Cloud Computing

Caltech | Center for Technology & Management Education

Post Graduate Program in Cloud Computing

Powerd by simplilearn

Cloud Computing

Caltech | Center for Technology & Management Education

PG CC - Microsoft Azure Architect Technologies: AZ:303

Powerd by simplilearn

Implement and manage Azure governance solutions

Learning Objectives

By the end of this lesson, you will be able to:

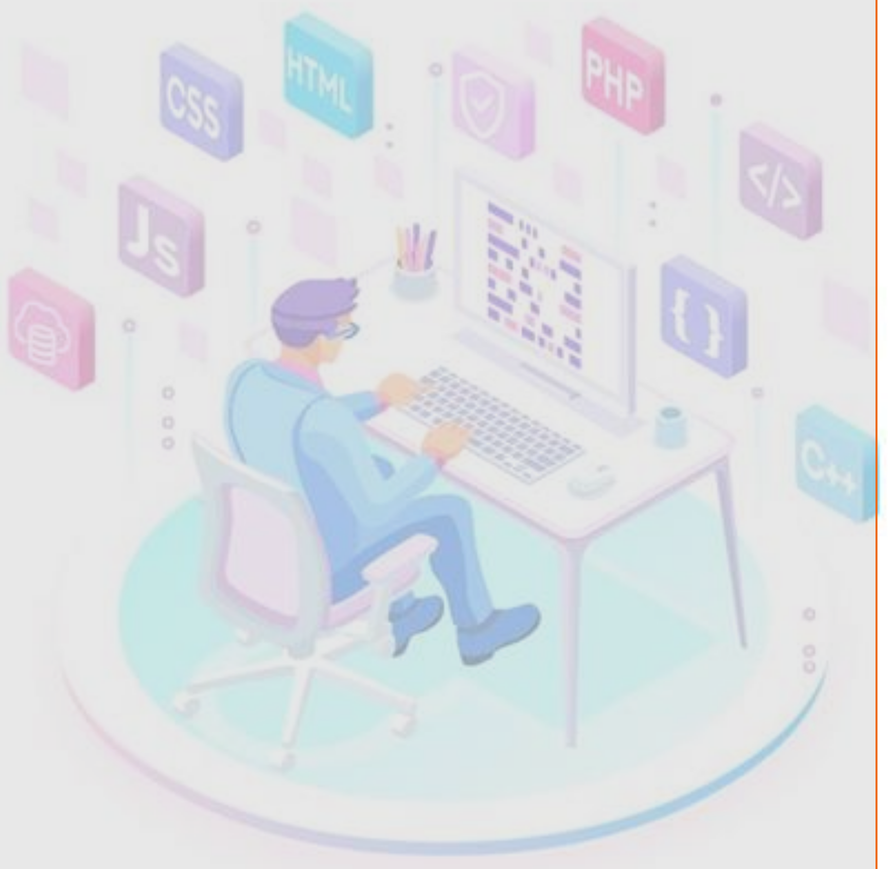
- Assign Role-based Access Control (RBAC)
- Use Access Reviews
- Implement and Configure an Azure Policy
- Illustrate Azure Blueprints

A Day in the Life of an Azure Architect

You are working for an organization as an Architect. Keeping the access security in mind, the organization is looking for an Azure solution that can help control the access based upon the service, resource group, or role.

You have been asked to advise the organization with a solution that can help manage who has access to Azure resources, what they can do with them, and what areas they have access to.

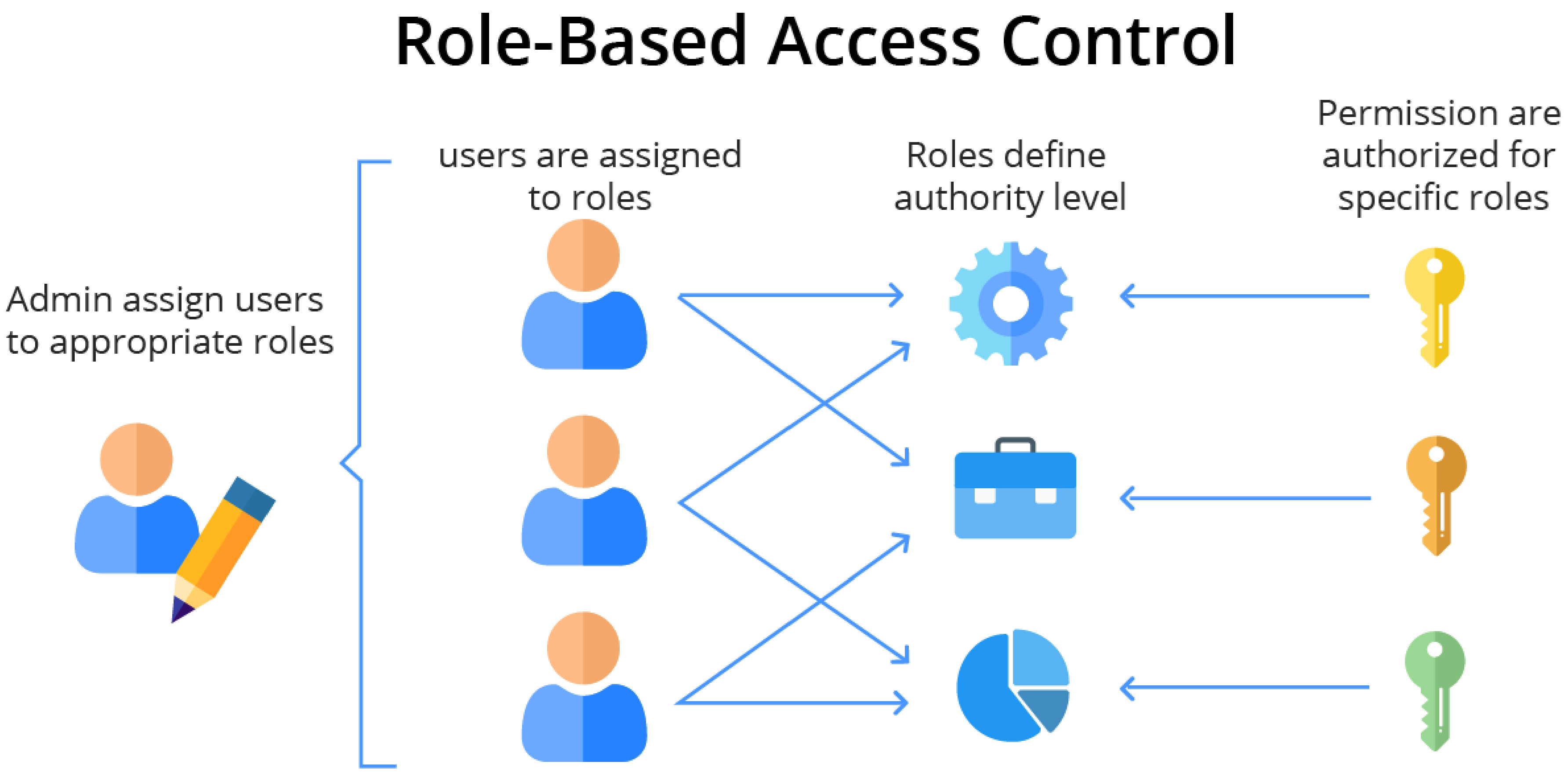
To achieve all of the above along with some additional features, we will be learning a few concepts in this lesson that will help you find a solution for the given scenario.



Role-Based Access Control

Role-Based Access Control

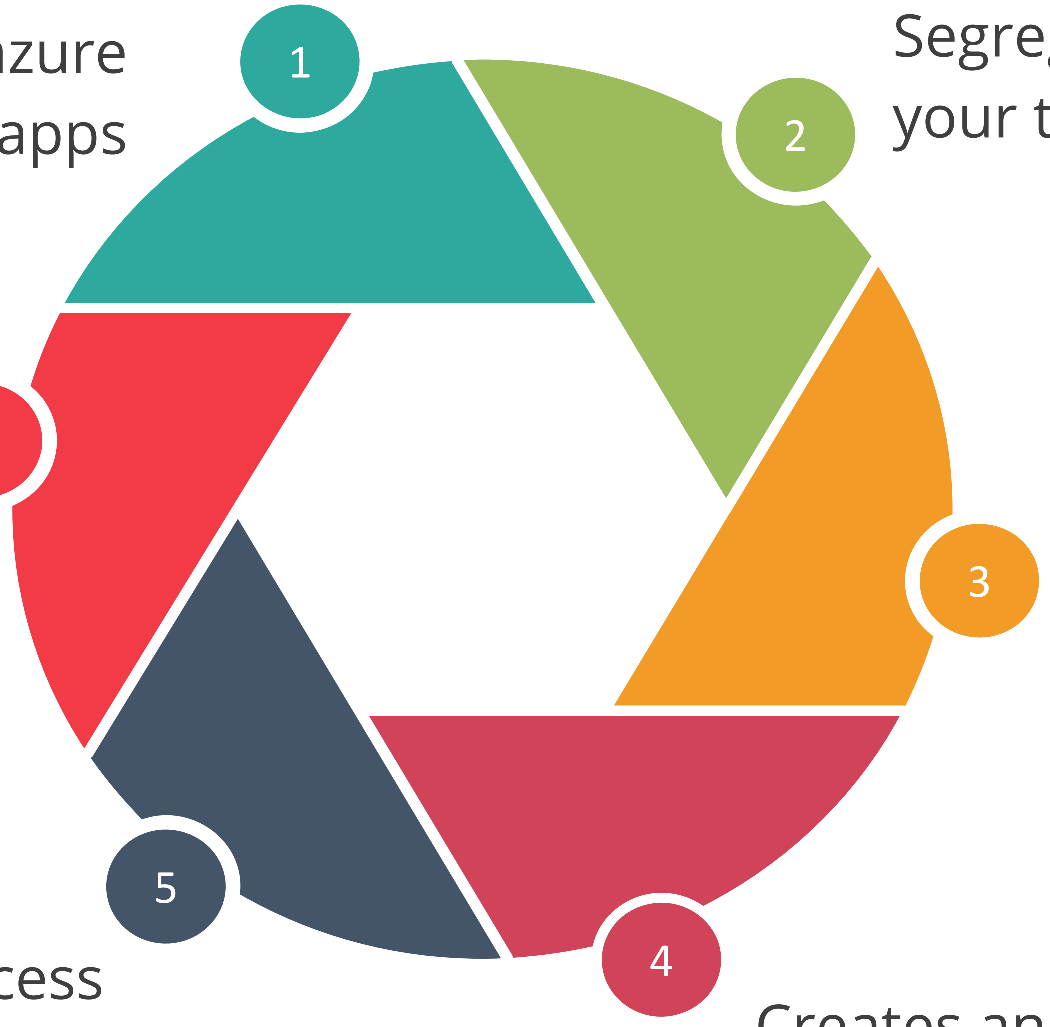
Role-based access control (RBAC) is the capability that allows you to grant appropriate access to Azure AD users, groups, and services.


