Microsoft Azure

# AZ-104T00A
# Module 02: Governance and Compliance

# Module Overview

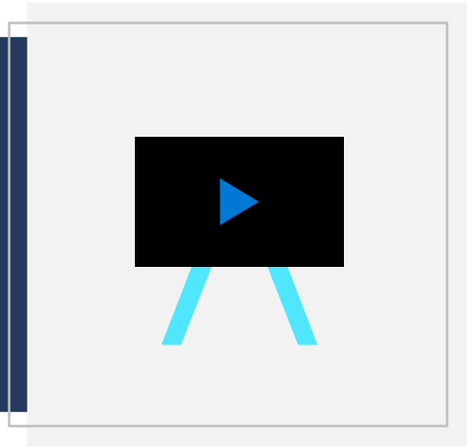
Lesson 01: Subscriptions and Accounts

Lesson 02: Azure Policy

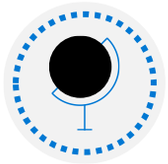
Lesson 03: Role-Based Access Control

Lesson 04: Module 02 Lab and Review

# Lesson 01: Subscriptions and Accounts

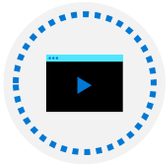


# Subscriptions and Accounts Overview



Regions

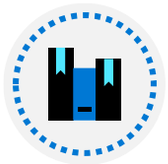
Azure Subscriptions



Getting a Subscription

Subscription Usage

Cost Management



Resource Tags

Cost Savings

# 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

Regions are paired for high availability

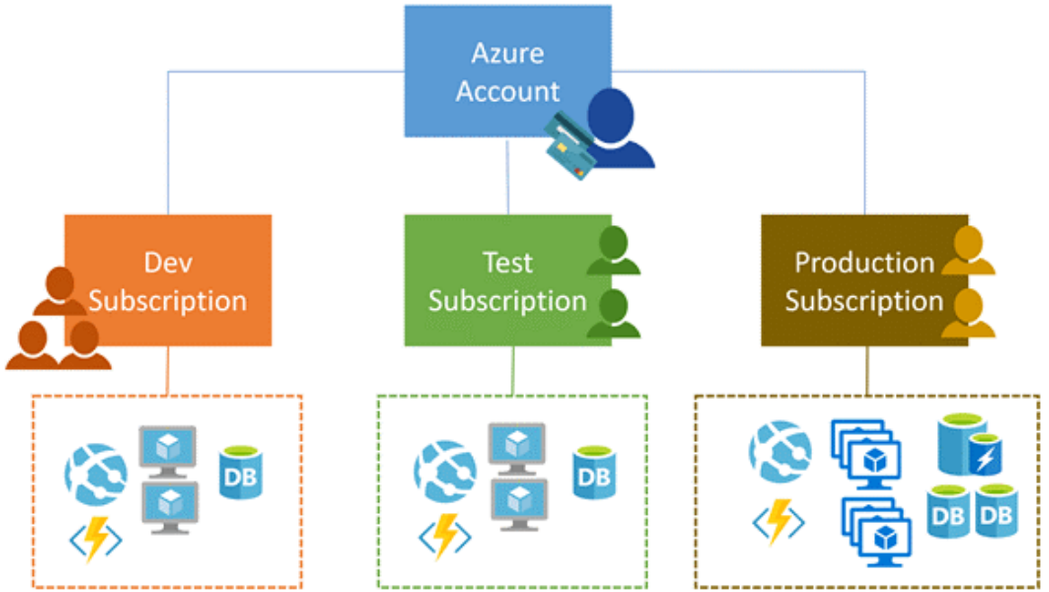

**Worldwide there are 60+ regions representing 140 countries**

# Azure Subscriptions

Only identities in Azure AD or in a directory that is trusted by Azure AD can create a subscription

