|  |
| --- |
|  |
| #Login in azure account |
|  | #$Azureacct=Read-host "please enter username" |
|  | #$Azurepassword=convertTo -SecureStriing "\*\*\*\*\*\*\*" -AsPlainText -Force |
|  | #$AzureCreds=New-Object System.Management.Automation.PsCredential($Azureacct,$Azurepassword) |
|  |  |
|  | #Login into the Azure portal |
|  | Login-AzureRmAccount |
|  | #create ResourceGroup |
|  | $RG=New-AzureRmResourceGroup -Name "PranithaRG" -Location "East Us" |
|  | #create Virtual Network |
|  | $VN=New-AzureRmVirtualNetwork -ResourceGroupName "PranithaRG" -Location "East Us" -Name "PranithaVN" -AddressPrefix "192.68.0.0/25" |
|  | $SubnetConfig1=Add-AzureRmVirtualNetworkSubnetConfig -Name Frontendsubnet -AddressPrefix 192.68.0.0/27 -VirtualNetwork $VN |
|  | $SubnetConfig2=Add-AzureRmVirtualNetworkSubnetConfig -Name Backendsubnet -AddressPrefix 198.68.0.32/28 -VirtualNetwork $VN |
|  | $VN | Set-AzureRmVirtualNetwork |
|  | # Create NSG rule to allow RDP in inbound to frontend subnet |
|  | $rule1 = New-AzureRmNetworkSecurityRuleConfig -Name 'Allow-RDP-All' -Description 'Allow RDP' -Access Allow -Protocol Tcp -Direction Inbound -Priority 100 -SourceAddressPrefix Internet -SourcePortRange \* -DestinationAddressPrefix \* -DestinationPortRange 3389 |
|  |  |
|  | # Create NSG rule to allow SSH to the front-end subnet. |
|  | $rule2 = New-AzureRmNetworkSecurityRuleConfig -Name 'Allow-SSH-All' -Description 'Allow SSH' -Access Allow -Protocol Tcp -Direction Inbound -Priority 110 -SourceAddressPrefix Internet -SourcePortRange \* -DestinationAddressPrefix \* -DestinationPortRange 22 |
|  |  |
|  | # Create an NSG rule to allow HTTP to the front-end subnet. |
|  | $rule3 = New-AzureRmNetworkSecurityRuleConfig -Name 'Allow-HTTP-All' -Description 'Allow HTTP' -Access Allow -Protocol Tcp -Direction Inbound -Priority 120 -SourceAddressPrefix Internet -SourcePortRange \* -DestinationAddressPrefix \* -DestinationPortRange 80 |
|  |  |
|  | # associate the front-end network security group |
|  | $nsgfe = New-AzureRmNetworkSecurityGroup -ResourceGroupName "PranithaRG" -Location "East Us" -Name FrontendsubnetNSG -SecurityRules $rule1,$rule2, $rule3 |
|  |  |
|  |  |
|  | #create NSG to allow MYSQL in inbound to the backend subnet |
|  | $rule4 = New-AzureRmNetworkSecurityRuleConfig -Name 'Allow-Mysql-All' -Description 'Allow Mysql' -Access Allow -Protocol Tcp -Direction Inbound -Priority 130 -SourceAddressPrefix Internet -SourcePortRange \* -DestinationAddressPrefix \* -DestinationPortRange 3306 |
|  |  |
|  |  |
|  | # Create NSG to deny HTTP |
|  | $rule5 = New-AzureRmNetworkSecurityRuleConfig -Name 'Deny-HTTP-All' -Description 'Deny HTTP' -Access Deny -Protocol Tcp -Direction Outbound -Priority 120 -SourceAddressPrefix Internet -SourcePortRange \* -DestinationAddressPrefix \* -DestinationPortRange 80 |
|  | $nsgfe = New-AzureRmNetworkSecurityGroup -ResourceGroupName "PranithaRG" -Location "East Us" -Name BackendsubnetNSG -SecurityRules $rule4,$rule5 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  | Set-AzureRmVirtualNetworkSubnetConfig -VirtualNetwork $VN -Name Backendsubnet -AddressPrefix 192.68.0.32/27 -NetworkSecurityGroup $nsgfe |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |