AZ-104 Azure RBAC - Assigning access to resources

Secure Azure RBAC

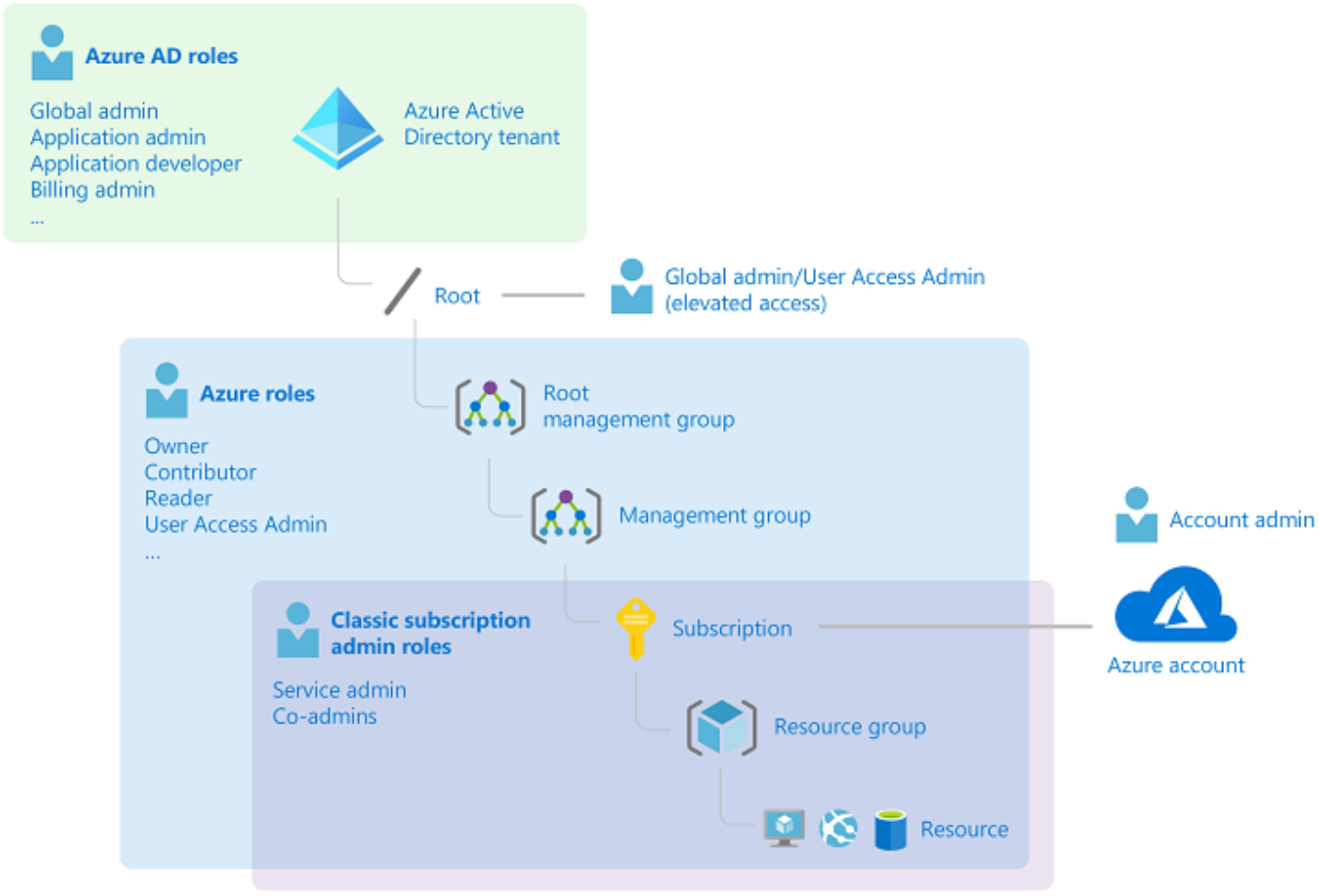
- Explaning Azure RBAC
- Understanding Role definitions
- Additive Property

