

Your fastest way to learn. Why wait?



Microsoft

Azure Administrator Associate - Supplementary Notes

Version 1.2

<https://firebrand.training>

| | |
|---|----|
| Introduction..... | 3 |
| Azure Management areas and tools | 4 |
| | 5 |
| Monitor | 5 |
| Configure | 5 |
| Govern | 6 |
| | 7 |
| Cloudyn | 7 |
| Secure | 7 |
| | 8 |
| Protect..... | 8 |
| | 9 |
| Migrate..... | 9 |
| | 17 |
| Storage Comparisons | 17 |
| Storage Replication | 17 |
| VM Related Resources | 23 |
| Maintenance for Virtual Machines in Azure | 24 |
| Disks used by VMs | 27 |
| Virtual Machines and Virtual Networks | 28 |
| Virtual Machine Images..... | 30 |
| Azure Load Balancer | 31 |
| | 33 |
| Traffic Manager..... | 33 |
| Application Gateway..... | 35 |
| Azure Active Directory | 37 |
| Azure Active Directory B2B | 38 |

Introduction

Azure PowerShell provides a set of cmdlets that use the Azure Resource Manager model for managing your Azure resources. Azure PowerShell uses .NET Standard, making it available for Windows, macOS, and Linux. Azure PowerShell is also available from Azure Cloud Shell.

Use Azure Cloud Shell to run Azure PowerShell in your browser or install locally.

EXERCISE: Get started with Azure PowerShell

<https://docs.microsoft.com/en-us/powershell/azure/get-started-azureps?view=azps-1.0.0>

EXERCISE: Automate Azure Tasks using scripts with PowerShell

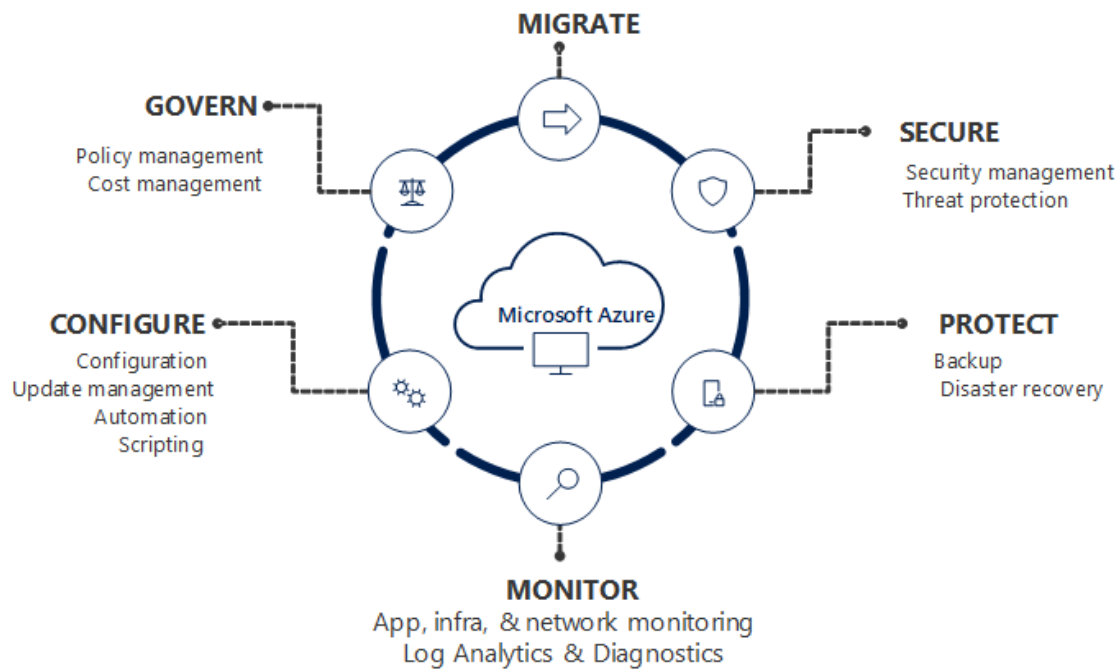
<https://docs.microsoft.com/en-us/learn/modules/automate-azure-tasks-with-powershell/>

Azure Virtual Machine PowerShell samples

<https://docs.microsoft.com/en-gb/azure/virtual-machines/windows/powershell-samples?toc=%2Fpowershell%2Fazure%2Ftoc.json>

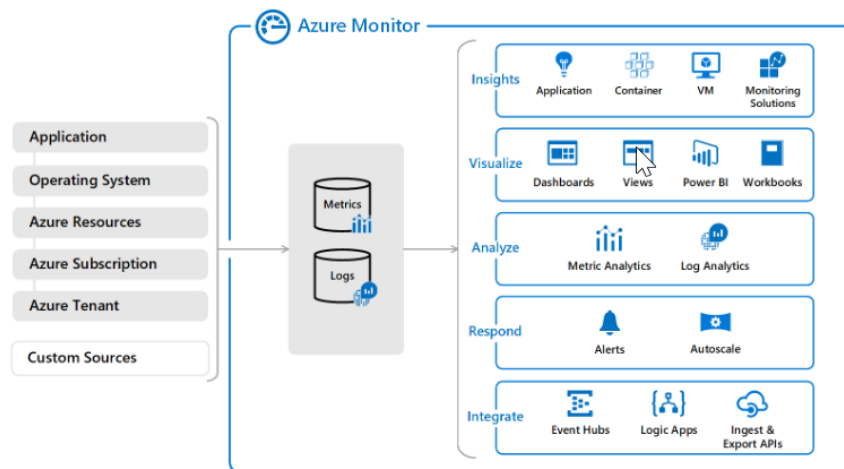
Azure Management areas and tools

The following diagram illustrates the different areas of management that are required to maintain any application or resource. These different areas can be thought of as a lifecycle. Each area is required in continuous succession over the lifespan of a resource. This resource lifecycle starts with the initial deployment, through continued operation, and finally when retired.



No single Azure service completely fills the requirements of a particular management area. Instead, each is realized by several services working together. Some services, such as Application Insights, provide targeted monitoring functionality for web applications. Others, like Log Analytics, store management data for other services. This feature allows you to analyze data of different types collected by different services.

Monitor





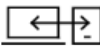


[Azure Monitor Overview](#)

Configure

Azure Automation delivers a cloud-based automation and configuration service that provides consistent management across your Azure and non-Azure environments. It consists of process automation, update management, and configuration features. Azure Automation provides complete control during deployment, operations, and decommissioning of workloads and resources.

Azure Automation capabilities

| | |
|---|--|
|  <p>Process Automation Orchestrate processes using graphical, PowerShell, and Python runbooks</p> |  <p>Shared capabilities Role based access control Secure, global store for variables, credentials, certificates, connections Flexible scheduling Shared modules Source control support Auditing Tags</p> |
|  <p>Configuration Management Collect inventory Track changes Configure desired state</p> | |
|  <p>Update Management Assess compliance Schedule update installation</p> |  <p>Heterogenous Windows & Linux Azure and on-premises</p> |

Build / Deploy resources - Deploy VMs across a hybrid environment using Runbooks and Azure Resource Manager templates. Integrate into development tools like Jenkins and Azure DevOps.

Configure VMs - Assess and configure Windows and Linux machines with the desired configuration for the infrastructure and application.

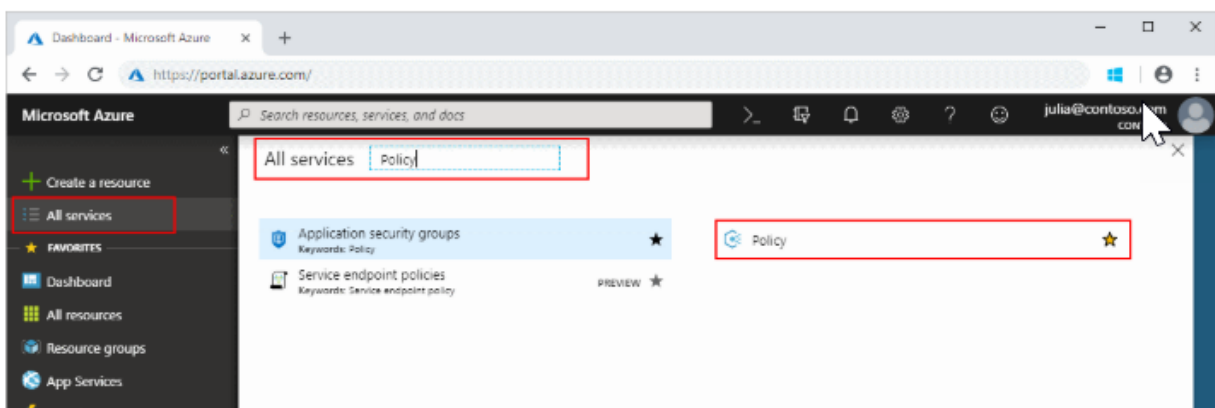
Monitor - Identify changes on machines that are causing issues and remediate or escalate to management systems.

Protect - Quarantine VM if security alert is raised. Set in-guest requirements.

Govern - Set up role-based access control for teams. Recover unused resources.

Govern

Azure Policy is a service in Azure that you use to create, assign and, manage policies. These policies enforce different rules and effects over your resources, so those resources stay compliant with your corporate standards and service level agreements. Azure Policy meets this need by evaluating your resources for non-compliance with assigned policies. For example, you can have a policy to allow only a certain SKU size of virtual machines in your environment. Once this policy is implemented, new and existing resources are evaluated for compliance. With the right type of policy, existing resources can be brought into compliance.



Cloudyn

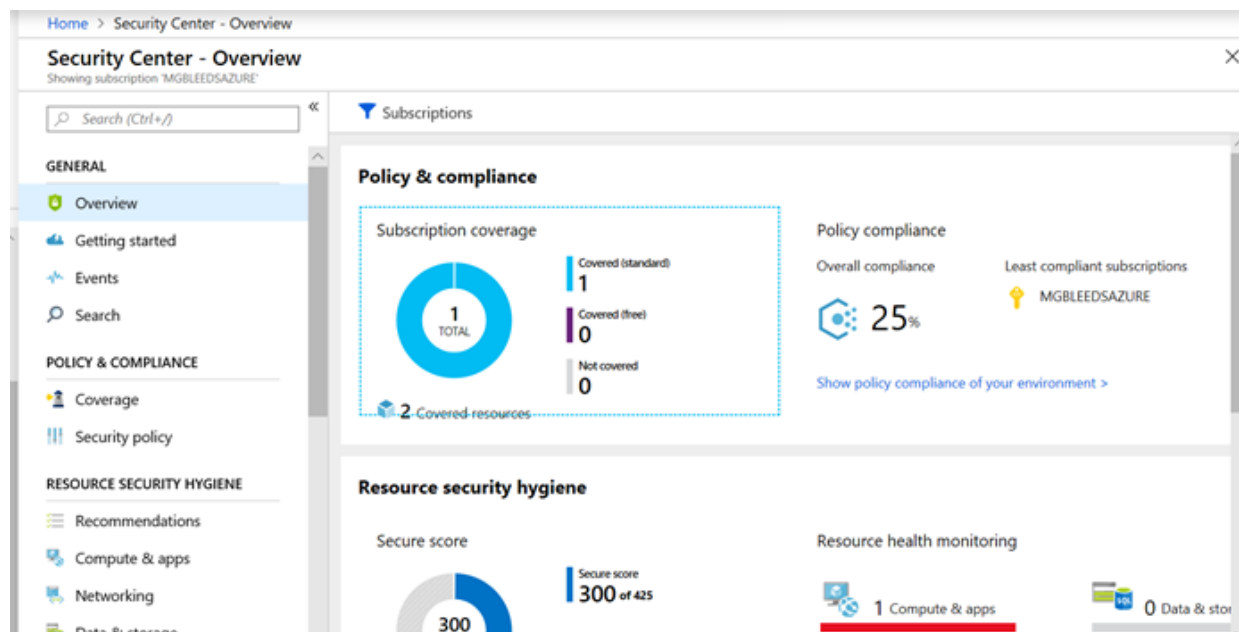
Cloudyn, a Microsoft subsidiary, allows you to track cloud usage and expenditures for your Azure resources and other cloud providers including AWS and Google. Easy-to-understand dashboard reports help with cost allocation and showbacks/chargebacks as well. Cloudyn helps optimize your cloud spending by identifying underutilized resources that you can then manage and adjust.

