



Redirecting Storage Platform to Azure Files

Virtual Desktop Service

Kris Gillette
April 14, 2021

This PDF was generated from https://docs.netapp.com/us-en/virtual-desktop-service/Architectural.change_data_layer.Azure_Files.html on July 20, 2021. Always check docs.netapp.com for the latest.

Table of Contents

Redirecting Storage Platform to Azure Files	1
Overview	1

Redirecting Storage Platform to Azure Files

Overview

Virtual Desktop Service deployment technologies allow for a variety of storage options depending on the underlying infrastructure. This guide addresses how to make a change to using Azure Files post-deployment.

Pre-requisites

- AD Connect installed and set up
- Azure global admin account
- AZFilesHybrid PowerShell module <https://github.com/Azure-Samples/azure-files-samples/releases>
- AZ PowerShell module
- ActiveDirectory PowerShell module


Create the new storage layer

1. Log in to Azure with the global admin account
2. Create a new Storage Account in the same location and resource group as the workspace

Create storage account ...



Basics Networking Data protection Advanced Tags Review + create

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below.

[Learn more about Azure storage accounts](#) 









Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

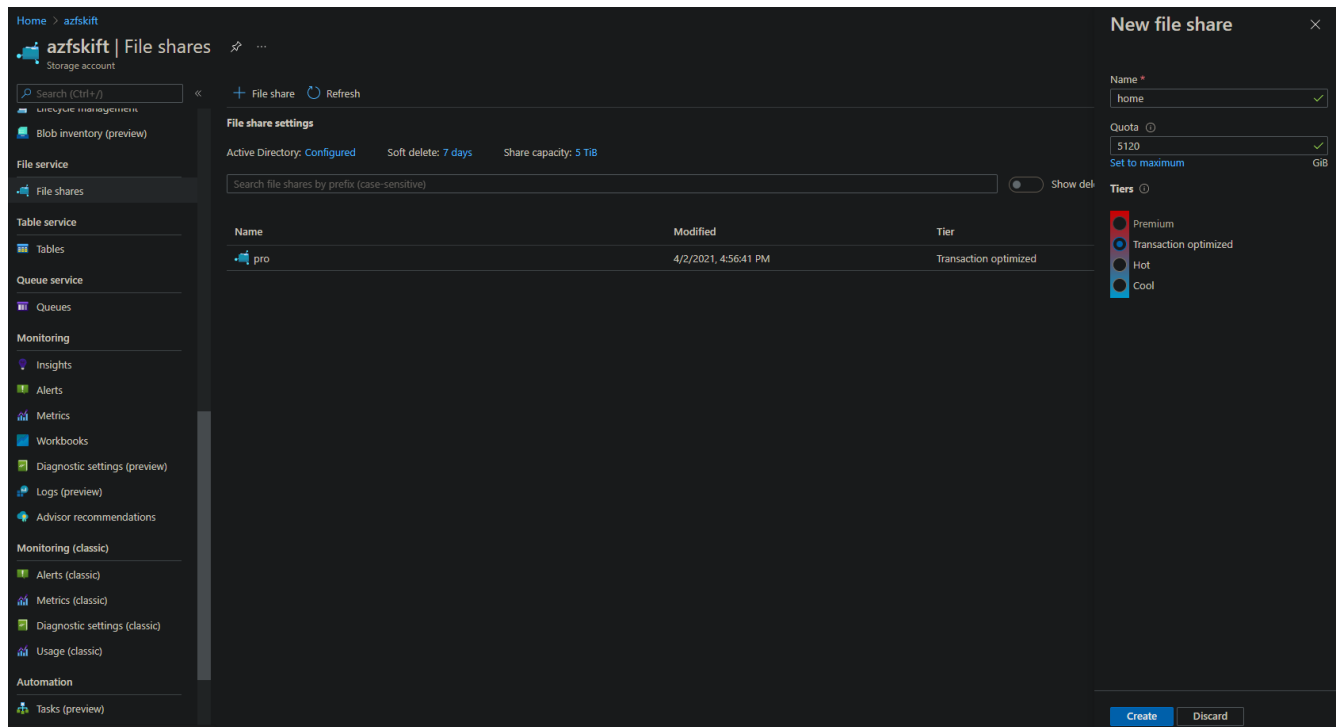
Subscription *	<div>Azure subscription 1 </div>
Resource group *	<div>vrg </div> <div>Create new</div>

Instance details

The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. [Choose classic deployment model](#)

