

Managing Governance



Michael Teske

AUTHOR EVANGELIST-CLOUD ENGINEER, PLURALSIGHT

@teskemj



Overview



Configure Management Groups

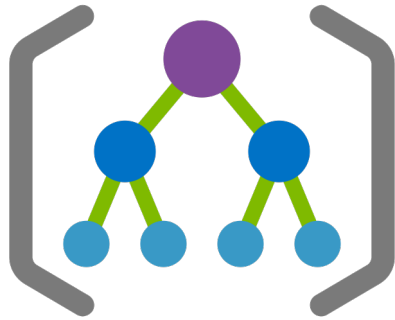
Configure Azure Policy

Configure resource locks

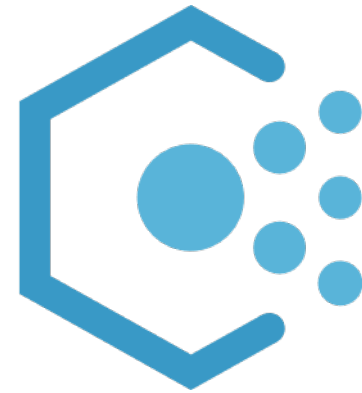
Create and manage resource groups

- Move resources
- Move resource groups

Azure Subscription Resources



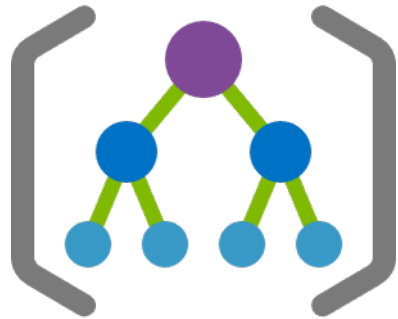
Azure Management Groups



Azure Policy



Azure Management Groups



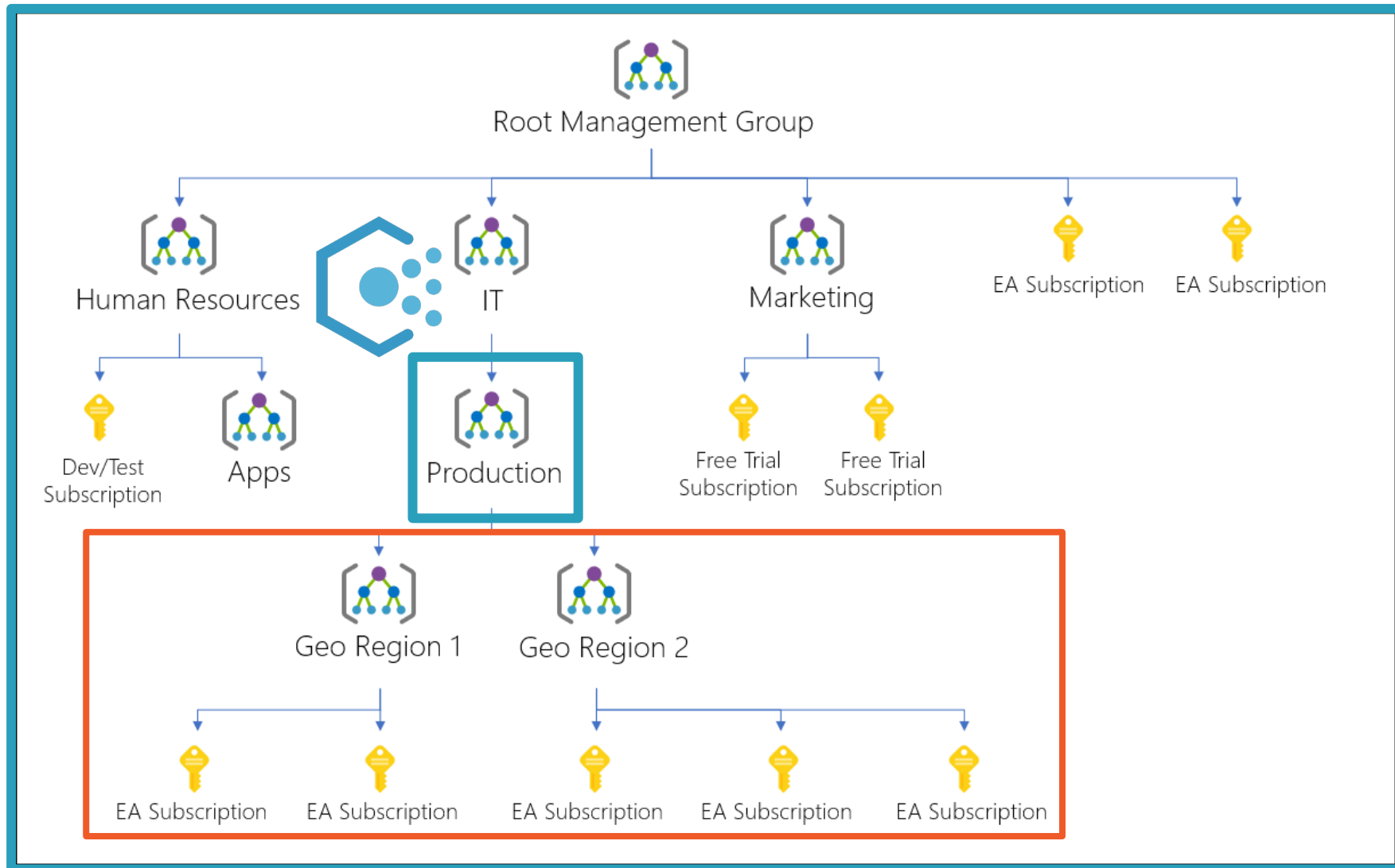
Used to efficiently manage access, policies and compliance

