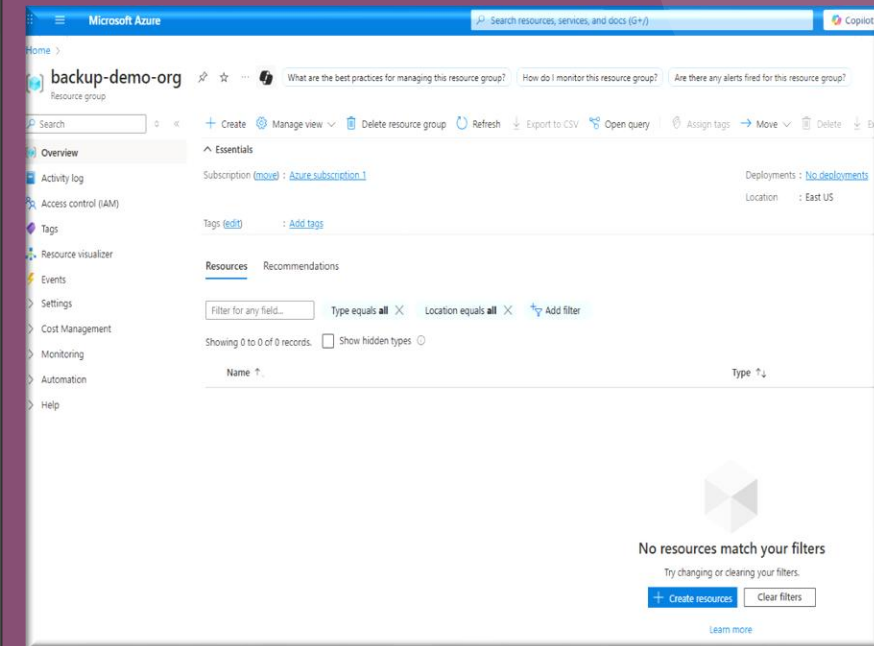
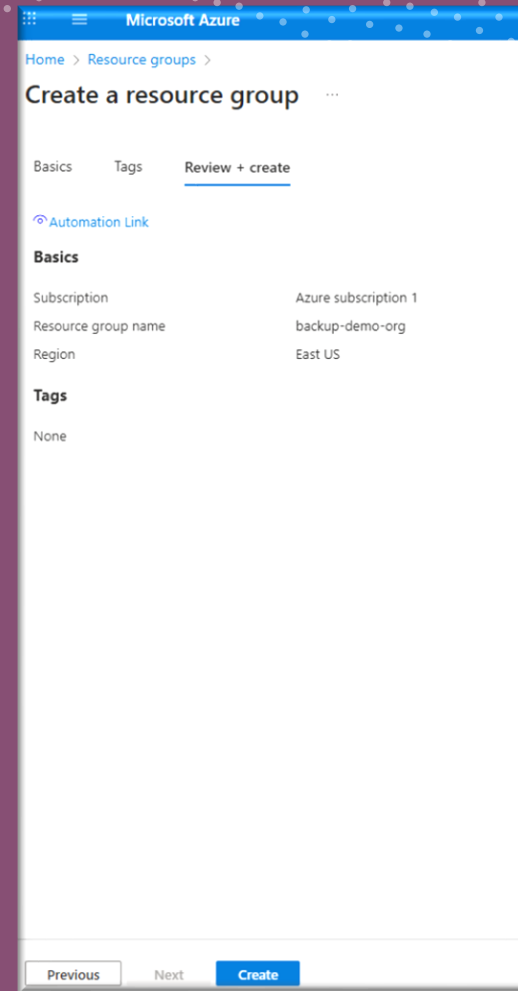




Step 1 – Create Resource Group

- 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..

Microsoft Azure

Home > Create a resource >

Create a storage account

Basics Advanced Networking Data protection Encryption Tags Review + create

[View automation template](#)

Basics

Subscription	Azure subscription 1
Resource group	backup-demo-org
Location	East US
Storage account name	perparimstorabackup01
Primary service	
Performance	Standard
Replication	Locally-redundant storage (LRS)



Advanced

Enable hierarchical namespace	Disabled
Enable SFTP	Disabled
Enable network file system v3	Disabled
Allow cross-tenant replication	Disabled
Access tier	Hot
Enable large file shares	Enabled

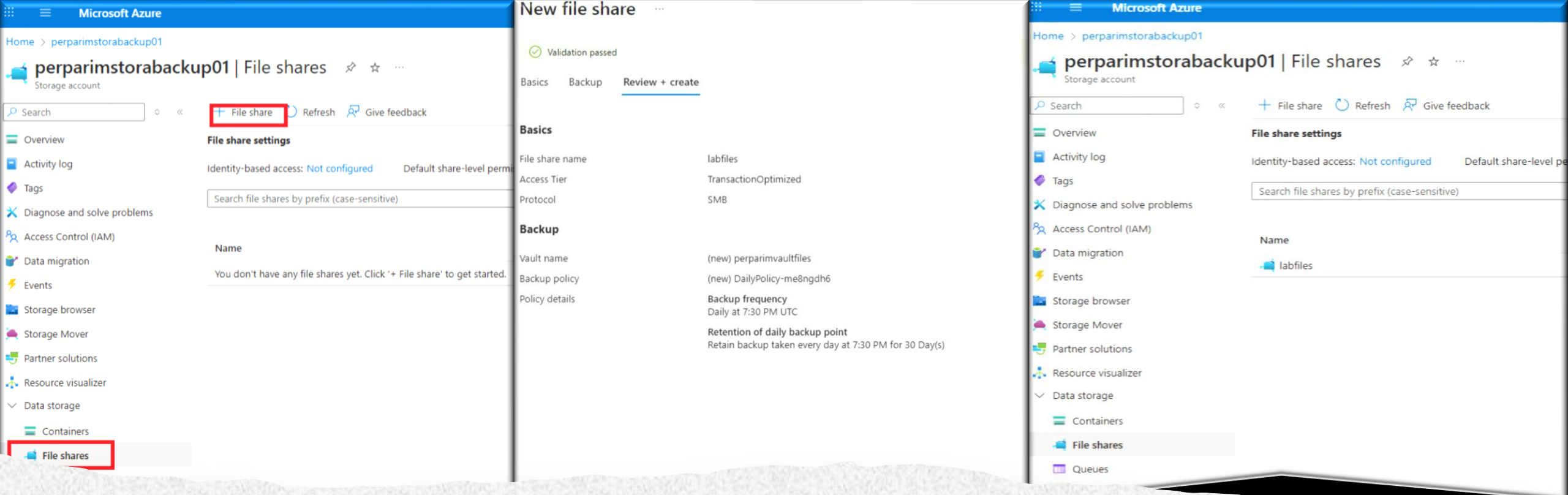
Security

Secure transfer	Enabled
Blob anonymous access	Disabled
Allow storage account key access	Enabled
Default to Microsoft Entra authorization in the Azure portal	Disabled
Minimum TLS version	Version 1.2
Permitted scope for copy operations	From any storage account

[Previous](#) [Next](#) [Create](#)

Recent		Favorite	
Name	Type	Last Viewed	
 perparimstorabackup01	Storage account	a few seconds ago	
 backup-demo-org	Resource group	a few seconds ago	

