Microsoft Azure Administrator: Manage Role-Based Access Control

MANAGE ROLE-BASED ACCESS CONTROL

Michael Teske

AUTHOR EVANGELIST-CLOUD ENGINEER, PLURALSIGHT

@teskemj

Course Coverage of Certification Objectives

Manage Role-Based Access Control

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

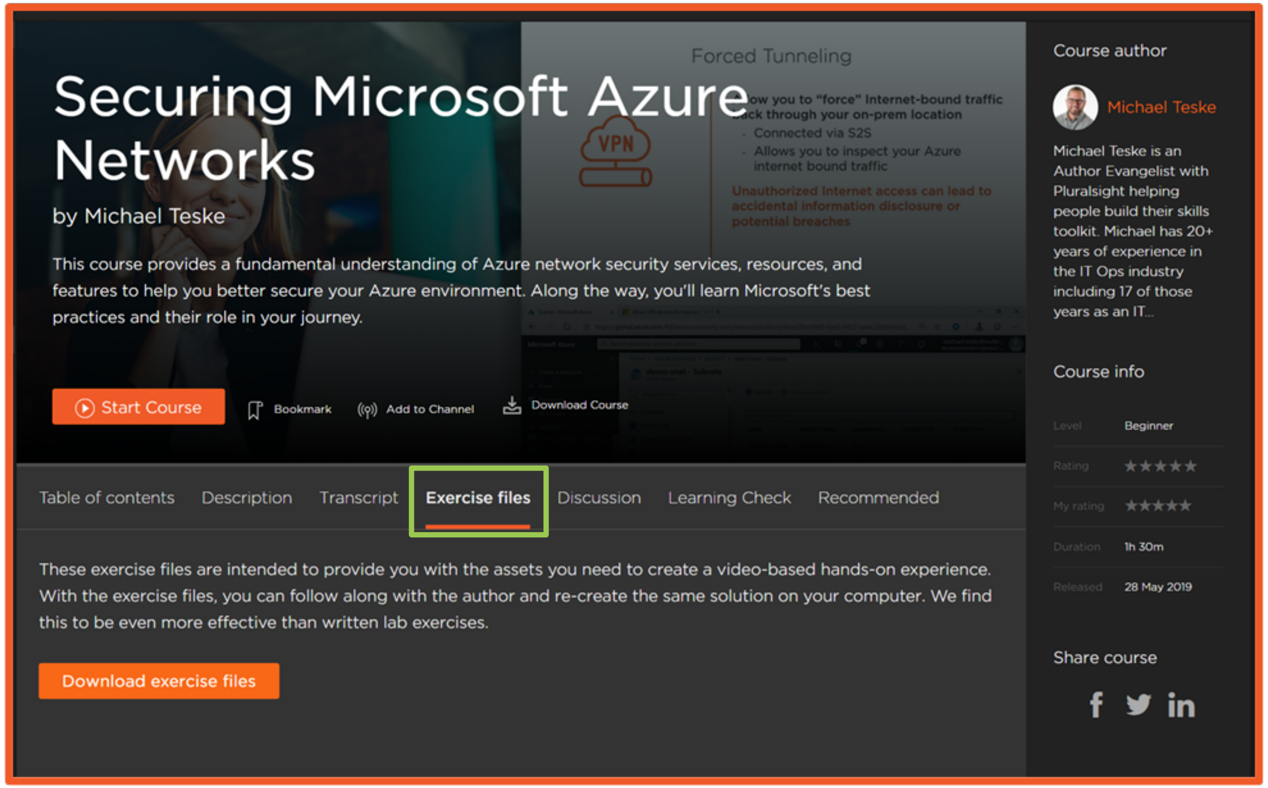
Full certification exam skills outline available at http://bit.ly/az104ms

Exercise Files

Slides

Code

Links to Resources



Forced Tunneling
…ow you to "force" Internet-bound traffic …ack through your on-prem location
Connected via S2S
Allows you to inspect your Azure internet bound traffic
Unauthorized Internet access can lead to accidental information disclosure or potential breaches
VPN

Securing Microsoft Azure Networks

by Michael Teske

This course provides a fundamental understanding of Azure network security services, resources, and features to help you better secure your Azure environment. Along the way, you'll learn Microsoft's best practices and their role in your journey.

Start Course
Bookmark
Add to Channel
Download Course
Table of contents
Description
Transcript
Exercise files
Discussion
Learning Check
Recommended

These exercise files are intended to provide you with the assets you need to create a video-based hands-on experience. With the exercise files, you can follow along with the author and re-create the same solution on your computer. We find this to be even more effective than written lab exercises.

Course author

Michael Teske

Michael Teske is an Author Evangelist with Pluralsight helping people build their skills toolkit. Michael has 20+ years of experience in the IT Ops industry including 17 of those years as an IT...

Course info

Level	Beginner
Rating	★★★★★
My rating	★★★★★
Duration	1h 30m
Released	28 May 2019

Share course

Role-based Access Control (RBAC)

Role-based Access Control

Role-based access control can be used to assign permissions to:

- Users
- Groups
- Applications

The scope of role assignment can be:

- Subscription
- Resource Group
- Single resource

Role-based Access Control

Allow one user to manage virtual machines in a subscription and another user to manage virtual networks

Allow a DBA group to manage SQL databases in a subscription

Allow an application to access all resources in a resource group

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

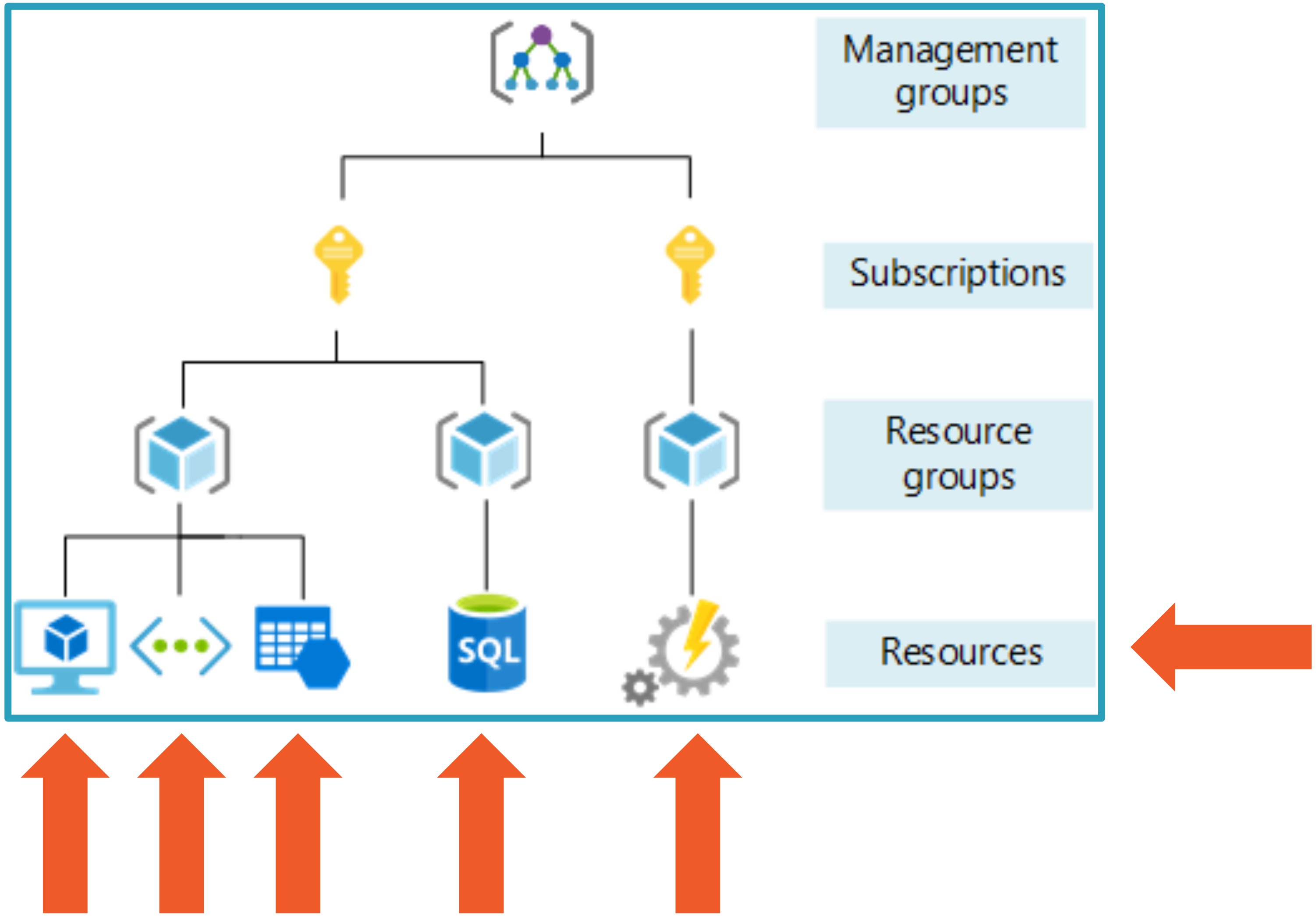
Deny Assignments

Blocks users from performing specific actions even if a role assignment allows it

Created and managed in Azure to protect resources

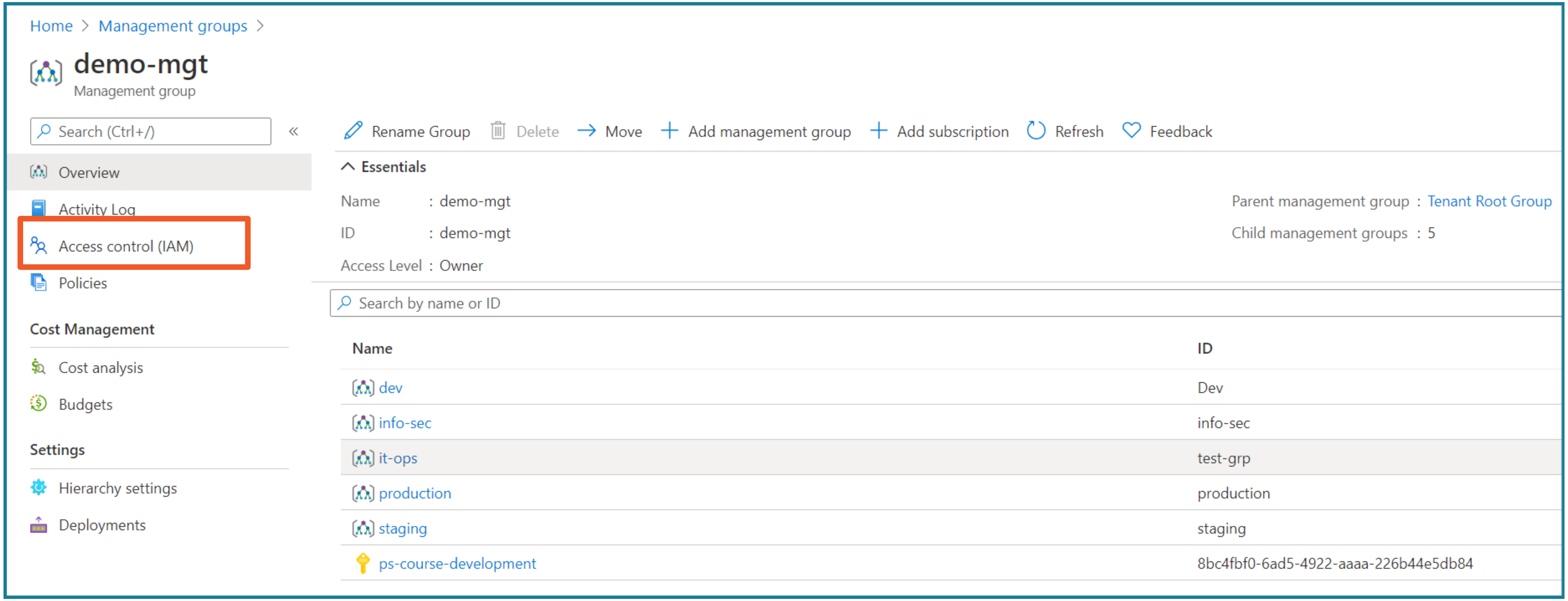
Can only be created using Azure Blue Prints or managed apps

