

INGRAM MICRO[®]

Azure



EASYDATA FILE SERVER

V1.0

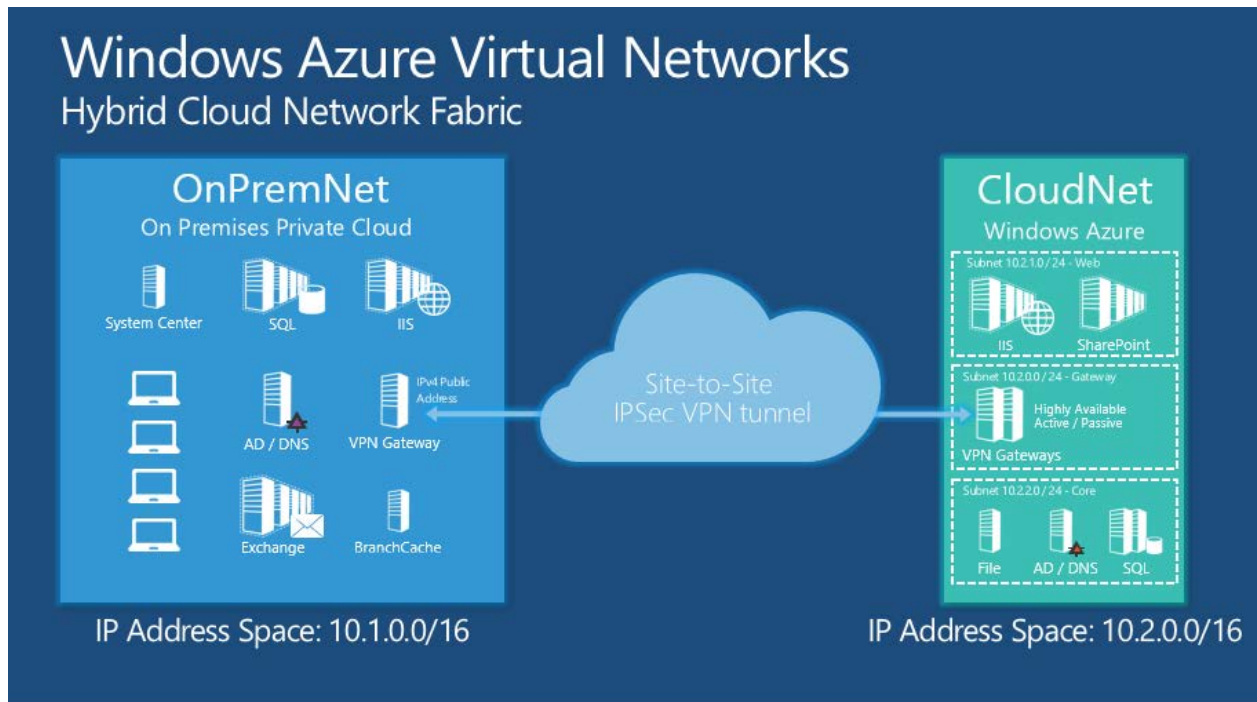
DOCUMENT OWNER: OUDHUIS, JONATHAN
INGRAM MICRO CLOUD
EUROPE

CONTENTS

1	Introduction.....	2
2	Creating and configuring a virtual machine.....	3
3	File Server Deployment.....	6
4	Access Tests.....	13
5	Configuring automatic backup	14

1 INTRODUCTION

EasyData File Server is a complete Windows server in the cloud, with file sharing and storage capacity that is easily expandable according to your needs. It is integrated with your environment via a VPN and is accessed in the same way as any other component in your network:



This service is implemented using a Windows 2016 virtual machine, on Azure, and the File Server role. The steps are identical to installing the role on 2012 R2 if that version is more preferred.

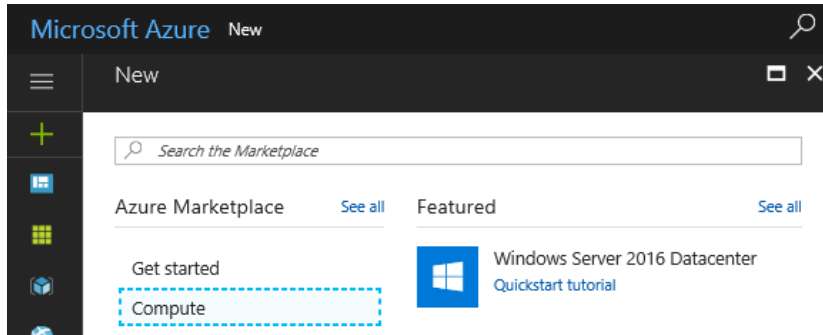
This document will guide you through the steps of setting up an Azure file server. You need an Azure account to use this service.

There are two prerequisites for the proper functioning of this script:

- A VPN connection between your on-premises environment and Azure
- Routing between your on-premises environment and the VLAN where you will deploy the server following this manual.

