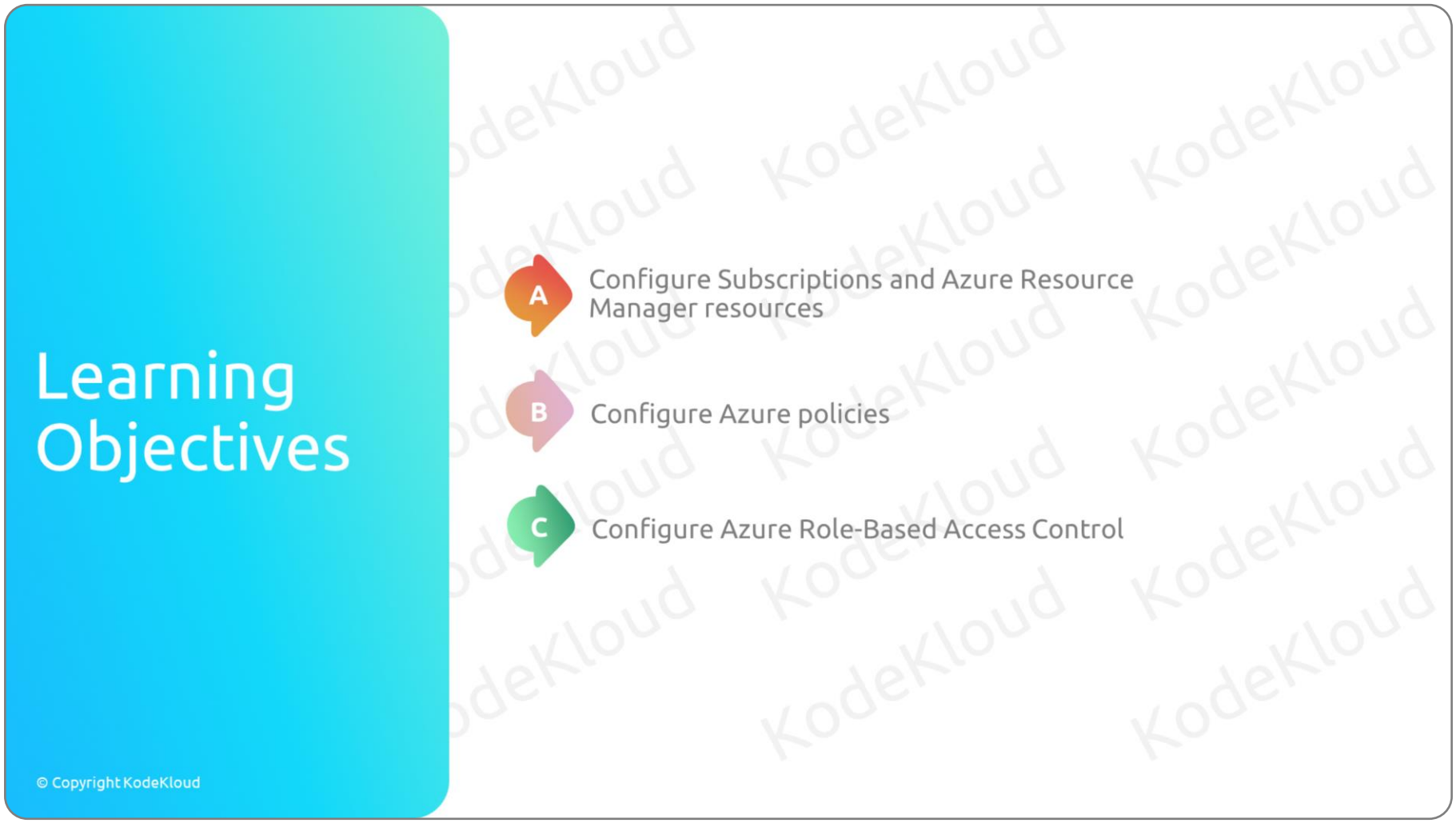
KodeKloud

Follow us on https://kodekloud.com/ to learn more about us.

Administer Governance and Compliance

These Learn modules are part of the AZ-104: Manage identities and governance in Azure (https://docs.microsoft.com/learn/paths/az-104-manage-identities-governance/) path.



Moved Lab 03a – Manage Azure resources with the Azure portal into this module. It covers resource locks.

