chawn
+44 (0)121 314 2253
info@chawn.com

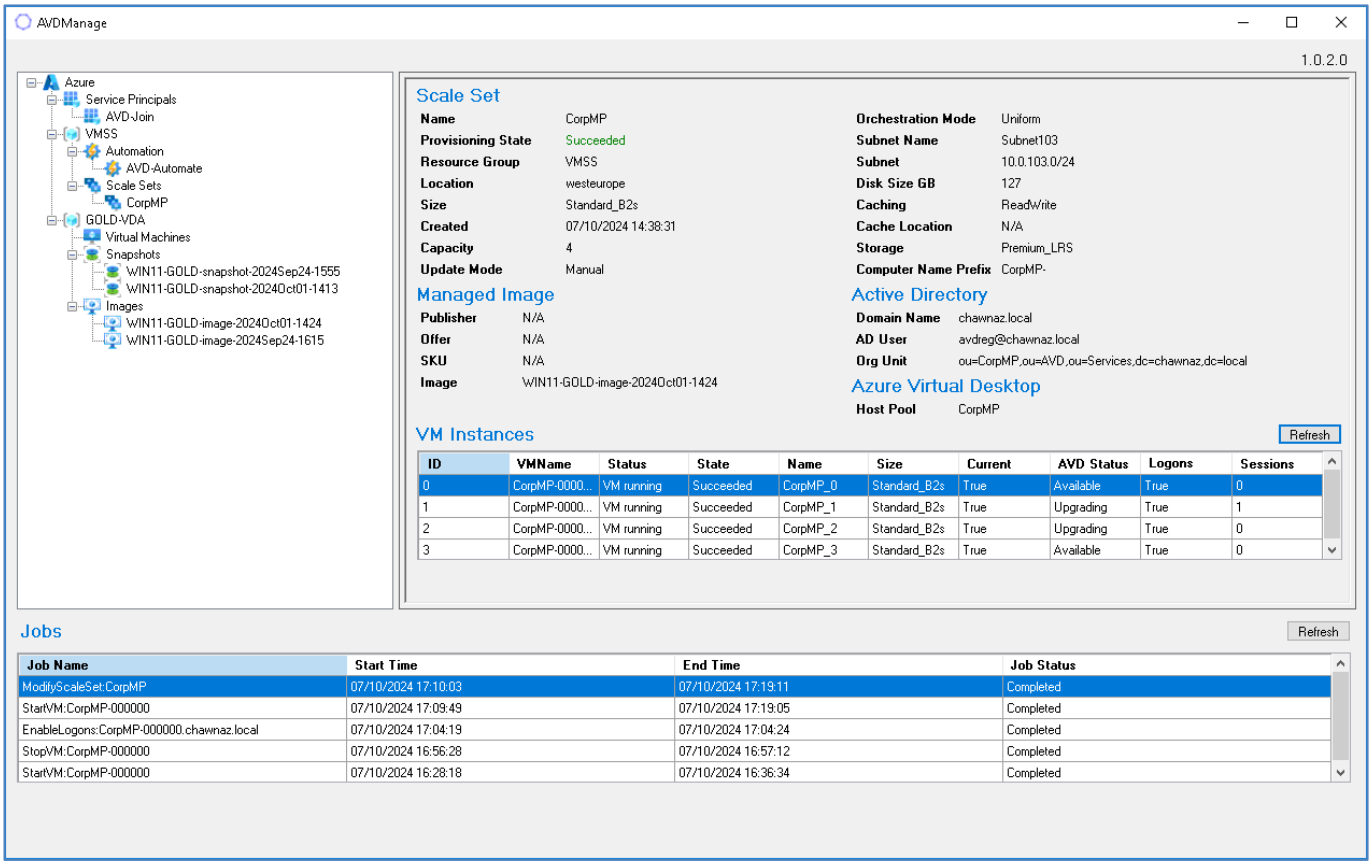
Desktops & Applications Virtualisation & Integration

AVDManage 1.0.2.0 Administration

chawn
+44 (0)121 314 2253
info@chawn.com

Document Details

Document Name	AVDManage 1.0.2.0 Administration
Author	DG – Chawn Limited
Version	1.0
Date	5th October 2024
Status	Final



Contents

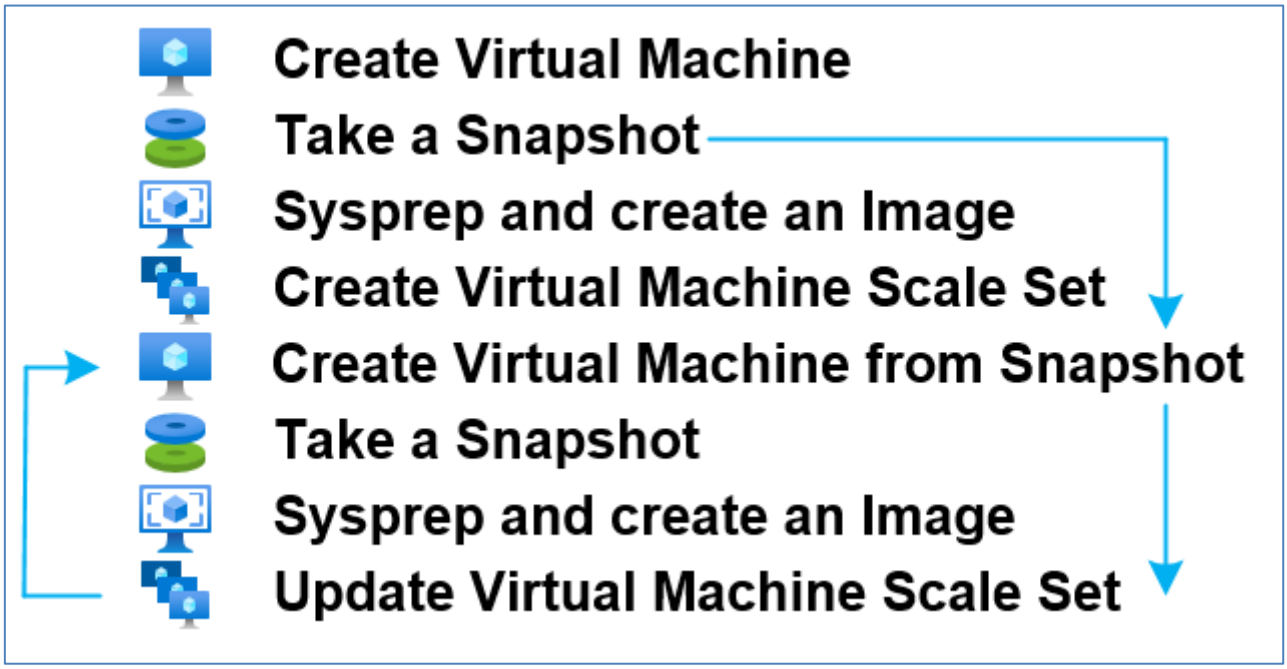
1. Introduction 6
2. Requirements 7
2.1 Operating System 7
2.2 Software 7
2.3 Azure 7
2.4 Azure Permissions 8
2.5 Microsoft Entra Permissions 8
2.6 Microsoft Active Directory 8
2.7 Virtual Machines 9
3. Getting Started 10
3.1 Create AVD-Admins Group 10
3.2 Resource Groups & Roles 10
3.3 Check AVDManage Requirements 11
3.4 Install AVDManage 13
3.4.1 Authentication 13
3.5 Configure AVDManage 14
3.6 Create a Service Principal – AVD-Join (Optional) 15
3.7 Create Automation Account – AVD-Automate (Optional) 17
4. Create (Master) VM 18
4.1 Modify the Master VM 20
4.2 Snapshot the Master VM 22
4.3 Sysprep the Master VM 23
4.4 Create Image of the Master VM 25
5. Create a Scale Set 26
6. Image Updates 29
6.1 Recreate the Master VM 29
6.2 Modify the Master VM 30
6.3 Snapshot the Master VM 31
6.4 Sysprep the Master VM 32
6.5 Create Image of the Master VM 33
7. Update a Scale Set 34
7.1 Create Update Runbook 36
7.2 Create Update Automation Task 38

8. Reference 40
8.1 Virtual Machines 40
8.1.1 Configuration 40
8.1.2 OS Disk Type: Persistent vs Ephemeral 40
8.1.3 Menu Actions 41
8.2 Virtual Machine Scale Sets 42
8.2.1 Orchestration Mode 42
8.2.2 Update Mode 42
8.2.3 Load Balancing 42
8.2.4 OS Disk Type: Persistent vs Ephemeral 42
8.2.5 Menu Actions 44
8.3 AVD-Join Service Principal 45
8.3.1 Menu Actions 46
8.4 AVD-Automate Automation Account 47
8.4.1 Menu Actions 47
8.5 Snapshots 47
8.5.1 Menu Actions 47
8.6 Images 48
8.6.1 Menu Actions 48
8.7 PowerShell 49
8.7.1 Module Installation for AVDManage 49
8.7.2 Module Installation for AVD-Join (Master VM) 49
8.8 Login Issues 50
8.8.1 Browser 50
8.8.2 Authentication Error 50
8.8.3 Authenticate Manually 50
8.8.4 Update PowerShell Modules 50
8.8.5 Disable Web Account Manager 50
8.8.6 Set Default Subscription 50
8.8.7 Corrupt PowerShell / Azure Profile 51

Standardise and Simplify Azure Virtual Desktop Image Management

- Create Virtual Machines, Snapshots & Images
- Create Uniform Virtual Machine Scale Sets
- Deploy, Re-Deploy, Re-Image, Update & Rollback Virtual Machine Scale Sets using Managed Images or Azure Gallery Images
- Scale Up / Down – Change VM Size
- Scale In / Out – Adjust Virtual Machine Scale Set VM instances
- Join Active Directory Domain during deployment / update
- **AVD-Join** - Join AVD Host Pool during deployment / update
- **AVD-Automate** – Schedule tasks for planned maintenance.
  E.g. Image Updates, Power Management, Scheduled Reboot

Consistent repeatable process for Image Continuity



1. Introduction

AVDManage leverages Microsoft Azure Virtual Machine Scale Sets to deploy, update and rollback Windows images to multiple uniform Virtual Machine instances.

Virtual Machine instances retain their machine identity when updating, re-imaging, re-deploying and rolling back. (Windows computername, Active Directory computername, AVD Session Host name)

Up to 1000 virtual machines may be deployed or updated from Azure Gallery Images or up to 600 virtual machines from a customised Windows Managed Image subject to Azure subscription quota and limits.

AVD-Join enables Scale Set Virtual Machine instances to join an Active Directory domain and an Azure Virtual Desktop host pool when deploying or updating Virtual Machine Scale Sets.

AVD-Automate enables tasks to be scheduled and assigned to Virtual Machine Scale Sets to Automate Tasks such as updating, restarting or power management.

AVDManage provides a simplified and consistent methodology and process for creating, updating, and deploying customised Windows images to Virtual Machine Scale Sets.

1. Create a Windows Master VM from an Azure Gallery Image
2. Configure the Master Image based on user desktop requirements
3. Create a Snapshot of the Master VM
4. Sysprep the Master VM
5. Create an Image from the sysprepped Master VM (master VM is deleted)
6. Deploy the Image to a new or existing Virtual Machine Scale Set

The Master VM can be recreated from the Snapshot that was created in step 3 enabling image control and consistency and continuity of future image updates.

VMs may be updated manually, or scheduled to update during planned maintenance windows using Azure Automation and **AVD-Automate**.

AVDManage can provision Virtual Machine Scale Sets in Automatic update mode however this is unlikely to be appropriate for an AVD host pool as user sessions would be interrupted during unscheduled automatic updates. It is recommended that Virtual Machine Scale Sets are deployed in Manual mode and **AVD-Automate** is used to deploy out-of-hours updates.

AVDManage supports Azure Virtual Desktop environments however **AVD-Join** and **AVD-Automate** are optional features therefore AVDManage may be used to manage image deployment to Virtual Machine Scale Sets for almost any Windows based image.

2. Requirements

2.1 Operating System

- Microsoft Windows 10 build 1607 or higher

2.2 Software

- Microsoft .Net Framework 4.7.2
- Microsoft Windows PowerShell 5.1 or higher
- Microsoft Windows PowerShell Modules
  - Az.Accounts 3.03+
  - Az.Compute 8.2.0+
  - Az.DesktopVirtualization 4.3.1+
  - Az.Resources 7.3.0
  - Az.Automation 1.10.0
  - Az.Network 7.8.1

2.3 Azure

- An Azure Tenant and Microsoft Entra Directory
- An Azure Subscription
- Azure Resource Groups for:
  - Master VM, Snapshots and Images
  - Virtual Machine Scale Sets and Automation Account
  - AVD Host pools and Application Groups
- Azure Virtual Network and Subnet(s)
- Azure Virtual Desktop Provider, Workspace, Host Pool, Application Group
- Sufficient Azure quota to deploy the intended number of VMs
- All Azure Objects in the AVDManage configuration must be in the same Azure location

Network access (Port 443) to:

- management.azure.com
- login.microsoftonline.com
- portal.azure.com
- www.powershellgallery.com

2.4 Azure Permissions

(Broad Scope Permissions)

- Contributor permissions to all in-scope Resource Groups
- Network Contributor Permissions to the Virtual Network

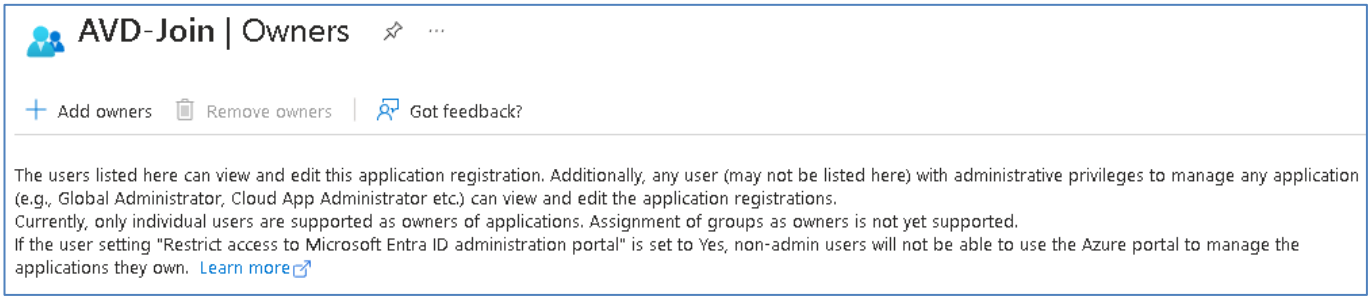
(Narrow Scope Permissions)

Resource	Permission
Scale Sets Resource Group	Automation Contributor Virtual Machine Contributor
Virtual Machines Resource Group	Virtual Machine Contributor Disk Snapshot Contributor Microsoft.Compute/images/write Microsoft.Compute/images/read Microsoft.Compute/images/delete
AVD Resource Group	Desktop Virtualization Contributor
Virtual Network Resource Group	Microsoft.Resources/subscriptions/resourceGroups/read Microsoft.Network/virtualNetworks/read Microsoft.Network/virtualNetworks/subnets/join

2.5 Microsoft Entra Permissions

- Application Administrator (Application.ReadWrite.All) – to create the **AVD-Join** Service Principal
- Owner Role of the AVD Host Pool Resource Group to assign the 'Desktop Virtualization Contributor' role to **AVD-Join** and **AVD-Automate**
- Owner Role of the VMSS Resource Group to assign the 'Virtual Machine Contributor' role to **AVD-Automate**

Virtual desktop admins may be assigned the Owner role to the 'App Registration' after creation to administer the **AVD-Join** Service Principal on a per user basis.



