Microsoft

AZ-104

Administer Governance and Compliance

AZ-104 Course Outline

01: Administer Identity
02: Administer Governance and Compliance   ← Roles Azure
                                             Policies Azure
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

Learning Objectives

- Configure Subscriptions

- Configure Azure Policy

- Configure Role-Based Access Control

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

Configure Subscriptions and Configure Azure Resource Manager Resources

ARM
Bicep Lang Template

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 = Locations

IaaS ⟶ PaaS
vm   App Service
        Docker K8s

Serverless
Func.

A region represents a collection of datacenters

Provides flexibility and scale
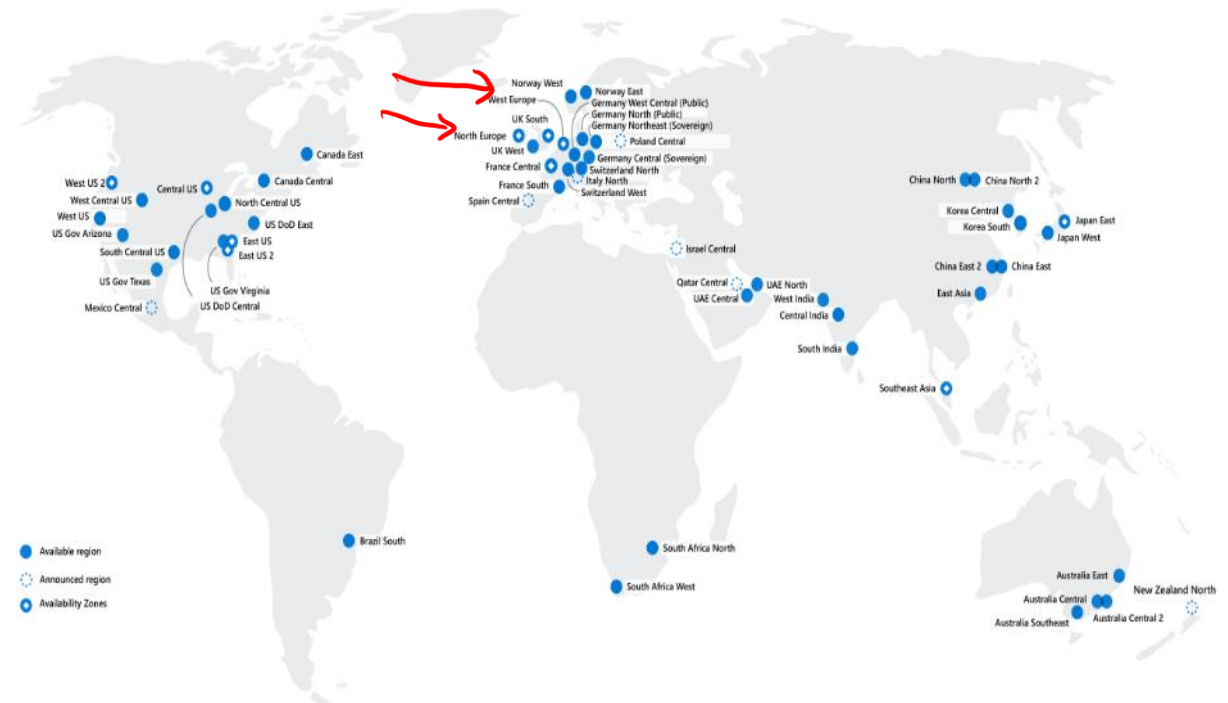
Preserves data residency

Select regions close to your users

Be aware of region deployment availability

There are global services that are region independent

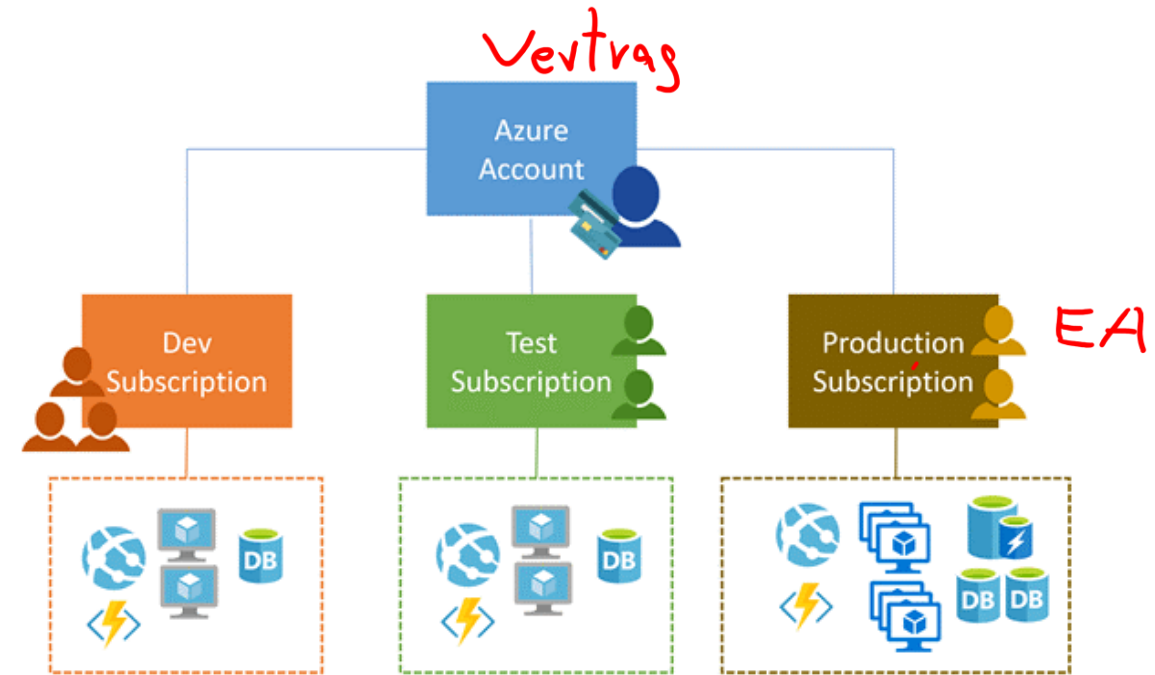Most regions are paired for high availability

