

AZ-104

Administer Governance and Compliance

LP
Learning Path



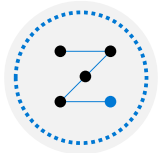
About this course: Course Outline



01: Administer Identity



Lab

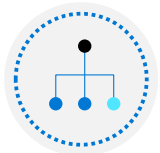


02: Administer Governance and Compliance

Lab



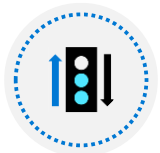
03: Administer Azure Resources



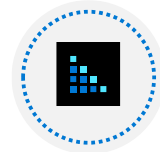
04: Administer Virtual Networking



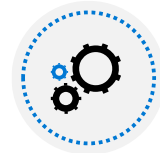
05: Administer Intersite Connectivity



06: Administer Network Traffic Management



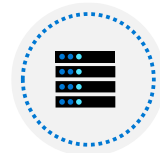
07: Administer Azure Storage



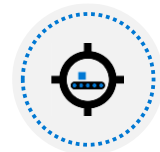
08: Administer Azure Virtual Machines



09: Administer PaaS Compute Options



10: Administer Data Protection

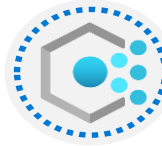


11: Administer Monitoring

Administer Governance and Compliance Introduction



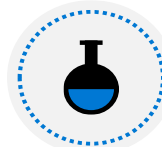
[Configure Subscriptions](#)



[Configure Azure Policy](#)



[Configure Role-Based Access Control](#) **RBAC**



[Lab 02a - Manage Subscriptions and RBAC](#)

[Lab 02b - Manage Governance via Azure Policy](#)

[Lab 03a – Manage Azure resources with the Azure portal](#)

Configure Subscriptions and Configure Azure Resource Manager Resources



Configure Subscriptions Introduction



Identify Regions



Implement Azure Subscriptions



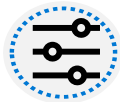
Identify Subscription Usage



Obtain a Subscription



Create Resource Groups



Determine Resource Limits



Create an Azure Resource Hierarchy



Apply Resource Tagging



Manage Costs



Summary and Resources

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

Regions are paired for high availability

(Northern Europe)

Peering

(Western Europe)

67

Avail zone

DC 1

DC 2

DC 3

##

Standalone VM

scale out

VM Scale Set

VM Avail Set



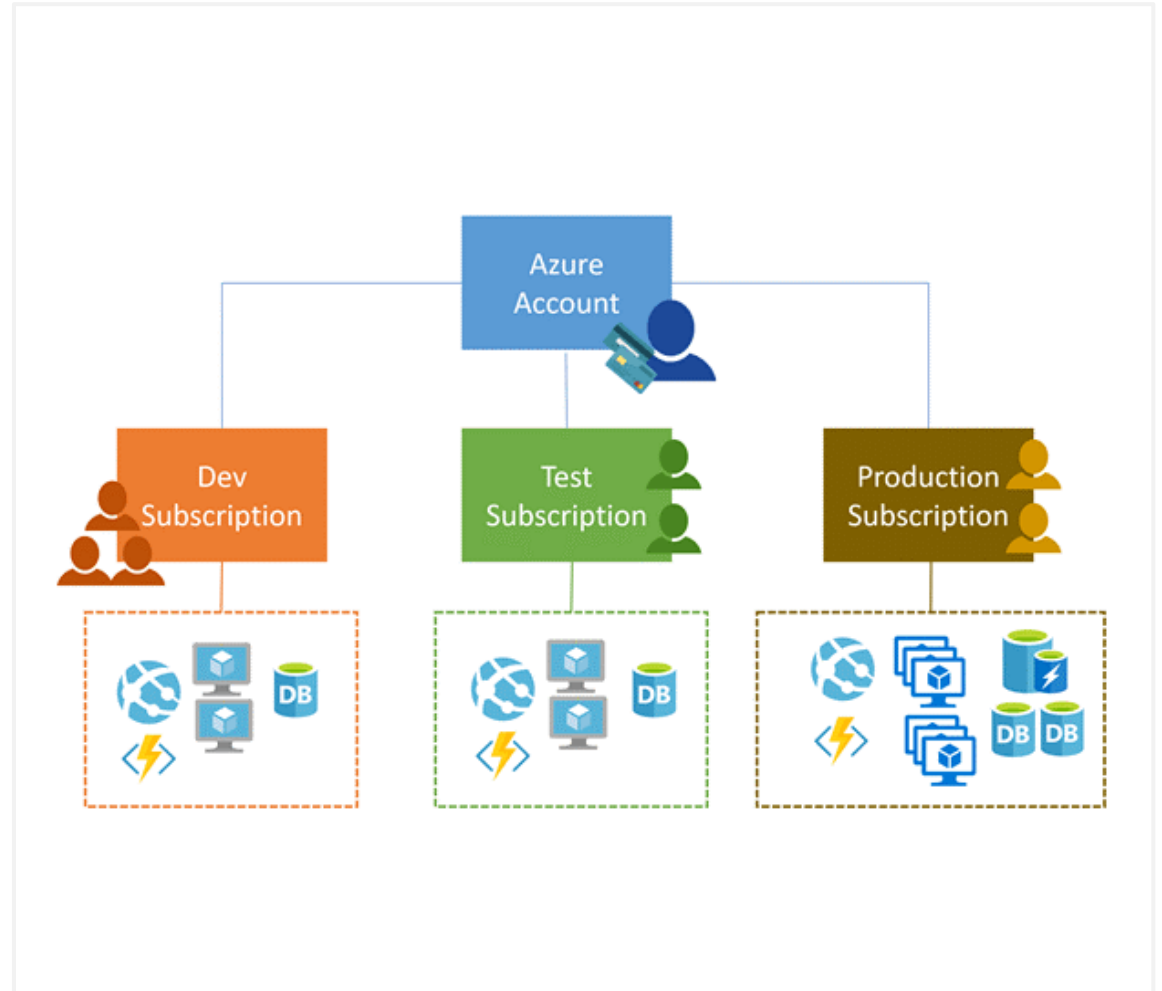
Worldwide there are 60+ regions representing 140 countries

