TD SYNNEX

AZURE VIRTUAL DESKTOP (AVD)

Click-to-Run™ Solution Deployment Guide

TD SYNNEX

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

TD SYNNEX

Azure Virtual Desktop Pre-Requisites:

☐ Verify that you have the Minimum acceptable licensing compatible for Azure Virtual Desktop Service.

Desired Operating System	License Requirements
Windows 10 Enterprise Multi-Session Windows 10 Enterprise Windows 11 Enterprise Multi-Session Windows 11 Enterprise	Microsoft 365 E3, E5, A3, A5 Microsoft 365 Business Premium Windows 10 E3, E5, A3, A5
Windows Server 2016, 2019	RDS Client Access License (CAL) with Software Insurance RDS CALS on Server Subscriptions through CSP

☐ Infrastructure Requirements

- **Azure AD Domain Services resource deployed in Azure –** TD SYNNEX Azure AD Domain Services Click-to-Run™ Solution is a great accompaniment and can be deployed separately and should be deployed prior to AVD.
  - If you have already deployed Azure AD Domain Services, please verify that the resource health must be shown as 'Running'. Password hash synchronization must be enabled on the tenant admin account (for domain joins).
- **OR – Use an On-Prem Domain Controller –** The customer or partner has extended their on-prem AD DS forest workloads to Azure. Resources are accessed via a VPN gateway connection to the DC's Vnet in Azure. AD Connect is configured and synced with their Azure AD identities.
- **OR – Choose to deploy a Domain Controller in Azure –** The customer or partner has a deployed domain controller in Azure with AD Connect configured and synced with their Azure AD identities. Please note TD SYNNEX offers a Click-to-Run™ Solution capable of deploying and configuring a Domain Controller on your behalf.

☐ **Security Defaults:** Ensure Security Defaults is disabled on your Azure AD tenant. User

☐ Access

- **Remote Desktop Client–** AVD users are expected to access published resources through the Remote Desktop client. This must be downloaded manually after deployment.
  Instructions for installation and setup will be included in this step-by-step guide.

TD SYNNEX

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)

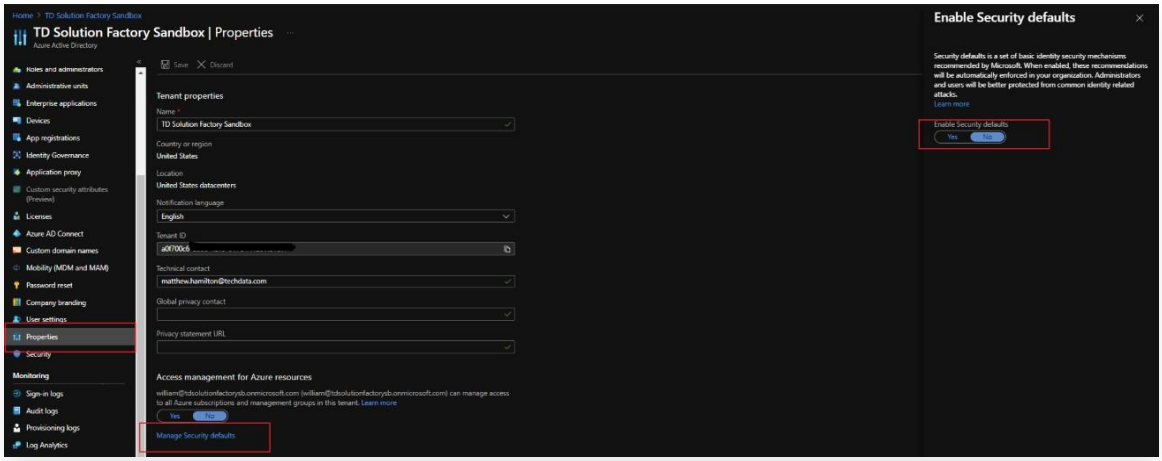
☐ Purchase and deploy the AADDS Solution.
☐ Ensure AADDS is returning a healthy 'Running' state. Deactivate Security
☐ Defaults on your tenant.
☐ Ensure Admin is a member of the AAD DC Administrators group. Reset Domain
☐ Admin password (for password hash sync).
☐ Ensure DNS is configured on the AADDS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

AADDS Pre-Deployment Steps

1. **Purchase the AADDS (Azure Active Directory Domain Services) solution**
   a. Configure solution in the digital locker

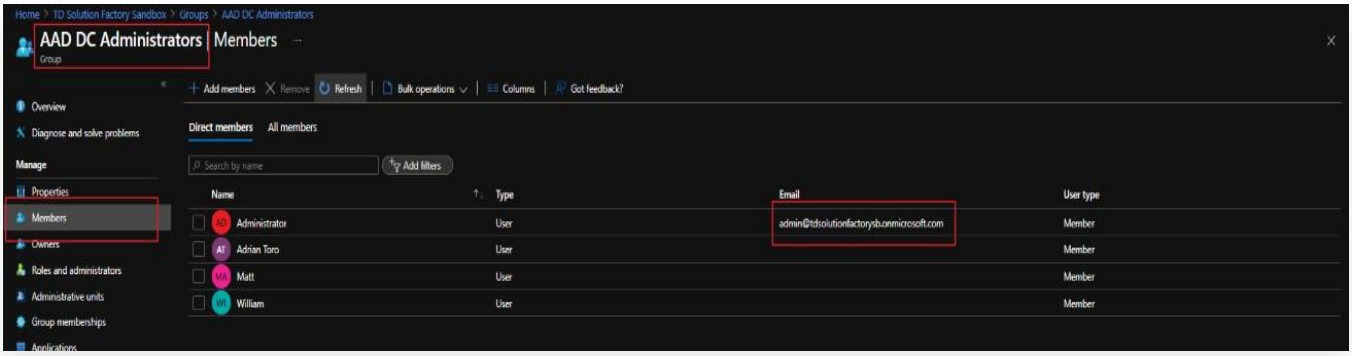
2. **Follow AADDS step by step guide for configuration**
   a. If at any point you are unsure, please reach out to us

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

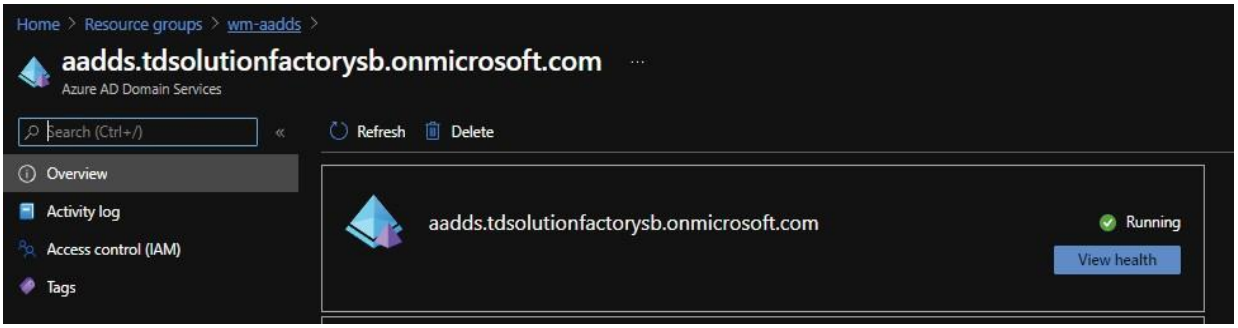


Step 3 continued from previous page

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

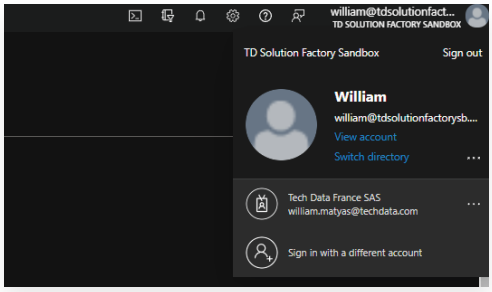


- [ ] Make note of domain ex- aadds.partnerAVDtest2020.onmicrosoft.com (you will need this in the AVD Section)

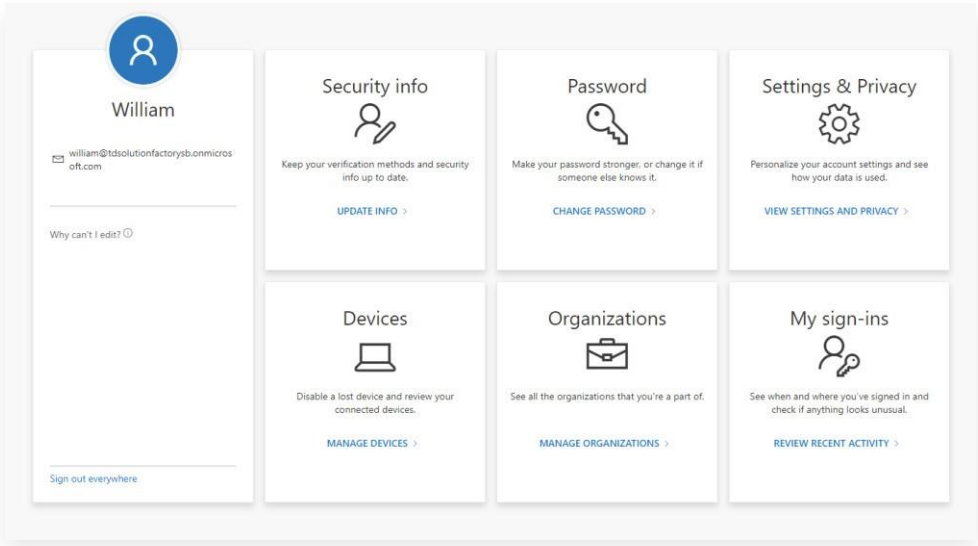


☐ Reset domain admin password (temporarily)

i. Click on your admin profile and on “View Account”



ii. Select ‘Change password.’

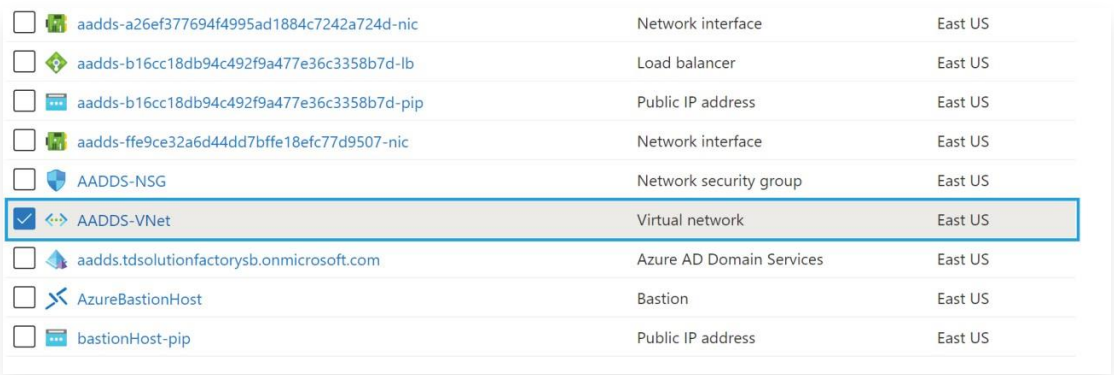


b. Log out and log back in as the domain admin. You must ensure the login and password are correct for the AVD Deployment.

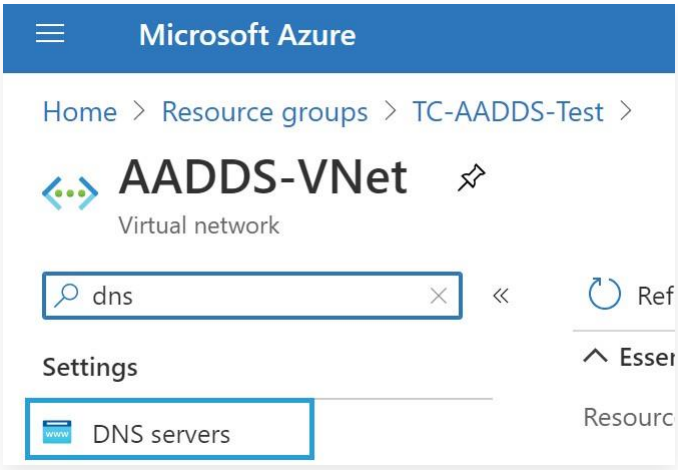
4. Partner (If using AADDS) Verify DNS Configuration

a. Verify custom DNS is configured on your AADDS VNet.

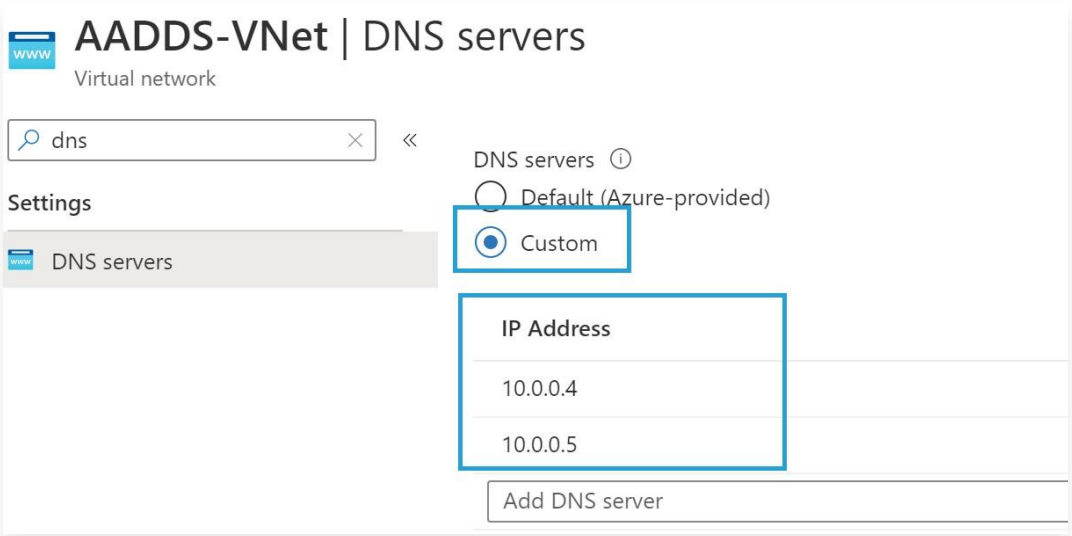
i. Locate your AADDS Vnet.



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:

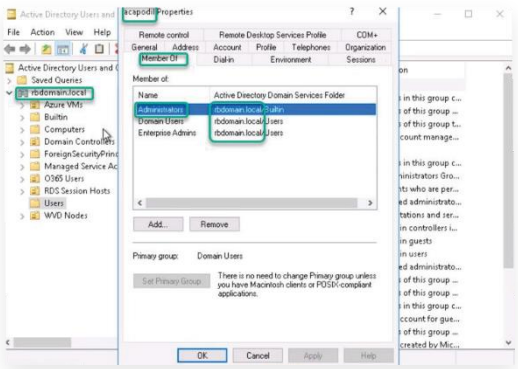
Pre-Deployment Steps (partner must complete)

- ☐ 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.

