Acronis

Backup Service for vCloud

Update 7

USER'S GUIDE

Table of contents

1 User's Guide

1.1 About the backup service

This service enables backup and recovery of virtual machines managed by VMware vCloud Director.

The service is available through a web interface. To log in to the backup service, use your vCloud Director credentials.

What you can do after logging in depends on the settings made by a system administrator for your organization. Due to these settings, some of the operations described in this guide may be not available to you.

1.2 Supported web browsers

- Google Chrome 12 or later
- Mozilla Firefox 12 or later
- Windows Internet Explorer 9 or later
- Safari 5 or later running in the Mac OS X and iOS operating systems

In other web browsers (including Safari browsers running in other operating systems), the user interface might be displayed incorrectly, or all functions might not be available.

Make sure that JavaScript is enabled in the browser.

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

1.3 Installing VMware Tools

We recommend installing VMware Tools on all virtual machines which you are planning to back up in the powered-on state.

Installing VMware Tools is a common requirement for backing up at a hypervisor level. The backup service uses VMware Tools to create a time-consistent backup of the machine. All data will be backed up as it was at the moment when the backup started, even if the data changes while the backup is running.

To install VMware Tools on a virtual machine

1. Log in to vCloud Director.
2. In the list of virtual machines, examine the **VMware Tools** column for the virtual machine. This column is hidden by default.
3. If this column shows **Not installed**, install the most recent version as follows:
   a. Power on the machine.
   b. Right-click the machine and then click **Install VMware Tools**.
   c. Follow the on-screen instructions.

For information about installing VMware Tools in a specific operating system, refer to the following VMware knowledge base article: http://pubs.vmware.com/vcd-51/topic/com.vmware.vcloud.users.doc_51/GUID-F0826E73-7F9F-489C-B0DB-17C7D742B1AF.html.

1.4 Basic operations

This section describes typical usage of the backup service.

1.4.1 Logging in to the service

You can log in to the backup service under the following conditions:

- A system administrator has enabled use of the service for your organization.
- [For non-administrative users] Your organization administrator has enabled use of the service for your account.

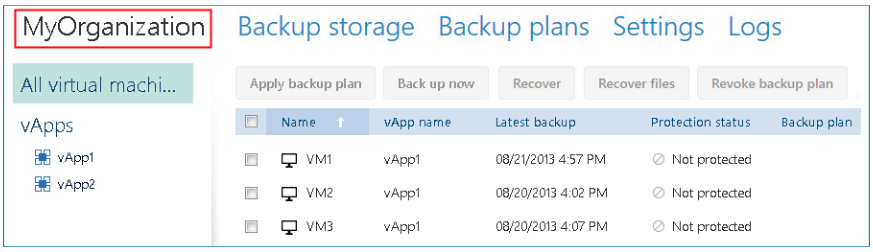
To log in to the backup service

1. Go to the login page of the backup service. The URL of the login page looks like:
   `https://backup.example.com/org/<Organization name>`

   If you are unsure about the address of the login page, contact the system administrator or the organization administrator.
2. Type the user name and password of your vCloud Director account.
3. Click **Log in**.

1.4.2 Backing up virtual machines

The virtual machines that you can back up are listed on the organization tab.

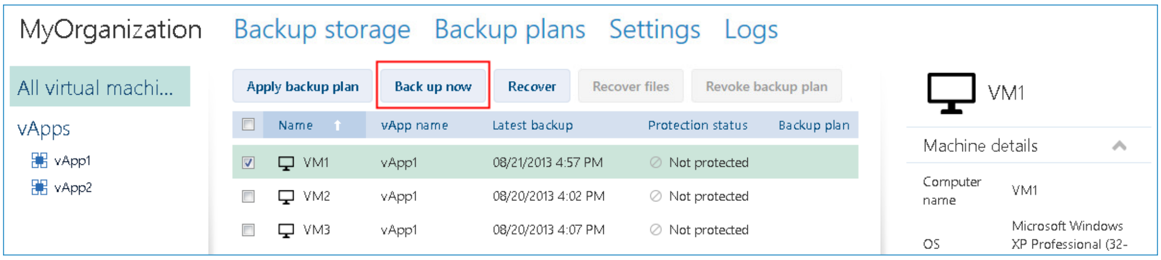


☐	Name	vApp name	Latest backup	Protection status	Backup plan
☐	VM1	vApp1	08/21/2013 4:57 PM	Not protected	
☐	VM2	vApp1	08/20/2013 4:02 PM	Not protected	
☐	VM3	vApp1	08/20/2013 4:07 PM	Not protected	

The **vApps** list shows all vApps that you own. The **All virtual machines** list shows all virtual machines from those vApps. (An organization administrator sees all vApps and virtual machines in the organization.)

Starting a backup

Select one or more virtual machines that you want to back up, and then click **Back up now**.



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

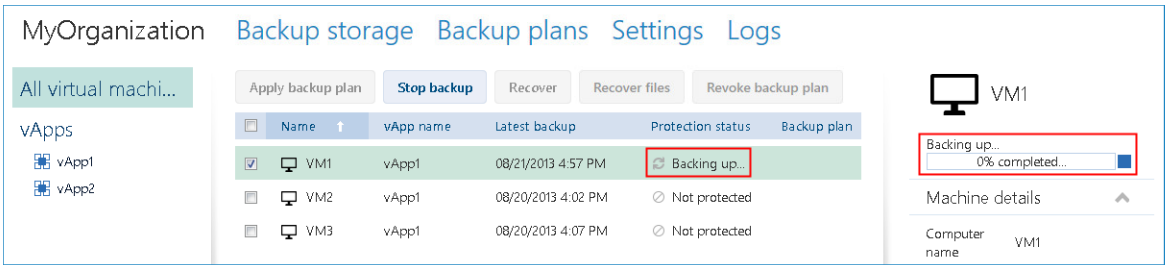
Computer name	VM1
OS	Microsoft Windows XP Professional (32-

If you want backups to run on a schedule, apply a backup plan (p. 5) instead.

