Redirecting Storage Platform to Azure Files

Virtual Desktop Service

Kris Gillette

April 14, 2021

Table of Contents

Redirecting Storage Platform to Azure Files

Overview

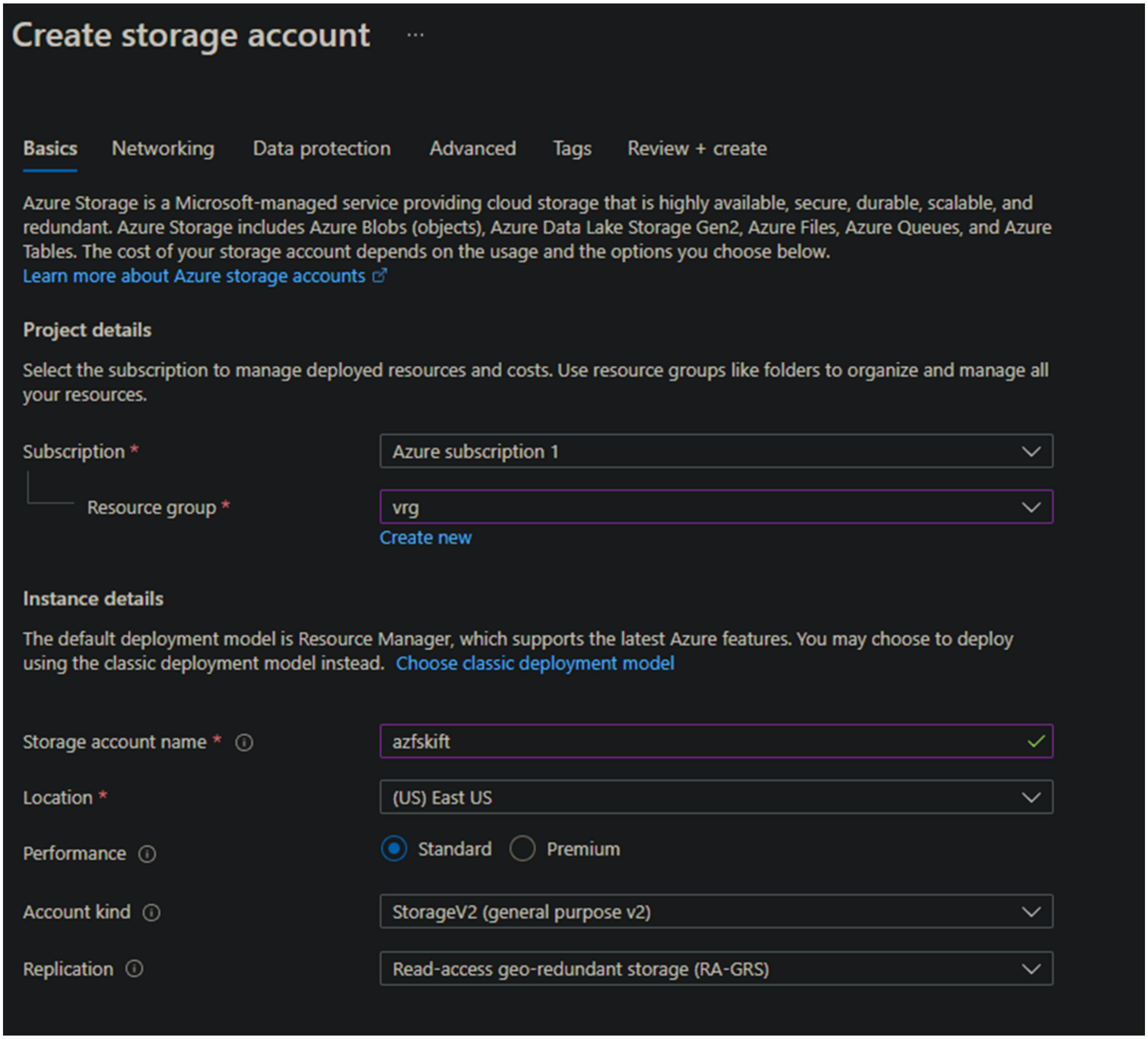
Virtual Desktop Service deployment technologies allow for a variety of storage options depending on the underlying infrastructure. This guide addresses how to make a change to using Azure Files post-deployment.

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 ···

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 * : Azure subscription 1

Resource group * : vrg

Create new

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 * : azfskift ✓

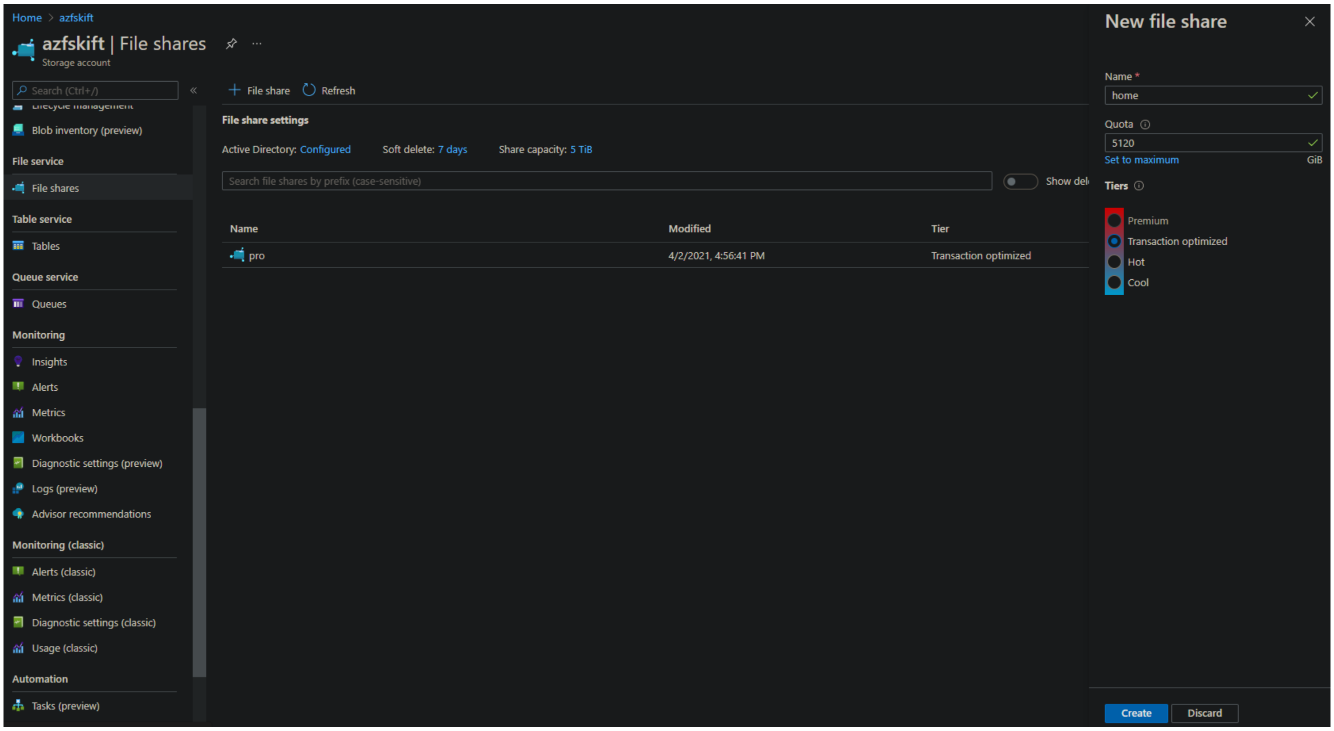
Location * : (US) East US

Performance : ● Standard ○ Premium

Account kind : StorageV2 (general purpose v2)

