

Acronis



Acronis Backup Advanced for vCloud

Update 8

QUICK START GUIDE

Copyright Statement

Copyright © Acronis International GmbH, 2003-2020. All rights reserved.

“Acronis” and “Acronis Secure Zone” are registered trademarks of Acronis International GmbH.

“Acronis Compute with Confidence”, “Acronis Startup Recovery Manager”, “Acronis Instant Restore” and the Acronis logo are trademarks of Acronis International GmbH.

Linux is a registered trademark of Linus Torvalds.

VMware and VMware Ready are trademarks and/or registered trademarks of VMware, Inc. in the United States and/or other jurisdictions.

Windows and MS-DOS are registered trademarks of Microsoft Corporation.

All other trademarks and copyrights referred to are the property of their respective owners.

Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of this work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

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 <https://kb.acronis.com/content/7696>

Acronis patented technologies

Technologies, used in this product, are covered and protected by one or more U.S. Patent Numbers: 7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234; and patent pending applications.

Table of contents

1	What is Acronis Backup Advanced for vCloud?	4
2	Software requirements	4
3	Components	6
4	What you need to start	7
5	Step-by-step instructions	8
5.1	Installing and configuring RabbitMQ Server	8
5.2	Installing Acronis Backup Advanced for vCloud	9
5.2.1	Installing the management server	9
5.2.2	Running the SQL Server configuration script	11
5.2.3	Integrating the management server with vCenter Server	12
5.2.4	Deploying Agent for VMware	15
5.2.5	Installing Agent for vCloud	17
5.2.6	Configuring Agent for vCloud	17
5.3	Enabling backup for an organization	20
5.4	Backing up virtual machines	21
5.5	Applying a backup plan	22
5.6	Overwriting a virtual machine with its backed-up version	23
5.7	Recovering a virtual machine	24
5.8	Recovering files from a virtual machine backup	25

This document describes how to quickly install and start using Acronis Backup Advanced for vCloud.

This document outlines the product usage and enables immediate "field testing." For more information about administering Acronis Backup Advanced for vCloud, please refer to the Administrator's Guide that you can open by clicking the **Help** link in the web interface of the product.

1 What is Acronis Backup Advanced for vCloud?

Acronis Backup Advanced for vCloud is a solution for backup and recovery of virtual machines managed by VMware vCloud Director.

Acronis Backup Advanced for vCloud provides the backup service at a system administrator level and organization user level. The backup service is available through a web interface. Users log in to the service by using their vCloud Director credentials.

2 Software requirements

Supported VMware vCloud Director versions

- VMware vCloud Director 1.5
- VMware vCloud Director 5.0
- VMware vCloud Director 5.1
- VMware vCloud Director 5.5, 5.6
- VMware vCloud Director 8.0, 8.1, 8.2
- VMware vCloud Director 9.0, 9.5, 9.7
- VMware vCloud Director 10.0

Supported guest operating systems

Acronis Backup Advanced for vCloud supports a wide range of guest operating systems, including Windows 10, Windows Server 2019, and all popular Linux distributions.

Supported web browsers

The web interface supports the following web browsers:

- Google Chrome 29 or later
- Mozilla Firefox 23 or later
- Opera 16 or later
- Windows Internet Explorer 10 or later
In cloud deployments, the management portal supports Internet Explorer 11 or later.
- Microsoft Edge 25 or later
- Safari 8 or later running in the macOS and iOS operating systems

In other web browsers (including Safari browsers running in other operating systems), the user interface might be displayed incorrectly or some functions may be unavailable.

Make sure that JavaScript is enabled in the browser.

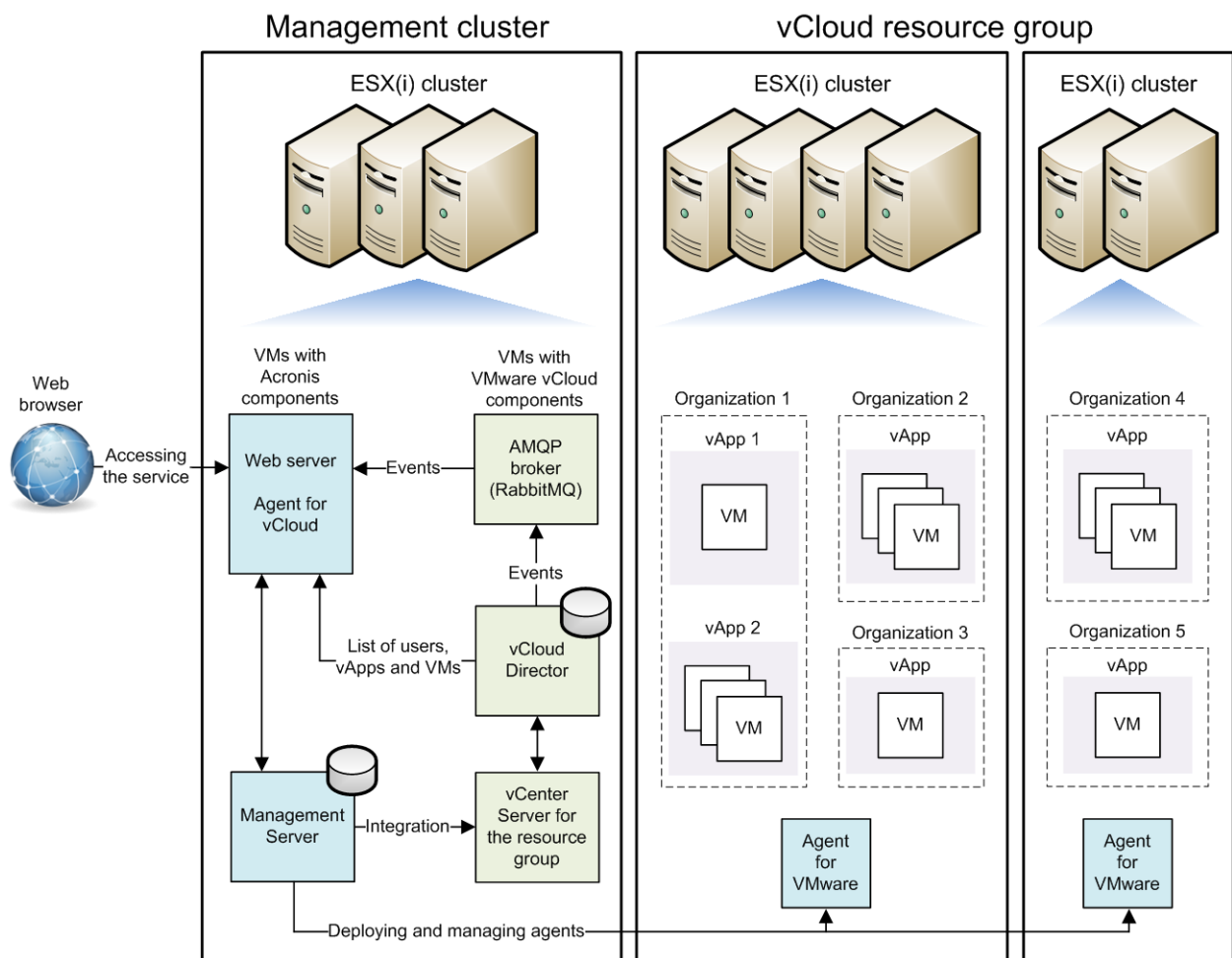
The screen resolution for displaying the graphical user interface must be 1024x768 or higher.

3 Components

Acronis Backup Advanced for vCloud consists of multiple components that need to be installed on separate machines.

- **Agents for VMware** run as virtual appliances in the vCloud resource group.
The default settings of the agent machine: 1 GB of memory, 6 GB of disk space, and two CPU.
- **Management Server** needs to be installed in the management cluster, on a virtual machine running Windows.
Minimum requirements for the machine: 3 GB of memory, 30 GB of disk space, and two CPU.
- **Agent for vCloud** needs to be imported from an Open Virtualization Format (OVF) template to the management cluster. The agent is a Linux virtual machine, which also serves as the web server.
The default settings of the agent machine: 2 GB of memory, 8 GB of disk space, and one CPU.

The following diagram illustrates a typical installation and interaction of the components.