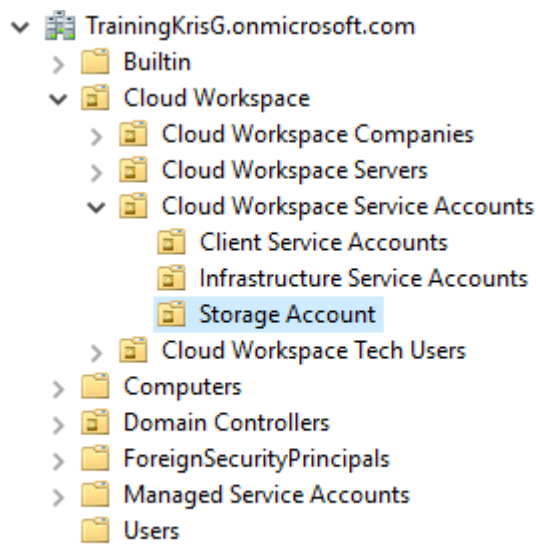
Storage account name * 	<div>azfskift </div>
Location *	<div>(US) East US </div>
Performance 	<div><input checked="" type="radio"/> Standard <input type="radio"/> Premium</div>
Account kind 	<div>StorageV2 (general purpose v2) </div>
Replication 	<div>Read-access geo-redundant storage (RA-GRS) </div>

3. Create the data, home, and pro file shares under the storage account



Set Up Active Directory

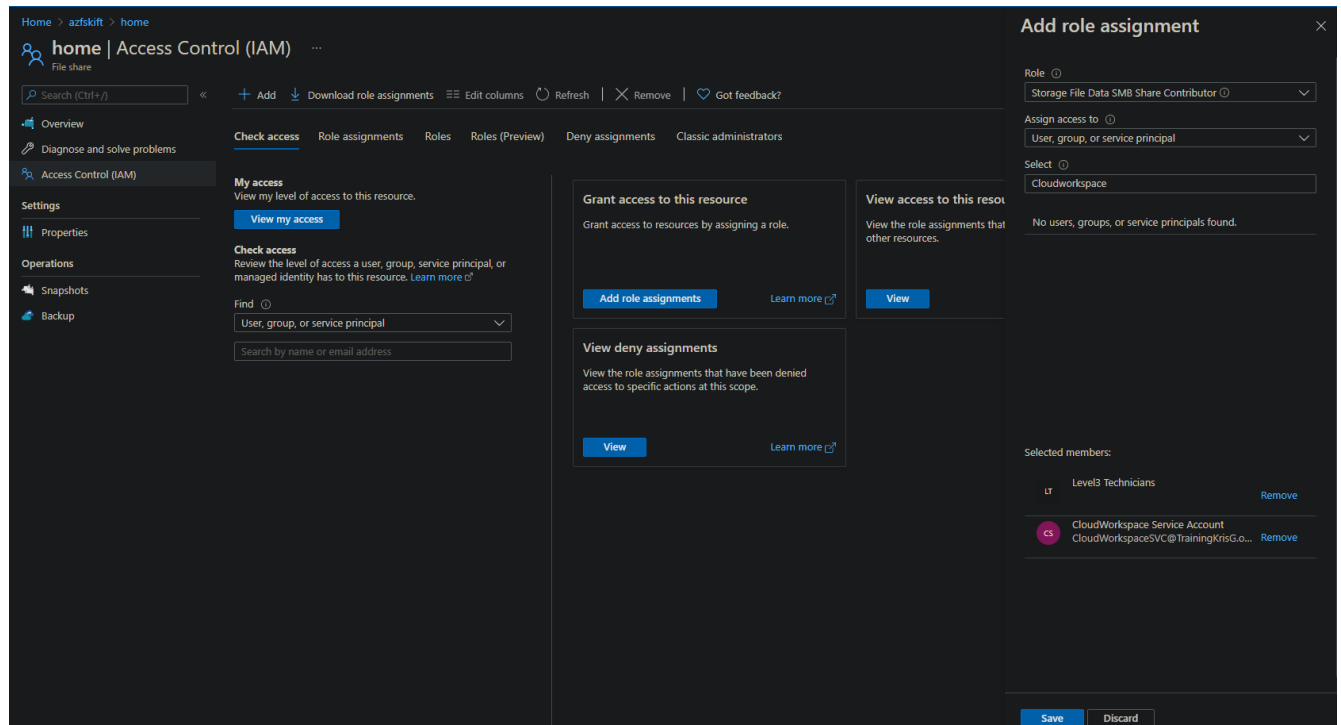
1. Create a new Organization Unit named "Storage Account" under the Cloud Workspace > Cloud Workspace Service Accounts OU



