



WHITEPAPER

# A Complete Guide to Backup and Disaster Recovery on Amazon Web Services



Moving data to the cloud is one way to help increase availability and reliability, as compared to on-premises infrastructure. However, even the best-managed clouds can fail. That's why having a data backup and recovery plan in place is critical, even if you use the cloud.

With that need in mind, this whitepaper explains backup and disaster recovery best practices for Amazon Web Services (AWS). It discusses the various services offered by AWS and explains how they can be used to facilitate efficient and reliable backup and recovery.

## Backup Scenarios

There are two metrics to think about when planning any type of data recovery strategy: Recovery Point Objective (RPO) and Recovery Time Objective (RTO). RPO reflects the amount of data a company can afford to lose after an outage. RTO defines the time between an outage and the full recovery of the infrastructure, which corresponds with the time taken for data from the latest backup to be retrieved.

Naturally, businesses want to get their information back from storage as quickly as possible and avoid the loss of any information. There are two ways to do so:

- ▶ Reduce RTO: For example, by retrieving data from storage faster.
- ▶ Reduce RPO: Make backups more often.

However, each company faces technical limitations in doing this.

For example, it takes about 24.5 hours to transfer a 10 terabyte copy through a 1 Gbps channel. Thus, the ability to reduce RTO is limited by network bandwidth. And for RPO, more frequent backups increase network load, making upload and download more difficult.

### 3-2-1 Backup Strategy

To ensure your data is safe and up to date, we recommend the 3-2-1 backup strategy, which is defined as follows:

- ▶ Have at least 3 copies of your data.
- ▶ Keep two copies of your data on two different types of media.
- ▶ Store one copy of your data offsite.

Three copies— the original data, and two clones — provide protection from human error, such as accidental deletion of data. Keeping data on at least two different kinds of storage devices makes it less likely for data to be lost due to a hardware fault. For example, Hard Disc Drives (HDDs) can crash individually within a short period; this is most likely to occur if they were purchased together and installed at the same time. Offsite storage maintains data outside your city or country, keeping it safe in case of a disaster that could destroy both hard disks and external storage.



Offsite storage is obviously extremely important. It should be:

- ▶ Reliable.
- ▶ Able to store any kind of data.
- ▶ Located as far as possible from your current location.
- ▶ Able to be accessed immediately.

AWS cloud facilities satisfy all these demands. Building your own data center is less secure and takes years of planning. Renting a rack in a commercial data center is less scalable and is not immune to disasters. Both options are much more expensive than the AWS Cloud.

## Types of Cloud Storage

AWS offers several types of storage options, each of which can be used to support different backup needs.

### File-Level Backup

The standard copying of select files and folders is the easiest way to back up data. It doesn't require much disk space compared to other methods and fits any kind of storage. File-level backup is mostly applied to working user data and documents. It's also possible to perform a quick rollback to the previous version, whereas deduplication services prevent backup size overflow by uploading only new or changed data. The best solution for keeping data safe is the file-level backup.

However, file-level backup is not ideal if you want to maintain a server in its exact state, or facilitate fast disaster recovery using a virtual machine image.

### Image-Based Backup Level

Image-based backup creates a copy of the operating system (OS), and the data associated with it, for its respective computer or virtual machine (VM). In the case of failure, users can use the image to retrieve data. All the machine's data — from working files to system configurations — is stored in a single image file. This strategy requires more space on a storage system, but it ensures the availability of all server data. MSP360 Backup directly connects to the cloud, uploads new images in real-time and analyzes images to identify the difference between previous images and only uploads modified data blocks so it doesn't use up additional disc space.

Folders and separate files can be easily restored from an image, too. An image-based backup is the main tool for server and cloud migration, as well as disaster recovery. Alongside simple restoration, images allow businesses to:

- ▶ Restore data as a virtual machine in the cloud (Amazon EC2).
- ▶ Restore with USB flash directly from the cloud.
- ▶ Restore to dissimilar hardware.
- ▶ Restore to Hyper-V, VMware or other virtualization platforms.

