

CloudBerry Backup

Installation and Configuration Guide

Getting Started with CloudBerry Backup

CloudBerry Backup (CBB) solution was designed to facilitate PC and server data backup operations to multiple remote locations. It is integrated with top Cloud storage providers, allowing you to access each of your storage or start a sign up to a Cloud platform directly from CBB. It also works fine with network destinations like NAS (Network Attached Storage) or directly connected drives.

This document is the complete guide to the CloudBerry Backup deployment, configuration, and usage.

Product Editions & Licensing

The CBB can be downloaded directly from CloudBerry website with several editions.

- [Windows Desktop](#) (including FREE Edition) / [Server](#).
- [Microsoft SQL Server](#).
- [Microsoft Exchange Server](#).
- [Oracle Database](#).
- [Ultimate \(former Enterprise\)](#).
- CloudBerry Backup for NAS ([QNAP](#) and [Synology](#)).

They differ in functionality, storage limits and individual solutions availability. We accomplished a chart with basic editions to give a clear perspective.

CBB Edition	Desktop Free	Desktop Pro	Server	MS SQL	MS Exchange	Ultimate
File-level Backup	+	+	+	+	+	+
Image	-	-	+	+	+	+



Based Backup						
MS SQL Server Backup	-	-	-	+	-	+
MS Exchange Server Backup	-	-	-	-	+	+
Encryption and Compression	-	-	+	+	+	+
Storage Limits (for one account)	200GB	1TB	1TB	1TB	1TB	Unlimited
Network Shares for Backup	1	1	5	5	5	Unlimited
Support Type	Superuser.com forum Only	Email, 48 hours response				

On the download page, there are also links for Mac and Linux Editions. For Windows, CBB is distributed within Universal Installer so that you can choose the desired edition after the download.

The license of a CloudBerry Lab products is permanent and can be moved over, in case you recover the computer as a virtual machine (VM) or using the new hardware. There is also a volume discount – the more copies you buy, the cheaper they are. Estimated personal price is available on the [Cost Calculator page](#).

CloudBerry Backup has free 15-days trial without limitations so that you can test any backup and recovery scenario before purchase. An upgrade to the advanced edition can be done just paying the difference and activating the new license in the GUI. Please find the [License Upgrade Wizard](#) on the separate page.

System Requirements

CloudBerry Backup is a cross-platform product, which follows the diversity of modern business IT-solutions. You can run CBB on:



- Windows Server 2003/ 2008/2008 R2/2012/2012 R2 (including Core option), Windows 7/8/10.
- Ubuntu 12/14; Suse 11/12; Red Hat 6.x/7.x; Fedora 12/21; CentOS 6/7; Oracle Linux 6.x/7.x.
- Mac OS 10.8 or newer.
- Synology or QNAP device with an Intel or ARM processor (for NAS editions respectively).

There are also special requirements for successful operation:

- Microsoft .NET Framework 4.0 (For Windows Edition).
- 1.4 GHz 64-bit processor.
- 512 MB RAM.
- 100 Mbps of network bandwidth (1Gbps is better).

To maintain a dedicated backup of Microsoft SQL Server and Exchange with CloudBerry Backup, you need to have such versions as:

- Microsoft SQL Server 2000/2003/2005/2008/2012/2014/2016 (including **Express** edition).
- Microsoft Exchange 2007/2010/2013.

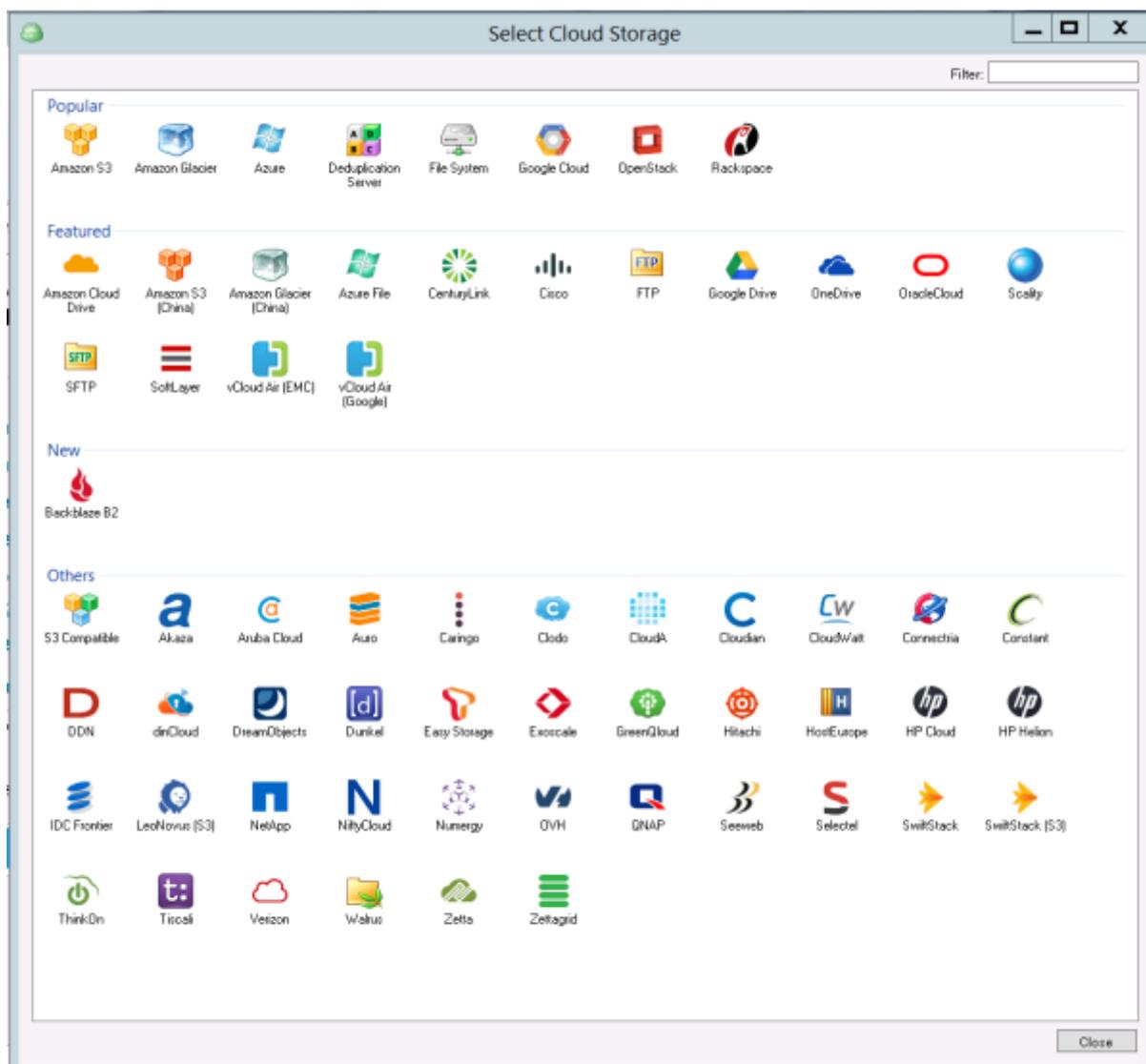
Supported Cloud Services

CBB can backup data to 59 different cloud storage facilities, which are listed on [CloudBerry Lab Partners](#) page. All supported providers for the current license are available under **Add Account** tab of **CBB Main Menu**.

The most popular destinations are:

- Amazon S3.
- Amazon Glacier.
- Azure.
- Google Cloud.
- OpenStack.
- Rackspace.
- Backblaze B2.
- Oracle Cloud.
- ...and others.





Architecture

CloudBerry Lab uses the “one machine – one instance” principle of the backup system deployment, which means that every maintained computer needs an individual copy of CBB installed. Nevertheless, with Ultimate you can backup data from multiple computers using network paths such as \\PC1\share\.

All backups of the computer identified by the individual **Backup Prefix**. If you specify the old prefix on the new machine, CBB will access all previously saved data on the storage. One backup prefix can be assigned to several computers to create a shared storage. It's useful with user workstations, which have almost similar OS and software bundlings. Find out more on the **How to Recover Jobs and Presets on the New Server** section of this document.

Backup with CBB is highly customizable. You can use any number of cloud or local storage facilities simultaneously. Moreover, the data can be freely moved between a cloud or a local storage systems

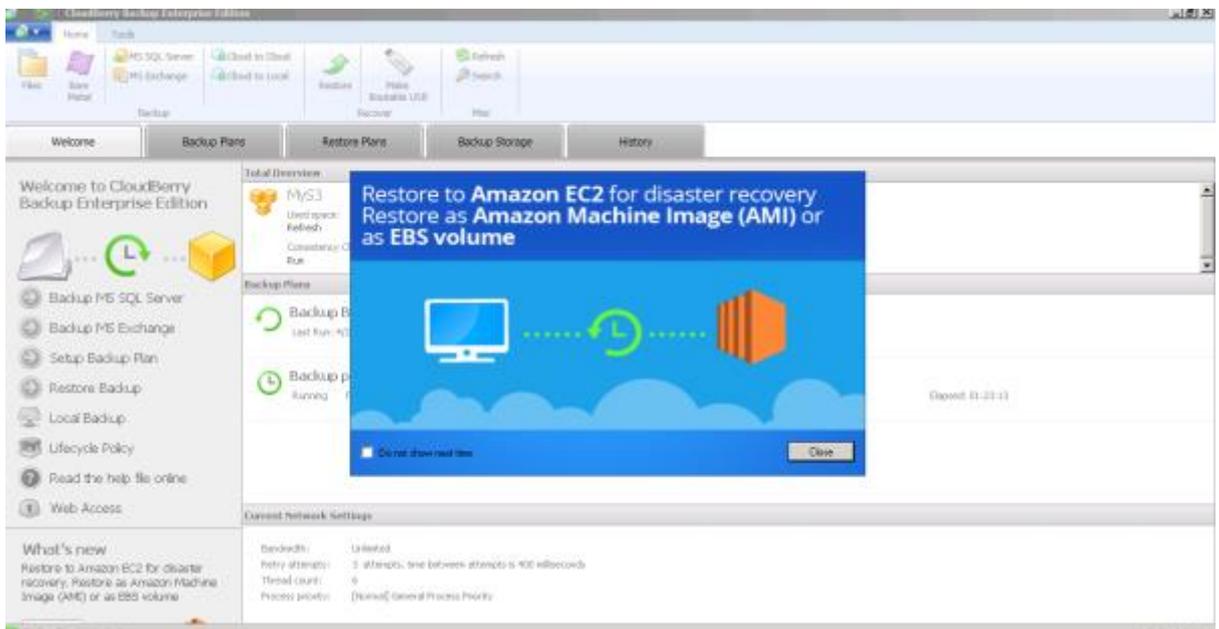


using built-in Wizard. Even if the backups are transferred manually to another storage, CBB can recognize them by the backup prefix.

How to Install

Note: in this example, we use Windows Server 2012 as a platform. The process is quite the same on the other systems, so find out more on [Mac](#) and [Linux](#) download pages.

1. Get the universal installer on the [CloudBerry Backup download page](#).
2. Double-click on the **.exe** file to launch the Windows installer. If the system needs the update or required software frameworks are missing, the installer will prompt to fix it.
3. On the first launch, choose licensing option to start CBB. It described in detail in **Activation** section below.
4. After starting the software, the home page with main options opens. They are gathered into a few groups: **Backup Plans**, **Restore Plans**, **Backup Storage**, **History**, and **Welcome**. We shall later come back to them later.

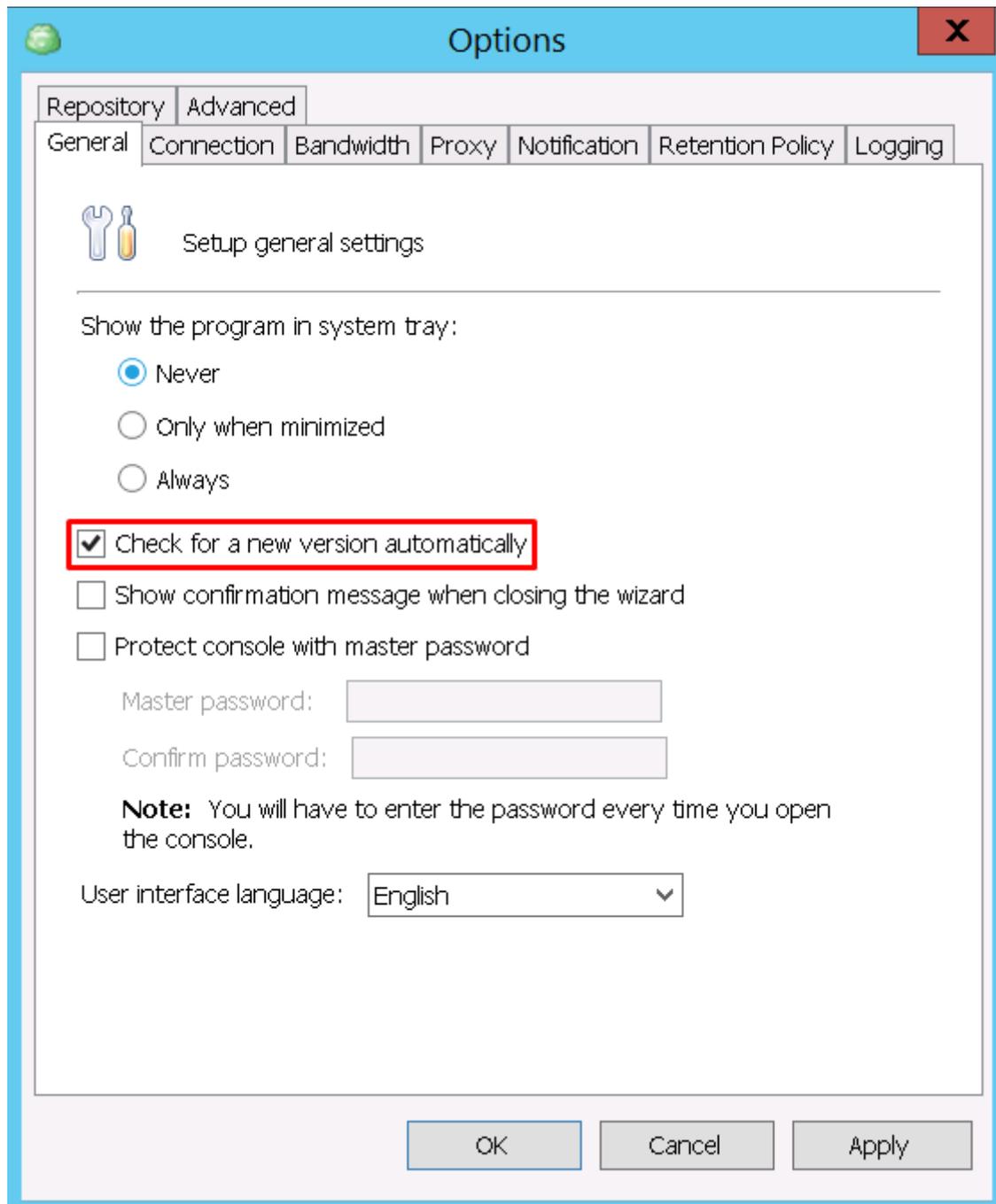


Version Update

During the first year, all the updates are free. You can check for the new releases in **Help – Check for Updates** section of CBB Main Menu, or enable the automatic update in the **General** tab of CBB **Options Menu**.

After the first year, updates are available only for customers with a support subscription. CloudBerry Backup Maintenance plan costs 20% of product price and includes annual updates and email-based technical support. You need only one support subscription for any number of CBB copies. Check the price and calculate the bill [on the special page](#).





Silent Mode Installation

You can also launch Installation in the silent mode by running the next command in the Windows Command Line:

```
CloudBerryBackup_vx.x.x.ULTIMATE.exe /S [/D=C:\custom installation folder]
```

Where **vx.x.x** is the version of CBB, and **ULTIMATE** is the edition.



Activation using GUI

There is a trial available in case you would like to try CBB first. Click the **Start Trial** button at the bottom left of the window and you'll get 15 days of free usage of the CloudBerry Backup. The activation procedure is explained in detail next.



1. You can activate the product at any time – during the trial period or when it is expired. Get the license on the [separate page](#) (same to **Buy Online** button) and click on **Activate commercial version** button on the main CloudBerry Backup start screen.



2. Enter the e-mail and license key received by email into the relevant fields, press **Activate**.



The program will verify the key and activate the acquired edition.

Note: if you want to change the product edition, e.g. you use Server Edition and want to upgrade to Ultimate, release the Server Edition license in the product and activate an Ultimate Edition. Press on the **Main Menu** button, and select **Help – Release Licence**.

If there is no internet connection on the computer, the key won't be verified. In this case, you can [activate the product offline](#).

Activation using Command Line

You can also use console commands to activate the CBB. To activate the trial, change the current path to the CBB installation folder:

```
cd "C:\Program Files\CloudBerryLab\CloudBerry Backup"
```

Then run the next command:

```
cbb.exe activatelicence -e "your_email_adress" -edition "ultimate" -t
```

Specify the desired edition instead of **ultimate**. To activate the commercial license, run the next command:

```
cbb.exe activatelicence -e "your_email_adress" -k "license_key" -or
```



Where `license_key` is the key received.

If you don't have the Internet connection at the moment, use the same command to request offline activation. In the output, you get a service key, which has to be sent to support@cloudberrylab.com.

```
C:\Program Files\CloudBerryLab\CloudBerry Backup>cbb.exe activatelicence -e "cbt
est@cloudberrylab.com" -k "b44c73f2-164e-46ed-a400-bcc798cf7" -or
CloudBerry Backup - Restore Only Command Line Interface started
Offline request generation
Offline request is generated. Please send the following to support@cloudberrylab
.com
YjrU7kWRUbcU9qnZxsYObYugQHn/ID3r9iHZZUjsolNfgaIzs6UMsU6QBDvALXA1JX0i43cpUMfvxoQ+
hcRcJyatetkBQsldyrejlQJatcQIRv6DvNiqlkwn73vKij9w4aRomhkHsbcm4ed5QkJyJA0I7DIH+H+3M
Snd0AfuksTshJwk+0kII5UaLJQq8oppCky/k6DBLBfRUMUfiE90jGL3ckJnj0zORgpUsalY6FnxvUbx1
LqUCLypxxIt9pPzkhgqxjxQtbXE18FRchj1tGicoULinBE2bCYRd7GUdy1w1R+p0fH0Ah5MgmkdUf7mg
JjEwY56cug4=MKpRFyDdmQoaUEfooth3HmW01od9CbS0sQ5a6ZDsJa2W5gGiK0fU6BL0BeI p6hgpUgu
XApdRm11TgkIACU6pWaLxjw8UIUFk9LdS4QcEHPDzaf+1geuNRx51zI8M6uJUTQ6oCuXxrPiZLw9TEH4
UtGmf pjnPQ9wKHnt@TTxaHkn yWa7+Xe76CGhM48k3Gkr@iaxKBbQQFo08HuPfaZN8tnscwM1eSgUqY8G
GUd/amE2HU0achRBCb/1UqU6KbmSuLTSIof9i26U=
C:\Program Files\CloudBerryLab\CloudBerry Backup>
```

Support will give the activation key. Use key as follows to activate the CBB:

```
cbb.exe activatelicence -e "email" -k "license_key" -oa "activation_key_received"
```

For more information, see the **Command Line Interface** section of this document.

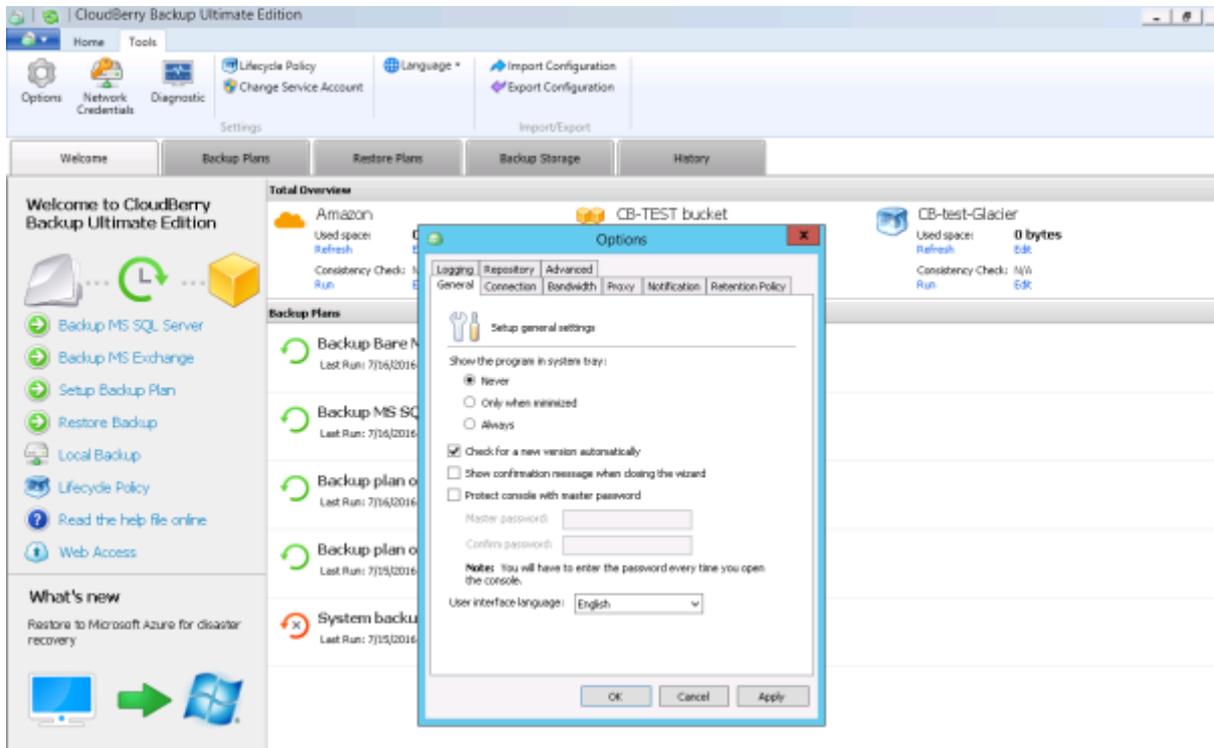
How to Backup

Before starting a backup, you may want to tune up CloudBerry Backup settings: set a proxy, limit bandwidth, set default settings for new backup plans, etc.



CloudBerry Backup Configuration

Click **Options** on the **Tools** tab to access application settings. Here you can change CloudBerry Backup parameters.



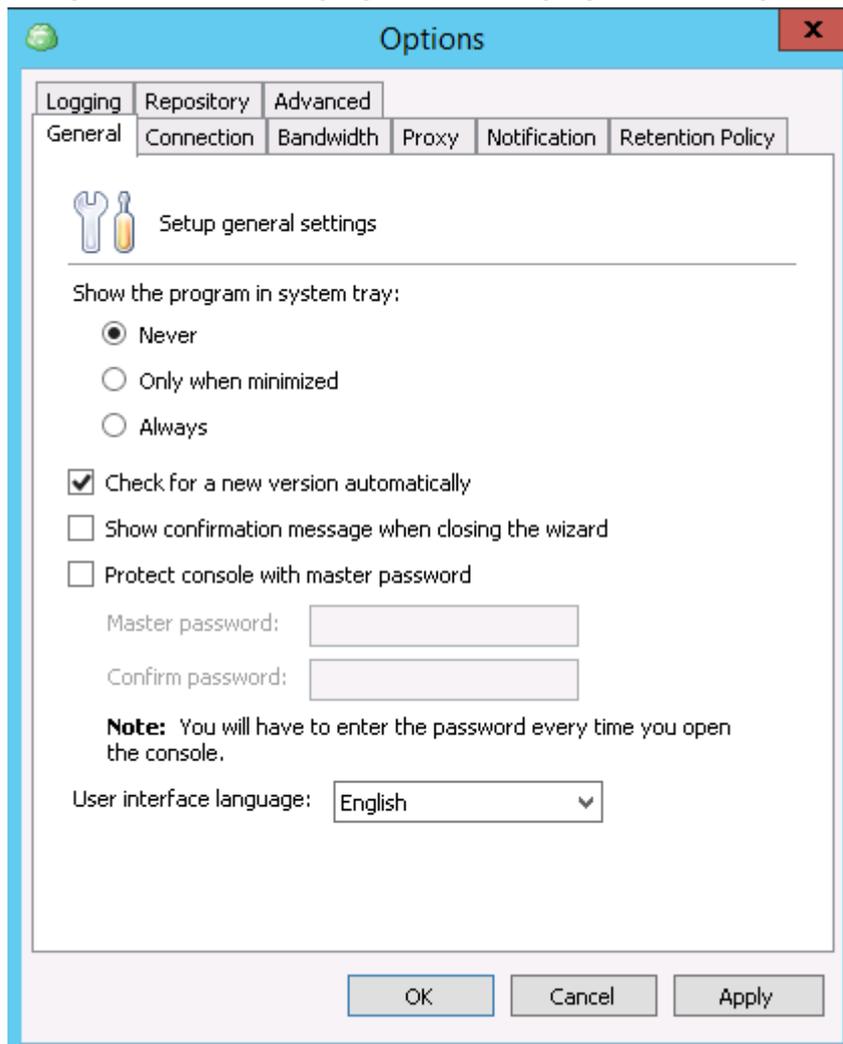
General

On the **General** tab of **Options**, you can do the following:

- Specify if the CBB icon appears in the system tray.
- Enable automatic version update.
- Prevent accidental Wizard closing with the confirmation window.
- Protect **Options** console with the password.

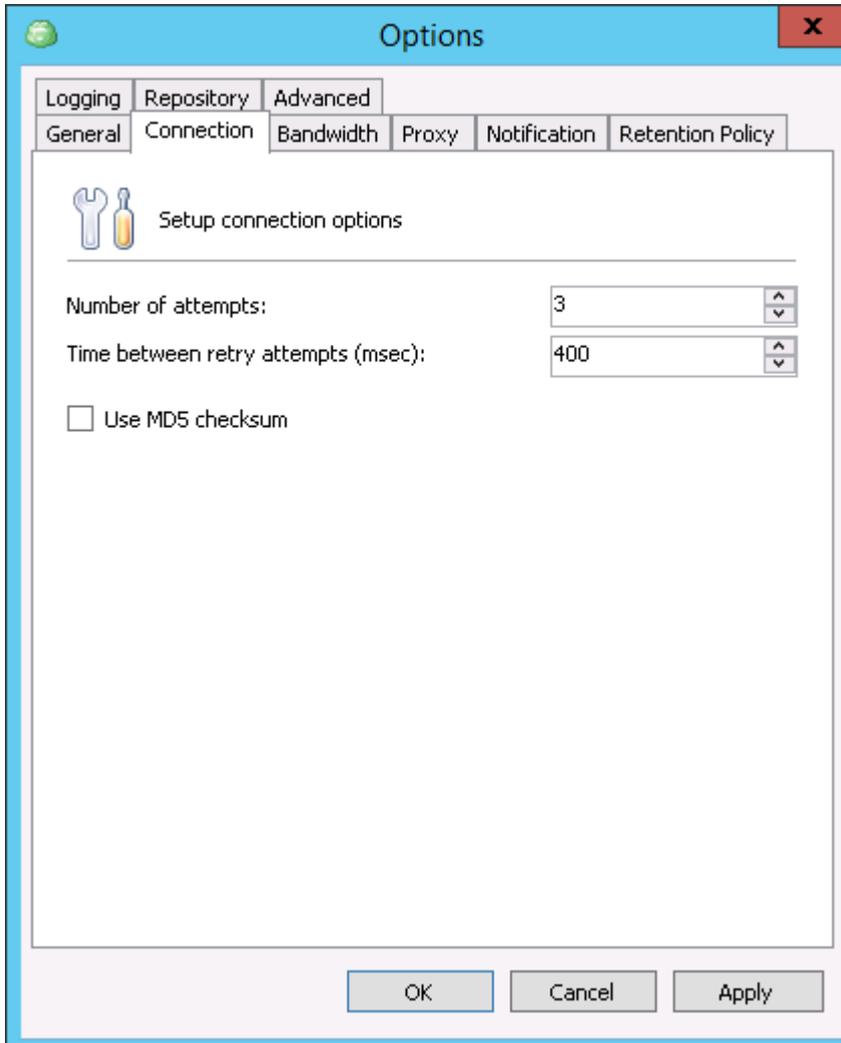


- Change interface language (15 languages including Chinese are available).



Connection

If CBB can't reach network destination, it makes several attempts to reestablish the connection before reporting an issue.

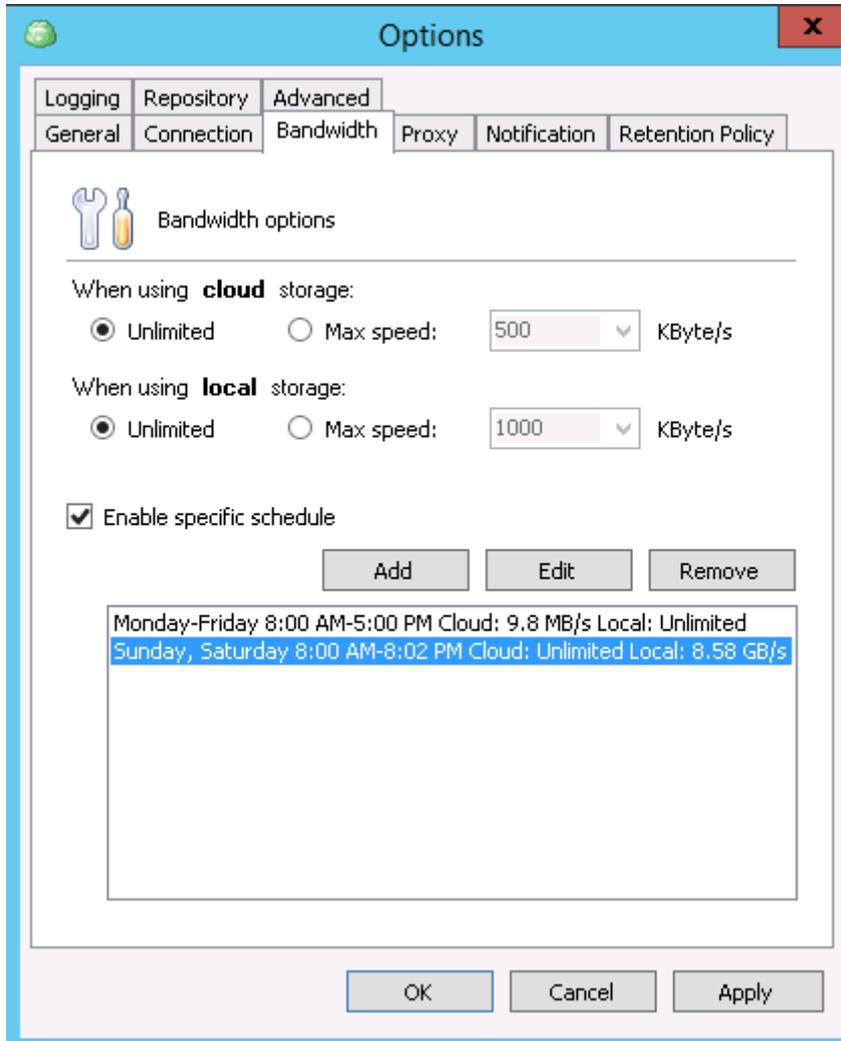


At the **Connection** tab, the options define the number of attempts and the timeout period.

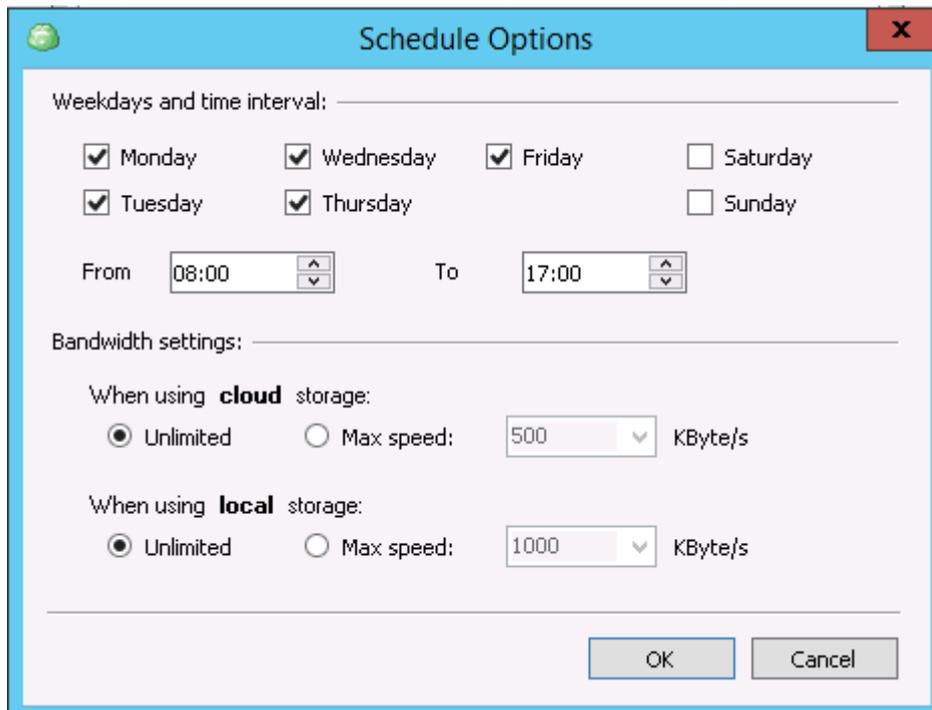


Bandwidth

The **Bandwidth** group controls CBB network utilization. It can specify the maximum speed for cloud or local destinations.



Enable specific schedule feature assigns network usage limits for each day of the week.

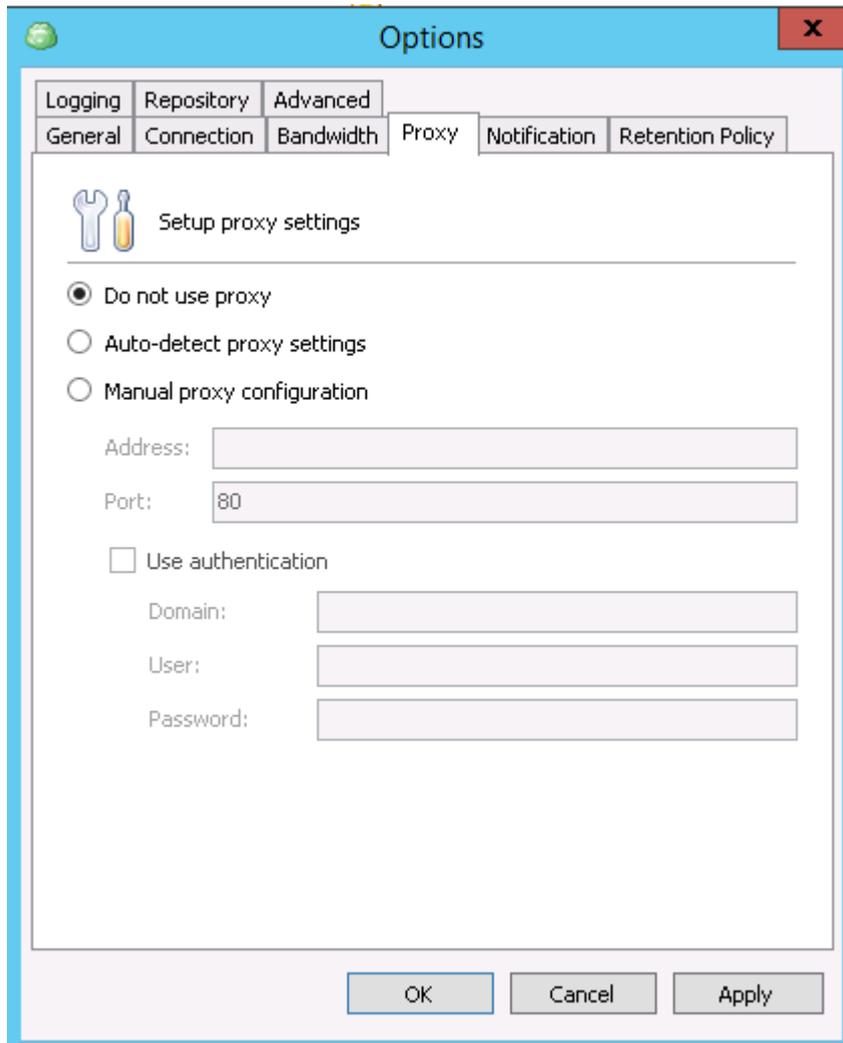


For time periods not covered by schedule, global settings are applied.



Proxy

At the **Proxy tab**, you can specify the intermediate server for the Internet access. With the **Auto-detect proxy settings** enabled, CloudBerry Backup will use operating system defaults.



We recommend testing of the new configurations by creating a backup plan.

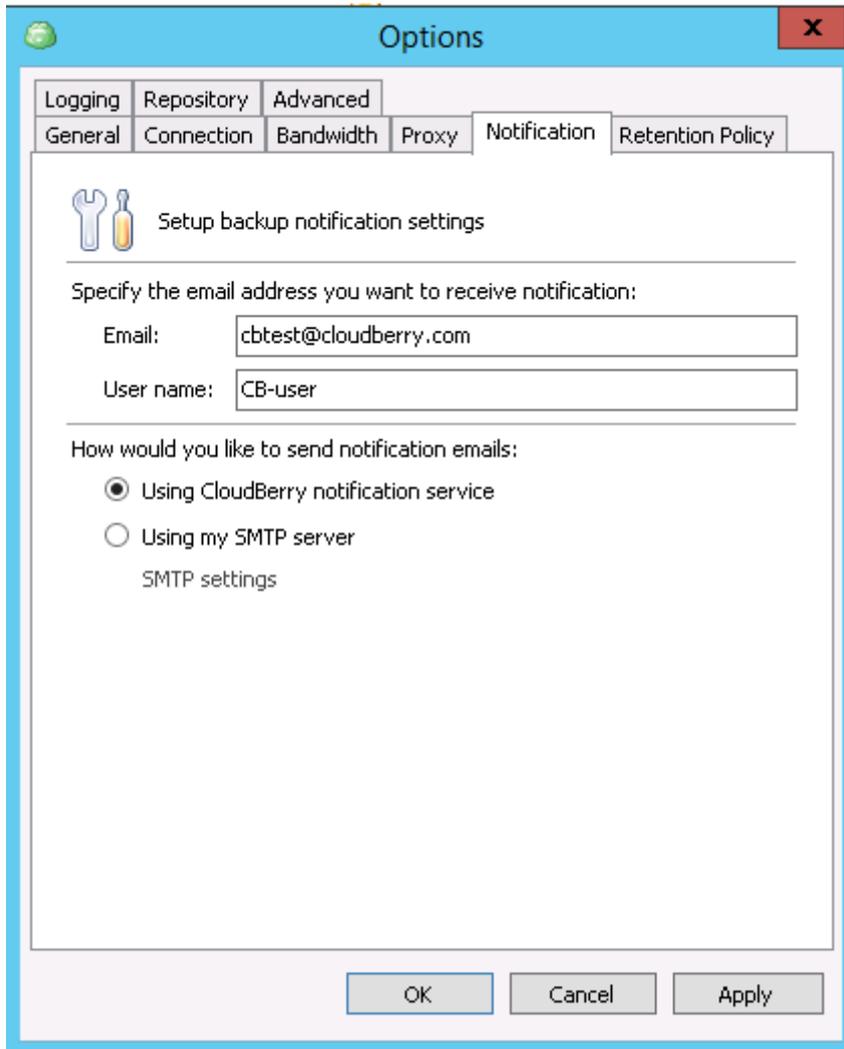
Notification

CBB can notice about backup or restoration process completion status via an email. The application will use the email and username specified as the default on the **Notification** step of any Backup and



Restore

Wizard.



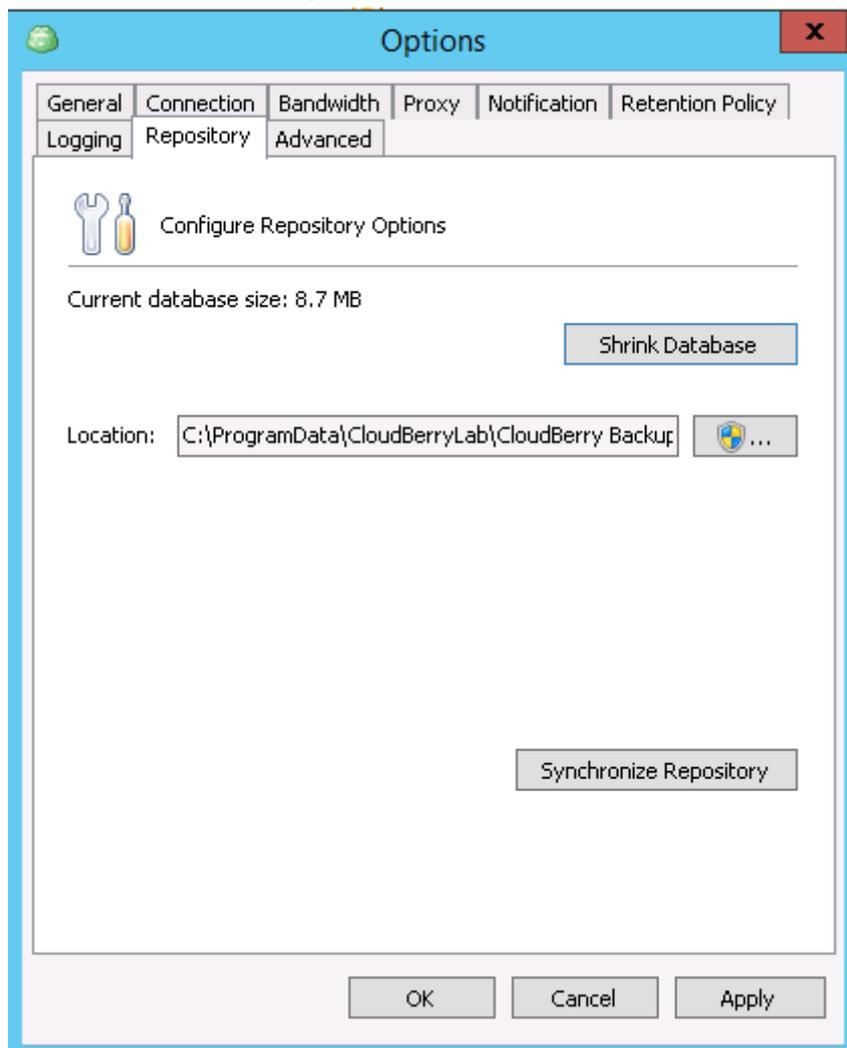
You may also connect own mail server by selecting of **Using my SMTP server** option

Repository

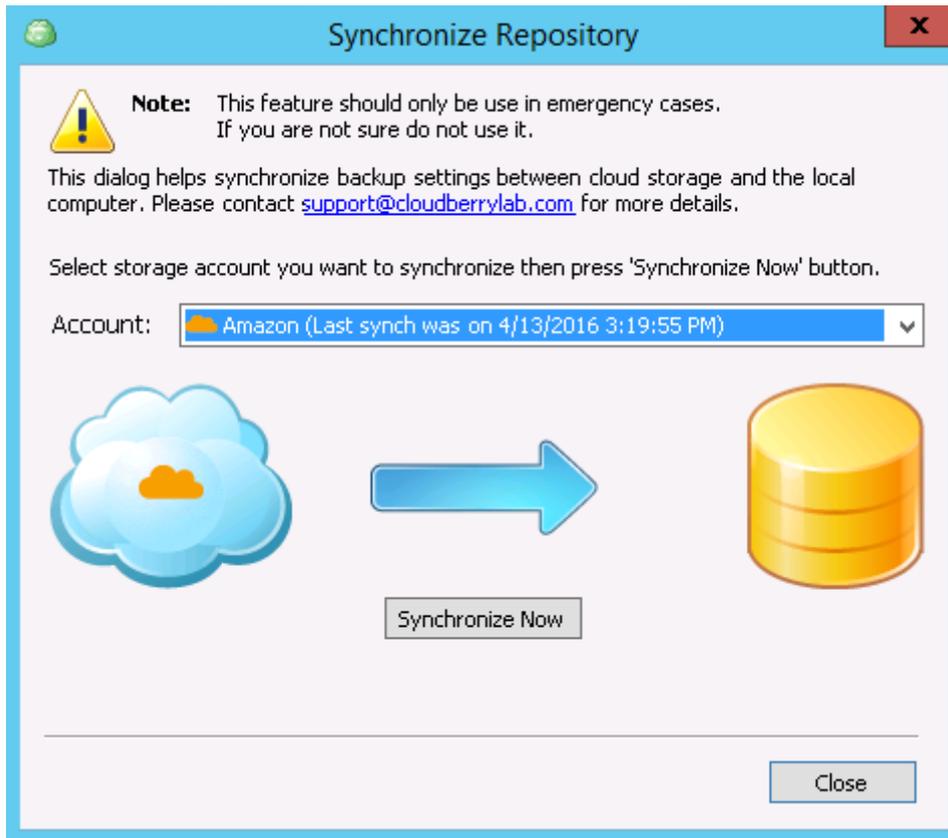
CBB uses the database to monitor the contents of the connected storage and track down modifications. File deletion, storage operation by third-party software and backup migration may increase its size, as CBB keeps the old records in case the user will restore data manually. Clicking on



the **Shrink Database** option will delete redundant records and decrease the database size.



Synchronize Repository feature force the update of backup storage database.



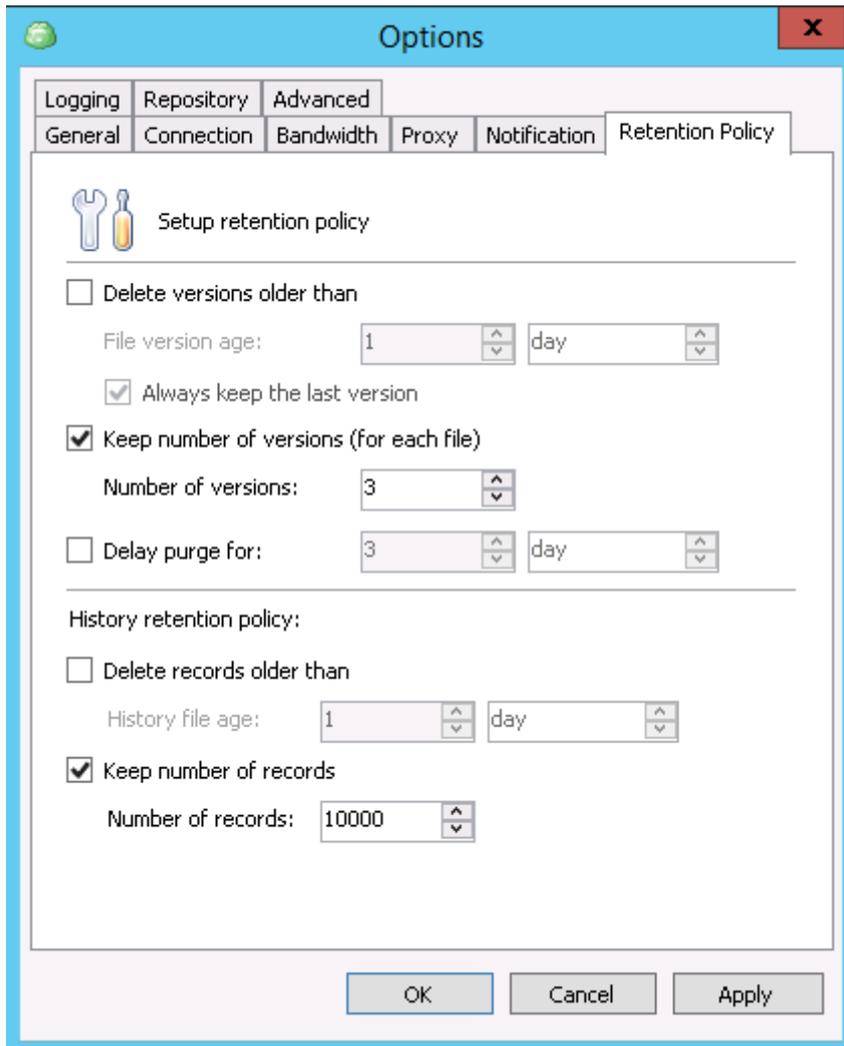
As the cloud providers usually charge for the data requests, you should use this features only in particular cases such as described in **Advanced Solutions – Glacier Restore** section of this document.

Retention Policy

Retention Policy defines the number of versions stored for each of backed up files, including their maximum age and the deleting delay time. You can establish custom retention policies for new backup plans, but keep in mind that larger versions history requires more storage space. Find out more in



Additional Features – **History** section of this document.



Other Options

Logging and **Advanced** options tabs are described in detail in **Troubleshooting** and **Advanced Solutions – CloudBerry Backup Advanced Options** sections of the document.

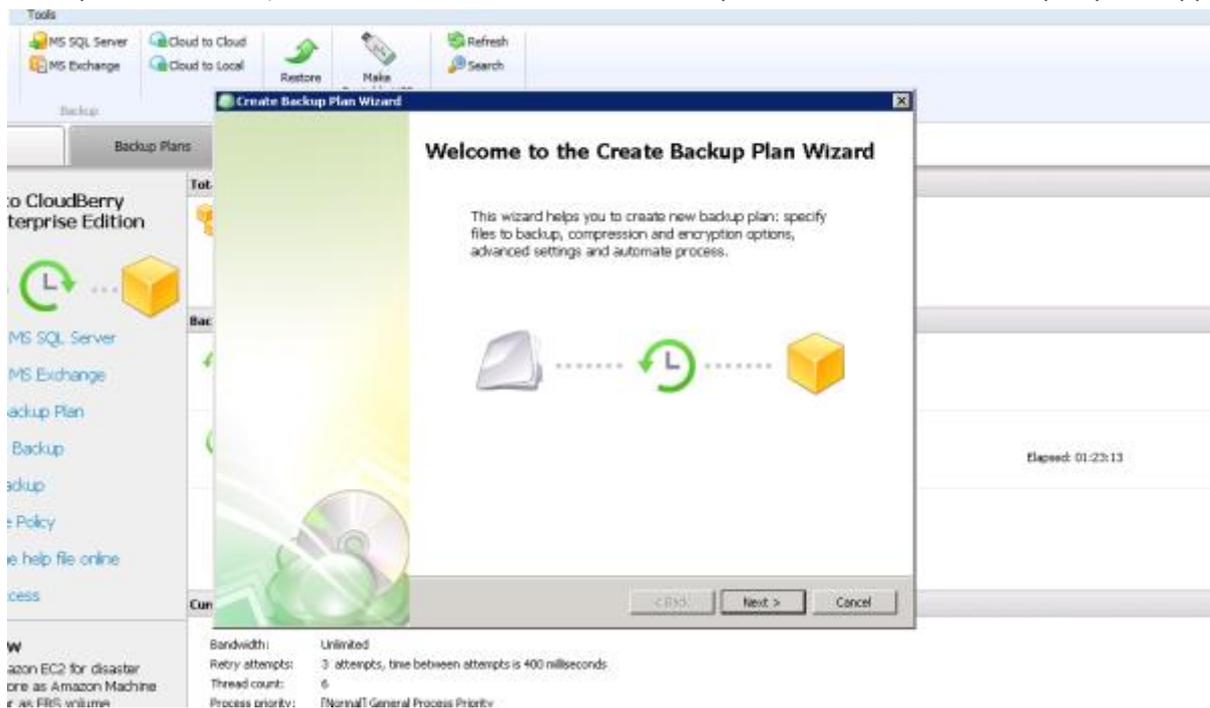
Backup Types

The **Backup** group of options provides the following data backup services:

- **File-level;**
- **Image-level;**
- **Synthetic;**
- **Microsoft SQL Server backup;**
- **Backup of a Microsoft Exchange Server;**
- **Cloud to Cloud and Cloud to Local transfers.**



If you click on any of these options, the **Backup Plan Wizard** launches, helping you to create the first Backup Plan (it is similar to Backup Job in third-party apps).



The Wizard will guide you through all required parameters of a backup plan you have chosen.

File-level Backup

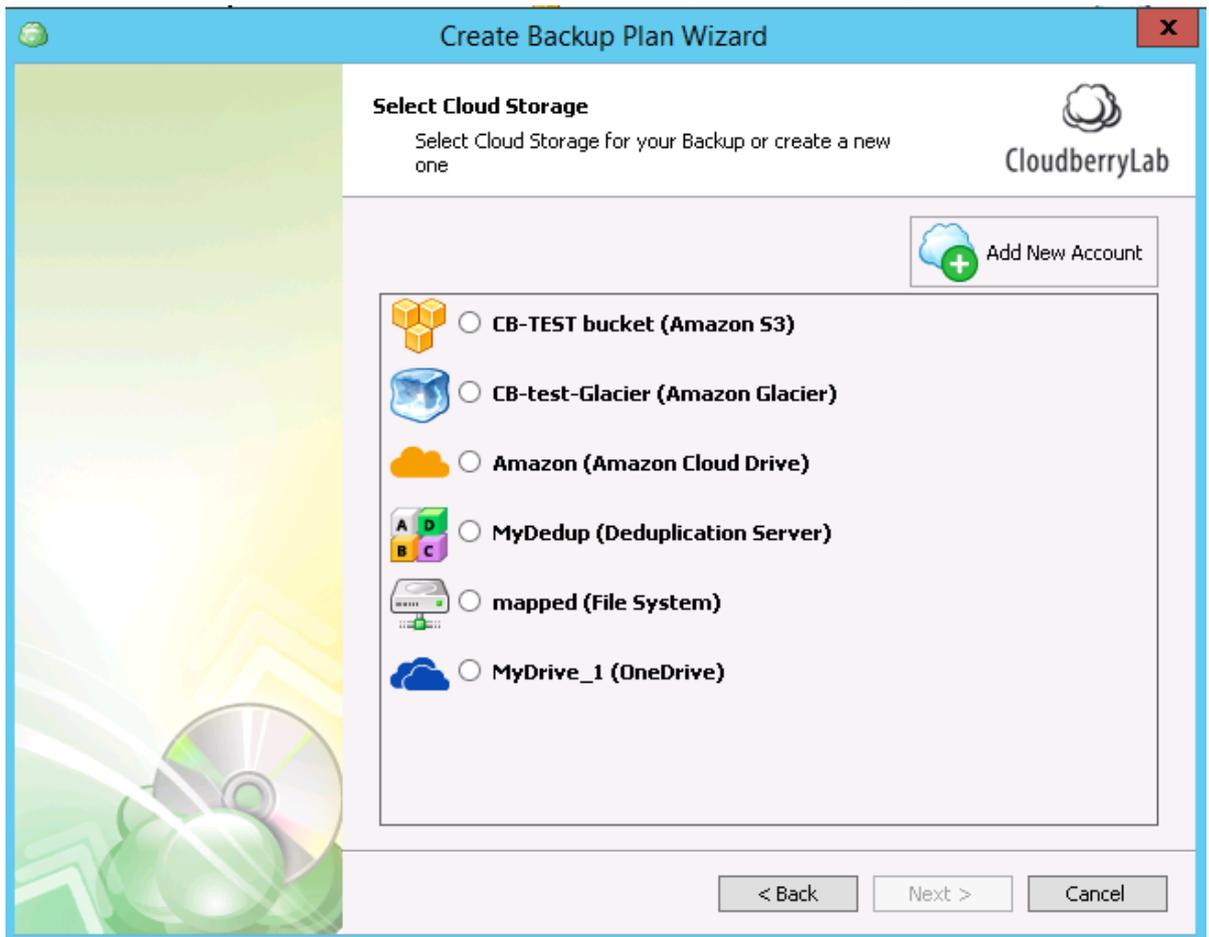
File-level Backup helps to save various files and folders on the computer. It is the best way to protect a user data since it doesn't require as much space as other backup types and performs generally faster. If you also need to protect OS system partitions, we recommend using Image-level backups.

To start protecting files and folders on the computer do the following:

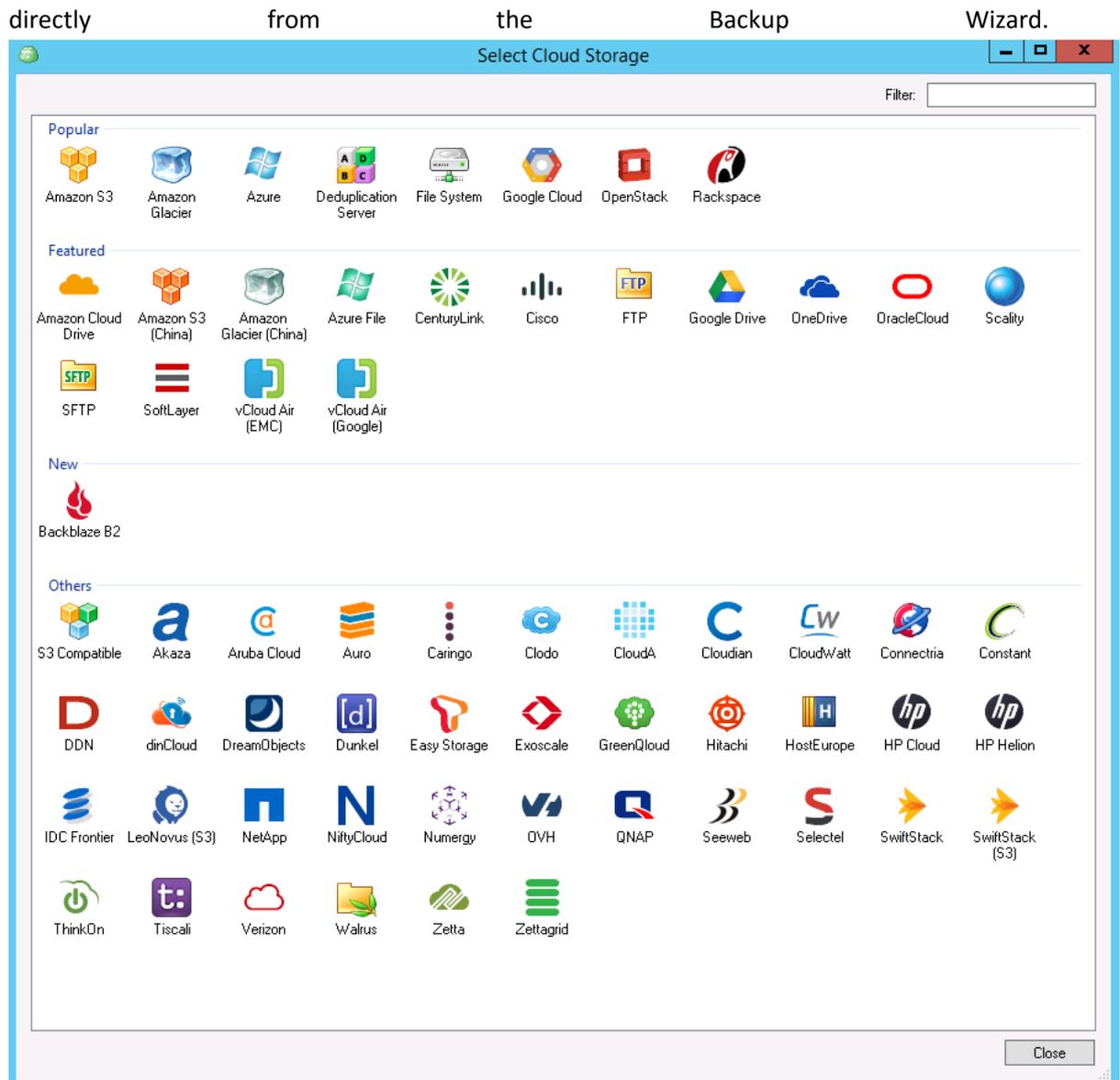
1. Click the **Files** button on the **Home** tab to launch the Wizard.