Implement 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



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

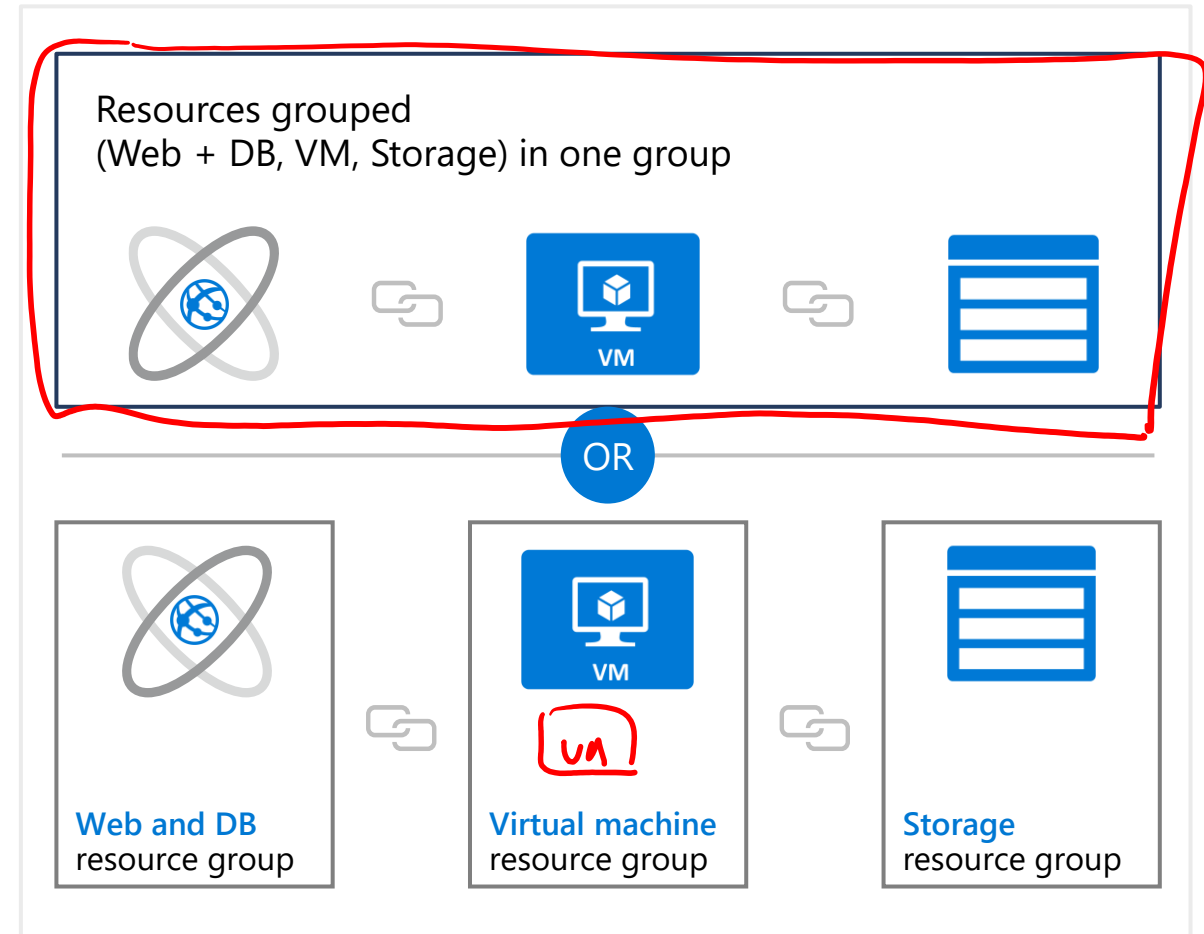
Resources can only exist in one resource group

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

Groups cannot be renamed or nested

Resource locks can prevent changes to the resources

You can move resources between groups



Determine Resource Limits

Quota

ASC DEMO | Usage + quotas

Subscription

Settings

Programmatic deployment

Resource groups

Resources

Usage + quotas

Policies

Security

Events

You can use each Microsoft Azure resource up to its quota. Each subscription has separate quotas and usage is tracked per subscription. If you reach a quota cap, you can request an increase via Help + Support. [Learn more](#)

Request Increase

Quota	Provider	Location	Usage
Total Regional vCPUs	Microsoft.Compute	East US	<div><div></div></div> 25 % 25 of 100
Total Regional vCPUs	Microsoft.Compute	West Europe	<div><div></div></div> 21 % 21 of 100
Total Regional vCPUs	Microsoft.Compute	Central US	<div><div></div></div> 17 % 17 of 100
Standard Dv2 Family vCPUs	Microsoft.Compute	West Europe	<div><div></div></div> 16 % 16 of 100
Standard Dsv2 Family vCPUs	Microsoft.Compute	Central US	<div><div></div></div> 14 % 14 of 100

Resources have a default limit also known as quota

Helpful to track current usage, and plan for future use

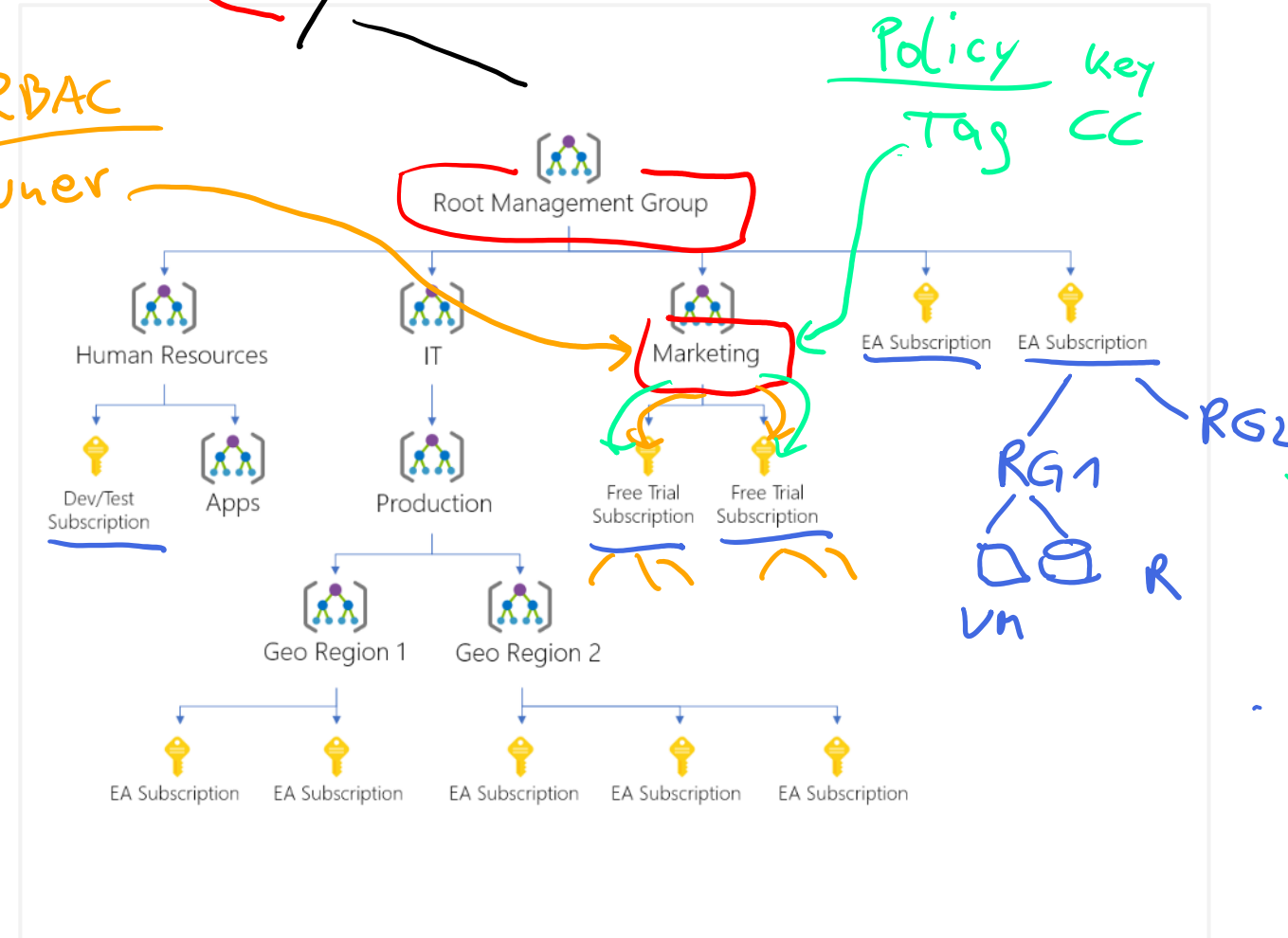
You can open a free support case to increase limits to published maximums

