

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

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



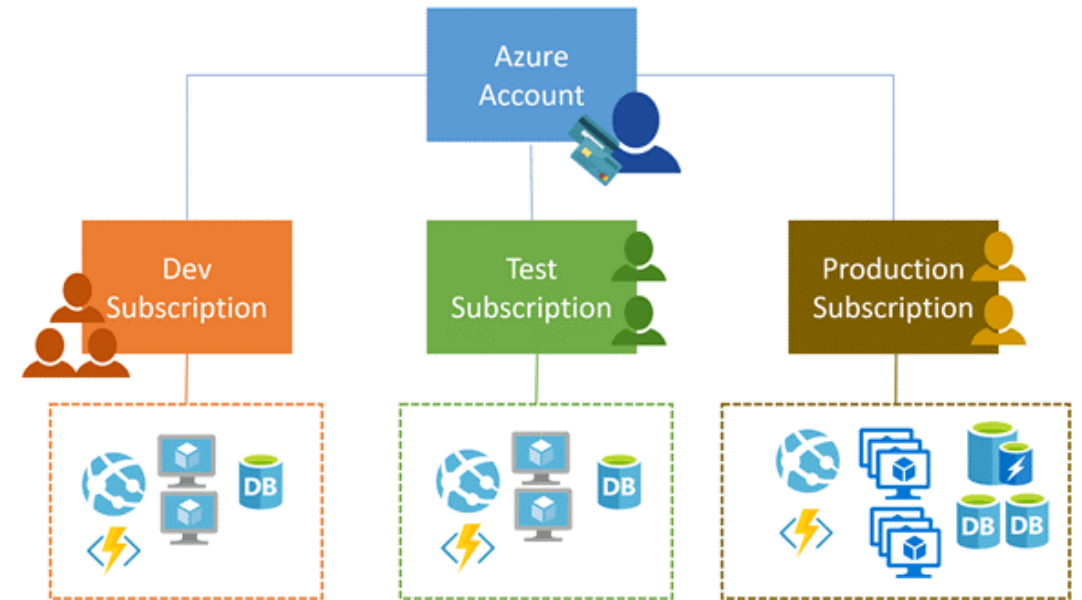
**Worldwide there are 60+ regions
representing 140 countries**

