Contents

Introduction to Azure Storage

2/12/2020 • 12 minutes to read • Edit Online

Azure Storage is Microsoft's cloud storage solution for modern data storage scenarios. Azure Storage offers a massively scalable object store for data objects, a file system service for the cloud, a messaging store for reliable messaging, and a NoSQL store. Azure Storage is:

- **Durable and highly available.** Redundancy ensures that your data is safe in the event of transient hardware failures. You can also opt to replicate data across datacenters or geographical regions for additional protection from local catastrophe or natural disaster. Data replicated in this way remains highly available in the event of an unexpected outage.
- **Secure.** All data written to Azure Storage is encrypted by the service. Azure Storage provides you with fine-grained control over who has access to your data.
- **Scalable.** Azure Storage is designed to be massively scalable to meet the data storage and performance needs of today's applications.
- **Managed.** Microsoft Azure handles hardware maintenance, updates, and critical issues for you.
- **Accessible.** Data in Azure Storage is accessible from anywhere in the world over HTTP or HTTPS. Microsoft provides client libraries for Azure Storage in a variety of languages, including .NET, Java, Node.js, Python, PHP, Ruby, Go, and others, as well as a mature REST API. Azure Storage supports scripting in Azure PowerShell or Azure CLI. And the Azure portal and Azure Storage Explorer offer easy visual solutions for working with your data.

Azure Storage services

Azure Storage includes these data services:

- Azure Blobs: A massively scalable object store for text and binary data.
- Azure Files: Managed file shares for cloud or on-premises deployments.
- Azure Queues: A messaging store for reliable messaging between application components.
- Azure Tables: A NoSQL store for schemaless storage of structured data.

Each service is accessed through a storage account. To get started, see Create a storage account.

Blob storage

Azure Blob storage is Microsoft's object storage solution for the cloud. Blob storage is optimized for storing massive amounts of unstructured data, such as text or binary data.

Blob storage is ideal for:

- Serving images or documents directly to a browser.
- Storing files for distributed access.
- Streaming video and audio.
- Storing data for backup and restore, disaster recovery, and archiving.
- Storing data for analysis by an on-premises or Azure-hosted service.

Objects in Blob storage can be accessed from anywhere in the world via HTTP or HTTPS. Users or client applications can access blobs via URLs, the Azure Storage REST API, Azure PowerShell, Azure CLI, or an Azure Storage client library. The storage client libraries are available for multiple languages, including .NET, Java, Node.js, Python, PHP, and Ruby.

For more information about Blob storage, see Introduction to Blob storage.

Azure Files

Azure Files enables you to set up highly available network file shares that can be accessed by using the standard Server Message Block (SMB) protocol. That means that multiple VMs can share the same files with both read and write access. You can also read the files using the REST interface or the storage client libraries.

One thing that distinguishes Azure Files from files on a corporate file share is that you can access the files from anywhere in the world using a URL that points to the file and includes a shared access signature (SAS) token. You can generate SAS tokens; they allow specific access to a private asset for a specific amount of time.

File shares can be used for many common scenarios:

- Many on-premises applications use file shares. This feature makes it easier to migrate those applications that share data to Azure. If you mount the file share to the same drive letter that the on-premises application uses, the part of your application that accesses the file share should work with minimal, if any, changes.
- Configuration files can be stored on a file share and accessed from multiple VMs. Tools and utilities used by multiple developers in a group can be stored on a file share, ensuring that everybody can find them, and that they use the same version.
- Diagnostic logs, metrics, and crash dumps are just three examples of data that can be written to a file share and processed or analyzed later.

At this time, Active Directory-based authentication and access control lists (ACLs) are not supported, but they will be at some time in the future. The storage account credentials are used to provide authentication for access to the file share. This means anybody with the share mounted will have full read/write access to the share.

For more information about Azure Files, see Introduction to Azure Files.

Queue storage

The Azure Queue service is used to store and retrieve messages. Queue messages can be up to 64 KB in size, and a queue can contain millions of messages. Queues are generally used to store lists of messages to be processed asynchronously.

For example, say you want your customers to be able to upload pictures, and you want to create thumbnails for each picture. You could have your customer wait for you to create the thumbnails while uploading the pictures. An alternative would be to use a queue. When the customer finishes their upload, write a message to the queue. Then have an Azure Function retrieve the message from the queue and create the thumbnails. Each of the parts of this processing can be scaled separately, giving you more control when tuning it for your usage.

For more information about Azure Queues, see Introduction to Queues.

Table storage

Azure Table storage is now part of Azure Cosmos DB. To see Azure Table storage documentation, see the Azure Table Storage Overview. In addition to the existing Azure Table storage service, there is a new Azure Cosmos DB Table API offering that provides throughput-optimized tables, global distribution, and automatic secondary indexes. To learn more and try out the new premium experience, please check out Azure Cosmos DB Table API.

For more information about Table storage, see Overview of Azure Table storage.

Disk storage

An Azure managed disk is a virtual hard disk (VHD). You can think of it like a physical disk in an on-premises server but, virtualized. Azure managed disks are stored as page blobs, which are a random IO storage object in Azure. We call a managed disk 'managed' because it is an abstraction over page blobs, blob containers, and Azure storage accounts. With managed disks, all you have to do is provision the disk, and Azure takes care of the rest.

For more information about managed disks, see Introduction to Azure managed disks.

Types of storage accounts

Azure Storage offers several types of storage accounts. Each type supports different features and has its own pricing model. Consider these differences before you create a storage account to determine the type of account that is best for your applications. The types of storage accounts are:

- **General-purpose v2 accounts**: Basic storage account type for blobs, files, queues, and tables. Recommended for most scenarios using Azure Storage.
- **General-purpose v1 accounts**: Legacy account type for blobs, files, queues, and tables. Use general-purpose v2 accounts instead when possible.
- **BlockBlobStorage accounts**: Storage accounts with premium performance characteristics for block blobs and append blobs. Recommended for scenarios with high transactions rates, or scenarios that use smaller objects or require consistently low storage latency.
- **FileStorage accounts**: Files-only storage accounts with premium performance characteristics. Recommended for enterprise or high performance scale applications.
- **BlobStorage accounts**: Legacy Blob-only storage accounts. Use general-purpose v2 accounts instead when possible.

