Microsoft

Swiss Post Cybersecurity

Administer Governance and Compliance

Learning Objectives

- Describe the core architectural components of Azure
- Azure Policy Initiatives
- Secure your Azure resources with role-based access control (RBAC)
- Lab 02a - Manage Subscriptions and RBAC
- Lab 02b - Manage Governance via Azure Policy

Describe the core architectural components of Azure

Learning Objectives – Subscriptions and Azure RM

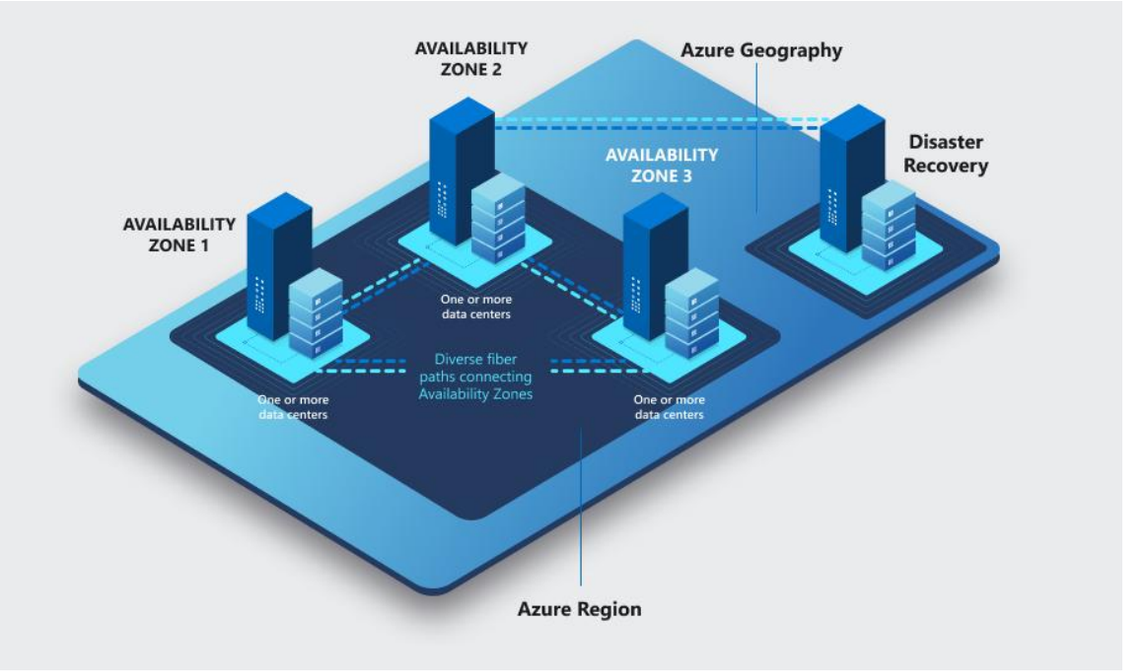
- Identify Regions
- Implement Azure Subscriptions
- Identify Subscription Usage
- Obtain a Subscription
- Create Resource Groups
- Determine Service Limits and Quotas
- Create an Azure Resource Hierarchy
- Apply Resource Tagging
- Manage Costs
- Learning Recap

Manage Azure identities and governance (20–25%): Manage subscriptions and governance

- Configure resource locks
- Apply and manage tags on resources
- Manage resource groups
- Manage subscriptions
- Manage costs by using alerts, budgets, and Azure Advisor recommendations
- Configure management groups

Identify Regions

- A region represents a collection of datacenters
- Provides flexibility and scale
- Preserves data residency
- Select regions close to your users
- Be aware of region deployment availability
- There are global services that are region independent
- Most regions are paired for high availability



Austria DC

Company News

28/07/2025

Microsoft will open datacenter region in Austria

[Microsoft will open datacenter region in Austria - Source EMEA]

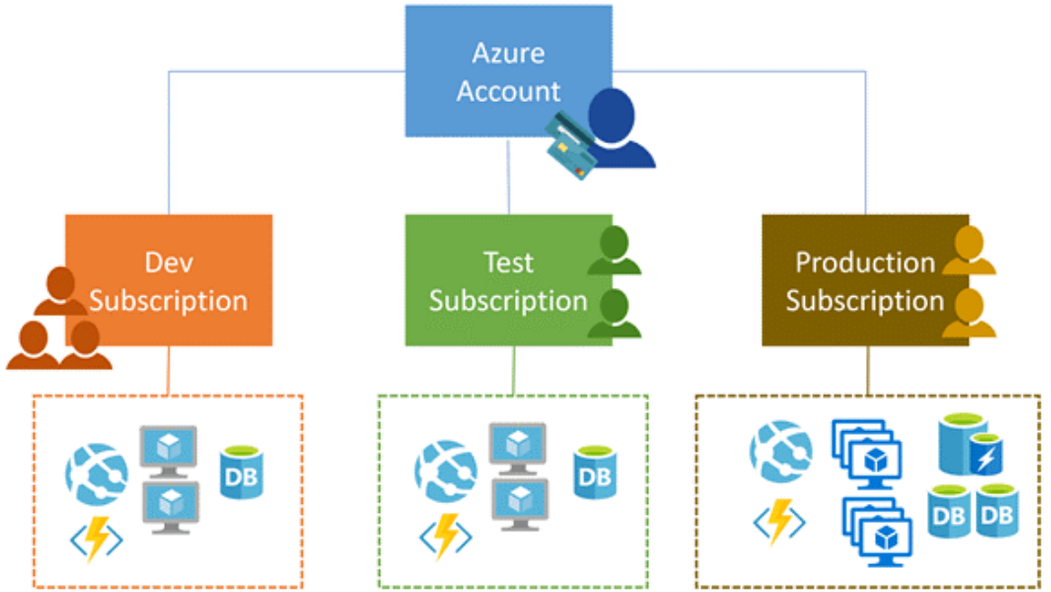
[List of Azure regions | Microsoft Learn]