2 CREATING AND CONFIGURING A VIRTUAL MACHINE

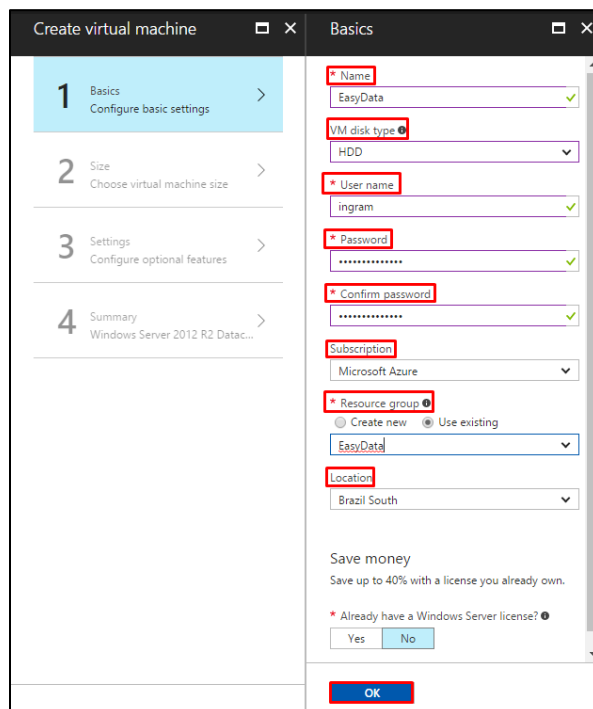
On the Hub menu, click **[+ New]**, **[Compute]**, select either **[Windows Server 2012 R2 Datacenter]** or **[Windows Server 2016 Datacenter]** and click **[Create]**:






On the **[Basics]** blade, enter a name for the machine in the **[Name]** field. In the **[VM disk type]** field, choose **HDD**.

Enter the user name of the machine administrator in the **[User Name]** field and in the **[Password]** and **[Confirm Password]** fields enter a password for this user. Make sure that the correct subscription is selected in the **[Subscription]** field and choose an existing resource group in the **[Resource group]** field. Also check the option in the **[Location]** field, which should be the closest to you and connected via VPN.

Then click **[OK]**.



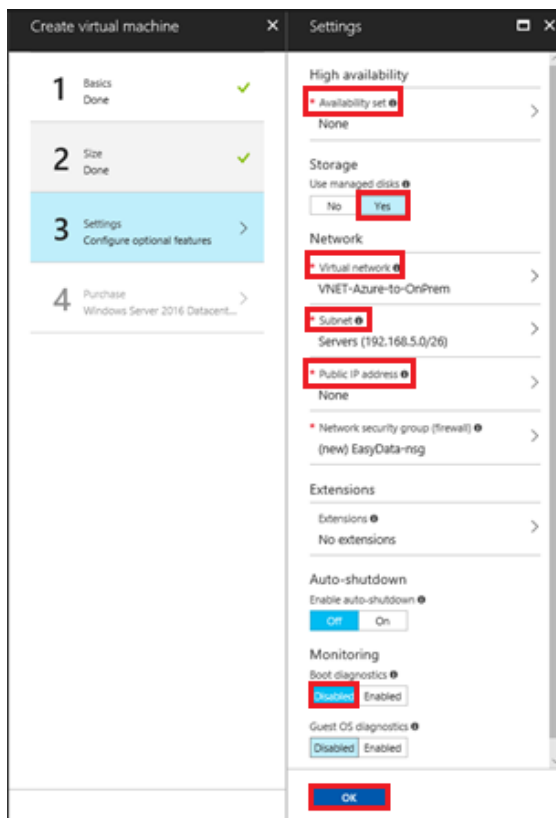
On the **[Size]** blade, select **A2_V2 Standard** (a more or less powerful machine can be selected depending on the needs. When storing large amounts of files, keep in mind that the number of disks, IOPS and throughput are important and might be different per VM Size) and click **[Select]**. If not visible, all size options can be displayed through the **[View All]** button:

A2_V2 Standard	
2	vCPUs
4	GB
	4 Data disks
	4x500 Max IOPS
	Load balancing

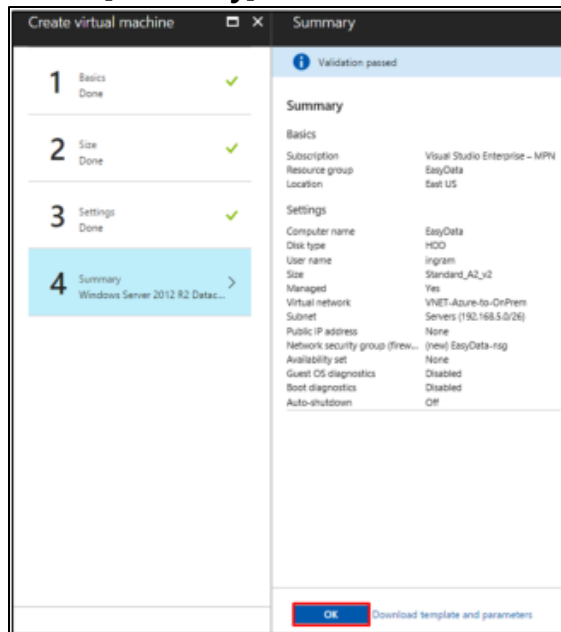
On the **[Settings]** blade, choose **Yes** under **[Use managed disks]**.

