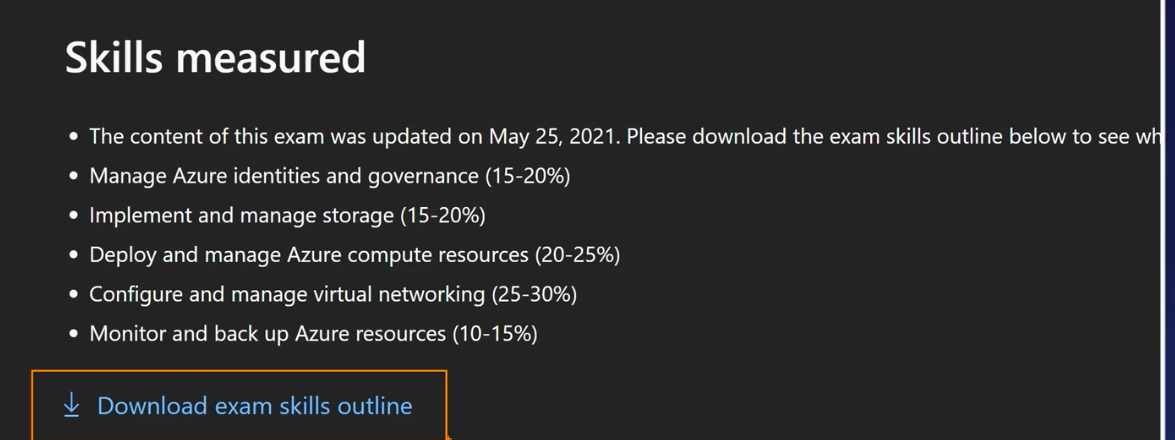
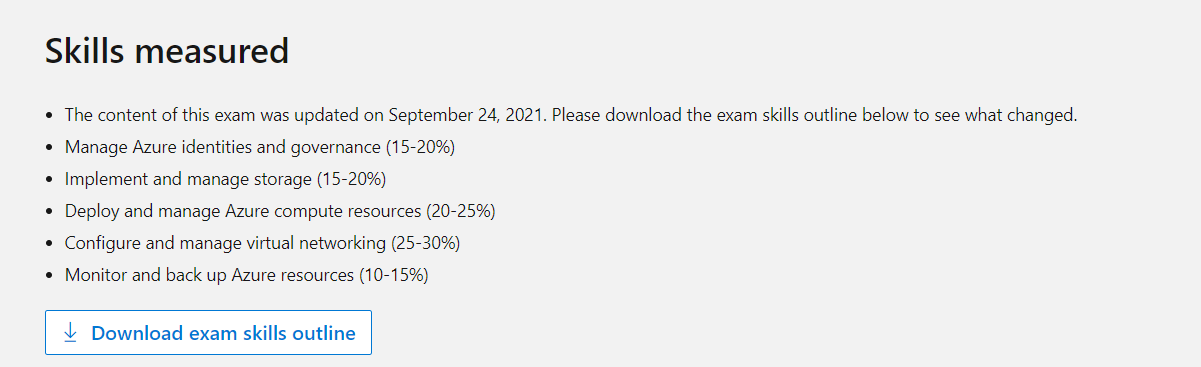
ITProTV



May 30 2022



# Manage Azure identities and governance (15–20%)

## Manage Azure Active Directory (Azure AD) objects

**create users and groups**

**create administrative units**

**manage user and group properties**

**manage device settings**

**perform bulk user updates**

**manage guest accounts**

**configure Azure AD join**

**configure self-service password reset**

## Manage role-based access control (RBAC)

* create a custom role
* provide access to Azure resources by assigning roles at different scopes
* interpret access assignments

## Manage subscriptions and governance

* configure Azure policies
* configure resource locks
* apply and manage tags on resources
* manage resource groups
* manage subscriptions
* manage costs
* configure management groups

# Implement and manage storage (15–20%)

## Secure storage

* configure network access to storage accounts
* create and configure storage accounts
* generate shared access signature (SAS) tokens
* manage access keys
* configure Azure AD authentication for a storage account
* configure access to Azure Files

## Manage storage

* export from Azure job
* import into Azure job
* install and use Azure Storage Explorer
* copy data by using AZCopy
* implement Azure Storage replication
* configure blob object replication

## Configure Azure files and Azure Blob Storage

* create an Azure file share
* create and configure Azure File Sync service
* configure Azure Blob Storage
* configure storage tiers
* configure blob lifecycle management

# Deploy and manage Azure compute resources (20–25%)

## Automate deployment of virtual machines (VMs) by using Azure Resource Manager templates

* modify an Azure Resource Manager template
* configure a virtual hard disk (VHD) template
* deploy from a template
* save a deployment as an Azure Resource Manager template
* deploy virtual machine extensions

## Configure VMs

* configure Azure Disk Encryption
* move VMs from one resource group to another
* manage VM sizes
* add data disks
* configure networking
* redeploy VMs
* configure high availability
* deploy and configure virtual machine scale sets

## Create and configure containers

* configure sizing and scaling for Azure Container Instances
* configure container groups for Azure Container Instances
* configure storage for Azure Kubernetes Service (AKS)
* configure scaling for AKS
* configure network connections for AKS
* upgrade an AKS cluster

## Create and configure Azure App Service

* create an App Service plan
* configure scaling settings in an App Service plan
* create an App Service
* secure an App Service
* configure custom domain names
* configure backup for an App Service
* configure networking settings
* configure deployment settings

# Configure and manage virtual networking (25–30%)

## Implement and manage virtual networking

* create and configure virtual networks, including peering
* configure private and public IP addresses
* configure user-defined network routes
* implement subnets
* configure endpoints on subnets
* configure private endpoints
* configure Azure DNS, including custom DNS settings and private or public DNS zones

## Secure access to virtual networks

* create security rules
* associate a network security group (NSG) to a subnet or network interface
* evaluate effective security rules
* implement Azure Firewall
* implement Azure Bastion

## Configure load balancing

* configure Azure Application Gateway
* configure an internal or public load balancer
* troubleshoot load balancing

## Monitor and troubleshoot virtual networking

* monitor on-premises connectivity
* configure and use Azure Monitor for Networks
* use Azure Network Watcher
* troubleshoot external networking
* troubleshoot virtual network connectivity

## Integrate an on-premises network with an Azure virtual network

* create and configure Azure VPN Gateway
* create and configure Azure ExpressRoute
* configure Azure Virtual WAN

# Monitor and back up Azure resources (10–15%)

## Monitor resources by using Azure Monitor

* configure and interpret metrics
* configure Azure Monitor logs
* query and analyze logs
* set up alerts and actions
* configure Application Insights

## Implement backup and recovery

* create a Recovery Services vault
* create a Backup vault
* create and configure backup policy
* perform backup and restore operations by using Azure Backup
* perform site-to-site recovery by using Azure Site Recovery
* configure and review backup reports

**The exam guide below shows the changes that were implemented on September 24, 2021.**

ITPROTV Course

User Source – Azure AD(cloud only identities), Microsoft Account(Used to create subscription), Windows Server AD (From on premises), Guest

Create a user or invite user (Guest)

On Premise accounts cannot be edited in Azure Active Directory

Azure Cli – **az** ad user create

Powershell - Connect-azureAD

Creating User via powershell needs 4 parameters. Displayname, password profile, upn and mailnickname

Deleted users are available for 30 days

### Create and Manage Groups

Group types – Security and Microsoft 365

Security – Assign permissions, roles and it’s a main type of group. Nested groups.

Microsoft 365 – Shared mailboxes, access to Sharepoint . Only users can be added.

Membership type for groups – Assigned, dynamic user and dynamic device

Assigned – Specify who is the member of the group.

You cannot change the group type

You can change the membership type

Dynamic Users – Conditional rules.

Dynamic Device – Conditional rules

Via Azure Cli - Create a group – az ad group create –display-name “blaa” –mail-nickname “blaa”

Via Azure PS – Connect-AzureAD | New-AzureADGroup -**DisplayName**”” -**MailEnabled** $value -**SecurityEnabled** $value -**MailNickName** “NotSet”

Security Enabled – AD group. If this is set to false then you will create Office 365 group

### Manage Guest Account

Access to people who don’t belong to organizations  
Invite them to organization  
We need the guest email address and invite

Can be added to roles, groups

Perform Bulk User Updates

BulkRestoring users – Get object ID of the users to restore in the template and upload bulk restore

30 days to restore from deleted items

Configure Azure AD Join

MS Learn

4 Tooling Options are available

1. Azure Portal
2. Azure Cli
3. Azure Powershell
4. Azure Cloud Shell

Azure Cloud Shell

* Linux users – Bash experience
* Windows users – PowerShell

Azure PowerShell – Linux, MacOS, Windows

* Can be added to Windows Powershell or Powershell Core
* Used to manage resources
* Interactive Mode (One command at a time) or Scripting Mode (Multiple commads)

AZ is the formal name for Azure PowerShell Module

Using AZ you can work with the following

1. Resource Groups
2. Storage
3. VM
4. Azure AD
5. Containers
6. Machine Learning

Azure CLI – Linux, MacOS, Windows

Azure CLI is a cmd line program

Admins can use terminal, cmdline or Script instead of web browser

Azure CLI is also available in browser in Azure Cloud Shell

Interactive or Scripted

Commands in CLI are structured in groups and subgroups (Storage – (account, blob, share, queue))

Key – To find commands use az find (az find blob) or if you need help az storage blob –help

Azure Management Options

1. Azure Portal – you cannot automate repetitive tasks. Time consuming and prone to error
2. Azure Powershell and CLI – Cross platform. For CLI – First login using az login command
3. Azure Cloud shell
4. Azure Mobile App – Monitoring and managing resources from mobile. IOS, Android,Phone/tab

To switch to powershell core from Bash – Type pwsh

Bash defaults to Azure CLI – az

Cloud shell has developer tools, text editors and others.

