



Windows Virtual Desktop Azure Active Directory Domain Services

Deployment Guide

Contents

Introduction.....	3
1 Pre-requirements.....	5
2 Preparing and deploying a VNet	6
2.1 Setting up DNS Servers for the VNET	9
3 Preparing and deploying AAD DS.....	10
4 Preparing WVD back-end resources.....	16
5 AAD DS Post deployment actions.....	24
6 Manage AAD DS.....	27
7 Image Management	37
7.1 Azure Managed Image + Shared Image Gallery	37
7.2 Azure Image Builder.....	46
8 Create a Service principal for WVD	47
9 Deploying WVD Session Hosts.....	49
9.1 VM Scale Sets + WVD	50
9.1.1 VM Scale Sets + WVD Architecture	50
9.1.2 Create Service account.....	52
9.1.3 Prepare Storage account	56
9.1.4 Prepare Log Analytics Workspace	62
9.1.5 Prepare Custom workflows	63
9.1.6 Deploy ARM Template	67
9.1.7 Verify VM Instance sizing.....	74
9.1.8 Deploy VM Instances	75
9.2 WVD Add session hosts wizard	76
10 Publish RemoteApps.....	81
11 Assign licenses.....	84
12 Access WVD	86
13 Deploy FSLogix Profile Containers	87
13.1 AAD DS - Deploying FSLogix Profile Containers on (PaaS) Azure File shares	88
13.2 Traditional AD DS - Deploying FSLogix Profile Containers on (PaaS) Azure File shares.....	101
13.3 Deploying FSLogix Profile Containers on (IaaS) File shares.....	115
13.4 !!DEPRECATED!! Deploying FSLogix Profile Containers in Blob Containers	121
14 Deploy Scaling Logic.....	125
14.1 Scripted scaling with VMs	125
14.2 Auto scaling with VM Scale Sets.....	126
14.3 Scripted Scaling with VM Scale Sets	128
15 Deploy Microsoft Teams	129

16 Deploy MSIX App Attach..... 130

Introduction

This document is intended to guide the reader through the process of creating a Windows Virtual Desktop (WVD) deployment backed by Azure Active Directory Domain Services (AAD DS), although traditional AD DS is supported and the deployment process is largely the same. Which is why this guide can still be referenced. This guide focuses on the WVD Spring Release, please contact us if you are looking for a classic deployment.

Please direct your questions or comments to: Microsoft@ingrammicro.nl

This document focuses on the practical deployment, however if you would like to learn more about WVD the sources below are available:

Microsoft Learn for WVD

<https://docs.microsoft.com/en-us/learn/paths/m365-wvd/>

Microsoft Mechanics WVD Playlist

https://www.youtube.com/playlist?list=PLXtHYVsvn_b8KAKw44YUpghpD6lg-EHev

Azure Academy WVD Playlist

<https://www.youtube.com/playlist?list=PL-V4YVm6AmwXGvQ46W8mHkpvm6S5IlitK>

AAD DS vs alternatives

Using a Windows Server Active Directory as Identity source (either on-prem through a VPN or an IaaS VM in Azure) rather than AAD DS is supported by WVD. Various pros and cons have been described in the figure below:

Option	Pros	Cons
Use Azure AD DS.	Great for test or isolated environments that do not need connectivity to on-premises resources. Azure AD will be your leading source for identities.	AD DS will always be running, resulting in a fixed charge per month.
Spin up a DC in your Azure subscription.	Can sync with on-premises DCs if VPN or ExpressRoute is configured. All familiar AD Group Policies can be used. Virtual machines can be paused or stopped when needed to reduce costs.	Adds additional management of a VM and Active Directory in Azure.
Use VPN or ExpressRoute and make sure you're on-premises DCs can be found in Azure.	No AD DS or Domain Controller required in Azure.	Latency could be increased adding delays during user authentication to VMs. This assumes you have an on-premises environment, not suitable for cloud only tests.

Figure 1 Azure AD DS vs alternatives

Another aspect to consider is that Seamless Single Sign-On (SSO) is not supported in AAD DS. This will result in the user being required to sign into Office 365 applications when starting them for the first time, in their respective WVD user session. For further details on AAD DS consult the source below:

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/faqs>

1 Pre-requirements

For optimal results achieved by following this deployment guide the following requirements have been defined:

- ✓ Access to a Microsoft tenant with an active Azure (CSP) subscription
- ✓ Global Administrator access to the Microsoft tenant
- ✓ A workstation with administrator access to PowerShell (a virtual machine can be created in Azure if an appropriate workstation is not available)
- ✓ Register the Windows Virtual Desktop provider: <https://docs.microsoft.com/en-us/learn/modules/m365-prepare-for-wvd/5-register-provider>
- ✓ Appropriate licenses for WVD users (details in chapter 9), to be fully compliant in production scenarios
- ✓ When using traditional AD DS configure both Hybrid Azure AD Join and Seamless Single Sign On (SSO) via [Configure Hybrid Azure AD Join](#) and [Configure Seamless Single Sign On \(SSO\)](#)

It is recommended to use a single administrator account throughout this guide to execute the Azure steps. The following roles/permissions are required for the selected administrator account:

- ✓ Global Administrator (of the selected Microsoft tenant to be used for the entire deployment)
- ✓ Contributor or Owner permissions on the selected Azure subscription (or on the Resource groups where WVD resources will be deployed to)

2 Preparing and deploying a VNet

The WVD Session Hosts are based on IaaS VM instances and will require a Virtual Network (VNet) in Azure to operate properly, which is why the first step is to prepare and deploy a VNet to be used in the WVD solution. The steps below will describe this process, names and references can be adjusted to meet your preferences.

- 1) Log in on the Azure Portal (for example: portal.azure.com) with your administrator account
- 2) Search for 'Virtual Networks' in the upper search bar and press the corresponding service

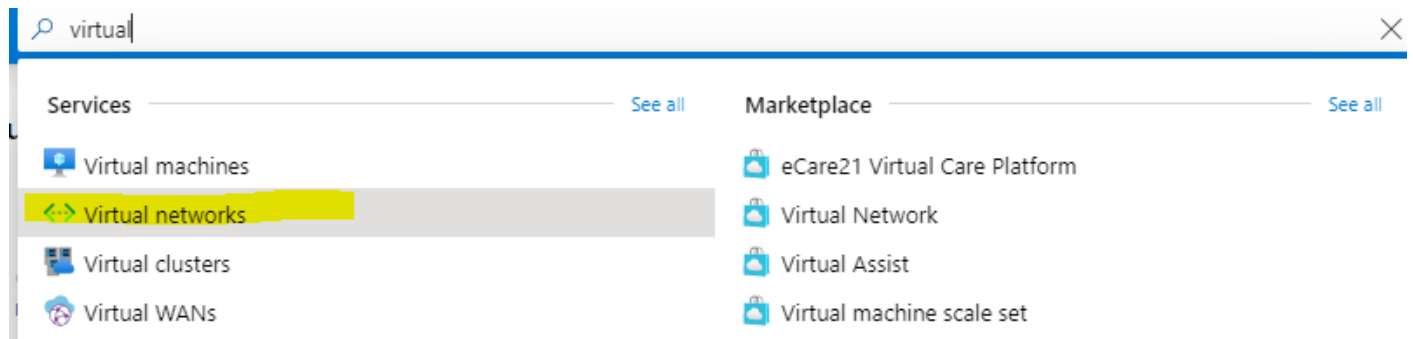


Figure 2 Search Virtual Network

- 3) Press **Add**

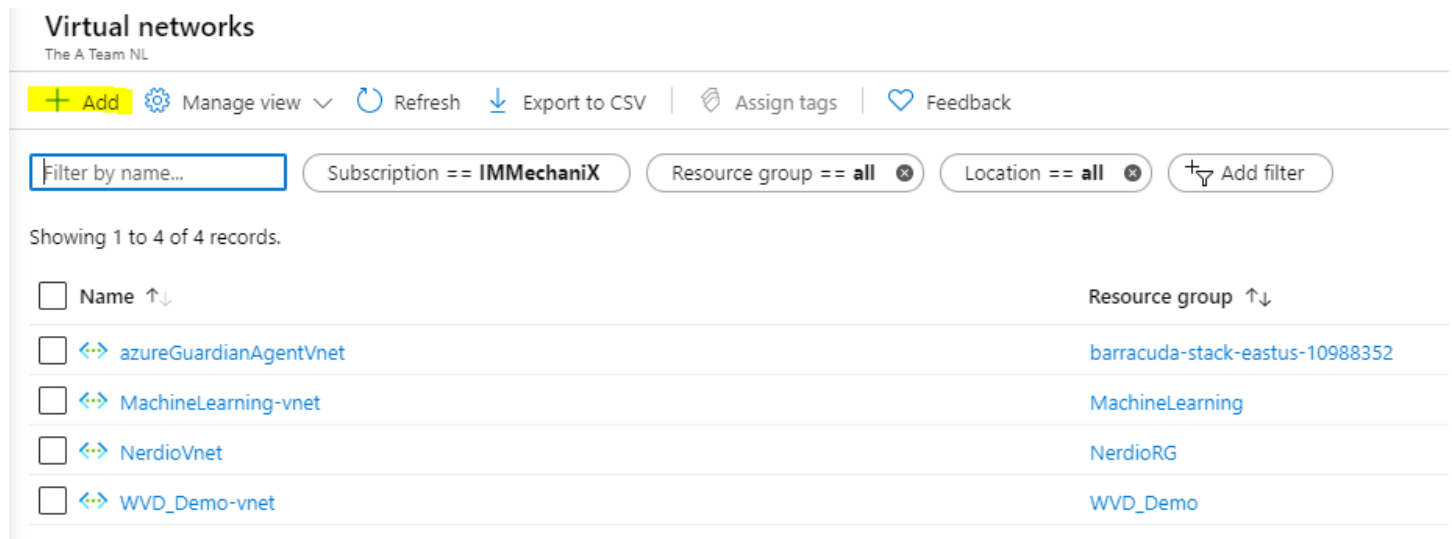


Figure 3 Add VNet

4) Fill in the 'Basics' page as depicted below and press **Next**

Basics IP Addresses Security Tags Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

Project details

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Instance details

Name *

Region *

Figure 4 VNet Basics

- 5) Fill in the 'IP Addresses' page as depicted on the next page:
- 6) Start by specifying the IPv4 address space

Optionally the box 'Add IPv6 address space' can be checked to provide a dual stack (both IPv4 and 6) VNet.

For more information regarding IPv6 on Azure consult the source below:

<https://aka.ms/ipv6vnetdoc>

- 7) Finally, create all the required/desired subnets via the **Add subnet** button. It is highly recommended to create a dedicated subnet for AAD DS to be deployed in (later).

Optionally you can select Azure (PaaS) Services to force communication with the subnet(s) through the Azure backbone network by configuring Service Endpoints. This has no disadvantages, although the limitation below should be considered.

Critical note: the subnet where AAD DS will be deployed in cannot be configured with any Service Endpoints.

For more information regarding Service Endpoints consult the source below:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview>

Basics IP Addresses Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

192.168.0.0/16 ✓ 🗑️

Add IPv6 address space ⓘ

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

+ Add subnet 🗑️ Remove subnet

<input type="checkbox"/> Subnet name	Subnet address range
<input type="checkbox"/> GatewaySubnet	192.168.0.0/24
<input type="checkbox"/> SUBNET-01-PL	192.168.1.0/24
<input type="checkbox"/> SUBNET-02-BL	192.168.2.0/24
<input type="checkbox"/> SUBNET-03-IL	192.168.3.0/24
<input type="checkbox"/> SUBNET-04-DL	192.168.4.0/24

Figure 5 VNet IP Addresses

- 8) Press **Review + Create**
- 9) Finally, press **Create**

The VNet and subnets will be created, verify successful creation by browsing to 'Virtual Networks' as done at step 2. Confirm that your VNet is in the list and contains the desired subnets.

2.1 Setting up DNS Servers for the VNET

The remaining steps in this chapter must be skipped if you will be deploying Azure AD DS, as DNS setup for AAD DS will be covered later in the guide. If you are using traditional/IaaS AD DS (Domain controller on a VM) you will need to manually set your DNS servers on the VNet (by following the steps below). This will allow for VMs created in this VNet to automatically contain the desired DNS settings.

- 10) Navigate to the previously created VNet
- 11) Press 'DNS servers'
- 12) Enter the IP address(es) of your Domain Controller(s)
- 13) Press **Save**

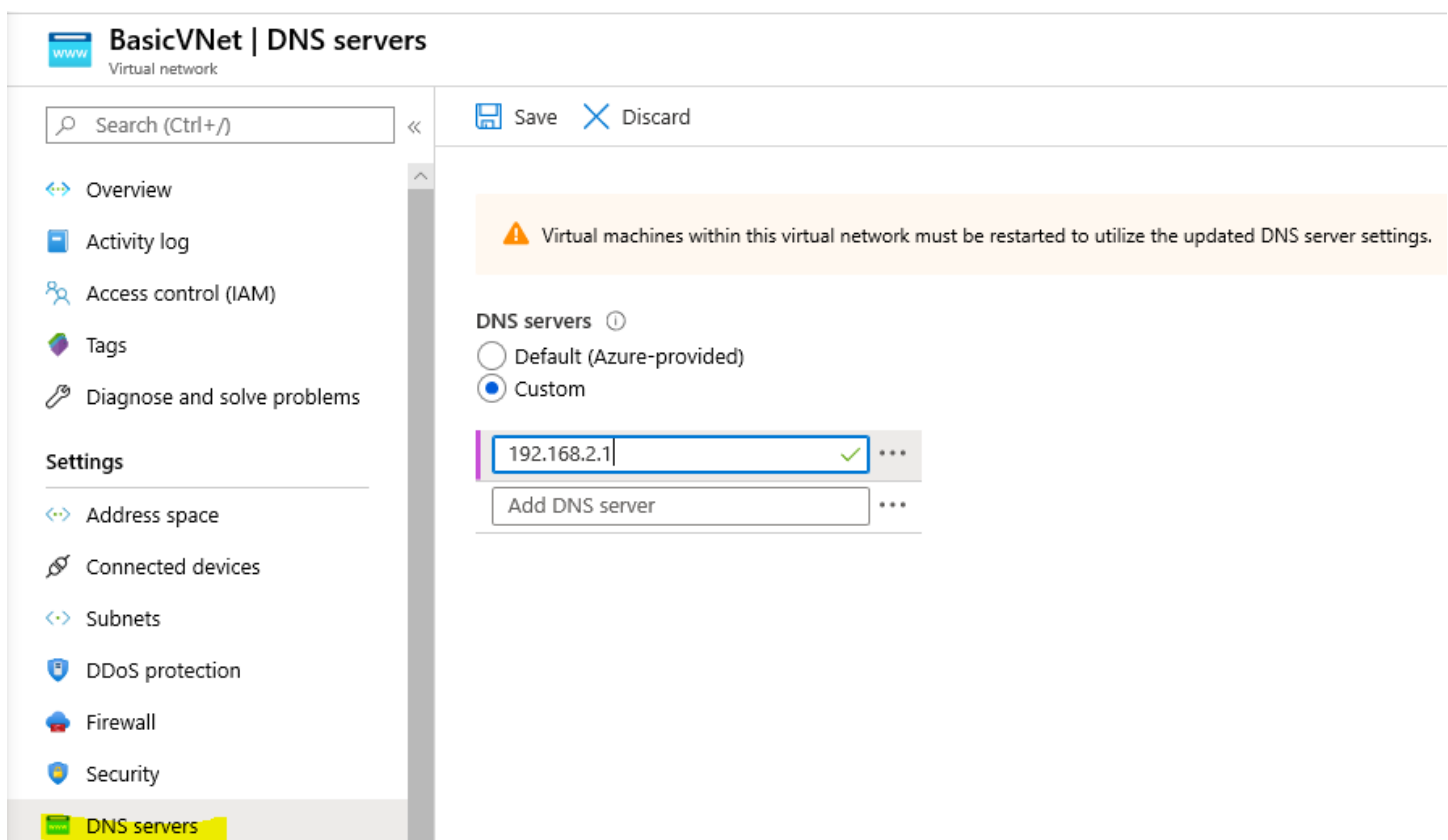


Figure 6 VNet - DNS servers

For more information on Azure Networking please consult our guide: 'Ingram Micro Azure Basic Networking Guide', or contact Microsoft@ingrammicro.nl if you have not received it yet.

3 Preparing and deploying AAD DS

Considering that the intended WVD deployment will be backed by Azure Active Directory Domain Services (AAD DS) the first major step is to deploy this solution within Azure.

Critical note: If you are using traditional AD DS (on a VM) this chapter can be skipped.

- 1) Log in on the Azure Portal (for example: portal.azure.com) with your administrator account
- 2) Search for 'Azure AD Domain Services' in the upper search bar and press the corresponding service

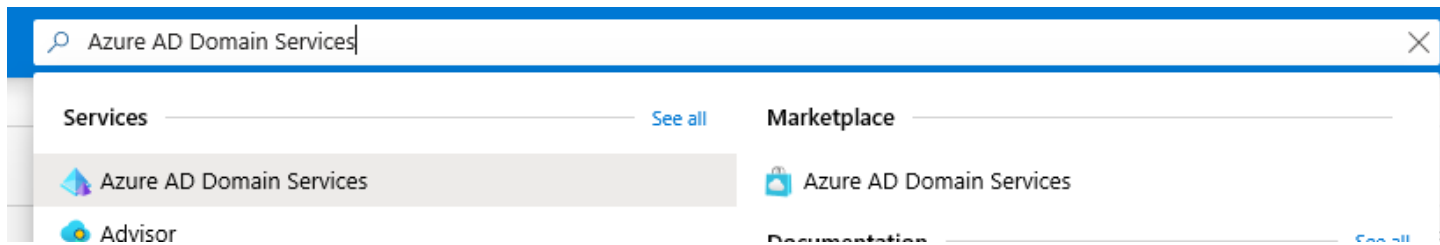


Figure 7 AAD DS

- 3) Press the **Create Azure AD Domain Services** button as depicted below

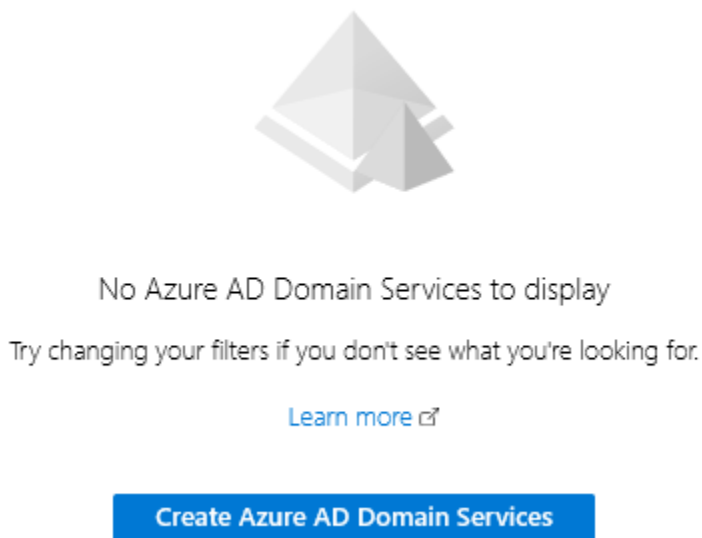


Figure 8 Create AAD DS

4) Fill in the Basics blade as depicted in the figure below. Keep the following points in mind:

DNS domain name: this will be the name of the domain as depicted in AD DS management tools, for the sake of simplicity it is recommended to use the primary custom domain name of Azure AD in this field. However, users can (later) be assigned other suffixes in their User Principal Name (UPN), if the suffix is a verified domain in Azure AD. Users will be synced (based on their UPN) from Azure AD to Azure AD DS.

SKU: Standard will suffice for medium environments it is advisable to consult the source below before deciding on a SKU: <https://azure.microsoft.com/en-us/pricing/details/active-directory-ds/>
 The SKU can be changed after the deployment of AAD DS.

Forest type: User type is recommended here as this creates a fully serviced Active Directory Domain. A Resource forest is only appropriate when identities must remain in an external (on-premises) domain but the technical objects in a domain must be hosted in Azure AD DS. This will allow identity sourcing and authentication to occur in the external (on-premises) AD DS, while technical resources (for example: a pilot for testing an application in the cloud) are hosted in Azure AD DS.

Project details

When choosing the basic information needed for Azure AD Domain Services, keep in mind that the subscription, resource group, DNS domain name, and location cannot be changed after creation.

Subscription *

Resource group * [Create new](#)

[Help me choose the subscription and resource group](#)

DNS domain name *

[Help me choose the DNS name](#)

Region *

SKU *

[Help me choose a SKU](#)

Forest type * User Resource (preview)

Figure 9 AAD DS Basics

5) Finally, press **Next**

6) Fill in the Networking blade, refer to the VNet created previously

Basics * Networking * Administration Synchronization Review + create


Azure AD Domain Services uses a dedicated subnet within a virtual network to hold all of its resources. If using an existing network, ensure that the network configuration does not block the ports required for Azure AD Domain Services to run. [Learn more](#)

Virtual network * ⓘ ▼
[Create new](#)

[Help me choose the virtual network and address](#)

Subnet * ⓘ ▼
[Manage](#)


[Help me choose the subnet and NSG](#)

 You have chosen a subnet which associates with an existing network security group. Review the guidelines for configuring NSGs to ensure you do not block Microsoft's ability to manage, patch, monitor and secure your managed domain.





[View NSG](#)

Figure 10 AAD DS Networking

- 7) If you receive the warning (Orange triangle) depicted above it means that the subnet you are trying to deploy AAD DS in already has a Network Security Group associated with it and the required security rules need to be configured manually. If you do not see the warning continue at step 14, if you do see the warning continue at step 8.
- 8) Press **View NSG**
- 9) Press **Inbound security rules**
- 10) Press **Add**
- 11) Create a rule that matches the one depicted below:

 **AzureActiveDirectoryDomainServices**
✕

NSG-03-IL

 Save
 Discard
 Basic
 Delete

Source * ⓘ

Service Tag
▼

Source service tag * ⓘ

AzureActiveDirectoryDomainServices
▼

Source port ranges * ⓘ

*

Destination * ⓘ

Any
▼

Destination port ranges * ⓘ

443,5986

Protocol *

Any
TCP
UDP
ICMP

Action *

Allow
Deny

Priority * ⓘ

100

Name

AzureActiveDirectoryDomainServices

Description

Synchronization with your Azure AD tenant and Management of your domain by Microsoft

Figure 11 AAD DS inbound security rule NSG

12) Finally, press **Add** to create the rule

For more information regarding AAD DS Network specifics consult the source below:

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/network-considerations>

13) Return to the AAD DS wizard by pressing the hyperlink as depicted below

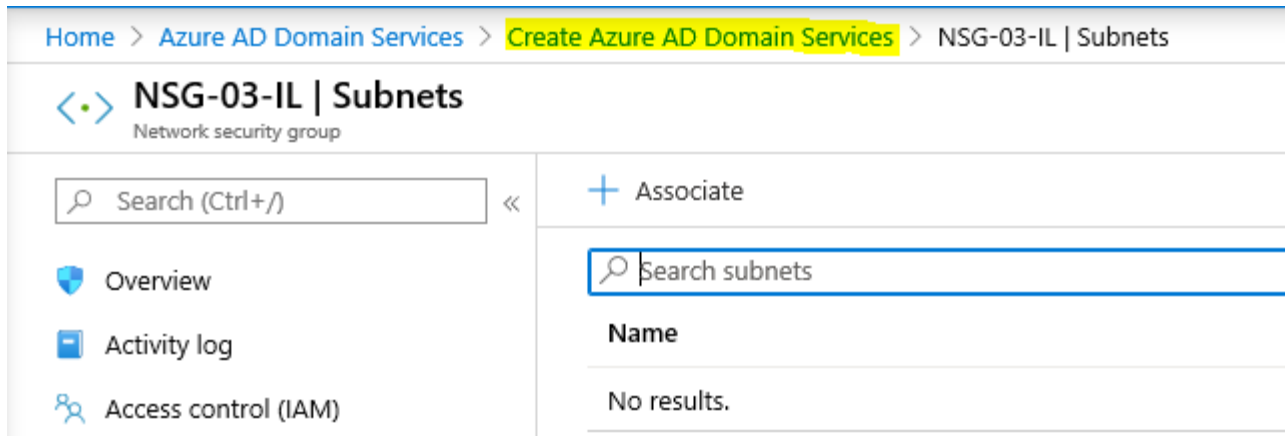


Figure 12 Return to AAD DS wizard

14) Press **Next**

15) Fill in the Administration blade as depicted below, optionally untick the 'Notifications' related boxes and/or add extra recipients

16) Press 'Manage group membership'

Basics * Networking * Administration Synchronization Review + create

Use these settings to specify which users should have administrative privileges and be notified of problems on your managed domain. [Learn more](#)

AAD DC Administrators ⓘ

Manage group membership

[Help me choose AAD DC Admins](#)

Notifications

These groups will be notified when you have an alert of warning or critical severity

- All Global Administrators of the Azure AD directory.
- Members of the AAD DC Administrators group.

Additional email recipients:

Figure 13 AAD DS Administration

- 17) Press **Add members** as depicted below to add administrators for your domain
- 18) Return to the AAD DS wizard by pressing the hyperlink as depicted below

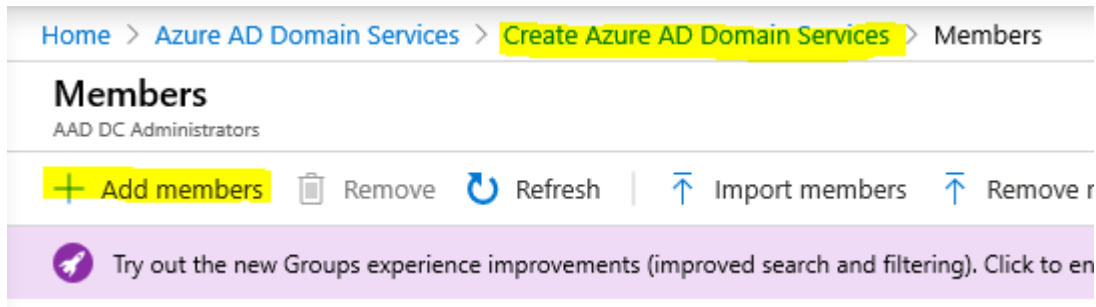


Figure 14 AAD DS add administrators

- 19) Press **Next**
- 20) Fill in the Synchronization blade as depicted below:

'All' will synchronize all Azure AD users in the tenant to the domain, while 'Scoped' will allow you to limit which users will be synchronized to Azure AD DS.

Basics * Networking * Administration Synchronization Review + create

Azure AD Domain Services provides a one-way synchronization from Azure Active Directory to the managed domain. In addition, only certain attributes are synchronized down to the managed domain, along with groups, group memberships, and passwords. [Learn more](#)

Synchronization type All Scoped

[Help me choose the synchronization type](#)

! Scoped synchronization can be modified with different group selections or converted to synchronize all users and groups. To change synchronization from "all" to "scoped", the managed domain needs to be deleted and re-created. [More information](#)

Figure 15 AAD DS Synchronization

- 21) Press **Next**
- 22) Verify the configuration and press **Create**

The deployment of the AAD DS managed domain is likely to take up to 60 minutes, which is why it is advised to continue with the rest of the guide while the deployment is running.

4 Preparing WVD back-end resources

Windows Virtual Desktop requires several back-end resources which will be created in this chapter and are depicted in the figure below:

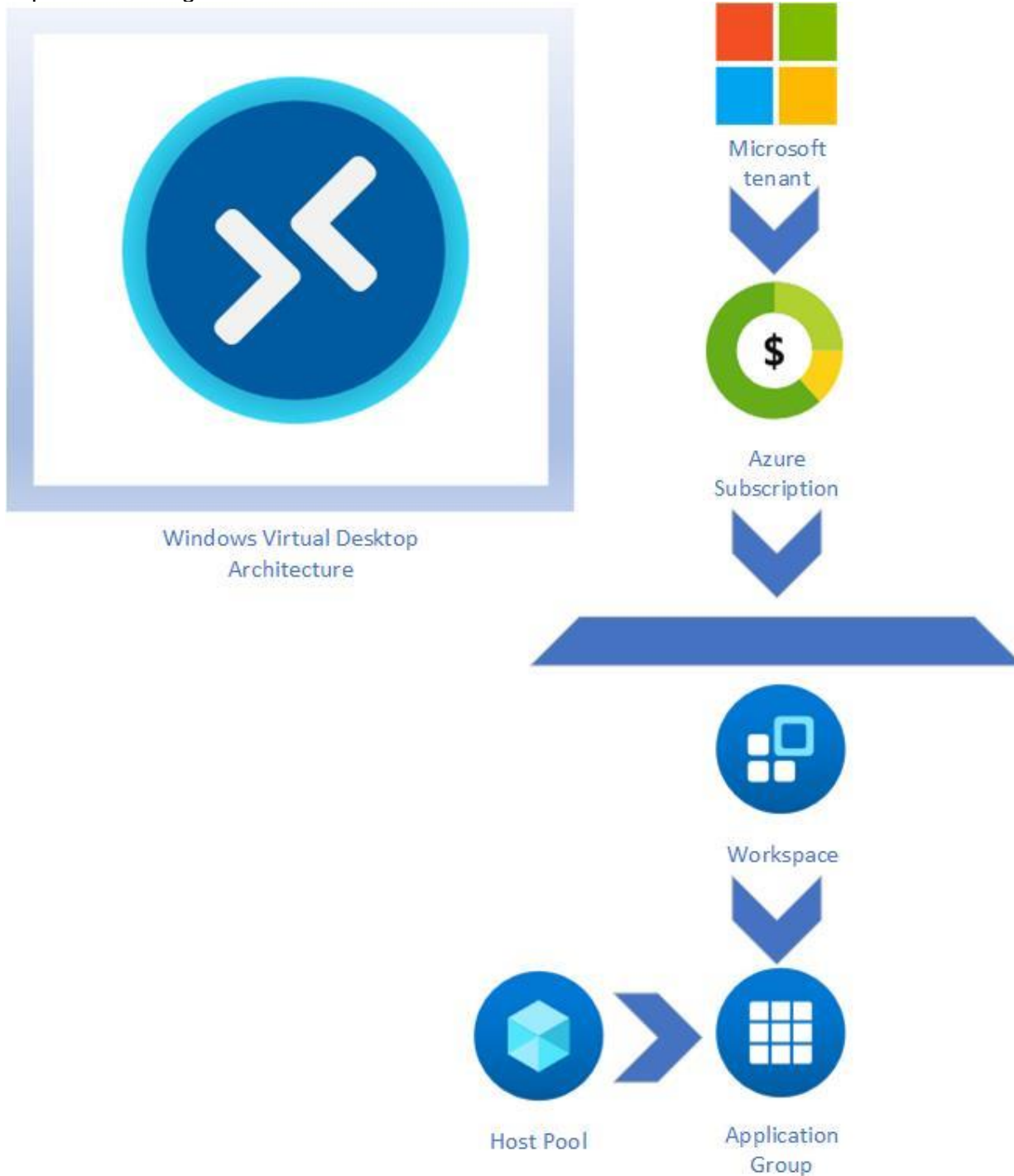


Figure 16 Windows Virtual Desktop Architecture

Microsoft tenant and Azure subscription: As mentioned in the pre-requirements, a Microsoft tenant and an active Azure subscription are required.

Workspace: A WVD Workspace is a logical container of the Host pool(s) and Application group(s). Although all three components are separate resources in Azure, a relationship between them is required (as depicted above) for WVD to operate.

Host pool: A WVD Host pool is effectively a collection of WVD session hosts, comparable to Remote Desktop Services (RDS) session hosts.

Application groups: An Application group is the entity which grants users permissions to Remote applications or complete virtual desktops. There are two types of Application groups: **Desktop** and **RemoteApp**. An Application group can only be created after a Host pool is created. After an Application group has been created it needs to be assigned to a Workspace.

