Synchronize Files Across Servers with Azure File Sync

<https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-firewall-and-proxy>

Invoke-AzStorageSyncCompatibilityCheck E:\FileSyncFolder\Reports

Environment validation results:

Computer name: localhost

OS version check: Passed.

File system check: Passed.

Namespace validation results:

Path: E:\FileSyncFolder\Reports

Number of files scanned: 0

Number of directories scanned: 1

There were no compatibility issues found with your files.

Test using UNC path

Invoke-AzStorageSyncCompatibilityCheck \\aueodsutdb001\e$\FileSyncFolder\Reports

Environment validation results:

Computer name: aueodsutdb001

OS version check: Passed.

File system check: Passed.

Namespace validation results:

Path: \\aueodsutdb001\e$\FileSyncFolder\Reports

Number of files scanned: 0

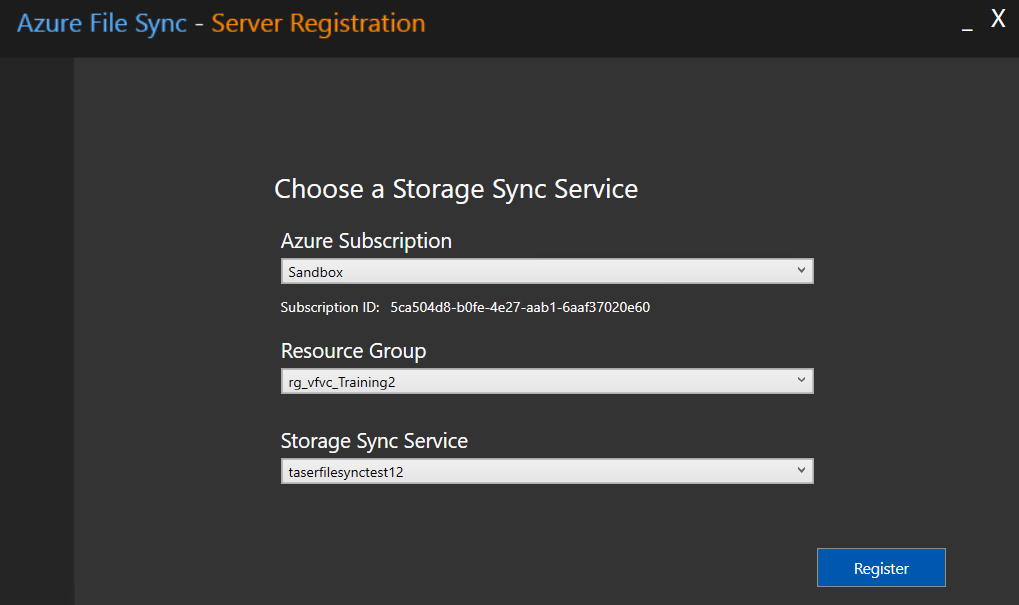
Number of directories scanned: 1

There were no compatibility issues found with your files.

**STEPS**

1. Create Storage Account & File share
2. Create File synch service
3. Create synch group
4. Download & install synch agent & set up