When accessing Cloud Shell – You need to create a Azure Storage Account.

This Storage area stores any scripts, data and used as your $HOME folder.

Azure Mobile App

* Check status and metrics
* Alerts and notifications
* Diagnose and fix issues
* Azure Alerts
* Start, stop and restart vm or web app
* Connect to vm
* RBAC management
* Run saved scripts

Programmatically control using REST API, Azure SDK

Open support tickets using Help and Support Options in the Portal

Azure Advisor – Recommend HA, Security, Performance, Operation Excellence and cost.

**Azure Resources and Resource Groups**

Scenario – No Standardization | Critical resources deleted | Who owns which resources | No organization of company resources

Azure Resource Manager: Work with resources in your solution as a group

* Deploy, Update or delete all resources in a single operation
* Template for deployment
* Provides Security, Auditing and Tagging to manage resources after deployment
* Consistent management layer – Do tasks through 5 options
  + Azure PowerShell, Azure CLI, Azure Portal, REST API and Client SDKs
* Deploy resources in consistent state
* Declarative templates
* Correct order of deployment by defining dependencies
* Apply Access control to all services in RG. RBAC is native to management platform.
* Apply tags to resources to logically organize all the resources in your subscription
* Same tag resources billing cost view

ARM Templates – Define and deploy infra via declarative syntax

Same lifecycle resource grouping

**Azure Resource Terminology**

Resource – Manageable item in Azure

Res group – Container for related resources.

Resource provider – A service that provides resource. (Microsoft.Compute – provides VM resource)

Template – JSON file with resource definition, dependencies. Consistent and repeated deployment

Declarative syntax – state the intention

**Resource Groups**

Logical collection of resources

Rules:

1. Resources can only exist in only one resource group
2. Resource Groups cannot be renamed
3. Resource groups can have many different services
4. Resource groups can have resources from many different regions
5. Resource groups cannot be nested

Resources in RG must have same lifecycle

RG can be used to scope access control for admin actions

A resource can interact with another resource in another RG

Creating RG – Provide location for that RG

Resource Manager Locks

Prevent accidental deletion of resources in azure

Lock can be done for Subscription, Resource Group or Resource

Locks are inherited by child resources

Lock types:

1. Read Only Lock – Prevent any changes to resources
2. Delete Lock – Prevent deletion only

Only Owner and User Access Administrator role can create or delete management locks

Reorganize Azure Resources

1. While moving resources – both source and destination groups are locked during operation
2. Write and delete operations are blocked until move is finished
3. Resources are available during move
4. Child resource is moved automatically with parent resource. Cannot be independently moved
5. Can be moved to another resource group, another subscription, and another region
6. Dependent resources must be moved along

Deleting Resources and Resource Group – Remove-AzResourceGroup

Deleting RG deletes all resources within

Resource Limits – Usage + Quotas

Tracked per subscription.

If you reach a quota cap, request to increase via Help and Support

Max limit reached – limit cannot be increased

**Configure Resources with ARM Templates – Faster and repeatable**

Scenario – Ensure VM deployments are consistent across the organization

Template benefits –

1. Consistency – Common language for deployment.
2. Express complex deployment – Deploy multiple resources in correct order
3. Reduces manual error prone tasks
4. Code – IaaC
5. Reusable
6. Linkable – link templates together
7. Simplify orchestration – deploy template to deploy resources

Template parameter – 256 limited

Azure Bicep – Domain specific Language. Uses declarative syntax.

Use bicep instead of json for ARM templates.

Transpilation – convert source code from 1 language to another

Bicep converts template to json

Bicep –

Simpler Syntax, Reference parameters and variables directly. Refer properties of resources directly instead of reference statements.

Modules, break complex template deployments into small modules. Refer in main template. Reuse

Auto dependency Management – Auto detects dependency b/w resources.

Type validation, intellisense

Azuredeploy.json – defines resources

Azuredeploy.parameters.json – provides values the template needs

Azure provides 3 administration tools – Win, linux, macos

The azure portal – cross platform

Azure CLi – cross platform

Azure PowerShell – cross platform

Windows Powershell and PS 7.x can be installed on Wind, MacOS and LInux

To run AZ powershell cmdlets you have to install Azure Powershell Module

Linux and macOS – Package Manager to install powershell core

Macos – homebrew package manager

Azure VM Status – Remove, Start,Stop, Restart, Update

User – user2022

Pass – lm$­­

Azure CLI – Linux, macOS and windows

Interactive or Scripited

Commands are structured in groups and subgroups

Login – az login

Create a resource group before creating any resources

Az find - helps finding commands

No need to sign in if you are already using cloud shell

Query – az group list –query “[?name == ‘value’]”

Resource cost depends on the app service plan for web apps.

Service plan determines the region used for the app datacenter, number of vms and pricing tier

To create a web app –

1. Create a service plan -name,rg,location,sku
2. Create web app – name,rg, planname
3. Optionally you can integrate github for deployment

­

JSON ARM Templates – Deploy infrastructure to Azure Consistently and Reliably

Declarative and reusable

Bicep is new language for defining azure resources. Use bicep instead of JSON

ARM templates – declare what you intend to deploy. You specify, resources and its properties.

Benefits :-

* Automate deployments using IaC
* Idempotent – deploy same template many times and get same resource types in same state
* RM orchestrates the deployment, so resources are in correct order
* Parallel resource creation
* Finishes faster than scripted deployment
* RM has built in validation. Checks template if will it succeed
* ARM templates can be broken down and linked at deployment time
* You can nest templates
* CI CD integration of ARM Templates via Azure Pipelines

Azure DevOps + ARM Template tasks = continuously build and deploy projects

ARM Template file structure

<https://docs.microsoft.com/en-us/learn/modules/create-azure-resource-manager-template-vs-code/2-explore-template-structure?tabs=azure-cli>

Required Sections:

1. Schema
2. contentVersion
3. resources

Optional Sections:

1. apiProfile
2. parameters – parameter file, cmd parameter or in azure portal
3. variables
4. functions – user defined functions
5. output – end of deployment return values

3 ways to deploy ARM template to Azure

1. Local Template
2. Linked Template
3. Continuous Deployment pipeline

To add resources to template – Know resourceprovider and its types of resources

{resource-provider}/{resource-type} – Microsoft.Storage/StorageAccounts

If you set AZ-Default – You can omit the parameters in later cmdlets

To deploy an ARM Template – you need a Resource Group and deployment file

*New-AzResourceGroupDeployment -Name $deploymentname -TemplateFile $template*

Instead of hardcoding values in the template file – Use parameters.

Parameters make the template reusable

1 template has 265 parameters

Parameter definitions can use template functions

Allowed parameters – String, Boolean, int, securestring, object, secureobject, array

Use secureString for passwords and secureObjects for sensitive data

Creating Parameter

1. Create parameter definition on the parameters section of ARM template
2. Use the parameter definition on the resources section – syntax is [parameters(‘parametername’)]. Use parameter function here
3. Deploy template by giving parametername along

*New-AzResourceGroupDeployment -Name $deploymentname -TemplateFile $template -parametername*

In Outputs – *reference* function gets the runtime state of the resource

In ARM templates – resources will be created only if they didn’t exist and updated only if there is a change

Lab –

1. Add a parameter to define the AZ storage account name during deployment
2. Add a parameter to define what storage account sku is allowed
3. Define which one to use for this deployment in sku
4. Add output

**Azure Active Directory – Free, Premium P1, P2, M365 Apps**

On premise uses – NTLM and Kerberos

AAD uses – OpenID, Oauth, SAML, WS Federation

Every M365, Azure and Dynamics CRM tenant is an Azure AD tenant

**Terminologies**

Identity – object that gets authenticated. Users, applications or other servers

Azure tenant/directory – dedicated and trusted instance of Azure AD.

Account – identity with data

**Characteristics of Azure AD**

Identity solution – Designed for Internet based apps by using http and https com., AAD is primary id solun

REST API Querying – Since AAD is http/https based, we cannot use ldap. AAD uses REST API over http/s

Com protocols – No Kerberos and no LDAP, so uses SAML, Open ID, WS fed for **authN**, Oauth for **authZ**

Federation service and 3rdparty services like Facebook

Flat Structure – No OU or GPO.

|  |  |  |  |
| --- | --- | --- | --- |
| Free | Premium p1 | Premium P2 | M365 Apps |
| Comes with AZ subscription  SSO available  Only 500000 directory objects | Available through  1. Enterprise Agreement  2. Open Volume License Program  3. Cloud Solution providers program  SSO available  Hybrid  Group access mgmt  CA | Available through  1. Enterprise Agreement  2. Open Volume License Program  3. Cloud Solution providers program  SSO available  Hybrid  Group access mgmt  CA  Identity Protection – risk based CA to apps and data  Identity Governance  PIM – discover, restrict and monitor admins and their access. JIT | SSO available  MFA, sspr for cloud users,branding, gp access mgmt |

**Azure AD Join –**

To Provide access to organizational apps and resources

To simplify windows deployments of work owned devices

Benefits :

1. SSO – SSO to azure managed SaaS apps and services. No additional authN prompts.

SSO works even if not connected to domain network

1. Enterprise state of roaming users settings across AZ Joined devices
2. Microsoft Store for business
3. Windows Hello – Secure and convenient access to work resources
4. Restriction of access – to apps from only devices that meet compliance policy
5. Seamless access to on prem resources – when device has line of sight to on prem DC

**Connection options – 1. Registration 2. Joining**

Register – Manage device identity.

