

Backup Solution Guide

ASUSTOR NAS 3-2-1-1-0 Advanced Data Protection Guide

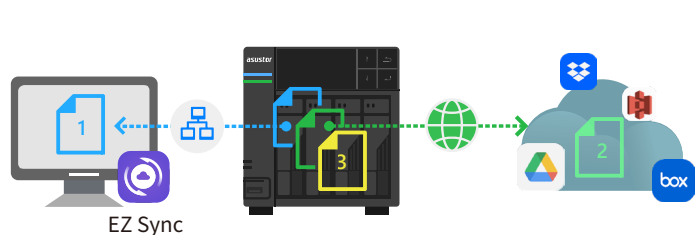


ASUSTOR NAS 3-2-1-1-0

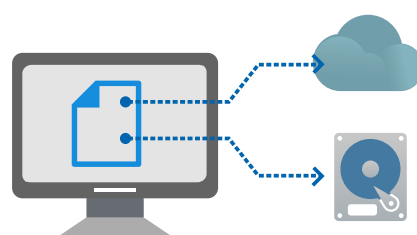
Advanced Data Protection

Whether a threat comes from a natural disaster or a man-made incidents, there are too many uncontrollable situations. Only comprehensive data backups can realize the concept of being prepared, allowing for data recovery when needed. With the evolution of ransomware and cybersecurity threats, ASUSTOR recommends upgrading your 3-2-1 backup strategy to a higher level of protection with the 3-2-1-1-0 backup principle. By leveraging the rich hardware and software features of ASUSTOR NAS, you can easily build a robust data protection network.

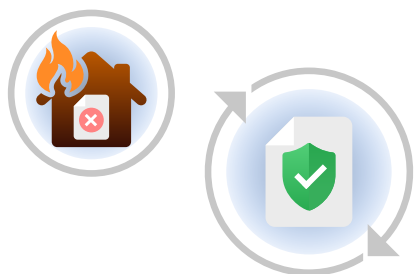
Decoding the 3-2-1-1-0 Backup Guidelines



3 Copies of Data: Prepare at least 3 copies of data, consisting of 1 original file plus 1 local backup and 1 offsite backup.



2 Different Types of Media: Store backups on 2 different types of storage media to diversify risk and avoid single points of failure.



1 Offsite Backup: In the event of fire, natural disasters, or equipment failure and human error, offsite backup is crucial for data recovery.



1 Offline or Immutable Backup: Ensure there is a copy of data isolated from the network, offline, or protected from tampering for a critical line of defense against ransomware encryption.

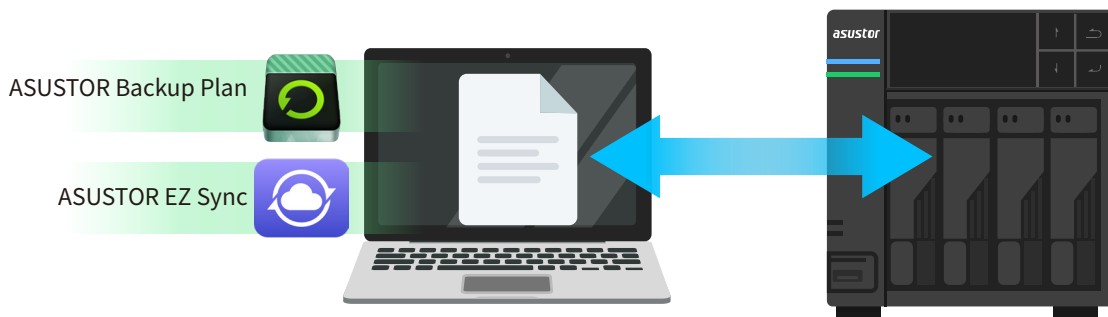


0 Backup Restoration Errors: The most important thing is to test whether data can be successfully restored after creating a backup strategy.