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

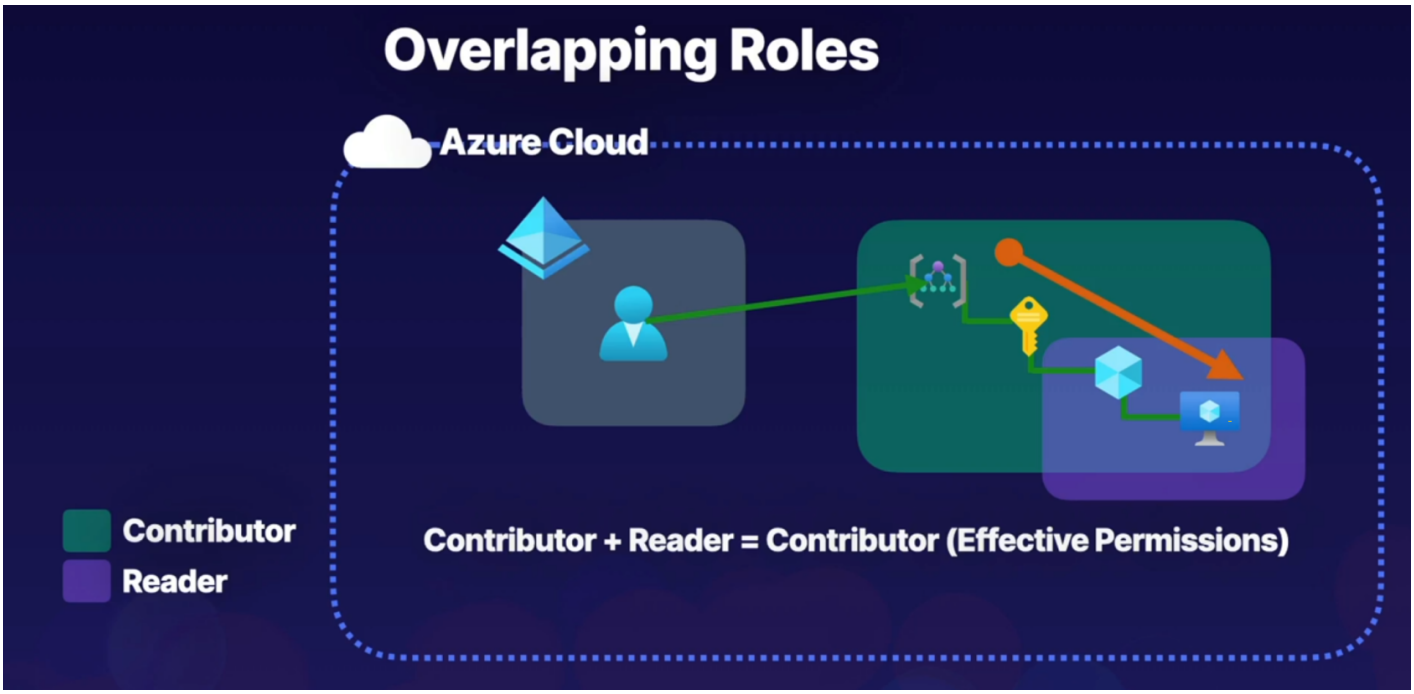
Contributor

- 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 actionssuch as working with data inside of Azure Storage accounts.