The following table describes the types of storage accounts and their capabilities:

STORAGE ACCOUNT TYPE	SUPPORTED SERVICES	SUPPORTED PERFORMANCE TIERS	SUPPORTED ACCESS TIERS	REPLICATION OPTIONS	DEPLOYMENT MODEL [1]	ENCRYPTION [2]
General-purpose V2	Blob, File, Queue, Table, Disk, and Data Lake Gen2 [6]	Standard, Premium [5]	Hot, Cool, Archive [3]	LRS, GRS, RA-GRS, ZRS, GZRS (preview), RA-GZRS (preview) [4]	Resource Manager	Encrypted
General-purpose V1	Blob, File, Queue, Table, and Disk	Standard, Premium [5]	N/A	LRS, GRS, RA-GRS	Resource Manager, Classic	Encrypted
BlockBlobStorage	Blob (block blobs and append blobs only)	Premium	N/A	LRS, ZRS [4]	Resource Manager	Encrypted
FileStorage	File only	Premium	N/A	LRS, ZRS [4]	Resource Manager	Encrypted
BlobStorage	Blob (block blobs and append blobs only)	Standard	Hot, Cool, Archive [3]	LRS, GRS, RA-GRS	Resource Manager	Encrypted

[1] Using the Azure Resource Manager deployment model is recommended. Storage accounts using the classic deployment model can still be created in some locations, and existing classic accounts continue to be supported. For

more information, see Azure Resource Manager vs. classic deployment: Understand deployment models and the state of your resources.

[2] All storage accounts are encrypted using Storage Service Encryption (SSE) for data at rest. For more information, see Azure Storage Service Encryption for Data at Rest.

[3] The Archive tier is available at level of an individual blob only, not at the storage account level. Only block blobs and append blobs can be archived. For more information, see Azure Blob storage: Hot, Cool, and Archive storage tiers.

[4] Zone-redundant storage (ZRS) and geo-zone-redundant storage (GZRS/RA-GZRS) (preview) are available only for standard general-purpose V2, BlockBlobStorage, and FileStorage accounts in certain regions. For more information about Azure Storage redundancy options, see Azure Storage redundancy.

[5] Premium performance for general-purpose v2 and general-purpose v1 accounts is available for disk and page blob only. Premium performance for block or append blobs are only available on BlockBlobStorage accounts. Premium performance for files are only available on FileStorage accounts.

[6] Azure Data Lake Storage Gen2 is a set of capabilities dedicated to big data analytics, built on Azure Blob storage. Data Lake Storage Gen2 is only supported on General-purpose V2 storage accounts with Hierarchical namespace enabled. For more information on Data Lake Storage Gen2, see Introduction to Azure Data Lake Storage Gen2.

For more information about storage account types, see Azure storage account overview.

Securing access to storage accounts

Every request to Azure Storage must be authorized. Azure Storage supports the following authorization methods:

- **Azure Active Directory (Azure AD) integration for blob and queue data.** Azure Storage supports authentication and authorization with Azure AD for the Blob and Queue services via role-based access control (RBAC). Authorizing requests with Azure AD is recommended for superior security and ease of use. For more information, see Authorize access to Azure blobs and queues using Azure Active Directory.
- **Azure AD authorization over SMB for Azure Files (preview).** Azure Files supports identity-based authorization over SMB (Server Message Block) through Azure Active Directory Domain Services. Your domain-joined Windows virtual machines (VMs) can access Azure file shares using Azure AD credentials. For more information, see Overview of Azure Active Directory authorization over SMB for Azure Files (preview).
- **Authorization with Shared Key.** The Azure Storage Blob, Queue, and Table services and Azure Files support authorization with Shared Key.A client using Shared Key authorization passes a header with every request that is signed using the storage account access key. For more information, see Authorize with Shared Key.
- **Authorization using shared access signatures (SAS).** A shared access signature (SAS) is a string containing a security token that can be appended to the URI for a storage resource. The security token encapsulates constraints such as permissions and the interval of access. For more information, refer to Using Shared Access Signatures (SAS).
- **Anonymous access to containers and blobs.** A container and its blobs may be publicly available. When you specify that a container or blob is public, anyone can read it anonymously; no authentication is required. For more information, see Manage anonymous read access to containers and blobs

Encryption

There are two basic kinds of encryption available for the Storage services. For more information about security and encryption, see the Azure Storage security guide.

Encryption at rest

Azure Storage encryption protects and safeguards your data to meet your organizational security and compliance commitments. Azure Storage automatically encrypts all data prior to persisting to the storage account and decrypts it prior to retrieval. The encryption, decryption, and key management processes are totally transparent to users. Customers can also choose to manage their own keys using Azure Key Vault. For more information, see Azure Storage encryption for data at rest.

Client-side encryption

The Azure Storage client libraries provide methods for encrypting data from the client library before sending it across the wire and decrypting the response. Data encrypted via client-side encryption is also encrypted at rest by Azure Storage. For more information about client-side encryption, see Client-side encryption with .NET for Azure Storage.

Redundancy

In order to ensure that your data is durable, Azure Storage stores multiple copies of your data. When you set up your storage account, you select a redundancy option.

Redundancy options for a storage account include:

- Locally redundant storage (LRS): A simple, low-cost redundancy strategy. Data is copied synchronously three times within the primary region.
- Zone-redundant storage (ZRS): Redundancy for scenarios requiring high availability. Data is copied synchronously across three Azure availability zones in the primary region.
- Geo-redundant storage (GRS): Cross-regional redundancy to protect against regional outages. Data is copied synchronously three times in the primary region, then copied asynchronously to the secondary region. For read access to data in the secondary region, enable read-access geo-redundant storage (RA-GRS).
- Geo-zone-redundant storage (GZRS) (preview): Redundancy for scenarios requiring both high availability and maximum durability. Data is copied synchronously across three Azure availability zones in the primary region, then copied asynchronously to the secondary region. For read access to data in the secondary region, enable read-access geo-zone-redundant storage (RA-GZRS).

For more information about redundancy options in Azure Storage, see Azure Storage redundancy.

Transferring data to and from Azure Storage

You have several options for moving data into or out of Azure Storage. Which option you choose depends on the size of your dataset and your network bandwidth. For more information, see Choose an Azure solution for data transfer.

