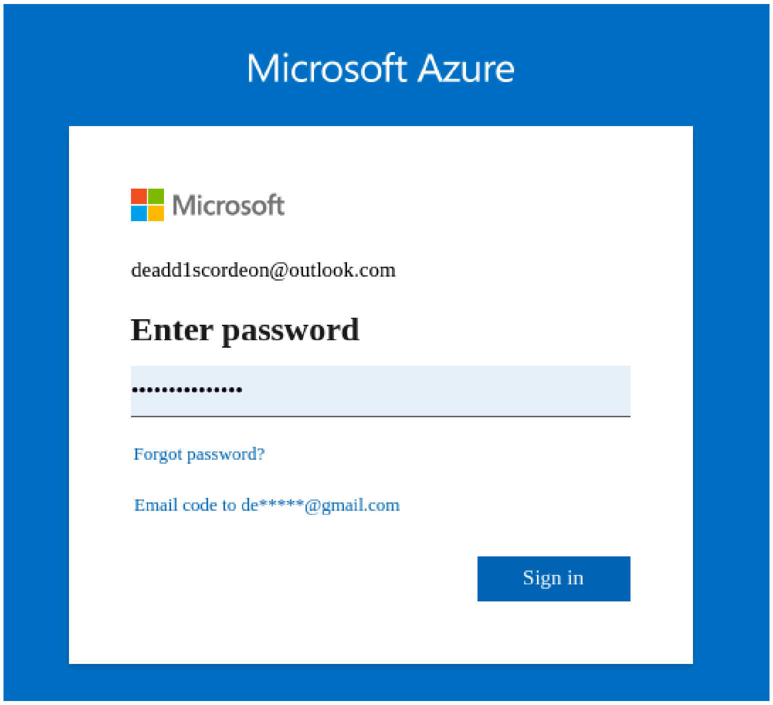
AZ-104-Microsoft Azure Administrator Kateryna Bakhmat

Lab 02a - Manage Subscriptions and RBAC

Task 1: Implement Management Groups

1.Sign in to the Azure portal - https://portal.azure.com.

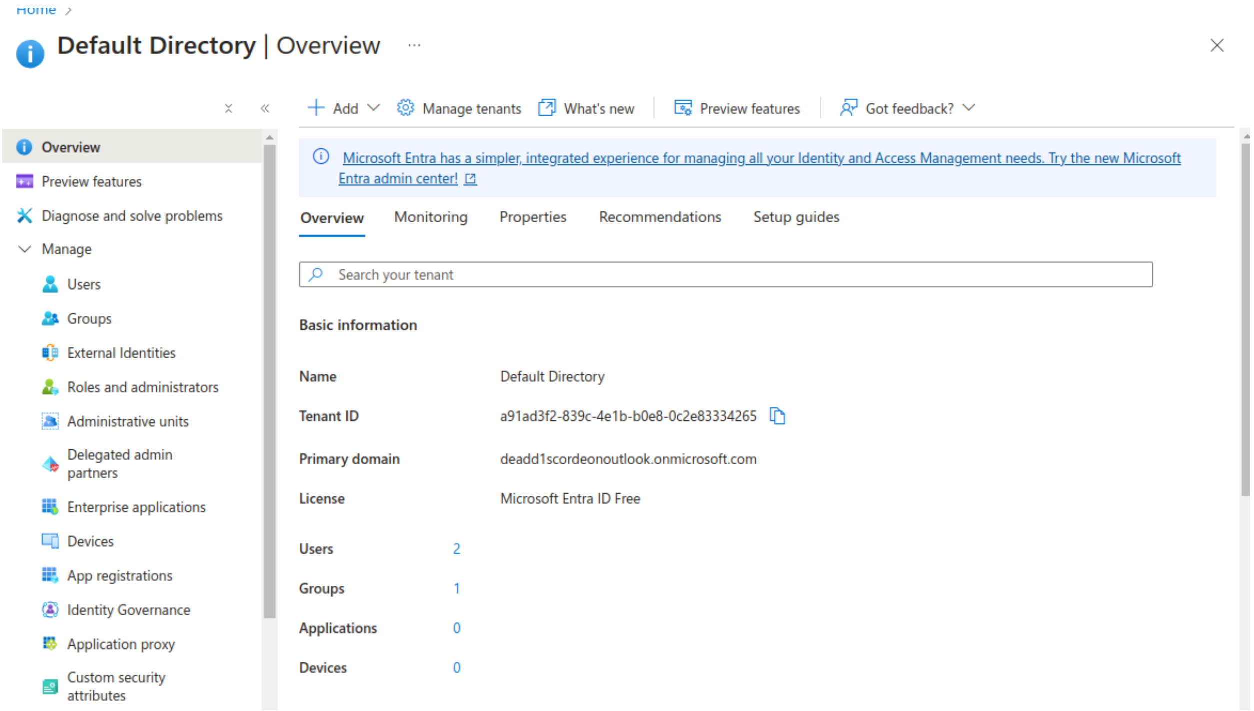


deadd1scordeon@outlook.com

Enter password

•••••••••••••••

2.Search for and select Microsoft Entra ID.

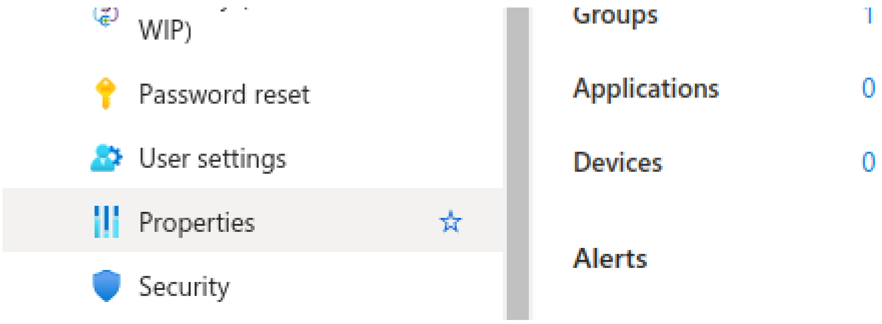


Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center!

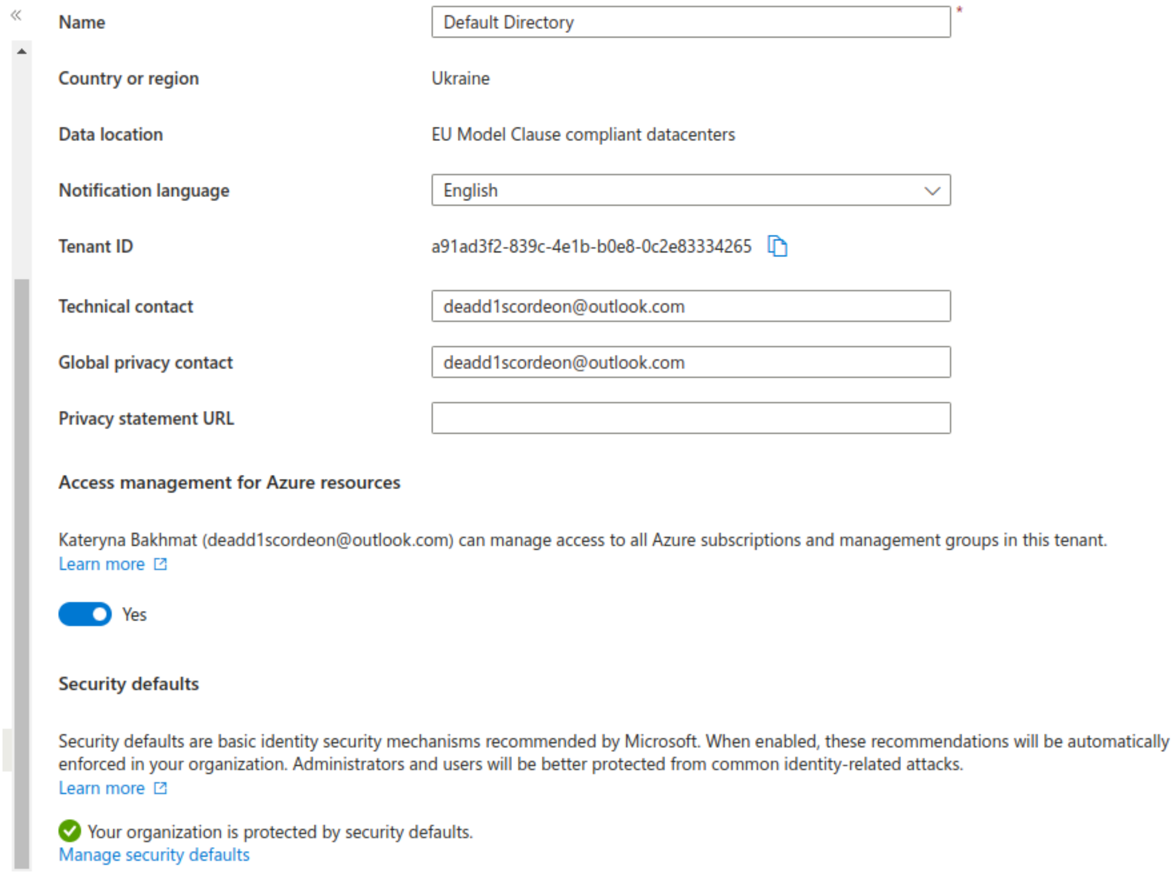
Basic information

Name	Default Directory
Tenant ID	a91ad3f2-839c-4e1b-b0e8-0c2e83334265
Primary domain	deadd1scordeonoutlook.onmicrosoft.com
License	Microsoft Entra ID Free
Users	2
Groups	1
Applications	0
Devices	0

3.In the Manage blade, select Properties.



4.Review the Access management for Azure resources area. Ensure you can manage access to all Azure subscriptions and management groups in the tenant.



Name	Default Directory *
Country or region	Ukraine
Data location	EU Model Clause compliant datacenters
Notification language	English
Tenant ID	a91ad3f2-839c-4e1b-b0e8-0c2e83334265
Technical contact	deadd1scordeon@outlook.com
Global privacy contact	deadd1scordeon@outlook.com
Privacy statement URL	

Access management for Azure resources

Kateryna Bakhmat (deadd1scordeon@outlook.com) can manage access to all Azure subscriptions and management groups in this tenant.
Learn more

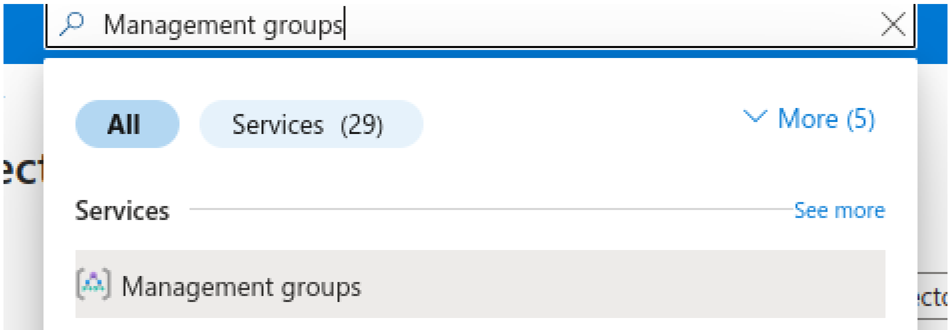
● Yes

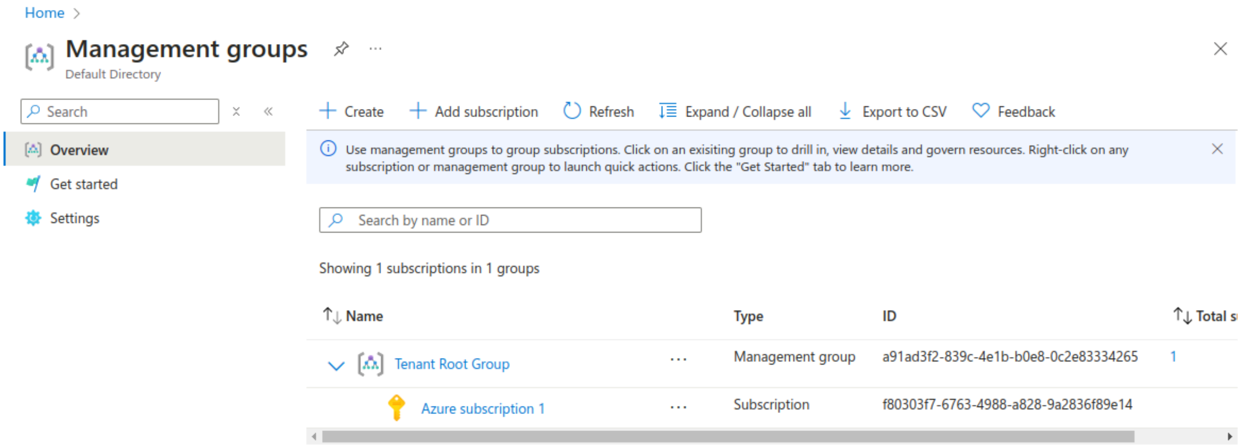
Security defaults

Security defaults are basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity-related attacks.
Learn more

✓ Your organization is protected by security defaults.
Manage security defaults

5.Search for and select Management groups.