2. Click **Next** and select a storage for your backups.



3. CBB helps facilitate backup management in a number of remote storage providers, so you need to subscribe for one of such cloud storage facility. Alternatively, you can start a sign up



4. Let's add Amazon S3 storage as an example. Once you login to S3, CBB will remember the account to choose it quickly for next backup plans. Click **Add New Account** and double click on the Amazon S3 icon in the appeared list.
5. In the **Amazon S3 Account** window, specify the display name for this storage and provide security keys to connect existing S3 account. If they are correct, the bucket will appear in the



Bucket name dropdown.

Amazon S3 Storage Account Cost Estimates Consistency Check

 Setup Amazon S3 settings

Amazon S3 account:
You can [import](#) an account from one of CloudBerry products.

Display name:

Use Access and Secret keys

Access key:

Secret key:

Use AWS IAM role policy
Applicable if you run application on AWS EC2 instance

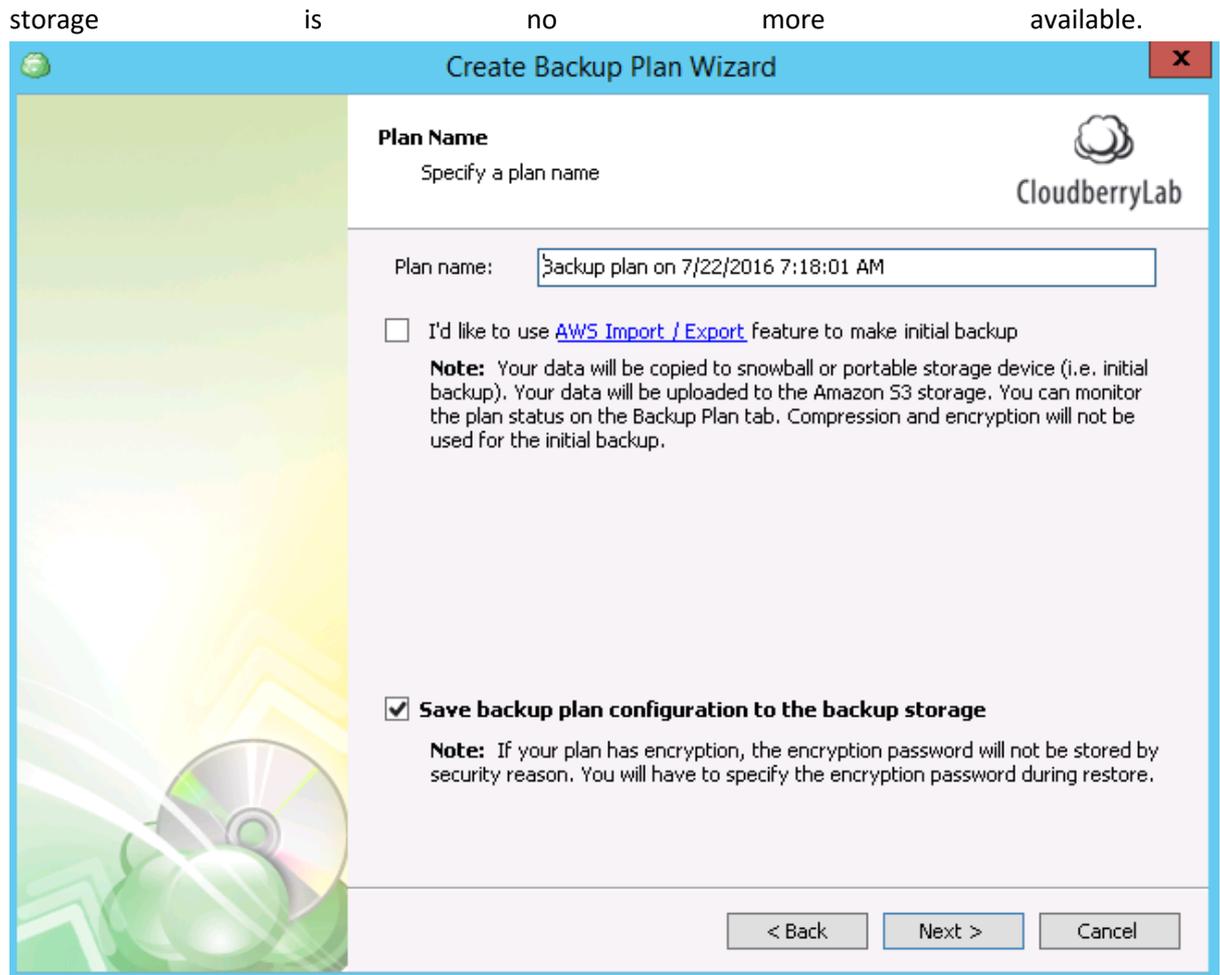
Bucket name:

[Advanced settings](#)
[Specify Proxy Settings](#)

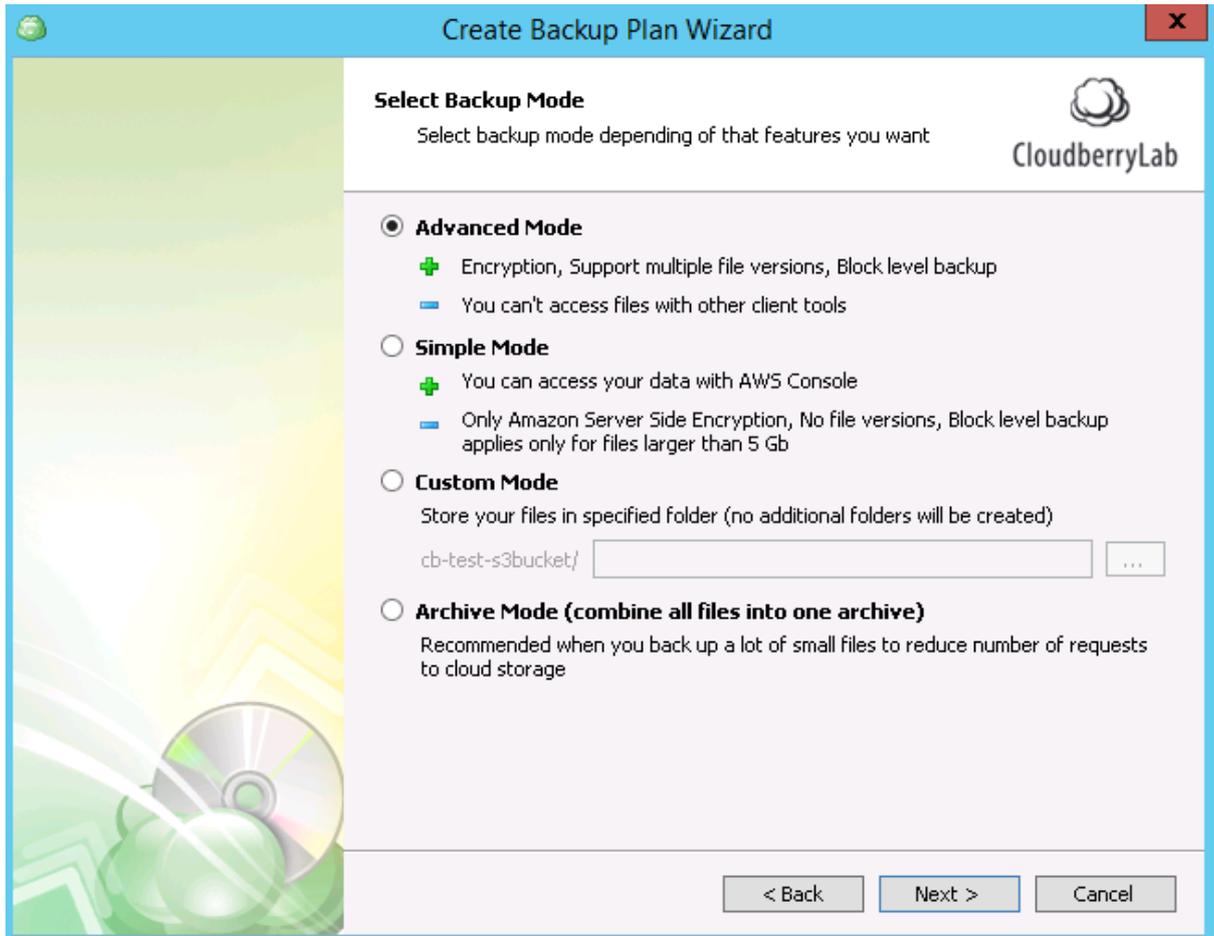
Don't have an **Amazon S3 account** ?
[Create an account](#) - It will take just a few minutes!

6. You can also choose to connect to S3 account via an IAM role policy or to import the credentials from another CloudBerry software. To establish a new S3 account right away, click the **Create a new account** link at the bottom to open AWS sign up page.
7. After selecting storage and clicking **Next**, specify the plan's name and decide whether to save its configuration on the cloud storage. That helps to restore jobs and presets in case the local



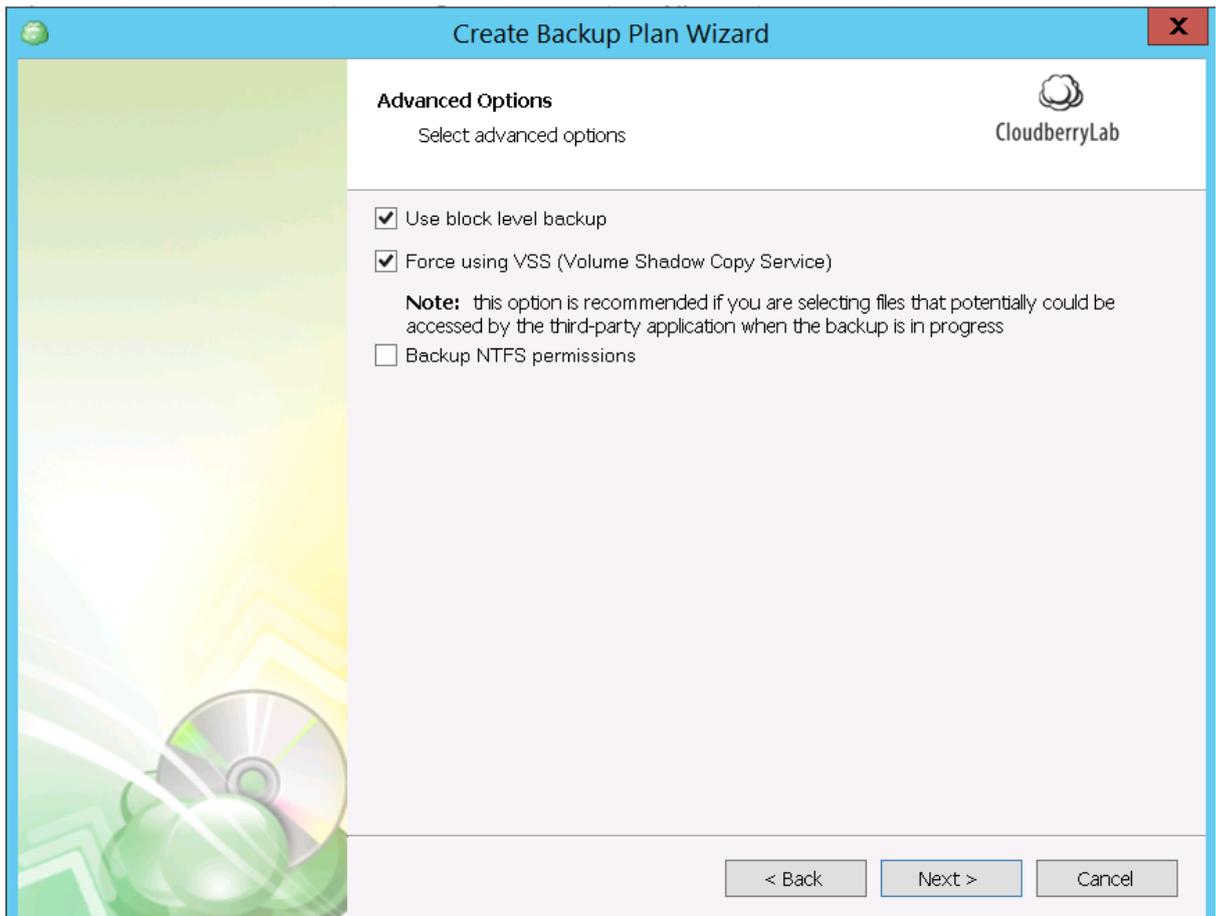


8. At the next step, select **Advanced**, **Simple** or **Custom** mode for backups. The **Advanced** mode enables many helpful CBB features such as, for example, data encryption and versioning.



9. If you've chosen the Advanced mode, you can decide whether to **use VSS** or backup NTFS permissions. Another useful feature is **Block Level Backup**. It reduces network and storage utilization by uploading only those parts of the files which have been modified since the last

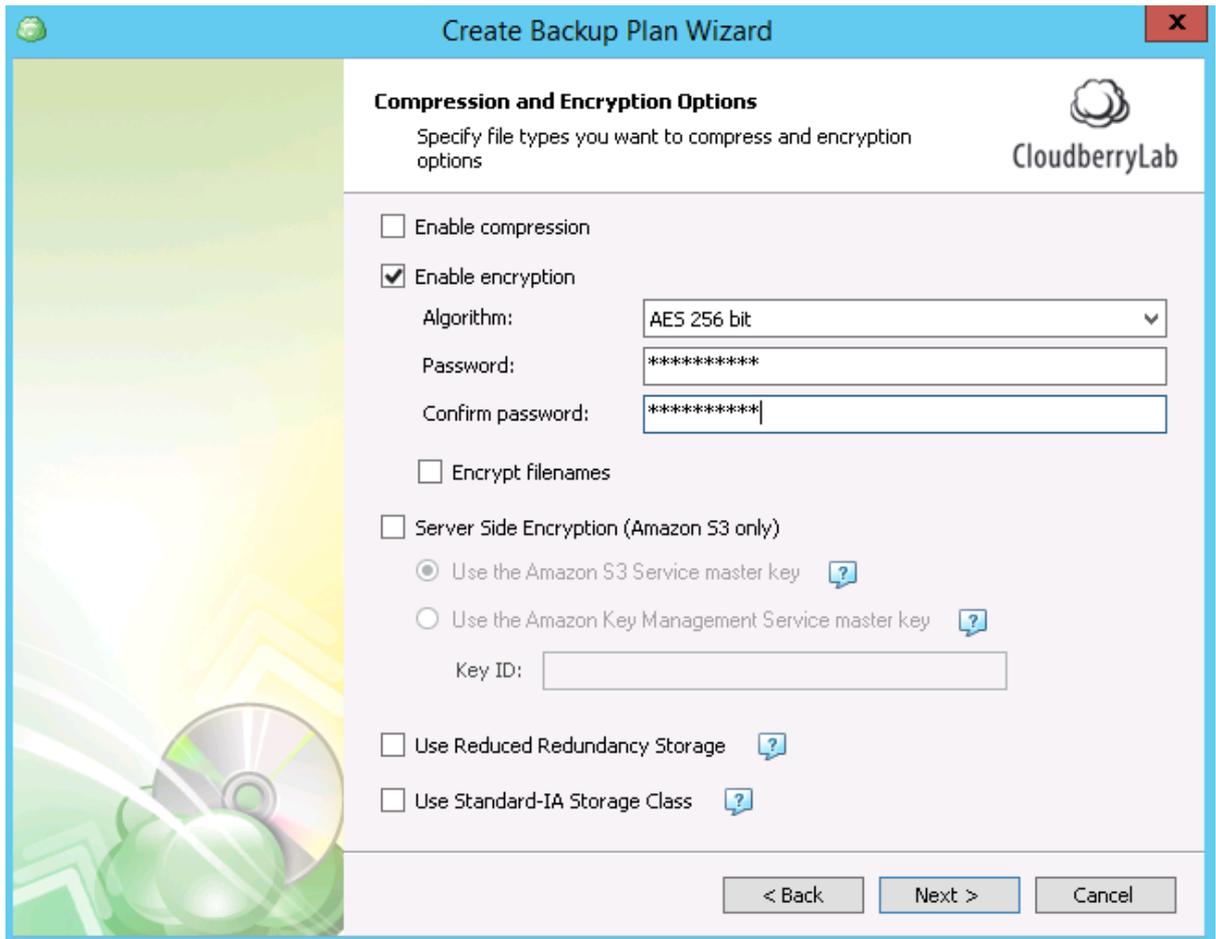
run. Properties of the feature adjusted on the **Full Backup Schedule Step**.



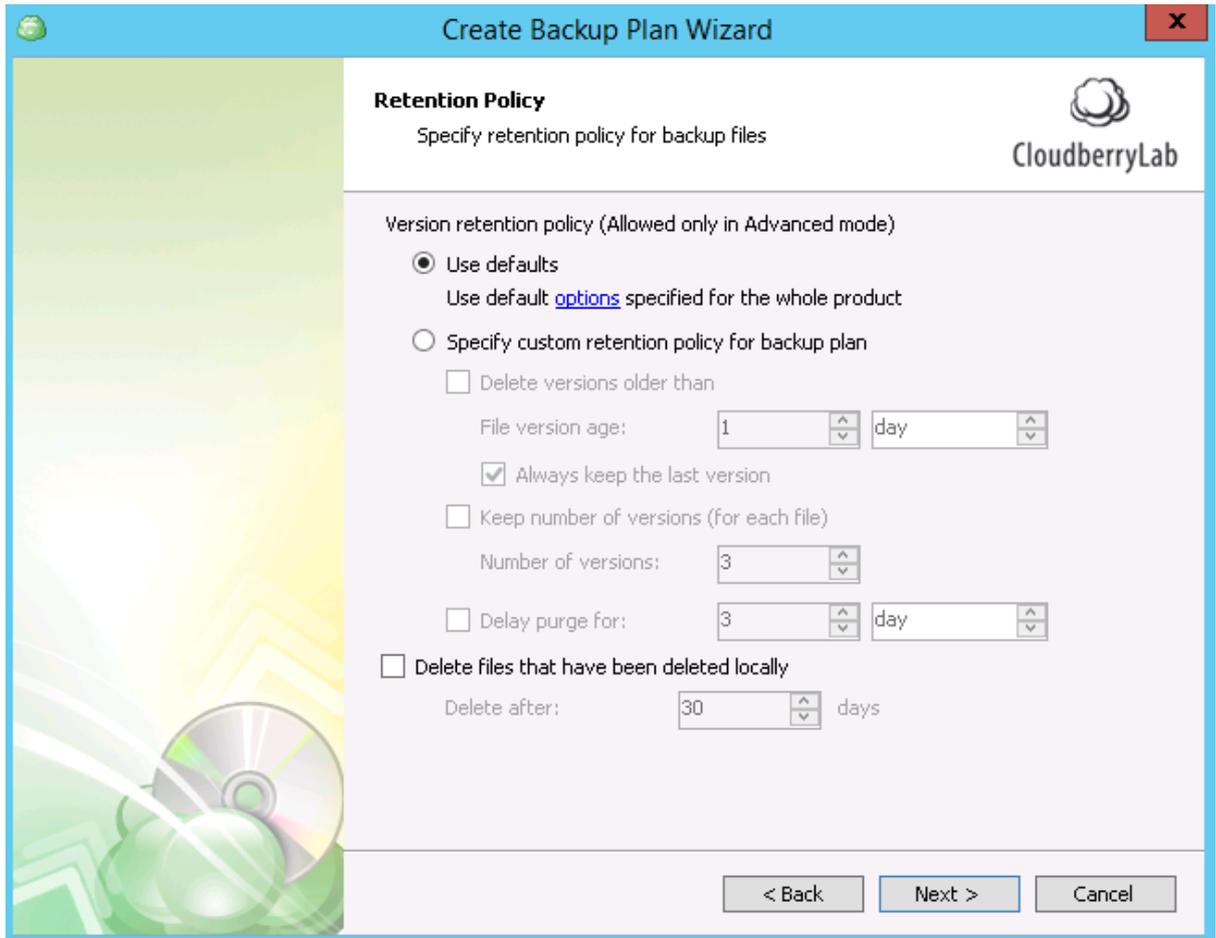
10. During the following steps, a number of other options are to be selected, such as types of files and folders to store, limitations by the time of their modification, data compression, and encryption. You can also use particular S3 storage classes to reduce storage expenses. Read



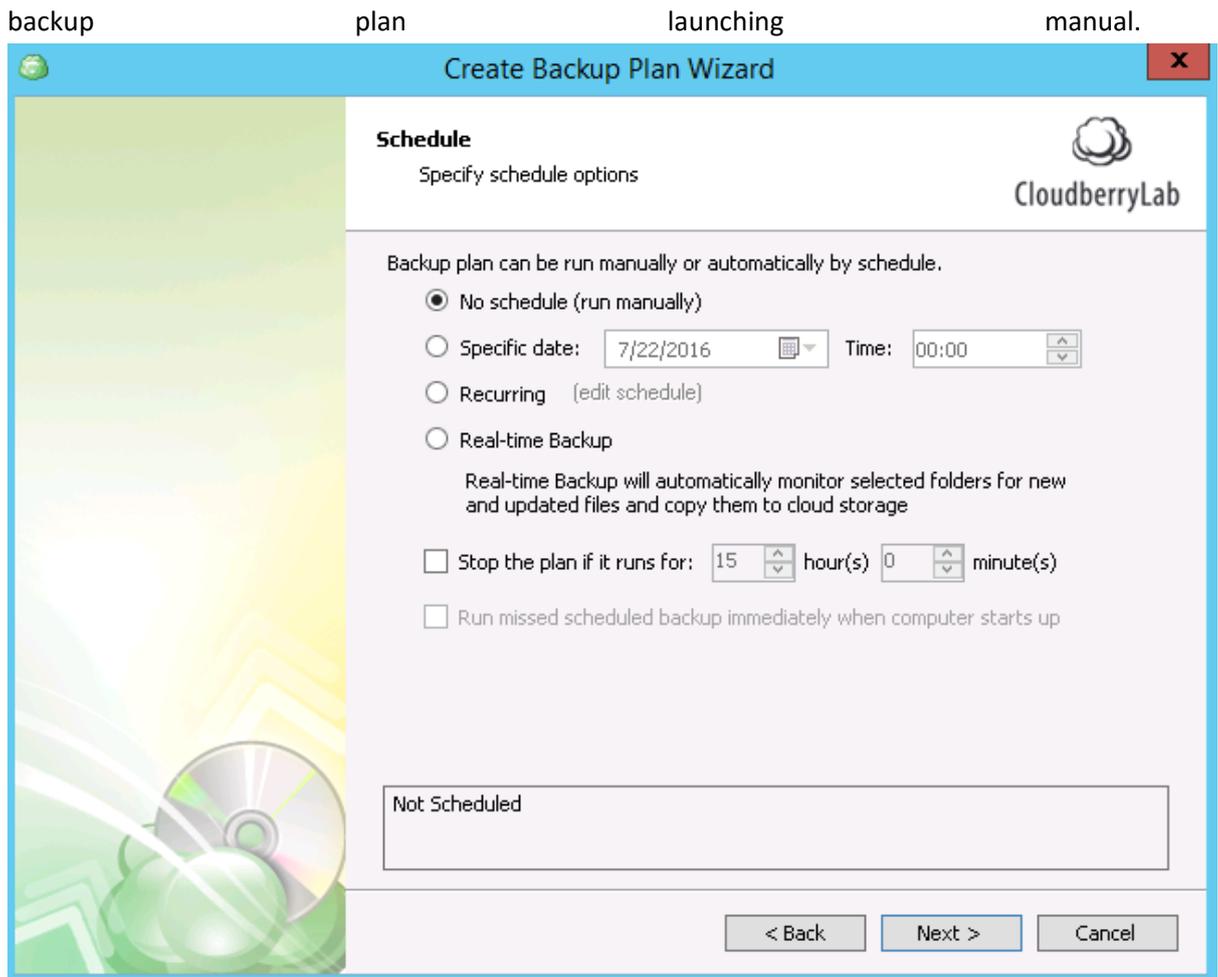
more on the [AWS S3 Storage Classes](#) page.



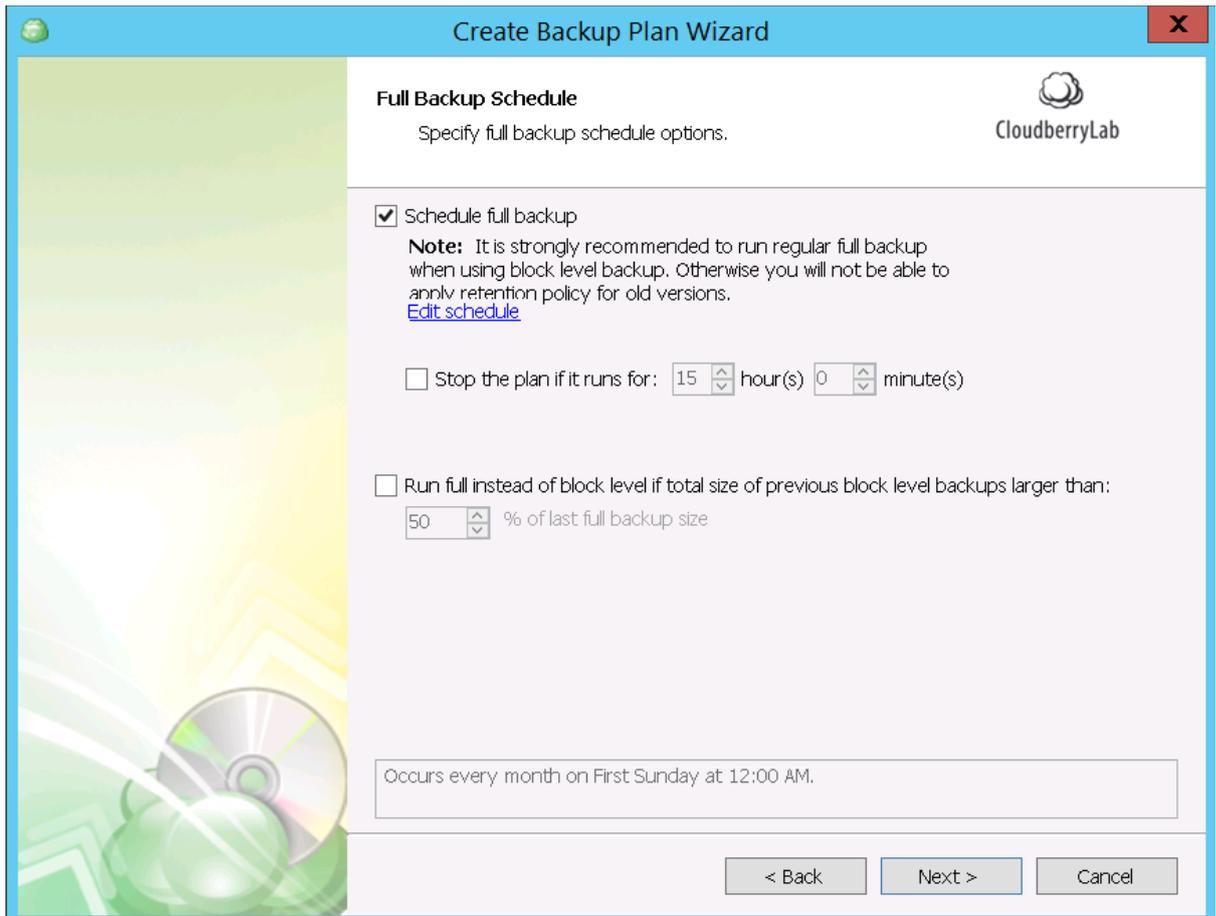
11. One of the most useful CBB features is **Retention Policy**. It allows specifying the number of versions to keep, their maximum age and the deletion delay timeout.



12. You also need to define a **Schedule** for the new plan, allowing CloudBerry Backup to handle backup plans automatically. You can also proceed next without a schedule, thus making the



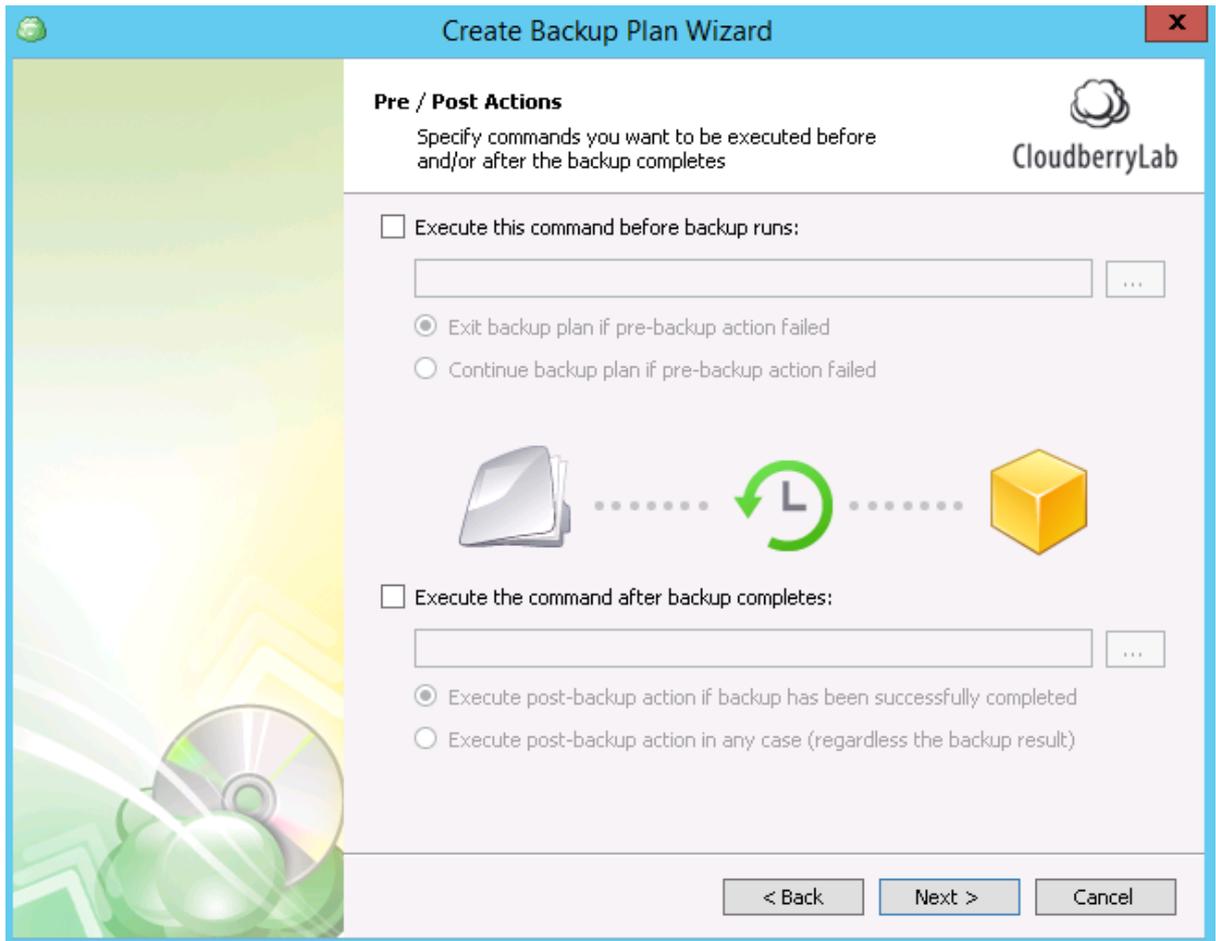
13. If you choose to use **block-level backup**, CBB can periodically copy all volume data. This **Full Backup Schedule** goes aside of general schedule, and isn't an inevitable thing. But if a block-level backup runs every day, it is recommended to make a full backup once a week to increase data durability and facilitate restoration.



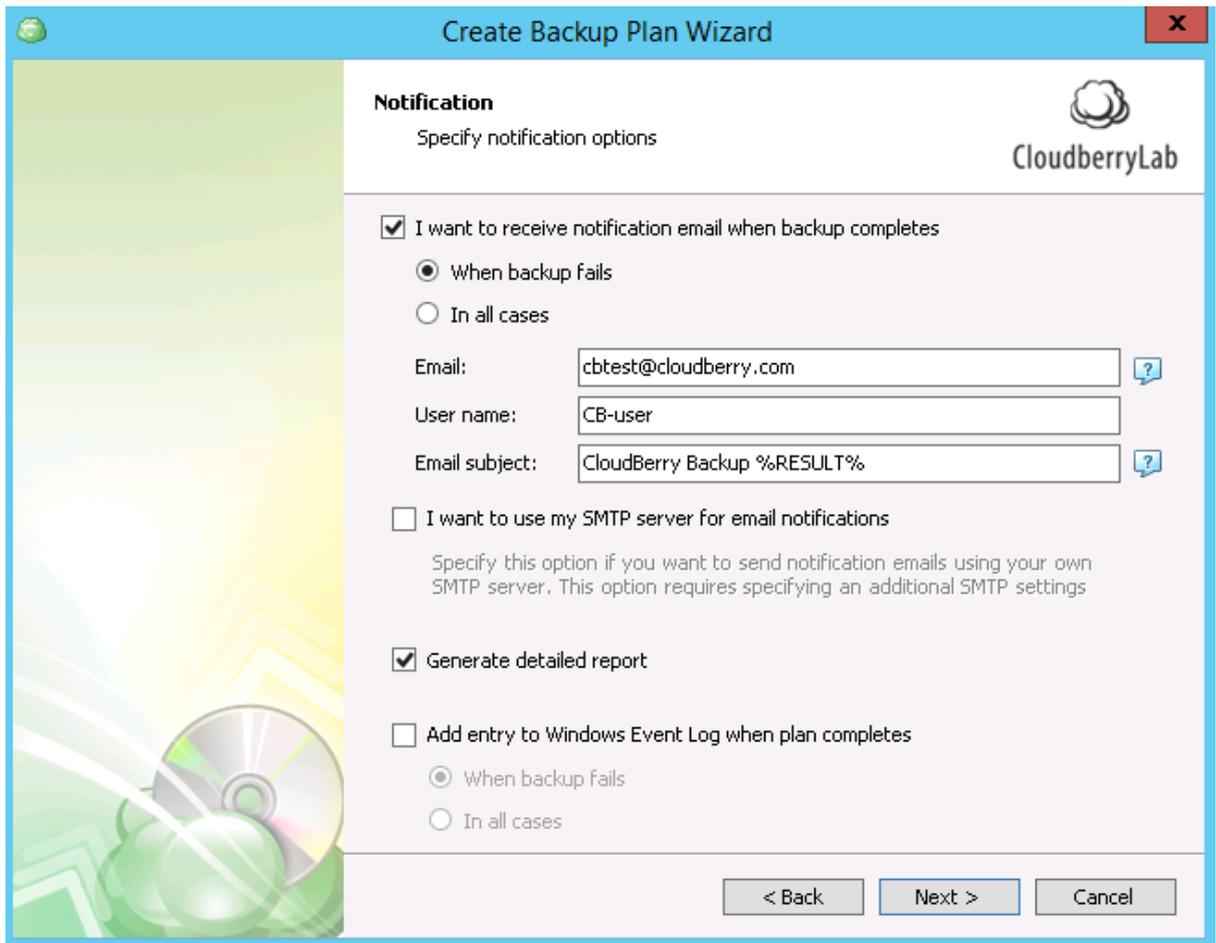
Remember that block-level recovery progresses in two steps: first, you recover the last full backup, then apply all the incremental backups made afterwards.

14. CBB can execute Windows Command Line scripts before or after the backup job. That helps involve third-party software into the backup process or perform additional CBB tasks. See **Advanced Solutions – CloudBerry Backup Advanced Options – Command Line Interface**

section of this document to find out about particular implementations of the feature.



15. Finally, it is possible to define how CBB can notify you. The backup plan can add status notifications to a Windows event log or send it by email.



16. After clicking **Next**, a new summary page opens so you could check new settings. Click **Next** to create and launch the new backup plan.

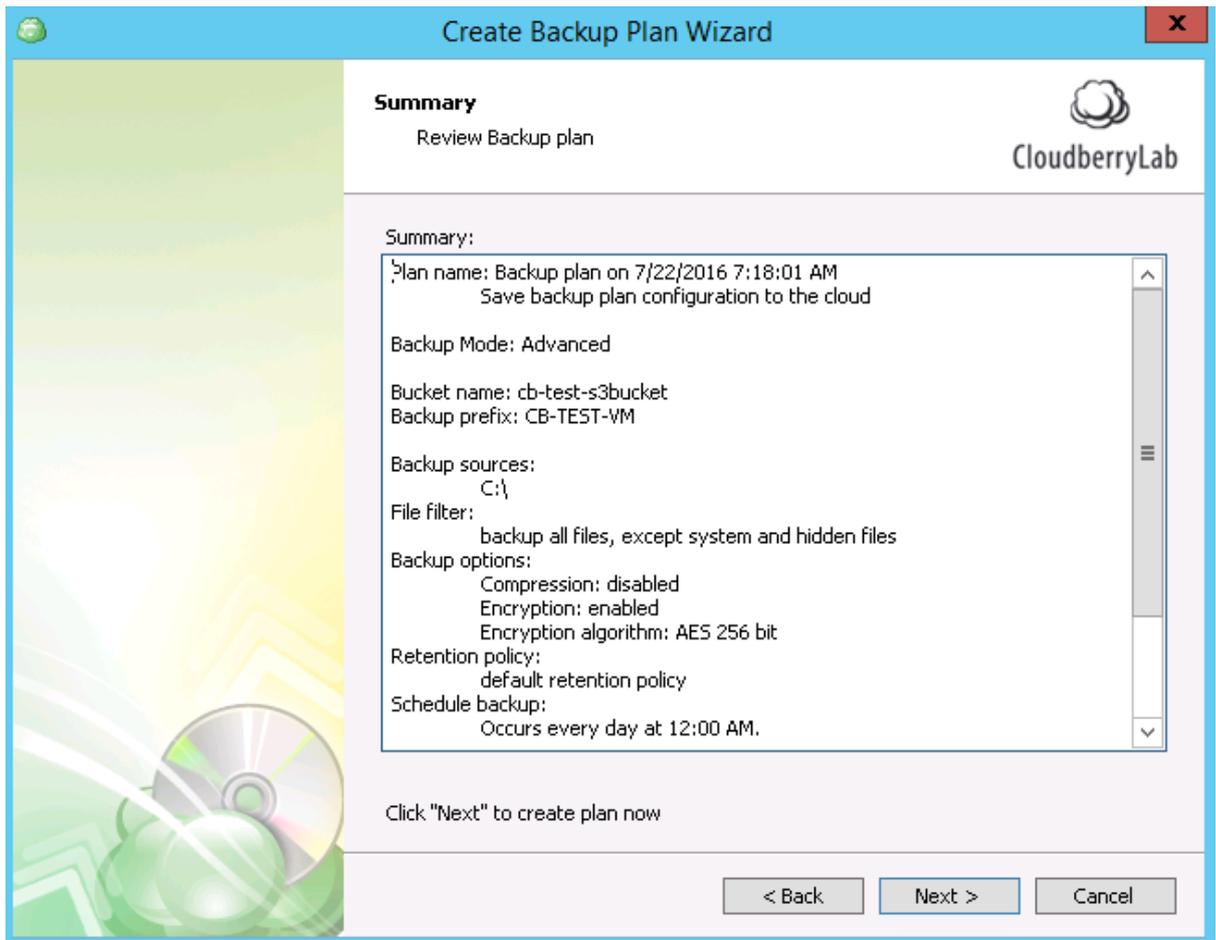


Image-level Backup

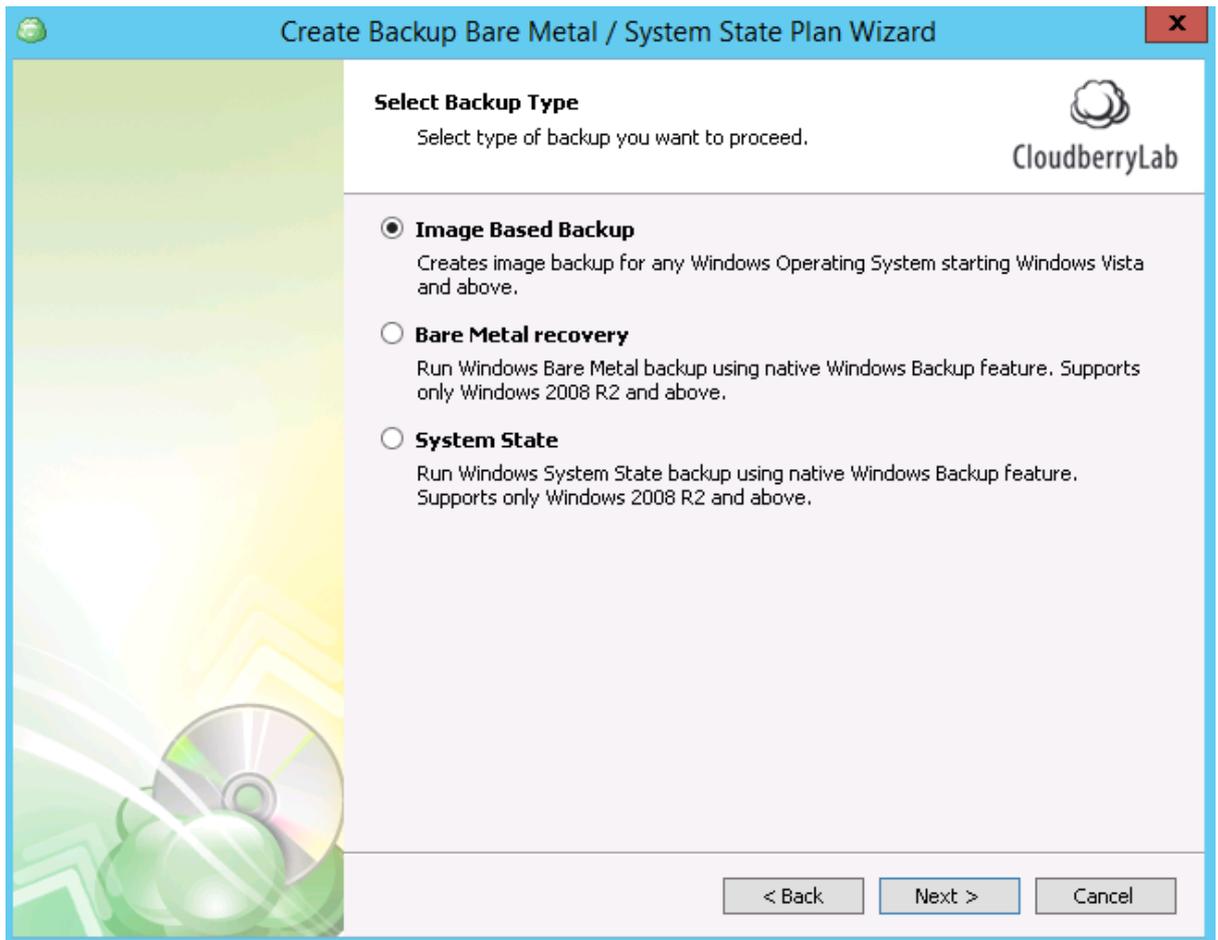
The image is the file containing the disk data, partitions, structure, file system, and other properties. Unlike the archive, the image copies data on a block level. But still, it is possible to retrieve separate files and folders from the image. This backup type is typically used for a disaster recovery, hardware migration, and virtual machines deployment.

To run the image-based backup, press **Bare Metal** button on the **Home** tab.

1. After the backup plan's name specification step you have to select the backup type:
 - **Image Based** option copies the disk or its separate partitions. You can also recover separate files from the image. This mode allows restoring VM to EC2, Azure or as a virtual disk.
 - **System Image (former Bare Metal)** option backups all root volume with boot files and OS using built-in Windows recovery feature. It's used for restoration to the new hardware or for repair of heavily corrupted system.



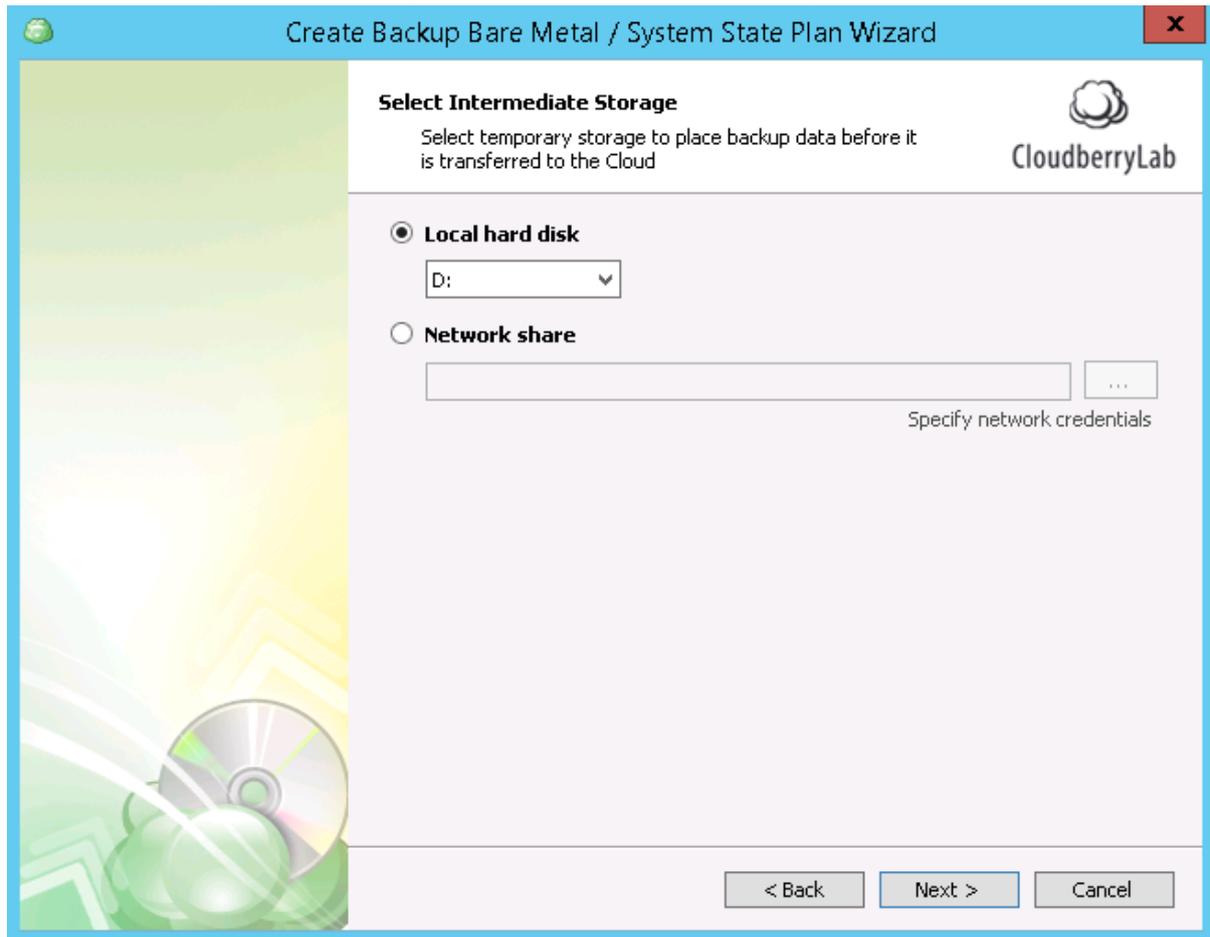
- **System State** option copies boot files, registry, drivers and other OS-crucial data with built-in Windows recovery feature. It is often used for a system repairment.



Both **System Image** and **System State** types require the installation of Windows Backup feature. Moreover, they need an intermediate storage on a separate logical disk or network storage, where



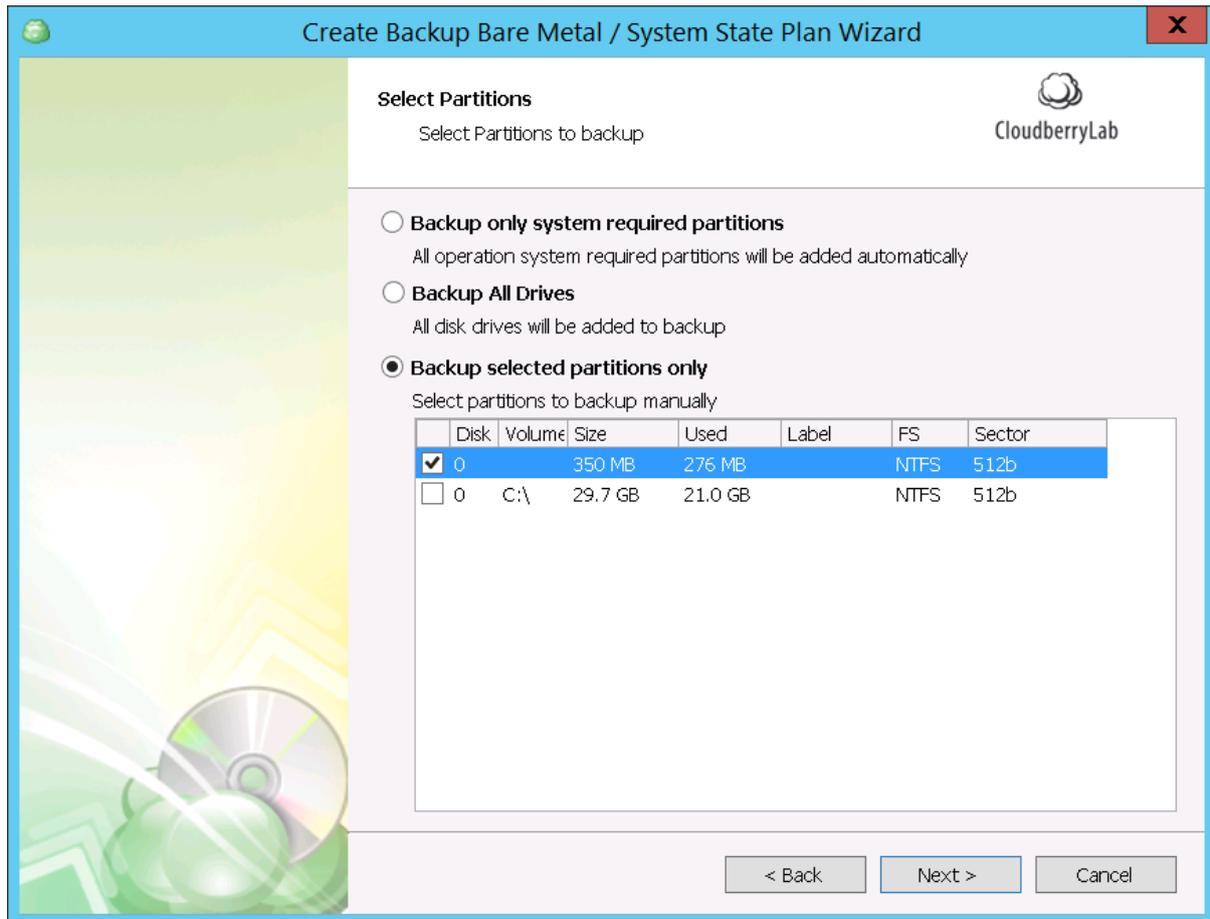
CBB accomplishes images before the upload to the cloud.



System Image Wizard has mostly the same steps as Files Wizard. An important specific option is selecting what partitions will be backed up (all drives, system required partitions or selected ones

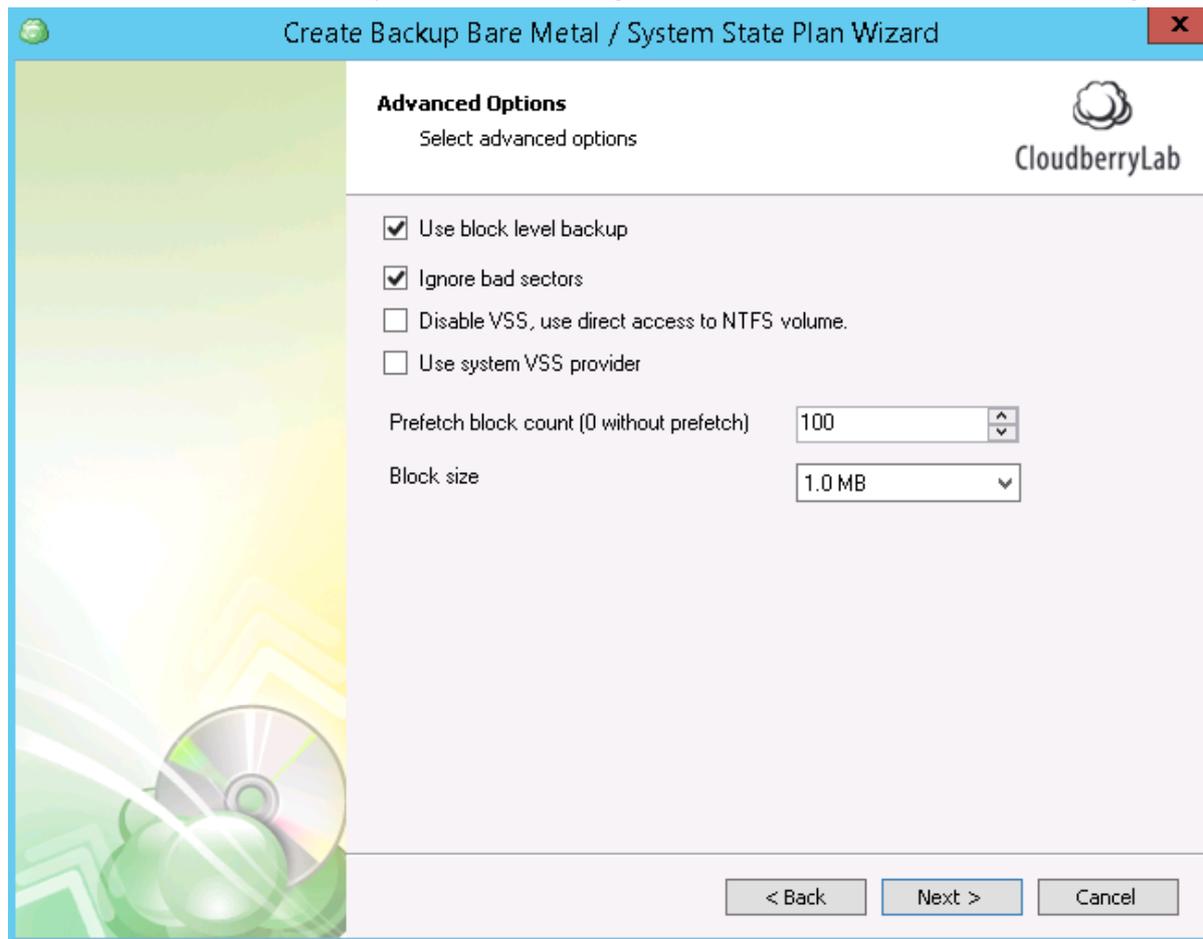


only).



Also, there are several advanced options such as **Ignoring damaged disk** sectors or using direct access to **NTFS partitions**. **Block-Level backup** is available as well, and you can specify custom block size to

make disk space saving even more significant.



Next, you can set up such options as encryption, compression, schedule, full backup schedule (if you've chosen block-level backup), notifications, etc. As always, you will see the summary of all enabled features at the end.

Synthetic Backup

CloudBerry Backup also supports **Synthetic Full Backup**. This enhancement decreases the amount of data upload to the cloud and accelerates the overall process. We are going to explain the technical background and show how to use the new feature.

Block-Level Analysis

CloudBerry Backup (CBB) features block-level backups which contain only modified image blocks which, in turn, decreases the amount of data transferred to the cloud. But avoiding data losses and making recovery faster requires regular full backups, which upload a large amount of data, even if it's already stored in the previous copies. You can read more about this process in [Block vs. Full Backup](#) post.

Synthetic Full Backup (SFB) helps to reduce the amount of data uploaded and accelerates a full backup creation. SFB compares local data blocks with the cloud repository and then uploads only



modified ones. Currently existing blocks in the cloud that haven't been modified since the last full backup or the last synthetic full session are automatically copied to the new backup file by AWS services within the cloud.

In the upshot, Synthetic Full Backup helps to substantially decrease upload volume from the local computer. According to our tests it makes backup process up to 20 times faster (since copying files within the cloud is considerably faster than copying them from the local PC to the cloud). At the moment, the feature sticks to the AWS as it is one of the few systems that allow moving data blocks within the cloud storage. Now we're working on implementing this feature for Azure Blob storage.

