Exam Alert: Manage Azure Identities and Governance

MANAGE AZURE IDENTITIES AND GOVERNANCE “NEED TO KNOW” EXAM INFORMATION

Michael Teske
AUTHOR EVANGELIST- PLURALSIGHT

@teskemj

Exam Breakdown of Functional Group

Manage Azure identities and governance (15-20%)

- Manage AD objects
- Manage role-based access control
- Manage subscriptions and governance

Manage AD Objects

Manage AD Objects

Skills measured

- Create users and groups
- Manage user and group properties
- Manage device settings
- Perform bulk user updates
- Manage guest accounts
- Configure Azure AD Join
- Configure self-service password reset

Create users and groups

Cloud identities

- Local Azure AD
- External Azure AD

Hybrid identities

- Directory-synchronized

Guest identities

- Azure AD B2B collaboration
- External identities

User or Global Administrator role

Create Azure Active Directory User

```
Install-Module -Name AzureAD

Connect-AzureAD

$PasswordProfile = New-Object `
    -TypeName Microsoft.Open.AzureAD.Model.PasswordProfile
$PasswordProfile.Password = "P@ssw0rd8!"
$PasswordProfile.EnforceChangePasswordPolicy = $true

New-AzureADUser -DisplayName "Pat Smith" -PasswordProfile $PasswordProfile `
    -UserPrincipalName "pats@timw.info" -AccountEnabled $true
```

Create Azure Active Directory User

```
Install-Module -Name AzureAD

Connect-AzureAD

$PasswordProfile = New-Object `
    -TypeName Microsoft.Open.AzureAD.Model.PasswordProfile
$PasswordProfile.Password = "P@ssw0rd8!"
$PasswordProfile.EnforceChangePasswordPolicy = $true

New-AzureADUser -DisplayName "Pat Smith" -PasswordProfile $PasswordProfile `
    -UserPrincipalName "pats@timw.info" -AccountEnabled $true
```

Create Azure Active Directory User

```
Install-Module -Name AzureAD

Connect-AzureAD


$PasswordProfile = New-Object `

    -TypeName Microsoft.Open.AzureAD.Model.PasswordProfile

$PasswordProfile.Password = "P@ssw0rd8!"

$PasswordProfile.EnforceChangePasswordPolicy = $true


New-AzureADUser -DisplayName "Pat Smith" -PasswordProfile $PasswordProfile `

    -UserPrincipalName "pats@timw.info" -AccountEnabled $true
```

Group

- Bulk add using CSV template in the portal

Dynamic Group

- Rule based assignment
- Can be group-assigned roles and licenses
- Cannot manually add users/devices

Manage user and group properties

Modify user profile in the portal

Modify group properties in the portal

Modify using PowerShell

- AzureAD module

User Administrator or Global Administrator role

Manage device settings

Cloud device administrator

- Add, Enable, disable, delete devices in Azure AD
- Cannot modify properties

Device administrator

- Local machine administrator, cannot modify object in Azure AD

Perform bulk user updates

Bulk add to groups using CSV template in the portal

Programmatically using PowerShell

Manage guest accounts

Requires Azure AD Premium P2

Guest identities

- Azure AD B2B collaboration
- External identities

Can be invited by:

- Administrators
- Users

Roles required for guest review

- Global administrator
- User administrator

Configure Azure AD join

Azure AD Join Options

Azure AD Registered	Azure AD Joined
Personally owned device	Organization owned device
MSA or local account sign-in	Azure AD sign-in
Windows 10	Windows 10
iOS	Windows Server 2019 VMs in Azure
Android	
macOS	

Configure self-service password reset

Configure self-service password reset

	Azure AD Free	Azure AD Premium P1 or P2
Cloud-only password change	✸	✸
Cloud-only password reset		✸
Hybrid password change or reset with on-prem writeback		✸

Manage role-based access control “Need to Know”

Michael Teske

AUTHOR EVANGELIST-CLOUD ENGINEER, PLURALSIGHT

@teskemj

Manage Role-Based Access Control

Skills Measured

- Provide access to Azure resources by assigning roles
- Interpret access assignments
- Create a custom role

Provide access to Azure resources by assigning roles

Security Principals

User **who has a profile in Azure AD, can be assigned to users in other tenants**

Multiple users are assigned to a *group,* roles assigned to group impact all the users