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



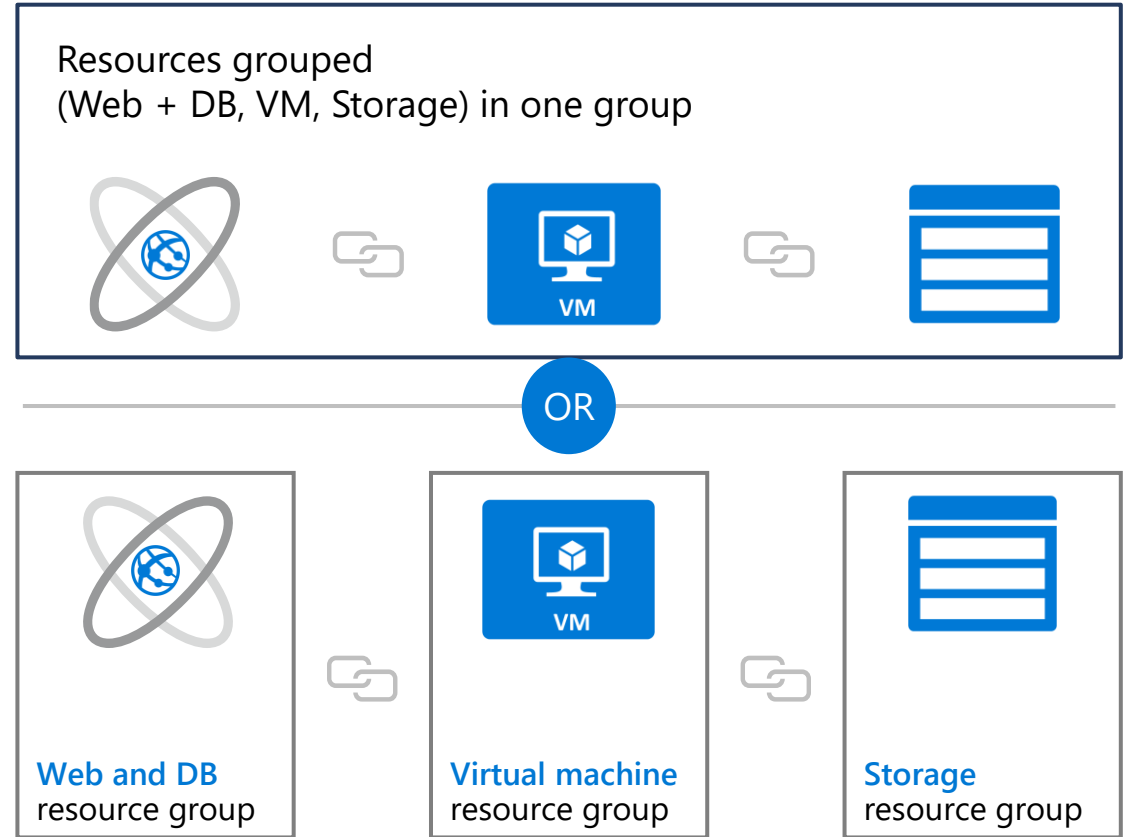
Create Resource Groups

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

You can move resources between groups





Determine Service Limits and Quotas


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
- a subscription quota

Helpful to track current usage,
and plan for future use

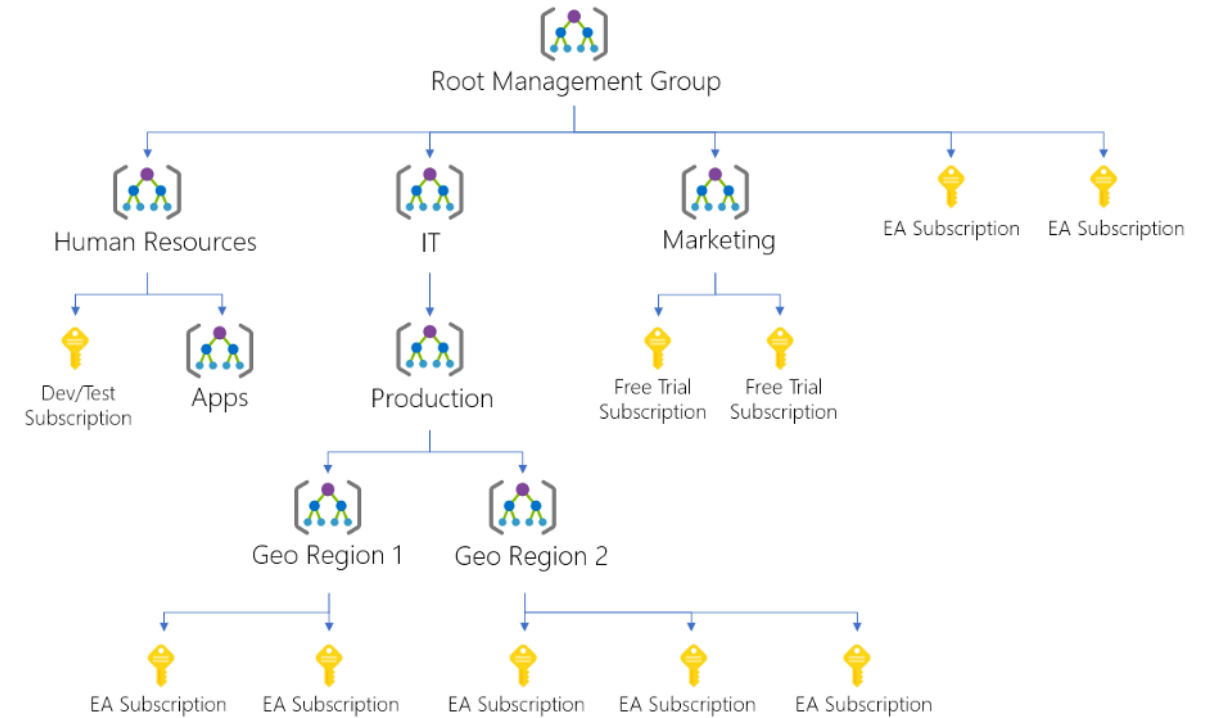
You can open a free support
case to increase limits to
published maximums