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

Security and billing boundary



# Getting 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


# 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 |

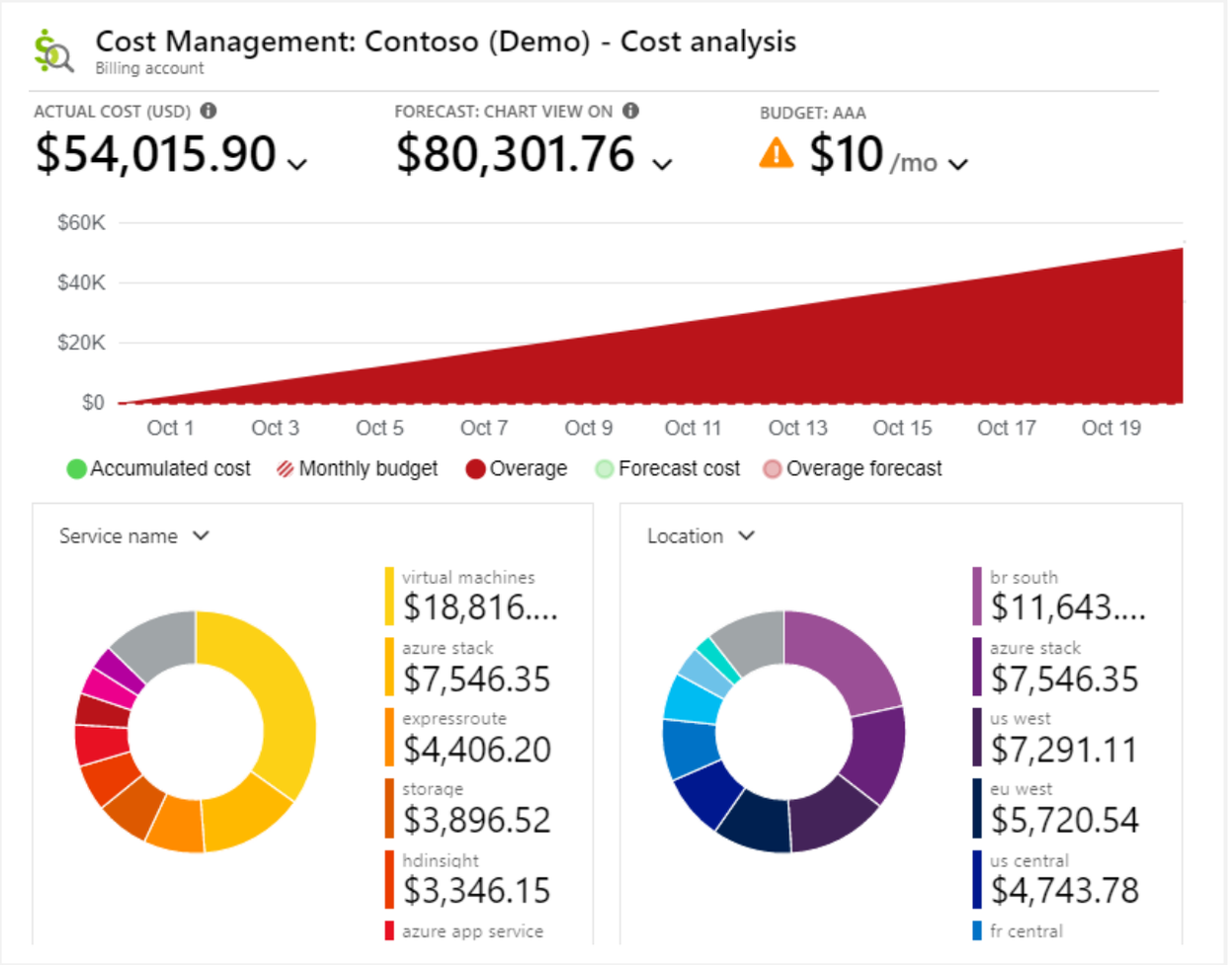
# Cost Management

Conduct cost analysis

Create a budget

Review recommendations

Export the data



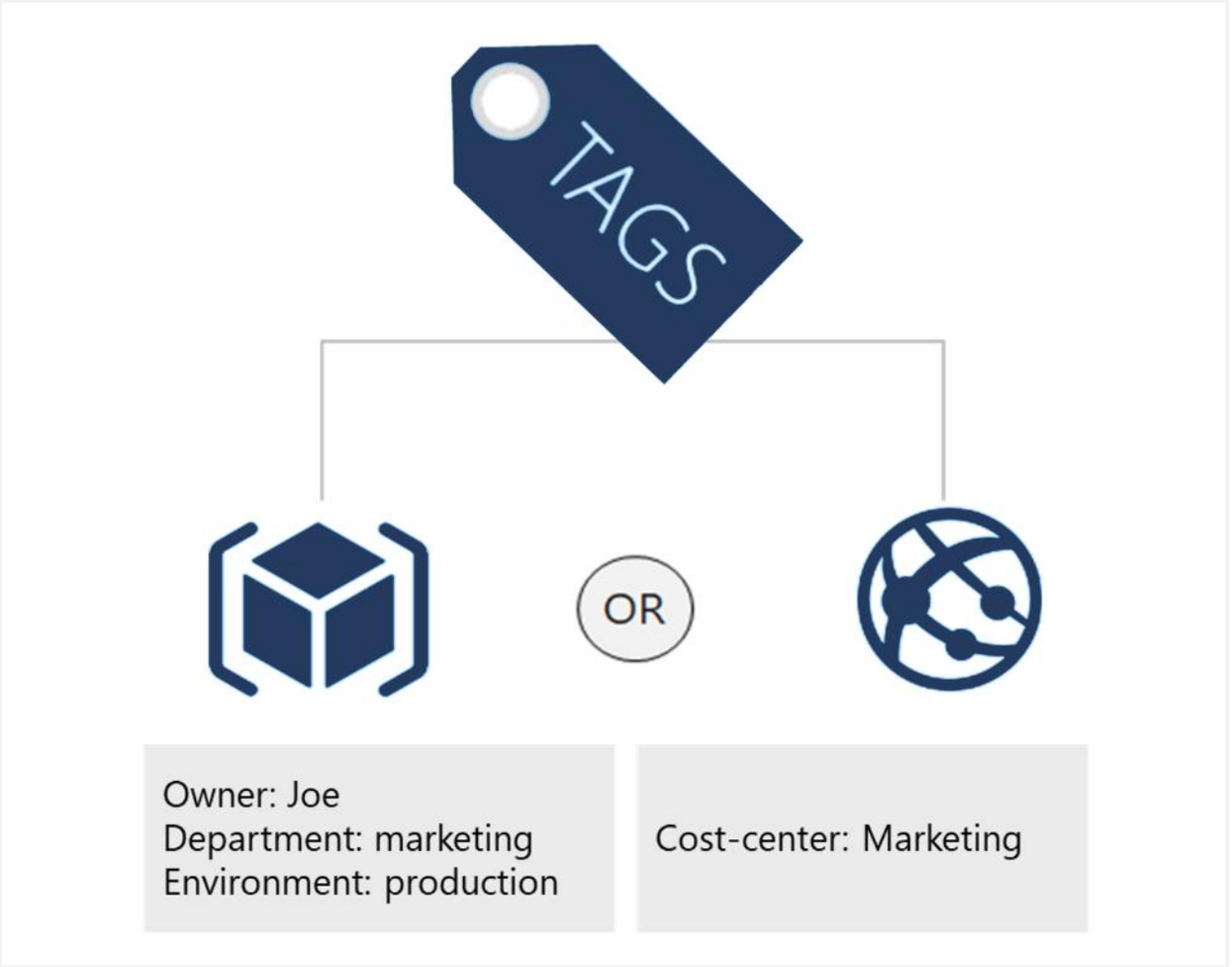
# Resource Tags

Provides metadata for your Azure resources

Logically organizes resources into a taxonomy

Consists of a name-value pair

Very useful for rolling up billing information



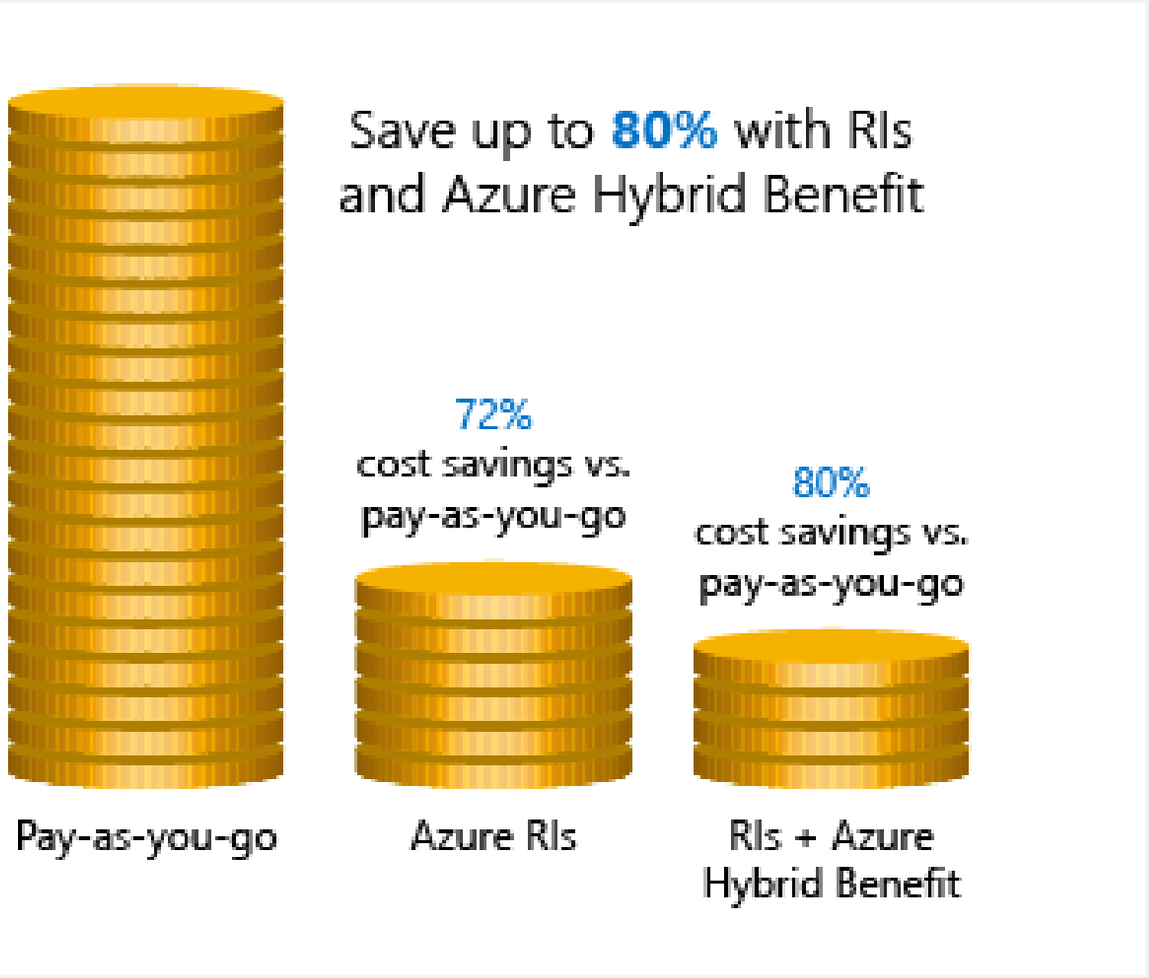
# Cost Savings

**Azure Reservations –** Helps you save money by pre-paying for services

**Azure Hybrid Benefits –** Use Windows Server and SQL Server on-premises licenses with Software Assurance

**Azure Credits –** Monthly credit benefit that allows you to experiment with, develop, and test new solutions on Azure

**Regions –** Choose low-cost locations and regions



# Lesson 02: Azure Policy

# Azure Policy Overview

Management Groups