Pricing

For detailed information about pricing for Azure Storage, see the Pricing page.

Storage APIs, libraries, and tools

Azure Storage resources can be accessed by any language that can make HTTP/HTTPS requests. Additionally, Azure Storage offers programming libraries for several popular languages. These libraries simplify many aspects of working with Azure Storage by handling details such as synchronous and asynchronous invocation, batching of operations, exception management, automatic retries, operational behavior, and so forth. Libraries are currently available for the following languages and platforms, with others in the pipeline:

Azure Storage data API and library references

- Azure Storage REST API
- Azure Storage client library for .NET
- Azure Storage client library for Java/Android
- Azure Storage client library for Node.js
- Azure Storage client library for Python
- Azure Storage client library for PHP
- Azure Storage client library for Ruby
- Azure Storage client library for C++

Azure Storage management API and library references

- Storage Resource Provider REST API
- Storage Resource Provider Client Library for .NET
- Storage Service Management REST API (Classic)

Azure Storage data movement API and library references

- Storage Import/Export Service REST API
- Storage Data Movement Client Library for .NET

Tools and utilities

- Azure PowerShell Cmdlets for Storage
- Azure CLI Cmdlets for Storage
- AzCopy Command-Line Utility
- Azure Storage Explorer is a free, standalone app from Microsoft that enables you to work visually with Azure Storage data on Windows, macOS, and Linux.
- Azure Storage Client Tools
- Azure Developer Tools

Next steps

To get up and running with Azure Storage, see Create a storage account.

Deciding when to use Azure Blobs, Azure Files, or Azure Disks

9/29/2019 • 2 minutes to read • Edit Online

Microsoft Azure provides several features in Azure Storage for storing and accessing your data in the cloud. This article covers Azure Files, Blobs, and Disks, and is designed to help you choose between these features.

Scenarios

The following table compares Files, Blobs, and Disks, and shows example scenarios appropriate for each.

FEATURE	DESCRIPTION	WHEN TO USE
Azure Files	Provides an SMB interface, client libraries, and a REST interface that allows access from anywhere to stored files.	You want to "lift and shift" an application to the cloud which already uses the native file system APIs to share data between it and other applications running in Azure. You want to store development and debugging tools that need to be accessed from many virtual machines.
Azure Blobs	Provides client libraries and a REST interface that allows unstructured data to be stored and accessed at a massive scale in block blobs. Also supports Azure Data Lake Storage Gen2 for enterprise big data analytics solutions.	You want your application to support streaming and random access scenarios. You want to be able to access application data from anywhere. You want to build an enterprise data lake on Azure and perform big data analytics.
Azure Disks	Provides client libraries and a REST interface that allows data to be persistently stored and accessed from an attached virtual hard disk.	You want to lift and shift applications that use native file system APIs to read and write data to persistent disks. You want to store data that is not required to be accessed from outside the virtual machine to which the disk is attached.

Next steps

When making decisions about how your data is stored and accessed, you should also consider the costs involved. For more information, see Azure Storage Pricing.

Some SMB features are not applicable to the cloud. For more information, see Features not supported by the Azure File service.

For more information about Azure Blobs, see our article, What is Azure Blob storage?.

For more information about Disk Storage, see our Introduction to managed disks.

For more information about Azure Files, see our article, Planning for an Azure Files deployment.

Introduction to Azure managed disks

12/16/2019 • 9 minutes to read • Edit Online

Azure managed disks are block-level storage volumes that are managed by Azure and used with Azure Virtual Machines. Managed disks are like a physical disk in an on-premises server but virtualized. With managed disks, all you have to do is specify the disk size, the disk type, and provision the disk. Once you provision the disk, Azure handles the rest.

The available types of disks are ultra disks, premium solid-state drives (SSD), standard SSDs, and standard hard disk drives (HDD). For information about each individual disk type, see Select a disk type for IaaS VMs.

Benefits of managed disks

Let's go over some of the benefits you gain by using managed disks.

Highly durable and available

Managed disks are designed for 99.999% availability. Managed disks achieve this by providing you with three replicas of your data, allowing for 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 infrastructure as a service (IaaS) disks, with an industry-leading ZERO% annualized failure rate.

Simple and scalable VM deployment

Using managed disks, you can create up to 50,000 VM **disks** of a type in a subscription per region, allowing you to create thousands of **VMs** in a single subscription. This feature also further increases the scalability of virtual machine scale sets by allowing you to create up to 1,000 VMs in a virtual machine scale set using a Marketplace image.

Integration with availability sets

Managed disks are integrated with availability sets to ensure that the disks of VMs in an availability set are sufficiently isolated from each other to avoid a single point of failure. Disks are automatically placed 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.

Integration with Availability Zones

Managed disks support Availability Zones, which is a high-availability offering that protects your applications from datacenter failures. Availability Zones are unique physical locations within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. To ensure resiliency, there’s a minimum of three separate zones in all enabled regions. With Availability Zones, Azure offers industry best 99.99% VM uptime SLA.

Azure Backup support

To protect against regional disasters, Azure Backup can be used to create a backup job with time-based backups and backup retention policies. This allows you to perform easy VM restorations at will. Currently Azure Backup supports disk sizes up to four tebibyte (TiB) disks. Azure Backup supports backup and restore of managed disks. Learn more about Azure VM backup support.

Granular access control

You can use Azure role-based access control (RBAC) to assign specific permissions for a managed disk to one or more users. Managed disks expose a variety of operations, including read, write (create/update), delete, and retrieving a shared access signature (SAS) URI for the disk. You can grant access to only the operations a person needs to perform their 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.

Upload your vhd

Direct upload makes it easy to transfer your vhd to an Azure managed disk. Previously, you had to follow a more involved process that included staging your data in a storage account. Now, there are fewer steps. It is easier to upload on premises VMs to Azure, upload to large managed disks, and the backup and restore process is simplified. It also reduces cost by allowing you to upload data to managed disks directly without attaching them to VMs. You can use direct upload to upload vhds up to 32 TiB in size.

To learn how to transfer your vhd to Azure, see the CLI or PowerShell articles.

Encryption

Managed disks offer two different kinds of encryption. The first is Server Side Encryption (SSE), which is performed by the storage service. The second one is Azure Disk Encryption (ADE), which you can enable on the OS and data disks for your VMs.