Joining – Sign in using work or school account

Registration+MDM – CA can be applied

**Self Service Password Reset**

Choose None, Selected or All

Choose Authentication methods types. 1 minimum. Email, Text or Code, *set of security questions(less secure)*

Azure Administrators can always reset their passwords no matter what is configured

**Azure User Account**

Cloud Identity – Exist in Azure AD. Can be in Azure AD or External Azure AD.

Directory Synchronized identities -On Prem AD accounts.

Guest User – Outside Azure. Other cloud providers, xbox live account. Invited users

Deleted users can be restored for 30 days

Sign in and Audit log information is available

Users can be added from Ms 365 Admin center, Microsoft Intune admin console and CLI

To create user in azure portal – Have Global Administrator or User Administrator Permission

Bulk user upload is possible via powershell and portal

**Azure group**

Security Groups – Needs Azure AD Administrator

M 365 Groups – Collaboration opportunities. Shared mailbox, calendar, files, sharepoint site

Users and Admins can use M365 groups

Adding members

1. Assigned – add and have unique permission
2. Dynamic user –
3. Dynamic device (security groups only) –

Administrative Units

To restrict administrative scope

Can be managed using Portal, Pwsh and scripts or MS Graph

Be a Global Administrator or Privileged Role Administrator

Admin units apply scope only to management permission

Members and admins can browse other users groups etc outside the admin unit

Contributor – Cannot assign roles RBAC, manage assignments in AZ Blueprints or share image galleries

**Azure Subscriptions**

Determine the correct region to locate Azure services.

**Region** – Atleast one but potentially many datacenters. DCs are in close proximity and low latency

60+ regions and 140 countries

Data residency and compliance and resiliency options

Some VM sizes and storage types are only available in some regions

Global services AAD, MS Azure Traffic Manager and Azure DNS – Needs no region to be selected

Regions in same geography are paired. Except Brazil south

**Region Pairs**

Physical Isolation, Platform provided replication (Geo Redundant Storage), Region recovery order, Sequential updates, Data residency

**Azure Subscription**

Logical unit of Azure services linked to Azure account – like development, production, testing

Billing is done per subscription

Programmatic access might require subscription id

Ways to get Azure Subscription :

1. Enterprise Agreement

Make upfront monetary commitment

99.95 SLA monthly

1. Reseller

Buy azure via Open Licensing Program – simple, flexible from MS reseller

1. Partners

Partner can design and implement

1. Personal Free

Free trial account.

Azure Accounts – Work or School or Microsoft Account, trusted by Azure AD

Types of subscriptions

1. Free

Credit for first 30 days

Free product access for 12 months

Access to more than 25 products always free

Need phone, credit card and MS account

1. Pay as you go

Charged monthly for the services used

1. Enterprise agreement

One agreement, discounts new licenses and Software Assurance

1. Student

12 months credit, no credit card.

Azure Cost Management

Use MS Cost Management and Billing for billing administration and Manage billing access to cost

Monitor and control azure spending

Optimize azure resource usage

Usage pattern and analytics

Reports for internal and external cost for usage and az marketplace charges

Predective analytics

Cost mgmt uses azure mgmt groups, budgets and recommendations

Integration with external systems can be done using Azure Portal or API for export automation

Automated billing data export and scheduled reports are available.

\*Cost analysis – explore and analyze org cost

\*Budgets - Prevent cost, set threshold or limits

\*Recommendations – identify idle and underutilized resources

\*Export cost mgmt data – store csv in azure storage

Resource tagging

Logically organize by category.

Retrieve all resource in subscription with tag name and value from different resource groups

Group billing data

Tags can be created via powershell, portal and cli

Azure policy ensures that the proper tags are assigned when resources are provisioned.

* Each resource or resource group can have a max of 50 tag name/value pairs
* Tags to resource groups are not inherited by the resources

Cost Savings

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Reservations | Budgets | Az Hybrid benefits | Azure credits | Azure regions |
| Pay ahead saving  1 or 3 years  Upto 72% saving on pay as you go  Billing discount | Track spending progress  Thresholds  Notifications | Bring on prem server or sql license to azure  Azure hybrid benefit saving calculator  Customers with software assurance | Monthly credits | Region to region pricing differs |

**Azure Policies –**

Use case - Regulations and Compliance rules

Manage subscription and governance

Management Groups

To effectively manage access, policies and compliance for multiple subscriptions. Use mgmt groups

MG provide a level of scope above subscriptions

Subscriptions are organized into containers called MGs

Governance conditions can be applied to MGs

MGs enable

* Custom hierarchy and grouping for az subscriptions
* Policy targeting
* Spend budgets across subscriptions and inheritance down the hierarchy
* Compliance and cost reporting by organization

Subscriptions inside the MG inherit the conditions applied on MG

Policy applied to MG is inherited to the MG inside it and subscriptions and resources under it

**Azure Policies service**

Used to create, assign and manage policies

For compliance and SLA rules are enabled on the resources by policies

Az policy runs evaluation and scans for resources that are non compliant

Advantages of azure policy – Enforcement, compliance, Scaling and remediation

Policy initiatives – Multiple Policies and aggregate policy

Define exclusion using scale

Policy is important when

1. Multiple teams are operating
2. Multiple subscription
3. Standardize/enforce cloud resources
4. Manage regulatory compliance, cost control, security or design consistent

Use case of Azure Policy

1. To specify resource types the organization can deploy
2. Specify set of VM SKU that can be deployed
3. Restrict deployment location
4. Enforce required tag and value
5. Audit if az backup is enabled for VMs

Implement azure policies

1. Browse policy definition – what to evaluate and what actions to take.

Every definition has condition using which it is enforced

Also has effect that takes place when cond Is not met

Example – Prevent vm form being deployed it it has public IP

1. Create initiative definition – Set of policy definitions. Helps tracking compliance state.

Example – Ensuring branch office is compliant

1. Scope the initiative defninition – Limit the scope to MG, resources group or subscription
2. View policy evaultation results – Evaluate the state of compliance. Excemptions

If you need geo compliance – Enable Allowed location policy

Import policy definitions from github

**RBAC**

AZ RBAC is an authorization system built on ARM

Provides fine grained access management of resources in Azure

Concepts:

1. Security principal – object that is requesting access. User, group, service principal, managed idty
2. Role definition or role – Collection of permisisons. Reader, contributor, Owner, User access admin, VM contributor
3. Scope – MG, Subscription, RG, resources
4. Assignment – Attaching a role defninition to SP for a scope.

Deny assignment are readonly and only be set by azure

Role assignments, Deny Assignments and Classic Administrators

Control to resources are done by role assignments

Role assignment key elements are security principal (who), role definition (what) and scope (where)

**Role Definition**

A role definition in Azure is a collection of permissions with a name that you can assign to a user, group, or application.

Set of properties defined in a JSON file. – Actions, No actions and data actions

/ means all scopes

Owner action - \* means allow all actions

Contributor allow all but delete or writing – NotActions -> Microsoft.Authorizatoin/\*/Delete,

Microsoft.Authorization/\*/write

Microsoft.Authorization/elevateAccess/Ation

Reader allow all read -> \*/read

1. Set the actions
2. Scope the role – Where the access is applied to.
3. Do Role assignment

Scoping the role can be done to Subscriptions, ResourceGroups or Resources

\*/subscriptions/[sub id]

\*/subscriptions/[sub id/resourcegroups/[rgname]

\*/subscriptions/[sub id/resourcegroups/[rgname]/[resources]

Multiple subscriptions will be like below

“/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e”, “/subscriptions/e91d47c4-76f3-4271-a796-21b4ecfe3624”

Make role available for network resource group

“/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e/resourceGroups/Network”

**Azure RBAC**

Azure AD and Azure RBAC work together

Every Azure subscription is associated with a single Azure AD directory

When you disable an on-premises Active Directory account, it automatically loses access to all Azure subscriptions connected with Azure AD

With Azure RBAC, you can grant the exact access that users need to do their jobs

A resource inherits role assignments from its parent resource.

A role assigned at a parent scope also grants access to the child scopes contained within it.

Built in roles

Owner – Has full access to all resources. Can delegate access to others

Contributor – Create and manage resources but cannot grant access to others

Reader – can view existing az resources

User access admin – lets u manage user access to azure

Scope can be applied to multiple levels – Parent scope access is inherited to child.

To grant access you create a role assignment. To revoke access, you remove role assignment

Changes to RBAC are stored in Azure Activity Log

**Classic subscription administrator roles vs Azure roles and Az AD Roles**

Azure Resource Manager roles should be used instead of Classic administrator roles.

Classic subscription:

* Account Administrator
* Server Administrator
* Co-Administrator

Role Based Access Control:

* Newer authorization system
* Provides fine grained access management
* Has many built in roles
* Roles can be assigned to different scopes
* Create own custom roles
* Manage access to az resources
* Scope can be specified for MG, Sub, RG or resources
* Role info can be accessed from Portal, CLI, PWSH,ARM, REST API

Azure AD Roles

* Manage access to Azure AD resources
* Scoped to tenant level
* Role info is accessed in AZ admin portal, M365 admin portal, Microsoft Graph AzAD Powershell

Inbuilt Azure Roles

* Owner- Has full access to all resources

Right to delegate access to others

Service admin and co administrator are assigned the owner role at subscription scope

* Contributor- Create and Manage all types of Azure resources but can’t grant access to others
* Reader- Can view existing az resources
* User Access Administrator- Manage user access to az resources

Azure AD User Accounts

User account access – has type of user, permissions and ownership of individual objects

To create a new user in Azure AD – you need Global admin or User Admin. New-azureaduser or az ad user create

Guest User – Restricted access to az ad organization permission

Send email invitiation or send a direct link to an app

Work, school or social id login

By default az AD member can invite guest user. Can be disabled by user admins.

