Cloud Computing

Caltech | Center for Technology & Management Education

PG CC - Microsoft Azure Architect Design: AZ:304

Cloud

Design Authorization

Caltech | Center for Technology & Management Education

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 Head of Cloud Security in an organization. As part of cloud resource compliance and security, you have been asked to provide your organization a solution for the below use cases:

- Restrict access to different scopes depending on the employee's designation and role and ensure you follow the principle of least privilege.
- Control who has access to Azure resources, what they can do with those resources, and what places they may access.
- Manage, regulate, and monitor access to critical resources in your company, such as Azure AD, Azure, and other Microsoft Online Services like Microsoft 365 or Microsoft Intune.

To achieve all of 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

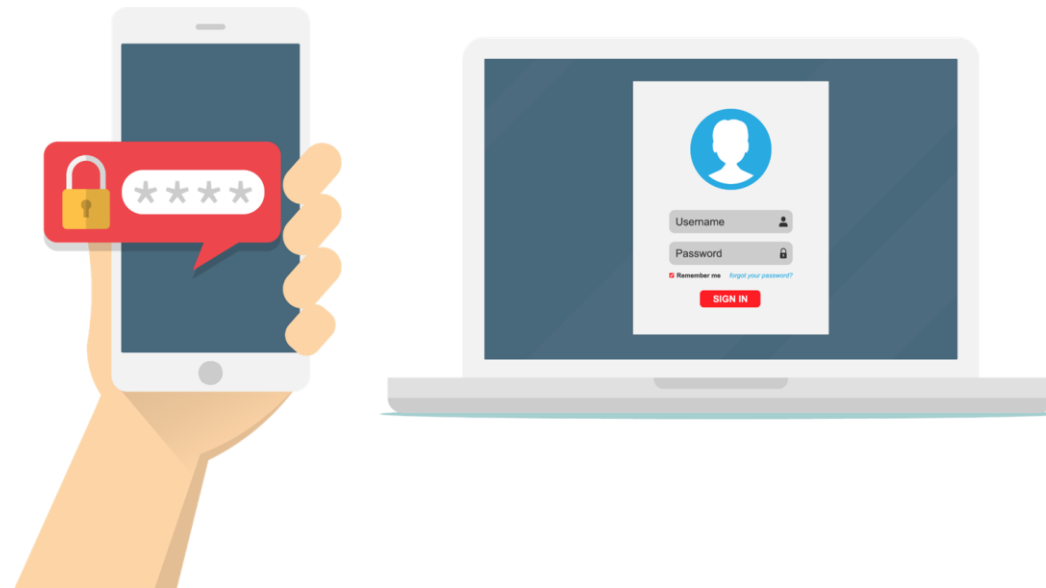It is the act of granting permission to an authenticated person to perform something.

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

OAuth Vs OpenID Connect

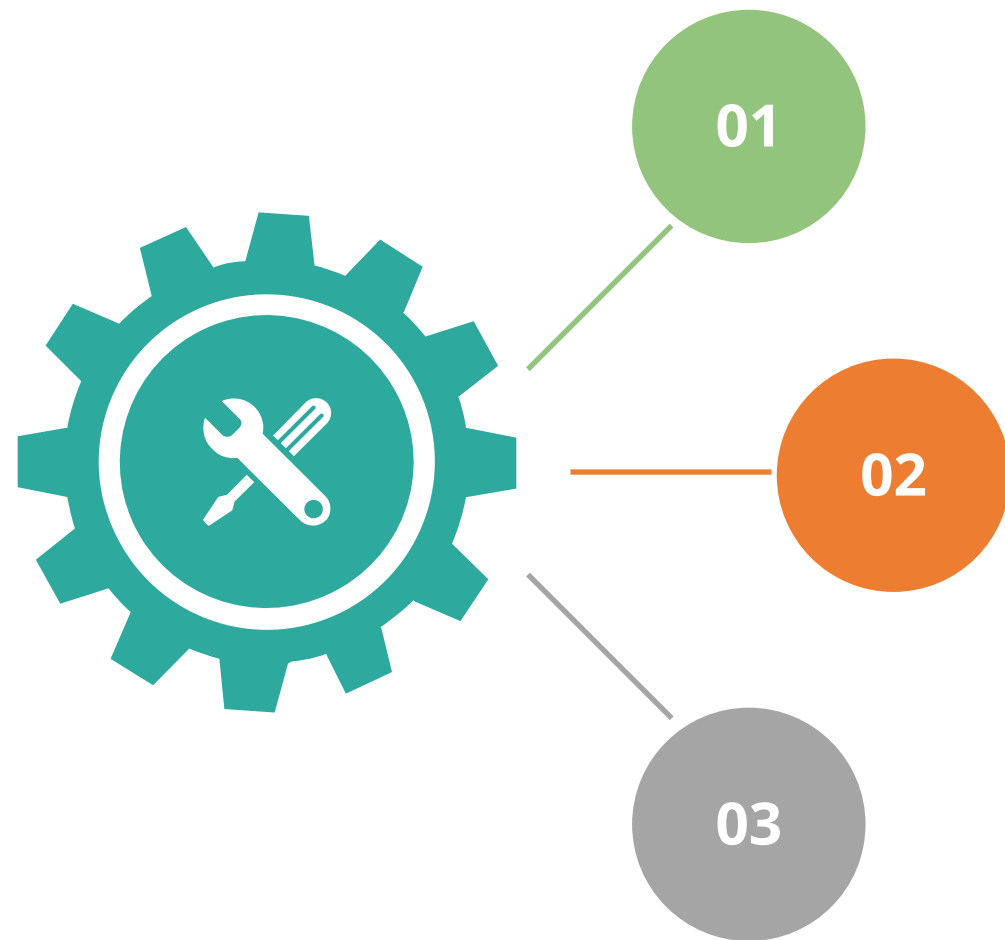OAuth is used for authorization and OpenID Connect (OIDC) is used for authentication.

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.

