

Windows Virtual Desktop on Azure

Azure Hands On Lab August 14th 2020

V3.1 by : Gido Veekens
Stephan van de Kruis



2tCloud



Content

Introduction	3
Activity 1 : Getting Started	4
Exercise 1a : Login to the Azure Portal	4
Exercise 1b: Create a Resource Group	6
Exercise 1c: Deploy Azure Active Directory Domain Services.....	7
Activity 2 : Deploy Windows Virtual Desktop	12
Exercise 2a: Finalize the AAD Domain Services deployment	12
Exercise 2b: Create a Test User	17
Exercise 2b : Prepare Windows Virtual Desktop	Error! Bookmark not defined.
Exercise 2c : Create Windows Virtual Desktop Workspace.....	19
Exercise 2D: Create a Windows Virtual Desktop Host Pool.....	20
Activity 3: Set up FSLogix on Azure Files	23
Exercise 3a: Prepare FSLogix Storage	23
Exercise 3b : Configure FSLogix.....	26
Exercise 3c: Check your configuration	29
Activity 4: Conditional Access	30
Exercise 4a: Configure Conditional Access for WVD	30
Exercise 4b: Test Conditional Access	32
Activity 4: Remove your resources	34
Extra resources	35

Introduction

Estimated time to complete this lab

150 minutes

Objectives

During this lab, you will learn how to get started with Azure to;

- Make your way through the Azure Portal
- Deploy Azure Active Directory Domain Services
- Deploy Windows Virtual Desktop
- Configure FSlogix
- Deploy Conditional Access for MFA

Prerequisites

To complete this course, you will be needing;

- Laptop/computer with Internet browser and WiFi connected
- Account with an Azure CSP Subscription
- A Microsoft 365 Business Premium subscription

Materials

All student materials are available for download here:

<https://github.com/Copaco/handsonlab/>

Activity 1 : Getting Started

Estimated time to complete this activity

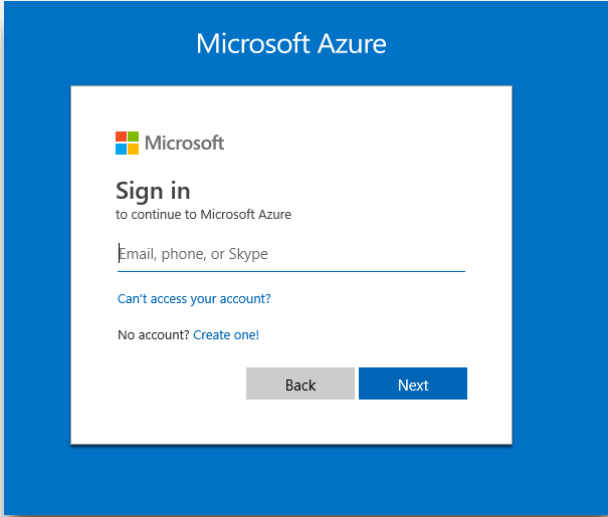
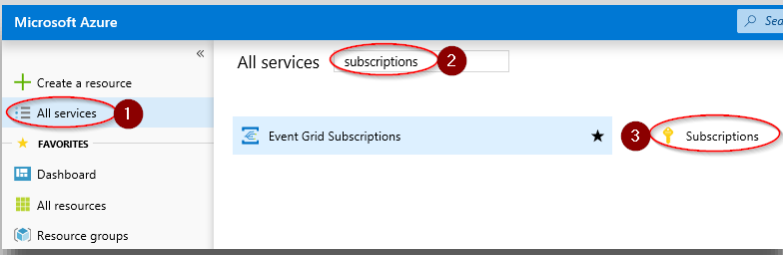
45 minutes

Objectives

In this activity, you will configure the components necessary to perform this lab;

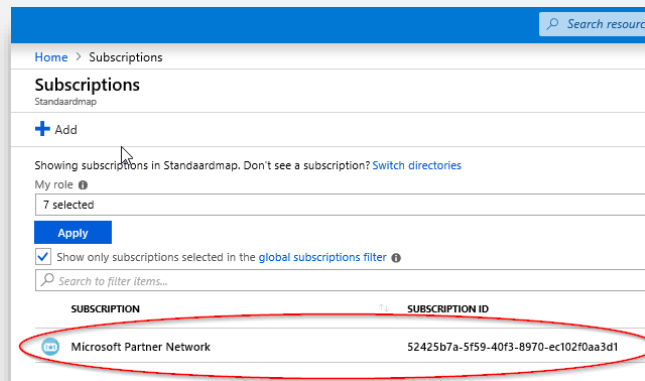
- Login to your Azure tenant
- Create a Resource Group
- Deploy Azure Active Directory Domain Services

Exercise 1a : Login to the Azure Portal

<p>1)</p>	<p>✦ <i>We also strongly recommend that you use InPrivate browsing to ensure that you are not automatically logged on with other credentials during the registration / activation process.</i></p>
<p>2) Using your <i>Work Account</i>, you can sign into the Azure Portal at:</p> <p>https://portal.azure.com</p>	
<p>3) Using the navigation bar on the left, use the <i>All services</i> menu to browse to the <i>Subscriptions</i> pane.</p> <p>The <i>Search</i> filter on the top will help you to find what you need.</p>	

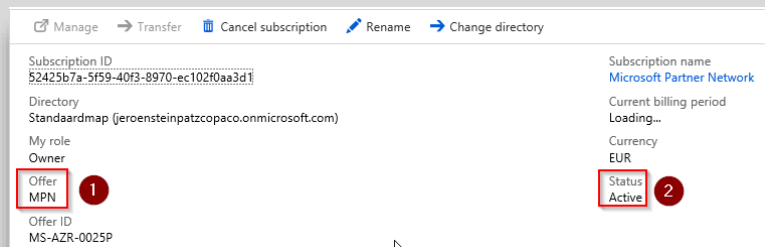


- 4) From the [Subscriptions](#) overview, click the active subscription.



- 5) In the [Overview](#) pane, check the Offer type for being either **CSP**, **MPN**, **MSDN**, **OPEN** or **EA**

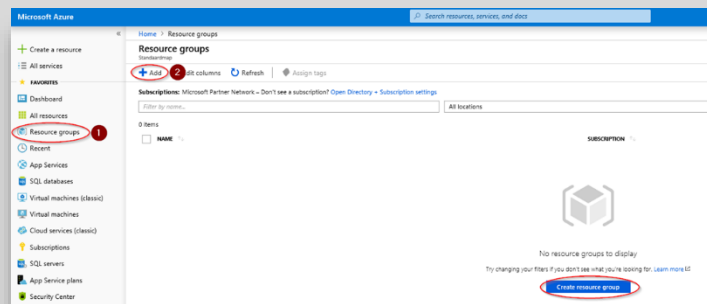
Check the [Status](#) for being **Active**.



✦ We also strongly recommend that you use *InPrivate* browsing to ensure that you are not automatically logged on with other credentials during the registration / activation process.

Exercise 1b: Create a Resource Group

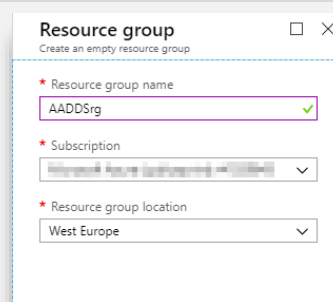
- 1) Click [Resource Groups](#)
Click [Add](#)



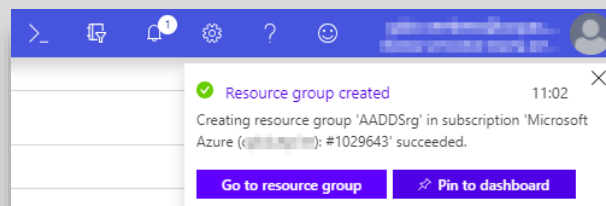
- 2) Add [Resource group name](#)
AADDSSrg

Select [Subscription](#)
Microsoft Azure (CSP)

Select [Location](#)
West Europe



- 3) After a few moments, the Resource Group "AADDSSrg" is created

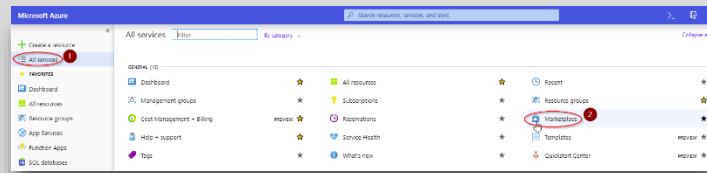


✦ You can choose a different name for the resource group if you like. However, the scripts that will be used in the following steps don't support special characters in the Resource Group name. So please prevent the use of underscores or hyphens in the name, as this will result in failures later on.

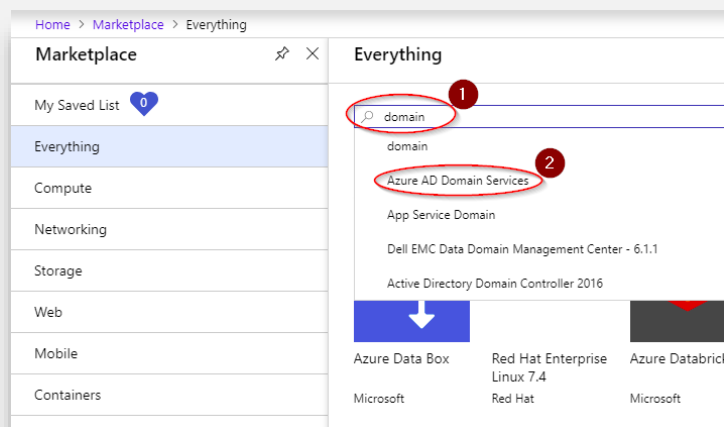
Exercise 1c: Deploy Azure Active Directory Domain Services

Important note: You can only deploy one instance of Domain Services per tenant. So if you attend this lab with a colleague, discuss who will deploy Domain Services in the tenant.

- 1) From the Azure Portal, click *All services* and go to the *Marketplace*



- 2) Use the Search Everything box to search and select *Azure AD Domain Services*



- 3) You will be presented with a summary of the service. Click the [Create](#) button.

Azure AD Domain Services

Microsoft

Azure Active Directory Domain Services lets you join Azure virtual machines to a domain without the need to deploy or manage domain controllers. Users sign in to these virtual machines using their corporate Active Directory credentials and can access resources seamlessly. Azure Active Directory Domain Services features domain join, LDAP, NTLM and Kerberos authentication are widely used in enterprises. Migrate legacy directory-aware applications running on premises to Azure without having to worry about identity requirements.