If you're using synthetic backup with Amazon S3 Standard-IA storage class, bear in mind one proviso regarding the pricing policy. When you initiate the second full back-up, the principal part of those files will be copied within the cloud itself. And you will be charged accordingly — \$0.01/GB.

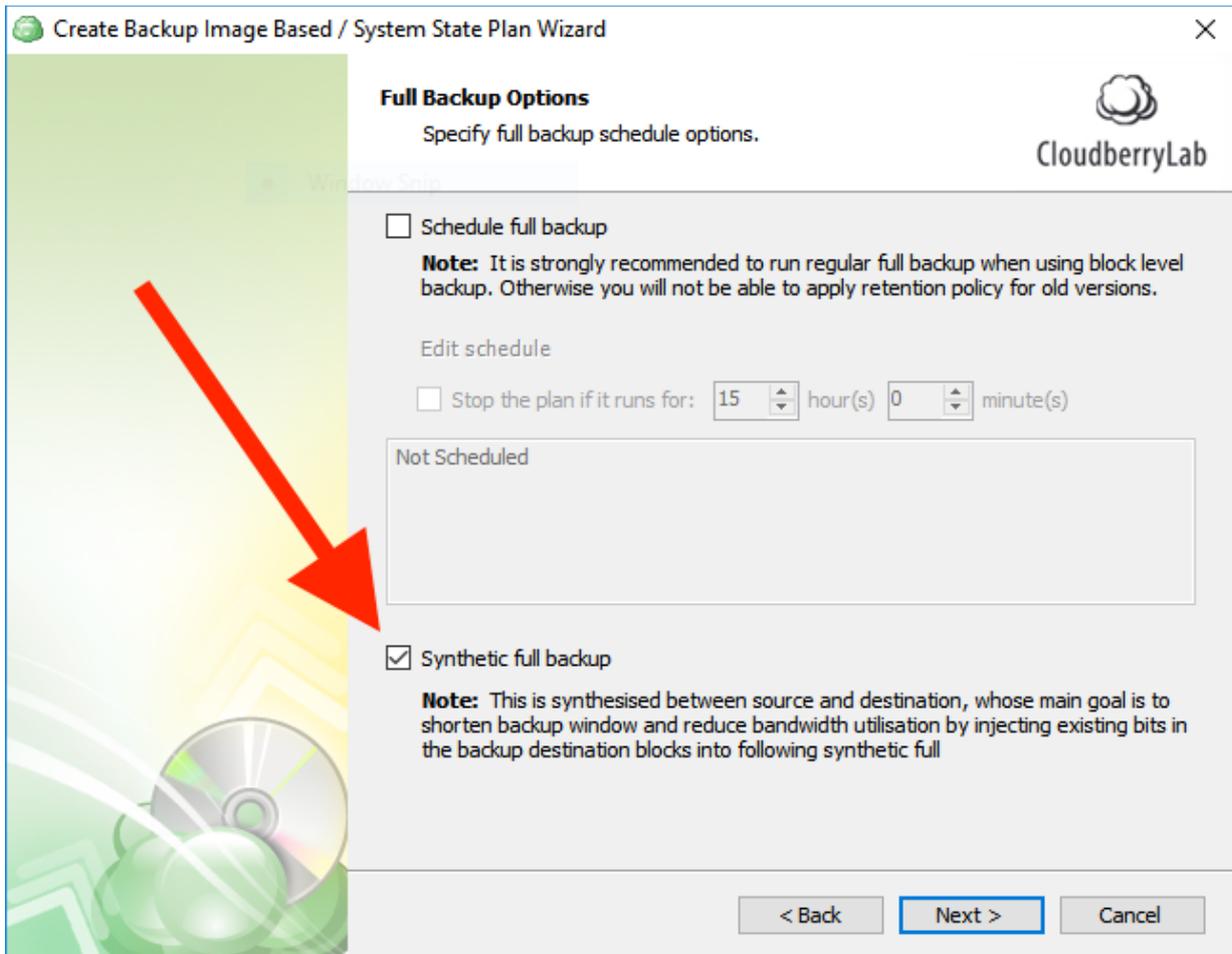
How to Enable Synthetic Backup?

There are some restrictions on using the Synthetic Full Backup:

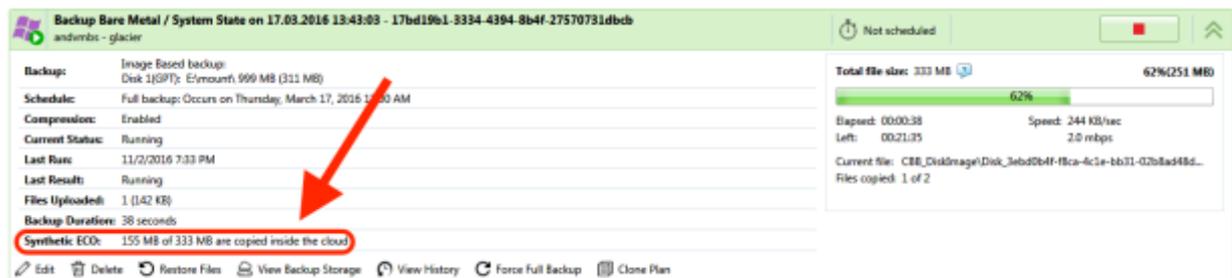
- Amazon S3 must be the target cloud storage.
- Encryption options must remain unchanged since the last full backup.
- One or more full backups have to be made before you activate synthetic backup.

To enable the new feature, create a new image-based plan. Select the **block-level** checkbox when configuring a particular plan. Then select the **Synthetic full backup** checkbox.



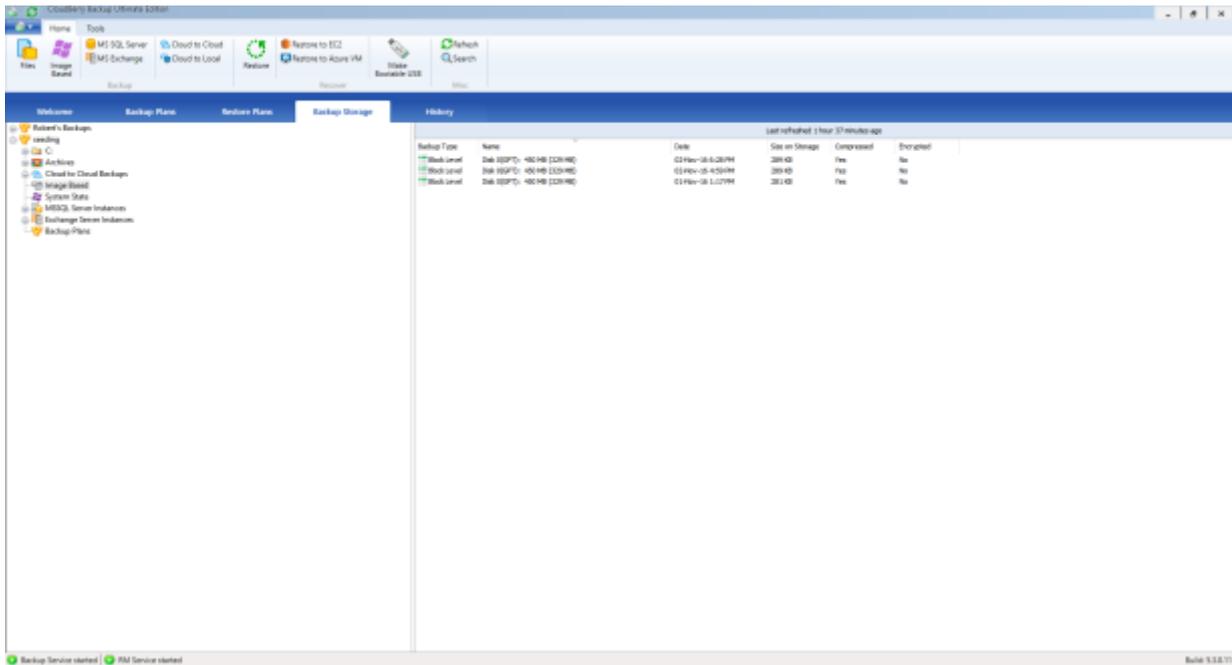


Then, force a full backup from the Backup Plans tab to start using the SFB feature. You can see it working in the Progress Bar.



The synthetic image will display under the **Backup Storage** tab.





CloudBerry Backup identifies synthetic image as a full backup because there is no technical distinction between them so that you can operate them with [CloudBerry Explorer](#), [CloudBerry Drive](#) or other third-party apps.

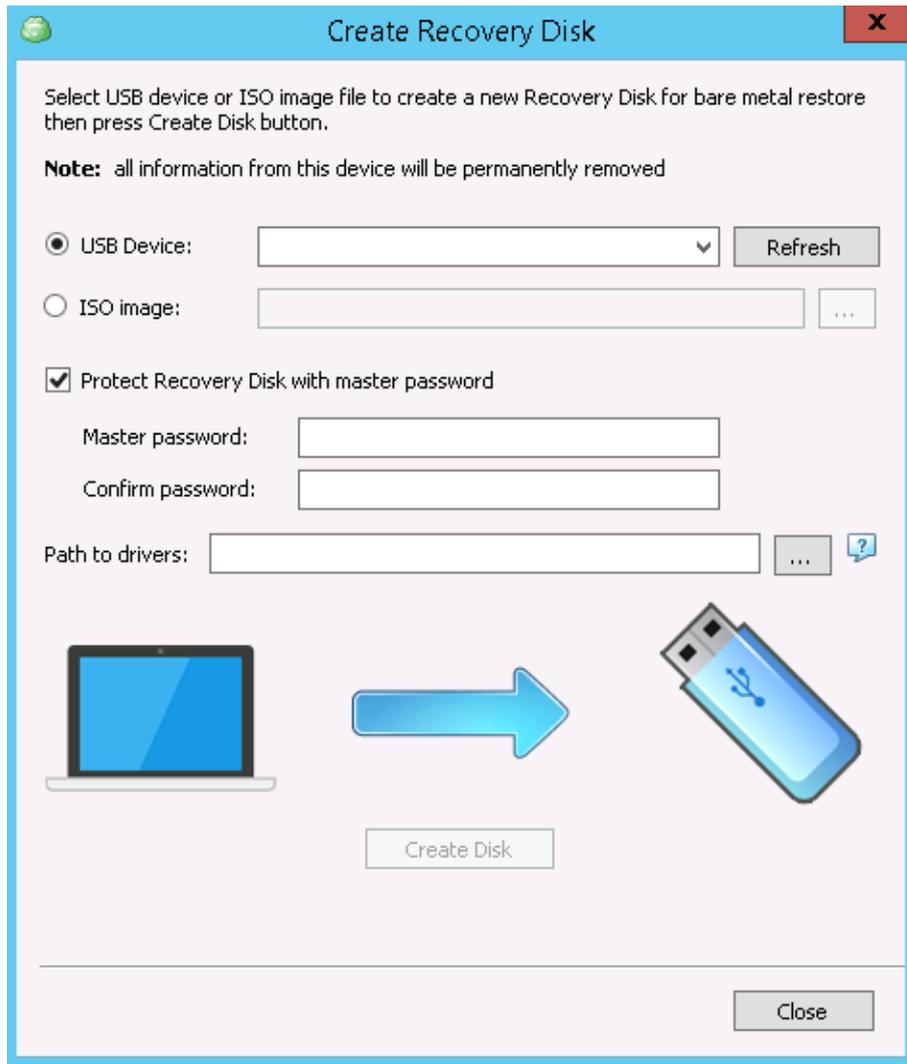
Note that using this feature makes sense only if the source partition is larger than 100MB.

Bootable USB Creation

With CloudBerry Backup it is possible to create a recovery disk, which can fix the system in case of a critical error, outage or to move the system to another device. As an option, it can create an ISO image to deploy the recovery data on other storage facilities such as optical disks, Storage Area Network devices, etc.

Click on **Make bootable USB** button on **Home** tab and select an option to create a bare metal restoration disk. You can also protect the drive with a password.





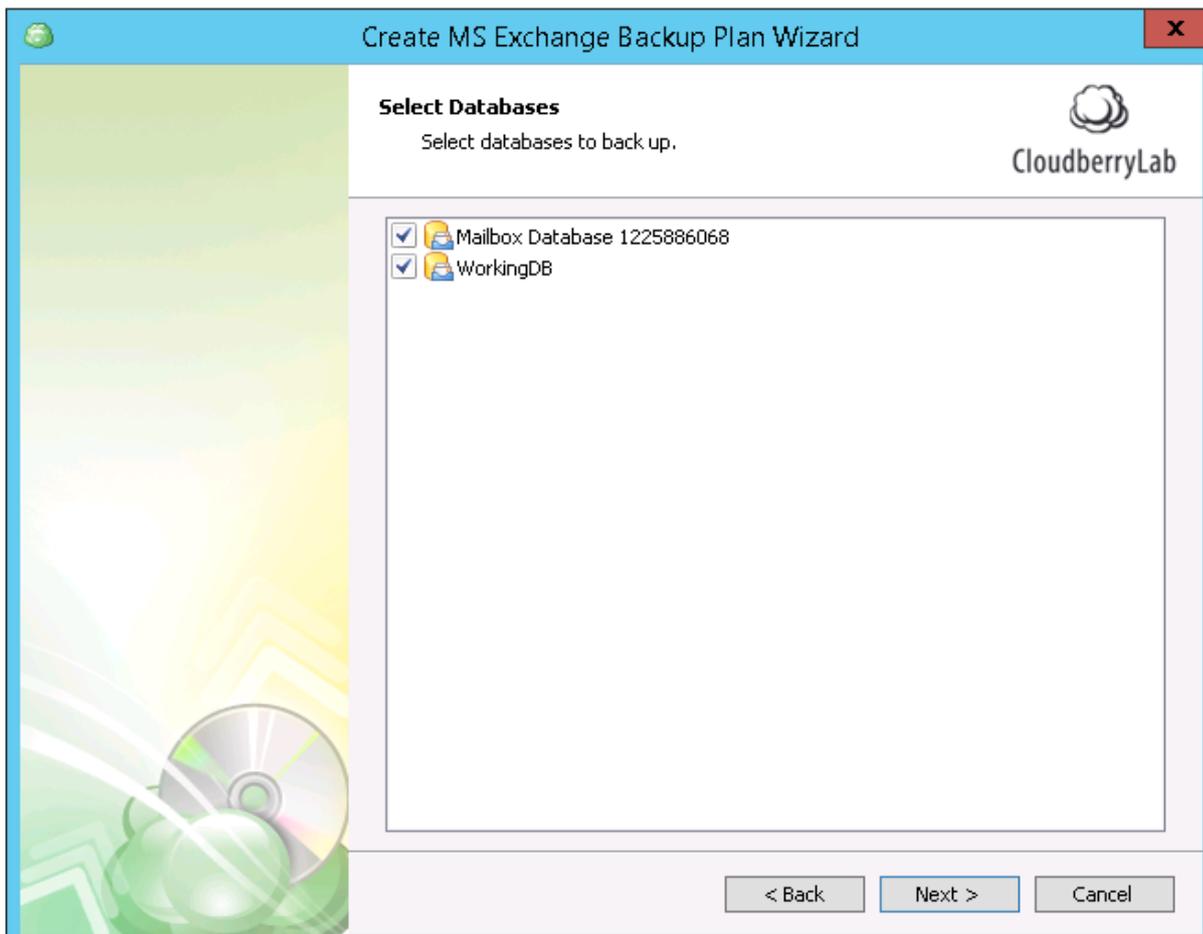
Microsoft Exchange Backup

Main structural units of Microsoft Exchange is **EDB-files and logs**, which contain all user data like emails, contacts, calendars, etc. File level backup is too clumsy here because it needs accurate option adjustment, and image-based takes too much storage place. To facilitate Exchange server maintenance, we designed particular backup technique.

Use Exchange Backup Wizard to create a separate backup of a Microsoft Exchange server. It starts by pressing **Microsoft Exchange** button on the **Home** tab, or picking **Backup Microsoft Exchange** on **Welcome** tab.

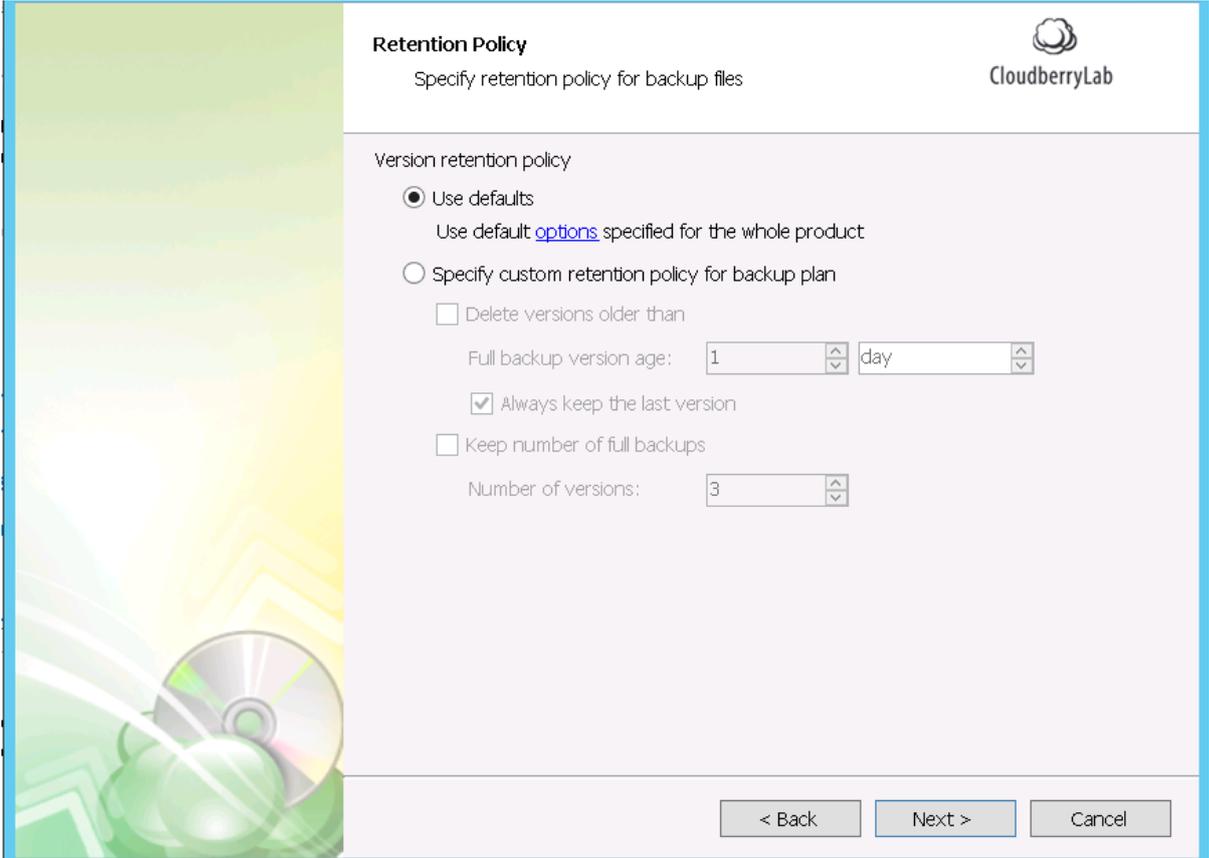


1. After choosing the storage account and specifying plan name, you have to select databases for backup.



2. During the next steps, you can enable encryption, compression, scheduling, and configure **Retention Policy**. In essence, it is similar to retention policy of file or image-level backup. CBB creates a version of the file on each time it is modified, thus limiting an amount of versions to

be kept for one file. This helps to avoid backup size overflow.



The screenshot shows the 'Retention Policy' configuration window in CloudBerry Backup. The window title is 'Retention Policy' and it includes the CloudBerryLab logo. Below the title, it says 'Specify retention policy for backup files'. The main section is 'Version retention policy' and contains the following options:

- Use defaults
Use default [options](#) specified for the whole product
- Specify custom retention policy for backup plan
 - Delete versions older than
 - Full backup version age: 1 day
 - Always keep the last version
 - Keep number of full backups
 - Number of versions: 3

At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'.

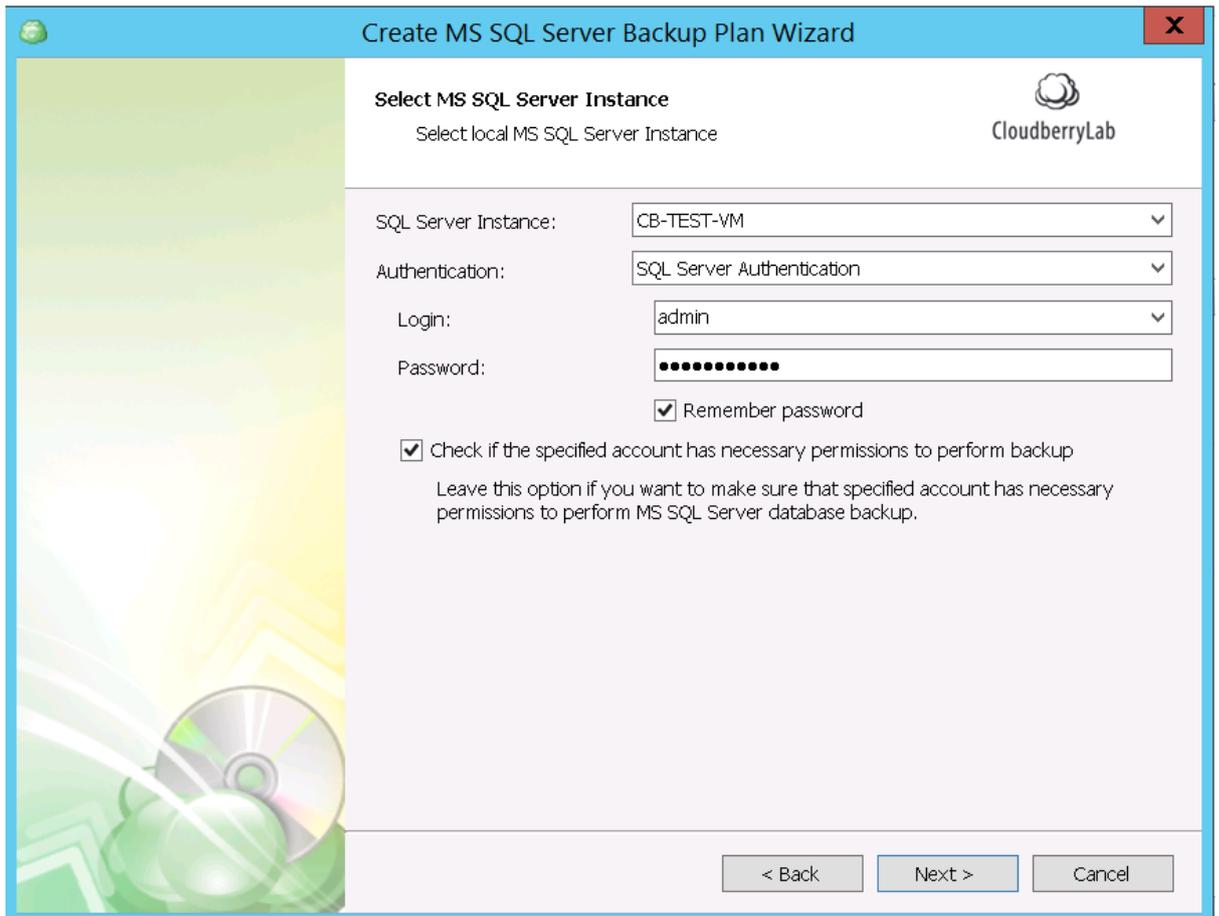
3. Then, you need to specify the **Schedules** of full and incremental backups. It works same as for block-level backup – to recover the database, you need to restore the latest full backup and then update it with the modified files.
4. Finally, it is necessary to set up the notifications and pre-post actions. The list of enabled functions displays at the final step.

Microsoft SQL Server Backup

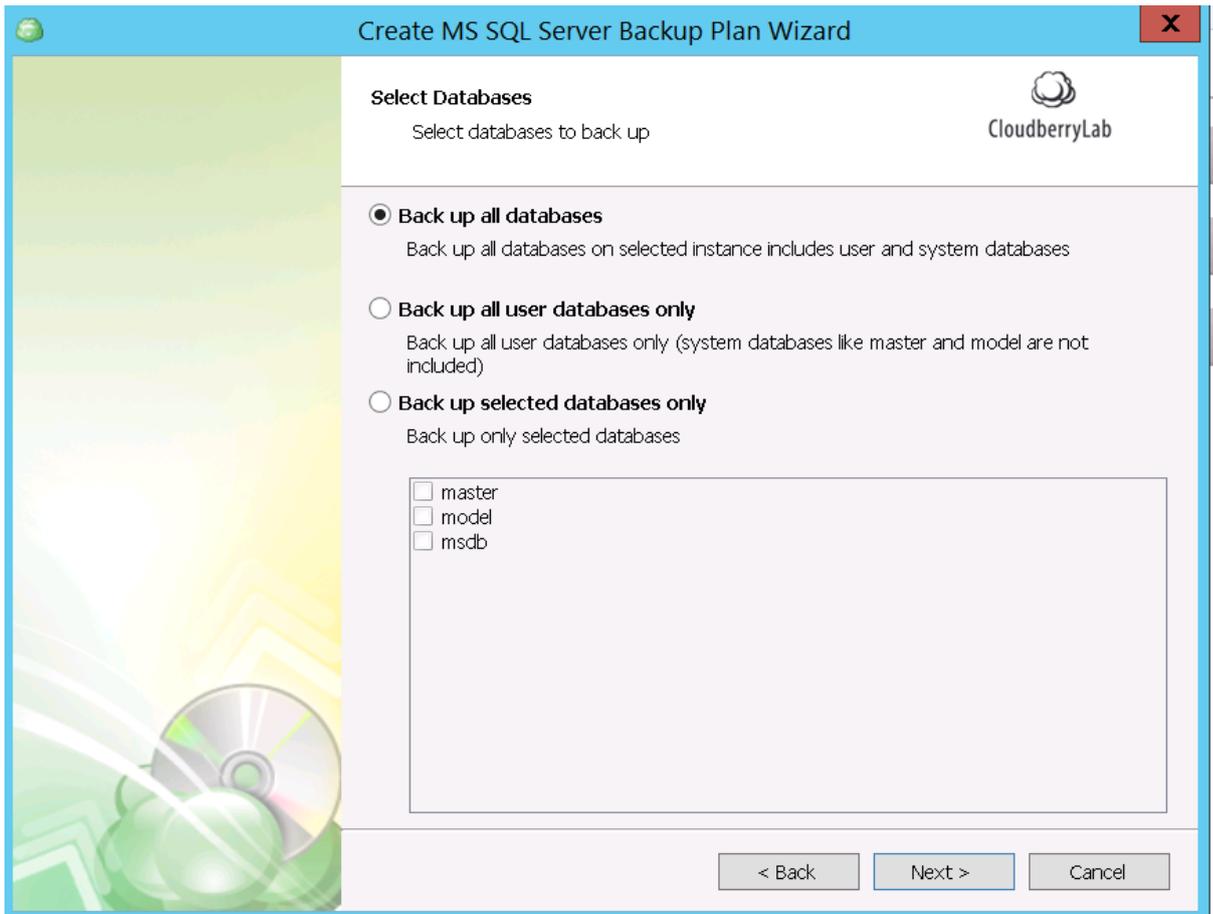
If you need to backup Microsoft SQL databases separately, CloudBerry Backup can easily cope with this task. CBB can use any of the authorization methods available and create a backup only of chosen database elements.

Activate Backup Plan Wizard by clicking on **Microsoft SQL Server** button on **Home** tab, or by selecting **Backup Microsoft SQL Server** on the **Welcome** tab.

1. Specify the backup plan name, and then select which **SQL instance to backup** and **authentication method** for CBB to access server. You can also check whether selected SQL login has **sysadmin** role, which is necessary for full-fledged backup.



2. Then select databases for backup.

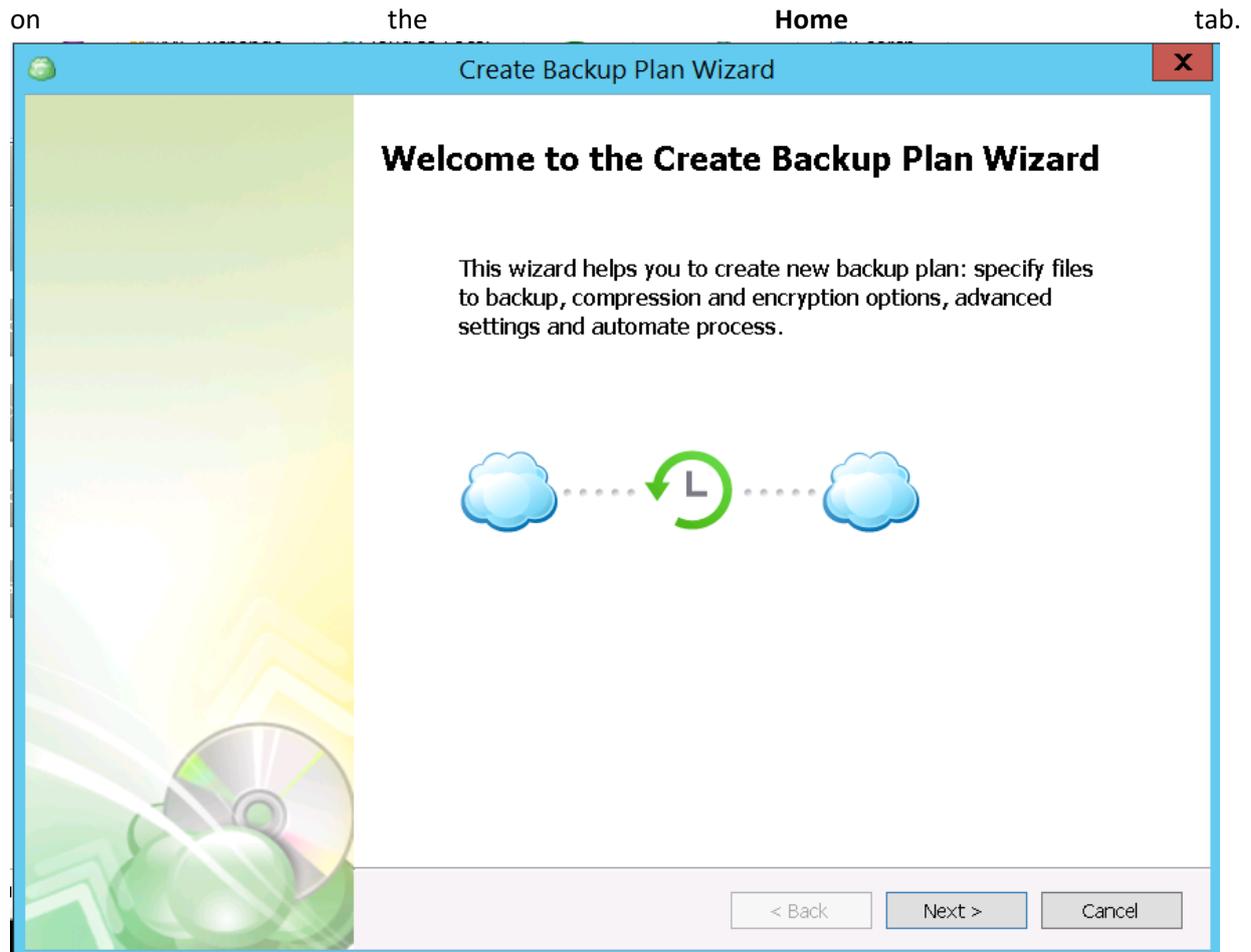


3. Finally, you set up the rest of the options: retention policy of database versions, email notifications, maintenance schedule, etc. All features enabled will display on the **Summary** screen.

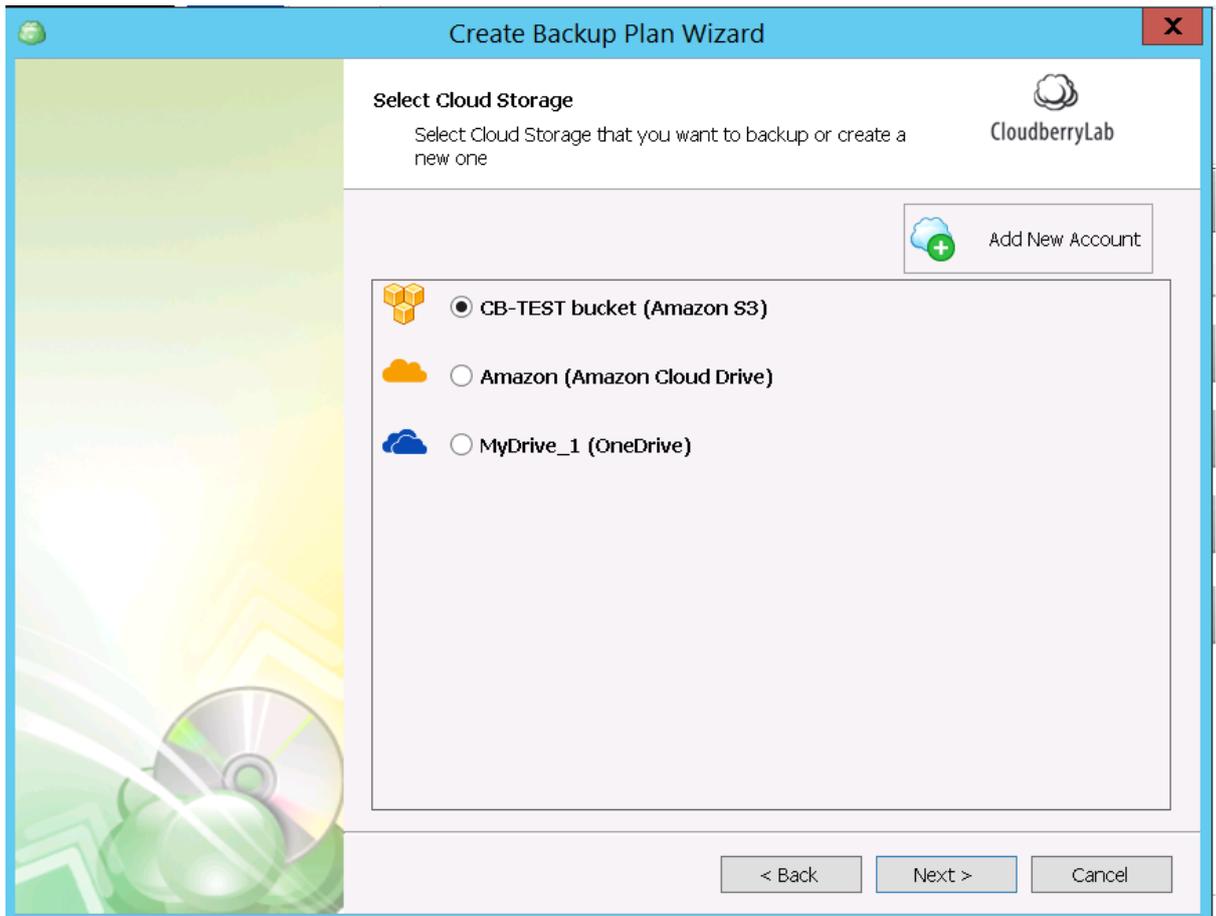
Cloud to Cloud Backup

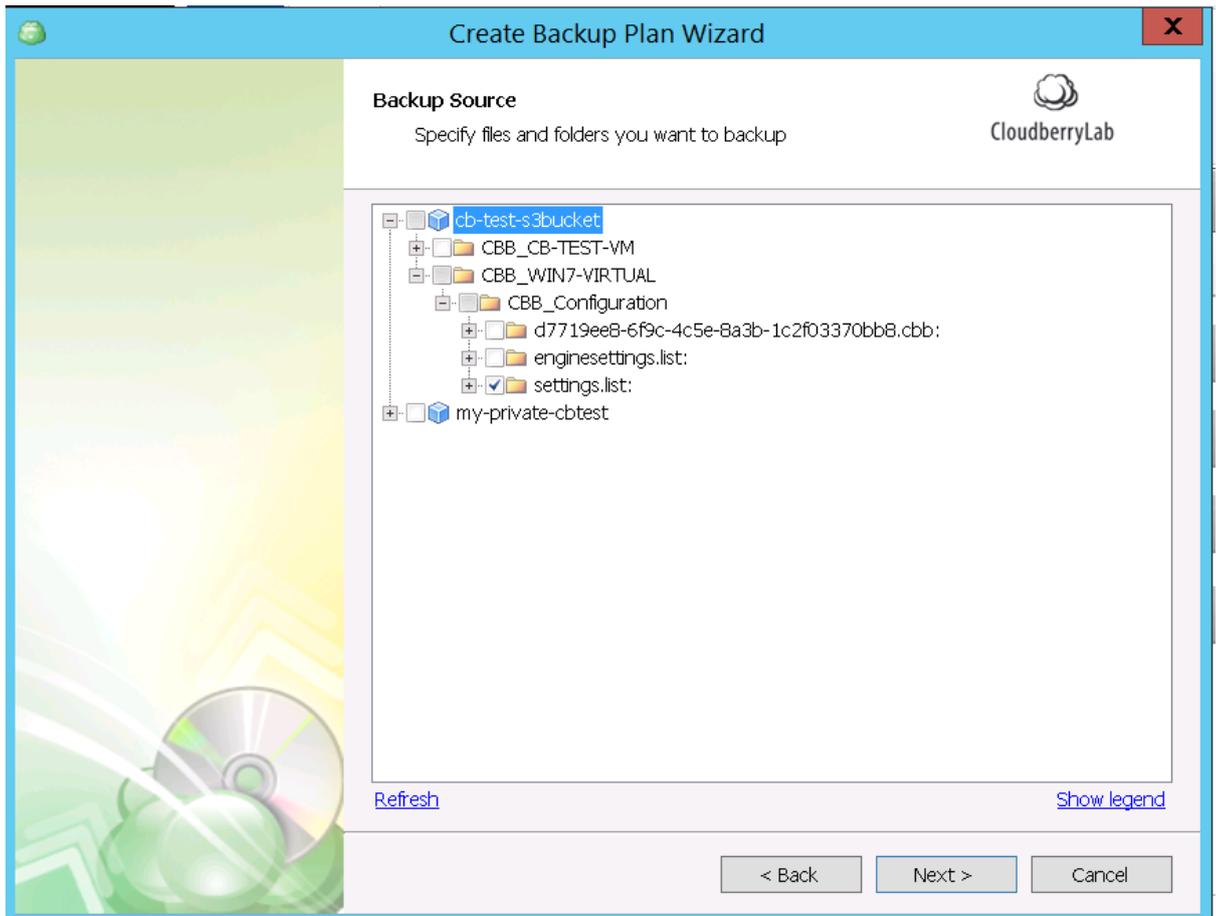
CBB can backup your data stored on the cloud storage, or increase durability of the offsite-stored backups with Cloud to Cloud Backup Plan Wizard, which accessible under the **Cloud to Cloud** button



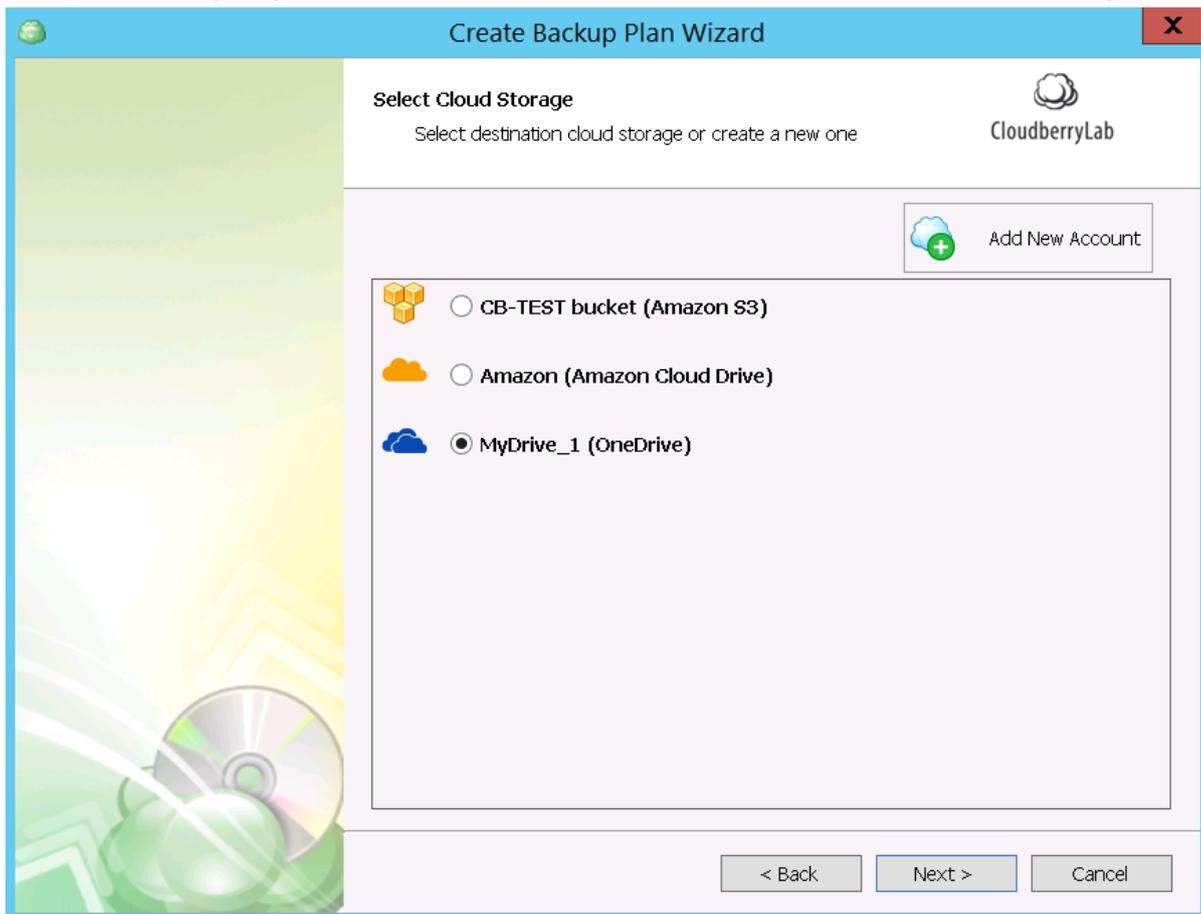


1. First, **Select Cloud Storage** and the exact buckets, folders, and files to be backed up.

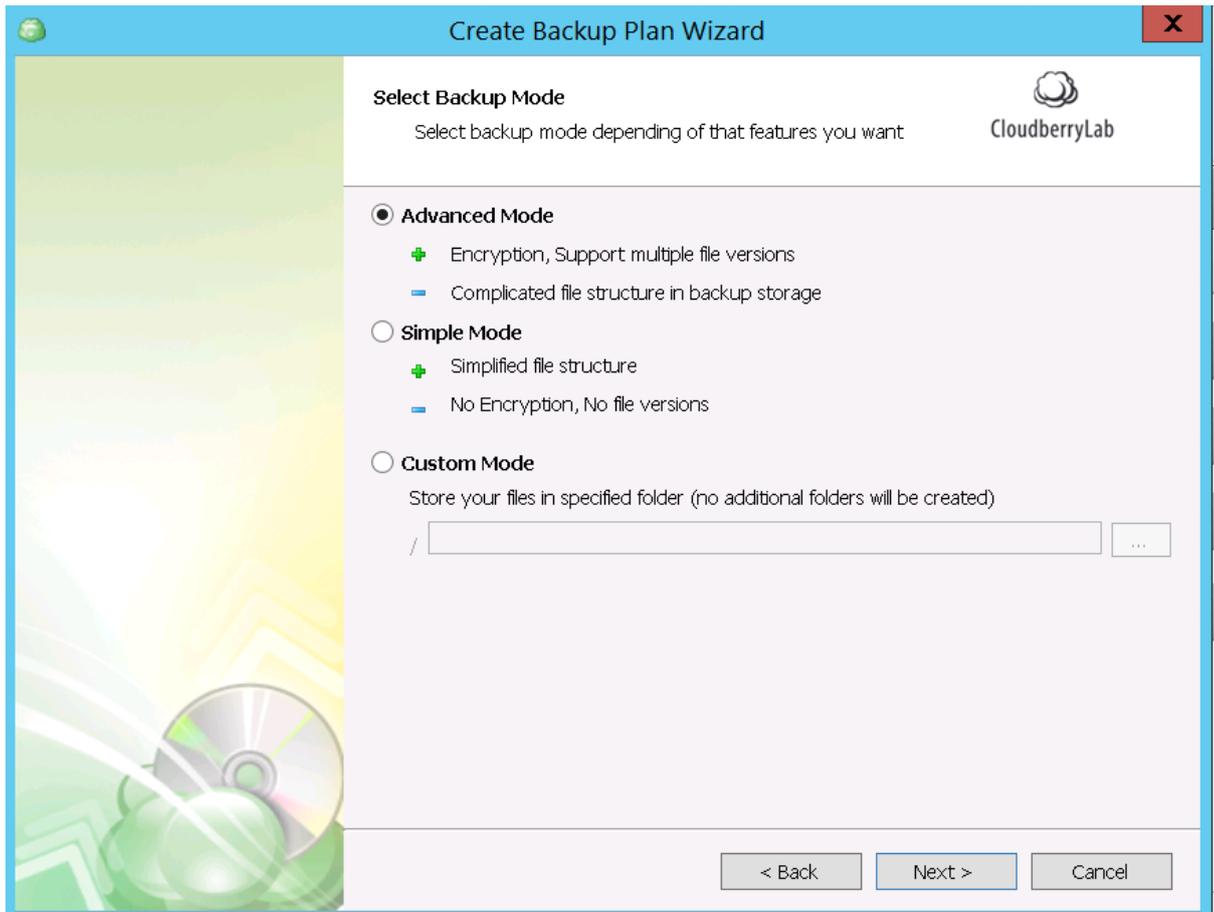




2. Then, specify the destination cloud storage.



- Next, choose a name for the newly created backup plan and select **Backup Mode**.



- Depending on previous step's presets, configure file filter options, encryption, compression, retention policy for file versions, schedule, etc.

Note: encryption and compression may be not supported on the destination storage.

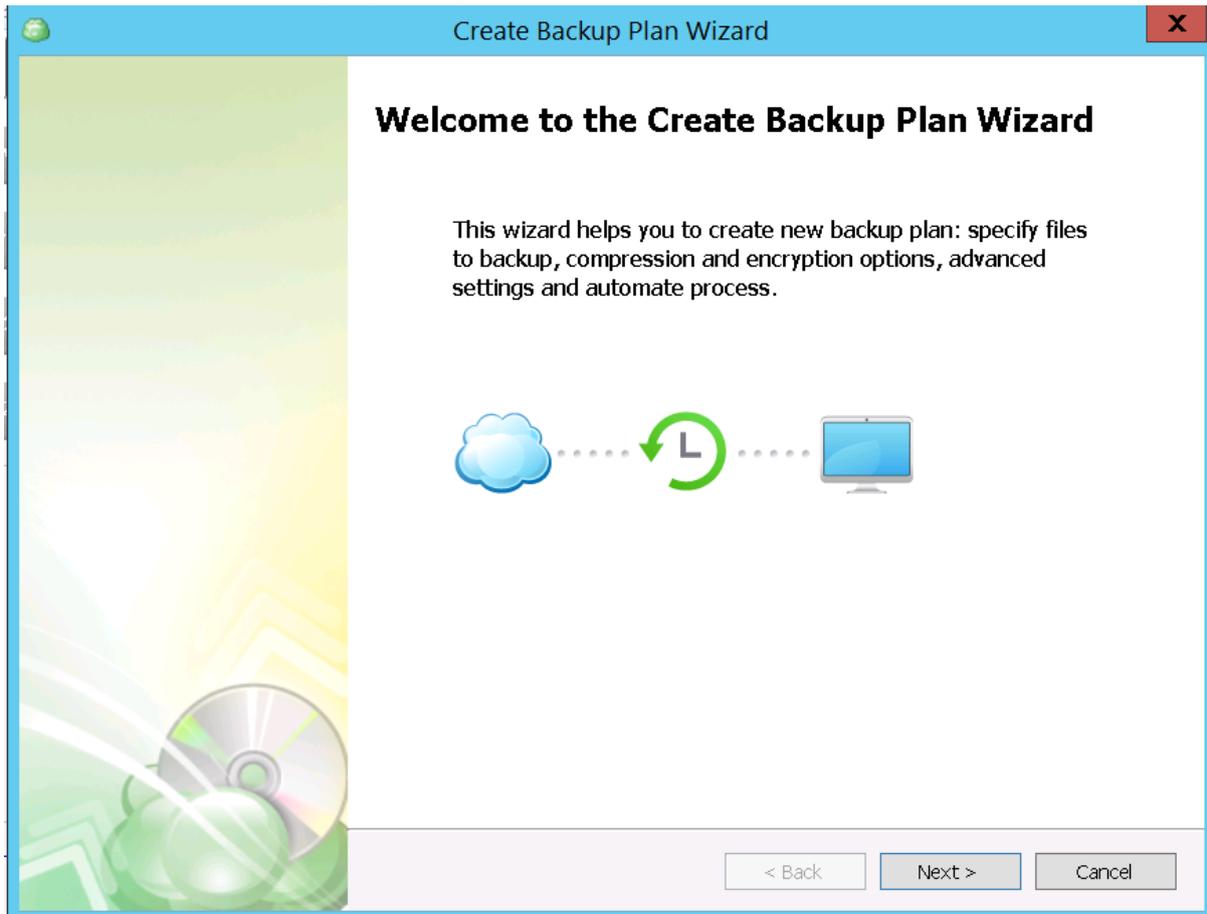
- On the final screen, you'll see the list of the options enabled.

Cloud to Local Backup

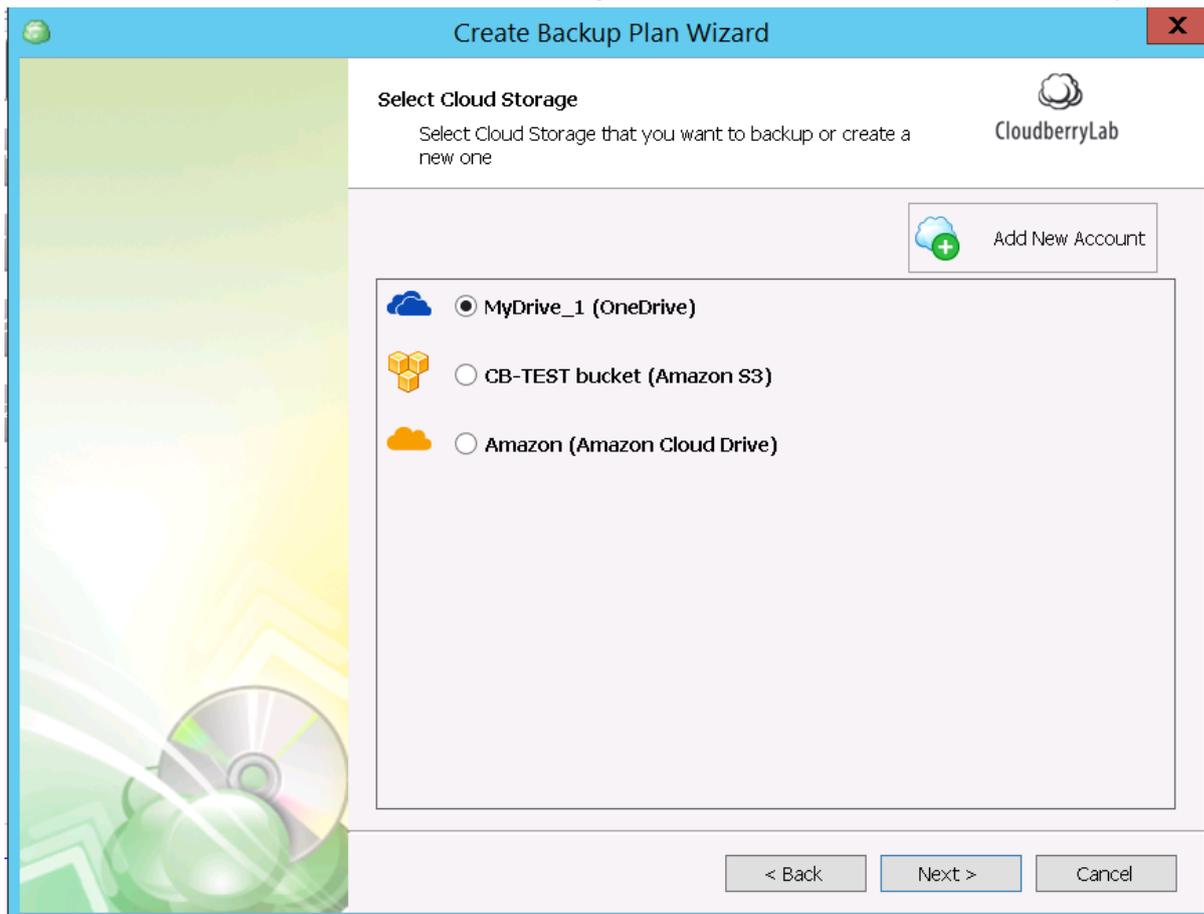
As a rule, local storage facilities are backed up to the cloud, but it's possible to do inversely and save on additional copies maintenance. It may also be a part of the data lifecycle when outdated files move on a low-cost storage facility. To help you with cloud to local backup, CBB has a special tool aboard.

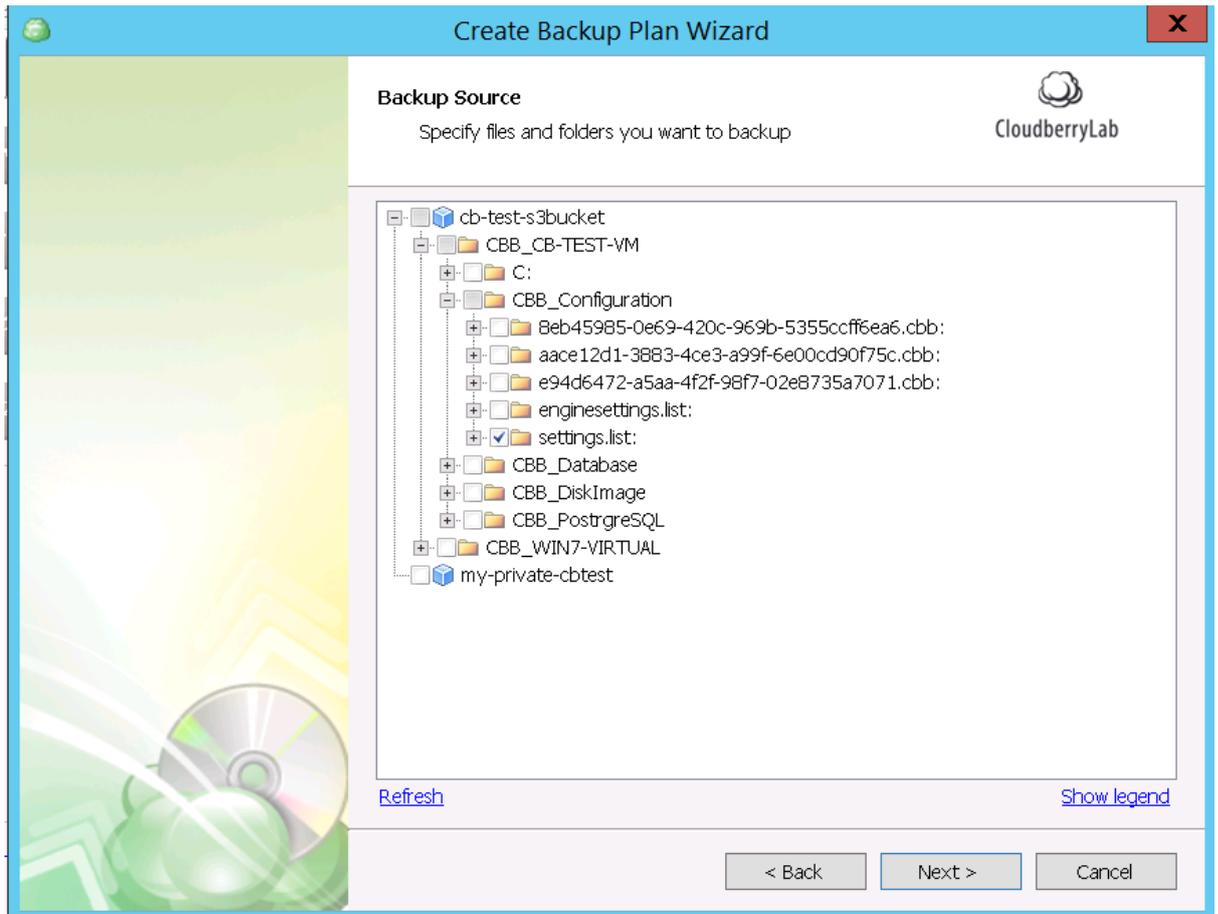


The Wizard starts by pressing on **Cloud to Local** button at the **Home** tab.