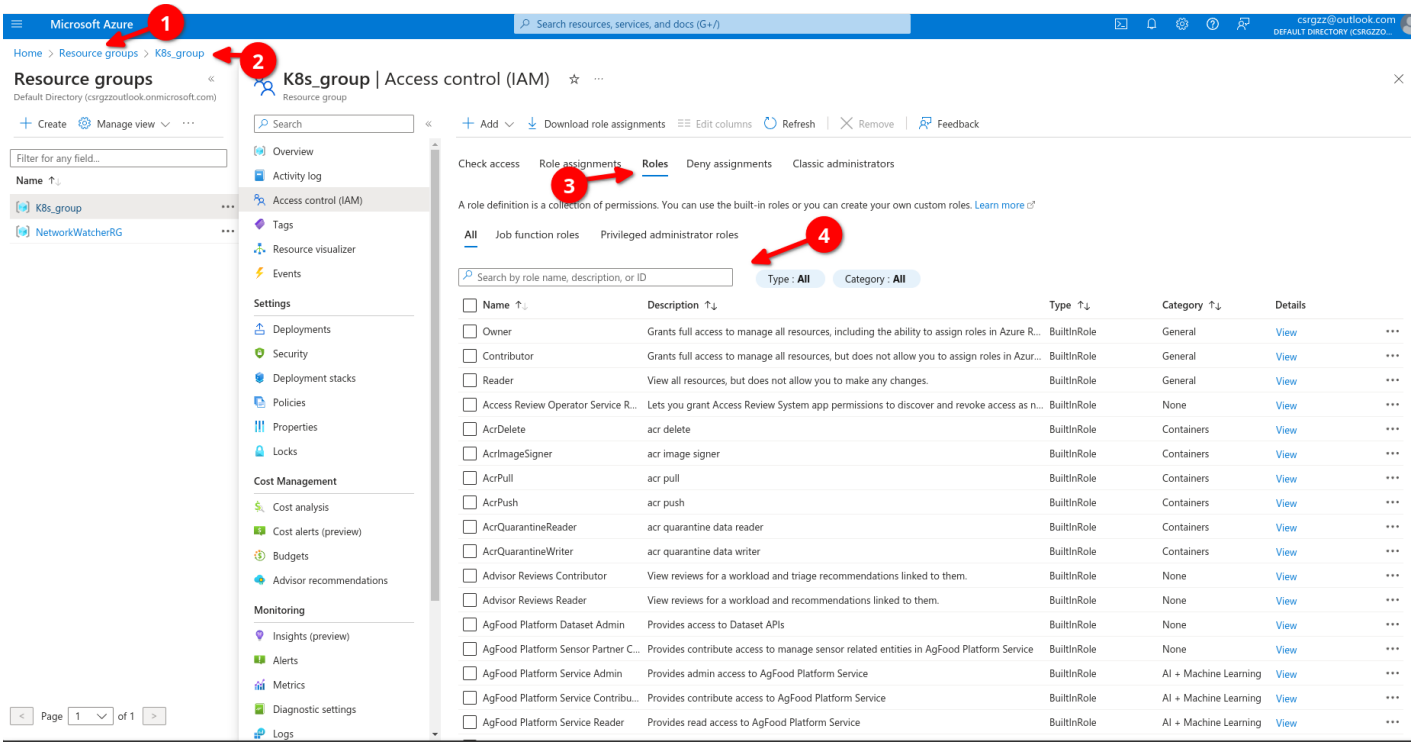
- AssignableScope: where we define where we're going to assign the scope for this resource. And it can be all the way down
  to a specific resource, where we assign the scope to a resource group, to a subscription, or even a management group.

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.

