Synology

Active Backup for Business Admin Guide for Linux

Based on Active Backup for Business 2.7.0

Last updated: May 6, 2026

Table of Contents

Introduction 2
About this guide 2
Intended audience 2
What is Active Backup for Business? 2
Features and Management Tools 3
Backup and recovery features 3
Backup management 4
Planning and Preparation 5
Requirements 5
Considerations and limitations 6
Backup tips 6
Backup Configuration 8
Linux backup 8
Create a backup task 9
Manage backup tasks 11
Restoration Guide 13
Recovery options 13
Restore an entire device 14
Recover individual files 14
Instantly restore as a virtual machine 15
Fully restore as a virtual machine 16
Instant Restore to Synology Virtual Machine Manager (VMM) 17
Best Practices 19
Maintain remote backup copies and relink 19
Learn more 21
Related articles 21
Software specs 21
Other resources 21

Introduction

About this guide

This guide will help you become familiarized with Active Backup for Business, walk you through the initial setup of a backup task, and provide information on recovery.

Intended audience

This guide is intended for anyone who wants to start using Active Backup for Business to back up their Linux devices.

What is Active Backup for Business?

Synology's all-in-one commercial data protection solution, **Active Backup for Business (ABB)**, is based on the award-winning DSM operating system. ABB centralizes data protection across a variety of IT environments, including virtual machines, physical servers, file servers, and personal computers. Administrators can deploy their preferred protection plan single-handedly through ABB's centralized admin console.

ABB also offers a wide range of backup options and restoration tools, as well as a number of optional technical and safety features.

Why should you use Active Backup for Business?

- **Your one-stop-backup solution** – Ensuring that everything in your backup environment is compatible can be a challenge, especially with so many factors to consider. ABB simplifies things by providing an all-in-one solution right on your Synology NAS.
- **Smart storage** – ABB is designed with cross-platform, device, and version deduplication to help reduce backup time and improve storage efficiency. (See applicable models)
- **Unrestricted expand-ability** – Increasing your number of devices and data? No problem. With ABB, you can protect an unlimited number of devices and data, license-free.
- **Centralized management** – Remove the burden on IT workers of managing backup tasks and devices across several platforms by using ABB's intuitive, web-based portal.
- **Integrated support** – When something goes wrong, whether it's hardware or software-related, Synology Technical Support is ready to help, reducing the time and effort needed when looking for help from different providers.

Features and Management Tools

Backup and recovery features

Incremental backup

Incremental backup is a backup feature that reduces the amount of data transferred for each backup, as well as the amount of duplicated data stored on your backup destinations. This is done by tracking changes and only backing up modified or new data in between full backups. This maximizes the number of available backup versions, minimizes the amount of storage used for backup retention, and also saves time and bandwidth on the source device.

The CBT technology adopted in Active Backup for Business is implemented through the snapshot driver that is installed on your device during installation of the Active Backup for Business Agent. This driver records the differences between the previous and current backups, so that only changed blocks are backed up.

Data deduplication

Active Backup for Business (ABB) detects and removes any data that are identical between different files, versions, or devices when storing backups on Synology NAS. Built-in deduplication technology can help cut back on storage use, especially when the devices share similar operating systems, software applications, or files.

For more detailed information on data deduplication techniques and how deduplication is calculated for ABB, refer to the Data Deduplication White Paper.

Built-in hypervisor

Active Backup for Business (ABB) can use **Synology Virtual Machine Manager (VMM)** as a recovery environment for physical server backups, supporting features such as **Backup Verification** and **Instant Restore**.

Synology VMM is supported only as a restore destination. Active Backup for Business (ABB) does not support backing up virtual machines created in Synology VMM.

Backup Verification

If **Backup Verification** is enabled, a scheduled trial restoration of physical server backups will be performed in VMM for a configured number of seconds. This process will be recorded into a video for your reference, so you can confirm that the backed up data can be successfully restored in case of sudden disaster.

