brainymotion

smart trainieren.
sicher können.

Modul 6: Identity Services Fundamentals

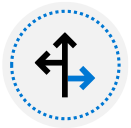
Lesson 1: Overview of AD DS

brainymotion

© Copyright Microsoft Corporation. All rights reserved.

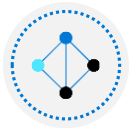
Overview of AD DS

What is AD DS?



AD DS objects

AD DS forests and domains



OUs

AD DS sign-in process

AD DS sign-in process

brainymotion

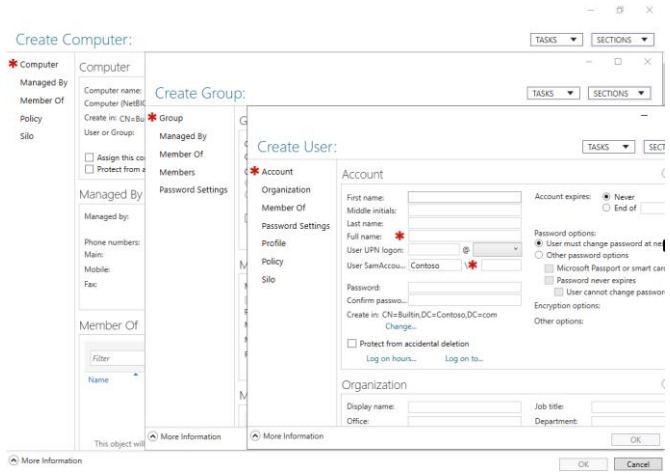
What is AD DS?

AD DS is composed of both logical and physical components

Logical components	Physical components
• Partitions • Schema • Domains • Domain trees • Forests • Sites • OUs • Containers	• Domain controllers • Data stores • Global catalog servers • RODCs

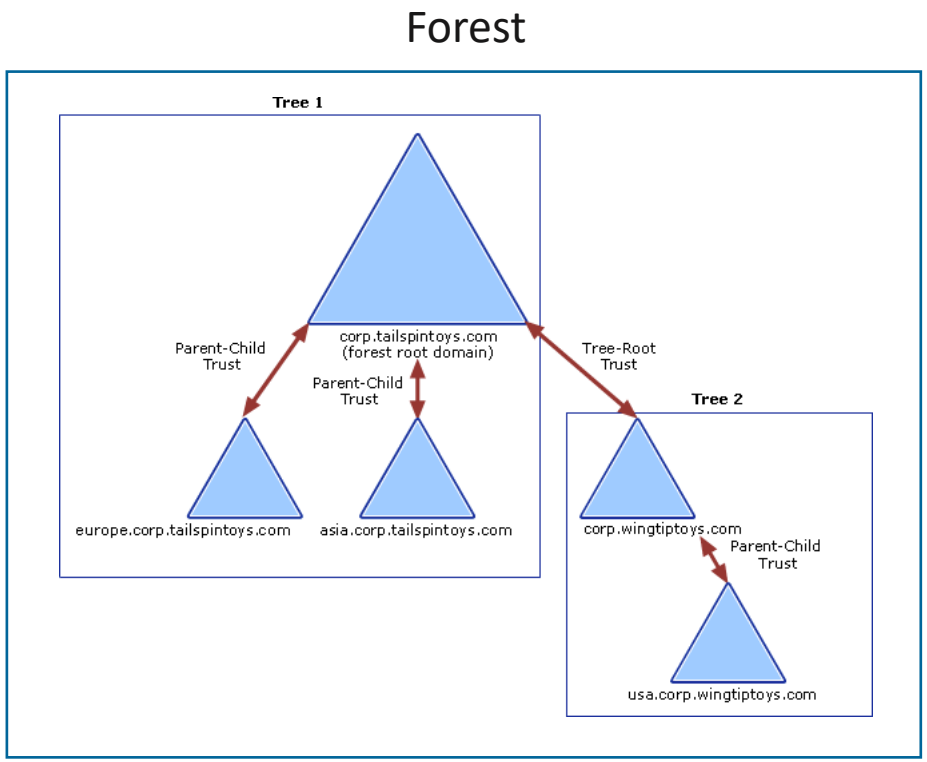
AD DS objects

- User objects
- Group objects
  - Group types: Security and distribution
  - Group scopes: Local, Domain-local, Global, and Universal
- Computer objects



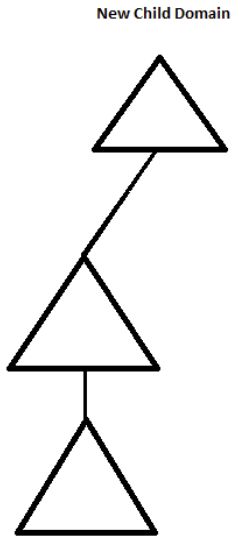
AD DS forests and domains (1 of 2)

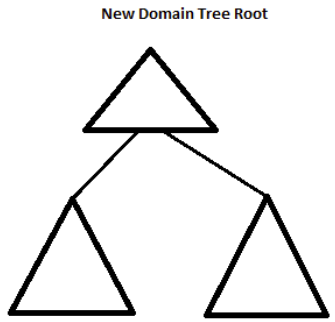
- A forest:
  - Is a security boundary
  - Is a replication boundary
- A domain:
  - Is a replication boundary
  - Is an administrative center
  - Provides:
    - Authentication
    - Authorization



AD DS forests and domains (2 of 2)

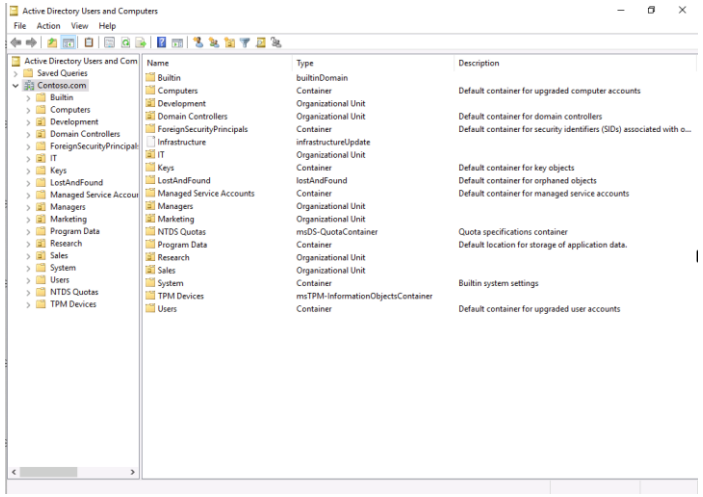
- Trust relationships:
- Provide access to resources in a complex AD DS environment
- Types of trust:
  - Parent and child
  - Tree-root
  - External
  - Realm
  - Forest
  - Shortcut



