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

Business Continuity with Azure Backup

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

This document is a walk-through of implementing Azure Backup (AzBackup) and Azure Files On-Demand within the new Windows Virtual Desktop (WVD) in Microsoft Azure. Data can be backed up and recovered at a granular level, including backup of files, folders, machine system state, and app-aware data backup. Azure Backup handles data at a more granular level than Azure Site Recovery.

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.

- An Azure Active Directory
- A Windows Server Active Directory in sync with Azure Active Directory. This can be enabled through:
    - Azure AD Connect
    - Azure AD Domain Services
- An Azure subscription, containing a virtual network that either contains or is connected to the Windows Server Active Directory
- A working Windows Virtual Desktop environment
- A file server within the subscription acting as the data source

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

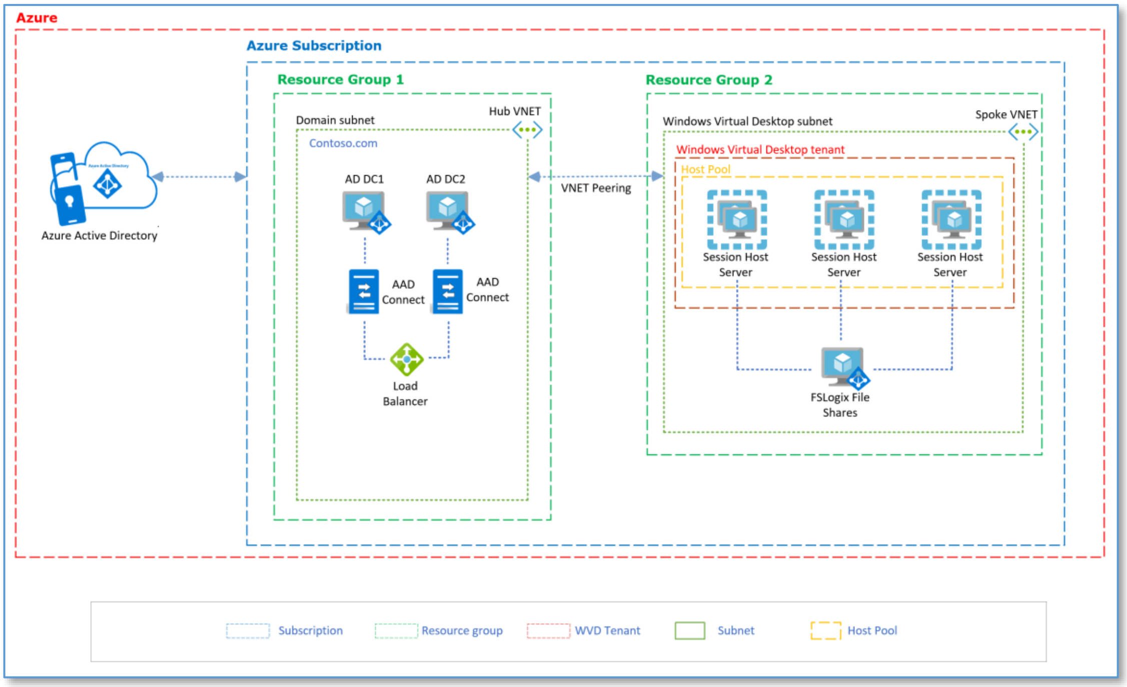
- Azure Networking & security Best Practices
- Azure Storage security overview
- Best practices for Azure VM security

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. OneDrive and Azure Files On-Demand for the Enterprise

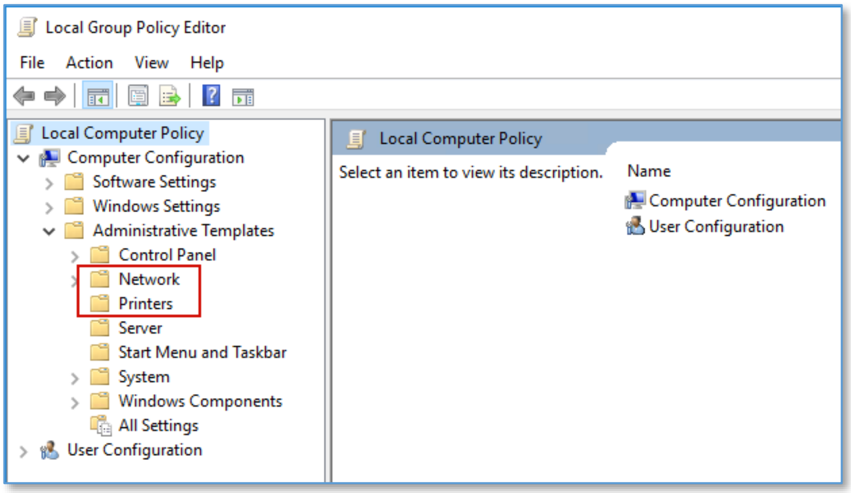
OneDrive Files On-Demand has been designed from the ground up for enterprises. Files On-Demand leverages the Windows Fall Creators update to simplify the user experience with cloud storage and sync, bring the power of the cloud into Windows File Explorer, and dramatically limit the network impact of sync on your corporate network. Since Files On-Demand already provides a backup feature, if enabled, we can exclude OneDrive and SharePoint files from our User Profile Disk backup strategy.

In our backup setup example below, we exclude the OneDrive files from the backup since we will have Files On-Demand enabled.

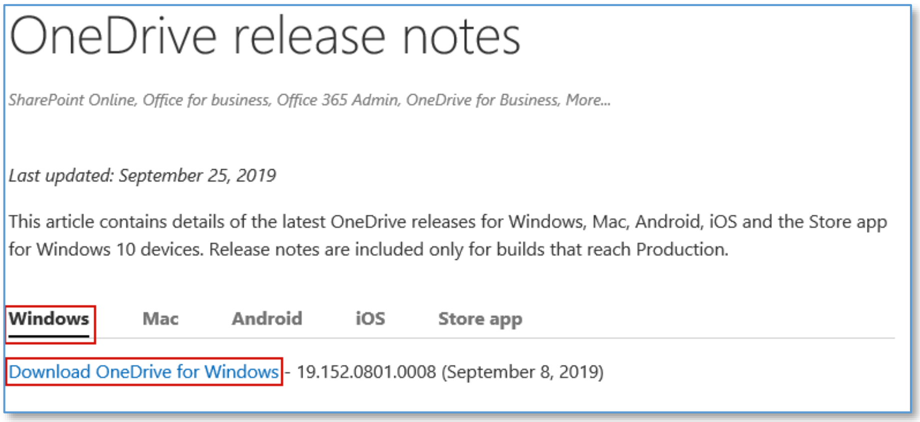
Enable Files On-Demand

To enable Files On-Demand, a Group Policy needs to be added for OneDrive. This policy will cause OneDrive to default to using online-only storage for designated users within the tenant.

In our example, we're using Windows 2016 Server VMs for the domain controllers, and they don't have the OneDrive Group Policy Administrative Templates installed by default:



1. To get the policies, we need to **download** and **install** the OneDrive sync client to a DC:



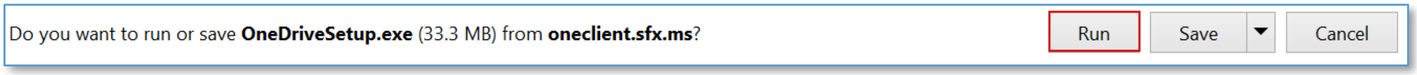
OneDrive release notes

SharePoint Online, Office for business, Office 365 Admin, OneDrive for Business, More...

Last updated: September 25, 2019

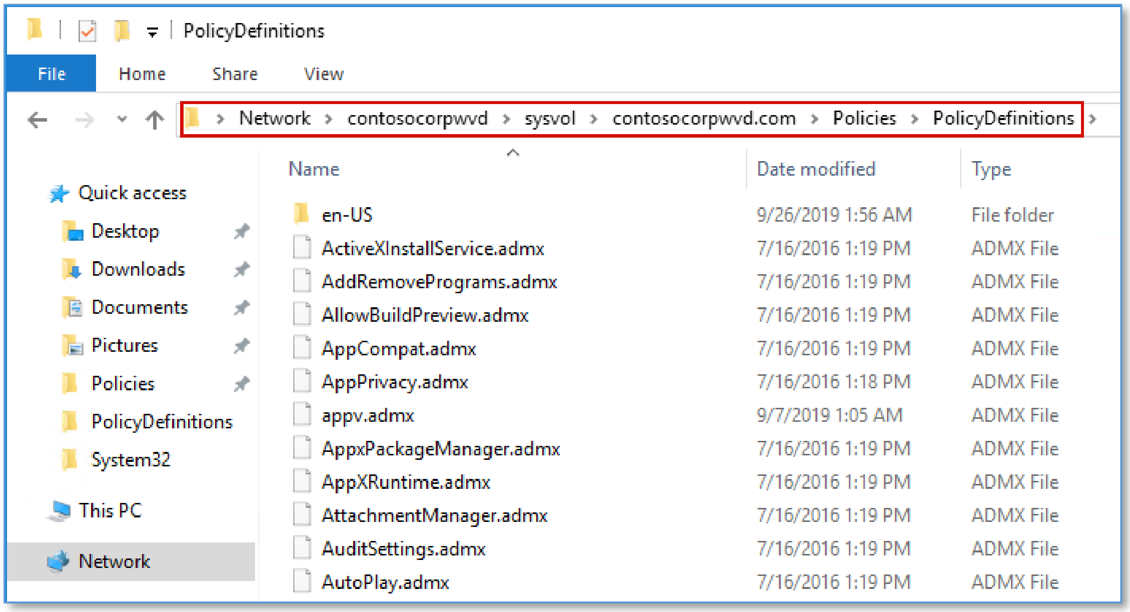
This article contains details of the latest OneDrive releases for Windows, Mac, Android, iOS and the Store app for Windows 10 devices. Release notes are included only for builds that reach Production.

Download OneDrive for Windows - 19.152.0801.0008 (September 8, 2019)



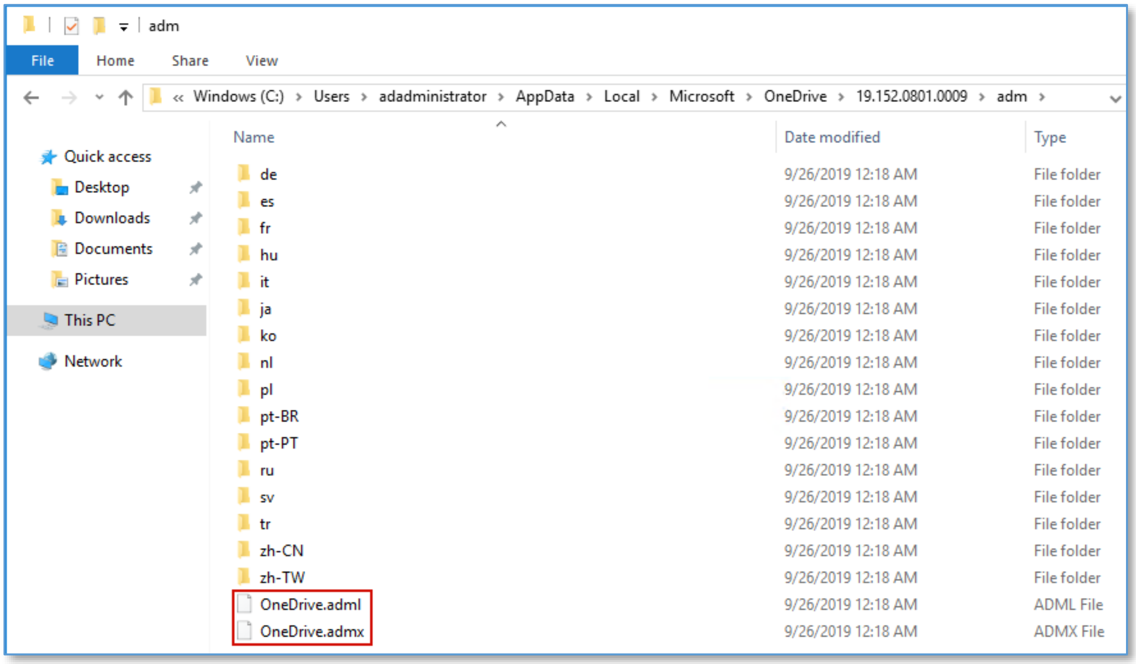
Do you want to run or save **OneDriveSetup.exe** (33.3 MB) from **oneclient.sfx.ms**?

2. Now, we'll setup a Group Policy Central Store for the new policies to be located within. On a domain controller, **copy** the folder and contents **C:\Windows\PolicyDefinitions** to **\\[*your domain*]\sysvol\[*your domain*]\Policies**: (if it's not already there)



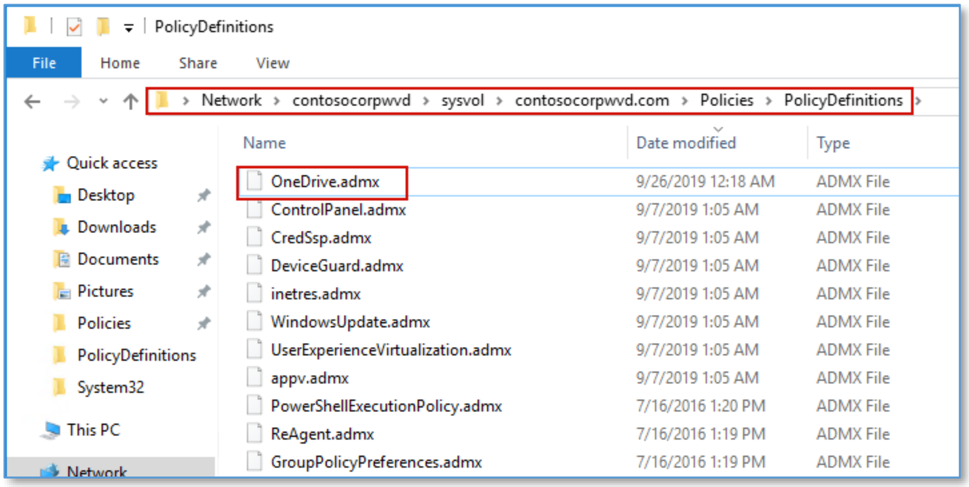
Name	Date modified	Type
en-US	9/26/2019 1:56 AM	File folder
ActiveXInstallService.admx	7/16/2016 1:19 PM	ADMX File
AddRemovePrograms.admx	7/16/2016 1:19 PM	ADMX File
AllowBuildPreview.admx	7/16/2016 1:19 PM	ADMX File
AppCompat.admx	7/16/2016 1:19 PM	ADMX File
AppPrivacy.admx	7/16/2016 1:18 PM	ADMX File
appv.admx	9/7/2019 1:05 AM	ADMX File
AppxPackageManager.admx	7/16/2016 1:19 PM	ADMX File
AppXRuntime.admx	7/16/2016 1:19 PM	ADMX File
AttachmentManager.admx	7/16/2016 1:19 PM	ADMX File
AuditSettings.admx	7/16/2016 1:19 PM	ADMX File
AutoPlay.admx	7/16/2016 1:19 PM	ADMX File

