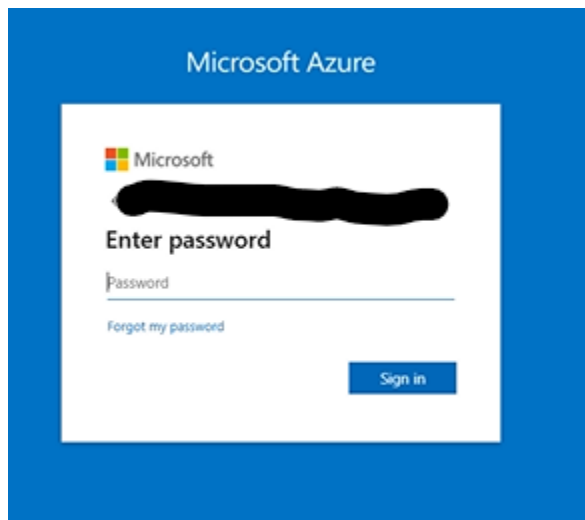


# Implement Azure Backup for Azure Virtual Machines

---

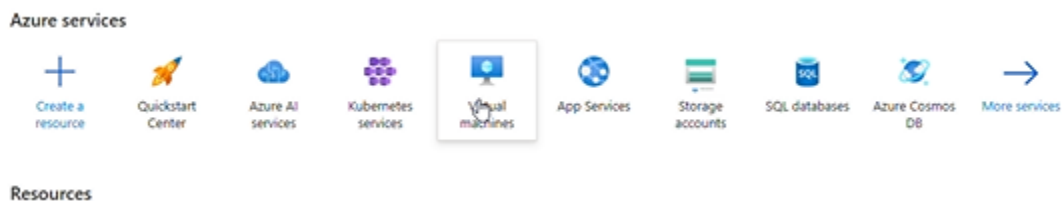
## Backup an Azure virtual machine by using the Azure portal

Sign in to Admin



To enable backups on the wanted virtual machine by using an Azure recovery services follow the following steps:

1. **Sign in to the Azure Portal** and navigate to **"Virtual Machines"**



2. Select the virtual machine you want to back up

Microsoft Azure

Search resources, services, and docs (G+/J)

Home >

Virtual machines

cloudslice (cloudslice.onmicrosoft.com)

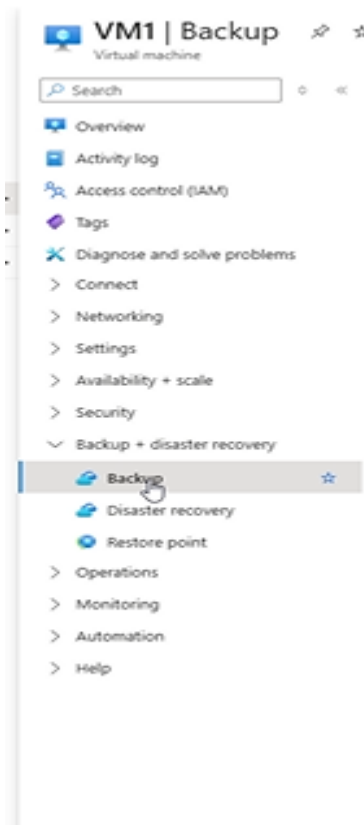
+ Create Switch to classic Reservations Manage view Refresh Export to CSV Open query Assign tags Start Restart Stop Delete Services

Filter for any field... Subscription equals all Type equals all Resource group equals all Location equals all Add filter

Showing 1 to 3 of 3 records.

Name	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disks
VM1	Challenge Labs 02	[REDACTED]	East US 2	Running	Windows	Standard_DS3_v2	[REDACTED]	2
VM2	Challenge Labs 02	[REDACTED]	East US 2	Running	Windows	Standard_DS3_v2	[REDACTED]	2
VM3	Challenge Labs 02	[REDACTED]	East US 2	Running	Windows	Standard_DS3_v2	[REDACTED]	2

- In the virtual machine menu, go to **"Backup + Disaster Recovery"** and select **"Backup"**



- On the backup page, click **"Create New"**, enter the required details, and choose **Standard** as the policy subtype. Click **"Enable Backup"**

**Welcome to Azure Backup for Azure VMs**  
 Simple and reliable VM backup to the Azure. [Learn more.](#) You are charged an instance fee based on the size of the VM and for backup data retained in Snapshots and the Recovery Services Vault. [Learn more about pricing.](#)  
 Review the following information and click on 'Enable backup' to start protecting your VM.