4 What you need to start

Make sure that:

- **vCloud Director is installed and configured.**
- **You have license keys in a TXT file.**
For multiple license keys, the text format is one line per key.
- **You have the Acronis Backup Advanced for vCloud installation package.**
The package consists of:
 - Acronis Backup Advanced setup program.
 - Agent for vCloud OVF template.
 - The script `enable_remote_sql_access.js`.
- **You have a virtual machine to install the management server on.**
 - The machine must run a Windows operating system (except for the Start, Home, and RT editions).
 - The machine must have network access to the vCenter Server for the resource group and to the resource group ESX(i) clusters.
- **You have a storage that supports any of the following network protocols: NFS, SMB, FTP, or SFTP.**

The storage capacity must be enough for storing the organizations' backups. For each organization, create a separate shared folder on this storage.

If you want to use NFS shares to store backups, install Microsoft Windows Services for NFS on the machine where the management server will be installed. On the machine where the NFS server is installed, choose a user account that will act as the anonymous account, and then configure the export folder by specifying the following parameters in the `/etc/exports` file:

```
/opt/backups *(rw,sync,all_squash,anonuid=1000,anongid=1000)
```

In this example, the folder name is `/opt/backups`, and the user ID and group ID of the anonymous account are 1000.

5 Step-by-step instructions

The following steps will guide you through the installation and basic use of Acronis Backup Advanced for vCloud. They describe how to:

- Install and configure the main components of the product and the required software.
- Enable the backup service for an organization.
- Back up organization's virtual machines.
- Apply a backup plan to the virtual machines.
- Overwrite a virtual machine with its earlier version.
- Recover a virtual machine.

5.1 Installing and configuring RabbitMQ Server

Agent for vCloud obtains events from vCloud Director via the RabbitMQ Server AMQP broker.

If your vCloud Director already uses a RabbitMQ Server, make sure that the exchange type is set to **topic**, and continue to "Installing Acronis Backup Advanced for vCloud" (p. 9).

If RabbitMQ Server is already installed, but **not** used by vCloud Director, skip to step 5 of the following procedure.

To install and configure RabbitMQ Server

1. Download RabbitMQ Server from <http://www.rabbitmq.com/download.html>.
2. If you want to install RabbitMQ Server on a machine running Windows, download and run Erlang Windows Binary File, which is available at <http://www.erlang.org/download.html>.
3. Follow the RabbitMQ installation instructions to install RabbitMQ on any convenient host. The host must have network access to vCloud Director.
4. The RabbitMQ management plug-in is required so that you can configure RabbitMQ Server. Do one of the following, depending on the operating system of the RabbitMQ Server host:

- In Linux, run the following commands:

```
rabbitmq-plugins enable rabbitmq_management  
service rabbitmq-server stop  
service rabbitmq-server start
```

- In Windows:

- Go to **Start > All programs > RabbitMQ Server > RabbitMQ Command Prompt**.
Ensure that the command prompt shows the folder containing the RabbitMQ Server executable files, such as C:\Program Files\RabbitMQ Server\rabbitmq_server-3.1.5\sbin.
If necessary, change the folder by using the **cd** command.
- Run the following command: **rabbitmq-plugins enable rabbitmq_management**
- Run **Start > All programs > RabbitMQ Server > RabbitMQ Service - stop**.
- Run **Start > All programs > RabbitMQ Server > RabbitMQ Service - start**.

5. Run the following commands on the RabbitMQ Server host to create a new user account:

```
rabbitmqctl add_user <username> <password>  
rabbitmqctl set_user_tags <username> management  
rabbitmqctl set_permissions -p / <username> ".*" ".*" ".*"
```

Here, <username> and <password> are the name and password of the user account to create.

Note You can use an existing RabbitMQ Server user account with permissions equal to or higher than those given by the commands above.

Acronis Backup Advanced for vCloud Agent for vCloud will use this account to receive event notifications from vCloud Director. Remember the account credentials, as you will be asked for them when configuring Agent for vCloud.

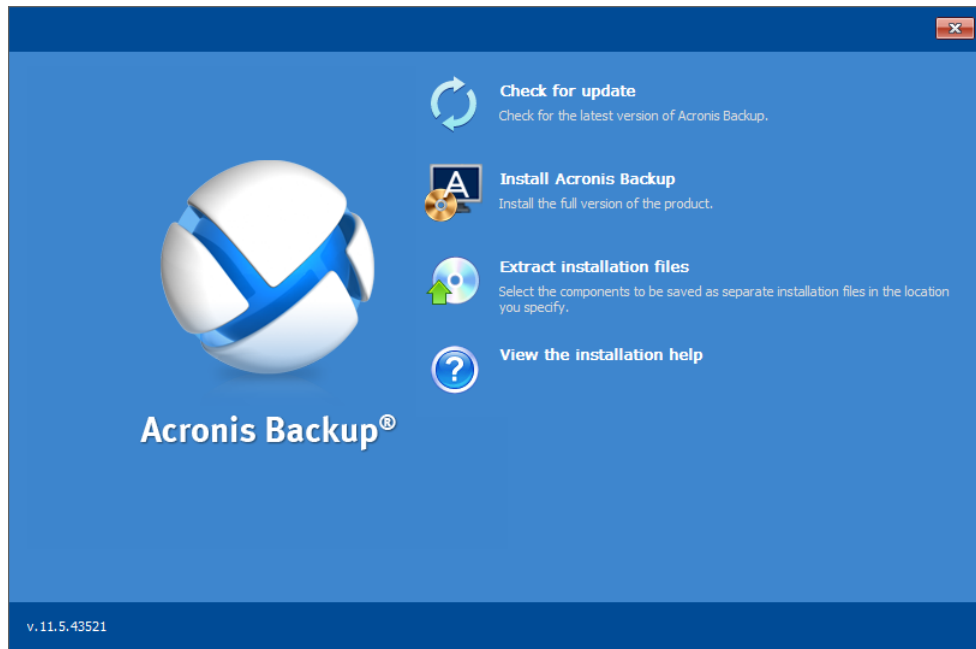
6. Open a web browser and go to the RabbitMQ Server Web UI located at: **http://<server name>:15672/**. Here, <server name> is the address of the RabbitMQ Server host.
7. Provide the credentials of the RabbitMQ Server user created in step 5.
8. Click **Exchanges**.
9. Under **Add a new exchange**:
 - a. In **Name**, specify a name for a new exchange that will be used by Agent for vCloud. For example, specify **vcdExchange**.
 - b. In **Type**, select **topic**.
 - c. Leave the default values for all other settings.
 - d. Click **Add exchange**.
10. Log in as an administrator to vCloud Director.
11. Click **Administration**.
12. Under **System settings**, click **Extensibility**.
13. Under **Notifications**, select the **Enable notifications** check box.
14. Under **AMQP Broker Settings**:
 - a. In **AMQP Host**, specify the name or IP address of the RabbitMQ Server host.
 - b. In **AMQP Port**, type 5672.
 - c. In **Exchange**, specify the name of the new exchange that you created in step 9.
 - d. In **vHost**, type **/**.
 - e. In **Prefix**, type **vcd**.
 - f. In **User Name** and **Password**, type the credentials of the user account created in step 5.
15. Click **Apply**.

5.2 Installing Acronis Backup Advanced for vCloud

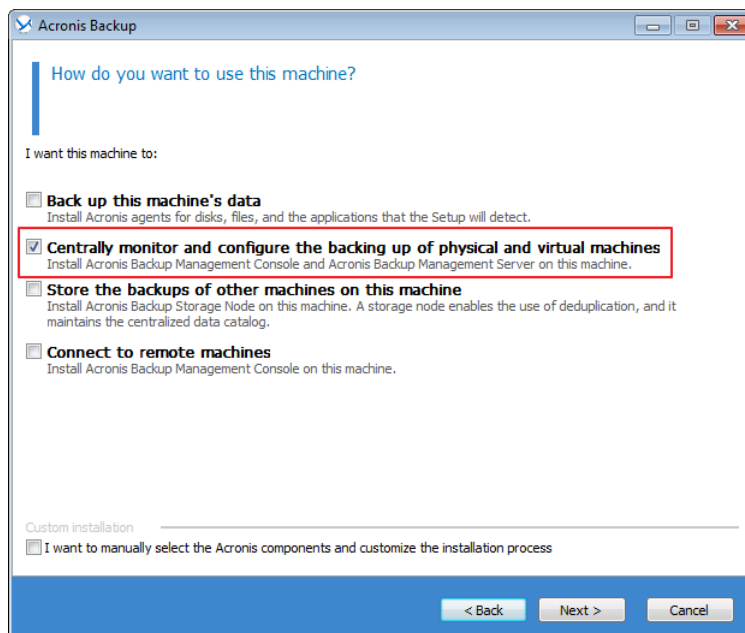
5.2.1 Installing the management server

1. On the machine that will act as the management server, log on as an administrator.
2. Start the Acronis Backup Advanced setup program.