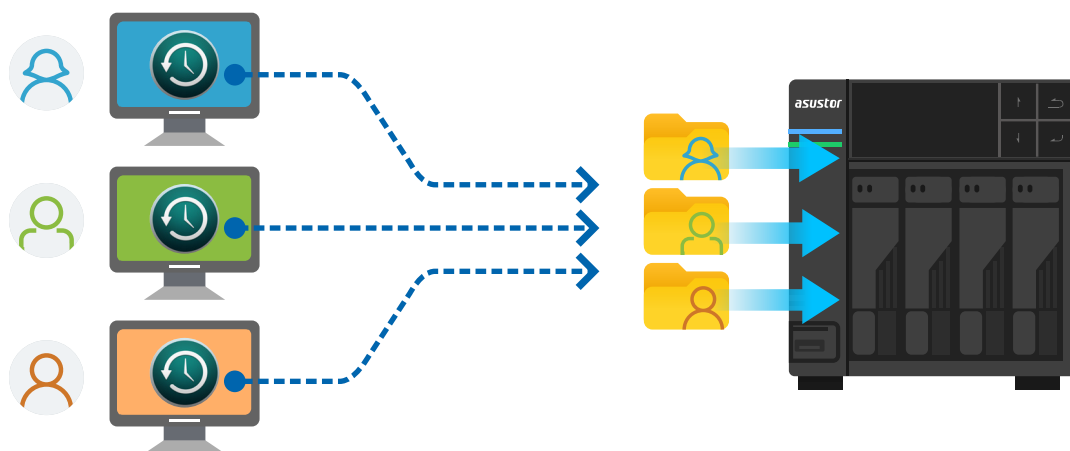
ASUSTOR NAS Comprehensive Backup Overview

To implement the 3-2-1-1-0 principle, the first step is to have your data stored in your ASUSTOR NAS, and the second step is to back up files from the NAS to separate local media while the third step is to back up to an offsite location. ASUSTOR provides extremely comprehensive backup tools, covering all common platforms and scenarios:

I. Backup from Endpoint Devices to ASUSTOR NAS for Centralization

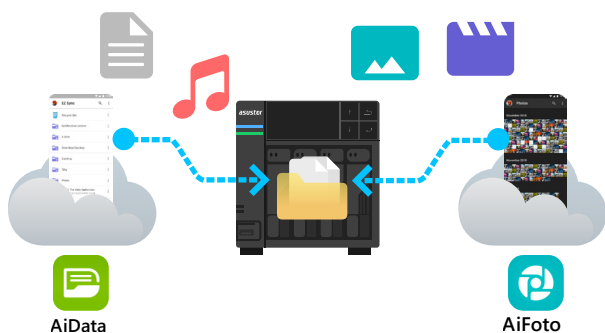


Windows: ASUSTOR's Backup Plan software performs real-time and scheduled backups. If original data is damaged, corrupt, or otherwise missing, data can be restored to its original location, minimizing damage. Additionally, use ASUSTOR EZ Sync to turn the NAS into a personal, high-capacity private cloud that synchronizes folders between your computer and NAS, and adds additional protection by supporting version history.

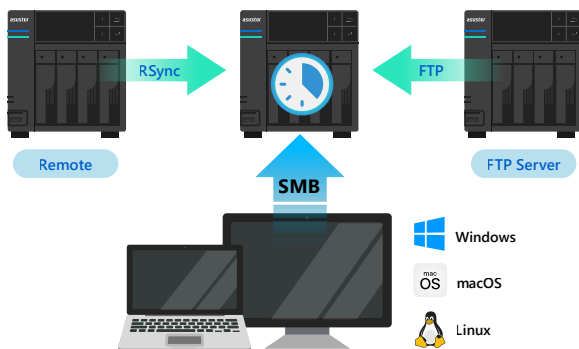


macOS: In addition to ASUSTOR EZ Sync, ASUSTOR NAS devices support Time Machine, which not only backs up your Mac completely to an ASUSTOR NAS but also supports multiple Macs. ASUSTOR NAS devices use separate accounts and storage locations ensuring that each Mac's backup exists independently and with privacy.