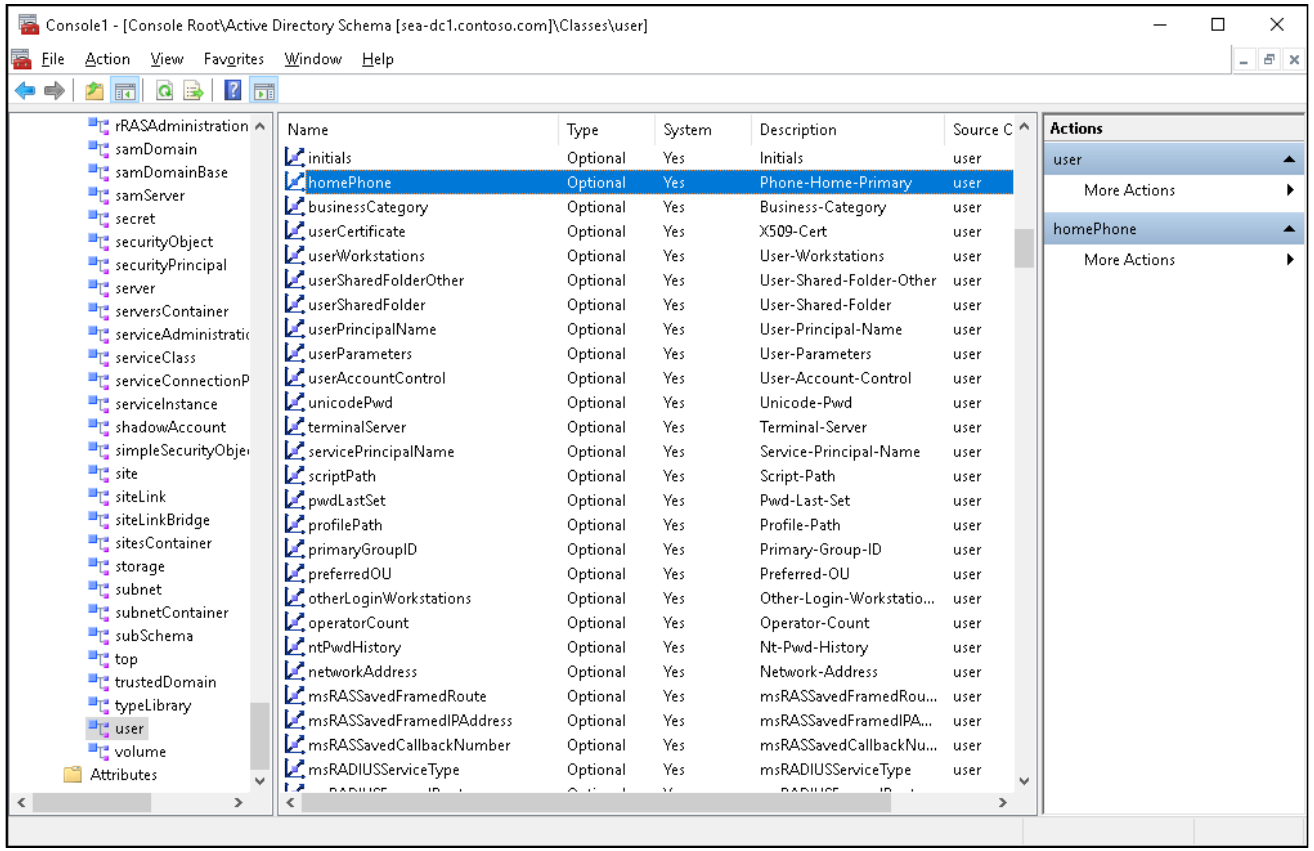


OUs

- Use containers to group objects within a domain:
  - You cannot apply GPOs to containers
  - Containers are used for system objects and as the default location for new objects
- Create OUs to:
  - Configure objects by assigning GPOs to them
  - Delegate administrative permissions



AD DS schema

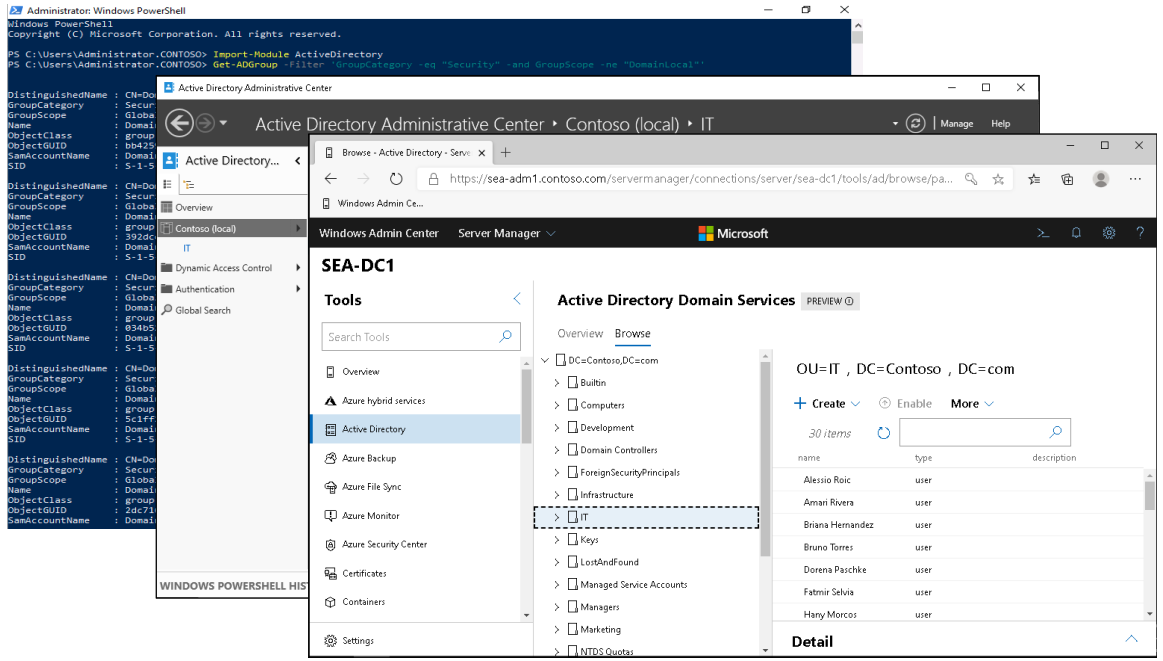

Console1 - [Console Root\Active Directory Schema [sea-dc1.contoso.com]\Classes\user]
File Action View Favorites Window Help
rRASAdministration
samDomain
samDomainBase
samServer
secret
securityObject
securityPrincipal
server
serversContainer
serviceAdministrati
serviceClass
serviceConnectionP
serviceInstance
shadowAccount
simpleSecurityObje
site
siteLink
siteLinkBridge
sitesContainer
storage
subnet
subnetContainer
subSchema
top
trustedDomain
typeLibrary
user
volume
Attributes
Name Type System Description Source C
initials Optional Yes Initials user
homePhone Optional Yes Phone-Home-Primary user
businessCategory Optional Yes Business-Category user
userCertificate Optional Yes X509-Cert user
userWorkstations Optional Yes User-Workstations user
userSharedFolderOther Optional Yes User-Shared-Folder-Other user
userSharedFolder Optional Yes User-Shared-Folder user
userPrincipalName Optional Yes User-Principal-Name user
userParameters Optional Yes User-Parameters user
userAccountControl Optional Yes User-Account-Control user
unicodePwd Optional Yes Unicode-Pwd user
terminalServer Optional Yes Terminal-Server user
servicePrincipalName Optional Yes Service-Principal-Name user
scriptPath Optional Yes Script-Path user
pwdLastSet Optional Yes Pwd-Last-Set user
profilePath Optional Yes Profile-Path user
primaryGroupID Optional Yes Primary-Group-ID user
preferredOU Optional Yes Preferred-OU user
otherLoginWorkstations Optional Yes Other-Login-Workstatio... user
operatorCount Optional Yes Operator-Count user
ntPwdHistory Optional Yes Nt-Pwd-History user
networkAddress Optional Yes Network-Address user
msRASSavedFramedRoute Optional Yes msRASSavedFramedRou... user
msRASSavedFramedIPAddress Optional Yes msRASSavedFramedIPA... user
msRASSavedCallbackNumber Optional Yes msRASSavedCallbackNu... user
msRADIUSServiceType Optional Yes msRADIUSServiceType user
Actions
user
More Actions
homePhone
More Actions

AD DS sign-in process

1. The user account is authenticated to the domain controller
2. The domain controller returns a TGT back to client
3. The client uses the TGT to apply for access to the workstation
4. The domain controller grants access to the workstation
5. The client uses the TGT to apply for access to the server
6. The domain controller returns access to the server

Overview of AD DS administration tools

- Active Directory Users an Computers
- Active Directory Administrative Center
- PowerShell



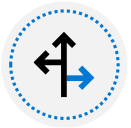
Lesson 2: Deploying Windows Server domain controllers

brainymotion

© Copyright Microsoft Corporation. All rights reserved.

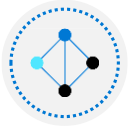
Deploying Windows Server domain controllers

What is a Domain Controller (DC)?



What is the global catalog?

What are operations masters?



Upgrade from a previous version of AD DS

Deploy a DC in Azure IaaS

brainymotion

What is a Domain Controller (DC)?

- Are servers that host the AD DS database (Ntds.dit) and SYSVOL
- Host the Kerberos authentication service and KDC services to perform authentication
- Have best practices for:
  - Availability:
    - Use at least two domain controllers in a domain
  - Security:
    - Use an RODC or BitLocker

What are operations masters?

- In the multimaster replication model, some operations must be single master operations
- Many terms are used for single master operations in AD DS, including:
  - Operations master (or operations master role)
  - Single master role
  - FSMO

The five FSMOs	
Forest: • Domain naming master • Schema master	Domain: • RID master • Infrastructure master • PDC emulator master

Upgrade from a previous version of AD DS

You have two options for upgrading AD DS to Windows Server 2019:

- Perform an in-place upgrade from Windows Server 2012 R2 or later to Windows Server 2019:
  - Benefit. Except for the prerequisite checks, all the files and programs stay in place, and no additional work is required
  - Risk. It might leave obsolete files and dynamic-link libraries
- Introduce a new server running Windows Server 2019 into the domain, and then promote it to be a domain controller (this option is usually preferred):
  - Benefit. The new server has no obsolete files and settings
  - Risk. It might require additional work to migrate administrators' files and settings

Deploy a DC in Azure IaaS

- Scenarios in which you might deploy AD DS on an Azure virtual machine include:
  - Disaster recovery
  - Geo-distributed domain controllers
  - User authentication for isolated applications
- Considerations during deployment include:
  - Network topology
  - Site topology
  - Service healing
  - IP addressing
  - DNS
  - Hard disk read/write caching

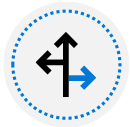
Lesson 3: Implementing Group Policy

brainymotion

© Copyright Microsoft Corporation. All rights reserved.

Implementing Group Policy

What are GPOs?



Overview of GPO scope and inheritance

Default domain GPOs

brainymotion

What are GPOs?

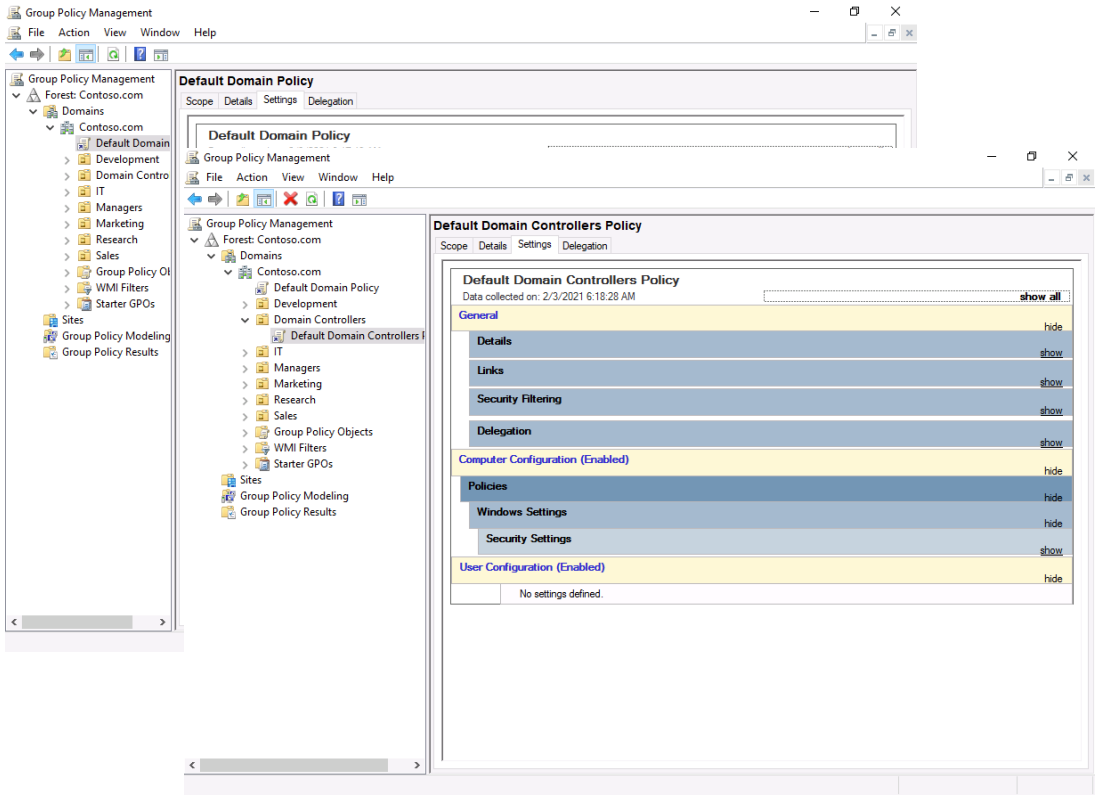
- Group Policy is a powerful administrative tool
- You can use it to enforce various types of settings to a large number of users and computers
- Typically, you use GPOs to:
  - Apply security settings
  - Manage desktop application settings
  - Deploy application software
  - Manage Folder Redirection
  - Configure network settings

Overview of GPO scope and inheritance

- You can scope GPOs by using:
  - GPO links
  - Security filters
  - WMI filters
- GPOs are processed on a client computer in the following order:
  1. Local GPOs
  2. Site-level GPOs
  3. Domain-level GPOs
  4. OU GPOs, including any nested (child) OUs

Default domain GPOs

- A domain has two default GPOs:
  - Default Domain Policy
  - Default Domain Controllers Policy



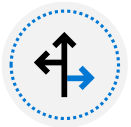
Lesson 4: Azure Active Directory

brainymotion

© Copyright Microsoft Corporation. All rights reserved.

Azure Active Directory

Configure Azure Active Directory



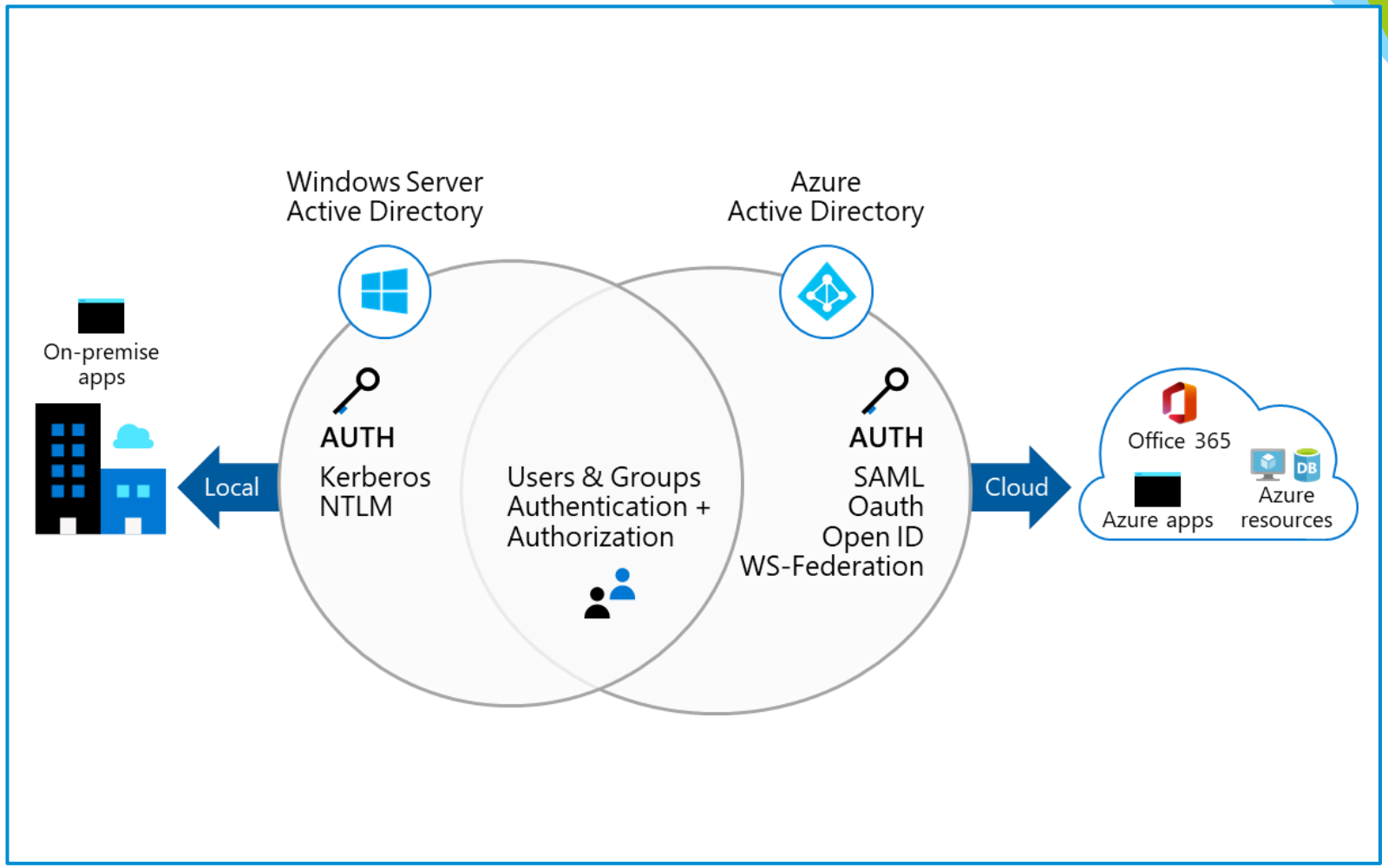
Configure User and Group Accounts

brainymotion

Describe Azure Active Directory Benefits and Features

A cloud-based suite of identity management capabilities that enables you to securely manage access to Azure services and resources for your users

Provides application management, authentication, device management, and hybrid identity



brainymotion

Describe Azure AD Concepts

Concept	Description
Identity	An object that can be authenticated
Account	An identity that has data associated with it
Azure AD account	An identity created through Azure AD or another Microsoft cloud service
Azure AD tenant/directory	A dedicated and trusted instance of Azure AD, a Tenant is automatically created when your organization signs up for a Microsoft cloud service subscription • Additional instances of Azure AD can be created • Azure AD is the underlying product providing the identity service • The term *Tenant* means a single instance of Azure AD representing a single organization • The terms *Tenant* and *Directory* are often used interchangeably
Azure subscription	Used to pay for Azure cloud services

Compare AD DS to Azure Active Directory

Azure AD is primarily an identity solution, and designed for HTTP and HTTPS communications

Queried using the REST API over HTTP and HTTPS. Instead of LDAP

Uses HTTP and HTTPS protocols such as SAML, WS-Federation, and OpenID Connect for authentication (and OAuth for authorization). Instead of Kerberos

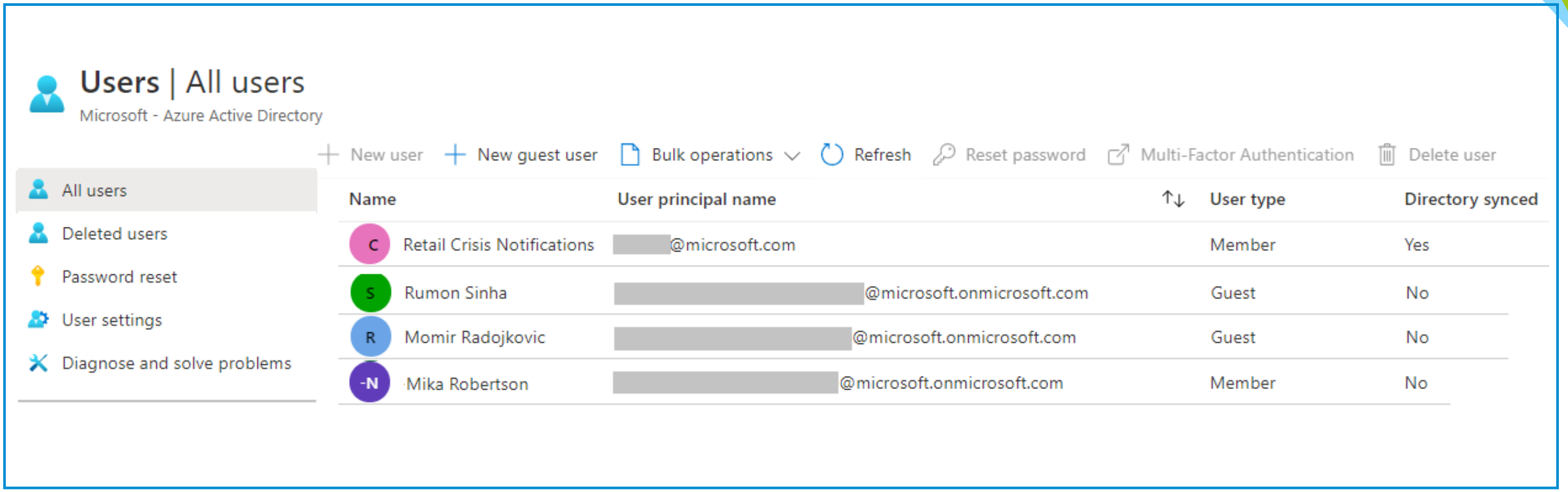
Includes federation services, and many third-party services (such as Facebook)

Azure AD users and groups are created in a flat structure, and there are no Organizational Units (OUs) or Group Policy Objects (GPOs)

Select Azure Active Directory Editions

Feature	Free	Microsoft 365 Apps	Premium P1	Premium P2
Directory Objects	500,000 objects	No object limit	No object limit	No object limit
Single Sign-On	Unlimited	Unlimited	Unlimited	Unlimited
Core Identity and Access	X	X	X	X
B2B Collaboration	X	X	X	X
Identity & Access for O365		X	X	X
Premium Features			X	X
Hybrid Identities			X	X
Advanced Group Access			X	X
Conditional Access			X	X
Identity Protection				X
Identity Governance				X

Create User Accounts



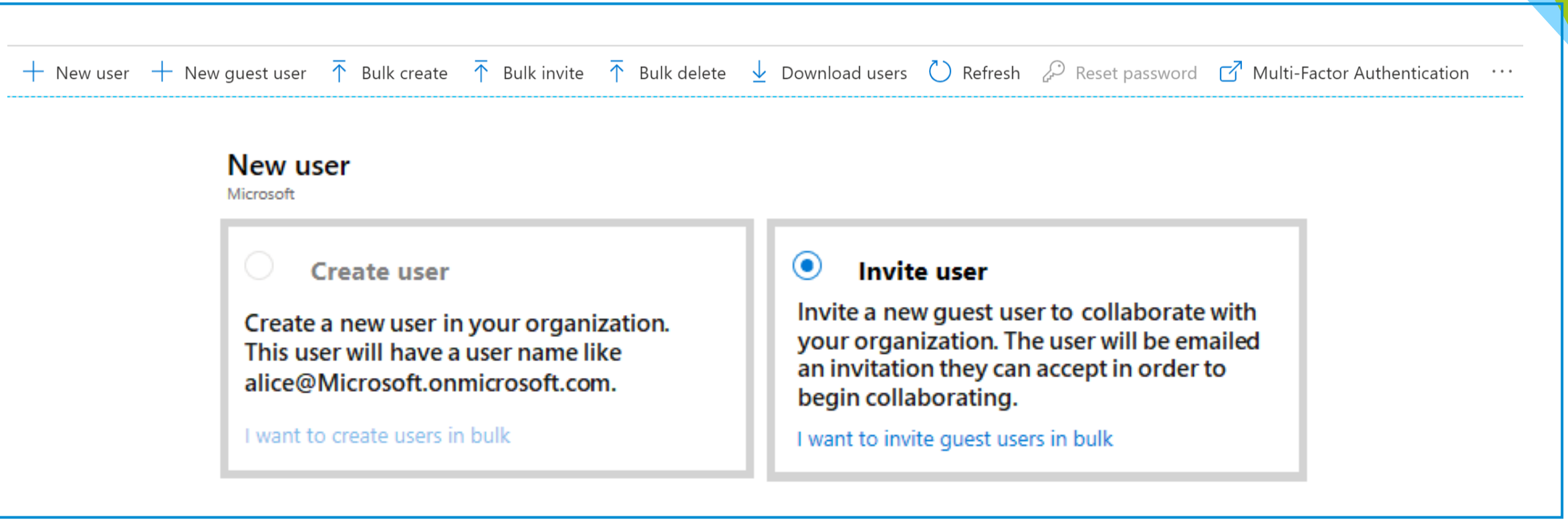
All users must have an account

The account is used for authentication and authorization

Each user account has additional properties

brainymotion

Manage User Accounts



Must be Global Administrator or User Administrator to manage users

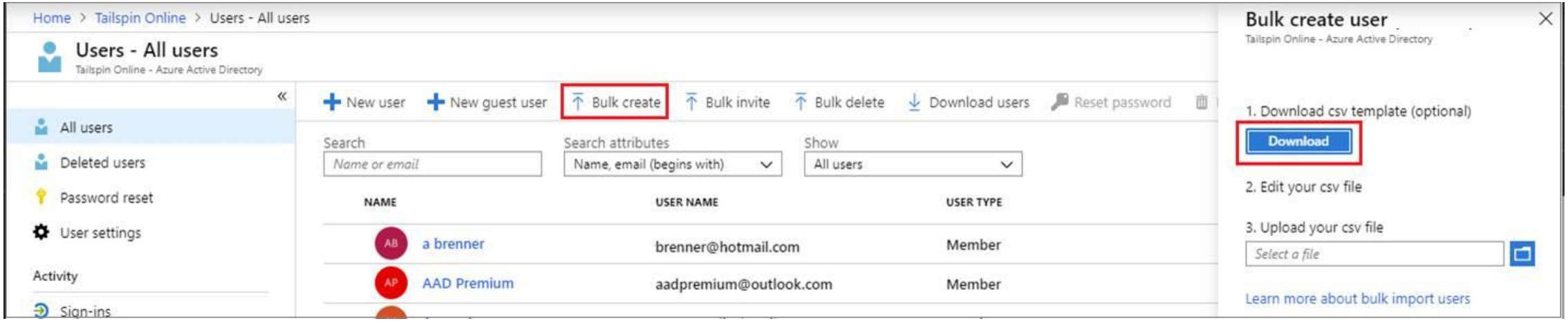
User profile (picture, job, contact info) is optional

Deleted users can be restored for 30 days

Sign in and audit log information is available

brainymotion

Create Bulk User Accounts



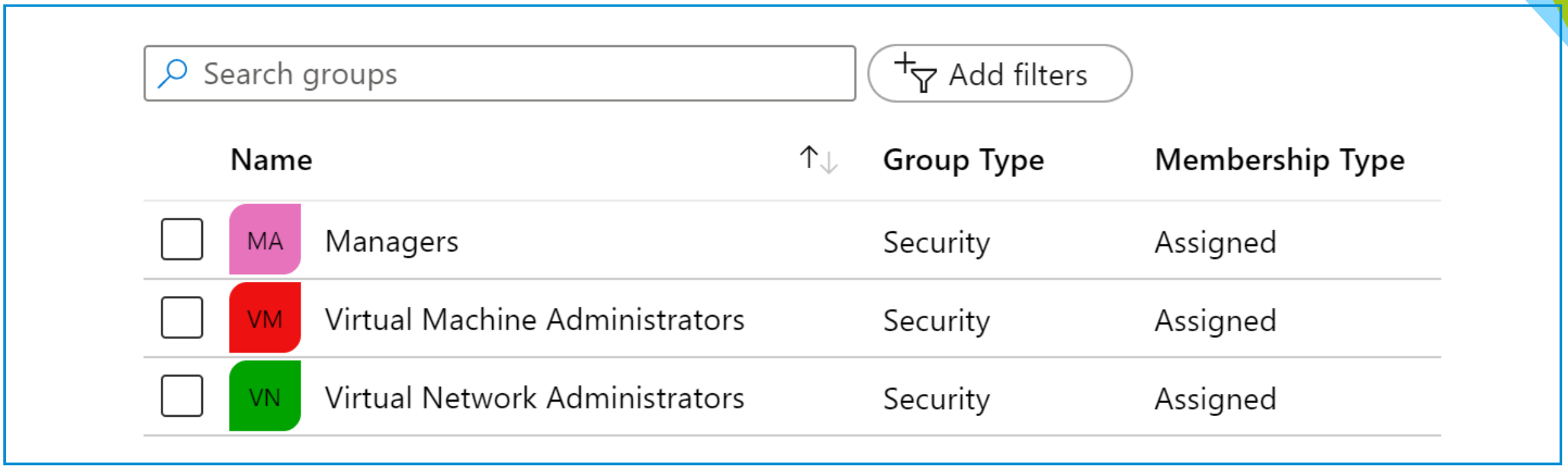
Azure AD supports bulk user create, delete, and list

Create the comma-separated values (CSV) template you can download from the Portal

Must be signed in as a Global administrator or User administrator

brainymotion

Create Group Accounts



Group Types

- Security groups
- Microsoft 365 groups

Assignment Types

- Assigned
- Dynamic User
- Dynamic Device (Security groups only)

brainymotion

Lesson 5: Configure Azure Policy

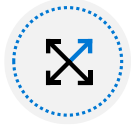
brainymotion

© Copyright Microsoft Corporation. All rights reserved.

Configure Azure Policy

Create Management Groups

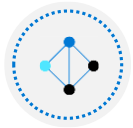
Implement Azure Policy



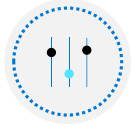
Create Azure Policies

Create Policy Definitions

Create Initiative Definitions



Scope the Initiative Definition



Determine Compliance

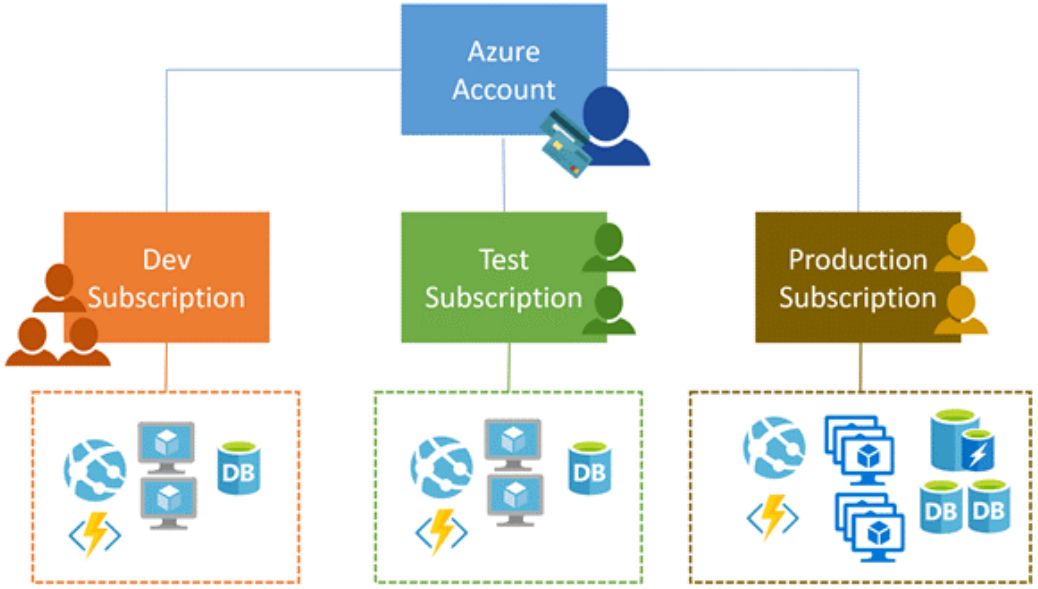
brainymotion

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



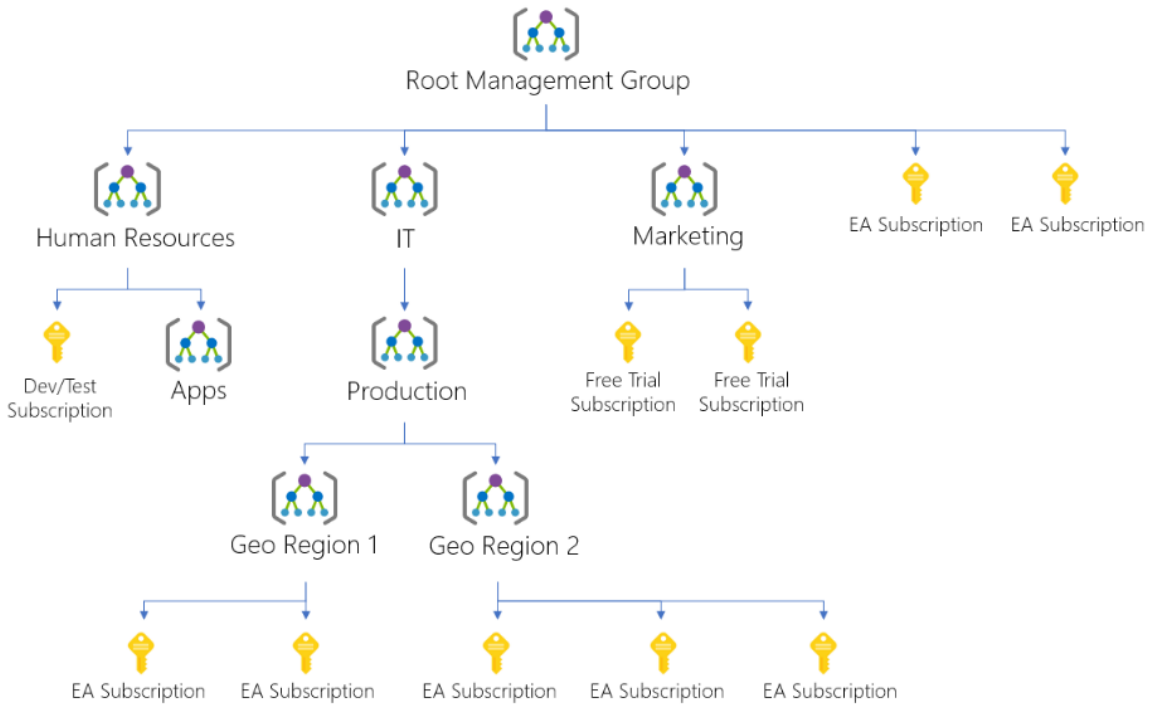
brainymotion

Create 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)



brainymotion

Implement Azure Policies

A service to create, assign, and manage policies

Runs evaluations and scans for non-compliant resources

Advantages:

Enforcement and compliance

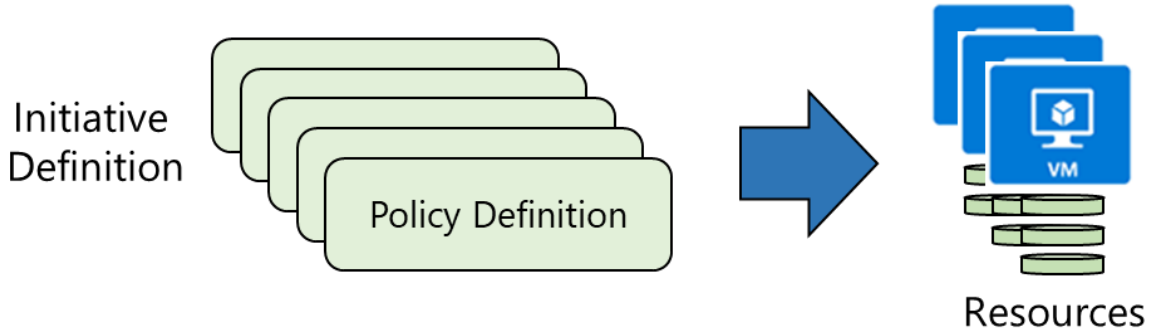
Apply policies at scale

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



brainymotion

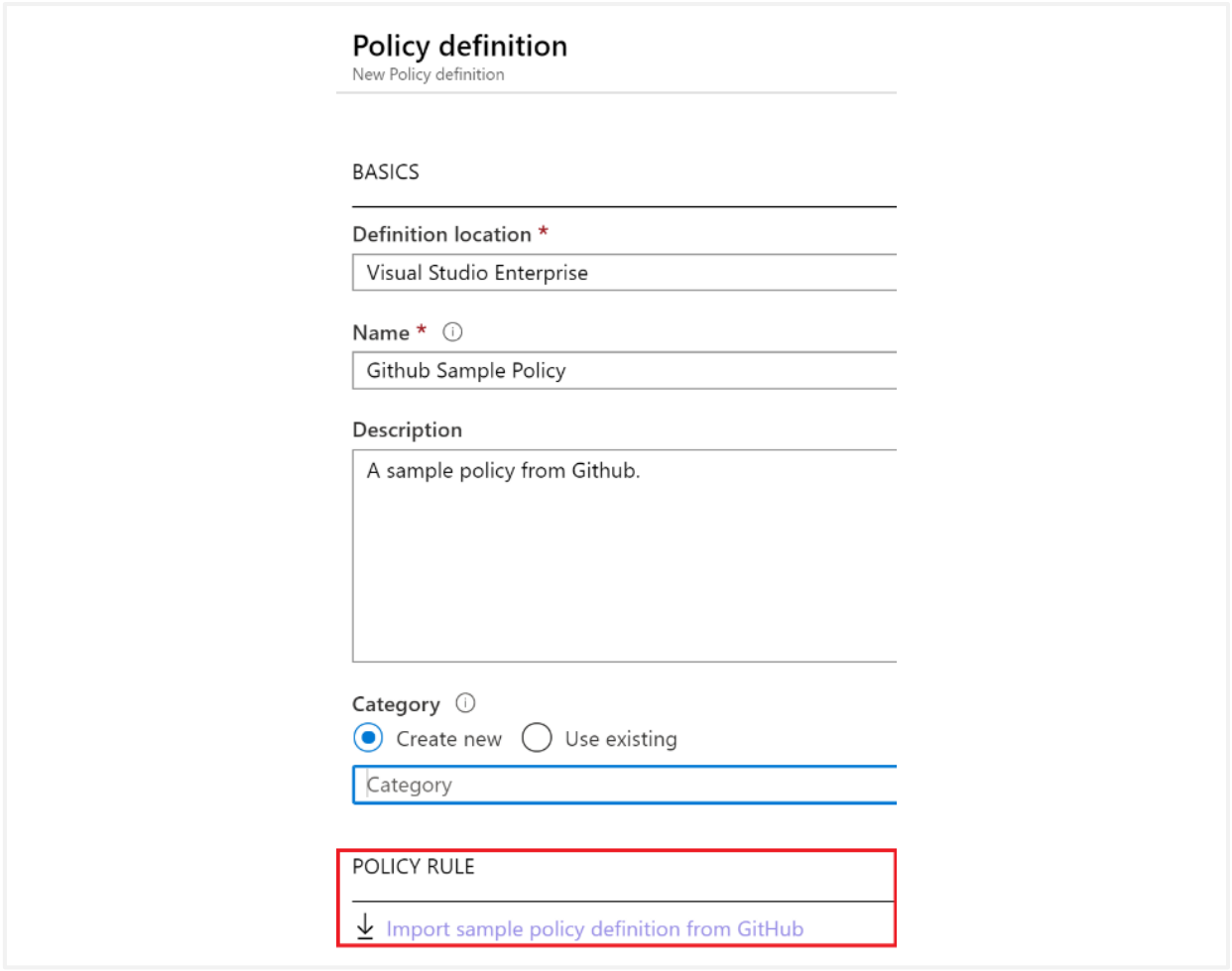
1. Create Policy Definitions

Many policy definitions are available

You can import policies from GitHub

Policy Definitions have a specific JSON format

You can create custom policy definitions



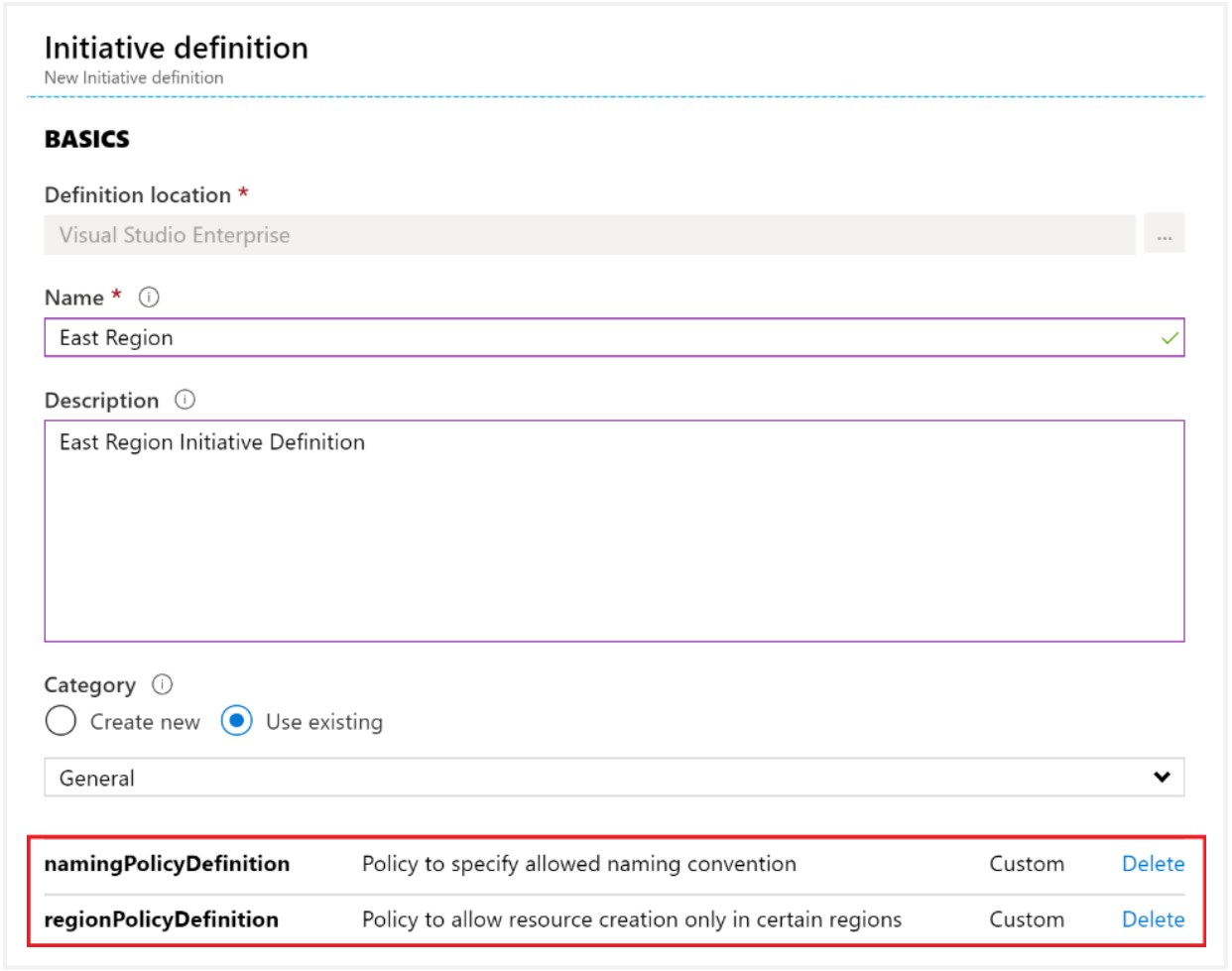
brainymotion

2. Create Initiative Definitions

Group policy definitions

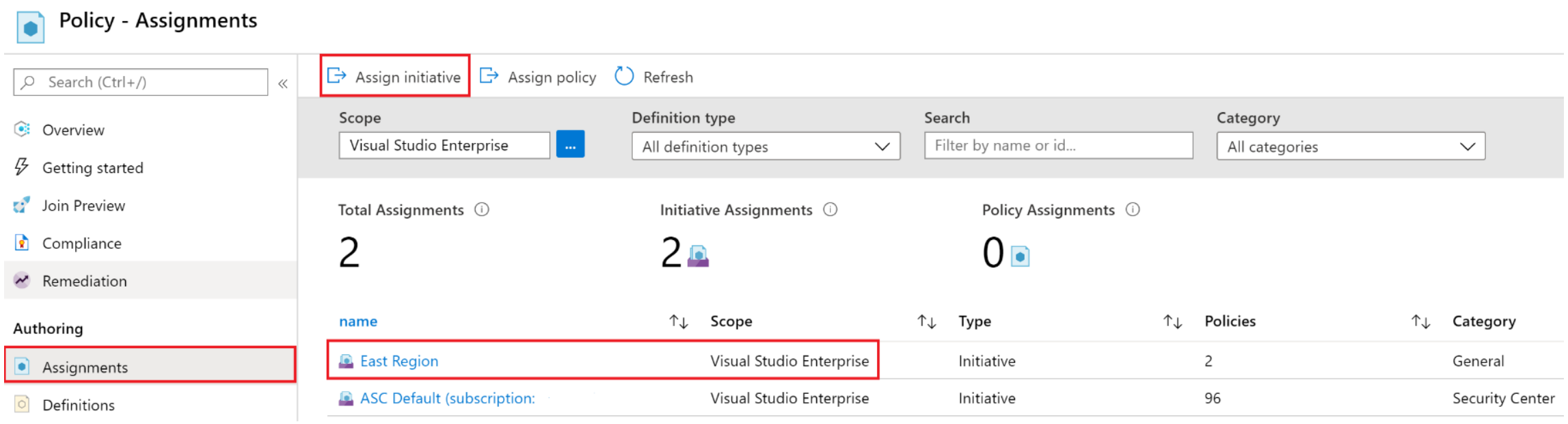
Include one or more policies

Requires planning



brainymotion

3. Scope the Initiative Definition



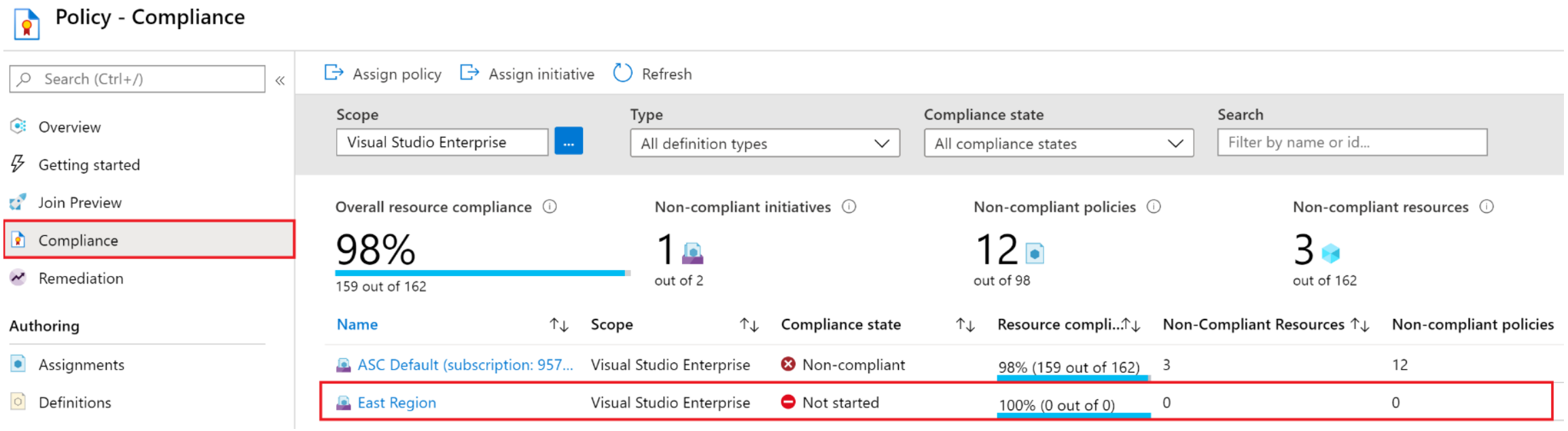
Assign the definition to a scope

The scope enforces the policy

Select the subscription, and optionally the resource group

brainymotion

4. Determine Compliance



Non-compliant initiatives

Non-compliant policies

Non-compliant resources

brainymotion

Lesson 5: Configure Role-Based Access Control

brainymotion

© Copyright Microsoft Corporation. All rights reserved.

