Extending Active Directory to Azure

Demo

# Objective

In this demo we’ll be connecting an existing on-premise network (simulated by an Azure infrastructure built on one VNET) with a virtual network in the another Azure VNET in a separate region via a secure Site-to-Site (S2S) IPsec VPN tunnel.  We will demonstrate the ability to host a full instance of Windows Server Active Directory, running on Windows Server 2012 R2, as a virtual machine in Azure cloud.

# Demo Prerequisites

This demo requires the following:

* A Windows Azure subscription
* Prior experience with Windows Server Active Directory.  This article also assumes that the reader is already somewhat familiar with configuring Windows Server 2012 Active Directory in an on-premise deployment
* This demo assumes the infrastructure with VNETs in two regions to have been setup and connected via S2S VPN. If needed, this prerequisite can be met by following the instructions [here](http://blogs.technet.com/b/canitpro/archive/2014/06/03/step-by-step-configure-vnet-to-vnet-connectivity-in-azure.aspx)
* This demo assumes the existence of a Windows Server 2012 R2 domain controller on one of the VNETs. This environment simulates the on-premises infrastructure. From here on out, we will refer to this infrastructure as ‘on-premises’

# Demo Preparation

## Configure On-Premise Active Directory Sites and Subnets

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Description | Action/Instruction | Screenshot |
| 1 | Launch the Active Directory Sites and Services tool on the on-premises Windows Server domain controller | In Windows Server 2012, this tool can be launched in Server Manager by selecting **Tools | Active Directory Sites and Services** |  |
| 2 | Create a new AD Site for Azure | In the Active Directory Sites and Services window, right-click on the Sites folder in the left navigation pane and select **New Site**  In the New Object – Site dialog box, enter WindowsAzure in the Name: field and click on DEFAULTIPSITELINK in the Link Name list. |  |
| 3 | Create a new AD Subnet for Windows Azure | In the Active Directory Sites and Services window, right-click on the Subnets folder located below the Sites folder in the left navigation pane. Select New Subnet |  |
| 4 |  | In the Prefix: field, enter the IPv4 subnet in which the Windows Server Active Directory replica domain controller in this scenario will be located using CIDR notation: 10.2.0.0/24 (this value comes from your existing VNET that represents the cloud infrastructure. Click **OK**. |  |
|  |  |  |  |

## Register DNS in Windows Azure

We’ll be registering our existing on-premise Active Directory-integrated DNS server with Windows Azure. We’ll also be registering the cloud-based Active Directory-integrated DNS server that will be provisioned in Exercise 4 as a Replica Domain Controller using Windows Azure VMs.

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Description | Action/Instruction | Screenshot |
| 1 | Launch the Windows Azure Management Portal | Sign in to an Azure Management Portal |  |
| 2 | Register the On-Premise Active Directory-integrated DNS Server | Click on the NETWORKS link in the left navigation pane of the Windows Azure Management Portal and then click the **+NEW** button located on the bottom toolbar |  |
|  |  | In the NEW menu, select Networks | Virtual Network | Register DNS Server. In the Name field, type SAPDC. In the DNS Server IP Address field, type the IPv4 address associated with the on-premise DNS Server in this scenario: 10.1.0.4. Click **Register DNS Server** |  |
| 3 | Register the Cloud-based Active Directory-integrated DNS Server | Click on the NETWORKS link in the left navigation pane of the Windows Azure Management Portal and then click the **+NEW** button located on the bottom toolbar |  |
|  |  | In the NEW menu, select Networks | Virtual Network | Register DNS Server. In the Name field, type CloudDNS. In the DNS Server IP Address field, type the IPv4 address associated with the cloud DNS Server that will be provisioned later: 10.0.2.44. Click **Register DNS Server** |  |

## Provision a New Replica Domain Controller in Windows Azure

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Description | Action/Instruction | Screenshot |
| 1 | Sign-in to Azure Management portal |  |  |
| 2 | Select Virtual Machines | 3.Click the +**NEW** button located on the bottom navigation bar and select **Compute | Virtual Machines** | From Gallery. Deploy a new VM with Windows Server 2012 R2 |  |
| 3 | Configure VM | On the Virtual Machine Config. page, complete the fields as follows:  - Virtual Machine Name: CloudAD  - New Password and Confirm Password fields: Choose and confirm a new local Administrator password.  - Size: Small (1 core, 1.75GB Memory)  Click the [Next](http://blogs.technet.com/cfs-file.ashx/__key/communityserver-blogs-components-weblogfiles/00-00-00-94-09-metablogapi/2804.image_5F00_392545A0.png)button to continue |  |
|  | Specify Name and network settings | For the VM creation, specify the values as the screenshot. This is done in the preview portal with Classic VM creation. The VNET name can be the VNET that represents the cloud infra. Storage account name can be any storage account in the cloud infra. region.  click the [Checkmark](http://blogs.technet.com/cfs-file.ashx/__key/communityserver-blogs-components-weblogfiles/00-00-00-94-09-metablogapi/7522.image_5F00_4B709D13.png)button to begin provisioning the new virtual machine. |  |
| 4 | Connect to the CloudAD VM |  |  |
| 5 | Add the AD Domain Services role to the VM | Using the **Server Manager** tool, install Active Directory Domain Services and promote this server to a Replica Domain Controller in an existing Active Directory domain with the following parameters:     - **Active Directory domain name:** DNS name of on-premise Active Directory domain: SAPDC    - **Active Directory site name:** WindowsAzure |  |
| 6 | Promote this server to a domain controller | When the installation of Active Directory Domain Services has completed, **do not** click the **Close** button.  Instead, click the link titled **Promote this server to a domain controller**.       This will launch the Active Directory Domain Services Configuration Wizard. |  |
| 7 |  | Specify the domain this server is being promoted into and enter the user credential with domain admin rights.  Click Next. |  |
| 8 |  | Select and options as shown and enter a password. |  |
| 9 |  | Click OK to ignore this message |  |
| 10 |  | Click Next |  |
| 11 |  | Accept Defaults for the paths |  |
| 12 |  | Verify there is no hard errors. The warnings on the screenshots are acceptable. Click Install. After the promotion, the server will reboot. |  |

# Performing the demo

The objective is to demonstrate the Windows Active Directory replication across VNETS in two regions.

|  |  |  |
| --- | --- | --- |
| Step | Description | Screenshot |
| 1 | Create a new testuser2  On the SAPDC server, find the AD Users and Computers tool. Right click **Users | New | User** to create a new ‘testuser2’ |  |
| 3 | Create testuser2 |  |
| 4 | Enter ‘Reset!22’ for password and confirm the password. Click **finish** when prompted |  |
| 5 | So far we are still working on the SAPDC domain controller.  Ensure the new user shows up |  |
| 6 | Since the default inter-site replication interval is 180 min, you won’t find the new user over the CloudAD domain controller.  **Need to force a replication**  On the **AD Sites and Services** tool, expand the **WindowsAzure** site, go the right pane right click on the **‘<automatically generated>** property setting, select **Replicate Now** |  |
| 7 | Back to the **Users and Computer** tool, the refresh doesn’t work too well, you may need to close out of the Users and Computer tool and come back to see the result of the replication |  |