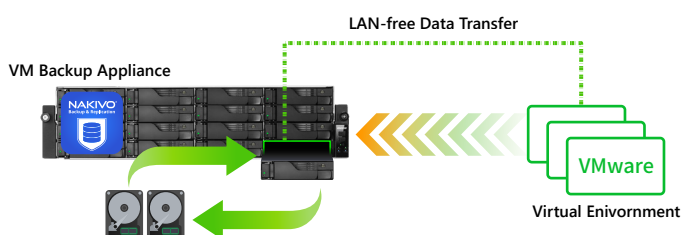
ASUSTOR NAS Comprehensive Backup Overview



Mobile Devices: Use AiData to display a file explorer on your phone to manually upload data to an ASUSTOR NAS for subsequent backup. To access, browse, and back up photos, AiFoto makes it easy to protect your photos on an ASUSTOR NAS and provides an easy way to instantly upload photos from your phone to an ASUSTOR NAS.



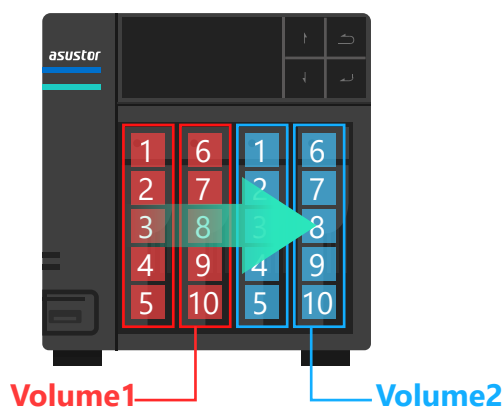
Cross-Platform: Use SMB backup to back up and restore data between most major operating systems. Windows, Mac, and Linux data can be backed up to an ASUSTOR NAS. For environments with frequently changing files and directories, Remote Sync on an ASUSTOR NAS provides block-level file copying. FTP backup supports incremental backup and allows you to configure scheduled tasks for the NAS to automatically operate, greatly reducing the burden on IT personnel.



Virtual Machines (VM): ASUSTOR partner, NAKIVO software, efficiently backs up individual VMware and Hyper-V virtual machines using global deduplication technology. Use NAKIVO to restore VMs to the virtual machine monitor, another VM execution host, or the NAS system running the virtual machine.

ASUSTOR NAS Comprehensive Backup Overview

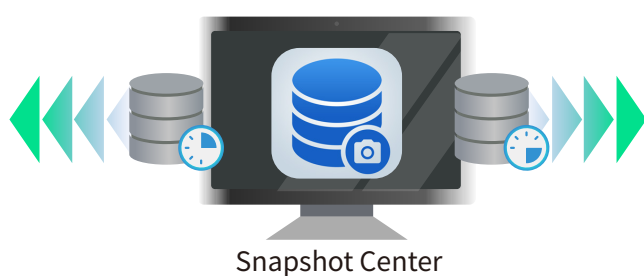
II. Advanced Protection



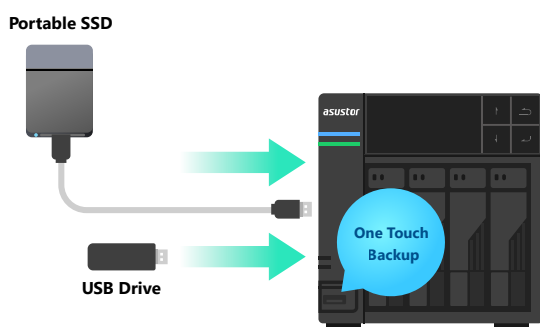
Backup Across Different Volumes:

Store backup data in an independent Volume within the same NAS system. This allows files to be restored when a single Volume is damaged or affected by ransomware.