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



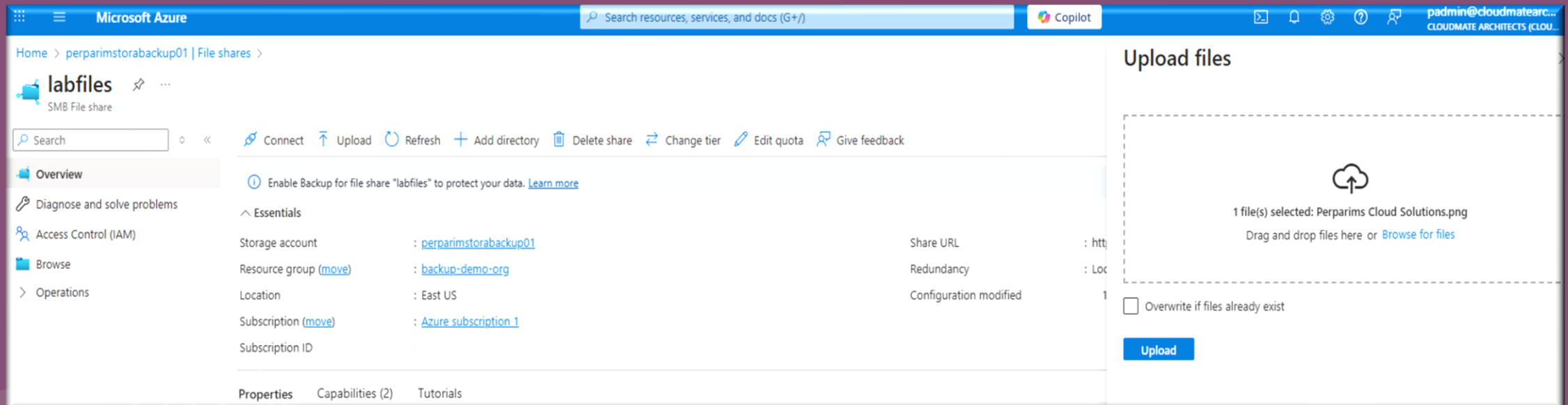
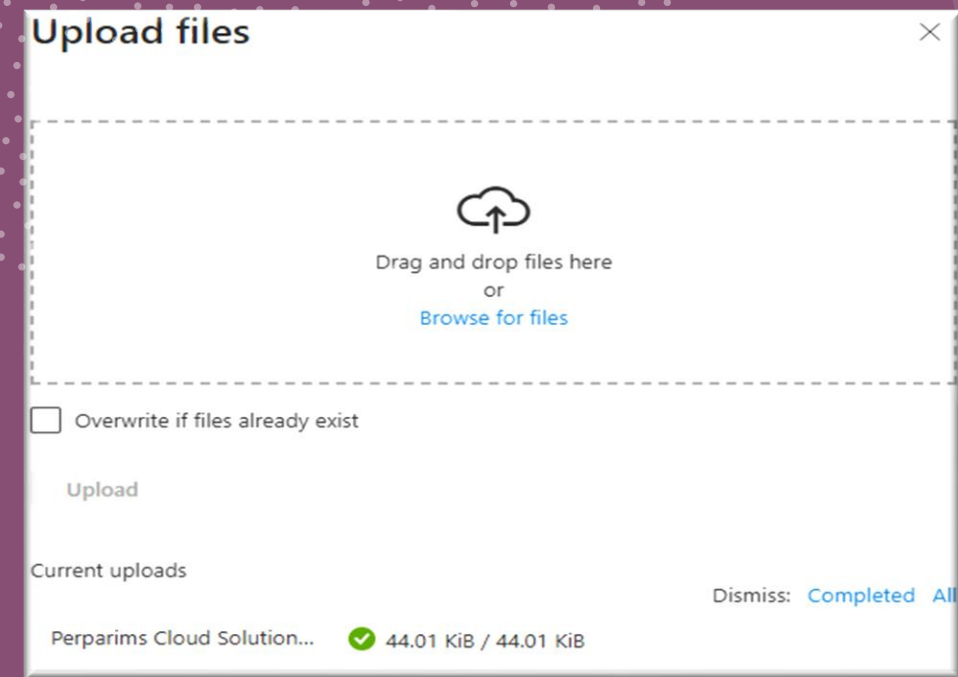
Step 3 – Create Azure File Share

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

💡 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.

The screenshots show the 'Create a virtual machine' wizard in the Microsoft Azure portal. The first screenshot displays the initial configuration page with the following settings:

- Subscription: Azure subscription 1
- Resource group: backup-demo-org
- Instance details:
 - Virtual machine name: perparim-vm-backup
 - Region: (US) East US
 - Availability options: No infrastructure redundancy required
 - Security type: Trusted launch virtual machines
 - Image: Windows Server 2022 Datacenter: Azure Edition Hotpatch - x64 Gen2
 - VM architecture: x64
- Run with Azure Spot discount: ☐
- Size: Standard_D2s_v3 - 2 vcpus, 8 GiB memory (\$137.24/month)
- Enable Hibernation: ☐
- Administrator account:
 - Username: 1padmin

The second screenshot shows the 'Validation passed' screen with a summary of the configuration:

- 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: (Details not visible)

The third screenshot shows the 'Management' and 'Monitoring' sections of the configuration:

- Management:
 - 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
 - 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

💡 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.