Server-side encryption

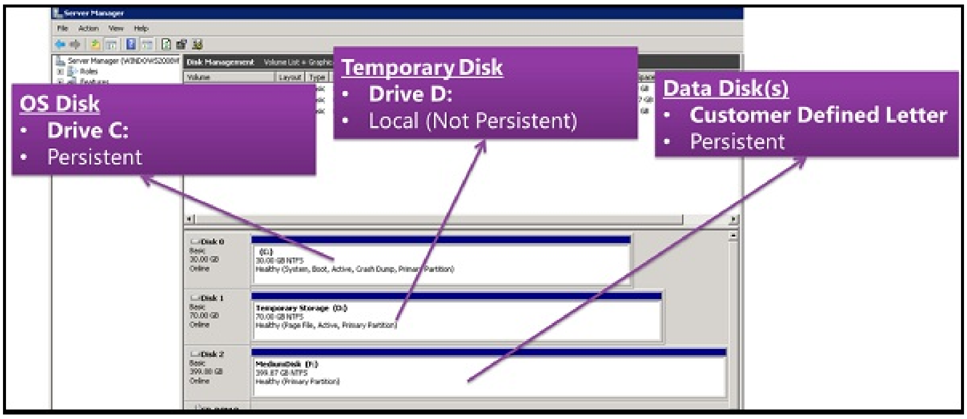
Azure Server-side Encryption provides encryption-at-rest and safeguards your data to meet your organizational security and compliance commitments. Server-side encryption is enabled by default for all managed disks, snapshots, and images in all the regions where managed disks are available. You can either allow Azure to manage your keys for you, these are platform-managed keys, or you can manage the keys yourself, these are customer-managed keys. Visit the Managed Disks FAQ page for more details.

Azure Disk Encryption

Azure Disk Encryption allows you to encrypt the OS and Data disks used by an IaaS Virtual Machine. This encryption 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. The encryption process is integrated with Azure Key Vault to allow you to control and manage the disk encryption keys. For more information, see Azure Disk Encryption for IaaS VMs.

Disk roles

There are three main disk roles in Azure: the data disk, the OS disk, and the temporary disk. These roles map to disks that are attached to your virtual machine.



Data disk

A data disk is a managed disk that's attached to a virtual machine to store application data, or other data you need to keep. Data disks are registered as SCSI drives and are labeled with a letter that you choose. Each data disk has a maximum capacity of 32,767 gibibytes (GiB). The size of the virtual machine determines how many data disks you can attach to it and the type of storage you can use to host the disks.

OS disk

Every virtual machine has one attached operating system disk. That OS disk has a pre-installed OS, which was selected when the VM was created. This disk contains the boot volume.

This disk has a maximum capacity of 2,048 GiB.

Temporary disk

Every VM contains a temporary disk, which is not a managed disk. The temporary disk provides short-term storage for applications and processes and is intended to only store data such as page or swap files. Data on the temporary disk may be lost during a maintenance event event or when you redeploy a VM. On Azure Linux VMs, the temporary disk is /dev/sdb by default and on Windows VMs the temporary disk is D: by default. During a successful standard reboot of the VM, the data on the temporary disk will persist.

Managed disk snapshots

A managed disk snapshot is a read-only crash-consistent full copy of a managed disk that 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.

Snapshots are billed based on the used size. For example, if you create a snapshot of a managed disk with provisioned capacity of 64 GiB and actual used data size of 10 GiB, that snapshot is billed only for the used data size of 10 GiB. You can see the used size of your snapshots by looking at the Azure usage report. For example, if the used data size of a snapshot is 10 GiB, the **daily** usage report will show 10 GiB/(31 days) = 0.3226 as the consumed quantity.

To learn more about how to create snapshots for managed disks, see the following resources:

- Create a snapshot of a managed disk in Windows
- Create a snapshot of a managed disk in Linux

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 (sysprepped) VM. This process captures a single image. This image contains all managed disks associated with a VM, including both the OS and data disks. This managed custom image enables creating hundreds of VMs using your custom image without the need to copy or manage any storage accounts.

For information on creating images, see the following articles:

- How to capture a managed image of a generalized VM in Azure
- How to generalize and capture a Linux virtual machine using the Azure CLI

