

AZURE VIRTUAL DESKTOP (AVD)

Click-to-Run™ Solution Deployment Guide



Azure Virtual Desktop (AVD) Click-to-Run™ Solution

Please note the Information below Includes a Pre-Deployment Checklist based on the Identity and Access Management method you will be utilizing for the Azure Virtual Desktop (AVD) Environment.

In addition to the Click-to-Run™ Solution a fully managed Azure Virtual Desktop Offering Is available upon request.

Table of Contents

- Page 2
Azure Virtual Desktop Pre-Requisites.
- Page 4
Pre-Deployment Checklist (using AADDS)
- Page 8
Pre-Deployment Checklist (using Domain Controller)
- Page 12
Azure Virtual Desktop Click-to-Run™ Deployment
- Page 29
Post deployment Checklist (using AADDS)
- Page 30
Post Deployment Checklist (using Domain Controller)
- Page 31
Common Error Deployment Catalog
- Page 33
Post Deployment – Create a Custom Image for your AVD deployment
- Page 39
Post Deployment - Configure Insights for AVD
- Page 41
Additional Considerations

Pre-Deployment Checklist

- Select and verify the appropriate Windows 10 Licensing is in place Choose your
- Identity Management Infrastructure
 1. Azure Active Directory Domain Services
 2. Connect to existing Domain Controller in Microsoft Azure
- Verify identity Management model is prepared for the AVD Deployment. (Additional Steps required.)
 - Azure AD Domain Services Page # 4 - 7 Domain
 - Controller in Azure Page # 8 - 12

Once the previous steps have been completed, please continue with the following tasks. Each will need to be completed prior to configuring and deploying Azure Virtual Desktop Click-to-Run Solution.

- Ensure Security Defaults are turned off temporarily (If Applicable)

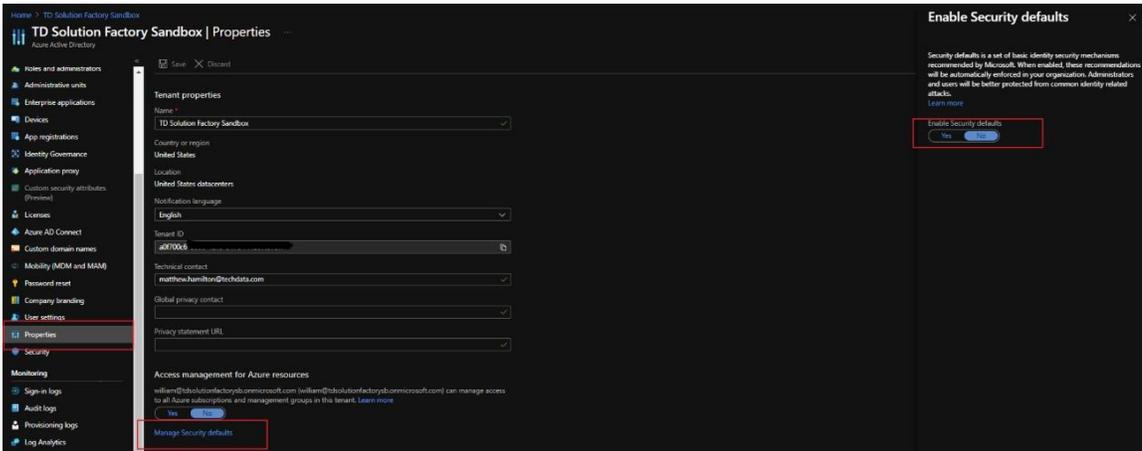
If Using AADDS:

Pre-Deployment Steps (partner must complete)

- Purchase and deploy the AADDS Solution.
- Ensure AADDS is returning a healthy 'Running' state. Deactivate Security
- Defaults on your tenant.
- Ensure Admin is a member of the AAD DC Administrators group. Reset Domain
- Admin password (for password hash sync).
- Ensure DNS is configured on the AADDS Subnet

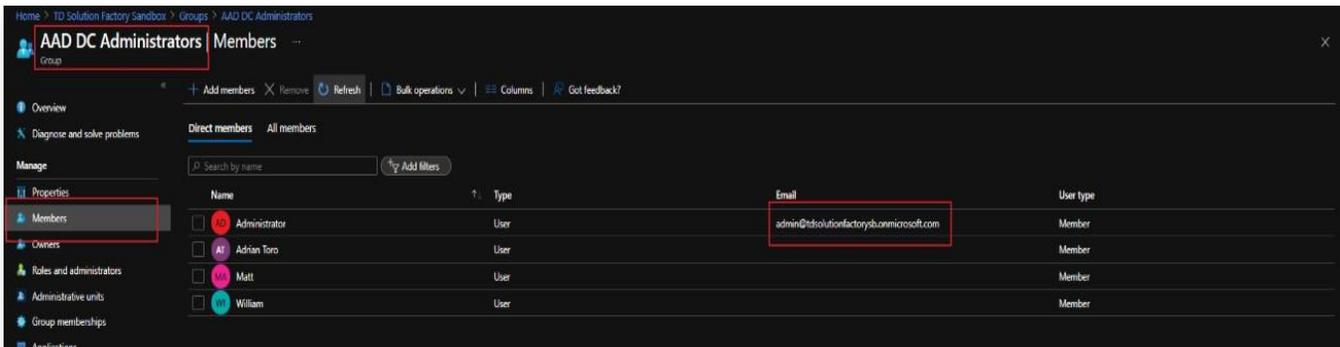
AADDS Pre-Deployment Steps

- 1. Purchase the AADDS (Azure Active Directory Domain Services) solution**
 - a. Configure solution in the digital locker
- 2. Follow AADDS step by step guide for configuration**
 - a. If at any point you are unsure, please reach out to us
- 3. Partner must do the following after the deployment completes AND returns a healthy status.**
 - a. Deactivate security defaults (Temporarily)
 - i. This can be turned back on after deployment

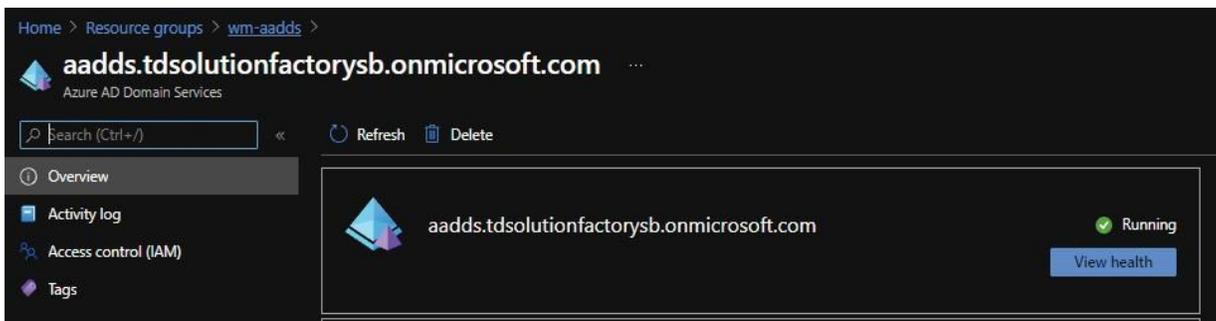


Step 3 continued from previous page

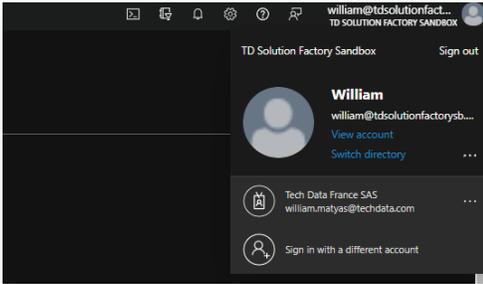
- Identify admin user (This can be found in the group AAD DC Administrators.) Identifying the
- Domain Admin:



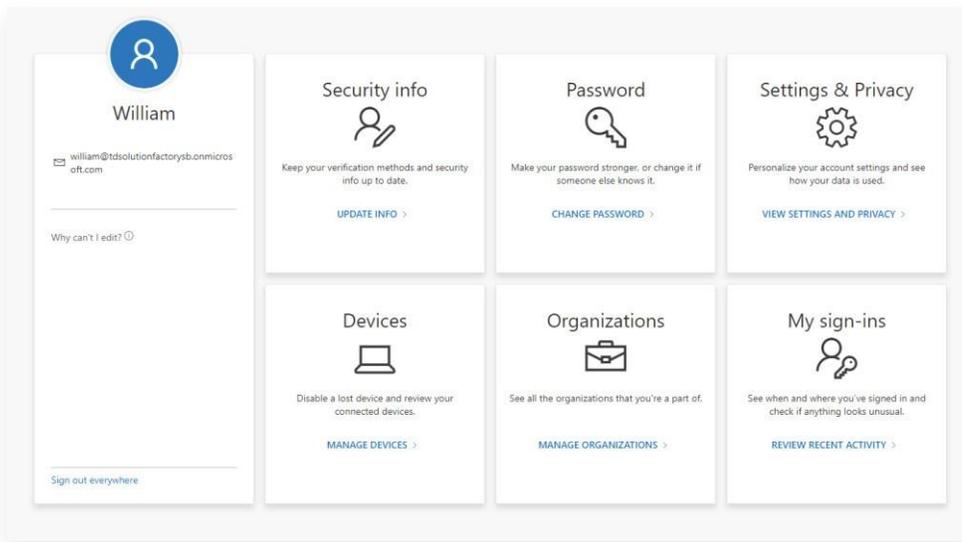
- Make note of domain ex- aadds.partnerAVDtest2020.onmicrosoft.com (you will need this in the AVD Section)



- Reset domain admin password (temporarily)
 - i. Click on your admin profile and on “View Account”



- ii. Select ‘Change password.’



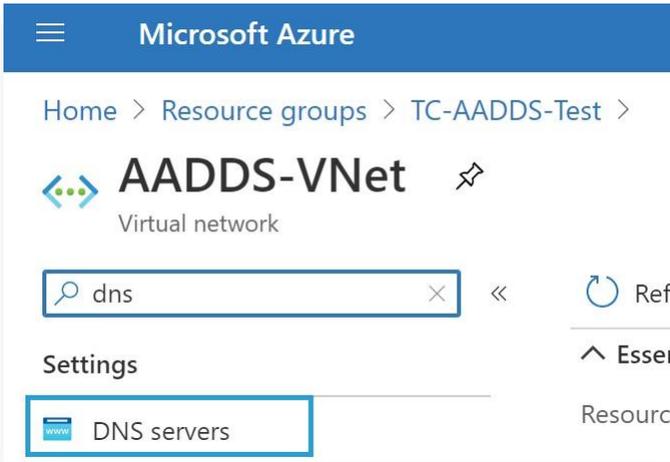
- b. Log out and log back in as the domain admin. You must ensure the login and password are correct for the AVD Deployment.

4. Partner (If using AADDs) Verify DNS Configuration

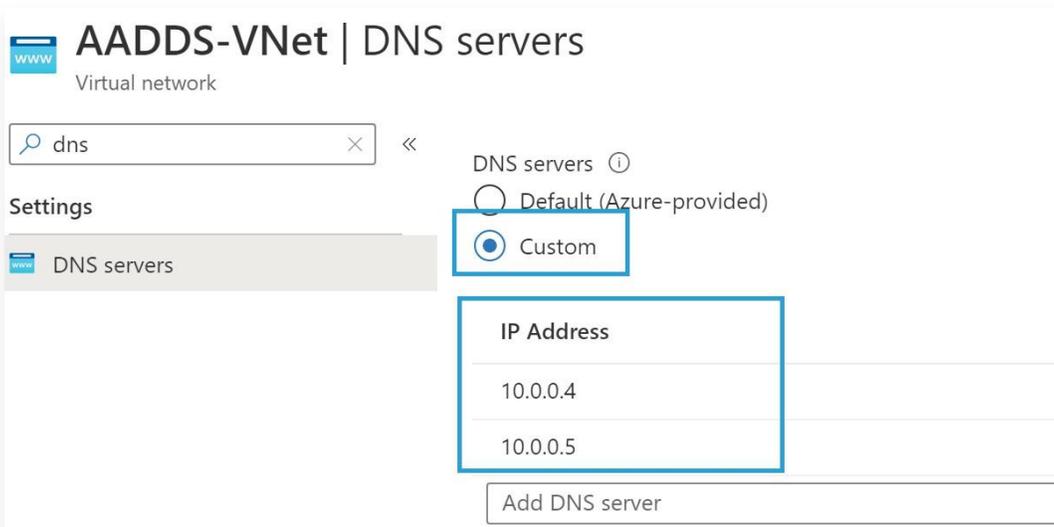
- a. Verify custom DNS is configured on your AADDs VNet.
 - i. Locate your AADDs Vnet.