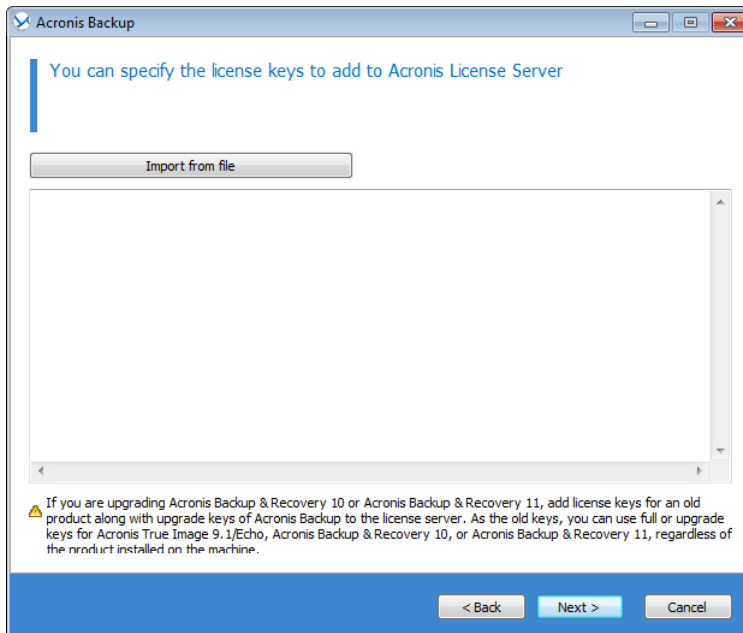
3. Click **Install Acronis Backup**.



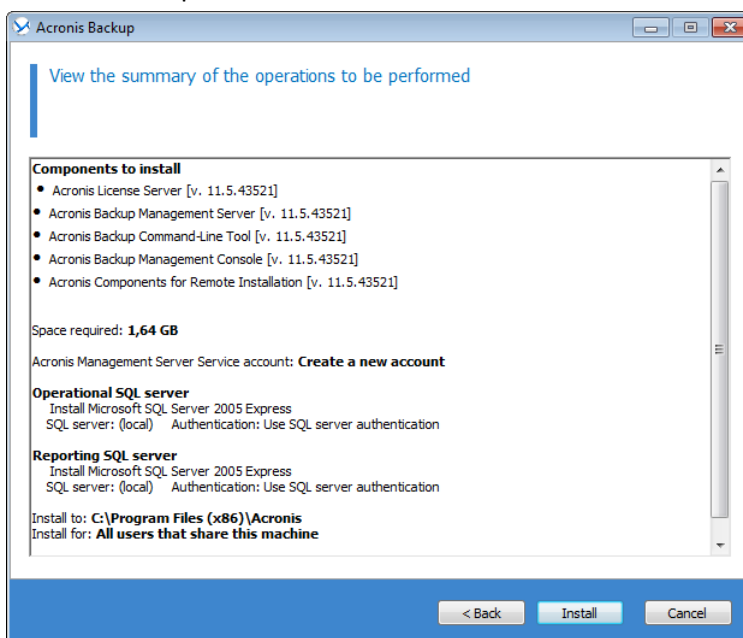
4. Accept the terms of the license agreement.
5. Select the **Centrally monitor and configure backing up of physical and virtual machines** check box.



6. Provide the license for Acronis Backup Advanced for vCloud. Enter your license keys or import them from a text file.



7. Choose whether the machine will participate in the Acronis Customer Experience Program (CEP).
8. Click **Install** to proceed with installation.



9. On successful installation, click **Finish** to close the wizard window.

5.2.2 Running the SQL Server configuration script

1. Copy the script **enable_remote_sql_access.js** that is distributed with the product, to the management server machine.

Details. The script configures the SQL Server instance to be accessible to Agent for vCloud. It creates a new SQL Server account that Agent for vCloud will use, configures the instance to listen to a static port, and configures Windows Firewall to allow connections through that port.

2. Run the script in the following format:

```
cscript enable_remote_sql_access.js <new-user-name> <new-password> [-p <port>]
```

Where:

- <new-user-name> and <new-password> are the user name and password for the new account.
- **-p** <port> is an optional parameter that enables you to specify the port to use.

For example:

```
C:\>cscript enable_remote_sql_access.js User 123
```

```
G:\Users\Administrator>cscript enable_remote_sql_access.js User 123
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

Processing instance 'ACRONIS'
Adding SQL authentication mode...
Enabling TCP protocol...
Picking free port...
Checking port 1433...
Port 1433 is picked
Setting port 1433 for IPAll Tcp protocol
Opening firewall port 1433
Restarting SQL services...
Stopping the service 'MSSQL$ACRONIS'
Starting the service 'MSSQL$ACRONIS'
Waiting for 4 seconds for SQL Server to come up
Adding SQL user 'User'...
```

If you do not specify the port, it will be chosen automatically. Examine the port number that was chosen by the script:

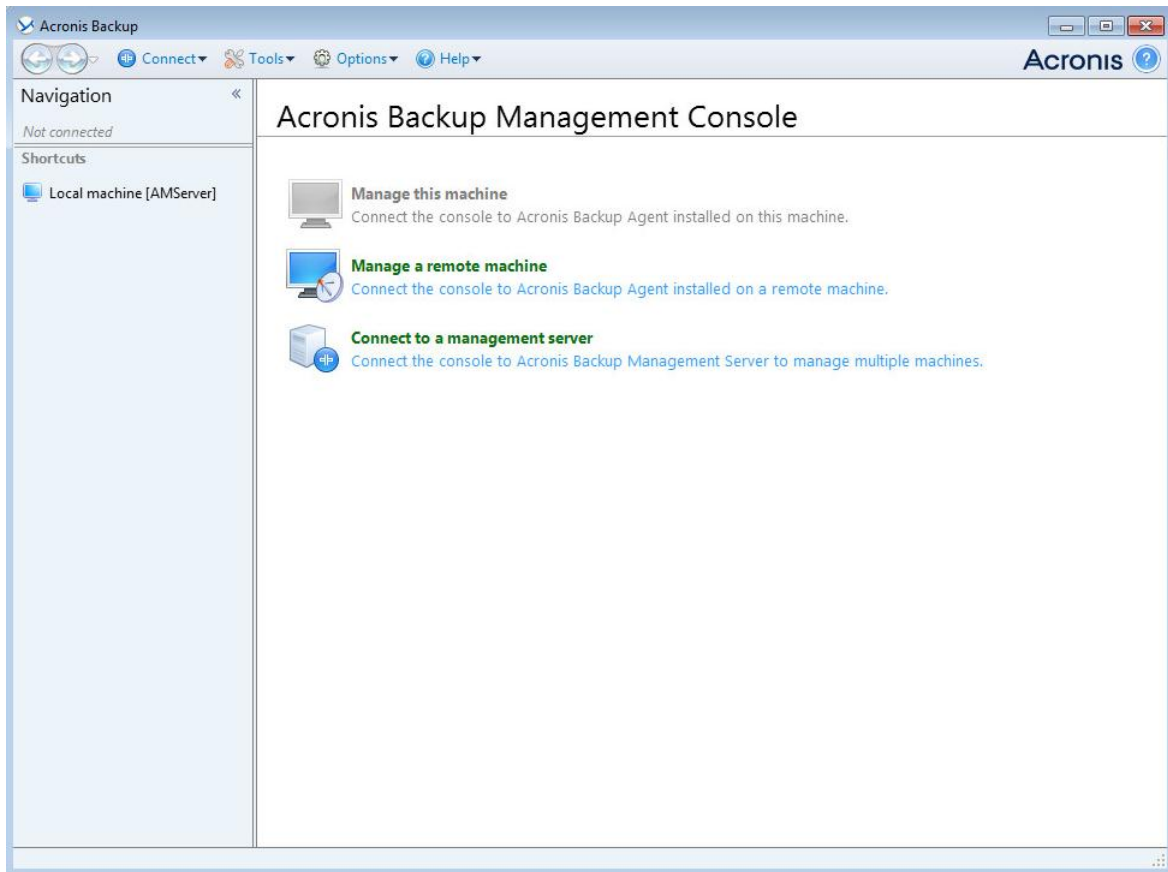
```
Port 1433 is picked
```

Important. Remember the credentials and the port number. You will be asked for them when configuring Agent for vCloud.

