

On the Replicas (**View** -> **Replicas**) page you can see all the created replicas that are detected on all the ESX(i) hosts added to the Acronis vmProtect 9 Agent. You can also manage your replicas here.

The replicas list contains information on the original replicated virtual machines, it's replicas, last update times and statuses (Replication scheduled/not scheduled). Select the VM replica to see it's detailed information.

In the **VM Info** tab on the right, you can see the summary information about the original VM for the selected replica:

- **ESX(i) Host** information.
- **Datastore** information.
- **Resource Pool** where original VM is stored.
- **Guest VM** information.



Replicated VM Manager

| Virtual Machines | Replica | Last Update | Status |
|---|---|---|---|
| Virtual Machine 4 | Virtual Machine 4_vmprep... | 9 min 7 sec ago | Replication is not scheduled. |
| Virtual Machine 3 | Virtual Machine 3_vmprep... | 2 h 3 min ago | Replication is not scheduled. |

| | |
|---|---|
| ESX(i) Host | 172.20.37.14 |
| Datastore | datastore 2 |
| Resource Pool | Resource Pool 2 |
| Guest OS | Microsoft Windows Server 2003, Enterprise Edition (32-bit) |

© Acronis International GmbH, 2002-2013. All Rights Reserved.

Replicated VM Manager

On the **Replica Info** tab you can see the summary information on the selected replica:

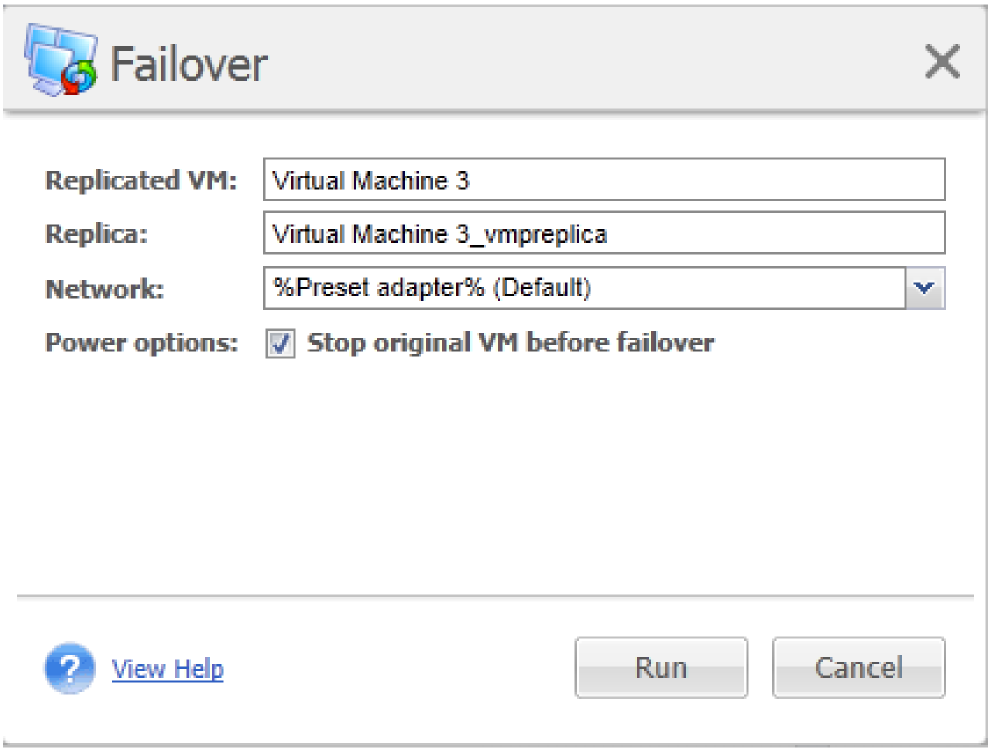
- **ESX(i) Host** information.
- **Datastore** information.
- **Resource Pool** where original VM is stored.

Here, you can also perform the basic operations - **Failover** and **Failback from replica**. The following sections describe these basic operations in detail.

## 8.2.2 Failover

If a replicated virtual machines crashes, you can start it quickly by running replica VM (Failover). The **Failover** feature helps you to get the critical service up and running even before the failed VM is recovered.

Select the replica VM you want to start and click the **Failover** button in the ribbon menu. In the drop-down menu, select if you want to use the network on the replica VM. If the original VM is running, you can choose to **Stop the Original VM before Failover**. Then click **Run**.



Replicated VM: Virtual Machine 3

Replica: Virtual Machine 3_vmpreplica

Network: %Preset adapter% (Default)

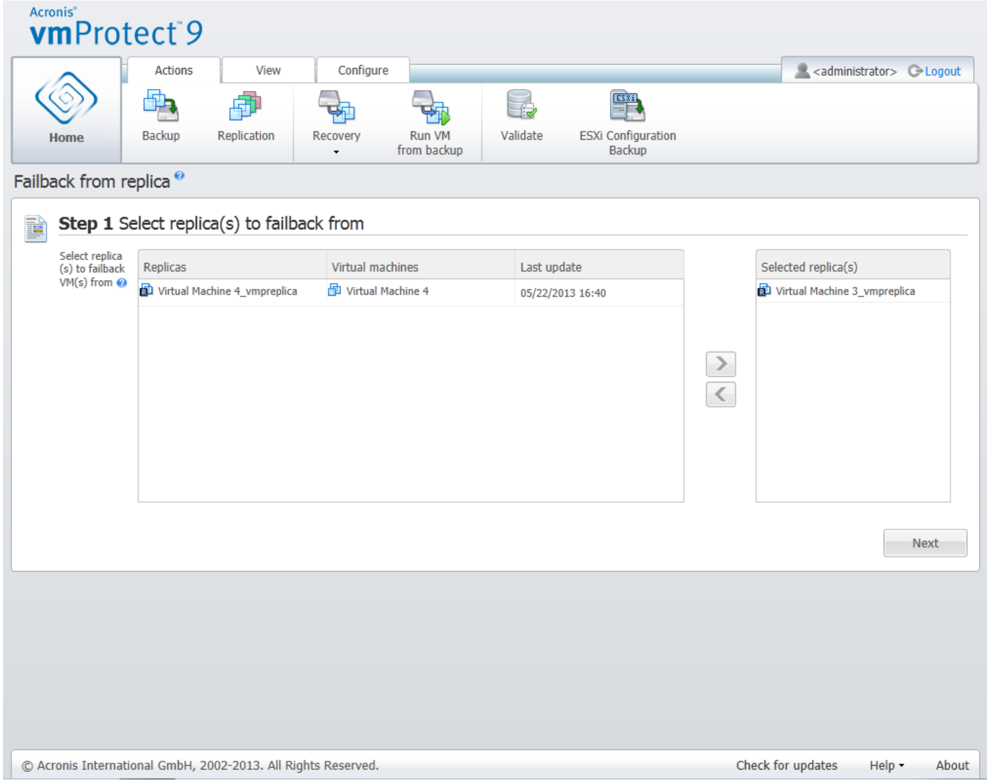
Power options: ☑ Stop original VM before failover

Failover

### 8.2.3 Failback VM from Replica

The failback operation (restoring a VM from replica) allows you to restore your original VM by using the replica VM. This operation can also be used if you decide to stop the replica VM after the **Failover** operation is started and save the changes to the original or new location. Click **Failback from Replica** to start the wizard.

In the first step of the wizard, **Failback from replica**, use the butterfly control to select the replicas you will restore VMs from, then click **Next**.



Failback from replica

**Step 1** Select replica(s) to failback from

Select replica (s) to failback VM(s) from

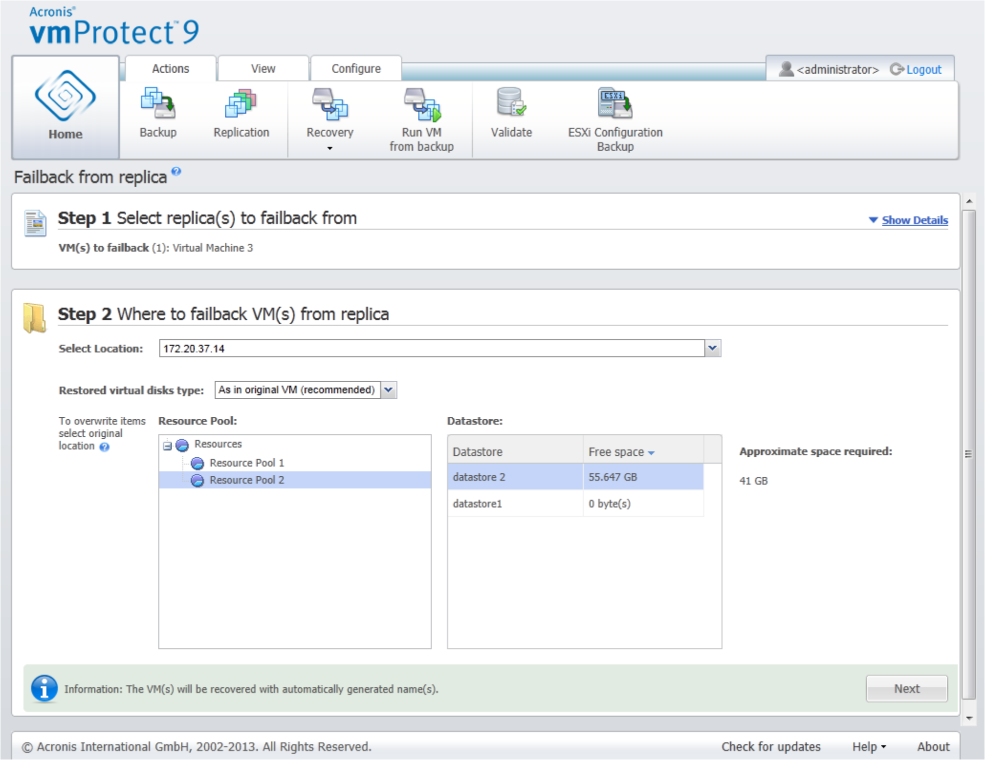
| Replicas | Virtual machines | Last update |
|---|---|---|
| Virtual Machine 4_vmpreplica | Virtual Machine 4 | 05/22/2013 16:40 |

| Selected replica(s) |
|---|
| Virtual Machine 3_vmpreplica |

© Acronis International GmbH, 2002-2013. All Rights Reserved.

Failback from Replica, step 1 “Select Replica(s) to failback from”

In the second step, **Where to failback VM(s) from replica**, select the VM(s) location. You can select the original location and choose to overwrite the original VM(s) or generate new names for the restored VM(s). You can also select a new location. Upon selecting the location, click **Next**.



Failback from replica

**Step 1** Select replica(s) to failback from

VM(s) to failback (1): Virtual Machine 3

**Step 2** Where to failback VM(s) from replica

Select Location: 172.20.37.14

Restored virtual disks type: As in original VM (recommended)

To overwrite items select original location

Resource Pool:

- Resources
  - Resource Pool 1
  - Resource Pool 2

Datastore:

| Datastore | Free space |
|---|---|
| datastore 2 | 55.647 GB |
| datastore1 | 0 byte(s) |

Approximate space required:

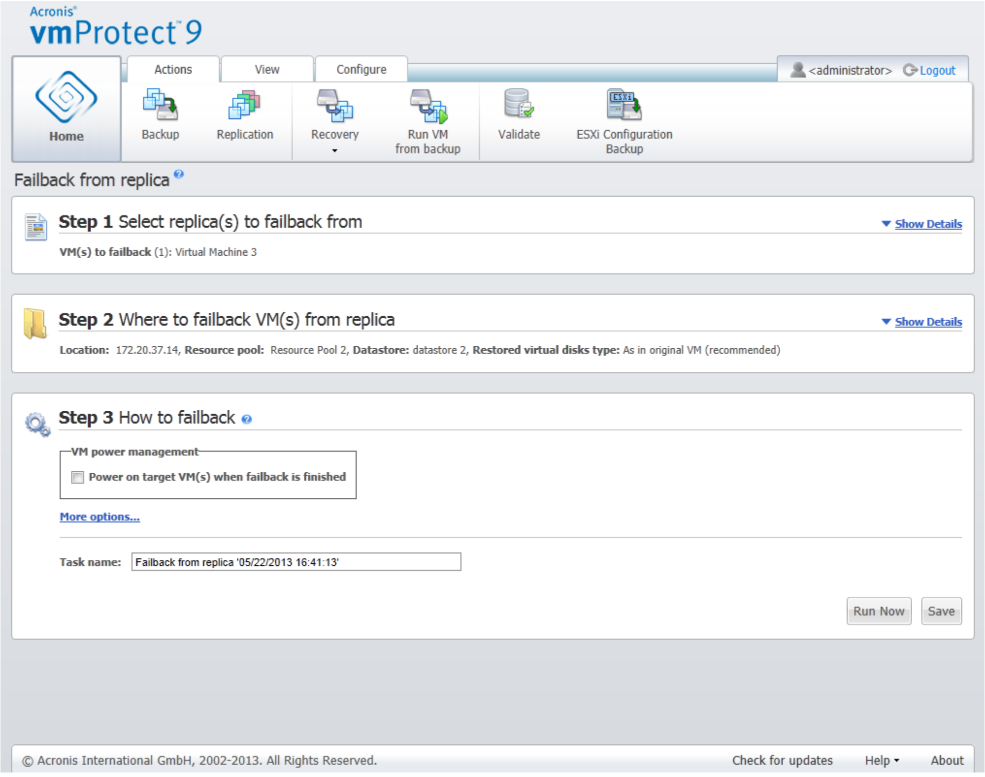
41 GB

Information: The VM(s) will be recovered with automatically generated name(s).

© Acronis International GmbH, 2002-2013. All Rights Reserved.

Failback from Replica, step 2 “Where to failback VM(s) from replica”

In the third step, **How to failback**, select the restore task options. In the **VM power management** block, select the check boxes for **Power off target VMs when starting failback** and **Power on target VMs when failback is finished** and other options. Define the task name.



Failback from replica

**Step 1** Select replica(s) to failback from

**VM(s) to failback** (1): Virtual Machine 3

**Step 2** Where to failback VM(s) from replica

**Location:** 172.20.37.14, **Resource pool:** Resource Pool 2, **Datastore:** datastore 2, **Restored virtual disks type:** As in original VM (recommended)

**Step 3** How to failback

VM power management

□ Power on target VM(s) when failback is finished

**Task name:** Failback from replica '05/22/2013 16:41:13'

Failback from Replica, step 3 “How to failback”

When you click on the **Save** button, all your task parameters will be saved. In the **Tasks** view, you will be able to see the **failback from replica** task which you have created. Clicking on the **Save & Run** button will save the task and run it right away.

In case replica VM is running, the **Failback VM from replica** task is restoring the original VM without stopping the replica VM. Only when the failback is finished, the replica VM is stopped. Finally, the **Failback VM from replica** task recovers the changes from replica VM to the original (new) VM that have been done during the time of the failback operation. It allows to minimize the downtime and to restore the VM state as much as close to its replica state.

## 8.2.4 Deleting Replica VM

Remove a replicated virtual machine by selecting it from the list and clicking the **Delete** button in the ribbon menu.

## 8.2.5 Permanent failover

Permanent failover converts the replica VM into the base virtual machine. Acronis tags will be removed from the .vmx file and this virtual machine will no longer be considered as replica by Acronis vmProtect 9. The existing replication task(s) may fail due to name conflict.

Selecting the **Power on the VM after permanent failover** check box starts the machine. Selecting the **Rename the VM after permanent failover** check box allows to set a new VM name.

# 9 Recovery

## 9.1 Restoring a Backup of Virtual Machines

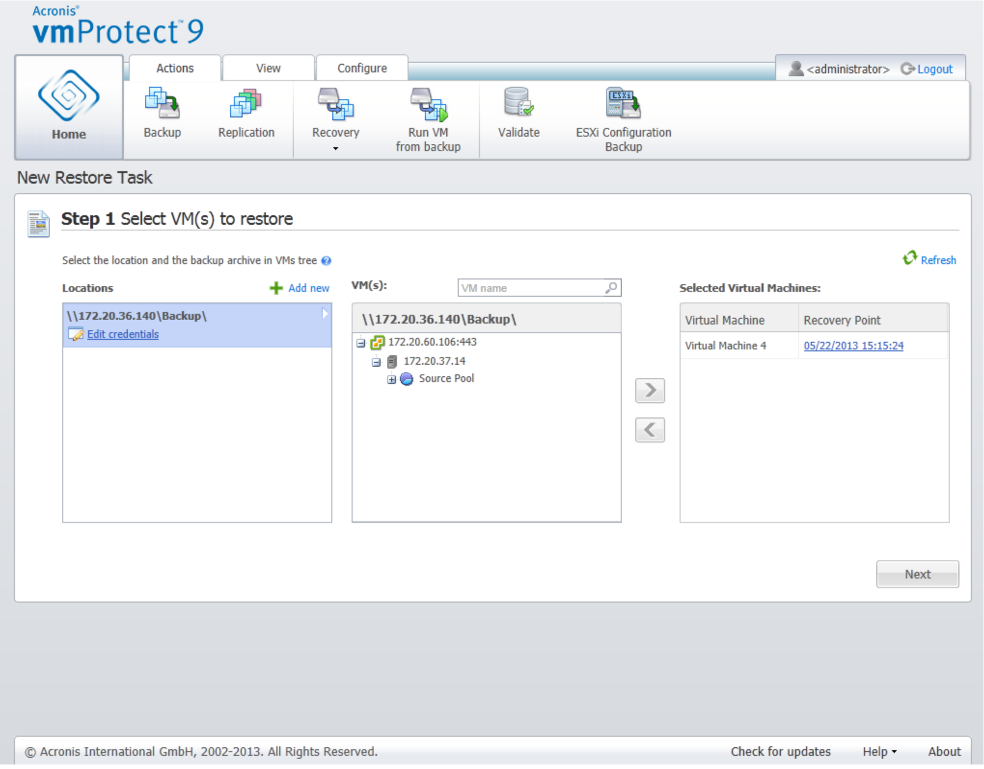
Select the **Recovery** -> **Entire VM** in the **Actions** tab of the main menu to restore one or several backed up virtual machines. The **New Restore Task** wizard opens in the main workspace area and asks you to provide the required information and configure the necessary settings for the new restore task. The wizard consists of the three consecutive steps which appear in the same area:

- Select VM(s) to restore.
- Where to restore.
- How to restore.

These three steps of the restore wizard and their possible options are described below.

### 9.1.1 Select VM(s) to restore

In the first step of the restore backup task wizard, you should define the backup location and select the virtual machines to be recovered. The chosen locations are scanned for the archives presence and contents, which is necessary to define the recovery point(s) for backup restore.



New Restore Task

**Step 1** Select VM(s) to restore

Select the location and the backup archive in VMs tree

Locations: \\172.20.36.140\Backup\ — Edit credentials

VM(s): VM name

\\172.20.36.140\Backup\
- 172.20.60.106:443
  - 172.20.37.14
    - Source Pool

Selected Virtual Machines:

| Virtual Machine | Recovery Point |
|---|---|
| Virtual Machine 4 | 05/22/2013 15:15:24 |

© Acronis International GmbH, 2002-2013. All Rights Reserved.

New Restore Task wizard, Step 1 “Select VM(s) to restore”

Note that if you select an archive which contains an image of a physical machine (when you need to perform “physical to virtual” or P2V migration), there will be no other options provided at this step, because such archives have a single recovery point inside.

If the selected location contains any password-protected archives or archives of physical machines, they are shown in the separate list under the **Encrypted and Physical machines Data**. To restore your data from these archives, you have to specify the password in the **Password** pop-up.

You can select any of the virtual machines from the left side list and move them to the **Selected Virtual Machines** section on the right. The selection of the virtual machines is done by moving the machines from the left side of the butterfly control to the right one by double-clicking it or via the **>** and **<** buttons. The list on the right shows all the virtual machines selected for recovery. The **>** button is used to add the VM to the recovery list, and the **<** button is used to remove the VM from this list. This list contains the selected virtual machines and their latest available recovery point(s), i.e. point(s) in time you can go back to.

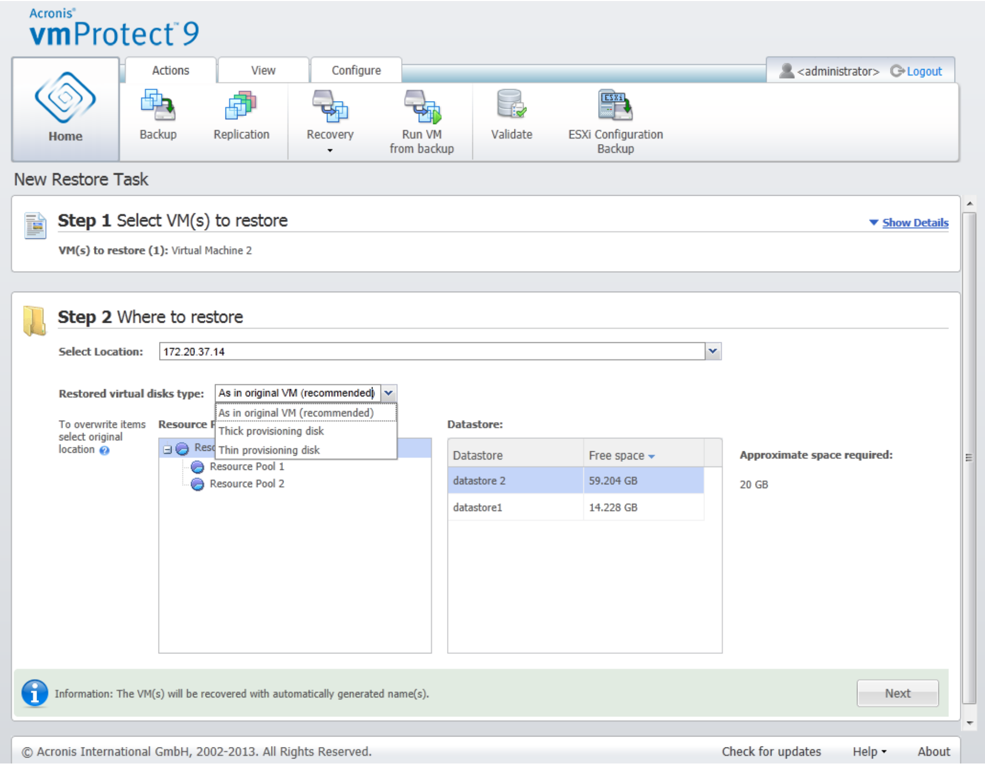
For each virtual machine the latest recovery point is selected by default. This recovery point could be changed by clicking on it. The pop-up window will appear where you can select a different recovery point.

In the Select Recovery Point pop-up you can see the list of all recovery points available for this virtual machine and select the recovery point to be restored. The list includes the name of the archive which includes this recovery point and its creation time.

After you selected "Select VM(s) to restore", click **Next** to finish the first step of the wizard and continue further on.

## 9.1.2 Where to restore

In the second step of the restore backup task wizard, you should define where to restore the selected virtual machine(s) to.



New Restore Task

**Step 1** Select VM(s) to restore

**VM(s) to restore (1):** Virtual Machine 2

**Step 2** Where to restore

**Select Location:** 172.20.37.14

**Restored virtual disks type:** As in original VM (recommended)

To overwrite items select original location

**Resource P**

Reso

Resource Pool 1

Resource Pool 2

**Datastore:**

| Datastore | Free space |
|---|---|
| datastore 2 | 59.204 GB |
| datastore1 | 14.228 GB |

**Approximate space required:**

20 GB

Information: The VM(s) will be recovered with automatically generated name(s).

© Acronis International GmbH, 2002-2013. All Rights Reserved.

New Restore Task wizard, Step 2 "Where to restore"

First of all, with the **Select location** drop-down list you should define the desired destination for your restore task. Please choose if you want to restore the selected virtual machine(s) to their original location or to a different ESX(i) host or datastore. The list shows only those ESX(i) hosts which are managed by Acronis vmProtect 9 Agent. If the ESX(i) host you need is not in this list, then make sure it is added in the **Configure** -> **ESX(i) hosts** view.

When the **Original Location** is selected for restoring VM(s), you can implement the incremental restore mode by selecting the **Use Incremental restore** check box. Incremental restore checks and restores only the blocks that have been changed on the original VM instead of restoring all the data over the virtual machine. This mode can help to increase the speed of recovering from the slow backup locations like Acronis Cloud Storage or other slow connections and help to minimize the traffic during recovering.

Note that the incremental restore mode can be used only if the recovery is performed over the original VM that has been used to create a backup. In case the recovery is performed to a new location or the original VM is missed, a full recovery is performed.

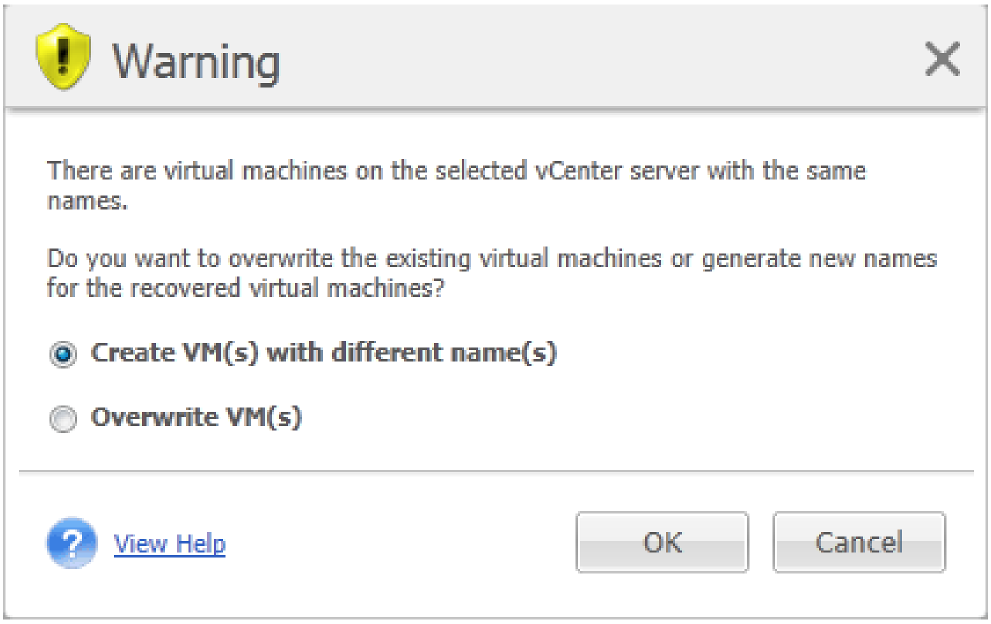
When restoring to **Original Location** the restored VM may not appear in the same location (automatically overwriting the existing VM) as it was at the moment of creating the recovery point. This will be the case if the selected VM (defined by the recovery point) has been migrated to a host and/or datastore, ESX(i) host, resource pool or vApp. Since VMs are preserving their UUIDs during migration, the recovery will go to the current location of the virtual machine. For example, at the moment of creating the recovery point the VM was in vApp1, but later it has migrated to vApp2. Then this VM will be restored to vApp2 overwriting the existing VM.