Worldwide there are 60+ regions representing 140 countries

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
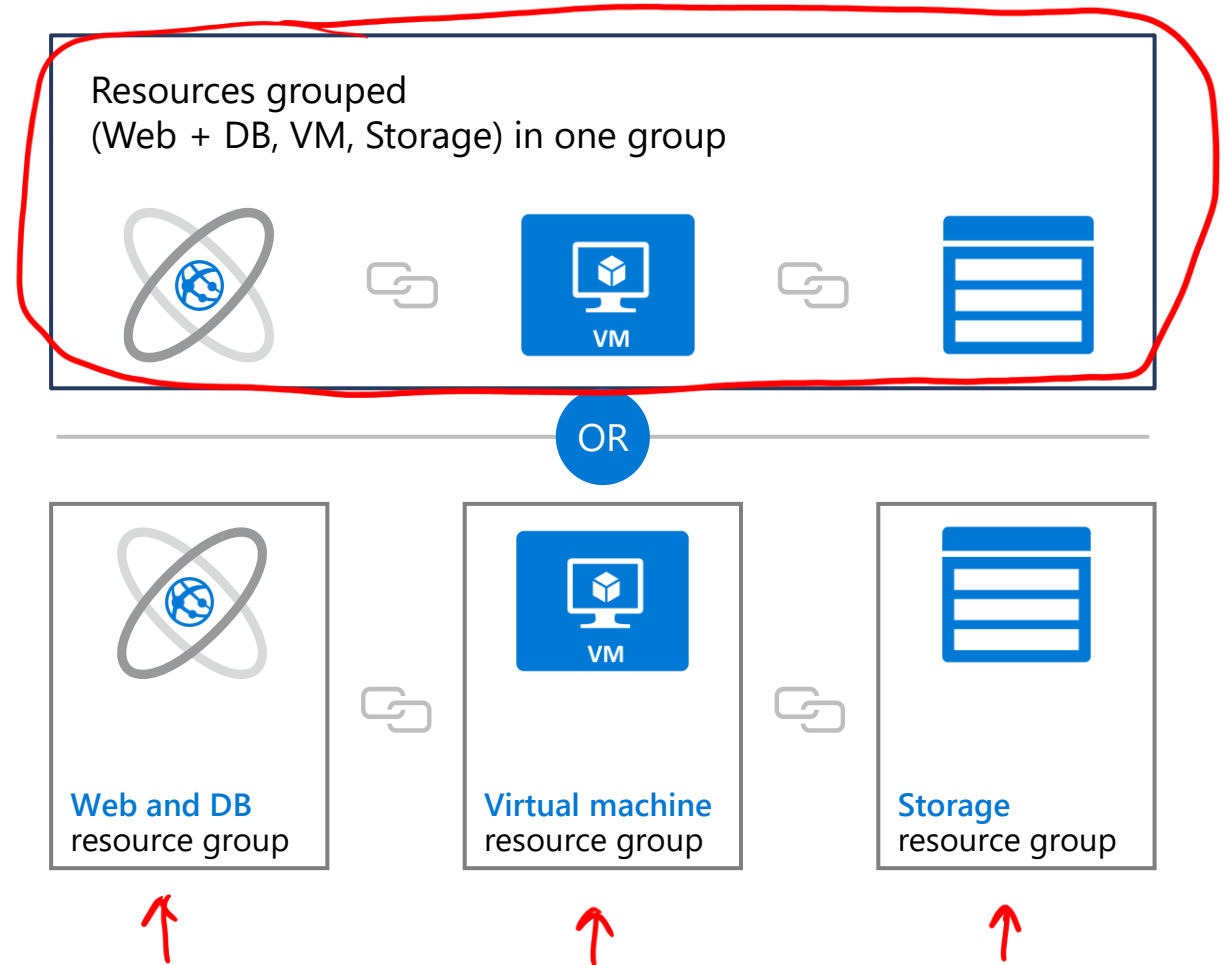
Personal free account – Start right away

Create Resource Groups

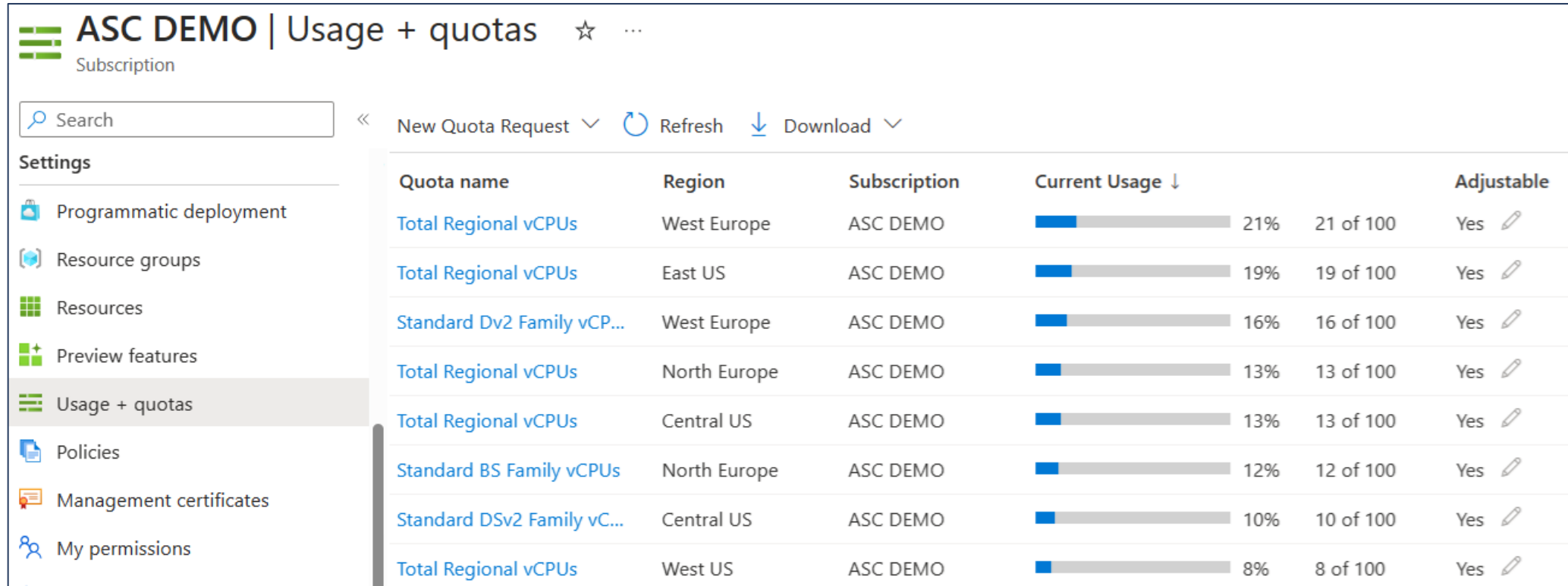Resources can only exist in one resource group

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

Resources grouped
(Web + DB, VM, Storage) in one group

OR

Web and DB
resource group

Virtual machine
resource group

Storage
resource group

Determine Service Limits and Quotas

Resources have a default limit - a subscription quota

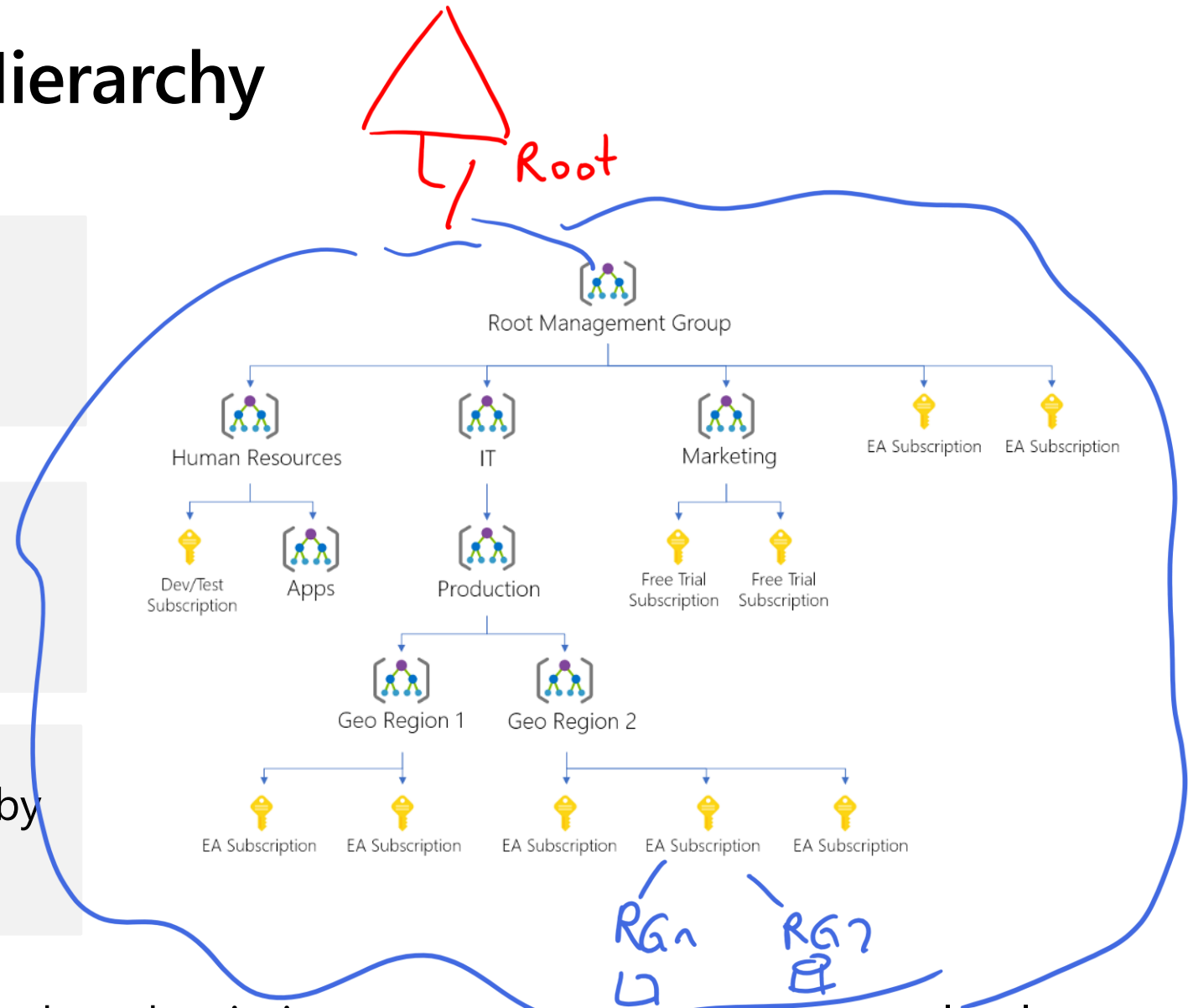Helpful to track current usage, and plan for future use