Monitoring a backup

A backup may start with a delay, depending on the backup service load.

When the backup starts, you can see its progress in the machine details area on the right.



☐	Name	vApp name	Latest backup	Protection status	Backup plan
☑	VM1	vApp1	08/21/2013 4:57 PM	Backing up...	
☐	VM2	vApp1	08/20/2013 4:02 PM	Not protected	
☐	VM3	vApp1	08/20/2013 4:07 PM	Not protected	

Backing up...
0% completed...

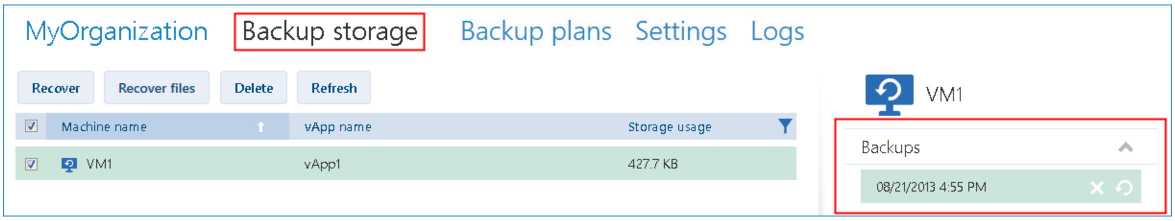
Computer name VM1

The number of machines that are backed up simultaneously and the order in which they are backed up are defined by the backup service.

If you need to stop the backup on a specific machine, select the machine, and then click **Stop backup** or click the stop button (■) near the progress bar.

Viewing the result

Once a virtual machine is successfully backed up, the newly created backup appears in the **Backups** column on the **Backup storage** tab.



☑	Machine name	vApp name	Storage usage
☑	VM1	vApp1	427.7 KB

08/21/2013 4:55 PM

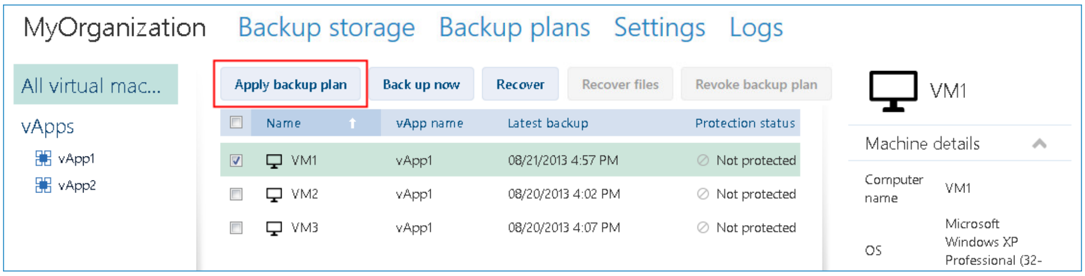
1.4.3 Applying a backup plan

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

Depending on how the backup service is configured, you may be able to create your own backup plans, apply backup plans shared by the system administrator, or both.

To apply a backup plan to virtual machines

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. Click **Apply backup plan**.

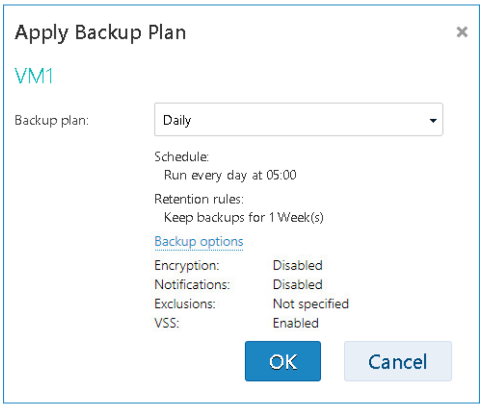


☐	Name	vApp name	Latest backup	Protection status
☑	VM1	vApp1	08/21/2013 4:57 PM	Not protected
☐	VM2	vApp1	08/20/2013 4:02 PM	Not protected
☐	VM3	vApp1	08/20/2013 4:07 PM	Not protected

Computer name VM1

OS Microsoft Windows XP Professional (32-

3. Select the backup plan that you want to apply to the machines. For example, select **Daily**.



Apply Backup Plan

VM1

Backup plan: Daily

Schedule:
Run every day at 05:00

Retention rules:
Keep backups for 1 Week(s)

Backup options

Encryption: Disabled
Notifications: Disabled
Exclusions: Not specified
VSS: Enabled

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** (p. 14).

4. Click **OK**.

The name of the applied backup plan appears in the **Backup plan** column. If another backup plan was previously applied to the machine, that backup plan is revoked.

Tips on usage

- The **Protection status** column shows whether the latest backup has completed successfully (**OK**) or failed (**Error**).
- Should you need to restart a failed backup, select a machine and click **Back up now**. The machine will be backed up according to the backup plan settings. However, the retention rules will not be applied this time.
- Change a backup plan to one with a different **Encryption** setting (including different password) only if it is really necessary. This operation is allowed, but it may cause some inconveniences. For details, refer to "Consequences of changing encryption" in "Editing a backup plan" (p. 16).