Once the ESX(i) host is defined, the list of available resource pools and datastores is build up automatically where you can define the exact location for the restored virtual machine(s).

You should also define the format of the restored virtual drives, **As in original VM (recommended)**, **Thick provisioning disk** or **Thin provisioning disk** with the respective drop-down list. Thin provisioning increases the VM storage utilization by enabling dynamic allocation and intelligent provisioning of the physical storage capacity.

Based on this selection, a hint will appear indicating how much space is required on the datastore for the successful recovery operation. You cannot proceed to the next step of the restore backup task wizard until the valid datastore with enough free space is selected.

Note that when restoring multiple virtual machines all of them will be placed to the destination defined at this step of the restore wizard, each to unique new VM on the selected datastore.



Warning

There are virtual machines on the selected vCenter server with the same names.

Do you want to overwrite the existing virtual machines or generate new names for the recovered virtual machines?

● Create VM(s) with different name(s)

○ Overwrite VM(s)

New Restore Task wizard, Step 2 “Where to restore”, overwrite the existing VM confirmation dialog

If there are virtual machines on the selected ESX(i) host or datastore with the same names, you will be asked to confirm overwriting the existing VMs. This choice defines the restored virtual machines naming. If you choose to “Overwrite VMs”, then the existing virtual machines will be replaced with the restored ones.

Note that in this case the datastore selection will be unavailable (since it is already defined by the target VM being overwritten), however, you can change the resource pool location for this VM by choosing corresponding item in the **Resource Pool** selection.

Note that if the existing machines are running, then for the successful recovery operation you should either stop them manually or select the **Power off target VMs when starting recovery** option in the recovery options dialogue (*see “VM power management” section* (p. 60)).

When choosing the **Create VMs with different names** option the restored VMs will be named according to the following convention:

“[Original_VM_name]_DATE”.

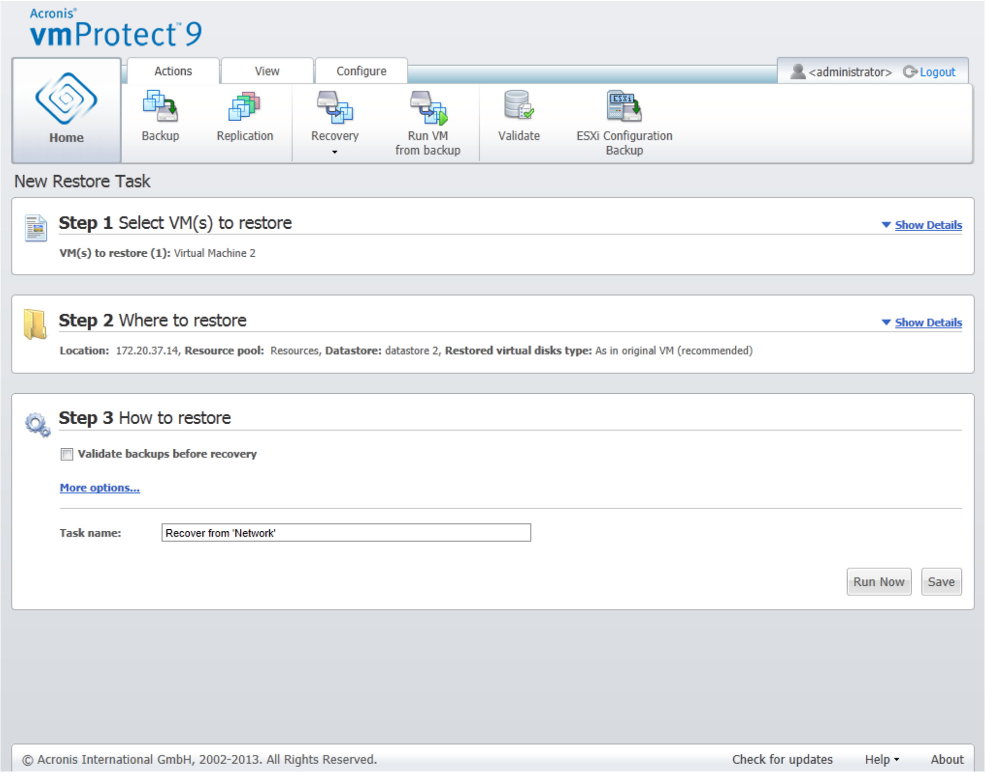
Where “Original_VM_name” is the initial name of the restored virtual machine, and DATE is the current date. For example if the restored VM was called “VM_original” then after recovery it will be named “VM_original_05/25/2011”.

After you completed the selection of “Where to restore”, click **Next** to finish the second step and proceed to the last one.

### 9.1.3 How to restore

In the third step of the restore backup task wizard, you should define the preferences of your recovery task.

Here you can specify whether to validate the archives before the recovery (*for further information on Backup validation, please refer to "Validating backups" section* (p. 90)). Also, here you can adjust the settings for your recovery task by clicking the **More options...** link.



New Restore Task

**Step 1** Select VM(s) to restore

**VM(s) to restore (1):** Virtual Machine 2

**Step 2** Where to restore

**Location:** 172.20.37.14, **Resource pool:** Resources, **Datastore:** datastore 2, **Restored virtual disks type:** As in original VM (recommended)

**Step 3** How to restore

□ **Validate backups before recovery**

More options...

**Task name:** Recover from 'Network'

New Restore Task wizard, Step 3 "How to restore"

To complete the wizard and create the restore backup task you must set up the task name and define how to run it. Note that [ ] { } ; , . symbols are not allowed for the task name.

When you click on **Run Now** button the task will be immediately executed with the specified parameters. You could see the task progress bar in the **Tasks** view and in the **Dashboard** view. This is your choice if you want to execute this task just once. The result of this task will be shown in the **Dashboard** or can be checked through the **Logs** view.

Clicking the **Save** button results in saving the task in the tasks list (**View** -> **Tasks**). This is more convenient if you plan to run this task manually later from the **Tasks view** page or run this task several times.

## 9.1.4 Options

Click **More options...** on the last step of the restore backup task wizard to open the pop-up with the additional settings.

In case of no changes made to the settings, they will retain their respective default values for your current restore task. Note that if later on you change certain settings and save them as default, it will not affect the tasks created with the default settings (these settings will retain the values which were default at the moment of the task creation).

### 9.1.4.1 Notifications

#### 1) E-mail notifications

This option allows setting up the e-mail notifications about the basic events during your restore task, such as successful completion, restore failure or need for user interaction. The default setting for this option is disabled.

Select the **Send e-mail notifications** check box to enable notifications.

Under **Send e-mail notifications** check box select the desired settings as follows:

- **When recovery completes successfully** – to send a notification when the restore task has completed successfully.
- **When recovery fails** – to send a notification when the restore task has failed.
- **Add full log to the notification** – to receive the full log.

Type one or several e-mail addresses where notifications will be sent. Addresses are entered in the **E-mail addresses** field separated by semicolons.

Indicate the desired **Subject** for your notification messages.

- **SMTP server** – enter the name of the outgoing mail SMTP server.
- **Port** – set the port of the SMTP server (the default port value is set to 25).
- **User name** – enter your username.
- **Password** – enter your password.

**From** – type the e-mail address of the user from whom the message will be sent. If you leave this field empty, messages will be sent as if they are from the destination address;

**Use encryption** – you can opt for the encrypted connection to the mail server and choose SSL or TLS encryption types.

Click **Send test e-mail message** to make sure all your settings are correct.

#### 2) SNMP notifications

This option defines whether the agent(s) operating on the managed machine have to send the logs of the restore operation events to the specified Simple Network Management Protocol (SNMP) managers. You can choose the types of events to be sent. The default setting for this option is disabled**.**

Select whether to send the restore operation events log messages to machines running SNMP management applications. Please choose one of the following:

- **Send SNMP notifications individually for restore operation events** – to send the events log of the restore operations to the specified SNMP managers.
  **Types of events to send** – choose the types of events to be sent: Info, Warnings or Errors.
  **Server name or it's IP** – type the name or IP address of the host running the SNMP management application the notifications will be sent to.
  **Community** – type the name of the SNMP community to which both the host running the SNMP

management application and the sending machine belong. The typical community is “public”; Click **Send test message** to make sure all your settings are correct.

- **Do not send SNMP notifications** – to disable sending the events log of the restore operations to SNMP managers.

### 9.1.4.2 Error Handling

These options enable you to specify how to handle errors that might occur during the restore operation. Select the **Re-attempt if an error occurs** check box for enabling the silent mode.

When a recoverable error occurs, the program re-attempts to perform the failed operation. You can set the **Interval between attempts** and the **Number of attempts**. The task finishes as soon as the restore operation succeeds OR the specified number of attempts is reached.

If you select the **Re-attempt if an error occurs** check box, set up the **Number of attempts** and the **Interval between attempts**. This option is enabled by default with the following settings: **Number of attempts** – 5, and **Interval between attempts** – 30 seconds. For example, if the restore network destination becomes unavailable or not accessible, the program will attempt to reach the destination every 30 seconds, but no more than 5 times. The attempts will be stopped as soon as the connection is resumed or if the specified number of attempts is reached.

Select the **Cancel all task operations upon failure** check box, for example, if you need to restore a number of interconnected VMs. Then in case of failure in restoring a single VM, all other restore operations will also be cancelled.

### 9.1.4.3 VM power management

#### Power on target VMs when recovery is finished

This option allows configuring the virtual machines power management after executing the restore backup task.

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

This option is disabled by default. Select the **Power On target VMs when recovery is finished** check box for starting up the virtual machine automatically.

### 9.1.4.4 Additional Settings

#### Use FTP in active mode

It is possible to use FTP active mode for FTP authentication and data transfer. The default setting for **Use FTP in active mode** is disabled.

Enable this option if your FTP server supports active mode and you want this mode to be used for file transfers.

After you finished with all the settings, click **OK** to close the pop-up and apply them for the current restore task only.

#### 9.1.4.5 Exchange Restore Settings

Prior to running **Microsoft Exchange Server Backup Extraction** you have to configure the **Default application extracting settings**. Extracting of mailboxes or mailbox contents requires temporary mounting of a specific VM from the backup. Go to **Application settings** tab and specify the VM mounting parameters.

- ESX(i) host.
- Resource Pool.
- Datastore.

### 9.1.5 Managing created restore task

When editing an existing restore task you will see all the sections (steps) of the wizard you completed while creating you restore task. All three steps of the wizard will appear on the screen at once. (*For further information, please refer to "Managing Tasks" section* (p. 81)).

## 9.2 File Recovery

Sometimes there is a need to recover just a single file or just a few files from a backup archive without restoring the whole virtual machine. The **File Recovery** feature allows browsing the archive and restoring the selected files for the pre-defined version of this archive (recovery point). The recovery destination is defined by the available options provided by the Internet browser which runs the vmProtect 9 Management Console (the dialogue is the same as you see when trying to save some Internet page via **File** -> **Save As…** option).

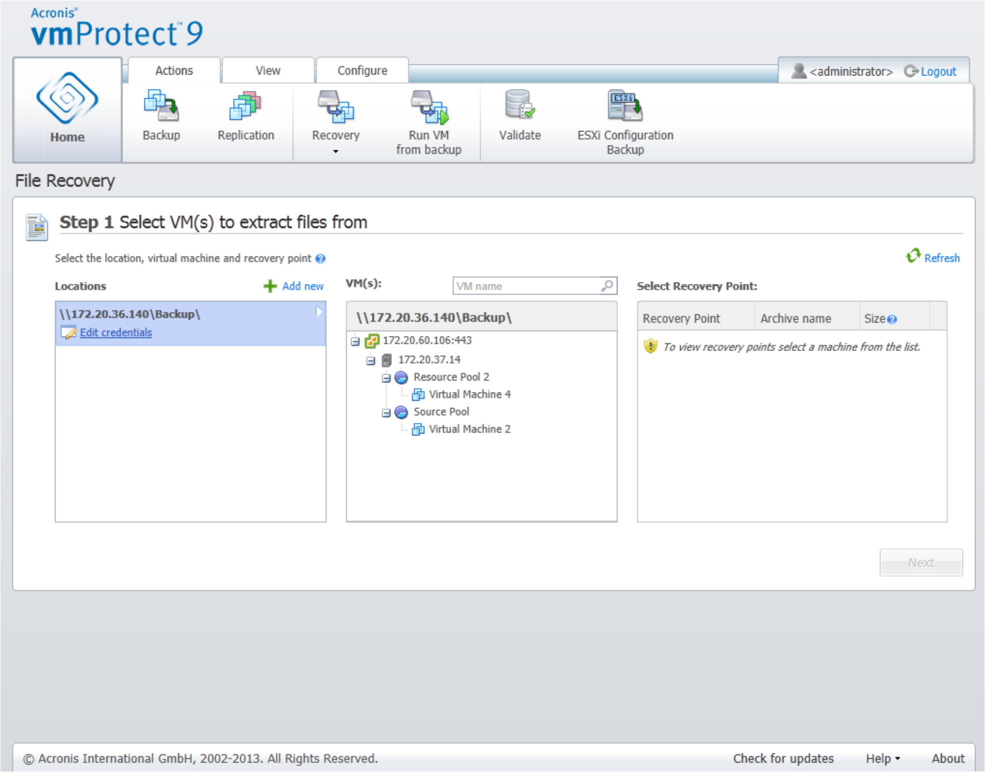
Click **Recovery** -> **Files and folders** in the **Actions** tab of the main menu to restore one or several backed up files. The **File Recovery** wizard opens in the main workspace area and asks you to provide the required information and configure the necessary settings for the file recovery task. The wizard consists of the two steps:

- Select VM(s) to extract files from.
- Explore recovery point.

**NOTE: File Recovery feature is not available for backups saved in Acronis Cloud Backup storage. You can only perform entire VM recovery from this type of backup storage.**

### 9.2.1 Select VM(s) to extract files from

First, you should define your backup location which will be then scanned for archives and their contents.



Step 1 Select VM(s) to extract files from

Select the location, virtual machine and recovery point

\\172.20.36.140\Backup\

\\172.20.36.140\Backup\
- 172.20.60.106:443
  - 172.20.37.14
    - Resource Pool 2
      - Virtual Machine 4
    - Source Pool
      - Virtual Machine 2

*To view recovery points select a machine from the list.*

© Acronis International GmbH, 2002-2013. All Rights Reserved.

File Recovery wizard, Step 1 “Select VM(s) to extract files from”

If the selected location contains any password-protected archives or archives of physical machines (Encrypted and Physical machines Data), you have to specify the password in order to restore your data from these archives.

The selected location is scanned for archives and their contents. As a result of the scan, on the left side you will see a tree-list of the virtual machines included in all archives stored in the selected location or inside the selected archive. By clicking on any virtual machine, you can check the list of all its recovery points on the right side.

For each machine, the latest recovery point is selected by default. The recovery point could be changed by clicking on it. Note that File Recovery allows the selection of just a single Virtual Machine and single recovery point at a time, while the Restore Backup task allows recovery of several VMs.

After selecting the recovery point for the virtual machine you can proceed to the next step. This recovery point defines the virtual machine state which you want to extract files or folders from.

## 9.2.2 Explore Recovery Point

In the second step of the **File Recovery** wizard you have to choose which files or folders to restore. Here you can see the selected VM recovery point contents with a Windows Explorer-like directory browser. In the browsing tree on the left side you can expand the volumes and folders and browse/select the contents of each volume/folder you want to recover on the right side.

Acronis vmProtect 9 **File Recovery** wizard has the built-in search feature. The search box is located in the top right corner above the files and folders list. You can use the search when you don’t know the exact file name you want to restore. You can filter files and folders in the list, and see only those that match any of the search criteria called “file masks”.

You can use one or more wildcard characters “*” and “?” as a file mask, for example: “C:\Finance\*.*”.

Also, you can sort the search results by any of the columns: name, date and time modified, size, and folder. If you select to sort first by a certain field, for example, by time, you can then select to sort by another field, for example, by name. In this case your data will have a sorting of 2 levels, first the name, and then the time. So you can easily find the needed files for recovery.

After you’ve selected all the files you would like to recover, click the **Download** button. You will see the default browser pop-up window (as for the right mouse click -> **Save target as…** pop-up) where you can select the destination for saving the selected backup files. All files and folders you selected will be downloaded there as a single .zip archive.

Note that **File Recovery** cannot be sucessfully done for the file names containing any invalid character: * : ? « < > | / \. For restoring such files please use **Run VM from backup** operation.

## 9.3 Microsoft Exchange Server Backup Extraction

Sometimes there is a need to extract just Exchange data from disk-level backups of Virtual Machines with Microsoft Exchange server installed. The **Extract Microsoft Exchange Server Items** feature allows:

- Extracting complete Exchange databases from VM backups.
- Extracting Exchange data (mailboxes, mailbox items) from VM backups.

***NOTE: Prior to running Extract Microsoft Exchange Server Items wizard you have to configure your backups to become “Application-Aware”. Optionally you can choose to truncate the transactions logs after backup. (For more information, please, refer to “Application-Aware Backup Settings” (p. 36) section).***

Click on the **Recovery** -> **Microsoft Exchange Server Items** button in the **Actions** tab of the main menu to extract the required Exchange items from your backup archive. The **Extract Microsoft Exchange Server Items** wizard consists of the several steps you have to go through in order to complete the operation. The steps of the wizard for extracting Exchange Databases and extracting Exchange mailboxes and mailbox contents are described in the sections below.

### 9.3.1 Extracting Databases

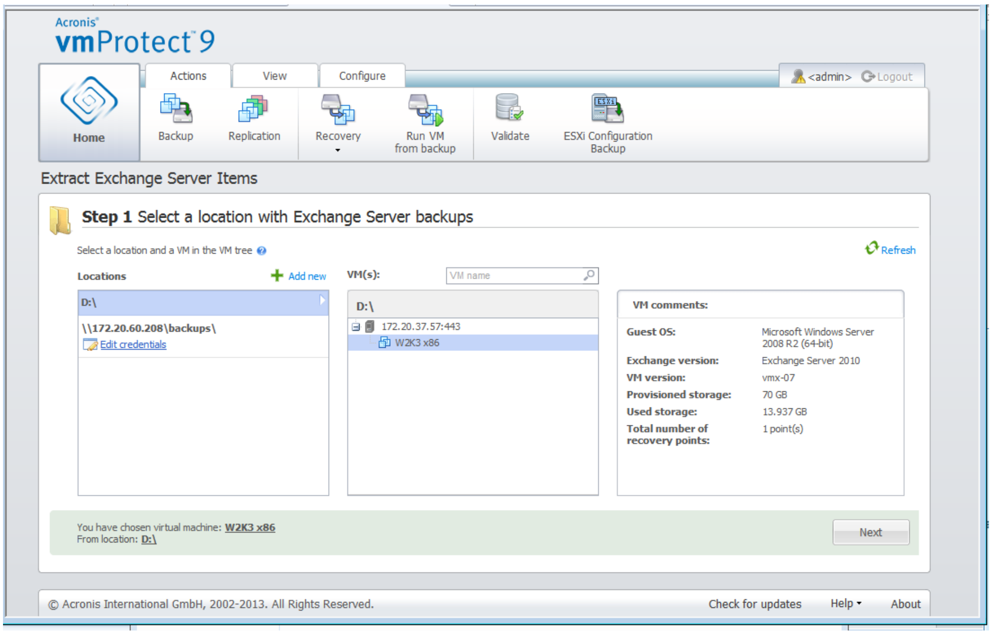
When choosing to extract Databases, you can extract the MS Exchange server databases in .edb format saving it over to a network share.

Recovering databases to the specified folder means that the database files along with transaction log files are extracted from the backup to a folder you specify. This can be useful if you need to extract data for audit or further processing by third party tools; or when you are looking for a workaround to mount the databases manually.

To extract Exchange databases you have to go through the following four steps:

1. **Select location with Exchange Server backups**.
2. **What do you want to extract?** (**Databases**).
3. **Select Databases and Recovery Point**.
4. **Where to extract Database?**

On the first step you have to select a location and a VM with Exchange Server backups. On the left you can see the list of backup locations. When choosing a location it is then scanned for Exchange VM backups which you see in the middle section. Select the VM you need to extract Exchange Databases from. On the right you can see the summary information. Then click **Next**.



Extract Exchange Server Items

**Step 1** Select a location with Exchange Server backups

Select a location and a VM in the VM tree

**Locations**

D:\

\\172.20.60.208\backups\

Edit credentials

**VM(s):** VM name

D:\

172.20.37.57:443

W2K3 x86

**VM comments:**

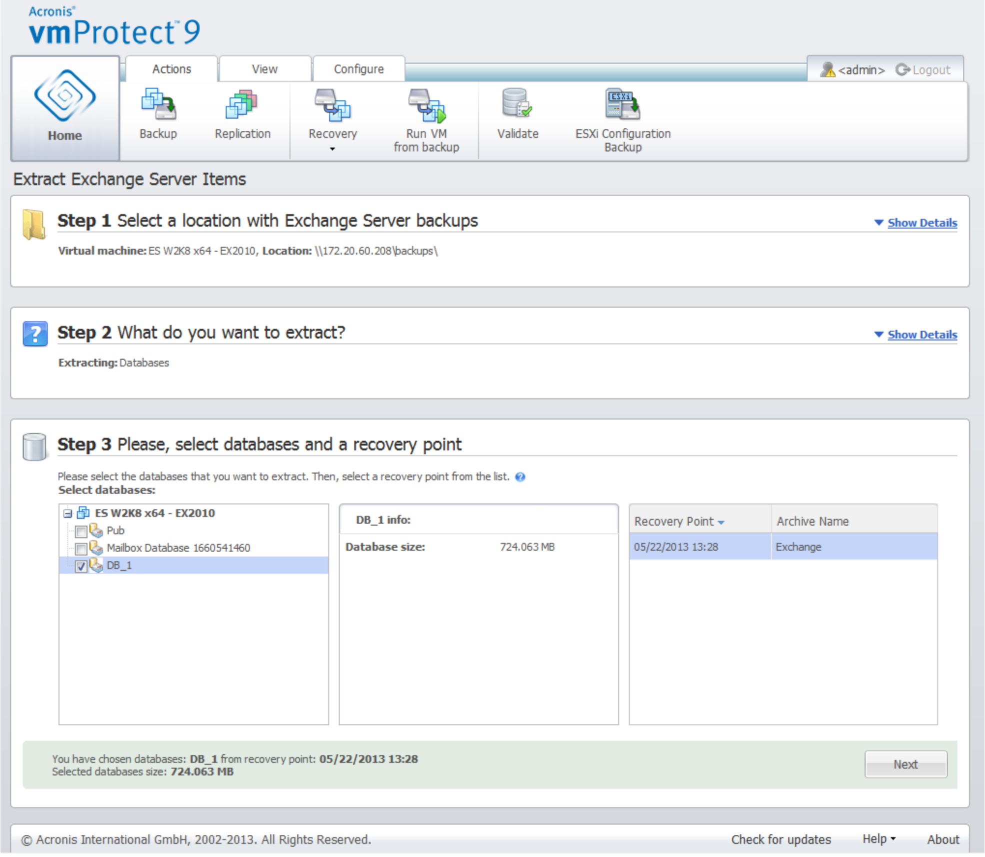
| | |
|---|---|
| **Guest OS:** | Microsoft Windows Server 2008 R2 (64-bit) |
| **Exchange version:** | Exchange Server 2010 |
| **VM version:** | vmx-07 |
| **Provisioned storage:** | 70 GB |
| **Used storage:** | 13.937 GB |
| **Total number of recovery points:** | 1 point(s) |

You have chosen virtual machine: **W2K3 x86**
From location: **D:\**

© Acronis International GmbH, 2002-2013. All Rights Reserved.

Extract Exchange Servet Items, Selecting a lication with Exchange Server backups

Select **Databases** on the second step. On the third step select your Exchange Server databases from the list on the left, and then select the recovery point on the right. By default, the latest recovery point is selected. Here you can see the information on the selected recovery point, database and its size. Click **Next**.



Extract Exchange Server Items

**Step 1** Select a location with Exchange Server backups

**Virtual machine:** ES W2K8 x64 - EX2010, **Location:** \\172.20.60.208\backups\

**Step 2** What do you want to extract?

**Extracting:** Databases

**Step 3** Please, select databases and a recovery point

Please select the databases that you want to extract. Then, select a recovery point from the list.

**Select databases:**

**ES W2K8 x64 - EX2010**
- □ Pub
- □ Mailbox Database 1660541460
- ☑ DB_1

**DB_1 info:**

**Database size:** 724.063 MB

| Recovery Point | Archive Name |
|---|---|
| 05/22/2013 13:28 | Exchange |

You have chosen databases: **DB_1** from recovery point: **05/22/2013 13:28**
Selected databases size: **724.063 MB**

© Acronis International GmbH, 2002-2013. All Rights Reserved.

Extract Exchange Servet Items, Selecting databases and a recovery point

Finally, click **Browse** and select the destination folder where to save the database archive. Click **Finish** to proceed with extraction.