Remove user – Remove-AzureADUser / az ad user delete

Accounts deleted are in suspended state for 30 days

**Manage App and Resources using AZ AD Groups**

AAD helps manage Cloud App, On Prem App and resources using Organization groups.

Resources can be in Azure AD or can be external to the organization like SaaS apps, Azure Services, SharePoint sites and On prem resources

Azure AD Access Management

Az AD roles – Users, groups, billing,licensing,app registration etc…

RBAC for Az resources – Manage access to VMs, SQL DB, or Storage.

Assignment

1. Direct Assignment
2. Group assignment
3. Rule based assignment – Based on country

You can Change the group type to Dynamic only if you have azure premium license

You need Premium license to create rule based group or dynamic user

B2B Collaboration

Invite user to Azure AD organization, group or app.

User is added as guest

In B2B no need to manage external users. External users are managed in their companies

Federation is more complex. A trust needs to be established with other organisations, or a collection of domains, for shared access to set of resources.

In Federation Users needs to be authenticated against ADFS. For people outside internal network, we need to setup web application proxy.

With B2B authentication is directly done through azure.

**Azure Self Service Password Reset**

Methods to use for authentication – 6 methods

1. Mobile App Notification
2. Mobile App Code
3. Email
4. Mobile Phone – code to phone in sms or automated call (Not recommended)
5. Office Phone – automated call and press #
6. Security question (Least preferred)

In free and trial Azure AD organizations, phone call options aren't supported.

Specify minimum number of authentication methods.

Specify min number of questions that the user must setup and minimum correct answer

A strong, two-method authentication policy is always applied to accounts with an administrator role, regardless of your configuration for other users.

The security questions method isn't available to accounts that are associated with an administrator role.

Notifications:

Notify users on password reset

Notify all admins when other admins reset password

License Requirements

Forgot password/expired – SSPR is for P1 P2, M365 Apps and M365

In Hybrid – password writeback to on prem ad must be enabled. Writeback is with p1, p2 and M365 app for business

SSPR Deployment Option

1. Azure AD connect
2. Cloud sync – Merger in another domain company can use this. Cloud sync provide High availability.

SSPR Scope

1. Disabled
2. Enabled
3. Selected

SSPR Configuration

1. Enable SSPR
2. Select authentication methods
3. Registration and Number of days before reconfirming authentication information
4. Setup notifications. User/Admin pass resets
5. Customization

**Implement and manage storage in Azure**

Azure Blob storage or object storage– Store large amounts of unstructured data. Like text or binary data, documents, application installers, media etc...

Use case – Media company with video libraries. Accessed thousands of times a day

Serving images directly on browsers, storing files for dfs, streaming AV, DR storage, archiving, analysis storage of data

Improve performance and Reduce cost – Use access tiers

Older videos – Lifecycle management plan

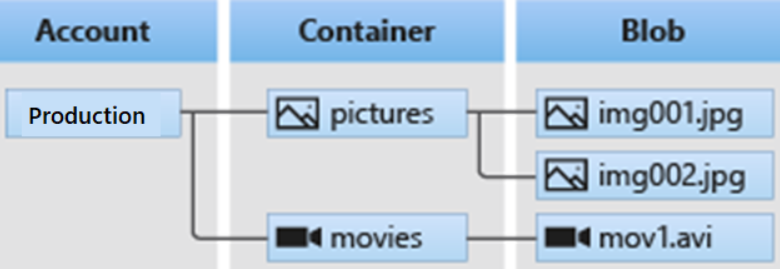
Failover – replication

Blob service resources

Account -This is the storage account

Containers – folder like grouping for blobs

Blob – objects inside the container. Must be inside a container.



Data in the container is private by default and accessible to account owner only.

**Public access level**

Private – no anonymous access to container and blob

Blob – anonymous read access public for blob only

Container – anonymous public read and list access to entire container

Create blob container via portal or New-AzStorageContainer

Azure blob access tiers

Hot – frequently accessed

Cool – infrequently accessed and stored atleast 30 days. Accessing data a bit expensive

Archive – 180 days archive, most cost effective. Accessing expensive than hot/cool

The lifecycle management policy lets you:

1. Transition blobs to a cooler storage tier (hot to cool, hot to archive, or cool to archive) to optimize for performance and cost.
2. Delete blobs at the end of their lifecycles.
3. Define rules to be run once per day at the storage account level.
4. Apply rules to containers or a subset of blobs.

Blob object replication copies asynchronously according to the rules.

Blob contents, versions, metadata and properties are all copied source -dest.

Object replication use case:

1. Minimize latency
2. Increase efficiency for compute workloads
3. Optimizing data distribution
4. Optimizing costs – access tiers

Object replication considerations

1. Requires versioning on both source and destination
2. No snapshot replication support for blobs
3. Replicates only hot cool tier. Source / destination can be in different tiers. Archive tier not supported for replication
4. Replication policy with source/destination SA. Source container and dest container

Uploading BLOBs

Blobs can be any type and size.

3 types of blobs – Cannot be changed once the type is defined.

1. Block blobs – text, videos, images. Blocks of data assembled to make a blob
2. Append blobs – Optimized for append operations. Used for Logging scenarios
3. Page blobs – can upto 8 TB size. Efficient and frequent read/write operations. AZ VM uses page blobs as OS and data disks

Blob upload tools

1. Azcopy – cmdline tool
2. Az Storage data movement library - .net library
3. Az Data Factory – uses account key, sas, sp, mi or az resource authentications
4. Blobfuse – linux. Virtual filesystem driver
5. Azure data box disk – SSD for onprem to Azure transfer
6. Az import/export – export large data from SA to on prem. Uses hardisk
7. Storage explorer

Storage pricing - [Determine storage pricing - Learn | Microsoft Docs](https://docs.microsoft.com/en-us/learn/modules/configure-blob-storage/8-determine-storage-pricing)

1. Performance tiers – cost increases as the tier gets hotter. Cooler – per GB price decreases
2. Data access cost – cooler access price is high. Per GB price for reading data
3. Transaction cost – per transaction charge for all tiers. Cooler tier – high cost
4. Geo replication data transfer cost – per gb charge for data transfer
5. Outbound data transfer cost – per gb
6. Changing storage tier – cool to hot (charge equal to reading all data). Hot to cool (Charge equal to writing all data)

**Azure Storage:**

Offers – scalable object store for data objects, a file system service for cloud, messaging store, noSQL store.

* Durable and highly available
* Secure – encrypted by the service.
* Scalable
* Managed – MS handles all
* Accessible – http/s, SDK, Scripting pwsh, cli, portal, storage explorer

3 categories

1. Storage for VM – disks and files. Disks are persistent. Files are fully managed fileshares in cloud
2. Unstructured data – Blobs and data Lake store. Blobs are highly scalable, REST based cloud object store. Data lake store is Hadoop DFS as a service.
3. Structured data – Tables, cosmosdb, azure sql db. Tables are key/value, autoscaling noSQL Store. CosmosDB is globally distributed db service. AZ SQL is fully managed db as a service built on SQL

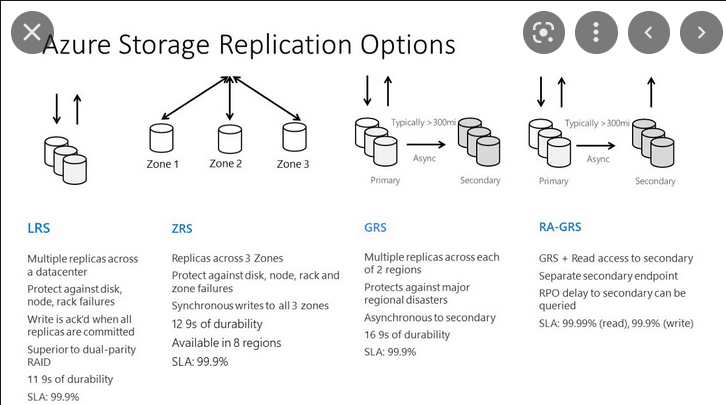
General purpose SA has 2 tiers

1. Standard – Magnetic drives HDD, lowest cost per GB. Good for storage with bulk storage requirements and infrequent data access
2. Premium - SSD drives, low latency performance. Good for Azure VM disk with I/O intensive app, db requirements

You can't convert a Standard storage account to a Premium storage account or vice versa. You must create a new storage account with the desired type and copy data, if applicable, to a new storage account.

Premium and Standard

Premium - only LRS



Azure Storage data services

1. Blobs – unstructured
2. Queues – store and retrieve messages. Q can be upto 64KB. Millions of messages, stores list of messages to be processed asynchrously
3. Files – Highly available network file shares. NFS or SMB support protocol. Rest and storage client library accessible. Can be accessed anywhere in the world using URL and includes shared access signature tokens SAS. SAS token allows access for a specific period of time.
4. Tables – Storing structured, non relational data.

All storage accounts are encrypted using Storage Service Encryption (SSE) for data at rest.

Kinds of storage accounts

1. General purpose v2 standard – LRS, GRS,ZRS, GZRS
2. Premium block blobs – LRS, ZRS
3. Premium file shares – LRS,ZRS
4. Premium page blobs - LRS

**Replication**

Azure storage always replicated.

Same datacenter, zonal, region, different region.



|  |  |  |  |
| --- | --- | --- | --- |
| LRS | ZRS | GRS | GZRS |
| Low cost replication  Least durability  Datacenter goes down then all are lost | Replicates data across 3 storage clusters in a single region | Data is replicated to secondary region.  16 9s durability  Storage scale unit – basic replication unit within DC.  LRS provides local replication.   1. GRS 2. RA GRS – read access from secondary region | ZRS + GRS  Replicated across 3 AZ availability zones in primary and secondary region.  16 9s |

Default endpoint url – storageaccountname.blob.core.windows.net. Custom domain can be used.