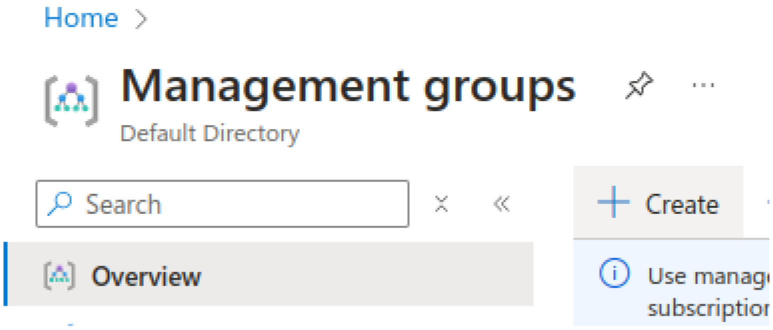


Use management groups to group subscriptions. Click on an exisiting group to drill in, view details and govern resources. Right-click on any subscription or management group to launch quick actions. Click the "Get Started" tab to learn more.

Showing 1 subscriptions in 1 groups

↑↓ Name		Type	ID	↑↓ Total s
Tenant Root Group	···	Management group	a91ad3f2-839c-4e1b-b0e8-0c2e83334265	1
Azure subscription 1	···	Subscription	f80303f7-6763-4988-a828-9a2836f89e14	

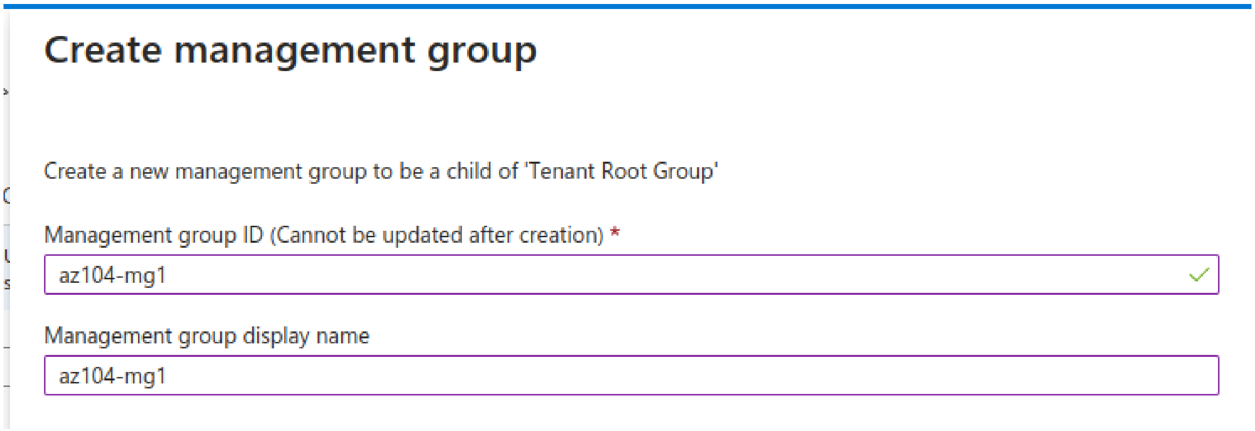
6. On the Management groups blade, click + Create.



Use manag
subscriptior

7. Create a management group with the following settings. Select Submit when you are done.

Setting	Value
Management group ID	`az104-mg1` (must be unique in the directory)
Management group display name	`az104-mg1`



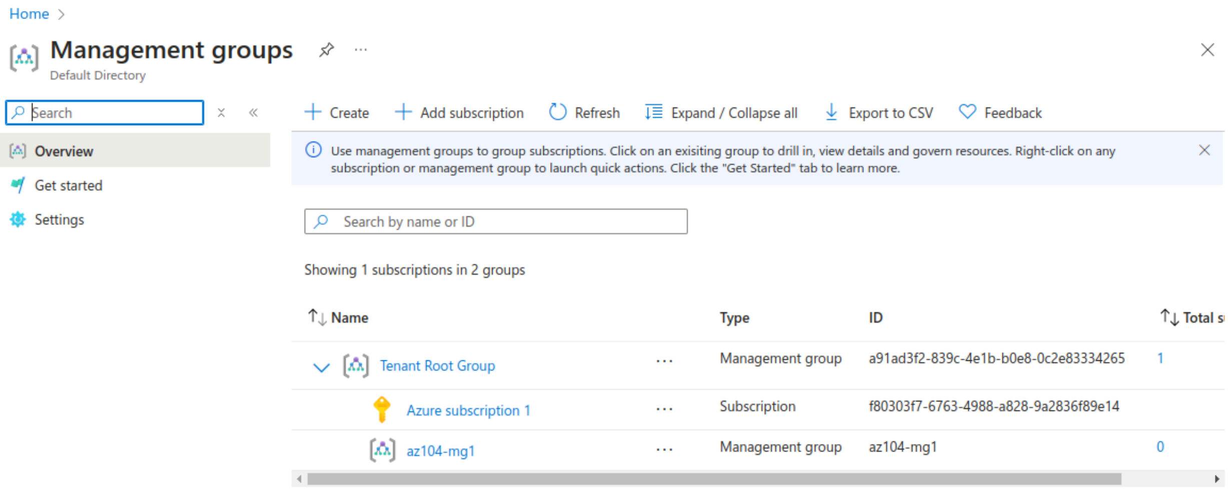
Create management group

Create a new management group to be a child of 'Tenant Root Group'

Management group ID (Cannot be updated after creation) *: az104-mg1

Management group display name: az104-mg1

8. Refresh the management group page to ensure your new management group displays. This may take a minute.



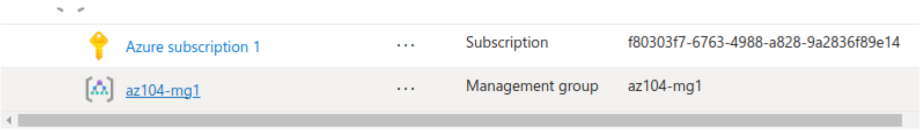
Use management groups to group subscriptions. Click on an exisiting group to drill in, view details and govern resources. Right-click on any subscription or management group to launch quick actions. Click the "Get Started" tab to learn more.

Showing 1 subscriptions in 2 groups

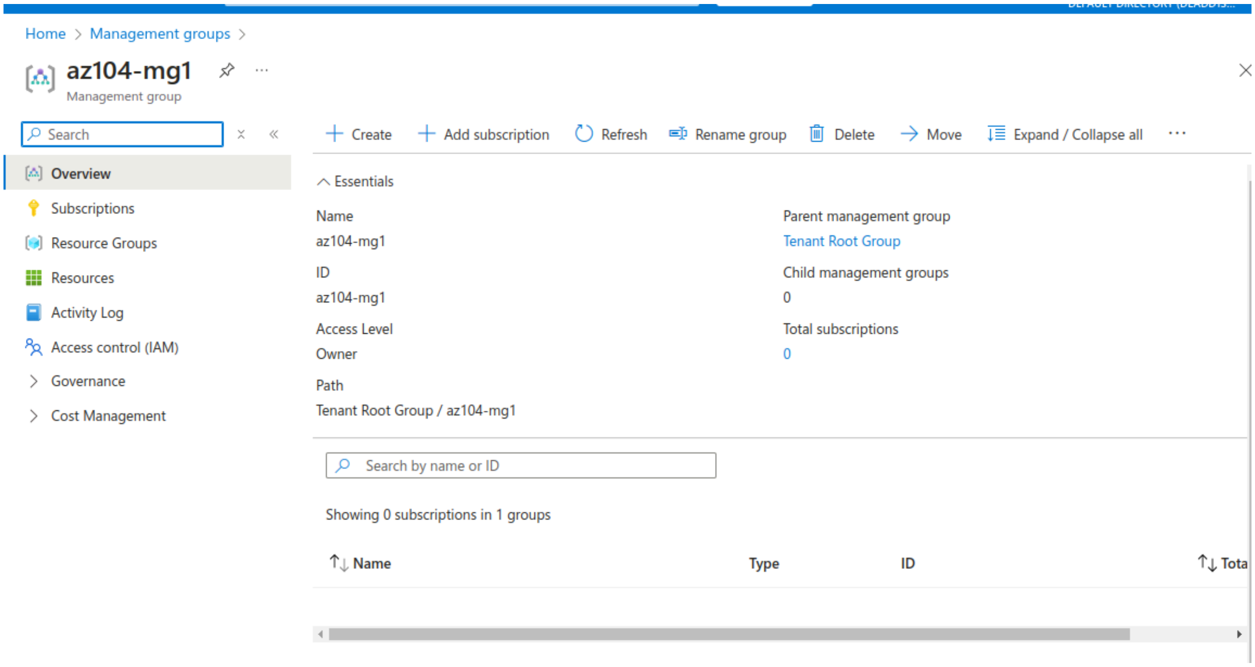
Name	Type	ID	Total s
Tenant Root Group	Management group	a91ad3f2-839c-4e1b-b0e8-0c2e83334265	1
Azure subscription 1	Subscription	f80303f7-6763-4988-a828-9a2836f89e14	
az104-mg1	Management group	az104-mg1	0

Task 2: Review and assign a built-in Azure role

1.Select the az104-mg1 management group.