Recovery Services vault ☐ Create new ☐ Select existing

Backup vault \*

Resource group

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 \*  [Edit this policy](#)

**Policy Details**

Full backup

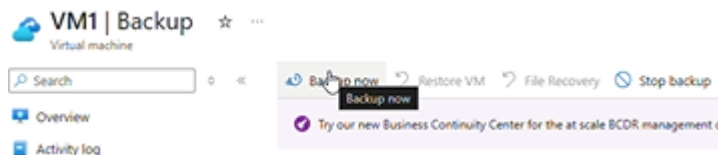
**Backup frequency**  
Daily at 8:00 AM UTC

**Instant restore**  
Retain instant recovery snapshot(s) for 2 day(s)

**Retention of daily backup point**  
Retain backup taken every day at 8:00 AM for 30 Day(s)

[Enable backup](#) [Cancel](#) [Give feedback](#)

5. To initiate the backup, return to the **Azure Portal**, navigate to **"Backup"**, and click **"Backup Now."** Confirm by selecting **OK**
6. Ensure the selected **retention period** aligns with your organization's backup policy.



*Note: Select the retainment date that goes with your policy and organization*

Azure Backup is a cloud-native solution that streamlines VM data protection without requiring complex on-premises infrastructure. It leverages **Recovery Services Vaults** for centralized backup management, with **Geo-Redundant Storage (GRS)** as the default option, replicating data to a secondary region for disaster recovery. Organizations can opt for **Locally Redundant**

**Storage (LRS)** for cost efficiency or **Zone-Redundant Storage (ZRS)** for increased regional resilience.

Backup policies define **scheduling and retention**, with the default setting performing **daily backups** and retaining data for **30 days**. The **first backup is full**, while subsequent ones are **incremental**, reducing storage costs and backup duration. **Application-consistent backups** ensure database integrity by capturing active transactions, preventing corruption.

Azure supports **four backup methods**:

1. **Azure Portal** – GUI-based management for ease of use.
2. **Azure PowerShell** – Automates backups via scripting.
3. **Azure CLI 2.0** – Enables command-line-based backup operations.
4. **ARM Templates** – Infrastructure-as-Code (IaC) approach for scalable deployment.

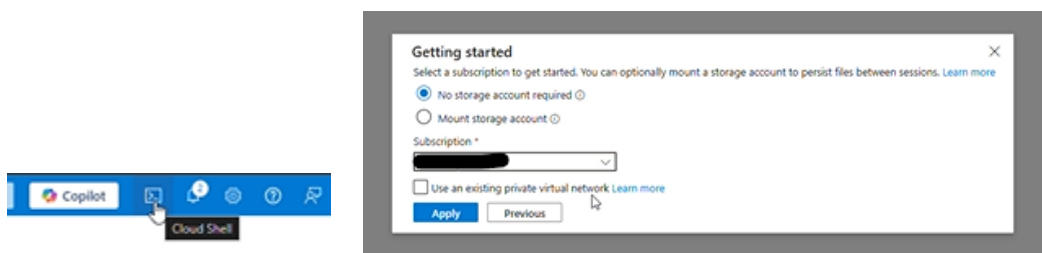
Security features include **Soft Delete**, which retains deleted backups for **14 days**, and **RBAC with Multi-User Authentication (MUA)** to prevent unauthorized access. **Flexible recovery options** allow restoring **entire VMs, disks, or files** to the original location or a new VM, ensuring minimal downtime.

**Azure Monitor and Backup Reports** provide real-time tracking, while **Azure Policy** enforces compliance. By automating backups, optimizing storage, and ensuring security, Azure Backup supports business continuity and disaster recovery while aligning with cloud security best practices.

---

## Enable backups on an Azure virtual machine by using Azure Powershell

1. Open an Azure Cloud Shell Powershell session without mounting a storage account



2. Set the Recovery Services Vault context:

- `Get-AzRecoveryServicesVault -Name "<Your-RecoveryServicesVault-Name>" | Set-AzRecoveryServicesVaultContext`
- This command retrieves the specified vault and sets it as the active context for subsequent backup and recovery operations

```
MODT: Azure Cloud Shell now includes Predictive IntelliSense! Learn more: https://aka.ms/CloudShell/IntelliSense
VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
PS /home/<redacted> > Get-AzRecoveryServicesVault -Name "<redacted>" | Set-AzRecoveryServicesVaultContext
PS /home/<redacted> >
```

3. Create a variable named `$policy` to store the default backup policy:

- `$policy = Get-AzRecoveryServicesBackupProtectionPolicy -Name "DefaultPolicy"`
- This policy defines backup schedules, retention periods, and settings for Azure VM backups

```
PS /home/<redacted> > $policy = Get-AzRecoveryServicesBackupProtectionPolicy -Name "DefaultPolicy"
PS /home/<redacted> >
```