2. Enable AD DS authentication (must be done using PowerShell) <https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-enable>
 - a. DomainAccountType should be "ServiceLogonAccount"
 - b. OrganizationalUnitDistinguishedName is the distinguished name of the OU created in the previous step (ie "OU=Storage Account,OU=Cloud Workspace Service Accounts,OU=Cloud Workspace,DC=TrainingKrisG,DC=onmicrosoft,DC=com")

Set the Roles for the Shares

1. In the Azure portal, give "Storage File Data SMB Share Elevated Contributor" role to CloudWorkspaceSVC and Level3 Technicians



2. Give "Storage File Data SMB Share Contributor" role to the "<company code>-all users" group

Add role assignment



Role ⓘ

Storage File Data SMB Share Contributor ⓘ



Assign access to ⓘ

User, group, or service principal



Select ⓘ

kift-all

No users, groups, or service principals found.

Selected members:



kift-all users

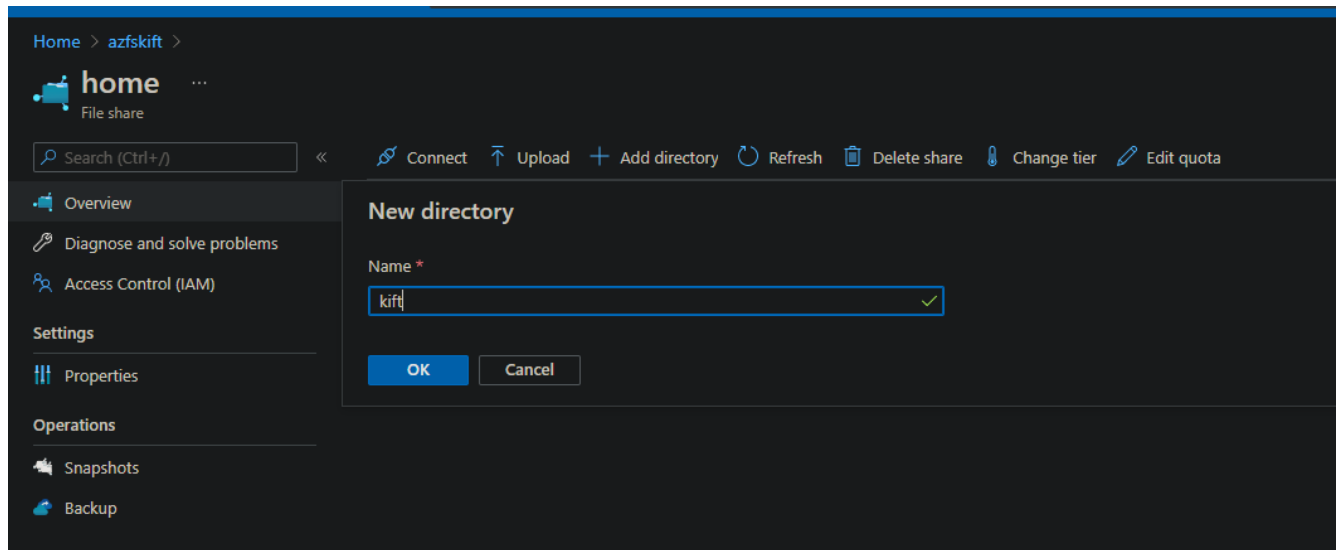
Remove

Save

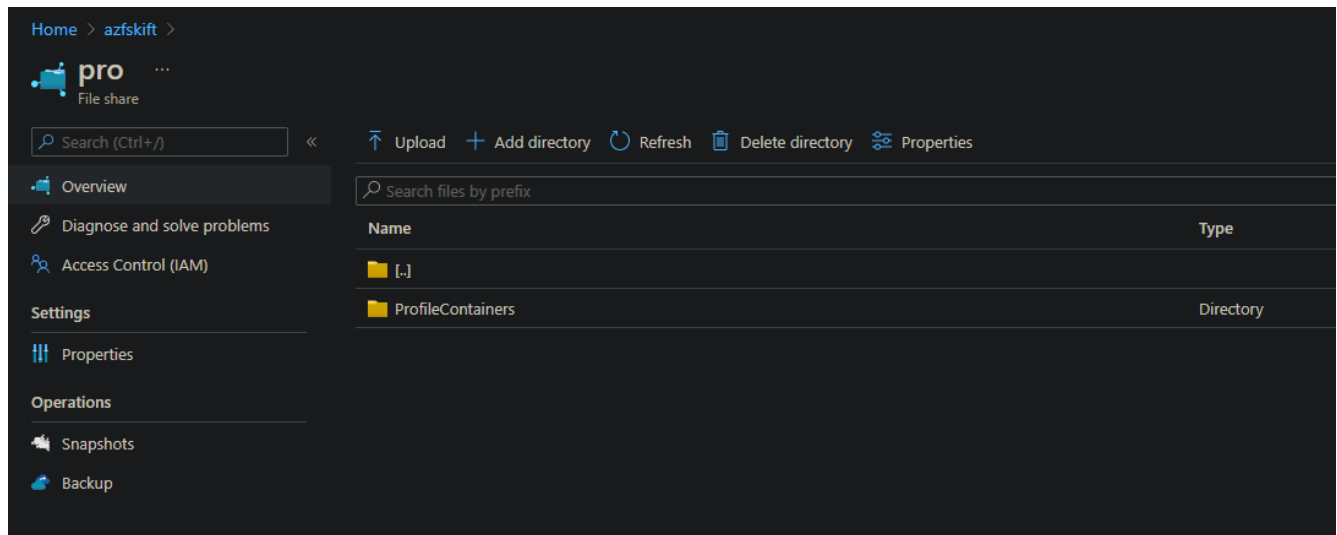
Discard

Create the directories

1. Create a directory in each share (data, home, pro) using the company code as the name (In this example, the company code is “kift”)

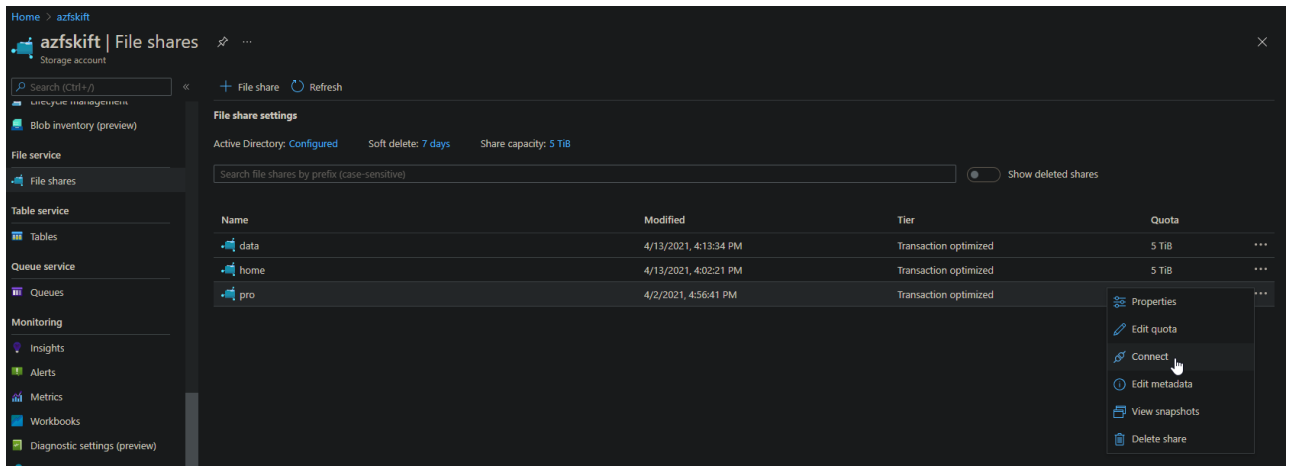


2. In the <company code> directory of the pro share, create a “ProfileContainers” directory



Set the NTFS Permissions


1. Connect to the shares
 - a. Navigate to the share under the storage account in the Azure portal, click the three dots, then click Connect