Authorization Use Cases

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

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

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

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

Caltech | Center for Technology & Management Education

Recommend a Hierarchical Structure for Access Control
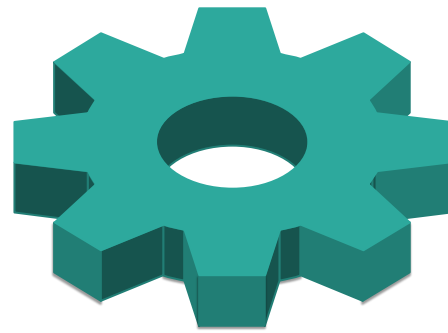
Management Groups

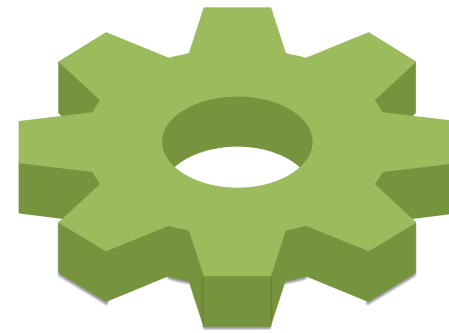The organized subscriptions into containers are called **Management Groups**.
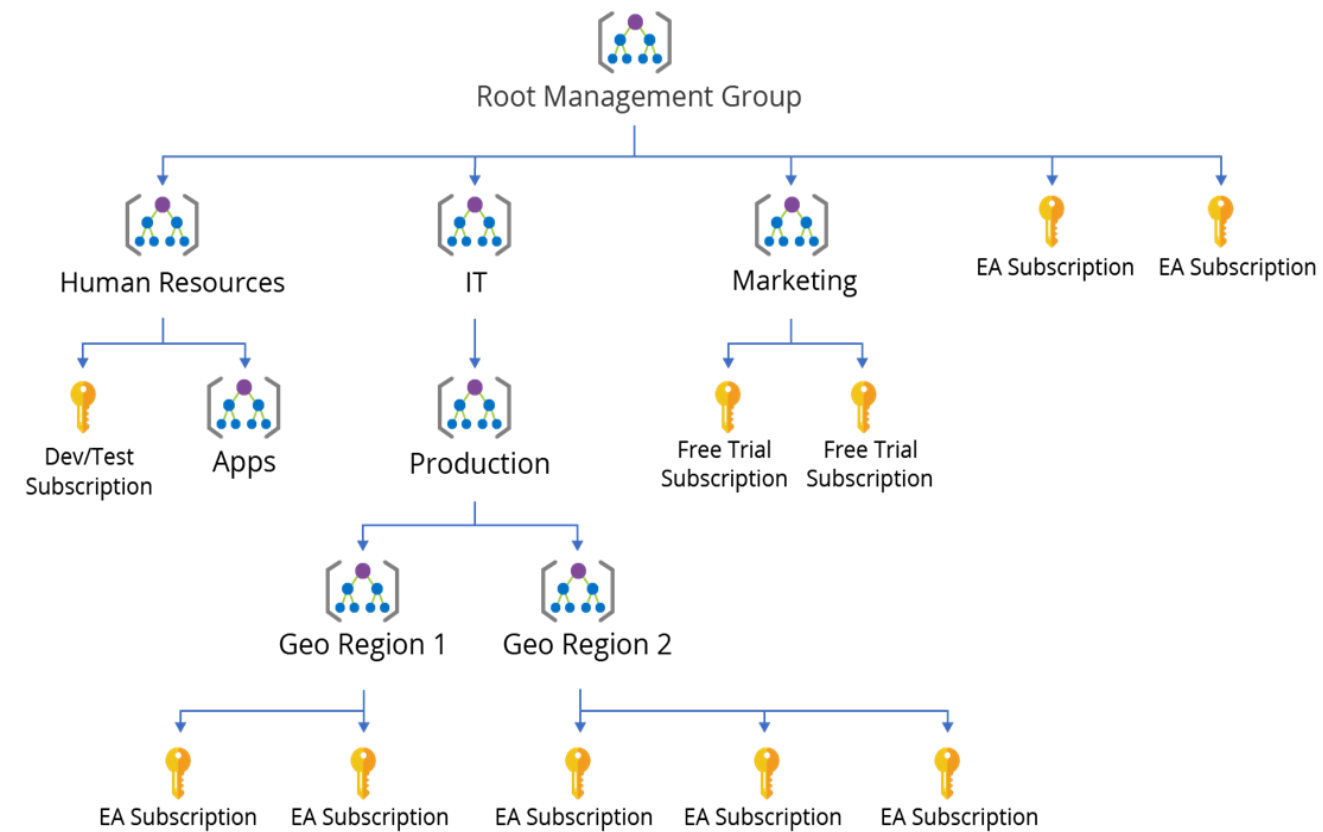
It provides a level of scope above subscriptions.
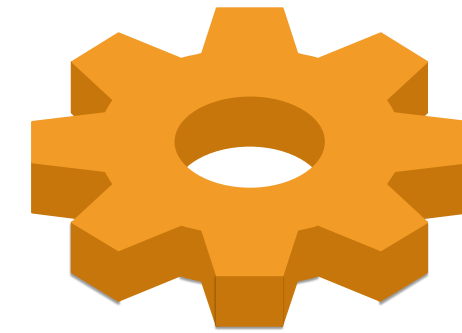
Management Groups

Features of Azure Management Groups:

Policy and spending budgets are targeted across subscriptions and inherited down the hierarchies.
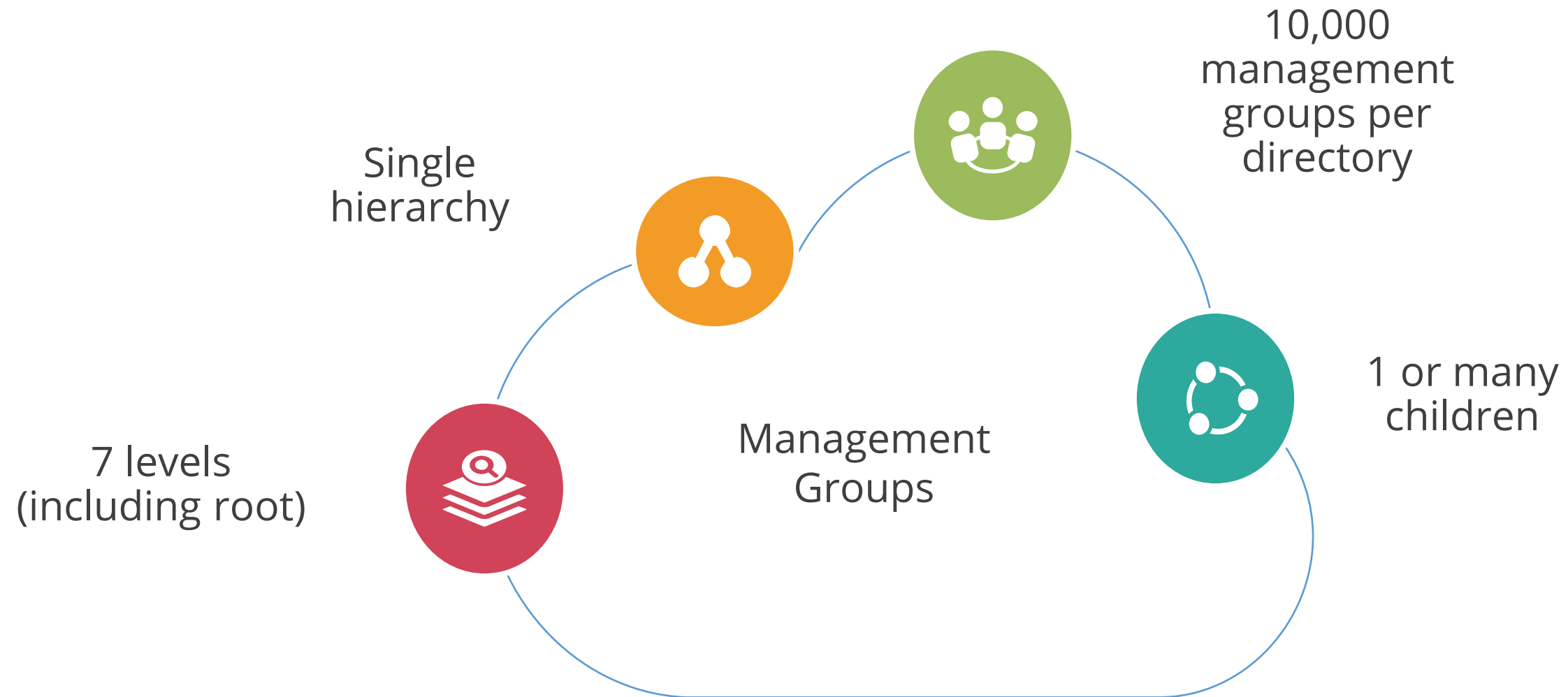
Compliance and cost reporting by organization (business/teams)

