CLOUDBERRY LAB IS NOW
MSP360
#1 MSP BACKUP

MSP360™ (CloudBerry) Backup 7.0 for Windows

CLOUDBERRY LAB IS NOW MSP360 #1 MSP BACKUP

MSP360™ (CloudBerry) Backup 7.0 for Windows

Release Notes

December 7, 2020

These release notes provide information about the latest release of MSP360™ (CloudBerry) Backup 7.0 for Windows.

Contents:

About MSP360™ (CloudBerry) Backup 7.0 for Windows

MSP360™ (CloudBerry) Backup 7.0 for Windows is a major release, featuring new functionality and enhanced performance. See the **New and Updated features** section 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 a 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, Wasabi, Backblaze B2, Microsoft Azure, Google Cloud, OpenStack, and various other cloud storage services
- Local backup to hard drives and NAS-like storage solutions
- Encryption and compression for more secure and swift backups
- Synthetic backup for file, image-based, and VMware backups supported for major storage providers
- Flexible backup & restore plans
- Easy setup of backup plans with the ability to configure schedules, retention policy, and email notifications
- Block-level backup for expedited upload.

New and Updated Features

New and updated features in MSP360 (CloudBerry) Backup 7.0 for Windows.

New Backup Format

The new backup format is a new vision of storing backup data on backup storage as a data container regardless of the backup type. This approach enables keeping backup plans completely independent from each other. Every backup plan is a separate entity that delivers backup data to a separate location on backup storage that allows avoiding any possible interference issues between plans.

Backup data is divided into blocks and blocks are the main operating entity. While uploading to the cloud, blocks are combined into data parts, which size can vary. A data part size depends on uploading speed and backup storage provider limitations. Uploading by parts enables supporting the continued upload in case of backup interruption.

The new backup format contains several new terms and entities that are to be explained to operate them in the future.

Bunch

Bunch is a notion of a backup plan in the main database. Bunch is linked to a directory in the database which in turn is linked to a destination. A destination can be modified. Bunch is always unique within the cloud folder and the plan type. This approach enables comfort data deletion on backup storage since all backup contents are stored in one directory.

Generation

Generation is a complete self-contained data set sufficient for data restoration. In other words, generation is a set of a full backup and chain of incremental backups for a selected backup plan.

Restore Point

Restore Point is a partial data set for restore. A full-fledged restore point contains at least one file or directory. If a restore point does not contain any file or directory, it is considered as empty, but successful can contain blocks for further subsequent runs. A valid Restore Point guarantees a correct restoration of backed-up data. As the opposite, invalid Restore point does not contain a complete data set for restore, but at the same time can contain blocks that are used for restore from other Restore Points.

The new backup format key features are:

- The number of requests to storage is reduced significantly
- Uploading by data parts enables continued upload in case of network issues
- Any characters (emoji, 0xFFFF, etc) and extra-long filenames supported
- Filename encryption in the box (one password for generation)
- Real full backup for file-level backups
- Fast synchronization (reduced number of objects in backup storage)
- Plan configuration is always included in a backup
- Backup logs are backed up along with backup data
- Object size is now limited to 256TB regardless of the storage provider limitations
- Fast purge (reduced number objects on backup storage, deletion of whole generation database)
- Password Hint
- Faster backup and restore for a large number of small files
- Lower costs for a large number of small files (not applied for S3 standard-IA with 128KB limit).

Currently, the new backup format is supported for file, image-based, and VMware backups only.

Read more about the new backup format in our help documentation.

Client-Side Deduplication

The new backup format reckons for a full backup plan independence, so each separate backup plan has its own deduplication database. Moreover, backup plan generations also have their own deduplication databases.

Once a backup plan is run, the application reads backup data in batches aliquot to block size. Once a block is read, it is compared with deduplication database records. If a block is not found, it is delivered to storage and is assigned with a block ID, which becomes a new deduplication database record. The block scanning continues, and if a block matches any of the deduplication database records, a block with such ID is excluded from a backup plan.

Synthetic Backup Support for File, Image-based, and VMware backups

The streamlined synthetic backup is now supported for most backup types and major storage providers. See the list of supported backup types and storage providers below.

Supported backup types:

- File backup
- Image-based backup
- VMware backup

Supported storage providers:

- Amazon S3 (except S3 Glacier and Deep Archive)
- Microsoft Azure
- Backblaze B2
- Wasabi
- S3-compatible storage (depends on the storage provider).

Mandatory and Full Consistency Checks

With the new backup format introduced, consistency check becomes mandatory for each backup plan run.

The consistency check is a technique that provides avoiding data losses. By finding any discrepancies, the user is notified if some backup objects are missing in backup storage or there is a mismatch between object sizes or modification dates.

Mandatory Consistency Check

In the new backup format, the mandatory consistency check is always a current generation check. The mandatory consistency check is executed for all backup plans in the new backup format before the backup plan runs.