Images versus snapshots

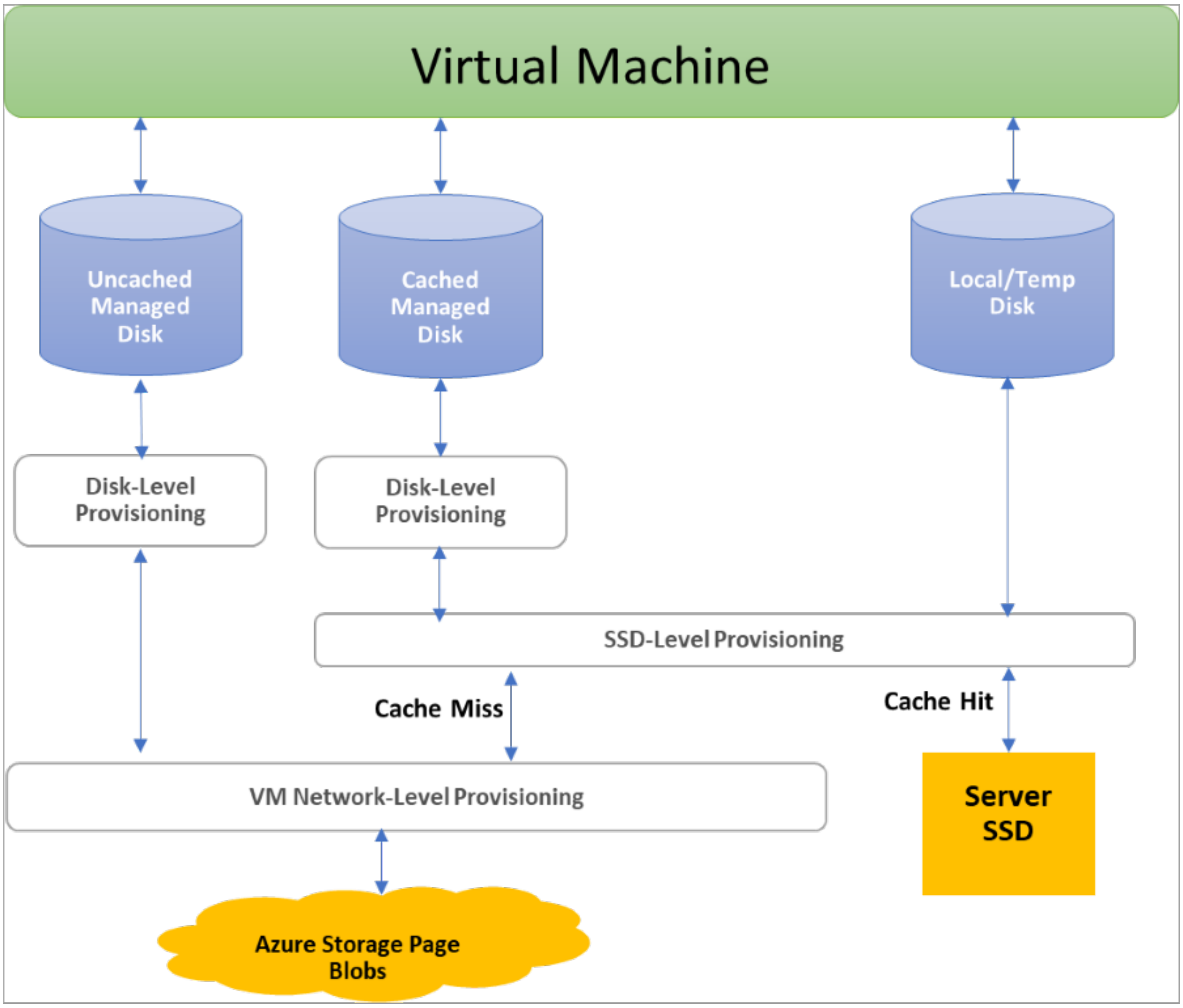
It's important to understand the difference between images and snapshots. With managed disks, you can take an image of a generalized VM that has been deallocated. This image includes all of the disks attached to the VM. You can use this image to create a VM, and it includes all of the disks.

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

A snapshot doesn't have awareness of any disk except the one it contains. This makes it problematic to use in scenarios that require the coordination of multiple disks, such as striping. Snapshots would need to be able to coordinate with each other and this is currently not supported.

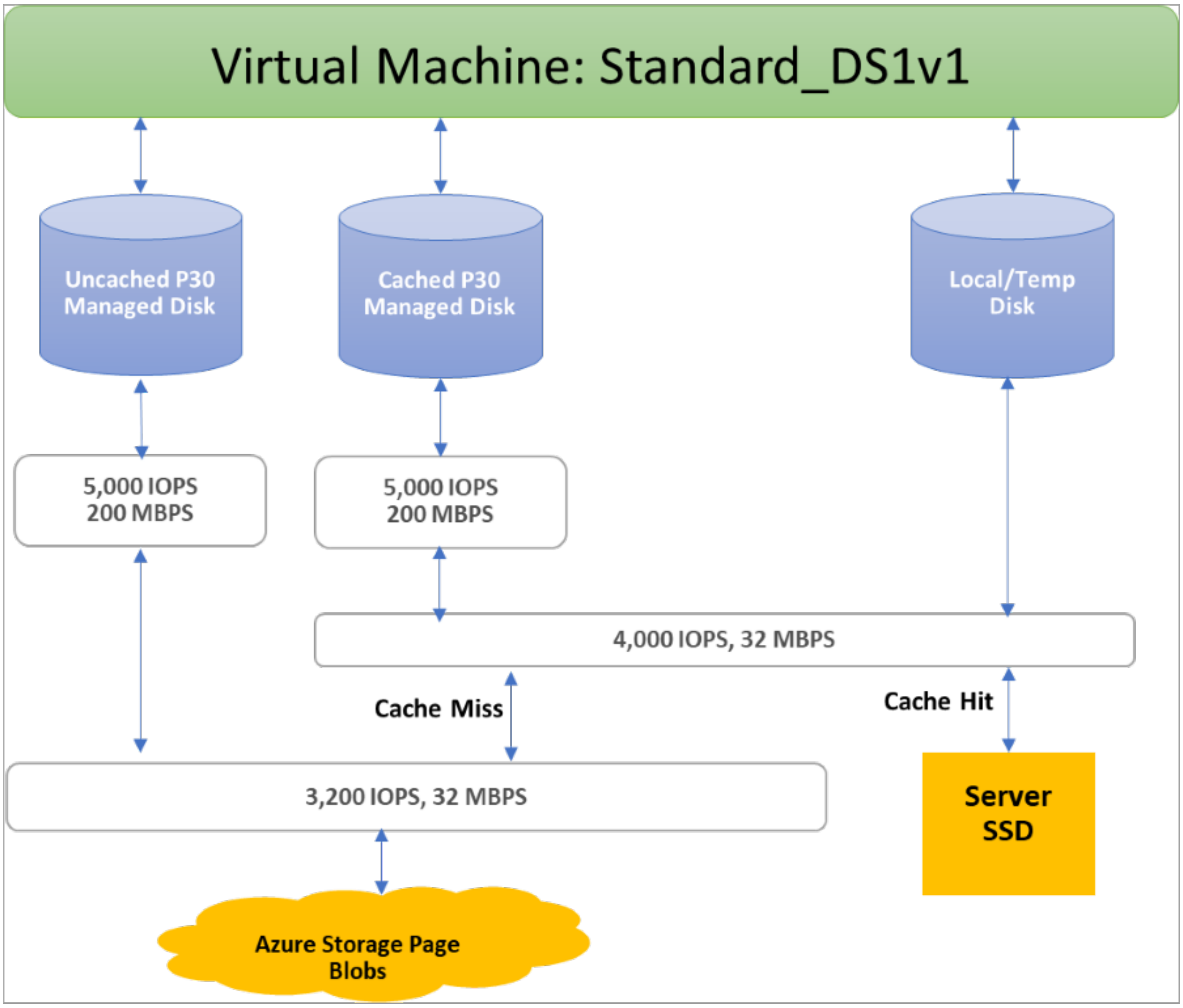
Disk allocation and performance

The following diagram depicts real-time allocation of bandwidth and IOPS for disks, using a three-level provisioning system:



The first level provisioning sets the per-disk IOPS and bandwidth assignment. At the second level, compute server host implements SSD provisioning, applying it only to data that is stored on the server's SSD, which includes disks with caching (ReadWrite and ReadOnly) as well as local and temp disks. Finally, VM network provisioning takes place at the third level for any I/O that the compute host sends to Azure Storage's backend. With this scheme, the performance of a VM depends on a variety of factors, from how the VM uses the local SSD, to the number of disks attached, as well as the performance and caching type of the disks it has attached.