<input type="checkbox"/>	aadds-a26ef377694f4995ad1884c7242a724d-nic	Network interface	East US
<input type="checkbox"/>	aadds-b16cc18db94c492f9a477e36c3358b7d-lb	Load balancer	East US
<input type="checkbox"/>	aadds-b16cc18db94c492f9a477e36c3358b7d-pip	Public IP address	East US
<input type="checkbox"/>	aadds-ffe9ce32a6d44dd7bffe18efc77d9507-nic	Network interface	East US
<input type="checkbox"/>	AADDs-NSG	Network security group	East US
<input checked="" type="checkbox"/>	AADDs-VNet	Virtual network	East US
<input type="checkbox"/>	aadds.tdsolutionfactorysb.onmicrosoft.com	Azure AD Domain Services	East US
<input type="checkbox"/>	AzureBastionHost	Bastion	East US
<input type="checkbox"/>	bastionHost-pip	Public IP address	East US

ii. Search for and select 'DNS Servers'



iii. Ensure your DNS settings are set to 'Custom' and are pointing to the IP address of your domain controller.



You may now proceed with the AVD Solution Deployment!

If Using Domain Controller with AD Connect:

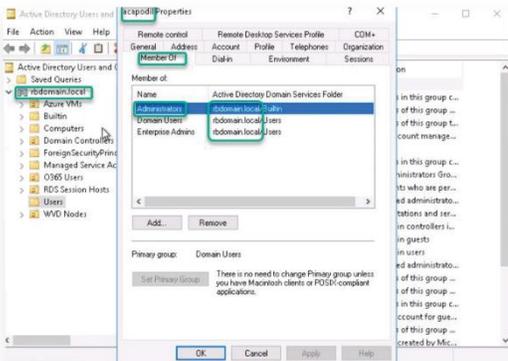
Pre-Deployment Steps (partner must complete)

- Ensure AD Connect is configured and syncing users Azure AD.
- Make sure the Domain Admin you plan to use is in both Domain Admins & Administrators groups
- Create the AVD-Admin & AVD-Users groups Deactivate
- Security Defaults on your tenant.
- Ensure custom DNS is configured on your Domain Controller Vnet.

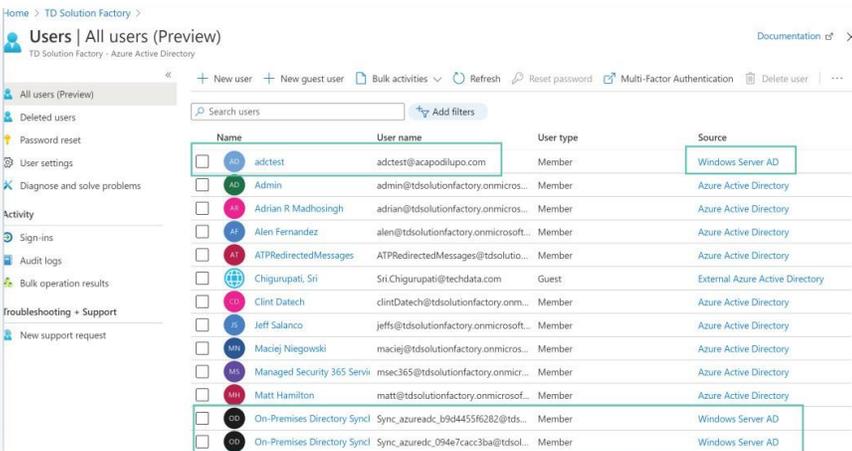
Active Directory with AD Connect Deployment and Considerations

1. **Partner (If using AD Connect or Hybrid)** must do the following. **You must have AD Connect replicating and healthy before proceeding.** Make note of domain from the Domain Controller (you will need this in the AVD Deployment Section).

- a. Verify the Identities (notably your On-Prem users) from your domain controller are synced with Azure AD. Navigate to 'All Users' in Azure

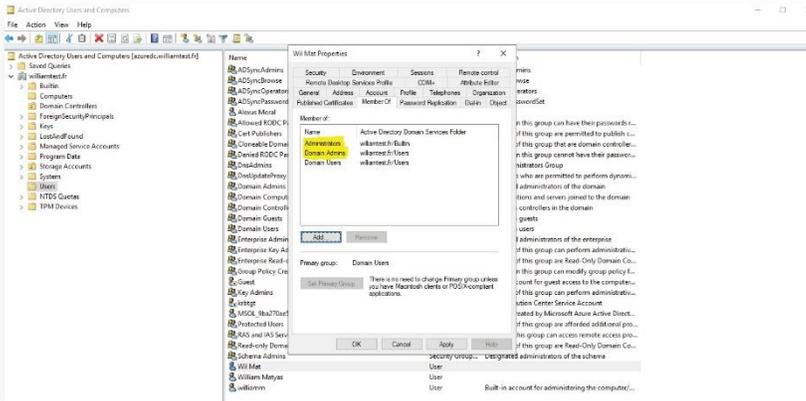


Ad to verify:



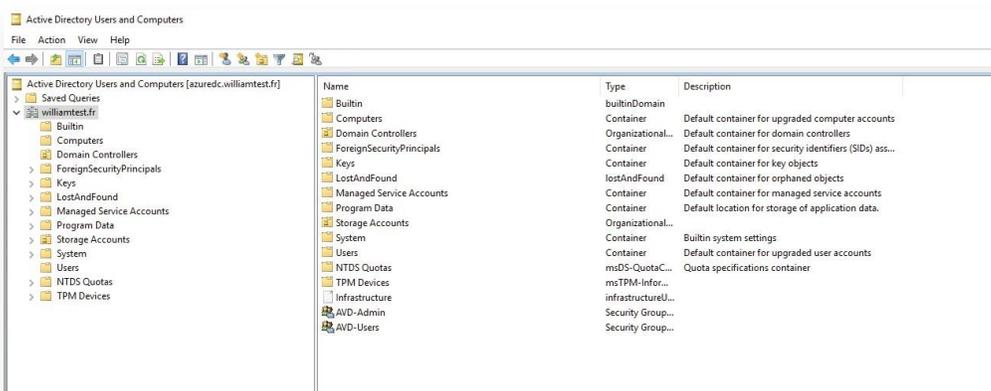
b. Make sure your Domain Admin is part of both the Administrators and Domain Admins groups.

During the deployment, we create a computer object to join the Azure File Share to the Domain. This is the main reason why we need the Domain Admin used during the deployment to be part of these two groups.



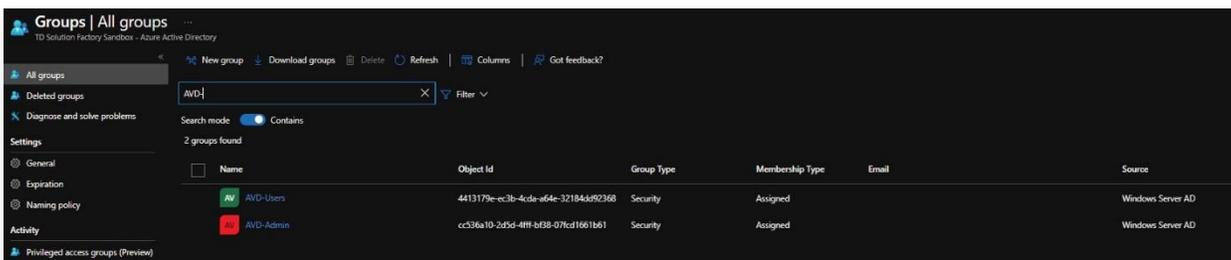
c. We also need you to create two Groups in your local Domain Controller:

- The AVD-Admin group
- The AVD-Users group

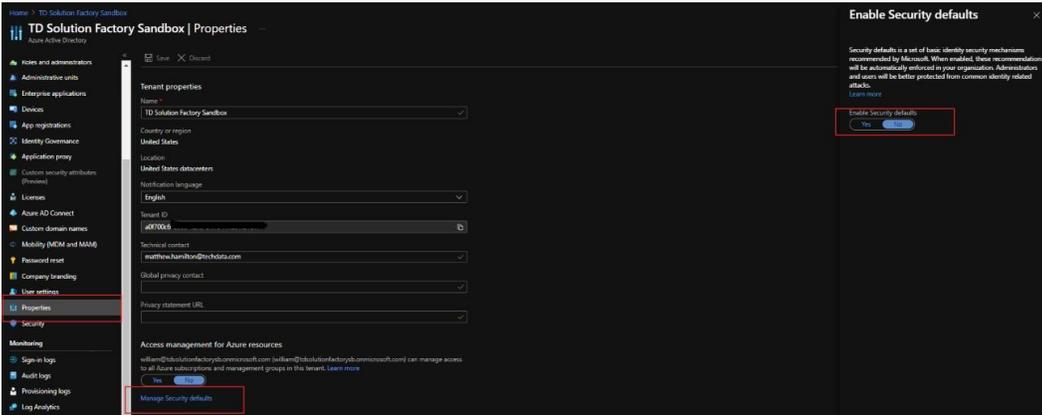


The AVD-Admin group will be used for Azure Virtual Desktop Admins. The AVD-Users group will be used for Azure Virtual Desktop Users.

Please make sure these two groups are synchronized to your Azure AD using Azure AD Connect.



- d. Deactivate security defaults (temporarily)
 - i. This can be turned back on after deployment



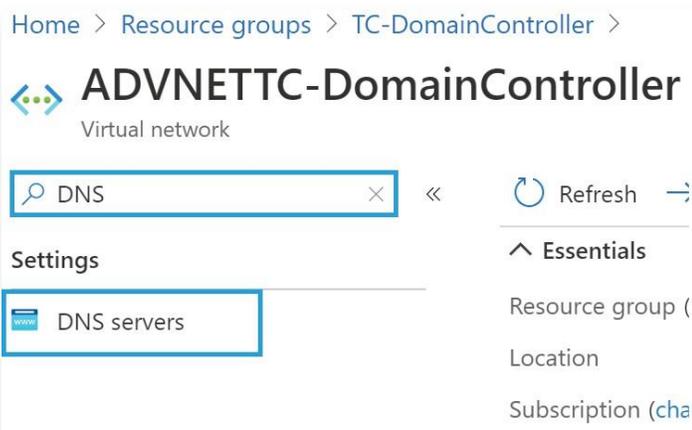
- e. **IMPORTANT NOTE: Do not proceed unless your domain is replicating and returns a healthy status in Azure.**

2. Partner (If using AD Connect) Verify DNS Configuration

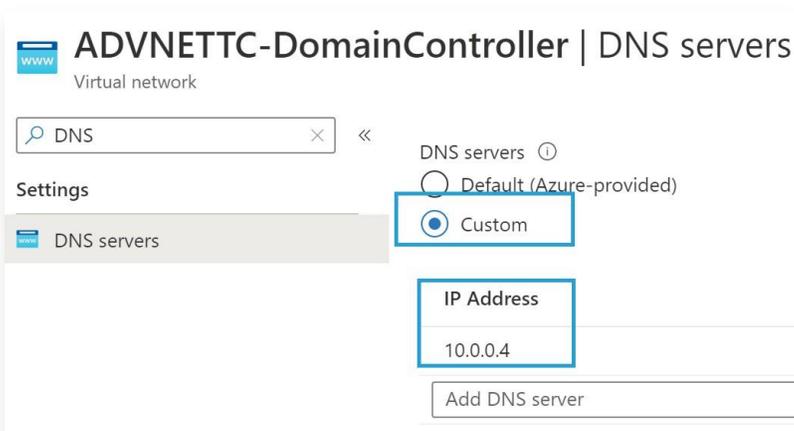
- a. Verify custom DNS is configured on your Domain Controller VNet.
 - i. Locate your AD Vnet.

Name ↑↓	Type ↑↓	Location ↑↓
<input checked="" type="checkbox"/> ADVNETTC-DomainController	Virtual network	East US
<input type="checkbox"/> ADVNETTC-DomainController-bastion	Bastion	East US
<input type="checkbox"/> ADVNETTC-DomainController-ip	Public IP address	East US
<input type="checkbox"/> azuredc	Virtual machine	East US
<input type="checkbox"/> azuredc-addtlDataDrive	Disk	East US
<input type="checkbox"/> azuredc-dcDataDrive	Disk	East US
<input type="checkbox"/> azuredc-nic	Network interface	East US

- ii. Search for and select 'DNS Servers'



iii. Ensure your DNS settings are set to 'Custom' and are pointing to the IP address of your domain controller.