- b. Choose Active Directory for Authentication method and click the Copy to clipboard icon in the lower right corner of the code

Connect

pro

 'Secure transfer required' is enabled on the storage account. SMB clients connecting to this share must support SMB protocol version 3 or higher in order to handle the encryption requirement. [Click here to learn more.](#)

WindowsLinuxmacOS

To connect to this Azure file share from Windows, choose from the following authentication methods and run the PowerShell commands from a normal (not elevated) PowerShell terminal:


Drive letter

Z

Authentication method


☒ Active Directory

☐ Storage account key

 Identity-based access is configured for this storage account. Ensure the account used with the following command has permissions to this share. [Learn more](#)

```
$connectTestResult = Test-NetConnection -ComputerName  
azfskift.file.core.windows.net -Port 445  
if ($connectTestResult.TcpTestSucceeded) {  
    # Mount the drive  
    New-PSDrive -Name Z -PSProvider FileSystem -Root  
    "\\azfskift.file.core.windows.net\pro" -Persist  
} else {
```

Copy to clipboard



This script will check to see if this storage account is accessible via TCP port 445, which is the port SMB uses. If port 445 is available, your Azure file share will be persistently mounted. Your organization or internet service provider (ISP) may block port 445, however you may use Azure [Point-to-Site \(P2S\) VPN](#), Azure [Site-to-Site \(S2S\) VPN](#), or [ExpressRoute](#) to tunnel SMB traffic to your Azure file share over a different port.