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)



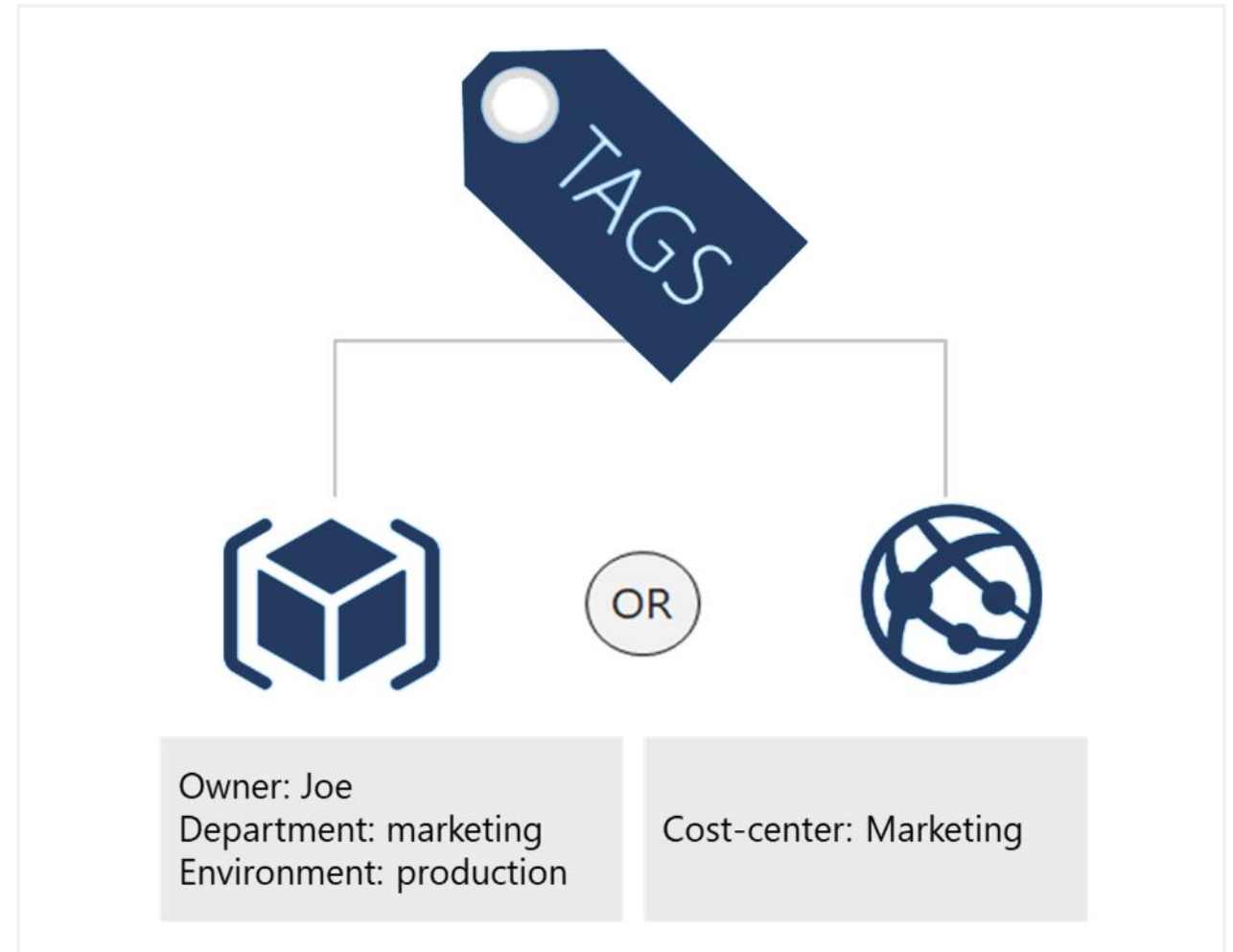
Apply Resource Tagging

Provides metadata for your Azure resources

Logically organizes resources

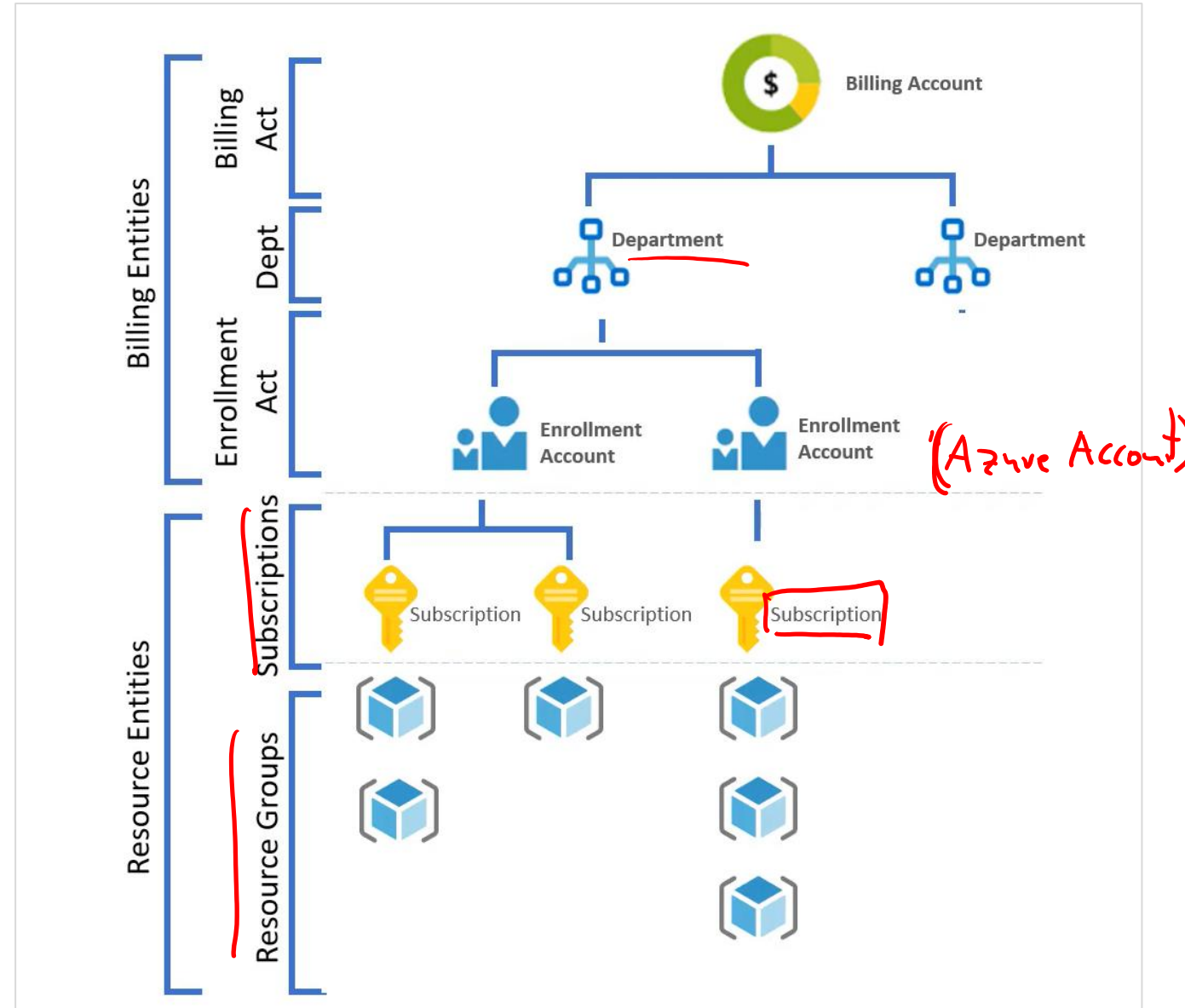
Consists of a name-value pair

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 recommendations



Summary and Resources - Configure Subscriptions

Knowledge Check Questions



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

[Introduction to analyzing costs and creating budgets with Azure Cost Management](#)

[Plan and manage your Azure costs \(Sandbox\)](#)

[Control and organize Azure resources with Azure Resource Manager](#)

A *sandbox* indicates a hands-on exercise.

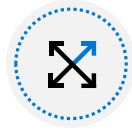
Configure Azure Policy



Configure Azure Policy Introduction



Implement Azure Policy



Create Azure Policies



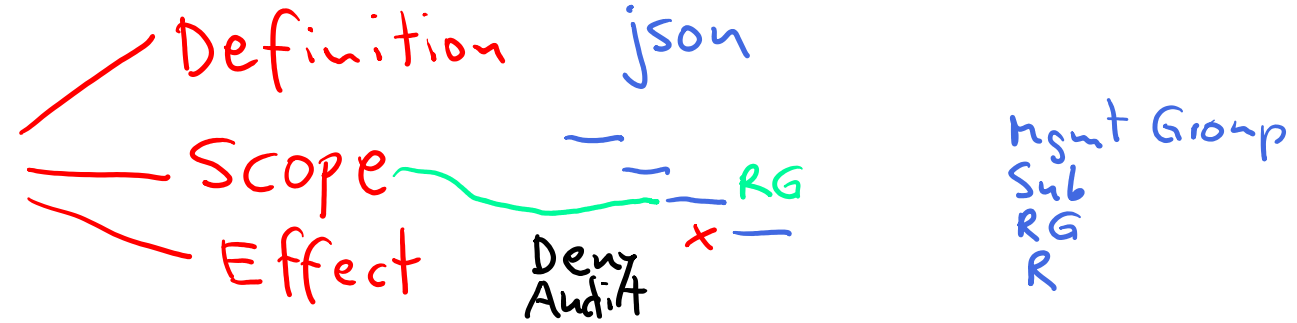
Demonstration – Azure Policies

- Create Policy Definitions
- Create and Scope the Initiative Definition
- Determine Compliance



