**PROJECT 3**

**BACKUP AND RESTORE OF AZURE VIRTUAL MACHINES**

**SUBMITTED BY**

**NANDHITHA DAS MOHANDAS**

**PROJECT OBJECTIVES:** To ensure business continuity and disaster recovery by configuring Azure Backup for Virtual Machines, performing a backup operation, and validating recovery by restoring the VM into a new instance**.**

**Step 1: Create a Virtual Machine (if not already available)**

1. Go to Azure Portal.
2. Navigate to:  
   Virtual Machines → + Create → Virtual Machine
3. Configure:
   * OS: Ubuntu/Windows (your choice)
   * Region, size, username, and authentication

Complete the deployment.

A screenshot of a computer

AI-generated content may be incorrect.

Fig 1: This screenshot is creation of VM in Canada central, name of VM is backuprestore-vm, we need to take backup of this VM

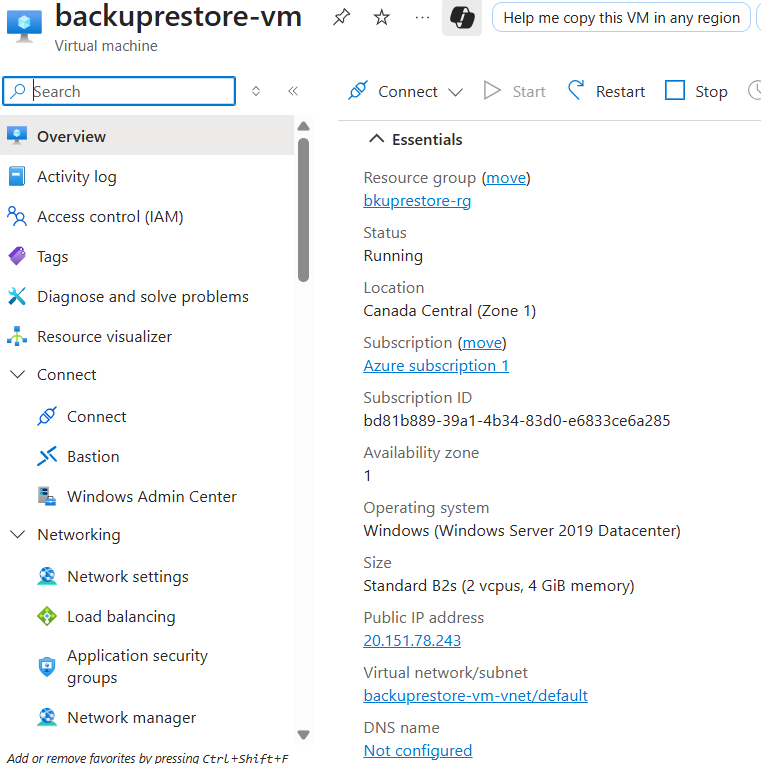


Fig 2: So created a Windows VM in Canada central with username and password, this screenshot is the overview of VM

**Step 2: Create a Recovery Services Vault**

1. Search for Recovery Services Vault in the portal.
2. Click + Create:
   * Name: MyBackupVault
   * Region: Same as your VM
   * Resource Group: Select or create new
3. Click Review + Create → Create

A screenshot of a computer

AI-generated content may be incorrect.

Fig 3: shows the creation of recovery service vault , name of the vault is MyBackupVault

**Step 3: Enable Backup for the VM**

1. Go to the Recovery Services Vault created.
2. In the left pane, click + Backup.
3. Configure Backup:
   * Where is your workload running? → Azure
   * What do you want to back up? → Virtual machine
4. Click Backup, then select your VM from the list.
5. Click Enable Backup.

A screenshot of a computer

AI-generated content may be incorrect.

Fig 4: configuration backup

A screenshot of a computer

AI-generated content may be incorrect.

Fig 5: successfully configured backup

In the backup items, we can see one azure virtual machine there.

A screenshot of a computer

AI-generated content may be incorrect.

Fig 6: In this we can see the number of backup items

**Step 4: Trigger an On-Demand Backup**

1. In the vault → go to Backup Items → Azure Virtual Machine
2. Select the VM → click Backup Now

Confirm and monitor backup status under Jobs

A screenshot of a computer

AI-generated content may be incorrect.

Fig 7: overview of backup item

A blue line with a white background

AI-generated content may be incorrect.

Fig 8: Initiate first backup

A screenshot of a computer

AI-generated content may be incorrect.

Fig 9: notification showing the backup was successfully taken

A screenshot of a computer

AI-generated content may be incorrect.

Fig 10: status of last backup is success.

**Step 5: Restore the Windows VM**

1. Go to the same vault → **Backup items → Azure Virtual Machine**.
2. Select your VM → click **Restore VM**.
3. Pick the **latest restore point**.
4. Choose **Restore Type → Create new VM**.
5. Provide a name (example: Restored-VM) → keep region as **Canada Central**.
6. Click **Restore**.

A screenshot of a computer

AI-generated content may be incorrect.

Fig 11: overview of backuprestore-vm

A screenshot of a computer

AI-generated content may be incorrect.

Fig 12: select the date for creating restore point

A screenshot of a computer

AI-generated content may be incorrect.

Fig 13: already created a staging location in storage account, creating a restore VM in the same region

**Restore Point**

* **Recovery Point (also known as Restore Point): A recovery point is a copy of the original data that's being backed up.**

A screenshot of a computer

AI-generated content may be incorrect.

Fig 14: automatically created a restore point collections

**Step 6: Verify Restored VM**

1. Go to Virtual Machines → Look for Restored-VM
2. Use Connect → RDP or SSH to log in and verify:
   * OS boots correctly
   * Disk and file contents are intact (if tested)

A screenshot of a computer

AI-generated content may be incorrect.

Fig 15: here we can see 2 VM

A screenshot of a computer

AI-generated content may be incorrect.

Fig : OS disks

A screenshot of a computer

AI-generated content may be incorrect.

Fig 16: this is Restore-vm

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Fig 17: successfully login to restore-vm and can see the backup items

Optional Enhancements

* Customize backup policy: increase frequency or retention (under Backup Policies).

1. Go to your **Recovery Services Vault**.
2. In the left menu → **Backup Policies**.
3. Click **+ Add** (or edit the default).
4. Configure:
5. **Backup Frequency**: Daily or Multiple Times/Day
6. **Retention**: Decide how many days/weeks/months/years to keep
7. Save the policy.
8. Assign this policy to your VM.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a backup schedule

AI-generated content may be incorrect.

* Enable soft delete and multi-user authorization for higher protection.

**Soft Delete:** Protects backups from accidental deletion. Deleted backup data is retained for **14 days** by default.

**Steps (via Azure Portal):**

1. Go to **Recovery Services Vault** → **Properties**.
2. Under **Soft Delete**, toggle **Enabled**.

A screenshot of a computer

AI-generated content may be incorrect.

Monitor backup health regularly via vault **Backup Jobs** and **Alerts**.

A screenshot of a computer

AI-generated content may be incorrect.