Azure Managed Disks Overview

Azure Managed Disks simplifies disk management for Azure IaaS VMs by managing the [storage accounts](https://docs.microsoft.com/en-in/azure/storage/common/storage-introduction) associated with the VM disks. You only have to specify the type ([Premium](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/premium-storage) or [Standard](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/standard-storage)) and the size of disk you need, and Azure creates and manages the disk for you.

Benefits of managed disks

Let's take a look at some of the benefits you gain by using managed disks, starting with this Channel 9 video, [Better Azure VM Resiliency with Managed Disks](https://channel9.msdn.com/Blogs/Azure/Managed-Disks-for-Azure-Resiliency). 

Simple and scalable VM deployment

Managed Disks handles storage for you behind the scenes. Previously, you had to create storage accounts to hold the disks (VHD files) for your Azure VMs. When scaling up, you had to make sure you created additional storage accounts so you didn't exceed the IOPS limit for storage with any of your disks. With Managed Disks handling storage, you are no longer limited by the storage account limits (such as 20,000 IOPS / account). You also no longer have to copy your custom images (VHD files) to multiple storage accounts. You can manage them in a central location – one storage account per Azure region – and use them to create hundreds of VMs in a subscription.

Managed Disks will allow you to create up to 10,000 VM **disks** in a subscription, which will enable you to create thousands of **VMs** in a single subscription. This feature also further increases the scalability of [Virtual Machine Scale Sets (VMSS)](https://docs.microsoft.com/en-in/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-overview) by allowing you to create up to a thousand VMs in a VMSS using a Marketplace image.

Better reliability for Availability Sets

Managed Disks provides better reliability for Availability Sets by ensuring that the disks of [VMs in an Availability Set](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/manage-availability#use-managed-disks-for-vms-in-an-availability-set) are sufficiently isolated from each other to avoid single points of failure. It does this by automatically placing the disks in different storage scale units (stamps). If a stamp fails due to hardware or software failure, only the VM instances with disks on those stamps fail. For example, let's say you have an application running on five VMs, and the VMs are in an Availability Set. The disks for those VMs won't all be stored in the same stamp, so if one stamp goes down, the other instances of the application continue to run.

Highly durable and available

Azure Disks are designed for 99.999% availability. Rest easier knowing that you have three replicas of your data that enables high durability. If one or even two replicas experience issues, the remaining replicas help ensure persistence of your data and high tolerance against failures. This architecture has helped Azure consistently deliver enterprise-grade durability for IaaS disks, with an industry-leading ZERO% Annualized Failure Rate.

Granular access control

You can use [Azure Role-Based Access Control (RBAC)](https://docs.microsoft.com/en-in/azure/active-directory/role-based-access-control-what-is) to assign specific permissions for a managed disk to one or more users. Managed Disks exposes a variety of operations, including read, write (create/update), delete, and retrieving a [shared access signature (SAS) URI](https://docs.microsoft.com/en-in/azure/storage/common/storage-dotnet-shared-access-signature-part-1) for the disk. You can grant access to only the operations a person needs to perform his job. For example, if you don't want a person to copy a managed disk to a storage account, you can choose not to grant access to the export action for that managed disk. Similarly, if you don't want a person to use an SAS URI to copy a managed disk, you can choose not to grant that permission to the managed disk.

Azure Backup service support

Use Azure Backup service with Managed Disks to create a backup job with time-based backups, easy VM restoration and backup retention policies. Managed Disks only support Locally Redundant Storage (LRS) as the replication option; this means it keeps three copies of the data within a single region. For regional disaster recovery, you must backup your VM disks in a different region using [Azure Backup service](https://docs.microsoft.com/en-in/azure/backup/backup-introduction-to-azure-backup) and a GRS storage account as backup vault. Currently Azure Backup supports data disk sizes up to 1TB for backup. Read more about this at [Using Azure Backup service for VMs with Managed Disks](https://docs.microsoft.com/en-in/azure/backup/backup-introduction-to-azure-backup#using-managed-disk-vms-with-azure-backup).

Pricing and Billing

When using Managed Disks, the following billing considerations apply:

* Storage Type
* Disk Size
* Number of transactions
* Outbound data transfers
* Managed Disk Snapshots (full disk copy)

Let's take a closer look at these.

**Storage Type:** Managed Disks offers 2 performance tiers: [Premium](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/premium-storage) (SSD-based) and [Standard](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/standard-storage)(HDD-based). The billing of a managed disk depends on which type of storage you have selected for the disk.

**Disk Size**: Billing for managed disks depends on the provisioned size of the disk. Azure maps the provisioned size (rounded up) to the nearest Managed Disks option as specified in the tables below. Each managed disk maps to one of the supported provisioned sizes and is billed accordingly. For example, if you create a standard managed disk and specify a provisioned size of 200 GB, you are billed as per the pricing of the S20 Disk type.