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)

Root

Root Management Group

Human Resources

IT

Marketing

EA Subscription

EA Subscription

Dev/Test Subscription

Apps

Production

Free Trial Subscription

Free Trial Subscription

Geo Region 1

Geo Region 2

EA Subscription

EA Subscription

EA Subscription

EA Subscription

EA Subscription

RG1

RG2

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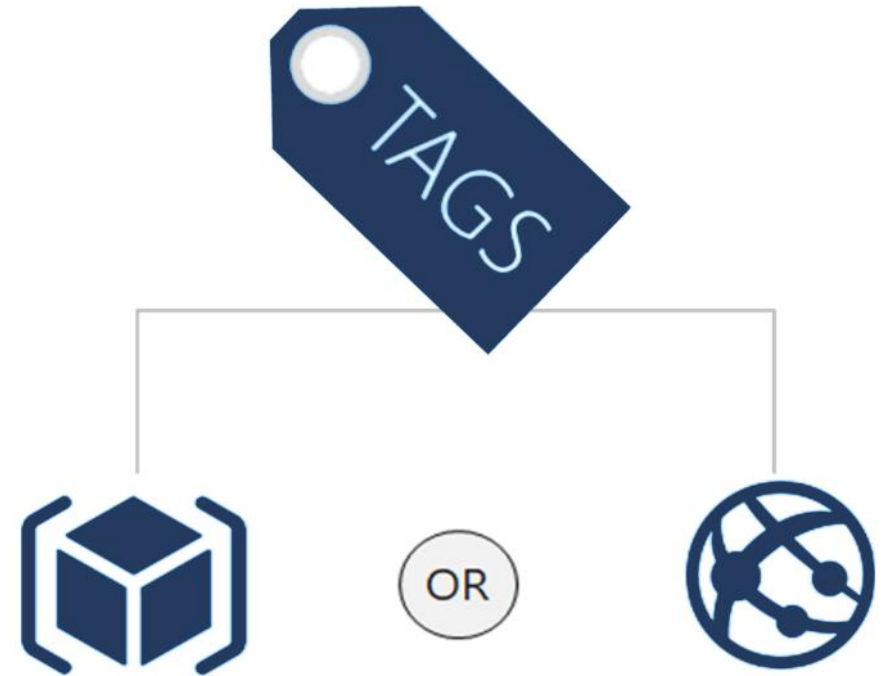
Apply Resource Tagging

