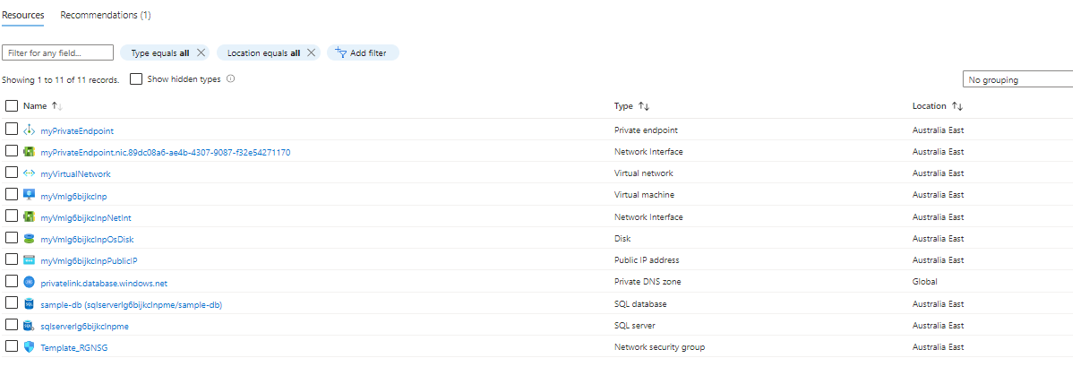
1. Template – ARM Set up

Attached tempate to set up the below environment





1. Create an NSG,
   1. Associate NSG to the Subnet where the VM in or associate it to the NIC of the VM
      1. Associate NSG to a subnet – NSG rules apply to all VMS inside the subnet
      2. Associate NSG to NIC - NSG rules apply to specific VMs with the NIC

Assocaite NSG to a subnet – NSG rules apply to all VMS inside the subnet

Assoaite NSG to NIC - NSG rules apply to specific VMs with the NIC

Graphical user interface, text, application

Description automatically generatedGraphical user interface

Description automatically generated

Text, application

Description automatically generated

1. Create inbound security rules for accessing to the VM

Graphical user interface, application

Description automatically generatedGraphical user interface, text, application, email

Description automatically generatedGraphical user interface, text, application, email