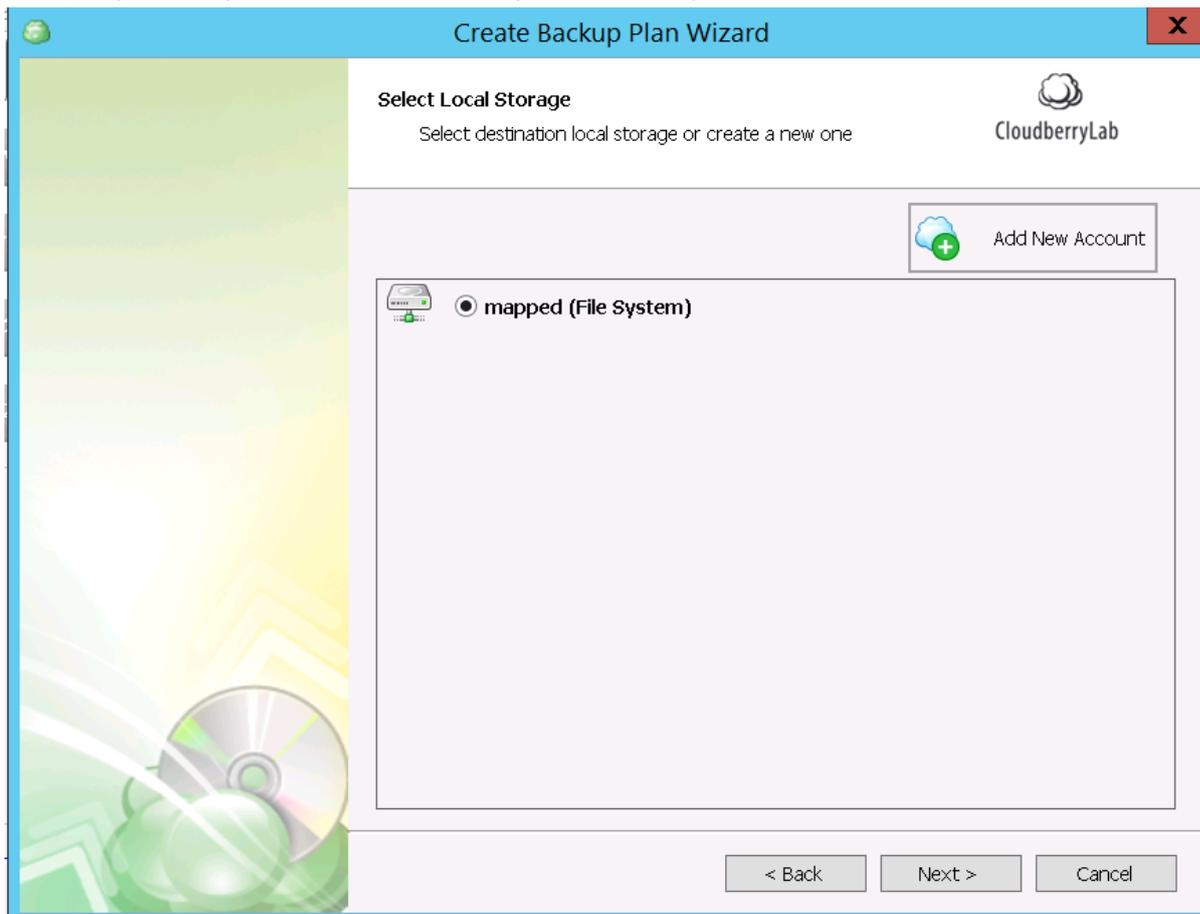


1. First, select the cloud storage and files for backup.





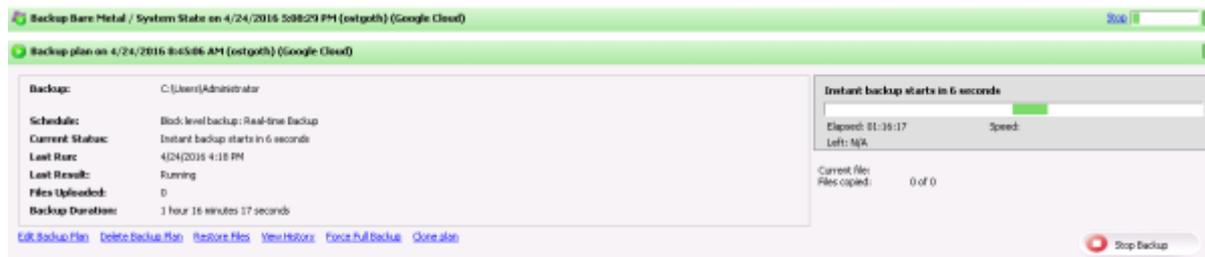
- Then, **pick up the local endpoint** facility or create a new one.



- Finally, configure the routine backup plan options like file filter, encryption, schedule, etc. The summary of all features enabled displays at the final screen of the Wizard. New Cloud to Local plan will function as the file-level backup.

Backup Plans Management

You can access all created backup plans at the **Backup Plans** tab.



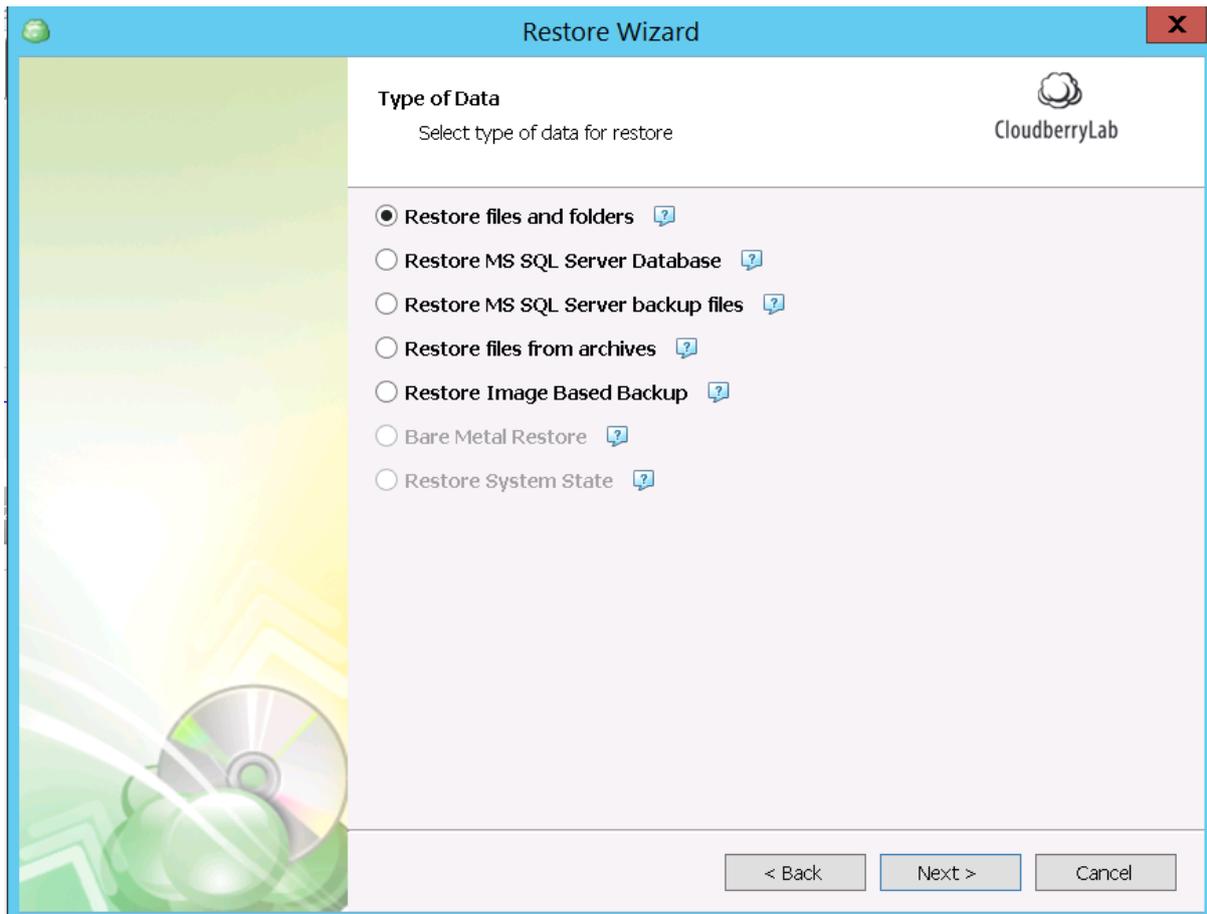
Click the green field to view a plan's details, check its progress, view history, edit or delete. You can also turn off/on backup schedule.



How to Restore

The **Restore** options provide the following data recovery services:

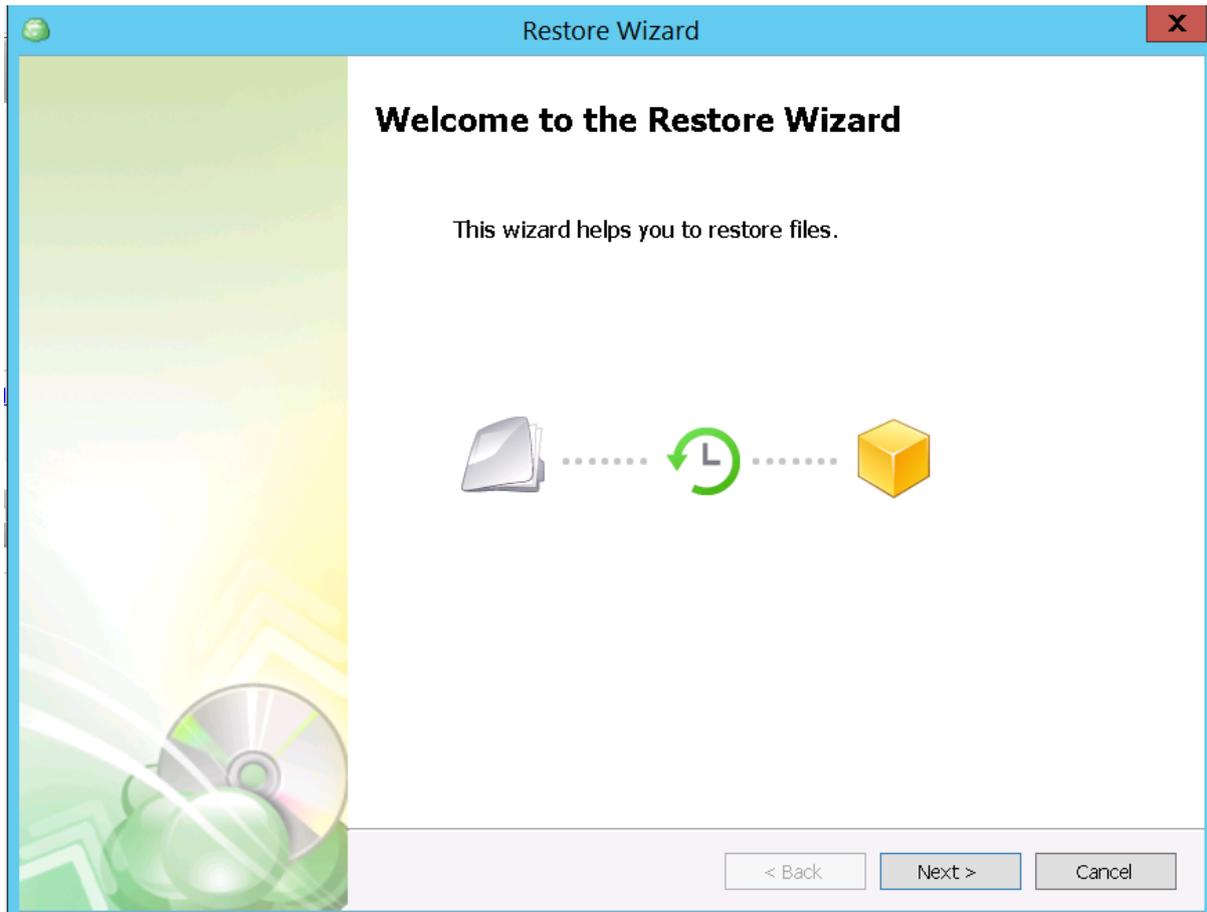
- **Files** – recovers separate files and folders.
- **Image and System State** – deploys system recovery kit on the local storage.
- **Cloud VM** – deploys a server image as Azure VM or Amazon EC2 instance (Google CE is coming soon).
- **Microsoft SQL Server** – recovers database files.
- **Microsoft Exchange Server** – restores Exchange data and logs.



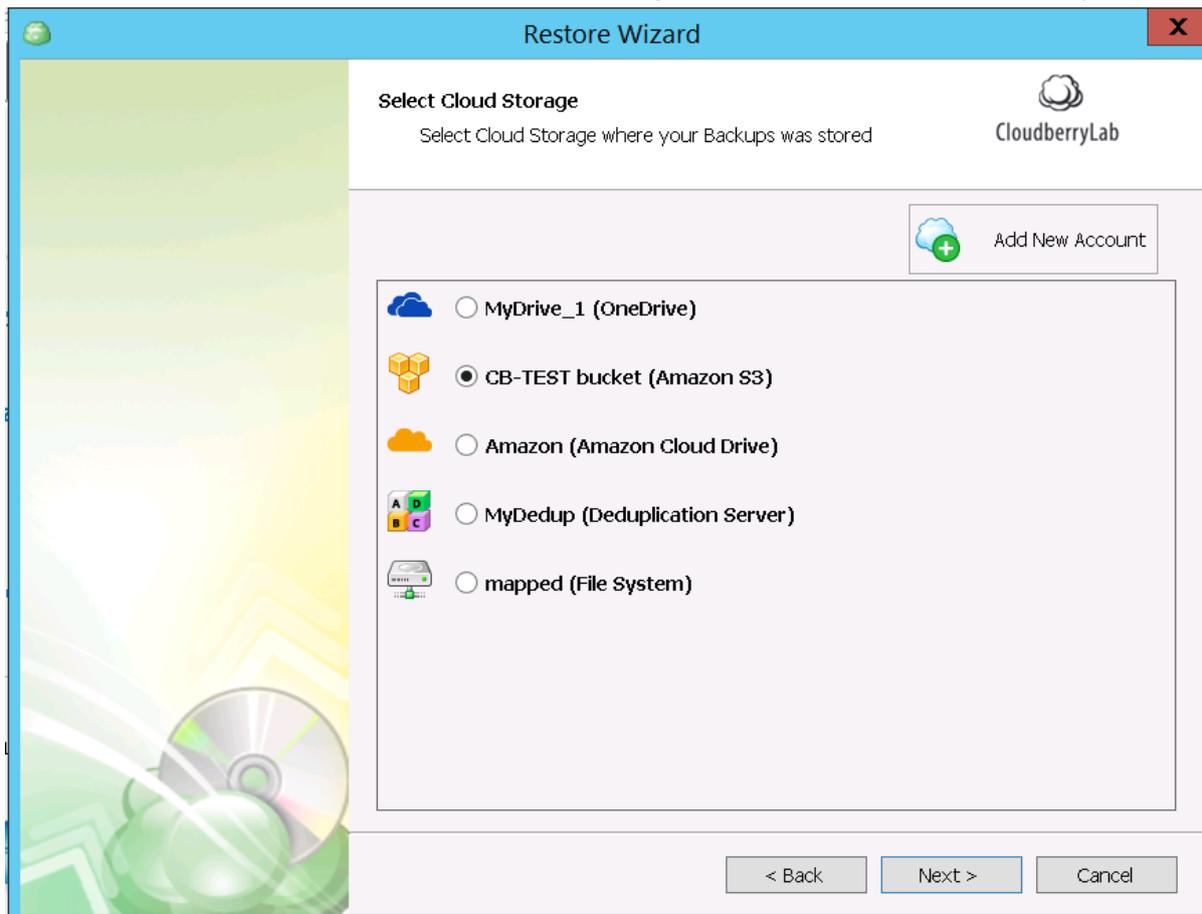
These options can be managed within the **Restore Wizard**. It starts by pressing the **Restore** button at the Home tab, or by picking **Restore Backup** at the **Welcome** tab.



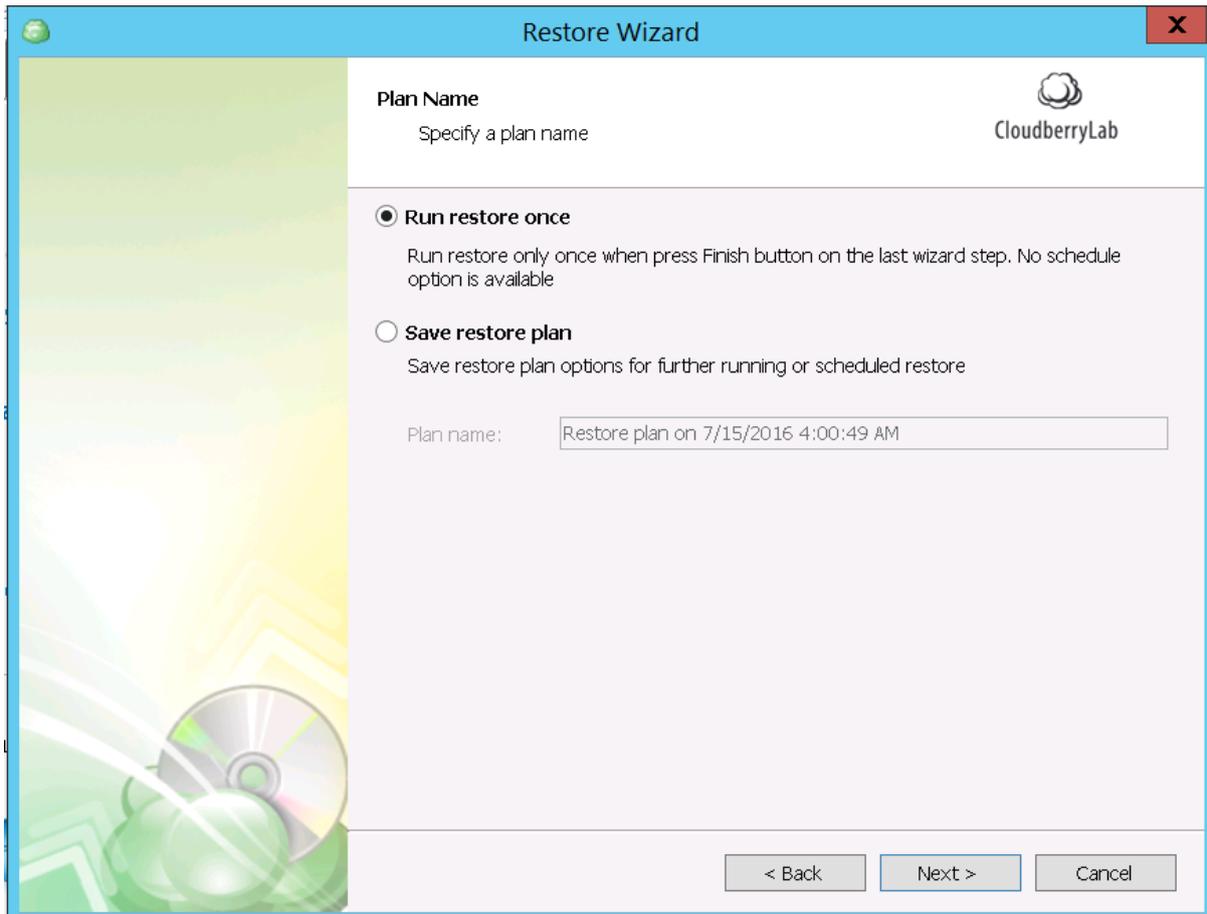
Note: CloudBerry Backup provide any kind of recovery for free – you don't need to activate a license or sign up for trial to retrieve the data.



After the Wizard started, choose the storage where the needed backups located.



Next, decide whether restore data once or save restore plan to schedule recovery.



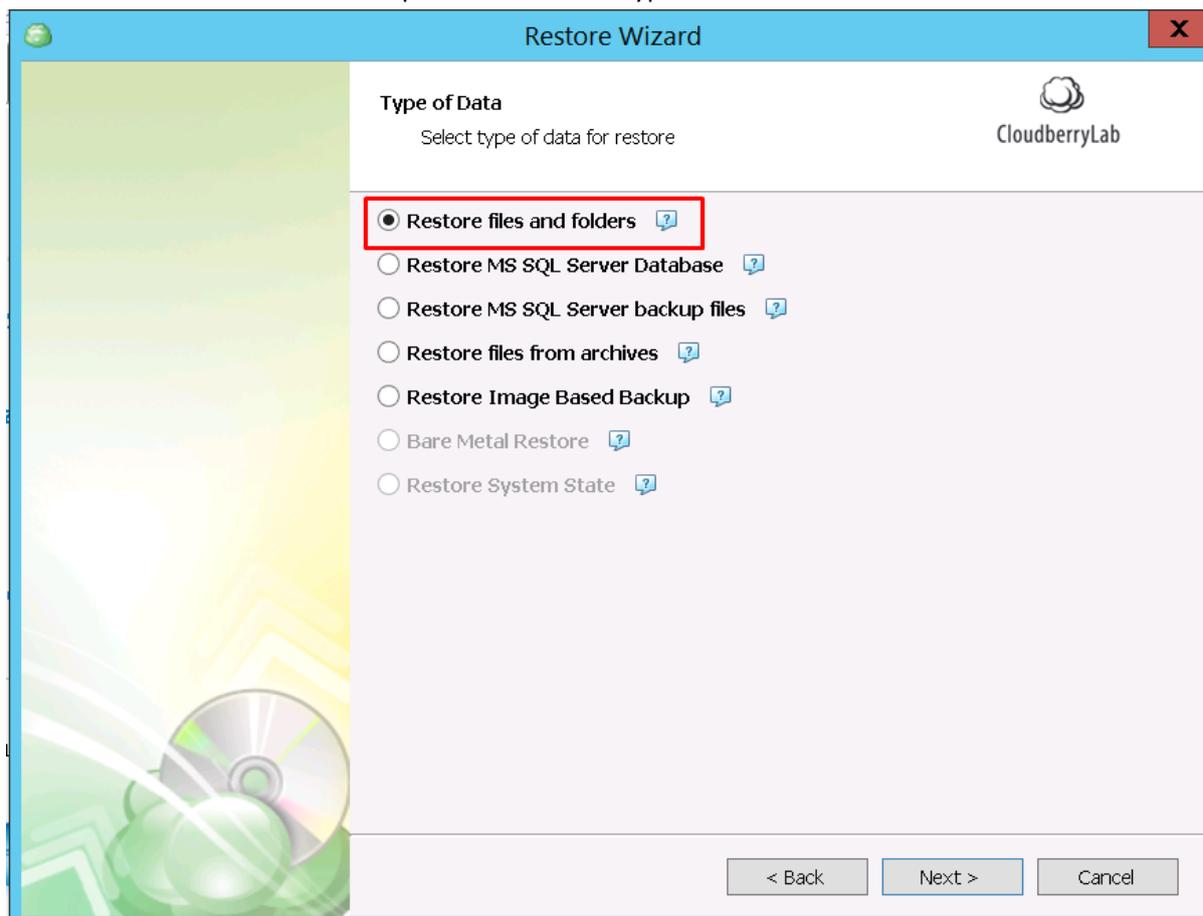
Finally, select a type of data to recover, and the Wizard will guide you through all the required steps for successful data restoration.

File-level Restore

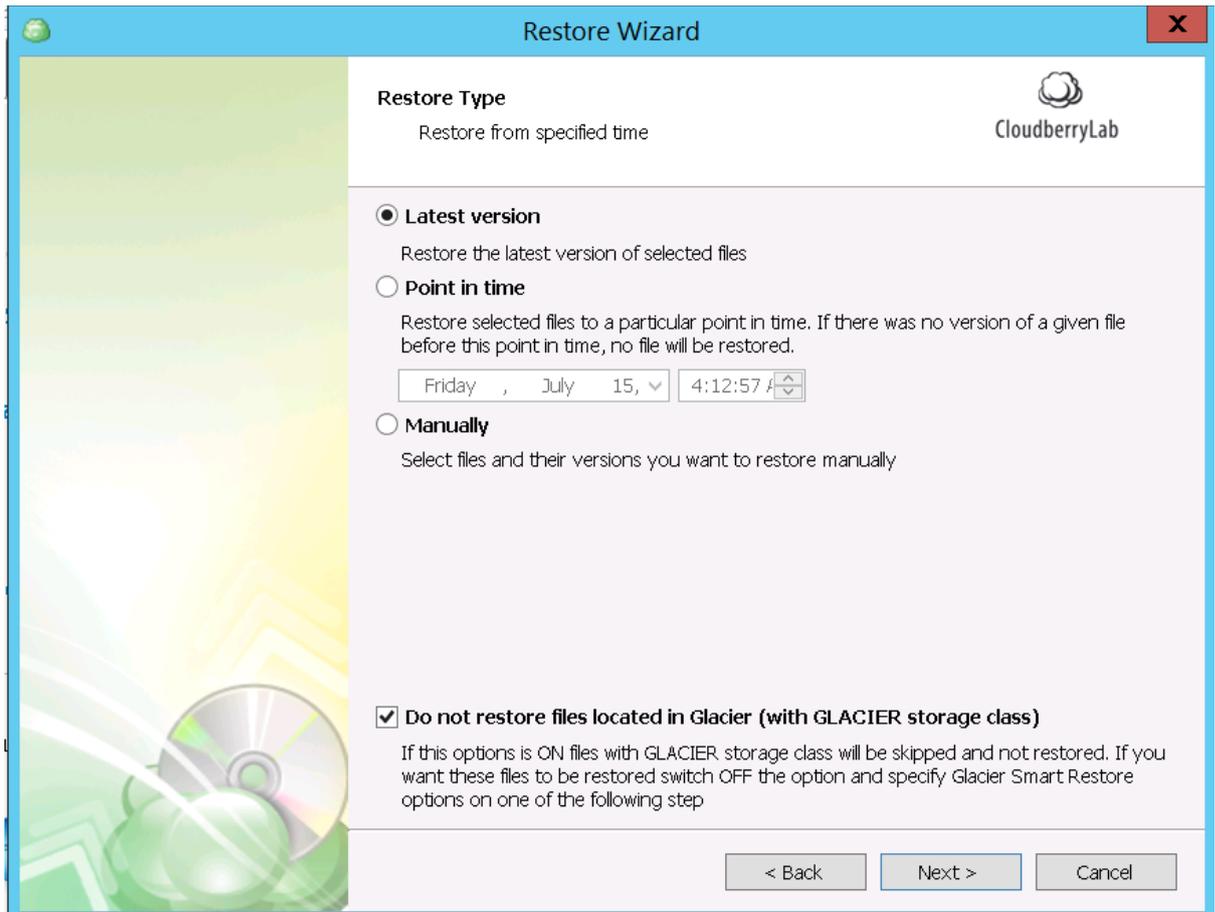
File recovery is commonly used to retrieve working data and restore particular elements of system and applications, e.g. configurations files, registry elements, etc. To start file-level recovery, select



Restore files and folders option on the type of data screen of Restore Wizard.

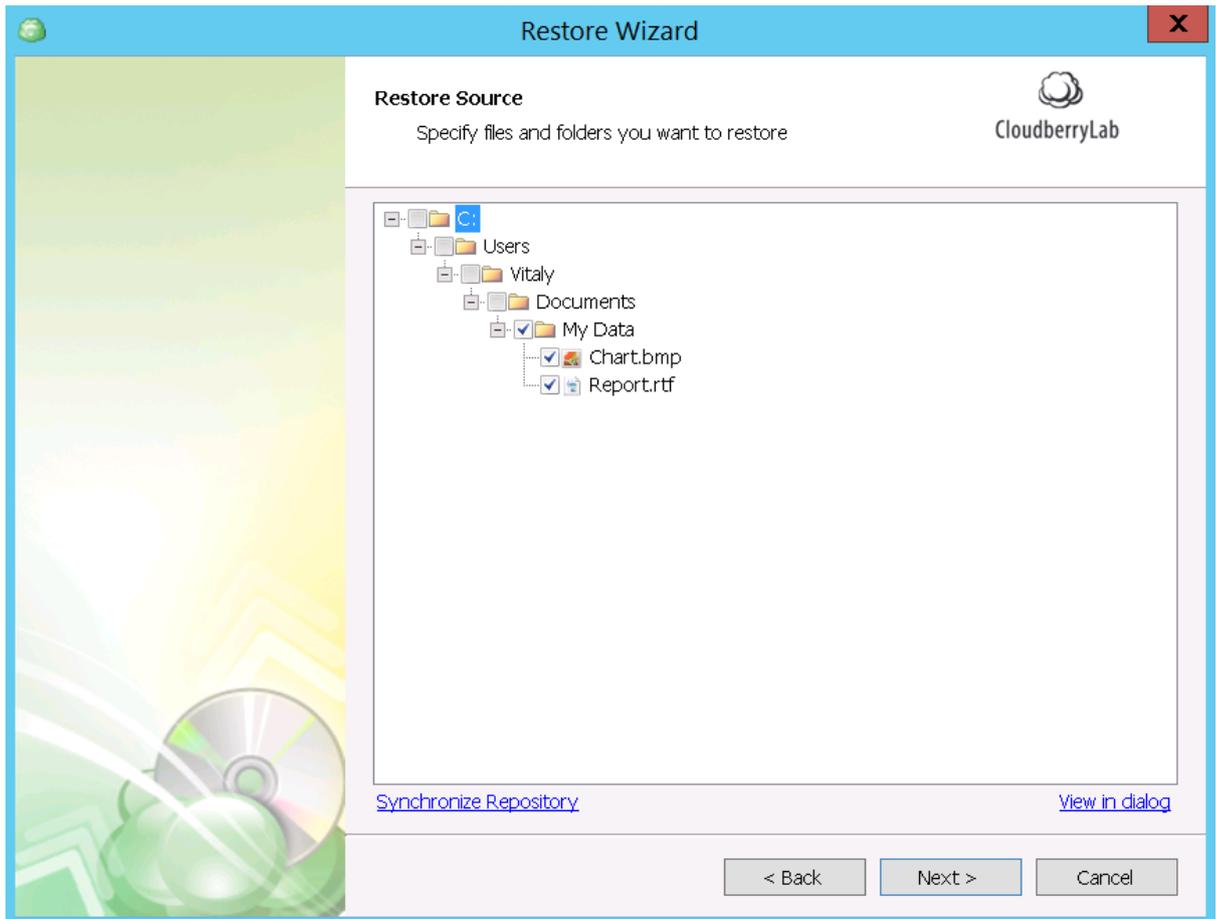


1. At the beginning, select the version of the data to recover. The **Latest version** will recover the last backup made, **Point in time** will restore the nearest backup version before specified time, and with **Manually** option you can choose the version for each file or folder separately.



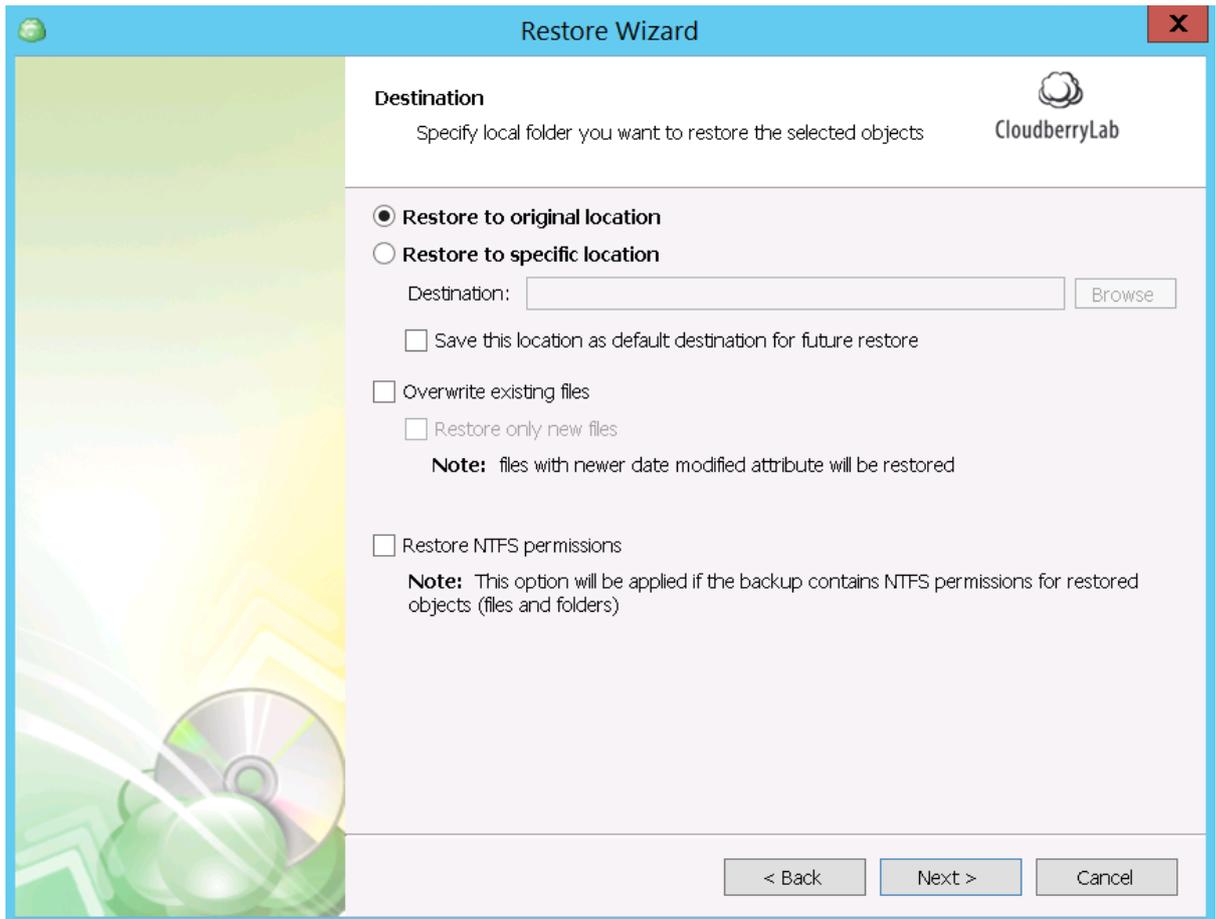
Do not restore files located in Glacier option will prevent unexpected expenses on files, which are placed to AWS Glacier according to lifecycle policies. Find out more in **Advanced Solutions – Archive to Glacier and Lifecycle Policies** section.

2. On the **Restore Source** step, specify exact files for recovery.



If the storage contents might have changed since the last backup, use **Synchronize Repository** option to update the CBB backup database. This feature explained in **How to Backup – CloudBerry Backup Configuration – Repository** section of this document.

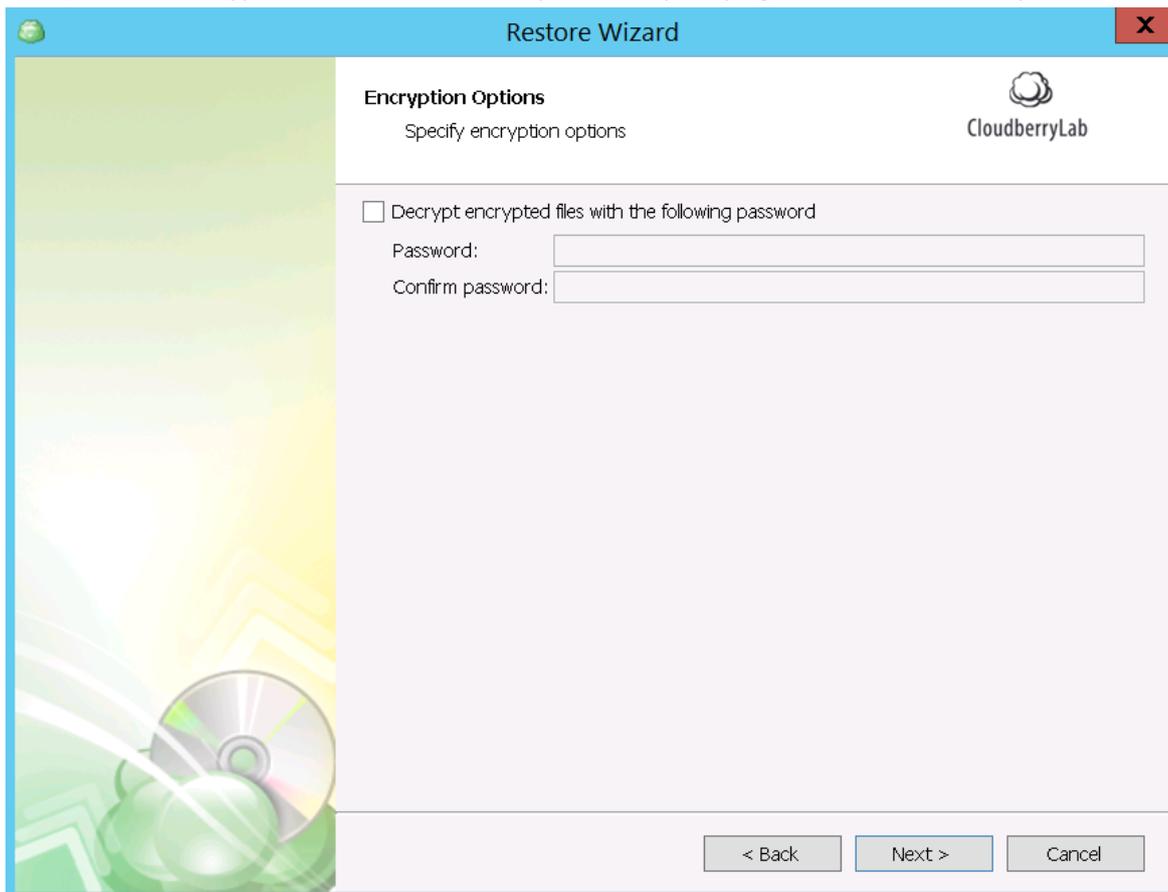
3. Next select recovery **Destination** and its options.



By default, data is restored to the original location, though you can download it to another folder, overwrite files with coinciding names and restore NTFS permissions (if they were backed up before).

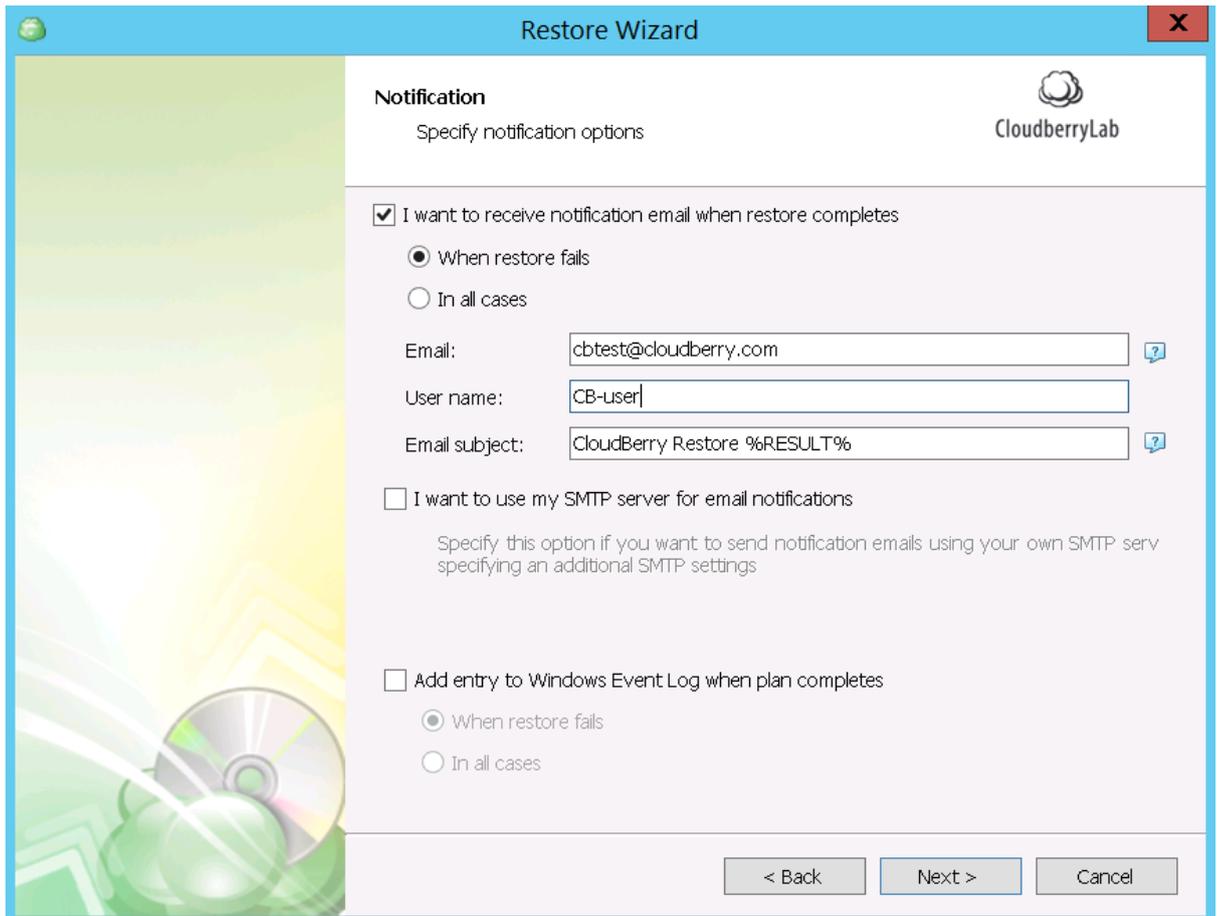


4. Then, decrypt files by specifying the password.



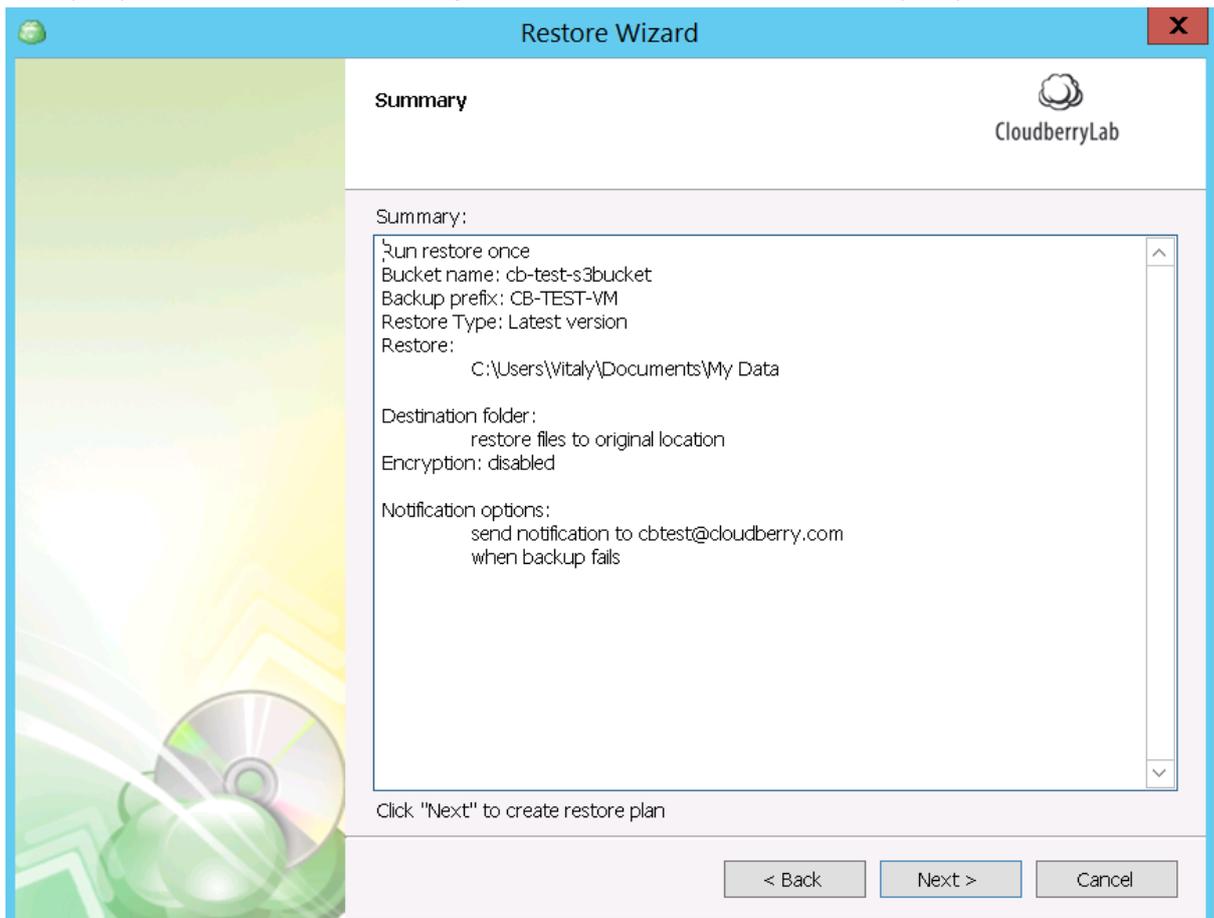
If the data is ciphered, but the password isn't fed into, CloudBerry Backup will download encrypted files for manual decryption.

5. On the next step, configure **Notification** settings. CBB can inform you about recovery status via email and add the corresponding entry to the Windows Events.



One can also use own SMTP server for notifications instead of built-in CBB service.

6. Finally, you'll see the **Summary** screen with all the recovery option chosen.



Press **Next** to create a Restore Plan and then **Finish** to begin the data recovery.

7. After the Wizard is finished, the **Restore Plans** tab will open – here you can track down the recovery process. If you've chosen **Restore Once** option, the restore plan will disappear after finishing the task.



Image-level Restore

There are several ways of image-based recovery:

- **Restore Image Based Backup** – recovers the whole machine from the image file. In this mode, you can also restore the data to Amazon Elastic Compute Cloud (EC2) and Azure virtual machines.

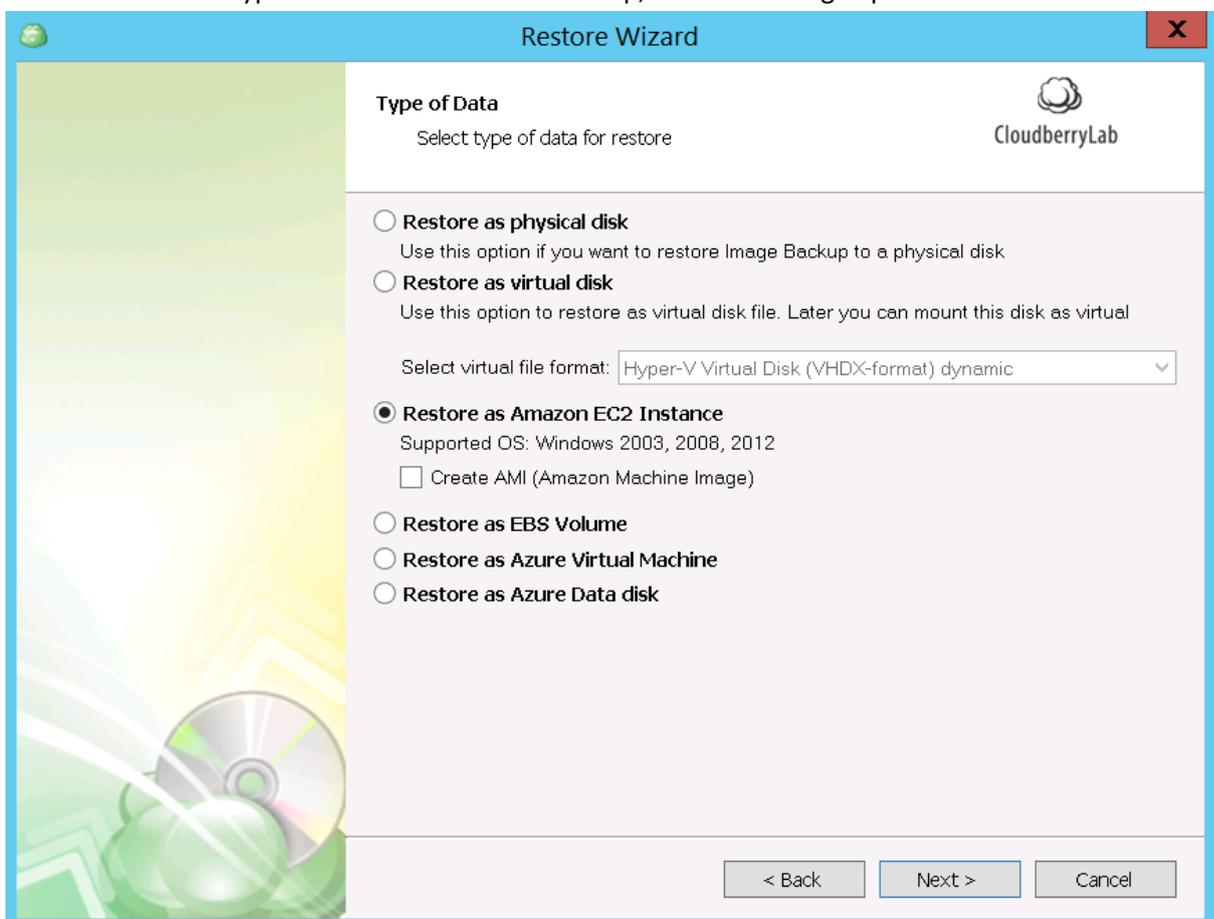


- **System Image (former Bare Metal) Restore** – recovers all root volume with boot files, thus used for restoration to the new hardware or for repair of the entire system.
- **System State Restore** – recovers boot and system files. It's designed for system repair tasks.

The last two options involve Windows restoration service, so the Wizard will prompt to install it. They also need enough disk space to download recovery images, which may be deleted after restore job finished.

Image and Virtual Machine Restore

1. After you choose the **Restore Image Based Backup** option, the Wizard will ask to specify **Restore Type** and choose which version of an image to retrieve. It works just like with files recovery.
2. Select the data type to recover. On this step, the following options are available:



- **Restore as physical disk** – formats the chosen local disk and deploy the image contents to it.
- **Restore as virtual disk** – creates a virtual disk file to be mounted within VirtualBox, Hyper-V or VMware virtual machine systems: you can also create a RAW disk image.
- **Restore as Amazon EC2 Instance** – deploys Amazon cloud virtual machine using the image data. You need to have the Amazon Web Services (AWS) account to use this option. *Note: If you select to convert the backup to .AMI (Amazon Machine Image) file, the virtual machine will start immediately after finishing the Wizard. Otherwise, you need to access it via Amazon Management Console and launch manually.*

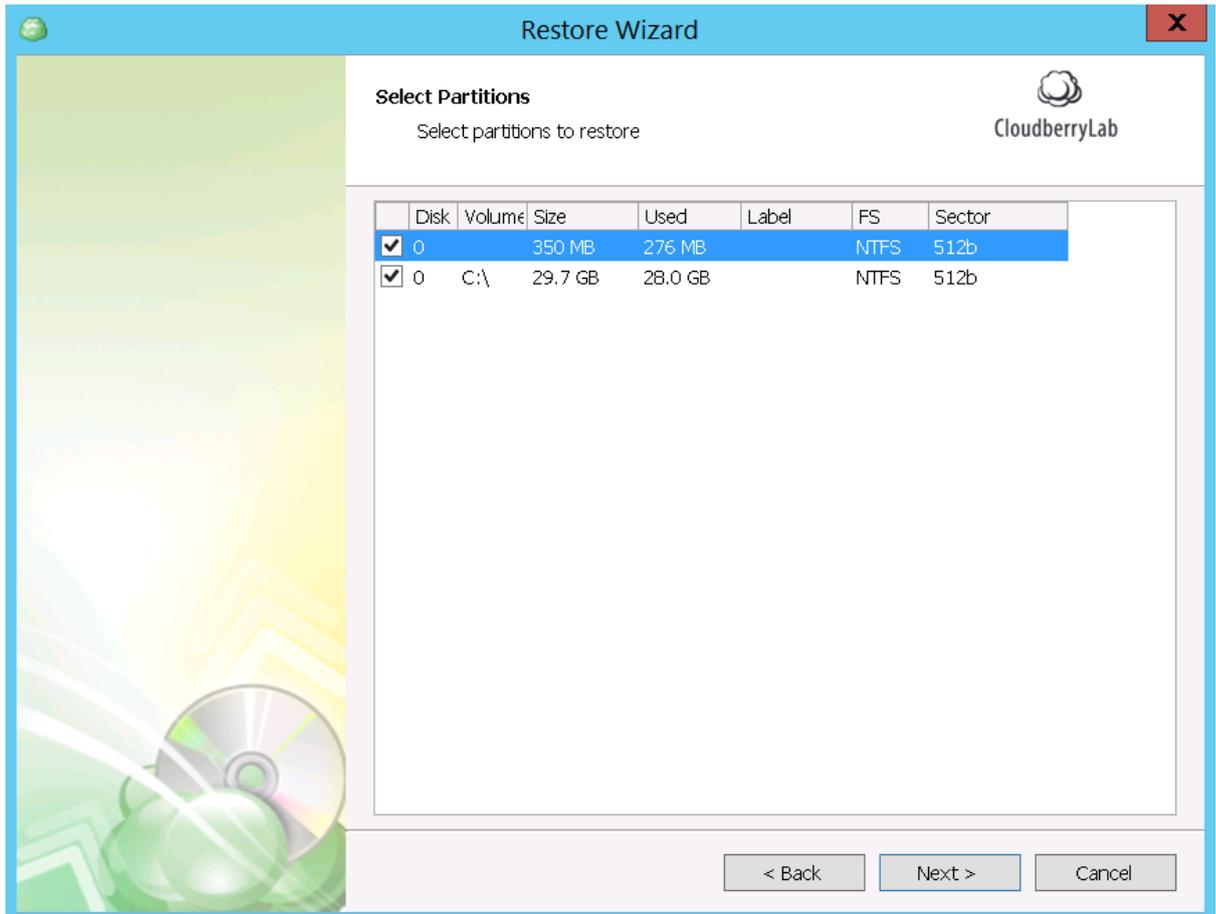


- **Restore as EBS volume** – creates Amazon Elastic Block storage volume to be mounted to EC2 instances or used separately. You need to have AWS account for this too.
- **Restore as Azure Virtual Machine** – deploys and automatically launches Microsoft Azure VM instance using the image data. You need to have Azure VM account to use this option.

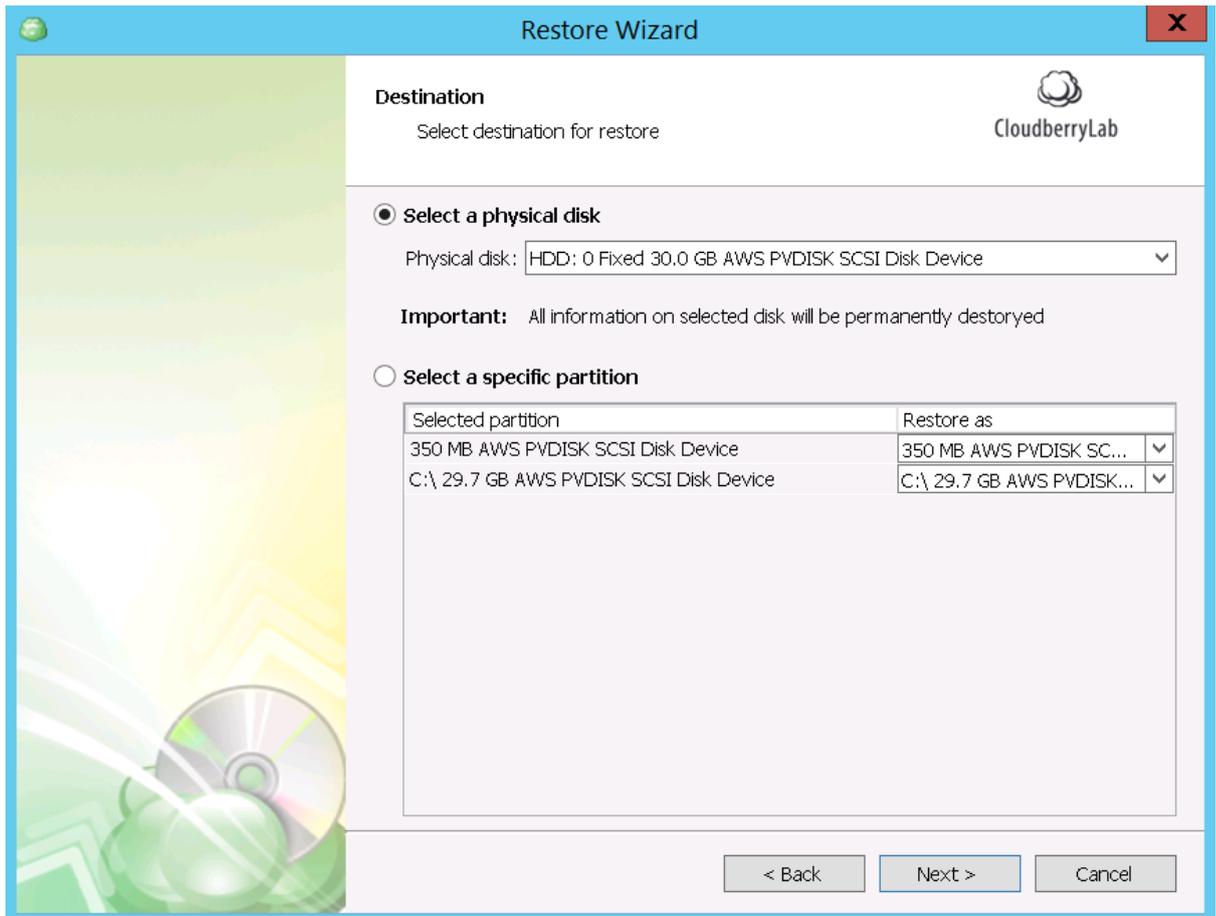
Each option requires specific adjustments. We shall look them over below.

Restore as physical disk

1. If you choose the recovery to the physical disk, select image partitions to restore on the next step.



2. Then, select a destination for the image data deployment. If it is a physical disk, CBB will format it according to the partition scheme of the image. You can also distribute data across existing local disks.