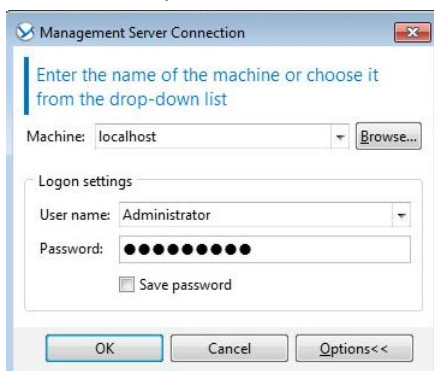
5.2.3 Integrating the management server with vCenter Server

1. On the machine where you installed the management server, click **Acronis Backup** on the desktop.

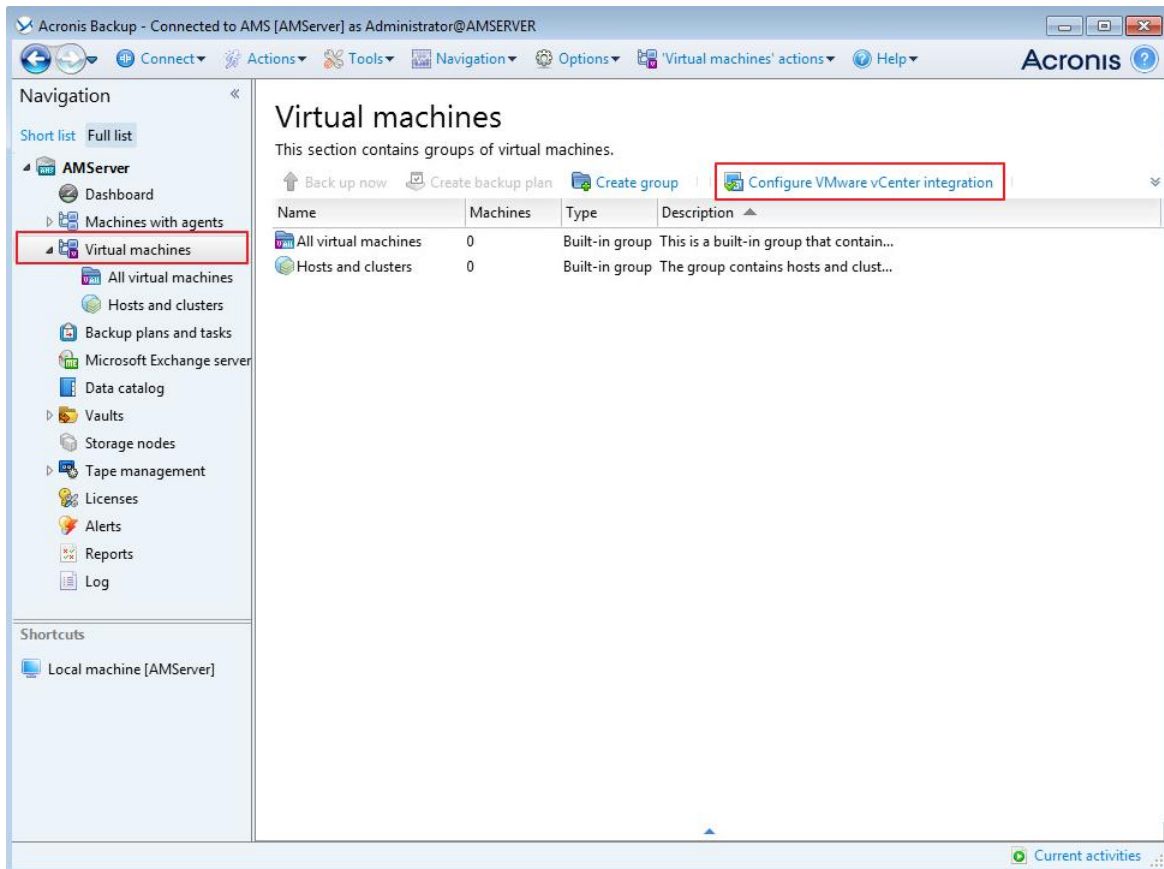
2. Click **Connect to a management server**.



3. Specify the host name or IP address of the current machine and the administrator credentials under which you installed the management server.

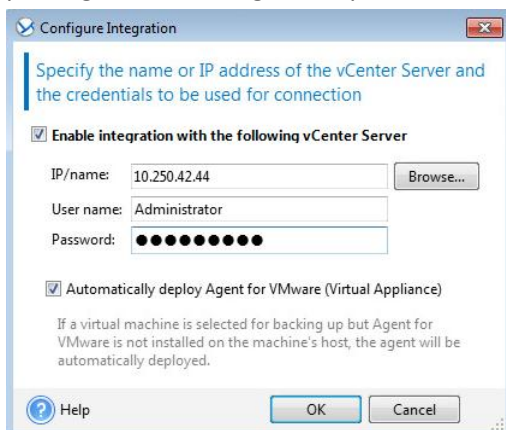


4. In the **Navigation tree**, click **Virtual machines** and then click **Configure VMware vCenter integration**.



5. Select the **Enable integration with the following vCenter Server** check box.
6. Specify the IP address or name of the vCenter Server for the resource group. Provide credentials of the vCenter Server administrator.

Details. The management server will use this account when deploying agents. The agents will use this account to connect to the vCenter Server. Therefore, the account must have the necessary privileges for creating, backup, and recovery of virtual machines.



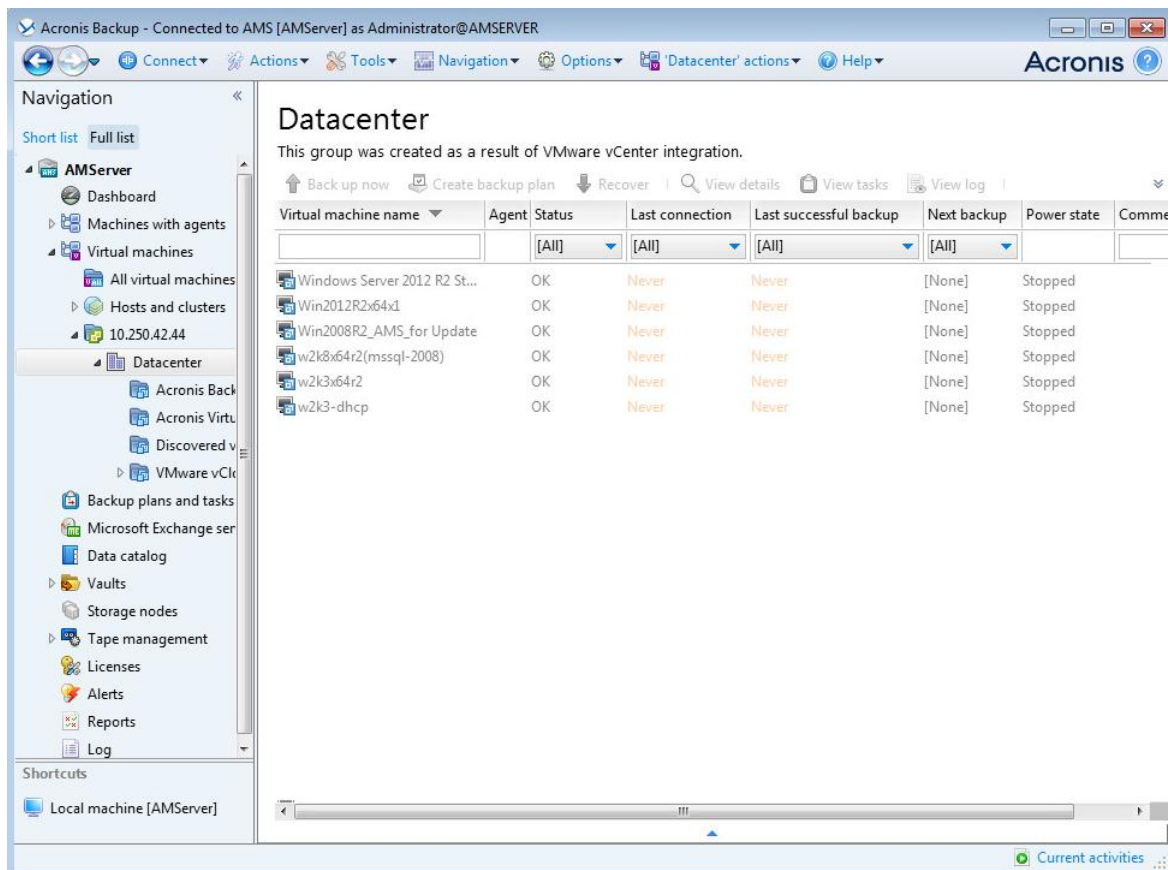
7. If you use VMware vSphere 6.5:
 - Clear the **Automatically deploy Agent for VMware (Virtual Appliance)** check box. You will need to manually import the agents from the OVF template as described in the "Importing Agent for VMware" section of the Administrator's Guide.