3. Browse to **%localappdata%\Microsoft\OneDrive\[*BuildNumber*]\adm**, (and to the subfolder for your language, as necessary) and **copy** the 2 files as shown:


adm
File
Home
Share
View
« Windows (C:) › Users › adadministrator › AppData › Local › Microsoft › OneDrive › 19.152.0801.0009 › adm ›
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network

Name	Date modified	Type
de	9/26/2019 12:18 AM	File folder
es	9/26/2019 12:18 AM	File folder
fr	9/26/2019 12:18 AM	File folder
hu	9/26/2019 12:18 AM	File folder
it	9/26/2019 12:18 AM	File folder
ja	9/26/2019 12:18 AM	File folder
ko	9/26/2019 12:18 AM	File folder
nl	9/26/2019 12:18 AM	File folder
pl	9/26/2019 12:18 AM	File folder
pt-BR	9/26/2019 12:18 AM	File folder
pt-PT	9/26/2019 12:18 AM	File folder
ru	9/26/2019 12:18 AM	File folder
sv	9/26/2019 12:18 AM	File folder
tr	9/26/2019 12:18 AM	File folder
zh-CN	9/26/2019 12:18 AM	File folder
zh-TW	9/26/2019 12:18 AM	File folder
OneDrive.adml	9/26/2019 12:18 AM	ADML File
OneDrive.admx	9/26/2019 12:18 AM	ADMX File

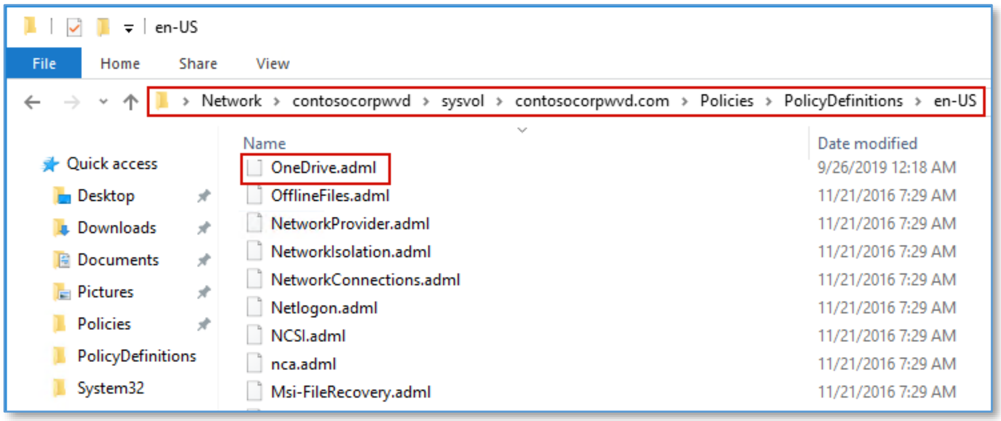
4. Paste the **OneDrive.admx** file into the **\\[*your domain*]\sysvol\[*your domain*]\Policies\PolicyDefinitions** folder:



Network › contosocorpwvd › sysvol › contosocorpwvd.com › Policies › PolicyDefinitions ›

Name	Date modified	Type
OneDrive.admx	9/26/2019 12:18 AM	ADMX File
ControlPanel.admx	9/7/2019 1:05 AM	ADMX File
CredSsp.admx	9/7/2019 1:05 AM	ADMX File
DeviceGuard.admx	9/7/2019 1:05 AM	ADMX File
inetres.admx	9/7/2019 1:05 AM	ADMX File
WindowsUpdate.admx	9/7/2019 1:05 AM	ADMX File
UserExperienceVirtualization.admx	9/7/2019 1:05 AM	ADMX File
appv.admx	9/7/2019 1:05 AM	ADMX File
PowerShellExecutionPolicy.admx	7/16/2016 1:20 PM	ADMX File
ReAgent.admx	7/16/2016 1:19 PM	ADMX File
GroupPolicyPreferences.admx	7/16/2016 1:19 PM	ADMX File

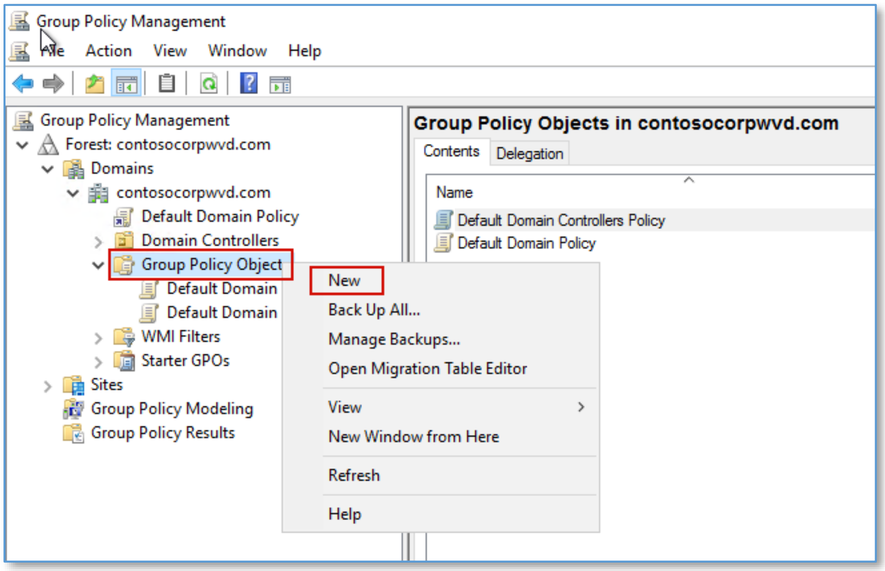
5. Paste the **OneDrive.adml** file into the sub-folder called **en-US**:



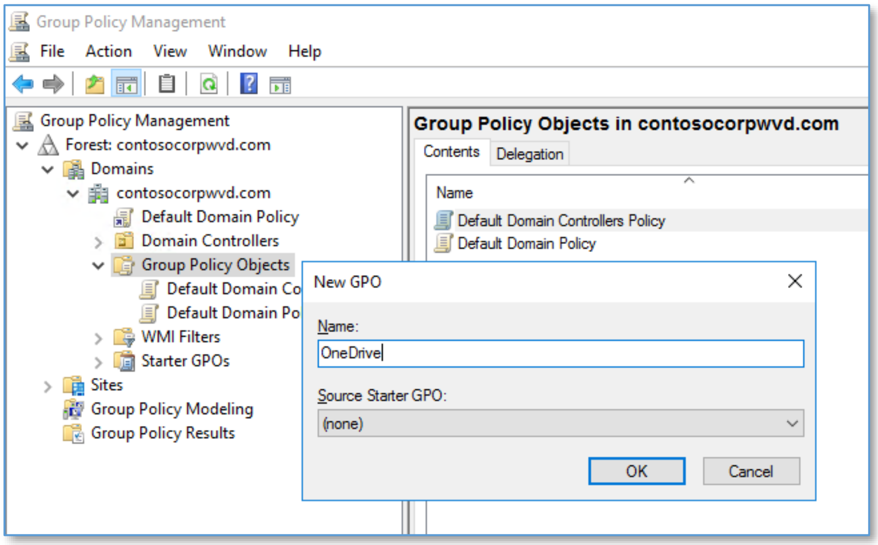
Network › contosocorpwvd › sysvol › contosocorpwvd.com › Policies › PolicyDefinitions › en-US

Name	Date modified
OneDrive.adml	9/26/2019 12:18 AM
OfflineFiles.adml	11/21/2016 7:29 AM
NetworkProvider.adml	11/21/2016 7:29 AM
NetworkIsolation.adml	11/21/2016 7:29 AM
NetworkConnections.adml	11/21/2016 7:29 AM
Netlogon.adml	11/21/2016 7:29 AM
NCSI.adml	11/21/2016 7:29 AM
nca.adml	11/21/2016 7:29 AM
Msi-FileRecovery.adml	11/21/2016 7:29 AM

6. Using **gpmc.msc**, **create** a new **OneDrive** Group Policy Object:



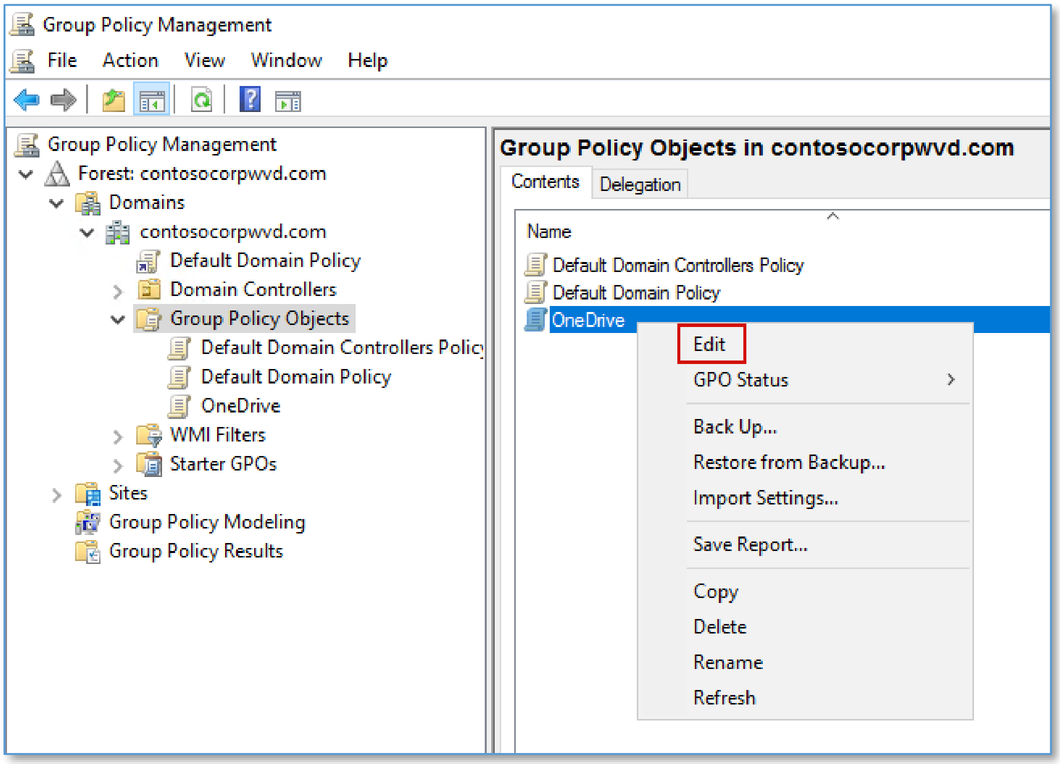
Name it...



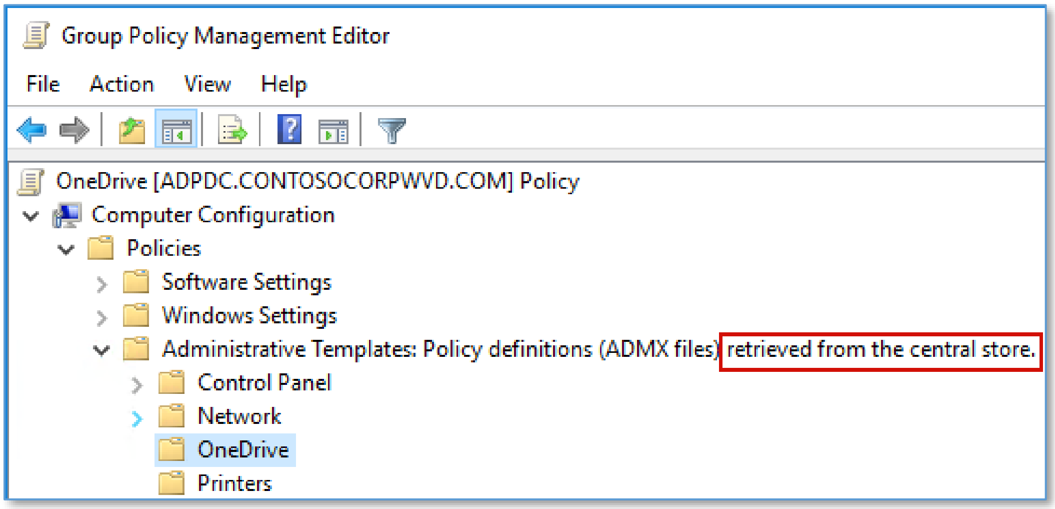
Name: OneDrive

Source Starter GPO: (none)

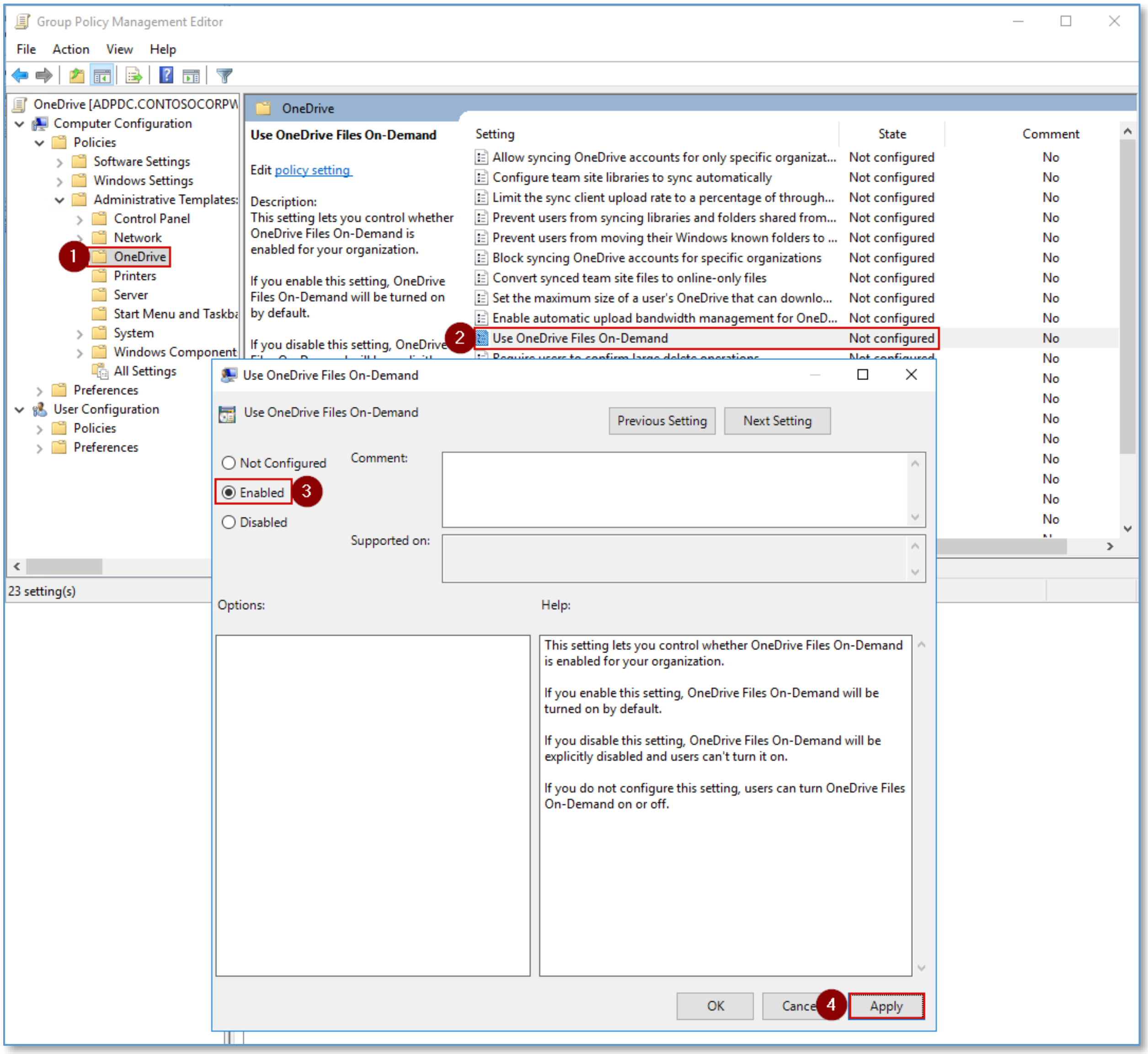
7. **Edit** the new OneDrive GPO:



The editor indicates that we're now using the Central Store:


Group Policy Management Editor
File
Action
View
Help
OneDrive [ADPDC.CONTOSOCORPWVD.COM] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Administrative Templates: Policy definitions (ADMX files) retrieved from the central store.
Control Panel
Network
OneDrive
Printers

8. **Enable** “Use OneDrive Files On-Demand” policy and close the editor:



Use OneDrive Files On-Demand

Edit policy setting

Description:
This setting lets you control whether OneDrive Files On-Demand is enabled for your organization.

If you enable this setting, OneDrive Files On-Demand will be turned on by default.

If you disable this setting, OneDrive

Setting	State	Comment
Allow syncing OneDrive accounts for only specific organizat...	Not configured	No
Configure team site libraries to sync automatically	Not configured	No
Limit the sync client upload rate to a percentage of through...	Not configured	No
Prevent users from syncing libraries and folders shared from...	Not configured	No
Prevent users from moving their Windows known folders to ...	Not configured	No
Block syncing OneDrive accounts for specific organizations	Not configured	No
Convert synced team site files to online-only files	Not configured	No
Set the maximum size of a user's OneDrive that can downlo...	Not configured	No
Enable automatic upload bandwidth management for OneD...	Not configured	No
Use OneDrive Files On-Demand	Not configured	No
Require users to confirm large delete operations	Not configured	No

23 setting(s)

Use OneDrive Files On-Demand

○ Not Configured
● Enabled
○ Disabled

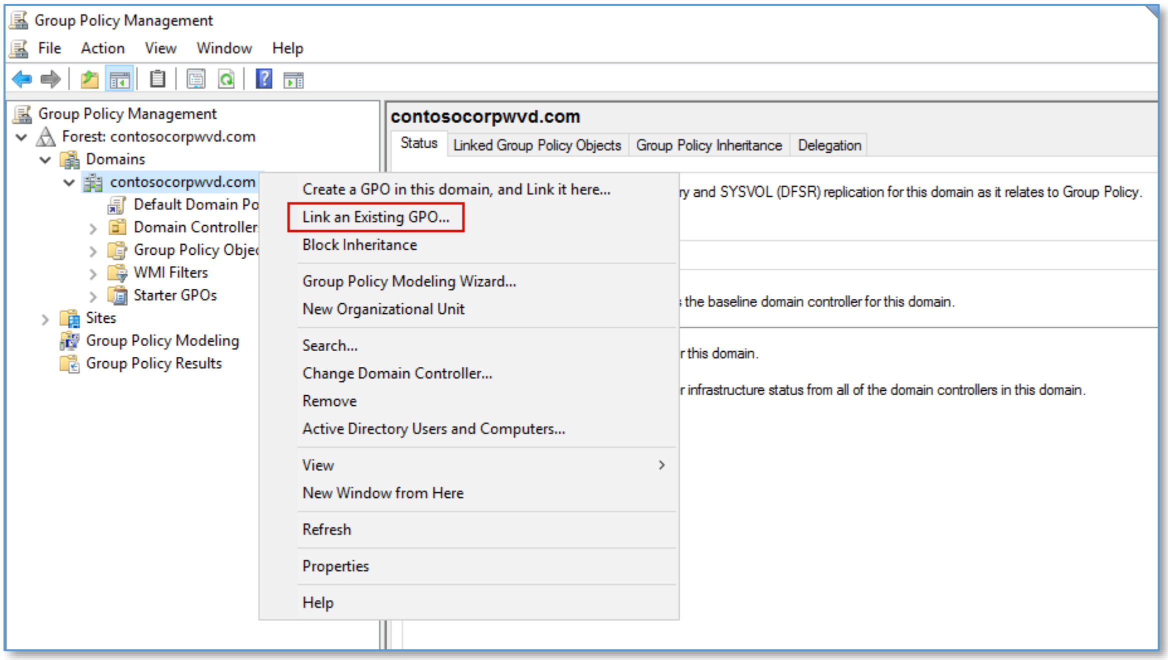
This setting lets you control whether OneDrive Files On-Demand is enabled for your organization.

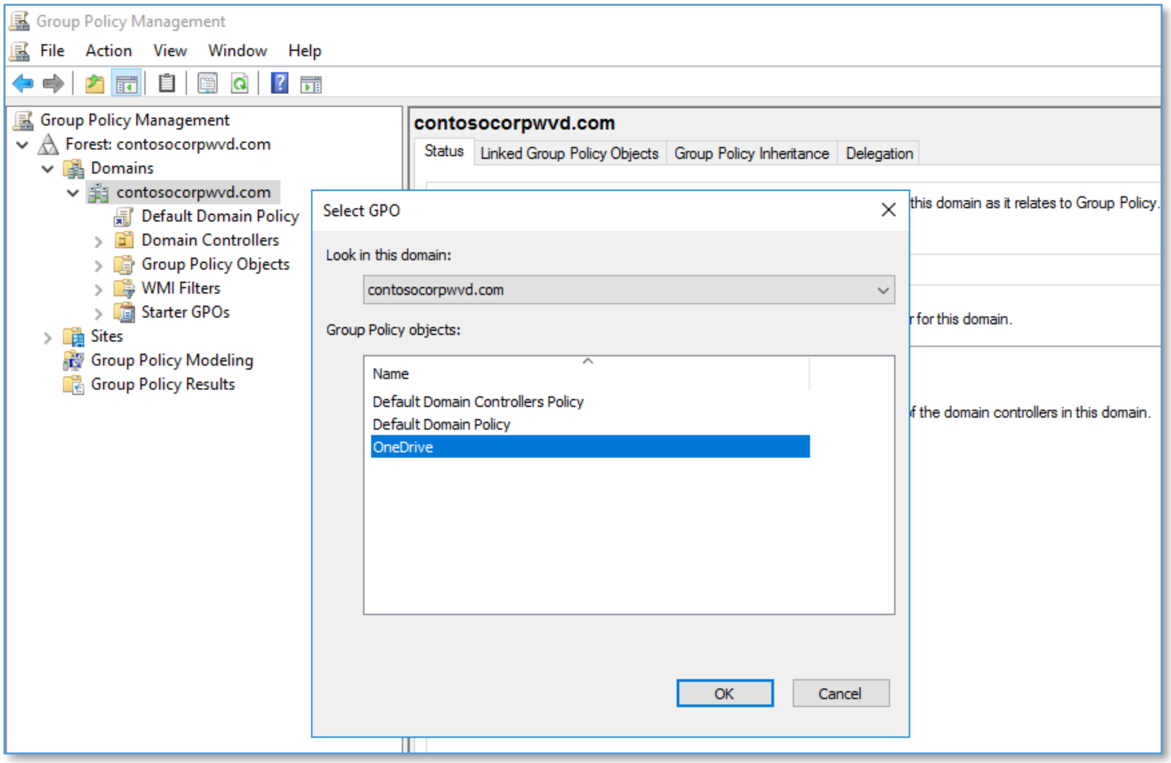
If you enable this setting, OneDrive Files On-Demand will be turned on by default.

If you disable this setting, OneDrive Files On-Demand will be explicitly disabled and users can't turn it on.

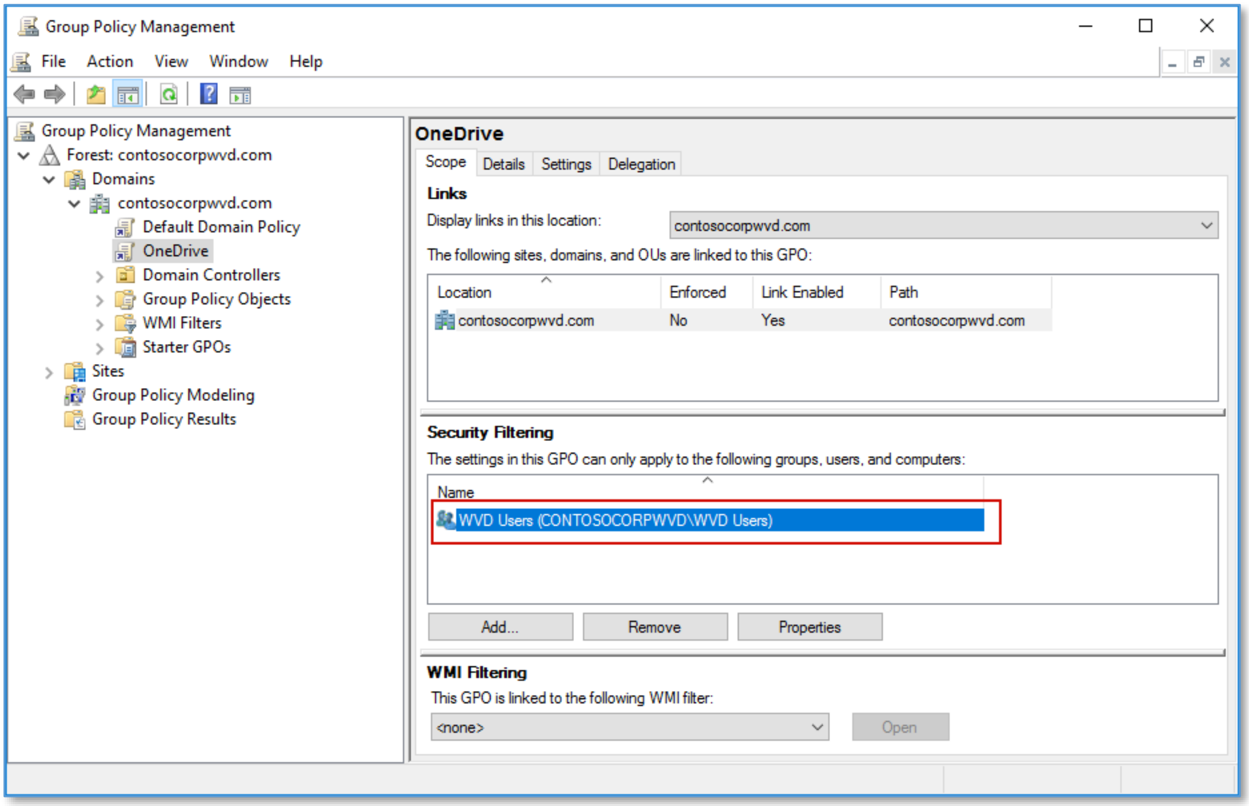
If you do not configure this setting, users can turn OneDrive Files On-Demand on or off.

9. Right-click the domain name and **link** the new OneDrive GPO to the domain:


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: contosocorpwvd.com
Domains
contosocorpwvd.com
Default Domain Po
Domain Controller
Group Policy Objec
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
contosocorpwvd.com
Status
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Create a GPO in this domain, and Link it here...
Link an Existing GPO...
Block Inheritance
Group Policy Modeling Wizard...
New Organizational Unit
Search...
Change Domain Controller...
Remove
Active Directory Users and Computers...
View
New Window from Here
Refresh
Properties
Help
y and SYSVOL (DFSR) replication for this domain as it relates to Group Policy.
the baseline domain controller for this domain.
r this domain.
r infrastructure status from all of the domain controllers in this domain.



10. **Edit** the GPO scope to apply to only users in our **WVD Users** security group:



OneDrive

Links

Display links in this location: contosocorpwvd.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
contosocorpwvd.com	No	Yes	contosocorpwvd.com

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
WVD Users (CONTOSOCORPWVD\WVD Users)

WMI Filtering

This GPO is linked to the following WMI filter:

<none>

Done!

4. Setup Azure Backup

In this section we'll implement Azure Backup using Recovery Services. A Recovery Services vault is a storage entity in Azure that houses data. The data stored is typically copies of files, or configuration information for virtual machines. In our example, we're going to backup the UDP folder used by FSLogix for storing user profiles in persistent desktops in WVD.

Create a Recovery Services vault

We need to create the vault in any region, except the source region. We'll create a resource group in which to create the vault. In the example below, the resource group is named VMDRtoAzurePS and is created in the East Asia region.