Provides metadata for your Azure resources

Logically organizes resources

Consists of a name-value pair

Very useful for rolling up billing information

TAGS

OR

Owner: Joe
Department: marketing
Environment: production

Cost-center: Marketing

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
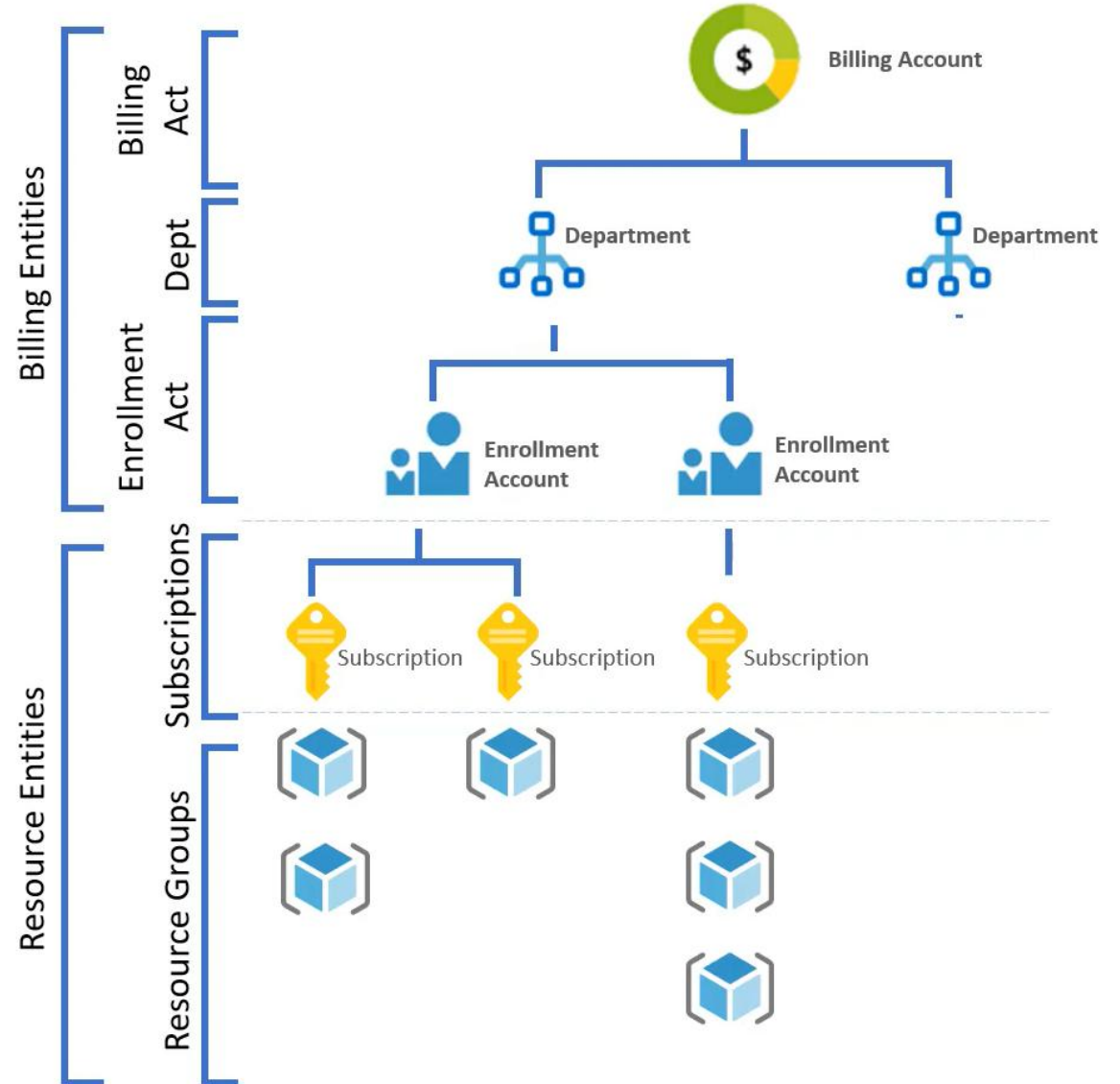
Learning Recap - Configure Subscriptions
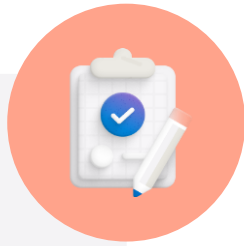
Check your knowledge questions and additional study

- Introduction to analyzing costs and creating budgets with Azure Cost Management