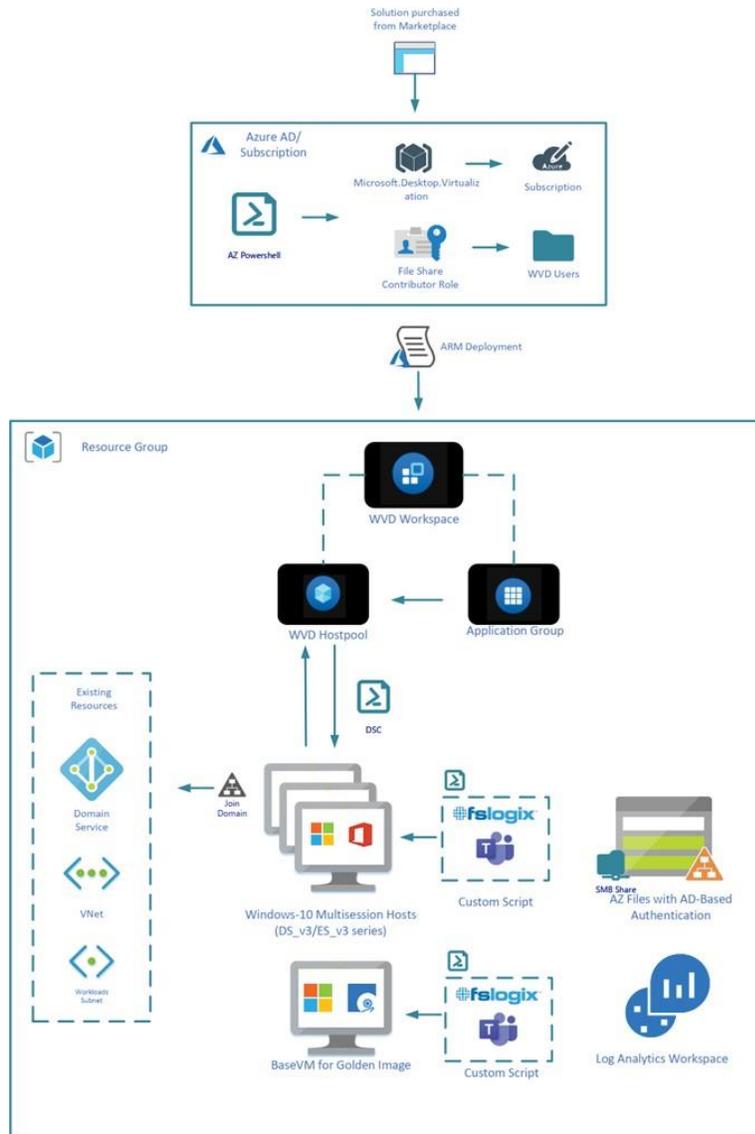


You may now proceed with the AVD Solution Deployment!

Solution Overview:

“Azure Virtual Desktop, or AVD in short – is a born in the cloud Desktop-As-a-Service platform service offering on top of the Microsoft Azure Cloud. All the infrastructure services, such as brokering, web access, load-balancing, management, and monitoring is all setup for you as part of the control plane offering.”

Deployment Architecture: General Workloads & Optional High Powered Apps Deployment



AVD Deployment and Considerations

Purchase the Azure Virtual Desktop Click-to-Run™ Solution through StreamOne and proceed to configure and deploy the solution.

Provision - Azure Virtual Desktop V1 Solution

1. Existing environment 2. 3. 4. 5.

? Help

Existing environment - Domain's virtual network integration

Select an existing Virtual Network

Select an existing subnet

Existing environment - Domain integration

Azure Virtual Desktop - Location

Data center location (based on selected virtual network) ⓘ

Resource group name (new)

Next

Let's get started with the User Interface!

Please select the existing Virtual Network where your Identity Solution is located and select the Subnet where you plan to deploy your Azure Virtual Desktop Infrastructure:

Existing environment - Domain's virtual network integration

Select an existing Virtual Network

AADDs-VNet (Location: westeurope) ▼

Select an existing subnet

Workloads (IP Subnet: 10.0.1.0/24) ▼

You will then be able to select your Domain Type between:

- a. Azure Active Directory Domain Services (AADDs)
- b. Active Directory (AD)

Existing environment - Domain integration

I am using an existing AADDs in my Azure tenant

I am using an existing Active Directory

a. Azure Active Directory Domain Services (AADDS)

To facilitate the deployment process, we have set up queries to retrieve the AADDS Domain Name and a drop-down menu with the list of the Admin Users from the AAD DC Administrators Group.

Please select the Admin username you plan to use and enter the Administrative Password tied to the user selected.

I am using an existing AADDS in my Azure tenant | I am using an existing Active Directory

Existing AADDS Domain to join ⓘ

AADDS Domain Name: aadds.tdsolutionfactorysb.onmicrosoft.com ▼

AAD DC Administrators Group for this AADDS ⓘ

AAD DC Administrators (GroupID: b266b75f-e3a3-4fbc-9e8f-591ff00a44d1) ▼

Administrative username for the existing AADDS Domain ⓘ

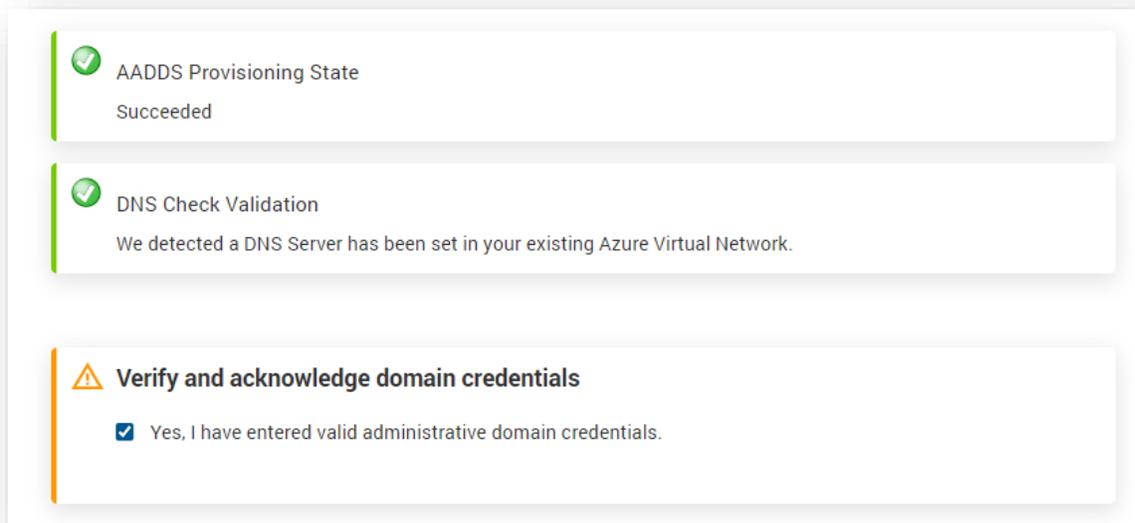
william@tdsolutionfactorysb.onmicrosoft.com (ObjectID: c2361407-b0a7-4f77-a066-e02495224e49) ▼

Administrative password for the existing domain

.....

ⓘ Note: we will not be able to validate the credentials entered during bundle configuration. Make sure all information is entered correctly and confirm below before proceeding. Invalid domain credentials will result in failed deployments.

We have also added up a logic to verify the DNS Server has been set up properly. Please verify and acknowledge domain credentials:



AADS Provisioning State
Succeeded

DNS Check Validation
We detected a DNS Server has been set in your existing Azure Virtual Network.

Verify and acknowledge domain credentials

Yes, I have entered valid administrative domain credentials.

a. Active Directory (AD) First, please enter the Existing Domain Name you plan to join:

I am using an existing AADDS in my Azure tenant I am using an existing Active Directory

Existing domain to join ⓘ

williamtest.fr

Then Select the location of the Active Directory Computer Location.

i. If it is located on-premises connected through a VPN Gateway, please enter the exact Computer name:

Active Directory Computer Location

Active Directory located in Azure

Active Directory located On-Premises, connected with a VPN Gateway

Name of the Local Domain Controller

azureDC

ii. If it is located in Azure, please select the Virtual Machine through the drop-down menu:

Active Directory Computer Location

Active Directory located in Azure

Active Directory located On-Premises, connected with a VPN Gateway

Select the Name of the Domain Controller you plan to use for the deployment.

Virtual Machine Name: vmanc

Then, please enter the Domain Admin Username in the UPN format and acknowledge that the admin User you provided in both the Domain Admin and Administrators group. (Reminder: During the deployment, we create a computer object to join the Azure File Share to the Domain. This is the main reason why we need the Domain Admin used during the deployment to be part of these two groups.)

Administrative username in the UPN format for the existing domain ⓘ

ⓘ Note: During the deployment we create a computer object for the Azure File Share in the Domain. To perform this action, the Domain Admin provided needs to be in both the "Domain Admin" group and the "Administrators" group

⚠ **Verify and acknowledge that the Domain Admin User provided is in both Domain Admin and Administrators groups**

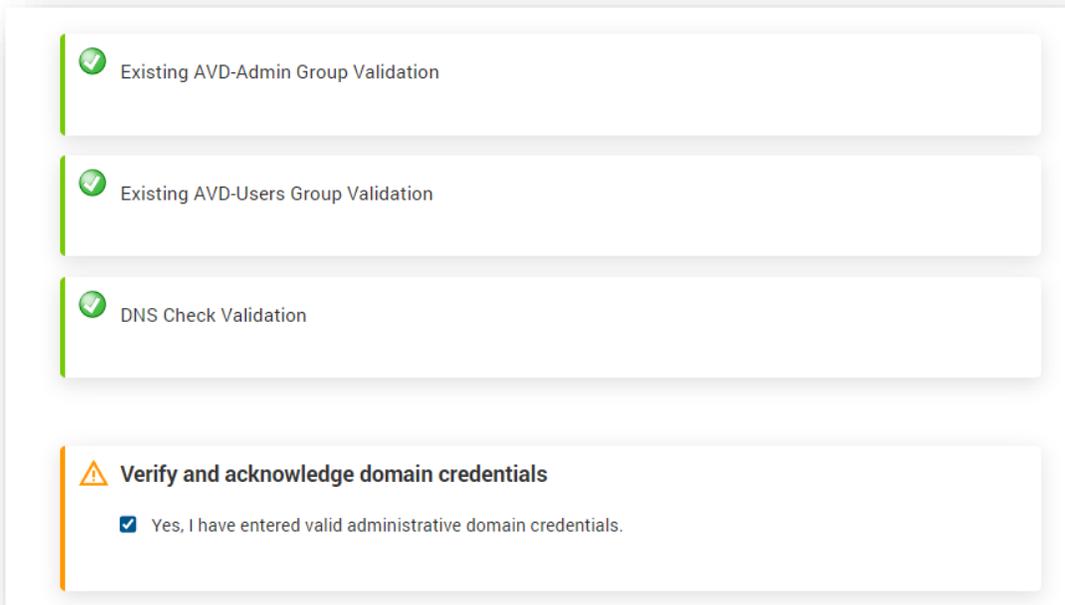
Yes, I have verified that this Admin User is a member of both Domain Admins and Administrators groups

Then enter the administrative password for the selected user:

Administrative password for the existing domain

ⓘ Note: we will not be able to validate the credentials entered during bundle configuration. Make sure all information is entered correctly and confirm below before proceeding. Invalid domain credentials will result in failed deployments.

We have added up a logic to verify that the AVD-Admin and AVD-Users groups have been created and synced beforehand. We are also verifying that the DNS Server has been set up properly. Please verify and acknowledge domain credentials:



Existing AVD-Admin Group Validation

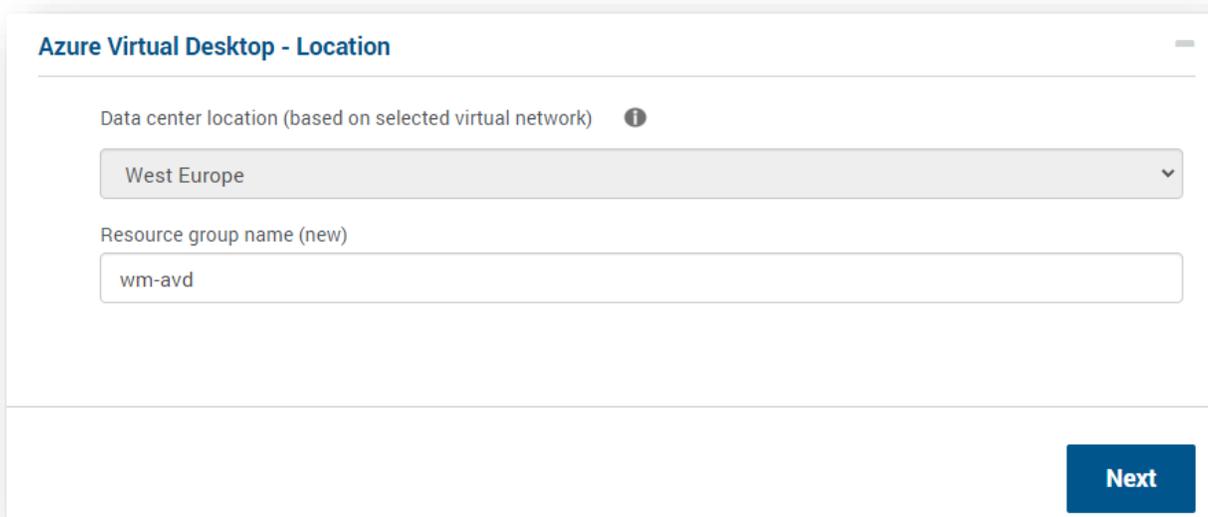
Existing AVD-Users Group Validation

DNS Check Validation

Verify and acknowledge domain credentials

Yes, I have entered valid administrative domain credentials.