Azure subscription 1	...	Subscription	f80303f7-6763-4988-a828-9a2836f89e14
az104-mg1	...	Management group	az104-mg1



Home > Management groups >

az104-mg1

Management group

Essentials

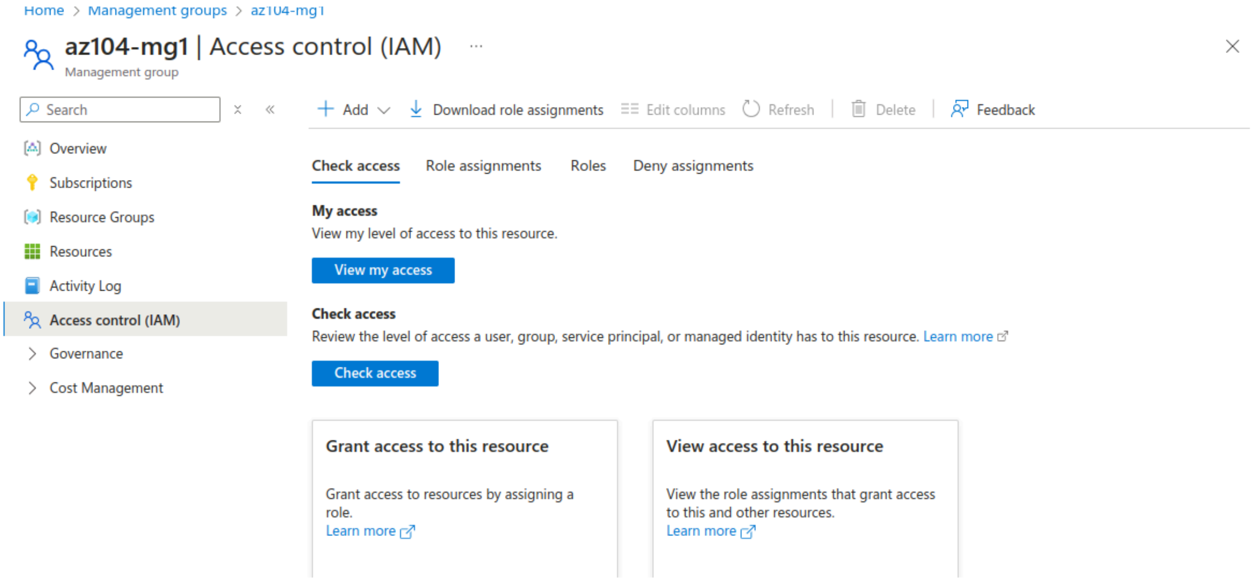
Name az104-mg1	Parent management group Tenant Root Group
ID az104-mg1	Child management groups 0
Access Level Owner	Total subscriptions 0
Path Tenant Root Group / az104-mg1	

Search by name or ID

Showing 0 subscriptions in 1 groups

Name	Type	ID	Tota

2. Select the Access control (IAM) blade, and then the Roles tab.



Home > Management groups > az104-mg1

az104-mg1 | Access control (IAM)

Management group

My access

View my level of access to this resource.

Check access

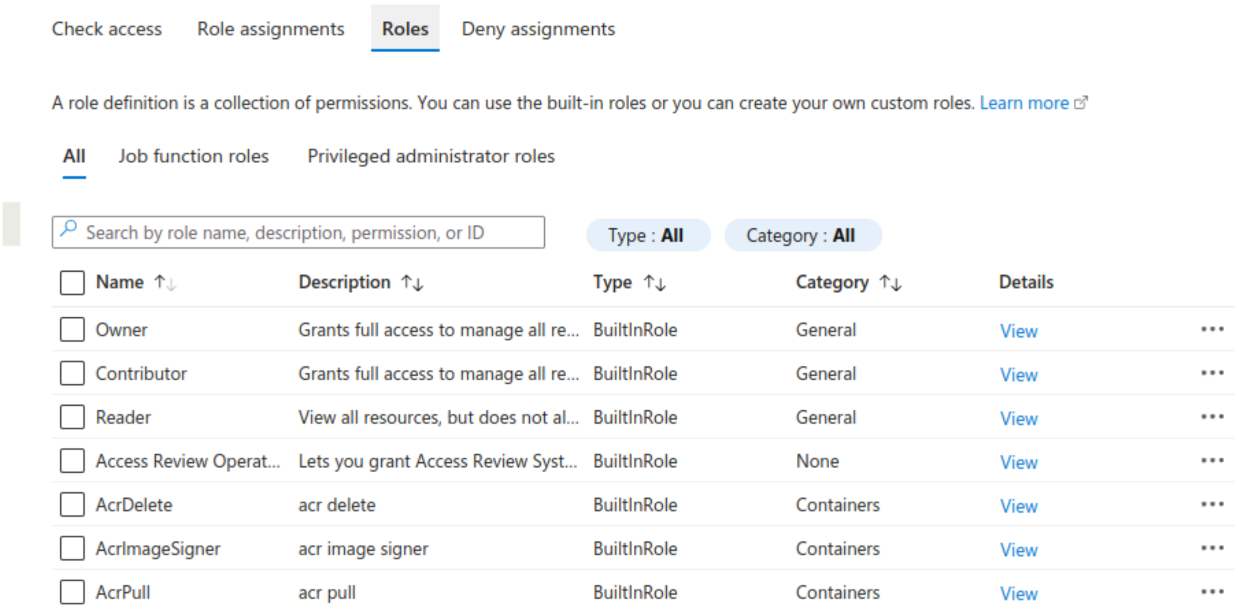
Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Grant access to this resource

Grant access to resources by assigning a role.
Learn more

View access to this resource

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



Check access | Role assignments | **Roles** | Deny assignments

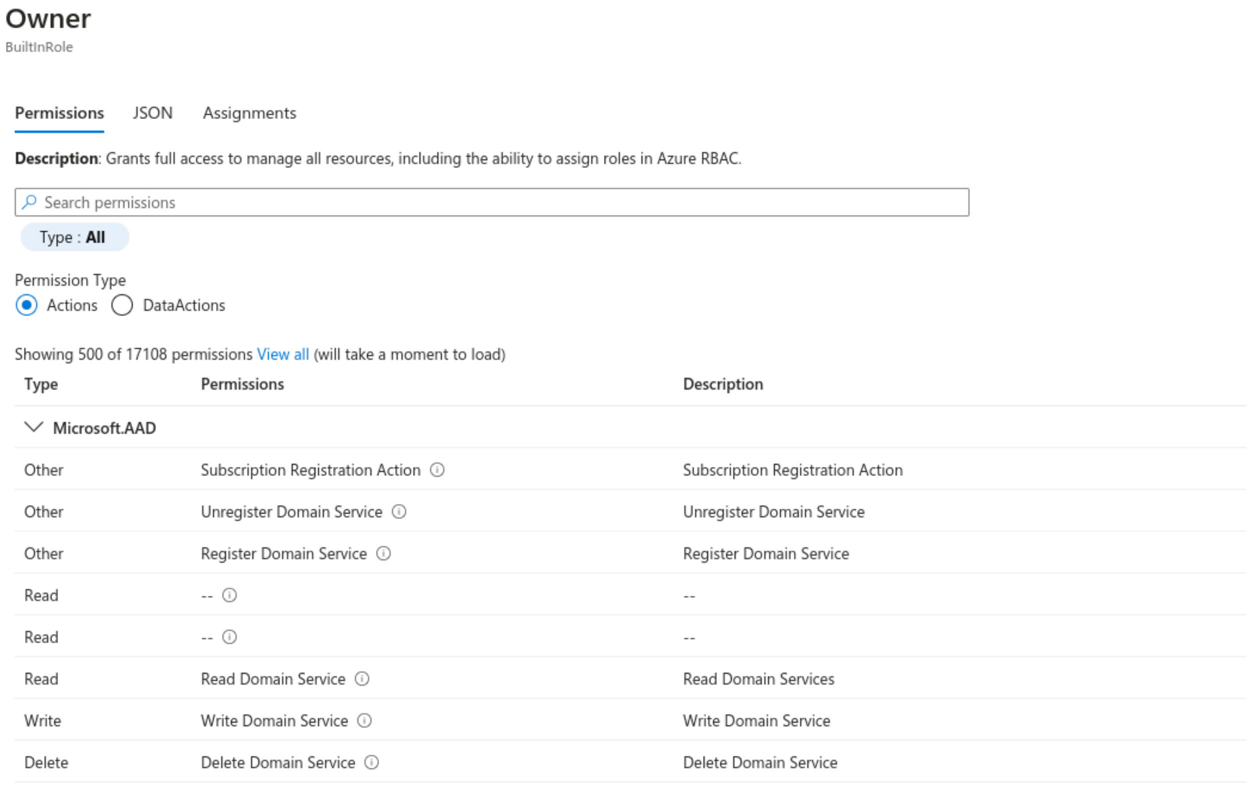
A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more

All | Job function roles | Privileged administrator roles

Search by role name, description, permission, or ID | Type : **All** | Category : **All**

□	Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details	
□	Owner	Grants full access to manage all re...	BuiltInRole	General	View	•••
□	Contributor	Grants full access to manage all re...	BuiltInRole	General	View	•••
□	Reader	View all resources, but does not al...	BuiltInRole	General	View	•••
□	Access Review Operat...	Lets you grant Access Review Syst...	BuiltInRole	None	View	•••
□	AcrDelete	acr delete	BuiltInRole	Containers	View	•••
□	AcrImageSigner	acr image signer	BuiltInRole	Containers	View	•••
□	AcrPull	acr pull	BuiltInRole	Containers	View	•••

3.Scroll through the built-in role definitions that are available. View a role to get detailed information about the Permissions, JSON, and Assignments. You will often use owner, contributor, and reader.



Owner

BuiltInRole

Permissions | JSON | Assignments

Description: Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.

Search permissions

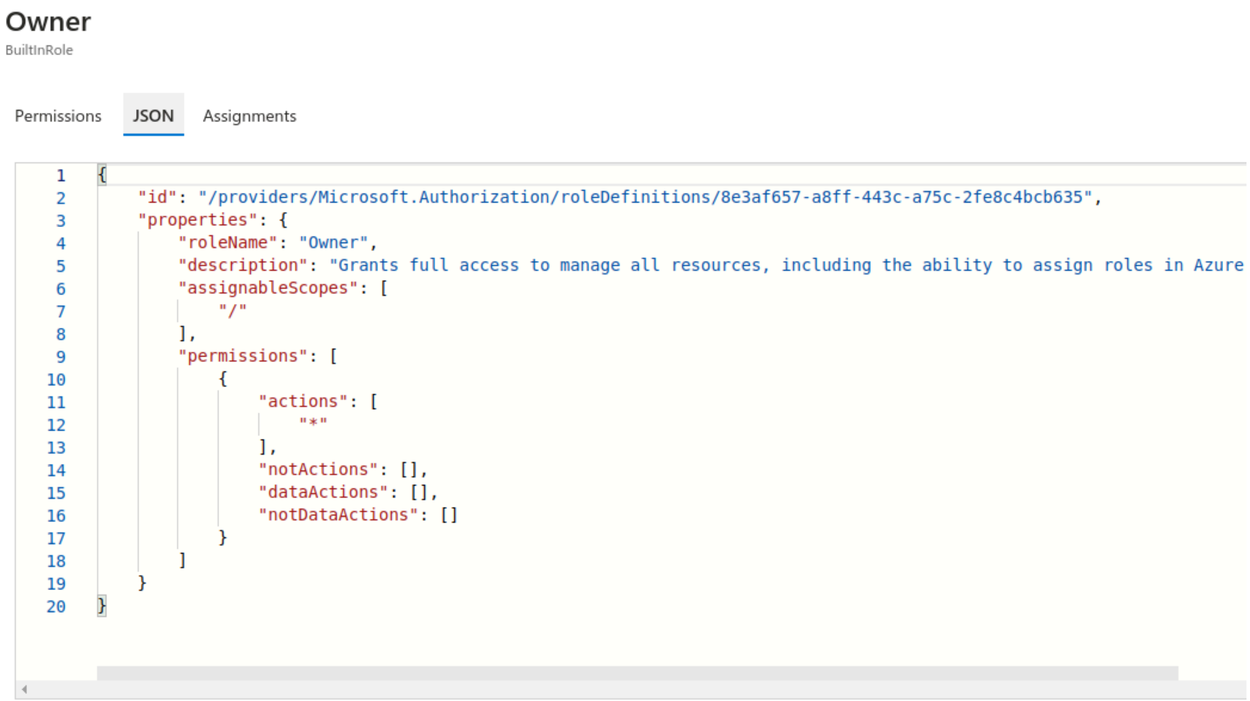
Type : **All**

Permission Type

● Actions ○ DataActions

Showing 500 of 17108 permissions View all (will take a moment to load)