[https://github.com/PeterSmallbone/WVD/wiki/WVD-\(Windows-Virtual-Desktop\)-Resources-and-Relationships](https://github.com/PeterSmallbone/WVD/wiki/WVD-(Windows-Virtual-Desktop)-Resources-and-Relationships)

Now that the WVD back-end resources have been explained the following steps can be used to create them.

- 1) Log in on the Azure Portal (for example: portal.azure.com) with your administrator account
- 2) Search for 'Windows Virtual Desktop' in the upper search bar and press the corresponding service

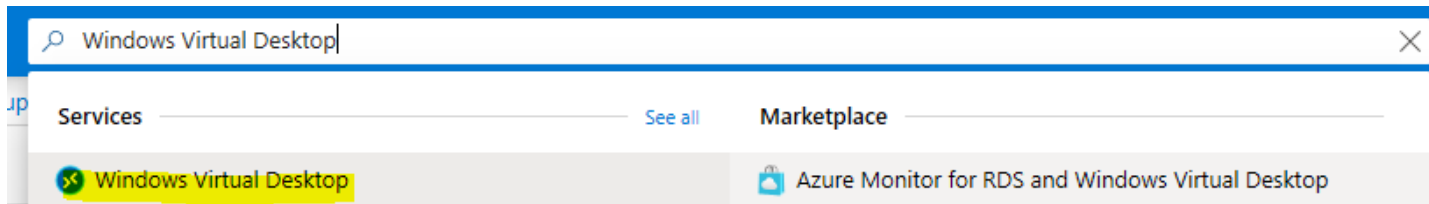


Figure 17 Windows Virtual Desktop

3) Press the **Workspaces** button as depicted below:

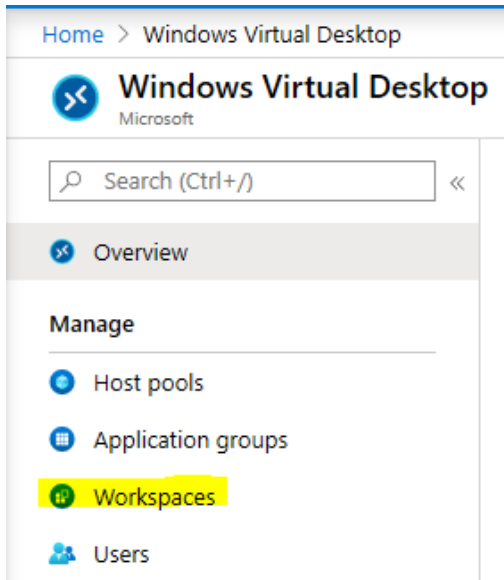


Figure 18 WVD Workspaces

4) Press **Add**

5) Fill in the 'Basics' blade as depicted below:

Keep in mind that **Friendly name** is the display name users will be confronted with.

Location (Europe scheduled for H1 2020) refers only to the meta data location for the back-end resources (Workspace, Host pool and Application group) and has no effect on performance. This is solely decided by the location of the WVD session hosts (will be deployed later) and the location of the end user's (physical) device.

Basics Application groups Tags Review + create

Work space is a logical grouping of application groups. Users will only be able to access an application group published to them if it is registered to a workspace. [Learn more](#)

Project details

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

Subscription * ⓘ	<input type="text" value="IMMechaniX"/>	▼
Resource group * ⓘ	<input type="text" value="(New) WVD-Backend"/>	▼

[Create new](#)

Instance details

Workspace name *	<input type="text" value="WVD-Ingram"/>	✓
Friendly name	<input type="text" value="Ingram Micro Virtual Workspace"/>	✓
Description	<input type="text" value="Ingram Micro Virtual Workspace based on WVD ARM (v2)"/>	✓
Location * ⓘ	<input type="text" value="(US) Central US"/>	▼

Figure 19 WVD Workspace Basics

- 6) Press **Review + Create**
- 7) Press **Create**

- 8) Return to 'Windows Virtual Desktop'
- 9) Press **Host pools** as depicted below:

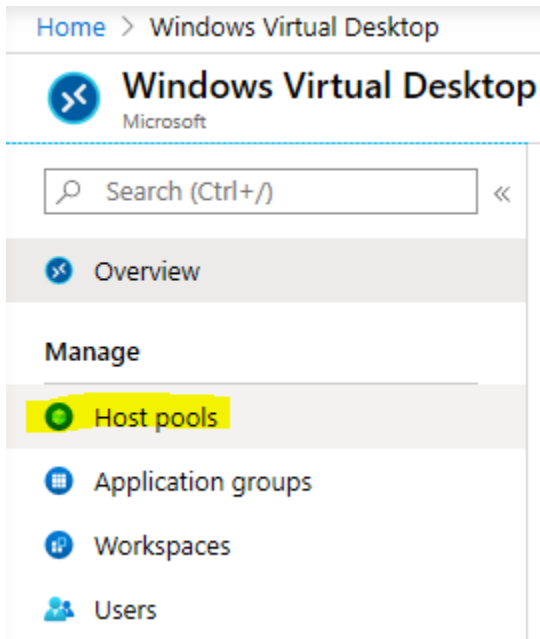


Figure 20 WVD Host pools

- 10) Press **Add**
- 11) Fill in the 'Basics' blade as depicted below:

Match **Location** with what was used to deploy the Workspace earlier.

Host pool type can be used to indicate whether multiple sessions will be allowed per WVD session host (Virtual machine) or whether each user will be assigned a personal WVD session host (1 VM per user).

Basics Virtual Machines Workspace Tags Review + create

Project details

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Host pool name * ✓

Location * ⓘ ✓
 Metadata will be stored in Central US

Host pool type

If you select pooled (shared), users will still be able to access their personalization and user data, using FSLogix.

Host pool type * ✓

Max session limit ⓘ ✓

Load balancing algorithm ⓘ ✓

Figure 21 WVD Host pool Basics

12) Press **Next: Virtual Machines**

13) Select **No** on **Add virtual machines** (depicted below), as we will do this later

Basics **Virtual Machines** Workspace Tags Review + create

Host pools are a collection of one or more identical virtual machines within Windows Virtual Desktop environments. Here you give details to create a resource group with virtual machines in an Azure subscription. [Learn more](#)

Add virtual machines No Yes

Figure 22 WVD Host pool VMs

14) Press **Next: Workspace**

15) Fill in the 'Workspace' blade as depicted below:

Select the Workspace created earlier. This will achieve the following: create the default Application group (Type: **Desktop**), associate it with the Host pool and associate the Host pool with the earlier created Workspace.

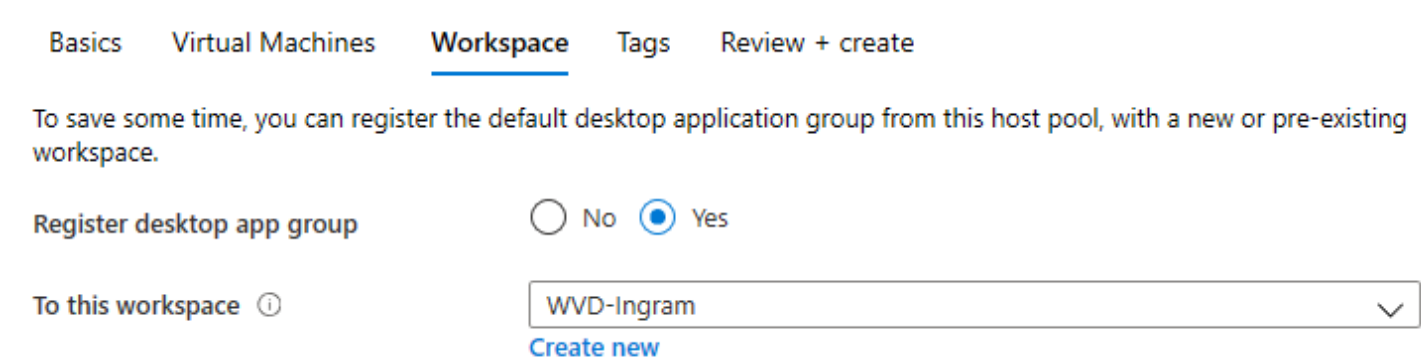


Figure 23 WVD Host pool back-end association

16) Press **Review + Create**

17) Press **Create**

18) Return to 'Windows Virtual Desktop' after the deployment

19) Press **Application groups** and verify the existence of the **DAG** (Default Application Group), as depicted below:

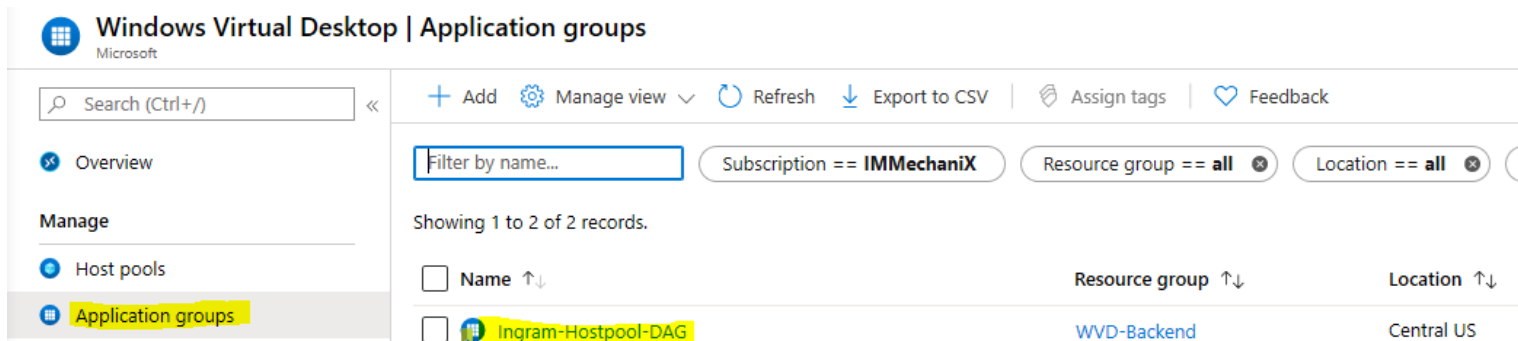


Figure 24 WVD Application Groups

20) Press the '**DAG**' titled Application group

21) Press **Properties**, as depicted below:

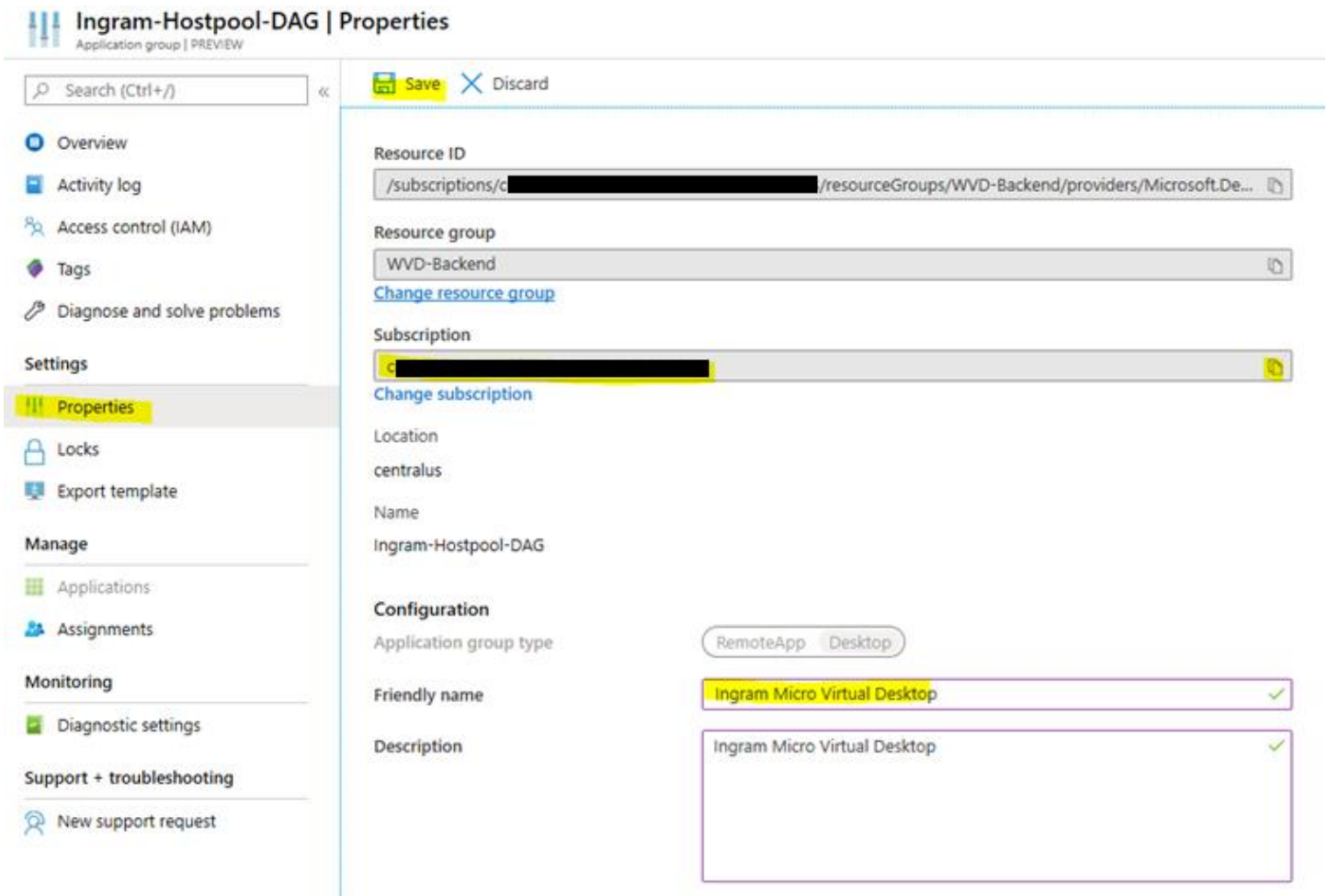


Figure 25 WVD DAG

- 22) Change the 'Friendly name' field to something representative for users
- 23) Copy the 'Subscription' string and save it. This is the Azure subscription where all your resources are located in and will be required later in the guide.
- 24) Press **Save**
- 25) Finally, press **Assignments** to assign users access to the Application group.

5 AAD DS Post deployment actions

Critical note: If you are using traditional AD DS (on a VM) this chapter can be skipped.

- 1) Log in on the Azure Portal (for example: portal.azure.com) with your administrator account
- 2) Search for 'Azure AD Domain Services' in the upper search bar and press the corresponding service

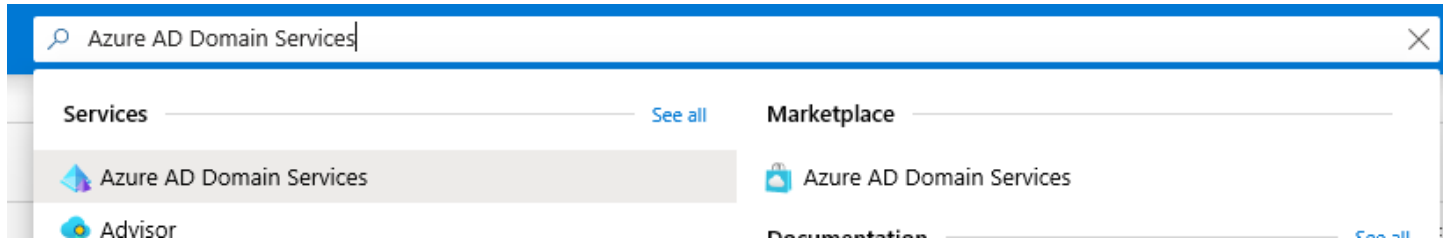


Figure 26 AAD DS

- 3) After the AAD DS deployment has completed and is marked as 'Running', as displayed in the figure below, a few more steps must be taken to finish the deployment fully. If the status is not 'Running', wait until it is.

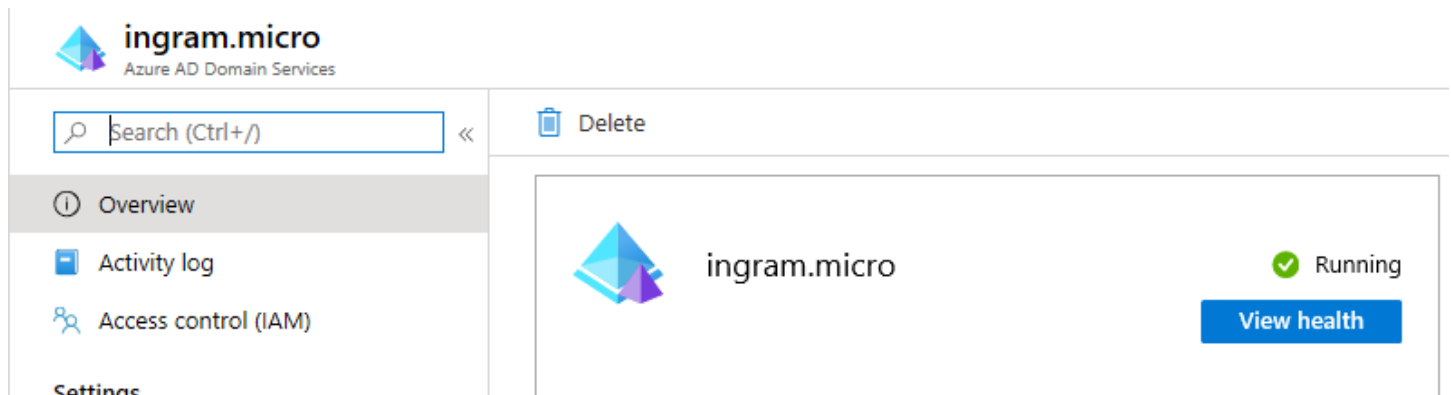


Figure 27 AAD DS status

- 4) To properly utilize the managed domain created in AAD DS the underlying Domain Controllers must be applied to the VNet's DNS propagation settings. Press the **Configure** button displayed in the figure below to achieve this

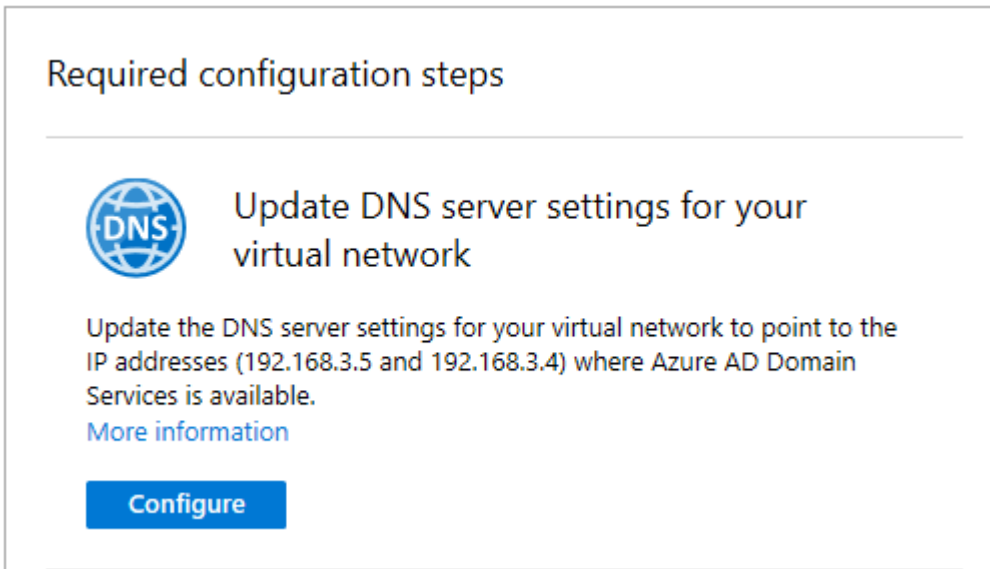


Figure 28 AAD DS DNS Update

- 5) Verify this by waiting for the operation to complete, as depicted below:

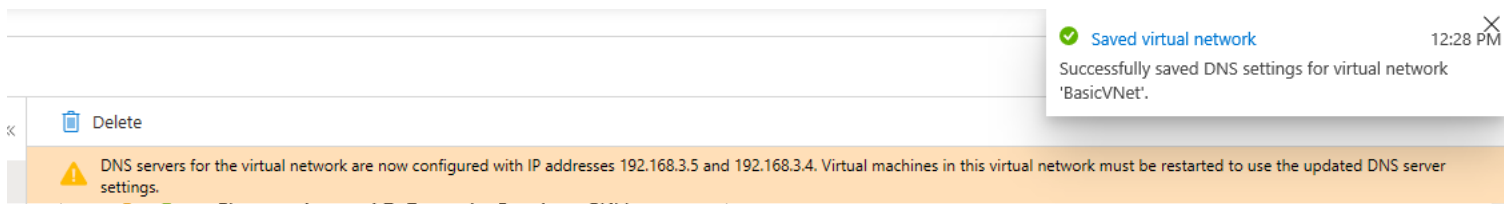


Figure 29 DNS Update

The next steps are required for all Azure AD accounts (**including administrators**) that existed prior to the deployment of AAD DS, not executing the instructions will result in ambiguous errors such as deployment and log on failures in the future.

The instructions for cloud-only (Azure AD) user accounts are quite straight forward: reset the password of all cloud-only user accounts, which forces password hash synchronization towards AAD DS. Without the hash synchronization AAD DS cannot handle (account) authentication, as Azure AD does not support NTLM/Kerberos authentication without AAD DS.

Refer to the figured depicted below:

<input type="checkbox"/>		Admin Maran	[REDACTED]	Member	Azure Active Directory
<input type="checkbox"/>		Andy IT Admin	[REDACTED]	Member	Windows Server AD
<input type="checkbox"/>		Angie Accounting	[REDACTED]	Member	Windows Server AD
<input type="checkbox"/>		Cecilia, Franklyn	[REDACTED]	Guest	External Azure Active Directory

Figure 30 Azure AD Types of accounts

3 types of account sources can be identified:

Azure Active Directory: this is a cloud-only account and only exists in this Azure AD directory/tenant. Resetting the password will force the password hash synchronization and allow this user to log in to AAD DS, and WVD once this guide has been completed.

For more background information on this consult the source below:

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-create-instance#enable-user-accounts-for-azure-ad-ds>

Windows Server AD: this is an account that is present in a traditional AD DS deployment and is being synchronized to Azure AD through Azure AD Connect. To allow these users to log on to AAD DS (and WVD) the steps in the source below must be taken:

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-configure-password-hash-sync>

Alternatively, the Azure AD Connect solution can be removed/stopped. This will transform all 'Windows Server AD' accounts to 'Azure Active Directory', making them cloud-only.

External Azure Active Directory (Guest/B2B): this is an account that originates from another Azure AD directory/tenant. The password hashes are only present in the Azure AD directory/tenant where the account originates from and thus cannot be synchronized to the AAD DS domain in your tenant. This means that these accounts will not be able to log on to AAD DS (and WVD by extension). Create a new account in your Azure AD directory/tenant where AAD DS was deployed in earlier to allow this person to access AAD DS and WVD. For reference consult the source below (the concept of only saving the password hash in the native/originating Azure AD tenant holds true for both AAD DS and traditional AD DS):

[Azure AD Domain Services - Guest Users](#)

6 Manage AAD DS

AAD DS (Azure AD Domain Services) is a PaaS (Platform-as-a-Service) solution to integrating Domain Services in your infrastructure, rather than hosting Domain Services on an IaaS (Infrastructure-as-a-Service) Virtual Machine (VM) yourself. Since we only have access to the platform offering of Domain Services and not the actual domain controllers (VMs) hosting it, we will need to create an IaaS VM to manage it with the appropriate tools such as Active Directory Users & Computers.

- 1) Log in on the Azure Portal (for example: portal.azure.com) with your administrator account
- 2) Search for 'Virtual Machines' in the upper search bar and press the corresponding service
- 3) Press **Add** as depicted below:

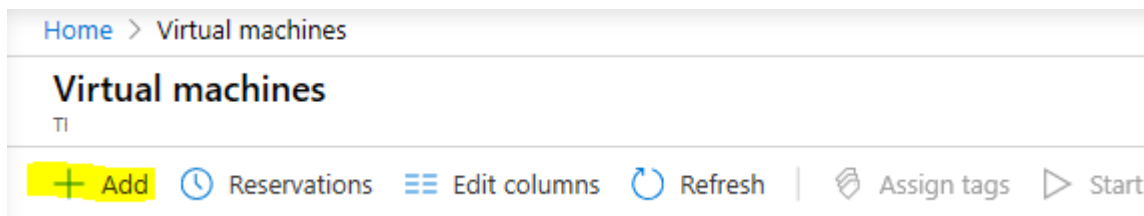


Figure 31 Add VM

- 4) Search for 'Virtual Machines' in the upper search bar and press the corresponding service
- 5) Fill in the 'Basics blade' as depicted below:

Basics Disks Networking Management Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image.

Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.

Project details

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

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Instance details

Virtual machine name * ⓘ ✓

Region * ⓘ

Availability options ⓘ

Image * ⓘ [Browse all public and private images](#)

Azure Spot instance ⓘ Yes No

Size * ⓘ **Standard B2s**
 2 vcpus, 4 GiB memory (Price unavailable)
[Change size](#)

Figure 32 VM Basics blade 1

Administrator account

Username * ⓘ ✓

Password * ⓘ ✓

Confirm password * ⓘ ✓

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ None Allow selected ports

Select inbound ports * ▼

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Save money

Save up to 49% with a license you already own using Azure Hybrid Benefit. [Learn more](#)

Already have a Windows Server license? * Yes No ⓘ

Figure 33 VM Basics blade 2

6) Fill in the 'Disks' blade as depicted below:

Basics Disks Networking Management Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

Disk options

OS disk type * ⓘ Standard SSD ▾

The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Encryption type * (Default) Encryption at rest with a platform-managed key ▾

Enable Ultra Disk compatibility ⓘ Yes No

Ultra Disk compatibility is not available for this VM size and location.

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching
Create and attach a new disk		Attach an existing disk		

▾ **Advanced**

Figure 34 VM Disks blade

7) Fill in the 'Networking' blade as depicted below:

Make sure to select the VNet where AAD DS was previously deployed in.

[Basics](#)
[Disks](#)
[Networking](#)
[Management](#)
[Advanced](#)
[Tags](#)
[Review + create](#)

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * ⓘ ▼
[Create new](#)

Subnet * ⓘ ▼
[Manage subnet configuration](#)

Public IP ⓘ ▼
[Create new](#)

NIC network security group ⓘ None Basic Advanced

i The selected subnet 'SUBNET-03-IL (192.168.3.0/24)' is already associated to a network security group 'NSG-03-IL'. We recommend managing connectivity to this virtual machine via the existing network security group instead of creating a new one here.

Accelerated networking ⓘ On Off
The selected VM size does not support accelerated networking.

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Place this virtual machine behind an existing load balancing solution? Yes No

Figure 35 VM Networking blade

8) Fill in the 'Management' blade as depicted below:

Basics Disks Networking Management Advanced Tags Review + create

Configure monitoring and management options for your VM.

Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads.

[Learn more](#)

✔ Your subscription is protected by Azure Security Center basic plan.

Monitoring

Boot diagnostics ⓘ On Off

OS guest diagnostics ⓘ On Off

Diagnostics storage account * ⓘ
[Create new](#)

Identity

System assigned managed identity ⓘ On Off

Azure Active Directory

Login with AAD credentials (Preview) ⓘ On Off

Auto-shutdown

Enable auto-shutdown ⓘ On Off

Backup

Enable backup ⓘ On Off

Figure 36 VM Management blade

9) Press **Review + Create**

10) Finally, press **Create**

- 11) Connect to the VM through RDP with the previously specified local administrator credentials. This requires an Azure Public IP to be assigned to the VM and the appropriate port (3389) to be accessible. An alternative is to deploy Azure Bastion and connect to the VM through HTML5 (if Azure Bastion has been deployed in your environment).
- 12) Open Server Manager as depicted below:

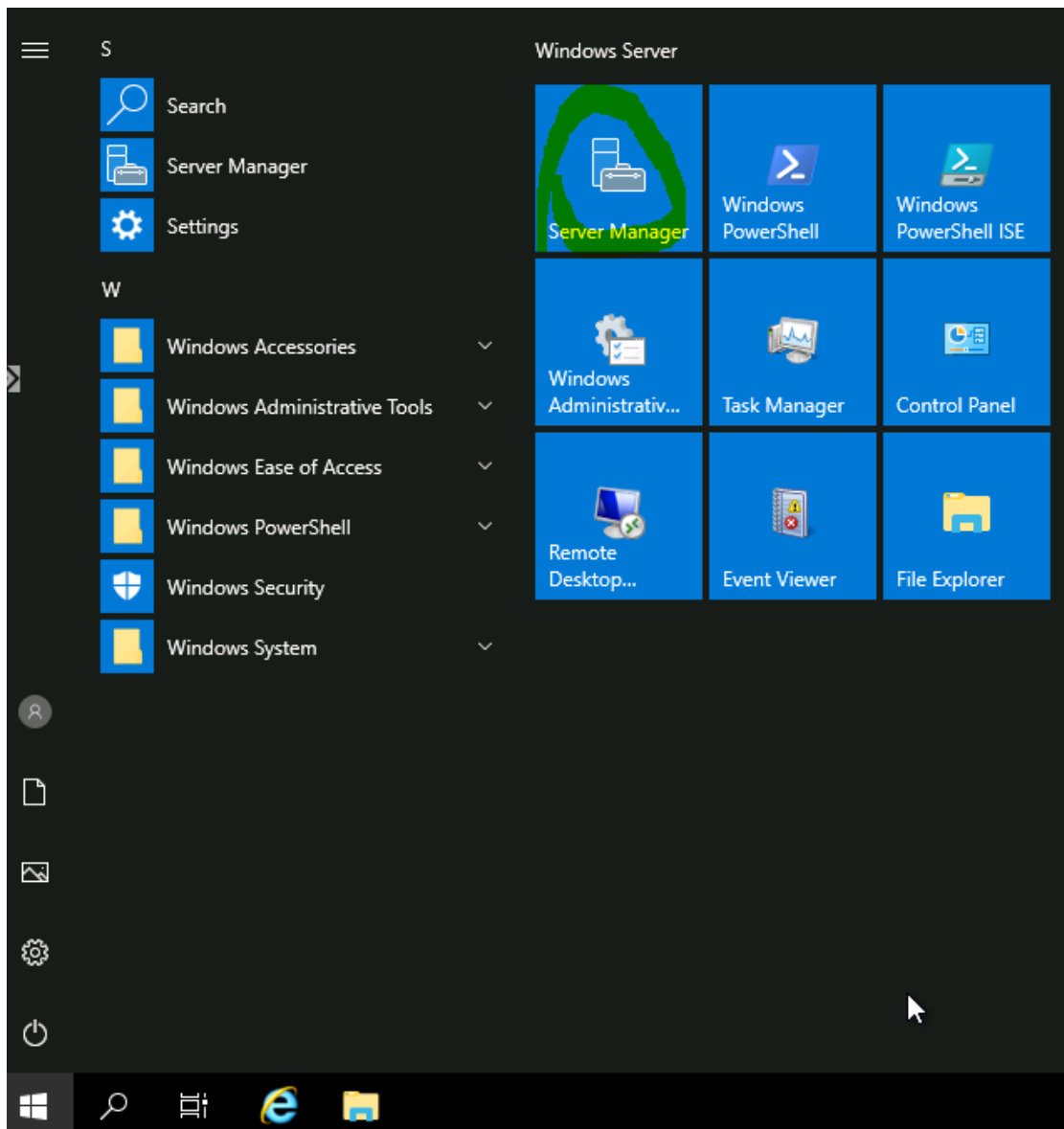


Figure 37 Server manager

13) Press **Add Roles and Features**

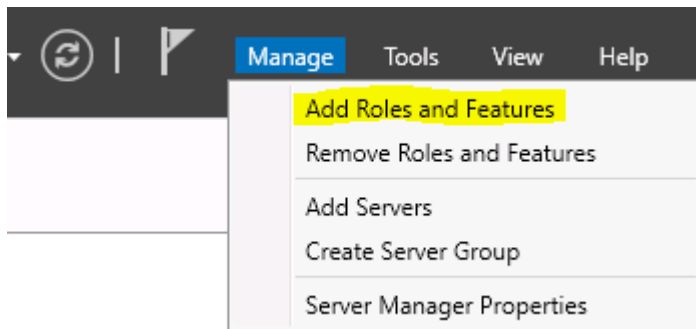


Figure 38 Add Roles and Features

14) Press Next four (4) times until you see the 'Features' screen

Select the 3 components below:

- Group Policy Management
- Remote Server Administration Tools -> Role Administration Tools -> AD DS and AD LDS Tools
- DNS Server Tools

15) Verify the components as depicted below and install the features

Installation progress

DESTINATION SERVER
AADD5-MG

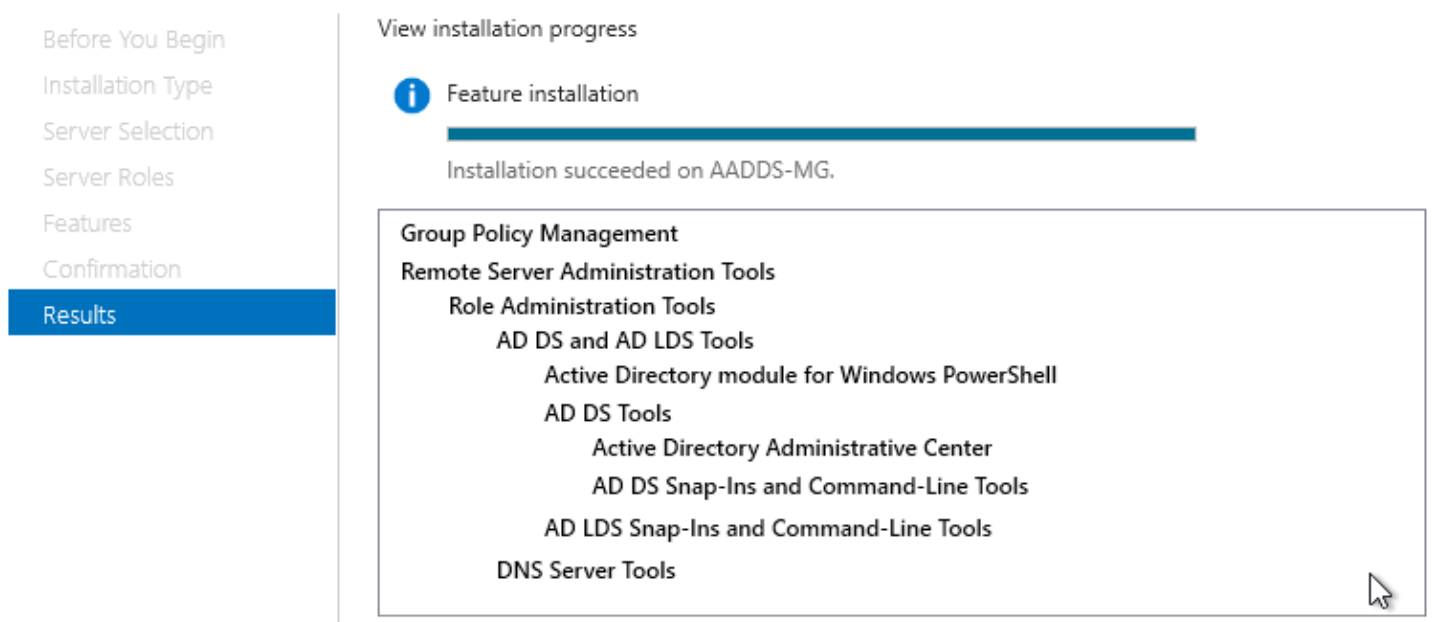


Figure 39 Feature installation

16) Finally, press **Close**

17) Navigate to **This PC** and press **Properties**

Navigate to **This PC**

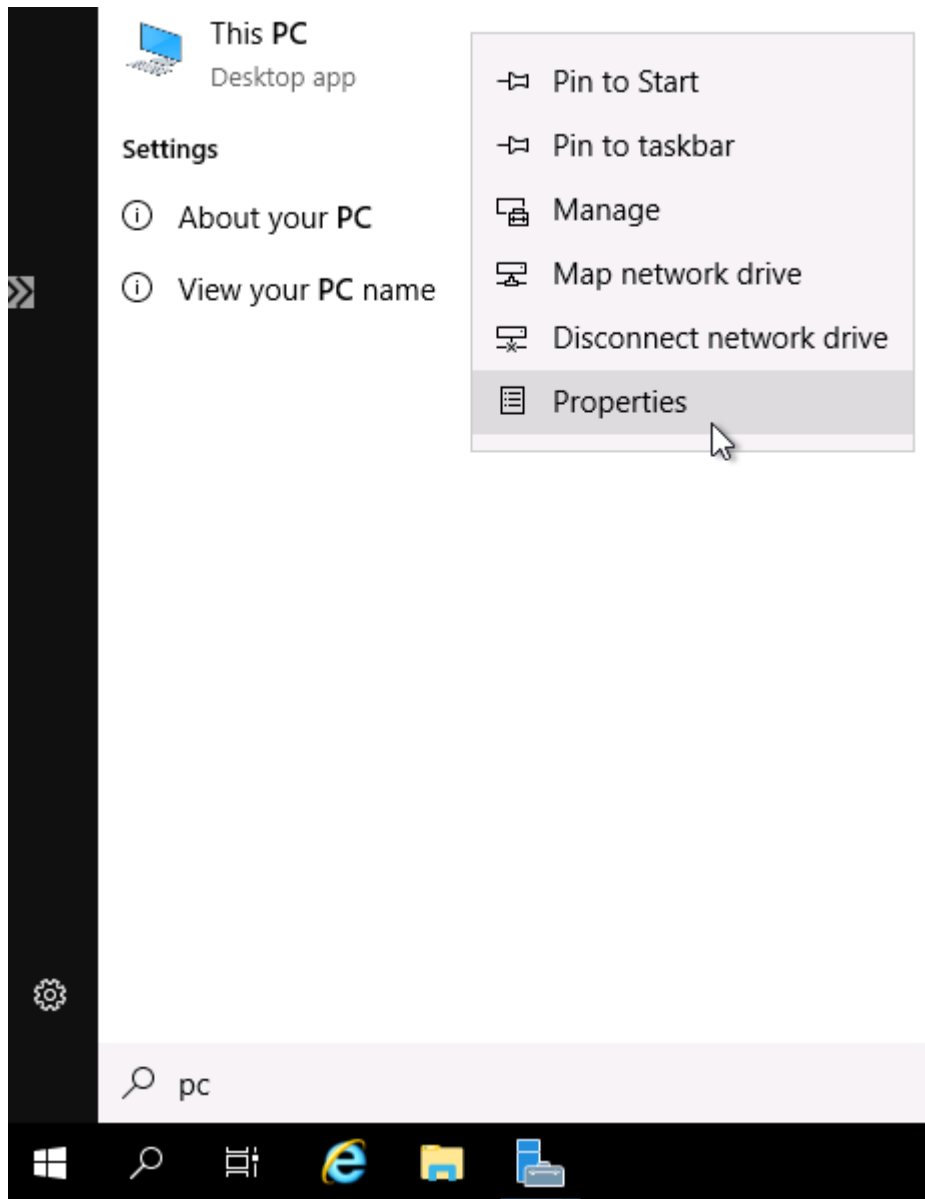


Figure 40 This PC - Properties

18) Press **Change Settings**

19) Press **Change**

20) Select **Domain** and specify the desired domain as depicted in the figure below:

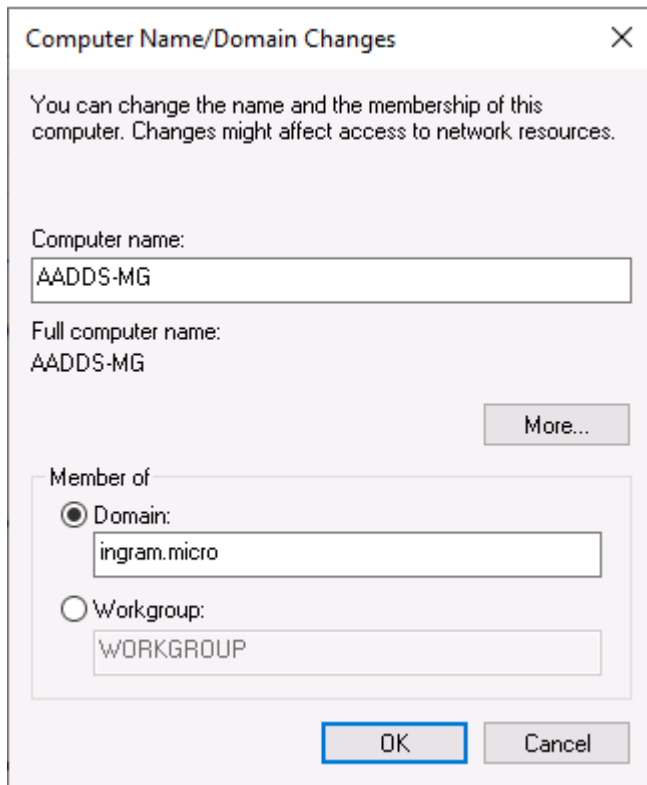


Figure 41 Domain join

21) Press **Ok**

22) Enter the credentials of an account that is allowed to add computer objects to the domain. For an AAD DS deployment this is the UPN (as stated in Azure AD) of a member of the '**AAD DC Administrators group**' in Azure AD. For a traditional AD DS deployment this is the UPN of a user with permissions to join computer objects to the domain (a Domain Admin for example).

23) Finally, press **Ok** and restart the VM

In case further assistance or information is desired please consult the references below:

Tutorial: Join a Windows Server virtual machine to a managed domain

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/join-windows-vm>

Tutorial: Create a management VM to configure and administer an Azure Active Directory Domain Services managed domain

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-create-management-vm>

Administer Group Policy in an Azure AD Domain Services managed domain

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/manage-group-policy>

7 Image Management

Critical note: this chapter only applies if you would like to create your own image for WVD Session hosts. Skip this chapter if (standard) Azure Marketplace Gallery Images are sufficient for you.

There are two main ways of creating a VM/VMSS image in Azure. One is preparing a VM to meet golden image preferences and subsequently using Sysprep to generalize it, allowing an Azure Managed Image to be created from it. The other is using Azure Image Builder, which is a code-based approach to creating an image based on settings defined in a JSON file.

Depending on your preference chapter 7.1 (Sysprep method) or 7.2 (Image builder method) can be referenced for the creation of a VM image. Both methods support the use of Shared Image Galleries (SIG), which allows for comprehensive image management and versioning.

7.1 Azure Managed Image + Shared Image Gallery

- 1) Log in on the Azure Portal (for example: portal.azure.com) with your administrator account
- 2) Search for 'Virtual Machines' in the upper search bar and press the corresponding service
- 3) Press **Add** as depicted below:

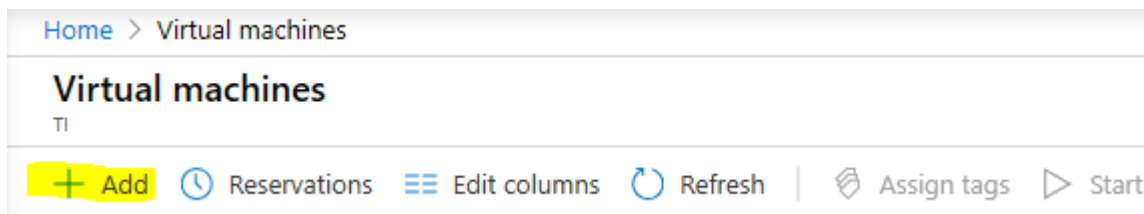


Figure 42 Add VM

- 4) Search for 'Virtual Machines' in the upper search bar and press the corresponding service
- 5) Fill in the 'Basics blade' as depicted below:

Basics Disks Networking Management Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image.

Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.

Project details

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

Subscription * ⓘ

Resource group * ⓘ
[Create new](#)

Instance details

Virtual machine name * ⓘ ✓

Region * ⓘ ▼

Availability options ⓘ ▼

Image * ⓘ ▼
[Browse all public and private images](#)

Azure Spot instance ⓘ Yes No

Size * ⓘ **Standard B2s**
 2 vcpus, 4 GiB memory (Price unavailable)
[Change size](#)

Figure 43 VM Basics blade 1

Administrator account

Username * ⓘ ✓

Password * ⓘ ✓

Confirm password * ⓘ ✓

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ None Allow selected ports

Select inbound ports * ▼

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Save money

Save up to 49% with a license you already own using Azure Hybrid Benefit. [Learn more](#)

Already have a Windows Server license? * Yes No ⓘ

Figure 44 VM Basics blade 2

6) Fill in the 'Disks' blade as depicted below:

Basics Disks Networking Management Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

Disk options

OS disk type * ⓘ Standard SSD ▾

The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Encryption type * (Default) Encryption at rest with a platform-managed key ▾

Enable Ultra Disk compatibility ⓘ Yes No

Ultra Disk compatibility is not available for this VM size and location.

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching
Create and attach a new disk		Attach an existing disk		

▾ **Advanced**

Figure 45 VM Disks blade

7) Fill in the 'Networking' blade as depicted below:

Make sure to select the VNet where AAD DS was previously deployed in.

Basics Disks **Networking** Management Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * ⓘ ▼
[Create new](#)

Subnet * ⓘ ▼
[Manage subnet configuration](#)

Public IP ⓘ ▼
[Create new](#)

NIC network security group ⓘ None Basic Advanced

i The selected subnet 'SUBNET-03-IL (192.168.3.0/24)' is already associated to a network security group 'NSG-03-IL'. We recommend managing connectivity to this virtual machine via the existing network security group instead of creating a new one here.

Accelerated networking ⓘ On Off
 The selected VM size does not support accelerated networking.

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Place this virtual machine behind an existing load balancing solution? Yes No

Figure 46 VM Networking blade

8) Fill in the 'Management' blade as depicted below:

Basics Disks Networking Management Advanced Tags Review + create

Configure monitoring and management options for your VM.

Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads.

[Learn more](#)

✔ Your subscription is protected by Azure Security Center basic plan.

Monitoring

Boot diagnostics ⓘ On Off

OS guest diagnostics ⓘ On Off

Diagnostics storage account * ⓘ
[Create new](#)

Identity

System assigned managed identity ⓘ On Off

Azure Active Directory

Login with AAD credentials (Preview) ⓘ On Off

Auto-shutdown

Enable auto-shutdown ⓘ On Off

Backup

Enable backup ⓘ On Off

Figure 47 VM Management blade

9) Press **Review + Create**

10) Finally, press **Create**

- 11) Connect to the VM through RDP with the previously specified local administrator credentials. This requires an Azure Public IP to be assigned to the VM and the appropriate port (3389) to be accessible. An alternative is to deploy Azure Bastion and connect to the VM through HTML5 (if Azure Bastion has been deployed in your environment).
- 12) Install Windows Updates
- 13) Restart the VM
- 14) Check for and install Windows Updates
- 15) Install the desired software on the VM, for it to become your golden image
- 16) If using FSLogix (recommended), refer to chapter 13 for deployment instructions, or install it manually.
- 17) If you would like to add Language packs refer to the source below:

<https://docs.microsoft.com/en-us/azure/virtual-desktop/language-packs>

- 18) Start PowerShell as administrator and run the script downloadable through the link below:

<https://raw.githubusercontent.com/MaranVerweij/IngramMicroAzure/MaranVerweij-Azure-Ingram1/Windows%20Virtual%20Desktop%20Guide/Sysprep.ps1>

This script will remove WVD agent software (as it needs to be installed per WVD session host), disable Windows Update and finally run Sysprep.

- 19) Wait until the VM has successfully shut down. This will happen automatically after Sysprep completes.
- 20) Navigate to the VM in the Azure Portal
- 21) Verify the status is 'Stopped' or 'Deallocated'
- 22) Press **Capture**, as depicted below:

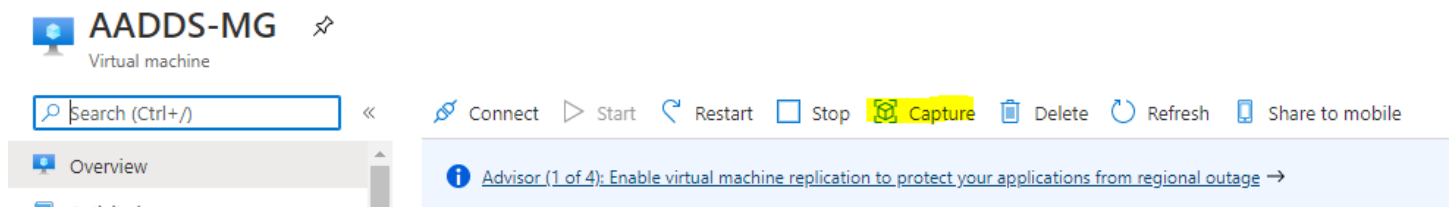


Figure 48 Capture Image

23) Fill in the options as depicted below:

Keep in mind that when a VM is deleted the Managed disks are not deleted. The same goes for Network Interface Cards and Public IP addresses. Delete them manually later to achieve a total clean up.

Select an existing Shared Image Gallery or create a new one. Keep in mind that when selecting an existing one it must be in the same Resource Group as your VM.

Select 'Generalized' as all unique identifiers have been removed through the use of Sysprep.

Select an existing Image Definition or create a new one. The Image Definition holds 1 or more Image Versions.

Do not select 'Exclude from latest' as this will cause the latest Image Version to not be deployed if your Image Definition is used to create VMs or VMSS instances from.

Share image to Shared image gallery ⓘ Yes, share it to a gallery as an image version.
 No, capture only a managed image.

Automatically delete this virtual machine after creating the image ⓘ

Gallery details

Target image gallery * ⓘ

Operating system state ⓘ Generalized: VMs created from this image require hostname, admin user, and other VM related setup to be completed on first boot
 Specialized: VMs created from this image are completely configured and do not require parameters such as hostname and admin user/password

⚠ Capturing a virtual machine image will make the virtual machine unusable. This action cannot be undone.

Target image definition * ⓘ

Version details

Version number * ⓘ

Exclude from latest ⓘ

End of life date ⓘ

Figure 49 Capture Image

- 24) Press **Review + create**
- 25) Press **Create**
- 26) Wait for the image to be created successfully
- 27) Navigate to 'Shared image galleries', as depicted below:

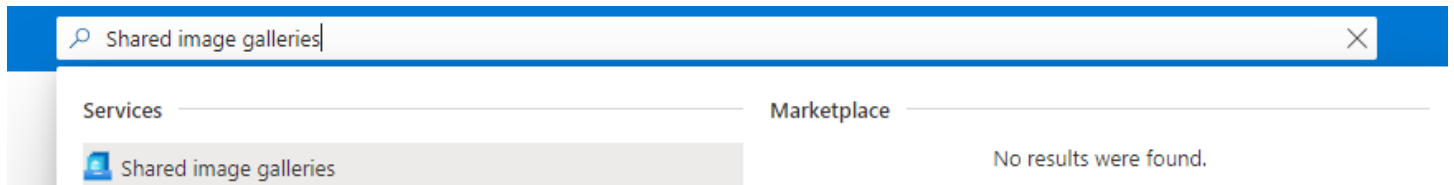


Figure 50 Shared image galleries

- 28) Press the recently created Shared image gallery
- 29) Press the recently created Image definition
- 30) Copy and document the 'Resource ID' of the Image definition, as this will be required later during the guide

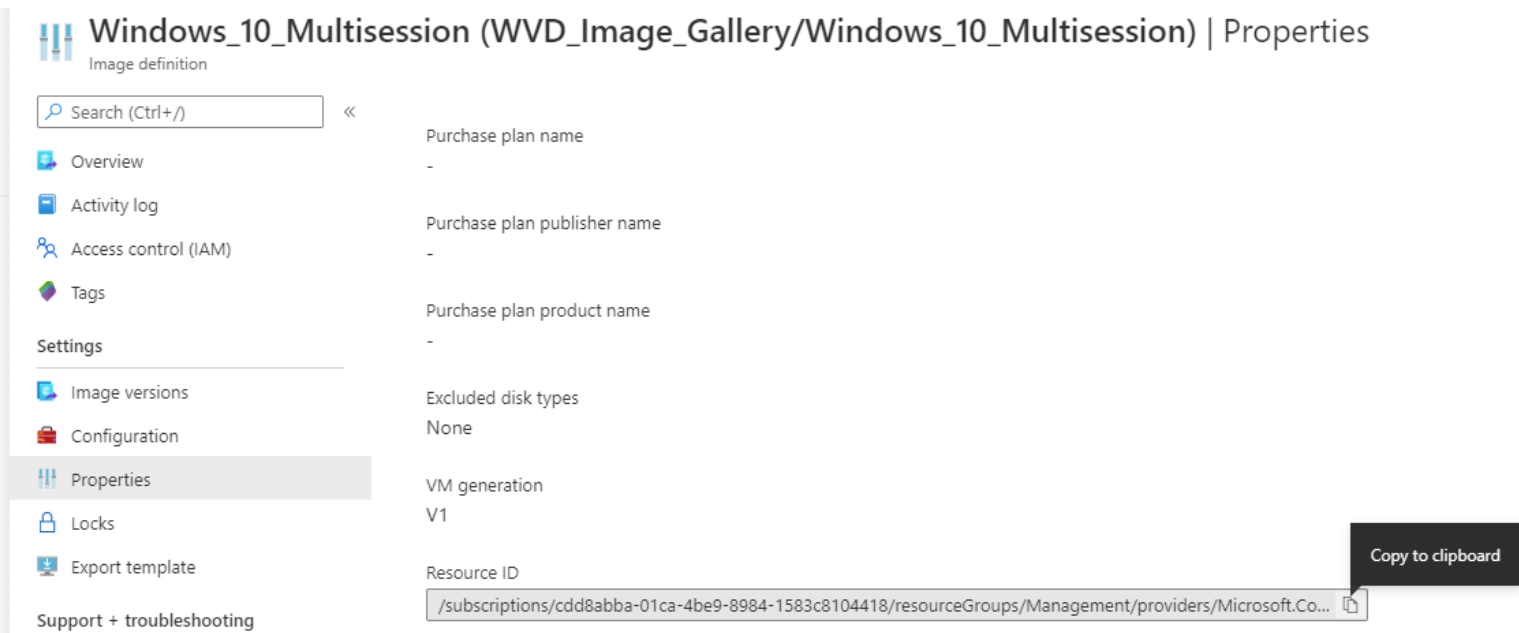


Figure 51 Image definition - Resource ID

7.2 Azure Image Builder

For information and instructions on using Azure Image Builder please consult the source below:

[https://docs.microsoft.com/en-us/learn/modules/customize-windows-server-iaas-virtual-machine-images/6-
implement-azure-image-builder](https://docs.microsoft.com/en-us/learn/modules/customize-windows-server-iaas-virtual-machine-images/6-implement-azure-image-builder)

8 Create a Service principal for WVD

Critical note: the Azure service principal will be required for automatic scaling and for the use of VM Scale Sets (detailed in chapter 9). If that is not relevant for your use case this chapter can be skipped.

Instead of using a user account (identity) to perform tasks an Azure service principal can be used. A service principal can be configured with only the permissions it needs to complete a task (comparable with a service account) whereas a user account tends to have permissions to perform multiple tasks in various categories (day to day activities). In this chapter we will create a service principal to perform tasks in the WVD workspace/tenant and the related Azure Subscription. Automated tasks, for example auto scaling, cannot run successfully when dependent on an identity that requires Multi-factor Authentication (MFA) because manual interaction breaks the concept of automation. In combination with the principle of least privilege and the support of extremely long passwords a service principal is the ideal identity type for scheduled/automated tasks. For further reference consult the Microsoft quote and source below:

“An Azure service principal is an identity created for use with applications, hosted services, and automated tools to access Azure resources. This access is restricted by the roles assigned to the service principal, giving you control over which resources can be accessed and at which level. For security reasons, it is always recommended to use service principals with automated tools rather than allowing them to log in with a user identity.

Automated tools that use Azure services should always have restricted permissions. Instead of having applications sign in as a fully privileged user, Azure offers service principals.”

<https://docs.microsoft.com/en-us/PowerShell/azure/create-azure-service-principal-azureps?view=azps-2.8.0>

The steps below will allow an Azure service principal to be created which has the appropriate permissions to manage the WVD workspace and the specified Azure subscription.

- 1) Navigate to the URL below and copy the PowerShell script:

https://github.com/MaranVerweij/IngramMicroAzure/blob/MaranVerweij-Azure-Ingram1/Windows%20Virtual%20Desktop%20Guide/Create_SVP_WVD_andgrantpermissions.ps1

The script must be executed on a workstation (virtual or physical) with Administrator access to PowerShell.

- 2) Start PowerShell (ISE) as Administrator and paste the script
- 3) The following variables need to be defined before running the script:

Azure_sub: The Azure subscription ID as noted earlier (end of Chapter 4)

SVP_Displayname: Create a (new) display name for the Azure service principal, take note of it as it will be required later.

Role_Scope: The default scope is the entire Azure subscription, do not change this unless you want to narrow this down further to a resource group (if all your WVD resources are limited to a predefined resource group). The scope string to specify a resource group looks like the line below and can be found under the properties section of a resource group in the Azure Portal:

```
/subscriptions/zzzzzzzz-zzzz-zzzz-zzzz-zzzzzzzzzzzzz/resourceGroups/YourResourceGroupName
```

- 4) Run the script and take note of the Service Principal (Application) **ID** produced in the output
- 5) Take note of the Service Principal (Application) ID **Secret/Password** produced in the output

The script will create an Azure AD Application Service Principal, an alternative is a System Managed Identity service principal. The differences between them are briefly described below:

Azure AD Application service principal	System Managed Identity service principal
Is created independently	Is created with an inherent connection to the system. For example, a Virtual Machine (VM). This allows you to assign Azure RBAC Roles to a system.
Can authenticate worldwide. For example, any workstation with PowerShell and an internet connection can authenticate to Azure via the 'Connect-AzAccount' CMDlet if the Azure AD Tenant ID, service principal Application ID and service principal secret/password are known. As such, it is recommended to utilize the maximum password length, to prevent brute force vulnerabilities.	This service principal can only be used from the referenced system. For example, via a PowerShell script, run on the system, which calls 'Connect-AzAccount -Identity'. This will open a management session to Azure. Keep in mind that all users logged in on the system (a VM for example) can utilize the service principal, which is why it is recommended to restrict PowerShell use for unprivileged users.

Figure 52 Service principal comparison

If you would like to implement a System Managed Identity service principal rather than an Azure AD Application service principal, please contact us.

9 Deploying WVD Session Hosts

Windows Virtual Desktop Session Hosts are very comparable to Remote Desktop Session Hosts and Terminal Servers. These VMs will be hosting the (virtual) user sessions according to WVD architecture.

Consult the source below for help with VM sizing: [Microsoft Virtual machine sizing guidelines](#)

If you would like to personally discuss VM sizing please contact us at: Microsoft@ingrammicro.nl

There are multiple ways of deploying WVD Session Hosts, keeping in mind that WVD Session Hosts are IaaS VMs (with a Windows OS) which are also configured with WVD agent software. Choose one of the two methods as described below:

9.1 VM Scale Sets + WVD (an Ingram Micro Solution) will cover the use of Virtual Machine Scale Sets (VMSS) for WVD session hosts. By using custom workflows (Custom script extensions) VMSS can be utilized for WVD.

Advantages:

- Up and down scaling becomes very simple thanks to the use of VMSS, either through manual input or auto scaling rules to increase/decrease the amount of WVD session hosts (VM Instances).
- When a new image is created it can be assigned to the entire VMSS, allowing all VM instances to be reimaged easily.
- Supports the use of Availability Zones.

Disadvantages: VM Instances cannot be backed up, although this is not problematic as using a VMSS requires an up-to-date image, optionally combined with a Custom script extension. This can be used to create new VM Instances in case the current ones need to be replaced in case of issues.

9.2 Add session host wizard will cover deploying WVD session hosts through the use of a graphical wizard via the Azure Portal.

Advantages: This is a simple wizard with interactive elements and the easiest option for newcomers.

Disadvantages:

- Adding more WVD session hosts (VMs) requires you to run the entire wizard again.
- If you want to deploy a new (OS) image on the existing WVD session hosts they (and all related components) must be (manually) deleted, as they will not be reimaged. Instead new VMs are created.
- Host pool needs to be deleted and recreated if the source image needs to be changed, unless you deployed the host pool using a Shared Image Gallery Image Definition. Which allows the latest Image version to be used when running the 'Add session host wizard' to create new WVD session hosts.

9.1 VM Scale Sets + WVD

Please contact us at Microsoft@ingrammicro.nl if you are interested in implementing this solution. As you will need to be granted access to the required templates. Below you can refer to the architecture of the solution.

9.1.1 VM Scale Sets + WVD Architecture

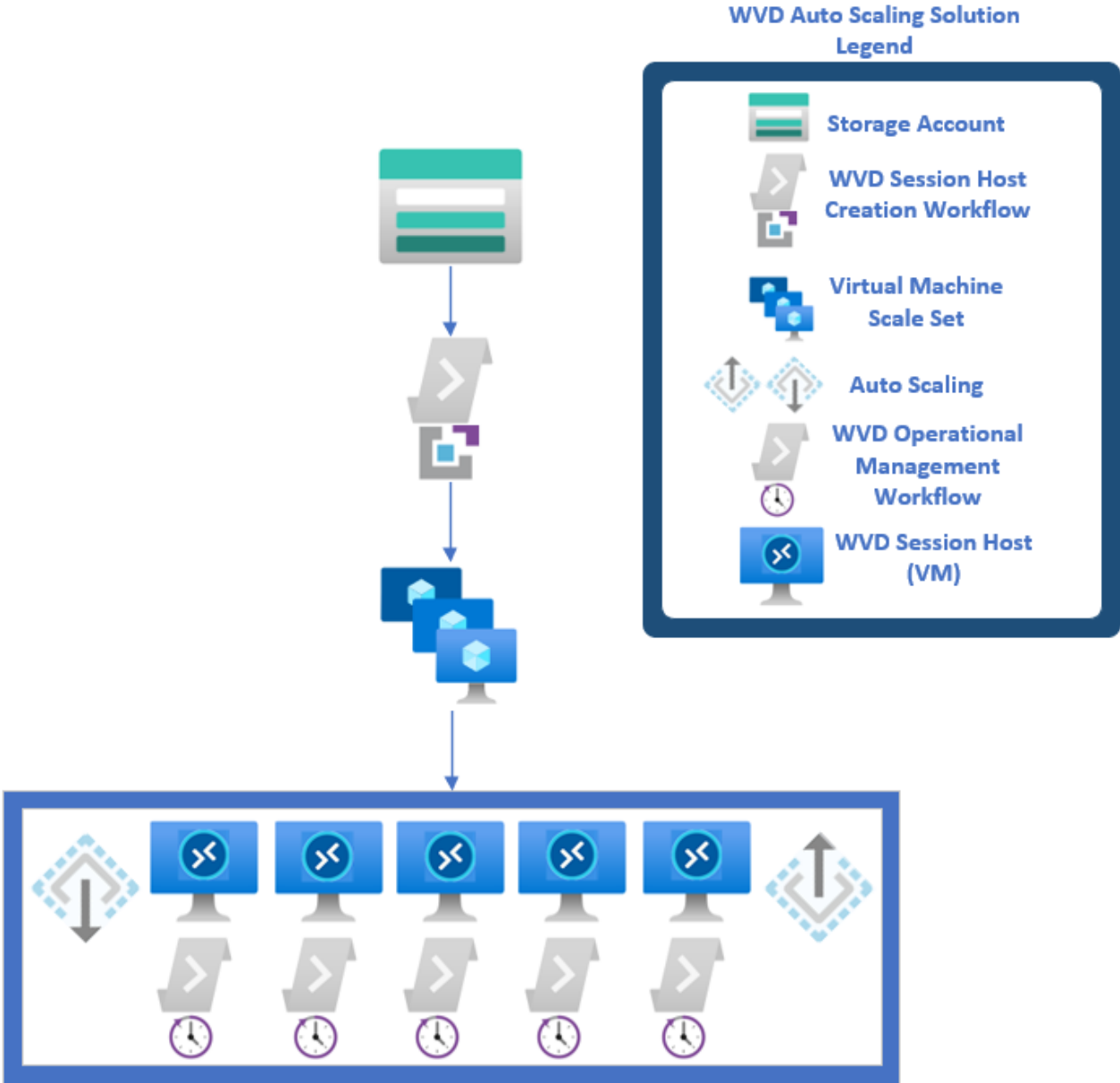


Figure 53 VMSS + WVD Solution

Storage account

The Storage account will hold the custom workflows that create a WVD session host and monitor the removal (scale-ins) of a WVD session host, to timely notify users and cleanly dispose of all WVD session host registrations.

