

# AZ-104 Azure RBAC - Assigning access to resources

## Secure Azure RBAC

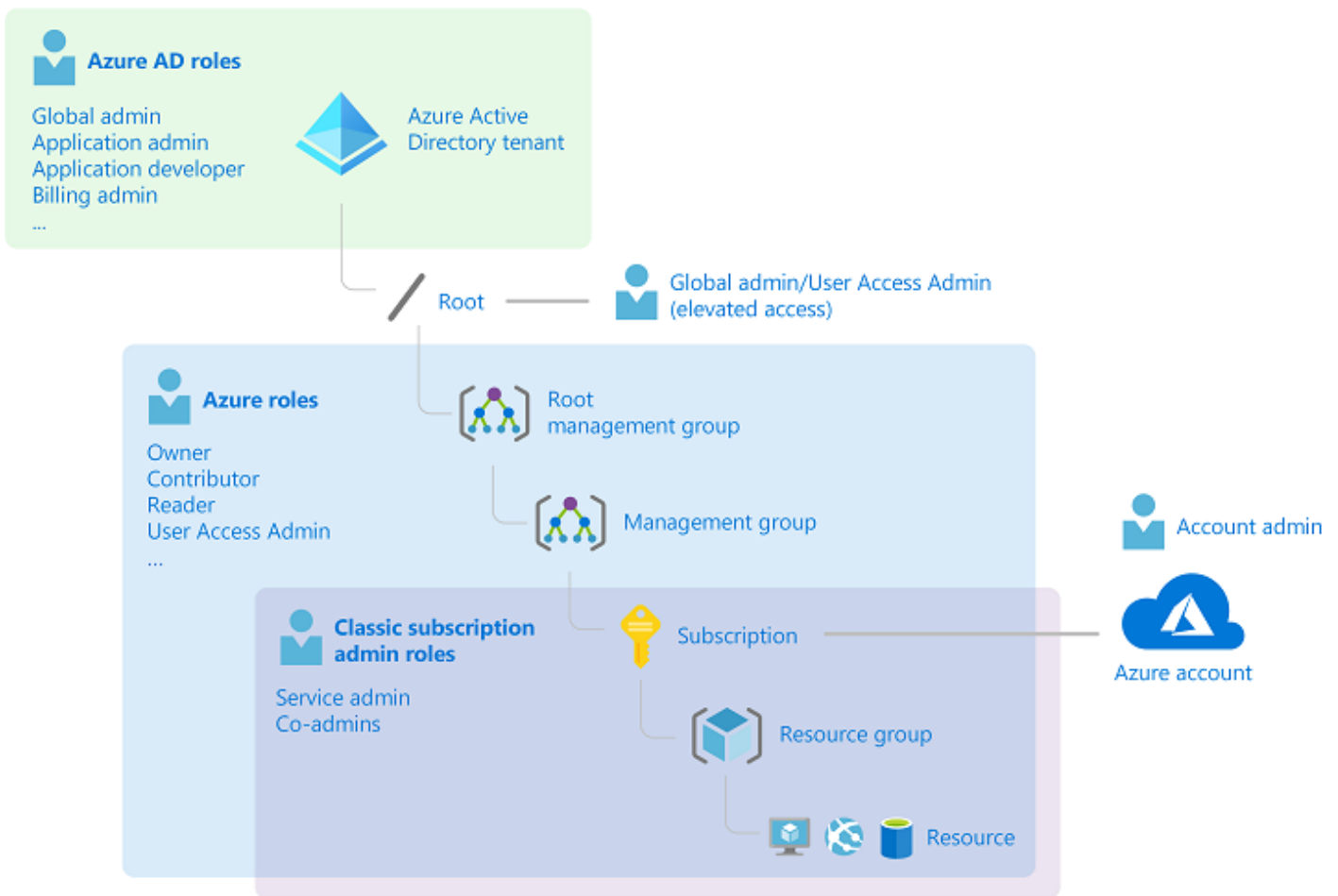
- Explaining Azure RBAC
- Understanding Role definitions
- Additive Property

## **Explaining Azure RBAC**

Azure RBAC is an authorization system

- Security Principal: Defining the who we want to authorize, WHO?
- Role Definition: assign a role definition to that identity, WHAT?
- Scope: where we are defining where we are going to perform this actions, WHERE?

We have to provide this access explicit, there is an implicit deny



## Understanding Role Definitions

### Contributor

- **Actions:** Define what actions are allowed to be performed on the management plane, managing resources inside of Azure like starting or stopping virtual machines.
- **NotActions:** Actions we are going to deny on managing resources inside of Azure. For example, if we wanted to allow a user to perform a restart on a virtual machine, we could outline that in Actions, but it could be overwritten and overruled by a NotAction denying that same action inside this role definition.

Then we have the next component, which are our DataActions, and our NotDataActions. And these are the same kind of thing as our Actions and NotActions, except for rather than being on the control plane of managing Azure resources, this will take an impact on data-related actions such as working with data inside of Azure Storage accounts.

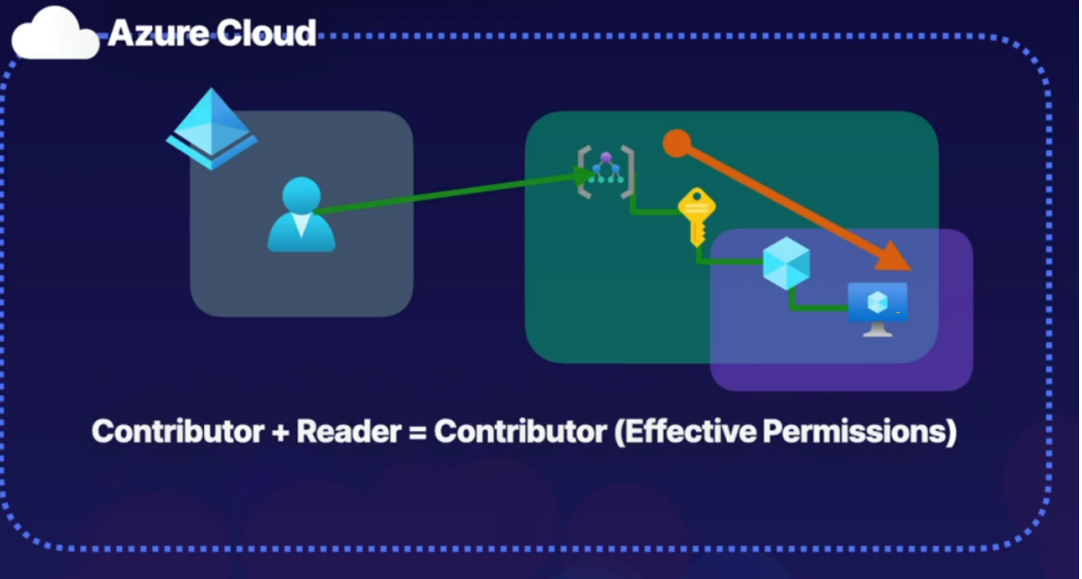
- **AssignableScope:** where we define where we're going to assign the scope for this resource. And it can be all the way down to a specific resource, where we assign the scope to a resource group, to a subscription, or even a management group.

# Contributor

```
"Actions": [
  "*"
],
"NotActions": [
  "Auth/*/Delete",
  ...
],
"DataAction": [],
"NotDataActions": [],
"AssignableScopes": [
  "/"
]
```

For example, if we have this user here in our Azure Active Directory tenant that is assigned the Contributor role at the management group scope here, but also assigned a Reader role at a resource group scope inside of the same hierarchical structure, what we have to understand when we have overlapping roles like this, and multiple role assignments for a single identity, is that roles follow an additive property. So what we do is we add the effective permissions of each of these role definitions, and by performing this addition, this will inform us what the effective permissions will be. So in this case, Contributor + Reader = Contributor, because Contributor provides Reader functionality. So effectively, this user will have Contributor at the management group scope, and that will be inherited all the way down. And there's no additional permissions that are being provided by actually having the Reader role assignment. So this user's permissions will just waterfall all the way down and be inherited to the lowest level.

# Overlapping Roles



## Assigning access

Lets go to resource groups and select a group (K8s\_group in example below) then if we go to roles we can see all role assignments, here we can determine a user can be a contributor (grants full access to manage all resources bu tdoes not allow you to assign roles in Azure RBAC)

Microsoft Azure | Search resources, services, and docs (G+)

Home > Resource groups > K8s\_group

Resource groups | Access control (IAM)

Overview | Activity log | Access control (IAM) | Tags | Resource visualizer | Events

Settings | Deployments | Security | Deployment stacks | Policies | Properties | Locks | Cost Management | Monitoring