The extracted databases will be in a **Dirty Shutdown** state and cannot be mounted. To be able to mount the databases you have to bring them to a **Clean Shutdown** state by using the **Eseutil /r <Enn>** command. **<Enn>** specifies the log file prefix for the database (or storage group that contains the database) into which you need to apply the transaction log files. For instructions on how to do this, refer to:

- http://technet.microsoft.com/en-us/library/dd876926.aspx
- http://technet.microsoft.com/en-us/library/aa998340(EXCHG.80).aspx

## 9.3.2 Extracting Mailboxes

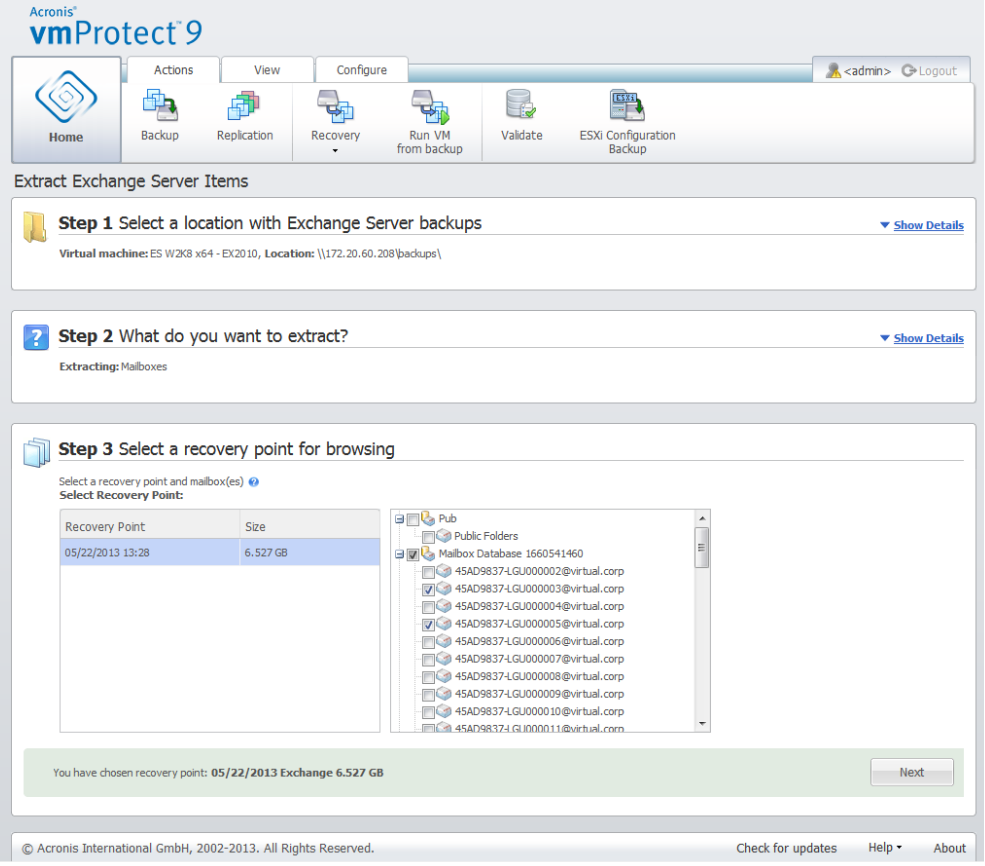
When choosing to extract **Mailboxes** you can extract specific Microsoft Exchange server mailboxes by going through the following steps:

1. **Select location with Exchange Server backups**.
2. **What do you want to extract?** (**Mailboxes**).
3. **Select Recovery Point for browsing and mailbox(es)**.
4. **Where to save selected Items**.

On the first step you have to select the location and a VM with Exchange Server backups. On the left you can see the list of backup locations. When choosing a location it is then scanned for Exchange VM backups which you see in the middle section. Select the VM you need to extract mailboxes from. On the right you can see the summary information. Click **Next**.

Select **Mailboxes** on the second step. If there is another active **Exchange items extraction** task you will get a pop-up warning to continue. In order to continue the current Exchange items browsing operation that already started task have to be terminated. Confirm stopping the other task to continue.

On the third step select the recovery point on the left. By default, the latest recovery point is selected. On the right browse the Exchange server and select the mailbox(es) you want to extract. Then click **Next**.



Extract Exchange Server Items

**Step 1** Select a location with Exchange Server backups

**Virtual machine:** ES W2K8 x64 - EX2010, **Location:** \\172.20.60.208\backups\

**Step 2** What do you want to extract?

**Extracting:** Mailboxes

**Step 3** Select a recovery point for browsing

Select a recovery point and mailbox(es)

**Select Recovery Point:**

| Recovery Point | Size |
|---|---|
| 05/22/2013 13:28 | 6.527 GB |

- □ Pub
  - □ Public Folders
- ☑ Mailbox Database 1660541460
  - □ 45AD9837-LGU000002@virtual.corp
  - ☑ 45AD9837-LGU000003@virtual.corp
  - □ 45AD9837-LGU000004@virtual.corp
  - ☑ 45AD9837-LGU000005@virtual.corp
  - □ 45AD9837-LGU000006@virtual.corp
  - □ 45AD9837-LGU000007@virtual.corp
  - □ 45AD9837-LGU000008@virtual.corp
  - □ 45AD9837-LGU000009@virtual.corp
  - □ 45AD9837-LGU000010@virtual.corp
  - □ 45AD9837-LGU000011@virtual.corp

You have chosen recovery point: **05/22/2013 Exchange 6.527 GB**

© Acronis International GmbH, 2002-2013. All Rights Reserved.

Extract Exchange Servet Items, Selecting a recovery point for browsing

On the final step click **Browse** to select the destination folder where to save the selected items, and click **Finish** to proceed with the extraction. Upon completing the wizard, the extraction task is created which you can see in the **Tasks** view (**View** -> **Task**) You will be able to track the progress and other statistics for your task. Note that it is not possible to edit this type of task.

Extracting mailboxes requires starting a temporary virtual machine directly from backup's selected recovery point which might take a few minutes. You could see the mounting operation progress. In case mounting failed, you might see the log and cancel the task.

Note that this temporary VM stays mounted for 15 minuted. If you leave the **Extract Exchange Server Items** wizard and then start it back again, you'll be opt to **Continue browsing the previously selected recovery point**.

The selected **Mailboxes** are saved to the specified destination as the Acronis vmProtect 9 self-extractible (.exe) archive. You can run this file on any machine which has Microsoft Outlook (2003+) installed in order to extract the e-mails and other items in .pst format.

When unpacking the data from the archive you can also select the contents to be extracted and indicate the folder where to exctract the data to. Click **Extract** to see the progress. The data will be extracted into a .pst file which can be opened by Microsoft Outlook (**File** -> **Open**). Note, that the machine where you run the extracting process should have Microsoft Outlook installed (since MAPI is required).

### 9.3.3 Extracting Mailboxes content

When choosing to extract **Mailboxes Content** you can browse mailboxes to extract specific content - folders and items - by going through the following steps:

1. **Select location with Exchange Server backups**.
2. **What do you want to extract?** (**Mailboxes Content**).
3. **Select Mailbox(es) for extraction or Recovery Point for browsing**.
4. **Select Folders or Items for extraction**.
5. **Where to save selected Items**.

On the first step you have to select the location and a VM with Exchange Server backups. On the left you can see the list of backup locations. When choosing a location it is then scanned for Exchange VM backups which you see in the middle section. Select the VM you need to extract mailboxes & mailboxes contents from. On the right you can see the summary information. Click **Next**.

Select **Mailboxes Content** on the second step.

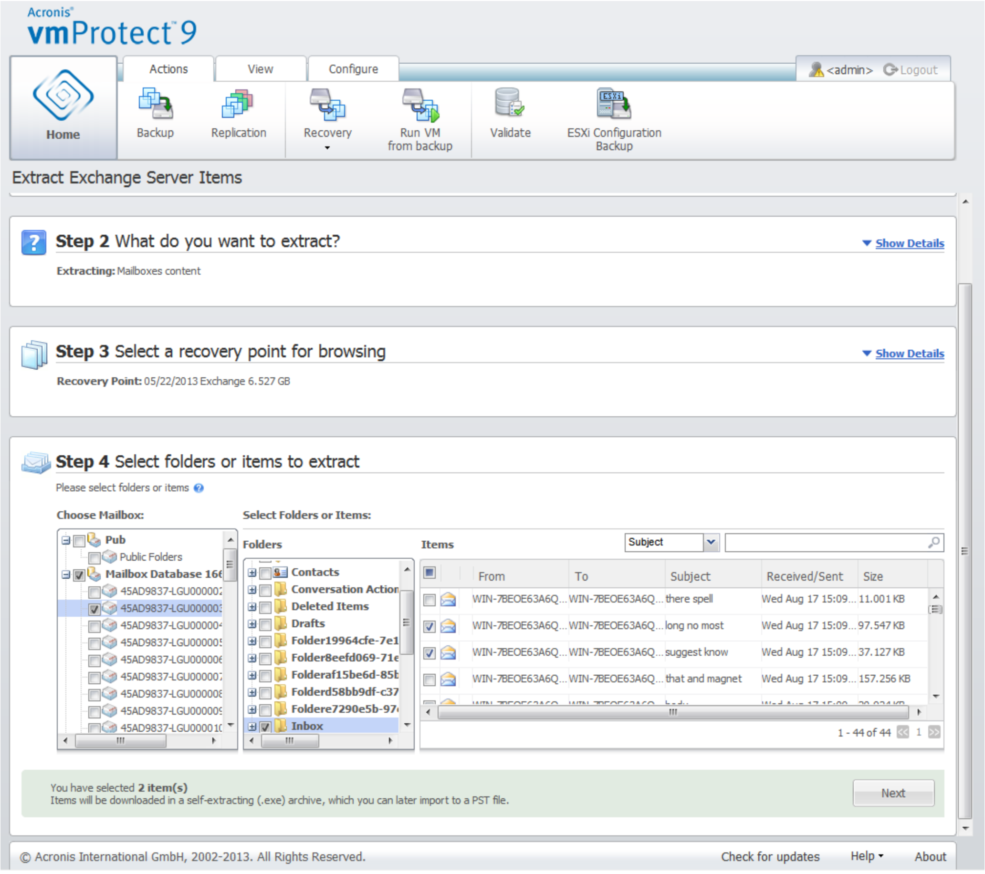
On the third step select the recovery point on the left. By default, the latest recovery point is selected.

On the fourth step click **Browse E-mails** to select the specific mailbox content you want to extract. Browsing the mailbox contents requires starting a temporary virtual machine directly from backup's selected recovery point which might take a few minutes. You could see the mounting operation progress. Upon successful completion you can select the mailbox(es) contents. In case mounting failed, you might see the log and cancel the task.

Note that this temporary VM stays mounted for 10 minutes. If you leave the **Extract Exchange Server Items** wizard and then start it back again, you'll be opt to **Continue browsing the previously selected recovery point**.

The selection of the mailbox(es) contents on the fourth step is as follows. The list of the available mailbox(es) is on the left side. Choose the mailbox, and you will see all its contents as folders and items. Select all the items you would like to extract. You can repeat the items selection with other mailboxes. When you're done, click **Next**.

On the final step click **Browse** to select the destination folder where to save the selected items, and click **Finish** to proceed with the extraction. You will see the Exchange items extract information pop-up.



Extract Exchange Server Items

**Step 2** What do you want to extract? ▼ Show Details

**Extracting:** Mailboxes content

**Step 3** Select a recovery point for browsing ▼ Show Details

**Recovery Point:** 05/22/2013 Exchange 6.527 GB

**Step 4** Select folders or items to extract

Please select folders or items

**Choose Mailbox:**

- ☐ **Pub**
  - ☐ Public Folders
- ☑ **Mailbox Database 166**
  - ☐ 45AD9837-LGU000002
  - ☑ 45AD9837-LGU000003
  - ☐ 45AD9837-LGU000004
  - ☐ 45AD9837-LGU000005
  - ☐ 45AD9837-LGU000006
  - ☐ 45AD9837-LGU000007
  - ☐ 45AD9837-LGU000008
  - ☐ 45AD9837-LGU000009
  - ☐ 45AD9837-LGU000010

**Select Folders or Items:**

**Folders**

- ☐ **Contacts**
- ☐ **Conversation Action**
- ☐ **Deleted Items**
- ☐ **Drafts**
- ☐ **Folder19964cfe-7e1**
- ☐ **Folder8eefd069-71e**
- ☐ **Folderaf15be6d-85b**
- ☐ **Folderd58bb9df-c37**
- ☐ **Foldere7290e5b-97**
- ☑ **Inbox**

**Items** Subject

| | From | To | Subject | Received/Sent | Size |
|---|---|---|---|---|---|
| ☐ | WIN-7BEOE63A6Q... | WIN-7BEOE63A6Q... | there spell | Wed Aug 17 15:09... | 11.001 KB |
| ☑ | WIN-7BEOE63A6Q... | WIN-7BEOE63A6Q... | long no most | Wed Aug 17 15:09... | 97.547 KB |
| ☑ | WIN-7BEOE63A6Q... | WIN-7BEOE63A6Q... | suggest know | Wed Aug 17 15:09... | 37.127 KB |
| ☐ | WIN-7BEOE63A6Q... | WIN-7BEOE63A6Q... | that and magnet | Wed Aug 17 15:09... | 157.256 KB |

1 - 44 of 44 1

You have selected **2 item(s)**
Items will be downloaded in a self-extracting (.exe) archive, which you can later import to a PST file.

Next

© Acronis International GmbH, 2002-2013. All Rights Reserved. Check for updates Help About

Extract Exchange Servet Items, Selecting destination for saving items

The selected **Mailboxes & Mailboxes Contents** are saved to the specified destination as the Acronis vmProtect 9 self-extractible (.exe) archive. You can run this file on any machine which has Microsoft Outlook (2003+) installed in order to extract the e-mails and other items in .pst format.

When unpacking the data from the archive you can also select the contents to be extracted and indicate the folder where to exctract the data to. Click **Extract** to see the progress. The data will be extracted into a .pst file which can be opened by Microsoft Outlook (**File** -> **Open**). Note, that the machine where you run the extracting process should have Microsoft Outlook installed (since MAPI is required).

## 9.4 Microsoft SQL Server Databases Extraction

The **Extract Microsoft SQL Server Databases** feature helps to restore an SQL database from disk-level backups of Virtual Machines with Microsoft SQL server installed.

***NOTE: Prior to running Extract Microsoft SQL Server Databases wizard you have to configure your backups to become "Application-Aware". Optionally you can choose to truncate the transactions logs after backup. (For more information, please, refer to "Application-Aware Backup Settings" (p. 36) section).***

Click on the **Recovery** -> **Microsoft SQL server** button in the **Actions** tab of the main menu to extract the required SQL databases from your backup archive. The **Extract Microsoft SQL Server Databases** wizard consists of the several steps you have to go through in order to complete the operation.

On the first step of the wizard you have to select a location and a VM with MS SQL Server backups in the VM tree. On the left you can see the list of backup locations. When choosing a location it is then scanned for VM(s) with MS SQL Server backups which you see in the middle section. Select the VM you need to extract MS SQL Server Database(s) from. On the right you can see the summary information. After finishing the selection, click **Next**.

On the second step you need to select the databases from the list on the left, and then select the recovery point on the right. By default, the latest recovery point is selected. Here you can see the information on the selected recovery point, database and its size. Upon completing the step, click **Next**.

On the final step click **Browse** and select the destination folder where to save the database archive. Click **Finish** to proceed with extraction.

## 9.5 Microsoft SharePoint Server Data Extraction

Here are the instructions for extracting your SharePoint Server Data. First, go to **Actions** -> **Recovery** -> **Microsoft SQL Server Databases** and proceed with extraction of Microsoft SQL Server database that contains the SharePoint data.

Then, download and install the Acronis SharePoint Explorer tool from the link on **Actions** -> **Recovery** -> **Microsoft SharePoint Data** page. It will be a separate .msi installation package which you can install on the machine running Microsoft SQL Server where the examined databases should be attached to for Microsoft SharePoint data extraction. The detailed installation and data extraction instructions you can find in a separate Acronis SharePoint Explorer help available after running the .msi installation package.

# 10 Running VM from Backup

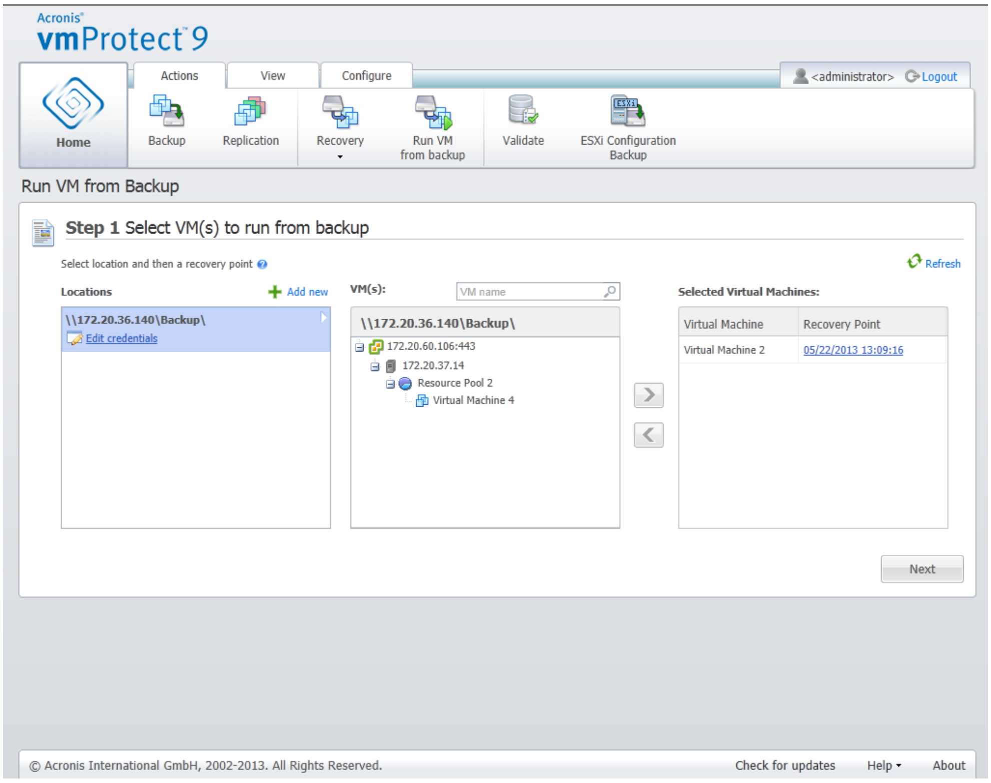
Click **Run VM from Backup** in the **Actions** tab of the main menu to mount certain backed up virtual machine without restoring it. The **Run VM from Backup** wizard opens in the main workspace area and asks you to provide the required information and configure the necessary settings for the **Run VM from Backup** task. The wizard consists of the three steps:

- Select VM(s) to run from backup.
- Where the VM(s) will be run.
- Additional settings.

These three steps of the **Run VM from Backup** wizard and their options are described below.

## 10.1 Select VM(s) to run from backup

In the first step of the **Run VM from Backup** wizard, you should first define the backup location and make a selection of the virtual machines to be run. The chosen locations are scanned for archives and their contents. This is necessary to pick up the recovery point(s) which will define the state of the virtual machine you want to run from backup. Running VM from backup process is also referred to as "mounting a virtual machine".



Run VM from Backup

**Step 1** Select VM(s) to run from backup

Select location and then a recovery point

Locations: \\172.20.36.140\Backup\ — Edit credentials

VM(s): \\172.20.36.140\Backup\

```
172.20.60.106:443
  172.20.37.14
    Resource Pool 2
      Virtual Machine 4
```

Selected Virtual Machines:

| Virtual Machine | Recovery Point |
|---|---|
| Virtual Machine 2 | 05/22/2013 13:09:16 |

© Acronis International GmbH, 2002-2013. All Rights Reserved.

Run VM from Backup wizard, Step 1 "Select VM(s) to run from backup"

Note that for Run Vm from Backup locations, you can only select **Network folders** or **Local folders**. Other locations, such as **Cloud backup storage** or **FTP/sFTP servers**, are not available here.

If the selected location contains any password-protected archives or archives of physical machines, then the VMs included in these archives cannot be shown, and you will be warned about it. You can select any of the virtual machines from the left side list and move them to the **Selected Virtual Machines** section on the right. The selection of the virtual machines is done by moving the machines from the left side of the butterfly control to the right one by double-clicking it or via the **>** and **<** buttons. The list on the right shows all the virtual machines selected for mounting. The **>** button is used to add the VM to this list, and the **<** button is used to remove the VM from the list. This list contains the selected virtual machines and their latest available recovery points, i.e. points in time you can go back to.

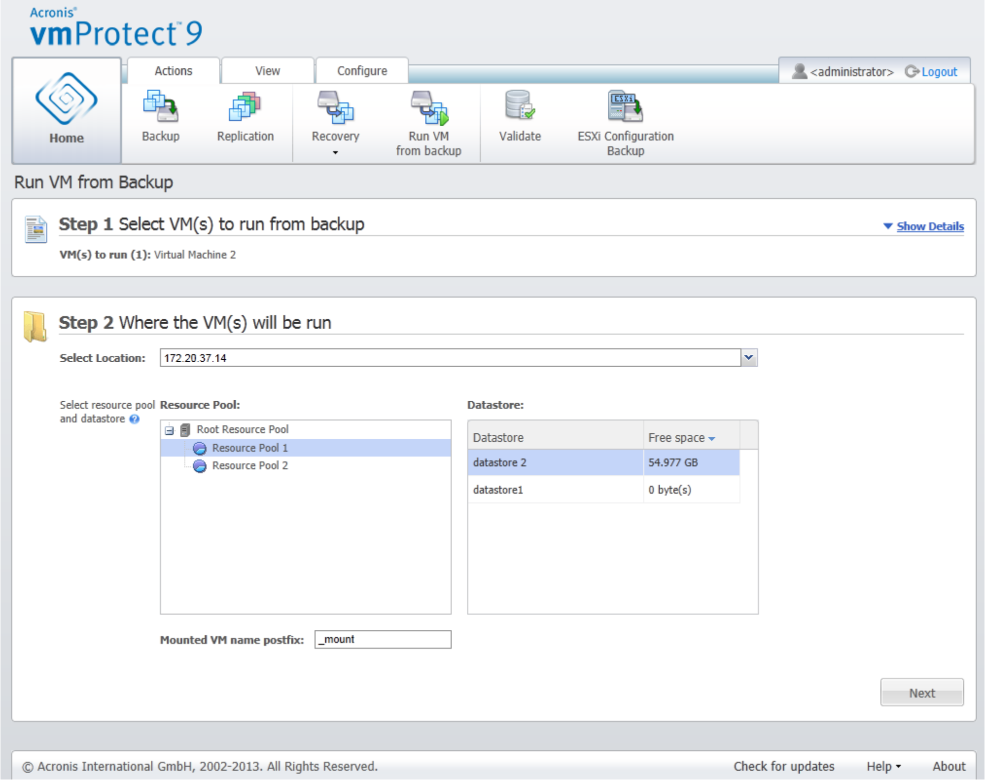
For each virtual machine the latest recovery point is selected by default. This recovery point could be changed by clicking on it. The pop-up window will appear where you can select a different recovery point.

In the **Select Recovery Point** pop-up you can see the list of all recovery points available for this virtual machine and select the recovery point to be mounted. The list includes the timestamps of the recovery points, the file name of the archive which includes this recovery point and its size.

After you selected VM(s) to run from backup, click **Next** to finish the first step of the wizard and continue further on.

## 10.2 Where the VM(s) will be run

In the second step you should define where to run the selected virtual machine(s).



Run VM from Backup

Step 1 Select VM(s) to run from backup

VM(s) to run (1): Virtual Machine 2

Step 2 Where the VM(s) will be run

Select Location: 172.20.37.14

Select resource pool and datastore

Resource Pool:

- Root Resource Pool
  - Resource Pool 1
  - Resource Pool 2

Datastore:

| Datastore | Free space |
|---|---|
| datastore 2 | 54.977 GB |
| datastore1 | 0 byte(s) |

Mounted VM name postfix: _mount

© Acronis International GmbH, 2002-2013. All Rights Reserved.

Run VM from Backup wizard, Step 2 “Where the VM(s) will be run”

First of all, with the **Select Location** drop-down list you should define the ESX(i) host where you want to mount the selected VMs on. The list shows only those ESX(i) hosts which are managed by Acronis vmProtect 9 Agent. If the ESX(i) host you need is not in this list, then make sure it is added in the **Configure** -> **ESX(i) hosts** view.

Once the ESX(i) host is defined, the list of available resource pools is build up automatically where you can define the exact location for the mounted virtual machine(s). The datastore selection is necessary to define where to store the changes made to the mounted virtual machine(s).

Note that when mounting multiple virtual machines all of them will be placed to the destination defined at this step of the **Run VM from backup** wizard, each to one particular resource pool. The changes made to these VMs will be saved to unique folder on the selected datastore.

Also, note that Acronis vmProtect 9 Agent is compatible with vMotion (Storage vMotion in particular). When the mounted VM is moved to another datastore via Storage vMotion, then upon unmounting it will remain in its new location. In this case the mounting process will be similar to backup restore since during vMotion all data is physically moved to the new datastore.

Please, specify the postfix for the mounted virtual machine name in the **Mounted VM name postfix** field. This is necessary since running two virtual machines with the same name on one ESX(i) host is not possible, especially when there is the original VM already running on it. The mounted VM will be named using the following convention:

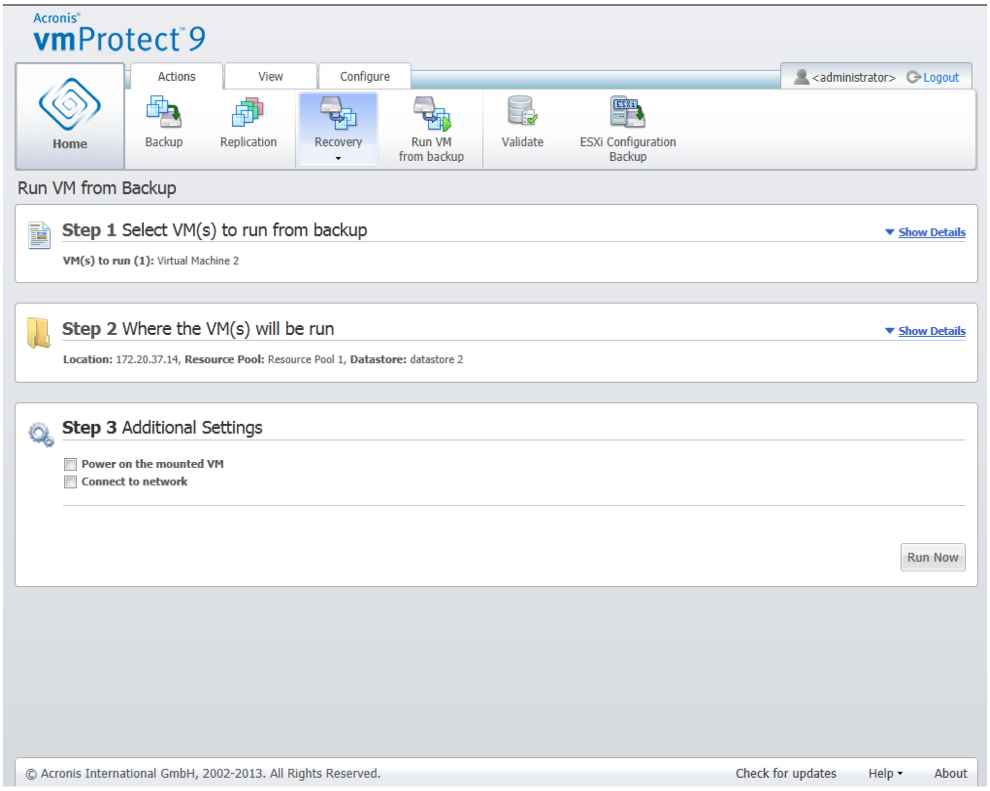
“[Original_VM_name]_mount”.