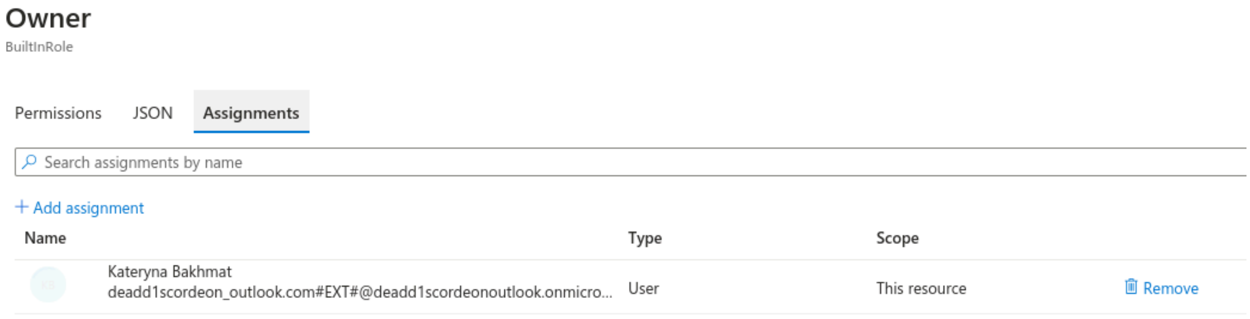
Type	Permissions	Description
Microsoft.AAD		
Other	Subscription Registration Action ⓘ	Subscription Registration Action
Other	Unregister Domain Service ⓘ	Unregister Domain Service
Other	Register Domain Service ⓘ	Register Domain Service
Read	-- ⓘ	--
Read	-- ⓘ	--
Read	Read Domain Service ⓘ	Read Domain Services
Write	Write Domain Service ⓘ	Write Domain Service
Delete	Delete Domain Service ⓘ	Delete Domain Service



Owner

BuiltInRole

```
{
    "id": "/providers/Microsoft.Authorization/roleDefinitions/8e3af657-a8ff-443c-a75c-2fe8c4bcb635",
    "properties": {
        "roleName": "Owner",
        "description": "Grants full access to manage all resources, including the ability to assign roles in Azure
        "assignableScopes": [
            "/"
        ],
        "permissions": [
            {
                "actions": [
                    "*"
                ],
                "notActions": [],
                "dataActions": [],
                "notDataActions": []
            }
        ]
    }
}
```

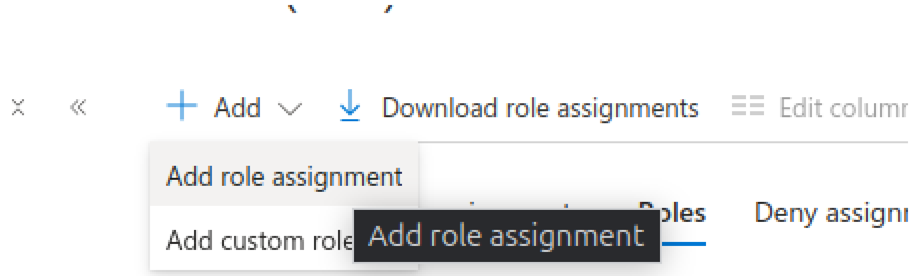


Owner

BuiltInRole

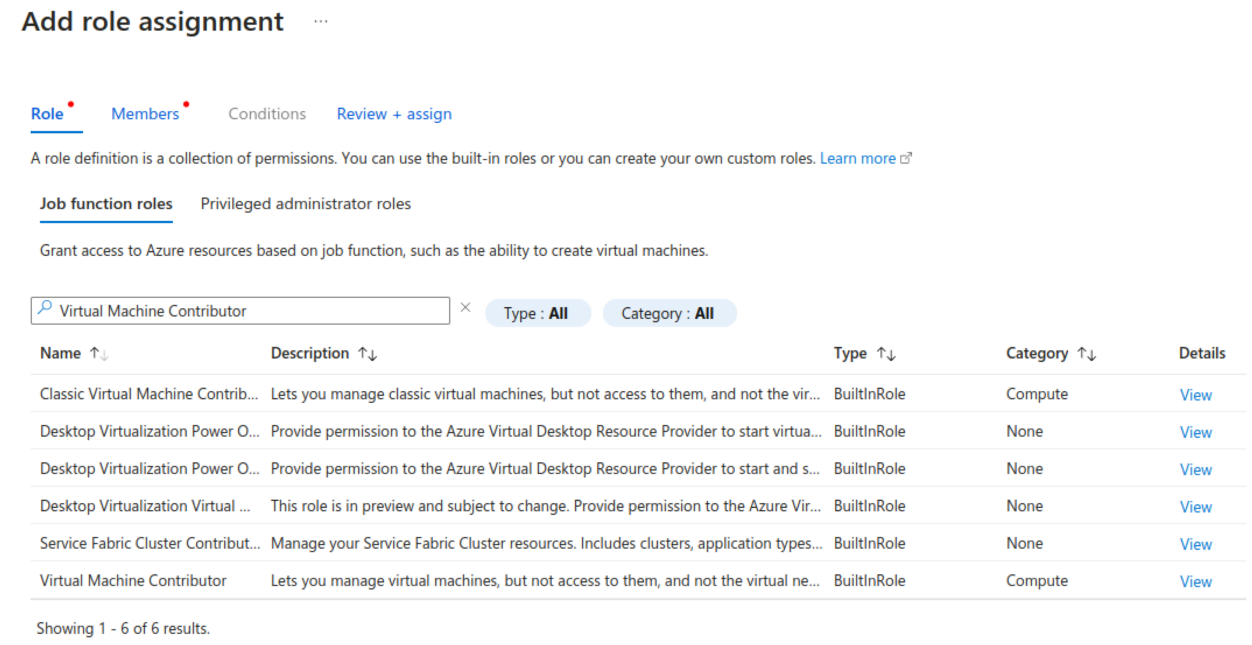
Name	Type	Scope	
Kateryna Bakhmat deadd1scordeon_outlook.com#EXT#@deadd1scordeonoutlook.onmicro...	User	This resource	Remove

4.Select + Add, from the drop-down menu, select Add role assignment.



5. On the Add role assignment blade, search for and select the Virtual Machine Contributor. The Virtual machine contributor role lets you manage virtual machines, but

not access their operating system or manage the virtual network and storage account they are connected to. This is a good role for the Help Desk. Select Next.



Add role assignment ···

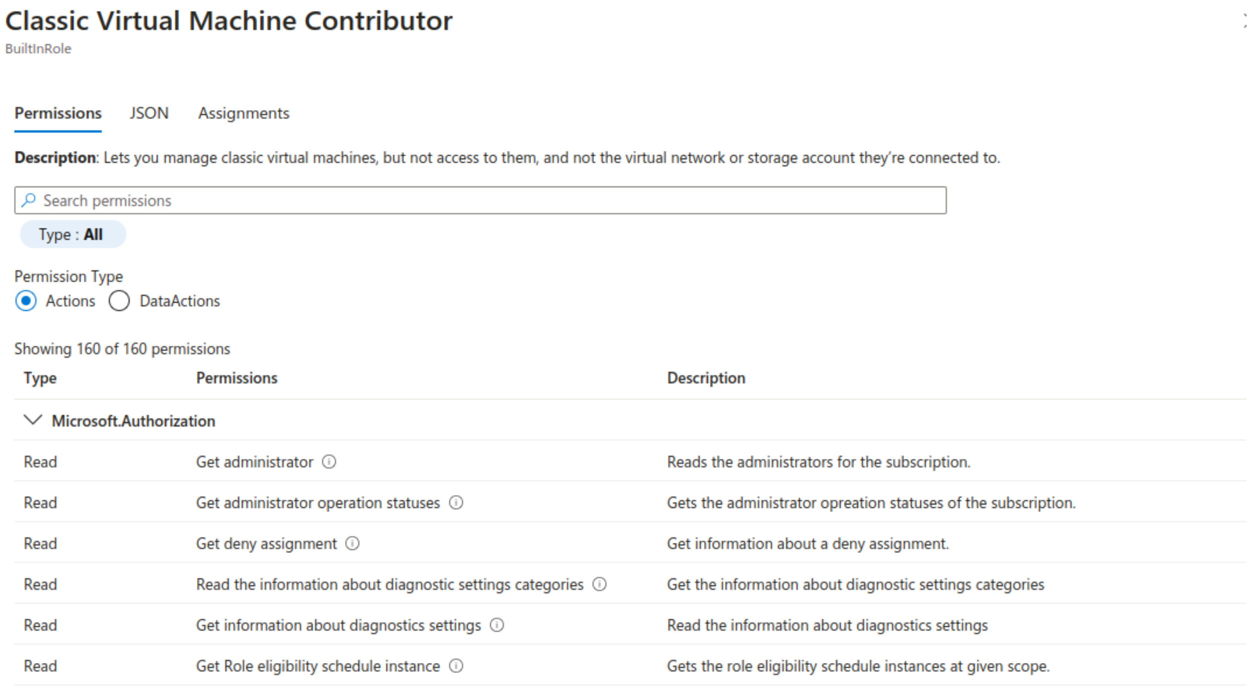
A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

Virtual Machine Contributor × Type : **All** Category : **All**

Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details
Classic Virtual Machine Contrib...	Lets you manage classic virtual machines, but not access to them, and not the vir...	BuiltInRole	Compute	View
Desktop Virtualization Power O...	Provide permission to the Azure Virtual Desktop Resource Provider to start virtua...	BuiltInRole	None	View
Desktop Virtualization Power O...	Provide permission to the Azure Virtual Desktop Resource Provider to start and s...	BuiltInRole	None	View
Desktop Virtualization Virtual ...	This role is in preview and subject to change. Provide permission to the Azure Vir...	BuiltInRole	None	View
Service Fabric Cluster Contribut...	Manage your Service Fabric Cluster resources. Includes clusters, application types...	BuiltInRole	None	View
Virtual Machine Contributor	Lets you manage virtual machines, but not access to them, and not the virtual ne...	BuiltInRole	Compute	View

Showing 1 - 6 of 6 results.



Classic Virtual Machine Contributor

BuiltInRole

Description: Lets you manage classic virtual machines, but not access to them, and not the virtual network or storage account they're connected to.

Search permissions

Type : **All**

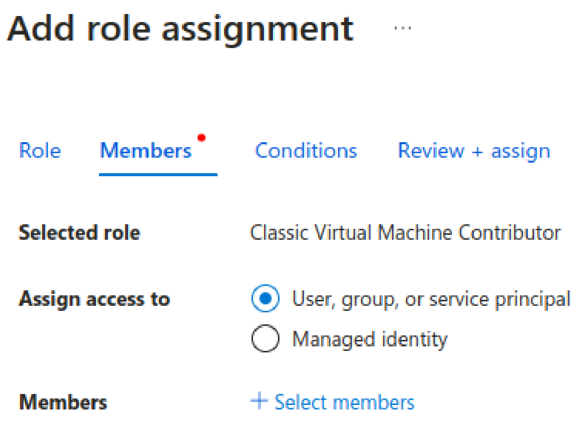
Permission Type

● Actions ○ DataActions

Showing 160 of 160 permissions

Type	Permissions	Description
Microsoft.Authorization		
Read	Get administrator ⓘ	Reads the administrators for the subscription.
Read	Get administrator operation statuses ⓘ	Gets the administrator opreation statuses of the subscription.
Read	Get deny assignment ⓘ	Get information about a deny assignment.
Read	Read the information about diagnostic settings categories ⓘ	Get the information about diagnostic settings categories
Read	Get information about diagnostics settings ⓘ	Read the information about diagnostics settings
Read	Get Role eligibility schedule instance ⓘ	Gets the role eligibility schedule instances at given scope.

