

Ahsay Online Backup Manager v8

Microsoft System Backup and Restore Guide

Ahsay Systems Corporation Limited

11 October 2021

Copyright Notice

© 2021 Ahsay Systems Corporation Limited. All rights reserved.

The use and copying of this product is subject to a license agreement. Any other use is prohibited. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system or translated into any language in any form by any means without prior written consent of Ahsay Systems Corporation Limited. Information in this manual is subject to change without notice and does not represent a commitment on the part of the vendor, Ahsay Systems Corporation Limited does not warrant that this document is error free. If you find any errors in this document, please report to Ahsay Systems Corporation Limited in writing.

This product includes software developed by the Apache Software Foundation (<https://www.apache.org/>).

Trademarks

Ahsay, Ahsay Cloud Backup Suite, Ahsay Online Backup Suite, Ahsay Offsite Backup Server, Ahsay Online Backup Manager, Ahsay A-Click Backup, Ahsay Replication Server, Ahsay BackupBox Firmware, Ahsay Universal Backup System and Ahsay NAS Client Utility, Ahsay Mobile are trademarks of Ahsay Systems Corporation Limited.

Amazon S3 is a registered trademark of Amazon Web Services, Inc., or its affiliates.

Apple and Mac OS X, macOS, and iOS are registered trademarks of Apple Computer, Inc.

Dropbox is a registered trademark of Dropbox Inc.

Google Cloud Storage, Google Drive, Google Authenticator, and Android are registered trademarks of Google Inc.

Wasabi Hot Cloud Storage is a registered trademark of Wasabi Technologies Inc.

Backblaze B2 Cloud Storage is a registered trademark of Backblaze Inc.

MariaDB is a registered trademark of MariaDB Corporation AB.

Lotus, Domino, and Notes are registered trademark of IBM Corporation.

Microsoft Windows, Microsoft Exchange Server, Microsoft SQL Server, Microsoft Hyper-V, Microsoft Azure, OneDrive, OneDrive for Business, Microsoft Authenticator, and Microsoft Office 365 are registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Oracle 11g, Oracle 12c, Oracle 18c, Oracle 19c, and MySQL are registered trademarks of Oracle Corporation.

Rackspace and OpenStack are registered trademarks of Rackspace US, Inc.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo and JBoss are registered trademarks of Red Hat, Inc. www.redhat.com in the U.S. and other countries.

Linux is a registered trademark of Linus Torvalds in the U.S. and other countries.

Ubuntu is a registered trademark of Canonical Ltd.

ShadowProtect is a registered trademark of StorageCraft Technology Corporation.

VMware ESXi, vCenter, and vSAN are registered trademarks of VMware, Inc.

All other product names are registered trademarks of their respective owners.

Disclaimer

Ahsay Systems Corporation Limited will not have or accept any liability, obligation or responsibility whatsoever for any loss, destruction or damage (including without limitation consequential loss, destruction or damage) however arising from or in respect of any use or misuse of reliance on this document. By reading and following the instructions in this document, you agree to accept unconditionally the terms of this Disclaimer and as they may be revised and/or amended from time to time by Ahsay Systems Corporation Limited without prior notice to you.

Revision History

Date	Descriptions	Type of modification
3 January 2020	Modified the diagram for the Overview on the Backup Process and added a diagram for the Detailed Process of Periodic Data Integrity Check in Ch. 6	New / Modification
30 July 2020	Added Periodic Backup Schedule in Ch. 3; Modified Periodic Data Integrity Check (PDIC) diagram in Ch. 7; Added Ch. 8.2 Configure Backup Schedule for Automated Backup	New / Modifications
23 September 2020	Updated Overview Backup Process and PDIC in Ch. 7	Modifications
25 January 2021	Updated screenshot in Ch. 2.5; Updated login steps in Ch. 5; Updated PDIC diagram in Ch. 7	Modifications
7 April 2021	Updated Ch. 7; Added sub-chapters for the detailed process diagrams in Ch. 7.1, 7.2, 7.2.1, 7.2.2 and 7.3	New / Modifications
11 October 2021	Updated login instructions in Ch. 5	Modifications

Table of Contents

1	Overview	1
1.1	What is this software?	1
1.2	System Architecture	1
2	Requirements	2
2.1	Hardware Requirement	2
2.2	Software Requirement.....	2
2.3	Antivirus Exclusion Requirement.....	2
2.4	AhsayOBM Installation	2
2.5	AhsayOBM Add-on Module Configuration	2
2.6	Backup Quota Requirement	2
2.7	Java Heap Size	3
2.8	License Requirement.....	3
2.9	Windows Requirement	3
2.10	Temporary Volume.....	4
3	Best Practices and Recommendations	7
4	Restore Consideration	10
5	Logging in to AhsayOBM	11
5.1	Login to AhsayOBM without 2FA.....	11
5.2	Login to AhsayOBM with 2FA using authenticator app	13
5.3	Login to AhsayOBM with 2FA using Twilio	16
6	Configuring a MS Windows System Backup Set	18
	Create a MS Windows System Backup Set.....	18
7	Overview on the Backup Process	30
7.1	Periodic Data Integrity Check (PDIC) Process.....	31
7.2	Backup Set Index Handling Process.....	33
7.2.1	Start Backup Job	33
7.2.2	Completed Backup Job	34
7.3	Data Validation Check Process	35
8	Running a Backup	36
8.1	Start a Manual Backup	36
8.2	Configure Backup Schedule for Automated Backup	43
9	Restore with a MS Windows System Backup Set	48
9.1	Login to AhsayOBM	48
9.2	Restore the System Image	48
9.3	Recovering Your Server	57

9.3.1	Recover Files and Folders.....	59
9.3.2	Recover Applications and Data	66
9.3.3	Recover Volumes	73
9.3.4	Recover Operating System or Full System	80
9.3.5	Recover a Full System (Non Server Platforms)	87
10	Contact Ahsay.....	94
10.1	Technical Assistance.....	94
10.2	Documentation	94
Appendix	95
Appendix A	Cloud Storage as Backup Destination:	95

1 Overview

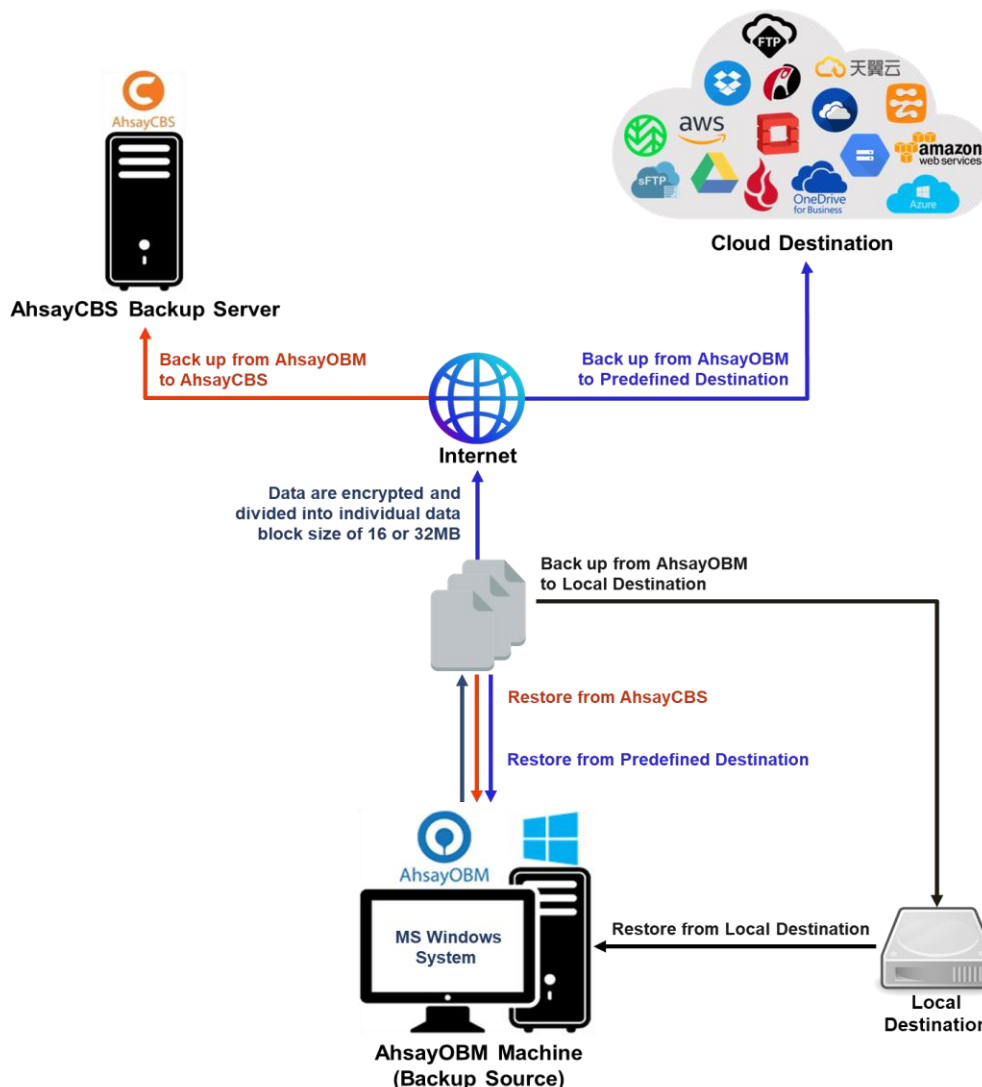
1.1 What is this software?

Ahsay brings you specialized client backup software, namely AhsayOBM, to provide a comprehensive backup solution for your MS Windows System backup. The MS Windows System Backup module of AhsayOBM provides you with a set of tools to protect your mission critical systems / personal computers on Windows operating system platforms. This includes an image-based / bare-metal backup feature, that leverages Microsoft's native Wbadmin command-line tool (<http://go.microsoft.com/fwlink/?LinkId=140216>), and recovery feature, to ensure that your servers and computers are protected even if they are lost or destroyed entirely. The image can be recovered onto a new device if necessary.

1.2 System Architecture

The following high-level system architecture diagram illustrates the major elements involved in the backup process of a MS Windows System backup with AhsayOBM and AhsayCBS.

In this user guide, we will focus on the software installation, as well as the end-to-end backup and restore process using the AhsayOBM as a client backup software.



2 Requirements

2.1 Hardware Requirement

Refer to the following article for the list of hardware requirements for AhsayOBM:
[FAQ: Ahsay Hardware Requirement List \(HRL\) for version 8.1 or above](#)

2.2 Software Requirement

Refer to the following article for the list of compatible Windows operating systems platforms:
[FAQ: Ahsay Software Compatibility List \(SCL\) for version 8.1 or above](#)

2.3 Antivirus Exclusion Requirement

To optimize performance of AhsayOBM on Windows, and to avoid conflict with your antivirus software, refer to the following link for the list of processes and directory paths that should be added to all antivirus software white-list / exclusion list:

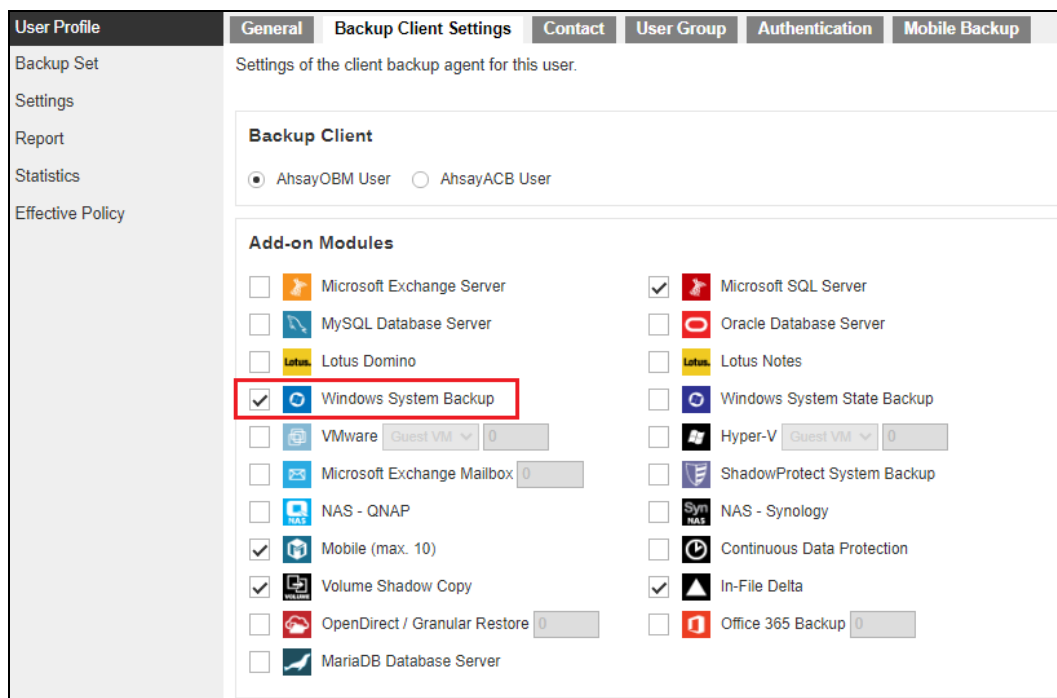
[FAQ: Suggestion on antivirus exclusions to improve performance of Ahsay software on Windows](#)

2.4 AhsayOBM Installation

Make sure that the latest version of AhsayOBM is installed on the computer to be backed up.

2.5 AhsayOBM Add-on Module Configuration

Make sure that the **Windows System Backup** add-on module is enabled in your AhsayOBM user account. Please contact your service provider for more details



2.6 Backup Quota Requirement

Make sure that your AhsayOBM user account has sufficient quota assigned to accommodate the storage for the system backup. Please contact your backup service provider for details.

2.7 Java Heap Size

The default maximum Java heap size on a 64bit Windows machine is 2048M. For better performance especially for in-file delta generation of large image files, it may be advantageous to increase the maximum Java heap size.

For best performance, consider increasing the memory allocation setting for AhsayOBM (Java heap space).

Refer to this link for more details about the modification of the java heap size setting for AhsayOBM:

[FAQ: How to modify the Java heap size setting of AhsayOBM / AhsayACB?](#)

2.8 License Requirement

AhsayOBM licenses are calculated on a per device basis:

- ▶ To back up users with 1 backup client computer (e.g. 1 AhsayOBM installed), 1 AhsayOBM license is required.
- ▶ To back up users with multiple backup client computers, the number of AhsayOBM licenses required is equal to the number of devices. For example, if there are 10 users to be backed up with 3 backup client computers, then 30 AhsayOBM licenses are required. Please contact your backup service provider for more details.

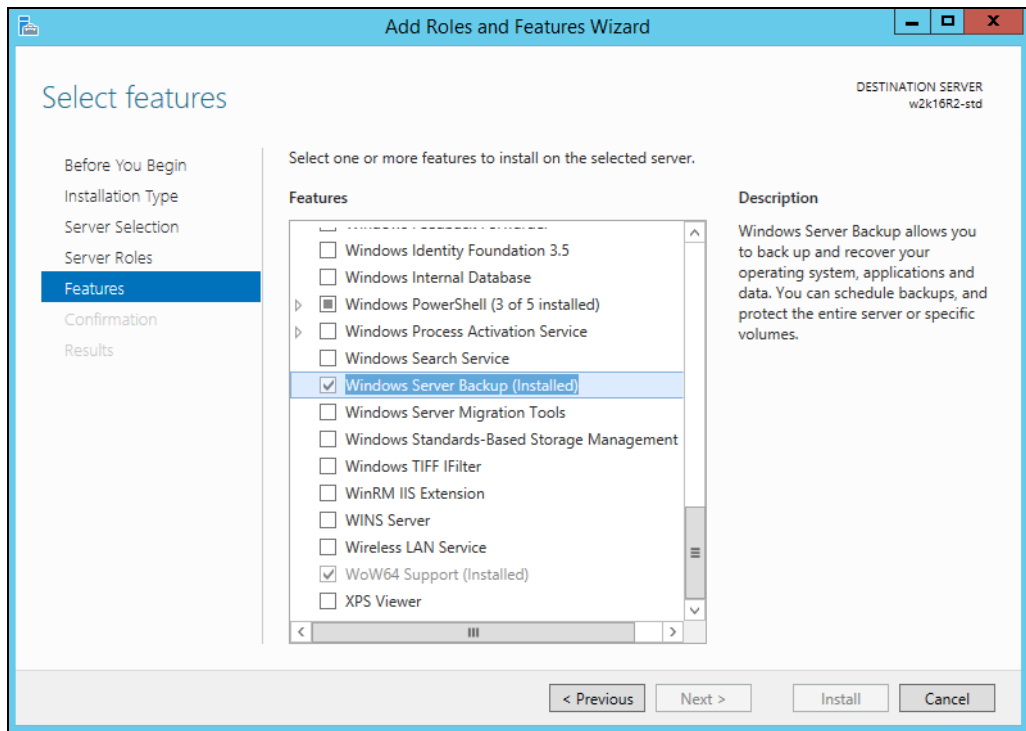
2.9 Windows Requirement

▶ Windows Server Backup (WSB) Features

The following Windows Server Backup features must be installed on the computer to be backed up:

- ◉ Windows Server Backup
- ◉ Command line Tool
- ◉ Windows PowerShell

This can be confirmed in the Server Manager. These features can be added by selecting **Add Roles and Features**.