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

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, or ID

Type: All | Category: All

Name	Description	Type	Category	Details
Owner	Grants full access to manage all resources, including the ability to assign roles in Azure R...	BuiltInRole	General	View
Contributor	Grants full access to manage all resources, but does not allow you to assign roles in Azur...	BuiltInRole	General	View
Reader	View all resources, but does not allow you to make any changes.	BuiltInRole	General	View
Access Review Operator Service R...	Lets you grant Access Review System app permissions to discover and revoke access as n...	BuiltInRole	None	View
AcriDelete	acr delete	BuiltInRole	Containers	View
AcriImageSigner	acr image signer	BuiltInRole	Containers	View
AcriPull	acr pull	BuiltInRole	Containers	View
AcriPush	acr push	BuiltInRole	Containers	View
AcriQuarantineReader	acr quarantine data reader	BuiltInRole	Containers	View
AcriQuarantineWriter	acr quarantine data writer	BuiltInRole	Containers	View
Advisor Reviews Contributor	View reviews for a workload and triage recommendations linked to them.	BuiltInRole	None	View
Advisor Reviews Reader	View reviews for a workload and recommendations linked to them.	BuiltInRole	None	View
AgFood Platform Dataset Admin	Provides access to Dataset APIs	BuiltInRole	None	View
AgFood Platform Sensor Partner C...	Provides contribute access to manage sensor related entities in AgFood Platform Service	BuiltInRole	None	View
AgFood Platform Service Admin	Provides admin access to AgFood Platform Service	BuiltInRole	AI + Machine Learning	View
AgFood Platform Service Contribu...	Provides contribute access to AgFood Platform Service	BuiltInRole	AI + Machine Learning	View
AgFood Platform Service Reader	Provides read access to AgFood Platform Service	BuiltInRole	AI + Machine Learning	View

We select contributor,, then add then add role assignment

K8s\_group | Access control (IAM) ☆ ...

Resource group

Search

Overview  
Activity log  
Access control (IAM)  
Tags  
Resource visualizer  
Events

Settings  
Deployments  
Security  
Deployment stacks  
Policies  
Properties  
Locks

Cost Management

Add assignments Roles Deny assignments Classic administrators

Add role assignment  
Add co-administrator  
Add custom role

lection 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, or ID

Type: All Category: All

Name ↑↓	Description ↑↓	Type ↑↓
<input type="checkbox"/> Owner	Grants full access to manage all resources, including the ability to assign roles in Azure R...	BuiltInRole
<input checked="" type="checkbox"/> Contributor	Grants full access to manage all resources, but does not allow you to assign roles in Azur...	BuiltInRole
<input type="checkbox"/> Reader	View all resources, but does not allow you to make any changes.	BuiltInRole
<input type="checkbox"/> Access Review Operator Service R...	Lets you grant Access Review System app permissions to discover and revoke access as n...	BuiltInRole
<input type="checkbox"/> AcrDelete	acr delete	BuiltInRole
<input type="checkbox"/> AcrImageSigner	acr image signer	BuiltInRole
<input type="checkbox"/> AcrPull	acr pull	BuiltInRole

Microsoft Azure

Search resources, services, and docs (G+)

Home > Resource groups > K8s\_group | Access control (IAM) >

### Add role assignment

Role Members Conditions Review + assign

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](#)

Job function roles Privileged administrator roles

Grant privileged administrator access, such as the ability to assign roles to other users.

⚠ Can a job function role with less access be used instead?

Search by role name, description, or ID

Type: All Category: All

Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details
Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.	BuiltInRole	General	<a href="#">View</a>
Contributor	Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share imag...	BuiltInRole	General	<a href="#">View</a>
Access Review Operator Service Role	Lets you grant Access Review System app permissions to discover and revoke access as needed by the access review process.	BuiltInRole	None	<a href="#">View</a>
Role Based Access Control Administrator	Manage access to Azure resources by assigning roles using Azure RBAC. This role does not allow you to manage access using other ways, such as Azure P...	BuiltInRole	None	<a href="#">View</a>
User Access Administrator	Lets you manage user access to Azure resources.	BuiltInRole	General	<a href="#">View</a>

Showing 1 - 5 of 5 results.

Microsoft Azure Search resources, services, and docs (G+)

Home > Resource groups > K8s\_group | Access control (IAM)

## Add role assignment

Role Members Conditions Review + assign

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](#)

Job function roles **Privileged administrator roles**

Grant privileged administrator access, such as the ability to assign roles to other users.

⚠ Can a job function role with less access be used instead?

