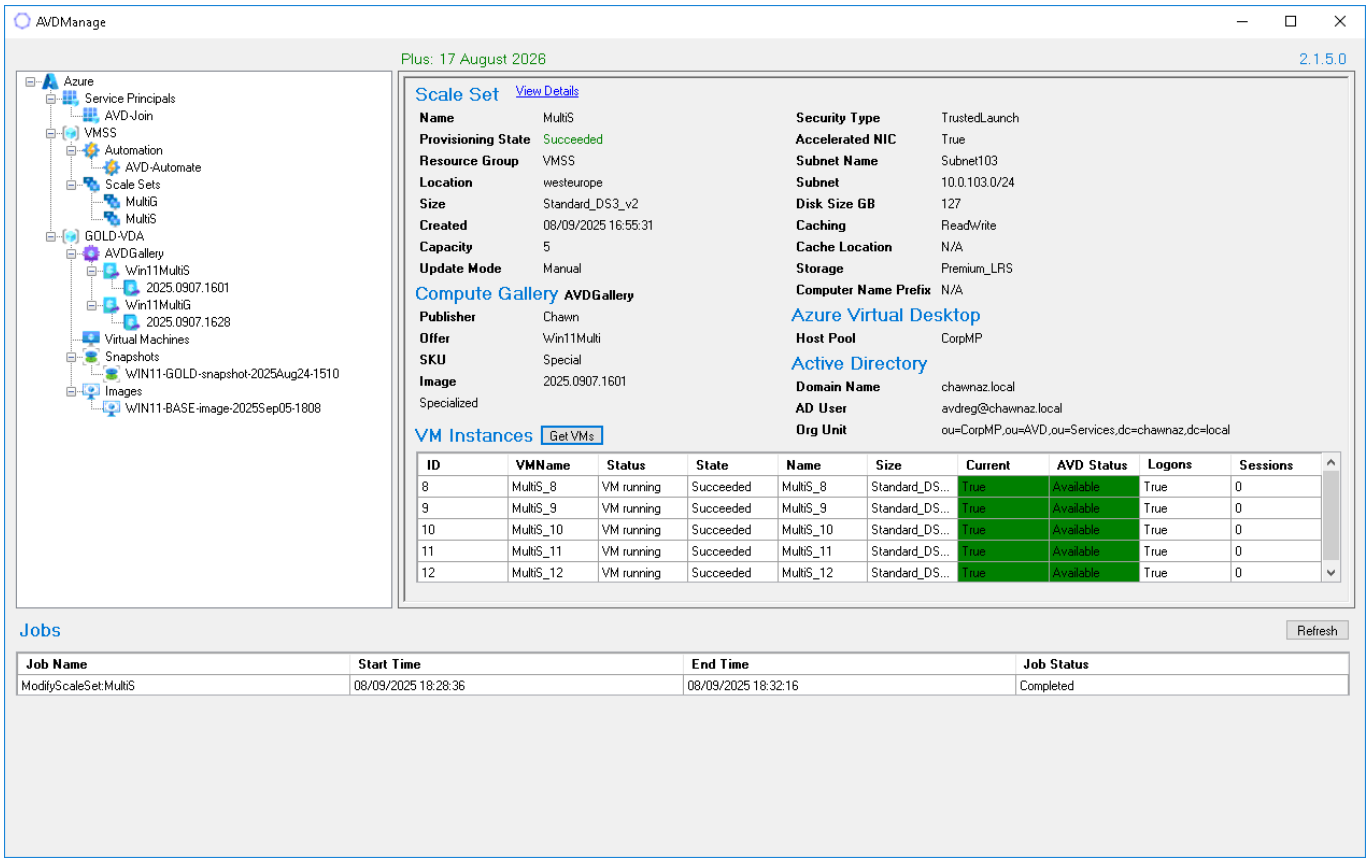
chawn
+44 (0)121 314 2253
info@chawn.com

Desktops & Applications  Virtualisation & Integration

AVDManage 2.1.0.0 Administration

Document Details

Document Name	AVDManage 2.1.0.0 Administration
Author	DG – Chawn Limited
Version	1.0
Date	15th August 2025
Status	Final

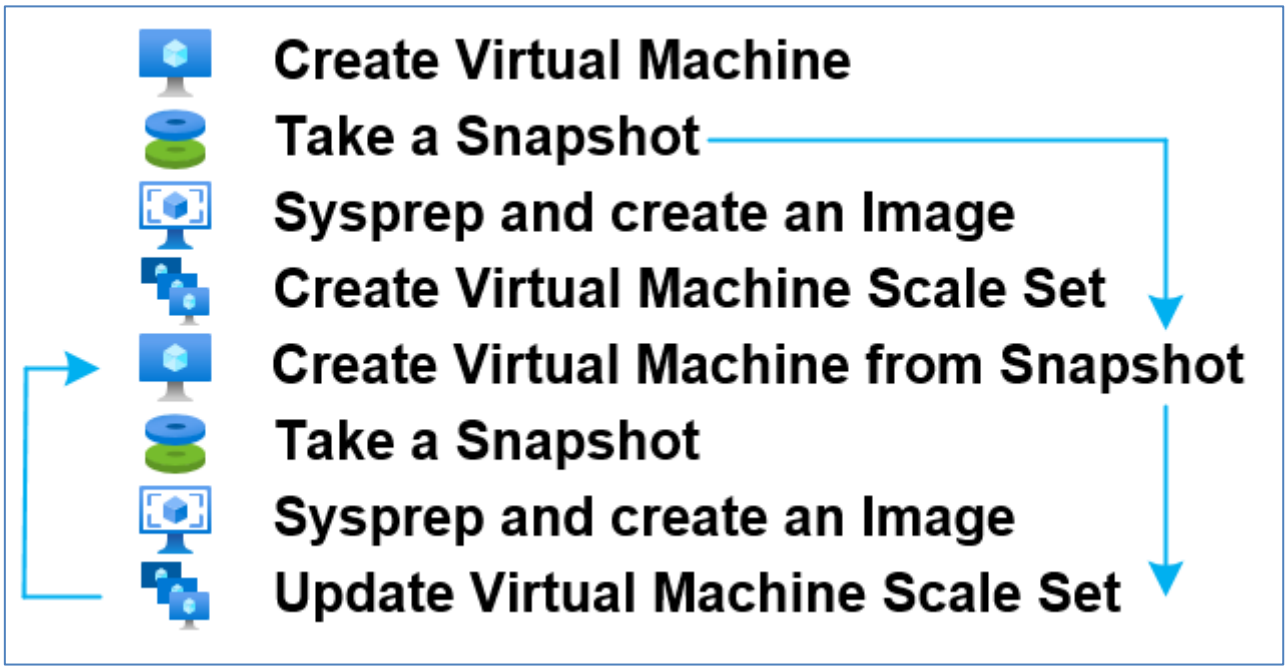


Contents

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, Azure Gallery Images or Compute 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-Turbo** – Join AD Domain & AVD Host Pool (specialized)
- **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, Entra Device ID)

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

JoinAD leverages the JsonADDomainExtension enabling Generalized Images to join an Active Directory Domain.

AVD-Join and **AVD-Turbo** leverage the Azure Custom Script Extension for Windows.

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

AVD-Turbo enables specialized Scale Set Virtual Machine instances to rename the computer according to the VM Name, join an Active Directory domain and an Azure Virtual Desktop host pool when deploying or updating Virtual Machine Scale Sets.

AVD-Automate leverages Azure Automation enabling 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
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.

1.1 Updates

Updates since the previous release.

Digitally Signed

- The AVDManage installer and application files are digitally signed
- AVD-Join.ps1 and AVD-Turbo.ps1 deployment scripts are digitally signed

Configuration

- Template Active Directory Domain information
- Automatic Job refresh

Virtual Machine Creation

- Enable accelerated networking

Virtual Machine Scale Set Creation

- Enable accelerated networking

Virtual Machine Scale Set Instance Deletion

- Deletes the Active Directory Computer object
- Deletes the Azure Virtual Desktop Session Host

1.2 Editions

AVDManage is available in two editions, Free and Plus.

AVDManage Plus enables deployment of images from Azure Compute Galleries. This allows for deployment of generalized and specialized images.

VMs and scale sets created from specialized images can be up and running quicker, because they're created from a source that has already been through first boot. VMs created from specialized images boot faster and can contain a greater degree of local customisation as they have not been sysprepped.

AVDManage Plus requires an evaluation or annual license. Please contact info@chawn.com for license enquiries.

	Free	Plus
Create VMs from Snapshots	✓	✓
Create Virtual Machines & Scale Sets from Azure Gallery	✓	✓
Create Virtual Machines & Scale Sets from Managed Images	✓	✓
Create Virtual Machines & Scale Sets from Compute Galleries		✓
Create Virtual Machines in any Resource Group in the base Location		✓
Deploy Generalized Windows Images	✓	✓
Deploy Specialized Windows Images		✓
Persistent & Ephemeral Disks	✓	✓
Accelerated Networking	✓	✓
Create Trusted Launch Virtual Machines & Scale Sets		✓
AVD-Automate	✓	✓
JoinAD – Join Active Directory Domain	✓	✓
AVD-Join – Join AVD Host Pool	✓	✓
AVD-Turbo (for Specialized Virtual Machines & Scale Sets) Renames Virtual Machine and optionally joins Active Directory Domain and AVD Host Pool		✓
AVD-Prep – Pre-stage the Remote Desktop Infrastructure and Boot Loader Agents	✓	✓

2. Estimated Deployment Times

Virtual Machine: Standard_DS3_v2 with Accelerated Networking and Trusted Launch (Managed Images are deployed with Standard Security)

O/S: win11-24h2-avd-m365

Storage: Premium LRS

Deployment times are based on deploying one Virtual Machine instance in a Scale Set.

Deployment times are based on the Job Start Time and End Time in AVDManage.

Source	Image	Disk Size	Deployment	AVD-Join / AVD-Turbo	Pre-Staged AVD-Prep	Total
Compute Gallery	Specialized	127	1m55s		1m00s	2m55s
Compute Gallery	Specialized	127	1m55s	1m45s		3m40s
Compute Gallery	Generalized	127	4m50s		1m00s	5m50s
Compute Gallery	Generalized	127	4m50s	1m45s		6m35s
Managed Image	Generalized	127	5m00s		1m00s	6m00s
Managed Image	Generalized	127	5m00s	1m45s		6m45s
Azure Gallery	Generalized	127	3m50s	3m10s		7m00s

The deployment of Specialized images is quickest as the image has already been through the first-boot process. Pre-staging the Remote Desktop Infrastructure and Boot Loader Agents further improves deployment times.

Specialized Images require a reboot after running AVD-Turbo which increases deployment time by about 20 seconds.

The deployment of Azure Gallery Images is slowest. Although deployment of the O/S is faster than Generalized Compute Gallery Images, deployment of the Remote Desktop Infrastructure and Boot Loader Agents requires that NuGet and two Powershell modules are installed, extending deployment times.

3. Requirements

3.1 Operating System

- Microsoft Windows 10 build 1607 or higher

3.2 Software

- Microsoft .Net Framework 4.7.2 or higher
- Microsoft Windows PowerShell 5.1 or higher
- Microsoft Windows PowerShell Modules
  - Az.Accounts 5.2.0
  - Az.Compute 10.2.0
  - Az.DesktopVirtualization 5.4.1
  - Az.Resources 8.1.0
  - Az.Automation 1.11.1
  - Az.Network 7.19.0
  - ActiveDirectory 1.0.1 (If *DeleteADComputer* is enabled)

3.3 Azure

- An Azure Tenant and Microsoft Entra Directory
- An Azure Subscription
- An Active Directory group for **AVD-Admins** (synced to Entra ID)
- Azure Resource Groups for:
  - Master VM, Snapshots, Images, Compute Gallery (AVDManage Plus)
  - 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

AVD Host Pools must NOT have a Session Host Configuration

3.4 Network

AVDManage requires access to Azure CLI Endpoints.

Endpoints used when installing the Azure CLI | Microsoft Learn

3.5 Azure Permissions

The following permissions are required by the **AVD-Admins** group.

(Broad Scope Permissions)

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

or

(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 Compute Gallery Artifacts Publisher ☺
AVD Resource Group	Desktop Virtualization Contributor
Virtual Network Resource Group	Microsoft.Resources/subscriptions/resourceGroups/read Microsoft.Network/virtualNetworks/read Microsoft.Network/virtualNetworks/subnets/join

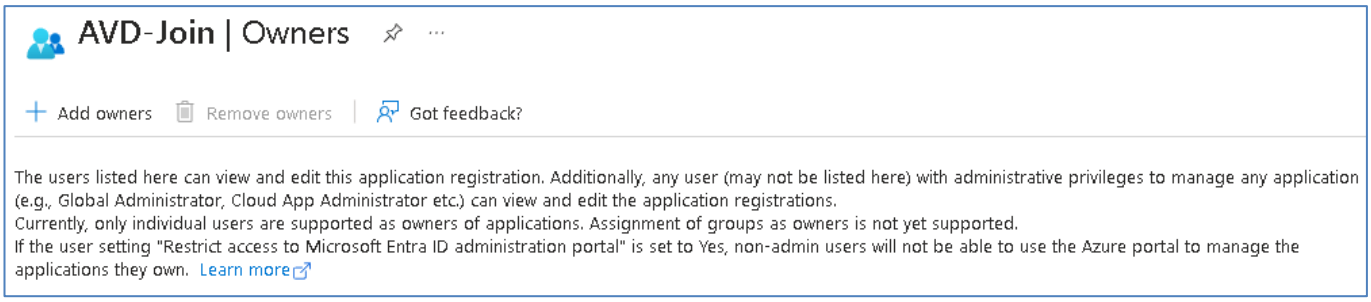
☺ *AVDManage Plus* only

3.6 Microsoft Entra Permissions

The following permissions are required to initially configure the AVDManage environment. They are not required by the **AVD-Admins** group.

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

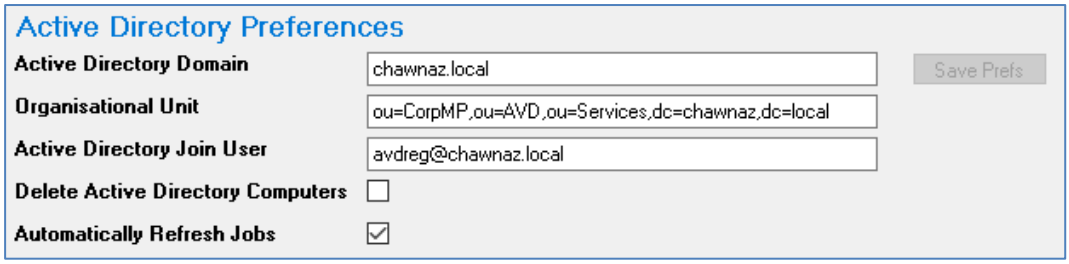
Members of the **AVD-Admins** group may be assigned the Owner role to the 'App Registration' after creation to administer the **AVD-Join** Service Principal on a per user basis. This allows named users to reset the client secret when required.



3.7 Microsoft Active Directory

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

A default domain, organisational unit and AD account can be configured as preferences, so that you do not have to type the same values when deploying VMs and Scale Sets.



Delete Active Directory Computers

If enabled, when Active Directory joined VM instances are deleted, the Active Directory computer accounts may also be deleted if the logged on user has sufficient permissions to the computers' Organizational Unit. Direct connectivity to a domain controller is required and the **ActiveDirectory** Powershell module must be installed.

The **AVD-Admins** group must be delegated permissions to **Delete Computer Objects**, and the AD Admin account must have been delegated permissions to **Create Computer Objects** on all required Active Directory Organisational Units to join VMs to the domain.

Automatically Refresh Jobs

AVDManage will update the status of submitted jobs in the background.