Moving on to the Azure Virtual Desktop configuration, please enter a Resource Group Name: (Data Center Location is based upon the location of the AADDS / AD you've previously deployed).



Azure Virtual Desktop - Location

Data center location (based on selected virtual network) ⓘ

West Europe

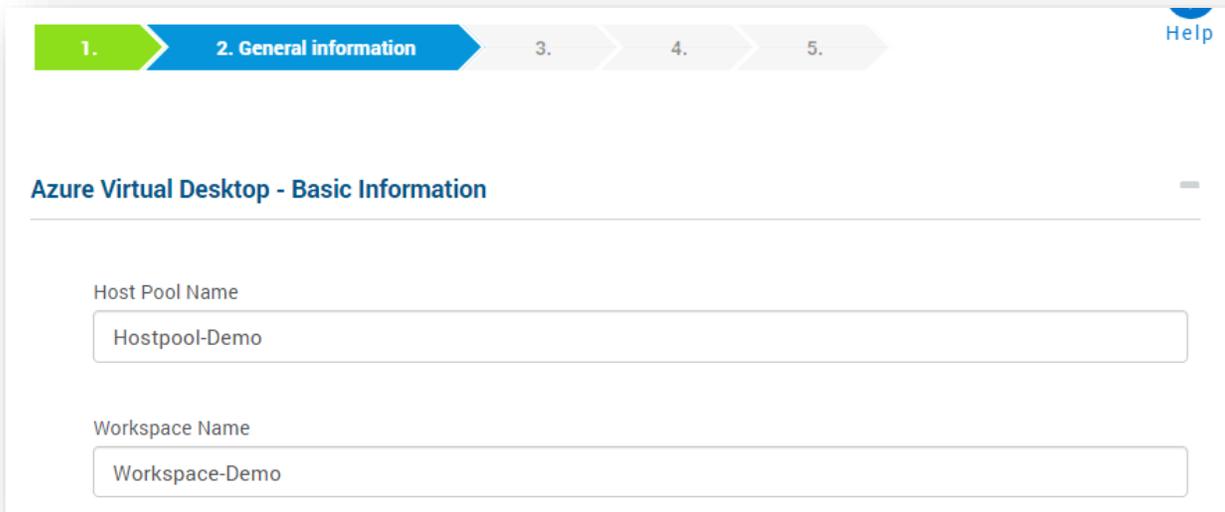
Resource group name (new)

wm-avd

Next

Click on Next

Then enter a Host Pool Name and a Workspace Name for the Azure Virtual Desktop:



1. 2. General information 3. 4. 5. Help

Azure Virtual Desktop - Basic Information

Host Pool Name
Hostpool-Demo

Workspace Name
Workspace-Demo

Please select the AVD Objects Location. This is where you will deploy your AVD Services (Host Pool, Workspace, Application Groups...). This does not define the location of your Session Hosts.



AVD Objects Location
West Europe

By default, we create a Default Application Group (DAG). You can also create an additional Application Group that would be dedicated for RemoteApp.



Create an Application Group for RemoteApp ⓘ

Moving on to Session Hosts Configuration. Please define a Session Hosts prefix. It will be limited to 8 characters as we append -host1, -host2... to the Virtual Machines and the Computer Name is limited to 15 characters.

Azure Virtual Desktop - Hosts Configuration

Virtual Desktop Session Host prefix ?

Then enter the local admin credentials you plan to use for the Session Hosts:

Administrator Username

Administrator Password

Confirm Password

Select the Session Host Image Sku you plan to use and the number of Session Hosts you plan to deploy:

Virtual Desktop Session Host Image SKU (Select 1 option.)

Windows 10 Enterprise Multi-Session Select ▼	Windows 11 Enterprise Multi-Session with Office 365 Professional Plus Selected	Windows Server 2019 Datacenter Edition Select ▼	Windows Server 2022 Datacenter Edition Select ▼
Windows 10 Enterprise Multi-Session with Office 365 Professional Plus Select ▼	Windows 11 Enterprise Multi-Session Select ▼		

Number of Session Hosts to deploy ⓘ

− 2 AVD Session Host(s) +

You will then be able to select your VM Profile Type and the VM Size.

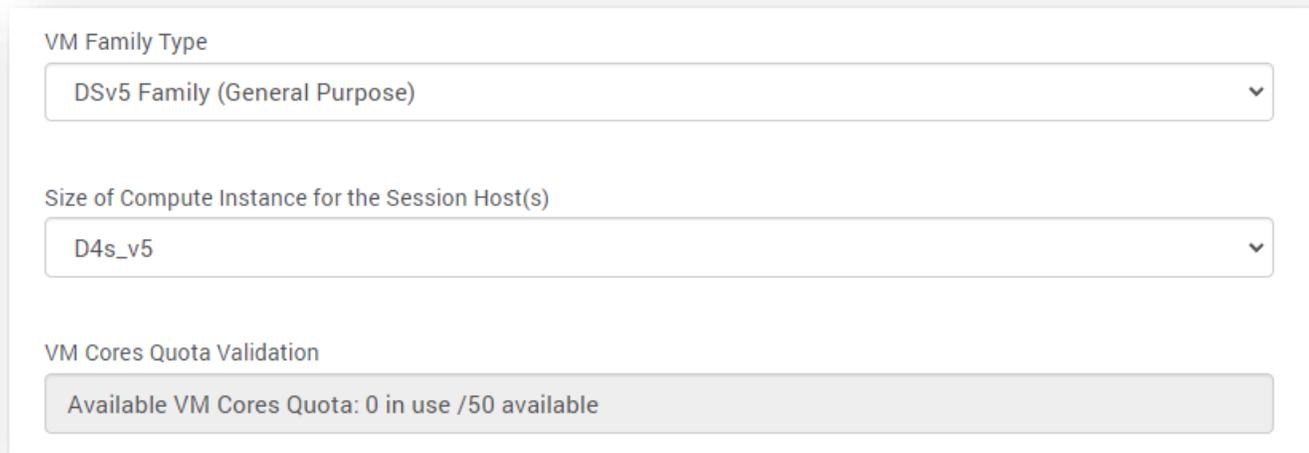
VM Family Type

DSv5 Family (General Purpose) ▼

Size of Compute Instance for the Session Host(s)

D4s_v5 ▼

We have added up a logic to validate VM Cores Quota validation. The number in the VM Size represents the number of cores each VM uses.



The screenshot shows a configuration panel with three sections:

- VM Family Type:** A dropdown menu with the selected option "DSv5 Family (General Purpose)".
- Size of Compute Instance for the Session Host(s):** A dropdown menu with the selected option "D4s_v5".
- VM Cores Quota Validation:** A grey bar displaying the text "Available VM Cores Quota: 0 in use /50 available".

Warning! Please bear in mind to multiply the number of cores a VM Size would use by the number of Session you plan to deploy!

Then please select the OS Disk size you plan to use:

Size of the OS Disk

256 GB

If available for the VM Size, you can enable Accelerated Networking:

Enable Accelerated Networking 

Please select if you plan to deploy a Base VM for Golden Image creation:

Deploy VM for Golden Image 

And finally, please enter a name for your Diagnostics Storage Account:

Diagnostics Storage Account Name

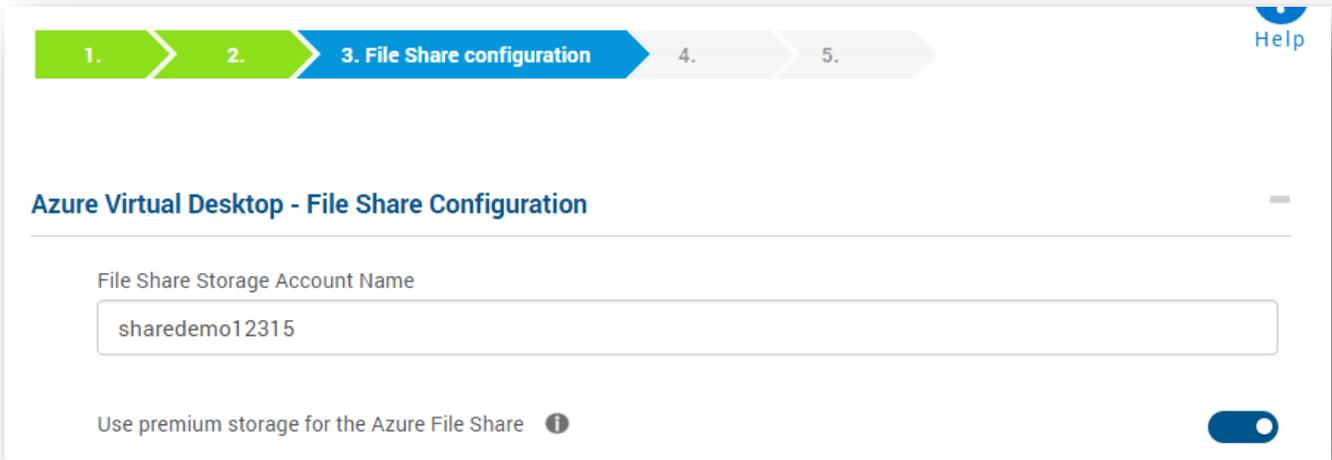
diagdemo13215

[Prev](#) [Next](#)

Then click on Next.

Now that we are done with the Session Hosts configuration, let's move on to the Azure File Share configuration.

The Azure File Share will be used to store User Profiles. Please enter a name for your File Share Storage Account and select if you want to use Premium Storage or not:



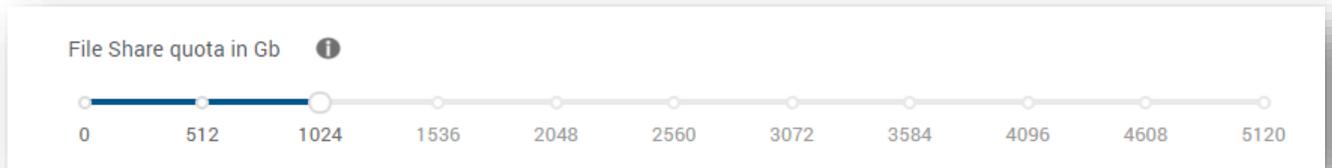
1. 2. **3. File Share configuration** 4. 5. Help

Azure Virtual Desktop - File Share Configuration

File Share Storage Account Name

Use premium storage for the Azure File Share ⓘ

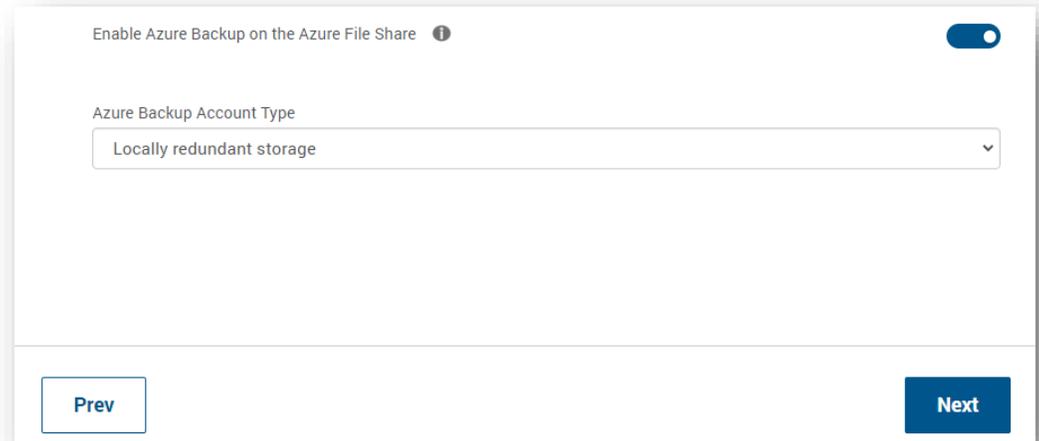
Then define the File Share Quota (Standard storage is Pay as you Go, but Premium Storage is provisioned):



File Share quota in Gb ⓘ

0 512 1024 1536 2048 2560 3072 3584 4096 4608 5120

And select if you want to use Azure Backup for your Azure File Share and the redundancy of your Azure Backup Account Type. Then click on next!

