Identity & Governance

Azure admins implement manage, monitor and organise the azure environment.

Manage azure ad objects:
Cloud identity is a Local azure user or external azure ad
Hybrid identity is a directory synced user
Guest identity is external users that have been invited into the domain

Bulk users can be created using a CSV file inside the portal.

Administer azure ad devices:
A device in this topic is a device that can join your azure instance and be managed by an mdm

Azure ad join -
Sign in with domain account, device usually owned by Company

Azure ad register-
Commonly used for BYOB

Self service password reset and multi factor requires P1 subscription

RBAC:
owner: full access to all resources and can grant access
contributor: can create and manage all resources, cannot grant access.
reader: can view existing resources

Deny assignment overrules any roles that are currently set.

Managing subs:
Management groups > subscriptions > resource groups > resources

You can move resources between subscriptions
You can transfer subscriptions between tenants
A single tenant can have multiple subscriptions

Cost management:

Cost analysis will let you see acteral and forecasted costs as well as offering granularity to see what resources are costing. You can also use the filter to check specific tags.

Storage:

Azure storage data objects:

Blob
File
Queue
Table
Disk

Storage accounts contain all azure storage objects, they require a unique name due to being accessible over the internet

Replication options:
Local redundant storage - 3 copies within its dc
Zone redundant storage - 3 copies in different locations within one region
Geo-redundant storage - 3 copies in 2 different regions but single dc
Geo zone redundant storage - 3 copies in 3 zones in 2 regions
Read access geo redundant storage
Read access geo-zone redundant storage

In order to make sure you are choosing the correct option prior planning is recurred

Management Groups

Used to efficiently manage access, Policies and compliance

Provides a level of Scope above Sub

Subscriptions within a group inherit Policies applied to the group

Azure Policy

Used to create, assign and manage Policies

Enforce rules to ensure resources are compliant

Focuses on resource properties for New and existing deployments

It DOESN'T apply remediation

Policy Concepts

A policy definition is a rule

An assignment is an application of an initiative or a policy to a specific scope

An initiative is a collection of policy definitions

Resource Locks

Each resource can have a lock applied

Lock types include:

- Read only
- Delete

Can apply to all resources and resource groups

Can be inherited from Parent Scopes

applies to all roles

Resource Groups

Resource groups are containers for resources

Resources can be moved from one group to another if supported

Moving resources does not change the location or region from where it was originally located

Deleting a resource group deletes all resources

Manage AD Objects

User or Global Administrator role is required to add or change users

You can't manually add users to dynamic groups

Guest accounts require Premium P2

Guest can be invited by users & Admin

Someone with user or global admin role must review invites

SSPR - Self Service Password Reset