Microsoft

AZ-104

Administer Governance and Compliance

AZ-104 Course Outline

01: Administer Identity

02: Administer Governance and Compliance

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

Identify Regions

= Location   ~67

Region
Avail
Zones

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

AMS

Dublin

?

Norway West
West Europe
UK South
North Europe
UK West
France Central
France South
Spain Central

Norway East
Germany West Central (Public)
Germany North (Public)
Germany Northeast (Sovereign)
Poland Central
Germany Central (Sovereign)
Italy North
Switzerland North
Switzerland West

Canada East

West US 2
West Central US
West US
US Gov Arizona
South Central US
US Gov Texas
Mexico Central

Central US
North Central US

Canada Central

East US
East US 2
US DoD East
US Gov Virginia
US DoD Central

China North   China North 2
Korea Central
Korea South   Japan East
Japan West
China East 2   China East
East Asia

Israel Central

Qatar Central   UAE North
UAE Central   West India
Central India

South India

Southeast Asia

Brazil South

South Africa North

South Africa West

Australia East
Australia Central   New Zealand North
Australia Southeast   Australia Central 2

• Available region
○ Announced region
◉ Availability Zones

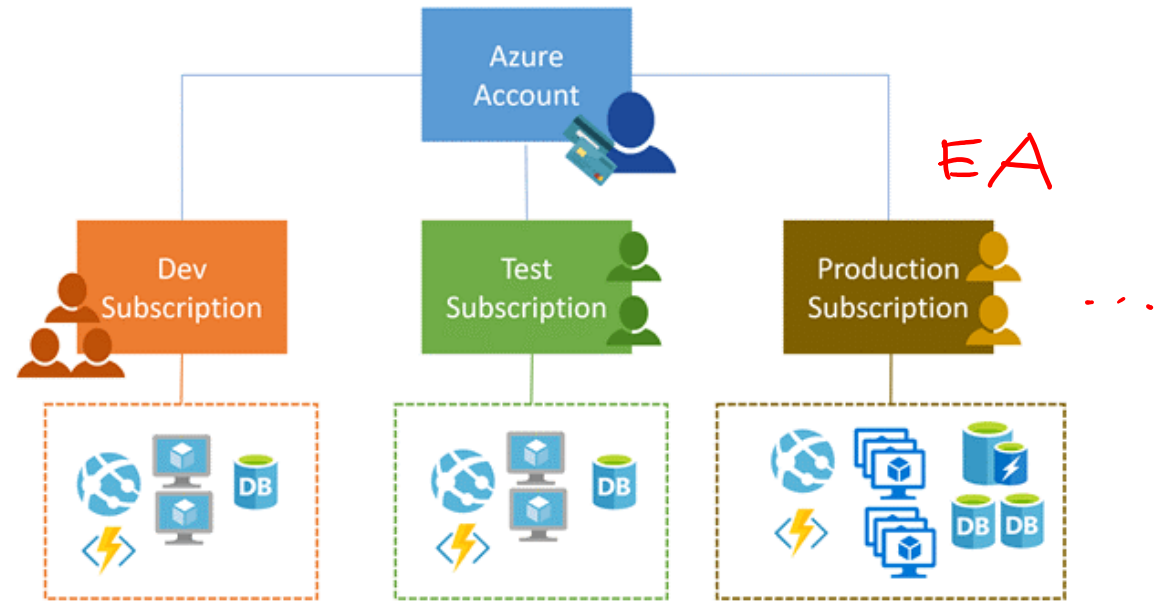## Worldwide there are 60+ regions representing 140 countries