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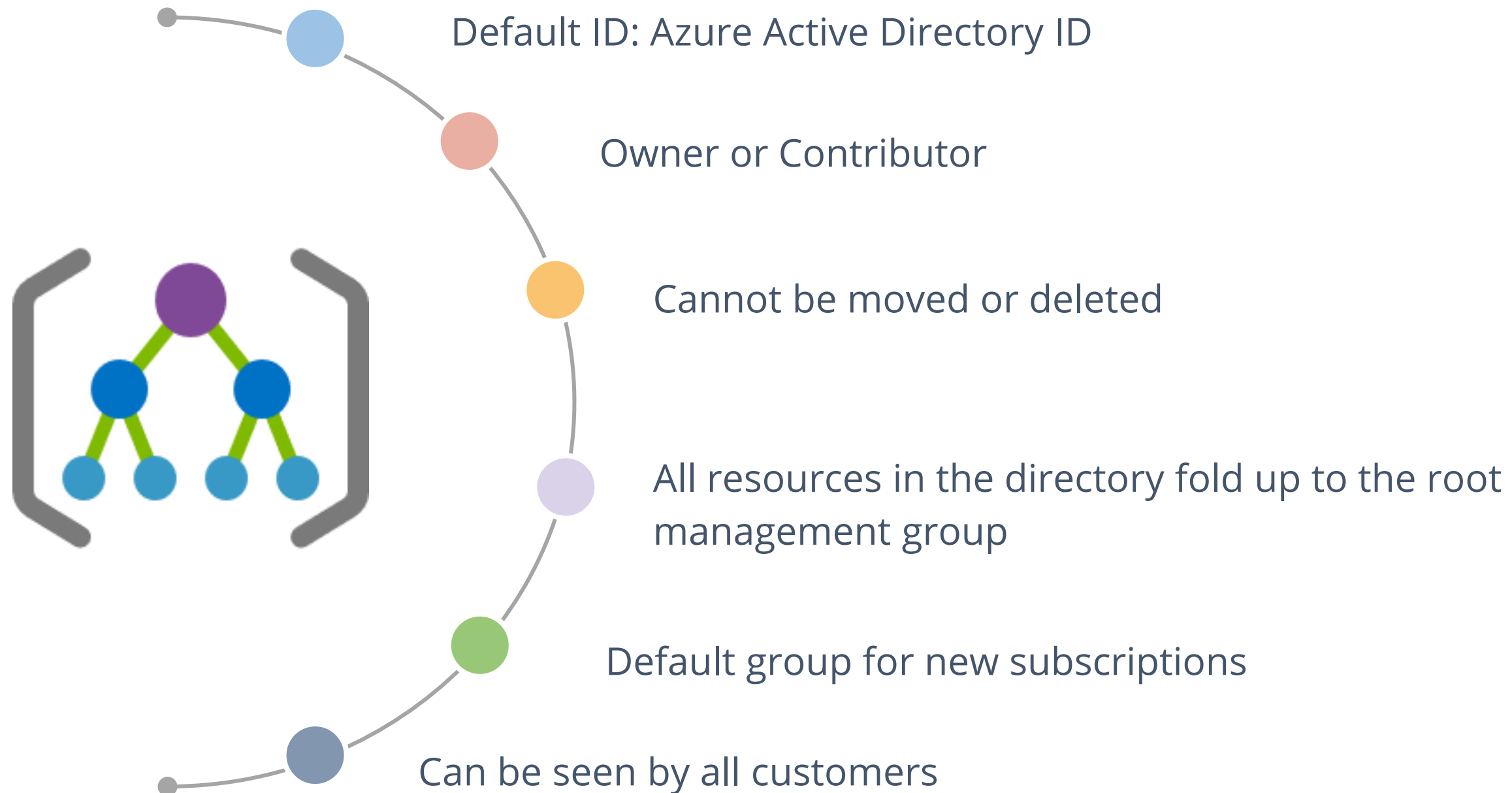
Management Groups

Facts about management groups:

10,000 management groups per directory

Single hierarchy

1 or many children

Management Groups

7 levels (including root)

Root Management Groups

The Root of Management Groups has the following features:

Default ID: Azure Active Directory ID

Owner or Contributor

Cannot be moved or deleted

All resources in the directory fold up to the root management group

Default group for new subscriptions

Can be seen by all customers

Caltech | Center for Technology & Management Education

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.