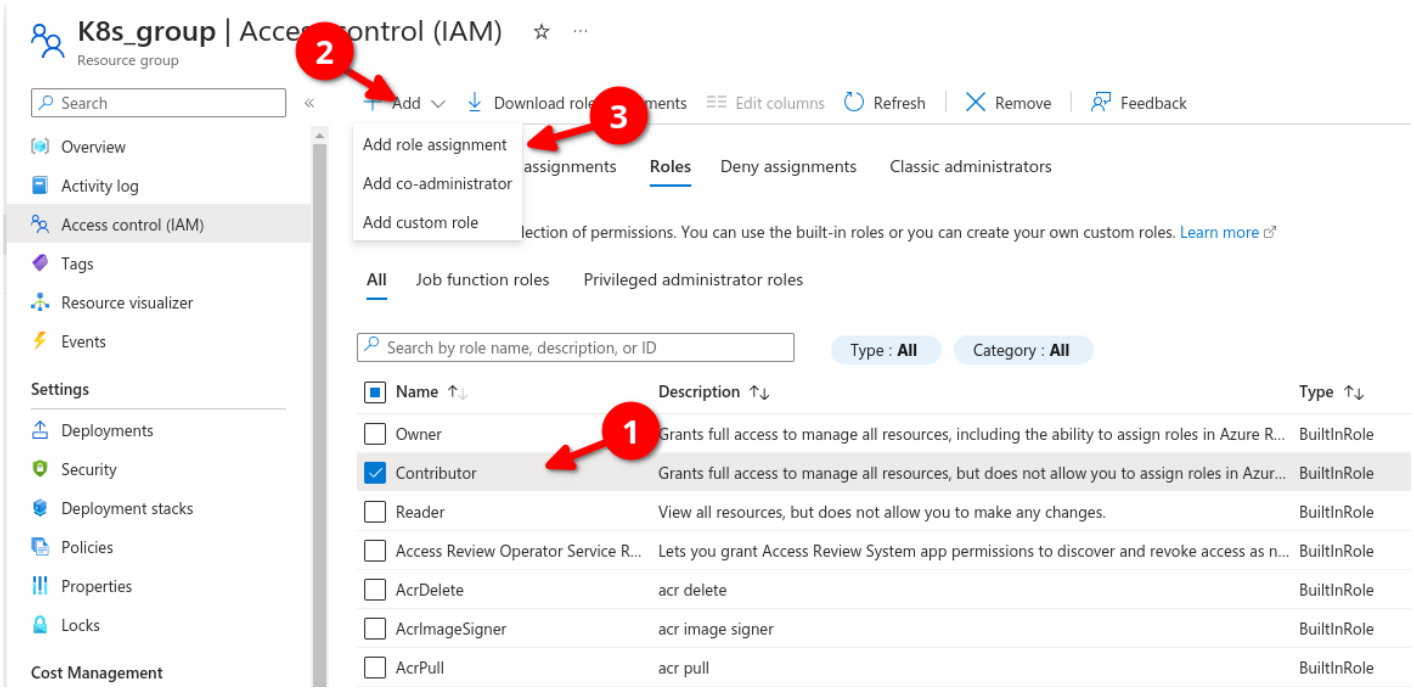


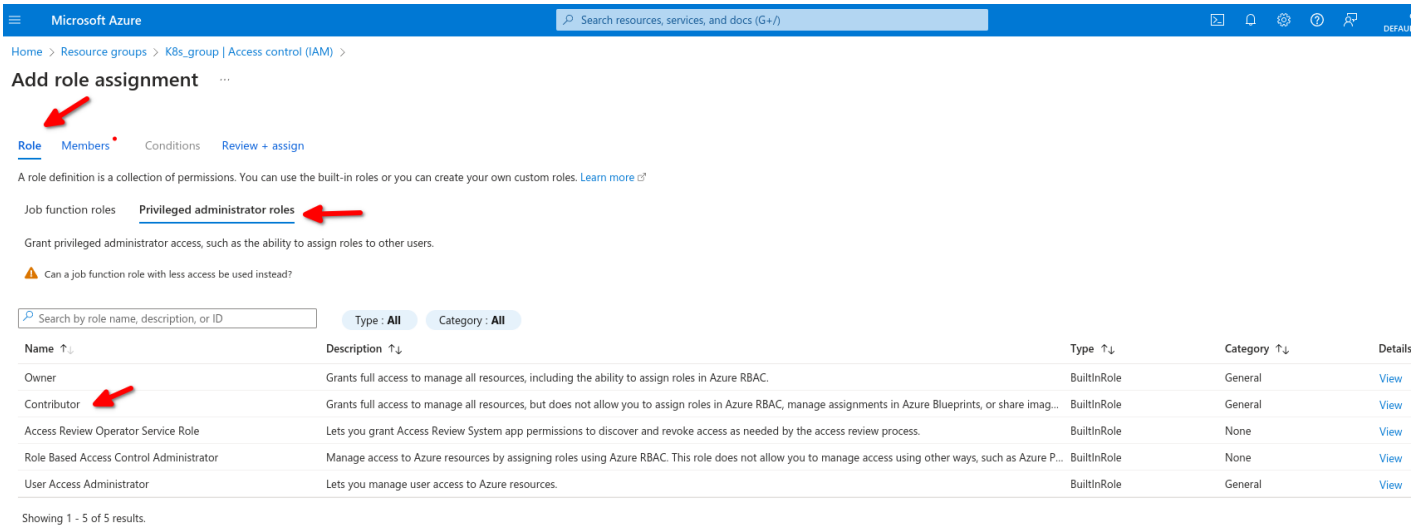
Assigning access

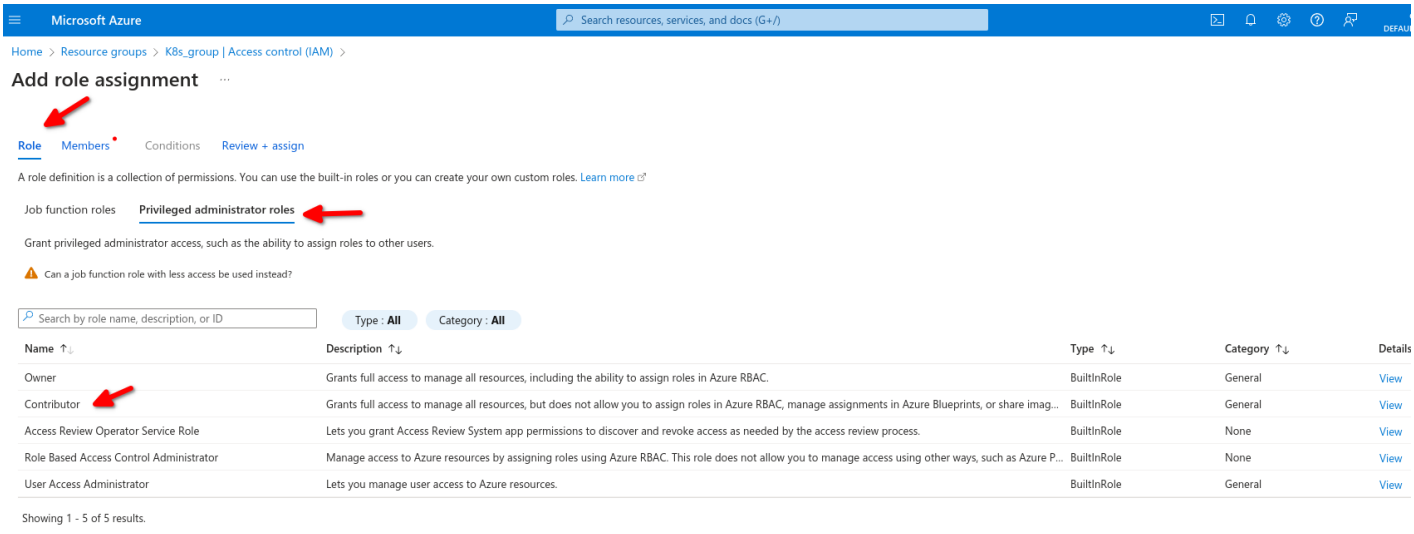
Lets go to resource groups and select a group (K8s_group in example below) then if we go to roles we can see all role assignments, here we can determine a user can be a contributor (grants full access to manage all roesources bu tdoes not allow you to assign roles in Azure RBAC)