The image displays two side-by-side screenshots of the Microsoft Azure portal interface, illustrating the process of enabling Azure Backup for a virtual machine (VM).

Left Screenshot (Configuration Page):

- Navigation:** The left sidebar shows the 'Backup + disaster recovery' section expanded, with 'Backup' selected.
- Header:** The page title is 'perparim-vm-backup | Backup'.
- Welcome Message:** 'Welcome to Azure Backup for Azure VMs. Simple and reliable VM backup to the Azure. Learn more. You are charged an instance fee for backup.' Below this, it says 'Review the following information and click on 'Enable backup' to start protecting your VM.'
- Configuration Options:**
 - Recovery Services vault:** 'Create new' (selected) or 'Select existing'.
 - Backup vault:** 'perparimvaultvm' (with a green checkmark).
 - Resource group:** 'backup-demo-org' (with a dropdown arrow).
 - Policy sub type:** 'Enhanced' (selected) or 'Standard'. Under 'Enhanced', it lists: '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'. Under 'Standard', it lists: 'Once-a-day backup', 'Up to 5 days operational tier retention'.
 - Choose backup policy:** '(new) EnhancedPolicy-me8ohgpr' (with a dropdown arrow and a link to 'Edit this policy').
- 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: Retain backup taken every day for 30 Days'.
- Buttons:** 'Enable backup' (blue) and 'Cancel' (white).

Right Screenshot (Overview Page):

- Navigation:** The left sidebar shows the 'Backup' section selected.
- Header:** The page title is 'perparim-vm-backup | Backup'.
- Actions:** A row of buttons: 'Backup now', 'Restore VM', 'File Recovery', 'Stop backup', 'Resume backup', 'Delete backup data', 'Restore to Secondary Region', 'Undelete', and 'Feedback'.
- Essentials:**
 - Try our new Business Continuity Center for the at scale BCDR management of your resources protected across Azure Backup and Site Recovery.
 - Recovery services vault:** 'perparimvaultvm'.
 - Subscription (move):** 'Azure subscription 1'.
 - Subscription ID:** (empty).
 - Alerts (in last 24 hours):** 'View alerts'.
 - Jobs (in last 24 hours):** 'View jobs'.
- Consistency Status:** Three bars showing '0' for 'CRASH CONSISTENT', 'APPLICATION CONSISTENT', and 'FILE-SYSTEM CONSISTENT'.
- Recovery points:** A section titled 'Recovery points' with a note: '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.' Below it, another note: 'Long term recovery points can be moved to vault-archive. To move all 'recommended recovery points' to vault-archive tier, click here.'
- Table:** A table with columns 'Creation time ↑↓', 'Consistency', and 'Recovery type'. The first row shows '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.

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.

The left screenshot displays the 'Business Continuity Center' 'Protection Overview' page. It features a sidebar with navigation options like 'Overview', 'Getting started', 'Protection inventory', 'Monitoring + Reporting', 'Alerts', 'Metrics', 'Jobs', 'Reports', 'Security + Threat management', 'Governance', 'Manage', and 'Support + Troubleshooting'. The main content area is divided into sections: 'Protection' showing 'Protectable resources' (0 Azure Virtual machines) and 'Protection status' (1 item); 'Security' showing 'BCDR security coverage' (0/1); and 'Monitoring' showing 'Alerts (last 6 hours across datasources)' (0 Critical).

The right screenshot displays the 'Business Continuity Center' 'Protected items' page. It includes a sidebar with similar navigation options. The main content area shows a notification about Azure Database for PostgreSQL, a 'Help me manage my protected items' button, and a summary of protection status for Azure managed Active resources. A table lists the following data:

Solution	Datasource type	Subscription	Resource group	Location	Tags
All	Azure Virtual machines	All	All	All	All

Total	Protected in both primary and secondary regions	Protected in primary region only	Protected in secondary region only	Not protected currently
1	0	0	0	1

Resource name	Protected item	Configured solutions	Protection status in primary region	Protection status in secondary region
perparim-vm-backup	perparim-vm-backup	Azure Backup	Pending protection	Not protected

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

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.