RBAC Scope


Management groups
Subscriptions
Resource groups
SQL
Resources

Managing Role-Based Access Control

Manage Role-based Access Control



Home > Management groups >

demo-mgt

Management group

Name : demo-mgt

ID : demo-mgt

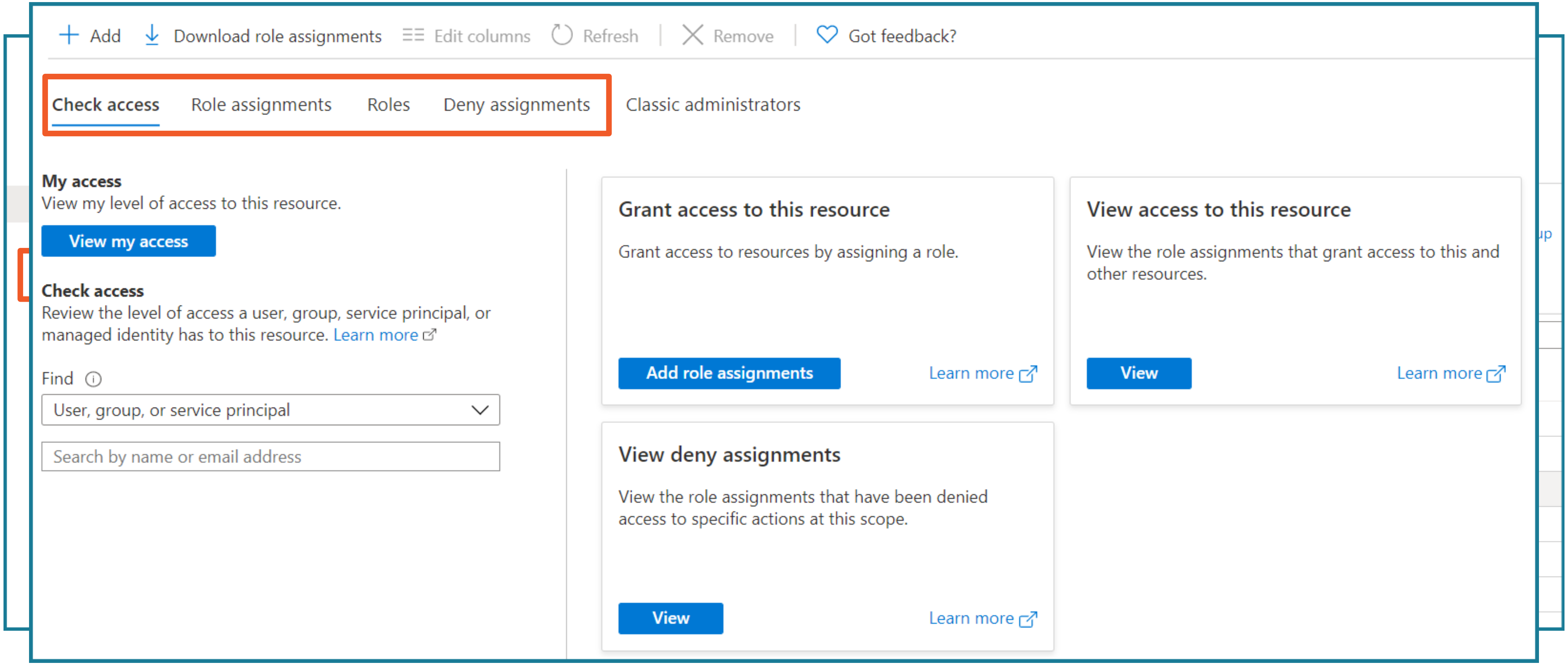
Access Level : Owner

Parent management group : Tenant Root Group

Child management groups : 5

Name	ID
dev	Dev
info-sec	info-sec
it-ops	test-grp
production	production
staging	staging
ps-course-development	8bc4fbf0-6ad5-4922-aaaa-226b44e5db84

Manage Role-based Access Control



＋ Add ↓ Download role assignments ☰ Edit columns ↻ Refresh | ✕ Remove | ♡ Got feedback?

Check access Role assignments Roles Deny assignments Classic administrators

My access

View my level of access to this resource.

View my access

Check access

Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Find ⓘ

User, group, or service principal

Search by name or email address

Grant access to this resource

Grant access to resources by assigning a role.

Add role assignments Learn more

View access to this resource

View the role assignments that grant access to this and other resources.