- **Windows Account Permission**

To perform recovery using Windows Server Backup, the operating system account you are using must be a member of the Backup Operators or Administrators group.

- **System Volume**

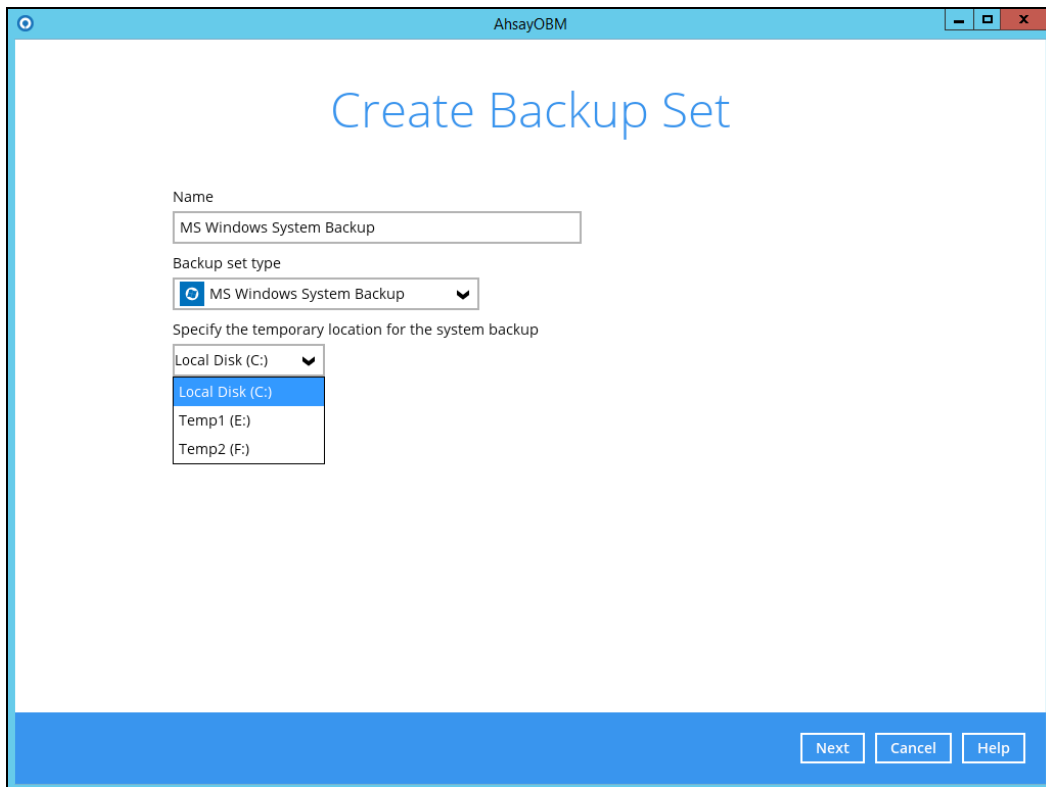
The system volume must be formatted with NTFS.

- **Latest Service Packs from Microsoft**

Ensure that you have the latest service packs installed. Updates to the Windows operating system improve its performance and resolve known issues with Windows Server Backup.

2.10 Temporary Volume

Make sure that the storage location configured for the system image is set to a supported location.



The temporary storage location is required by the WBADMIN utility to temporarily store the image file during the backup job.

The machine requires an additional drive to accommodate the spooling of the System State image file. As you can see on our sample screen shot above, we have three (3) drives in total, Local Disk C:, Temp1 E:, and Temp2 F:

If the machine has only one (1) drive, then one of the following options will need to be implemented to create the temporary volume.

- A USB drive needs to be connected
- The existing C: drive will need to be repartitioned to create an additional drive, i.e. D:
- An extra physical drive will need to be installed
- Set up a network drive (the least preferred option as it will affect the backup performance)

For more details about the restrictions, please refer to the following link:

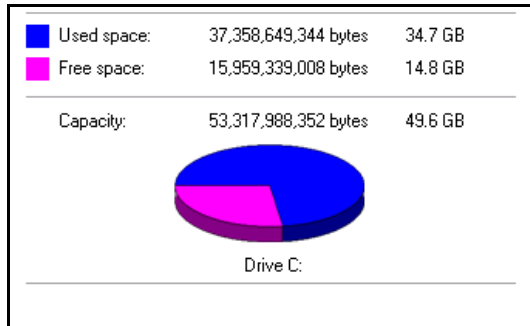
[FAQ: Restrictions on the temporary storage location for the Windows System State and System backup image file](#)

● **Disk Space Available in Temporary Storage Location**

Make sure that there is sufficient disk space available in the storage location for the backup set.

For a system backup, it will typically require disk space of the total used size of all volumes selected for backup.

Note: *Used space, not free space of all volumes selected for backup.*



• **Maximum Supported Disk Size**

For Windows Vista, or 2008 / 2008 R2 Server, source volumes with size greater than 2 TB (e.g. 2040 GB - 2 MB = 2088958 MB) are not supported.

This limitation is related to the .vhd file size limit.

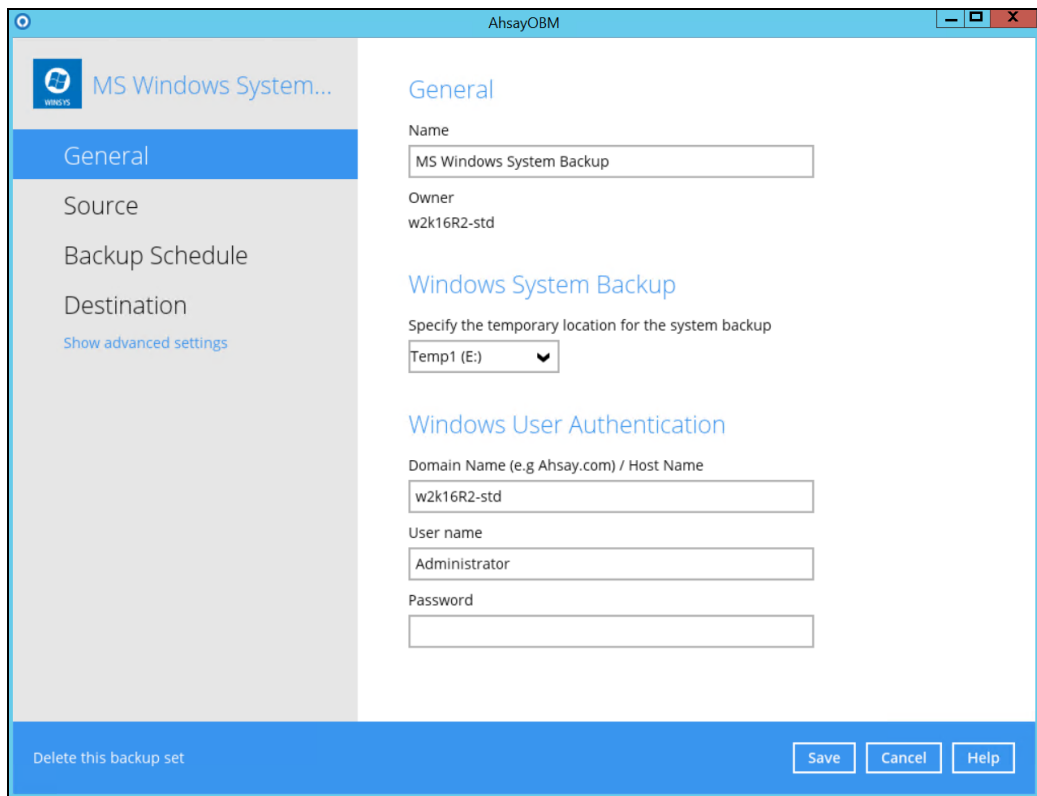
Note: This limitation does not apply to Windows 8 or newer releases of Windows platforms.

3 Best Practices and Recommendations

The following are some best practices or recommendations that we strongly recommend, before you start any Microsoft System backup and restore:

1 Temporary Directory Folder Location

For best performance, it is recommended that the temporary storage location of a MS Windows System backup set is set to a supported local volume, and not to a network volume (e.g. to improve I/O performance). The temporary storage location is highly recommended to be set on a directory with sufficient free disk space and located to another location other than Drive C: (e.g. Drive E:).



NOTE

Kindly note that for Windows Server 2008 or newer releases, the restriction on temporary volume (Ch 2.10) must also be considered.

1 Backup Destination

To provide maximum data protection and flexible restore options, it is recommended to configure:

- At least one offsite or cloud destination
- At least one local destination for fast recovery

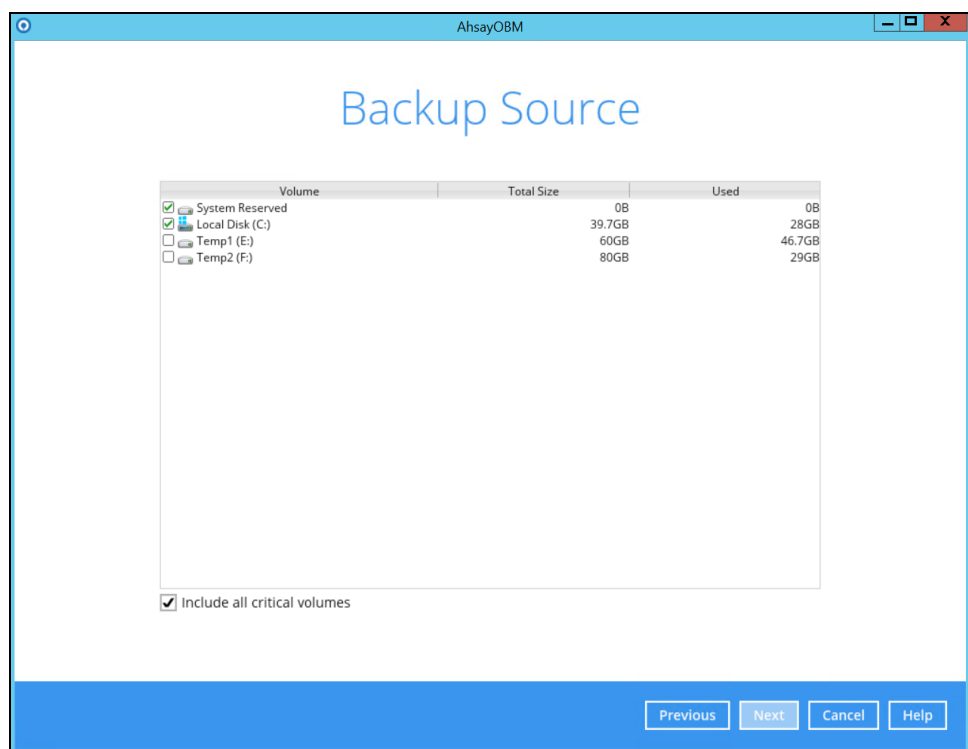
1 Backup Frequency

MS Windows System backup should be performed at least once per week.

Performance Recommendations

Consider the following best practices for optimized performance of the backup operations:

- Enable schedule backup jobs when system activity is low to achieve the best possible performance.
- Perform test restores periodically to ensure your backup is set up and performed properly. Performing recovery test can also help identify potential issues or gaps in your recovery plan. It's important that you do not try to make the test easier, as the objective of a successful test is not to demonstrate that everything is flawless. There might be flaws identified in the plan throughout the test and it is important
- It is highly recommended to enable the **Include all critical volumes** option to select all critical volumes for backup automatically.



This will ensure that the backup image can be used for full-system / bare-metal recovery.

Not a Replacement for File Backup

An image-based / bare-metal backup should never be considered a replacement for a nightly data backup plan.

Firstly, image-based backups do not lend themselves easily to recovery of a single file. The nature of image-based backup requires a complete restore of the system image file, even if you only want to recover a single file.

System Recovery Plan

Consider performing routine system recovery test to ensure your system backup is setup and performed properly. Performing system recovery test can also help identify potential issues or gaps in your system recovery plan.

For best result, it is recommended that you should keep the test as close as possible to a real situation. Often when a recovery test is to take place, administrators will plan for the test (e.g. reconfiguring the test environments, restoring certain data in advance). For real recovery situation, you will not get a chance to do that.

It's important that you do not try to make the test easier, as the objective of a successful test is not to demonstrate that everything is flawless. There might be flaws identified in the plan throughout the test and it is important to identify those flaws.

❶ **Restore to Alternate Computer**

You can restore a system backup to the same physical computer from which the system backup was created, or to a different computer that has the same make, model, and configuration (identical hardware). Microsoft does not support restoring a system backup from one computer to a second computer of a different make, model, or hardware configuration.

Please refer to the following article for more details:

<http://support.microsoft.com/kb/249694>

❷ **Periodic Backup Schedule**

The periodic backup schedule should be reviewed regularly to ensure that the interval is sufficient to handle the data volume on the machine. Over time, data usage pattern may change on a production server, i.e. the number of new files created, the number of files which are updated/deleted, and new users may be added etc.

Consider the following key points to efficiently handle backup sets with periodic backup schedule.

- ❶ Hardware – to achieve optimal performance, compatible hardware requirements is a must. Ensure you have the backup machine's appropriate hardware specifications to accommodate frequency of backups
 - so that the data is always backed up within the periodic backup interval
 - so that the backup frequency does not affect the performance of the production server.
- ❷ Network – make sure to have enough network bandwidth to accommodate the volume of data within the backup interval.
- ❸ Retention Policy - also make sure to consider the retention policy settings and retention area storage management which can grow because of the changes in the backup data for each backup job.

4 Restore Consideration

Please consider the following before performing a MS System restore:

- Windows Account Permission

To perform recovery using Windows Server Backup, the operating system account that you use, must be a member of the Backup Operators or Administrators group.

- Disk Size

For recovery of operating system to a new hard disk, ensure that the disk that you restore to is at least the size of the disk that contained the volumes that were backed up, regardless of the size of those volumes within.

For example, if there was only one volume of size 100 GB created on a 1 TB disk during backup, then you should use a disk that is at least 1 TB when recovering.

- Windows Recovery Environment

For recovery of operating system, the processor architecture for a given instance of Windows Recovery Environment and the computer whose system you are trying to restore must match.

For example, Windows Recovery Environment for an x64 based version of the operating system will only work on an x64 based server.

- Caution on Recovery to Dissimilar Hardware

This recovery method requires the restore target system to have similar hardware and the exact same boot type as the source system from which the backup was taken. Disk adapters are especially sensitive. If dissimilar hardware is used, the restored system might not be boot.

For example, if the system backup image was taken from a BIOS-based system, the recovery environment must be booted in BIOS mode.

- BitLocker Drive

For server with BitLocker Drive Encryption enabled, make sure to re-apply BitLocker Drive Encryption to the server after a restore.

This will not happen automatically; it must be enabled explicitly.