Summary and Resources

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

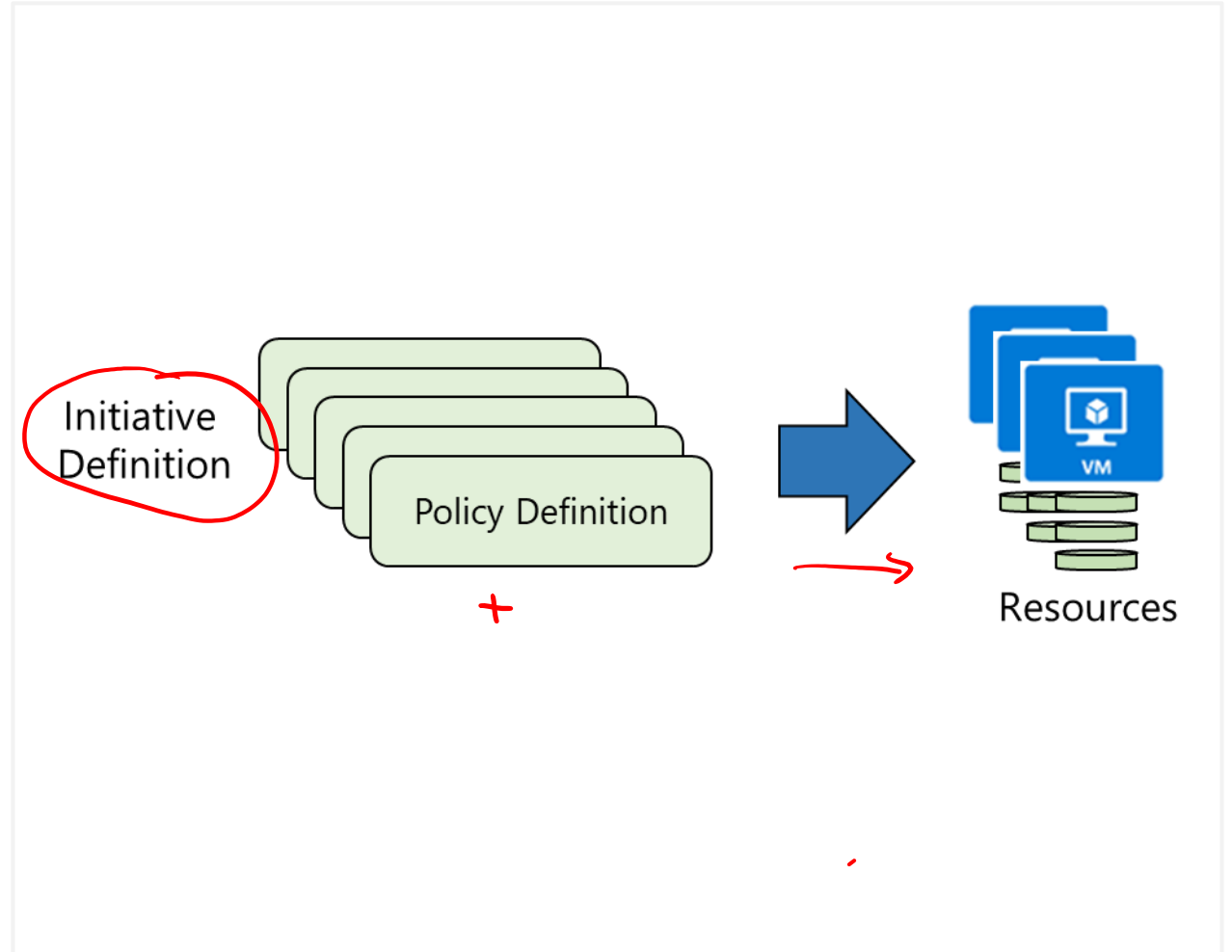
Create Azure Policies

1. Create Policy Definitions

2. Create Initiative Definitions

3. Scope the Initiative Definition

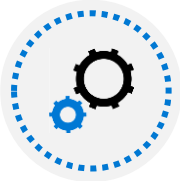
4. Determine Compliance



Demonstration – Azure Policy



Assign a policy



Create and assign an initiative definition



Check for compliance



Check for remediation tasks



Remove your policy and initiative

1. Create 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

Policy definition

New Policy definition

BASICS

Definition location *

Visual Studio Enterprise

Name * ⓘ

Github Sample Policy

Description

A sample policy from Github.

Category ⓘ

☒ Create new ☐ Use existing

Category

POLICY RULE

↓ [Import sample policy definition from GitHub](#)

2. Create Initiative Definitions

Group policy definitions

Include one or more policies

Requires planning

Initiative definition

New Initiative definition

BASICS

Definition location *

Visual Studio Enterprise

Name * ⓘ

East Region

Description ⓘ

East Region Initiative Definition

Category ⓘ

☐ Create new

☒ Use existing

General

namingPolicyDefinition

Policy to specify allowed naming convention

Custom

Delete

regionPolicyDefinition

Policy to allow resource creation only in certain regions

Custom

Delete

3. Scope the Initiative Definition

Policy - Assignments

Search (Ctrl+ /)

Overview

Getting started

Join Preview

Compliance

Remediation

Authoring

Assignments

Definitions

Assign initiative

Assign policy

Refresh

Scope

Visual Studio Enterprise

Definition type

All definition types

Search

Filter by name or id...

Category

All categories

Total Assignments

2

Initiative Assignments

2

Policy Assignments

0

name	Scope	Type	Policies	Category
East Region	Visual Studio Enterprise	Initiative	2	General
ASC Default (subscription: ...)	Visual Studio Enterprise	Initiative	96	Security Center

Assign the definition to a scope

The scope enforces the policy

Select the subscription, and optionally the resource group

4. Determine Compliance

Policy - Compliance

Search (Ctrl+ /)

Overview

Getting started

Join Preview

Compliance

Remediation

Authoring

Assignments

Definitions

Assign policy

Assign initiative

Refresh

Scope

Visual Studio Enterprise

Type

All definition types

Compliance state

All compliance states

Search

Filter by name or id...

Overall resource compliance

98%

159 out of 162

Non-compliant initiatives

1

out of 2

Non-compliant policies

12

out of 98

Non-compliant resources

3

out of 162

Name	Scope	Compliance state	Resource compli...	Non-Compliant Resources	Non-compliant policies
ASC Default (subscription: 957...	Visual Studio Enterprise	Non-compliant	98% (159 out of 162)	3	12
East Region	Visual Studio Enterprise	Not started	100% (0 out of 0)	0	0

Non-compliant initiatives, policies and resources

Evaluates and reports about once an hour

Automatic remediations is available

Summary and Resources – Configure Azure Policy

Knowledge Check Questions



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

[Introduction to Azure Policy](#)

[Build a cloud governance strategy on Azure](#)

Configure Role-Based Access Control



Configure Role-Based Access Control Introduction



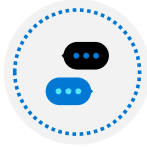
Compare Azure RBAC Roles to Azure AD Roles



