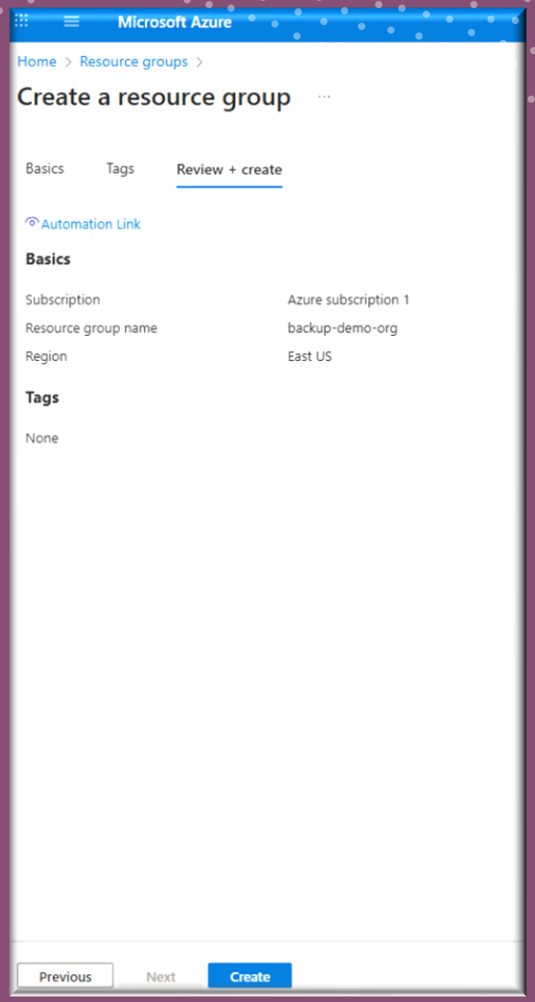
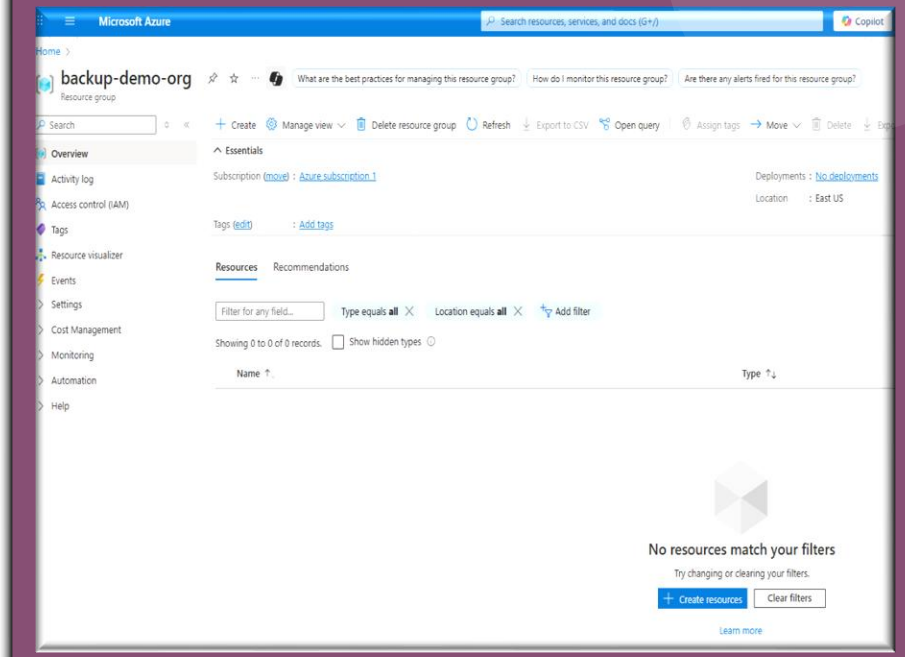
# Step 1 – Create Resource Group

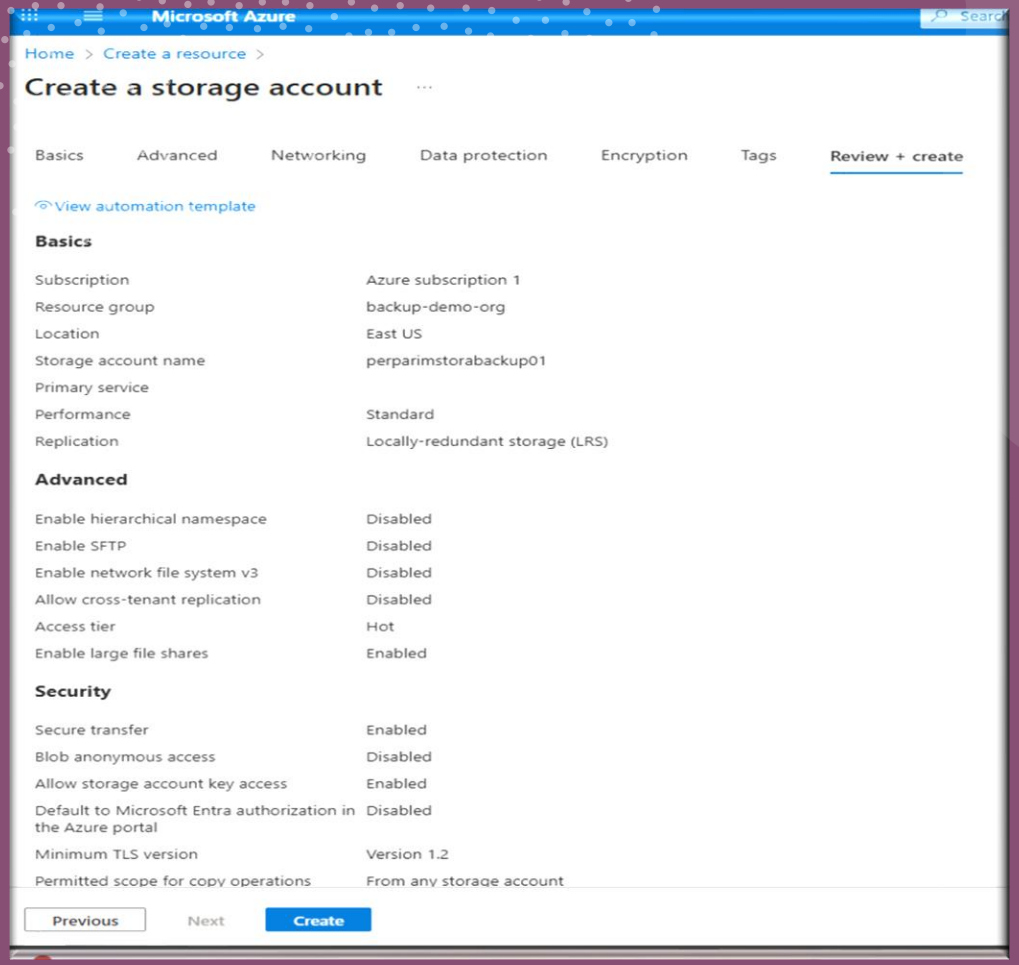
- We begin by creating a dedicated **Resource Group** to organize all lab resources in one place. This ensures simplified management, clear separation from other workloads, and makes cleanup effortless after completing the backup and recovery demonstration

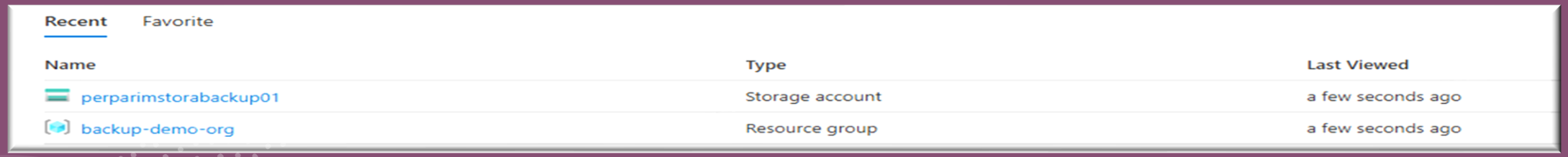


# Step 2 – Create a Storage Account

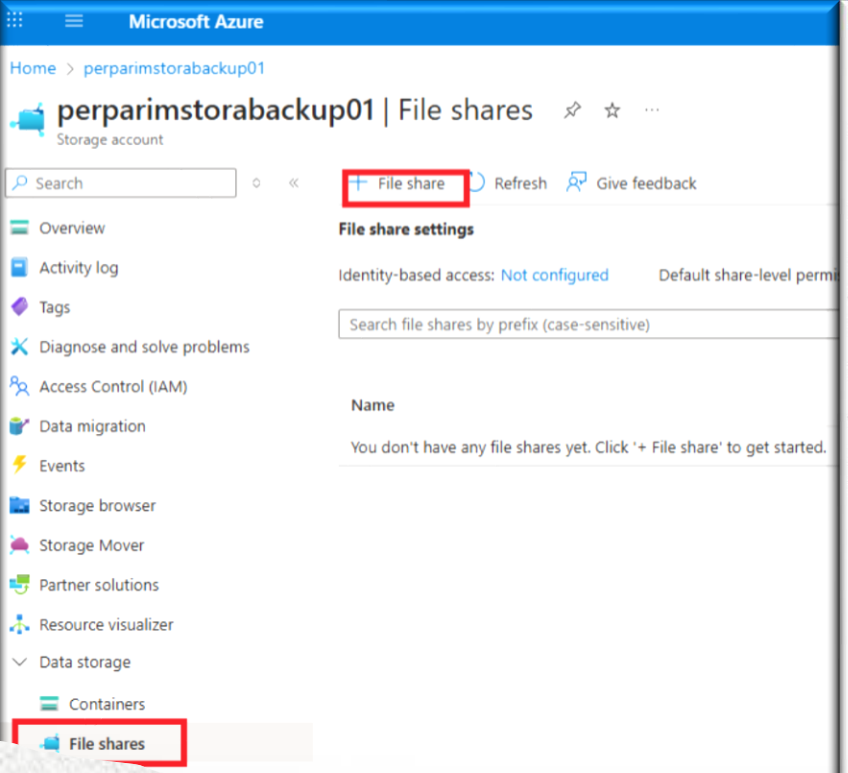
- We create a dedicated Storage Account inside our Resource Group to host the Azure File Share. This provides the foundation for storing and managing our backup data..