[Save for later](#)

PUBLISHER	Microsoft
USEFUL LINKS	Service overview Documentation Pricing

[Create](#)

- 4) Now it is time to choose some setup preferences.

For the domain name, **accept the provided** value. In production environment, you would use a custom public domain name.

Choose the same Subscription, Resource Group and Location as used in earlier steps.

For Sku choose **Standard**

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 *

Migratie Subscription Copaco

Resource group * ⓘ

[Create new](#)

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

DNS domain name * ⓘ

id.20250797.onmicrosoft.com

[Help me choose the DNS name](#)

Region * ⓘ

(Europe) West Europe

SKU * ⓘ

Standard

[Help me choose a SKU](#)

Forest type * ⓘ

User Resource (preview)

[Help me choose a forest type](#)



- 5) As AAD Domain Services are deployed in a Virtual Network, we'll have to create one.

Select [Create New](#)

- 6) For this lab, we'll be fine using the defaults for this Virtual Network. Adjust only the VNET Name, so it aligns with the naming convention

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 * ⓘ (new) aad05-vnet [Create new](#)

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

Subnet * ⓘ (new) aad05-subnet (10.0.2.0/24) [Help me choose the subnet and NSG](#)

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

Address range	Addresses	Overlap
<input type="checkbox"/> 10.0.2.0/24	10.0.2.0 - 10.0.2.255 (256 addresses)	None

Subnets
The subnet's address range in CIDR notation. It must be contained by the address space of the virtual network.

Subnet name	Address range	Addresses
<input type="checkbox"/> aad05-subnet	10.0.2.0/24	10.0.2.0 - 10.0.2.255 (256 addresses)

Warning: A network security group will be automatically created and associated to the subnet to protect AAD Domain Services. The network security group will be configured according to [guidelines for configuring NSGs](#).

- 7) You'll be notified that a Network Security Group will be created. We won't be covering the details in this lab, but you can safely ignore the warning and proceed.

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 * ⓘ (new) AAD05vn [Create new](#)

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

Subnet * ⓘ (new) aad05-subnet (10.0.2.0/24) [Help me choose the subnet and NSG](#)

Warning: A network security group will be automatically created and associated to the subnet to protect AAD Domain Services. The network security group will be configured according to [guidelines for configuring NSGs](#).

- 8) By default, a new security group will be created in the Azure Active Directory. Accept the suggested group.

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:

[Help me choose who gets notifications](#)

- 9) For this lab leave the Synchronization type to all.

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](#)

- 10) You will be prompted with a summary. Please review and correct if necessary, before proceeding.

Validating

Basics * Networking * Administration Synchronization **Review + create**

Basics

Name	M365x635797.onmicrosoft.com
Subscription	Migratie Subscription Copaco
Resource group	rg-dc
Region	West Europe
SKU	Standard
Forest type	User

Network

Virtual network	(new) AADDsvn
Subnet	(new) aadds-subnet
Subnet Address	10.0.2.0/24
Network security group	(new) aadds-nsg

Administrator group

Administrator group	AAD DC Administrators
Membership Type	Assigned

Notifications

Notify global administrators	Yes
Notify AAD DC administrators group	Yes

Synchronization

Synchronization scope	All
-----------------------	-----

- 11) After you select Create, the deployment will start. In the notification pane, the deployment task will be shown. Select the [Deployment in progress](#) for details.

Notifications

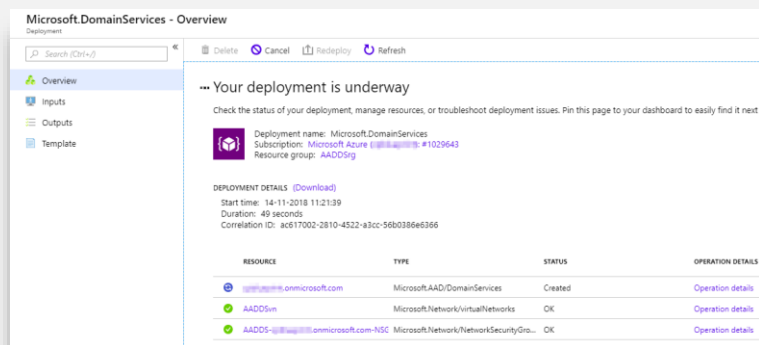
[More events in the activity log](#) [Dismiss all](#)

Deployment in progress... Running

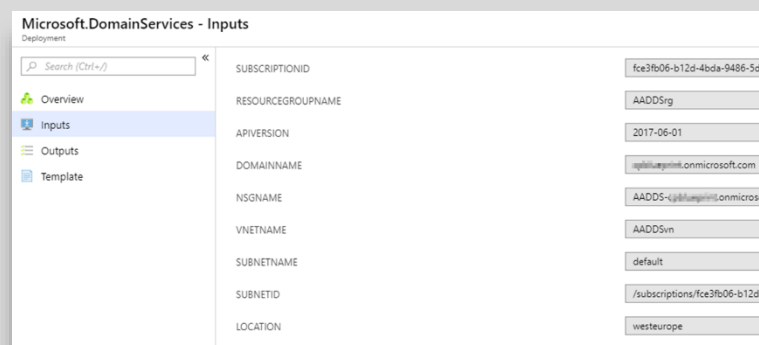
Deployment to resource group 'AADDsrg' is in progress.

by me a few seconds ago

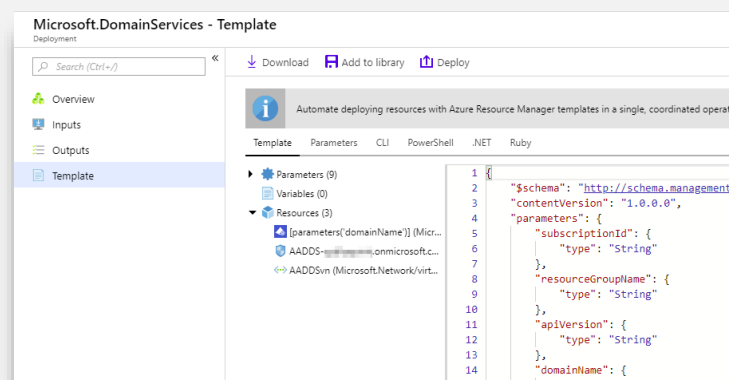
- 12) The deployment will be shown in detail. On the [Overview](#) pane, you'll get an overview of the resources deployed with their progress.



- 13) On the Inputs pane, the parameters used will be shown.



- 14) On the Template pane, you'll see the ARM template that the Azure Portal has generated with your input. This template can be used to redeploy this deployment or as a base for automating other deployments.



- 15) You're done for this exercise! Wait for the deployment to finish.

★ This deployment will run for about 30 minutes.

Activity 2 : Deploy Windows Virtual Desktop

Estimated time to complete this activity

60 minutes

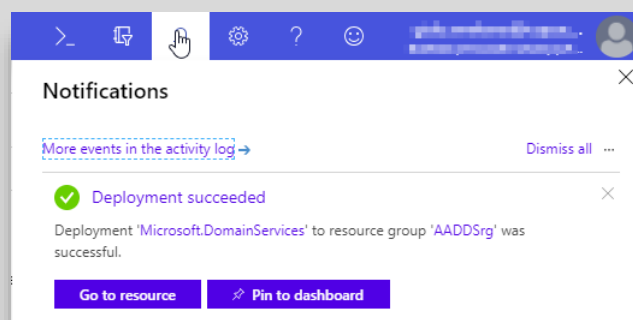
Objectives

In this activity, you will configure the components necessary to perform this lab;

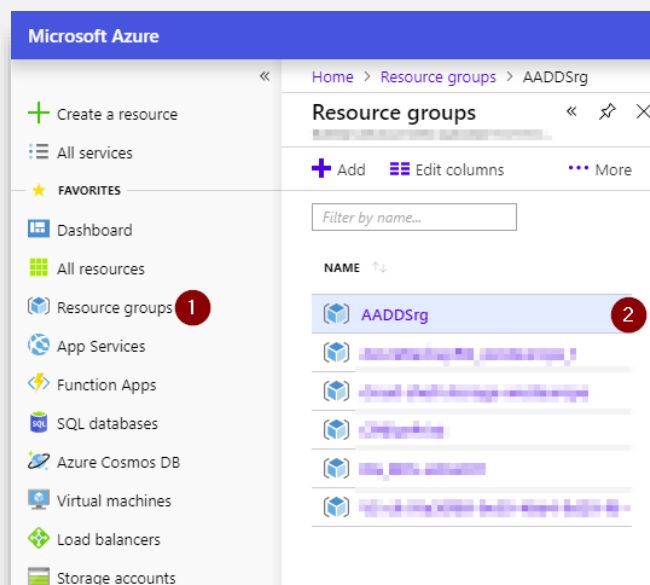
- Finalize the AAD Domain Services deployment
- Prepare and create a Windows Virtual Desktop environment

Exercise 2a: Finalize the AAD Domain Services deployment

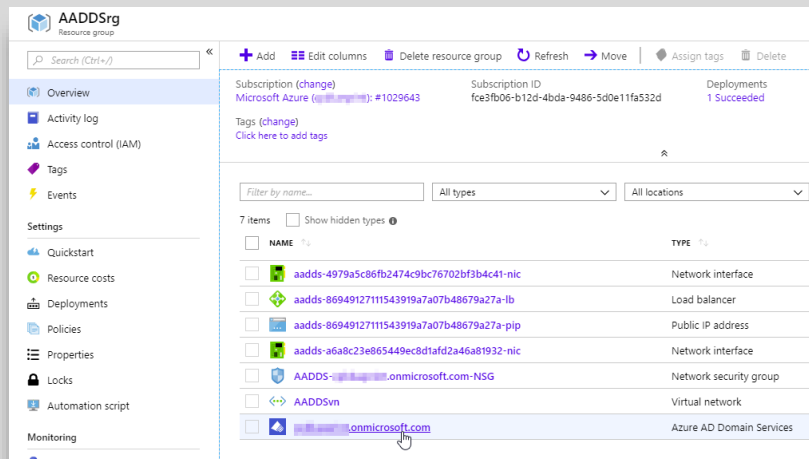
- 1) Verify that the deployment has finished successfully



- 2) Click *Resource Groups* and open *AADDsrg*

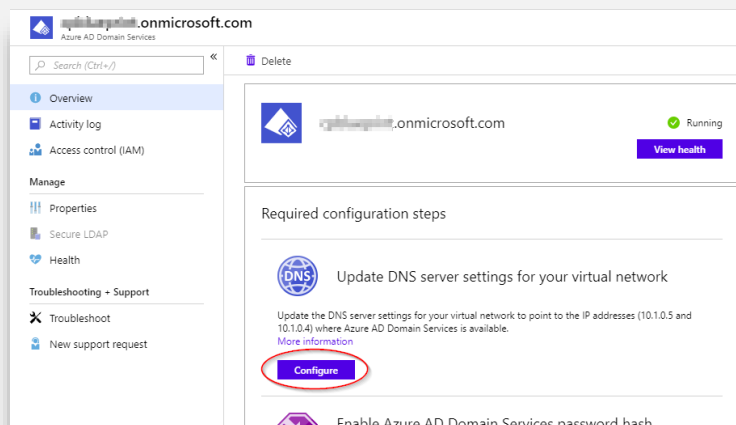


- 3) You can see there are several resources deployed. Open the [Azure AD Domain Services](#) resource by clicking the name.