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 *CC*
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
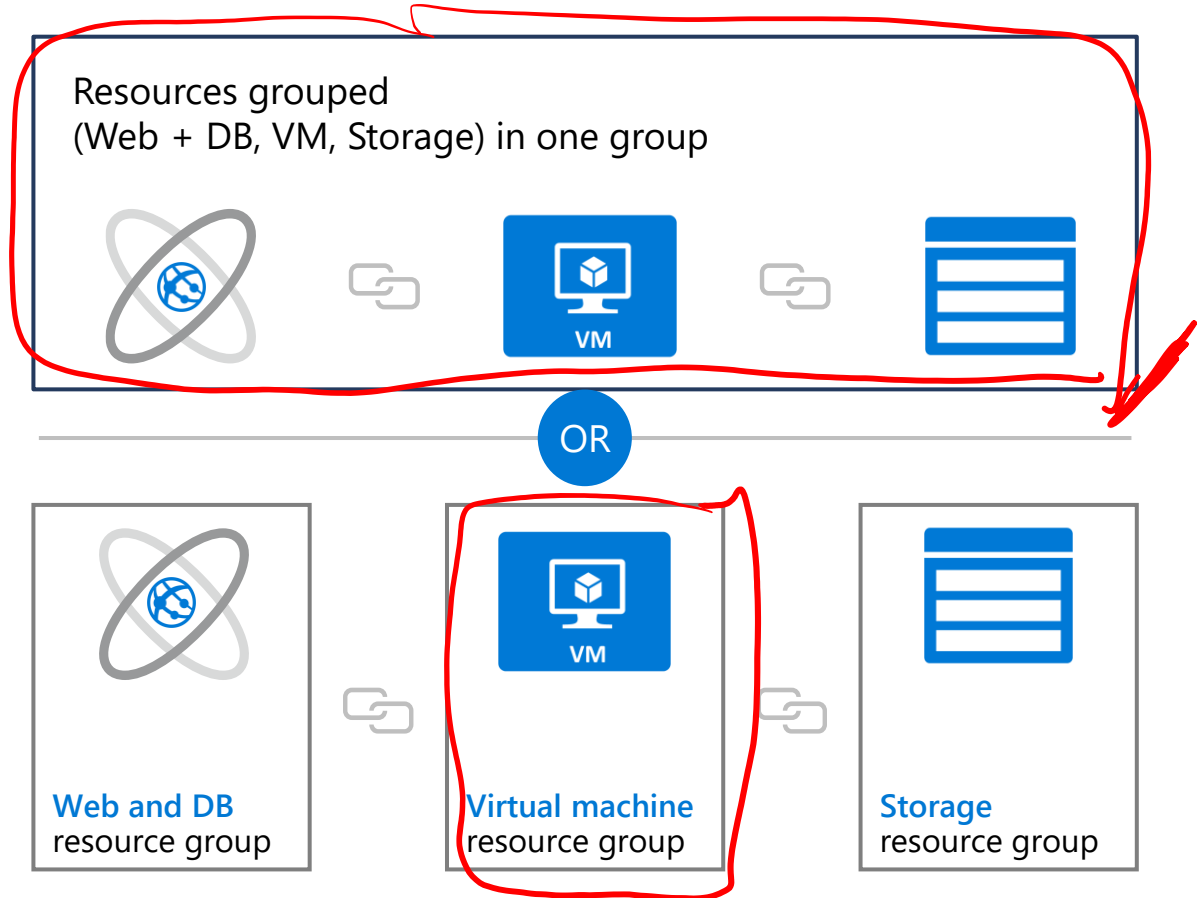
Determine Service Limits and Quotas