4. Enable VM backup using the retrieved policy

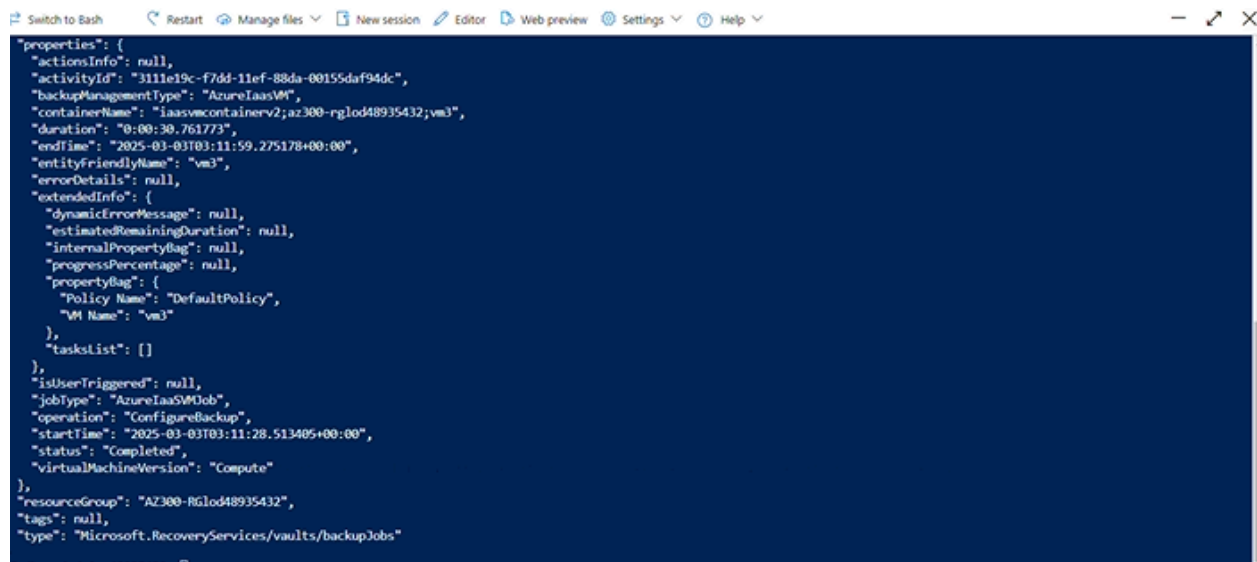
- `Enable-AzRecoveryServicesBackupProtection -ResourceGroupName "<Your-ResourceGroup-Name>" -Name "<Your-VM-Name>" -Policy $policy`
- This command ensures that the specified VM is included in Azure Backup according to the selected backup policy

```
VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
PS /home/<redacted> > Get-AzRecoveryServicesVault -Name "<redacted>" | Set-AzRecoveryServicesVaultContext
PS /home/<redacted> > $policy = Get-AzRecoveryServicesBackupProtectionPolicy -Name "DefaultPolicy"
PS /home/<redacted> > Enable-AzRecoveryServicesBackupProtection -ResourceGroupName "<redacted>" -Name "VM0" -Policy $policy
WARNING: Ignite (November) 2023 onwards Virtual Machine deployments using PS and CLI will default to Trusted Launch configuration. You need to ensure Policy Name used with this command is of type Enhanced Policy for Trusted Launch VMs. Non-Trusted Launch Virtual Machines will not be impacted by this change. To know more about default change and Trusted Launch, please visit https://aka.ms/TLAD.

WorkloadName  Operation      Status      StartTime      EndTime        JobID
-----
vm2            ConfigureBackup Completed    3/3/2025 3:08:39 AM  3/3/2025 3:09:10 AM  23dfe489-5890-4136-988a-4ada656231ed
PS /home/admin-48935432> Get-AzRecoveryServicesVault -Name "<redacted>" | Set-AzRecoveryServicesVaultContext
```

## Enable backups on an Azure virtual machine by using Azure CLI 2.0

1. Open a command-line interface with Azure CLI installed.
2. Run the following command to enable backup protection for the virtual machine:
  - `az backup protection enable-for-vm --resource-group "<Your-ResourceGroup-Name>" --vault-name "<Your-RecoveryServicesVault-Name>" --vm "<Your-VM-Name>" --policy-name "<Your-Backup-Policy-Name>"`
  - This command applies the specified backup policy to the virtual machine, ensuring scheduled backups are performed automatically



```
Switch to Bash  Restart  Manage files  New session  Editor  Web preview  Settings  Help

{"properties": {"actionsInfo": null,
"activityId": "3111e19c-f7dd-11ef-88da-00155daf94dc",
"backupManagementType": "AzureIaaSVM",
"containerName": "iaasvmcontainerv2;az300-rglod48935432;vm3",
"duration": "0:00:30.761773",
"endTime": "2025-03-03T03:11:59.275178+00:00",
"entityFriendlyName": "vm3",
"errorDetails": null,
"extendedInfo": {
"dynamicErrorMessage": null,
"estimatedRemainingDuration": null,
"internalPropertyBag": null,
"progressPercentage": null,
"propertyBag": {
"Policy Name": "DefaultPolicy",
"VM Name": "vm3"
},
},
"tasksList": []
},
"isUserTriggered": null,
"jobType": "AzureIaaSVMJob",
"operation": "ConfigureBackup",
"startTime": "2025-03-03T03:11:28.513405+00:00",
"status": "Completed",
"virtualMachineVersion": "Compute"
},
"resourceGroup": "AZ300-RGlod48935432",
"tags": null,
"type": "Microsoft.RecoveryServices/vaults/backupJobs"
}
```