Azure storage does not support https with custom domain, Use CDN for that

Firewalls and Virtual Networks restricts access to the Storage Account from specific Subnets on Virtual Networks or public IPs.

Subnets and Virtual Networks must exist in the same Azure Region or Region Pair as the Storage Account.

Read-access geo-redundant storage is the default replication option. Geo-redundant storage (GRS) copies the data synchronously three times within a single physical location in the primary region using LRS. It then copies the data asynchronously to a single physical location in the secondary region.

The storage account name is used as part of the URI for API access, so it must be globally unique.

**Configure Storage Security**

Secure Storage

* Generating Shared Access Signature tokens. SAS
* Manage access keys
* Azure AD authentication

Encryption – All data written to azure storage is encrypted automatically using storage service enc SSE

Authentication – Azure AD and RBAC

Data in transit – Client side encryption, https or smb 3.0

Disk encryption – OS and data disk encrypted using Azure disk encryption

Shared Access Signature – Delegated access to data objects in az storage

Authorization options

Azure AD

Shared key – Relies on account access keys and other param., produces encrypted signature string that is passed on the request in the authz header

Shared access signatures – delegate to particular resource for specified time interval

Anonymous access to containers and blobs – make blob resources public at container or blob level.

Create SAS shared access signatures

SAS is a URI, this grants restricted access to az storage resources.

No need to give storage account key to clients. Instead distribute these SAS URI to clients­­

Account level SAS can delegate access to multiple SA

Start time and expiry time defined

SAS provides Account level and service level control

Account level – one or more storage account resource access

Service level – just one storage account resource access

IP ranges can be specified.

Protocol can be specified.

Stored access policy – service level control on server side.

Policy can be applied

Encryption

SSE – Azure storage service encryption – encrypts data at rest.

SSE automatically encrypts data before persisisting to azure managed disk, b, f, q tables

SSe enabled for all new and existing SA and cannot be disabled.

CMK – Azure key vault can manage encryption keys.

Create own key and store in key vault or use azure key vault api to generate enc keys

CMK more flexible and control. Create, delete, audit, rotate and access control

CMK can be used with SSE. SA and keyvault must be in same region but can be in diff subscriptions

**SAS best practices**

1. Use https
2. Use storage access policies – if you don’t want to regenerate storage account keys, with SAP you can revoke permissions.
3. Near term expiration times on unplanned SAS
4. Clients renew SAS automatically before expiration
5. SAS start time – set it in past or don’t set it
6. Specific resource to be accessed – minimum privilege
7. Validate data written using SAS
8. Monitor your application using storage analytics

SAS will change access based on permissions or duration by replacing the policy with a new one or deleting it altogether to revoke access.

The default network rule is to allow all connections from all networks.

Stored Access policies aren't the best solution for the production app.

Access keys provide unrestricted access to the storage resources, which is the requirement for production apps in this scenario.

**Configure Azure Files and File sync**

File storage – Offers shared storage for apps using smb protocol.

VMs and Cloud services shares via mounted shares

On premise app can also access file data in the share

Simultaneously access file storage share

Use case.

Replace on prem servers

Access anywhere – win, macos, linux.

Lift and shift

Azure file sync – replicate to on prem or cloud

Shared applications – settings, config files etc..

Diagnostic data – logs metrics, dumps etc..

Tools and utilities – storage

|  |  |
| --- | --- |
| Azure Files | Azure Blobs |
| Smb, nfs, rest, client libraries.  Access from anywhere  True directory objects  Accessed through file shares  Shared access across multiple vms | Client libraries, rest interface. Unstructured data  Access at massive scale in block blobs  Flat namespace  Accessed via containers  Az disks are exclusive to single vm |

File Share Tiers

Premium – only for premium storage accounts

Transaction optimized – premium level latency. File storage as backend store

Hot – general purpose file sharing, teamshares and az file sync

Cool - online archiving

Secure transfer required for connecting to file share means – allowing requests to SA by secure connection. Like https.

File share snapshots – backups or point in time capture. Read only copy of the data

Provided at the file share level.

Retrieval is provided at individual file level.

To delete a share – delete snapshots first

Snapshots are incremental.

Azure File Sync

Centralize file shares

Smb, nfs, ftps

Can have many caches anywhere

Provides write access to the same data across win servers and azure files

Branch offices

Backup and DR

Cloud tiering – non used data moved to azure

File archving

Cloud tiering is an optional feature of Azure File Sync in which frequently accessed files are cached locally on the server while all other files are tiered to Azure Files based on policy settings. When a file is tiered, the Azure File Sync file system replaces the file locally with a pointer, or reparse point. The reparse point represents a URL to the file in Azure Files. When a user opens a tiered file, Azure File Sync seamlessly recalls the file data from Azure Files without the user needing to know that the file is actually stored in Azure. Cloud Tiering files will have greyed icons with an offline O file attribute to let the user know the file is only in Azure.

Filesyncsvc.exe – monitors changes on server endpoints. Initiates sync sessions to azure

Storagesync.sys – az file sync file system filter. Tiering azure files

Pwsh cmdlets

An Azure files share can be a member of only one sync group

Sync group defines sync topology

Registerd server – trust relationship between server and storage sync service

Storage sync service – top level azure resource for file sync. Multiple storage sync service possible

Server endpoint – location on server. Like folder

Cloud endpoint – azure file share that is part of sync group

[Identify file sync components - Learn | Microsoft Docs](https://docs.microsoft.com/en-us/learn/modules/configure-azure-files-file-sync/6-identify-components)

Sync service Registration on the server requires your Subscription ID, Resource Group, and Storage Sync Service (created in step 1). A server (or cluster) can be registered with only one Storage Sync Service at a time.

A server endpoint integrates an entire volume or a subfolder from a registered server for syncing

Servers must be registered to athe storage sync service

A location on server can only sync with one sync group

Azure Storage Explorer

Windows, mac and linux. Used to access multiple accounts and subscriptios and manage storage content

Storage explorer requires management ARM and data layer permissions. Azure AD permissions to access storage account, containers and data in containers

Use access keys to connect external storage accounts

Access keys provide access to entire storage. You will have 2 access keys so you can use 1 when regenerating other.

Rotating access keys will not interrupt disks connected to azure vm

Azure Import/Export service – data copy, encryption and creation of journal files

Jobs can be created using portal or REST api

Cost effective way to move large data to/from azure

Content distributions

Backup scenario

Data recovery

Supply your own hardisk

Tool – WAImportExport Tool : Drive preparation and repair tool.

Use of internal SATA ii/iii hdd or ssd.

Single NTFS volume disk encrypted with bitlocker.

AZcopy – win, macos, linux

Copy data between storage accounts, filesystem to storage account

Copy entire account to another account for blob

List /remove files and blobs

AAD and SAS token authentication

Creating azure Storage Account

Multiple db options like azure sql db, cosmos db and table storage.

Multiple store and send message options – Azure Queues and Event hubs

Store loose files – Azure files and Azure blobs

Azure Files, Blobs, Tables and Queues – 4 data services

Settings specified during SA creation is applied to all services inside it

Deleting a SA deletes all services in it

Azure SQL and cosmosdb are independed and cannot be included in a SA

Subscription, performance (Standard, premium) , Virtual network, replication Billing, location and accessible by are defined in policy in Sa

Azure automatically maintains 3 copies of data within a DC.

The minimum replication is called LRS (entire datacenter fails, data loss)

SA Properties

Name – lowercase, 3 – 24 char, digits, globally unique

Deployment Model – Resource manager or Classic

Resource manager supports resource groups. Classic doesn’t support grouping

Account Kind – 3 kinds.

Storage V2 general purpose v2 – latest features with all storage types

Storage general purpose v1 – legacy with all storage types but no all features (cheap pricing per transation)

Blob Storage – legacy. Allows only allow block blobs and append blobs

Tools for creating SA

Portal, Azure powershell, Azure cli and management client libraries.

Azure storage doesn't support SSL for custom domain names, this option cannot be used with a custom domain name.

**Control access to azure storage with SAS Shared Access Signatures:**

Features of SAS, Stored access policies, program

In Azure Blob storage every request to access files stored needs authorization.

SAS provides secure, delegated access to the resources in storage account

Files in azure are accessed via http/https

There are 4 methods to access file stored in Azure.

1. Public Access
2. Azure AD
3. Shared Key
4. Shared Access Signatures SAS

Public Access – anonymous public read access for containers and blobs

1. Storage account – If AllowBlobPublicAccess is enabled on the storage level, then you can allow public access to the blob. To allow public access to the blob, the container must allow public access
2. The Container – Public read access for blobs or public read access for container and its blobs.

Anonymous access is controlled at the container level and not at the blob level.

In public access – no need to share keys with clients

Azure AD – Useful when you have app with managed identities or security principle configured.

1. Authenticate and get eh OAuth 2.0 token
2. Pass the token to azure storage to enable authorization

Shared Key

Azure storage creates 2 512 Bit access keys for every storage account

These keys are shared to clients

Anyone with the key has root access to the storage

Best practice is to manage storage keys with Azure key vault so u can rotate it

**Shared Access Signature** – Grants granular access to files. Read only or Read Write access.

Supports expiration time as well.

SAS is a key and must be protected same like access keys.

3 types of SAS are available

1. User delegation SAS – Used only for Blob and secured with Azure AD
2. Service SAS – Secured using Storage account key. Delegates access to resources in Azure Blob, Files, Tables and Queues
3. Account SAS – Secured using storage account key. Same as service SAS but also can control access to service level operations such as Get Service Stats.

A stored access policy can be associated with a Service SAS.

A stored access policy can be associated with up to 5 SAS

Good for granularity and revoking SAS

In ad hoc SAS the only way to revoke or change is to change the storage account keys

Best practices with SAS

1. Use https
2. Use user delegation SAS. Since no need to store storage account keys.
3. Set expiration date to smallest value
4. Apply minimum required privileges
5. Create middle tier service to manage users and access

Most flexible and secure way to use service or account sas is to associate the SAS tokens with Stored access policy.

