Managing Resources

James Bannan
MICROSOFT MVP, SOLUTIONS ARCHITECT

@jamesbannan www.jamesbannanit.com

Module Overview

- Explore Role Based Access Control
- Add User to Built-in RBAC Role
- Explore RBAC Custom Roles
- Create and Verify Custom Role
- Explore Resource Tags
- Add Tags to Resources
- Explore ARM Policies
- Create and Verify ARM Policy

Role Based Access Control (RBAC)

Resource-level access management

Controlled via Azure Active Directory

Access can be inherited from parent resource

Owner

Contributor

Reader

RBAC Built-in Roles

User	Group	Application
Subscription	Resource Group	Resource

https://azure.microsoft.com/en-us/documentation/articles/role-based-access-built-in-roles/

RBAC Built-in Roles

```
Get-AzureRmRoleDefinition | Select-Object Name
```

```
Name
----
API Management Service Contributor
Application Insights Component Contributor
Automation Operator
BizTalk Contributor
CDN Endpoint Contributor
CDN Endpoint Reader
CDN Profile Contributor
CDN Profile Reader
Classic Network Contributor
Classic Storage Account Contributor
Classic Virtual Machine Contributor
ClearDB MySQL DB Contributor
Contributor
Data Factory Contributor
......
```

RBAC Role Actions

```
(Get-AzureRmRoleDefinition -Name 'Virtual Machine Contributor').Actions
```

```
Microsoft.Authorization/*/read
Microsoft.Compute/availabilitySets/*
Microsoft.Compute/locations/*
Microsoft.Compute/virtualMachines/*
Microsoft.Compute/virtualMachineScaleSets/*
Microsoft.Insights/alertRules/*
Microsoft.Network/applicationGateways/backendAddressPools/join/action
Microsoft.Network/loadBalancers/backendAddressPools/join/action
Microsoft.Network/loadBalancers/inboundNatPools/join/action
Microsoft.Network/loadBalancers/inboundNatRules/join/action
Microsoft.Network/loadBalancers/read
Microsoft.Network/locations/*
Microsoft.Network/networkInterfaces/*
Microsoft.Network/networkSecurityGroups/join/action
Microsoft.Network/networkSecurityGroups/read
......
```

Demo

Explore built-in roles

Create new User

Assign User to built-in role

Verify access

RBAC Custom Roles

```
{
      “Name”: <NAME>,
      “Id”: <ID>,
      “IsCustom”: true,
      “Description”: <DESCRIPTION>,
      “Actions”: [
            <ACTION1>,
            <ACTION2>
      ],
      “NotActions”: [
            <NOTACTION1>,
            <NOTACTION2>
      ],
      “AssignableScopes”: [
            <SCOPE1>,
            <SCOPE2>
      ]
}
```

- JSON formatting
- Actions: Which operations the role can perform
- NotActions: Which operations the role cannot perform
- NotActions: Not a DENY rule
- AssignableScopes: Which scopes (subscription / group / resource) the role can be assigned to

Get Available Provider Operations

```
Get-AzureRmProviderOperation Microsoft.Compute/* | `
Select-Object Operation,OperationName
```

```
Operation
---------
Microsoft.Compute/register/action
Microsoft.Compute/virtualMachineScaleSets/read
Microsoft.Compute/virtualMachineScaleSets/write
Microsoft.Compute/virtualMachineScaleSets/delete
Microsoft.Compute/virtualMachineScaleSets/start/action
Microsoft.Compute/virtualMachineScaleSets/powerOff/action
Microsoft.Compute/virtualMachineScaleSets/restart/action
......
```

```
OperationName
-------------
Register Subscription for Compute
Get Virtual Machine Scale Set
Create or Update Virtual Machine Scale Set
Delete Virtual Machine Scale Set
Start Virtual Machine Scale Set
Power Off Virtual Machine Scale Set
Restart Virtual Machine Scale Set
```

Get Available Provider Actions

```
Get-AzureRmProviderOperation Microsoft.Compute/*/action | `
Select-Object Operation,OperationName
```

```
Operation                                                          OperationName
---------                                                          -------------
Microsoft.Compute/register/action                                  Register Subscription for Compute
Microsoft.Compute/virtualMachineScaleSets/start/action             Start Virtual Machine Scale Set
Microsoft.Compute/virtualMachineScaleSets/powerOff/action          Power Off Virtual Machine Scale Set
Microsoft.Compute/virtualMachineScaleSets/restart/action           Restart Virtual Machine Scale Set
Microsoft.Compute/virtualMachineScaleSets/deallocate/action        Deallocate Virtual Machine Scale Set
Microsoft.Compute/virtualMachineScaleSets/manualUpgrade/action     Manual Upgrade Virtual Machine Scale Set
Microsoft.Compute/virtualMachineScaleSets/virtualMachines/start/action Start Virtual Machine in a Virtual Machine Scale Set
......
```