Where “Original_VM_name” is the original name of the mounted virtual machine and “_mount” is the postfix you can change. For example, if the mounted VM had the “VM_original” name then after mounting it will be named “VM_original_mount”.

After you selected where the VM(s) will be run, click **Next** to finish the second step and proceed to the last one.

## 10.3 Additional Settings

In the third step of the wizard you can select the check boxes for the **Power on the mounted VM** and **Connect to network** options.



Run VM from Backup

**Step 1** Select VM(s) to run from backup

**VM(s) to run (1):** Virtual Machine 2

**Step 2** Where the VM(s) will be run

**Location:** 172.20.37.14, **Resource Pool:** Resource Pool 1, **Datastore:** datastore 2

**Step 3** Additional Settings

□ Power on the mounted VM
□ Connect to network

Run VM from Backup wizard, Step 3 “Additional Settings”

Select the **Power on the mounted VM** option to automatically run your machine upon completion of the wizard. Note that the mounted machine's replica (e.g. the original machine) might appear on the network. Theerefore, for safe operation, it’s advisable to power on the mounted virtual machine manually after taking the necessary precautions.

Select the **Connect to network** check box when mounting a failed VM which is no longer present in the network. If you are mounting a VM for testing purposes (to ensure some data consistency inside) while the original VM is currently running, keep this check box cleared. Before you power on a VM, you should manually change the VM network configuration settings to disconnect it from the production network and re-connect to an isolated non-production network to avoid possible conflicts.

After clicking on the **Run Now** button, the selected VM will appear in VMware Infrastructure Client and you will be able to manage it like any other virtual machine in your environment. In order to dismount (stop running) the VM you should go to the **View** -> **Mounted VMs** view.

## 10.4 Managing created “Run VM from Backup” activity

There is no way to edit the existing **Run VM from Backup** activity. You can only unmount the mounted VMs from the **View** -> **Mounted VMs** page.

Besides **Unmount**, there is also an **Unmount and Save** option which shuts down the mounted VM and when the machine is stopped it incrementally backs up it's changes. Note that if the machine cannot be stopped during 5 minutes it shuts down (powers off) forcibly.

# 11 P2V Migration

## 11.1 How to Perform a P2V Migration

To reduce hardware requirements, there is often a need to migrate physical machines to virtual ones. To perform a physical to virtual migration (P2V), you need to boot your physical machine from Acronis bootable Media, create a full backup and then restore it to a virtual machine.

To perform a P2V migration the following steps are to be made:

1. Create Acronis Bootable Media. Download the Acronis Bootable Media Builder of Acronis vmProtect 9 from the My products & Downloads section of your account at the Acronis website. Install it.
2. Boot the physical machine that you need to migrate to virtual from Acronis Bootable Media.
3. Create a full backup of the physical machine.
4. Run Acronis vmProtect 9 web console, connect to the Acronis Agent and click **Restore** on the **Actions** tab.
5. Select the created backup and choose the target ESX(i) host where to restore the backup.

# 12 Bare Metal Recovery of ESXi Hosts

The Acronis vmProtect 9 Bare Metal Recovery (BMR) of the ESXi host feature provides a totally unique functionality that helps you minimize the recovery time if the ESXi server crashes, fails to start or doesn’t work properly after a patch update. The feature allows you to restore ESXi server binaries and patches, ESXi configuration, and missing VMs (VMs present in backups, but missing on the datastores; VMs should be backed up separately) after the ESXi server is recovered and started.

Bare Metal Recovery supports only VMware ESXi version 4.1, 5.0 and 5.1, and does not support ESX.

The following sections describe how **ESXi host configuration backup** and recovery can be configured.

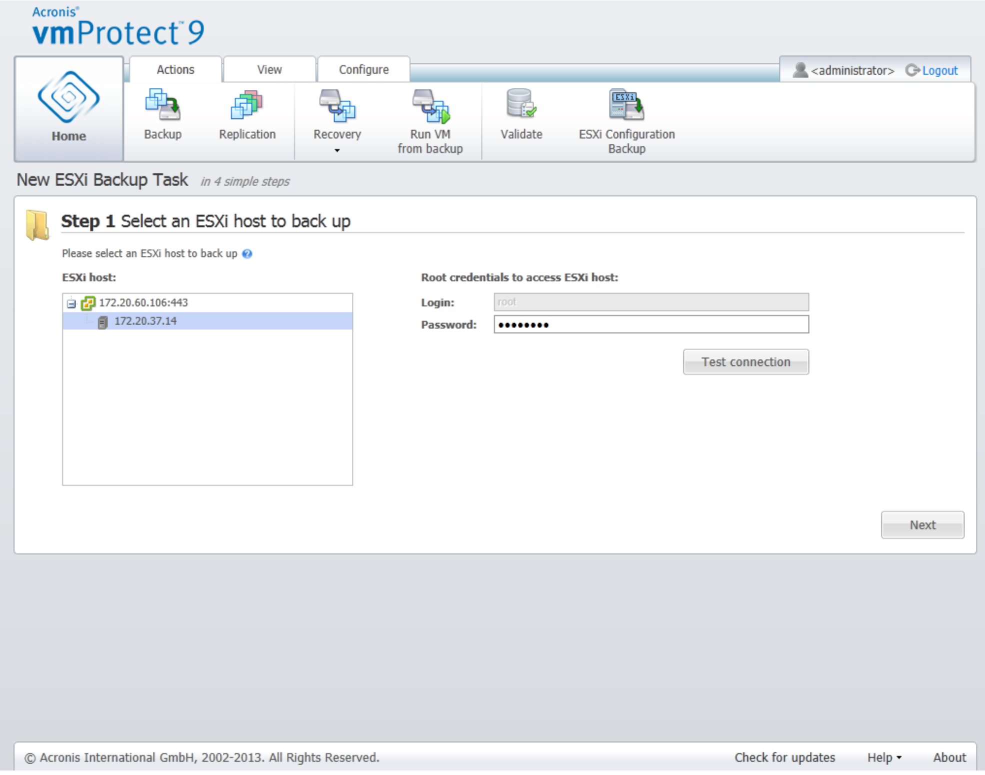
## 12.1 ESXi host configuration backup

**ESXi host configuration backup** in Acronis vmProtect 9 differs from the backup of Virtual Machines.

**Note that the ESXi host configuration backup will forcibly enable SSH access for the ESXi host, i.e. its configuration will automatically be adjusted in order to enable ESXi configuration backups.**

To back up an ESXi host configuration, run the **New ESXi Backup Task** wizard by clicking **Actions** -> **ESXi Configuration Backup**. In the first step of the **New ESXi Backup Task** wizard (**Select an ESXi host to back up**), select the ESXi host whose configuration you want to back up. Select the ESXi host from the list of all ESXi hosts/vCenter managed by Acronis vmProtect 9 Agent. If you don’t see the exact host that you are looking for in the **ESXi hosts** list, make sure that it's added at the **Configure** -> **ESX(i) Hosts** page. Note that **ESXi backup** supports only ESXi servers. ESX servers cannot be selected for backup.

After selecting the ESXi host, enter the root credentials (login/password) to access it. In order to create a backup of ESXi binaries and patches, a connection to the ESXi server is performed via SSH. This means that root credentials are required. You can check that the submitted credentials are valid by clicking **Test connection**. Click **Next**.



New ESXi Backup Task *in 4 simple steps*

**Step 1** Select an ESXi host to back up

Please select an ESXi host to back up

**ESXi host:**

- 172.20.60.106:443
  - 172.20.37.14

**Root credentials to access ESXi host:**

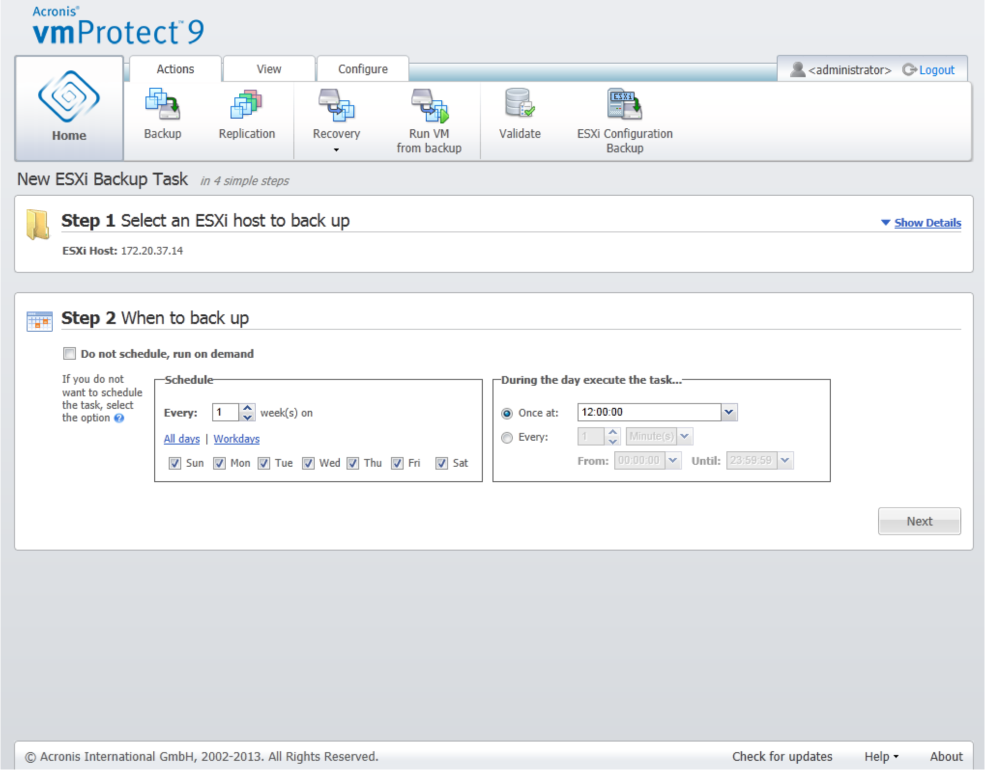
**Login:** root

**Password:** ••••••••

© Acronis International GmbH, 2002-2013. All Rights Reserved.

New ESXi Backup Task, Select an ESXi Host to back up

In the second step (**When to Backup**), you can schedule the backup. The options of the BMR backup task scheduler are the same as for the VM backup wizard.



New ESXi Backup Task *in 4 simple steps*

**Step 1** Select an ESXi host to back up

**ESXi Host:** 172.20.37.14

**Step 2** When to back up

☐ **Do not schedule, run on demand**

If you do not want to schedule the task, select the option

**Schedule**

**Every:** 1 week(s) on

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

**During the day execute the task...**

● Once at: 12:00:00

○ Every: 1 Minute(s)

**From:** 00:00:00 **Until:** 23:59:59

© Acronis International GmbH, 2002-2013. All Rights Reserved.

New ESXi Backup Task, When to back up

In the third step (**Where to back up**), select the location for storing your ESXi configuration backup archive and archive name. Click **Browse** to open the pop-up, select the location among one of the following and then click **OK**:

- **Local folders**.
- **Network folders**.
- **FTP servers**.
- **SFTP servers**.

ESXi backup is created only in the Multiple files backup scheme (legacy mode archive) (p. 9). The **Save all backups in one file (Recommended)** option is disabled.

Select **Automatically delete old backups** check box to set up the clean up rules. The details for these settings are explained in the "Where to back up" section (p. 32).

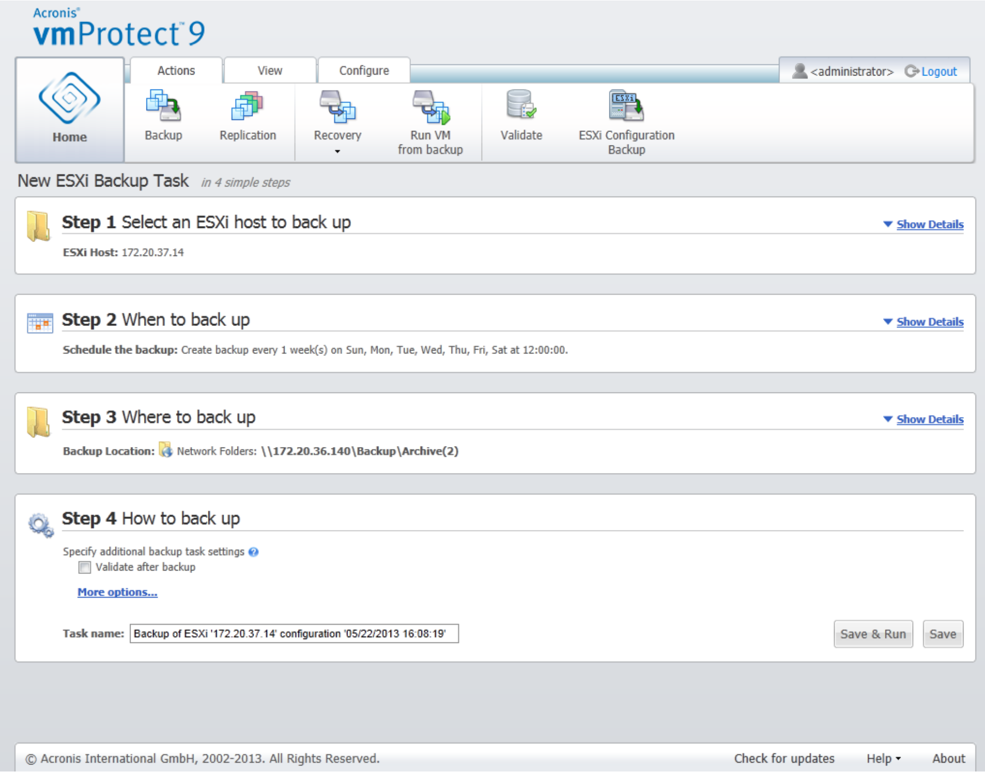
Select **Copy the backup to a second location** check box. The following settings allow you to configure the backup copying options. Select the second location where you would also like to store your backups and the **archive name**. Click Browse and select from the available list of locations.

From the **When to copy** drop-down list select if you would like to copy the backup to the second location immediately after each backup is created. Or you can indicate the specific days for performing your backup copy, other than the backup schedule days. In this case you can also choose to **copy all missed recovery points** or **copy last created recovery points only**.

The **Copy last created recovery points** option might be useful when the first location selected is sometimes unreachable. In case the **Copy all missed recovery points** option is selected and the retention rules for the first storage are executed on the main location, then the software deletes the recovery points that should be removed by these rules, even if these recovery points were not copied to the second location. So when the retention rules are executed it is not checked if the recovery points were already copied to the second storage or not.

By default, the backup type and the clean up rules for the copied backups are the same as the respective primary backup settings. Meanwhile, you can choose to specify different settings, for example, change the clean up rules options.

In the final step (**How to Backup**), select the **Validate after backup** check box, if necessary. Click **More options...** to open the pop-up with additional settings. These options are described in the Backup options (p. 38) section. Note that the following options will be unavailable: **Archive Protection**, **Additional Settings** -> **Deduplication**, **Additional Settings** -> **CBT backup**.



New ESXi Backup Task *in 4 simple steps*

**Step 1** Select an ESXi host to back up

**ESXi Host:** 172.20.37.14

**Step 2** When to back up

**Schedule the backup:** Create backup every 1 week(s) on Sun, Mon, Tue, Wed, Thu, Fri, Sat at 12:00:00.

**Step 3** Where to back up

**Backup Location:** Network Folders: **\\172.20.36.140\Backup\Archive(2)**

**Step 4** How to back up

Specify additional backup task settings

□ Validate after backup

**Task name:** Backup of ESXi '172.20.37.14' configuration '05/22/2013 16:08:19'

© Acronis International GmbH, 2002-2013. All Rights Reserved.

New ESXi Backup Task, How to back up

To complete the **New ESXi Backup Task** wizard, you should name the task. Note that [ ] { } ; , . symbols are not allowed for the task name. The default task name is “Backup of ESXi configuration [date/time]”.

When you click on the **Save** button, all the parameters of your **New ESXi Backup Task** will be saved and you will see the created task in the **Tasks** view. Clicking on the **Save & Run** button will save the task and run it right away.

## 12.2 ESXi host configuration recovery

ESXi host configuration recovery (BMR restore) can be used to quickly recover the ESXi server when, for example, it crashes and cannot be booted. **ESXi Host Restore** wizard allows you to configure the recovery of the previous configuration of the ESXi host stored in a previously created backup. Through the wizard you can check and reconfigure local datastores (datastores created on local disks) and remap vSwitches that were previously mapped to physical NICs. Also, you can define which backup locations should be used for the recovery of the missing VMs after the ESXi host is restored and boots up.

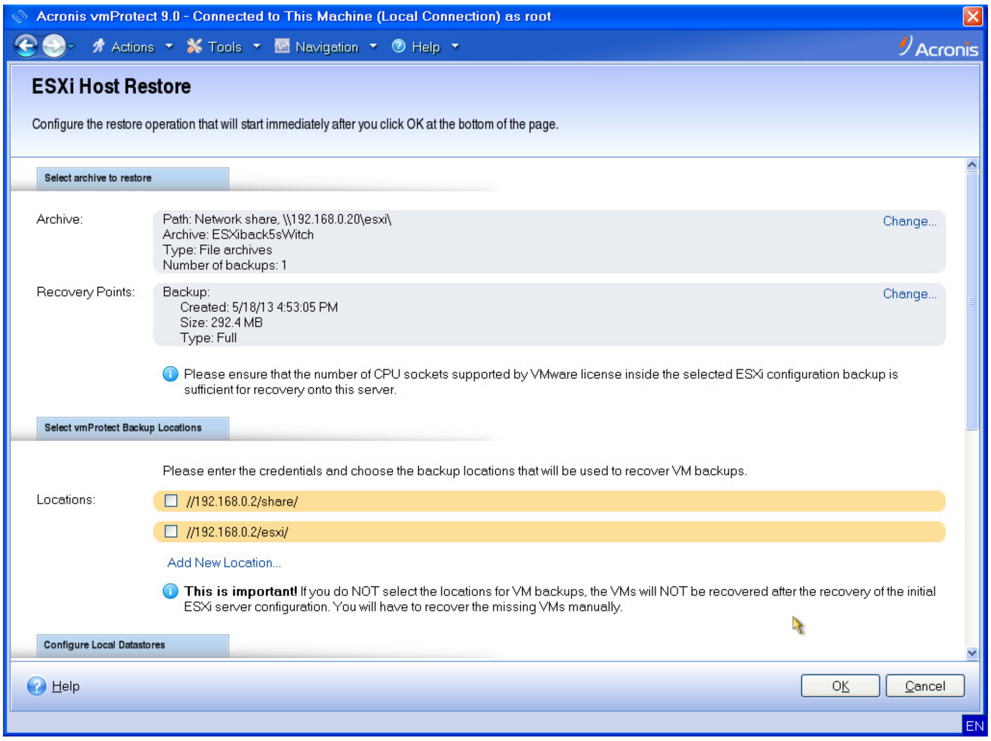
**ESXi Host Restore** wizard is available from Acronis Bootable Media interface only. The media can be created by Acronis Bootable Media Builder. It is a separate installation package. This functionality cannot be run from the Acronis vmProtect 9 Agent Web Interface.

In the first step select the **Archive** and the **Recovery Point** that will be restored. Open the pop-up and select the location where the ESXi host configuration backup archive is stored. Then, select the **Archive** with the **ESXi Host Backup**. When the archive is selected, the latest recovery point is chosen by default. However you can change the default selection.

The second step is to **Select vmProtect 9 Backup Locations**. Select the check box for the backup location and enter its credentials in the pop-up window. The locations are listed. The selected locations are colored grey and the locations that are not selected are colored yellow.

Locations are listed according to the contents of the ESXi host configuration backup archive, where the information about VMs backup locations is stored (**Recent Locations** paths). You can add new locations in this step. All these locations will be used to restore VMs backups after the ESXi host is up and running. Moreover, the locations can be password protected and the credentials will be required to access data after the ESXi server is recovered and Acronis vmProtect 9 starts to recover the missing VMs. Only the following locations can be selected in this step:

- **Network folders**.
- **FTP servers**.
- **SFTP servers**.


Acronis vmProtect 9.0 - Connected to This Machine (Local Connection) as root
Actions
Tools
Navigation
Help
Acronis
Select archive to restore
Change...
Change...
Select vmProtect Backup Locations
Add New Location...
Configure Local Datastores
Help
OK
Cancel
EN

ESXi Host Restore

Configure the restore operation that will start immediately after you click OK at the bottom of the page.

Archive: Path: Network share, \\192.168.0.20\esxi\
Archive: ESXiback5sWitch
Type: File archives
Number of backups: 1

Recovery Points: Backup:
Created: 5/18/13 4:53:05 PM
Size: 292.4 MB
Type: Full

Please ensure that the number of CPU sockets supported by VMware license inside the selected ESXi configuration backup is sufficient for recovery onto this server.

Please enter the credentials and choose the backup locations that will be used to recover VM backups.

Locations:
☐ //192.168.0.2/share/
☐ //192.168.0.2/esxi/

**This is important!** If you do NOT select the locations for VM backups, the VMs will NOT be recovered after the recovery of the initial ESXi server configuration. You will have to recover the missing VMs manually.

ESXi Host Configuration Recovery

Note, if you do not select the VMs backup locations here, these VMs will not be recovered automatically after the recovery of the initial ESXi server configuration. In this case, you will have to recover the missing VMs manually.

Also note, that unpredictable issues may occur if you restore ESXi host configuration to a new machine while the original ESXi host is active and managed by a vCenter. Before doing so please remove the original ESXi host from vCenter and add it back after performing the recovery.

The third step is to **Configure Local Datastores**. Because the original ESXi server can become faulty or the system hard disk drive and the datastore can be lost, the destination configuration may differ from the original server.

The list shows the detected HDDs and their size. Here you can see the datastores already present on the detected HDDs. If the datastore on HDDs matches with the datastore in the original configuration (stored inside the ESXi configuration backup), its name appears in green. If the datastore is detected but does not match the original configuration, its name appears in yellow. If the detected datastore is going to be cleaned up for a new datastore creation, its name appears in red. Select the **Use for new datastores** check box to use the HDD for a new datastore creation.

The new datastore will be created on all the disks selected on this step overwriting any existing data on these disks. Therefore, you should carefully verify the selection.

The ESXi system partitions will be created on the disk which you check under "Restore ESXi to:" column. You can select the detected local or flash drive(s) here.

The fourth step is to **Configure Virtual Network**. This step is required to map the vSwitches present in the ESXi configuration backup being restored to physical NICs. You can recover the ESXi configuration backup on the same server or on different hardware. This step allows the following:

- By default, automatic mapping is used. The current hardware is scanned for NICs in order to automatically match them with the vSwitches present in the ESXi configuration backup. You may check the automatic mapping of the vSwitches and remap them if required.
- During the ESXi recovery process you can check if the cable is plugged to the vmnicX or not.

After going through all the steps, click **OK** to start the recovery. Here's what happens after you proceed with the recovery:

1. The first HDD (by BIOS order) is used to create ESXi system partitions and then the system will be rebooted into the ESXi environment.
2. Upon boot-up, the ESXi executes a special script which configures the vSwitches and datastores according to the settings specified in the ESXi configuration recovery wizard.
3. Acronis vmProtect 9 Agent (Virtual Appliance) is deployed to the newly created datastore. Then, it executes the recovery of the missing virtual machines from the backup locations specified in the ESXi configuration recovery wizard. It also scans these backup locations for the source ESXi host VMs backed up after the ESXi configuration backup and restores these virtual machines.

- A virtual machine is considered "missing", if it is not detected in any of the datastores currently recognized by the restored ESXi host.
- The virtual machines are restored to all the detected datastores steadily filling them up and leaving there at least 10% of the free space.

# 13 Managing Tasks

Click **Tasks** in the **View** tab of the main menu to open the **Tasks** page (**View** -> **Tasks**), where you can see the details and perform the operations with your tasks. Note that the **Tasks** page allows performing the basic operations with the existing tasks only, and doesn't let you create new tasks (for creating a new Backup/Restore/Validation/etc. task you have to go to the **Home** tab of the main tool bar).

The page presents a general list of all the tasks created in Acronis vmProtect 9 Agent. The tasks list contains the Backup, Restore, Validate, etc. operations which were created at the respective sections of the **Home** tab in the main tool bar.

The task list presents the following information about the task:

- **Task name** – the unique task identifier.
- **Task type** – *Backup*, *Restore, Validation*, etc.
- **Last finish time** – the time passed since this task finished last.
- **Next run** – the time when the task will be run or *Manual*.
- **Status** – *Idle* or *In Progress.*

Tasks that are currently stopped appear as "idle" ones. If the task is currently running, then the **Status** field shows the progress of the current activity in percentage (e.g. 35%).

Moreover, all the tasks which have already been executed have the last result status – **Succeeded** (last run was successful), **Warning** (the task finished with warnings at the last run) or **Error** (the task ended in failure last time). You can see the task logs by clicking the last result status. Those tasks which were not run yet don't have this status, and have the **Last finish time** field empty.

You can sort the tasks by selecting the sort criterion from the drop-down list in the top right corner. You can sort the tasks by its **Creation time**, **Last finish time**, **Last result**, **Name**, **Next start time**, **Status** and **Task type** in the ascending or descending order.

On the **Tasks** management page you can **Run**, **Cancel**, **Edit** or **Delete** any of the tasks in the list by using the respective buttons (*please, see subsections below*).

You can check the details for any of the tasks in the list by viewing the **Summary** and **Source and Target** tabs (*please, see "Viewing task details" section* (p. 82)).

## 13.1 Running a task

You can run the selected idle task by clicking the **Run** button. Upon running, the status of the task will be changed from "**Idle**" to "**Running**" with the progress bar and the current percentage of the task's completion.

Note that you can only view task logs (*see "Viewing task logs" section* (p. 82)) and **Cancel** (*see "Cancelling a task" section* (p. 82)) the active running task. Other control buttons – **Run**, **Edit** and **Delete** – are disabled. In order to edit or delete the active task, you have to stop it first.

## 13.2 Cancelling a task

You can cancel the selected active task by clicking the **Cancel** button. You'll be asked to confirm the operation. Upon confirmation the progressing task will be immediately stopped and will go into the idle state.

The **Cancel** button for the idle task is disabled, as you can only cancel the task that is currently running.

## 13.3 Editing a task

You can edit the selected task by clicking the **Edit** button. Depending on the task type, you will go to the respective section of the **Actions** tab – backup, restore, validate, etc. There, you will see all the sections of the backup/restore/validation/etc. wizard which you completed while creating that task. All the steps of the wizard will appear on the screen at once, where you can see the current task settings and can change any of these settings. (*For further information, please, refer to sections "Creating a backup of virtual machines" (p. 30), "Restoring a backup of virtual machines" (p. 54) , "Validating backups" (p. 90), etc.*).

