|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Management Groups | Subscriptions | Resource Groups | Resources | General |
| Access Control  Policies  Compliance | Manage Costs  Set limits and quotas  Inherit from MG | Logical grouping  Lifecycle management  RBAC scope |  | AZ Region-minimum 3 AZ  ARM – Accesscontrol, locks and tags  Application security must be handled by your application.  RBAC – no app or data control |

# Describe Core Azure Architecture Components

Organizing structure for resources in Azure

1. Management Groups
2. Subscriptions
3. Resource Groups
4. Resources

Resources are instances of services you create

Resource Groups is a logical container where resources are managed and deployed

Subscriptions – used to manage costs. Can set limits or quotas

Management groups – Manage access, policy, and compliance for multiple subscriptions.

Subscriptions inherit conditions applied to management group

Azure Region – 1 or many datacenters that are nearby with low latency network.

Global services - AAD, Az Traffic Manager and Azure DNS doesn’t need to choose region

Azure Availability Zones – Physically separate datacenters within an azure region.

1 or more DC with independent power, cooling, and networking

Isolation boundary. 1 goes down other continues working.

High speed fiber optics connection

Availability zones are primarily used for – VM, Managed disks, LB, SQL DBs

3 Service category that support Availability zones

1. Zonal – pin resource to specific zone (VM, managed disk, IP)
2. Zone redundant service – Replication across zones automatically (ZRS, SQL DB)
3. Non Regional services – Available from azure geographies. Resilient to zone/region wide outages

AZs are either 1 or multiple DCs.

An AZ Region will have minimum of 3 Availability zones

Resource Groups:

* Logical container for resources
* 1 resource can only be member of 1 resource group
* Resources can be moved between resource groups
* Resource groups cannot be nested

RGs are useful for Logical Grouping, Life cycle management of resources, RBAC Authorization scope

ARM – Azure Resource Manager

* Deployment and management service for azure
* Provides management layer to create, update and delete resources
* Provides features such as Access control, locks and tags
* Uses JSON file for ARM templates
* Dependencies between resources can be defined

Azure subscription

* Logical unit of Azure services that links to azure account
* Allows us to provision resources
* Can be used to define boundaries around azure products, services, and resources
* 2 types of subscription boundaries - 1. Billing Boundary and 2. Access control boundary
* Account can have 1 or multiple subscription
* Access management policy is applied at subscription level
* Costs are aggregated first at the subscription level
* Helps manage and track costs
* Max Azure express route circuits per subscription is 10
* There are subscription limitations

Every Billing profile has its own monthly invoice and payment method

Multiple invoices within the same billing account can be done

Azure Management Groups

* To efficiently manage access, policies, and compliance for multiple subscriptions – use MG
* Governance conditions are applied to management groups
* Subscriptions inherit the conditions applied at management group
* Policies are inherited (ex: allows VMs from a particular region only) to subscriptions and resources
* Unified access and policy management

To provide user access to multiple subscriptions, move those subscriptions to a singe Management Group and apply RBAC to that management group. This will be inherited to all subscriptions.

Management group facts:

* 10000 MG per directory
* Management group tress supports to 6 level depth (root level and subscription level excluded)
* Only one parent per management group and subscription is supported
* Each management group can have many children
* All subscriptions and management groups are withing single hierarchy in the directory

## Build cloud governance strategy on Azure

Governance – General process of establishing rules and policies and ensuring that those rules and policies are enforced

A good governance strategy helps to maintain control over applications and resources.

Ensuring that the organization stays in compliance

Governance is very beneficial when:

* Multiple people working on azure
* Multiple subscriptions
* Regulatory requirements
* Standards to be followed for cloud resources

**Learning objectives**

* Make organizational decisions about your cloud environment by using the Cloud Adoption Framework for Azure.
* Define who can access cloud resources by using Azure role-based access control.
* Apply a resource lock to prevent accidental deletion of your Azure resources.
* Apply tags to your Azure resources to help describe their purpose.
* Control and audit how your resources are created by using Azure Policy.
* Enable governance at scale across multiple Azure subscriptions by using Azure Blueprints.

## Define who can access cloud resources by using Azure role-based access control

* Define own rules or use existing RBAC rules
* RBAC is applied to a scope. A Scope is a resource or set of resources
* Permissions are inherited by child scopes from parent scope (Parent -> child)
* RBAC does not enforce access permissions at the application or data level
* RBAC uses allow model

Assign user as owner to MG - > User is owner for all subscriptions  
Assign group as Reader to subscription -> Group can view all RG and resources within the sub  
Assign application a contributor role to RG -> application can manage all resources in that RG

**How RBAC Enforced**  
\* Any action that is initiated against azure resources through ARM  
\* Uses allow model

**To whom RBAC applies to**  
\* Individual person or group  
\* Service principals and Managed identities ( Applications and services use these identities to automate access to azure resources)

## Apply a resource lock to prevent accidental deletion of your Azure resources.

Prevent resources from being accidentally deleted or changed

* Locks are applied to Subscriptions, Resource Group or individual resources
* CanNotDelete and ReadOnly Locks are available
* CanNotDelete – Authorized people can read/modify but cannot delete
* ReadOnly – Authorized people can read a resource but they cannot delete or change
* Resource locks apply regardless of RBAC permission

Use Azure BluePrints – Can define set of standard azure resources that your organization requires.

## Apply tags to your Azure resources to help describe their purpose.

* Organize resources using resource tags
* Tags provide metadata about resources
* Metadata is useful for:
  + Resource management
  + Cost management and optimization – Group resources for cost report, estimations, forecast, tracking budgets
  + Operations Management – Group resources by criticality. SLA
  + Security – Classify data
  + Governance and regulatory compliance
  + Workload optimization and automation – Use azure devops to automate things based on tags
* Tags are not automatically applied to child objects, unless enforced by a policy

## Control and audit how your resources are created by using Azure Policy.

How do you ensure that your resources are compliant? Can you be alerted if a resource configuration is changed?

Azure Policies:

* Create, assign and manage policies that control or audit azure resources
* Enables to define individual policies are collection of related policies called initiatives
* Evaluates and highlights resources that are not compliant
* Prevents non compliant resources from being created
* Built in policy and initiative definitions for - storage, networking, compute, security center and monitoring

Example : Allow only a particular Stock Keeping Unit – SKU for a VM to be created

* Automatically remediate non compliant resources and configurations

Example: Tag all resources in a resource group

* Integration with azure devops for CI/CD pipeline