If you use VMware vSphere versions earlier than 6.5:

- If a DHCP server is present on the network, you may want to leave the **Automatically deploy...** check box selected. When a backup is about to start, the management server will automatically deploy Agent for VMware to every cluster that has virtual machines to be backed up but does not have the agent yet.
- If the network uses static IP addresses, or if you prefer to deploy the agents manually, or if the automatic deployment fails, clear the **Automatically deploy...** check box. You will need to perform a few additional steps described in "Deploying Agent for VMware" (p. 15).

8. Click **OK** to confirm the changes.

The virtual machines managed by the vCenter Server appear in the **Virtual machines** section of the **Navigation tree**. The virtual machines are shown as grayed out because Agent for VMware has not been deployed yet.



5.2.4 Deploying Agent for VMware

If you use VMware vSphere 6.5

Refer to the "Importing Agent for VMware" section of the Administrator's Guide.

If you use VMware vSphere versions earlier than 6.5

Agent for VMware (Virtual Appliance) will be deployed automatically as necessary, if this option was enabled when integrating the management server with the vCenter Server (p. 12).

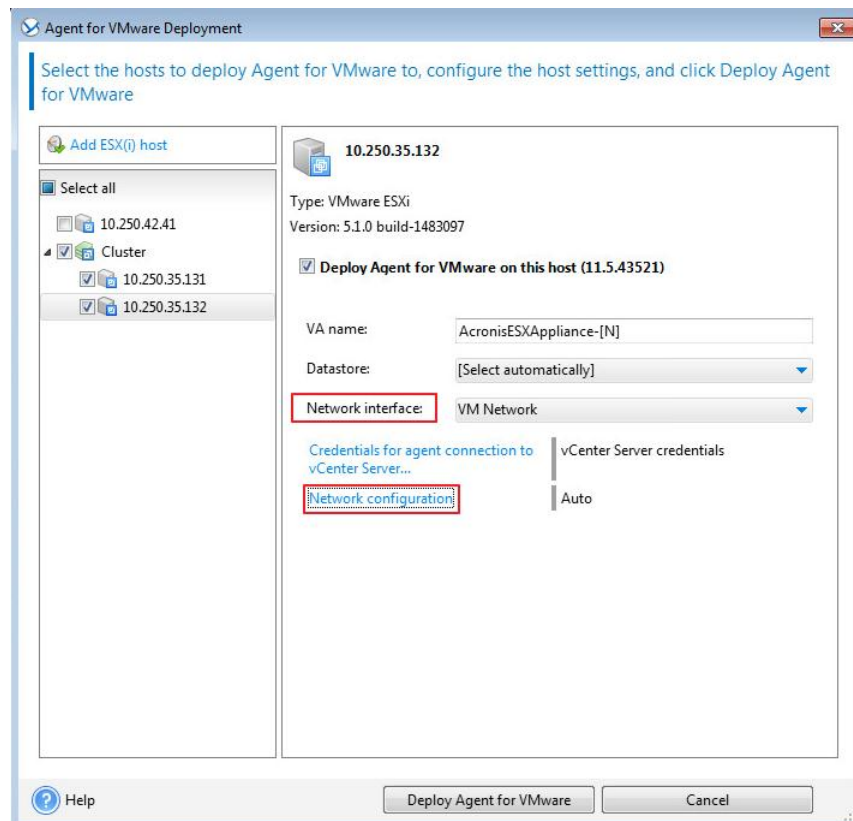
If you disabled the automatic deployment, deploy the agent to every ESX(i) cluster whose virtual machines will be backed up.

To deploy Agent for VMware

1. Connect the console to the management server as described in "Using the management console".
2. In the **Navigation** tree, expand **Virtual machines**, and then right-click the IP address or name of the vCenter Server for the resource group.
3. Click **Deploy Agent for VMware**.
4. For each of the clusters whose virtual machine will be backed up, do the following:
 - a. Select a host to which you want to deploy the agent.
 - b. In **Network interface**, select the network interface that provides access to the management server, the vCenter Server for the resource group, the cluster virtual machines, and the backup storage.
 - c. The **Network configuration** link enables you to select whether the agent will use a dynamic (provided by a DHCP server) or a static IP address. If you want to leave the default setting of using a dynamic address, skip this step.

If you want the agent to use a static IP address:

- Click **Network configuration**.
- Select **Use the following network settings**.
- Specify the appropriate network settings for the agent, and then click **OK**.



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

5. Click **Deploy Agent for VMware**.

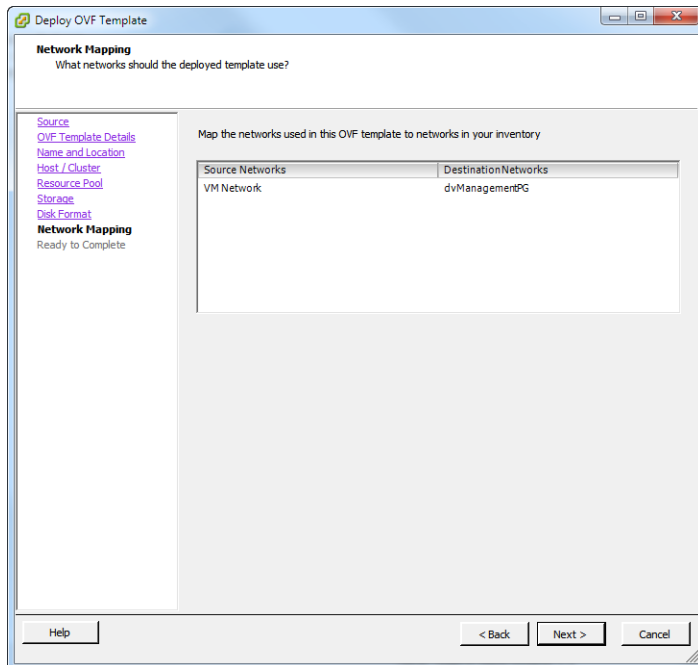
The management server starts deploying Agent for VMware. The progress is shown at the bottom of the window.

Once the agent is successfully deployed, the agent machine appears in the **Machines with agents** view of the management server.

5.2.5 Installing Agent for vCloud

Agent for vCloud is delivered as an OVF template.

To install the agent, deploy the OVF template to your management cluster. Map the network in the OVF template to a network that provides access to the management cluster virtual machines and to the RabbitMQ Server host.



For general information about deploying an OVF template, refer to the following VMware knowledge base article:

http://pubs.vmware.com/vsphere-50/topic/com.vmware.vsphere.vm_admin.doc_50/GUID-6C847F77-8CB2-4187-BD7F-E7D3D5BD897B.html.

5.2.6 Configuring Agent for vCloud

Logging in

Log in as a root user to the machine with Agent for vCloud. The default credentials are:

- User name: **root**
- Password: **Default0** (case-sensitive)

Configuring the time zone

Set the time zone to that of the vCloud Director machine. This will enable Agent for vCloud to convert time between user's and vCloud Director's time zones.

1. Find out the time zone of the vCloud Director machine. If you are not sure, log on to the machine and run the **date** command. The output contains the time zone abbreviation. For example:

```
Mon Aug 26 23:00:00 EST 2013
```

EST stands for Eastern Standard Time. This time zone includes parts of the United States and Canada, and some countries in South America. For more abbreviations see <http://www.timeanddate.com/library/abbreviations/timezones/>.

2. On the machine with Agent for vCloud, in the **/usr/share/zoneinfo** directory, find the file that corresponds to your region and time zone.

