Microsoft

Desktop-as-a-Service (DaaS)
Using Windows Virtual Desktop (WVD)

Dynamic Scaling of Host Pools

Prepared for:
Service Provider Partners
Oct. 2019

Prepared by:
Microsoft – **O**ne **C**ommercial **P**artner (OCP)

MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Contents

1. Overview

For many Windows Virtual Desktop Preview deployments in Azure, the virtual machine costs represent a significant portion of the total Windows Virtual Desktop deployment cost. To reduce costs, it's best to shut down and deallocate session host virtual machines (VMs) during off-peak usage hours, then restart them during peak usage hours.

This walkthrough illustrates the required steps for implementing dynamic scaling of host pools within the new Windows Virtual Desktop (WVD) service in Microsoft Azure.

Please be advised this information is provided to help understand/summarize this process and your enterprises` implementation may contain additional customizations and/or settings that **might not** be covered in this document.

2. Prerequisites

Azure & Windows Active Directory Prerequisites

Before getting started, **all** items listed below **must** be checked/validated to ensure the most basic requirements are in place to proceed with executing the remaining steps in this guide.

- A Windows Virtual Desktop tenant with at least 1 host pool.
- A Service Principal with permissions to
    - o query the WVD tenant (such as RDS Contributor.)
    - o the subscription (such as Contributor.)
- Session host pool VMs configured and registered with the Windows Virtual Desktop service.
- A Log Analytics workspace in Azure

General Best Practices

Since everyone's business and technical requirements vary across the board, it is always a good idea to familiarize yourselves with the standard best practices across the different Azure technologies & services.

- Please follow the guidance here to maintain a consistent naming convention across your resources, unless you are already using a naming system.
- Azure security best practices and patterns
- Azure Active Directory Hybrid Identity best practices
- Azure identity management and access control security best practices
- Azure Networking & security Best Practices

- Azure Storage security [overview](#)
- [Best practices for Azure VM security](#)

Azure Networking

The recommendation is to design your Azure Networking using a [Hub-Spoke topology](#). Consider the HUB like a DMZ deployed with your Virtual network Gateways and other security/edge appliances like Firewalls Etc. while the Spoke will act as the backend zone where your session hosts servers are deployed to and is peered with the HUB. This is our design for this walk-through, so you'll need this already setup before proceeding.

Azure Architectural Diagram

Below is a diagram of the Azure environment that we'll use. It shows the objects created in Azure and their relationships within the environment. In this example, the company name will be Contoso.
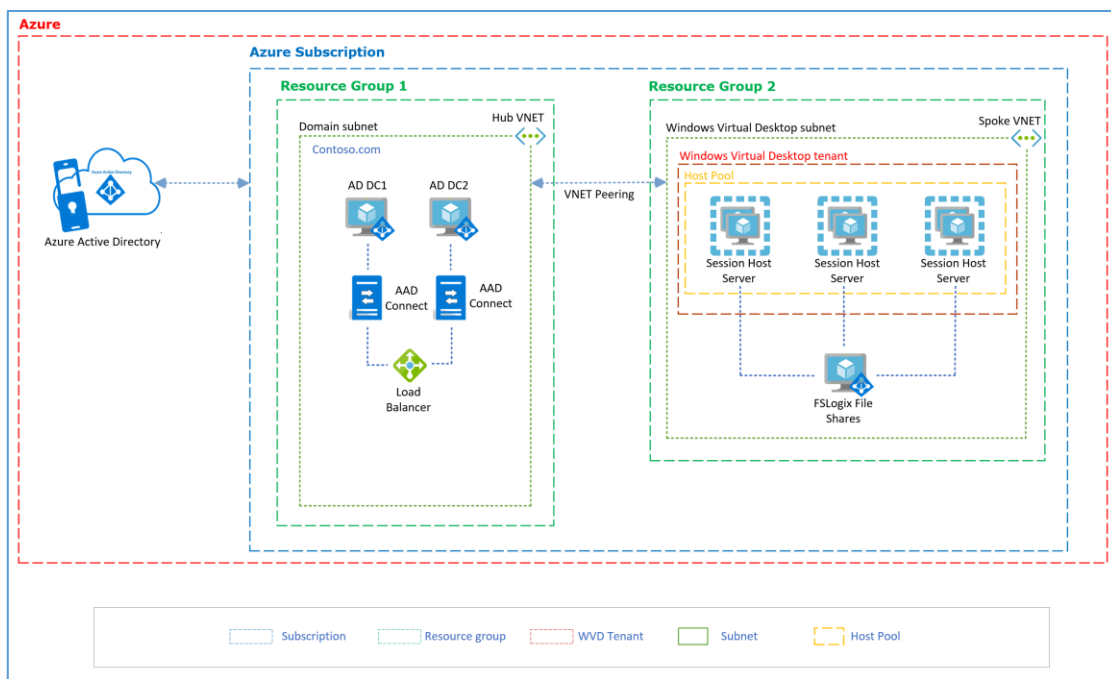
3. Configuring Dynamic Scaling with PowerShell

