

ASSIGNING POLICIES AND ROLES TO ACTIVE DIRECTORY MEMBERS

Services used

Active Directory

Active Directory stores information about objects on the network and makes this information easy for administrators and users to find and use. Active Directory uses a structured data store as the basis for a logical, hierarchical organization of directory information

AM (identity and access management)

It is a framework of policies and technologies to ensure that the right users have the appropriate access to technology resources

Policies

Policy is a rule about specific security conditions that you want controlled.

Let's create a policy to deploy any resource in subscription which can be done only on Central India location

- Portal > search policy > assignments > assign a policy > define

Assign policy ...

Basics Advanced Parameters Remediation Non-compliance messages Review + create

Scope

Scope [Learn more about setting the scope](#) *

Free Trial

Exclusions

Optionally select resources to exclude from the policy assignment.

Basics

Policy definition *

Allowed locations

Assignment name * ⓘ

Allowed locations

Description

resources can only be deployed in central india

Policy enforcement ⓘ

Enabled Disabled

To check the working of the assigned policy,

- lets create a vm in Canada region

Create a virtual machine ...

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

i This subscription may not be eligible to deploy VMs of certain sizes in certain regions.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Instance details

Virtual machine name * ⓘ

Region * ⓘ

x Policy enforcement. Value does not meet requirements on resource: Microsoft.Compute/virtualMachines
The field 'Location' with the value '(Canada) Canada Central' is denied: [Policy e56962a6-4747-49cd-b67b-bf8b01975c4c details](#)

we are unable to create a virtual machine in central Canada due to the deployed policy

Now lets create a role to,

- deny storage accounts from viewing shared key access
- portal > subscriptions > add a custom role and enter the following:

Setting	Value
Custom role name	Access key
Baseline permissions	clone a role
Role to clone	Owner

- In permissions tab, click on exclude permissions and search for microsoft.account then press ctrl+F and search "Returns the access keys for the specified storage account"
- In available scopes tab, delete the existing scope and create a new scope

Setting	Value
Type	Resource group
Subscription	Select your appropriate subscription
Resource group	demo_RG

- Select create + review and create
- Now assign the policy to any user in your Azure AD
- Go to demo_RG and select IAM and add role assignments

Setting	Value
Roles	Privileged administrator roles
Search	Access key

- In members tab, enter the following:

Setting	Value
Assign access to	Users, groups or principal
Members	Select the appropriate member


- Select create+review and create
- The assigned role can be verified by the screenshot provided below

policydemo69 | Access keys ☆ ...

Storage account

Search

- Overview
- Activity log
- Tags
- Diagnose and solve problems
- Access Control (IAM)
- Data migration
- Events
- Storage browser
- Storage Mover
- Data storage
- Containers
- File shares
- Queues
- Tables
- Security + networking
- Networking



AuthorizationFailed

Summary

Session ID
f974f42c87c840269b248ee58f8114a9

Resource ID
/subscriptions/4095d462-3fb3-4d5d-9eff-bc9008ac3e...

Extension
Microsoft_Azure_Storage

Content
KeyManagementBladeV2

Error code
403

Storage Request ID
8e42c95d-a02b-4681-8367-6a3ca72004a4

Details

- The client 'demo@hireshr1234outlook.onmicrosoft.com' with object id 'd983bcb6-f7d4-4403-beae-4202a210f6d1' does not have authorization to perform action 'Microsoft.Storage/storageAccounts/listKeys/action' over scope '/subscriptions/4095d462-3fb3-4d5d-9eff-bc9008ac3ecd/resourceGroups/Failover-RG/providers/Microsoft.Storage/storageAccounts/policydemo69' or the scope is invalid. If access was recently granted, please refresh your credentials.
- [Learn more about authorizing access to Azure Storage](#)