Create a Role Definition



Create a Role Assignment



Apply RBAC Authentication



Demonstration – Azure RBAC



Summary and Resources

Compare Azure RBAC Roles to Azure AD Roles

RBAC roles provide fine-grained access management

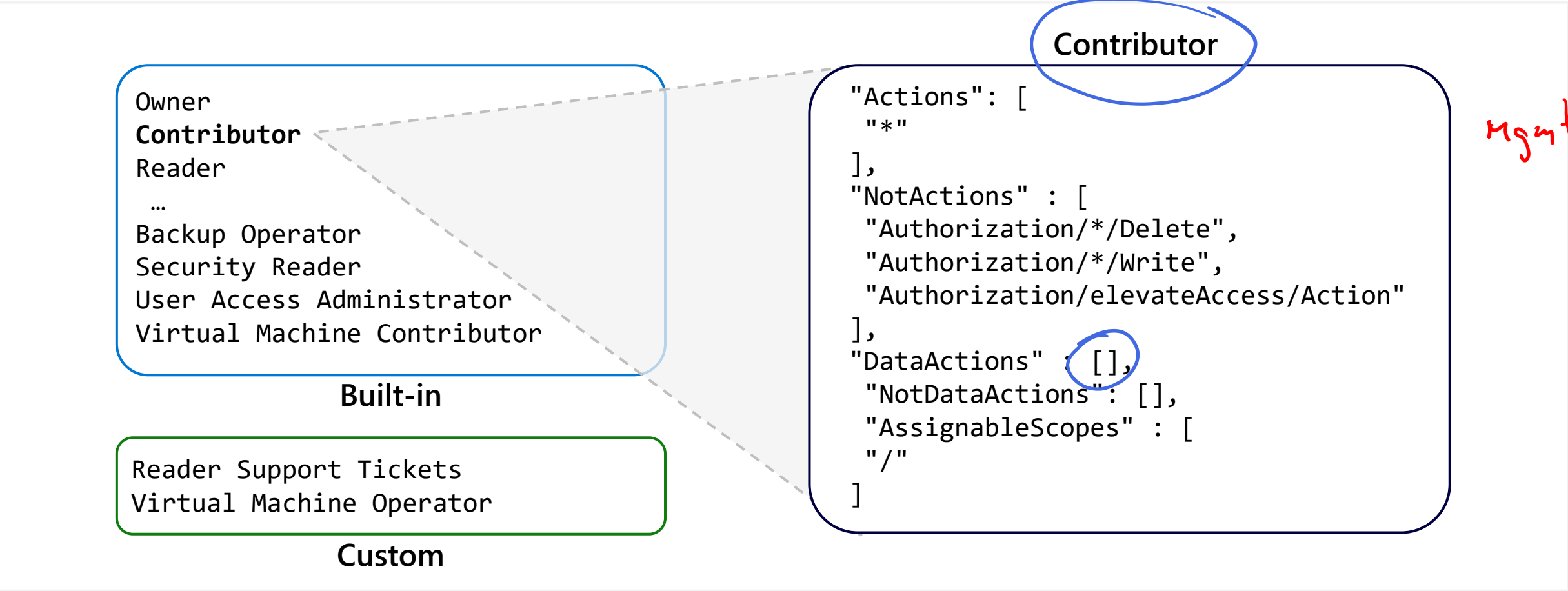
Azure RBAC roles	Azure AD roles
Manage access to Azure resources	Manage access to Azure AD objects
Scope can be specified at multiple levels	Scope is at the tenant level
Role information can be accessed in the Azure portal, Azure CLI, Azure PowerShell, Azure Resource Manager templates, REST API	Role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



