

Cloud Computing

Caltech

**Center for Technology &
Management Education**

Designing Infrastructure Solutions on Azure



Design Authorization

Learning Objectives

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

- Choose an authorization approach
- Recommend an access management solution
- Recommend access management best practices
- Recommend a hierarchical structure for access control



A Day in the Life of an Azure Architect

You are working as an architect in an organization that has decided to grant you permission to perform all read, write, and delete operations. The company assigns built-in roles to users, groups, service principals, and managed identities. When assigning a role to a user, consider what actions the role can perform and what the scope of those operations is.

- You can assign built-in roles to users, groups, service principals, and managed identities to Azure.
- You can use security groups to assign permissions.
- Instead of assigning permissions to individual users, use Azure AD groups to manage access. Create a comprehensive delegation model that incorporates management groups, subscriptions, and RBAC resource groups.

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



Choose an Authorization Approach

Authorization

It is the act of granting permission to an authenticated person to perform something.



Microsoft identity platform implements the OAuth 2.0 protocol for handling authorization.

OAuth Definition

OAuth is an open-standard authorization protocol or framework that defines how unconnected servers and services can enable authorized access to their assets without sharing the original, related, single login credential.



OpenID Connect Definition

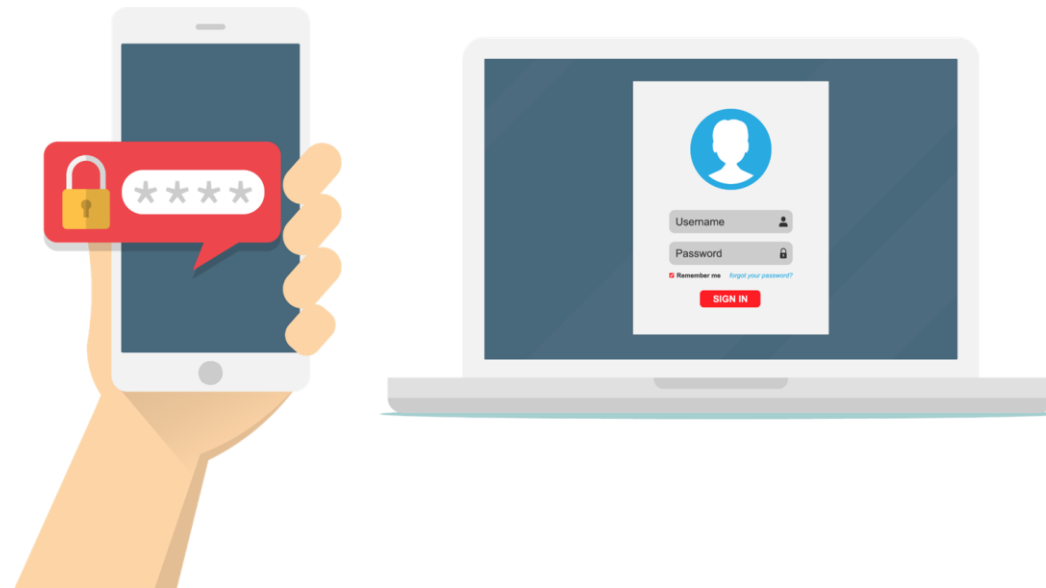
OpenID Connect is a cross-platform authentication system based on the OAuth 2.0 standard family. It employs basic REST/JSON message flows with the purpose of "making simple things simple while still making sophisticated things feasible."



OAuth Vs OpenID Connect

OAuth is used for authorization and OpenID Connect (OIDC) is used for authentication.

OpenID Connect is built on top of OAuth 2.0



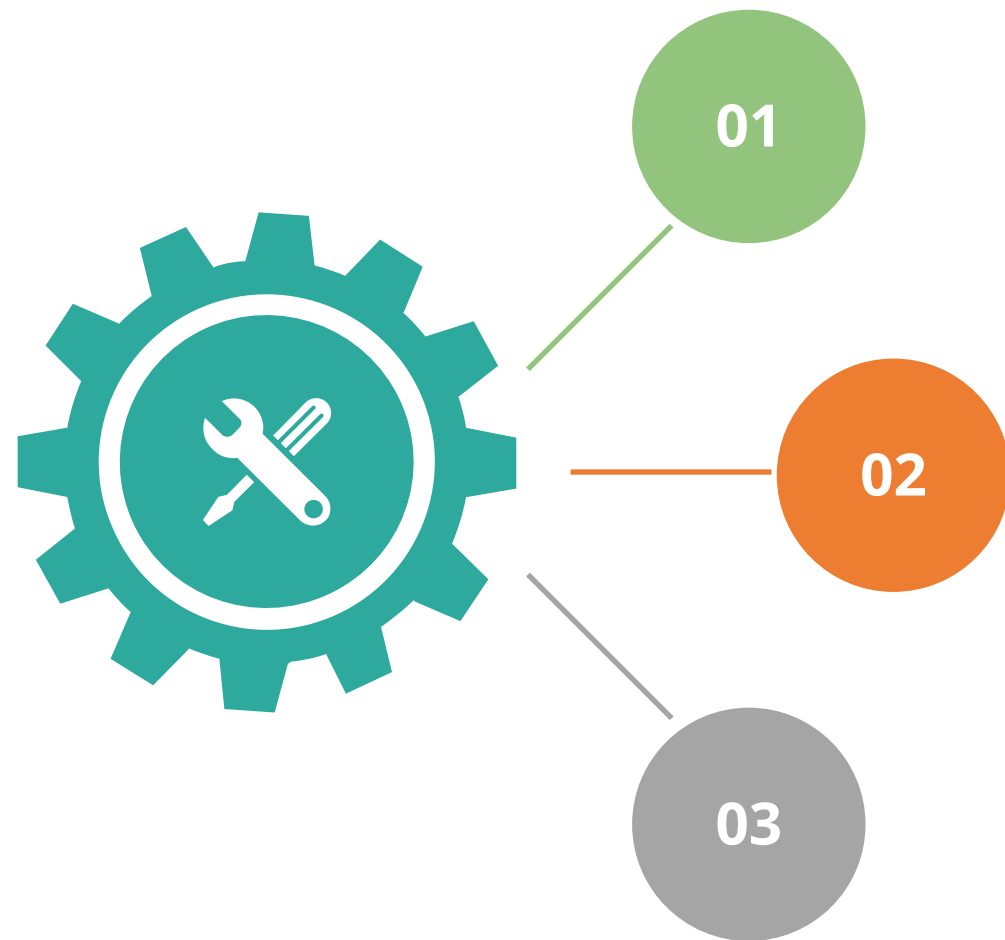
A user can get authorization to access a protected resource owned (using OAuth 2.0) in one request.