In this walkthrough, we'll use a scaling script to automatically scale session host virtual machines in a Windows Virtual Desktop environment. Using Azure Automation, the script is designed to periodically start and stop session host VMs based upon user utilization.

Download the PowerShell Scaling Script

1. Browse to the scaledeployment.psi Github repository and click the **Raw** button:
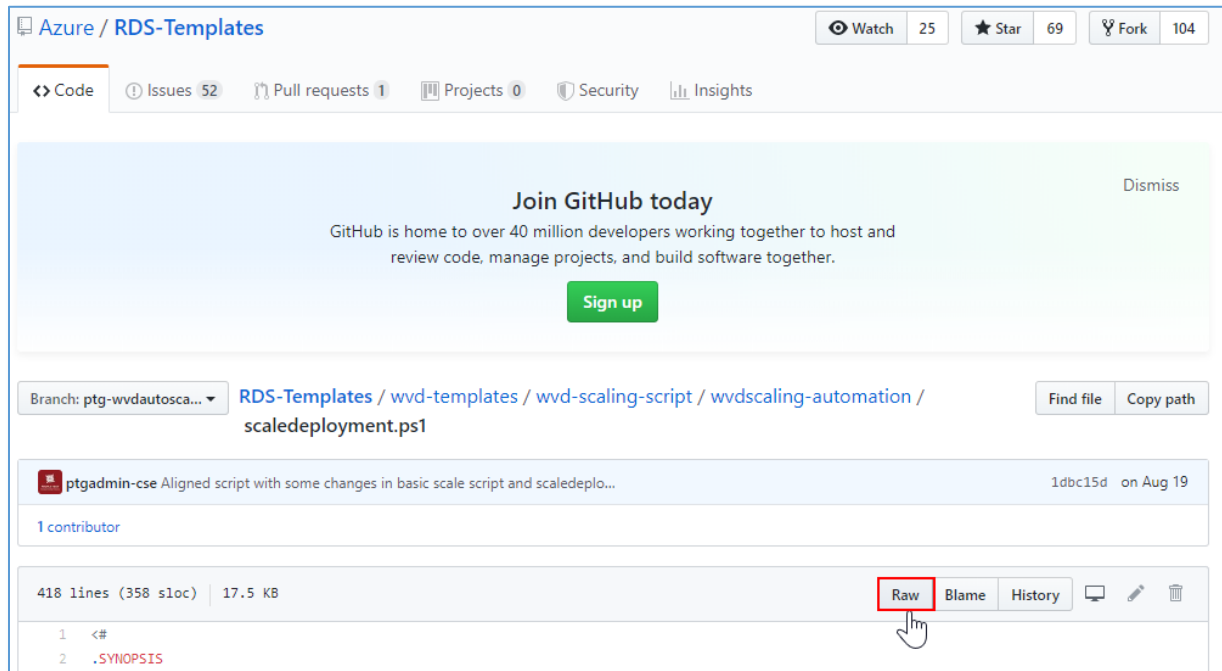
2. Right-click the background and select **Save as**:
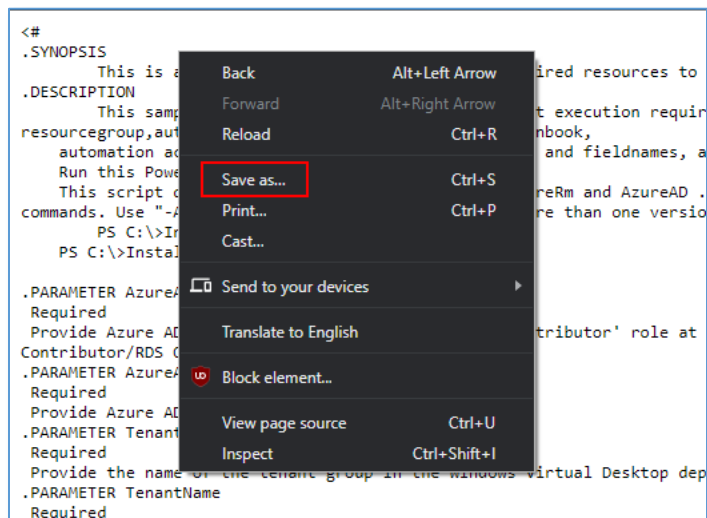
3. **Save** the script to a folder and remember where it is located: (note the file extension)
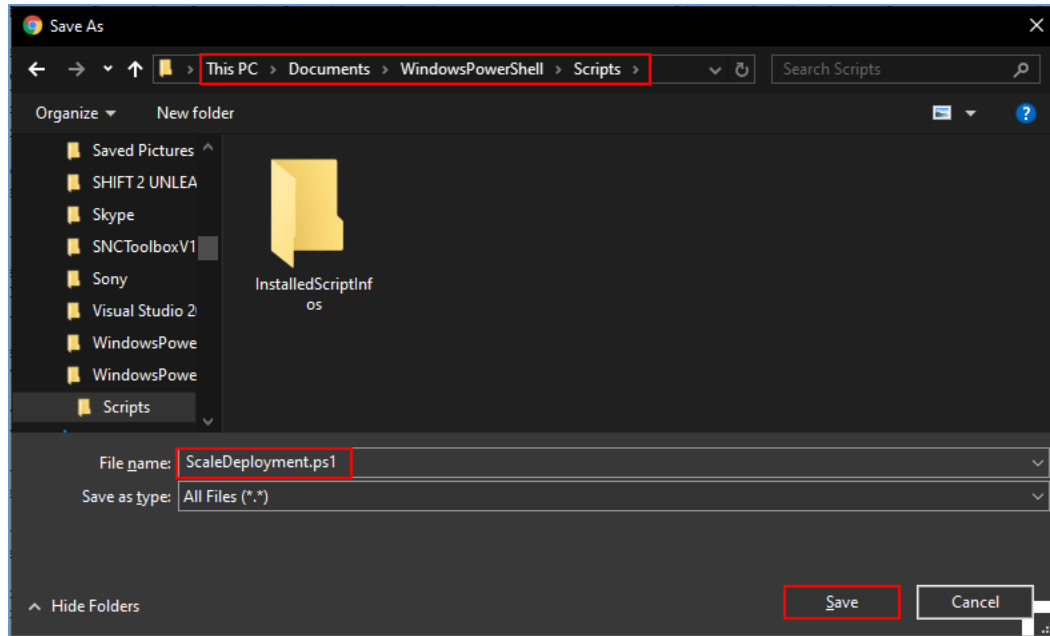
Preparing to run the script

4. Ensure that the Service Principal has been granted **Azure Service Management** API access:
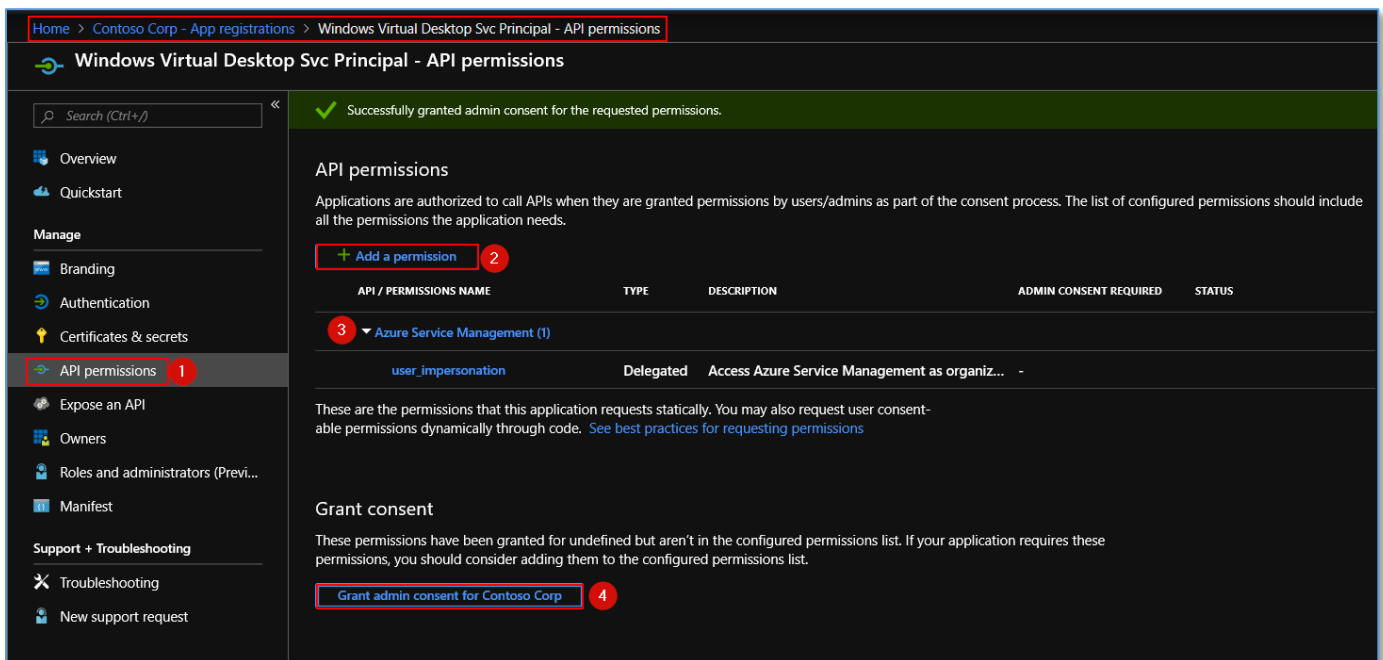
5. From a **PowerShell** session running in Admin mode, update the **CD** command below with your own folder location from above, then execute the cmdlet:

```
# Change directory to ScalingScript download folder:
CD C:\Users\Develop\Documents\WindowsPowerShell\Scripts\
```

6. Run the below cmdlet to import all necessary modules. Install if necessary by uncommenting the applicable line(s):

```
Install-Module -Name Microsoft.RDInfra.RDPowerShell -Force
Import-Module -Name Microsoft.RDInfra.RDPowerShell

Install-Module -Name AzureAD -Force
Import-Module -Name AzureAD

Install-Module -Name Az -AllowClobber -Force # PowerShell AZ
Import-Module -Name Az
```

7. Update the parameters below to logon to Azure:

```
## Logon to Azure using a USER ACCOUNT (non-MFA):
$azureTenantId = "12345678-b9fa-4163-8f1d-3d3569a3c717"
$Subscription = "12345678-a4e8-4bab-94f7-6639ac4af7a7"
$User = "wvdadmin@contosocorpwvd.com" # Single-factor auth only
$Password = ConvertTo-SecureString -String "password" -AsPlainText -Force
```

8. Run the below to logon to Azure:

```
$Credential = New-Object -TypeName "System.Management.Automation.PSCredential" -ArgumentList $User,$Password

# Connect to run Azure commands:
Connect-AzAccount -Credential $Credential -TenantId $azureTenantId -Subscription $Subscription

# Enable AzureRM commands: (the scaling deployment script uses AzureRM)
Enable-AzureRmAlias
```