For instructions, refers to the following: <http://go.microsoft.com/fwlink/?LinkID=143722>

5 Logging in to AhsayOBM

Starting with AhsayOBM v8.5.0.0, there are several login scenarios depending on the setting of the account you are using. The different scenarios will be discussed below:

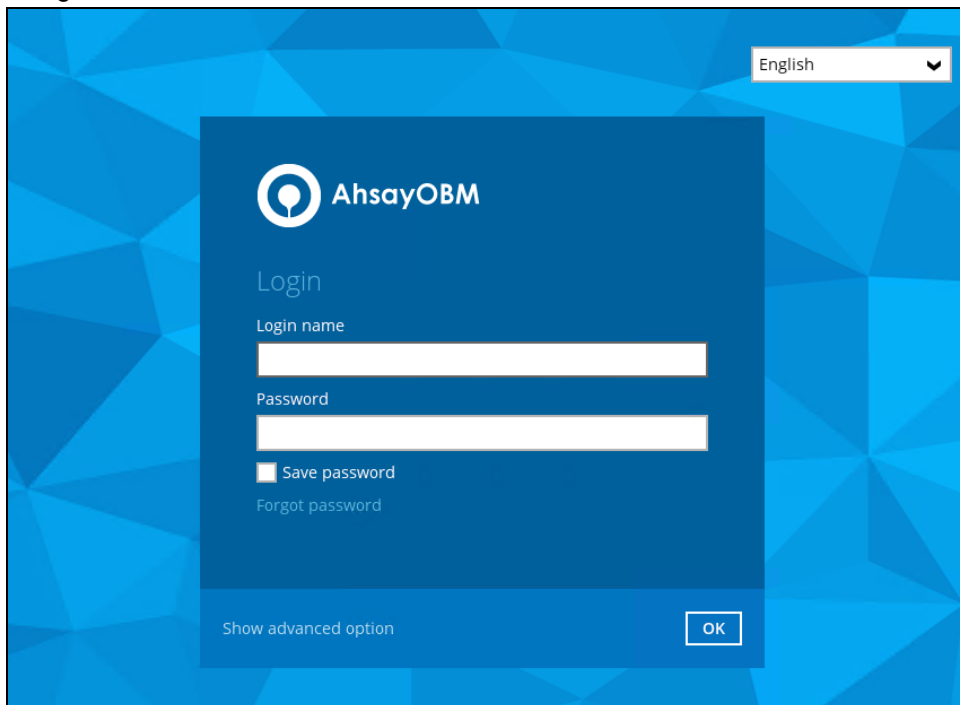
- [Login without 2FA](#)
- [Login with 2FA using authenticator app](#)
- [Login with 2FA using Twilio](#)

5.1 Login to AhsayOBM without 2FA

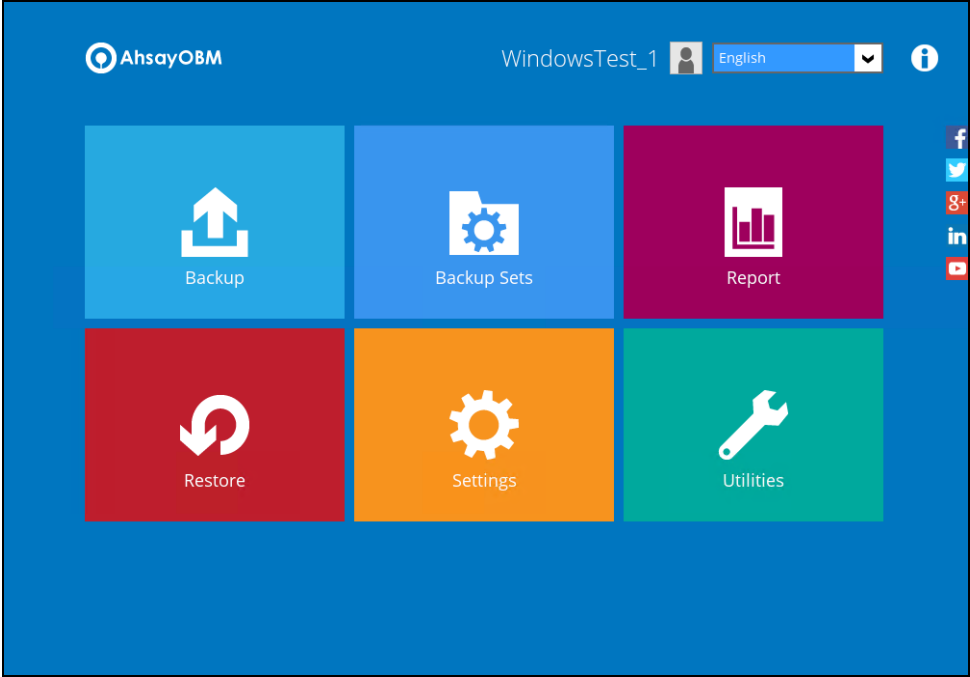
1. Log in to the AhsayOBM application user interface. Double-click the AhsayOBM desktop icon to launch the application.



2. Enter the **Login name** and **Password** of your AhsayOBM account, then click **OK** to log in.

The image shows the AhsayOBM login interface. It features a dark blue background with a white AhsayOBM logo and the text 'AhsayOBM' at the top. Below the logo, the word 'Login' is displayed. There are two input fields: 'Login name' and 'Password'. Below the 'Password' field, there is a checkbox labeled 'Save password' and a link for 'Forgot password'. At the bottom left, there is a link for 'Show advanced option', and at the bottom right, there is an 'OK' button. In the top right corner, there is a language dropdown menu set to 'English'.

3. After successful login, the following screen will appear.



5.2 Login to AhsayOBM with 2FA using authenticator app

1. Log in to the AhsayOBM application user interface. Double-click the AhsayOBM desktop icon to launch the application.



2. Enter the **Login name** and **Password** of your AhsayOBM account, then click **OK** to log in.

The image shows the AhsayOBM login form. It features a dark blue background with a white AhsayOBM logo and the text 'AhsayOBM'. Below the logo, the word 'Login' is displayed. There are two input fields: 'Login name' and 'Password'. A 'Save password' checkbox is present, along with a 'Forgot password' link. At the bottom, there is a 'Show advanced option' link and an 'OK' button. A language dropdown menu in the top right corner is set to 'English'.

3. One of the two authentication methods will be displayed to continue with the login:

- [Push Notification and TOTP when using Ahsay Mobile app](#)
- [TOTP only](#)

➤ If **Ahsay Mobile app** was configured to use Push Notification and TOTP, then there are two 2FA modes that can be used:

- Push Notification (default)

Push notification is the default 2FA mode. Accept the login request on Ahsay Mobile to complete the login.

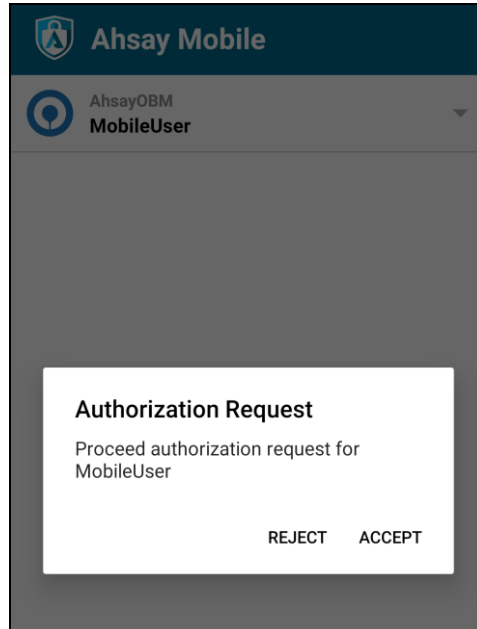
Two-Factor Authentication

Please approve notification request in one of registered Authenticator App.

⌚ Waiting for response (00:04:36)

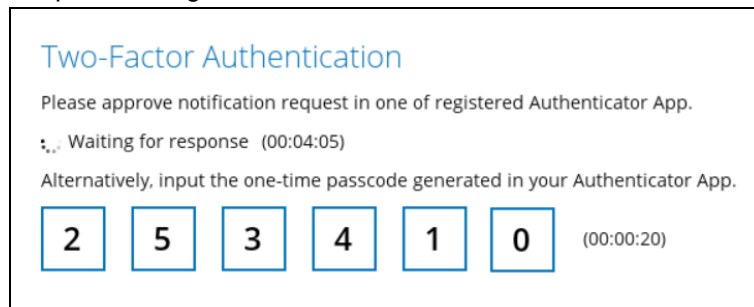
[Authenticate with one-time password](#)

Example of the login request sent to the Ahsay Mobile app.

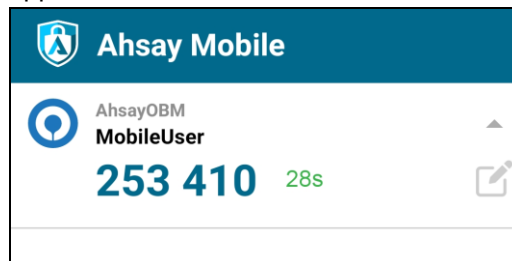


- TOTP

However, if push notification is not working or you prefer to use one-time passcode, click the [Authenticate with one-time password](#) link, then input the one-time passcode generated by Ahsay Mobile to complete the login.

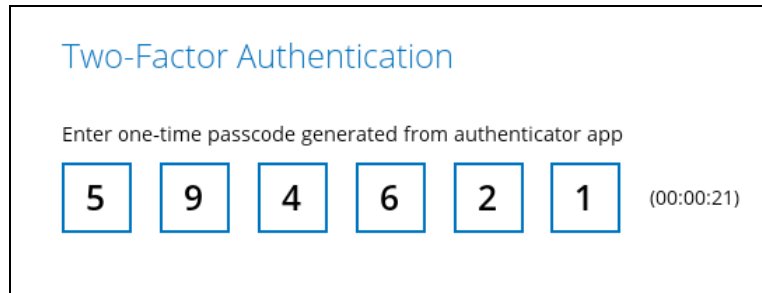


Example of the one-time passcode generated in the Ahsay Mobile app.

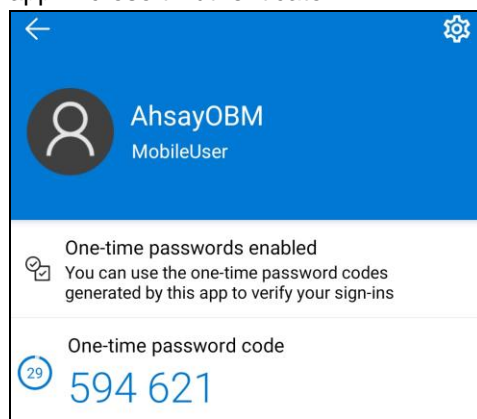


➤ TOTP only

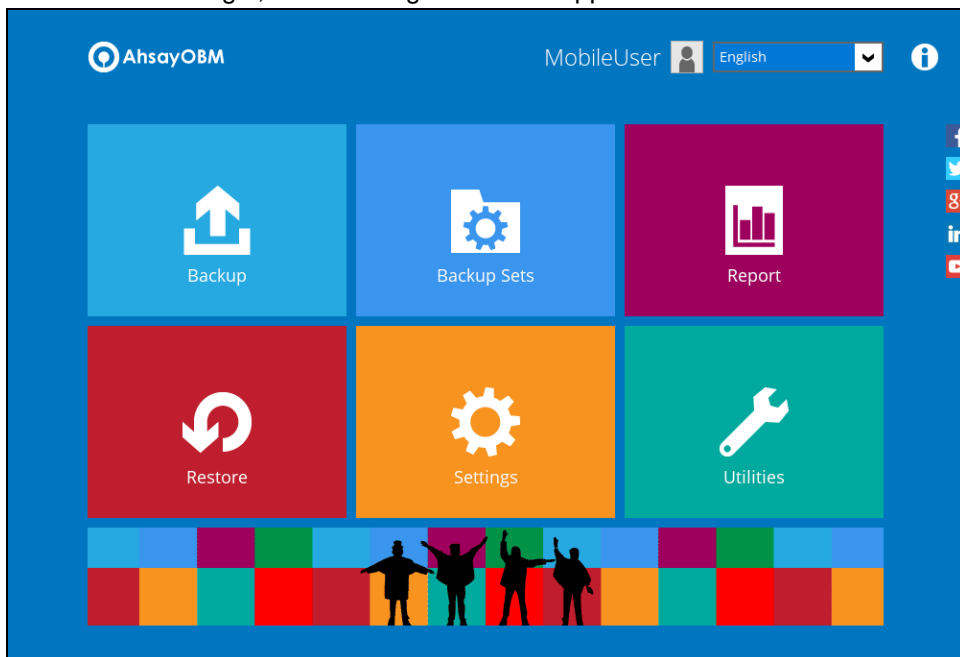
Enter the one-time passcode generated by the authenticator app to complete the login.



Example of the one-time passcode generated in the third-party authenticator app Microsoft Authenticator.



4. After successful login, the following screen will appear.



NOTE

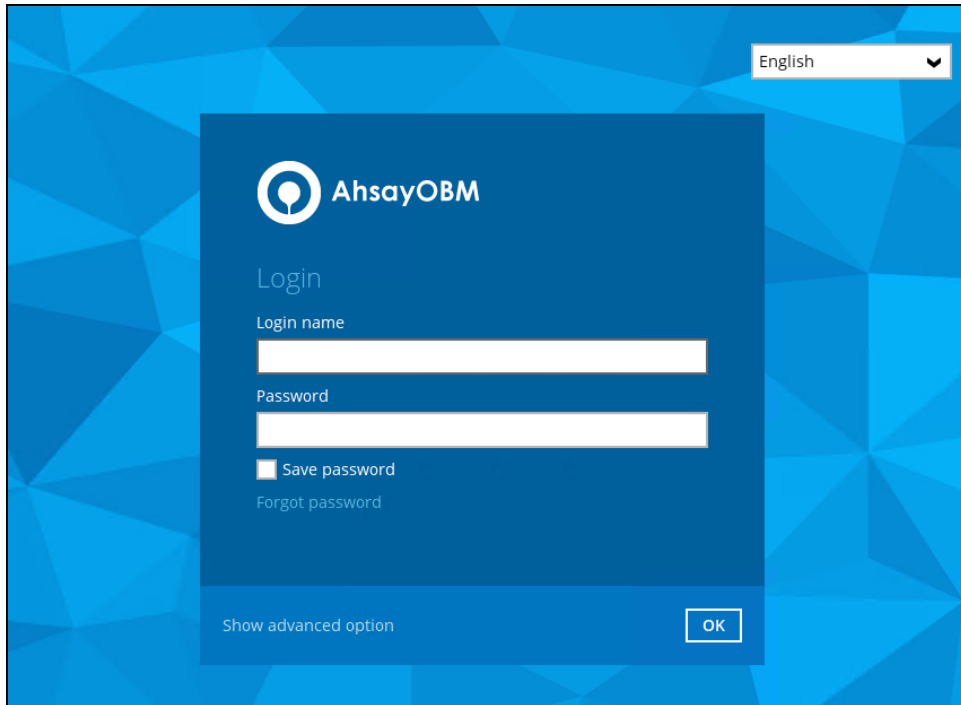
If you have trouble logging in using the authenticator app, please refer to Chapter 9 of the [AhsayOBM Quick Start Guide for Windows](#) for more information.

5.3 Login to AhsayOBM with 2FA using Twilio

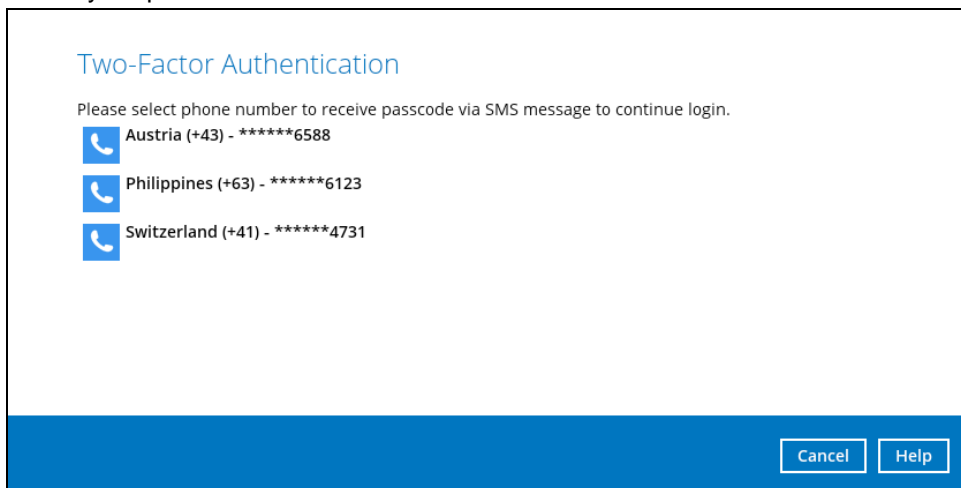
1. Log in to the AhsayOBM application user interface. Double-click the AhsayOBM desktop icon to launch the application.



2. Enter the **Login name** and **Password** of your AhsayOBM account, then click **OK** to log in.

The image shows the AhsayOBM login interface. It features a blue background with a geometric pattern. In the top right corner, there is a language dropdown menu set to 'English'. The main content is a dark blue login box with the AhsayOBM logo and name at the top. Below the logo, the word 'Login' is displayed. There are two input fields: 'Login name' and 'Password'. Below the password field, there is a checkbox for 'Save password' and a link for 'Forgot password'. At the bottom of the login box, there is a 'Show advanced option' link and an 'OK' button.

3. Select your phone number.

The image shows the Two-Factor Authentication (2FA) screen. The title is 'Two-Factor Authentication'. Below the title, there is a message: 'Please select phone number to receive passcode via SMS message to continue login.' There are three radio button options, each with a phone icon: 'Austria (+43) - *****6588', 'Philippines (+63) - *****6123', and 'Switzerland (+41) - *****4731'. At the bottom right, there are 'Cancel' and 'Help' buttons.