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

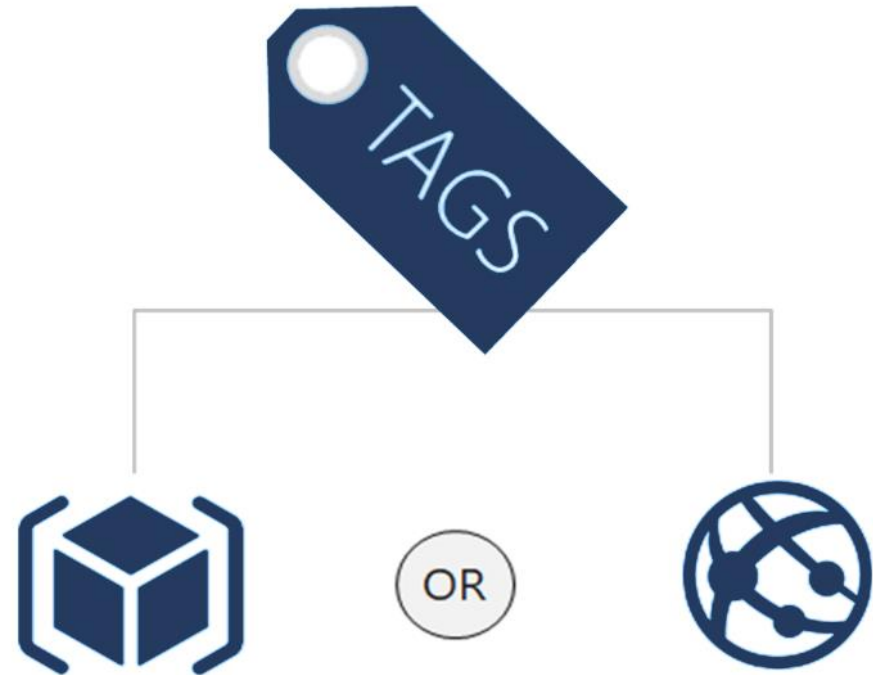
Apply Resource Tagging

Provides metadata for your Azure resources

Logically organizes resources

Consists of a name-value pair

Very useful for rolling up billing information



Owner: Joe
Department: marketing
Environment: production

Cost-center: Marketing

Configure 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

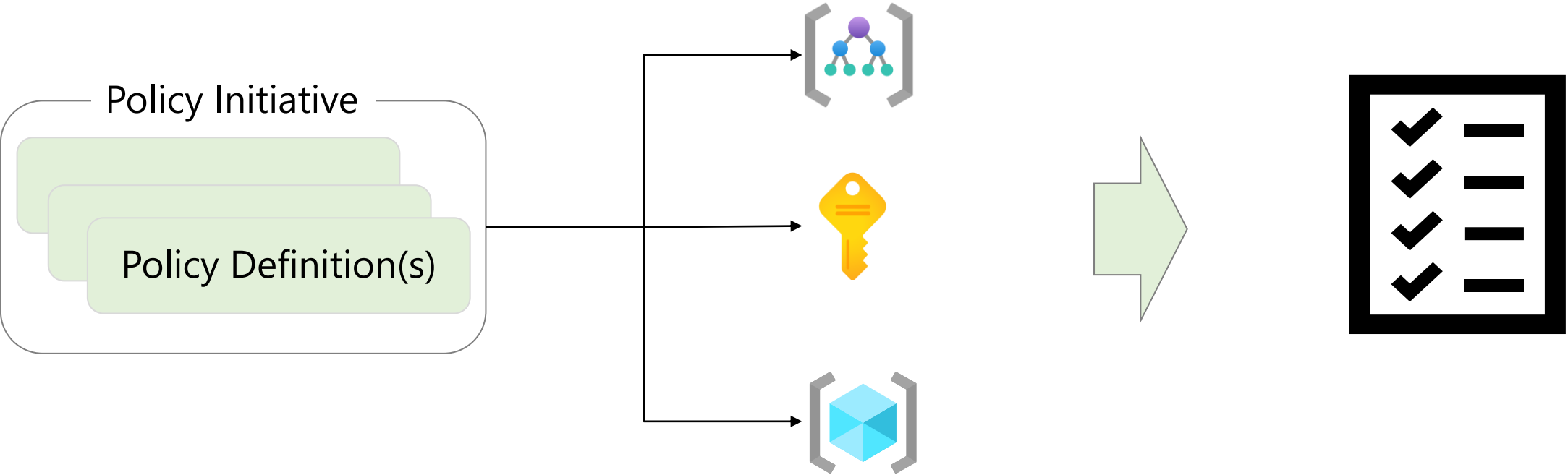
Azure Backup should be enabled for Virtual Machines – Audit if Azure Backup service is enabled for all Virtual machines