For example, for the Eastern Time Zone of the United States, the time zone file is:

/usr/share/zoneinfo/US/Eastern

3. Delete the old time zone settings:

```
rm -f /etc/localtime
```

4. Specify the new time zone settings:

```
ln -s <time_zone_file> /etc/localtime
```

For example:

```
ln -s /usr/share/zoneinfo/US/Eastern /etc/localtime
```

Configuring connection parameters

1. Go to the **/opt/acronis/vcd-agent/bin** folder and run the **configure.sh** command.

All available configuration scenarios are shown.

```
[root@localhost ~]# /opt/acronis/vcd-agent/configure/configure.sh
-----
Acronis Agent for vCloud configuration:
'1' Configure Agent for vCloud as a new installation
'2' Start migration from existing Acronis Backup Advanced for vCloud

'0' Exit
Action: 1
-----
Acronis Agent for vCloud configuration:
'1' Initial agent configuration
'2' Show agent configuration
'3' Change agent configuration
'4' Show network settings
'5' Change network settings
'0' Back
Action [2]:
```

2. Choose the **Initial agent configuration** scenario.
3. Provide the vCloud Director connection parameters:
 - vCloud Director host name or IP address
 - vCloud Director system administrator credentials
4. Provide the credentials of the RabbitMQ Server user that you created when configuring RabbitMQ Server.
5. Provide the management server connection parameters:
 - Host name or IP address of the management server machine
 - The administrator credentials under which you installed the management server
6. Provide the connection parameters for the SQL Server instance that stores the management server databases:
 - **Host name/IP address:** Host name or IP address of the management server

- **Port [1433]:** The port that was defined when running the configuration script on the management server
 - **User name, Password:** The credentials you entered when running the configuration script on the management server
7. Do the following to enable users to recover files from backups of virtual machines (p. 25):
- At the **Do you want to enable users to recover individual files...** prompt, press **y**.
 - Specify the path to a network folder that will be used as the temporary storage for the recovered files, and the access credentials to that folder.

We recommend that you use a shared folder *on the management server's machine*. Specify the folder in the following format: **//Server/Share/Folder** (note the *forward slashes*). Allow at least 20 GB of space for the temporary files. If necessary, add a separate disk to the management server's machine and create the folder on that disk. If the machine is a member of an Active Directory domain, specify the user name in the **<Domain name>\\<User name>** (note the double backslash) or **<User name>@<Domain name>** format.

Alternatively, you can use an export folder on an NFS server. For example, you can use the machine with Agent for vCloud as the NFS server. To specify the export folder, use the following format: **nfs://Server/ExportPath:/PathInExportFolder** (note the colon before the final slash). For information about how to properly configure the export folder, see the "Configuring an NFS storage" section of the Administrator's Guide.

Configuring network settings

The machine with Agent for vCloud has one network adapter, **ens192**, that does the following:

- Connects to the internal network where Acronis Backup Advanced for vCloud components communicate with VMware vCloud components. It also accepts incoming connections from SSH clients and web browsers in the internal network.
- Accepts incoming connections from web browsers in the external network. Make sure that your firewall, NAT router, and other components of the network security system allow external connection to this adapter through ports 80 and 443.

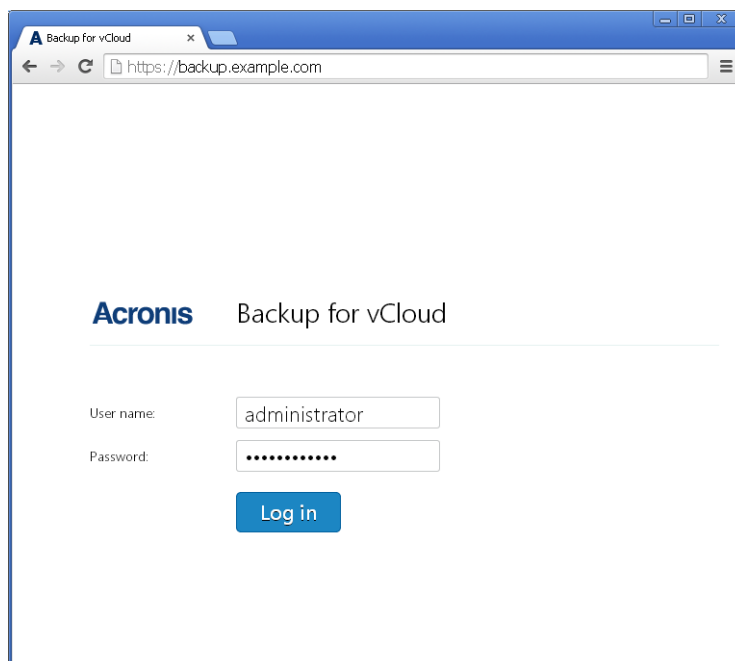
By default, the adapter takes network settings from a DHCP server. You can assign a static IP address to this adapter. For example, to ease port forwarding, you may want to assign a static IP address to the adapter.

To change Agent for vCloud network settings

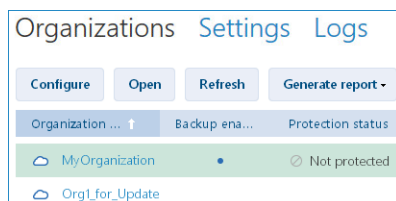
1. Run the **configure.sh** command and choose the **Change network settings** scenario.
2. Specify network settings for the adapter.
 - To take the network settings from a DHCP server, press **y**.
 - To specify the network settings with a static IP address, press **n**, and then:
 - a. Specify the static IP address for the adapter, such as: **10.250.0.10**
 - b. Specify the subnet mask for the adapter, such as: **255.255.0.0**
 - c. Specify the IP address of the default gateway for the adapter, such as: **10.250.0.1**
3. If you configured the adapter to use a static IP address, specify the following:
 - a. In **DNS server 1**, specify the IP address of the DNS server.
 - b. [Optional] In **DNS server 2**, specify the IP address of the secondary DNS server.

5.3 Enabling backup for an organization

1. Go to the login page of the backup service. The address of the login page looks as follows:
https://<BackupServiceAddress>/
 - When connecting from an internal network: <BackupServiceAddress> is the fully qualified domain name, or the IP address of the Agent for vCloud host in this network.
For example, **https://vcloudagent.vcloud.example.com/** or **https://10.200.200.10/**
 - When connecting from an external network: <BackupServiceAddress> is the URL of the backup service as it appears on the public side of a firewall, load balancer, NAT/reverse proxy, and other network components that you may have in front of your infrastructure.
For example: **https://backup.example.com/**
2. Type the user name and password of your vCloud Director system administrator account.
3. Click **Log in**.



4. Click the **Organizations** tab.
A list of organizations registered in vCloud Director is shown.



5. Select the organization to enable backup for.

6. Click **Configure**.

Configure Backup for Organization [X]

MyOrganization

☒ Enable backup for the organization

Backup storage | System backup plans | User privileges

Backup storage: \\backups\myorg

Examples:
nfs://server/opt/export/backups:/org,
\\server\backups\org,
ftp://server/backups/org

User name: admin

Password: ••••••••

☒ Quota: 1 GB

This is a soft quota. Exceeding it does not prevent creating new backups. Only an alert will be shown to you and to all users in the organization.

OK Cancel

7. On the **Backup storage** tab, in **Backup storage**, specify the path to the shared folder allocated for storing organization's backups. If authentication is required to access the folder, specify the credentials of a user account that has read/write permissions for this folder.
8. Confirm the changes.

5.4 Backing up virtual machines

1. Select the organization.

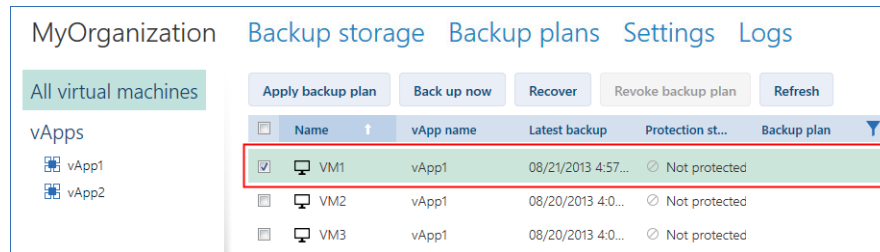
Organizations | Settings | Logs

Configure | Open | Refresh | Generate Report

Organization name	Backup enabled	Protection sta...	Quota
MyOrganization	Yes	None	16 GB

2. Click **Open**.
You are now in the organization administrator's interface.
3. Select one or more virtual machines that you want to back up.