1.4.4 Overwriting a virtual machine with its backed-up version

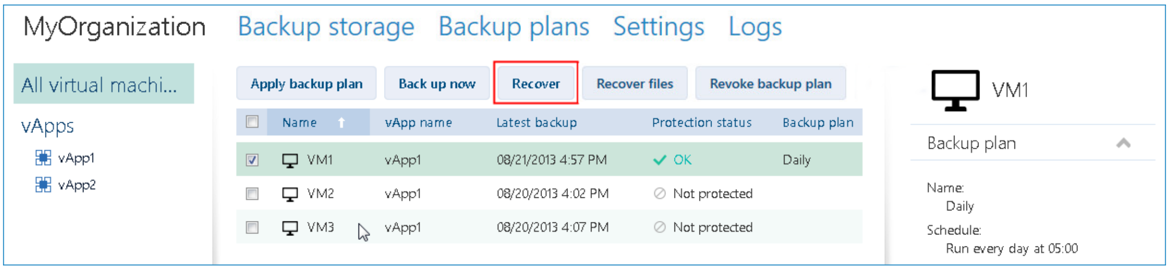
This recovery procedure can be easily run directly from the organization tab.

Overwriting a machine means that only the content of its original disks is overwritten. The content of hard disks that were added after the backup will remain the same. The machine settings, such as CPU and memory settings, and the MAC addresses (also known as physical addresses) of the network adapters are also preserved.

A machine that was renamed or moved to a different vApp is considered a new machine. To overwrite it, you need a backup that was created after renaming or moving the machine. If you need to use an older backup, proceed as described in "Recovering a virtual machine" (p. 7).

Setting up the recovery

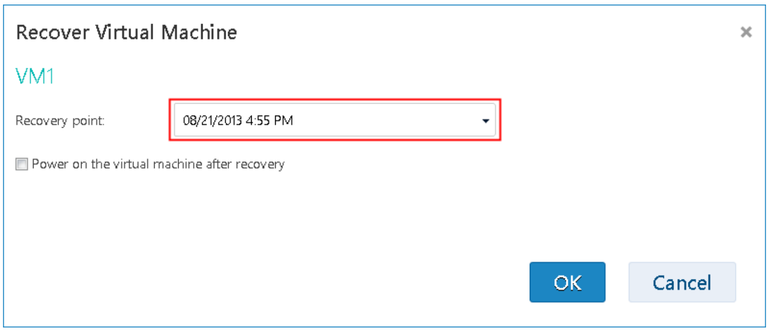
1. On the organization tab, select the machine that you want to recover, and then click **Recover**.



☐	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	

Name:
Daily
Schedule:
Run every day at 05:00

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



Recovery point: 08/21/2013 4:55 PM

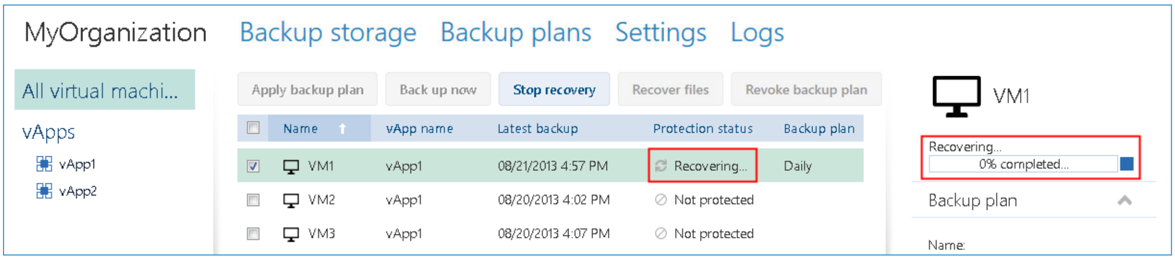
☐ Power on the virtual machine after recovery

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.

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

Monitoring the recovery progress

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.



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

Recovering...
0% completed... ■

Name:

If you need to stop the recovery, click the **Stop recovery** button or the stop button (■) near the progress bar. The original machine will likely become corrupted.

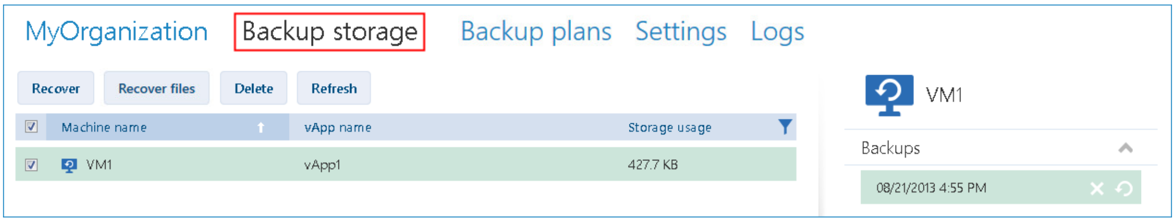
After the recovery is completed, the information about its success or failure is shown in the machine details area.

1.4.5 Recovering a virtual machine

This is a common recovery procedure. Unlike overwriting an existing virtual machine, this 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.