[Cloudyn Overview](#)

Secure

Azure Security Centre is a unified infrastructure security management system that strengthens the security posture of your data centres and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as well as on premises.

[Security Centre Overview](#)



Protect

Azure Backup is the Azure-based service you can use to back up (or protect) and restore your data in the Microsoft cloud. Azure Backup replaces your existing on-premises or off-site backup solution with a cloud-based solution that is reliable, secure, and cost-competitive. Azure Backup offers multiple components that you download and deploy on the appropriate computer, server, or in the cloud. The component, or agent, that you deploy depends on what you want to protect. All Azure Backup components (no matter whether you're protecting data on-premises or in the cloud) can be used to back up data to a Recovery Services vault in Azure.

[Azure Backup Overview](#)

Azure Site Recovery - As an organization you need to adopt a business continuity and disaster recovery (BCDR) strategy that keeps your data safe, and your apps and workloads up and running, when planned and unplanned outages occur.

Azure Recovery Services contribute to your BCDR strategy:

Site Recovery service: Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at your primary site, you fail over to secondary location, and access apps from there. After the primary location is running again, you can fail back to it.

Backup service: The Azure Backup service keeps your data safe and recoverable by backing it up to Azure.

Site Recovery can manage replication for:

Azure VMs replicating between Azure regions.

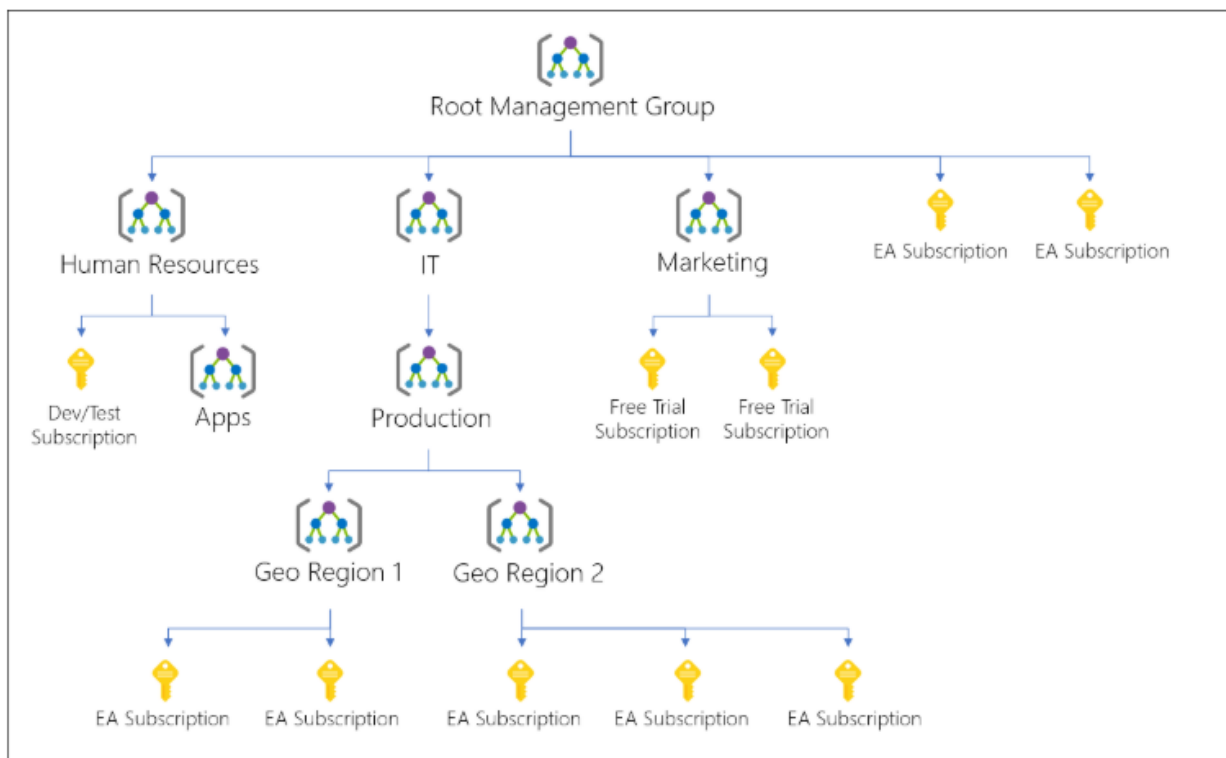
On-premises VMs, Azure Stack VMs and physical servers.

Migrate

The Azure Migrate service assesses on-premises workloads for migration to Azure. The service assesses the migration suitability of on-premises machines, performs performance-based sizing, and provides cost estimations for running on-premises machines in Azure. If you're contemplating lift-and-shift migrations, or are in the early assessment stages of migration, this service is for you. After the assessment, you can use services such as Azure Site Recovery and Azure Database Migration Service, to migrate the machines to Azure.

[Azure Migrate Overview](#)

If your organization has many subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions. Azure management groups provide a level of scope above subscriptions. You organize subscriptions into containers called "management groups" and apply your governance conditions to the management groups. All subscriptions within a management group automatically inherit the conditions applied to the management group. Management groups give you enterprise-grade management at a large scale no matter what type of subscriptions you might have.



One area where you would use management groups is to provide user access to multi subscriptions. By moving many subscriptions under that management group, you can create one role-based access control (RBAC) assignment on the management group, which will inherit that access to all the subscriptions. One assignment on the management group can enable users to have access to everything they need instead of scripting RBAC over different subscriptions.

Azure Resource Graph is a service in Azure that is designed to extend Azure Resource Management by providing efficient and performant resource exploration with the ability to query at scale across all subscriptions and management groups so that you can effectively govern your environment. These queries provide the following features:

- Ability to query resources with complex filtering, grouping, and sorting by resource properties.
- Ability to iteratively explore resources based on governance requirements and convert the resulting expression into a policy definition.
- Ability to assess the impact of applying policies in a vast cloud environment.

Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements. Azure Blueprints makes it possible for development teams to rapidly build and stand up new environments with trust they're building within organizational compliance with a set of built-in components -- such as networking -- to speed up development and delivery.

Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artefacts such as:

- Role Assignments
- Policy Assignments
- Azure Resource Manager templates
- Resource Groups

[Azure Blueprints Overview](#)

- **Resource** - A manageable item that is available through Azure. Some common resources are a virtual machine, storage account, web app, database, and virtual network, but there are many more.
- **Resource group** - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. See Resource groups.
- **Resource provider** - A service that supplies the resources you can deploy and manage through Resource Manager. Each resource provider offers operations for working with the resources that are deployed. Some common resource providers are Microsoft.Compute, which supplies the virtual machine resource, Microsoft.Storage, which supplies the storage account resource, and Microsoft.Web, which supplies resources related to web apps. See Resource providers.
- **Resource Manager template** - A JavaScript Object Notation (JSON) file that defines one or more resources to deploy to a resource group. It also defines the dependencies between the deployed resources. The template can be used to deploy the resources consistently and repeatedly. See Template deployment.
- **Declarative syntax** - Syntax that lets you state "Here is what I intend to create" without having to write the sequence of programming commands to create it. The Resource Manager template is an example of declarative syntax. In the file, you define the properties for the infrastructure to deploy to Azure.

Guidance:

1. Define and deploy your infrastructure through the declarative syntax in Resource Manager templates, rather than through imperative commands.
2. Define all deployment and configuration steps in the template. You should have no manual steps for setting up your solution.
3. Run imperative commands to manage your resources, such as to start or stop an app or machine.
4. Arrange resources with the same lifecycle in a resource group. Use tags for all other organizing of resources.

Resource Groups




There are some important factors to consider when defining your resource group:

1. All the resources in your group should share the same lifecycle. You deploy, update, and delete them together. If one resource, such as a database server, needs to exist on a different deployment cycle it should be in another resource group.
2. Each resource can only exist in one resource group.
3. You can add or remove a resource to a resource group at any time.
4. You can move a resource from one resource group to another group. For more information, see [Move resources to new resource group or subscription](#)
5. A resource group can contain resources that reside in different regions.
6. A resource group can be used to scope access control for administrative actions.
7. A resource can interact with resources in other resource groups. This interaction is common when the two resources are related but don't share the same lifecycle (for example, web apps connecting to a database).

RBAC

Using RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs. Instead of giving everybody unrestricted permissions in your Azure subscription or resources, you can allow only certain actions at a particular scope.

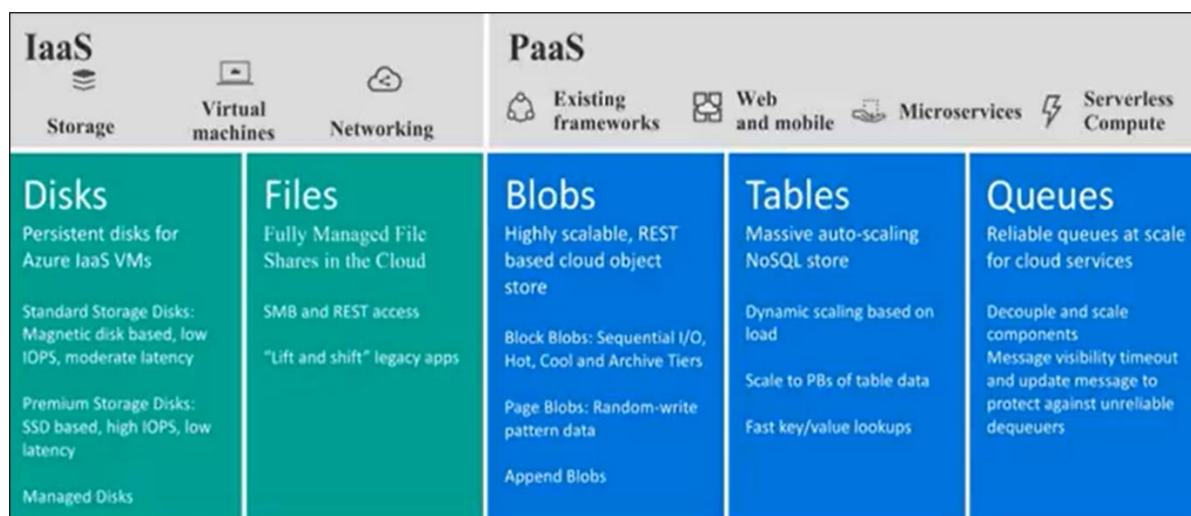
When planning your access control strategy, it's a best practice to grant users the least privilege to get their work done. The following diagram shows a suggested pattern for using RBAC.

| | | Role | | | |
|-------|---|---------------------|----------------------------------|-------------|--------|
| | | Reader | Resource-specific or custom role | Contributor | Owner |
| Scope |  Subscription | Observers | Users managing resources | | Admins |
| |  Resource group | | | | |
| |  Resource | Automated processes | | | |

Resource Manager Templates

With Resource Manager, you can create a template (in JSON format) that defines the infrastructure and configuration of your Azure solution. By using a template, you can repeatedly deploy your solution throughout its lifecycle and have confidence your resources are deployed in a consistent state. When you create a solution from the portal, the solution automatically includes a deployment template. You don't have to create your template from scratch because you can start with the template for your solution and customize it to meet your specific needs.

```
"resources": [  
  {  
    "apiVersion": "2016-01-01",  
    "type": "Microsoft.Storage/storageAccounts",  
    "name": "mystorageaccount",  
    "location": "westus",  
    "sku": {  
      "name": "Standard_LRS"  
    },  
    "kind": "Storage",  
    "properties": {  
    }  
  }  
]
```



Azure Storage Accounts

This table shows the various kinds of storage accounts and which objects can be used with each.

| Type of storage account | General-purpose Standard | General-purpose Premium | Blob storage, hot and cool access tiers |
|--------------------------|---|-------------------------|---|
| Services supported | Blob, File, Queue, and Table Services | Blob Service | Blob Service |
| Types of blobs supported | Block blobs, page blobs, and append blobs | Page blobs | Block blobs and append blobs |

(Azure Data Lake Gen2 now in preview, built on top of Azure Blob storage offering low cost of storage capacity and transactions. Unlike other cloud storage services, data stored in Data Lake Storage Gen2 is not required to be moved or transformed prior to performing analysis)

There are two kinds of general-purpose storage accounts:

Standard storage

The most widely used storage accounts are standard storage accounts, which can be used for all types of data. Standard storage accounts use magnetic media to store data.