- Log into your Azure subscription using the Connect-AzAccount cmdlet:

```
Azure PowerShell:
Connect-AzAccount
```

- Select the Azure subscription you want to back up your data to. In our example we'll use the Contoso subscription:

```
Azure PowerShell:
Select-AzSubscription -SubscriptionName "Contoso Subscription"
```

- Create a resource group in which to create the Recovery Services vault and choose any region, except the source region. In our example, we'll use **ContosoRSVRG** & **East Asia**:

```
Azure PowerShell:
New-AzResourceGroup -Name "ContosoRSVRG" -Location "East Asia"
```

```
Result:
ResourceGroupName : ContosoRSVRG
Location          : eastasia
ProvisioningState : Succeeded
Tags              :
ResurceId         : /subscriptions/…
```

- Create a Recovery services vault. We'll call ours **ContosoRSV**:

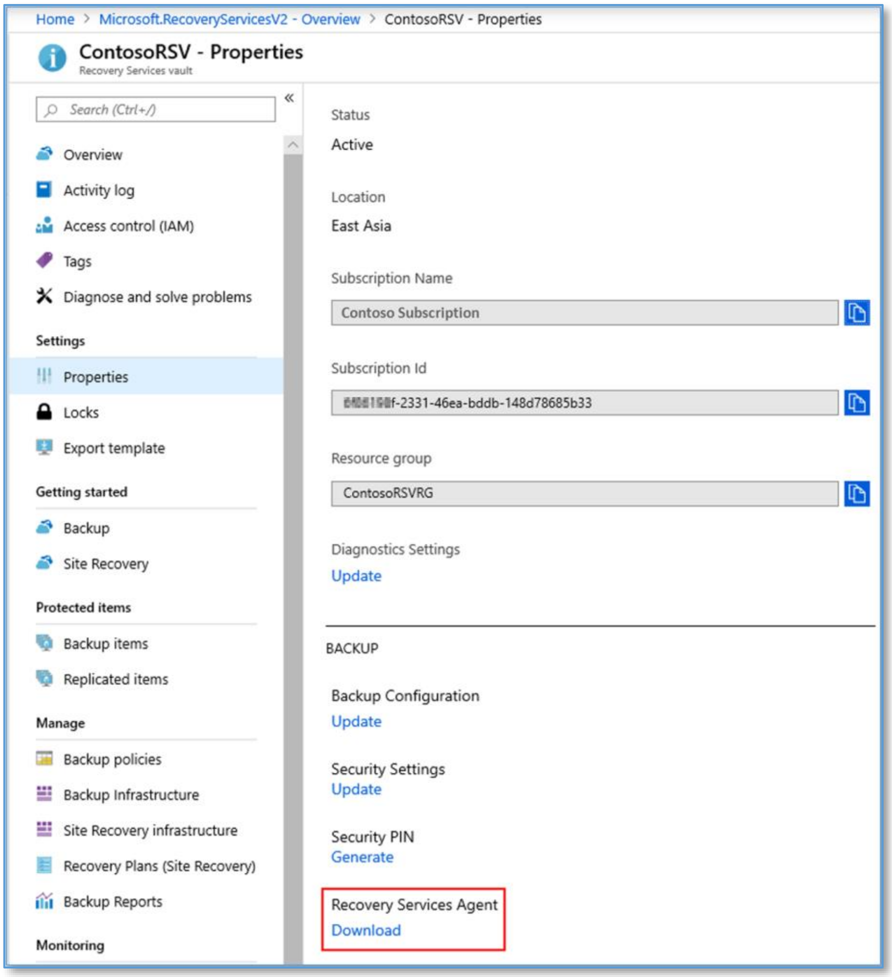
```
Azure PowerShell:
New-AzRecoveryServicesVault -Name "ContosoRSV" -Location "East Asia" -
ResourceGroupName "ContosoRSVRG"
```

```
Result:
Name              : ContosoRSV
ID                : /subscriptions/…
Type              : Microsoft.RecoveryServices/vaults
Location          : eastasia
ResourceGroupName : ContosoRSVRG
SubscriptionId    : xxxxxxxx-xxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Properties        : Microsoft.Azure.Commands.RecoveryServices.ARSVaultProperties
```

Install Recovery Service Agent on a File Server

Login to the Azure portal and click on the new **ContosoRSV** Recovery Services vault.

1. In **Settings** > **Properties**, download the **Recovery Services Agent** and **Backup credentials** file:



ContosoRSV - Properties
Recovery Services vault

Status
Active

Location
East Asia

Subscription Name
Contoso Subscription

Subscription Id
[redacted]f-2331-46ea-bddb-148d78685b33

Resource group
ContosoRSVRG

Diagnostics Settings
Update

BACKUP

Backup Configuration
Update

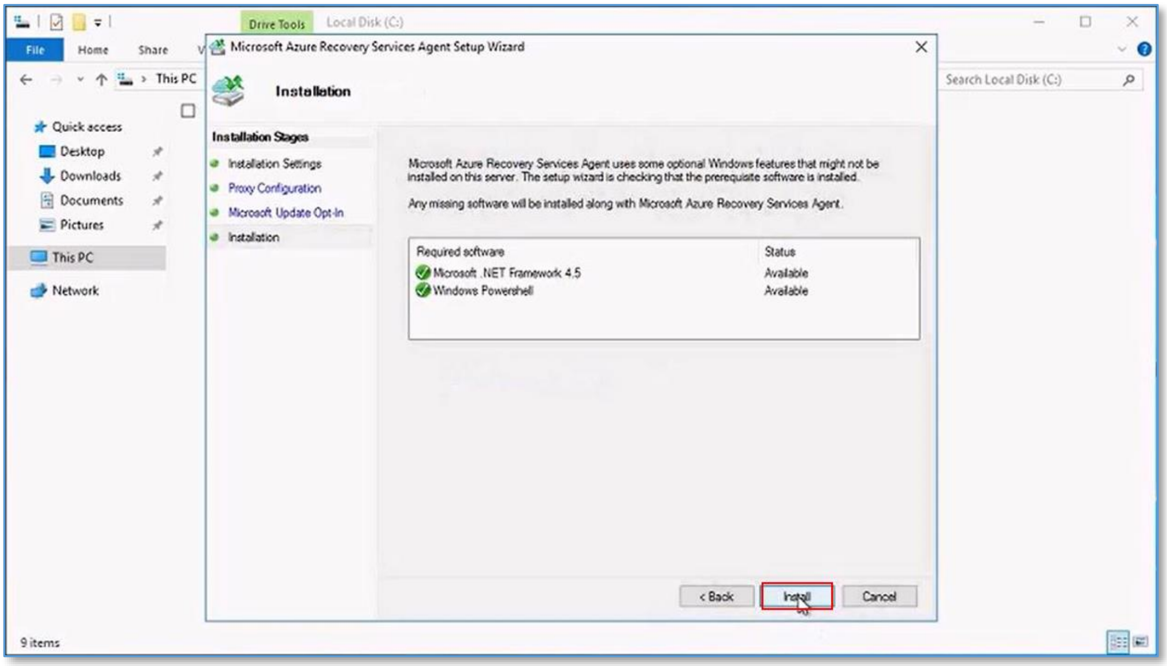
Security Settings
Update

Security PIN
Generate

Recovery Services Agent
Download

2. **Copy** the downloaded files to the Files Server with the data that needs to be backed up. In our example, we’re using fs01.contoso.local.

3. On the file server, double-click the **MARSAgent** installer file, to start the installation wizard, then click **Install:**



Microsoft Azure Recovery Services Agent Setup Wizard

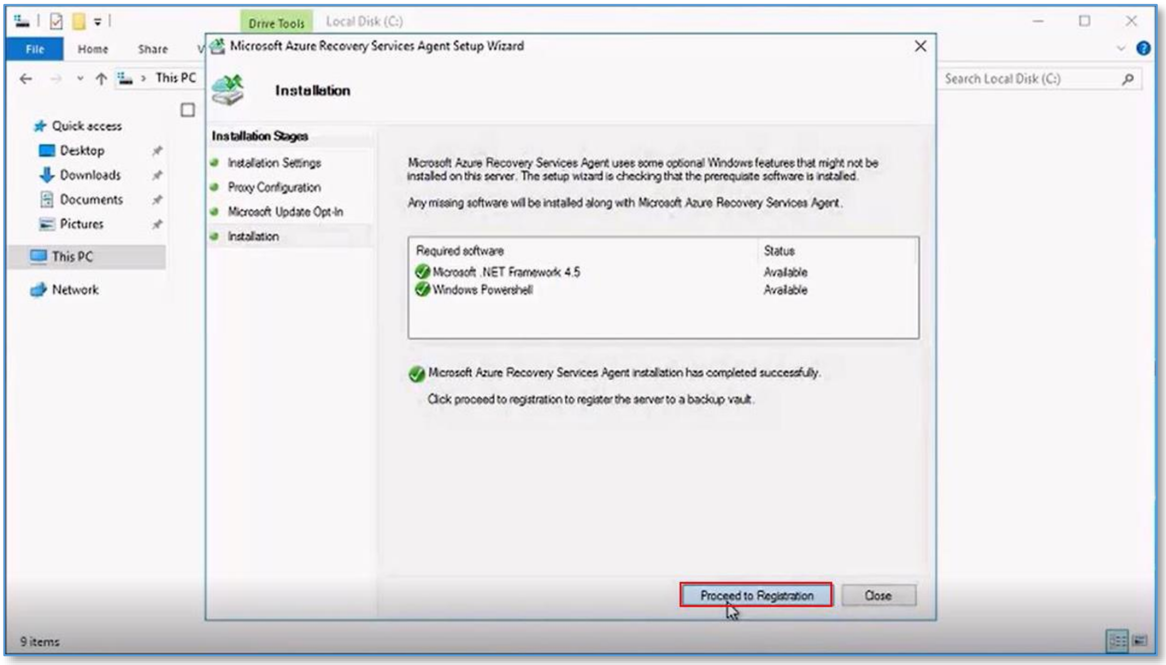
Installation

Microsoft Azure Recovery Services Agent uses some optional Windows features that might not be installed on this server. The setup wizard is checking that the prerequisite software is installed.

Any missing software will be installed along with Microsoft Azure Recovery Services Agent.

Required software	Status
✓ Microsoft .NET Framework 4.5	Available
✓ Windows Powershell	Available

4. Click **Proceed to Registration**



Microsoft Azure Recovery Services Agent Setup Wizard

Installation

Microsoft Azure Recovery Services Agent uses some optional Windows features that might not be installed on this server. The setup wizard is checking that the prerequisite software is installed.

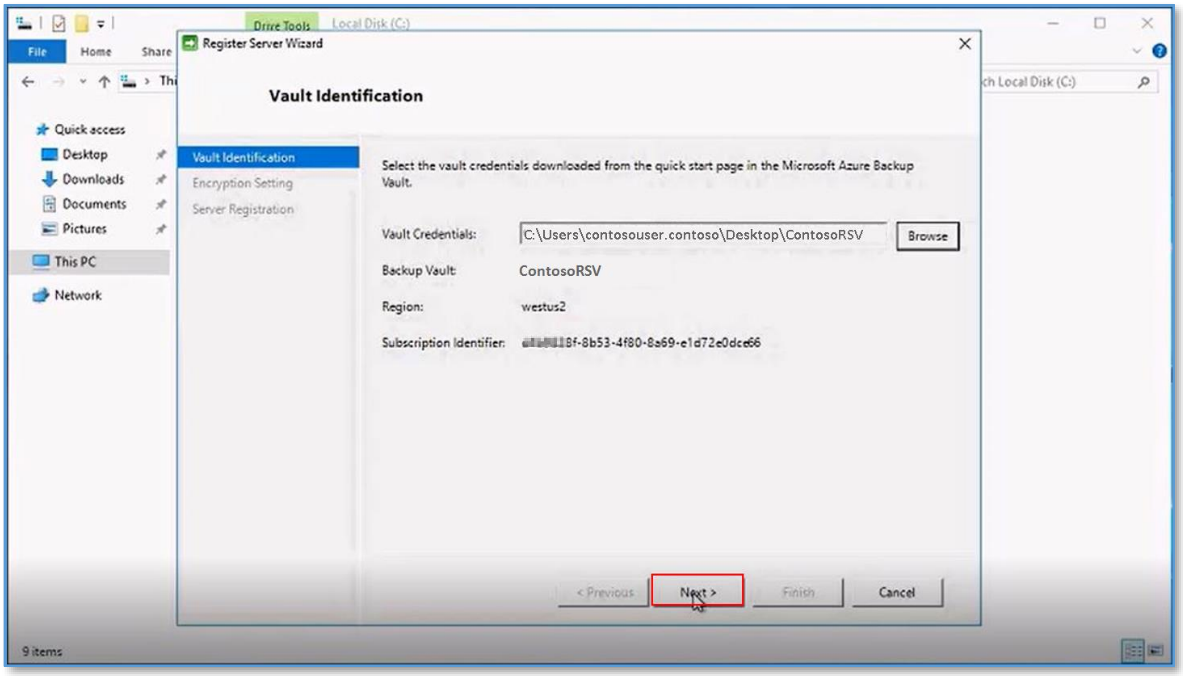
Any missing software will be installed along with Microsoft Azure Recovery Services Agent.

Required software	Status
✓ Microsoft .NET Framework 4.5	Available
✓ Windows Powershell	Available

✓ Microsoft Azure Recovery Services Agent installation has completed successfully.

Click proceed to registration to register the server to a backup vault.

5. In **Vault Identification**, select the vault credentials downloaded from the quick start page in the Microsoft Azure Backup Vault



Vault Identification

Select the vault credentials downloaded from the quick start page in the Microsoft Azure Backup Vault.

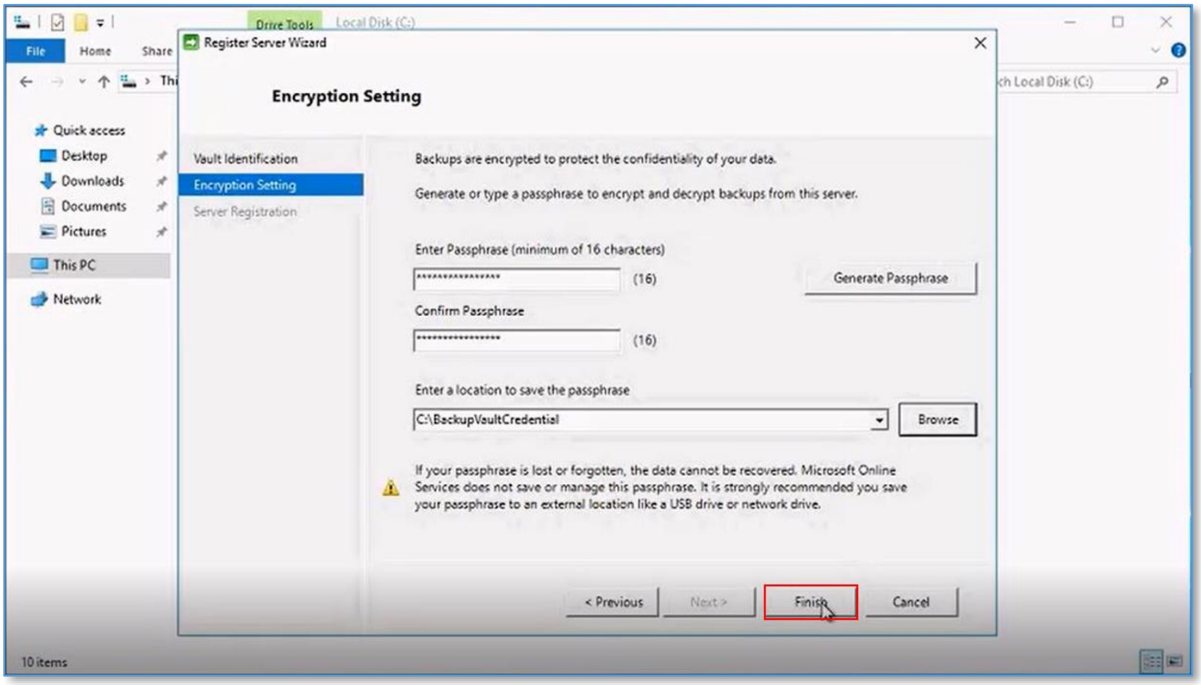
Vault Credentials: C:\Users\contosouser.contoso\Desktop\ContosoRSV

Backup Vault: ContosoRSV

Region: westus2

Subscription Identifier: [redacted]8f-8b53-4f80-8a69-e1d72e0dce66

6. In **Encryption setting,** enter a paraphrase and save it to a secure location, then click **Finish**



Encryption Setting

Backups are encrypted to protect the confidentiality of your data.