Role-Based Access Control
Admin assign users to appropriate roles
users are assigned to roles
Roles define authority level
Permission are authorized for specific roles

Azure RBAC is an access management system for Azure resources built on Azure Resource Manager.

image source: https://docs.microsoft.com/en-in/

Role-Based Access Control Features



1. Offers deny assignments which are currently read-only, set by azure blueprints, and Azure managed apps

2. Segregates duties within your team

3. Grants appropriate access to users that they need to perform their jobs

4. Creates an assignment that users can use to grant access

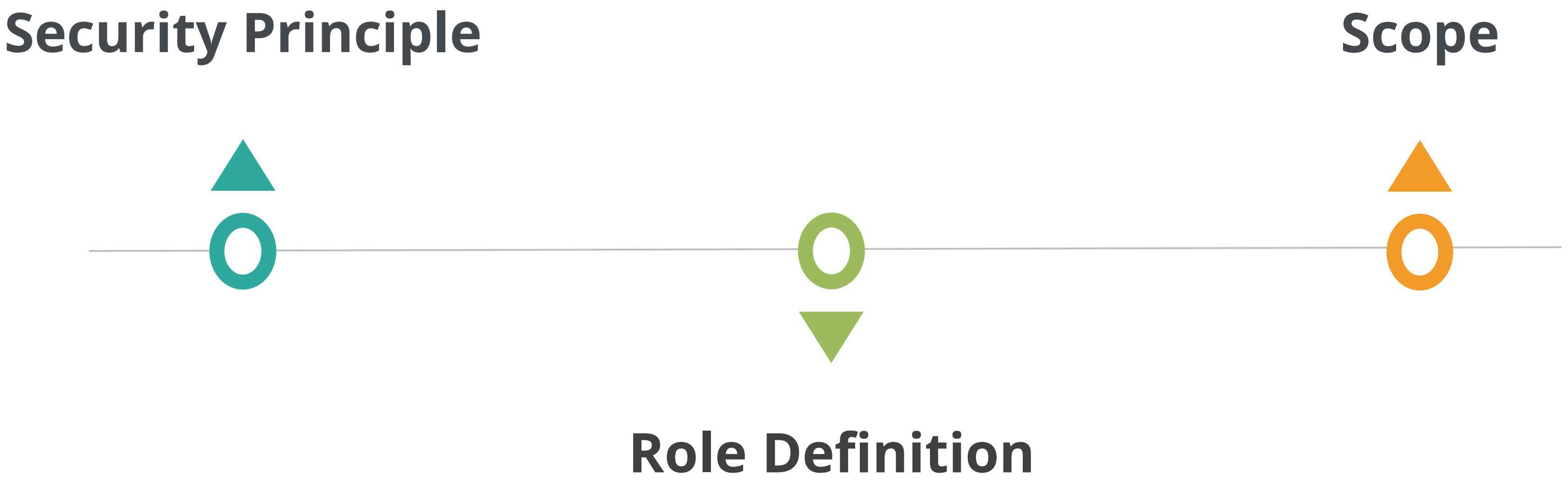
5. Provides fine-grained access management of resources in Azure

6. Based on Azure Resource Manager

Role-Based Access Control

RBAC is used to restrict access to resources by assigning Azure roles.

A role assignment has three components, mentioned:



Security Principle

Role Definition

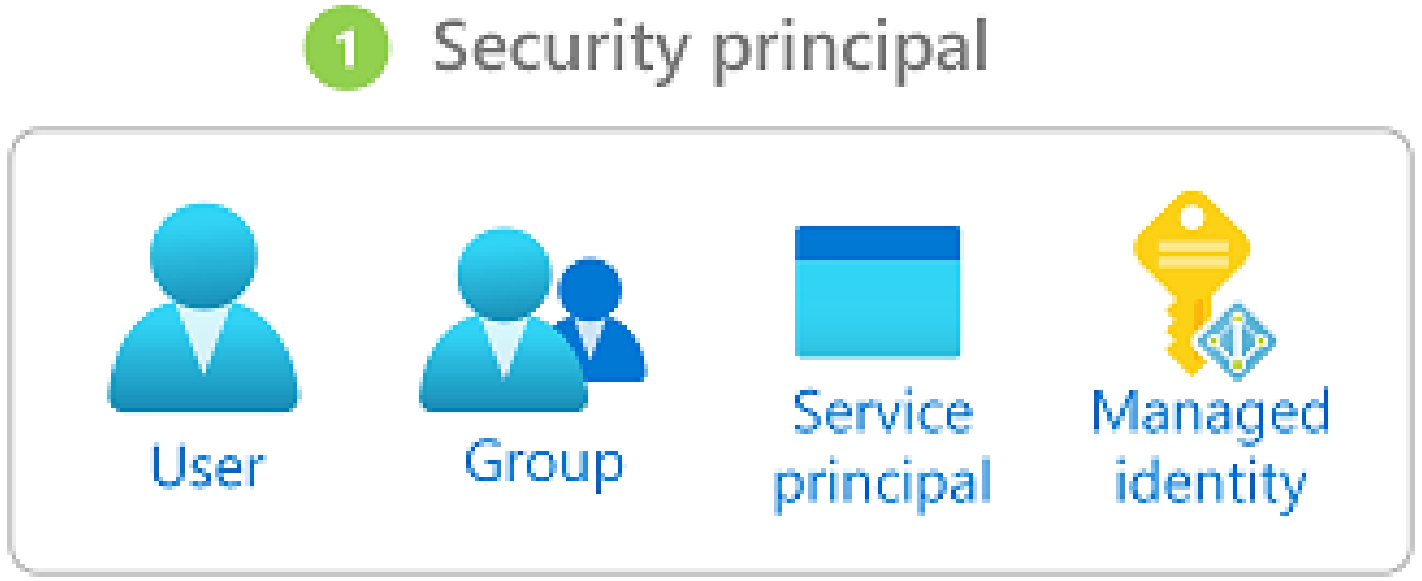
Scope

Note

These components can be considered as **who**, **what**, and **where**.

Security Principal

A user, group, service principal, or managed identity that requests access to Azure resources is referred to as a security principal.



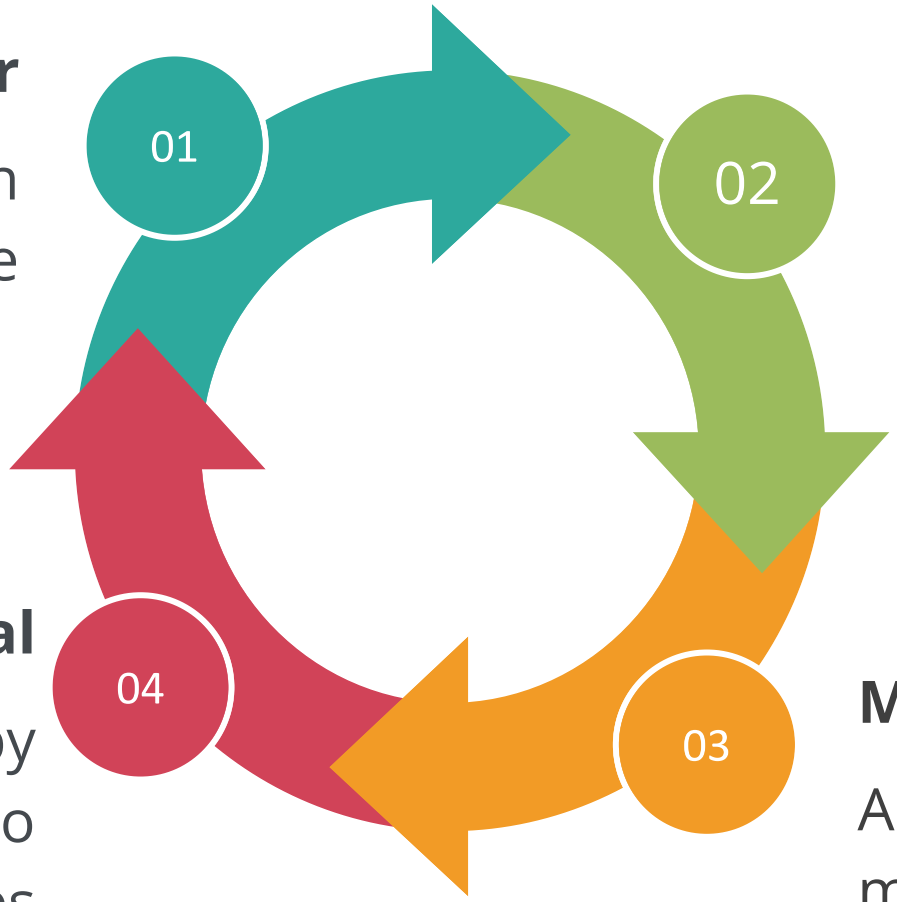
A role can be assigned in any of these four security principals.

Source: https://docs.microsoft.com/

image source: https://docs.microsoft.com/en-in/

Security Principal

Types of security principals:



User

An Individual having an Azure active directory profile

Group

A set of users created in Azure Active Directory

Managed Identity

An identity in Azure active directory managed by Azure, by default

Service Principal

A security identity used by application or services to access Azure resources

Role Definition

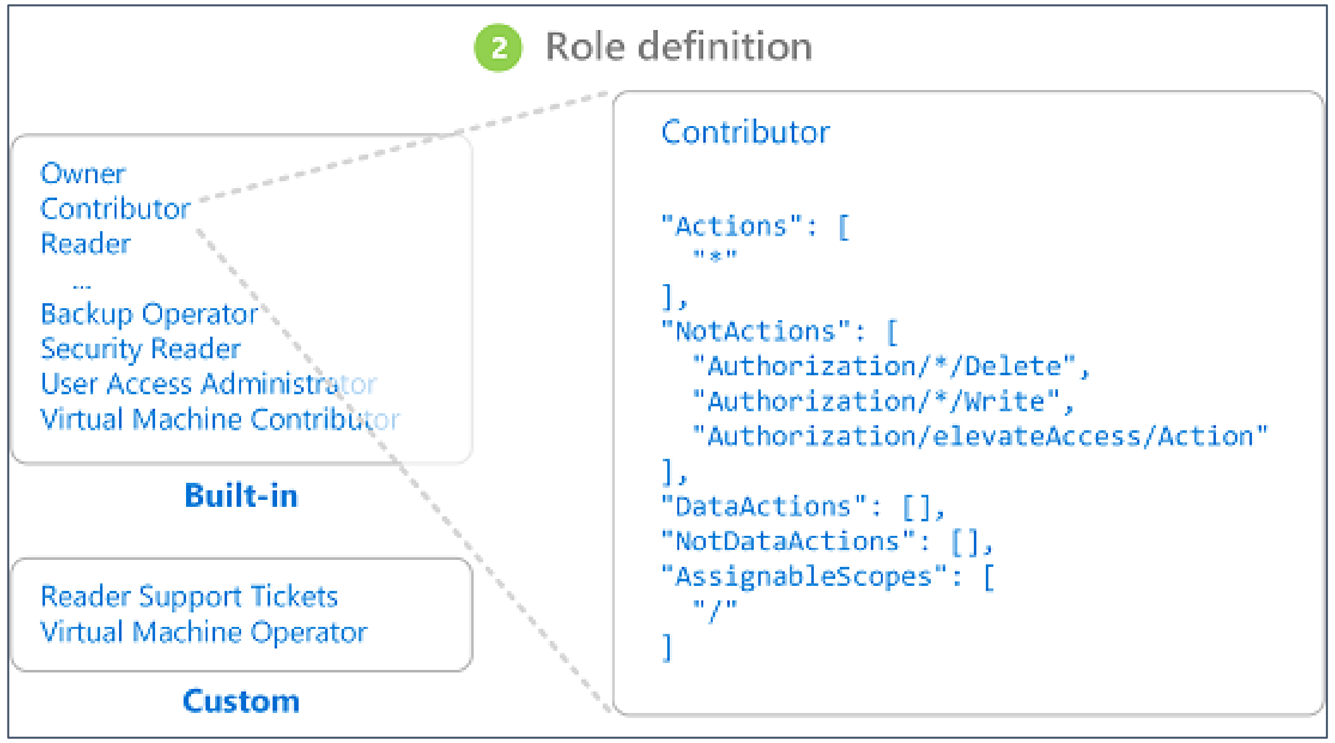
A role definition is a collection of actions that can be performed on Azure resources.