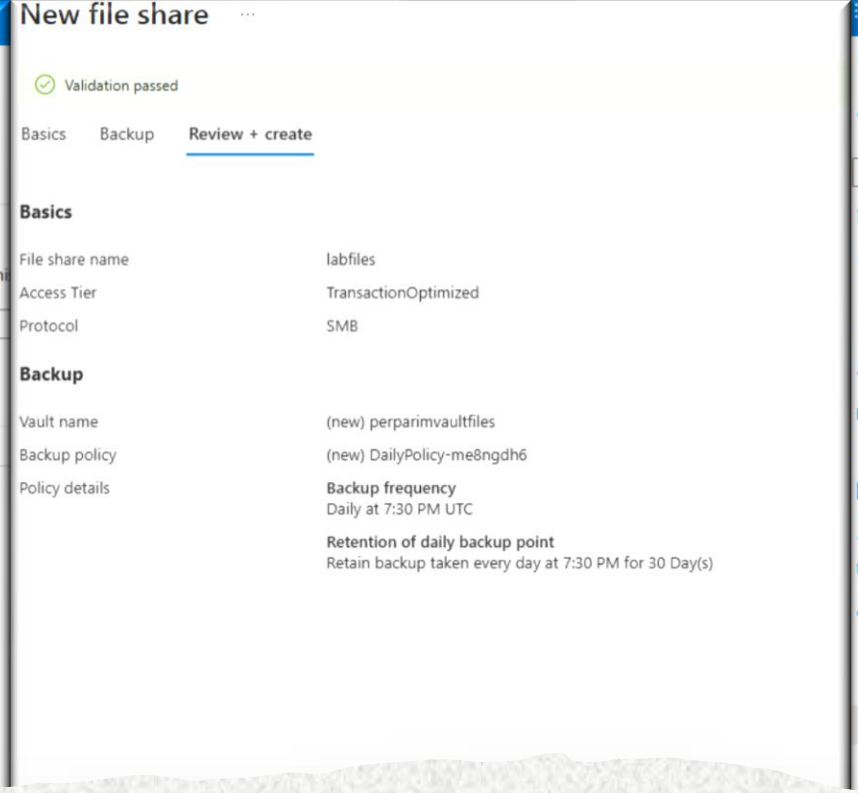


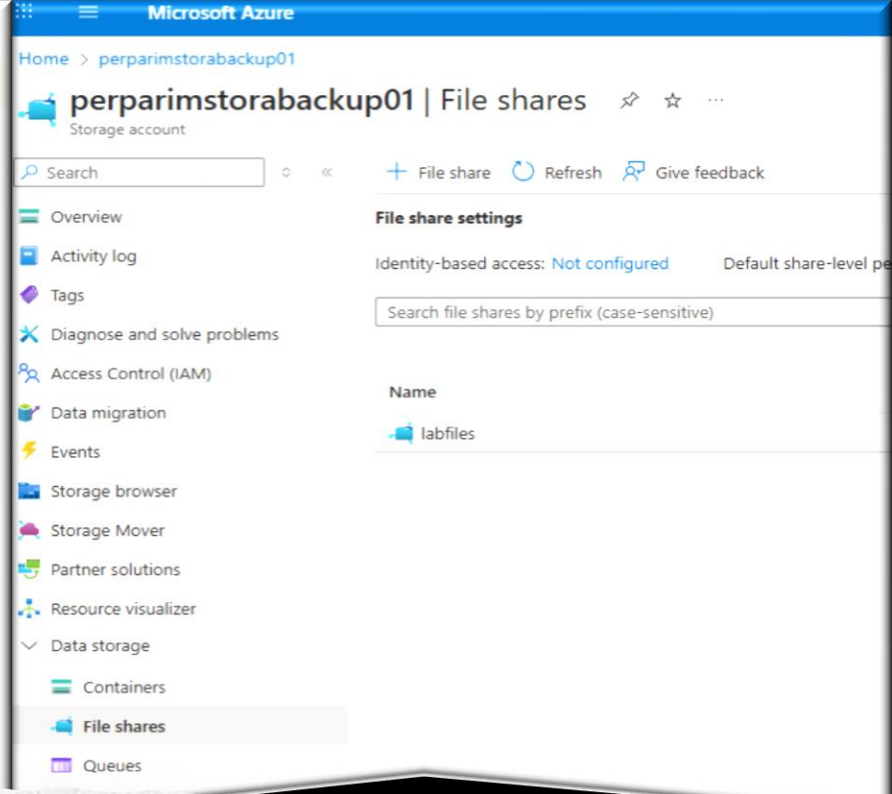




💡 Pro Tip: Use a clear naming convention for storage accounts to make them easy to identify across environments.

PerparimLabs




# Step 3 – Create Azure File Share

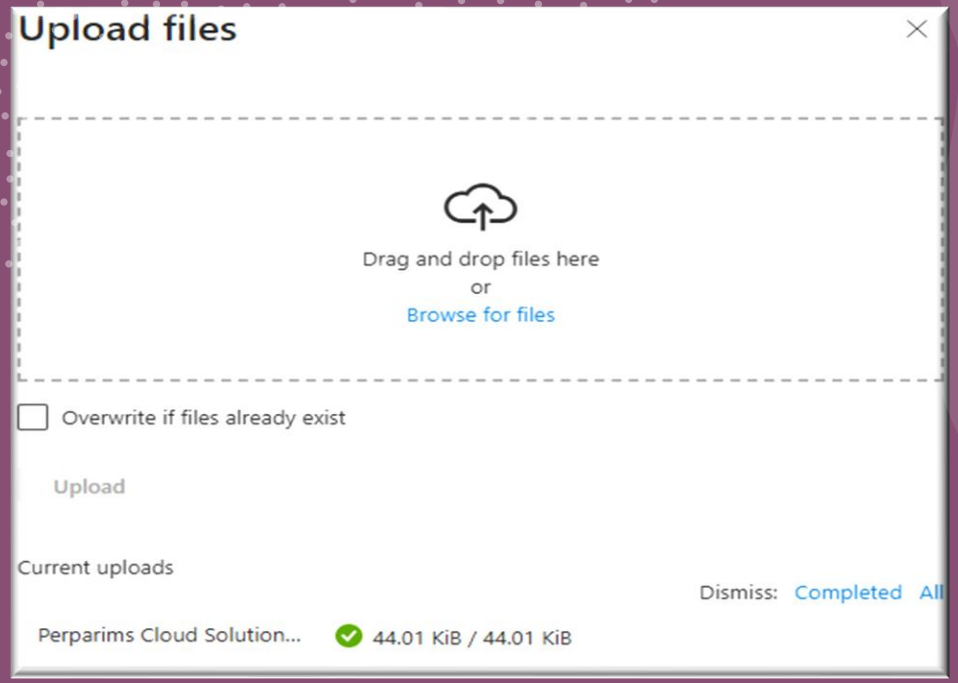
- Inside the Storage Account, we create an Azure File Share that will hold the lab files for our backup demo.