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 Management Group

Human Resources

IT

Marketing

EA Subscription

EA Subscription

Dev/Test Subscription

Apps

Production

Free Trial Subscription

Free Trial Subscription

Policy

Role

Geo Region 1

Geo Region 2

EA Subscription

EA Subscription

EA Subscription

EA Subscription
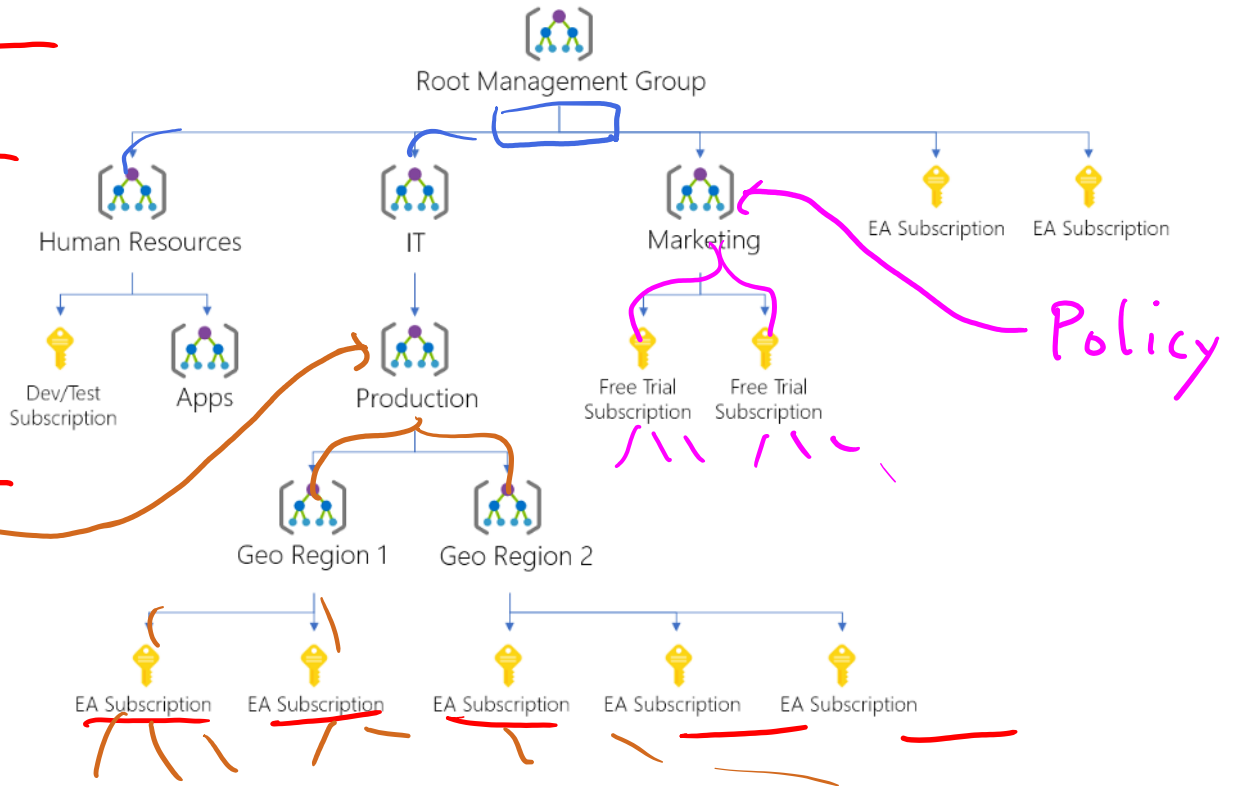
EA Subscription

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

Apply Resource Tagging

Provides metadata for your Azure resources
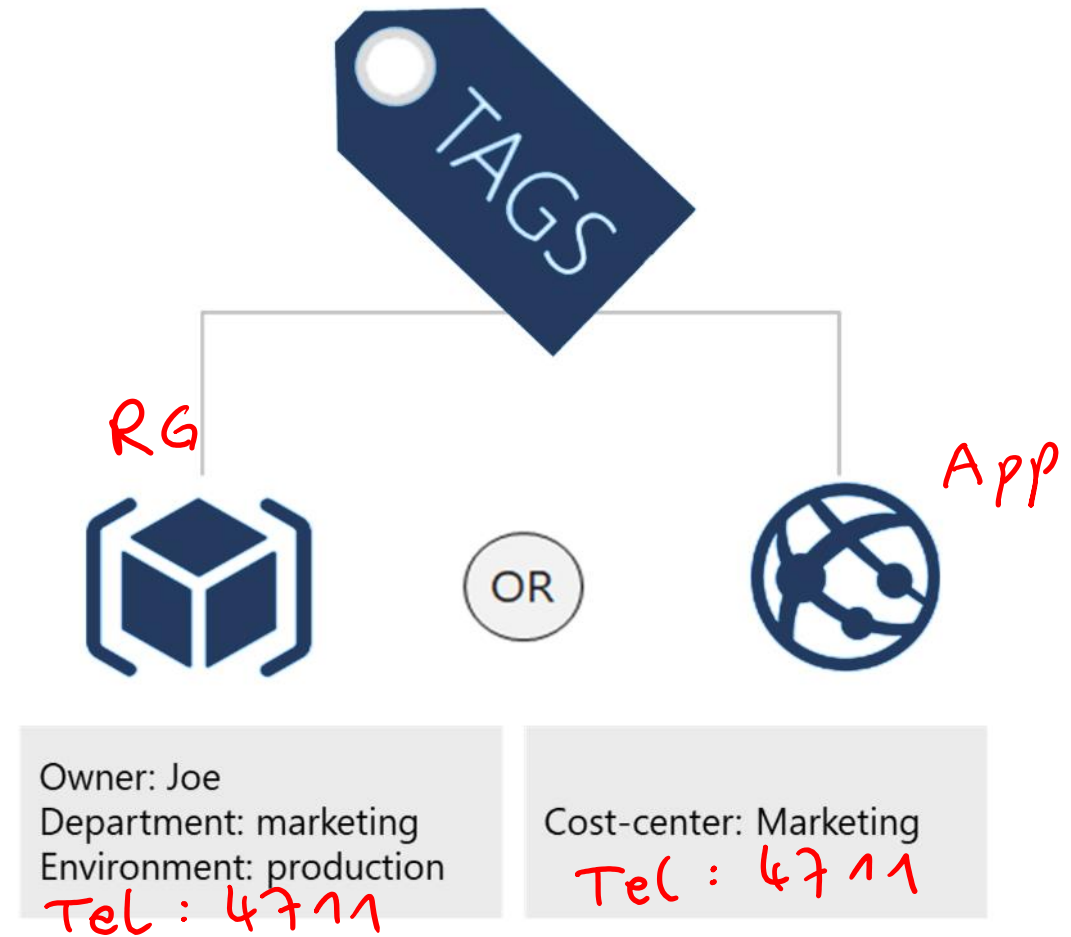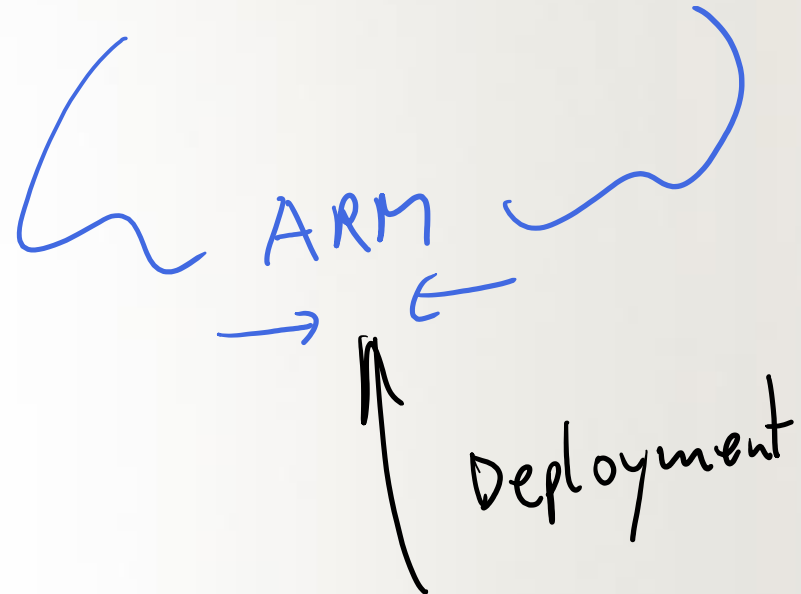
Logically organizes resources