- Control and organize Azure resources with Azure Resource Manager

- Use Azure Resource manager

Configure Azure Policy

Definition
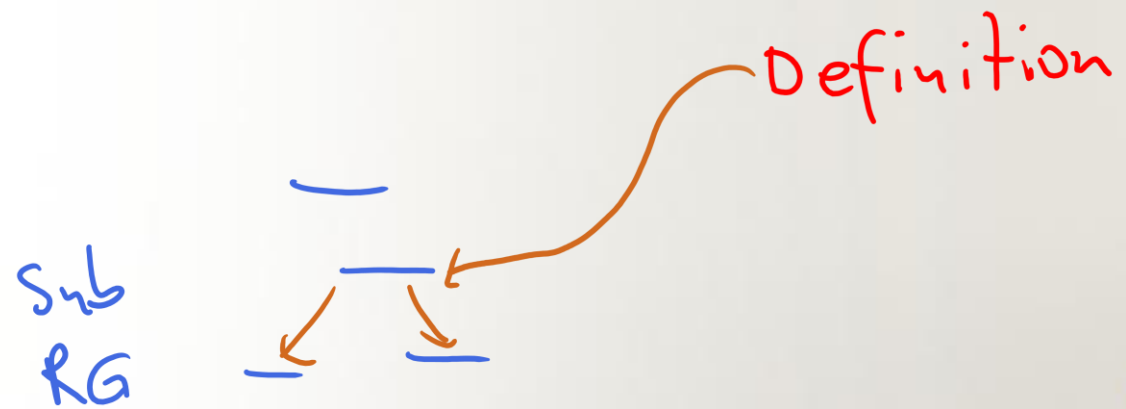
Location
westeurope

json

Sub
RG

Implement Azure Policies

Deployment
→ ARM

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

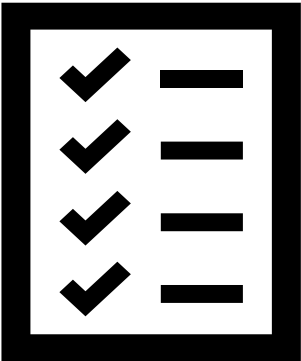Define and create
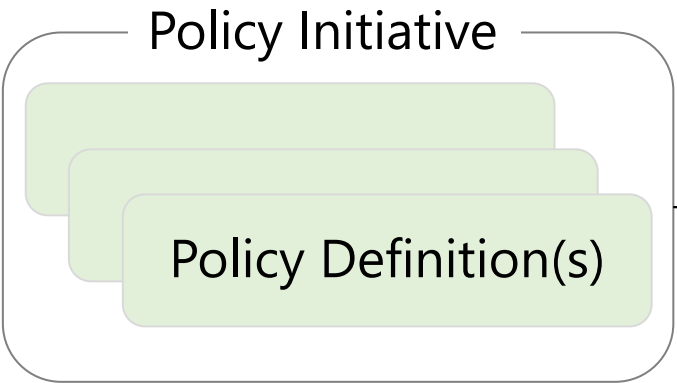
Scope and assign

Assess compliance

Policy Initiative

Policy Definition(s)
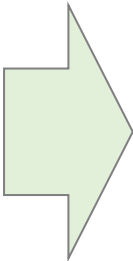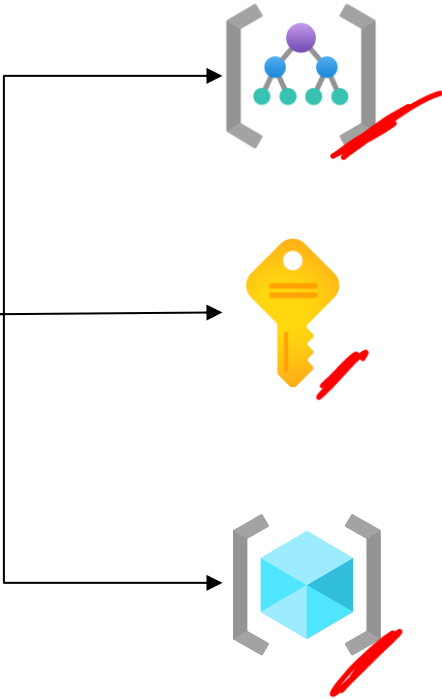
Learning Recap – Configure Azure Policy
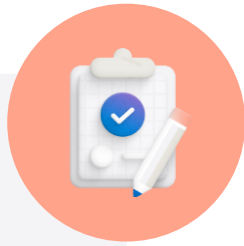
Check your knowledge questions and additional study

- Introduction to Azure Policy
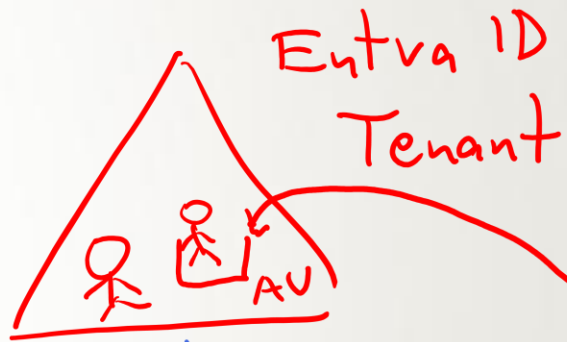
Compare Azure RBAC Roles to Entra ID Roles

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, Azure Active Directory PowerShell for Graph

(handwritten annotation near "Azure RBAC roles": Owner)

(handwritten annotation near "Entra ID roles": Global A.)

✔ **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

Owner
Contributor
Reader
 …
Backup Operator
Security Reader
User Access Administrator
Virtual Machine Contributor