Users, groups, and service principles

Azure Active Directory

Authentication and Authorization

Azure resources in resource groups

Azure Subscription(s)
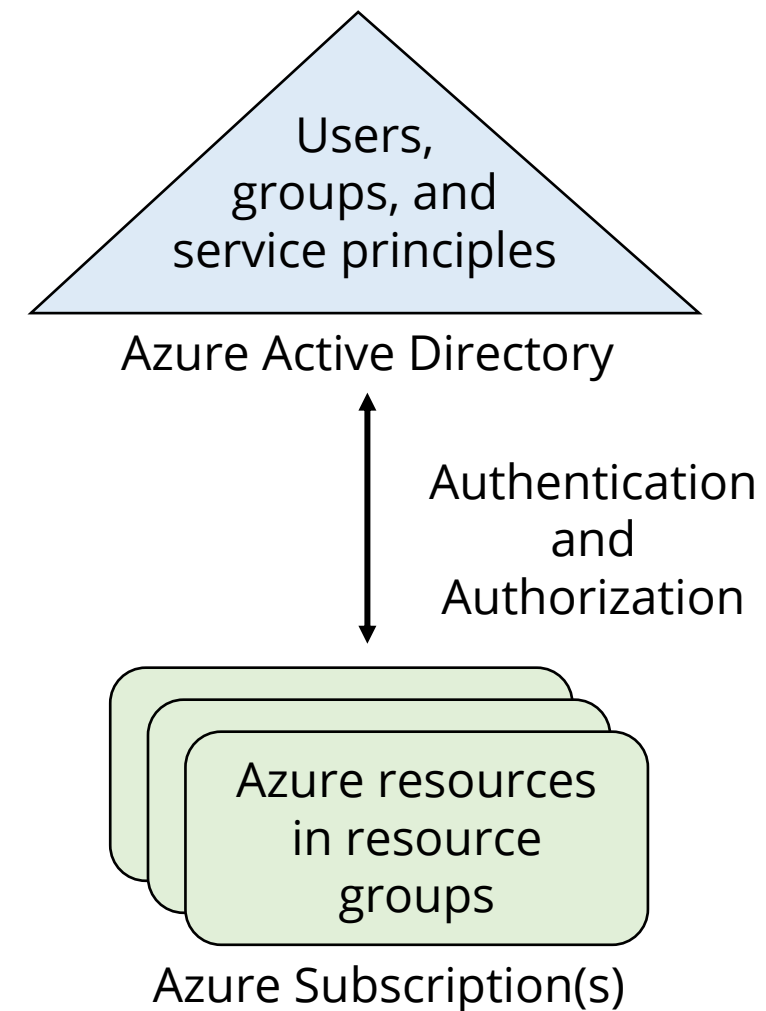
Azure Subscriptions and Accounts

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

Powerd by simplilearn

Caltech | Center for Technology & Management Education

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

Caltech | Center for Technology & Management Education

Resource Groups

A resource group is a fundamental concept of the Azure platform.
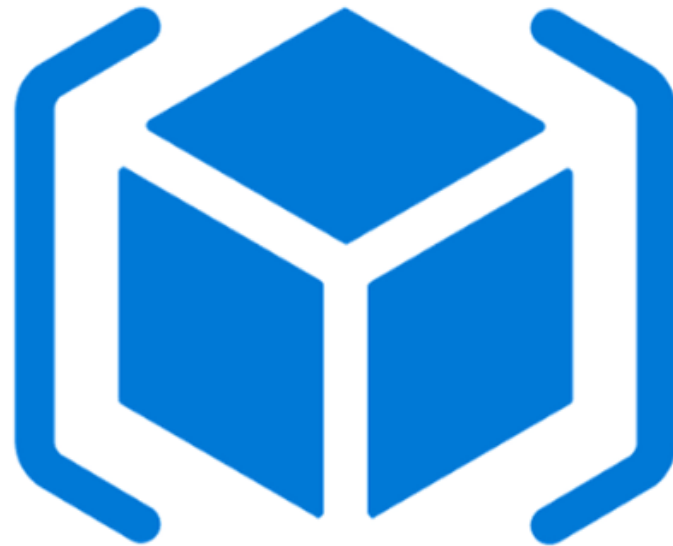
- It represents logical grouping of resources

- It ties to resource's life cycle

- It cannot be nested

Caltech | Center for Technology & Management Education

Resource Groups

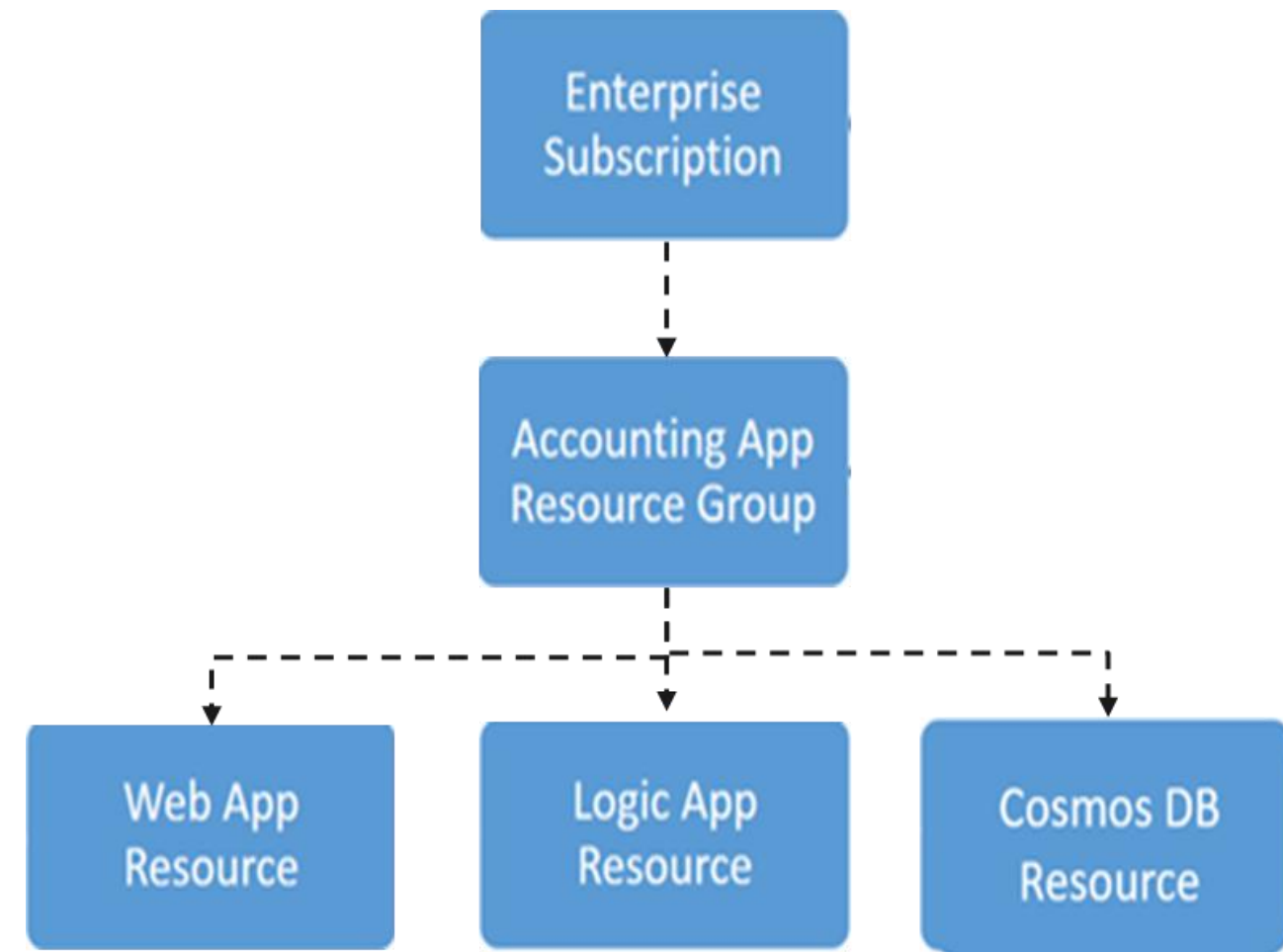Most resources can be moved between resource groups.
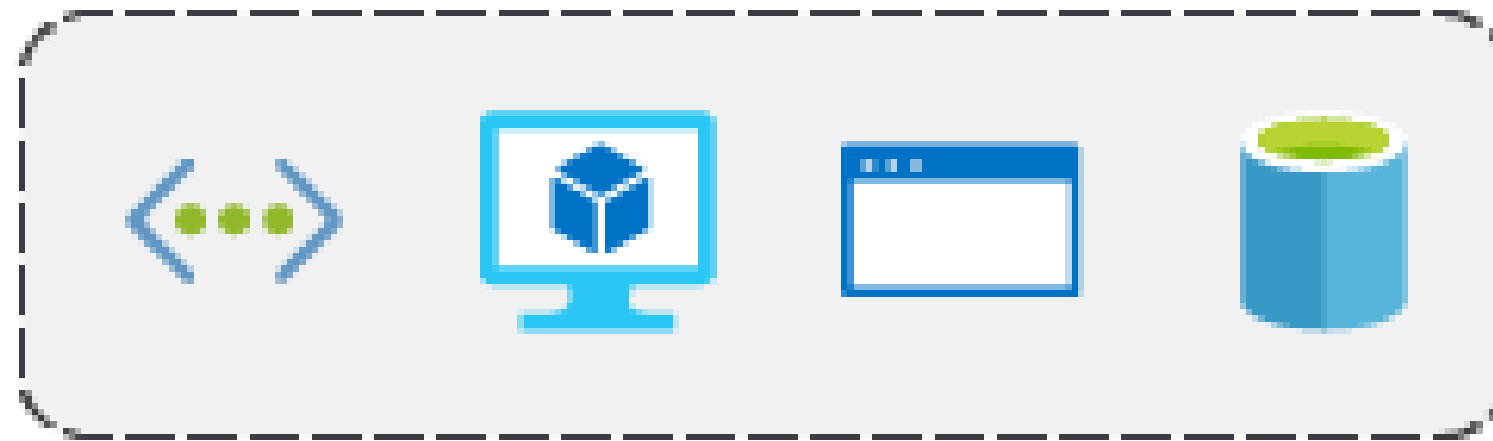
Each resource must belong to a resource group.

