01 / PLAN - VIDEO 00:00

Proxmox Backup Server

Install PBS as a virtual machine, give it somewhere to keep backups, then back up and restore a guest before setting a schedule.

The route

Existing host ZFS mirror > PBS VM > extra virtual data disk > datastore > connect Proxmox VE > manual backup > restore > nightly jobs.

Before you start

- ☐ A working Proxmox VE host or cluster with administrator access and a recovery console.
- ☐ An existing healthy ZFS mirror with spare capacity, as used in the video. This guide does not create the mirror.
- ☐ Room for a PBS VM: the example uses 4 CPU cores, 8 GB RAM and a 32 GB operating-system disk. These are example allocations, not universal sizing rules.
- ☐ A separate data disk for the VM, a spare fixed IP address, gateway, DNS details and an email address you check.
- ☐ A small guest you can back up and enough target storage to restore another copy without overwriting it.

A mirror is only one storage location

Two mirrored disks help with a disk failure. They do not provide independent backup history or an offsite copy. PBS running on a host also depends on that host. Keep another independent copy and a recovery plan.

Use your own names, disk sizes and addresses throughout. The example network address is not a setting to copy. Write down the PBS VM ID, datastore name and the physical host holding its disks.

Watch alongside the Proxmox Backup Server video. Tech without the technobabble. The backup is allowed to be boring; that is rather the point.

02 / PREPARE AND INSTALL - VIDEO 02:01 TO 11:03

Give PBS a home

Keep the operating system and backup data on separate virtual disks so the choices remain clear.

1 Register the existing mirror - 02:01

In Proxmox VE, open **Datacenter > Storage > Add > ZFS**. Give the entry a recognisable ID, select the existing backup pool and restrict it to the node that owns the disks. Allow disk images. The video uses thin provisioning and a 16K block size. Confirm the storage becomes available; do not create or wipe a pool here.

2 Download and upload the ISO - 04:29

Download the PBS installer ISO from Proxmox Downloads. In the intended node's ISO-capable storage, open **ISO Images > Upload** and choose that file. Wait for the upload to finish.

3 Create the virtual machine - 06:12

Choose **Create VM** on the intended node. Use a unique VM ID and a clear name. Attach the PBS ISO, choose Linux, use a 32 GB system disk, 4 cores and 8192 MiB RAM for this example, and disable memory ballooning. Connect the network interface to your intended bridge. Enable start at boot; this walkthrough does not add the VM to HA.

4 Run the installer - 09:18

Start the VM and open its console. Choose the graphical installer. Read the licence and select the small system disk. Set location, time zone and keyboard, then a strong root password and working email. Enter your own hostname, fixed address with subnet prefix, gateway and DNS. Review the summary before installing. [1]

Check the installation target

The installer overwrites the selected disk. At this point the VM should have only its new system disk attached. Do not pass through a disk containing valuable data. After installation, remove the ISO from the virtual drive if it tries to install again.

03 / STORAGE - VIDEO 11:04 TO 17:28

Make space for backups

The host mirror holds a virtual disk. Inside PBS, that virtual disk becomes an ext4 datastore.

5 Add the data disk - 11:04

Shut PBS down cleanly. In its Proxmox VE **Hardware** tab, choose **Add > Hard Disk**, use SCSI and select the storage backed by your existing mirror. The example adds 600 GB from a larger pool, leaving spare space. Choose a size your pool can support and start the VM again. Thin allocation does not create extra physical capacity.

6 Sign in to PBS - 12:45

Open **https://YOUR-PBS-ADDRESS:8007** in a browser. Sign in as root using the Linux PAM realm and the installation password. Check the address, clock and system information. If a certificate needs checking, verify the server identity and fingerprint rather than accepting an unexpected destination. [1]

7 Create the directory and datastore - 15:44

Open **Administration > Storage/Disks**. Identify the extra disk by its size and that it is unused. In **Directory**, choose **Create**, select that data disk, use **ext4**, enter a clear name such as **wd-mirror**, and tick **Add as Datastore**. Confirm creation, then open the new datastore and check its available capacity. [2]

Formatting removes existing data

Creating the directory filesystem partitions and formats the selected disk. The example uses /dev/sdb, but your disk name may differ. Recheck size and identity; never select the 32 GB PBS system disk or an existing data disk.

Three names, three jobs

The **host pool** supplies virtual disks. The **PBS datastore** stores backup chunks and snapshots. The **PVE backup storage ID** is the name you will select when starting a guest backup. They can have different names. Technology does enjoy a naming opportunity.

04 / SUPPLEMENT - BEFORE THE FIRST BACKUP

Connect Proxmox VE to PBS

This supplementary step follows the official documentation. It is needed if PBS is not already a backup target in your Proxmox VE interface.

8 Prepare an account and fingerprint

In PBS, use **Configuration > Access Control** to create a dedicated user in the PBS realm, for example **pve-backup@pbs**, with a strong password. Add a permission for that user on your exact datastore path, for example **/datastore/wd-mirror**, with role **DatastoreBackup**. This permits backup and restore of backups it owns. New users have no permissions until you grant them. [3]

For this simple route use the dedicated username and password; an API token is an alternative, not a required extra step. Keep credentials in your password manager. Copy the certificate fingerprint from the trusted PBS dashboard or obtain it directly on PBS using **proxmox-backup-manager cert info**. [3, 4]

9 Add the target in Proxmox VE

Open **Datacenter > Storage > Add > Proxmox Backup Server**. Enter a unique storage ID such as **pbs-backup**, your PBS address, full username including **@pbs**, its password and the exact datastore name. For a self-signed certificate, enter the verified fingerprint. Make the target available to the nodes that will back up to it, enable it and save. [4, 5]

Prove the connection before continuing

Open the new PBS storage in PVE. It should be available, show capacity and offer backup content. An empty list before the first backup is normal. If it is unavailable, check address/port 8007, credentials, realm, datastore permissions and fingerprint. Do not create a second datastore to fix a spelling error.