Instant Restore

Instant Restore allows you to instantly restore physical servers and VMware vSphere or Microsoft Hyper-V virtual machine backups from ABB as virtual machines in Synology VMM. You can use this feature to implement rapid recoveries while continuing to use services in case of system crashes.

Backup management

Active Backup for Business Agent

The **Active Backup for Business Agent** is a utility that is installed on your client device before backing up data in order to carry out backup tasks. Administrative privileges are required to install, update, or uninstall the agent.

This tool is available for download in the Download Center. Refer to the ABB Agent help article for installation instructions, details on mass deployment, and other information.

Active Backup for Business Portal

The **Active Backup for Business Portal** is ABB's affiliated restoration portal. This portal allows administrators and end users appointed by an administrator to access, browse, download, and restore backed-up data.

This tool is automatically installed during the installation of the Active Backup for Business package. Refer to the ABB Portal help article to learn more about how to navigate the portal, perform restores, and for other settings.

Active Backup for Business Recovery Media Creator

Synology **Active Backup for Business Recovery Media Creator for Linux** is a desktop tool that can be used with ABB. This tool should be installed on your Linux device when creating recovery media for bare-metal or volume-level restores.

For Linux devices, you need to create a bootable USB recovery drive with ISO burning software, for Legacy BIOS, or for UEFI. Refer to create a bootable USB recovery drive for Linux devices for detailed instructions.

For more information about recovery media creation for Linux, refer to the **Create Recovery Media for a Linux Device** section in the Recovery Media Creation Guide.

Planning and Preparation

Requirements

See the full specifications for Active Backup for Business for detailed information.

NAS system requirements

See How to select a suitable NAS for running Active Backup for Business? for recommendations.

Item	Requirements
Operating system	• DSM 7.0 and above (ABB 2.2.0 and above) • DSM 6.2 and above (ABB 2.2.0 and above)
CPU architecture	64-bit x86 (x64)
System memory	4 GB RAM recommended for ideal backup performance
File system	Btrfs

Supported systems

Backup type	System / version

Linux	• System kernel versions from 2.6 to 6.8
	• Supported distribution platforms:
	  ◦ CentOS 7.8, 7.9, 8.1, 8.5
	  ◦ RHEL 6.10, 7.8, 7.9, 8.1, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4
	  ◦ Ubuntu 16.04, 18.04, 20.04, 22.04, 24.04
	  ◦ Fedora 38, 39, 40
	  ◦ Debian 10, 11, 12

For a full list of requirements for backups and restorations, refer to the Requirements and Limitations.

Considerations and limitations

NAS

- To maximize backup performance, avoid running too many packages at once in DSM.
- To perform a backup task, there should be at least 8 GB of free space both on the backup destination and on the volume where the package is installed.

Backup client (Linux devices)

- The backup client should use the **ext2**, **ext3**, **ext4**, or **XFS** file system.
- ABB leverages Linux snapshot driver-based Changed Block Tracking to perform incremental backups. Make sure to reserve an appropriate amount of disk capacity for snapshot storage.
- For external devices: Only external hard drives can be backed up. The backup of other external devices, such as floppy disks, thumb drives, and flash card readers is not supported.
- The backup of computers with 4Kn disks is not supported.
- The backup of virtual hard disks (VHDs) on Windows is not supported. To back up VHDs, you need to either back up the **entire device** or back up the **volume** where the VHD files are located.
- Only the following device types are supported: /dev/sdx, /dev/hdx, /dev/vdx, /dev/nvmex, /dev/mdx.

Network

- To establish a secure connection between the NAS and the client, make sure that DSM has a valid certificate for ABB.
- If you will use DDNS or an IP address to connect to the server from the agent, refer to our suggested network configurations.