Consists of a name-value pair

Very useful for rolling up billing information

RG

App

Owner: Joe
Department: marketing
Environment: production
Tel : 4711

Cost-center: Marketing
Tel : 4711

ARM

Deployment

Configure Azure Policy

mnss in westenrope sein
(json)

Definition

Effect
Deny ✳
Andit

Mgnt Group
Sub
RG

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

B2 Serie (handwritten annotation)

Create Azure Policies

Define and create
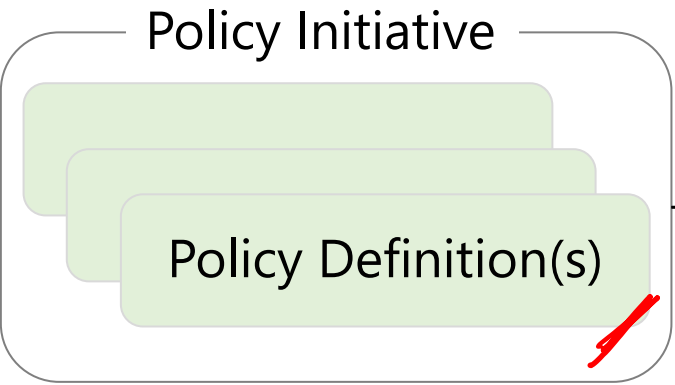
Scope and assign

Assess compliance

Policy Initiative

Policy Definition(s)
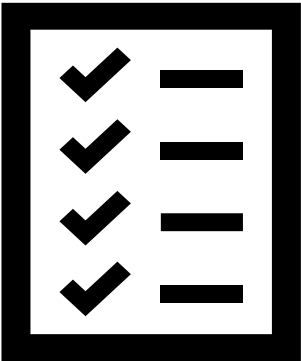
42%

Configure Role-Based Access Control (RBAC)

Compare Azure RBAC Roles to Entra ID Roles

RBAC roles provide fine-grained access management

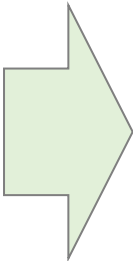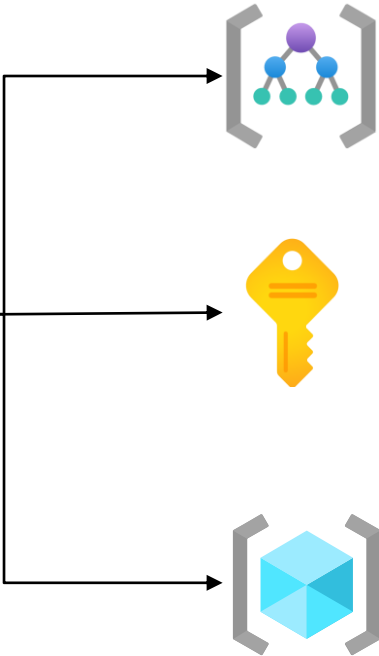| Azure RBAC roles *IAM*	Entra ID roles *+ M365*
Manage access to Azure resources *json*	Manage access to Entra ID objects
Scope can be specified at multiple levels	Scope is at the tenant level *or AU*
Role information can be accessed in the Azure portal, Azure CLI, Azure PowerShell, Azure Resource Manager templates, REST API	Role information can be accessed in Azure portal, Microsoft 365 admin portal, Microsoft Graph, Azure Active Directory PowerShell for Graph *ADAL*