A *service principal* is a security ID for applications or services

A *managed identity* is typically used in developing cloud applications to handle credential management

Roles

Owner has full access to all resources **and** grant access

Contributor can create/manage all resources, **cannot** grant access

Reader can view existing resources

User Access Administrator lets you manage user access

```
New-AzRoleAssignment -SignInName janis.thomas@becausesecurity.com `
    -RoleDefinitionName "Virtual Machine Contributor" `
    -ResourceGroupName ps-course-rg
```

Add role assignment using PowerShell

Deny Assignments

- Blocks users from performing specific actions even if a role assignment allows it
- Created and managed in Azure to protect resources
- Can only be created using Azure Blue Prints or managed apps

Interpret access assignments

Interpret Access Assignments

```
PS G:\> Get-AzRoleAssignment -ResourceGroupName ps-course-rg

RoleAssignmentId   : /subscriptions/8bc4fbf0-6ad5-4922-aaaa-226b44e5db84/resourceGroups/ps-course-rg/providers/Microsof
                     t.Authorization/roleAssignments/b0d8875e-fd1b-4e16-91fc-683733e54f83
Scope              : /subscriptions/8bc4fbf0-6ad5-4922-aaaa-226b44e5db84/resourceGroups/ps-course-rg
DisplayName        : Janis Thomas
SignInName         : janis.thomas@becausesecurity.com
RoleDefinitionName : Reader
RoleDefinitionId   : acdd72a7-3385-48ef-bd42-f606fba81ae7
ObjectId           : b0d81f06-dfc9-4874-a496-1744e2aa0ede
ObjectType         : User
CanDelegate        : False
Description        :
ConditionVersion   :
Condition          :
```

Interpret Access Assignments

```
PS G:\> az role assignment list --resource-group ps-course-rg
[
  {
    "canDelegate": null,
    "id": "/subscriptions/8bc4fbf0-6ad5-4922-aaaa-226b44e5db84/resourceGroups/ps-course-rg/providers
tion/roleAssignments/b0d8875e-fd1b-4e16-91fc-683733e54f83",
    "name": "b0d8875e-fd1b-4e16-91fc-683733e54f83",
    "principalId": "b0d81f06-dfc9-4874-a496-1744e2aa0ede",
    "principalName": "janis.thomas@becausesecurity.com",
    "principalType": "User",
    "resourceGroup": "ps-course-rg",
    "roleDefinitionId": "/subscriptions/8bc4fbf0-6ad5-4922-aaaa-226b44e5db84/providers/Microsoft.Aut
itions/acdd72a7-3385-48ef-bd42-f606fba81ae7",
    "roleDefinitionName": "Reader",
    "scope": "/subscriptions/8bc4fbf0-6ad5-4922-aaaa-226b44e5db84/resourceGroups/ps-course-rg",
    "type": "Microsoft.Authorization/roleAssignments"
  }
]
```

```
# PowerShell get role assignments
Get-AzRoleAssignment
Get-AzDenyAssignment

# Azure CLI get role assignments
az role assignment list
```

Interpret Access Assignments

Create a custom role

Create a Custom Role

Portal

- Clone existing role

ARM Template

PowerShell

- Modify existing role definition
- Create new role using modified definition

Role Action Examples

Operation String	Action
*/read	Grants read access to all resource types of all resource providers
Microsoft.compute/*	Grants access to all operations for all resource types in the Microsoft.Compute resource provider
microsoft.web/sites/restart/Action	Grants access to restart a web app

Create a Custom Role

```
$role = Get-AzRoleDefinition "Virtual Machine Contributor"
$role.Id = $null
$role.Name = “VM Reader"
$role.Description = “Can see VMs"
$role.Actions.Clear()
$role.Actions.Add("Microsoft.Storage/*/read")
$role.Actions.Add("Microsoft.Network/*/read")
$role.Actions.Add("Microsoft.Compute/*/read")
$role.AssignableScopes.clear()
$role.AssignableScopes.Add("/subscriptions/00000-1111-2222-aaaa-123456778")
New-AzRoleDefinition -Role $role
```

Manage subscriptions and governance "Need to Know"

Michael Teske

AUTHOR EVANGELIST-CLOUD ENGINEER, PLURALSIGHT

@teskemj

Manage Subscriptions and Governance

Skills measured

- Configure Azure policies
- Configure resource locks
- Apply tags
- Create and manage resource groups
- Manage subscriptions
- Configure Cost Management
- Configure management groups