Three most common roles:

Owner can manage everything, including the access

Contributors can manage everything except access

Readers can view everything but can't make changes



```
"Actions": [
  "*"
],
"NotActions": [
  "Authorization/*/Delete",
  "Authorization/*/Write",
  "Authorization/elevateAccess/Action"
],
"DataActions": [],
"NotDataActions": [],
"AssignableScopes": [
  "/"
]
```

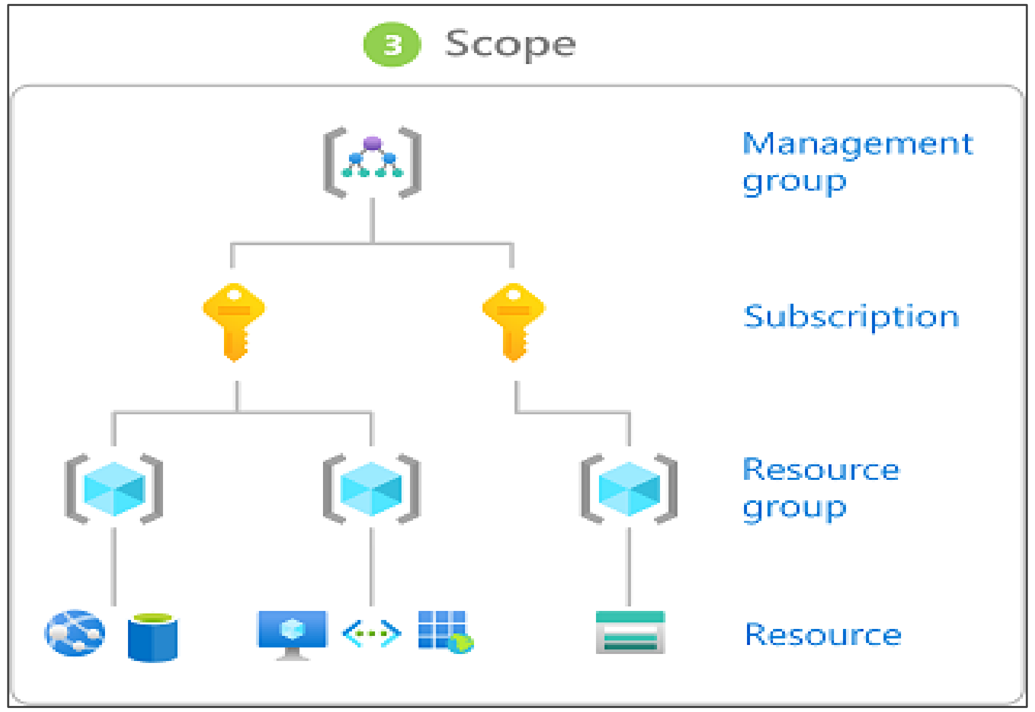
image source: https://docs.microsoft.com/en-in/

Source: https://docs.microsoft.com/

Scope

The scope is a set of resources to which the access principle is applicable.

It can be specified at four levels:



Subscription

Management group

Resource group

Resource

Note

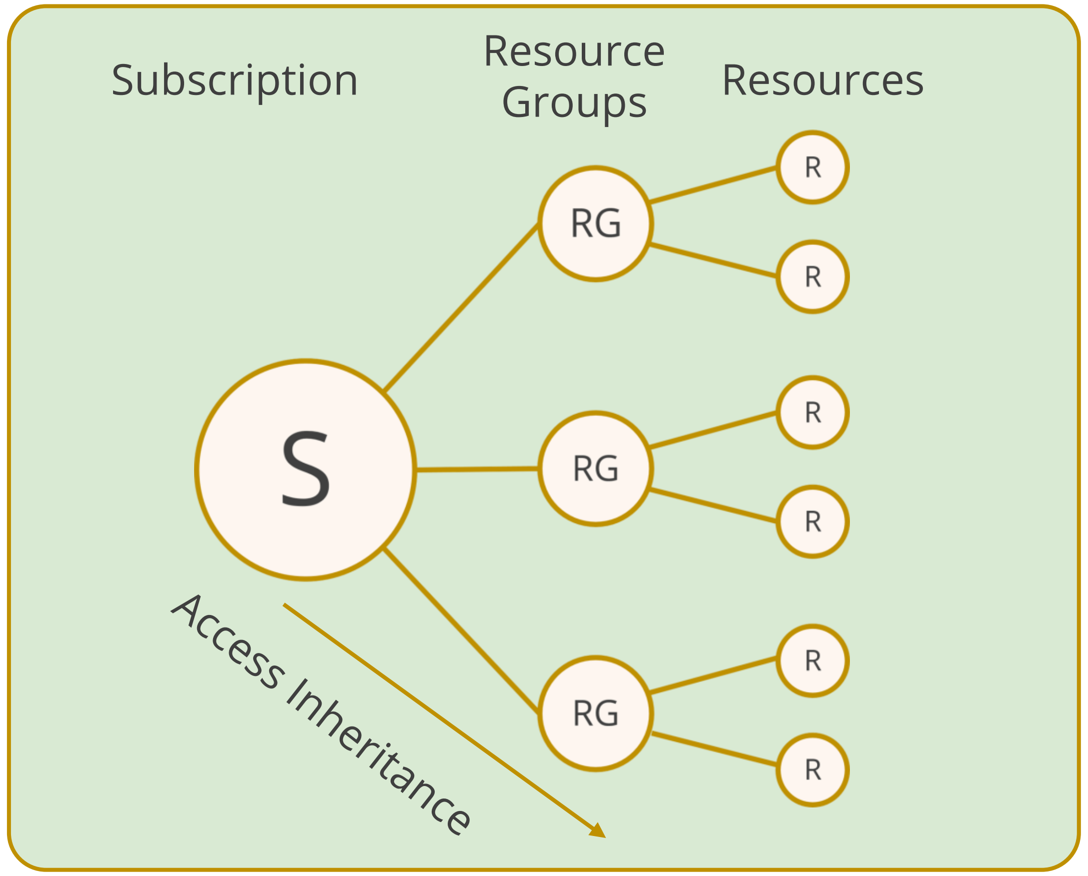
It's simple to determine the scope of a management group, subscription, or resource group by knowing the subscriber's name and subscription ID. However, it takes extra efforts when it comes to determining the scope of a resource.

Source: https://docs.microsoft.com/

image source: https://docs.microsoft.com/en-in/

Resource Scope

Roles can be assigned for resources groups as well as for individual resources.



Role Assignment Scopes

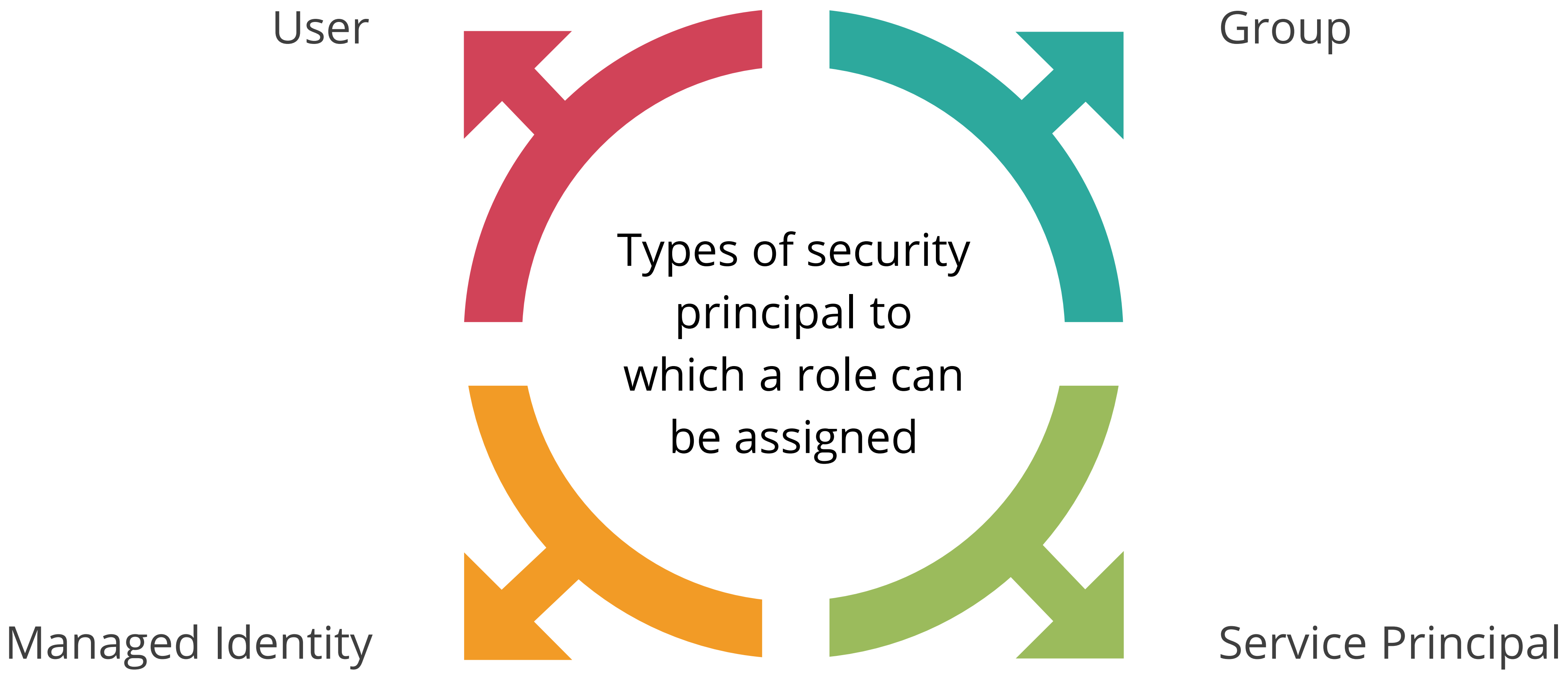
Example:

If a user, group, or a service is granted access to only a resource group within a subscription, they will be able to access only that resource group and resources within it, and not other resources groups within the subscription.

A resource inherits role assignments from its parent resources.

Role Assignment

It is a process of assigning a role definition to a user, group, service principal, or managed identity at a certain scope for the purpose of giving access.



Source: https://docs.microsoft.com/

Deny Assignment

Azure creates and manages deny assignments to safeguard resources.

Features

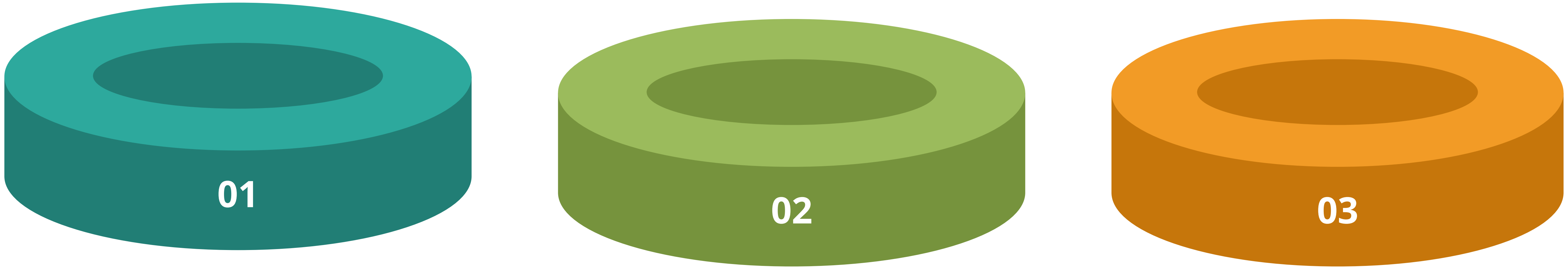
- Deny Assignment attaches a set of deny actions to a user, group, service principal, or managed identity at a particular scope for the purpose of denying access.
- Deny assignments prevent users from executing specific tasks even if a role assignment gives access.
- Deny assignments take precedence over role assignments.

Source: https://docs.microsoft.com/

Role-Based Access Control: Roles

Role

There are three general groups of roles in the context of Azure and Azure AD.



Classic subscription administrator roles

Azure roles

Azure AD roles

Source: https://docs.microsoft.com/

Azure RBAC Roles

The following table summarizes the differences between three basic classic subscription administrative roles:

Role	Limit	Permissions	Notes
Account Administrator	1 per Azure account	Access the Azure Account Center Manage all subscriptions in an account Change the Service Administrator	Account Administrator has no access to the Azure portal.
Service Administrator	1 per Azure subscription	Manage services in the Azure portal Assign users to the Co-Administrator role	Service Administrator has the equivalent access of a user who is assigned the Owner role at the subscription scope.
Co-Administrator	200 per subscription	Same access privileges as the Service Administrator, but can't change the association of subscriptions to Azure directories Assign users to the Co-Administrator role, but cannot change the Service Administrator	Co-Administrator has the equivalent access of a user who is assigned the Owner role at the subscription scope.