Implement Azure Subscriptions

Only identities in Entra ID, or in a directory that is trusted by Entra ID, can create a subscription

Logical unit of Azure services that is linked to an Azure account

Security and billing boundary*



Identify Subscription Usage

Subscription	Usage
Free	Includes a $200 credit for the first 30 days, free limited access for 12 months
Pay-As-You-Go	Charges you monthly
CSP	Agreement with possible discounts through a Microsoft Cloud Solutions Provider Partner – typically for small to medium businesses
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

Obtain a Subscription

Enterprise Agreement customers make an upfront monetary commitment and consume services throughout the year

Resellers provide a simple, flexible way to purchase cloud services

Partners can design and implement your Azure cloud solution

Personal free account – Start right away

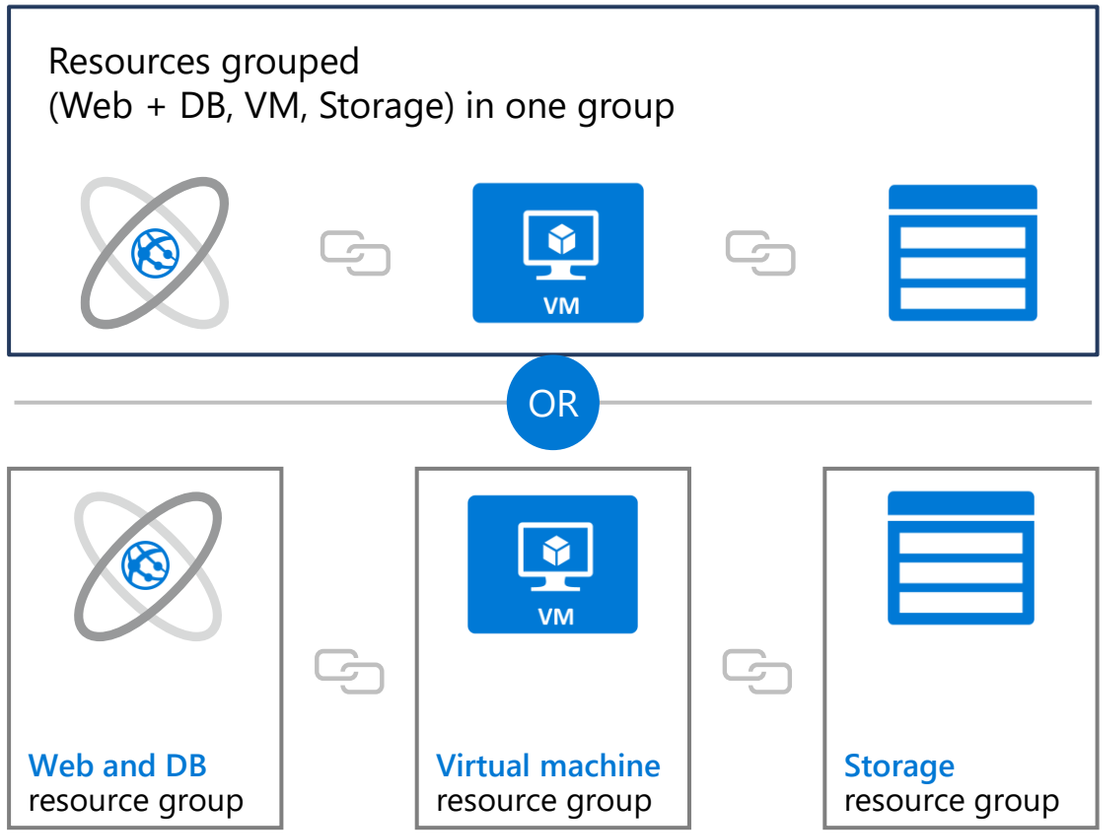
Create Resource Groups

Resources can only exist in one resource group

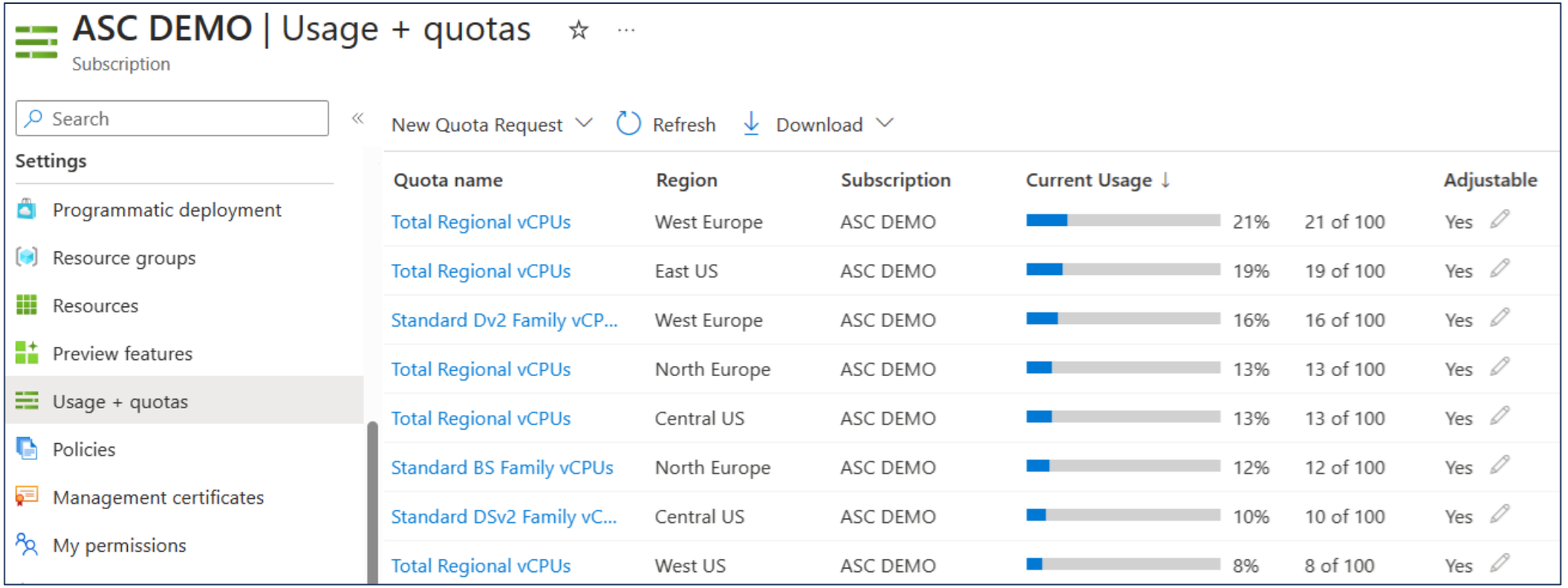
Groups can have resources of many different types (services) and from many different regions