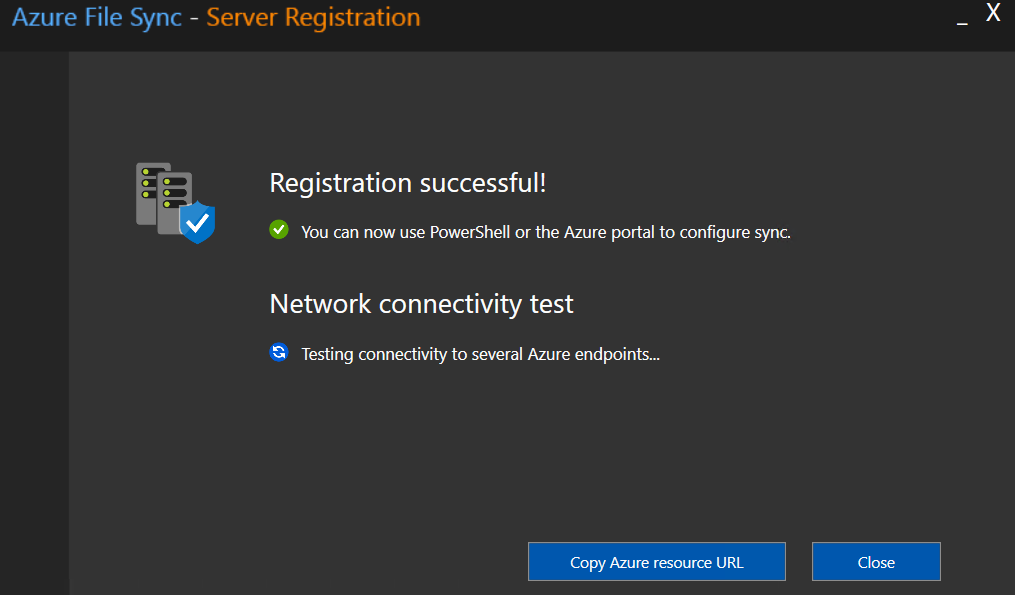
Synch agent steps



Click Register

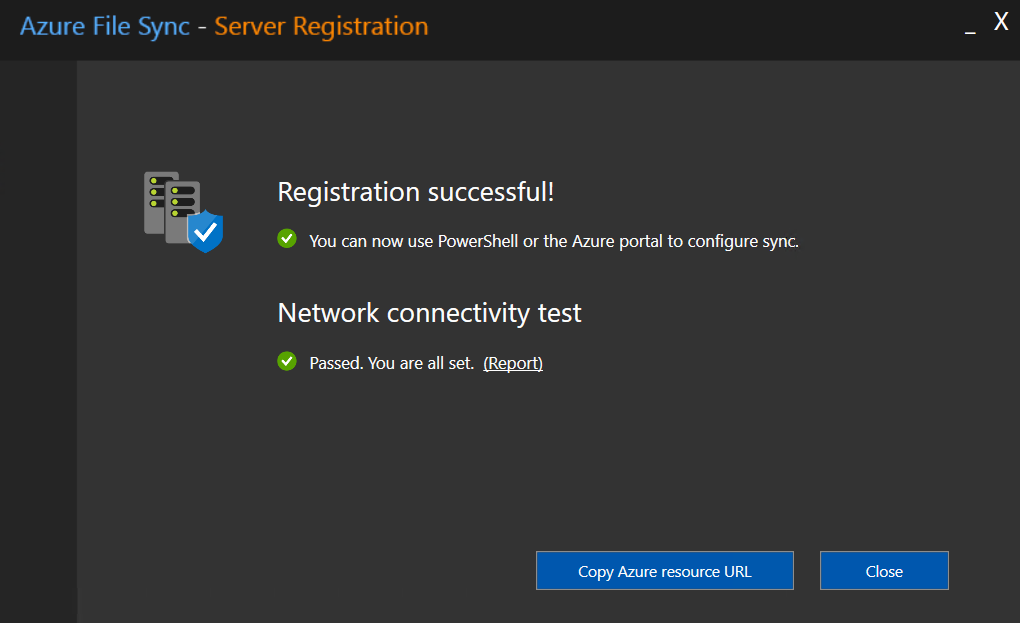
You will need to authenticvate one more time (this will be removed in the next ver of File Sync Agent)

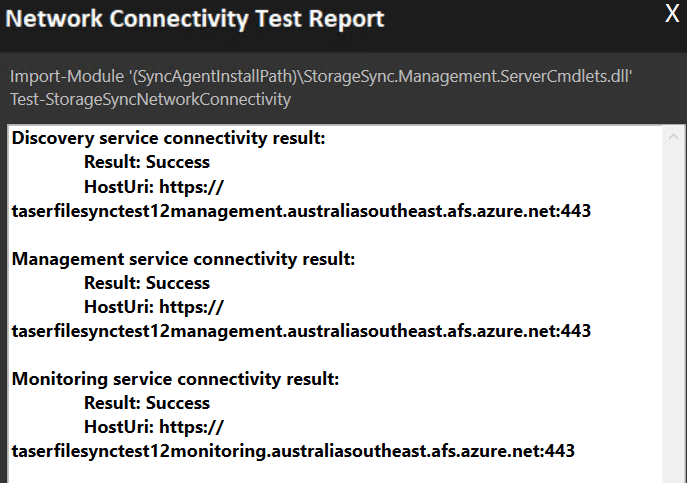
You will get a scren that shows registration successful



Click the copy Azure Resource URL as you will need this in the next step

Wait till you see the testing connectivity as Passed





If you have connectivity issues. Make sure the firewalls are open / send firewall request to Infrastructure team to open required firewalls