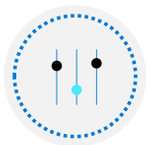
Azure Policy

Implementing Azure Policy

Policy Definitions

Create Initiative Definitions

Scope the Initiative Definition



Determine Compliance

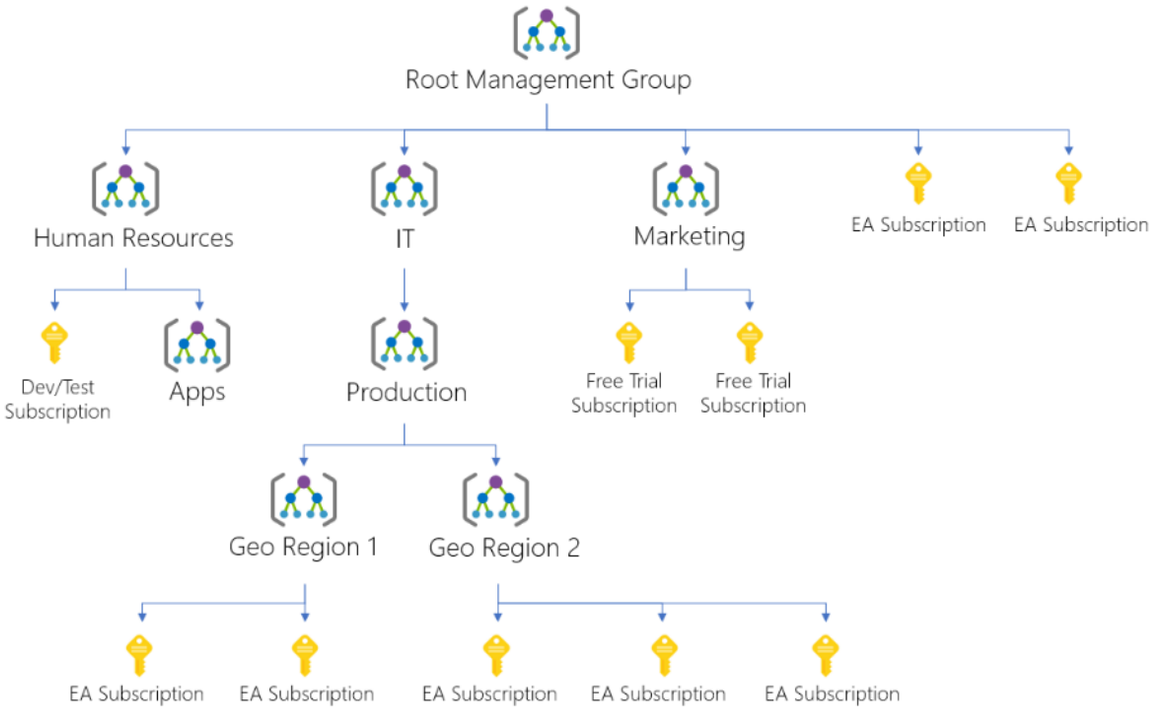
Demonstration – Azure Policy

# Management Groups

Provides a level of scope above subscriptions

Targeting of policies and spend budgets across subscriptions and inheritance down the hierarchies

Compliance and cost reporting by organization (business/teams)



# Azure Policy

Azure Policy is a service in Azure that you use to create, assign and, manage policies

Azure Policy runs evaluations and scans for non-compliant resources

**Advantages:**

Enforcement and compliance

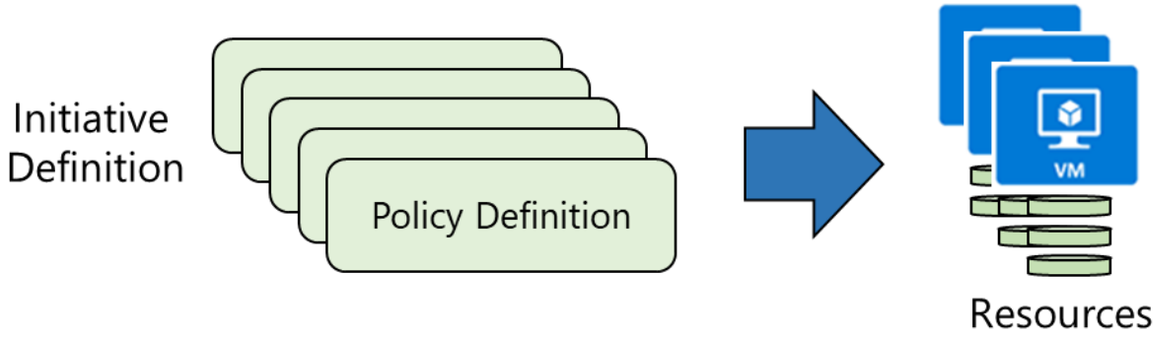
Apply policies at scale

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 |

# Implementing Azure Policy

1. Browse Policy Definitions
2. Create Initiative Definitions
3. Scope the Initiative Definition
4. View Policy evaluation results



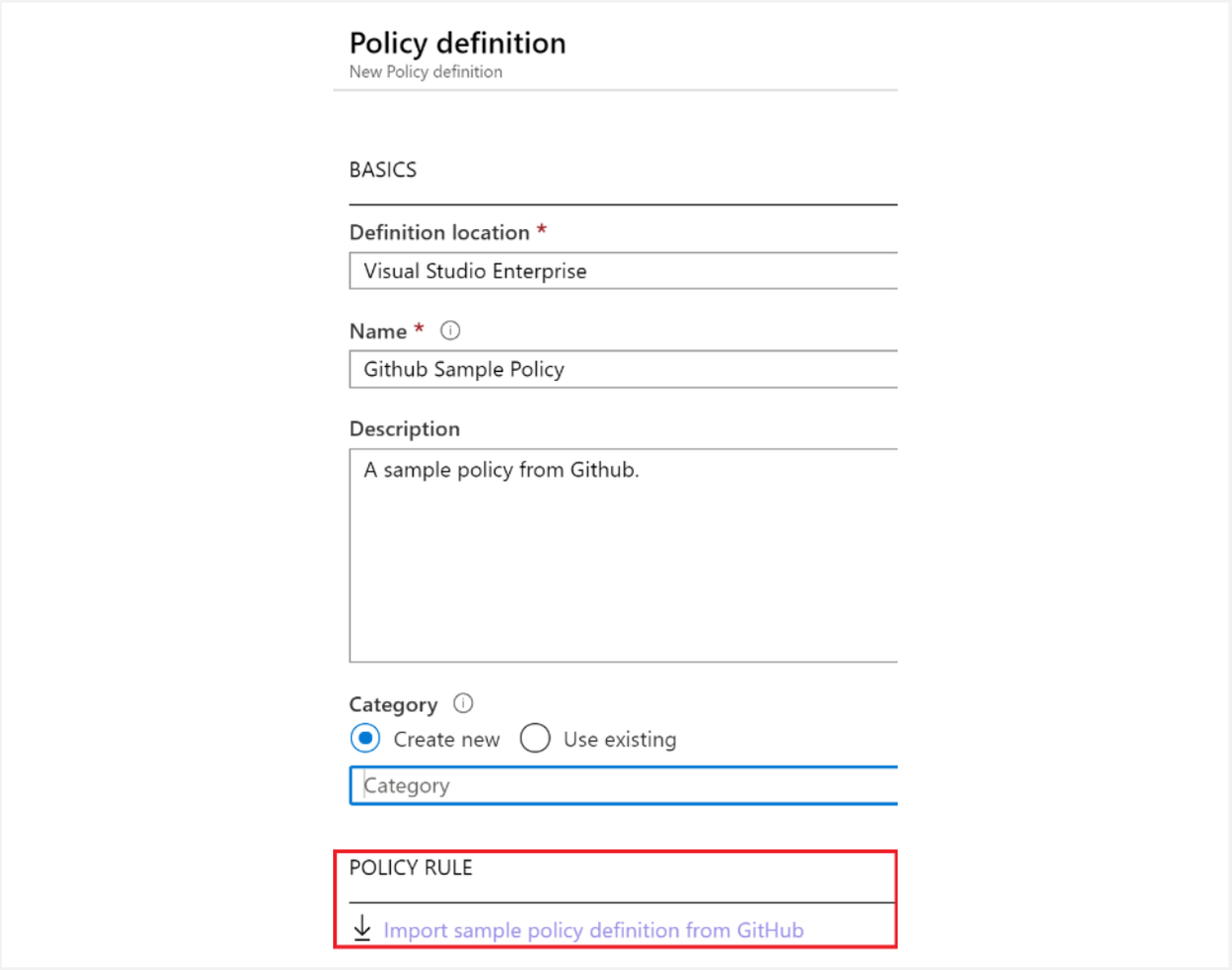
# Policy Definitions

Many policy definitions are available

You can import policies from GitHub

Policy Definitions have a specific JSON format

You can create custom policy definitions

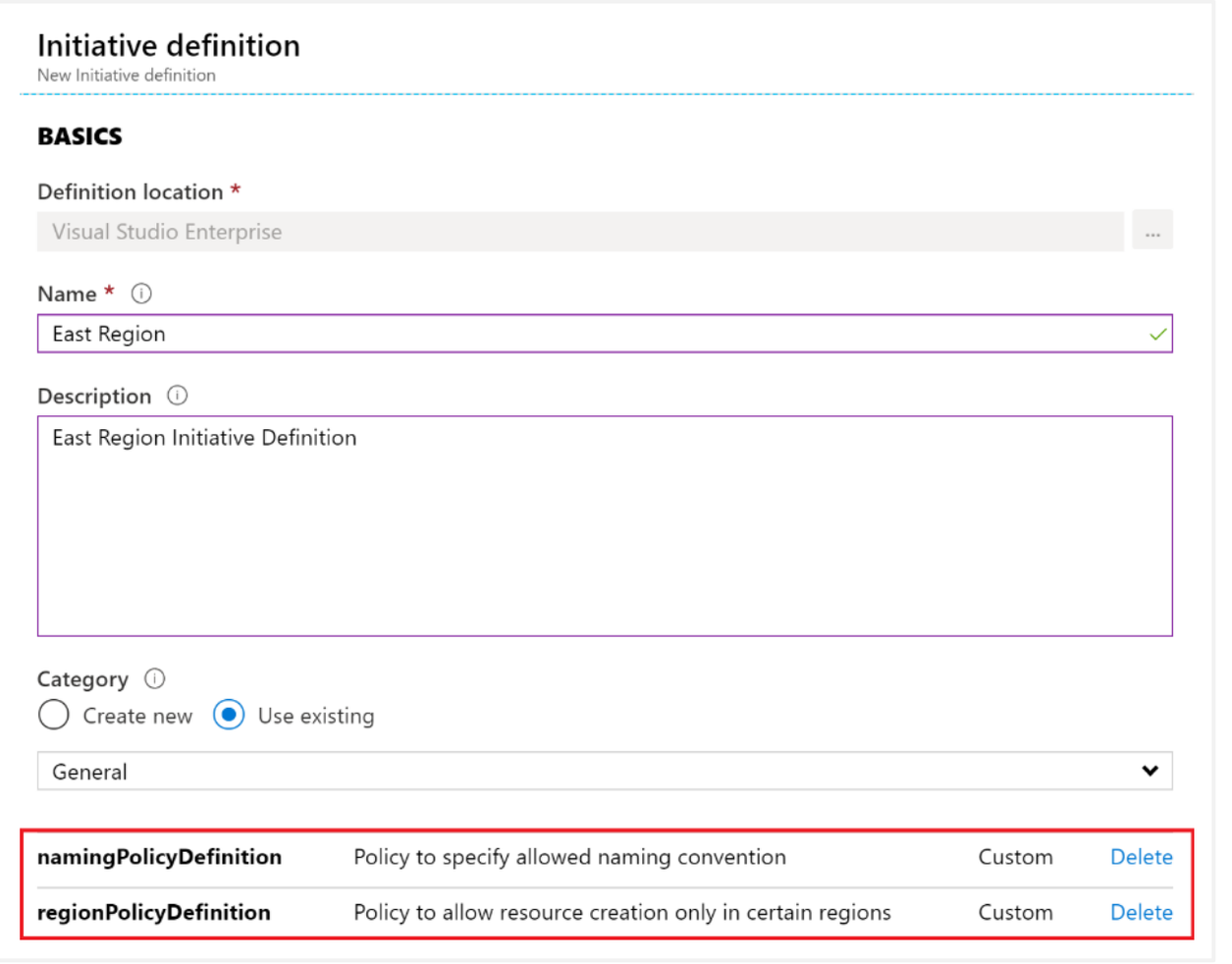


# Create Initiative Definitions

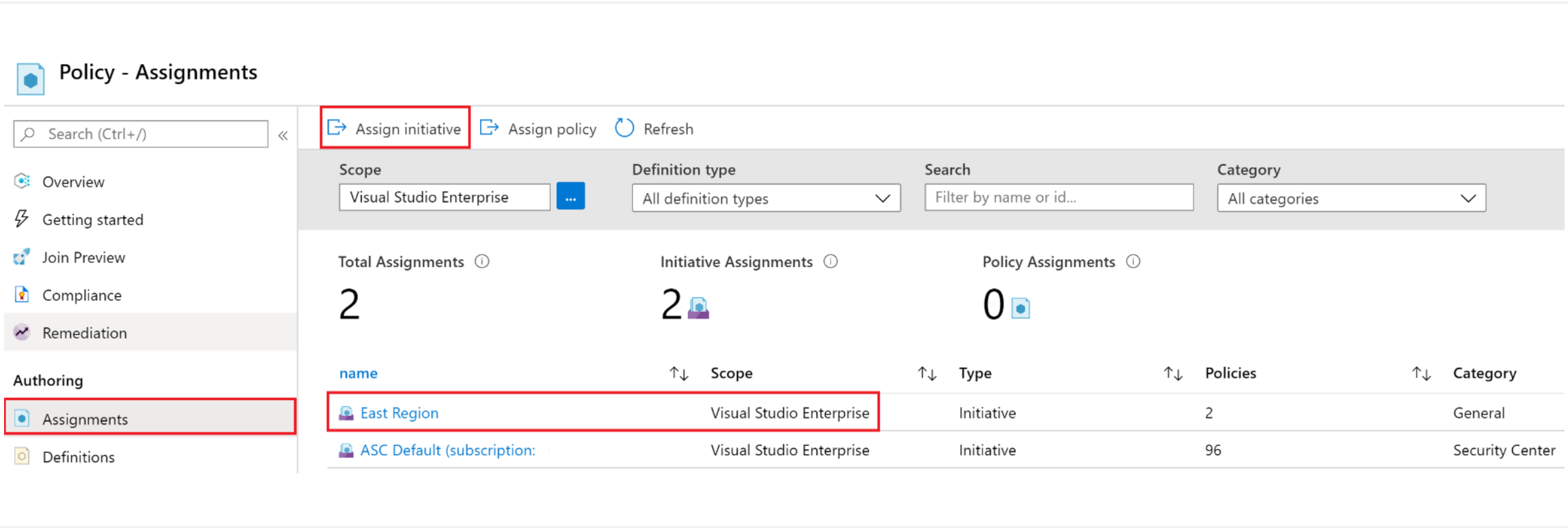
Group policy definitions

Include one or more policies

Requires planning



# Scope the Initiative Definition

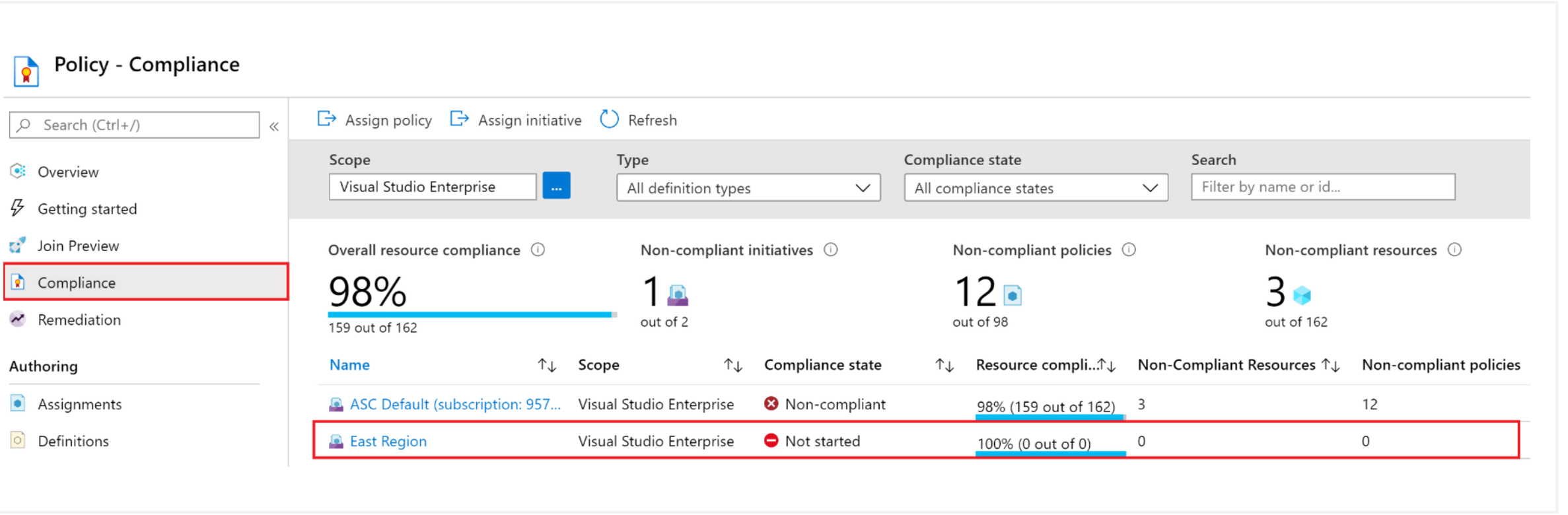



Assign the definition to a scope

The scope enforces the policy