Generate or type a passphrase to encrypt and decrypt backups from this server.

Enter Passphrase (minimum of 16 characters)

**************** (16)

Confirm Passphrase

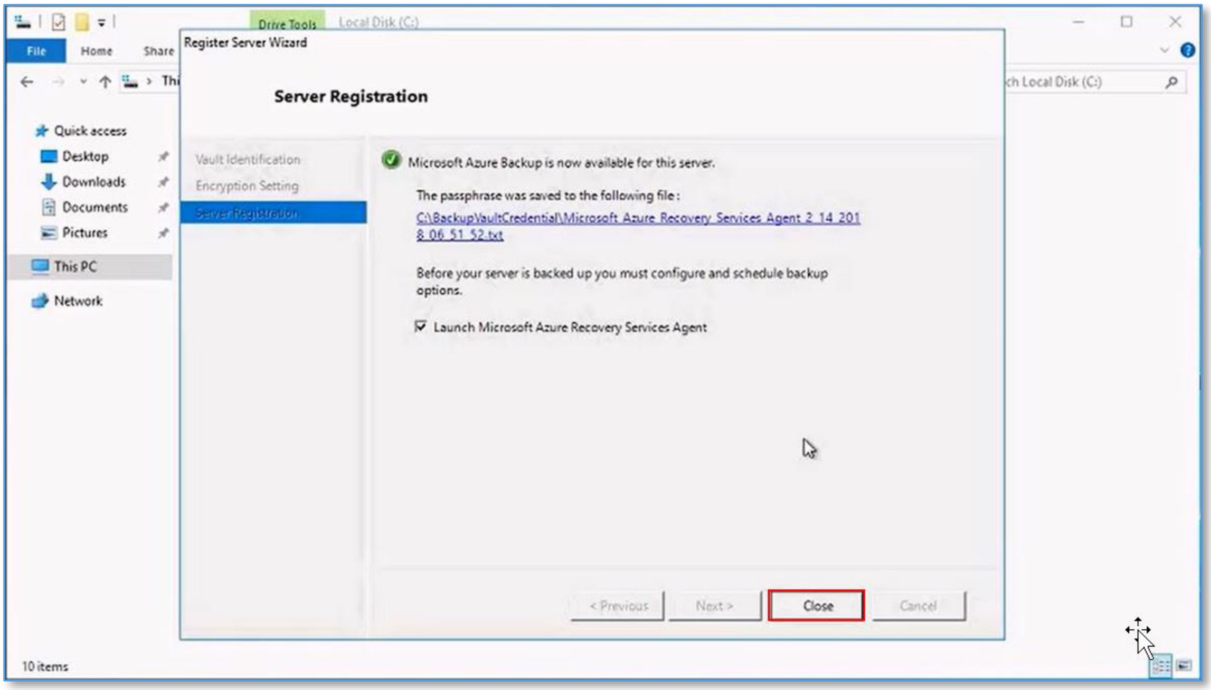
**************** (16)

Enter a location to save the passphrase

C:\BackupVaultCredential

⚠ If your passphrase is lost or forgotten, the data cannot be recovered. Microsoft Online Services does not save or manage this passphrase. It is strongly recommended you save your passphrase to an external location like a USB drive or network drive.

7. Check the **Launch Microsoft Azure Recovery Services Agent**, then click **Close**



Server Registration

Microsoft Azure Backup is now available for this server.

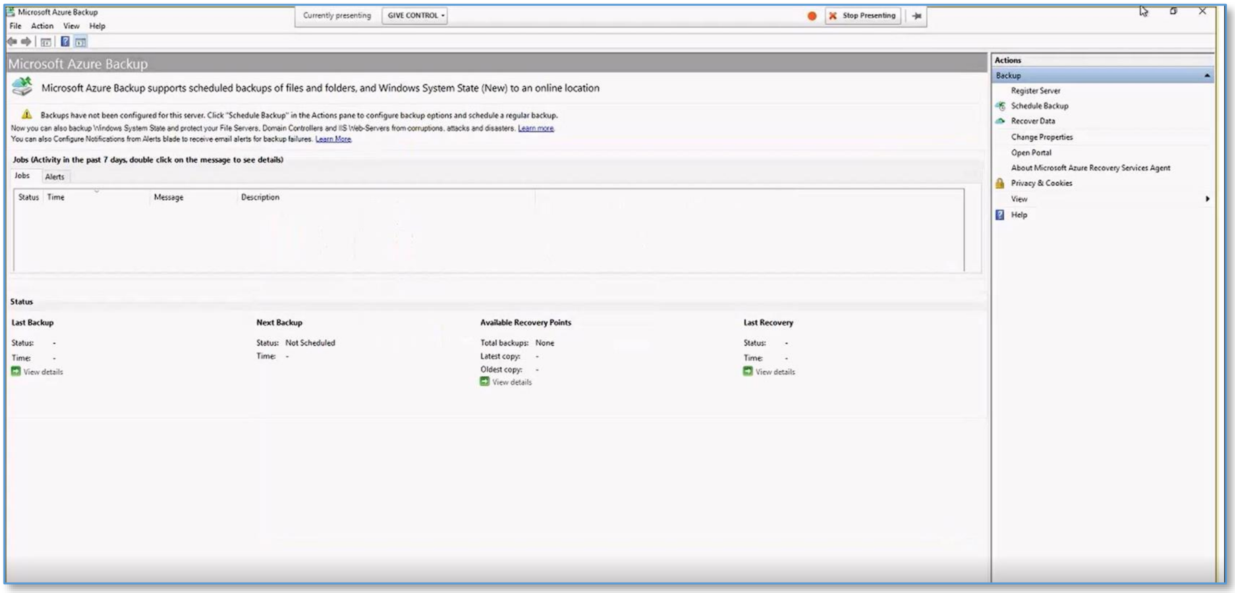
The passphrase was saved to the following file:
C:\BackupVaultCredential\Microsoft_Azure_Recovery_Services_Agent_2_14_2018_06_51_52.txt

Before your server is backed up you must configure and schedule backup options.

☑ Launch Microsoft Azure Recovery Services Agent

- Microsoft Azure Backup Agent is now installed.
- A Backup Agent icon is created on the desktop.

8. Double-click the Backup Agent icon to launch the **BackUp Agent Wizard**:



Microsoft Azure Backup

Microsoft Azure Backup supports scheduled backups of files and folders, and Windows System State (New) to an online location

Backups have not been configured for this server. Click "Schedule Backup" in the Actions pane to configure backup options and schedule a regular backup.
Now you can also backup Windows System State and protect your File Servers, Domain Controllers and IIS Web-Servers from corruptions, attacks and disasters. Learn more
You can also Configure Notifications from Alerts blade to receive email alerts for backup failures. Learn More

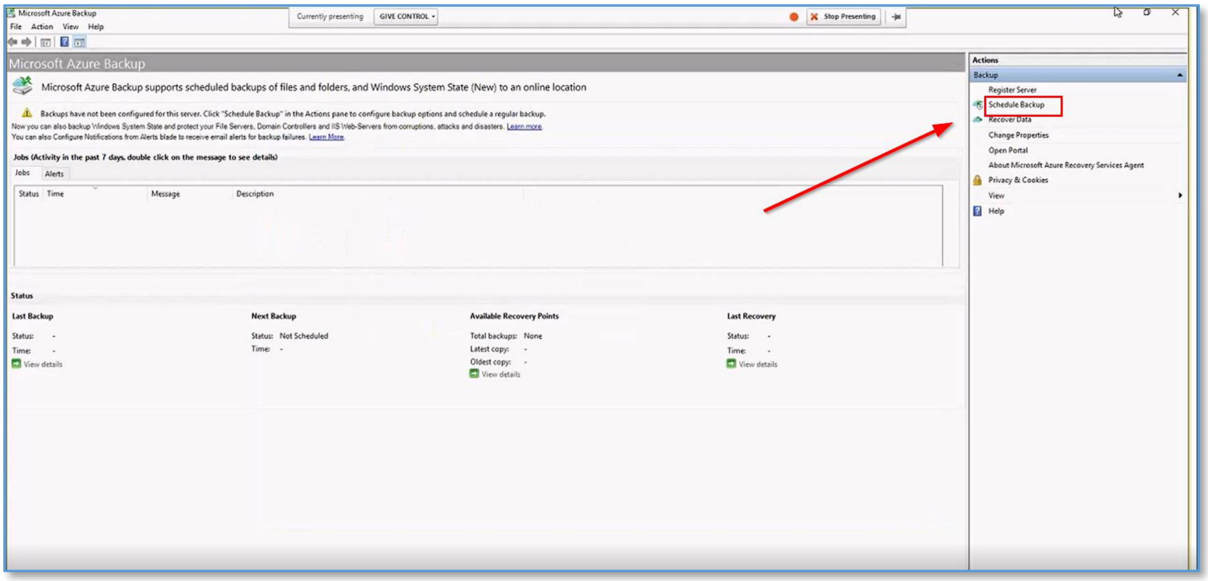
Jobs (Activity in the past 7 days, double click on the message to see details)

Status

Last Backup	Next Backup	Available Recovery Points	Last Recovery
Status: -	Status: Not Scheduled	Total backups: None	Status: -
Time: -	Time: -	Latest copy: -	Time: -
		Oldest copy: -	

Schedule a Backup

1. In the **Microsoft Azure Backup Agent**, click **Schedule Backup**



Microsoft Azure Backup supports scheduled backups of files and folders, and Windows System State (New) to an online location

Backups have not been configured for this server. Click "Schedule Backup" in the Actions pane to configure backup options and schedule a regular backup.
Now you can also backup Windows System State and protect your File Servers, Domain Controllers and IIS Web-Servers from corruptions, attacks and disasters. Learn more
You can also Configure Notifications from Alerts blade to receive email alerts for backup failures. Learn More

Jobs (Activity in the past 7 days, double click on the message to see details)

Jobs | Alerts

Status	Time	Message	Description

Status

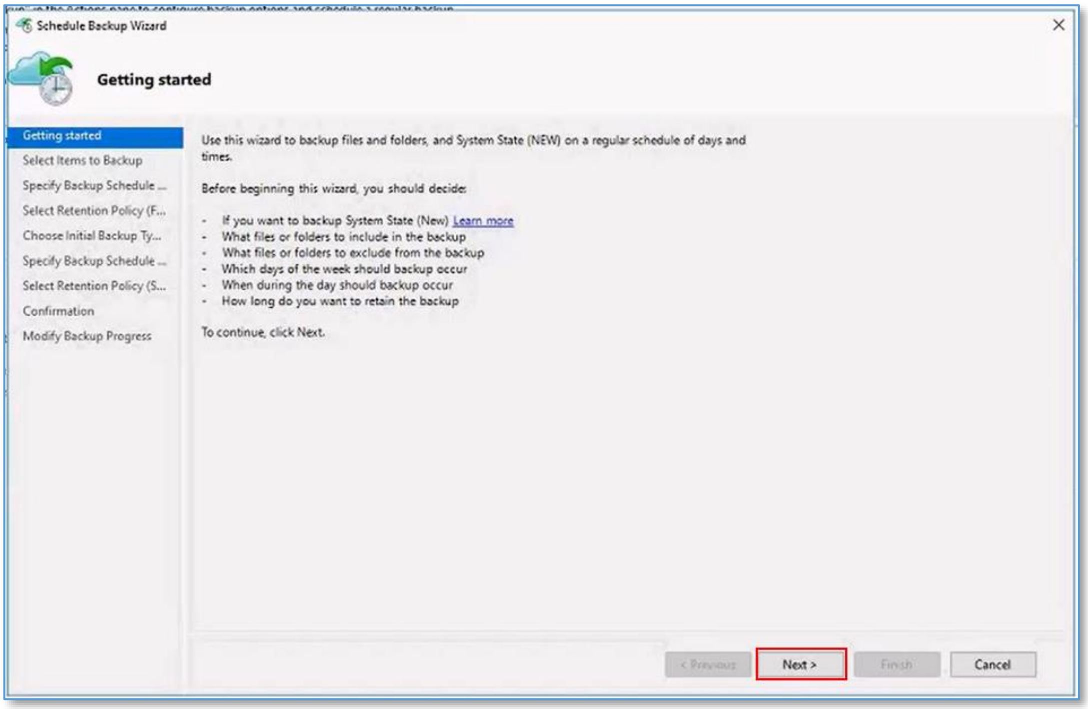
Last Backup
Status: -
Time: -
View details

Next Backup
Status: Not Scheduled
Time: -

Available Recovery Points
Total backups: None
Latest copy: -
Oldest copy: -
View details

Last Recovery
Status: -
Time: -
View details

2. In the **Schedule Backup Wizard** - **Getting started** dialog, click **Next**


Schedule Backup Wizard
Getting started
Getting started
Select Items to Backup
Specify Backup Schedule ...
Select Retention Policy (F...
Choose Initial Backup Ty...
Specify Backup Schedule ...
Select Retention Policy (S...
Confirmation
Modify Backup Progress
< Previous
Next >
Finish
Cancel

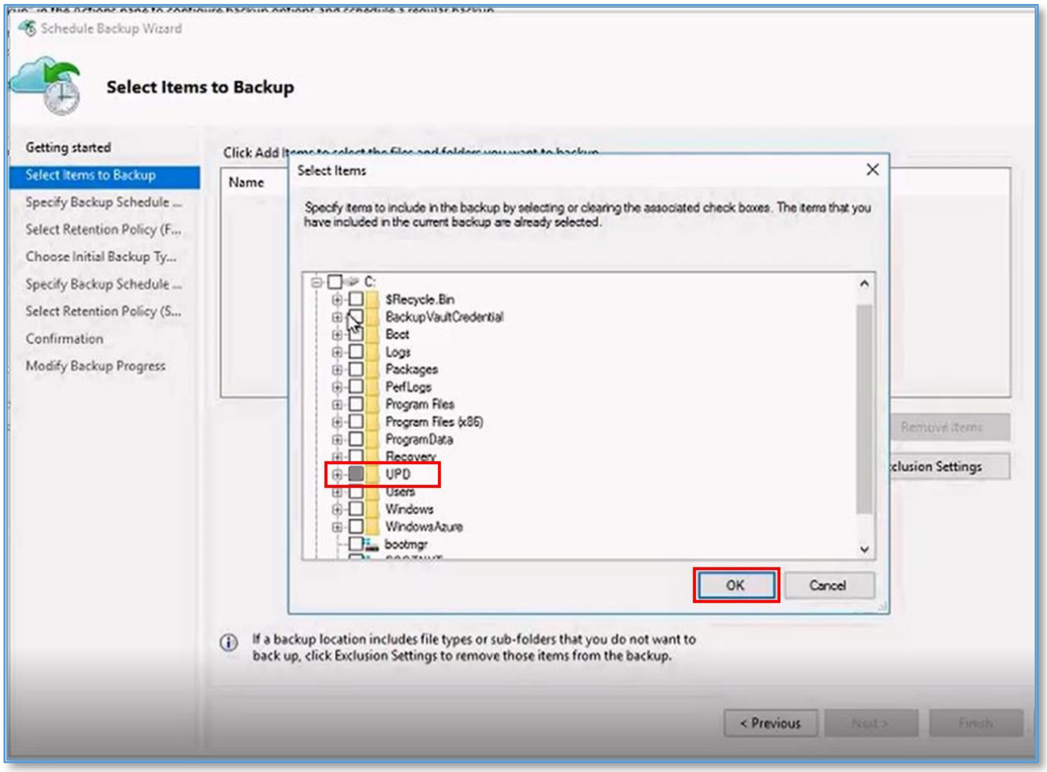
Use this wizard to backup files and folders, and System State (NEW) on a regular schedule of days and times.