Description automatically generated

Table

Description automatically generated

Graphical user interface, application, Word

Description automatically generated

Graphical user interface, application, Word

Description automatically generated

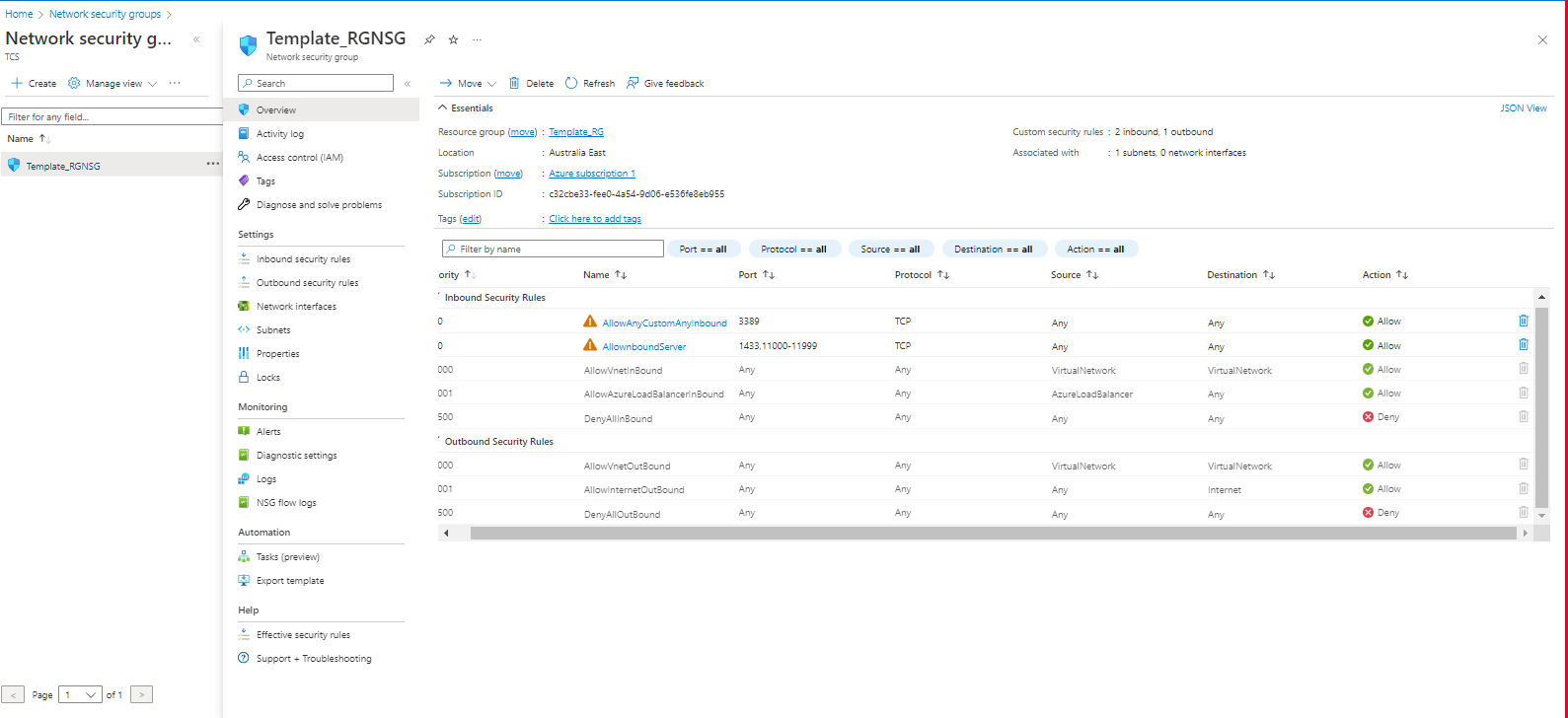
Note:-

Outbound rules are not necessary - As per Screen shot 1 ,Screen shot 2 and Screen shot 3;