User preferences are stored in the registry and may be edited according to your environment.

[HKEY_CURRENT_USER\SOFTWARE\Chawn\AVDManage\Config]

AutoRefresh = True
DefaultADAdmin
DefaultDomain
DefaultOU
DeleteADComputer = False
DefaultVM = Standard_DS3_v2

3.8 Virtual Machines

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

- Az.Accounts
- Az.DesktopVirtualization

Virtual Machines require network access to:

- The **AVD-Join.ps1** and **AVD-Turbo.ps1** PowerShell Scripts

https://raw.githubusercontent.com/ChawnLimited/AVDManage/refs/heads/main/AVD-Join.ps1

https://raw.githubusercontent.com/ChawnLimited/AVDManage/refs/heads/main/AVD-Turbo.ps1

PowerShell Gallery for PowerShell Modules.

https://www.powershellgallery.com

Nuget

https://packages.nuget.org

- 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

AVD-Join.ps1, AVD-Turbo.ps1 and Microsoft Remote Desktop Service source media are downloaded by Virtual Machines when deploying and updating.

- Required FQDNs and Endpoints for Azure Virtual Desktop

  Required FQDNs and endpoints for Azure Virtual Desktop | Microsoft Learn

Default outbound internet access for Azure VMs will be retired on 30th September 2025. Ensure that Virtual Machines have a valid route to required internet endpoints.

Azure Default Outbound Internet Access

Plan for inbound and outbound internet connectivity | Microsoft Learn

3.9 Microsoft Entra hybrid Join

Microsoft Entra hybrid join is required on Virtual Machines to enable SSO and Conditional Access.

Configure Microsoft Entra hybrid join - Microsoft Entra ID | Microsoft Learn

Configuration requires:

- Microsoft Entra Connect
- Service Connection Point
- Group Policy Object linked to the dedicated organisational units for each AVD Host Pool

Computer Configuration\Policies\Administrative Templates

Windows Components/Device Registrations
Register domain joined computers as devices - Enabled

Windows Components/Internet Explorer/Internet Control Panel/Security Page
Site to Zone Assignment List
https://device.login.microsoftonline.com
https://autologon.microsoftazuread-sso.com
https://enterpriseregistration.windows.net
https://login.microsoftonline.com

Windows Components/Internet Explorer/Internet Control Panel/Security Page/Intranet Zone
Allow updates to status bar via script - Enabled

Preferences Registry
Hive HKEY_LOCAL_MACHINE
Key path SOFTWARE\Microsoft\Windows\CurrentVersion\CDJ\AAD
Value name TenantID
Value type REG_SZ
Value data xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

Hive HKEY_LOCAL_MACHINE
Key path SOFTWARE\Microsoft\Windows\CurrentVersion\CDJ\AAD
Value name TenantName
Value type REG_SZ
Value data xxxxxxxx.onmicrosoft.com / domain.com

When devices join Active Directory, they will sync to Entra ID.
When redeployed, devices re-join Active Directory, they will sync to Entra ID.
When devices are deleted from Active Directory, the deletion will sync to Entra ID.

The lowest sync cycle interval for Entra ID Connect is thirty minutes. When deploying, updating and deleting VMs, it is recommended to force synchronisation of Entra ID Connect.

Start-ADSyncSyncCycle -PolicyType Delta

4. Getting Started

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

- 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.

4.1 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.

4.2 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 ☺ Compute Gallery Artifacts Publisher ☺

☺ *AVDManage Plus* only

☺ 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 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).

4.3 Check AVDManage Requirements

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

Open PowerShell as Administrator

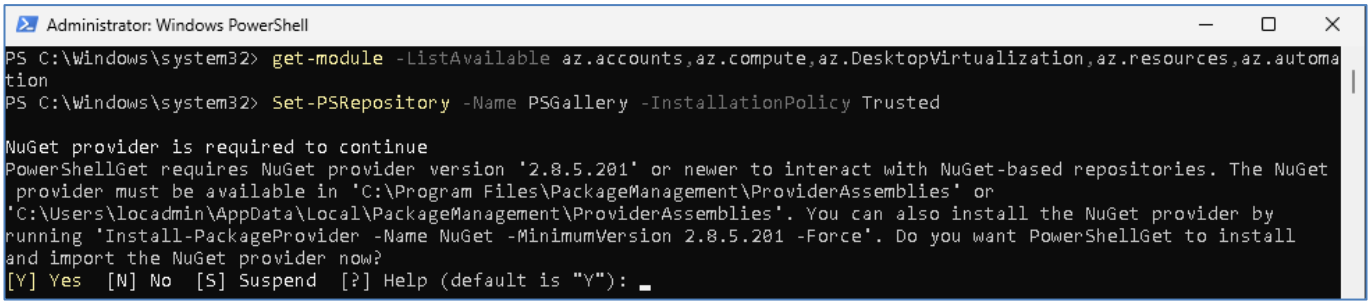
Run

```
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



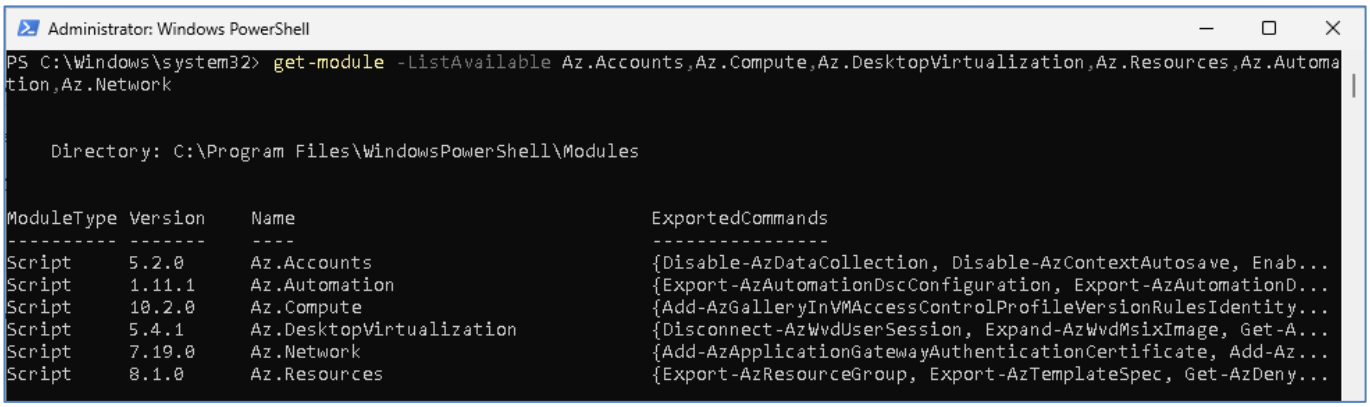
After NuGet is installed, run

```
Install-Module -Name Az.Accounts -RequiredVersion 5.2.0 -Scope AllUsers
Install-Module -Name Az.Compute -RequiredVersion 10.2.0 -Scope AllUsers
Install-Module -Name Az.DesktopVirtualization -RequiredVersion 5.4.1 -Scope AllUsers
Install-Module -Name Az.Resources -RequiredVersion 8.1.0 -Scope AllUsers
Install-Module -Name Az.Automation -RequiredVersion 1.11.1 -Scope AllUsers
Install-Module -Name Az.Network -RequiredVersion 7.19.0 -Scope AllUsers
```

Re-run

```
get-module -ListAvailable Az.Accounts,Az.Compute,Az.DesktopVirtualization,Az.Resources,Az.Automation,Az.Network
```

You should see all six required modules.

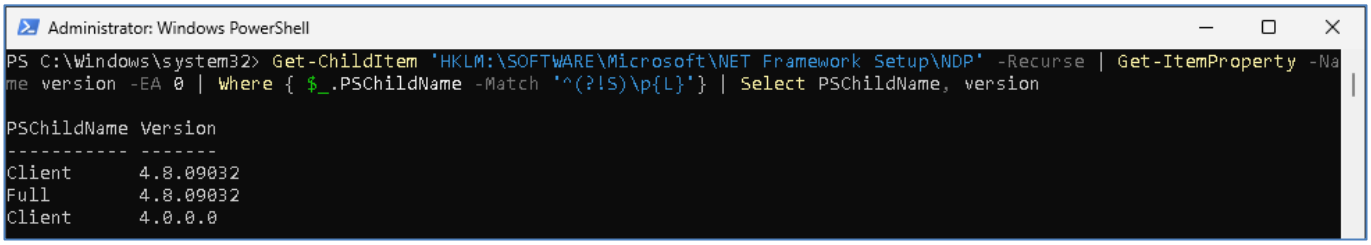


Check the .Net Framework Version

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.



If you want to delete Active Directory Computer accounts when modifying or deleting a Scale Set, install the **ActiveDirectory** PowerShell Module.

Desktop O/S

```
Add-WindowsCapability -Online -Name Rsat.ActiveDirectory.DS-LDS.Tools
```

Server OS