Before beginning this wizard, you should decide:

- If you want to backup System State (New) Learn more
- What files or folders to include in the backup
- What files or folders to exclude from the backup
- Which days of the week should backup occur
- When during the day should backup occur
- How long do you want to retain the backup

To continue, click Next.

3. Select any folders that you want to backup into Azure. In our example, we'll backup the **UPD** folder. Expanding the UPD folder will allow you to de-select the OneDrive folders for each user. This keeps the backup footprint smaller.



Schedule Backup Wizard

Select Items to Backup

- Getting started
- Select Items to Backup
- Specify Backup Schedule ...
- Select Retention Policy (F...
- Choose Initial Backup Ty...
- Specify Backup Schedule ...
- Select Retention Policy (S...
- Confirmation
- Modify Backup Progress

Click Add Items to select the files and folders you want to backup.

Name

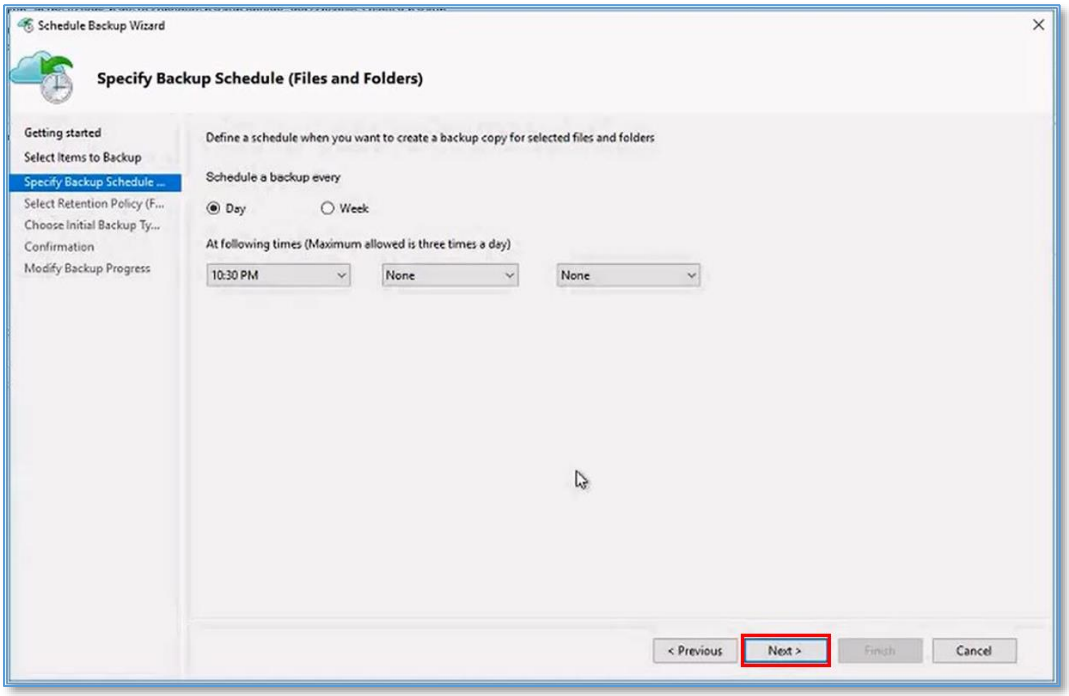
Select Items

Specify items to include in the backup by selecting or clearing the associated check boxes. The items that you have included in the current backup are already selected.

- □ C:
  - □ $Recycle.Bin
  - □ BackupVaultCredential
  - □ Boot
  - □ Logs
  - □ Packages
  - □ PerfLogs
  - □ Program Files
  - □ Program Files (x86)
  - □ ProgramData
  - □ Recovery
  - ■ UPD
  - □ Users
  - □ Windows
  - □ WindowsAzure
  - □ bootmgr

If a backup location includes file types or sub-folders that you do not want to back up, click Exclusion Settings to remove those items from the backup.

4. Specify **Backup Schedule** parameters for the operation, then click **Next**:



Schedule Backup Wizard

Specify Backup Schedule (Files and Folders)

- Getting started
- Select Items to Backup
- Specify Backup Schedule ...
- Select Retention Policy (F...
- Choose Initial Backup Ty...
- Confirmation
- Modify Backup Progress

Define a schedule when you want to create a backup copy for selected files and folders

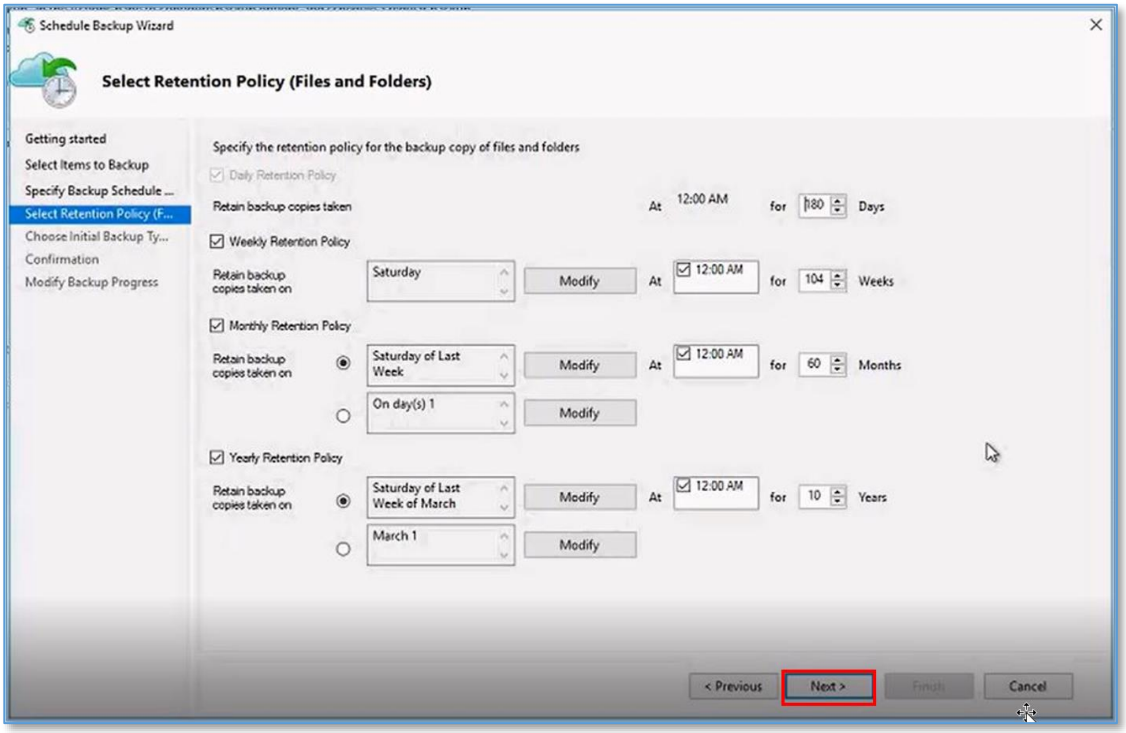
Schedule a backup every

● Day ○ Week

At following times (Maximum allowed is three times a day)

10:30 PM | None | None

5. Select **Retention Policy** parameters for the operation



Select Retention Policy (Files and Folders)

Specify the retention policy for the backup copy of files and folders

☑ Daily Retention Policy

Retain backup copies taken At 12:00 AM for 180 Days

☑ Weekly Retention Policy

Retain backup copies taken on Saturday At ☑ 12:00 AM for 104 Weeks

☑ Monthly Retention Policy

Retain backup copies taken on ● Saturday of Last Week At ☑ 12:00 AM for 60 Months

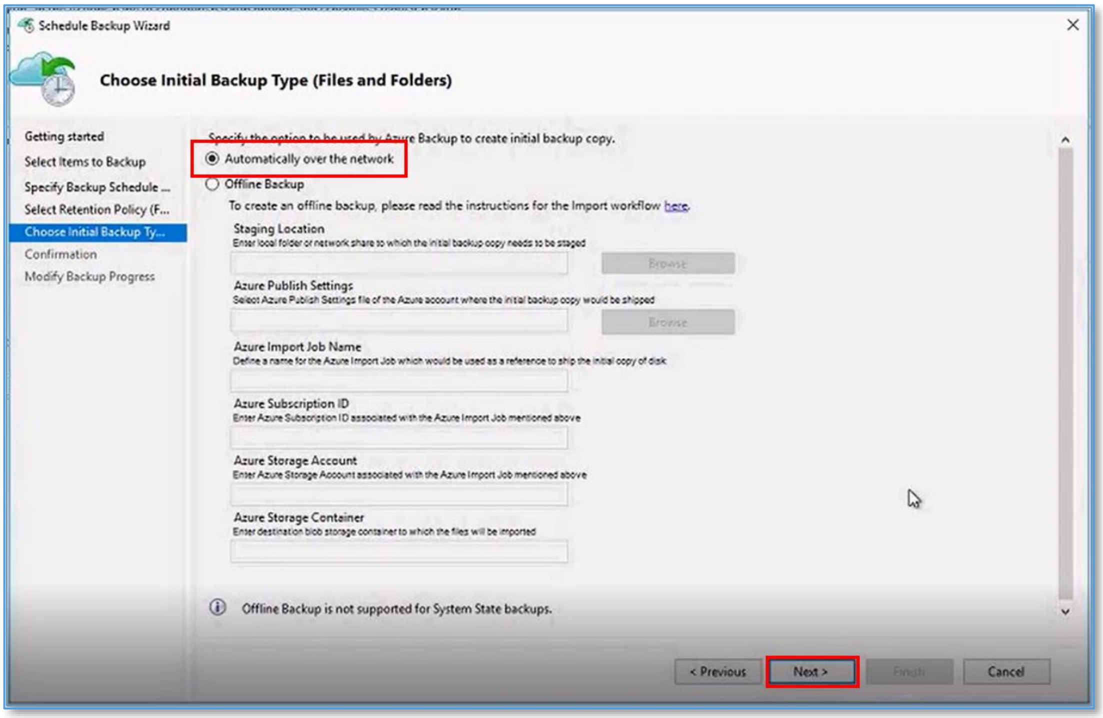
○ On day(s) 1

☑ Yearly Retention Policy

Retain backup copies taken on ● Saturday of Last Week of March At ☑ 12:00 AM for 10 Years

○ March 1

6) Choose **Initial Backup Type** for the operation. In our example, we'll select the default:



Choose Initial Backup Type (Files and Folders)

Specify the option to be used by Azure Backup to create initial backup copy.

● Automatically over the network

○ Offline Backup

To create an offline backup, please read the instructions for the Import workflow here.

Staging Location
Enter local folder or network share to which the initial backup copy needs to be staged

Azure Publish Settings
Select Azure Publish Settings file of the Azure account where the initial backup copy would be shipped

Azure Import Job Name
Define a name for the Azure Import Job which would be used as a reference to ship the initial copy of disk

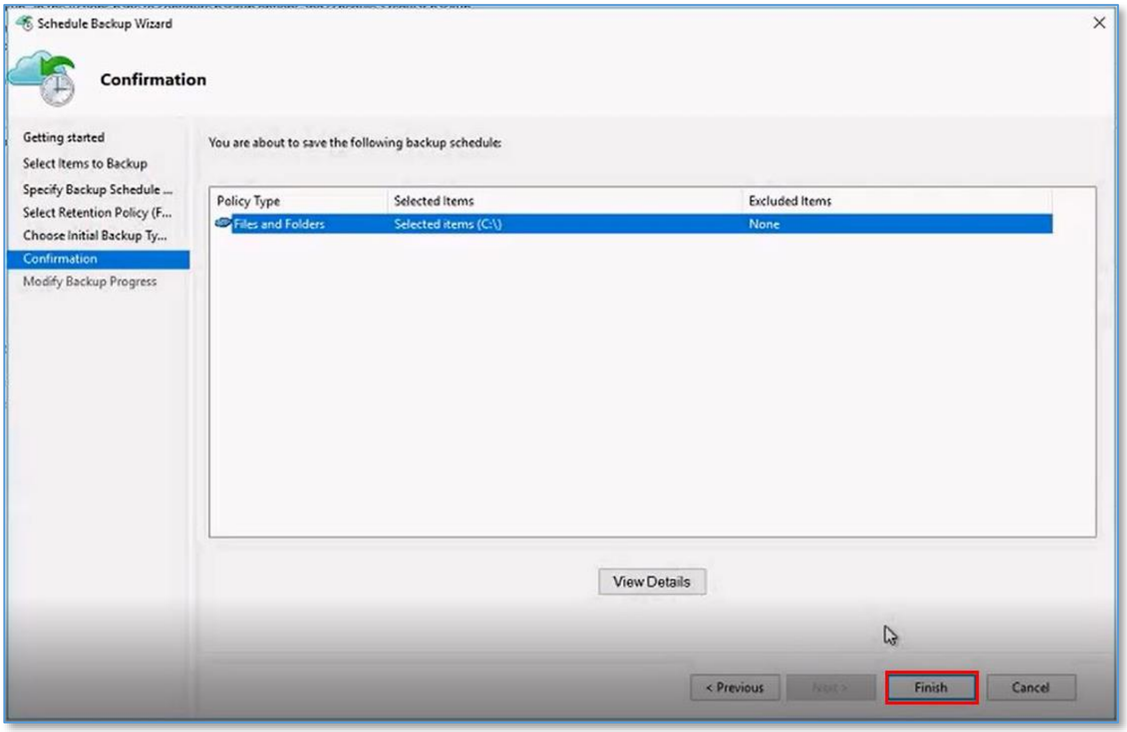
Azure Subscription ID
Enter Azure Subscription ID associated with the Azure Import Job mentioned above

Azure Storage Account
Enter Azure Storage Account associated with the Azure Import Job mentioned above

Azure Storage Container
Enter destination blob storage container to which the files will be imported

Offline Backup is not supported for System State backups.