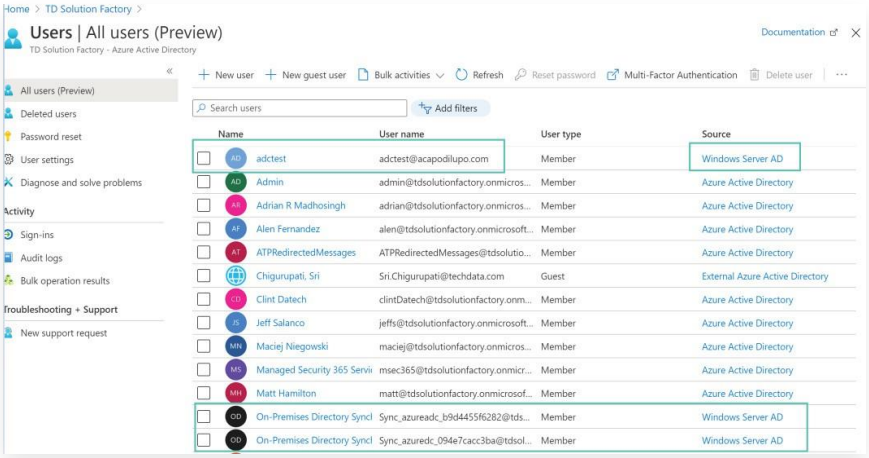
Active Directory with AD Connect Deployment and Considerations

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

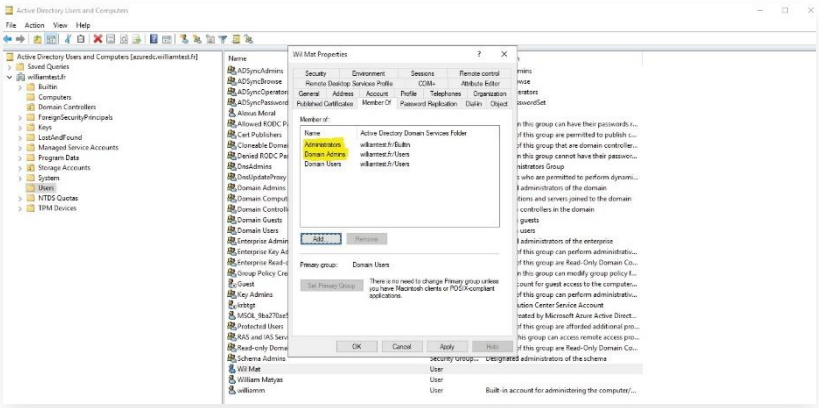


Ad to verify:

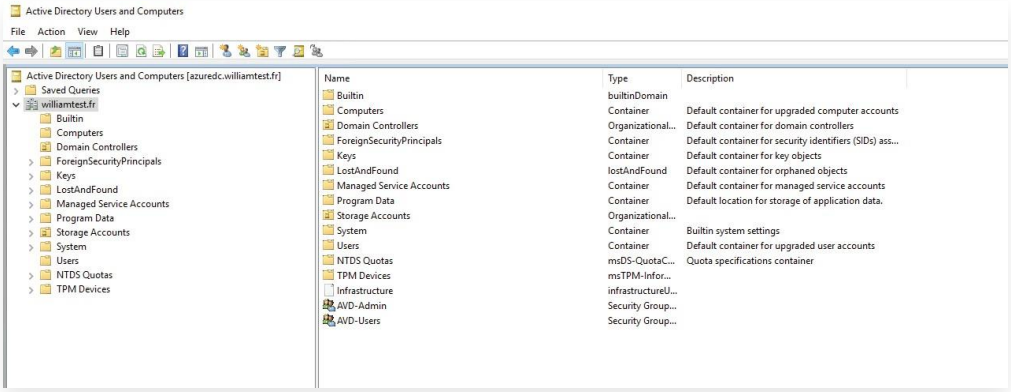


b. Make sure your Domain Admin is part of both the Administrators and Domain Admins groups.

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.

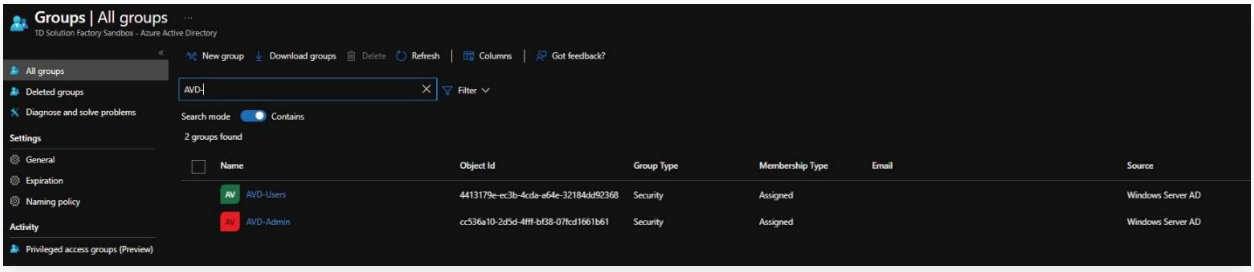


c. We also need you to create two Groups in your local Domain Controller:
   - The AVD-Admin group
   - The AVD-Users group

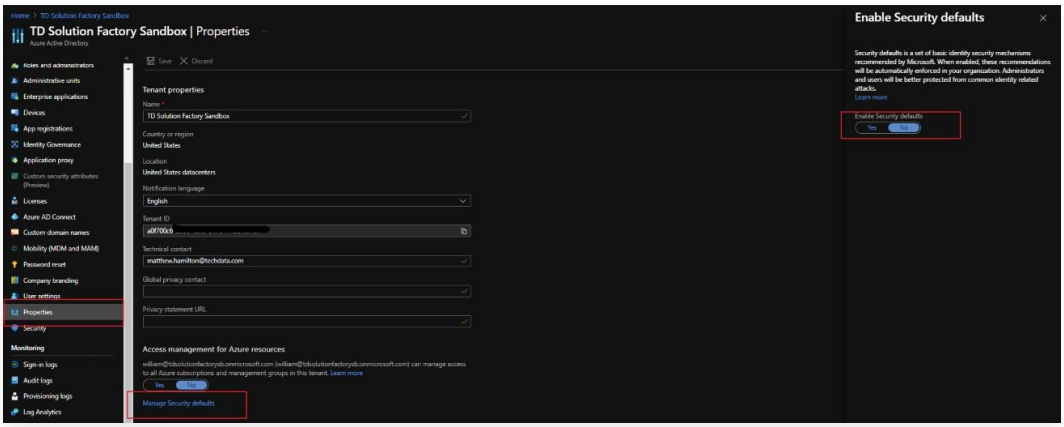


The AVD-Admin group will be used for Azure Virtual Desktop Admins. The AVD-Users group will be used for Azure Virtual Desktop Users.

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



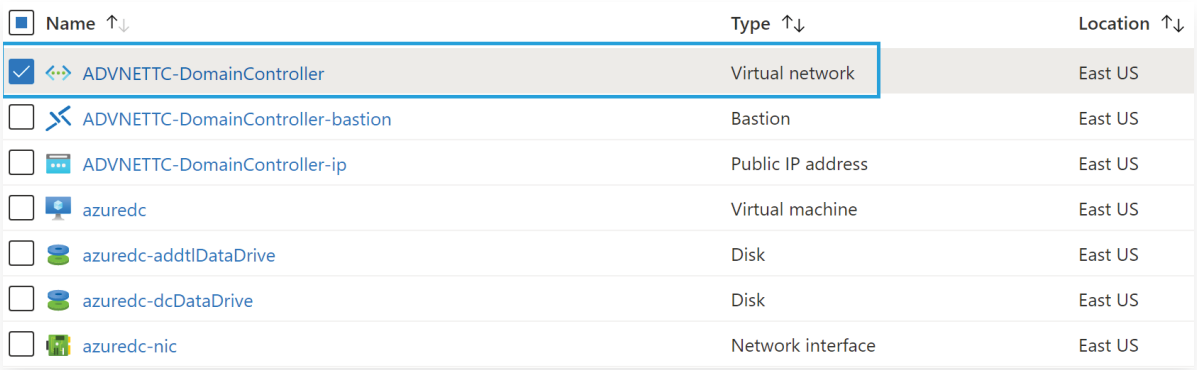
d. Deactivate security defaults (temporarily)
   i. This can be turned back on after deployment



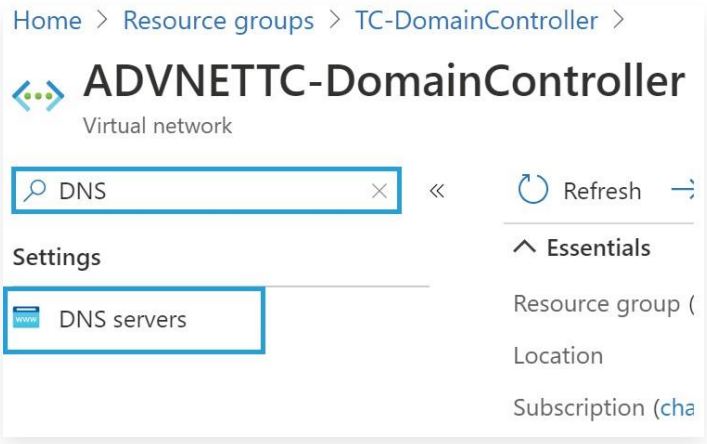
e. IMPORTANT NOTE: **Do not proceed unless your domain is replicating and returns a healthy status in Azure.**

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

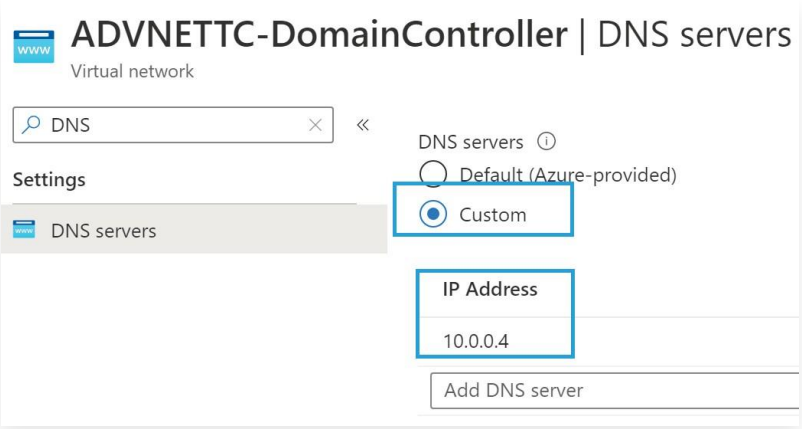
a. Verify custom DNS is configured on your Domain Controller VNet.
   i. Locate your AD Vnet.



   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.

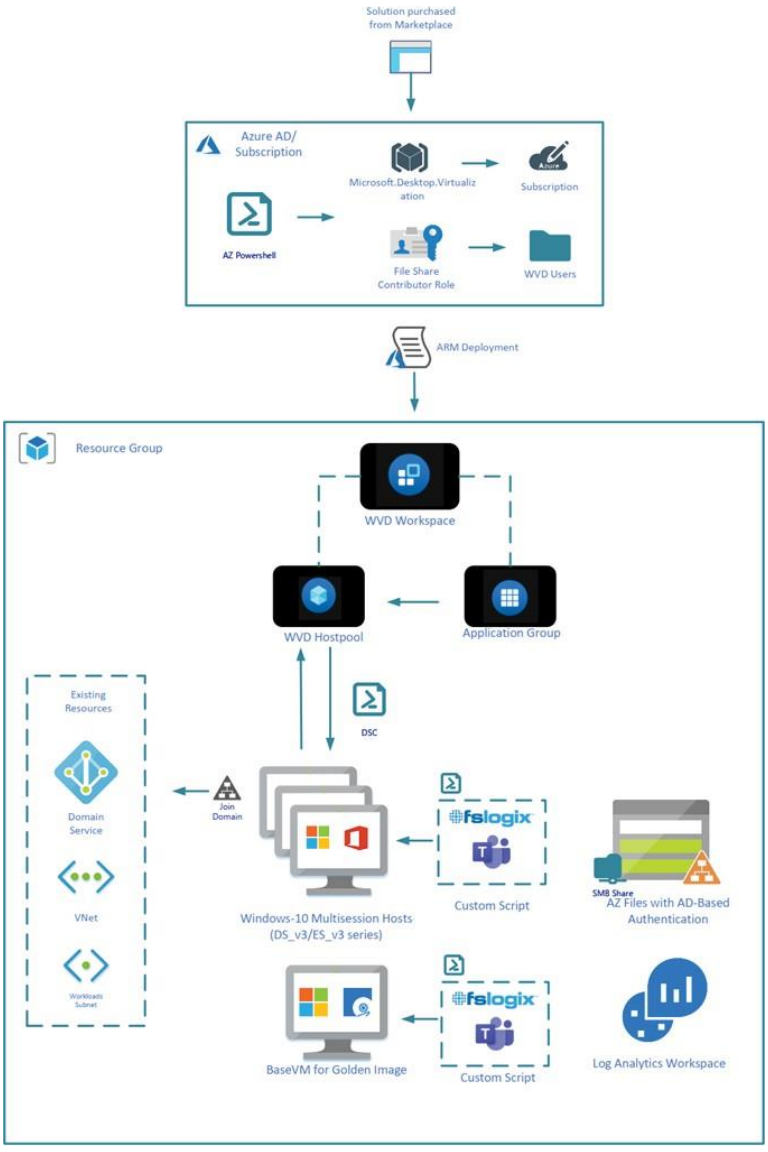


You may now proceed with the AVD Solution Deployment!

Solution Overview:

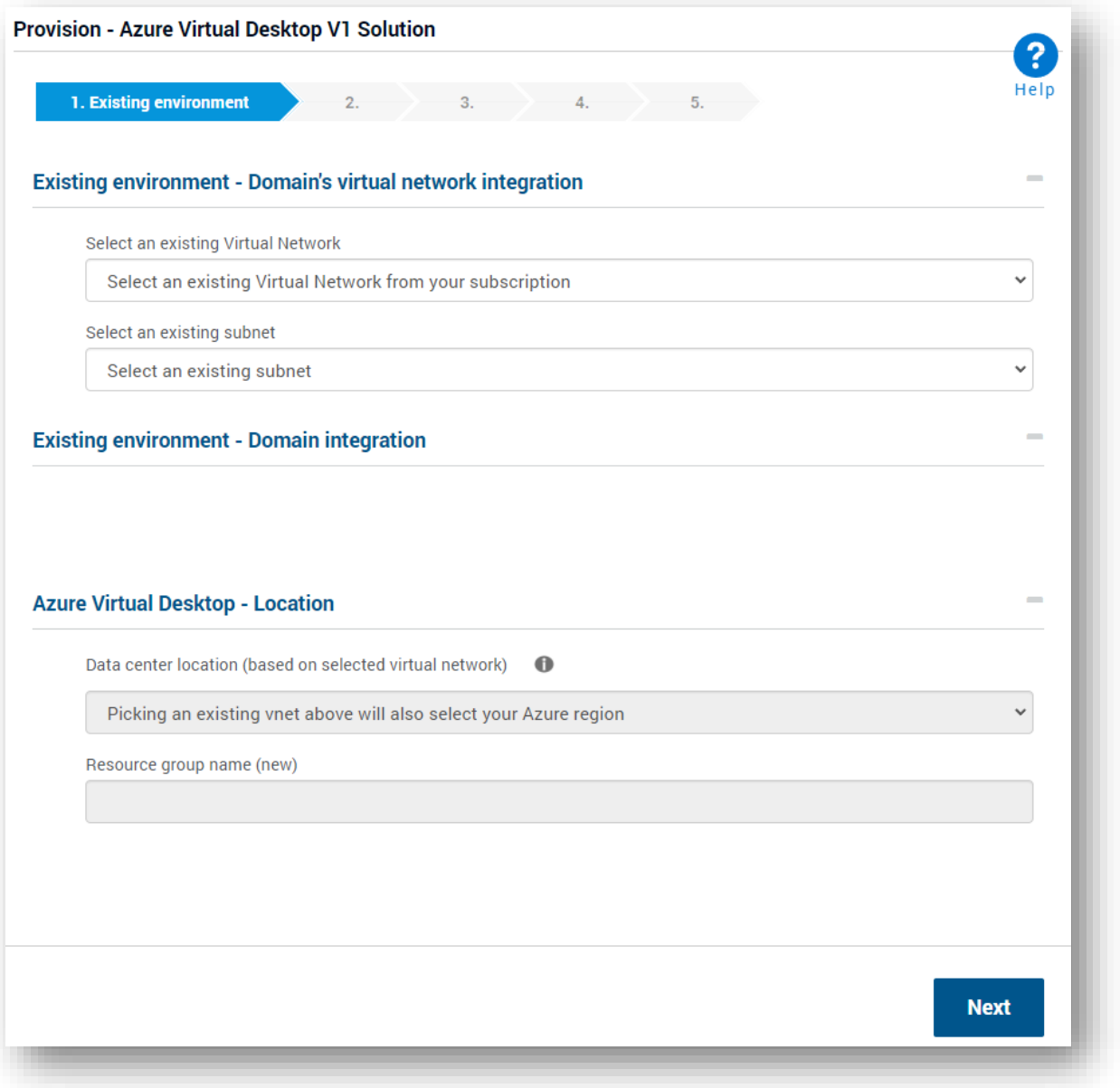
"Azure Virtual Desktop, or AVD in short – is a born in the cloud Desktop-As-a-Service platform service offering on top of the Microsoft Azure Cloud. All the infrastructure services, such as brokering, web access, load-balancing, management, and monitoring is all setup for you as part of the control plane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

Deployment Architecture: General Workloads & Optional High Powered Apps Deployment



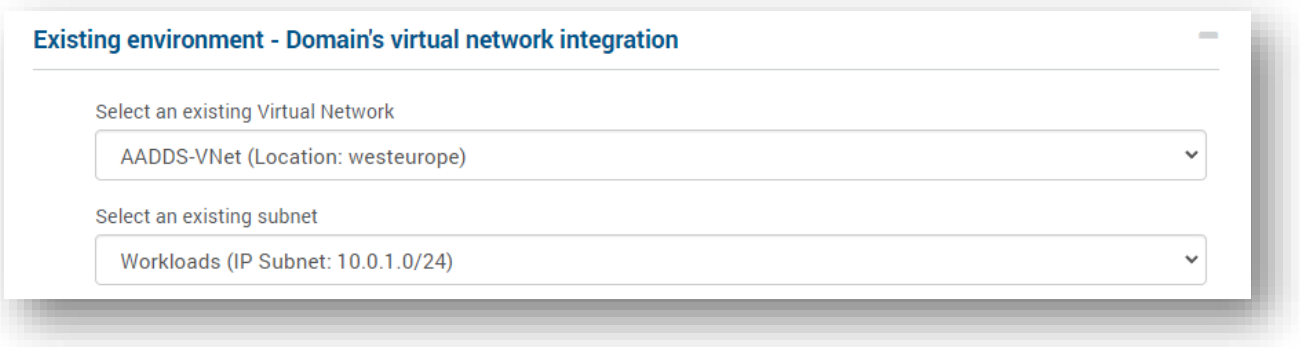
AVD Deployment and Considerations

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



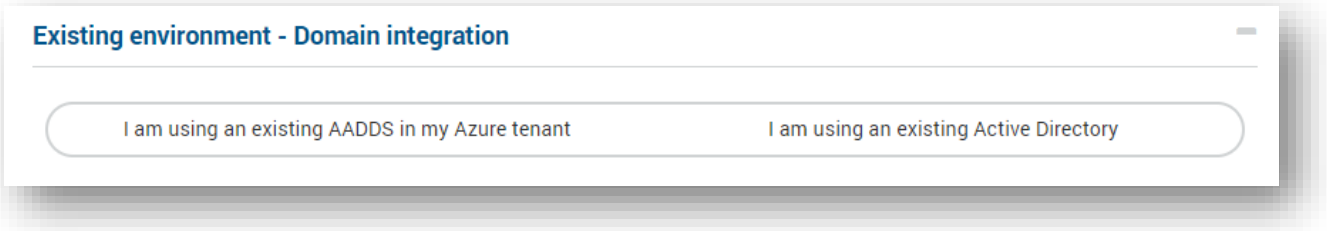
Let's get started with the User Interface!

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:



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

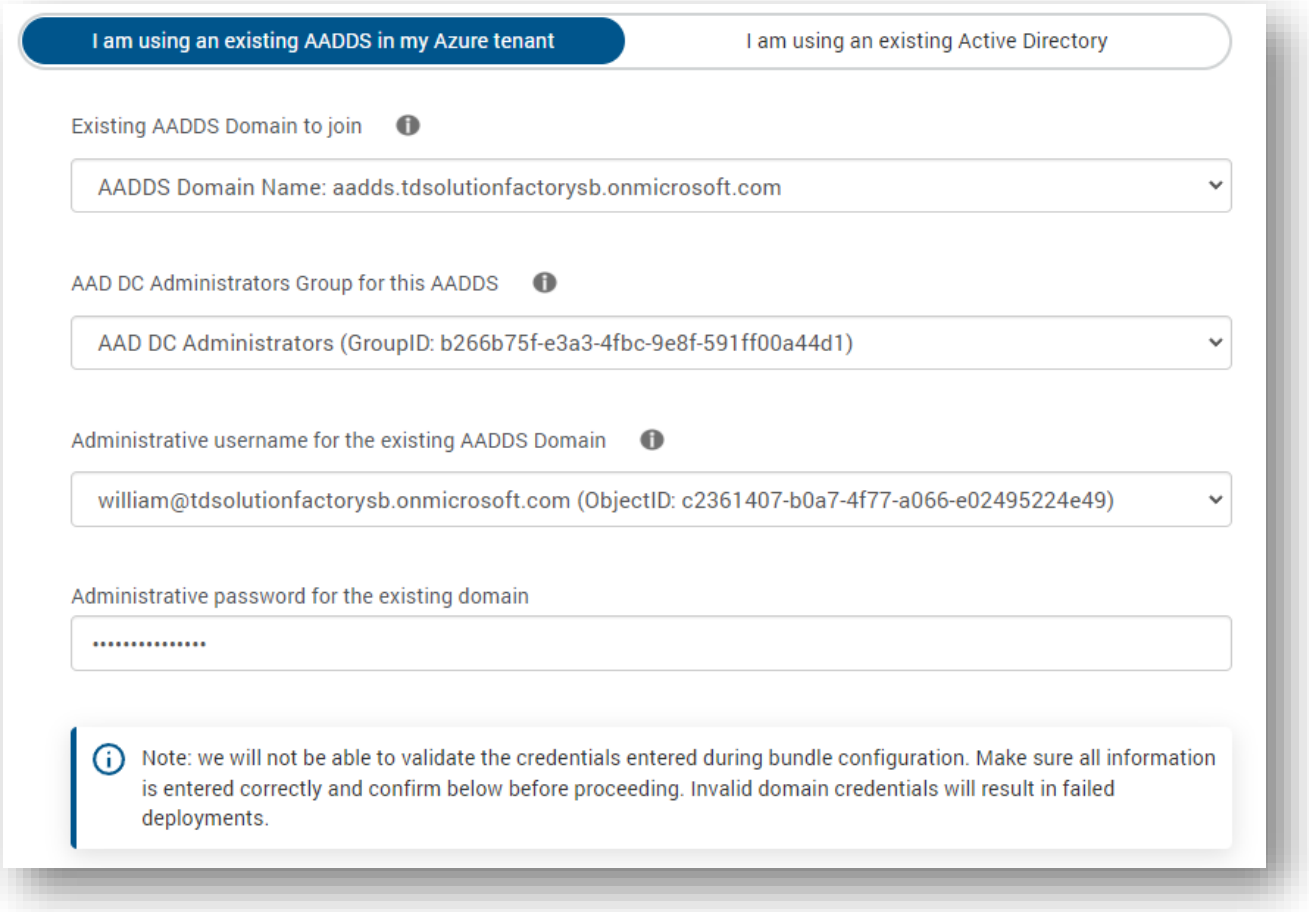
a. Azure Active Directory Domain Services (AADDS)
b. Active Directory (AD)



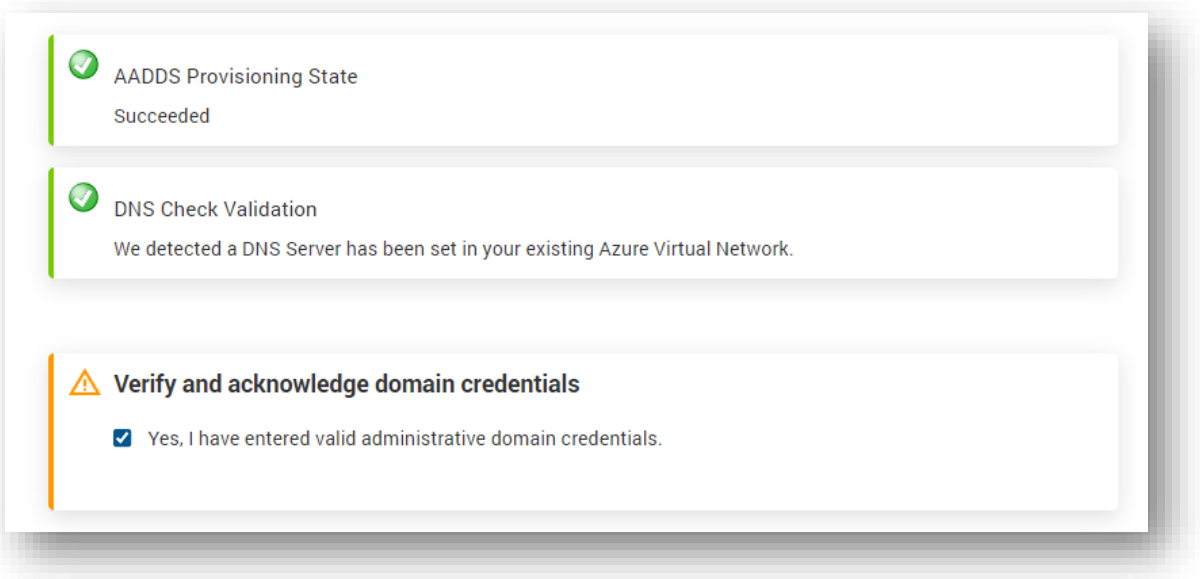
a. Azure Active Directory Domain Services (AADDS)

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.

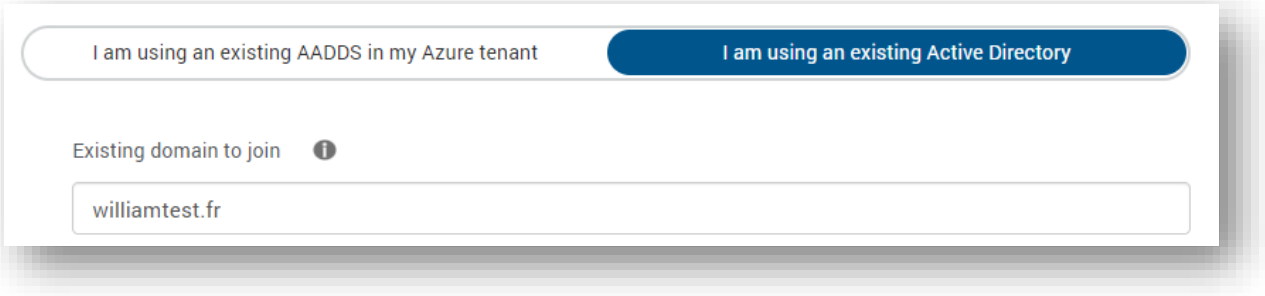
Please select the Admin username you plan to use and enter the Administrative Password tied to the user selected.



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

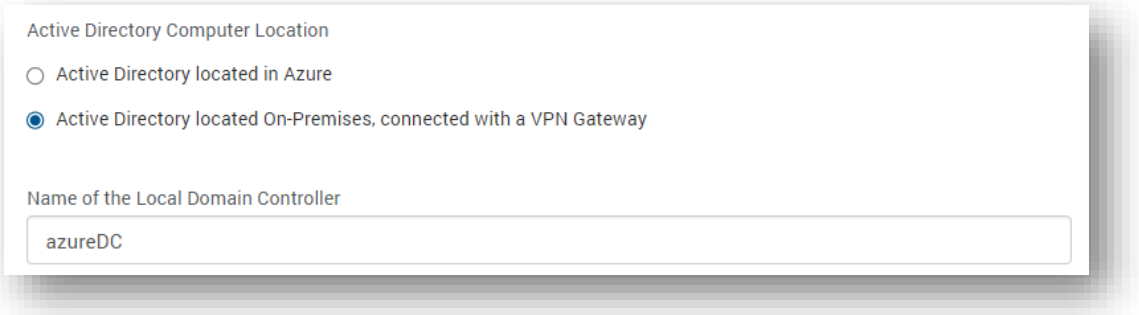


a. Active Directory (AD) First, please enter the Existing Domain Name you plan to join:

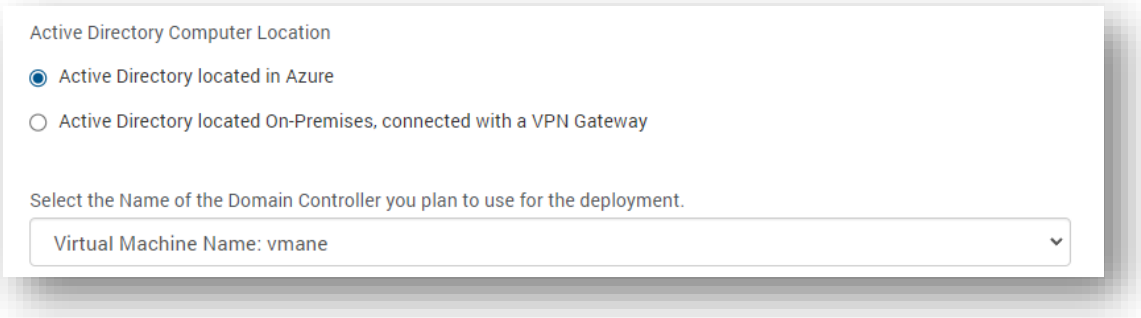


Then Select the location of the Active Directory Computer Location.

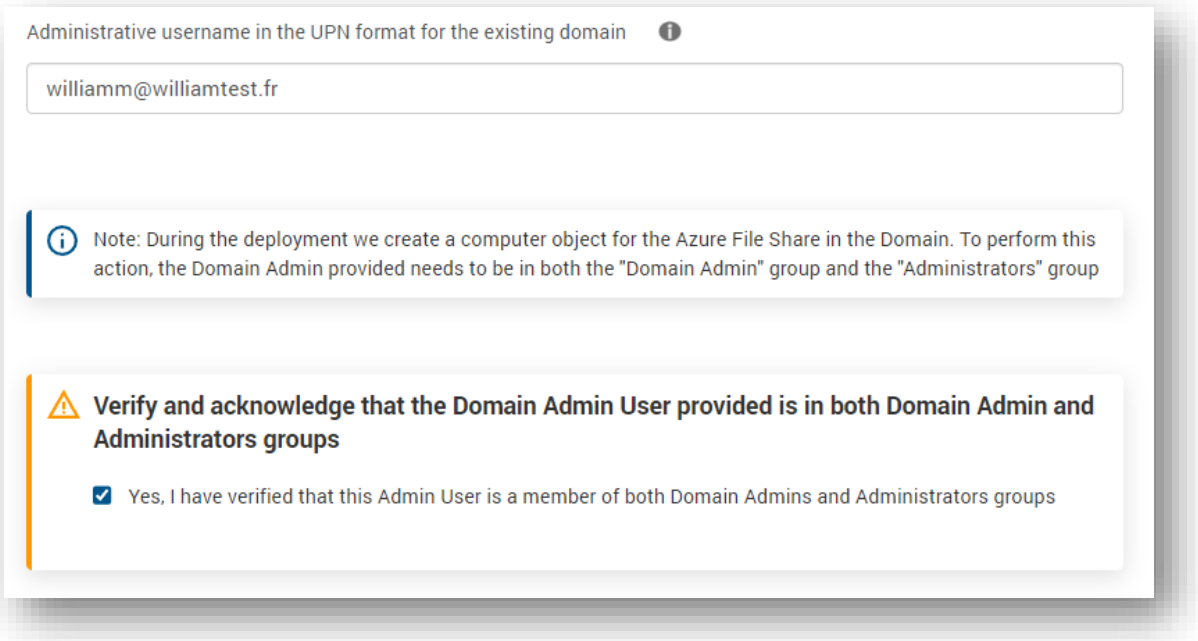
i. If it is located on-premises connected through a VPN Gateway, please enter the exact Computer name:



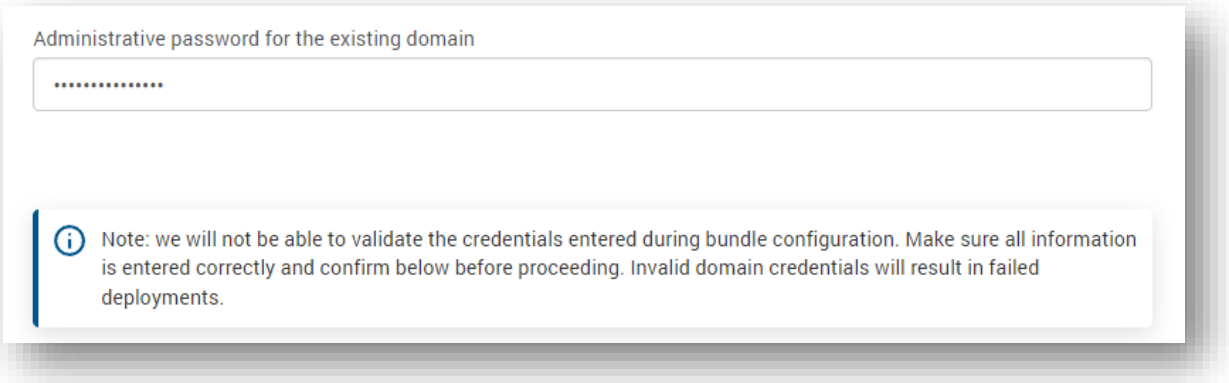
ii. If it is located in Azure, please select the Virtual Machine through the drop-down menu:



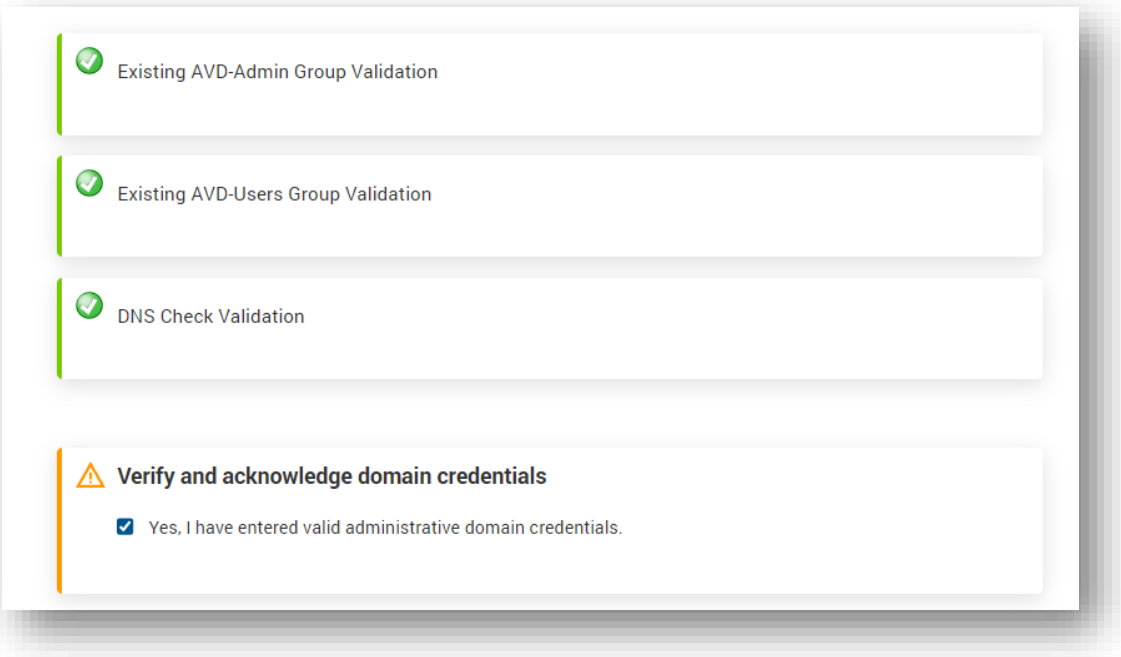
Then, please enter the Domain Admin Username in the UPN format and acknowledge that the admin User you provided in both the Domain Admin and Administrators group. (Reminder: During the deployment, we create a computer object to join the Azure File Share to the Domain. This is the main reason why we need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



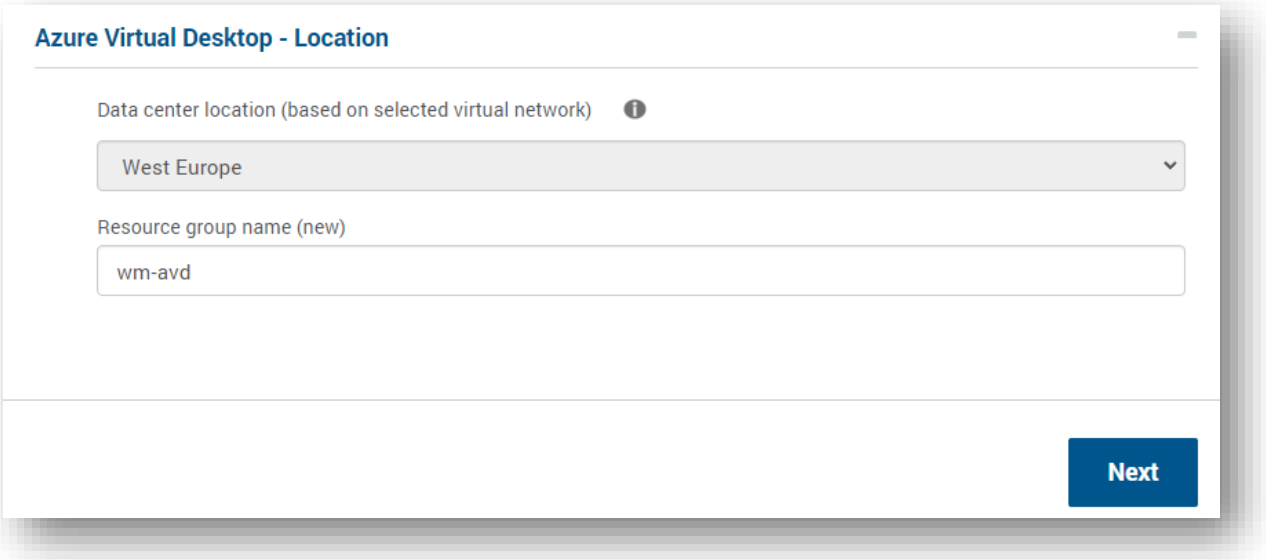
Then enter the administrative password for the selected user:



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:

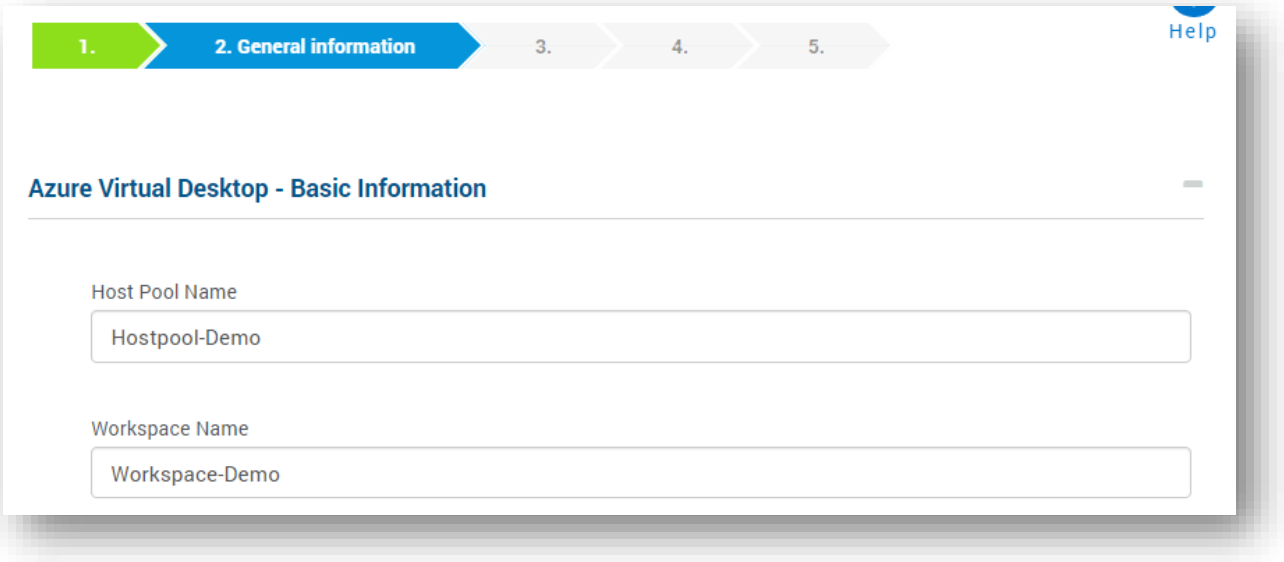


Moving on to the Azure Virtual Desktop configuration, please enter a Resource Group Name: (Data Center Location is based upon the location of the AADDS / AD you've previously deployed).

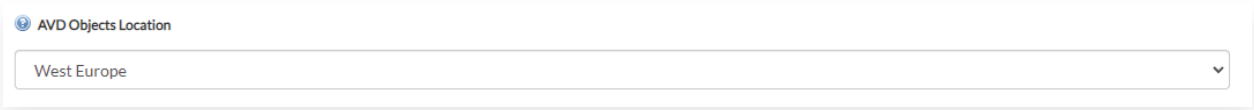


Click on Next

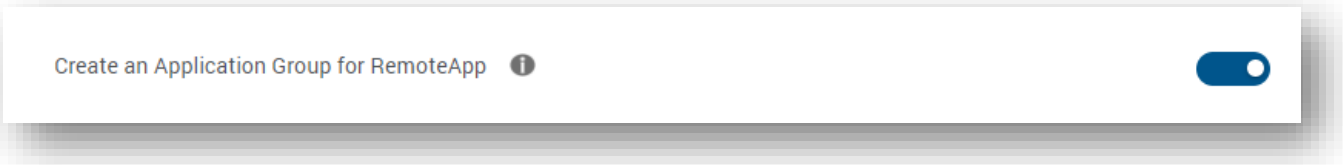
Then enter a Host Pool Name and a Workspace Name for the Azure Virtual Desktop:



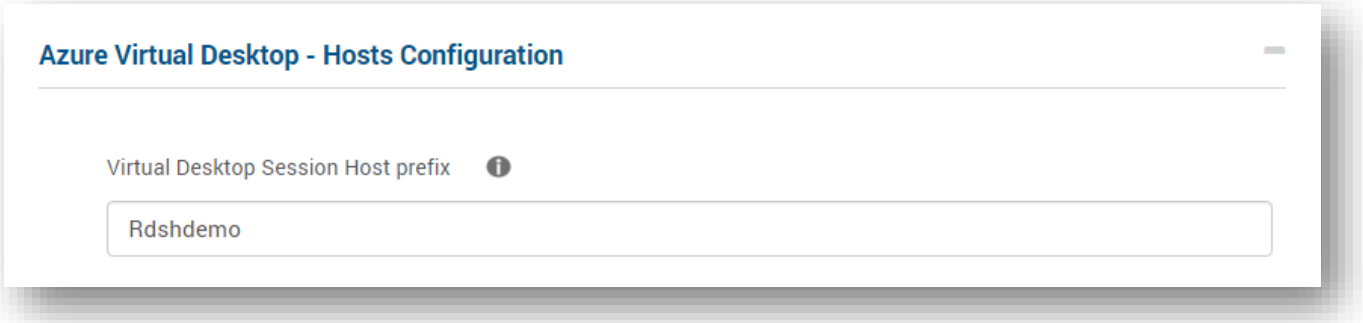
Please select the AVD Objects Location. This is where you will deploy your AVD Services (Host Pool, Workspace, Application Groups…). This does not define the location of your Session Hosts.



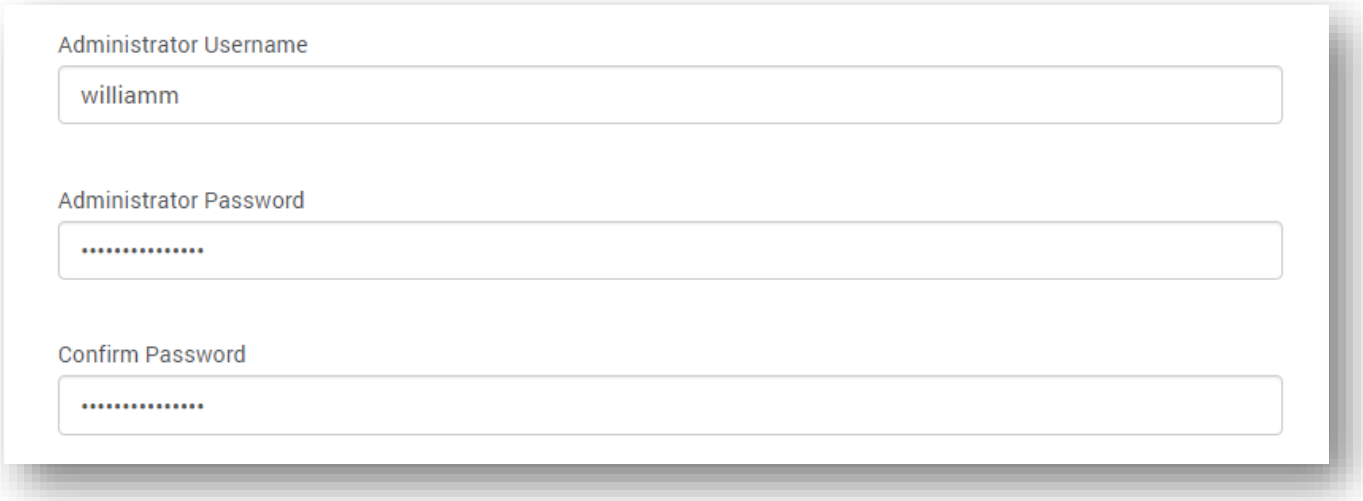
By default, we create a Default Application Group (DAG). You can also create an additional Application Group that would be dedicated for RemoteApp.



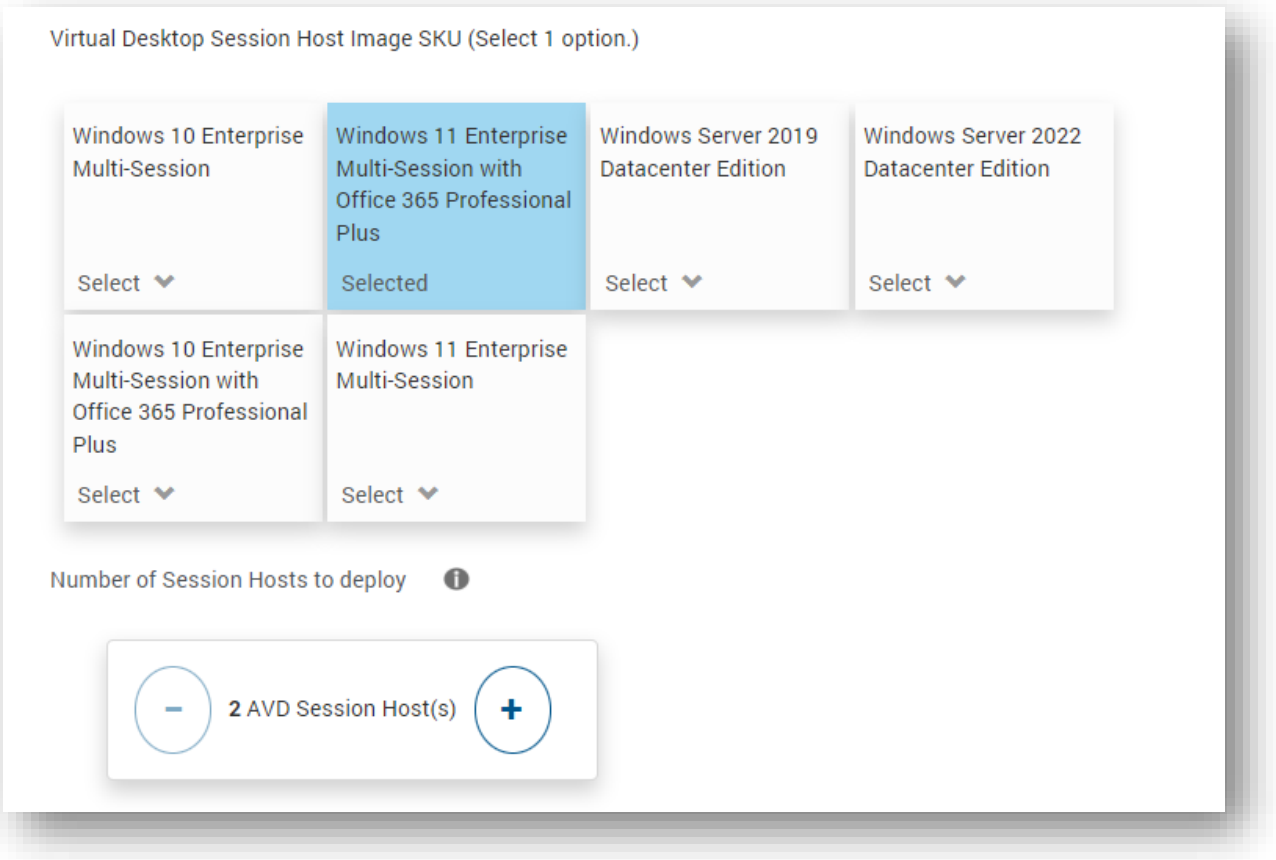
Moving on to Session Hosts Configuration. Please define a Session Hosts prefix. It will be limited to 8 characters as we append -host1, -host2… to the Virtual Machines and the Computer Name is limited to 15 characters.