Learning Objectives

A Configure Subscriptions and Azure Resource Manager resources

01 Managing subscriptions

02 Resource Groups and Limits

03 Understanding the hierarchy

04 Azure Resource Tags

05 Azure Resource Locks

06 Manage costs

Learning Objectives

B Configure Azure policies

01 Azure Policy

02 Initiatives

Learning Objectives

C Configure Azure Role-Based Access Control

01 Role Based Access Control

02 Azure RBAC vs Microsoft Entra ID Roles

Managing Subscriptions

Azure Subscriptions

Logical container that defines the billing boundary for usage

Resources deployed in Azure will be mapped to an Azure subscription

Subscriptions can also help in setting up environmental boundaries

Every subscription has a unique ID called the subscription ID

An account can have multiple subscriptions

Identities that are part of Microsoft Entra ID or an identity from any trusted Microsoft cloud service can sign up for subscription

Subscriptions are of different types based on the use case scenario

Subscription also acts as a scope for access management

Subscription Offer Types

Enterprise Agreements

Pay-as-You-Go

Cloud Solution Provider

Free Trial

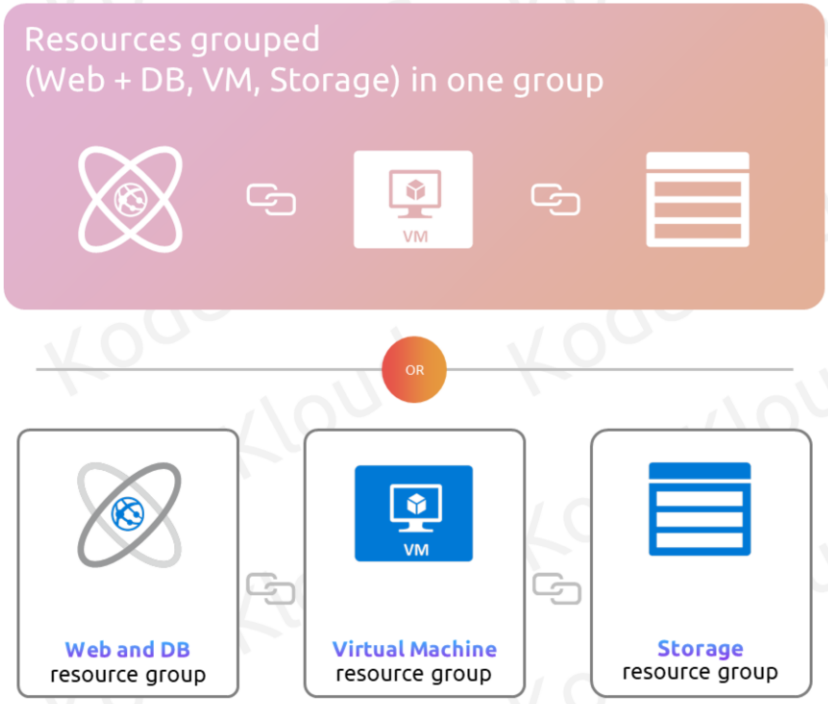
Azure for Students

Visual Studio

Resource Groups and Limits

Create Resource Groups

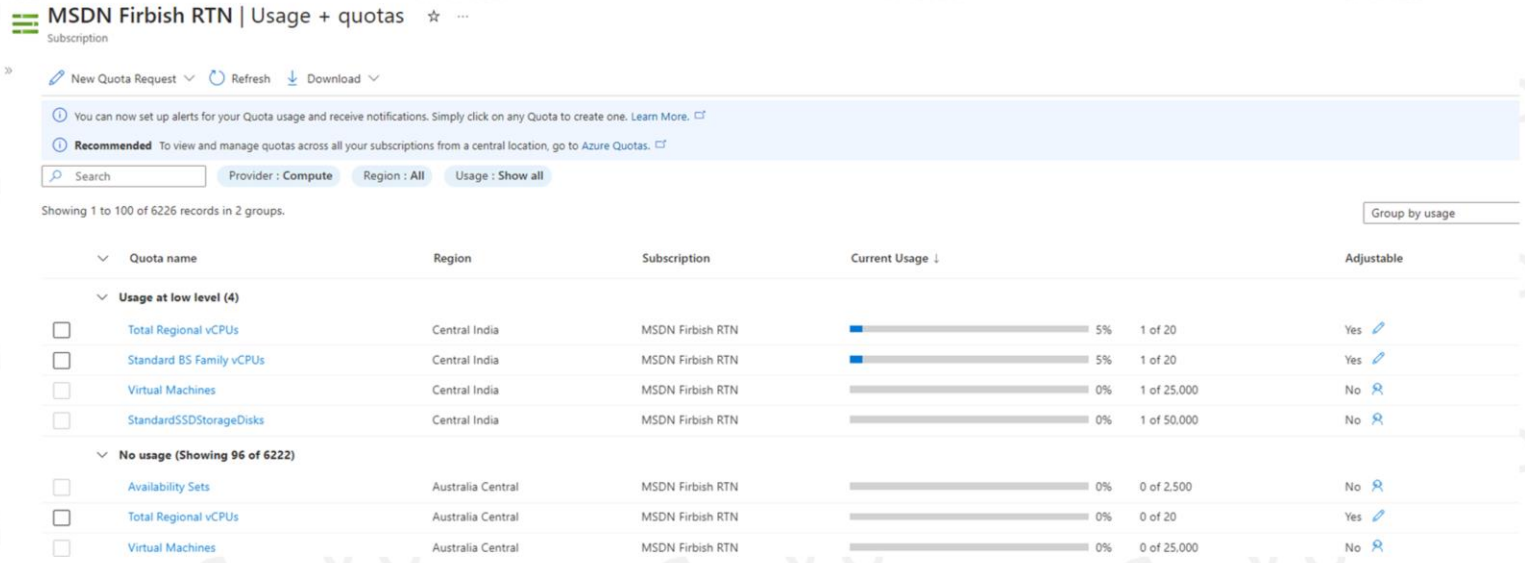
- A single resource group can be the sole container for any given resource.
- Resource groups can hold a diverse array of services that are deployed in multiple geographic locations.
- It is not possible to change the name of a resource group or to nest them inside another resource group.
- It is allowed to transfer resources from one group to another using Azure Resource Mover.



Manage Azure Resource Manager resource groups by using the Azure portal - https://docs.microsoft.com/azure/azure-resource-manager/management/manage-resource-groups-portal

There is an excellent Learn module, Use Azure resources, https://learn.microsoft.com/training/modules/use-azure-resource-manager/. This covers the Azure Resource Manager, resources, limits, locks, and groups.

Determine Service Limits and Quotas



Resources have a default limit – a subscription quota

Help track current usage and plan for future use

You can open a free support case to increase limits to published maximums

Azure subscription and service limits, quotas, and constraints - https://docs.microsoft.com/azure/azure-resource-manager/management/azure-subscription-service-limits

Understanding the Hierarchy

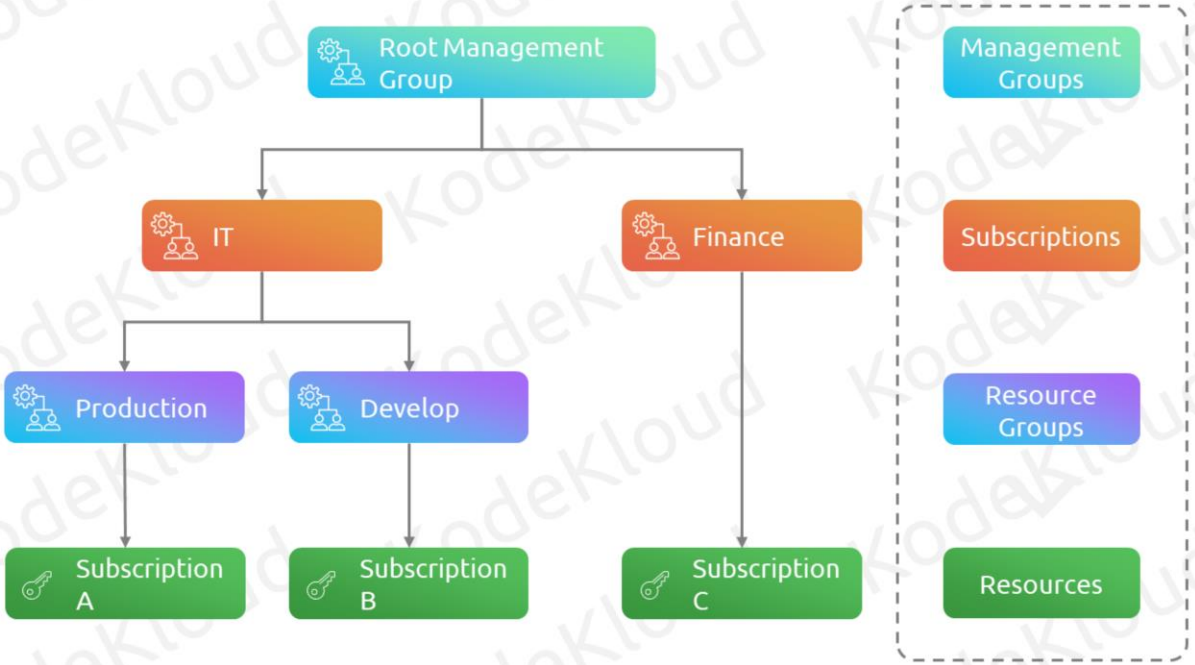
Understanding the Hierarchy

Management groups offer a scope above subscriptions by which you will be able to group subscriptions together.

Root Management group is created by default, and you have up to 6 levels of nested groups, excluding the root group.

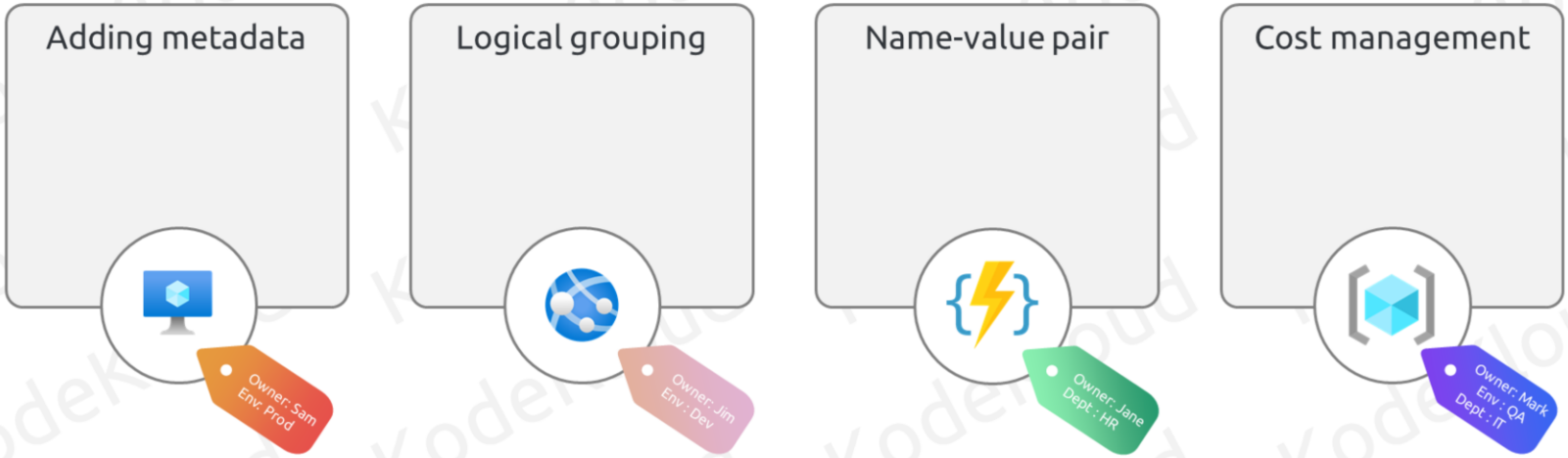
Each subscription will contain one or more resource groups for logically grouping resources like virtual machines, databases, etc.

Hierarchy helps in implementing policies, access, and cost management.



Azure Resource Tags

Azure Resource Tags



Tags don't follow inheritance by default; we can use Azure Policy to inherit tags from resource group or subscription.

Resource Locks

Resource Locks

Avoid accidental changes

With the help of resource locks, we can protect our resources from accidental changes or deletion.

Inheritance

Locks can be applied at the subscription, resource group, and resource level. The lock will inherit to the lower scopes.

Read-only locks

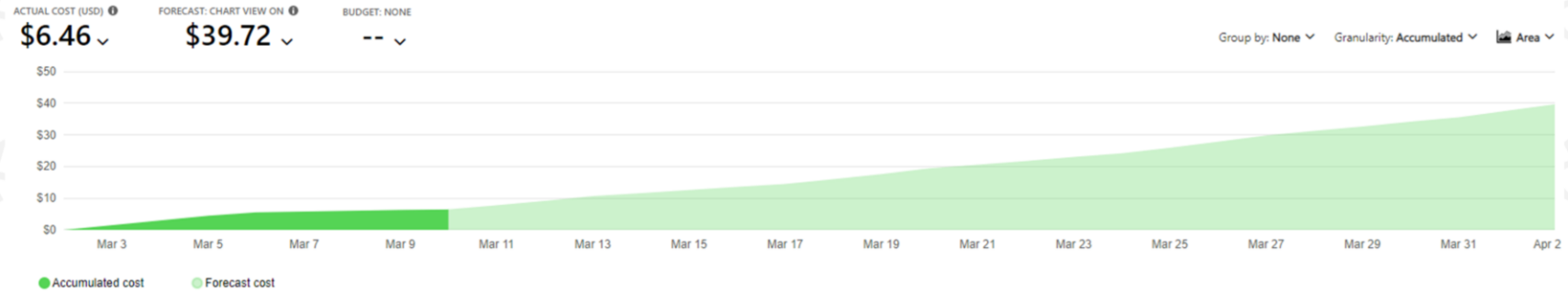
Resources with read-only locks cannot be modified, and this will prevent any changes to the resource.

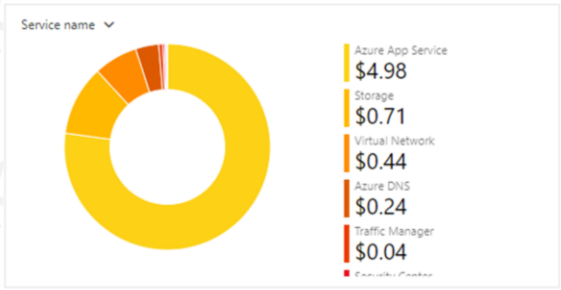
Delete locks

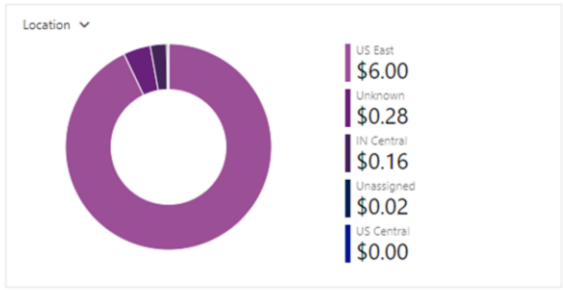
Resources with delete lock can be modified, but they cannot be deleted. Ideal for resources which you would like to modify and, at the same time, prevent accidental deletion.

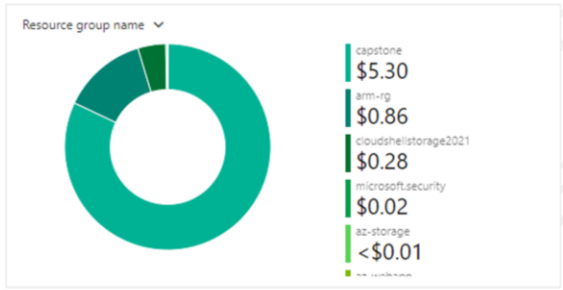
Managing Costs

Analyzing Costs









Cost Analysis

Budgets and Recommendations

Export Data

Cost Saving

Azure Reserved Instances (RI)

For instances that are planned for the long term and are running 24x7 can be reserved. Reservations can be purchased for 1 year or 3 years with upfront payment or equated monthly payments.

Azure Hybrid Benefit (AHUB)

You can purchase Windows and SQL licenses from Software Assurance and can use them with your Azure VMs and PaaS services. AHUB is cheaper than PAYG licensing cost.

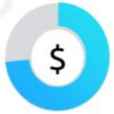
Credits

Credit-based subscriptions such as Visual Studio Enterprise, Visual Studio Professional, and MPN could provide you monthly credits that can be used for testing and developing solutions on Azure.

Regions

In Azure, every region has a different pricing. When deploying resources, choose low-cost regions. While selecting low-cost regions, do not compromise the compliance or performance of your workloads.

100%
PAYG



60%
Azure RI

80%
Azure RI + AHUB

Configuring Azure Policy

Azure Policy

Helps us to create, manage, and assign policies. Policies can be used to define organizational standards and identify non-compliant resources.

Definition

Policy definition is a JSON document which is used to define the policy and its effect. Azure has built-in policies that we can use, or you can write your own custom policies.

Scope

Like RBAC, we must specify the scope to which we want to enforce the policy. We can scope to management group, subscription, or to resource group.

Assignment

Assignment is the process of assigning a policy definition to a scope. Once it's assigned, policy enforcement is done.

Compliance

After assigning the policy, we can evaluate the compliance to understand compliant and non-compliant resources.

Azure Policy – Use Cases

Allowed resource types

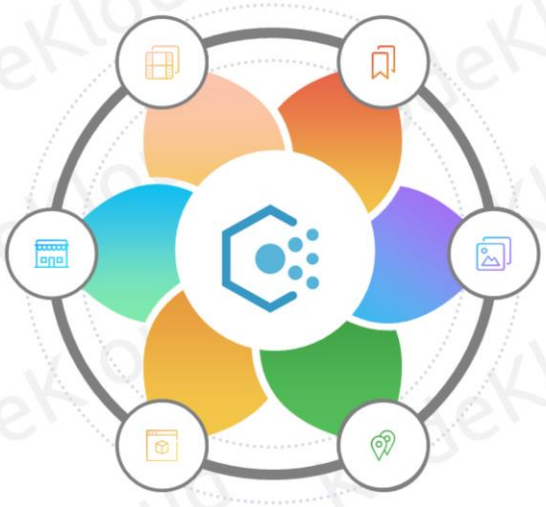
Define a set of resources that can be created in the selected scope

Allowed resource group locations

List of locations where you can create resource groups

Allowed virtual machine SKUs

Define a set of VM SKUs that can be deployed



Require tags

Enforce tags that need to be added to the resources

Inherit tags

Inherit tags from subscription or resource group

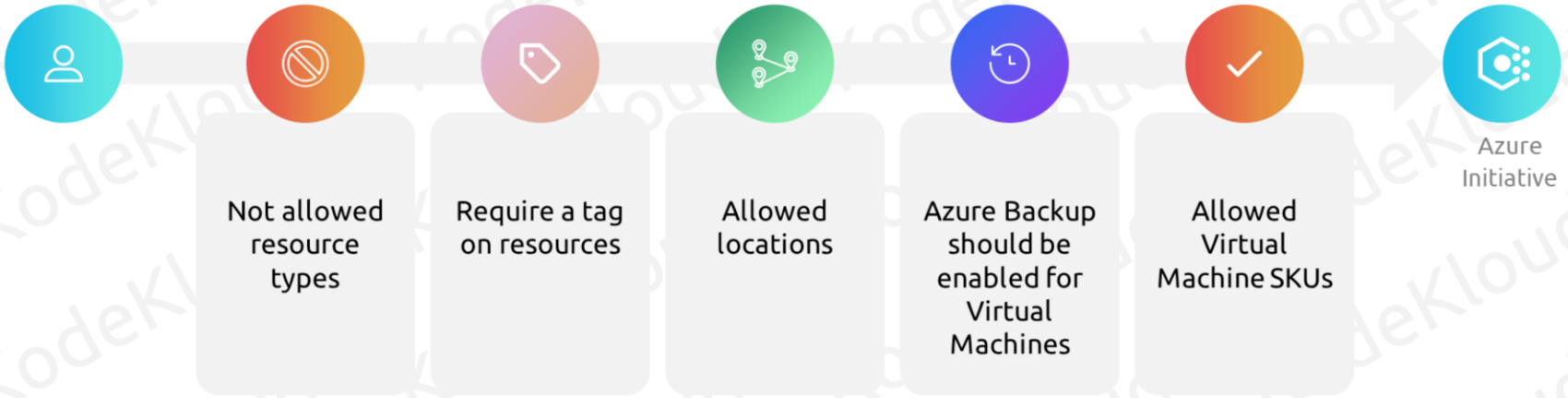
Allowed locations

Define a set of cloud locations where we can deploy resources

Configuring Initiatives

Initiative

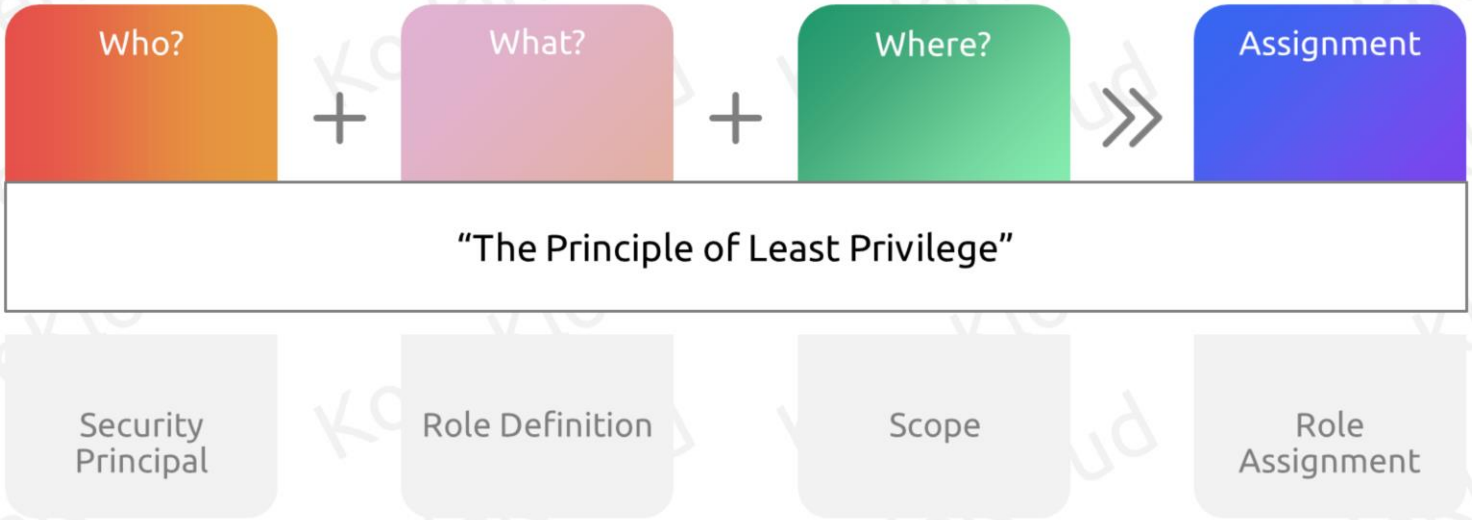
Chaining policy definitions so that they can be assigned as a single item and compliance can be evaluated.



Configure Role-Based Access Control (RBAC)

Role-Based Access Control

Enables administrators to grant access to Azure resources and segregate duties within the team.



Role Definition

Built-in roles

Owner
Contributor
Reader

User Access Administrator
Virtual Machine Contributor

Custom roles

Helpdesk Admin
Webapps Operator

Contributor

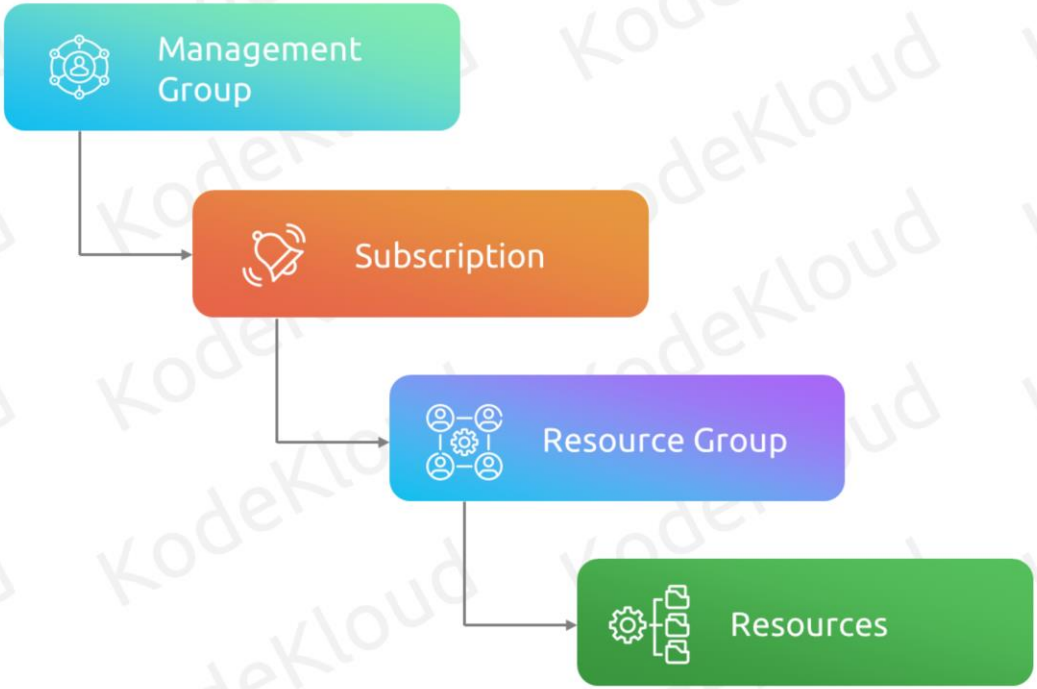
```
{
    "Name":  "Contributor",
    "Id":  "b24988ac-6180-42a0-ab88-20f7382dd24c",
    "IsCustom":  false,
    "Description":  "Grants full access to manage all resources, but does not allow you to
assign roles in Azure RBAC, manage assignments in Azure Blueprints
, or share image galleries.",

    "Actions":  [
        "*"
                ],
    "NotActions":  [
       "Microsoft.Authorization/*/Delete",
       "Microsoft.Authorization/*/Write",
       "Microsoft.Authorization/elevateAccess/Action",
       "Microsoft.Blueprint/blueprintAssignments/write",
       "Microsoft.Blueprint/blueprintAssignments/delete",
       "Microsoft.Compute/galleries/share/action"
                   ],
    "DataActions":  [

                    ],
    "NotDataActions":  [

                       ],
    "AssignableScopes":  [
        "/"
                         ]
}
```

Scope



Azure RBAC v/s Microsoft Entra ID Roles

Azure RBAC vs Microsoft Entra ID Roles

Azure RBAC

- Used to manage access to Azure resources
- Scopes include Management groups, Subscriptions, Resource Groups, and Resources
- Role assignments can be managed via Azure Portal, Azure PowerShell, Azure CLI, ARM templates, and REST API
- Example roles include Owner, Contributor, Reader, User Access Administrator, etc.