Stored Access Policy - Cli, portal or c#

Applied to 4 services blob, file share, q, table

Azure Storage Explorer

Easily access and edit data in azure

Storage explorer can access the below types

1. Azure blob storage
2. Azure Table storage – stores NoSQL, semi structured data
3. Azure Queue storage – Store message in queue, accessed by http/s calls
4. Azure files – smb
5. Azure Data Lake Storage – based on apache Hadoop. Large volumes and can be structured/unstructured data. Gen1 is a dedicated service. Gen2 is a Azure blob storage with hierarchical namespace feature enabled on the account

Local emulators

Used during development phase. Devs can use this to emulate storage

2 types – Storage Emulators and Azurite

Azure Storage Emulator – uses local sql 2012 express db. Emulates Tables, queues and Blob

Azurite – Node.js based. Opensource and support most azure storage commands through an api

Azure Storage Explorer Permission

2 types of permission required – management and Data

Can access only data layer permission as well. (blobs, containers and other)

To see list of various storage accounts, containers and service endpoints – Give management role access

Ways to connect Storage Explorer to SA

1. Azure AD – Azure data lake blob container or standard blob container
2. SAS URI -4 services. SAS url from portal or storage explorer.
3. Data lake URI
4. Connection string
5. Name and key – quick connection.
6. Local emulator

Storage explorer can manage azure data lake.

Data lake is used for storing and analyzing large data sets. Any size and speed.

Security, scalability, reliability, manageability and availability

Gen1 and gen2 support in storage explorer.

Azure Virtual Machines

Provisioning vm needs, network,name,location, size, pricing model, storage, os

Vnets provide private connectivity b/w azure vm and other services.

Services outside the virtual network cannot connect to services within virtual network

VNets can be configured to access external service/onprem

VM Name – upto 15 characters for windows and 64 characters for linux

Locations can limit your availability options some configurations are not available in all regions

There are price differences between locations

Compute has different charge and storage has different charge

Compute is priced on hour basis but billed per minute

If u stop and deallocate vm then no charge

Storage cost – separate than compute. Even if vm is stopped/deallocated you are charged for storage

Payment Option for Compute cost

|  |  |
| --- | --- |
| Consumption based | Reserved virtual machine instances |
| Pay for compute capacity by second  Short term, workloads that cannot be interrupted  Ex – quick test, dev app in vm | Advance purchase of vm for 1 or 3 years in a specified region  Upfront commitment  72% price savings than pay as you go  Early termination fee  Best for vm which runs continuously, budget |

6 types of VM Sizing

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| General purpose | Compute optimized | Memory Optimized | Storage Optimized | GPU | High performance compute |
| Testing, dev, small db, medium web servers | Medium web, network appliance, batch process and app servers | Caches, rdbms, in memory analytics | High IO, Big data, NoSQL db, warehouse | Graphic, video editing, deep learning | Fast, power |

Resizing vm can cause – temporary outage or IP change

VM Disks

OS Disks – SATA C Drive

Temporary – D drive

Data disks – SCSI

VM Storage Options

Azure Premium Storage – High performing, low latency disks. High I/O. SSD based.

Multiple premium storage can be attached to vm – upto 256TB of storage/VM. 80000 IOPS Per VM. Disk Trhoughput upto 2000 megabytes per sec per VM. Low read latency

Managed Disks – VHD. Like on premise hardisk. Azure Managed disks are stored as page blobs. Ultra SSD, Premium SSD, Standard SSD and Standard HDD. Azure takes care of the disk management

Limit cost by keeping in Standard Azure Storage

Managed disks are required for the single instance virtual machine SLA.

Azure Bastion  
Fully PaaS Service that is provisioned inside your virtual network.  
Provides secure and seamless RDP/SSH connection to VM directly in azure portal over SSL  
Connecting via Bastion does not need VM to have public IP  
VMs are connected directly from azure portal. No need of additional client agent or software

Connect

RDP-  
The Azure portal automatically enables the Connect button on the Azure Windows VM blade if the VM is running and accessible via a public or private IP address, and if it accepts inbound traffic on TCP port 3389  
Get-AZRemoteDesktopFile

Window Remote Management WinRM –

Commandline sessions to azure vm.

Non interactive powershell scripts can be run

Security by certificates uploaded to azure keyvault

Port 5986

1. Create key vault
2. Create self signed cert
3. Upload cer to keyvault
4. Id the URL and reference the url in azure vm configuration

Linux Connection

SSH keys

Public key – placed on linux VM

Private Key – placed locally

2048 bit key length and SSH RSa format for public and private keys required

Virtual machine availability

Unplanned hardware maintenance – live migration -VM paused for short time

Unexpected downtime – Migrates vm – vm might be rebooted or lose temp drive

Planned maintenance – periodic maintenance – no impact on vm

Availability Sets

Logical feature. No single point of failure.

Azure ensures the availability sets runs across multiple physical server, racks, storage units and network switches.

Only a subset of vm is impacted

* Redundancy – configure multiple vms in availability set
* Make each application tier into separate AS
* Combine a load balancer with AS
* Use managed disk with VM

SLA

2 or more instance in 2 or more AZ in same region – VM connectivity by 99.99%

2 or more instance in same Availability set – 99.95%

Single instance vm using premium storage for all OS and data disk – 99.9%

You can create a virtual machine and an Availability Set at the same time. A VM can only be added to an Availability Set when it is created. To change the Availability Set, you need to delete and then recreate the virtual machine.

|  |  |
| --- | --- |
| Update Domain | Fault Domain |
| Group of nodes that are upgraded together during the process of service upgrade.  Incremental or rolling upgrades performed  VMs/physical hw are updated and rebooted at the same time  During planned maintenance only one UD is rebooted at a time  Default 5 non user configurable UD.  Can configure upto 20 UD | FD – group of nodes that represent a physical unit of failure.  Group of machines that share common hardware.  Single point of failure  Ex – a server rack.  FD – Nodes belonging to the same physical rack |

Placing your virtual machines into an availability set does not protect your application from operating system or application-specific failures. For that, you need to review other disaster recovery and backup techniques.

Availability Zones – Protects against data center failure

* Unique physical locations within an azure region
* 1 or more datacenter with independent cooling, networking, powers
* Resiliency purpose there are minimum 3 separate zones in all enabled regions
* ZRS uses Availabilty zones
* 99.99 VM uptime SLA

Services supporting Availability Zones

Zonal Services – Pins resources to specific zones

VMs, Managed Disks, Standard IP addresses

Zone Redundant Services – Platform replicates automatically across zones

Zone Redundant Storage, SQL DB

To achieve comprehensive business continuity on Azure, build your application architecture using the combination of Availability Zones with Azure region pairs.

Vertical Scaling / Horizontal Scaling

* VS – has more limitations on hardware availability by region.
* VS – requires VM to stop and restart
* HS – Flexible/ 1000s of VM to handle load

**VM Scale Sets**

Auto scale up or down VMs

Supports Azure Load Balancer for layer 4 traffic distribution

Layer 7 and SSL termination is done by Azure Application Gateway

Supports 1000 VM Instances.

Custom VM images are supported upto 600 VMs

Initial instance count -Number of virtual machines in the scale set (0 to 1000).

Instance size - The size of each virtual machine in the scale set.

Azure spot instance - Low-priority VMs are allocated from Microsoft Azure's excess compute capacity. Spot instances enable several types of workloads to run at a reduced cost.

Enable scaling beyond 100 instances - If No, the scale set will be limited to one placement group with a max capacity of 100. If Yes, the scale set can span multiple placement groups. This allows for capacity to be up to 1,000 but changes the availability characteristics of the scale set.

Spreading algorithm - We recommend deploying with max spreading for most workloads. This approach provides the best spreading.

**Autoscale**

Autoscale minimizes the number of unnecessary VM instances that run your application when demand is low, while customers continue to receive an acceptable level of performance as demand grows and additional VM instances are automatically added.

**Virtual Machine Extensions – allows to avoid configuration drift**

Extensions are small applications that gives post deployment configuration and automation task

Software installation, av protection, configuration script inside

VM Extensions can be managed with CLI, pwsh,ARM and portal

Different for windows and linux

Custom Script Extension CSE:

Automatically launch and execute virtual machine customization tasks post configuration.

Can do simple task like stop vm or install software or even complex tasks or series of tasks.

Set-AzVmCustomScriptExtension cmdlet

Set-AzVmCustomScriptExtension -FileUri https://scriptstore.blob.core.windows.net/scripts/Install\_IIS.ps1 -Run "PowerShell.exe" -VmName vmName -ResourceGroupName resourceGroup -Location "location"

Consideration

Timeout period is 90 minutes

Make sure dependencies like storage or networking is available

Failure events – low disk space etc

Sensitive data protection

DSC – Powershell desired state configuration

Contains configuration block, node blocks, resource blocks

**APP Service**

App runs in an App Service Plan.

App service plan – set of compute resources for a web app to run.