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.

Caltech | Center for Technology & Management Education

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.

Caltech | Center for Technology & Management Education

Resource Group Organization

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

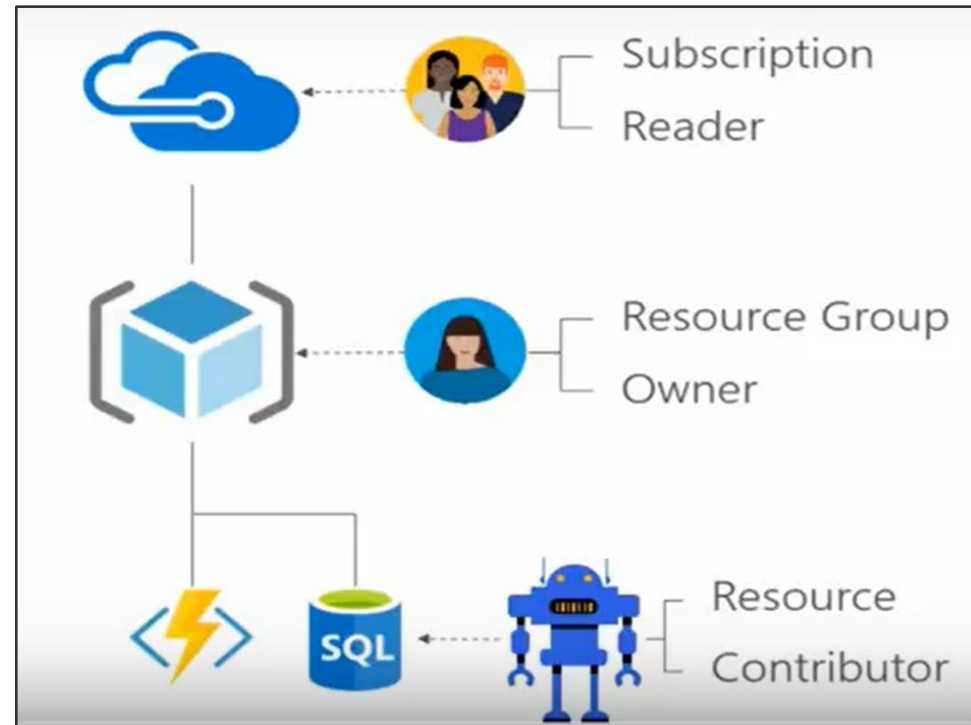**Organizing for authorization**

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

Caltech | Center for Technology & Management Education

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.

Caltech | Center for Technology & Management Education

How RBAC Works

RBAC allows access control to the resource by assigning roles.

To create a role assignment, three elements are required:

01 — A security principal

02 — A role definition

03 — A scope

Caltech | Center for Technology & Management Education
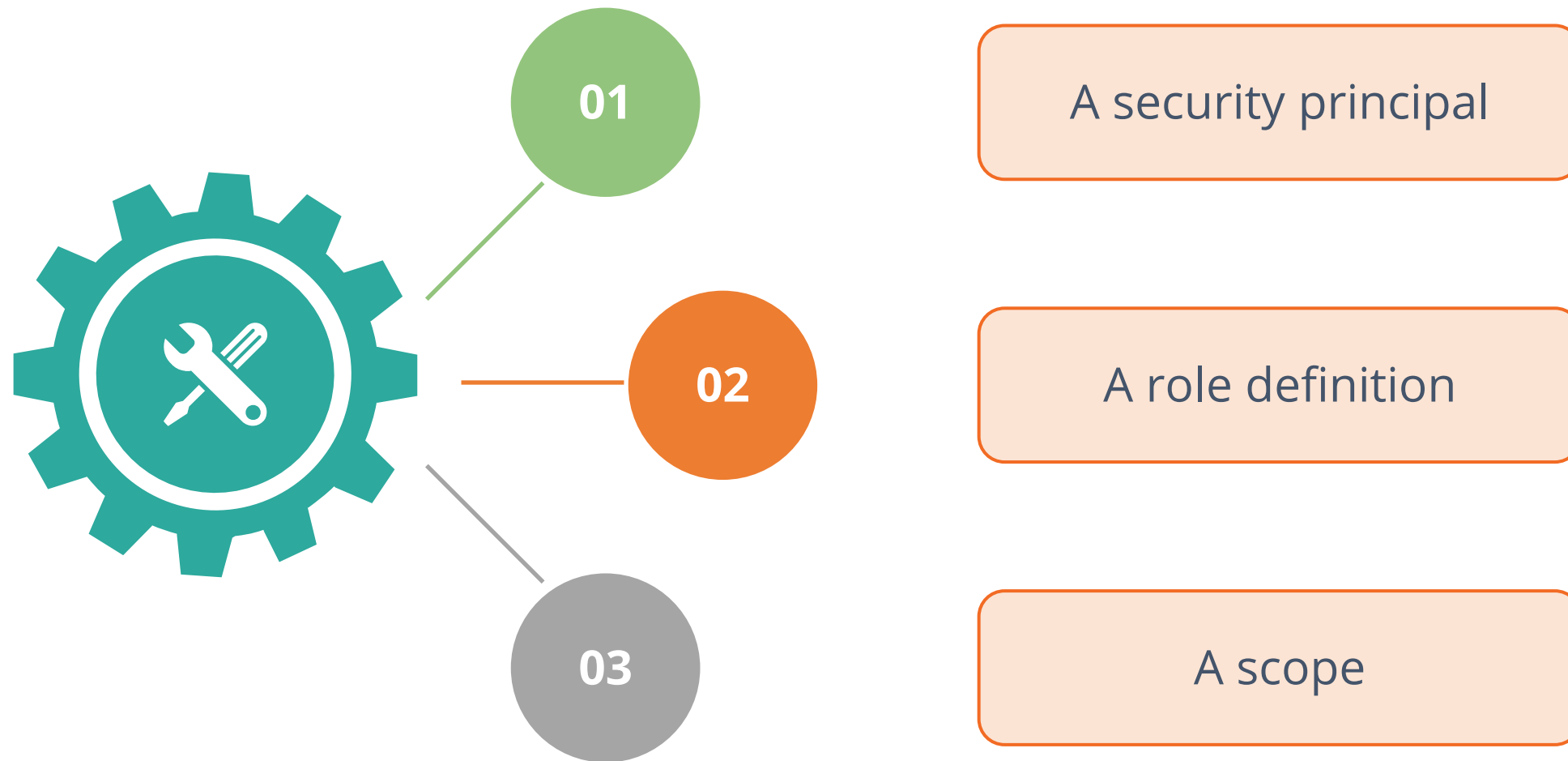
Security Principal

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

Role Definition

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

Role Definition

Three most common roles are:
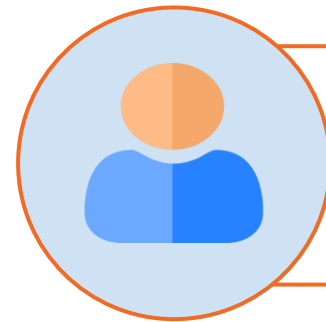
Owner

Can manage everything, including access
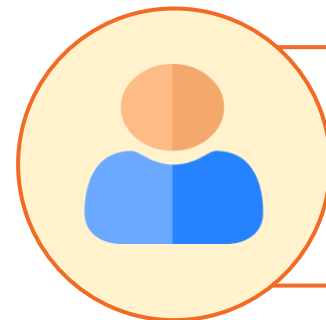
Contributors

Can manage everything except access
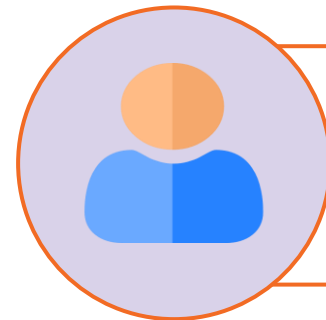
Readers

Can view everything but can't make changes

Caltech | Center for Technology & Management Education

Scope

Scope is where the access applies to.

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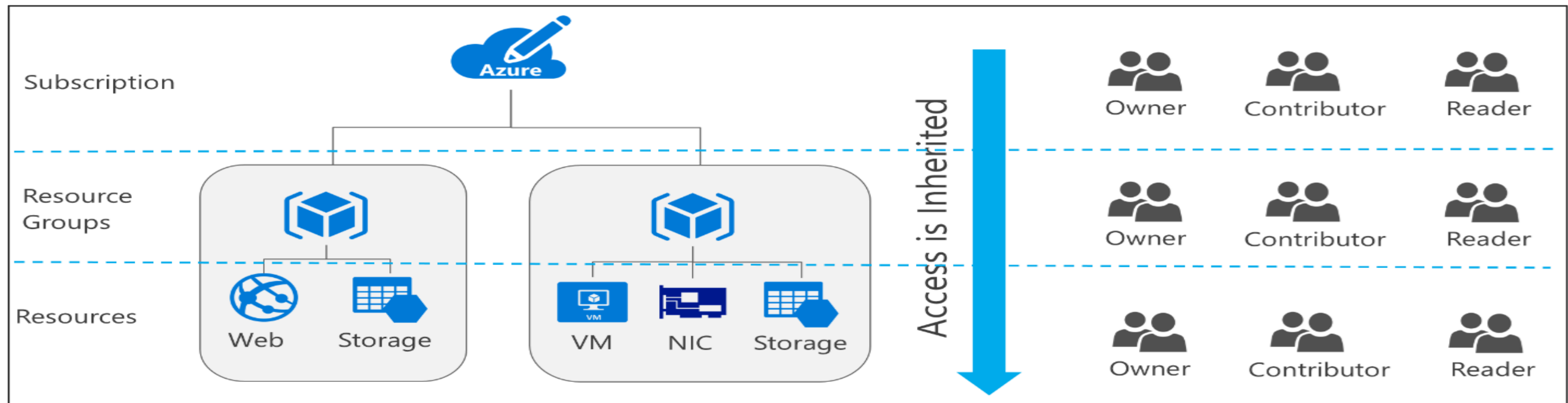
Role Assignment

A role assignment is created that associates a security principal to a role.
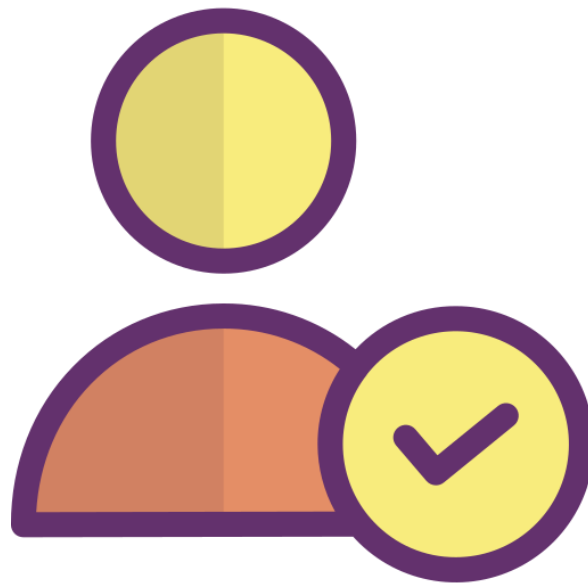
The security principal defines the access policy and permissions for the user/application in the Azure AD tenant.

