Microsoft Azure Administration

Module-02 : Azure Fundamental Concepts

NOVATEC
IT TRAINING & SERVICES

Contents

- Introduction of Microsoft Azure
- Azure Global Infrastructure
- Lab: Creating an Azure Free tier Account
- Overview of Azure Account and Portal
- Azure Subscriptions
- Azure Resource and Resource group
- Subscription governance strategy
- Role Based Access Control (RBAC)

Introduction to Microsoft Azure

Introduction to Microsoft Azure

- **Microsoft Azure** is the public cloud computing platform by Microsoft which offers software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS)
- It comprises more than 200+ cloud services and supports varied operating systems, databases, and developer tools
- Azure Products and Services ranges from Compute, Storage, Networking, Security, Database, Analytics, Monitoring, and many more

Azure Web Services

Virtual Machines

Disks

Backup

Scale Sets

Application Gateway

Application Insights

Azure DevOps

App Services

App Service Plans

Function Apps

Virtual Networks

VNet NAT

Network Security Groups

Storage Accounts

Container Instances

Container Registries

Azure Active Directory

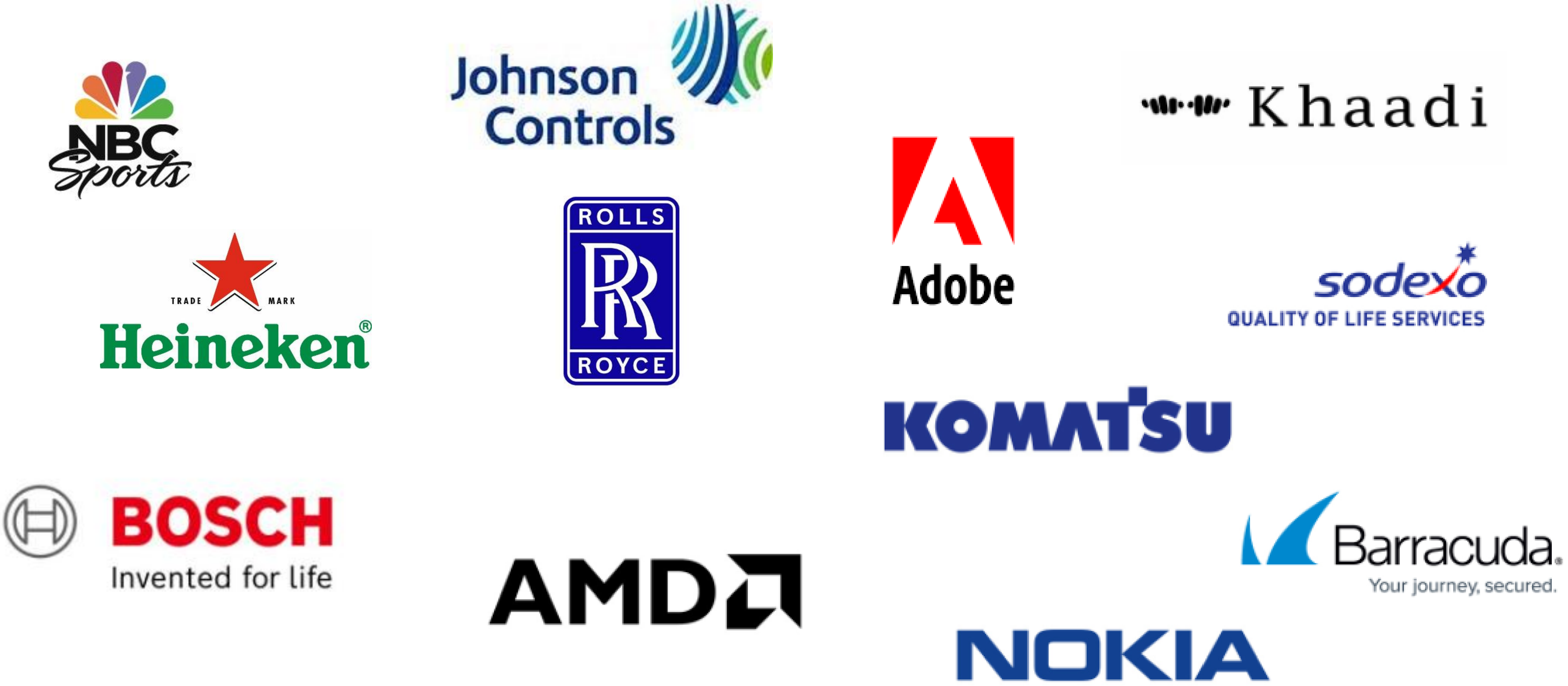
Recovery Service Vaults

Cost & Billing Management

ARM Templates

Key Vault

Microsoft Azure Customers and Partners



For more visit https://azure.microsoft.com/en-us/resources/customer-stories/

Introduction to Microsoft Azure

- Microsoft Azure is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centers
- Azure Datacenters are in about 50+ geographic regions
- **Each region is geographic group of one or more datacenters**
- Deciding the region is the first consideration you need to make before deploying any Azure cloud service
- **Azure region pairs** – Each Azure region is paired with another region. They are connected directly

Ref: https://azure.microsoft.com/en-in/global-infrastructure/geographies/

Different ways of accessing Azure services

Access Microsoft Azure Web-services

Azure Portal

- portal.azure.com
- See all the resources
- Billing and Security
- Customizable

Azure PowerShell

- Azure Modules
- Cross platform
- Leverages PowerShell base knowledge

Azure CLI

- Bash like interface
- Cross platform

Azure Mobile App

- iOS and Android
- Manage resources
- Azure Cloud Shell

Azure REST API

- ARM is based on a REST API

Microsoft Azure Global Infrastructure

Overview Azure Global Infrastructure

- Azure global infrastructure is made up of two key components—***physical infrastructure*** and ***connective network components***
- The physical component is comprised of 200+ physical datacenters, arranged into regions and linked by one of the largest interconnected networks
- With the connectivity of the global Azure network, each of the Azure datacenters provides high availability, low latency, scalability and the latest advancements in cloud infrastructure—all running on the Azure platform

Ref: https://infrastructuremap.microsoft.com/

Azure Global Infrastructure Terminologies

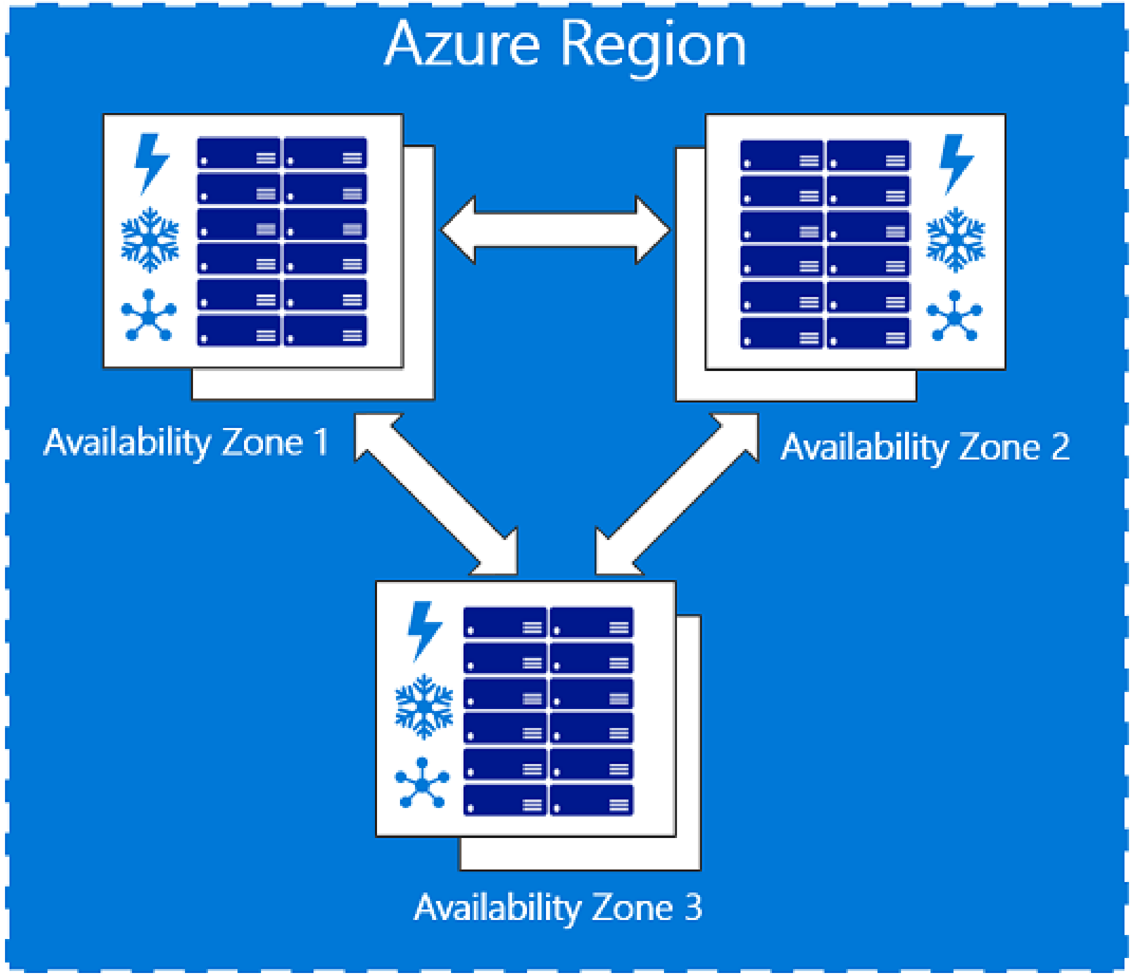
- **Azure Datacenters**: Azure datacenters are unique physical buildings located all over the globe—that house a group of networked computer servers
- **Azure Region**: An Azure region is a set of datacenters, deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network
- **Azure Availability Zone**: Azure Availability Zones are unique physical locations within an Azure region and offer high availability to protect your applications and data from datacenter failures. Each zone is made up of one or more datacenters equipped with independent power, cooling and networking

Azure Global Infrastructure Terminologies

- **Azure Global Network**: The Azure global network refers to all the components in networking and is comprised of the Microsoft global wide-area network (WAN), points of presence (PoPs), fiber etc.
- **Azure Geographies**: Each Azure geography contains one or more **regions** and meets specific data residency and compliance requirements. This lets you keep your business-critical data and apps nearby on fault-tolerant, high-capacity networking infrastructure

Azure Geographies

(Ref: https://azure.microsoft.com/en-in/global-infrastructure/geographies/)



Azure Geographies (Regions and Availability Zones)

- **Region**: A region is a set of datacenters deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network
- **Availability Zones**: An Availability Zone is a high-availability offering that protects your applications and data from datacenter failures
  1. Availability Zones are unique physical locations within an Azure region
  2. Each zone is made up of one or more datacenters equipped with independent **power, cooling, and networking**
  3. To ensure resiliency, there's a minimum of three separate zones in all enabled regions
  4. The physical separation of Availability Zones within a region protects applications and data from datacenter failures

Ref: https://docs.microsoft.com/en-us/azure/availability-zones/az-overview

Different ways of buying Azure services

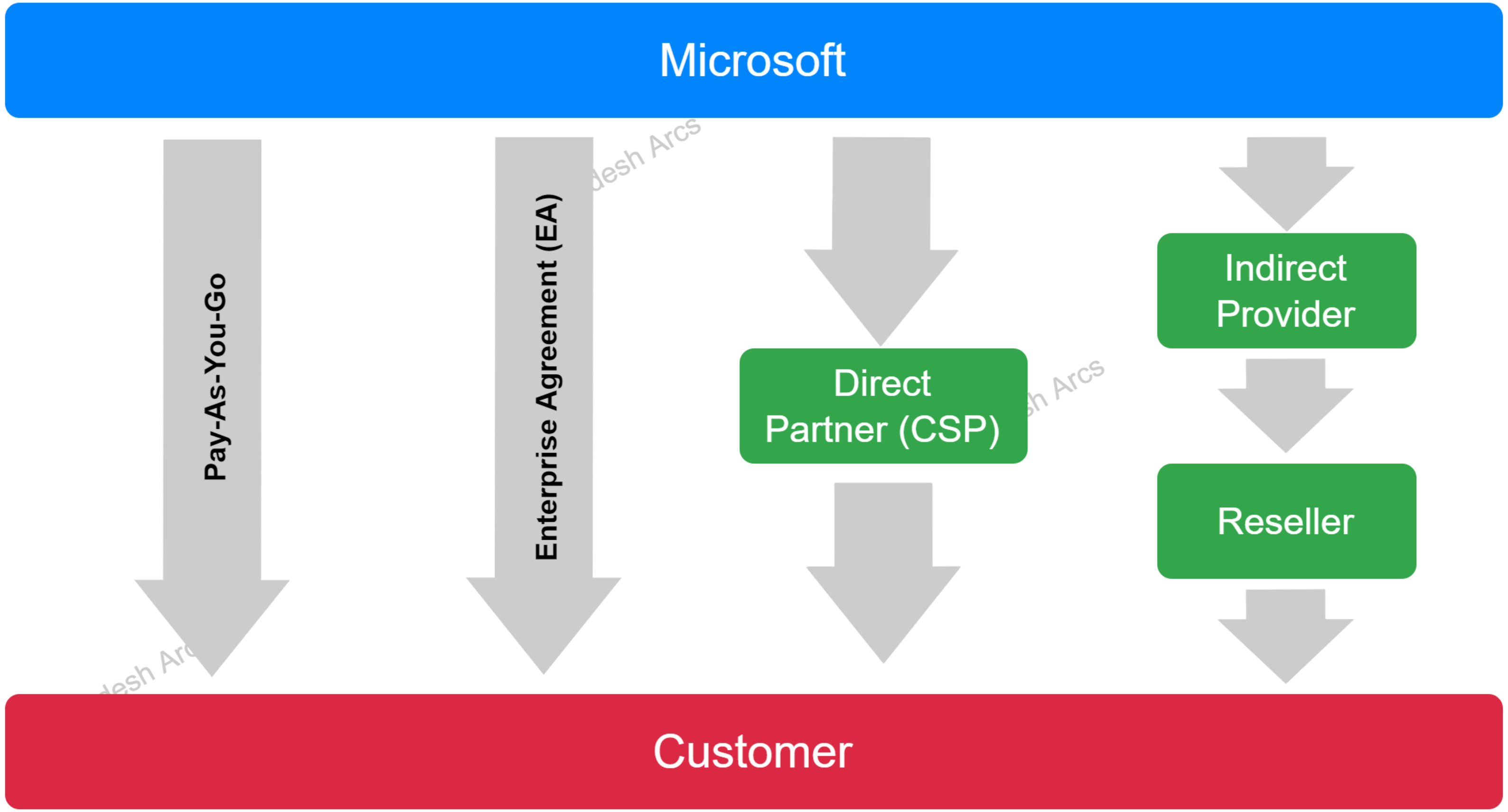
Different ways of buying Azure services

There are basically three different ways how you can buy Azure Services:

1. Buy direct from Microsoft (Pay-as-you-Go)
2. Enterprise Agreement (EA)
3. Cloud Solution Partner (CSP)

Ref: https://azure.microsoft.com/en-in/pricing/purchase-options/

Different ways of buying Azure services



1. Direct from Microsoft 1 of 2

- You can buy Azure Services directly from Microsoft.
- It means that the invoice is generated directly by Microsoft, and any issues that you have will be handled directly with them.
- Microsoft does not offer support from how to setup and configure Azure Services
- You just buy Azure Services, and you are fully responsible for configuring and managing them
- From the cost perspective, usually, when you buy services directly from Microsoft, you have Pay-As-You-Go subscriptions, where the Azure resources price are the same as the one listed on Azure Pricing. You don't get special discounts or deals

1. Direct from Microsoft 2 of 2

- **Pros**
  1) Continue with usual procurement of Azure Cloud Services
  2) Extensive technical support experience
- **Cons**
  1) Higher rates for products
  2) Slower support turnaround
  3) Lack of Implementation/Installation
  4) Poor business consultation

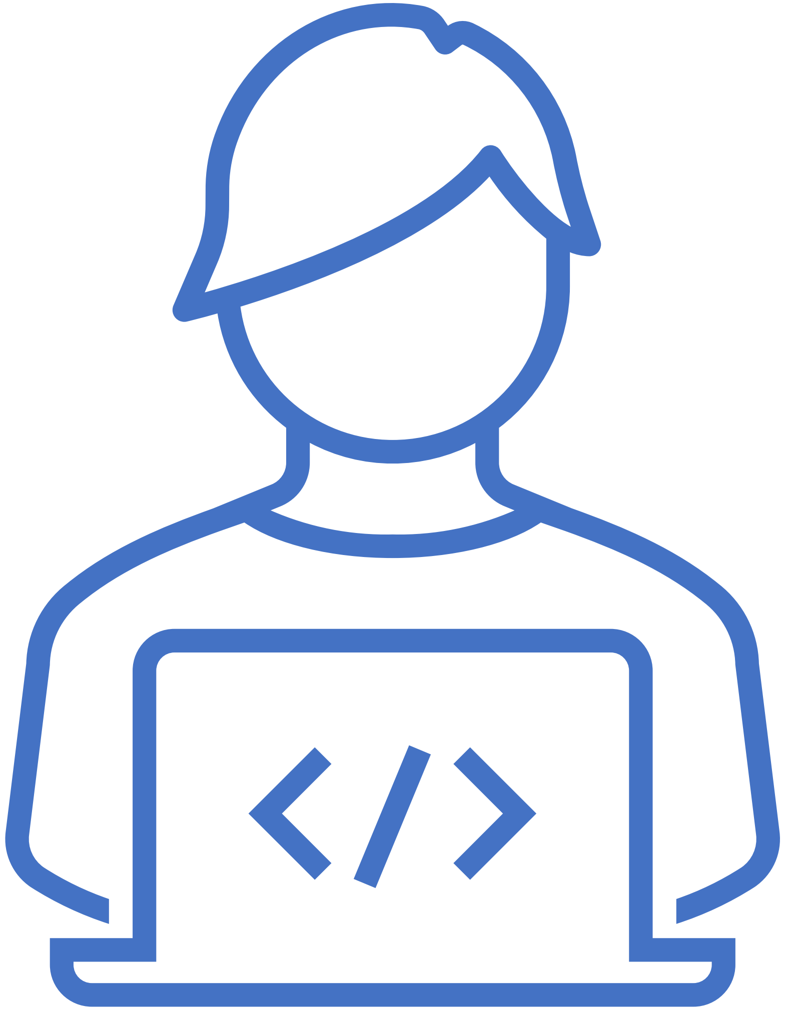
2. Enterprise Agreement (EA)

- An Enterprise Agreement is designed for very large organizations (only the largest customers qualify for an EA) that want to license software and cloud services for a **minimum three-year period**
- With this long-term commitment and volume, customers are given a substantial discount
- Pros
  1) Large enterprises can buy cloud services and licenses under one agreement
  2) Substantial discounts for high volume purchases
- Cons
  1) Lack of flexibility
  2) Locked into long term contracts for licenses

3. Cloud Solution Partners (CSP)

- Direct CSP work directly with Microsoft
- They receive deeply discounted prices for Azure Cloud Services and offers an extensive level of digital transformation and support
- Pros
  1) Azure Cloud Services are discounted in comparison to Indirect CSP and Microsoft offerings
  2) A personable technical support experience from an accredited team
  3) Consultants in place to examine your business and suggest solutions
  4) Ability to turn services on or off as needed
- Cons
  1) Prices higher than EA

Hands-on Labs

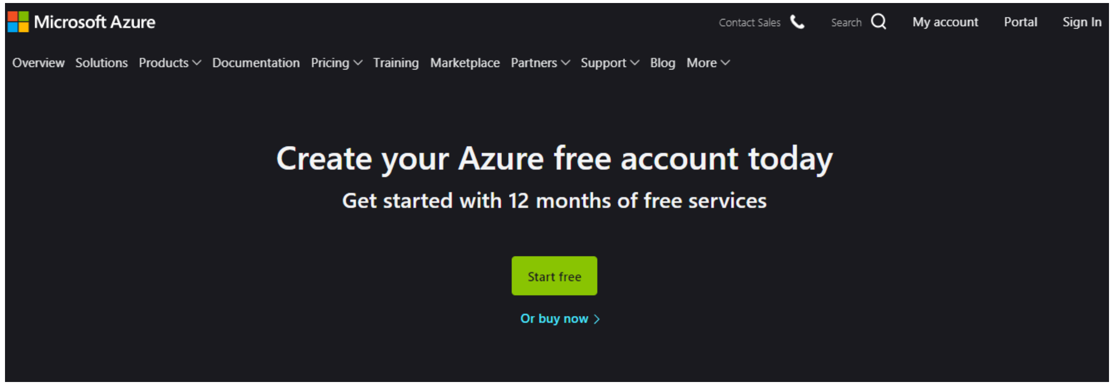


Lab – Creating an Azure Account (Free Tier)

Hand-on Lab: Creating an Azure Account (Free Tier)

1) Go to https://azure.microsoft.com/en-in/free/

2) Click on Start Free button



Create your Azure free account today

Get started with 12 months of free services

3) This will take you to Microsoft sign-in page. Enter you credentials and proceed (in case you do not have one, then sign-up first)

4) Enter your personal details and then credit card details in the payment option

Hand-on Lab: Creating an Azure Account (Free Tier)

5) You’ll also need to supply a valid credit card. Prepaid credit cards won’t work — you’ll need a “normal” credit or debit card.

6) There is no charge involved with the setting up of a trial account. Microsoft just wants to see your card to verify your identity. There will be, however, a record for a $0 transaction on your bank statement. Next – tick “I agree” and click “Sign Up.”

7) Within a few seconds, your account will be ready. That’s it! Your Microsoft Azure account has been created.

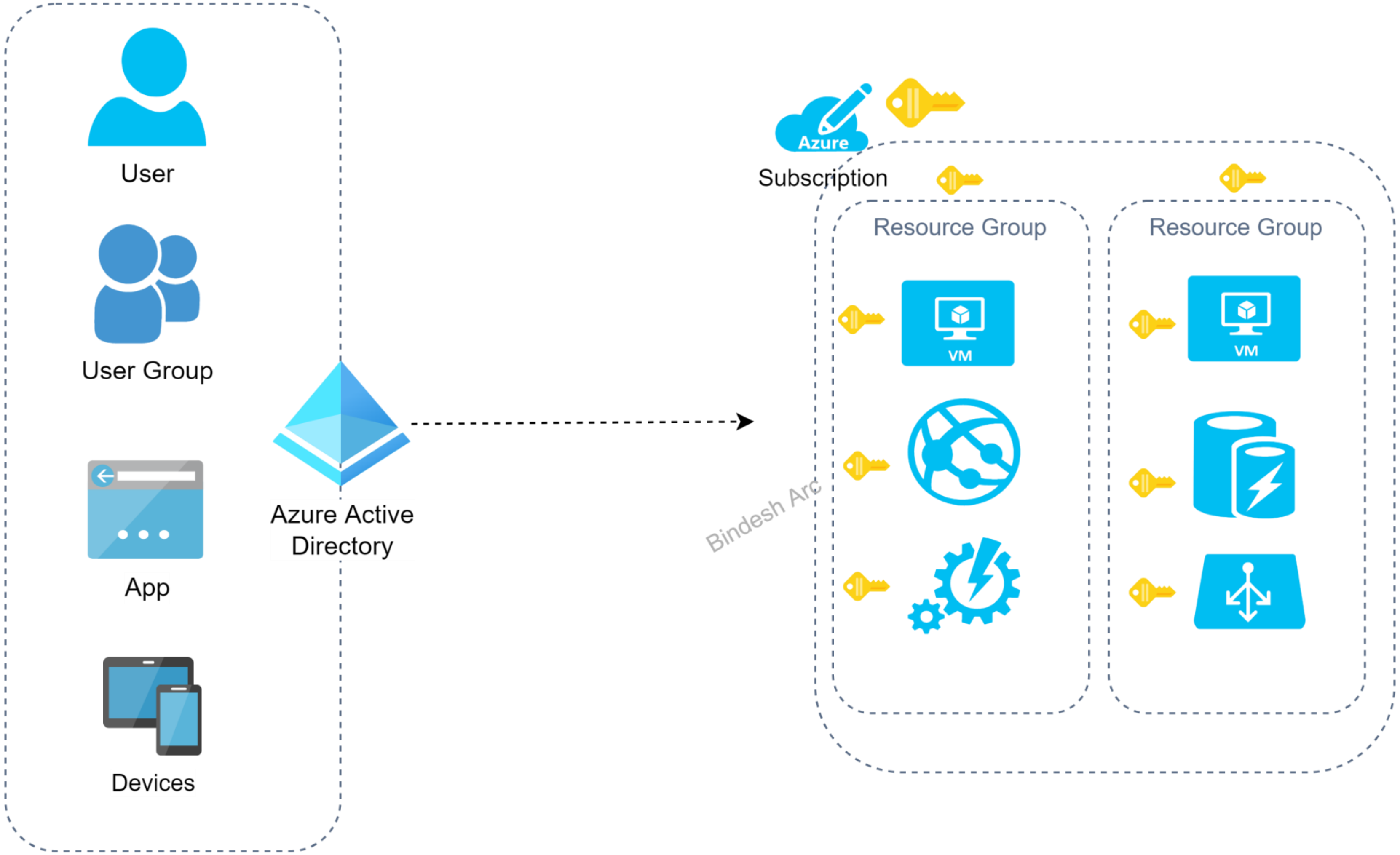
8) To continue, click the “My Account” link at the top right corner or go straight to the Microsoft Azure portal: https://www.portal.azure.com/

Lab – Installation of Az PowerShell Module

Ref: https://docs.microsoft.com/en-us/powershell/azure/install-az-ps

Walkthrough of MS Azure Portal

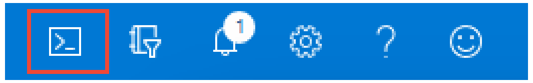
Microsoft Azure Account Architecture



Azure Cloud Shell

Overview of Azure Cloud Shell

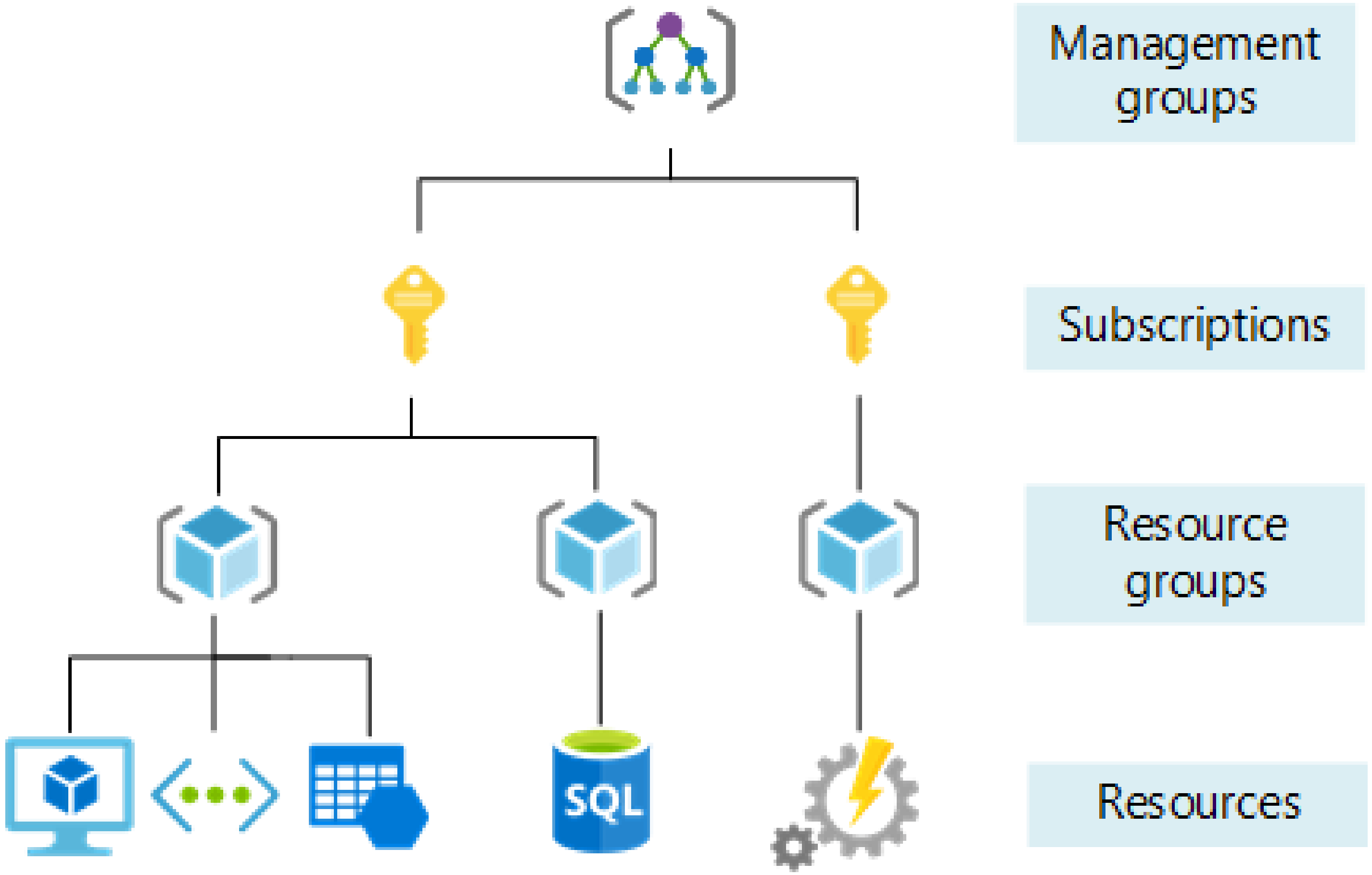
- Azure Cloud Shell is an interactive, authenticated, browser-accessible shell for managing Azure resources
- It provides the flexibility of choosing the shell experience that best suits the way you work, either **Bash** or **PowerShell**
- You can access the Cloud Shell basically in two ways:
  1. **Direct link**: Open a browser to https://shell.azure.com
  2. **Azure portal**: Select the Cloud Shell icon on the Azure portal



- Difference between Azure PowerShell and Azure CLI
- Sample PowerShell command: Get-AzResourceGroup
- Sample Azure CLI command: az group list

Microsoft Azure Organization Hierarchy

Azure Organization Hierarchy



Azure Accounts

- Azure is primarily organized by **Accounts** and **Subscriptions**
- Each Account can have multiple subscriptions associated with it
- The primary account delegates privileges at subscription level
- **Account administrator** is the user created with the account
- **Account administrator** can create the Billing method
- **Account administrator** can create/cancel subscriptions
- **Account administrator** can create/change the subscription level administrator

Azure Management Groups

- **Management groups** are containers that help you manage access, policy, and compliance across multiple subscriptions.
- Create these containers to build an effective and efficient hierarchy that can be used with **Azure Policy** and **Azure Role Based Access Controls (RBAC)**.

Ref : https://docs.microsoft.com/en-us/azure/governance/management-groups/create-management-group-portal

Azure Subscriptions

- An **Azure subscription** is a logical container used to provision resources in Azure
- To consume Azure services, you need **Subscriptions**
- **Subscriptions** can be personal or organizational
- **Subscriptions** have isolation of administration & billing
- Separate privileges can be assigned to separate subscriptions
- Subscriptions have quotas and limits
- Subscriptions have RBAC roles

Azure Subscriptions – Principles

- Administrative security boundary
- Support RBAC (Role Based Access Control) delegation
- A billing unit
- Logical limit of scale
- First container that you create
- Subscriptions do not cost anything
- Each subscription has its own Admins, although a single account can be an admin in multiple subscriptions
- Subscriptions are global

Azure Resource Overview

Role Considerations

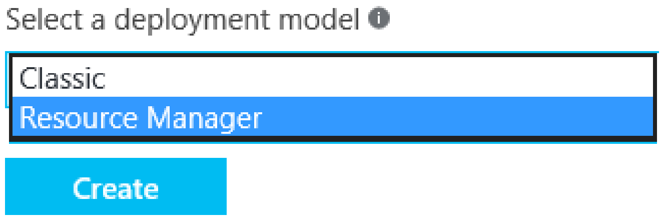
Azure Subscriptions have two administrative models:

Classic (v1)

- Azure Service Management (ASM)

Resource Manager (v2)

- Azure Resource Manager (ARM)



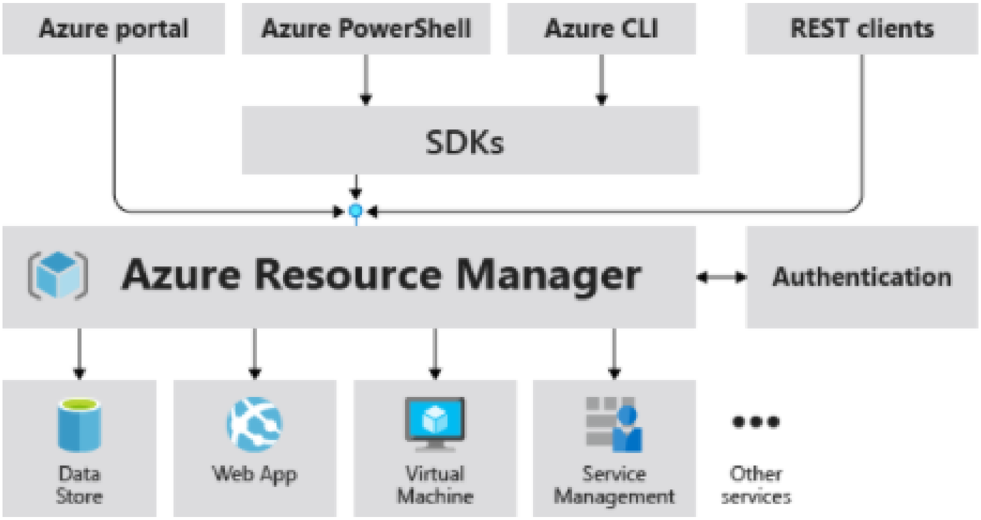
Select a deployment model

Classic

Resource Manager

What is Azure Resource Manager (ARM)?

- **Azure Resource Manager** is the deployment and management service for Azure
- It provides a management layer that enables you to create, update, and delete resources in your Azure account
- You use management features, like access control, locks, and tags, to secure and organize your resources after deployment
- Consistent Management layer

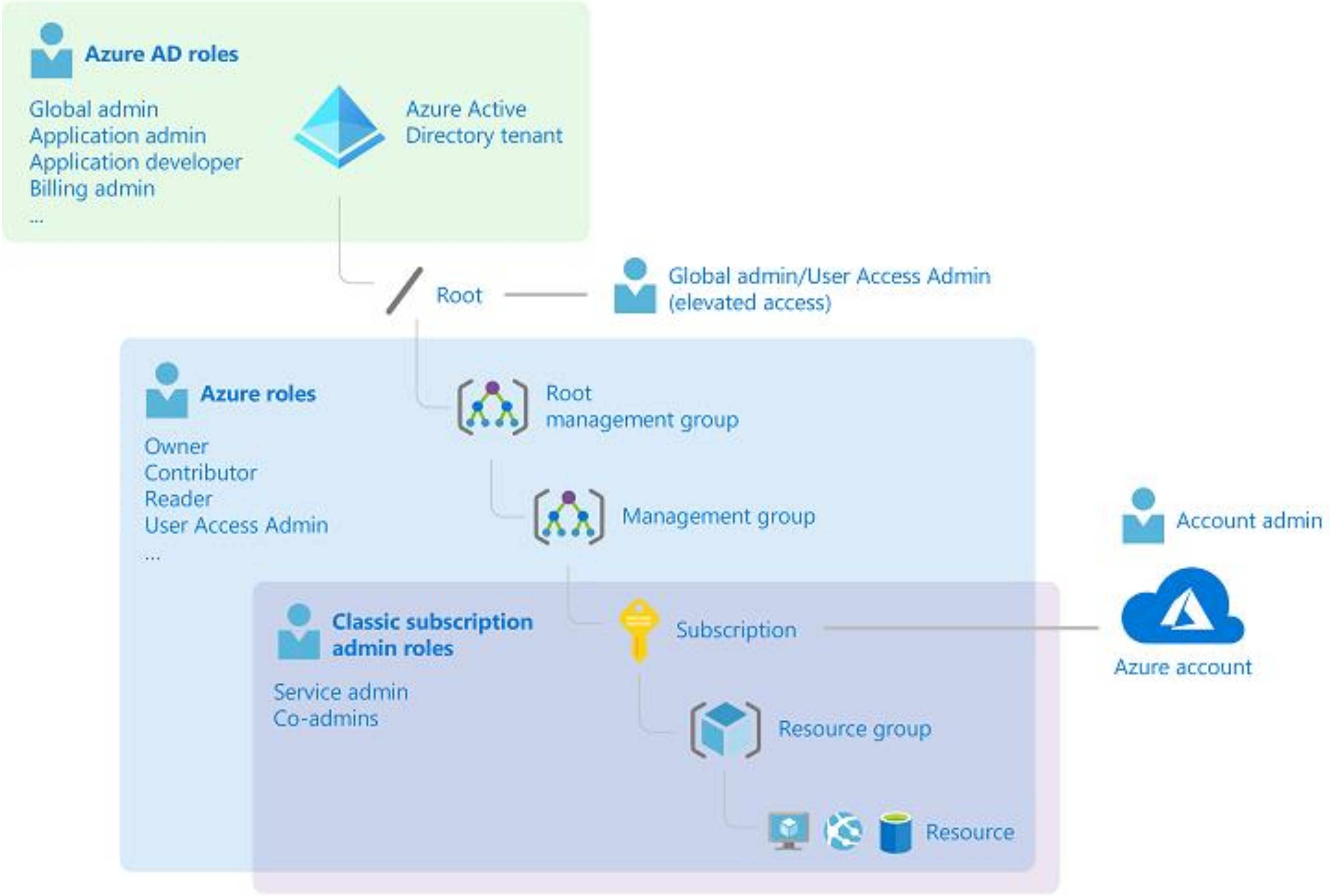


Resources in Microsoft Azure

- Azure Resource Management (ARM) environment, a subscription now has two administrative models: **Azure Service Management (ASM)** and **Azure Resource Management (ARM)**
- With ARM the subscription is no longer needed as an administrative boundary
- ARM provides a more granular Roles Based Access Control (RBAC) model for assigning administrative rights at the resource level
- RBAC is currently being released in stages, 70 new roles have been released and user defined roles is coming in a future release
- There will be some complexity during the coexistence of the service management and resource management environments and will need to be carefully considered

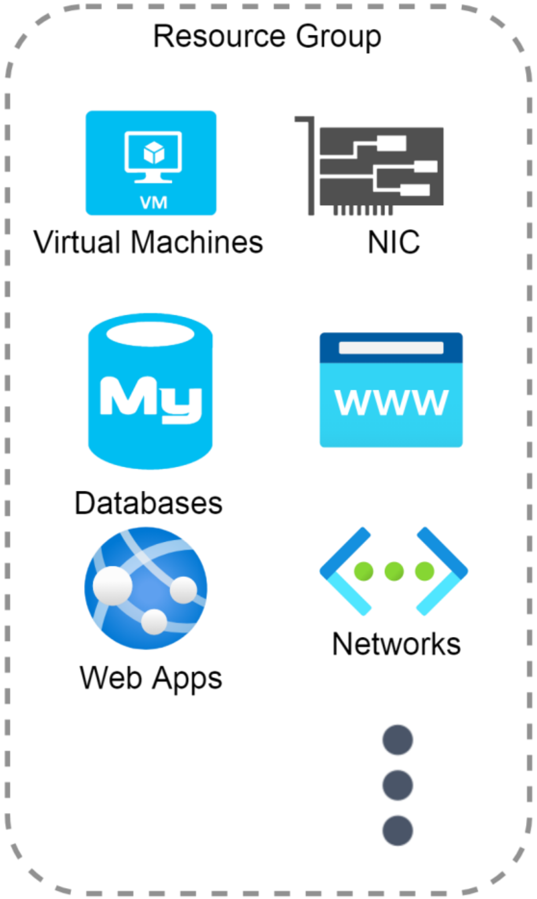
Important Terminologies

1) **Resource** - A manageable item that is available through Azure. Virtual machines, storage accounts, web apps, databases, and virtual networks are examples of resources.
2) **Resource Group** - A container that holds related resources for an Azure solution. The resource group includes those resources that you want to manage as a group.
3) **Azure Resource Manager (ARM) template** - A JavaScript Object Notation (JSON) file that defines one or more resources to deploy to a resource group, subscription, management group, or tenant.

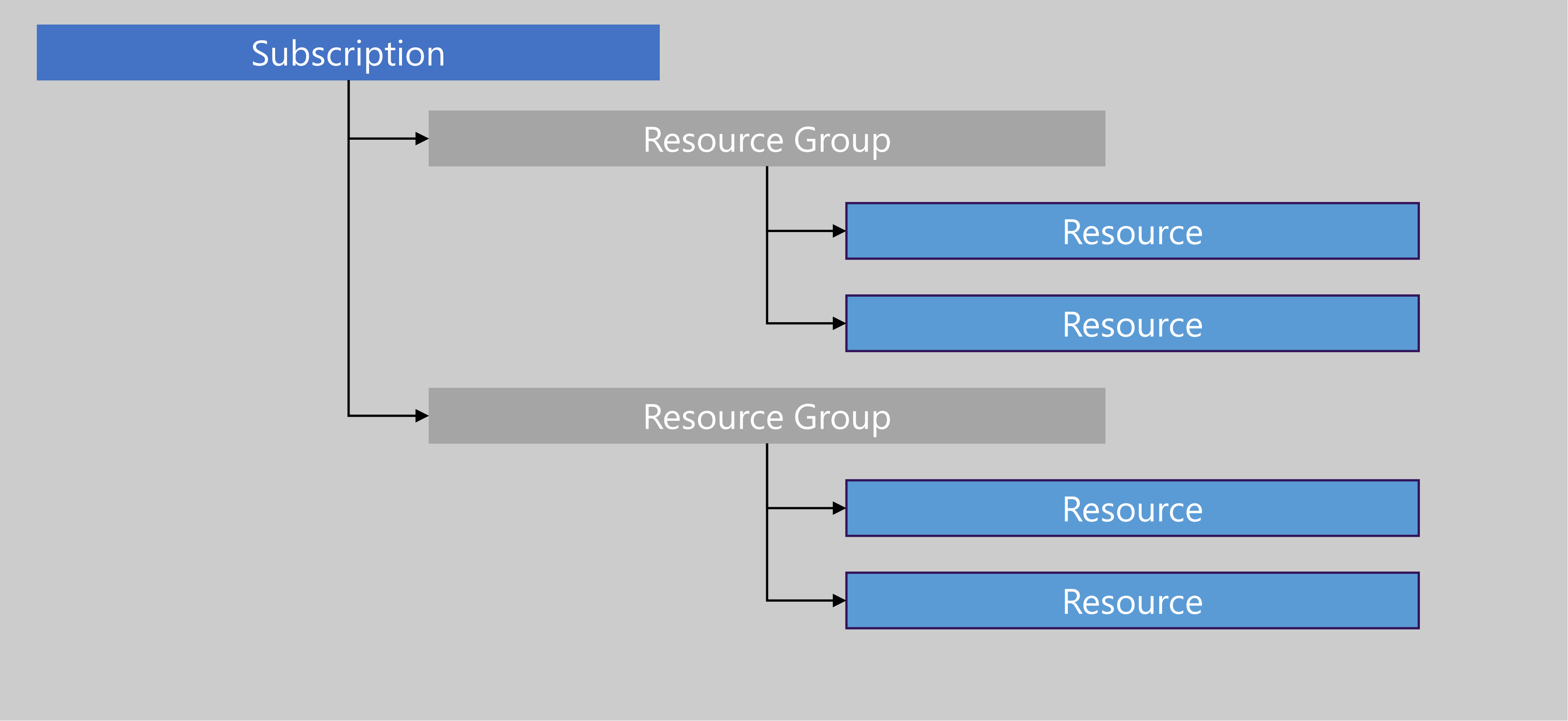

Azure AD roles
Global admin
Application admin
Application developer
Billing admin
...
Azure Active Directory tenant
Root
Global admin/User Access Admin (elevated access)
Azure roles
Owner
Contributor
Reader
User Access Admin
...
Root management group
Management group
Account admin
Classic subscription admin roles
Service admin
Co-admins
Subscription
Azure account
Resource group
Resource

What is Azure Resource Group?

- A **resource group** is a container that holds related resources for an Azure solution.
- The **resource group** can include all the resources for the solution, or only those resources that you want to manage as a group.
- You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization.
- Generally, add resources that share the same lifecycle to the same resource group so you can easily deploy, update, and delete them as a group.



Resource Groups and Hierarchy



Subscription

Resource Group

Resource

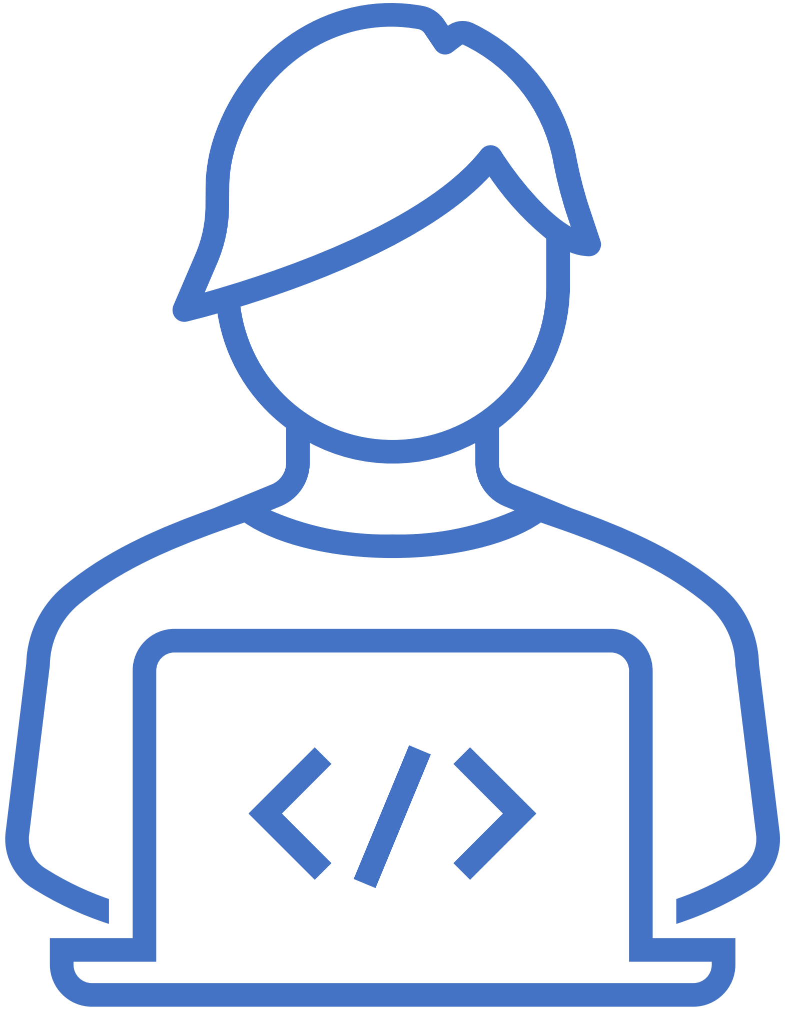
Resource

Resource Group

Resource

Resource

Hands-on Labs



Hand-on Lab: Creating a Resource Group

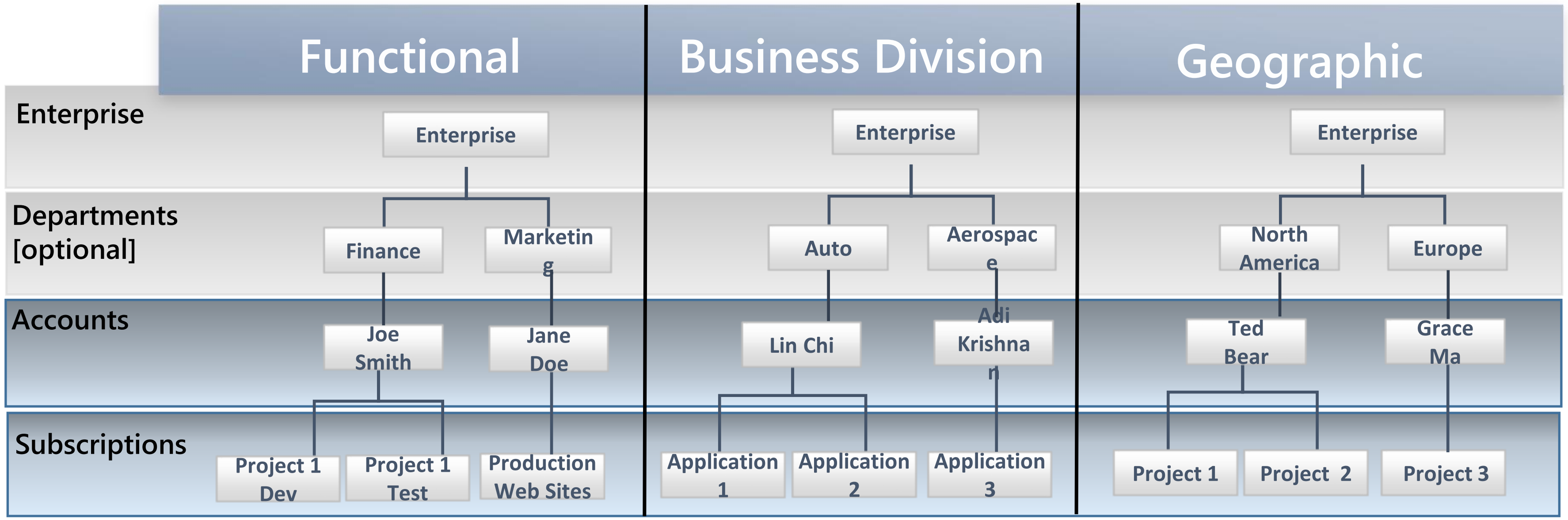
1) Create an Azure Resource Group from Azure Portal

2) Create an Azure Resource Group using PowerShell

```
New-AzResourceGroup -Name <ResourceGrpName> -Location "South Central US"
```

Azure Subscription Governance Strategies

Azure Subscription Governance strategies



	Functional	Business Division	Geographic
Enterprise	Enterprise	Enterprise	Enterprise
Departments [optional]	Finance Marketing	Auto Aerospace	North America Europe
Accounts	Joe Smith Jane Doe	Lin Chi Adi Krishnan	Ted Bear Grace Ma
Subscriptions	Project 1 Dev Project 1 Test Production Web Sites	Application 1 Application 2 Application 3	Project 1 Project 2 Project 3

- The Azure governance layers, roles, portals etc.. provide the technical means that can be used in different ways
- Some customer prefer to use functional differentiation, others business division based or geographical or even a combination

Subscription Considerations

Management approach

- Single team or distributed
- RBAC

Security requirements

- Data or network security
- Environments - Sandbox, Dev, Test, UAT, Pre-Prod, Prod

Connectivity requirements

- Single point of ingress?
- Multiple regions?

Application requirements : Data flow, Compliance

Subscription per Department (Customer Managed)

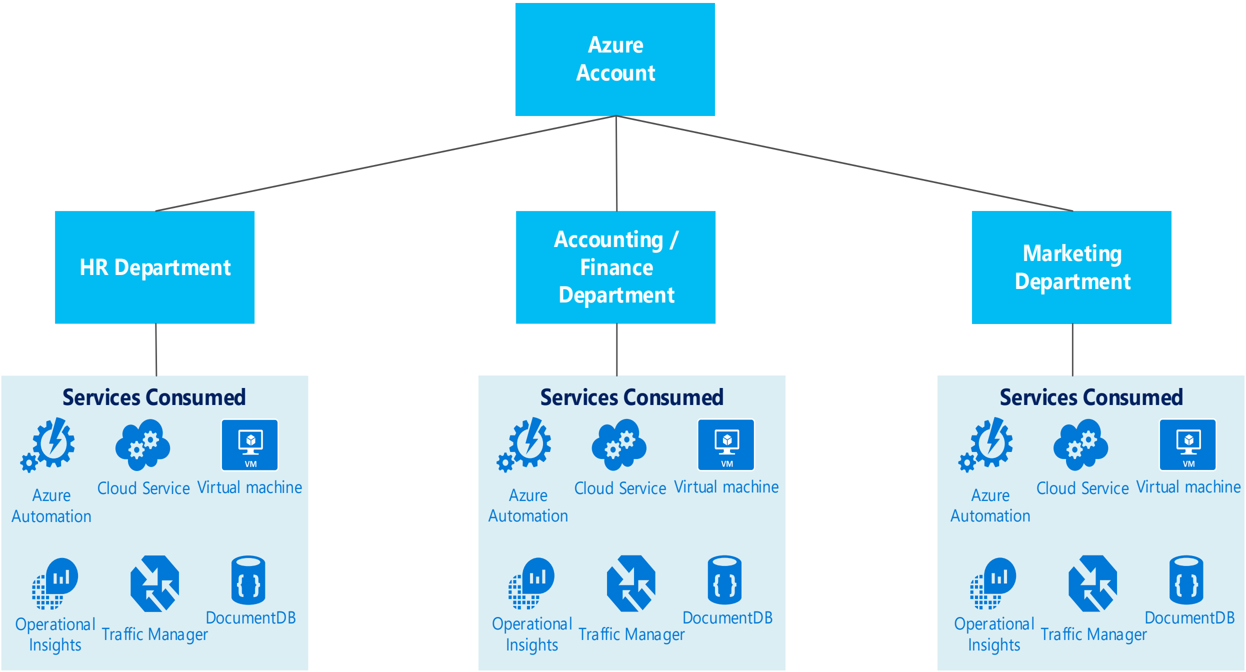
Each department contains different types of environments (e.g. Prod, Non-Prod). Virtual Networks will wrap the different environments for traffic separation. Subnets will be created within each environment to establish required security isolation zones between applications.

Pros

- Low ExpressRoute Circuit Costs
- Simplified Subscription Management
- No Vnet Subscription Limit

Cons

- Granular RBAC model required
- Subscription Limit Issues in Cores, Storage, NSGs
- Complex Vnet addressing
- Mistake in management will affect all environments



Subscription per Environment (Customer Managed)

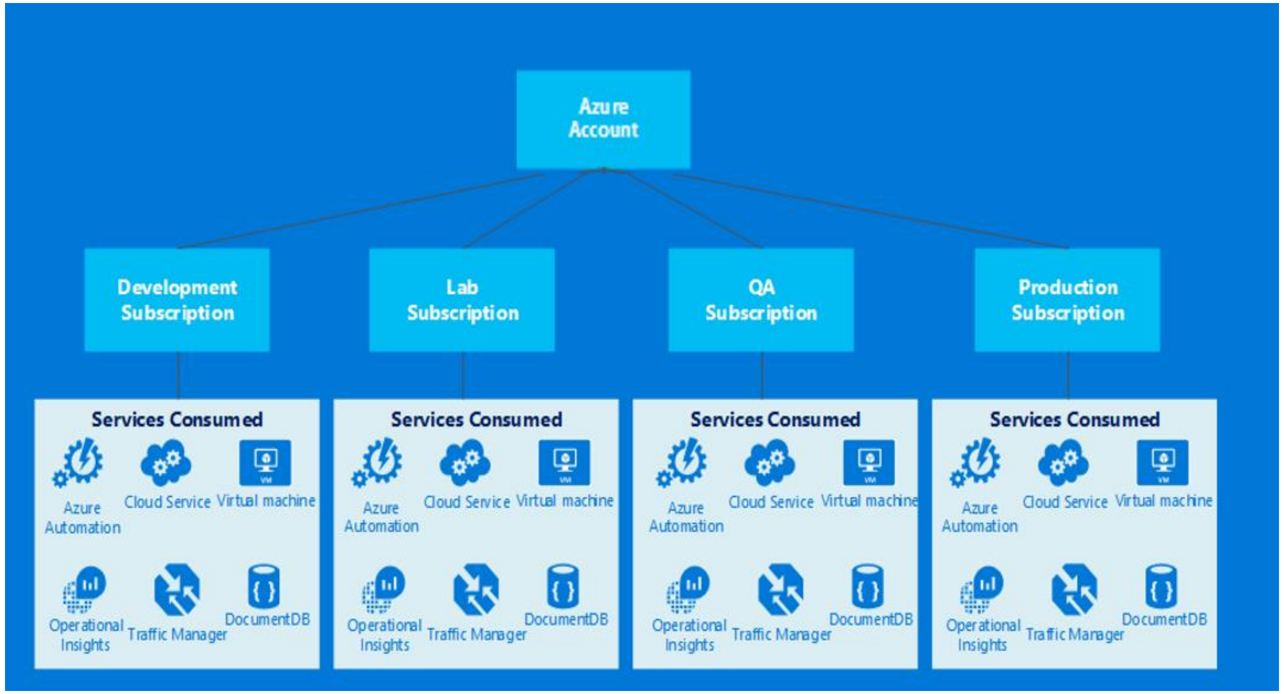
Each environment contains the different types of applications. Virtual Networks will wrap the different applications for traffic separation. Subnets will be created within each environment to establish required security isolation zones among application tiers.

Pros

- Shared ExpressRoute circuit model
- Low Vnet subscription limit issues (Limit Per 100th application)
- Vnet address spaces can be tailored per application

Cons

- New ExpressRoute circuit required per 10th application, or ER Premium
- Granulated Application RBAC model
- Requires medium capacity planning
- Max of 10 dedicated circuits per subscription, max of 100 applications



Subscription per Application (Customer Managed)

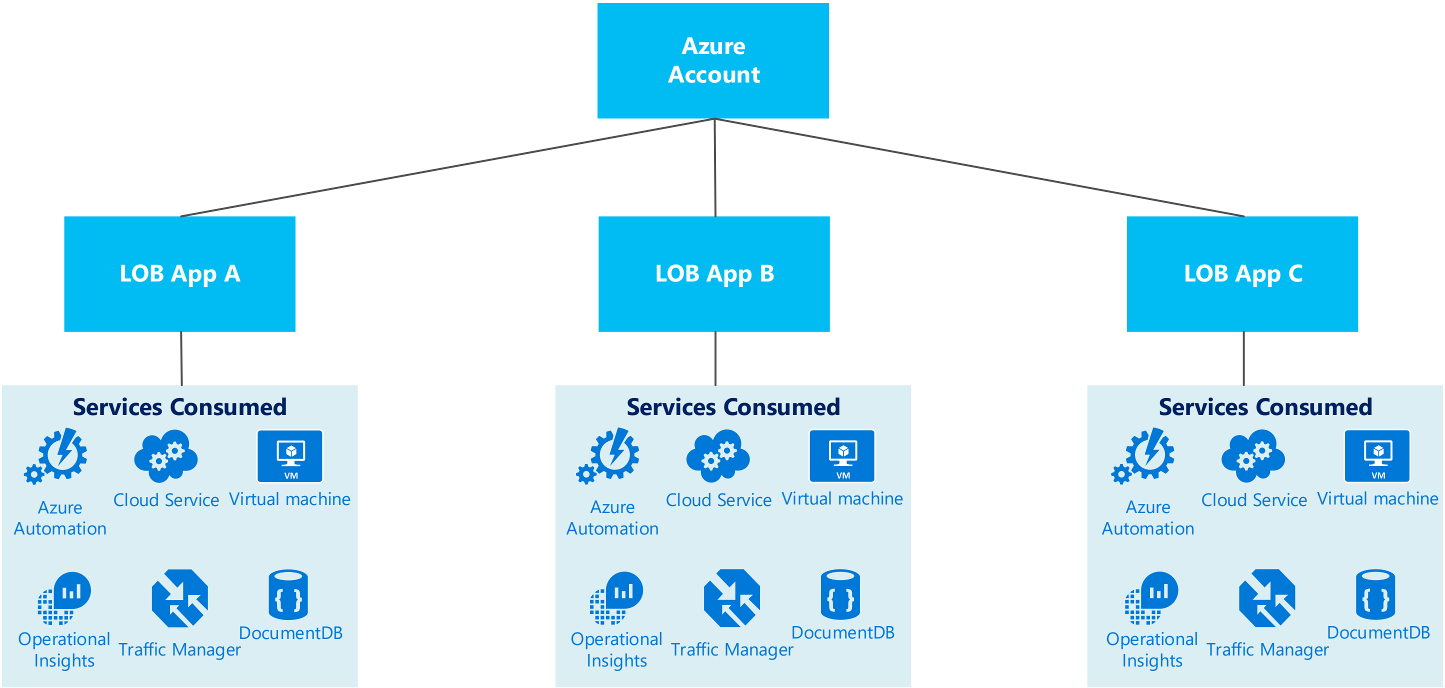
Each application contains the different tiers. Virtual Networks will wrap the different tiers for traffic separation. Subnets will be created within each tier to establish required security isolation zones.

Pros

- Minimal Subscription limit issues.
- Minimal Capacity Planning
- Per Application RBAC model

Cons

- Increased Network Costs
- Management Complexity



Create a Subscription Governance Strategy

- At the beginning of any cloud governance implementation, you identify a cloud organization structure that meets your business needs
- Teams often start their Azure governance strategy at the subscription level
- There are three main aspects to consider when you create and manage subscriptions:

  1. Billing – US Team, India Team
  2. Access control – Test, UAT, QA, Production
  3. Subscription limits

Azure Management Portals

Portal	Location	Purpose
Enterprise Portal	https://ea.azure.com/	• Manage access • Manage accounts • Manage subscriptions • View price sheet • View usage summary • Manage usage & lifecycle email notifications • Manage Authentication Types
Management Portal	https://portal.azure.com	• Provision/de-provision Azure services • Manage co-administrators on subscriptions • Open support tickets for issues within the subscription

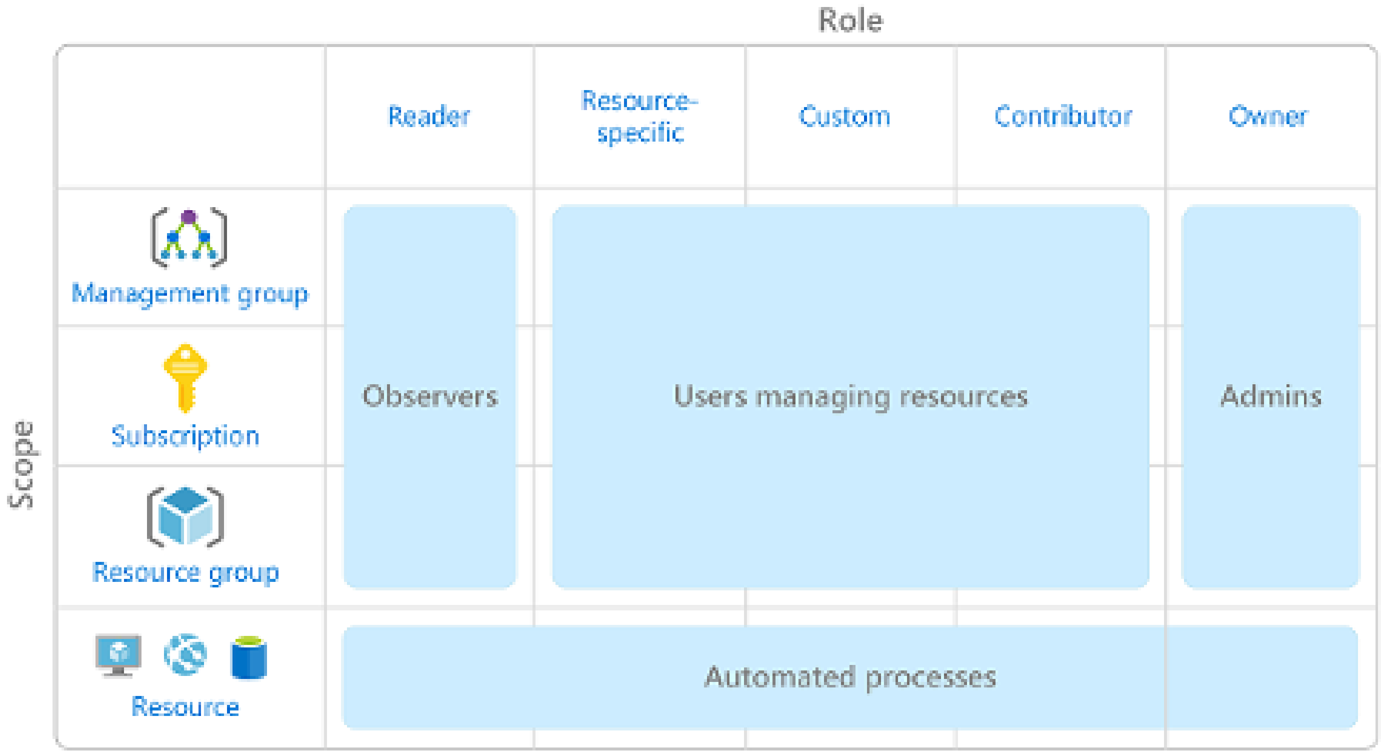
Role Based Access Control (RBAC)

What is RBAC?

- RBAC stands for **Role Based Access Control**
- When you have multiple IT teams, you can control what access they must have to the resources in your cloud environment
- It's a good security practice to grant users only the rights they need to perform their job, and only to the relevant resources
- Instead of defining the detailed access requirements for everyone, and then updating access requirements when new resources are created, Azure enables you to control access through **Azure role-based access control (Azure RBAC)**

How is RBAC is applied to Azure resources?

Role-based access control is applied to a scope, which is a resource or set of resources that this access applies to.



How RBAC is applied to Azure resources?

When you grant access at a parent scope, those permissions are inherited by all child scopes.

1. When you assign the Owner role to a user at the management group scope, that user can manage everything in all subscriptions within the management group
2. When you assign the Reader role to a group at the subscription scope, the members of that group can view every resource group and resource within the subscription
3. When you assign the Contributor role to an application at the resource group scope, the application can manage resources of all types within that resource group, but not other resource groups within the subscription

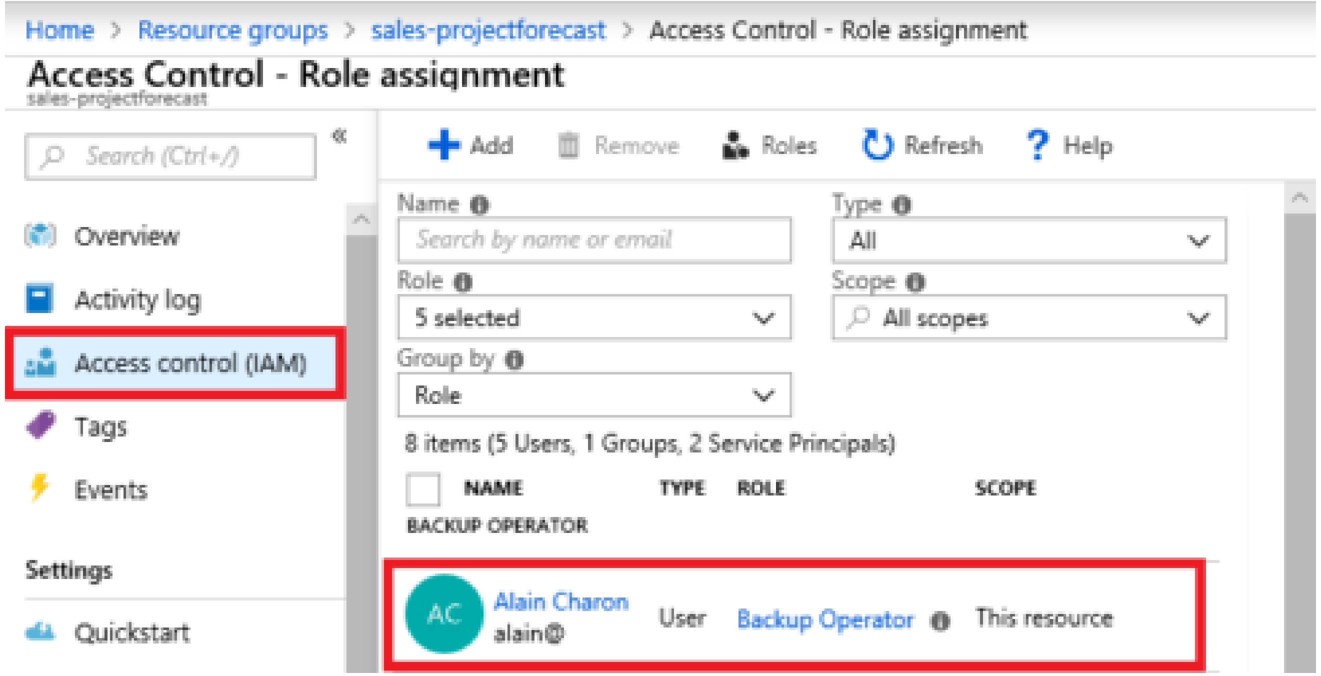
When to Use RBAC?

