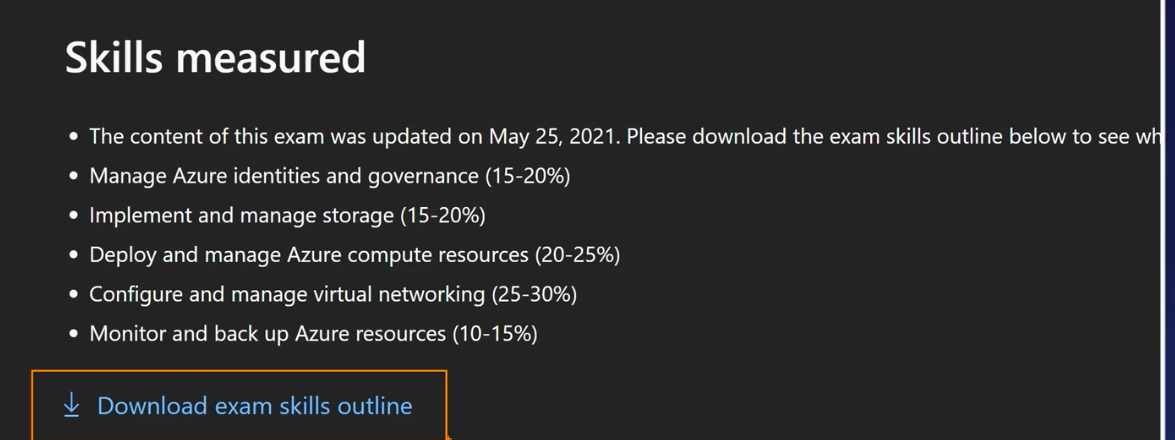
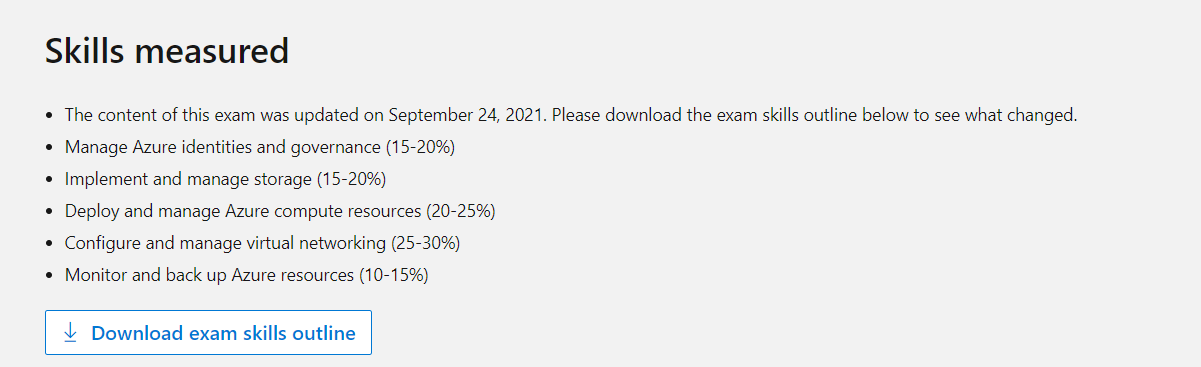
ITProTV



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

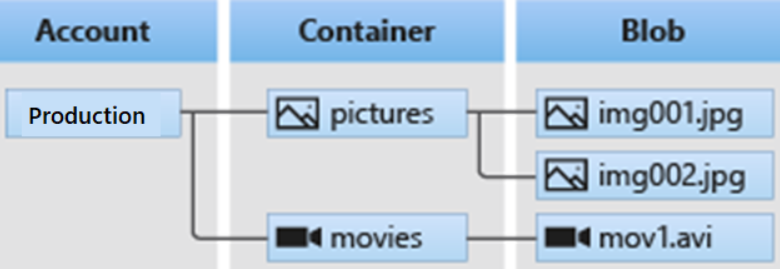
Failover – replication

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

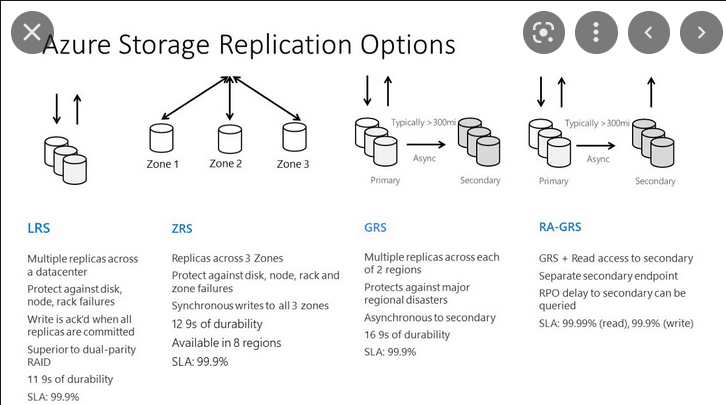
General purpose SA has 2 tiers

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.

---------- 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