Create Azure Policies

Define and create

Scope and assign

Assess compliance



Configure Role-Based Access Control (RBAC)



Compare Azure RBAC Roles to Entra ID Roles

RBAC roles provide fine-grained access management

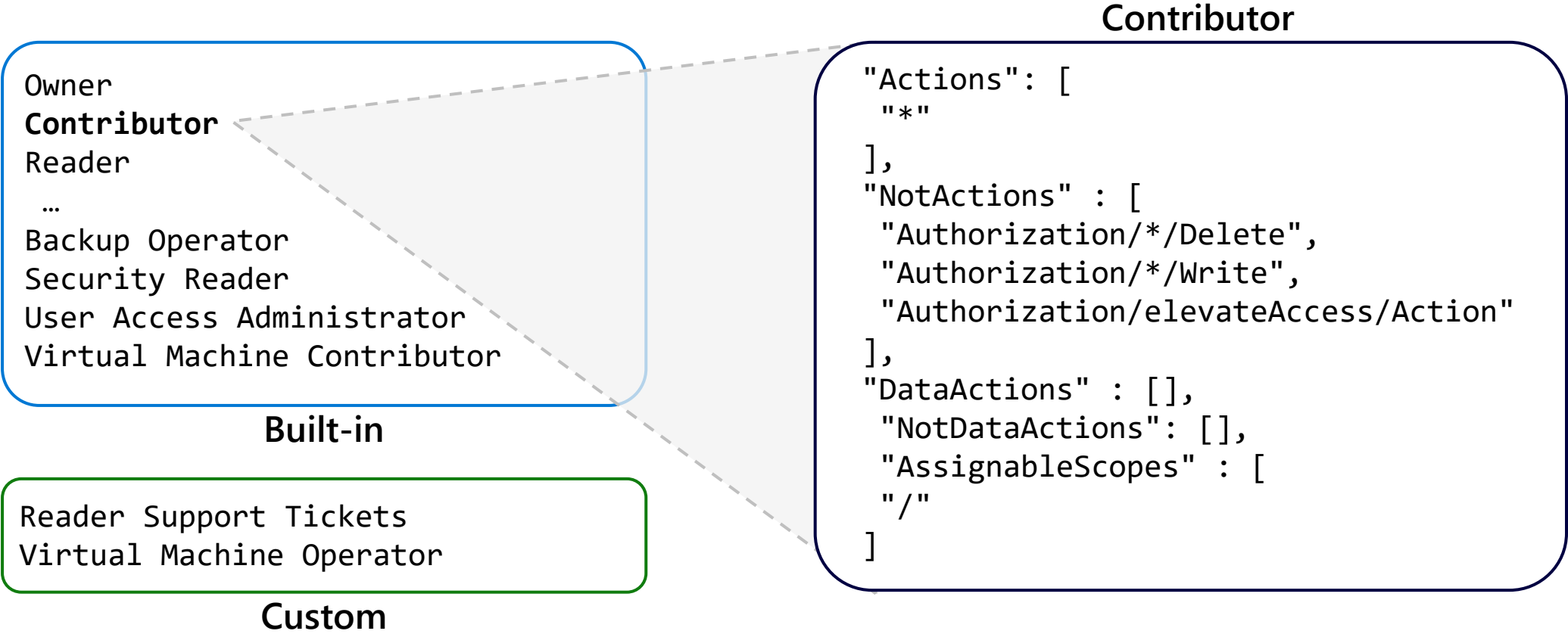
Azure RBAC roles	Entra ID roles
Manage access to Azure resources	Manage access to Entra ID objects
Scope can be specified at multiple levels	Scope is at the tenant level
Role information can be accessed in the Azure portal, Azure CLI, Azure PowerShell, Azure Resource Manager templates, REST API	Role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