Source: https://docs.microsoft.com/

Azure Roles

The following table summarizes the differences between three basic Azure RBAC roles:

Azure role	Permissions	Notes
Owner	● Full access to all resources ● Delegate access to others	● Service administrator and co-administrators are assigned the owner role as the subscription scope applies to all resource types.
Contributor	● Create and manage all types of Azure resources ● Create a new tenant in Azure Active Directory ● Cannot grant access to others	● Applies to all resource types
Reader	● View Azure resources	● Applies to all resource types
User Access Administrator	● Manage user access to Azure resources	

Source: https://docs.microsoft.com/

Azure AD Roles

The following are the three basic Azure AD roles:

Global Administrator

User Administrator

Billing Administrator

Permissions

- Access management for all administrative features in Azure Active Directory, as well as services that federate to Azure Active Directory
- Assigns Administrator roles
- Resets passwords for administrators and users

Source: https://docs.microsoft.com/

Azure AD Roles

The following are the three basic Azure AD roles:

Global Administrator

User Administrator

Billing Administrator

Permissions

- Create and manage all aspects of users and groups
- Manage support tickets
- Monitors service health
- Change passwords for users, helpdesk administrators, and other user administrator

Source: https://docs.microsoft.com/

Azure AD Roles

The following are the three basic Azure AD roles:

Global Administrator

User Administrator

Billing Administrator

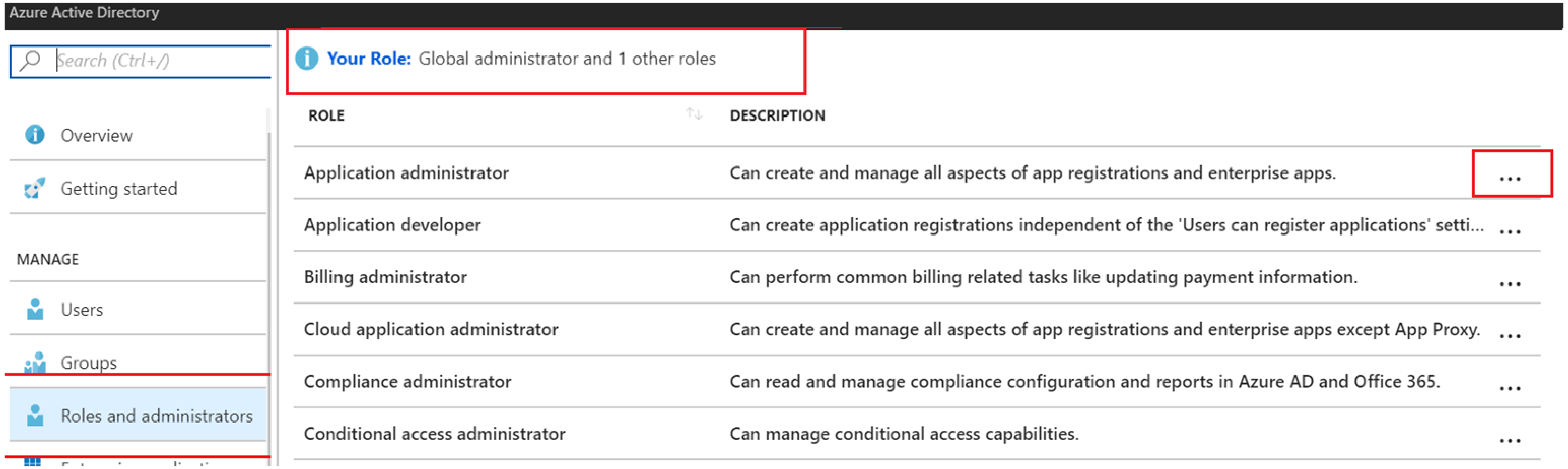
Permissions

- Make purchases
- Manage subscriptions
- Manage support tickets
- Monitors service health

Source: https://docs.microsoft.com/

Administrator Permissions

Using Azure AD, a user can designate separate administrators for different functions.



Your Role: Global administrator and 1 other roles

ROLE	DESCRIPTION
Application administrator	Can create and manage all aspects of app registrations and enterprise apps.
Application developer	Can create application registrations independent of the 'Users can register applications' setti...
Billing administrator	Can perform common billing related tasks like updating payment information.
Cloud application administrator	Can create and manage all aspects of app registrations and enterprise apps except App Proxy.
Compliance administrator	Can read and manage compliance configuration and reports in Azure AD and Office 365.
Conditional access administrator	Can manage conditional access capabilities.

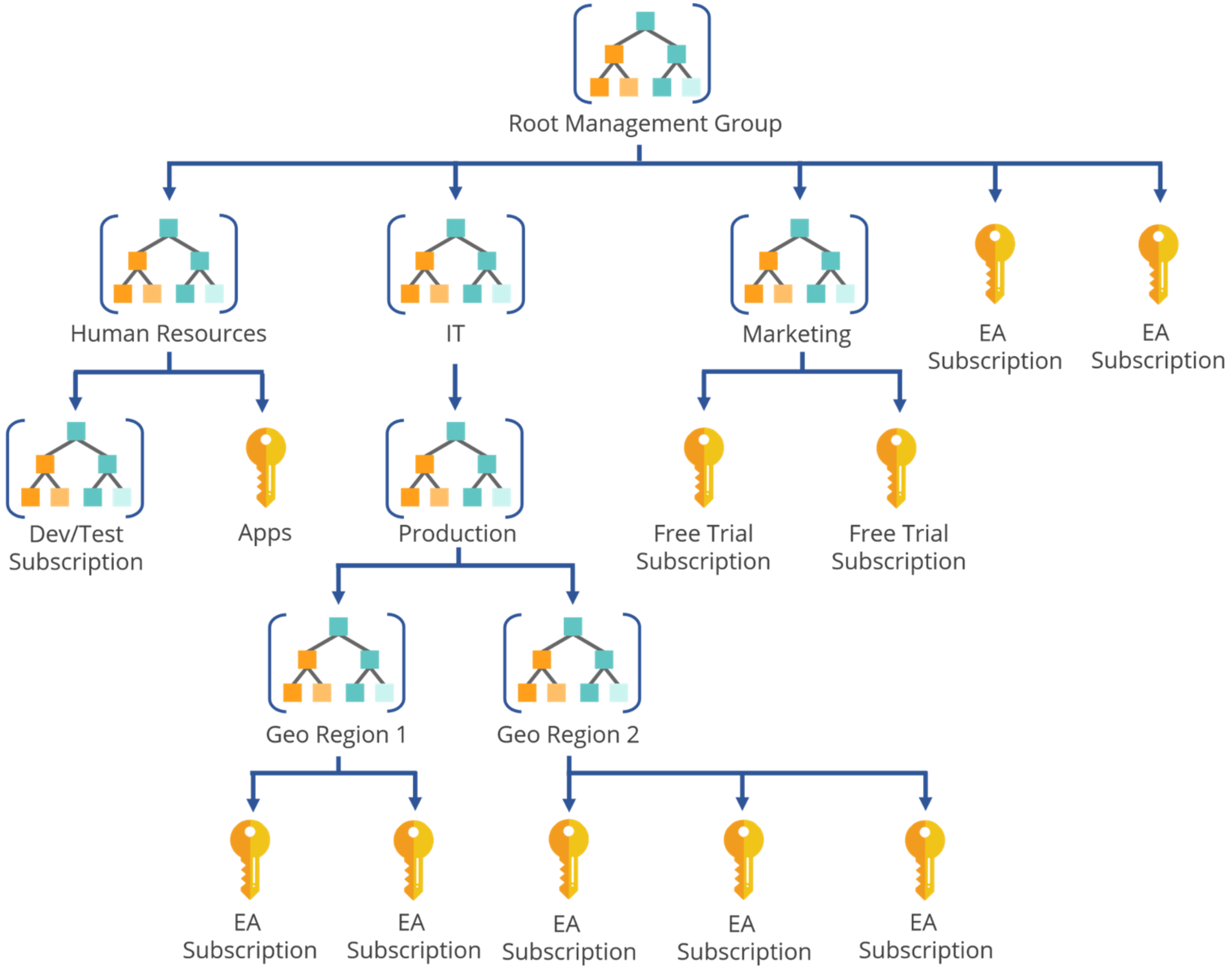
Note

- Global administrators can access all administrative features
- Global administrators can assign administrator roles to other users

Source: https://docs.microsoft.com/

Management Groups

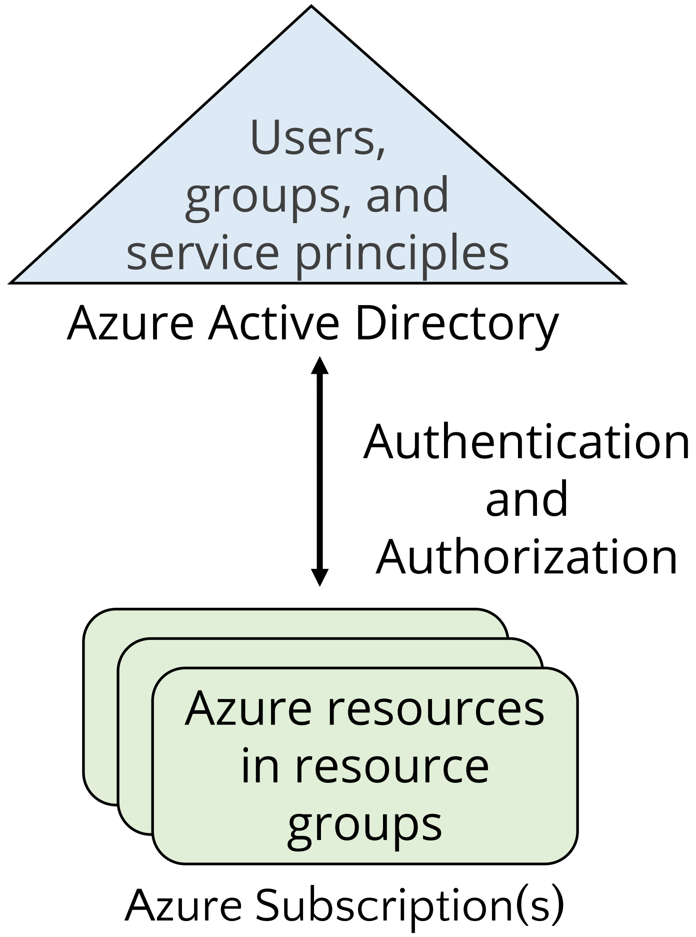
To manage multiple subscriptions in an organization, subscriptions are organized into containers called "Management Groups."



Azure Subscriptions

A subscription is a logical unit of Azure services that is linked to an Azure account.

It has accounts and are associated with Azure AD.