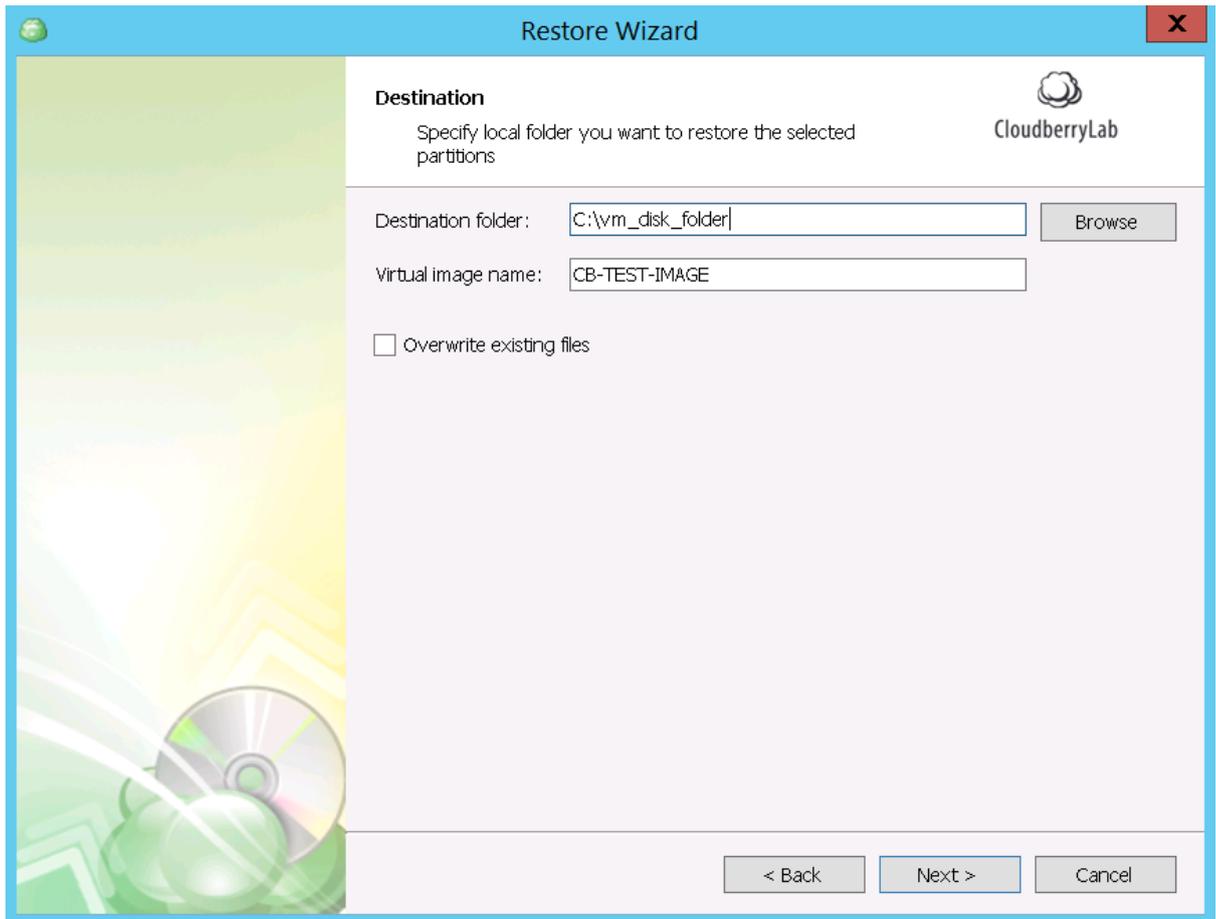
Note: recovery to the boot volume is not allowed.

3. Next, specify the decryption password if needed and set up notifications. All chosen option will be displayed on the Summary screen.
4. After the Wizard has finished, CBB will download the image and deploy it onto the chosen disk. It will disappear in Windows Explorer when the recovery begins. If the restored disk has a boot volume, the firmware will recognize it, and the system on the disk will start on this or another computer after proper BIOS setting.

Restore as virtual disk

1. If virtual disk option selected, choose partitions for recovery. Next, pick up **Destination** to save the virtual disk and specify its name.



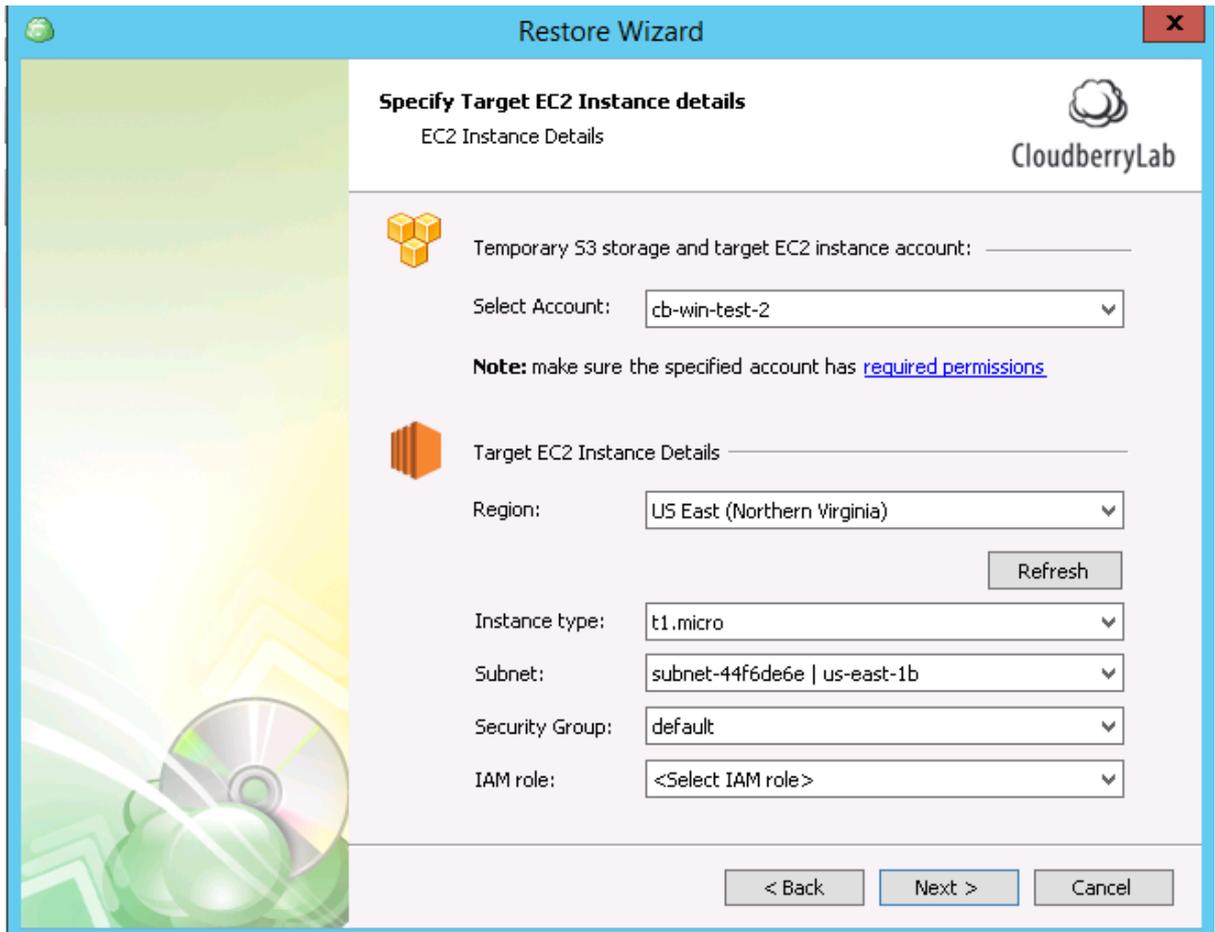


2. Configure file deciphering, notifications options, etc.
3. Then, you can attach this disk to the existent VM or deploy a new one based on the disk data. Here are the guides how to do it in [Virtualbox](#), [VMware](#) and [Hyper-V](#) systems.

Restore as EC2 Instance

1. If you choose to recover the image as Amazon EC2 virtual machine, specify target instance details and choose the AWS account on the next step. Use the account already registered in CloudBerry Backup or add a new one. To setup an instance, you must have a role with name **vmimport** in AWS account.



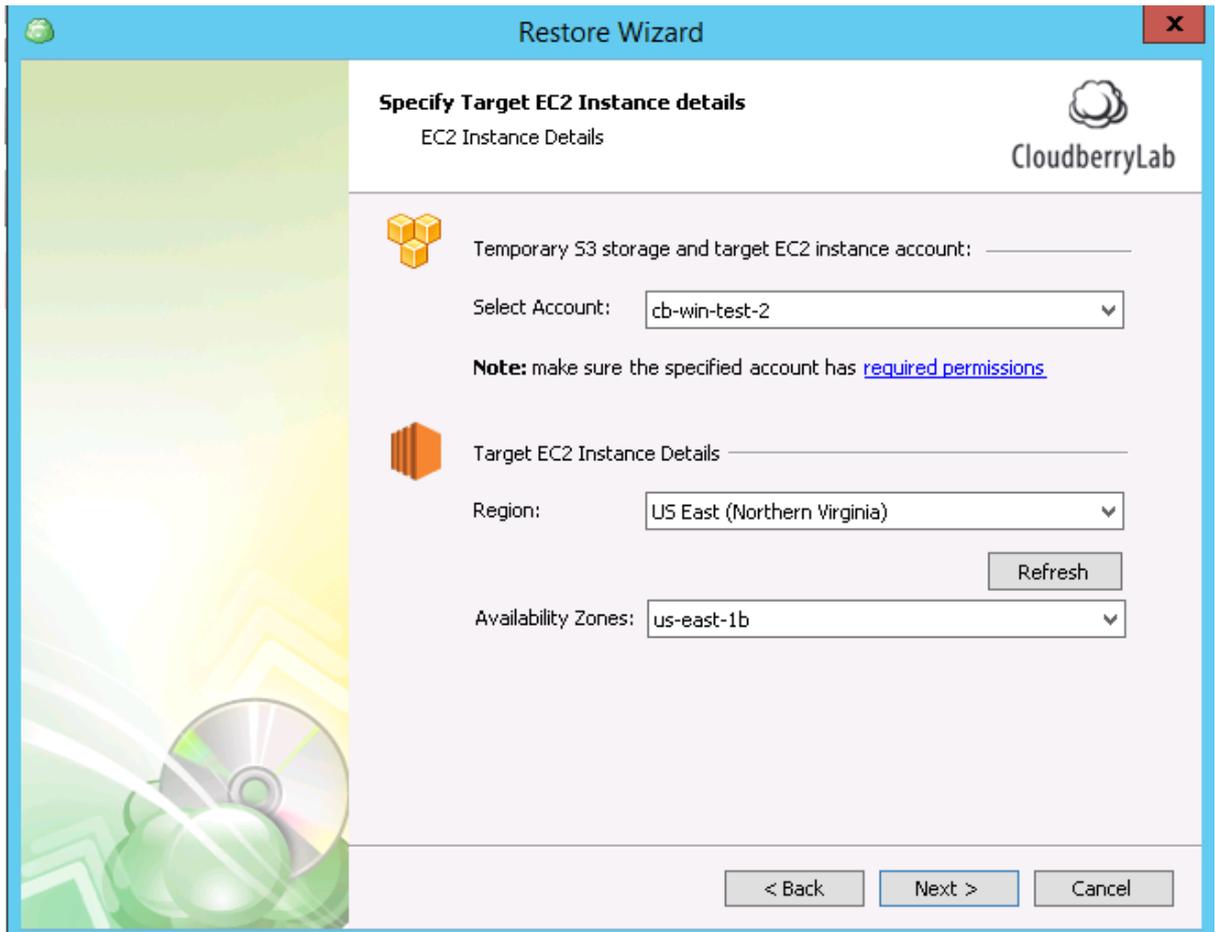


If the target account is configured correctly, you can select instance type and other EC2 credentials.

2. Configure file deciphering, notifications options, etc.

Restore as EBS Volume

1. If you want to restore the image as the Amazon Elastic Block Storage volume, select Amazon S3 account or create a new one. Then choose the **Region** and **Availability Zone** for a volume. You need to know that:
 - a. Newly created EBS instance won't be prepared to function as a boot volume.
 - b. The AWS account must have the required permissions. Visit [AWS Controlling Access to Amazon EC2 Resources page](#) to find out more.

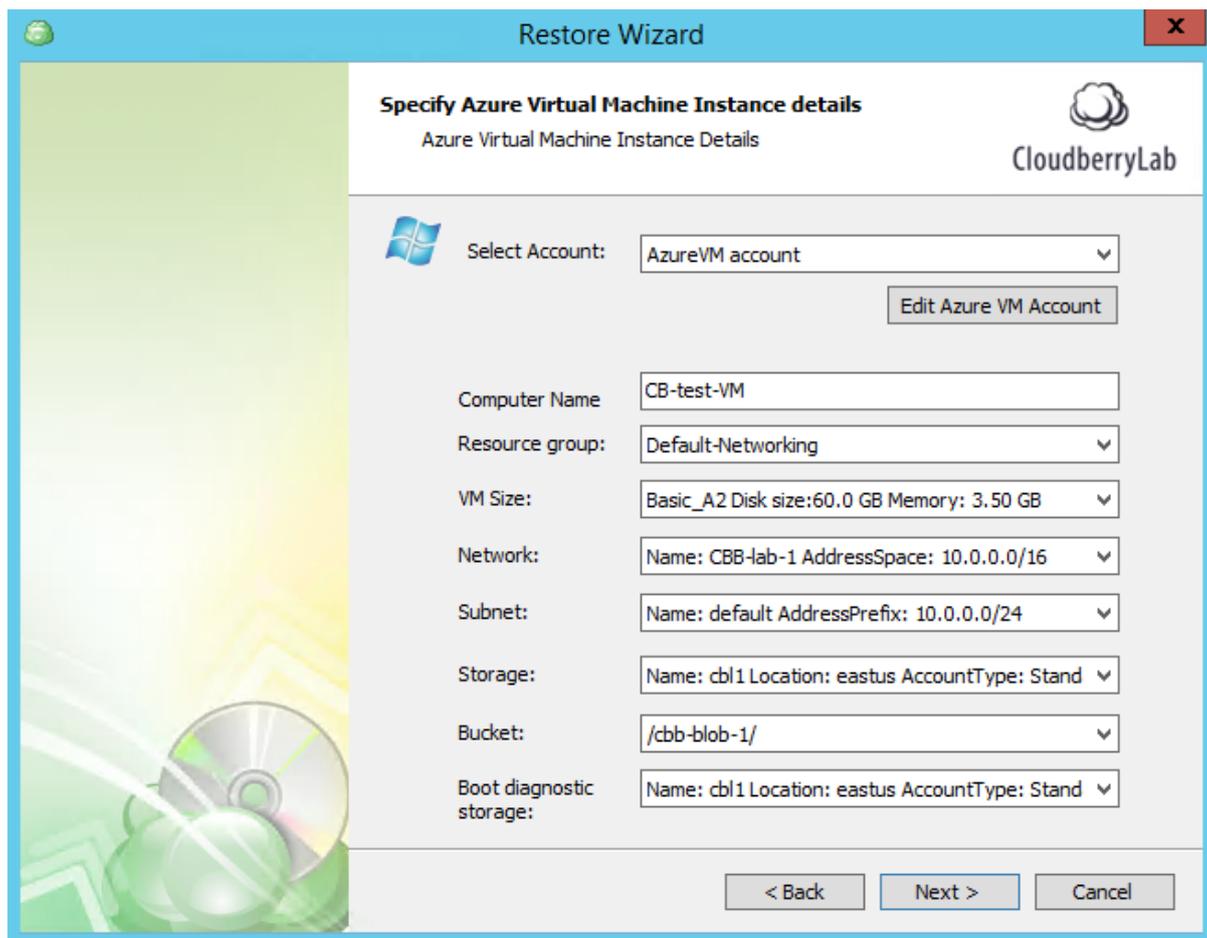


2. Select partitions for restoration and configure deciphering, notifications options, etc.
3. After the Wizard finishes, you may find new EBS Volume in Amazon EC2 Management Console and attach it to any desired instance.

Restore as Azure Virtual Machine

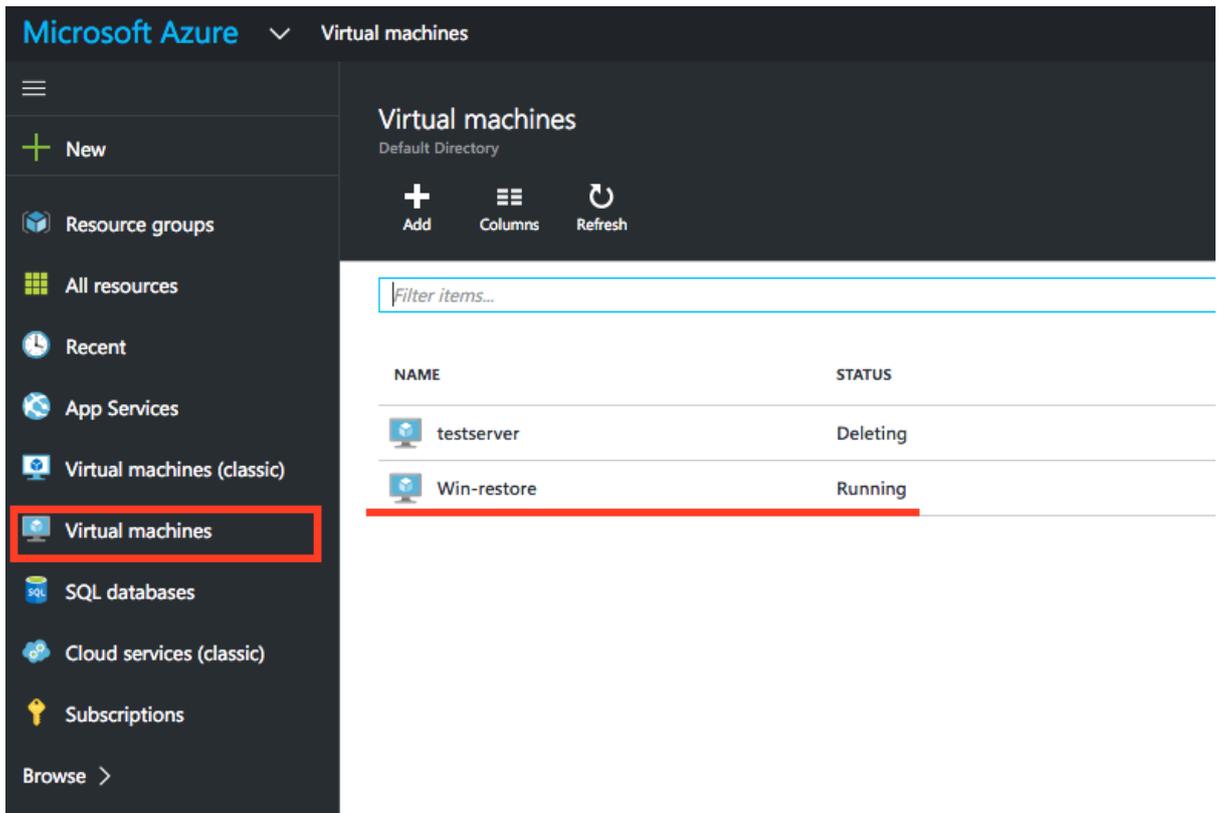
1. After you choose to restore image as Azure VM, select Azure VM account registered within CloudBerry Backup or add a new one, and then specify details of the new virtual machine instance. You can find all fields parameters in the Azure Control Panel.





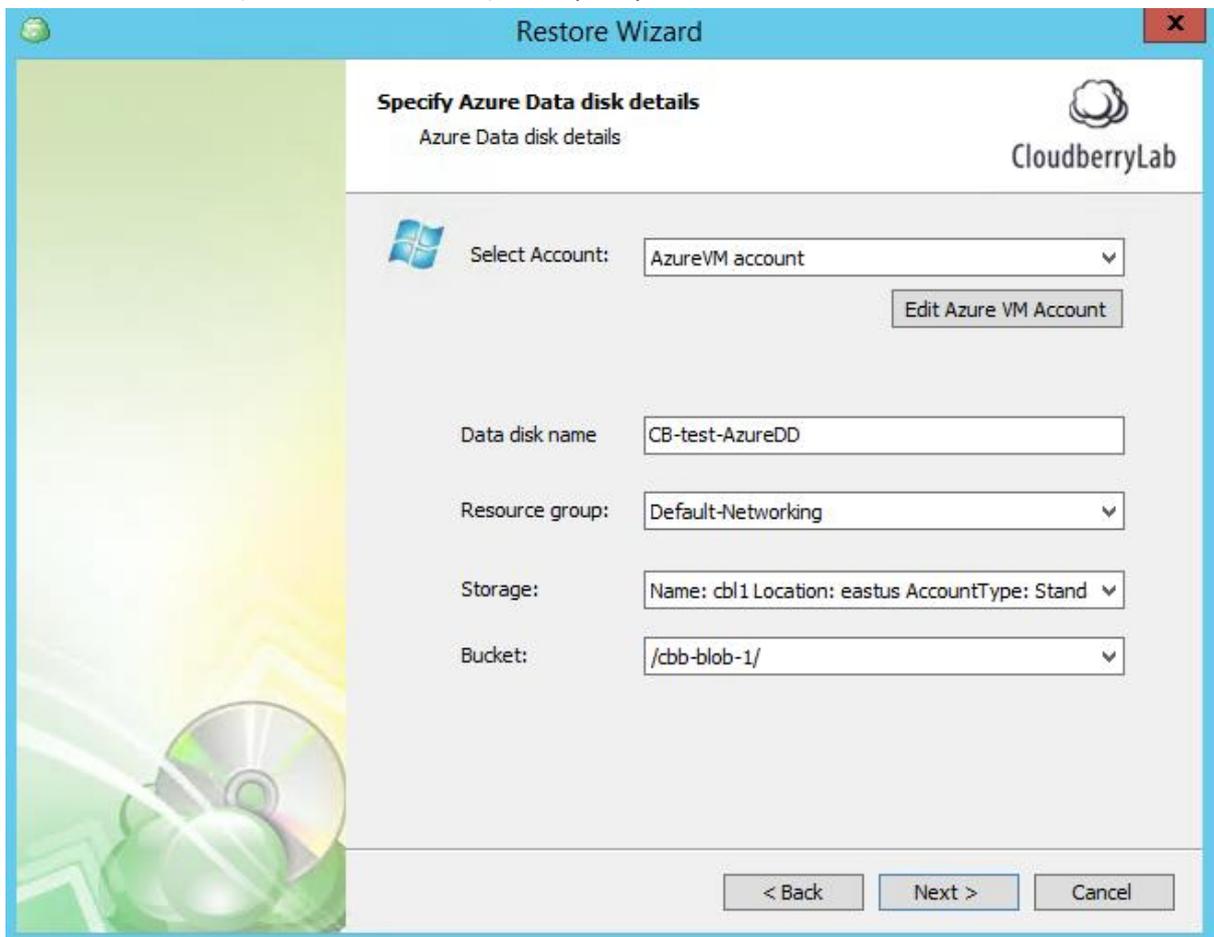
2. Then, choose the image partitions for recovery and configure notifications, decryption, etc.

3. Finish the Wizard. One restore task completes, VM starts automatically and displays in the Microsoft Azure console.



Restore as Azure Data Disk

1. If you want to create Azure Data Disk instance with the contents of the backup image, select Azure VM Account (or create a new one), and specify the custom name and other disk details.

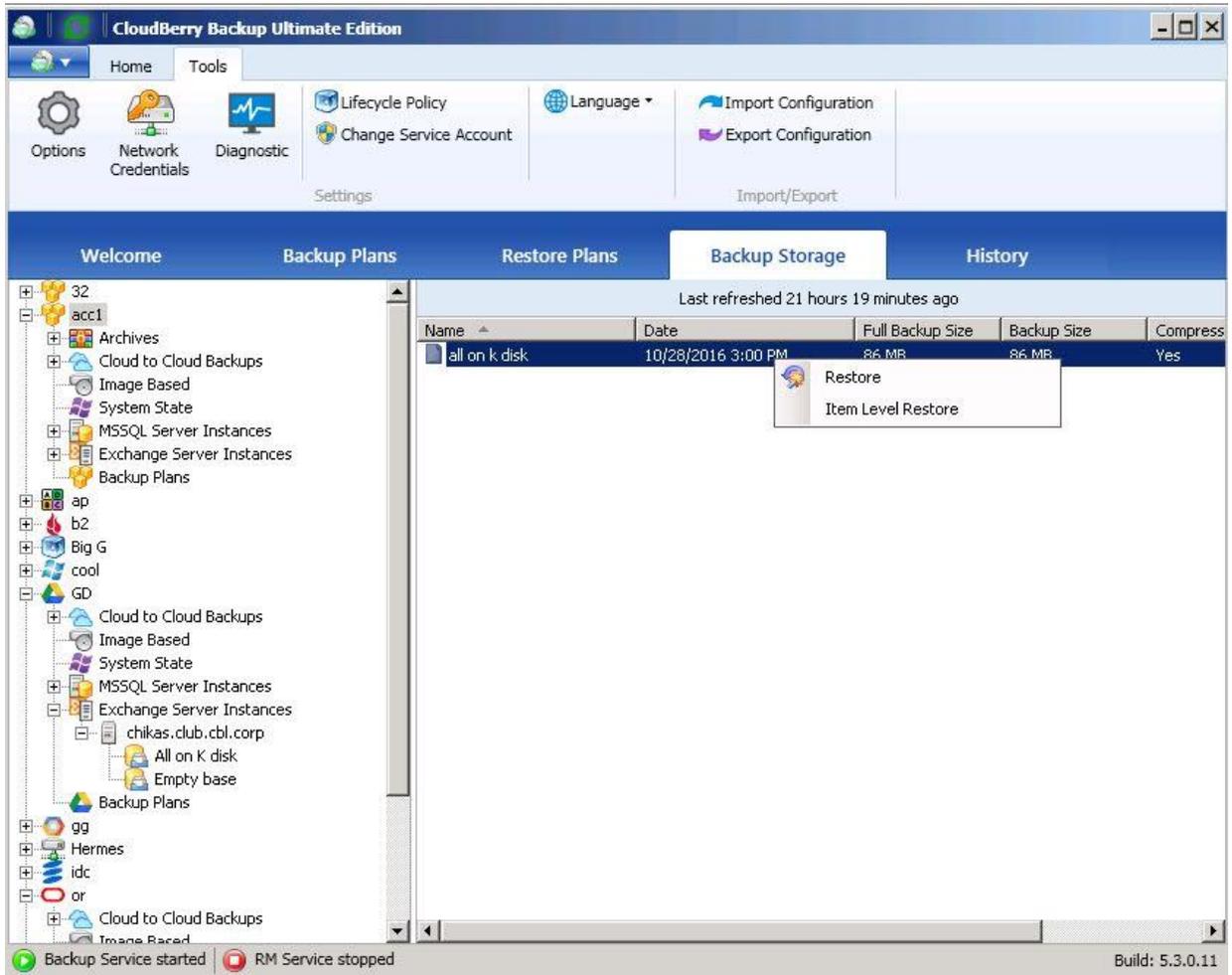


2. Next, select disk partitions to restore and set up notifications and deciphering to complete the Wizard.
3. When the recovery has finished, new disk displays in Microsoft Azure Management console. You can attach it to existing Azure VM instance or deploy a new one based on the disk data. Find out more [on special Azure guide page](#).

Item-level restore for Microsoft Exchange.

Starting from version 5.2, CloudBerry Backup enhances support for Microsoft Exchange. Formerly, you were somewhat limited when it comes to restoring your Exchange files. To wit, you could only restore complete EDB files and logs from the Exchange server, which is sufficient for essential tasks; however, many professionals found it to be deficient. Well, no longer! Now we're gonna explain how to perform item-level Microsoft Exchange restore.

To enable the feature, you must make a new full backup of the Exchange database. It is due to significant changes in the backup format. Having done so, open CloudBerry Backup 5.2 or newer. Under **Backup Storage** locate your database. Right-click on it and click **Item Lever restore**.

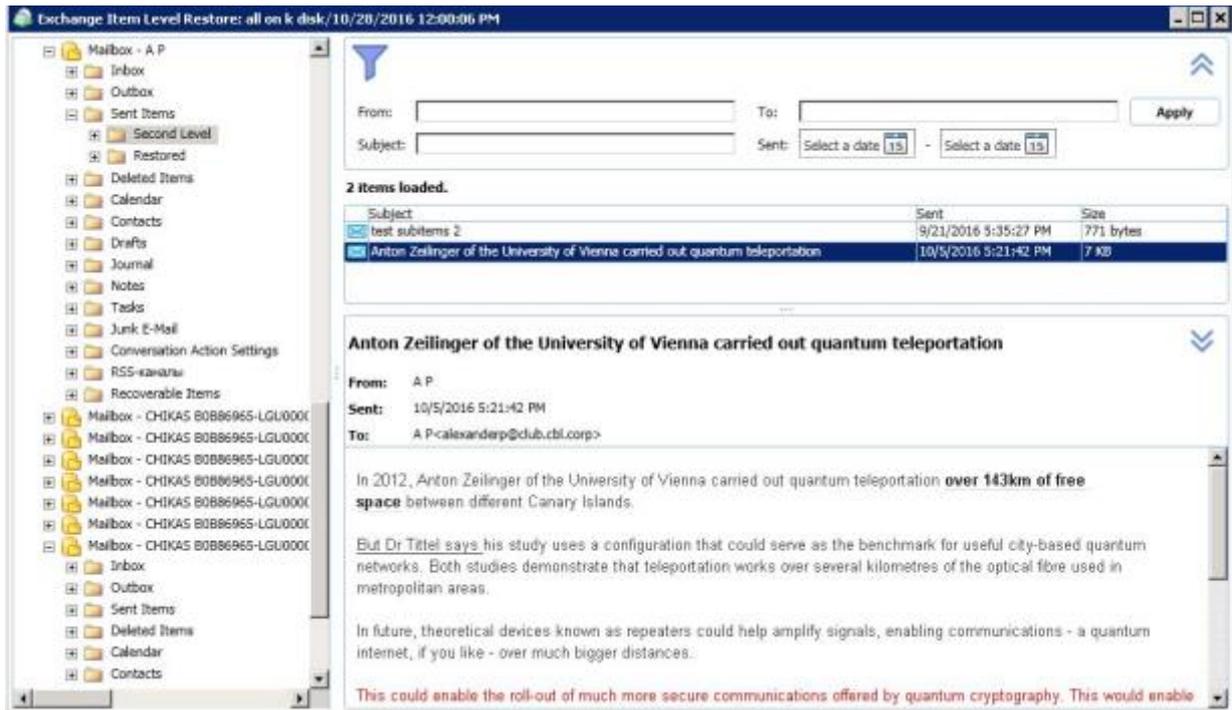


A pop-up window will appear and ask you if you wish to apply logs. Roughly speaking, it would add information from the logs to the database and subsequently remove unnecessary logs.



A newly appeared window is the Microsoft Exchange item-level restore assistant. On the left you can see a file structure of your mailboxes, emails, calendar events, contacts, etc. Select the files you want to restore.

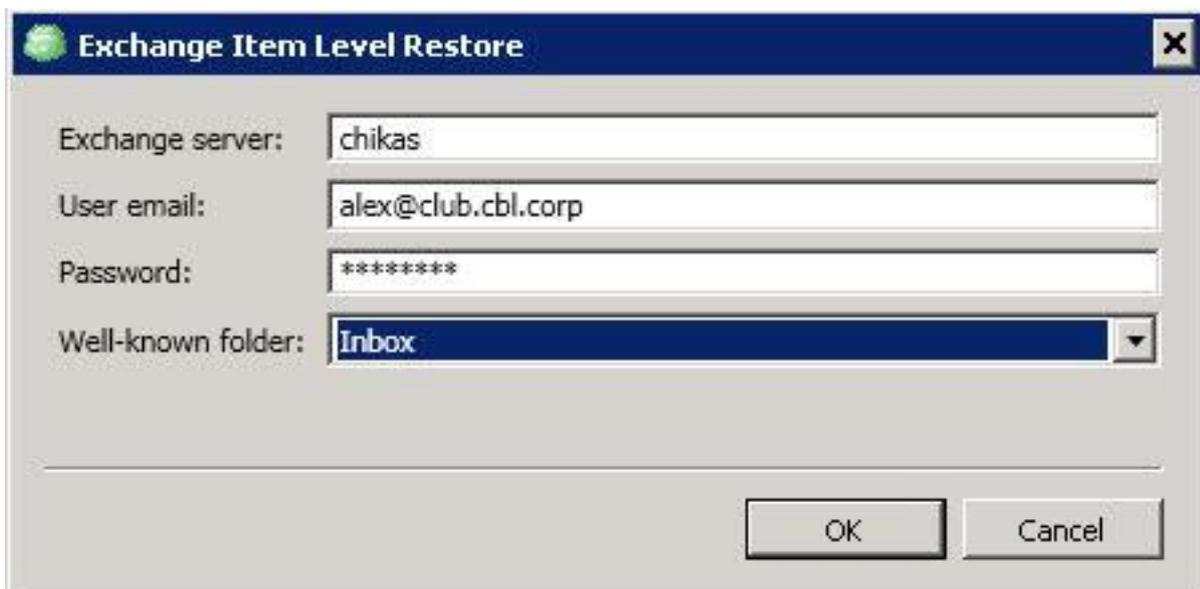




Right-click on them and click **Restore**.



Now enter your Microsoft Exchange credentials and click **OK**.

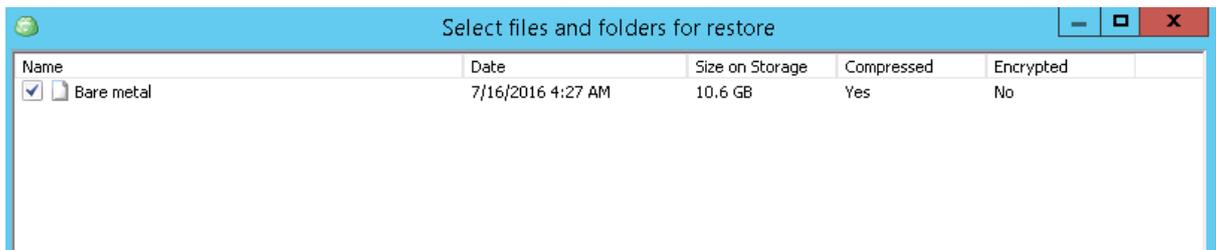


Done! Your files should be successfully restored by now.

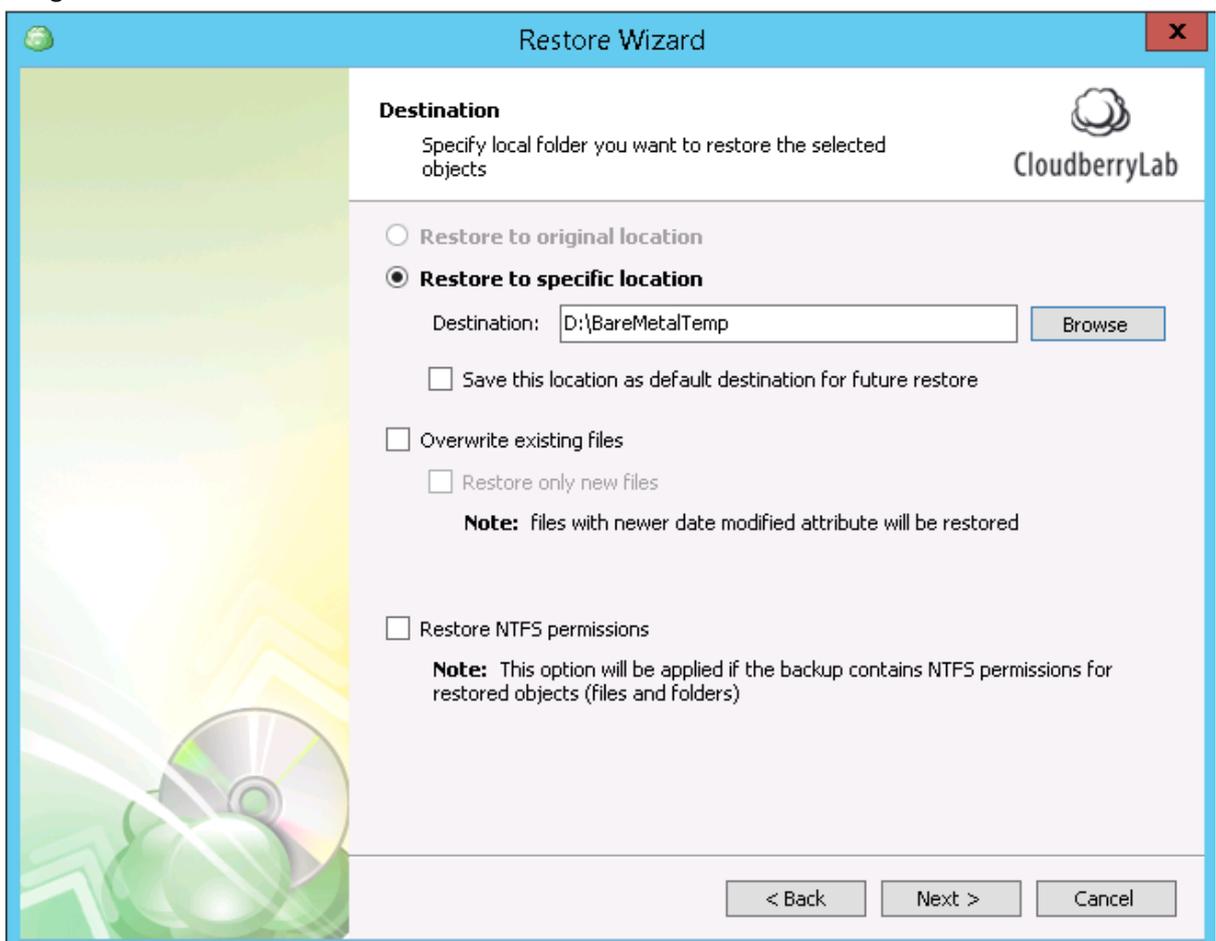
Currently, CloudBerry Backup is only compatible with MS Exchange 2010. We keep working on the Exchange Backup and will introduce a full-featured items recovery in the near future to support MS Exchange 2007, 2013 and 2016.

System Image (formerly Bare-Metal) Restore

1. In the Restore Wizard, choose backup storage and the version of the image file. Then, pick up **System Image Restore** option on the **Type of Data** step and select the backup to recover.
2. On the **Restore Source** step, pick up the exact recovery file. Here one can check the backup date, the size of the image and see if the file is compressed or encrypted. You can access the properties table in a more convenient way by clicking on the **View in dialog** option.



3. On the **Destination** step, choose the folder on the external drive to download the system image.



The **Restore to specific location** option is not available because you just need to extract the recovery image for Windows native repair service.

4. Configure decryption and notification settings and review the **Summary** screen.
5. After the Wizard has finished, CloudBerry Backup will switch to the **Restore Plans** tab to track the process.



When the download completes, check the **WindowsImageBackup** folder on the external drive.

6. Connect this drive to the machine you want to recover. Then, do the next:
 - a. If there is no OS on the computer, just reboot it.
 - b. If there is an OS installed, plug in Windows installation disk and choose to boot from it in your firmware settings. Then, reboot the machine.
 - c. Otherwise, reboot the computer, press **F8** while firmware starts and select **Repair Your Computer** option.

Windows Install & Repair Wizard will initialize. The System-Image recovery goes in a few steps:



1. Choose **language, time format, and input** method.



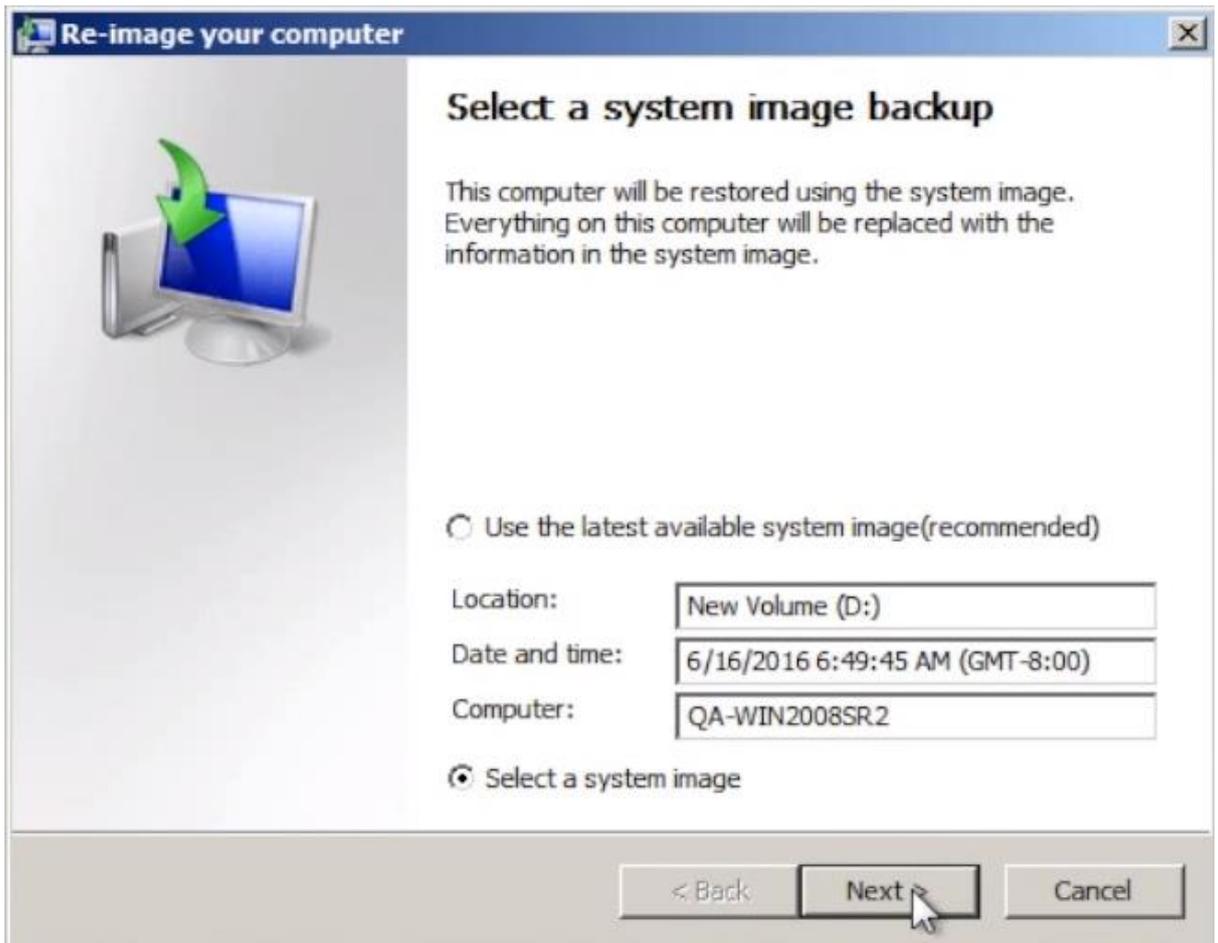
2. Select **Repair your computer** option.



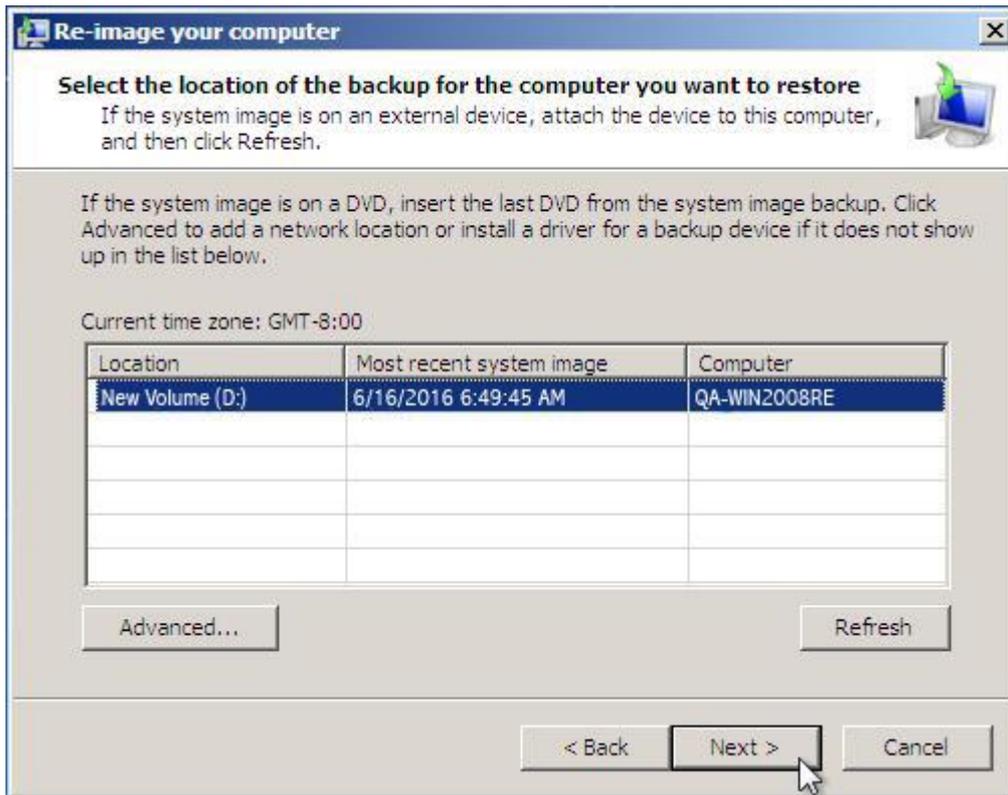
3. Check **Restore your computer using a system image that you created earlier** option.



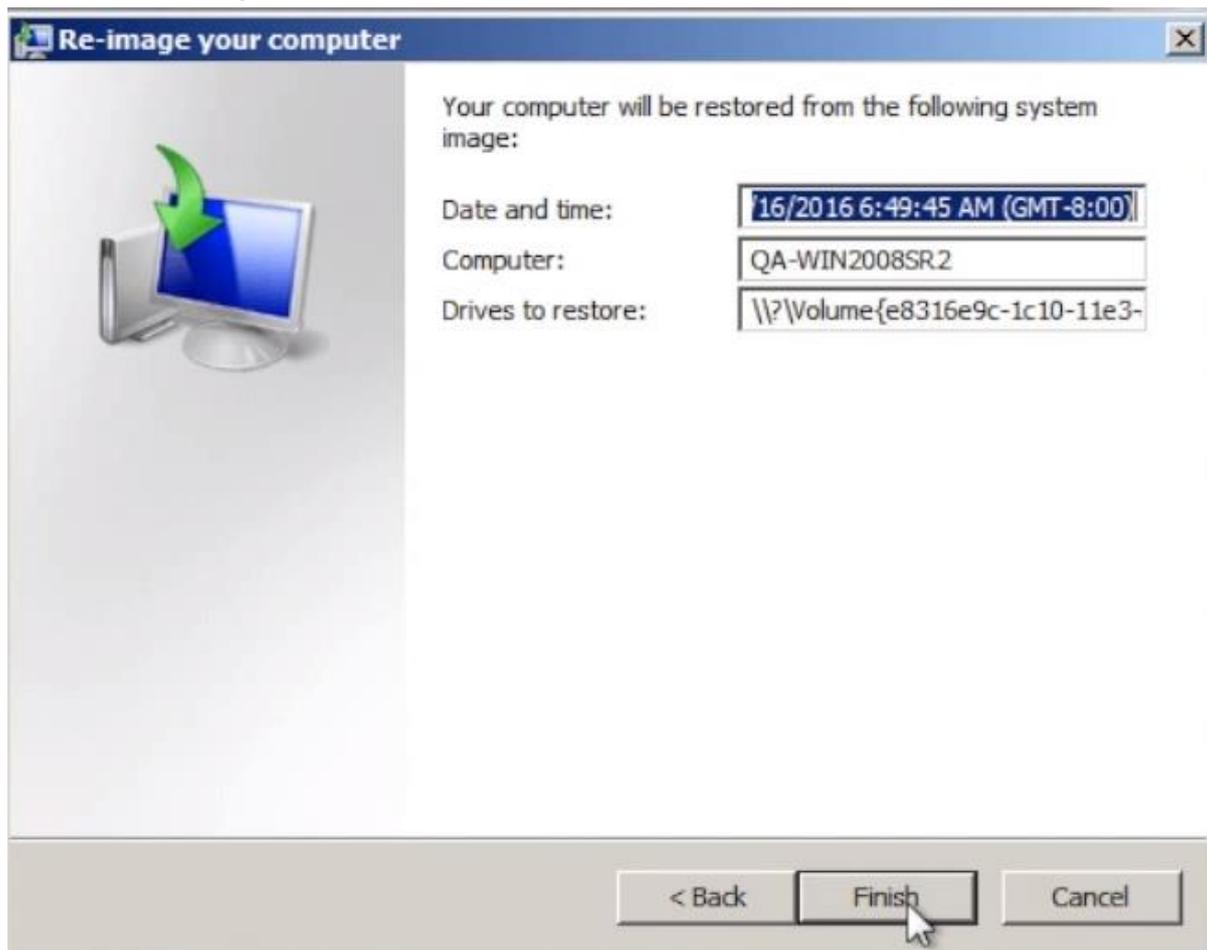
4. Choose **Select a system image** option.



5. Select the system image from the connected drive.



6. Check the image credentials and click **Finish** to launch the restoration.

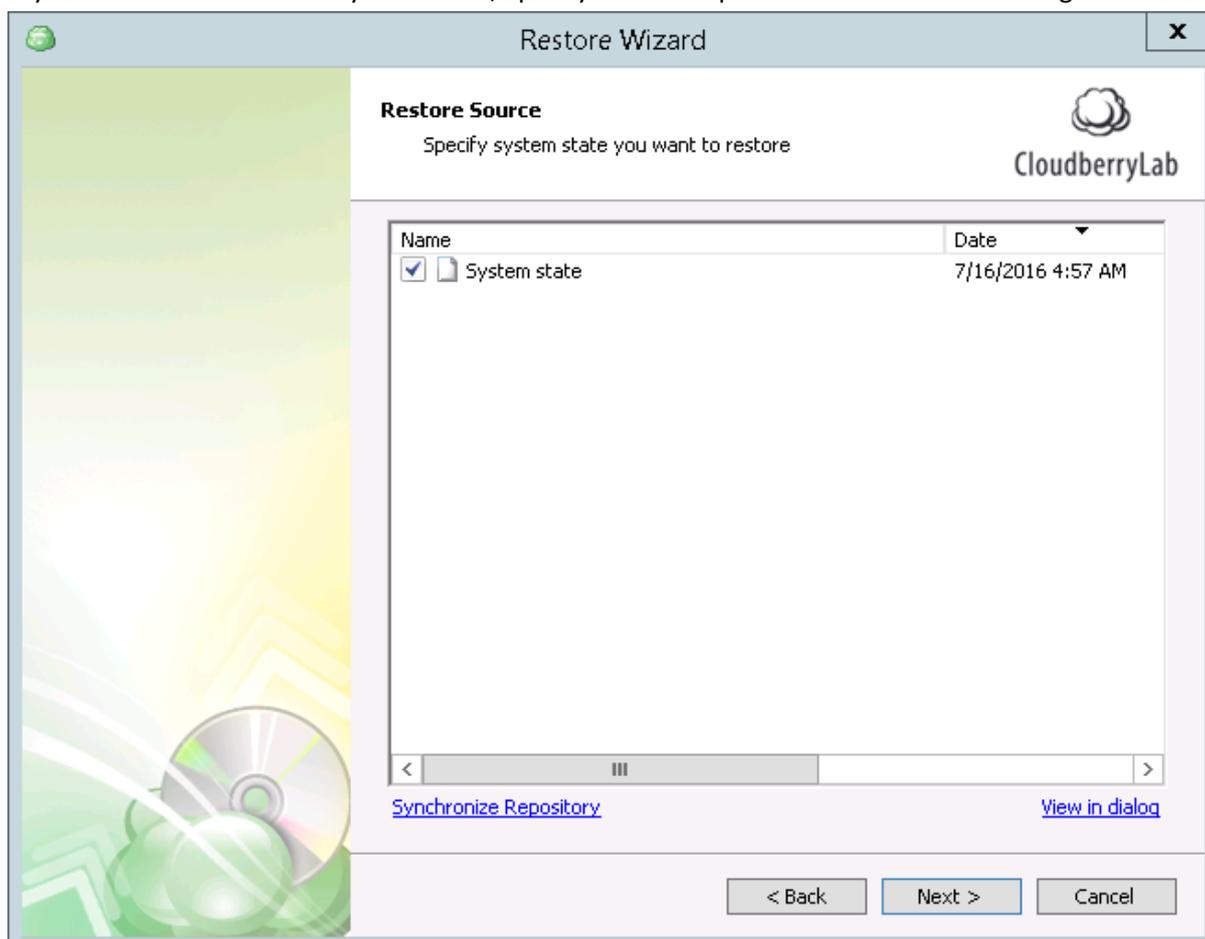


7. When the restoration is completed, relaunch the machine.

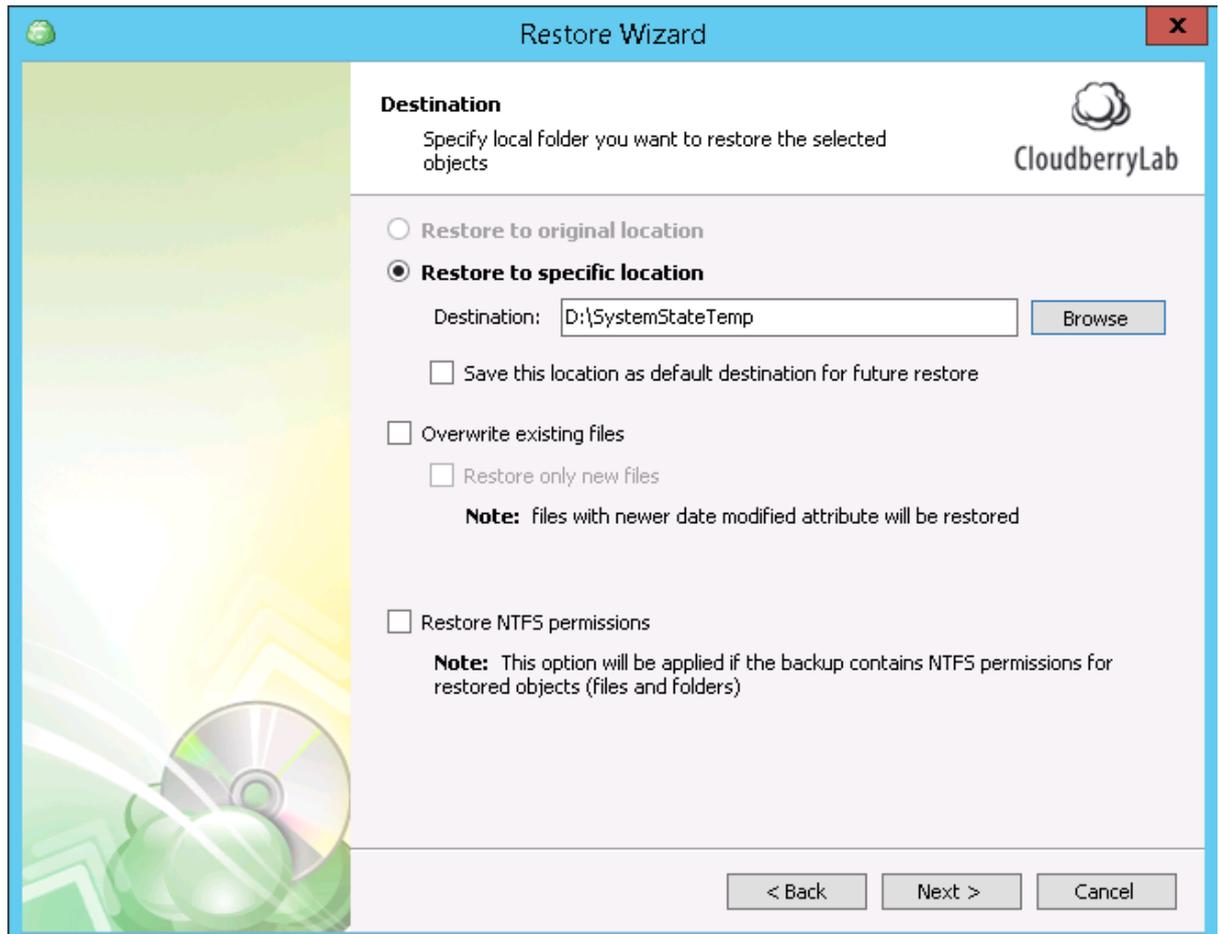


System State Restore

1. If you want to recover the system state, specify the backup version and the exact image file.



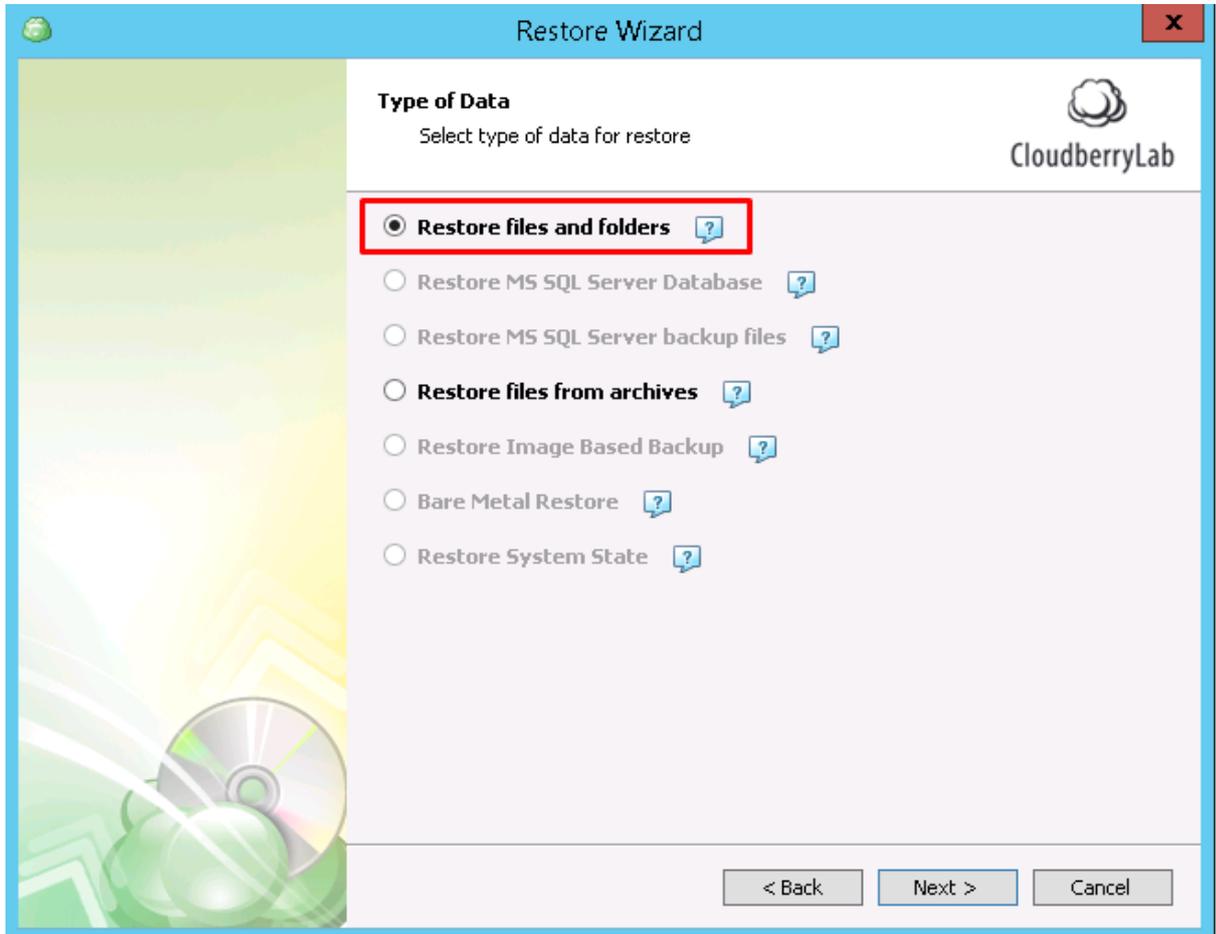
2. Then, you need to choose the external drive to deploy the recovery data kit.