**** Please note that RAID only provides protection against disk failures and does not replace a proper backup strategy.**



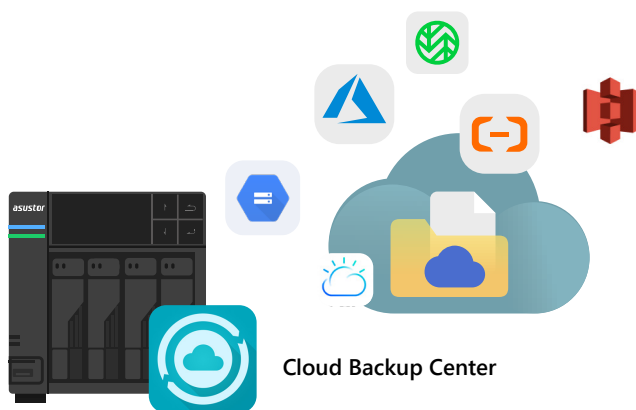
Snapshot Center: Use Btrfs to schedule or take manual snapshots to turn back the clock when data is lost or modified incorrectly. Snapshot Center supports the management of volume snapshots and iSCSI LUN snapshots, making it convenient to browse and restore data. Snapshots are not backups and serve to complement your backup strategy.



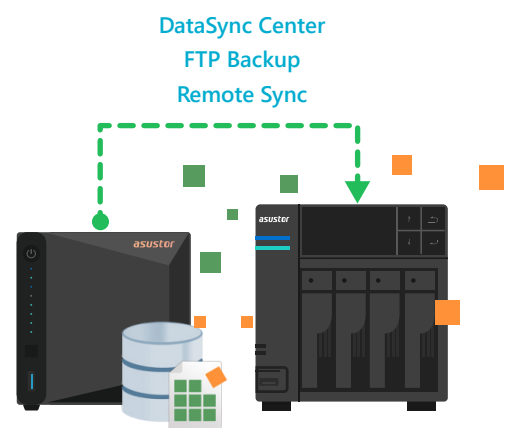
USB One-touch Backup: Use USB one-touch backup to set the direction and folders for backing up data using the one-touch backup button in front of an ASUSTOR NAS. After applying settings, simply connect an external USB drive to the front USB port and press the one-touch backup button to automatically perform a backup.

ASUSTOR NAS Comprehensive Backup Overview

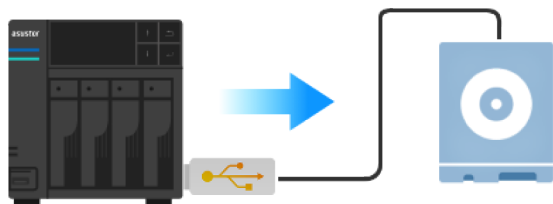
III. Building Offsite and Offline Protection Networks



Public Cloud Services: Cloud Backup Center can back up multiple common commercial cloud spaces, including, but not limited to Backblaze B2, Microsoft Azure Blob Storage, Amazon S3, and Google Cloud Storage. Cloud Backup Center supports immediate or scheduled backups as well as multi-account tasks. DataSync Center performs similar functionality with more mainstream cloud services like Dropbox, Microsoft OneDrive, Yandex, Baidu Netdisk, and Google Drive.



Backing Up to Another ASUSTOR NAS: Use SMB backup or Rsync to back up data to another ASUSTOR NAS easily. To back up to an ASUSTOR NAS in a remote location, use the Rsync network protocol, FTP backup, or DataSync Center for synchronization and backup.



External Device Backup: External device backup supports bidirectional and scheduled backups, allowing you to back up data to an external hard drive. Bringing the external hard drive to a different location completes the offsite backup.

