

CloudBerry Backup for Windows 5.8

Release Notes

Nov 22, 2017

These release notes provide information about the latest release of CloudBerry Backup for Windows (5.8).

Contents:

[About CloudBerry Backup](#)

[Key benefits](#)

[New and Updated features](#)

[Resolved issues](#)

[Known issues](#)

[System Requirements](#)

[Getting Started](#)

[About CloudBerry Lab](#)

About CloudBerry Backup 5.8

CloudBerry Backup 5.8 is a major release, featuring new functionality and enhanced performance. See **New and Updated features** to get a closer look at the novelties. CloudBerry Backup is a cross-platform, cost-effective, flexible, and versatile backup and recovery solution that enables businesses and ordinary users to perform automatic backups to various cloud storage services. Advanced features like encryption, compression, and synthetic backups facilitate more efficient, swift, and secure file transfer between your local computer and the cloud. Ultimately, the result is an unmatched conflation of reliable backup, automatic scheduling, and highly customizable backup configuration.



Key benefits

- Cloud backup to Amazon S3, Glacier, Microsoft Azure, Google Cloud, OpenStack, Rackspace, and various other cloud storage services.
- Local backup to hard drives and NAS-like storage solutions.
- Cloud to cloud backup.
- Image-based backup.
- Encryption and compression for more secure and swift backups.
- Flexible backup & restore plans.
- Restoration of image-based backups as instances of Amazon EC2 and Microsoft Azure VM.
- Easy setup of backup plans with the ability to configure schedule, email notifications, retention policy, and email notifications.
- Initial backup with the help of AWS Snowball.
- Synthetic and block-level backup for expedited upload.



New and Updated Features

New and updated features in Cloudberry Backup 5.8.

Ransomware Protection

This year has certainly been troublesome for businesses around the world when it comes to data security. Numerous cyber attacks have disrupted the normal business continuity, locking corporate computers and demanding ransom. With that in mind, we've decided to implement ransomware protection functionality in the latest iteration of Cloudberry Backup — release 5.8.

Let us first highlight that this feature is primarily tasked with detecting ransomware, rather than deactivating it. Namely, the implemented ransomware detection mechanism will utilize a few mathematical techniques to determine whether the files subject to backup have been encrypted. If so, a pop-up window will appear following the execution of the backup plan, notifying you of potential data corruption by ransomware. Read more about the feature in a dedicated [blog post](#).

Support for Changed Block Tracking in ESXi

Virtual machines running on VMware's ESXi hypervisor can track disk sectors that have been modified. This feature is called Changed Block Tracking (CBT). CBT provides the foundation for differential backup of ESXi's virtual disks. Therefore, whenever you perform a differential backup of your ESXi virtual machine, Cloudberry Backup request via a certain method the list of modified disk sectors of the given machine and then backs them up to the backup destination. It is virtually identical to what Cloudberry Backup is capable out of the box, except for the fact that VMware's mechanism can prove to be more efficient because both ESXi and CBT are developed by the same company. Read [here](#) how to enable the feature in Cloudberry Backup 5.8.



Disk Capacity Tool

One of the foremost features of Cloudberry Backup 5.8 is the ability to visualize your storage device, be it a hard drive or an SSD. The brand-new *Disk Capacity Tool* displays the breakdown of folder sizes and facilitates the analysis of the occupied disk space. Once the tool is started, you will be presented with a table of folders sorted by size by default. To the left of a child folders' names is a pie chart that vividly illustrates the share of the parent folder occupied by the child folder. Similarly, you can open up any folder and see its contents sorted by size. Read our [blog post](#) that dives deeper into the new feature.

Increased EC2 & Azure disk limits

Microsoft and Amazon have recently increased the disk volume limits for their virtual machines running on Azure and EC2. Needless to say, we always keep up with the developments in the industry and today announce the support for the Azure's and EC2's increased disk sizes in Cloudberry Backup 5.8.