MSP360 Backup empowers you to not only to create, restore, and transform images on the fly but also deploy VMs on AWS from your backups. An image-based backup is typically combined with file-level backups. Images are



created to deal with system or hardware failures and disaster recovery, whereas file backups are good for daily routine losses and errors.

## SQL Database Backup

While SQL server data can be backed as part of an OS image, the database itself is often the most valuable thing on the server. It is possible to only protect the database, with no extra storage expenses and efforts.

There are two main database backup strategies:

- ▶ Full Backup: Save all data and logs. Commonly used for periodical service or initial data seeding to storage.
- ▶ Differential Backup: Only update the modified data blocks. This is part of a basic maintenance strategy.

The best strategy for database backups is making a full backup as the initial seed, then updating it with differential backups as often as possible.

Amazon offers three database platforms:

**Amazon Relational Database Service (RDS)** offers a wide choice of relational database engines, compute and storage options, Multi-AZ availability, and more. The main feature here is management simplicity.

**Amazon DynamoDB** provides a fast, scalable, and cost-effective NoSQL database, where data is automatically replicated among data centers.

**Amazon RedShift** is a tool for fast, scalable big data storage management. Its primary function is data warehouse maintenance.

MSP360 Backup supports SQL server clusters and transaction log backups. AWS lets you deploy your database from your backups as a virtual machine on the cloud, or add it to your existing database.

Further reading

[The Ultimate Guide to MS SQL Server Backup and Recovery](#)

## Microsoft Exchange Backup

There are two primary backup approaches for Microsoft Exchange:

- ▶ Enterprise Database (EDB) files - the database by itself.
- ▶ Log files attached to EDBs.

These two items depend on each other. Therefore, optimizing their backup requires caution and accuracy.

Block-level maintenance is extremely useful for databases since database backup can easily exceed storage capacity. MSP360 Backup provides a special purge feature that maximizes the benefits of block-level backup without risking the loss of data.

The best strategy for Exchange maintenance is to upload a full backup once a week and update it by purging block-level backups without overloading the network and system while keeping everything up to date.

Further reading

[Guide to Full System Backup and Recovery](#)



## NAS Backup

Network Attached Storage (NAS) can be used for backups or maintaining working user data. MSP360 Backup can be installed on supported NAS devices to manage cloud data backup. Another MSP360 feature useful for network storage services is its consistency check. If the disk was removed from the NAS or the backup was corrupted, a consistency check will help to solve the issue. To guarantee accuracy, MSP360 uses timestamps to track changes made and compares them to see if there were any modifications.

## Mac & Linux Backup

Backup rules are the same for any operating system. MSP360 and AWS enhance tools and cloud support for Mac and Linux. A variety of backup instruments, with both graphical and command-line interfaces, give you the opportunity to match any kind of machines and storage types. AWS allows you to store and virtualize most Linux and macOS versions.

## EC2 Backup

Amazon Elastic Compute Cloud (EC2), as a VM, supports both file-level and image-based backup. EC2 instances are deployed from preset software packs using Amazon Machine Images (AMIs) and simple images. You can focus on protecting configuration and stateful data using a simple file or app-level backup types. This makes it possible to create backups more often, resulting in recovery with minimum data losses.

## Large Backups Upload and Initial Seeding

All backup strategies, beginning at the image-level, can scale. Data is easily transferred on the local level via fast-speed inner networks within AWS, but sending large sets of data to offsite storage requires significantly more work. Transferring backups to cloud storage via the Internet can take time and incur additional costs.

Fortunately, Amazon offers solutions to facilitate remote data transfers.

- ▶ **Amazon S3 Transfer Acceleration:** A new feature that is built into Amazon S3. When enabled, it speeds up data exchange with selected S3 buckets by a factor of up to 6. Increased speed is realized by selecting Amazon transfer routes with a higher bandwidth rate, giving your data upload priority.
- ▶ **AWS Snowball:** Allows up to 80 terabytes of data to be stored and transferred to the cloud by physically transferring hard drives from your location to AWS. It is self-encrypted, armored, and has a hijack tracker, making it impossible for third parties to access the data. It connects directly to your local network, accelerating download and upload speeds.