Provides a level of scope over subscriptions

Subscriptions within a group inherit policies applied to the group



Hierarchy of Groups and Subscriptions



Root Management Groups



Each directory has a single top-level group called the “Root”



Allows for global policies and RBAC assignments at the directory level



AD Global admin needs to elevate to User Access Administrator role



Root management group cannot be moved or deleted

Demo

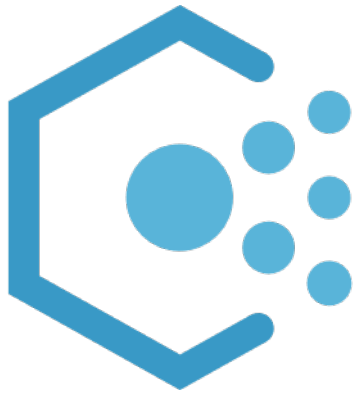


Azure subscription and governance resources

- Azure Management Groups



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
```



Demo



Azure subscription and governance resources

- Azure Policy



Managing Access to Resources



Resource locks



Resource Groups

Resource Locks



Each resource can have a lock applied

Locks types include:

- Read-only
- Delete





Can apply to all resources and resource groups

Can be inherited from parent scopes

- For both existing and new resources


Applies to all users and roles

Resource Locks


 Add  Resource group  Subscription  Refresh

Add lock

Lock name

dont-delete 

Lock type

Delete 

Notes

don't delete this resource!

OK

Cancel



Resource Locks

PowerShell

```
New-AzResourceLock -Locklevel CanNotDelete -LockName LockSite -ResourceName  
examplesite
```

Azure CLI

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



Demo



Managing access to resources

- Resource locks



Creating and Managing Resource Groups



Resource groups are containers that hold related Azure resources



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
```



Demo



Managing access to resources

- Resource Groups
 - Moving resources
 - Moving resource groups



Summary



Management groups provide scope over subscriptions

Azure Policies can be applied to a management group

- All subscriptions and resources inherit from parent policies

Resource locks can be applied to all resources

- DoNotDelete
- Read-only

Supported resources can be moved between resource groups or subscriptions

- Does not change the location of the resource