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

Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details
Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.	BuiltInRole	General	<a href="#">View</a>
Contributor	Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share imag...	BuiltInRole	General	<a href="#">View</a>
Access Review Operator Service Role	Lets you grant Access Review System app permissions to discover and revoke access as needed by the access review process.	BuiltInRole	None	<a href="#">View</a>
Role Based Access Control Administrator	Manage access to Azure resources by assigning roles using Azure RBAC. This role does not allow you to manage access using other ways, such as Azure P...	BuiltInRole	None	<a href="#">View</a>
User Access Administrator	Lets you manage user access to Azure resources.	BuiltInRole	General	<a href="#">View</a>

Showing 1 - 5 of 5 results.

Microsoft Azure Search resources, services, and docs (G+)

Home > Resource groups > K8s\_group | Access control (IAM)

## Add role assignment

Role Members Conditions Review + assign

**Selected role** Contributor

**Assign access to**  User, group, or service principal  Managed identity

**Members** + Select members

Name	Object ID	Type
No members selected		

**Description** Optional

Select members

Select

Search by name or email address

- Cris Gzz cris@csrgzzoutlook.onmicrosoft.com
- Cesar Gonzalez csrgzz\_outlook.com#EXT#@csrgzzoutlook.onmicros...
- HTF Admin htfdadmin@csrgzzoutlook.onmicrosoft.com
- Laura Gzz laura@csrgzzoutlook.onmicrosoft.com
- Security Group

Selected members: No members selected. Search for and add one or more members you want to assign to the role for this resource. [Learn more about RBAC](#)

Now back on resources group we can see the role assignments

Microsoft Azure | Search resources, services, and docs (G+)

Home > Resource groups > K8s\_group

### Resource groups

Default Directory (csgzzoutlook.onmicrosoft.com)

+ Create Manage view ...

Filter for any field...

Name ↑

- K8s\_group
- NetworkWatcherRG

Access control (IAM)

Overview Activity log Access control (IAM) Tags Resource visualizer Events

Settings

- Deployments
- Security
- Deployment stacks
- Policies
- Properties
- Locks

Cost Management

- Cost analysis
- Cost alerts (preview)
- Budgets
- Advisor recommendations

Monitoring

### K8s\_group | Access control (IAM)

Resource group

Search

+ Add Download role assignments Edit columns Refresh Remove Feedback

Check access **Role assignments** Roles Deny assignments Classic administrators

Number of role assignments for this subscription 3 Privileged 3

View assignments

All Job function (0) Privileged (3)

Search by name or email Type: All Role: All Scope: All scopes Group by: Role

3 items (3 Users)

Name	Type	Role	Scope
Owner (1)			
<input type="checkbox"/> Cesar Gonzalez csgzz_outlook.com#EXT#@csg...	User	Owner	Subscription (Inherited)
Contributor (2)			
<input type="checkbox"/> Cris Gzz cris@csgzzoutlook.onmicrosof...	User	Contributor	This resource
<input type="checkbox"/> HTF Admin htfadmin@csgzzoutlook.onmi...	User	Contributor	This resource

Same inside those resources it inherited the assignment

Microsoft Azure | Search resources, services, and docs (G+)

Home > Resource groups > K8s\_group > htfmx.onmicrosoft.com

### htfmx.onmicrosoft.com | Access control (IAM)

B2C Tenant

Search

+ Add Download role assignments Edit columns Refresh Remove Feedback

Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Settings

- Properties

Automation

- Tasks (preview)

Help

- Support + Troubleshooting

Check access **Role assignments** Roles Deny assignments Classic administrators

Number of role assignments for this subscription 3 Privileged 3

View assignments

All Job function (0) Privileged (3)

Search by name or email Type: All Role: All Scope: All scopes Group by: Role

3 items (3 Users)

Name	Type	Role	Scope	Condition
Owner (1)				
<input type="checkbox"/> Cesar Gonzalez csgzz_outlook.com#EXT#@csgzzoutlook...	User	Owner	Subscription (Inherited)	None
Contributor (2)				
<input type="checkbox"/> Cris Gzz cris@csgzzoutlook.onmicrosoft.com	User	Contributor	Resource group (Inherited)	None
<input type="checkbox"/> HTF Admin htfadmin@csgzzoutlook.onmicrosoft.com	User	Contributor	Resource group (Inherited)	None

## Authorization system

- Provide identities with access to azure resources

- Roles are a collection of permissions
  - There is a scoping hierarchy for role assignment
  - Implicit deny - Explicit Allow - Explicit Deny
- 

Revision #2

Created 19 February 2024 23:36:22 by Cesar Gzz

Updated 20 February 2024 00:11:25 by Cesar Gzz