Execute the deployment script

9. Update the parameters below, then execute, to run the scaling deployment script:

```
# Complete required parameters and execute script:
.\scaledeployment.ps1  -AzureADApplicationId "12345678-605a-4526-bafd-34f083866ef2" `
-AzureAdApplicationSecret $azurePassword `
-AADTenantID "12345678-b9fa-4163-8f1d-3d3569a3c717" `
-SubscriptionID "12345678-a4e8-4bab-94f7-6639ac4af7a7" `
-TenantGroupName "Default Tenant Group" `
-TenantName "ContosoCorpWVD2" `
-HostPoolName "NPW10MS" `
-PeakLoadBalancingType "DepthFirst" `
-MaintenanceTagName "WVDAutoScale" `
-RecurrenceInterval "15" `
-WorkspaceName "WVDOpsData" `
-BeginPeakTime "9:00" `
-EndPeakTime "17:00" `
-TimeDifference "-8:00" `
-SessionThresholdPerCPU 2 `
-MinimumNumberOfRDSH 1 `
-LimitSecondsToForceLogOffUser 20 `
-LogOffMessageTitle "System Under Maintenance" `
-LogOffMessageBody "Please save your work and logoff!" `
-Location "East U S2"
```

10. The script will take quite a while to run and will create a number of resources such as:

```
Azure authentication successfully Done. Result:

VERBOSE: Performing the operation "Replacing resource group ..." on target "WVDAutoScaleResourceGroup".
VERBOSE: 5:55:05 PM - Created resource group 'WVDAutoScaleResourceGroup' in location 'eastus2'


ResourceGroupName : WVDAutoScaleResourceGroup
Location          : eastus2
ProvisioningState : Succeeded
Tags              :
ResourceId        : /subscriptions/███████-4bab-94f7-6639ac4af7a7/resourceGroups/WVDAutoScaleResourceGroup

Resource Group was created with name WVDAutoScaleResourceGroup

SubscriptionId        : ████████-4bab-94f7-6639ac4af7a7
ResourceGroupName     : WVDAutoScaleResourceGroup
AutomationAccountName  : WVDAutoScaleAutomationAccount
Location              : East U S2
State                 : Ok
Plan                  : Basic
CreationTime          : 10/1/2019 5:55:16 PM -07:00
LastModifiedTime      : 10/1/2019 5:55:16 PM -07:00
LastModifiedBy        :
Tags                  : {}
```
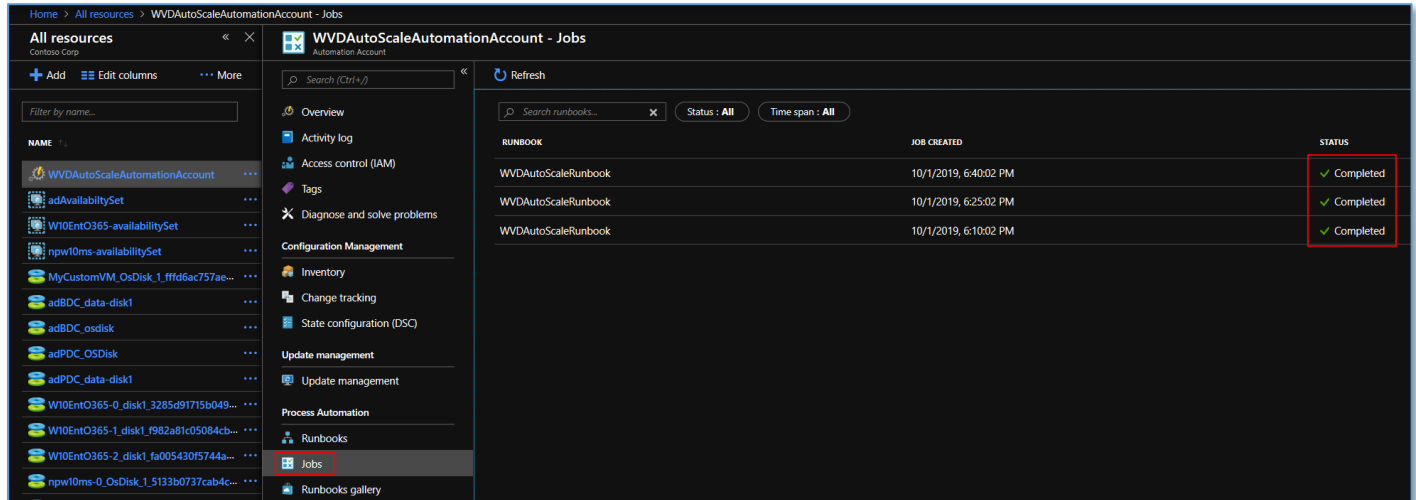
If everything went well, then you'll eventually see something like the below:

```
VERBOSE: 6:09:25 PM - Resource Microsoft.Scheduler/jobCollections/jobs 'WVDAutoScaleSchedulerJobCollection/NPW10MS-Job' provisioning status is succeeded
VERBOSE: 6:09:25 PM - Resource Microsoft.Scheduler/jobCollections 'WVDAutoScaleSchedulerJobCollection' provisioning status is succeeded
NPW10MS-job Azure Scheduler job was created successfully
```