```
Add-WindowsFeature -Name RSAT-AD-PowerShell
```

4.4 Install AVDManage

- Download AVDManage from www.chawn.com/downloads/AVDManage2.zip
- Extract the MSI installer from the zip file.
- Install AVDManage.msi as an Administrator

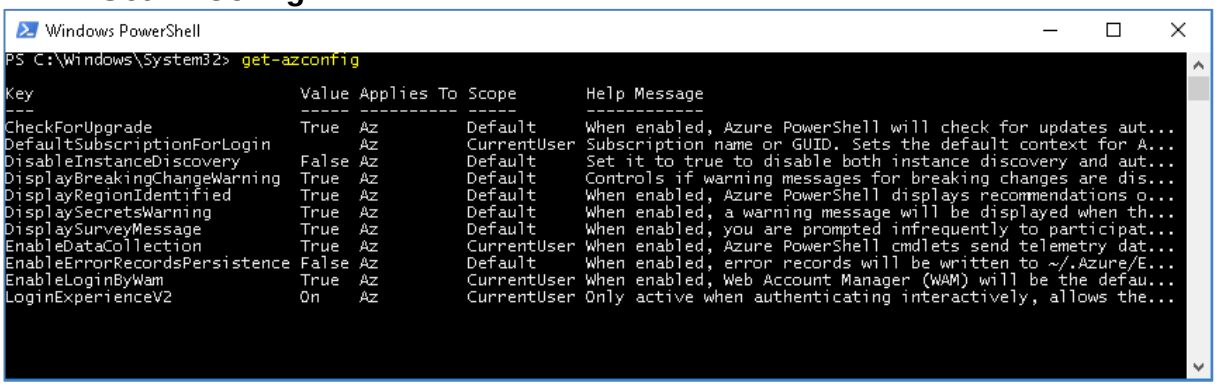
4.4.1 Silent Installation

AVDManage may be installed silently using the following command.

msiexec /i AVDManage.msi COMPANYNAME="Company Name" /qb

4.4.2 Authentication

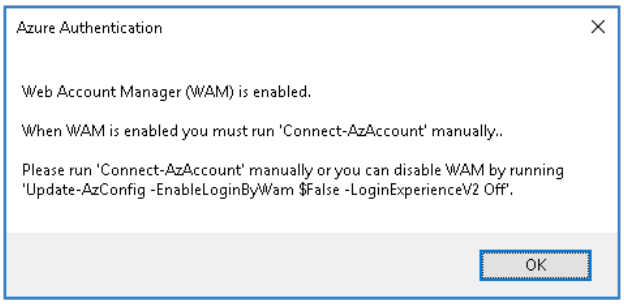
Before authenticating, check your Azure PowerShell Configuration by running
Get-AZConfig



If EnableLoginByWAM and LoginExperienceV2 are enabled, you will need to run
Connect-AzAccount
to authenticate to Azure before launching AVDManage.

You can disable EnableLoginByWAM and LoginExperienceV2 by running
Update-AzConfig -EnableLoginByWam $false -LoginExperienceV2 Off
to force Web based authentication.

If you do not have a valid Azure Access Token and EnableLoginByWam and LoginExperienceV2 are enabled, you will receive the following message.



If you have a valid Azure Access Token when launching AVDManage, AVDManage will ask if you want to logon as the current user.

Click OK to continue as the current user or click Cancel to launch Azure Browser Authentication and logon as a different account. If authentication is not completed within 2 minutes, AVD Manage will exit. The exit timeout value may be modified in the registry.

[HKEY_LOCAL_MACHINE\SOFTWARE\Chawn\AVDManage\Config]

"LoginTimeout"=120 DWord (Decimal)

4.5 Configure AVDManage

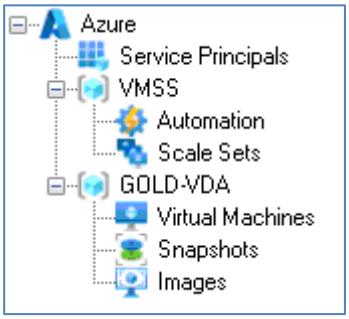
Authenticate to Azure as an Azure Subscription Owner and an Entra Global Administrator

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.

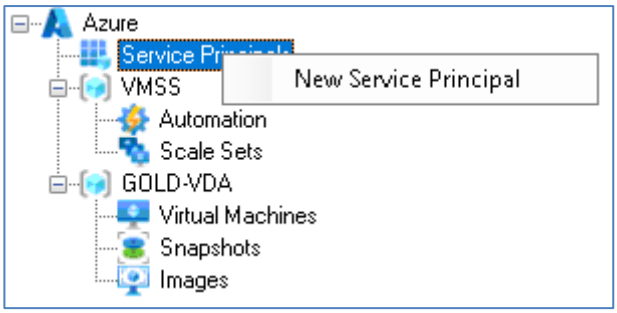
4.6 Create a Service Principal – AVD-Join (Optional)

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

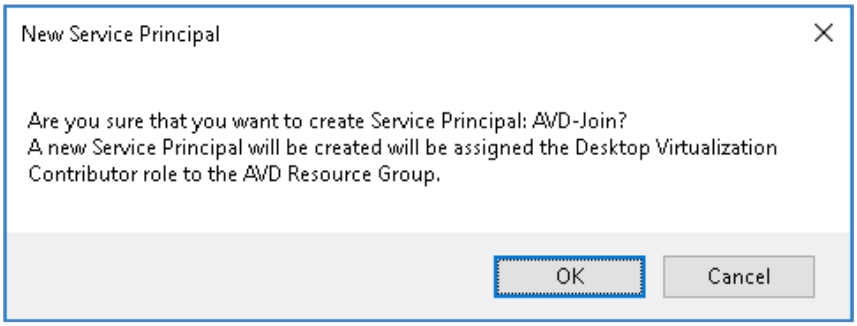
The Azure Service Principal is named **AVD-Join**.

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**

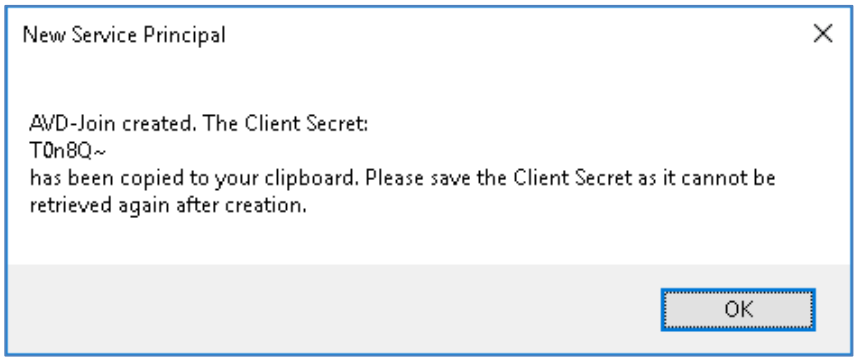


Confirm that you want to create **AVD-Join**

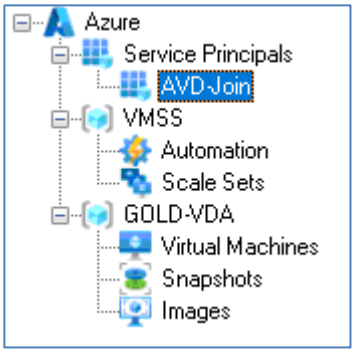


A confirmation message is displayed and the Client Secret is placed onto the clipboard.

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



AVD-Join is created.



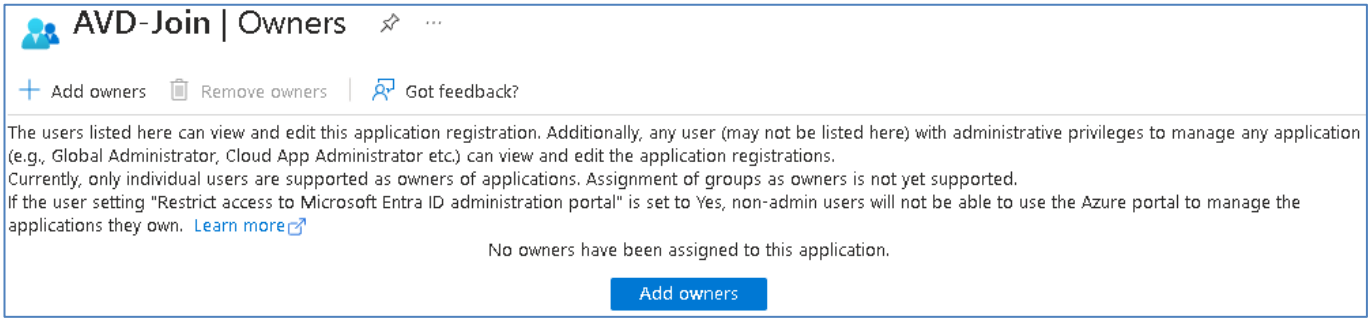
The AppID and Client Secret will be required when creating Scale Sets with **AVD-Join**.

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*.

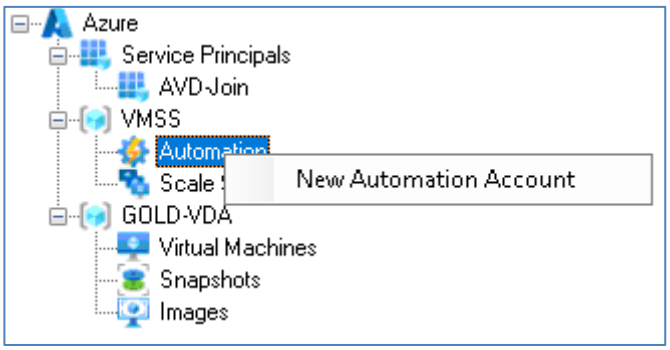


- Add required owners

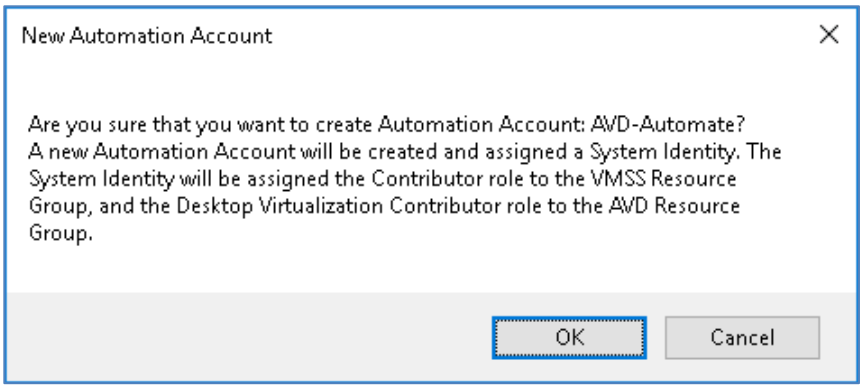
4.7 Create Automation Account – AVD-Automate (Optional)

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.

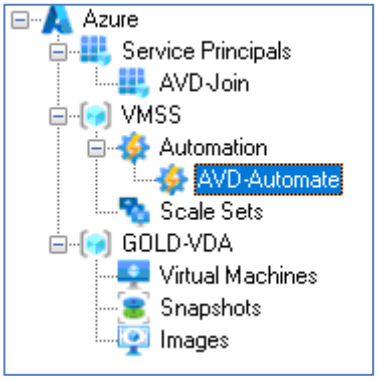


You will be asked to confirm that you want to create an Automation Account named AVD-Automate.



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.



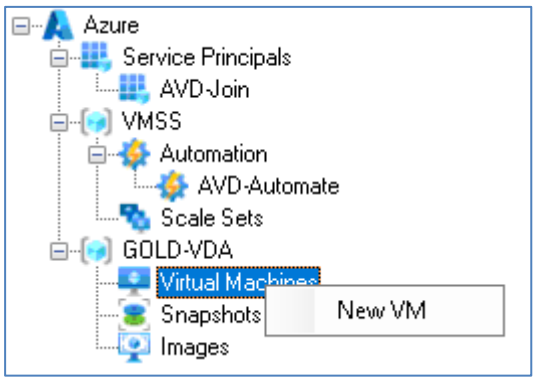
Configuration Complete. **AVD-Admins** can now use all features of AVDManage.

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

5. Create (Master) VM

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

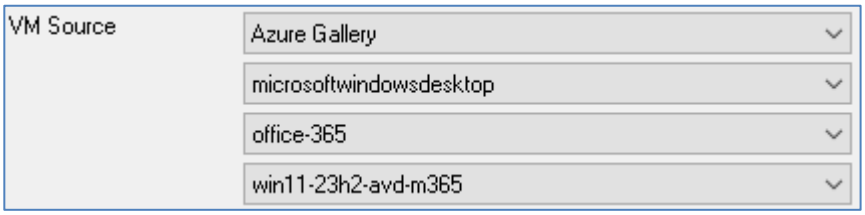
Right click Virtual Machines and select New VM.



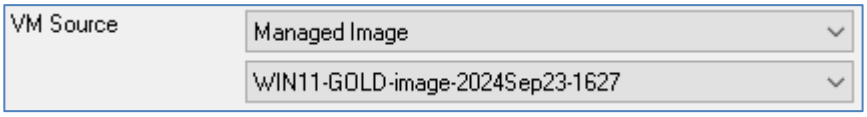
Supply parameters for the following properties.

VM Source

This can be either an Azure Gallery Image,



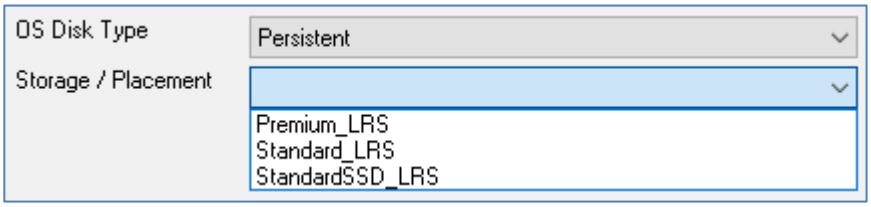
or a Managed Image.



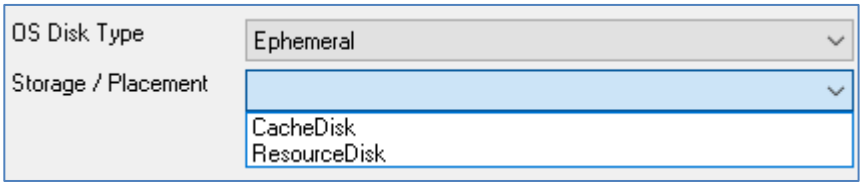
It is recommended that the Master VM is created from an Azure Gallery Image as Microsoft does not recommend deploying a Master VM from a managed image that has been previously sysprepped.

OS Disk Type

This can either be Persistent



or Ephemeral.

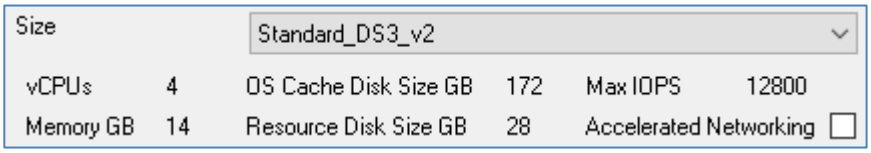


The Master VM must be created using a Persistent OS Disk as VMs with Ephemeral OS Disks cannot be shutdown, sysprepped or used to create Images.

(VM) Size

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

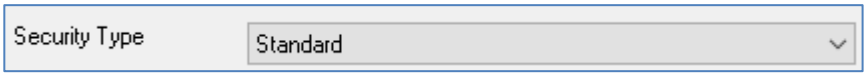
If supported you can enable Accelerated Networking however this is not recommended for Master VMs.



Security Type

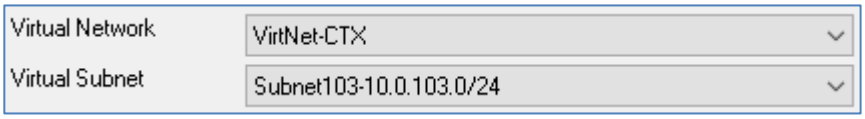
AVDManage (Free) – Security Type is always Standard as Managed Images do not support Trusted Launch.

AVDManage (Plus) – You can choose Trusted Launch however Standard Security is recommended for Master VMs.



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. When 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

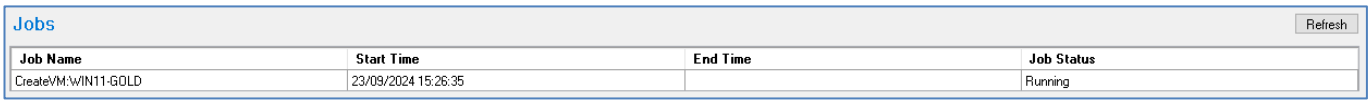
Org Unit: The name of the target AD Organizational Unit in LDAP format

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

Password: Password of the AD User

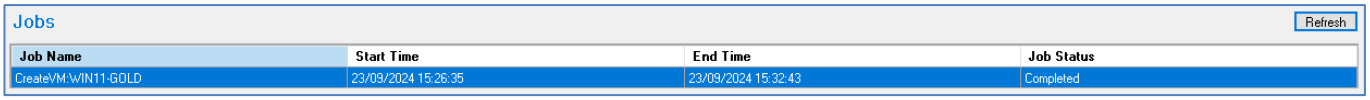
It is not necessary to join an Active Directory Domain however it may simplify access to application resources while building the Master VM. It is recommended that the Master VM is removed from the Active Directory Domain before running sysprep on the Master VM.

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.

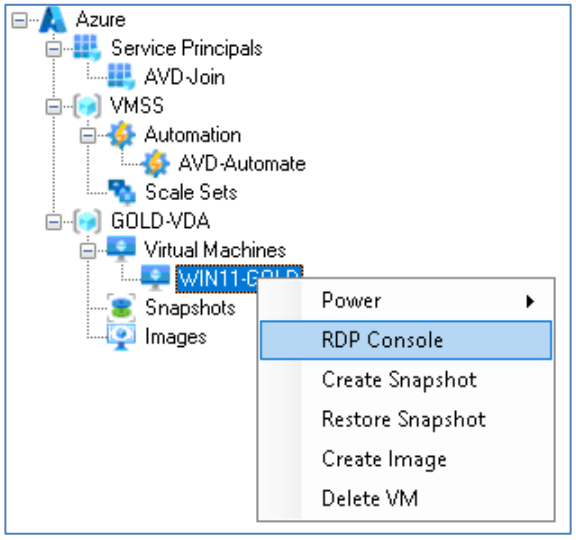
When the job is complete, the Job Status will change to Completed.



Estimated time to complete: 6 mins

5.1 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** or **AVD-Turbo** when deploying a Virtual Machine Scale Set.

If **AVD-Join** or **AVD-Turbo** 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:

- Disable BitLocker
- Add / Remove required Applications and Features
- Remove unwanted Microsoft Store Apps
- Install required Language Packs
- Install all available Windows and Application updates

- Install required Printer Drivers
- Configure the Default User Profile
- Configure Regional Settings – Apply to current and new users
- 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.

AVD-Update may be used to update Windows and primary software.

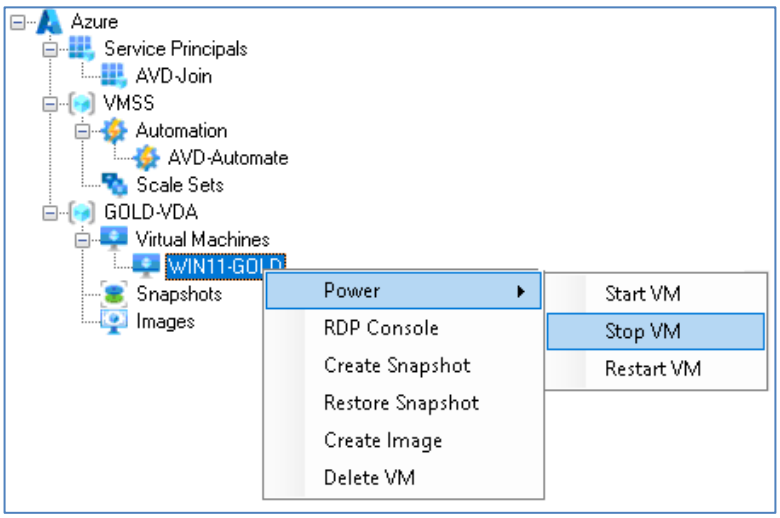
AVD-Optimise may be used to optimise the system.

Alternatively the Virtual-Desktop-Optimization-Tool maybe used to optimize the system.

The following script downloads VDOT, extracts the archive and applies known optimizations.