For .one.microsoft.com & .afs.azure.net we can limit to the below since we will use Australia East & Sth East Only

1. .afs.azure.net

Australia East https://australiaeast01.afs.azure.net

Australia Southeast https://australiasoutheast01.afs.azure.net

2. .one.microsoft.com

https://kailani-aue.one.microsoft.com

https://tm-kailani-aue.one.microsoft.com

https://tm-australiasoutheast01.afs.azure.net

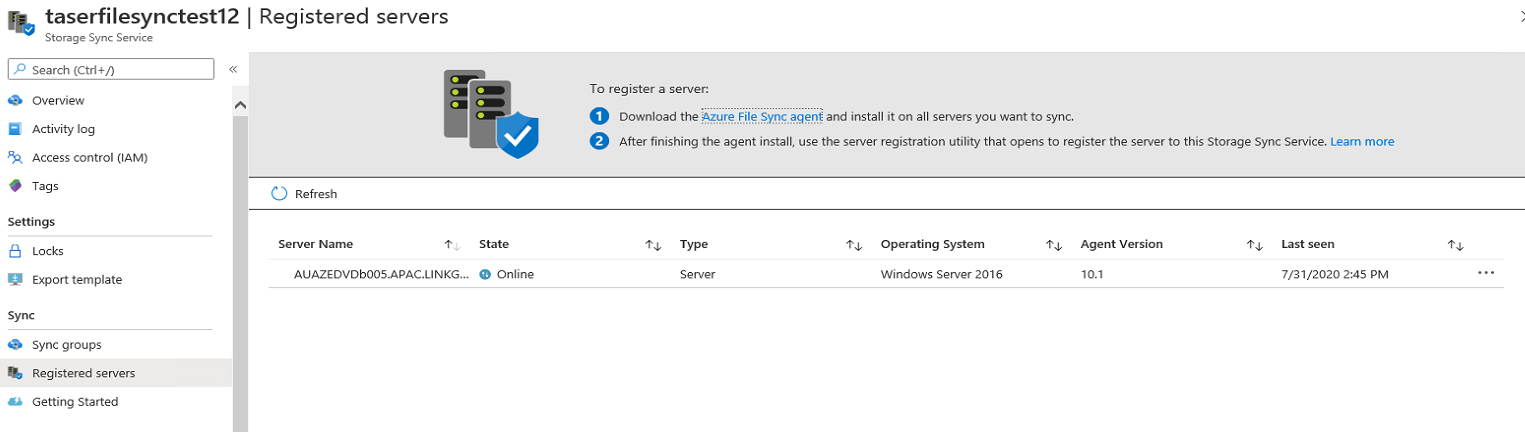
Port 443

You will need the URL so copu it

<https://portal.azure.com/#resource/subscriptions/5ca504d8-b0fe-4e27-aab1-6aaf37020e60/resourceGroups/rg_vfvc_Training2/providers/Microsoft.StorageSync/storagesyncservices/taserfilesynctest12>

Now go back to portal & click refresh in the sync service

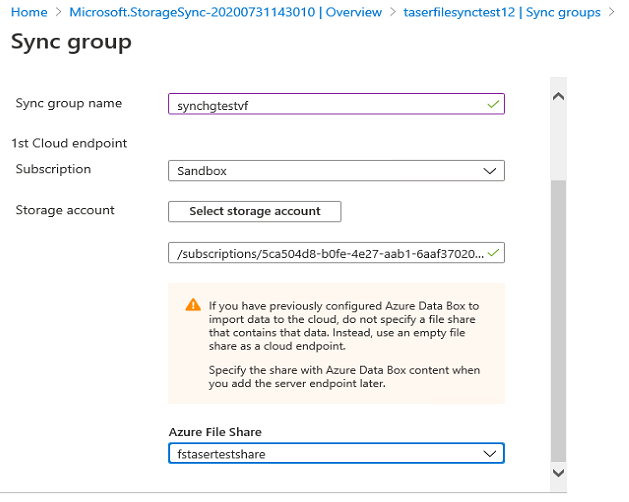
If you click Registered Servers, you will see the windows 2016 server that was just registerd with Sync agent