Replication : Read-access geo-redundant storage (RA-GRS)

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



File share settings

Active Directory: Configured   Soft delete: 7 days   Share capacity: 5 TiB

Name	Modified	Tier
pro	4/2/2021, 4:56:41 PM	Transaction optimized

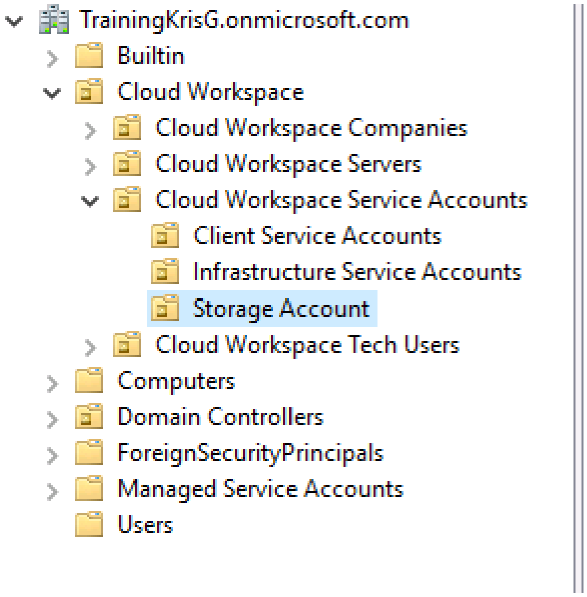
Name *: home

Quota: 5120 GiB

Tiers:
○ Premium
● Transaction optimized
○ Hot
○ Cool

Set Up Active Directory

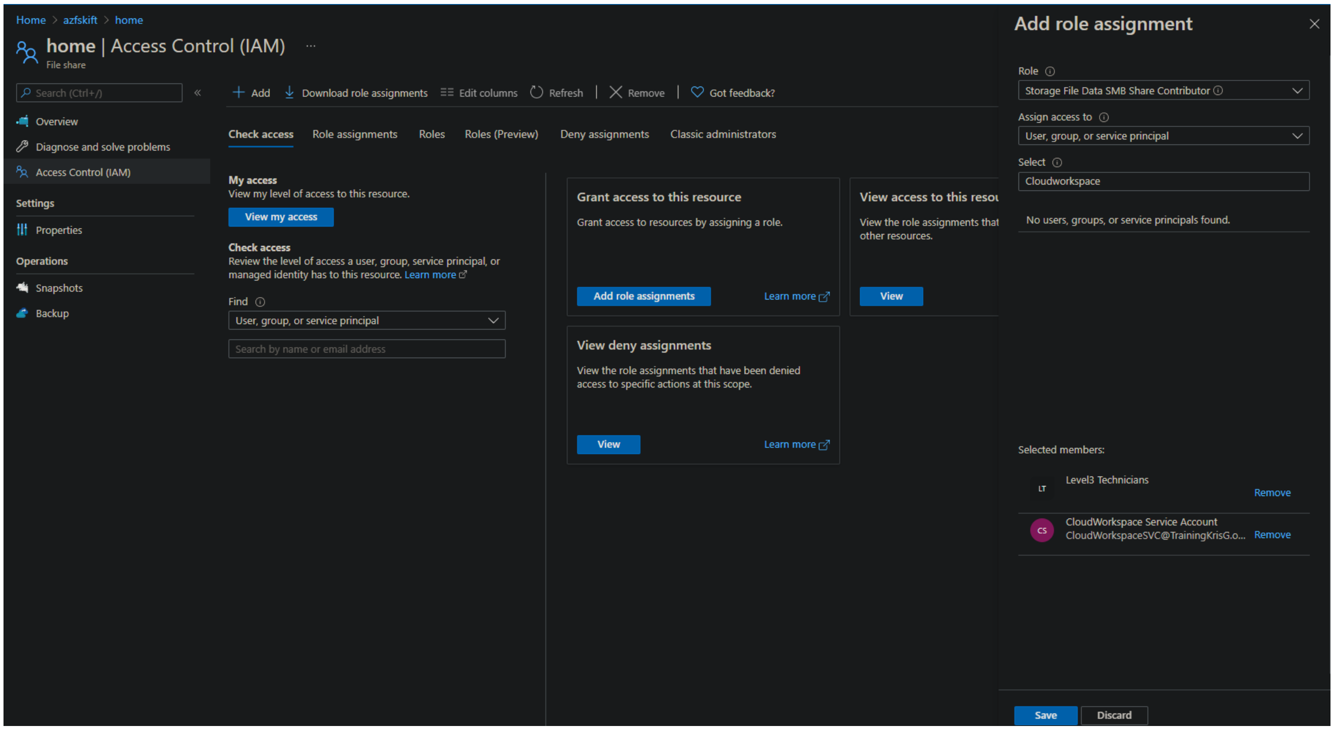
1. Create a new Organization Unit named “Storage Account” under the Cloud Workspace > Cloud Worksapce Service Accounts OU


TrainingKrisG.onmicrosoft.com
Builtin
Cloud Workspace
Cloud Workspace Companies
Cloud Workspace Servers
Cloud Workspace Service Accounts
Client Service Accounts
Infrastructure Service Accounts
Storage Account
Cloud Workspace Tech Users
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users

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. OraganizationalUnitDistinguishedName 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



Home > azfskift > home
home | Access Control (IAM) ...
File share
Search (Ctrl+/)
Overview
Diagnose and solve problems
Access Control (IAM)
Settings
Properties
Operations
Snapshots
Backup
+ Add
Download role assignments
Edit columns
Refresh
Remove
Got feedback?
Check access
Role assignments
Roles
Roles (Preview)
Deny assignments
Classic administrators
My access
View my level of access to this resource.
View my access
Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more
Find
User, group, or service principal
Search by name or email address
Grant access to this resource
Grant access to resources by assigning a role.
Add role assignments
Learn more
View access to this resou
View the role assignments that other resources.
View
View deny assignments
View the role assignments that have been denied access to specific actions at this scope.
View
Learn more
Add role assignment
Save
Discard