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

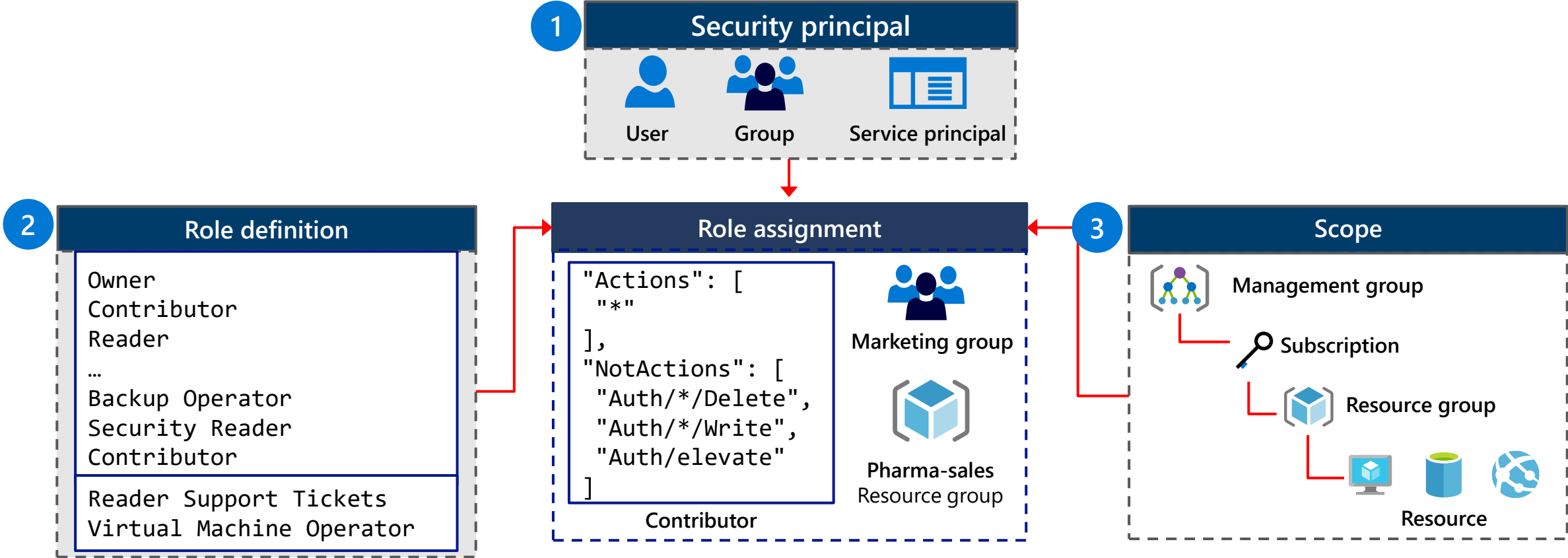
Create a Role Definition

Collection of permissions that lists the operations that can be performed

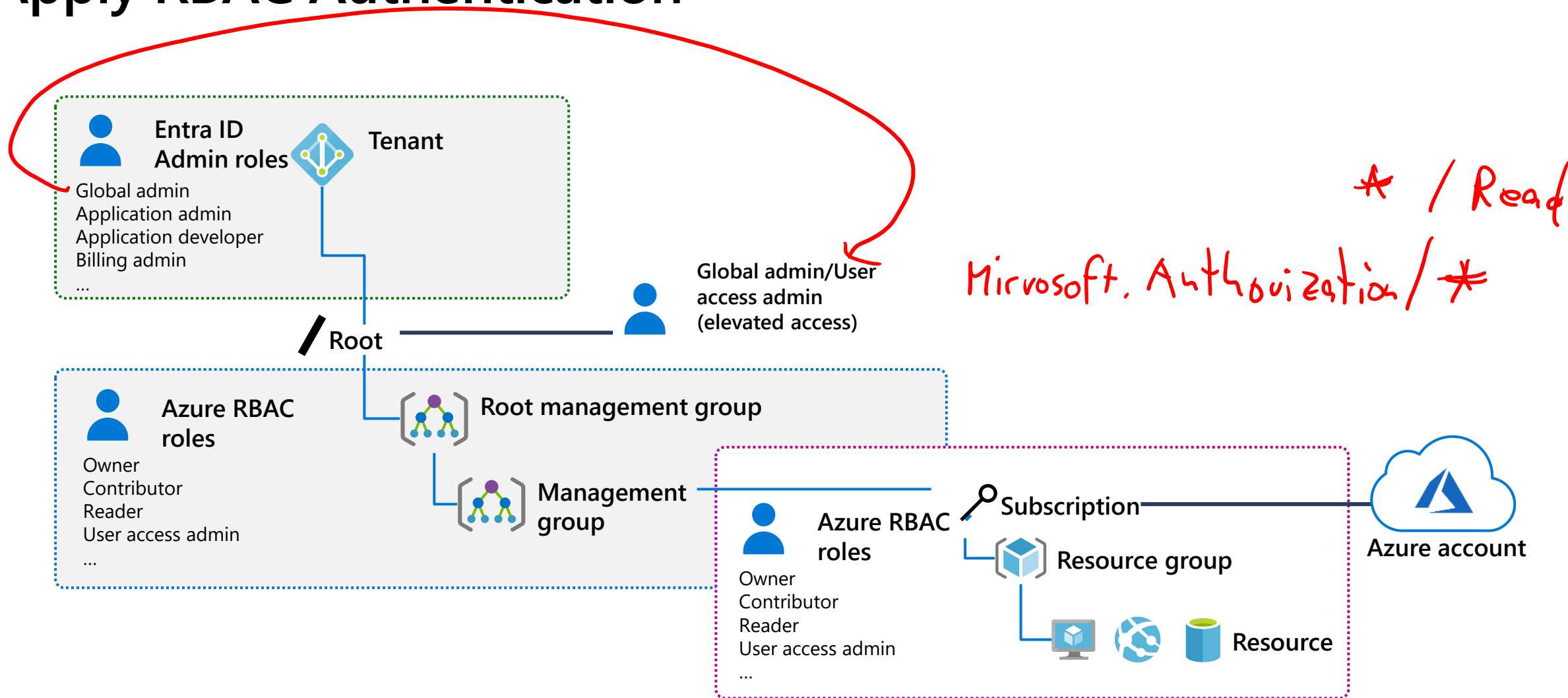