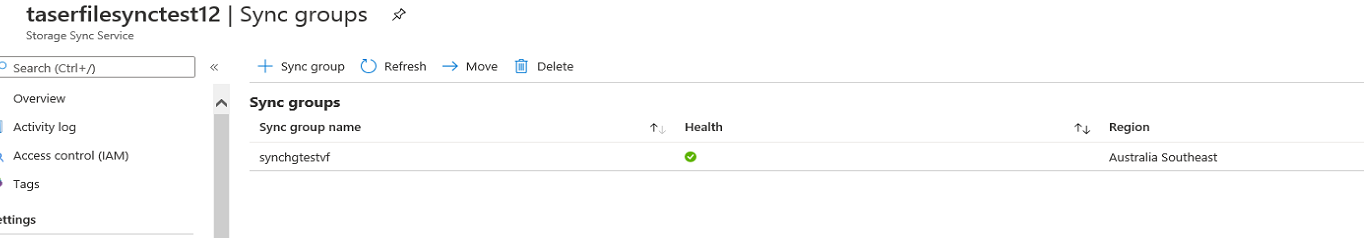


Now create the synch group (we want to tell the server to synch something)

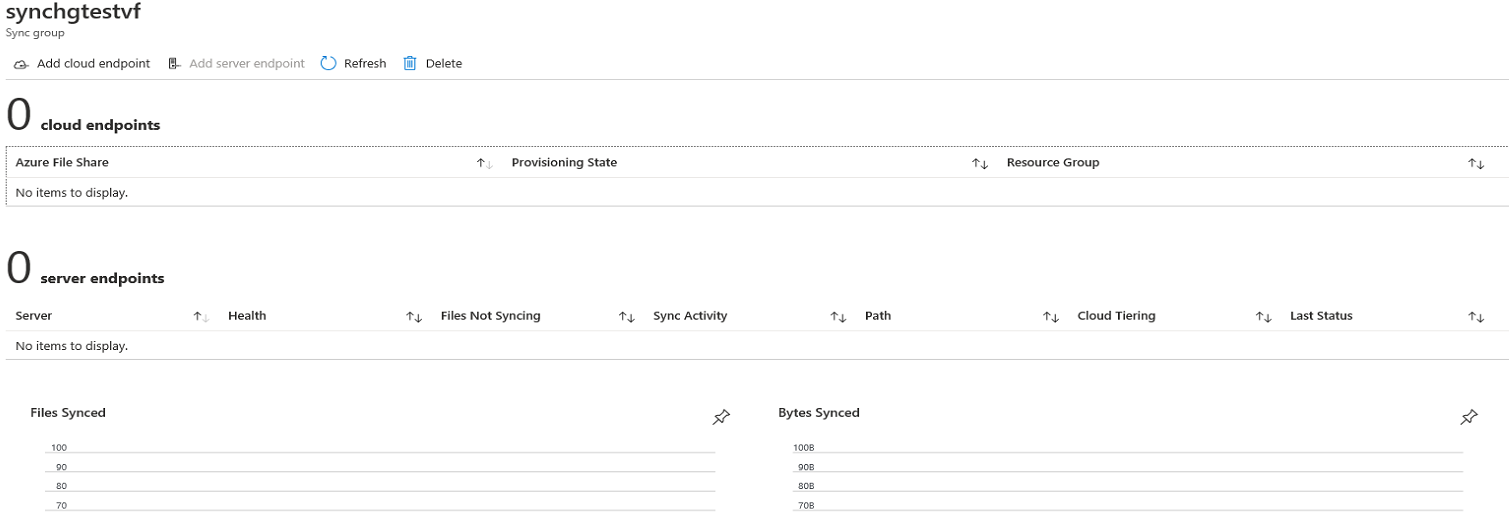
Click on the synch service & click New Sync group



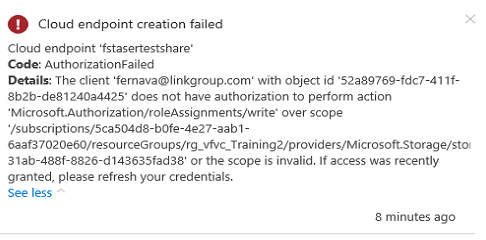




Now we have a synch group, if you refresh, you should see a cloud end point automatically being created



If it does nto create it might be errors due to permissions



* Cloud endpoint creation failed

Cloud endpoint 'fstasertestshare'  
**Code**: AuthorizationFailed  
**Details**: The client 'fernava@linkgroup.com' with object id '52a89769-fdc7-411f-8b2b-de81240a4425' does not have authorization to perform action 'Microsoft.Authorization/roleAssignments/write' over scope '/subscriptions/5ca504d8-b0fe-4e27-aab1-6aaf37020e60/resourceGroups/rg\_vfvc\_Training2/providers/Microsoft.Storage/storageAccounts/sataserfilesharetest/providers/Microsoft.Authorization/roleAssignments/489ed380-31ab-488f-8826-d143635fad38' or the scope is invalid. If access was recently granted, please refresh your credentials.