An app in a app service plan scales it scales all vm, when app runs it runs on all vms etc…

Tiers - Free, shared, basic, standard, premium, Isolated

Auto scale feature is not available in Free/Shared/Basic Plans

No max instances in free/shared/basic

A screenshot of a computer

Description automatically generated with medium confidence

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Free | Shared | Basic | Standard | Premium | Isolated |
| Runs on same azure vm  No SLA  Metered on per app basis  1 GB disk | Same as Free  Custom domain name  1 GB disk | No autoscale, traffic management  Built in NLB  Plan with linux supports web app for containers  Upto 3 inst  SSL  10 gb | Production workloads  Built in NLB  Autoscale  Upto 10  Staging environments  50 gb | Enhanced performance  Dv2 series vm  Fast processor, ssd, memory  Upto 30  250gb | Mission critical workloads  Virtual network  Private and dedicated environment  App service environment is private  100 instances and more upon request  1TB |

Web App Scaling – Auto or manual

|  |  |
| --- | --- |
| Scale Up | Scale Out |
| More cpu, memory, disk  Dedicated vms  Custom domains and certificates  Staging slots  Autoscaling  Do this by changing the pricing tier or the app service plan | Increase number of vm  As many as 30 instances  100 in isolated tier  Autoscale – based on rules and schedules |

Rules in autoscale – Metric Based and time Based

App Service use reasons

* Multiple Languages and frameworks
* DevOps optimization
* Global scale with HA
* Connections to SaaS platforms and on premises data
* Security ad compliance – authenticate with azure ad or with social login
* Application templates – wordpress joomla drupal etc
* VS integration
* API and mobile features
* Serverless code

Web app Devops

Automated – Github, Azure DevOps, Bitbucket

Manual – Git, CLI webapp up, Visualstudio, FTP/S

Deployment slots – Standard, premium or isolated

App content and config can be swapped between 2 deployment slots including production slot

When auto swap is enabled from a slot into production, every time you push your code changes to that slot, App Service automatically swaps the app into production after it's warmed up in the source slot. Auto swap isn't currently supported in web apps on Linux.

To map a custom DNS name to a web app, the web app's App Service plan must be a paid tier.

**Backup App Service – Standard or premium tier**

App service can backup, file content, app configuration and database connected to the app

Azure storage account and container in the same subscription as the app

10 Gb

Application insights

Feature of azure monitor

Monitors live apps

Automatically detects performance anomalies

Powerful analytic tools to see what users do with the app

DevOps integration

Monior and analyze data from mobile apps using visual studio app center

**Azure Containers**

ACI Azure container instances – runs container in azure without managing vm

Containers uses Azure disk for local storage for single node and Azure Files smb shares for multiple node

Deploy multi container group – using ARM Template or YAML. ARM preferred

containers within the group share a port namespace, port mapping isn't supported

**AKS**

In Kubernetes distribute traffic via load balancer

Routing of app traffic can be done with ingress controllers

Security and filtering – Kubernetes network policies

A best practice is to include resource limits for all pods to help the Kubernetes Scheduler understand what resources are needed and permitted.

**Virtual Networking**

VNets – provision and manage VPNs in azure

Link Vnets to other VNets in azure or on premise

Each VNet has its own CIDR block

CIDR blocks should not overlap

DNS Server Setting in VNet

Subnets

Provides seucirty, performance and management

The subnet range must be unique within the address space in the VNet

The range cannot overlap

Address space must be in CIDR notation /

To connect to on premise over Azure VPN Gateway, th VNet must have dedicated subnet for the gateway

Routing between subnets are allowed by default. To override this, use Network Virtual Appliance NVA

To limit access to az resources such as storage account or sql db to specific subnets – Use Virtual network service endpoint. You can also deny access from internet.

NetworkSecurityGroup – 0 or 1 NSG to each subnet in a VNET

NSG – Rules to allow or deny traffic to and from sources and destinations

Private Links - connectivity to Azure PaaS, customer owned or MS partner services. No data exposure to public internet.

Azure reserves 5 IP addresses in each subnet(0 – network, 1 – gateway, 2,3 – Azure DNS IP to VNet, 255- Broadcast)

**Pubic and Private IP address**

Public IP SKU must match the SKU of the Load Balancer with which it is used

Name must be unique in that RG

Dynamic address can change if the VM is stopped deallocated and then restarted. This is released when a Pip is disassociated from a resource

Static address are released when the resource is deleted.

In IPV6 – Basic SKU (Dynamic) and Standard SKU (Dynamic)

Public IP Association – Virtual Machine Network interfaces(NIC), Internet facing Load balancers(Front end configurations), VPN Gateways(Gateway IP) and Application gateways (Front end configuration)

|  |  |
| --- | --- |
| Basic SKU | Standard |
| Dynamic or static IP  Open security  Nic, VPNgw,App gw, Int LB  Not zone redundant | Static Only  Closed Inbound traffic  Network interfaces or public standard LB  Zone redundant by default |

**Network Security Groups –** Associated with Subnets or Nic

NSG can be associated multiple times

Using NSG – can create DMZ

0 or 1 NSG per subnet/Nic

3 default IN/Out rules in NSG – 65000, 65001, 65500(deny all)

Priority. Rules are processed in priority order. The lower the number, the higher the priority.

The value is between 100-4096

**Application Security Groups**

Limited ASG per subscription

One ASG as the source and destination

All NIC assigned to ASG must exist in same Virtual Network. Cannot add network interfaces from different Virtual Network to the same ASG

**Azure Firewall**

Managed, cloud based.

Protects virtual network resources

Fully stateful

Uses static public IP

Fully integrated with Azure monitor for logging and analytics

Traffic denied by default

Threat intel, NAT, net and app traffic filtering

Built in HA

Multiple AZ for increased availability

Scales up as much as needed

Application FQDN filtering

Network filtering rules by source, destination, Port and protocol

Malicious IP address and domain block using Threat intelligence

Multiple Public IP

Hub and spoke network topology is preferred – Hub is the Azure Virtual network

Traffic flows b/w hub and spoke via Express Rout or VPN gateway

There are 3 kinds of firewall rules

1. NAT Rule
2. Network rule
3. Application rule

|  |  |  |
| --- | --- | --- |
| NAT | Network | Application |
| Destination NAT – Translate and filter inbound traffic to subnets  Each rule is a Public to private IP translation  NAT rule must be accompanied by a matching network rule to allow traffic  Source, Destination address and destination ports are all external  Translated address and Port are internal | Any non http/s traffic should have network rule | FQDN that can be accessed by the subnet.  Source – ip  Target FQDN – DNS Name |

Rule processing

1. Network Rule
2. Application rules

Custom domain Names

1. Add
2. Verify

Azure DNS Zones

Added in the virtual network

To host domain in azur dns – we need dns zone for that domain name

When delegating a domain to Azure DNS, you must use the name server names provided by Azure DNS. You should always use all four name server names, regardless of the name of your domain.

Setting up a subdomain follows the same process as typical delegation. The only difference is that NS records must be created in the parent zone contoso.com in Azure DNS, rather than in the domain registrar.

Private DNS Zones – Name resolution for VMs within VNet and between VNet

Split Horizon – Private and Public DNS Zone to share same name

DNS records for private zone are not visible

Azure automatically maintains Hostname for VMs -enable auto registration in the link configuration.

Private dns zone – shared between virtual networks

Powershell, ARM and REST

**VNet Peering**

Regional – connects azure vnet in same region

Global – different regions. Not in government region.

Only peer vnet in same region in government

Seamless. The ability to transfer data across Azure subscriptions, deployment models, and across Azure regions is provided by vnet peering

gateway transit allows peered virtual networks to share the gateway and get access to resources

When virtual networks are peered, you configure a VPN gateway in the peered virtual network as a transit point.

To reduce the number of VNet peering and use a hub and spoke model – Configure User defined routes and service chaining

User defined route – IP of VM or VPN Gateway

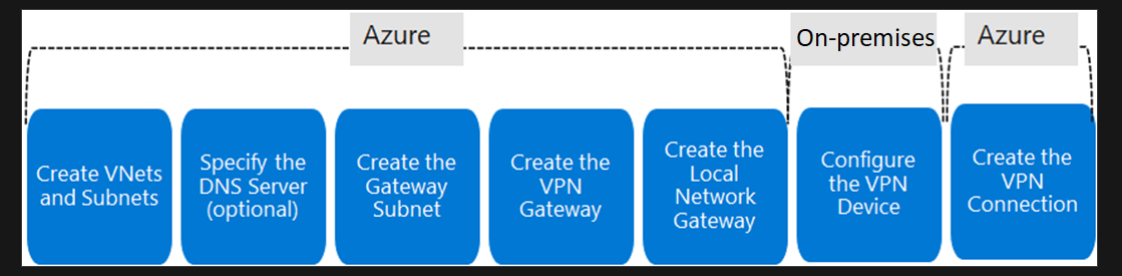
Service Chaining – Lets to define user routes. These routes directs traffic from on VM to a Virt appliance or virtual network gateway

VPN Gateway

Each Vnet can have only one vpn gateway

Virtual network gateway – 2 or more vms deployed to subnet (gateway subnet)

Vnet gateway – contains routing tables and services



Gateway Subnet – Before creating virtual network gateway. Gateway subnet needs to be created

Gateway subnet must be named GatewaySubnet

Virtual Gateway

Type – Route based or Policy Based. Most are route based.

Policy based gw support only ikev1

Generation 1 – Basic and VpnGw1 SKU

Generation 2 – VpnGw4 and 5

A virtual network cannot be associated with more than 1 gateway

P2S requires route based.

S2S require a VPN device

Policy based PVN – only available with Basic gateway SKU

Only one tunnel when using policy based vpn

Only S2S uses policy based vpn

Once a virtual network gateway has been created, you can't change the VPN type.

Local Network Gateway - On Premise Location

VPN gateway is a specific type of virtual network gateway that is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public Internet. You can also use a VPN gateway to send encrypted traffic between Azure virtual networks over the Microsoft network.

Azure System Routes

Direct network traffic between virtual machines, on prem net, and internet

Traffic b/w vms in same subnet, different subnet but same vnet, vm to internet

Destination in routing table can be - IP, virtual network gateway, a virtual appliance or the internet

Each route table can be associated to multiple subnets, but a subnet can only be associated to a single route table.