Full Consistency Check

Full consistency check features all backup plan generation checks except current generation. Once the full consistency check succeeds, the user can be sure that backed up data is ready for restore.

Built-In Restore Verification for Image-based Backups

Restore verification is an auxiliary restore plan that retrieves only necessary backup parts from backup storage, mounts a Hyper-V virtual machine on the fly, then performs a system logon.

Note: Restore Verification feature has some limitations with long-term storage classes such as S3 Glacier or Deep Archive. If the Restore Verification is run and backup data is stored in long-term storage, all backup data is retrieved. This may take significant time and is subject to extra charges by storage providers. For this reason, Restore Verification is disabled for long-term storage by default

Restore Verification can be enabled for each image-based backup plan in the new backup format and is supported for Windows 8 (Pro and Enterprise editions) and later versions, and Windows Server 2012 and later versions.

Modified Block Tracking for Image-based Backups

Modified block tracking is an algorithm that features a decrease in backup source data reading on incremental image-based backups.

Each time an image-based backup plan runs, the state of the blocks at the moment of a backup plan start is saved. Once a first full backup is made, each block in MFT (Master File Table) is marked. On subsequent incremental backup runs, the MFT is being read again and blocks are compared. If a block is modified, the block tracking mechanism determines which files have been modified and locates disk clusters that contain file data. Once all blocks are compared, only modified blocks are sent for reading with subsequent upload to backup storage.

Restore On Restore Points

Restore Point is such a backup state that enables the guaranteed restoration of backup data. If a full or incremental backup terminates successfully, a new restore point appears on backup storage.

Restore points are displayed in the backup tree of Backup Storage browser, so restore became

Improved GUI

Backup 7.0 for Windows comes with a new GUI that features the renewed Backup Storage browser and detailed information on backup and restore plan progress.

Resolved Issues

The following table illustrates issues addressed in MSP360™ (CloudBerry) Backup 7.0 for Windows.

Resolved Issue	Issue ID
Microsoft Azure: special characters are not supported	8212
Wasabi: special characters are not supported	6532
Engine: Connections are not closed, sockets are left intact	7821
An attempt was made to create more links on a file than the file system supports.	1508
Backblaze B2: Long filenames are not supported	1337
Restore-Only mode: VMware full backup is not displayed correctly	2734
Current backup format: VMware VM config is not displayed if backup data is in Glacier	2752
Repository sync: cannot display characters for xml hexadecimal value 0xFFFF	4577
VMware backup: forced full backup of a stopped virtual machine is displayed wrong	4763
Hyper-V backup: full backup size is displayed wrong	4771
Archive mode: files on backup storage are not displayed in the History tab	5014
Archive mode: backup time is too long when backup consists of numerous small files	6597
VM restore: just created device is not displayed (NVME controller 0)	6871
File and Image-based backup: conflict while two backup plans (file and image-based) are running simultaneously	7767
Hyper-V backup: force full backup fails after full backup if at least one VM is powered off	7853
High memory consumption on backup plan consistency check when filename encryption enabled	8268
Restore from NAS: username or password is incorrect	8280
Restore NTFS permissions: permissions are not inherited after restoration	8387
Overflow on a backup of big amounts of files and frequent synchronization/consistency checks	8390
Image-based backup: Slow execution of block-level backups	8730
Invalid password request on the deletion of file backed up with filename encryption previously deleted from backup storage on Backup Storage tab	9171

System Requirements

Before installing MSP360™ (CloudBerry) Backup 7.0 for Windows, make sure that your computer meets the following requirements:

Component	Requirement
CPU	1.4 GHz 64-bit processor
RAM	512 Mb or more
Disk Space	100 Mb or more
Operating System	Windows 7/8/10 Windows Server 2008/ 2008 R2/2012/ /2016/2019
Software Installed	Microsoft .NET Framework 4.0 or higher

Getting Started

Installation Instructions

1. Download the universal installer from MSP360™ website.
2. Run the Windows installer. If some required software frameworks are missing, the installer will prompt you to fix it.
3. Follow the installation wizard steps. To learn more, refer to the Installation section of the help documentation.
4. Upon the first launch, select the licensing option.
5. Once all is set, you can begin configuring backup & restore plans.

Additional Resources

You can get the latest information on our products, various tutorials, and other similar information on our blog at https://www.msp360.com/resources/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 https://kb.msp360.com/.

About MSP360™

Established in 2011 by a group of experienced IT professionals, MSP360™ (formerly CloudBerry Lab) provides cloud-based backup and file management services to SMBs.

MSP360'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 all the major cloud storage providers, including Amazon S3, Microsoft Azure, Google Cloud, Wasabi, and others. MSP360™ also partners with thousands of VARs and MSPs to provide them with turnkey, white-label data protection services.

Contact MSP360™

Sales: sales@msp360.com

Tech Support: support@msp360.com

Copyright