Users, groups, and service principles

Azure Active Directory

Authentication and Authorization

Azure resources in resource groups

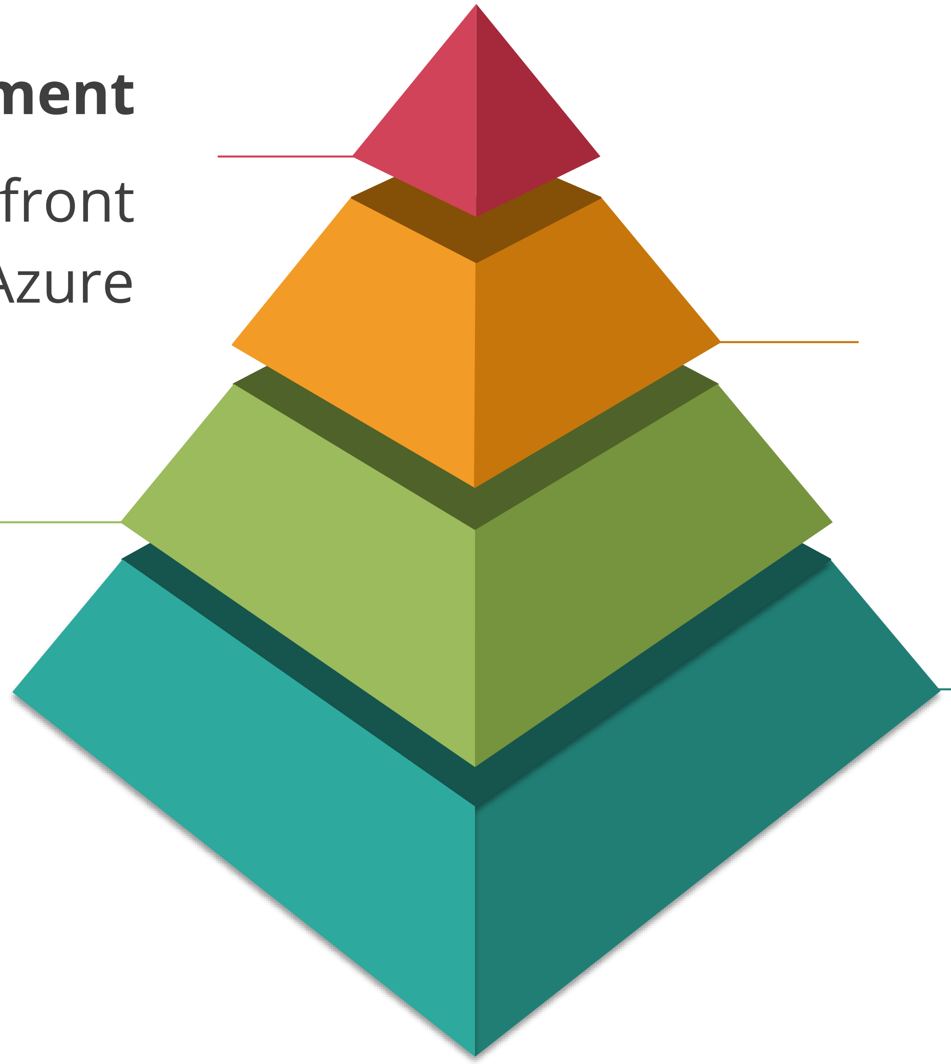
Azure Subscription(s)

Note

Billing for Azure services is done on a per-subscription basis.

Azure Subscriptions

Types of Azure subscription:



Enterprise Agreement

Consumer makes an upfront monetary commitment to Azure

Microsoft Partner

Find a partner that can design and implement your cloud solution

Reseller

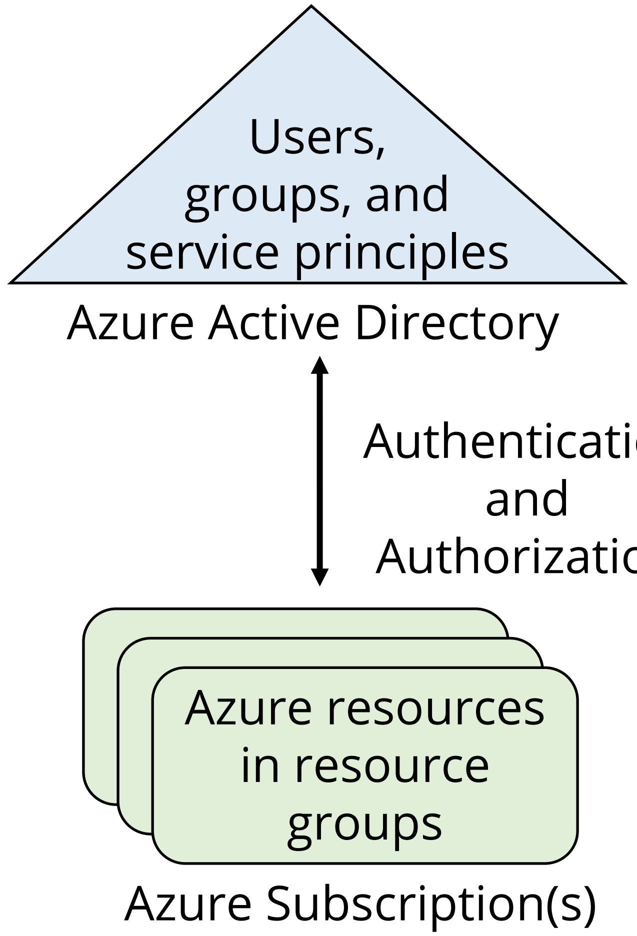
Open licensing program

Free Trial Account

Try Azure services with free credit

Azure Account

An account is an identity in Azure AD or in a directory that is trusted by Azure AD.


Users, groups, and service principles
Azure Active Directory
Authentication and Authorization
Azure resources in resource groups
Azure Subscription(s)

Note

To grant a user access to your Azure resources, you must add them to the Azure AD directory associated with your subscription.

Source: https://docs.microsoft.com/

Subscriptions Usage

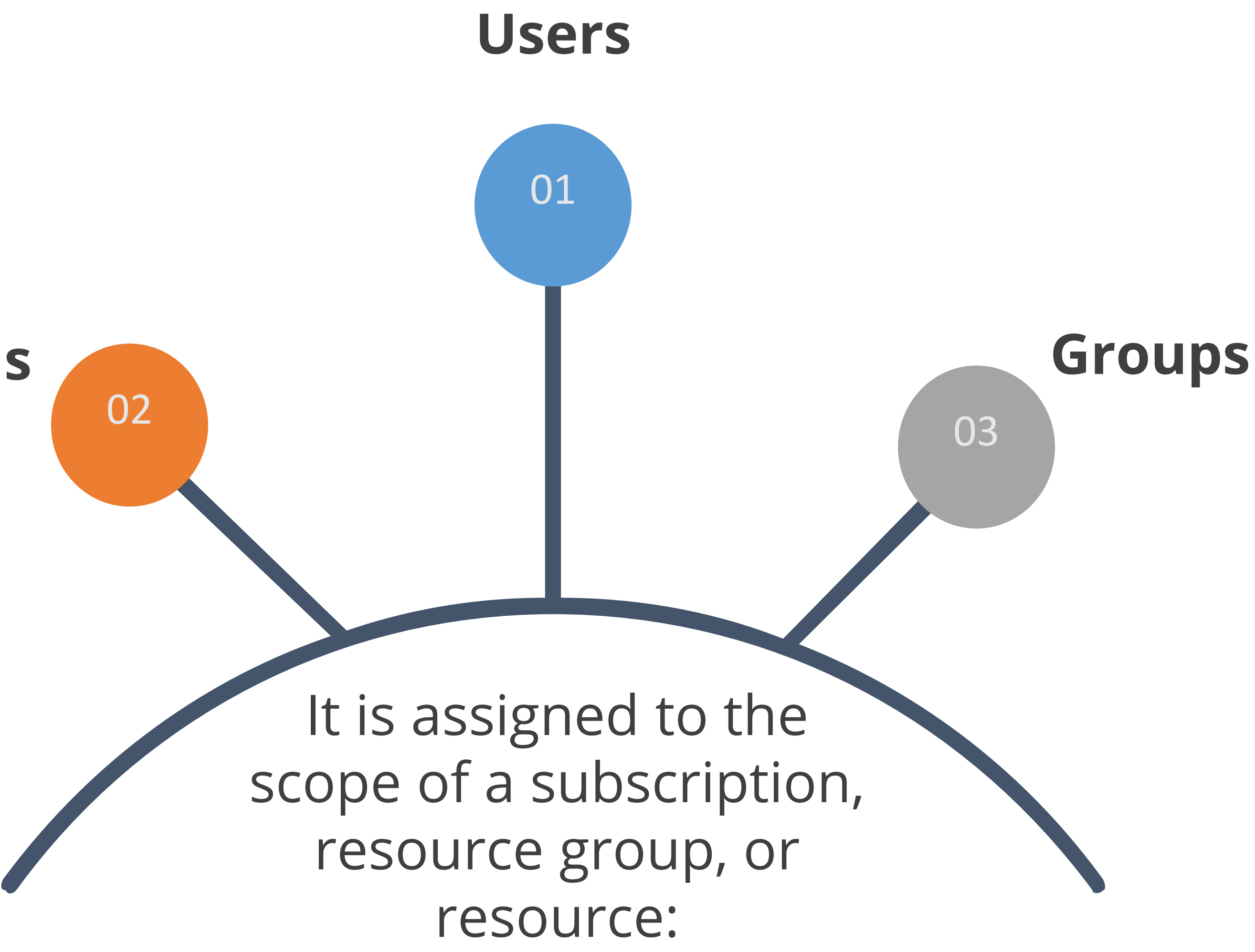
The following table lists and details the subscription and usage information:

Subscription	Usage
Free	Includes a $200 credit for the first 30 days, free limited access for first 12 months
Pay-As-You-Go	Charged on a monthly basis
Enterprise	One agreement, with discounts for new licenses and software assurance - targeted at enterprise-scale organizations.
Student	Includes $100 for 12 months – verified student access

Custom RBAC Role

Custom RBAC Role

It allows user to define roles that meet the specific needs of user organization.



Users

01

Service principals

02

Groups

03

It is assigned to the scope of a subscription, resource group, or resource:

Assisted Practice

Azure RBAC

Duration: 10 Min.

Problem Statement:

You've been assigned the task of implementing Azure RBAC to manage who has access to Azure resources, what they can do with them, and what areas they have access to.

Assisted Practice: Guidelines

Steps to create an Azure RBAC:

1. Login to your Azure portal
2. Click on All services and select the scope
3. Click the specific resource for that scope
4. Click Access control (IAM) and select Role assignments
5. Add and assign the new roles

Access Review

Azure AD Access Reviews

It enables organizations to efficiently manage:

Group memberships

Enterprise applications

Role assignments

Azure AD Access Reviews

Azure AD access reviews enables user to collaborate internally within the organization and with external organizations, such as partners.

Why are access reviews important?

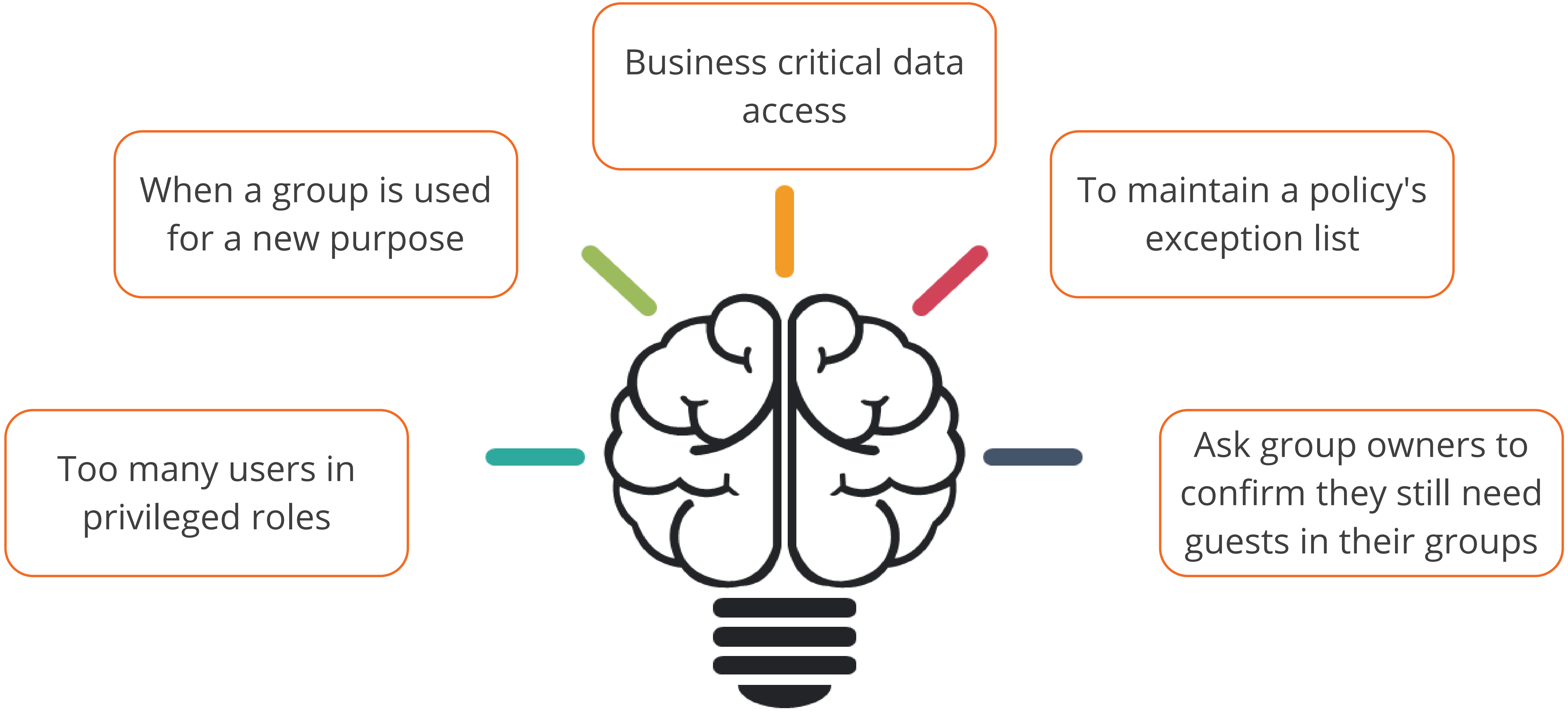
Ensure the new employees has the right access for productive

Ensure access removal when people move teams or leave the company, especially when it involves guests

Excessive access rights can lead to audit findings and compromises as they indicate a lack of control over access

Engage with resource owners to ensure they regularly review the access to their resources

Azure AD Access Reviews



Business critical data access

When a group is used for a new purpose

To maintain a policy's exception list

Too many users in privileged roles

Ask group owners to confirm they still need guests in their groups

When to use access reviews?