✔ **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

Contributor

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

Built-in

Reader Support Tickets
Virtual Machine Operator

Custom

json

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

Root
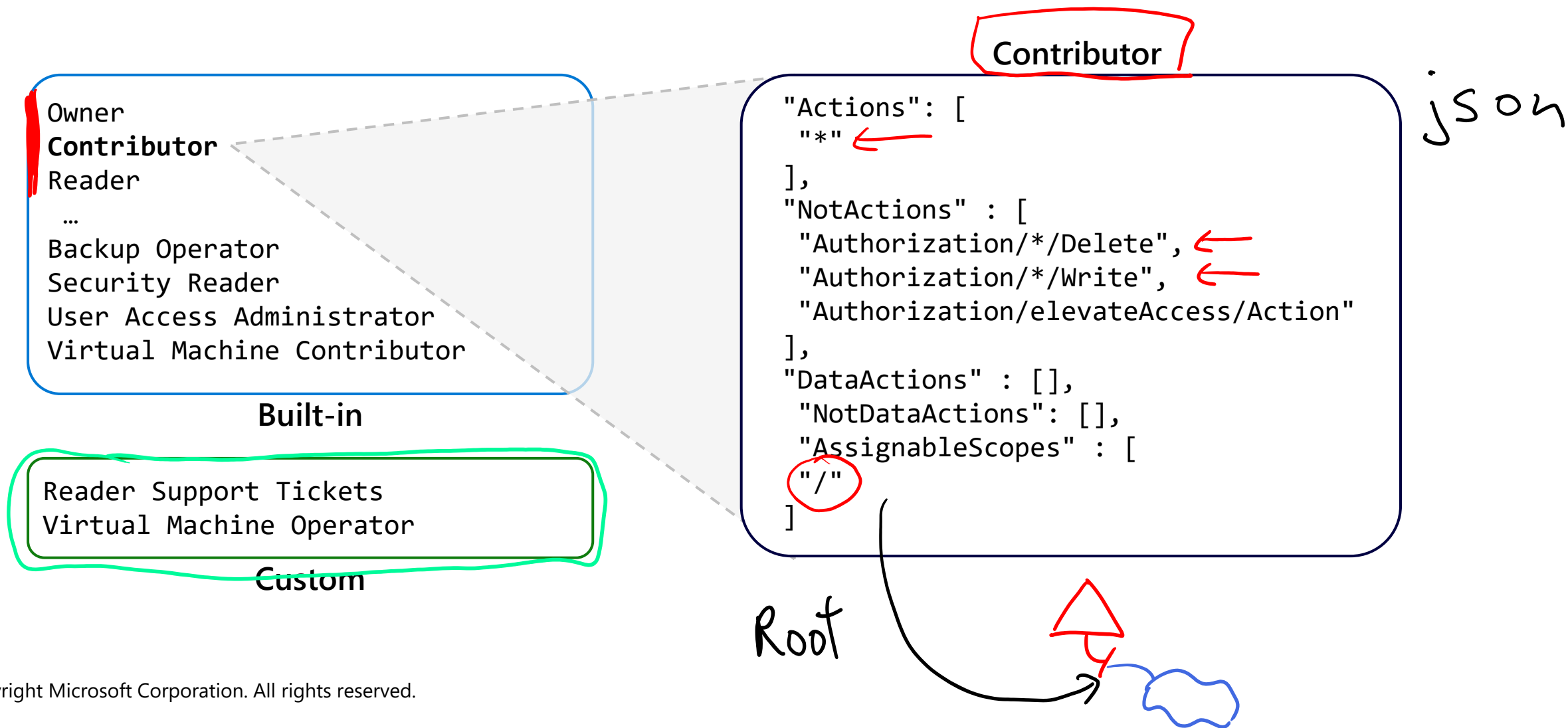
Create a Role Assignment

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 = App

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

Global admin
Application admin
Application developer
Billing admin
...

self elevate

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
...