3. After notification and deciphering options setup, check recovery configuration on the **Summary** screen. Then CloudBerry Backup will download the restoration pack to the external drive.
4. Next, launch the Windows Recovery Wizard in the next ways:
 - a. Plug in Windows installation disk and choose to boot from it in the firmware settings, reboot the machine.
 - b. Reboot the computer, press **F8** while firmware starts and select **Repair Your Computer** option.
5. The Wizard will start. Proceed its steps to complete the recovery.

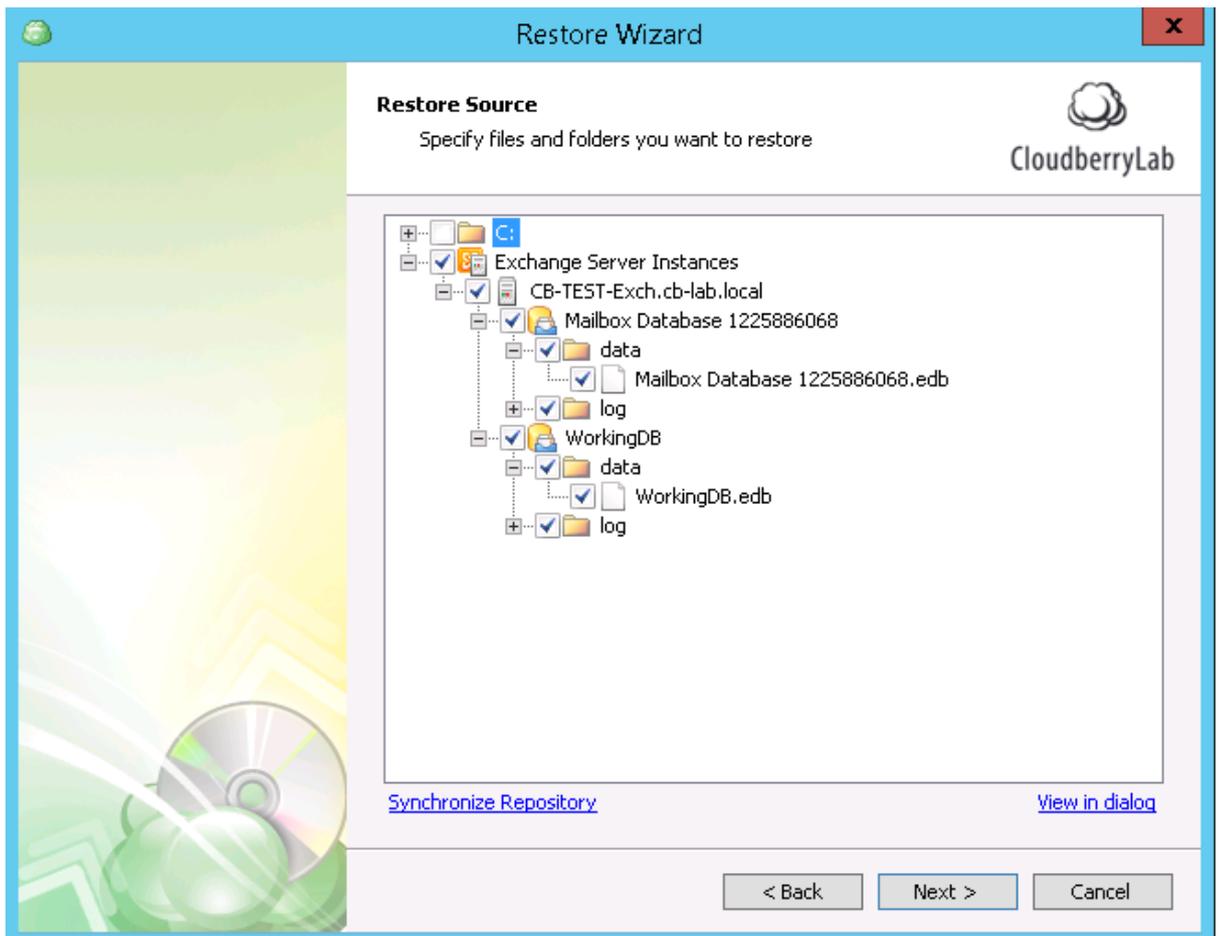
Microsoft Exchange Server Restore

1. If you want to recover Microsoft Exchange data, choose **Restore files and folders** option on the **Type of Data** step of the Wizard.

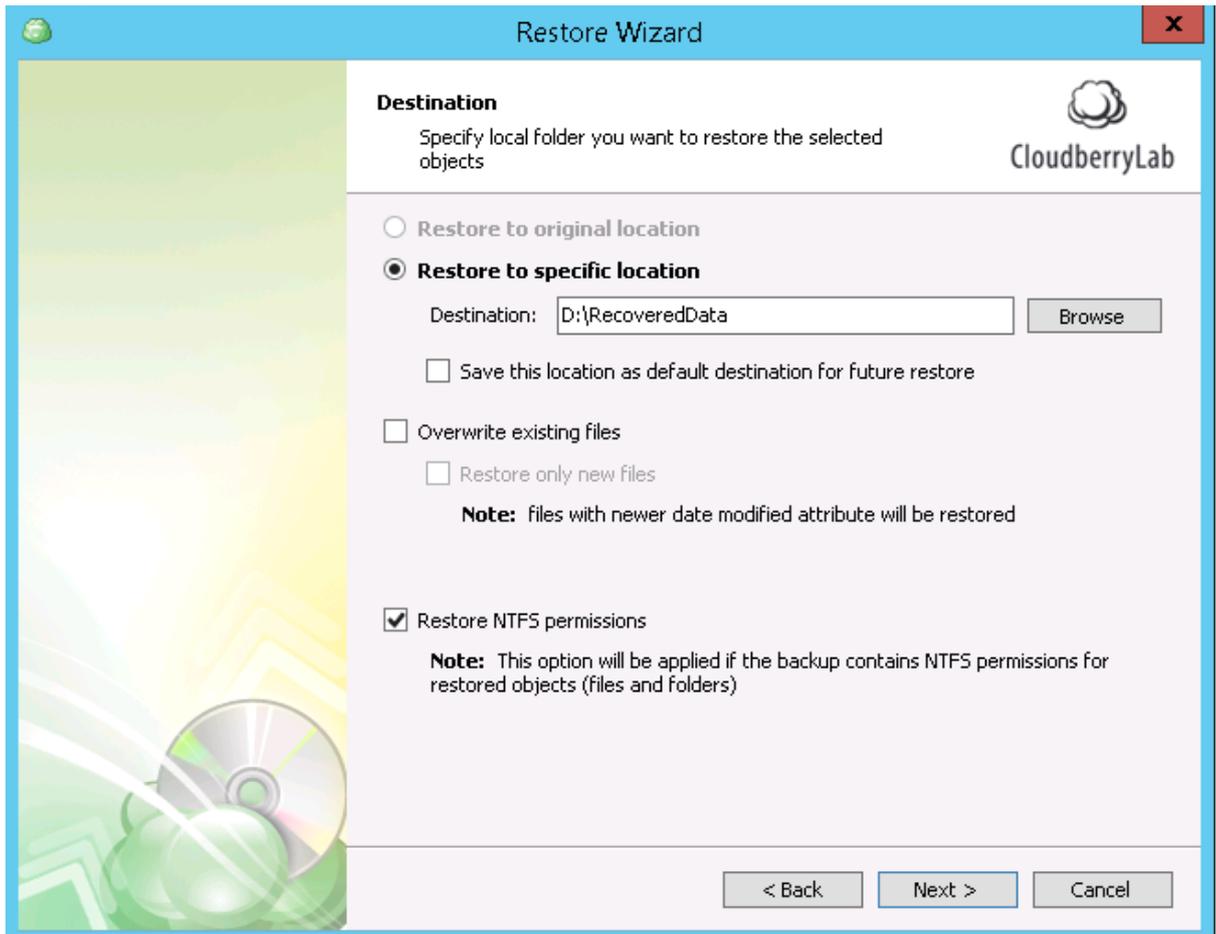


2. Choose the version of Exchange to recover and proceed to **Restore Source** step, where all data on backup storage exposed. Choose **Exchange Server Instances** and check the files to

recover.



3. Specify the folder to download the databases.



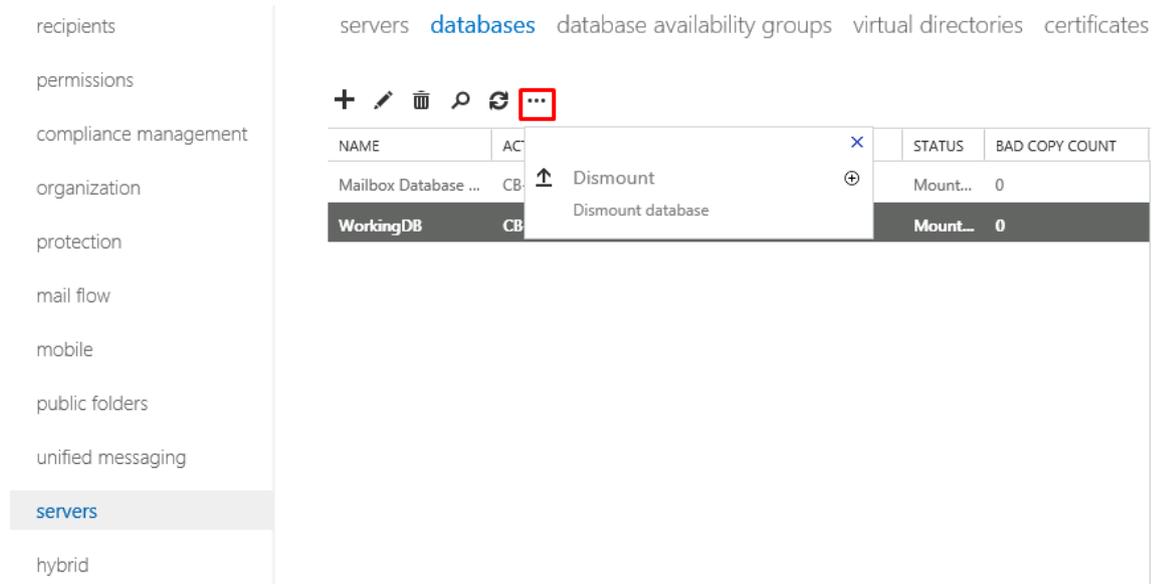
The Wizard can't restore data to the original folder directly. To recover to the original location, dismount current databases and replace existing files with the restored ones manually. You can do it in a few ways:

- a. Login to Exchange Admin Center (EAC) and choose **Servers** in console management tree on the right. Go under **Databases** tab, click on the desired database, press **Three**



Dots button above items table and select **Dismount**.

Exchange admin center



b. Use Exchange Management Shell command:
Dismount-Database -Identity DBNAME -Confirm:\$False

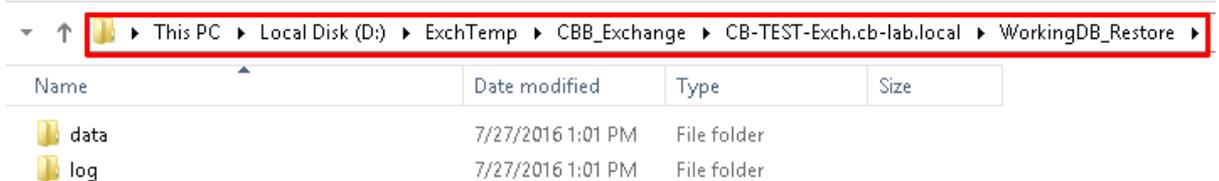
Where **DBNAME** is the name of the database to dismount. It can also dismount all the databases via the next command:

Get-MailboxDatabase -Server SERVERNAME | Dismount-Database -Confirm:\$False
 Where **SERVERNAME** is the name of Exchange instance.

- Finally, specify decryption and notification options. Recovery configuration will be reported on the **Summary** screen.

To mount restored databases, do the next:

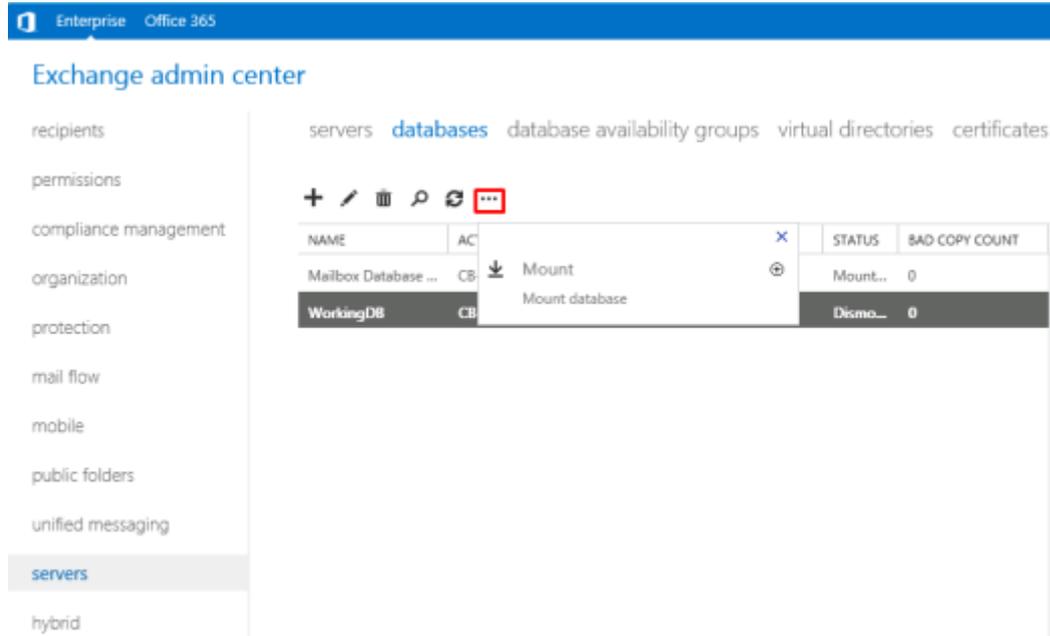
- Open EAC and dismount the database instances you want to recover.
- Open the temporary download folder specified in Restore Wizard. There is recovery data kit on the path **%Download Folder Name%/CBB_Exchange/%Your Exchange Instance Name%**. Rename the repository you want to recover, e.g. add the prefix **Restore** to the **%Your Exchange Instance Name%**.



- Paste **data** and **log** folders' contents from recovery data kit to **Mailbox/%Your Instance Name%** folder in the Exchange directory. Override the existing files.
- To mount the recovered database, do the next:



- a. Open EAC, choose **Servers** on the management tree, move under **Databases** tab. Then, select the database, press on the **Three Dots** button and choose **Mount**.



- b. Use Exchange Management Shell command:
Mount-Database -Identity DBNAME -Confirm:\$False
Where **DBNAME** is the database name. To mount all the available databases, use the next command:
Get-MailboxDatabase -Server SERVERNAME | Mount-Database -Confirm:\$False

Microsoft SQL Server Restore

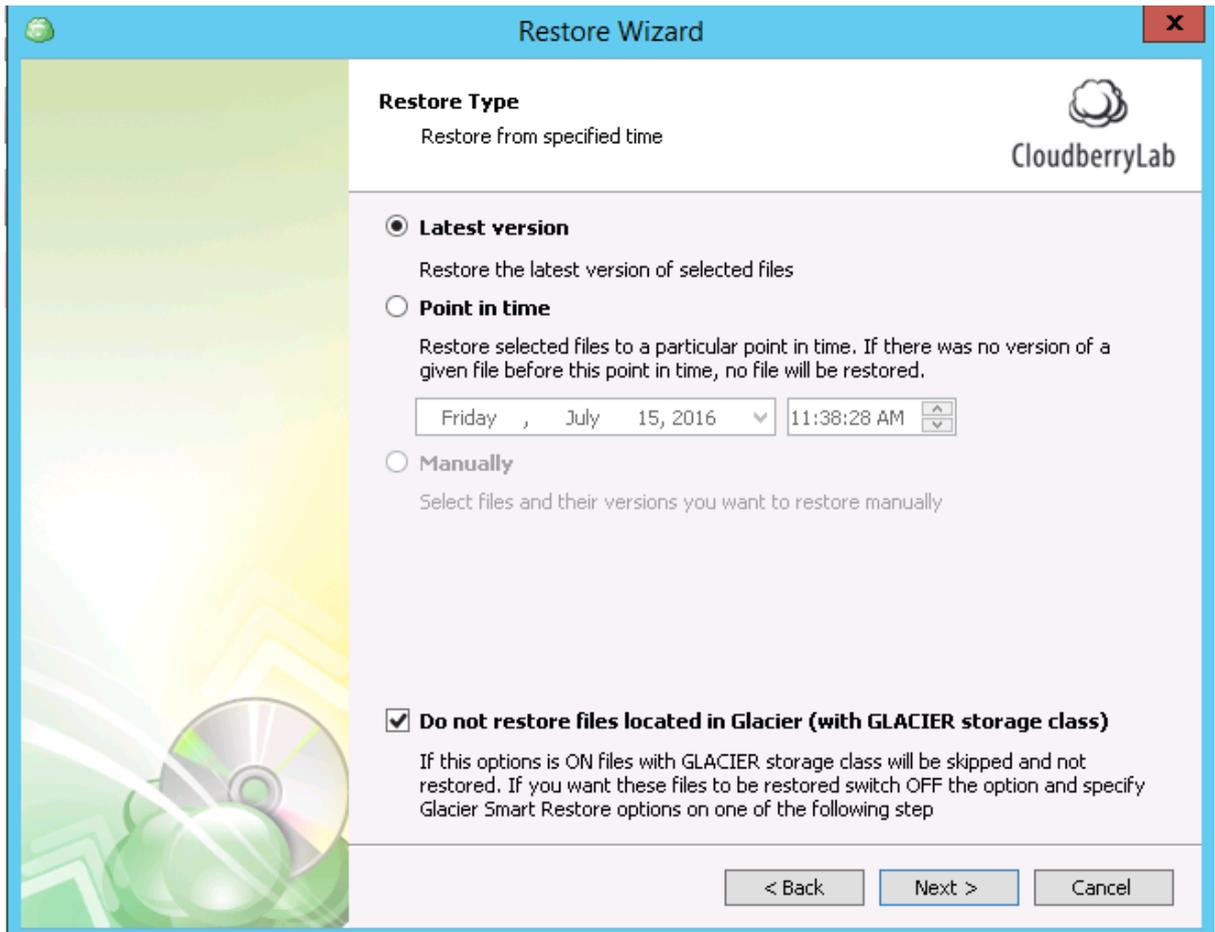
Microsoft SQL Server Restore option of CloudBerry Backup comes in two variants:

- **Restore Microsoft SQL Server Database** – this option restores backed up databases to the active database engine using REPLACE method.
- **Restore Microsoft SQL Server backup files** – this option recovers database files to the specific location.

Restore Microsoft SQL Database

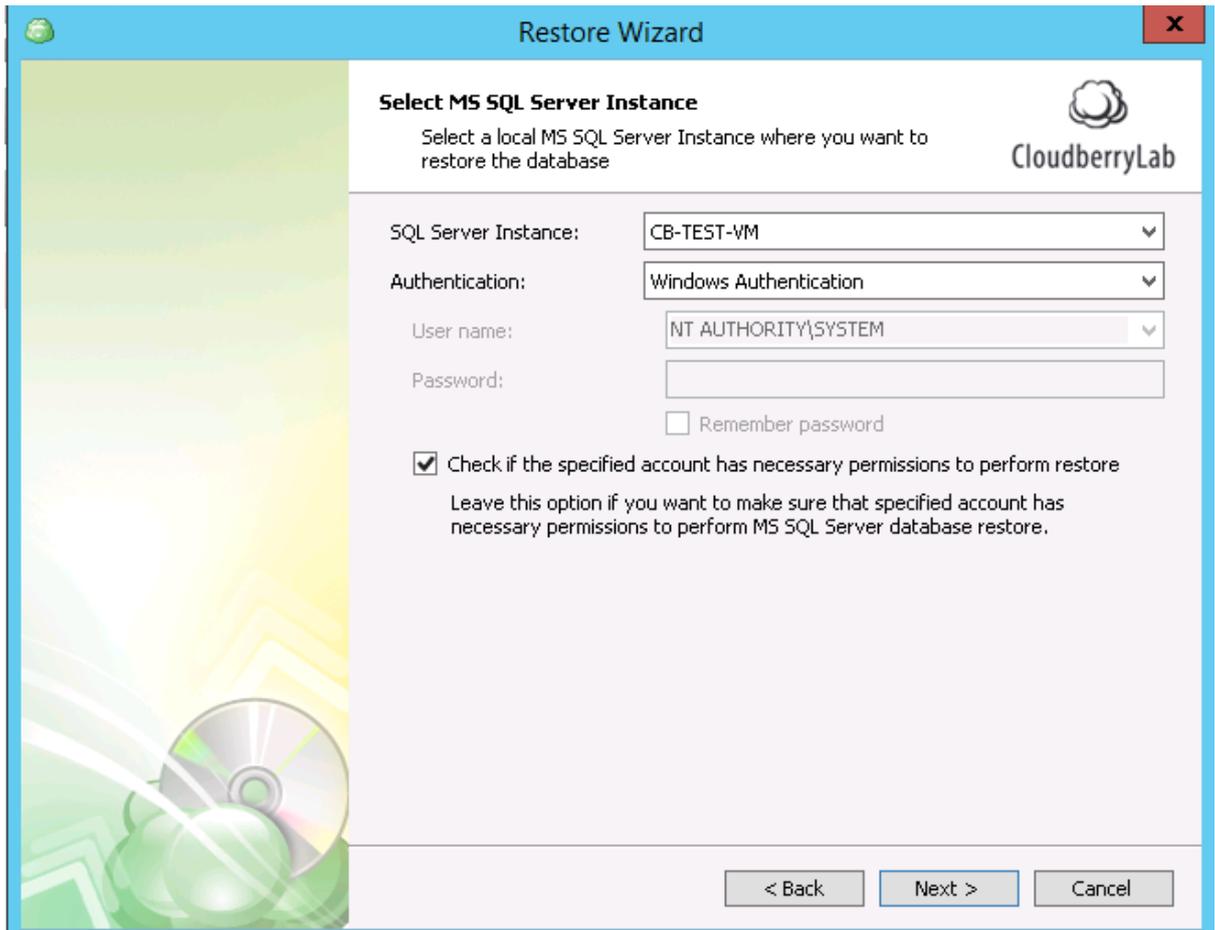
1. If you want to recover the active database server, the Wizard will offer to choose the backup version.





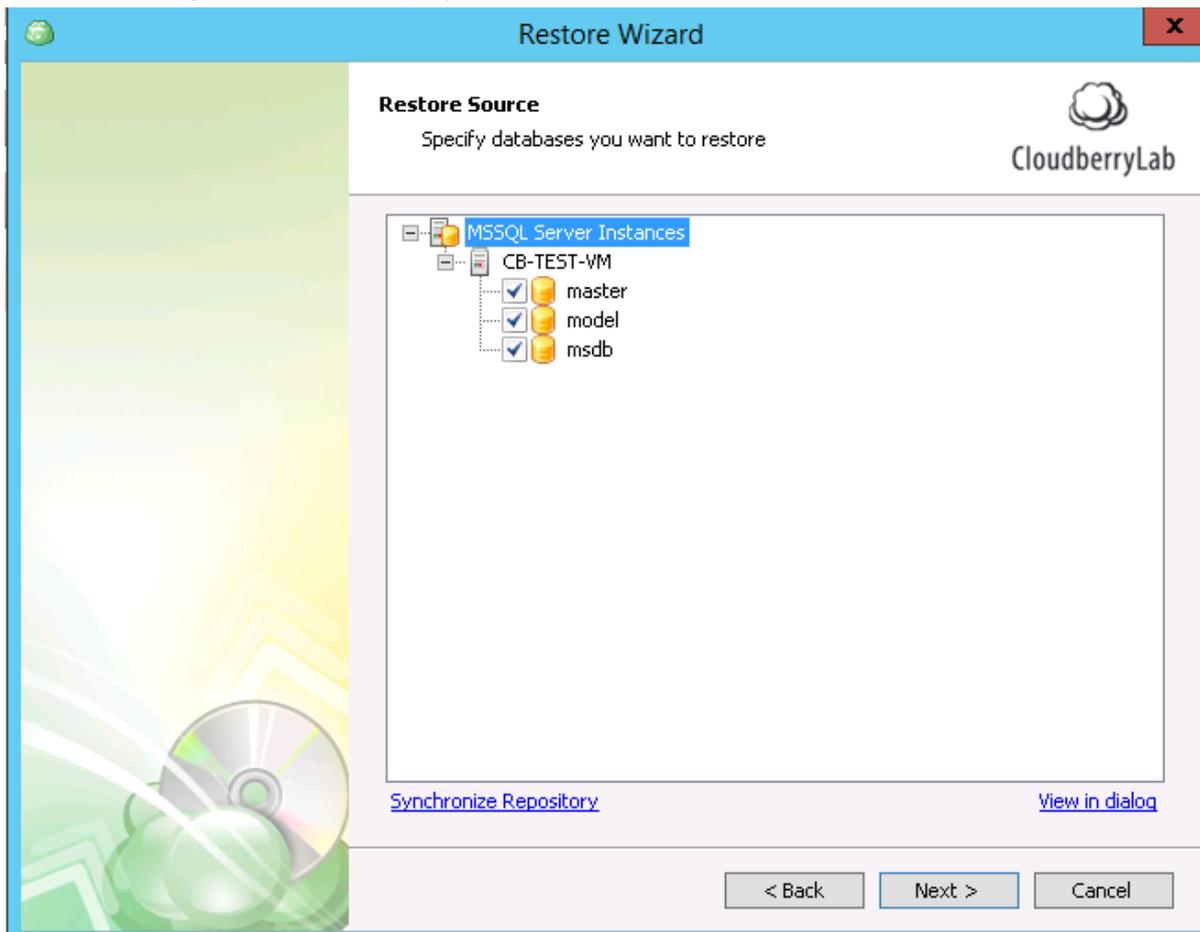
Like in file-level restore, you can select among the latest database version, point in time and manual management.

- Next, you need to select SQL instance and authentication method.

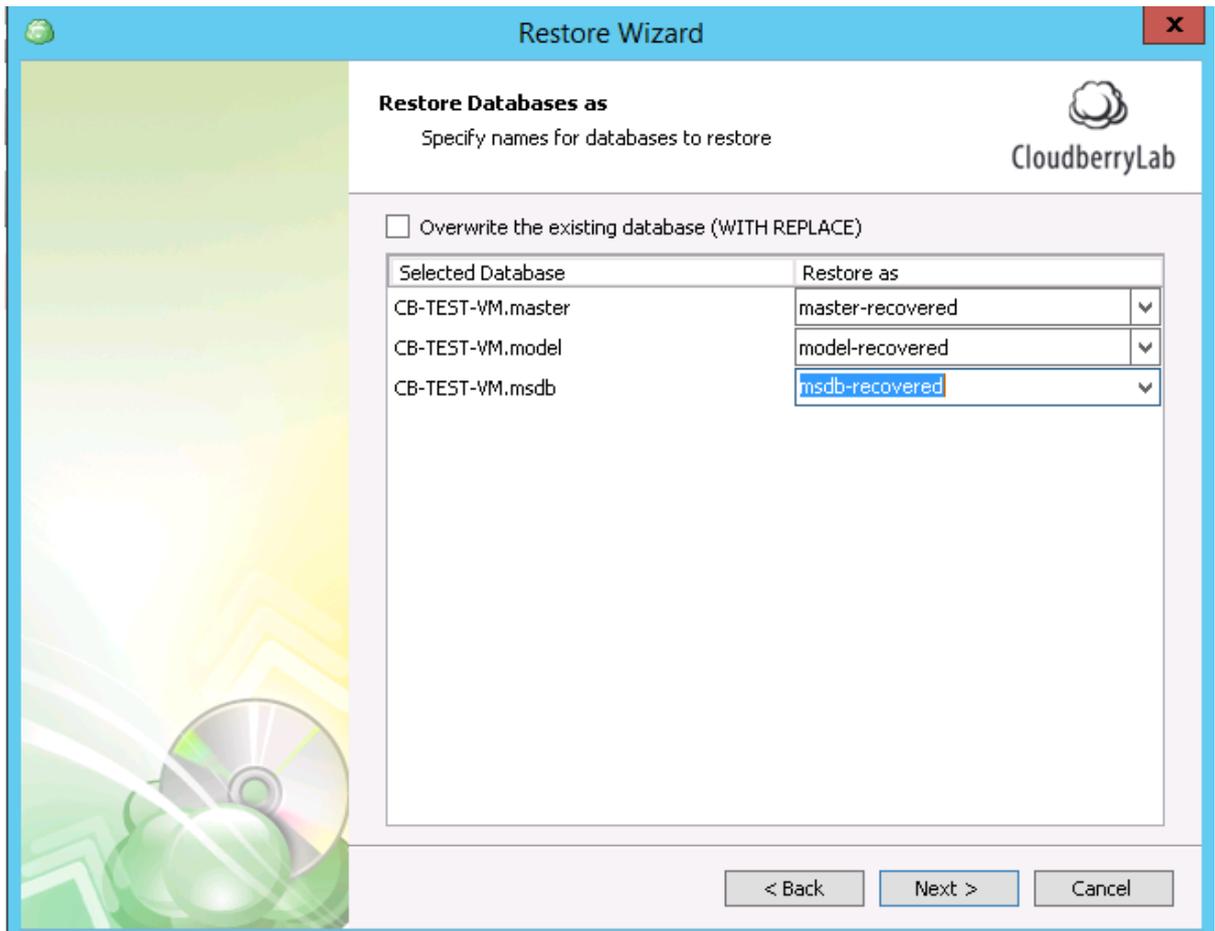


Keep in mind that the account must have SQL **sysadmin** role to perform the restoration. To verify it before proceeding, enable **Check if the specified account has necessary permissions to perform restore** option.

3. After selecting the instance, you can choose the databases for restoration.



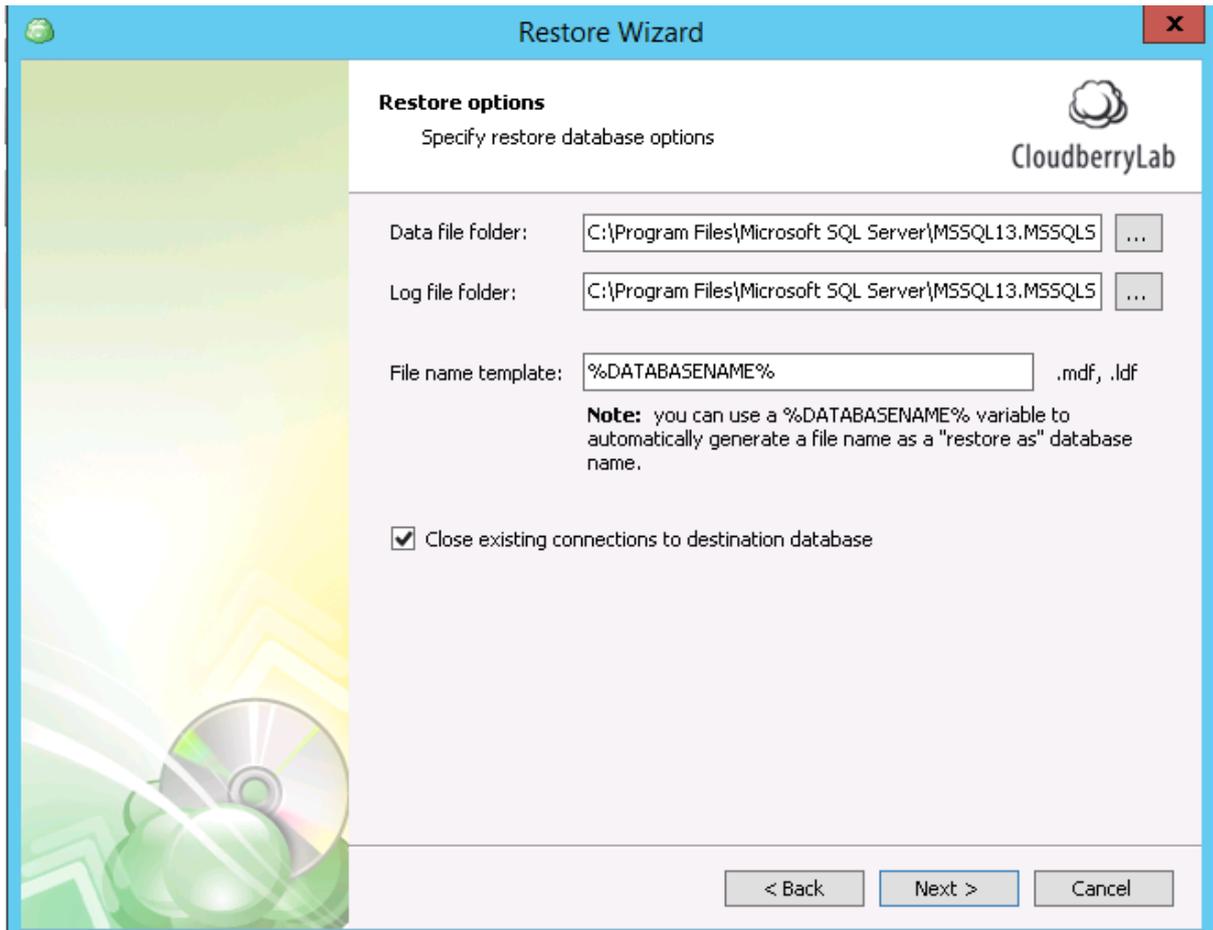
- Then you may specify names for recovered databases, or allow them to overwrite the existing ones. Renamed databases will attach automatically to the server.



- On the next step, you need to specify data and log file folders. By default, these are the folders of your active database. It's also possible to close connections to Microsoft SQL server



to avoid accidental data corruption while recovery.

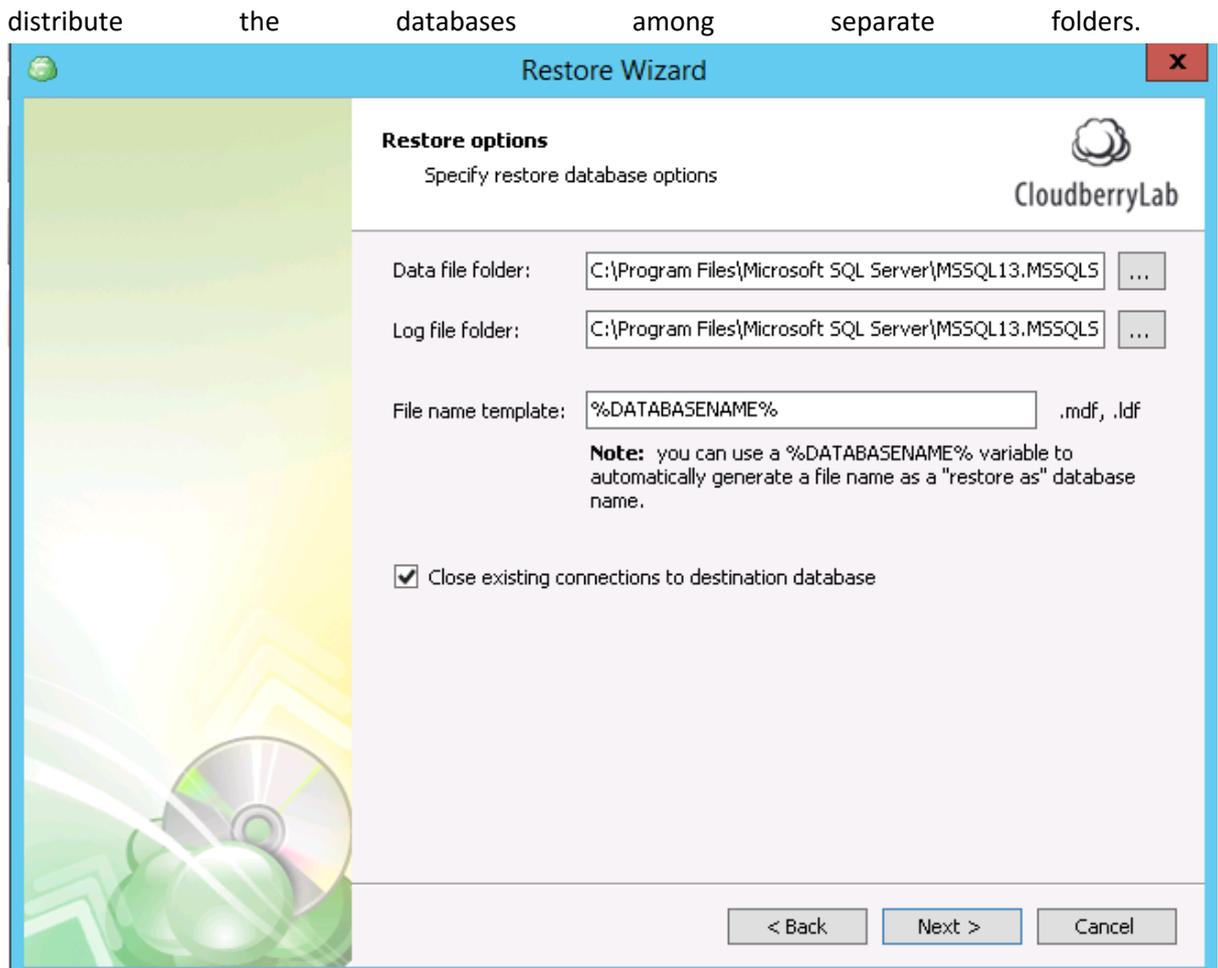


6. To finish the recovery configuration, set up notification and deciphering options. On the Summary screen, you'll see all the enabled tasks and options for restoration.

Restore Microsoft SQL Database Files

1. Firstly, specify the backup version and exact databases for recovery. On the **Restore Options** screen, select the **folder to save the files**. You can also create the file name template and





2. On the next steps, adjust notification and decryption options.
3. Then, you can attach downloaded databases to Microsoft SQL database engine. See the complete guide on the [Microsoft Developers Network page](#).

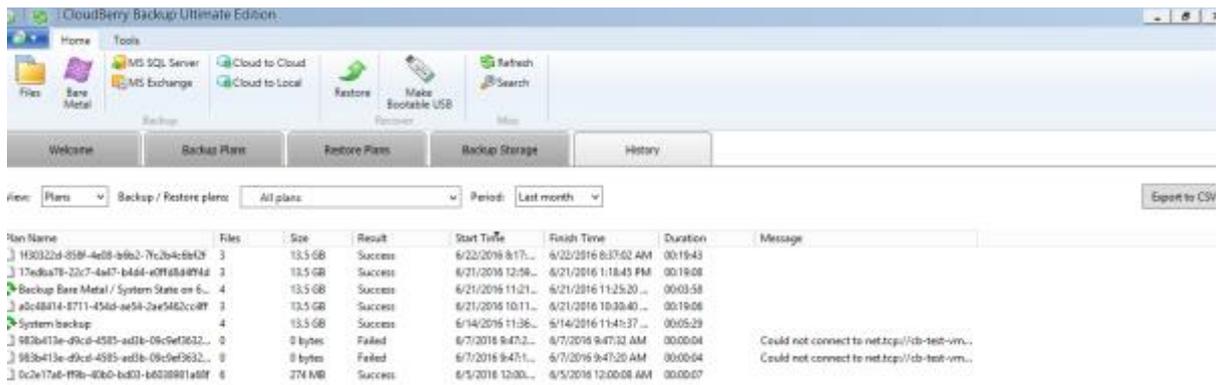
Additional Features

CloudBerry Backup provides a number of tools to keep in touch with the backup process and track down modifications made in the system.

History

The **History** tab contains an overview of a backup and restores operations for a chosen period: last day, last week or last month.

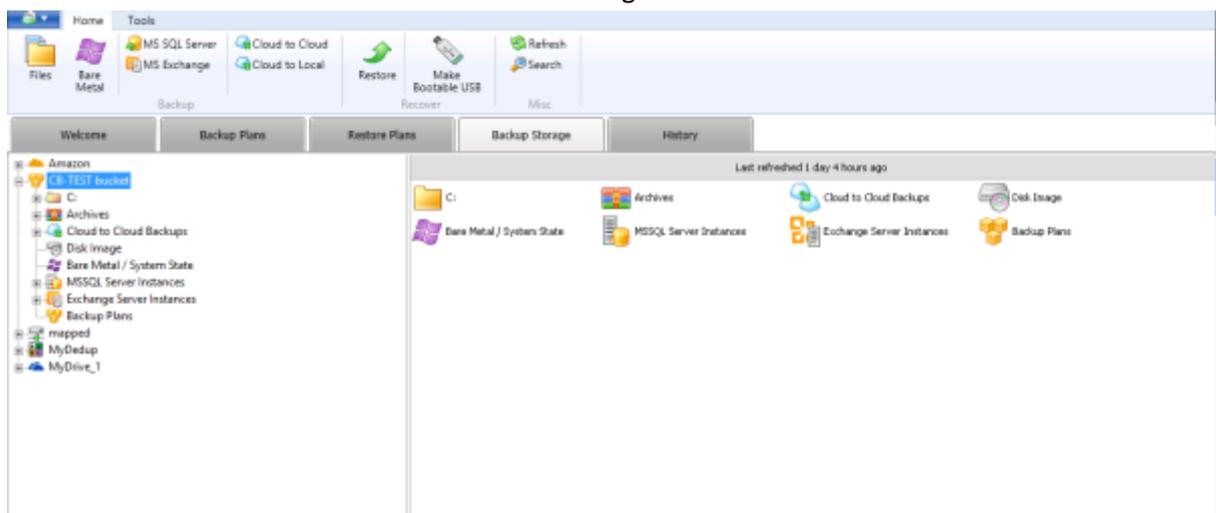




Here you can see how many files were transferred, how much traffic did it take, and also check a possible failure details. You can also export the data in comma-separated format using the button **Export to CSV**.

Backup Storage Explorer

Under **Backup Storage** tab, you can overview existing storage destinations. At the left, there is a list of cloud buckets previously registered in the CloudBerry client, as well as disks and servers available at the **working** instance.

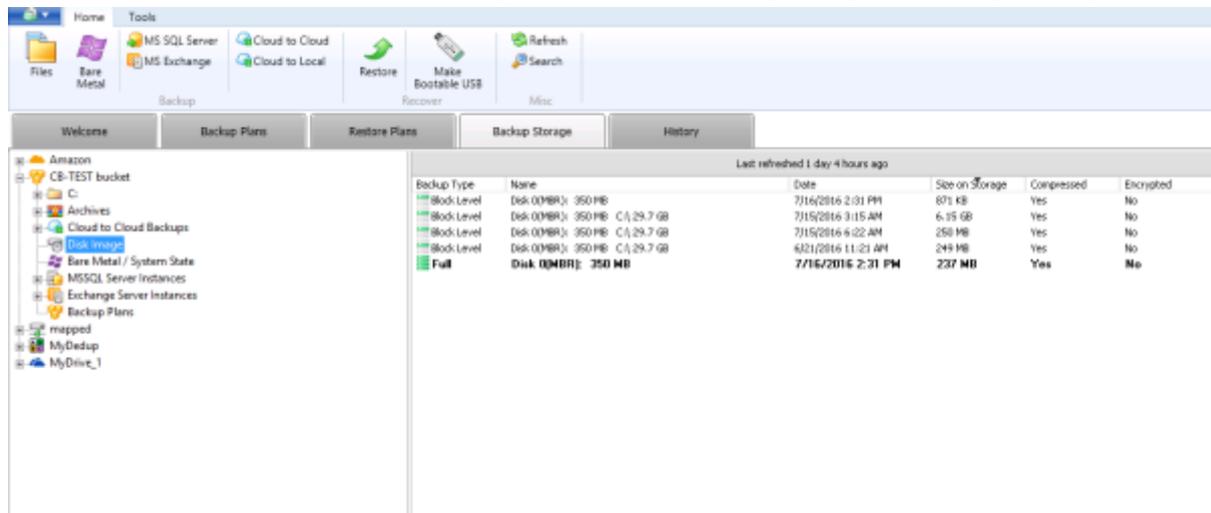


It has a number of useful features that make data backup experience better.



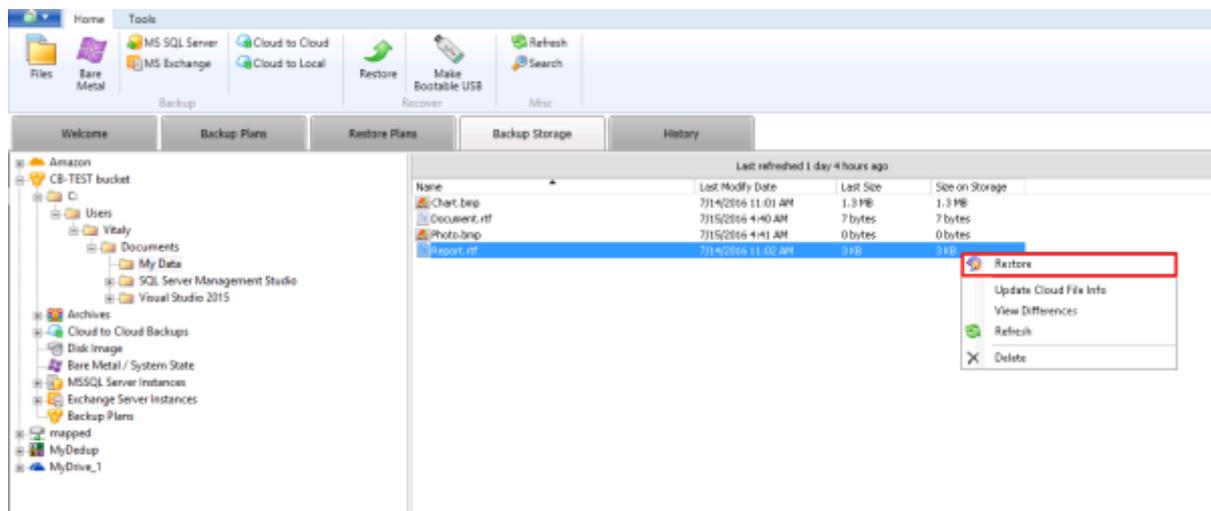
Block-Level Backup Monitor

If the selected item supports block-level backup, you can also see the list of its full and incremental backups. Click on the item in the management tree on the right (e.g. **Disk Image**) to open the list.



Manual Data Recovery

At the **Backup Storage** tab you can manually recover files. Just find the file you want to retrieve, right-click on it and choose **Restore** from the context menu.

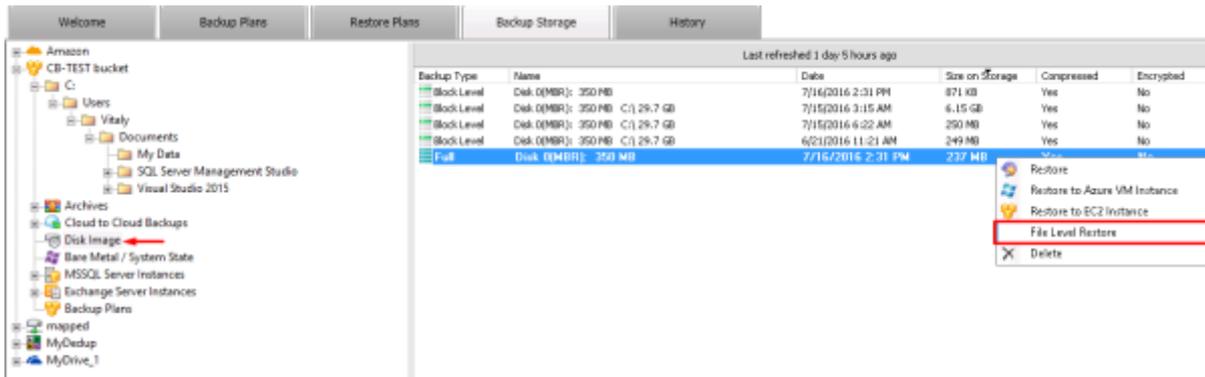


Recover Files from Backup Images

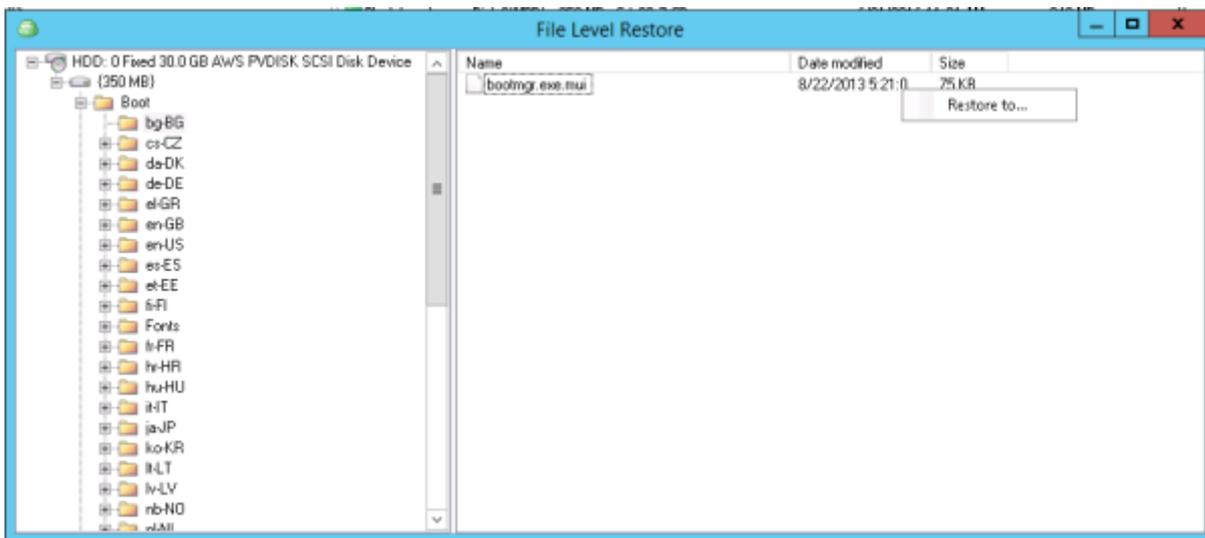
It's also possible to recover separate files and folders from the backup images:



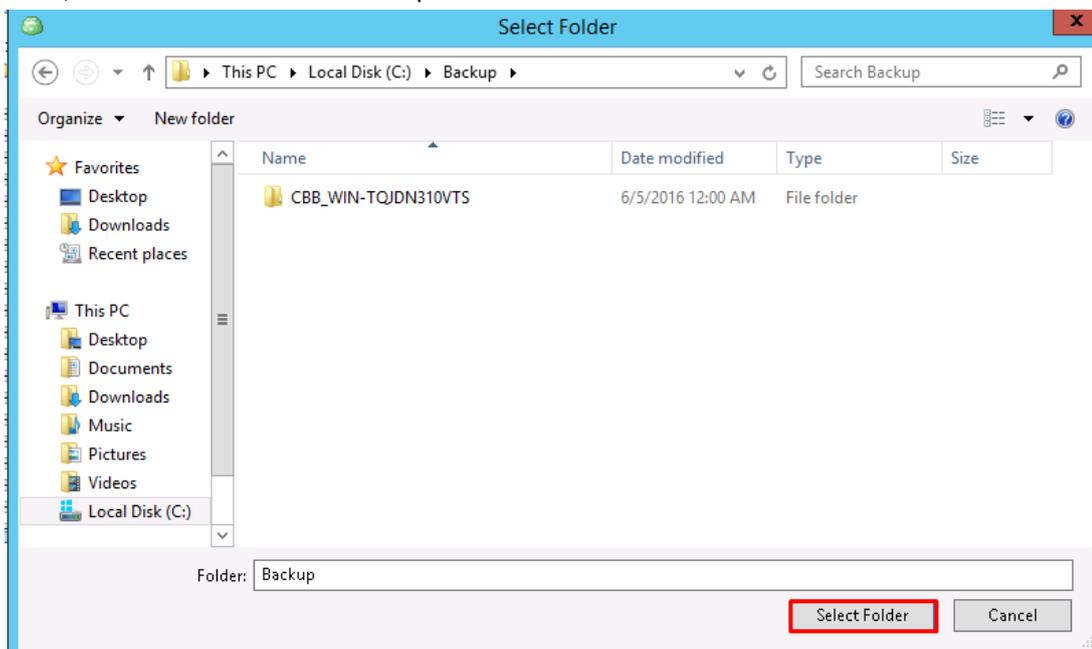
1. Switch to **Disk Image** section, right-click on the desired image and choose **File Level Restore**.



2. This will launch the relevant Wizard, where you can look through image contents. To recover the file or folder, right-click on it and select **Restore to...**.



3. Then, choose the place where to recover the data.

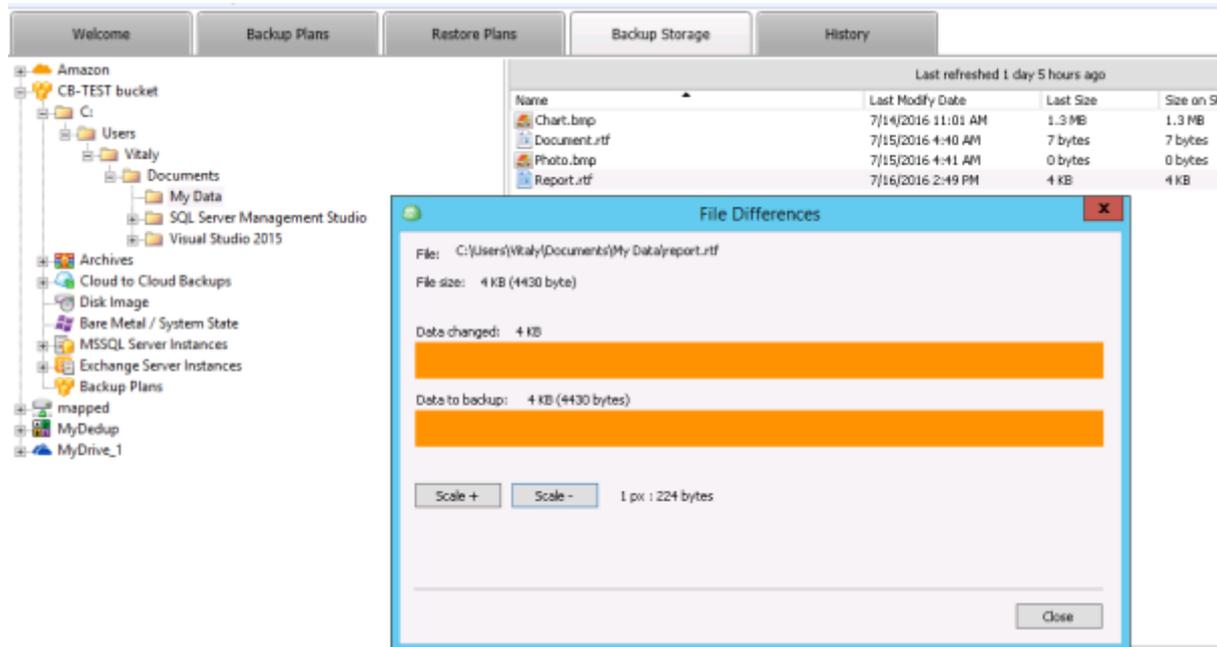


Press **Select Folder** button to complete the restoration.



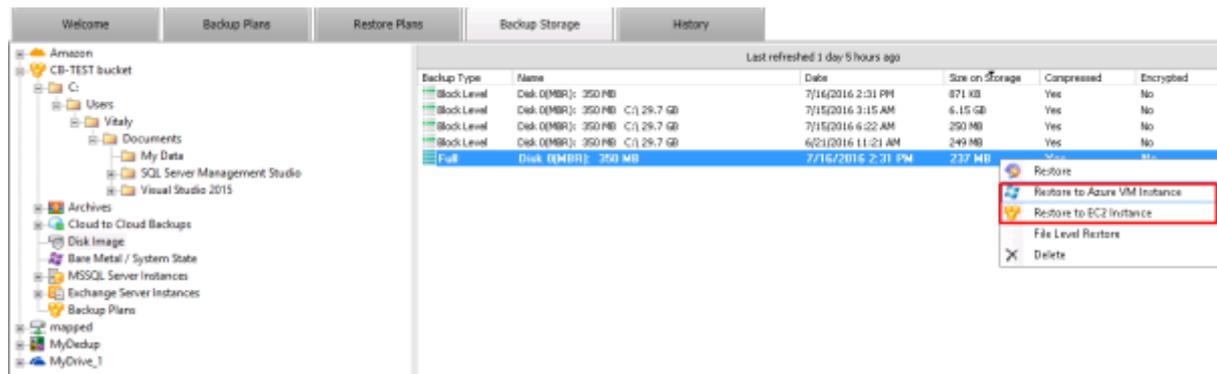
File Difference Monitor

You may also check if there were any item modifications. Right-click on the file, choose **View Difference** from the context menu, and CBB will compare the existing file and the file in the storage facility.