Azure AD Access Reviews

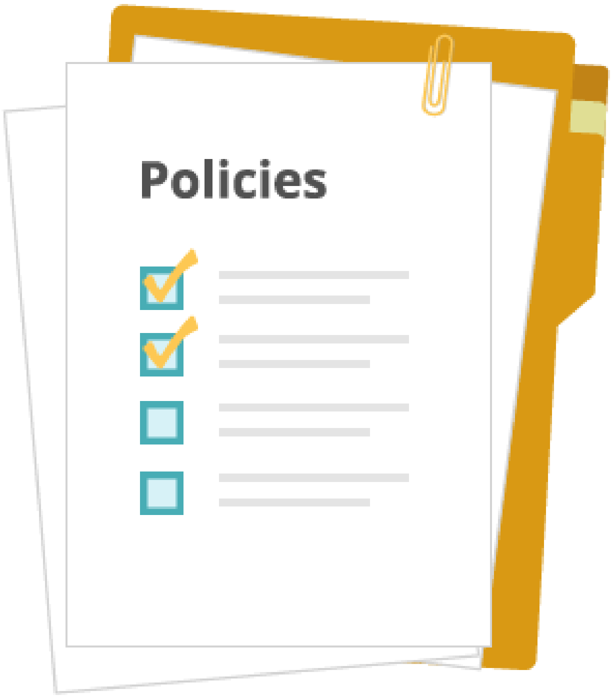
To create access to reviews, follow the table:

Access rights of users	Reviewers can be	Review created in	Reviewer experience
Security group members office group members	Specified reviewers Group owners Self-review	Azure AD access reviews Azure AD groups	Access panel
Assigned to a connected app	Specified reviewers Self-review	Azure AD access reviews Azure AD enterprise apps (in preview)	Access panel
Azure AD role	Specified reviewers Self-review	Azure AD PIM	Access panel
Azure resource role	Specified reviewers Self-review	Azure AD PIM	Access panel

Azure Policy

Azure Policy

Azure Policy is a service to create, assign, and manage policies. Policies enforce different rules and effects over resources, so those resources stay compliant with your corporate standards and service level agreements.



Example

A user can have a policy to allow only a certain SKU size of virtual machines in your environment.

Azure Policy: Advantages

The advantages of Azure policies such as:

Apply policies at scale

Apply multiple policies and aggregate policy states with policy initiative

Enforcement and compliance

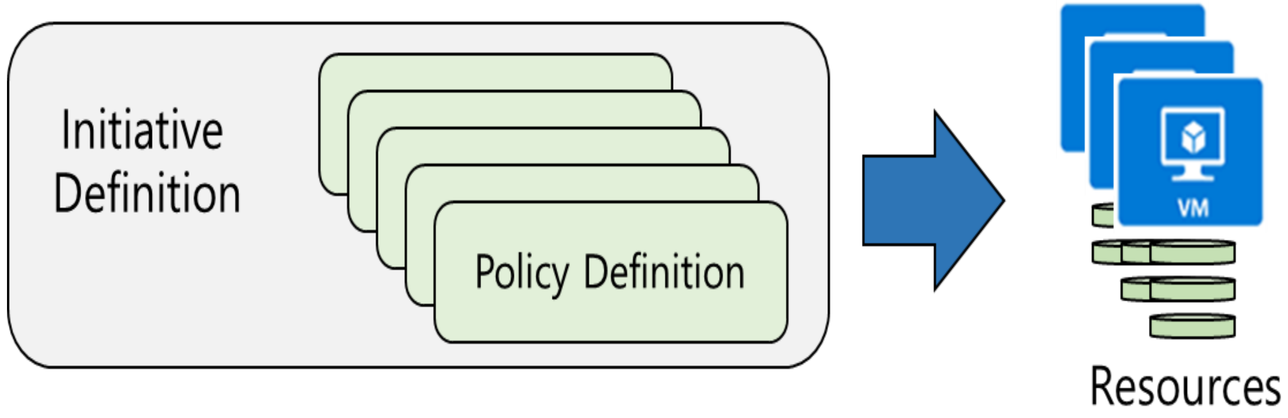
Turn on policies for resources and get real time policy evaluation and enforcement

Remediation

Real time remediation

Implementing Azure Policies

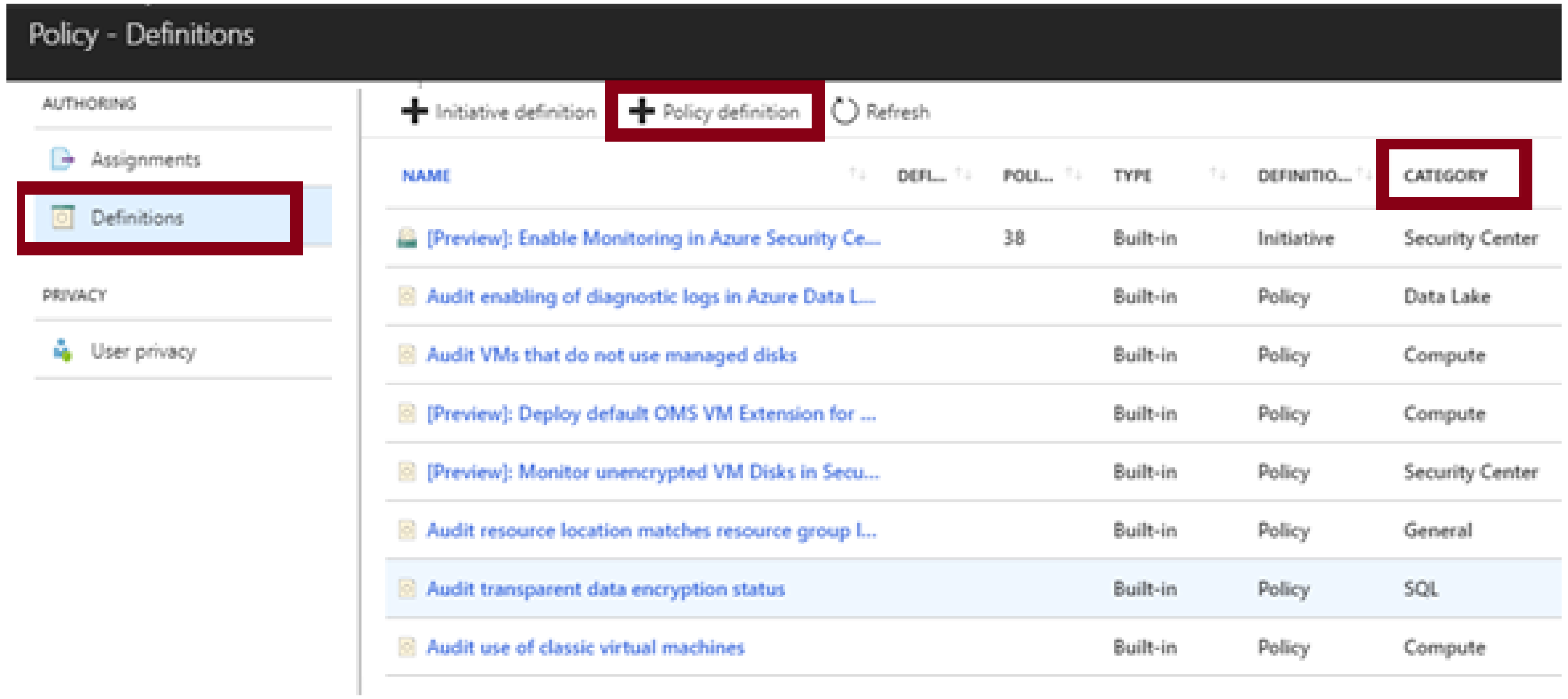
Below are the Azure policy objects:



1. Policy Definitions
2. Initiative Definitions
3. Assignment

Policy Definitions

Policy definitions define under what condition a policy is enforced and what effects to take.



NAME	DEFI...	POLI...	TYPE	DEFINITIO...	CATEGORY
[Preview]: Enable Monitoring in Azure Security Ce...		38	Built-in	Initiative	Security Center
Audit enabling of diagnostic logs in Azure Data L...			Built-in	Policy	Data Lake
Audit VMs that do not use managed disks			Built-in	Policy	Compute
[Preview]: Deploy default OMS VM Extension for ...			Built-in	Policy	Compute
[Preview]: Monitor unencrypted VM Disks in Secu...			Built-in	Policy	Security Center
Audit resource location matches resource group l...			Built-in	Policy	General
Audit transparent data encryption status			Built-in	Policy	SQL
Audit use of classic virtual machines			Built-in	Policy	Compute

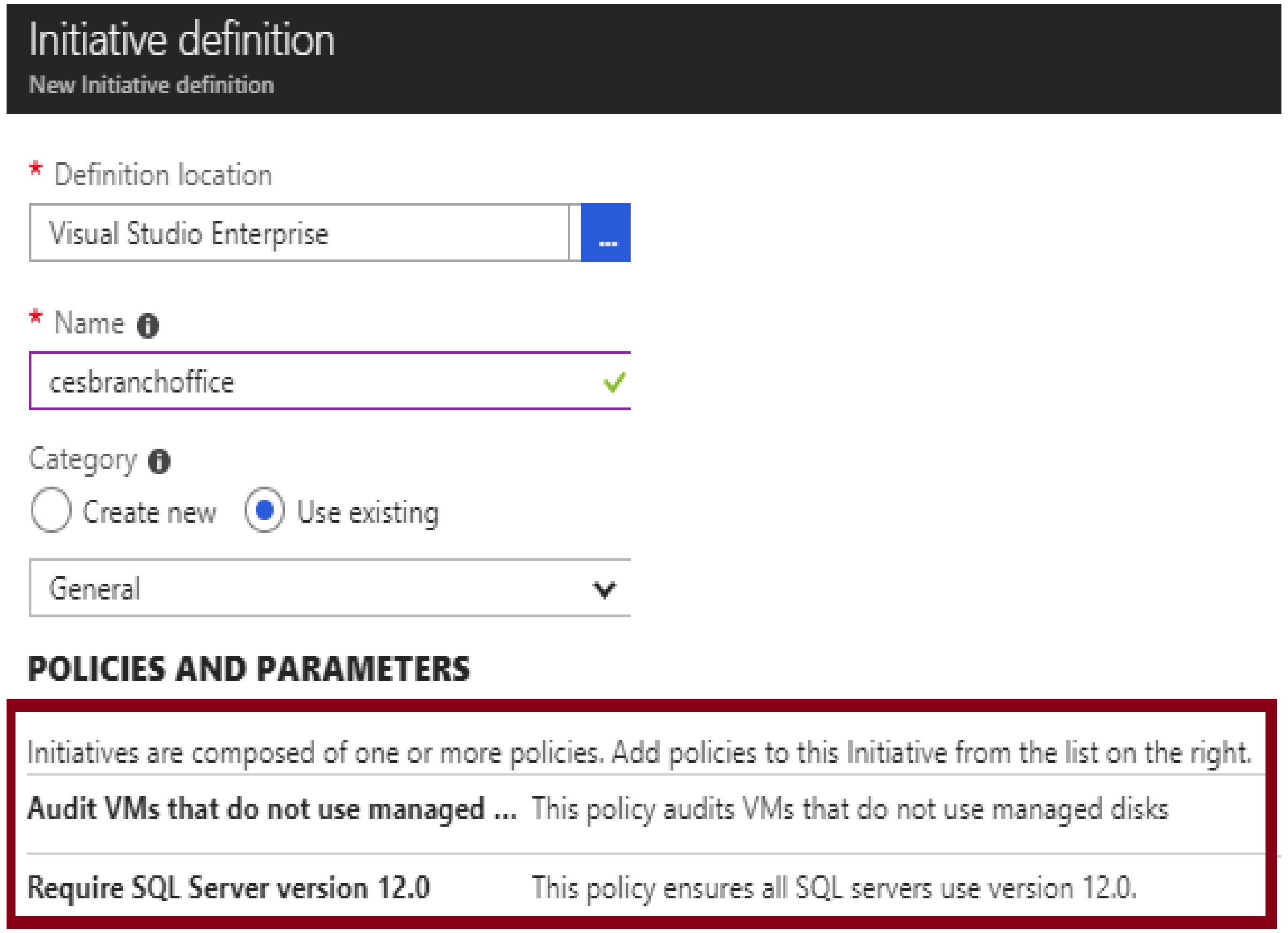
Example:

- A user could prevent VMs from being deployed if they are exposed to a public IP address.
- A user can import policies from GitHub.

It has a specific JSON format.

Initiative Definitions

Initiative definitions is a collection of policy definitions that are developed to achieve a unique overall goal.



* Definition location

Visual Studio Enterprise

* Name

cesbranchoffice ✓

Category

○ Create new ● Use existing

General

POLICIES AND PARAMETERS

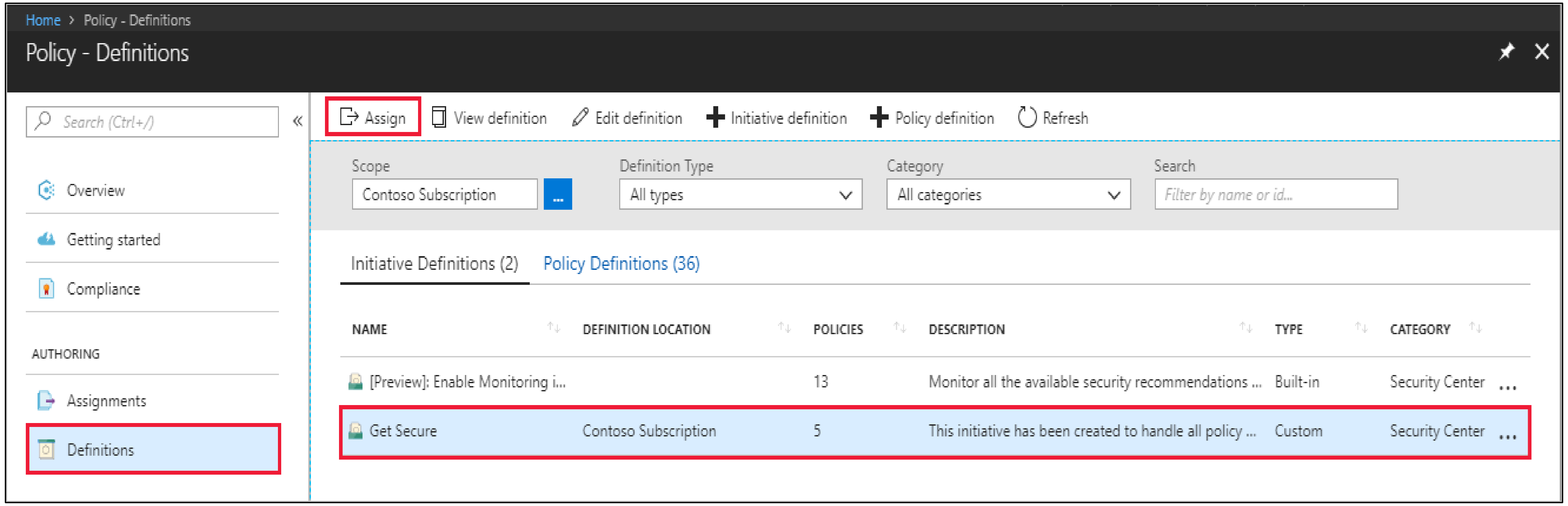
Initiatives are composed of one or more policies. Add policies to this Initiative from the list on the right.

Audit VMs that do not use managed ...	This policy audits VMs that do not use managed disks
Require SQL Server version 12.0	This policy ensures all SQL servers use version 12.0.

It simplifies managing and assigning policy definitions by grouping a set of policies as one single item.

Assignment

Assignment is a policy definition or initiative that has been given a particular scope. The scope determines on what resources or a group of resources the policy gets enforced.



Home > Policy - Definitions

Policy - Definitions

Search (Ctrl+/)

- Overview
- Getting started
- Compliance

AUTHORING

- Assignments
- Definitions

Assign | View definition | Edit definition | Initiative definition | Policy definition | Refresh

Scope: Contoso Subscription

Definition Type: All types

Category: All categories

Search: Filter by name or id...

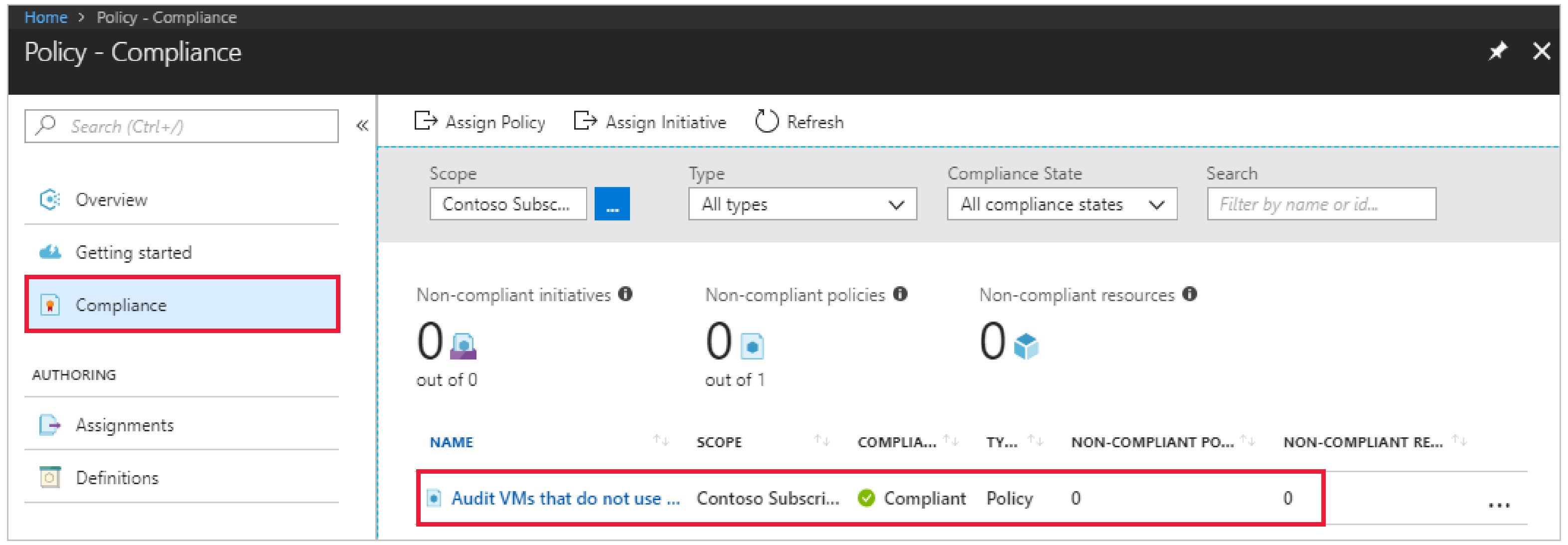
Initiative Definitions (2) | Policy Definitions (36)

NAME	DEFINITION LOCATION	POLICIES	DESCRIPTION	TYPE	CATEGORY	
[Preview]: Enable Monitoring i...		13	Monitor all the available security recommendations ...	Built-in	Security Center	...
Get Secure	Contoso Subscription	5	This initiative has been created to handle all policy ...	Custom	Security Center	...

Note: Currently, an initiative definition can have up to 100 policies.

Determine Compliance

Non-compliant initiatives are two types:



Scope: Contoso Subsc...

Type: All types

Compliance State: All compliance states

Search: Filter by name or id...

Non-compliant initiatives: 0 out of 0

Non-compliant policies: 0 out of 1

Non-compliant resources: 0

NAME	SCOPE	COMPLIA...	TY...	NON-COMPLIANT PO...	NON-COMPLIANT RE...
Audit VMs that do not use ...	Contoso Subscri...	✓ Compliant	Policy	0	0

Non-compliant policies

Number of policy assignments with at least one non-compliant resource.

Non-compliant resources

When a condition is applied to existing user resources and found to be true, the resources are flagged as non-compliant with the policy.

Assisted Practice

Azure Policy Creation: assign it to a resource

Duration: 15 Min

Problem Statement:

You've been given the task of creating an Azure Policy and assigning it to a resource in order to enforce organizational rules and analyze compliance on a large scale.

Assisted Practice: Guidelines

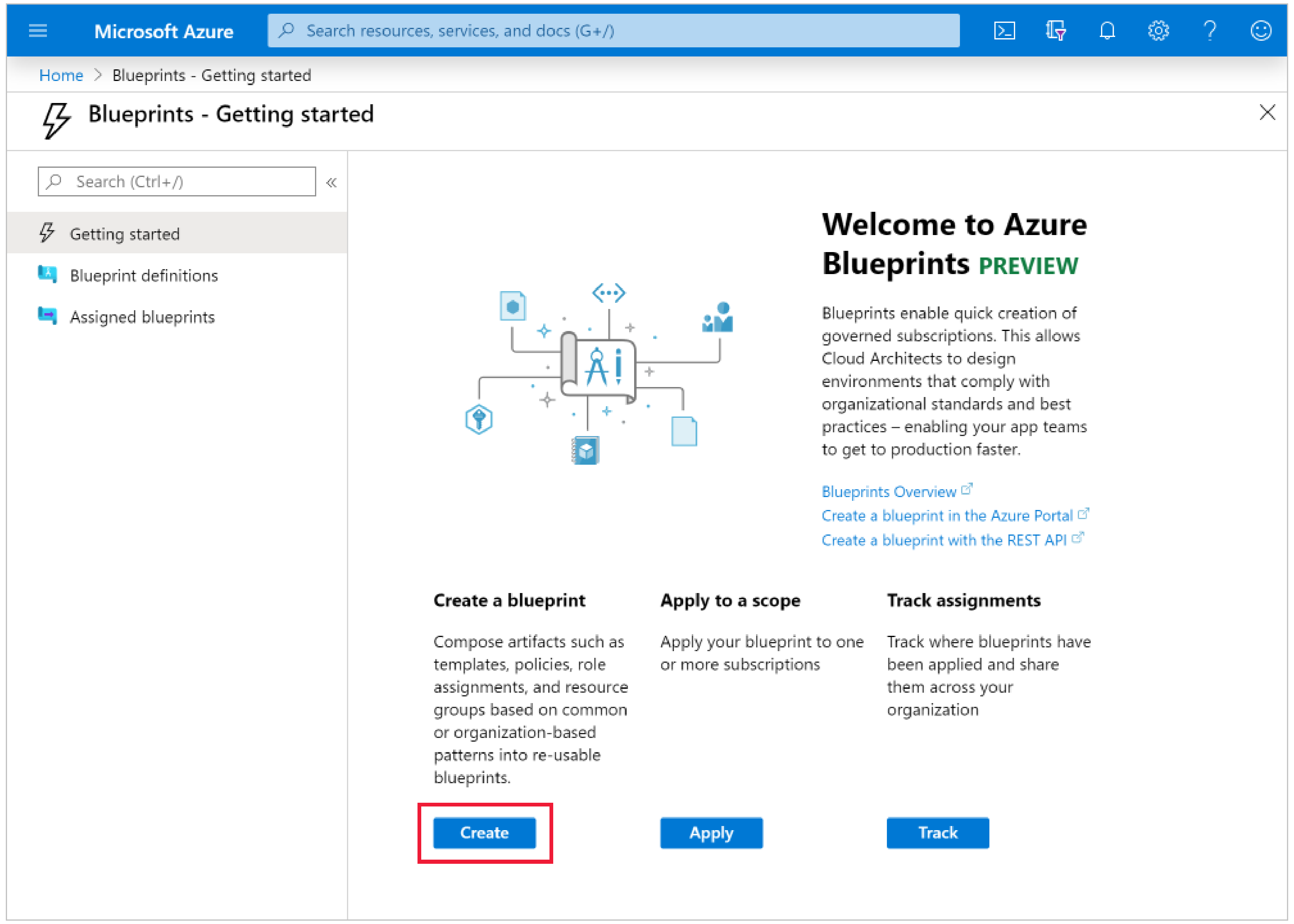
Steps to create an Azure policy are:

1. Login to your Azure portal
2. Select Azure Policy
3. Create new Policy definition page
4. Add information in the new policy page
5. Assign a resource

Azure Blueprint

Azure Blueprints

Azure Blueprints enable defining a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements.