With **service endpoints,** the virtual machine IP addresses switches from public to private IPv4 addresses. Existing Azure service firewall rules using Azure public IP addresses will stop working with this switch. Ensure Azure service firewall rules allow for this switch before setting up service endpoints. You may also experience temporary interruption to service traffic from this subnet while configuring service endpoints.

**Azure Private Link provides** private connectivity from a virtual network to Azure platform as a service (PaaS), customer-owned, or Microsoft partner services.

No data exposure to public internet

Private link is global

Integrates with on prem and peered networks

Data exfilteration protection

Virtual network endpoints extend the private address space in Azure. Endpoints restrict the flow of traffic. As service endpoints are created, Azure creates routes in the route table to direct the traffic.

---------- Casual Notes---------

Root Management Group – Top level folding of all management groups and subscriptions

Allows global policies and Azure role assignments applied at directory level

By default azure global admin don’t have access – Elevation to User Access Admin is required

Azure AD and Azure resources are secured independently from one another

Concept Works

Azure Identity Models

1. Cloud Identity – Azure AD User, a cloud account
2. Synced Identity – Synced from On Prem
3. Managed Identity – login.microsoftonline.com – Azure AD authentication
   * Password Synchronization
   * Passthrough Authentication – No need of domain federation
4. Federated Identity – Authentication happens on Prem – ADFS

Portal.office.com -> login.microsoftonline.com – ADFS – AD

AD -> ADFS -> login.microsoftonline.com -token ->portal.office.com

**Azure AD Connect**

Sync users and use applications provisioned on Azure AD to use – Gallery, custom apps, on prem apps

AAD connect procedure:

1. Verify domain in azure ad
2. Domain joined windows server 2008 r2 or later
3. Add 50k objects in azure ad and 300k after verifying
4. Need global admin cred
5. SQL express installed. More than 100k objects use SQL full

Methods: 3 methods

|  |  |  |
| --- | --- | --- |
| Password Synchronization | Pass Through Authentication | Federation with ADFS or PingFederate |
| Has synced to Azure AD  Authentication is processed by Azure AD  Authentication request is processed by Azure AD and no by on Prem AD  Domain is managed | Authentication processed by azure AD  Authentication request is passed to On Prem AD  Domain is managed | Authentication to be processed by on prem idp  Authentication request are redirected to on prem |

3 Accounts are created when installing AAD Connect

1. MSOL\_guid – Read/Write operation on Local AD – Query on prem AD – Created on prem
2. Sync\_guid – query info in Azure AD – Read/Write - Created in Azure AD
3. Service Account – AAD (AD sync service account) – Read / Write to database

A picture containing diagram

Description automatically generated

Sync Rules of AAD Connect

1. Local AD Connector space
2. Metaverse
3. Azure AD Connector space

UDEMY – ALAN

When we create resource we need Azure subscription first

Vm will be inside RG (Logical Grouping)

OS Disk, Data Disk, Public IP Address

VM Must be part of Virtual network

VM pricing is per hr

public IP addresses of the Standard SKU, by default, require that the network interfaces to which they are assigned are protected by a network security group. In order to allow Remote Desktop connections, you will create a network security group explicitly allowing inbound RDP traffic from Internet and assign it to network interfaces of both virtual machines.

Azure Private DNS provides a reliable, secure DNS service to manage and resolve domain names in a virtual network without the need to add a custom DNS solution. By using private DNS zones, you can use your own custom domain names rather than the Azure-provided names available today. Using custom domain names helps you to tailor your virtual network architecture to best suit your organization's needs. It provides name resolution for virtual machines (VMs) within a virtual network and between virtual networks. Additionally, you can configure zones names with a split-horizon view, which allows a private and a public DNS zone to share the name.

Insight into performance and configuration of azure resources – Azure monitor / log analytics

Azure Monitoring collects host-level metrics - like CPU utilization, disk and network usage - for all virtual machines without any additional software. For more insight into this virtual machine, you can collect guest-level metrics, logs, and other diagnostic data using the Azure Diagnostics agent. You can also send diagnostic data to other services like Application Insights.

Note: By default, log collection includes critical, error, and warning entries from the Application Log and System log, as well as Audit failure entries from the Security log. Here as well you can switch to the Custom view for more detailed configuration settings.

Pay as you go plans

Basic Developer, standard, professional direct

Geo-redundant storage (GRS) copies your data synchronously three times within a single physical location in the primary region using LRS It then copies your data asynchronously to a single physical location in a secondary region that is hundreds of miles away from the primary region.

Storage accounts configured with the Premium performance setting only support LRS.

Any storage account already configured with ZRS cannot be changed or directly switched to another replication setting. In this scenario, the only storage account that is not set to LRS or Premium performance is storage2, which can be switched to use Geo-redundant storage.

You would only use Capture if you wanted to create an image of the existing VM. However, this will make the source VM unusable. There are also several preparation tasks to complete before capturing the VM image. You would not select Redeploy + reapply as these two options are used to address failed connections or VM states. Availability and scaling is used to set up and manage VM high availability, not for creating additional VMs based upon a set configuration setting.

To enable support for Azure Disk Encryption, you need to modify the Access policies for the key vault. This provides an option to enable access to Azure Disk Encryption for volume encryption.

Recovery Services vault supports Azure Virtual Machines, SQL in Azure VM, Azure Files, SAP HANA in Azure VM, Azure Backup Server, Azure Backup Agent, and DPM.

Backup vault supports Azure Database for PostgreSQL servers, Azure Blobs, and Azure disks.

Lifecycle management policies apply rules to supported storage accounts to control the transition of data to cooler storage tiers. Lifecycle management policies are supported for block blobs and append blobs in general-purpose v2, premium block blob, and Blob Storage accounts. FileStorage and general purpose v1 storage accounts do not support lifecycle management.

App Service – You can publish a web app as a code, docker container or static web app

Subscription/RG hold only Metadata of resources and hence can move as it doesn't impact on their location

a Resource that cannot be removed is Azure Disks,

Stop the backup before deleting

Contributor role | Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.

DevTest Labs User role only lets you connect, start, restart, and shutdown virtual machines in your Azure DevTest Labs.

he Logic App Contributor role lets you manage logic app, but not access to them. It provides access to view, edit, and update a logic app.

Logic App Operator - Lets you read, enable, and disable logic apps, but not edit or update them.

The Contributor role can manage all resources (and add resources) in a Resource Group.

You can only move a resource to a Resource Group or Subscription, but the location stays the same

"Azure Traffic Manager is a DNS-based traffic load balancer. This service allows you to distribute traffic to your public facing applications across the global Azure regions."

You can't delete a vault that contains backup data. Once backup data is deleted, it will go into the soft deleted state.

B: The azcopy sync command replicates the source location to the destination location. However, the file is skipped if the last modified time in the destination is more recent.

C: The azcopy copy command copies a directory (and all the files in that directory) to a blob container. The result is a directory in the container by the same name.

D: The az storage blob copy start-batch command copies multiple blobs to a blob container.

Azure Import/Export service supports the following of storage accounts:

✑ Standard General Purpose v2 storage accounts (recommended for most scenarios)

✑ Blob Storage accounts

✑ General Purpose v1 storage accounts (both Classic or Azure Resource Manager deployments),

Azure Import/Export service supports the following storage types:

✑ Import supports Azure Blob storage and Azure File storage

✑ Export supports Azure Blob storage. Azure Files not supported.

Azure table can be used in Storage and Storage V2

Azure blob storage can be used in storage, storagev2 and blob storage accounts

Hot, cool, archive tier – supports storage v2 and blob.

Storage v2 is less costly than blob

You may only tier your object storage data to hot, cool, or archive in Blob storage and General Purpose v2 (GPv2) accounts. General Purpose v1 (GPv1) accounts do not support tiering.

A sync group contains one cloud endpoint, or Azure file share, and at least one server endpoint.  
Azure File Sync does not support more than one server endpoint from the same server in the same Sync Group.  
Multiple server endpoints can exist on the same volume if their namespaces are not overlapping (for example, F:\sync1 and F:\sync2) and each endpoint is syncing to a unique sync group.

Allow trusted Microsoft services to access this storage account as an exception to enable Azure Backup service to access the network restricted storage account.

files are never overwritten. If the file exists, it will get a new name on the endpoint  
File that is older will get name of the hosting server added. for example: srv01 creates a new version of "file1" so older version (hosted on srv02) gets renamed to "file1-srv02"

"Live migration is supported only for storage accounts that use LRS or GRS replication. If your account uses RA-GRS, then you need to first change your account's replication type to either LRS or GRS before proceeding. This intermediary step removes the secondary read-only endpoint provided by RA-GRS before migration."

"ZRS supports general-purpose v2 accounts only"

only standard storage account types support live migration. Premium storage accounts must be migrated manually.

By default, storage accounts accept connections from clients on any network. To limit access to selected networks, you must first change the default action.

Zone-redundant storage (ZRS) replicates your data synchronously across three storage clusters in a single Region.

GRS protects against Zone failure, while ZRS protects against data center failure.

LRS would not remain available if a data center in the region fails.

GRS and RA GRS use asynchronous replication.

ZRS only support GPv2.

Azure Import/Export – Dataset.csv and driveset.csv files to prepare the drives for import job

You can't delete a Recovery Services vault if it is registered to a server and holds backup data. If you try to delete a vault, but can't, the vault is still configured to receive backup data.

Remove vault dependencies and delete vault

Blobs cannot be backup up to service vaults.

Note: To create a Vault to protect VMs, the Vault must be in the same Region as the VMs.

Only VM and Fileshare is allowed to Backup.

AzCopy is a command-line utility that you can use to copy blobs or files to or from a storage account.  
You can provide authorization credentials by using Azure Active Directory (AD), or by using a Shared Access Signature (SAS) token.

- Blob storage: Azure AD & SAS

- File storage: SAS only