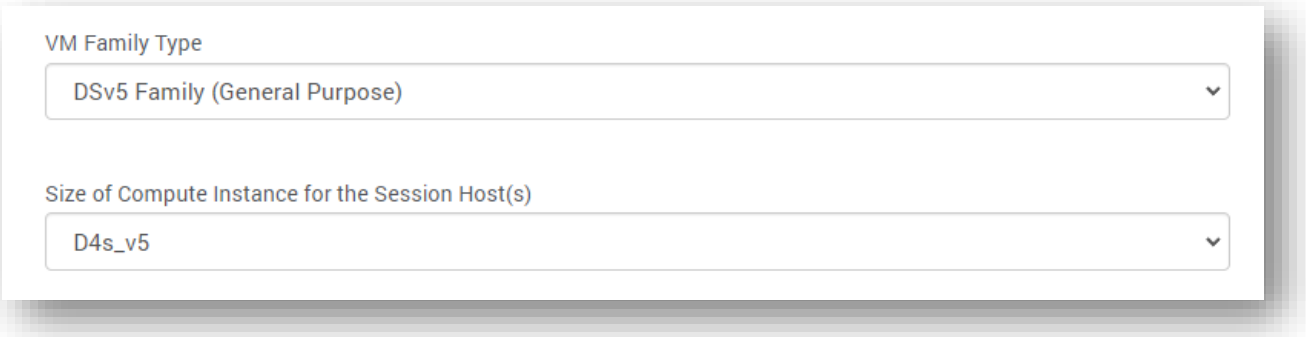
Then enter the local admin credentials you plan to use for the Session Hosts:



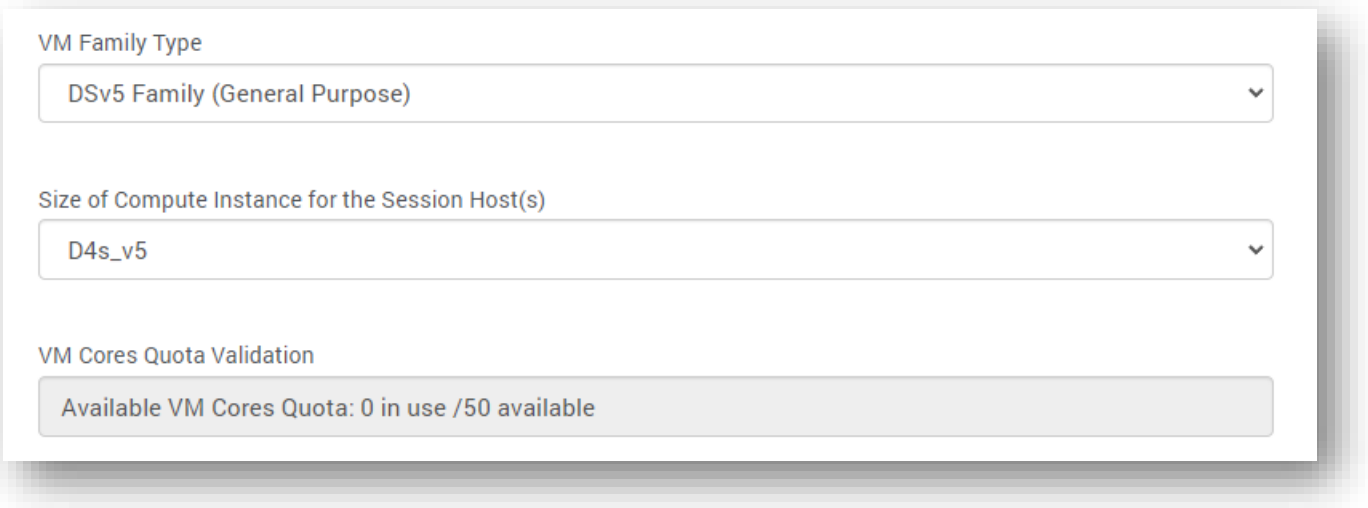
Select the Session Host Image Sku you plan to use and the number of Session Hosts you plan to deploy:



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

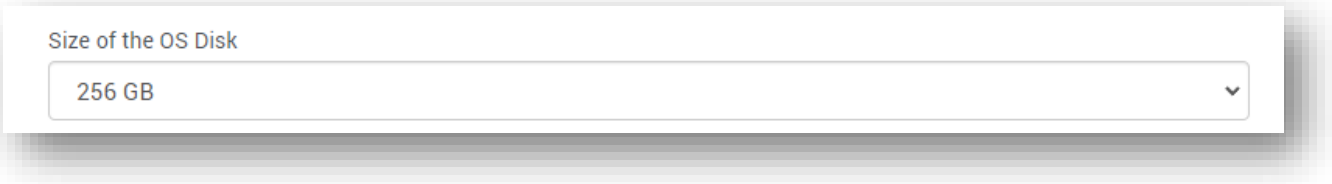


We have added up a logic to validate VM Cores Quota validation. The number in the VM Size represents the number of cores each VM uses.

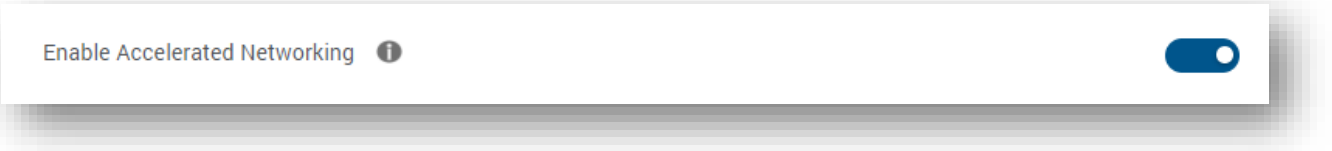


Warning! Please bear in mind to multiply the number of cores a VM Size would use by the number of Session you plan to deploy!

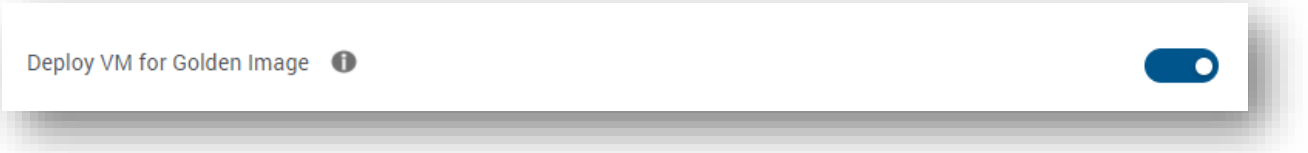
Then please select the OS Disk size you plan to use:



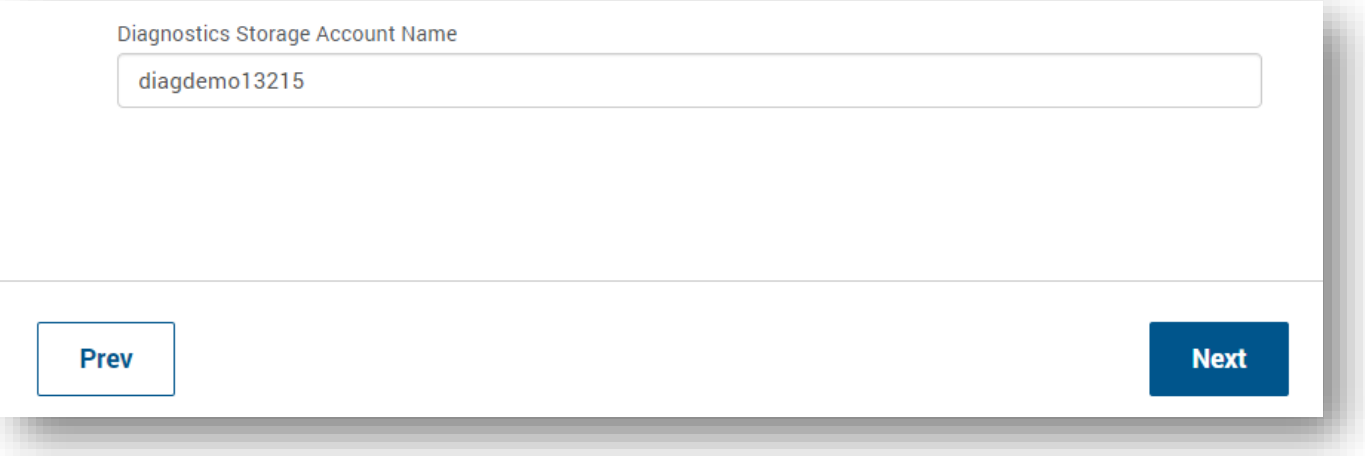
If available for the VM Size, you can enable Accelerated Networking:



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

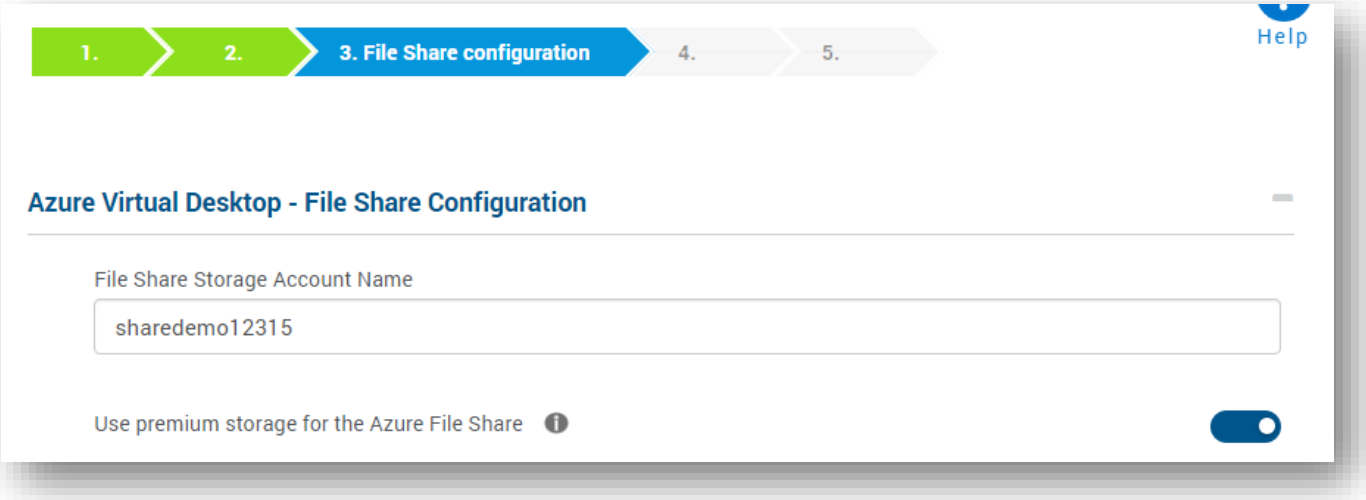


And finally, please enter a name for your Diagnostics Storage Account:

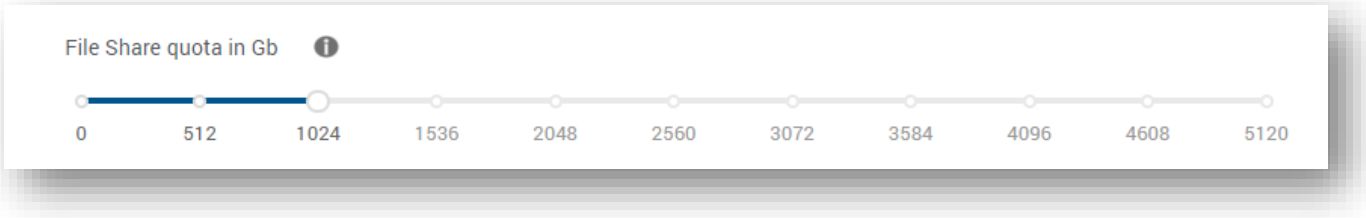


Then click on Next.

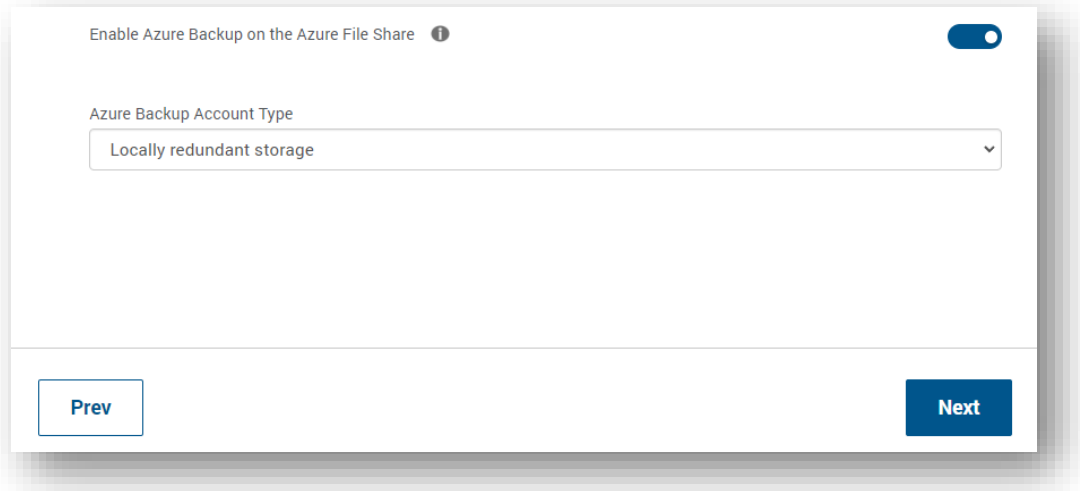
Now that we are done with the Session Hosts configuration, let's move on to the Azure File Share configuration.
The Azure File Share will be used to store User Profiles. Please enter a name for your File Share Storage Account and select if you want to use Premium Storage or not:



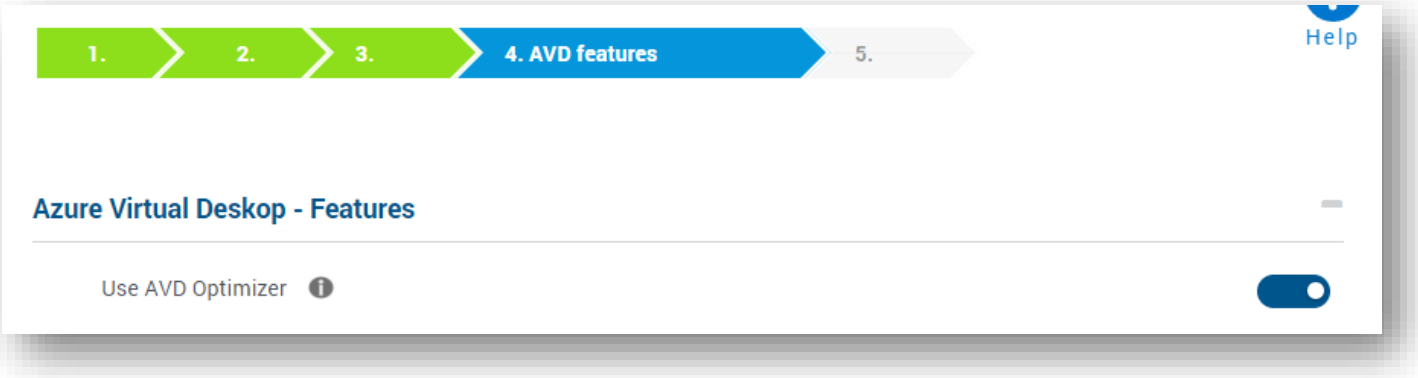
Then define the File Share Quota (Standard storage is Pay as you Go, but Premium Storage is provisioned):



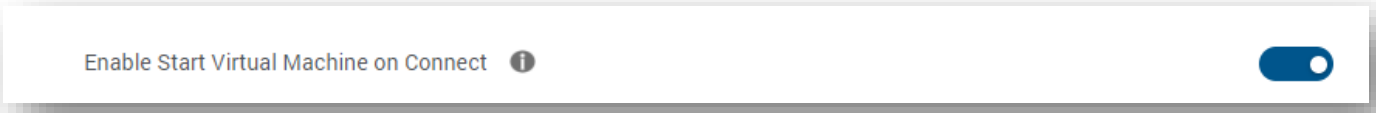
And select if you want to use Azure Backup for your Azure File Share and the redundancy of your Azure Backup Account Type. Then click on next!