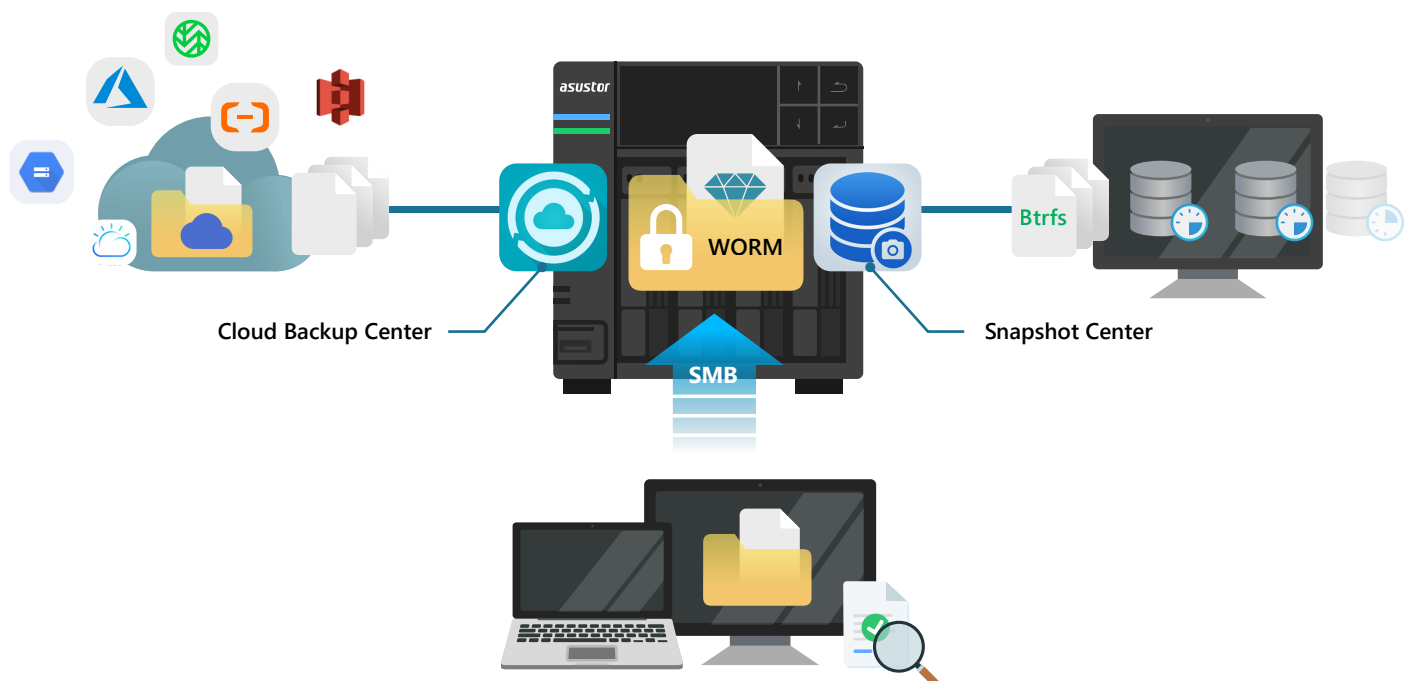


MyArchive Offline Archive: This is an ASUSTOR feature that turns NAS hard drives into immediately removable archive drives. After backing up data, removing and storing it offsite not only allows for instant plug-and-play convenience, but is also the best weapon against ransomware through physical isolation through an air gap.

3-2-1-1-0 Best Practice Demonstration

Best Practice One: Protection for Office Documents and Servers for Small and Medium-Sized Enterprises

For businesses that value business continuity, documents should not only be stored on a business computer, should be stored on an ASUSTOR NAS for centralized management allowing for instant access while a USB external drive backs up data locally. Then, IT personnel install Cloud Backup Center to synchronize important files to business clouds like Amazon S3, achieving 1 offsite copy. To prevent ransomware, the company enables Snapshot Center and configures WORM folders (achieving 1 immutable copy) and uses Btrfs to schedule snapshots. Finally, IT personnel must monthly test snapshots and restoration operations to ensure that files can be successfully restored, preventing wasted effort (achieving 0 restoration errors).



3-2-1-1-0 Best Practice Demonstration

Best Practice Two: Protecting Image Assets for Professional Photographers

A photographer's mobile phone photos automatically upload and back up to their studio's NAS through AiFoto, while the work Mac performs a complete backup to the NAS through SMB. Because video files are too large to be uploaded to the cloud, the photographer uses external drive backups to schedule backups of the NAS data to an external hard drive to achieve three copies of data on separate media. After the project ends, the photographer stores important original photo libraries that require long-term retention into a hard drive with the MyArchive feature of ASUSTOR, removes the drive and takes it home for storage to simultaneously achieve 1 offsite and 1 offline copy. Before storing, the photographer reads the hard drive back into the NAS and tests whether the files are complete (achieving 0 restoration errors).