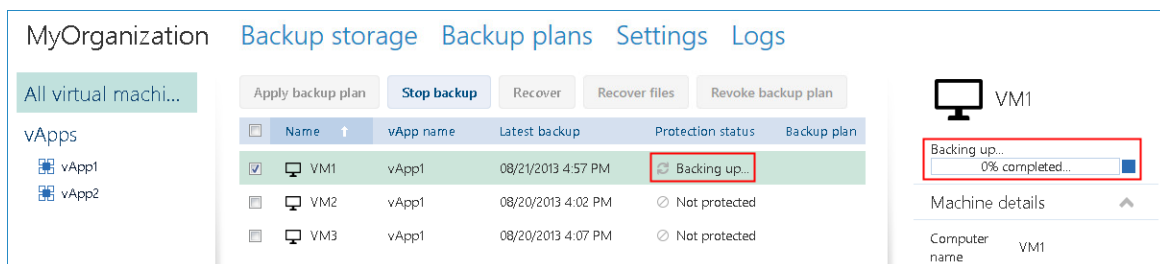
You can select a virtual machine either from the vApp to which the machine belongs, or from the **All virtual machines** list.



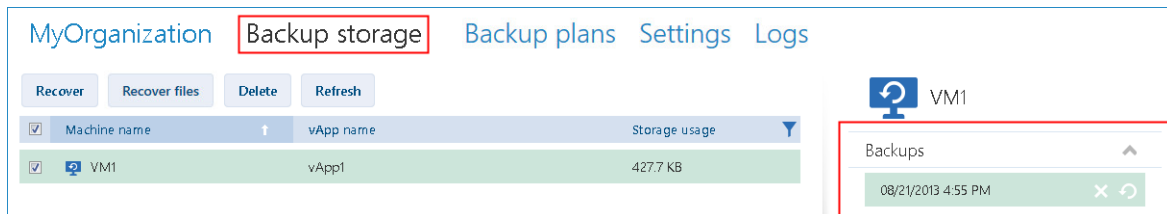
4. Click **Back up now**.

The software can simultaneously back up as many as 10 virtual machines. The default number is 5.

When the backup starts, up to five of the machines will have the **Backing up** protection status. The backup progress for a selected machine is displayed in the machine details area on the right.



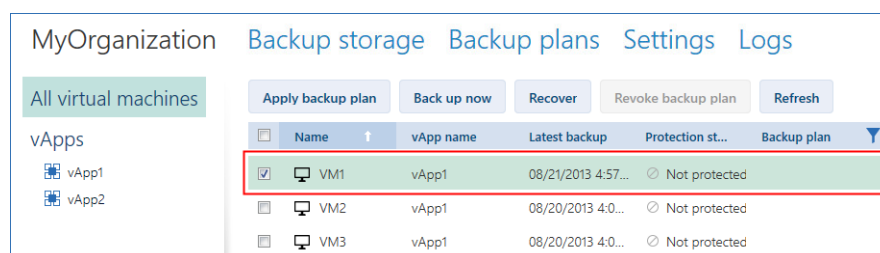
All of the organization's backups are displayed on the **Backup storage** tab.



5.5 Applying a backup plan

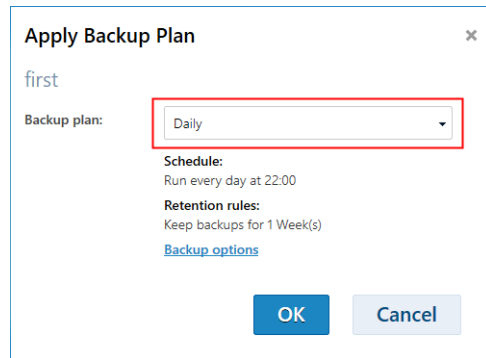
Applying a backup plan to a virtual machine enables you to automate creating and deleting the machine's backups.

1. Select one or more virtual machines in the **All virtual machines** list, or select an entire vApp in the **vApps** list. If you select an entire vApp, the backup plan will be applied to all machines in the vApp and to any new machines that appear in the future.
2. Select one or more virtual machines.



3. Click **Apply backup plan**.
4. Select a backup plan to apply.

Currently, you can select from the backup plans that are initially delivered with the software.



A backup plan contains the following instructions for the backup service:

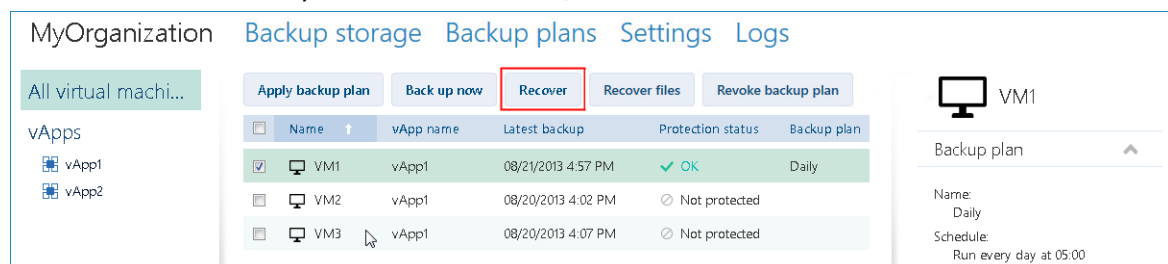
- **Schedule:** When and how often to do backups
- **Retention rules:** How long to store the backups
- **Backup options:** Whether to exclude specific files and folders (**Exclusions**); to send notifications about backup operation results (**Notifications**); and to encrypt backups (**Encryption**)

5. Click **OK**. The name of the applied backup plan appears the **Backup plan** column.

5.6 Overwriting a virtual machine with its backed-up version

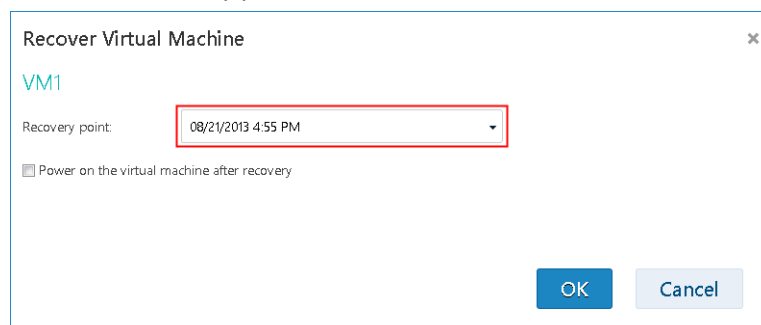
This recovery procedure can be easily run directly from the organization tab.

1. In the organization administrator's interface, click the tab with the organization name.
2. Select the machine that you want to overwrite, and then click **Recover**.



Name	vApp name	Latest backup	Protection status	Backup plan
VM1	vApp1	08/21/2013 4:57 PM	OK	Daily
VM2	vApp1	08/20/2013 4:02 PM	Not protected	
VM3	vApp1	08/20/2013 4:07 PM	Not protected	

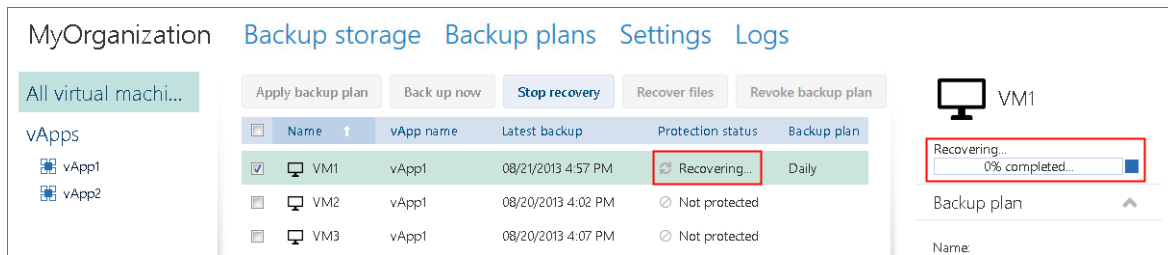
3. In **Recovery point**, select the date and time to which the machine will be recovered. By default, the latest recovery point is selected.



If the vApp no longer has one or more networks that were used by the backed-up machine, you are prompted to map the network adapters of the virtual machine to the networks of the vApp.

4. [Optional] Select the **Power on the virtual machine after recovery** check box.
5. Click **OK**.

When the recovery starts, the machine will have the **Recovering** protection status. The progress of recovery is shown in the machine details area on the right.