Setting up the recovery

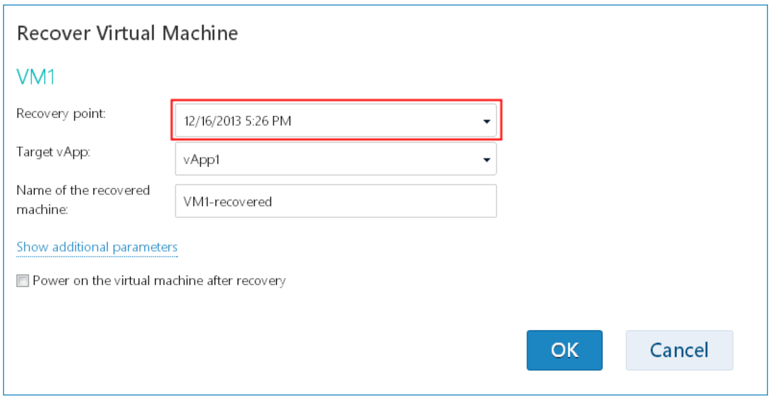
1. Open the **Backup storage** tab.



☑	Machine name	vApp name	Storage usage
☑	VM1	vApp1	427.7 KB

08/21/2013 4:55 PM

2. In the list of backed-up machines, select the machine that you want to recover, and then click **Recover**.



Recovery point: 12/16/2013 5:26 PM

Target vApp: vApp1

Name of the recovered machine: VM1-recovered

□ Power on the virtual machine after recovery

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

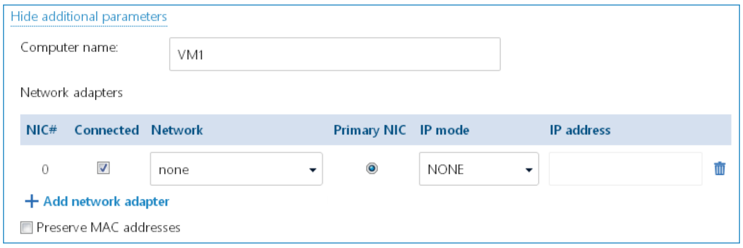
4. In **Target vApp**, specify the vApp to which the machine will be recovered. By default, the original vApp is selected.

   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:



Computer name: VM1

Network adapters

NIC#	Connected	Network	Primary NIC	IP mode	IP address
0	☑	none	●	NONE	

□ Preserve MAC addresses

- In **Computer name**, change or specify the name that the machine will have on the network. This is the name defined in the guest operating system (**Control Panel** > **System** > **System Properties** > **Computer Name**).
- Under **Network adapters**, change or specify the settings for the existing adapters, or add or delete network adapters.

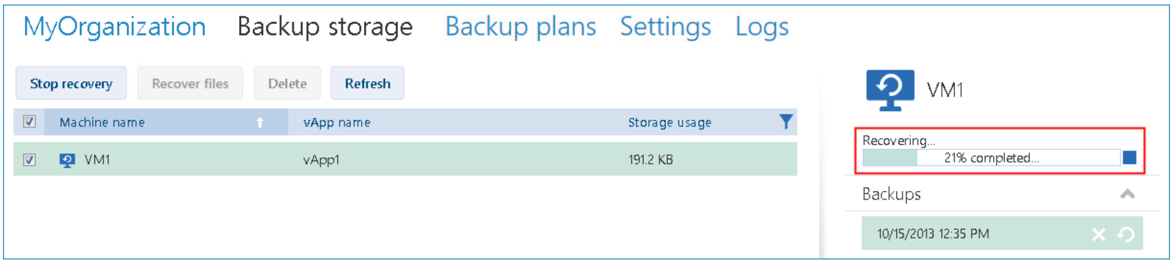
  Details. To add a network adapter, click **Add network adapter**, and then specify the settings for it. To delete a network adapter, click the **Delete** (🗑) button next to it.

- 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. To prevent a MAC address conflict, avoid selecting this check box if the original machine exists and will not be overwritten.

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

Monitoring the recovery progress

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



☑	Machine name	vApp name	Storage usage
☑	VM1	vApp1	191.2 KB

Recovering...
21% completed...

10/15/2013 12:35 PM

If you need to stop the recovery, click the **Stop recovery** button or the stop button (■) near the progress bar.

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

1.4.6 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.

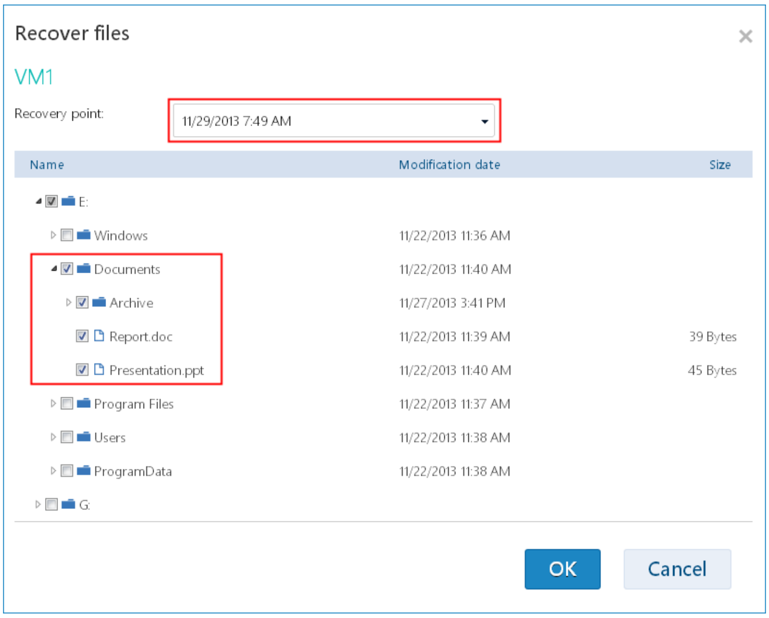
The files and folders that you select will be available for download as a .zip file.