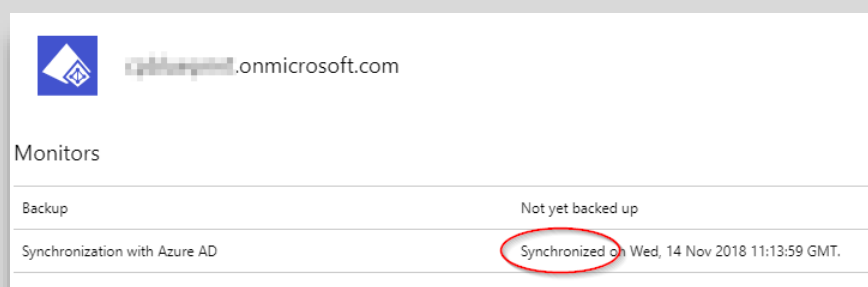
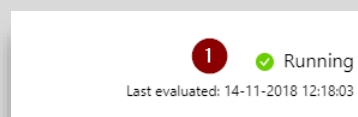
- 4) You'll see that AAD Domain Services is running. To make sure all VM's in the virtual network will use the corresponding DNS Servers, click the [Configure](#) button.

You will be notified to reboot all servers in the virtual network. As there are none, you can safely ignore the notification.

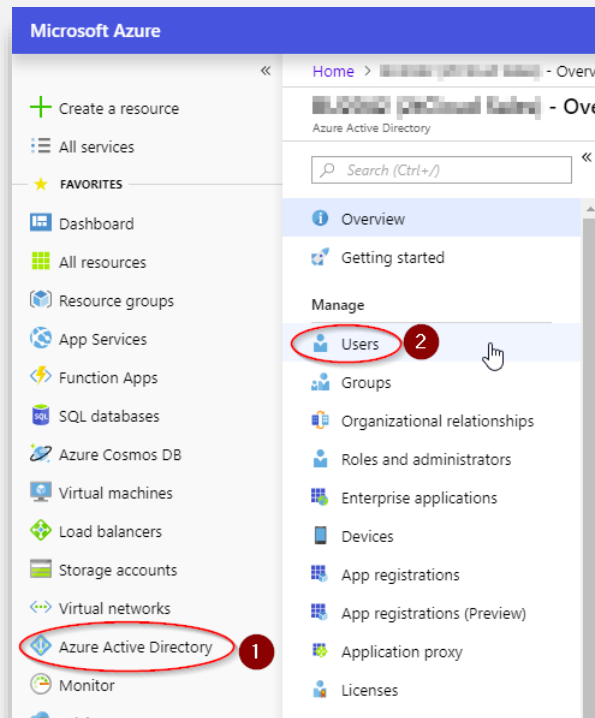


- 5) Browse to the [Health](#) pane and check if the service is [Running](#) and the [synchronization](#) between AAD and AAD Domain Services has taken place.

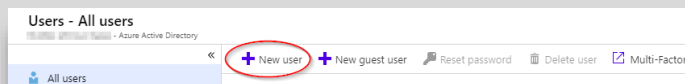
Unfortunately this process can take some time, anywhere from half an hour to several hours. There is no way of speeding this up.



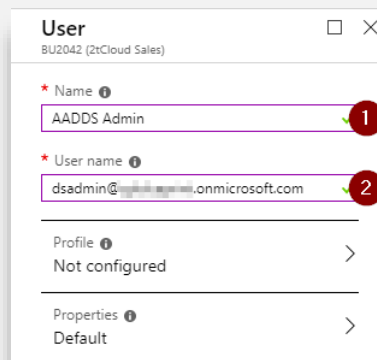
- 6) From the Azure Portal navigation bar, select [Azure Active Directory](#) and browse to [Users](#).



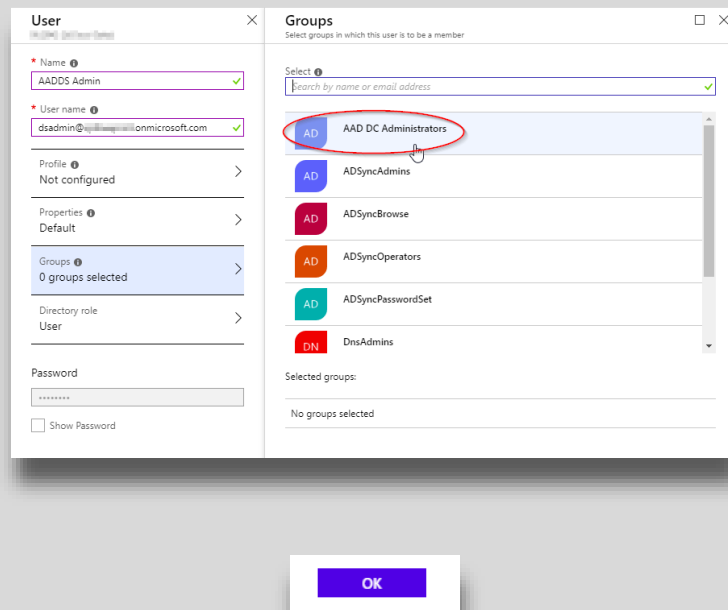
- 7) Create a New User



- 8) Give the new user a recognizable [Name](#), such as **dsadmin@**. Giving your user a upn like admin or administrator will cause problems later on in the process. Please be aware that you should use the same domain that AAD Domain Services is using. **Choose a password that has more than 8 characters!**



- 9) Make the new user member of the *AAD DC Administrators* group.

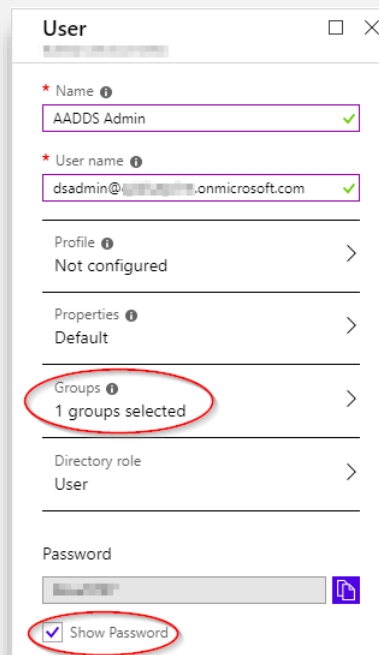


- 10) Make sure the number of *Groups* have now changed.

Please note that this user doesn't need an administrative role in the Azure Active Directory.

Also, select the *Show Password* field.

Make sure you remember the *User Name* and *Password*.



- 11) Open a different browser or open a new InPrivate browser session.

Browse to:
myapps.microsoft.com

Log on using the newly created user account. As this is the first logon, the password has to be changed. Please do so.



Microsoft

dsadmin@ onmicrosoft.com

Uw wachtwoord bijwerken

U moet uw wachtwoord bijwerken omdat u zich voor het eerst aanmeldt of omdat uw wachtwoord is verlopen.

.....

.....

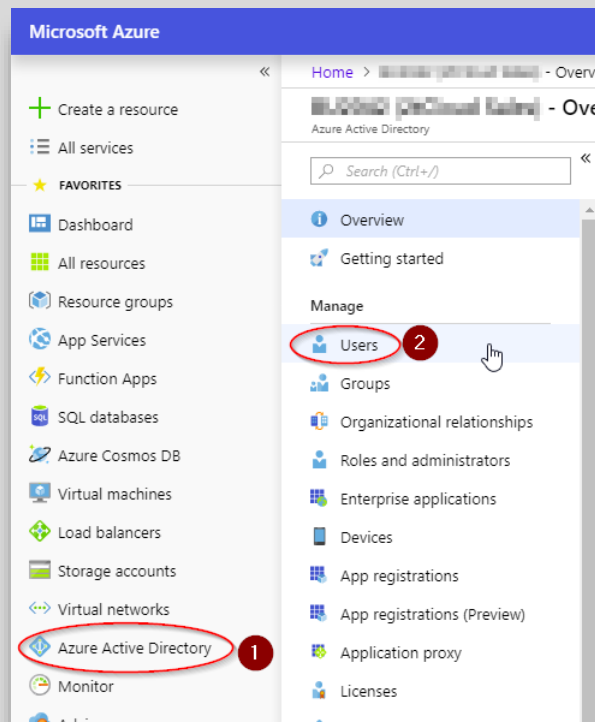
.....

Aanmelden

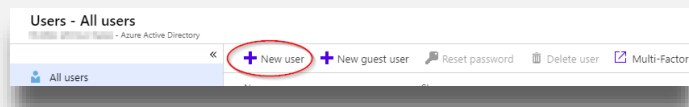
- 12) You will be logged on.
You can safely close the browser session.

Exercise 2b: Create a Test User

- 1) From the Azure Portal navigation bar, select [Azure Active Directory](#) and browse to [Users](#).



- 2) Create a New User

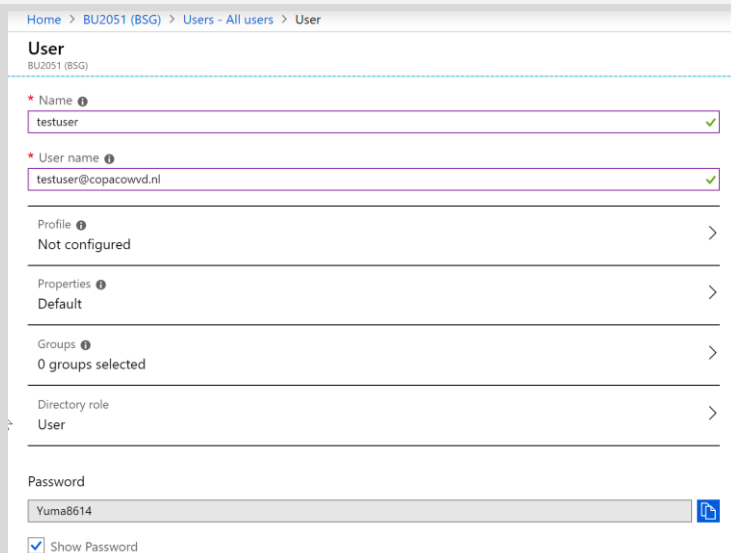


- 3) Give the new user a recognizable [Name](#), For example **TestUser@**

Also, select the [Show Password](#) field.

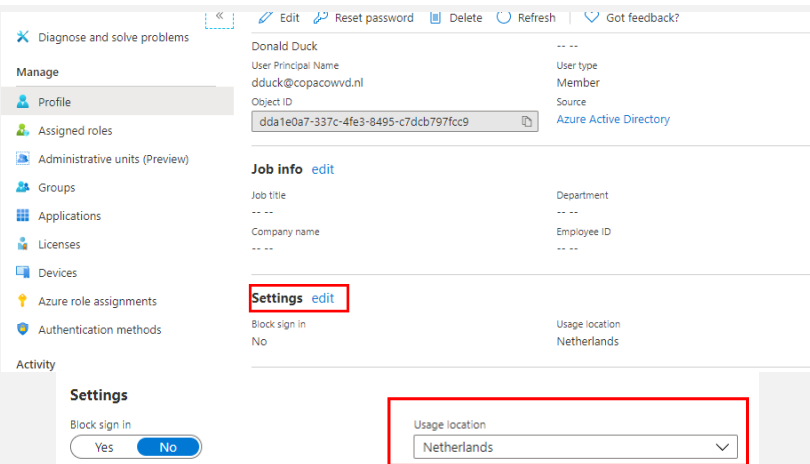
Make sure you remember the [User Name](#) and [Password](#).

Choose Create



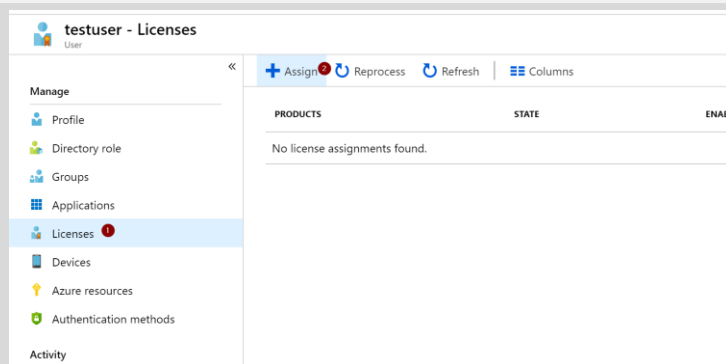
- 4) For the test user edit the settings for the test user.

Set the Usage Location to Netherlands



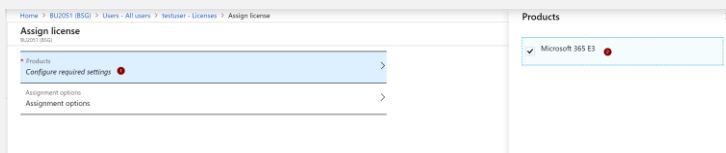
The screenshot shows the Azure Active Directory user interface. On the left, the 'Manage' section includes links for Profile, Assigned roles, Administrative units (Preview), Groups, Applications, Licenses, Devices, Azure role assignments, and Authentication methods. The main area displays user details for 'Donald Duck' (User Principal Name: dduck@copacowvd.nl, Object ID: dda1e0a7-337c-4fe3-8495-c7dcb797fcc9). The 'Settings' tab is highlighted, showing 'Block sign in' as 'No' and 'Usage location' as 'Netherlands'.

- 5) After the test user is created you can open the user and select Licences and Assign



The screenshot shows the 'testuser - Licenses' page. The left sidebar has 'Licenses' selected. The main area shows a table with columns 'PRODUCTS', 'STATE', and 'ENABLED'. Below the table, it says 'No license assignments found.' The 'Assign' button is visible at the top right of the main area.

- 6) Choose Configure required settings and select the Microsoft 365 Business Premium License (or another M 365 license) and choose Select and Assign

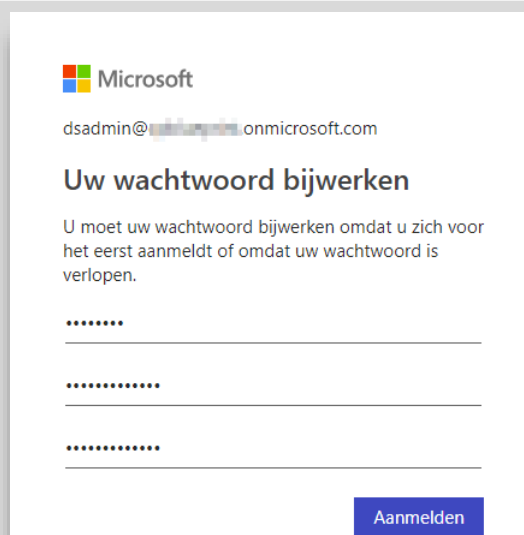


The screenshot shows the 'Assign license' dialog box. The 'Products' tab is selected, and 'Microsoft 365 E3' is chosen. The 'Assign license' button is visible at the bottom right of the dialog.

- 7) Open a different browser or open a new InPrivate browser session.

Browse to:
myapps.microsoft.com

Log on using the newly created user account. As this is the first login, the password has to be changed. Please do so.

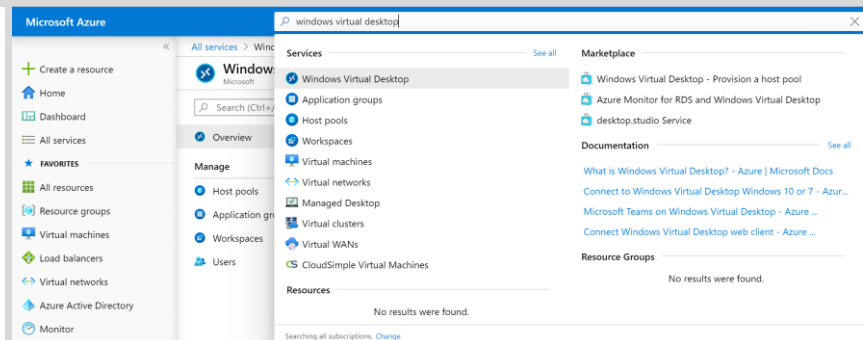


The screenshot shows the Microsoft login page. The user is 'dsadmin@...onmicrosoft.com'. The page prompts the user to change their password: 'U moet uw wachtwoord bijwerken omdat u zich voor het eerst aanmeldt of omdat uw wachtwoord is verlopen.' There are three password input fields and an 'Aanmelden' button.

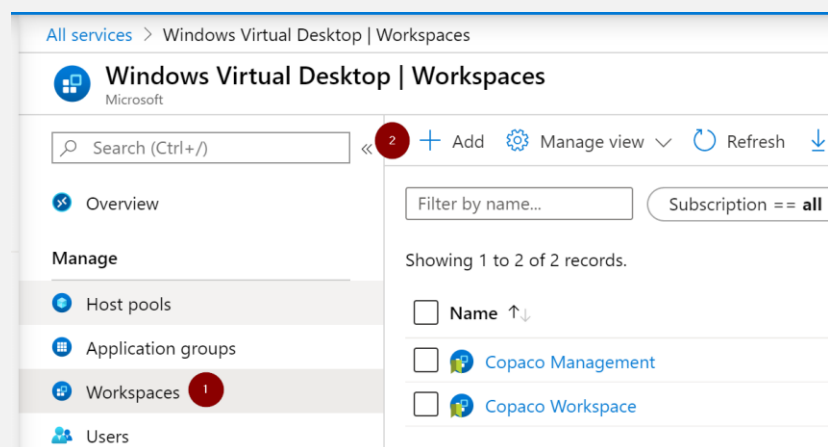
- 8) You will be logged on. You can safely close the browser session.

Exercise 2c : Create Windows Virtual Desktop Workspace

- 1) Log in into the Azure Portal and search for Windows Virtual Desktop



- 2) Select Workspaces and select Add

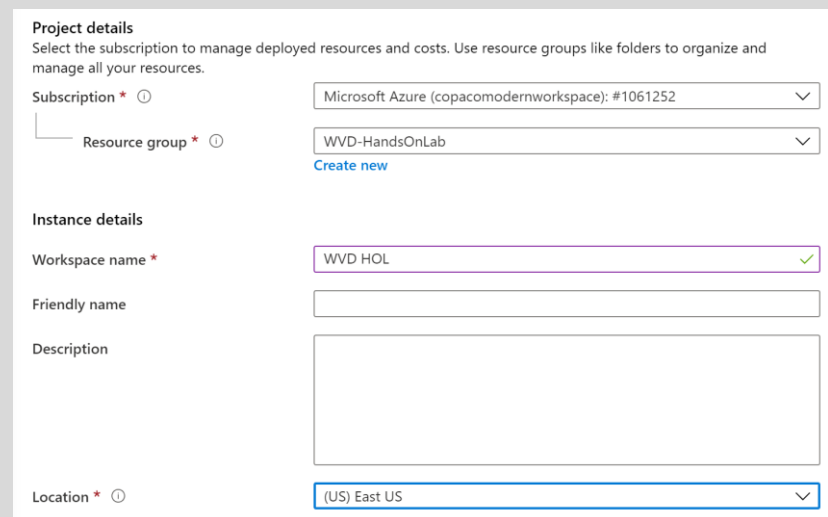


- 3) Select your Resource Group

Give the Workspace a name. This name will be visible to end users.

Choose a location. During the preview only US regions are available.

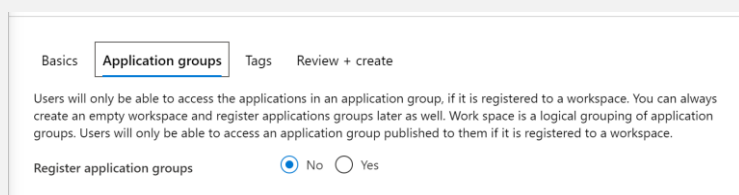
Choose Next: Application Groups



The screenshot shows the 'Project details' form for creating a Windows Virtual Desktop workspace. The form is divided into several sections: 'Subscription', 'Resource group', 'Instance details', and 'Location'. The 'Subscription' dropdown is set to 'Microsoft Azure (copacomodernworkspace); #1061252'. The 'Resource group' dropdown is set to 'WVD-HandsOnLab'. The 'Instance details' section includes a 'Workspace name' field with the value 'WVD HOL' and a green checkmark, a 'Friendly name' field, and a 'Description' text area. The 'Location' dropdown is set to '(US) East US'. There is a 'Create new' link next to the 'Resource group' dropdown.

- 4) Set Register application groups to **No**.

Select Review and Create



The screenshot shows the 'Application groups' tab in the 'Review + create' step of the workspace creation process. The tab is selected, and the 'Basics' tab is also visible. The 'Tags' and 'Review + create' tabs are also present. The main content area contains a message: 'Users will only be able to access the applications in an application group, if it is registered to a workspace. You can always create an empty workspace and register applications groups later as well. 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.' Below this message is a checkbox labeled 'Register application groups' with the 'No' option selected.

Exercise 2D: Create a Windows Virtual Desktop Host Pool

- 1) On the Host Pools tab, select Add

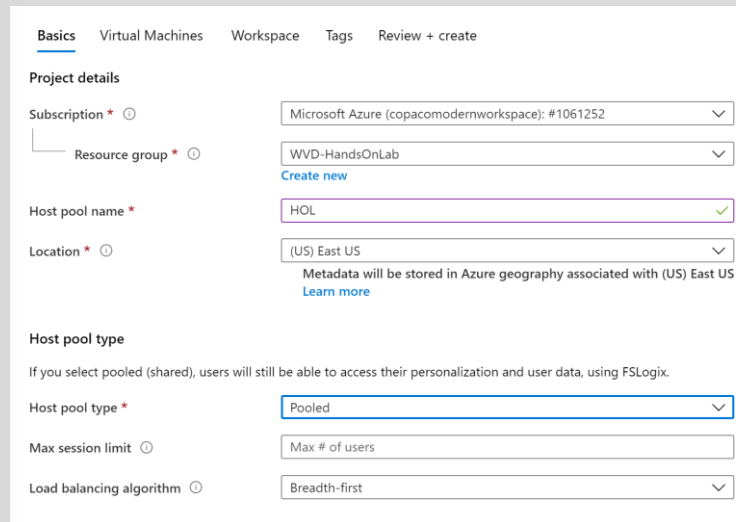
Select your Resource Group

Give the Host Pool a name.

For Location you can only choose US based locations. Once the spring release becomes GA you will be able to select West Europe

Host pool type will be pooled

for load balancing select Breadth first



Basics Virtual Machines Workspace Tags Review + create

Project details

Subscription * ⓘ Microsoft Azure (copacomodernworkspace): #1061252

Resource group * ⓘ WVD-HandsOnLab

Host pool name * HOL

Location * ⓘ (US) East US

Metadata will be stored in Azure geography associated with (US) East US [Learn more](#)

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 * Pooled

Max session limit ⓘ Max # of users

Load balancing algorithm ⓘ Breadth-first

- 2) On the Virtual machine tab choose yes to add VM's

Select the correct resource group

Virtual machine location, select West Europe

Vm size should be the D2as V4

Number of VMs = 1

choose a name prefix

Image type is Gallery and choose the W 10 Enterprise multi session

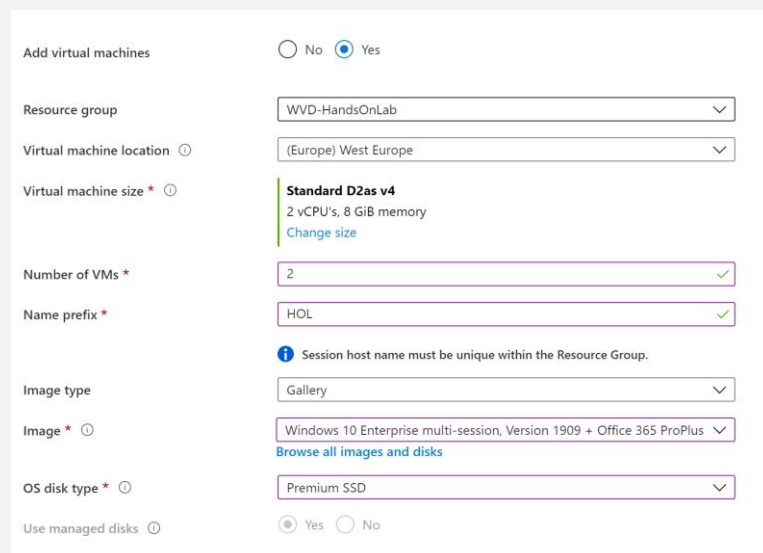
Os disk type should be set to premium ssd

Virtual network should be the vnet that you created in exercise 1c. In the lab this was called **AADDsvn**

select the correct Vnet

No public ip address

No Network security group



Add virtual machines ☐ No ☒ Yes

Resource group WVD-HandsOnLab

Virtual machine location ⓘ (Europe) West Europe

Virtual machine size * ⓘ Standard D2as v4
2 vCPU's, 8 GiB memory
[Change size](#)

Number of VMs * 2

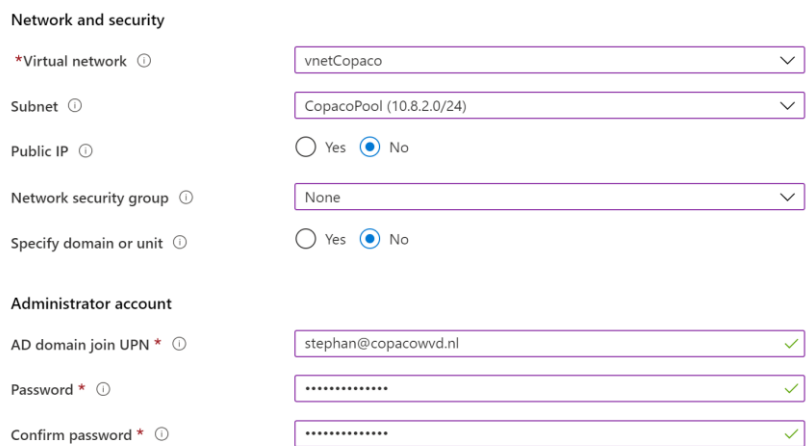
Name prefix * HOL

Image type Gallery

Image * ⓘ Windows 10 Enterprise multi-session, Version 1909 + Office 365 ProPlus
[Browse all images and disks](#)

OS disk type * ⓘ Premium SSD

Use managed disks ⓘ ☒ Yes ☐ No



Network and security

*Virtual network ⓘ vnetCopaco

Subnet ⓘ CopacoPool (10.8.2.0/24)

Public IP ⓘ ☐ Yes ☒ No

Network security group ⓘ None

Specify domain or unit ⓘ ☐ Yes ☒ No

Administrator account

AD domain join UPN * ⓘ stephan@copacowvd.nl

Password * ⓘ *****

Confirm password * ⓘ *****

AD Domain Join UPN is the Azure AD Domain services account you have created in exercise 1c

- 3) On the workspace tab select the workspace that was created in exercise 2b

Basics Virtual Machines **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 desktop app group ☐ No ☒ Yes

*To this workspace [Create new](#)

- 4) Choose review and create
- 5) Wait for the deployment to finish

■ ■ ■ Your deployment is underway

Deployment name: HostPool-05e5037e-c4d0-435a-a0b9-18e6811... Start time: 5/25/2020, 1:47:30 PM
Subscription: Microsoft Azure (copacomodernworkspace): #1061252 Correlation ID: 7721cd1e-eb5f-4de4-a5b6-167b2fe60728
Resource group: WVD-HandsOnLab

Deployment details [\(Download\)](#)

Resource	Type	Status	Operation details
No results.			

- 6) After the deployment is ready you can view your host pool

Windows Virtual Desktop | Host pools

Search (Ctrl+/) << + Add Manage view Refresh Export to CSV Assign tags Feedback

Filter by name... Subscription == all Resource group == wvd-handsonlab Location == all

Showing 1 to 1 of 1 records.

Name	Resource group
HOL	WVD-HandsOnLab

- 7) To give permissions to join the host pool, Select your host pool and select Application groups

HOL | Application groups

Search (Ctrl+/) << + Add Refresh Remove

Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Settings Properties Locks Export template

Manage **Application groups** Session hosts

Monitoring Diagnostic settings Support + troubleshooting New support request

Desktop application group
Click to configure the desktop application group. There can only be one desktop per host pool.

Name	Users
HOL-DAG	0

RemoteApp application groups

Name	Friendly name	Location	Subscription	Resource group
There are no RemoteApp application groups within this host pool.				

- 8) Select the Desktop Application group, in the example this is called HOL-DAG

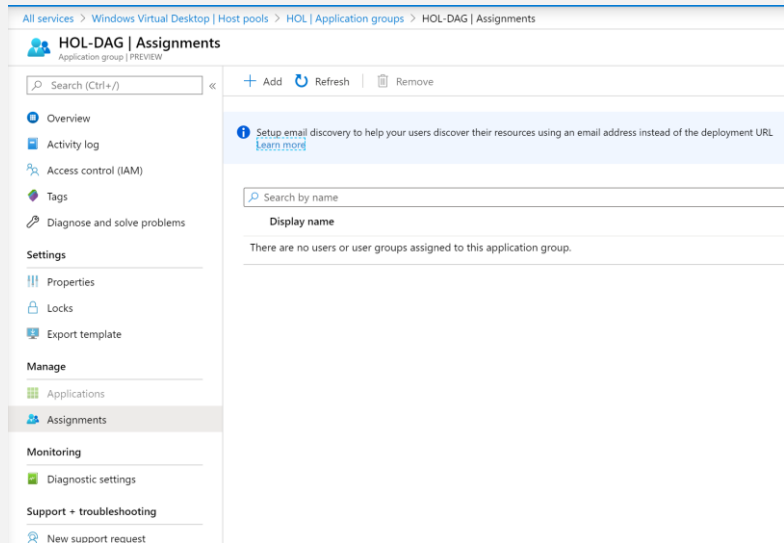
Desktop application group
Click to configure the desktop application group. There can only be one desktop per host pool.

Name	Users
HOL-DAG	0

RemoteApp application groups

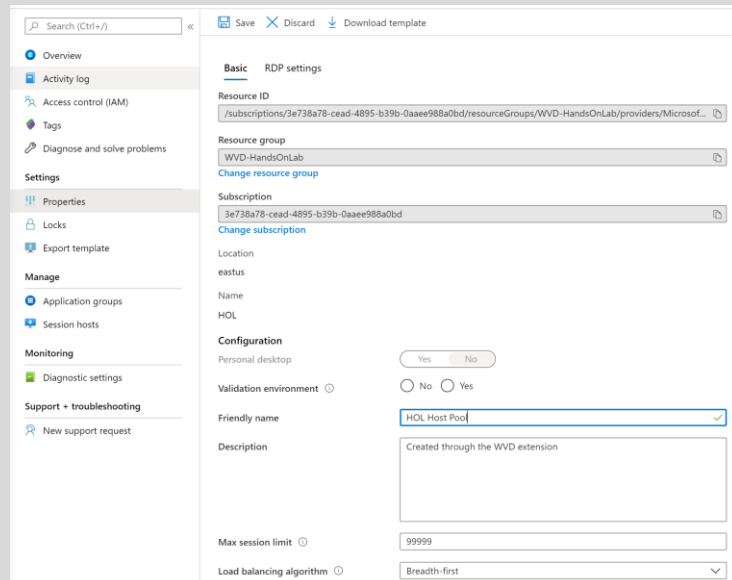
Name	Friendly name	Location	Subscription	Resource group	Ap
There are no RemoteApp application groups within this host pool.					