## 13.4 Deleting a task

You can delete the selected task by clicking the **Delete** button. You'll be asked to confirm the operation. Upon the confirmation, it will be immediately erased.

## 13.5 Viewing task logs

You can see the selected task logs by clicking the last result status. You will go to the **Logs** view (**View** -> **Show Logs**) section, where you can see all the logs for the current task (*Please, see "Managing Logs" sections* (p. 93)).

## 13.6 Viewing task details

Upon selecting any task in the task list, you can view its details in the **Summary** and **Source and Target** tabs. Note that the tabs could present the varying information depending on the task type – backup, restore, validation, etc. The sections below describe the tabs contents for the backup task.

The **Summary** tab gives overview details of the current selected task. Here is an example of the possible contents of the **Summary** section for the backup task:

**Start time**: 06/29/2012 12:49
**Remaining time**: 41 sec
**Last finish time**: N/A
**Last result**: Not run yet
**Bytes transmitted**: 1.219 GB

**Backing up**: N/A
**Speed**: 8.053 Mb/s
**Schedule**: N/A

The **Options** section on the right shows the settings of the current selected task. This section shows only the options which differ from default values. If all task options are default, then this section just states “**Options: default**” without listing any specific values. Here is an example:

**Archive protection**: On
**Archive encryption algorithm**: AES 128
**Number of attempts**: 10
**Interval between attempts**: 1 Minute(s)
**Deduplication**: Off
**CBT backup**: Off
**Use FTP in active mode**: On
**Validate after backup**: On

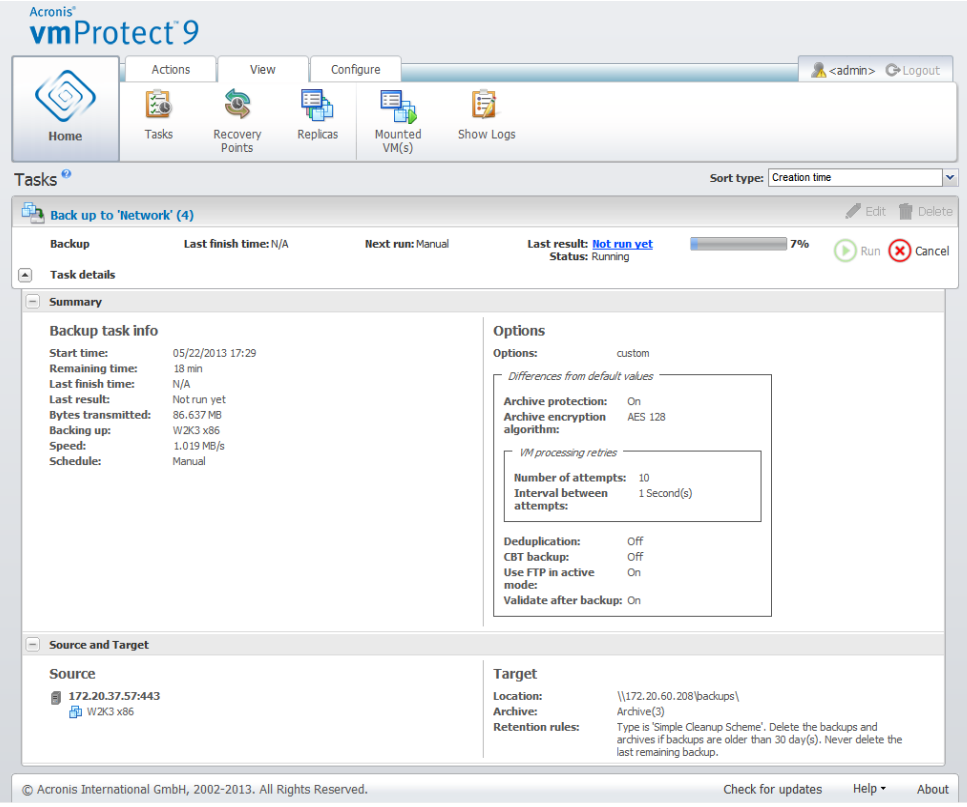
The **Source and Target** tab in the **Source** section on the left presents the tree of ESX(i) hosts+vApps/VMs included into the backup task. The tree is build up dynamically. If there was an entire ESX(i) host selected for backup, then this tree will be shown for the current state of the machines (the same list) same as in VMware IC. To the right of the ESX(i) host there should be a mark that the entire group is being backed up (“All virtual machines” mark). Here is an example:

ESX Host 1 “All Virtual Machines”:
Small_vm

ESX Host 2 :
AcronisESXAppliance (10.250.40.30)

The **Target** section on the right presents the information on the location of the backed up archive. Here is an example:

**Location**: \\NAS1\Backups\AcronisESX_Appliance_1557\azz11006765454cv\
**Archive**: Archive_name
**Retention rules**: Delete Backups older than 30 days / Keep only last 30 backups



Tasks

Sort type: Creation time

Back up to 'Network' (4)

Backup | Last finish time: N/A | Next run: Manual | Last result: Not run yet | Status: Running | 7%

Task details

Summary

Backup task info

Start time: 05/22/2013 17:29
Remaining time: 18 min
Last finish time: N/A
Last result: Not run yet
Bytes transmitted: 86.637 MB
Backing up: W2K3 x86
Speed: 1.019 MB/s
Schedule: Manual

Options

Options: custom

*Differences from default values*

Archive protection: On
Archive encryption algorithm: AES 128

*VM processing retries*

Number of attempts: 10
Interval between attempts: 1 Second(s)

Deduplication: Off
CBT backup: Off
Use FTP in active mode: On
Validate after backup: On

Source and Target

Source

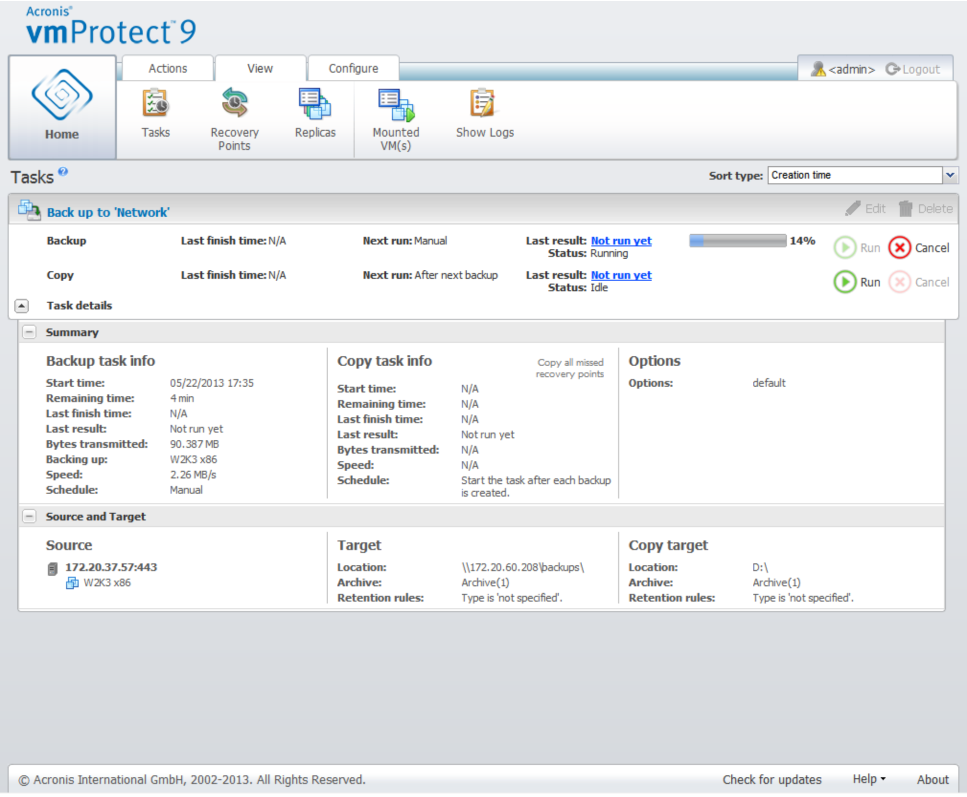
172.20.37.57:443
W2K3 x86

Target

Location: \\172.20.60.208\backups\
Archive: Archive(3)
Retention rules: Type is 'Simple Cleanup Scheme'. Delete the backups and archives if backups are older than 30 day(s). Never delete the last remaining backup.

Managing tasks, View task details, Summary tab, Source and Target tab

If the backup task was configured to **Copy the backup to a second location** then the summary tab of the task details will consist of both the **Backup task info** and the **Copy tack info**, as shown in the picture below.



Tasks

Sort type: Creation time

Back up to 'Network'

Backup | Last finish time: N/A | Next run: Manual | Last result: Not run yet | Status: Running | 14%

Copy | Last finish time: N/A | Next run: After next backup | Last result: Not run yet | Status: Idle

Task details

Summary

Backup task info

Start time: 05/22/2013 17:35
Remaining time: 4 min
Last finish time: N/A
Last result: Not run yet
Bytes transmitted: 90.387 MB
Backing up: W2K3 x86
Speed: 2.26 MB/s
Schedule: Manual

Copy task info

Start time: N/A
Remaining time: N/A
Last finish time: N/A
Last result: Not run yet
Bytes transmitted: N/A
Speed: N/A
Schedule: Start the task after each backup is created.

Options

Options: default

Source and Target

Source

172.20.37.57:443
W2K3 x86

Target

Location: \\172.20.60.208\backups\
Archive: Archive(1)
Retention rules: Type is 'not specified'.

Copy target

Location: D:\
Archive: Archive(1)
Retention rules: Type is 'not specified'.

Managing tasks, Viewing task details, Backup and Copy task info

# 14 Managing Recovery Points

Click the **Recovery Points** button in the **View** tab of the main menu to open the **Recovery Points** page.

The **Recovery Points** view of Acronis vmProtect 9 provides you with an interface to manage the recovery points available for the virtual machines in your environment or the points in time which you can go back to for each virtual machine. Upon the successful execution of each backup task, a new recovery point is created and the recovery points list is updated automatically.

After selecting the recovery point, you can perform basic operations with it. Operations on the selected recovery point can be executed by clicking the corresponding button on the main tool bar. All these operations, as described below, are wizard-driven and provide you with a simple way to accomplish the desired task.

The **Recovery Points** view contains 3 main sections:

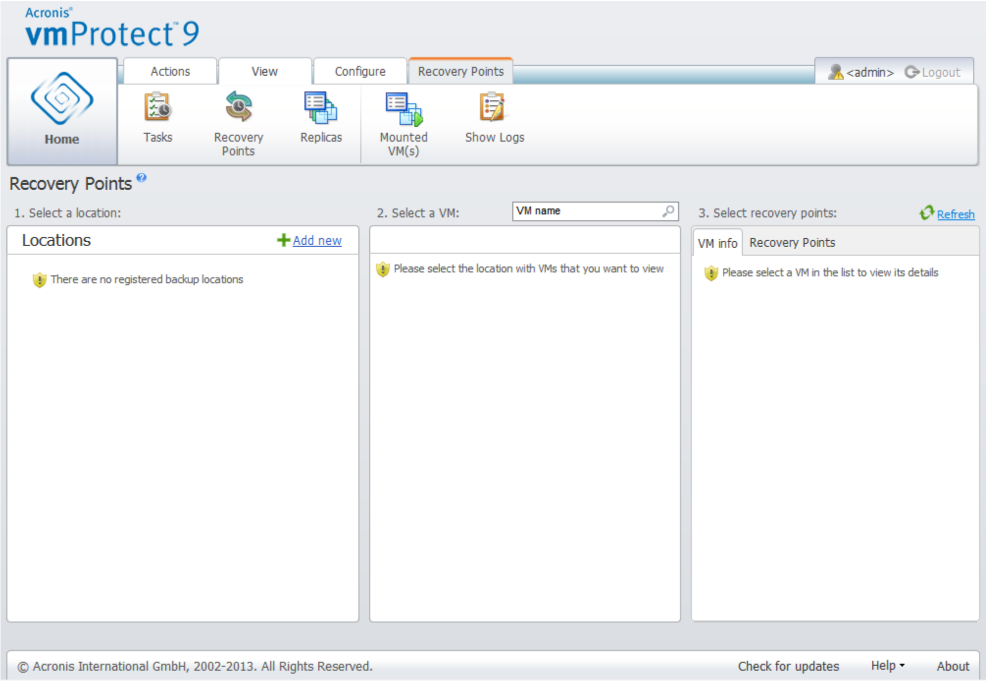
- the Backup locations.
- the Virtual Machines catalog.
- the Recovery Points list.

The main idea for navigating this page is that you should first define the backup location (in the left section) which will then be scanned for the archives and their contents. The scan will show you a tree-list (in the middle section) of the virtual machines included in all archives stored in the selected location. When clicking on any virtual machine in this middle section you can check the list of available recovery points and summary details for this machine. This list is located in the section on the right.

The **Locations** list on the left side shows the registered backup locations (any location that has ever been used as backup target or recovery source). The **Locations** list includes the following elements, each location in a separate bloc:

- **Location** path, e.g. \\NAS1\Backups\Acronis\Recent\
- **Location** statistics:
  - **Backups size**, e.g. 3.242 Gb (22%).
  - **Used space**, e.g. 5.242 Gb (36%).
  - **Free Space**, e.g. 9.412 Gb (64%).
  - **Total Space** (**Used space** + **Free space**), e.g. 14.654 Gb.
- **Total backups** (i.e. total number of recovery points in the location).
- **Edit Credentials** button which allows to change the access credentials to the location (if applicable).
- **Remove Location** button which removes the location from the list of registered locations.

While there are no locations added, the widget will show empty field with the following text: “There are no registered backup locations.” The other 2 sections will not be shown up at all.



There are no registered backup locations

Please select the location with VMs that you want to view

Please select a VM in the list to view its details

© Acronis International GmbH, 2002-2013. All Rights Reserved.

Managing Recovery Points, no locations available

## 14.1 Adding a backup location

Optionally, you can add or remove the backup locations right from the **Locations** list. Click the **Add New** link on the top to open the **Add Location** pop-up.

Note that the remove operation will not physically remove the archives from the location, but will just delete the location from the Acronis vmProtect 9 configuration. All the backups will remain intact inside the location and you can see them when you add it back via the **Add new** link. Removing and adding locations may be required if you have some unnecessary backup locations which are no longer actual and you don't want to see them anymore.

The left side of the **Add Location** pop-up shows the list of:

- Cloud backup storages.
- Local folders.
- Network folders.
- FTP servers.
- SFTP servers.

You can select the desired location by expanding the appropriate folder group and choosing it in the folder tree or by entering the full path to the location in the **Location** field.

Choose one of the backup location types from the browse tree on the left side. If the selected location (Cloud backup storage, Network folders or FTP/SFTP servers) requires an authentication, you will first see the dialogue for submitting your credentials in the right pane. After successfully logging in, this pane shows the contents of the selected location, i.e. the archives inside this location.

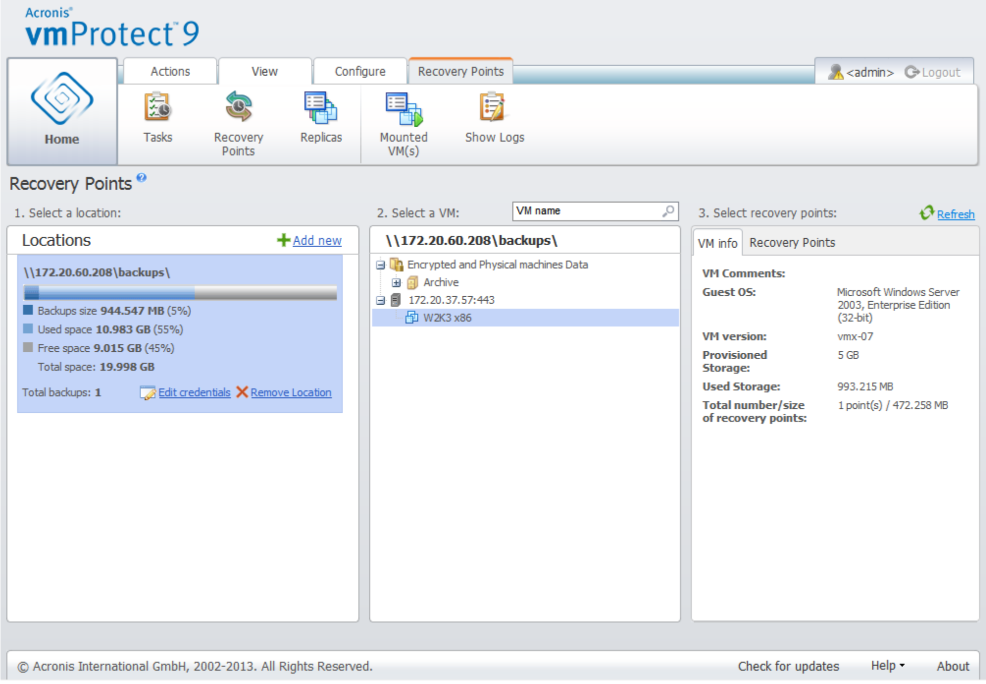
An alternative to browsing the location in the tree is entering the path in the corresponding **Location** field below and clicking the **Go** button to explore this location. In this case, you will also see the same authentication dialogue in the right pane where you are asked to enter your login and password.

You have to select or specify the path in the **Location** field in order to complete the wizard, and then click **OK**. The **OK** button is grayed out until there is a valid location selected.

## 14.2 Virtual Machines catalog

The middle section of the **Recovery Points** view presents the Virtual Machines catalog. This tree list of virtual machines and vApps is built based on parsing through the archives found in the location selected in the left section.

If the selected location contains any password-protected archives or archives of physical machines, they are shown in the separate list under the **Encrypted and Physical machines Data**. To view the contents of these archives, you have to specify the password in the **Password** pop-up.



\\172.20.60.208\backups\

Backups size **944.547 MB** (5%)
Used space **10.983 GB** (55%)
Free space **9.015 GB** (45%)
Total space: **19.998 GB**
Total backups: **1**

\\172.20.60.208\backups\
- Encrypted and Physical machines Data
  - Archive
- 172.20.37.57:443
  - W2K3 x86

| | |
|---|---|
| **VM Comments:** | |
| **Guest OS:** | Microsoft Windows Server 2003, Enterprise Edition (32-bit) |
| **VM version:** | vmx-07 |
| **Provisioned Storage:** | 5 GB |
| **Used Storage:** | 993.215 MB |
| **Total number/size of recovery points:** | 1 point(s) / 472.258 MB |

Managing Recovery Points

Only one virtual machine can be selected in this list at a time. The details window (the right section) for the selected virtual machine contains 2 tabs as explained below – the **Recovery Points** list and the **Recovery Points** details.

## 14.3 Recovery Points list

The **Recovery Points** list in the details section presents the list of all available recovery points which includes the following columns:

- **Recovery Points**: the column shows the date and time values corresponding to creation of each recovery point in the list.
- **Archive Name**: shows the file name (in the selected backup location) this recovery point belongs to.
- **Size**: shows the physical size of the archive (in MB/GB) this recovery point belongs to.

From the **Recovery Points** list you can switch to the **Summary** view (see “Summary tab” section (p. 88)).

After selecting a certain recovery point in the list you can perform any of the operations described in the “Operations on selected items” section (p. 88).

## 14.4 Summary tab

You can see the summary information on the selected recovery point by switching to the **Summary** tab. This tab shows the following information:

- **VM Comments** (taken from VMware vSphere client **Summary** tab for the selected VM).
- **Guest OS** (taken from VMware vSphere client **Summary** tab for the selected VM).
- **VM version** (taken from VMware vSphere client **Summary** tab for the selected VM).
- **Provisioned Storage** (taken from VMware vSphere client **Summary** tab for the selected VM).
- **Used Storage** (taken from VMware vSphere client **Summary** tab for the selected VM).
- **Total number/size of recovery points**, for example 23 points/120Gb.

## 14.5 Operations on selected items

The **Recovery Points** view has the following operating buttons in the ribbon menu, which allow performing the basic operations with the selected recovery point:

- **Restore**.
- **Exchange Recovery**.
- **Run VM from backup**.
- **File Recovery** (Guest Files download).
- **Validate**.
- **Delete**.

These operations are enabled when selecting a certain recovery point in the list (in the details section for the selected virtual machine as described in the “Recovery points list” section (p. 87)).

### 14.5.1 Restore

Click the **Restore** button in the ribbon menu to perform recovery from the selected recovery point by running the restore task wizard. The wizard will be pre-filled with the selected recovery point settings described in the “Restoring a backup of virtual machines” section (p. 54).

### 14.5.2 Exchange Recovery

Click the **Exchange Recovery** button in the ribbon menu to extract the Exchange data from the selected recovery point by running the **Extract Exchange Server Items** wizard. The wizard will be pre-filled with the selected recovery point settings described in the “Exchange Server Backup Extraction” section (p. 63).

### 14.5.3 Run VM from backup

Click the **Run VM from backup** button in the ribbon menu to perform the Mounting VM operation by activating the Run VM from backup wizard. The wizard will be pre-filled with the selected recovery point settings described in the “Running VM from backup” section (p. 70).

### 14.5.4 File recovery

Click the **File recovery** button in the ribbon menu to perform the Guest File Download operation by running the File Recovery wizard. The wizard will be pre-filled with the selected recovery point settings described in the “File recovery” section (p. 61).

### 14.5.5 Validate

Click the **Validation** button in the ribbon menu to perform the Backup Validation by running the new validation task. The validation wizard will be pre-filled with the selected recovery point settings described in the “Validating backups” section (p. 90).

### 14.5.6 Delete

Click the **Delete** button in the ribbon menu to remove the selected recovery point. The **Delete Recovery Point(s)** pop-up will appear where you can see the list of recovery points selected for deletion.

Note, that in a Legacy Mode archive (p. 9) some recovery points may have dependencies. This means that deleting a single recovery point is impossible. In this case, the entire chain of recovery points which depend on the selected one will be designated for deletion. The recovery points which belong to the Always Incremental archive (p. 10) can be deleted without any constraints and you will see the single recovery point in the deletion list.

After confirming the operation by clicking the **Delete** button in the pop-up, the deletion task will appear in the **Tasks** view. This task will disappear upon completion. The result can be seen in the **Dashboard** view and in the log file.

# 15 Other Operations

## 15.1 Validating backups

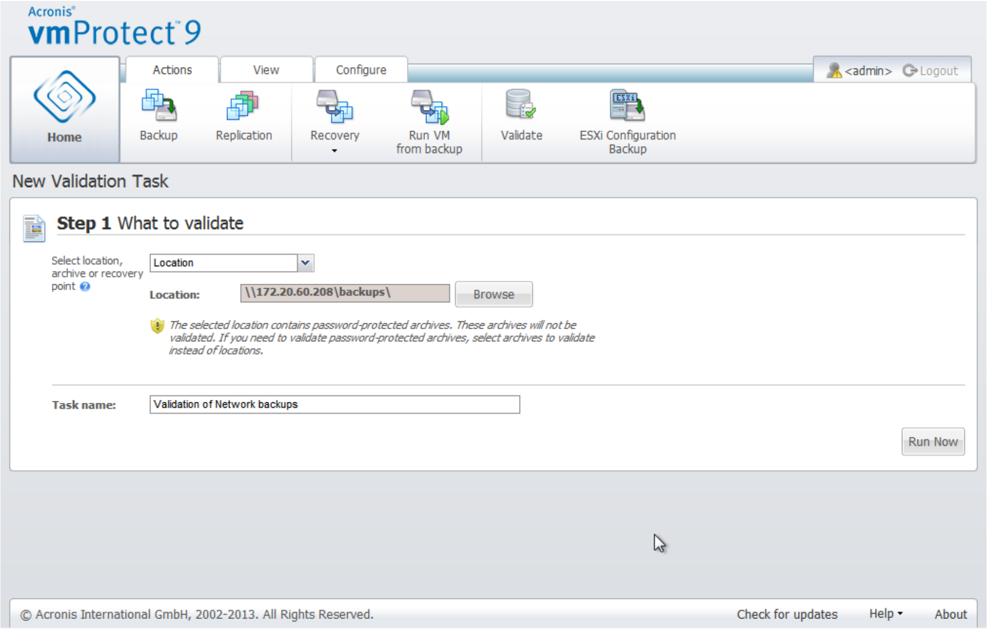
Validating backups is an operation that checks the possibility of data recovery from a backup. Note that while successful validation means high probability of successful recovery, it does not check all factors that influence the recovery process. If you back up the operating system, only a test recovery to a new virtual machine can guarantee success of the recovery.

In Acronis vmProtect 9 you can validate a **Location**, an **Archive** or a **Recovery Point**. Validation of a recovery point imitates recovery of all files from the backup to a dummy destination. Validation of an archive will validate all recovery points stored in this archive. Validation of a location will check the recovery of all archives stored in this location.

### 15.1.1 What to validate

First of all, you should define which item type you want to validate from 3 available options: **Location**, **Archive** or **Recovery Point**.

**Location** – Validating a location will check the integrity of all the archives inside this location. Note that this is usually a more time-consuming process than granular validation of specific archives or recovery points (especially if you store multiple archives in the location). The validation time also depends on the number of the backups (recovery points) included in each archive in the selected location. Note that password-protected archives will not be validated in this case. You should choose the option to validate Archive instead.



New Validation Task

**Step 1** What to validate

Select location, archive or recovery point: Location

Location: \\172.20.60.208\backups\

*The selected location contains password-protected archives. These archives will not be validated. If you need to validate password-protected archives, select archives to validate instead of locations.*

Task name: Validation of Network backups

New Validation Task. What to validate. Location.

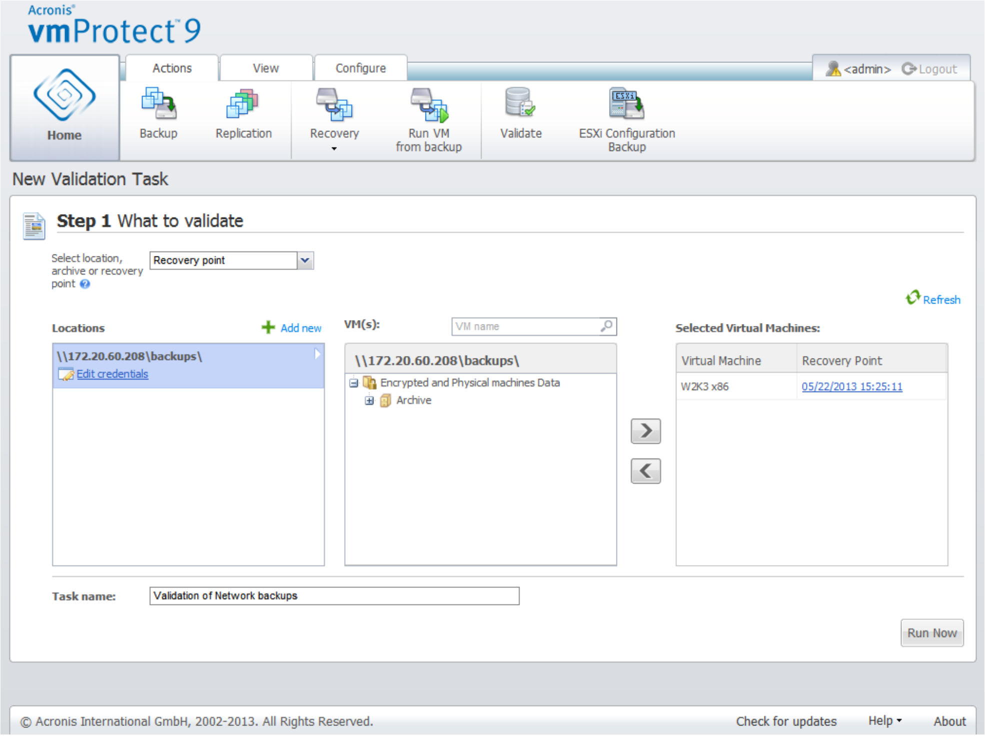
**Archive** – Validating an archive will check the integrity of all backups (recovery points) inside the specified archive. In general, this procedure will be faster than validating the whole location. However, it is slower than validating a specific recovery points inside this archive.

**Recovery Point** – To ensure that you can revert back to some specific recovery point, you can perform granular validation of just the selected recovery points (they don't have to reside within one archive).

After selecting the validation item type, define the backup location. You can either specify a location or location and an archive in order to retrieve the list of recovery points. If you are validating a recovery point, the selected archive or location will be scanned for recovery points included there. This is needed in order to pick up the recovery point(s) to be validated. Depending on the selected validation item type, some controls will be disabled (for example, you will not see the list of recovery points if you validate a location or archive).

You can see a tree-list of the virtual machines included in all archives stored in the selected location and select any of these virtual machines by moving them to the Selected Virtual Machines section. In the Selected Virtual Machines section you can see a list of the selected virtual machines with their available recovery points, i.e. point in time which contains a particular machine state. The recovery point can be selected by clicking on it.

To complete the validation task creation wizard, you must set the task name. Note that [ ] { } ; , . symbols are not allowed for the task name.



New Validation Task

**Step 1** What to validate

Select location, archive or recovery point: Recovery point

Locations: \\172.20.60.208\backups\ — Edit credentials

VM(s): \\172.20.60.208\backups\
- Encrypted and Physical machines Data
  - Archive

Selected Virtual Machines:

| Virtual Machine | Recovery Point |
|---|---|
| W2K3 x86 | 05/22/2013 15:25:11 |

Task name: Validation of Network backups

New Validation Task. What to validate. Recovery point.

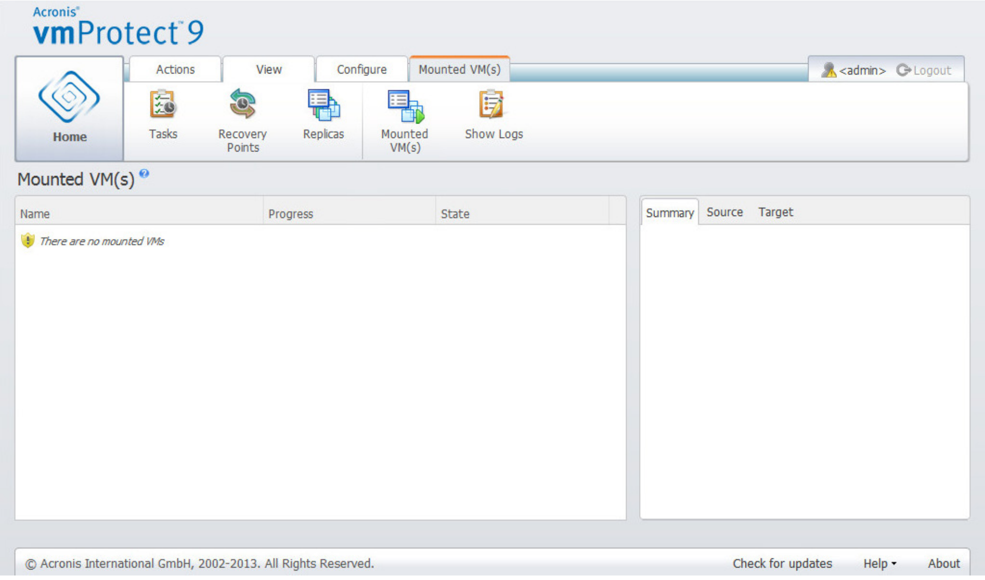
After clicking on the **Run Now** button, the selected items will be validated and you will see the progress of your newly created validation task in the **Tasks** view. You will see its result in the **Dashboard** view and in the **Show Logs** view.

## 15.2 Managing mounted VMs

Click **Mounted VMs** in the **View** tab of the Acronis vmProtect 9 main ribbon menu to open the **Mounted VMs** page.

### 15.2.1 Mounted VMs list

The **Mounted VMs** view provides an overview on the virtual machines which are currently mounted or running from backup on an ESX(i) host.



There are no mounted VMs

Mounted VMs view.

At first, when you don't have any virtual machines running, the Mounted VMs list is empty. After you performed **Run VM from backup** operation (see "Running VM from backup" section (p. 70)), this Mounted VMs view will automatically open where you could see the machine you've just run.

In the table, you can see the list of these machines and their state: "Running" (if the machine is running) or "Stopped" (if not).

### 15.2.2 Mounted VMs details

You can check the details for any of the mounted virtual machines by selecting it from the list. The details of the selected virtual machine will appear in the right section where you can switch between the tabs to check the additional details.

Upon selecting any virtual machine in the list, you can view its details in the right section. The information about the currently selected task is presented with a tab view. There are three tabs – Summary, Source and Target (the default tab is Summary).

The first **Summary** tab presents overview details of the currently selected virtual machine. Here is an example of the possible contents of the **Summary** tab:

**Start Time/Date**: 20:11 11/05/2011

The **Source** tab presents the tree of mounted ESX(i) hosts+vApps/VMs. Here is an example of the **Source** tab contents:

**Location**: \\Backups\
**Archive**: Archive_name

ESX Host 1 (10.250.40.30) "All Virtual Machines":
Small_vm

The **Target** tab presents the information on the location where the selected VM runs. Here is an example of the **Target** tab contents:

ESX Host 1 (10.250.40.30) "All Virtual Machines":
Small_vm

### 15.2.3 Unmounting VMs

At the Mounted VMs view there are two control buttons in the context tool bar – **Unmount** and **Unmount & Save**.

When selecting a Virtual Machine in the Mounted VMs list, you can unmount it (stop running it from backup) by clicking the **Unmount** button.

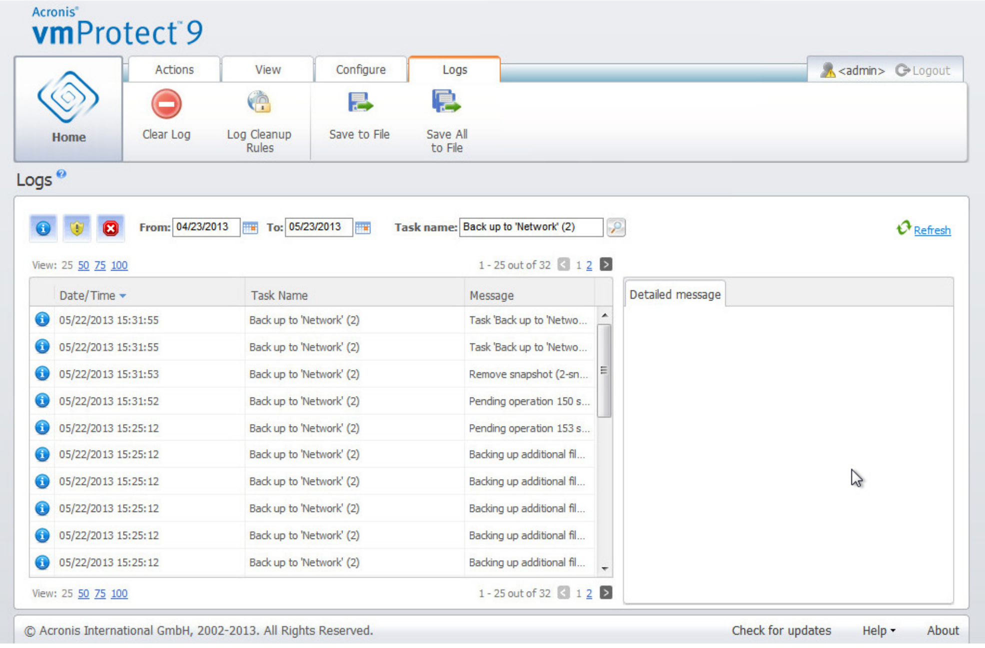
Performing the **Unmount & Save** operation stops running the machine from the backup and commits all the changes made to this machine back into the archive adding a new recovery point to it. Note, that the recovery point is created without an "Application-Aware" option.

## 15.3 Managing logs

Click **Show logs** in the **View** tab of the Acronis vmProtect 9 main ribbon menu to open the **Logs** page.

### 15.3.1 Logs list

The **Show Logs** view provides a list of events that have occured on Acronis vmProtect 9 Agent. This includes backup, restore, run VM from backup and other tasks as well as system messages such as establishing connection to managed ESX(i) hosts/vCenter, etc.



From: 04/23/2013 To: 05/23/2013 Task name: Back up to 'Network' (2)

View: 25 50 75 100 1 - 25 out of 32 1 2

| Date/Time | Task Name | Message |
|---|---|---|
| 05/22/2013 15:31:55 | Back up to 'Network' (2) | Task 'Back up to 'Netwo... |
| 05/22/2013 15:31:55 | Back up to 'Network' (2) | Task 'Back up to 'Netwo... |
| 05/22/2013 15:31:53 | Back up to 'Network' (2) | Remove snapshot (2-sn... |
| 05/22/2013 15:31:52 | Back up to 'Network' (2) | Pending operation 150 s... |
| 05/22/2013 15:25:12 | Back up to 'Network' (2) | Pending operation 153 s... |
| 05/22/2013 15:25:12 | Back up to 'Network' (2) | Backing up additional fil... |
| 05/22/2013 15:25:12 | Back up to 'Network' (2) | Backing up additional fil... |
| 05/22/2013 15:25:12 | Back up to 'Network' (2) | Backing up additional fil... |
| 05/22/2013 15:25:12 | Back up to 'Network' (2) | Backing up additional fil... |
| 05/22/2013 15:25:12 | Back up to 'Network' (2) | Backing up additional fil... |

View: 25 50 75 100 1 - 25 out of 32 1 2

© Acronis International GmbH, 2002-2013. All Rights Reserved.

Logs list.

The logs list contains the **Date/Time**, **Task name** and **Message** columns. You can sort the logs list by clicking the column header. For switching between the ascending and descending sort order click the column header one more time.

Also, you can filter the log events using several filters located above the list:

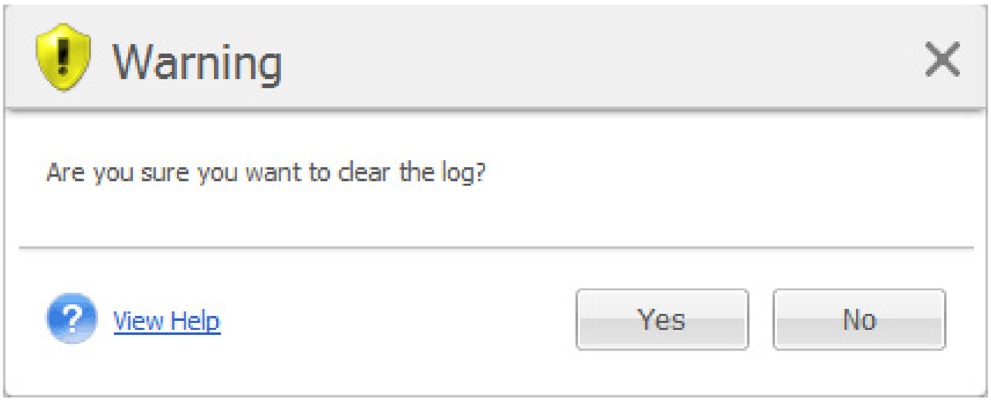
- Event flags (Success, Warning or Error).
- Date/Time.
- Task Name.

Click the log event in the list to see the detailed message for this log in the right window. **Click for More Information** link opens the Acronis Knowledge Base in new browser window. This link is available for “error” type log events only.

From the context tool bar, you can clear up the log events or set up automatic clean up rules to keep the size of the logs within the certain limits. These operations are described in the subsections below.

## 15.3.2 Clear logs

Click the **Clear Log** button in the main tool bar to erase all logs entries. This action will clear up all entries in the Acronis vmProtect 9 logs. You will get the “Are you sure you want to clear the log?” warning message in order to confirm the delete logs operation. Upon your confirmation, all logs will be cleared.

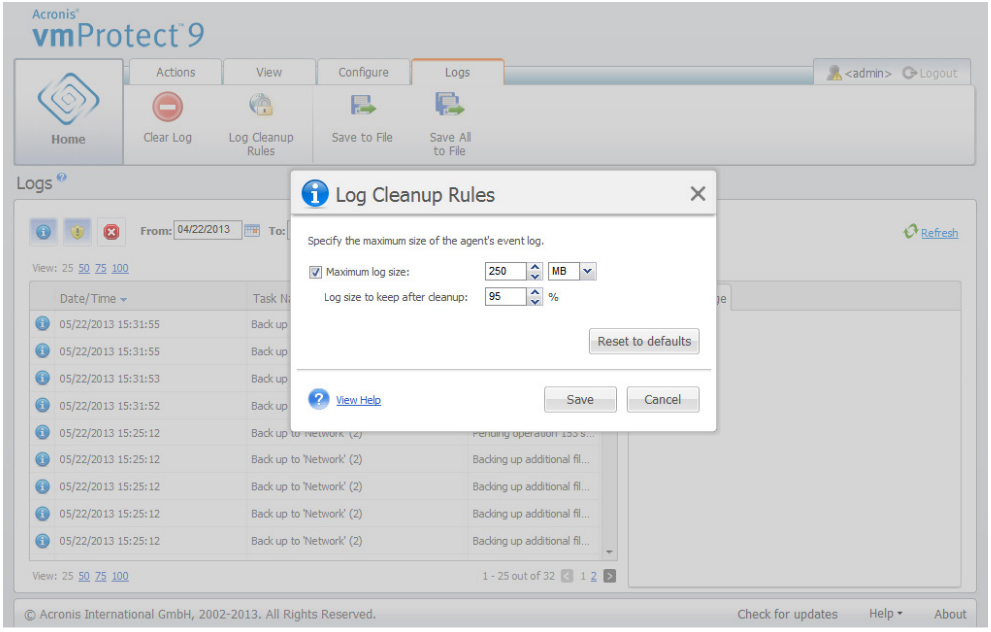

Warning

Are you sure you want to clear the log?

Clear log dialog.

## 15.3.3 Log cleanup rules

Click the **Log Cleanup Rules** button in the main tool bar to set up your rules for keeping the log entries. In other words, this option specifies how to clean up the Acronis vmProtect 9 agent log.


Log Cleanup Rules

Specify the maximum size of the agent's event log.

☑ Maximum log size: 250 MB

Log size to keep after cleanup: 95 %

**Log Cleanup Rules dialog.**

Select the check box in order to enable this **Log cleanup rules** option. Then, define the maximum size of the agent log folder (for example, in Windows XP/2003 Server %ALLUSERSPROFILE%\Application Data\Acronis\vmProtect\VMMS\LogEvents).

Along with the **Maximum log size** value, you can set up the amount of log entries you want to keep.

The default values for **Log cleanup rules** settings are:

- **Maximum log size**: 50Mb.
- **Log size to keep after cleanup**: 95%.

The **Reset to defaults** button reverts these values for the preset.

When the **Log cleanup rules** option is enabled, then after every 100 log entries, the program will compare the actual log size with the pre-set **maximum log size**. Once the maximum log size is exceeded, the program deletes the oldest log entries. The default 95% setting will keep most of the log. With the minimum 1% setting, the log will be nearly cleared.

### 15.3.4 Save logs to file

Click the **Save to File** button in the ribbon bar to save the filtered log entries from the logs list. This operation allows you to get the .zip file with the selected logs and save it to your local PC. You may need to perform Save logs to file operation for troubleshooting the problems you might encounter.

You can also save all your Acronis vmProtect 9 log entries history by clicking the **Save All to File** button.

## 15.4 Managing licenses

Click **Licenses** in the **Configure** tab of the Acronis vmProtect 9 main ribbon menu to open the **Licenses** page.

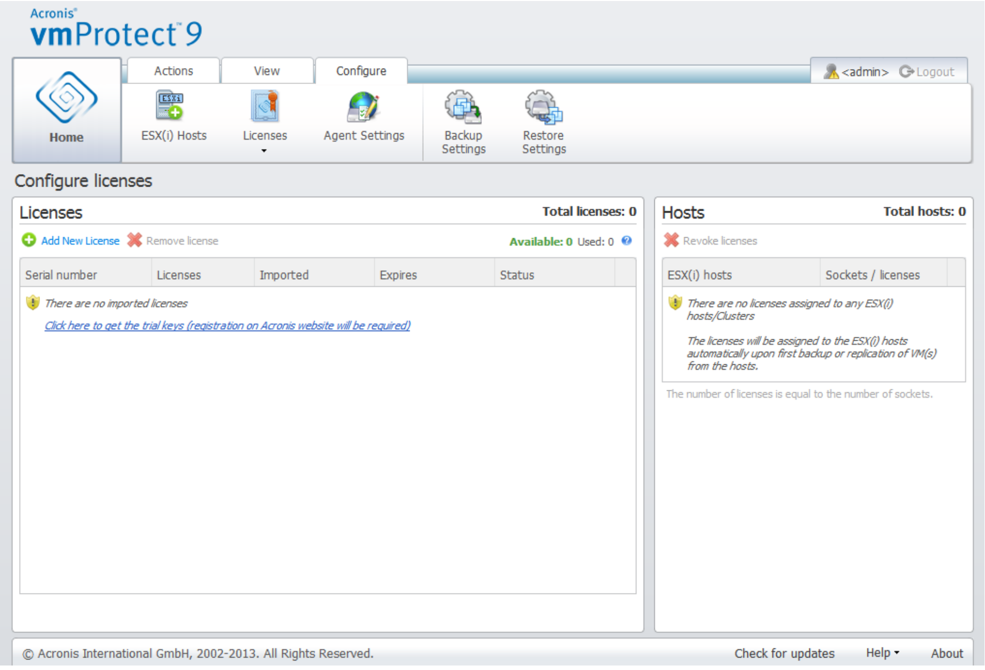
The **Licenses** view provides you with an overview of the licenses imported into the vmProtect 9 Agent. Here you can **Add** the license serial numbers and **Remove** the binding of licenses to ESX(i) hosts by using the corresponding buttons in the tool bar. Removing the license binding allows to free them up.

The licensing scheme in vmProtect 9 implies that each CPU on the managed ESX(i) host/cluster consumes a license.

At the first run of Acronis vmProtect 9 there are no licenses bound to any ESX(i) hosts/clusters. Without a license binding you can back up VMs only to the Acronis Cloud Backup storage as a backup destination. A new license can be added as described below.

The imported (added) serial numbers may contain a number of licenses inside. The right section on the **Licenses** page shows the serial numbers list, the number of licenses, as well as their import date and expiration date.

The left section represents the list of the ESX(i) hosts/clusters with some licenses bound. Licenses are bound to the ESX(i) host/cluster upon first backup or restore operation with virtual machines running on this host. In case of a cluster, the licenses will be bound to all hosts included in this cluster. If a host is removed from the cluster, the license is not freed up automatically. You can remove the license binding by selecting the ESX(i) host/cluster here and clicking on the **Remove** button in the tool bar. The licenses which were bound to this host will be free again and can be reused on another ESX(i) host/cluster.



Configure licenses

Licenses — Total licenses: 0

Available: 0 Used: 0

| Serial number | Licenses | Imported | Expires | Status |
|---|---|---|---|---|

*There are no imported licenses*

*Click here to get the trial keys (registration on Acronis website will be required)*

Hosts — Total hosts: 0

| ESX(i) hosts | Sockets / licenses |
|---|---|

*There are no licenses assigned to any ESX(i) hosts/Clusters*

*The licenses will be assigned to the ESX(i) hosts automatically upon first backup or replication of VM(s) from the hosts.*

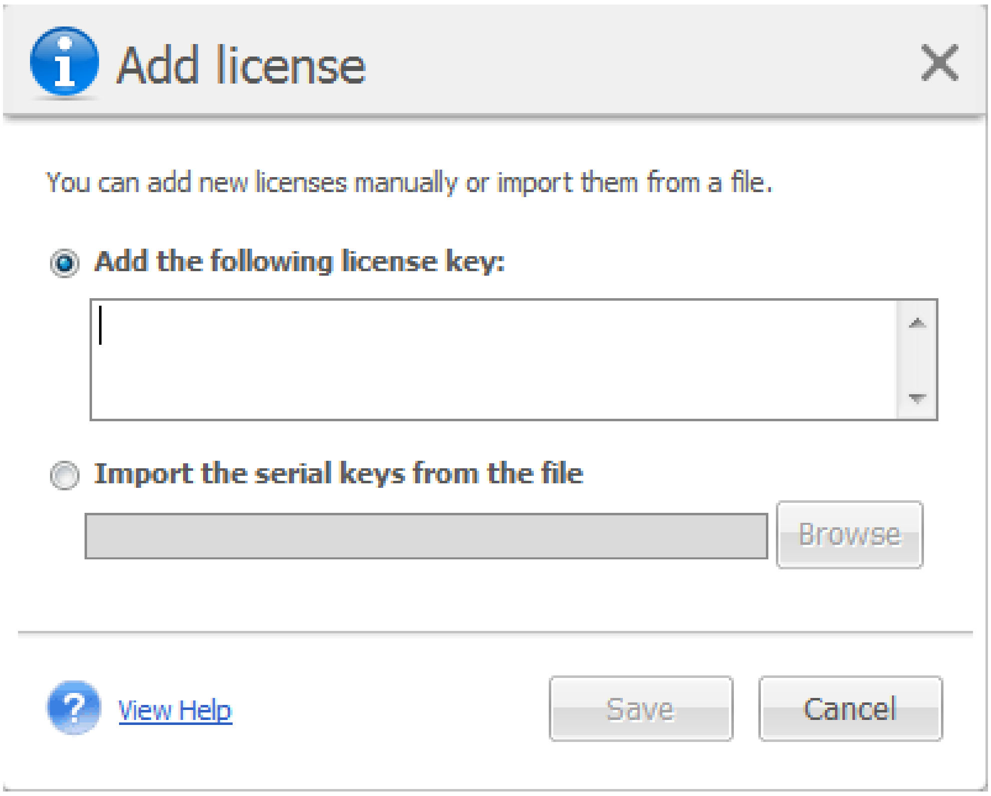
The number of licenses is equal to the number of sockets.

© Acronis International GmbH, 2002-2013. All Rights Reserved.

Managing Licenses page, licenses list.

## 15.4.1 Adding license

You can add licenses by copy-pasting them into the corresponding field or by browsing the file with the licenses you would like to import. Acronis vmProtect 9 supports .txt or .csv file format.



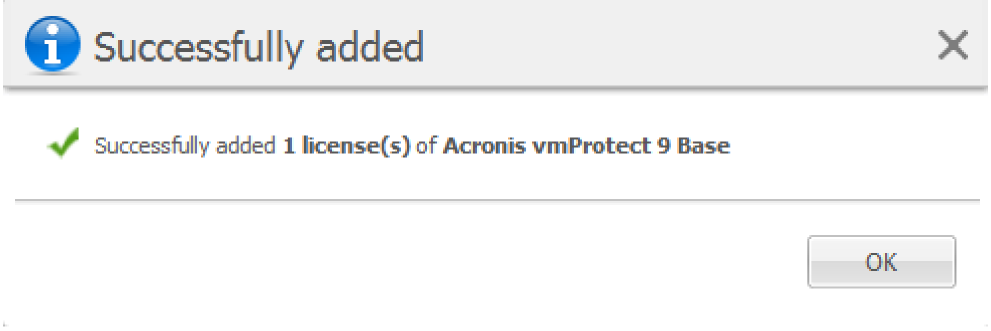
You can add new licenses manually or import them from a file.

● Add the following license key:

○ Import the serial keys from the file

Managing Licenses page, Add license dialog.

Upon adding new licenses you will get the following message indicating the number of licenses added.



Successfully added

✓ Successfully added **1 license(s)** of **Acronis vmProtect 9 Base**

Managing Licenses page, “Successfully added” message.

## 15.4.2 Adding license failure

Adding a license may fail due to the following reasons:

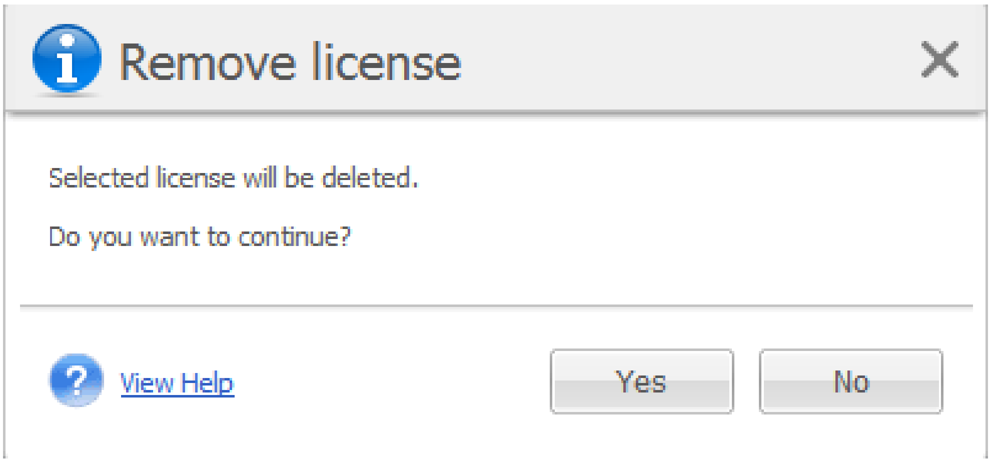
- The license is already imported.
- The license is incorrect.