Role: Storage File Data SMB Share Contributor

Assign access to: User, group, or service principal

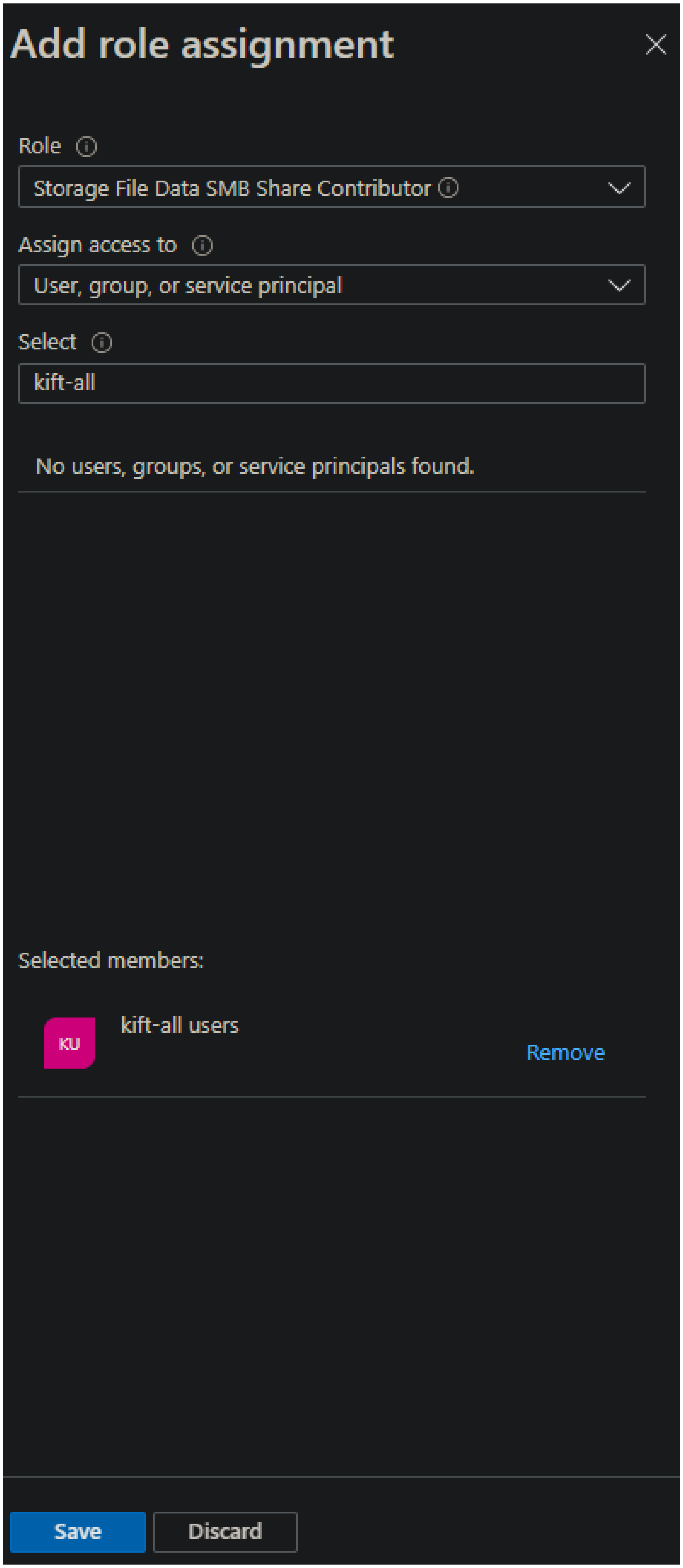
Select: Cloudworkspace

No users, groups, or service principals found.

Selected members:

- LT Level3 Technicians — Remove
- CS CloudWorkspace Service Account, CloudWorkspaceSVC@TrainingKrisG.o... — Remove

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

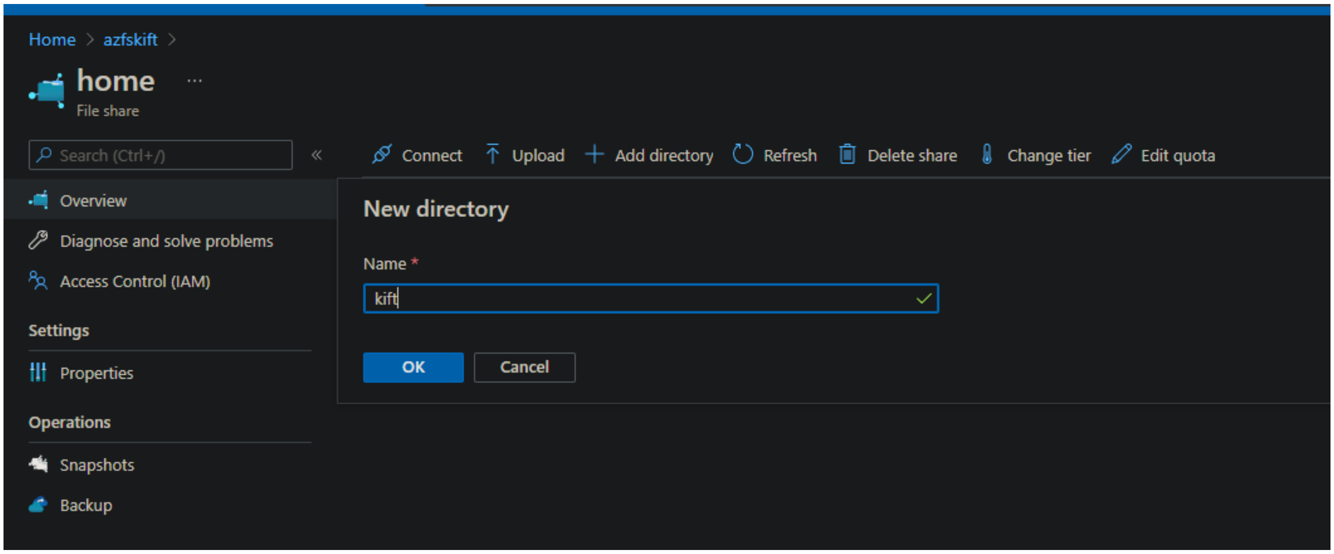
No users, groups, or service principals found.

Selected members:

KU kift-all users

Create the directories

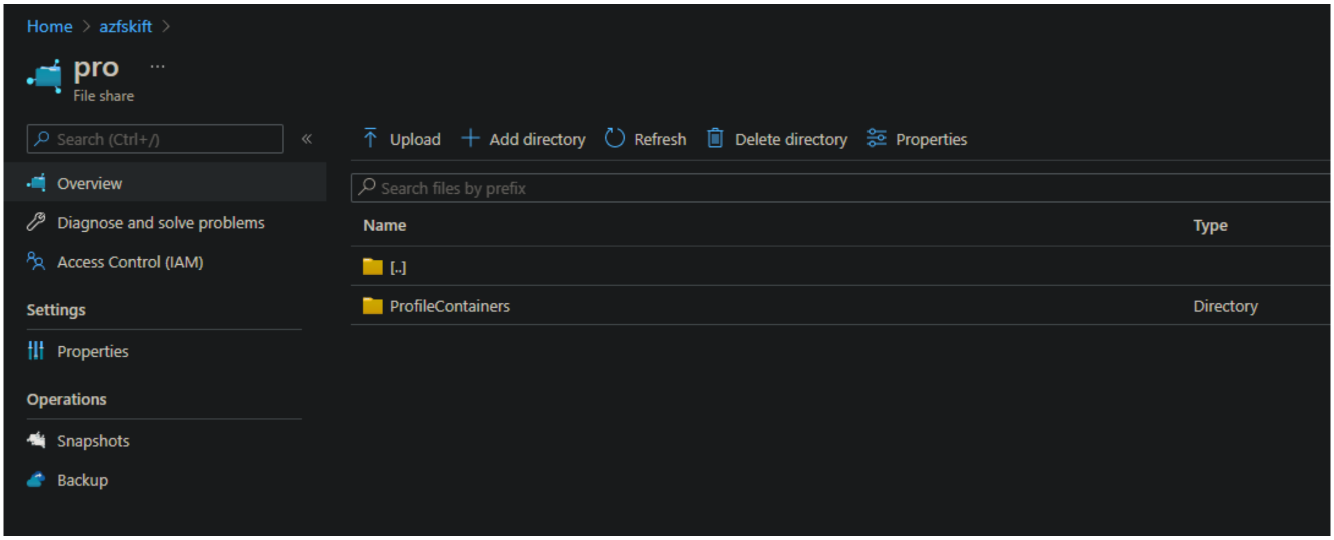
1. Create a directory in each share (data, home, pro) using the company code as the name (In this example, the company code is “kift”)



New directory

Name *: kift

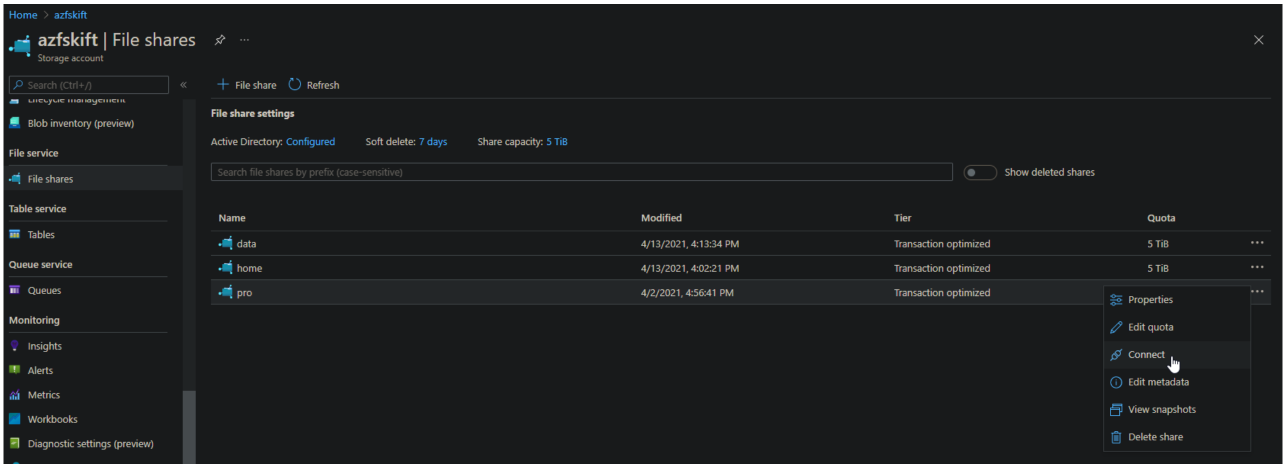
2. In the <company code> directory of the pro share, create a “ProfileContainers” directory



Name	Type
[..]	
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

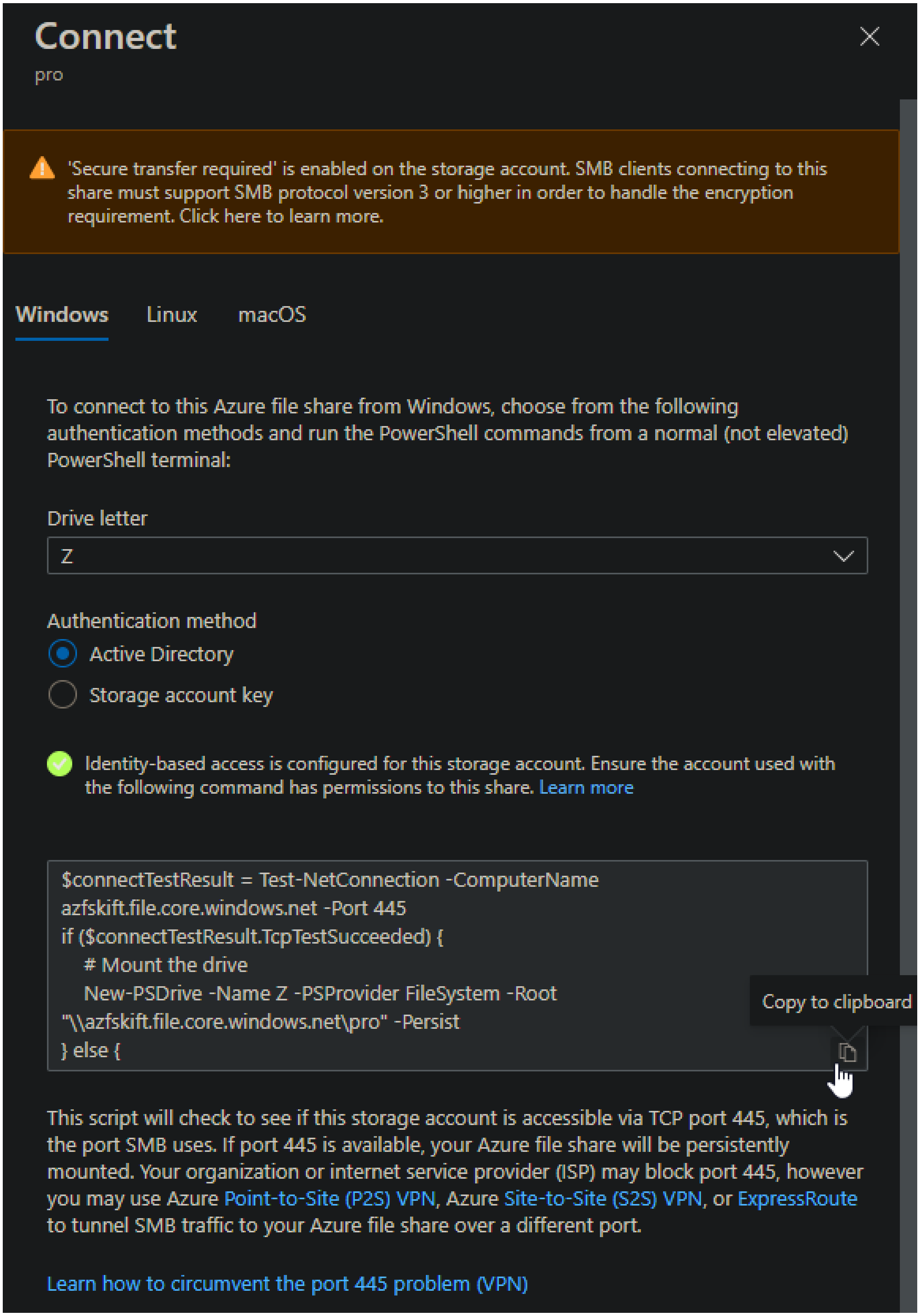


File share settings

Active Directory: Configured   Soft delete: 7 days   Share capacity: 5 TiB

Name	Modified	Tier	Quota
data	4/13/2021, 4:13:34 PM	Transaction optimized	5 TiB
home	4/13/2021, 4:02:21 PM	Transaction optimized	5 TiB
pro	4/2/2021, 4:56:41 PM	Transaction optimized	

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.

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 {
```

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.

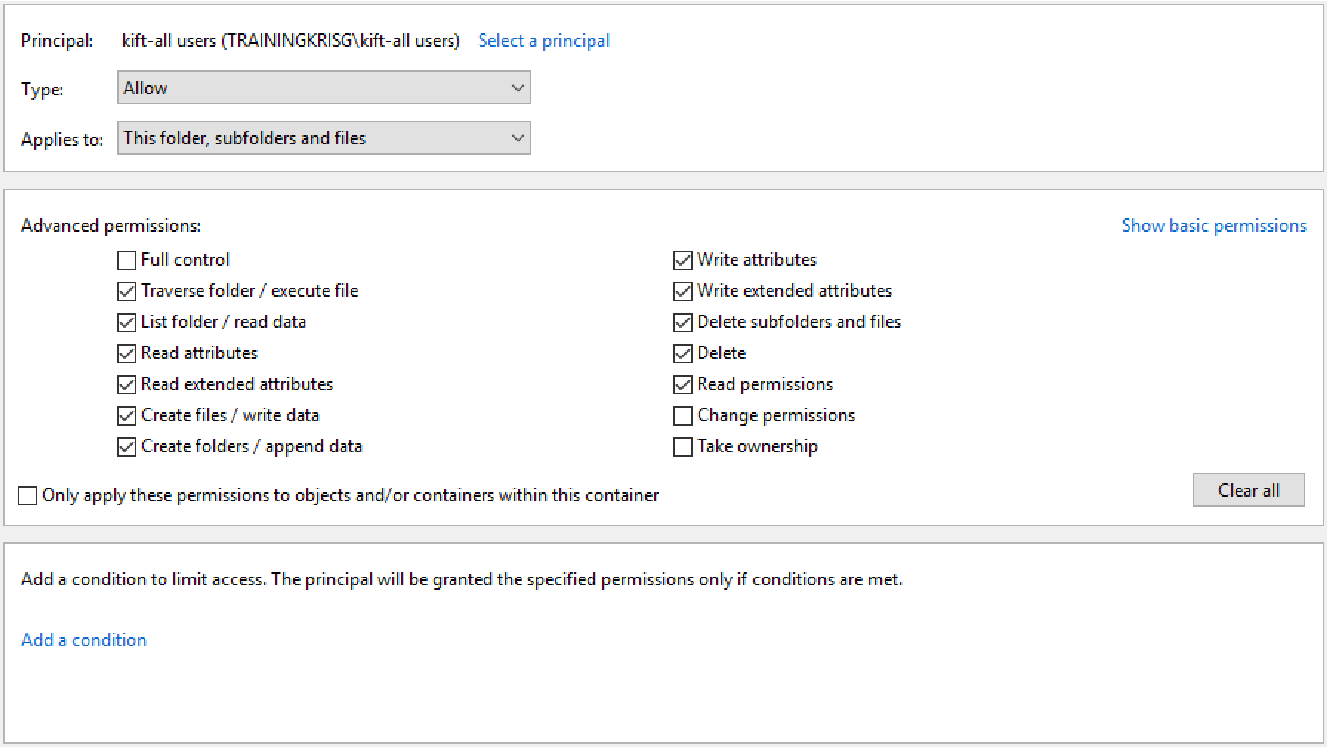
Learn how to circumvent the port 445 problem (VPN)

c. Log in to the CWMGR1 server with an account that is a member of the Level3 Technicians group

d. Run the copied code in PowerShell to map the drive

e. 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 permissons 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)

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

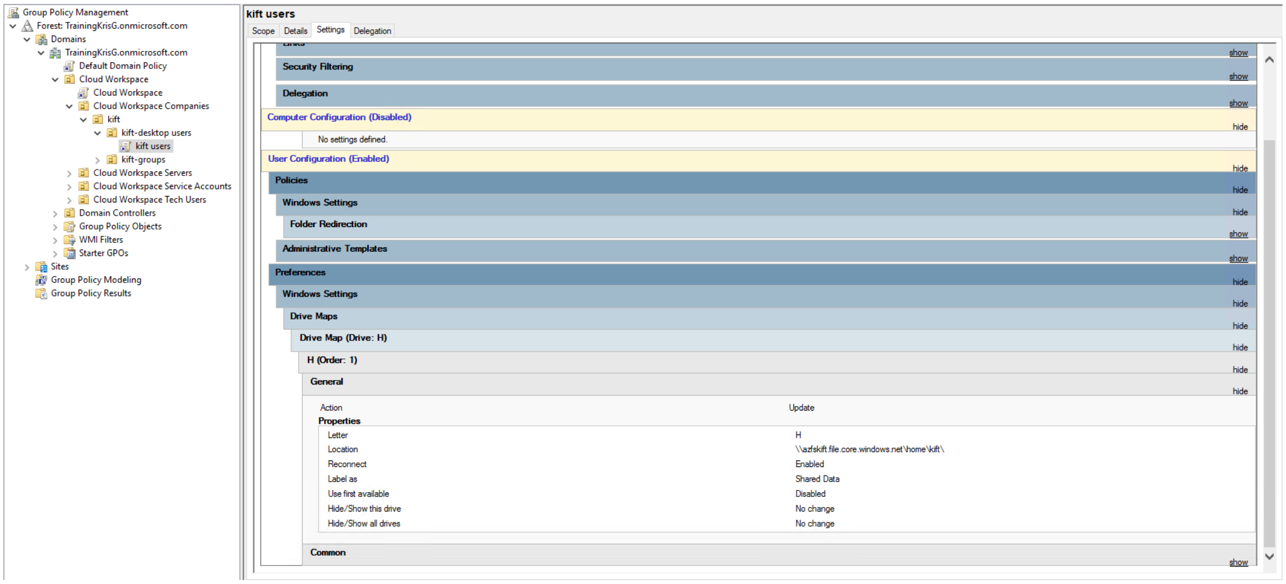
☐ Only apply these permissions to objects and/or containers within this container

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

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

Update Group Policy Objects

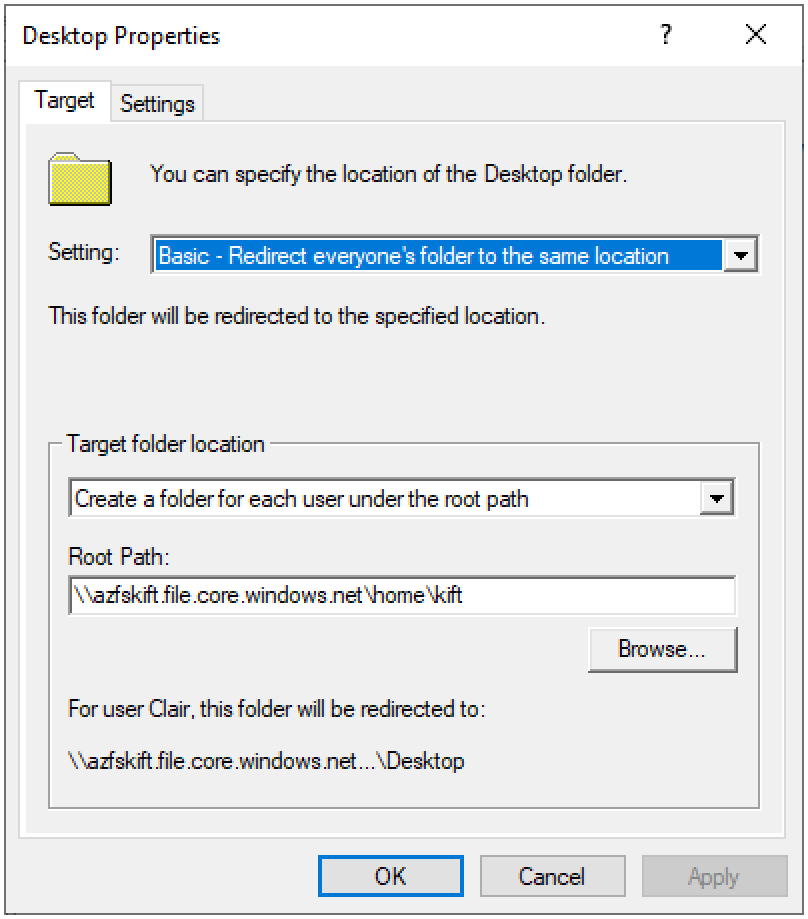
1. Update the GPO <company code> users located under Cloud Workspace > Cloud Workspace Companies > <company code> > <company code>-desktop users
   a. Change the Home drive mapping to point the new home share



No settings defined.

Action	Update
Properties	
Letter	H
Location	\\azfskift.file.core.windows.net\home\kift\
Reconnect	Enabled
Label as	Shared Data
Use first available	Disabled
Hide/Show this drive	No change
Hide/Show all drives	No change

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



You can specify the location of the Desktop folder.

Setting: Basic - Redirect everyone's folder to the same location

This folder will be redirected to the specified location.

Target folder location

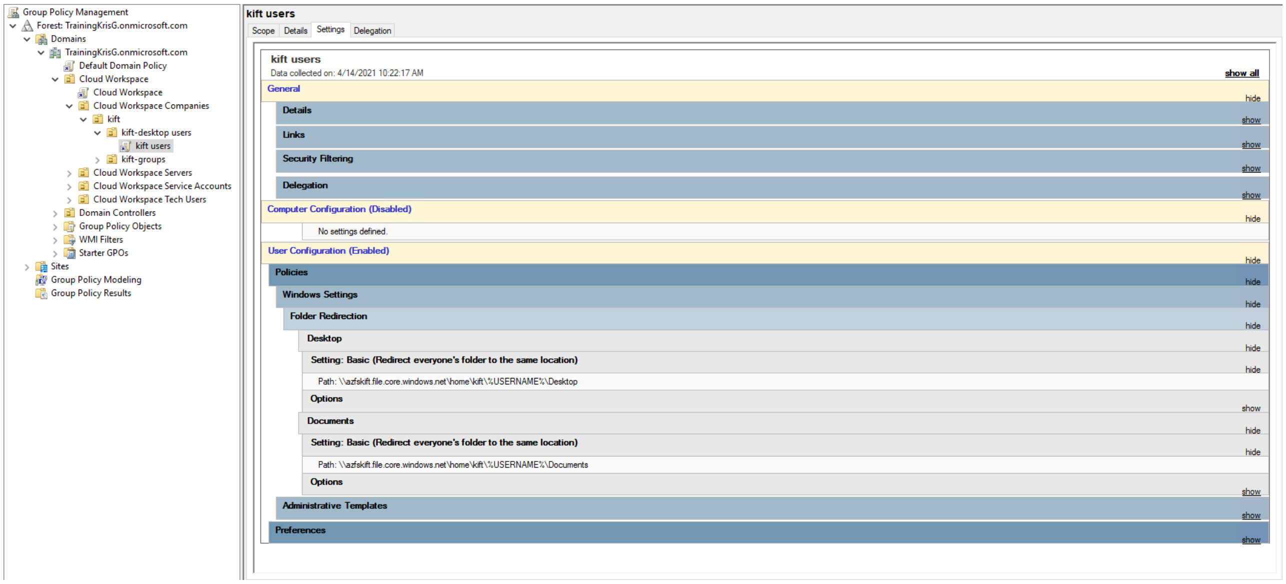
Create a folder for each user under the root path

Root Path:

\\azfskift.file.core.windows.net\home\kift

For user Clair, this folder will be redirected to:

\\azfskift.file.core.windows.net...\Desktop



kift users

Data collected on: 4/14/2021 10:22:17 AM

General
- Details
- Links
- Security Filtering
- Delegation

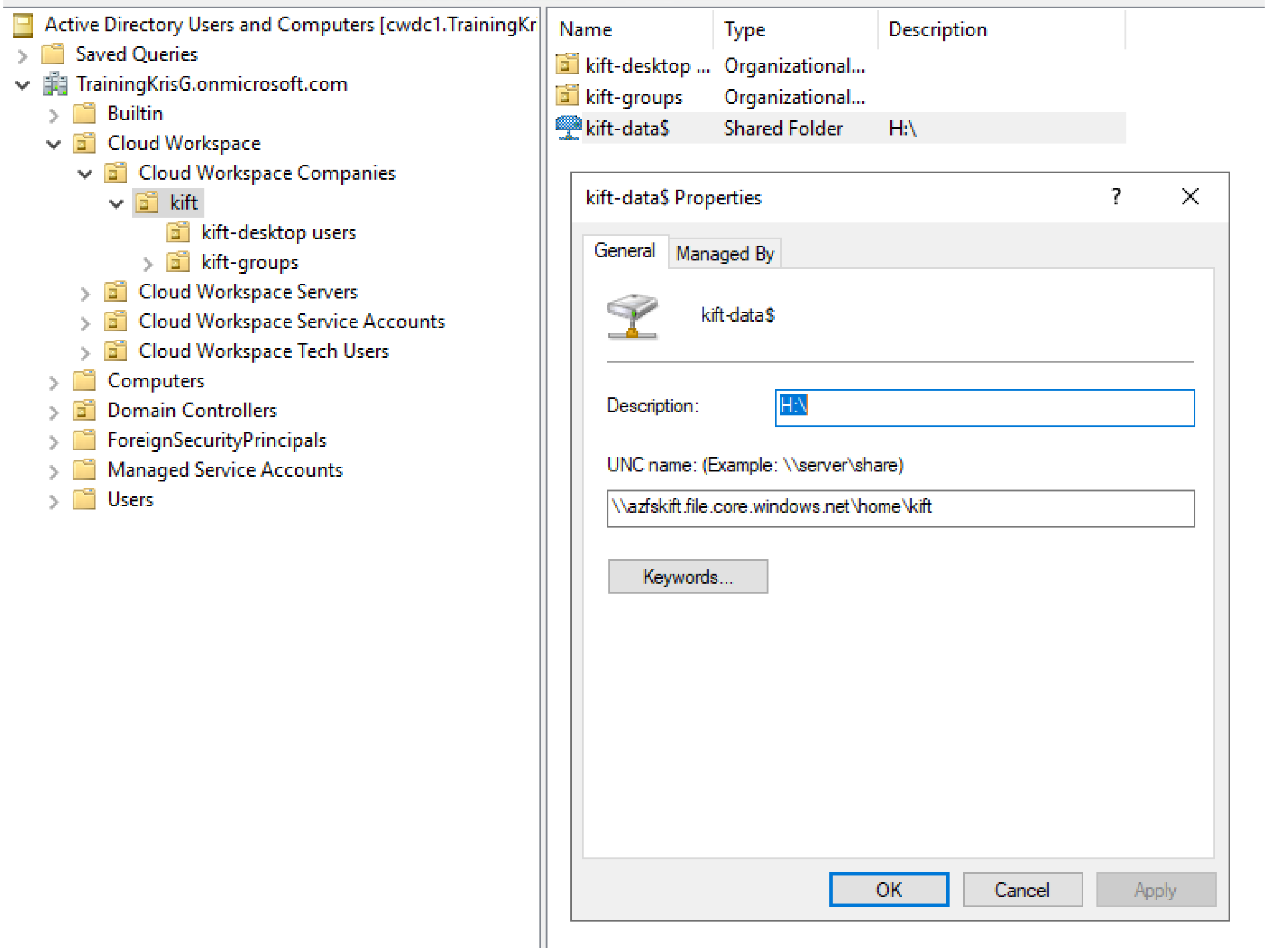
Computer Configuration (Disabled)

No settings defined.

User Configuration (Enabled)
- Policies
  - Windows Settings
    - Folder Redirection
      - Desktop
        - Setting: Basic (Redirect everyone's folder to the same location)
          - Path: \\azfskift.file.core.windows.net\home\kift\%USERNAME%\Desktop
        - Options
      - Documents
        - Setting: Basic (Redirect everyone's folder to the same location)
          - Path: \\azfskift.file.core.windows.net\home\kift\%USERNAME%\Documents
        - Options
  - Administrative Templates
- Preferences

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



Name	Type	Description
kift-desktop ...	Organizational...	
kift-groups	Organizational...	