7) Confirm the selected files and folders, then click **Finish**


Schedule Backup Wizard

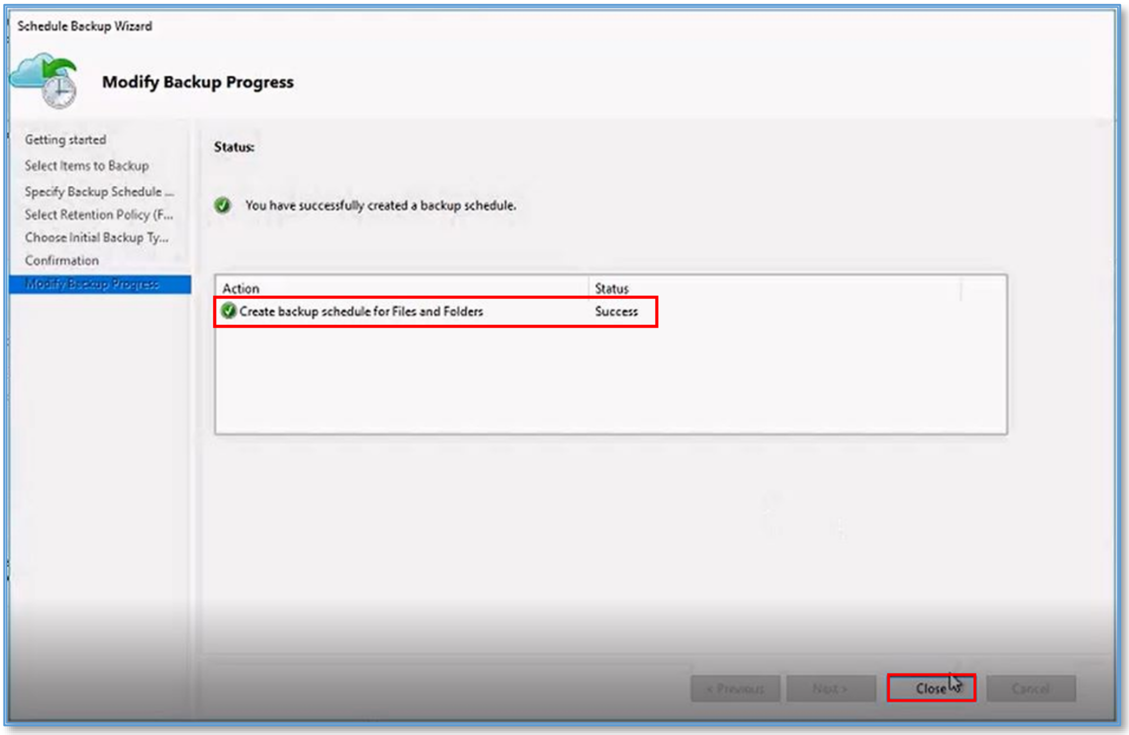
Confirmation

Getting started
Select Items to Backup
Specify Backup Schedule ...
Select Retention Policy (F...
Choose Initial Backup Ty...
Confirmation
Modify Backup Progress

You are about to save the following backup schedule:

Policy Type	Selected Items	Excluded Items
Files and Folders	Selected items (C:\)	None

8) In **Modify Backup Progress**, see the progress of a backup operation, and click **Close** when a backup schedule is successfully created


Schedule Backup Wizard

Modify Backup Progress

Getting started
Select Items to Backup
Specify Backup Schedule ...
Select Retention Policy (F...
Choose Initial Backup Ty...
Confirmation
Modify Backup Progress

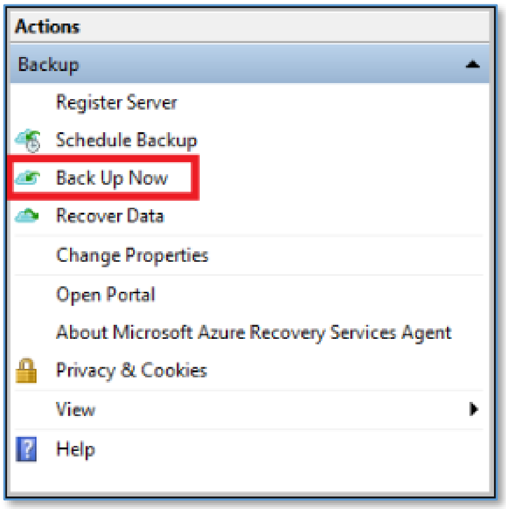
Status:

You have successfully created a backup schedule.

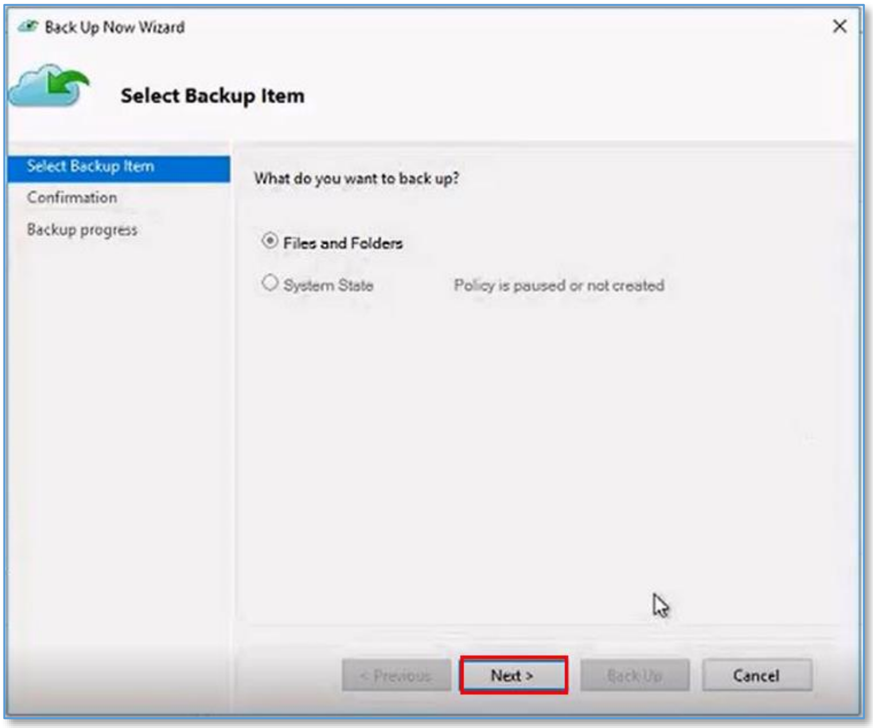
Action	Status
Create backup schedule for Files and Folders	Success

Trigger Dynamic Backup

1) In **Microsoft Azure Backup Agent**, click **Back Up Now**, to take a forced back up for the purpose of testing:



2) In the **Back Up Now Wizard** > **Select Backup item**> **Files and Folders**, then click **Next**

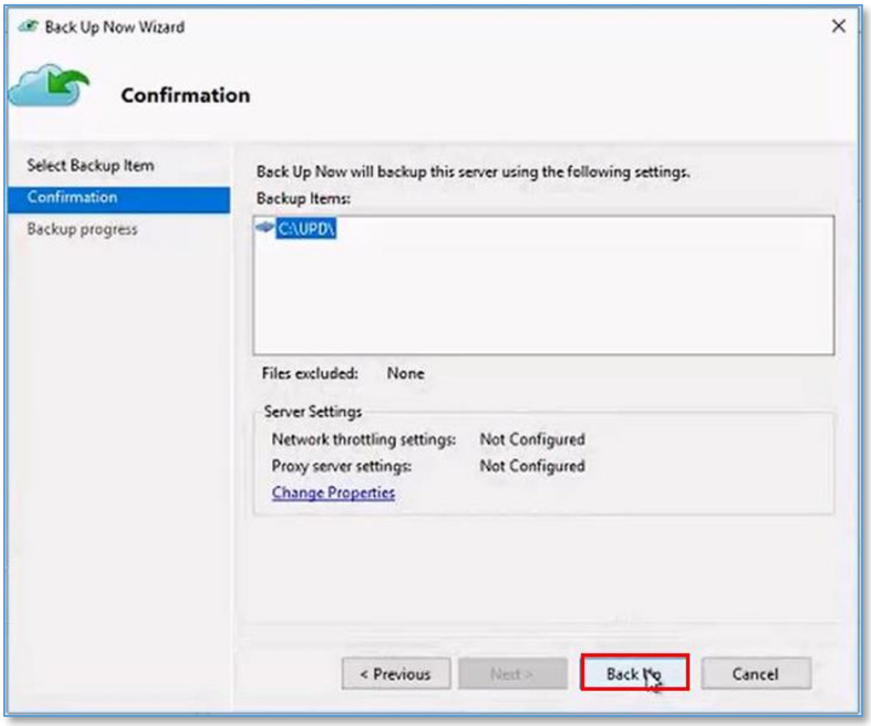


What do you want to back up?

● Files and Folders

○ System State   Policy is paused or not created

3) In **Confirmation**, check the location of files/folder to be backed up, and then click **Back Up.** For the purposes of this example, we are selecting our **C:\UPD** folder:



Back Up Now will backup this server using the following settings.

Backup Items:

C:\UPD\

Files excluded: None

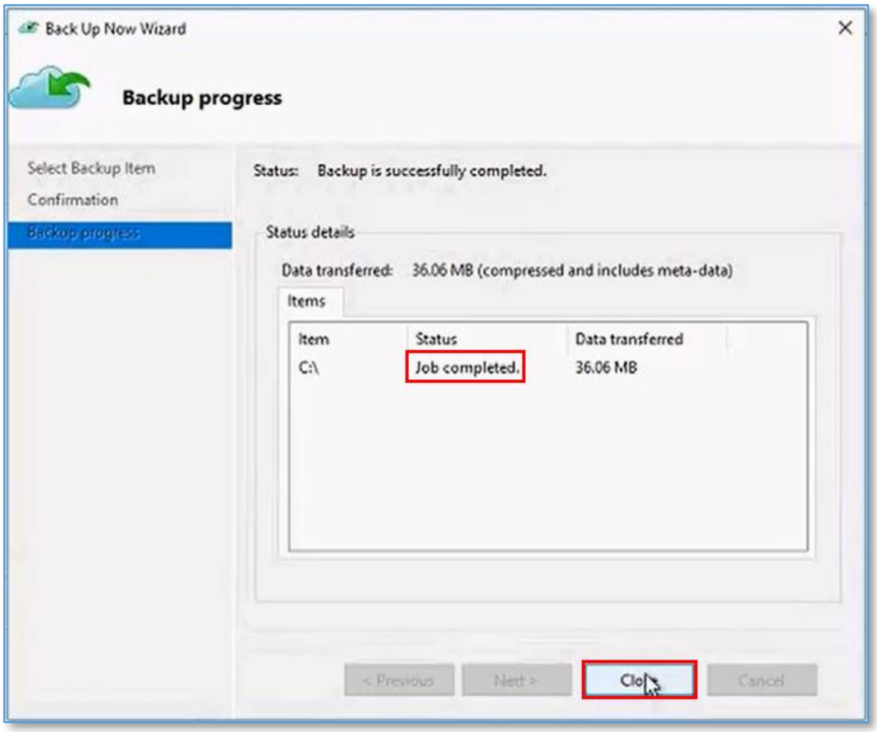
Server Settings

Network throttling settings: Not Configured

Proxy server settings: Not Configured

Change Properties

4) Check **Backup progress**, then click **Close** once the Backup is completed successfully



Status: Backup is successfully completed.

Status details

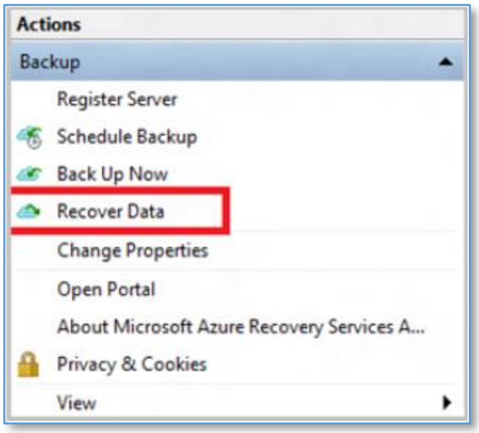
Data transferred: 36.06 MB (compressed and includes meta-data)

Item	Status	Data transferred
C:\	Job completed.	36.06 MB

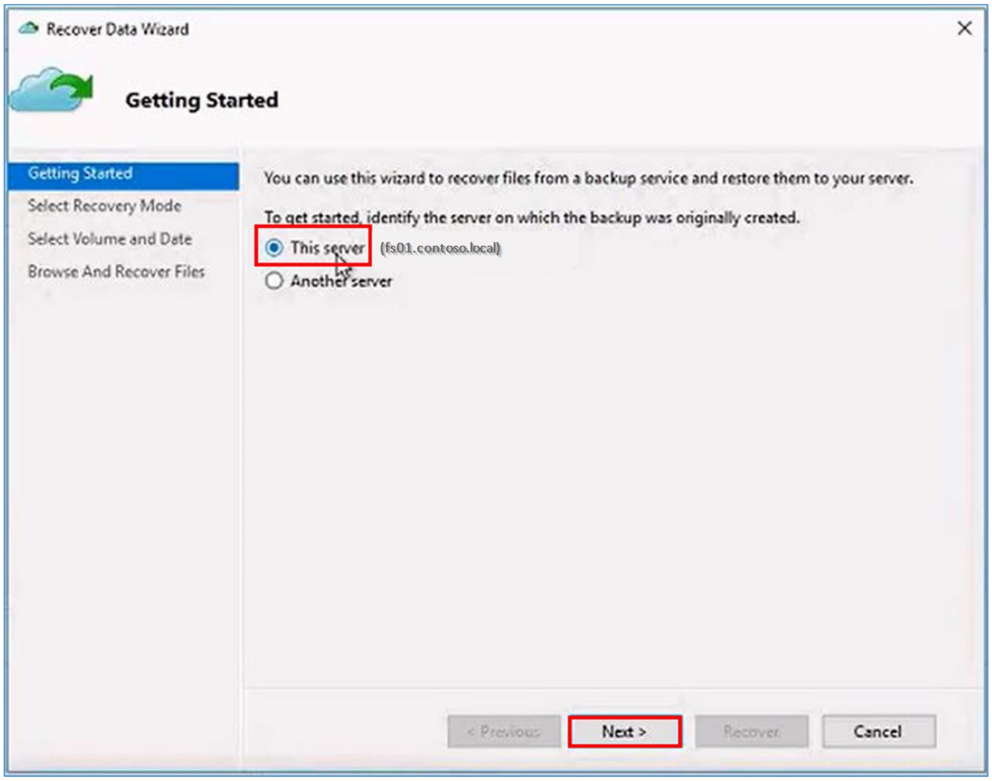
Recover Data Exercise

In this walk-through, we'll recover some files that were backed-up by the Azure Backup Agent.