6. On the Members tab, Select Members.

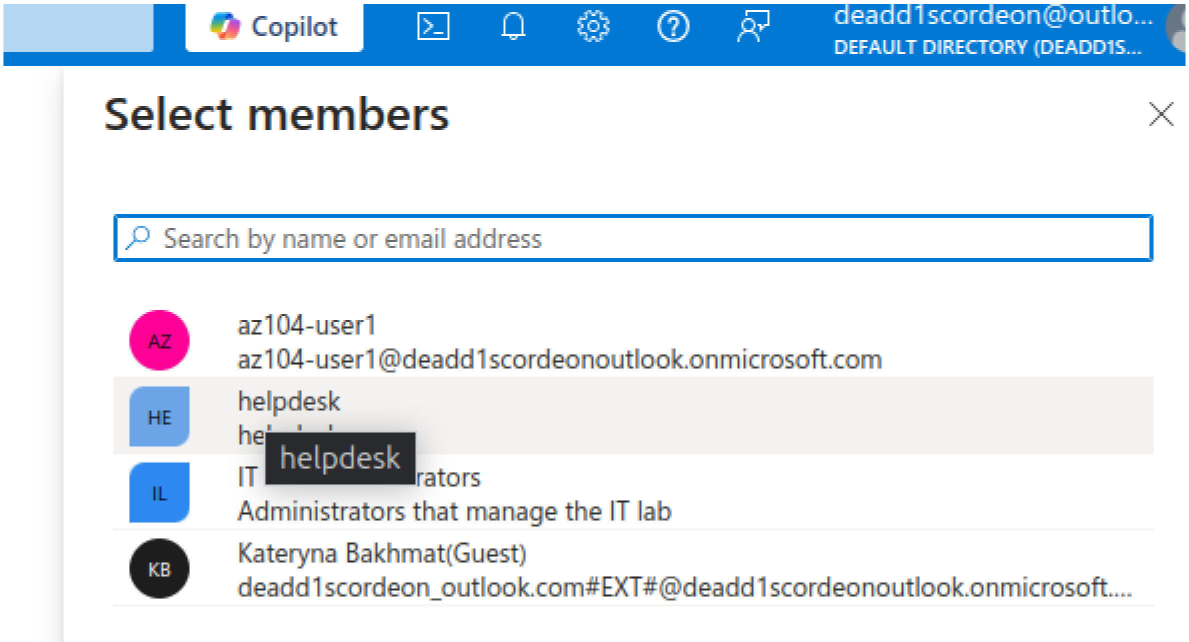


Selected role: Classic Virtual Machine Contributor

Assign access to: ● User, group, or service principal ○ Managed identity

Members

7. Search for and select the helpdesk group. Click Select.


Copilot
deadd1scordeon@outlo...
DEFAULT DIRECTORY (DEADD1S...
Select members
Search by name or email address
AZ
HE
IL
KB
helpdesk

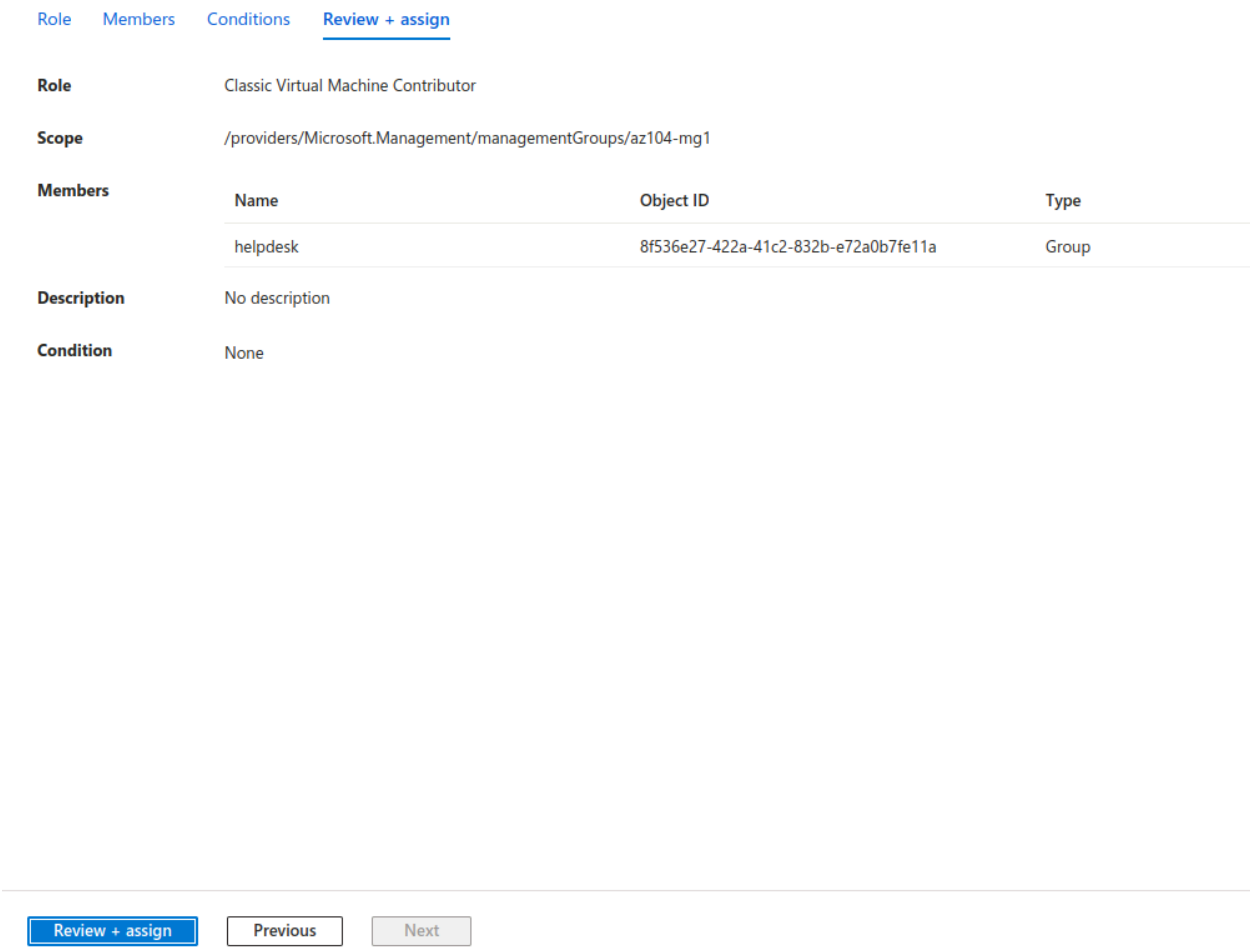
az104-user1
az104-user1@deadd1scordeonoutlook.onmicrosoft.com

helpdesk
he

IT rators
Administrators that manage the IT lab

Kateryna Bakhmat(Guest)
deadd1scordeon_outlook.com#EXT#@deadd1scordeonoutlook.onmicrosoft....

8. Click Review + assign twice to create the role assignment.

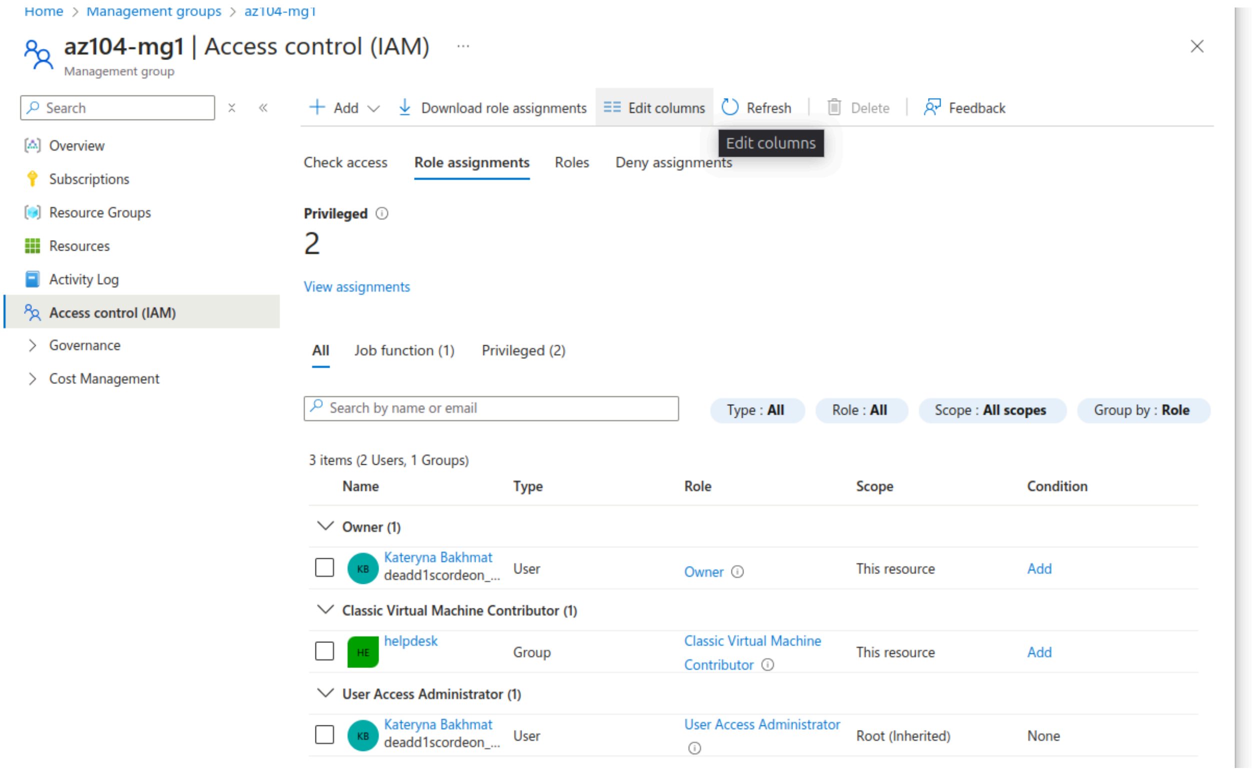


Role	Classic Virtual Machine Contributor
Scope	/providers/Microsoft.Management/managementGroups/az104-mg1
Members	

Name	Object ID	Type
helpdesk	8f536e27-422a-41c2-832b-e72a0b7fe11a	Group

Description	No description
Condition	None

9. Continue on the Access control (IAM) blade. On the Role assignments tab, confirm the helpdesk group has the Virtual Machine Contributor role.



Home > Management groups > az104-mg1

az104-mg1 | Access control (IAM) ...