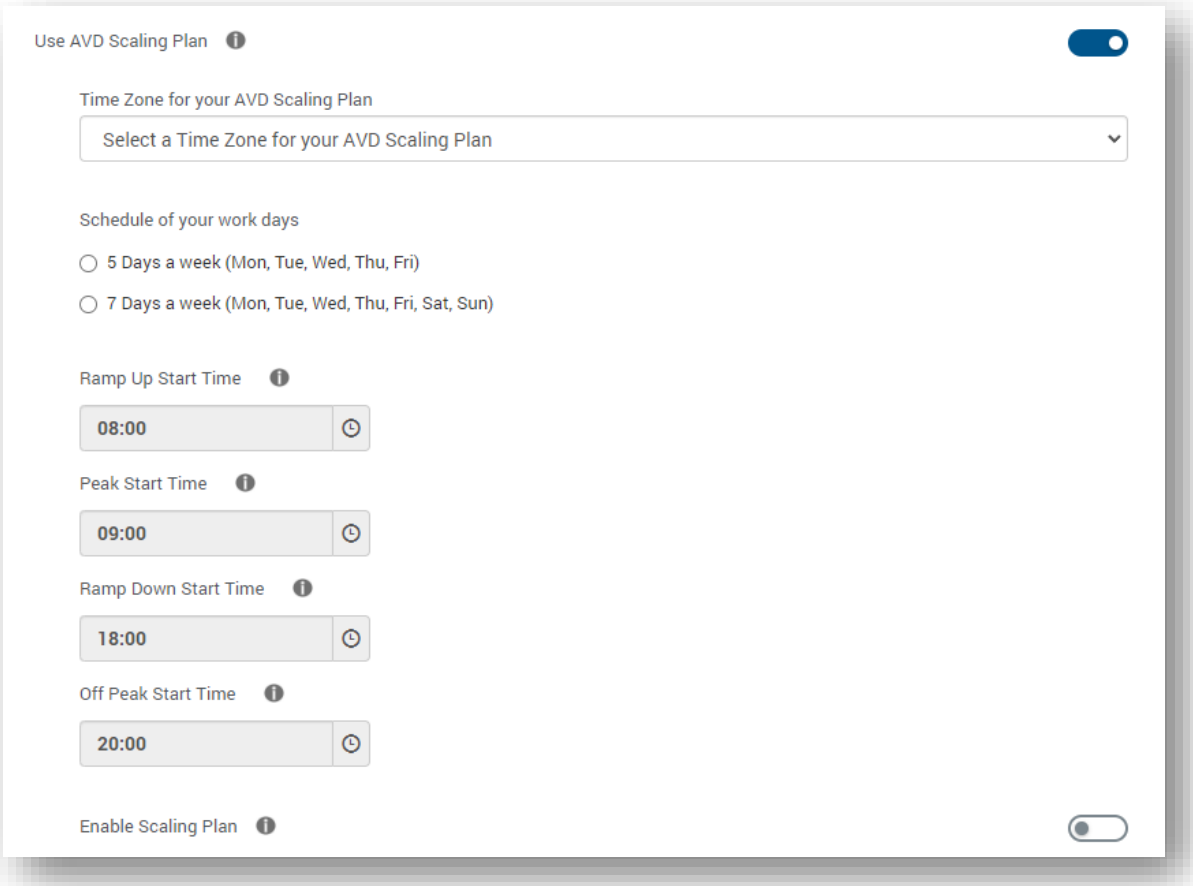
Moving on to extra Azure Virtual Desktop features, you can select if you want to use the AVD Optimizer:



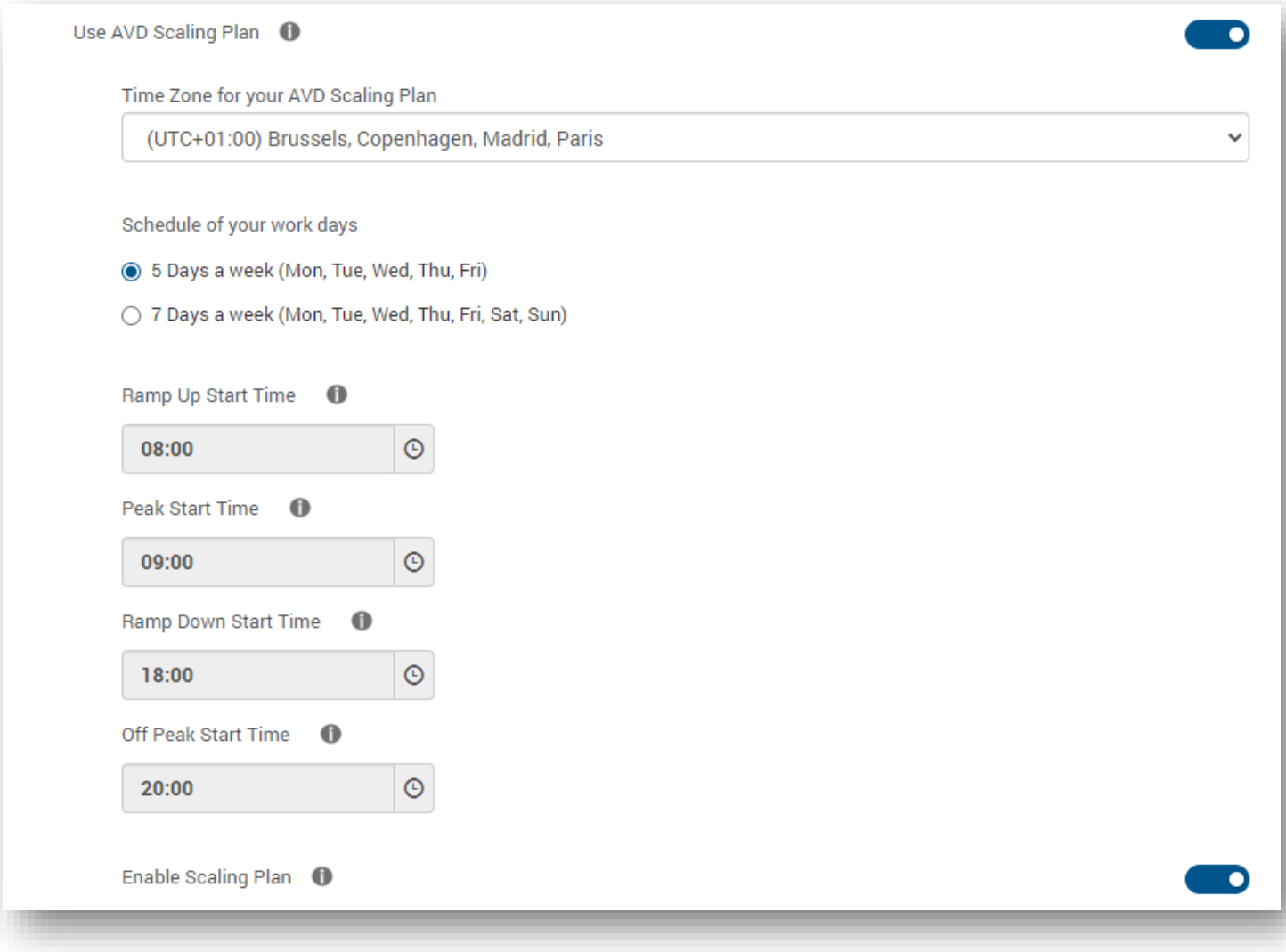
If you plan to enable the "Start Virtual Machine On Connect" feature:



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

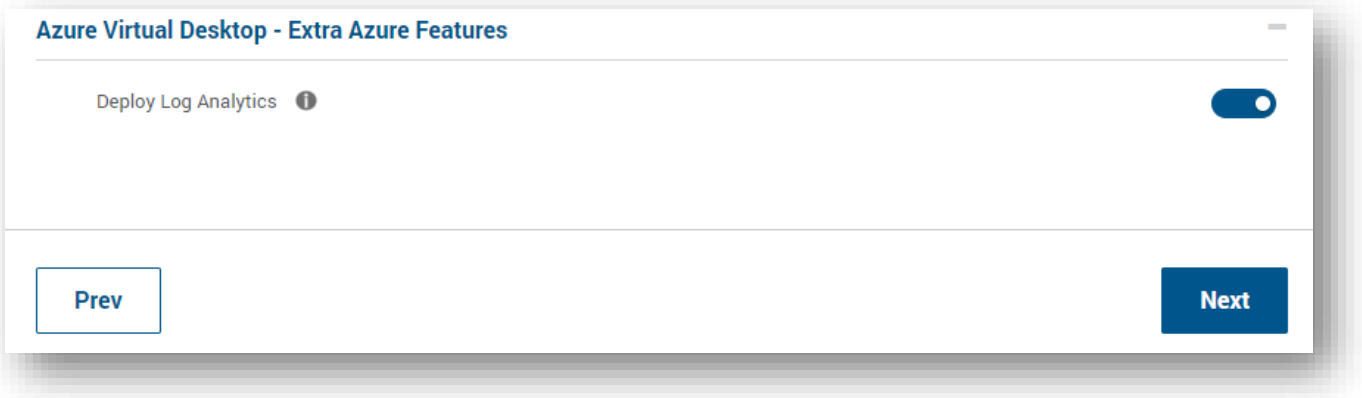


To configure it, please select the adequate Time Zone, your Workdays Schedule, the different Start Times and if you plan to directly Enable the newly created Scaling Plan:

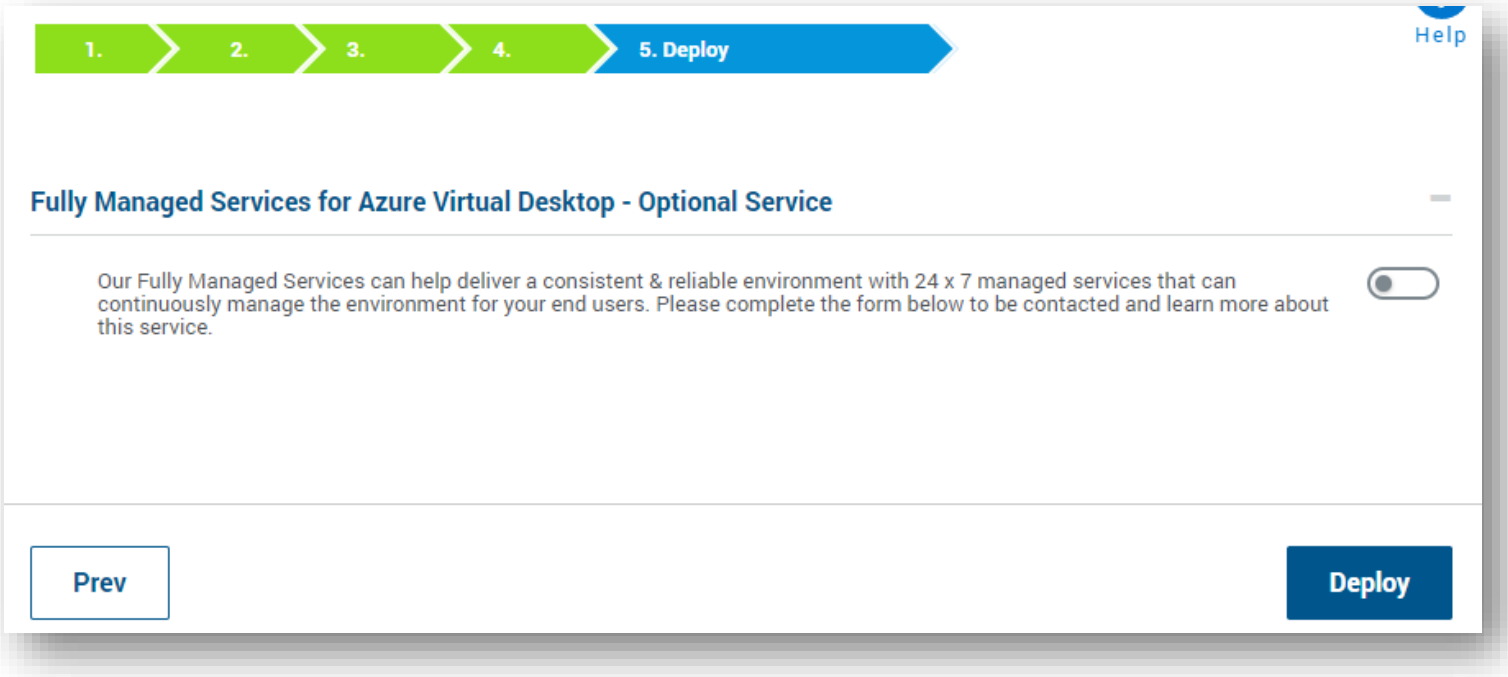


By default, the Ramp Up Load Balancing Algorithm is Breadth First and the Ramp Down Load Balancing Algorithm is Depth First.
The Peak Load Balancing Algorithm is Depth First and the Off Peak Load Balancing Algorithm is Depth First.
The Ramp Up Minimum Hosts Percentage is 20% and the Ramp Up Capacity 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:



Then click on next.



You can then click on Deploy Now!

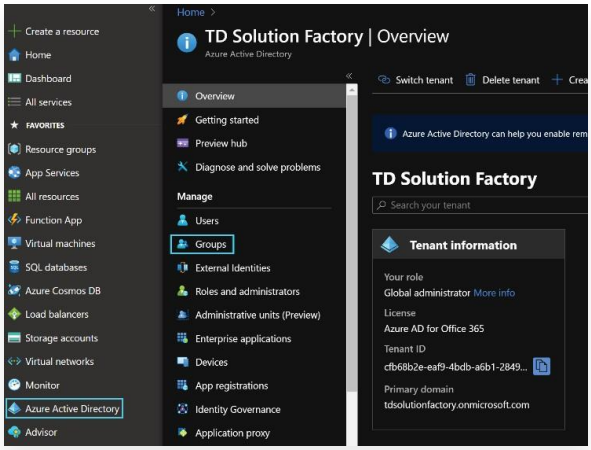
Post-Deployment Checklist for Azure AD Domain Services (partner must complete)

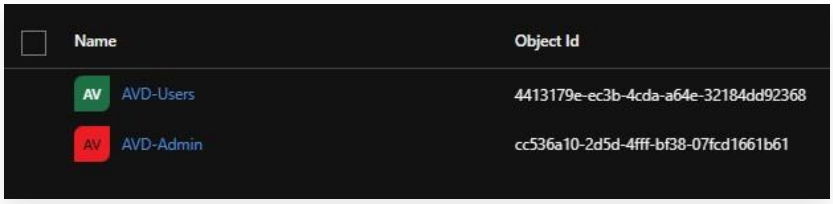
☐ Assign users to AVD Users / AVD Admin group.