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:

Identify and manage users assigned to administrative roles

Recognize which privilege positions should be deleted since they are underutilized or have excessive privileges

Azure PIM

Create rules to ensure that privileged roles are secured using multi-factor authentication

Create rules to ensure that privileged roles are only issued for as long as the privileged task requires
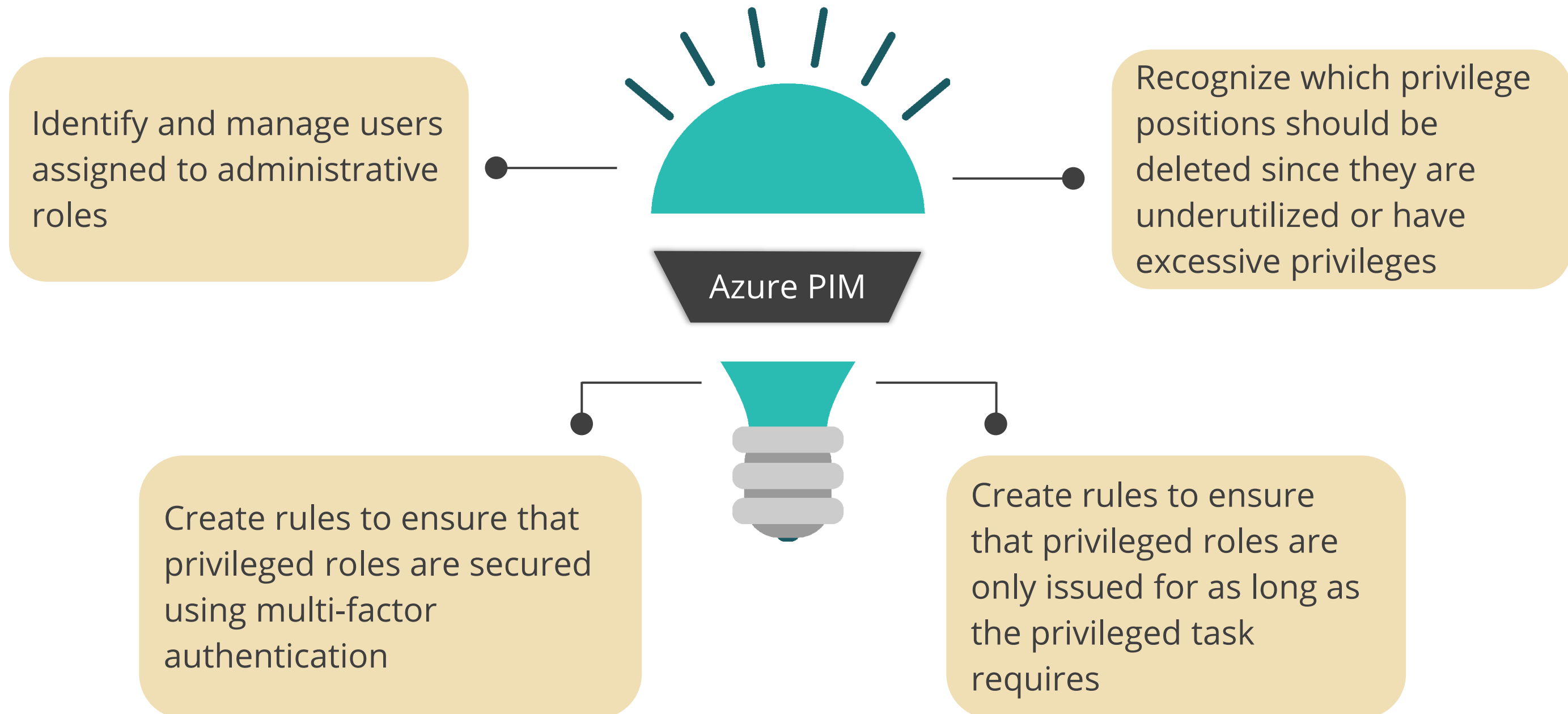
Azure Active Directory Identity Protection

Protection allows organizations to accomplish three key tasks:

Automate the detection and remediation of identity-based risks

Investigate risks using data presented in the Azure portal

Export risk detection data to third-party utilities for further analysis

Caltech | Center for Technology & Management Education
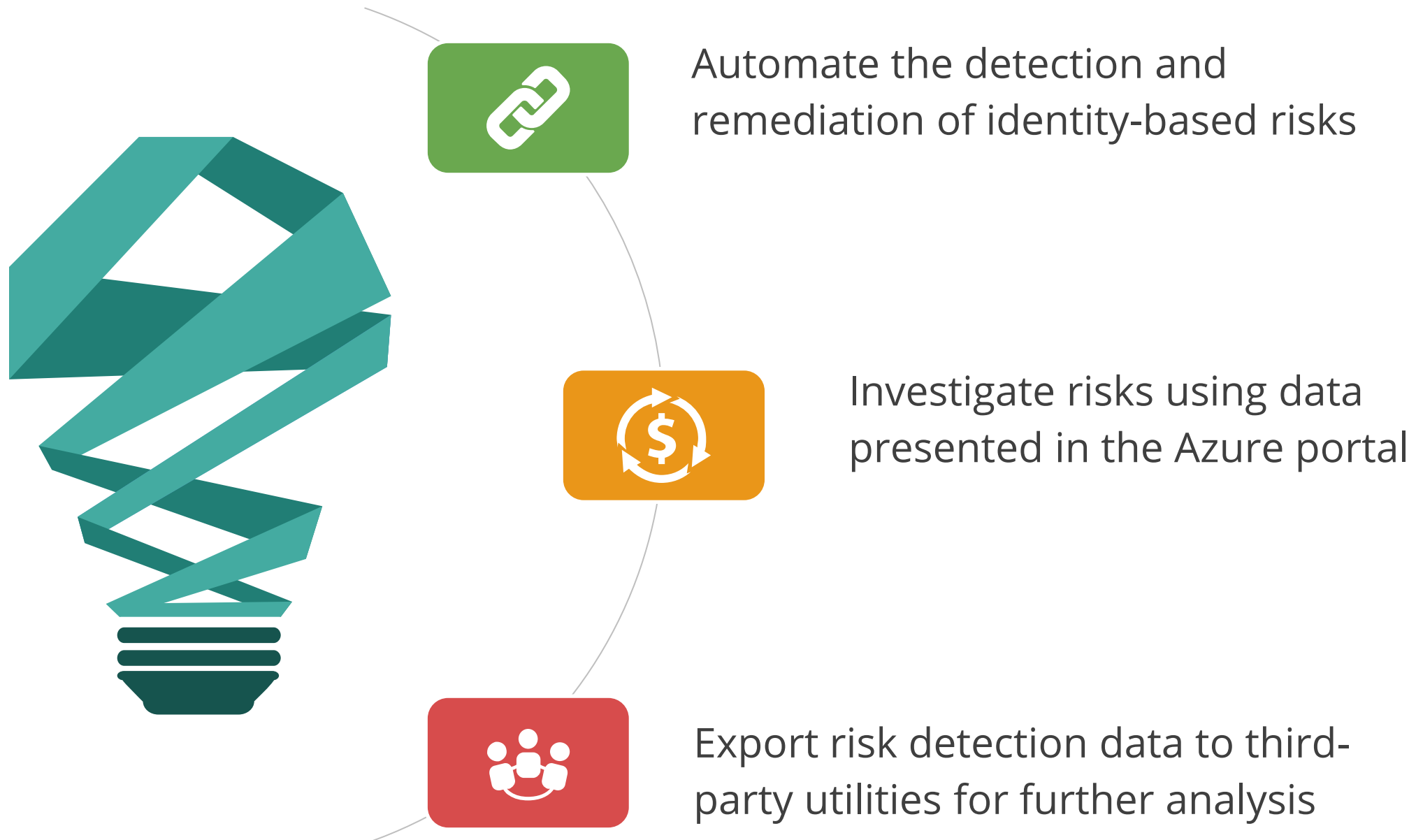
Azure Active Directory Identity Protection