Manual Restore to the Virtual Machine

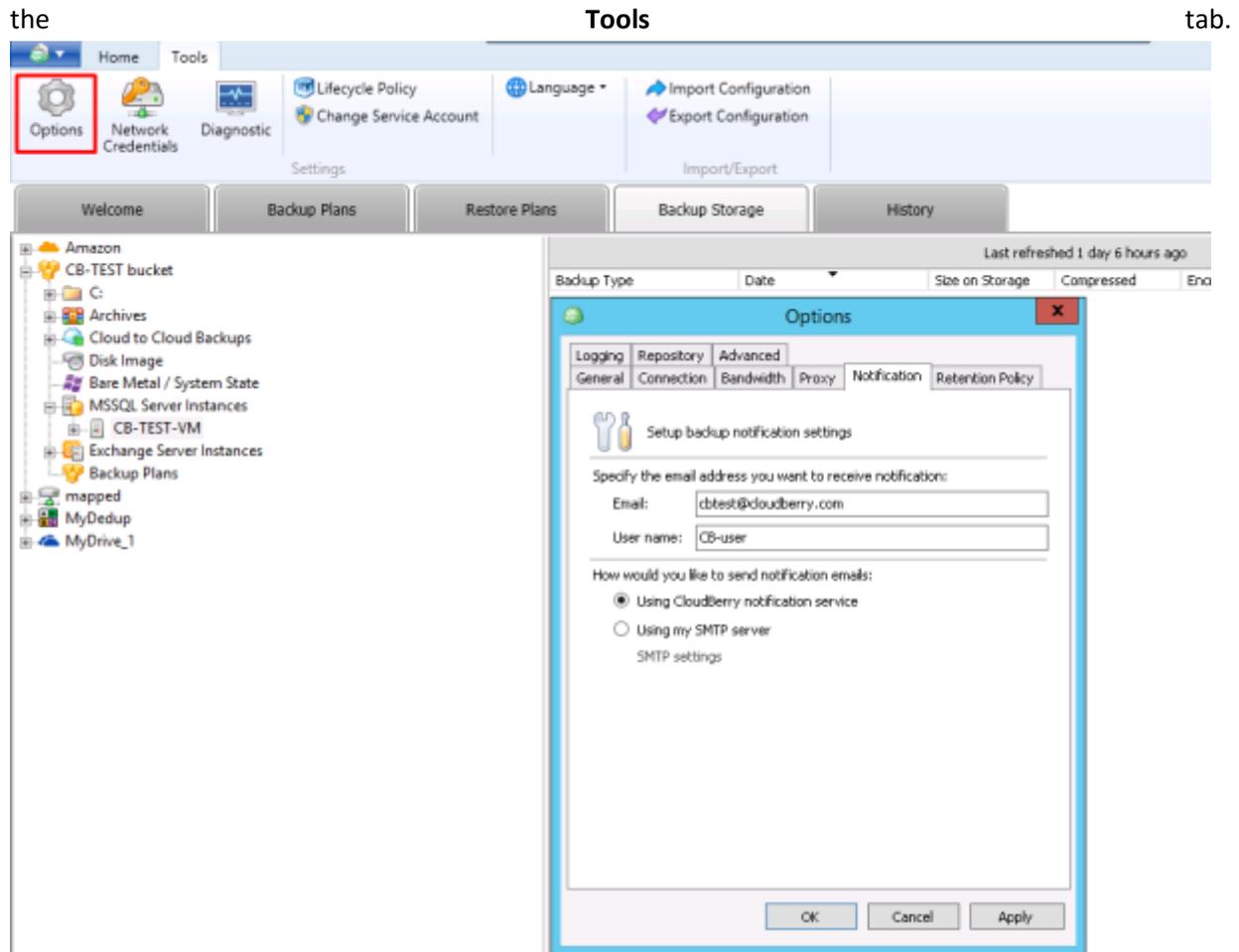
CBB can recover computer images as Azure VM or EC2 virtual machine straight away. Just right-click on the image and pick the desired variant to launch the deployment Wizard (described in **How to Restore – Image-level Restore – Image and Virtual Machine Restore** section). Proceed its steps to complete the recovery.



Email Notifications

CloudBerry Backup can also inform you about the backup progress via email. Notification policy can be configured for each backup plan, but you can also set up global settings in the **Options** menu under





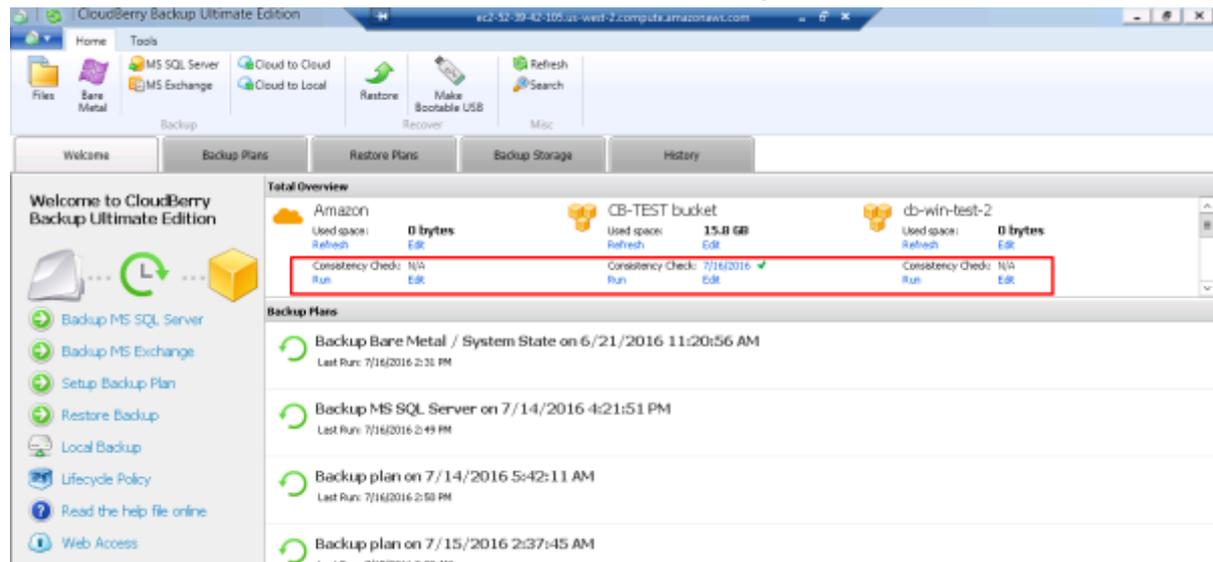
Here you can specify your email as a default option for new backup plans or mount an SMTP server. It's possible to use SSL (Secure Socket Layer) protocol to increase privacy level.

Consistency Check

You can increase the durability of your backup by using the **Consistency Check** feature. It checks the backup storage for file modifications made beyond CloudBerry Backup. Its interface displays under the



Welcome tab near the storage accounts overviews.



Press **Run** to see if everything is alright. If the backup data has been deleted or modified, Consistency Check status will change to the warning sign, and the exact consistency differences will display under the **History** tab.

Advanced Solutions

Nowadays, there is a great variety of IT-infrastructure configurations and data types, and its backup often requires sophisticated tools. CloudBerry Backup supports a variety of advanced features that can facilitate such tasks.

Big Data Transfer

Business often generates terabytes of data, which collects dust in the archive. It's easy to keep onsite, but uploading to the cloud storage is a good option that may be issued by network bandwidth. If you have 100TB of data, it may take 120 days to send them to the cloud storage via 100-Mbps channel, which is unaffordable for initial data seeding. In the real life, it would take even longer, because other corporate services also use bandwidth resources.

If you use Amazon Web Services (AWS), it is possible to accelerate data migration. There are a hardware solution **Amazon S3 Snowball** and networking improvement service called **S3 Transfer Acceleration**. CloudBerry Backup support both features, making transfer tasks convenient and efficient.

Amazon Snowball

Amazon Snowball is a hardware solution for an offline data transfer, which can fit up to 80TB of data per device. It connects to the local network via high-speed interfaces, has physical armor-case



protection and strong encryption. You don't need to purchase it – Amazon sends it to your place, and then you transfer it back to the datacenter. Find out details [on the official page](#).

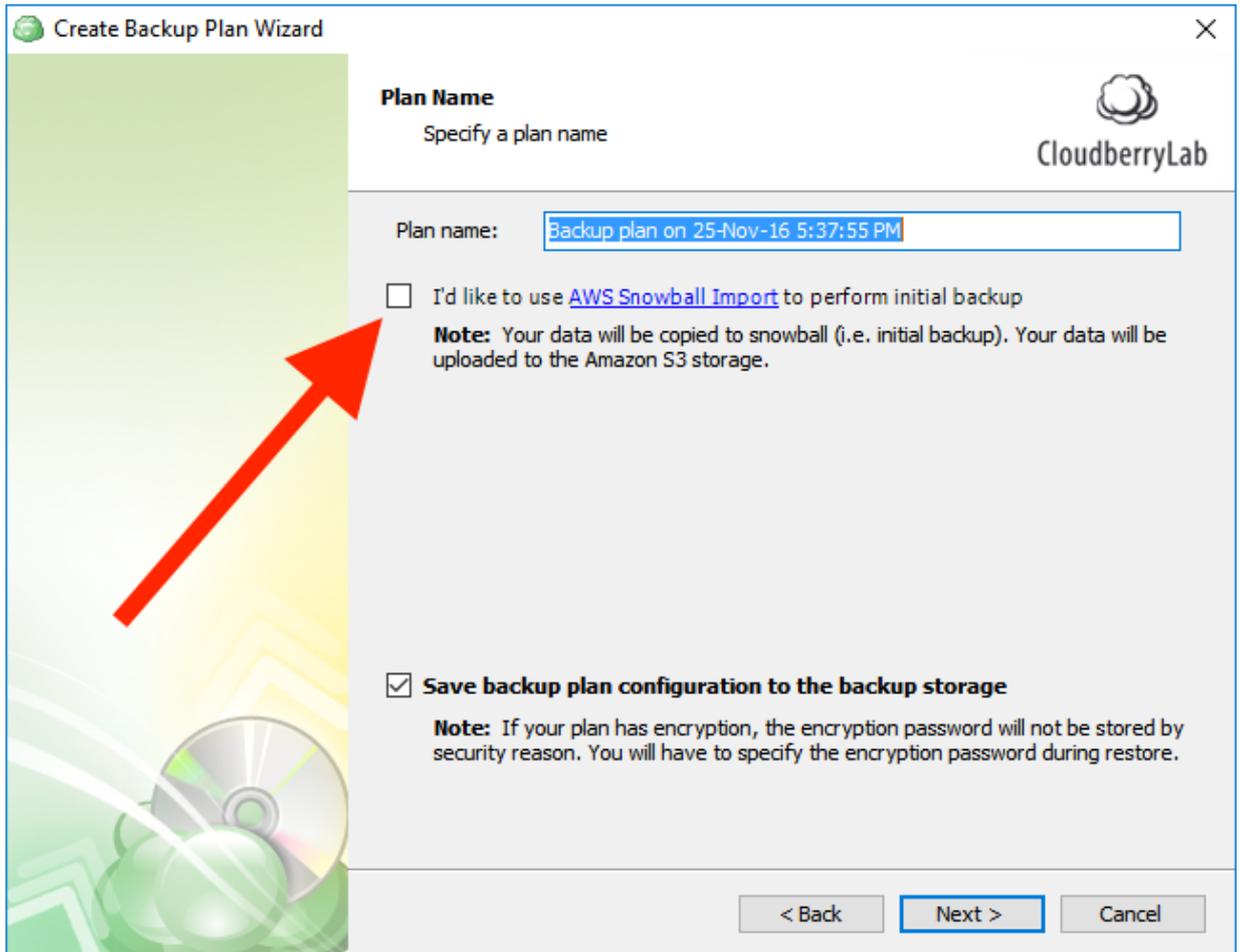
You can request Snowball via AWS Management Console ([press here to open the guide](#)) or via the CloudBerry Backup interface. CBB can also manage data import to Snowball device. It works on the file level, so make images and snapshots beforehand and place it on the local storage.

Here is a guide how to manage Snowball Export Job with CBB:

1. To create an export task, start **Create Backup Plan** Wizard for files, and choose or add **Amazon S3 storage** account on which you want to upload the data.

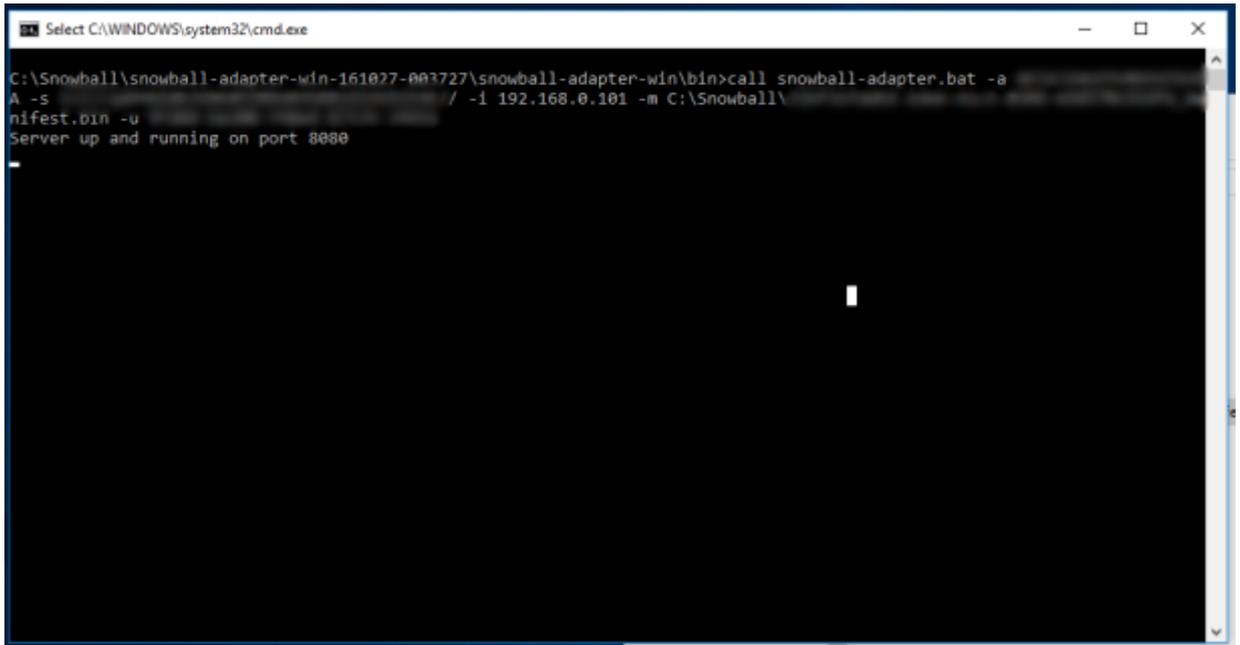


2. On the **Plan Name** step, choose the "I'd like to use **AWS Import / Export** feature to make **initial backup**" option.



3. Specify the data for backup and configure other options like file-filter and notifications.
Note: *compression and encryption won't work with Snowball because it uses its own equivalents. Schedule option doesn't make sense either; moreover, it can corrupt the data on the attached Snowball device.*
4. Continue setting up the plan. Soon enough you'll reach the **AWS Snowball** step that describes further procedures. Click on the link in step №2 to download Amazon S3 adapter. Once downloaded, unzip it and launch the command line. Navigate to the folder that contains Amazon S3 adapter and execute the following command:





```
Select C:\WINDOWS\system32\cmd.exe
C:\Snowball\snowball-adapter-win-161077-00727\snowball-adapter-win\bin>call snowball-adapter.bat -a [redacted]
A -s [redacted] / -i 192.168.0.101 -m C:\Snowball\
manifest.bin -u [redacted]
Server up and running on port 8080
```

where:

- **-a** and **-s** are the **access and security keys**, respectively.
- **-i** is the IP address (can be looked up on the box)
- **-m** and **-u** are the **path to the manifest file and the client unlock code**, respectively. Both of these can be found in your **AWS Console**.

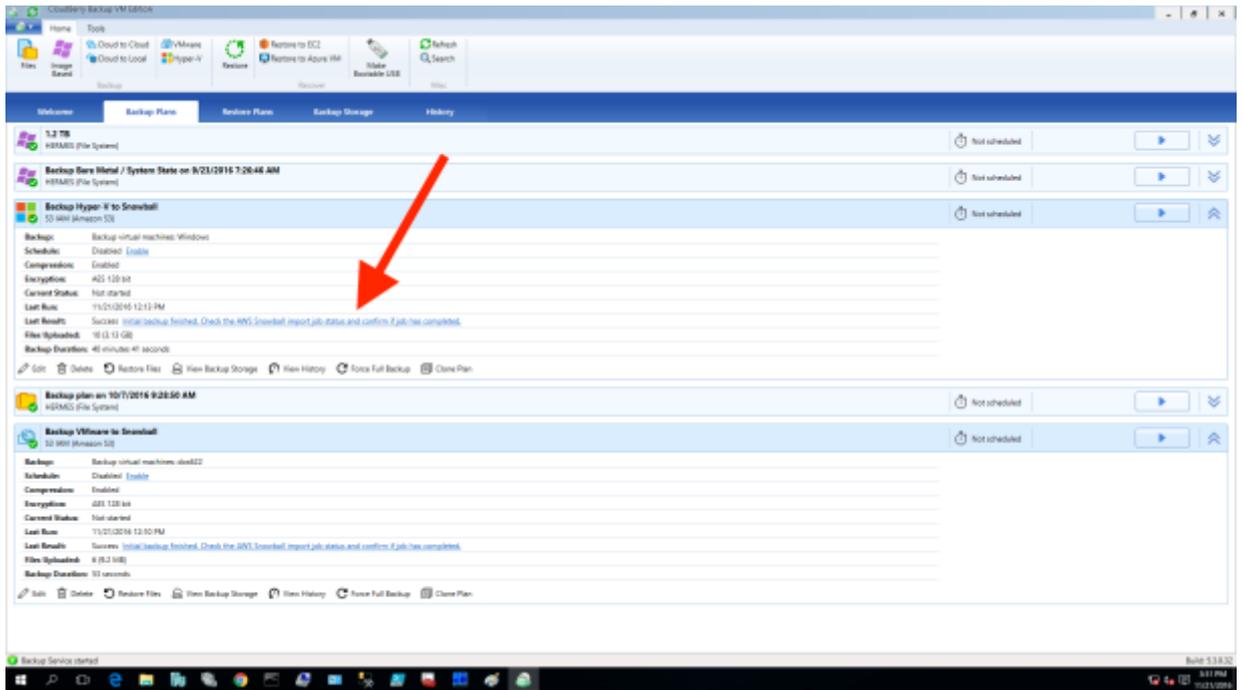
If you've done everything correctly, you should see a message in the terminal akin to **"Server up and running on port 8080"**.

Do not close the command line! It should be running all throughout the process. Now go back to CloudBerry Backup and conclude setting up the backup plan. Upon finishing, run it and wait for it to complete.

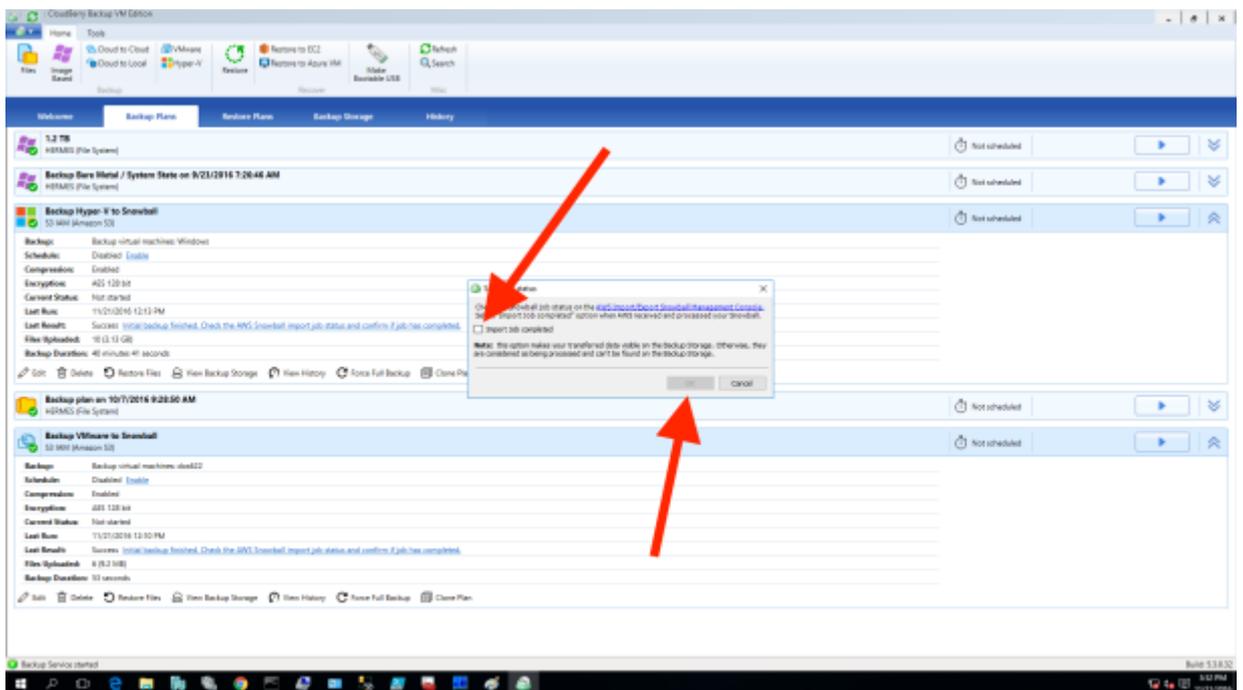
When the data has been successfully transferred to the AWS Snowball, ship the box back to Amazon. When they notify you of your data having been moved to your bucket, go ahead and confirm it in CloudBerry Backup. Click on **"Initial backup finished..."**.



CloudBerry Backup Installation and Configuration Guide



Select the **Import Job Completed** checkbox and click **OK**.



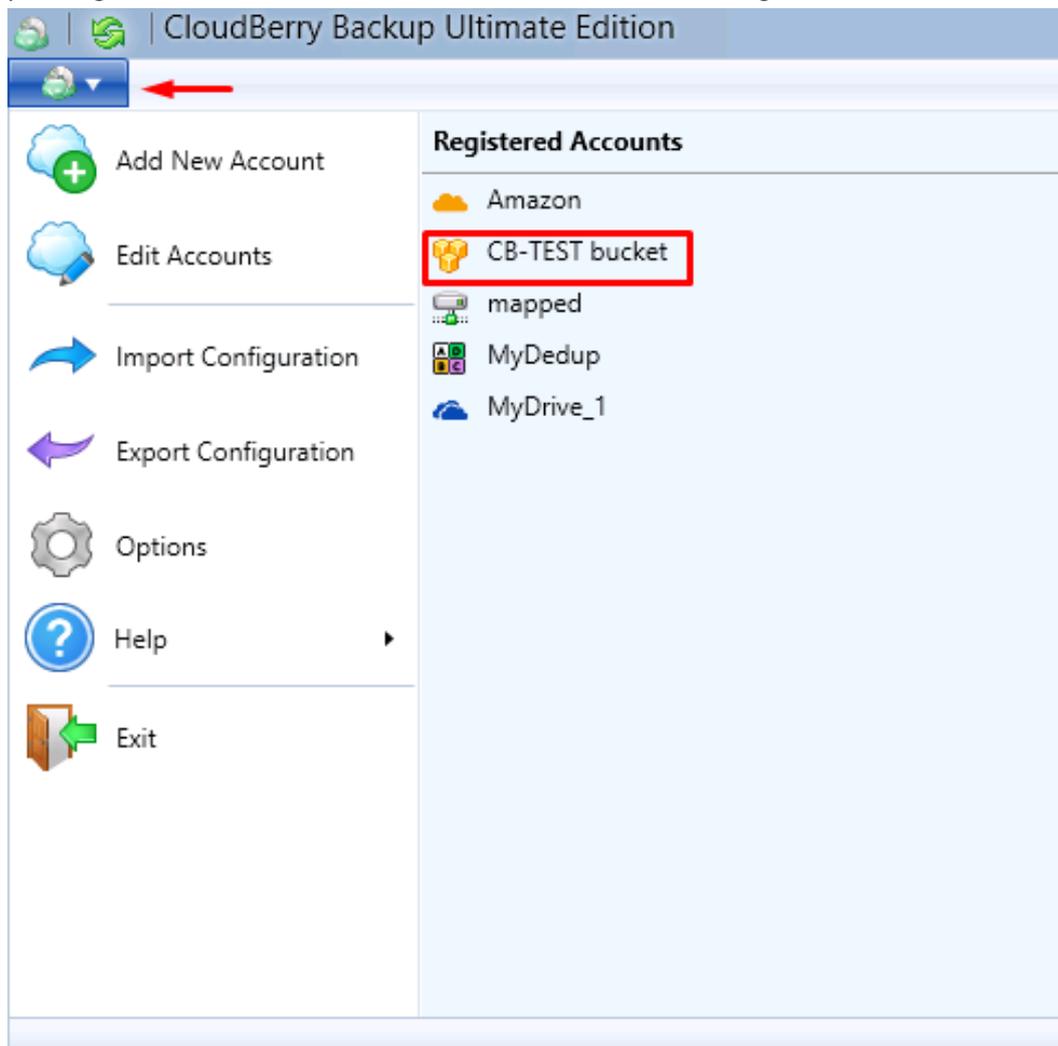
Your files are now being renamed in the cloud. This process takes place because of certain peculiarities of CloudBerry Backup and the way our software works with file structures. Afterward, there is nothing else to be done! Voila! Your initial backup has been successfully performed with the help of AWS Snowball. All future backups will be performed as usual from your PC into the cloud by means of CloudBerry Backup.

NB: Do NOT Sync Repository before the files are all renamed in the cloud. This may lead to unintended repercussions.

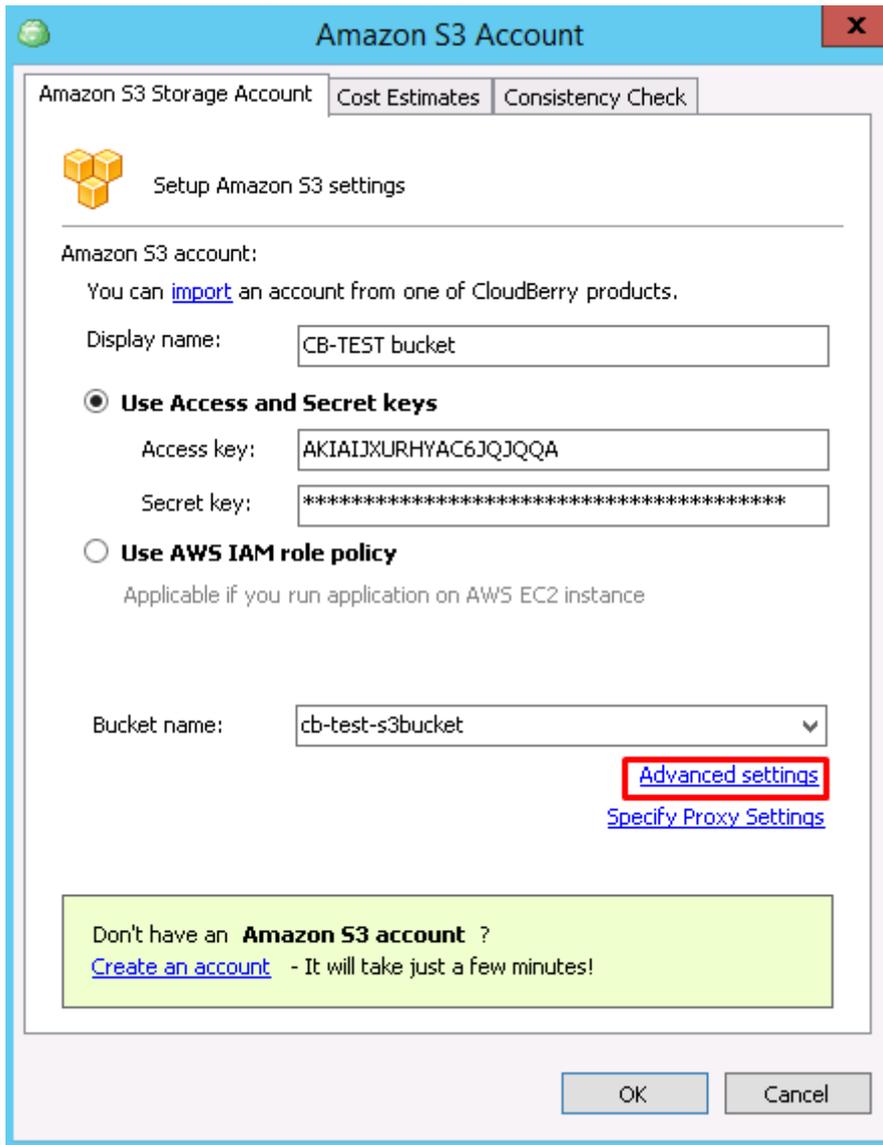
AWS S3 Transfer Acceleration

Amazon S3 Transfer Acceleration is a bandwidth speed-up solution, which can make the connection with the data center up to 6 times faster. The acceleration is achieved by using the optimized network routes between Amazon S3 storage facilities and AWS Edge Locations. Find out more information on [AWS S3 FAQ page](#).

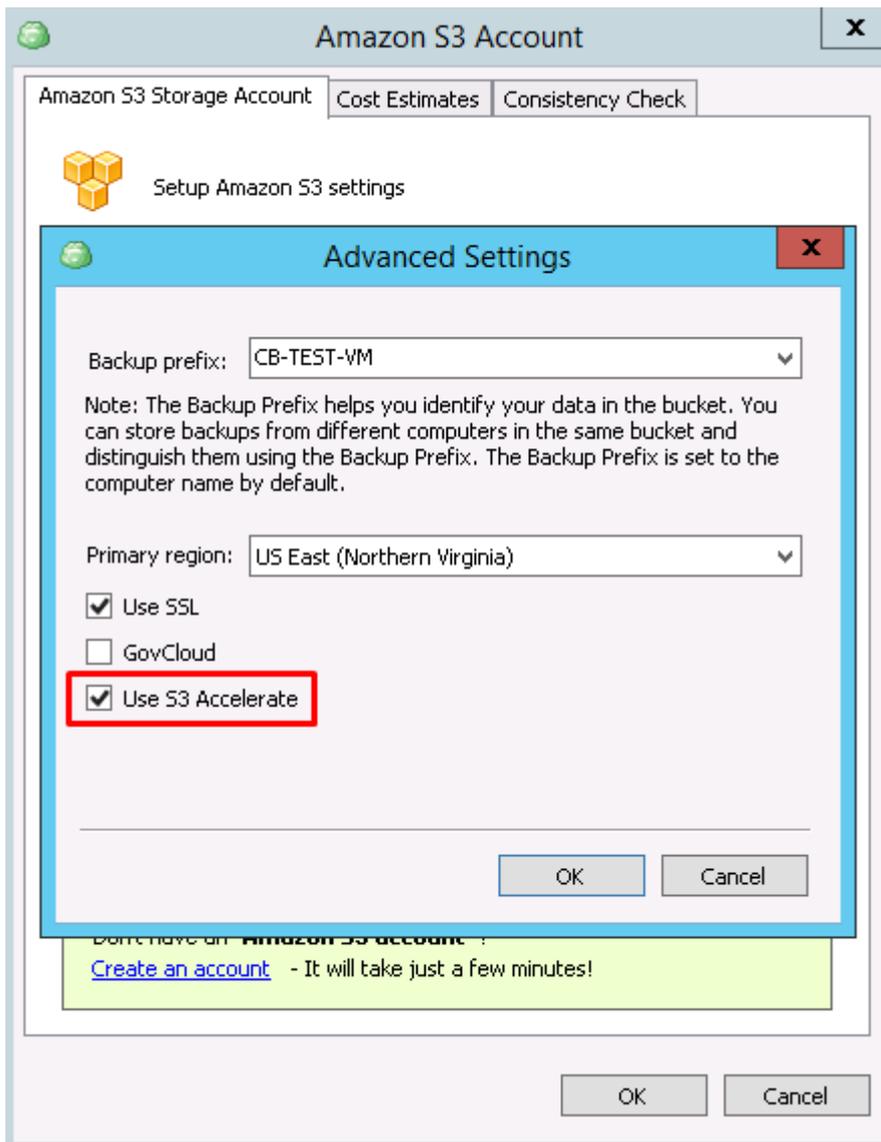
1. You can enable Transfer Acceleration for any of S3 buckets registered in CloudBerry Backup by pressing the **Main Menu** button and selecting the relevant account.



2. On the configuration page, choose **Advanced settings** option.



- Click on the **Use S3 Accelerate** box. Now Transfer Acceleration is enabled.



You can switch it off in the CBB Account options or via Amazon Management Console.

Archive to Glacier and Lifecycle Policies

If you use AWS services, you can make a profit of storing the archive data on the [Amazon Glacier](#). It's a low-cost storage for infrequently accessed data. The point is that one cannot access data on Glacier immediately – it may take 3-5 hours to create the link. The data can automatically move to Glacier from other AWS facilities according Lifecycle Policies. [Find out more about this feature on the AWS page.](#)

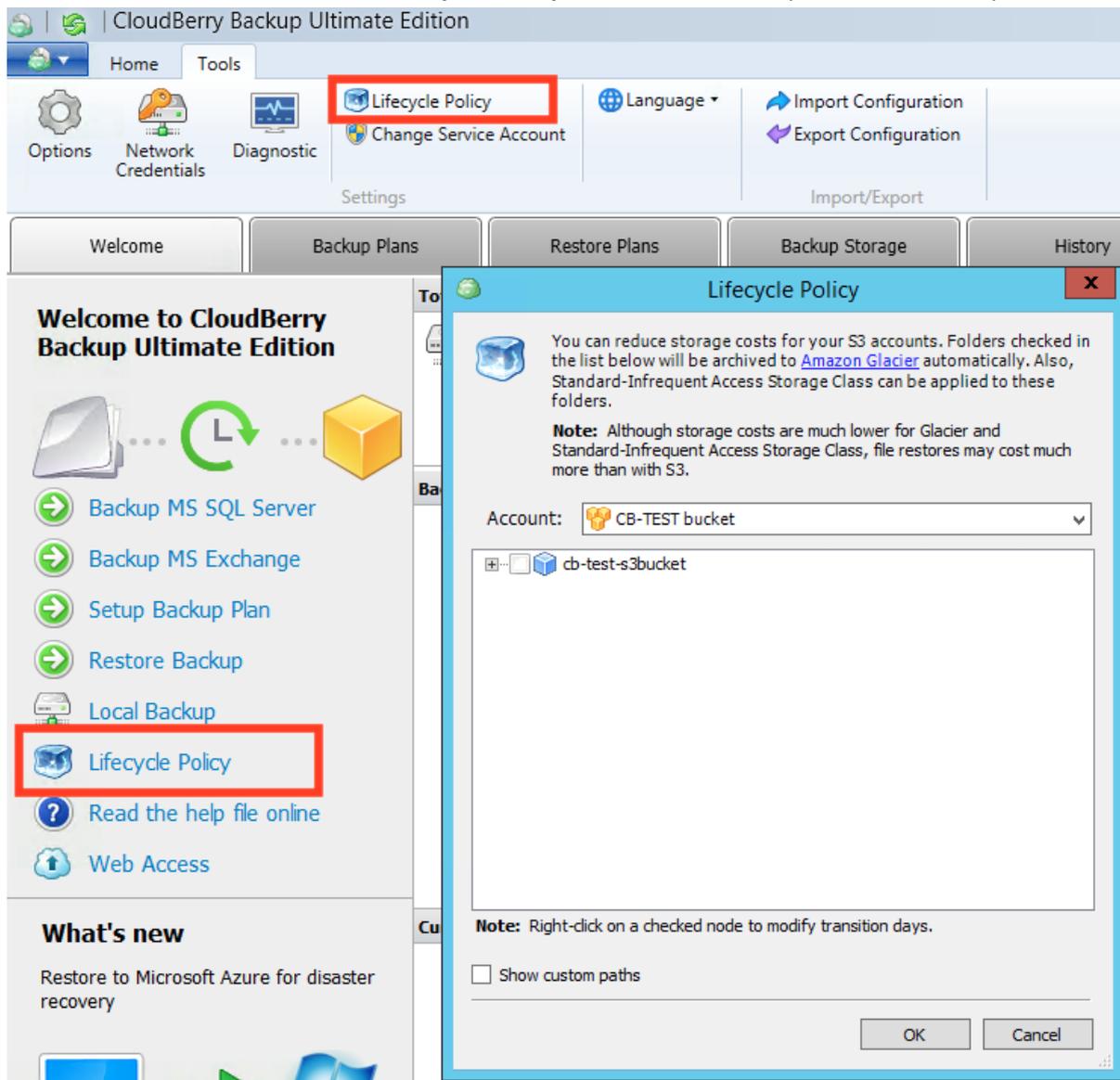
CloudBerry Backup supports native AWS Lifecycle Policies feature, so CBB settings won't conflict with Amazon Management Console presets. It's also possible to upload data directly to the Glacier.



How to Configure Lifecycle Policies

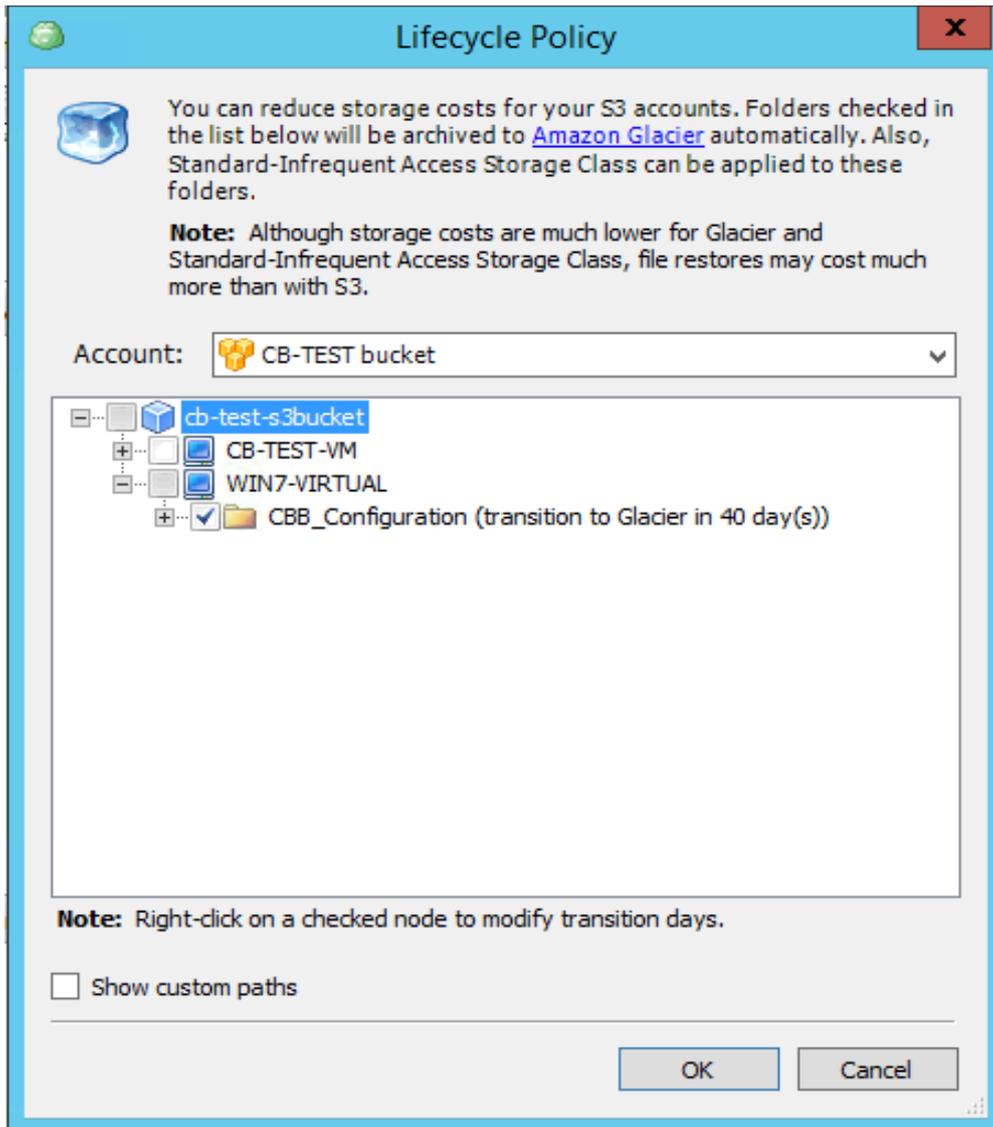
Here is a guide on transferring data to Amazon Glacier using CloudBerry Backup user interface:

1. Go to the **Tools** menu and click **Lifecycle Policy** or use the same option on the left panel.



2. Use **Lifecycle Policy** dialog window to choose data to be automatically uploaded to Amazon Glacier. It is possible to specify transition timeouts for each item and choose source data to be transferred to Amazon IA storage first (here is the [article about Amazon storage classes](#)).



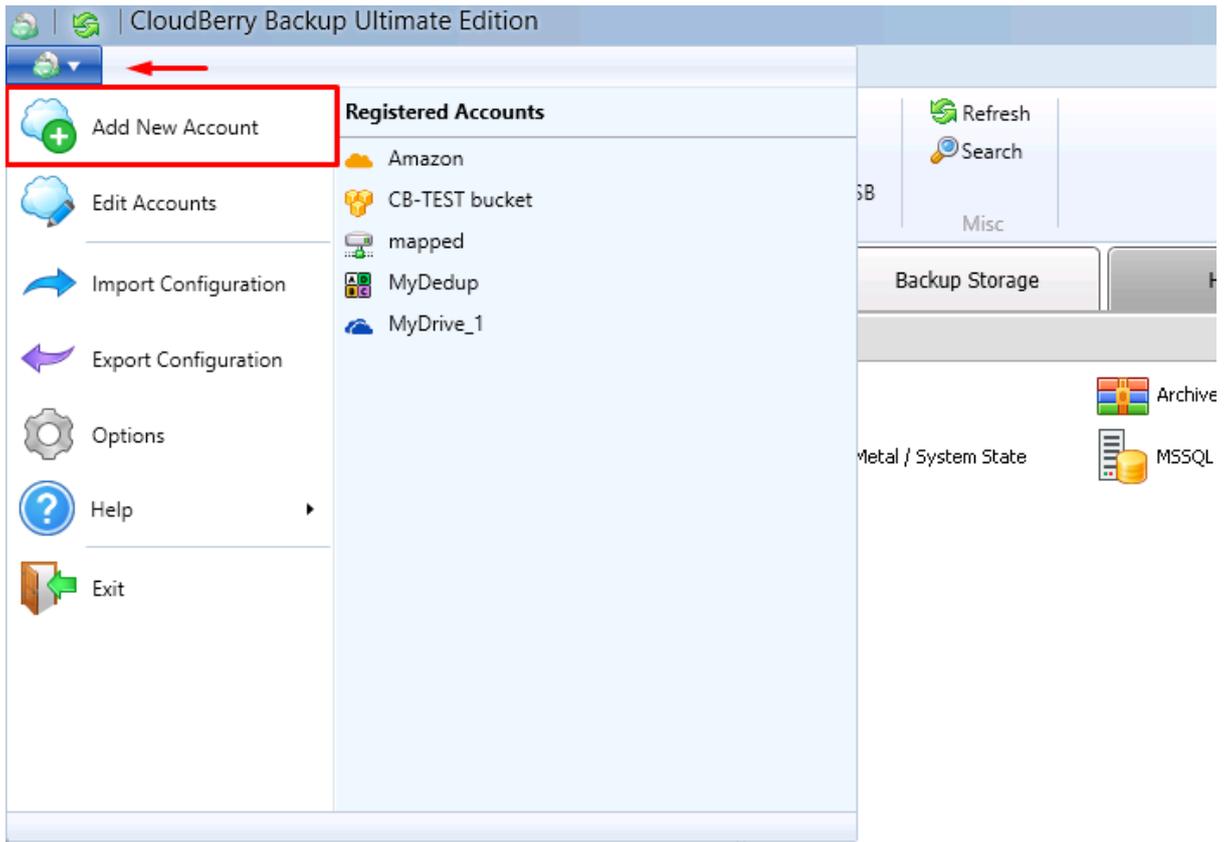


After completion of the transfer operation, the backups will appear in the Archives section. From Amazon AWS control panel perspective, the data transferred are not displayed in Glacier storage, but it is still available in the S3 bucket.

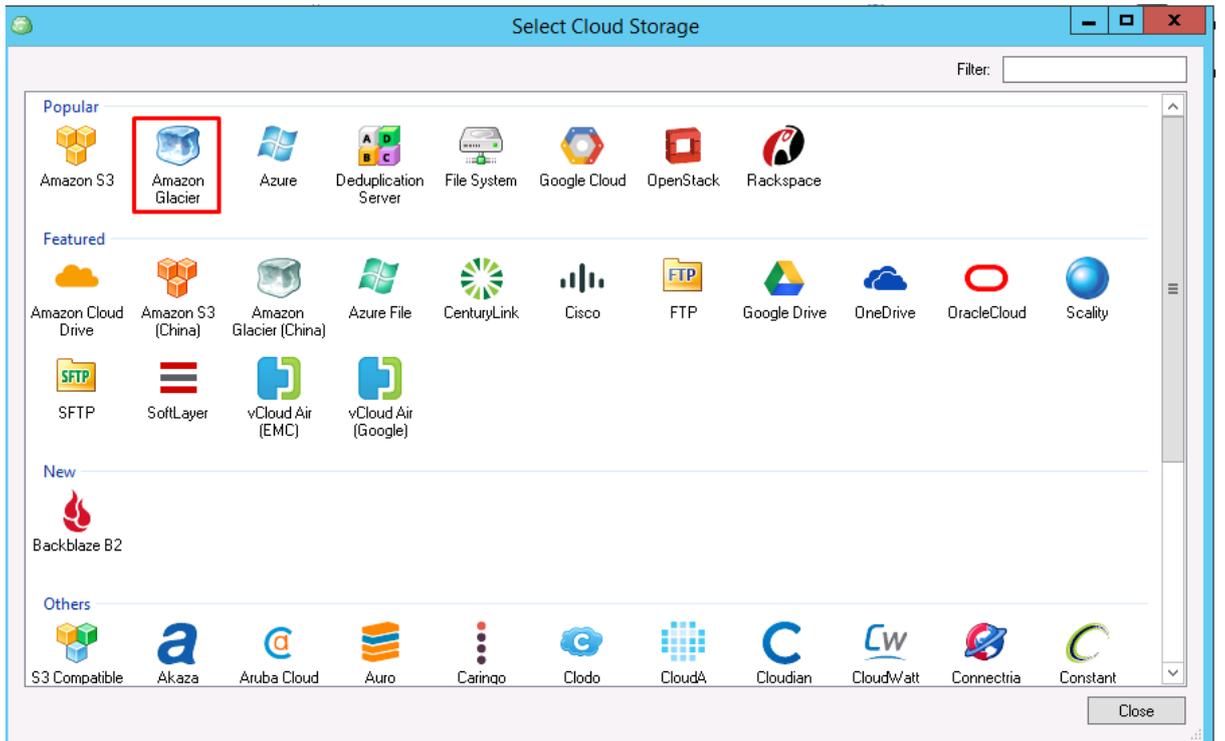
Backup to Glacier

You can also set up Glacier as a standard CloudBerry Backup storage:

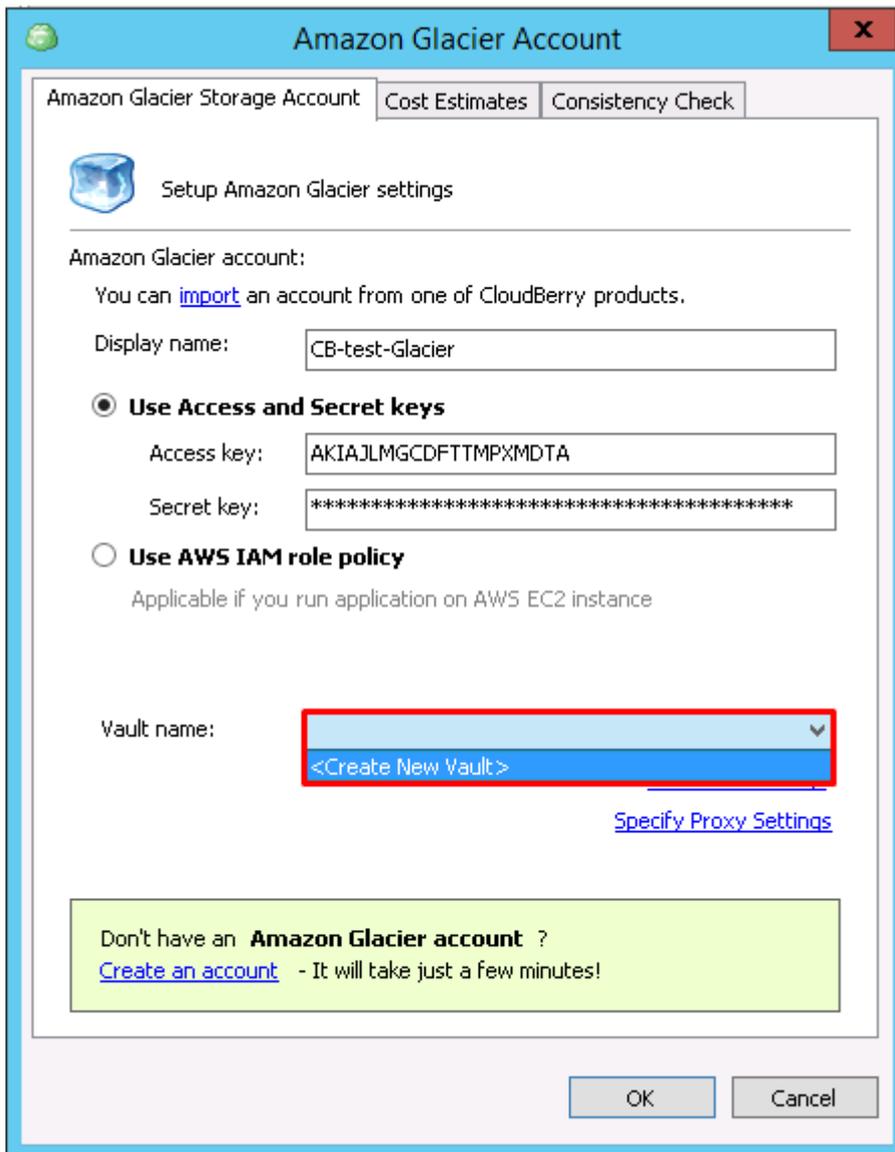
1. Click on the **Main Menu** button and choose **Add New Account**.



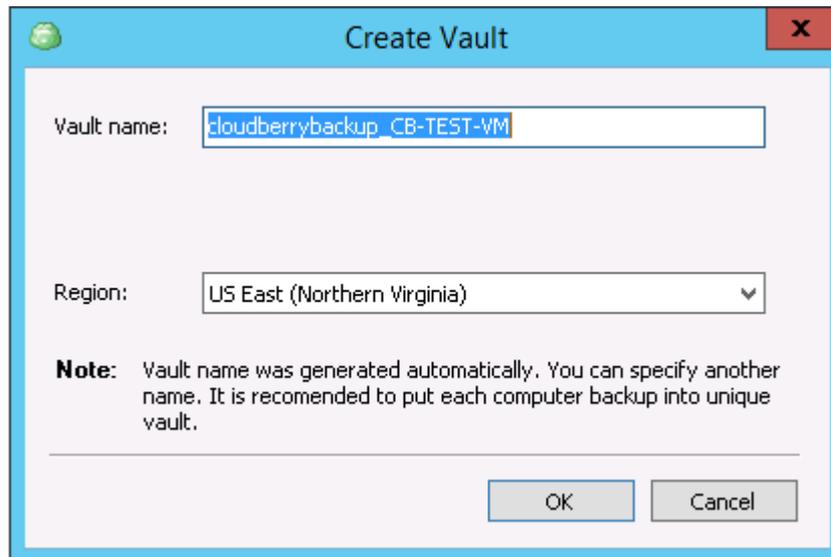
2. Select **Amazon Glacier** storage facility.



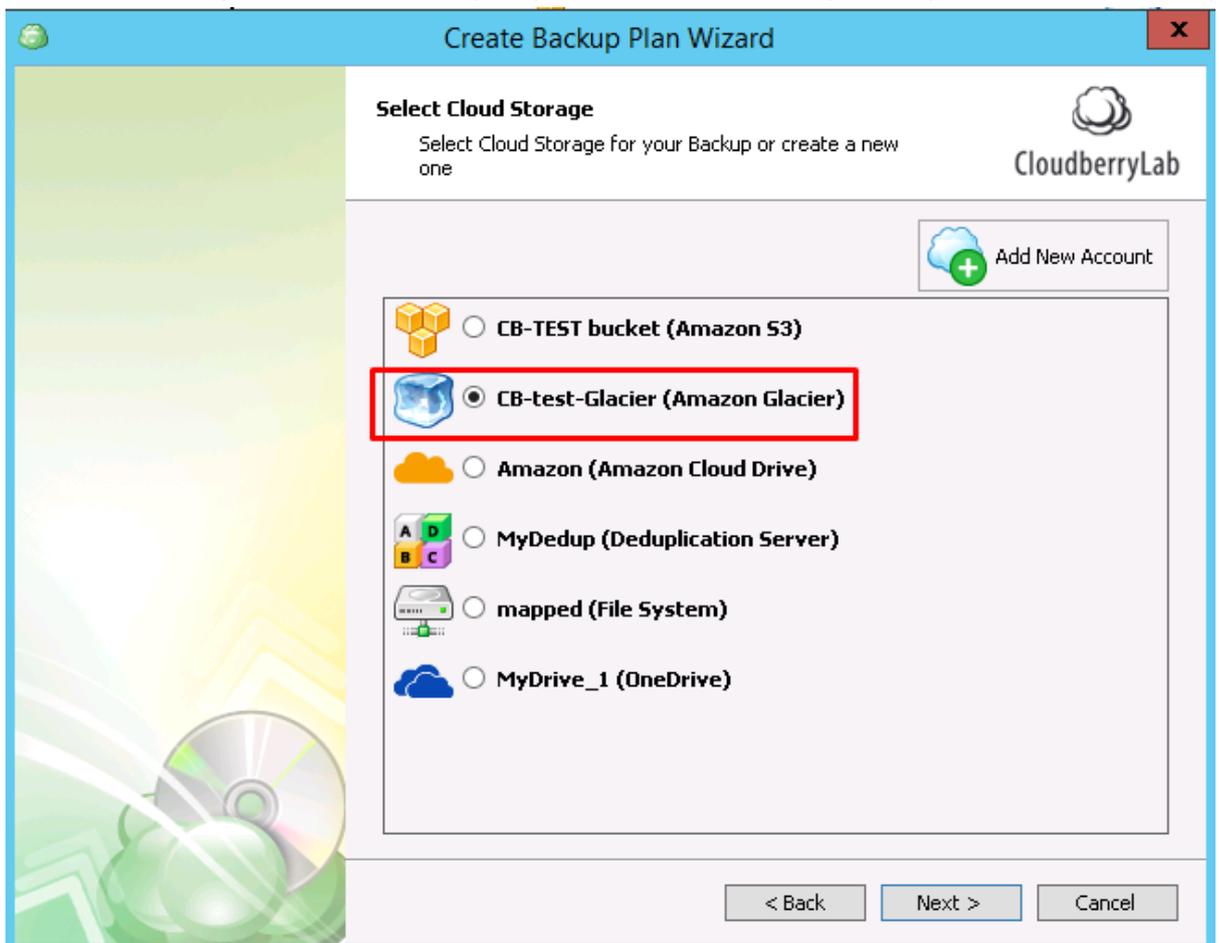
3. On the next step, specify the AWS account credentials and select the Glacier vault.