Difference Between OAuth and OpenID Connect

	OpenID	OAuth
Dates from	2005	2006
Current version	OpenID 2.0	OAuth 2.0
Main purpose	Single sign-on for consumers	API authorization between applications
Protocols used	XRDS, HTTP	JSON, HTTP
No. of related CVEs	24	3

Authorization Use Cases

Delegating authentication and authorization to Azure AD enables scenarios such as:



Conditional Access policies that require a user to be in a specific location

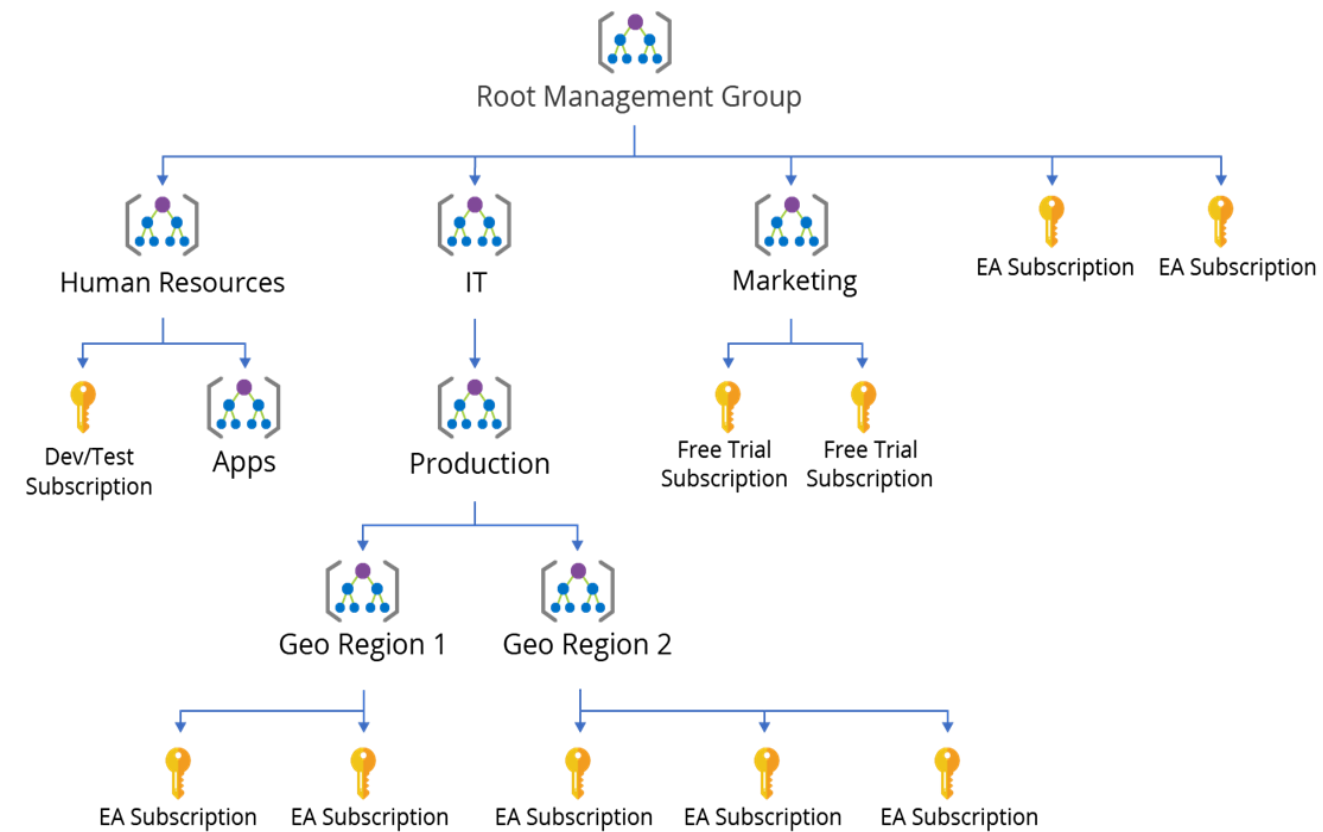
The use of multi-factor authentication, also called two-factor authentication or 2FA

Single Sign-On enables a user to sign in once and be automatically signed into all of the web apps

Recommend a Hierarchical Structure for Access Control

Management Groups

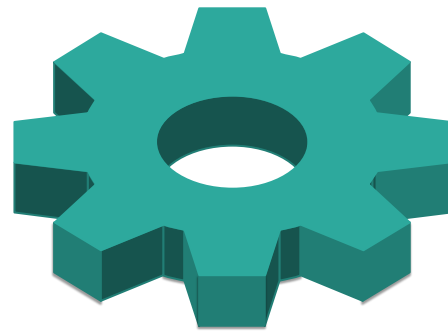
The organized subscriptions into containers are called **Management Groups**.



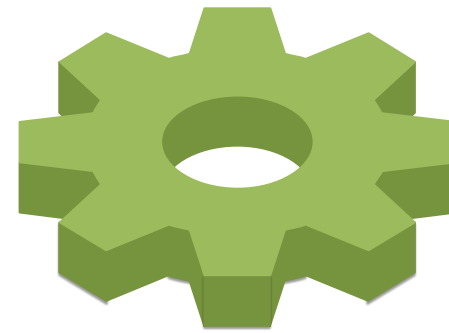
It provides a level of scope above subscriptions.

Management Groups

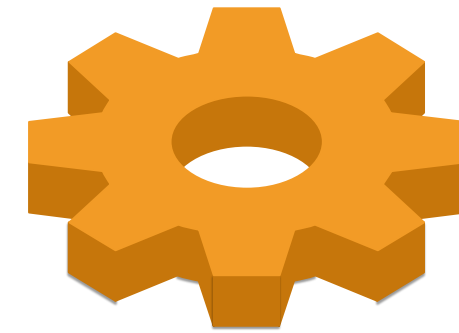
Features of Azure Management Groups:



Policy and spending budgets are targeted across subscriptions and inherited down the hierarchies.



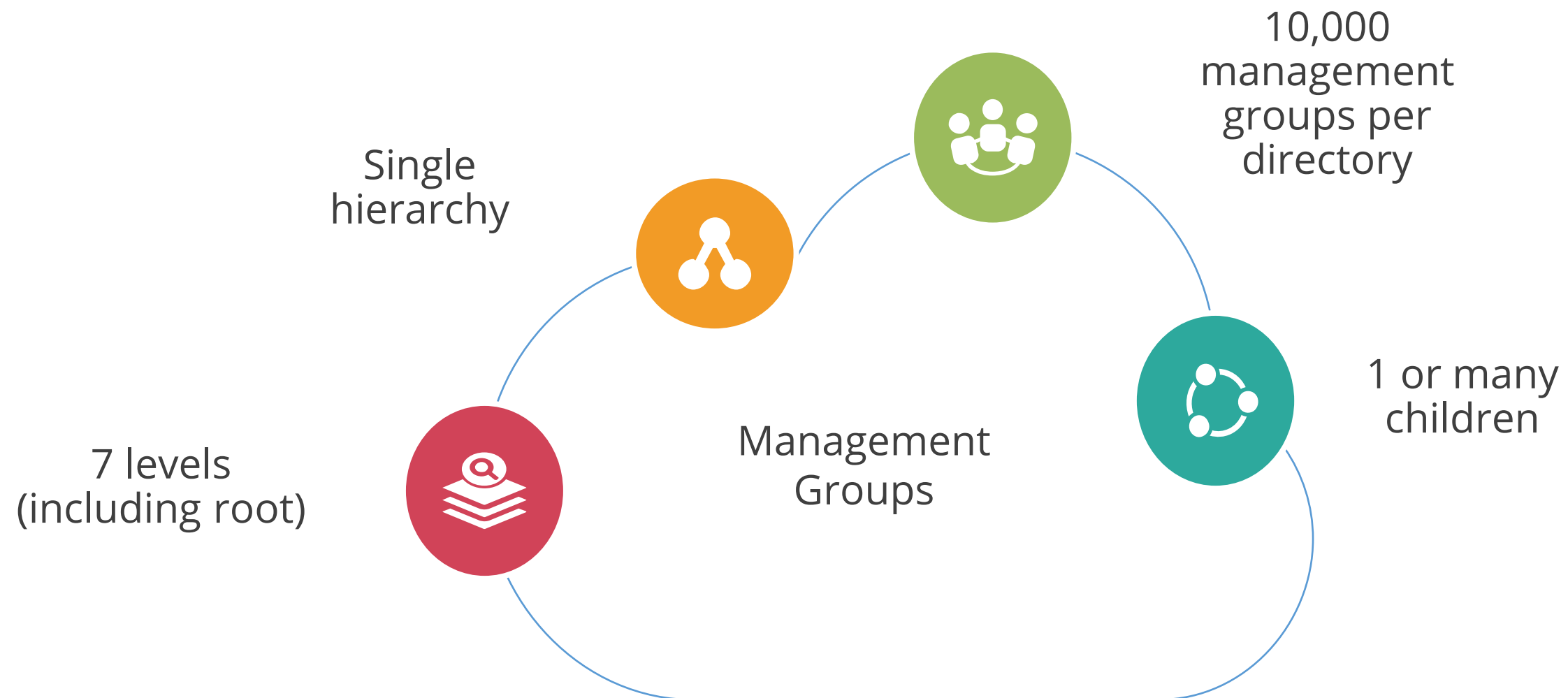
Compliance and cost reporting by organization (business/teams)