Create a Custom Role with PowerShell

```powershell
$role = Get-AzureRmRoleDefinition -Name 'Virtual Machine Contributor'

$role.Id = $null
$role.Name = 'Virtual Machine Operator'
$role.Description = 'Can monitor, start, and restart virtual machines.'
$role.Actions.RemoveRange(0,$role.Actions.Count)
$role.Actions.Add('Microsoft.Compute/*/read')
$role.Actions.Add('Microsoft.Compute/virtualMachines/start/action')
$role.Actions.Add('Microsoft.Compute/virtualMachines/restart/action')
$role.Actions.Add('Microsoft.Compute/virtualMachines/downloadRemoteDesktopConnectionFile/action')
$role.Actions.Add('Microsoft.Network/*/read')
$role.Actions.Add('Microsoft.Storage/*/read')
$role.Actions.Add('Microsoft.Authorization/*/read')
$role.Actions.Add('Microsoft.Resources/subscriptions/resourceGroups/read')
$role.Actions.Add('Microsoft.Resources/subscriptions/resourceGroups/resources/read')
$role.Actions.Add('Microsoft.Insights/alertRules/*')
$role.Actions.Add('Microsoft.Support/*')
$role.AssignableScopes.Remove('/') | Out-Null
$role.AssignableScopes.Add('/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e')

New-AzureRmRoleDefinition -Role $role
```

Demo

Create custom role with PowerShell

Verify new role

Assign User to role

Verify role access

Resource Tags

Logically classify resources

Business-specific metadata

Not supported by classic resources

15 tags maximum

512 tag name limit

256 tag value limit

Demo

Create new Tags for VM resources

Verify Tag data

Azure Resource Manager Policies

Scenario:

Require resource Tags for department/BU charge-back

Scenario:

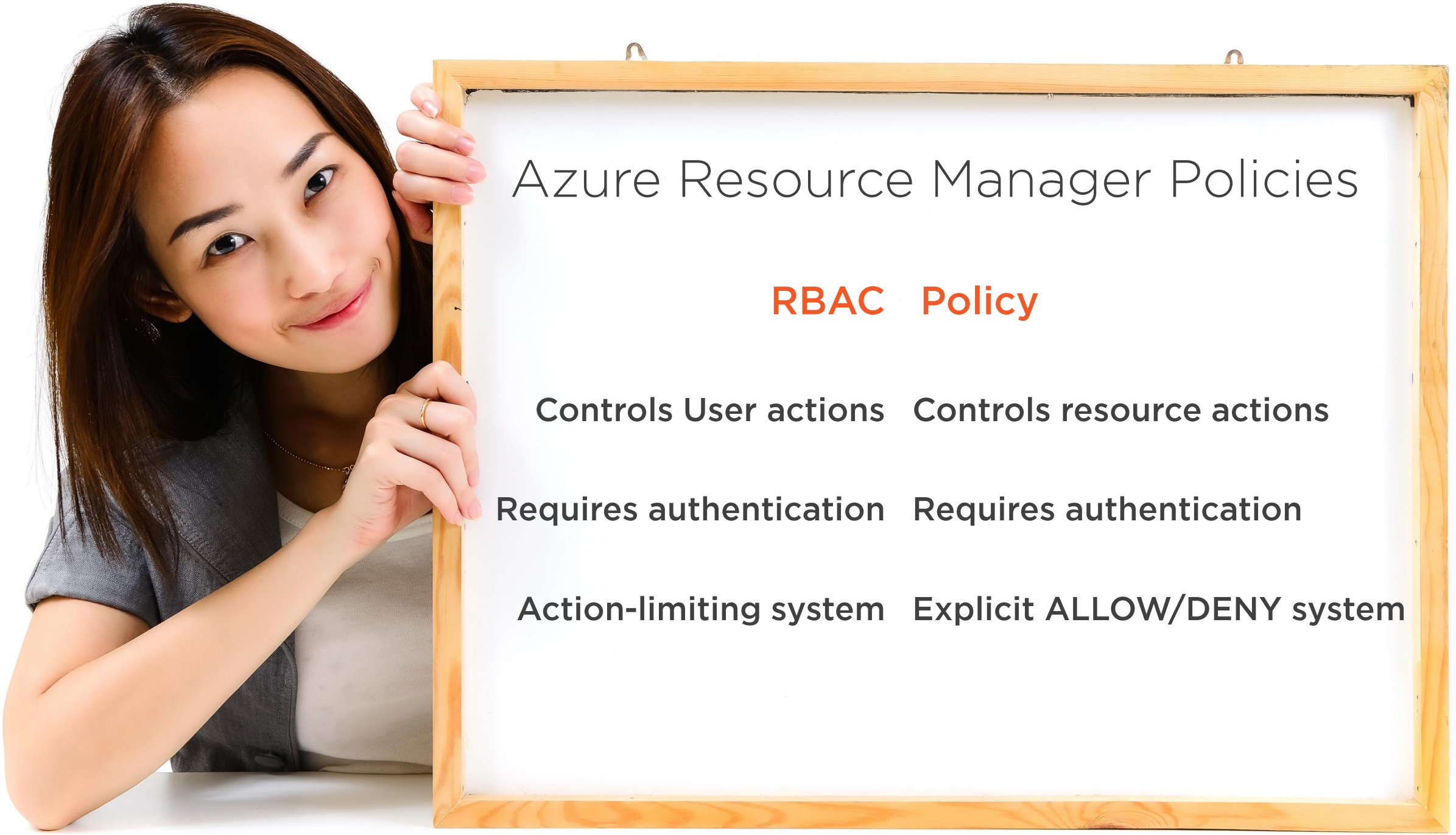
Limit which Azure geo-political regions resources can be deployed to