Make sure the **[Virtual Network]** and **[Subnet]** fields are in accordance with the prerequisites. You do not need to set a public IP so click on the **[Public IP Address]** field and select the **[None]** option. Make sure that the **[None]** option is selected in the **[Availability set]** field and that diagnostics is **Disabled** in the **[Monitoring]** fields.

Then click **[OK]**.



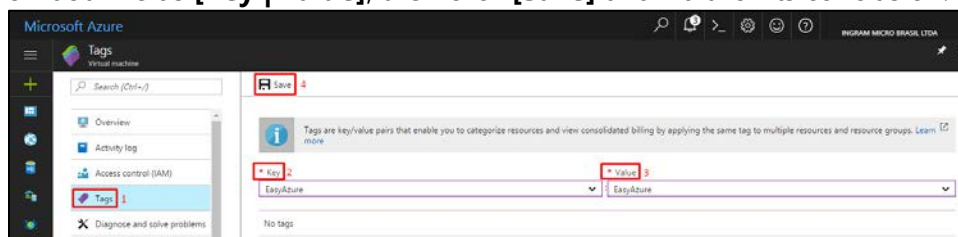
On the **[Summary]** blade, check the information and press **[OK]**.



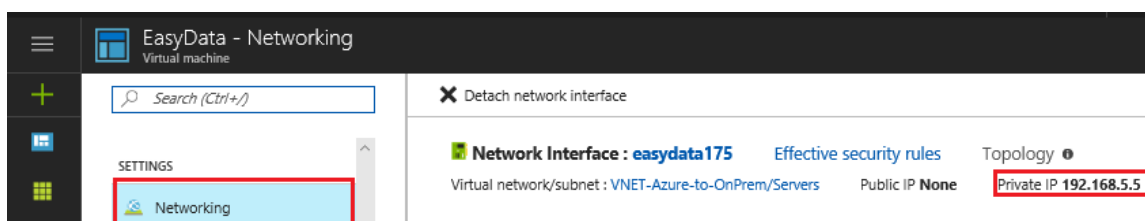
On the Azure dashboard, you can monitor the machine's deployment process:



When deployment is finished, open the machine properties, click **[Tags]**, then type **[EasyAzure]** on both fields **[Key | Value]**, then click **[Save]** and wait for its conclusion.



Select **[Networking]**. The internal IP address linked to this new machine will appear on the right blade. Write down the number for the next steps:

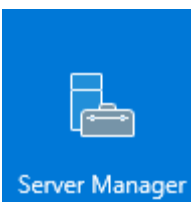


3 FILE SERVER DEPLOYMENT

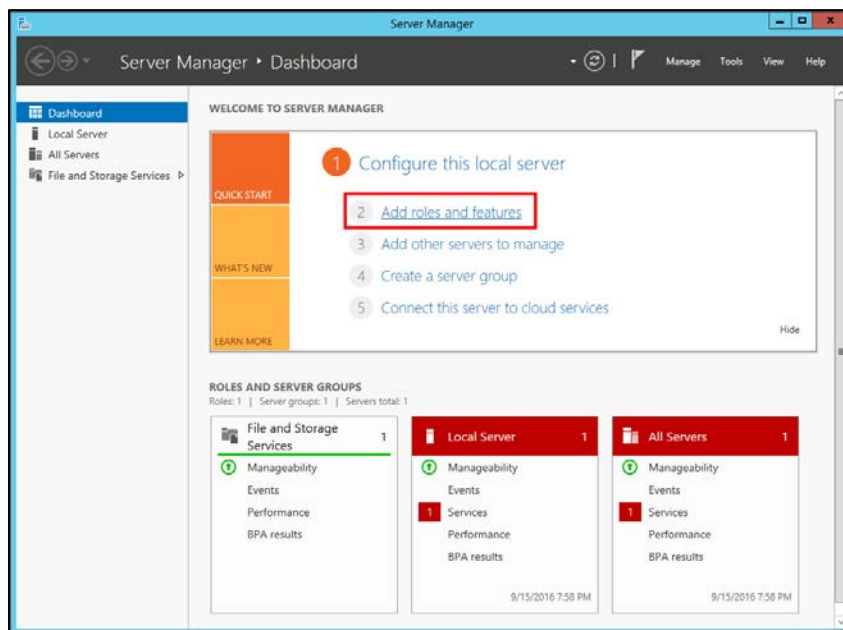
After completion of the deployment, connect to the virtual machine using Remote Desktop Connection, using the IP address from the previous step.

It is advised to join the server to your domain before continuing.