You can recover files from volumes with the following file systems: FAT, FAT32, NTFS, Ext2, Ext3, and Ext4. Regardless of the file system, you cannot recover files from volumes that are managed by Linux Logical Volume Manager (LVM), also known as logical volumes; and from multiple-disk (MD) devices, also known as Linux Software RAID.

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.



Recover files

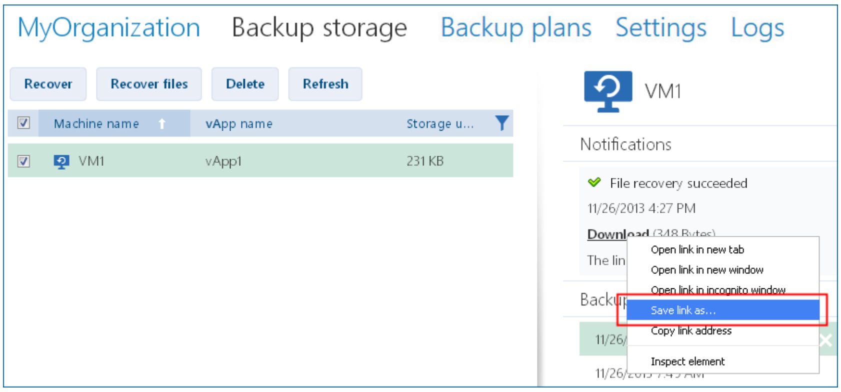
VM1

Recovery point: 11/29/2013 7:49 AM

Name	Modification date	Size
☑ E:		
□ Windows	11/22/2013 11:36 AM	
☑ Documents	11/22/2013 11:40 AM	
☑ Archive	11/27/2013 3:41 PM	
☑ Report.doc	11/22/2013 11:39 AM	39 Bytes
☑ Presentation.ppt	11/22/2013 11:40 AM	45 Bytes
□ Program Files	11/22/2013 11:37 AM	
□ Users	11/22/2013 11:38 AM	
□ ProgramData	11/22/2013 11:38 AM	
□ G:		

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.



☑	Machine name	vApp name	Storage u...
☑	VM1	vApp1	231 KB

VM1

Notifications

✓ File recovery succeeded

11/26/2013 4:27 PM

Download (348 Bytes)

The lin

Backu

11/26/

11/26/2013 7:49 AM

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.

Recovering files to the original machine

To recover the files directly to the original virtual machine, use any of the following methods:

- **Extract the files to a system network share.** After you download the .zip file to your machine, power on the original virtual machine and extract the file to a network share such as **\\VM1\c$** (this network share corresponds to the C volume of the **VM1** virtual machine). This method of recovery works only for a virtual machine running Windows. You must provide the credentials of a local administrator on that virtual machine.
- **Log in to the service on the virtual machine.** Power on the virtual machine, start the browser, log in to the service, and then download the .zip file and extract the files from it.

1.4.7 Monitoring protection statuses

The **Protection status** column on the organization tab indicates how well a virtual machine or a vApp is protected.

Protection statuses of machines

The table below lists protection statuses of a machine by order of *severity*, from the least severe to the most severe.

Status	Meaning
Not protected	No backup plan is applied to the machine.
Never backed up	A backup plan is applied to the machine, but no backup has been run.
OK	A backup plan is applied to the machine and the latest backup was completed successfully.
Error	A backup plan is applied to the machine, and the latest backup failed.

Instead of these statuses, the **Backing up...** or **Recovering...** status is shown when a backup operation or a recovery operation is running.

***Note** The "Back up now" operation does not affect a protection status unless a backup plan is applied to the machine.*

Protection statuses of vApps

The protection status of a vApp is the *most severe* status among the machines in the vApp. This status does not depend on whether a machine is currently being backed up or recovered.

1.5 Operations with backups

The **Backup storage** tab shows the list of backed-up virtual machines. Each of the machines has one or more backups, also called recovery points. The backups are listed in the **Backups** area on the right.

Once you select a backup, the **Machine details** area shows the computer name, the guest operating system, and the IP addresses for the machine *at the time of backup*.

The following operations with backups are available:

- **To recover a machine from a backup**, select the machine and click **Recover**. Refer to "Recovering a virtual machine" (p. 7).
- **To delete one or more backups of a machine**, select the machine and click **Delete**. In the opened window, select the backups that you want to delete and click **Delete**.
- **To delete all backups of two or more machines**, select the machines and click **Delete**.

Storage usage/Backed-up data

This area contains information related to either the storage usage or the backed-up data, depending on the backup service quota settings.

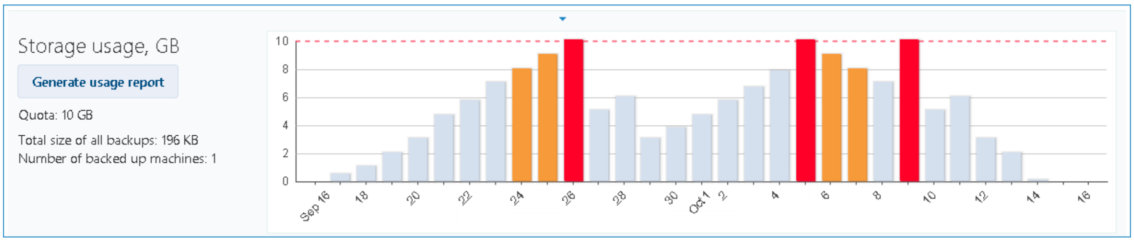
This area is available only to administrators. It contains the following parameters:

- The storage quota for the organization (if set by the system administrator).
- The total size of backups stored in the backup storage or the total amount of data that was backed up.