1. On the system that the backup was taken from, open the **Microsoft Azure Backup** snap-in and click **Recover Data:**



2. On the **Getting started** page> **This server**, click **Next:**



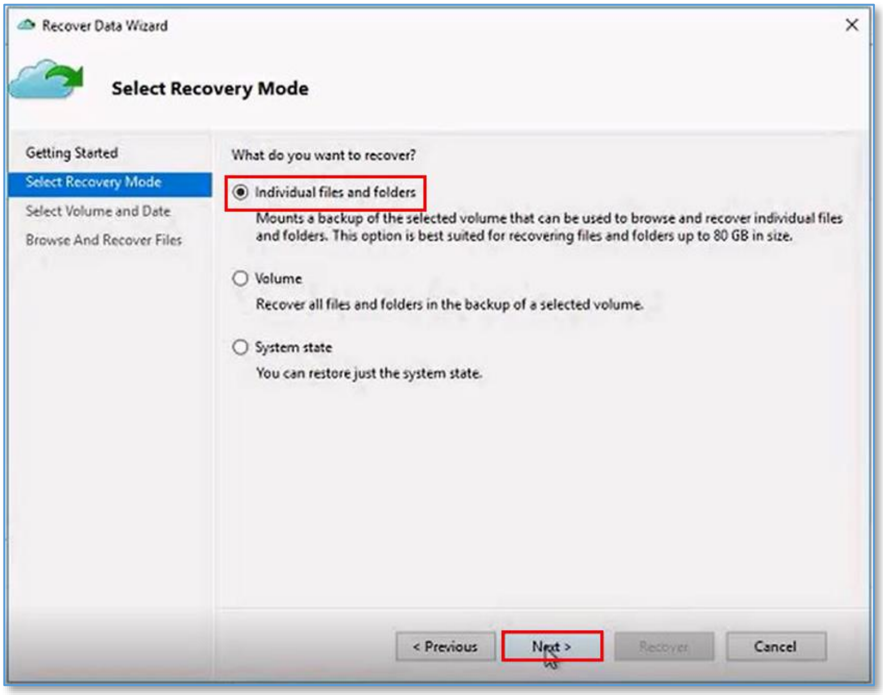
You can use this wizard to recover files from a backup service and restore them to your server.

To get started, identify the server on which the backup was originally created.

● This server (fs01.contoso.local)

○ Another server

3. In **Select Recovery Mode** > **Individual files and folders**, click **Next**



What do you want to recover?

● Individual files and folders

Mounts a backup of the selected volume that can be used to browse and recover individual files and folders. This option is best suited for recovering files and folders up to 80 GB in size.

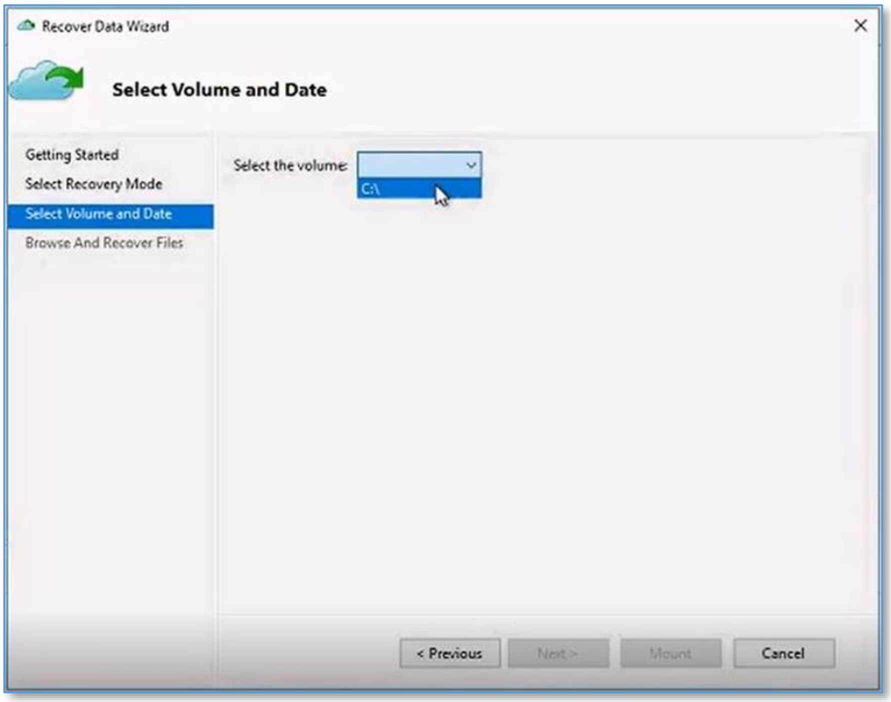
○ Volume

Recover all files and folders in the backup of a selected volume.

○ System state

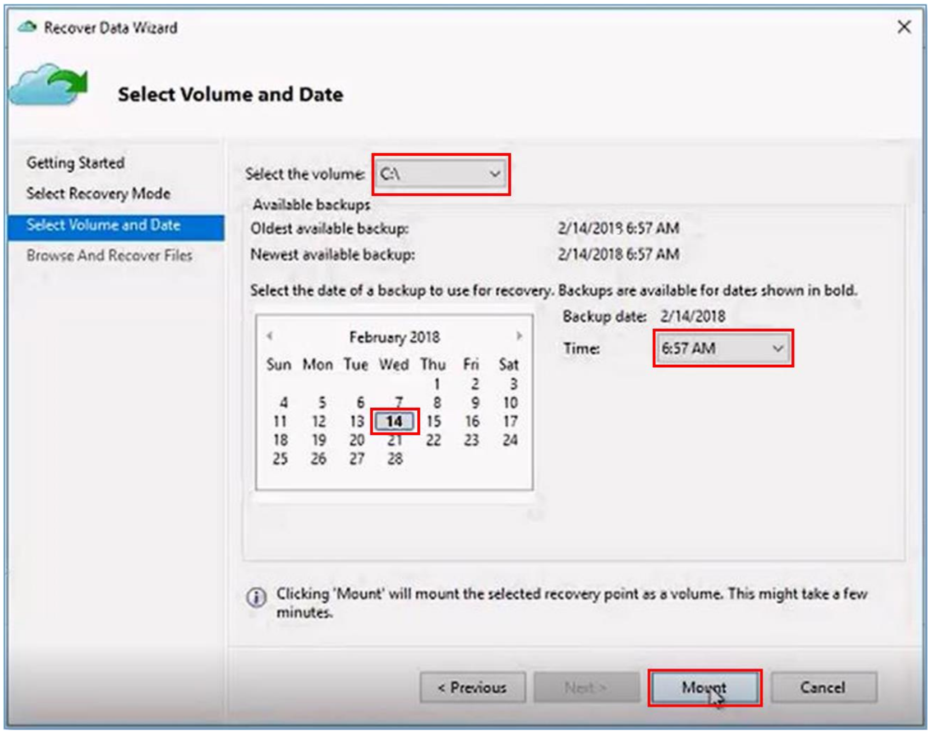
You can restore just the system state.

4. In Select **Volume and Date** select **C:\** as the volume specified for the recovery point:



Select the volume: C:\

5. Select the **date and time** of the Backup to use for this recovery, then click **Mount**



Select Volume and Date

Select the volume: C:\

Available backups

Oldest available backup: 2/14/2018 6:57 AM

Newest available backup: 2/14/2018 6:57 AM

Select the date of a backup to use for recovery. Backups are available for dates shown in bold.

Backup date: 2/14/2018

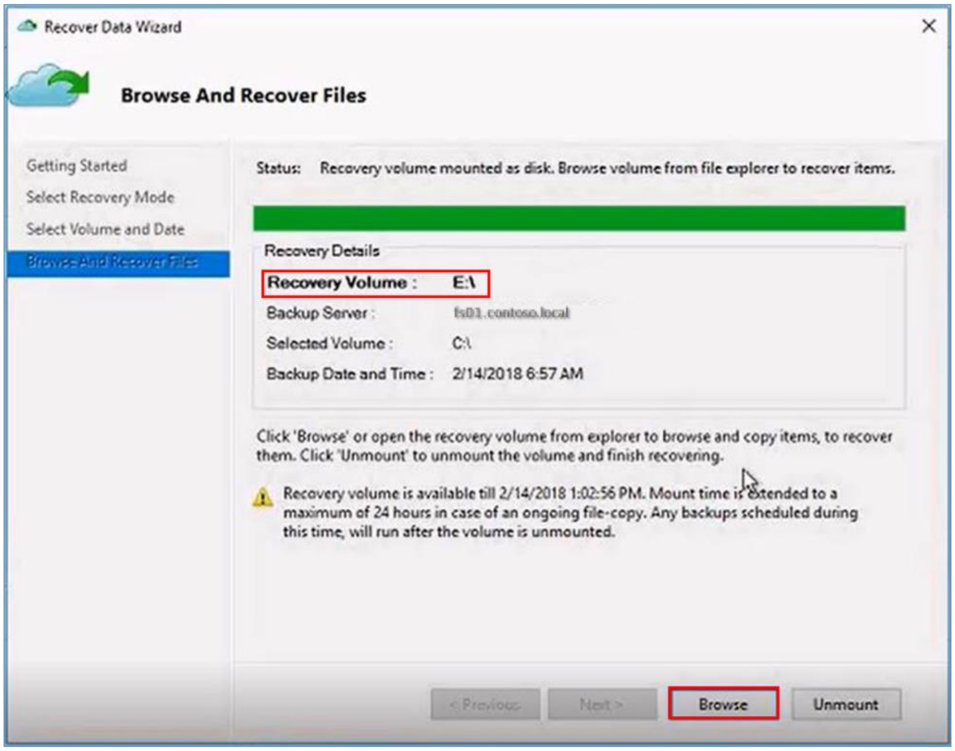
Time: 6:57 AM

February 2018

Sun	Mon	Tue	Wed	Thu	Fri	Sat
				1	2	3
4	5	6	7	8	9	10
11	12	13	**14**	15	16	17
18	19	20	21	22	23	24
25	26	27	28			

ⓘ Clicking 'Mount' will mount the selected recovery point as a volume. This might take a few minutes.

6. Once the files have been recovered, click **Browse** to see the recovered files.



Browse And Recover Files

Status: Recovery volume mounted as disk. Browse volume from file explorer to recover items.

Recovery Details

Recovery Volume : E:\

Backup Server : fs01.contoso.local

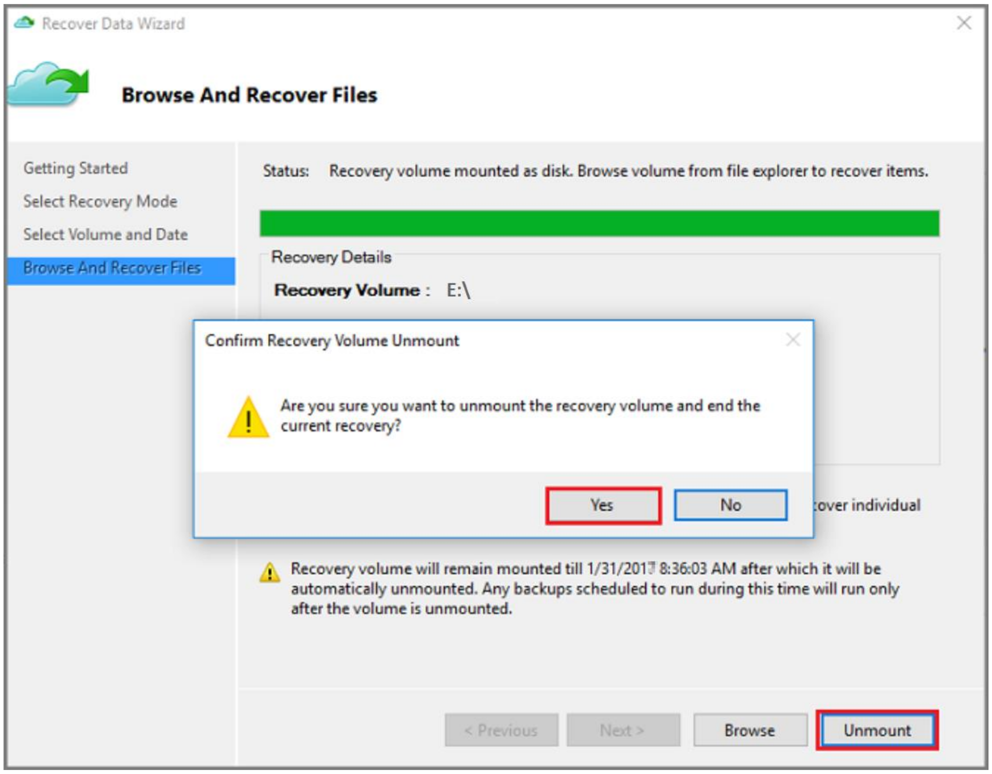
Selected Volume : C:\

Backup Date and Time : 2/14/2018 6:57 AM

Click 'Browse' or open the recovery volume from explorer to browse and copy items, to recover them. Click 'Unmount' to unmount the volume and finish recovering.

⚠ Recovery volume is available till 2/14/2018 1:02:56 PM. Mount time is extended to a maximum of 24 hours in case of an ongoing file-copy. Any backups scheduled during this time, will run after the volume is unmounted.

7. In Windows Explorer, copy the files and folders you want to restore to a different location, then click **Unmount**:



Status: Recovery volume mounted as disk. Browse volume from file explorer to recover items.

Recovery Volume : E:\

Are you sure you want to unmount the recovery volume and end the current recovery?

…over individual

Recovery volume will remain mounted till 1/31/2017 8:36:03 AM after which it will be automatically unmounted. Any backups scheduled to run during this time will run only after the volume is unmounted.

5. Additional Resources

- Back up Windows machines with the Mars agent

6. 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/