Organizational alignment for users' Azure subscriptions through custom hierarchies and grouping

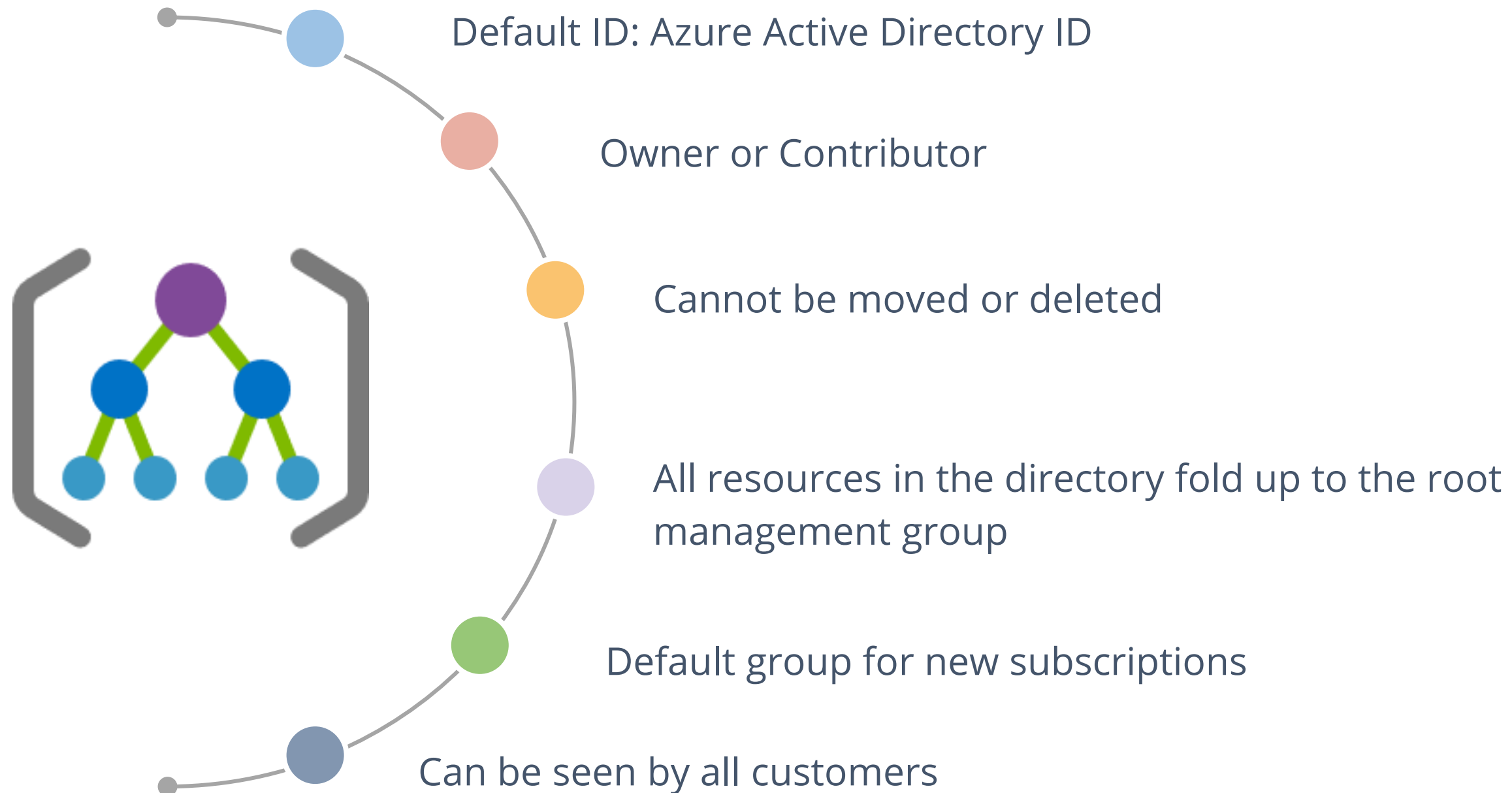
Management Groups

Facts about management groups:



Root Management Groups

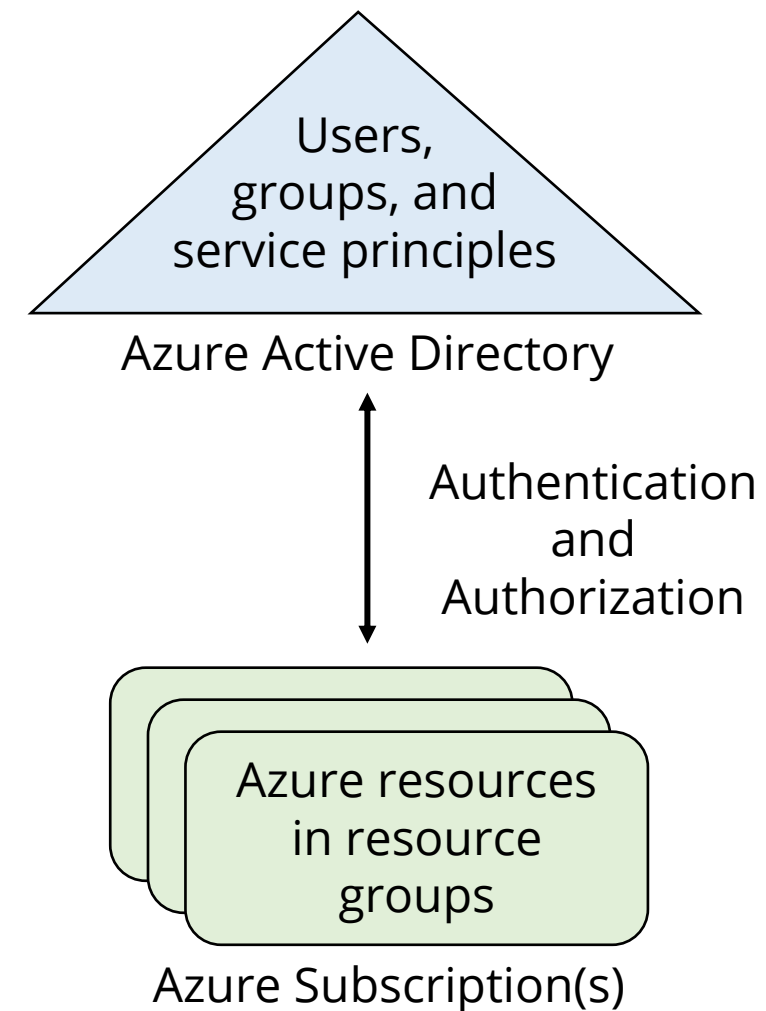
The Root of Management Groups has the following features:



Azure Subscriptions and Accounts

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

- Billing for Azure services is done on a per-subscription basis.
- Subscriptions have accounts and are associated with Azure AD.