Premium storage

Premium storage provides high-performance storage for page blobs, which are primarily used for VHD files. Premium storage accounts use SSD to store data. Microsoft recommends using Premium Storage for all your VMs.

Storage Comparisons

[Azure Storage Types](#)

Storage Replication

To ensure that your data is durable, Azure Storage replicates multiple copies of your data. When you set up your storage account, you select a replication type. In most cases, this setting can be modified after the storage account has been created.

Replication options for a storage account include:

- [Locally-redundant storage \(LRS\)](#): A simple, low-cost replication strategy. Data is replicated within a single storage scale unit.
- [Zone-redundant storage \(ZRS\)](#): Replication for high availability and durability. Data is replicated synchronously across three availability zones.
- [Geo-redundant storage \(GRS\)](#): Cross-regional replication to protect against region-wide unavailability.
- [Read-access geo-redundant storage \(RA-GRS\)](#): Cross-regional replication with read access to the replica.

In the event of failure use the information on the following link to help your recovery:

[Storage DR](#)

Azure Storage provides a comprehensive set of security capabilities that together enable developers to build secure applications:

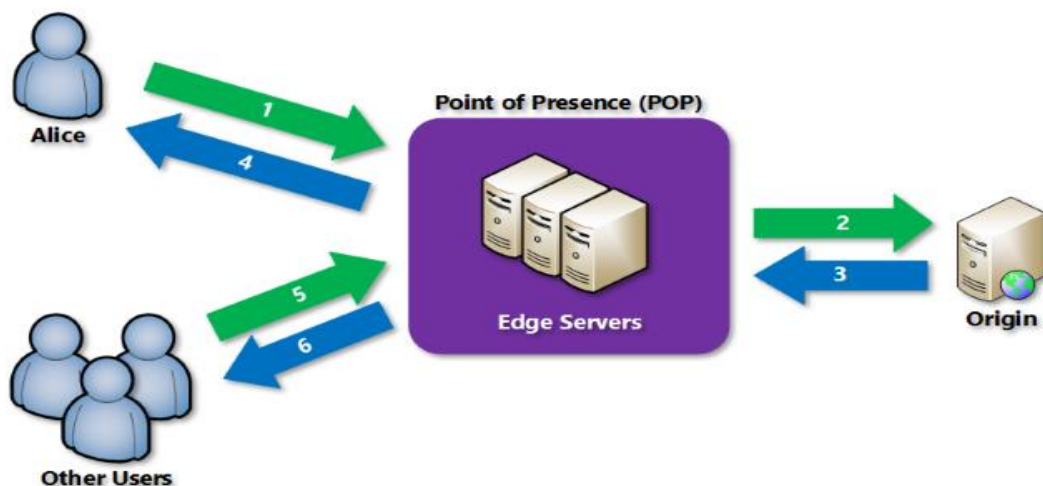
- All data written to Azure Storage is automatically encrypted using [Storage Service Encryption \(SSE\)](#). For more information, see [Announcing Default Encryption for Azure Blobs, Files, Table and Queue Storage](#).
- Azure Active Directory (Azure AD) and Role-Based Access Control (RBAC) are supported for Azure Storage for both resource management operations and data operations, as follows:
 - You can assign RBAC roles scoped to the storage account to security principals and use Azure AD to authorize resource management operations such as key management.
 - Azure AD integration is supported in preview for data operations on the Blob and Queue services. You can assign RBAC roles scoped to a subscription, resource group, storage account, or an individual container or queue to a security principal or a managed identity for Azure resources. For more information, see [Authenticate access to Azure Storage using Azure Active Directory \(Preview\)](#).
- Data can be secured in transit between an application and Azure by using [Client-Side Encryption](#), HTTPS, or SMB 3.0.
- OS and data disks used by Azure virtual machines can be encrypted using [Azure Disk Encryption](#).
- Delegated access to the data objects in Azure Storage can be granted using [Shared Access Signatures](#)

A content delivery network (CDN) is a distributed network of servers that can efficiently deliver web content to users. CDNs store cached content on edge servers in point-of-presence (POP) locations that are close to end users, to minimize latency.

The benefits of using Azure CDN to deliver web site assets include:

- Better performance and improved user experience for end users, especially when using applications in which multiple round-trips are required to load content.
- Large scaling to better handle instantaneous high loads, such as the start of a product launch event.
- Distribution of user requests and serving of content directly from edge servers so that less traffic is sent to the origin server.

How it works



Azure CDN offers the following key features:

- [Dynamic site acceleration](#)
- [CDN caching rules](#)
- [HTTPS custom domain support](#)
- [Azure diagnostics logs](#)
- [File compression](#)
- [Geo-filtering](#)

Import and Export Service

Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacentre. This service can also be used to transfer data from Azure Blob storage to disk drives and ship to your on-premises sites. Data from one or more disk drives can be imported either to **Azure Blob storage** or **Azure Files**.

Import / Export components

- **Import/Export service:** This service available in Azure portal helps the user create and track data import (upload) and export (download) jobs.
- **WALImportExport tool:** This is a command-line tool that does the following:
 - Prepares your disk drives that are shipped for import.
 - Facilitates copying your data to the drive.
 - Encrypts the data on the drive with BitLocker.
 - Generates the drive journal files used during import creation.
 - Helps identify numbers of drives needed for export jobs.
- **Disk Drives:** You can ship Solid-state drives (SSDs) or Hard disk drives (HDDs) to the Azure datacentre. When creating an import job, you ship disk drives containing your data. When creating an export job, you ship empty drives to the Azure datacenter. For specific disk types, go to [Supported disk types](#).

AzCopy

AzCopy is a command-line utility designed for copying data to/from Microsoft Azure Blob, File, and Table storage, using simple commands designed for optimal performance. You can copy data between a file system and a storage account, or between storage accounts.

Examples:

```
AzCopy /Source:<source> /Dest:<destination> [Options]
```

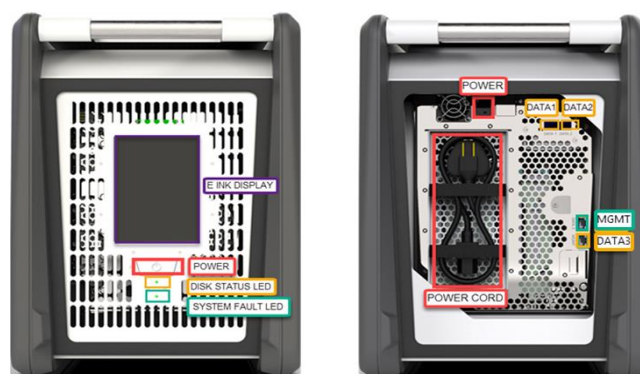
```
AzCopy /Source:https://myaccount.blob.core.windows.net/mycontainer  
/Dest:C:\myfolder /SourceKey:key /Pattern:"abc.txt"
```

```
AzCopy /Source:https://myaccount.blob.core.windows.net/mycontainer  
/Dest:C:\myfolder /SourceKey:key /S
```

Azure Data Box

The Microsoft Azure Data Box cloud solution lets you send terabytes of data into Azure in a quick, inexpensive, and reliable way. The secure data transfer is accelerated by shipping you a proprietary Data Box storage device. Each storage device has a maximum usable storage capacity of 80 TB and is transported to your datacentre through a regional carrier. The device has a rugged casing to protect and secure data during the transit.

- **One time migration** - when large amount of on-premises data is moved to Azure.
 - Moving a media library from offline tapes into Azure to create an online media library.
 - Migrating your VM farm, SQL server, and applications to Azure
 - Moving historical data to Azure for in-depth analysis and reporting using HDInsight
- **Initial bulk transfer** - when an initial bulk transfer is done using Data Box (seed) followed by incremental transfers over the network.
 - For example, backup solutions partners such as Commvault and Data Box are used to move initial large historical backup to Azure. Once complete, the incremental data is transferred via network to Azure storage.
- **Periodic uploads** - when large amount of data is generated periodically and needs to be moved to Azure. For example, in energy exploration, where video content is generated on oil rigs and windmill farms.



Data Box front view (left) and back view (right)

In addition to the Data Box service Microsoft Azure also have available the Azure Disk for smaller volumes and Azure Data Box Heavy for larger volumes of data you have the need to move from on-prem to Azure.



Azure Data Factory

You can use Copy jobs in Azure Data Factory to copy data to and from Azure Blob storage. You can copy data from any supported source data store to Blob storage. You also can copy data from Blob storage to any supported sink data store

What do I need to think about before creating a VM?

- The names of your application resources
- The location where the resources are stored
- The size of the VM
- The maximum number of VMs that can be created
- The operating system that the VM runs
- The configuration of the VM after it starts
- The related resources that the VM needs

VM Related Resources

The resources in this table are used by the VM and need to exist or be created when the VM is created.

| Resource | Required | Description |
|-------------------|----------|---|
| Resource group | Yes | The VM must be contained in a resource group. |
| Storage account | Yes | The VM needs the storage account to store its virtual hard disks. |
| Virtual network | Yes | The VM must be a member of a virtual network. |
| Public IP address | No | The VM can have a public IP address assigned to it to remotely access it. |
| Network interface | Yes | The VM needs the network interface to communicate in the network. |
| Data disks | No | The VM can include data disks to expand storage capabilities. |

VM Types and Sizes

| Type | Sizes | Description |
|--------------------------|--|---|
| General purpose | B, Dsv3, Dv3, DSv2, Dv2, Av2, DC | Balanced CPU-to-memory ratio. Ideal for testing and development, small to medium databases, and low to medium traffic web servers. |
| Compute optimized | Fsv2, Fs, F | High CPU-to-memory ratio. Good for medium traffic web servers, network appliances, batch processes, and application servers. |
| Memory optimized | Esv3, Ev3, M, GS, G, DSv2, Dv2 | High memory-to-CPU ratio. Great for relational database servers, medium to large caches, and in-memory analytics. |
| Storage optimized | Lsv2, Ls | High disk throughput and IO ideal for Big Data, SQL, NoSQL databases, data warehousing and large transactional databases. |
| GPU | NV, NVv2, NC, NCv2, NCv3, ND, Ndv2 (Preview) | Specialized virtual machines targeted for heavy graphic rendering and video editing, as well as model training and inferencing (ND) with deep learning. Available with single or multiple GPUs. |
| High performance compute | H | Our fastest and most powerful CPU virtual machines with optional high-throughput network interfaces (RDMA). |

Maintenance for Virtual Machines in Azure

Azure periodically updates platform to improve the reliability, performance, and security of the host infrastructure for virtual machines. These updates range from patching software components in the hosting environment, upgrading networking components, to hardware decommissioning. The majority of these updates have no impact to the hosted virtual machines. However, there are cases where updates do have an impact and Azure chooses the least impactful method for updates:

- If a non-rebootful update is possible, the VM is paused while the host is updated, or it is live migrated to an already updated host.
- If maintenance requires a reboot, you get a notice of when the maintenance is planned. Azure will also give a time window where you can start the maintenance yourself, at a time that works for you. Azure is investing in technologies to reduce the cases when the VMs must be rebooted for planned platform maintenance.

