WHITEPAPER

Windows Backup Best Practices

Taking regular backups of your data is the most basic backup best practice. But optimizing backup routines and maximizing your chances of successful data recovery following a disaster require going further.

Read on for tips on getting the most out of backups. This whitepaper focuses on Windows backups in particular, although many of the takeaways apply to any type of environment.

Basic Windows Backup Rules

Core Windows backup best practices can be distilled into a set of basic rules:

- 3-2-1 backup: Always follow the 3-2-1 backup rule, which ensures you maintain at least three copies of your data at all times on two separate storage media, including one backup that exists off-site.
- **Define a data retention plan:** To avoid filling up your storage media or (if you store data in the cloud) spending money to store outdated backups, establish a data retention policy for removing older backups.
- Encryption is critical: Backups should always be encrypted. Except in rare cases, there is simply no reason not to encrypt.
- **Don't exclude files:** Unless you have a good reason, don't exclude files from backups. You may end up needing them later, even if you think you won't.
- **Enforce access controls:** Restrict access to backup tools and data to only those users who specifically require it. Resist the temptation to let anyone who happens to be on your team manage backups.
- **Test backups regularly:** Backups are of little use if you don't test them regularly to make sure that you can perform a successful recovery based on them.

Further reading Backup Testing Best Practices

- **Label backups:** Apply logical labels to backup data images, directories, and other files. Define labels based on the date of the backup and the system or data it includes.
- **Have a disaster recovery plan:** When something goes wrong and you need to restore from a backup, the last thing you should be doing is figuring out how to perform the restore. Make (and test!) a disaster recovery plan ahead of time, so you can proceed efficiently.

Further reading Building a Cloud Disaster Recovery Plan: Tips and Approaches

Other Best Practices for Windows Backups

Beyond these core best practices, you may want to consider some other policies for Windows backups, depending on the type of environment you are supporting.

Windows Backup Destinations

In general, Windows data should be backed up to two locations.

External Hard Drive Backups

Backing up data to external hard disks allows you to move the disks easily if you need to take them off-site during recovery. You can also replace aging disks quickly, without having to open up a physical server or worry about hot-swapping internal drives.

While you can buy individual external hard drives and manage them manually, you can streamline large-scale Windows backups by setting up a RAID array and (optionally) connecting it to the network so that you can back up multiple systems to one set of disks. RAID arrays may be overkill for simple backup needs, but they maximize backup reliability for high-value data.

Cloud Backup

In addition to external drives, you should also back data up to the cloud. Storage costs in the cloud may be lower than the cost of on-premises disks, and cloud providers tend to have a better record of ensuring data availability than local IT teams. Cloud backups are also immune to the risk of unauthorized physical access.

Although not all Windows backup tools support direct backup to the cloud, selecting a tool that does makes it easy to back up data quickly and easily to reliable, cost-effective cloud storage.

Windows Backup and Restore Terminology

Following are common terms that you might encounter when designing a Windows backup and restore strategy:

- Backup window. This refers to the span of time during which you allow backups to be performed. Since backup routines can drain your system resources, it may be advantageous to set your backup window for a time when you are not normally using your computer, or when your server is not experiencing heavy load.
- Full backup. A full backup means that you back up all data on your disk, including system files. In some cases, such as when you are backing up a Windows server, this is useful. For personal computers, it is more common to back up only personal files.
- Incremental backup. Incremental backups mean that, instead of creating an entirely new copy of your data each time you perform a backup, you copy only what has changed since the last backup.
- Open-file backup. In an open-file backup, you back up a file while it is in use. Depending on the type of file and the application that is using it, this may not work well. In general, it is better to back up files when they are not being used. However, modern backup applications are able to back up files in use, using the Windows VSS Snapshot service.
- Restore. When you need to recover data after a failure, your restore process is how you get it back in place. Planning a quick restore process is just as important as making sure to back up your data effectively.

Backup Scheduling Best Practices

To ensure backup consistency and prevent data loss, you need a solid backup schedule.

Types of Backup Schedules

There are three main types of backup schedules:

- **Real-time backup:** You back up files as soon as they are created or changed. This type of backup is best for your most important data.
- **Periodic backups:** You perform backups at fixed intervals, such as once per day. This approach works best when backing up large volumes of data.
- **Manual backups:** You can perform manual backups in the event that your automated backups fail for some reason, or they exclude important files. In general, however, you should avoid manual backups, because they are less reliable and require much more effort.

How to Choose a Suitable Backup Schedule

There is no one-size-fits-all rule for backup scheduling, but you should generally base your schedule on how often your data changes. The more changes that take place, the more often you'll need to perform backups.

You may also want to perform more frequent backups if you require more restore points. If you are worried about making a configuration change that breaks a system, for example, having multiple restore points to choose from when rolling back to an earlier configuration is an advantage.

Backup Scheduling Tips

Whichever approach you take, you can get the most value out of backup scheduling by following these rules:

- **Space out backups:** Leave some time between backup routines to ensure that each backup completes before the next one starts. Otherwise, you risk placing an unnecessary burden on your systems by running two backups at once.
- **Use lightweight backups:** Consider performing "lightweight" backups during the day for critical files. Save "heavy" backups -- meaning those that cover all of your files -- for nights or weekends.
- **Manage storage:** Carefully monitor your backup storage to ensure you don't run out of space. A small mistake when managing backup storage could have big consequences in the event that an important backup fails to run due to lack of space.

Use the Right Backup Software

There are lots of tools capable of backing up data. Some do it much more efficiently, affordably, and reliably than others.

MSP360 Managed Backup for Windows is a reliable and cost-effective solution that supports multiple cloud storage options, ensures security of your backups, and offers centralized management of backup jobs. Ensure the best Windows backups by choosing backup software that can work with any type of data and any storage location, all without breaking your budget.

About MSP360

Established in 2011 by a group of IT professionals, MSP360™ (formerly CloudBerry Lab) provides cutting-edge SaaS solutions that are simple, cloud-based, and profitable for Managed Service Providers.

MSP360™ Managed Backup (MBS) is the number one easy-to-use MSP backup solution for Managed Service Providers and IT departments worldwide. MBS allows MSPs to leverage the power of public cloud storage like AWS, Microsoft Azure, Backblaze B2, and Wasabi to increase profit while delivering best-in-class data protection to their customers.