2.6 Microsoft Active Directory

- Active Directory Domain
- Dedicated organisational unit for Master VM
- Dedicated organisational unit for each AVD Host Pool
- AD account to join VMs to the domain

2.7 Virtual Machines

If VMs will be joined to an AVD Host Pool with **AVD-Join**, install the following PowerShell Modules on the Master VM:

- Az.Accounts
- Az.DesktopVirtualization

Virtual Machines require network access to:

- The **AVDJoin.ps1** PowerShell Script

https://raw.githubusercontent.com/ChawnLimited/AVDManage/refs/heads/main/AVDJoin.ps1

- Installation media for the Microsoft Remote Desktop Service Infrastructure Agent and Boot Agent

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWrmXv

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWrxrH

AVDJoin.ps1 and Microsoft Remote Desktop Service source media are downloaded by Virtual Machines when deploying and updating.

3. Getting Started

The user performing these tasks should be an **Azure Subscription Owner** and an **Entra Global Administrator** to create:

- An Azure Group named **AVD-Admins**
- Resource Groups
- Service Principal **AVD-Join** and assign the **Desktop Virtualization Contributor** role to the AVD Resource Group
- Automation Account **AVD-Automate** and assign **Desktop Virtualization Contributor** role to the AVD Resource Group, and the **Virtual Machine Contributor** role to the VMSS Resource Group.

3.1 Create AVD-Admins Group

The **AVD-Admins** group may be synced from an Active Directory Domain using Microsoft Entra Connect, or manually created in Microsoft Entra.

Add required members to the **AVD-Admins** group.

3.2 Resource Groups & Roles

Create the following Resource Groups and assign Roles to the **AVD-Admins** group.

Suggested Name	Purpose	AVD-Admins Roles
VMSS	Contains Virtual Machine Scale Sets and **AVD-Automate** Automation Account	Virtual Machine Contributor Automation Contributor
AVD	Contains AVD Host Pools, Application Groups and WorkSpaces	Desktop Virtualization Contributor
GOLD-VDA	Contains Master VMs, Snapshots and Images	Virtual Machine Contributor Disk Snapshot Contributor Image Contributor ☺

☺ You will need to create a Custom Role named **Image Contributor** with the following permissions:

- Microsoft.Compute/images/write
- Microsoft.Compute/images/read
- Microsoft.Compute/images/delete

AVD-Admins will require permissions to join VMs to a Virtual Subnet.

Create a Custom Role named **Network Joiner** with the following permissions.

- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/read
- Microsoft.Network/virtualNetworks/subnets/join/action

Assign the **Network Joiner** custom role to **AVD-Admins** on the Resource Group containing your Virtual Network(s).

3.3 Check AVDManage Requirements

The user performing this task must be a Windows local administrator.

Open PowerShell as Administrator

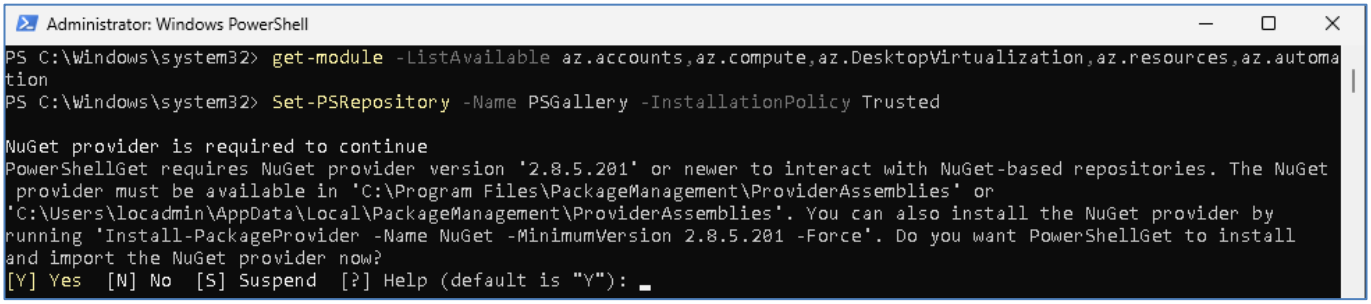
Run

```
get-module -ListAvailable
az.accounts,az.compute,az.DesktopVirtualization,az.resources,az.automation,az.network
```

If no modules are returned then run

```
Set-PSRepository -Name PSGallery -InstallationPolicy Trusted
```

If prompted to install the the Nuget Provider, type Y



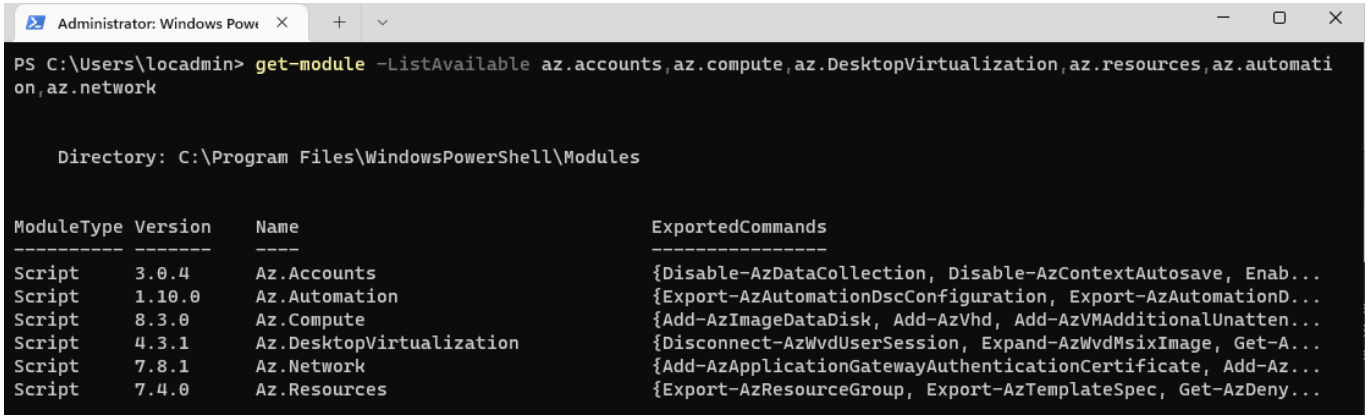
After NuGet is installed, run

```
install-module
az.accounts,az.compute,az.DesktopVirtualization,az.resources,az.automation,az.network
```

Re-run

```
get-module -ListAvailable
az.accounts,az.compute,az.DesktopVirtualization,az.resources,az.automation,az.network
```

You should see all six required modules.

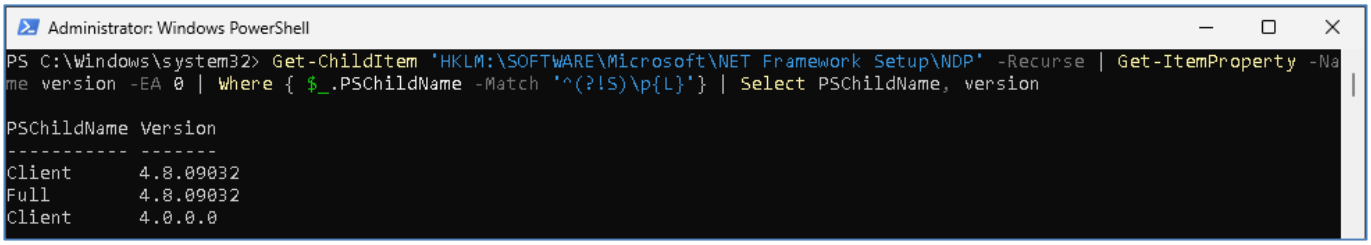


Check the .Net Framework Version

Run

```
Get-ChildItem 'HKLM:\SOFTWARE\Microsoft\NET Framework Setup\NDP' -Recurse | Get-ItemProperty -Name version -EA 0 | Where { $_.PSChildName -Match '^(?!S)\p{L}'} | Select PSChildName, version
```

The output should be similar to below. Check that the .Net Framework Version is 4.72 or higher.



3.4 Install AVDManage

- Download AVDManage from www.chawn.com/downloads/AVDManage.zip
- Extract the MSI installer from the zip file.
- Install AVDManage.msi as an Administrator

3.4.1 Authentication

AVDManage will use your current Azure Credentials to authenticate.
If you are not authenticated to Azure, in PowerShell run **Connect-AzAccount** and complete the authentication process and then launch AVDManage.

If you would prefer to specify your credentials every time you launch AVDManage then you need to disable Web Account Manager when authenticating to Azure.

In PowerShell, run

Update-AzConfig -EnableLoginByWam $False

This will enforce browser authentication instead of using Web Account Manager. This is helpful for users who need to logon to multiple tenants. When AVDManage is launched, the default browser opens and presents the Azure authentication dialog.

3.5 Configure AVDManage

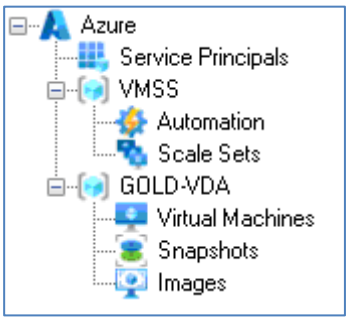
Authenticate to Azure as an Azure Subscription Owner and an Entra Global Administrator

Configure AVDManage

- Provide a Config Name
- Select the target Azure Tenant
- Select the target Azure Subscription
- Select the target Azure Location
- Select the Resource Group for Virtual Machine Scale Sets and the Automation Account
- Select the Resource Group for the Master VM(s), Snapshots and Images
- Select the Resource Group that contains your AVD host pools – If you do not wish to use **AVD-Join**, just select the Master VM Resource Group

Save the configuration file.

AVDManage will open and display the following items.



Service Principals - This is a container for **AVD-Join** which joins VMs to AVD Host Pools

<ResourceGroupName> - VMSS - Resource Group containing:

Automation - A container for the Automation account.
Scale Sets - A container for the Virtual Machine Scale Sets.

<ResourceGroupName> - GOLD-VDA - Resource Group containing:

Virtual Machines - A container for Master VM Virtual Machines
Snapshots - A container for Master VM snapshots
Images - A containers for Master VM images.

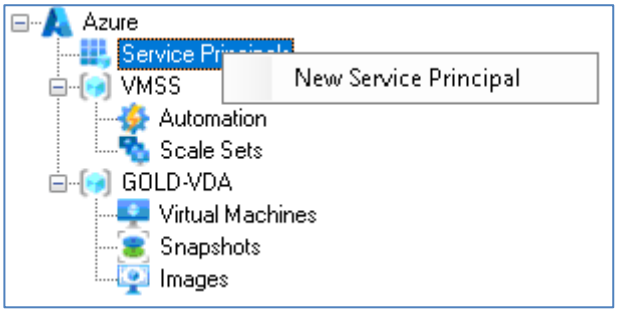
3.6 Create a Service Principal – AVD-Join (Optional)

If you want to join VMs to an AVD host pool, you will need to create an Azure Service Principal.

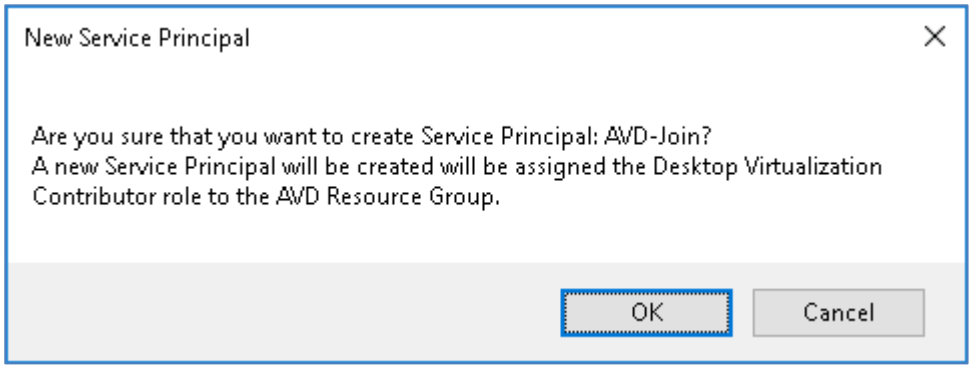
The Azure Service Principal is named **AVD-Join**.

