



ROLE-BASE ACCESS CONTROL FOR AZURE KUBERNETES CLUSTER

Azure RBAC



BY
TIMOTHY FABELURIN

Role-based access control (RBAC)

Access to cloud resource is a critical function that cloud user need to manage properly. RBAC is an authorization system that maintains the less privilege principle for access management to cloud resource. Azure RBAC was implemented in this work, and it helped to manage who has access to resources and the function they can undertake with those resources and the area the individual has access to. Without a doubt, this security measure curbs many attackers' exploit.

The process includes:

Role definition: collection of permissions known as role. Role indicates the actions that can be perform. Examples are read, write, and delete.

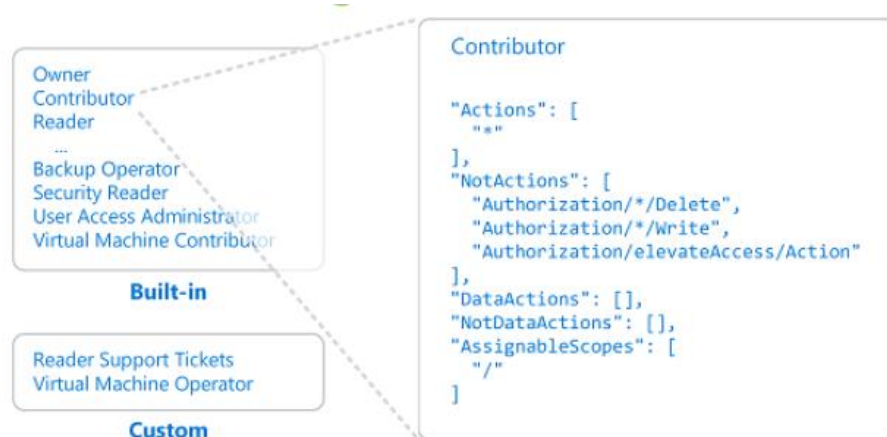


Figure 4.1 Role Definition (Robert Lyon, 2022)

Scope: This is the set of resources that access created is applied to, as the role created are limited by the scope.

Role assignment: this refers to the process of attaching defined role to user or group or service principal within a particular scope for access creation.

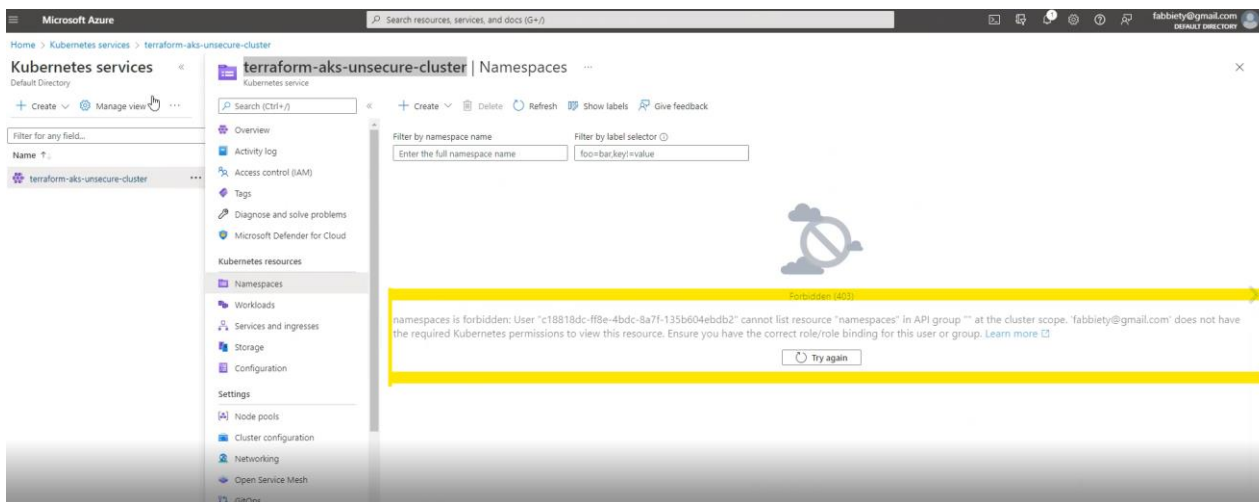
PROCESS

To test this feature, a user on the cloud platform, could successfully log into the portal but could not gain access to the Kubernetes cluster. This user was given the role of

“Admin” but because the role assignment was not done, it still could not gain access.