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

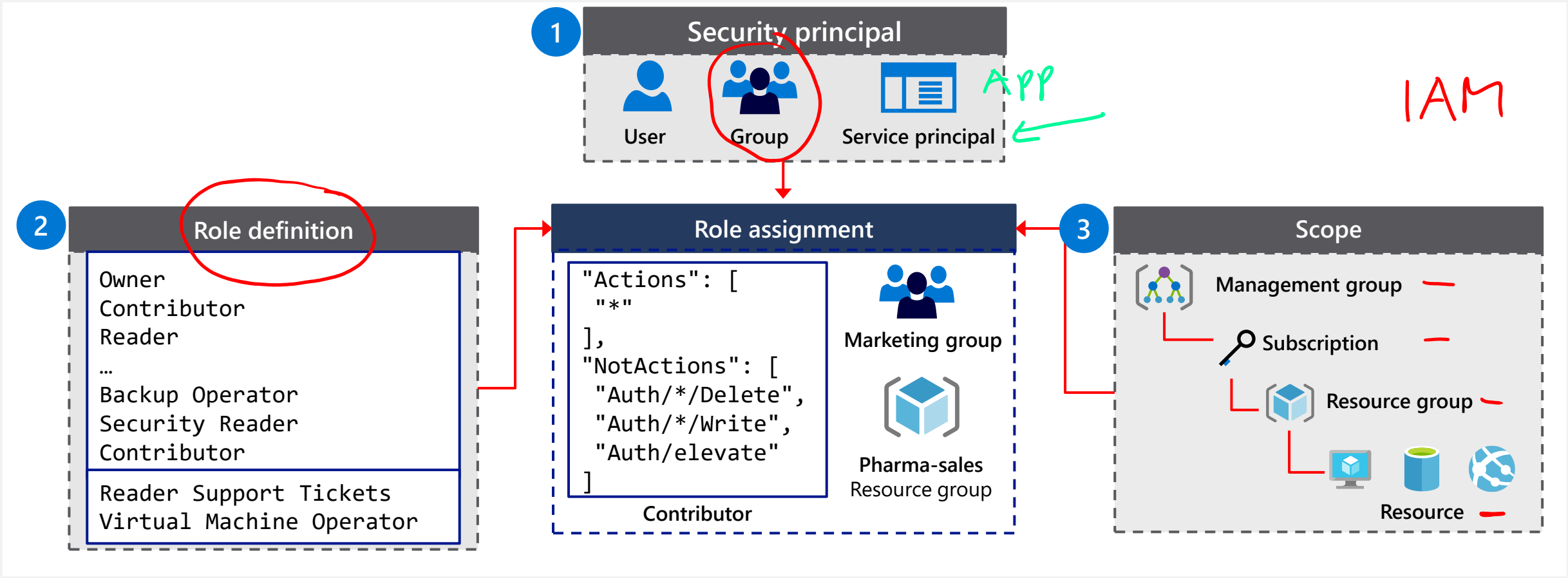
Create a Role Definition

Collection of permissions that lists the operations that can be performed



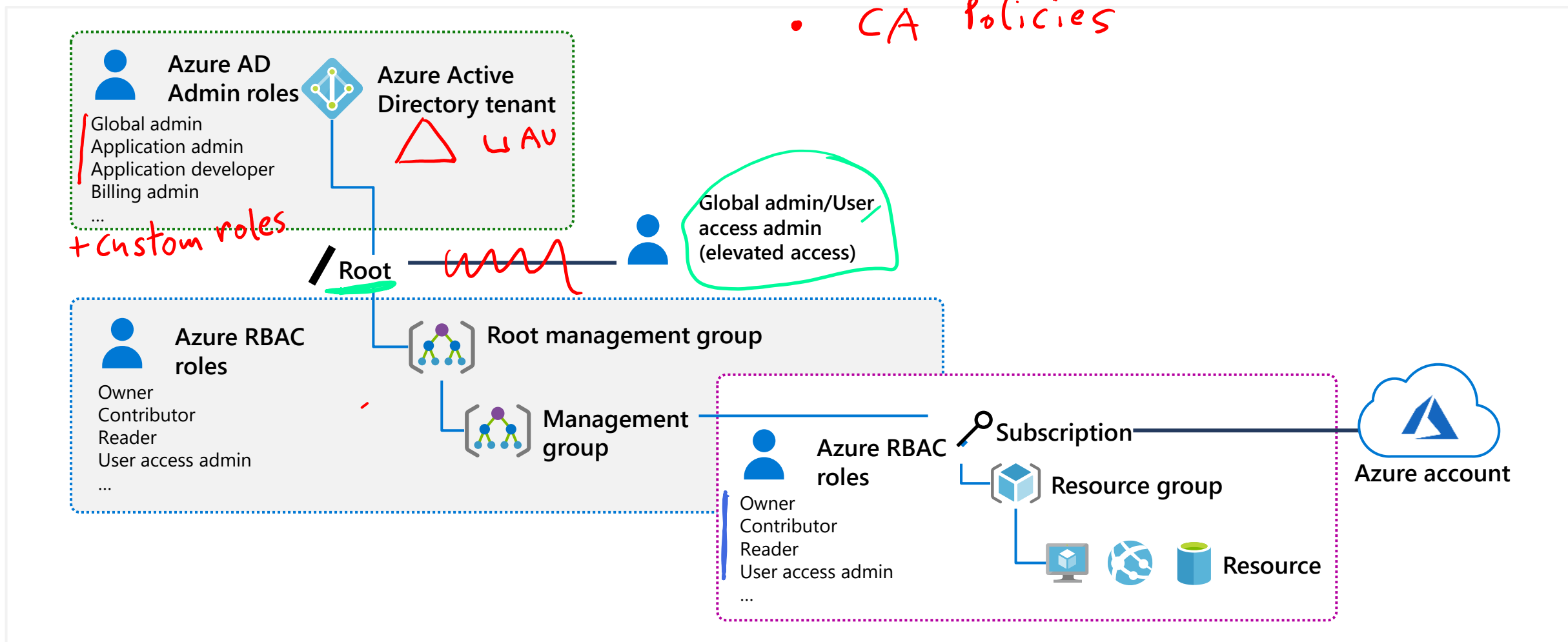
Create a Role Assignment

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

- Privileged Id Management PIM von bis
- ID Protection
- CA Policies



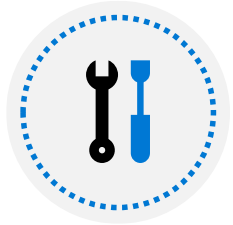
Demonstration – Azure RBAC



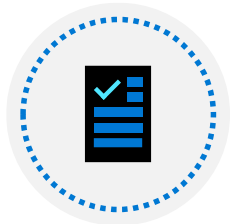
Locate the Access Control blade



Review role permissions



Add a role assignment



Explore PowerShell commands

Summary and Resources – Configure RBAC

Knowledge Check



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

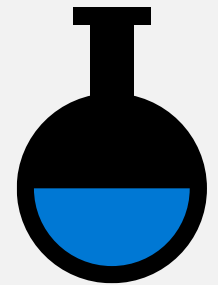
[Create custom roles for Azure resources with Azure role-based access control](#)

[Manage access to an Azure subscription by using Azure role-based access control](#)

[Secure your Azure resources with Azure role-based access control \(Sandbox\)](#)

A *sandbox* indicates a hands-on exercise.

Lab 02a - Manage Subscriptions and RBAC
Lab 02b - Manage Governance via Azure Policy
Lab 03a – Manage Azure resources with the Azure portal



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:

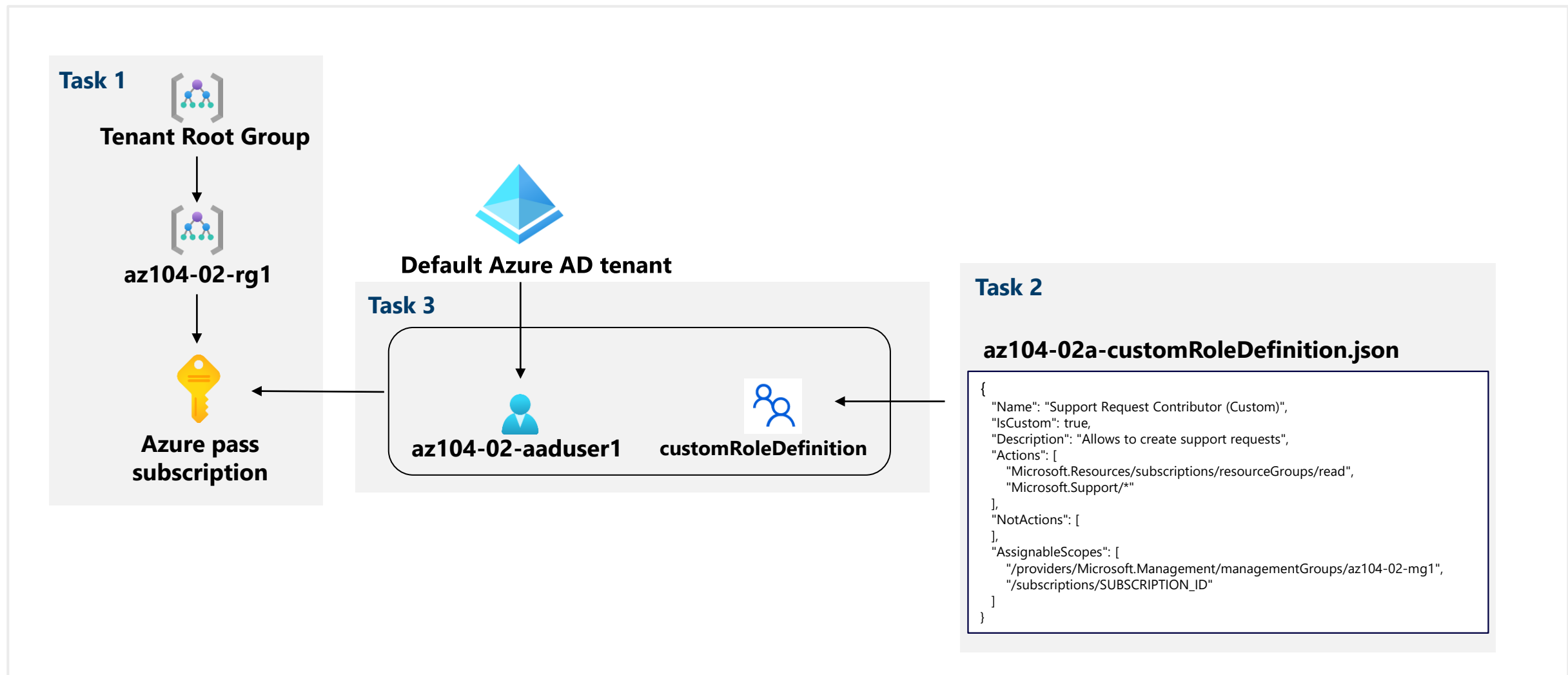
Create custom RBAC roles

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:

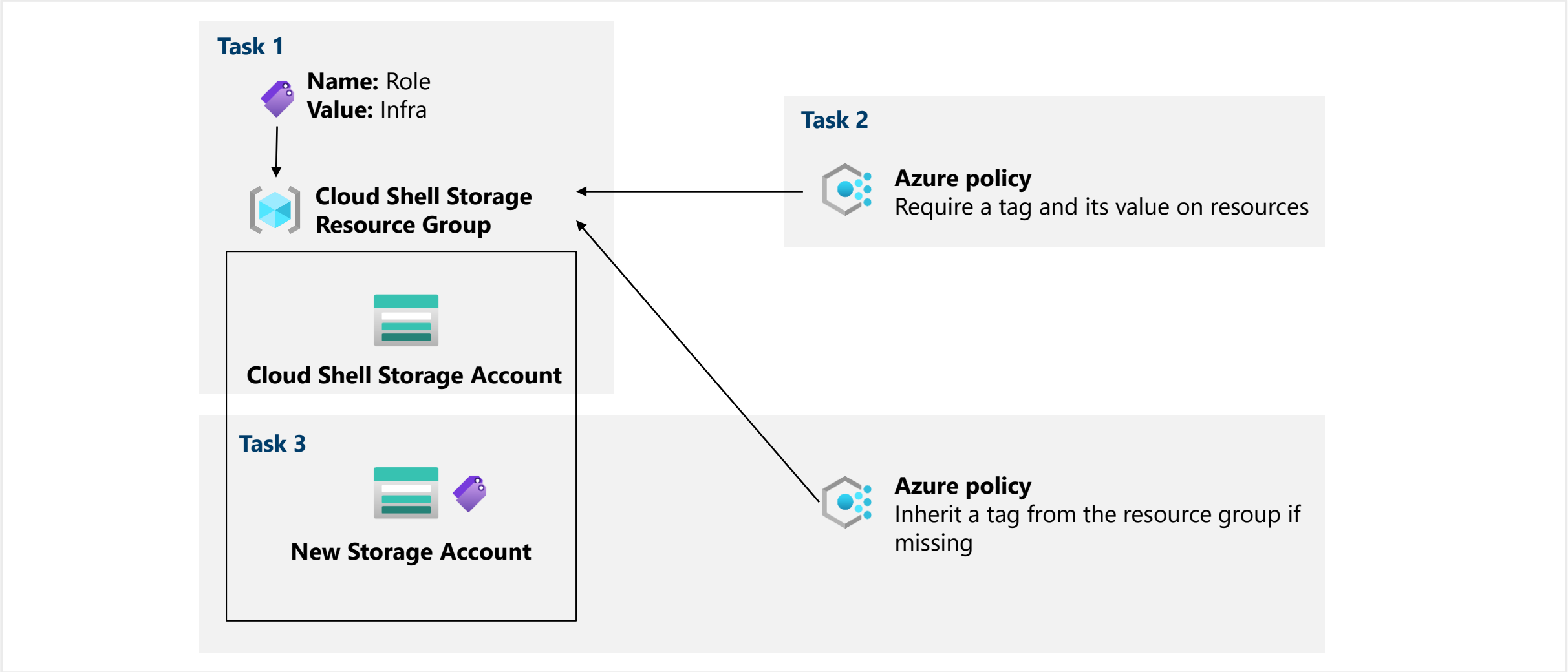
Enforce tagging via an Azure Policy

Task 3:

Apply tagging via an Azure Policy

Next slide for an architecture diagram 

Lab 02b – Architecture diagram



Lab 03a – Manage Azure resources with the Azure portal

Lab scenario

You need to explore the basic Azure administration capabilities associated with provisioning resources and organizing them based on resource groups, including moving resources between resource groups. You also want to explore options for protecting disk resources from being accidentally deleted, while still allowing for modifying their performance characteristics and size

Objectives

Task 1:

Create resource groups and deploy resources to resource groups

Task 2:

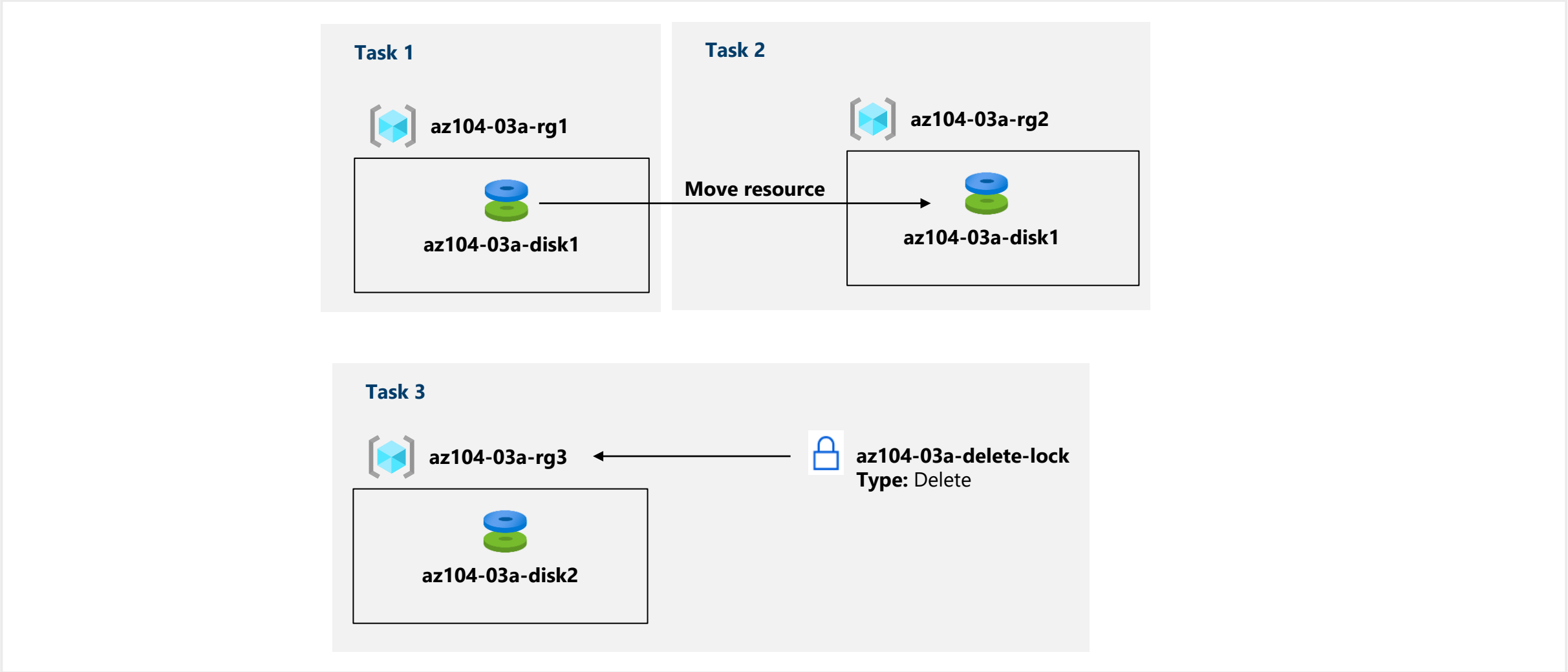
Move resources between resource groups

Task 3:

Implement and test resource locks

Next slide for an architecture diagram 

Lab 03a – Architecture diagram



End of presentation