Management group

Privileged ⓘ

2

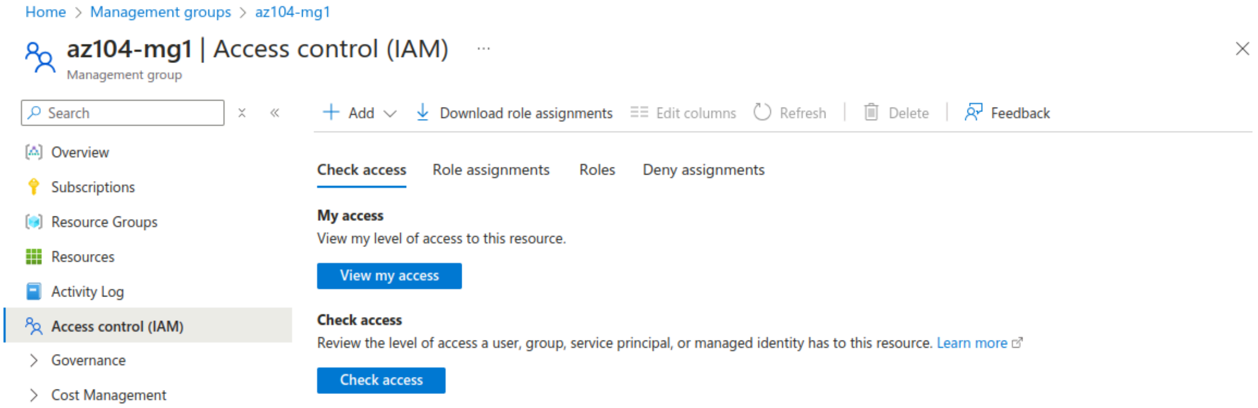
View assignments

3 items (2 Users, 1 Groups)

Name	Type	Role	Scope	Condition
Owner (1)				
□ KB Kateryna Bakhmat deadd1scordeon_...	User	Owner ⓘ	This resource	Add
Classic Virtual Machine Contributor (1)				
□ HE helpdesk	Group	Classic Virtual Machine Contributor ⓘ	This resource	Add
User Access Administrator (1)				
□ KB Kateryna Bakhmat deadd1scordeon_...	User	User Access Administrator ⓘ	Root (Inherited)	None

Task 3: Create a custom RBAC role

1. Continue working on your management group. Navigate to the Access control (IAM) blade.



Home > Management groups > az104-mg1

az104-mg1 | Access control (IAM) ...

Management group

My access

View my level of access to this resource.

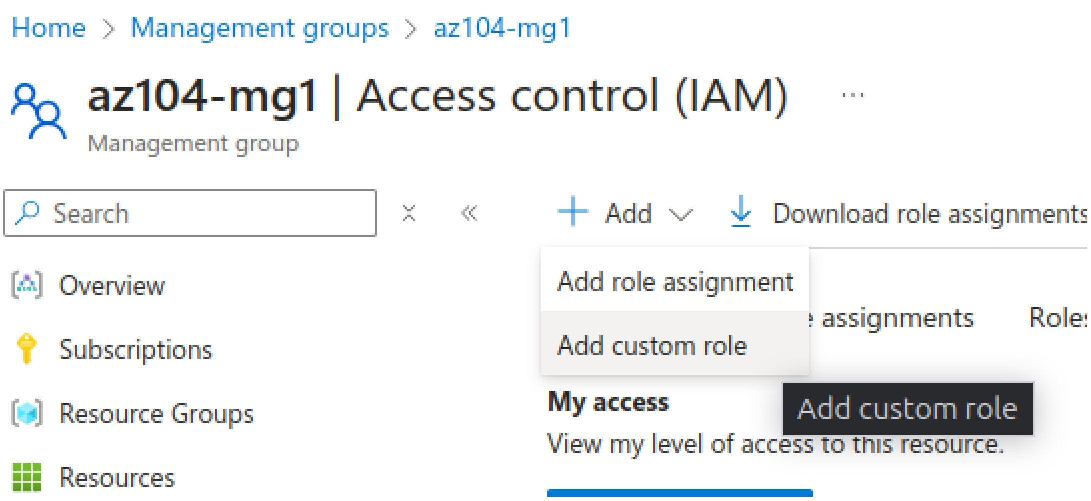
View my access

Check access

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

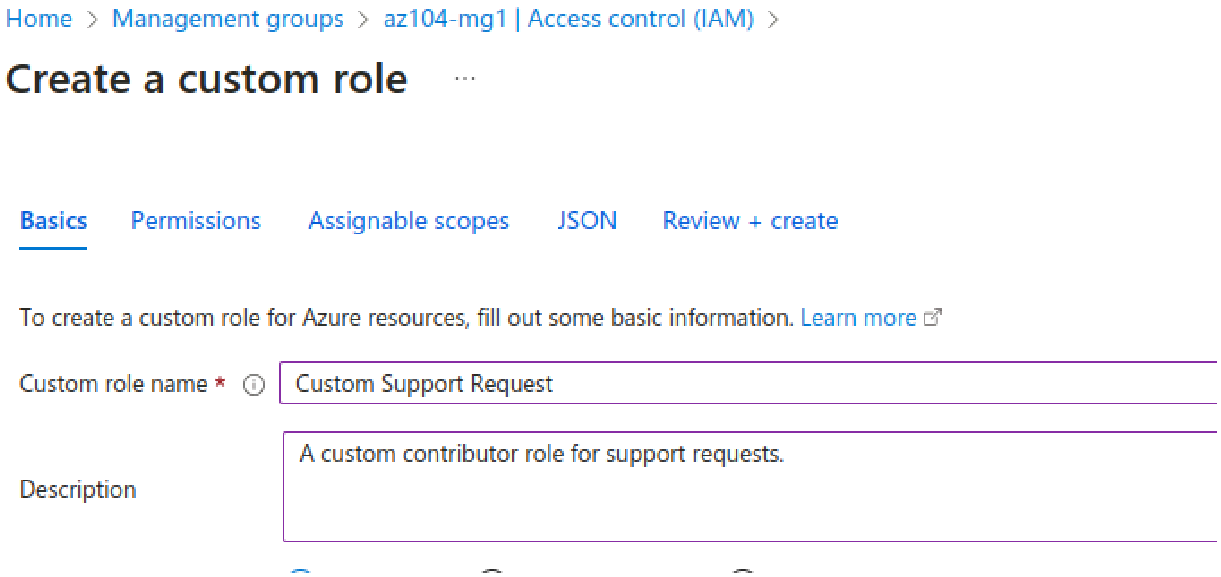
Check access

2. Select + Add, from the drop-down menu, select Add custom role.



3. On the Basics tab complete the configuration.

Setting	Value
Custom role name	`Custom Support Request`
Description	`A custom contributor role for support requests.`

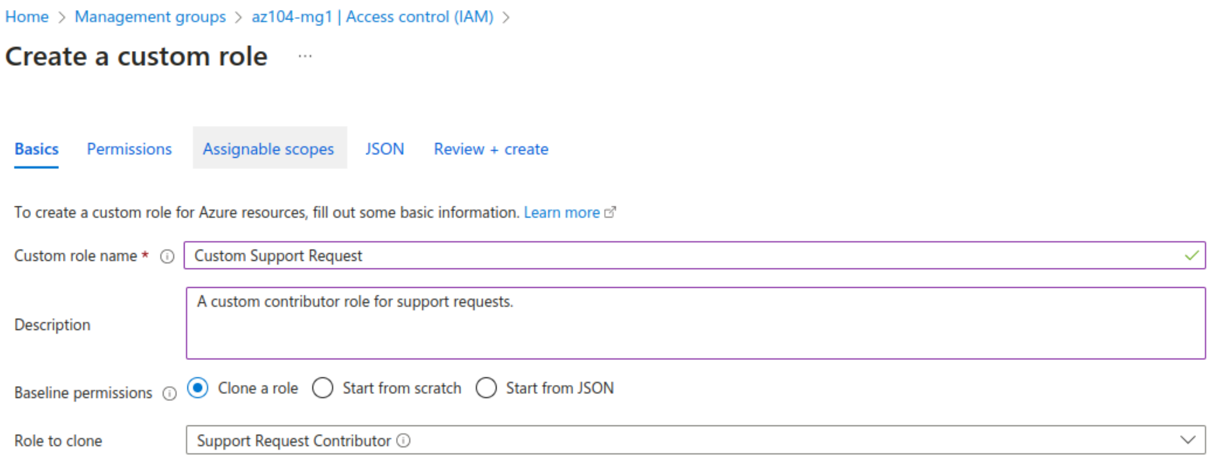


To create a custom role for Azure resources, fill out some basic information. Learn more

Custom role name * Custom Support Request

Description A custom contributor role for support requests.

4. For Baseline permissions, select Clone a role. In the Role to clone drop-down menu, select Support Request Contributor.



Home > Management groups > az104-mg1 | Access control (IAM) >

Create a custom role ...

Basics | Permissions | Assignable scopes | JSON | Review + create

To create a custom role for Azure resources, fill out some basic information. Learn more

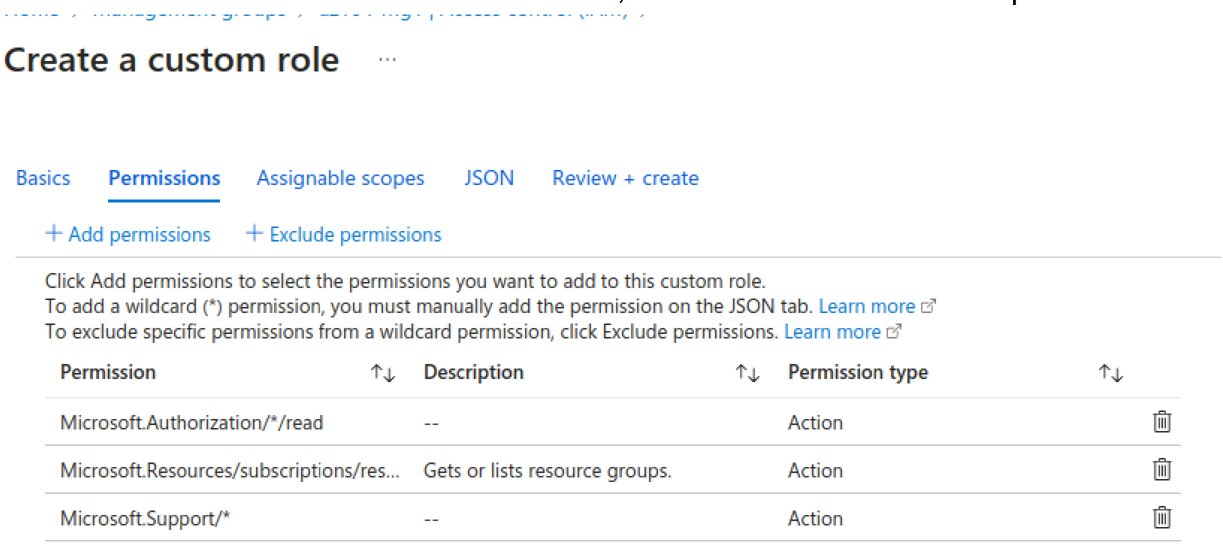
Custom role name * ⓘ Custom Support Request ✓

Description: A custom contributor role for support requests.

Baseline permissions ⓘ ● Clone a role ○ Start from scratch ○ Start from JSON

Role to clone: Support Request Contributor ⓘ

5. Select Next to move to the Permissions tab, and then select + Exclude permissions.



Create a custom role ...