This test was simply to indicate that all the implementation stages needed to be carried out before an access can be granted.

To the end, if for by any chance, an attacker gain access into the cloud environment, if the authorization is not explicitly provided to access the cluster, the attacker will not be able to perform any act.



```
PS C:\Users\Fabbiety\Desktop\Project\06-Azure-MySQL-for-AKS-Storage> az role assignment create --role "Azure Kubernetes Service RBAC Admin" --assignee fabbiety@gmail.com#EXT#@fabbiety@gmail.onmicrosoft.com --scope /subscriptions/191fe5ed-49ee-4667-9fed-a70b6461f460/resourcegroups/terraform-aks-unsafe/providers/Microsoft.ContainerService/managedClusters/terraform-aks-unsafe-cluster
{
  "canDelegate": null,
  "condition": null,
  "conditionVersion": null,
  "description": null,
  "id": "/subscriptions/191fe5ed-49ee-4667-9fed-a70b6461f460/resourcegroups/terraform-aks-unsafe/providers/Microsoft.ContainerService/managedClusters/terraform-aks-unsafe-cluster/providers/Microsoft.Authorization/roleAssignments/ca97ae84-7eb5-4dc5-8ff8-028f7582ef7e",
  "name": "ca97ae84-7eb5-4dc5-8ff8-028f7582ef7e",
  "principalId": "c18818dc-ff8e-4bdc-8a7f-135b604ebdb2",
  "principalType": "User",
  "resourceGroup": "terraform-aks-unsafe",
  "roleDefinitionId": "/subscriptions/191fe5ed-49ee-4667-9fed-a70b6461f460/providers/Microsoft.Authorization/roleDefinitions/3498e952-d568-435e-9b2c-8d77e338d7f7",
  "scope": "/subscriptions/191fe5ed-49ee-4667-9fed-a70b6461f460/resourcegroups/terraform-aks-unsafe/providers/Microsoft.ContainerService/managedClusters/terraform-aks-unsafe-cluster",
  "type": "Microsoft.Authorization/roleAssignments"
}
```

Role was assigned to the user

Home > Default Directory > Users >

315211e9-307b-462f-98da-54ddef3b9f8f bc173ca1-dbd9-4b25-89f8-a416f9ce93b4 ...

User

Search (Ctrl+/) << Delete Refresh Reset password Revoke sessions Got feedback?

Overview Audit logs Sign-in logs Diagnose and solve problems

Manage

- Assigned roles
- Administrative units
- Groups
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods

Troubleshooting + Support

New support request

Overview Monitoring Properties

Basic info

User principal name	fabbiety_gmail.com#EXT#@fabbietygmail.onmicrosoft.com	Group member...	1
Object ID	c18818dc-ff8e-4bdc-8a7f-135b604ebdb2	Applications	1
Created date time	Sep 17, 2018, 9:37 AM	Assigned roles	1
User type	Member	Assigned licens...	0
Identities	MicrosoftAccount		

My Feed

Account status

Enabled

Edit

B2B collaboration

Convert this internal user to be a B2B user.

Manage (resend invitation / reset status)

Quick actions

It can be seen from the capture that the role assignment was successful, and access is now granted to the AKS cluster.

Microsoft Azure

Search resources, services, and docs (G+I)

Home > Kubernetes services > terraform-aks-unsafe-cluster

Kubernetes services

Default Directory

+ Create Manage view

Filter for any field...

Name 1

terraform-aks-unsafe-cluster

terraform-aks-unsafe-cluster | Namespaces

Search (Ctrl+/) + Create Delete Refresh Show labels Give feedback

Filter by namespace name Enter the full namespace name

Filter by label selector foo=bar;key=value

<input type="checkbox"/>	Name	Status	Age
<input type="checkbox"/>	default	Active	2 days
<input type="checkbox"/>	gatekeeper-system	Active	2 days
<input type="checkbox"/>	kube-node-lease	Active	2 days
<input type="checkbox"/>	kube-public	Active	2 days
<input type="checkbox"/>	kube-system	Active	2 days
<input type="checkbox"/>	prometheus	Active	14 hours

Namespaces

- Workloads
- Services and ingresses
- Storage
- Configuration
- Settings
- Node pools
- Cluster configuration
- Networking
- Open Service Mesh
- CI/CD
- Deployment center (preview)
- Policies
- Properties