4. Enter the passcode and click **Verify** to login.

Two-Factor Authentication

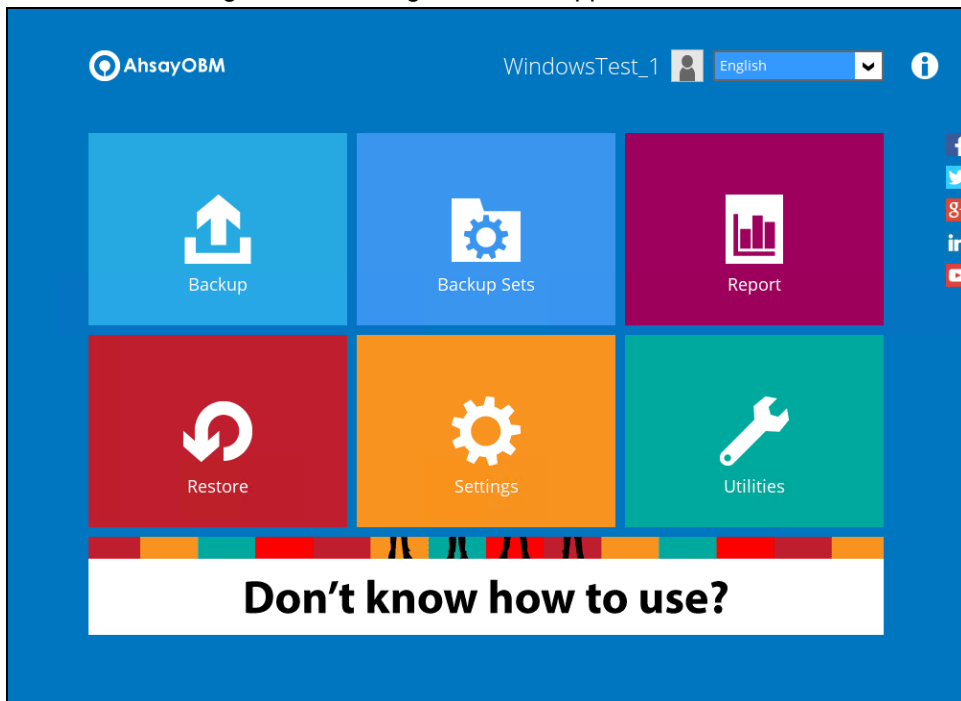
SMS message with a passcode was already sent to the phone number Philippines (+63) - *****6123
Please enter the passcode to continue login.

EUVS - (00:03:59)

[Resend passcode](#)

[Verify](#) [Cancel](#) [Help](#)

5. After successful login, the following screen will appear.




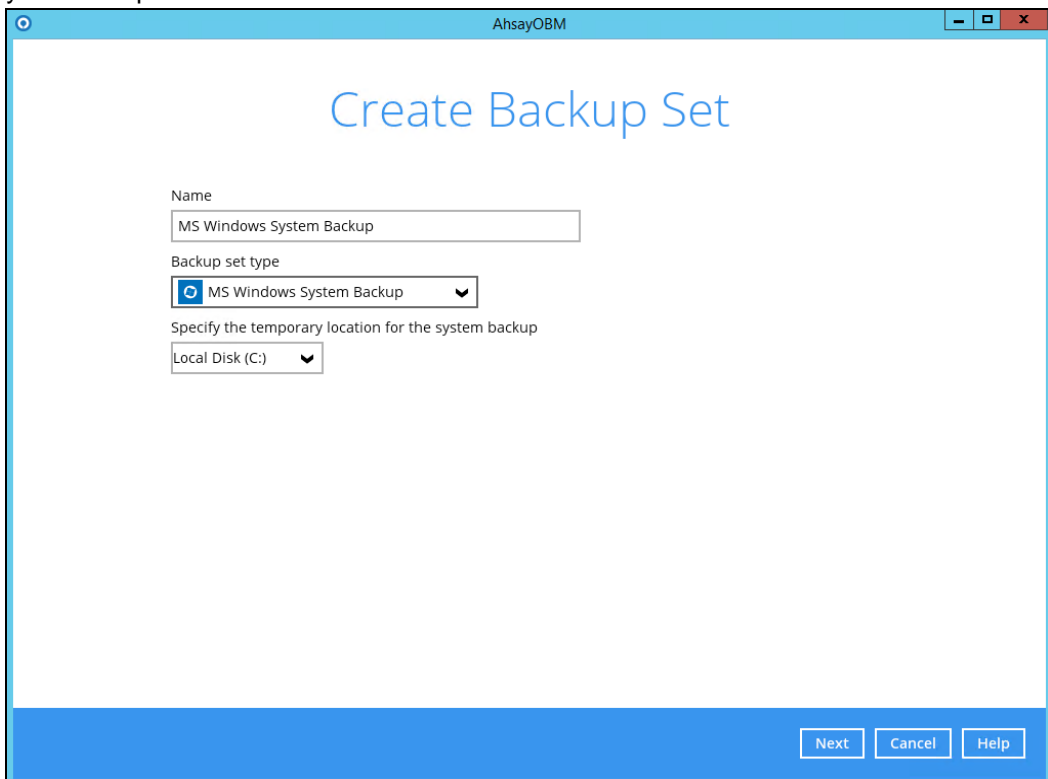
6 Configuring a MS Windows System Backup Set

Create a MS Windows System Backup Set

1. In the AhsayOBM main interface, click **Backup Sets**.



2. Create a MS Windows System backup set by clicking  next to **Add new backup set**.
3. Select **MS Windows System Backup** as the **Backup set type**; then enter a **Name** for your backup set.

A screenshot of the 'Create Backup Set' dialog box in the AhsayOBM application. The window title is 'AhsayOBM'. The main heading is 'Create Backup Set'. There are three input fields: 'Name' with the value 'MS Windows System Backup', 'Backup set type' with a dropdown menu showing 'MS Windows System Backup' selected, and 'Specify the temporary location for the system backup' with a dropdown menu showing 'Local Disk (C:)' selected. At the bottom right, there are three buttons: 'Next', 'Cancel', and 'Help'.

4. Select the location where you would like to store the system image before generating the backup data.

Select a local volume from the dropdown menu.

AhsayOBM

Create Backup Set

Name
MS Windows System Backup

Backup set type
 MS Windows System Backup

Specify the temporary location for the system backup
Local Disk (C:) ▼
Local Disk (C:)
Temp1 (E:)
Temp2 (F:)

Next Cancel Help

Or

Enter the UNC path to a network volume that is accessible to the client computer.

AhsayOBM

Create Backup Set

Name
MS Windows System Backup

Backup set type
 MS Windows System Backup

Specify the temporary location for the system backup
\\UNC_path\share ▼

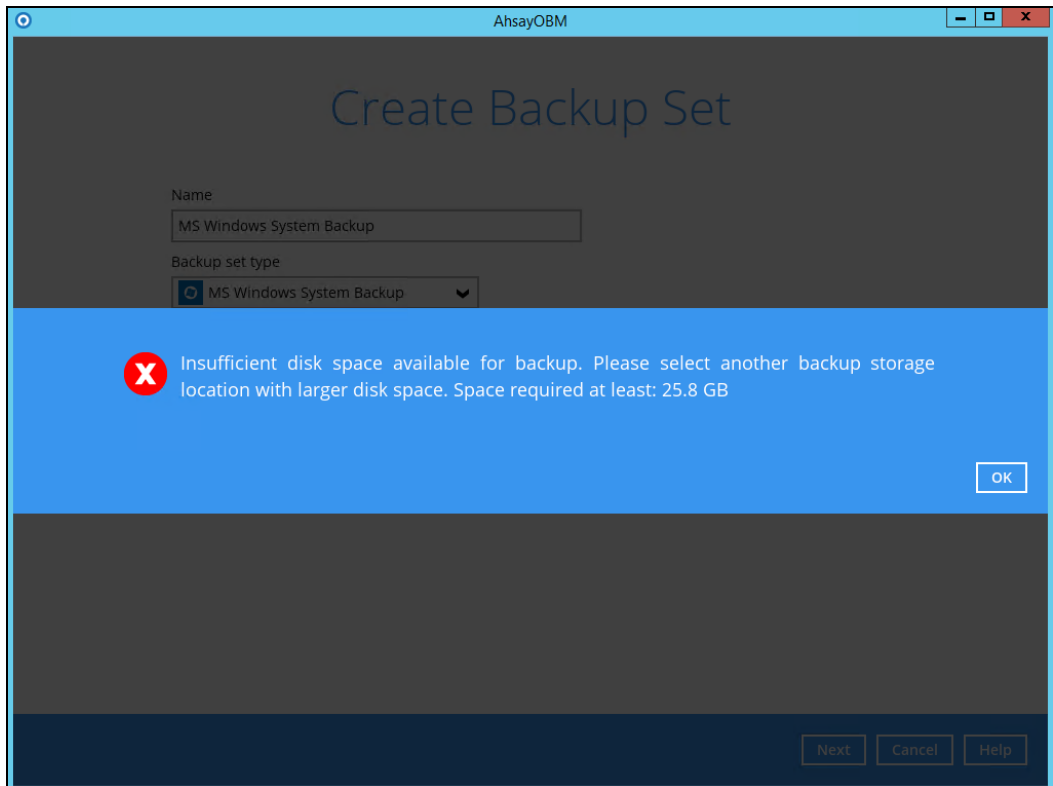
Next Cancel Help

Note: Make sure that the storage location configured for the system image is set to a supported location.

Refer to the link to know the restrictions on the temporary storage location for Windows System State and System Backup Image File

[FAQ: Restrictions on the temporary storage location for the Windows System State and System backup image file](#)

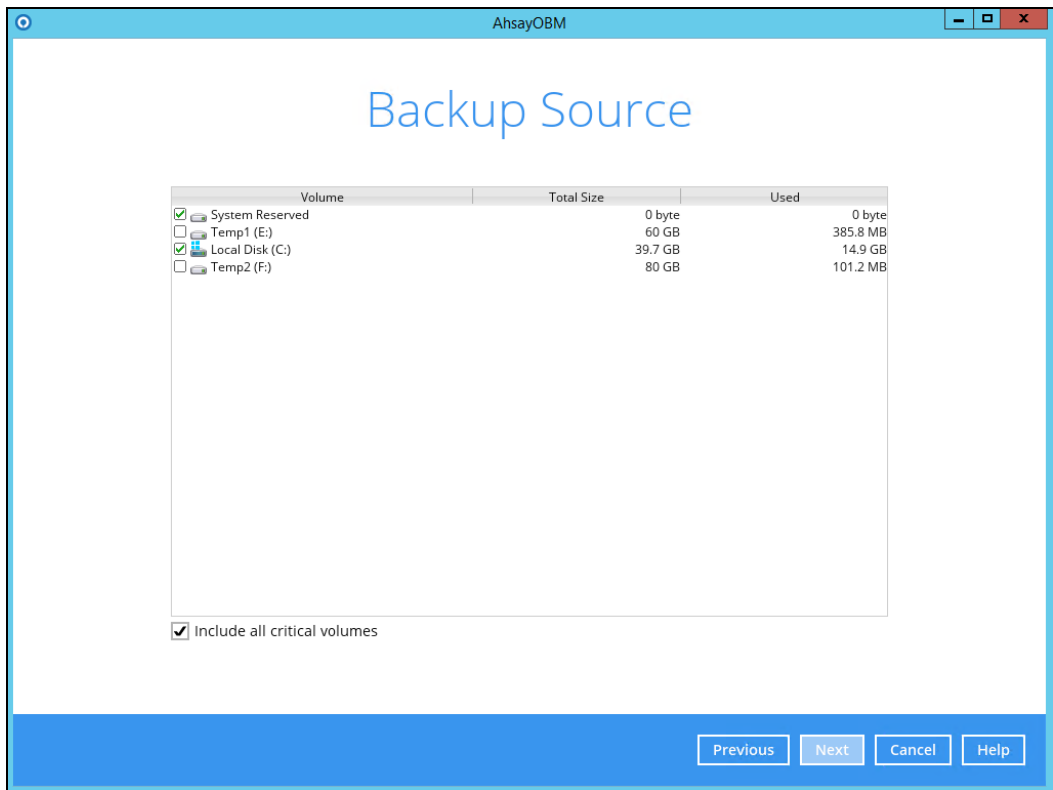
Click **Next** to proceed.



Note: If the disk you selected has insufficient space then this alert message will be displayed.

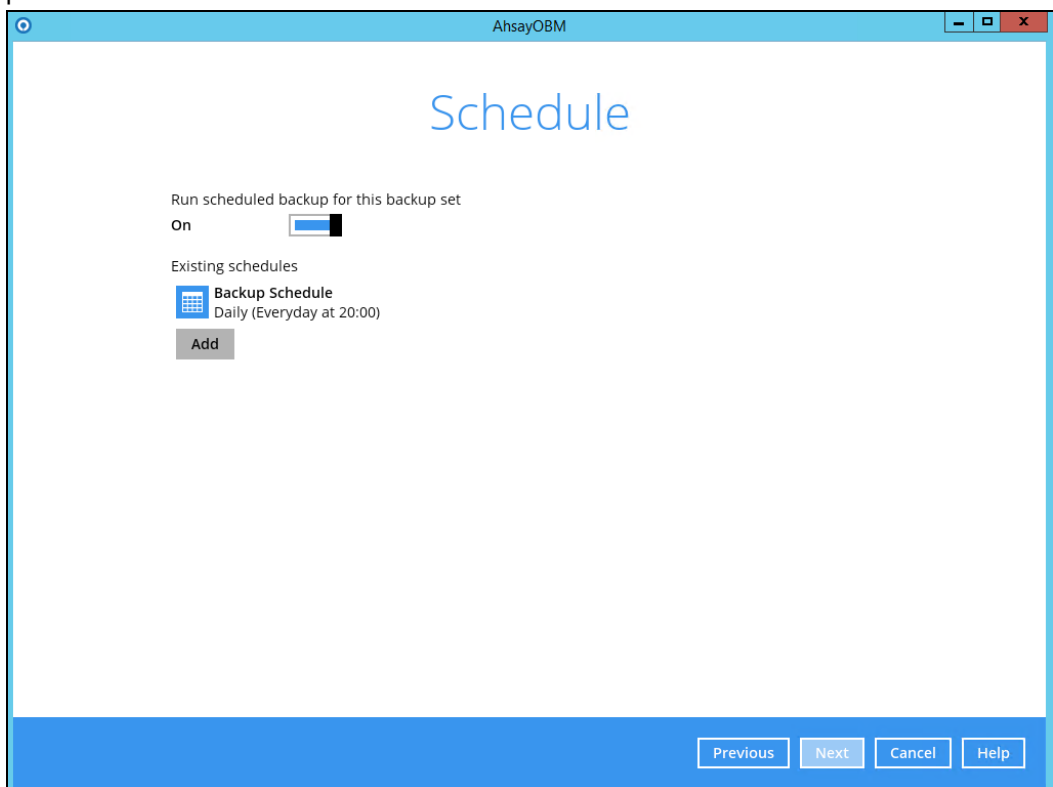
5. In the Backup Source menu, select the volume(s) which you would like to backup.

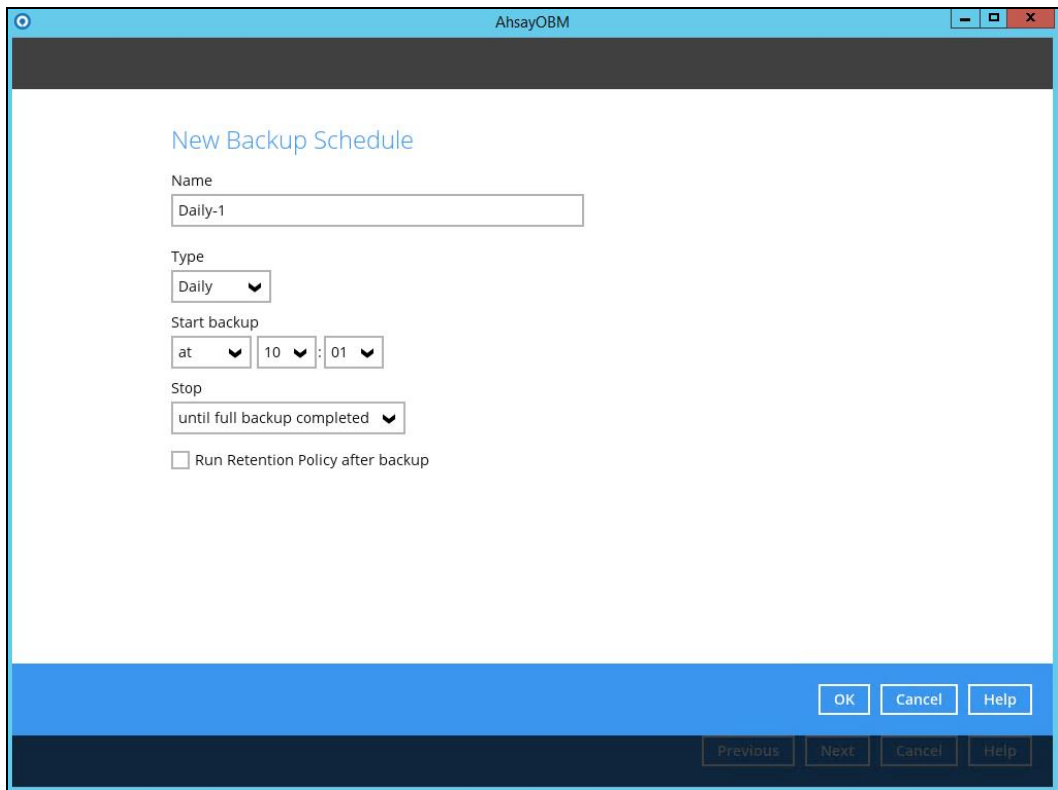
Enable the **Include all critical volumes** option to select all critical volumes for backup automatically. This will ensure that the backup image can be used for full-system / bare-metal recovery.