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.

Risky users

01

Risky sign-ins

02

Risk detections

03

There are three key reports that administrators use for investigations in identity protection

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

Caltech | Center for Technology & Management Education

Assisted Practice

Azure RBAC

Duration: 10 Min.

Problem Statement:

As an Azure Architect, you've been asked to provide your company with an azure authorization solution that allows you to control who has access to Azure resources, what they can do with those resources, and what places they may access.

Assisted Practice: Guidelines

Steps to create Azure RBAC:

1. Sign in to the Azure portal as an administrator

2. Click the specific resource for that scope

3. Click Access control (IAM) and click on the Role assignments tab to view the role assignments at this scope

4. The Add role assignment pane opens

Caltech | Center for Technology & Management Education

Assisted Practice

Azure AD PIM   **Duration: 10 Min.**

Problem Statement:

As an Azure Architect, you've been asked to provide your company with an azure authorization solution that allows you to manage, regulate, and monitor access to critical resources in your company, such as Azure AD, Azure, and other Microsoft Online Services like Microsoft 365 or Microsoft Intune.

Assisted Practice: Guidelines
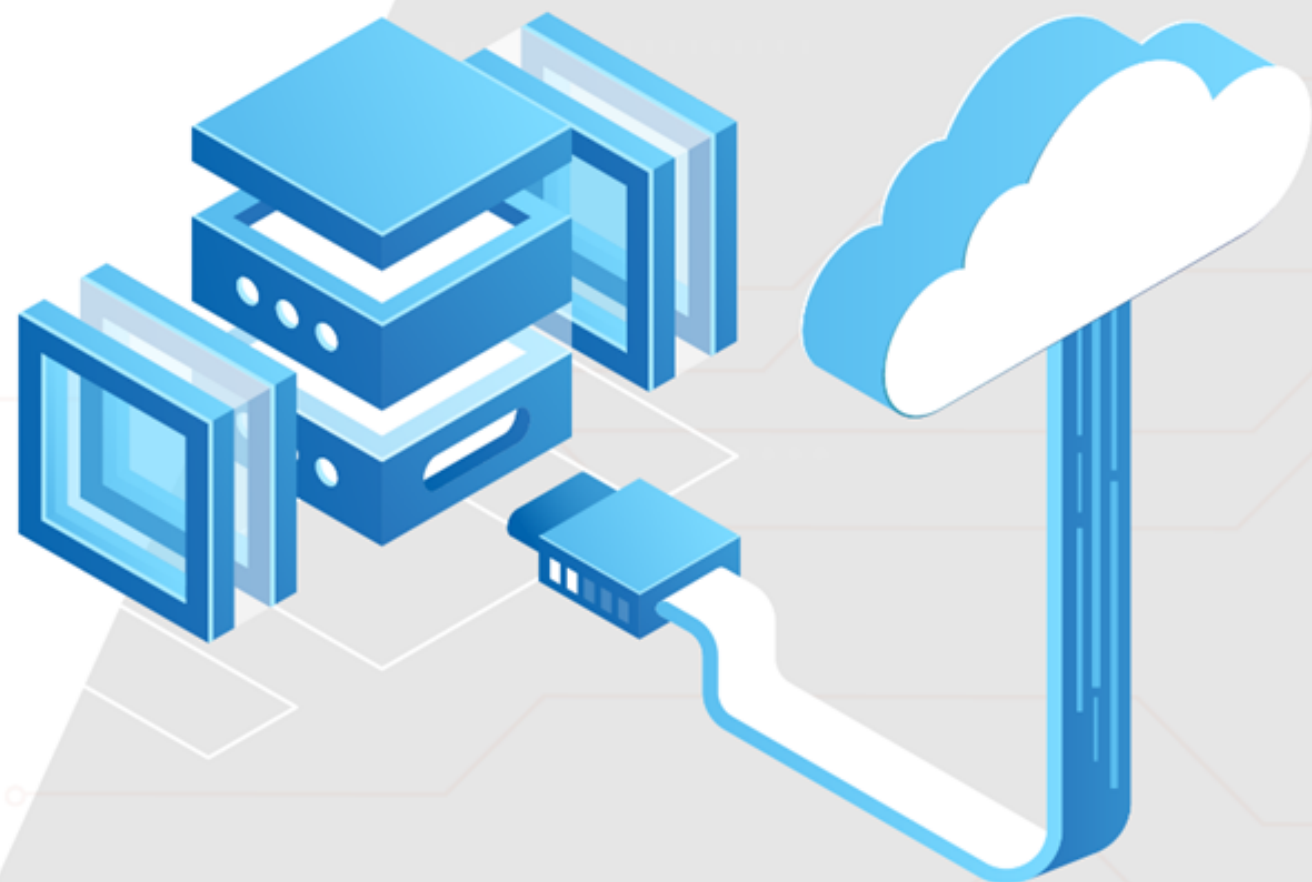
Steps to discover the resources:

1. Login to your Azure portal

2. Search for Azure AD Privileged Identity Management and select it

3. In the Privileged Identity Management pane, select Azure Resources

4. Select Discover Resources to launch the discovery experience

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.

Thank you