Groups cannot be renamed or nested

You can move resources between groups



Determine Service Limits and Quotas



Resources have a default limit - a subscription quota

Helpful to track current usage, and plan for future use

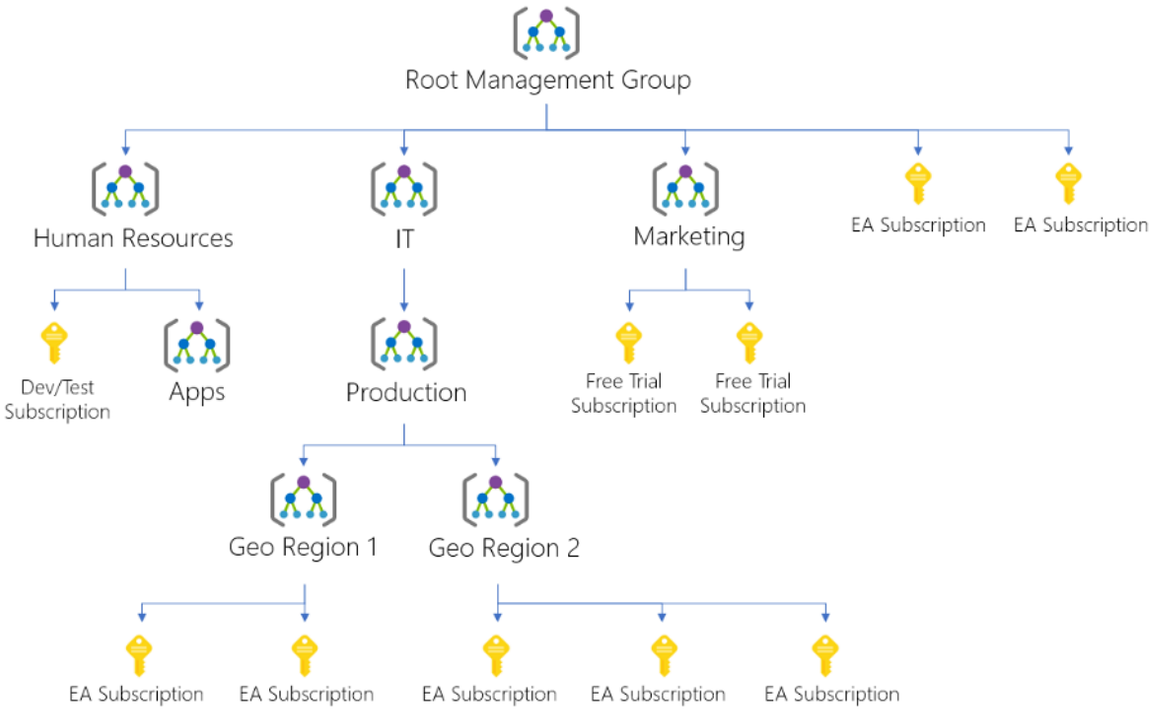
You can open a free support case to increase limits to published maximums

Create an Azure Resource Hierarchy

Management groups provides a level of scope above subscriptions

Target policies and spend budgets across subscriptions and inheritance down the hierarchies

Implement compliance and cost reporting by organization (business/teams)



* To prevent changes, apply resource locks at the subscription, resource group, or resources level