WVD Session Host Creation Workflow

This workflow is used to turn VM instances into WVD session hosts. To ensure resiliency and consistency in the process basic Artificial Intelligence (AI) is used.

Virtual Machine Scale Set

The Virtual Machine Scale Set (VMSS) is used to automatically (or manually) scale out and/or in. It also allows for central management of VM instances in the VMSS.

WVD Operational Management Workflow

This workflow is used to inform WVD users if their respective session host is being scaled in (removed) so they have 10 minutes to sign off and (back) on to continue working on another session host. The workflow also takes care of removing WVD and Active Directory registrations for the to be scaled in session host. The workflow is present on all WVD session hosts in the form of a .PS1 file and a referring scheduled task.

9.1.2 Create Service account

The Azure Service Principal which was assigned required Azure RBAC (Role Based Access Control) roles was already created in chapter 8. However, since WVD also requires access to a Domain Services deployment a service account that can take care of joining WVD Session host computers to a domain is also required. The account will also get Remote Management access to be able to remove AD computer objects when a WVD Session host is decommissioned. The following steps will describe how to create an account for that purpose, while utilizing the concept of least privilege.

- 1) Log in on a Domain Controller (preferably with a Domain Admin account) or in case of AAD DS log in on the earlier created Management VM (with a member of AAD DC Administrators)
- 2) Open 'Active Directory Users and Computers'
- 3) Create a user called "adjoin" (or similar). A never expiring password is recommended as it will serve as a service account. **Be careful not to include the '\$' character or (double) quotes as these will have to be escaped when used in PowerShell variables, which will be configured later on.**

Keep in mind that, in case of AAD DS, creating a user in 'Active Directory Users and Computers' will result in it not being synchronized to Azure AD. As Azure AD has a one-way sync to AAD DS (not the other way around).

- 4) Create an Organizational Unit (OU) called "WVD_Session_Hosts" (or similar). This OU should/will contain the AD Computer objects of the WVD Session hosts.
- 5) Open 'Group Policy Management'
- 6) Right mouse click on the recently created OU
- 7) Press 'Create a GPO in this domain, and Link it here', as depicted below:

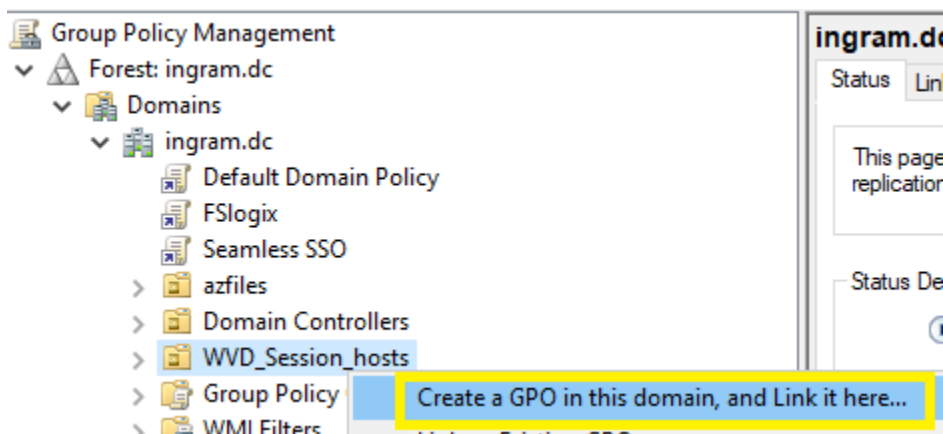


Figure 54 Create GPO

- 8) State a name for the GPO, such as: WVD service account settings
- 9) Press **Ok**
- 10) Right mouse click on the recently created GPO and press **Edit**
- 11) Navigate to Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Restricted Groups
- 12) Right mouse click on 'Restricted Groups'
- 13) Press **Add Group**
- 14) Select 'Remote Management Users', as a local group (not on domain level)
- 15) Press **Ok**
- 16) Under 'Members of this group' press **Add**
- 17) Select the recently created service account (alternatively a group of which the service account is a member can be selected)
- 18) Press **Ok**
- 19) For an example of the end result refer to the figure below:

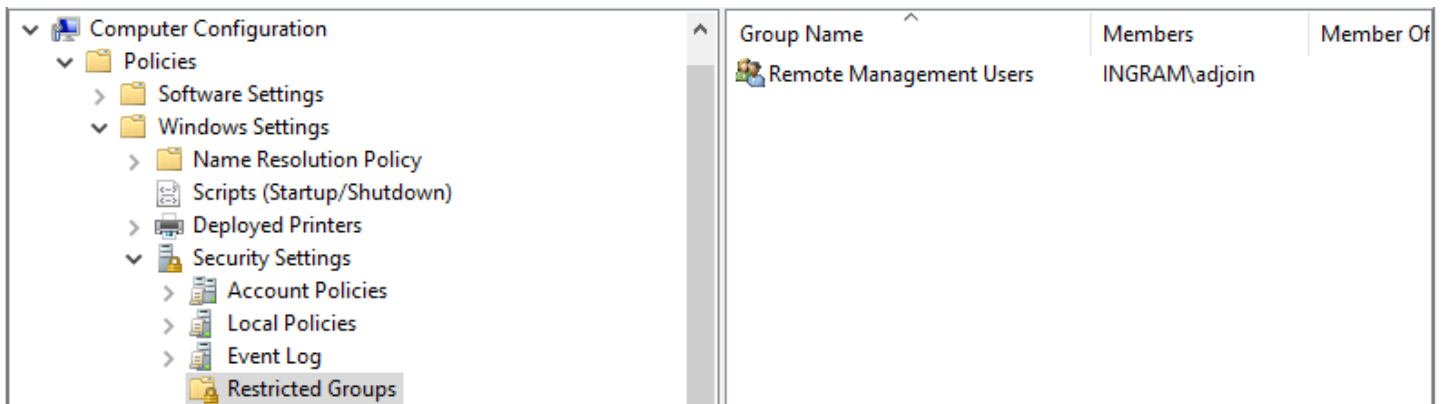


Figure 55 GPO Restricted Groups

This GPO will allow the service account to perform Remote management on behalf of the WVD Session hosts, while still being limited to permissions that will be set in the next steps.

- 20) Open 'Active Directory Users and Computers'
- 21) Right mouse click on the recently created OU
- 22) Press **Delegate Control**
- 23) Press **Next**
- 24) Press **Add**
- 25) Add the recently created service account
- 26) Press **Next**
- 27) Select 'Create a custom task to delegate'
- 28) Press **Next**

29) Configure the settings as depicted below (Computer objects, Create selected and Delete selected):

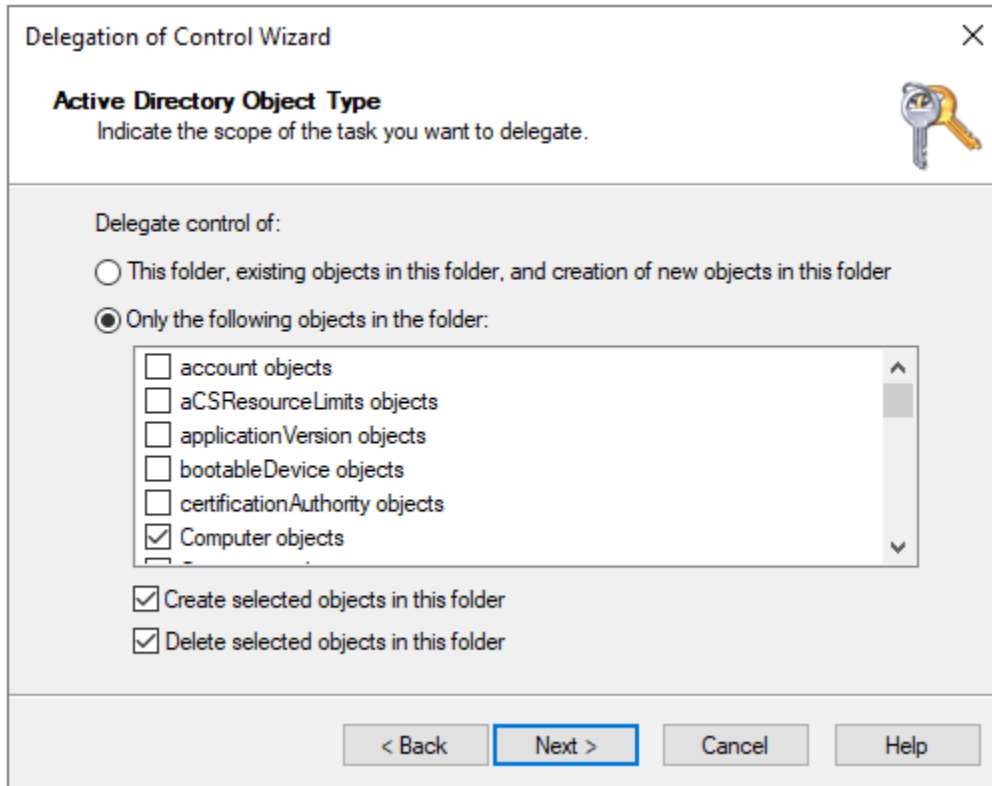


Figure 56 Delegate Control 1

30) Press **Next**

31) Configure the settings as depicted below (General, Validated write to DNS, Validated write to service):

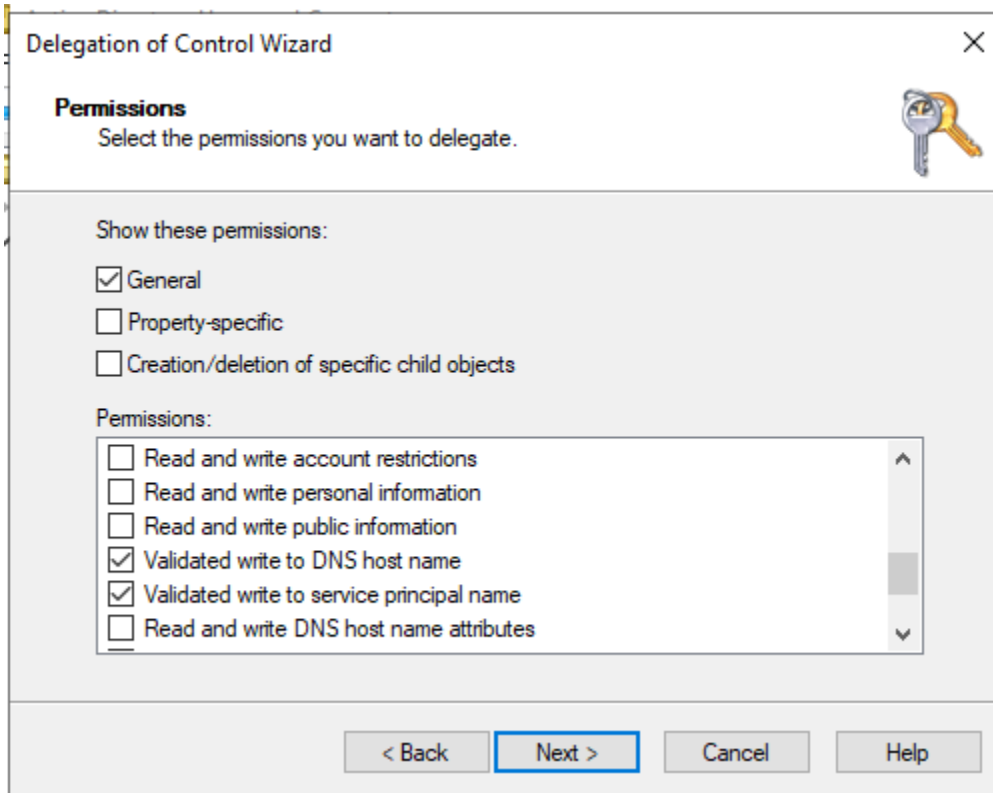


Figure 57 Delegated control 2

- 32) Press **Next**
- 33) Press **Finish**
- 34) Press **View**
- 35) Select **Advanced Features**
- 36) Right mouse click on the recently created OU
- 37) Press **Properties**
- 38) Press the 'Security' tab
- 39) Press **Advanced**
- 40) Select one of the permission entries for your service account
- 41) Press **Edit**
- 42) Select 'Delete subtree'
- 43) Press **Ok**

The service account is now configured to add and remove computers to and from the domain.

9.1.3 Prepare Storage account

A storage account is required to hold the custom workflows that will ensure automated WVD session host deployment and manage operational matters.

- 1) Log in on the Azure Portal (for example: portal.azure.com) with your administrator account
- 2) Search for 'Storage accounts' in the upper search bar and press the corresponding service

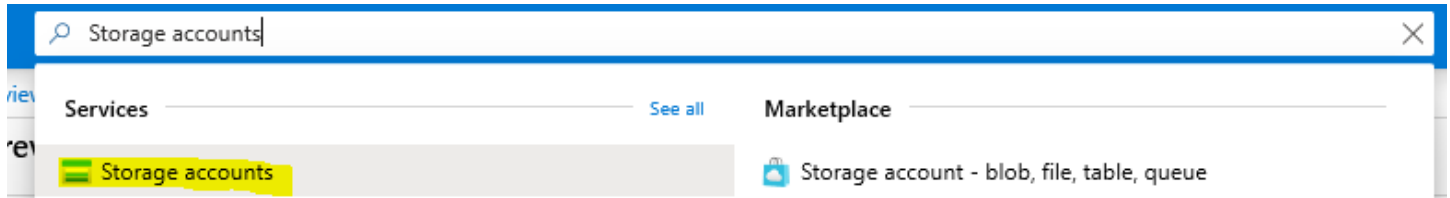


Figure 58 Storage accounts

- 3) Press **Add**
- 4) Fill in the 'Basics' blade as depicted on the next page:

Your storage account name needs to be (globally) unique and cannot contain special characters.

The **Location** should be the same as where your (A)AD DS deployment resides.

Basics Networking 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 * ▼

Resource group * ▼

[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 * ⓘ ✓

Location * ▼

Performance ⓘ Standard Premium

Account kind ⓘ ▼

Replication ⓘ ▼

Access tier (default) ⓘ Cool Hot

Figure 59 Storage Account - Basics

5) Press **Next: Networking**

6) Fill in the 'Networking' blade as depicted below:

Select the **Virtual Network** where AAD DS was previously deployed to.
 Select the **Subnet** where WVD session hosts will be deployed to (alternatively, select multiple subnets).
 Hosts in these subnets will be able to make an authentication attempt with the Azure Storage Account but will still require (further) authorization before succeeding.

The screenshot shows the 'Networking' configuration page for an Azure Storage Account. The 'Networking' tab is selected, with other tabs being 'Basics', 'Advanced', 'Tags', and 'Review + create'. The 'Network connectivity' section explains that storage accounts can be accessed publicly or privately. The 'Connectivity method' is set to 'Public endpoint (selected networks)'. The 'Virtual networks' section states that only the selected network can access the storage account. Three dropdown menus are filled: 'Virtual network subscription' is 'IMMechaniX', 'Virtual network' is 'BasicVNet', and 'Subnets' is 'SUBNET-02-BL (192.168.2.0/24)'. There are also links for 'Create virtual network' and 'Manage selected virtual network'.

Figure 60 Storage Account - Networking

- 7) Press **Review + Create**
- 8) Press **Create**
- 9) When done creating, navigate to your Storage account
- 10) Press **Networking**

Search (Ctrl+ /)

- Overview
- Activity log
- Tags
- Diagnose and solve problems
- Access Control (IAM)
- Data transfer
- Storage Explorer (preview)
- Settings
 - Access keys
 - CORS
 - Configuration
 - Encryption
 - Shared access signature
 - Networking**
 - Properties
 - Locks

Firewalls and virtual networks Private endpoint connections

Save Discard Refresh

Allow access from
 All networks Selected networks

Configure network security for your storage accounts. [Learn more](#)

Virtual networks

+ Add existing virtual network + Add new virtual network

Virtual Network	Subnet	Address r.
> BasicVNet	4	

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. [Learn more.](#)

Add your client IP address ('83.8: ') ⓘ

Address range

IP address or CIDR

Exceptions

Allow trusted Microsoft services to access this storage account ⓘ

Allow read access to storage logging from any network

Figure 61 Storage Account Networking

- 11) Select the 'Add your client IP address' checkbox, as depicted above
- 12) Verify that your desired VNet is listed, as depicted above
- 13) Finally, press **Save**

- 14) Navigate to and press **Storage Explorer**, as depicted below
- 15) Right mouse click on 'BLOB CONTAINERS'
- 16) Press **Create blob container**

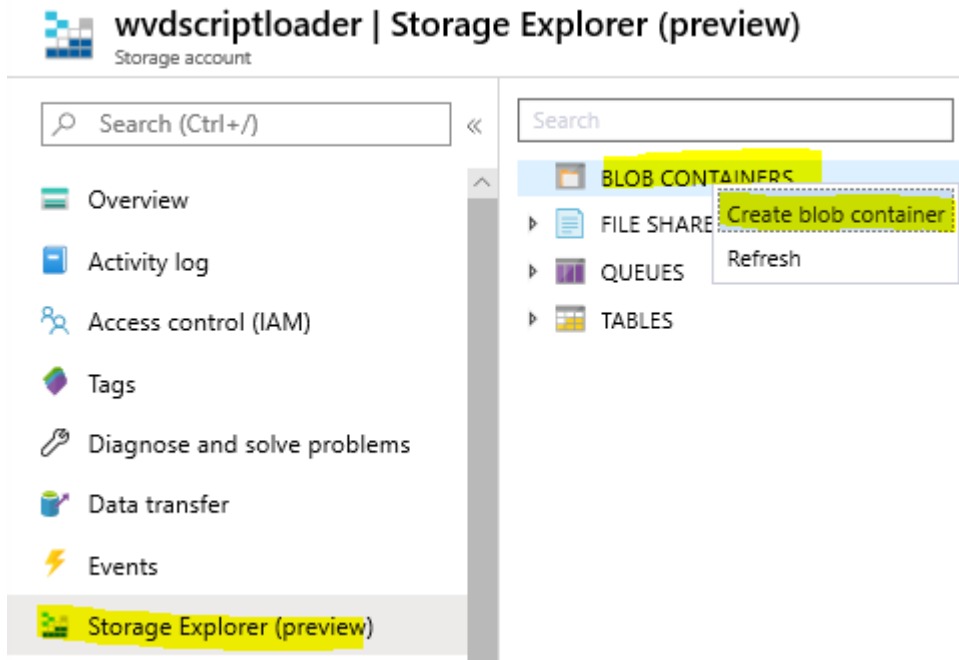


Figure 62 Storage Explorer

17) Enter a name for the container that will hold the custom workflows (.PS1 files), as depicted below:
 Anonymous action should not be allowed as these files will hold sensitive credentials.

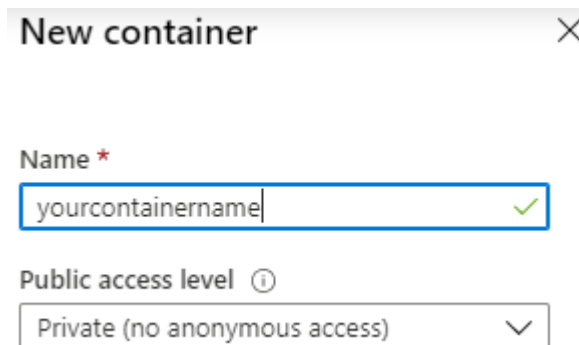


Figure 63 New Container

- 18) Press **Create**
- 19) Take note of your Storage account name and container name as this will be required later.
- 20) Press **Access Control (IAM)** as depicted below:

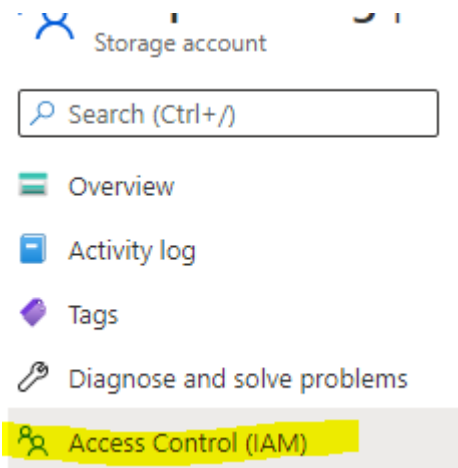


Figure 64 Storage Account Access Control

- 21) Press **Add**
- 22) Press **Add role assignment**

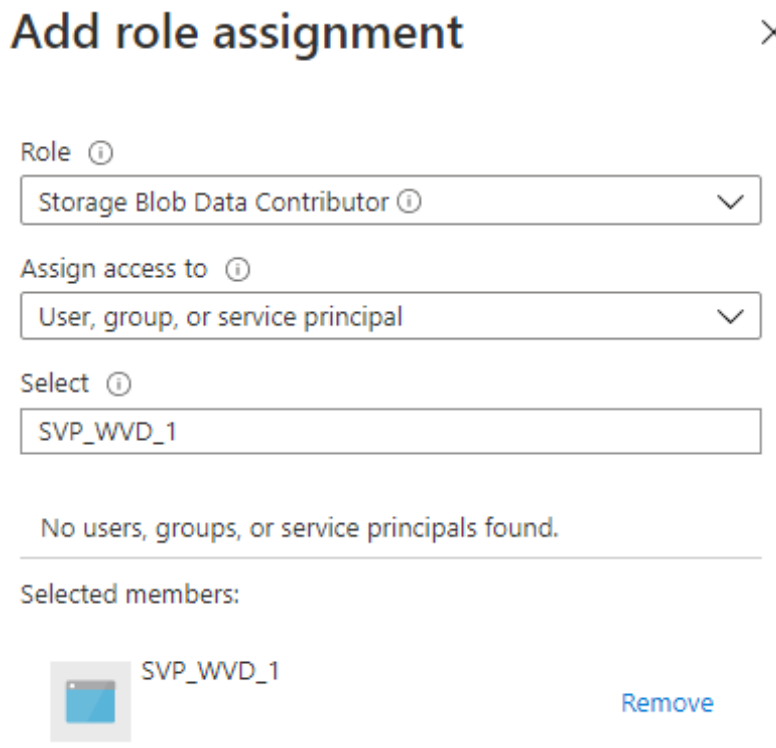


Figure 65 Storage Account Role assignment

- 23) Create a role assignment as depicted above, for the Azure Service Principal that was created earlier.
- 24) Press **Save**

9.1.4 Prepare Log Analytics Workspace

To connect the VMSS to Azure Monitor a Log Analytics Workspace is required.

- 1) Log in on the Azure Portal (for example: portal.azure.com) with your administrator account
- 2) Search for 'Log Analytics workspaces' in the upper search bar and press the corresponding service

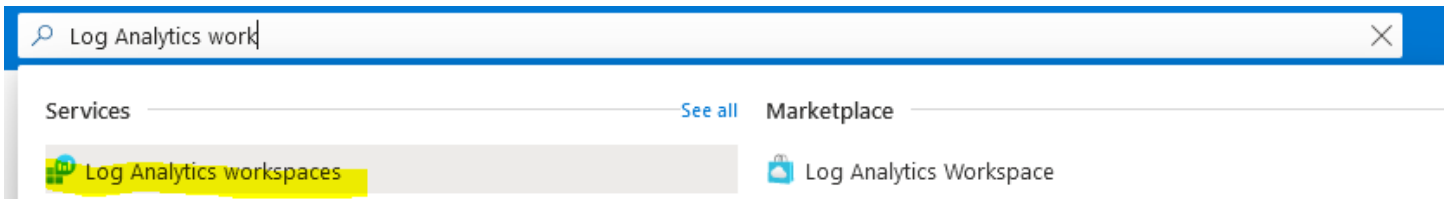


Figure 66 Log Analytics workspaces

- 3) Press **Add**
- 4) Fill in the 'Basics' blade.

The **Region** should be the same as where your (A)AD DS deployment resides.

- 5) Press **Review + Create**
- 6) Press **Create**
- 7) Wait for the deployment to complete
- 8) Press **Go to resource** or navigate to the created Log Analytics workspace
- 9) Press **Agents management**, depicted below:

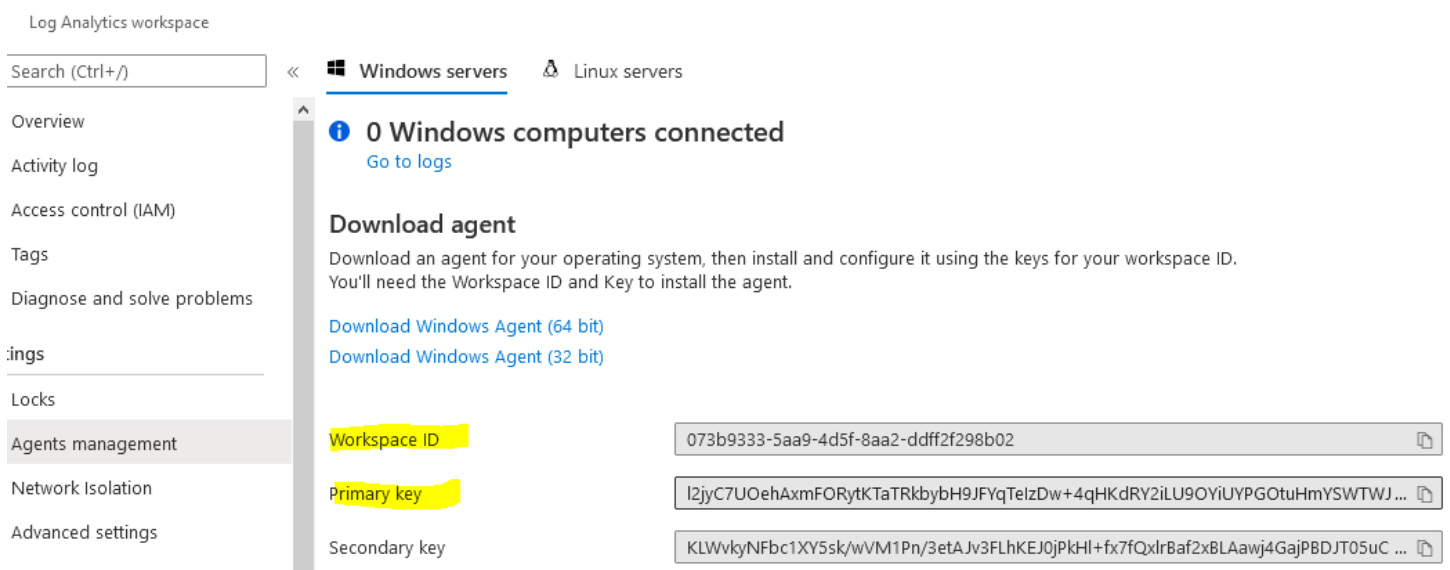


Figure 67 Agents management

- 10) Copy and save the 'Workspace ID', this will be required later.
- 11) Copy and save the 'Primary Key', this will be required later.

9.1.5 Prepare Custom workflows

Now that the Storage account has been prepared the custom workflow (PowerShell scripts) templates need to be prepared and placed in the Storage account. Ensure that you have access to the templates called 'wvd_hostpooljoin.ps1' and 'wvd_opmanagement.ps1' before continuing.

wvd_hostpooljoin.ps1

- 1) Open 'wvd_hostpooljoin.ps1' in a text editor
- 2) The following variables need to be defined to adjust the template to your Azure environment:

SVP_App_ID: Provide the previously created WVD service principal Application ID

SVP_Password: The password for the WVD service principal

AzureAD_Tenant_ID: Provide the Azure AD tenant/directory ID, this can be located by following the steps below:

- 3) Log in on the Azure Portal (for example: portal.azure.com) with your administrator account
- 4) Search for 'Azure Active Directory' in the upper search bar and press the corresponding service

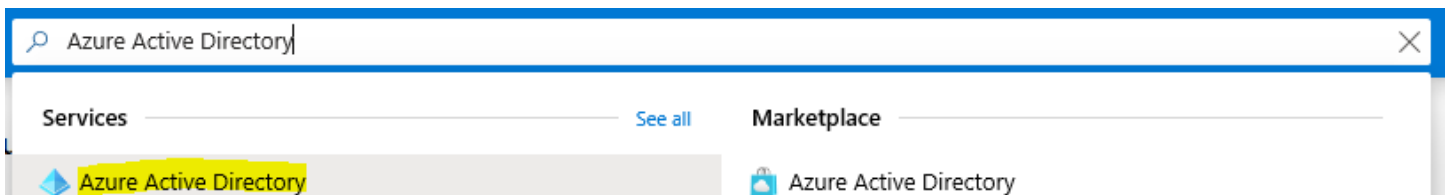


Figure 68 Azure AD

- 5) Press **Properties**
- 6) Copy the 'Directory ID' as depicted below:

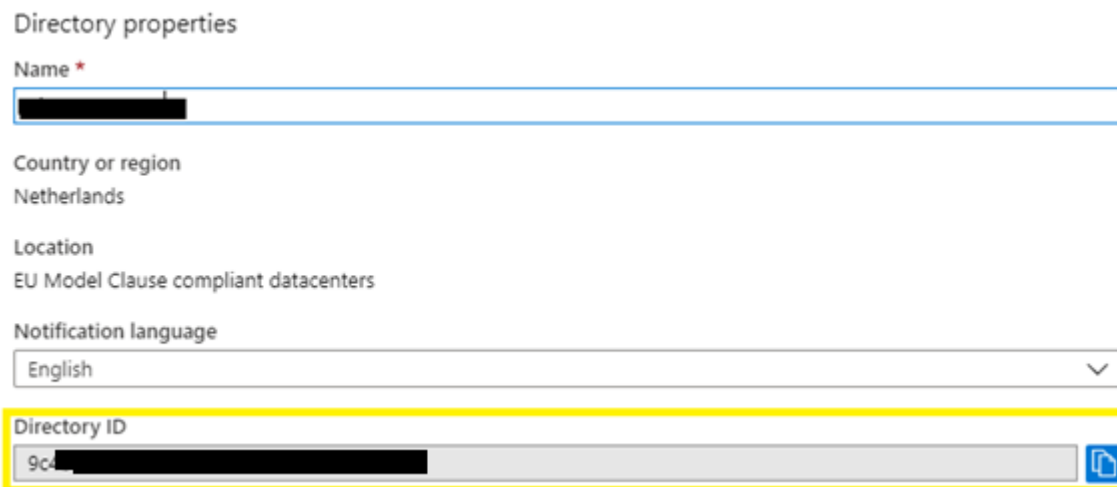


Figure 69 Azure AD Directory ID

WVD_Hostpool_RG: Provide the name of the Resource Group where the WVD back-end resources were previously (Chapter 4) deployed to

WVD_Hostpool: Provide the name of the previously created (Chapter 4) WVD Host pool

Az_Sub_Id: Provide the Azure subscription ID/string, previously gathered at the end of Chapter 4

Storage_Acc_Name: Provide the name of the previously created Storage account

Container_Name: Provide the name of the previously created container in the Storage account specified above.

Blob_Name: Provide the file name of the operational maintenance script. It is recommended to leave this default at 'wvd_opmanagement.ps1', as it will be referenced later.

Log_Analytics_Workspace_ID: Provide the previously noted Workspace ID

Log_Analytics_Workspace_Key: Provide the previously noted (Workspace) Primary key

- 7) After the variables have been defined to match your Azure environment, save the file. It is recommended to **not** change the name, as it will be referenced later.

wvd_opmanagement.ps1

- 8) Open 'wvd_opmanagement.ps1' in a text editor
- 9) The top 6 variables can be copied from the previously edited 'wvd_opmanagement.ps1'.
- 10) The remaining 5 variables need to be defined to adjust the template to your Azure environment:

Domain_Username: To be able to automatically remove computer objects from (A)AD DS an account with permissions to do so needs to be declared here. This ensures no stale computer objects are left behind when a VMSS instance (WVD session host) is removed manually or scaled in automatically. Specify the UPN of an account that will perform the domain join/removal operation for the WVD session hosts. Keep in mind that the UPN as specified in Azure AD or Active Directory Users & Computers must be used. The figure below is an example of the latter:

User logon name:

@TheATeamNL.onmicrosoft.cor
▼

Figure 70 Example UPN

Critical note: Keep in mind that this account will effectively be a service account. As such it is highly recommended to not let its password expire and to limit its permissions to joining & removing computer objects from Active Directory.

Domain_Password: The password for the account stated in **Domain_Username**

Title: When a VMSS instance (WVD session host) is to be terminated (removed manually or scaled in automatically) the relevant users will receive a message 10 and 5 minutes before hand. Define the title of the message users will be confronted with.

Body1: Define the body/content of the message users will be confronted with 10 minutes before termination.

Body2: Define the body/content of the message users will be confronted with 5 minutes before termination.

11) After the variables have been defined to match your Azure environment, save the file. It is recommended to **not** change the name, as it will be referenced later.

Now that both 'wvd_hostpooljoin.ps1' and 'wvd_opmanagement.ps1' have been adjusted to match your Azure environment they need to be uploaded to the previously created Blob container.

12) Log in on the Azure Portal (for example: portal.azure.com) with your administrator account

13) Search for 'Storage accounts in the upper search bar and press the corresponding service

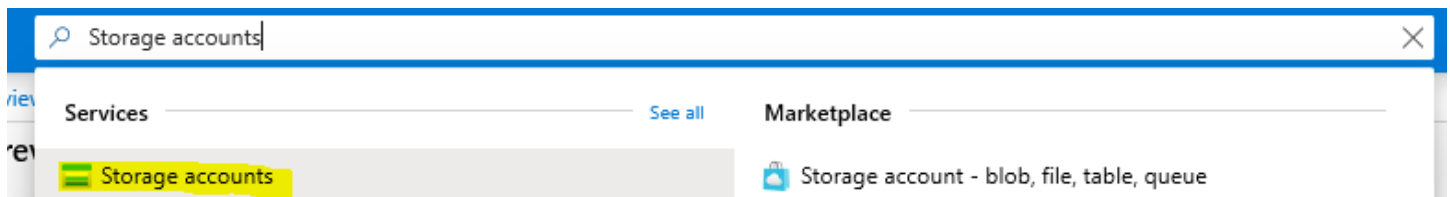


Figure 71 Storage accounts

14) Press the previously created Storage account

15) Press **Storage Explorer**

16) Press the previously created container

17) Press **Upload**, as depicted below:

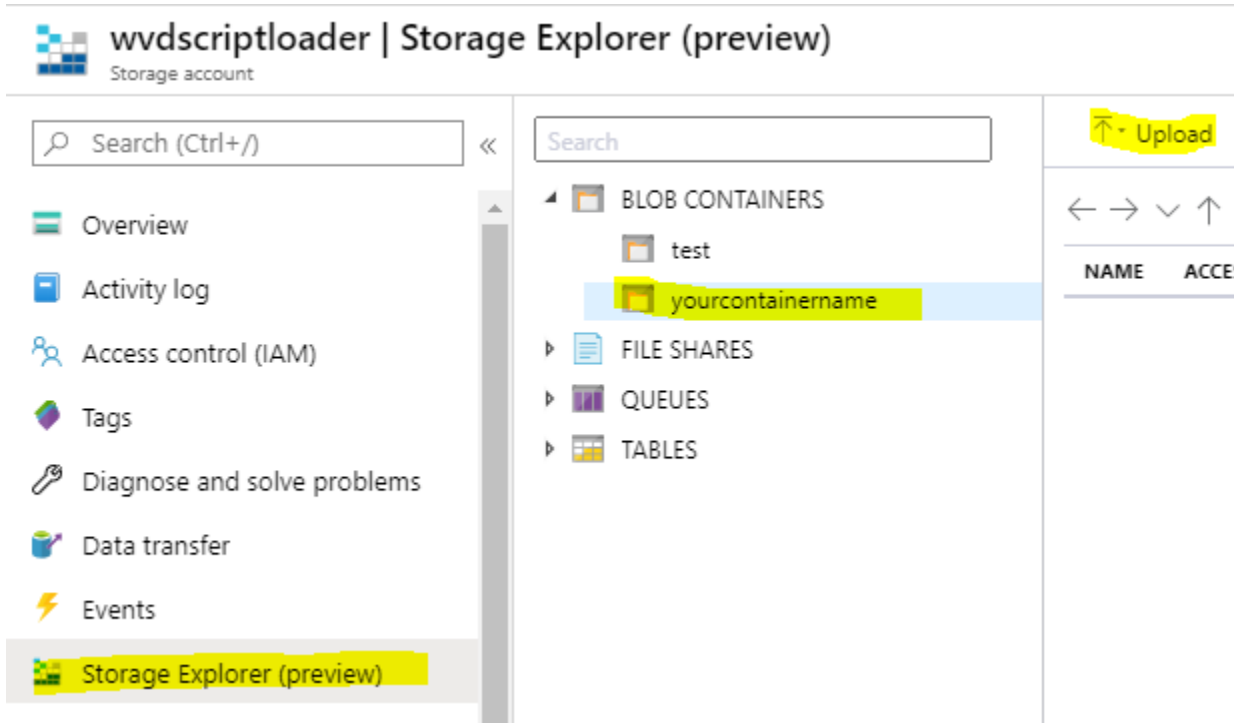


Figure 72 Storage Explorer - Blob container

18) Press the browse icon (depicted below) and select both 'wvd_hostpooljoin.ps1' and 'wvd_opmanagement.ps1'.

19) Press **Upload**

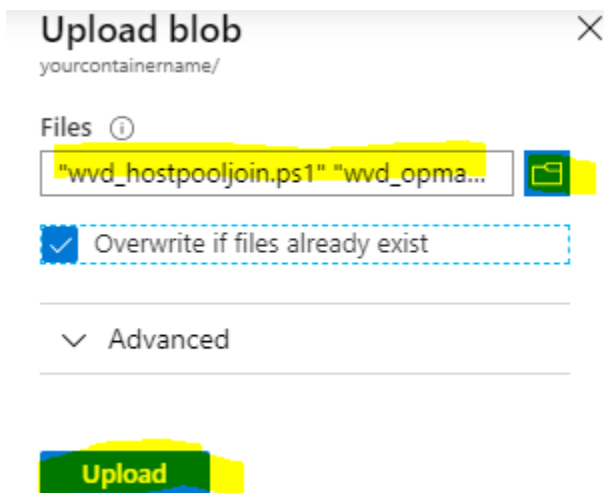


Figure 73 Storage account upload

20) Verify both files are uploaded successfully.

9.1.6 Deploy ARM Template

To deploy the Virtual Machine Scale Set (VMSS) easily an Azure Resource Manager (ARM) template has been developed. These steps will explain how to adjust the template to your Azure environment and subsequently deploy it.

Ensure you have access to (a local copy of) 'wvd_vmss_arm_template.json'.

- 1) Log in on the Azure Portal (for example: portal.azure.com) with your administrator account
- 2) Search for 'Template specs' in the upper search bar and press the corresponding service

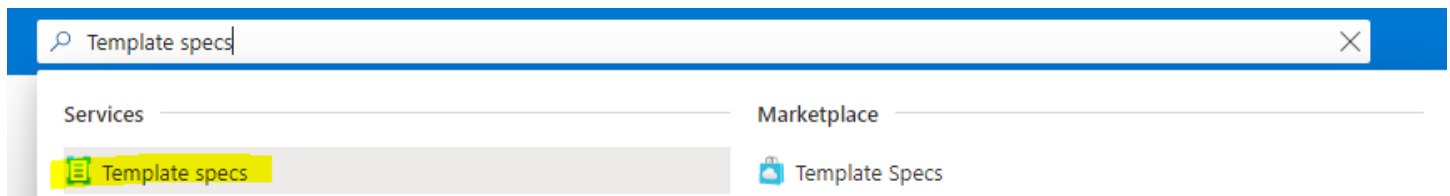


Figure 74 Templates

- 3) Press **Import template**
- 4) Select the 'wvd_vmss_arm_template.json' file
- 5) Press **Import**
- 6) Fill in the 'Basics' page, depicted below:

Basics Edit Template Tags Review + Create

Name * ✓

Subscription * ▼

Resource Group * ▼
[Create new](#)

Location * ▼

Description ✓

First version

Basic info about the first version of the template spec. The template you provide in the next step will be used for the first version of this template spec.

Version * ✓

Change notes

Figure 75 WVD VMSS ARM Template

- 7) Press **Review + Create**
- 8) Press **Create**
- 9) Press the recently created Template spec
- 10) Press **Deploy**

You will be confronted with the deployment screen. The following parameters must be defined for the deployment to succeed:

Resource Group: Select (or create) a Resource Group where the VMSS (the WVD Session hosts) will be deployed to. The region of the Resource Group will decide the deployment's Azure region/location, ensure this is the same region as your (A)AD DS deployment.

Virtual Machine Scale Set Name: Specify a (new) name for the Virtual Machine Scale Set

Virtual Network ID: Specify the resource ID of the Virtual Network where your (A)AD DS deployment is present. Follow the steps below to find the resource ID:

- 11) Log in on the Azure Portal (for example: portal.azure.com) with your administrator account
- 12) Search for 'Virtual Networks' in the upper search bar and press the corresponding service

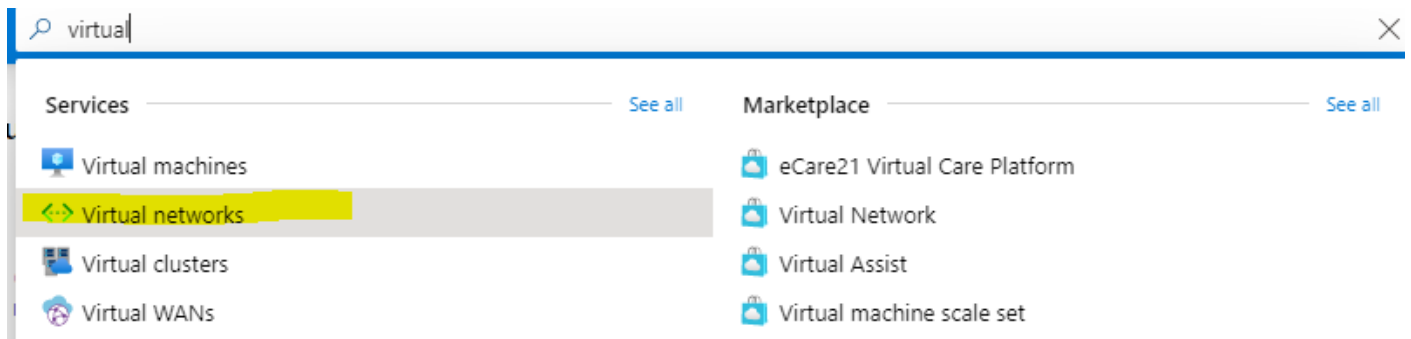


Figure 76 Search Virtual Network

- 13) Press the relevant VNet's name
- 14) Press **Properties**
- 15) Copy the 'Resource ID' as depicted below:

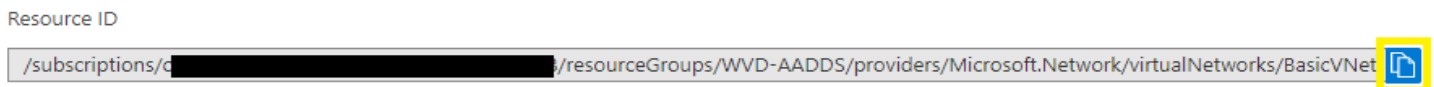


Figure 77 VNet Resource ID

Subnet Name: Specify the subnet name within the VNet. To view available subnets within the VNET follow the steps below:

16) Press **Subnets**

17) Take note of the name of the subnet where the WVD session hosts will be deployed to, as depicted below:

Name	Address range	IPv4 av.
GatewaySubnet	192.168.0.0/24	251
SUBNET-01-PL	192.168.1.0/24	251
SUBNET-02-BL	192.168.2.0/24	249
SUBNET-03-IL	192.168.3.0/24	248
SUBNET-04-DL	192.168.4.0/24	251
AzureBastionSubnet	192.168.5.0/24	250

Figure 78 VNet Subnets

Session Host Computer Name Prefix: Specify a name prefix for the computer names of the VM instances. This may be no longer than 9 characters, ensure this is the case or an error will be thrown later.

New Local Admin Username: Specify a name for the (new) local administrator which will be created on all VM instances.

New Local Admin Password: Specify a password for the local administrator.

Storage Account Name: Specify the Storage Account name, where the scripts (.ps1 files) have been saved in. Navigate to the Storage Account in the Azure portal to verify its name.

Figure 79 Storage Account Name

Storage Account Key: Specify the Storage Account Key. Navigate to the Storage Account in the Azure portal and press the tab 'Access keys', then copy the value from 'Key' depicted below (market in yellow).

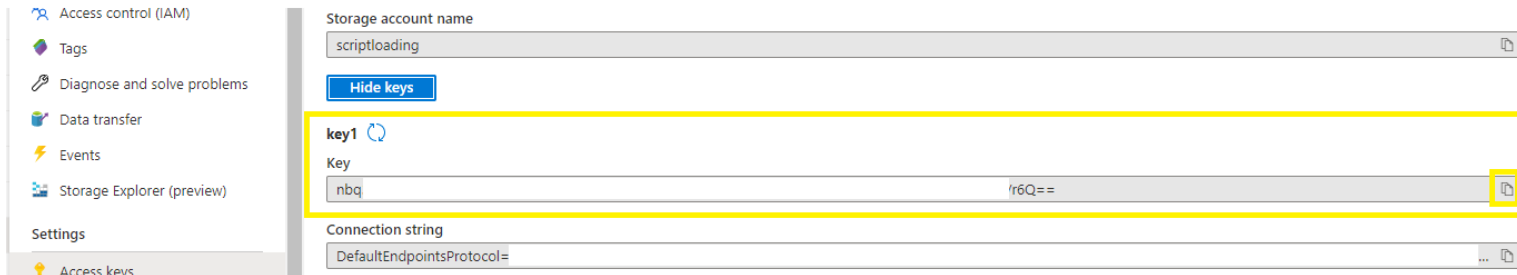


Figure 80 Storage Account Access Key

Storage Account URI: Specify the URI to the 'wvd_hostpooljoin.ps1' file stored in the Storage Account.

- 18) Navigate to the Storage Account in the Azure portal
- 19) Press **Storage Explorer**
- 20) Press **Blob Containers**
- 21) Press the container which stores the 'wvd_hostpooljoin.ps1' file
- 22) Select the file
- 23) Press **Copy URL**, as depicted below:

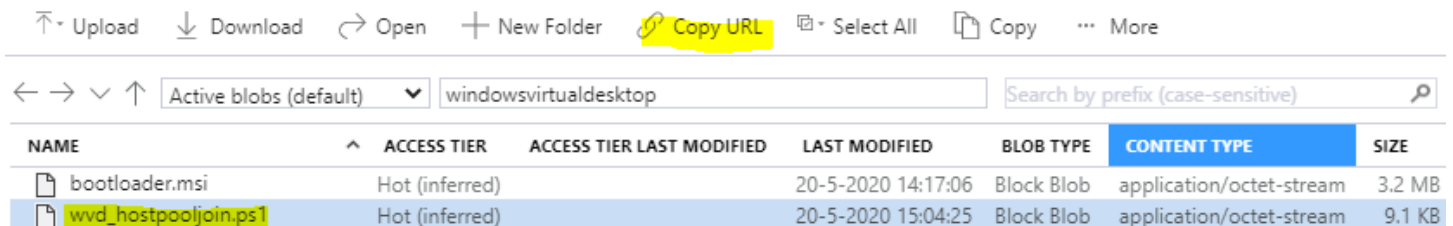


Figure 81 Storage Account URI

24) Paste the URL in the 'Storage Account URI' parameter field. An example is:

'https://scriptloading.blob.core.windows.net/windowsvirtualdesktop/wvd_hostpooljoin.ps1'

Storage Account URI: Specify the script name. For example:









Figure 82 Specify Host pool join script name

Domain To Join: Specify the (full) domain name (FQDN) that the WVD session hosts will be joined to. In case of Azure AD DS you can navigate to it via the Azure portal to find the domain name. Marked in yellow below:

Azure AD Domain Services

The A Team NL

+ Add  Manage view  Refresh  Export to CSV  Open query |  Assign tags |  Feedback

Filter by name... Subscription == IMMechaniX Resource group == (all) X Location == (all) >

Showing 1 to 1 of 1 records.

<input type="checkbox"/>	Name 	Type 
<input type="checkbox"/>	 ingram.micro	Azure AD Domain Services

Figure 83 Azure AD DS - Domain name

Ou Path: Optionally, specify an OU path where the (AD) Computer objects of the WVD session hosts will be placed in. For example:

Ou Path

Figure 84 WVD session hosts OU path

Domain Username: Specify the UPN of an account that will perform the domain join/removal operation for the WVD session hosts. It is recommended to use the same account that was specified earlier in the custom workflows. Keep in mind that the UPN as specified in Azure AD or Active Directory Users & Computers must be used. The figure below is an example of the latter:

User logon name:
 @TheATeamNL.onmicrosoft.cor 

Figure 85 Example UPN

Critical note: Keep in mind that this account will effectively be a service account. As such it is highly recommended to not let its password expire and to limit its permissions to joining & removing computer objects from Active Directory.

Domain Password: Specify the password of the previously specified account.

Vm Size: Specify the sizing of the VM instances that will be created later. The list in the ARM template is only a small selection of available choices. Later in the guide the VM sizing will be double checked (before actually creating VM instances) and can be changed if desired. At that point the entire VM sizing catalogue can be accessed.

Os License Type: Specify whether you will be using a Windows Server or Windows Client (7, 8, 10 etc.) image for WVD session hosts. Both Server and Client type will ensure no Windows OS license costs are charged for the WVD session host VM instances.

Use Availability Zones: Specify 'Yes' to equally distribute VM instances among the 3 Availability zones (Azure datacenter sites) in an Azure region (specified earlier in the 'Location' parameter field). Ensure Availability zones are supported in the selected Azure region when specifying 'Yes'.

For more information regarding Availability zones consult the sources below:

<https://docs.microsoft.com/en-us/azure/availability-zones/az-overview>

<https://azure.microsoft.com/en-us/pricing/details/bandwidth/>

Os Disk Tier:

There are 3 choices available to host the OS disk on (128GB):

StandardSSD_LRS

This is a Standard SSD (Azure Managed Disk).

Premium_LRS

This is a Premium SSD (Azure Managed Disk).

Ephemeral

This hosts the OS disk on ephemeral storage. This means the OS disk will be hosted on the temporary (local) storage of the physical hypervisor host, which subsequently means storage is accessed very fast and with a high amount of IOPS. The downside is that the storage will be emptied when the physical hypervisor host is restarted or the VM is moved to another host (fail over), i.e. the storage is not persistent and will revert back to the state of the (OS) image after a failover or redeployment. For more information on Ephemeral storage consult the source below:

<https://docs.microsoft.com/en-us/azure/virtual-machines/ephemeral-os-disks>

Selecting the option 'Ephemeral' will change the VM sizing to E8s_v3 regardless of what was specified in the 'Vm Size' parameter field, to ensure enough temporary storage is available to host the OS image on. Later in the guide the VM sizing will be double checked (before actually creating VM instances) and can be changed if desired.

Image Definition Id: Specify the Image definition ID that was gathered earlier when setting up the Shared image gallery.

Log Analytic Workspace Id: Provide the previously noted Workspace ID

Log Analytic Workspace Key: Provide the previously noted (Workspace) Primary key


25) Press **Review + Create**

26) Press **Create**














9.1.7 Verify VM Instance sizing

After the VMSS has been deployed successfully the VM instance sizing can be changed, if desired.

- 1) Log in on the Azure Portal (for example: portal.azure.com) with your administrator account
- 2) Navigate to 'Virtual Machine Scale Sets'
- 3) Select the recently created VMSS
- 4) Press **Size**
- 5) Verify if the 'Current size' value is set to your preference
- 6) If change is desired, press **See all sizes** (as depicted below)

 Most used sizes by Azure users

Showing 12 of 380 VM sizes. | Subscription: IMMechaniX | Region: West Europe | **Current size: Standard_D2s_v3** | [Learn more about VM sizes](#)

VM Size ↑↓	Family ↑↓	vCPUs ↑↓	RAM (GiB) ↑↓	Data disks ↑↓	Max IOPS ↑↓	Temp storage (GiB) ↑↓	Premium disk ↑↓	Cost/month ↑↓
DS1_v2 	General purpose	1	3.5	4	3200	7	Supported	Unavailable
D2s_v3 	General purpose	2	8	4	3200	16	Supported	Unavailable
B2s 	General purpose	2	4	4	1280	8	Supported	Unavailable
B1s 	General purpose	1	1	2	320	4	Supported	Unavailable
B2ms 	General purpose	2	8	4	1920	16	Supported	Unavailable
B1ms 	General purpose	1	2	2	640	4	Supported	Unavailable
DS2_v2 	General purpose	2	7	8	6400	14	Supported	Unavailable
B4ms 	General purpose	4	16	8	2880	32	Supported	Unavailable
D4s_v3 	General purpose	4	16	8	6400	32	Supported	Unavailable
DS3_v2 	General purpose	4	14	16	12800	28	Supported	Unavailable
D8s_v3 	General purpose	8	32	16	12800	64	Supported	Unavailable
B1ls  	General purpose	1	0.5	2	160	4	Supported	Unavailable

[See all sizes](#)

Figure 86 VM Instance sizing

- 7) If change is desired, select a size and press **Resize**

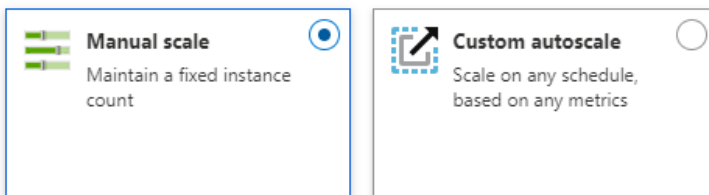
9.1.8 Deploy VM Instances

- 1) Navigate to the recently created VMSS
- 2) Press **Scaling**
- 3) Enter the desired instance count number, as depicted below:

Configure Scale-In Policy Run history JSON Notify Diagnostics settings

Autoscale is a built-in feature that helps applications perform their best when demand changes. You can choose to scale your resource manually to a specific instance count, or via a custom Autoscale policy that scales based on metric(s) thresholds, or scheduled instance count which scales during designated time windows. Autoscale enables your resource to be performant and cost effective by adding and removing instances based on demand. [Learn more about Azure Autoscale](#)

Choose how to scale your resource



Manual scale

Override condition

Instance count 0

Figure 87 VMSS Manual scaling

- 4) Press **Save**
- 5) Wait for the VM instances to be deployed successfully

If you would like to configure 'Custom autoscale' refer to chapter 14.2 Autoscaling with VM Scale Sets.

9.2 WVD Add session hosts wizard

- 1) Log in on the Azure Portal (for example: portal.azure.com) with your administrator account
- 2) Search for 'Windows Virtual Desktop' in the upper search bar and press the corresponding service

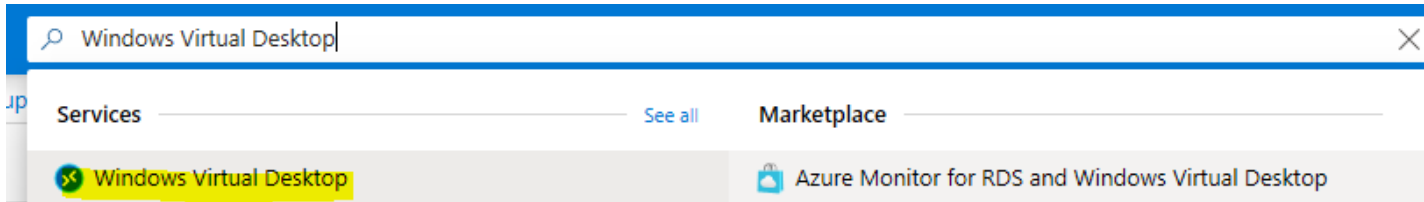


Figure 88 Windows Virtual Desktop

- 3) Navigate to the Host pool created earlier
- 4) Press **Registration key**, as depicted below

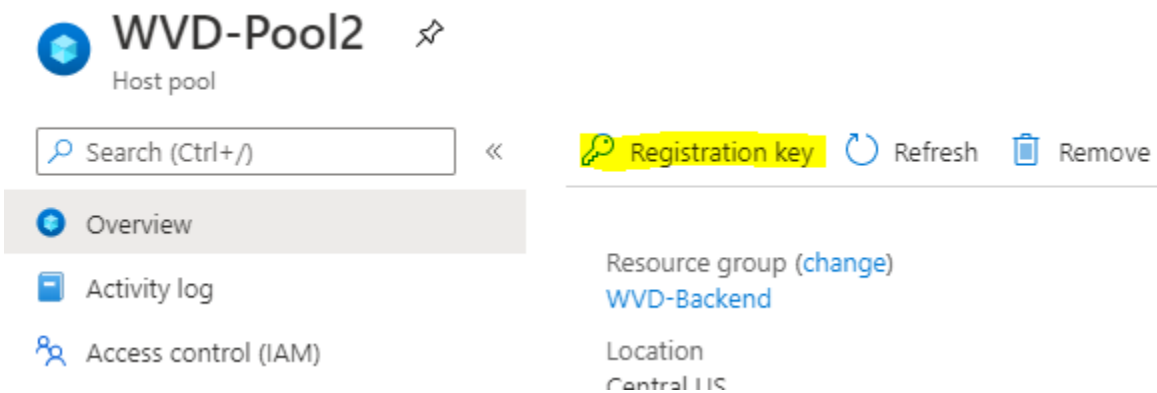



Figure 89 WVD Host pool registration key

- 5) Press **Generate new key**
- 6) Fill in an expiration date
- 7) Press **Ok**

 Generate new key

Generate a new registration key

Expiration date. Select between 1 hour and 27 days.

08/25/2020 	12:00:00 AM
--	-------------

OK	Cancel
-----------	--------

Figure 90 WVD Host pool join key

- 8) Back in the Host pool menu press **Session hosts**, as depicted below
- 9) Press **Add**

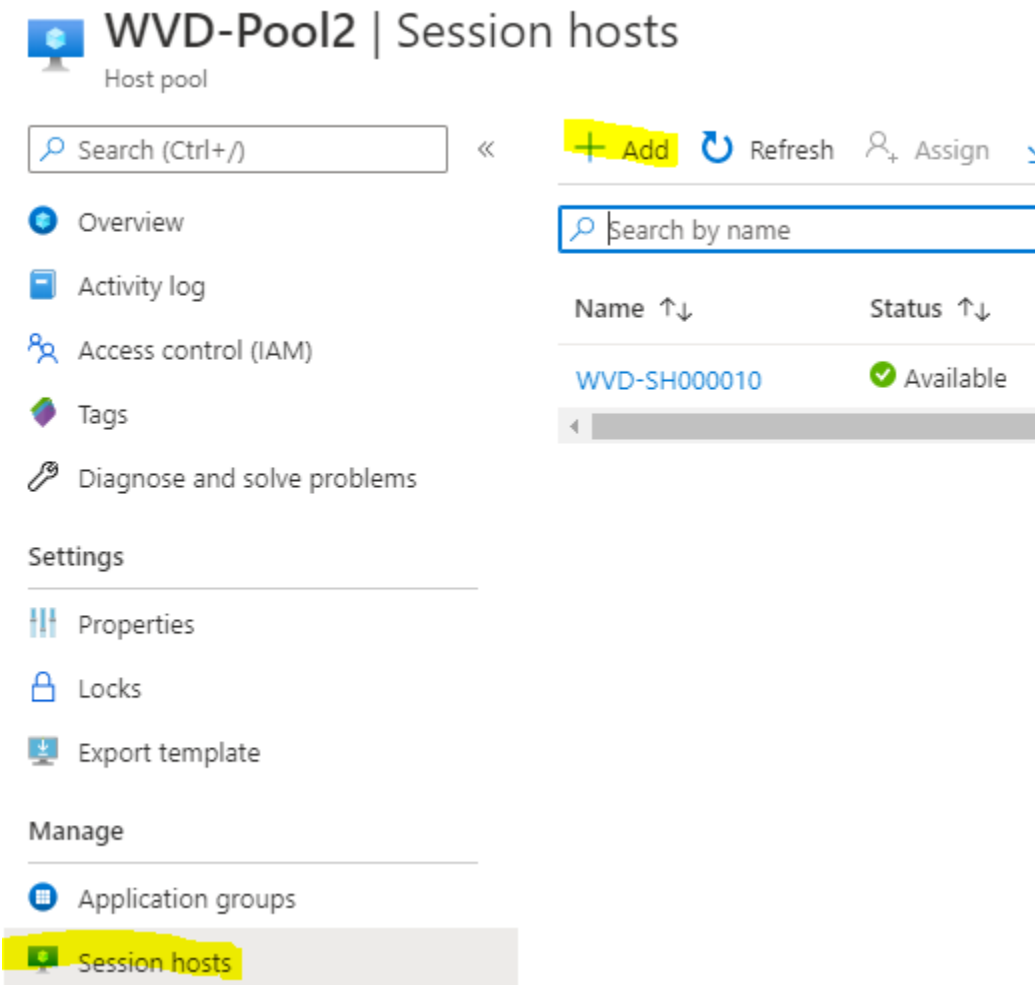


Figure 91 WVD Add session hosts

- 10) Press **Add**
- 11) Press **Next: Virtual Machines**
- 12) Fill in the required information

13) Pay close attention to the Network and Account settings as depicted below:

Network and security

Virtual network * ⓘ	BasicVNet
Subnet ⓘ	SUBNET-03-IL (192.168.3.0/24)
Public IP ⓘ	<input type="radio"/> Yes <input checked="" type="radio"/> No
Network security group ⓘ	None
Specify domain or unit ⓘ	<input checked="" type="radio"/> Yes <input type="radio"/> No
Domain to join * ⓘ	ingram.micro ✓
Organizational Unit path ⓘ	Optional
Administrator account	
AD domain join UPN * ⓘ	vmjoiner@contoso.com
Password * ⓘ	
Confirm password * ⓘ	

Figure 92 Add WVD session hosts

Virtual Network: Make sure to select the same VNet where your (A)AD DS was deployed in earlier.

Subnet: The WVD session hosts can be deployed in a different subnet than (A)AD DS, as long as the subnets can communicate with each other.

Public IP: WVD session hosts do not require a public IP address

Network Security Group (NSG): NSGs are easier to manage on a subnet level than on individual VM level, which is why we recommend stating 'None' here. For more information on configuring NSGs please request our Ingram Micro Azure Basic Networking Guide.

Domain to join: Present the full name of the AD DS domain

Organizational Unit Path: Optionally, specify an OU path where the (AD) Computer objects of the WVD session hosts will be placed in. For example:

Ou Path

OU=WVD SHs,DC=ingram,DC=micro

Figure 93 WVD session hosts OU path

Administrator account:

Specify the UPN of an account that will perform the domain join/removal operation for the WVD session hosts. It is recommended to use the same account that was specified earlier in the custom workflows. Keep in mind that the UPN as specified in Azure AD or Active Directory Users & Computers must be used. The figure below is an example of the latter:

User logon name:

adjoin @TheATeamNL.onmicrosoft.cor

Figure 94 Example UPN

- 14) Press **Create + Review**
- 15) Press **Create**
- 16) Wait for the VMs to be deployed

After the deployment has finished successfully the VMs (WVD Session hosts) can be found in the specified Host pool.

10 Publish RemoteApps

Instead of publishing a full desktop to WVD users it is also possible to publish specific applications, as long as they are installed on the VM (Instances) in a WVD Host pool.

- 1) Log in on the Azure Portal (for example: portal.azure.com) with your administrator account
- 2) Search for 'Windows Virtual Desktop' in the upper search bar and press the corresponding service

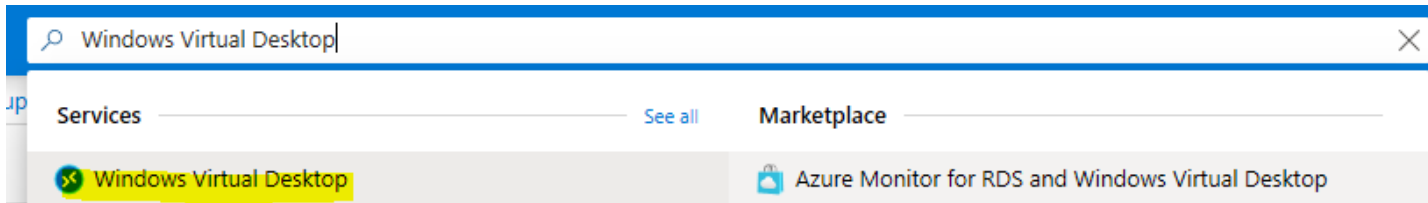


Figure 95 Windows Virtual Desktop

- 3) Press **Application Groups**
- 4) Press **Add**
- 5) Fill in the 'Basics' blade
- 6) Press **Next: Assignments**
- 7) Press '+ Add Azure AD users or user groups' to grant users access to the Application Group
- 8) Press **Next: Applications**
- 9) Press 'Add Applications'
- 10) Fill in the required information as depicted below:

Keep in mind that in 'Application source' you can either pull an application from the Windows start menu or state a file path to the application that will be published.

Add application ×

Select an application from your start menu or add from a file path.

Application source *	Start menu ▼
Application *	Snipping Tool ▼
Display name	Snipping Tool ✓
Description	<div style="border: 1px solid #ccc; height: 100px;"></div>
Application path ⓘ	C:\windows\system32\SnippingTool.exe
Icon path	C:\windows\system32\SnippingTool.exe
Icon index	0
Require command line	<input checked="" type="radio"/> No <input type="radio"/> Yes

Figure 96 Add Applications

- 11) Optionally: Set 'Require command line' to 'Yes' if you would like to insert parameters (arguments, switches etc.) for the application when users start it.
- 12) Press **Save**

13) Verify that the application is visible in the list depicted below:

Basics Assignments Applications Workspace Tags Review + create

Add applications to this application group. You can always add or manage applications any time later.

Name ↑↓	File path ↑↓	
Snipping Tool	C:\windows\system32\SnippingTool.exe	

[+ Add applications](#)

Figure 97 Application added

14) Press **Next: Workspaces**

15) Select 'Yes' on 'Register application group' to register it with a WVD workspace.

If you select 'No' you will have to do this manually later (in Workspaces) as the users will not be able to see the RemoteApps until the Application Group is registered to a Workspace.

Basics Assignments Applications Workspace Tags Review + create

To save some time, you can register the default desktop application group from this host pool, with a new or pre-existing workspace.

Register application group No Yes

Register application group ⓘ ▼

i Another application group in WVD-Pool2 has already been registered, so this app group will also be registered to that same workspace.

Figure 98 Add Application Group to Workspace

16) Press **Review + Create**

17) Press **Create**

11 Assign licenses

Now that the host pool has been successfully created it is time to create a user, assign the proper licenses and connect to the Windows Virtual Desktop.

Critical note: if you are using traditional AD DS the users will have to be synchronized to Azure AD using Azure AD Connect before continuing. Refer to Chapter 1 for details.

To be compliant with Microsoft licensing demands it is important to assign the proper licenses. A license for WVD is required, and an Azure AD Premium license is recommended as you are likely to make use of Multi-Factor Authentication and/or Azure AD Conditional Access in a live environment. Consult the following source for WVD qualifying licenses:

<https://azure.microsoft.com/en-us/pricing/details/virtual-desktop/>

TYPE	DESCRIPTION	ELIGIBILITY
Virtualize Windows 10 and Windows 7	Access Windows 10 Enterprise and Windows 7 Enterprise desktops and apps at no additional cost if you have an eligible Windows or Microsoft 365 license. Get free Extended Security Updates until January 2023 for your Windows 7 virtual desktop—offering more options to support legacy apps while you transition to Windows 10.	You are eligible to access Windows 10 and Windows 7 with Windows Virtual Desktop if you have one of the following per user licenses*: <ul style="list-style-type: none"> • Microsoft 365 E3/E5 • Microsoft 365 A3/A5/Student Use Benefits • Microsoft 365 F3 • Microsoft 365 Business Premium** • Windows 10 Enterprise E3/E5 • Windows 10 Education A3/A5 • Windows 10 VDA per user
Virtualize Windows Server	Access desktops powered by Windows Server Remote Desktop Services desktops and apps at no additional cost if you are an eligible Microsoft Remote Desktop Services (RDS) Client Access License (CAL) customer.	You are eligible to access Windows Server 2012 R2 and newer desktops and apps if you have a per-user or per-device RDS CAL license with active Software Assurance (SA).

Figure 99 WVD licensing

For more details and information on Microsoft licenses please fill in the form below to receive the Microsoft CSP portfolio via Ingram Micro. This includes exact details on all licensing options:

<https://www.ingrammicrocloud.com/nl/nl/blogs/het-microsoft-csp-portfolio-van-ingram-micro/>

- 1) Log in on the Azure Portal (for example: portal.azure.com) with your administrator account
- 2) Search for 'Azure Active Directory' in the upper search bar and press the corresponding service

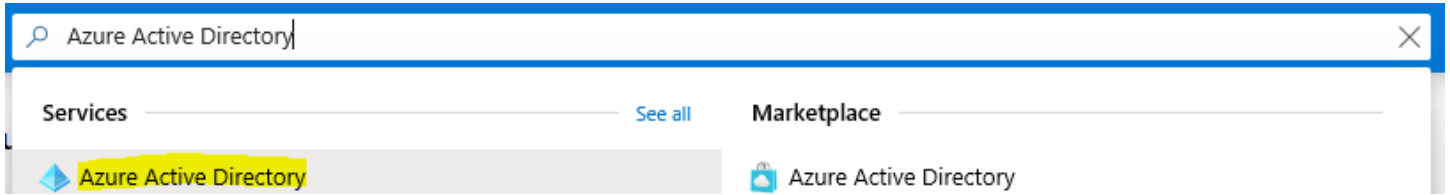


Figure 100 Azure AD

- 3) Press **Users**, if you want to assign licenses to users. Press **Groups** if you want to assign licenses to groups.
- 4) Select a user or group
- 5) Assign the required/chosen license to the user by pressing **Licenses** and subsequently **Assignments**, as depicted below:

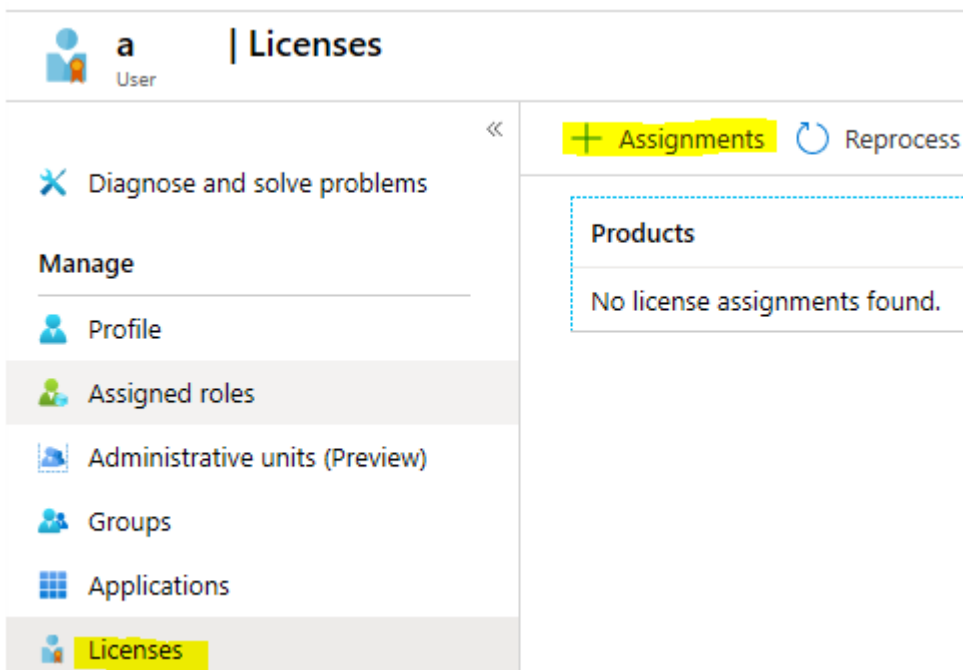


Figure 101 Azure AD licenses

12 Access WVD

Now that all the required steps have been taken it is time to log in to WVD. There are two ways to access your WVD solution: through a HTML5 web client or a downloadable client application.

WVD Web client URL (HTML5):

<https://rdweb.wvd.microsoft.com/arm/webclient>

WVD (RemoteDesktop) Client instructions:

<https://docs.microsoft.com/nl-nl/azure/virtual-desktop/connect-windows-7-10#install-the-windows-desktop-client>

Log in using the access method of your choice with the previously created user and select the Application Group created earlier to access the WVD published desktop.

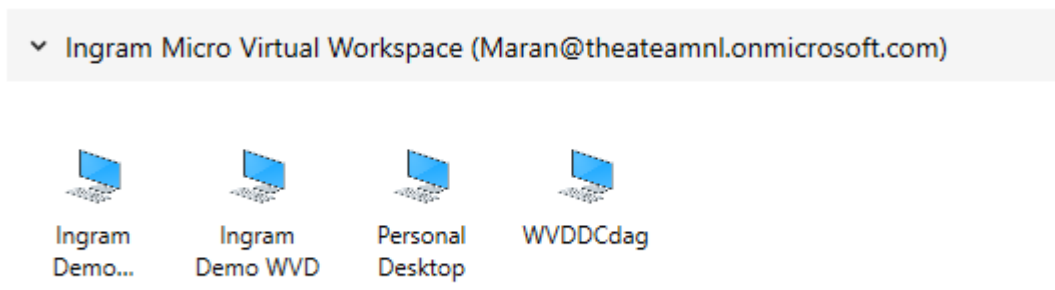


Figure 102 WVD Application Groups

Keep in mind that the region of the WVD Control plane for the end user is assigned based on the DNS server that the end user has configured on his/her workstation. For example, a user in the Netherlands that has an American DNS server configured on his workstation will have his RDP connection routed through the WVD Control plane in America, regardless of the WVD session hosts being located in West-Europe (the Netherlands).

The 'Windows Virtual Desktop Experience Estimator' can be consulted below to find the most fitting Azure region for your location:

<https://azure.microsoft.com/en-us/services/virtual-desktop/assessment/>

13 Deploy FSLogix Profile Containers

FSLogix Profile Containers are a user profile solution which encapsulates the entire profile and saves this in a container (a virtual hard disk) that is mounted to the user session when a user account signs on. This method prevents the traditional (storage) bottleneck because the profile is loaded on a bit-level rather than at a file-level. FSLogix Profile Containers can be stored on traditional/IaaS based file shares or on Azure Storage Accounts. This can either be a 'General Purpose V2' Storage Account or an 'FileStorage' Storage Account. The major difference with regards to storage is that the first will provide you with containers/blobs that contain the FSLogix Profile Containers while the latter is dedicated to Azure Files and will provide an Azure File Share that contains the FSLogix Profile Containers. The major difference with regards to security is that authentication on a General Purpose V2 storage account happens based on Access Keys while Azure Files also supports authentication based on AAD DS, effectively creating Identity based authentication.

Side note: Although General Purpose V2 accounts (standard performance tier) also support Azure Files this was not mentioned in the description above to emphasize the difference between storing FSLogix Profile Containers on container/blob-level and on File share-level.

Four different methods will be described in this chapter, only one is required:

13.1 AAD DS - Deploying FSLogix Profile Containers on (PaaS) Azure File shares

This method involves using Azure File Shares as a storage solution for FSLogix Profile Containers while authenticating based on user identities (from Azure AD Domain Services).

13.2 Traditional AD DS - Deploying FSLogix Profile Containers on (PaaS) Azure File shares

This method involves using Azure File Shares as a storage solution for FSLogix Profile Containers while authenticating based on user identities (from traditional/IaaS AD Domain Services).

13.3 Deploying FSLogix Profile Containers on (IaaS) File shares

This method involves using a traditional/IaaS file share as a storage solution for FSLogix Profile Containers while authenticating based on user identities from (from Azure AD Domain Services or traditional/IaaS AD Domain Services).

13.4 **!!DEPRECATED!!** Deploying FSLogix Profile Containers in Blob Storage

This method involves using Azure Blob storage as storage solution for FSLogix Profile containers. This method has been discontinued because performance is slightly slower, takes up (temporary) storage space on the session hosts (whereas profiles are 100% streamed when using file shares) and costs are disproportionately larger because of page blob provisioning.

13.1 AAD DS - Deploying FSLogix Profile Containers on (PaaS) Azure File shares

Azure AD DS (AAD DS) support for Azure File Shares is Globally Available. Refer to the steps below to configure this:

- 1) Log in on the Azure Portal (for example: portal.azure.com) with your administrator account
- 2) Create a Security Group called 'WVD_Users' (or similar name) in Azure AD
- 3) Add all WVD users to this Security Group
- 4) Search for 'Storage accounts' in the upper search bar and press the corresponding service

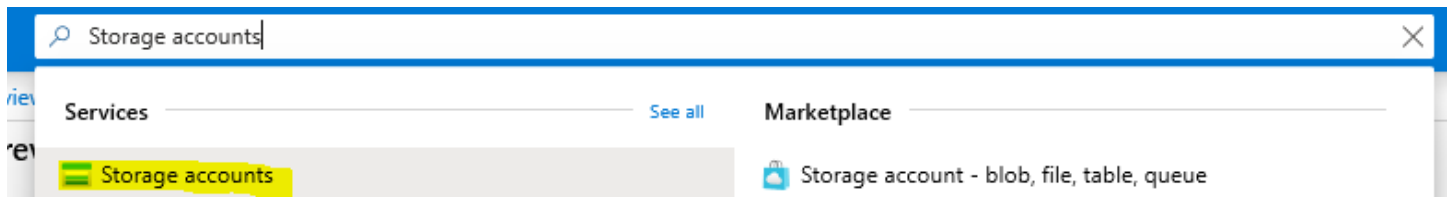


Figure 103 Storage accounts

- 5) Press **Add**
- 6) Fill in the 'Basics' blade as depicted on the next page:

Your storage account name needs to be (globally) unique and cannot contain special characters.

The **Location** should be the same as where your AAD DS deployment resides, for optimal performance.

Subscription *

Resource group * [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 * ⓘ

Location *

Performance ⓘ Standard Premium

Account kind ⓘ ⓘ This account kind allows you to create Azure file shares with premium performance characteristics that can be tailored to your needs. [Learn more about file storage](#)

Replication ⓘ ⓘ Accounts with the selected kind, replication, and performance type only support file shares. Blobs, tables, and queues will not be available.

Figure 104 Azure FileStorage Storage account

- 7) Press **Next: Networking**
- 8) Fill in the 'Networking' blade as depicted on the next page:

Select 'Public endpoint (selected networks)'. Alternatively select 'all networks', but the entire internet can try to authenticate with the Azure Storage Account then. These settings can be changed later. Select the **Virtual Network** where AD DS was previously deployed to (i.e. where the Domain Controllers are).

Select the **Subnet** where WVD session hosts will be deployed to. Select multiple subnets if you have a management VM in a different subnet than the WVD session hosts. VMs in the selected subnets will be able to make an authentication attempt with the Azure Storage Account but will still require (further) authorization before succeeding.

Basics **Networking** Advanced Tags Review + create

Network connectivity

You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

Connectivity method *

Public endpoint (all networks)
 Public endpoint (selected networks)
 Private endpoint

Virtual networks

Only the selected network will be able to access this storage account. [Learn more about service endpoints](#) ↗

Virtual network subscription ⓘ IMMechaniX ▾

Virtual network ⓘ BasicVNet ▾

[Create virtual network](#)
[Manage selected virtual network](#)

Subnets * ⓘ SUBNET-02-BL (192.168.2.0/24) ▾

Figure 105 Storage Account - Networking

- 9) Press **Review + Create**
- 10) Press **Create**
- 11) When done creating, navigate to your Storage account

12) Press **Networking**

Search (Ctrl+/) <<

- Overview
- Activity log
- Tags
- Diagnose and solve problems
- Access Control (IAM)
- Data transfer
- Storage Explorer (preview)
- Settings
 - Access keys
 - CORS
 - Configuration
 - Encryption
 - Shared access signature
 - Networking**
 - Properties
 - Locks

Firewalls and virtual networks Private endpoint connections

Save Discard Refresh

Allow access from
 All networks Selected networks

Configure network security for your storage accounts. [Learn more](#)

Virtual networks

+ Add existing virtual network + Add new virtual network

Virtual Network	Subnet	Address r.
> BasicVNet	4	

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. [Learn more.](#)

Add your client IP address ('83.8: ') ⓘ

Address range

IP address or CIDR

Exceptions

Allow trusted Microsoft services to access this storage account ⓘ

Allow read access to storage logging from any network

Figure 106 Storage Account - Networking

- 13) Select the 'Add your client IP address' checkbox, as depicted above
- 14) Verify that your desired VNet is listed, as depicted above
- 15) Finally, press **Save**
- 16) Press **Overview**
- 17) Note the Storage Account name, the Resource Group it is in and the Subscription ID. These 3 values will be required later.
- 18) Press **Configuration**
- 19) Set 'Azure Active Directory Domain Services (Azure AD DS)' to **Enabled**
- 20) Press **Save**
- 21) Press **File shares**
- 22) Press **+ File share**

23) State a name for the Azure file share

24) State the size quota of the file share in GiB. This amount will be billed, regardless of the actual amount of data placed on a file share. The size quota of the file share can be increased/decreased afterwards.

New file share ×

Name *

fslogixprofiles ✓

Sizing your file share:

- A premium file share is billed by provisioned share size, regardless of the used capacity.
- Share sizes can range from 100 GiB to 102,400 GiB.
- Provisioned share size is specified by share quota.
- IO and network bandwidth limits scale with the provisioned share size.

[Learn more](#)

Provisioned capacity * ⓘ

1024

GiB

Allowed IO/s ⓘ : **1024**

Burst IO/s ⓘ : **3072**

Egress Rate ⓘ : **121.4 MiBytes / s**

Ingress Rate ⓘ : **81.0 MiBytes / s**

Figure 107 Azure file share

25) Press **Create**

26) Navigate to the file share after creation is complete, as depicted below, and press **Connect**:

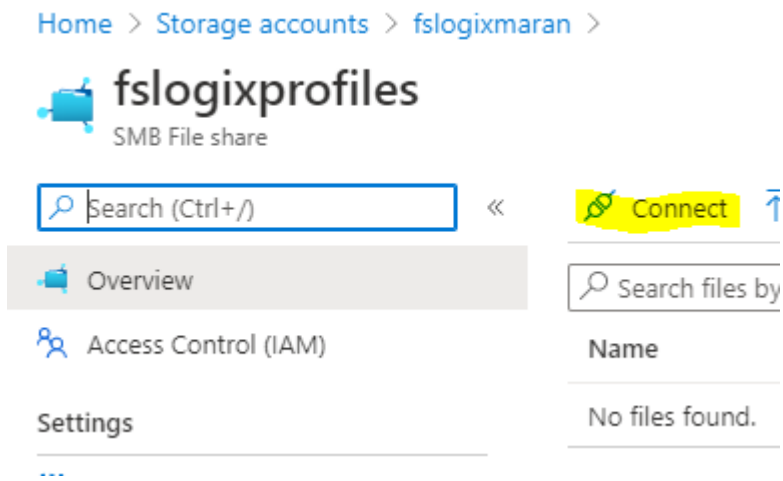


Figure 108 Azure file share

27) Press Copy (icon) next to the PowerShell connect code, as depicted below:

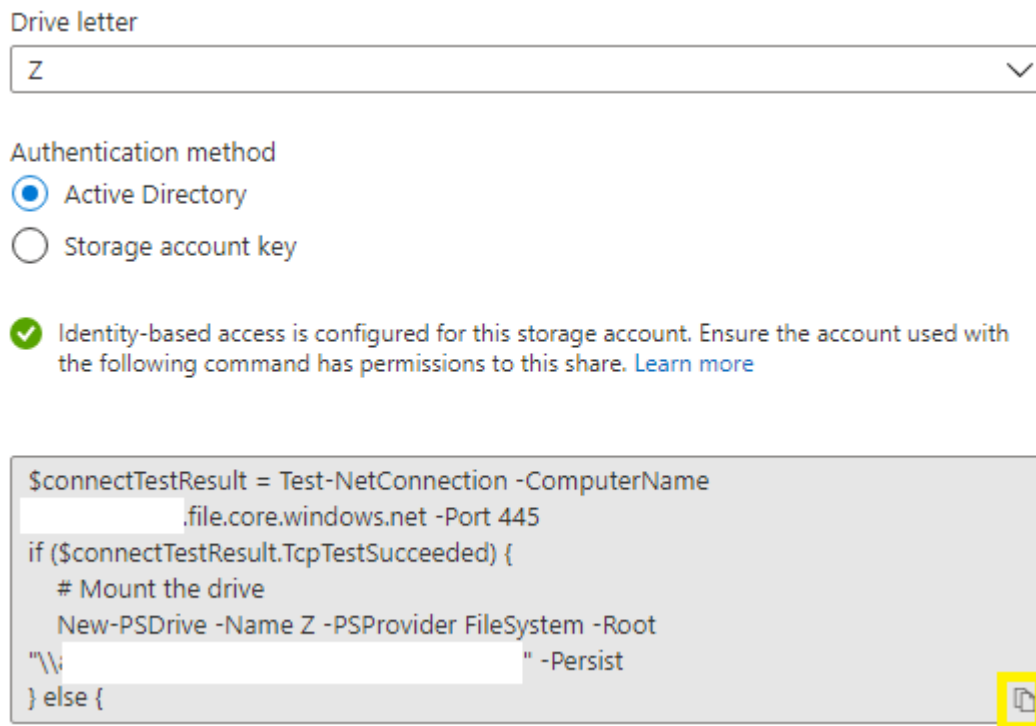


Figure 109 Azure file share mounting

28) Save the PowerShell connect code. This will be required later to set NTFS permissions.

- 29) Return to the Storage account 'Overview' blade (not of the File share)
- 30) Press **Access Control** -> **Add** -> **Add role assignment**

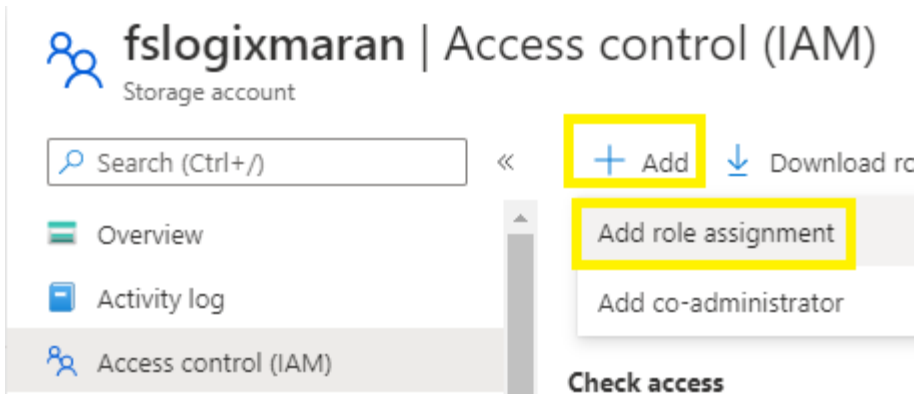


Figure 110 Storage account Access control

- 31) Select the role as depicted below:

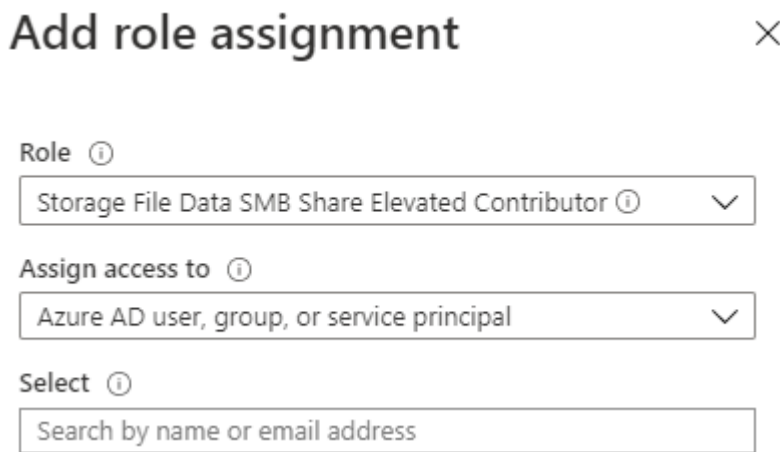


Figure 111 Storage account role assignment 1

- 32) Select an administrator account or group (under 'Select' as depicted above)
- 33) Press **Save**
- 34) If the administrator does not have the 'Owner' or 'Contributor' role assigned on the Storage Account (or Azure Subscription), assign that as well.

35) Add another role assignment to the Storage account, as depicted below:

Add role assignment ×

Role ⓘ
 Storage File Data SMB Share Contributor ⓘ

Assign access to ⓘ
 Azure AD user, group, or service principal

Select ⓘ
 WVD_Users

WV WVD_Users

Figure 112 Storage account role assignment 2

36) Select a group (or users) that will be working with FSLogix profiles (under 'Select' as depicted above)

The 'Storage File Data SMB Share Contributor' role will grant them 'Change' permissions (in terms of traditional file share permissions). Just as with traditional file share permissions they will be combined with NTFS permissions (will be set later on in the guide), where the most restrictive permissions will apply.

37) Press **Save**

38) Log in to a Domain Controller (via RDP or Azure Bastion for example) with the administrator account that was earlier granted the 'Storage File Data SMB Share Elevated Contributor' role.

39) Start PowerShell normally (**do not run as administrator**)

40) Run the PowerShell (connect) code/script that was saved earlier to connect to the Azure file share.

41) Open Windows File Explorer

42) Verify that Azure file share has been mounted as depicted below:

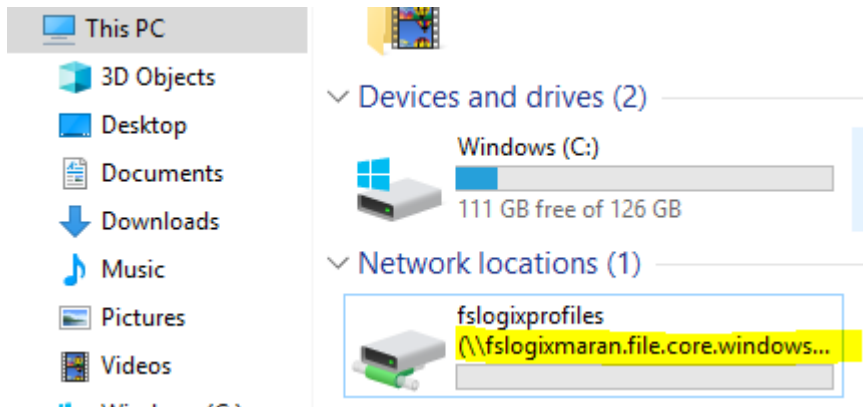


Figure 113 Azure file share in Windows

Now we can configure NTFS permissions. There are multiple ways to achieve a functioning FSLogix profile environment, this guide will execute Microsoft’s best practice regarding NTFS permissions for FSLogix.

- 43) Right mouse click on the Network Drive
- 44) Press **Properties**
- 45) Press **Security**
- 46) Press **Advanced**
- 47) Press **Disable inheritance** (will prevent warnings when removing/adding principals)
- 48) Configure the permissions to match the figure below (or equivalent):

Permissions	Share	Auditing	Effective Access	
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).				
Permission entries:				
Type	Principal	Access	Inherited from	Applies to
Allow	CREATOR OWNER	Full control	None	Subfolders and files only
Allow	Hybrid_Admins (INGRAM\Hy...	Full control	None	This folder, subfolders and files
Allow	WVD_Users (INGRAM\WVD_U...	Modify	None	This folder only

Figure 114 Required NTFS permissions

Note that in our example ‘Hybrid_Admins’ is an Azure AD Security Group synchronized to the AAD DS Domain. This group has been assigned the ‘Storage File Data SMB Share Elevated Contributor’ role on the Storage account. **Ensure at least one Hybrid AD Group/User has Full control permissions on the share at all times, to prevent losing access to the share entirely.**

Source:

<https://docs.microsoft.com/en-us/fslogix/fslogix-storage-config-ht>

- 49) Download the FSLogix Administrative Template for use with Group Policy Objects (GPOs) from the following URL and extract the ZIP file:
https://aka.ms/fslogix_download
- 50) Place the file called 'fslogix.admx' in C:\Windows\PolicyDefinitions (or an alternate SYSVOL location)
- 51) Place the file called 'fslogix.adml' in C:\Windows\PolicyDefinitions\en-US (or an alternate SYSVOL location)
- 52) Open 'Active Directory Users & Computers' and create a new OU (Organizational Unit) called 'WVD_Sessionhosts'. This will allow for a GPO that only targets relevant computers.
- 53) Move the WVD Session host computer objects to the previously created OU and close the interface
- 54) Open 'Group Policy Management'
- 55) Create a new GPO called 'FSLogix Profile Containers' and link it to the previously created OU
- 56) Edit the previously created GPO and navigate to 'Computer Configuration -> Policies -> Windows Settings -> Scripts -> Startup'
- 57) Press 'Browse files', this will open the source repository for startup scripts/installers. Take note of the location (UNC path) as this will be needed in the next step.
- 58) Locate the 'FSLogixAppsSetup.exe' file in the x64 folder (of the previously extracted ZIP file) and copy it to the location referred to in the previous step. This can be done manually or via PowerShell (example):

```
Copy-Item C:\Users\wvddc\Desktop\FsLogix_Apps_2.9.7349.30108\x64\Release\FsLogixAppsSetup.exe
"\\ingram.dc\SysVol\ingram.dc\Policies\{AA04BAEE-F461-42B5-B093-644BDD5060E7}\Machine\Scripts\Startup"
```

- 59) Return to the GPO
- 60) Press 'Add'
- 61) Press 'Browse', the 'FSLogixAppsSetup.exe' file should be visible in the File Explorer that is displayed
- 62) Select the 'FSLogixAppsSetup.exe' file and press 'Open' (or double click it)
- 63) Specify '/install /quiet' as Script Parameters
- 64) Press 'Ok', for reference see the figure below:

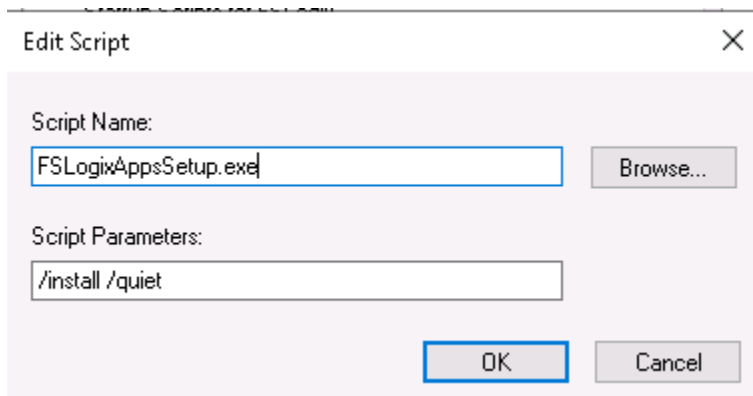


Figure 115 FSLogix Script Installer

- 65) Press 'Ok'. These settings will allow for FSLogix to be installed automatically on targeted computers.

66) Configure the remaining required settings according to the figure below:

Computer Configuration -> Policies -> Administrative Templates -> FSLogix -> Profile Containers	Configuration
Enabled	Enabled (with Options: 'Enabled' checkbox selected)
Size in MBs	50000 (a size cap for the FSLogix Profile Container, changing later requires a profile reset)
Delete local profile when FSLogix Profile should apply	Enabled (with matching checkbox selected)
Computer Configuration -> Policies -> Administrative Templates -> FSLogix -> Profile Containers -> Advanced	
Locked VHD retry count	Enabled -> 3
Locked VHD retry interval	Enabled -> 3
Computer Configuration -> Policies -> Administrative Templates -> FSLogix -> Profile Containers -> Container and Directory Naming	
SID directory name matching string	Enabled -> %userdomain%_%username%
SID directory name pattern string	Enabled -> %userdomain%_%username%
Virtual disk type	Enabled -> VHDX

Figure 116 FSLogix GPO Configuration

67) Navigate to: Computer Configuration -> Policies -> Administrative Templates -> FSLogix -> Profile Containers -> VHDLocation -> Network path to file share (depicted below)

Ensure the network path is in the following format:

`\\Yourstorageaccountname.file.core.windows.net\Yourazurefilesharename`

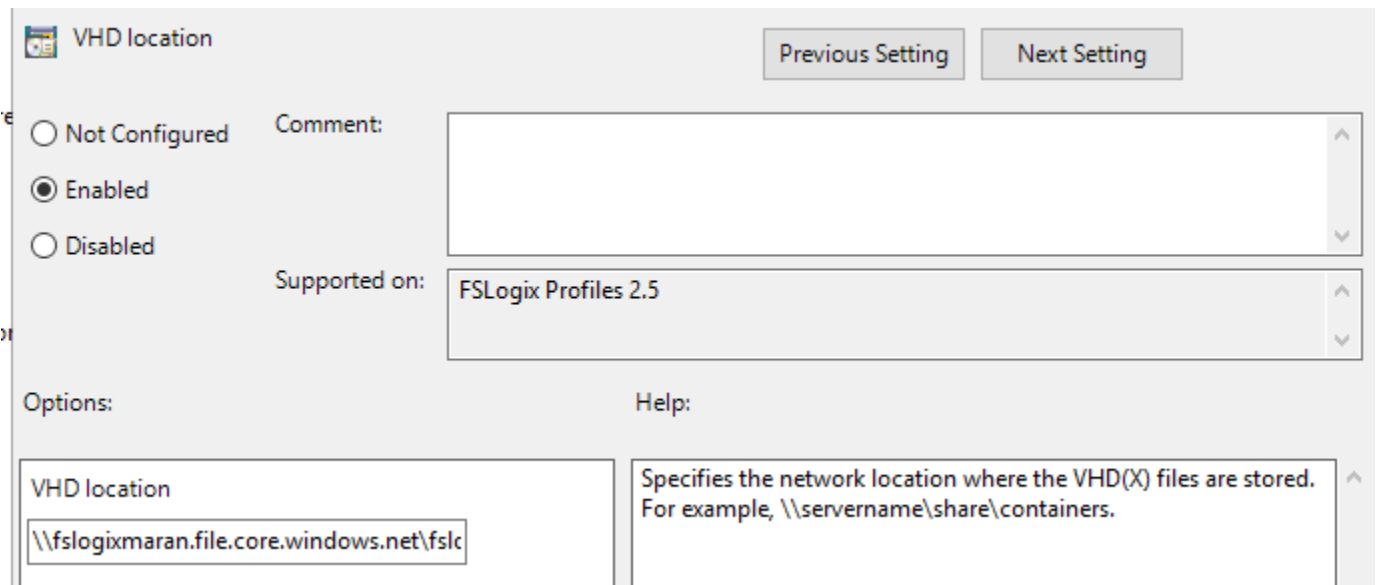


Figure 117 FSLogix file share

FSLogix installation creates a local group (on the systems it is installed on) to exclude members from receiving an FSLogix Profile Container. This group is called 'FSLogix Profile Exclude List', by making a domain scoped group a member of this local group you can control this behavior on a domain scale.

Keep in mind that although an FSLogix Profile Container can encapsulate (contain) the entire user profile it may be wise to redirect certain libraries, such as 'My Documents', to an alternate location which has file-level backups and restores implemented. This can be done via a GPO, such as Known Folder redirection (for OneDrive).

FSLogix Profile Containers also support exclusions. This will redirect file paths out of the FSLogix Profile Container to the local storage (a WVD session host in our case), which will subsequently be deleted after the user signs out. For more information consult the source below:

<https://docs.microsoft.com/en-us/fslogix/manage-profile-content-cncpt>

Critical note: Most FSLogix GPO settings make permanent registry changes which means that even after a GPO (setting) is removed, the registry setting will likely remain on the (once) targeted systems. Depicted below is an example of a configuration that previously used Cloud Cache, resulting in the 'CCDLocations' registry key. Despite that the GPO setting was removed, the registry key remained. The 'CCDLocations' registry key needs to be removed in this case since having both Cloud Cache and direct FSLogix Profile Containers (VHDLocation GPO setting) configured will cause profiles to not be loaded at all.

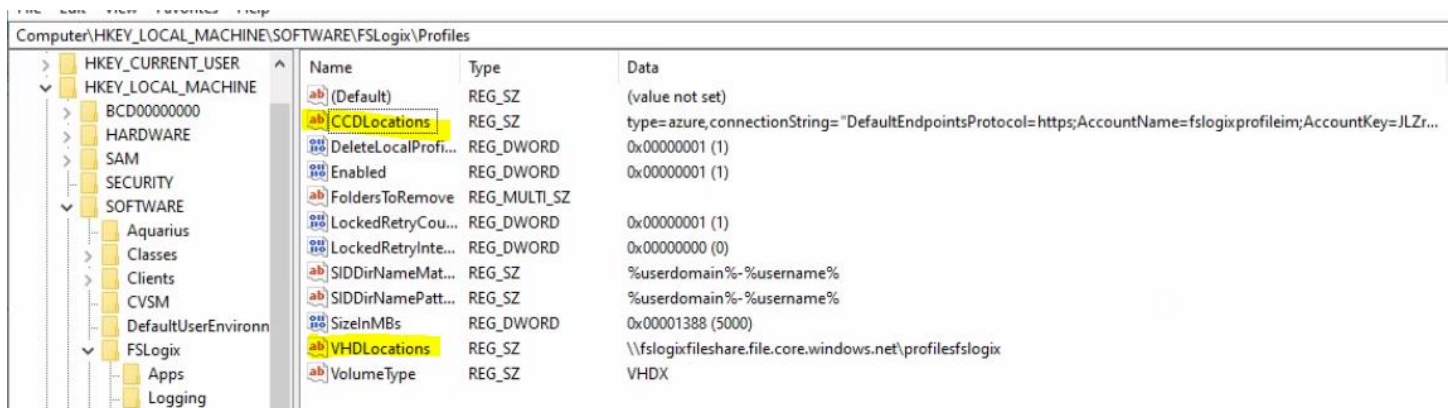


Figure 118 FSLogix incorrect configuration

For further reference on GPO settings consult the source below:

<https://docs.microsoft.com/en-us/fslogix/profile-container-configuration-reference>

Keep in mind that Microsoft advises deploying only one Azure file share per Storage account, but there are no technical restrictions on hosting more file shares. Refer to the following quote and source for more information:

“Paying attention to a storage account's IOPS limitations when deploying Azure file shares. Ideally, you would map file shares 1:1 with storage accounts, however this may not always be possible due to various limits and restrictions, both from your organization and from Azure. When it is not possible to have only one file share deployed in one storage account, consider which shares will be highly active and which shares will be less active to ensure that the hottest file shares don't get put in the same storage account together.”

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-planning#file-share-performance-tiers>

13.2 Traditional AD DS - Deploying FSLogix Profile Containers on (PaaS) Azure File shares

Traditional/laaS/on-premises based AD DS support for Azure File Shares is Globally Available. Refer to the steps below to configure this:

- 1) Create a Security Group called 'WVD_Users' (or similar name) in your AD DS domain
- 2) Add all WVD users to this Security Group. When making another Security Group a member of 'WVD_Users' ensure that both Security Groups are synchronized to Azure AD (through AAD Connect).
- 3) Log in on the Azure Portal (for example: portal.azure.com) with your administrator account
- 4) Ensure all WVD users have synchronized to Azure AD (Azure portal -> Azure Active Directory -> Users)
- 5) Ensure all required Security Groups such as 'WVD_Users' have been synchronized to Azure AD (Azure Portal -> Azure Active Directory -> Groups) and ensure they have the expected members.
- 6) Search for 'Storage accounts' in the upper search bar and press the corresponding service

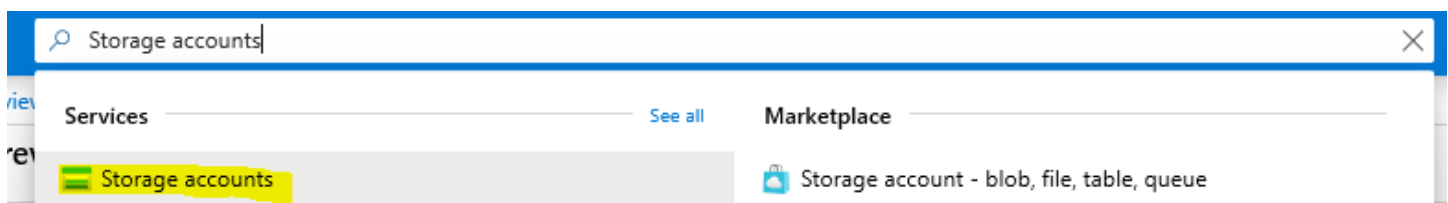


Figure 119 Storage accounts

- 7) Press **Add**
- 8) Fill in the 'Basics' blade as depicted on the next page:

Critical note: ensure your Storage account name is no longer than 17 characters.

Your storage account name needs to be (globally) unique and cannot contain special characters.

The **Location** should be the same as where your AD DS deployment resides, for optimal performance.

Subscription *

Resource group * [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 * ⓘ

Location *

Performance ⓘ Standard Premium

Account kind ⓘ ⓘ This account kind allows you to create Azure file shares with premium performance characteristics that can be tailored to your needs. [Learn more about file storage](#)

Replication ⓘ ⓘ Accounts with the selected kind, replication, and performance type only support file shares. Blobs, tables, and queues will not be available.

Figure 120 Azure FileStorage Storage account

9) Press **Next: Networking**

10) Fill in the 'Networking' blade as depicted on the next page:

Select 'Public endpoint (selected networks)'. Alternatively select 'all networks', but the entire internet can try to authenticate with the Azure Storage Account then. These settings can be changed later. Select the **Virtual Network** where AD DS was previously deployed to (i.e. where the Domain Controllers are).

Select the **Subnet** where WVD session hosts will be deployed to. Select multiple subnets if you have a management VM in a different subnet than the WVD session hosts. VMs in the selected subnets will be able to make an authentication attempt with the Azure Storage Account but will still require (further) authorization before succeeding.

Basics **Networking** Advanced Tags Review + create

Network connectivity

You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

Connectivity method *

Public endpoint (all networks)
 Public endpoint (selected networks)
 Private endpoint

Virtual networks

Only the selected network will be able to access this storage account. [Learn more about service endpoints](#) ↗

Virtual network subscription ⓘ IMMechaniX ▼

Virtual network ⓘ BasicVNet ▼

[Create virtual network](#)
[Manage selected virtual network](#)

Subnets * ⓘ SUBNET-02-BL (192.168.2.0/24) ▼

Figure 121 Storage Account - Networking

- 11) Press **Review + Create**
- 12) Press **Create**
- 13) When done creating, navigate to your Storage account

14) Press **Networking**

Search (Ctrl+/) <<

- Overview
- Activity log
- Tags
- Diagnose and solve problems
- Access Control (IAM)
- Data transfer
- Storage Explorer (preview)

Settings

- Access keys
- CORS
- Configuration
- Encryption
- Shared access signature
- Networking**
- Properties
- Locks

Firewalls and virtual networks Private endpoint connections

Save Discard Refresh

Allow access from
 All networks Selected networks

Configure network security for your storage accounts. [Learn more](#)

Virtual networks

+ Add existing virtual network + Add new virtual network

Virtual Network	Subnet	Address r.
> BasicVNet	4	

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. [Learn more.](#)

Add your client IP address ('83.8: ') ⓘ

Address range

IP address or CIDR

Exceptions

Allow trusted Microsoft services to access this storage account ⓘ

Allow read access to storage logging from any network

Figure 122 Storage Account - Networking

- 15) Select the 'Add your client IP address' checkbox, as depicted above
- 16) Verify that your desired VNet is listed, as depicted above
- 17) Finally, press **Save**
- 18) Press **Overview**
- 19) Note the Storage Account name, the Resource Group it is in and the Subscription ID. These 3 values will be required later.
- 20) Press **File shares**
- 21) Press **+ File share**

22) State a name for the Azure file share

23) State the size quota of the file share in GiB. This amount will be billed, regardless of the actual amount of data placed on a file share. The size quota of the file share can be increased/decreased afterwards.

New file share ×

Name *

fslogixprofiles ✓

Sizing your file share:

- A premium file share is billed by provisioned share size, regardless of the used capacity.
- Share sizes can range from 100 GiB to 102,400 GiB.
- Provisioned share size is specified by share quota.
- IO and network bandwidth limits scale with the provisioned share size.

[Learn more](#)

Provisioned capacity * ⓘ

1024

GiB

Allowed IO/s ⓘ : **1024**

Burst IO/s ⓘ : **3072**

Egress Rate ⓘ : **121.4 MiBytes / s**

Ingress Rate ⓘ : **81.0 MiBytes / s**

Figure 123 Azure file share

24) Press **Create**

25) Navigate to the file share after creation is complete, as depicted below, and press **Connect**:

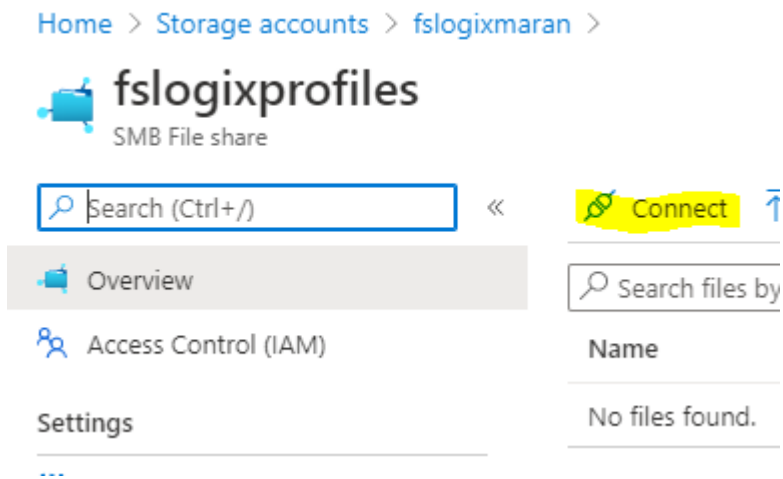


Figure 124 Azure file share

26) Press **Copy** (icon) next to the PowerShell connect code, as depicted below:

Windows Linux macOS

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



Figure 125 Azure file connect PowerShell code

27) Save the PowerShell connect code. This will be required later to set NTFS permissions.

- 28) Return to the Storage account 'Overview' blade (not of the File share)
- 29) Press **Access Control** -> **Add** -> **Add role assignment** (as depicted below)

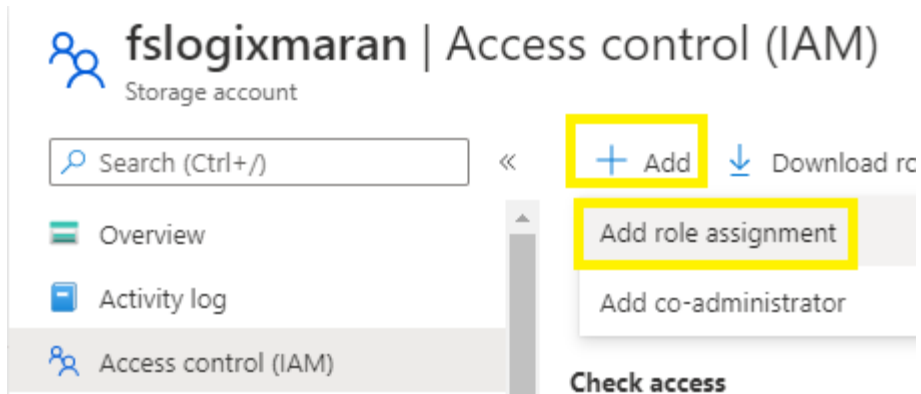


Figure 126 Storage account Access control

- 30) Select the role as depicted below:

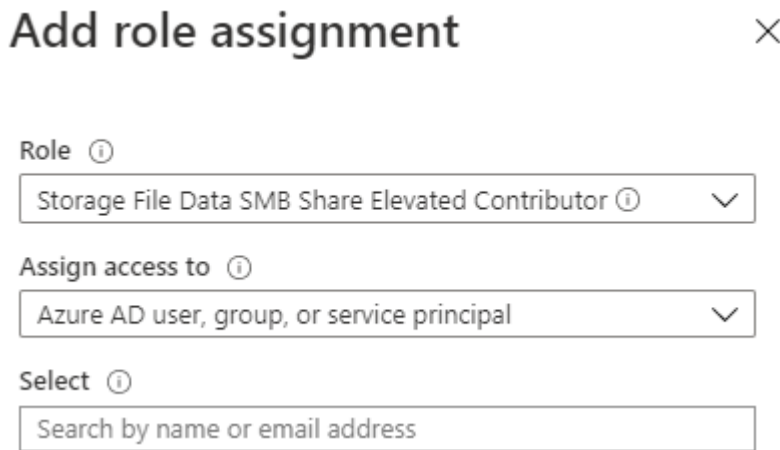


Figure 127 Storage account role assignment 1

- 31) Select an administrator account or group (under 'Select' as depicted above)

Critical note: a Cloud only user may not be used here. This administrator account must be synced (through AAD Connect) from the AD DS domain to Azure AD. The administrator account should (at least) be a member of the Domain Administrator group in the AD DS domain.

- 32) Press **Save**
- 33) If the administrator does not have the 'Owner' or 'Contributor' role assigned on the Storage Account (or Azure Subscription), assign that as well.

34) Add another role assignment to the Storage account, as depicted below:

Add role assignment ×

Role ⓘ
 Storage File Data SMB Share Contributor ⓘ

Assign access to ⓘ
 Azure AD user, group, or service principal

Select ⓘ
 WVD_Users

WVD_Users

Figure 128 Storage account role assignment 2

35) Select a group (or users) that will be working with FSLogix profiles (under 'Select' as depicted above)

The 'Storage File Data SMB Share Contributor' role will grant them 'Change' permissions (in terms of traditional file share permissions). Just as with traditional file share permissions they will be combined with NTFS permissions (will be set later on in the guide), where the most restrictive permissions will apply.

36) Press **Save**

37) Log in to a Domain Controller (via RDP or Azure Bastion for example) with the administrator account that was earlier granted the 'Storage File Data SMB Share Elevated Contributor' role.

38) Start Windows PowerShell ISE as an Administrator

39) Download the script referenced below:

https://raw.githubusercontent.com/MaranVerweij/IngramMicroAzure/MaranVerweij-Azure-Ingram1/Windows%20Virtual%20Desktop%20Guide/ADDS_AzureFiles.ps1

40) Paste the PowerShell code in the PowerShell ISE script pane or open the script in a text editor

41) Fill in the required variables (4 of them, placed at the top of the script)

42) Run the script

43) When confronted with a Microsoft Authentication prompt login with the administrator account (the User Principal Name is specified in Azure AD)

44) Verify that the script ran without errors and verify that a service account was created in the designated OU (account name is: 'Az_Yourstorageaccountname')

Critical note: keep in mind that the service account created during this process should have a never expiring password. If that is not configured the script referenced earlier will have to be run each time the service account's password expires.

- 45) Start PowerShell normally (do not run as administrator)
- 46) Run the PowerShell (connect) code/script that was saved earlier to connect to the Azure file share.
- 47) Open Windows File Explorer
- 48) Verify that Azure file share has been mounted as depicted below:

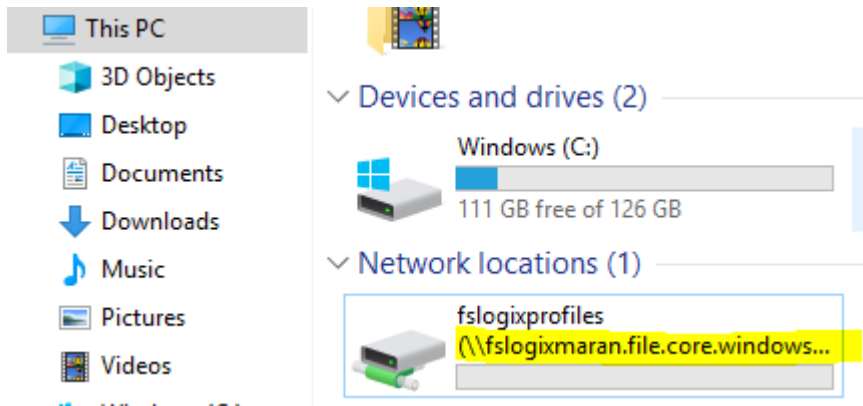


Figure 129 Azure file share in Windows

Now we can configure NTFS permissions. There are multiple ways to achieve a functioning FSLogix profile environment, this guide will execute Microsoft's best practice regarding NTFS permissions for FSLogix.

- 49) Right mouse click on the Network Drive
- 50) Press **Properties**
- 51) Press **Security**
- 52) Press **Advanced**
- 53) Press **Disable inheritance** (will prevent warnings when removing/adding principals)

54) Configure the permissions to match the figure below (or equivalent):

Permissions	Share	Auditing	Effective Access	
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).				
Permission entries:				
Type	Principal	Access	Inherited from	Applies to
Allow	CREATOR OWNER	Full control	None	Subfolders and files only
Allow	Hybrid_Admins (INGRAM\Hy...	Full control	None	This folder, subfolders and files
Allow	WVD_Users (INGRAM\WVD_U...	Modify	None	This folder only

Figure 130 Required NTFS permissions

Note that in our example 'Hybrid_Admins' is an AD DS Security Group synchronized to Azure AD. This group has been assigned the 'Storage File Data SMB Share Elevated Contributor' role on the Storage account. **Ensure at least one Hybrid AD Group/User has Full control permissions on the share at all times, to prevent losing access to the share entirely.**

Source:

<https://docs.microsoft.com/en-us/fslogix/fslogix-storage-config-ht>

55) Download the FSLogix Administrative Template for use with Group Policy Objects (GPOs) from the following URL and extract the ZIP file:

https://aka.ms/fslogix_download

56) Place the file called 'fslogix.admx' in C:\Windows\PolicyDefinitions (or an alternate SYSVOL location)

57) Place the file called 'fslogix.adml' in C:\Windows\PolicyDefinitions\en-US (or an alternate SYSVOL location)

58) Open 'Active Directory Users & Computers' and create a new OU (Organizational Unit) called 'WVD_Sessionhosts'. This will allow for a GPO that only targets relevant computers.

59) Move the WVD Session host computer objects to the previously created OU and close the interface

60) Open 'Group Policy Management'

61) Create a new GPO called 'FSLogix Profile Containers' and link it to the previously created OU

62) Edit the previously created GPO and navigate to 'Computer Configuration -> Policies -> Windows Settings -> Scripts -> Startup'

63) Press 'Browse files', this will open the source repository for startup scripts/installers. Take note of the location (UNC path) as this will be needed in the next step.

64) Locate the 'FSLogixAppsSetup.exe' file in the x64 folder (of the previously extracted ZIP file) and copy it to the location referred to in the previous step. This can be done manually or via PowerShell (example):

```
Copy-Item C:\Users\wvddc\Desktop\FSLogix_Apps_2.9.7349.30108\x64\Release\FSLogixAppsSetup.exe
"\ingram.dc\SysVol\ingram.dc\Policies\{AA04BAEE-F461-42B5-B093-644BDD5060E7}\Machine\Scripts\Startup"
```

- 65) Return to the GPO
- 66) Press 'Add'
- 67) Press 'Browse', the 'FSLogixAppsSetup.exe' file should be visible in the File Explorer that is displayed
- 68) Select the 'FSLogixAppsSetup.exe' file and press 'Open' (or double click it)
- 69) Specify '/install /quiet' as Script Parameters
- 70) Press 'Ok', for reference see the figure below:

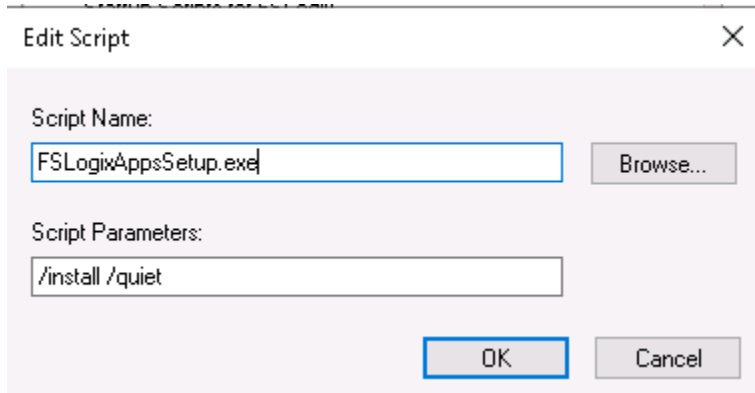


Figure 131 FSLogix Script Installer

- 71) Press 'Ok'. These settings will allow for FSLogix to be installed automatically on targeted computers.

72) Configure the remaining required settings according to the figure below:

Computer Configuration -> Policies -> Administrative Templates -> FSLogix -> Profile Containers	Configuration
Enabled	Enabled (with Options: 'Enabled' checkbox selected)
Size in MBs	50000 (a size cap for the FSLogix Profile Container, changing later requires a profile reset)
Delete local profile when FSLogix Profile should apply	Enabled (with matching checkbox selected)
Computer Configuration -> Policies -> Administrative Templates -> FSLogix -> Profile Containers -> Advanced	
Locked VHD retry count	Enabled -> 3
Locked VHD retry interval	Enabled -> 3
Computer Configuration -> Policies -> Administrative Templates -> FSLogix -> Profile Containers -> Container and Directory Naming	
SID directory name matching string	Enabled -> %userdomain%_%username%
SID directory name pattern string	Enabled -> %userdomain%_%username%
Virtual disk type	Enabled -> VHDX

Figure 132 FSLogix GPO Configuration

73) Navigate to: Computer Configuration -> Policies -> Administrative Templates -> FSLogix -> Profile Containers -> VHDLocation -> Network path to file share (depicted below)

Ensure the network path is in the following format:

`\\Yourstorageaccountname.file.core.windows.net\Yourazurefilesharename`

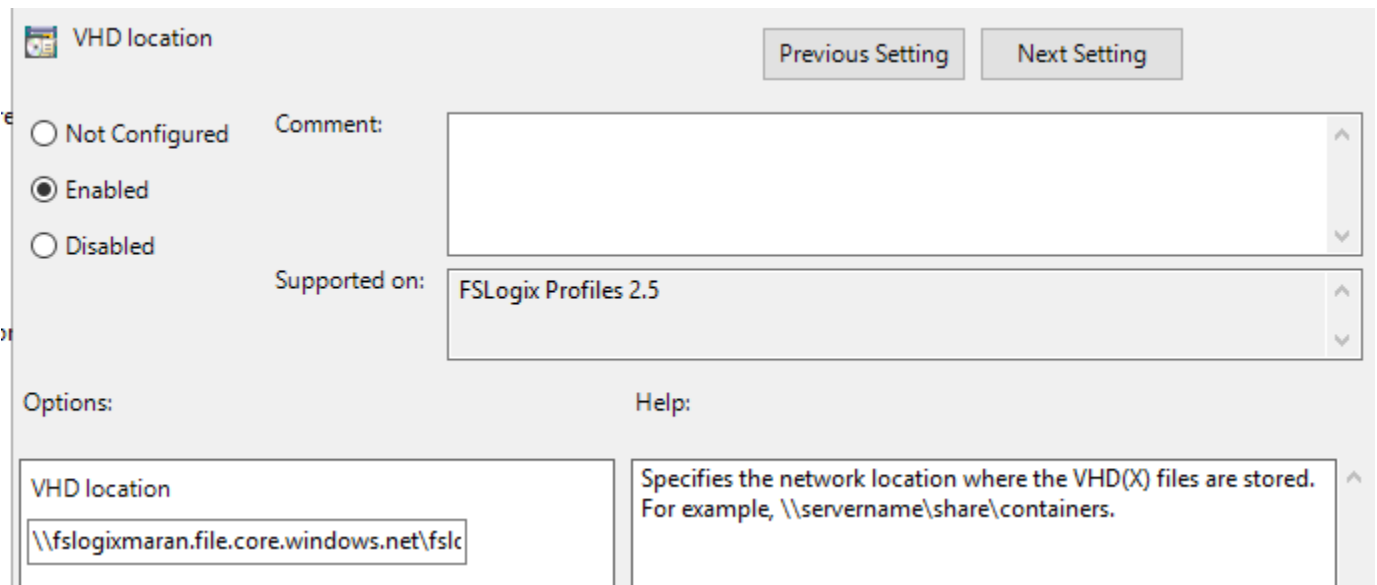


Figure 133 FSLogix file share

FSLogix installation creates a local group (on the systems it is installed on) to exclude members from receiving an FSLogix Profile Container. This group is called 'FSLogix Profile Exclude List', by making a domain scoped group a member of this local group you can control this behavior on a domain scale.

Keep in mind that although an FSLogix Profile Container can encapsulate (contain) the entire user profile it may be wise to redirect certain libraries, such as 'My Documents', to an alternate location which has file-level backups and restores implemented. This can be done via a GPO, such as Known Folder redirection (for OneDrive).

FSLogix Profile Containers also support exclusions. This will redirect file paths out of the FSLogix Profile Container to the local storage (a WVD session host in our case), which will subsequently be deleted after the user signs out. For more information consult the source below:

<https://docs.microsoft.com/en-us/fslogix/manage-profile-content-cncpt>

Critical note: Most FSLogix GPO settings make permanent registry changes which means that even after a GPO (setting) is removed, the registry setting will likely remain on the (once) targeted systems. Depicted below is an example of a configuration that previously used Cloud Cache, resulting in the 'CCDLocations' registry key. Despite that the GPO setting was removed, the registry key remained. The 'CCDLocations' registry key needs to be removed in this case since having both Cloud Cache and direct FSLogix Profile Containers (VHDLocation GPO setting) configured will cause profiles to not be loaded at all.