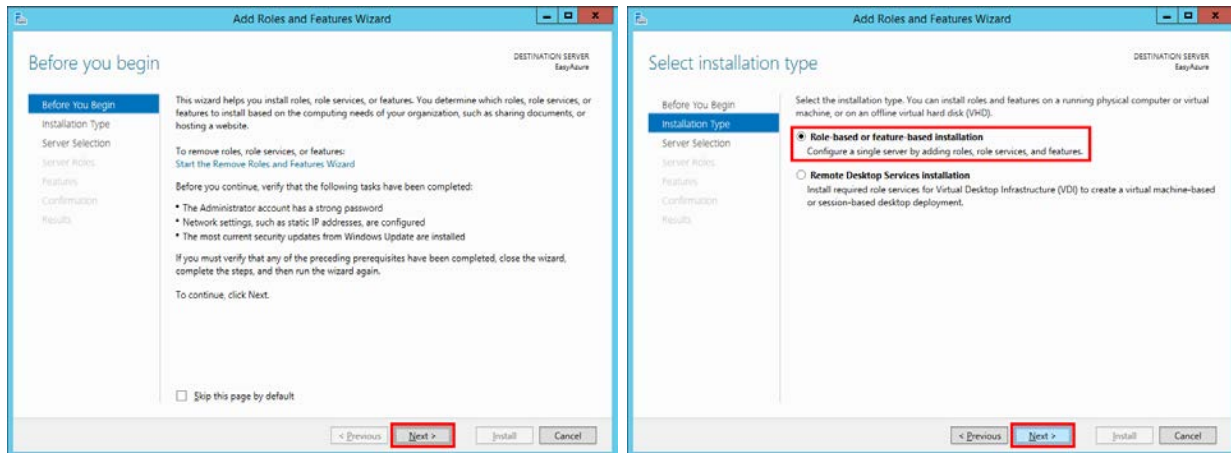
Once connected, the **Server Manager Dashboard** should start automatically. If not, look for **Server Manager** on the start menu:



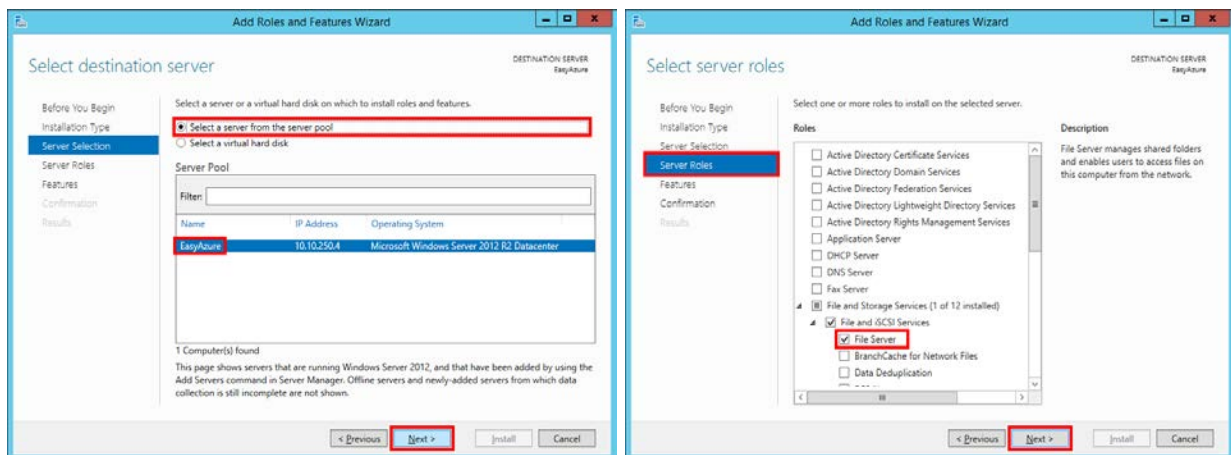
On the Dashboard, click **[Add roles and features]**:



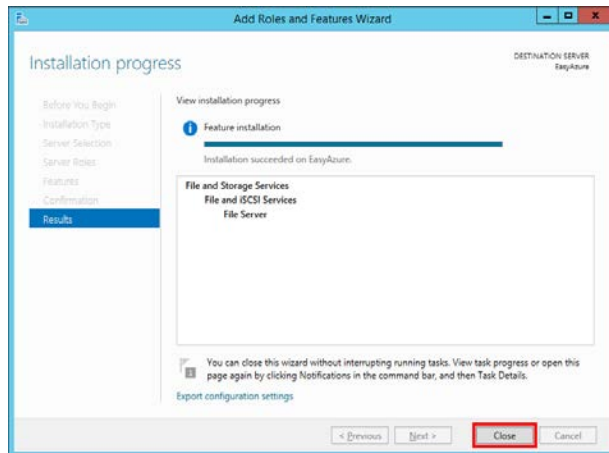
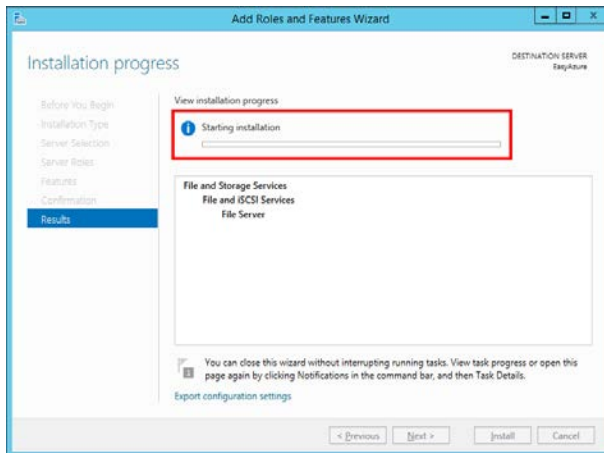
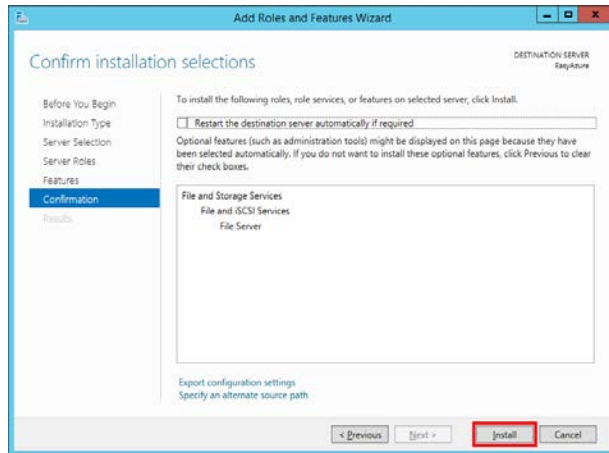
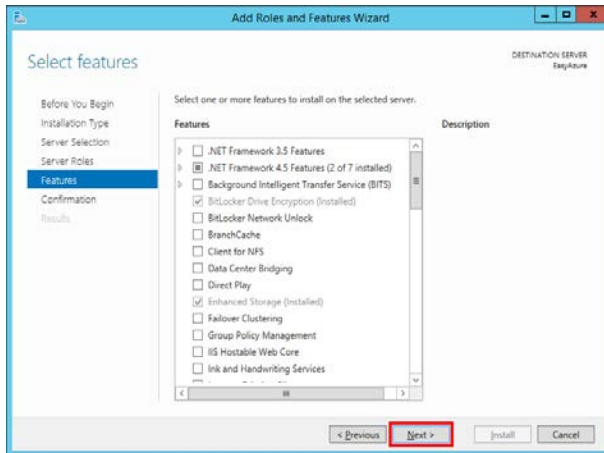
In the **[Before you begin]** window, click **[Next]** and in the **[Select installation type]** window, make sure the **[Role-based or feature-based installation]** option is selected and click **[Next]**:



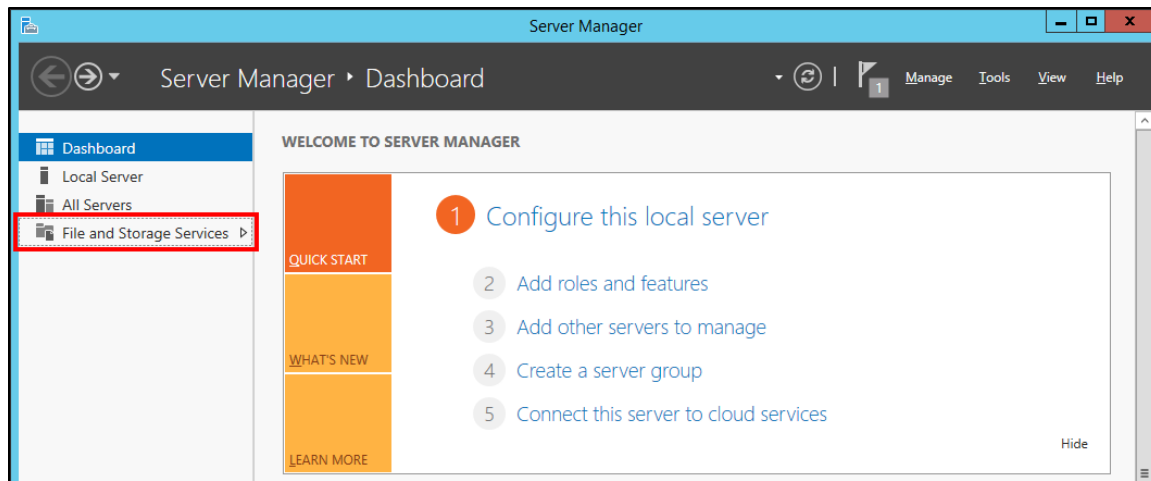
In the **[Select destination server]** window, make sure the **[Select a server from the server pool]** option is selected and click **[Next]**. In the **[Select server roles]** window, click **[File Server]**:



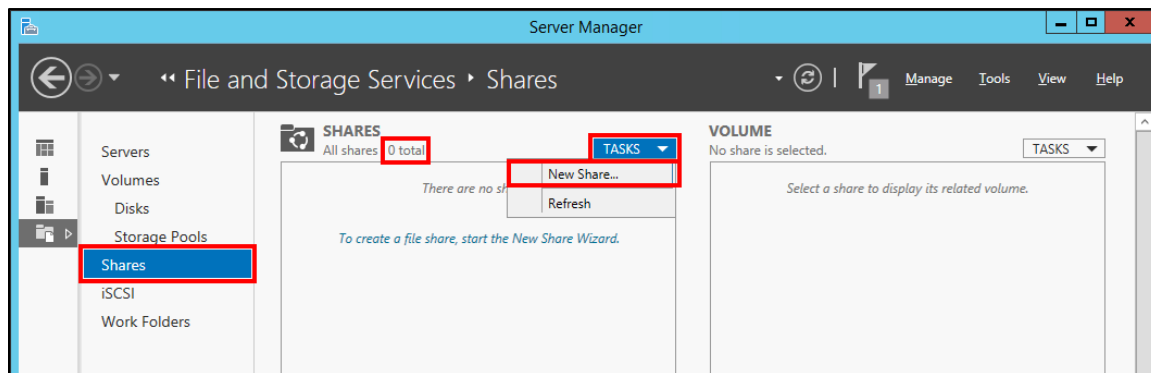
In the next windows, click **[Next]** and wait. After installation finishes, click **[Close]**.