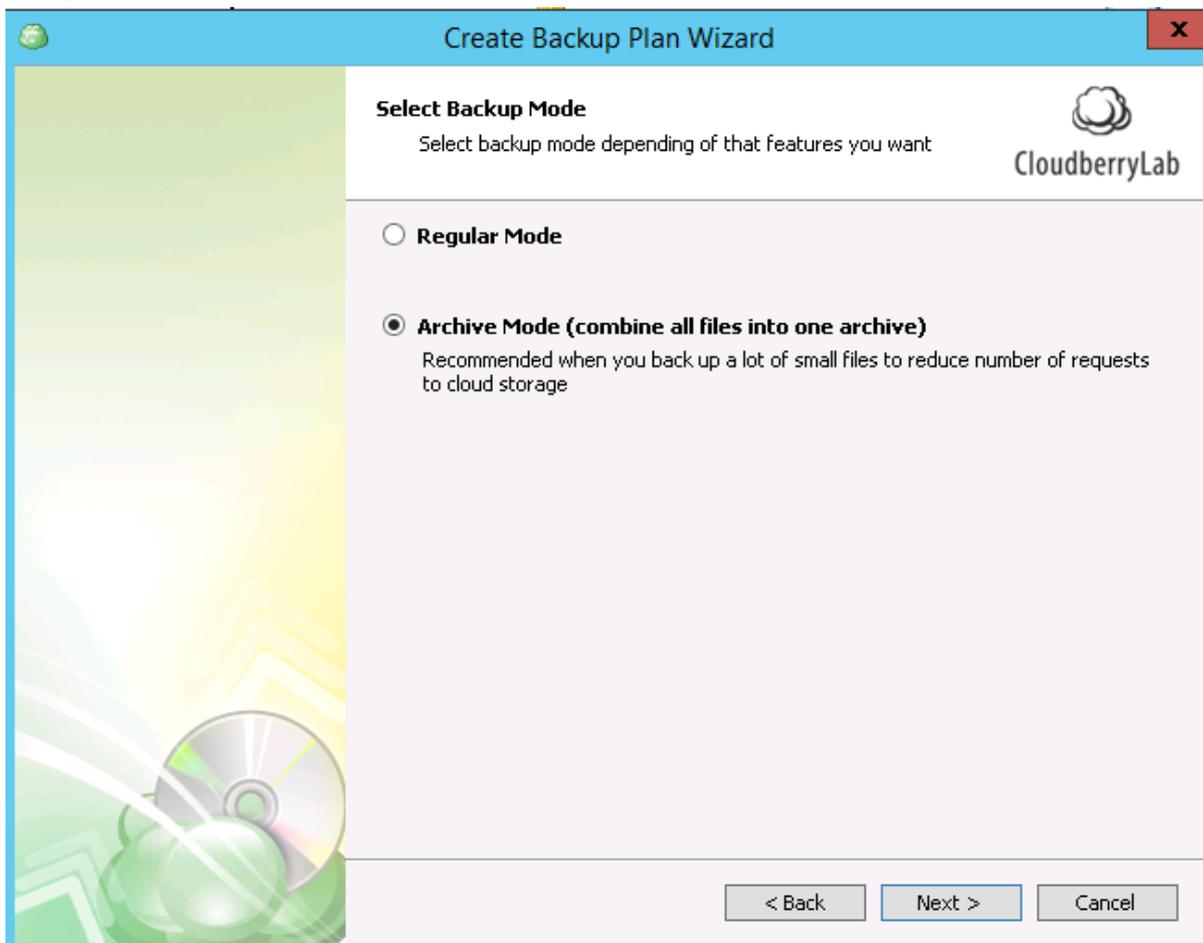
- a. If you don't have a vault yet, you can create a new one from CBB interface. Press on **Create New Vault** and choose its name and location region.



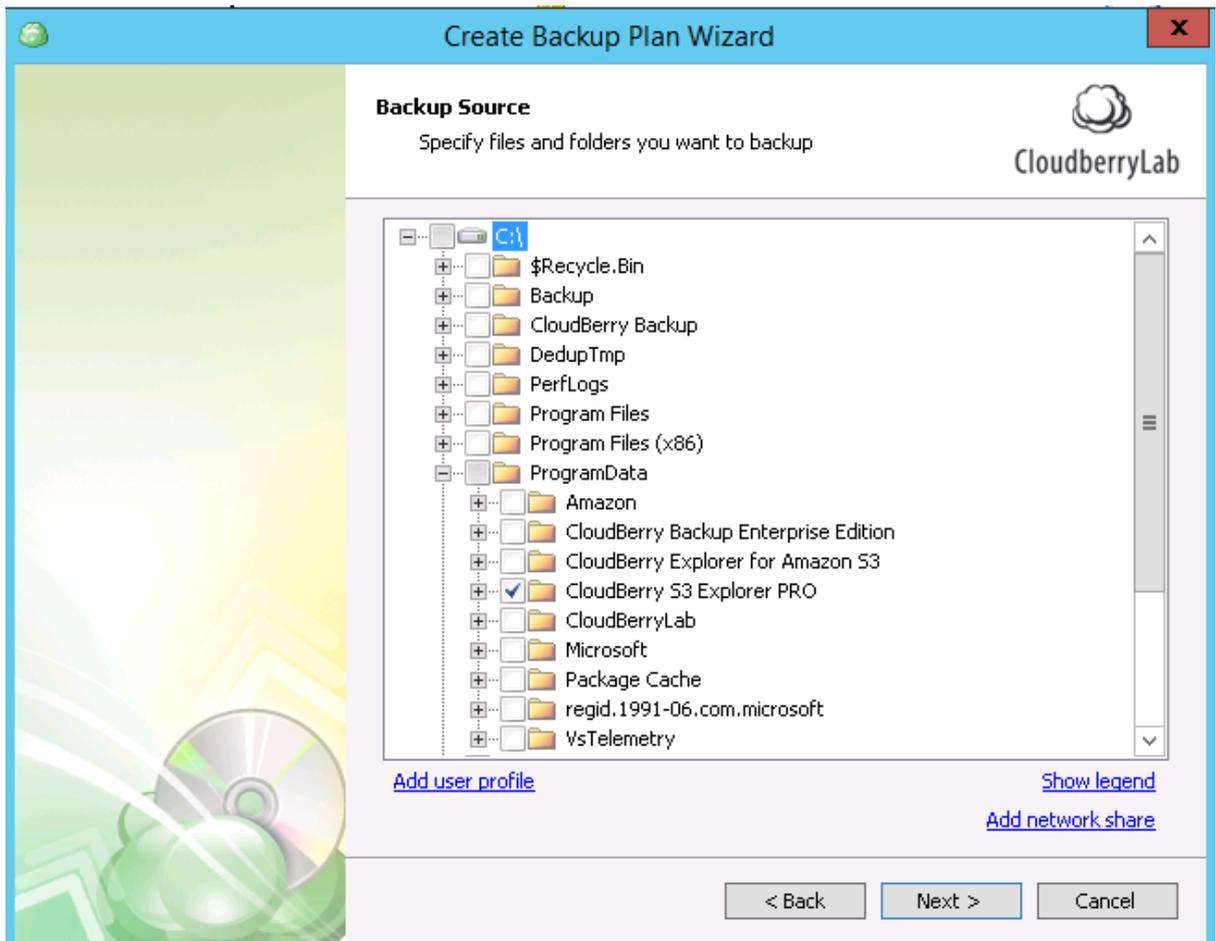
4. If you have made backups to this vault before, it will take 3-5 hours to synchronize repositories. If no, the Glacier account will appear immediately, and you are ready to create a Backup Plan.
5. Press **Setup Backup Plan** at the **Welcome** tab to start the Wizard. Choose Glacier account as a cloud storage and specify the backup plan name.



6. On the next step, choose the backup mode. On the **Regular Mode**, files will be uploaded separately. On the **Archive Mode**, data will be compressed in the one file to save on requests charge.



7. Then, specify the files for backup.

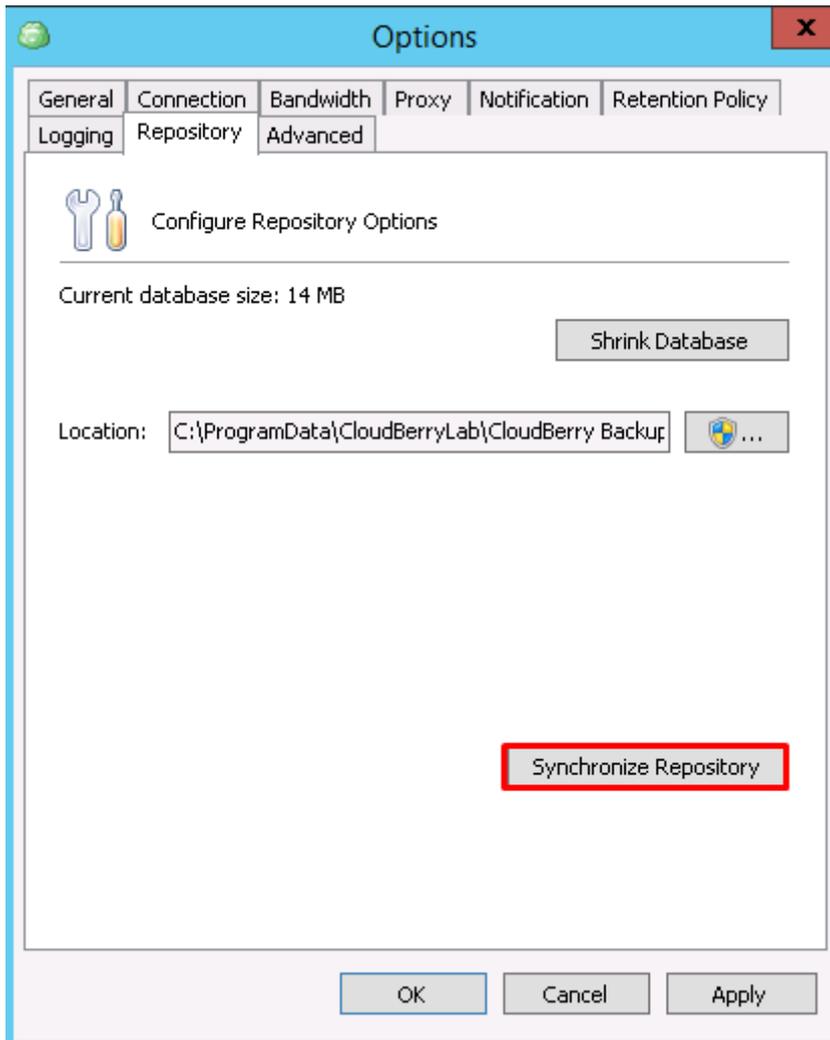


8. Configure others options like encryption, compression, e-mail notifications, etc., and launch the backup plan to upload the data to Glacier.

Glacier Restore

If Glacier storage hasn't been used for backup on the computer before, or its contents changed since the last backup, you need to synchronize it with local repository:

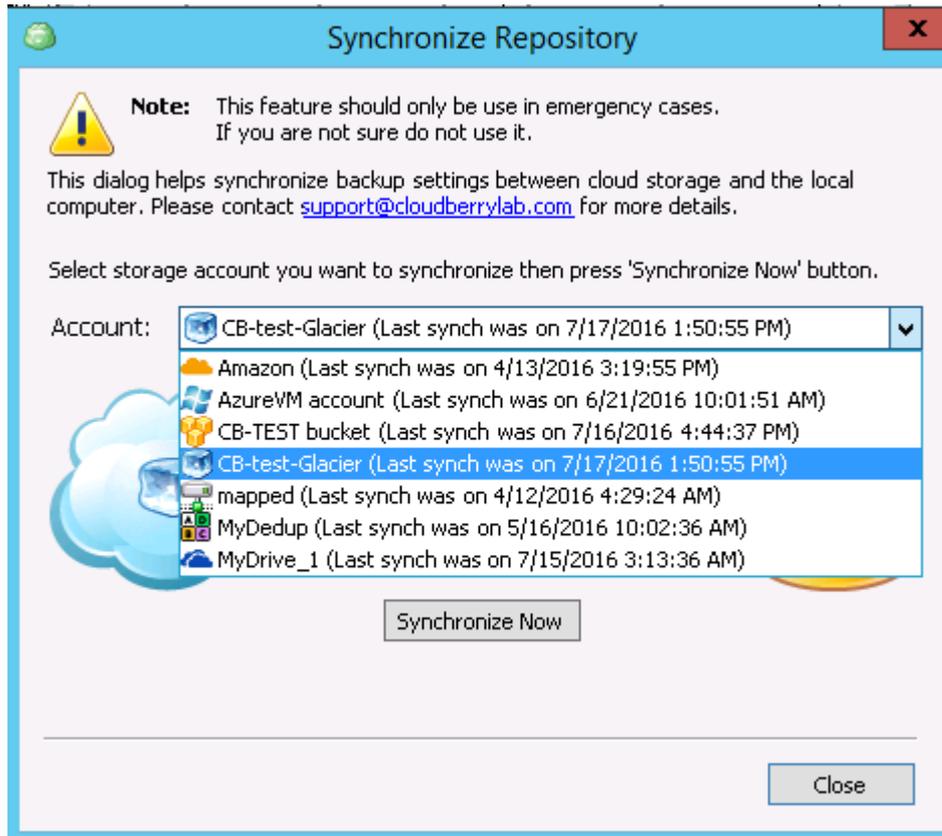
1. Open the **Tools** tab, press **Options** and switch to **Repository** section.



2. Click on the **Synchronize Repository** button. On the next screen, choose the Glacier Account from the drop-down list and press **Synchronize Now**. *Note: If you have made uploads during the*



last 24 hours, the Glacier Global inventory may not occur and files may not be available.



If the data is already synchronized, you can start the recovery. Click **Restore** at the **Home** tab. This will start the Recovery Wizard.

Glacier retrieval options

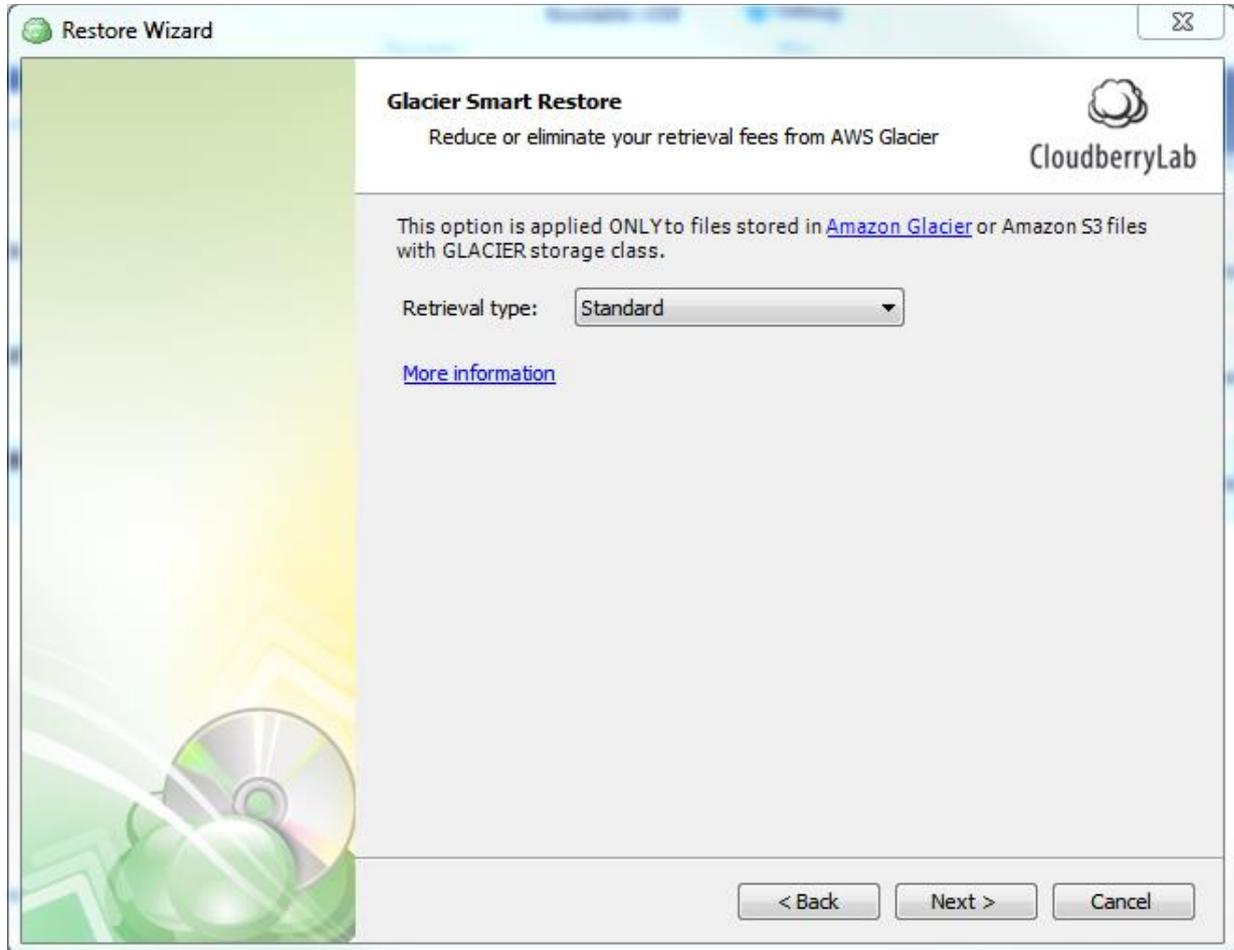
Formerly, if you wanted to retrieve your files from Amazon Glacier, the only way you could do so is via the so-called Standard retrieval. Well, not anymore. Amazon has introduced 2 new tiers:

- **Expedited:** for those who are willing to spend a little more for higher speeds. You can get you data in as little as 1 to 5 minutes. Retrievals cost \$0.03 per GB and \$0.01 per request. Note that there are some provisions that may impede smooth restoration. If you need to get your data back in this time frame even in rare situations where demand is exceptionally high, you can provision retrieval capacity. Once you have done this, all Expedited retrievals will automatically be served via your Provisioned capacity. Each unit of Provisioned capacity costs \$100 per month and ensures that you can perform at least 3 Expedited Retrievals every 5 minutes, with up to 150 MB/second of retrieval throughput. If you exceed that limit, expect errors on the part of Amazon.
- **Bulk:** for those who want to limit expenses by sacrificing access time. It is perfect for planned or non-urgent cases, with retrieval taking anywhere from 5 to 12 hours at a cost of \$0.0025 per GB and every 1000 requests amounting to \$0.025.



The **Standard** tier with your typical retrieval hours (3 to 5) also remains, costing \$0.01 per GB along with \$0.05 for every 1,000 requests.

CloudBerry Backup 5.3 or newer allows you to select the preferable retrieval tier when setting up a restore plan.

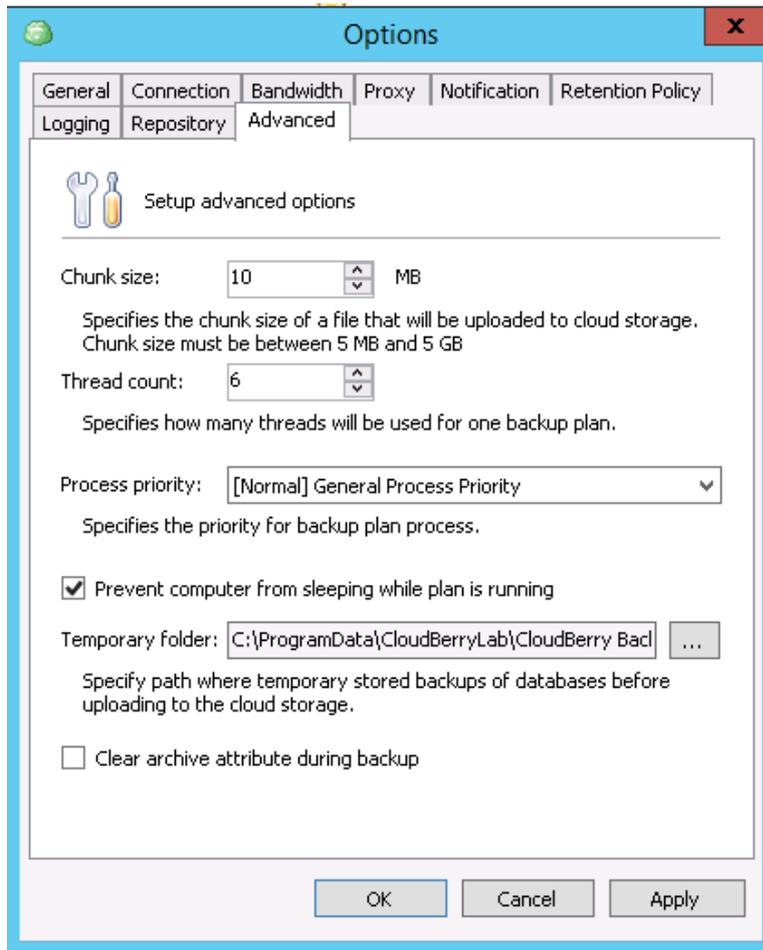


By default, the Standard tier is used to retrieve data. So if you don't explicitly specify the tier, expect the Standard fees and retrieval waiting time.

CloudBerry Backup Advanced Options

CBB has some features which can resolve specific cloud storage issues. They can be found on the **Advanced** tab of the **Options** window.



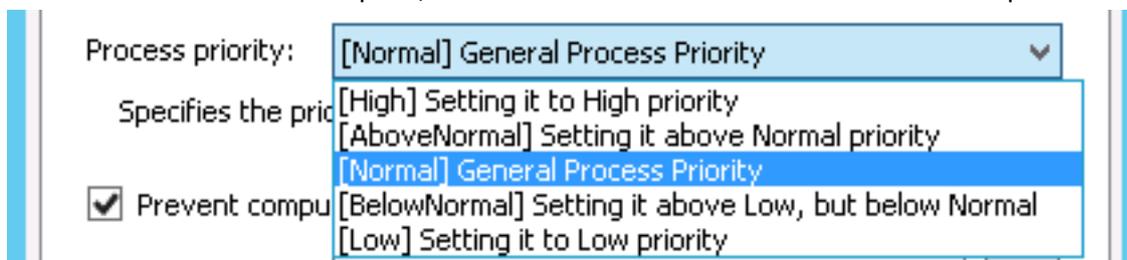


Multipart Upload

This feature breaks big files into the smaller chunks before uploading and then assembles them on the destination storage. This feature allows to:

- Ignore network errors and re-upload corrupted parts.
- Transfer data in multiple threads to increase the upload speed.
- Stop and start the upload at the Backup Plans tab.

At the **Advanced** tab, you can select the chunk size and specify number of threads. The bigger chunk size increases transmission speed, but it will take more time to continue interrupted transfer task.



You can also assign CloudBerry Backup **process priority** to manage performance.



Clear Archive Bit

The Archive Bit (ArB) is a file attribute that is set when a file is created or modified. It basically indicates whether the file is a new one or modified, so the system can decide to archive it or just skip.

Let's look at an example:

- You create a new file. The Archive Bit attribute is automatically set for this file.
- A daily backup schedule starts from Monday. It performs a full backup, and it completes successfully. The ArB is turned off.
- If here were no file modifications on Tuesday, CBB incremental backup skips this file since the ArB turned off.
- You modify the file on Wednesday. The ArB automatically turns on again.
- Incremental backup starts on Wednesday. CBB backs up the modified file and turns off the ArB attribute.
- The ArB will stay turned off and CBB will skip the file until you modify it again.

It is possible to **clear archive attribute during backup** by checking the relevant box at the Advanced tab. The option may be useful if you have re-deployed CBB on the machine, and there were file modifications in between.

Command Line Interface

CloudBerry Backup has a command line interface, which can manage all backup or restore features. It may also be used in Pre/Post Actions in backup plans, or by external software. The interface tool is **cbb.exe**, which is located in the CloudBerry Backup root folder. By default, it's **C:\Program Files\CloudBerryLab\CloudBerry Backup**.

Here are some examples of CloudBerry Backup CLI usage:

- **Configure global settings.** For instance, run the next command to set bandwidth speed to 100Kbit/sec:

```
cbb.exe -o -bw 100
```

- **Create a backup plan** using the next command:

```
cbb.exe backup -a myStorage -f "C:\Users\Administrator\Documents\Image.bmp" -d "C:\Users\Administrator\Documents\Data" -ifm "*.rtf;*.bmp"
```

CBB perform a one-time backup of **image.bmp** in **Administrator\Documents** and save all **.rtf** and **.bmp** files from the **\Data** folder to **myStorage** account. The backup process will be tracked in the Command Line.

- **Recover data.** Run the following command:

```
cbb.exe restore -a "myStorage" -d "C:\Users\Administrator\Documents -rl original -rt latest -o
```



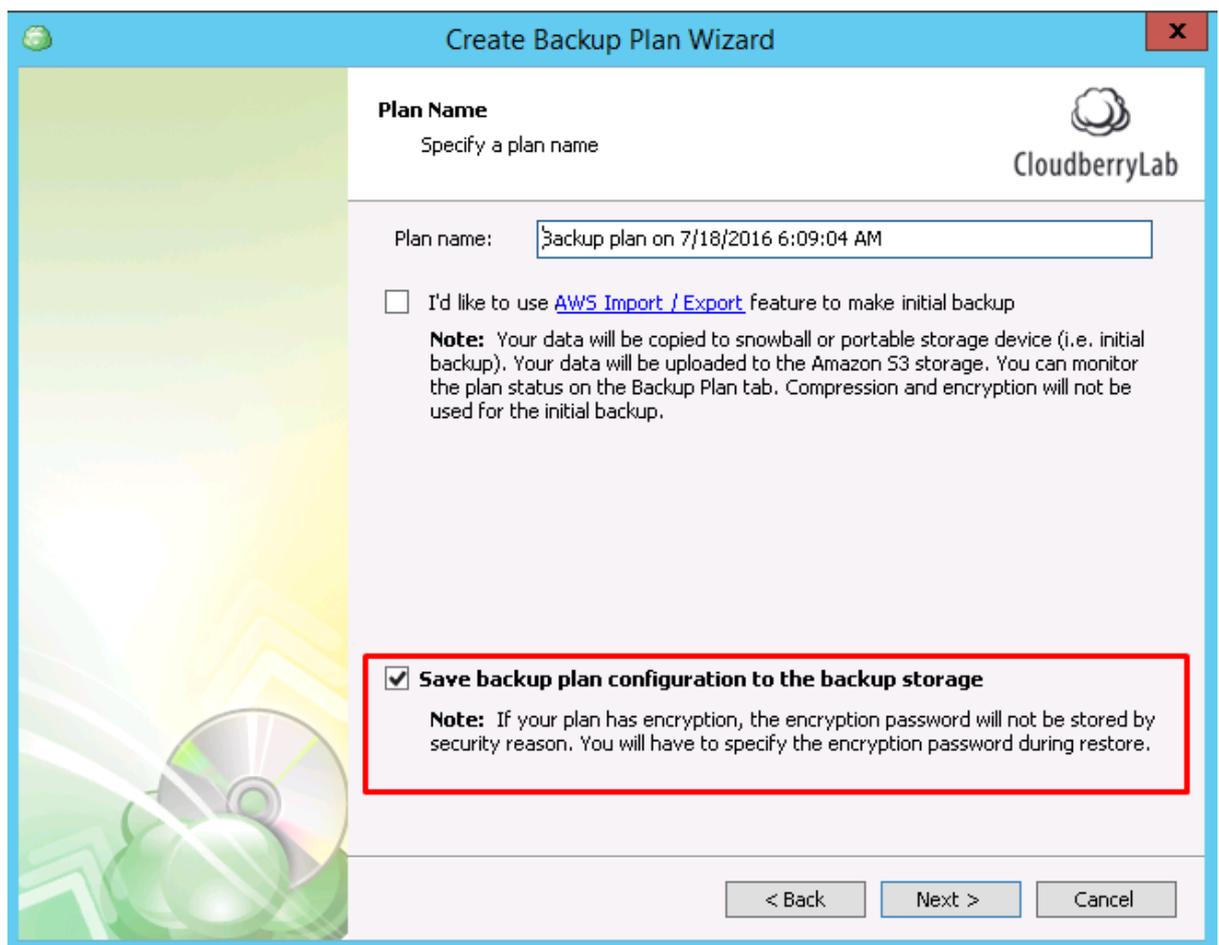
All files assigned to the **Documents** folder will be restored to their original location overwriting the existing files if any.

Full commands list and advanced scenarios can be found on the [Command Line Interface page](#).

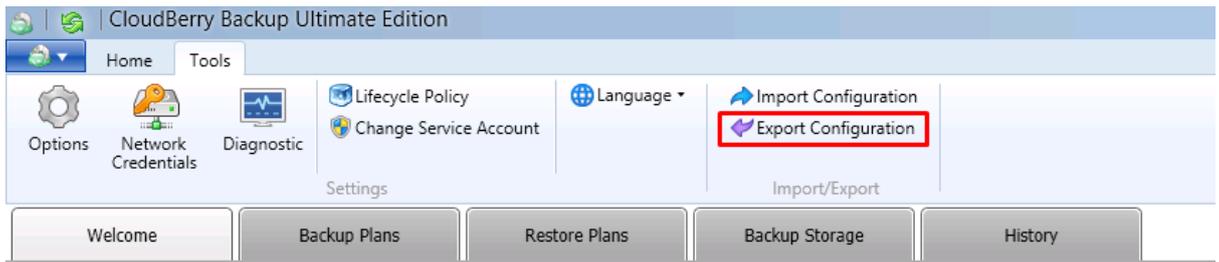
How to Recover Jobs and Presets on the New Server

When the disaster happens, first step is the hardware renewal. Whether you get new computers or choose cloud services, the next thing is the restoration of backup service and data recovery. There should be some precautions made before:

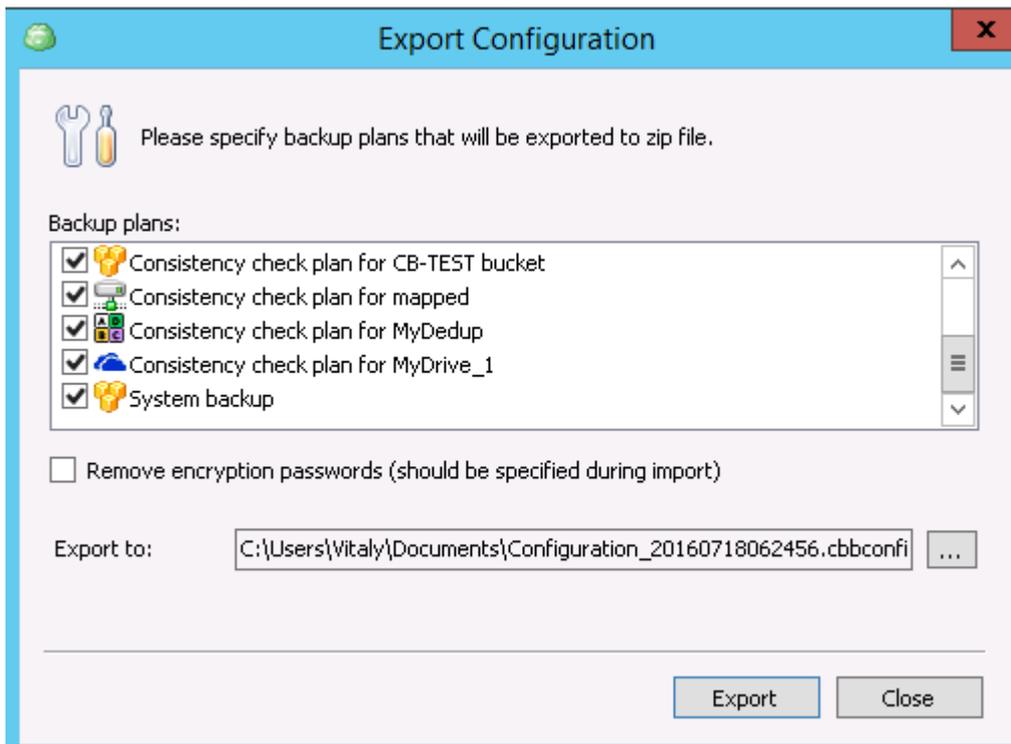
1. Each Backup Plan should be created with the **Save backup plan configuration to the backup storage** option enabled. It won't take much storage space and helps to restore task configuration even if the initial machine is lost.



2. Preserve CBB settings to facilitate the recovery by pressing on **Export Configuration** button at the **Tools** tab.

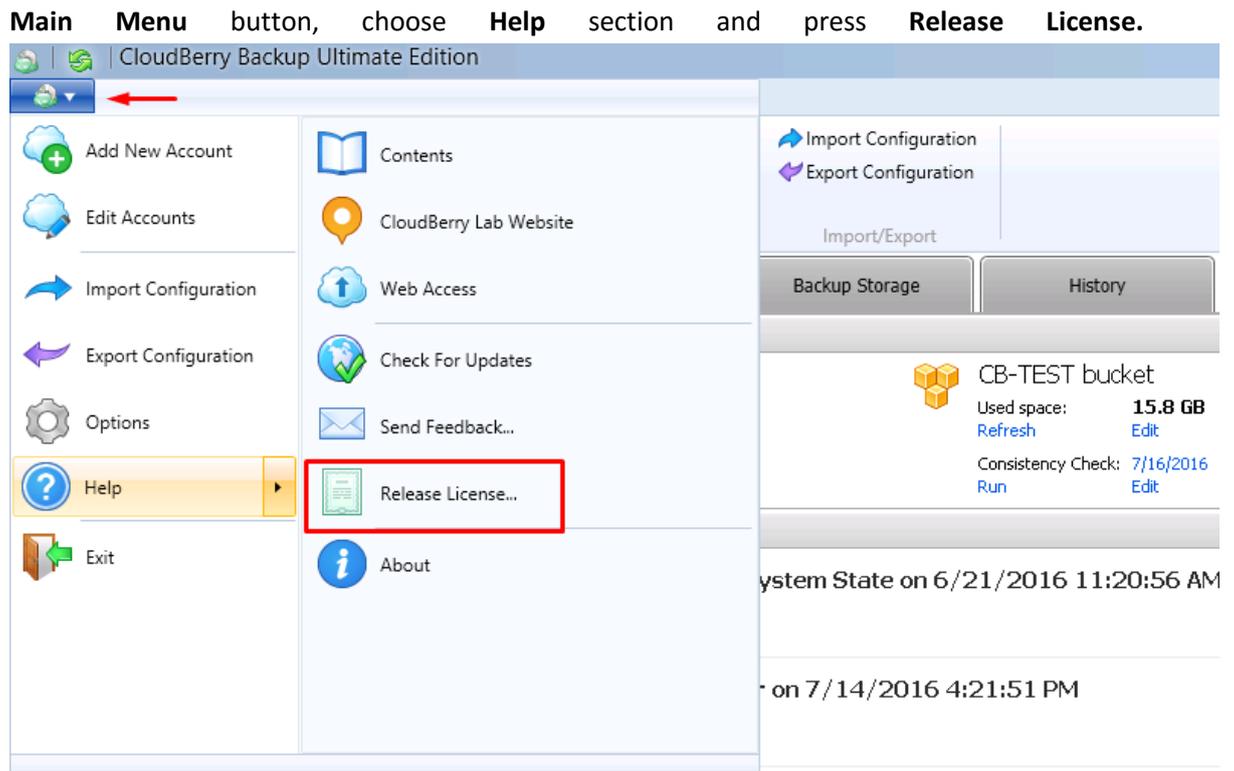


3. On the window appeared, choose plans to be saved and specify export location. You may create a backup task for configurations file to recover it easier later.

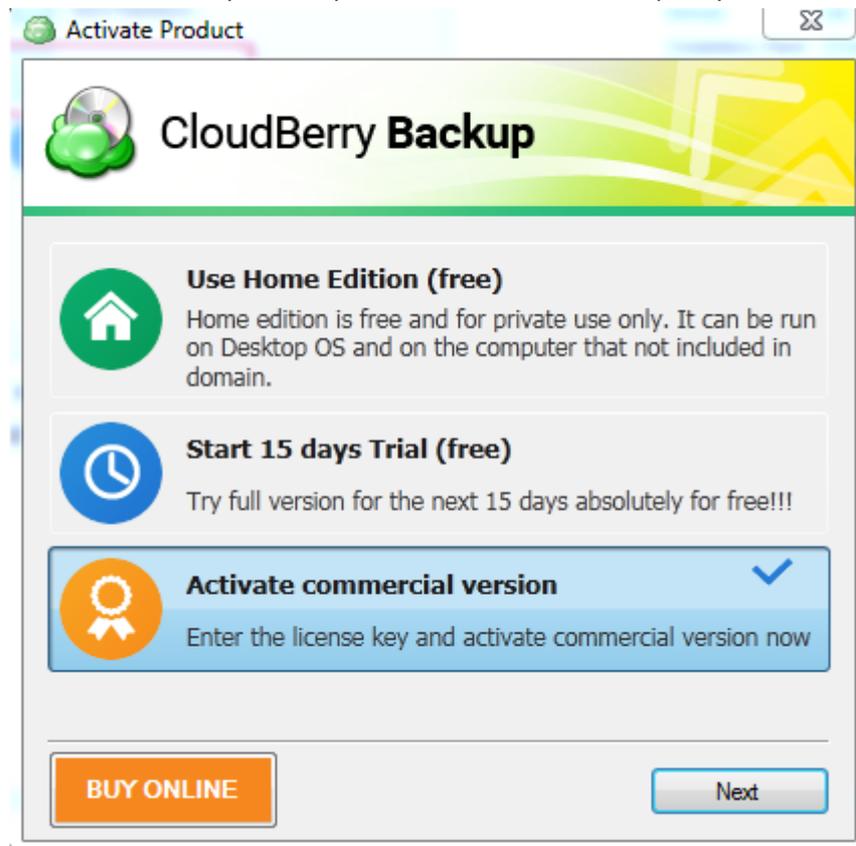


After all preparations are made, move to the new instance and proceed the following steps:

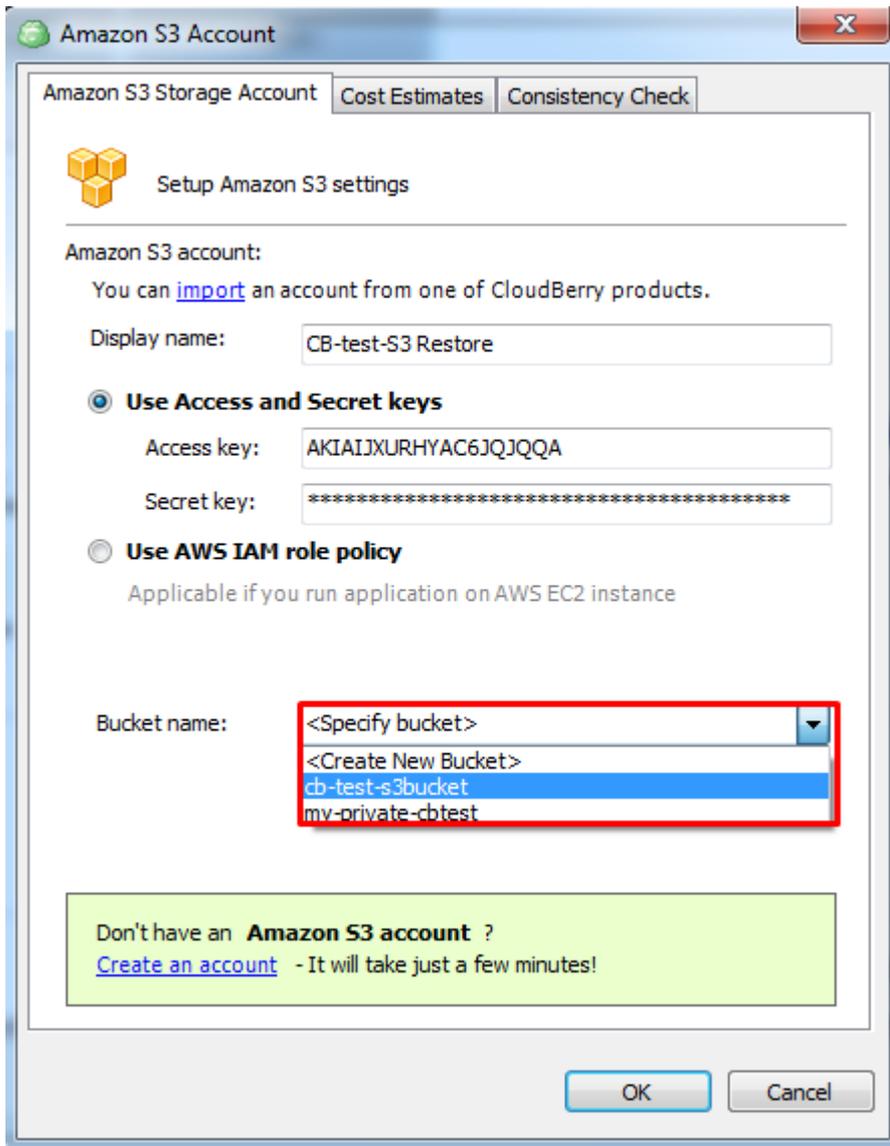
1. First of all, release the license to continue it on the new instance. You may [contact the support](#) to create a request or do it by yourself if the previous machine still accessible. Click on the



2. Install CloudBerry Backup. On the first run, specify license key or start a trial.

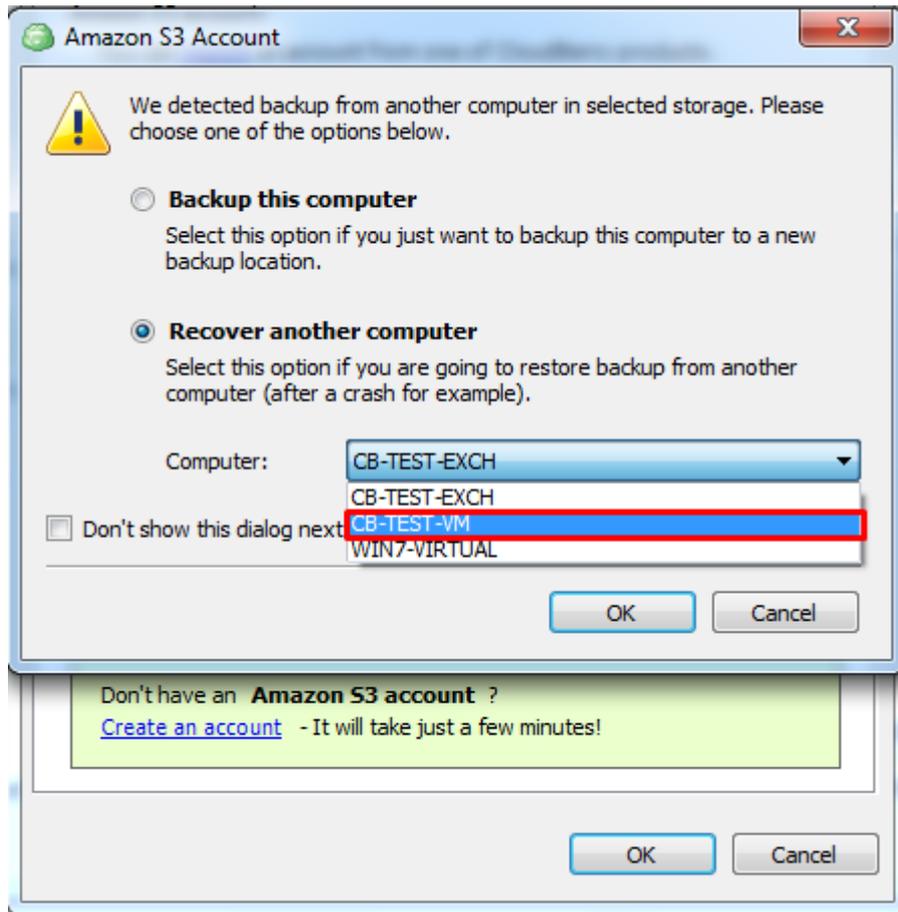


3. Click on the **Main Menu** button and select **Add Account**. Choose the same bucket and display name as before and specify security credentials.

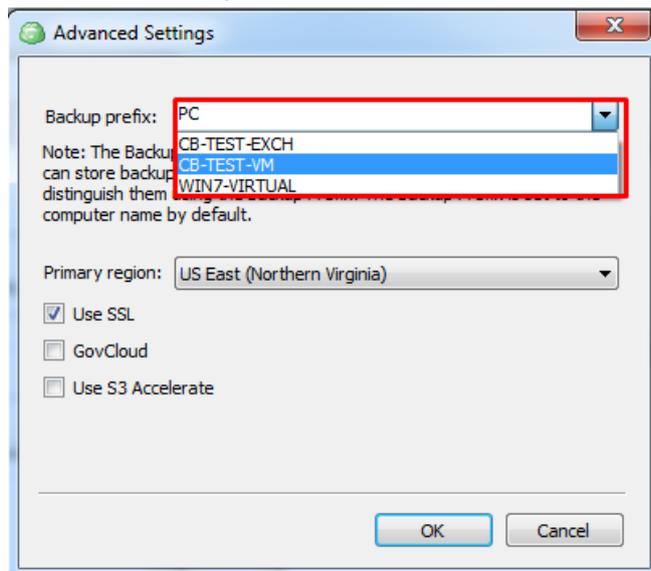


4. There are three ways to restore jobs and presets on the new computer:
 - a. After pressing **OK** while renewing the account, CloudBerry will scan the storage for previous backups. If there is one, CBB will ask if you want to recover another

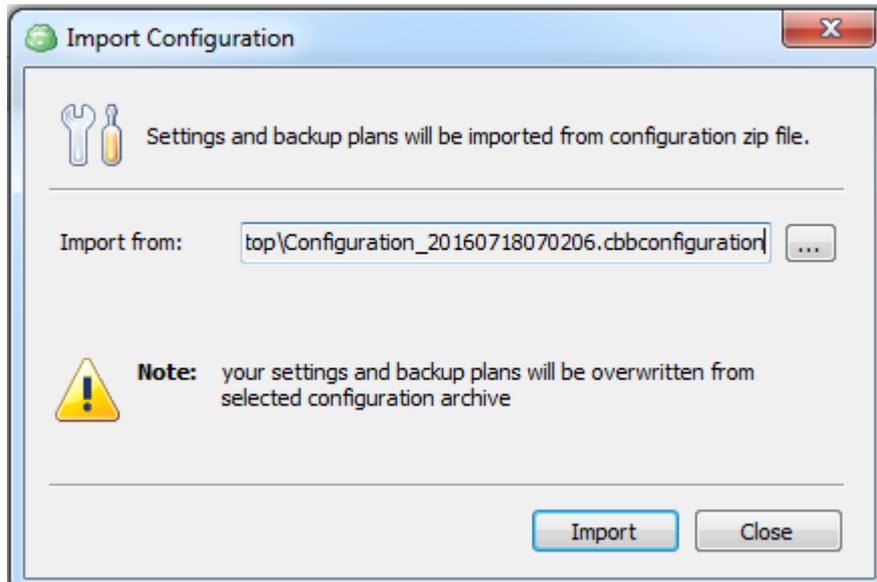
computer. Select the previous machine from the drop-down list.



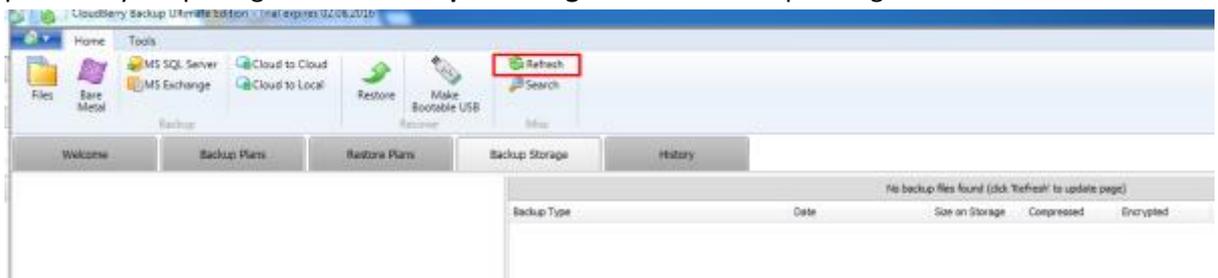
- b. If the previous step missed, assign CBB to the previous computer via Backup Prefix. Press **Edit Account** in the **Main Menu**, choose the **Advanced Settings** option and specify the backup prefix of the desired computer. There is a drop-down list with existed prefixes on the storage too.



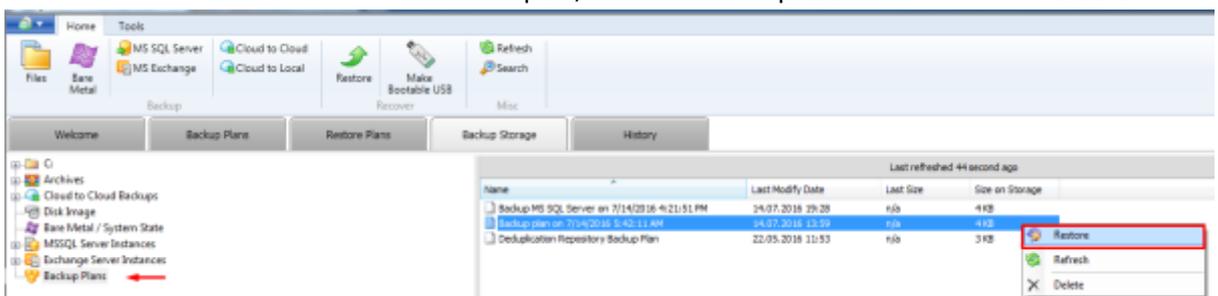
- c. You can also recover backup jobs and presets by renewing the configurations. Choose the **Import Configuration** at the **Tools** tab and specify the **.cbbconfiguration** file.



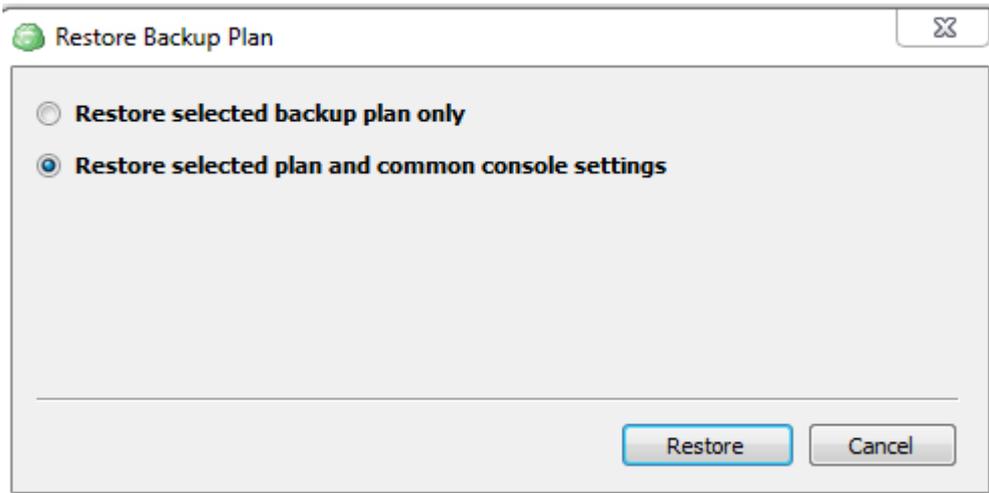
- 5. If used backup-prefix restoration, synchronize with the storage facility and renew backup plans by opening the **Backup Storage** tab and pressing **Refresh** button.



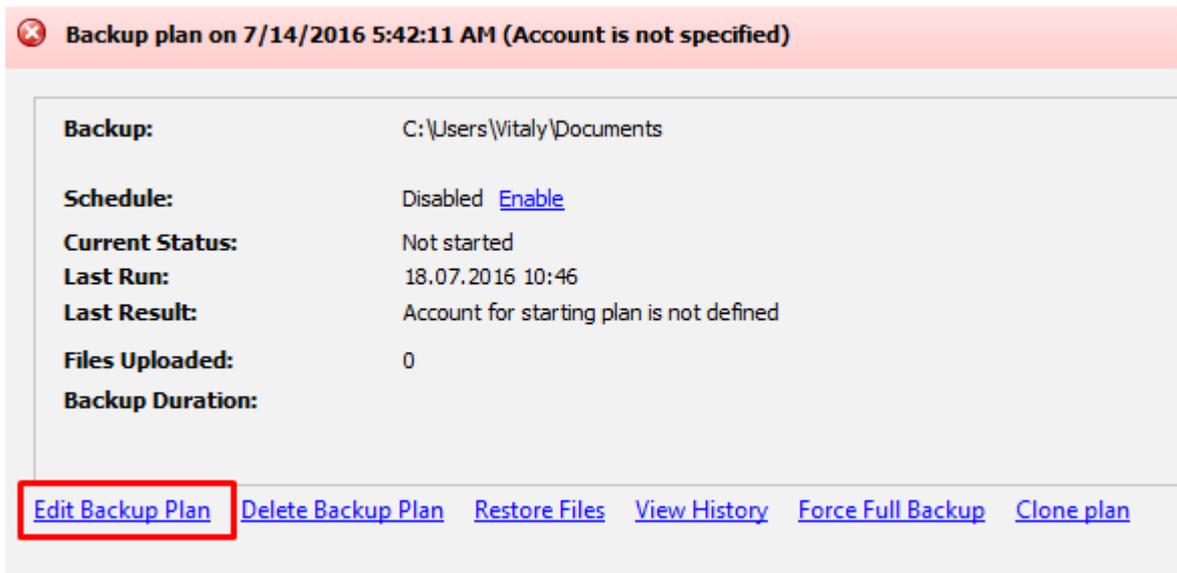
- 6. This displays the list of the storage contents. Choose **Backup Plans** section and right-click on the desired plan, press **Restore**.



7. Then choose **Restore selected plan and common console settings**.



8. Now plans are active at the **Backup Plans** tab. If you have specified the dissimilar name for the storage account, attach the plan to the storage manually by clicking on the **Edit Backup Plan** option.



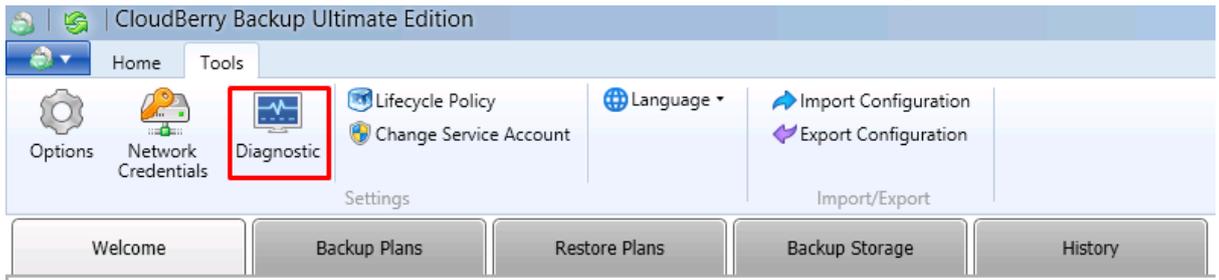
Troubleshooting

If something goes wrong with the CloudBerry Backup, we will do our best to help you. On the [Customer Support page](#), you can find frequently asked questions, read about the common issues or create a support ticket.

You can also contact us immediately within CBB interface in a few ways:



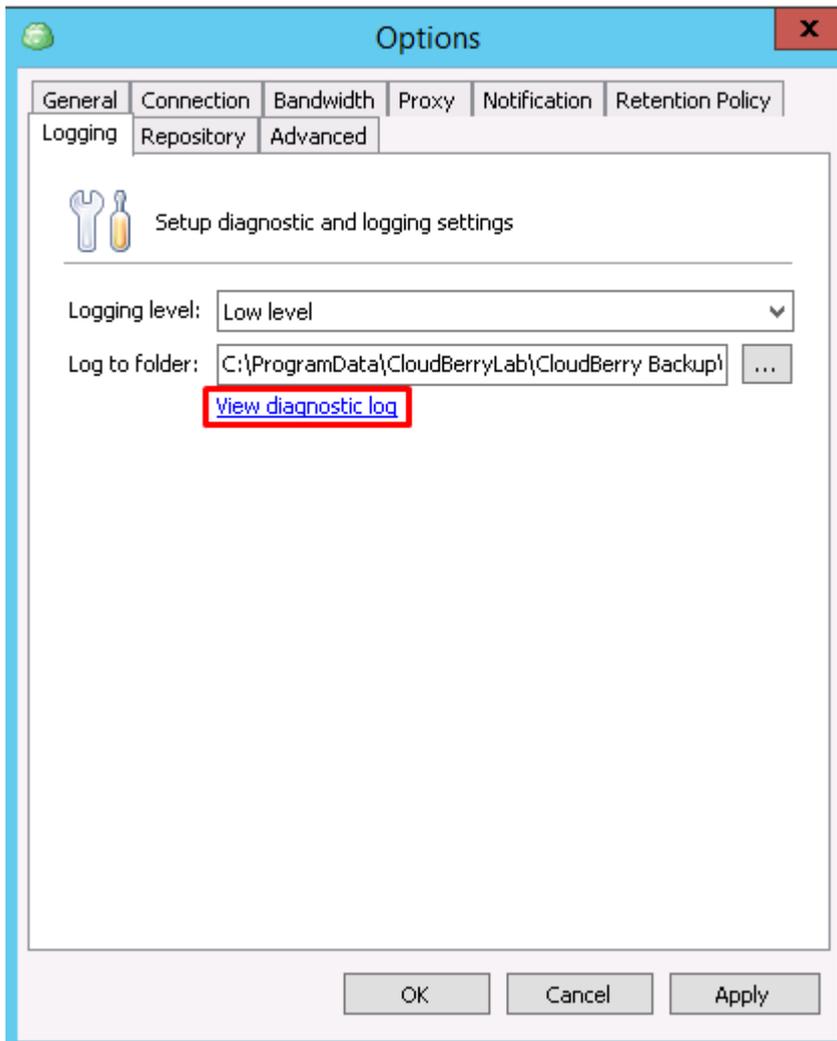
1. Open the **Tools** tab and click on the **Diagnostic** button.



2. Press **Report an issue** in the **Last Result** line of the failed backup plan.



3. Open CBB **Options** and go to the Logging tab. Here you can set up logging level (not recommended to change without a need). Press **View diagnostic log** to contact the support.



All these actions will open the **Diagnostic** window, where you can describe a problem and send logs to the CloudBerry Lab Support Team.

Diagnostic

Send us this diagnostic information in case of trouble

Name*: CB-user

Email*: cbtest@cloudberry.com

Ticket: please fill if you have one

Please enter the problem description here (limited to 4000 characters):

The log file will automatically be sent to us and a support ticket will be created. Our support staff will contact you shortly.

[Open in Folder](#)

Send to Support Close

Summary

Now you are aware of all fundamental features of CloudBerry Backup and know the basics of backing up to the cloud. To find out more, you may want to visit these resources:

- [CloudBerry Lab Blog](#), where we introduce new features, publish guidelines and analyze cloud services market.
- [CloudBerry Backup FAQ](#), where you can find the solution of typical issues.
- [Customer success stories](#) about CloudBerry Backup implementation.
- [Videos page](#) with guides and reviews.

If you still have questions left, don't hesitate to [contact us!](#) CloudBerry Backup is a ripe product for business tasks, but we still develop new features to keep pace with storage providers and customer demands.