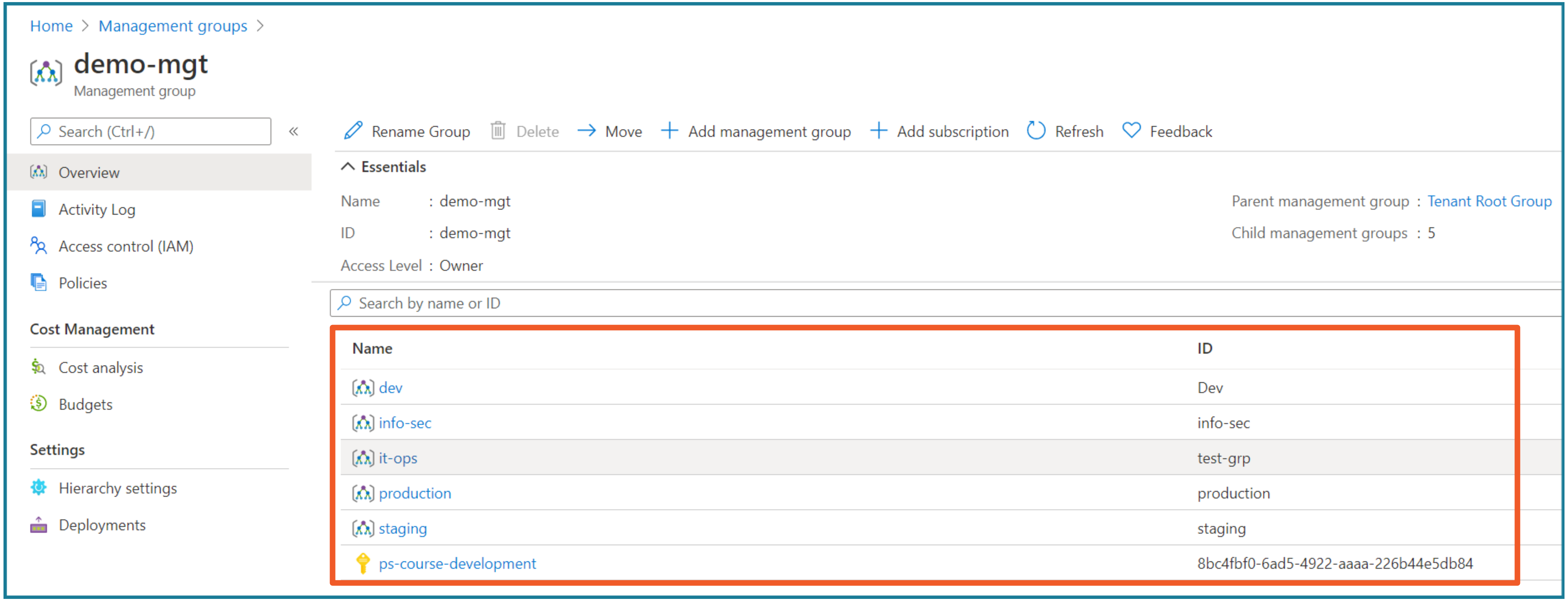
View Learn more

View deny assignments

View the role assignments that have been denied access to specific actions at this scope.

View Learn more

Manage Role-based Access Control



demo-mgt

Management group

Name : demo-mgt

ID : demo-mgt

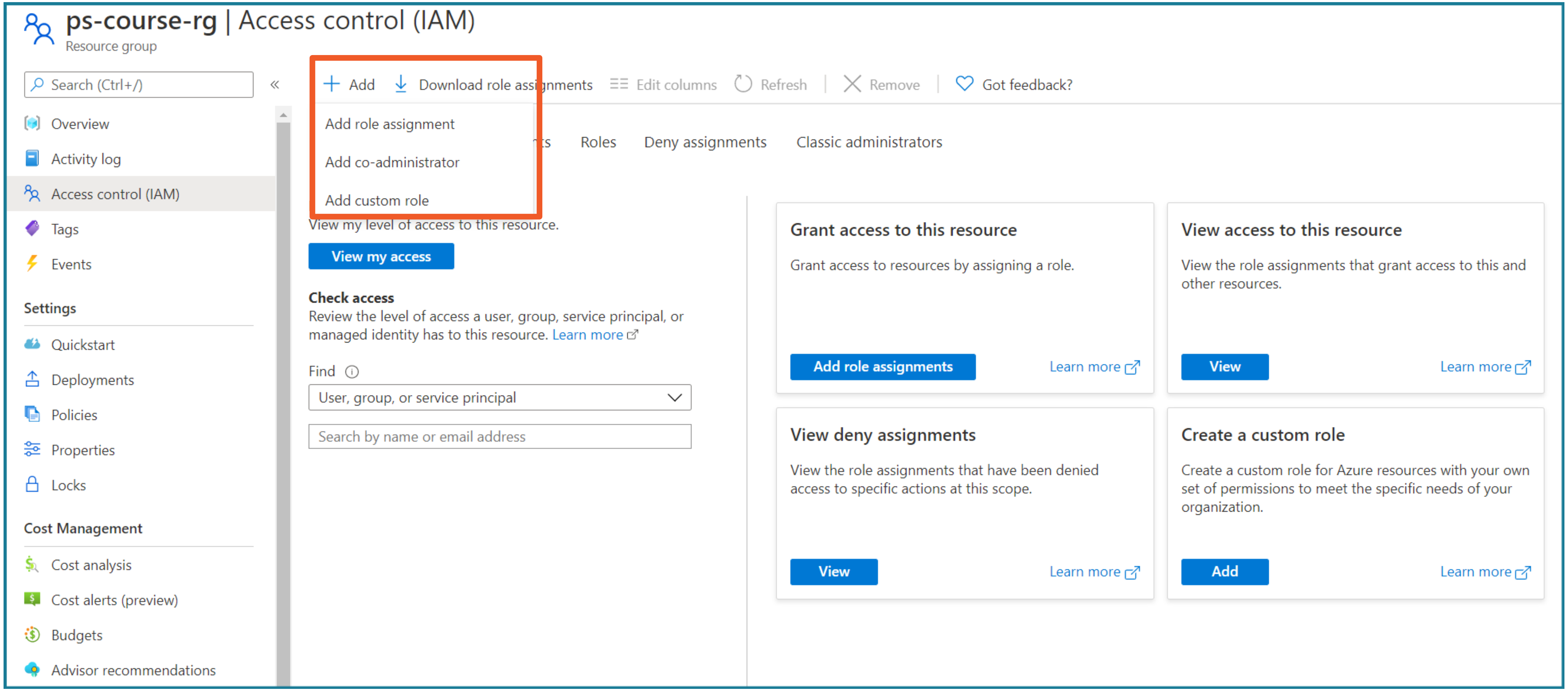
Access Level : Owner

Parent management group : Tenant Root Group

Child management groups : 5

Name	ID
dev	Dev
info-sec	info-sec
it-ops	test-grp
production	production
staging	staging
ps-course-development	8bc4fbf0-6ad5-4922-aaaa-226b44e5db84

Manage Role-based Access Control



View my level of access to this resource.

Check access

Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Find: User, group, or service principal

Search by name or email address

Grant access to this resource

Grant access to resources by assigning a role.

View access to this resource

View the role assignments that grant access to this and other resources.