Memory preserving maintenance

The goal for most non-rebootful updates is less than 10 seconds pause for the VM. In certain cases memory preserving maintenance mechanisms are used, which pauses the VM for up to 30 seconds and preserves the memory in RAM. The virtual machine is then resumed and the clock of the virtual machine is automatically synchronized. Azure is increasingly using live migration technologies and improving memory preserving maintenance mechanism to reduce the pause duration.

These non-rebootful maintenance operations are applied fault domain by fault domain, and progress is stopped if any warning health signals are received.

Maintenance requiring a reboot

In the rare case when VMs need to be rebooted for planned maintenance, you are notified in advance. Planned maintenance has two phases: the self-service window and a scheduled maintenance window.

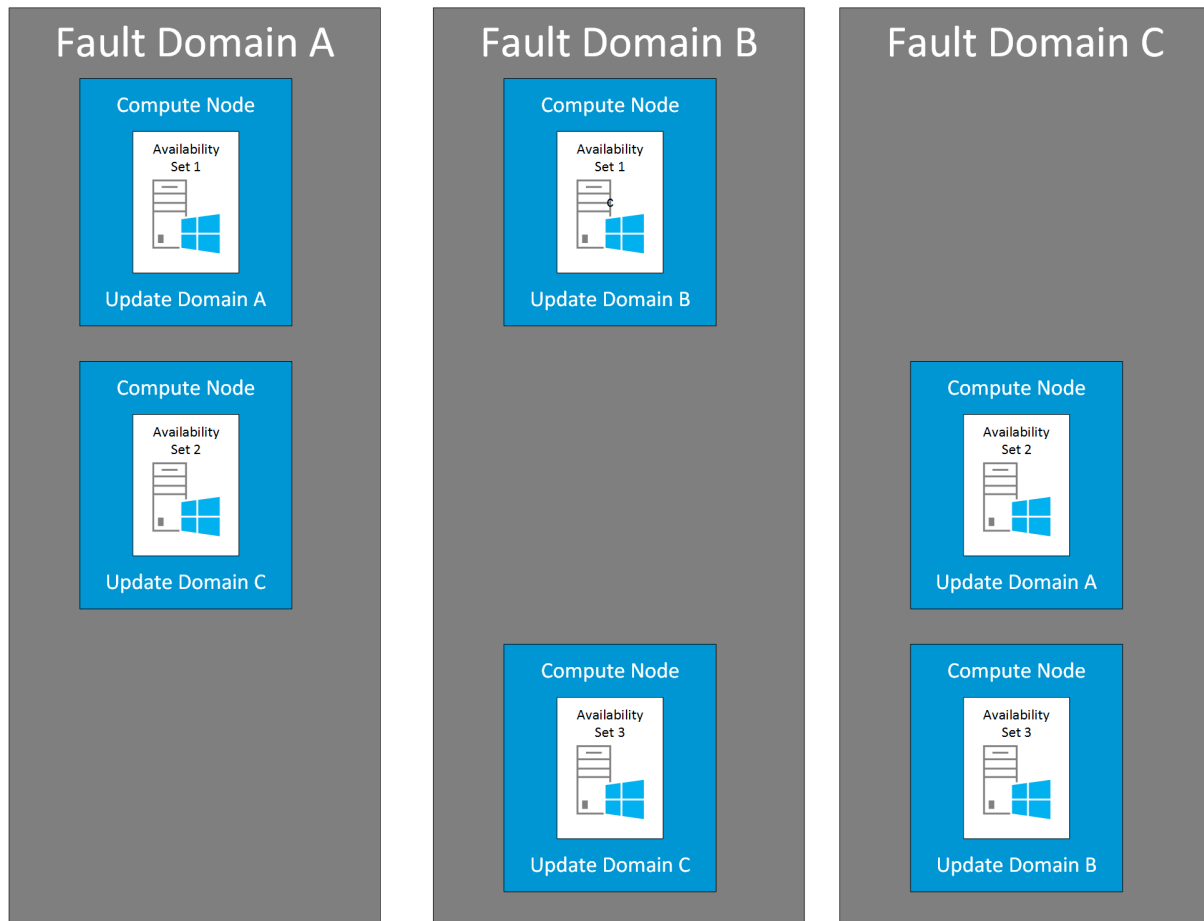
The **self-service window** lets you start the maintenance on your VMs. During this time, you can query each VM to see their status and check the result of your last maintenance request.

When you start self-service maintenance, your VM is redeployed to an already updated node. Because the VM reboots, the temporary disk is lost and dynamic IP addresses associated with virtual network interface are updated.

If you start self-service maintenance and there is an error during the process, the operation is stopped, the VM is not updated and you get the option to retry the self-service maintenance.

When the self-service window has passed, the **scheduled maintenance window** begins. During this time window, you can still query for the maintenance window, but can't start the maintenance yourself.

Availability sets



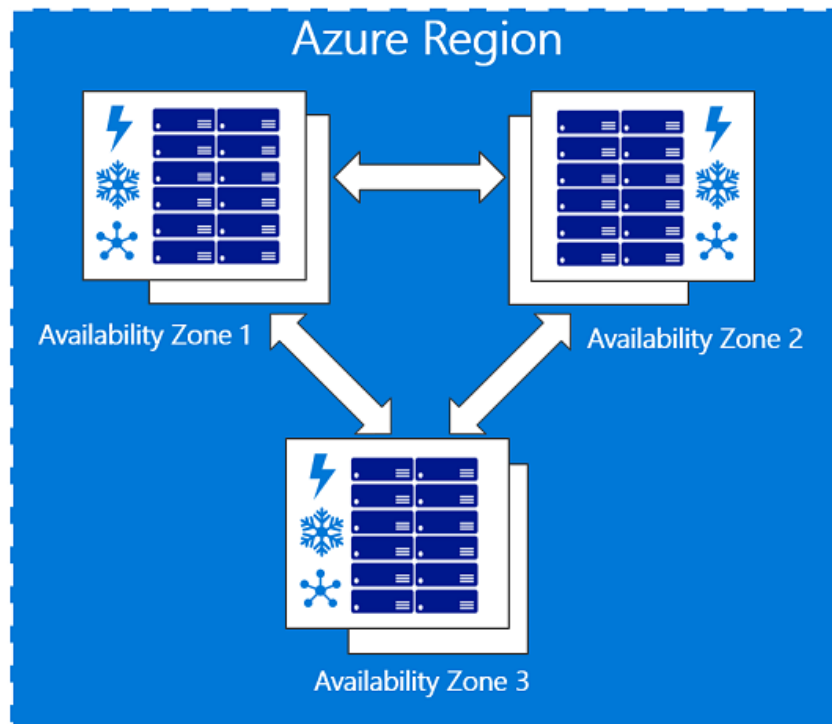
When deploying a workload on Azure VMs, you can create the VMs within an availability set to provide high availability to your application. This ensures that during either an outage or rebootful maintenance events, at least one VM is available.

Within an availability set, individual VMs are spread across up to 3 fault domains and 20 update domains (UDs).

Fault domains define the group of virtual machines that share a common power source and network switch. While placing your virtual machines into an availability set does not protect your application from operating system or application-specific failures, it does limit the impact of potential physical hardware failures, network outages, or power interruptions.

During scheduled maintenance, only a single update domain is updated at any given time. The order of update domains being updated doesn't necessarily happen sequentially.

Availability Zones



Availability Zones is a high-availability offering that protects your applications and data 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. The physical separation of Availability Zones within a region protects applications and data from datacenter failures. Zone-redundant services replicate your applications and data across Availability Zones to protect from single-points-of-failure. With Availability Zones, Azure offers industry best 99.99% VM uptime SLA. The full Azure SLA explains the guaranteed availability of Azure as a whole.

An Availability Zone in an Azure region is a combination of a fault domain and an update domain. For example, if you create three or more VMs across three zones in an Azure region, your VMs are effectively distributed across three fault domains and three update domains. The Azure platform recognizes this distribution across update domains to make sure that VMs in different zones are not updated at the same time.

Availability zones is currently available in a limited number of Azure Regions:

- Central US
- East US
- East US 2
- West US
- France Central
- North Europe
- West Europe

- UK South
- Japan East
- Southeast Asia

Only in 10 out of 54 Azure Regions.

Even in these different regions not all services support Availability Zones at the same level. You can find an exhaustive list at <https://docs.microsoft.com/en-us/azure/availability-zones/az-overview#services-support-by-region>

You can find more information about Availability Zones here:

<https://docs.microsoft.com/en-us/azure/availability-zones/az-overview>

Virtual Machines Scale Sets (VMSS)

Virtual machine scale sets are an Azure compute resource that enables you to deploy and manage a set of identical VMs as a single resource. The scale set is automatically deployed across update domains, like VMs in an availability set. Just like with availability sets, with scale sets only a single update domain is updated at any given time during scheduled maintenance.

Disks used by VMs

Operating system disk

Every virtual machine has one attached operating system disk. It's registered as a SATA drive and labelled as the C: drive by default. This disk has a maximum capacity of 2048 gigabytes (GB).

Temporary disk

Each VM contains a temporary 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 or when you redeploy a VM.

Data disk

A data disk is a VHD 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 labelled with a letter that you choose. Each data disk has a maximum capacity of 4,095 GB, managed disks have a maximum capacity of 32,767 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. At the time of writing this you can have a max of 64 data disks in a single Virtual Machine.

Types of disks

Azure Disks are designed for 99.999% availability. Azure Disks have consistently delivered enterprise-grade durability, with an industry-leading ZERO% Annualized Failure Rate.