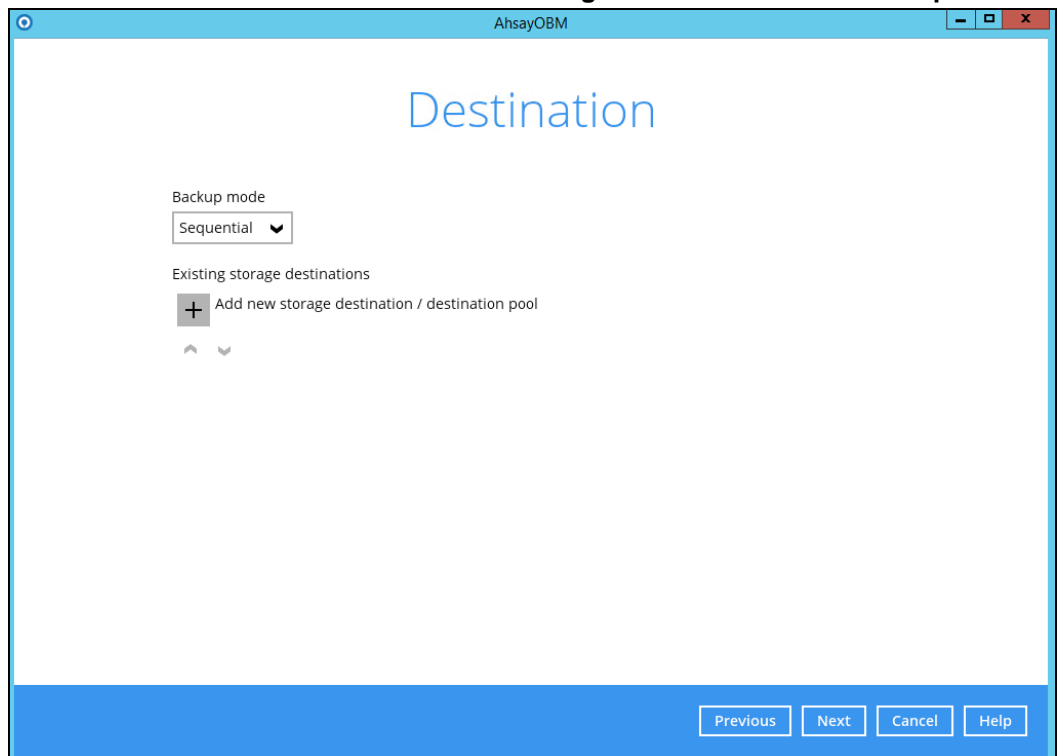
Click **Next** to proceed.

6. In the Schedule menu, configure a backup schedule for backup job to run automatically at your specified time interval. Click **Add** to add a new schedule, then click **Next** to proceed afterward.





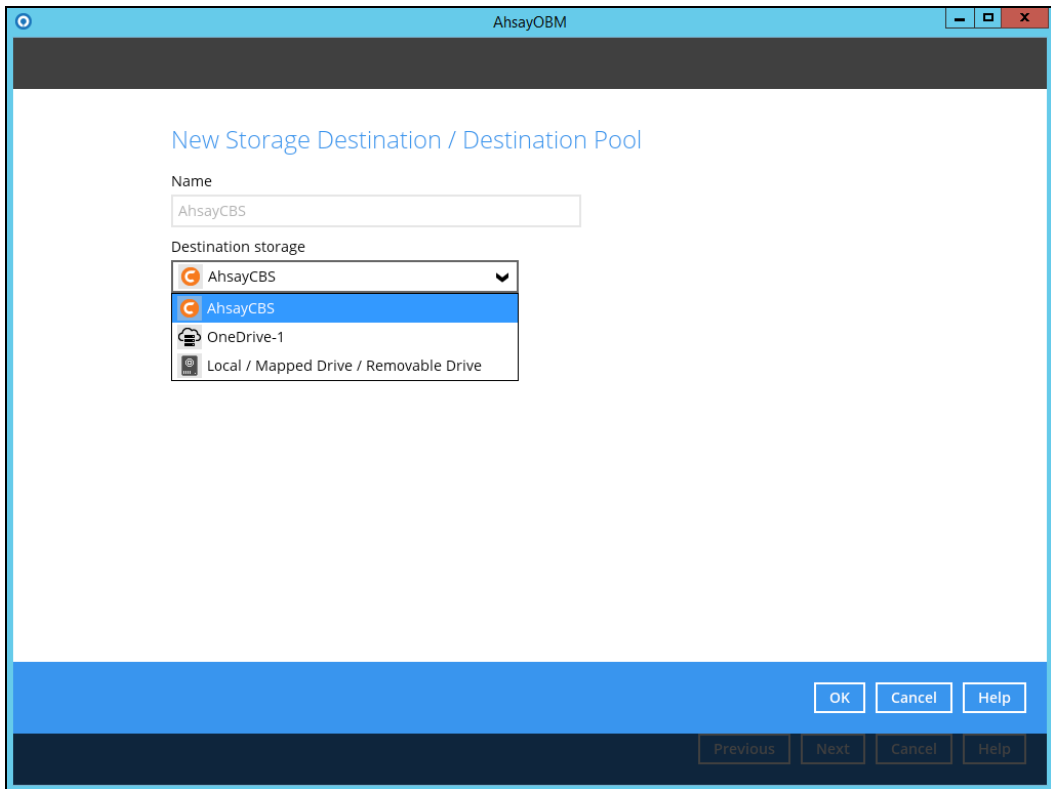
7. In the Destination menu, select a backup destination where the backup data will be stored. Click the “+” icon next to **Add new storage destination / destination pool**.



Note: For more details on Backup Destination, refer to this link [FAQ: Frequently Asked Questions on Backup Destination](#)

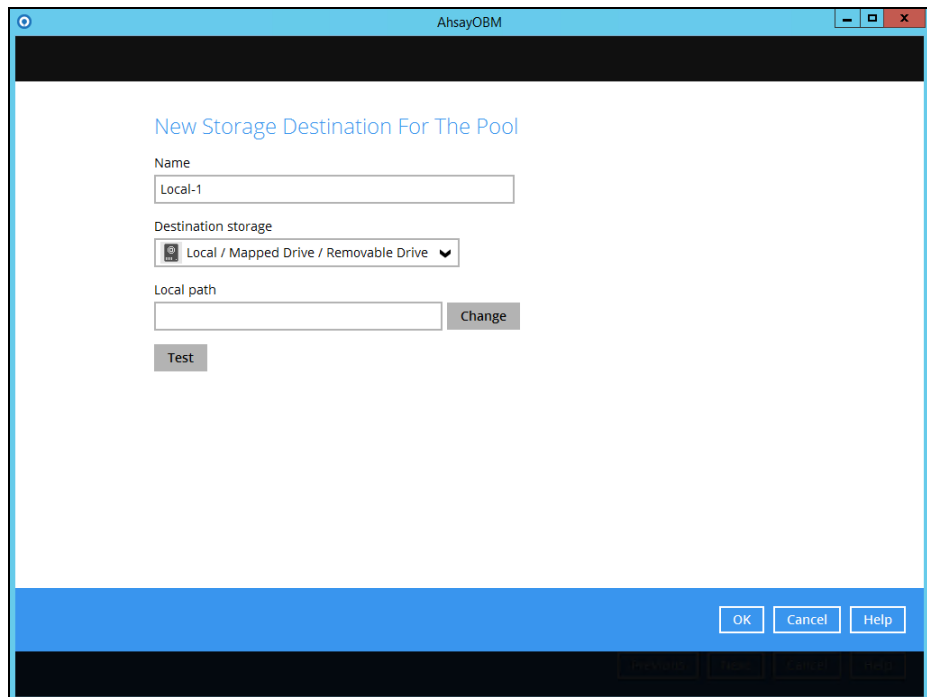
For more details on configuration of cloud storage as backup destination, refer to the [Appendix A](#) section in this guide.

8. Select the Destination storage.

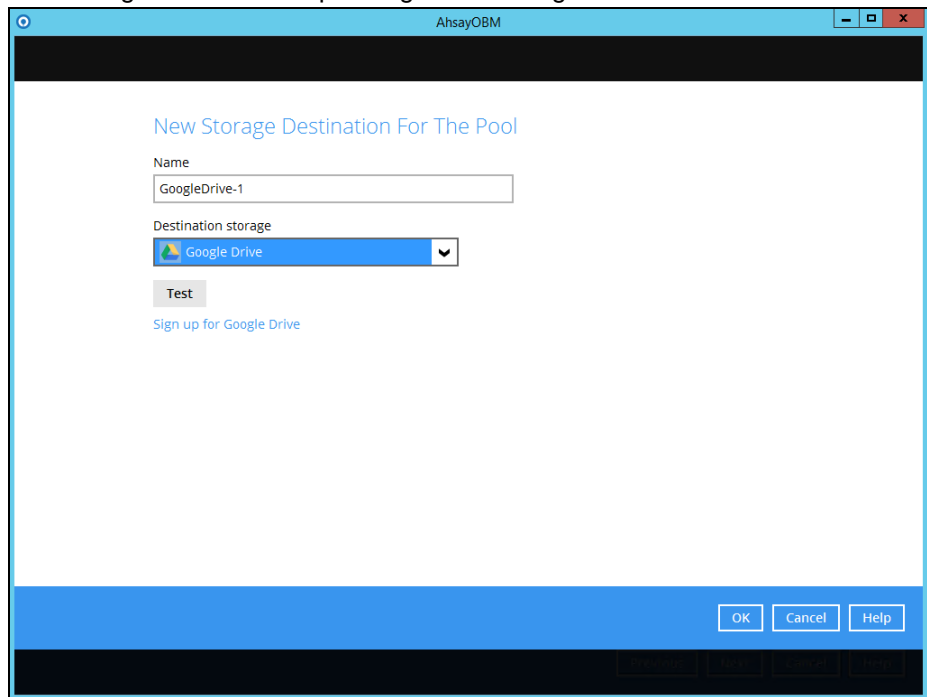


You can choose a storage combination of the Local/Mapped drive/Removable Drive, Cloud storage or FTP. Click **OK** to proceed when you are done with the settings.

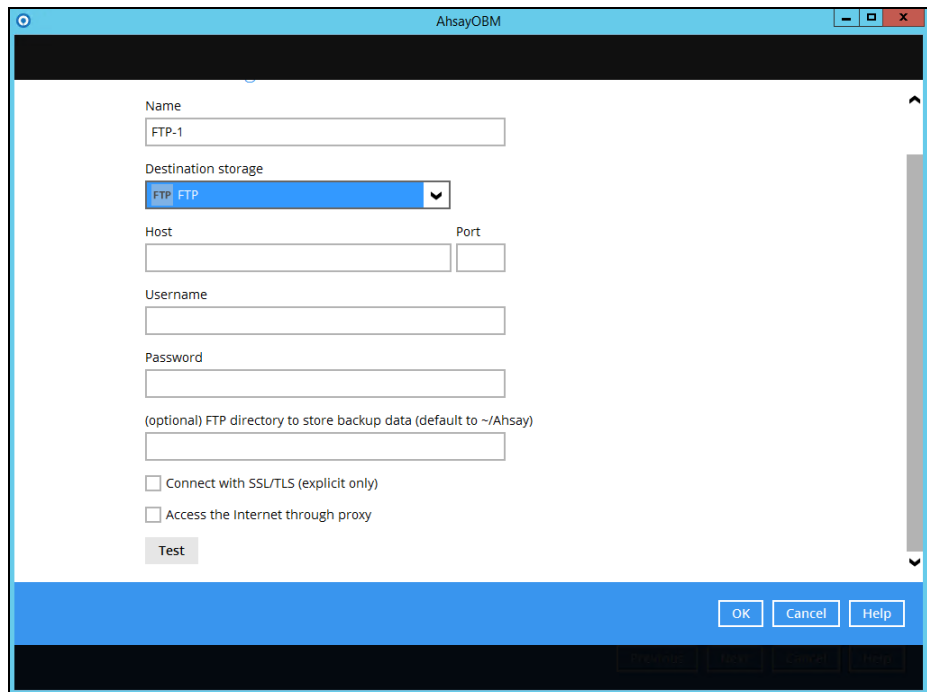
- If you have chosen the Local/Mapped Drive/Removable Drive option, click **Change** to browse to a directory path where backup data will be stored, then click **Test** to validate the path. **Test completed successfully** shows when the validation is done.





- If you have chosen to store the backup files in another Cloud Storage, click **Test** to log in to the corresponding cloud storage service.

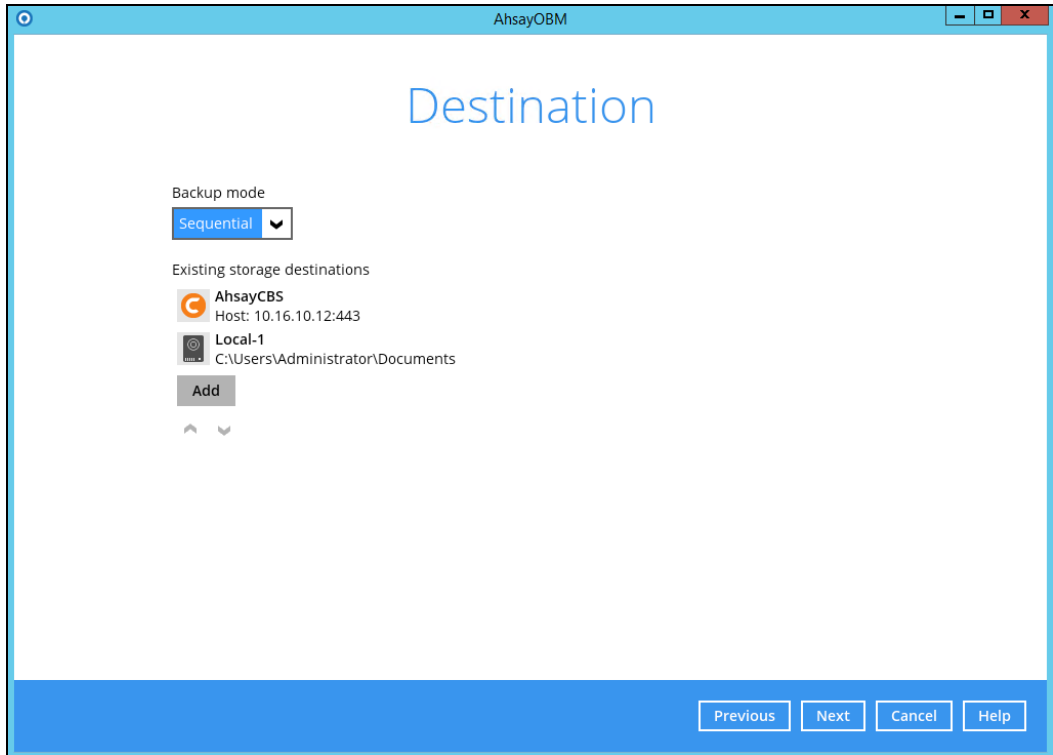


- If you have chosen the FTP as the destination, enter the the Host, Username and Password details.

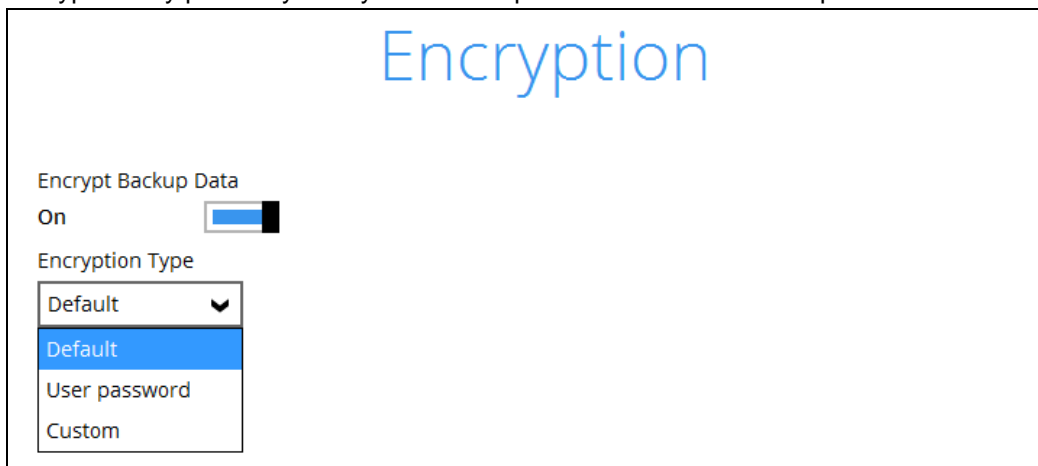


9. You can add multiple storage destinations. The backup data will be uploaded to all the destinations you have selected in the order you added them. Press the   icon to

alter the order. Click **Next** to proceed when you are done with the selection.



10. In the Encryption window, the default **Encrypt Backup Data** option is enabled with an encryption key preset by the system which provides the most secure protection.



You can choose from one of the following three Encryption Type options:

- **Default** – an encryption key with 44 alpha numeric characters will be randomly generated by the system
- **User password** – the encryption key will be the same as the login password of your AhsayOBM at the time when this backup set is created. Please be reminded that if you change the AhsayOBM login password later, the encryption keys of the backup sets previously created with this encryption type will remain unchanged.

- **Custom** – you can customize your encryption key, where you can set your own algorithm, encryption key, method and key length.

Encryption

Encrypt Backup Data
On

Encryption Type
Custom ▾

Algorithm
AES ▾

Encryption key

Re-enter encryption key

Method
 ECB CBC

Key length
 128-bit 256-bit

Note: For best practice on managing your encryption key, refer to the following wiki article.

[FAQ: Best practices for managing encryption key for AhsayOBM or AhsayACB](#)

Click **Next** when you are done setting.

11. If you have enabled the Encryption Key feature in the previous step, the following pop-up window shows, no matter which encryption type you have selected.

Encryption

Encrypt Backup Data
On

Encryption Type
Default ▾

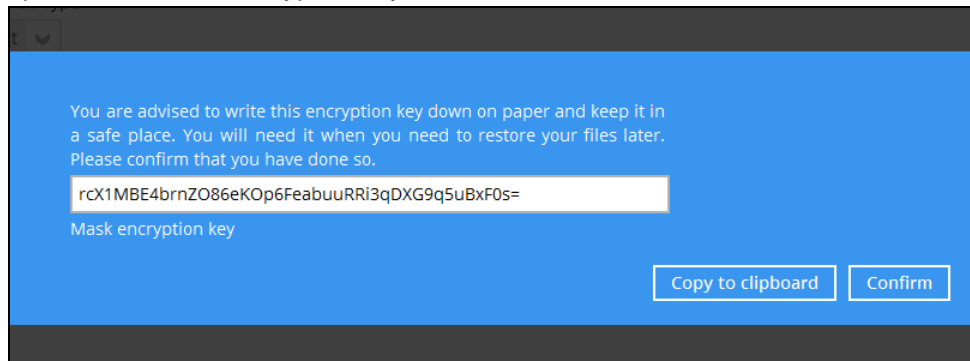
You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.

Unmask encryption key

Copy to clipboard Confirm

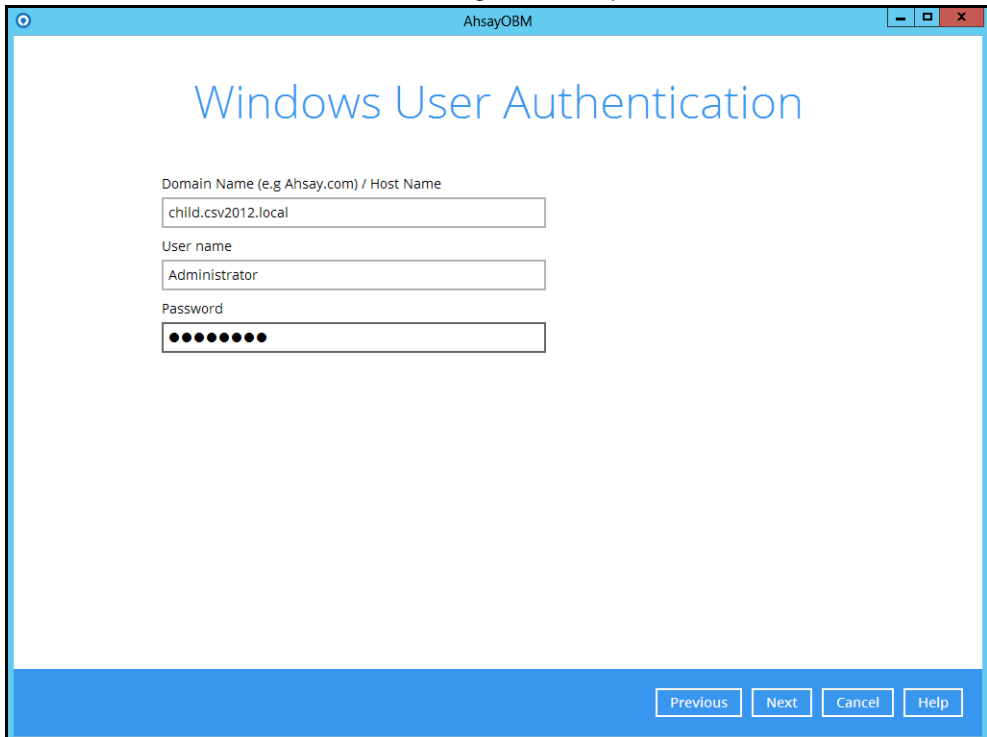
The pop-up window has the following three options to choose from:

- **Unmask encryption key** – The encryption key is masked by default. Click this option to show the encryption key.



- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.
- **Confirm** – Click to exit this pop-up window and proceed to the next step.

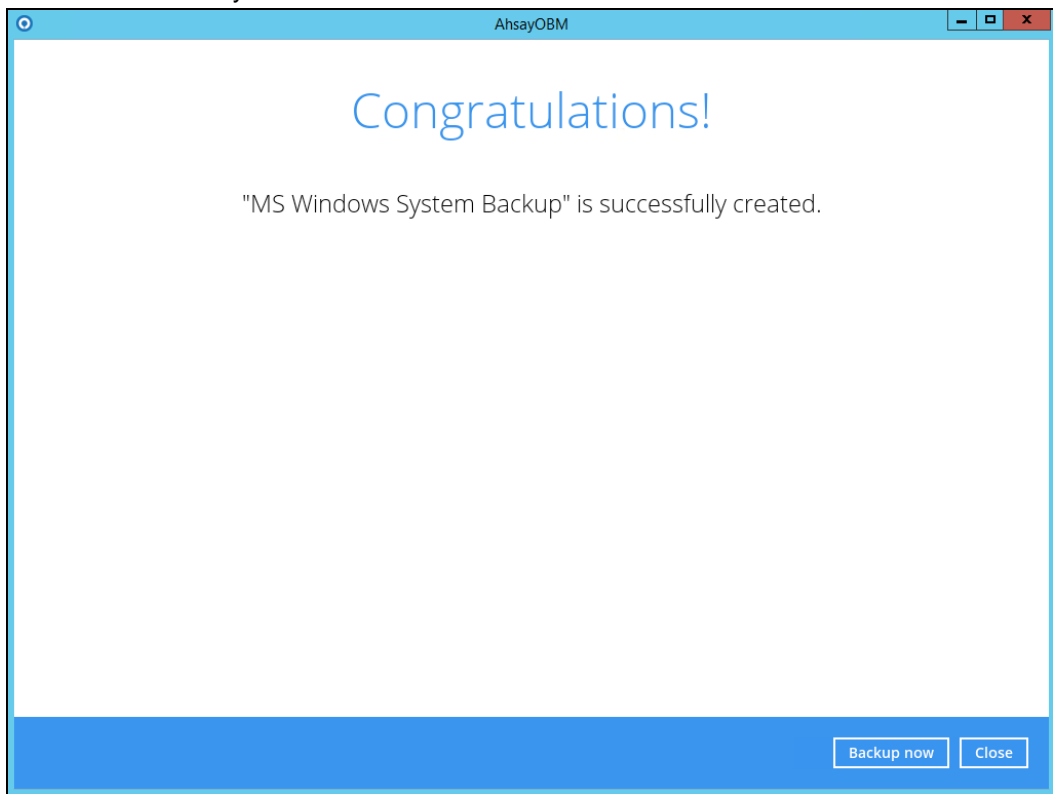
12. Enter the **Domain Name / Host Name** of the computer, **User Name** and **Password** of the Windows account that will be running the backup.

A screenshot of a Windows User Authentication dialog box titled "AhsayOBM". The dialog box has a blue header and a white body. The title "Windows User Authentication" is displayed in blue. Below the title, there are three input fields: "Domain Name (e.g Ahsay.com) / Host Name" with the value "child.csv2012.local", "User name" with the value "Administrator", and "Password" with a masked password represented by seven black dots. At the bottom of the dialog box, there are four buttons: "Previous", "Next", "Cancel", and "Help".

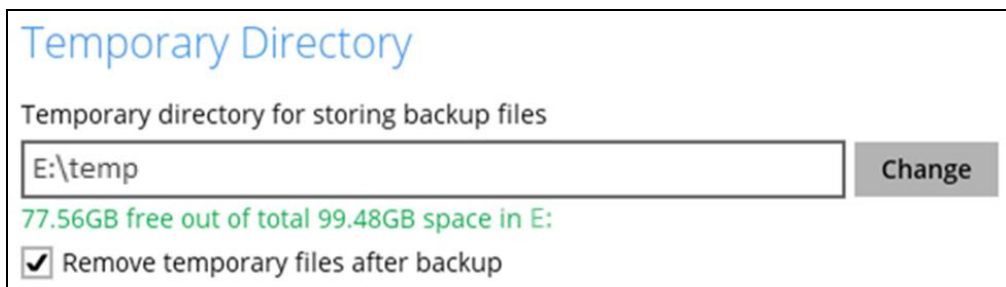
Note: This menu will only be displayed if a backup schedule is configured in the previous step.

13. Click **Next** to create the backup set.

14. The following screen is displayed when the new MS Windows System backup set is created successfully.



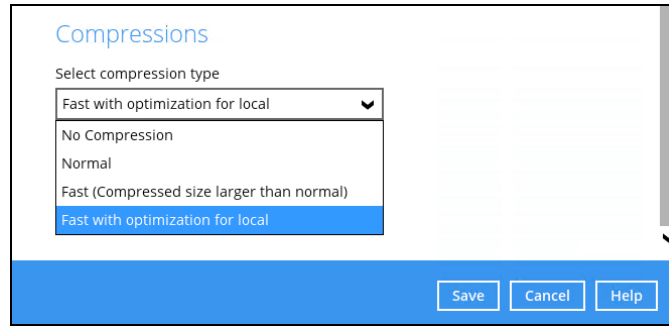
15. Based on [Best Practices and Recommendations](#), it is highly recommended to set the temporary directory to another location other than Drive C: (e.g. Drive E:). To do this, go to **Backup Sets > Others > Temporary Directory** and click the **Change** button to browse for another location.



16. Optional: Select your preferred **Compression** type. By default, the compression type is Fast with optimization for local.

Go to **Others > Compressions**, then select from the following:

- No Compression
- Normal
- Fast (Compressed size larger than normal)
- Fast with optimization for local



7 Overview on the Backup Process

The following steps are performed during a backup job. For an overview of the detailed process for Steps 3, 5, 11, and 13, refer to the following chapters:

- [Periodic Data Integrity Check \(PDIC\) Process \(Step 3\)](#)
- [Backup Set Index Handling Process](#)
 - [Start Backup Job \(Step 5\)](#)
 - [Completed Backup Job \(Step 13\)](#)
- [Data Validation Check \(Step 11\)](#)



7.1 Periodic Data Integrity Check (PDIC) Process

For AhsayOBM v8.3.6.0 (or above), the PDIC will run on the first backup job that falls on the corresponding day of the week from **Monday to Friday**.

To minimize the impact of the potential load of large number of PDIC jobs running at the same time on the AhsayCBS server, the schedule of a PDIC job for each backup set is automatically determined by the result of the following formula:

PDIC schedule = %BackupSetID% modulo 5

or

%BackupSetID% mod 5

The calculated **result** will map to the corresponding day of the week (i.e., from Monday to Friday).

0	Monday
1	Tuesday
2	Wednesday
3	Thursday
4	Friday

NOTE: The PDIC schedule cannot be changed.

Example:

Backup set ID: 1594627447932

Calculation: $1594627447932 \text{ mod } 5 = 2$

2	Wednesday
----------	------------------

In this example:

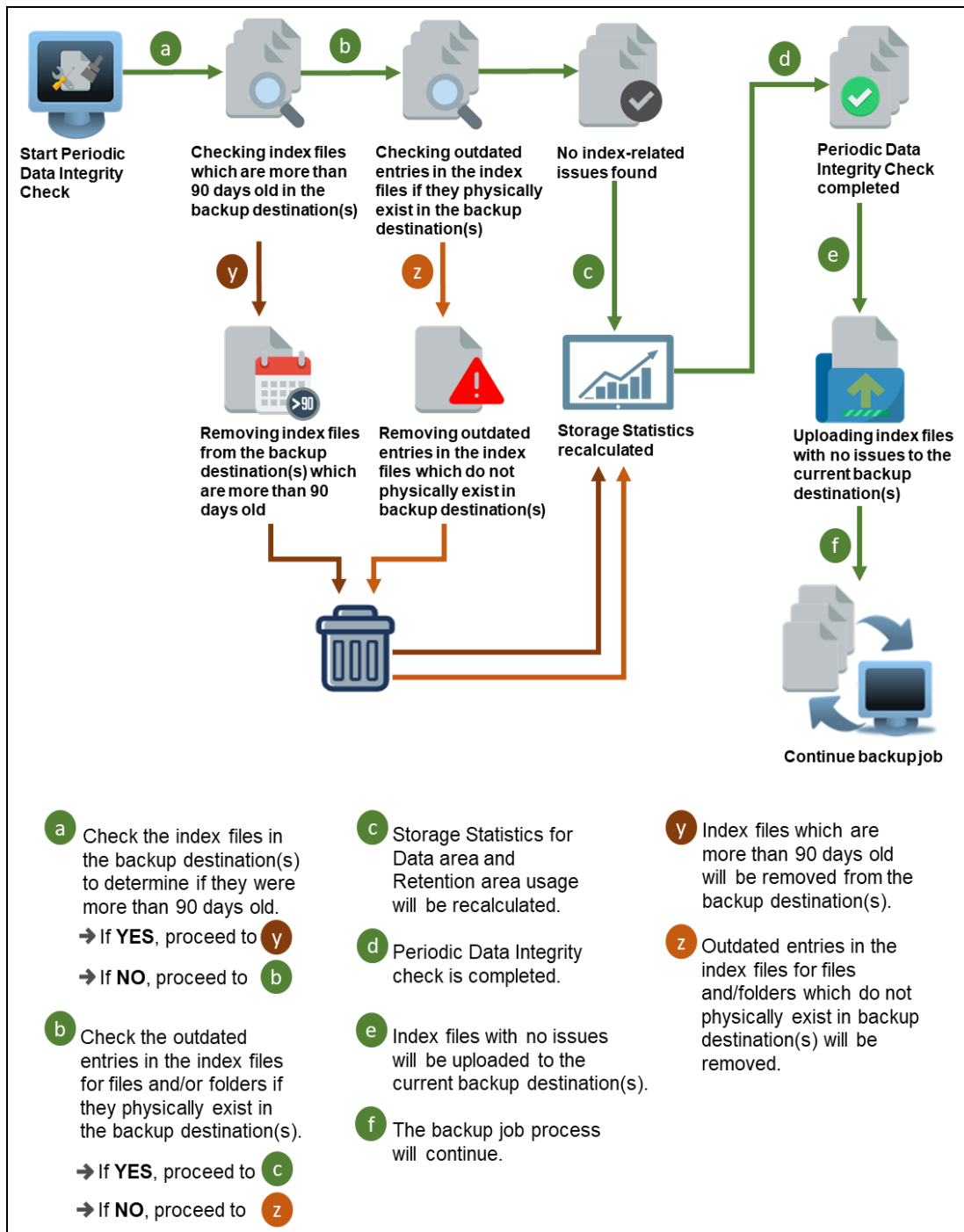
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

NOTE

Although according to the PDIC formula for determining the schedule is ***%BackupSetID% mod 5***, this schedule only applies if the previous PDIC job was actually run more than 7 days prior.