10.000€
🔍 Subscription

Resource group

Resource

Azure account

2011

Classic Roles

Admin
Service Admin

Legal

Lab 02a - Manage Subscriptions and RBAC

Lab 02b - Manage Governance via Azure Policy

Lab 02a – Manage Subscriptions and Azure RBAC

Contoso needs to improve the management of Azure resources, specifically:

- Use management groups for the Azure subscriptions
- Grant user permissions for submitting support requests. This user would only be able to create support request tickets and view resource groups
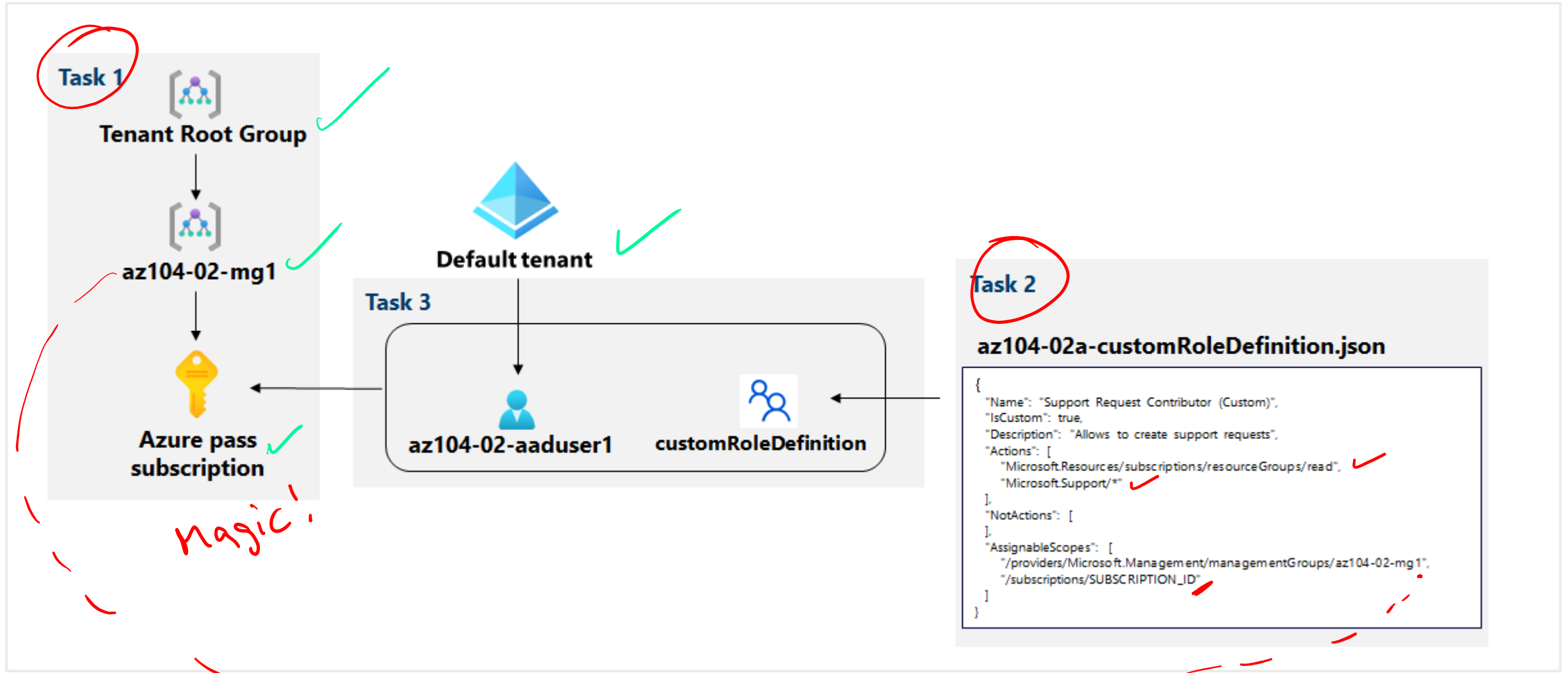
Objectives

Task 1: Implement Management Groups

Task 2: Create custom RBAC roles

Task 3: Assign RBAC roles

Lab 02a – Architecture diagram

Lab 02b – Manage Governance via Azure Policy

Contoso needs to improve the management of Azure resources, specifically:

- Tagging resource groups that include only infrastructure resources

- Ensuring that only properly tagged infrastructure resources can be added to infrastructure resource groups