```
$URI=" https://github.com/The-Virtual-Desktop-Team/Virtual-Desktop-Optimization-Tool/archive/refs/heads/main.zip";Invoke-WebRequest -Uri $URI -OutFile C:\Scripts\VDOT.zip -UseBasicParsing;
Expand-Archive -Path "VDOT.zip" -DestinationPath 'C:\Scripts\VDOT'
cd C:\Scripts\VDOT\Virtual-Desktop-Optimization-Tool-main
.\Windows_VDOT.ps1 -Optimizations All -Verbose
```

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]

[Optimizing Windows configuration for VDI desktops | Microsoft Learn]

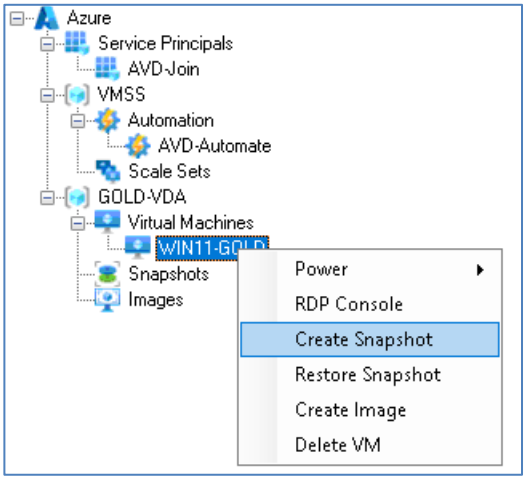
5.2 Snapshot the Master VM

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. The snapshot allows for the original VM to be recreated in the future.

Check the VM status is Deallocated.

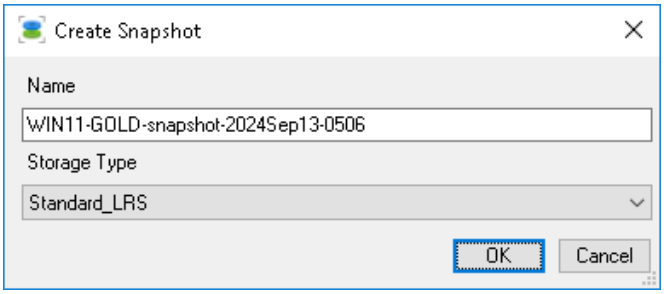
Right click the VM and select Create Snapshot



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.

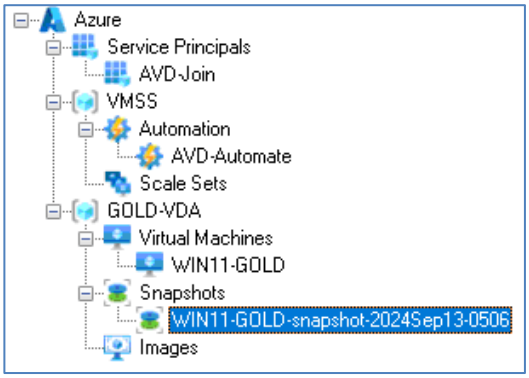


Storage

Select from

- Standard_LRS
- Premium_LRS
- Standard_ZRS

The new Snapshot is displayed under the Snapshots node.



Estimated time to complete: 10-20 seconds

5.3 Sysprep the Master VM

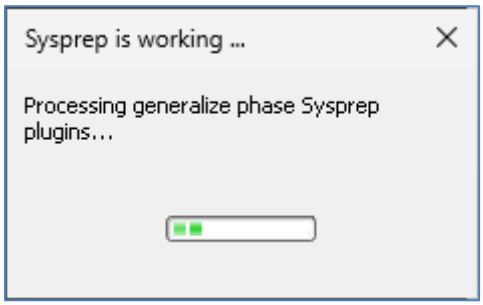
Start the VM.

When the VM is running, connect using 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.

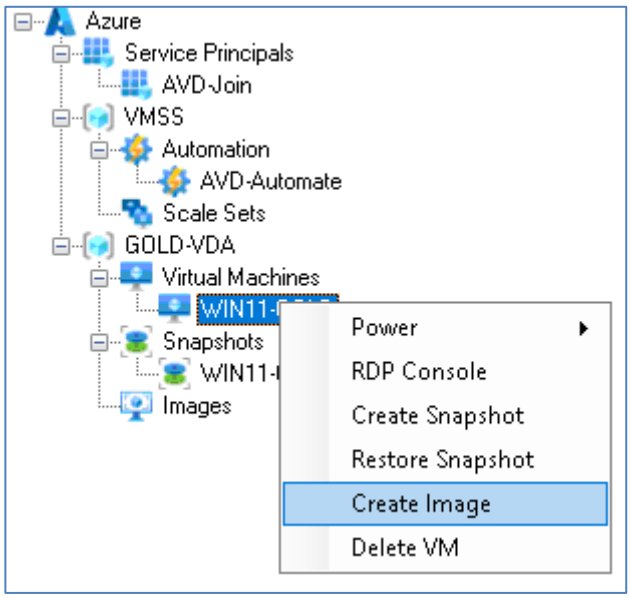
It is recommended that a ***Seal Script*** is used to shut down and sysprep the VM. A seal script can perform tasks that affect the state of the VM.

AVD-Seal may be used as a seal script to prepare the master image and run Sysprep.

5.4 Create Image of the Master VM

Check the VM status is Stopped or Deallocated.

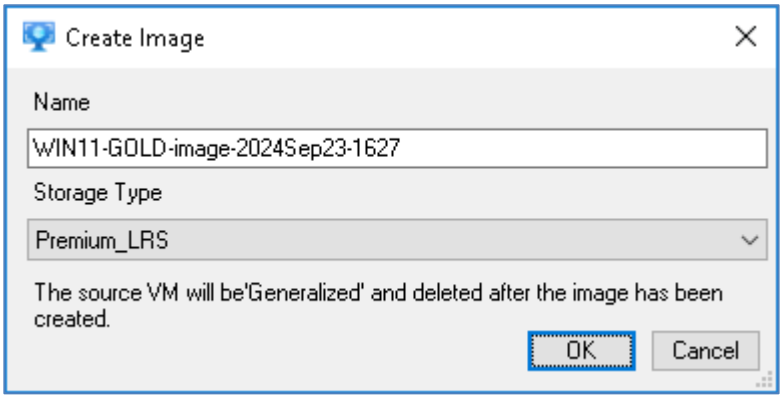
Right click the VM and select Create Image



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.



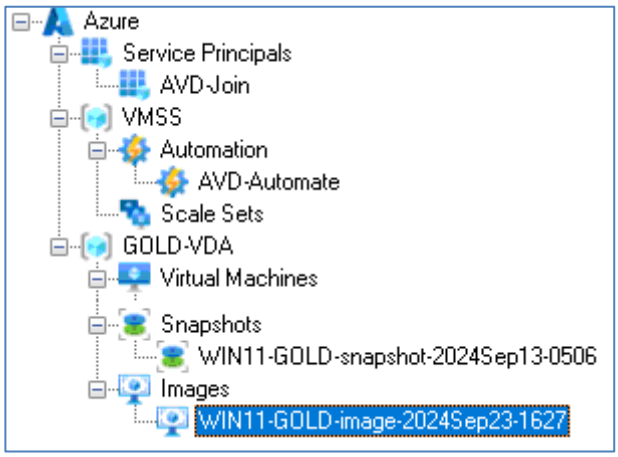
Storage

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.

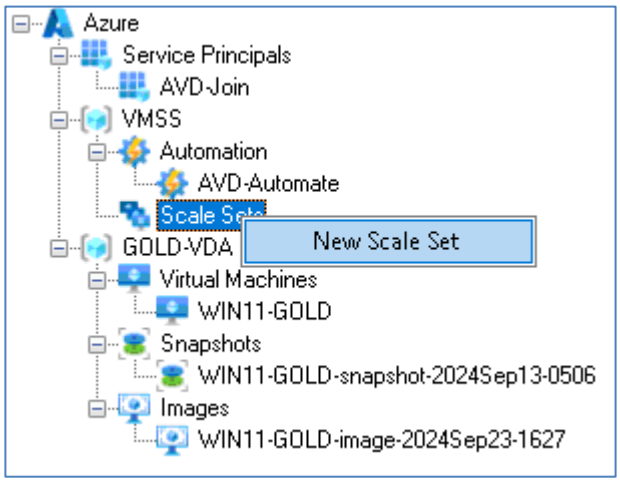
The new Image is displayed under the Images node.



Estimated time to complete: 60 seconds

6. Create a Virtual Machine Scale Set

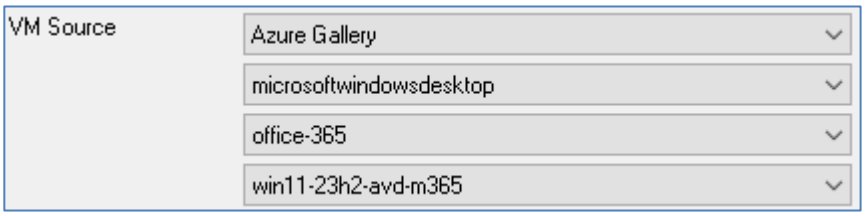
Right Click Scale Sets and select New Scale Set



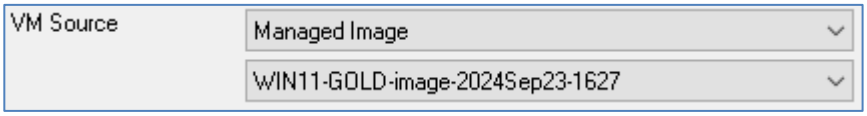
Supply parameters for the following properties.

VM Source

This can be either an Azure Gallery Image,

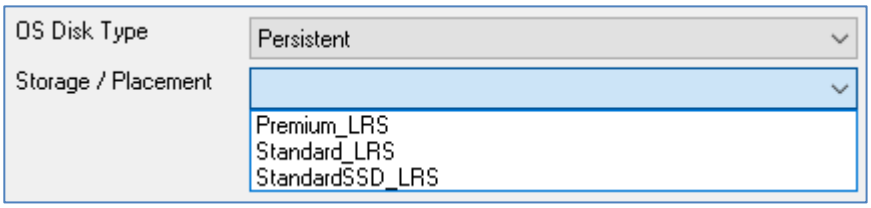


or a Managed Image.

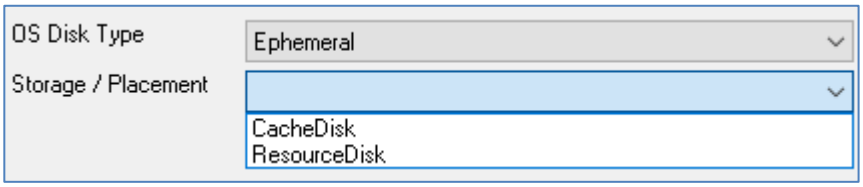


OS Disk Type

This can either be Persistent



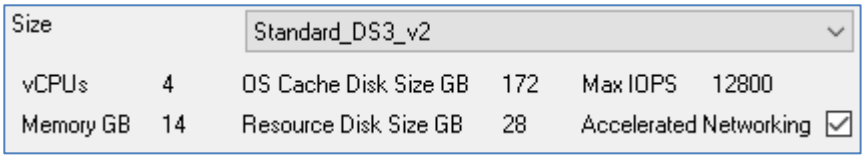
or Ephemeral.



(VM) Size

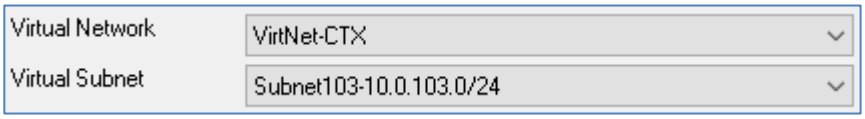
The Size of the VM is filtered based on the OS Disk Type.

If supported you can enable Accelerated Networking.



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)

By default VM instances is set to 1. Reduce to 0 to simply create the Scale Set. You can add VM instances later.

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.

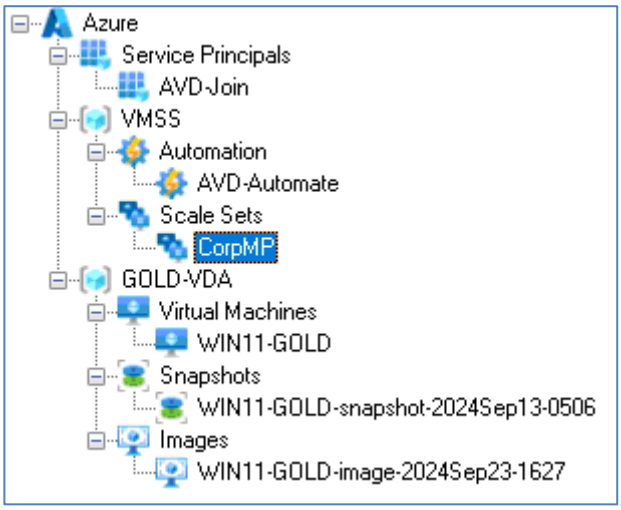
Host Pool: Select a Host Pool name

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: ~8 minutes (5 VM instances)

7. Image Updates

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

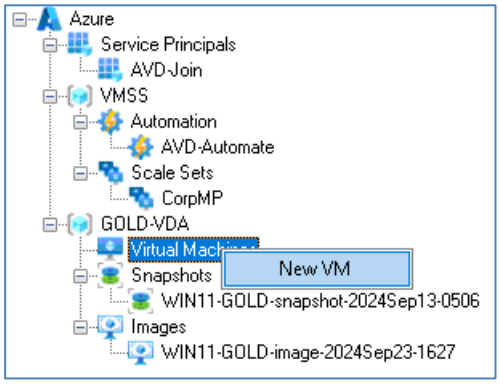
Managed Images will require updating at least once per month.

Updates may include:

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

7.1 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.

Security Type

This is inherited from the Snapshot and may not be adjusted.

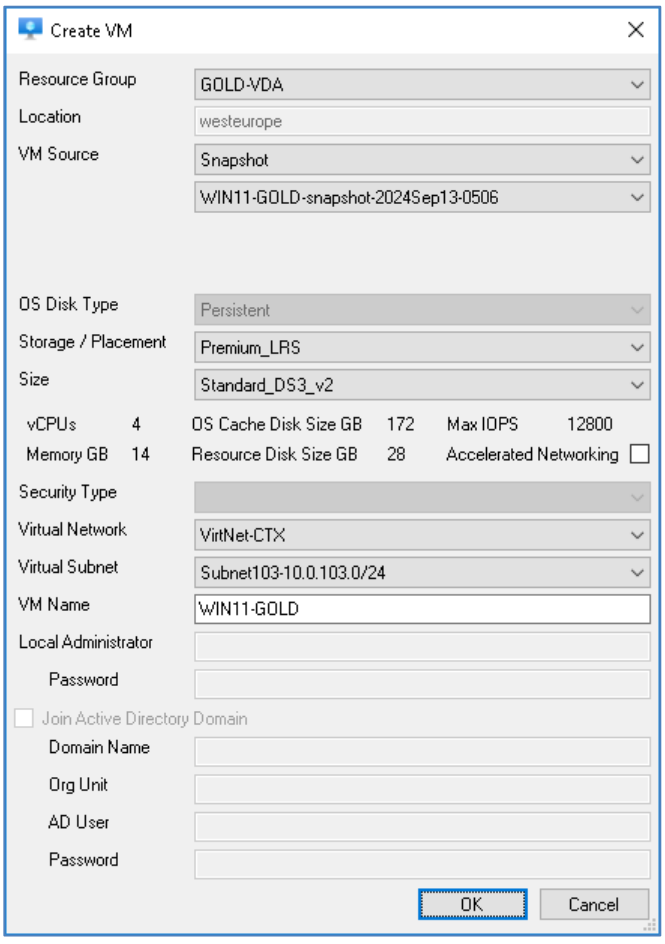
Virtual Network / Virtual Subnet

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.

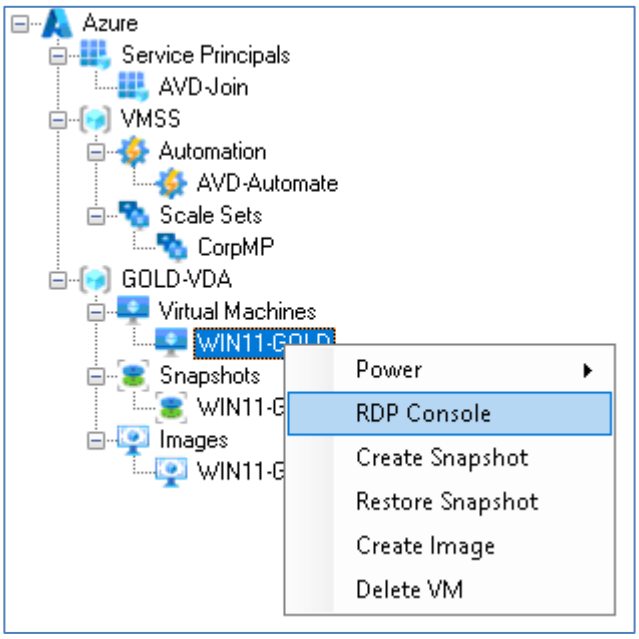
If the Master VM was previously domain joined when the snapshot was created, it will still be domain joined after creation.



Estimated time to complete: 2 minutes

7.2 Modify the Master VM

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

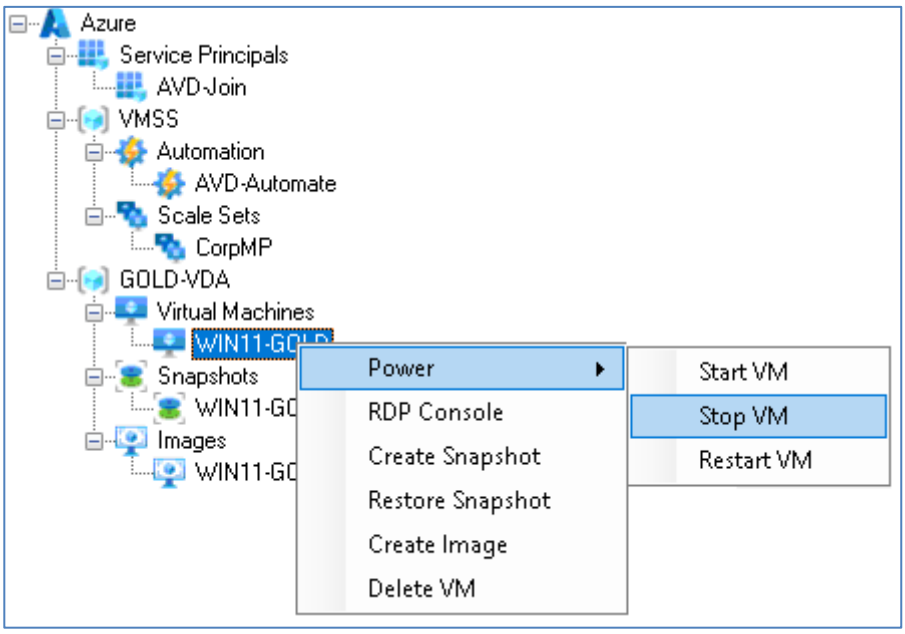


Updates may include:

- 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.



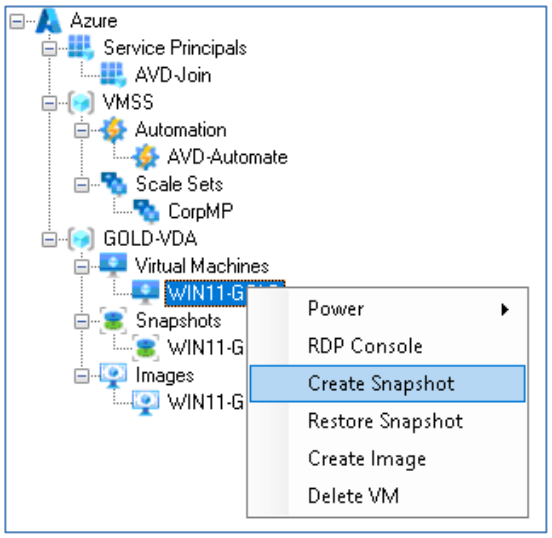
7.3 Snapshot the Master VM

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. The snapshot allows for the original VM to be recreated in the future.

Check the VM status is Deallocated.

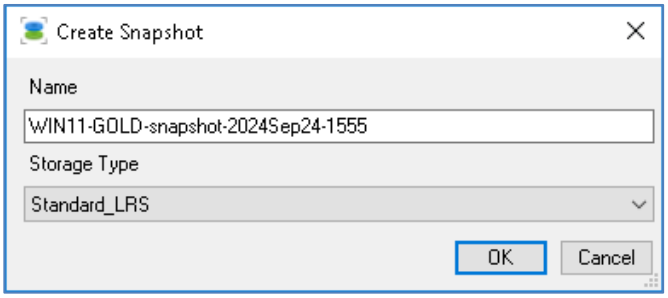
Right click the VM and select Create Snapshot



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.

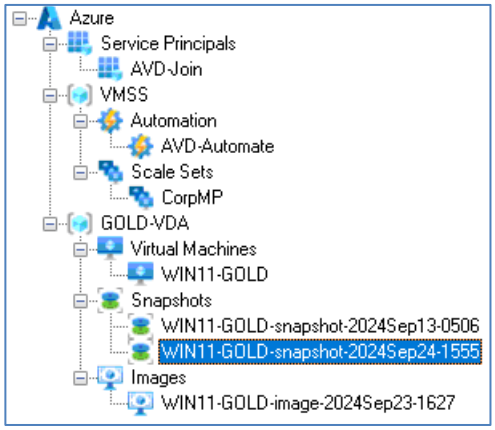


Storage

Select from

- Standard_LRS
- Premium_LRS
- Standard_ZRS

The new Snapshot is displayed under the Snapshots node.



Estimated time to complete: 10-20 seconds

7.4 Sysprep the Master VM

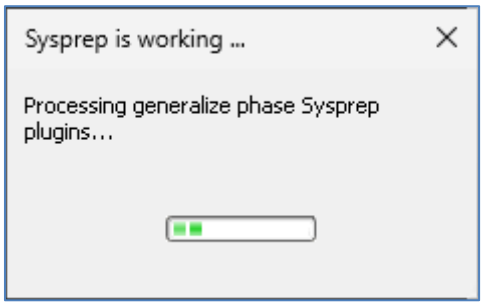
Start the VM.

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

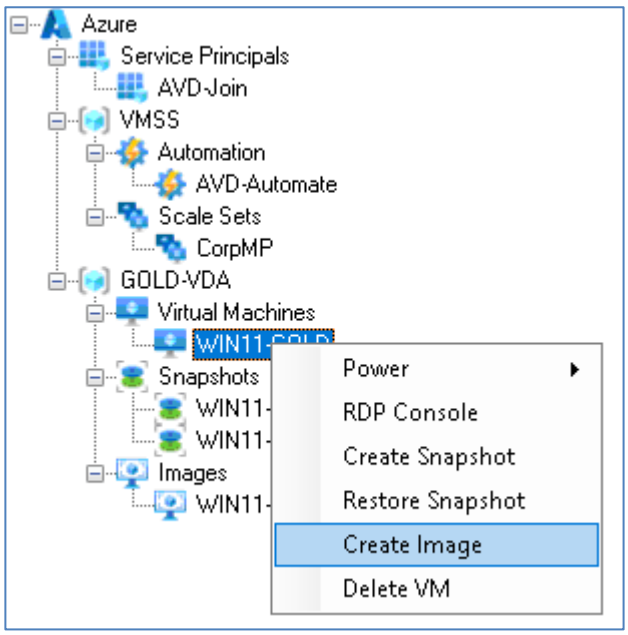


After several minutes the VM will shutdown.
After shutdown, the VM status will be stopped.

7.5 Create Image of the Master VM

Check the VM status is Stopped or Deallocated.

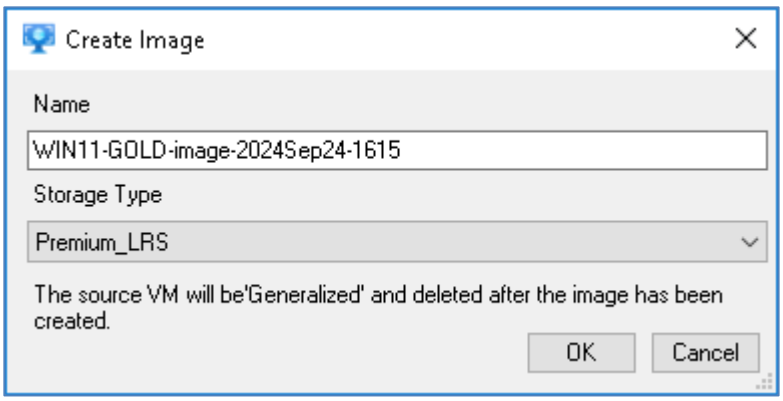
Right click the VM and select Create Image



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.



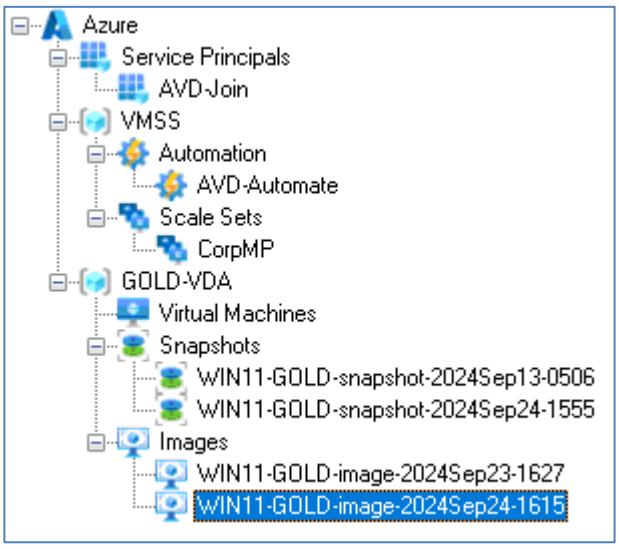
Storage

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.



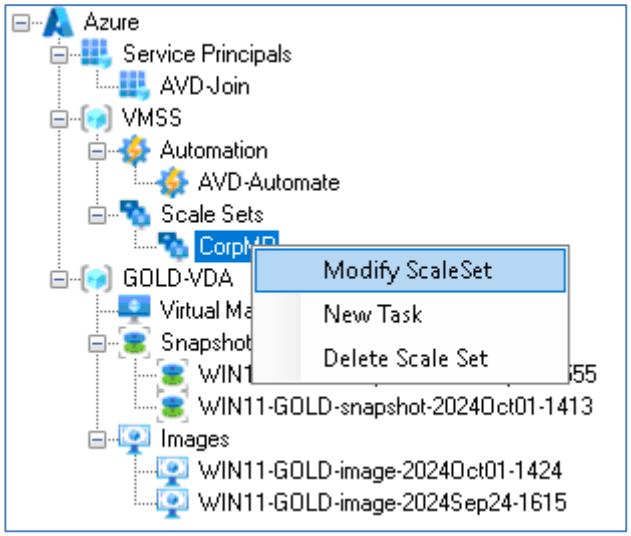
Estimate time to complete: 60 seconds

8. 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.