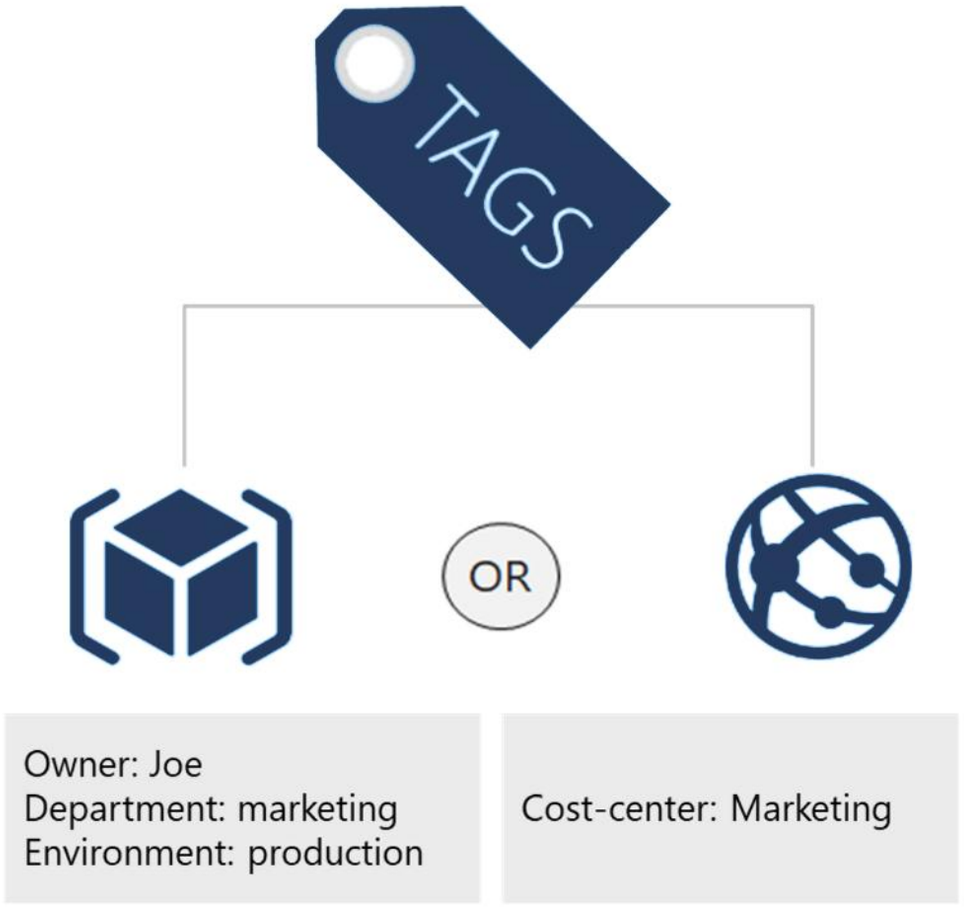
Apply Resource Tagging

Provides metadata for your Azure resources

Logically organizes resources

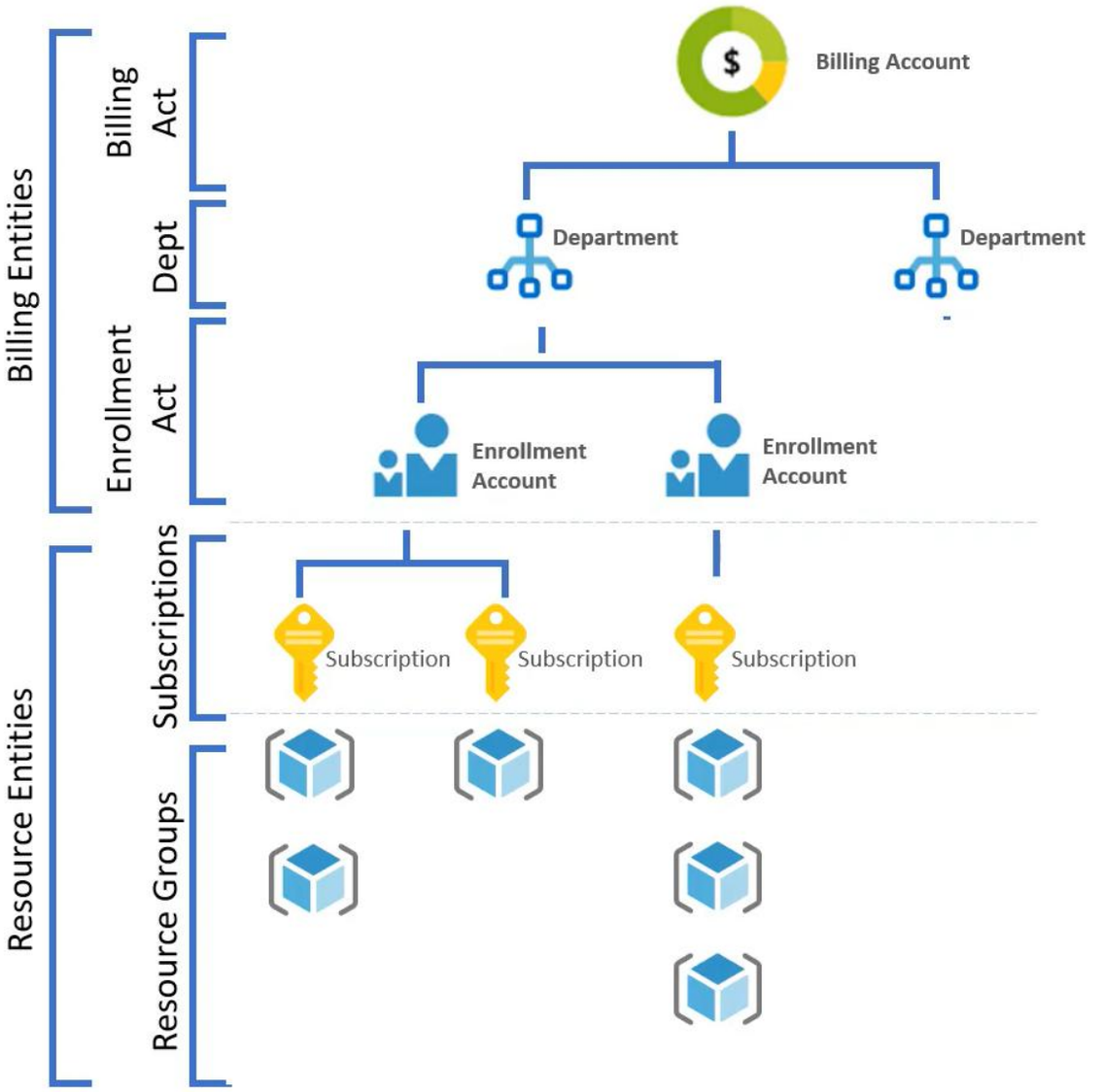
Consists of a name-value pair

Very useful for rolling up billing information

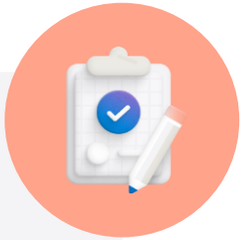


Manage Costs

- Costs are resource-specific
- Usage costs may vary between locations
- Costs for inbound and outbound data transfers differ
- Pre-pay with Azure reserved instances
- Use your on-premises licenses with Azure Hybrid Benefit
- Optimize with alerts, budgets, and Azure Advisor recommendations



