VNET - RBAC permission needed to add VNET from another subscription

Last updated by | Vitor Tomaz | Aug 5, 2020 at 12:40 PM PDT

Contents

Issue

Assuming the user has the required permission on the SQL resource side. But he wants to add VNET rule which belongs to another subscription. Thus he will need following permission to be added in the VNET subscription:

Steps

Basically you can create a custom role with following permissions and added to the subscription level which has the VNET resource.

Microsoft.Network/virtualNetworks/subnets/joinViaServiceEndpoint/action,

Microsoft.Network/virtualNetworks/subnets/read,

Microsoft.Network/virtualNetworks/read,

You will be able to see all the VNETs in that subscription and add the eligible subnets to SQL firewall rules.

If you want to limit to one particular VNET only, you will need at least following permissions:

Granted at the VNET scope:

Microsoft.Network/virtualNetworks/subnets/joinViaServiceEndpoint/action,

Microsoft.Network/virtualNetworks/subnets/read,

Microsoft.Network/virtualNetworks/read,

Microsoft.Network/virtualNetworks/write

Granted at the route table scope;

Microsoft.Network/routeTables/join/action

How good have you found this content?