[Learn how to circumvent the port 445 problem \(VPN\)](#)

- Log in to the CWMGR1 server with an account that is a member of the Level3 Technicians group
- Run the copied code in PowerShell to map the drive
- Do the same for each share while choosing a different drive letter for each

2. Disable inheritance on the <company code> directories
3. System and the AD Group ClientDHPAccess should have Full Control to the <company code> directories
4. Domain Computers should have Full Control to the <company code> directory in the pro share as well as the ProfileContainers directory within
5. The <company code>-all users AD group should have List folder/read data permissions to the <company code> directories in the home and pro shares
6. The <company code>-all users AD group should have the below Special permissions for the directory in the data share

Principal: kift-all users (TRAININGKRISG\kift-all users) [Select a principal](#)

Type: Allow

Applies to: This folder, subfolders and files

Advanced permissions:

☐ Full control
☒ Traverse folder / execute file
☒ List folder / read data
☒ Read attributes
☒ Read extended attributes
☒ Create files / write data
☒ Create folders / append data

☒ Write attributes
☒ Write extended attributes
☒ Delete subfolders and files
☒ Delete
☒ Read permissions
☐ Change permissions
☐ Take ownership

☐ Only apply these permissions to objects and/or containers within this container

[Show basic permissions](#)

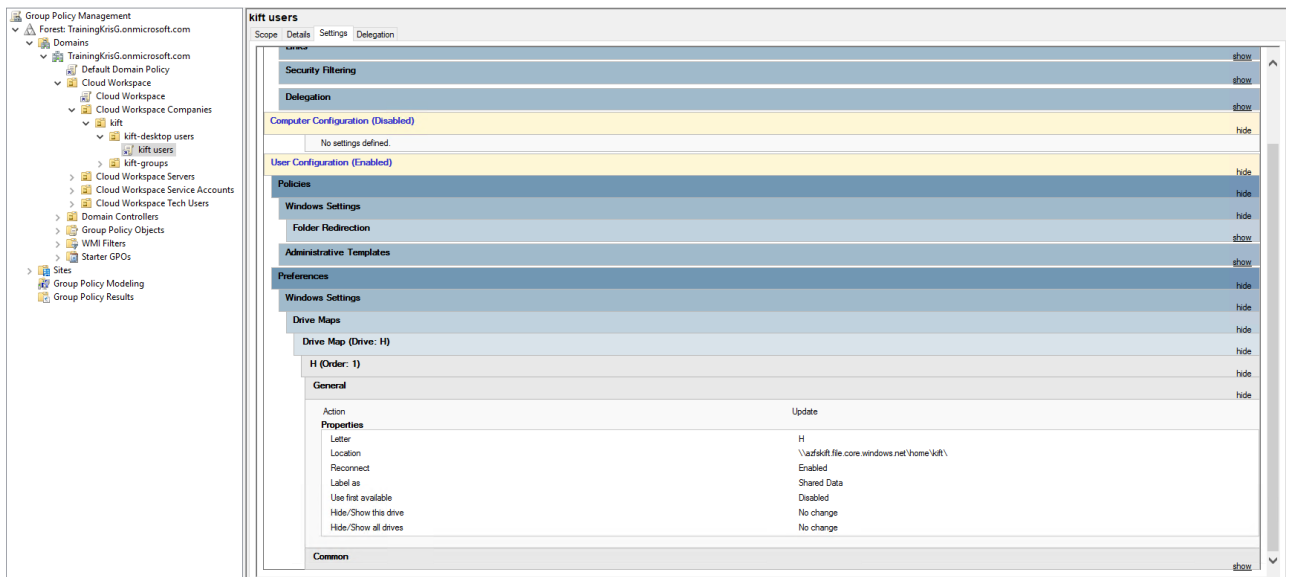
Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.