Learning Recap - Describe core architectural components



Check your knowledge questions and additional study

Reference modules

- Describe the core architectural components of Azure
- Control and organize Azure resources with Azure Resource Manager

Azure Policy Initiatives

Learning Objectives – Azure Policy initiatives

- Implement Azure Policy
- Implement Azure Policies
- Create Azure Policies
- Demonstration – Azure Policy
- Learning Recap

Manage Azure identities and governance (20–25%): Manage subscriptions and governance

- Configure and manage Azure Policy

Implement Azure Policies

A service to create, assign, and manage policies

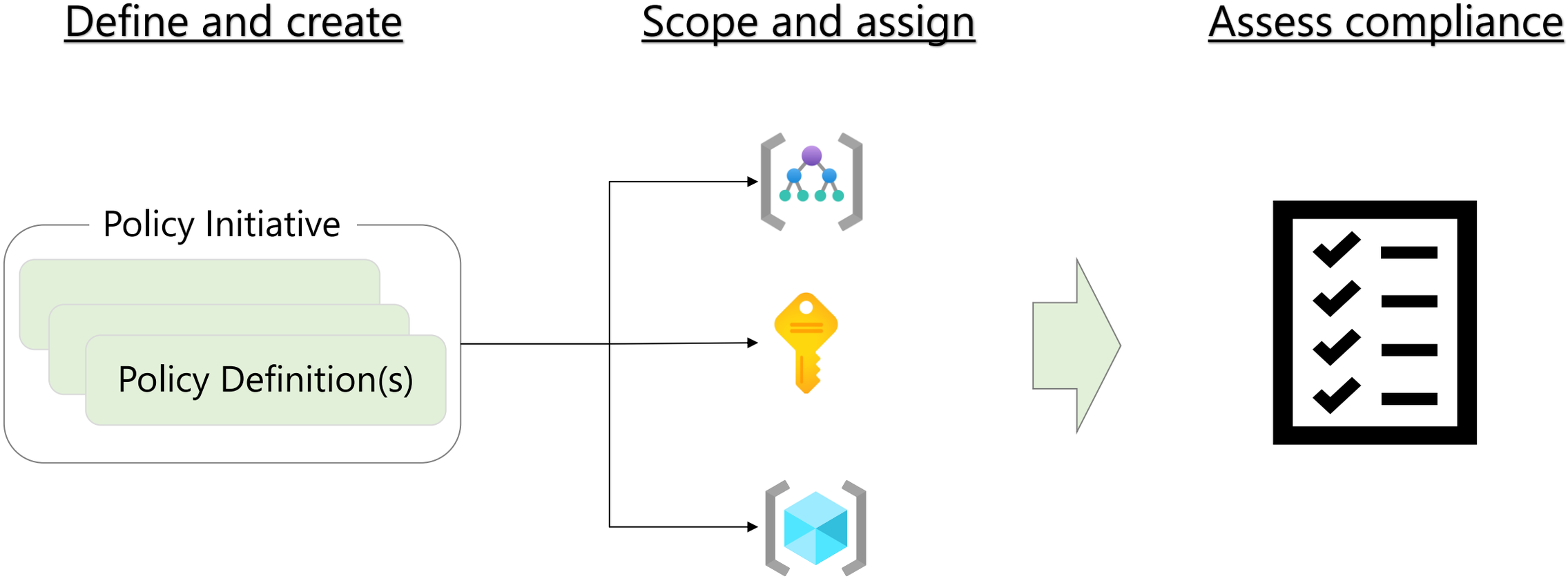
Runs evaluations and scans for non-compliant resources

Advantages:

- Enforcement and compliance
- Apply policies at scale
- Remediation

Usage Cases
Allowed resource types – Specify the resource types that your organization can deploy
Allowed virtual machine SKUs – Specify a set of virtual machine SKUs that your organization can deploy
Allowed locations – Restrict the locations your organization can specify when deploying resources
Require tag and its value – Enforces a required tag and its value
Azure Backup should be enabled for Virtual Machines – Audit if Azure Backup service is enabled for all Virtual machines

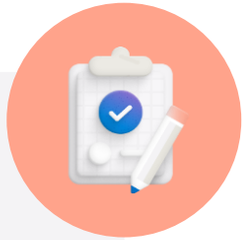
Create Azure Policies



Demonstration – Azure Policy

- Assign a policy
- Create and assign an initiative definition
- Check for compliance
- Check for remediation tasks
- Remove your policy and initiative

Learning Recap – Configure Azure Policy



Check your knowledge questions and additional study

Reference modules

- Introduction to Azure Policy
- Azure Policy initiatives
- Implement access management for Azure resources

Secure your Azure resources with Azure role-based access control (Azure RBAC)

Learning Objectives - RBAC

- Compare Azure RBAC Roles to Entra ID Roles
- Create a Role Definition
- Create a Role Assignment
- Apply RBAC Authentication
- Demonstration – Azure RBAC
- Learning Recap

Manage Azure identities and governance (20–25%): Manage access to Azure resources

- Manage built-in Azure roles
- Assign roles at different scopes
- Interpret access assignments