Microsoft Entra ID Roles

- Used to manage Microsoft Entra ID features
- Scope is at the Microsoft Entra ID tenant level
- Roles can be managed via Azure Portal, M365 Admin Portal, Microsoft Graph API, Microsoft Entra ID, and Graph PS module
- Example roles include Global Administrator, Billing Administrator, Global Reader, etc.

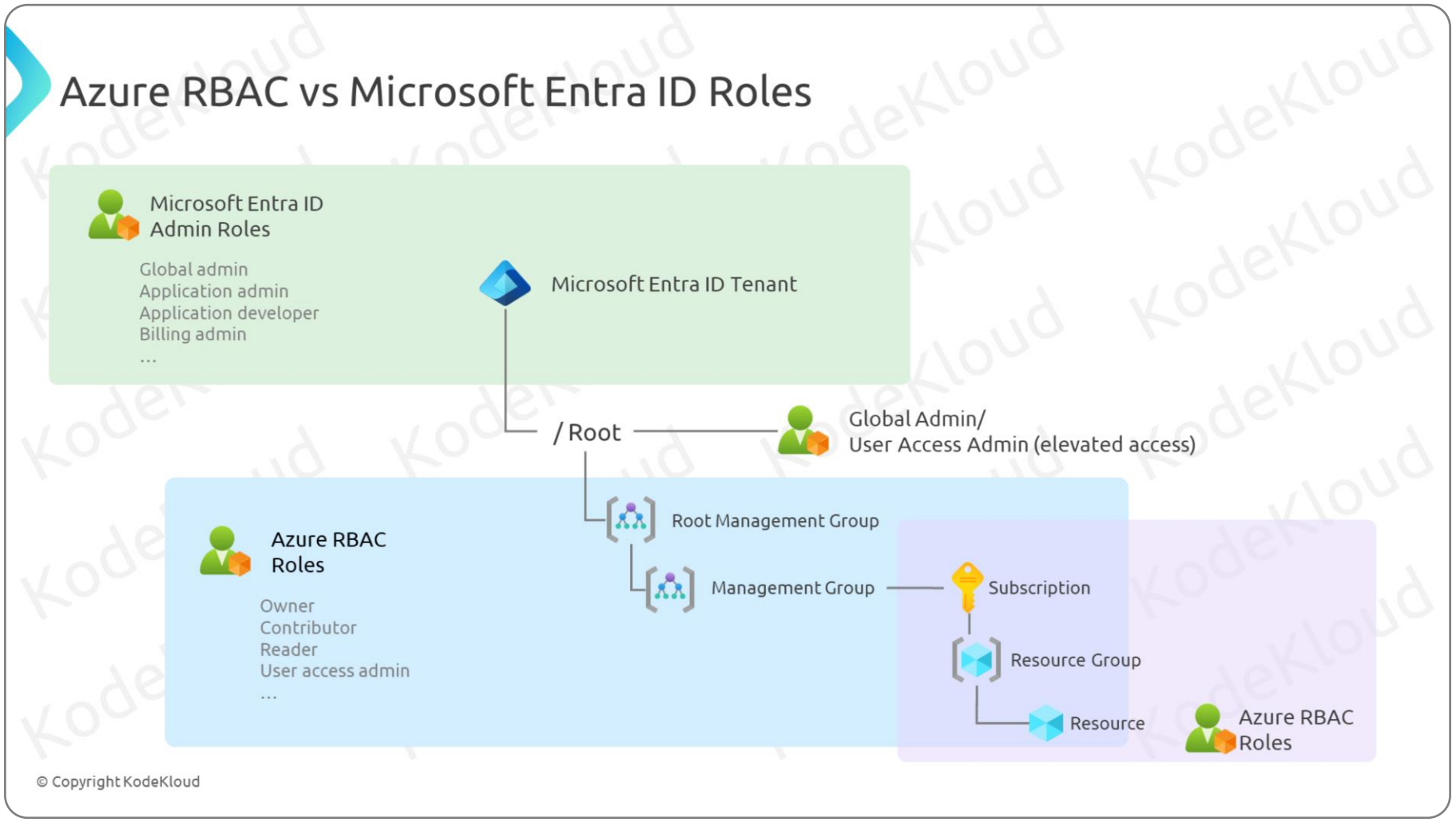


Image source: https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles?WT.mc_id=modinfra-28824-socuff

KodeKloud

Follow us on https://kodekloud.com/ to learn more about us.