Blueprints - Getting started

Welcome to Azure Blueprints PREVIEW

Blueprints enable quick creation of governed subscriptions. This allows Cloud Architects to design environments that comply with organizational standards and best practices – enabling your app teams to get to production faster.

Blueprints Overview

Create a blueprint in the Azure Portal

Create a blueprint with the REST API

Create a blueprint

Compose artifacts such as templates, policies, role assignments, and resource groups based on common or organization-based patterns into re-usable blueprints.

Create

Apply to a scope

Apply your blueprint to one or more subscriptions

Apply

Track assignments

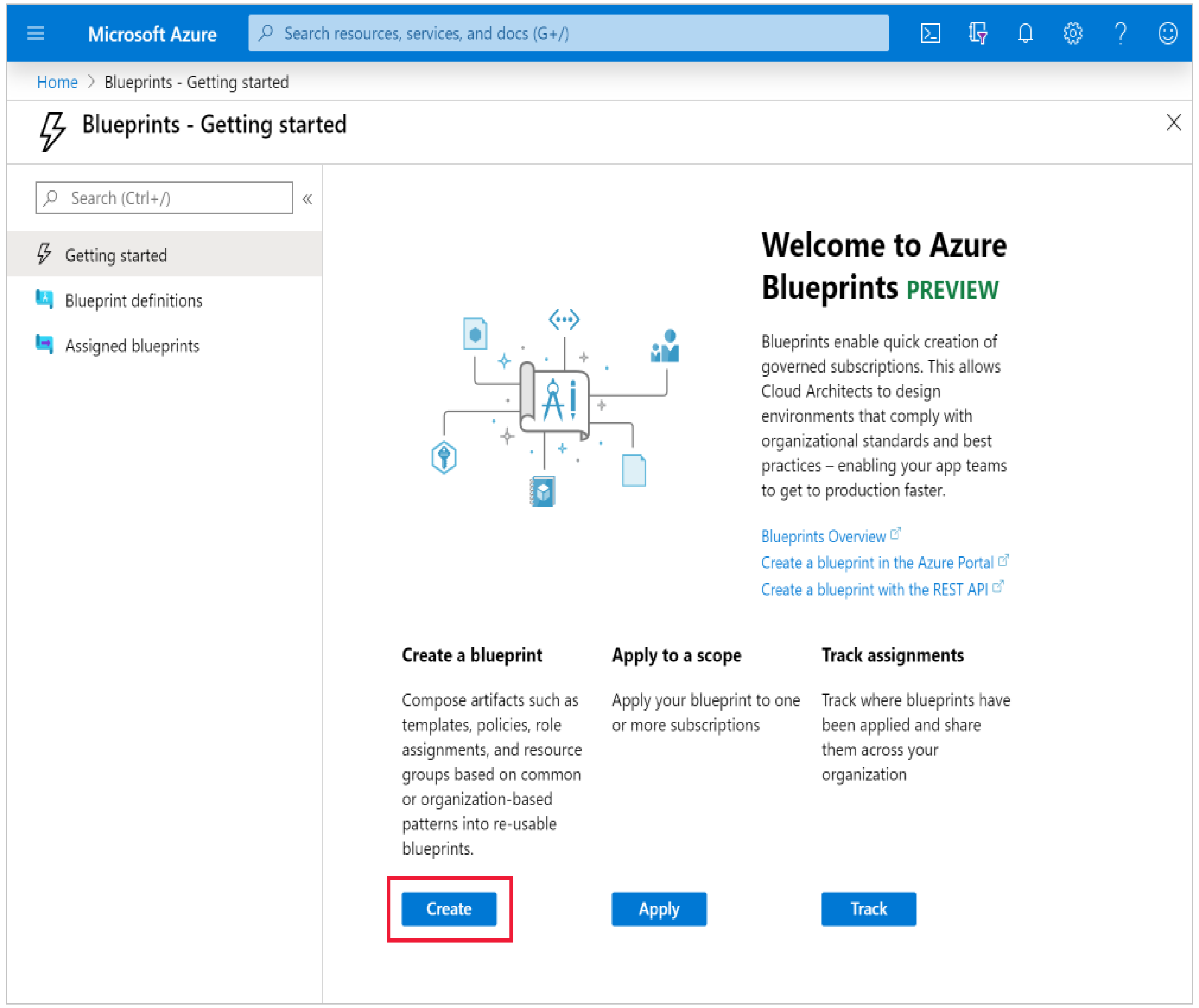
Track where blueprints have been applied and share them across your organization

Track

Azure Blueprints

Azure Blueprints is a declarative way to orchestrate the deployment of artifacts such as:

- Policy
- Role assignments
- Policy assignments
- ARM templates
- Resource groups



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Blueprints - Getting started

Blueprints - Getting started

Welcome to Azure Blueprints PREVIEW

Blueprints enable quick creation of governed subscriptions. This allows Cloud Architects to design environments that comply with organizational standards and best practices – enabling your app teams to get to production faster.

Blueprints Overview
Create a blueprint in the Azure Portal
Create a blueprint with the REST API

Create a blueprint

Compose artifacts such as templates, policies, role assignments, and resource groups based on common or organization-based patterns into re-usable blueprints.

Apply to a scope

Apply your blueprint to one or more subscriptions

Track assignments

Track where blueprints have been applied and share them across your organization

Azure Policy Versus Azure Blueprints

Azure Policy

- Helps to enforce organizational standards and to assess compliance at-scale
- Provides an aggregated view to evaluate the overall state of the environment
- Helps in getting resources to compliance through bulk remediation

Azure Blueprints

- Allows cloud architects and central IT groups to identify a repeatable set of Azure services
- Makes it possible for development teams to quickly create and deploy new environments

Key Takeaways

- Azure RBAC is an access management system for Azure resources, built on Azure Resource Manager.
- The request of access to Azure resources by a user, group, service principal, or managed identity is called as security principal.
- Global, User, and Billing are the three basic azure AD roles.
- Policies enforce different rules and effects over resources
- Azure Blueprints enable a user to create a repeatable set of Azure resources that adheres to an organization's standards.

Implementing Role-based Access Control

Duration: 25 Min.

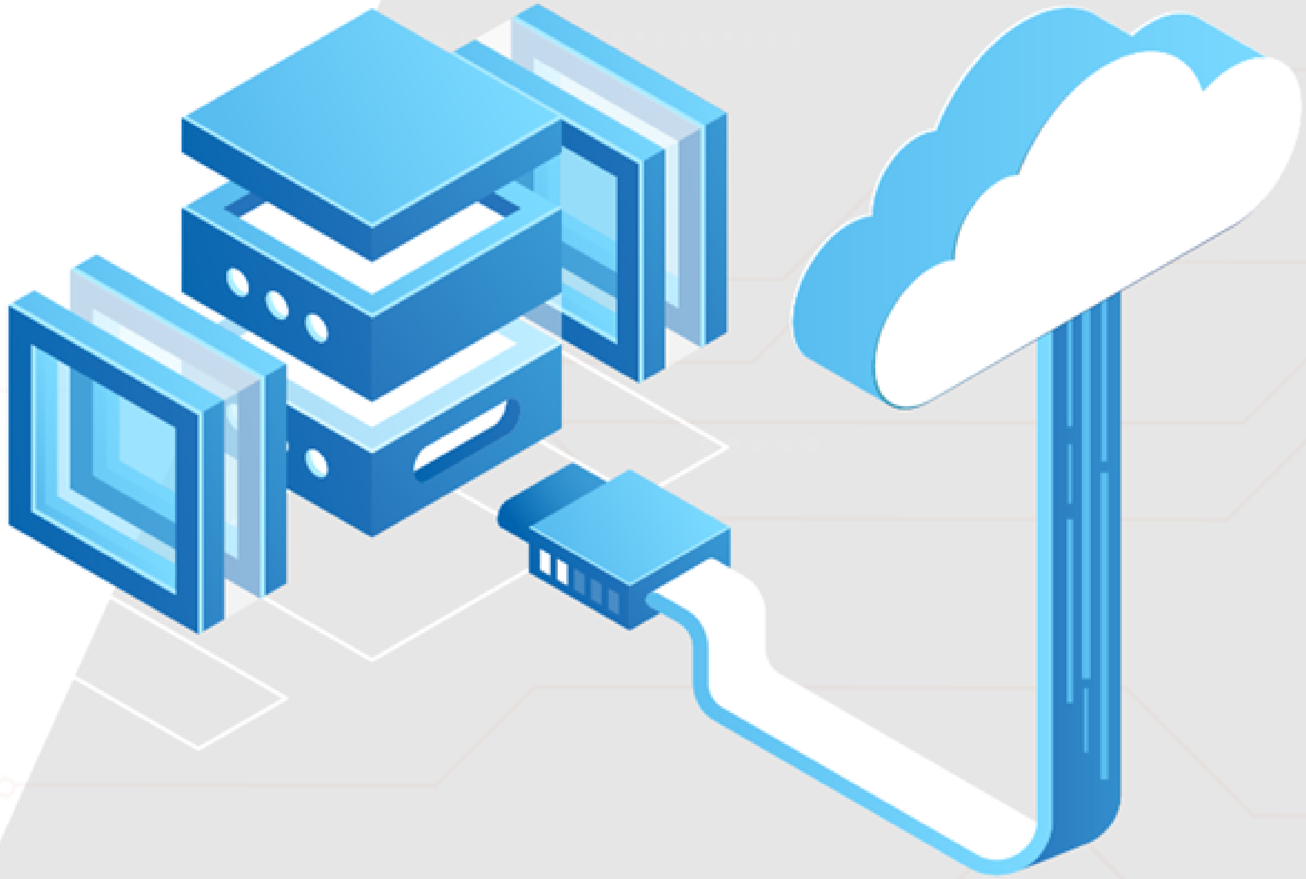
LESSON-END PROJECT

Project agenda: To implement Role-based Access Control

Description: You have been given a project to create two Resource Groups, one for production environment and another for development environment. Once these are created, you need to create two groups in Azure AD that would be used for granting RBAC on these resource groups. Add two users to each of these groups. After this you need to grant contributor access to these groups having scope restricted at resource group levels.

Perform the following:

Create two resource groups initially. Once done, create two groups in Azure AD and add two users in each group. After grant contributor access to these groups having scope restricted at resource group levels using role assignment.



Thank you