Azure Subscriptions and Accounts

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

Typically to grant a user access to Azure resources, a user would add them to the Azure AD directory associated with their particular subscription.



Getting an Azure Subscription

Following fields are covered while creating an Azure Subscription:



Enterprise Agreement

Customers make an upfront monetary commitment to Azure



Reseller

Open licensing program



Microsoft partner

To look for a client or partner who can design and implement cloud solution



Free trial account

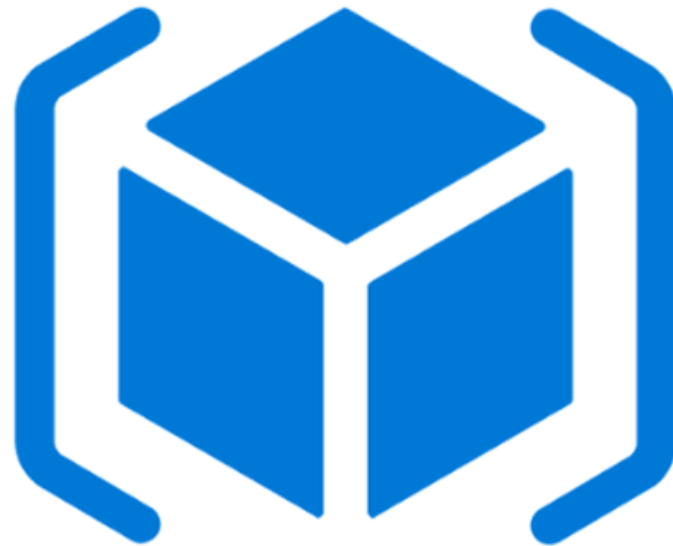
Subscription Usage

Below are the details of Azure Subscription usage as per the subscription category:

Subscription	Usage
Free	Includes a \$200 credit for the first 30 days, free limited access for 12 months
Pay-as-you-go	Charges user monthly
Enterprise	One agreement, with discounts for new licenses and software assurance: targeted at enterprise-scale organizations
Student	Includes \$100 for 12 months: must verify student access

Resource Groups

A resource group is a fundamental concept of the Azure platform.



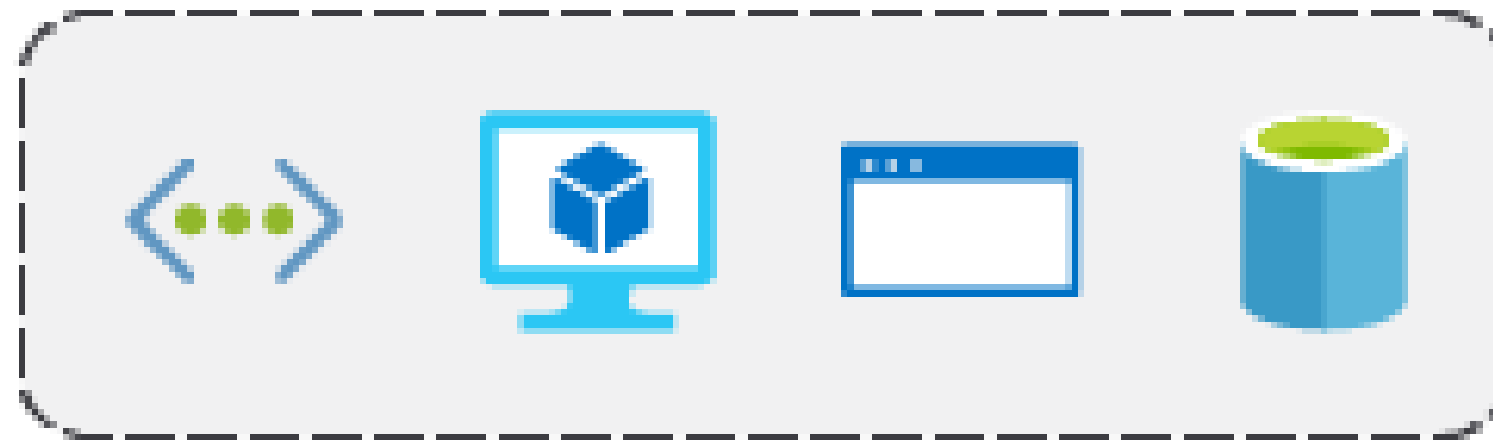
- It represents logical grouping of resources
- It ties to resource's life cycle
- It cannot be nested

Resource Groups

Most resources can be moved between resource groups.



Resource Group

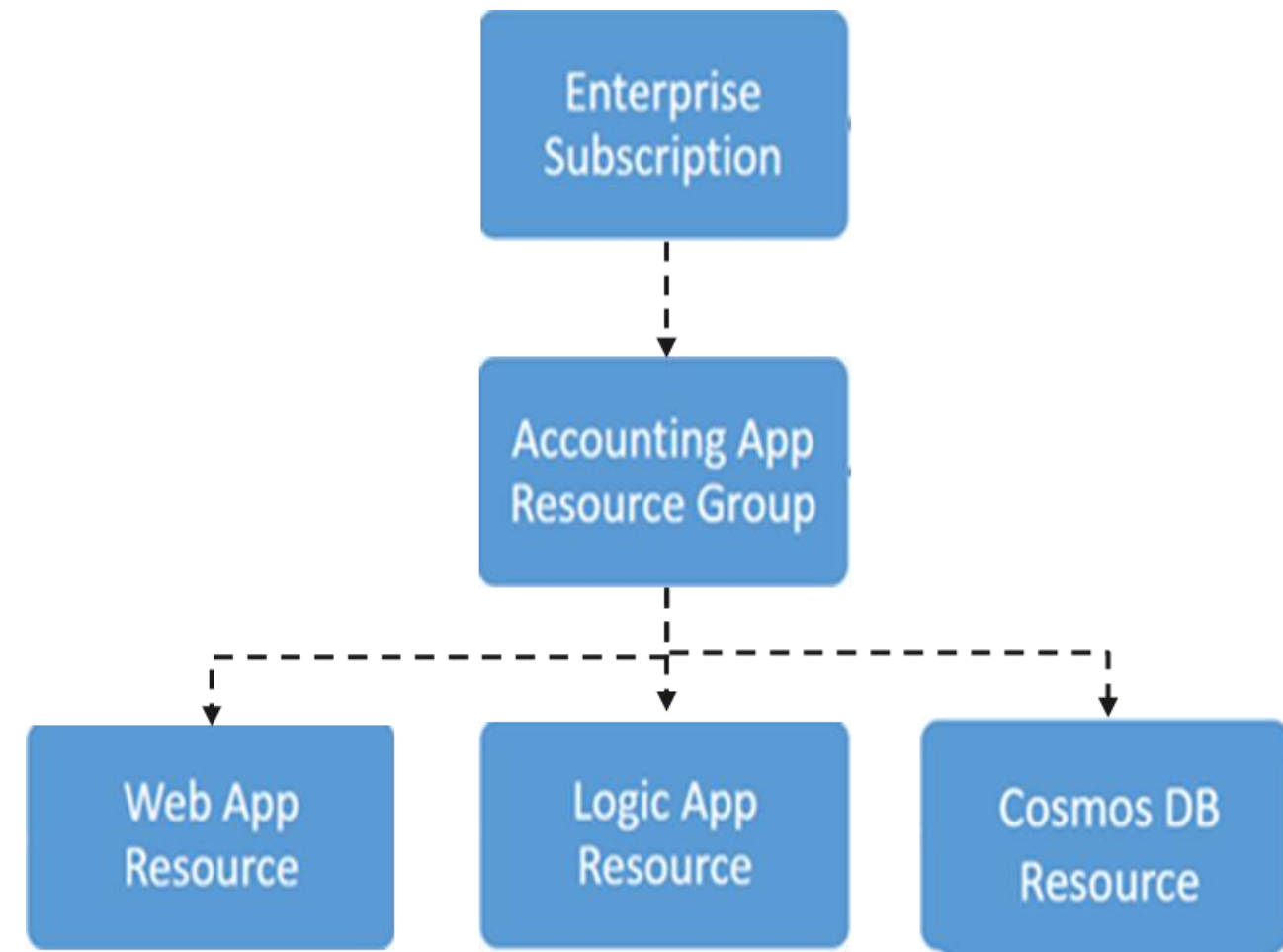


Each resource must belong to a resource group.