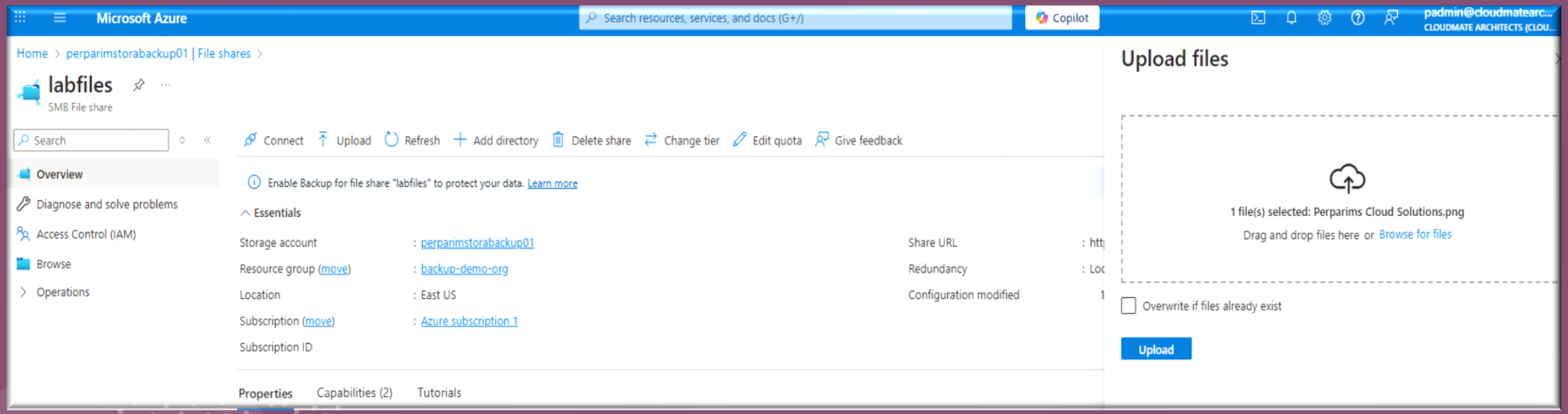
PerparimLabs

💡 Pro Tip: Choose the correct access tier and enable backup right away to simplify protection of your files.

# Step 4 – Upload Files to Azure File Share

- We upload our test file to the newly created Azure File Share. This file will be used later to validate the backup and restore process.




💡 Pro Tip: Use small, clearly named files for lab work. This speeds up uploads and makes it easier to confirm the correct file during restoration.

# Step 5 – Create a Virtual Machine for Backup Testing

- We deploy a Windows Server 2022 Datacenter VM that will be used to connect to our Azure File Share and perform backup/restore operations.

Microsoft Azure

Home > Create a resource >

## Create a virtual machine

Help me create a low cost VM | Help me choose the right VM size for m

Subscription * : Azure subscription 1

Resource group * : backup-demo-org

Create new

**Instance details**

Virtual machine name * : perparim-vm-backup

Region * : (US) East US

Deploy to an Azure Extended Zone

Availability options : No infrastructure redundancy required

Security type : Trusted launch virtual machines

Configure security features

Image * : Windows Server 2022 Datacenter: Azure Edition Hotpatch - x64 Gen2

See all images | Configure VM generation

VM architecture : Arm64 / x64

Arm64 is not supported with the selected image.

Run with Azure Spot discount

Size * : Standard_D2s_v3 - 2 vcpus, 8 GiB memory ($137.24/month)

See all sizes

Enable Hibernation

Hibernate is not supported by the size that you have selected. Choose a size that is compatible with Hibernate to enable this feature. Learn more

**Administrator account**

Username * : 1padmin

< Previous | Next : Disks > | Review + create

Microsoft Azure

Home > Create a resource >

## Create a virtual machine

Help me create a low cost VM | Help me choose t

Validation passed

| | |
|---|---|
| Subscription | Azure subscription 1 |
| Resource group | backup-demo-org |
| Virtual machine name | perparim-vm-backup |
| Region | East US |
| Availability options | No infrastructure redundancy required |
| Zone options | Self-selected zone |
| Security type | Trusted launch virtual machines |
| Enable secure boot | Yes |
| Enable vTPM | Yes |
| Integrity monitoring | No |
| Image | Windows Server 2022 Datacenter: Azure Edition Hotpatch - Gen2 |
| VM architecture | x64 |
| Size | Standard D2s v3 (2 vcpus, 8 GiB memory) |
| Enable Hibernation | No |
| Username | 1padmin |
| Public inbound ports | RDP |
| Already have a Windows license? | No |
| Azure Spot | No |

**Disks**

| | |
|---|---|
| OS disk size | Image default |
| OS disk type | Standard HDD LRS |
| Use managed disks | Yes |
| Delete OS disk with VM | Enabled |
| Ephemeral OS disk | No |

**Networking**

< Previous | Next > | Create

Microsoft Azure

Home > Create a resource >

## Create a virtual machine

Help me create a low cost VM | Help me choose the righ

Validation passed

| | |
|---|---|
| Virtual network | (new) perparim-vm-backup-vnet |
| Subnet | (new) default (10.0.0.0/24) |
| Public IP | (new) perparim-vm-backup-ip |
| Accelerated networking | Off |
| Place this virtual machine behind an existing load balancing solution? | No |
| Delete public IP and NIC when VM is deleted | Disabled |

**Management**

| | |
|---|---|
| Microsoft Defender for Cloud | Basic (free) |
| System assigned managed identity | Off |
| Login with Microsoft Entra ID | Off |
| Auto-shutdown | On |
| Backup | Disabled |
| Site Recovery | Disabled |
| Enable periodic assessment | Off |
| Enable hotpatch | On |
| Patch orchestration options | Azure-orchestrated patching (preview): patches will be installed by Azure |
| Reboot setting | Reboot if required |

**Monitoring**

| | |
|---|---|
| Alerts | Off |
| Boot diagnostics | Off |
| Enable OS guest diagnostics | Off |
| Enable application health monitoring | Off |

PerparimLabs

< Previous | Next > | Create

💡 Pro Tip: Use a small VM size for lab scenarios to save costs. Make sure RDP is enabled and note the admin credentials for later access.

# Step 6 – Enable Azure Backup for the VM

- We configure Azure Backup directly from the VM's **Backup** blade, creating a new Recovery Services Vault and applying an enhanced policy for higher retention and instant restore.

Microsoft Azure

Home > backup-demo-org > perparim-vm-backup

**perparim-vm-backup | Backup**
Virtual machine

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Connect
- Networking
- Settings
- Availability + scale
- Security
- Backup + disaster recovery
  - Backup
  - Disaster recovery
  - Restore point
- Operations
- Monitoring
- Automation
- Help

**Welcome to Azure Backup for Azure VMs**
Simple and reliable VM backup to the Azure. Learn more. You are charged an instance fee ba

Review the following information and click on 'Enable backup' to start protecting your VM.

Recovery Services vault: Create new / Select existing

Backup vault *: perparimvaultvm

Resource group: backup-demo-org
Create new

Policy sub type *: Enhanced
- Multiple backups per day
- Up to 30 days operational tier retention
- Support for Trusted Launch Azure VM
- Support for VMs with Ultra Disks and Premium SSD v2

Standard
- Once-a-day backup
- Up to 5 days operational tier retention

Choose backup policy *: (new) EnhancedPolicy-me8ohgpr
Edit this policy

Protecting a VM with enhanced policy can incur additional snapshot charges. Please note that once you enable a VM backup with enhanced policy, changing to standard policy type is not possible. Learn more.

**Policy Details**

Full backup

**Backup frequency**
Every 4 hour(s) starting 8:00 AM UTC for 12 Hour(s)

**Instant restore**
Retain instant recovery snapshot(s) for 7 day(s)

**Retention of daily backup point**

Enable backup | Cancel

Microsoft Azure | Search resources, services, and docs (G+/) | Copilot

Home > perparim-vm-backup

**perparim-vm-backup | Backup**
Virtual machine

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Connect
- Networking
- Settings
- Availability + scale
- Security
- Backup + disaster recovery
  - Backup
  - Disaster recovery
  - Restore point
- Operations
- Monitoring
- Automation
- Help

Backup now | Restore VM | File Recovery | Stop backup | Resume backup | Delete backup data | Restore to Secondary Region | Undelete | Feedback

Try our new Business Continuity Center for the at scale BCDR management of your resources protected across Azure Backup and Site Recovery. →

**Essentials**

| | | | |
|---|---|---|---|
| Recovery services vault | : perparimvaultvm | Backup Pre-Check | : Passed |
| Subscription (move) | : Azure subscription 1 | Last backup status | : Warning (Initial backup pending) |
| Subscription ID | | Backup policy | : EnhancedPolicy-me8ohgpr (Enhanced) |
| Alerts (in last 24 hours) | : View alerts | Oldest restore point | : - |
| Jobs (in last 24 hours) | : View jobs | Included disk(s) | : All disks |

**Recovery points**

This list is filtered for last 30 days of recovery points. To recover from recovery point older than 30 days, as well as vault-archive, click here.