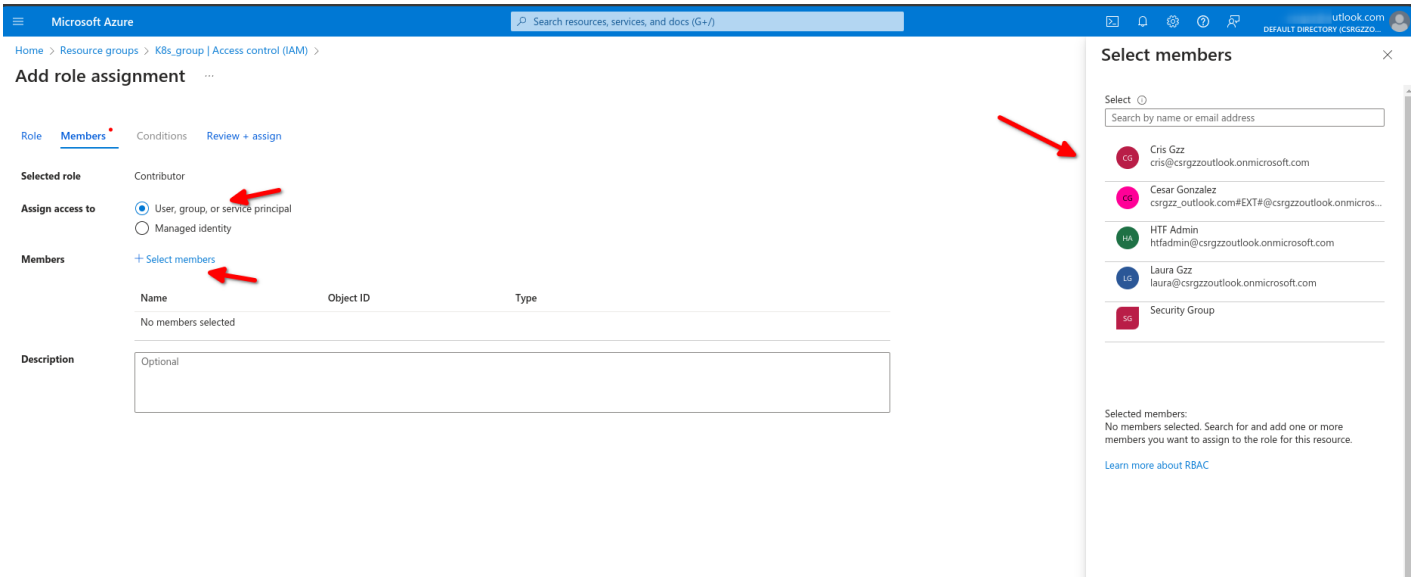


We select contributor,, then add then add role assignment

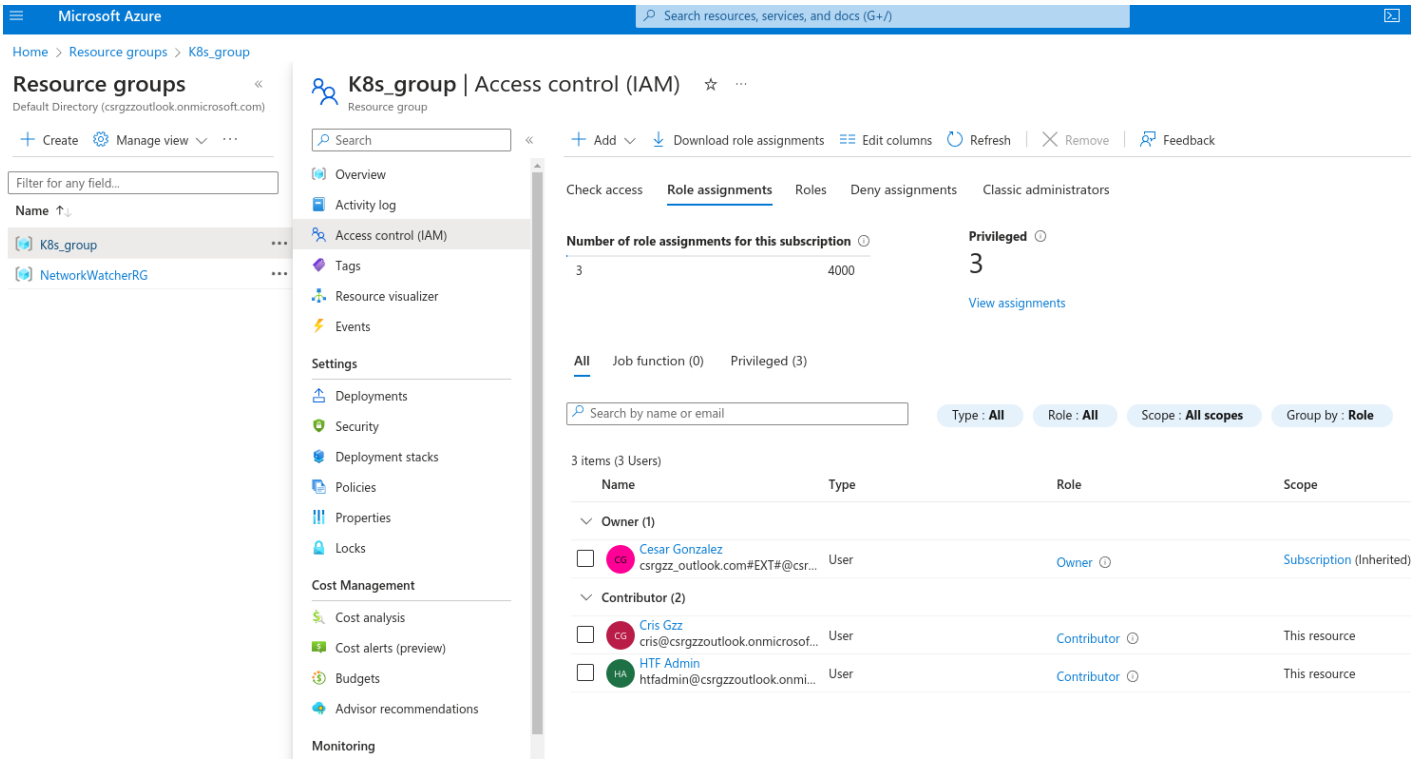

K8s_group | Access control (IAM)
Resource group
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Deployments
Security
Deployment stacks
Policies
Properties
Locks
Cost Management
Add
Download role assignments
Edit columns
Refresh
Remove
Feedback
Add role assignment
Add co-administrator
Add custom role
Roles
Deny assignments
Classic administrators
Learn more
All
Job function roles
Privileged administrator roles
Search by role name, description, or ID
Type : All
Category : All
Name
Description
Type
Owner
Grants full access to manage all resources, including the ability to assign roles in Azure R...
BuiltInRole
Contributor
Grants full access to manage all resources, but does not allow you to assign roles in Azur...
BuiltInRole
Reader
