Deploy Highly Available DCs in IaaS-Part 2

This guide provides an introduction to some basic Azure VM concepts. In this demonstration you will show how to

* Add a VM to an existing domain
* Configure SYSVOL and network security

Contents

[Pre-Requisites 1](#_Toc430902149)

[Setup 1](#_Toc430902150)

[Demo Steps 1](#_Toc430902151)

[Clean Up 4](#_Toc430902152)

## Pre-Requisites

This section lists the pre-requisites required for this demonstration.

* Azure subscription

## Setup

Estimated time: 15 minutes

|  |  |
| --- | --- |
| 1. Open the new Azure Portal |  |
| 1. Open GitHub |  |

## Demo Steps

Estimated time: 8 mins

|  |  |
| --- | --- |
| 1. **BEGIN PART 2** |  |
| 1. Navigate to the resource group you just created |  |
| 1. Navigate to the PDC you created |  |
| 1. Select the network interfaces |  |
| 1. Select the IP addresses. Highlight that the portal template assigned a static IP address |  |
| 1. Select DNS Servers |  |
| 1. Enter the DNS server for the current machine |  |
| 1. Select the BDC domain controller |  |
| 1. Configure the IP address and DNS settings to point to the first DC |  |
| 1. If you use the ARM template to deploy, currently the network security group is not exposed via the portal. Create a new NSG via PowerShell | Connect to your account using: Add-AzureAccount |
| 1. Run the following PS | New-AzureNetworkSecurityGroup -ResourceName ‘[ENTER A NAME]’ -Location ‘[ENTER A LOCATION]’ -ResourceGroupName ‘[ENTER A NAME]’ |
| Enter new rules to allow DC1 and DC2 to talk to each other. For now we will create an ANY/ANY rule for the subnet for TCP and UDP  \*\* NOTE: some of the samples no longer work due to syntax differences https://azure.microsoft.com/en-us/documentation/articles/virtual-networks-nsg/ | $nsg = Get-AzureNetworkSecurityGroup -Name [NAME ENTERED ABOVE] –ResourceGroupName [RESOURCE GROUP NAME]  new-AzureNetworkSecurityRuleConfig -Name INTERNALTCP -Direction Inbound -Priority 100 -Access Allow –SourceAddressPrefix '10.0.0.0/24' -SourcePortRange '\*' -DestinationAddressPrefix '10.0.0.0/24' –DestinationPortRange '\*' -Protocol TCP  new-AzureNetworkSecurityRuleConfig -Name INTERNALUDP -Direction Inbound -Priority 100 -Access Allow –SourceAddressPrefix '10.0.0.0/24' -SourcePortRange '\*' -DestinationAddressPrefix '10.0.0.0/24' –DestinationPortRange '\*' -Protocol UDP  new-AzureNetworkSecurityRuleConfig -Name INTERNALTCP-OUT -Direction Outbound -Priority 100 -Access Allow –SourceAddressPrefix '10.0.0.0/24' -SourcePortRange '\*' -DestinationAddressPrefix '10.0.0.0/24' –DestinationPortRange '\*' -Protocol TCP  new-AzureNetworkSecurityRuleConfig -Name INTERNALUDP-OUT -Direction Outbound -Priority 100 -Access Allow –SourceAddressPrefix '10.0.0.0/24' -SourcePortRange '\*' -DestinationAddressPrefix '10.0.0.0/24' –DestinationPortRange '\*' -Protocol UDP |
| 1. Attach the NSG to the VMs |  |
| 1. RDP into the second DC |  |
| 1. Add a new disk and initialize it on the second machine. This will hold the SYSVO shareL |  |
| 1. Add the DC role to the machine using the add roles and features wizard |  |
| 1. Once complete promote the machine to a domain controller |  |
| 1. If you have configured a new AD site, select it here |  |
| 1. Click next and accept the defaults until you get to the following screen |  |
| 1. Point out the paths to the C drive and change this to the F drive | Point out that this drive is new |
| 1. Click next and accept the defaults for the next screens |  |
| 1. When the DC is promoted and added to the domain, the VM will reboot. This takes around 2-5mins |  |
| End demo |  |

## Clean Up

To clean up this environment delete the resource group you created in the Setup section.