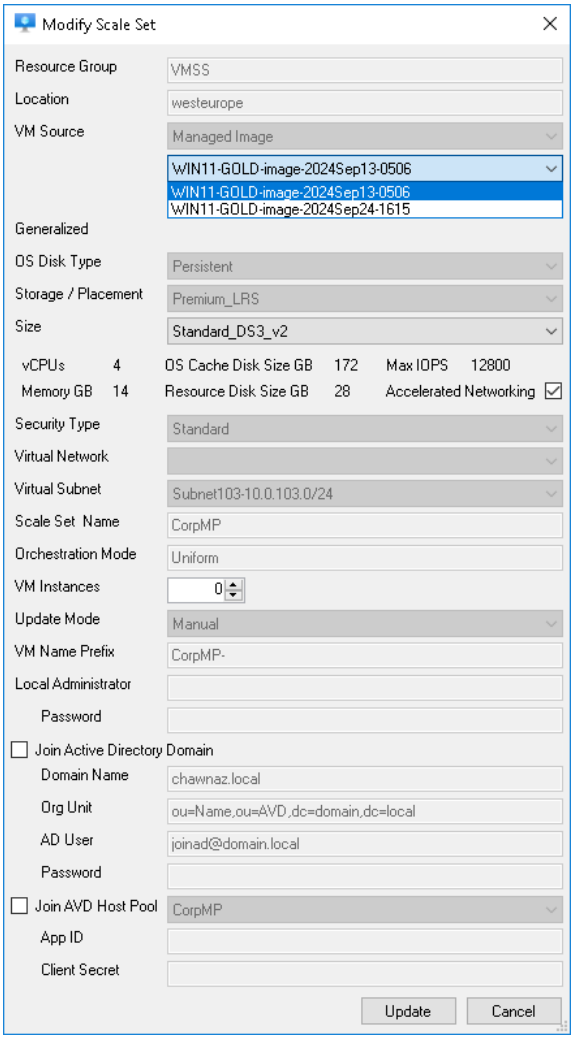
Right click the Scale Set and select Modify Scale Set.



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.



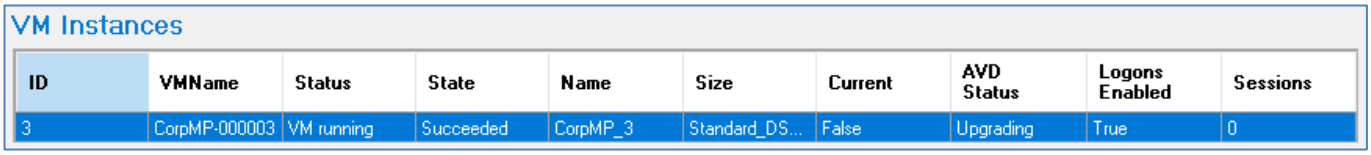
If the Scale Set is configured to Join Active Directory, you can update the AD User and Password.

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.

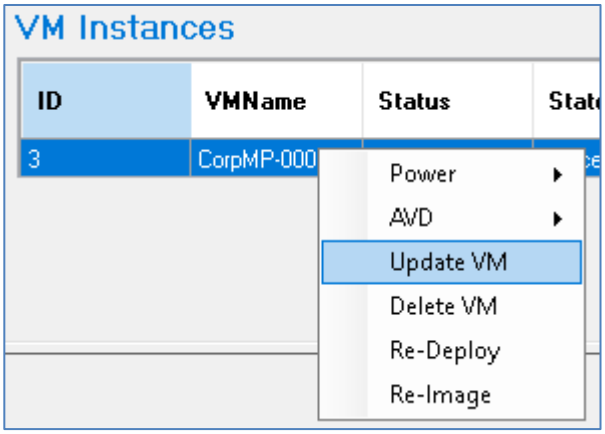
If you do not select the checkbox, the Join AVD configuration remains the same.

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.



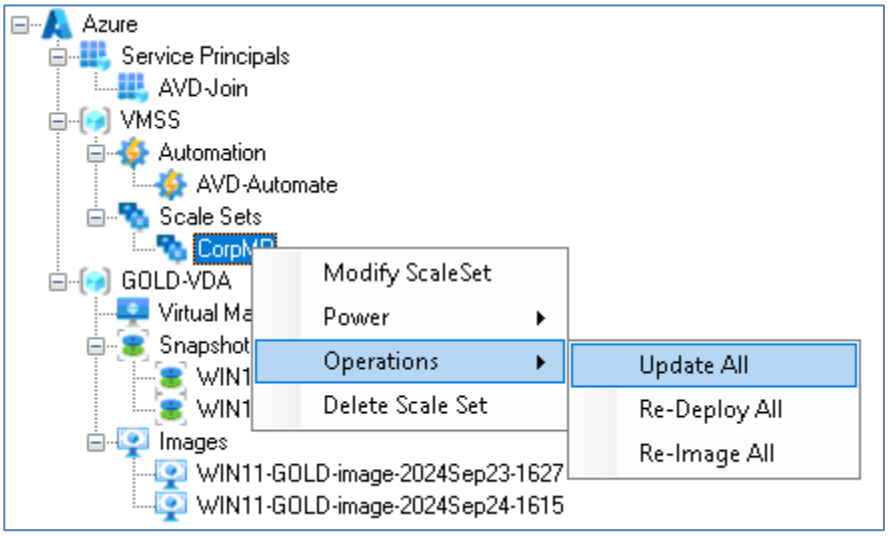
A specific VM instance may be updated by right clicking the VM and selecting update.

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.

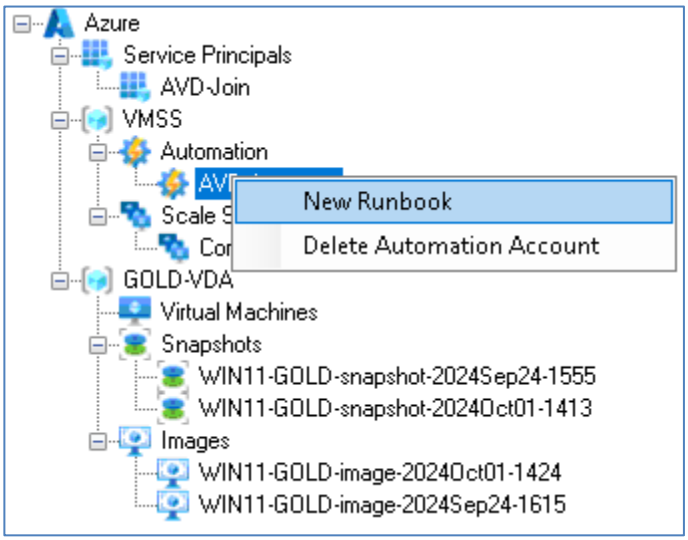
Immediate updating of VMs is unlikely to be appropriate if the VMs are hosting AVD sessions.

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

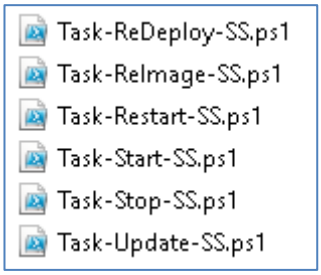
8.1 Create Update Runbook

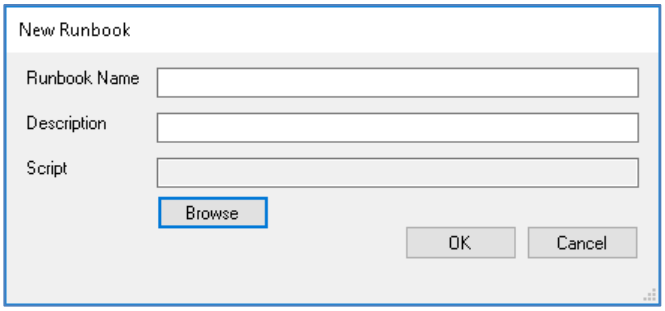
Task-Update-SS.ps1 is used to create an Automation Task that updates all the VM Instances at the same time during a planned maintenance window. The VMs will be re-deployed with the new Scale Set configuration such as an updated Image.

Right Click AVD-Automate and select New Runbook.



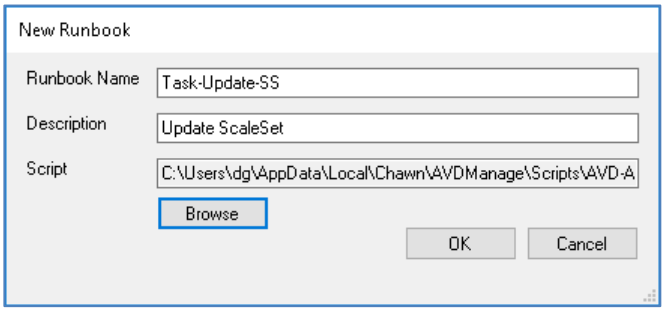
Click Browse and select a Runbook script.



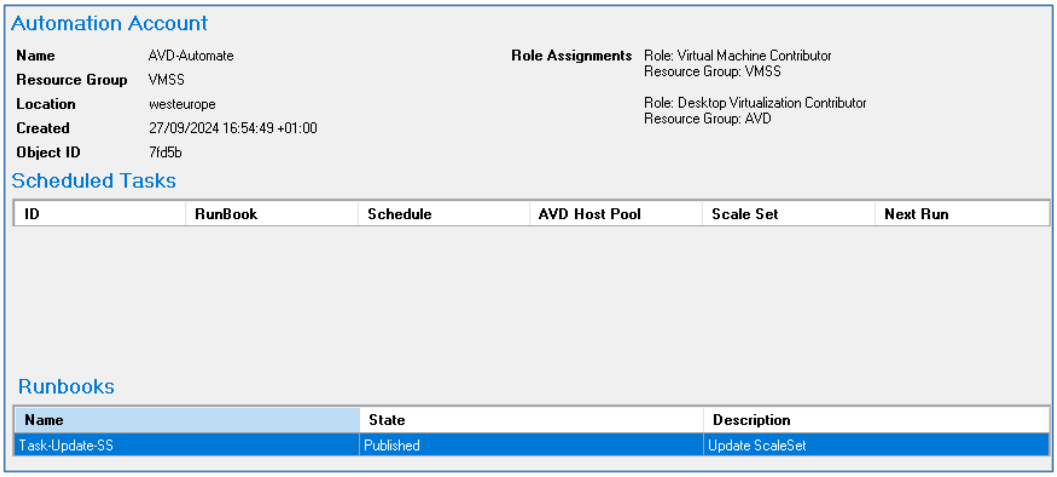


The Runbook name and Description are auto-filled but may be modified.

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

8.2 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

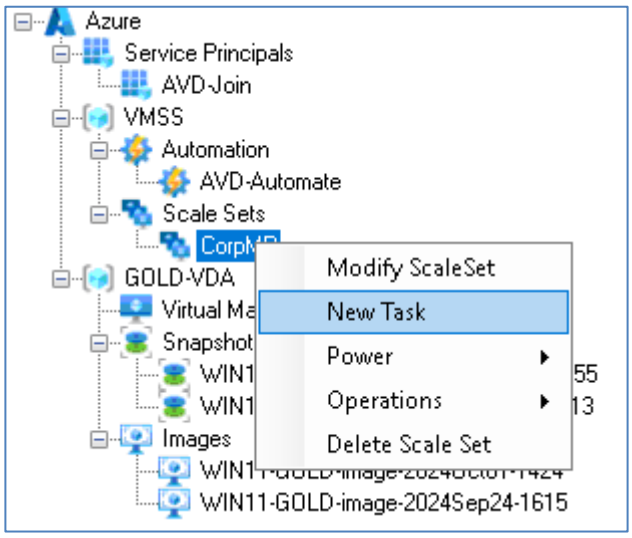
Parameters:

Target Scale Set Name: CorpMP

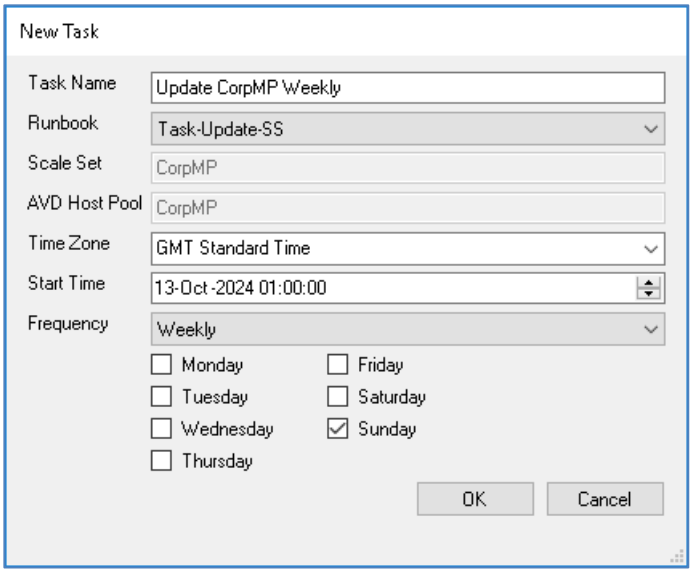
Target AVD Host Pool: CorpMP

Schedule: Weekly. Every Sunday at 1am

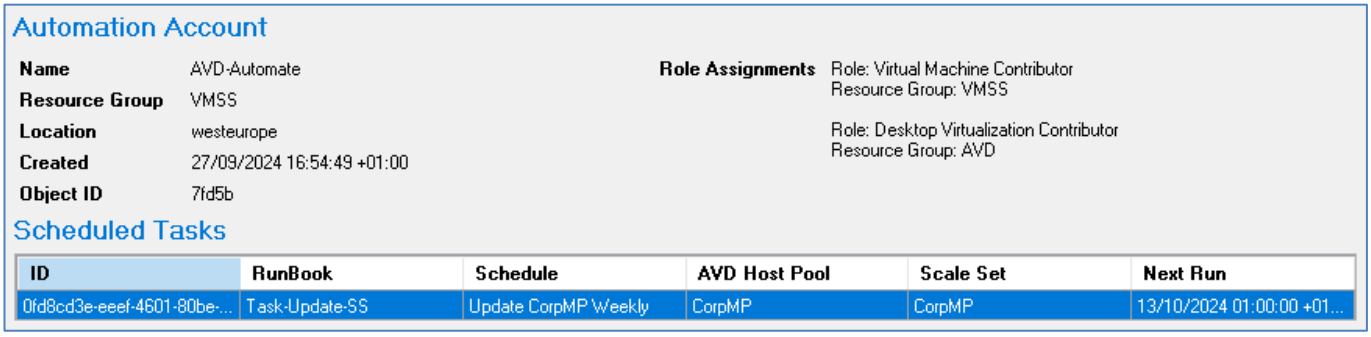
Right Click a Scale Set and select New Task.



- 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.

9. AVDManage Plus

AVDManage Plus has the same configuration requirements as AVDManage Free as described in Getting Started.

9.1 Azure Permissions

As noted in Resource Groups & Roles, the AVD-Admins group requires the ***Compute Gallery Artifacts Publisher*** role to the Virtual Machines Resource Group. Compute Galleries, Image Definitions and Image versions are located in the Virtual Machines Resource Group.

9.2 Licensing

AVDManage Plus is enabled with a 30 days evaluation license or a full annual license.

To request a 30 days evaluation license, email info@chawn.com stating:

- Contact Name
- Contact Details
- Company Name

You will receive a 30 days evaluation license file and registration code.

The license file may then be copied to the installation folder (C:\Program Files\Chawn\AVDManage). Users will be prompted for a registration code at the next launch.

9.3 Additional Features

AVDManage Plus leverages Azure Compute Galleries to provide the following features:

- Create Virtual Machines & Scale Sets from Compute Galleries
- Create Virtual Machines in any Resource Group in the base Location
- Deploy Specialized Windows Images
- Create Trusted Launch Virtual Machines & Scale Sets
- AVDTurbo (for Specialized Virtual Machines & Scale Sets)

> Generalizing or deprovisioning a VM is not necessary for creating an image in an Azure Compute Gallery unless you specifically want to create an image that has no machine specific information, like user accounts. Generalizing is still required when creating a managed image outside of a gallery.
>
> Generalizing removes machine specific information so the image can be used to create multiple VMs. Once the VM has been generalized or deprovisioned, you need to let the platform know so that the boot sequence can be set correctly.

Deprovision or generalize a VM before creating an image - Azure Virtual Machines | Microsoft Learn

> **Important**
>
> When you create a new VM from a specialized image, the new VM retains the computer name of the original VM. Other computer-specific information, like the CMID, is also kept. This duplicate information can cause issues. When copying a VM, be aware of what types of computer-specific information your applications rely on.

Create a VM from a specialized image version - Azure Virtual Machines | Microsoft Learn

There are two operating system states supported by Azure Compute Gallery. Typically images require that the VM used to create the image has been generalized before taking the image. Generalizing is a process that removes machine and user specific information from the VM. For Linux, you can use waagent `-deprovision` or `-deprovision+user` parameters. For Windows, the Sysprep tool is used.

Specialized VMs haven't been through a process to remove machine specific information and accounts. Also, VMs created from specialized images don't have an `osProfile` associated with them. This means that specialized images will have some limitations in addition to some benefits.

- VMs and scale sets created from specialized images can be up and running quicker. Because they're created from a source that has already been through first boot, VMs created from these images boot faster.
- Accounts that could be used to log into the VM can also be used on any VM created using the specialized image that is created from that VM.