Select the subscription, and optionally the resource group

# Determine Compliance




Non-compliant initiatives

Non-compliant policies

Non-compliant resources

# Lesson 03: Role-Based Access Control

# Role-Based Access Control Overview

Role-Based Access Control

Role Definition

Role Assignment

Azure RBAC Roles vs Azure AD Administrator Roles

RBAC Authentication

Azure RBAC Roles

Demonstration – RBAC Roles

# Role-Based Access Control

## Provides fine-grained access management of resources in Azure

Built on Azure Resource Manager

Segregate duties within your team

Grant only the amount of access to users that they need to perform their jobs

## Concepts

**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

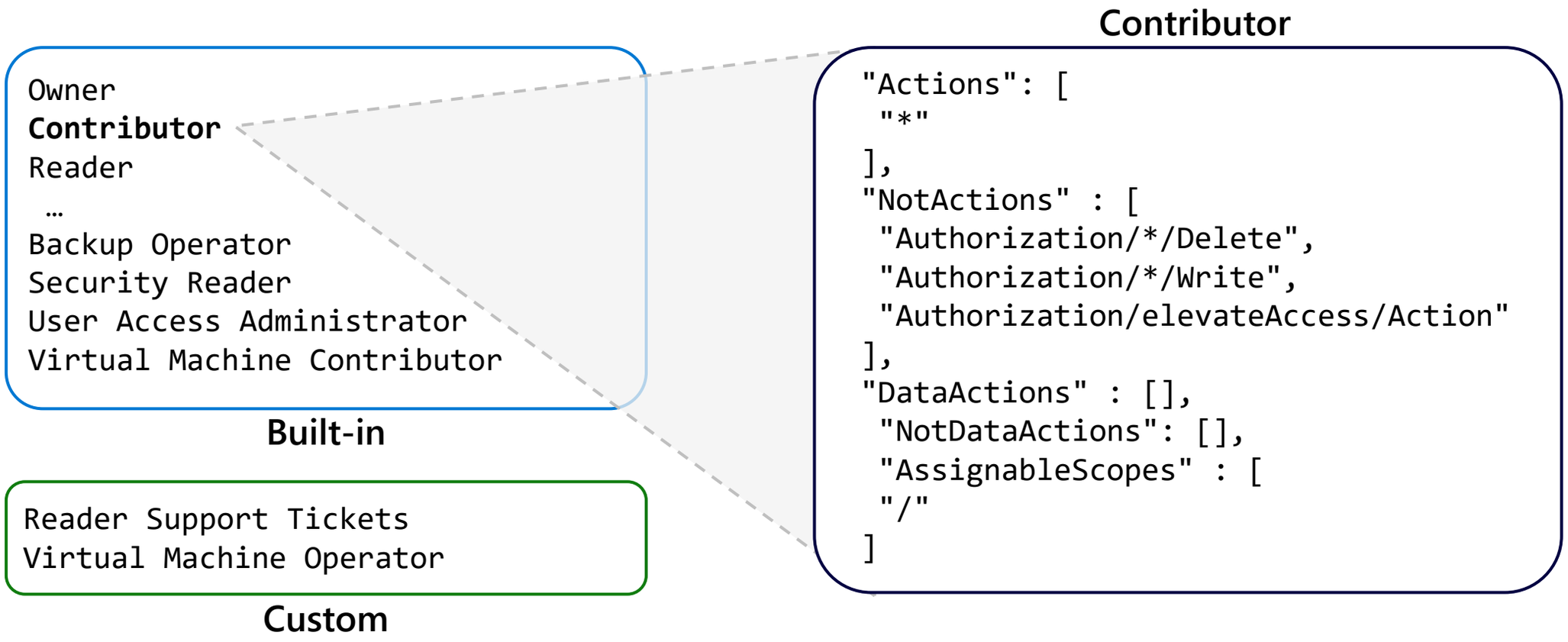
**Scope.** Boundary for the level of access that is requested

**Assignment.** Attaching a role definition to a security principal at a particular scope:

- Users can grant access described in a role definition by creating an assignment
- Deny assignments are currently read-only and are set by Azure Blueprints and Azure Managed Apps