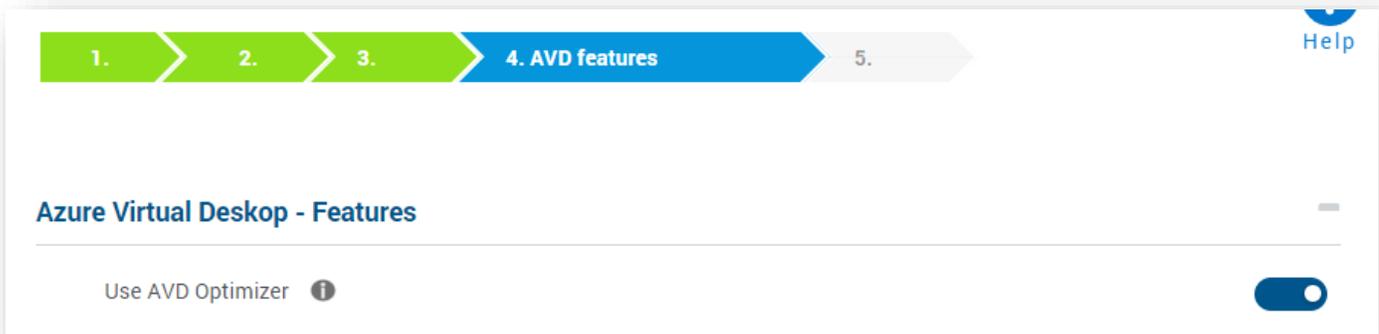


Enable Azure Backup on the Azure File Share ⓘ

Azure Backup Account Type

Prev Next

Moving on to extra Azure Virtual Desktop features, you can select if you want to use the AVD Optimizer:



1. 2. 3. 4. AVD features 5. Help

Azure Virtual Desktop - Features

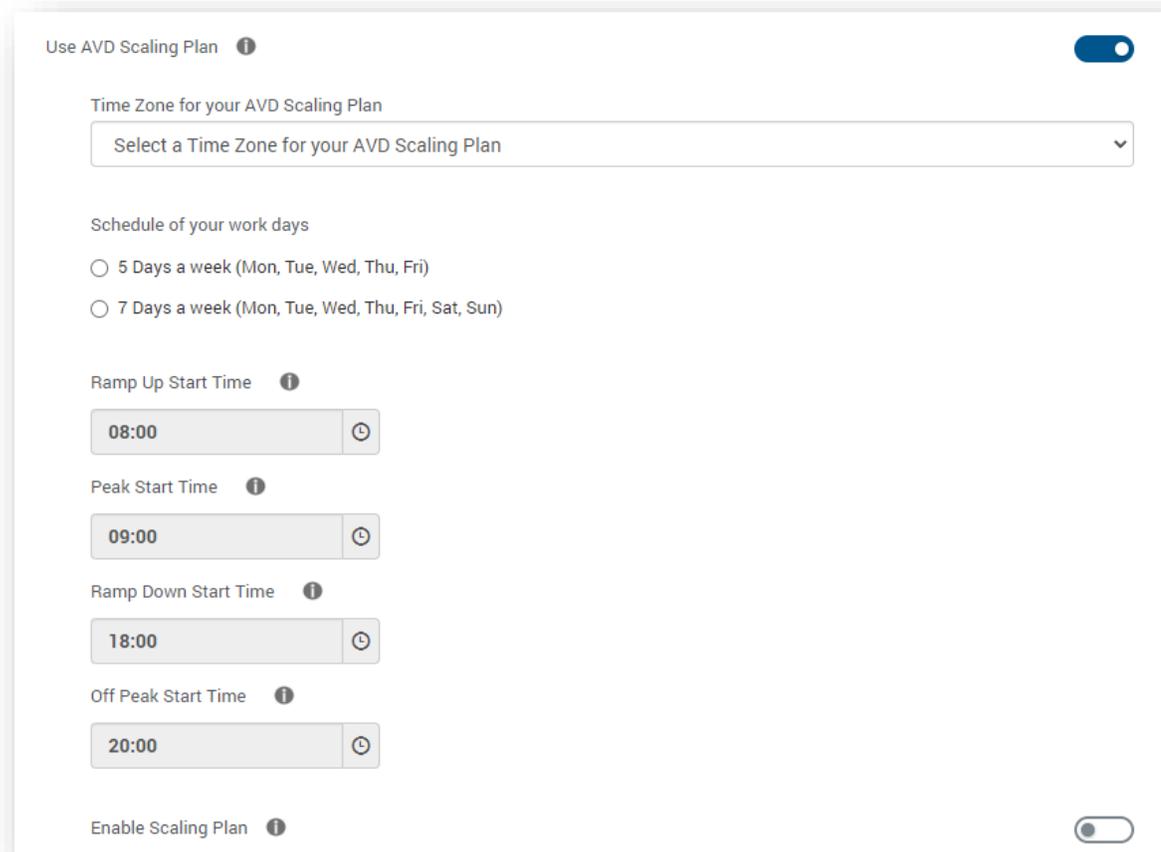
Use AVD Optimizer ?

If you plan to enable the “Start Virtual Machine On Connect” feature:



Enable Start Virtual Machine on Connect ?

And if your AVD Location supports it, you can use the AVD Scaling Plan feature:



Use AVD Scaling Plan ?

Time Zone for your AVD Scaling Plan
Select a Time Zone for your AVD Scaling Plan ▼

Schedule of your work days

5 Days a week (Mon, Tue, Wed, Thu, Fri)

7 Days a week (Mon, Tue, Wed, Thu, Fri, Sat, Sun)

Ramp Up Start Time ?
08:00 ⌚

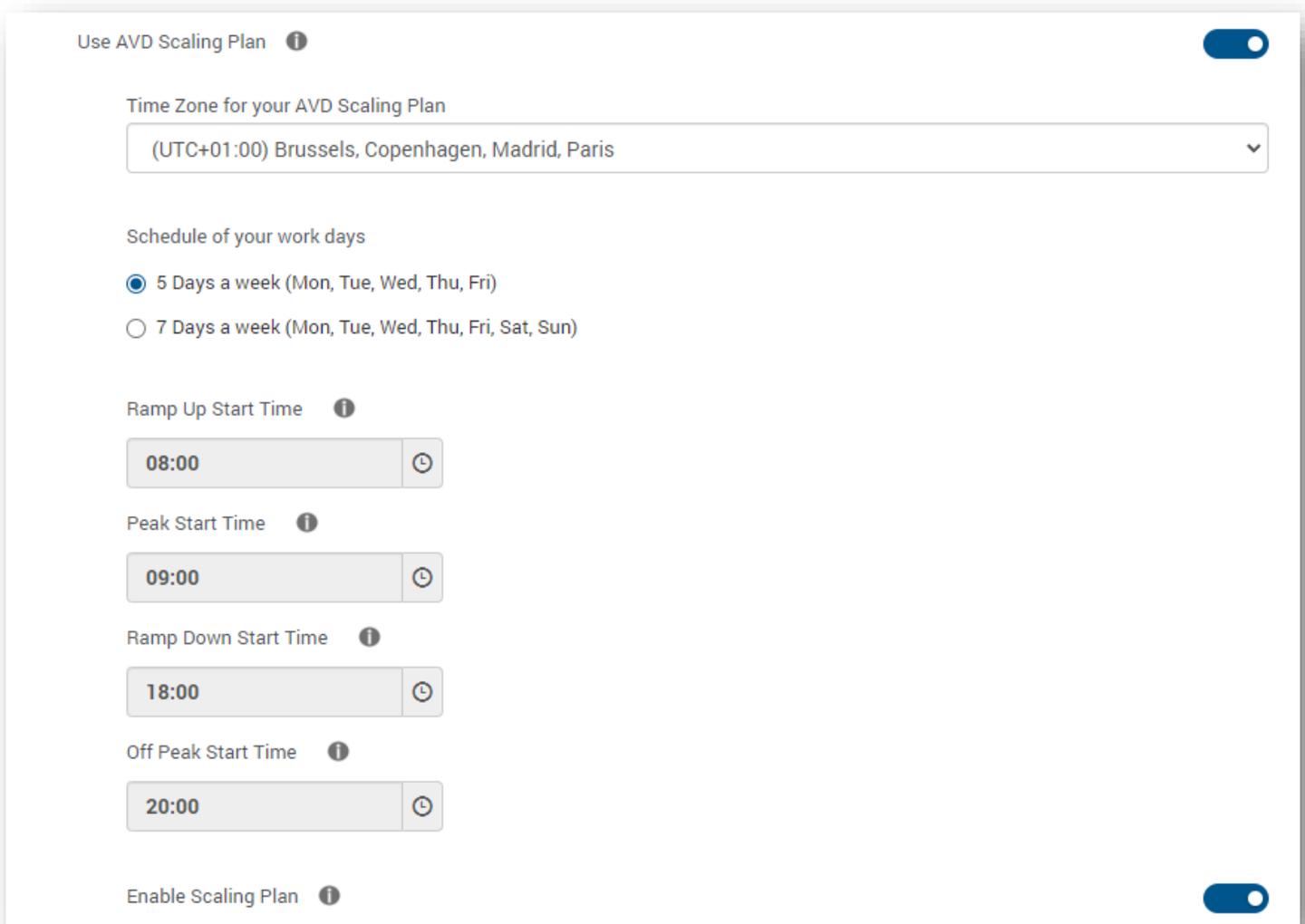
Peak Start Time ?
09:00 ⌚

Ramp Down Start Time ?
18:00 ⌚

Off Peak Start Time ?
20:00 ⌚

Enable Scaling Plan ?

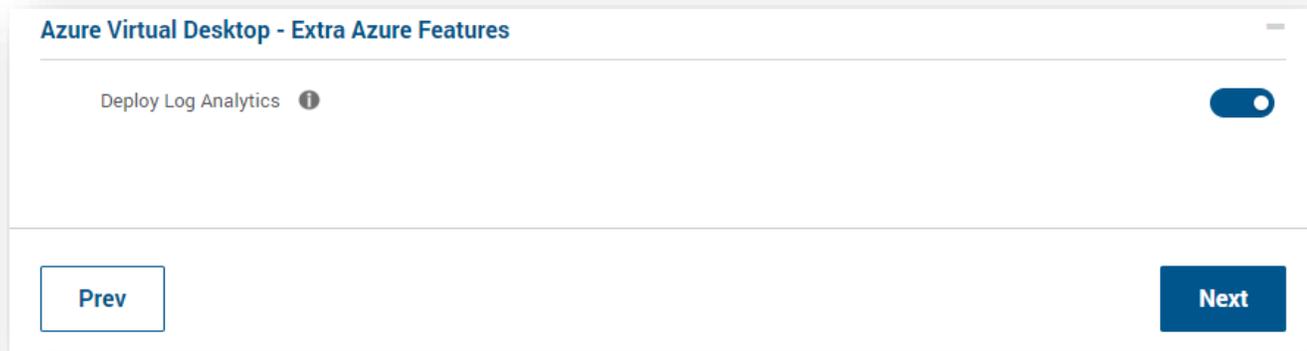
To configure it, please select the adequate Time Zone, your Workdays Schedule, the different Start Times and if you plan to directly Enable the newly created Scaling Plan:



The screenshot shows a configuration window for an AVD Scaling Plan. At the top left, there is a toggle switch labeled "Use AVD Scaling Plan" which is turned on. Below this is a dropdown menu for "Time Zone for your AVD Scaling Plan" with the selected value "(UTC+01:00) Brussels, Copenhagen, Madrid, Paris". Underneath is a section for "Schedule of your work days" with two radio button options: "5 Days a week (Mon, Tue, Wed, Thu, Fri)" which is selected, and "7 Days a week (Mon, Tue, Wed, Thu, Fri, Sat, Sun)". Below the schedule are four time selection fields, each with a clock icon: "Ramp Up Start Time" set to 08:00, "Peak Start Time" set to 09:00, "Ramp Down Start Time" set to 18:00, and "Off Peak Start Time" set to 20:00. At the bottom left, there is another toggle switch labeled "Enable Scaling Plan" which is also turned on.

By default, the Ramp Up Load Balancing Algorithm is Breadth First and the Ramp Down Load Balancing Algorithm is Depth First. The Peak Load Balancing Algorithm is Depth First and the Off Peak Load Balancing Algorithm is Depth First. The Ramp Up Minimum Hosts Percentage is 20% and the Ramp Up Capacity Threshold is 60% while the Ramp Down Minimum Hosts Percentage is 10% and the Ramp Down Capacity Threshold is 90%. The Ramp Down force logs off Users 30 minutes after they receive the notification message "You will be logged off in 30 min. Make sure to save your work."