Backup tips

- Make sure that the device that you want to back up is supported on your version of ABB.
- Set up a **Retention Policy** for your backup tasks to delete older backup versions so your backups don't take up too much space.
- Configure a **backup schedule** to maintain regular backups of your data.
- Allow users access to the **Active Backup for Business Portal** so they can browse backups and recover individual files or entire folders as needed.
- Add a second layer of protection to your data by implementing the 3-2-1 backup rule (3 backups: 2 on different storage mediums and 1 offsite) using **Hyper Backup** or **Snapshot**

Replication.

Backup Configuration

The following sections provide instructions on preparing backup targets, creating and executing backup tasks, and configuring options and settings.

Linux backup

Active Backup for Business allows you to back up your Linux devices with the help of the Synology Active Backup for Business Agent.

Before you start

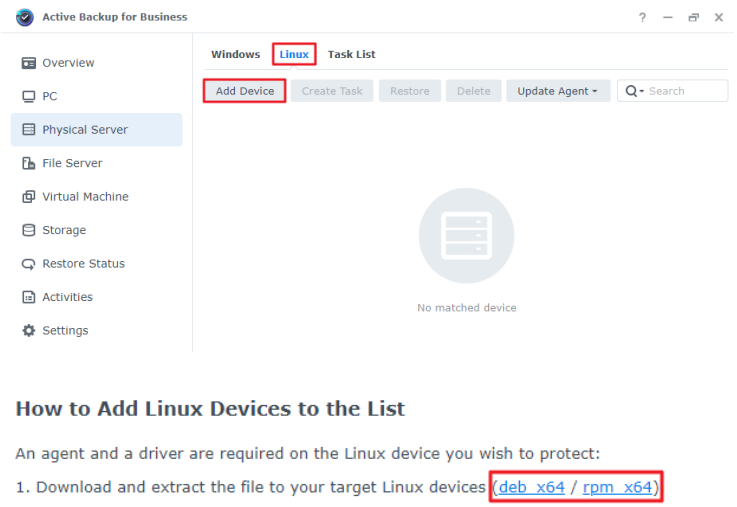
1. Install the **Synology Active Backup for Business Agent** on the target device that you want to protect. Go to the Synology Download Center or **Active Backup for Business Physical Server** > **Add device** to download the 32-bit or 64-bit installer for the device.
2. Configure a **template** in **Active Backup for Business**. Go to **Settings** > **Template** > **Create** to make a new template, or select the default template and click **Edit**.

Notes:

- ABB uses TCP network port **5510**.
- Configuring backup settings in a **template** allows you to apply the same backup settings to multiple devices. The default backup template is always listed and cannot be removed.
- When creating a template, you can select the **backup type**, **backup schedule**, **compression settings**, **encryption settings**, and **version retention policy**.

Add a device

1. Download the **Synology Active Backup for Business Agent** with the compatible file type from the Download Center > **Desktop Utilities**, or via **Active Backup for Business** > **Physical Server** > **Linux** > **Add Device**.



2. After extracting the downloaded file on your target Linux device, follow the steps in the README file and execute sudo ./install.run to install the snapshot driver and agent on your Linux device.

Create a backup task

Once the Active Backup for Business Agent is installed on the Linux device connected to your NAS, a backup task is created according to an applicable **template**. You can create more than one backup task for each device.

1. Go to **Physical Server** > **Linux**, select a device, and click **Create Task**. You can also do this at **Physical Server** > **Task List** > **Create**.
2. If you didn't select a device before clicking **Create**, a **Select Target Device** page will appear. Select your physical server from the list.
3. Follow the steps in the wizard to name the task, select a target device (if not yet selected), and choose a backup destination.

Select a source type

You can select:

- **Entire device**: Back up full servers, including settings and applications.
- **System volume**: Protect partitions with Linux system data.
- **Customized volume**: Manually select backup targets. Note that external devices other than external hard drives are not supported.

Select a backup destination

1. Make sure that your backup destination is using a **Btrfs file system**. A shared folder named "**ActiveBackupforBusiness**" is automatically created when you install Active Backup for

Business on your NAS.