There could also be other problems. If you are sure that your license is a correct one but it still fails to be added, please contact Acronis support (p. 110).

## 15.4.3 Removing license/ESX(i) host

Choose one of the ESX(i) hosts/Clusters in the list and click the **Remove** button. The license assignment will be reset for the selected ESX(i) host and the licenses will be freed up. The licenses will be automatically re-assigned to this host if you perform backup or restore operation with any of the machines running on this host.

You would have to confirm removing the license binding by choosing **Yes** in the dialog.



Remove license

Selected license will be deleted.

Do you want to continue?

Managing Licenses page, “Remove license” confirmation dialog.

### 15.4.4 Available Licenses

There are several license types that can be used by Acronis vmProtect 9:

- Acronis vmProtect 6/7 Standard Licenses
- Acronis vmProtect 9 Upgrade Licenses
- Acronis vmProtect 9 Standard Licenses
- Acronis vmProtect Trial Licenses

Acronis vmProtect 9 uses “per-socket” licensing scheme, where each CPU socket of an ESX(i) host requires one license of Acronis vmProtect 9. The licenses are assigned to the ESX(i) host upon first backup or replication of a VM from this ESX(i) host. If this host is a part of VMware cluster then the licenses will also be assigned to all other ESX(i) hosts which are included into this cluster.

All serial numbers with their details and statuses are listed according to their license types.

Acronis vmProtect 9 uses either Acronis vmProtect 9 Standard License, or Acronis vmProtect 9 Upgrade License. To add Acronis vmProtect 9 Upgrade License there must be sufficient number of Acronis vmProtect 6/7 Standard License registered already, or otherwise adding the Acronis vmProtect 9 Upgrade License will fail.

The number of available licenses shows how many licenses (vmProtect 9 Standard Licenses and vmProtect 9 Upgrade License) can still be used to assign to the ESX(i) hosts. Used licenses are the licenses already assigned to their respective ESX(i) hosts. Total number of licenses are used and available licenses combined. The number of not upgraded licences indicate vmProtect 6/7 standard licenses for which there are no vmProtect 9 upgrade licenses added.

## 15.5 Managing ESX(i) hosts

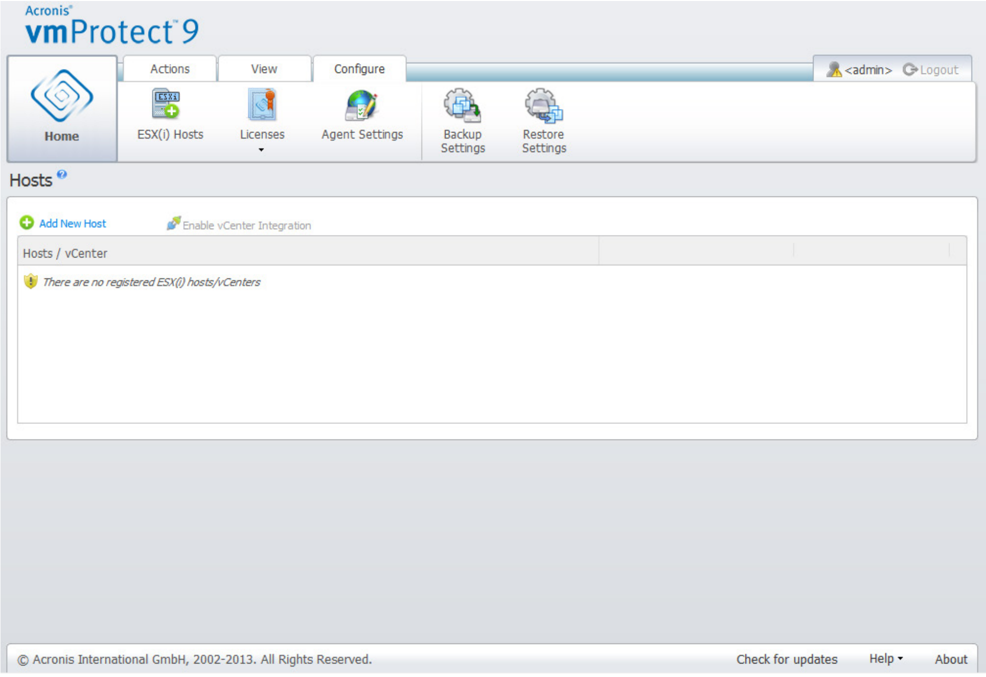
Click **ESX(i) hosts** in the **Configure** tab of the Acronis vmProtect 9 main ribbon menu to open the **ESX(i) hosts** page.

### 15.5.1 ESX(i) hosts list

The **Hosts** view provides an overview and management interface for the ESX(i) hosts/vCenter registered in the vmProtect 9 Agent settings. The ribbon buttons allow you to add other ESX(i) hosts to the list or remove them.

At the first run of Acronis vmProtect 9 there are no registered ESX(i) hosts/clusters. On this page you can add new ESX(i) hosts as described below.

After adding an ESX(i) host/vCenter, it will appear in the hosts list.



*There are no registered ESX(i) hosts/vCenters*

© Acronis International GmbH, 2002-2013. All Rights Reserved.

Configuring ESX(i) Hosts page, Hosts list.

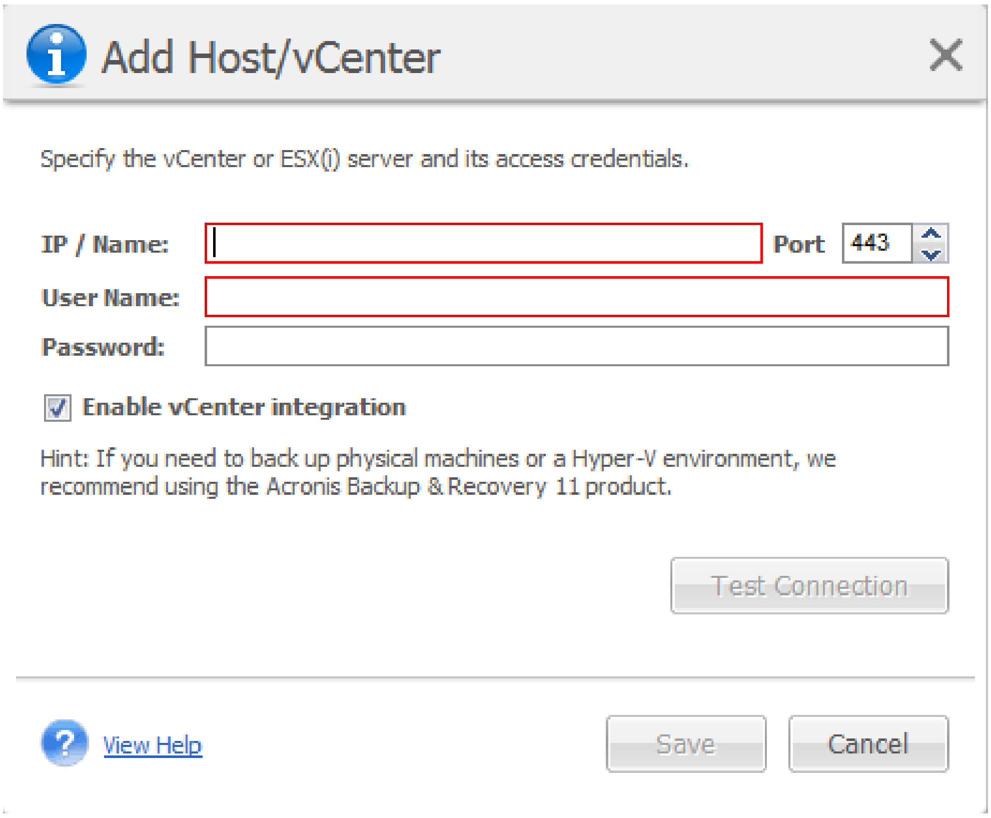
Adding an ESX(i) host/vCenter will not bind the licenses to it automatically. It will be bound only when you execute a backup/restore task with a virtual machine running on this host. After you add an ESX(i) host/vCenter you will be able to perform backup/recovery tasks with the virtual machines running on this ESX(i) host/vCenter.

Removing an ESX(i) host/vCenter will result in the disappearance of all tasks applied to virtual machines running on this ESX(i) host/vCenter. If the task included virtual machines from different ESX(i) hosts, then removing one of these ESX(i) hosts from configuration will not remove the task.

In order to successfully manage an ESX(i) host/vCenter, the login credentials are required. You can enter the credentials here, and they will be recorded until you remove the ESX(i) host/vCenter or change the credentials manually. Changing the credentials operation may be required if your company policy requires changing passwords due to security restrictions. For that, select the ESX(i) host/vCenter in the list and click the **Edit credentials** button on the right.

## 15.5.2 Adding ESX(i) host

In order to add an ESX(i) host/vCenter you have to provide the IP address/hostname and user credentials to access the desired ESX(i) host/vCenter. You can also specify the custom port. You can check the connection with **Test connection** button to ensure that the provided credentials are correct. Click **Save** to add your ESX(i) host/vCenter.



Add Host/vCenter

Specify the vCenter or ESX(i) server and its access credentials.

IP / Name: 
Port 443
User Name: 
Password:

☑ Enable vCenter integration

Hint: If you need to back up physical machines or a Hyper-V environment, we recommend using the Acronis Backup & Recovery 11 product.

Managing ESX(i) hosts page, Add Host/vCenter dialog.

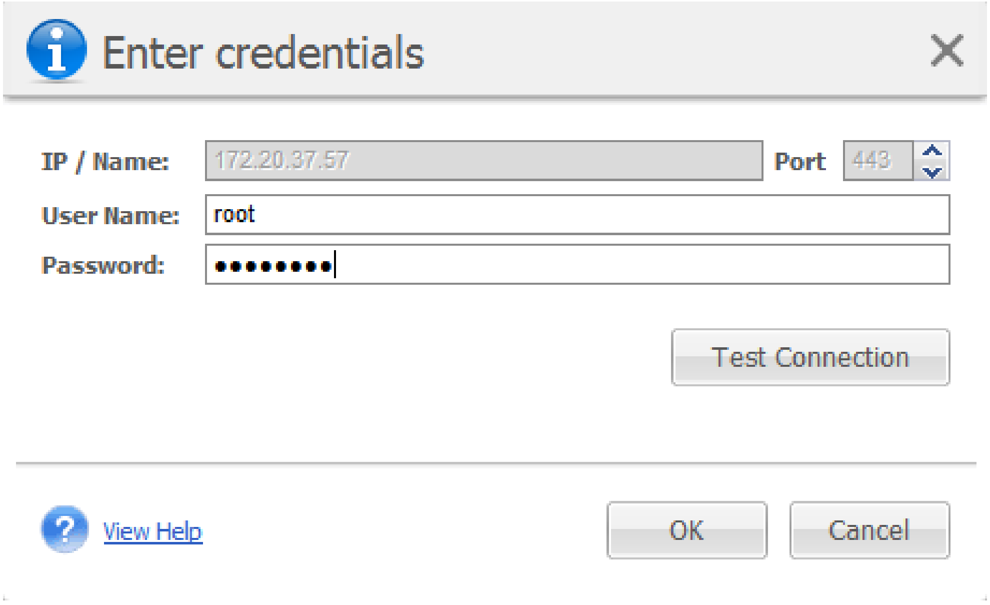
## 15.5.3 Adding an ESX(i) host which is a part of vCenter

When you directly add an ESX(i) host which is a part of vCenter instead of adding the vCenter itself, the main concern is that Acronis vmProtect 9 Agent will not be able to track the changes made to the ESX(i) host on behalf of the vCenter. This may cause unpredictable results. For example, if you run a VM from backup, upon unmounting, the temporary files will not be deleted from the ESX(i) host since they will be locked by the vCenter. Therefore, it is strongly recommended that you add the vCenter instead of adding separate ESX(i) hosts.

When you are trying to add an ESX(i) host which is a part of vCenter, you will get the following warning message. Click **No** in order to add the vCenter.

## 15.5.4 Login credentials

Changing the credentials operation may be required if your company policy requires changing password due to security restrictions. Select the ESX(i) host/vCenter is the list, click **Edit credentials** and provide the login/password information for the ESX(i) host/vCenter connection. If you are running Acronis vmProtect 9 in a domain environment, the username has to be specified in a domain\username format. You can check the connection with the **Test connection** button to ensure that the provided credentials are correct. Click **OK** to add your ESX(i) host/vCenter.


Enter credentials

IP / Name: 172.20.37.57 Port 443

User Name: root

Password: ••••••••

Managing ESX(i) Hosts page, Enter credentials dialog.

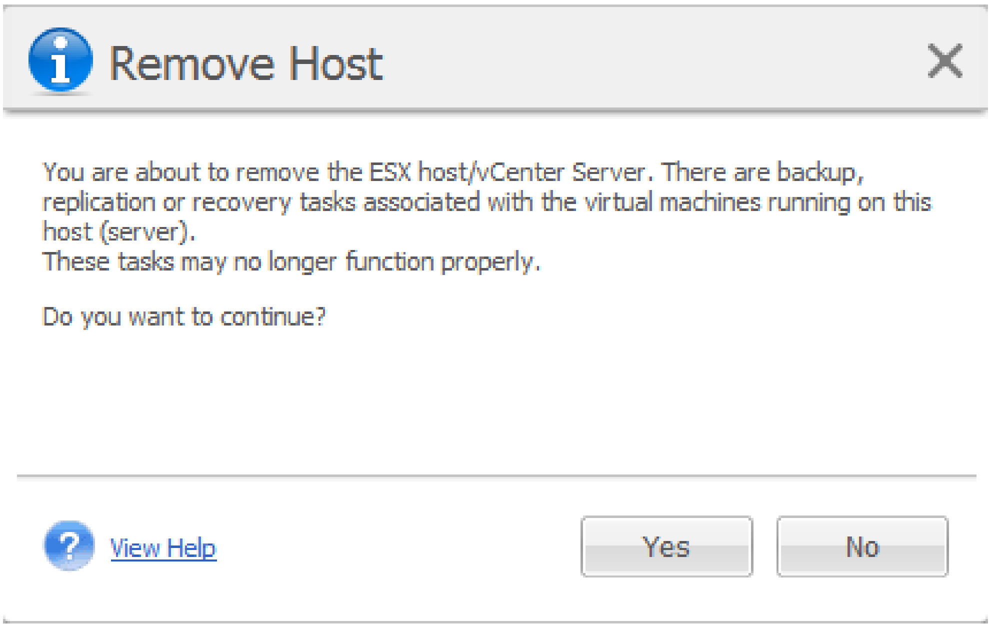
### 15.5.5 Removing ESX(i) host

Removing an ESX(i) host from Acronis vmProtect 9 configuration may be required if you no longer want to perform backup/recovery operations over the virtual machines running on this ESX(i) host. The licenses assigned to this host will not be removed automatically. To remove binding licenses, you have to go to Configure -> Licenses (p. 96) page.

Removing an ESX(i) host/vCenter will cause the existing tasks to malfunction; therefore, when doing so, you will be prompted with the following warning message:

"You are about to remove an ESX(i) host/vCenter while there are backup or restore tasks associated with the virtual machines running on this host. These tasks may no longer function properly. Do you want to continue?"

Choosing **Yes** will result in the disappearance of all Acronis vmProtect 9 tasks applied to the virtual machines running on this ESX(i) host/vCenter. If the task included virtual machines from different ESX(i) hosts, this task will be automatically modified to remove unnecessary virtual machines from the task configuration. This leaves only the virtual machines which can be managed by the ESX(i) hosts remaining in registration.



Remove Host

You are about to remove the ESX host/vCenter Server. There are backup, replication or recovery tasks associated with the virtual machines running on this host (server).
These tasks may no longer function properly.

Do you want to continue?

Managing ESX(i) Hosts page, Remove Host dialog.

# 15.6 Managing settings

## 15.6.1 Cloud Backup Subscription

Go to the **Configure** tab, click **Agent Settings** and select the **Acronis Cloud Backup Subscription** section.

First, you have to specify your credentials to log in to Acronis Cloud Backup Storage and click **OK**. Make sure you have an account at the Acronis website. If you do not have an account, you will need to create one.

Then, from the list select the available subscription you want to assign to the machine and click on **Activate now**. When you click **OK** to confirm, the selected subscription becomes activated. The activation may take several minutes, and when it completes you will see the selected machine, its used quota and expiration date in the list of activated subscriptions. When you need to increase storage quota or subscription period, go to account management web page and upgrade or renew your subscription.

Note that Cloud Backup subscriptions are independent from vmProtect licenses, which means that having valid Acronis vmProtect Cloud Backup subscription allows you to back up your VMs to cloud without having any Cloud vmProtect licenses. In other words there is no dependency on the amount of sockets of your ESXi hosts. You can back up any number of VMs using just Cloud Backup subscription.

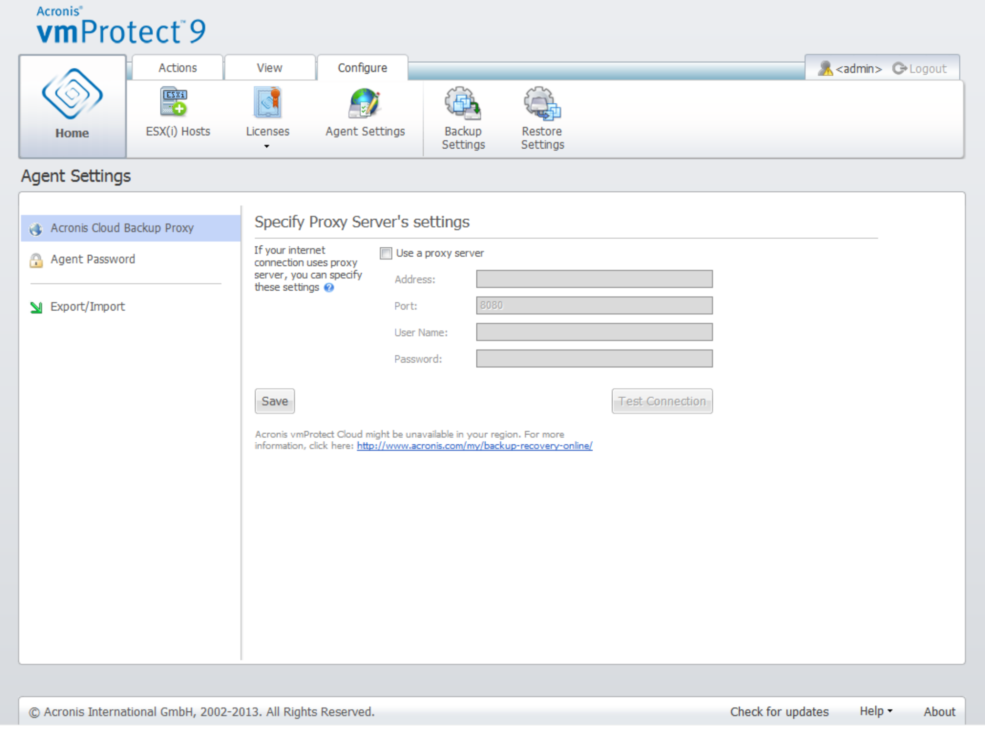
## 15.6.2 Cloud Backup Proxy

Go to the **Configure** tab, click **Agent Settings** and select the **Acronis Cloud Backup Proxy** section.

Cloud backup proxy settings are effective only for backup to and recovery from the Acronis Cloud Backup Storage over the Internet.

This option defines whether the Acronis agent will connect to the Internet through a proxy server.

Note that the Acronis vmProtect 9 Cloud Backup Storage supports only HTTP and HTTPS proxy servers.



Specify Proxy Server's settings

If your internet connection uses proxy server, you can specify these settings

□ Use a proxy server

Address:

Port: 8080

User Name:

Password:

Acronis vmProtect Cloud might be unavailable in your region. For more information, click here: http://www.acronis.com/my/backup-recovery-online/

Configuring settings, Cloud backup proxy.

To set up proxy server settings:

Select the **Use a proxy server** check box.

- In **Address**, specify the network name or IP address of the proxy server, for example: proxy.example.com or 192.168.0.1
- In **Port**, specify the port number of the proxy server, for example: 80
- If the proxy server requires authentication, specify the credentials in **User name** and **Password** fields.

To test the proxy server settings, click **Test connection**.

To apply the settings, click **Save**.

If you do not know the proxy server settings, contact your network administrator or Internet service provider for assistance.

Alternatively, you can try to find out what these settings are by looking in your Web browser's configuration. This is how to find them in 3 popular browsers.

- Microsoft Internet Explorer. On the **Tools** menu, click **Internet Options**. On the **Connections** tab, click **LAN settings**.

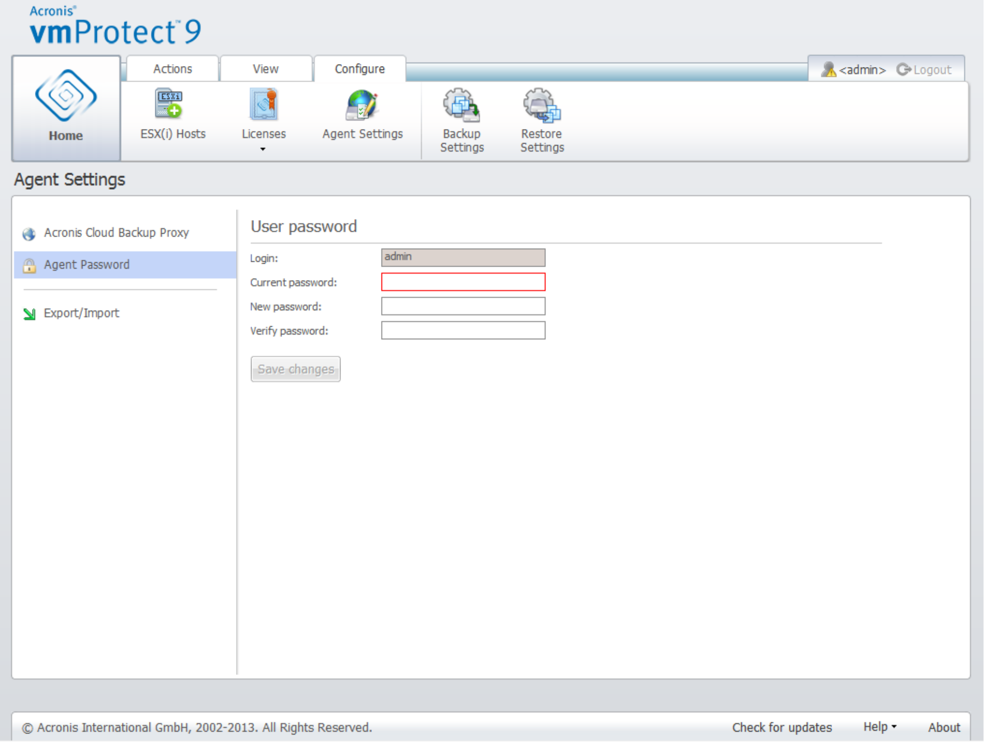
- Mozilla Firefox. On the **Tools** menu (accessible through the main **Firefox** button, or by pressing the Alt button on the keyboard), click **Options** and then click **Advanced**. On the **Network** tab, under **Connection**, click **Settings**.
- Google Chrome. In **Options**, click **Under the Hood**. Under **Network**, click **Change proxy settings**.

### 15.6.3 Agent Password

To change your **User password** go to the **Configure** tab, click **Agent Settings** and select the **Agent Password** section.

Here you can change the password for the user of Acronis vmProtect 9 Agent. The username (login) cannot be changed. In order to change the password you have to first provide the old password and then enter and confirm the new password in the corresponding fields.

Note that Managing **Agent Password** option is available only when the Agent is installed as a Virtual Appliance (p. 17). For Windows Agent (p. 18) connection Acronis vmProtect 9 uses Windows users accounts (any account with local logon permissions: user must be added to **Allow log on locally** security policy under **Start** -> **Secpol.msc** -> **Local Policies** -> **User Rights Assignment**).



User password

Login: admin

Current password:

New password:

Verify password:

Configuring settings, User password.

### 15.6.4 Export/Import Configuration

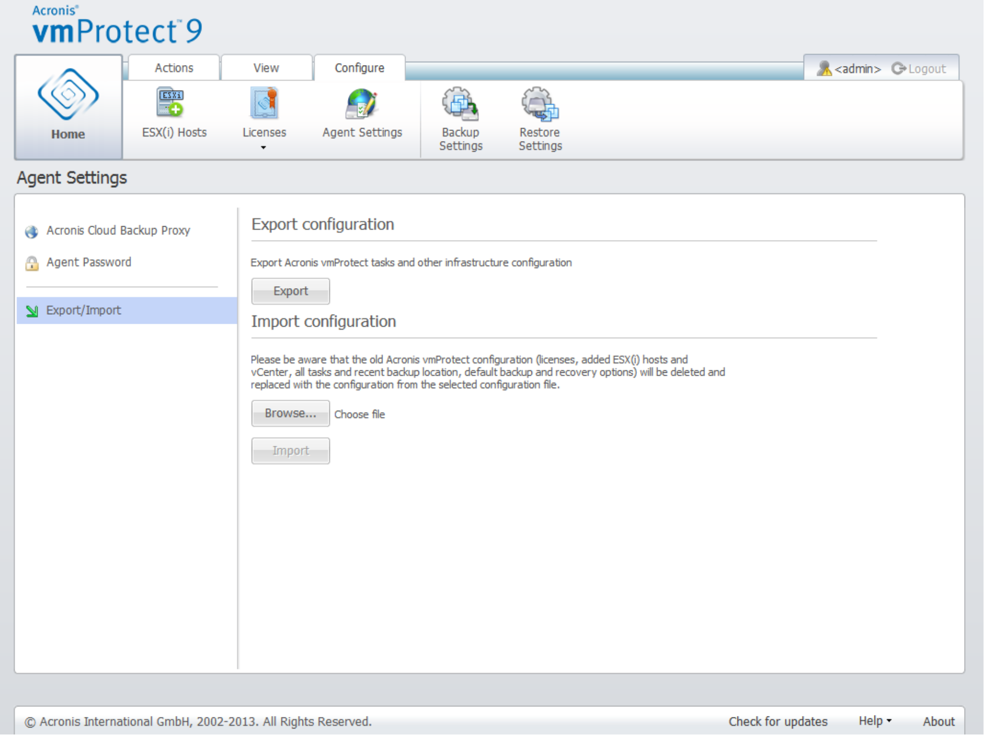
Go to the **Configure** tab, click **Agent Settings** and select the **Export/Import** section.

Here you can export and import the configuration of your Acronis vmProtect 9 Agent (Virtual Appliance/Windows Agent). This feature allows you to protect the agent against possible software/hardware crash by exporting the current configuration and reverting it back if required. You can also import the saved configuration on an another agent if for any reason you would need to reinstall it.

## Export Configuration

Click the **Export** button to save the Acronis vmProtect tasks and other infrastructure configuration as an .xml file to your local computer. The exported configuration includes:

- A list of added ESX(i) hosts with credentials to access these hosts/vCenter.
- A list of added licenses.
- All current tasks and their schedule.
- Recent backup locations such as Local Folders, Network Share, FTP/SFTP, Acronis Cloud Backup.
- Default backup/restore settings with credentials for e-mail notifications and archive protection (if set).
- Acronis Cloud Backup proxy settings.
- Log Cleanup rules.



Export Acronis vmProtect tasks and other infrastructure configuration

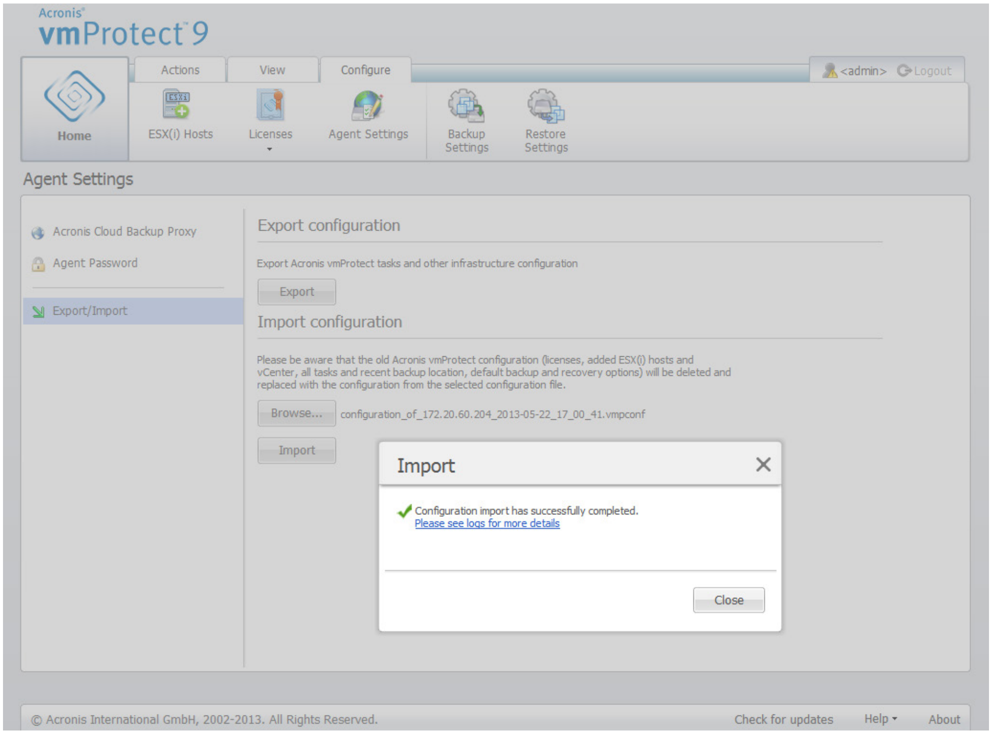
Please be aware that the old Acronis vmProtect configuration (licenses, added ESX(i) hosts and vCenter, all tasks and recent backup location, default backup and recovery options) will be deleted and replaced with the configuration from the selected configuration file.

© Acronis International GmbH, 2002-2013. All Rights Reserved.

Configuring settings, Export/Import configuration.

## Import Configuration

**Browse** to select your saved configuration file, then click the **Import** button to start the importing process. Please be aware that the old Acronis vmProtect configuration (licenses, added ESX(i) hosts and vCenter, all tasks and recent backup location, default backup and recovery settings) will be deleted and replaced with the configuration from the selected configuration file.



Export configuration

Export Acronis vmProtect tasks and other infrastructure configuration

Import configuration

Please be aware that the old Acronis vmProtect configuration (licenses, added ESX(i) hosts and vCenter, all tasks and recent backup location, default backup and recovery options) will be deleted and replaced with the configuration from the selected configuration file.

configuration_of_172.20.60.204_2013-05-22_17_00_41.vmpconf

✓ Configuration import has successfully completed.
Please see logs for more details

© Acronis International GmbH, 2002-2013. All Rights Reserved.

Configuring settings, Import configuration.

# 16 Best Practices

In this section we will give a few examples of some operations with Acronis vmProtect 9.

After you installed your Acronis vmProtect 9 Agent you have to connect to it with your access credentials.

### 1. Add ESX(i) host

First of all, to be able to perform backup and other operations, you have to specify the IP address/hostname and credentials for your vCenter or individual ESX(i) host where your virtual machines are running. Click **Configure ESX(i) Hosts** in the **Dashboard**'s **Quick Start**, or go to **ESX(i) Hosts** view in the **Configure** menu and click **Add**. Specify the vCenter or ESX(i) server and its access credentials. Detailed information can be found in the "Managing ESX(i) hosts" section (p. 99).

### 2. Add Licenses

Setting up an ESX(i) host will not bind the licenses to it automatically. You have to follow to the **Licenses** page to set up your licenses. Click **Configure Licenses** in the **Dashboard**'s **Quick Start**, or click **Licenses** view in the **Configure** menu. Then click **Add**, and submit your license key. The detailed information can be found in the "Managing licenses" section (p. 96).

After that is done you can practically start backing up your virtual infrastructure.

## 16.1 Backing up virtual machines to a network share

Let's discuss how to create a backup of several (for example, 5) virtual machines and save them over to a network share.

After setting up your **ESX(i) hosts** and **Licenses**, you have to run the **Create backup task** wizard, which will guide you through all the steps of the backup process. Click **Create Backup Task** in the **Dashboard's Quick Start**, or click **Backup** in the **Home** tab of the main menu. Then go through the **New Backup Task** wizard. Detailed information can be found in the "Creating a backup of virtual machines" section (p. 30).

On the step 1 of the **New Backup Task** wizard select your 5 virtual machines. Then on the step 2 browse the desired network share location where you would like to store your backup archives. On the steps 3 and 4 select the desired scheduling and backup method. And then finish the wizard. The created backup task will then perform what you needed to do. You can see the progress of this task in both **Dashboard** and in **Tasks** (**View** -> **Tasks**) views of Acronis vmProtect 9 interface.

## 16.2 Restoring a backup of a virtual machine to a new location

So you've made your backup. Now let's consider how to restore your backed up virtual machine, for example, to a new location.

In order to do that, you have to run the **Restore backup task** wizard which will guide you through all the steps of the restore process. Click **Restore** in the **Home** tab of the main menu. Then go through the wizard. The detailed information can be found in the "Restoring a backup of virtual machines" section (p. 54).

On the first step of the wizard select a backed up virtual machine. On the step 2 select the desired new location where you would like to restore your machine. On the step 3 select the preferences for your restore task, and then finish the wizard. Click on **Run Now** to restore the machine right away or Save to restore it later.

## 16.3 File/folders recovery

The first two cases show how to perform your backup and restore operations with Acronis vmProtect 9. Let's give one more example of how you could restore selected files from a specific archive. That's the case when you need to recover just a single file or just a few files from a backup archive without restoring the whole virtual machine.

Run the **File Recovery** wizard by clicking the **File Recovery** in the **Home** tab of the main menu. On the first step of the File Recovery wizard you need to select the recovery point for the virtual machine which defines the VM state you want to extract files or folders from. Then on the second step select the necessary files for recovery and click **Download**. The detailed information on **File Recovery** can be found in the "File recovery" section (p. 61).

Let's discuss another way to run the same wizard by accessing the recovery point directly from the **Recovery Points** view. Go to the **View** tab and click **Recovery Points**. Select the Virtual Machine state you want to recover your files from. After selecting the exact recovery point in the right section, click the **File Recovery** button in the context menu. You will go to the **File Recovery** wizard where Step 1 will be already pre-filled with the selected recovery point and you would just have to click **Next** to go to the Step 2. Then you have to select the files and/or folders you need to recover, and click **Download**.

# 17 Support

## 17.1 Technical Support

### Maintenance and Support Program

If you need assistance with your Acronis product, please go to http://www.acronis.eu/support/

### Product Updates

You can download the latest updates for all your registered Acronis software products from our website at any time after logging into your **Account** (https://www.acronis.eu/my) and registering the product. See **Registering Acronis Products at the Website** (http://kb.acronis.com/content/4834) and **Acronis Website User Guide** (http://kb.acronis.com/content/8128).

## 17.2 Troubleshooting

When having any troubles using Acronis vmProtect 9 or when contacting Acronis Technical Support, please save your working logs and send them to us. Please, go to **Logs** (p. 93) page and click **Save All to File** (p. 96).

More information about contacting Acronis Technical Support is available at http://www.acronis.eu/support/.

# 18 Glossary

## A

### Agent (Acronis vmProtect 9 Agent)

An application that performs backup and recovery of the virtual machines and enables other management operations on the VMware ESX(i) infrastructure such as task management and operations with available backups, machines, etc.

Acronis vmProtect 9 includes the Agent for backing up virtual machines residing on a VMware ESX(i) virtualization server which the Agent is connected to. There could be several ESX(i) hosts or a vCenter managed by one Agent. The best practice is to register vCenter on the Agent instead of specific ESX(i) hosts which are managed by this vCenter. Otherwise, vMotion (p. 121) will not be supported.

The Agent component can be either Windows-based, i.e. installed on a Windows platform, or Appliance-based, i.e. running on a special virtual machine on an ESX(i) host.

### Always Incremental archive

A new generation of the archive (p. 111) format which may contain several backups (p. 111) from different virtual machines inside. All backups are saved to this archive in incremental mode (p. 118). Physically all data is located inside one file as opposed to Legacy mode archive format where each backup is stored in a separate TIB file. Here is the description of how the backups rotation is performed inside the Always Incremental archive:

When one backup becomes expired according to the pre-defined retention rules (which say for example to “delete all backups older than 5 days”), the program marks the old blocks which belong to the expired backup as “free” ones. The blocks of the expired backup which have any dependencies (they may be used in newer backups due to incremental backup technology) are not marked as “free” to ensure the archive consistency. The archive will still be taking the same space on the storage as before. However, newer backups saved into this archive will first write data to the “free” blocks and will increase the total size of the archive only when all the “free” blocks are used.

This approach allows us to keep the archive size as small as possible and prevents it from growing indefinitely.

### Archive

See Backup archive (p. 112).

# B

## Backup

The result of a single backup operation (p. 112) as a single recovery point (p. 118) inside archive (p. 112). Physically, it is a file that contains a copy of the backed up data (virtual machine volumes) from specific date and time for a specific virtual machine. Backup files created by Acronis vmProtect 9 have a TIB extension. One backup file may include useful data from multiple machines plus necessary metadata inside.

## Backup archive (Archive)

A set of backups (p. 111) created and managed by a backup task (p. 113). An archive in Legacy mode format can contain multiple full backups (p. 117) as well as incremental (p. 118) and differential backups (p. 115). An archive of Always Incremental (p. 111) format can contain only incremental backups (the first backup will always be a full one). Backups belonging to the same archive are always stored in the same location. Multiple backup tasks can back up the same source data to the same archive, but a basic scenario is "one task – one archive".

Backups in an archive are managed by the backup task. Manual operations with archives (validation (p. 120), viewing contents, mounting and deleting backups) should be performed only using Acronis vmProtect 9. Do not modify your archives/backups using non-Acronis tools such as Windows Explorer or third-party file managers.

## Backup operation

An operation that creates a copy of the data that exists on a machine's hard disk for the purpose of recovering or reverting the data to a specified date and time.

## Backup options

Configuration parameters of a backup operation (p. 112), such as archive protection, source files exclusion or data compression level. Backup options are a part of a backup task (p. 113).

## Backup scheme

A part of the backup task (p. 113) that includes the backup schedule, [optionally] the retention rules, and the cleanup (p. 114) schedule. For example: perform full backup (p. 117) monthly on the last day of the month at 10:00AM and incremental backup (p. 118) on Sundays at 10:00PM (for old generation format archive (p. 111)). Delete backups that are older than 3 months. Check for such backups every time the backup operation is completed. If the backup is performed in Always Incremental (p. 111) mode, then there is no need to define it's type, i.e. Full or Incremental.

Acronis vmProtect 9 provides the ability to use well-known optimized backup schemes, such as GFS (p. 117), to create a custom backup scheme or to back up data once.

## Backup task (Task)

A set of rules that specify how the given virtual machine or a set of virtual machines will be protected. A backup task specifies:

- What data to back up (i.e. which machines to back up).
- Where to store the backup archive (the backup archive name and location).
- The backup scheme, including the backup schedule and [optionally] the retention rules.
- [Optionally] the archive validation rules.
- The backup options.

For example, a backup task can contain the following information:

- Back up virtual machines “VM1”, “VM2” (this is the data the task will protect).
- Set the backup archive name as MySystemVolume and it's location as \\server\backups\.
- Perform a full backup monthly on the last day of the month at 10:00AM and an incremental backup on Sundays at 10:00PM (for old generation format archive (p. 111)). Delete backups that are older than 3 months (this is a backup scheme).
- Validate the last backup immediately after its creation (this is a validation rule).
- Protect the archive with a password (this is an option).

Physically, a backup task is a set of pre-defined actions configured for execution on the Agent (p. 111) side in accordance with the specified parameters (Backup Options (p. 112)).

## Bootable agent

A bootable rescue utility that includes the backup functionality of the Acronis vmProtect 9 Agent (p. 111). It's typically for P2V (p. 118) migration. Bootable agent is based on Linux kernel. A machine can be booted into a bootable agent using the bootable media (p. 113). Operations can be configured and controlled only locally through the GUI.

## Bootable media

A physical media (CD, DVD, USB flash drive or other media supported by a machine BIOS as a boot device) that contains the bootable agent (p. 113).

Bootable media in Acronis vmProtect 9 is used to back up a physical machine in order to perform P2V (p. 118) migration.

# C

## CBT (Changed Block Tracking)

A feature of VMware ESX(i) which allows to identify which blocks of the virtual disks have changed and to transfer only those blocks during the backup/replication process. For example when using CBT technology, the incremental backup speed can increase up to 20 times.

## Cleanup

Deleting backups (p. 111) from a backup archive (p. 112) in order to get rid of outdated backups or prevent the archive from exceeding the desired size.

Cleanup consists of applying to an archive the retention rules set by the backup task (p. 113) that produces the archive. This operation checks if the archive has exceeded its maximum size and/or for expired backups. This may or may not result in deleting backups depending on whether the retention rules are violated or not.

For more information please refer to the User Guide (p. 32).

## Console (Acronis vmProtect 9 Management Console)

The console is the web-based user interface provided by the Acronis vmProtect 9 Agent in order to access the product functionality. This interface is accessible from any supported Internet browser after you go to specified URL, for example https://192.168.0.23:9876/, where 192.168.0.23 is the IP address of Acronis vmProtect 9 Agent (p. 111) and 9876 is the port. Using the direct web-based console-agent connection, the administrator performs direct management (p. 115).

# D

## Datastore

A logical container that holds virtual machine files and other files necessary for operations with virtual machine. Datastores can exist on different types of physical storage, including local storage, iSCSI, Fibre Channel SAN, or NFS. A datastore can be VMFS-based or NFS-based.

## Deduplication

A method of storing different duplicates of the same information only once.

Acronis vmProtect 9 can apply the deduplication technology to any backup archives (p. 112) of both Legacy mode (p. 118) and Always Incremental (p. 111) archive formats. This minimizes the storage space taken by the archives, backup traffic and network usage during the backup.

Deduplication in Acronis vmProtect 9 is managing data within only one backup archive. For example if the backups are saved into 2 different archives (even if they are in the same location) then there will be no relations between these archives and they may contain duplicated data.

## Differential backup

A differential backup stores changes to the data against the latest full backup (p. 117). You need access to the corresponding full backup to recover the data from a differential backup.

## Direct management

Any management operation that is performed on the Agent (p. 111) using the console (p. 114)-agent (p. 111) connection.

## Disk group

A number of dynamic disks (p. 116) that store the common configuration data in their Logical Disk Manager (LDM) databases and therefore can be managed as a whole. Normally, all dynamic disks created within the same machine are members of the same disk group.

As soon as the first dynamic disk is created by the LDM or another disk management tool, the disk group name can be found in the registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\dmio\Boot Info\Primary Disk Group\Name.

The next created or imported disks are added to the same disk group. The group exists until there is at least one of its members. Once the last dynamic disk is disconnected or converted to basic, the group is discontinued, though its name is kept in the above registry key. In case a dynamic disk is created or connected again, a disk group with an incremental name is created.

When moved to another machine, a disk group is considered as ‘foreign’ and cannot be used until imported into the existing disk group. The import updates the configuration data on both the local and the foreign disks so that they form a single entity. A foreign group is imported as is (will have the original name) if no disk group exists on the machine.

For more information about disk groups, please refer to the following Microsoft knowledge base article:

222189 Description of Disk Groups in Windows Disk Management
http://support.microsoft.com/kb/222189/EN-US/.

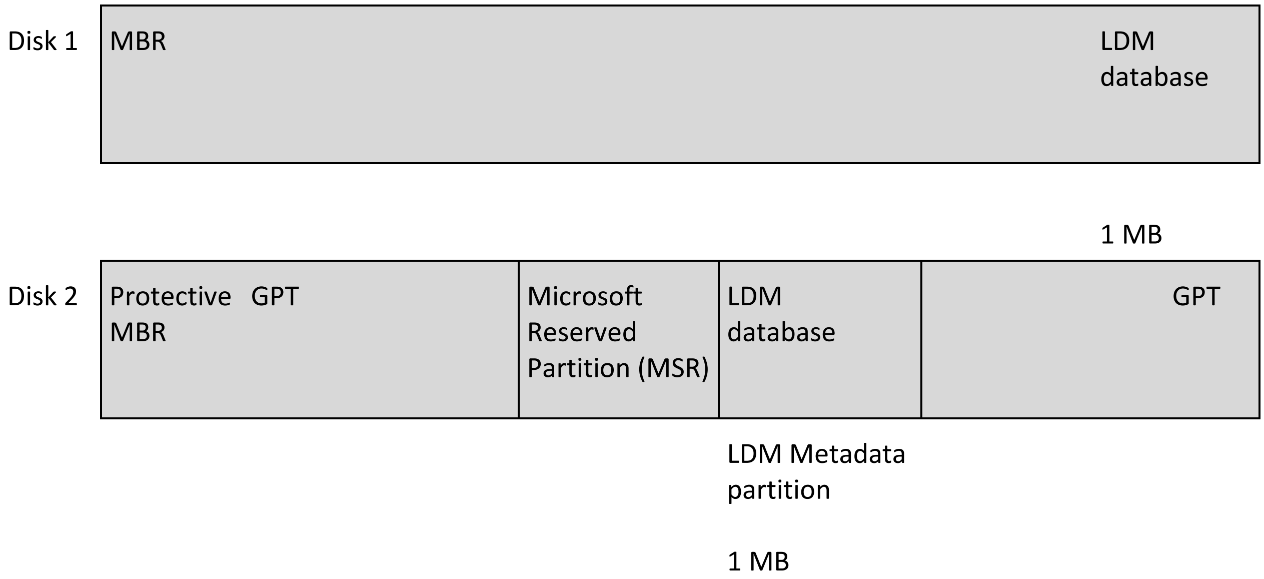
## Distributed Resource Scheduler (DRS)

A VMware vCenter specific feature which allows automatic load balancing of a ESX(i) cluster using vMotion (p. 121).

## Dynamic disk

A hard disk managed by Logical Disk Manager (LDM) that is available in Windows starting with Windows 2000. LDM helps flexibly allocate volumes on a storage device for better fault tolerance, better performance or larger volume size.

A dynamic disk can use either the master boot record (MBR) or GUID partition table (GPT) partition style. In addition to MBR or GPT, each dynamic disk has a hidden database where the LDM stores the dynamic volumes' configuration. Each dynamic disk holds the complete information about all dynamic volumes existing in the disk group which makes for better storage reliability. The database occupies the last 1MB of an MBR disk. On a GPT disk, Windows creates the dedicated LDM Metadata partition, taking space from the Microsoft Reserved Partition (MSR).



Dynamic disks organized on MBR (Disk 1) and GPT (Disk 2) disks.

For more information about dynamic disks please refer to the following Microsoft knowledge base articles:

Disk Management (Windows XP Professional Resource Kit) http://technet.microsoft.com/en-us/library/bb457110.aspx.

816307 Best practices for using dynamic disks on Windows Server 2003-based computers http://support.microsoft.com/kb/816307.

## Dynamic volume

Any volume located on dynamic disks (p. 116), or more precisely, on a disk group (p. 115). Dynamic volumes can span multiple disks. Dynamic volumes are usually configured depending on the desired goal:

- To increase the volume size (a spanned volume).

- To reduce the access time (a striped volume).
- To achieve fault tolerance by introducing redundancy (mirrored and RAID-5 volumes).

When backing up virtual machines which contain dynamic disks inside, Acronis vmProtect 9 backs up the logical dynamic volumes instead of the entire dynamic disks structure.

# E

## Encrypted archive

A backup archive (p. 112) encrypted according to the Advanced Encryption Standard (AES). When the encryption option and a password for the archive are set in the backup options (p. 112), each backup belonging to the archive is encrypted by the agent (p. 111) before saving the backup to its destination.

The AES cryptographic algorithm operates in the Cipher-block chaining (CBC) mode and uses a randomly generated key with a user-defined size of 128, 192 or 256 bits. The encryption key is then encrypted with AES-256 using a SHA-256 hash of the password as a key. The password itself is not stored anywhere on the disk or in the backup file; the password hash is used for verification purposes. With this two-level security, the backup data is protected from any unauthorized access, but recovering a lost password is not possible.

# F

## Full backup

A self-sufficient backup (p. 111) containing all data selected for backup. To recover the data from a full backup, access to any other backup is not needed.

# G

## GFS (Grandfather-Father-Son)

A popular backup scheme (p. 112) aimed at maintaining the optimal balance between a backup archive (p. 112) size and the number of recovery points (p. 118) available from the archive. GFS enables recovering with daily resolution for the last several days, weekly resolution for the last several weeks and monthly resolution for any time in the past.

For more information please refer to GFS backup scheme.

# H

## High Availability (HA)

VMware vCenter specific feature which, in case of cluster hardware failure, allows to automatically restart the virtual servers on another host in the cluster.

# I

## Incremental backup

A backup (p. 111) that stores changes to the data against the latest backup. You need access to other backups from the same archive (p. 111) to restore data from an incremental backup.

# L

## Legacy mode Archive

See Backup archive (p. 112).

# M

## Machine (Virtual machine)

A virtual computer uniquely identified by an operating system installation.

## Media builder

A dedicated tool for creating bootable media (p. 113).

# P

## P2V

Migration of physical machine to virtual environment. Typically P2V process includes the following steps:

- Create a backup of physical machine using special bootable media (p. 113).
- Restore it to virtual environment (ESX(i) server).

# R

## Recovery point

Date and time to which the backed up data can be reverted.

## Registered machine

A virtual machine managed by Acronis vmProtect 9 Agent. All virtual machines which reside on the registered ESX(i) host or vCenter are automatically registered and can be managed by Acronis vmProtect 9 Agent.

## Replication

A process of replicating the virtual machine to new location (new datastore and/or resource pool). As the result of this process there will be a duplicate virtual machine created which is running independently from the original one.

## Resource Pool

A VMware term describing the concepts of resource management in an ESX(i) virtualized environment. A resource pool provides a way to divide the resources of a stand-alone ESX(i) host or an ESX(i) cluster into smaller pools. A resource pool is configured with a set of CPU and memory resources that the virtual machines that run in the resource pool share. Resource pools are self-contained and isolated from other resource pools.

One can combine multiple physical servers into a single resource pool that aggregates CPU and memory capacity.

Virtual machines execute in, and draw their resources from, resource pools. This arrangement allows virtual machine workloads to continuously balance across resource pools. When the workload increases, the vCenter Server automatically allocates additional resources and transparently migrates virtual machines between hosts in the resource pool.

# S

## Storage vMotion

VMware vCenter specific feature which allows moving a running virtual machine from one storage device to another.

# T

## Task

In Acronis vmProtect 9, a task is a sequence of actions to be performed on a registered machine at a certain time or when a certain event occurs. The actions are described in an xml script file. The start condition (schedule) exists in the protected registry keys (for Windows-based Agent) or in protected files (for Appliance-based Agent).

# U

## Universal Restore (Acronis Universal Restore)

The Acronis proprietary technology that helps boot up Windows on dissimilar hardware or a virtual machine. The Universal Restore handles differences in devices that are critical for the operating system start-up, such as storage controllers, motherboard or chipset.

In Acronis vmProtect 9 the Universal Restore technology is primarily used for P2V (p. 118) migration scenarios.

Universal Restore is not available when recovering Linux.

# V

## Validation

An operation that checks the possibility of data recovery from a backup (p. 111).

Validation of a virtual machine backup calculates a checksum for every data block saved in the backup. This procedure is resource-intensive.

While the successful validation means a high probability of successful recovery, it does not check all factors that influence the recovery process. If you back up the operating system, only a test recovery to new/existing virtual machine or running virtual machine from the backup can guarantee successful recovery in the future.

## Validation rules

A part of the backup task (p. 113). Rules that define when and how often to perform validation and whether to validate the entire archive (p. 111) or the latest backup in the archive.

## vApp

A group of virtual machines that can be managed as a single object. vApps simplify management of complex, multi-tiered applications that run on multiple interdependent virtual machines. vApps have the same basic operations as virtual machines and resource pools. With vApps, you can set the order in which the virtual machines in the vApp power on, automatically assign IP addresses to virtual machines in the vApp, and provide application-level customization.

In terms of Acronis vmProtect 9 product the “vApp” is considered to be a container for VMs. This container has its own properties which are included into the backup and are restored along with vApp once some parts of it (or entire vApp) are restored.

## vCenter

VMware vCenter Server, formerly VMware VirtualCenter, centrally manages VMware vSphere environments allowing IT administrators dramatically improved control over the virtual environment compared to other management platforms.

See more details at http://vmware.com/products/vcenter-server/.

In terms of Acronis vmProtect 9 product the “vCenter” item is considered to be a container for the ESX(i) virtual infrastructure including datacenters, ESX(i) hosts, etc.

## vMotion

A VMware vCenter specific feature which allows the migration of operational guest virtual machines between similar but separate hardware hosts sharing the same storage. Each of these transitions is completely transparent to any users on the virtual machine at the time it is being migrated.