[Add a condition](#)

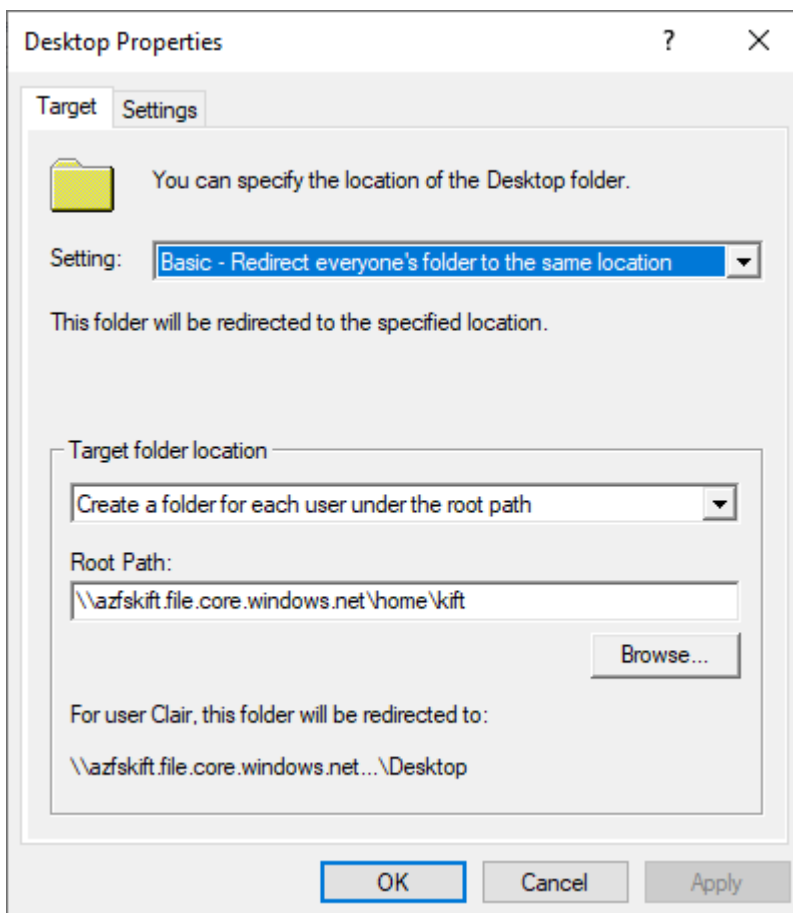
7. The <company code>-all users AD group should have the Modify permission on the ProfileContainers directory

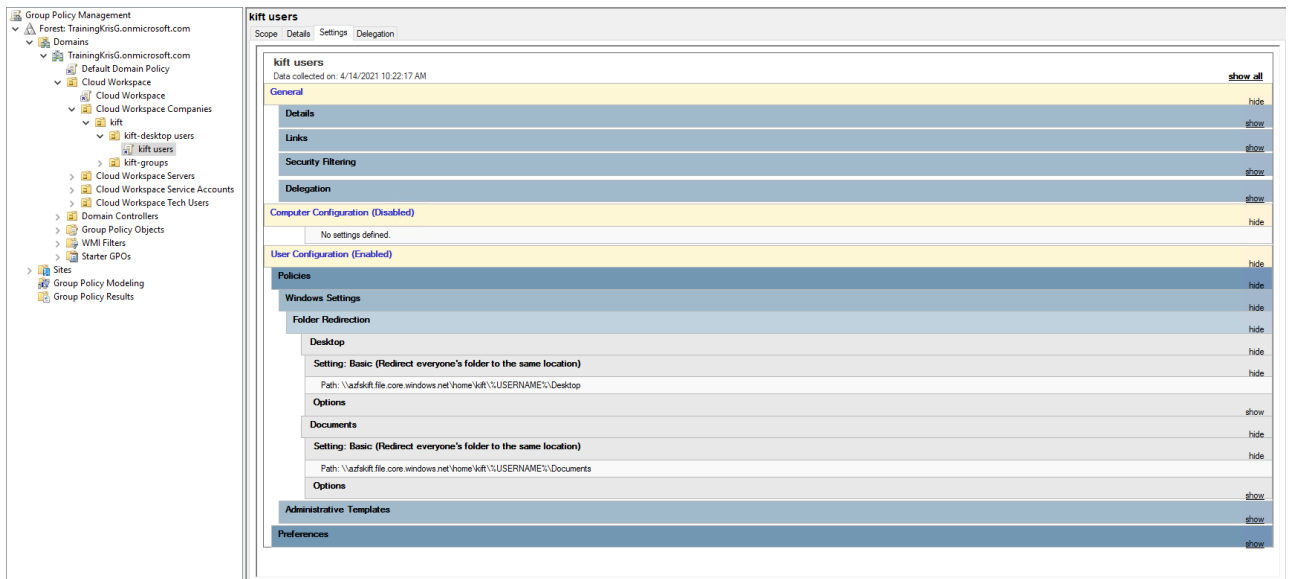
Update Group Policy Objects

1. Update the GPO <company code> users located under Cloud Workspace > Cloud Workspace Companies > <company code> > <company code>-desktop users
 - a. Change the Home drive mapping to point the new home share