2. Select a shared folder in the Btrfs file system as the backup destination.

Task settings

- You can enable data transfer compression, data transfer encryption, and application-aware backup.
- Compression and encryption can be enabled for the backup destination.
- You can select **Backup Verification** to run scheduled trial restorations of physical server backups in **Virtual Machine Manager**. The entire process will be recorded as a video for reference, so that you can confirm that the backup can be successfully restored.
- You can customize pre/post scripts when performing **physical server** backups.

Notes:

- The compression and encryption settings of a backup destination **cannot** be changed after the first backup task is created. If you want to use different settings for future tasks, create a task in a new destination.
- If compression or encryption are enabled for the backup destination, NAS models with the following package arches **cannot** perform **Instant Restore to Microsoft Hyper-V**, **Instant Restore to Virtual Machine Manager**, or **Backup Verification**: Avoton, Braswell, Bromolow, Cedarview, and Grantley.
- **Synology Virtual Machine Manager (VMM)** must be installed to enable **Backup Verification** for physical server backups. Virtual machines created in Synology VMM can't be backed up or restored directly through ABB. Synology VMM is used only for backup verification and as a restore destination.

Schedule backup tasks

- **Manual backup** requires you to start each backup task manually.
- **Scheduled backups** can be set to run on an hourly, daily, or weekly basis.

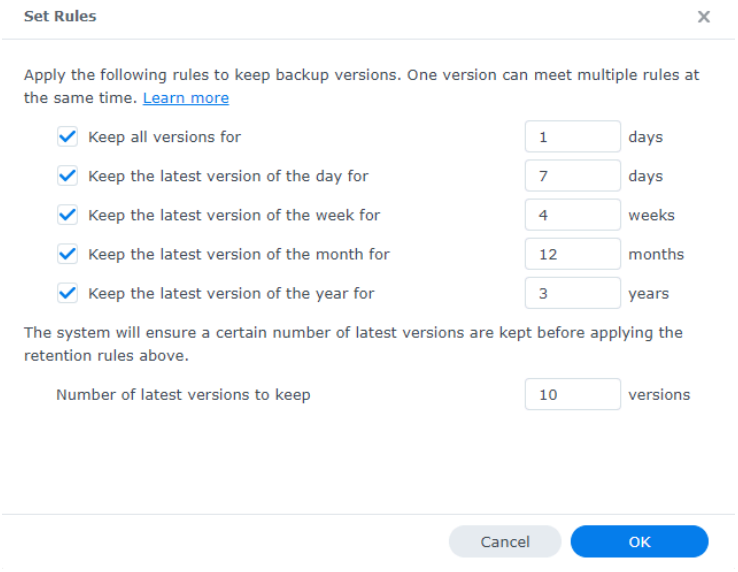
If you don't want tasks to run while your IT infrastructure is under heavy use, select **Configure Backup Windows** and set time slots for when the backup task can run each week.

Select a Retention Policy

- You can choose to store all versions of your backup, limit the number of stored versions, or only keep certain versions according to a schedule.
- You can choose to set rules for keeping backup versions, such as to retain the latest version of each day, week, month, or year. You can edit the retention policy at **Active Backup for**

Business > **Physical Server** > **Task List** > select the task > **Edit** > **Retention** > **Advanced retention policy** > **Set Rules**.

- Selecting the **Keep only the latest ... versions** option will store a certain number of versions regardless of the time intervals set. If more than one backup version exists within a certain time range, only the latest one will be kept. For example, if you set a policy as **Keep the latest version of the day for** "1" **day** for a backup task that will run every hour, only the version backed up at 23:00 will be kept.
- A version can meet more than one retention rule at a time. For example, a version can be retained by the weekly retention rule and the daily retention rule at the same time. Advanced retention policy employs a **Long-Term Retention Policy (GFS)**.



Manage backup tasks

All existing tasks are displayed under **Active Backup for Business** > **Physical server** > **Task List**.