Configure Role-Based Access Control Introduction

Implement Role-Based Access Control

Create a Role Definition

Create a Role Assignment

Compare Azure RBAC Roles to Azure AD Roles

Apply RBAC Authentication

Determine Azure RBAC Roles

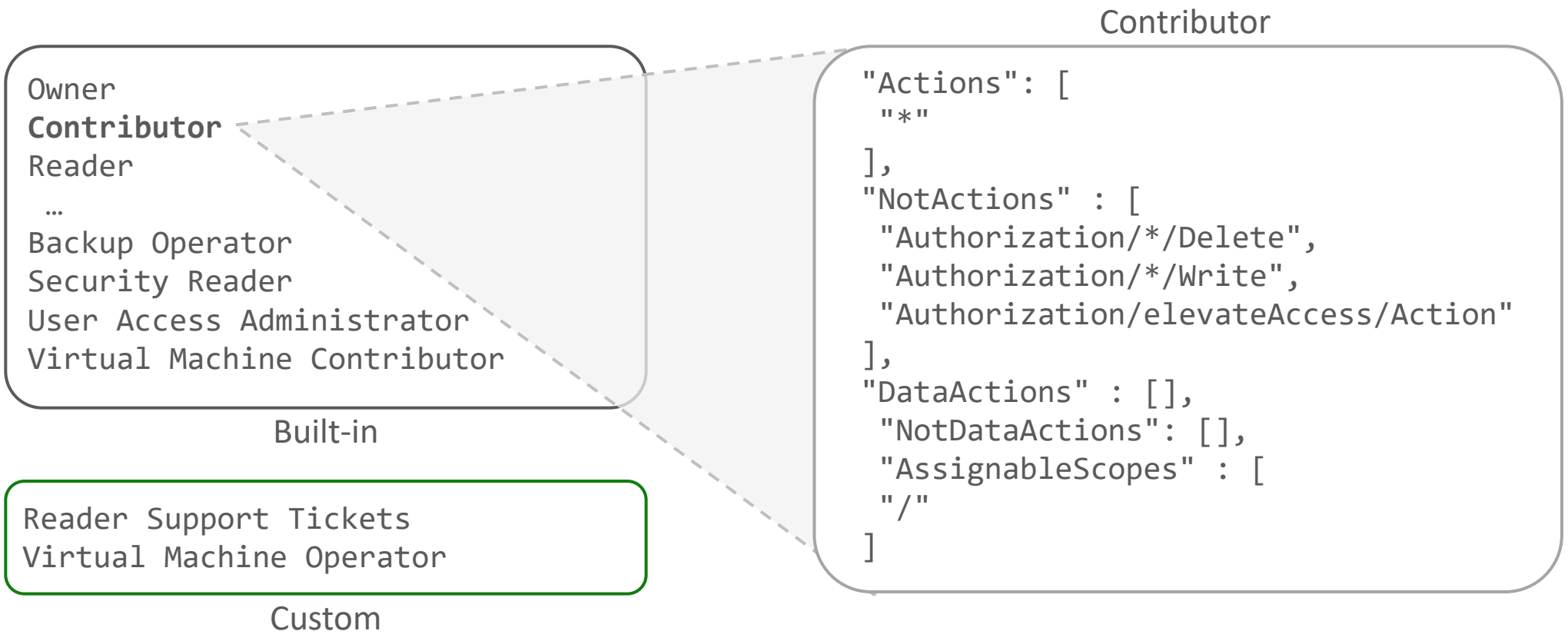
brainymotion

Implement Role-Based Access Control

Provides fine-grained access management of resources in Azure	Concepts
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	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

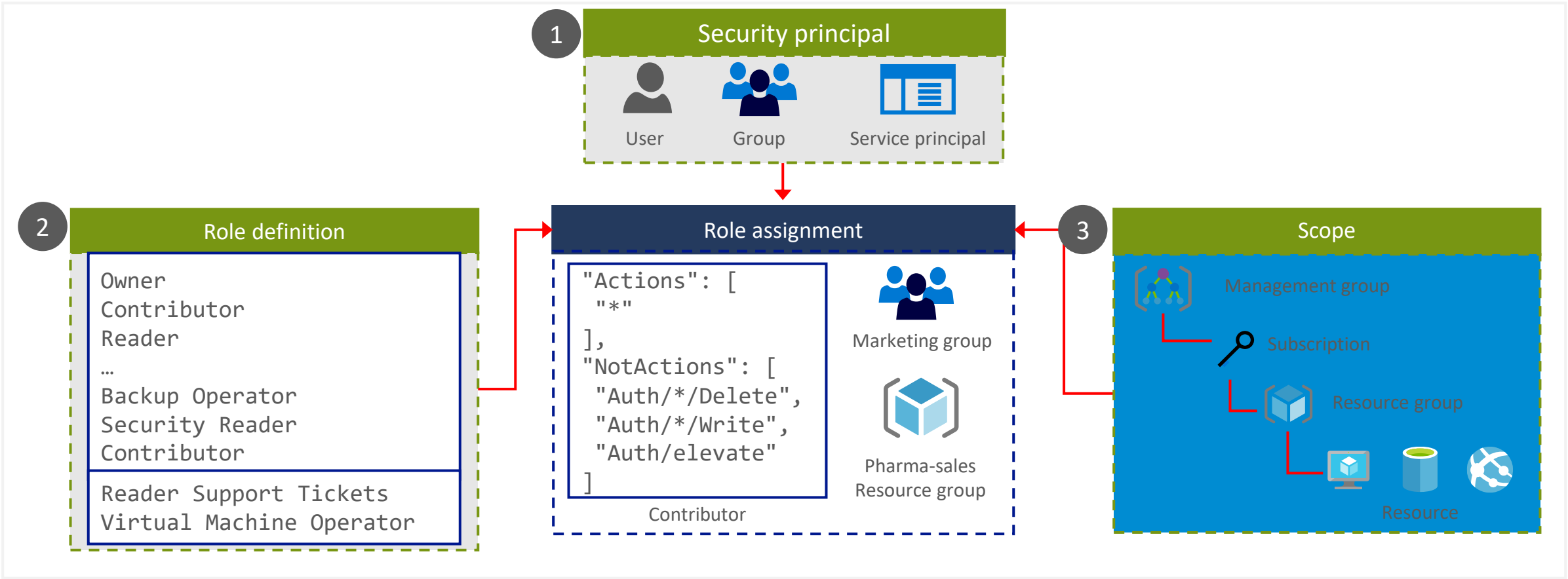
Create a Role Definition

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



brainymotion

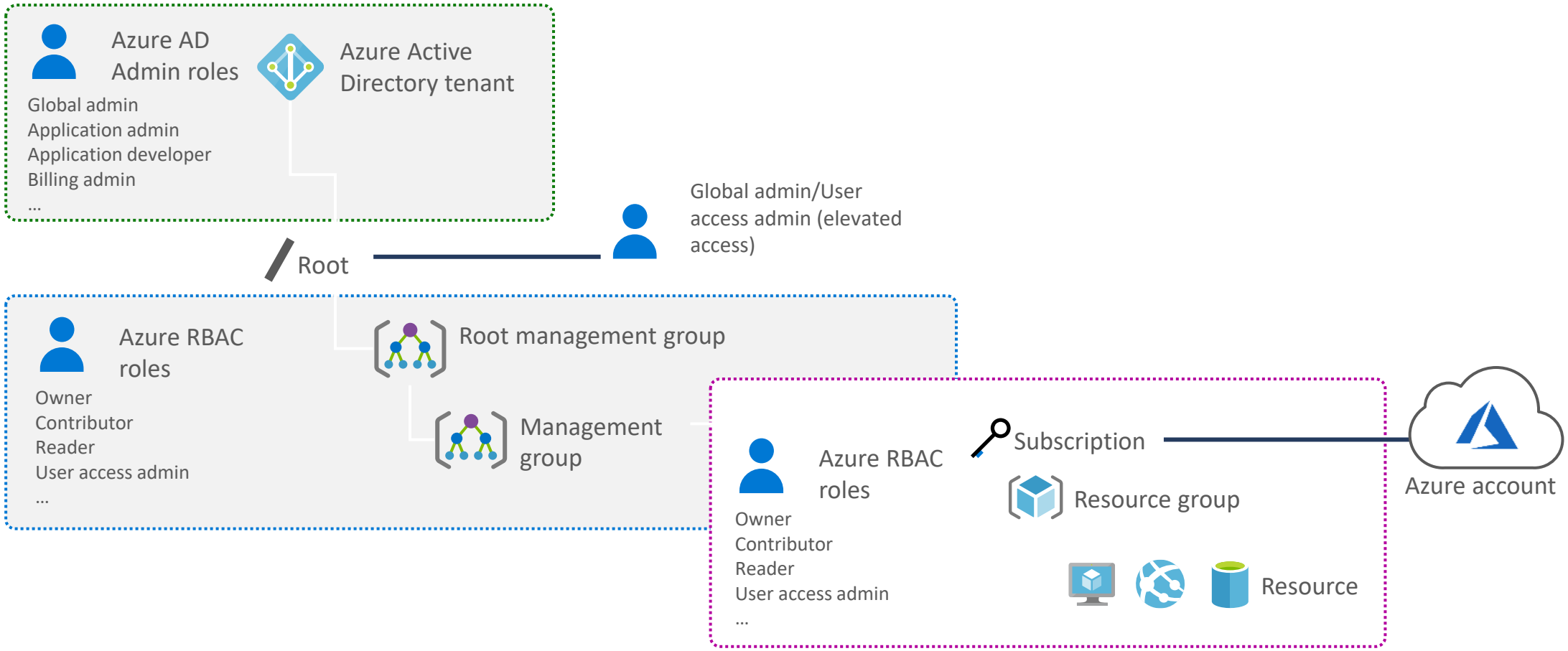
Compare Azure RBAC Roles to Azure AD Roles

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

Apply RBAC Authentication



brainymotion

brainymotion

The End