- VMs will have the **Computer name** of the VM the image was taken from. You should change the computer name to avoid collisions.
- The `osProfile` is how some sensitive information is passed to the VM, using `secrets`. This may cause issues using KeyVault, WinRM and other functionality that uses `secrets` in the `osProfile`. In some cases, you can use managed service identities (MSI) to work around these limitations.

Generalized and Specialized Images - Azure Virtual Machines | Microsoft Learn

When deploying specialized images, **AVDTurbo**;

- Renames the Computer to match the VM Name
- Optionally joins and Active Directory Domain
- Optionally joins an Azure Virtual Desktop Host Pool

9.4 Install AVDManage

Run the following command to install AVDManage with a Registration code.

msiexec /i AVDManage.msi COMPANYNAME="Company Name" SERIALBODYTEXT="1234567890" /qb

This prevents users being prompted to enter licensing information.

9.5 Overview

AVDManage Free can deploy VMs and Scale Sets from Managed Images only. Managed Images must be Generalized. Managed Images do not support:

- Specialized Images
- TrustedLaunch security

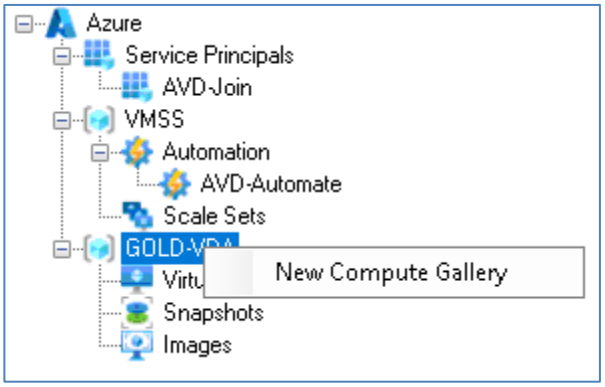
AVDManage Plus can deploy VMs and Scale Sets from Managed Images and Azure Compute Galleries. Azure Compute Galleries support Generalized and Specialized Images and TrustedLaunch security.

Create an Azure Compute Gallery		
Create an Image Definition (Generalized or Specialized)		
Create a Master VM		
	Generalized	**Specialized**
	Shutdown the VM and take a Snapshot	Run AVD-Seal-Special.ps1. **VM will shutdown**
	Power on the VM and run AVD-Seal.ps1 or Sysprep. **VM will shutdown**	Snapshot the VM
	Create a Generalized Compute Gallery Image Version	Create a Specialized Compute Gallery Image Version
Create a Virtual Machine Scale Set using the Image Version		

9.6 Create an Azure Compute Gallery

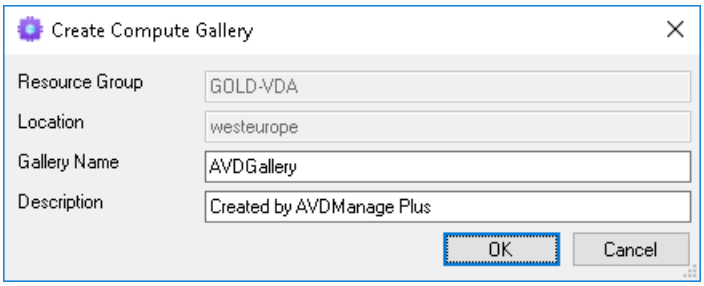
The user performing these tasks should be a member of **AVD-Admins**.

Right click the Master Resource Group and select New Compute Gallery.



Name the Gallery and optionally provide a description.

Click OK.



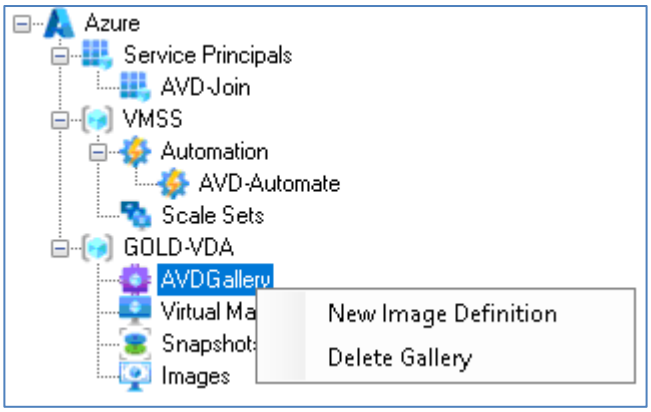
Estimated time to complete: 60 seconds

9.7 Create an Image Definition

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

9.7.1 Specialized Image Definition

Right Click the Compute Gallery and select New Image Definition.

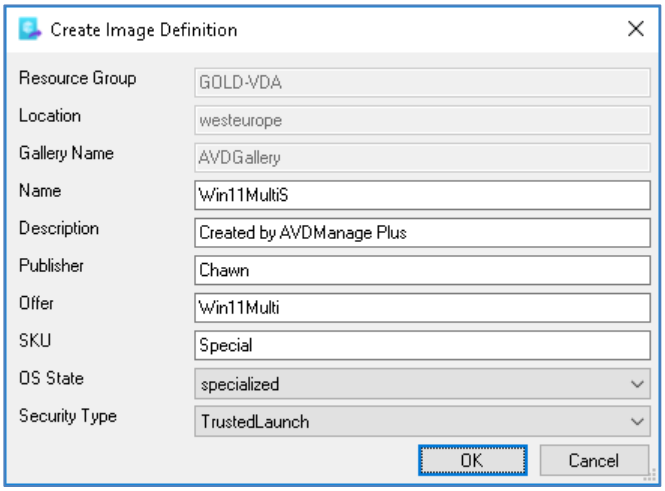


Enter a name and optionally provide a description.

Enter a Publisher, Offer and SKU.

Specify the intended OS State.

Specify the Security Type for VMs deployed from this Image Definition.

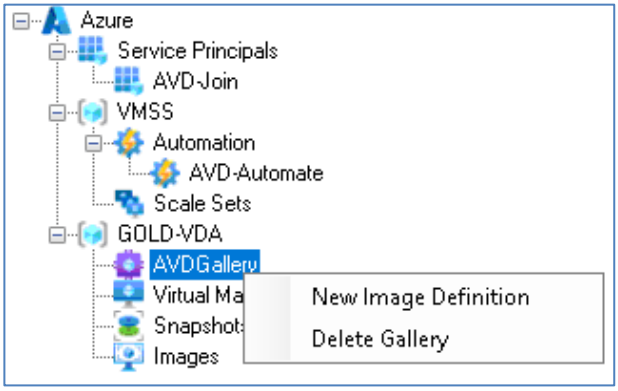


When creating Image Definitions, the Publisher, Offer and SKU combination cannot be the same as any other Image Definition in the Gallery.

Estimated time to complete: 60 seconds

9.7.2 Generalized Image Definition

Right Click the Compute Gallery and select New Image Definition.

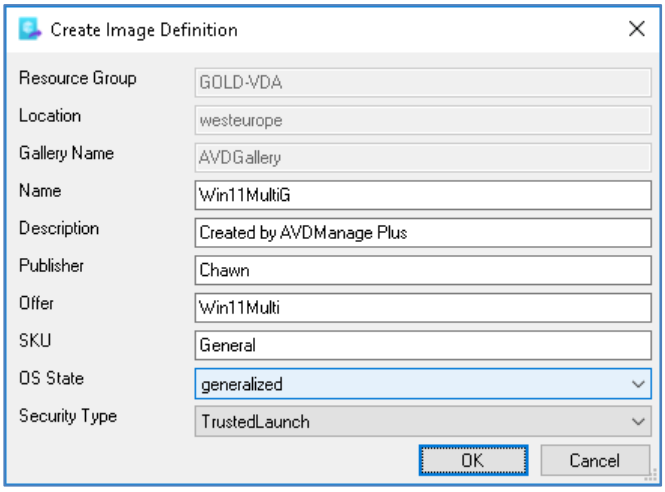


Enter a name and optionally provide a description.

Enter a Publisher, Offer and SKU.

Specify the intended OS State.

Specify the Security Type for VMs deployed from this Image Definition.



When creating Image Definitions, the Publisher, Offer and SKU combination cannot be the same as any other Image Definition in the Gallery.

Estimated time to complete: 60 seconds

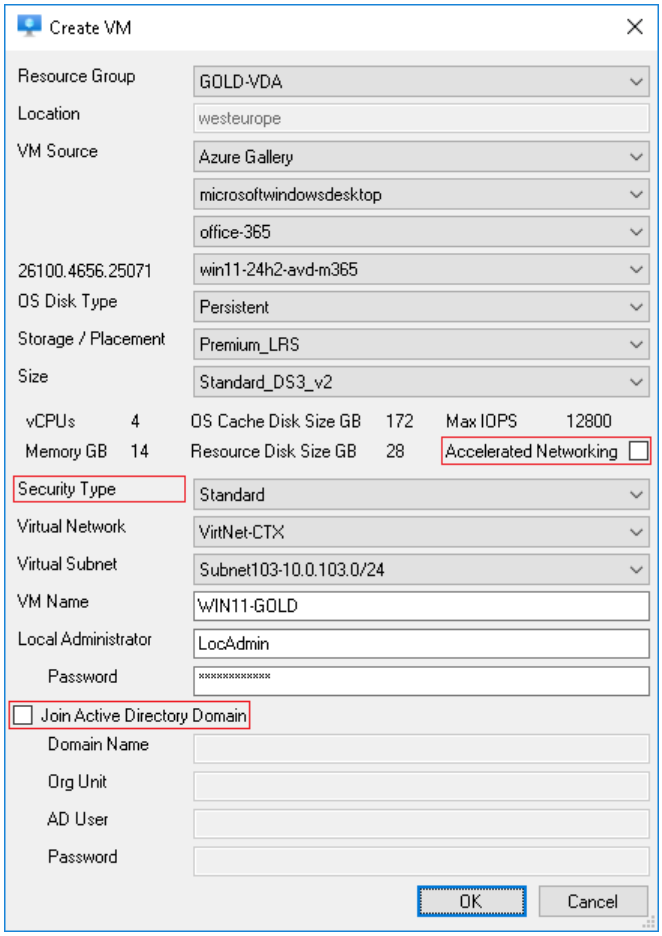
9.8 Create (Master) VM

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

Recommendations:

- Record the local administrator password. It will be required when recreating the Master VM from snapshots and if deploying Specialized images.
- Use the same VM Size that will be used by the Virtual Machine Scale Set.
- The OS Disk Type must be Persistent.
- Don't join an Active Directory Domain
- Don't enable Accelerated Networking. This can be enabled when creating a Virtual Machine Scale Set. If Accelerated Networking is enabled in the Master VM, all Scale Set VM instances will have a ghost Mellanox network adapter.
- Don't enable TrustedLaunch security.
    - A Standard security VM may be added to a Compute Gallery Image Definition with Standard or TrustedLaunch security however a TrustedLaunch security VM cannot be added to Compute Gallery Image Definition with Standard security.
    - TrustedLaunch can be enabled when creating a Virtual Machine Scale Set
    - Windows 11 24H2 now enables Bitlocker by default. This is not required in a Master VM and prevents Sysprep from completing

Create a VM from the Azure Gallery.



Estimated time to complete: 6 mins

Modify the VM as described in Modify the Master VM

Depending on your imaging and deployment strategy, either Generalize the Master VM by running Sysprep or shut down the Master VM for a specialized image.

It is important that the Windows Azure Agent is neutralised when creating a specialized image. A new Virtual Machine configuration file is created at the next startup which includes the Virtual Machine name. **AVDTurbo** uses the latest configuration file to set the computername correctly.

Whether generalizing or specializing the Master VM, AVD-Seal.ps1 and AVD-Seal-Special.ps1 contain the following commands to remove previous Azure Guest Agent configuration files.