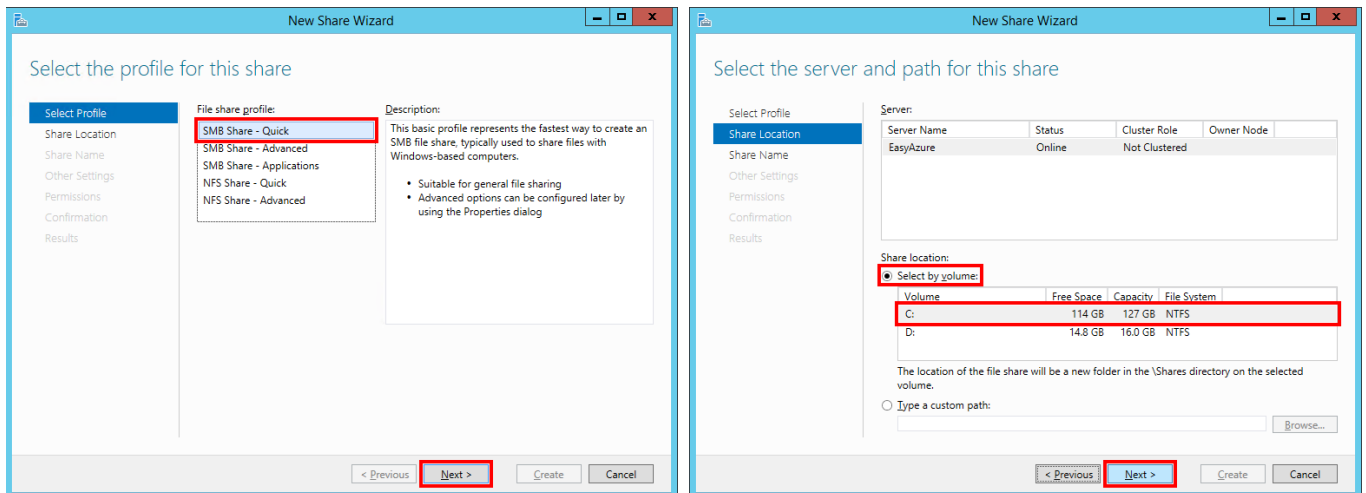
After installing the File Server role, click **[File and Storage Services]**:



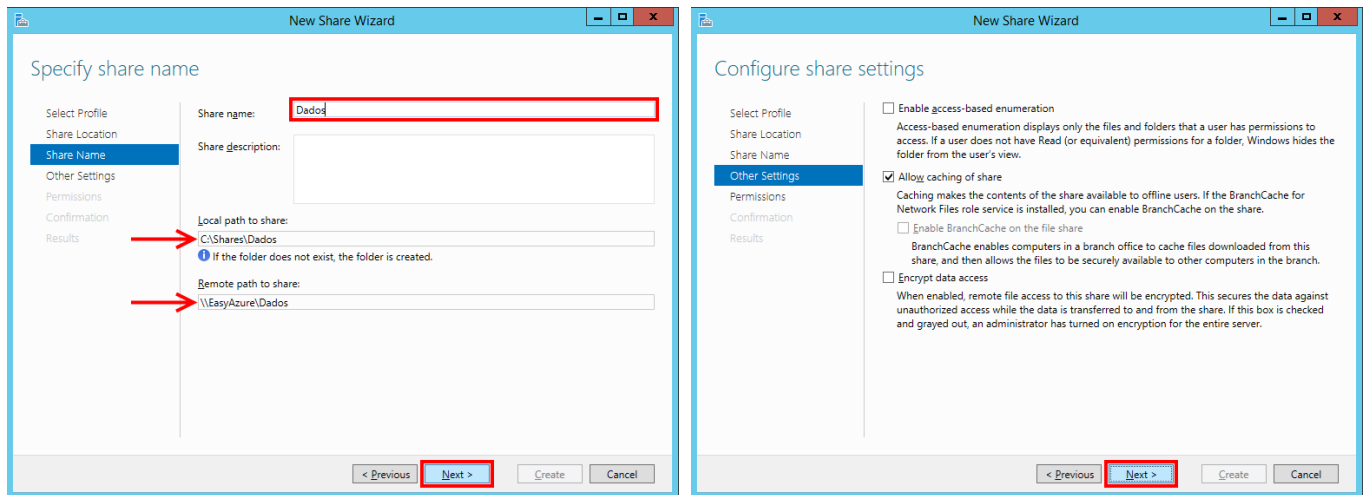
Click **[Shares]** and note that the quantity of shares is zero. Click **[TASKS]** and then **[New Share...]**:



In the **[Select the profile for this share]** window, make sure that the **[SMB Share - Quick]** option is selected and click **[Next]**. In the **[Select the server and the path for this share]** window, click **[Select by volume]** and volume **[C:]**. Then click **[Next]**:



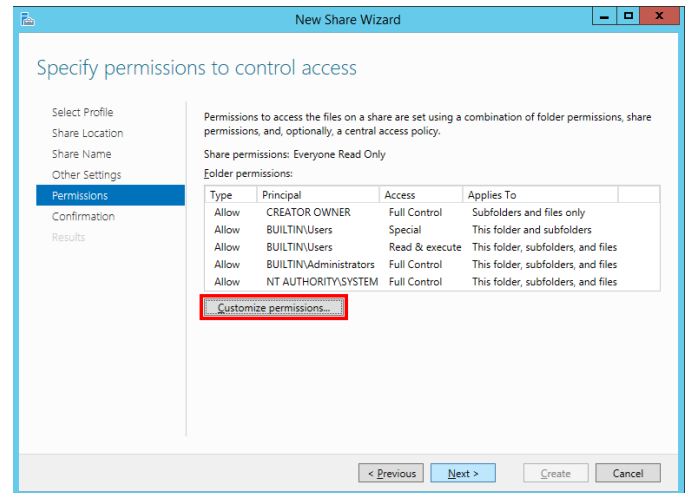
In the **[Specify share name]** window, enter a name for the share. Note that the **[Local path to share]** and **[Remote path to share]** fields are adjusted automatically. Write down the values to use in the next step. Click **[Next]**. In the **[Configure share settings]** window click **[Next]**:



By default, the created share will allow access to read-only files.

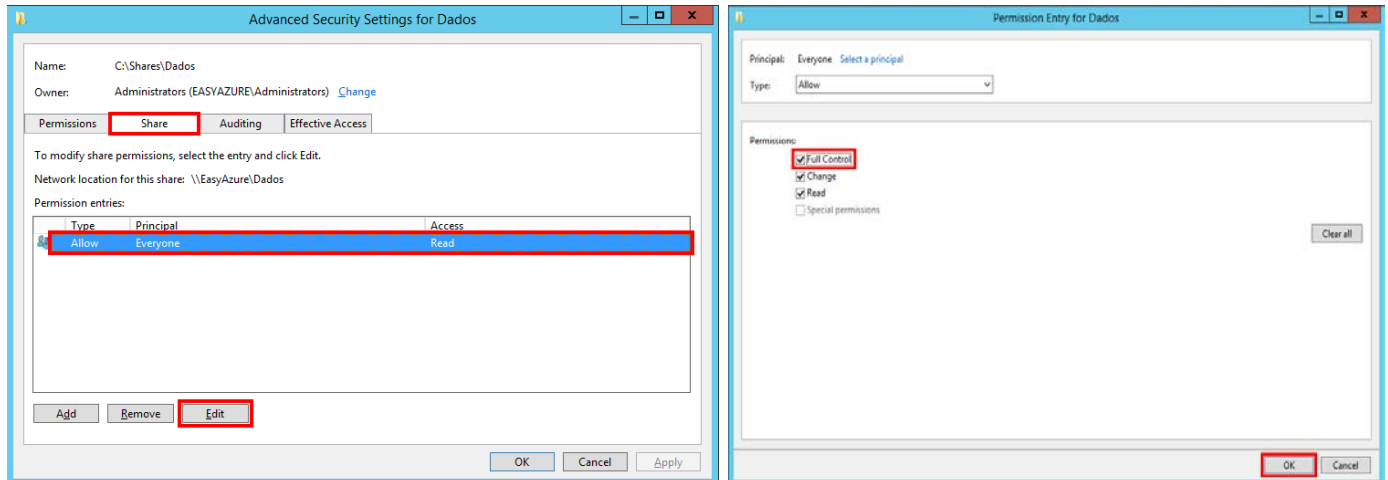
It is possible to create local users in this environment or use domain users when joined to a domain.

To change this feature to allow writing, click **[Customize permissions...]** in the **[Specify permissions to control access]** window.