Edit or delete backup tasks

To edit tasks individually or several tasks simultaneously, go to **PC** or **Physical Server** > **Task List**, select one or several tasks (Ctrl + left click), and click **Edit**.

- The **Backup destination** cannot be changed.
- **Task settings** and **Source type** can be changed both individually and simultaneously.
- The **Task name** can only be changed individually.

To delete backup tasks, select one or more tasks in the corresponding task list. Once you confirm the action, all backed up data will be removed along with the backup task.

Deleting tasks does not remove **Active Backup for Business Agent** from the client devices, which will continue to be displayed under **Physical Server**. Templates are preserved under **Settings** >

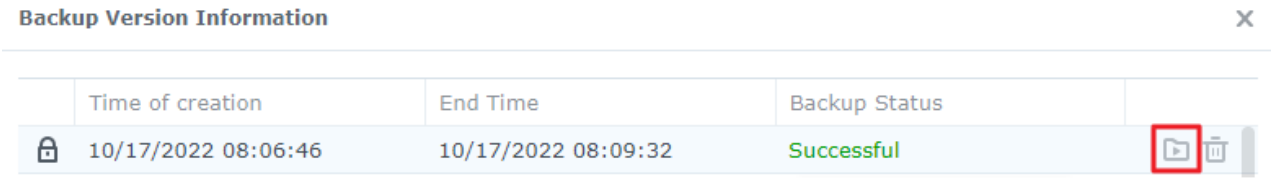
Template.

Details

To view information on the **Status** and **Logs** for your task, such as the source, execution time, duration, and log time of backups, select your task and click **Details**.

Versions

To view information about backed up versions, such as the status and time of creation, select your task and click **Version**. You can also click the **folder** icon to browse your backed-up data and the live video of the backup if **Backup Verification** is enabled.



Update the agent

If your Synology NAS is connected to the internet, go to **Active Backup for Business** > **Physical Server**. Select the target device that needs an update and click **Update Agent**.

If your Synology NAS is **not** connected to the internet, but is on a private network:

1. Download the **Active Backup for Business Agent** installer from the Download Center, and upload it to any folder on your Synology NAS using **File Station**. Make a note of the location of the installer.
2. Sign in to DSM with root permissions on your device.
3. Execute the following command to install the agent on your target devices:

   ```
   cp /[volume_where_you_uploaded_the_installer_]/[name_of_the_folder_where_you_uploaded_installer]/[installer_name]/[volume_where_you_installed_Active_Backup_for_Business]/\@tmp/
   ```

   For example, if the location of the installer is */volume1/Files/Synology Active Backup for Business Agent-2.2.0-1531-x64-deb* and Active Backup for Business is installed on *volume1*, then the command should be:

   ```
   cp /[volume1]/[Files]/[Synology Active Backup for Business Agent-2.2.0-1531-x64-deb]/[volume1]/\@tmp/
   ```

4. After completing the setup, the agent will be successfully updated.

Restoration Guide

Active Backup for Business offers several methods to restore your Linux device backups. Which method is best for your case depends on if you only want to recover files or restore an entire device to a previous state. Linux backup tasks also support recovery as a virtual machine.

Recovery options

- **Entire device restore**: Create a bootable ISO image or USB drive and boot your device into the wizard via the **Active Backup for Business Recovery Media for Linux**. You can later restore your full device (bare-metal restoration) or a specific volume over the network via your Synology NAS if necessary.
- **Granular (file or folder-level) restore**: Choose a backup version, select files or folders for recovery in the **Active Backup for Business Portal** and automatically restore them to their original location, or download the data to a different device or location. You can also assign end users restore or download permissions via **Control Panel** in DSM.