As an example of these limitations, a Standard_DS1v1 VM is prevented from achieving the 5,000 IOPS potential of a P30 disk, whether it is cached or not, because of limits at the SSD and network levels:



Azure uses prioritized network channel for disk traffic, which gets the precedence over other low priority of network traffic. This helps disks maintain their expected performance in case of network contentions. Similarly, Azure Storage handles resource contentions and other issues in the background with automatic load balancing. Azure Storage allocates required resources when you create a disk, and applies proactive and reactive balancing of resources to handle the traffic level. This further ensures disks can sustain their expected IOPS and throughput targets. You can use the VM-level and Disk-level metrics to track the performance and setup alerts as needed.

Refer to our design for high performance article, to learn the best practices for optimizing VM + Disk configurations so that you can achieve your desired performance

Next steps

If you'd like a video going into more detail on managed disks, check out: Better Azure VM Resiliency with Managed Disks.

Learn more about the individual disk types Azure offers, which type is a good fit for your needs, and learn about their performance targets in our article on disk types.

Select a disk type for IaaS VMs

Introduction to Azure managed disks

12/16/2019 • 9 minutes to read • Edit Online

Azure managed disks are block-level storage volumes that are managed by Azure and used with Azure Virtual Machines. Managed disks are like a physical disk in an on-premises server but, virtualized. With managed disks, all you have to do is specify the disk size, the disk type, and provision the disk. Once you provision the disk, Azure handles the rest.

The available types of disks are ultra disks, premium solid-state drives (SSD), standard SSDs, and standard hard disk drives (HDD). For information about each individual disk type, see Select a disk type for IaaS VMs.

Benefits of managed disks

Let's go over some of the benefits you gain by using managed disks.

Highly durable and available

Managed disks are designed for 99.999% availability. Managed disks achieve this by providing you with three replicas of your data, allowing for 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 infrastructure as a service (IaaS) disks, with an industry-leading ZERO% annualized failure rate.

Simple and scalable VM deployment

Using managed disks, you can create up to 50,000 VM **disks** of a type in a subscription per region, allowing you to create thousands of **VMs** in a single subscription. This feature also further increases the scalability of virtual machine scale sets by allowing you to create up to 1,000 VMs in a virtual machine scale set using a Marketplace image.

Integration with availability sets

Managed disks are integrated with availability sets to ensure that the disks of VMs in an availability set are sufficiently isolated from each other to avoid a single point of failure. Disks are automatically placed 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.

Integration with Availability Zones

Managed disks support Availability Zones, which is a high-availability offering that protects your applications from datacenter failures. Availability Zones are unique physical locations within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. To ensure resiliency, there’s a minimum of three separate zones in all enabled regions. With Availability Zones, Azure offers industry best 99.99% VM uptime SLA.

Azure Backup support

To protect against regional disasters, Azure Backup can be used to create a backup job with time-based backups and backup retention policies. This allows you to perform easy VM restorations at will. Currently Azure Backup supports disk sizes up to four tebibyte (TiB) disks. Azure Backup supports backup and restore of managed disks. Learn more about Azure VM backup support.

Granular access control

You can use Azure role-based access control (RBAC) to assign specific permissions for a managed disk to one or more users. Managed disks expose a variety of operations, including read, write (create/update), delete, and retrieving a shared access signature (SAS) URI for the disk. You can grant access to only the operations a person needs to perform their 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.

Upload your vhd

Direct upload makes it easy to transfer your vhd to an Azure managed disk. Previously, you had to follow a more involved process that included staging your data in a storage account. Now, there are fewer steps. It is easier to upload on premises VMs to Azure, upload to large managed disks, and the backup and restore process is simplified. It also reduces cost by allowing you to upload data to managed disks directly without attaching them to VMs. You can use direct upload to upload vhds up to 32 TiB in size.

To learn how to transfer your vhd to Azure, see the CLI or PowerShell articles.

Encryption

Managed disks offer two different kinds of encryption. The first is Server Side Encryption (SSE), which is performed by the storage service. The second one is Azure Disk Encryption (ADE), which you can enable on the OS and data disks for your VMs.

Server-side encryption

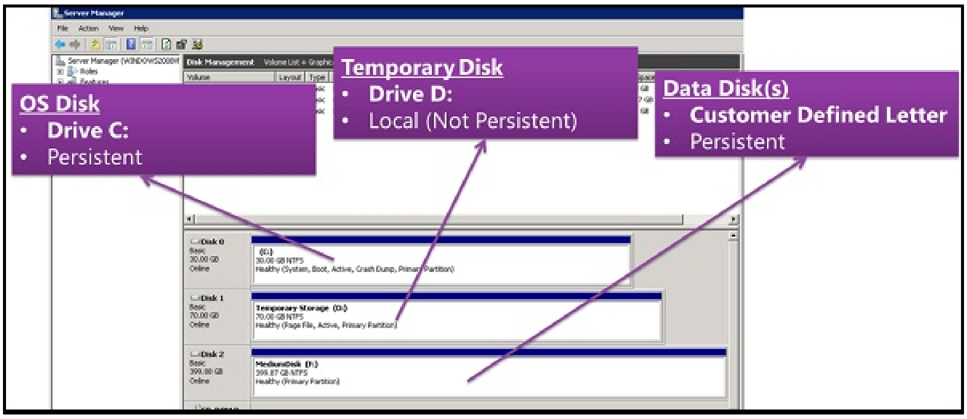
Azure Server-side Encryption provides encryption-at-rest and safeguards your data to meet your organizational security and compliance commitments. Server-side encryption is enabled by default for all managed disks, snapshots, and images in all the regions where managed disks are available. You can either allow Azure to manage your keys for you, these are platform-managed keys, or you can manage the keys yourself, these are customer-managed keys. Visit the Managed Disks FAQ page for more details.