Compare Azure RBAC Roles to Entra ID Roles

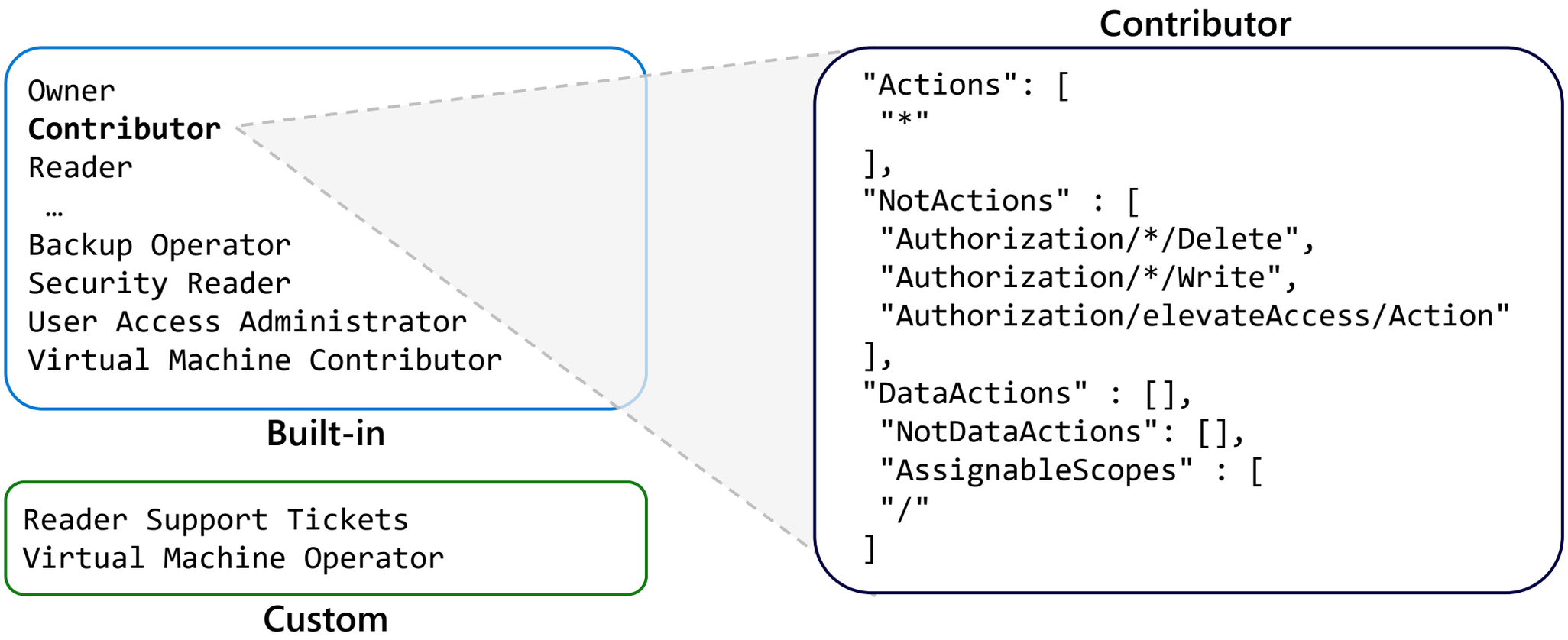
RBAC roles provide fine-grained access management

Azure RBAC roles	Entra ID roles
Manage access to Azure resources	Manage access to Entra ID objects
Scope can be specified at multiple levels	Scope is at the tenant level
Role information can be accessed in the Azure portal, Azure CLI, Azure PowerShell, Azure Resource Manager templates, REST API	Role information can be accessed in Azure portal, Microsoft 365 admin portal, Microsoft Graph PowerShell