Long term recovery points can be moved to vault-archive. To move all 'recommended recovery points' to vault-archive tier, click here.

| CRASH CONSISTENT | APPLICATION CONSISTENT | FILE-SYSTEM CONSISTENT |
|---|---|---|
| 0 | 0 | 0 |

| Creation time ↑↓ | Consistency | Recovery type |
|---|---|---|
| No restore points available. | | |

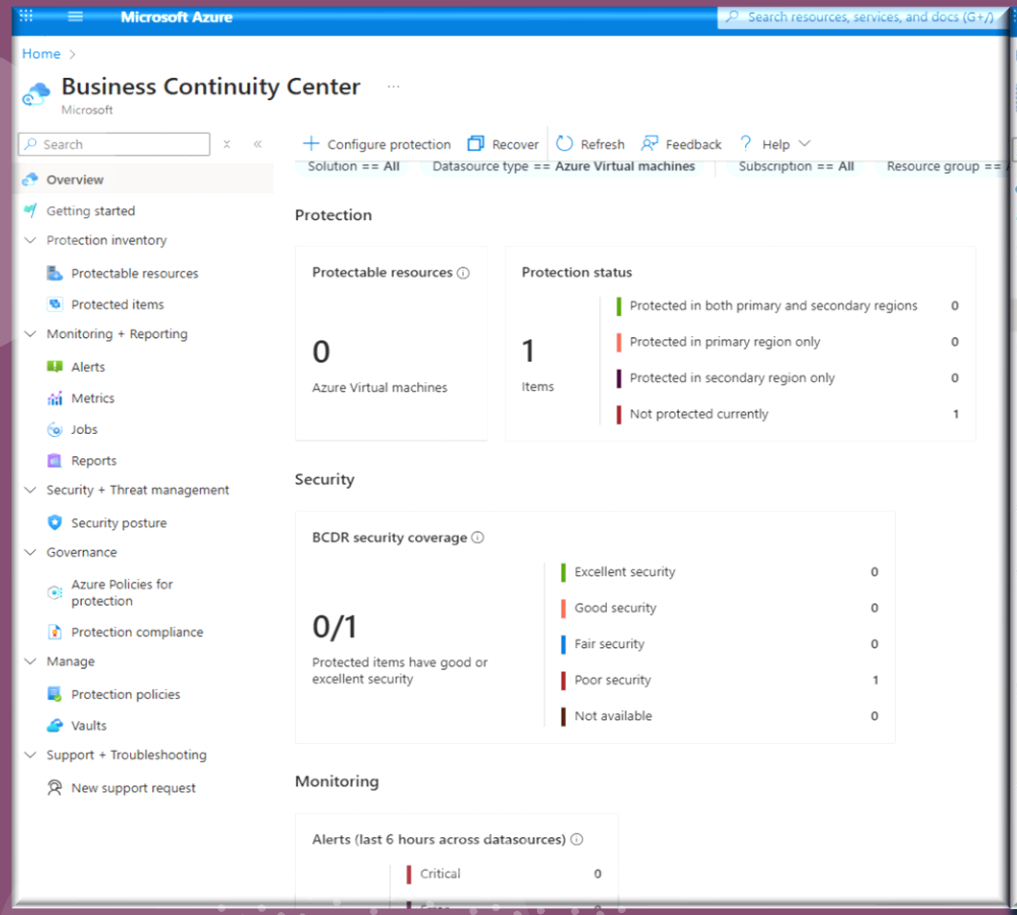
💡 Pro Tip: Enhanced policies provide up to 30 days operational restore and 7 days snapshot retention—ideal for lab testing and production-critical workloads.

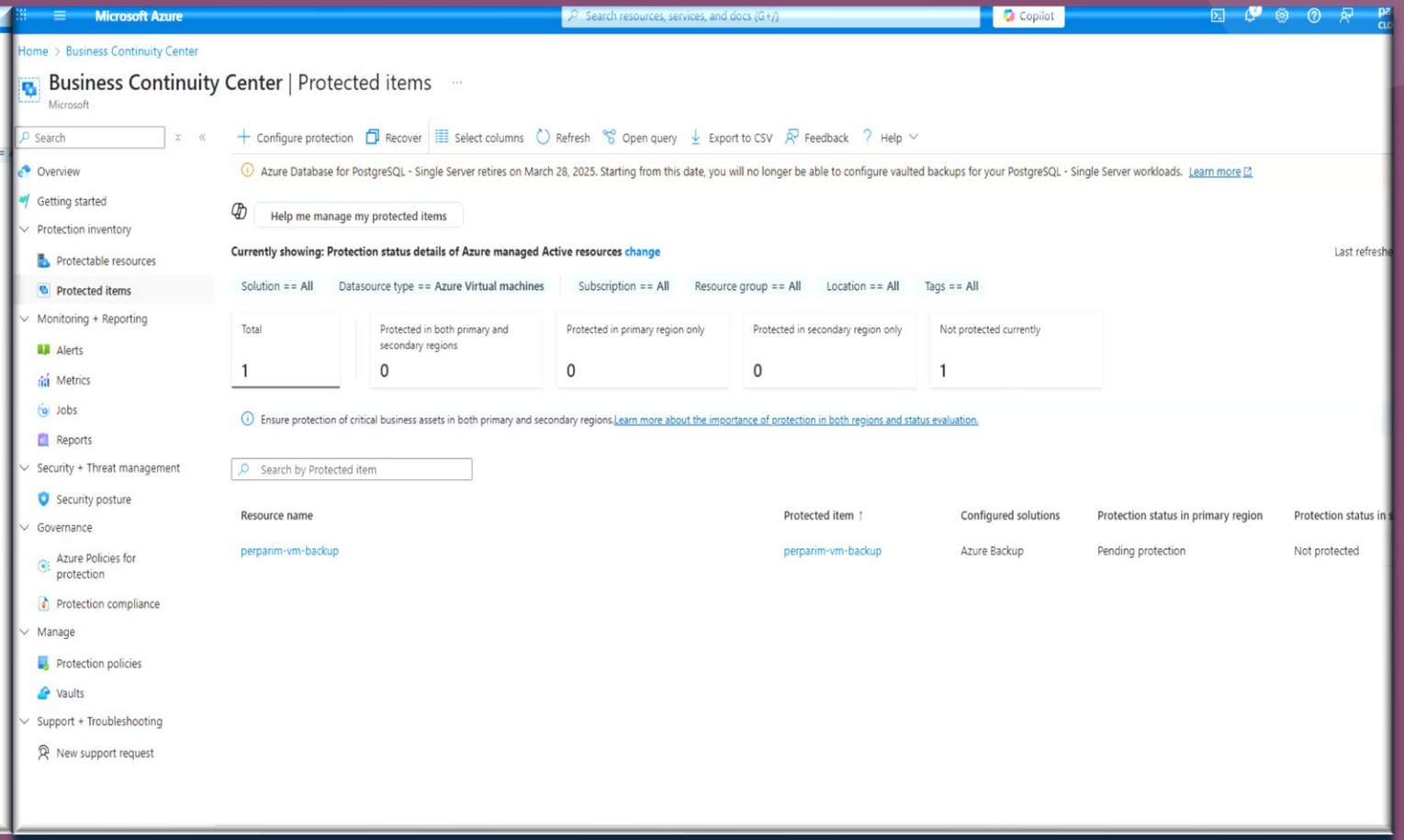
PerparimLabs

# Step 7: Review Backup Protection Status

**Action:**
In the **Business Continuity Center**, open **Protection Overview** and **Protected Items** to see which resources are protected and their regional coverage.

**Context:**
This view confirms your backup configuration, showing which workloads are fully protected, region coverage (primary/secondary), and any unprotected assets.



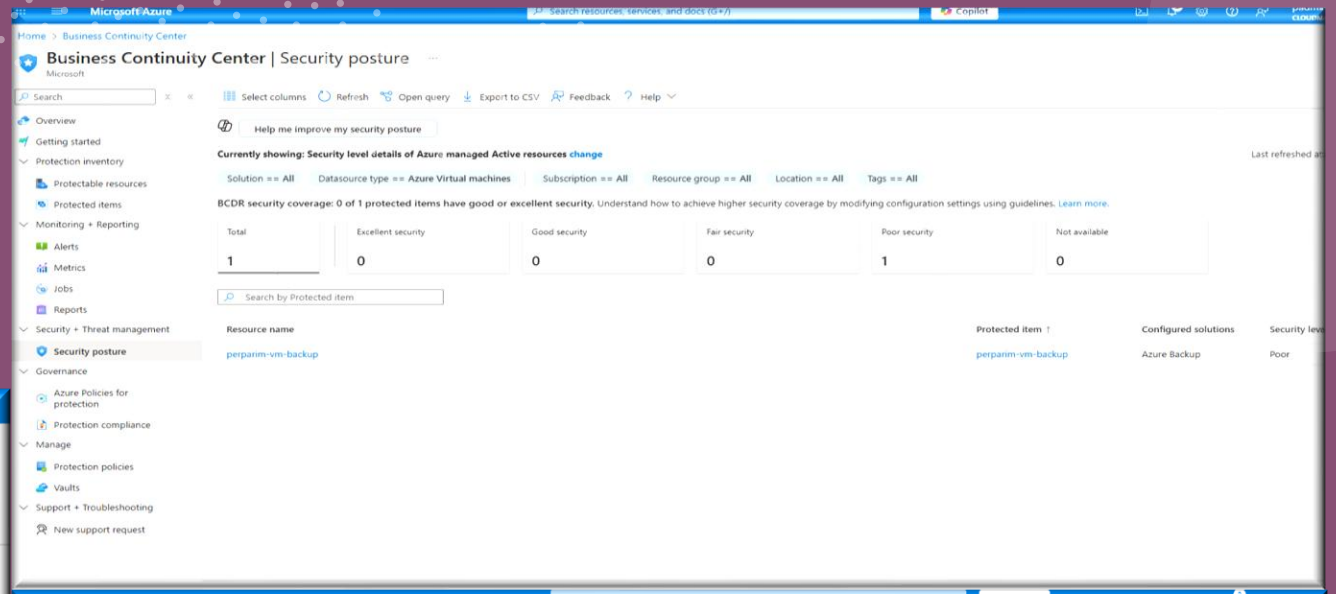

Pro Tip: Check this dashboard after each backup policy change to quickly verify that new workloads are included in protection.

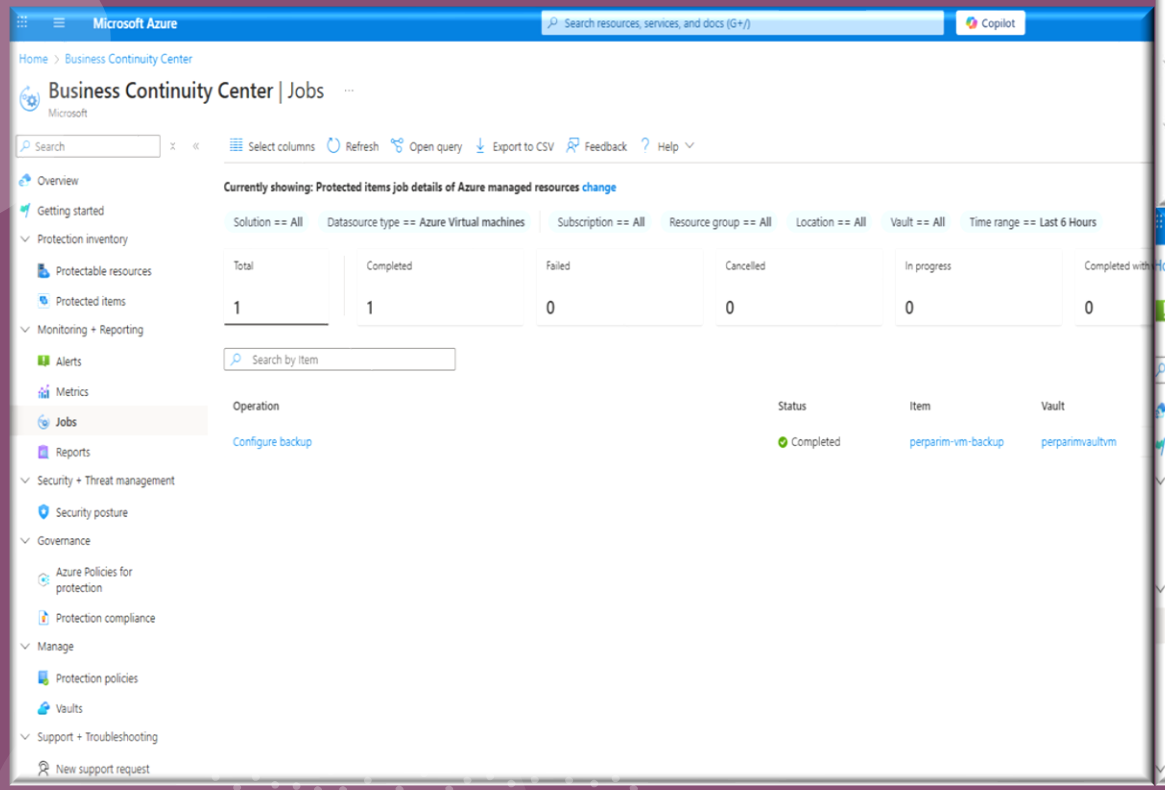
PerparimLabs

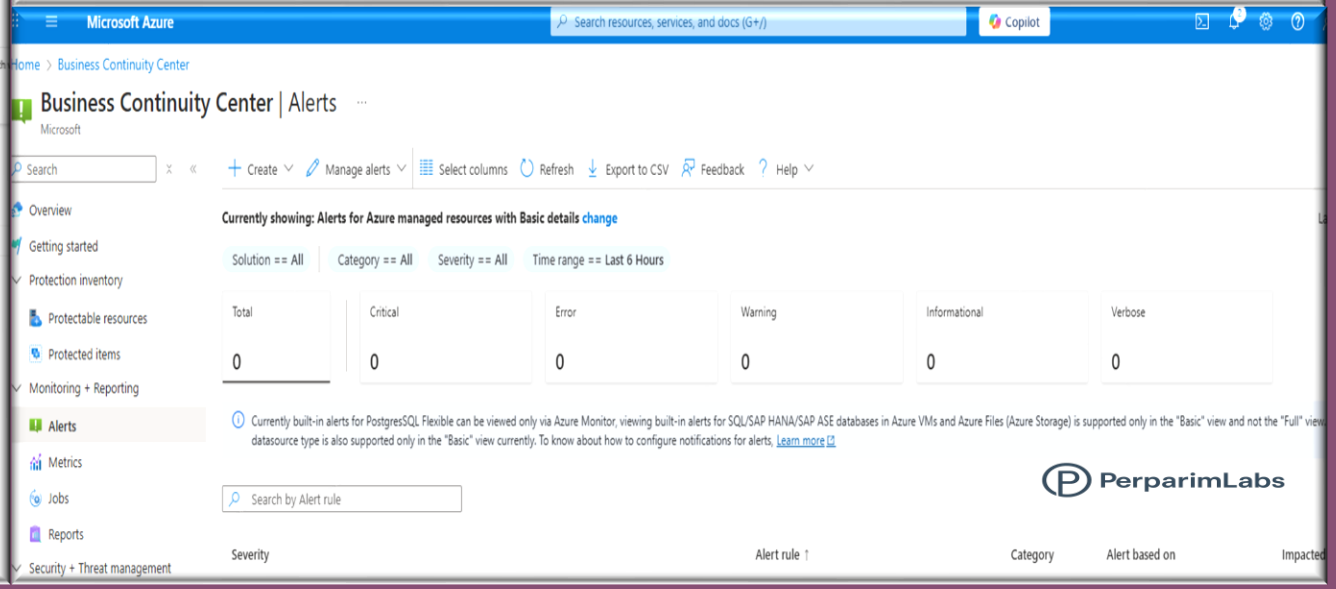
# Step 8: Monitor Backup Security & Jobs

**Action:**
Navigate to **Security Posture**, **Alerts**, and **Jobs** in the Business Continuity Center to validate protection health and recent job statuses.

**Context:**
Security Posture highlights the protection strength of your workloads, Alerts notify you of potential risks, and Jobs confirm whether backup operations completed successfully.