Create a Role Assignment

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



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

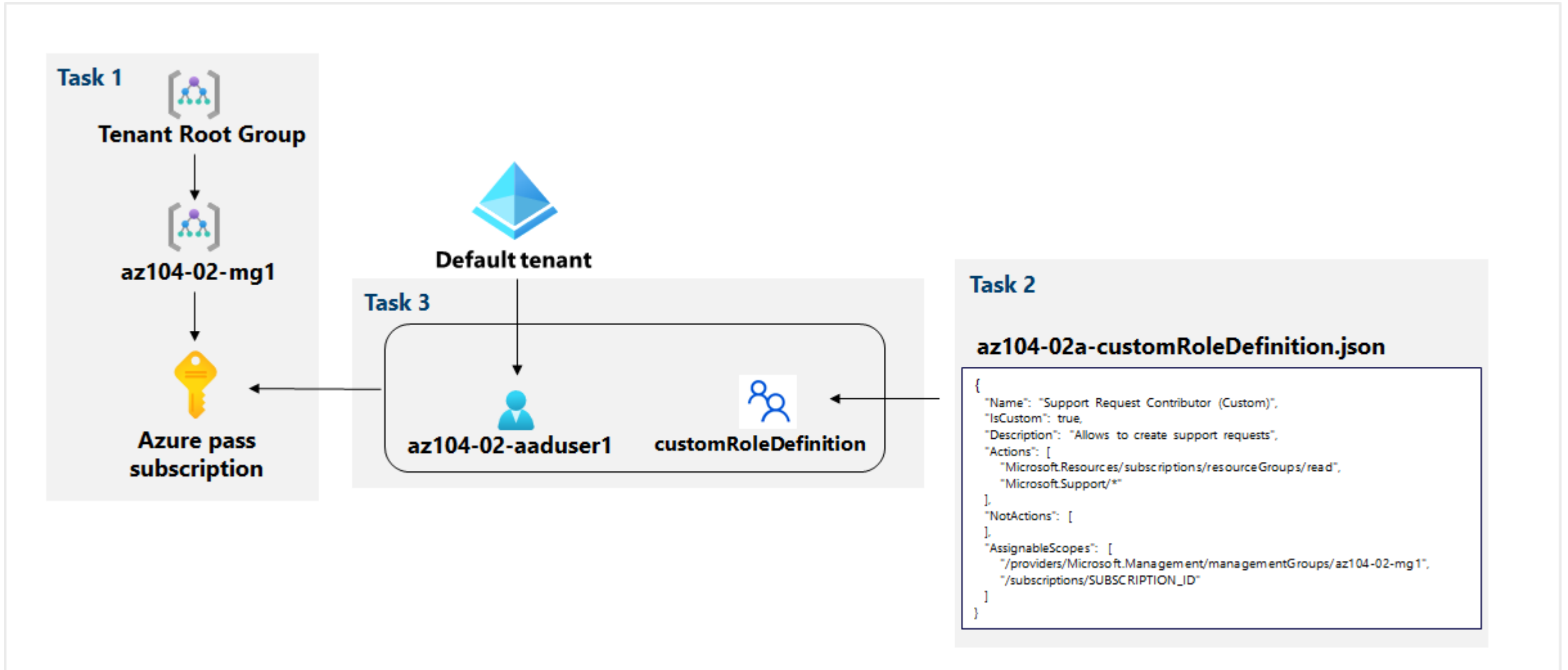
Objectives