- 9) Go to assignments and choose Add
- 10) Here you add the users that need to access you Host pool. Note that you can also select groups (this was not available pre spring update 2020)



- 11) Go back the the Host pool tab.

select Properties. Here you can change some basic settings like giving the Host Pool a friendly name.



Activity 3: Set up FSlogix on Azure Files

Estimated time to complete this activity

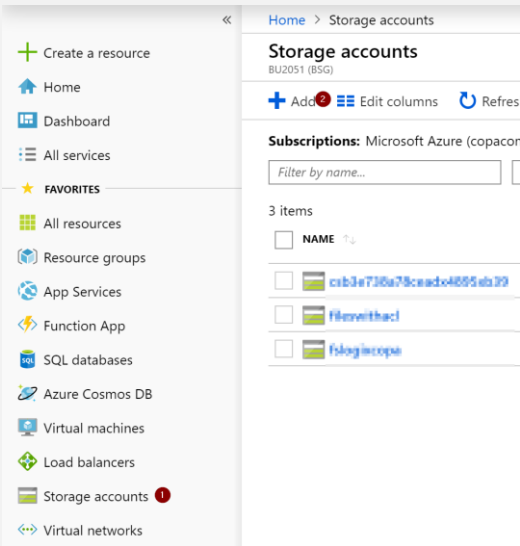
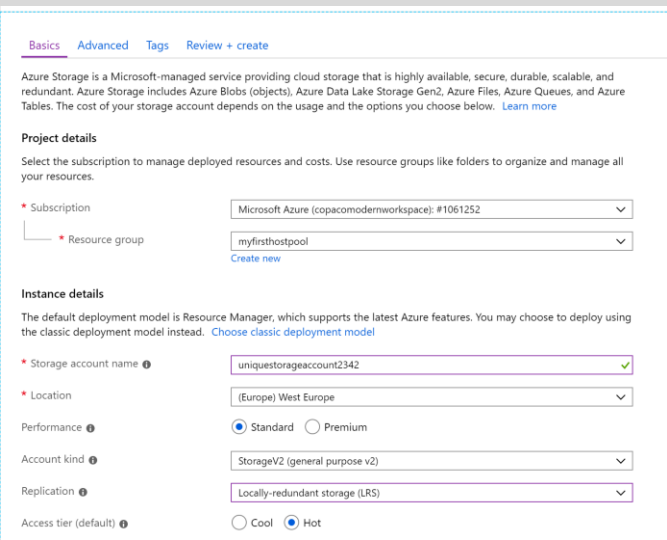
60 minutes

Objectives

In this activity, you will configure the components necessary to perform this lab;

- Deploy FSlogix for user profiles

Exercise 3a: Prepare FSlogix Storage

<p>1) Login in the Azure Portal</p>	<p>https://portal.azure.com</p>
<p>2) Select Storage accounts and click Add</p>	
<p>3) Use the following settings:</p> <p>a) Subscription: Select your test subscription</p> <p>b) Resource Group, choose a resource group or create a new one</p> <p>c) Storage account name: Give you storage account a globally unique name The name has a limit of 15 characters</p>	

d) Location: **West Europe**

e) Performance: Standard

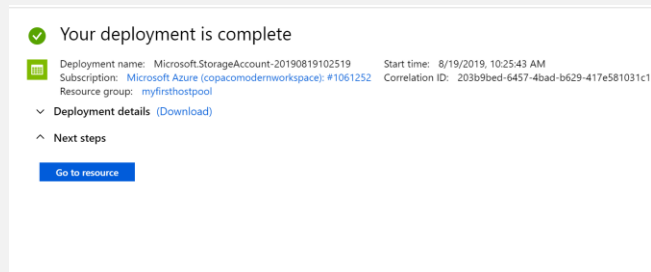
f) Account kind: StorageV2

g) Replication: Locally-redundant storage)

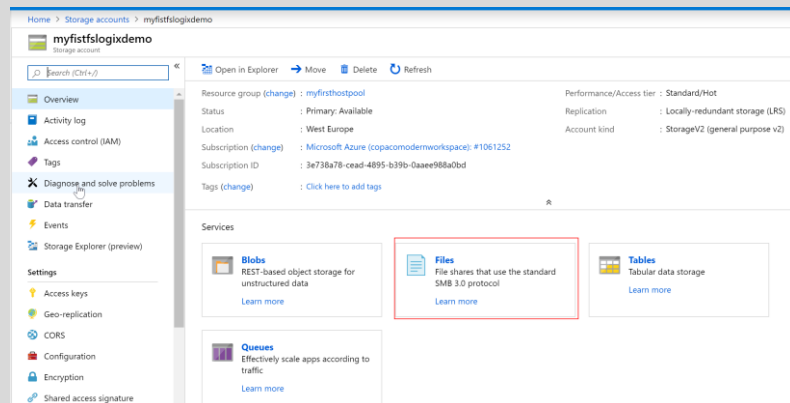
h) Access tier: Hot

- 4) Select review + create
- 5) Choose to create

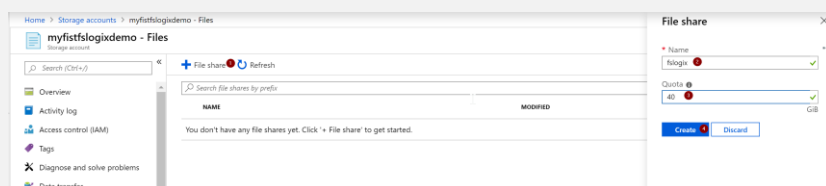
- 6) When finished you **go to the resource**



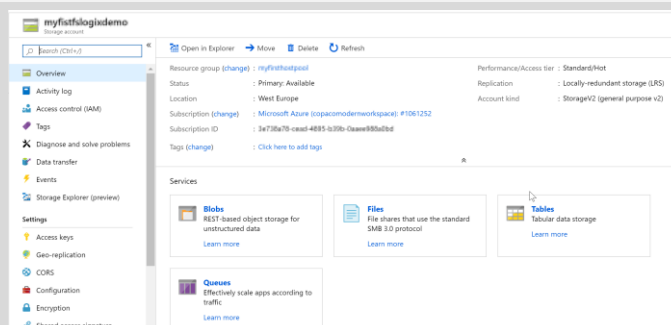
- 7) Here you can select **Files**



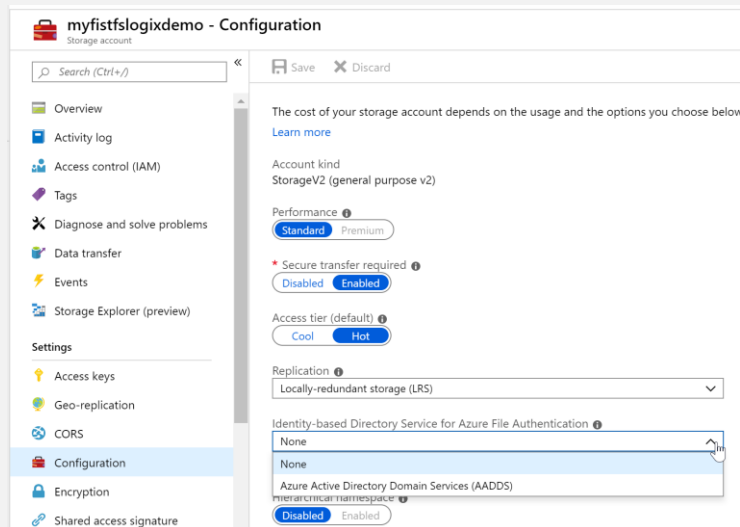
- 8) Choose + **File Share**
- 9) Give your file share a name (fslogix)
- 10) Give your file share a quota (40)
- 11) Click Create



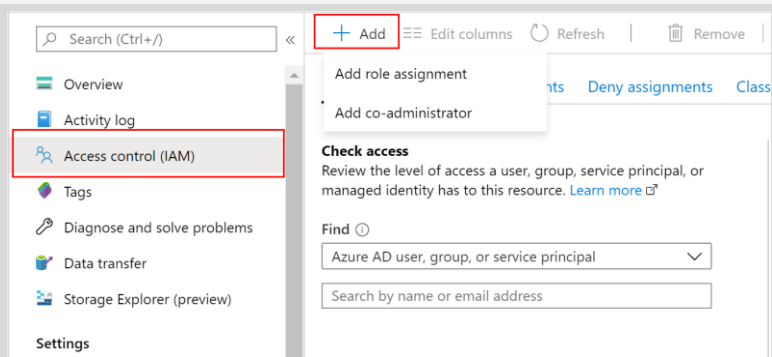
- 12) From the left pane choose **Configuration**



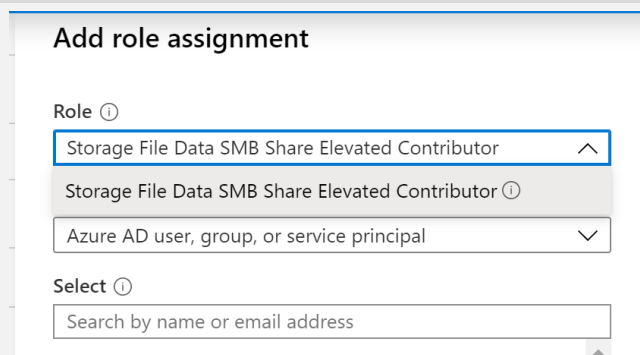
- 13) In the configuration select Azure Active Directory Domain Services (AADDS) in the Identity-based Directory Services for Azure File Authentication.
- 14) Choose **Save**



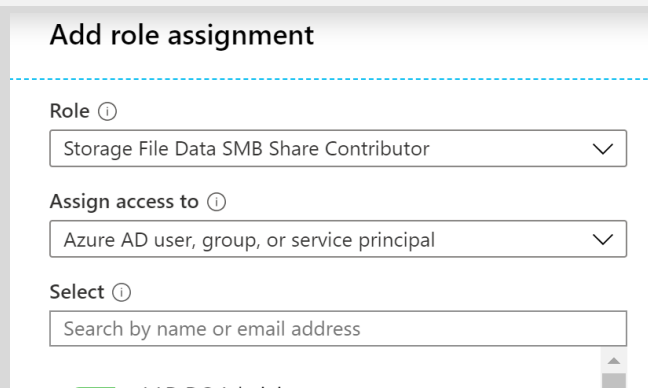
- 15) From the left pane select Access control (IAM)
- 16) Choose Add and Add role assignment



- 17) For role you select **Storage File Data SMB Share Elevated Contributor** and for user you select your **admin user**
- 18) Choose save.



- 19) Repeat the step but now select **Storage File Data SMB Share Contributor** and for user select your **test user**



Exercise 3b : Configure FSLogix

1) Open a web browser and go to:

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

- 2) Sign in with your **admin credentials**
- 3) Open the desktop you created
- 4) Review the Access Local resources settings and choose to allow
- 5) Sign in using the admin credentials

WVD Copaco



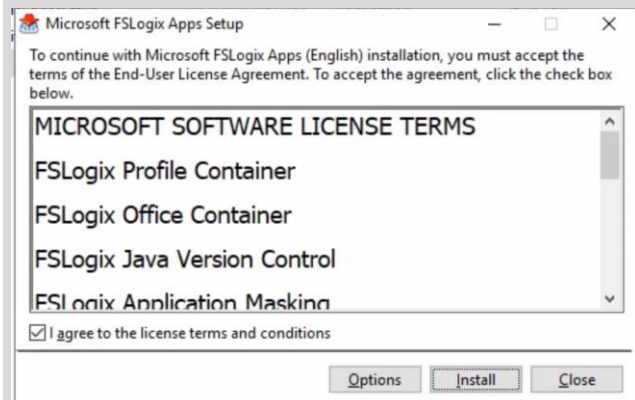
6) Go to the link to download the software

<https://docs.microsoft.com/en-us/fslogix/install-#download-fslogix>

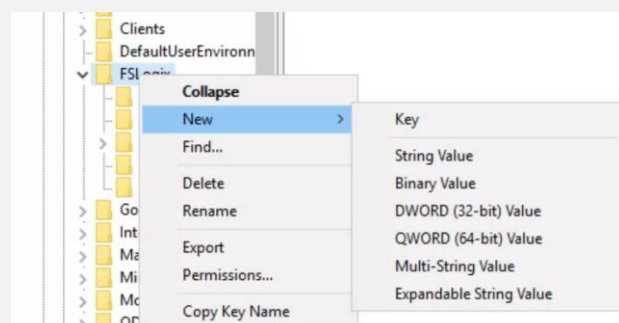
- 7) Extract the downloaded folder and open the x64 and release folder
- 8) Run the FSLogixAppSetup as **an administrator**

Name	Date modified	Type
FSLogixAppsJavaRuleEditorSetup	8/19/2019 11:01 AM	Application
FSLogixAppsRuleEditorSetup	8/19/2019 11:02 AM	Application
FSLogixAppsSetup	8/19/2019 11:02 AM	Application

- 9) Select I Agree to the license terms and conditions
- 10) Choose to install
- 11) After the installation is finished open regedit as **an administrator**



12) In Fslogix create a new **Key** names **Profiles**



13) In the newly created profiles key create **2 entries**

a) REG_DWORD with Name **Enabled** and value **1**

b) Multi-string Value with name **VHDLocations** and value is the path to your file share

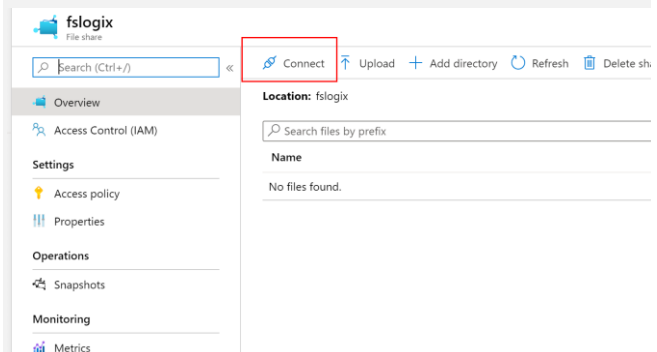
\\[NameStorageAccount.file.core.windows.net\[NameFileshare]



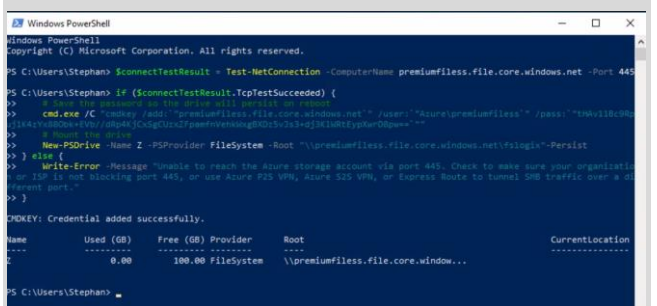
14) Now we have to mount the file share to the client. To do this go to the azure portal and to the storage account.

here go to your created share where you can find the Connect button

15) Copy the Powershell commands

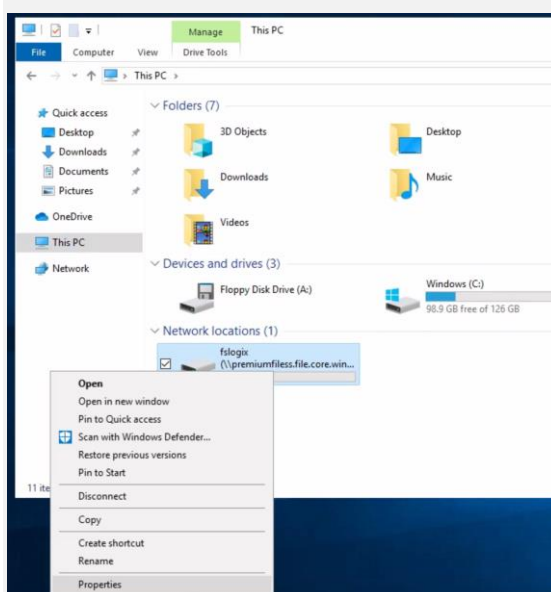


16) Go back to your WVD web session and open a normal Powershell command (no admin rights required) and paste the command in the powershell window.



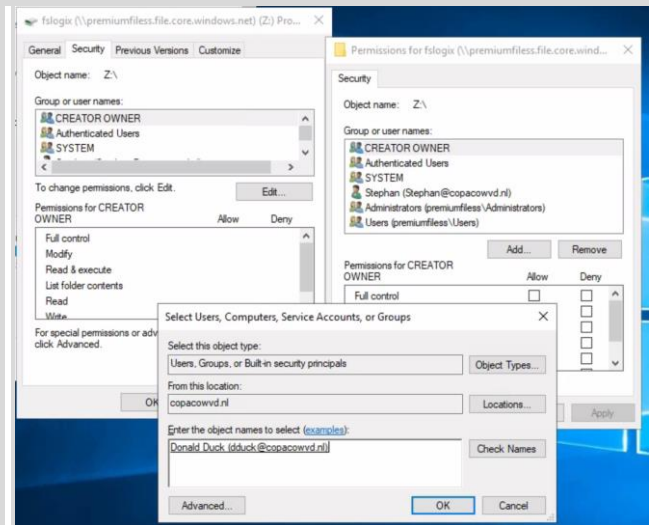
17) Open the file explorer and here you should see the newly added drive.

18) Select the drive and select properties.





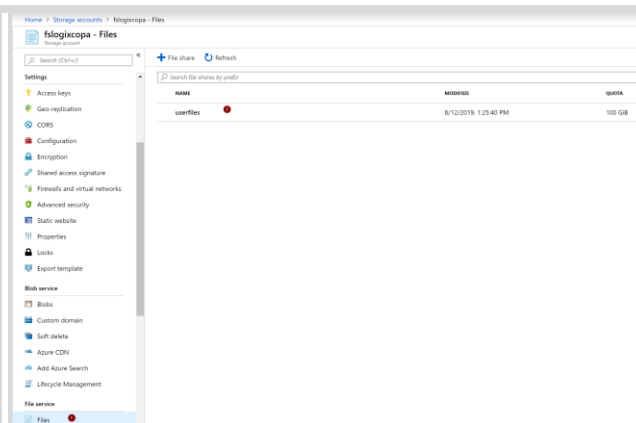
- 19) Go to Security
- 20) Select Edit
- 21) Select add. Here you can add domain users.
Make sure to give this user Full Control Rights.



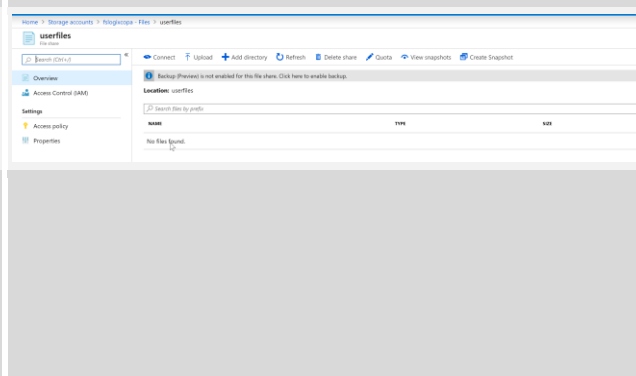
- 22) Reboot the server

Exercise 3c: Check your configuration

- 1) Go to the **Azure portal** and select **storage accounts** and your **storage account**
- 2) Go to **Files** and open your **file share**

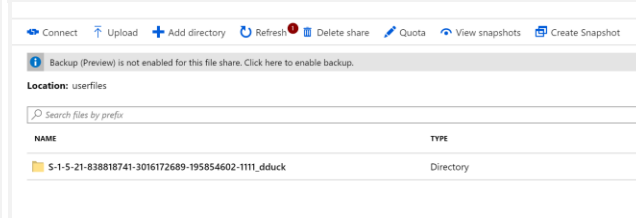


- 3) Note that the file share is empty



- 4) Open a new browser and go to <https://rdweb.vwd.microsoft.com/arm/webclient/index.html>
- 5) Sign in using the credentials for your **test account**
- 6) Launch your **WVD desktop**
- 7) Wait for the session to start

- 8) Go back to the Azure Portal and refresh the view. You should now see a new folder containing the vhd file .



Activity 4: Conditional Access

Estimated time to complete this activity

30 minutes

Objectives

In this activity, you will configure the components necessary to perform this lab;

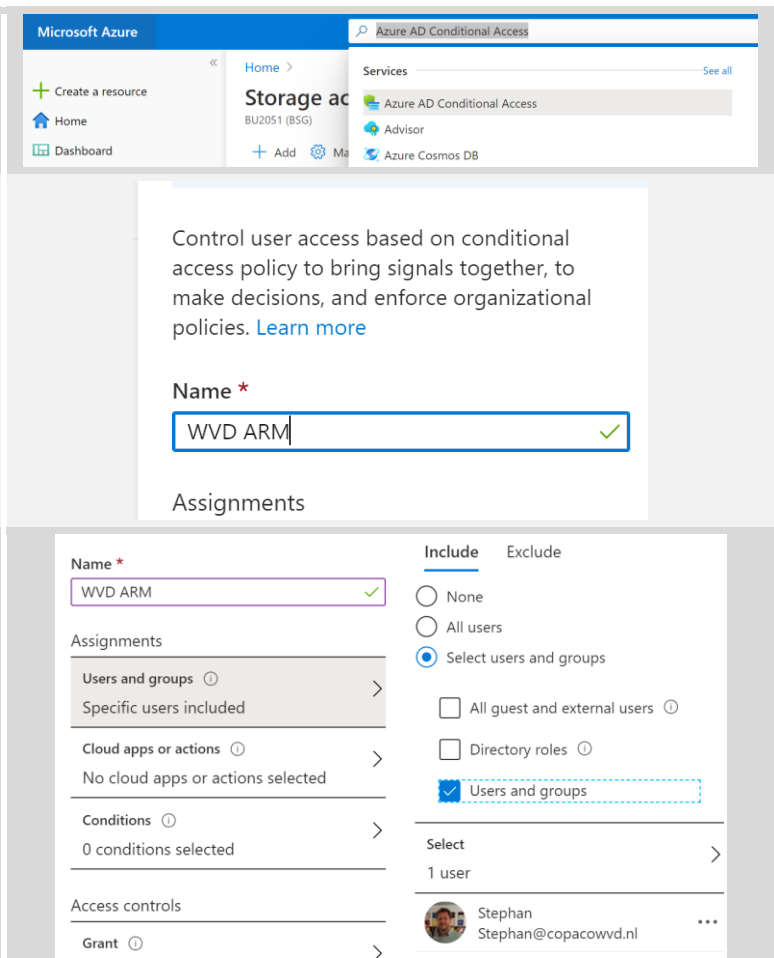
- Use Conditional Access to enforce MFA on WVD

Exercise 4a: Configure Conditional Access for WVD

- 1) Go to the Azure portal and search for Azure AD Conditional Access

- 2) Select + New Policy
- 3) Give the new policy a name

- 4) Select Users and groups
- 5) Select Select users and groups, there you select your test users.



The screenshot shows the Azure portal interface for configuring a new Azure AD Conditional Access policy. The top navigation bar includes 'Microsoft Azure' and a search bar. The left sidebar shows 'Home' and 'Dashboard'. The main content area is titled 'Azure AD Conditional Access' and displays a list of services, including 'Azure AD Conditional Access', 'Advisor', and 'Azure Cosmos DB'. Below this, a card titled 'Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)' is visible. The 'Name' field is set to 'WVD ARM'. The 'Assignments' section is expanded, showing 'Users and groups' selected. The 'Include' tab is active, and the 'Select users and groups' option is chosen. The 'Users and groups' section is expanded, showing a list of users, including 'Stephan' (Stephan@copacowvd.nl).



- 6) Select Cloud apps or actions
- 7) Select, Select apps
- 8) Search for Windows virtual Desktop (App ID 9cdead84-a844-4324-93f2-b2e6bb768d07)

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *
WVD ARM ✓

Assignments

Users and groups ⓘ
Specific users included >

Cloud apps or actions ⓘ
1 app included >

Conditions ⓘ
0 conditions selected >

Access controls

Grant ⓘ
0 controls selected >

Session ⓘ
0 controls selected >

Control user access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to
Cloud apps User actions

Include Exclude

☐ None
☐ All cloud apps
☒ Select apps

Select >

Windows Virtual Desktop

WV Windows Virtual Desktop
9cdead84-a844-4324-93f2-b2e6bb768d07

- 9) Select Grant
- 10) Here you select Grant Access

Require Multi-factor authentication

Require all the selected controls

Grant

Control user access enforcement to block or grant access. [Learn more](#)

- ☐ Block access
☒ Grant access

☒ Require multi-factor authentication ⓘ

☐ Require device to be marked as compliant ⓘ

☐ Require Hybrid Azure AD joined device ⓘ

☐ Require approved client app ⓘ
[See list of approved client apps](#)

☐ Require app protection policy (Preview) ⓘ
[See list of policy protected client apps](#)

For multiple controls

- ☒ Require all the selected controls
☐ Require one of the selected controls

- 11) Select Session
- 12) Select Sign-in frequency

enter 1


select hours

Session

Control user access based on session controls to enable limited experiences within specific cloud applications.

[Learn more](#)

☐ Use app enforced restrictions ⓘ

 This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Click here to learn more.

☐ Use Conditional Access App Control ⓘ

☒ Sign-in frequency ⓘ

1

Hours

☐ Persistent browser session ⓘ

- 13) You can now Enable the policy and select Create

Make sure you only selected your test user, don't lock yourself out of the environment!

Enable policy

Report-only **On** Off

Create

Exercise 4b: Test Conditional Access

To test is your Conditional Access policy is working you can use the What If dialog.

- 1) In the Conditional Access panel select What If

Home > Conditional Access | Policies

Azure Active Directory

Polices << + New policy What If Got feedback?

Create your own policies and target specific conditions like Cloud apps, Sign-in risk, and Device platforms with Azure AD Premium →

Policy Name	State
Baseline policy: Require MFA for admins (Preview)	Off
Baseline policy: End user protection (Preview)	Off
Baseline policy: Block legacy authentication (Preview)	Off
Baseline policy: Require MFA for Service Management (Preview)	Off
Windows Virtual Desktop	Rep
MFA	On
WVD ARM	On

- 2) Select your test users
- 3) Cloud apps, select Windows virtual desktop (App ID 9cdead84-a844-4324-93f2-b2e6bb768d07)

Info

Test the impact of conditional access on a user when signing in under certain conditions.

[Learn more](#)

*User ⓘ
dduck@copacowvd.nl

Cloud apps or actions ⓘ
1 app selected

- 4) Select What If
- 5) If the policy is applied you will see the policy appear in the overview.

What If Reset

Evaluation result

Policies that will apply Policies that will not apply

Policy Name	Grant controls	Session controls	State
WVD ARM	Require multi-factor authentication	Sign-in frequency - 1 hour	On

- 6) You can also test the policy by opening a new in private browser session and try to log in with the test account

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

7)



dduck@copacowvd.nl

Approve sign in request

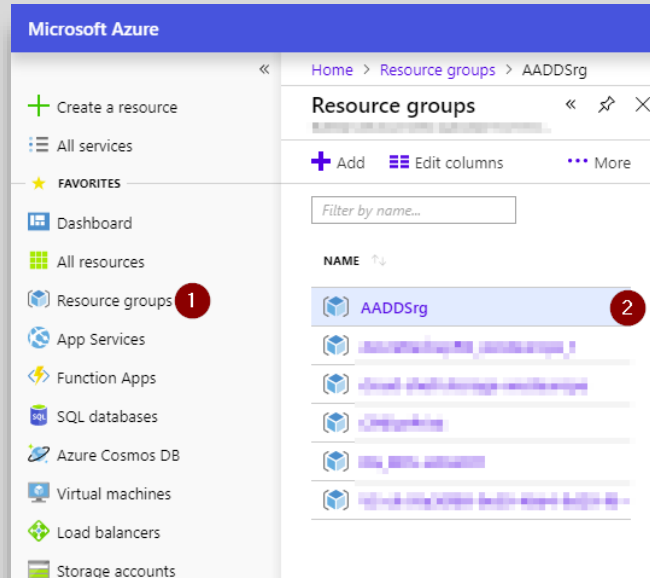
- 🔒 We've sent a notification to your mobile device. Please open the Microsoft Authenticator app to respond.

Having trouble? [Sign in another way](#)

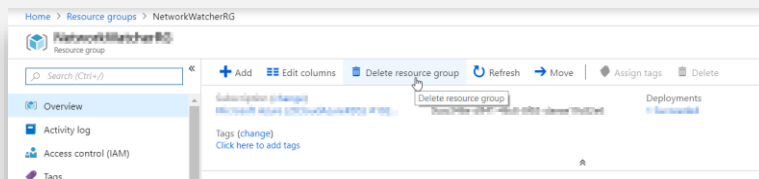
Activity 4: Remove your resources

All the resources you created will cost money if you don't delete them, so if you are ready please delete them

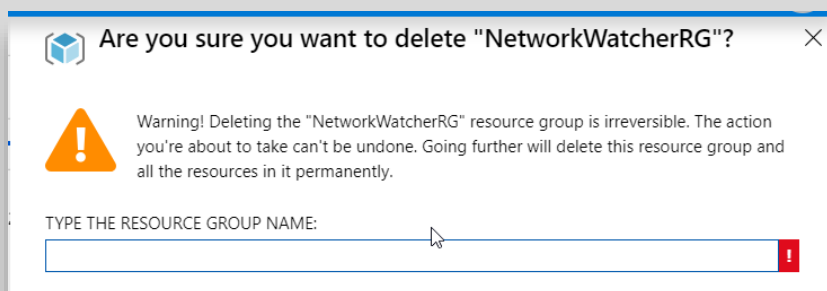
- 1) Click Resource Groups and open AADDsrg



- 2) Choose Delete resource group



- 3) Type the name of the resource group and press delete



Extra resources

RDS 2016 on Azure video

<https://www.youtube.com/watch?v=Xi89A2b5b5w>

RDS architecture designs

<https://docs.microsoft.com/nl-nl/windows-server/remote/remote-desktop-services/desktop-hosting-logical-architecture#highly-available-deployment>

RDS Geo redundant datacenter deployment

<https://docs.microsoft.com/nl-nl/windows-server/remote/remote-desktop-services/rds-multi-datacenter-deployment>

MFA extension

<https://docs.microsoft.com/nl-nl/azure/active-directory/authentication/howto-mfa-nps-extension-rdg>

Azure AD Domain Services

<https://docs.microsoft.com/nl-nl/windows-server/remote/remote-desktop-services/rds-azure-adds>

Azure AD Application Proxy

<https://docs.microsoft.com/nl-nl/azure/active-directory/manage-apps/application-proxy-integrate-with-remote-desktop-services>