Resource Groups and Deployments

Resources can only exist in one resource group.

- Groups cannot be renamed
- Groups can have resources of different types (services)
- Groups can have resources from different regions
- Deployments are incremental



By scoping permissions to a resource group, you can add/remove and modify resources easily.

Why Does a Resource Group Need a Location?

The resource group stores metadata about the resources. Therefore, when users specify a location for the resource group, they are specifying where that metadata is stored.



For compliance reasons, one may need to ensure that their data is stored in a particular region.

Resource Group Organization

The factors that help in making a strategy to organize resources are:

**Organizing for
authorization**

Organizing for life cycle

Organizing for billing

Since resource groups are a scope of RBAC, you can organize resources by who will be in charge of administering them.

Resource Group Organization

The factors that help in making a strategy to organize resources are:

Organizing for authorization

Organizing for life cycle

Organizing for billing

If you delete a resource group, you delete all the resources in it. Use this where resources are more disposable, like non-production environments.

Resource Group Organization

The factors that help in making a strategy to organize resources are:

**Organizing for
authorization**

Organizing for life cycle

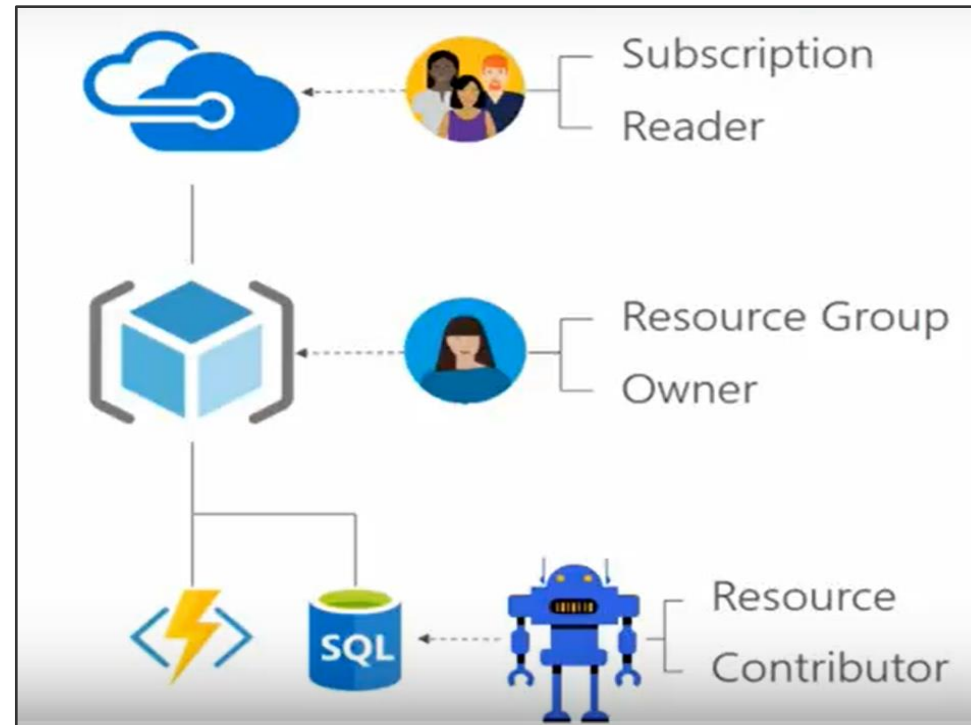
Organizing for billing

Placing resources in the same resource group is a way to group them for usage in billing reports.

Recommend an Access Management Solution

Role-Based Access Control

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



Role-Based Access Control

Role-based access control provides fine-grained access management of resources in Azure.



- Is built on Azure Resource Manager
- Segregates duties within your team
- Grants the users access to only perform the job

Role-Based Access Control

Users can grant access described in a role definition by creating an assignment.

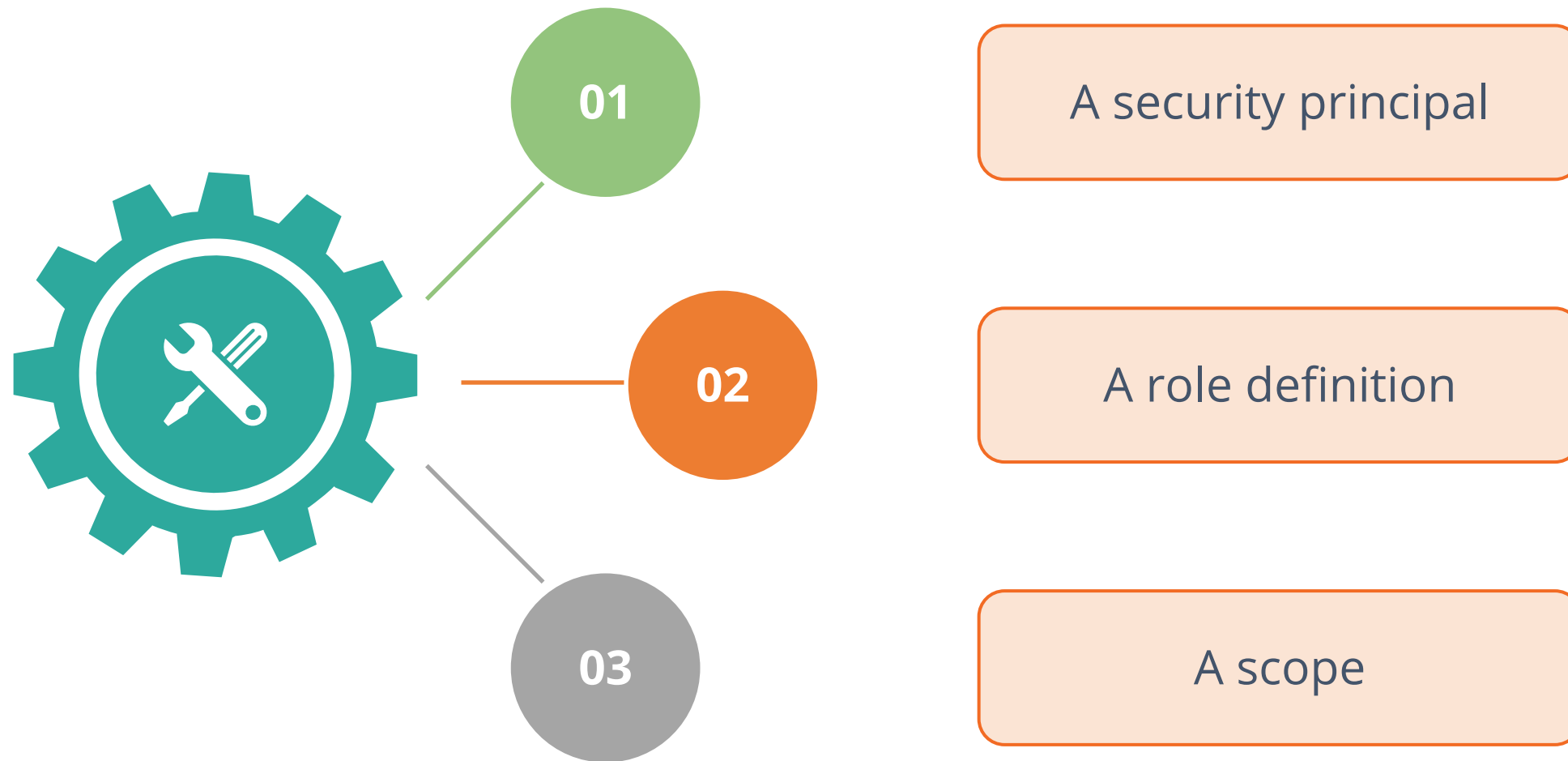
Concept	Definition
Security principal	Object that represents something that is requesting access to resources
Role definition	Collection of permissions that lists the operations that can be performed
Scope	Boundary for the level of access that is requested
Assignment	Attaching a role definition to a security principal at a particular scope

Deny assignments are currently read-only and are set by Azure Blueprints and Azure Managed Apps.

How RBAC Works

RBAC allows access control to the resource by assigning roles.

To create a role assignment, three elements are required:



Security Principal

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

1 Security principal



User



Group



Service
principal





Managed
identity

Role Definition

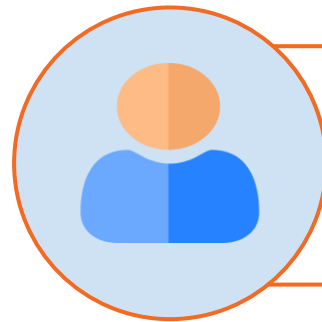
A role is a collection of actions that can be performed on Azure resources.

The screenshot shows the Azure portal interface for the 'ContosoBlueAD' resource group. The left sidebar contains a list of resource groups, with 'ContosoBlueAD' selected. The main pane displays the 'Access control (IAM)' page, which includes a search bar and a table of roles. The table has columns for NAME, TYPE, ROLE, and SCOPE. The 'Add' button in the top right of the table is highlighted with a red box. The 'Access control (IAM)' link in the left sidebar is also highlighted with a red box.

NAME	TYPE	ROLE	SCOPE
OWNER			
 coreyhynes@outlook.com coreyhynes@outlook.com	User	Owner ⓘ	Subscription (Inherited) >
VIRTUAL MACHINE CONTRIBUTOR			
<input type="checkbox"/>  admin admin@contosoblu...	User	Virtual Machine Contributor ⓘ	This resource

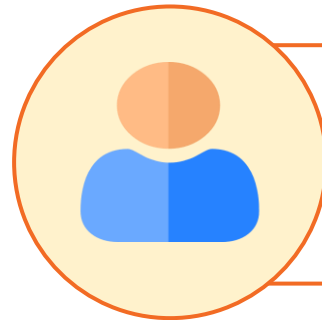
Role Definition

Three most common roles are:



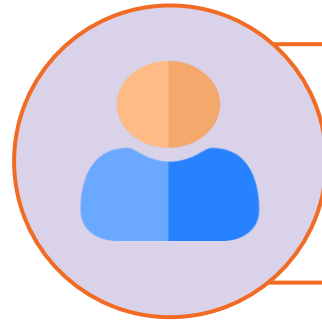
Owner

Can manage everything, including access



Contributors

Can manage everything except access



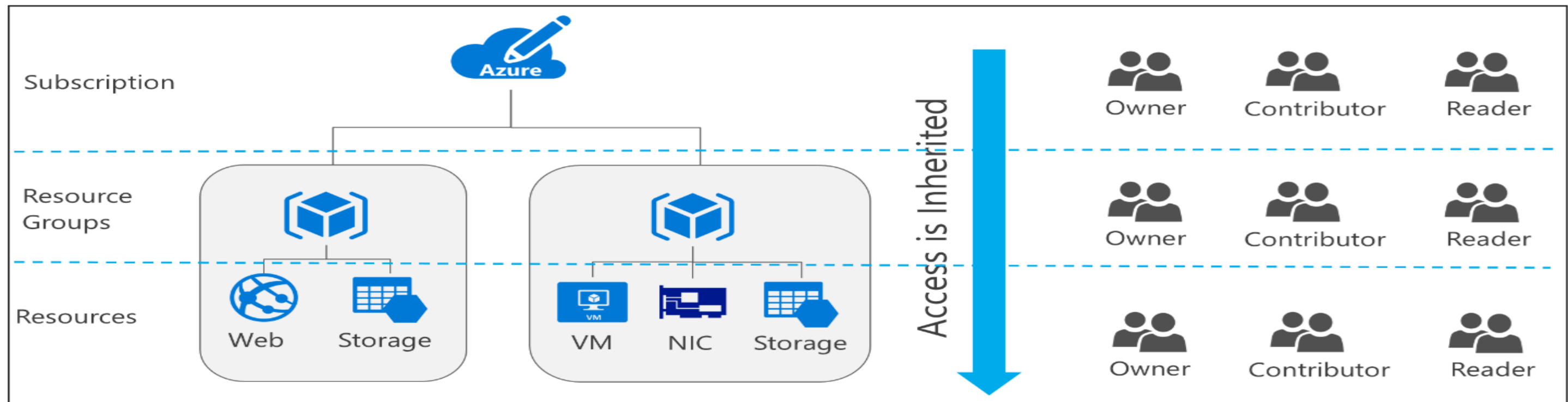
Readers

Can view everything but can't make changes

Scope

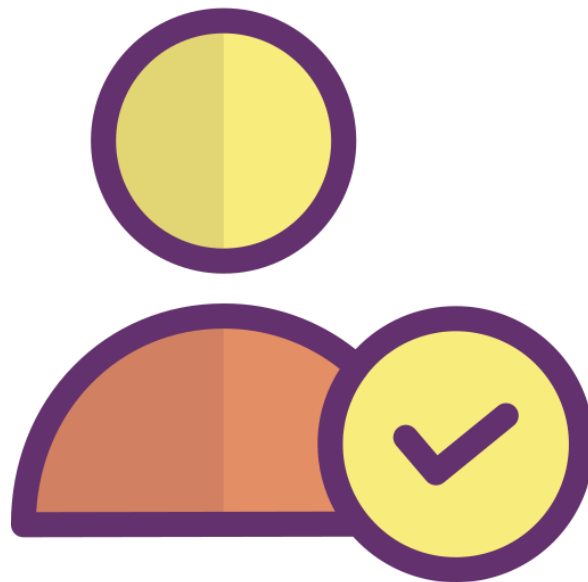
Scope is where the access applies to.

The user can limit the scope to a subscription, a resource group, or specific resources.



Role Assignment

A role assignment is created that associates a security principal to a role.



The security principal defines the access policy and permissions for the user/application in the Azure AD tenant.

Role Assignment

Roles can be assigned to the following types of Azure AD security principals:

Users

Groups

Service Principals

- Is assigned to organizational users in the AD associated with the subscription
- Can also be assigned to external Microsoft accounts in the same directory

Role Assignment

Roles can be assigned to the following types of Azure AD security principals:

Users

Groups

Service Principals

- Assigned to Azure AD security groups
- The best practice is to manage access through groups, adding roles, and assigning users.

