A. Schedule Daily Backup of VM at 3:00 AM Using Recovery Services Vault

1. Create a Recovery Services Vault

A Recovery Services Vault is a storage entity in Azure that houses backup data for various Azure resources, including virtual machines (VMs). To create one:

- **Azure Portal**: Navigate to **All Services** > **Backup Center** > **+ Backup**. Follow the prompts to create a new vault.
- **Azure CLI**:

```
az backup vault create --name MyRecoveryVault --resource-group MyResourceGroup --location eastus
```

Note: The location of the vault should ideally match the region of the VM to optimize performance and compliance.

2. Register the VM with the Vault and Enable Backup

Once the vault is created, register your VM to enable backup:

- **Azure Portal**: In the Recovery Services Vault, go to **Backup** > **Backup Goal** > **Azure Virtual Machines**. Select your VM and follow the prompts to enable backup.
- **Azure CLI**:

```
az backup protection enable-for-vm --resource-group MyResourceGroup --vault-name MyRecoveryVault --vm MyVM --policy-name DefaultPolicy
```

Note: The DefaultPolicy is a predefined policy that schedules daily backups. You can create a custom policy if specific configurations are needed.

3. Create a Custom Backup Policy with a 3:00 AM Schedule

To set a backup schedule at 3:00 AM:

- **Azure Portal**: In the Recovery Services Vault, navigate to **Backup Policies** > **+ Add**. Define the schedule to run daily at 3:00 AM.
- **Azure CLI**: While the Azure CLI doesn't directly support creating custom schedules, you can use PowerShell or the REST API to define a backup policy with a specific schedule.

Note: The backup schedule is based on UTC time. Ensure you adjust for your local timezone if necessary.

4. Apply the Backup Policy to the VM

After creating the policy:

- **Azure Portal**: In the Recovery Services Vault, go to **Backup Items** > **Azure Virtual Machine**. Select your VM and apply the newly created backup policy.
- **Azure CLI**:

```
az backup protection set-policy --resource-group MyResourceGroup --vault-name MyRecoveryVault --item-name MyVM --policy-name MyCustomPolicy
```

Note: Ensure that the VM is not in a soft-deleted state, as it won't be visible for backup configuration until the soft delete period expires.

B. Create an Alert Rule for VM CPU Usage > 80% with Email Notification

1. Create an Action Group

An Action Group defines the actions to take when an alert is triggered:

- **Azure Portal**: Navigate to **Monitor** > **Action Groups** > **+ Add**. Define the action group with an email notification.
- **Azure CLI**:

```
az monitor action-group create --resource-group MyResourceGroup --name CPUAlertGroup --short-name alertgrp --email-receiver name=AdminEmail email=admin@example.com
```

Note: Replace admin@example.com with your actual email address.

2. Create a Metric Alert Rule for CPU Usage

To monitor CPU usage:

- **Azure Portal**: Go to **Monitor** > **Alerts** > **+ New Alert Rule**. Select the target resource (your VM), define the condition (CPU usage > 80%), and associate the action group created earlier.
- **Azure CLI**:

```
az monitor metrics alert create --name HighCPUAlert --resource-group MyResourceGroup --scopes $(az vm show --name MyVM --resource-group MyResourceGroup --query id -o tsv) --condition "avg Percentage CPU > 80" --description "Alert when CPU > 80%" --action-group CPUAlertGroup
```

Note: The alert will trigger when the average CPU percentage exceeds 80% over the evaluation period.

C. Provision Backups Using Backup Center

1. Navigate to Backup Center

- **Azure Portal**: Go to **All Services** > **Backup Center**.

2. Configure Backup

- Click on **+ Backup**.
- For **Where is your workload running?**, select **Azure**.
- For **What do you want to back up?**, choose **Azure Virtual Machines**.
- Select your Recovery Services Vault and the VM(s) you wish to back up.
- Apply the desired backup policy and enable backup.

Note: Backup Center provides a unified management experience for backup operations, allowing you to monitor and manage backups across your environment.

D. Configure Retention Period and Retain Old Backups

1. Define Retention Policy

Retention policies determine how long backup data is retained:

- **Azure Portal**: In the Recovery Services Vault, navigate to **Backup Policies** > **Modify**. Adjust the retention settings as needed.
- **Azure CLI**: Use the az backup policy set command to modify the retention settings of an existing policy.

Note: Azure Backup supports retention periods ranging from 7 days up to 9999 days. The default retention for daily backups is 30 days, but this can be customized based on your requirements.

2. Apply the Retention Policy

After defining the retention policy:

- **Azure Portal**: Apply the modified policy to your VM by navigating to **Backup Items** > **Azure Virtual Machine** and selecting the appropriate policy.
- **Azure CLI**:

```
az backup policy set --resource-group MyResourceGroup --vault-name MyRecoveryVault --policy-name MyCustomPolicy --retention-policy "Daily:30"
```

Note: Ensure that the retention policy aligns with your organization's data retention and compliance requirements.

Summary Table

Task	**Tool**	**Description**
Create Recovery Services Vault	Azure CLI	az backup vault create
Register VM and Enable Backup	Azure CLI	az backup protection enable-for-vm
Create Custom Backup Policy	Azure Portal	Define schedule and retention settings
Apply Backup Policy to VM	Azure CLI	az backup protection set-policy
Create Action Group for Alerts	Azure CLI	az monitor action-group create
Create Metric Alert Rule for CPU Usage	Azure CLI	az monitor metrics alert create
Provision Backups Using Backup Center	Azure Portal	Configure backup for VM(s)
Configure Retention Period	Azure Portal	Modify backup policy retention settings