**Note: the delivery speed of hardware data devices  
is determined only by postal service performance.**



MSP360 supports online and offline upload services. You can access acceleration tools and hardware storage delivery pages directly from the GUI. MSP360 products track the entire lifecycle of Amazon Snowball transfers.

The best strategy for backup upload depends on the data size, urgency, and the transfer facilities available.

For example, if a full enterprise backup comprises 15 of data and the Internet connection bandwidth is 100Mbps, it will take approximately 18 days to upload the initial seed with 80% network utilization. Amazon Snowball operates faster. It takes approximately two days for a Snowball device to be delivered to customers, after which data can be uploaded instantly. Amazon S3 Transfer Acceleration is best used for uploading weekly and monthly backups. Disk Export helps with backing up new elements introduced into the IT-structure.

When choosing the tool for your backup transfer, take the special needs of your region into accounts, such as the quality of your Internet connection and the data upload destination. This topic is further discussed in the **Data Transfer** section of this document.

## Storage Facilities

Amazon Web Services offers different classes of storage for various usage scenarios. This allows organizations to reduce storage costs for backups which are not accessed often. Classes have a high level of reliability and support SSL data encryption during transmission, but differ in cost. AWS offers the following for data maintenance:

### Amazon S3 Standard

Amazon S3 Standard is designed for high-usage scenarios and has the following features:

- ▶ High capacity and low latency.
- ▶ 99.999999999% reliability (risk losing one object for every one-hundred billion).
- ▶ 99.99% availability (one hour of unavailability for every ten thousand hours).
- ▶ The use of storage is covered by the Amazon S3 Service Level Agreement, which provides for compensation if the level of uninterrupted operations is lower than promised.

Standard storage is suitable for file-level backup of working files and documents. These may be rolled back, changed, and recovered dozens of times per day. S3 is also the first place where data transferred from Snowball is uploaded. It is common practice to use S3 intermediate storage for image-level and database backups.

## The Ultimate MSP Guide to Providing Backup-as-a-Service with MSP360 and AWS

Are you an MSP? Leverage potential of Amazon S3 as a part of your BaaS offering

[Download Now](#)



## Amazon S3 RRS

**Amazon S3 Reduced Redundancy Storage (RRS)** reduces storage costs for replicable and non-critical data. Amazon RRS is intended to sustain the loss of data for single facilities. This can be achieved by reducing the amount of data replicated across multiple devices and facilities. The main difference between RRS and S3 Standard is reliability (99.99%). This solution is perfect for non-critical, or easily replicable, data of applications. It doesn't suit maintenance for crucial data, though it can be used as a data buffer if you are dealing with large backups being transferred to multiple storage systems.

## Amazon S3 Standard Infrequent Access

Amazon Standard Infrequent Access (S3-IA) is designed for data that requires less frequent access than the Standard class. Low delays combined with high capacity and reliability (99.999999999%) ensure the safety of objects for a long period of time. Amazon S3-IA differs from Standard in the following ways:

- ▶ It offers 99.9% availability (which means it has a slightly greater chance of downtime, compared to standard storage).
- ▶ It imposes fees for data retrieval.

The minimum storage period is 30 days, and the minimum size of an object is 128 KB. This tier is recommended for long-term storage of user files, disaster recovery data, and backups.

## Amazon S3 One Zone - Infrequent Access

Amazon S3 Z-IA is 20% less expensive than the Amazon S3 Standard IA and has the same characteristics except for availability. Amazon S3 Z-IA stores files in only one physical data-center and has 99.5% data availability instead of the 99.9% offered by Amazon S3 Standard Infrequent Access and 99.99% availability in Amazon S3 Standard.

## Amazon Glacier

Amazon Glacier is for the long-term storage and archiving of backups that don't require instant access. The service allows storing large volumes of data at a low price. Amazon Glacier differs from S3 Standard in the following ways:

- ▶ Extremely low cost.
- ▶ Uninterrupted operation is not guaranteed by the Amazon S3 Service Level Agreement.
- ▶ The minimum period of storage is 90 days.
- ▶ There is a charge for data retrieval of more than 5% of the average monthly volume. You can access your data in four hours after the first request.



The service is optimized for infrequently accessed data, with retrieval time of several hours. It's beneficial for storing items such as old backups and outdated database records. AWS does not save objects directly in Glacier. S3 archives data in accordance with the Lifecycle Policy.

## Amazon Glacier Deep Archive

AWS has introduced Amazon Glacier Deep Archive, which builds on the features of standard Amazon Glacier storage. With the price for storing 1gigabyte/month starting at \$0.00099, it is the cheapest storage solution on the market.

In Amazon Glacier Deep Archive you don't have an option for an expedited data retrieval; the fastest retrieval time is up to 12 hours. The longest option — bulk retrieval — will take up to 48 hours.

Further reading

[Guide to Archiving to the Cloud: Cold Storage](#)

## Lifecycle Policy

All Amazon S3 classes are supported by the lifecycle policy, meaning you can optimize storage costs for objects by setting rules for automatic transfer to cheaper storage. It is also possible to set up the lifecycle termination policy so that the files are automatically removed after a certain period. This is useful for recovery data maintenance, as hot backups will always be available and old backups will go to the archive, resulting in reduced expenses.

For example, you can save a backup using Amazon S3 Standard, transfer it to Standard IA/Z-IA storage, and finally to Glacier. Later the backup can be removed, or placed into archive storage.

## Recovery

MSP360 Backup can make the recovery process easier with built-in consistency verification and by setting up multiple backup schedules. Make sure that the lifecycle policies on your local and cloud storage are correctly configured.

## Image-Level Recovery

If your storage is accessible, the process of full system restoration from an image can be initiated by a couple of clicks via the MSP360 Backup GUI. Image recovery is a difficult process. To avoid the loss of data, it is important to follow best practices to execute a successful recovery fully. Take precautions to avoid losing data that has been added or changed since the last image update. Here are a few actions to take before image-level recovery:

- ▶ Make a fresh backup of working data, system and application settings.
- ▶ Make sure that the databases are maintained separately, and their last backup is up to date.
- ▶ Carry out file-level recovery after image restoration to bring the machine into the state of readiness.

Be aware of any special requirements of your application regarding data recovery. For example, Microsoft Exchange and Active Directory restoration may require you to carry out additional adjustments after being unpacked from the image.





How do you go about performing an image-level restoration in case of disaster recovery? The steps are nearly identical, but you may not have a chance to make a differential file backup. A well-planned maintenance schedule and consequent image and file-level backups are key to IT infrastructure safety.

Data transfers should also be taken into consideration. Downloading images from 20 desktops and 3 servers can take a while. You must be ready for extensive downtime while backups are transferred, or additional costs for quick data transfer. AWS is faster and more convenient than offsite tape or disk storage services, as there are additional measures that can be taken to simplify recovery.

## Cloud to Virtual Machine Recovery

Amazon Web Services enables you to decrease your systems' downtime with virtual machines located in the same cloud as your backups. Recovery to Amazon EC2 can be performed directly within MSP360 Backup's Recovery Wizard. Here you can configure the virtual machine's type, connect it to the subnet, and adjust all other settings. The steps for achieving full recovery are the same as those for image-level recovery: Start with the latest full image, then deploy the latest version of working data.

While deploying Amazon EC2 instances from MSP360, you can choose to create AMIs. This option can be initiated from the AWS console anytime and helps start your machine with a personalized IP-address right after finishing Recovery Wizard. Otherwise, IP addresses should be configured within the Amazon Elastic IP service. Newly created instances should be launched from the Amazon EC2 Management Console.

## "Pilot Light" Recovery

The term pilot "light" describes a disaster recovery scenario in which a version of an environment is always running in a cloud. The term "pilot light" comes from a gas heating system that always has a small flame burning, as an ignition source for when the entire heater is turned on and more gas comes in. This principle can be used in recovery by deploying an AWS virtual machine that runs the most important core element of your IT infrastructure. If your local infrastructure fails, you can deploy all other elements, such as databases and file storage systems, around the pilot light core.

To provision the rest of your infrastructure, you should preconfigure the servers or other multi-user networking machines and save them as AMIs, which are ready to deploy on-demand. When starting recovery, EC2 instances come up quickly from these AMIs with their predefined roles (for example, Web or App servers).

The auto-scaling feature of AWS ensures that virtually recovered infrastructure has enough computing resources to cope with the existing workloads. However, you still need to restore working data to get the system to operating condition.

There are a few typical recovery scenarios that may be used at your discretion. Regardless of the strategy, ensure that your backups are fully functional, and recovery goes well by following these tips:

- ▶ Perform regular backup consistency checks to make sure that files are not corrupted.
- ▶ Perform recovery tests to ensure that restored systems and applications are functional.
- ▶ Create additional copies so that you have a plan B if something goes wrong (remember the 3-2-1 backup rule discussed above).



## Large Dataset Recovery

Nowadays businesses generate huge amounts of data, making recovery to new hardware and local storage systems more complex. While ordinary downloads from the Internet are possible, alternative tools are very useful with large recoveries. For recovery, download tools that are also used for uploading backups. Consider the peculiarities of your region, the quality of your Internet connection, and your data upload destination.

## Data Transfer

Not all data needs to be treated with the same level of urgency. A company may need a set of assets on a daily, weekly or yearly basis. Therefore, backup and recovery operations can be tailored to different scenarios:

- ▶ Archived information that is infrequently accessed.
- ▶ Immediate recovery for information that is crucial to business operations, where backup occurs daily.

The second scenario is common for big companies. The bigger a business's infrastructure, the more prone it is to data loss.

A standard AWS storage scheme copies user data to a geographically distant AWS server. Distance increases latency so that creating several large backups is more challenging. Amazon has developed two features to avoid reduce time spent on backup: S3 Transfer Accelerator and AWS Snowball.

## Amazon S3 Acceleration

Amazon S3 Transfer Acceleration is a built-in feature implemented in Amazon S3. When enabled for a bucket, it speeds up data exchange with the bucket by up to 6 times. Users can enable data transfer acceleration for a single S3 bucket, using a special Accelerated mode. After that, an alternative name is generated for the bucket. Specifying this name in the backup plan enables faster uploading and downloading.

Amazon uses its own networking resources to ensure accelerated data transfer. For each session, an optimal route based on AWS's own backbone network is selected. This route is built dynamically: channels with bigger bandwidth and less traffic load are found for each separate upload/download session.

Speeding up data transfer does not result in security level reduction. All data uploaded in the accelerated mode, as well as standard mode, are encrypted. Data is not stored in transit AWS edge locations, eliminating the risk of their leakage.

## AWS Snowball

As noted above, AWS Import/Export Snowball is a hardware solution that transports up to 80 terabytes of data directly from the user's location to the AWS network. Snowball devices are shipped to AWS customers on demand. A request is sent from the standard AWS console and takes approximately two days to ship.



Upon receiving an Amazon Snowball, the user must connect it to their network, install an AWS S3 client on it, transfer the file or system image copies, then ship it back to AWS. The data transferred to a Snowball device are automatically encrypted. After the device is shipped back, the user receives notifications on the progress of data extraction and transfer to the user's S3 buckets. In the United States, the overall cost of creating a large backup using Snowball will be several times lower than transferring the data via a high-speed Internet connection, if you are dealing with very large data sets.

**Total cost of retrieving 50 TB of data:  
comparison between S3 Acceleration and S3 Snowball**

	S3 Acceleration	S3 Snowball (80TB)
Cost	$\$0.04 \text{ (acc. fee)} + 0.07 \text{ (std. fee)} * 50 * 1024\text{GB (data retrieved)} = \$5,632$	$\$250 \text{ (device)} + \$0.03 \text{ (fee)} * 50 * 1024 \text{ GB (data retrieved)} = \$1,786$
Time	5 days	2 days
Additional Fees	None	Shipping fees
Other issues	Depends on your network	Depends on your physical location

Physically transporting large volumes of data this way helps to save networking resources. Imagine a situation where the user needs to make a 25 terabyte backup to an AWS S3 bucket but the network can supply only 4 Gbps. It will take about 25 hours to complete the transfer over the network (and that's assuming that network bandwidth is maximized at all times, which is unlikely because in practice it's rare to have full bandwidth continuously). The retrieval time will also vary depending on the type of data retrieved and changes in traffic load. In contrast, a Snowball device will transfer all necessary data offline, making the user's network fully available for other tasks.

MSP360 and Amazon collaborate closely to provide the best experience for customers leveraging AWS storage. MSP360 Backup and MSP360 Explorer support Amazon S3 Acceleration and Amazon Snowball Edge features. All options for your S3 bucket can be accessed directly from the MSP360 Backup user interface.

## Billing Calculations

Now, when you are aware of cloud-based backup and recovery, it's time to estimate its cost. Let us imagine a common company office with the following infrastructure:

- ▶ 20 desktop computers with Windows installed.
- ▶ 1 Microsoft SQL Database server.
- ▶ 1 Microsoft Exchange server.
- ▶ 1 file server.



The total amount of enterprise data is 10 terabyte. 70% of that consists of hot data (documents, working files, backups of crucial importance, etc.), database archives, and old system images. The business is growing quickly, with its data volume increasing 20% per year. The company chose the Amazon Northern Virginia region for offsite storage.

How might the company go about backing up this infrastructure, and how much does it cost per year? Let's walk through the different factors.

## Software Licensing Cost

For the office depicted above, the cost of MSP360 Backup would be the following:

- ▶ 20 MSP360 Backup Desktop Edition copies will cost \$39.99 per computer: \$799.80 total.  
**Note:** *The basic price is \$49.99 per copy. The wholesale discount for 20 computers is 20%.*
- ▶ MSP360 Backup for MS SQL costs \$149.99 per machine.
- ▶ MSP360 Backup for MS Exchange costs \$229.99 per machine.
- ▶ MSP360 Backup Server Edition for the file server costs \$119.99 per machine.
- ▶ You might also want to have MSP360 on the administrator desktop, which allows you to manage storage and data transfer. It costs \$39.99 in the Pro Edition.

The total price for MSP360 Backup licensing is \$1299.77 (without Explorer). There is no limit on how many times or how many user accounts the product supports on each machine, and you don't need to relicense recovered machines. If you have moved to different hardware or want to use MSP360 with recovered servers, the license can be easily moved from the old infrastructure to the new one.

## Storage Cost

For a 10 terabyte stack, comprised of 70% hot data and 30% cold data, the billing would be the following:

- ▶ 7 terabyte of frequent access data on Amazon S3 Standard costs \$2,541.84 per year.
- ▶ 3 terabyte of old archive data on Amazon S3 Standard Infrequent Access with 1 terabyte per month retrieval possibility costs \$583.68 per year (or \$466.94 using Amazon S3 OZ-IA).
- ▶ Since the data grows, 3 terabytes of archives will be superseded to Amazon Glacier Storage, costing \$258.12 per year.

**Note:** AWS technical support is provided for free for all kinds of storage systems.

The annual fee for AWS will be \$3,383.64 This total cost would be much lower if there was less hot data.



## Initial Seed Transfer Cost

Let's estimate the fee for sending a full enterprise data block to the cloud:

- ▶ Using the standard upload method, it will be free to send data, but it will also be time-consuming — at 100 Mbps, it takes 233 hours to transfer 10 terabytes of data.
- ▶ With Amazon S3 Transfer Acceleration it will cost \$400 (\$0.04 per gigabyte) when powered by the US, Europe, and Japan Edge locations, or \$800 (\$0.08 per gigabyte) if the bandwidth is accelerated by other locations.
- ▶ Transfer via AWS Snowball is priced in two stages. First, you pay a service fee for a Snowball job, which will be \$200 for a 50 terabyte device. Then shipping expenses are paid, and after that, a Snowball device can be located for 10 days free onsite. For every day beyond the initial ten days, a \$15 daily fee is charged. Uploading data to an Amazon data center is free.