Configure Azure policies

Azure Policy

Used to create, assign and manage policies in Azure

Enforce rules to ensure your resources remain compliant

Focuses on resource properties for both new deployments and existing

It does not apply remediations to resources that are not compliant

Policy Concepts

A **policy definition** is a rule

An **assignment** is an application of an initiative or a policy to a specific scope

An **initiative** is a collection of policy definitions

Azure Policy Creation-PowerShell

```
# Get a reference to the resource group that is the scope of the assignment
$rg = Get-AzResourceGroup -Name '<resourceGroupName>'

# Get a reference to the built-in policy definition to assign
$definition = Get-AzPolicyDefinition | Where-Object { $_.Properties.DisplayName `
-eq 'Audit VMs that do not use managed disks' }

# Create the policy assignment with the built-in definition against your resource group
New-AzPolicyAssignment -Name 'audit-vm-manageddisks’ `
     -DisplayName 'Audit VMs without managed disks Assignment' -Scope $rg.ResourceId `
     -PolicyDefinition $definition
```

Configure resource locks

Locks types include:

- Read-only
- Delete

Can be inherited from parent scopes

- For both existing and new resources

Applies to all users and roles

Resource Locks

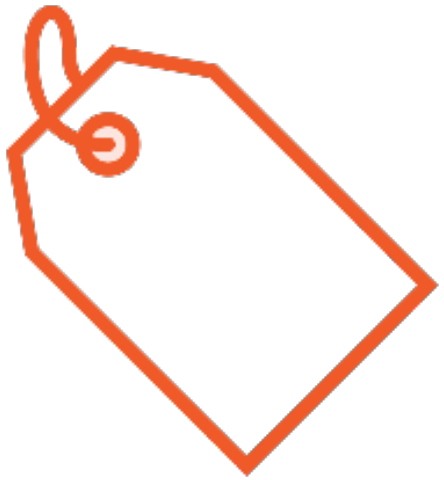
```
# PowerShell

New-AzResourceLock –LockLevel CanNotDelete –LockName LockSite –ResourceName examplesite

# Azure CLI

az lock create --name LockGroup --lock-type CanNotDelete --resource-
group exampleresourcegroup
```

Apply tags

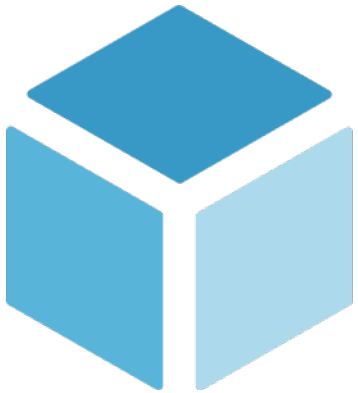


Used to organize resources and management hierarchy

Each tag consists of name and value pair

Must have write access to Microsoft.Resources/tags

Create and manage resource groups



Resources can be moved from one resource group to another if that is supported by that resource

Moving resources does not change the location/region where it was originally created

Deleting a resource group deletes all resources in that resource group

Creating and Managing Resource Groups

```
# PowerShell

New-AzResourceGroup –Name example-rg –Location eastus2


# Azure CLI

az group create --name example-rg --location eastus2
```

Manage subscriptions

You can move resources between subscriptions

You can transfer subscriptions between different tenants

A single tenant can have multiple subscriptions

Configure Cost Management

Analyze costs and trends using ***Cost Analysis***

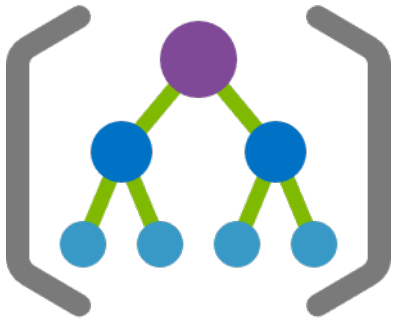
Cost Alerts can be generated to alert when a threshold you define is met

Apply ***Budgets*** to apply cost thresholds and limits to control your Azure spend

Recommendations displays ways to control costs through identifying trends in your usage