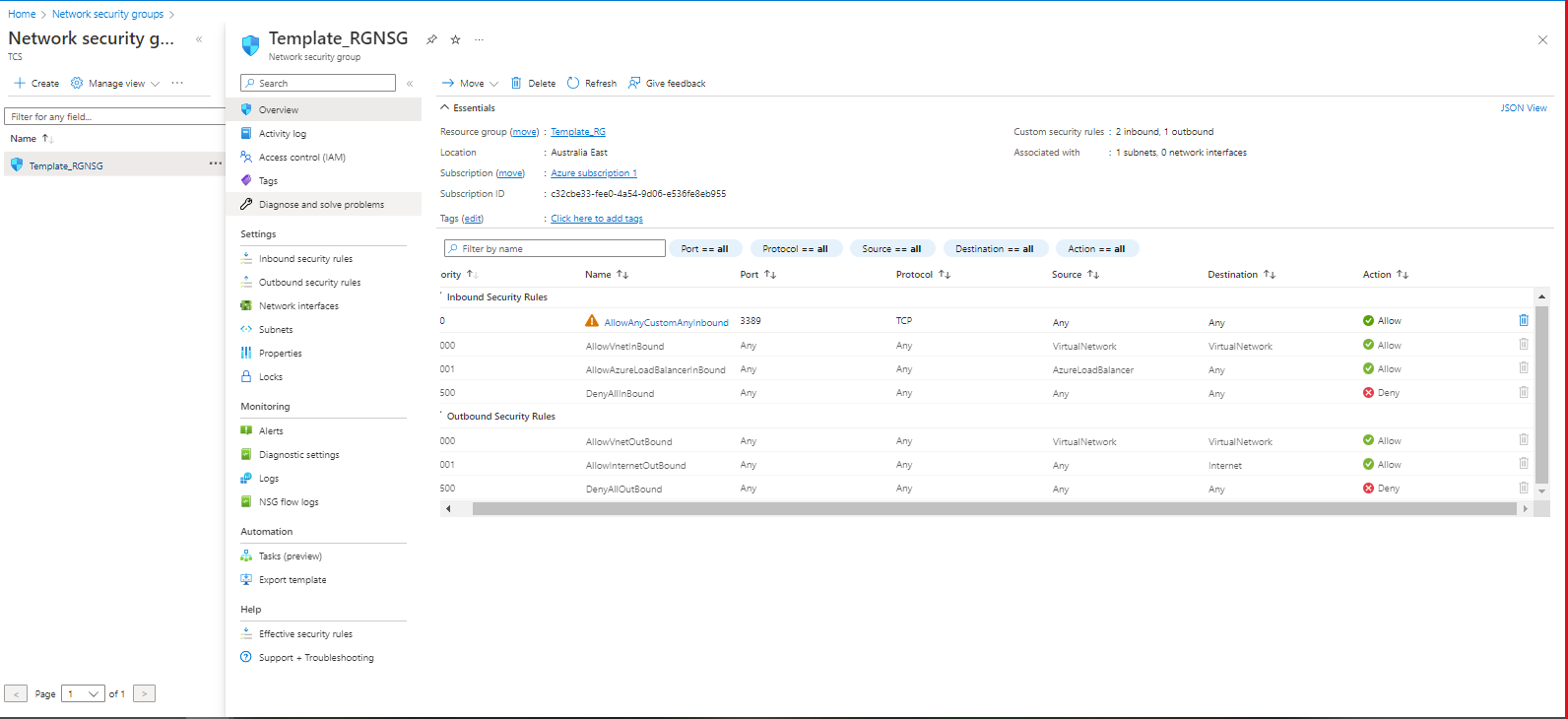
we don't need to set the inbound rules for the SQL servers because

* SQL servers are in the VNET (VM need to have access to “this” VNET) and,
* We (VM) always send the request from this VM to the SQL server/s.
  + So, the traffic will go outbound to the SQL Server; we need to focus on the outbound rules.
  + But there are already default rules to allow the traffic outbound to the Virtual Network.

Screen shot 1



Screen shot 2



Screen shot 3

Graphical user interface

Description automatically generated

1. Associate the Subnet to the NSG
   1. If we do not associate this subnet to the NSG , we will not be able to access the VM within the VNET.
   2. NSG is necessary for all VMs to protect it ( deny) all outside public traffic until you add the rules to allow the traffic from internet.