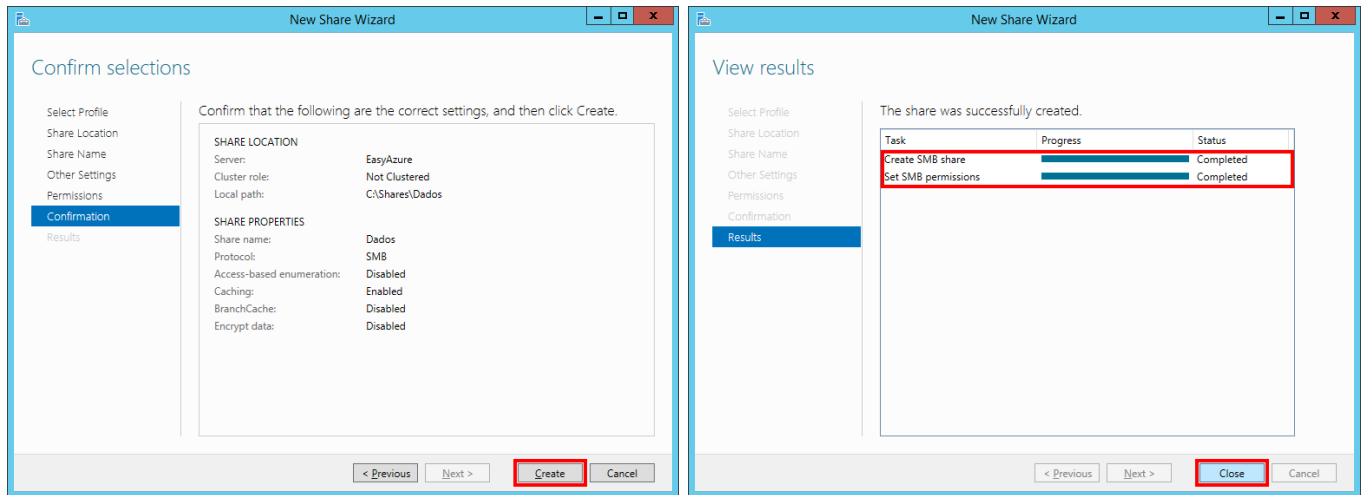
In the **[Advanced Security Settings]** window, click the **[Share]** tab. Verify that **Access** displays **Full Control**.

If not, click the line and click **[Edit]**. In the **[Permission Entry]** window, click **[Full Control]** and **[OK]** this changes the share permissions only. NTFS permissions are not changed.:



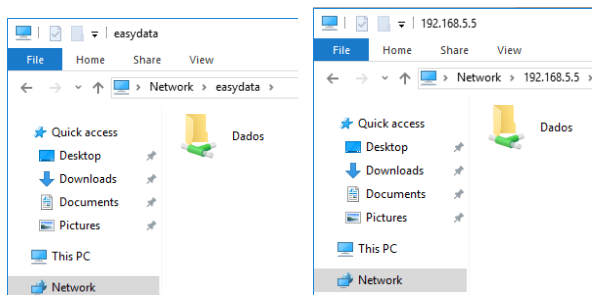
Click **[OK]** to return to the previous screen and then **[Next]** to continue.

In the **[Confirm selections]** window, review the information and click **[Create]**. In the **[View results]** window, wait until deployment has finished and then click **[Close]**:

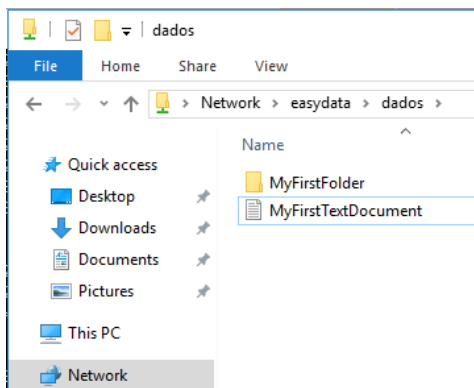


4 ACCESS TESTS

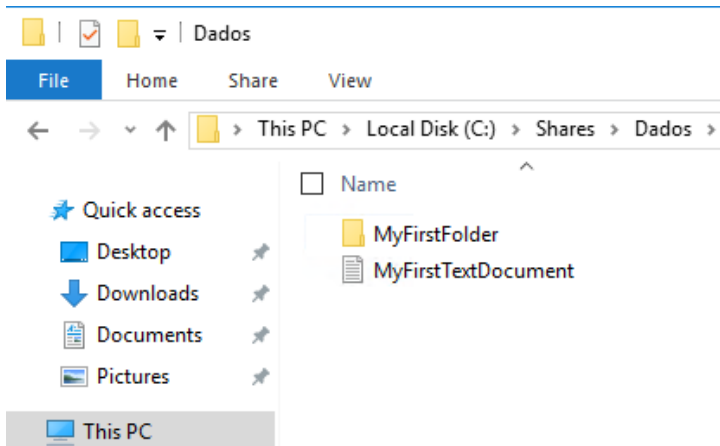
To test operation, access the server via Windows Explorer, using the name (preferable) or the IP address as written down in the previous step:



Test writing by creating some files:



On the server, the data will be in the folder that was set by the **[Local path to share]** option in the previous step:



For production environments it is highly recommended to use a separate disk to store your shared files and folders. However, by following this manual, you get a clear idea about the deployment within Azure and how this can be integrated with your on-premises environment.

5 CONFIGURING AUTOMATIC BACKUP

To configure automatic backup, follow the procedures outlined in the document Easy Backup Azure or one of the other EasyAzure backup solutions.

The information contained in EasyData File Server is believed to be accurate. However Ingram Micro expressly disclaims any warranty, expressed or implied, concerning the accuracy, completeness or suitability of any information or services provided herein. The information, services, products and materials contained in the EasyData File Server including without limitations text, graphics and links are provided on an "as is" basis with no warranty, express or implied. Users are to implement the steps described in the EasyData File Server in a non-production environment before adopting the solution into the user's production environment.