There are many built-in roles, or you can create your own custom role

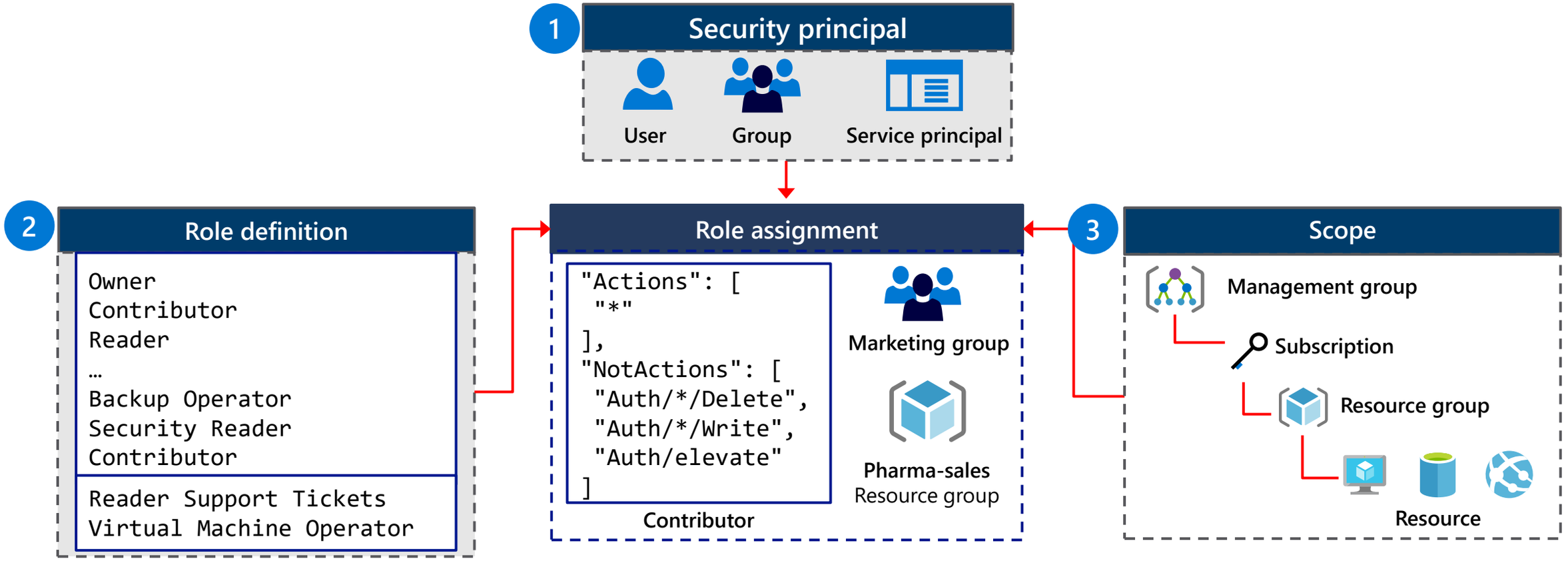
Create a Role Definition

Collection of permissions that lists the operations that can be performed

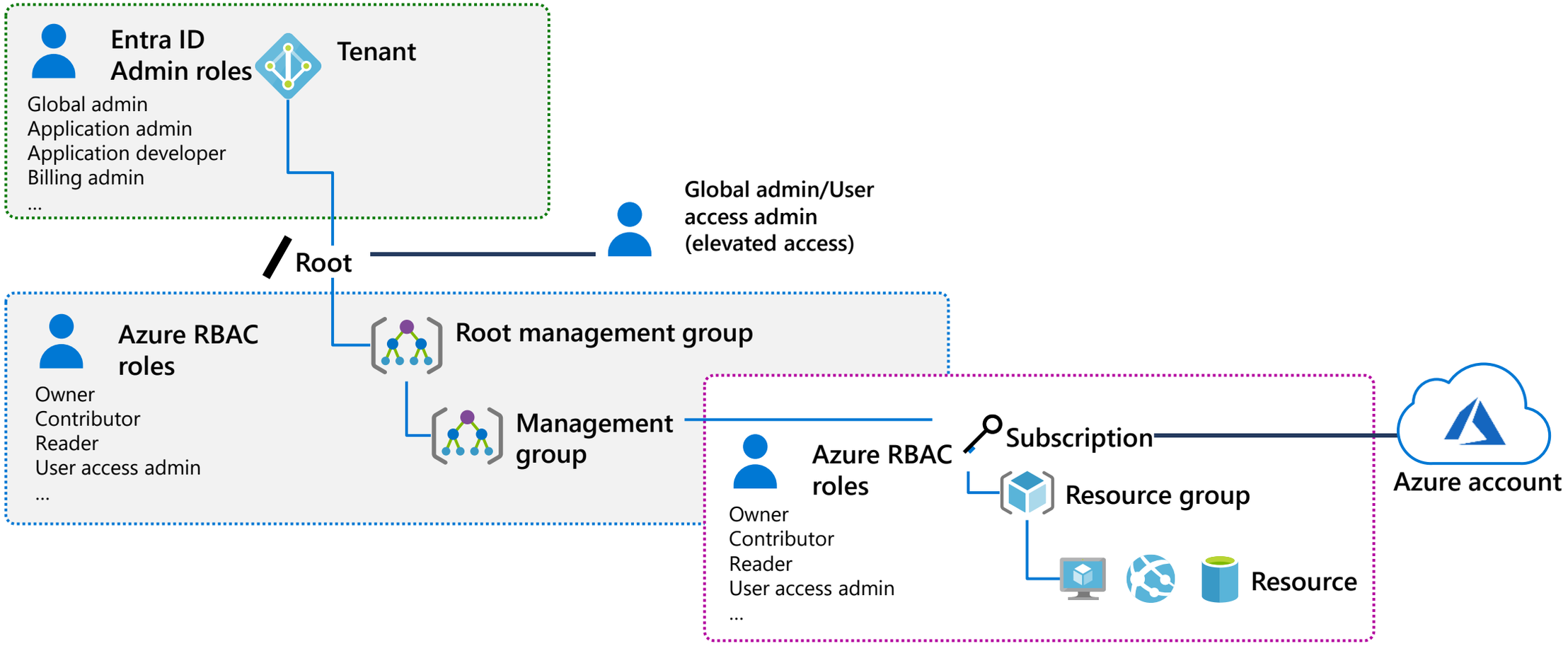


Create a Role Assignment

Process of binding a role definition to a user, group, or service principal at a scope for the purpose of granting access



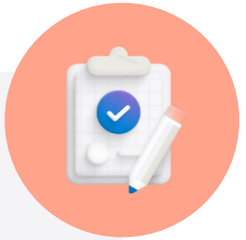
Apply RBAC Authentication



Demonstration – Azure RBAC

- Locate the Access Control blade
- Review role permissions
- Add a role assignment

Learning Recap– Secure resources with RBAC



Check your knowledge questions and additional study

Reference modules

- Secure your Azure resources with Azure role-based access control
- Create custom roles for Azure resources with Azure role-based access control

Lab 02a - Manage Subscriptions and RBAC
Lab 02b - Manage Governance via Azure Policy

Lab 02a – Manage Subscriptions and Azure RBAC

In this lab, you learn about role-based access control.

You learn how to use permissions and scopes to control what actions identities can and cannot perform.

You also learn how to make subscription management easier by using management groups.

Job Skills

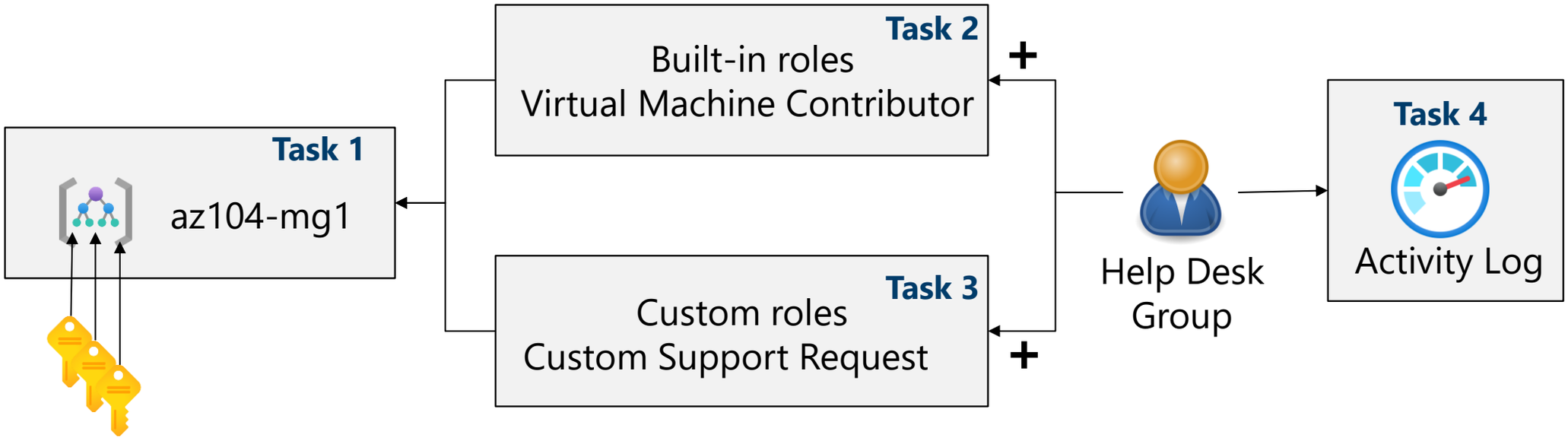
Task 1: Implement management groups.