AVD-Join is assigned the *Desktop Virtualization Contributor* role to the Resource Group containing AVD Host Pools. This enables **AVD-Join** to join and remove Session Hosts from the AVD Host Pools when deploying, or updating Virtual Machine Scale Sets.

Right click the Service Principals node and select **New Service Principal**

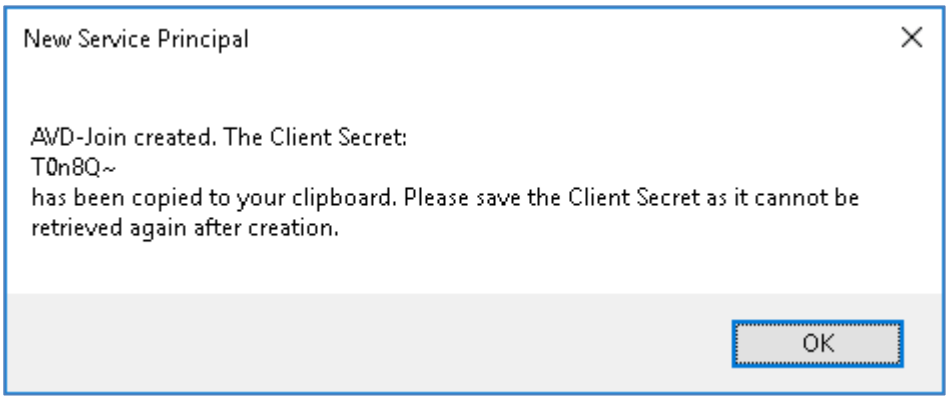


Confirm that you want to create **AVD-Join**

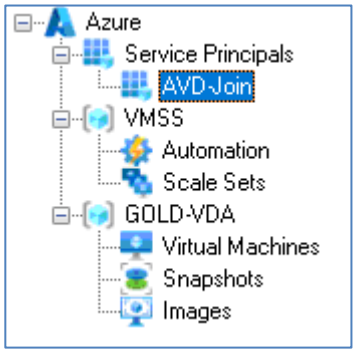


A confirmation message is displayed and the Client Secret is placed onto the clipboard.

Paste the Client Secret into a text file for later use when configuring Scale Sets.



AVD-Join is created.



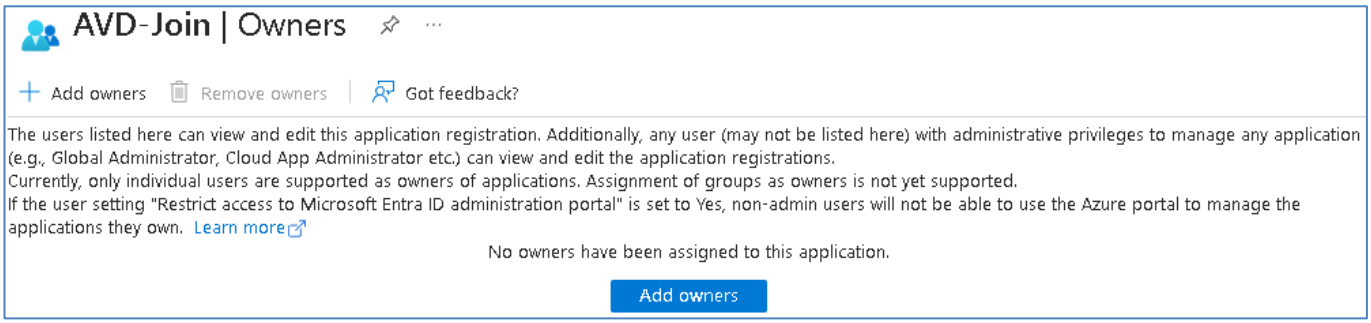
The AppID and Client Secret will be required when creating Scale Sets with **AVD-Join**.

The Client Secret will expire after 12 months. You can reset the Client Secret at any time however you must update all Scale Sets with the new Client Secret.

AVDManage users must be *Owners* of the **AVD-Join** App Registration in Microsoft Entra to reset the Client Secret.

- Locate the **AVD-Join** App Registration in the Entra portal
- Select Owners in the left pane

You cannot add the **AVD-Admins** Entra Group. Only named users can currently be assigned as *Owners*.

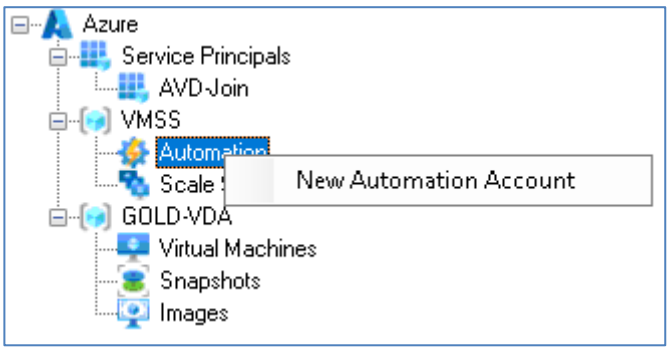


- Add required owners

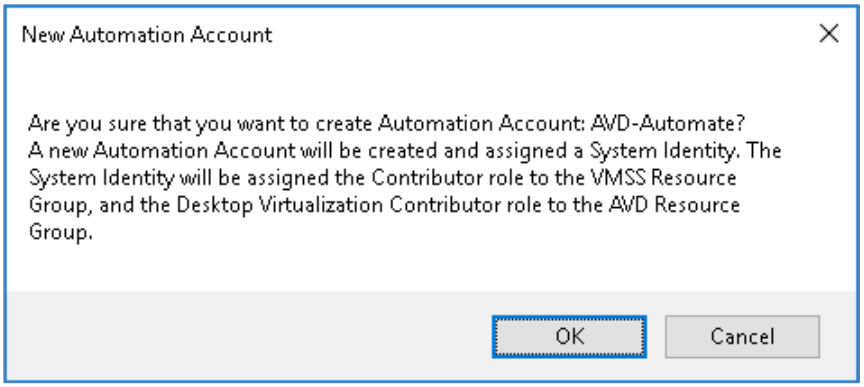
3.7 Create Automation Account – AVD-Automate (Optional)

An Automation Account may be used to run PowerShell scripts at specific times to Automate Tasks such as updating, restarting or power management of Virtual Machine Scale Sets.

Right Click Automation and select New Automation Account.

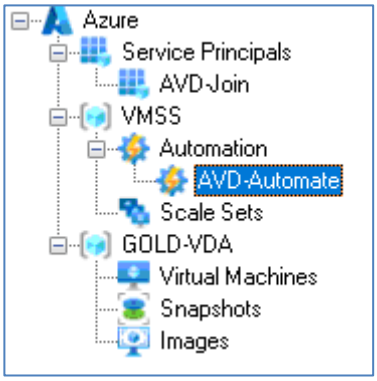


You will be asked to confirm that you want to create an Automation Account named AVD-Automate.



The AVD-Automate Automation Account will be created and assigned a System Identity.

The System Identity will be assigned the *Virtual Machine Contributor* role to the Resource Group containing Virtual Machine Scale Sets, and the *Desktop Virtualization Contributor* role to the Resource Group containing AVD Host Pools.



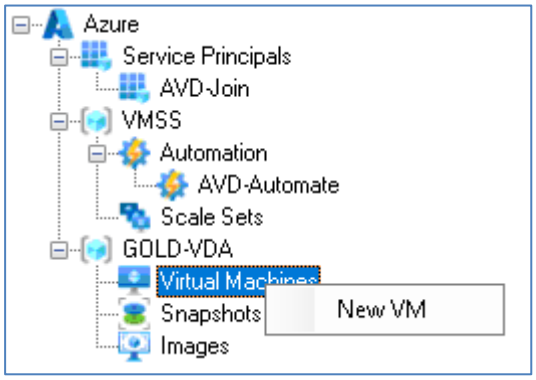
Configuration Complete. **AVD-Admins** can now use all features of AVDManage.

You can distribute the config file to **AVD-Admins**, or they can create their own config file using identical parameters.

4. Create (Master) VM

The user performing these tasks should be a member of **AVD-Admins**.

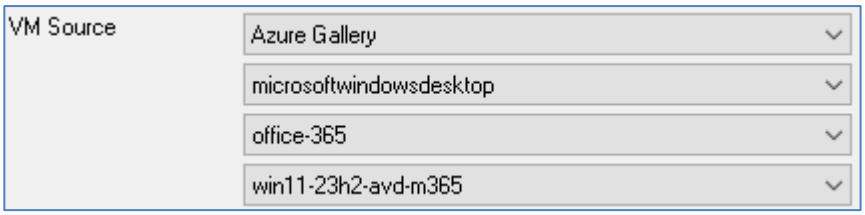
Right click Virtual Machines and select New VM.



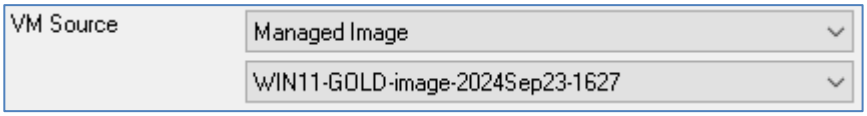
Supply parameters for the following properties.

VM Source

This can be either an Azure Gallery Image,



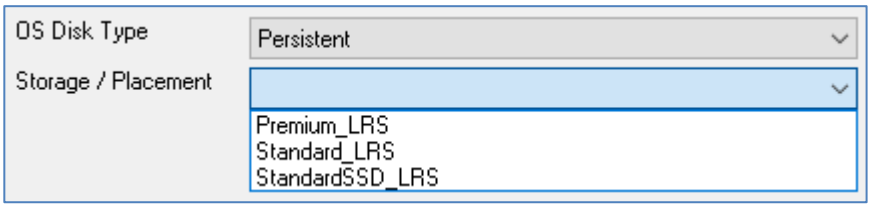
or a Managed Image.



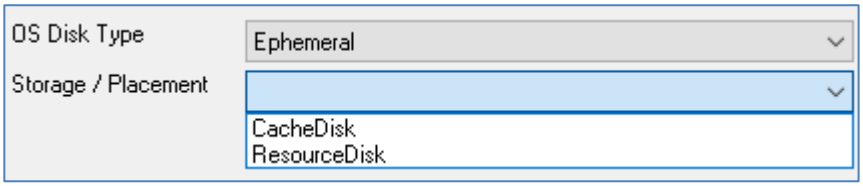
It is recommended that the Master VM is created from an Azure Gallery Image as Microsoft does not recommend deploying a Master VM from an image that has been previously sysprepped.

OS Disk Type

This can either be Persistent



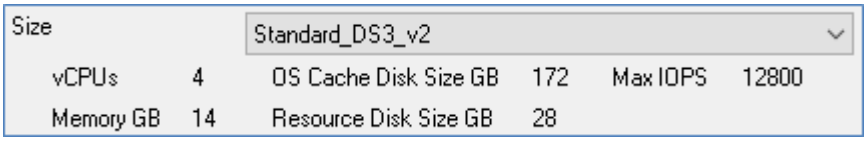
or Ephemeral.



The Master VM is must be created using a Persistent OS Disk as VMs with Ephemeral OS Disks cannot be shutdown, sysprepped or used to create Images.

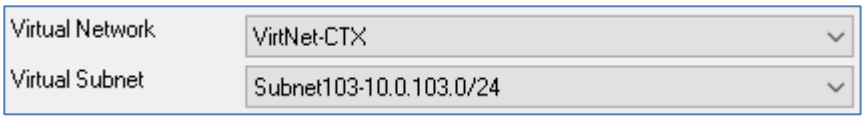
(VM) Size

The Size of the VM is filtered based on the OS Disk Type.



Virtual Network / Virtual Subnet

Select a Virtual Network and Virtual Subnet.



VM Name

Maximum length: 15 characters

VM names can only contain alphanumeric characters and hyphens.

Local Administrator

The name of the Local Administrator Account.

Maximum length: 20 characters

(Local Administrator) Password

Maximum length: 123 characters

The Local Administrator password must contain characters from at least three of the following categories. One upper case letter, one lower case letter, a number, one special character.

Make a note of the Local Administrator name and password. If the VM is recreated in the future from a snapshot, you will need the same credentials to logon.

Join Active Directory Domain (Optional)

Domain Name: The name of the target Active Directory Domain

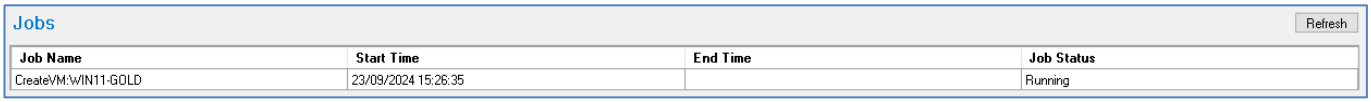
Org Unit: The name of the target AD Organizational Unit in LDAP format

AD User: The userPrincipalName of a user with sufficient privileges to join the VM to the Domain

Password: Password of the AD User

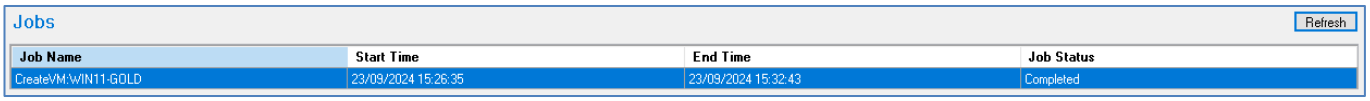
It is not necessary to join an Active Directory Domain however it may simplify access to application resources while building the Master VM. It is recommended that the Master VM is removed from the Active Directory Domain before running sysprep on the Master VM.

A new job will be created to deploy the Virtual Machine



You can click Refresh to update the status of the job and right click the job to view its details.