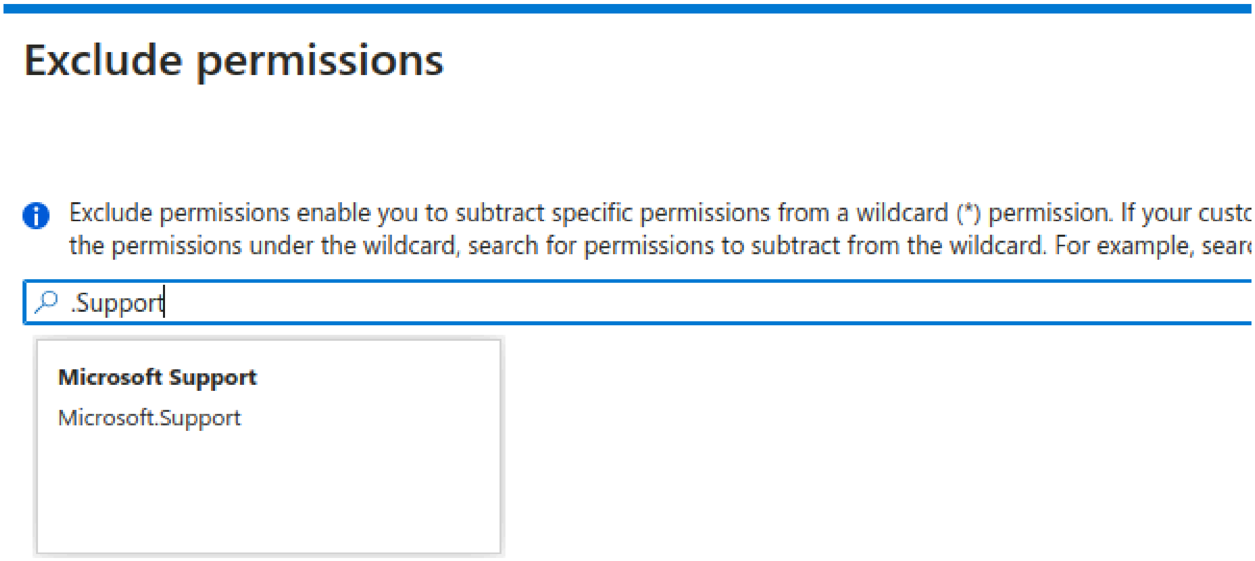
Basics | Permissions | Assignable scopes | JSON | Review + create

+ Add permissions + Exclude permissions

Click Add permissions to select the permissions you want to add to this custom role.
To add a wildcard (*) permission, you must manually add the permission on the JSON tab. Learn more
To exclude specific permissions from a wildcard permission, click Exclude permissions. Learn more

Permission ↑↓	Description ↑↓	Permission type ↑↓
Microsoft.Authorization/*/read	--	Action
Microsoft.Resources/subscriptions/res...	Gets or lists resource groups.	Action
Microsoft.Support/*	--	Action

6. In the resource provider search field, enter .Support and select Microsoft.Support.



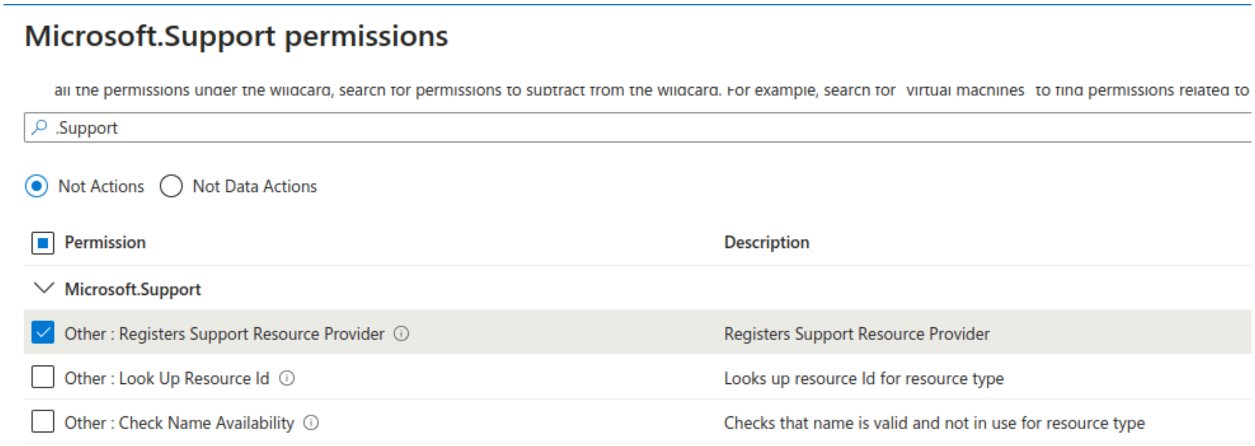
Exclude permissions

Exclude permissions enable you to subtract specific permissions from a wildcard (*) permission. If your custc
the permissions under the wildcard, search for permissions to subtract from the wildcard. For example, searc

.Support

Microsoft Support
Microsoft.Support

7. In the list of permissions, place a checkbox next to Other: Registers Support Resource Provider and then select Add. The role should be updated to include this permission as a NotAction.



Microsoft.Support permissions

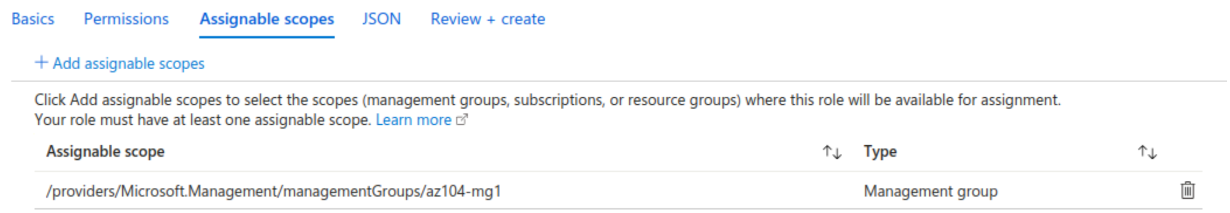
all the permissions under the wildcard, search for permissions to subtract from the wildcard. For example, search for 'virtual machines' to find permissions related to

.Support

● Not Actions ○ Not Data Actions

▣ Permission	Description
Microsoft.Support	
☑ Other : Registers Support Resource Provider ⓘ	Registers Support Resource Provider
□ Other : Look Up Resource Id ⓘ	Looks up resource Id for resource type
□ Other : Check Name Availability ⓘ	Checks that name is valid and not in use for resource type

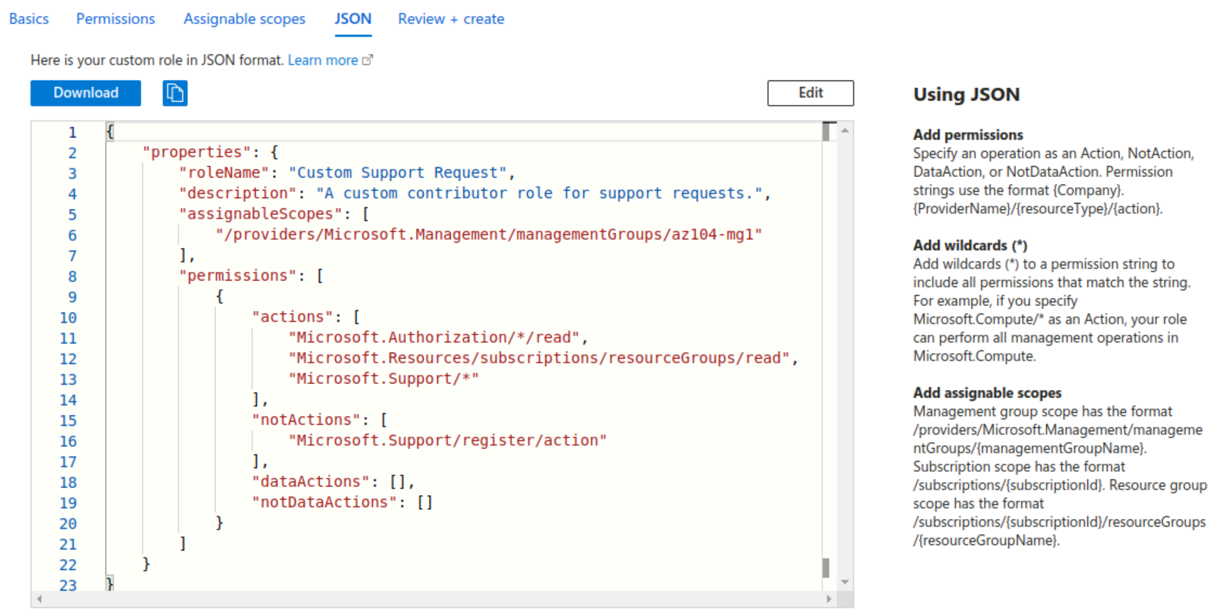
8. On the Assignable scopes tab, ensure your management group is listed, then click Next.



Click Add assignable scopes to select the scopes (management groups, subscriptions, or resource groups) where this role will be available for assignment.
Your role must have at least one assignable scope. Learn more

Assignable scope	Type
/providers/Microsoft.Management/managementGroups/az104-mg1	Management group

9. Review the JSON for the Actions, NotActions, and AssignableScopes that are customized in the role.



Here is your custom role in JSON format. Learn more

```
{
    "properties": {
        "roleName": "Custom Support Request",
        "description": "A custom contributor role for support requests.",
        "assignableScopes": [
            "/providers/Microsoft.Management/managementGroups/az104-mg1"
        ],
        "permissions": [
            {
                "actions": [
                    "Microsoft.Authorization/*/read",
                    "Microsoft.Resources/subscriptions/resourceGroups/read",
                    "Microsoft.Support/*"
                ],
                "notActions": [
                    "Microsoft.Support/register/action"
                ],
                "dataActions": [],
                "notDataActions": []
            }
        ]
    }
}
```

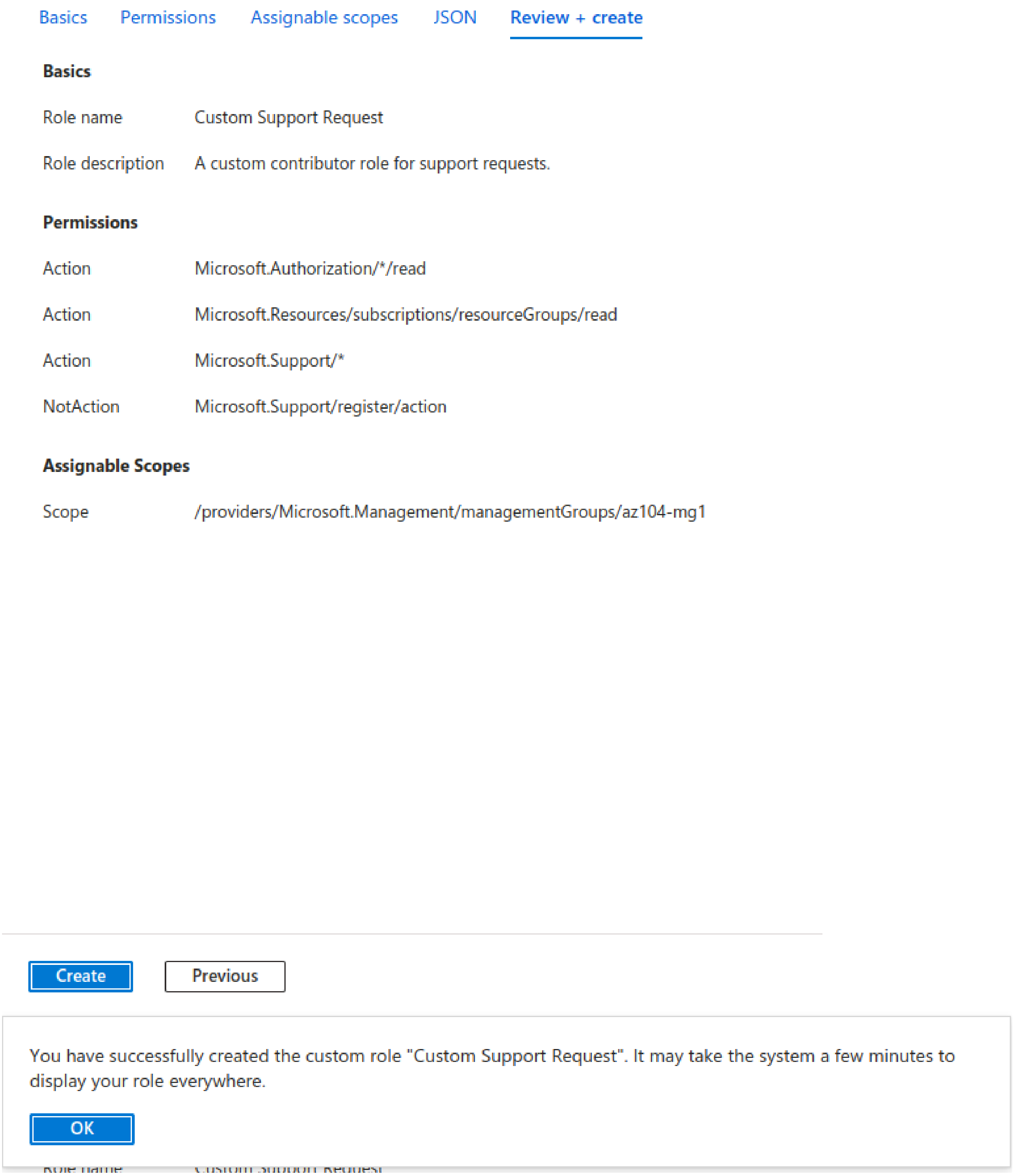
Using JSON

Add permissions
Specify an operation as an Action, NotAction, DataAction, or NotDataAction. Permission strings use the format {Company}.{ProviderName}/{resourceType}/{action}.