**Description**

Azure File Sync centralizes your company's file shares in Azure Files. Azure File Sync transforms Windows Servers running on-premises or in the cloud into a quick cache of your Azure file share. When you choose Azure File Sync, you do not need to sacrifice the flexibility, performance, or compatibility of an on-premises file server. Any protocol supported by Windows Server, including SMB, NFS, and FTPS, can be used to access the data locally.

In this Lab, you will create an Azure File Sync sync topology consisting of two Windows Server 2016 VMs running in Azure. You will then try out the synchronization and cloud tiering capabilities of Azure File Sync to better understand how the service works.

**Lab Objectives**

Upon completion of this Lab, you will be able to:

* Explain when to use and when not to use Azure File Sync
* Create and test a mutli-server sync group in Azure File Sync
* Understand cloud tiering and how it can improve file sharing performance and save costs
* Understand the fast disaster recovery feature of Azure File Sync

**Lab Prerequisites**

You should be familiar with:

* Basic Azure compute and storage services, particularly VMs and storage accounts

### Updates

July 8th, 2020 - Updated the screenshots to match the new Azure UI

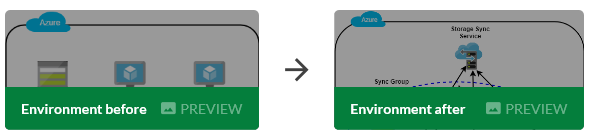
May 5th, 2020 - Added a validation check function to check the work done in the lab

January 14th, 2020 - Updated lab startup resources to avoid unsupported regions

November 15th, 2019 - Changed lab region to South Central US to avoid an issue that prevented completion of the lab in West US

June 26th, 2019 - Updated instructions for creating the Storage Sync Service to match the latest Portal experience

May 7th, 2019 - Added instructions to workaround an Azure bug that causes the create cloud endpoint permission check to fail despite the student user having the required permissions



### Exercise 0: Prepare the lab environment

The main tasks for this exercise are as follows:

1. Deploy an Azure VM by using an Azure Resource Manager template

#### Task 1: Deploy an Azure VM by using an Azure Resource Manager template

1. From the lab virtual machine, start Microsoft Edge, browse to the Azure portal at [**http://portal.azure.com**](http://portal.azure.com/) and sign in by using a Microsoft account that has the Owner role in the Azure subscription you intend to use in this lab.
2. In the Azure portal, navigate to the **New** blade.
3. From the **New** blade, search Azure Marketplace for **Template deployment**.
4. Use the list of search results to navigate to the **Custom deployment** blade.
5. On the **Custom deployment** blade, select the **Build your own template in the editor**.
6. From the **Edit template** blade, load the template file **Labfiles\Module\_12\Implementing\_File\_Sync\az-100-02b\_azuredeploy.json**.
7. Save the template and return to the **Custom deployment** blade.
8. From the **Custom deployment** blade, navigate to the **Edit parameters** blade.
9. From the **Edit parameters** blade, load the parameters file **Labfiles\Module\_12\Implementing\_File\_Sync\az-100-02b\_azuredeploy.parameters.json**.
10. Save the parameters and return to the **Custom deployment** blade.
11. From the **Custom deployment** blade, initiate a template deployment with the following settings:
    1. Subscription: the name of the subscription you are using in this lab
    2. Resource group: the name of a new resource group **az1000201b-RG**
    3. Location: the name of the Azure region which is closest to the lab location and where you can provision Azure VMs
    4. Vm Size: **Standard\_DS2\_v2**
    5. Vm Name: **az1000201b-vm1**
    6. Admin Username: **Student**
    7. Admin Password: **Pa55w.rd1234**
    8. Virtual Network Name: **az1000201b-vnet1**