Finally, please select if you plan to deploy Log Analytics:

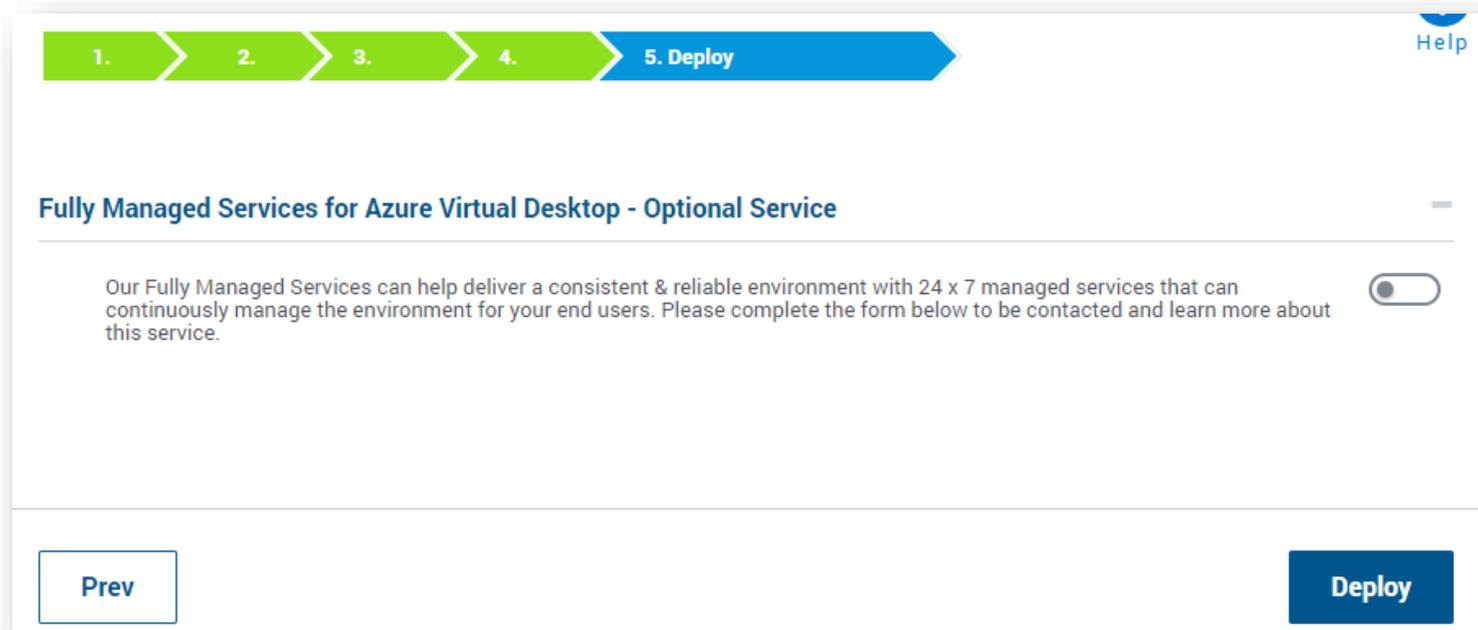


Azure Virtual Desktop - Extra Azure Features

Deploy Log Analytics ?

[Prev](#) [Next](#)

Then click on next.



1. 2. 3. 4. 5. Deploy [Help](#)

Fully Managed Services for Azure Virtual Desktop - Optional Service

Our Fully Managed Services can help deliver a consistent & reliable environment with 24 x 7 managed services that can continuously manage the environment for your end users. Please complete the form below to be contacted and learn more about this service.

[Prev](#) [Deploy](#)

You can then click on Deploy Now!

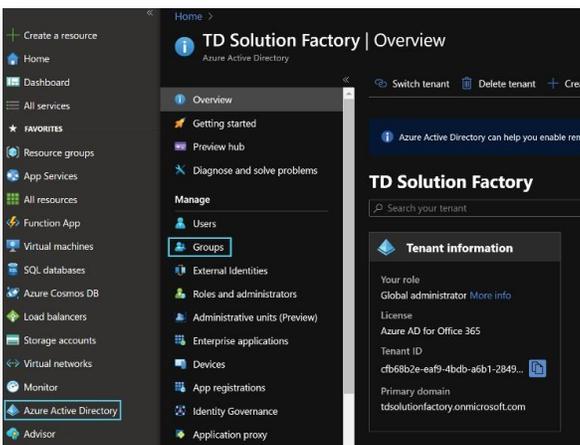
Post-Deployment Checklist for Azure AD Domain Services (partner must complete)

- Assign users to AVD Users / AVD Admin group.

Adding users to 'AVD Users' AAD Group

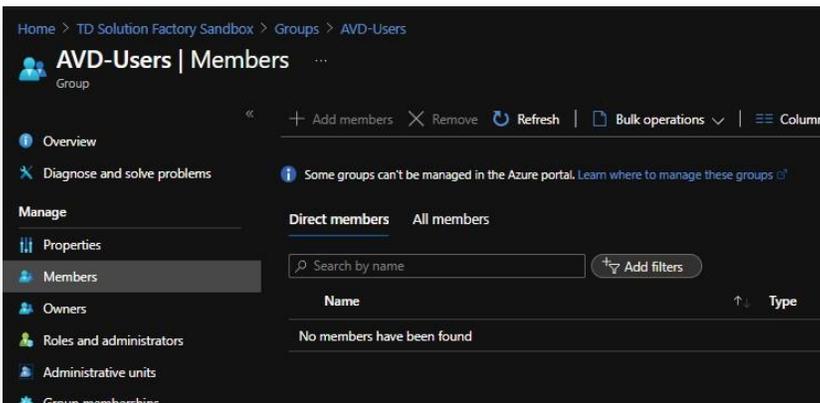
For AADDS Scenarios, we automate the creation of a custom security group called 'AVD-Users.' Any users or groups who you would like to grant access to your environment should be added to 'AVD-Users.'

1. Go to your Azure AD and select 'Groups' you should see the 'AVD-Users' group in the listing. Select the group.



<input type="checkbox"/>	Name	Object Id
<input checked="" type="checkbox"/>	AVD-Users	4413179e-ec3b-4cda-a64e-32184dd92368
<input checked="" type="checkbox"/>	AVD-Admin	cc536a10-2d5d-4fff-bf38-07fcd1661b61

2. Select 'Members,' then 'Add Members.' Add any Azure AD users or custom groups that you wish to provide access to your AVD environment.

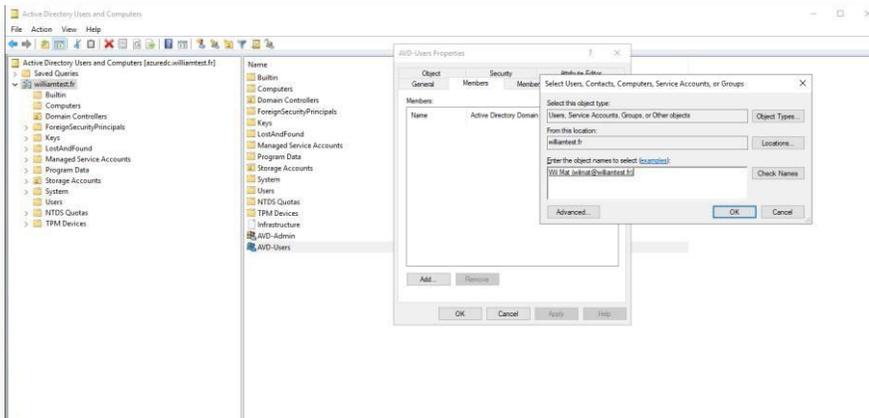


Post-Deployment Checklist for Domain Controller Deployments (partner must complete)

- Add users to the Local AD Group.

AVD (Domain Controller with AD Connect): Post Deployment Steps

Go to your local AD and add up users to the 'AVD-Users' group.



AVD Error Deployment Log

Azure Error:

"VM has reported a failure when processing extension 'joindomain'. Error message:
\\\\"Exception(s) occurred while joining Domain <Domain Name>\\\\"\\r\\n\\r\\nMore information on troubleshooting is available at <https://aka.ms/vmextensionwindowstroubleshoot> \\"

Description: Domain Join Failure Potential

Causes (if Using AADDS):

- AADDS is not returning a healthy 'running' state.
- The domain admin account password has not been reset after deploying AADDS (password hash sync step).
- An invalid domain name was supplied. This needs to be the AADDS Resource name.
- Invalid administrator credentials were supplied.
- The domain admin user supplied is not a member of the AAD DC Administrators security group.
- The VM name supplied at deployment already exists in AADDS, causing a duplicate naming conflict.
- Multifactor authentication is enabled on the domain administrator account in Azure AD.
- AADDS is not configured to be your primary DNS source.

Potential Causes (if Using Domain Controller with ADConnect):

- An invalid domain name was supplied. This must be the forest name of your current Active Directory.
- Invalid administrator credentials were supplied. This must be a domain admin on your domain controller.
- Username supplied at deployment is not a Domain Administrator on your AD server.
- The domain admin name supplied has not been synced up to Azure AD with ADConnect.
- The VM name supplied at deployment already exists in AD, causing a duplicate naming conflict.
- Multifactor authentication is enabled on the domain admin account supplied.
- Your domain controller is not configured to be your primary DNS source.
- Your Domain Controller Vnet does not have DNS configured.

Azure Error:

"code": "NetworkAclsValidationFailure", "message": "Validation of network acls failure: SubnetsHaveNoServiceEndpointsConfigured:Subnets workloads of virtual network <Vnet Resource ID here> do not have ServiceEndpoints for Microsoft.Storage resources configured. Add Microsoft.Storage to subnet's ServiceEndpoints collection before trying to ACL Microsoft.Storage resources to these subnets.."

Description: Service Endpoint Not configured

Cause: The Microsoft.Storage service endpoint has not been configured on your Domain VNet.

Steps to resolve:

- Resolve this by going to your AADDS or DC Vnet
- Select the subnet you are deploying to (i.e., your 'Workloads' subnet)
- Select the dropdown under 'Services'
- Ensure the 'Microsoft.Storage' service endpoint has been added
- Consult the AVD Click-to-Run step-by-step guide for more information

Azure Error:

"VM has reported a failure when processing extension 'installcustomscript'. Error message: '\\\\'Command execution finished, but failed because it returned a non-zero exit code of: '1

Description: Custom Script Extension Failure

Cause: The custom script extension failed to execute. This could be due to your tenant configuration, User account, or conditional access policy. **More information about this issue may be viewed on the deployed session host under C:\DeploymentLogs.**

Steps to resolve:

- Ensure your domain admin user does not have MFA enabled.
- Ensure Security Defaults is Disabled on your tenant.
- Verify that you do not have an azure policy that could conflict with running custom scripts.
- Check your conditional access policies for anything that may be preventing 3rd party scripts from running within your tenant.
- If these policies exist and cannot be modified, ensure that an appropriate exception has been created for the domain admin user supplied for the AVD deployment.
- For scenarios where a new admin user was created for the AVD deployment, ensure you do not have an enforced MFA/multi device setup for new users upon first login.
- Ensure there are not any Azure Firewall configurations in place that may interfere with custom scripts from being run in your subscription and selected VNet.

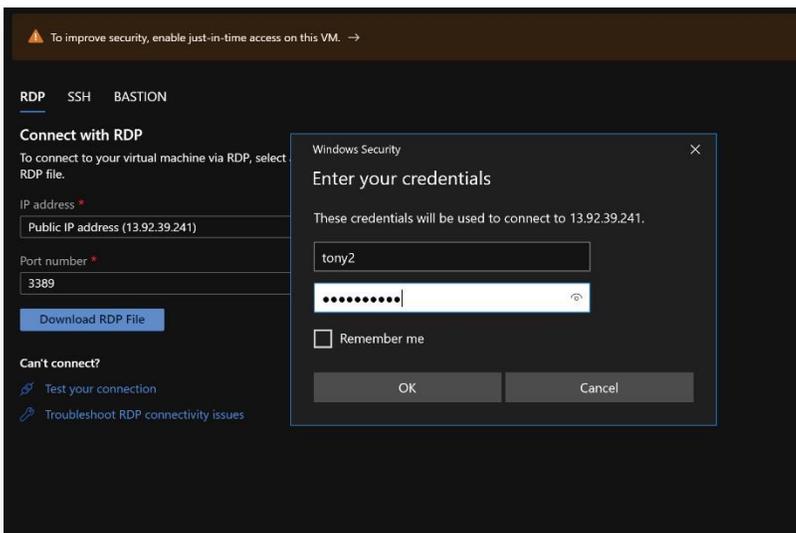
AVD V1 Click-to-Run: Creating Your custom Image

The AVD Click-to-Run solution provides the option to deploy a partially configured Windows 10 Multisession VM from which you may create a custom image for your AVD deployment. Follow the steps below to create a golden image from the deployed VM and update your Host Pool. Please note the custom image that is being created will be unique to this AVD deployment.

1. If you have enabled the deployment of 'a base VM for Golden Image' from the UI, the solution will provision a VM called 'imageVM' that will be used to build your golden image.

Name ↑↓	Type ↑↓	Location ↑↓
autodeskHP	Host pool	East US
autodeskHP-DAG	Application group	East US
autodeskWS	Workspace	East US
firstVM-0	Virtual machine	East US
firstVM-0-nic	Network interface	East US
firstVM-0_OsDisk_1_5d8cd50b1be849e885afe737783633cb	Disk	East US
firstVM-availabilitySet-eastus	Availability set	East US
imageVM	Virtual machine	East US
imageVM-nic	Network interface	East US
imageVM-PIP	Public IP address	East US
imageVM_OsDisk_1_d460a7327def4dadac6b2cfddeb17da1	Disk	East US
p3op2kxbpukcousers	Storage account	East US
WVDMonitor-p3op2kxbpukco	Log Analytics workspace	East US

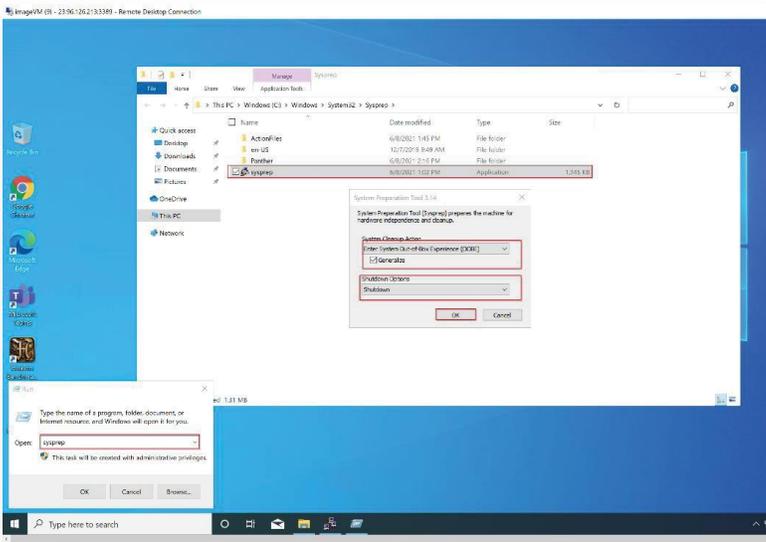
2. Sign in to imageVM with local admin credentials. For your convenience, the Image VM has been configured to allow connections via RDP.