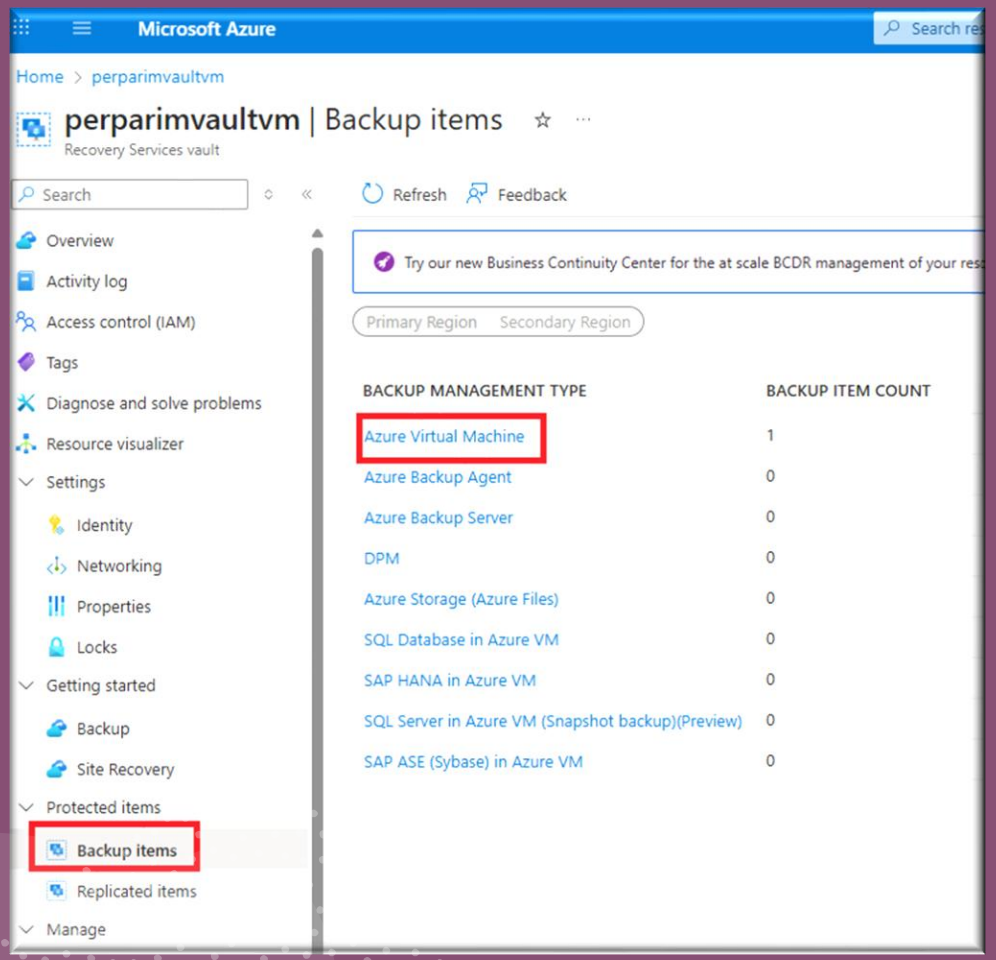



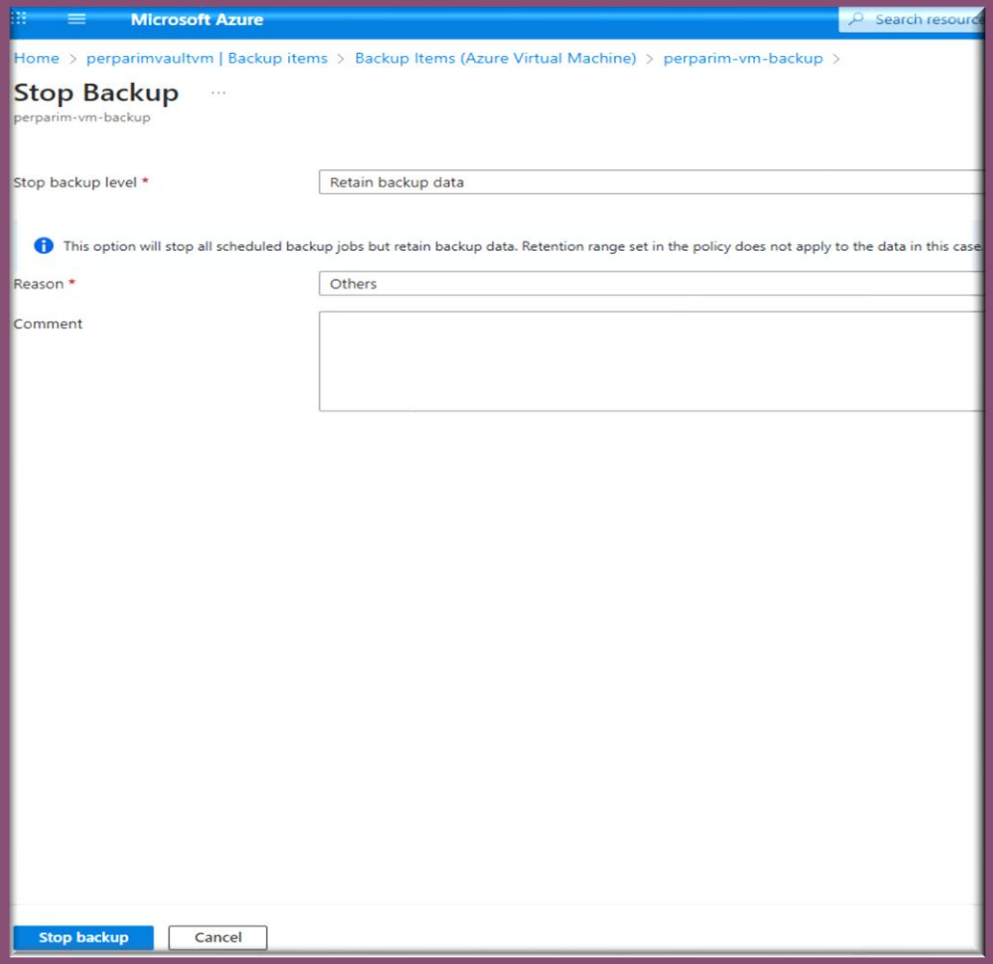

PerparimLabs

Pro Tip: Enable alert notifications for failed or skipped jobs to proactively respond before recovery points are missed.

# Step 9: Stop the Backup (Retain Data)

- From the Recovery Services vault, go to **Backup items** → select the VM backup → click **Stop backup**. Choose the option to **retain backup data** so you can delete it later if needed.

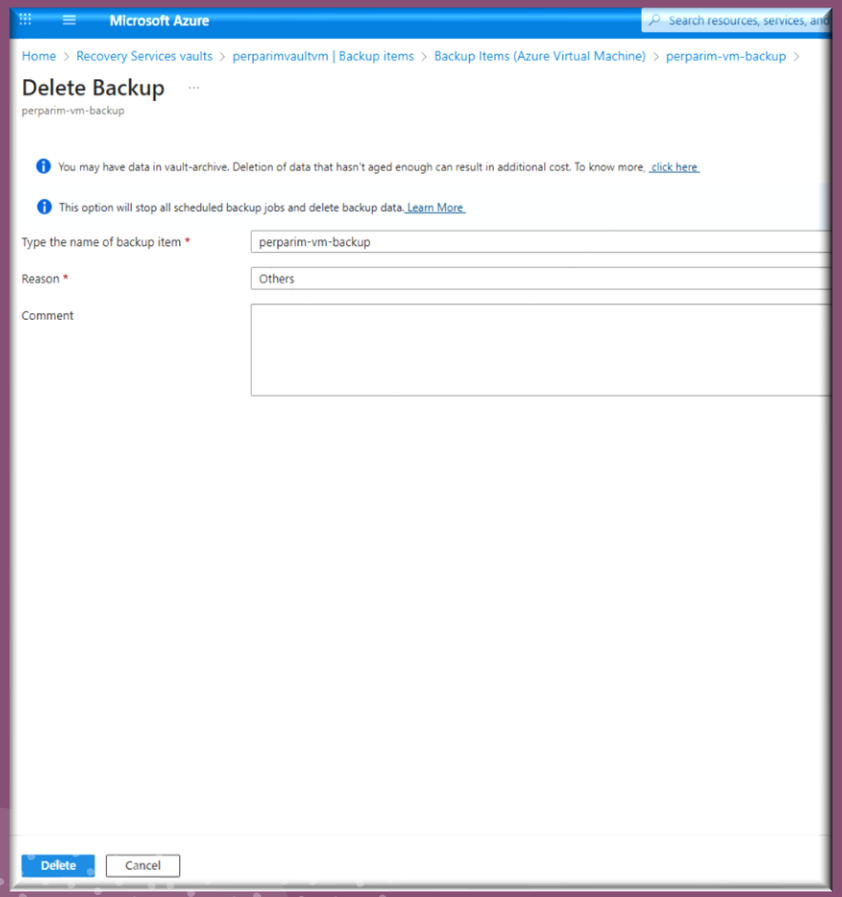


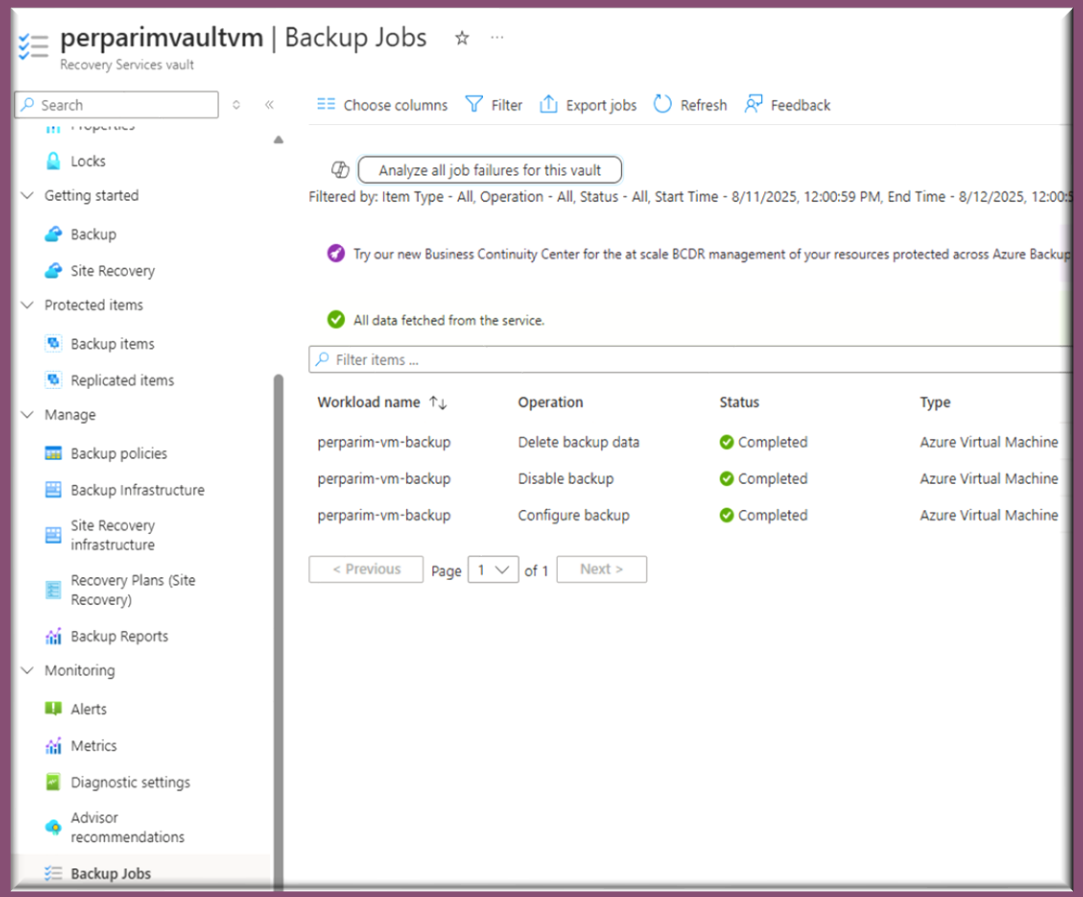




PerparimLabs

# Step 10: Delete the Backup

- Once the backup is stopped, click **Delete backup**. This permanently removes the backup data from the vault