Azure Disk Encryption

Azure Disk Encryption allows you to encrypt the OS and Data disks used by an IaaS Virtual Machine. This encryption 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. The encryption process is integrated with Azure Key Vault to allow you to control and manage the disk encryption keys. For more information, see Azure Disk Encryption for IaaS VMs.

Disk roles

There are three main disk roles in Azure: the data disk, the OS disk, and the temporary disk. These roles map to disks that are attached to your virtual machine.



Data disk

A data disk is a managed disk that's attached to a virtual machine to store application data, or other data you need to keep. Data disks are registered as SCSI drives and are labeled with a letter that you choose. Each data disk has a maximum capacity of 32,767 gibibytes (GiB). The size of the virtual machine determines how many data disks you can attach to it and the type of storage you can use to host the disks.

OS disk

Every virtual machine has one attached operating system disk. That OS disk has a pre-installed OS, which was selected when the VM was created. This disk contains the boot volume.

This disk has a maximum capacity of 2,048 GiB.

Temporary disk

Every VM contains a temporary disk, which is not a managed disk. The temporary disk provides short-term storage for applications and processes and is intended to only store data such as page or swap files. Data on the temporary disk may be lost during a maintenance event event or when you redeploy a VM. On Azure Linux VMs, the temporary disk is /dev/sdb by default and on Windows VMs the temporary disk is D: by default. During a successful standard reboot of the VM, the data on the temporary disk will persist.

Managed disk snapshots

A managed disk snapshot is a read-only crash-consistent full copy of a managed disk that 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.

Snapshots are billed based on the used size. For example, if you create a snapshot of a managed disk with provisioned capacity of 64 GiB and actual used data size of 10 GiB, that snapshot is billed only for the used data size of 10 GiB. You can see the used size of your snapshots by looking at the Azure usage report. For example, if the used data size of a snapshot is 10 GiB, the **daily** usage report will show 10 GiB/(31 days) = 0.3226 as the consumed quantity.

To learn more about how to create snapshots for managed disks, see the following resources:

- Create a snapshot of a managed disk in Windows
- Create a snapshot of a managed disk in Linux

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 (sysprepped) VM. This process captures a single image. This image contains all managed disks associated with a VM, including both the OS and data disks. This managed custom image enables creating hundreds of VMs using your custom image without the need to copy or manage any storage accounts.

For information on creating images, see the following articles:

- How to capture a managed image of a generalized VM in Azure
- How to generalize and capture a Linux virtual machine using the Azure CLI

Images versus snapshots

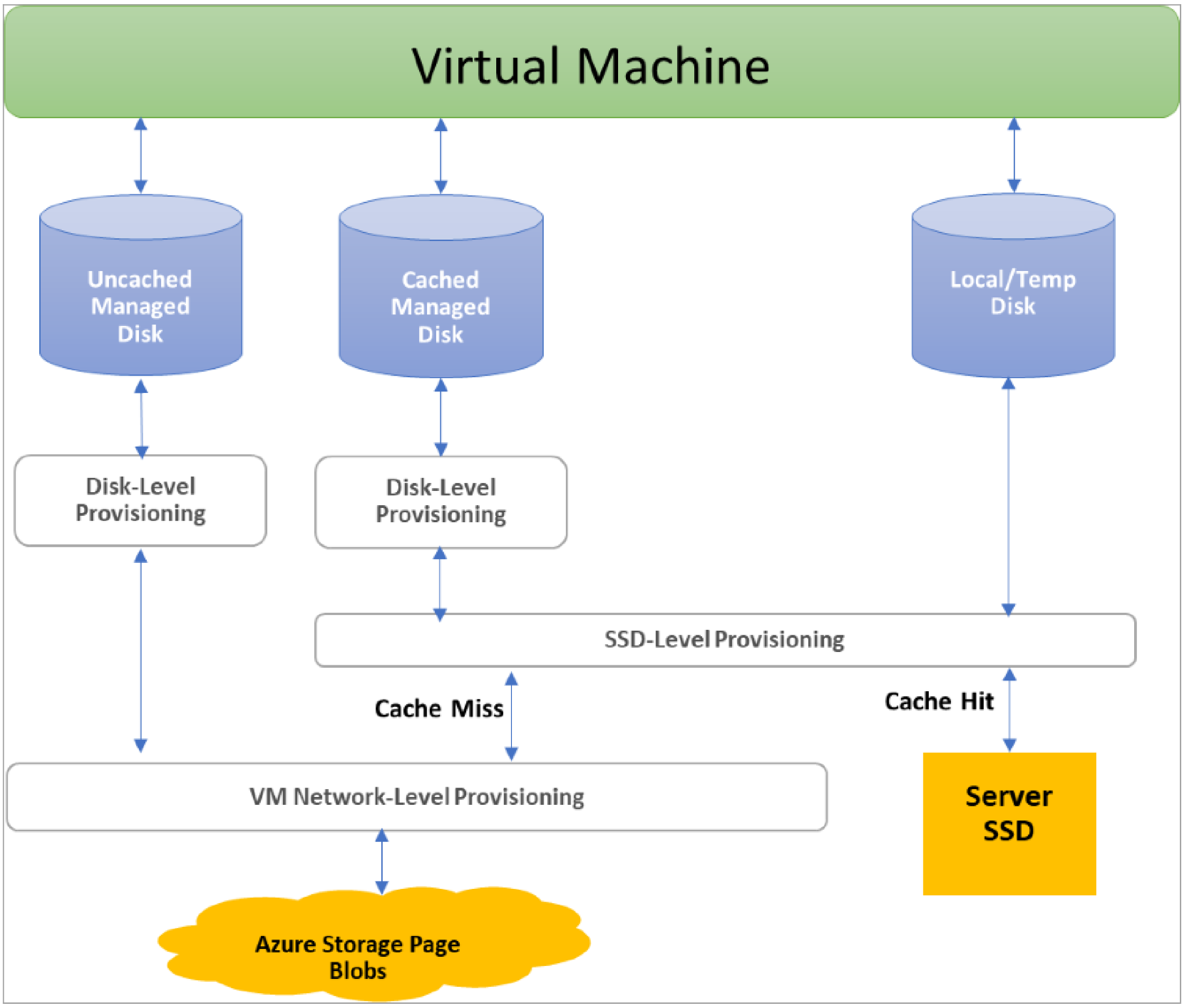
It's important to understand the difference between images and snapshots. With managed disks, you can take an image of a generalized VM that has been deallocated. This image includes all of the disks attached to the VM. You can use this image to create a VM, and it includes all of the disks.