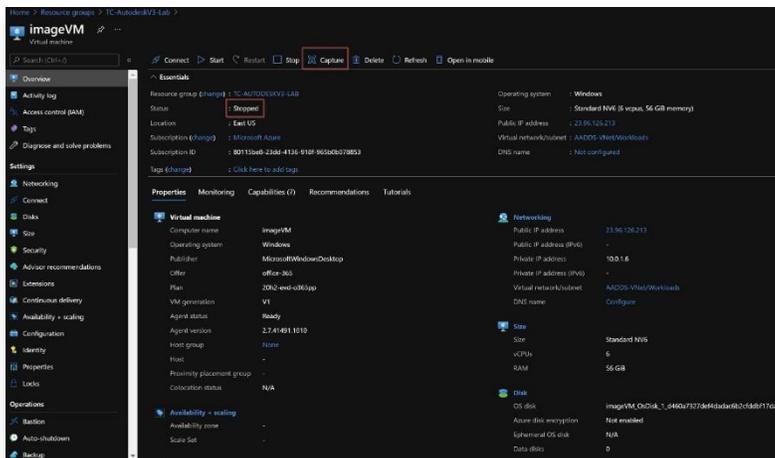
3. Configure the virtual machine with any LOB applications, Group Policy Settings, or other configurations.

Note: the FSLogix Agent has been configured for you already, and the VHD locations have been mapped to the Click-to-Run storage account. If you enabled the teams install during deployment, this will be configured on imageVM as well.

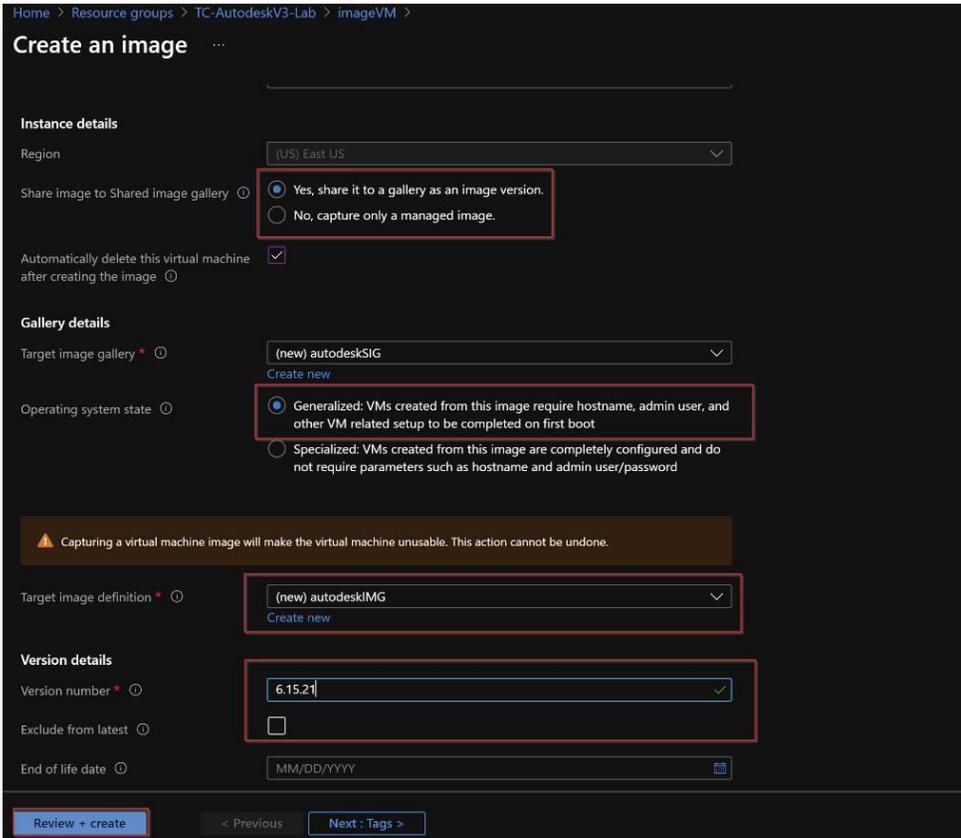
4. When finished Making your configurations, you must run sysprep on imageVM. This can be done by selecting **start->Run->Sysprep**. Open the Sysprep application and select **‘Enter System Out-of-Box-Experience (OOBE)’** and select ‘Generalize’. Under shutdown options select ‘Shutdown’. After clicking ‘Ok’ the sysprep process will begin. **Important: This will generalize the imageVM and you will not be able to access it again after the sysprep process begins!**



5. Once the sysprep process has completed, the image VM will be in the ‘Stopped’ state in Azure. To create the custom image select ‘Capture’.



6. Follow the prompts to create the image. We recommend creating a Shared Image Galley during this step to simplify Image management and updates. Make sure the OS state selected is set to 'Generalized.' When you have finished specifying your inputs, select 'Review and Create' to begin the image creation process. This will also create the Shared Image Gallery and definitions.

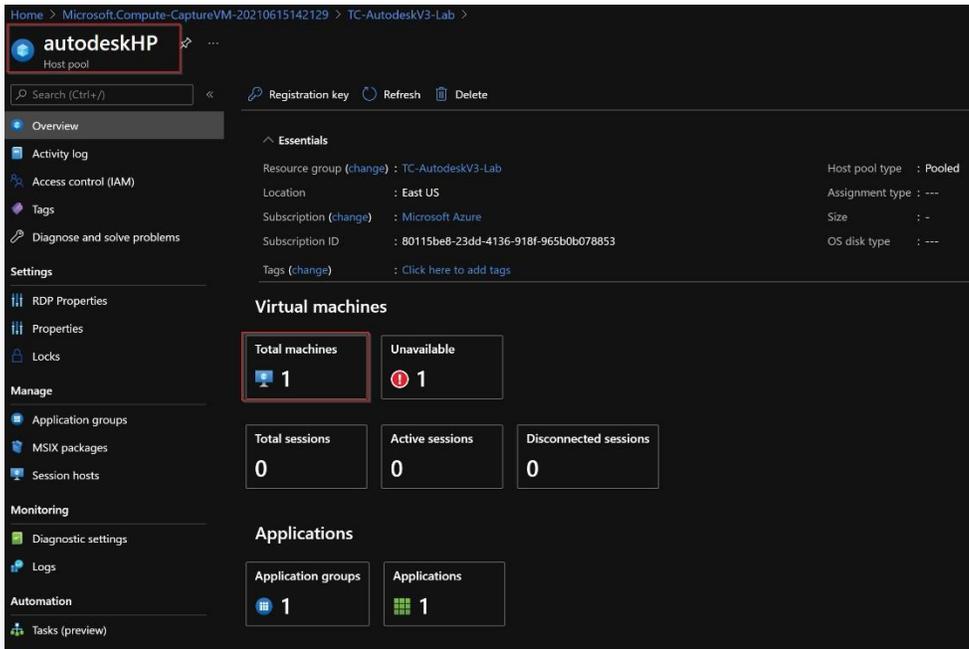


7. You will then see the Shared Image Gallery and associated Image versions appear in your AVD resource group! This managed image may be used to update your existing AVD Host Pool.

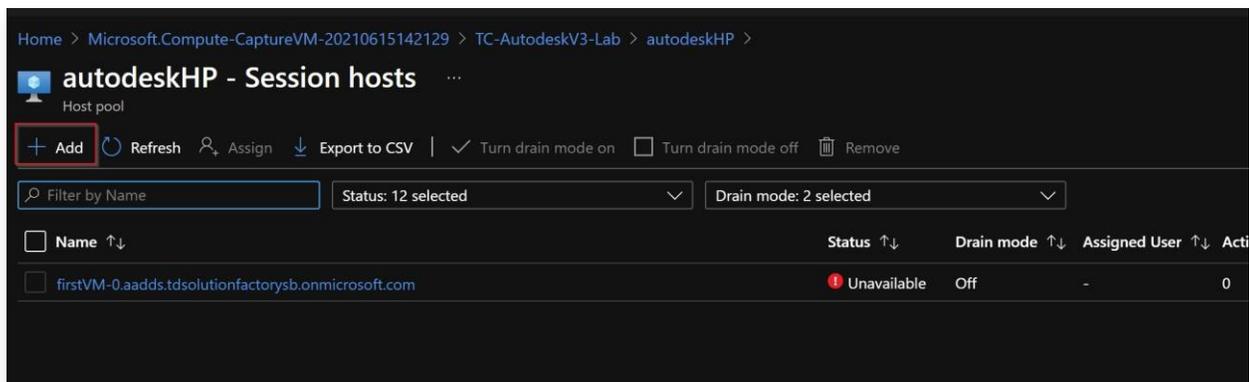
<input type="checkbox"/>	autodeskIMG (autodeskSIG/autodeskIMG)	Image definition
<input type="checkbox"/>	autodeskSIG	Shared image gallery
<input type="checkbox"/>	autodeskWS	Workspace

AVD V1 Click-to-Run: Updating your Host Pool with Custom Image

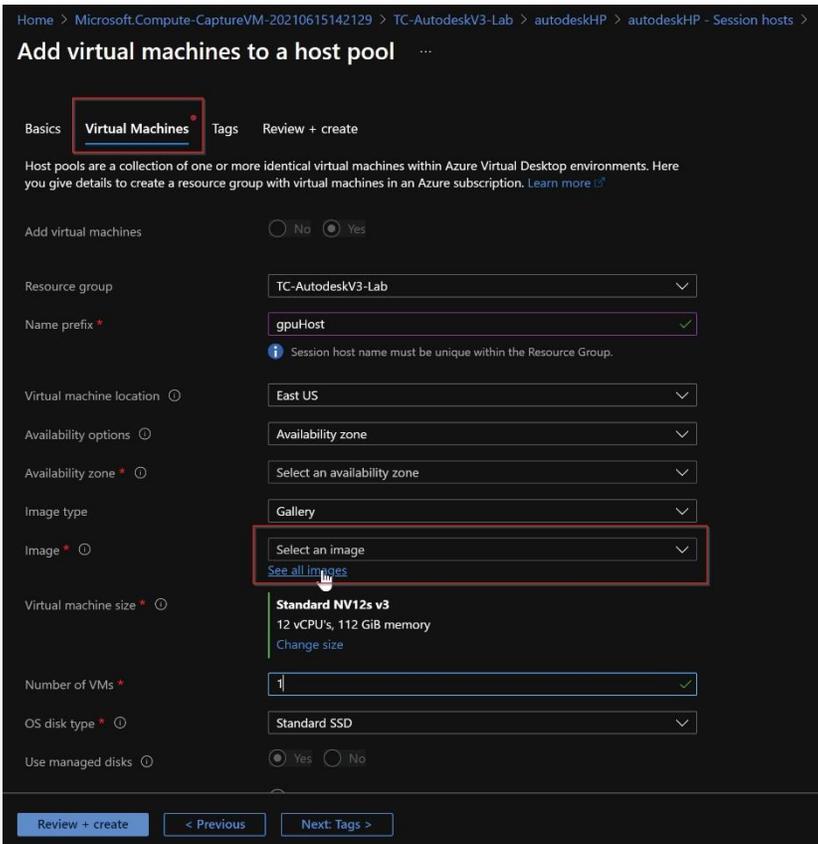
1. To update your AVD Host Pool with your newly created custom image, navigate to your Host Pool resource and select 'Total Machines'.