Here are the disk sizes available for a premium managed disk:

| **Premium Managed  Disk Type** | **P4** | **P6** | **P10** | **P20** | **P30** | **P40** | **P50** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Disk Size | 32 GB | 64 GB | 128 GB | 512 GB | 1024 GB (1 TB) | 2048 GB (2 TB) | 4095 GB (4 TB) |

Here are the disk sizes available for a standard managed disk:

| **Standard Managed  Disk Type** | **S4** | **S6** | **S10** | **S20** | **S30** | **S40** | **S50** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Disk Size | 32 GB | 64 GB | 128 GB | 512 GB | 1024 GB (1 TB) | 2048 GB (2 TB) | 4095 GB (4 TB) |

**Number of transactions**: You are billed for the number of transactions that you perform on a standard managed disk. There is no cost for transactions for a premium managed disk.

**Outbound data transfers**: [Outbound data transfers](https://azure.microsoft.com/pricing/details/data-transfers/) (data going out of Azure data centers) incur billing for bandwidth usage.

For detailed information on pricing for Managed Disks, see [Managed Disks Pricing](https://azure.microsoft.com/pricing/details/managed-disks).

Managed Disk Snapshots

A Managed Snapshot is a read-only full copy of a managed disk which is stored as a standard managed disk by default. With snapshots, you can back up your managed disks at any point in time. These snapshots exist independent of the source disk and can be used to create new Managed Disks. They are billed based on the used size. For example, if you create a snapshot of a managed disk with provisioned capacity of 64 GB and actual used data size of 10 GB, snapshot will be billed only for the used data size of 10 GB.

[Incremental snapshots](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/incremental-snapshots) are currently not supported for Managed Disks, but will be supported in the future.

To learn more about how to create snapshots with Managed Disks, please check out these resources:

* [Create copy of VHD stored as a Managed Disk using Snapshots in Windows](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/snapshot-copy-managed-disk)
* [Create copy of VHD stored as a Managed Disk using Snapshots in Linux](https://docs.microsoft.com/en-in/azure/virtual-machines/linux/snapshot-copy-managed-disk)

Images

Managed Disks also support creating a managed custom image. You can create an image from your custom VHD in a storage account or directly from a generalized (sys-prepped) VM. This captures in a single image all managed disks associated with a VM, including both the OS and data disks. This enables creating hundreds of VMs using your custom image without the need to copy or manage any storage accounts.

For information on creating images, please check out the following articles:

* [How to capture a managed image of a generalized VM in Azure](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/capture-image-resource)
* [How to generalize and capture a Linux virtual machine using the Azure CLI 2.0](https://docs.microsoft.com/en-in/azure/virtual-machines/linux/capture-image)

Images versus snapshots

You often see the word "image" used with VMs, and now you see "snapshots" as well. It's important to understand the difference between these. With Managed Disks, you can take an image of a generalized VM that has been deallocated. This image will include all of the disks attached to the VM. You can use this image to create a new VM, and it will include all of the disks.

A snapshot is a copy of a disk at the point in time it is taken. It only applies to one disk. If you have a VM that only has one disk (the OS), you can take a snapshot or an image of it and create a VM from either the snapshot or the image.

What if a VM has five disks and they are striped? You could take a snapshot of each of the disks, but there is no awareness within the VM of the state of the disks – the snapshots only know about that one disk. In this case, the snapshots would need to be coordinated with each other, and that is not currently supported.

Managed Disks and Encryption

There are two kinds of encryption to discuss in reference to managed disks. The first one is Storage Service Encryption (SSE), which is performed by the storage service. The second one is Azure Disk Encryption, which you can enable on the OS and data disks for your VMs.

Storage Service Encryption (SSE)

[Azure Storage Service Encryption](https://docs.microsoft.com/en-in/azure/storage/common/storage-service-encryption) provides encryption-at-rest and safeguard your data to meet your organizational security and compliance commitments. SSE is enabled by default for all Managed Disks, Snapshots and Images in all the regions where managed disks is available. Starting June 10th, 2017, all new managed disks/snapshots/images and new data written to existing managed disks are automatically encrypted-at-rest with keys managed by Microsoft. Visit the [Managed Disks FAQ page](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/faq-for-disks#managed-disks-and-storage-service-encryption) for more details.

Azure Disk Encryption (ADE)

Azure Disk Encryption allows you to encrypt the OS and Data disks used by an IaaS Virtual Machine. This includes managed disks. For Windows, the drives are encrypted using industry-standard BitLocker encryption technology. For Linux, the disks are encrypted using the DM-Crypt technology. This is integrated with Azure Key Vault to allow you to control and manage the disk encryption keys. For more information, please see [Azure Disk Encryption for Windows and Linux IaaS VMs](https://docs.microsoft.com/en-in/azure/security/azure-security-disk-encryption).