There are three performance tiers for storage that you can choose from when creating your disks:

- Premium SSD
- Standard SSD
- Standard HDD

Also, there are two types of disks:

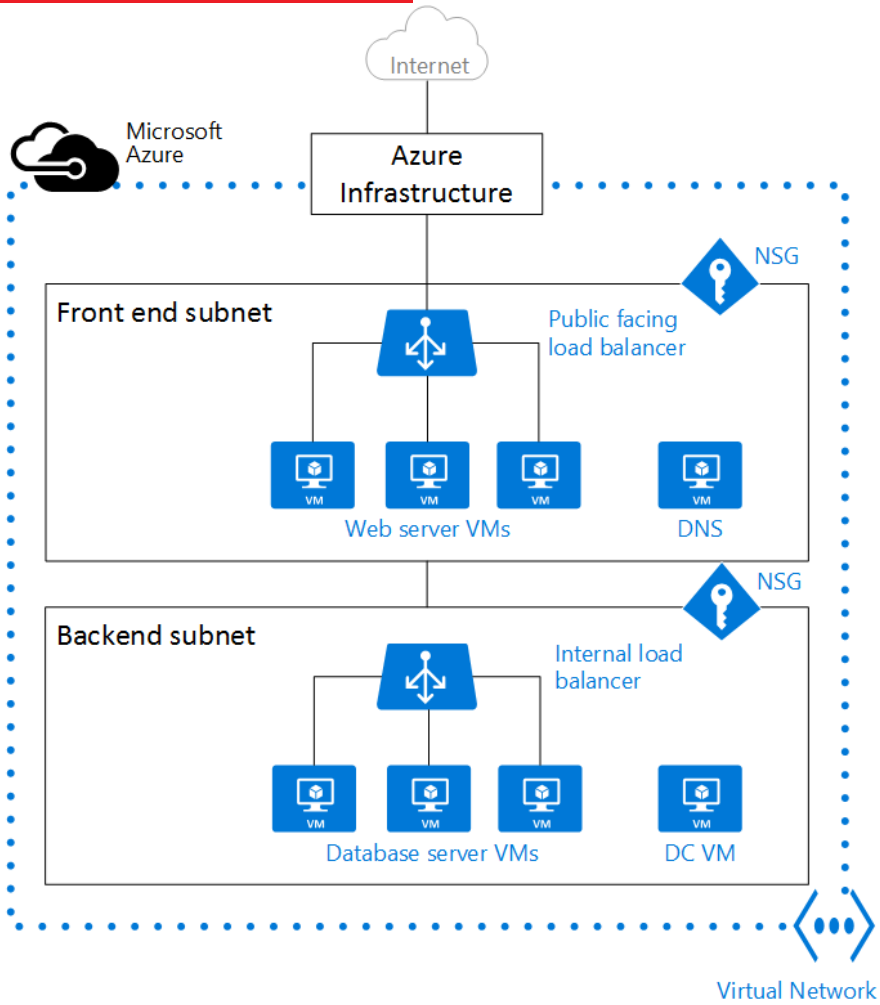
- Unmanaged disks
- Managed disks

[For more information on disk types follow this link](#)

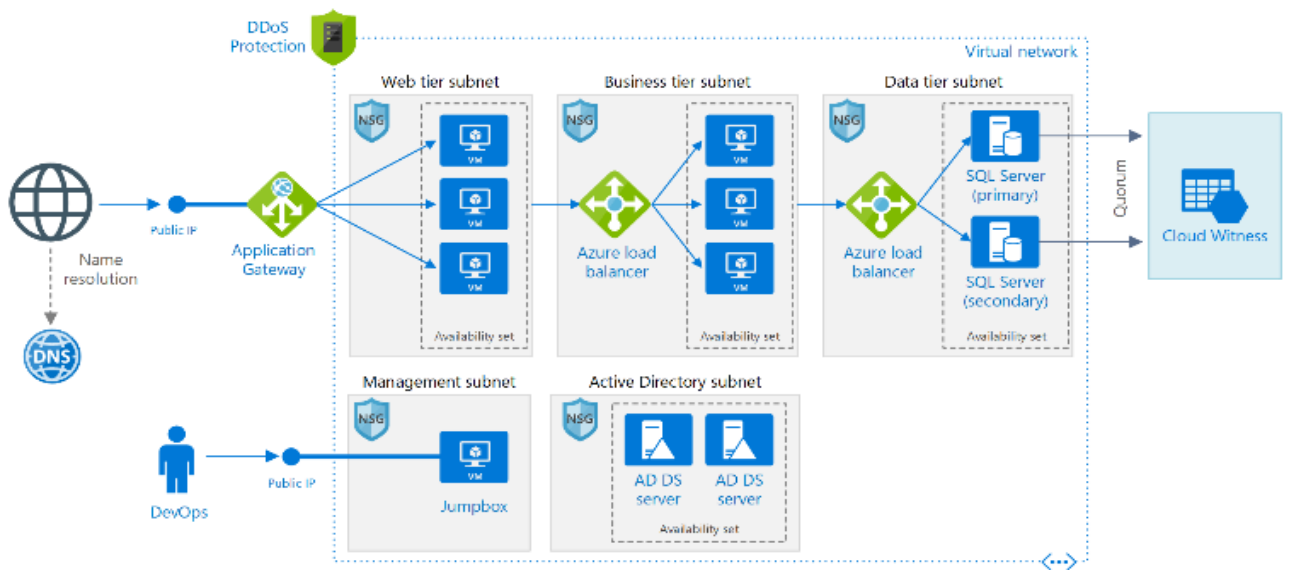
Virtual Machines and Virtual Networks

When you create an Azure virtual machine (VM), you must create a [virtual network](#) (VNet) or use an existing VNet. You also need to decide how your VMs are intended to be accessed on the VNet. It is important to [plan before creating resources](#) and make sure that you understand the [limits of networking resources](#).

In the following figure, VMs are represented as web servers and database servers. Each set of VMs are assigned to separate subnets in the VNet.



Example N-Tier Application Architecture



[For full details about this architecture, follow this link](#)

Virtual Machine Images

In the Azure Marketplace you can find an extensive list of Virtual Machine images. These images are updated by the publishers and in most cases is a best practice to use them instead of creating your own images.

A Marketplace image in Azure has the following attributes:

- Publisher: The organization that created the image. Examples: Canonical, MicrosoftWindowsServer
- Offer: The name of a group of related images created by a publisher. Examples: UbuntuServer, WindowsServer
- SKU: An instance of an offer, such as a major release of a distribution. Examples: 18.04-LTS, 2019-Datacenter
- Version: The version number of an image SKU.

Before your exam, make sure you take a good look at Virtual Machine images and how you can deploy them using PowerShell and Bash.

You can find more information's here: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/cli-ps-findimage>

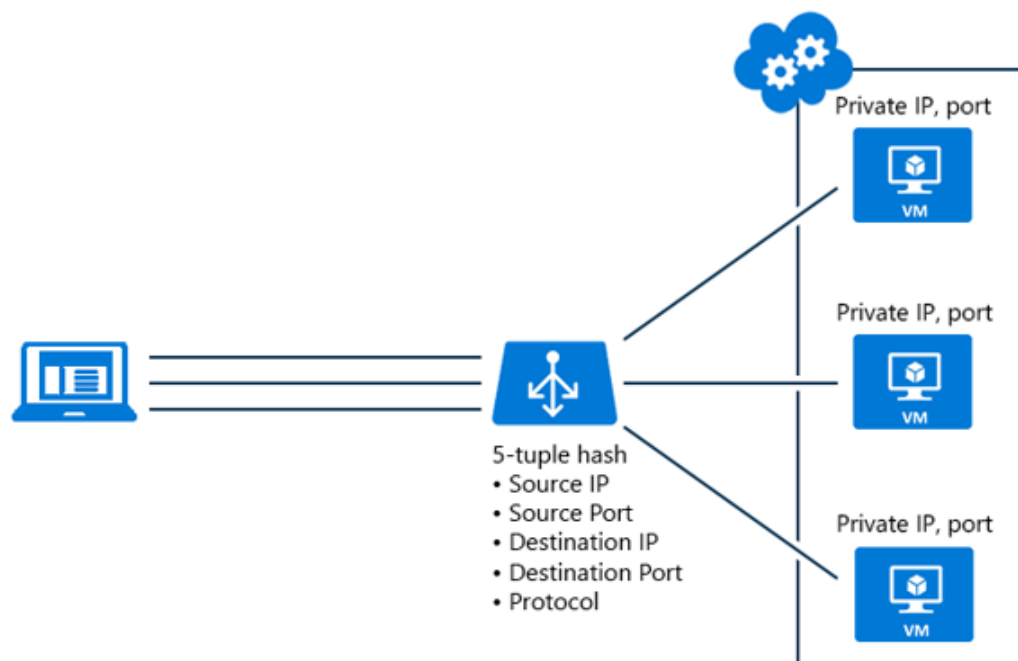
Azure Load Balancer

With Azure Load Balancer, you can scale your applications and create high availability for your services. Load Balancer supports inbound and outbound scenarios, provides low latency and high throughput, and scales up to millions of flows for all TCP and UDP applications.

Load Balancer distributes new inbound flows that arrive on the Load Balancer's frontend to backend pool instances, according to rules and health probes.

Additionally, a public Load Balancer can provide outbound connections for virtual machines (VMs) inside your virtual network by translating their private IP addresses to public IP addresses.

Azure Load Balancer is available in two SKUs: Basic and Standard. There are differences in scale, features, and pricing. Any scenario that's possible with Basic Load Balancer can also be created with Standard Load Balancer, although the approaches might differ slightly. As you learn about Load Balancer, it is important to familiarize yourself with the fundamentals and SKU-specific differences.

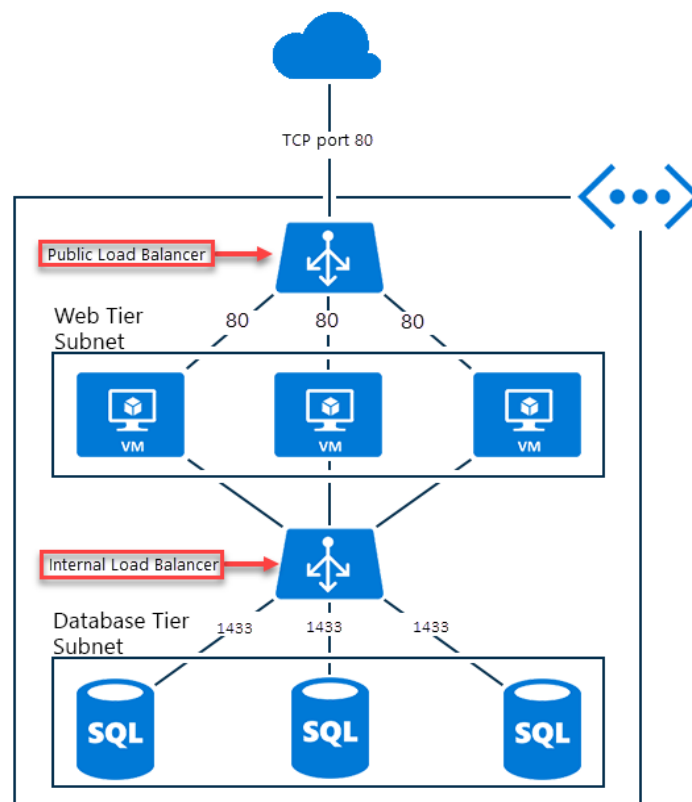


Standard and Basic SKUs

| | Standard SKU | Basic SKU |
|----------------------------|--|--|
| Backend pool size | Supports up to 1000 instances | Supports up to 100 instances |
| Backend pool endpoints | Any virtual machine in a single virtual network, including blend of virtual machines, availability sets, virtual machine scale sets. | Virtual machines in a single availability set or virtual machine scale set. |
| Health probes | TCP, HTTP, HTTPS | TCP, HTTP |
| Health probe down behavior | TCP connections stay alive on instance probe down and on all probes down. | TCP connections stay alive on instance probe down. All TCP connections terminate on all probes are down. |
| Availability Zones | In Standard SKU, zone-redundant and zonal frontends for inbound and outbound, outbound flows mappings survive zone failure, cross-zone load balancing. | Not Available |

For full SKU information: [Azure Load Balancer Overview](#)

Public and Internal Load Balancer Example



Traffic Manager

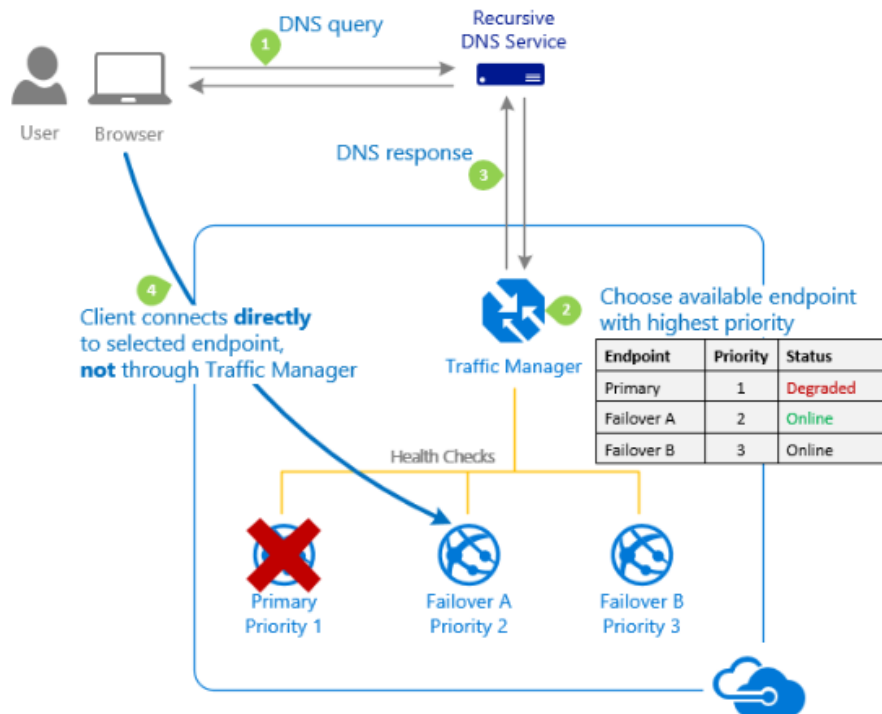
Azure Traffic Manager is a DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness.