Use Azure RBAC when you need to:

- ✓ Allow one user to manage VMs in a subscription and another user to manage virtual networks.
- ✓ Allow a database administrator group to manage SQL databases in a subscription.
- ✓ Allow a user to manage all resources in a resource group, such as virtual machines, websites, and subnets.
- ✓ Allow an application to access all resources in a resource group.

How to manage Azure RBAC Permissions?

- You can manage access permissions on the **Access control (IAM)** pane in the Azure portal.
- This pane shows who has access to what scope and what roles apply.
- You can also grant or remove access from this pane.



Home > Resource groups > sales-projectforecast > Access Control - Role assignment

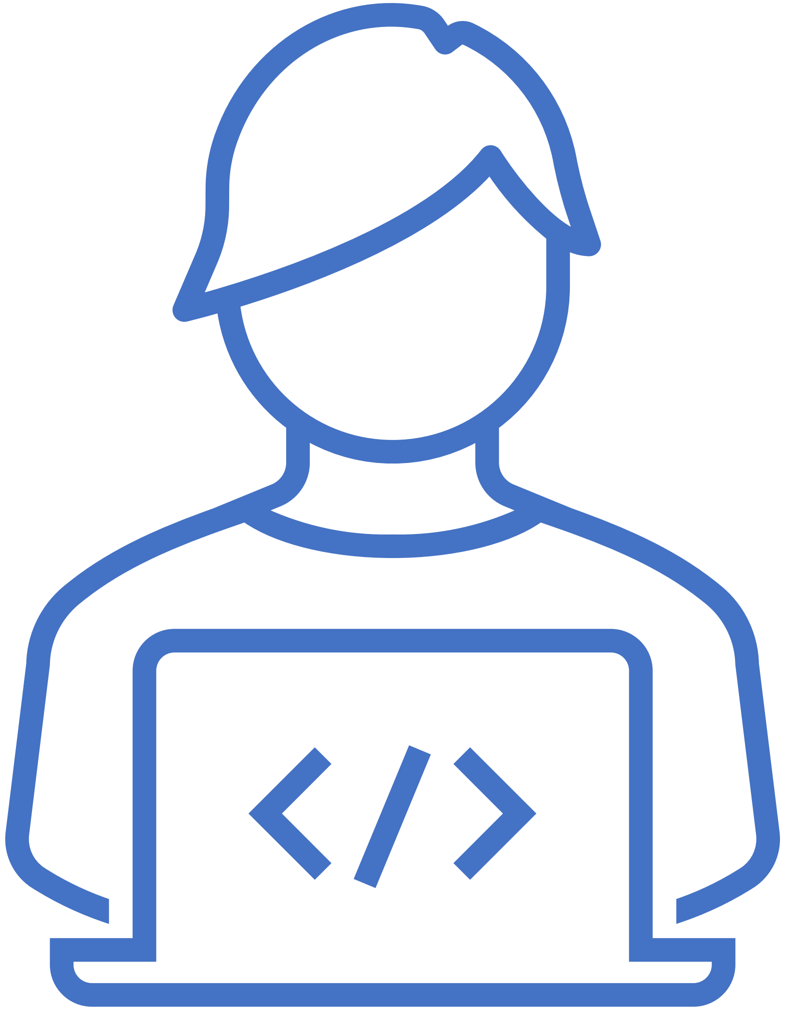
Access Control - Role assignment
sales-projectforecast

Name: Search by name or email
Type: All
Role: 5 selected
Scope: All scopes
Group by: Role

8 items (5 Users, 1 Groups, 2 Service Principals)

NAME	TYPE	ROLE	SCOPE
BACKUP OPERATOR			
Alain Charon alain@	User	Backup Operator	This resource

Hands-on Labs



Hands-on Lab – Apply RBAC Policies

1

APPLY RBAC POLICY AT SUBSCRIPTION LEVEL

2

APPLY RBAC POLICY AT RESOURCE GROUP LEVEL

3

APPLY RBAC POLICY AT RESOURCE LEVEL

Resource Locks

Azure Resource Locks (to prevent accidental changes)

- A **resource lock** prevents resources from being accidentally deleted or changed.
- Even with Azure role-based access control (Azure RBAC) policies in place, there's still a risk that people with the right level of access could delete critical cloud resources.
- **Resource lock** is a warning system that reminds you that a resource should not be deleted or changed.
- You can apply locks to a **subscription, a Resource Group, or an individual resource.**
- You can set the lock level to **CanNotDelete** or **ReadOnly**.

Hands-on Lab – Apply Resource Locks

Create a Resource Group and Apply Resource Lock to prevent it from accidental deletions and then verify it

Create a Resource(Storage Account or VM) and Apply Resource Lock to prevent it from accidental deletions

Azure Resource Tags

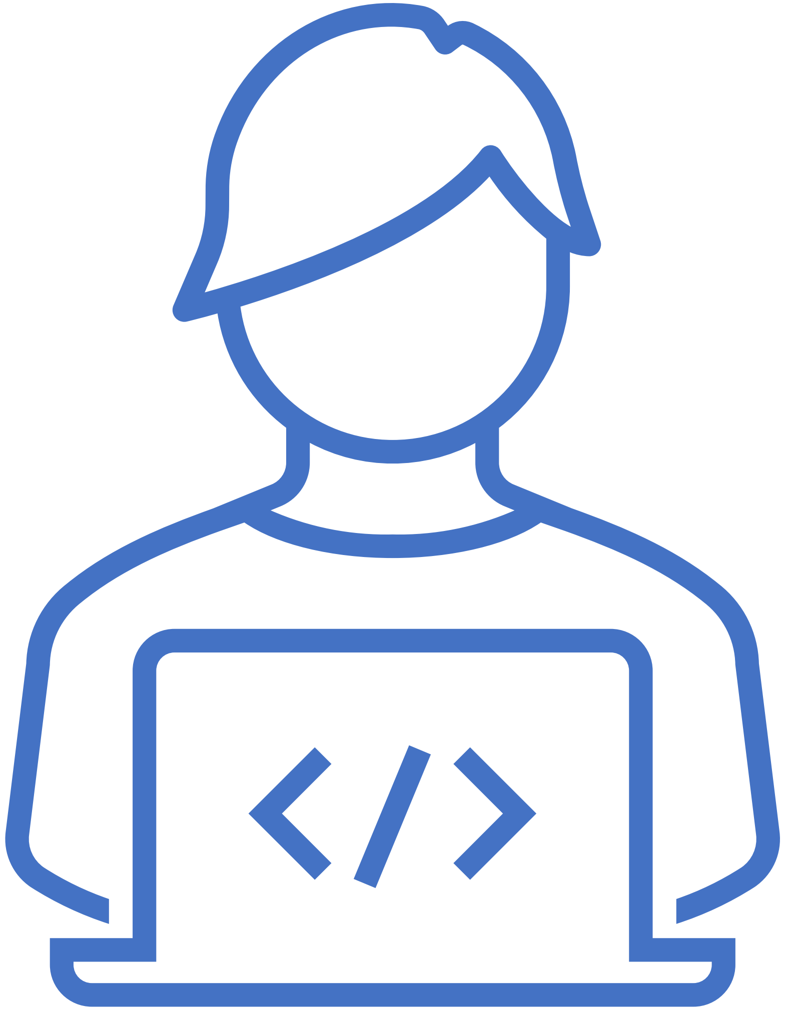
Azure Resource Tags

- As the cloud usage grows, it's increasingly important to stay organized. A good organization strategy helps you understand your cloud usage and can help you manage costs.
- Resource ***tags*** are way to organize resources. Tags provide extra information, or metadata, about your resources.
- This metadata is useful for:

1. Resource management
2. Cost management and optimization

   Operations management
3. Security

Hands-on Labs

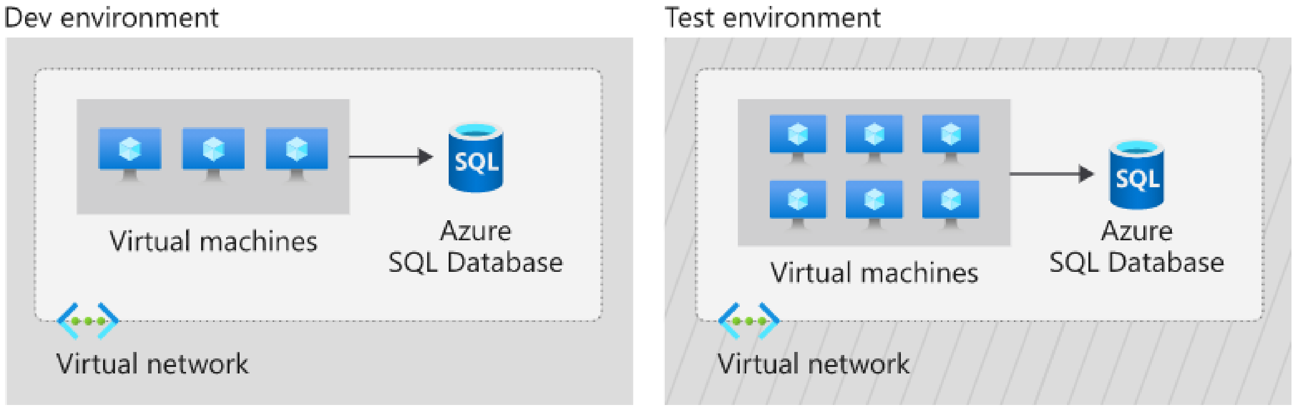


Lab: Create an Azure Resource Group and Apply Tags to it using Azure Portal and PowerShell

Azure Policies (Control and audit your Resources)

- Azure Policies ensure that your resources *stay* compliant
- You will be alerted if a resource's configuration has changed
- Azure Policy is a service in Azure that enables you to create, assign, and manage policies that control or audit your resources
- These policies enforce different rules and effects over your resource configurations so that those configurations stay compliant with corporate standards

Knowledge Check



1. How will you allow some users to control only the Azure Virtual Machines in each environment and prevent them from modifying networking and other resources in the same resource group or Azure subscription?
2. Which is likely the best way here to identify which billing department each Azure resource belongs to?