kift-data$	Shared Folder	H:\

kift-data$

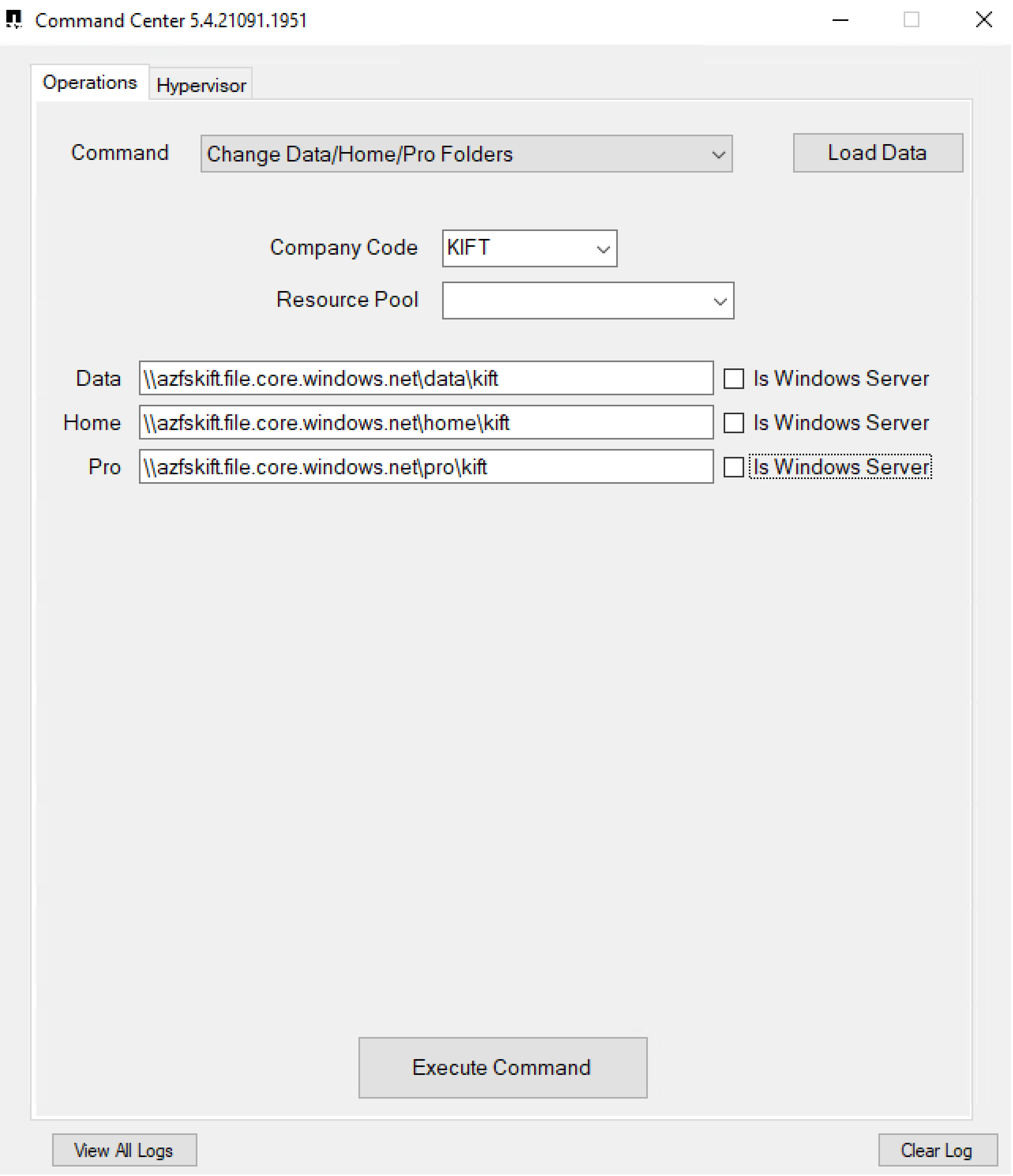
Description: H:\

UNC name: (Example: \\server\share)

\\azfskift.file.core.windows.net\home\kift

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 patsh 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

Command: Change Data/Home/Pro Folders

Company Code: KIFT

Resource Pool:

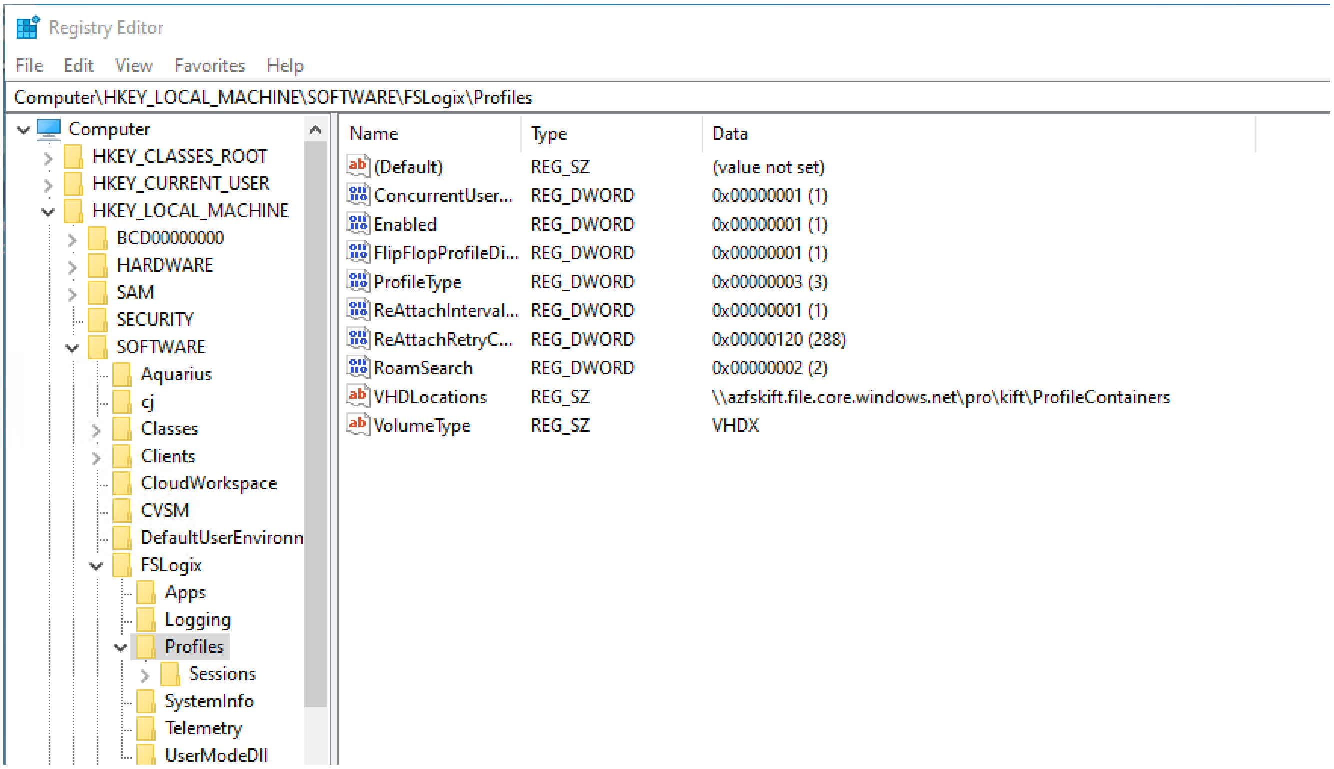
Data: \\azfskift.file.core.windows.net\data\kift ☐ Is Windows Server

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

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

Update FSLogix profile paths

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



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\FSLogix\Profiles

Name	Type	Data
(Default)	REG_SZ	(value not set)
ConcurrentUser...	REG_DWORD	0x00000001 (1)
Enabled	REG_DWORD	0x00000001 (1)
FlipFlopProfileDi...	REG_DWORD	0x00000001 (1)
ProfileType	REG_DWORD	0x00000003 (3)
ReAttachInterval...	REG_DWORD	0x00000001 (1)
ReAttachRetryC...	REG_DWORD	0x00000120 (288)
RoamSearch	REG_DWORD	0x00000002 (2)
VHDLocations	REG_SZ	\\azfskift.file.core.windows.net\pro\kift\ProfileContainers
VolumeType	REG_SZ	VHDX

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 Backukp
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

Trademark Information