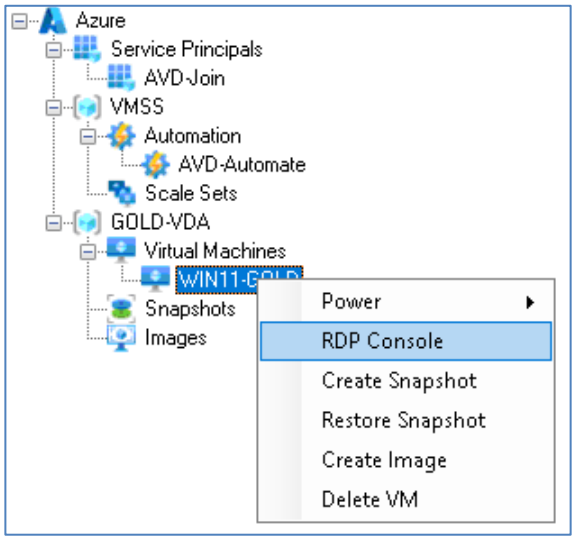
When the job is complete, the Job Status will change to Completed.



Estimated time to complete: 6 mins

4.1 Modify the Master VM

If you have a private network connection to Azure, you can RDP to the new VM.



Don't install the Remote Desktop Service Infrastructure Agent or Boot Agent. These will be deployed later with **AVD-Join** when deploying a Virtual Machine Scale Set.

If **AVD-Join** is required, install the following Windows PowerShell Modules on the Master VM to enable VMs to join an AVD host pool at startup:

- Az.Accounts
- Az.DesktopVirtualization

Standard modifications:

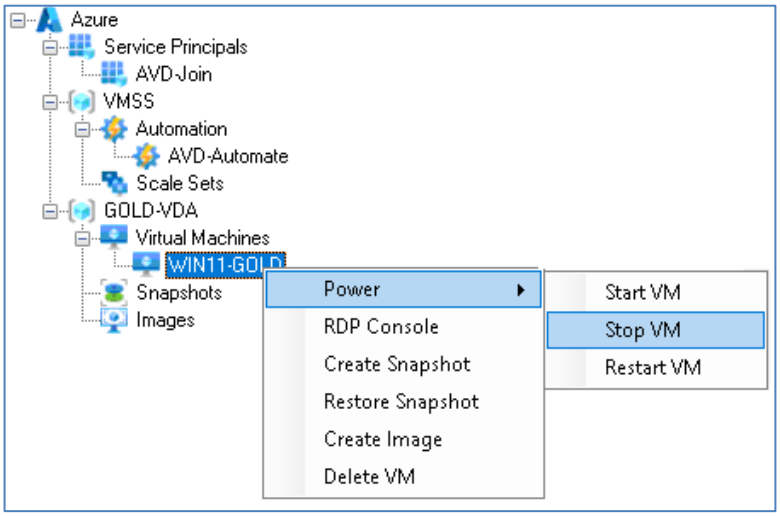
- Add / Remove required Applications and Features
- Remove unwanted Microsoft Store Apps
- Install required Language Packs
- Install all available Windows and Application updates
- Configure the Default User Profile
- Modify the All Users Start Menu
- Disable unnecessary Scheduled Tasks
- Disable unnecessary Services
- Enable required Services (Windows Search)
- Enable Firewall Rules (Domain Profile)
- Delete Temporary Files and Source Media on the OS Disk
- Apply known optimizations

Prevent Machine Password Changes

```
REG ADD
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters" /v
DisablePasswordChange /t REG_DWORD /d 1 /f
```

If a Master VM is domain joined, it will have a machine password which will change within a forty day window. If the domain joined Master VM is created from a snapshot in the future, it may have an old out-of-date machine password and fall out of the domain. Applying the registry setting above prevents this issue.

When you have made all required changes to the Master VM, shut the VM down using AVDManage so that the VM status is deallocated.



[Create an Azure Virtual Desktop golden image | Microsoft Learn]
[Prepare and customize a VHD image of Azure Virtual Desktop - Azure | Microsoft Learn]
[Recommended configuration for VDI desktops | Microsoft Learn]
[Prepare a Windows VHD to upload to Azure - Azure Virtual Machines | Microsoft Learn]
[(Azure) Virtual Desktop Optimization Tool now available - Microsoft Community Hub]

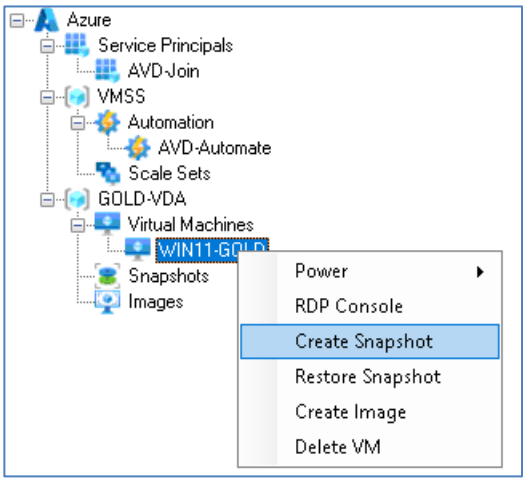
4.2 Snapshot the Master VM

A snapshot is required so that the Master VM can be recreated in the future in the same state as its last update.

After the snapshot has been created, the next step is to sysprep the Master VM which will render the Master VM unusable. Therefore the snapshot allows for the original VM to be recreated in the future.

Check the VM status is Deallocated.

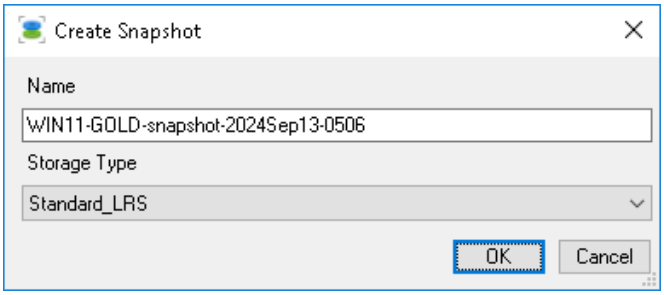
Right click the VM and select Create Snapshot



Name

Maximum length: 80 characters

The name is auto-generated based on the name of the VM and the current date / time. It may be modified. Snapshot names can only contain Alphanumeric characters, hyphens and underscores.

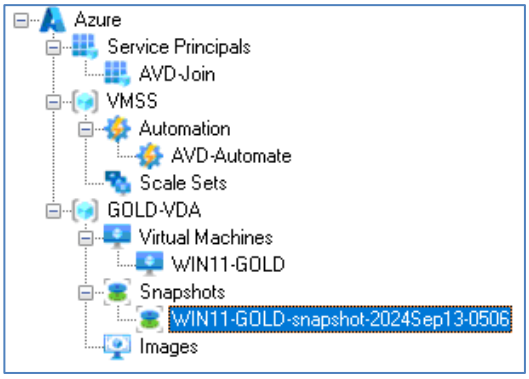


Storage

Select from

- Standard_LRS
- Premium_LRS
- Standard_ZRS

The new Snapshot is displayed under the Snapshots node.



Estimated time to complete: 10-20 seconds

4.3 Sysprep the Master VM

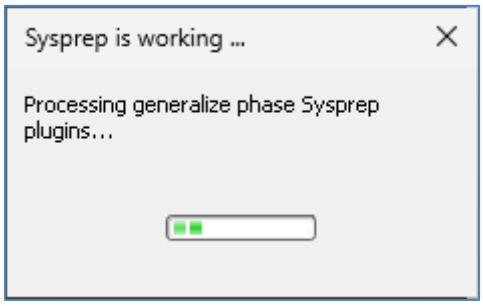
Start the VM.

When the VM is running, RDP to the new VM.

If the VM is joined to an Active Directory Domain, remove the VM from the Domain and restart.

Open a command prompt as Administrator and run:

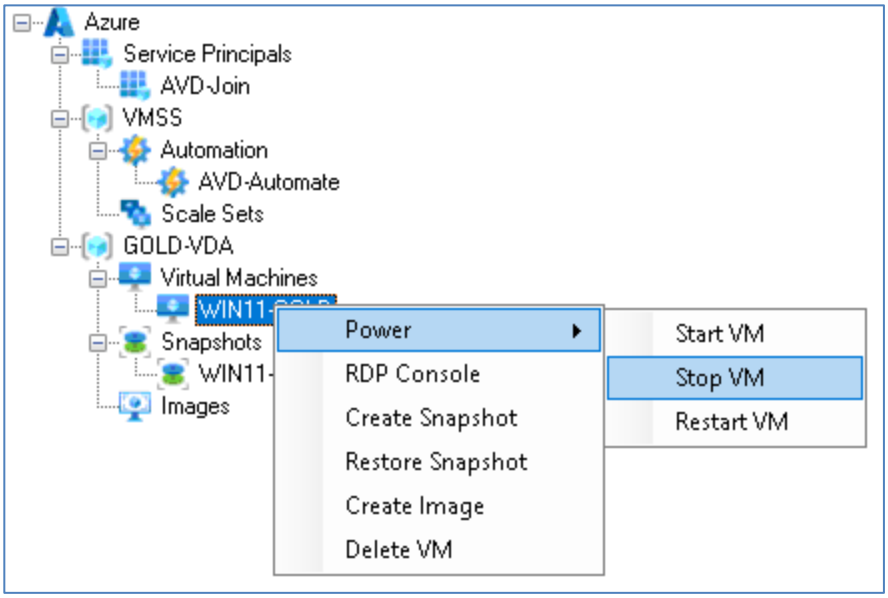
C:\Windows\System32\Sysprep\sysprep.exe /oobe /generalize /shutdown



After several minutes the VM will shut down.

After shutdown, the VM status will be stopped.

Use AVDManage to Stop the VM so that it is in a deallocated state.



It is recommended that a ***Seal Script*** is used to shut down and sysprep the VM. A seal script can perform tasks that affect the state of the VM.

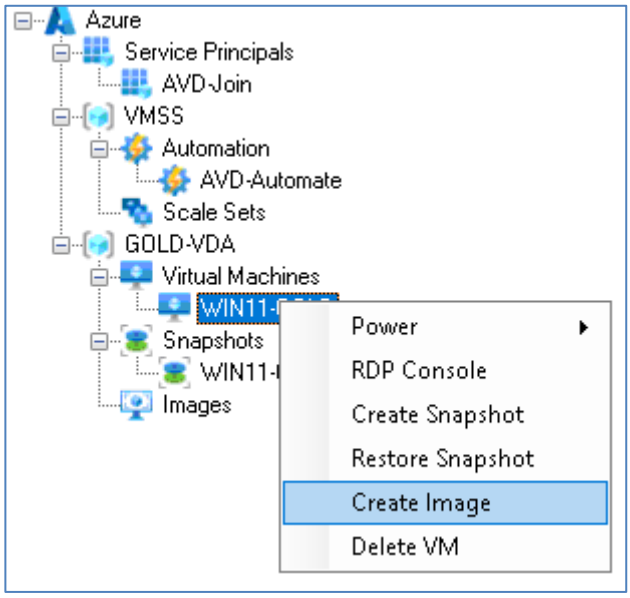
The example script below removes non-essential directories, clears the event logs and then runs sysprep.

```
# Clear folders
Remove-Item -Path C:\Packages\ -Recurse -Force -ErrorAction Ignore
Remove-Item -Path C:\WindowsAzure\Logs -Recurse -Force -ErrorAction Ignore
Stop-Service wuauserv -Force
Stop-Service bits -Force
Stop-Service msiserver -Force
Remove-Item -Path C:\Windows\SoftwareDistribution -Recurse -Force -ErrorAction Ignore
Remove-Item -Path C:\Windows\Panther -Recurse -Force -ErrorAction Ignore
#Clear Event Logs
wevtutil cl Application
wevtutil cl System
wevtutil cl Security
# Run Sysprep
C:\Windows\System32\Sysprep\sysprep.exe /oobe /generalize /shutdown
```

4.4 Create Image of the Master VM

Check the VM status is Deallocated.

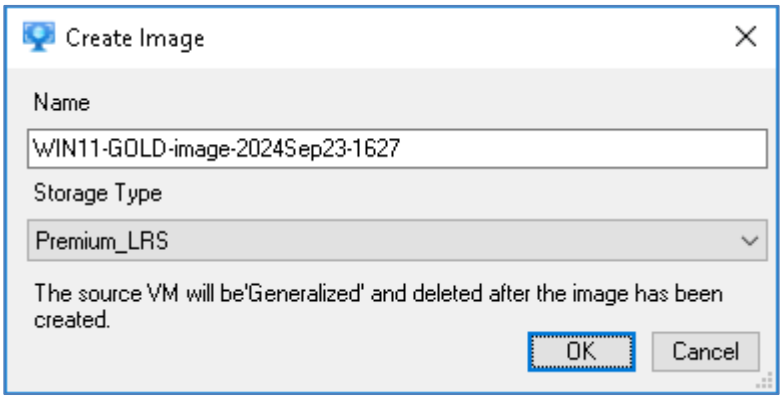
Right click the VM and select Create Image



Name

Maximum length: 80 characters

The name is auto-generated based on the name of the VM and the current date / time. It may be modified. Image names can only contain Alphanumeric characters, hyphens and underscores.



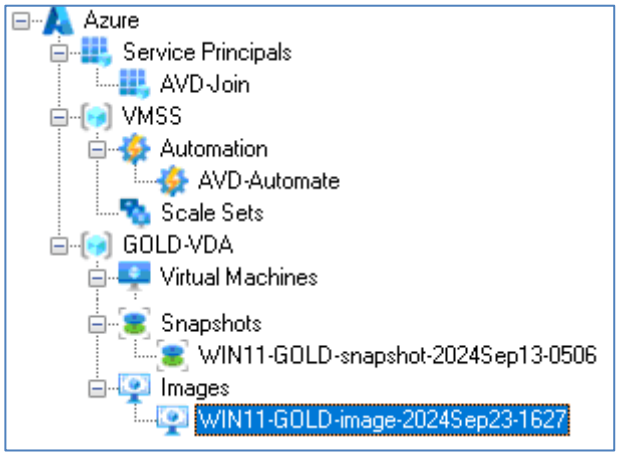
Storage

Select from

- Standard_LRS
- Premium_LRS
- Standard_ZRS

The VM will be marked as generalized before an Image is created and the VM is deleted.