- The number of backed-up virtual machines.
- The alerts about an almost-reached quota (80 percent or more is used) or an exceeded quota (100 percent or more is used).

To see historical data on the storage usage, expand the area.

- The column chart represents the service usage for the last 30 days. In the chart, red columns show days when the storage quota was exceeded and orange columns show days when the storage quota was almost reached.


Storage usage, GB

Generate usage report

Quota: 10 GB

Total size of all backups: 196 KB

Number of backed up machines: 1

- To generate a comprehensive report on the service usage for a specific period, click **Generate usage report** (p. 17).

1.6 Operations with backup plans

The **Backup plans** tab shows the backup plans that you can apply to your virtual machines.

The following backup plans are shown:

- **System backup plans** (). System backup plans are shared with your organization by the system administrator. Their schedule and retention rules can be changed only by using the system administrator's interface. However, you can enable backup options for these plans, such as encryption or notifications. To do so, click **Set options**. These options will be effective only within your organization.
- **Backup plans created within the organization** (). If you are an organization administrator, you can perform any operations with these backup plans. Non-administrative users can perform any operations with the backup plans they created. The **Owner** column shows who created the backup plan. The owner of backup plans created by a system administrator is **System**.

1.6.1 Creating a backup plan

In addition to using existing backup plans, you can create your own backup plans.

To create a backup plan

1. Open the **Backup plans** tab.
2. Click **Create**.
3. Type the name of the backup plan. The name must differ from names of other backup plans in the list of backup plans.
4. Specify the schedule type: **Daily**, **Weekly**, **GFS (Grandfather-Father-Son)**, or **Hourly**.
5. On the **Schedule** and **Retention rules** tabs, specify the schedule and retention rules (p. 13) for the backup plan.
6. On the **Options** tab, specify the backup options (p. 14).
7. Click **OK**.

After creating the backup plan, you can apply it to your virtual machines (p. 5).

1.6.1.1 Schedule and retention rules

The backup operation runs according to the schedule you specify. The resulting backups are kept according to the retention rules and then deleted.

The scheduled time is displayed according to the time zone set on the machine from which you are logged in to the backup service. If you schedule backups to run, say, at 07:00, they will run when your machine clock reaches 07:00, regardless of the time zone where the vCloud infrastructure is physically located. If you change the time zone setting on the machine, the schedule will not change, but you will see different start time.

The following schedule types and the corresponding retention rules are available:

Hourly backup

Schedule. Select the days of week to run backups and the time interval between the backups. In **From** and **To**, specify the beginning and the end of the period when the backups will be run.

Retention rules. Specify how long you want to retain the backups.

By default, backups will run every four hours on workdays. The backups are retained for one week.

Daily backup

Schedule. Select the days of week and the time to run backups.

Retention rules. Specify how long you want to retain the backups.

By default, the backups will run Monday through Friday at 22:00. The resulting backups will be retained for one week.

Weekly backup

With this schedule, the backups will run once in the specified number of weeks.

Schedule

1. Select the number of weeks.
2. Select the day of week and the time to run backups.

By default, the backups will run every week at 22:00, on the day of week on which the backup plan was created.

Retention rules

Specify how long you want to retain the backups.

By default, the backups will be retained for four weeks.

GFS (Grandfather-Father-Son)

This schedule is useful for long-term storage of backups.

With this schedule, you have a single backup for each of the recent days and for each of the recent weeks. For earlier periods of time, you have a single backup for each month.

Schedule

1. Select the days of week and the time when to run backups.

2. Out of these days of week, choose the one to **Do weekly/monthly backups on**. Backups that are performed on that day will be considered as *weekly backups* and *monthly backups*. Backups that are performed on other days will be considered as *daily backups*.

By default, the backups will run Monday through Friday at 22:00. Friday is chosen for Weekly/Monthly backups.

Retention rules

Specify how long you want to retain the daily, weekly, and monthly backups.

The default settings are the following:

- Daily backups: 5 days (recommended minimum)
- Weekly backups: 7 weeks
- Monthly backups: 12 months

Example

Suppose that you use the default settings (run backups Monday through Friday, Weekly/Monthly backups on Friday, the default retention rules) and apply the backup plan on Monday, March 1.

The following table shows which daily (D), weekly (W), and monthly (M) backups will remain on Friday, April 30. Backups that are shown on the gray background will be deleted by that day.

	Mon	Tue	Wed	Thu	Fri	Sat	Sun
March 1–7	*D*	*D*	*D*	*D*	*W*	–	–
March 8–14	*D*	*D*	*D*	*D*	W	–	–
March 15–21	*D*	*D*	*D*	*D*	W	–	–
March 22–28	*D*	*D*	*D*	*D*	M	–	–
March 29–April 4	*D*	*D*	*D*	*D*	W	–	–
April 5–11	*D*	*D*	*D*	*D*	W	–	–
April 12–18	*D*	*D*	*D*	*D*	W	–	–
April 19–25	*D*	*D*	*D*	*D*	W	–	–
April 26–May 2	D	D	D	D	M	–	–

1.6.1.2 Backup options

On the **Options** tab, configure the parameters of the backup operation.

Encryption

Specify the password to be used for encrypting the backups. The password prompt will appear when someone tries to delete a backup or recover data from it.

The backups will be encrypted with the AES-256 encryption algorithm.