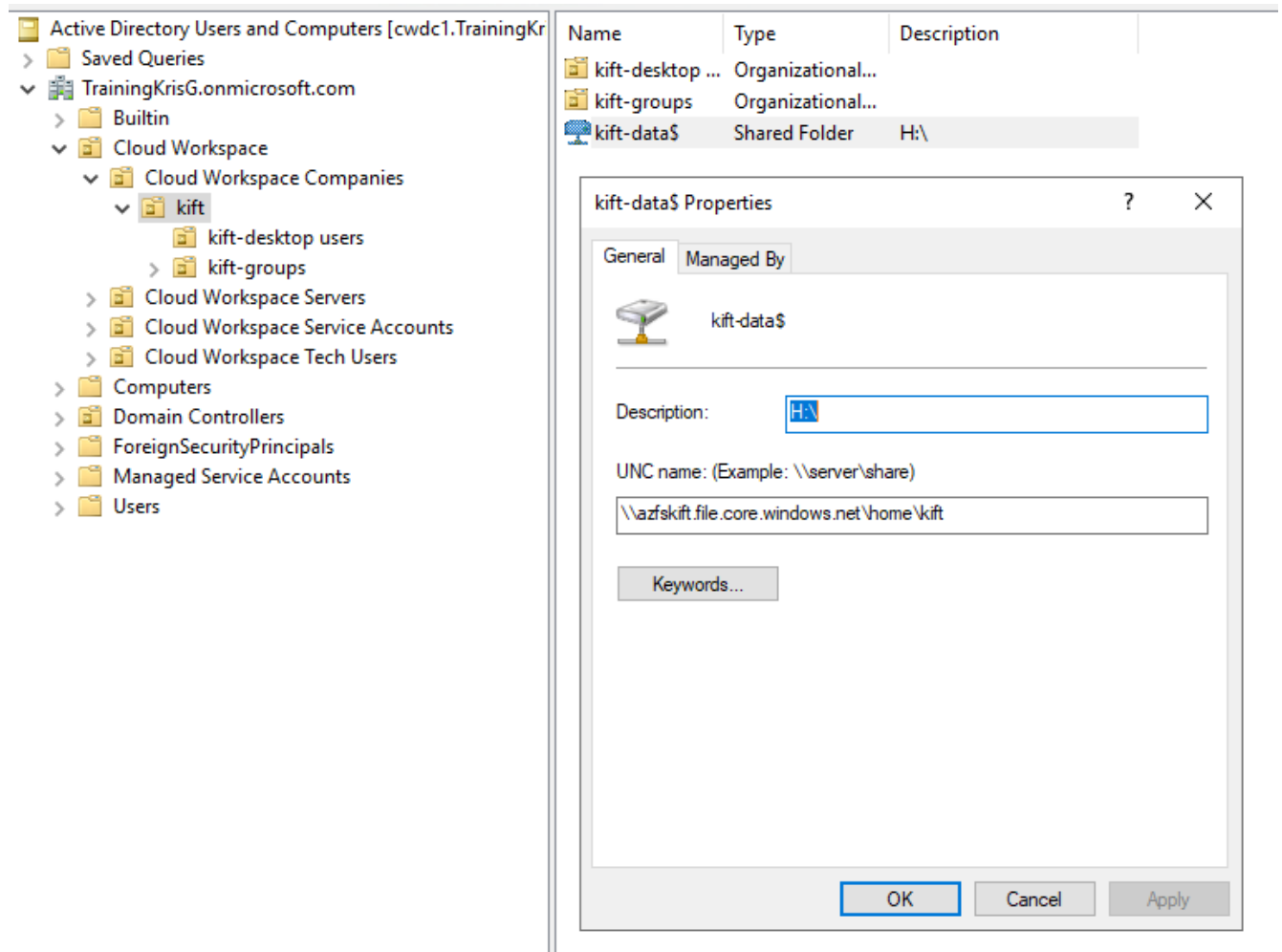
b. Change the Folder Redirection to point the home share for Desktop and Documents





Update the share in Active Directory Users and Computers

1. With classic or hybrid AD, the share in the company code OU needs to be updated to the new location



Update Data/Home/Pro paths in VDS

1. Log in to CWMGR1 with an account in the Level3 Technicians group and launch Command Center
2. In the Command drop down, select Change Data/Home/Pro Folders
3. Click the Load Data button, then be sure the proper company code is selected from the drop down
4. Enter the new path for the data, home, and pro locations
5. Uncheck the Is Windows Server box
6. Click the Execute Command button