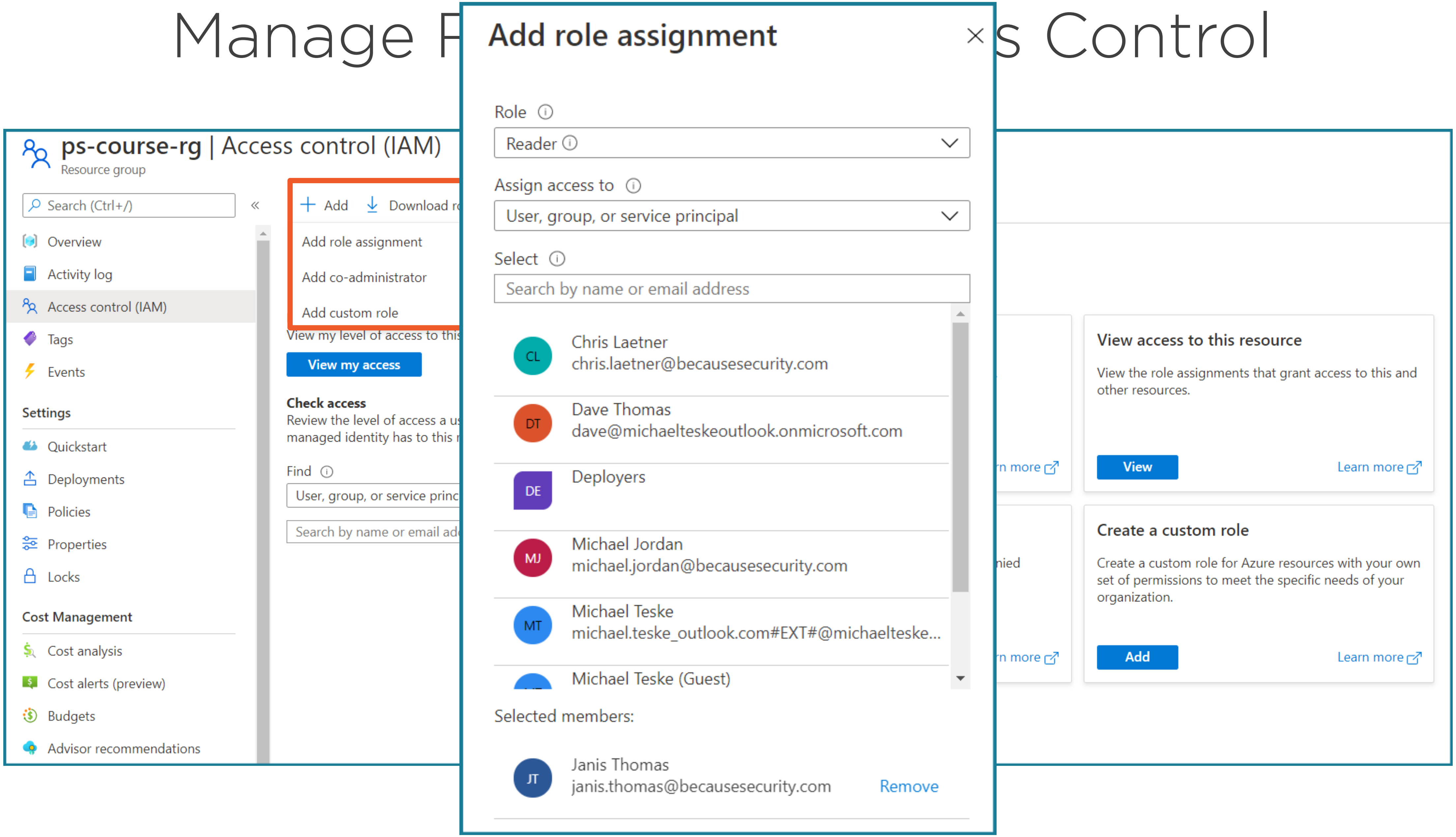
View deny assignments

View the role assignments that have been denied access to specific actions at this scope.

Create a custom role

Create a custom role for Azure resources with your own set of permissions to meet the specific needs of your organization.

Manage R s Control



ps-course-rg | Access control (IAM)

Resource group

Add role assignment

Role: Reader

Assign access to: User, group, or service principal

Select: Search by name or email address

- CL Chris Laetner chris.laetner@becausesecurity.com
- DT Dave Thomas dave@michaelteskeoutlook.onmicrosoft.com
- DE Deployers
- MJ Michael Jordan michael.jordan@becausesecurity.com
- MT Michael Teske michael.teske_outlook.com#EXT#@michaelteske...
- Michael Teske (Guest)

Selected members:

- JT Janis Thomas janis.thomas@becausesecurity.com Remove

View my level of access to this

Check access

Review the level of access a u managed identity has to this r

Find: User, group, or service princ

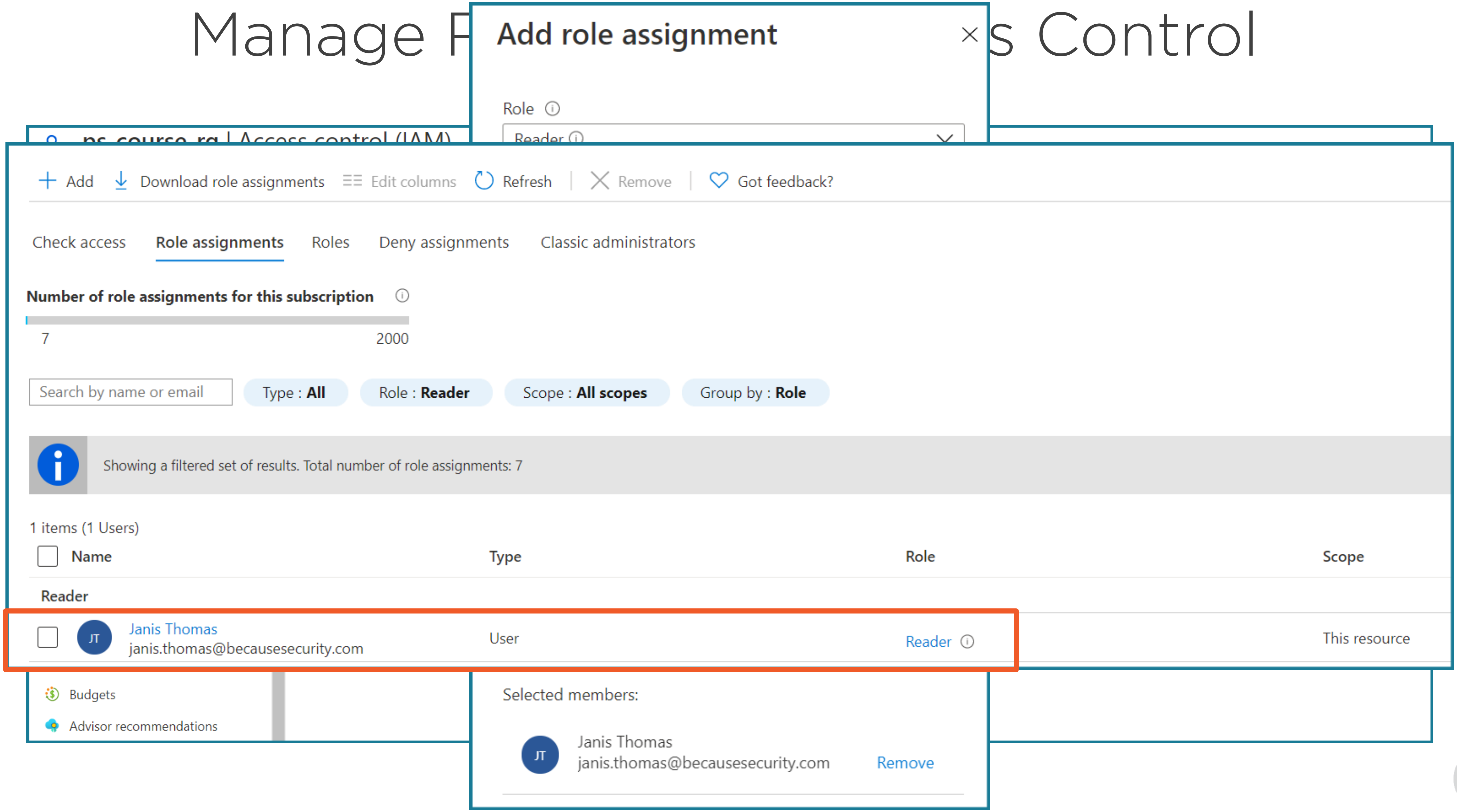
View access to this resource

View the role assignments that grant access to this and other resources.

Create a custom role

Create a custom role for Azure resources with your own set of permissions to meet the specific needs of your organization.

Manage F s Control



ps-course-rg | Access control (IAM)

Add role assignment

Role ⓘ

Reader ⓘ

Number of role assignments for this subscription ⓘ

7 2000

Type : **All** Role : **Reader** Scope : **All scopes** Group by : **Role**

Showing a filtered set of results. Total number of role assignments: 7

1 items (1 Users)

□ Name	Type	Role	Scope
Reader			
□ JT Janis Thomas janis.thomas@becausesecurity.com	User	Reader ⓘ	This resource

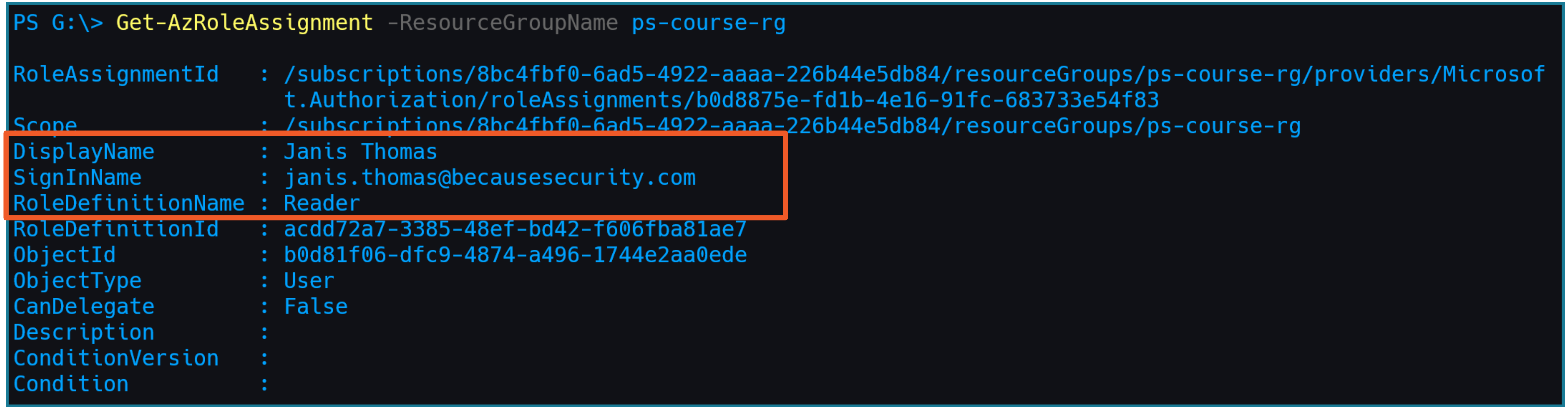
Selected members:

JT Janis Thomas
janis.thomas@becausesecurity.com Remove

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

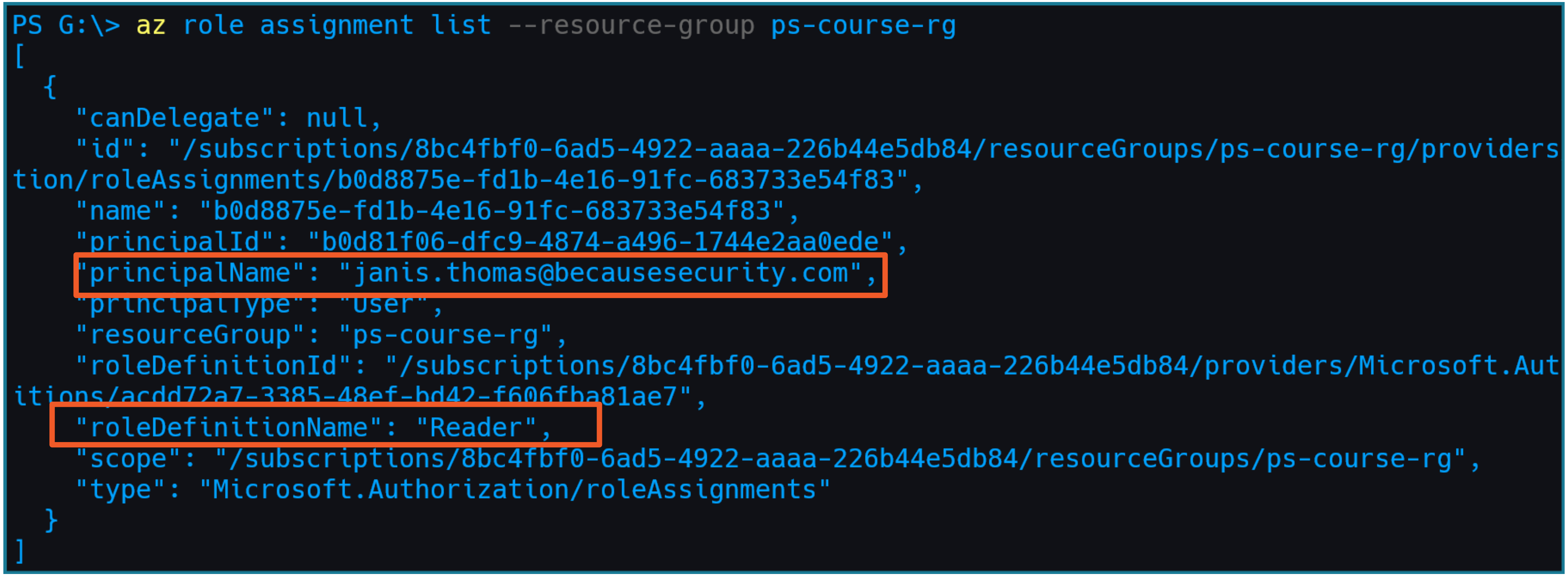
Add role assignment using PowerShell

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

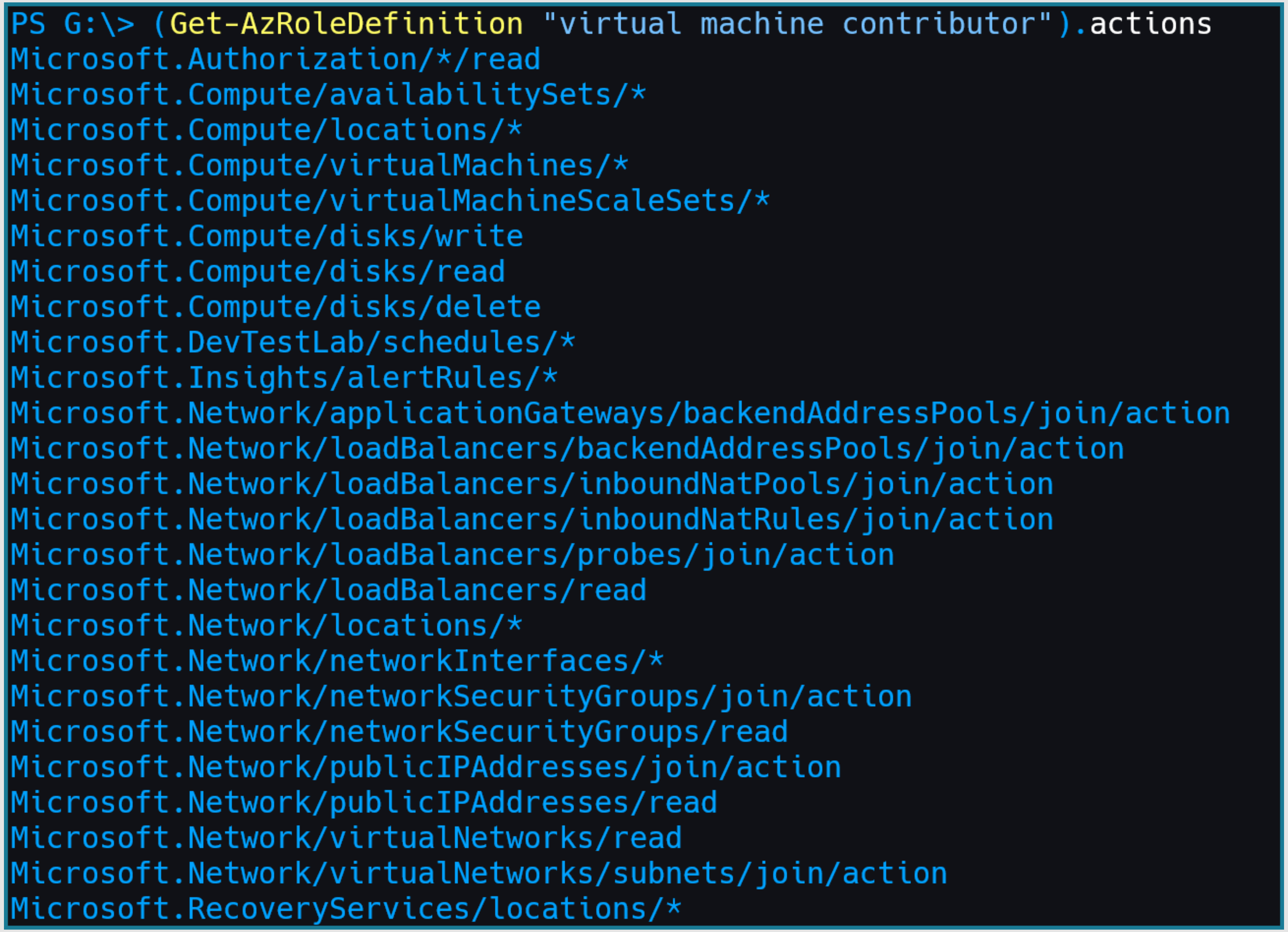
Custom Role Required Properties

Property	Type	Description
Name	String	Display name
ID	String	Unique ID
IsCustom	String	True for custom
Description	String	Max 1024 chars
Actions	String[]	Array of actions
AssignableScopes	String[]	Array of scopes