Under certain conditions, the PDIC may not run strictly according to this formula. For example:

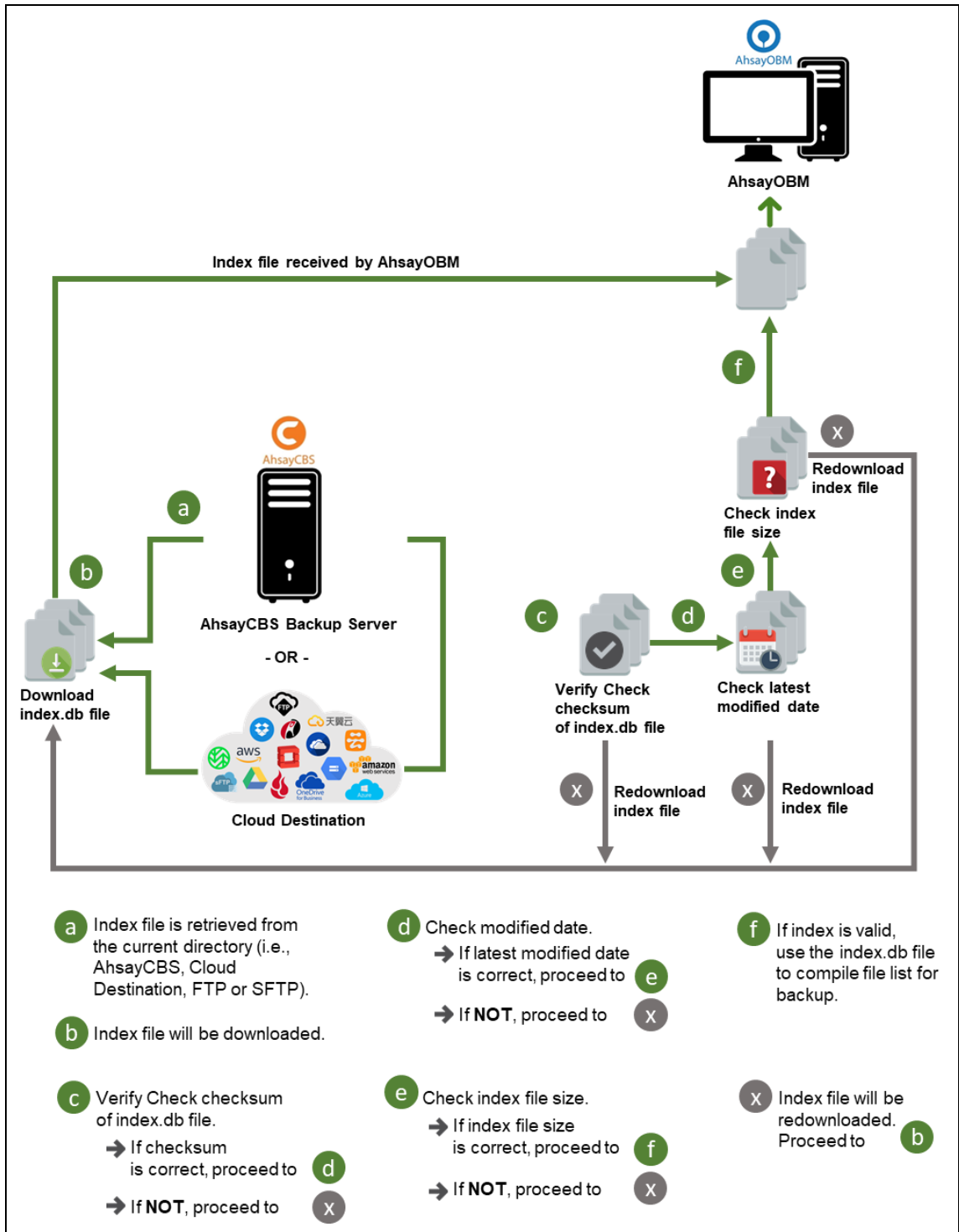
1. If AhsayOBM was upgraded to v8.5 (or above) from an older version v6, v7, or pre-8.3.6.0 version. In this case, the PDIC job will run on the first backup job after upgrade.
2. If backup jobs for a backup set are not run on a regular daily backup schedule (for example: on a weekly or monthly schedule), then the PDIC job will run if it detects that the previous PDIC job was run more than 7 days ago.



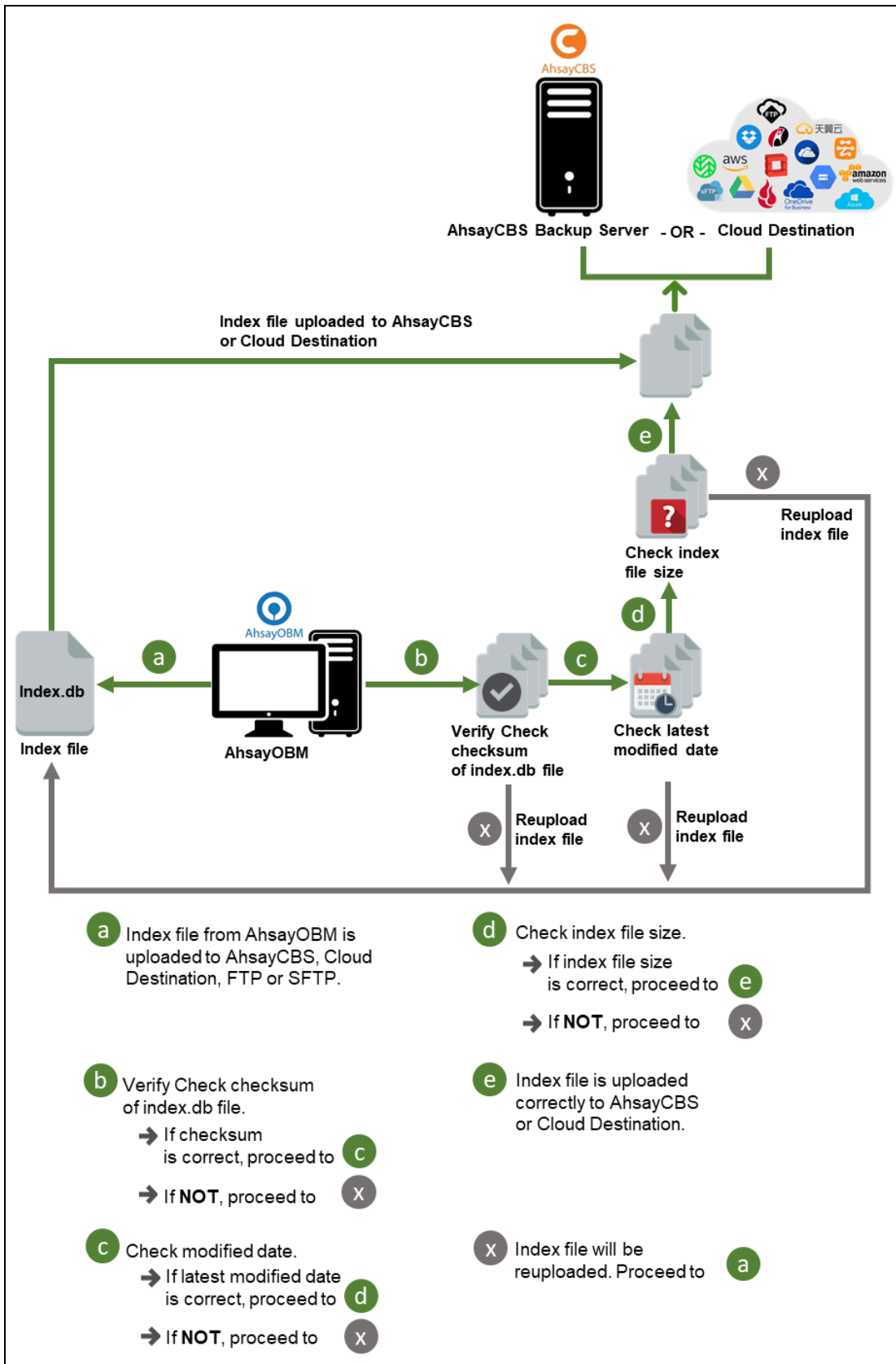
7.2 Backup Set Index Handling Process

To minimize the possibility of index related issues affecting backups, each time index files are downloaded from and uploaded to backup destination(s); the file size, last modified date, and checksum is verified to ensure index file integrity.

7.2.1 Start Backup Job

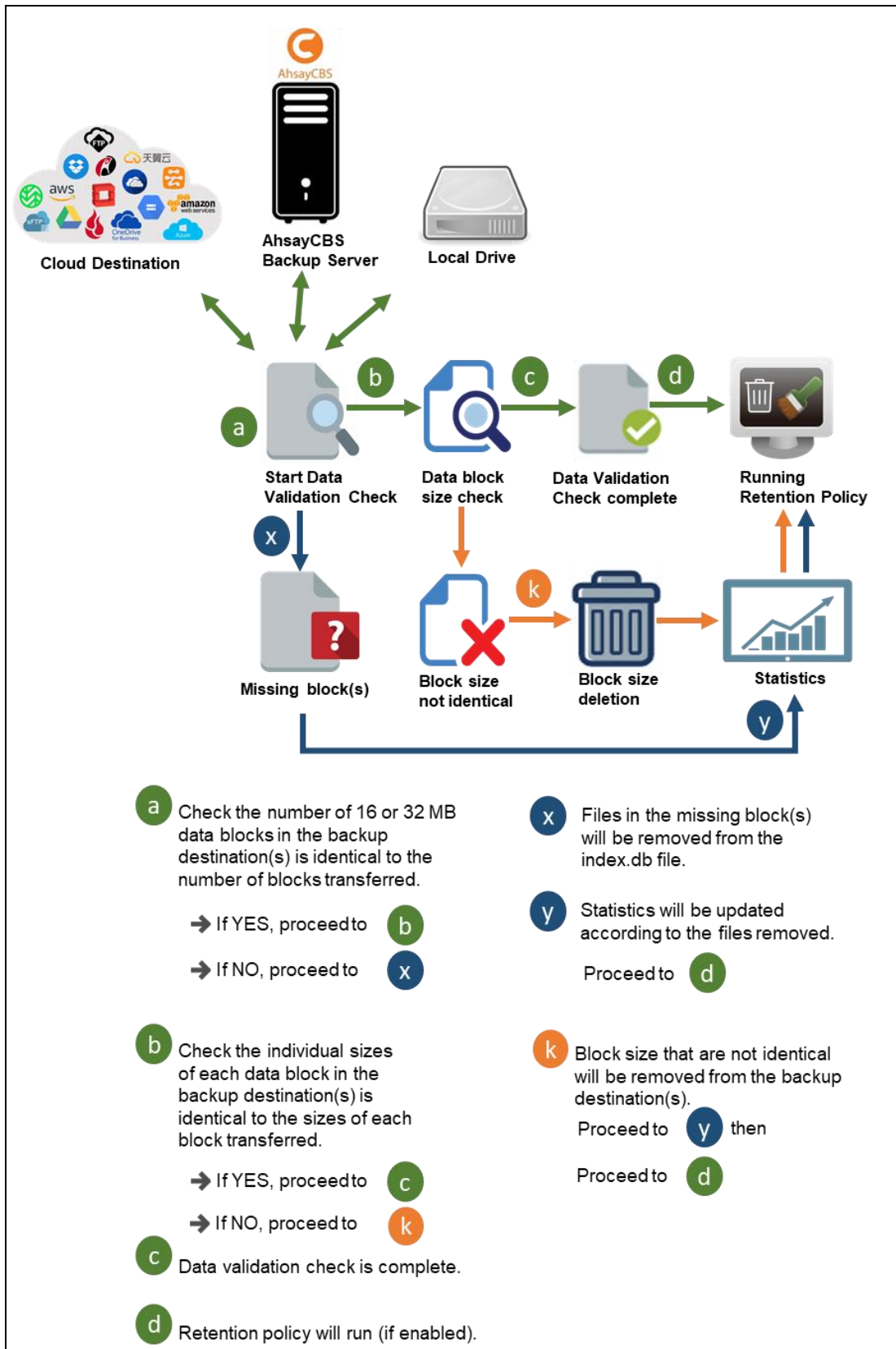


7.2.2 Completed Backup Job



7.3 Data Validation Check Process

As an additional measure to ensure that all files transferred to the backup destination(s) are received and saved correctly, both the number of 16 or 32 MB data block files and the size of each block file are checked again after the files are transferred.



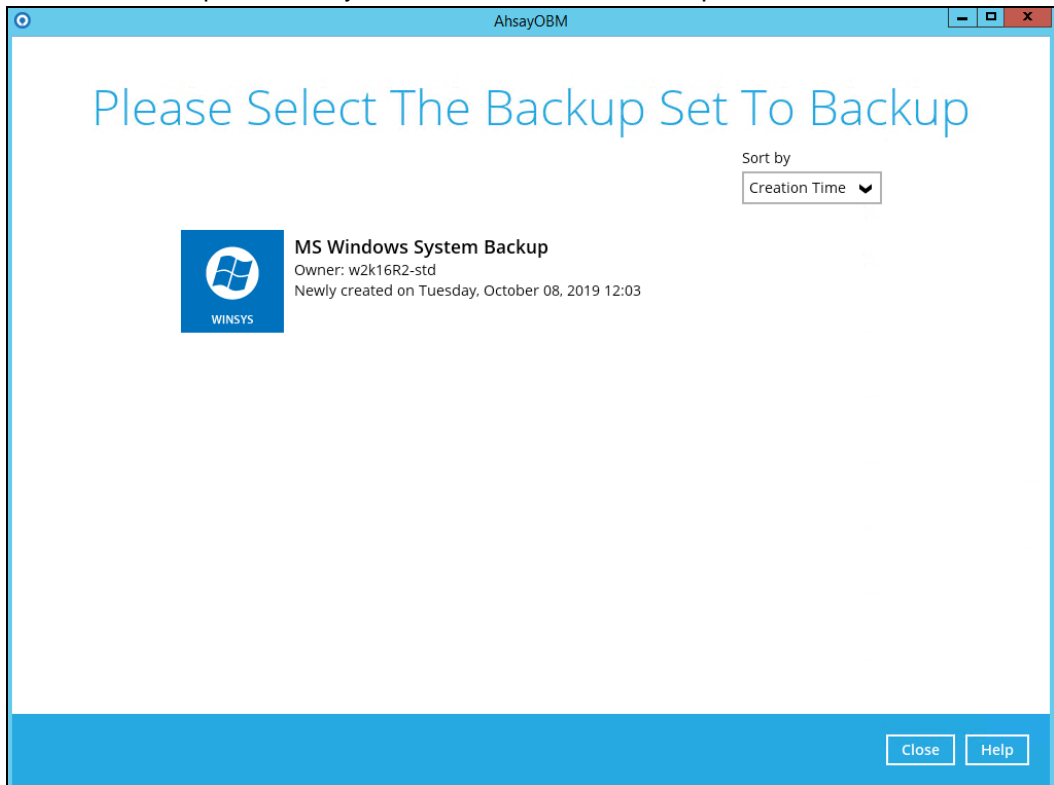
8 Running a Backup

8.1 Start a Manual Backup

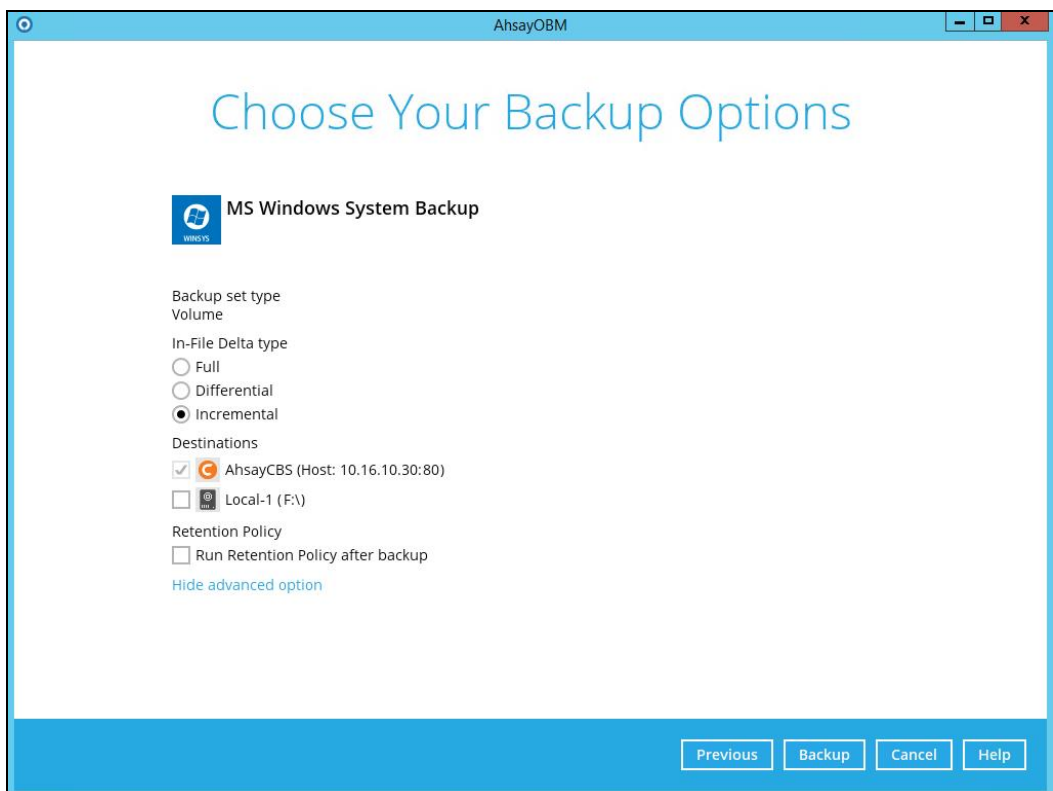
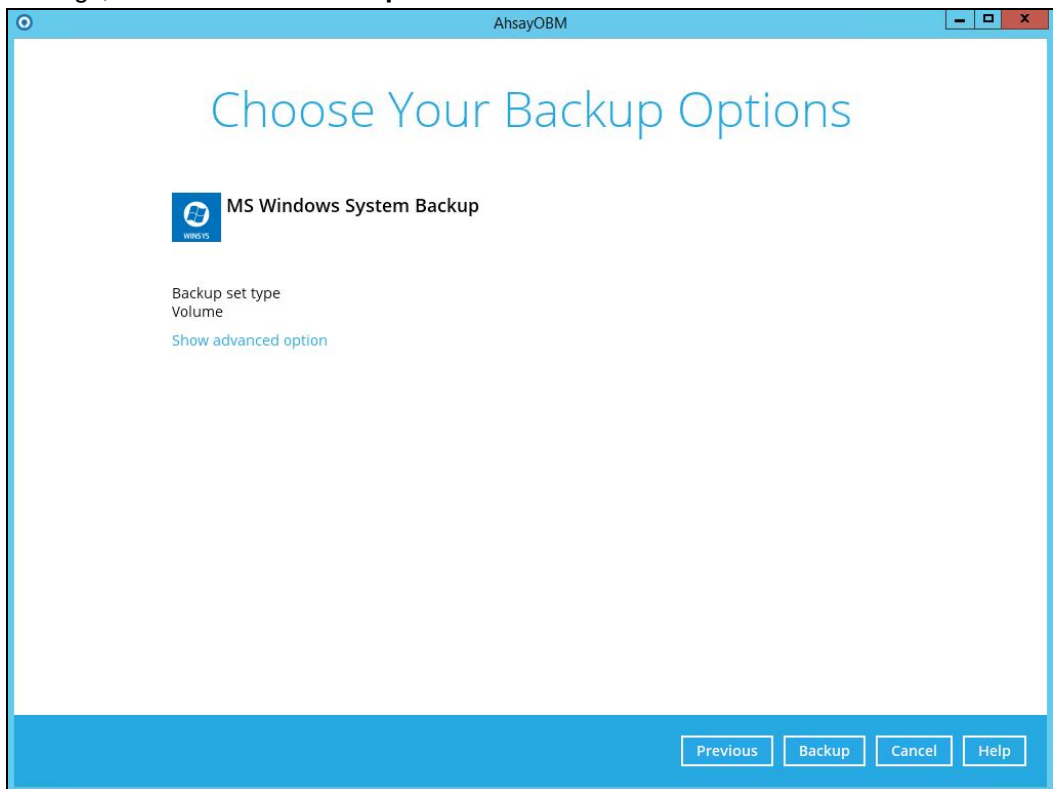
1. Click the **Backup** icon on the main interface of AhsayOBM.