Configure management groups

Azure Management Groups

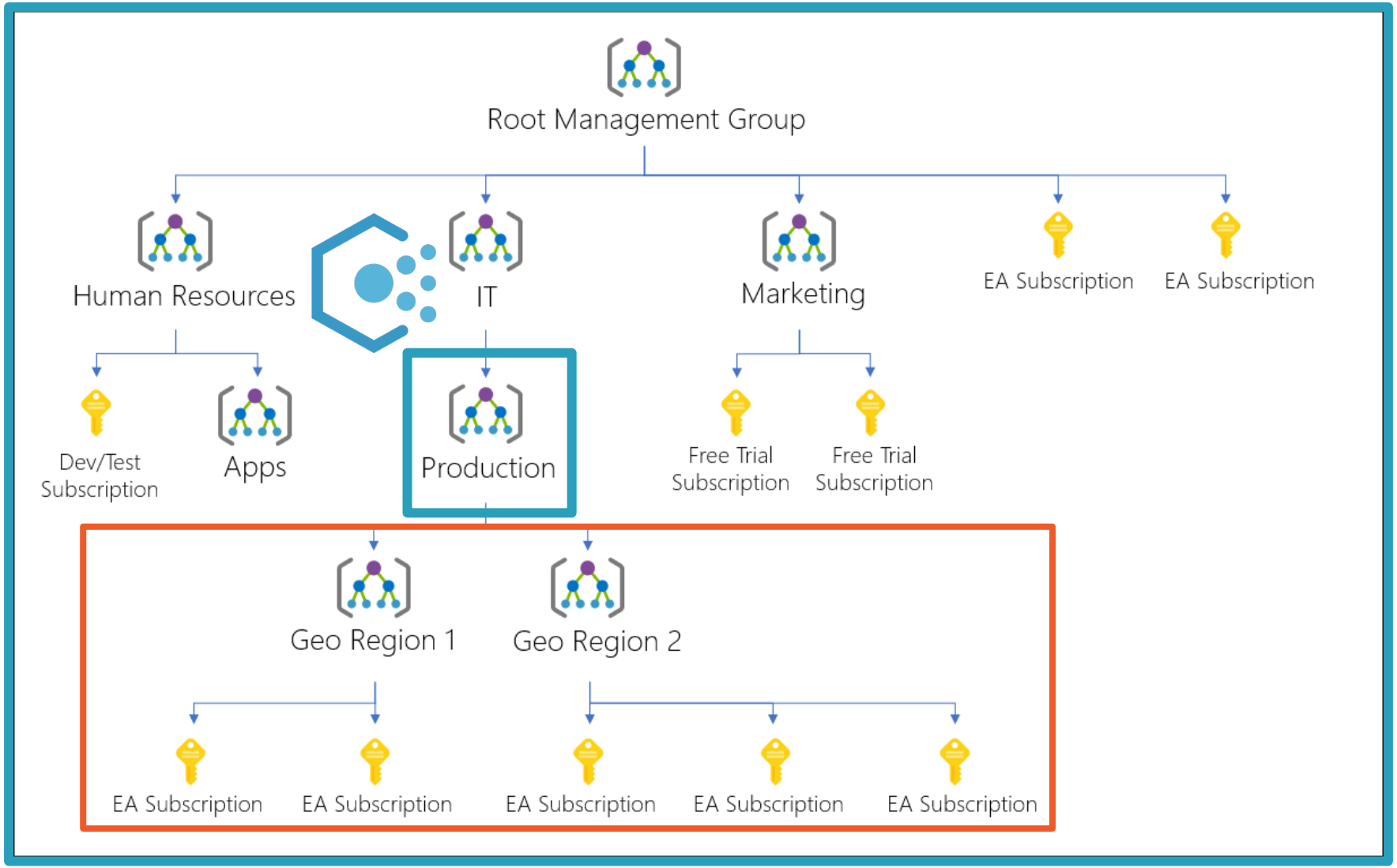


Used to efficiently manage access, policies and compliance

Provides a level of scope over subscriptions

Subscriptions within a group inherit policies applied to the group

Hierarchy of Groups and Subscriptions



Exam Strategy

- Schedule your exam
- Review the links in the exercise files
- Manage your time by how the functional groups are weighted
- Focus on your weaknesses
- Be familiar with implementations in portal and with code
- Check out Pluralsight's hands on labs
- Good luck! You got this!

Exam Strategy

Courses: https://bit.ly/3ftbUip

Twitter: @teskemj

LinkedIn: https://bit.ly/3iuD1dx