Traffic Manager uses DNS to direct client requests to the most appropriate service endpoint based on a traffic-routing method and the health of the endpoints. An endpoint is any Internet-facing service hosted inside or outside of Azure.

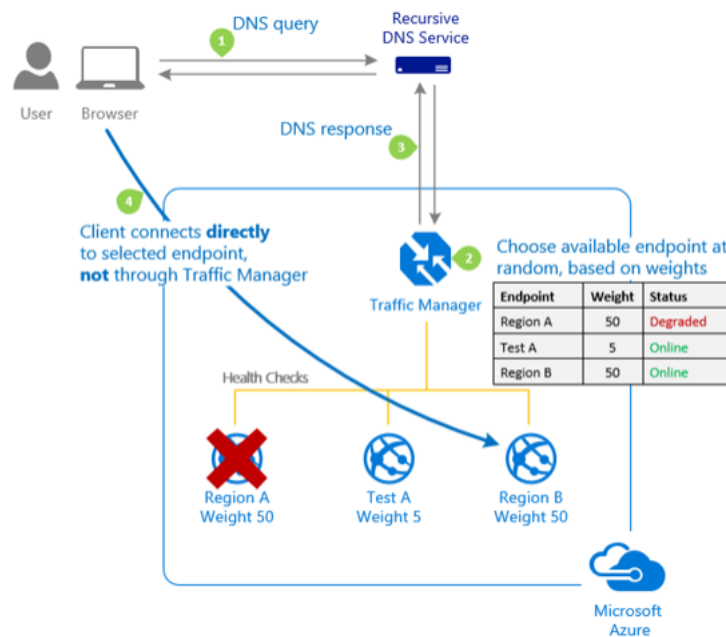
The following traffic routing methods are available in Traffic Manager:

- **Priority**: Select **Priority** when you want to use a primary service endpoint for all traffic and provide backups in case the primary or the backup endpoints are unavailable.
- **Weighted**: Select **Weighted** when you want to distribute traffic across a set of endpoints, either evenly or according to weights, which you define.
- **Performance**: Select **Performance** when you have endpoints in different geographic locations and you want end users to use the "closest" endpoint in terms of the lowest network latency.
- **Geographic**: Select **Geographic** so that users are directed to specific endpoints (Azure, External, or Nested) based on which geographic location their DNS query originates from. This empowers Traffic Manager customers to enable scenarios where knowing a user's geographic region and routing them based on that is important. Examples include complying with data sovereignty mandates, localization of content & user experience and measuring traffic from different regions.
- **Multivalue**: Select **MultiValue** for Traffic Manager profiles that can only have IPv4/IPv6 addresses as endpoints. When a query is received for this profile, all healthy endpoints are returned.
- **Subnet**: Select **Subnet** traffic-routing method to map sets of end-user IP address ranges to a specific endpoint within a Traffic Manager profile. When a request is received, the endpoint returned will be the one mapped for that request's source IP address.

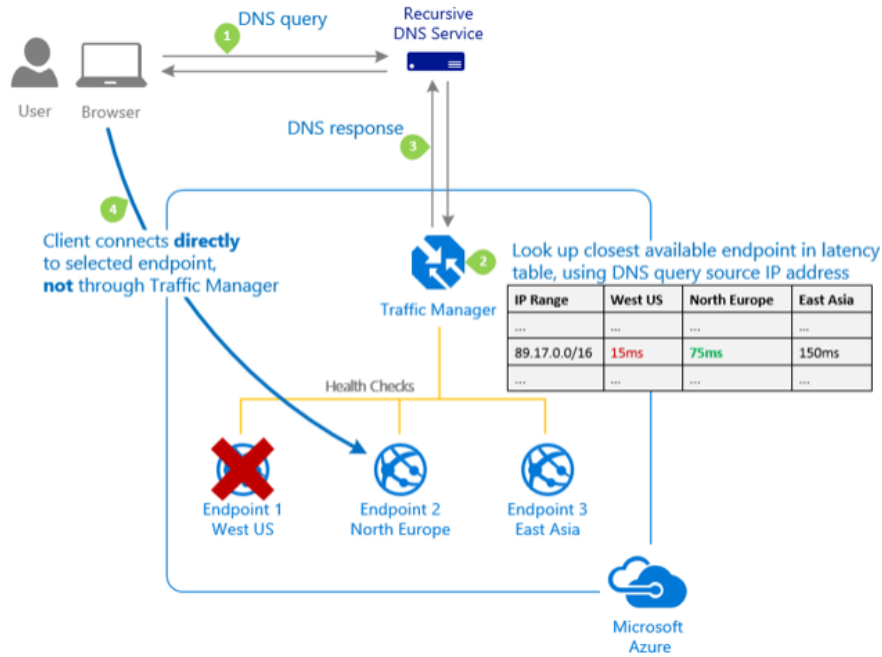
Priority Traffic Routing Example



Weighted Traffic Routing Example



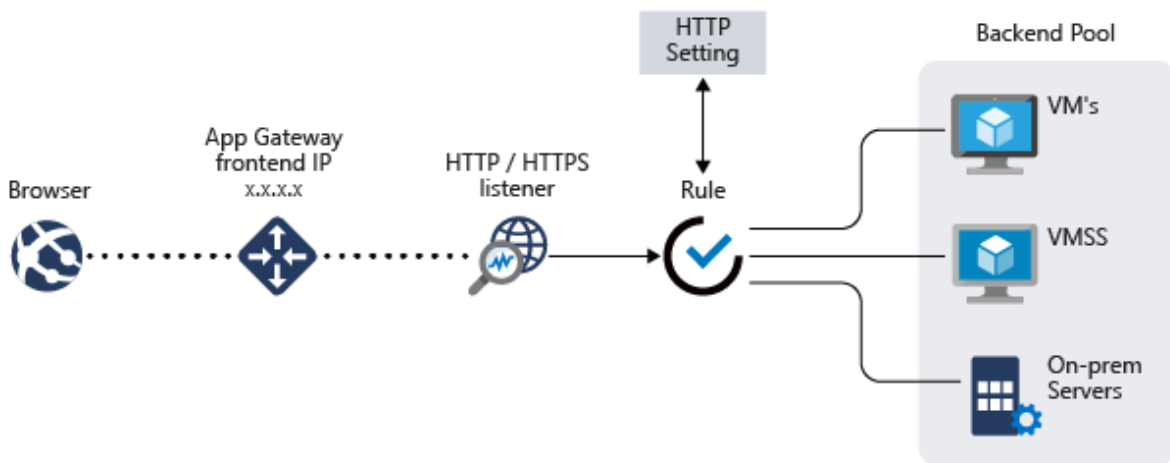
Performance Traffic Routing Example



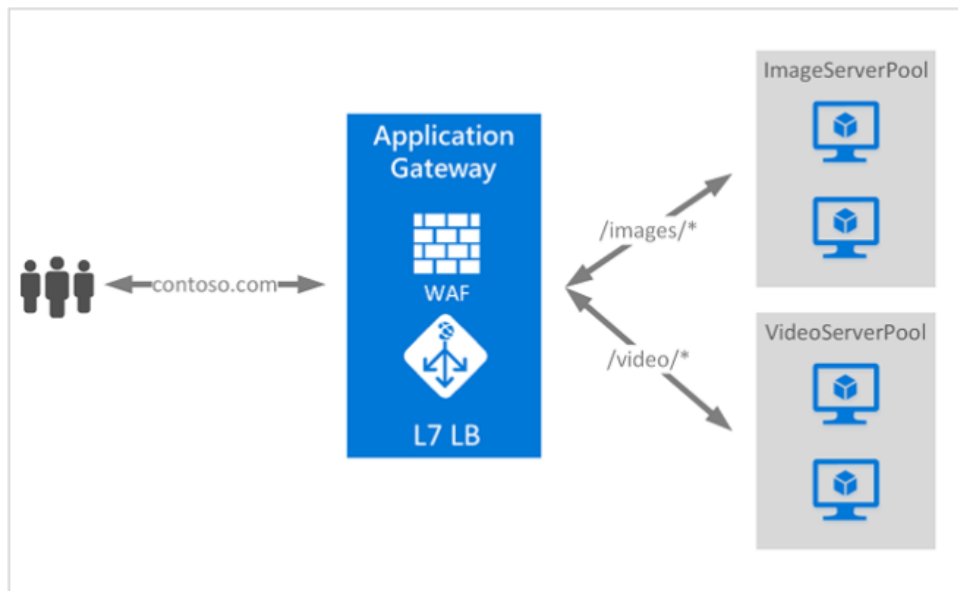
Traffic Manager Routing Methods

Application Gateway

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. Traditional load balancers operate at the transport layer (OSI layer 4 - TCP and UDP) and route traffic based on source IP address and port, to a destination IP address and port.



But with the Application Gateway you can be even more specific. For example, you can route traffic based on the incoming URL. So, if `/images` is in the incoming URL, you can route traffic to a specific set of servers (known as a pool) configured for images. If `/video` is in the URL, that traffic is routed to another pool optimized for videos.



This type of routing is known as application layer 7 load balancing. Application Gateway can do URL-based routing and more like for example:

- Secure Sockets Layer (SSL) termination
- Autoscaling
- Zone redundancy
- Static VIP
- Web Application firewall
- Multiple-site hosting
- Redirection
- Session affinity
- WebSocket and HTTP/2 traffic

Note: More features are being added.

You can find more about the Azure Application Gateway here:

<https://docs.microsoft.com/en-us/azure/application-gateway/overview>

Azure Active Directory

Azure Active Directory (AAD) is Microsoft's cloud-based identity and access management service. With Azure Active Directory users can sign in and access resources in:

- External resources, such as Microsoft 365, Azure portal, and other SaaS applications, like for example Salesforce, LinkedIn, ...
- Internal resources, such as apps on your corporate network and intranet, along with any cloud apps developed by your own organization.

Licensing

Azure Active Directory is licensed by user. There is a free tier, so for basic implementations there is no charge associated in using AAD, but to enhance your Azure AD implementation, you can also add paid capabilities by upgrading to Azure Active Directory Basic, Premium P1, or Premium P2 licenses. Azure AD paid licenses are built on top of your existing free directory, providing self-service, enhanced monitoring, security reporting, and secure access for your mobile users.