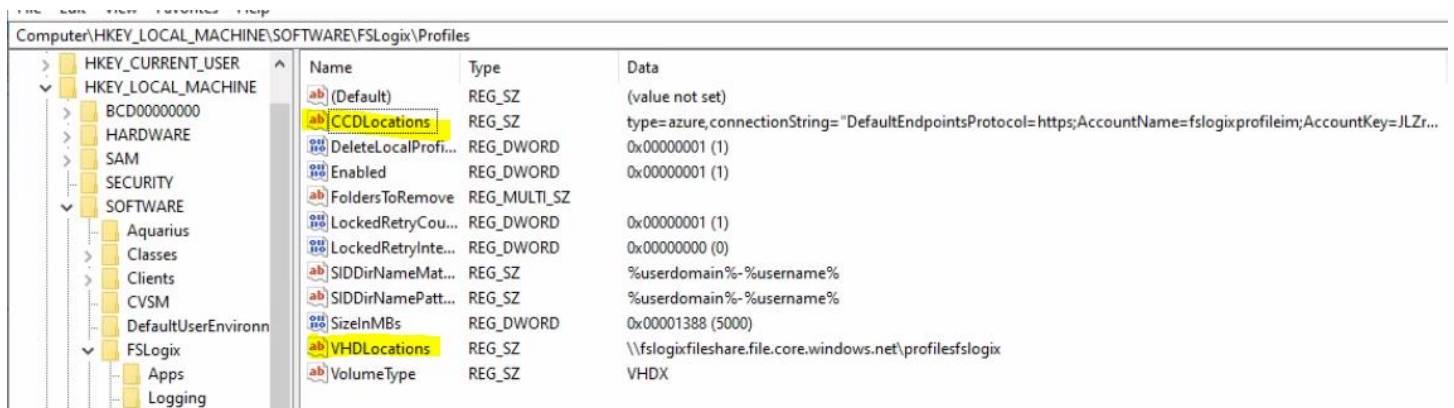


Figure 134 FSLogix incorrect configuration

For further reference on GPO settings consult the source below:

<https://docs.microsoft.com/en-us/fslogix/profile-container-configuration-reference>

Keep in mind that Microsoft advises deploying only one Azure file share per Storage account, but there are no technical restrictions on hosting more file shares. Refer to the following quote and source for more information:

“Paying attention to a storage account's IOPS limitations when deploying Azure file shares. Ideally, you would map file shares 1:1 with storage accounts, however this may not always be possible due to various limits and restrictions, both from your organization and from Azure. When it is not possible to have only one file share deployed in one storage account, consider which shares will be highly active and which shares will be less active to ensure that the hottest file shares don't get put in the same storage account together.”

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-planning#file-share-performance-tiers>

13.3 Deploying FSLogix Profile Containers on (IaaS) File shares

With this approach the FSLogix Profile Containers will be hosted on a file share and subsequently streamed to the user session directly. It is recommended to create this share on a volume that is based on a Premium SSD managed disk. Also consider creating the file share on a central server with little to no down time as users will not be able to load their profiles if the share is not available.

- 1) Log in on the server which will be hosting the FSLogix Profile Containers file share
- 2) Navigate to the location where the share will be hosted and create a folder
- 3) Right mouse click on the folder -> Properties -> Sharing -> 'Advanced Sharing', as depicted below

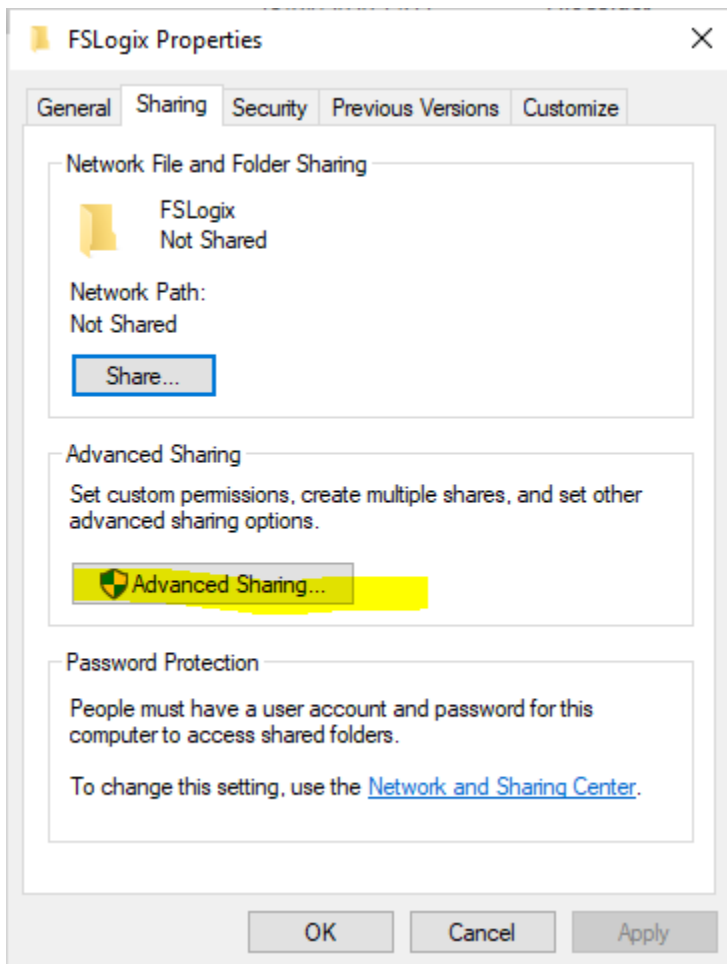


Figure 135 FSLogix location

- 4) Check the box 'Share this folder'
- 5) Configure the user limit to be 9999, or less if you want to limit the amount of FSLogix users
- 6) Press 'Permissions'
- 7) Configure 'Everyone' or 'Authenticated Users' to have Full Control
- 8) Take note of the file share (Network) path as it will be required later

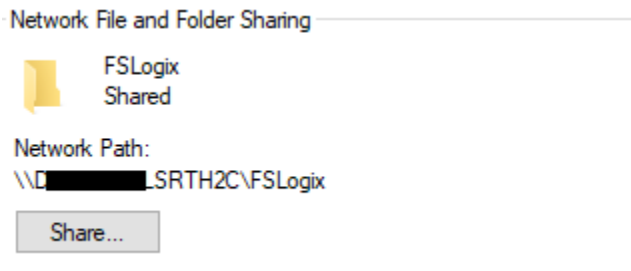


Figure 136 File share network path

- 9) Navigate to the 'Security' tab and press 'Advanced'
- 10) Configure the permissions to match the figure below (or equivalent):

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Authenticated Users	Modify	None	This folder only
Allow	CREATOR OWNER	Modify	None	Subfolders and files only
Allow	Domain Admins (INGRAM\...)	Full control	None	This folder, subfolders and files

Figure 137 Required NTFS permissions

Source:

<https://docs.microsoft.com/en-us/fslogix/fslogix-storage-config-ht>

- 11) Connect (via RDP or Azure Bastion) to the AAD DS Management VM that was previously created
- 12) Download the FSLogix Administrative Template for use with Group Policy Objects (GPOs) from the following URL and extract the ZIP file:

https://aka.ms/fslogix_download

- 13) Place the file called 'fslogix.admx' in C:\Windows\PolicyDefinitions
- 14) Place the file called 'fslogix.adml' in C:\Windows\PolicyDefinitions\en-US
- 15) Open 'Active Directory Users & Computers' and create a new OU (Organizational Unit) called 'WVD_Sessionhosts'. This will allow for a GPO that only targets relevant computers.
- 16) Move the WVD Session host computer objects to the previously created OU and close the interface
- 17) Open 'Group Policy Management'
- 18) Create a new GPO called 'FSLogix Profile Containers' and link it to the previously created OU
- 19) Edit the previously created GPO and navigate to 'Computer Configuration -> Policies -> Windows Settings -> Scripts -> Startup'

- 20) Press 'Browse files', this will open the source repository for startup scripts/installers. Take note of the location (UNC path) as this will be needed in the next step.
- 21) Locate the 'FSLogixAppsSetup.exe' file in the x64 folder (of the previously extracted ZIP file) and copy it to the location referred to in the previous step.
- 22) Return to the GPO
- 23) Press 'Add'
- 24) Press 'Browse', the 'FSLogixAppsSetup.exe' file should be visible in the File Explorer that is displayed
- 25) Select the 'FSLogixAppsSetup.exe' file and press 'Open'
- 26) Specify '/install /quiet' as Script Parameters
- 27) Press 'Ok', for reference see the figure below:

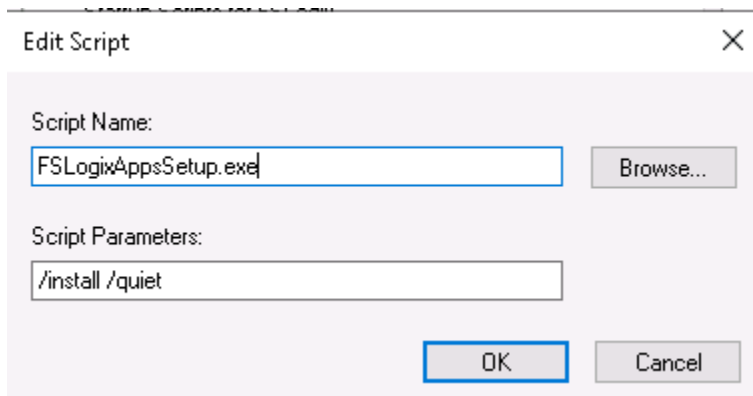


Figure 138 FSLogix Script Installer

- 28) Press 'Ok'. These settings will allow for FSLogix to be installed automatically on targeted computers.

29) Configure the remaining required settings according to the figure below:

Computer Configuration -> Policies -> Administrative Templates -> FSLogix -> Profile Containers	Configuration
Enabled	Enabled (with Options: 'Enabled' checkbox selected)
Size in MBs	50000 (a size cap for the FSLogix Profile Container, changing later requires a profile reset)
Delete local profile when FSLogix Profile should apply	Enabled (with matching checkbox selected)
Computer Configuration -> Policies -> Administrative Templates -> FSLogix -> Profile Containers -> Advanced	
Locked VHD retry count	Enabled -> 3
Locked VHD retry interval	Enabled -> 3
Computer Configuration -> Policies -> Administrative Templates -> FSLogix -> Profile Containers -> Container and Directory Naming	
SID directory name matching string	Enabled -> %userdomain%_%username%
SID directory name pattern string	Enabled -> %userdomain%_%username%
Virtual disk type	Enabled -> VHDX

Figure 139 FSLogix GPO Configuration

30) Navigate to: Computer Configuration -> Policies -> Administrative Templates -> FSLogix -> Profile Containers -> VHDLocation -> Network path to file share (depicted below)

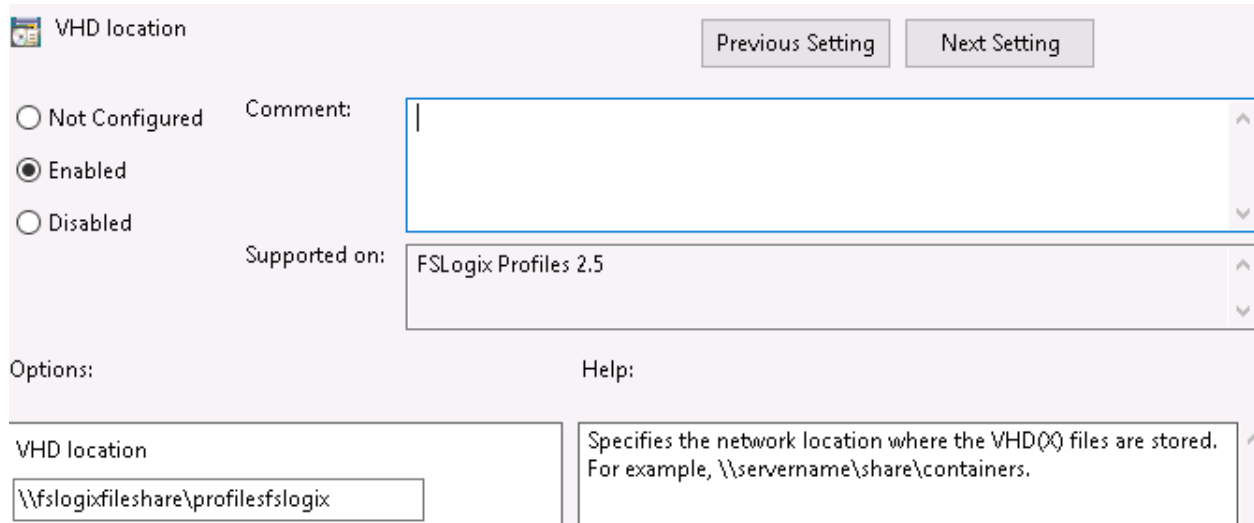


Figure 140 FSLogix file share

FSLogix installation creates a local group (on the systems it is installed on) to exclude members from receiving an FSLogix Profile Container. This group is called 'FSLogix Profile Exclude List', by making a domain scoped group a member of this local group you can control this behavior on a domain scale.

Keep in mind that although an FSLogix Profile Container can encapsulate (contain) the entire user profile it may be wise to redirect certain libraries, such as 'My Documents', to an alternate location which has file-level backups and restores implemented. This can be done via a GPO, such as Known Folder redirection (for OneDrive).

FSLogix Profile Containers also support exclusions. This will redirect file paths out of the FSLogix Profile Container to the local storage (a WVD session host in our case), which will subsequently be deleted after the user signs out. For more information consult the source below:

<https://docs.microsoft.com/en-us/fslogix/manage-profile-content-cncpt>

Critical note: Most FSLogix GPO settings make permanent registry changes which means that even after a GPO (setting) is removed, the registry setting will likely remain on the (once) targeted systems. Depicted below is an example of a configuration that previously used Cloud Cache, resulting in the 'CCDLocations' registry key. Despite that the GPO setting was removed, the registry key remained. The 'CCDLocations' registry key needs to be removed in this case since having both Cloud Cache and direct FSLogix Profile Containers (VHDLocation GPO setting) configured will cause profiles to not be loaded at all.

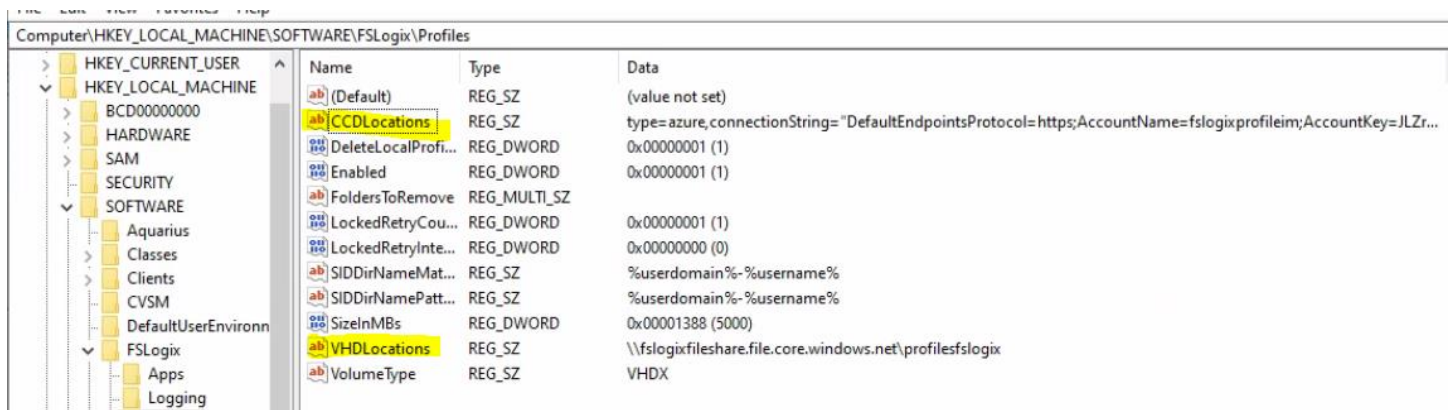


Figure 141 FSLogix incorrect configuration

For further reference on GPO settings consult the source below:

<https://docs.microsoft.com/en-us/fslogix/profile-container-configuration-reference>

13.4 **!!DEPRECATED!!** Deploying FSLogix Profile Containers in Blob Containers

- 1) Create a General Purpose V2 account with Premium performance tier (for optimal performance) in the Azure Portal.

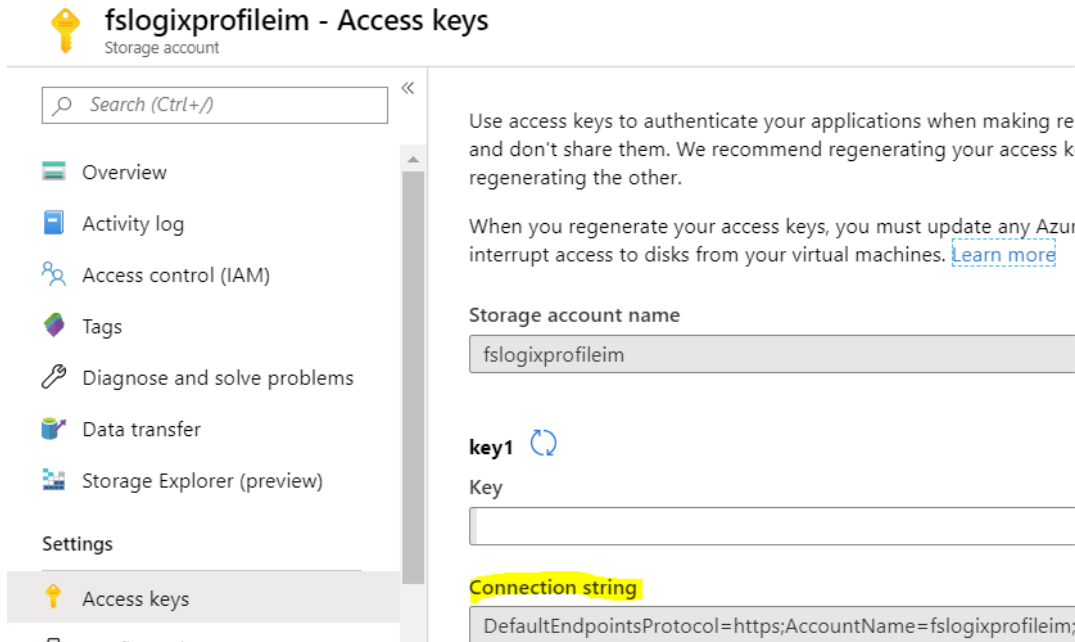


Figure 142 Storage Account Access Keys

- 2) Navigate to the Access Keys blade on the previously created Azure Storage account and copy the 'Connection string' below key1 entirely and save it for later use. For reference see the figure above.

Critical note: if the 'Key' field contains a '/' press the refresh(renew) button to generate a key without a '/' in it. There is a known issue where FSLogix can not interpret a '/' as part of a key and may cause a critical error as displayed in the figure below.

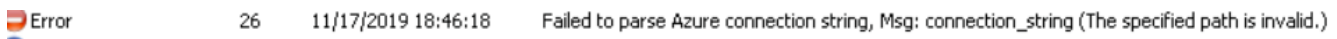


Figure 143 FSLogix Azure Connection string error

- 3) Connect (via RDP or Azure Bastion) to the AAD DS Management VM that was previously created.
- 4) Download the FSLogix Administrative Template for use with Group Policy Objects (GPOs) from the following URL and extract the ZIP file:

<https://go.microsoft.com/fwlink/?linkid=2084562>

- 5) Place the file called 'fslogix.admx' in C:\Windows\PolicyDefinitions
- 6) Place the file called 'fslogix.adml' in C:\Windows\PolicyDefinitions\en-US

- 7) Open Active Directory Users & Computers and create a new OU (Organizational Unit) called 'WVD_Sessionhosts'
- 8) Move the WVD Session host computer objects to the previously created OU and close the interface.
- 9) Locate the 'FSLogixAppsSetup.exe' file in the x64 folder (of the previously extracted file) and save it to a central location.
- 10) Open Group Policy Management
- 11) Create a new GPO called 'FSLogix Profile Containers' and link it to the previously created OU
- 12) Edit the previously created GPO and navigate to 'Computer Configuration -> Windows Settings -> Scripts -> Startup'
- 13) Press 'Browse files', this will open the source repository for startup scripts/installers.
- 14) Place the 'FSLogixAppsSetup.exe' file in this location, close the window and return to the GPO
- 15) Press 'Add' and enter 'FSLogixAppsSetup.exe' in the field named 'Script name'
- 16) In the 'Script parameters' box copy and paste the following text:
 /silent ProductKey=MSFT0-YXKIX-NVQI4-I6WIA-O4TXE
 Press 'Ok' and finally 'Ok'. For reference see the figure below,

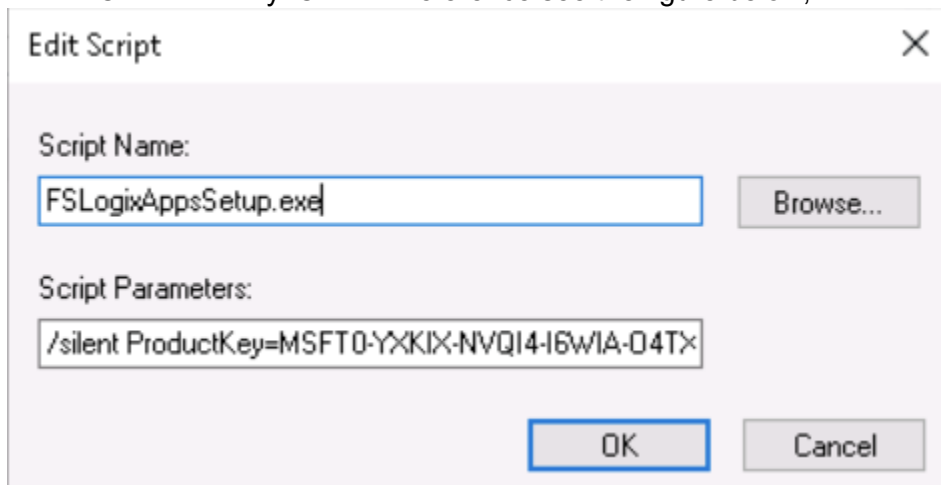


Figure 144 FSLogix Installer Script

17) Configure the remaining required settings according to the figure below:

Computer Configuration -> Policies -> Administrative Templates -> FSLogix -> Profile Containers	Configuration
Enabled	Enabled (with Options: 'Enabled' checkbox selected)
Size in MBs	5000 (a size cap for the FSLogix Profile Container)
Delete local profile when FSLogix Profile should apply	Enabled (with matching checkbox selected)
Computer Configuration -> Policies -> Administrative Templates -> FSLogix -> Profile Containers -> Advanced	
Locked VHD retry count	Enabled -> 1
Locked VHD retry interval	Enabled -> 0
Computer Configuration -> Policies -> Administrative Templates -> FSLogix -> Profile Containers -> Container and Directory Naming	
SID directory name matching string	Enabled -> %userdomain%-%username%
SID directory name pattern string	Enabled -> %userdomain%-%username%
Virtual disk type	Enabled -> VHDX

Figure 145 FSLogix GPO Configuration

18) Navigate to: Computer Configuration -> Policies -> Administrative Templates -> FSLogix -> Profile Containers -> Cloud Cache -> Cloud Cache Locations

19) Perform the following configuration (where YOURCONNECTIONSTRING is replaced by the connection string saved earlier during step 2)

Enabled -> type=azure,connectionString="YOURCONNECTIONSTRING"

Reference example:

```
type=azure,connectionString="DefaultEndpointsProtocol=https;AccountName=fslogixprofileim;AccountKey=XqdummykeyyJRG+msTTIfg6fdaRvop+finAYUFnnowE3JiaBHHNKqzpRr9ToGIp+W777eeUxFhtJKIYUIGRAzNNA==;EndpointSuffix=core.windows.net"
```

20) Log in to a WVD Session host and confirm that a container is created in the storage account that was previously created. This can be achieved by navigating to the 'Storage Explorer' blade located under a storage account via the Azure Portal.

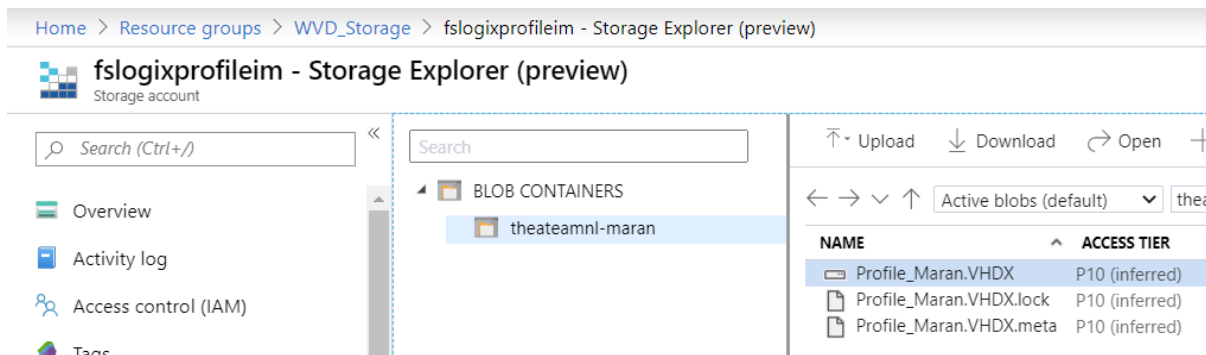


Figure 146 FSLogix Profile Container in Azure Storage Account

FSLogix installation creates a local group (on the systems it is installed on) to exclude members from receiving an FSLogix Profile Container. This group is called 'FSLogix Profile Exclude List', by making a domain scoped group a member of this local group you can control this behavior on a domain scale.

Keep in mind that although an FSLogix Profile Container can encapsulate (contain) the entire user profile it may be wise to redirect certain libraries, such as 'My Documents', to an alternate location which has file-level backups and restores implemented. This can be done via a GPO, such as Known Folder redirection (for OneDrive).

FSLogix Profile Containers also support exclusions. This will redirect file paths out of the FSLogix Profile Container to the local storage (a WVD session host in our case), which will subsequently be deleted after the user signs out. For more information consult the source below:

<https://docs.microsoft.com/en-us/fslogix/manage-profile-content-cncpt>

Critical note: Keep in mind that although an FSLogix Profile Container can encapsulate (contain) the entire user profile it may be wise to redirect certain libraries, such as 'My Documents', to an alternate location which has file-level backups and restores implemented. FSLogix Profile Containers support exclusions (of file locations) for these types of scenarios.

14 Deploy Scaling Logic

Considering that WVD Session hosts are Virtual Machines (VMs) the performance and capacity of a WVD solution is largely decided by the compute and storage resources allocated to these VMs. Subsequently the costs of a WVD solution are largely decided by the sizing of the VMs and how their scaling is configured.

The basic concept behind an auto scaling solution (if not considering VMSS Auto Scaling) is:

- Create enough WVD session hosts to support the maximum user load (peak) at any given time
- Creating automation (through a PowerShell script) to turn WVD session hosts on or off based on a set metric. For example, when a WVD session host reaches 20 concurrent user sessions or start/stop WVD session hosts based on a time schedule

Microsoft has published a solution for the basic scenario described above. For reference material please consult the URL below:

<https://docs.microsoft.com/en-us/azure/virtual-desktop/set-up-scaling-script>

The rest of this chapter will cover the various solutions available through & developed by Ingram Micro.

14.1 Scripted scaling with VMs

Although the Ingram Micro scripted scaling solution for Azure VMs only supports starting and stopping WVD session hosts (VMs) based on a time schedule, the implementation is also less complex as the script can be run via scheduled task or an Azure Function (on a schedule).

If you would like access to this script or help setting up an automated/scripted scaling solution please contact us at Microsoft@ingrammicro.nl

14.2 Auto scaling with VM Scale Sets

Auto scaling with VMSS leads to VM instances being created or removed (not shut down), either based on a time schedule or real time resource (CPU) usage. Scaling out (creating new VM instances) is done based on the image assigned to the VMSS and the VM extensions (PowerShell scripts for example), which will be executed when a new VM instance is created. Scaling in (deleting existing VM instances) can also be done based on a time schedule or real time resource (CPU) usage.

If you would like to be able to shut down VM instances, so that they can be started again later, please refer to '14.3 Scripted Scaling with VM Scale Sets'.

Follow the steps below to configure Auto Scaling:

- 1) Log in on the Azure Portal (for example: portal.azure.com) with your administrator account
- 2) Navigate to Virtual Machine Scale Sets (VMSS)
- 3) Select the desired VMSS
- 4) Press **Scaling**
- 5) Select 'Custom autoscale'
- 6) Define a 'Default' rule, this will apply when other rules do not (for example a rule that only applies on weekdays). The rule defined below will ensure that only 1 VM instance exists, if no other rules apply.

Default* Auto created scale condition ✖

Delete warning
 ⓘ The very last or default recurrence rule cannot be deleted. Instead, you can disable autoscale to turn off autoscale.

Scale mode Scale based on a metric Scale to a specific instance count

Instance count*

Schedule **This scale condition is executed when none of the other scale condition(s) match**

Figure 147 Default rule

- 7) Press **+ Add a scale condition**
- 8) Define a scaling rule that will have a higher priority than the Default rule.

The example below scales out when the aggregated average CPU load of all VM instances in the VMSS is higher than 50%. When the load is below 25% the VMSS will start scaling in (removing VM instances). This rule only applies on Mondays through Fridays between 6:00 and 18:00.

Auto created scale condition 1 🗑️

Scale mode Scale based on a metric Scale to a specific instance count

Rules

Scale out

When	WVD-VMSS-Ephemeral	(Average) Percentage CPU > 50	Increase count by 1
------	--------------------	-------------------------------	---------------------

Scale in

When	WVD-VMSS-Ephemeral	(Average) Percentage CPU > 25	Decrease count by 1
------	--------------------	-------------------------------	---------------------

[+ Add a rule](#)

Instance limits

Minimum ⓘ	Maximum ⓘ	Default ⓘ
5 ✔	15 ✔	5 ✔

Schedule Specify start/end dates Repeat specific days

Repeat every

<input checked="" type="checkbox"/> Monday	<input checked="" type="checkbox"/> Tuesday	<input checked="" type="checkbox"/> Wednesday	<input checked="" type="checkbox"/> Thursday
<input checked="" type="checkbox"/> Friday	<input type="checkbox"/> Saturday	<input type="checkbox"/> Sunday	

Timezone (UTC+01:00) Amsterdam, Berlin, Bern, Rom... ▼

Start time 06:00

End time 18:00

Specify an end time, else this scale condition will apply for all days until it reaches the start time of another scale condition

Figure 148 VMSS Auto scale rule

To ensure optimal user performance it is recommended to leave the load balancing algorithm in the WVD Host pool to its default setting: 'Breadth-first'. As this will ensure that new user sessions are routed to the most recently scaled out VM instance, considering that this load balancing algorithm ensures each WVD session host (VM instance) receives an equal number of users.

If you would like more information about VM Scale Sets for WVD or need help setting up a scaling solution please contact us at Microsoft@ingrammicro.nl

14.3 Scripted Scaling with VM Scale Sets

Critical note: if your VMSS uses Ephemeral storage this script is not supported, as VM instances with Ephemeral storage can not be deallocated (only removed entirely). Refer to '13.2 Auto scaling with VM Scale Sets' instead.

If you would like access to this script or help setting up an automated/scripted scaling solution please contact us at Microsoft@ingrammicro.nl

15 Deploy Microsoft Teams

If you would like to deploy Microsoft Teams in your Windows Virtual Desktop environment, please refer to the source below:

<https://docs.microsoft.com/en-us/azure/virtual-desktop/teams-on-wvd>

16 Deploy MSIX App Attach

If you would like to deploy applications from a central repository rather than having them installed on each WVD session host individually consider using MSIX App Attach. Refer to the source below for more information:

<https://docs.microsoft.com/en-us/azure/virtual-desktop/app-attach>