Adding users to 'AVD Users' AAD Group

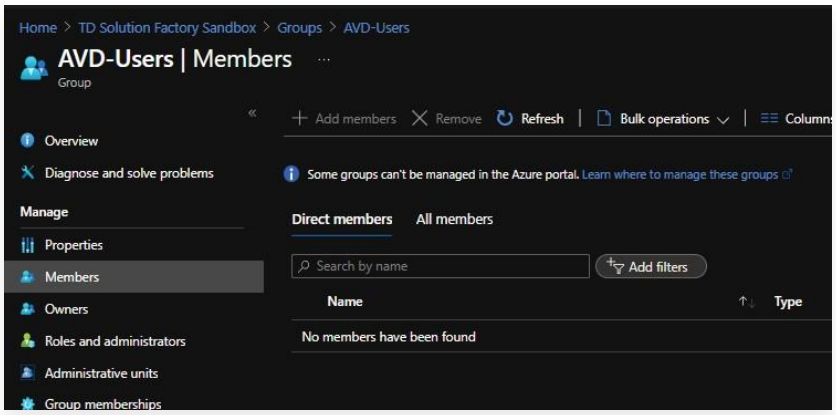
For AADDS Scenarios, we automate the creation of a custom security group called 'AVD-Users.' Any users or groups who you would like to grant access to your environment should be added to 'AVD-Users.'

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





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

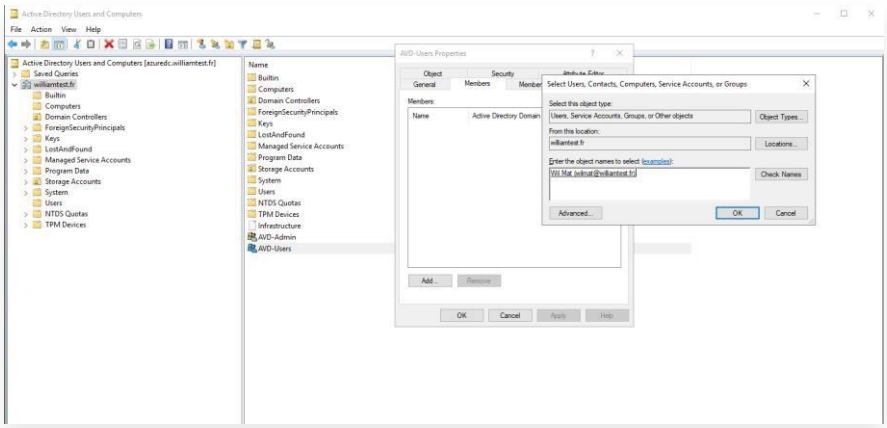


Post-Deployment Checklist for Domain Controller Deployments (partner must complete)

☐ 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.



TD SYNNEX

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 Doman 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.**

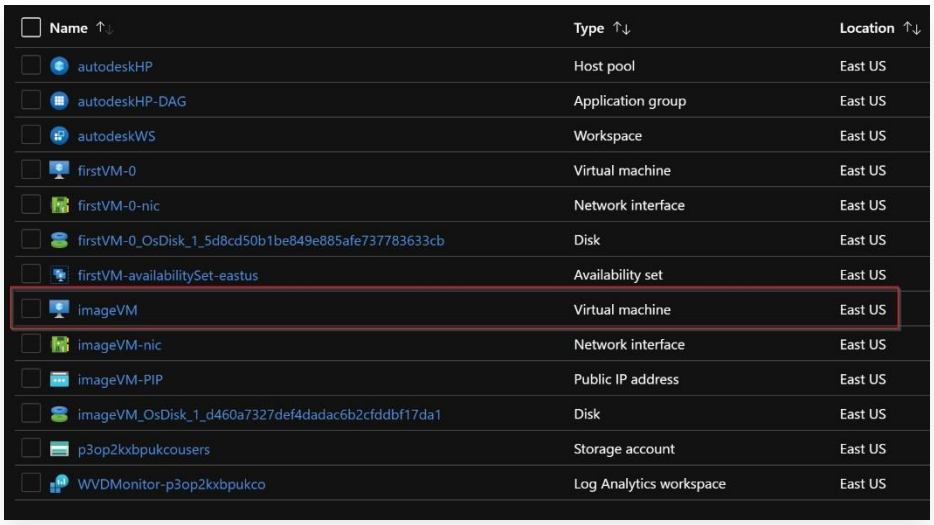
Steps to resolve:

- 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.

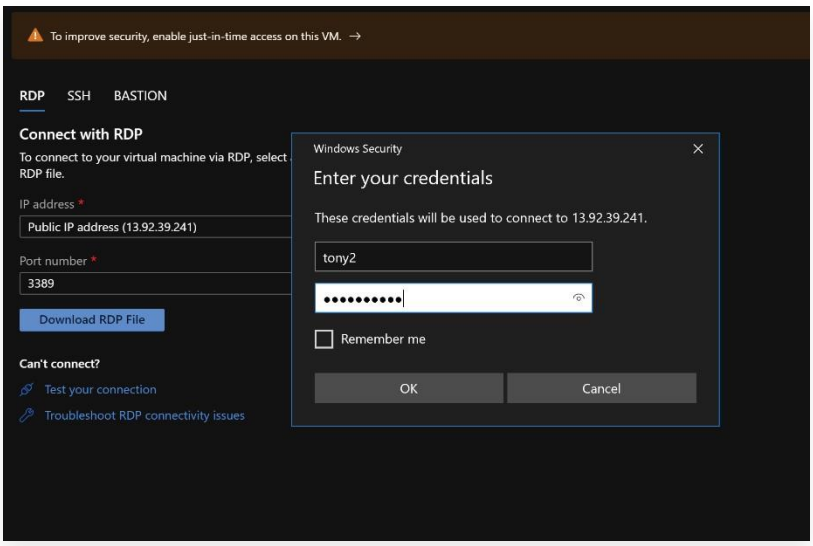
AVD V1 Click-to-Run: Creating Your custom Image

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.

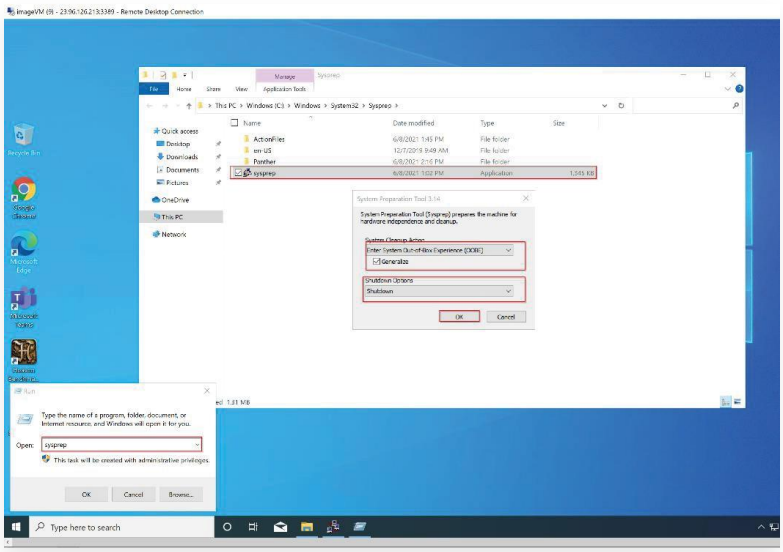


2. Sign in to imageVM with local admin credentials. For your convenience, the Image VM has been configured to allow connections via RDP.

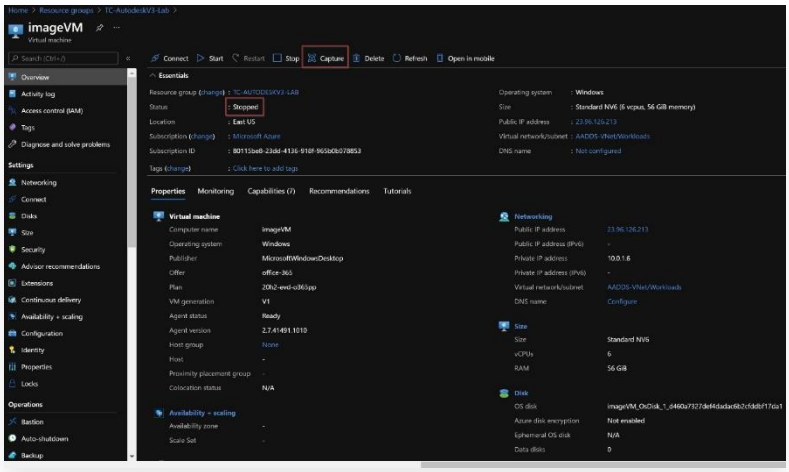


3. Configure the virtual machine with any LOB applications, Group Policy Settings, or other configurations.
   Note: the FSLogix Agent has been configured for you already, and the VHD locations have been mapped to the Click-to-Run storage account. If you enabled the teams install during deployment, this will be configured on imageVM as well.

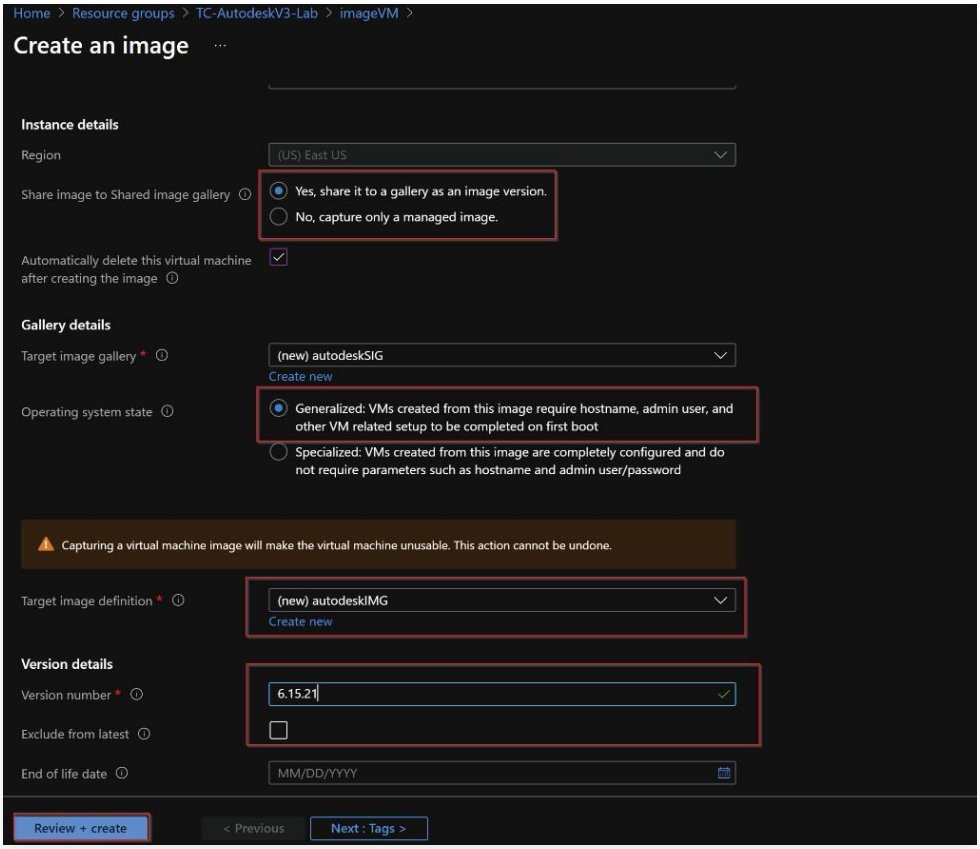
4. When finished Making your configurations, you must run sysprep on imageVM. This can be done by selecting **start->Run->Sysprep**. Open the Sysprep application and select **'Enter System Out-of-Box-Experience (OOBE)'** and select 'Generalize'. Under shutdown options select 'Shutdown'. After clicking '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'.



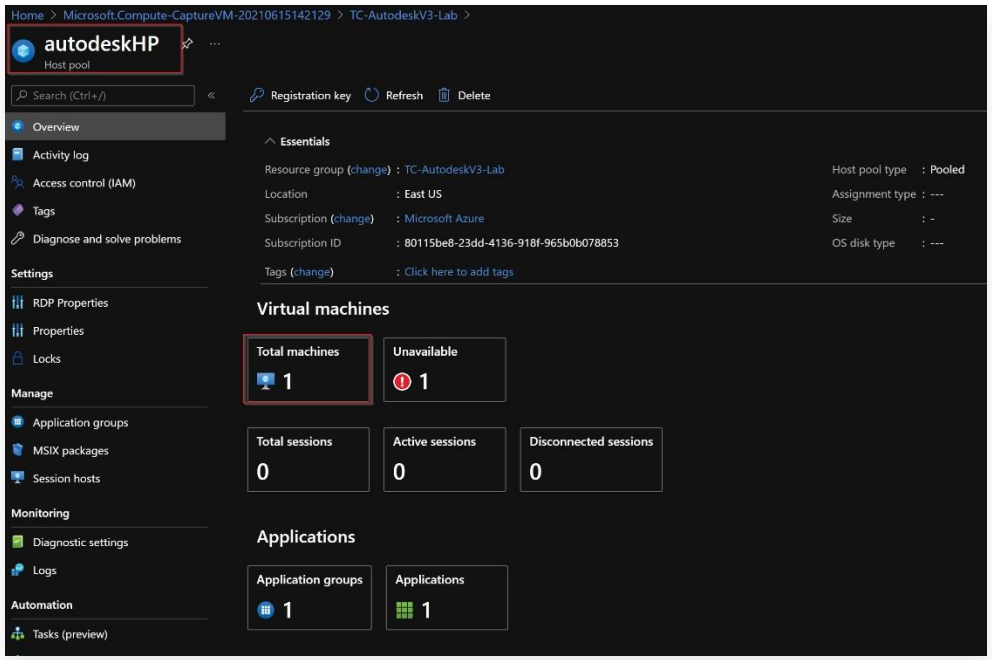
6. Follow the prompts to create the image. We recommend creating a Shared Image Galley during this step to simplify Image management and updates. Make sure the OS state selected is set to 'Generalized.' When you have finished specifying your inputs, select 'Review and Create' to begin the image creation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



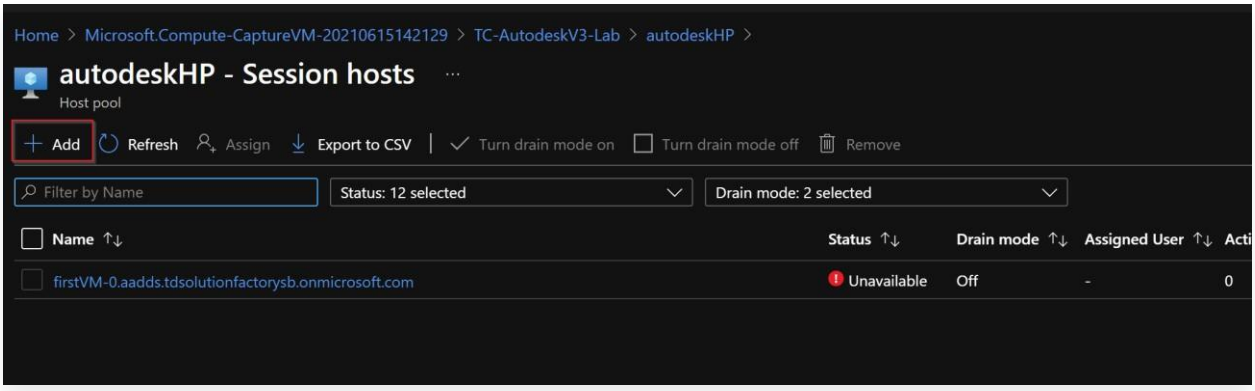
7. You will then see the Shared Image Gallery and associated Image versions appear in your AVD resource group! This managed image may be used to update your existing AVD Host Pool.

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

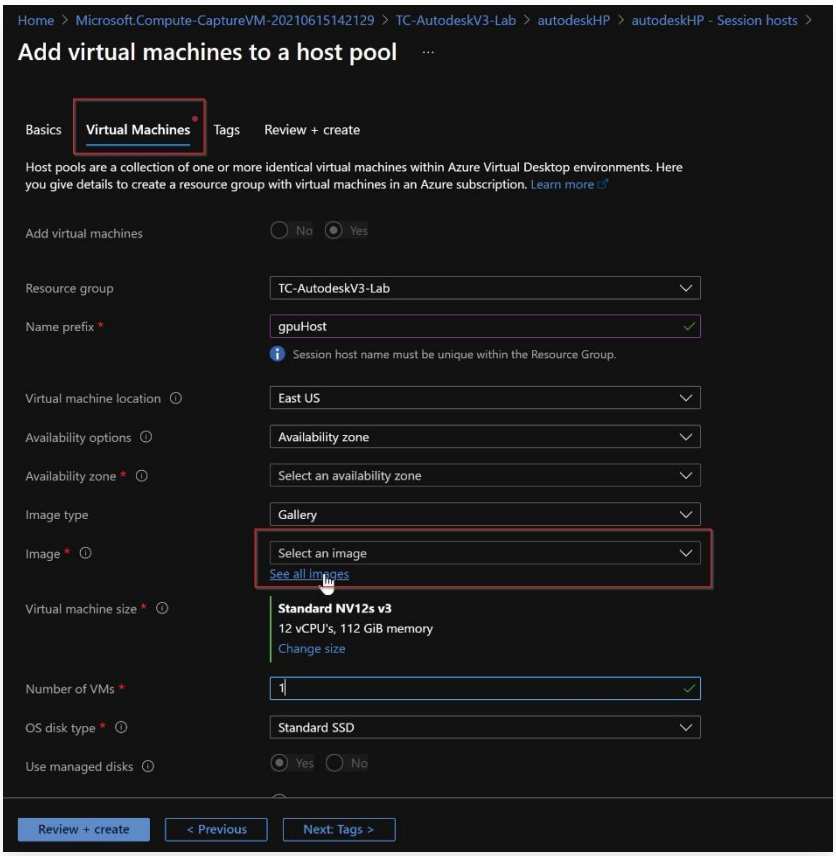
1. To update your AVD Host Pool with your newly created custom image, navigate to your Host Pool resource and select 'Total Machines'.



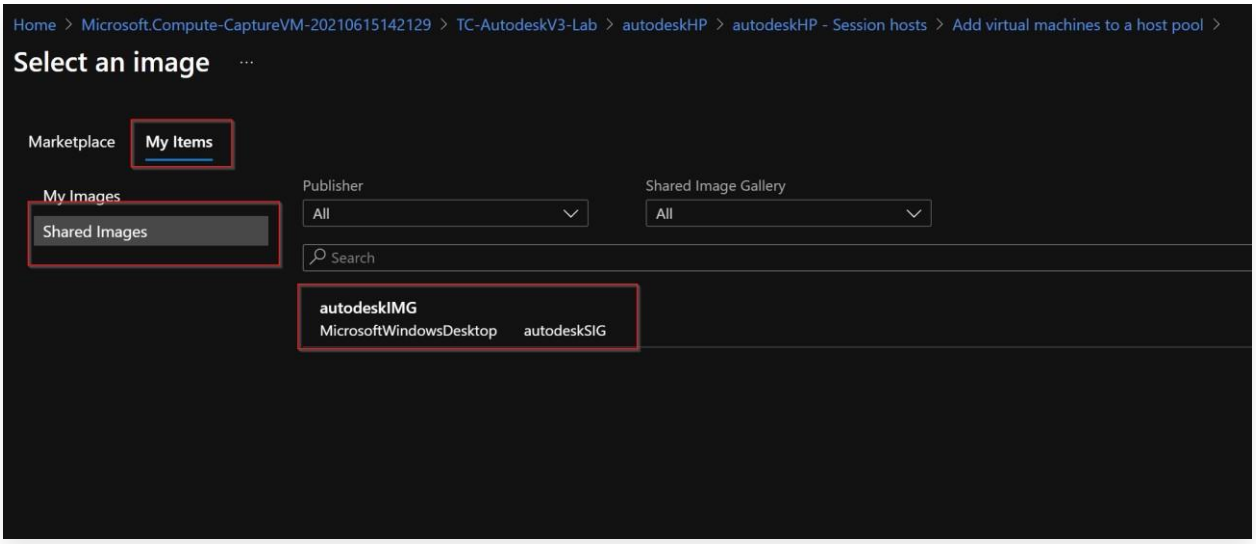
Select 'Add' from your Host Pool settings:



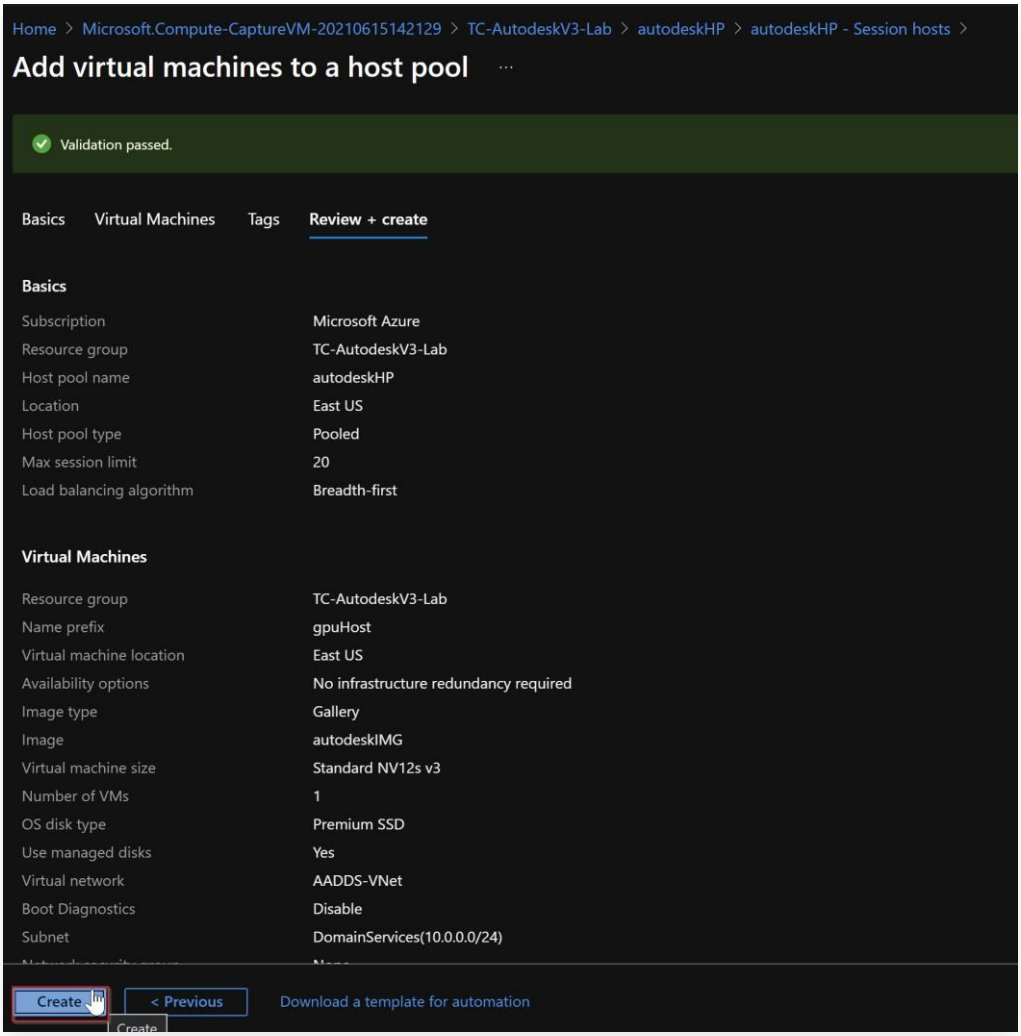
2. Specify your session host name, AD domain credentials, Region ETC. To use your newly created Image, select 'See All Images' from the 'Image' parameter.



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



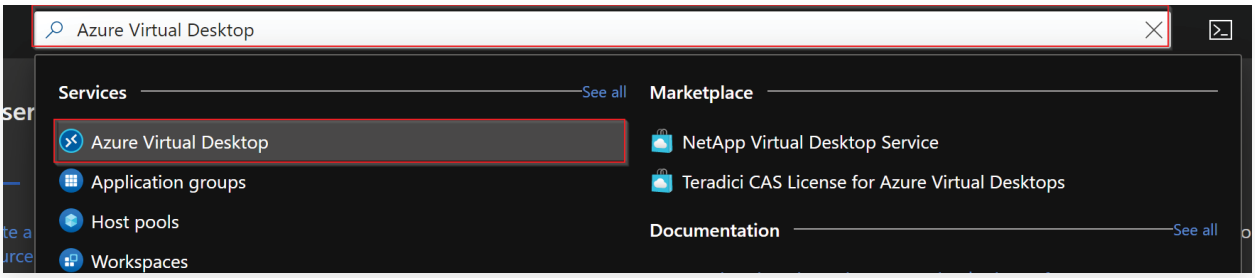
4. Select ‘Create’ to add your session host to the AVD Host Pool.



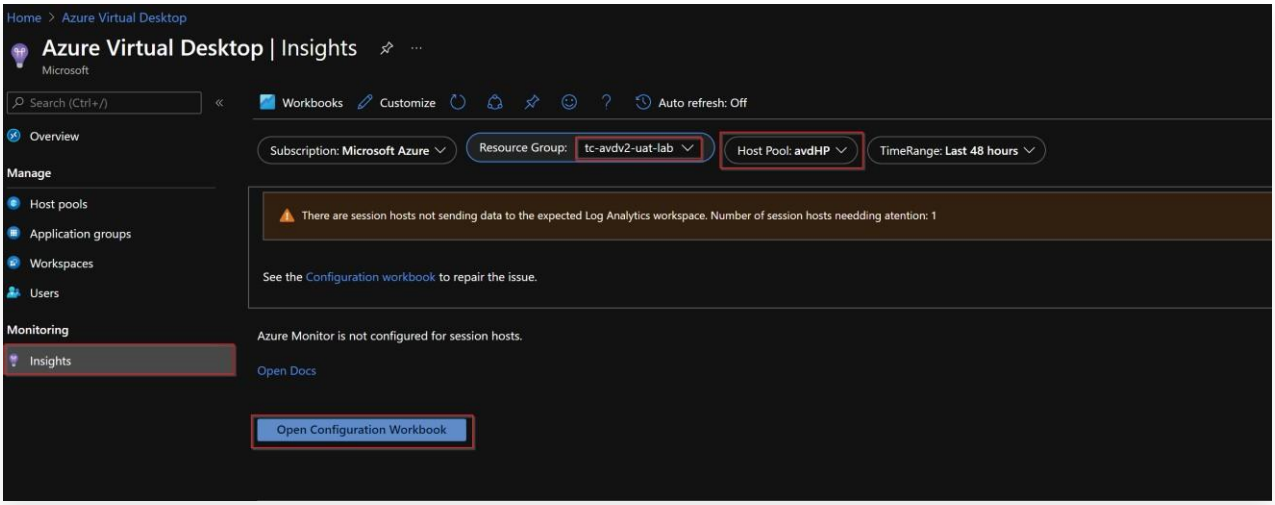
AVD Click-to-Run: Enabling Insights for your AVD Deployment

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:

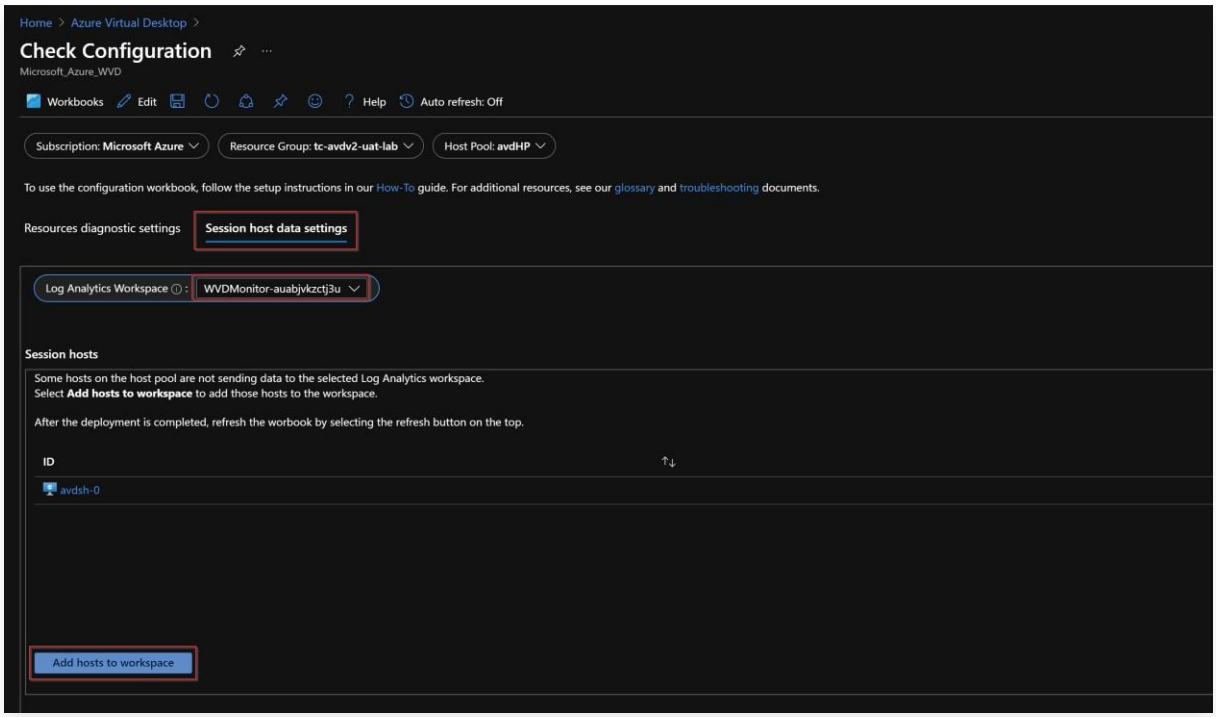
1. Navigate to the AVD management portal within Azure. This can be found by searching for 'Azure Virtual Desktop in the portal.



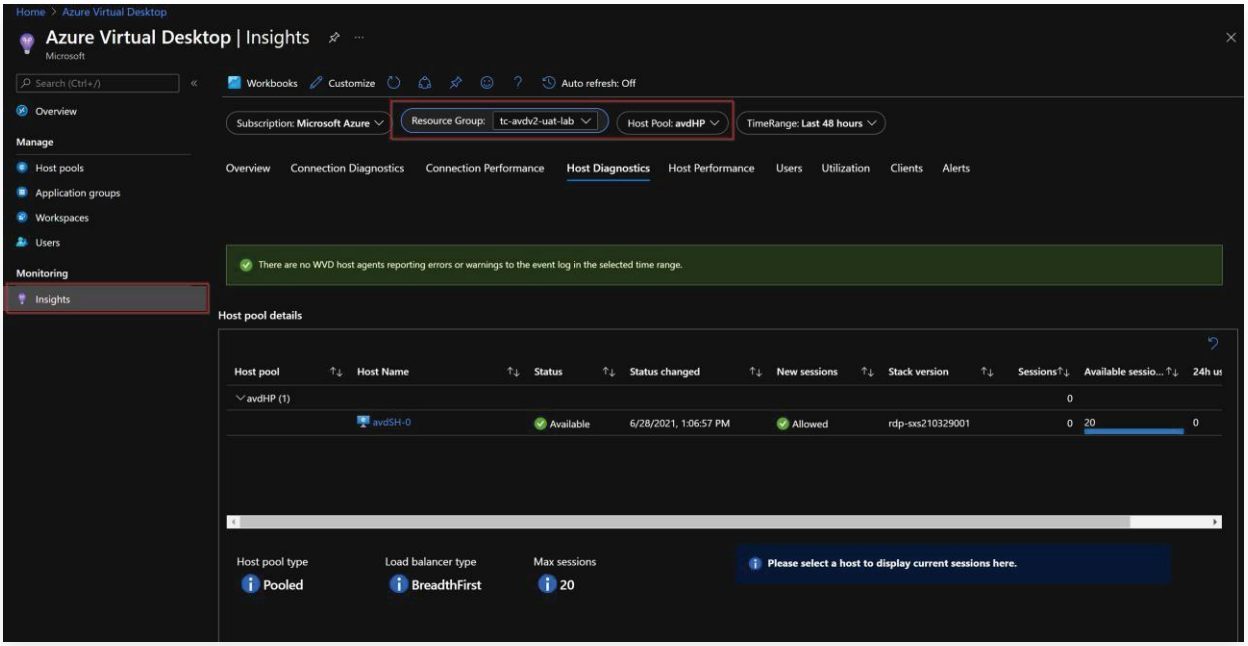
2. Select Insights. From here select your AVD Host Pool and Resource Group from the drop-down. You should see an alert that there are session hosts that need to be configured. Select 'Open Configuration Workbook'.



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.



TD SYNNEX

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!