You can check an updated list with pricing and feature details here:

<https://azure.microsoft.com/en-us/pricing/details/active-directory/>

In Azure Active Directory you can find the following types of subscriptions:

- **Azure Active Directory Free**
Provides user and group management, on-premises directory synchronization, basic reports, and single sign-on across Azure, Office 365, and many popular SaaS apps.
- **Azure Active Directory Basic**
In addition to the Free features, Basic also provides cloud-centric app access, group-based access management, self-service password reset for cloud apps, and Azure AD Application Proxy, which lets you publish on-premises web apps using Azure AD.
- **Azure Active Directory Premium P1**
In addition to the Free and Basic features, P1 also lets your hybrid users access both on-premises and cloud resources. It also supports advanced administration, such as dynamic groups, self-service group management, Microsoft Identity Manager (an on-premises identity and access management suite) and cloud write-back capabilities, which allow self-service password reset for your on-premises users.
- **Azure Active Directory Premium P2**

In addition to the Free, Basic, and P1 features, P2 also offers Azure Active Directory Identity Protection to help provide risk-based conditional access to your apps and critical company data and Privileged Identity Management to help discover, restrict, and monitor administrators and their access to resources and to provide just-in-time access when needed.

- **"Pay as you go" feature licenses**

You can also get additional feature licenses, such as Azure Active Directory Business-to-Customer (B2C). B2C can help you provide identity and access management solutions for your customer-facing apps. For more information, see Azure Active Directory B2C documentation.

You can find more information about Azure Active Directory (AAD) here:

<https://docs.microsoft.com/en-us/azure/active-directory/>

Azure Active Directory B2B

Azure Active Directory (Azure AD) business-to-business (B2B) collaboration lets you securely share your company's applications and services with guest users from any other organization, while maintaining control over your own corporate data. Work safely and securely with external partners, large or small, even if they don't have Azure AD or an IT department. A simple invitation and redemption process lets partners use their own credentials to access your company's resources. Developers can use Azure AD business-to-business APIs to customize the invitation process or write applications like self-service sign-up portals.

You can find more information about Azure Active Directory B2B here:

<https://docs.microsoft.com/en-us/azure/active-directory/b2b/index>

Azure Active Directory B2C

Azure Active Directory (Azure AD) B2C is a business-to-consumer identity management service. This service enables you to customize and control how users securely interact with your web, desktop, mobile, or single-page applications. Using Azure AD B2C, users can sign up, sign in, reset passwords, and edit profiles. Azure AD B2C implements a form of the OpenID Connect and OAuth 2.0 protocols.

The important key in the implementation of these protocols is the security tokens and their claims that enable you to provide secure access to resources.

A user journey is a request that specifies a policy, which controls the behaviour of how the user and your application interact with Azure AD B2C. Two paths are available to you for defining user journeys in Azure AD B2C.

If you're an application developer with or without identity expertise, you might choose to define common identity user flows using the Azure portal. If you are an identity professional, systems integrator, consultant, or on an in-house identity team, are comfortable with OpenID Connect flows, and understand identity providers and claims-based authentication, you might choose XML-based custom policies.

Before you start defining a user journey, you need to create an Azure AD B2C tenant and register your application and API in the tenant. After you've completed these tasks, you can get started defining a user journey with either user flows or custom policies. You can also optionally, add or change identity providers, or customize the way the user experiences the journey.

You can find more information about Azure Active Directory B2C here:
<https://docs.microsoft.com/en-us/azure/active-directory-b2c/index>

Azure Multi-Factor Authentication

The security of two-step verification lies in its layered approach. Compromising multiple authentication factors presents a significant challenge for attackers. Even if an attacker manages to learn the user's password, it is useless without also having possession of the additional authentication method. It works by requiring two or more of the following authentication methods:

- Something you know (typically a password)
- Something you have (a trusted device that is not easily duplicated, like a phone)
- Something you are (biometrics).



Multi-Factor Authentication comes as part of the following offerings:

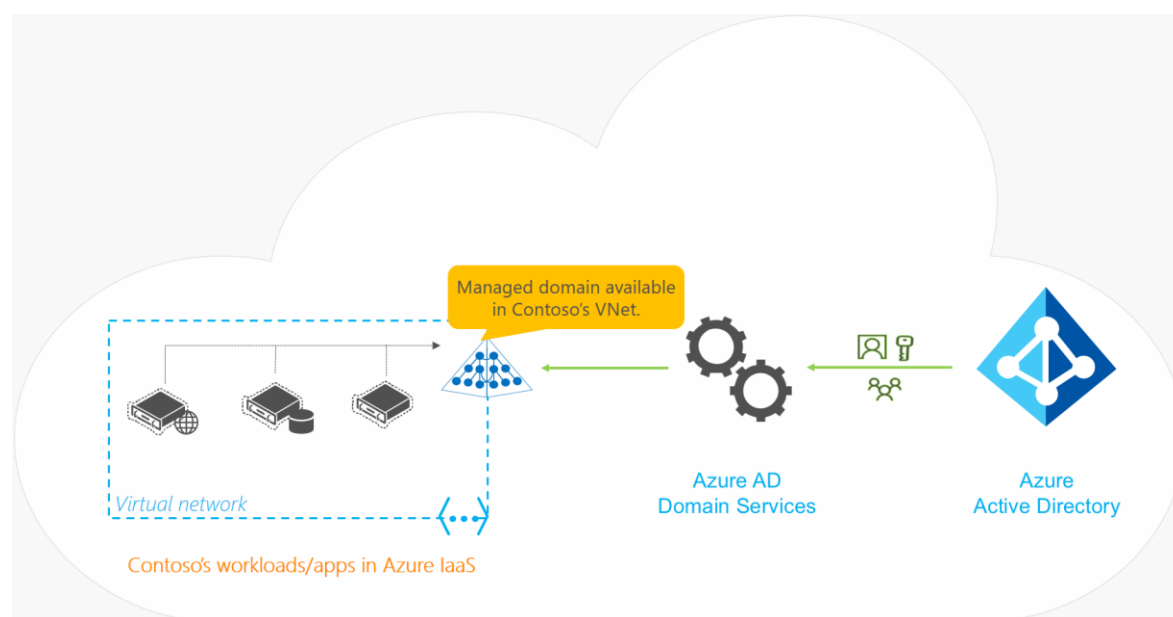
- Azure Active Directory Premium licenses - Full featured use of Azure Multi-Factor Authentication Service (Cloud) or Azure Multi-Factor Authentication Server (On-premises).
- Azure MFA Service (Cloud) - This option is the recommended path for new deployments. Azure MFA in the cloud requires no on-premises infrastructure and can be used with your federated or cloud-only users.
- Azure MFA Server - If your organization wants to manage the associated infrastructure elements and has deployed AD FS in your on-premises environment this way may be an option.
- Multi-Factor Authentication for Office 365 - A subset of Azure Multi-Factor Authentication capabilities are available as a part of your subscription. For more information about MFA for Office 365, see the article Plan for multi-factor authentication for Office 365 Deployments.
- Azure Active Directory Global Administrators - A subset of Azure Multi-Factor Authentication capabilities are available as a means to protect global administrator accounts.

You can find more information about Azure Active Directory Multi Factor Authentication (MFA) here: <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks>

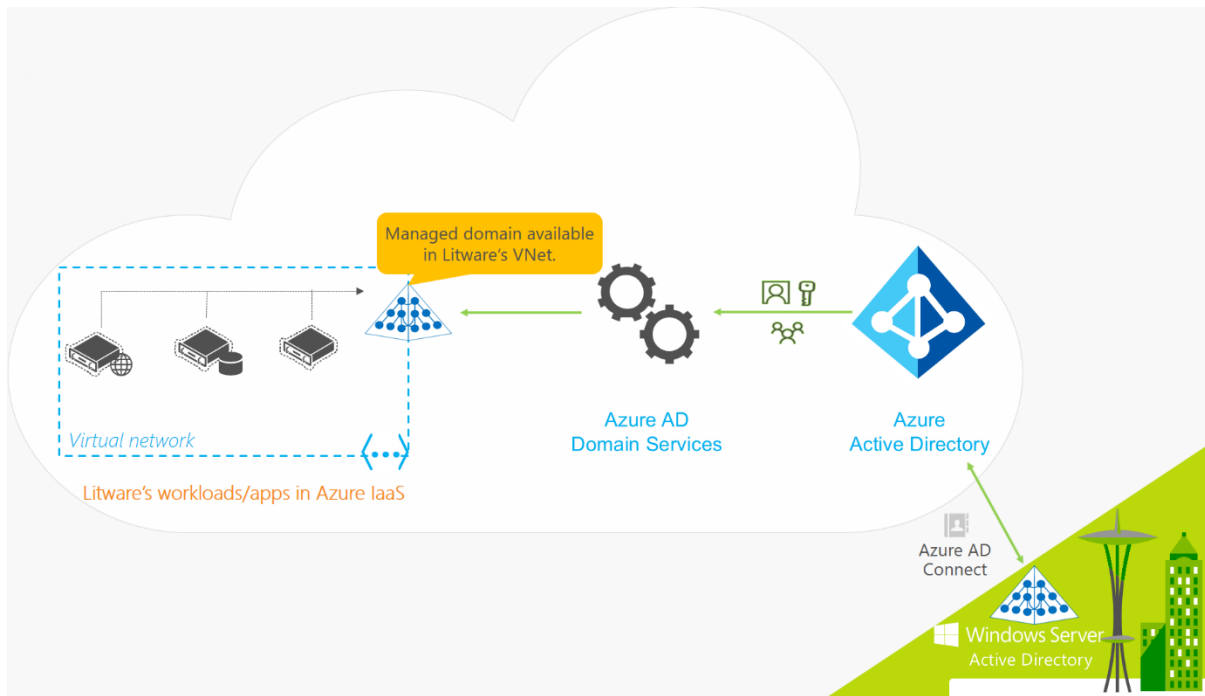
Azure AD Domain Services

Azure enables you to deploy virtual machines and other services in a very fast way. Azure AD Domain Services (AADDS) provides managed domain services, like domains join, authentications using LDAP and Kerberos/NTLM and GPO deployment. You can consume these domain services without the need for you to deploy, manage, and patch domain controllers in the cloud. Azure AD Domain Services integrates with your existing Azure AD tenant, thus making it possible for users to log in using their corporate credentials. Additionally, you can use existing groups and user accounts to secure access to resources, thus ensuring a smoother 'lift-and-shift' of on-premises resources to Azure Infrastructure Services.