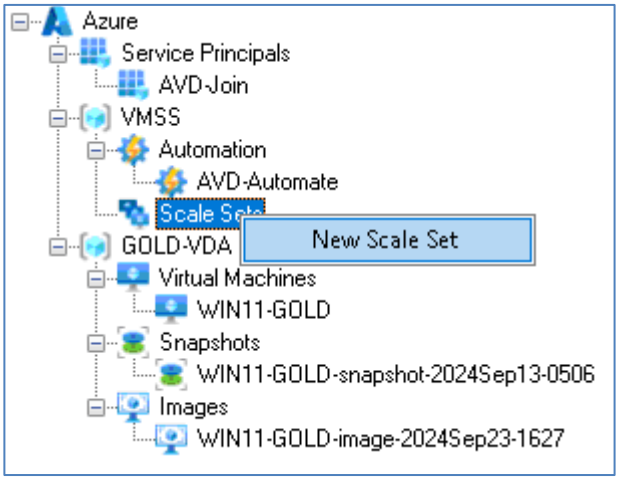
The new Image is displayed under the Images node.



Estimate time to complete: 60 seconds

5. Create a Scale Set

Right Click Scale Sets and select New Scale Set

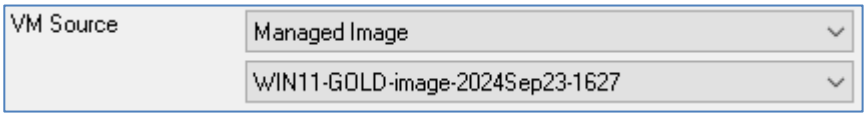


Supply parameters for the following properties.

VM Source

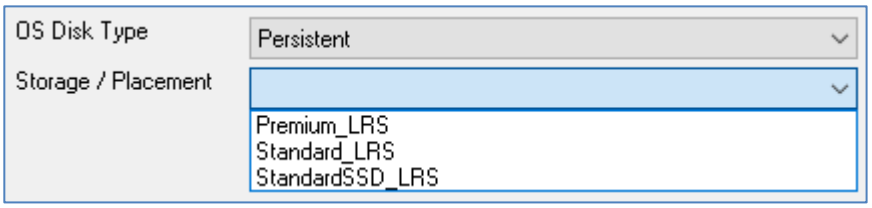
This can be either an Azure Gallery Image,

or a Managed Image.

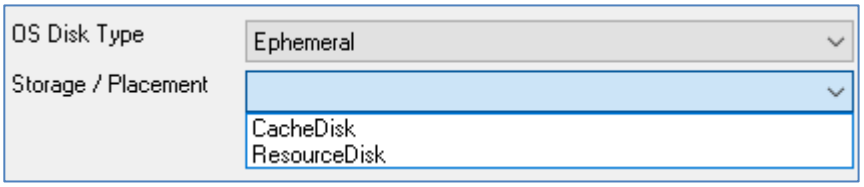


OS Disk Type

This can either be Persistent

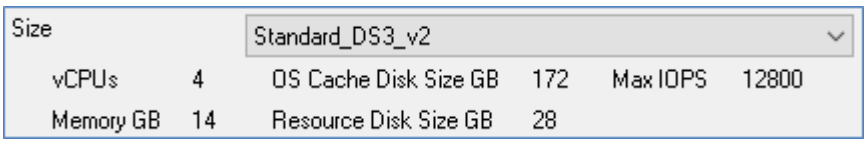


or [Ephemeral](#).



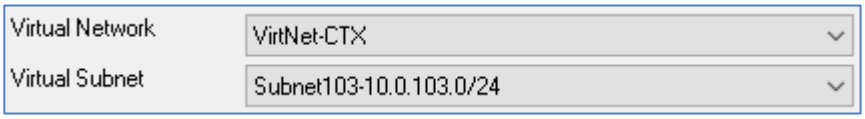
(VM) Size

The Size of the VM is filtered based on the OS Disk Type.



Virtual Network / Virtual Subnet

Select a Virtual Network and Virtual Subnet.



Scale Set Name

Maximum length: 15 characters

Scale Set names can only contain Alphanumeric characters and hyphens.

Orchestration Mode

This cannot be modified. All Scale Sets are deployed in Uniform mode.

VM Instances

Up to 1000 VMs may be created from an Azure Gallery Image.

Up to 600 VMs may be created from a Managed Image.

(Subject to Azure Subscription limits & quotas)

Update Mode

Manual mode is preferred for AVD Scale Sets so that updates and maintenance can be scheduled for appropriate times using an Automation Account.

Automatic mode is available however the scale set makes no guarantees about the order of virtual machines being brought down. The scale set might take down all virtual machines at the same time to perform upgrades.

VM Name Prefix

Maximum length: 9 characters

VM names can only contain alphanumeric characters and hyphens.

Local Administrator

The name of the Local Administrator Account.

Maximum length: 20 characters

(**Local Administrator) Password**

Maximum length: 123 characters

The Local Administrator password must contain characters from at least three of the following categories. One upper case letter, one lower case letter, a number, one special character.

Join Active Directory Domain (Optional)

Domain Name: The name of the target Active Directory Domain

Org Unit: The name of the target AD Organizational Unit in LDAP format

AD User: The userPrincipalName of a user with sufficient privileges to join the VM to the Domain

Password: Password of the AD User

Join AVD Host Pool (Optional)

You must have created the Service Principal **AVD-Join**. The AppID and Client Secret are required when joining an AVD Host Pool.

You must have created an AVD Host Pool in the AVD Resource Group.

You must enable and configure **Join Active Directory Domain** to enable this option.

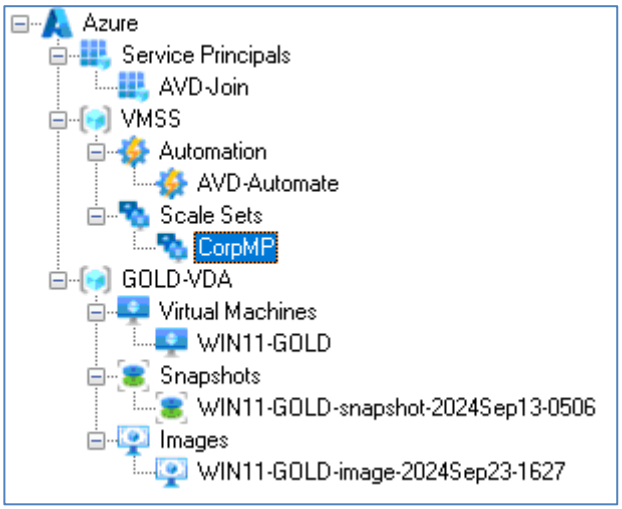
Host Pool: Select a Host Pool name

App ID: The App ID is auto-populated using the App ID of AVD-Join

Client Secret: Paste the Client Secret which was provided when creating **AVD-Join**.

The time to create the Scale Set can vary depending on how many VMs are created and the VM Size.

When the Scale Set has been created, a new node will appear under Scale Sets.



Estimated time to complete: 6-8 minutes

6. Image Updates

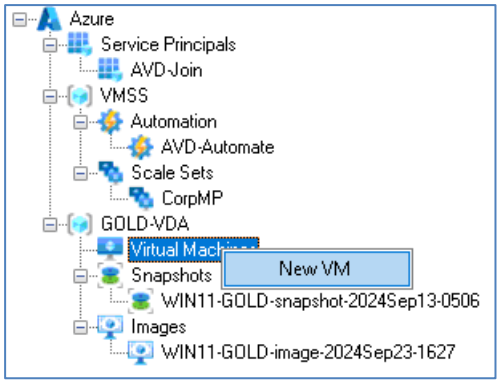
The user performing these tasks should be a member of **AVD-Admins**.

Managed Images will require updating at least once per month.
Updates may include:

- Windows Updates
- Application Updates
- Add / Remove Applications
- Fixes to discovered issues

6.1 Recreate the Master VM

Right click Virtual Machines and select New VM.



VM Source

Select Snapshot then select the last known good snapshot.

Storage / Placement

The OS Disk Type is Persistent. Select a storage tier.

(VM) Size

Select a virtual machine size.

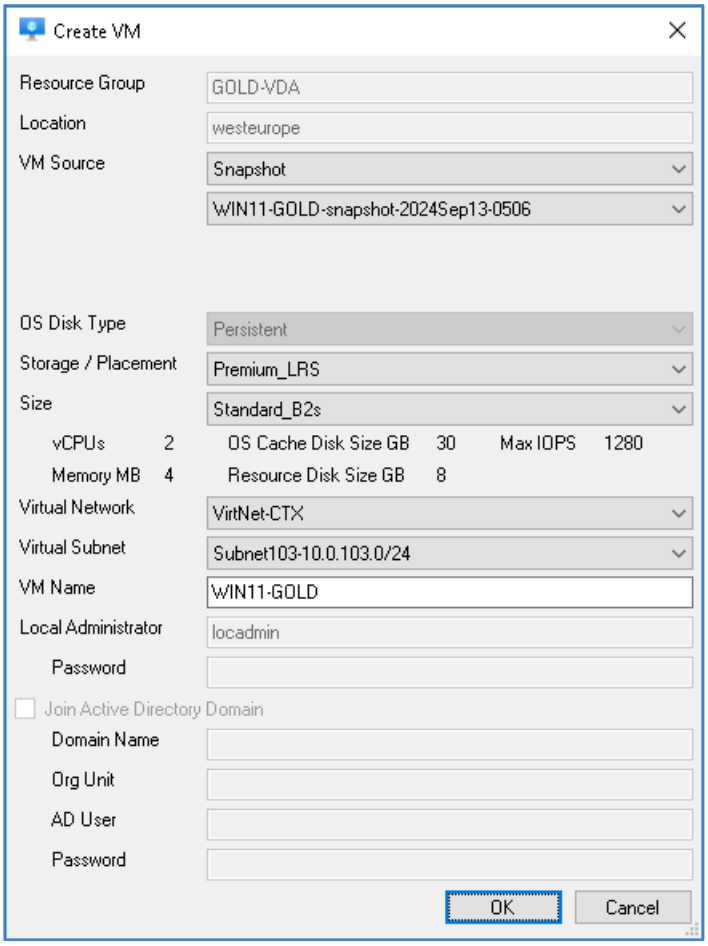
Virtual Network / Virtual Subnet

Select a Virtual Network and Virtual Subnet.

VM Name

The Master VM will have the same Windows computername as before so it is recommended to name the VM accordingly.

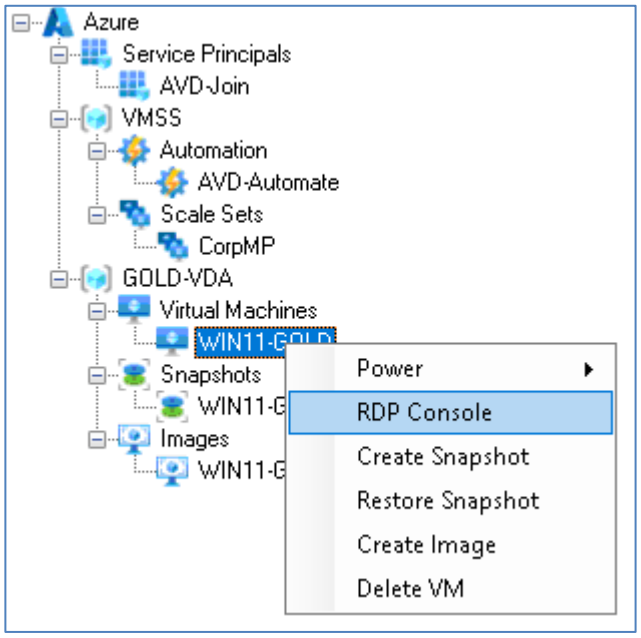
If the Master VM was previously domain joined when the snapshot was created, it will still be domain joined after creation.



Estimate time to complete: 3 minutes

6.2 Modify the Master VM

If you have a private network connection to Azure, you can RDP to the new VM.

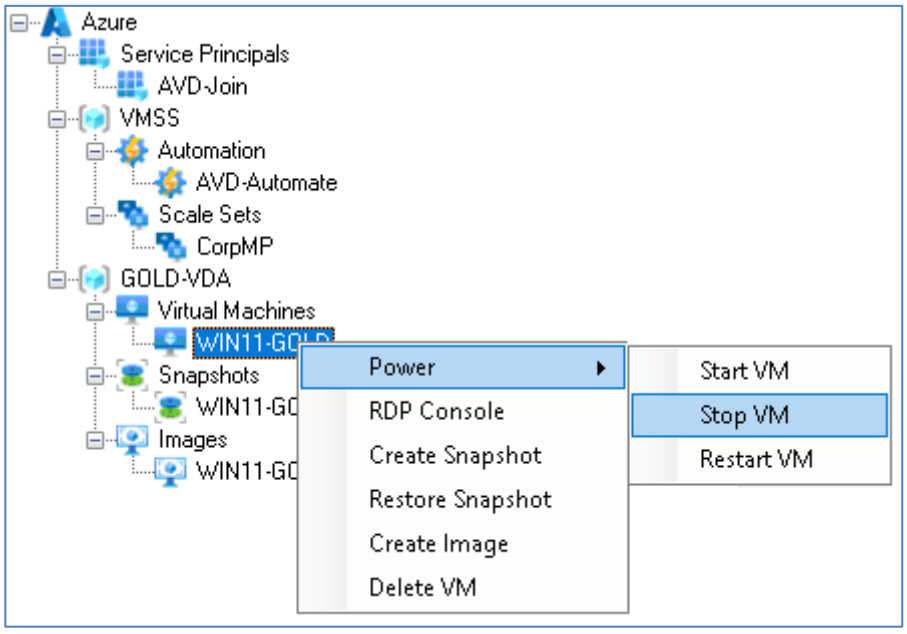


Updates may include:

- Windows Updates
- Application Updates
- Add / Remove Applications
- Fixes to discovered issues

When applying Windows Updates and rebooting, the VM may not be contactable for several minutes.

When you have made all required changes to the Master VM, shut the VM down using AVDManage so that the VM status is deallocated.



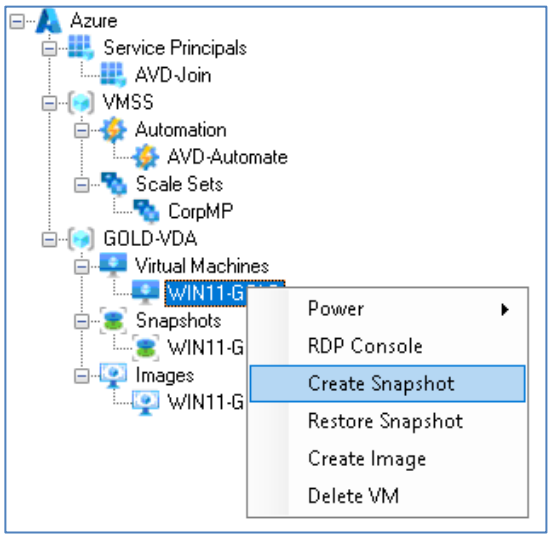
6.3 Snapshot the Master VM

A snapshot is required so that the Master VM can be recreated in the future in the same state as its last update.

After the snapshot has been created, the next step is to sysprep the Master VM which will render the Master VM unusable. Therefore the snapshot allows for the original VM to be recreated in the future.

Check the VM status is Deallocated.

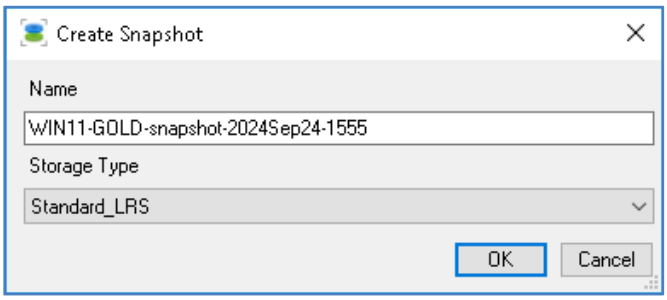
Right click the VM and select Create Snapshot



Name

Maximum length: 80 characters

The name is auto-generated based on the name of the VM and the current date / time. It may be modified. Snapshot names can only contain Alphanumeric characters, hyphens and underscores.

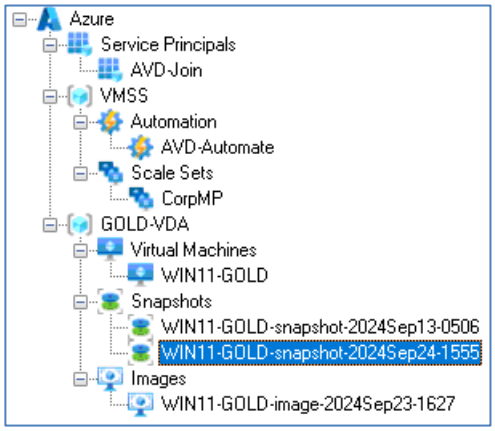


Storage

Select from

- Standard_LRS
- Premium_LRS
- Standard_ZRS

The new Snapshot is displayed under the Snapshots node.



Estimated time to complete: 10-20 seconds

6.4 Sysprep the Master VM

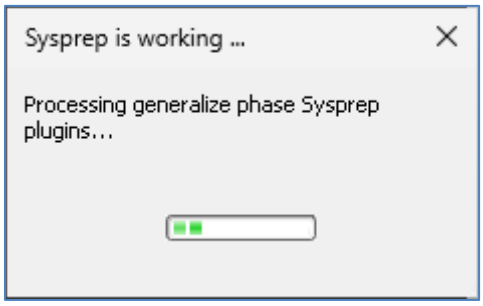
Start the VM.

When the VM is running, RDP to the new VM.

If the VM is joined to an Active Directory Domain, remove the VM from the Domain and restart.

Open a command prompt as Administrator and run a seal script or:

C:\Windows\System32\Sysprep\sysprep.exe /oobe /generalize /shutdown



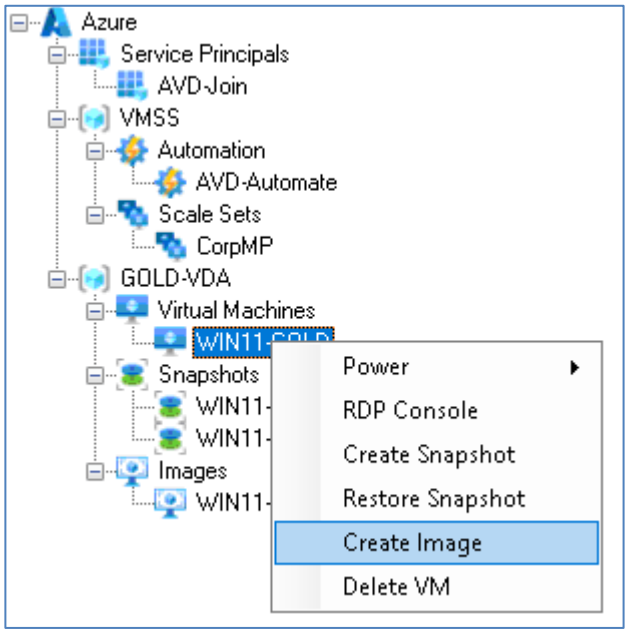
After several minutes the VM will shutdown.

After shutdown, the VM status will be stopped.
Use AVDManage to Stop the VM so that it is in a deallocated state.

6.5 Create Image of the Master VM

Check the VM status is Deallocated.

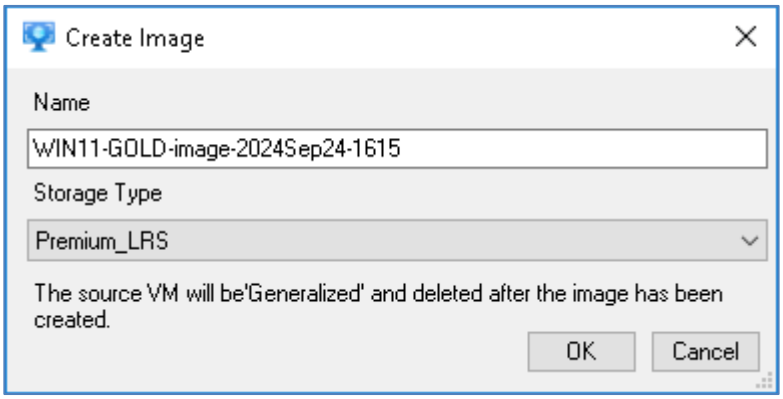
Right click the VM and select Create Image



Name

Maximum length: 80 characters

The name is auto-generated based on the name of the VM and the current date / time. It may be modified. Image names can only contain Alphanumeric characters, hyphens and underscores.



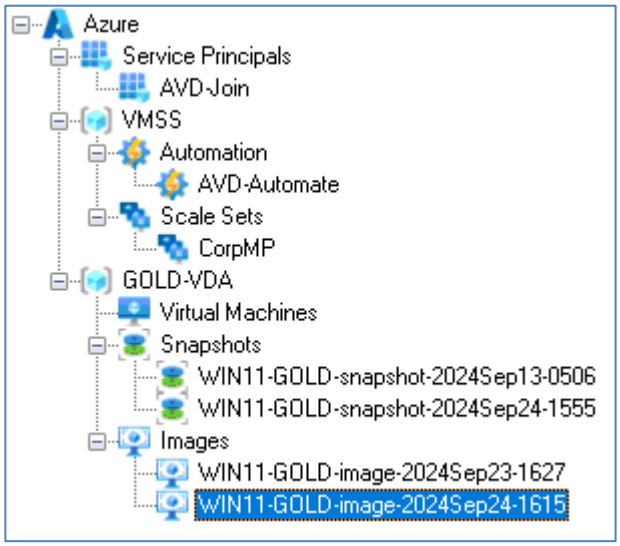
Storage

Select from

- Standard_LRS
- Premium_LRS
- Standard_ZRS

The VM will be marked as generalized before an Image is created and the VM is deleted.

The new Image is displayed under the Images node.



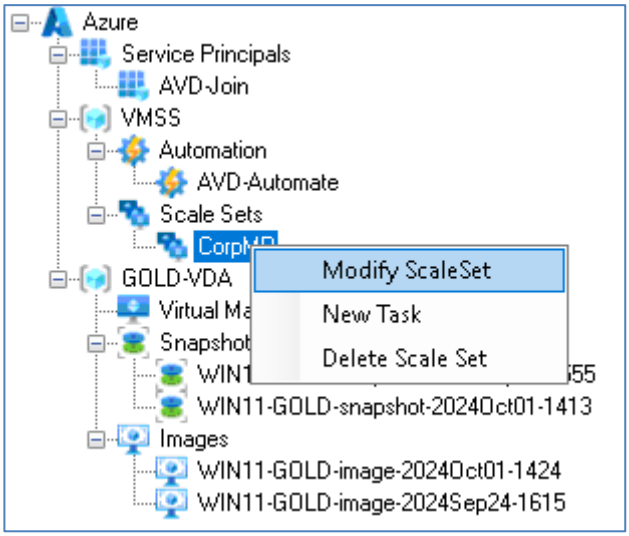
Estimate time to complete: 60 seconds

7. Update a Scale Set

The user performing these tasks should be a member of **AVD-Admins**.

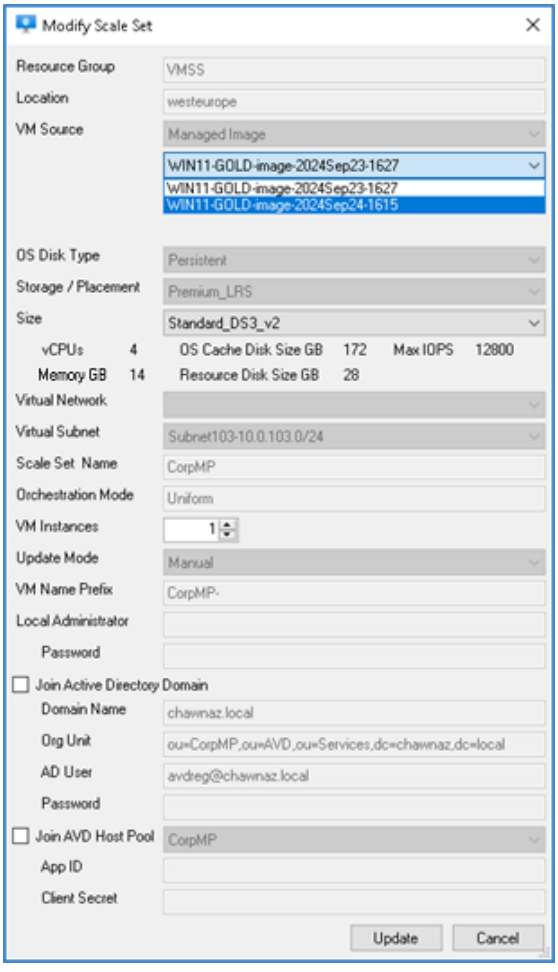
When a new image has been prepared, the Scale Set configuration may be updated.

Right click the Scale Set and select Modify Scale Set.



You can modify the:

- **VM Source**
- **(VM) Size – Scale Up**
- **(VM Instances) – Scale Out**



In this instance, the VM Source is being updated to the newer Managed Image.

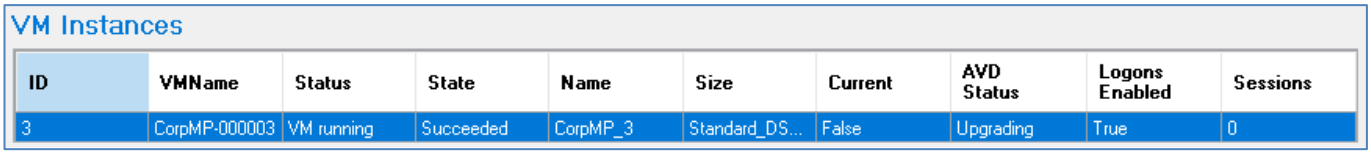
If the Scale Set is configured to Join Active Directory, you can update the AD User and Password.

If you do not select the checkbox, the Active Directory configuration remains the same.

If the Scale Set is configured to Join and AVD Host Pool, you can update the AppID and Client Secret.

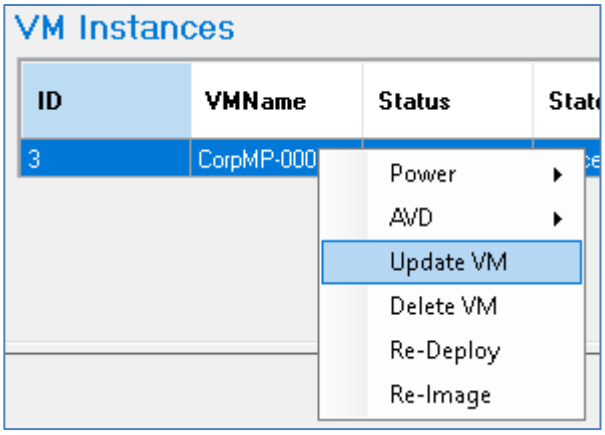
If you do not select the checkbox, the Join AVD configuration remains the same.

The **Current** status of the VM instances will change from True to False. They are still running the old image and do not have the latest Scale Set configuration.



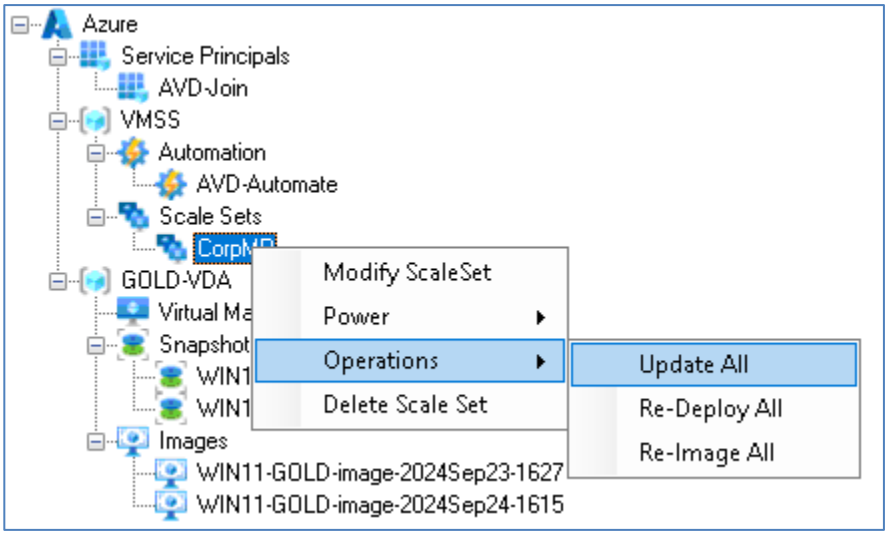
A specific VM instance may be updated by right clicking the VM and selecting update.

The VM will shut down and be unavailable while updating.



All VM instances in the Scale Set may be updated by right clicking the Scale Set and selecting Update All.

All VMs will shut down and be unavailable while updating.



When updating Ephemeral and Persistent Virtual Machine instances, they will retain their VMName, VM Instance name, Windows computername and Active Directory computername.

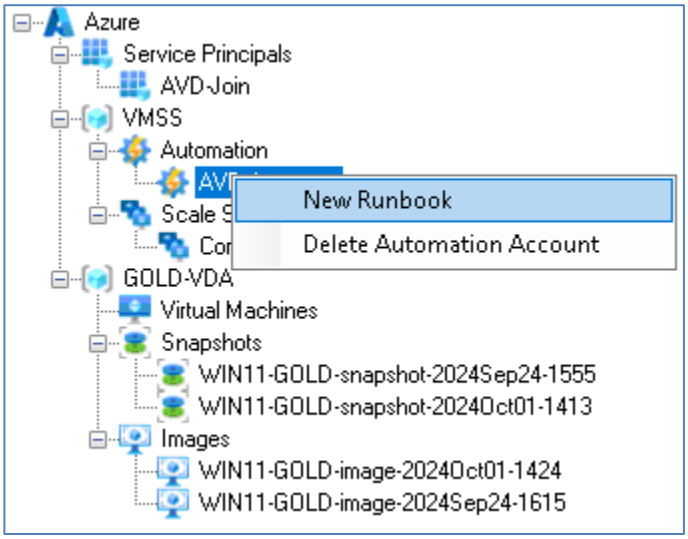
Immediate updating of VMs is unlikely to be appropriate if the VMs are hosting AVD sessions.

It is recommended that Scale Set updates are scheduled during a planned maintenance window using Azure Automation and ***AVD-Automate***.

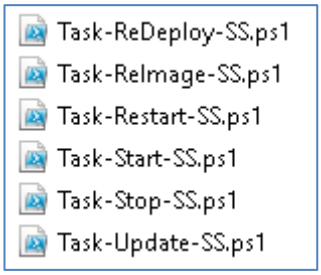
7.1 Create Update Runbook

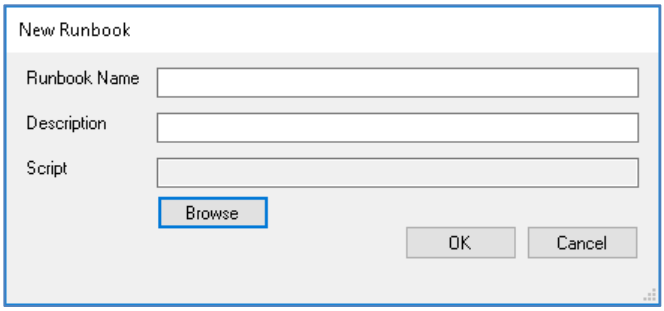
Task-Update-SS.ps1 is used to create an Automation Task that updates all the VM Instances at the same time during a planned maintenance window. The VMs will be re-deployed with the new Scale Set configuration such as an updated Image.

Right Click AVD-Automate and select New Runbook.



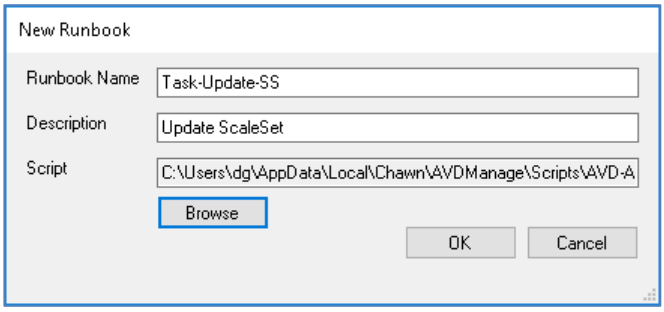
Click Browse and select a Runbook script.



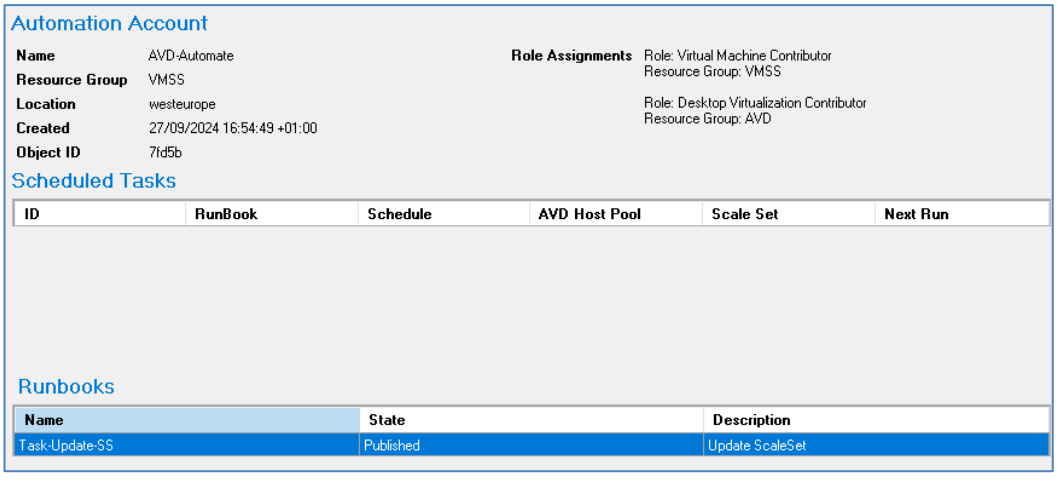


The Runbook name and Description are auto-filled but may be modified.

Click OK.



The new Runbook is visible when clicking on the AVD-Automate node.



A single runbook can be applied to multiple Scale Sets.

Runbook scripts are stored in **%LOCALAPPDATA%\Chawn\AVDManage\Scripts\AVD-Automate**.

Additional Task Scripts will be made available at https://github.com/ChawnLimited/AVDManage.

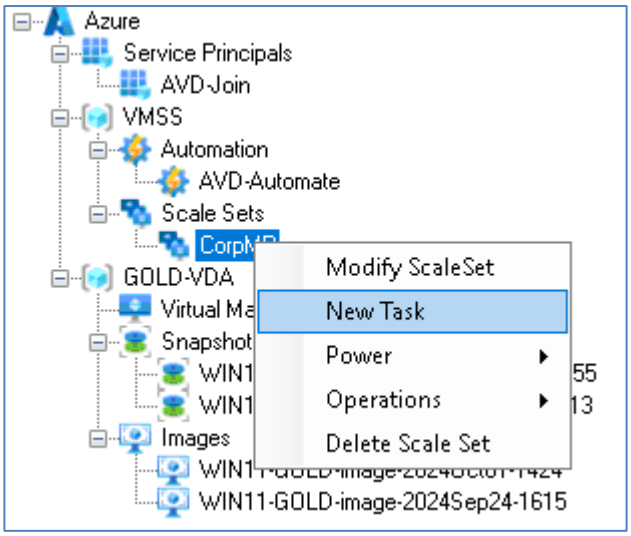
Runbook Script	Purpose
Task-DisableLogons-SSAVD.ps1	Disable AVD logons for Scale Set VM instances
Task-EnableLogons-SSAVD.ps1	Enable AVD logons for Scale Set VM instances
Task-LogOffSessions-SSAVD.ps1	Logoff all AVD sessions on Scale Set VM instances
Task-ReDeploy-SS.ps1	Re-Deploy all Scale Set VM instances
Task-ReImage-SS.ps1	Re-Image all Scale Set VM instances
Task-Restart-SS.ps1	Restart all Scale Set VM instances
Task-Start-SS.ps1	Start all Scale Set VM instances
Task-Stop-SS.ps1	Stop all Scale Set VM instances
Task-Update-SS.ps1	Update all Scale Set VM instances

7.2 Create Update Automation Task

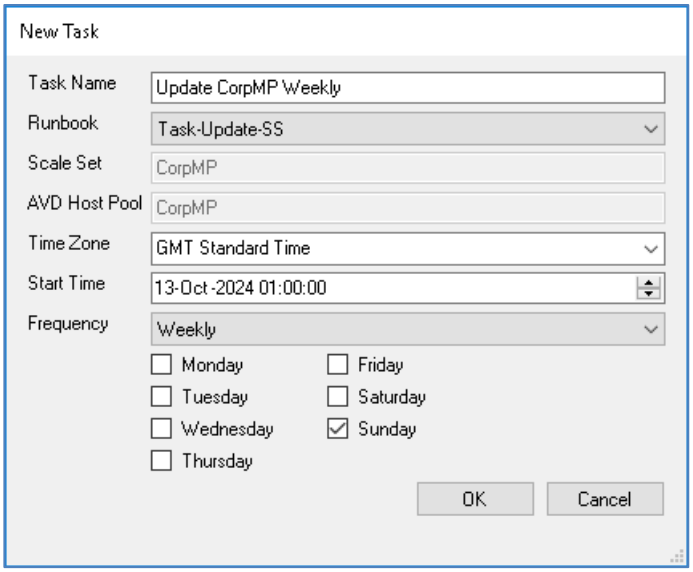
A Task is required to associate a Scale Set with a Runbook. The Runbook will execute at the time specified in the Task schedule.

Runbook: Task-Update-SS
Parameters:
Target Scale Set Name: CorpMP
Target AVD Host Pool: CorpMP
Schedule: Weekly. Every Sunday at 1am

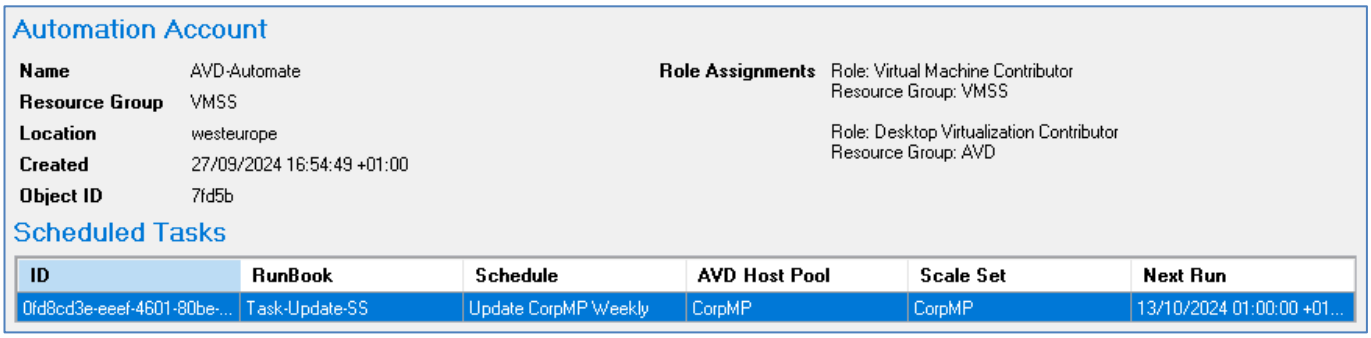
Right Click a Scale Set and select New Task.



- Enter a Task Name
- Select a Runbook
- The Scale Set and AVD Host Pool values are pre-filled.
- Adjust the Time Zone if necessary
- Specify a Start Time and Frequency.
- Click OK



The new task is visible when clicking on the AVD-Automate node.



You can right click the task to delete it or view further schedule details.

8. Reference

8.1 Virtual Machines

Only Microsoft Windows Virtual Machines may be created.

Virtual Machines may be created from:

- Azure Gallery Images
- Managed Images
- Snapshots

8.1.1 Configuration

All Virtual Machines (and Virtual machine Scale Set VM Instances) have the following configuration.

PublicIP	None
BootDiagnostics.Enabled	False
HyperVGeneration	V2
EnableAcceleratedNetworking	False
NetworkSecurityGroups	None
ProvisionVMAgent	True
PatchMode	AutomaticByOS
SecurityType	Standard

The following events may be logged due to the SecurityType as vTPM and SecureBoot are not enabled. These events may be ignored.

Log: System	Source: TPM-WMI	Event ID: 1796
The Secure Boot update failed to update a Secure Boot variable with error Secure Boot is not enabled on this machine.. For more information, please see https://go.microsoft.com/fwlink/?linkid=2169931		

Log: System	Source: Wininit	Event ID: 15
Credential Guard and/or VBS Key Isolation are configured but the secure kernel is not running; continuing without them.		

8.1.2 OS Disk Type: Persistent vs Ephemeral

Most VMs will be created with a Persistent disk however VMs with Ephemeral disks may be created for short term testing.

VMs with Ephemeral disks may not be used to create snapshots or images.