```
# Neutralise the WindowsAzure Agent
Get-Service -Name WindowsAzureGuestAgent | stop-service
Get-ChildItem -Path C:\WindowsAzure\config -Filter *.*  | Remove-Item -Force
```

Generalized Image	**Specialized Image**
Shutdown the VM and **take a Snapshot**	Run AVD-Seal-Special.ps1. **VM will shutdown**
Power on the VM and run AVD-Seal.ps1 or Sysprep. **VM will shutdown**	**Take a Snapshot**
Create a Generalized Compute Gallery Image Version	Create a Specialized Compute Gallery Image Version

9.9 Create a Compute Gallery Image Version

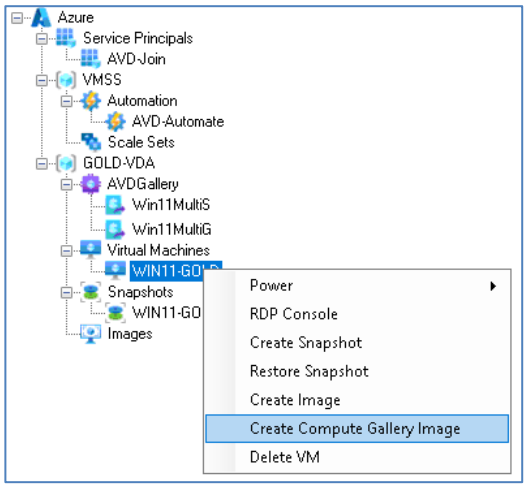
The user performing these tasks should be a member of **AVD-Admins**.

Before creating an Image Version or deleting the Master VM, ensure that you have taken a snapshot.

9.9.1 Specialized Image

Before creating the Image Version, ensure that you have run AVD-Seal-Special.ps1 and the VM has shutdown.

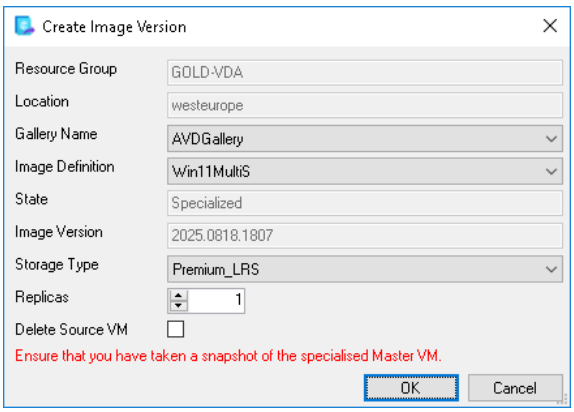
Right click the Master VM and select Create Compute Gallery Image.



Select the Compute Gallery.

Select the Image Definition. The image definition will indicate if it is intended for Specialized or Generalized deployments.

The Name is automatically created based on yyyy.MMdd.hhmm.



Select the Storage Type.

Microsoft recommend that you have 1 replica for every 20 VMs that you intend to deploy. E.g. 100 VMs would require 5 replicas.

Choose whether to delete the Source VM.

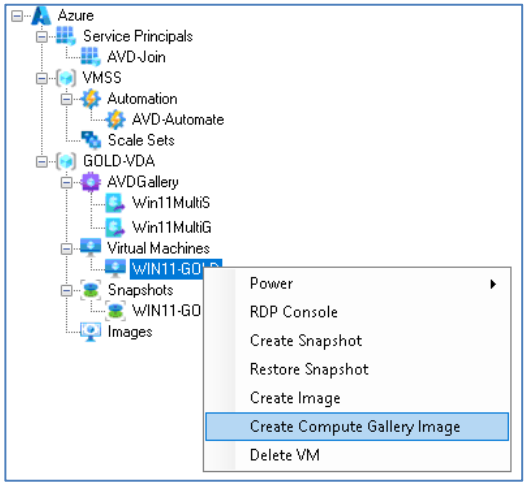
Click OK.

Estimated time to complete: 15 Minutes (Depending on the number of replicas)

9.9.2 Generalized Image

Before creating the Image Version, ensure that you have Generalized the Master VM by running Sysprep and the VM has shutdown.

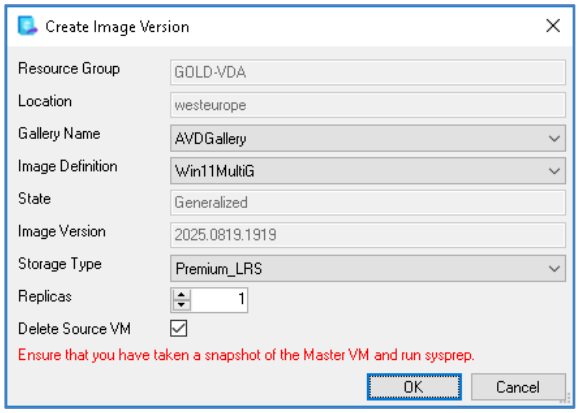
Right click the Master VM and select Create Compute Gallery Image.



Select the Compute Gallery.

Select the Image Definition. The image definition will indicate if it is intended for Specialized or Generalized deployments.

The Name is automatically created based on yyyy.MMdd.hhmm.



Select the Storage Type.

Microsoft recommend that you have 1 replica for every 20 VMs that you intend to deploy. E.g. 100 VMs would require 5 replicas.

Choose whether to delete the Source VM.

Click OK.

When creating a Generalized Image, the Master VM is marked as ‘Generalized’ and therefore cannot be started afterwards.

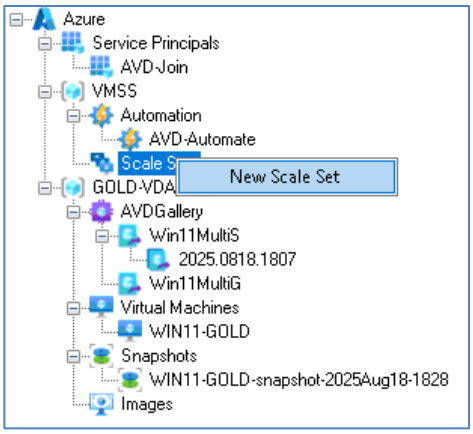
Estimated time to complete: 15 Minutes (Depending on the number of replicas)

9.10 Create a Virtual Machine Scale Set

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

9.10.1 Specialized Image

Right click the Scale Sets node and select New Scale Set.



Select Compute Gallery as the source.

Select your Azure Compute Gallery, Image Definition, and Image Version.

Select OS Disk Type, Storage / Placement and VM Size.

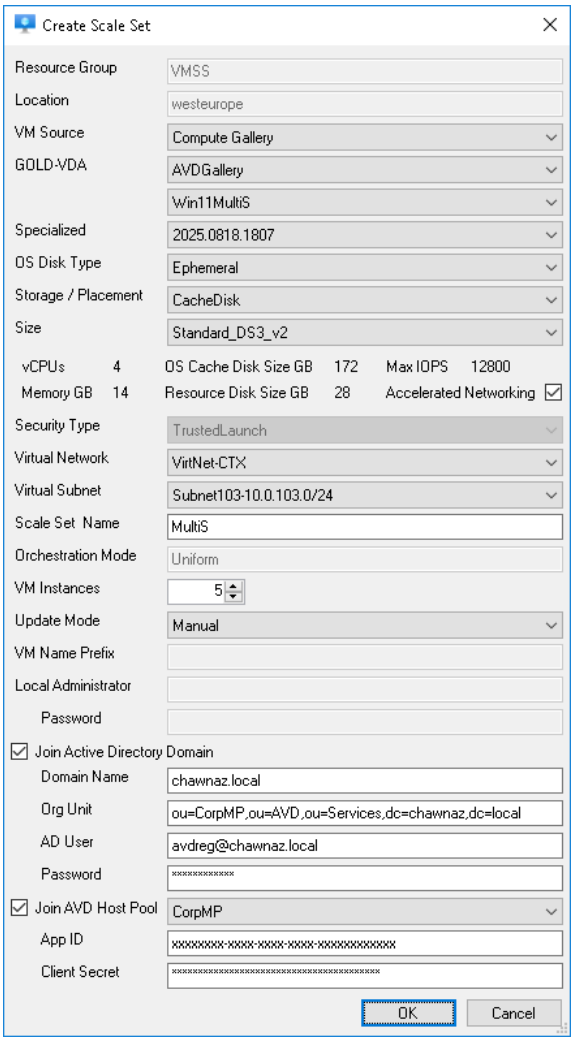
Security Type is inherited from the Image Definition.

Select the number of required VMs.

Update Mode is set to Manual by default but may be changed to Automatic.

VM Name Prefix is not configurable for a Specialized Image. The VM Name Prefix is based on the Scale Set name. The Scale Set name is limited to 11 characters which allows for a minimum of 9999 available VM names.

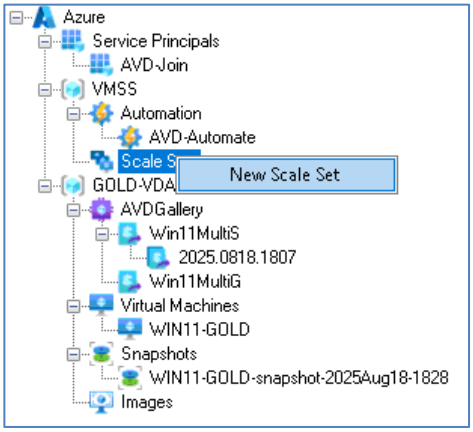
For more available VM Names, use a shorter Scale Set Name.



Estimated time to complete: ~4 Minutes (5 VM instances)

9.10.2 Generalized Image

Right click the Scale Sets node and select New Scale Set.



Select Compute Gallery as the source.

Select your Azure Compute Gallery, Image Definition, and Image Version.

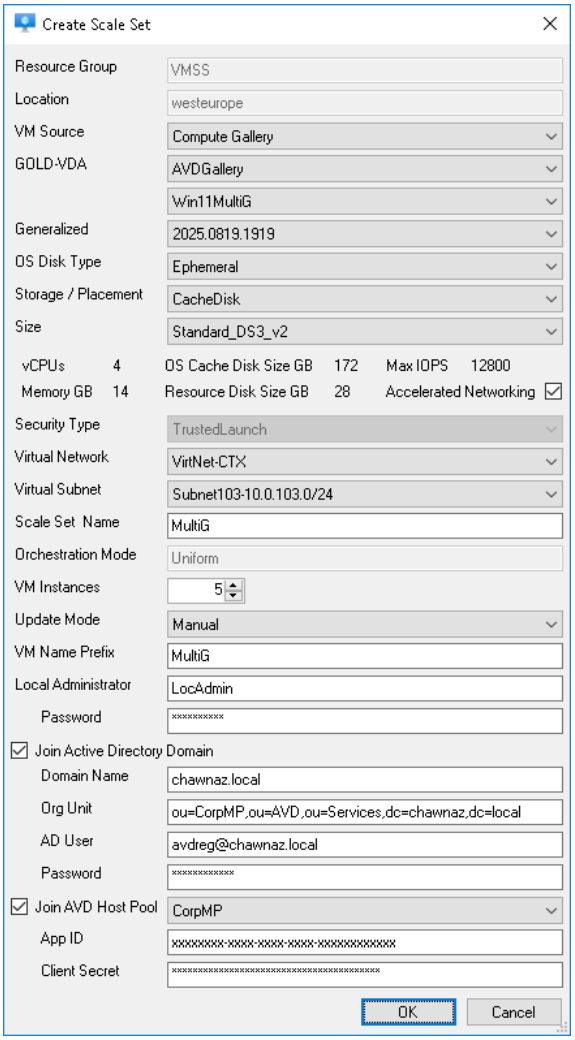
Select OS Disk Type, Storage / Placement and VM Size.

Security Type is inherited from the Image Definition.

Select the number of required VMs.

Update Mode is set to Manual by default but may be changed to Automatic.

VM Name Prefix is limited to 9 characters which allows for over 16 million available VM Names.



Estimated time to complete: ~7 Minutes (5 VM instances)

9.11 Image Updates

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

Images require updating at least once per month.

Recreate the Master VM as described in Recreate the Master VM.

Modify the Master VM.

Updates may include:

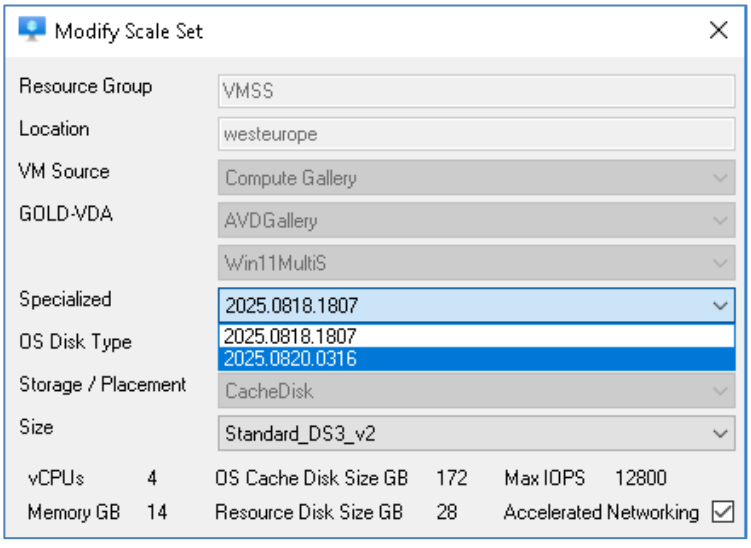
- Windows Updates
- Application Updates
- Add / Remove Applications
- Fixes to discovered issues

Depending on your image strategy

Generalized Image	Specialized Image
Shutdown the VM and **take a Snapshot**	Run AVD-Seal-Special.ps1. **VM will shutdown**
Power on the VM and run AVD-Seal.ps1 or Sysprep. **VM will shutdown**	**Take a Snapshot**
Create a Generalized Compute Gallery Image Version	Create a Specialized Compute Gallery Image Version

Update a Scale Set

Right Click a Scale Set and select **Modify Scale Set**.

The new Image Version may be selected to update the Scale Set. The VM Size, Accelerated Networking and VM instances may be modified if required. The password for the Active Directory user may be updated. The Client Secret for Azure Virtual Desktop may be updated.	

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.

10. AVD-Prep - Pre-Stage the Remote Desktop Infrastructure and Boot Loader Agents

A typical deployment time for AVD-Join and AVD-Turbo is around 1 minute 45 seconds.

This includes 45 seconds while installing the Remote Desktop Infrastructure and Boot Loader Agents.

By pre-staging the Agents on the Master VM, the deployment time can be reduced accordingly.

The Agents may be pre-staged on a Generalized or Specialized Image.

Re-Create the Master VM from a snapshot.

Logon and download AVD-Prep.ps1

Open Powershell as Administrator and run AVD-Prep.ps1.

The script will:

- Download and Install Az.Accounts and Az.DesktopVirtualization Powershell Modules
- Download the Remote Desktop Infrastructure and Boot Agents to C:\Source
- Install the Remote Desktop Infrastructure Agent with an INVALIDTOKEN
- Install the Remote Desktop Boot Loader Agent
- Stop and Disable the Remote Desktop Boot Loader Agent Service
- Delete HKLM:\SOFTWARE\Microsoft\RDInfraAgent
- Create HKLM:\SOFTWARE\Microsoft\RDInfraAgent\RegistrationToken ="AVDTurbo"
- Create HKLM:\SOFTWARE\Microsoft\RDInfraAgent\HostPoolType = "Default"
- Create HKLM:\SOFTWARE\Microsoft\RDInfraAgent\IsRegistered= 0

Complete the Image update process.

	Generalized	**Specialized**
	Shutdown the VM and take a Snapshot	Run AVD-Seal-Special.ps1. **VM will shutdown**
	Power on the VM and run AVD-Seal.ps1 or Sysprep. **VM will shutdown**	Snapshot the VM
	Create a Generalized Compute Gallery Image Version	Create a Specialized Compute Gallery Image Version

When AVD-Turbo or AVD-Join run, they check for HKLM:\SOFTWARE\Microsoft\RDInfraAgent\RegistrationToken ="AVDTurbo".

If it is present, the script immediately passes the WVDRegistration token into the VM's registry and starts the Remote Desktop Boot Loader Agent.

The WinSXS Network and Geneva Agents will then be downloaded and installed.

If pre-staging the Remote Desktop Infrastructure and Boot Loader Agents ensure that you run AVD-Prep.ps1 during every update so that the latest versions of the Agents are present in the Master Image.

11. Reference

11.1 Virtual Machines

Only Microsoft Windows Virtual Machines may be created.

Virtual Machines may be created from:

- Azure Gallery Images
- Compute Gallery Images (AVDManage Plus)
- Managed Images
- Snapshots

11.1.1 Configuration

All Virtual Machines have the following configuration.

PublicIP	None
BootDiagnostics.Enabled	False
HyperVGeneration	V2
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.		

11.1.2 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.

11.1.3 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. The VM must be in a stopped or deallocated state. (Persistent only)
Create Compute Gallery Image	AVDManage Plus. Creates a Compute Gallery Image Version. The VM may be generalized or specialized. The VM must be in a stopped or deallocated state. (Persistent only)
Delete VM	Deletes the VM, Disk and NIC

11.2 Virtual Machine Scale Sets

Only Microsoft Windows Virtual Machines can be created.

Virtual Machine Scale Sets may be created from:

- Azure Gallery Images
- Compute Gallery Images (AVDManage Plus)
- Managed Images

11.2.1 Orchestration Mode

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

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

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

11.2.2 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

11.2.3 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 does not 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.

11.2.4 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 can be considered as ‘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 OS 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.

11.2.5 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

When deleting a Scale Set or Scale Set VM instances, the Azure Virtual Session Desktop Session Host instance is also deleted.

If DeleteAD is enabled and the ActiveDirectory Powershell module is installed, the Active Directory Computer object may also be deleted.

11.3 AVD-Join Service Principal

AVD-Join is an Entra Service Principal. It can be viewed as an App Registration and Enterprise Application in the Azure portal.

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** or **AVD-Turbo** can be configured as a Microsoft Azure CustomScriptExtension.

The following parameters are included:

AVD-Join	AVD-Turbo
• AVD Host Pool to join • AVD-Join AppID • AVD-Join Client Secret • Entra Tenant ID • Azure Subscription ID	• AD Domain • AD Organisational Unit • AD Admin User • AD Admin Password • AVD Host Pool to join • AVD-Join AppID • AVD-Join Client Secret • Entra Tenant ID • Azure Subscription ID

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

After a Generalized VM has joined an Active Directory Domain, AVD-Join will download

https://raw.githubusercontent.com/ChawnLimited/AVDManage/refs/heads/main/AVD-Join.ps1

AVD-Join.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, if not will attempt to install them
- 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
- Waits for the Windows SXS Network and Geneva Health agents to install
- Disconnects from Azure

AVD-Join.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**

After a Specialized VM has started up, AVD-Turbo will download

https://raw.githubusercontent.com/ChawnLimited/AVDManage/refs/heads/main/AVD-Turbo.ps1

AVD-Turbo.ps1

- Renames the Computer
- Joins Active Directory
- Checks that the Microsoft RDS Infrastructure Agent is not already installed
- Checks that the VM is domain joined
- Checks required PS Modules are present, if not will attempt to install them
- 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
- Waits for the Windows SXS Network and Geneva Health agents to install
- Disconnects from Azure
- Reboots

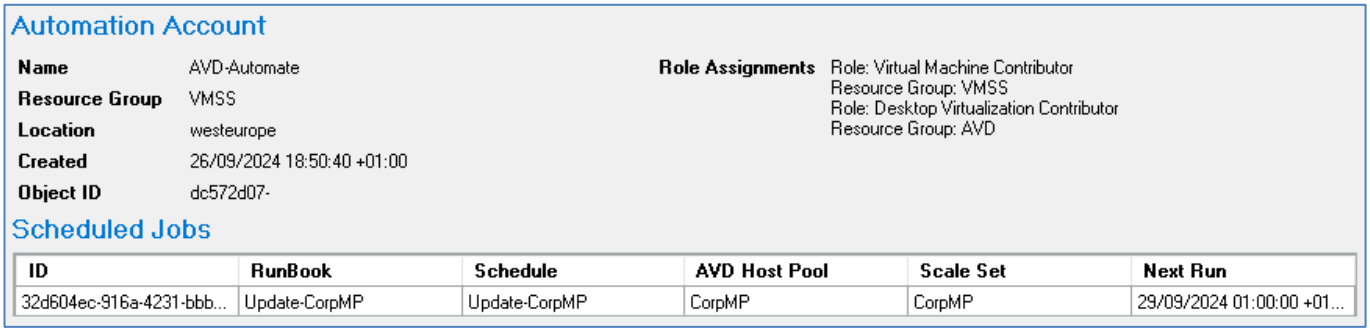
CustomScriptExtension logs and RDS Agent installation logs are located in

C:\WindowsAzure\Logs\Plugins\Microsoft.Compute.CustomScriptExtension\x.x.x

11.3.1 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 removes the Role assignments

11.4 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.

11.4.1 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

11.5 Snapshots

Snapshots will accumulate over time and incur storage costs.

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

11.5.1 Menu Actions

Delete Snapshot	Deletes the Snapshot

11.6 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.

11.6.1 Menu Actions

Delete Image	Deletes the Image

11.7 PowerShell

Minimum PowerShell Version: 5.1

11.7.1 Module Installation for AVDManage

Install minimal PowerShell Modules for AVDManage.

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

If prompted to install the the Nuget Provider, type Y