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

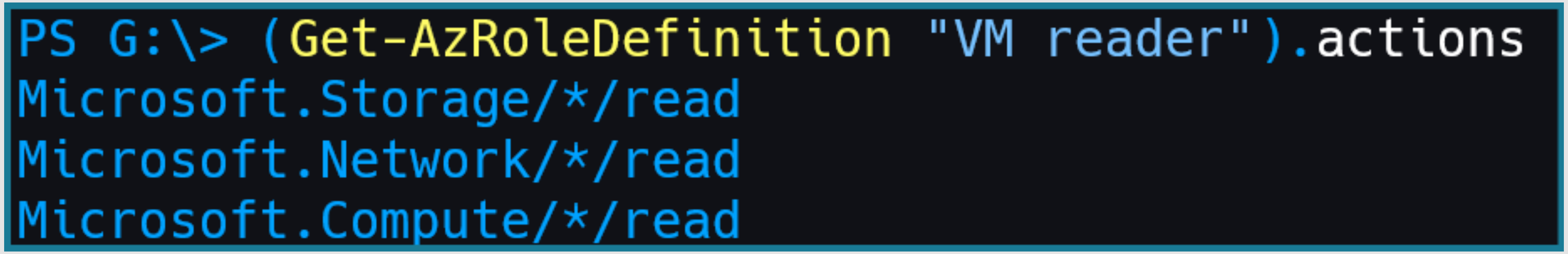


```
PS G:\> (Get-AzRoleDefinition "virtual machine contributor").actions
Microsoft.Authorization/*/read
Microsoft.Compute/availabilitySets/*
Microsoft.Compute/locations/*
Microsoft.Compute/virtualMachines/*
Microsoft.Compute/virtualMachineScaleSets/*
Microsoft.Compute/disks/write
Microsoft.Compute/disks/read
Microsoft.Compute/disks/delete
Microsoft.DevTestLab/schedules/*
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/probes/join/action
Microsoft.Network/loadBalancers/read
Microsoft.Network/locations/*
Microsoft.Network/networkInterfaces/*
Microsoft.Network/networkSecurityGroups/join/action
Microsoft.Network/networkSecurityGroups/read
Microsoft.Network/publicIPAddresses/join/action
Microsoft.Network/publicIPAddresses/read
Microsoft.Network/virtualNetworks/read
Microsoft.Network/virtualNetworks/subnets/join/action
Microsoft.RecoveryServices/locations/*
```

Create a Custom Role

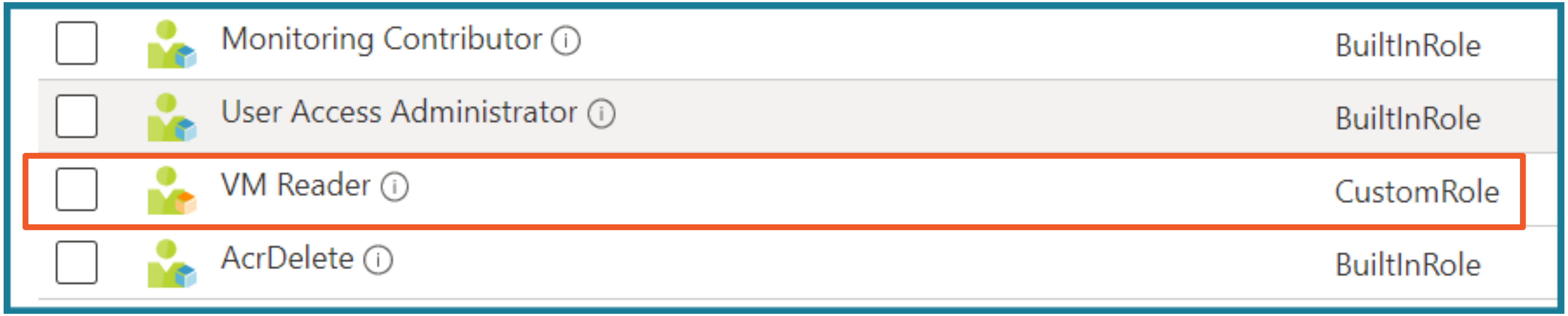
```
$role = Get-AzRoleDefinition "Virtual Machine Contributor"

$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
```

Create a Custom Role



```
PS G:\> (Get-AzRoleDefinition "VM reader").actions
Microsoft.Storage/*/read
Microsoft.Network/*/read
Microsoft.Compute/*/read
```

Custom Role Assignments



□	Monitoring Contributor ⓘ	BuiltInRole
□	User Access Administrator ⓘ	BuiltInRole
□	VM Reader ⓘ	CustomRole
□	AcrDelete ⓘ	BuiltInRole

Demo

Manage Role-based Access Control

Exam Review

Manage Role-based access control

- Roles can be assigned to:
  - Users
  - Groups
  - Applications
- Security principals include:
  - Users
  - Groups
  - Service principal
  - Managed identity
- Custom roles can be assigned across tenants

Exam Review

Manage Role-based access control

- Roles include
  - Owner
  - Contributor
  - Reader
  - User access administrator
- Deny assignment overrules all
- View effective role assignments
  - Get-AzRoleAssignment
- Custom roles
  - Modify existing role
    - Get-AzRoleDefinition
    - New-AzRoleDefinition

For Further Learning

Remember the course exercise files

- Links to the Azure Docs sites for additional studying and deeper dives
- Any code used in the demos.
- PowerPoint slides for review purposes

Questions?

- Join the conversation in the discussion tab in the Pluralsight player
- Hit me up on the Twitter @teskemj