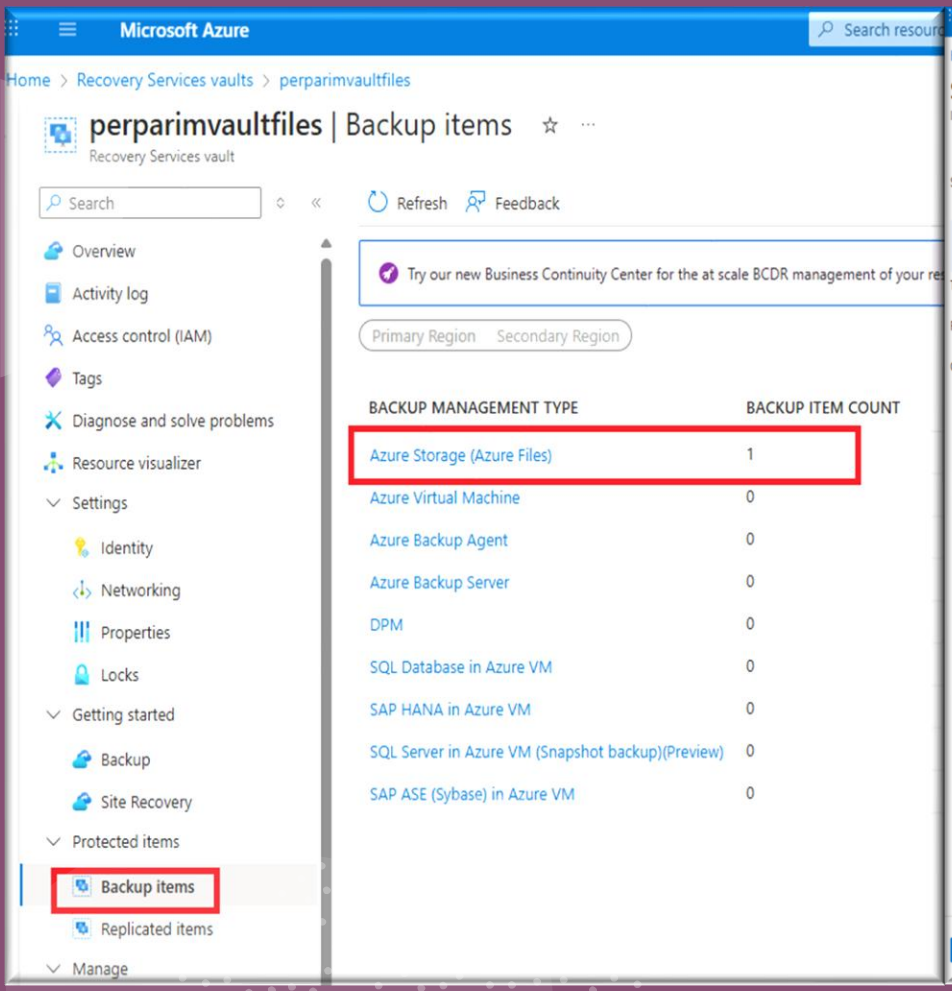

PerparimLabs

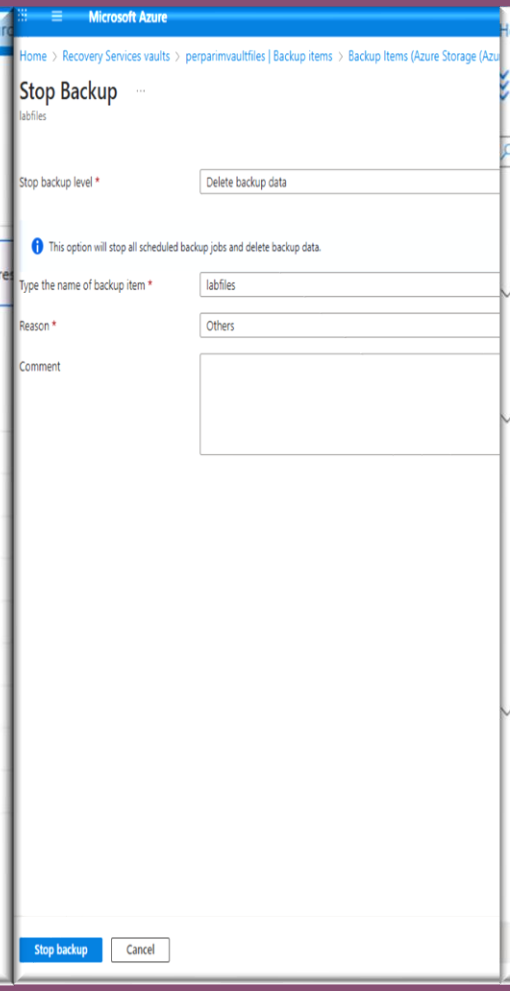
# Stop Backup & Job Status

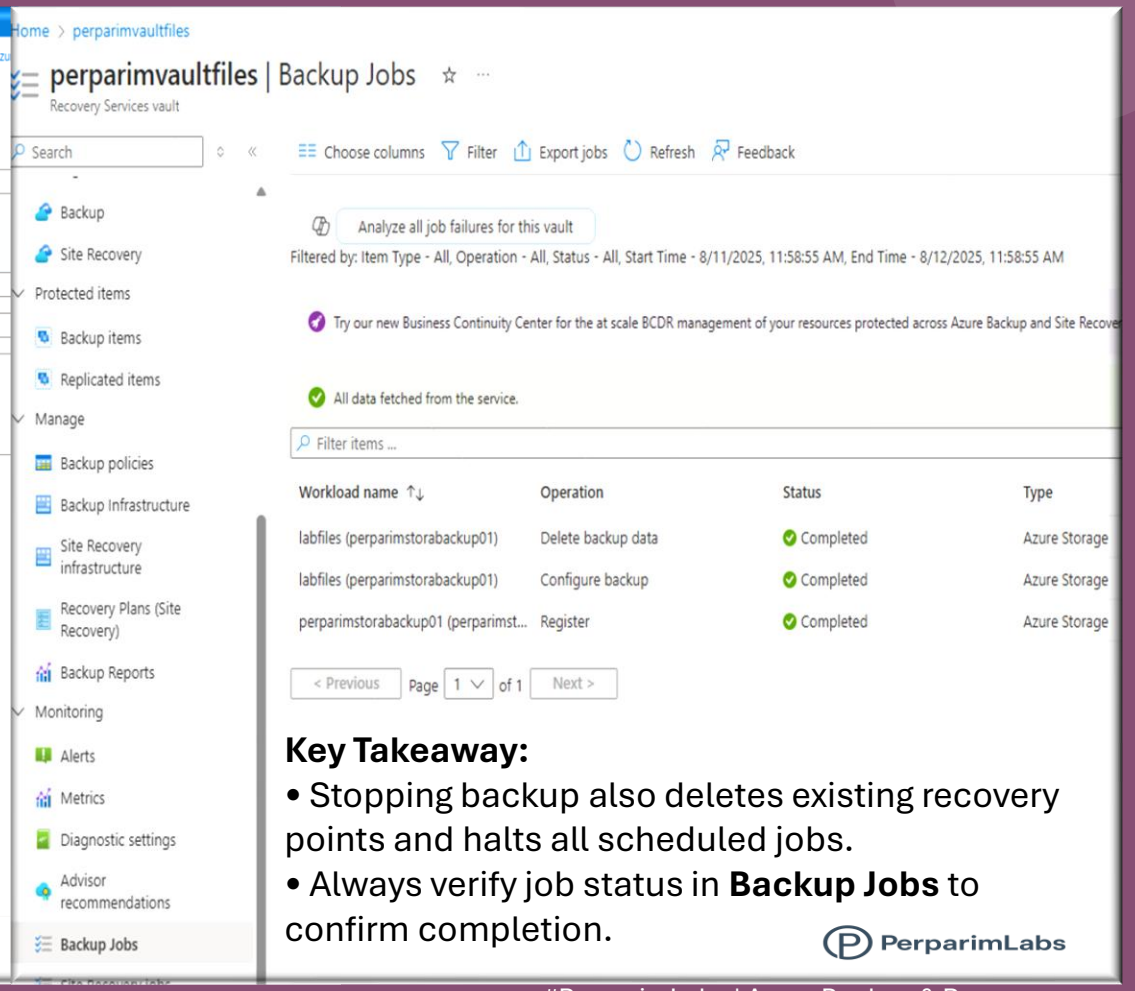
- Highlight the **Backup Items** pane in the Recovery Services vault.
- Select **Azure Storage (Azure Files)** → target your backup item (labfiles).
- Click **Stop Backup** → choose **Delete backup data** option.
- Reason: *Others* (with optional comment).