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

A snapshot doesn't have awareness of any disk except the one it contains. This makes it problematic to use in scenarios that require the coordination of multiple disks, such as striping. Snapshots would need to be able to coordinate with each other and this is currently not supported.

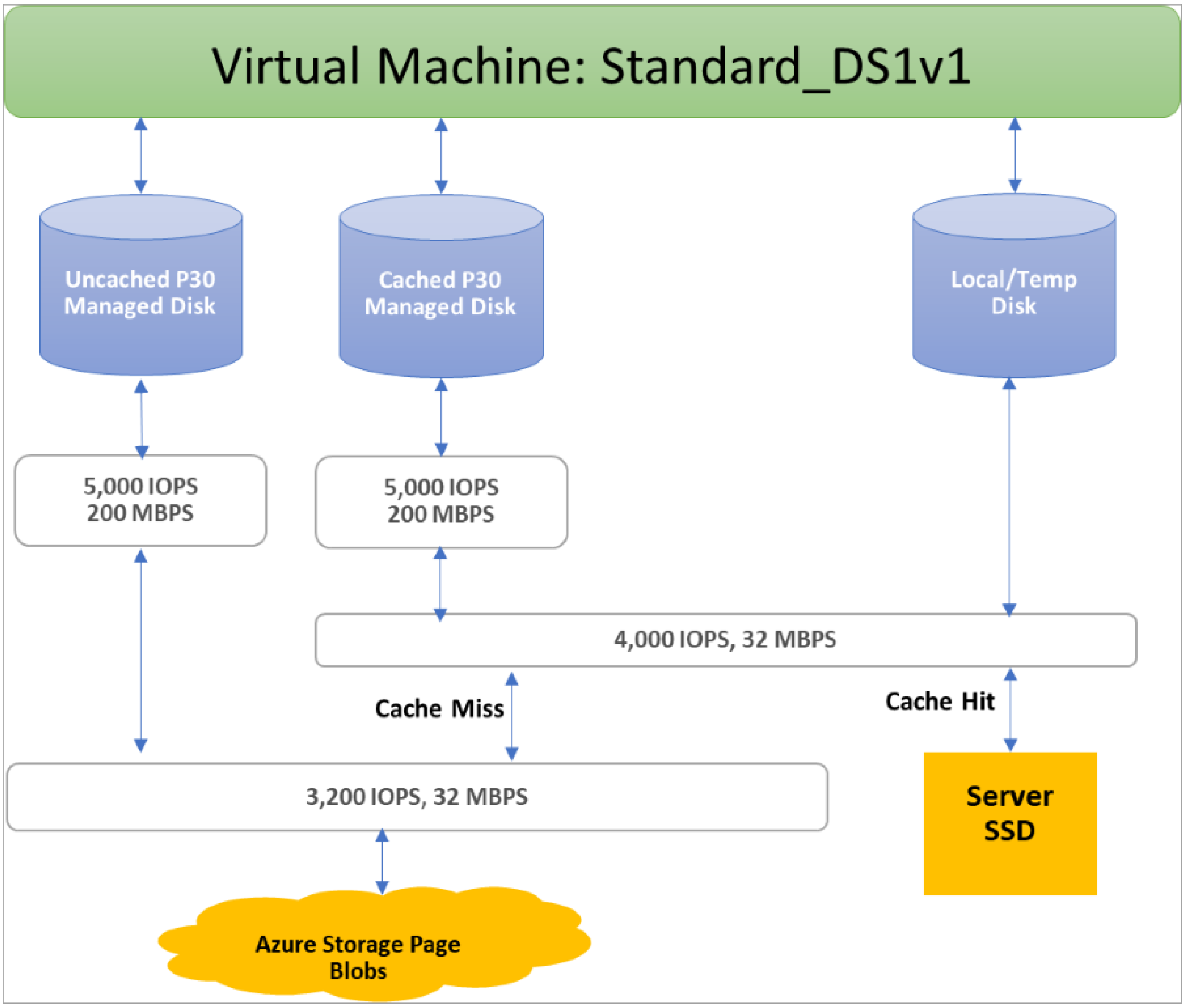
Disk allocation and performance

The following diagram depicts real-time allocation of bandwidth and IOPS for disks, using a three-level provisioning system:



The first level provisioning sets the per-disk IOPS and bandwidth assignment. At the second level, compute server host implements SSD provisioning, applying it only to data that is stored on the server's SSD, which includes disks with caching (ReadWrite and ReadOnly) as well as local and temp disks. Finally, VM network provisioning takes place at the third level for any I/O that the compute host sends to Azure Storage's backend. With this scheme, the performance of a VM depends on a variety of factors, from how the VM uses the local SSD, to the number of disks attached, as well as the performance and caching type of the disks it has attached.

As an example of these limitations, a Standard_DS1v1 VM is prevented from achieving the 5,000 IOPS potential of a P30 disk, whether it is cached or not, because of limits at the SSD and network levels:



Azure uses prioritized network channel for disk traffic, which gets the precedence over other low priority of network traffic. This helps disks maintain their expected performance in case of network contentions. Similarly, Azure Storage handles resource contentions and other issues in the background with automatic load balancing. Azure Storage allocates required resources when you create a disk, and applies proactive and reactive balancing of resources to handle the traffic level. This further ensures disks can sustain their expected IOPS and throughput targets. You can use the VM-level and Disk-level metrics to track the performance and setup alerts as needed.

Refer to our design for high performance article, to learn the best practices for optimizing VM + Disk configurations so that you can achieve your desired performance

Next steps

If you'd like a video going into more detail on managed disks, check out: Better Azure VM Resiliency with Managed Disks.

Learn more about the individual disk types Azure offers, which type is a good fit for your needs, and learn about their performance targets in our article on disk types.

Select a disk type for IaaS VMs