Linux physical server backup tasks can also be restored as virtual machines to VMware vSphere, Microsoft Hyper-V, or Synology VMM via the following methods:

- **Instant Restore**: Convert the Linux device's backed-up images to a virtual machine in VMware or Hyper-V. This method can restart a virtual machine directly from a compressed and deduplicated backup file to minimize the downtime of the virtual machine. This method can restart a virtual machine within seconds, but has limited I/O performance.
- **Full Virtual Machine Restore**: Convert the Linux device's backed-up images into a virtual machine in VMware or Hyper-V. This method can restore an entire virtual machine from a backup file to its most recent state or a previous point in time if the primary virtual machine fails. This method requires more time and resources, but has full I/O disk performance.
- **Instant Restore to Synology Virtual Machine Manager (VMM)**: During urgent cases when tolerance for downtime is limited, mount the backed-up image of your physical server onto **Synology Virtual Machine Manager (VMM)** and power it on to continue operations. This method requires Synology VMM to be installed on DSM.

The following table compares available recovery methods for physical server backups:

Item	Full Restore	Instant Restore to VMware	Instant Restore to Hyper-V	Instant Restore to VMM
Recovery Time Objective (RTO)	Long RTO	Short RTO	Short RTO	Short RTO

I/O performance	Full disk	Limited disk	Limited disk	Full disk (NAS)
Service location	VMware or Hyper-V	VMware	Hyper-V	NAS
Backup data storage location	VMware or Hyper-V	NAS	NAS	NAS
Post-restoration requirements	No further action required if restoring to the production site	Need to migrate back to the production site to finalize	Need to export and import back to the production site to finalize	Need to migrate back to the production site to finalize

Restore an entire device

Synology Active Backup for Business Recovery Media for Linux is implemented through the use of ISO images, which can also be burned to a USB. To create recovery media for Linux, go to the Download Center and download **Synology Active Backup for Business Recovery Media for Linux (Synology-Recovery-Media.iso)**.

To create a bootable USB recovery drive with ISO burning software, for Legacy BIOS, or for UEFI, refer to the instructions in create a bootable USB recovery drive for Linux devices.

Since the recovery wizard is already embedded in the **Active Backup for Business Recovery Media for Linux (Synology-Recovery-Media.iso)**, it will start up automatically when booting up your Linux device using recovery media.

Recover individual files

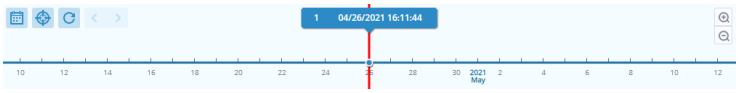
Individual file and folder restore is done through the **Active Backup for Business Portal**. Administrators can delegate restore permissions during task creation and task editing.

Restore files or folders from DSM

Administrators and accounts administrating Active Backup for Business can access the **Restore Portal** from any device. Use the following steps to restore files to the original backup source device or download them via your browser.

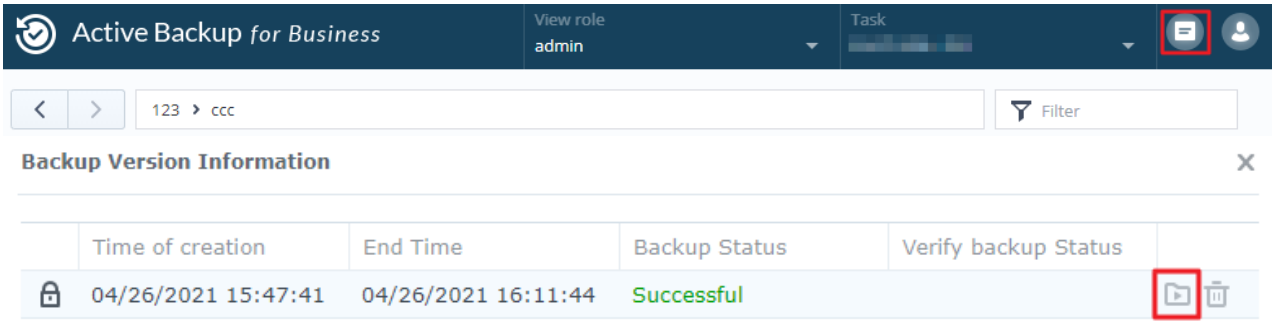
1. Go to the **DSM Main Menu** and select **Active Backup for Business Portal**.
2. Under **View role** at the top of the page, select a user with the appropriate restoration privileges.