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

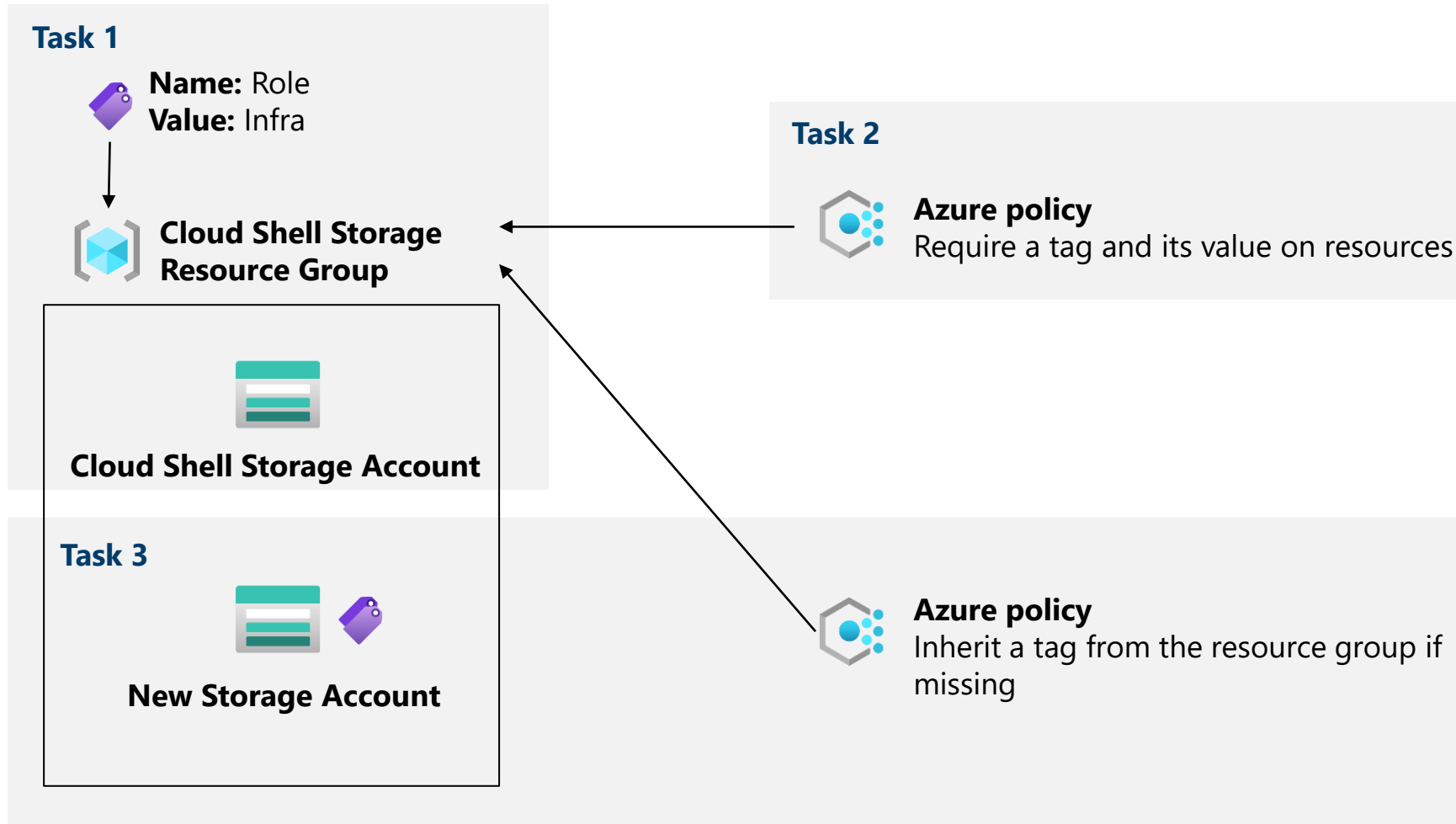
Task 1: Create and assign tags via the Azure portal

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



End of presentation