In short, the new disk volume limits for EC2 and Azure virtual machines are as follows:

- 2 terabytes for MBR-partitioned disks;
- 4 terabytes for GPT-partitioned disks.

Traditionally, you can learn more about the novelty in a dedicated [blog post](#).

Support for Sao Paolo region for Google Cloud Platform

Microsoft Another small new feature worth mentioning is the support for new Sao Paolo region for Google Cloud Platform. In essence, you will now be able to restore your image-based backups as GCP virtual machines in the new region. Should be useful to our Brazilian customers!



Resolved Issues

In CloudBerry Backup 5.8

The following table illustrates issues addressed in release 5.8.

Resolved Issue	Issue ID
Inability to remove empty folders	1145
Failure to refresh OneDrive token	3080
Invalid bucket ID in B2	3975
Excessively small chunk size when uploading to B2	4093
Malfunctioning search in the Backup Wizard	3426
Failure to restore virtual machines backed up from the Hyper-V server with configuration version 8.0	3577
Failure to list the OS image when configuring a Google Temporary Instance	4127
Cancelled EC2 restore displays as failed	3101
High-DPI issues	1735, 3733, 4186, 2799
Localization issues	3827, 3940
Improper error message when performing image-based backup of unavailable disks	3929
Failure to restore an Intel RAID from bootable USB	4087
Backups occurring every X months appear to be occurring every month	3632
Insufficient output for addAccount command in terminal	3953



Inability to enable real-time backup in Hybrid backup	4113
Scheduled backups fail to execute after switching from a trial license to commercial	3968

Known Issues

The following table displays known issues that are to be addressed in the future releases of Cloudberry Backup.

Issue	Issue ID
NTFS permissions of deleted files remain in the cloud	2245
Compression indicator shows n/a for SQL backups following repository sync	2707
Preservation of deleted files' data in the cloud	2168
App-level bandwidth limit	1807



System Requirements

Before installing Cloudberry Backup 5.8, ensure that your computer meets the following minimum software and hardware requirements.

Hardware requirements:

- 1.4 GHz 64-bit processor;
- 512 MB RAM;
- 100 MB of free disk space;
- Internet connection.

Software requirements:

- Windows 7/8/10 or Windows Server 2003/2008/2012/2016.



Getting Started

Installation Instructions

1. Get the universal installer on our [website](#).
2. Double-click on the **.exe** file to launch the Windows installer. If some required software frameworks are missing, the installer will prompt you to fix it.
3. On the first launch, select the requisite licensing option.
4. After launching the program, you can begin configuring backup & restore plans. Read our comprehensive [installation guide](#) that exhaustively explains all the pitfalls of setting up Cloudberry Backup.

Additional Resources

You can get the latest information on our products, various tutorials, and other similar information on our blog at <http://www.cloudberrylab.com/blog>.

Also, check out our knowledge base that features various workarounds for frequently experienced issues as well as some tips on how to enhance your interaction with our flagship backup solution at kb.cloudberrylab.com.



About CloudBerry Lab

Established in 2011 by a group of experienced IT professionals, CloudBerry Lab™ provides cloud-based backup and file management services to small and mid-sized businesses (SMBs).

CloudBerry's offerings include powerful, easy-to-use backup management capabilities and military-grade encryption using customer-controlled keys. Customers can choose to store their backup data with more than 20 online storage providers, including Amazon S3, Microsoft Azure & OneDrive, Google Cloud, HP Cloud, Rackspace, IBM Softlayer, and many others. CloudBerry also partners with thousands of VARs and MSPs to provide them with turnkey, white-label data protection services. CloudBerry Lab is an Amazon Web Services Advanced Technology Partner.

Contact CloudBerry Lab

Sales: sales@cloudberrylab.com

Pre-sales hotline: +1 212 863 9918

Tech Support: support@cloudberrylab.com

Copyright

Copyright ©2017 CloudBerry Lab.

ALL RIGHTS RESERVED.