The password is not stored anywhere on the disk or in the backup file. Make sure you remember the password. Recovering a lost password is not possible.

If you edit the backup plan (p. 16) and change or remove the password, the retention rules will no longer apply to the backups with the old encryption setting. Also, separate entries will be shown in the backup storage for sets of backups with different encryption settings. During recovery, you will need to select the correct entry and type the correct password.

Notifications

Specify whether to send e-mail notifications after a successful backup, after a failed backup, or both.

Specify the address to send the notifications. Separate multiple e-mail addresses with a semicolon. For example: **user1@example.com; user2@example.com**

The notifications will be sent from the e-mail address specified by a system administrator.

Exclusions

Type one or more criteria. Files and folders that match any of the specified criteria will not be backed up.

This option is effective only for files and folders that are stored on the following file systems:

- FAT
- NTFS
- Ext3
- Ext4

Regardless of the file system, this option is not effective for volumes that are managed by Linux Logical Volume Manager (LVM), also known as logical volumes; and for multiple-disk (MD) devices, also known as Linux Software RAID.

How to specify criteria

You can use the following criteria:

- **The full path to a file or folder**, starting with the drive letter (when backing up Windows) or the root directory (when backing up Linux).

  Both in Windows and Linux, you can use a forward slash in the file or folder path (for example: **C:/Temp** and **C:/Temp/File.tmp**). In Windows, you can also use the traditional backslash (for example: **C:\Temp** and **C:\Temp\File.tmp**).
- **The name of a file or folder**; for example: **Document.txt**. All files and folders with that name will be excluded.

Separate multiple criteria with a semicolon (;).

The criteria are *not* case-sensitive. For example, if you choose to exclude all **.tmp** files and the **C:\Temp** folder, also excluded will be all .Tmp files, all .TMP files, and the C:\TEMP folder.

Wildcard characters

You can use one or more wildcard characters * and ? in a criterion. These characters can be used within the full path and in the file or folder name.

The asterisk (*) substitutes for zero or more characters in a file name. For example, the criterion **Doc*.txt** covers files such as Doc.txt and Document.txt.

The question mark (?) substitutes for exactly one character in a file name. For example, the criterion **Doc?.txt** covers files such as Doc1.txt and Docs.txt, but not the files Doc.txt or Doc11.txt.

VSS

Specify whether to use Volume Shadow Copy Service (VSS) during backup.

This option is effective only for machines where VMware Tools is installed (p. 3).

This option ensures that the file system will be backed up in a consistent state. For machines running Windows, this option also ensures the consistent state of all data that is used by VSS-aware applications, such as by Microsoft SQL Server.

Without this option, the backup process is faster, but data consistency cannot be guaranteed.

1.6.2 Editing a backup plan

***Important:** The changes you make to a backup plan affect all virtual machines to which the backup plan is applied, both your machines and other users' machines.*

To edit a backup plan

1. Open the **Backup plans** tab.
2. Select the backup plan that you want to edit, and then click **Edit**.
3. View or change the name, schedule, retention rules (p. 13), and backup options (p. 14).
4. Click **OK**.

Consequences of changing encryption

If you need to change the **Encryption** setting (to enable or disable encryption or to change the password), consider the following:

- **Retention rules will no longer apply** to the backups with the old encryption setting. You can only delete those backups manually (p. 16).
- **Separate entries will be shown** in the backup storage for sets of backups with different encryption settings. During recovery, you will need to select the correct entry and type the correct password.

The same happens when you apply a backup plan to a machine where another backup plan with a different **Encryption** setting is applied.

1.6.3 Revoking a backup plan

When you revoke a backup plan from a machine, a currently running backup (if any) is stopped. The machine will no longer be backed up until a backup plan is applied again. Backups of the machine are retained in the backup storage until you delete them manually (p. 11).

To revoke a backup plan

1. Open the tab with the organization name.
2. Select one or more machines from which you want to revoke backup plans.
3. Click **Revoke backup plan**.

1.6.4 Deleting a backup plan

When you delete a backup plan, it is revoked (p. 16) from all machines to which it is applied (both your machines and other users' machines) and it is removed from the list of backup plans.

To delete a backup plan

1. Open the **Backup plans** tab.
2. Select the backup plan that you want to delete, and then click **Delete**.
3. Confirm the deletion of the backup plan.

1.7 Generating usage reports

This functionality is available only to administrators.

Usage reports provide historical data about using the backup service in your organization. You may need these reports to calculate how much your organization will be charged for the service.

Reporting parameters

The values of all parameters are checked every day at 23:55 according to the time settings of vCloud Director. The report uses the values as they were at that time.

The report includes the following parameters for the organization:

- **Number of protected VMs**: The total number of protected machines (that is, the machines to which backup plans are applied), no matter whether backups of those machines exist
- **Storage usage**: The total size of all backups in the backup storage (in gigabytes). This parameter may be excluded from the report, depending on the backup service settings.
- **Backed-up data**: The total amount of data that was backed up. This amount includes the initial content of the virtual machine disks and the subsequent incremental changes to that content.
- **Over quota**: The amount of data that exceeds the quota set for the organization (in gigabytes)
- **Disk size of protected VMs**: The total size of hard disks of the protected machines (in gigabytes), regardless of the occupied space on those disks
- **RAM size of protected VMs**: The total amount of memory of the protected machines (in gigabytes)
- **CPU number of protected VMs**: The total number of CPUs of the protected machines

To generate a usage report

1. Open the **Backup storage** tab.
2. Expand the **Storage usage** area on the bottom, and then click **Generate usage report**.
3. In **Period**, select the reporting period:
   - **Current calendar month**: The report will include data from the first day of the current month up to the current day (when generating the report after 23:55) or up to the previous day (when generating the report before 23:55).
   - **Previous calendar month**: The report will include data from all days of the previous month. For example, in April you will get a report for the time interval from March 1 through March 31.
   - **Custom period**: The report will include data from the interval that you specify.
4. In **Type**, select the report type:
   - **Daily statistics**: The report will include the values of the reporting parameters for each day of the reporting period. The report also includes the *summary*: the minimum, maximum, and average values of each of the reporting parameters throughout the period.
   - **Summary report**: The report will include only the summary (see the previous option).
5. Click **OK**. The report appears in a separate browser window or tab.