- Navigate to **Backup Jobs** to confirm status.
- Shows the sequence:

1. Delete backup data → **Completed**
2. Configure backup → **Completed**
3. Register → **Completed**



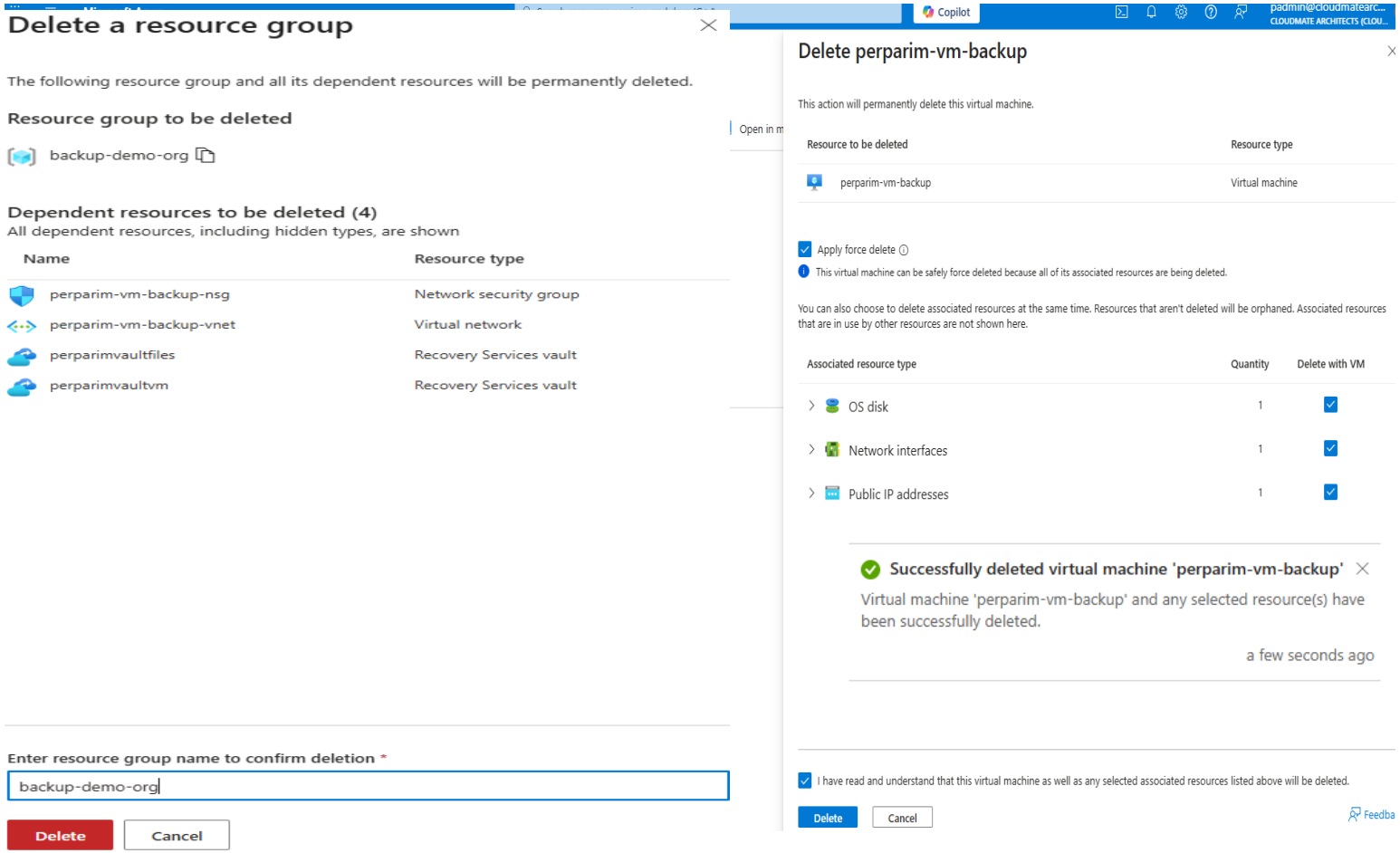

**Key Takeaway:**

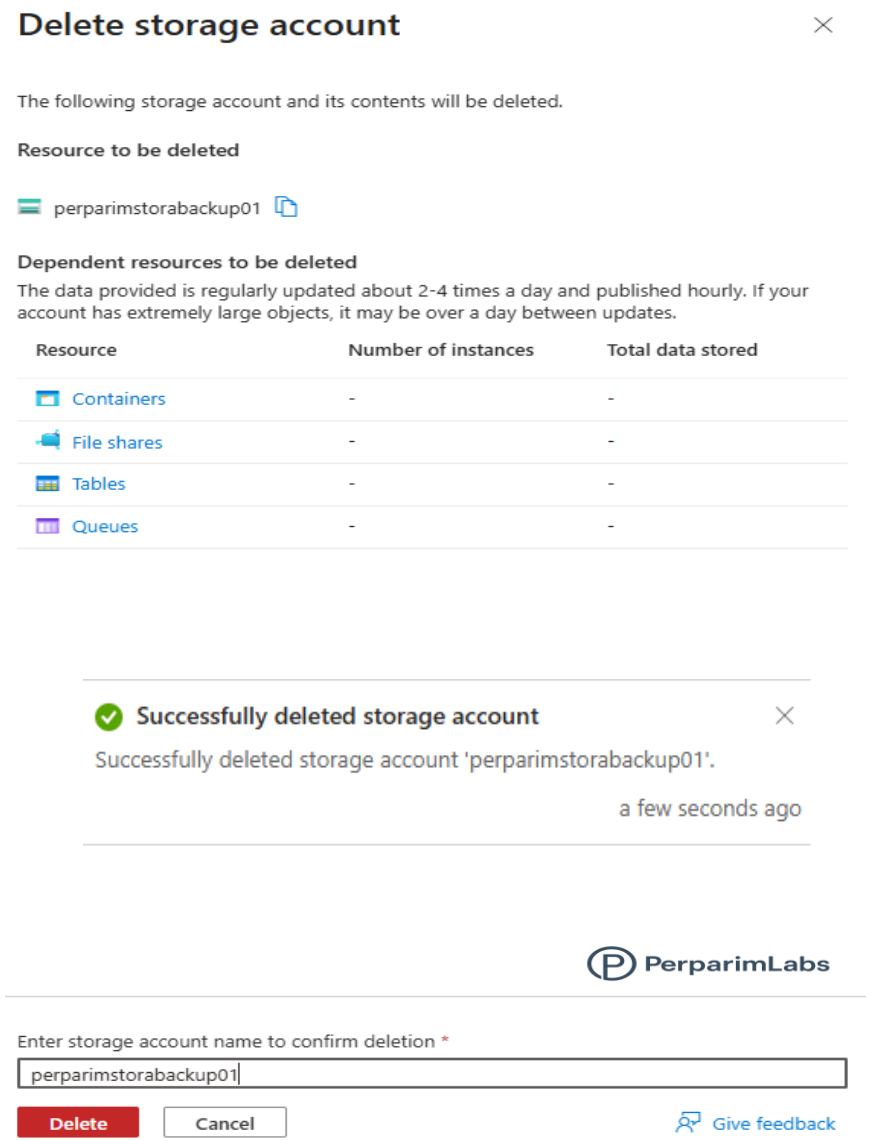
- Stopping backup also deletes existing recovery points and halts all scheduled jobs.
- Always verify job status in **Backup Jobs** to confirm completion.

PerparimLabs

# Final Cleanup – Deleting Remaining Resources

- **Delete Storage Account** – Removed perparimstorabackup01 with confirmation and received success notification.
- **Delete VM Resource** – Deleted perparim-vm-backup along with OS disk, NICs, and Public IPs.
- **Delete Resource Group** – Removed backup-demo-org including all dependent resources (NSG, VNet, Recovery Services Vaults).



# 🚀 Ready to Explore Azure Backup & Recovery?

- I hope this lab walk-through helped you understand the full lifecycle — from setup to cleanup — of Azure Backup for Azure File Shares.
  💬 What's your experience with Azure Backup? Have you tried restoring from a Recovery Services Vault?
- Let's share knowledge! Comment below or connect with me to discuss more real-world Azure scenarios.

PerparimLabs

#PerparimLabs #AzureBackup #MicrosoftAzure #CloudSkills