Role Assignment

Roles can be assigned to the following types of Azure AD security principals:

Users

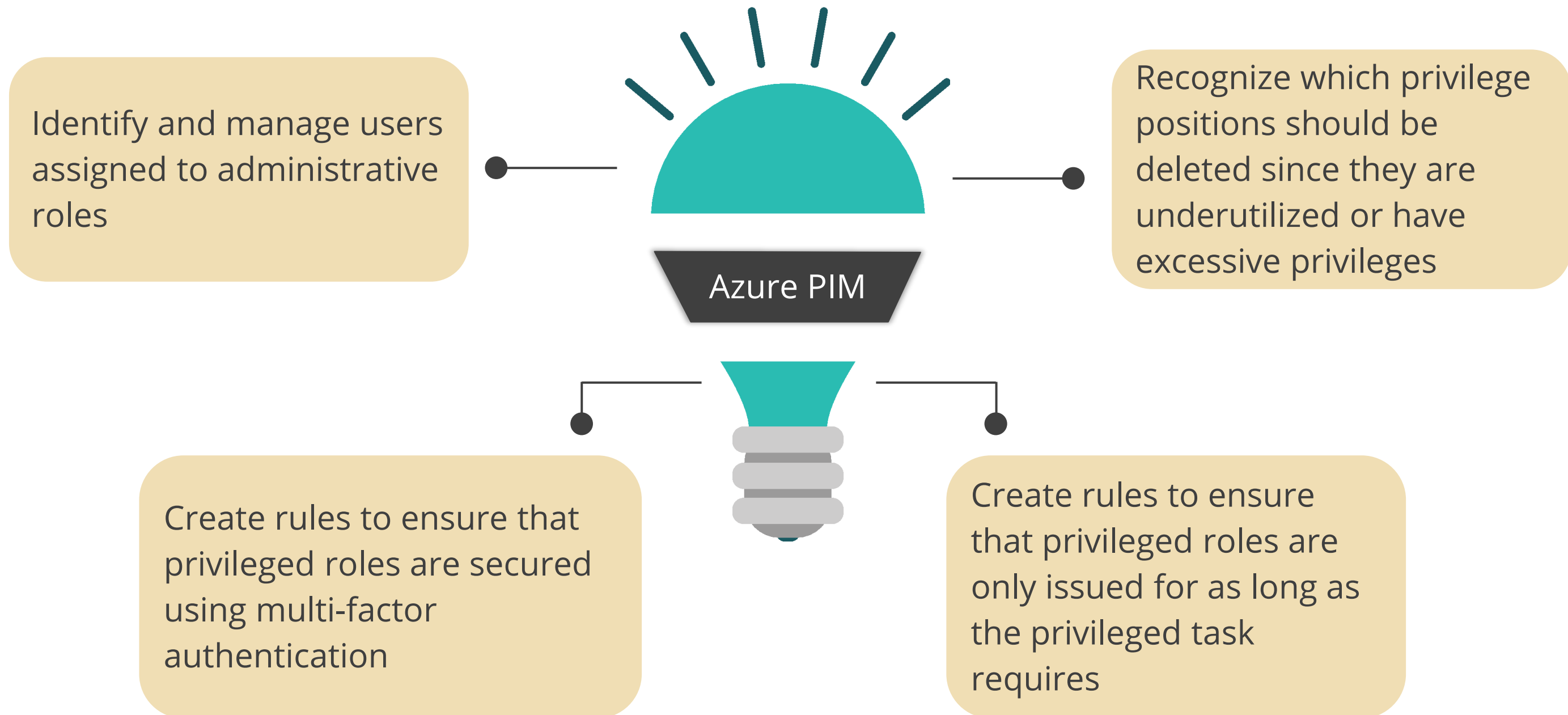
Groups

Service Principals

- Service identities are represented as service principals in the directory.
- Authenticate with Azure AD and securely communicate with one another

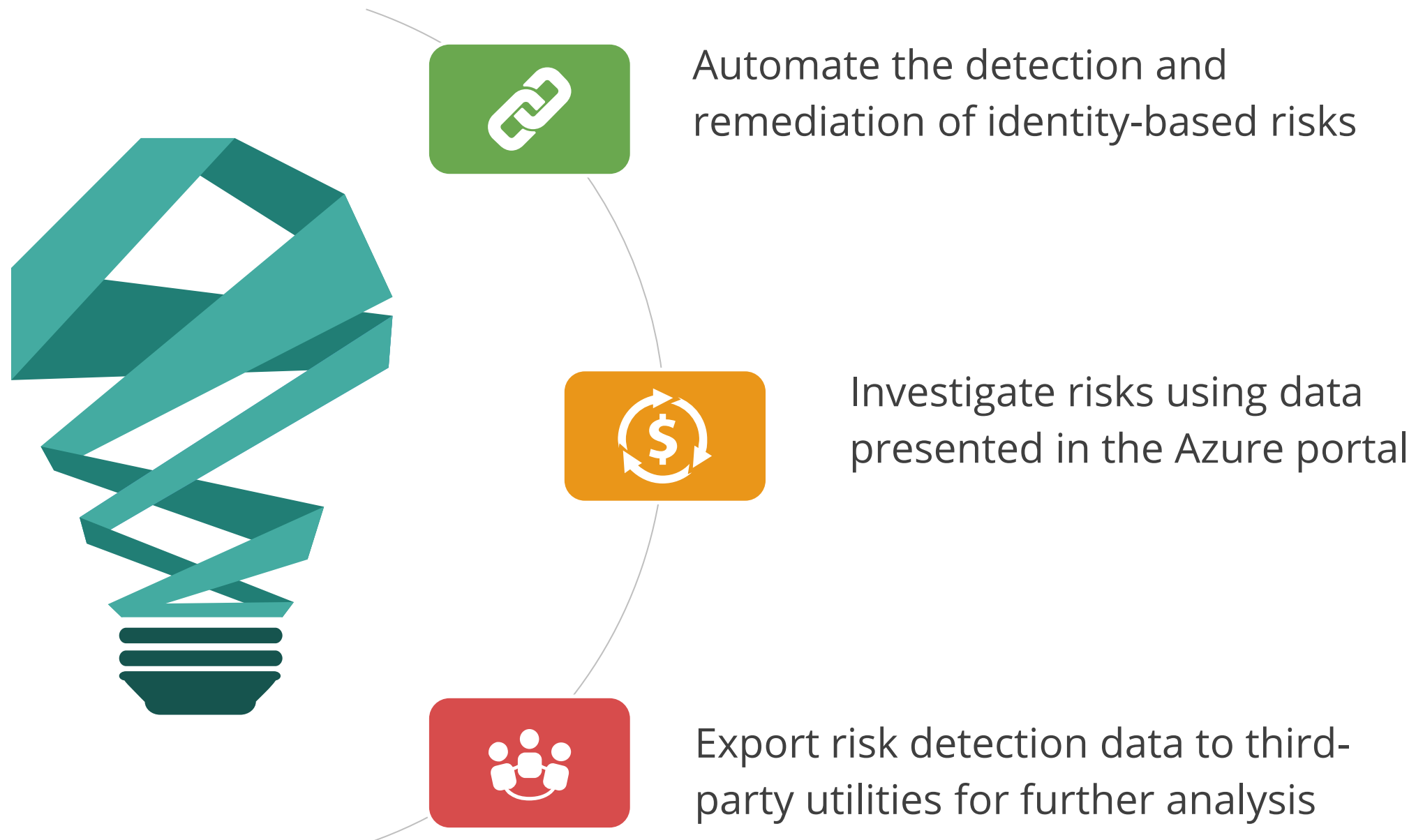
Azure AD Privileged Identity Management

Azure AD Privileged Identity Management (PIM) helps you minimize account privileges by:



Azure Active Directory Identity Protection

Protection allows organizations to accomplish three key tasks:



Azure Active Directory Identity Protection

Risk detection and remediation are given in the table below:

Risk detection type	Description
Atypical travel	Sign in from an atypical location based on the user's recent sign-ins
Anonymous IP address	Sign in from an anonymous IP address (for example: Tor browser, anonymizer VPNs)
Unfamiliar sign-in properties	Sign in with properties we have not seen recently for the given user
Malware linked IP address	Sign in from a malware linked IP address
Leaked credentials	This risk detection indicates that the user's valid credentials have been leaked
Azure AD threat intelligence	Microsoft's internal and external threat intelligence sources have identified a known attack pattern

Azure Active Directory Identity Protection

Administrators can review detections and take manual action on them if needed.