Azure AD Domain Services for Cloud-only:



Azure AD Domain Services for Hybrid:



You can find more information about Azure Active Directory Domain Services (AADS) here: <https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-overview>

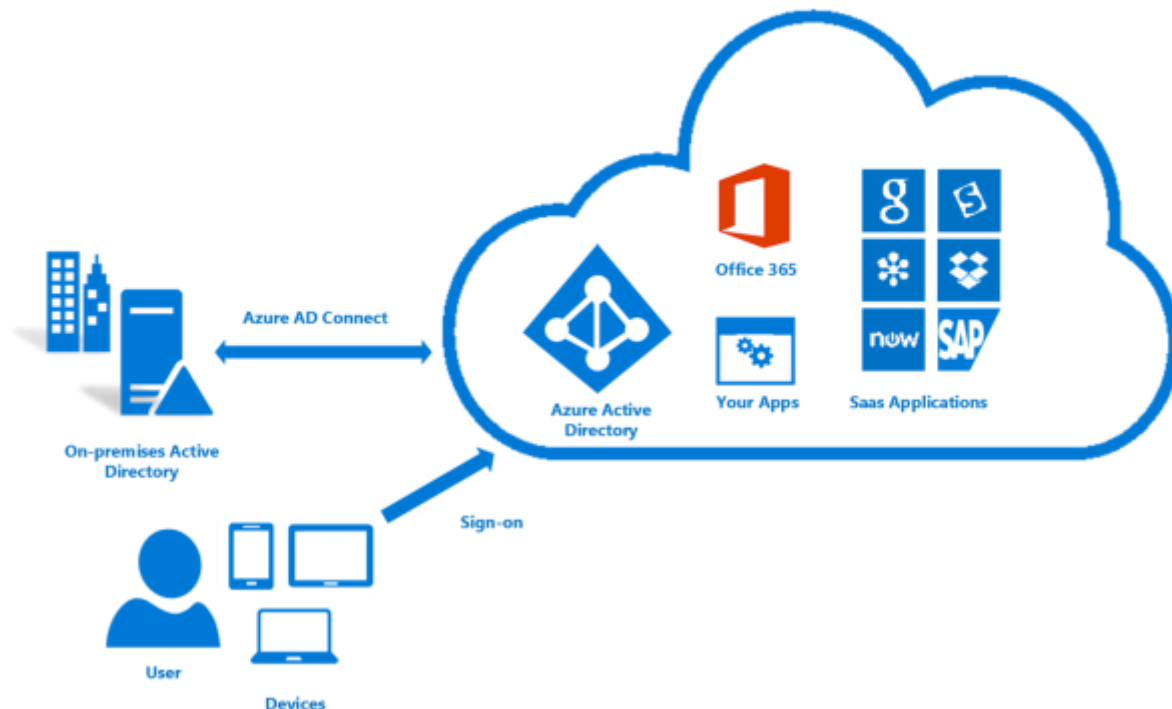
Azure AD Connect

When implementing Azure some organizations already have an identity system on-prem. It's crucial to integrate this on-prem system with the Azure identity one. This is accomplished by implementing Azure AD Connect. Azure AD Connect integrates your on-premises AD with Azure AD providing a common identity for accessing both cloud and on-premises resources. Users and organizations can take advantage of using a single identity to access on-premises applications and cloud services, such as Office 365.

To make this integration possible, Microsoft provides the Azure AD Connect tool, and when it's installed and configured on a DC, it synchronizes the local identities found in the on-premises AD to the Azure AD.

You can download Azure AD Connect at: <https://www.microsoft.com/en-us/download/details.aspx?id=47594>

What is Azure AD Connect?



Azure AD Connect is the Microsoft tool designed to meet and accomplish your hybrid identity goals. It provides the following features:

- Password hash synchronization**
 A sign-in method that synchronizes a hash of a user's on-premises AD password with Azure AD.
- Pass-through authentication**
 A sign-in method that allows users to use the same password on-premises and in the cloud but doesn't require the additional infrastructure of a federated environment.
- Federation integration**
 Federation is an optional part of Azure AD Connect and can be used to configure a hybrid environment using an on-premises AD FS infrastructure. It also provides AD FS management capabilities such as certificate renewal and additional AD FS server deployments.
- Synchronization**

Responsible for creating users, groups, and other objects. As well as, making sure identity information for your on-premises users and groups is matching the cloud. This synchronization also includes password hashes.

- **Health Monitoring**

Azure AD Connect Health can provide robust monitoring and provide a central location in the Azure portal to view this activity.

Integrating your on-premises directories with Azure AD makes your users more productive by providing a common identity for accessing both cloud and on-premises resources.

Authentication methods

When the Azure AD hybrid identity solution is your new control plane, authentication is the foundation of cloud access. Choosing the correct authentication method is a crucial first decision in setting up an Azure AD hybrid identity solution. Implement the authentication method that is configured by using Azure AD Connect, which also provisions users in the cloud.

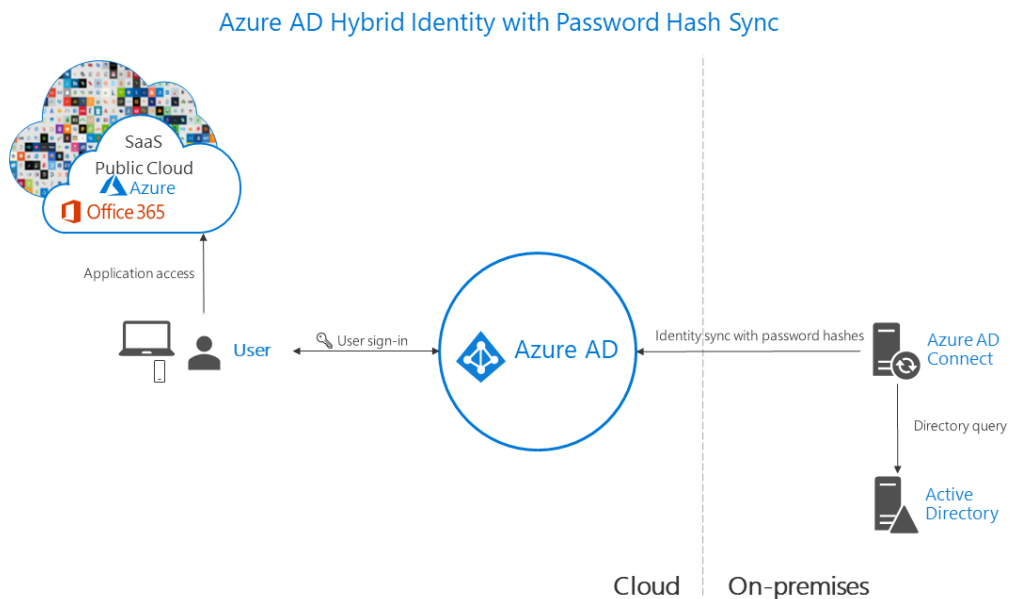
To choose an authentication method, you need to consider the time, existing infrastructure, complexity, and cost of implementing your choice. These factors are different for every organization and might change over time.

At the time of writing, Azure AD supports the following authentication methods for hybrid identity solutions:

Cloud authentication

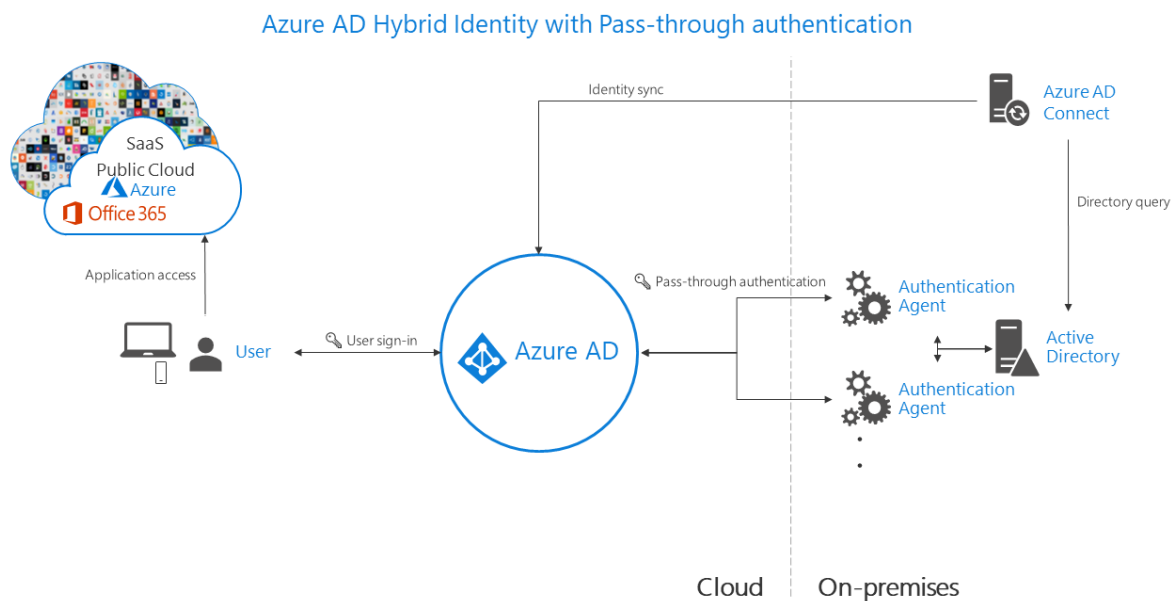
When you choose this authentication method, Azure AD handles users' sign-in process. Coupled with seamless single sign-on (SSO), users can sign in to cloud apps without having to re-enter their credentials. With cloud authentication, you can choose from two options:

Azure AD password hash synchronization.



The simplest way to enable authentication for on-premises directory objects in Azure AD. Users can use the same username and password that they use on-premises without having to deploy any additional infrastructure. Some premium features of Azure AD, like Identity Protection and Azure AD Domain Services, require password hash synchronization, no matter which authentication method you choose.

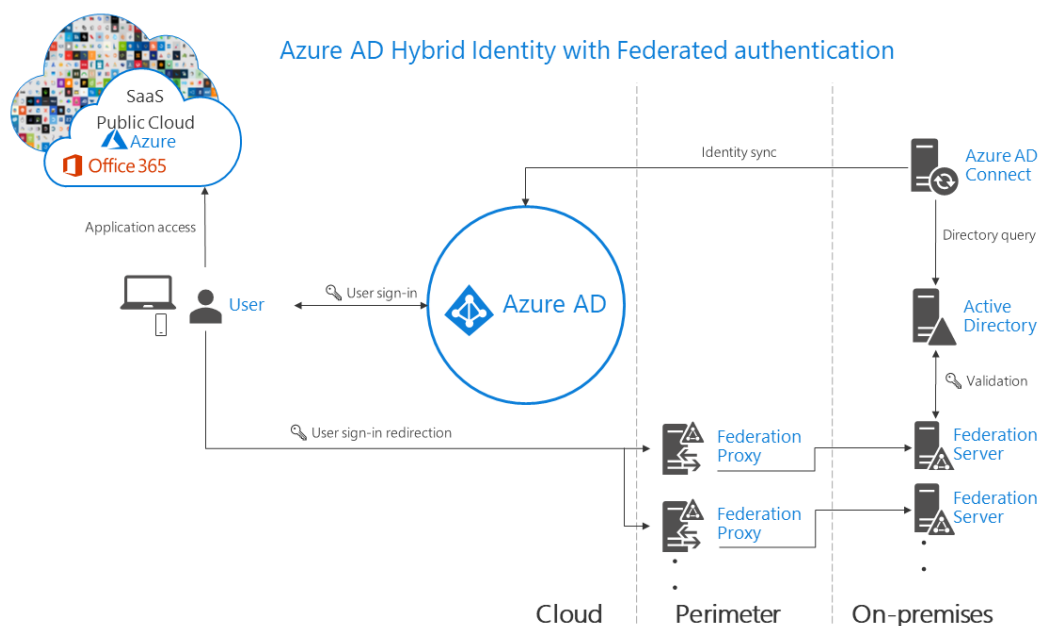
Azure AD Pass-through Authentication



Provides a simple password validation for Azure AD authentication services by using a software agent that runs on one or more on-premises servers. The servers validate the users directly with your on-premises Active Directory, which ensures that the password validation doesn't happen in the cloud.

Companies with a security requirement to immediately enforce on-premises user account states, password policies, and sign-in hours might use this authentication method. For more information on the actual pass-through authentication process, see [User sign-in with Azure AD pass-through authentication](#).

Federated authentication



When you choose this authentication method, Azure AD hands off the authentication process to a separate trusted authentication system, such as on-premises Active Directory Federation Services (AD FS), to validate the user's password.

The authentication system can provide additional advanced authentication requirements. Examples are smartcard-based authentication or third-party multifactor authentication. For more information, see [Deploying Active Directory Federation Services](#).

The following section helps you decide which authentication method is right for you by using a decision tree. It helps you determine whether to deploy cloud or federated authentication for your Azure AD hybrid identity solution.

You can find more information about Azure Active Directory Connect here:
<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect>