Azure Backup:

For Azure VMs that are selected for backup, Azure Backup starts a backup job according to the backup schedule you specify.

1. During the first backup, a backup extension is installed on the VM if the VM is running.
   * For Windows VMs, the *VMSnapshot* extension is installed.
   * For Linux VMs, the *VMSnapshotLinux* extension is installed.
2. For Windows VMs that are running, Backup coordinates with Windows Volume Shadow Copy Service (VSS) to take an app-consistent snapshot of the VM.
   * By default, Backup takes full VSS backups.
   * If Backup can't take an app-consistent snapshot, then it takes a file-consistent snapshot of the underlying storage (because no application writes occur while the VM is stopped).

For Linux VMs, Backup takes a file-consistent backup. For app-consistent snapshots, you need to manually customize pre/post scripts.

In each Azure subscription, you can create up to 500 vaults.

https://docs.microsoft.com/en-us/azure/backup/backup-azure-backup-faq

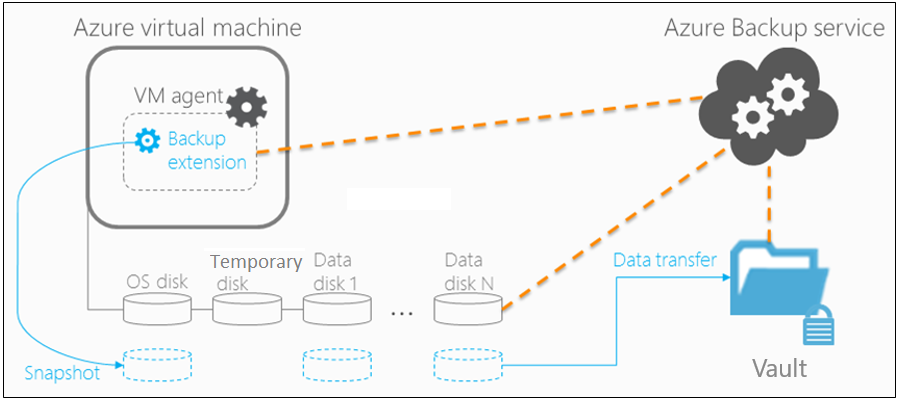
After Backup takes the snapshot, it transfers the data to the vault.

The backup is optimized by backing up each VM disk in parallel.

For each disk that's being backed up, Azure Backup reads the blocks on the disk and identifies and transfers only the data blocks that changed (the delta) since the previous backup.

Snapshot data might not be immediately copied to the vault. It might take some hours at peak times. Total backup time for a VM will be less than 24 hours for daily backup policies.

1. Changes made to a Windows VM after Azure Backup is enabled on it are:
   * Microsoft Visual C++ 2013 Redistributable(x64) - 12.0.40660 is installed in the VM
   * Startup type of Volume Shadow Copy service (VSS) changed to automatic from manual
   * IaaSVmProvider Windows service is added
2. When the data transfer is complete, the snapshot is removed, and a recovery point is created.



**Snapshot creation**

Azure Backup takes snapshots according to the backup schedule.

* **Windows VMs:** For Windows VMs, the Backup service coordinates with VSS to take an app-consistent snapshot of the VM disks.
  + By default, Azure Backup takes full VSS backups. [Learn more](https://blogs.technet.com/b/filecab/archive/2008/05/21/what-is-the-difference-between-vss-full-backup-and-vss-copy-backup-in-windows-server-2008.aspx).
  + To change the setting so that Azure Backup takes VSS copy backups, set the following registry key from a command prompt:

**REG ADD "HKLM\SOFTWARE\Microsoft\BcdrAgent" /v USEVSSCOPYBACKUP /t REG\_SZ /d TRUE /f**

* **Linux VMs:** To take app-consistent snapshots of Linux VMs, use the Linux pre-script and post-script framework to write your own custom scripts to ensure consistency.
  + Azure Backup invokes only the pre/post scripts written by you.
  + If the pre-scripts and post-scripts execute successfully, Azure Backup marks the recovery point as application-consistent. However, when you're using custom scripts, you're ultimately responsible for the application consistency.
  + [Learn more](https://docs.microsoft.com/en-us/azure/backup/backup-azure-linux-app-consistent) about how to configure scripts.

### Snapshot consistency

The following table explains the different types of snapshot consistency:

| **Snapshot** | **Details** | **Recovery** | **Consideration** |
| --- | --- | --- | --- |
| **Application-consistent** | App-consistent backups capture memory content and pending I/O operations. App-consistent snapshots use a VSS writer (or pre/post scripts for Linux) to ensure the consistency of the app data before a backup occurs. | When you're recovering a VM with an app-consistent snapshot, the VM boots up. There's no data corruption or loss. The apps start in a consistent state. | Windows: All VSS writers succeeded  Linux: Pre/post scripts are configured and succeeded |
| **File-system consistent** | File-system consistent backups provide consistency by taking a snapshot of all files at the same time. | When you're recovering a VM with a file-system consistent snapshot, the VM boots up. There's no data corruption or loss. Apps need to implement their own "fix-up" mechanism to make sure that restored data is consistent. | Windows: Some VSS writers failed   Linux: Default (if pre/post scripts aren't configured or failed) |
| **Crash-consistent** | Crash-consistent snapshots typically occur if an Azure VM shuts down at the time of backup. Only the data that already exists on the disk at the time of backup is captured and backed up.  A crash-consistent recovery point doesn't guarantee data consistency for the operating system or the app. | Although there are no guarantees, the VM usually boots, and then it starts a disk check to fix corruption errors. Any in-memory data or write operations that weren't transferred to disk before the crash are lost. Apps implement their own data verification. For example, a database app can use its transaction log for verification. If the transaction log has entries that aren't in the database, the database software rolls transactions back until the data is consistent. | VM is in shutdown state |