The screenshot shows the 'Jobs' page in the Business Continuity Center. The left sidebar includes 'Overview', 'Getting started', 'Protection inventory', 'Monitoring + Reporting', 'Security + Threat management', and 'Governance'. The 'Jobs' section is selected. The main content area shows a table of job details for 'perparim-vm-backup'.

Operation	Status	Item	Vault
Configure backup	Completed	perparim-vm-backup	perparimvaultvm

The screenshot shows the 'Security posture' page. It displays a summary of security coverage for 'perparim-vm-backup'. The 'Currently showing: Security level details of Azure managed Active resources' section includes a table with the following data:

Total	Excellent security	Good security	Fair security	Poor security	Not available
1	0	0	0	1	0

The screenshot shows the 'Alerts' page. It displays a summary of alerts for 'perparim-vm-backup'. The 'Currently showing: Alerts for Azure managed resources with Basic details' section includes a table with the following data:

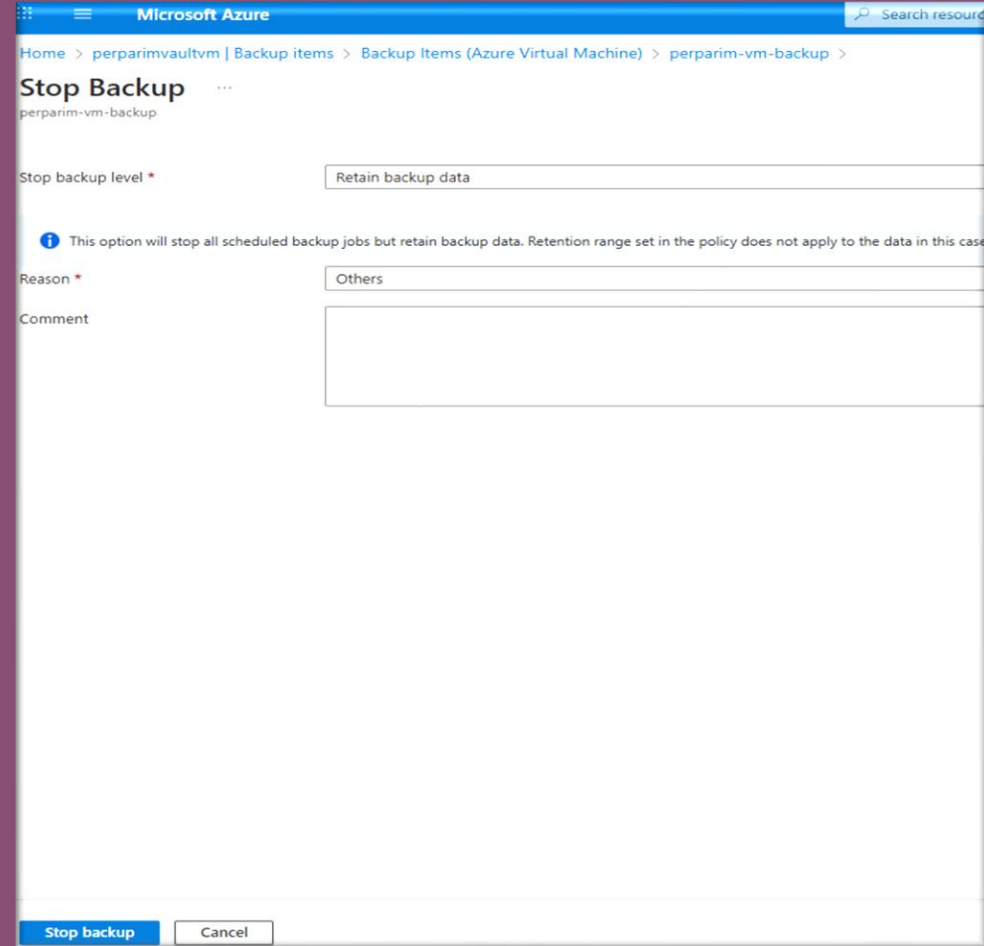
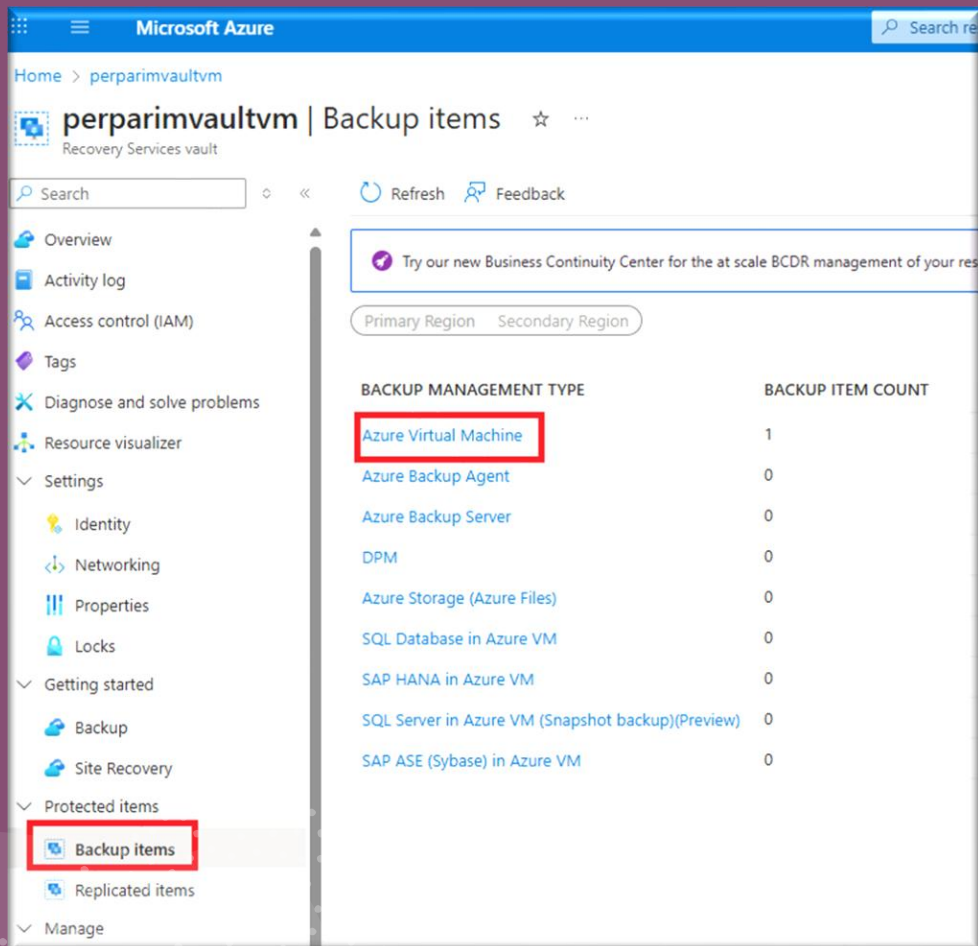
Total	Critical	Error	Warning	Informational	Verbose
0	0	0	0	0	0