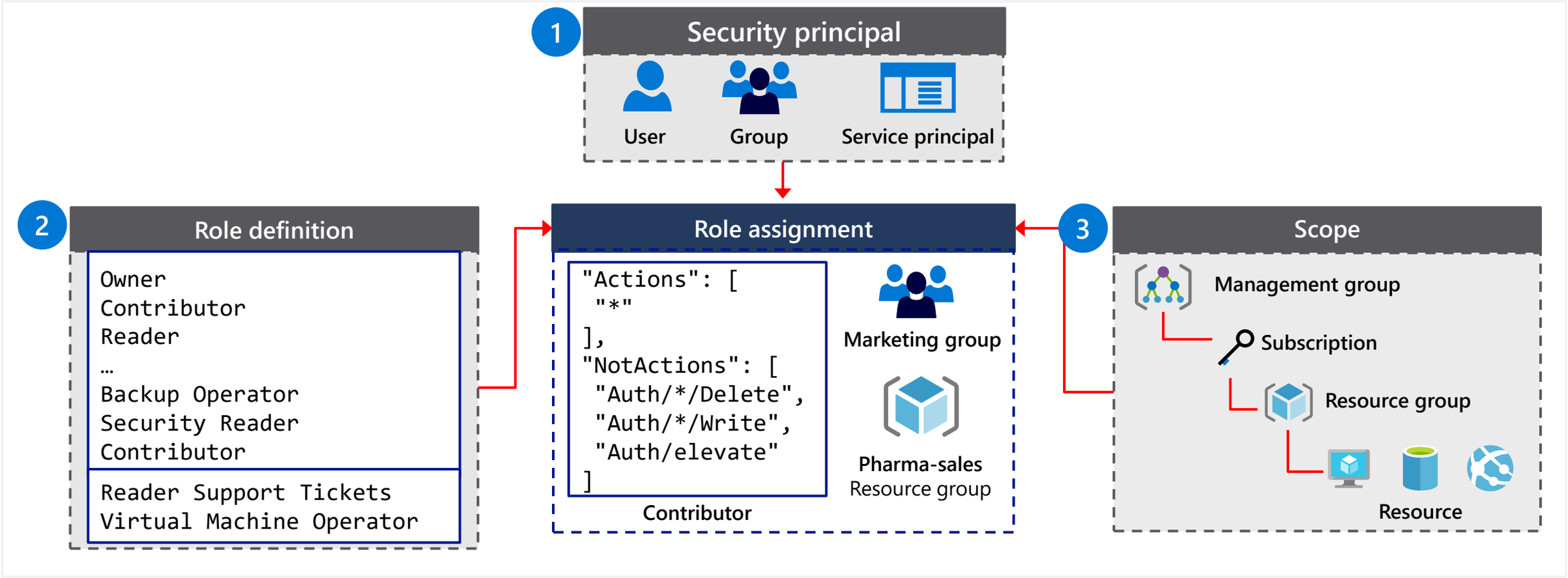
# Role Definition

## Collection of permissions that lists the operations that can be performed



# Role Assignment

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



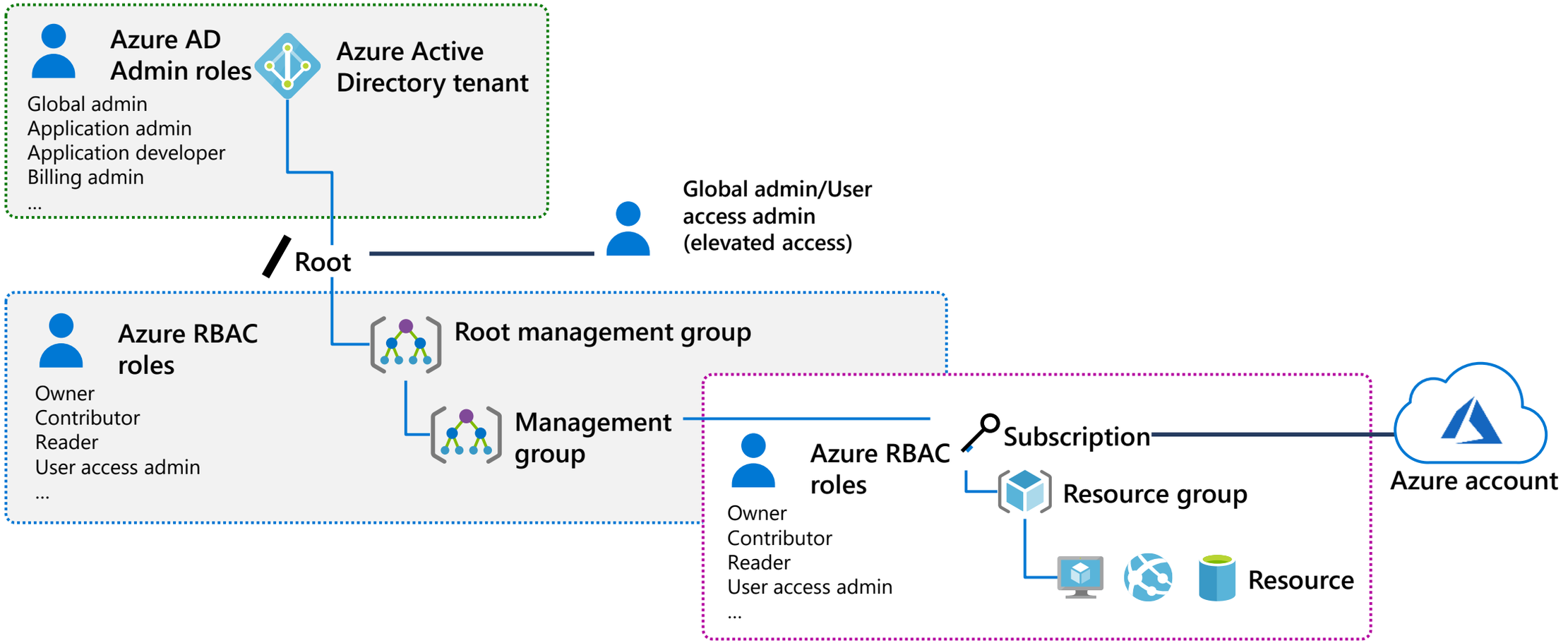
# Azure RBAC Roles vs. Azure AD Roles

## Azure and Azure AD offer two types of roles

| Azure RBAC roles | Azure AD roles |
| --- | --- |
| Manage access to Azure resources | Manage access to Azure AD 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, Azure Active Directory PowerShell for Graph |

**Classic administrator roles should be avoided if using Azure Resource Manager**

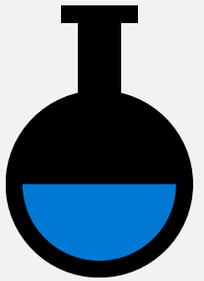
# RBAC Authentication



# Azure RBAC Roles

| RBAC role in Azure | Permissions | Notes |
|---|---|---|
| **Owner** | Has full access to all resources and can delegate access to others | The Service Administrator and Co-Administrators are assigned the Owner role at the subscription scope. This applies to all resource types |
| **Contributor** | Creates and manages all types of Azure resources but cannot grant access to others | This applies to all resource types |
| **Reader** | Views Azure resources | This applies to all resource types |
| **User Access Administrator** | Manages user access to Azure resources | This applies to managing access, rather than to managing resources |

# Lesson 04: Module 02 Lab and Review



# Lab 02a – Manage Subscriptions and Azure RBAC

## Lab scenario

To improve the management of Azure resources in Contoso, you have been tasked with implementing the following functionality:

- Using management groups for the Contoso's Azure subscriptions
- Granting user permissions for submitting support requests. This user would only be able to create support request tickets and view resource groups