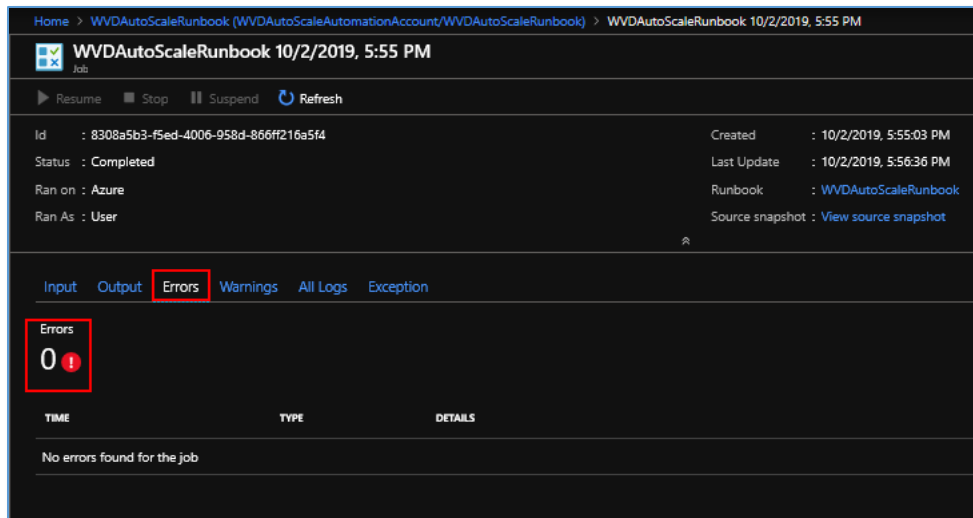# Verify that the automation job has been successfully running

You can verify that the job is running by clicking the automation account in the portal:

Click the latest Runbook entry, click **Errors** and you should see:

4. Support

Opening tickets

In case of an issue for Windows Virtual Desktop go to the Azure Portal and open a technical ticket based on your existing support plan at https://azure.microsoft.com/en-us/support/create-ticket/

Look for Service under **COMPUTE** and select **Windows Virtual Desktop-Preview**. You will find options to create tickets for the WVD service itself and for Office:

For Office issues you can file tickets during public preview in the Azure Portal when using Office in context of Windows Virtual Desktop.

Information you should provide for failed connection or management interactions when using the service:

- Use the diagnostics service to retrieve the **Activity ID** for failed connections or management interactions.
- Provide the approximate timeframe the issue happened

NOTE: This workflow will change post general availability.

Other resources you can leverage

Windows Virtual Desktop contains a number of knowledge articles as well as trouble shooting guides. Pay attention to the updated diagnostics chapter that provides Error scenarios you can mitigate: https://docs.microsoft.com/azure/virtual-desktop/overview

Exchange on our community forum on issues important to you for Windows Virtual Desktop: https://techcommunity.microsoft.com/t5/Windows-Virtual-Desktop/bd-p/WindowsVirtualDesktop

When setting up your environment you will be using other Azure Services. You can watch the health dashboard here to verify health state on any Azure service you are consuming:
https://azure.microsoft.com/en-us/status/