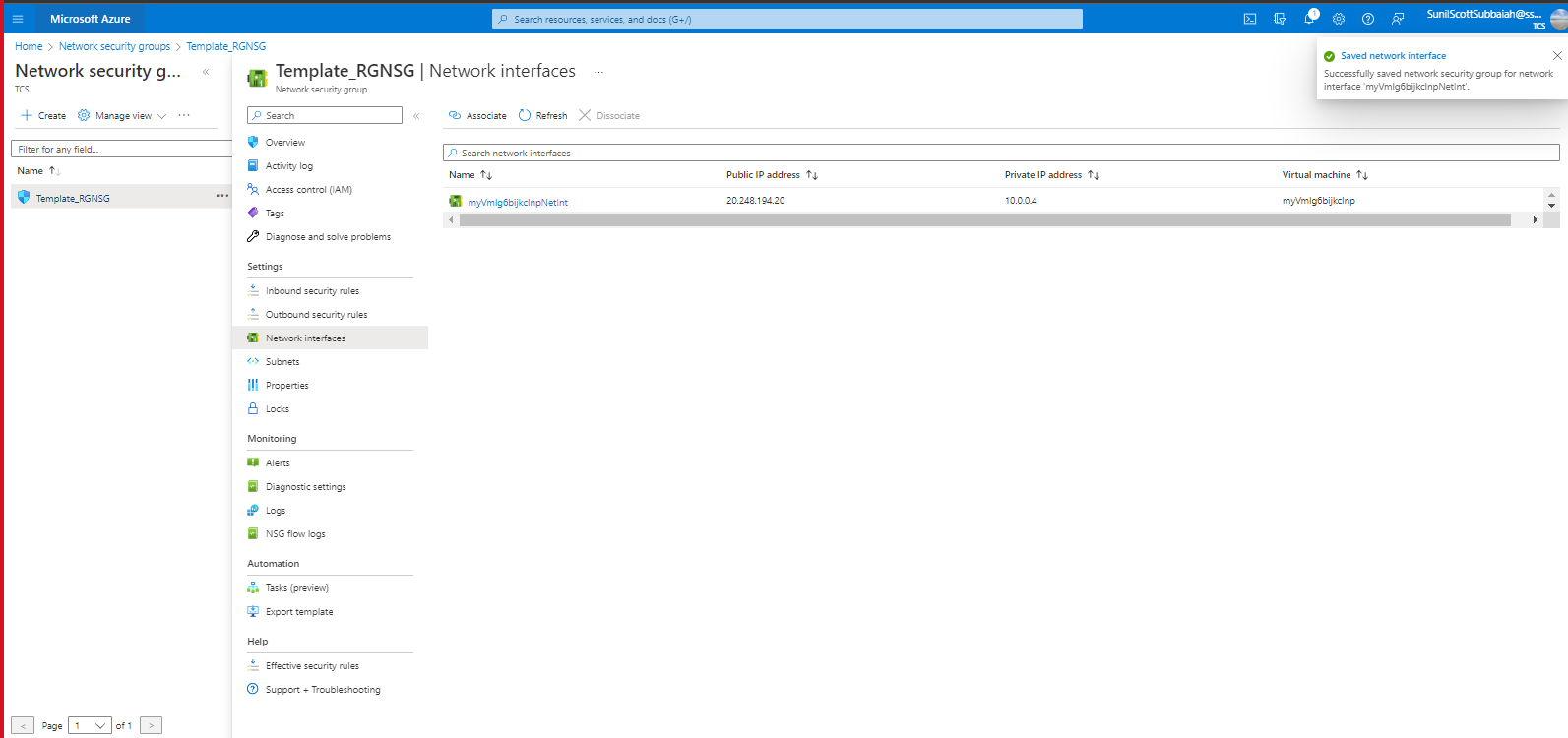
Graphical user interface, application

Description automatically generatedA picture containing graphical user interface

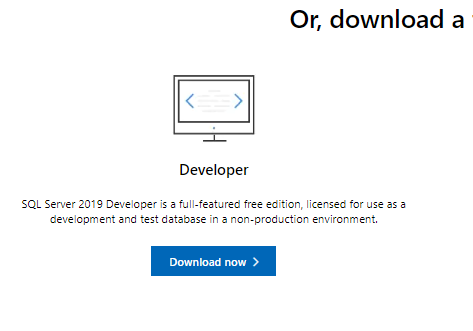
Description automatically generated

Graphical user interface, text, application, email

Description automatically generated



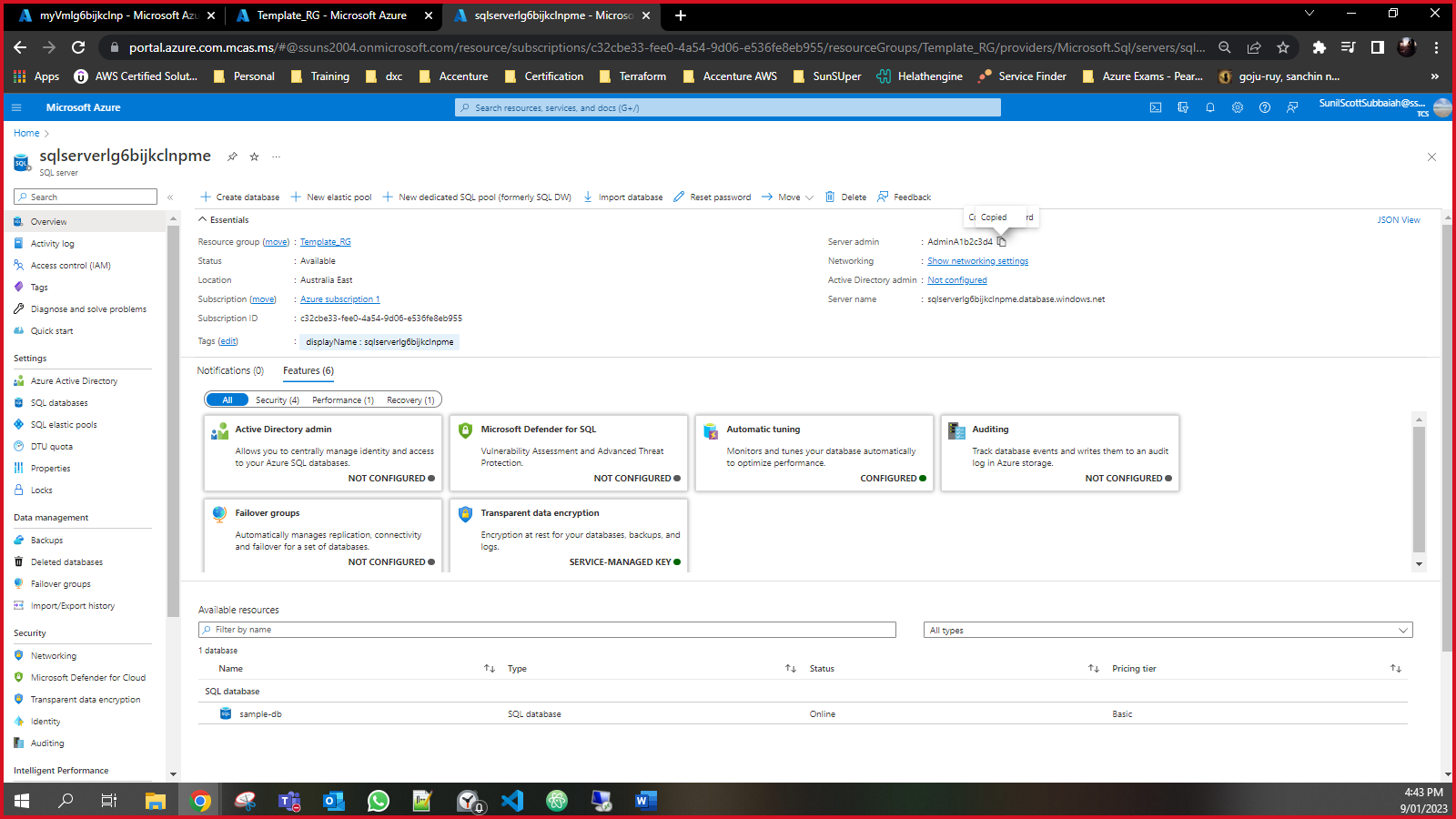
1. Install DB and SSMS on the VM Machine

<https://www.microsoft.com/en-in/sql-server/sql-server-downloads> 

<https://learn.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-ver16> Graphical user interface, text, application, email

Description automatically generated

1. Connect to SSMS over VM



Note: -

client to all Azure SQL IP addresses in the region on ports in the range of 11000 to 11999. Use the Service Tags for SQL to make this easier to manage.

Graphical user interface, application

Description automatically generated

AdminA1b2c3d4

A1b2c3d42023

Graphical user interface, text, application

Description automatically generated Graphical user interface, text, application, email

Description automatically generated

Graphical user interface

Description automatically generated

Text

Description automatically generated

Graphical user interface

Description automatically generated

Graphical user interface, text, application

Description automatically generated

After whitelisting a few IP’s addresses and switching from Disable to Selected Networks

Graphical user interface, text, application, email

Description automatically generated

Text

Description automatically generated Graphical user interface, application

Description automatically generated