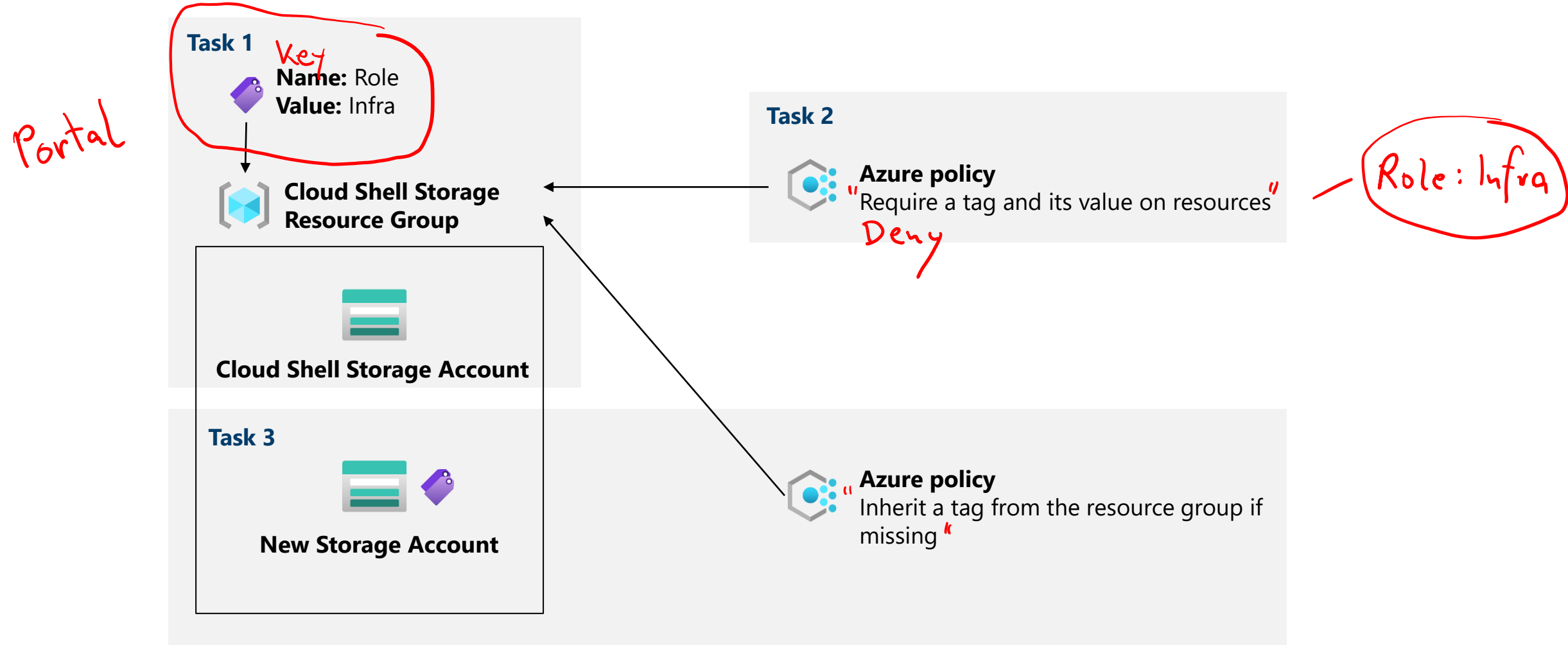- Remediating any non-compliant resources

Objectives

Task 1: Create and assign tags via the Azure portal

Task 2: Enforce tagging with an Azure Policy

Task 3: Apply tagging with an Azure Policy

Next slide for an architecture diagram →

Lab 02b – Architecture diagram

Task 1

Key

Name: Role
Value: Infra

Cloud Shell Storage Resource Group

Cloud Shell Storage Account

Task 3

New Storage Account

Task 2

Azure policy
"Require a tag and its value on resources"

Deny

Azure policy
Inherit a tag from the resource group if missing

Portal

Role : Infra

End of presentation