Task 2: Review and assign a built-in Azure role.

Task 3: Create a custom RBAC role.

Task 4: Monitor role assignments with the Activity Log.

Lab 02a – Architecture diagram



Lab 02b – Manage Governance via Azure Policy

In this lab, you learn how to implement your organization's governance plans.

You learn how Azure policies can ensure operational decisions are enforced across the organization.

You learn how to use resource tagging to improve reporting.

Job Skills

Task 1: Create and assign tags via the Azure portal.

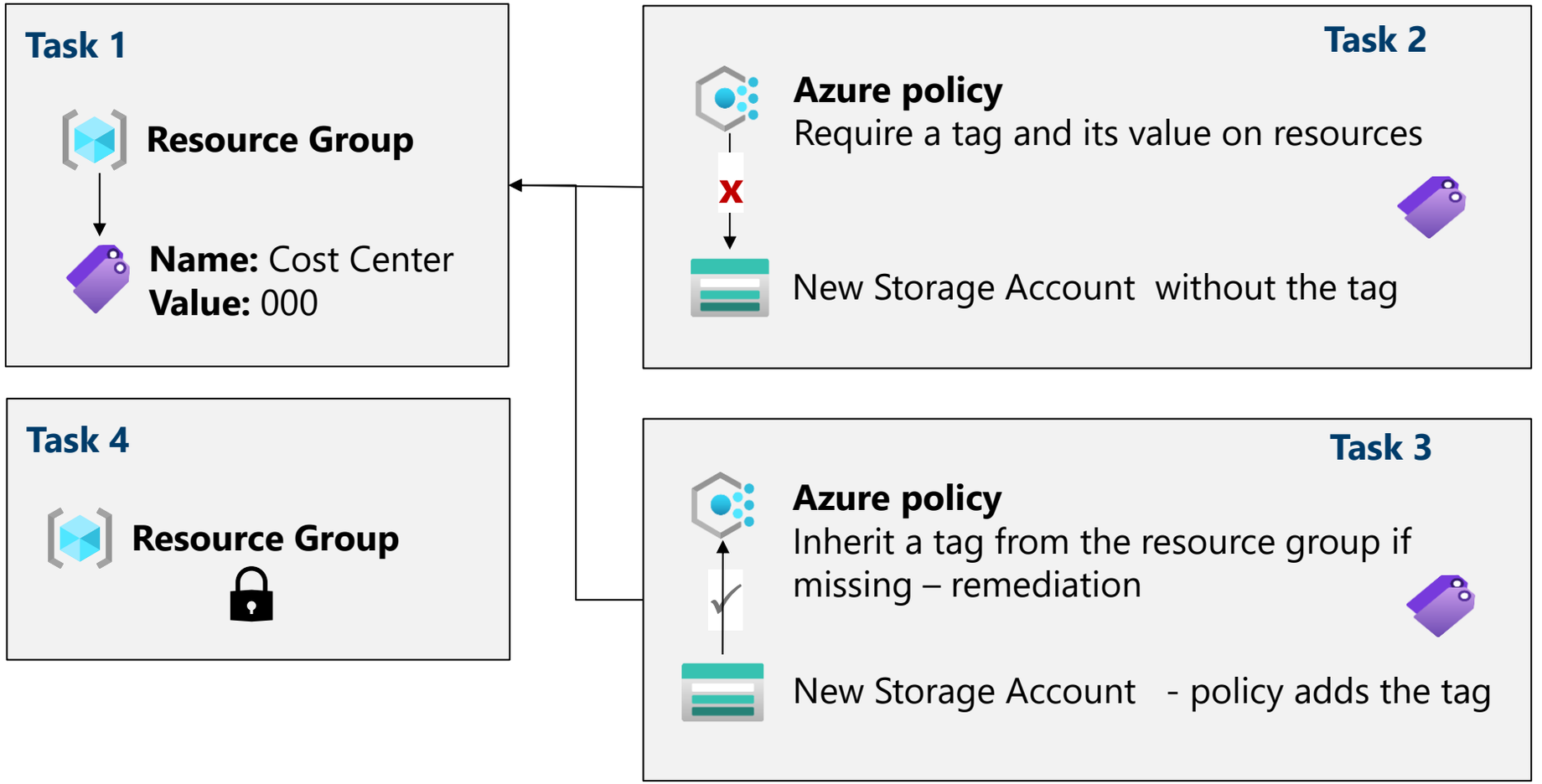
Task 2: Enforce tagging via an Azure Policy.

Task 3: Apply tagging via an Azure Policy.

Task 4: Configure and test resource locks.

Next slide for an architecture diagram

Lab 02b – Architecture diagram



Swiss Post
Cybersecurity

Questions?

Microsoft
Solutions Partner
Security

Specialist
Threat Protection