Built-in

Reader Support Tickets
Virtual Machine Operator

Custom

Contributor

```
"Actions": [
 "*"
],
"NotActions" : [
 "Authorization/*/Delete",
 "Authorization/*/Write",
 "Authorization/elevateAccess/Action"
],
"DataActions" : [],
 "NotDataActions": [],
 "AssignableScopes" : [
 "/"
]
```
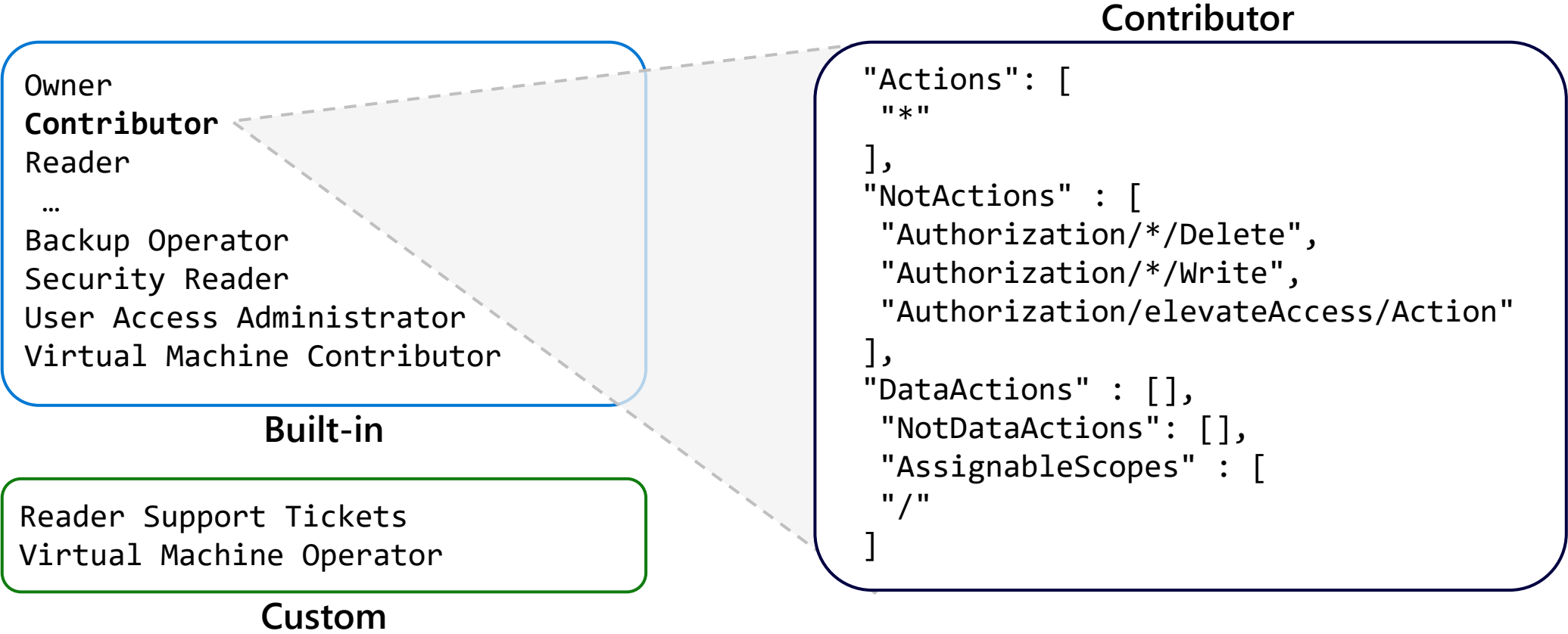
Create a Role Assignment

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

1 — Security principal

User | Group | Service principal

2 — Role definition

```
Owner
Contributor
Reader
…
Backup Operator
Security Reader
Contributor

Reader Support Tickets
Virtual Machine Operator
```

Role assignment

```
"Actions": [
  "*"
],
"NotActions": [
  "Auth/*/Delete",
  "Auth/*/Write",
  "Auth/elevate"
]
```
Contributor

Marketing group

Pharma-sales
Resource group

3 — Scope

Management group
Subscription
Resource group
Resource

Apply RBAC Authentication

Entra ID Admin roles — Tenant — AU

Global admin
Application admin
Application developer
Billing admin
...

Global admin/User access admin (elevated access)

Root

Azure RBAC roles

Owner
Contributor
Reader
User access admin
...

Root management group

Management group

Azure RBAC roles

Owner
Contributor
Reader
User access admin
...

Subscription

Resource group

Resource

Azure account

Learning Recap– Configure RBAC
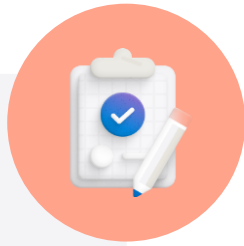
Check your knowledge questions and additional study
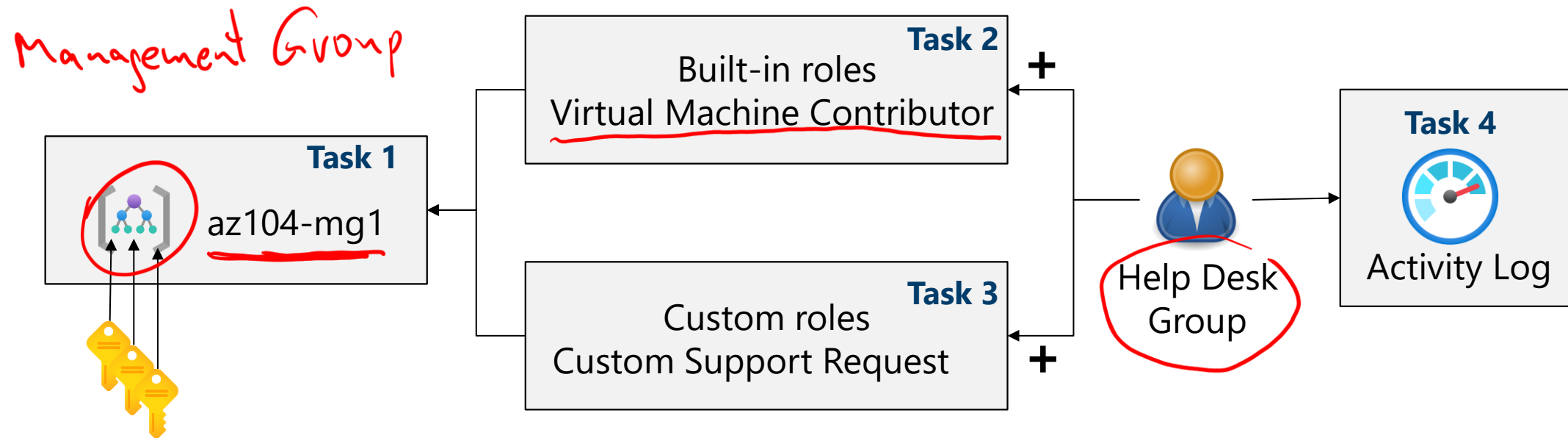
- Create custom roles for Azure resources with Azure role-based access control
- Manage access to an Azure subscription by using Azure role-based access control
- Secure your Azure resources with Azure role-based access control