## Backup and restore considerations

| **Consideration** | **Details** |
| --- | --- |
| **Disk** | Backup of VM disks is parallel. For example, if a VM has four disks, the Backup service attempts to back up all four disks in parallel. Backup is incremental (only changed data). |
| **Scheduling** | To reduce backup traffic, back up different VMs at different times of the day and make sure the times don't overlap. Backing up VMs at the same time causes traffic jams. |
| **Preparing backups** | Keep in mind the time needed to prepare the backup. The preparation time includes installing or updating the backup extension and triggering a snapshot according to the backup schedule. |
| **Data transfer** | Consider the time needed for Azure Backup to identify the incremental changes from the previous backup.  In an incremental backup, Azure Backup determines the changes by calculating the checksum of the block. If a block is changed, it's marked for transfer to the vault. The service analyzes the identified blocks to attempt to further minimize the amount of data to transfer. After evaluating all the changed blocks, Azure Backup transfers the changes to the vault.  There might be a lag between taking the snapshot and copying it to vault.  At peak times, it can take up to eight hours for backups to be processed. The backup time for a VM will be less than 24 hours for the daily backup. |
| **Initial backup** | Although the total backup time for incremental backups is less than 24 hours, that might not be the case for the first backup. The time needed for the initial backup will depend on the size of the data and when the backup is processed. |
| **Restore queue** | Azure Backup processes restore jobs from multiple storage accounts at the same time, and it puts restore requests in a queue. |
| **Restore copy** | During the restore process, data is copied from the vault to the storage account.  The total restore time depends on the I/O operations per second (IOPS) and the throughput of the storage account.  To reduce the copy time, select a storage account that isn't loaded with other application writes and reads. |

### Backup performance

These common scenarios can affect the total backup time:

* **Adding a new disk to a protected Azure VM:** If a VM is undergoing incremental backup and a new disk is added, the backup time will increase. The total backup time might last more than 24 hours because of initial replication of the new disk, along with delta replication of existing disks.
* **Fragmented disks:** Backup operations are faster when disk changes are contiguous. If changes are spread out and fragmented across a disk, backup will be slower.
* **Disk churn:** If protected disks that are undergoing incremental backup have a daily churn of more than 200 GB, backup can take a long time (more than eight hours) to complete.
* **Backup versions:** The latest version of Backup (known as the Instant Restore version) uses a more optimized process than checksum comparison for identifying changes. But if you're using Instant Restore and have deleted a backup snapshot, the backup switches to checksum comparison. In this case, the backup operation will exceed 24 hours (or fail).

## Best practices

When you're configuring VM backups, we suggest following these practices:

* Modify the default schedule times that are set in a policy. For example, if the default time in the policy is 12:00 AM, increment the timing by several minutes so that resources are optimally used.
* If you're restoring VMs from a single vault, we highly recommend that you use different [general-purpose v2 storage accounts](https://docs.microsoft.com/azure/storage/common/storage-account-upgrade) to ensure that the target storage account doesn’t get throttled. For example, each VM must have a different storage account. For example, if 10 VMs are restored, use 10 different storage accounts.
* For backup of VMs that are using premium storage, with Instant Restore, we recommend allocating 50% free space of the total allocated storage space, which is required **only** for the first backup. The 50% free space is not a requirement for backups after the first backup is complete
* The restores from a general-purpose v1 storage layer (snapshot) will be completed in minutes because the snapshot is in the same storage account. Restores from the general-purpose v2 storage layer (vault) can take hours. In cases where the data is available in general-purpose v1 storage, we recommend that you use the [Instant Restore](https://docs.microsoft.com/en-us/azure/backup/backup-instant-restore-capability) feature for faster restores. (If the data must be restored from a vault, then it will take more time.)
* The limit on the number of disks per storage account is relative to how heavily the disks are being accessed by applications that are running on an infrastructure as a service (IaaS) VM. As a general practice, if 5 to 10 disks or more are present on a single storage account, balance the load by moving some disks to separate storage accounts.

## Backup costs

Azure VMs backed up with Azure Backup are subject to [Azure Backup pricing](https://azure.microsoft.com/pricing/details/backup/).

Billing doesn't start until the first successful backup finishes. At this point, the billing for both storage and protected VMs begins. Billing continues as long as any backup data for the VM is stored in a vault. If you stop protection for a VM, but backup data for the VM exists in a vault, billing continues.

Billing for a specified VM stops only if the protection is stopped and all backup data is deleted. When protection stops and there are no active backup jobs, the size of the last successful VM backup becomes the protected instance size used for the monthly bill.

The protected-instance size calculation is based on the actual size of the VM. The VM's size is the sum of all the data in the VM, excluding the temporary storage. Pricing is based on the actual data that's stored on the data disks, not on the maximum supported size for each data disk that's attached to the VM.

Similarly, the backup storage bill is based on the amount of data that's stored in Azure Backup, which is the sum of the actual data in each recovery point.

For example, take an A2-Standard-sized VM that has two additional data disks with a maximum size of 4 TB each. The following table shows the actual data stored on each of these disks:

| **Disk** | **Max size** | **Actual data present** |
| --- | --- | --- |
| OS disk | 4095 GB | 17 GB |
| Local/temporary disk | 135 GB | 5 GB (not included for backup) |
| Data disk 1 | 4095 GB | 30 GB |
| Data disk 2 | 4095 GB | 0 GB |

The actual size of the VM in this case is 17 GB + 30 GB + 0 GB = 47 GB. This protected-instance size (47 GB) becomes the basis for the monthly bill. As the amount of data in the VM grows, the protected-instance size used for billing changes to match.