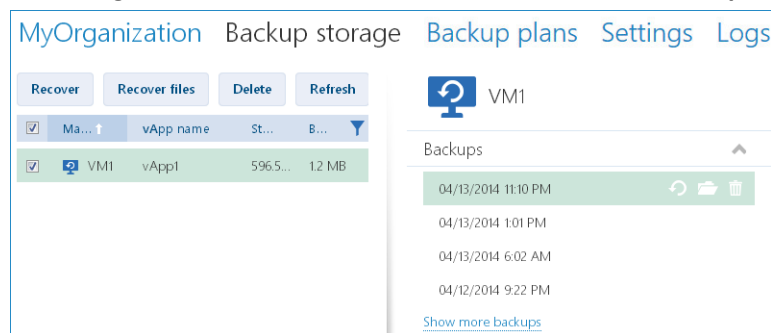


After the recovery is completed, the information about its success or failure is shown in the machine details area.

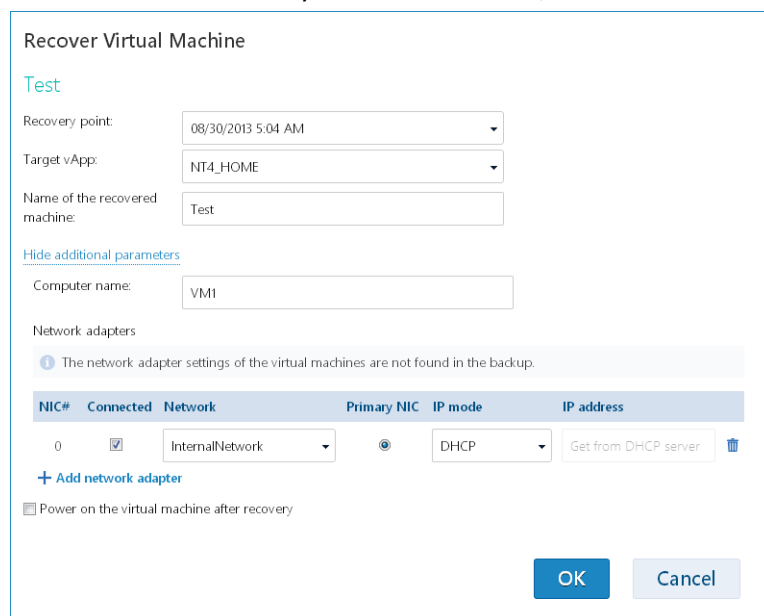
5.7 Recovering a virtual machine

This is a common recovery procedure. Unlike overwriting an existing virtual machine, it enables you to recover a deleted virtual machine, create a new virtual machine by recovering it from a backup, and change the machine's network settings.

1. In the organization administrator's interface, click the **Backup storage** tab.



2. Select the machine that you want to recover, and then click **Recover**.



3. In **Recovery point**, select the date and time to which the machine will be recovered. By default, the latest recovery point is selected.

4. In **Target vApp**, specify the vApp to which the machine will be recovered. By default, the original vApp is selected.

If the original vApp no longer exists in the organization, you can recreate the original vApp and recover the machine to it. To do so, select **Recreate original vApp**. The vApp will be created with parameters that it had when the machine was backed up.

5. In **Name of the recovered machine**, type a name that the recovered machine will have in the vApp. By default, the original machine's name is selected.

If a machine with the same name exists in this vApp, the software examines the machine's unique identifier in vCloud Director. A machine with the same unique identifier will be overwritten. If the machine has a different unique identifier, the software creates a new virtual machine and adds a suffix like **(1)** to its name.

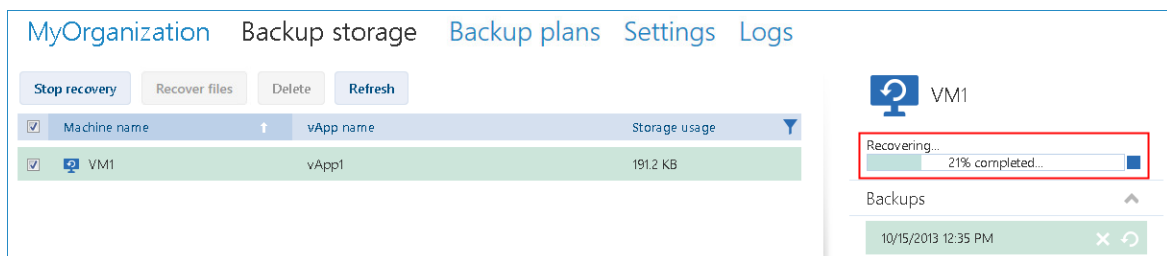
6. Under **Show additional parameters**, you can do any of the following:

- In **Computer name**, change or specify the name that the machine will have on the network.
- In **Network adapters**, change or specify the settings for the machine's network adapters, or add or delete network adapters.
- In **Preserve MAC addresses**, specify whether the machine's network adapters (except the newly added ones) will have the same MAC addresses as those of the original machine.

7. [Optional] Select the **Power on the virtual machine after recovery** check box.

8. Click **OK**.

The progress of recovery is shown in the machine details area on the right.



After the recovery is completed, the information about its success or failure is shown in the machine details area.

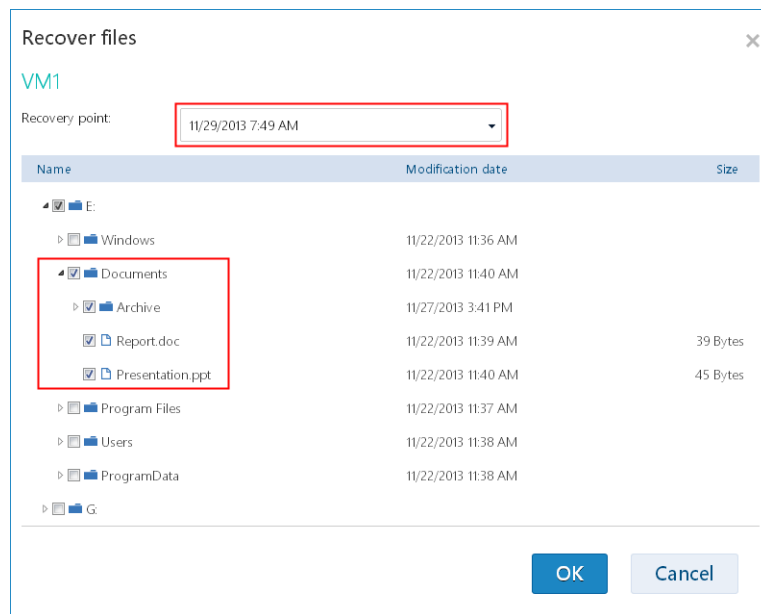
5.8 Recovering files from a virtual machine backup

This procedure enables you to recover files and folders from a backup of a virtual machine without recovering the virtual machine itself. The files and folders that you select will be available for download as a .zip file.

To recover files of a virtual machine

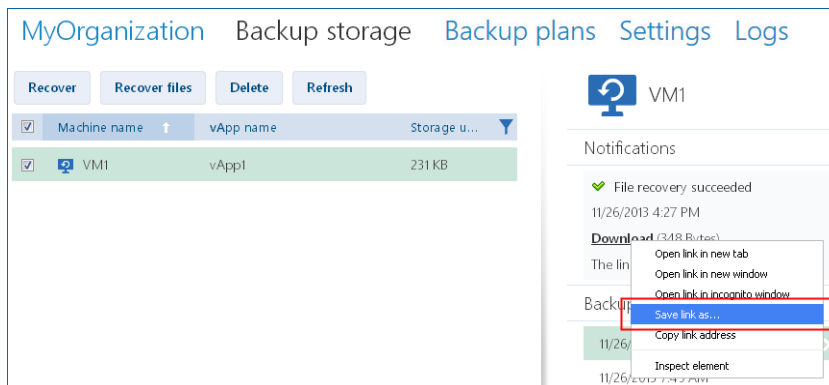
1. Open the organization tab or the **Backup storage** tab.
2. Select the virtual machine whose files you want to recover, and then click **Recover files**.
3. In **Recovery point**, select the date and time that you want to recover the files to.

The service shows the volumes, files, and folders that were present on the machine at that time. Volumes that you cannot recover files from are not shown.



Select the files and folders that you want to recover, and then click **OK**.

After the recovery is completed, the link to download the .zip file appears on the **Backup storage** tab in the machine details area on the right.



The link is valid for 24 hours. You can use the link only when you are logged in to the service.

The files are stored in the .zip file together with their entire folder structure. For example, the file **C:\Documents\Report.doc** will be stored in the .zip file in the **Drive(C)\Documents** folder.