**Vnet (Virtual Network) Peering**

TASK: To connect 2 VMs which are in the different Region and Resource Group.

1. Create the first VM:

a. Navigate to the Azure portal (https://portal.azure.com) and sign in with your Azure account.

b. Locate and select the resource group where you want to create the first VM, or create a new resource group if needed.

c. Within the selected resource group, click on the "Add" button to add a new resource.

d. Search for "Virtual machine" and select the "Virtual machine" option from the search results.

e. Click on the "Create" button to create a new VM.

f. Fill in the required information for the VM, including the name, region, availability options, subscription, and resource group.

g. Configure the network settings, such as the virtual network, subnet, and public IP address.

h. Specify the operating system, disk settings, and other desired configurations for the VM.

i. Review the settings and click on the "Review + Create" button.

j. After the validation is complete, click on the "Create" button to create the first VM.

2. Create the second VM:

a. Repeat steps 1a to 1j, but choose a different name, select the desired region, and choose the second resource group created in step 1b.

3. Establish a virtual network peering:

a. Navigate to the resource group of the first VM.

b. Select the virtual network associated with the first VM.

c. In the virtual network's overview page, click on the "Peerings" option in the left-hand menu.

d. Click on the "+ Add" button to add a new peering connection.

e. Provide a unique name for the peering connection.

f. In the "Virtual network" field, select the virtual network associated with the second VM.

g. Configure the remaining settings based on your requirements.

h. Click on the "OK" button to create the virtual network peering.

4. Configure network security groups (NSGs):

a. Navigate to the resource group of the first VM.

b. Select the first virtual network from the list of resources.

c. In the virtual network's overview page, click on the "Subnets" option in the left-hand menu.

d. Select the subnet associated with the first VM.

e. In the subnet's settings page, click on the "Network security group" link.

f. Click on "Inbound security rules" and add a rule to allow inbound traffic from the source IP address or subnet of the second VM.

g. Repeat steps 4a to 4f for the second virtual network, allowing inbound traffic from the source IP address or subnet of the first VM.

5. Test the connection:

a. Remote into the first VM using the appropriate method (RDP for Windows or SSH for Linux).

b. From the first VM, try to communicate with the private IP address or hostname of the second VM using the desired protocol (e.g., ping, telnet, or any other application-specific method).

c. Repeat the same steps from the second VM to test connectivity to the first VM.