## Objectives

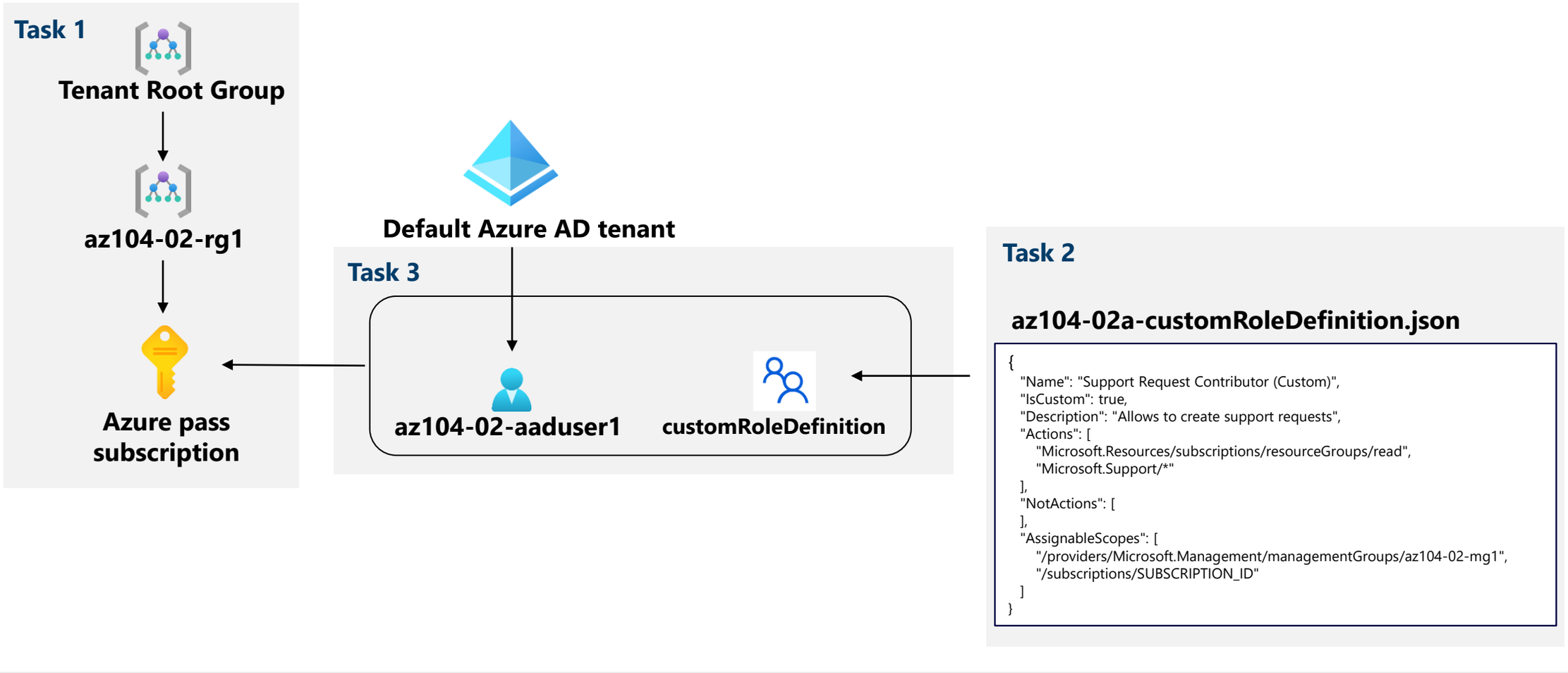
### Task 1:
Implement Management Groups

### Task 2:
Create custom RBAC roles

### Task 3:
Assign RBAC roles

Next slide for an architecture diagram

# Lab 02a – Architecture diagram



# Lab 02b – Manage Governance via Azure Policy

## Lab scenario

To improve management of Azure resources in Contoso, you have been tasked with implementing the following functionality:

- Tagging resource groups that include only infrastructure resources
- Ensuring that only properly tagged infrastructure resources can be added to infrastructure resource groups
- Remediating any non-compliant resources

## Objectives

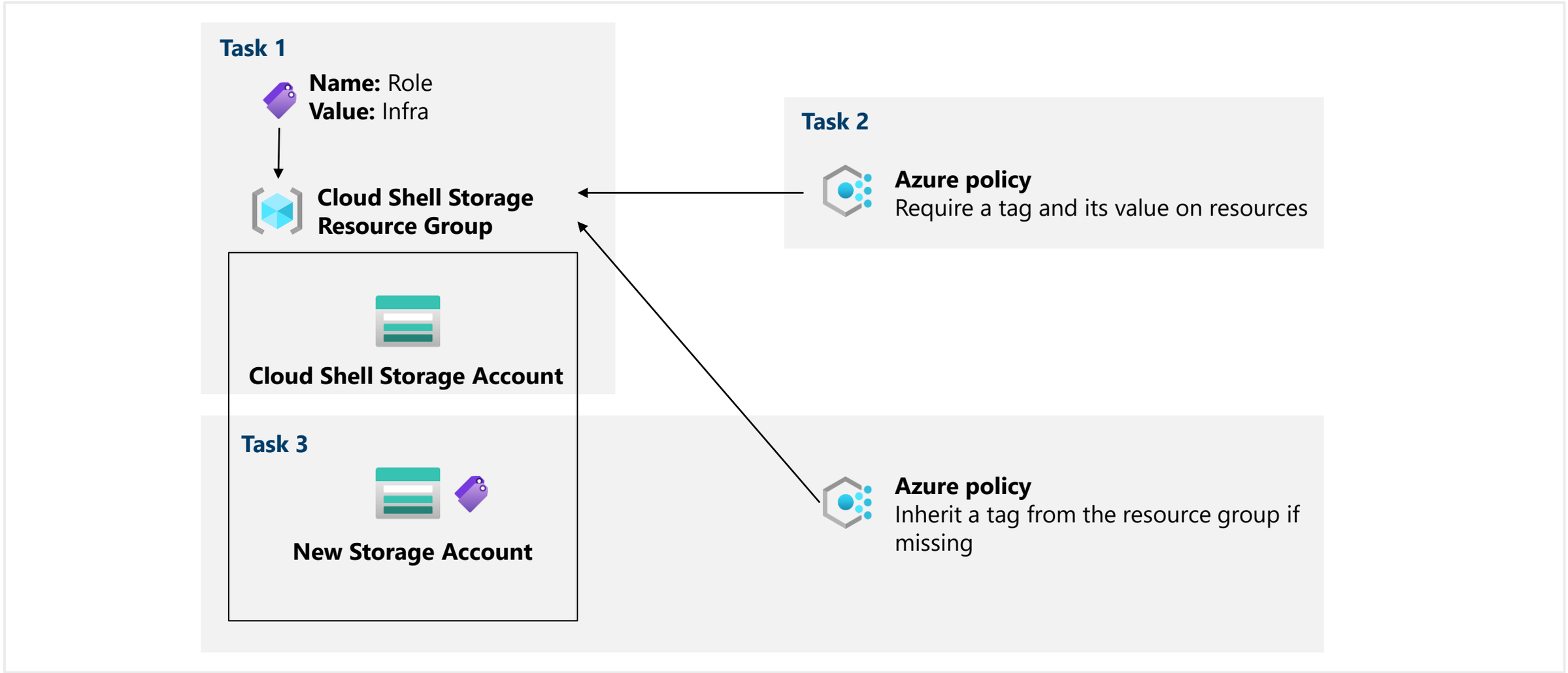
### Task 1:
Create and assign tags via the Azure portal

### Task 2:
Enforce tagging via an Azure Policy

### Task 3:
Apply tagging via an Azure Policy

Next slide for an architecture diagram

# Lab 02b – Architecture diagram



# Module Review

## Module Review Questions

## Microsoft Learn Modules (docs.microsoft.com/Learn)

Analyze costs and create budgets with Azure Cost Management

Predict costs and optimize spending for Azure

Control and organize Azure resources with Azure Resource Manager

Apply and monitor infrastructure standards with Azure Policy

Create custom roles for Azure resources with role-based access control (RBAC)

Manage access to an Azure subscription by using Azure role-based access control (RBAC)

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

# End of presentation