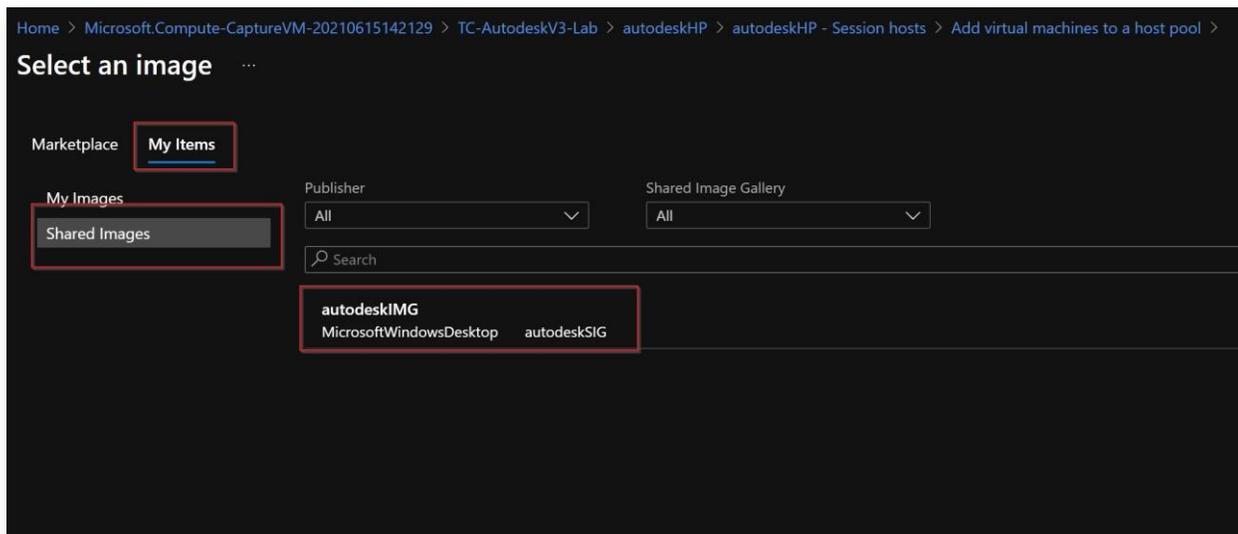
Select 'Add' from your Host Pool settings:



2. Specify your session host name, AD domain credentials, Region ETC. To use your newly created Image, select 'See All Images' from the 'Image' parameter.



3. Select your custom image under 'My Items', you may now proceed with the session host deployment!



4. Select 'Create' to add your session host to the AVD Host Pool.

Home > Microsoft.Compute-CaptureVM-20210615142129 > TC-AutodeskV3-Lab > autodeskHP > autodeskHP - Session hosts >

Add virtual machines to a host pool ...

Validation passed.

Basics Virtual Machines Tags **Review + create**

Basics

Subscription	Microsoft Azure
Resource group	TC-AutodeskV3-Lab
Host pool name	autodeskHP
Location	East US
Host pool type	Pooled
Max session limit	20
Load balancing algorithm	Breadth-first

Virtual Machines

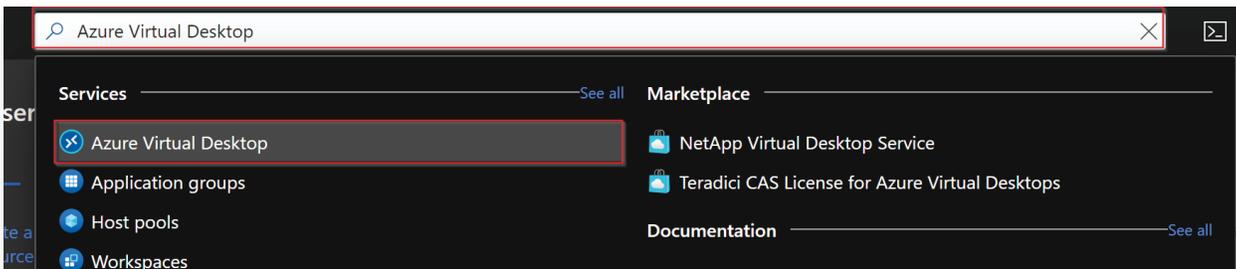
Resource group	TC-AutodeskV3-Lab
Name prefix	gpuHost
Virtual machine location	East US
Availability options	No infrastructure redundancy required
Image type	Gallery
Image	autodeskIMG
Virtual machine size	Standard NV12s v3
Number of VMs	1
OS disk type	Premium SSD
Use managed disks	Yes
Virtual network	AADDs-VNet
Boot Diagnostics	Disable
Subnet	DomainServices(10.0.0/24)

Create < Previous Download a template for automation

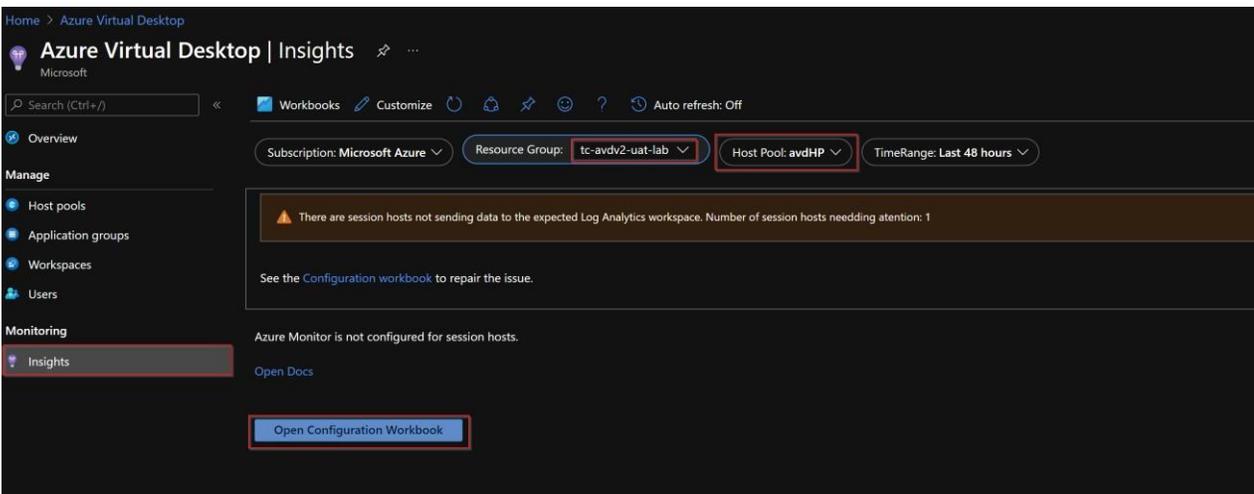
AVD Click-to-Run: Enabling Insights for your AVD Deployment

The AVD Click-to-Run solution gives you the option to provision a log analytics workspace to work with the Insights feature in the AVD management portal. The workspace has been pre-configured with the necessary performance counters and diagnostic settings. To complete the configuration, follow the steps below:

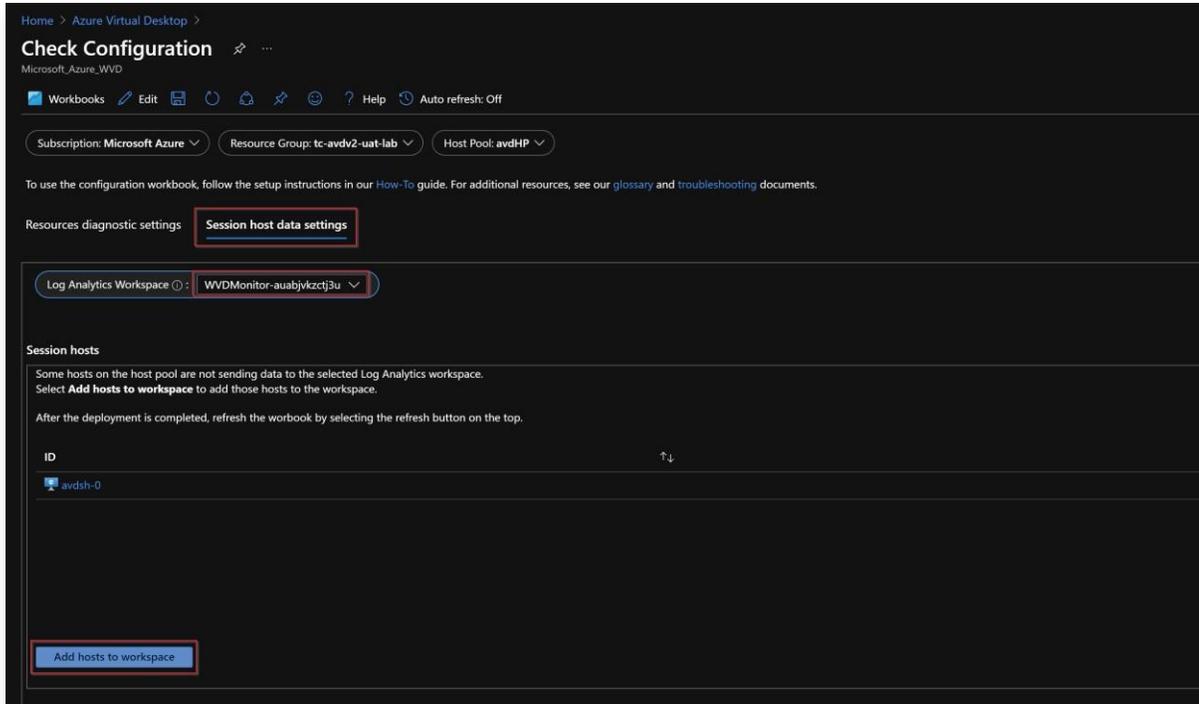
1. Navigate to the AVD management portal within Azure. This can be found by searching for 'Azure Virtual Desktop' in the portal.



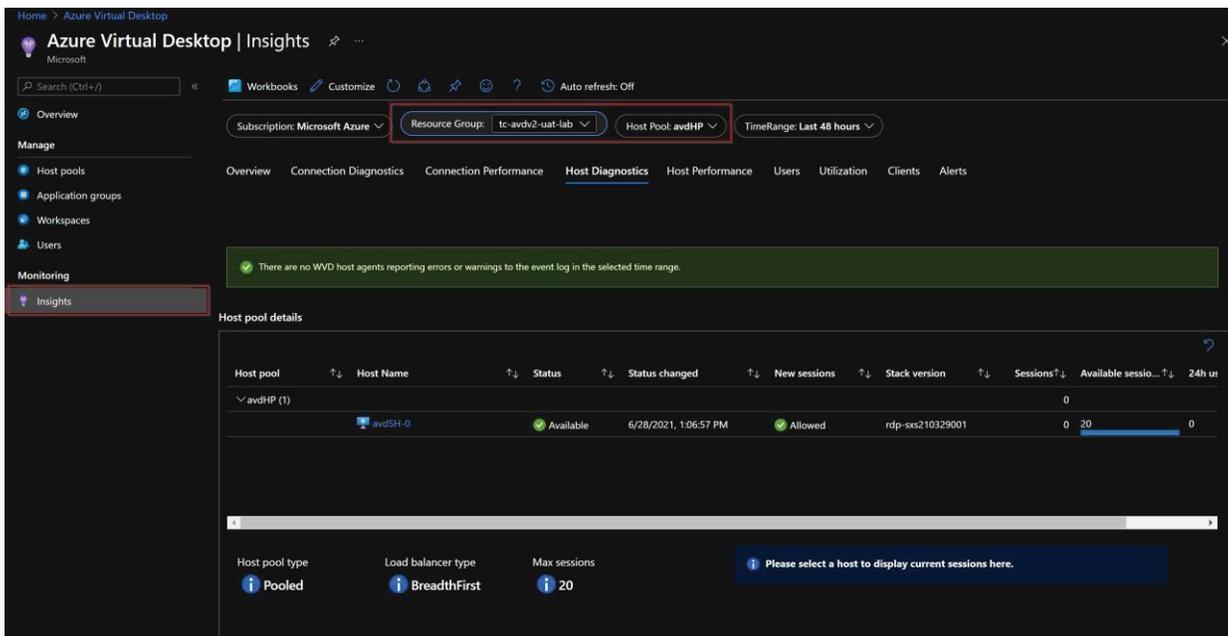
2. Select Insights. From here select your AVD Host Pool and Resource Group from the drop-down. You should see an alert that there are session hosts that need to be configured. Select 'Open Configuration Workbook'.



3. Select 'Session host data settings' and the Log analytics workspace that was provisioned by the Click-to-Run. Click 'Add Hosts to Workspace'. When prompted, click 'Deploy'.



4. You can now view diagnostic data and dashboards of your AVD deployment from the insights section of the AVD management portal.



AVD Click-to-Run: Additional Considerations

MSIX App Attach:

Please note that the current updates to configuring MSIX Applications via the Azure portal are not compatible with hosts joined to Azure AD Domain Services. Because of this, configuration options around MSIX App Attach are not included for the current Click-to-Run solution. However, if you are using an Active Directory server for the AVD resources, MSIX may be configured manually.

Host Pool Type:

This solution was scoped and authored to deploy a pooled host pool with breadth first load balancing. Personal host pools may be configured manually after deploying the Click-to-Run.

App Group Type:

This solution deploys a default 'Remote Desktop Group' to assign your AVD Users. However, you may set up a 'Remote Application Group' manually, post deployment, to work with the Click-to-Run.

AVD Optimization Script:

This is a community-driven tool intended to optimize your AVD session host performance. It disables services and features in windows that are not required for using AVD. This can be run on existing AVD session hosts. This should not be built into a custom image- the sysprep process will conflict with some of the configurations the tool performs.

Please note, this is not officially supported by Microsoft or TD SYNnex!