Encryption is a separate decision

The video makes an unencrypted backup. If you enable client-side encryption, save the recovery key separately from the protected host and test recovery with it. Losing the key can make the backup unusable. Do not turn encryption off simply to hide an error. [5]

A dedicated account cannot automatically read backups owned by a different account. Use the matching owner or consult the access-control documentation before altering permissions. [3]

05 / FIRST BACKUP AND RESTORE - VIDEO 17:41 TO 24:58

Try a small guest first

A successful backup task is a good start. A restored application doing its job is the useful finish.

10 Make the first backup - 17:41

In Proxmox VE, select your small guest, open **Backup > Backup now** and choose the PBS storage target. The example uses Pi-hole. Run the backup and wait for completion. Read the task log, then check the snapshot under the PBS datastore content, including the guest ID and date. Check which guest disks or external data are excluded from backup before relying on it.

11 Restore without overwriting - 23:05

In PVE, open the PBS storage and its backup list. Select the correct guest snapshot and click **Restore**. Choose an unused VM ID across the cluster, suitable destination disk storage and enough free space. Leave **Start after restore** unticked. Review the settings and run the restore; wait for a successful task result.

A new VM ID does not mean a new IP address

The restored guest can retain the original hostname, IP and service identity. Starting both copies on the normal network can cause conflicts. Disconnect every virtual network adapter before starting a test copy, or place it on a deliberately isolated test network. Check passthrough devices too.

12 Finish the recovery test - 24:18

The video stops after the restore task completes. For your own test, review the restored hardware and boot settings, start the isolated copy and inspect its console. Check the expected files and application. If testing network services, use an isolated client and test network. Do not let a test Pi-hole or DHCP service reach your live network.

- ☐ Backup snapshot has the intended guest ID and date.
- ☐ Restore task completes to a separate unused VM ID.
- ☐ Restored guest boots and the application/service check passes.
- ☐ Record the result and stop the test copy before changing its network.

Keep the original guest and backup. Do not delete either as part of this test. A tick beside a task is not a full recovery rehearsal, however reassuring the tick looks.

06 / AUTOMATE - VIDEO 25:28 TO 29:20

Give backups a schedule

Check one manual backup and restore before asking the scheduler to look after the rest.

13 Schedule the guest backups - 25:28

In PVE, open **Datacenter > Backup > Add**. Select the PBS storage target and the required nodes and guests. The example uses a daily overnight job, snapshot mode and the selected guests, excluding the PBS VM. Name the job clearly, enable it, review its retention and notification choices and save. Confirm the displayed next run time rather than copying an ambiguous spoken time.

Keep PBS out of its own datastore job

Exclude the PBS VM from the job writing into its own datastore. Plan protection of the PBS configuration and recovery information separately, on independent storage. Also check how newly created guests will be included: a fixed selection may need updating.

14 Choose retention deliberately - 27:59

In PBS, open the datastore **Prune & GC** area and add a prune job. The video keeps the last two snapshots and runs pruning every two hours. Treat two as a demonstration value: choose history that covers the mistakes you may discover later. Inspect the affected groups and any existing PVE retention settings before enabling deletion. Pruning also applies to eligible manual backups. [6]

Pruning removes restore points

Review retention before the first prune run. An extra manual backup can become one of the newest two, so keep-last 2 is not necessarily two separate days. Protected snapshots can be useful for changes you may need to undo. Do not assume another retention setting will save a snapshot already removed.

15 Set garbage collection - 29:02

Set a GC schedule on the datastore. The video uses Saturday at 02:00. Pruning removes snapshot references; GC later reclaims chunks no retained snapshot needs. Pending removals can remain through a grace period, so space need not return immediately. Avoid overlapping heavy jobs where practical. [6]

PVE chooses when to create backups. PBS pruning chooses which restore points remain. Garbage collection reclaims unused space. Three jobs, three different chores. None of them makes the tea.

07 / KEEP AND CHECK - VIDEO 29:37

Check tomorrow. Then repeat.

A schedule is an intention. Look for the new backup and read the result.

Your completion checklist

- ☐ PBS starts after a host restart; the data disk and datastore remain available.
- ☐ The overnight job produced fresh snapshots for every intended guest.
- ☐ A restore to a separate ID has passed a boot and service test.
- ☐ Retention is intentional; prune and GC tasks complete successfully.
- ☐ Supplement: configure PBS Verify Jobs and review their results. Verification checks stored data, not whether the application boots. [6]
- ☐ Keep an independent copy away from this host and plan an offsite copy. Record how to recover if the PBS host fails.

If something does not match

No PBS page: check the VM is running, its address, network bridge and port 8007.
Storage unavailable: revisit the account realm, permissions, datastore name and fingerprint.
No new backup: inspect the PVE task log, job enabled state, guest selection and next run.
Restore fails: check the selected snapshot, target capacity, VM ID and encryption key if used.
Disk remains full: check both pruning and GC, then pending removals; do not delete chunk files by hand.

Video and official references

Watch the source video | Matching video article
[1] PBS installer and first login
[2] PBS disks and datastores
[3] Users, permissions and tokens
[4] Proxmox VE integration
[5] PBS storage configuration and encryption
[6] Pruning, garbage collection and verification

PBS address / datastore / backup storage ID

Last restore test date and result / independent copy location (no passwords)

As an Amazon Associate I earn from qualifying purchases.