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

#PerparimLabs | Azure Backup & Recovery

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.



Step 10: Delete the Backup

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

The screenshot shows the 'Delete Backup' page in the Microsoft Azure portal. The breadcrumb trail is: Home > Recovery Services vaults > perparimvaultvm | Backup items > Backup Items (Azure Virtual Machine) > perparim-vm-backup >. The page title is 'Delete Backup' with a three-dot menu icon. Below the title, there are two informational messages: 'You may have data in vault-archive. Deletion of data that hasn't aged enough can result in additional cost. To know more, [click here](#).' and 'This option will stop all scheduled backup jobs and delete backup data. [Learn More](#).' The form has three fields: 'Type the name of backup item' with the value 'perparim-vm-backup', 'Reason' with the value 'Others', and a 'Comment' text area. At the bottom, there are 'Delete' and 'Cancel' buttons.

The screenshot shows the 'perparimvaultvm | Backup Jobs' page in the Azure portal. The breadcrumb trail is: perparimvaultvm | Backup Jobs >. The page title is 'perparimvaultvm | Backup Jobs' with a star icon and a three-dot menu icon. Below the title, there is a search bar and a list of navigation links: 'Locks', 'Getting started', 'Backup', 'Site Recovery', 'Protected items', 'Backup items', 'Replicated items', 'Manage', 'Backup policies', 'Backup Infrastructure', 'Site Recovery infrastructure', 'Recovery Plans (Site Recovery)', 'Backup Reports', 'Monitoring', 'Alerts', 'Metrics', 'Diagnostic settings', 'Advisor recommendations', and 'Backup Jobs'. The main content area shows a table of backup jobs. The table has four columns: 'Workload name', 'Operation', 'Status', and 'Type'. The table contains three rows of data, all with a status of 'Completed'. Below the table, there is a pagination bar showing 'Page 1 of 1'.

Workload name	Operation	Status	Type
perparim-vm-backup	Delete backup data	Completed	Azure Virtual Machine
perparim-vm-backup	Disable backup	Completed	Azure Virtual Machine
perparim-vm-backup	Configure backup	Completed	Azure Virtual Machine

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**

The first screenshot shows the 'perparimvaultfiles' Recovery Services vault. The 'Backup items' pane is highlighted with a red box. A table lists backup management types and their counts:

BACKUP MANAGEMENT TYPE	BACKUP ITEM COUNT
Azure Storage (Azure Files)	1
Azure Virtual Machine	0
Azure Backup Agent	0
Azure Backup Server	0
DPM	0
SQL Database in Azure VM	0
SAP HANA in Azure VM	0
SQL Server in Azure VM (Snapshot backup)(Preview)	0
SAP ASE (Sybase) in Azure VM	0

The second screenshot shows the 'Stop Backup' dialog. The 'Delete backup data' option is selected. The 'Reason' is set to 'Others'.

The third screenshot shows the 'Backup Jobs' page. A table displays the sequence of jobs:

Workload name	Operation	Status	Type
labfiles (perparimstorabackup01)	Delete backup data	Completed	Azure Storage
labfiles (perparimstorabackup01)	Configure backup	Completed	Azure Storage
perparimstorabackup01 (perparimst...	Register	Completed	Azure Storage

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).

Delete a resource group

The following resource group and all its dependent resources will be permanently deleted.

Resource group to be deleted

backup-demo-org

Dependent resources to be deleted (4)

All dependent resources, including hidden types, are shown

Name	Resource type
perparim-vm-backup-nsg	Network security group
perparim-vm-backup-vnet	Virtual network
perparimvaultfiles	Recovery Services vault
perparimvaultvm	Recovery Services vault

Enter resource group name to confirm deletion *

backup-demo-org

DeleteCancel

Delete perparim-vm-backup

This action will permanently delete this virtual machine.

Resource to be deleted

perparim-vm-backup

Resource type

Virtual machine

☒ Apply force delete ⓘ

This virtual machine can be safely force deleted because all of its associated resources are being deleted.

You can also choose to delete associated resources at the same time. Resources that aren't deleted will be orphaned. Associated resources that are in use by other resources are not shown here.

Associated resource type	Quantity	Delete with VM
OS disk	1	<input checked="" type="checkbox"/>
Network interfaces	1	<input checked="" type="checkbox"/>
Public IP addresses	1	<input checked="" type="checkbox"/>

☒ Successfully deleted virtual machine 'perparim-vm-backup'

Virtual machine 'perparim-vm-backup' and any selected resource(s) have been successfully deleted.

a few seconds ago

☒ I have read and understand that this virtual machine as well as any selected associated resources listed above will be deleted.

DeleteCancel

Delete storage account

The following storage account and its contents will be deleted.

Resource to be deleted

perparimstorabackup01

Dependent resources to be deleted

The data provided is regularly updated about 2-4 times a day and published hourly. If your account has extremely large objects, it may be over a day between updates.

Resource	Number of instances	Total data stored
Containers	-	-
File shares	-	-
Tables	-	-
Queues	-	-

Successfully deleted storage account

Successfully deleted storage account 'perparimstorabackup01'.

a few seconds ago



Enter storage account name to confirm deletion *

perparimstorabackup01

Delete

Cancel

Give feedback

#PerparimLabs | Azure Backup & Recovery

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.