View all resources, but does not allow you to make any changes.
BuiltInRole
Access Review Operator Service R...
Lets you grant Access Review System app permissions to discover and revoke access as n...
BuiltInRole
AcrDelete
acr delete
BuiltInRole
AcrImageSigner
acr image signer
BuiltInRole
AcrPull
acr pull
BuiltInRole
1
2
3


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
View
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
View
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
View
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
View
User Access Administrator
Lets you manage user access to Azure resources.
BuiltInRole
General
View
Showing 1 - 5 of 5 results.

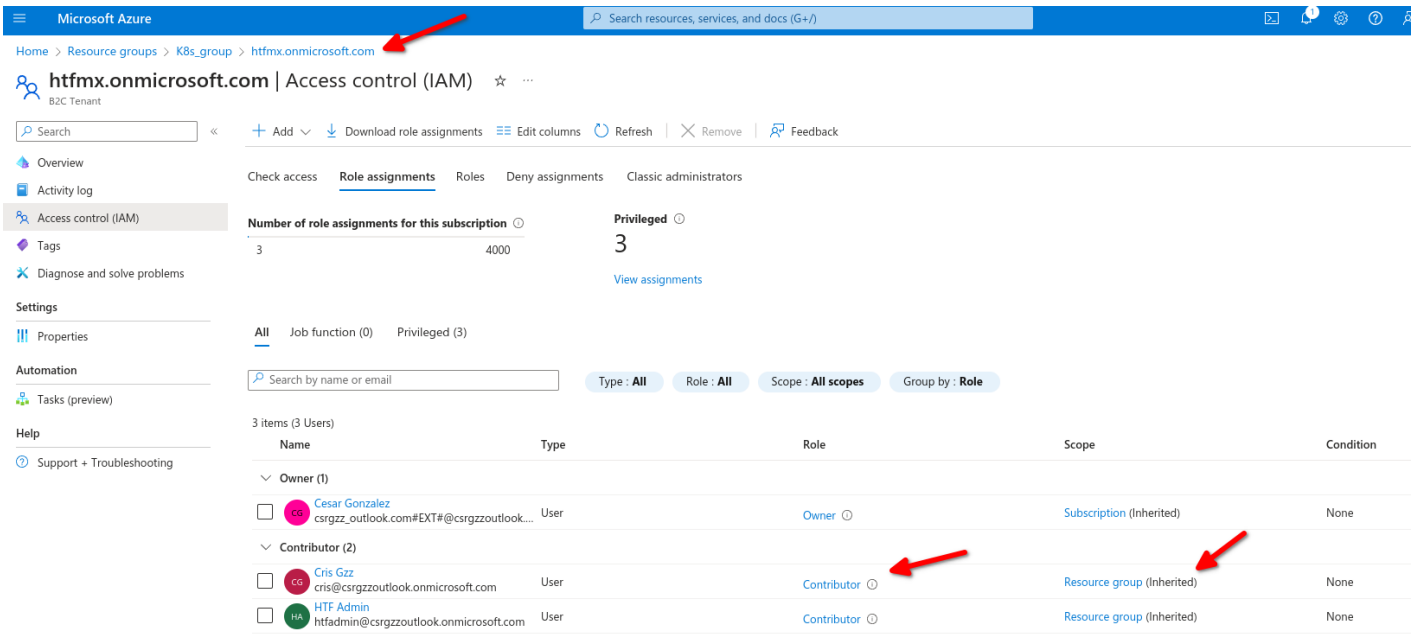




Now back on resources group we can see the role assignments



Same inside those resources it inherited the assignment



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