8.1.3 Menu Actions

Power - Start VM	Starts the VM. (Persistent only)
Power - Restart VM	Restarts the VM.
Power - Stop VM	Stops and De-Allocates the VM. (Persistent only)
RDP Console	Attempts to connect via RDP using the VM IP Address.
Create Snapshot	Creates a Snapshot. The VM must be in a deallocated state. (Persistent only)
Restore Snapshot	Reverts the VM to the previous Snapshot State. The VM must be in a deallocated state. (Persistent only)
Create Image	Creates an Image of the VM. The VM should have been sysprepped before. The VM must be in a deallocated state. (Persistent only)
Delete VM	Deletes the VM, Disk and NIC

8.2 Virtual Machine Scale Sets

Only Microsoft Windows Virtual Machines can be created.

Virtual Machine Scale Sets may be created from:

- Azure Gallery Images
- Managed Images

8.2.1 Orchestration Mode

Uniform: Optimized for large-scale stateless workloads with identical instances

Flexible: Achieve high availability at scale with identical or multiple virtual machine types

AVDManage only created Virtual Machine Scale Sets in **Uniform** Orchestration mode.

Orchestration modes for Virtual Machine Scale Sets in Azure - Azure Virtual Machine Scale Sets | Microsoft Learn

8.2.2 Update Mode

You can choose between Manual and Automatic modes.

Manual: You choose when to update the scale set instances. Nothing happens automatically to the existing virtual machines when changes occur to the scale set model. New instances added to the scale set use the most update-to-date model available.

Automatic: The scale set makes no guarantees about the order of virtual machines being brought down. The scale set might take down all virtual machines at the same time to perform upgrades

Manual update is preferred for Scale Sets hosting AVD sessions. **AVD-Automate** can be used to update VM instances during planned maintenance windows.

Rolling update mode is not supported by AVDMAnage.

Upgrade policies for Virtual Machine Scale Sets (preview) - Azure Virtual Machine Scale Sets | Microsoft Learn

8.2.3 Load Balancing

Virtual Machine Scale Sets are frequently created with an Azure Load Balancer to spread traffic across multiple VMs, such as a web server farm.

AVDManage doe note create any Load Balancers when creating Virtual Machine Scale Sets however you are free to configure your own Load Balancer in the Azure portal after VMSS creation.

8.2.4 OS Disk Type: Persistent vs Ephemeral

Ephemeral OS disks are created on the local virtual machine (VM) storage and not saved to the remote Azure Storage. Ephemeral OS disks work well for stateless workloads, where applications are tolerant of individual VM failures but are more affected by VM deployment time or reimaging of individual VM instances. With Ephemeral OS disk, you get lower read/write latency to the OS disk and faster VM reimage.

The key features of ephemeral disks are:

- Ideal for stateless applications.
- Supported by Marketplace, custom images, and by Azure Compute Gallery (formerly known as Shared Image Gallery).
- Ability to fast reset or reimage VMs and scale set instances to the original boot state.
- Lower latency, similar to a temporary disk.
- Ephemeral OS disks are free, you incur no storage cost for OS disks.
- Available in all Azure regions.

	Persistent	**Ephemeral**
Size	All VM Sizes	Restricted by Cachedisk or ResourceDisk size
Persistence	OS disk data written to OS disk are stored in Azure Storage	Data written to OS disk is stored on local VM storage and isn't persisted to Azure Storage.
Stop/Start	Supported	Not supported. Always running. Cannot be deallocated.
ReDeploy	OS Disk is preserved	VM is re-deployed
Disk Storage Costs	Yes	No

As stated above, Ephemeral disks are ‘Ideal for stateless applications’.

However as AVDManage can redeploy Persistent and Ephemeral VM instances both Persistent and Ephemeral disks should be considered stateless.

VMs with Ephemeral disks can be slightly more complicated to manage.

Imagine you have a Scale Set with 10 VM instances all joined to an AVD Host Pool.

The Session Hosts are only required between 6am and 9pm therefore you can reduce PAYG costs by powering off the VM instances at 9pm and powering on at 5.30am.

This is not an issue for Persistent VMs. They can be powered off and will start with the same machine identity and computername at 5.30am.

Ephemeral VMs cannot be powered off so you would have to delete all VM instances at 9pm and recreate them at 5.30pm.

In both cases the AVD Host Pool would be operational however the Ephemeral VMs will have new machine identities and computernames. The old names will be left behind in Active Directory, the AVD Host Pool and Microsoft Entra resulting in increased redundant objects and administration.

If you wish to run Ephemeral VMs 24h/24h, they will maintain their identities when updating, re-imaging and re-deploying.

8.2.5 Menu Actions

New Scale Set	Create a new Scale Set
Power – Start All	Start all VM instances (Persistent only)
Power – Restart All	Restart all VM instances
Power - Stop All	Stop all VM instances (Persistent only)
Modify Scale Set	Modify and update the Scale Set configuration. • VMImageSource • VMSize • VMInstances • ADJoin • Join-AVD
New Task	Create and schedule a new task
Operations – Update All	Rebuild all VM instances with the latest Scale Set configuration
Operations – Re-Deploy All	Deploy all VM instances to a new host with the existing VM instance configuration
Operations – Re-Image All	Rebuild all VM instances with the existing VM instance configuration
Delete Scale Set	Delete the Scale Set and all VM instances

8.3 AVD-Join Service Principal

AVD-Join is an Entra Service Principal. It can be viewed as an App Registration in the Azure portal and as an Enterprise Application but this can only be located using the search bar.

The Client Secret is valid for 12 months. It can be reset using AVDManage if the user has been assigned as an owner of the **AVD-Join** App Registration.

The Secret Expires date colour will change to Red 37 days before expiry.

When creating a Scale Set, **AVD-Join** can be configured as a CustomScriptExtension.
The following parameters are included:

- AVD Host Pool to join
- AVD-Join AppID
- AVD-Join Client Secret

All parameters are created in ProtectedSettings. Protected settings are encrypted through a key known only to Azure and the VM.

After the VM has joined an Active Directory Domain, AVD-Join will download
https://raw.githubusercontent.com/ChawnLimited/AVDManage/refs/heads/main/AVDJoin.ps1
AVDJoin.ps1

- Checks that the Microsoft RDS InfraStructure Agent is not already installed
- Checks that the VM is domain joined
- Checks required PS Modules are present
- Authenticates to Azure as AVD-Join
- Removes the existing VM from the AVDHostPool (if it exists)
- Generates a new AVD Registration Token if it has expired
- Download the Remote Desktop Services Infrastructure Agent & Boot Loader
- Join the AVDHostPool using the AVD Token
- Disconnects from Azure

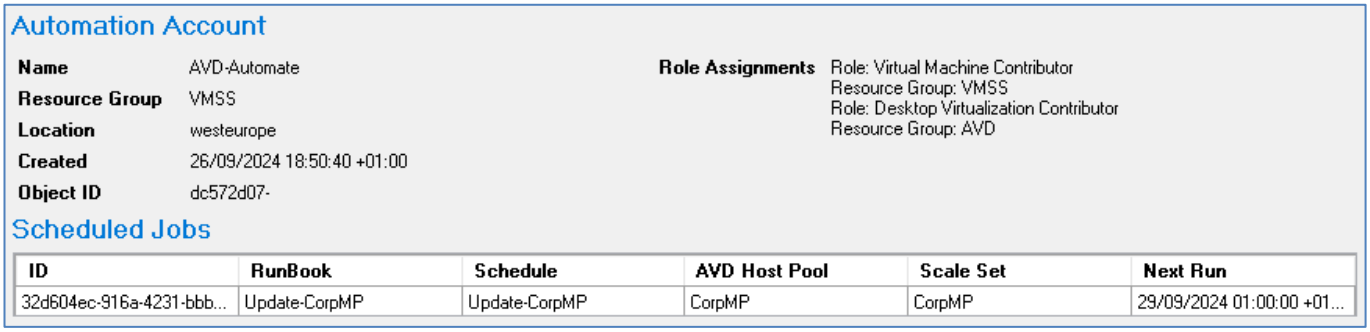
AVDJoin.ps1, AVDJoin.log and source media and installation log files will be left in
C:\Packages\Plugins\Microsoft.Compute.CustomScriptExtension\x.x.x\Downloads\x

CustomScriptExtension logs are located in
C:\WindowsAzure\Logs\Plugins\Microsoft.Compute.CustomScriptExtension\x.x.x

8.3.1 Menu Actions

New Service Principal	Creates a new ServicePrincipal named AVD-Join and assigns the *Desktop Virtualization Contributor* role to the Resource Group containing AVD Host Pools Menu action is disabled after creation
Reset Client Secret	Generate a new Client Secret
Delete AVD-Join	Delete AVD-Join ServicePrincipal and and removes the Role assignments

8.4 AVD-Automate Automation Account



AVD-Automate is an Automation Account and can invoke Automation Runbooks at scheduled times.

An Automation Runbook is a PowerShell script that is executed with parameters

AVD-Automate is a Managed Identity. A managed identity from Microsoft Entra ID allows your runbook to easily access other Microsoft Entra protected resources. The identity is managed by the Azure platform and doesn't require you to provision or rotate any secrets.

This allows AVD-Automate to perform tasks against Virtual Machine Scale Sets and AVD Host Pools.

Scripts are located in %LOCALAPPDATA%\Chawn\AVDManage\Scripts\AVD-Automate

Scripts are available to download from https://github.com/ChawnLimited/AVDManage

Tasks may be scheduled to run One Time, Daily, or Weekly on specific days.

8.4.1 Menu Actions

New Automation Account	Creates a new Automation Account named AVD-Automate and assigns the Virtual Machine Contributor role to the Resource Group containing Virtual Machine Scale Sets, and the Desktop Virtualization Contributor role to the Resource Group containing AVD Host Pools Menu action is disabled after creation
Delete Automation Account	Deletes the AVD-Automate Automation Account and removes the Role assignments

8.5 Snapshots

Snapshots will accumulate over time and incur storage costs.

It is recommended that the last three good snapshots are retained for rollback purposes.

8.5.1 Menu Actions

Delete Snapshot	Deletes the Snapshot

8.6 Images

Images will accumulate over time and incur storage costs.

It is recommended that the last three good Images are retained for rollback purposes.

Do not delete Images that are still in use by a Scale Set.

Use Premium storage for faster deployments particularly when using VMs with Ephemeral Disks.

8.6.1 Menu Actions

Delete Image	Deletes the Image

8.7 PowerShell

Minimum PowerShell Version: 5.1

8.7.1 Module Installation for AVDManage

Install minimal PowerShell Modules for AVDManage.

```
Set-PSRepository -Name PSGallery -InstallationPolicy Trusted
Install-Module Az.Accounts, Az.Compute, Az.DesktopVirtualization, Az.Resources, Az.Automation, Az.Network
```

Or install all Azure PowerShell Modules.

```
Set-PSRepository -Name PSGallery -InstallationPolicy Trusted
Install-Module Az.*
```

Update all Azure PowerShell Modules.

```
Set-PSRepository -Name PSGallery -InstallationPolicy Trusted
Update-Module Az.*
```

8.7.2 Module Installation for AVD-Join (Master VM)

Install minimal Powershell Modules for AVD-Join on the Master VM.

```
Set-PSRepository -Name PSGallery -InstallationPolicy Trusted
Install-Module Az.Accounts, Az.DesktopVirtualization
```

Update Powershell Modules for AVD-Join on the Master VM.

```
Set-PSRepository -Name PSGallery -InstallationPolicy Trusted
Update-Module Az.Accounts, Az.DesktopVirtualization
```

8.8 Login Issues

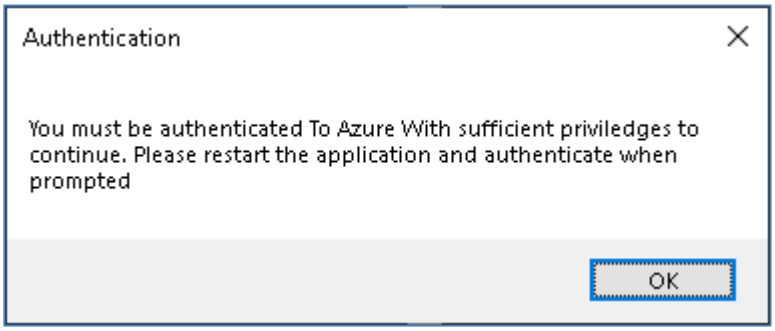
8.8.1 Browser

Ensure that you have a modern up to date browser installed and that it is set as the Default browser.

8.8.2 Authentication Error

If you continually receive the message even though Azure permissions are correct.

"You must be authenticated To Azure With sufficient privileges to continue. Please restart the application and authenticate when prompted"



Try the following:

8.8.3 Authenticate Manually

Open PowerShell and run

Connect-AzAccount

Complete the authentication process.

Launch AVDManage.

8.8.4 Update PowerShell Modules

Ensure that required PowerShell modules, specifically Az.Accounts, are up to date.

8.8.5 Disable Web Account Manager

This will enforce browser authentication.

In PowerShell, run

Update-AzConfig -EnableLoginByWam $False

This will enforce browser authentication instead of using Web Account Manager. This is helpful for users who need to logon to multiple tenants. When AVDManage is launched, the default browser opens and presents the Azure authentication dialog.

8.8.6 Set Default Subscription

Open PowerShell and run

Connect-AzAccount

If you successfully authenticate, get the required Subscription ID

Get-AzSubscription

Update you AZConfig so that the required Subscription ID is the default
Update-AzConfig –DefaultSubscriptionForLogin xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

8.8.7 Corrupt PowerShell / Azure Profile

Make a backup copy of the following folders

- %USERPROFILE%\.Azure
- %LOCALAPPDATA%\.IdentityService

Close all browsers, PowerShell consoles and AVDManage.

Delete the contents of the following folders:

- %USERPROFILE%\.Azure
- %LOCALAPPDATA%\.IdentityService

Open Powershell and run
Connect-AzAccount