Identity and Access Management Best Practices

Some of the best practices for identity and access management are:



- Single enterprise directory
- Synchronize identity systems
- Use cloud provider identity source for third parties
- Passwordless or Multi-Factor Authentication for admins

Identity and Access Management Best Practices



- Block legacy authentication
- Don't synchronize on-premises admin accounts to cloud identity providers
- Use modern password protection offerings
- Use cross-platform credential management

Assisted Practice

Manage Subscriptions and RBAC

Duration: 10 Min.

Problem Statement:

You have been asked to implement the following:

- Creating a management group that would include all of Sim-Edu's Azure subscriptions
- Granting permissions to submit support requests for all subscriptions in the management group to a designated Azure Active Directory user. That user's permissions should be limited only to:
- Creating support request tickets
- Viewing resource groups

Assisted Practice: Guidelines

Steps to manage subscriptions and RBAC are:

1. Log into the Azure portal at <https://portal.azure.com>
2. Implement management groups
3. Create custom RBAC roles and assign the RBAC roles



Assisted Practice

Azure AD Identity Protection

Duration: 10 Min.

Problem Statement:

You have been asked to demonstrate Azure AD premium feature for identity protection.

Assisted Practice: Guidelines

Steps to demonstrate the features of identity protection are:

1. Log into the Azure portal at <https://portal.azure.com>
2. Deploy an Azure VM (Virtual Machine) by using an Azure Resource Manager template
3. Implement Azure AD (Active Directory) Identity Protection
4. Validate Azure AD Identity Protection configuration by simulating risk events



Assisted Practice

Azure RBAC and Policy

Duration: 10 Min.

Problem Statement:

You have been asked to configure delegation of provisioning and management of Azure resources by using built-in Role-Based Access Control (RBAC) roles and built-in Azure policies.

Assisted Practice: Guidelines

Steps to demonstrate RBAC and policy are:

1. Log into the Azure portal at <https://portal.azure.com>
2. Create Azure Active Directory (AD) users and groups
3. Create Azure resource groups
4. Delegate management of an Azure resource group via a built-in RBAC role
5. Assign a built-in Azure policy to an Azure resource group



Assisted Practice

Azure AD PIM

Duration: 10 Min.

Problem Statement:

You have been asked to discover resources using Azure AD PIM.

Assisted Practice: Guidelines

Steps to demonstrate Azure AD PIM are:

1. Log into the Azure portal at <https://portal.azure.com>
2. Search for Azure AD Privileged Identity Management and select it
3. Configure Azure AD PIM



Key Takeaways

- Microsoft identity platform implements the OAuth 2.0 protocol for handling authorization.
- The root management group's display name is the Tenant root group, and this is the Azure Active Directory ID.
- The resource group stores metadata about the resources.
- Role-based access control (RBAC) is the capability to grant appropriate access to Azure AD users, groups, and services.
- To create a role assignment in RBAC, three elements are required, namely security principal, role definition, and scope.



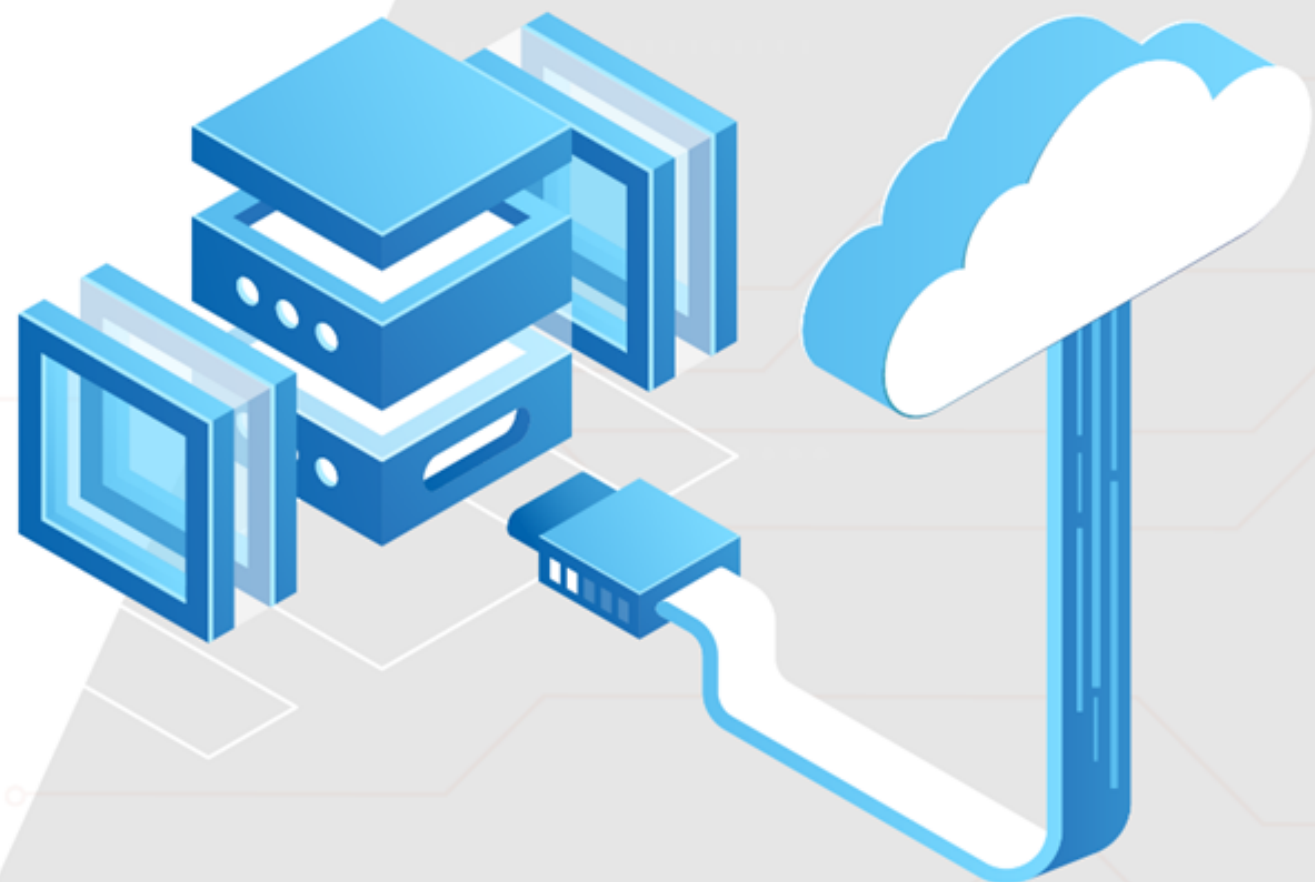


Project Agenda: To implement role-based access control

Description: You are working as the head of Cloud Security in an organization. You have been given a project to design authorization as part of cloud resource compliance and security. You have been asked to restrict access to different scopes depending on the employee's designation and the role and ensure you follow the principle of least privilege.

Perform the following:

1. Creating two resource groups in two different regions
2. Creating two groups under two resource groups in Azure AD
3. Creating two users and adding them to each of the resource groups in Azure AD
4. Granting contributor access and security assessment contributor access to the DEVELOPMENT group and SECURITY ANALYST group



Thank you