Add wildcards (*)
Add wildcards (*) to a permission string to include all permissions that match the string. For example, if you specify Microsoft.Compute/* as an Action, your role can perform all management operations in Microsoft.Compute.

Add assignable scopes
Management group scope has the format /providers/Microsoft.Management/managementGroups/{managementGroupName}. Subscription scope has the format /subscriptions/{subscriptionId}. Resource group scope has the format /subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}.

10. Select Review + Create, and then select Create.



Basics

Role name	Custom Support Request
Role description	A custom contributor role for support requests.

Permissions

Action	Microsoft.Authorization/*/read
Action	Microsoft.Resources/subscriptions/resourceGroups/read
Action	Microsoft.Support/*
NotAction	Microsoft.Support/register/action

Assignable Scopes

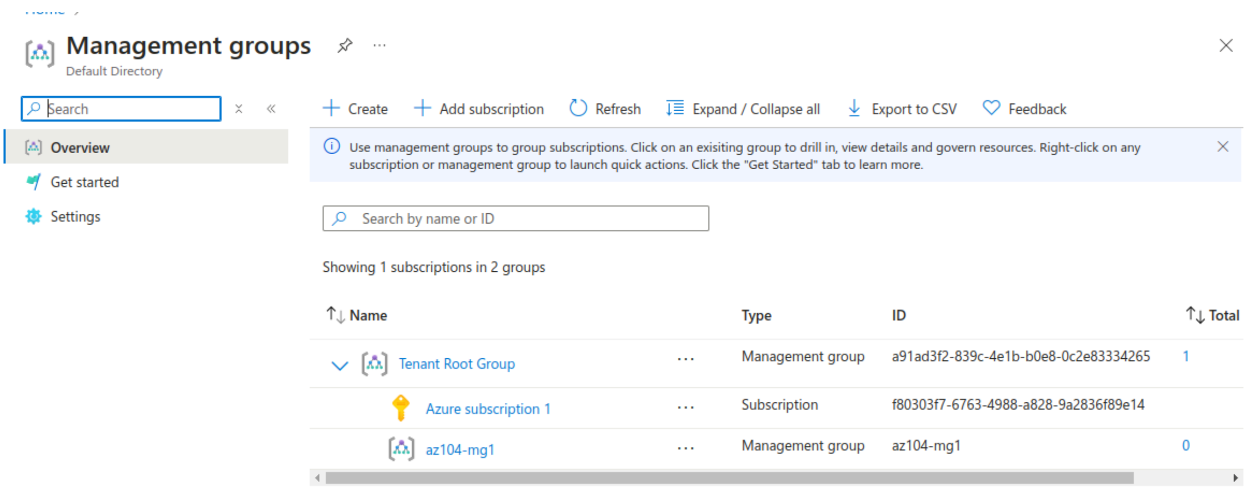
Scope	/providers/Microsoft.Management/managementGroups/az104-mg1

You have successfully created the custom role "Custom Support Request". It may take the system a few minutes to display your role everywhere.

Role name Custom Support Request

Task 4: Monitor role assignments with the Activity Log

1. In the portal locate the az104-mg1 resource and select Activity log. The activity log provides insight into subscription-level events.

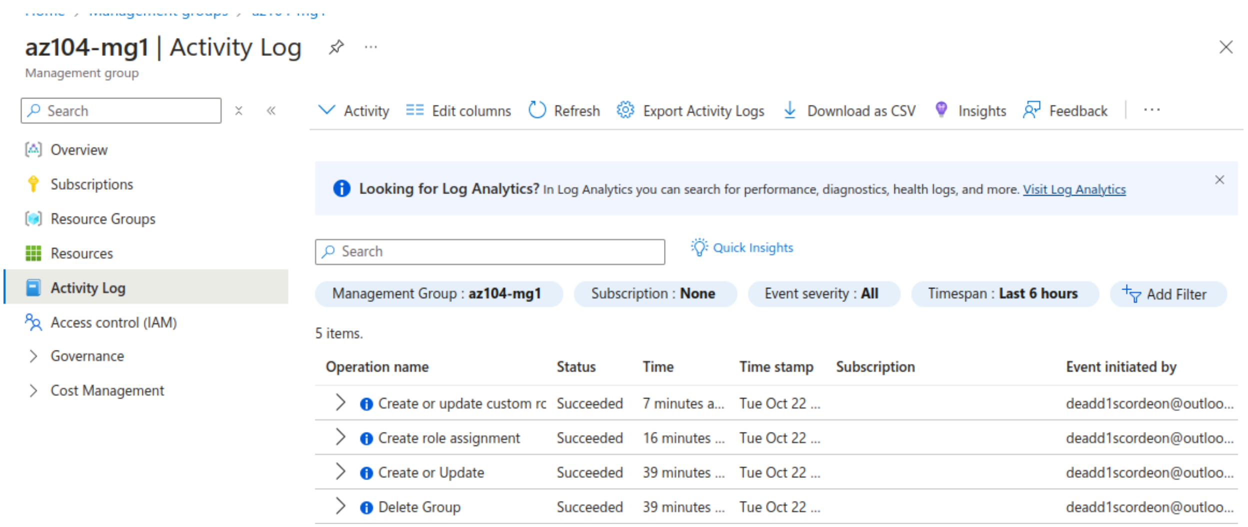


Management groups
Default Directory

Use management groups to group subscriptions. Click on an exisiting group to drill in, view details and govern resources. Right-click on any subscription or management group to launch quick actions. Click the "Get Started" tab to learn more.

Showing 1 subscriptions in 2 groups

Name		Type	ID	Total
Tenant Root Group	···	Management group	a91ad3f2-839c-4e1b-b0e8-0c2e83334265	1
Azure subscription 1	···	Subscription	f80303f7-6763-4988-a828-9a2836f89e14	
az104-mg1	···	Management group	az104-mg1	0



az104-mg1 | Activity Log
Management group

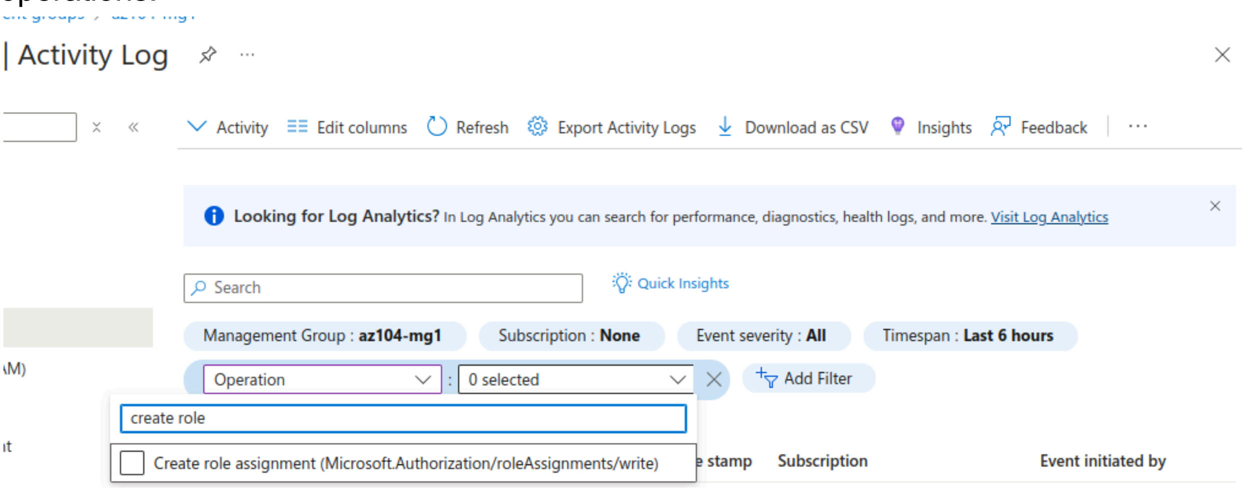
Looking for Log Analytics? In Log Analytics you can search for performance, diagnostics, health logs, and more. Visit Log Analytics

Management Group : **az104-mg1** Subscription : **None** Event severity : **All** Timespan : **Last 6 hours** Add Filter

5 items.

Operation name	Status	Time	Time stamp	Subscription	Event initiated by
Create or update custom rc	Succeeded	7 minutes a...	Tue Oct 22 ...		deadd1scordeon@outloo...
Create role assignment	Succeeded	16 minutes ...	Tue Oct 22 ...		deadd1scordeon@outloo...
Create or Update	Succeeded	39 minutes ...	Tue Oct 22 ...		deadd1scordeon@outloo...
Delete Group	Succeeded	39 minutes ...	Tue Oct 22 ...		deadd1scordeon@outloo...

2.Review the activites for role assignments. The activity log can be filtered for specific operations.



| Activity Log

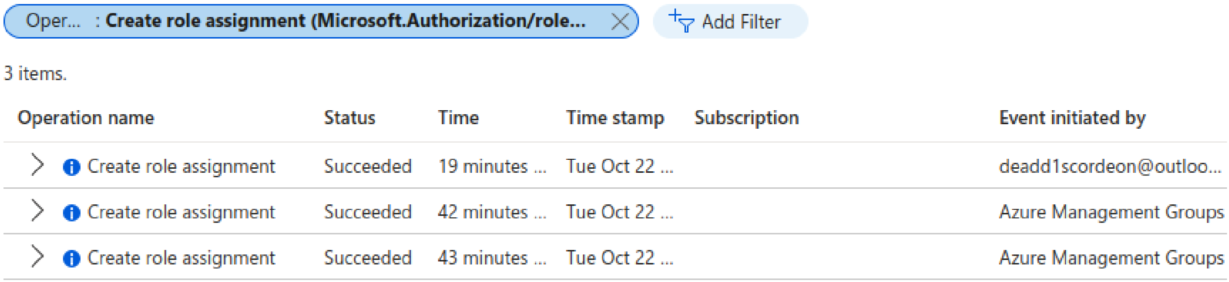
Looking for Log Analytics? In Log Analytics you can search for performance, diagnostics, health logs, and more. Visit Log Analytics

Management Group : **az104-mg1** Subscription : **None** Event severity : **All** Timespan : **Last 6 hours**

Operation : 0 selected × Add Filter

create role

□ Create role assignment (Microsoft.Authorization/roleAssignments/write)



Oper... : **Create role assignment (Microsoft.Authorization/role...**

3 items.

Operation name	Status	Time	Time stamp	Subscription	Event initiated by
Create role assignment	Succeeded	19 minutes ...	Tue Oct 22 ...		deadd1scordeon@outloo...
Create role assignment	Succeeded	42 minutes ...	Tue Oct 22 ...		Azure Management Groups
Create role assignment	Succeeded	43 minutes ...	Tue Oct 22 ...		Azure Management Groups