## Disaster Recovery Cost

The first thing to do is to initialize recovery data download. The charge for doing so is as follows:

- ▶ With standard Internet transfer, you pay \$921.52 to get 10 terabyte data from S3 Standard Storage, and \$30.72 for access to 3 terabytes of S3 Infrequent Access data, totaling \$952.24.
- ▶ Using Amazon S3 Transfer Acceleration, you will be charged \$400 for getting all data out of the cloud. Together with the standard transfer fee, it will cost \$1321.52.
- ▶ AWS Snowball will cost \$200 per device and \$300 for downloading 10 terabytes of data from the cloud, \$500 in total. An additional \$15 will be charged every day upon exceeding the 10-day limit of onsite usage.
- ▶ AWS Disk expenses are the same as with backup upload: \$80 for device handling and \$14.94 for upload, totaling \$94.49. Keep in mind that the price of the disk is not included.

## Backup to Virtual Machine Recovery

Whatever data transfer approach you choose, it will take some time to download all data. It is a good idea to recover your infrastructure to EC2 virtual machines. AWS currently has 4 different pricing tiers for various EC2 use-cases, including:

- ▶ On-Demand Pricing and Spot Instances, useful for when you need to spin up a virtual machine suddenly, and could not plan ahead.
- ▶ Reserved Instances and Dedicated Hosts, useful for planned occasions.

Setting up Elastic IP and attaching Amazon EBS (Elastic Block Storage) volumes will require an additional fee, which depends on your system networking demands. Find out more on the Amazon EC2 pricing page.



To weigh all pros and cons, we have created a table with common pricing figures:

	Cost	Term
<b>SOFTWARE</b>		
MSP360 Licensing	\$1299.77	Forever
MSP360 Maintenance	\$300.00	1 year
<b>STORAGE ON AWS</b>		
7 TB of "hot" S3 Standard data	\$2,541.84	1 year
3 TB of "cool" S3 Standard IA data	\$583.68	1 year
3 TB of "cold" Glacier data	\$258.12	1 year
<b>RECOVERY TO A VIRTUAL MACHINE</b>		
3 servers (File Server, SQL, Exchange)	\$91.88*	7 days
<b>BACKUP UPLOAD COST</b>		
Standard Internet Upload	Free	
S3 Transfer Acceleration	\$400 (\$800 outside the USA)	
AWS Snowball	\$200**	
AWS Import/Export Disk	\$94.49***	
<b>RECOVERY DATA DOWNLOAD COST</b>		
Standard Internet Upload	\$952.24	
S3 Transfer Acceleration	\$1321.52	
AWS Snowball	\$500**	

\*EBS and networking cost is not included.

\*\*Delivery cost is not included



## Conclusion

The ideal backup strategy hinges on planning. Files should be maintained more often than full system images, and configurations should be maintained even more frequently to be ready for cloud recovery — because every minute of downtime means money lost. Moreover, the different data transfer options available to you should be explored.

Network transfer features must be tested so disk drives are prepared for data import and export. Amazon Web Services provides a universal platform for backup storage, virtual machine deployment, and data transfer. High levels of customization and a large array of tools optimize your IT operations on the cloud. MSP360's solutions empower you to master your infrastructure.

### Subscribe for more MSP content

Subscribe for our email newsletter to receive updates on the latest news, tutorials and comparisons

**Subscribe**

## About Amazon Web Services

For 10 years, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud platform. AWS offers over 90 services for compute, storage, databases, analytics, mobile, Internet of Things (IoT) and enterprise applications from 66 Availability Zones (AZs) across 21 geographic regions in the United States, Australia, Brazil, Canada, China, Germany, India, Ireland, Japan, Korea, Singapore, and the United Kingdom. AWS services are trusted by millions of active customers around the world — including the fastest-growing startups, largest enterprises, and leading government agencies — to power their infrastructure, make them more agile, and lower costs. To learn more about AWS, visit [aws.amazon.com](https://aws.amazon.com).

## About MSP360

Established in 2011 by a group of experienced IT professionals, MSP360™ provides cloud-based backup and file management services to small and mid-sized businesses (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 more than 20 online storage providers, including Amazon S3 and Amazon Glacier. MSP360 also collaborates with thousands of VARs and MSPs to provide them with turnkey, white-labeled data protection services. The company has been an Amazon Web Services Advanced Technology Partner since 2012. MSP360 has also achieved Storage Competency Partner status in the AWS Partner Network.