Command Center 5.4.21091.1951

Operations Hypervisor

Command: Change Data/Home/Pro Folders Load Data

Company Code: KIFT

Resource Pool:

Data: \\azfskift.file.core.windows.net\data\kift ☐ Is Windows Server

Home: \\azfskift.file.core.windows.net\home\kift ☐ Is Windows Server

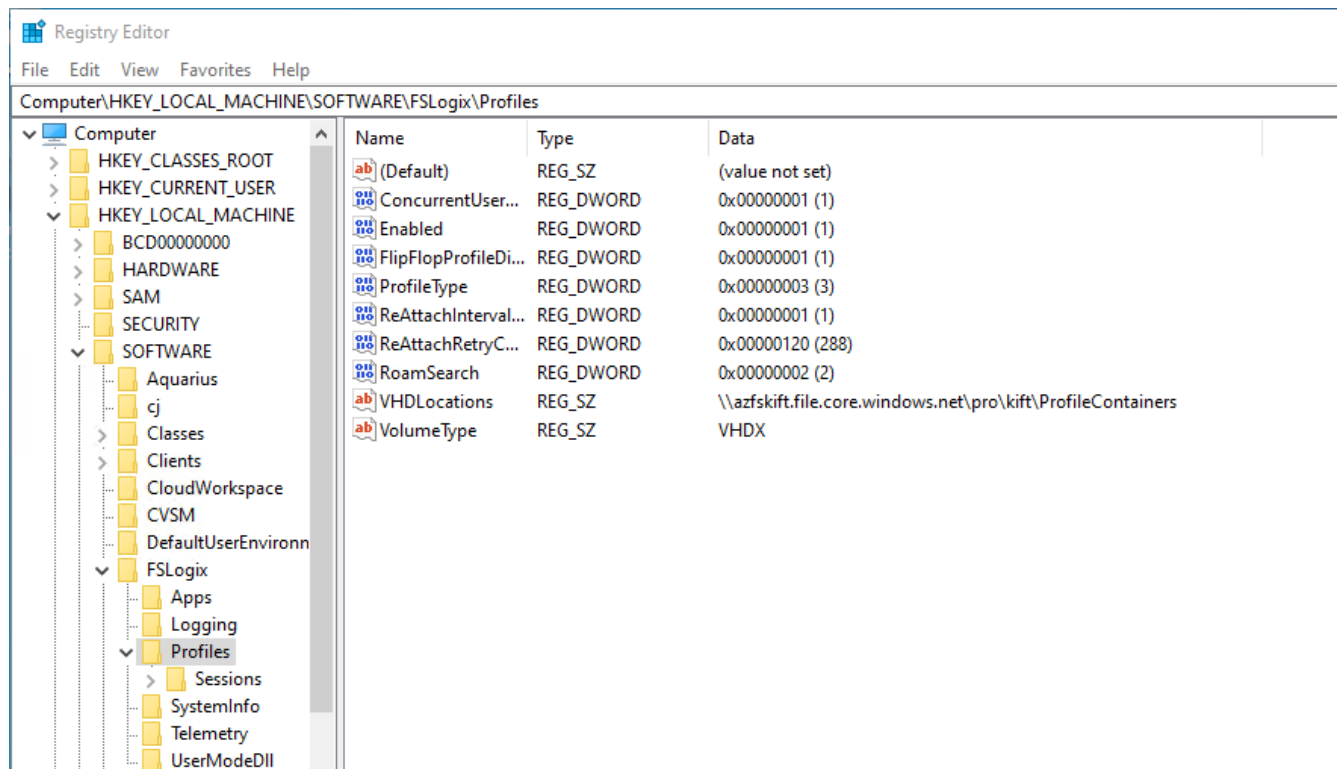
Pro: \\azfskift.file.core.windows.net\pro\kift ☐ Is Windows Server

Execute Command

View All Logs Clear Log

Update FSLogix profile paths

1. Open registry editor on the session hosts
2. Edit the VHDLocations entry at HKLM\SOFTWARE\FSLogix\Profiles to be the UNC path to the new ProfileContainers directory



Configure Backups

1. It is recommended to set up and configure a backup policy for the new shares
2. Create a new Recovery Services Vault in the same resource group
3. Navigate to the vault and select Backup under Getting Started
4. Choose Azure for where the workload is running and Azure file share for what you want to back up then click Backupp
5. Select the storage account used to create the shares
6. Add the shares to back up
7. Edit and Create a backup policy that fits your needs

Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.