3. Under **Task**, select the source device to which or from which you want to restore files.
4. Select the folders or files that you want to restore.
5. Use the slider at the bottom of the page to select a backup version from which you wish to restore folders or files, then click through the folder structure in the file explorer to select the directory or file.



6. Choose if you want to **Restore** or **Download** the data. If you select **Restore**, your backup agent will download the files or folders and restore them to the specified location on your device. You can also choose if you want files with the same name to be skipped during the restoration by ticking the related checkbox. If you select **Download**, then the selected files will be downloaded via your browser to your chosen download location.
7. Choose the destination where you want to restore your files, then click **Apply**.

You can view the progress of the restoration by clicking the **Restore Task** icon in the upper right-hand corner.



Instantly restore as a virtual machine

With **Instant Restore to VMware** and **Instant Restore to Hyper-V**, you can launch the restore wizard to restore a physical server as a virtual machine to its most recent state or to any available restore point through the methods below.

Launch the Instant Restore Wizard

1. Go to **Active Backup for Business** > **Physical Server** > **Linux**, select the device that you want to restore, and click **Restore** to launch the restore wizard.
2. Select the device and restore points, choose **Restore to VMware vSphere** or **Restore to Microsoft Hyper-V**, and then select **Instant Restore**.

Notes:

- Make sure that the hypervisor is authorized to access and mount the iSCSI target on your Synology NAS. When performing **Instant Restore to Hyper-V**, a backup image will be cloned to a temporary iSCSI target on your Synology NAS, and then the hypervisor will mount the iSCSI target.
- **iSCSI Initiator Service** must be enabled on the source server for the system to perform **Instant Restore to Hyper-V**.

Configure restore settings

Specify a name for the new VM, then select the folder, Hypervisor, and network where you want to restore the device.

Apply and Restore

A summary of the restoration will be shown. Once you have confirmed the information to be restored, click **Done**. You will then be automatically directed to **Restore Status** to monitor the restoration progress.

For **Instant Restore to VMware**, click the **Migrate VM** button to finalize the process.

Enable **Power on VM automatically after restoration** to immediately run the virtual machine. If you are performing **Instant Restore** for testing purposes, we recommend you to keep this option **deactivated** and to manually disconnect the initial virtual machine from the production network to avoid any conflicts.

Fully restore as a virtual machine

With **Full Virtual Machine Restore**, the backed-up images of your Linux device will be converted to a virtual machine in VMware or Hyper-V. The virtual machine can then be restarted in VMware or Hyper-V directly from a compressed and deduplicated physical server backup file to minimize downtime.

Launch the Full VM Restore Wizard

1. Go to **Active Backup for Business** > **Physical Server** > **Linux**, select the device that you want to restore, and click **Restore** to launch the restore wizard.
2. Select the device and restore point, choose **Restore to VMware vSphere** or **Restore to Microsoft Hyper-V**, and then select **Full Virtual Machine Restore**.

Configure restore settings

Specify a name for the new VM, then select the folder, Hypervisor, Datastore, and network where you want to restore the device.

Apply and Restore

A summary of the restoration will be shown. Once you have confirmed the information to be restored, click **Done**. You will then be automatically directed to **Restore Status** to monitor the restoration progress.

Enable **Power on VM automatically after restoration** to immediately run the virtual machine. If you are performing **Full VM Restore** for testing purposes, it is recommended to keep this option **deactivated** and to manually disconnect the initial virtual machine from the production network and connect it to an isolated non-production network to avoid any conflicts.

Instant Restore to Synology Virtual Machine Manager (VMM)

Active Backup for Business can use **Synology Virtual Machine Manager (VMM)** as a restore environment for Linux physical server backups. This provides an alternative method for disaster recovery, browsing and restoring application data, and setting up test environments.