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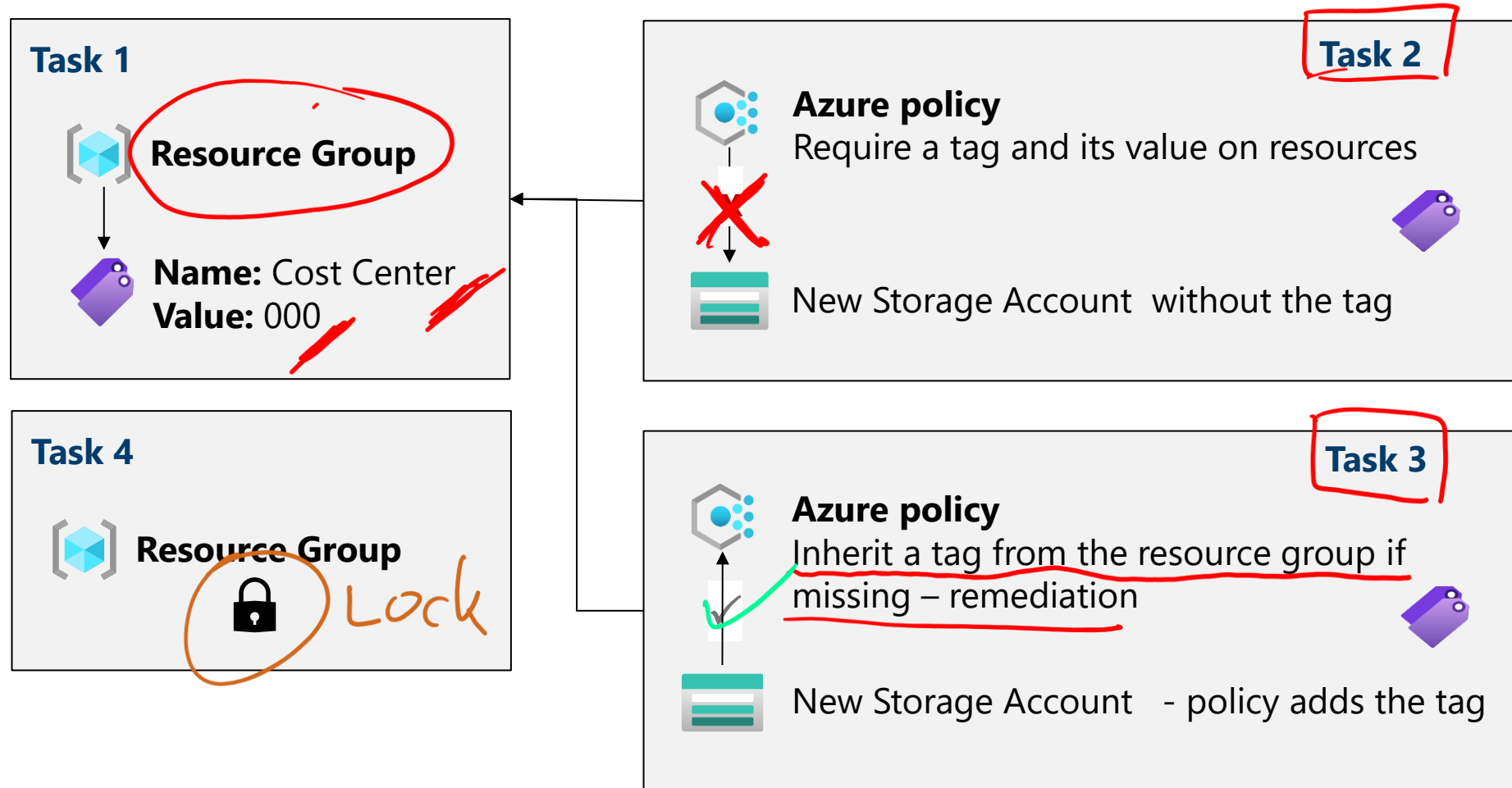Lab 02b - Manage Governance via Azure Policy

Lab 02a – Architecture diagram

Management Group

Task 1
az104-mg1

Task 2
Built-in roles
Virtual Machine Contributor

+

Task 3
Custom roles
Custom Support Request

+

Help Desk Group

Task 4
Activity Log

Azure Policy

Lab 02b – Architecture diagram

Task 1

Resource Group

Name: Cost Center
Value: 000

Task 2

Azure policy
Require a tag and its value on resources

New Storage Account without the tag

Task 4

Resource Group

Lock

Task 3

Azure policy
Inherit a tag from the resource group if missing – remediation

New Storage Account   - policy adds the tag

End of presentation