**Configuring VM Backups in Azure**

**1. Why Protect Virtual Machine Data?**

Virtual machines (VMs) often run critical workloads. Data loss due to accidental deletion, corruption, ransomware, or disasters can lead to severe business impact. Azure provides multiple backup and disaster recovery solutions to ensure **business continuity and disaster recovery (BCDR)**.

**2. Backup Options for Azure VMs**

Azure offers three main approaches for VM data protection:

**a) Azure Backup**

* **Purpose:** Protects Azure VMs running production workloads.
* **How it works:** Creates **application-consistent snapshots** and stores them in a **Recovery Services vault**.
* **Features:**
  + Incremental backups (only changed blocks are transferred).
  + Supports **encryption at rest** using Storage Service Encryption (SSE) and Azure Disk Encryption.
  + **Soft Delete** feature prevents accidental backup deletion for 14 days.
  + **Instant Restore** allows quick recovery using local snapshots before data transfer completes.
* **Use case:** Daily backups, long-term retention, compliance needs. [[About Azur...soft Learn]](https://learn.microsoft.com/en-us/azure/backup/backup-azure-vms-introduction)

**b) Azure Site Recovery (ASR)**

* **Purpose:** Disaster Recovery (DR) solution for **region-wide outages** or catastrophic failures.
* **How it works:** Continuously replicates VMs to a secondary Azure region or on-premises site.
* **Features:**
  + **Failover & Failback:** Seamless switch to secondary site during outages.
  + **RPO/RTO:** Recovery Point Objective as low as 30 seconds for Hyper-V; near real-time replication for Azure VMs.
  + **Custom Recovery Plans:** Automate failover sequences using Azure Automation.
  + **Non-disruptive DR drills:** Test without impacting production.
* **Use case:** Business continuity during **natural disasters, regional outages, or large-scale failures**. [[About Azur...soft Learn]](https://learn.microsoft.com/en-us/azure/site-recovery/site-recovery-overview)

**c) Managed Disk Snapshots**

* **Purpose:** Quick, point-in-time backup of VM disks.
* **How it works:** Creates a **read-only copy** of a managed disk (OS or data disk).
* **Features:**
  + Independent of the source disk.
  + Can be used to create new disks or VMs.
  + **Billing:** Based on used size, not provisioned size.
* **Use case:** Short-term backup before maintenance, troubleshooting, or migration. [[Create an...irtual ...]](https://learn.microsoft.com/en-us/azure/virtual-machines/snapshot-copy-managed-disk)

**3. Azure Backup Job Phases**

An Azure VM backup job has **two main phases**:

1. **Snapshot Phase:** A VM snapshot is taken (app-consistent, file-consistent, or crash-consistent).
2. **Transfer Phase:** Snapshot data is transferred to the **Recovery Services vault**.
   * **Instant Restore:** Allows recovery from local snapshots without waiting for vault transfer.
   * Snapshots are incremental after the first full backup, reducing storage and bandwidth costs. [[Azure Inst...Azure Docs]](https://docs.azure.cn/en-us/backup/backup-instant-restore-capability)

**4. Types of Snapshot Consistency**

* **Application-consistent:** Captures in-memory data and pending I/O (best for databases).
* **File-system consistent:** Captures file system state; apps may need repair.
* **Crash-consistent:** Captures disk state only; similar to pulling the power plug. [[About Azur...soft Learn]](https://learn.microsoft.com/en-us/azure/backup/backup-azure-vms-introduction)

**5. Steps to Back Up Azure VMs**

**a) Create a Recovery Services Vault**

* Go to **Azure Portal → Business Continuity Center → +Vault → Recovery Services Vault**.
* Provide:
  + **Name** (unique within subscription).
  + **Region** (must match VM region).
  + **Resource Group**.
* Configure **storage redundancy**:
  + **GRS (Geo-Redundant Storage):** Default, for high durability.
  + **LRS (Locally Redundant Storage):** Cheaper, single-region.
  + **ZRS (Zone-Redundant Storage):** For zone-level resiliency.
* Enable **Cross-Region Restore** if needed. [[Create and...ure Backup]](https://learn.microsoft.com/en-us/azure/backup/backup-create-recovery-services-vault)

**b) Enable Backup for VM**

* In the vault, select **Backup → Azure → Virtual Machine**.
* Choose **Backup Policy** (default: daily backup, 30-day retention).
* Start **Initial Backup** (full snapshot).

**6. Implementing Azure Backup Server (MABS)**

For **on-premises workloads** or **advanced scenarios**:

* **Install MABS** on a Windows Server (on-prem or Azure VM).
* **Register with Recovery Services Vault**.
* **Deploy Protection Agents** on machines to protect.
* **Configure Protection Groups** for workloads (SQL, Hyper-V, VMware, etc.).
* **Backup Flow:**
  + Short-term: Local disk (DPM/MABS storage).
  + Long-term: Azure cloud via **MARS agent**.
* **Note:** MABS does not support tape backup and must run on a dedicated server. [[Use Azure...ure Backup]](https://learn.microsoft.com/en-us/azure/backup/backup-azure-microsoft-azure-backup)

**7. Best Practices**

* **Use Application-Consistent Backups** for databases and critical apps.
* **Enable Soft Delete** to prevent accidental backup deletion.
* **Test Restores Regularly** to validate recovery plans.
* **Monitor Backup Jobs** using **Azure Backup Center**.
* **Plan for Costs:** Consider snapshot retention, vault storage, and network egress.