```
Uninstall-module -name Az.Accounts -AllVersions
Uninstall-module -name Az.Compute -AllVersions
Uninstall-module -name Az.DesktopVirtualization -AllVersions
Uninstall-module -name Az.Resources -AllVersions
Uninstall-module -name Az.Automation -AllVersions
Uninstall-module -name Az.Network –AllVersions

Install-Module -Name Az.Accounts -RequiredVersion 5.2.0 -Scope AllUsers
Install-Module -Name Az.Compute -RequiredVersion 10.2.0 -Scope AllUsers
Install-Module -Name Az.DesktopVirtualization -RequiredVersion 5.4.1 -Scope AllUsers
Install-Module -Name Az.Resources -RequiredVersion 8.1.0 -Scope AllUsers
Install-Module -Name Az.Automation -RequiredVersion 1.11.1 -Scope AllUsers
Install-Module -Name Az.Network -RequiredVersion 7.19.0 -Scope AllUsers
```

If you want to delete Active Directory Computer accounts when modifying or deleting a Scale Set, install the ActiveDirectory PowerShell Module.

Desktop O/S

```
Add-WindowsCapability -Online -Name Rsat.ActiveDirectory.DS-LDS.Tools
```

Server OS

```
Add-WindowsFeature -Name RSAT-AD-PowerShell
```

11.7.2 Module Installation for AVD-Join (Master VM)

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

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

If prompted to install the the Nuget Provider, type Y

```
Uninstall-module -name Az.Accounts -AllVersions
Uninstall-module -name Az.DesktopVirtualization -AllVersions

Install-Module -Name Az.Accounts -RequiredVersion 5.2.0 -Scope AllUsers
Install-Module -Name Az.DesktopVirtualization -RequiredVersion 5.4.1 -Scope AllUsers
```

11.8 Verify Installed Modules

```
Get-Module -Name Az.Accounts,Az.Compute,Az.DesktopVirtualization,Az.Resources,Az.Automation,Az.Network -ListAvailable | select name,version
```

Module Installation for AVDManage

11.9 Login Issues

11.9.1 Browser

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

11.9.2 Authenticate Manually

If EnableLoginByWAM and LoginExperienceV2 are enabled, you will need to run
Connect-AzAccount
to authenticate to Azure before launching AVDManage.

You can disable EnableLoginByWAM and LoginExperienceV2 by running
Update-AzConfig -EnableLoginByWam $false -LoginExperienceV2 Off
to force Web based authentication.

11.9.3 Update PowerShell Modules

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

11.10 SysPrep Failure

Error:

> Sysprep was not able to validate your Windows installation. Review the log file at %WINDIR%\System32\Sysprep\Panther\setupact.log for details. After resolving the issue, use Sysprep to validate your installation again.

%WINDIR%\System32\Sysprep\Panther\setupact.log

> ActionPlatform::LaunchModule: Failure occurred while executing 'ValidateBitLockerState' from C:\Windows\System32\BdeSysprep.dll

Bitlocker is enabled on the Master VM. Sysprep cannot run on an encrypted drive.

Run

> **Manage-bde –off C:**

It will take a few minutes for the volume to decrypt. You can check the status of decryption by running

> **Manage-Bde -Status**

When the Drive is fully decrypted, run Sysprep again.

BitLocker overview | Microsoft Learn