6. [Optional] To print the report, click **Print**. To save the report as a comma-separated values (.csv) file, click **Save as .csv file**.

1.8 Enabling non-administrators to use the service

Using the backup service includes logging in to it, performing backup and recovery, and managing backups and backup plans. A system administrator may want to create a dedicated vCloud Director role for the backup service access.

Organization administrators can enable members of any vCloud Director role to use the service.

To enable members of a vCloud Director role to use the service

1. Log in to the backup service.
2. Click the **Settings** tab.

   The software displays a list of vCloud Director roles.
3. Select the **Service enabled** check box for the role.

Any member of this role will be able to use the backup service. If you need advice on how to assign a vCloud Director role to a user, read the next section.

1.8.1 Assigning a vCloud Director role to a user

The following procedure is effective for both of the following types of users:

- **Local users:** Users whose accounts were created in vCloud Director
- **LDAP users:** Users whose accounts were imported to vCloud Director from a Lightweight Directory Access Protocol (LDAP) directory, such as Active Directory

To assign a role to a user

1. Log in to vCloud Director.
2. Click **Administration** > **Users**.
3. Assign the role with the backup service access to the user.

The user can start using the service as soon as you have assigned the role.

Alternative method for LDAP users

If your organization has a large number of non-administrative LDAP users, you may want to follow a different procedure to enable them to use the service.

To assign a role to an LDAP group

1. Log on to the LDAP server (such as an Active Directory domain controller), from which user accounts are imported into vCloud Director.
2. Create a group in the LDAP directory (for example: **vCloud Backup Service Users**).
3. Add all users whom you want to access the service to the group created in step 2.

   You can now log out from the LDAP server.
4. Log in to vCloud Director.
5. On the **Groups** page, find the group that you created in step 2.
6. Assign the role with the backup service access to the group.

By adding or removing group members on the LDAP server, you can change who can use the service.

1.9 Viewing audit logs

The backup service includes an audit log, which records operations performed by users.

System and organization administrators have a view into the log scoped to their area of control.

To view the audit log

1. Log in to the service.
2. Click the **Logs** tab.

2 Terminology reference

Agent for vCloud

The backup service infrastructure component that runs on a dedicated virtual machine within a vCloud Director management cluster.

Backup (operation)

An operation that saves information about a virtual machine in a packaged form, for the purpose of recovery.

Backup (recovery point)

The result of a single backup operation.

A backup represents a point in time to which a user can recover the virtual machine. The data that is necessary for recovery is stored in two locations. The content of the virtual disks and the virtual machine configuration are stored in the backup storage. The metadata that reflects the machine's membership in vCloud (the virtual network adapters configuration, the computer name, the vApp the machine is part of) is stored inside Agent for vCloud.

Backup plan

A set of rules that define how to protect virtual machines.

The rules include the backup schedule, retention rules and backup options such as protecting backups with a password. For example: perform backup every day at midnight, delete backups that are older than one month, and protect the backups with a password.

Backup plan owner

An organization user who created the backup plan.

The system backup plans have a special owner called **System**. The owner is also **System** for backup plans created by the system administrator within the organization.

Backup storage

A folder allocated by a system administrator for storing an organization's backups.

Management cluster

An ESX(i) cluster that contains the vCloud Director infrastructure components.

Organization administrator

A user who has the Organization Administrator role in vCloud Director.

An organization administrator can back up and recover any virtual machine in the organization.

Protected machine

A virtual machine to which a backup plan is applied.

Recovery

An operation that creates or overwrites a virtual machine by using the data that was earlier saved in a backup. When you select for recovery the same machine that was backed up, it is overwritten. Otherwise, a new virtual machine is created.

Resource group

One or more ESX(i) clusters that contain virtual machines of vCloud Director organizations.

Retention rules

A part of backup plan that specifies how long backups are kept.

Storage quota (quota)

The amount of storage space allocated for an organization.

If the quota is exceeded, the system administrator and the organization users see alerts in the backup service interface. Restrictions on using the backup service are not applied unless the system administrator does this manually.

System administrator

A user who has the System Administrator role in vCloud Director.

A system administrator can back up and recover any virtual machine in any organization. A system administrator can allow organization users to back up virtual machines in their organization.

System backup plan

A ready-to-use backup plan predefined by the system administrator in order to make it available across many organizations. Organization users can apply system backup plans to their virtual machines.

Changes to the schedule or retention rules of a system backup plan affect all organizations to which the plan was made available.

User

A person who has a user account in vCloud Director.

Depending on the permissions that are assigned to the user account in vCloud Director, a user can be a system administrator, an organization administrator, or a non-administrative user in an organization.

vApp

A set of virtual machines that is created in vCloud Director and that can be managed in vCloud Director as a single entity.