Scenario:

Restrict which resources or resource types can be deployed

Scenario:

Enforce standard naming conventions across resources


Azure Resource Manager Policies
RBAC
Policy
Controls User actions
Controls resource actions
Requires authentication
Requires authentication
Action-limiting system
Explicit ALLOW/DENY system

Policy Structure

```
{
  "if" : {
    "not" : {
      "field" : "location",
      "in" : ["northeurope" , "westeurope"]
    }
  },
  "then" : {
    "effect" : "deny"
  }
}
```

- **Basic structure**
  - If / Then
- **Operator**
  - Not / And / Or
- **Field**
  - Name / Kind / Type / Location
  - Tags / Alias
- **Condition**
  - Equals / Like / Contains
  - In / ContainsKey
- **Effect**
  - Deny / Audit / Append

Deploy ARM Policy with PowerShell/JSON

```
New-AzureRmPolicyDefinition `
    -Name regionPolicyDefinition `
    -Description ‘Allow resource creation in certain regions' `
    -Policy 'path-to-policy-json-on-disk'
```

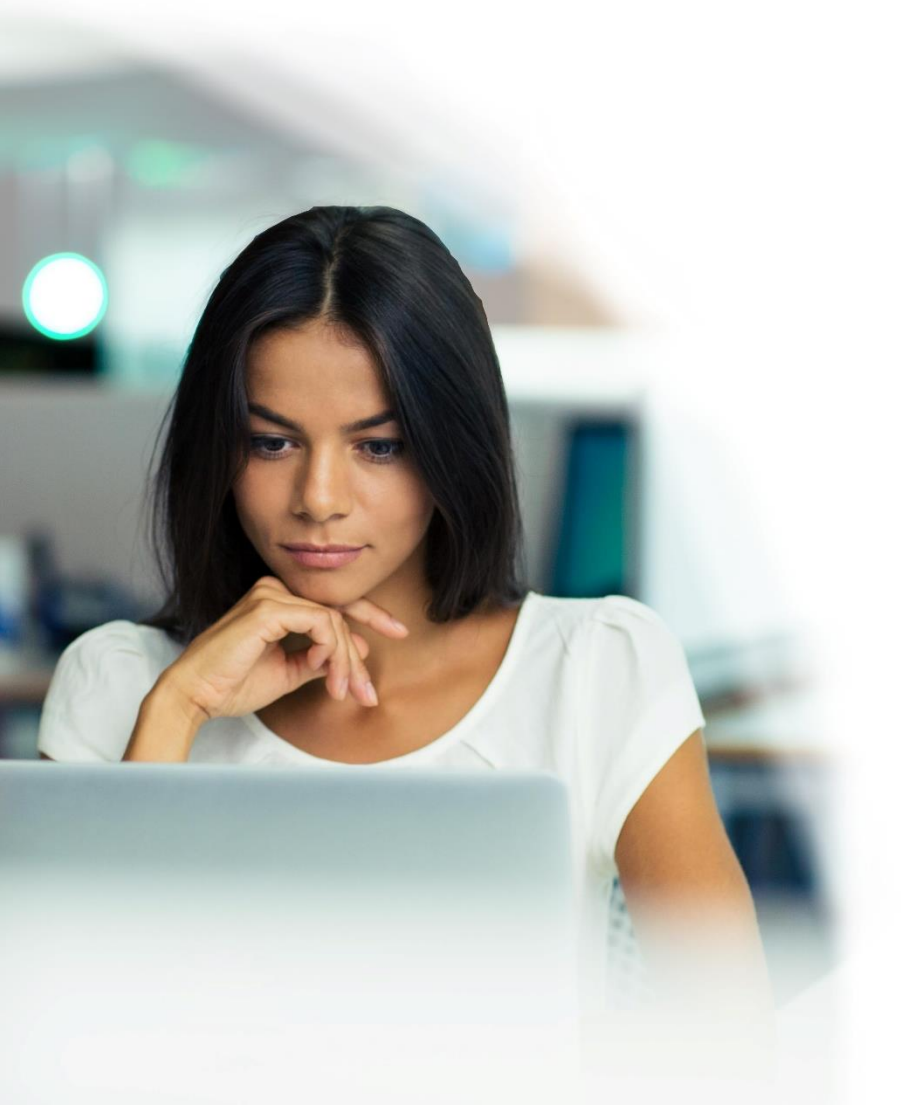
Demo

Create new ARM policy

Deploy ARM policy

Verify ARM policy

Module Summary



Add User to Built-in RBAC Role

Create and Verify Custom Role

Add Tags to Resources

Create and Verify ARM Policy

Coming next:
Authoring Deconstructed Templates