When you need to limit downtime as much as possible, you can mount the backed-up image of your Linux physical server on **Synology Virtual Machine Manager (VMM)** and power it on to continue operations. To do this, **Synology Virtual Machine Manager** must be installed on DSM.

This section provides the prerequisites and instructions for instantly restoring your backed up device via Synology VMM.

Refer to the Virtual Machine Manager product specifications for more information on its limitations, features, and other details.

Launch Synology VMM Wizard

Go to **Active Backup for Business** > **Physical Server** > **Linux** and select the device that you want to restore. Click **Restore** to launch the restore wizard, choose the device and restore point, and then select **Instant Restore to Synology Virtual Machine Manager (VMM)**.

Notes:

- Only one physical server backup can be instantly restored to Synology VMM at a time. Multiple physical server backups cannot be run as virtual machines at the same time.

Configure virtual machine settings

Once you have selected a physical server and restore point, you will need to configure the virtual machine settings in the Synology VMM wizard.

Apply and restore

After you have configured the settings, click **Done**. The backed-up physical server will be imported to Synology VMM as a virtual machine, and you can power it on in the Synology VMM console.

Best Practices

The following sections provide recommendations for how you can protect your backup data against loss by creating remote backup copies and relinking.

Maintain remote backup copies and relink

Active Backup for Business safely stores backup data from all of your devices on your Synology NAS. However, issues that occur on one device can affect an entire infrastructure.

Natural disaster, theft, or network issues can prevent you from retrieving your data or slow down the recovery process. Therefore, we strongly recommend you to keep remote copies of all of your backups on a different device and in a different location.

Keep in mind that you should always maintain three copies of your data (the original copy, a backup, and a copy of that backup in a different location). This is referred to as the 3-2-1 backup strategy. To make things easy, Synology NAS has everything you need to implement this strategy.

Create remote copies

The following two DSM applications can be used to copy your Active Backup for Business data and configurations from Synology NAS to other devices or the public cloud.

- **Snapshot Replication**: This option is recommended if you have access to a secondary Synology NAS. You can replicate your ABB data and settings to another Synology NAS and quickly restart all of your ABB tasks on that device.
- **Hyper Backup**: This option allows you to back up your ABB data and settings to other locations, such as portable drives, file servers, and public cloud storage. However, recovery requires you to first restore the backup to a functioning Synology NAS before relinking and restarting ABB tasks.

Relink

After creating a replication or backup task, it is important to make sure that you can successfully restore or relink your existing Active Backup for Business tasks and backup data, whether they exist on a secondary NAS, in public clouds, or other storage media.

For detailed instructions on how to back up and relink your Active Backup for Business data using **Snapshot Replication** and **Hyper Backup**, refer to the following tutorial:

- How do I back up and relink Active Backup for Business data to a destination Synology NAS?

Make sure that your Synology NAS has 64-bit processors, is running DSM 6.1.7 or above, is running Active Backup for Business 2.0.4 or above, and has the necessary packages installed. See the **Environment** section in the tutorial for more details.

Learn more

Related articles

- Frequently asked questions about Active Backup for Business
- How do I select a suitable NAS for running Active Backup for Business?
- How do I back up and relink Active Backup for Business data to a destination Synology NAS?
- How can I restore entire device backups from Active Backup for Business in Virtual Machine Manager?
- I restored my Linux system with Active Backup for Business, but it fails to boot. What can I do?
- How many devices can I back up concurrently with Active Backup for Business?

Software specs

Refer to the Active Backup for Business software specifications to learn more about the package's features, components, and limitations.

Other resources

For more step-by-step tutorials and visual information, feel free to also check out Synology's YouTube channel. There, you can find related videos by searching for "Active Backup for Business".

You can also find admin guides, brochures, technical specifications, user guides, white papers and more for Active Backup for Business in Synology Documentation.