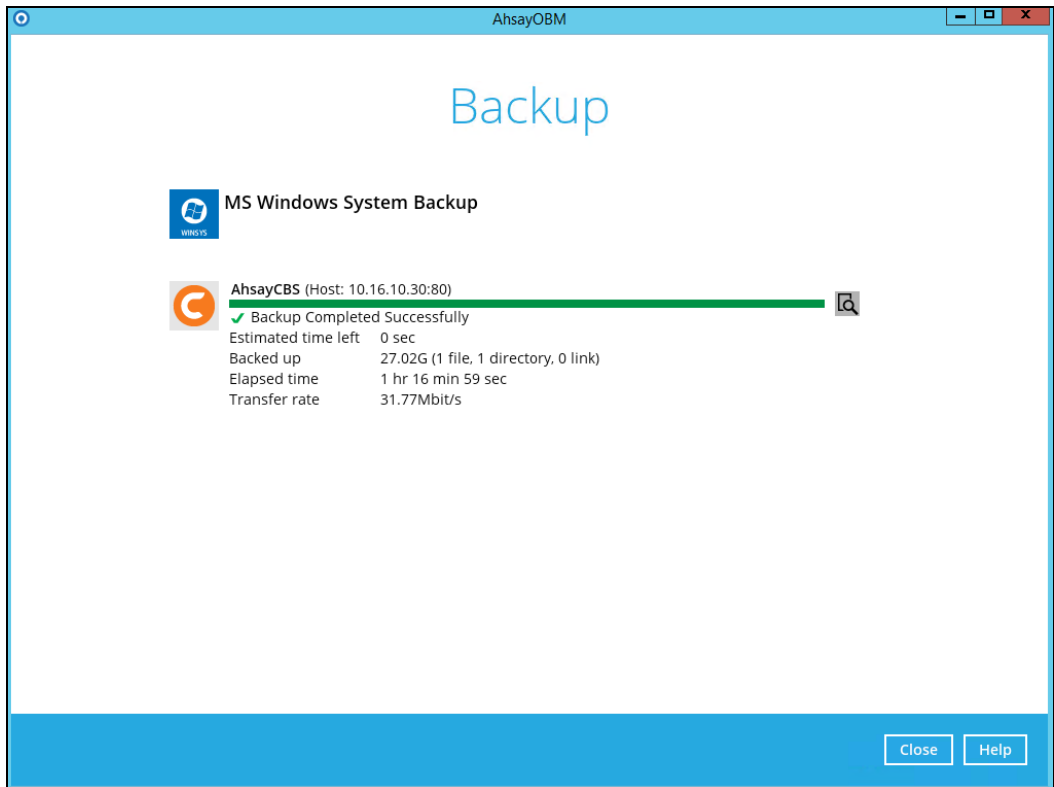
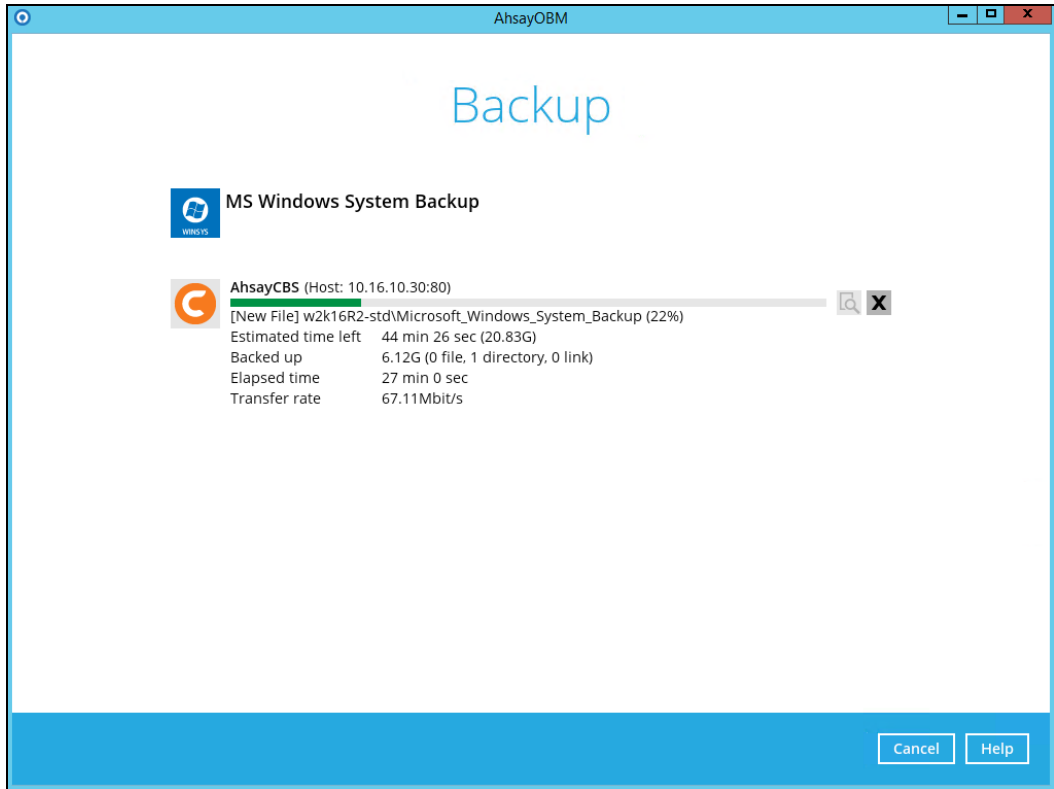
2. Select the backup set which you would like to start a backup for.




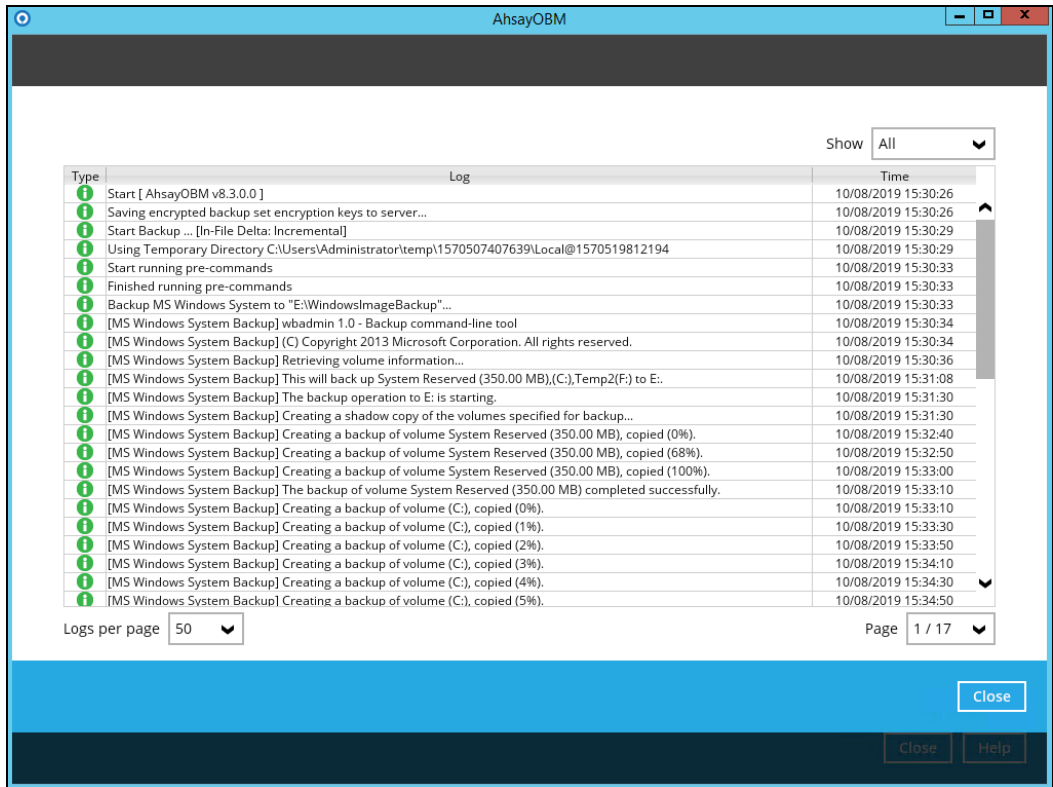
3. If you would like to modify the In-File Delta type, Destinations and Retention Policy Settings, click **Show advance option**.



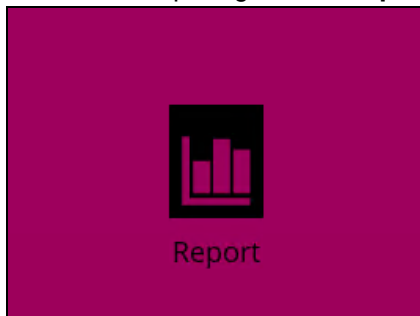
4. Click **Backup** to start the backup and wait until the backup is done.



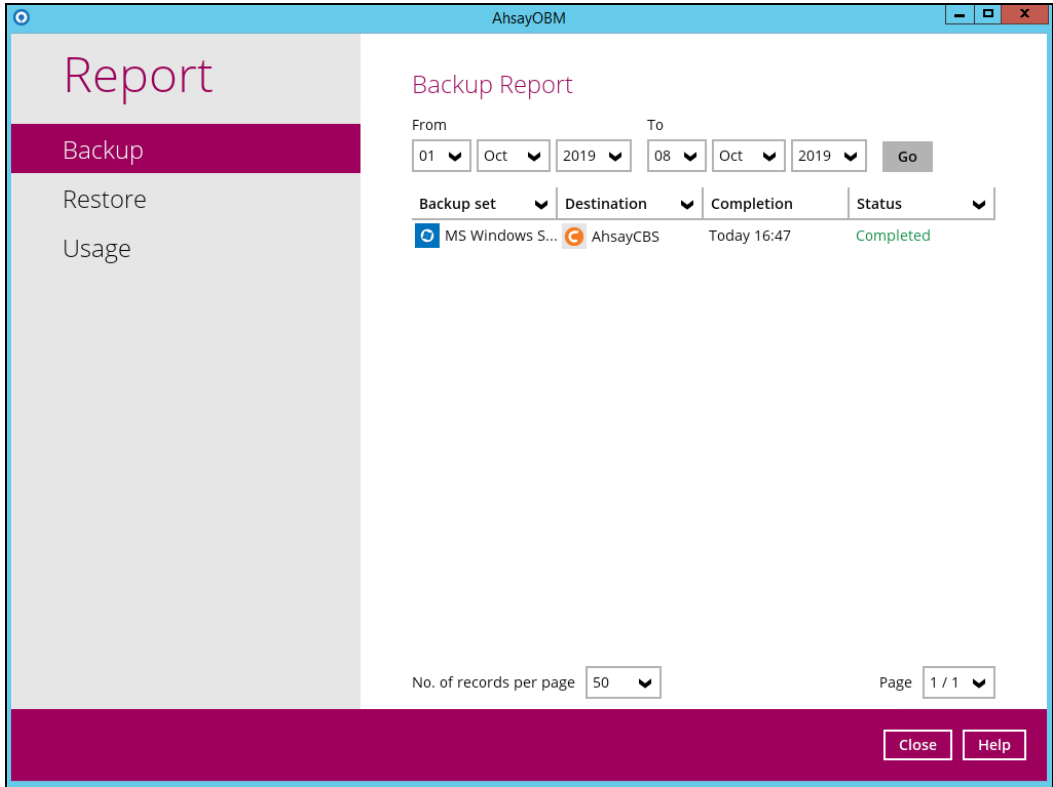
- Check the log of your backup by clicking this icon . It will show you the log of your backup with corresponding date and time.



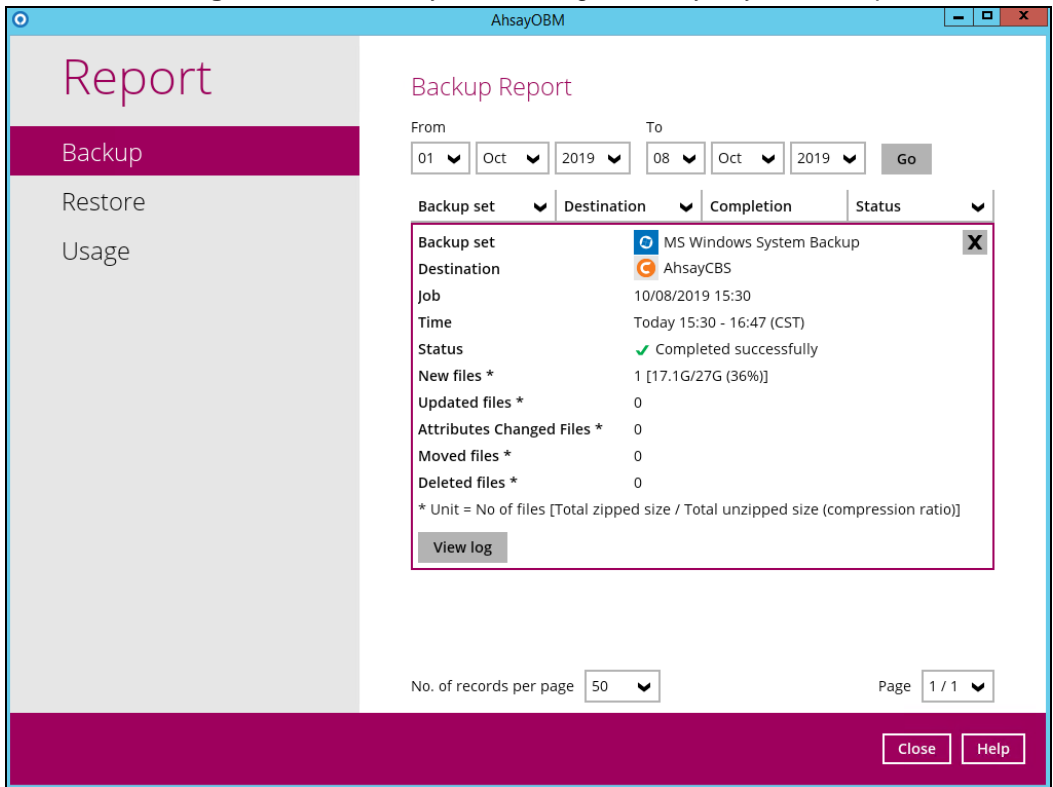
To view the report, go to the **Report > Backup**

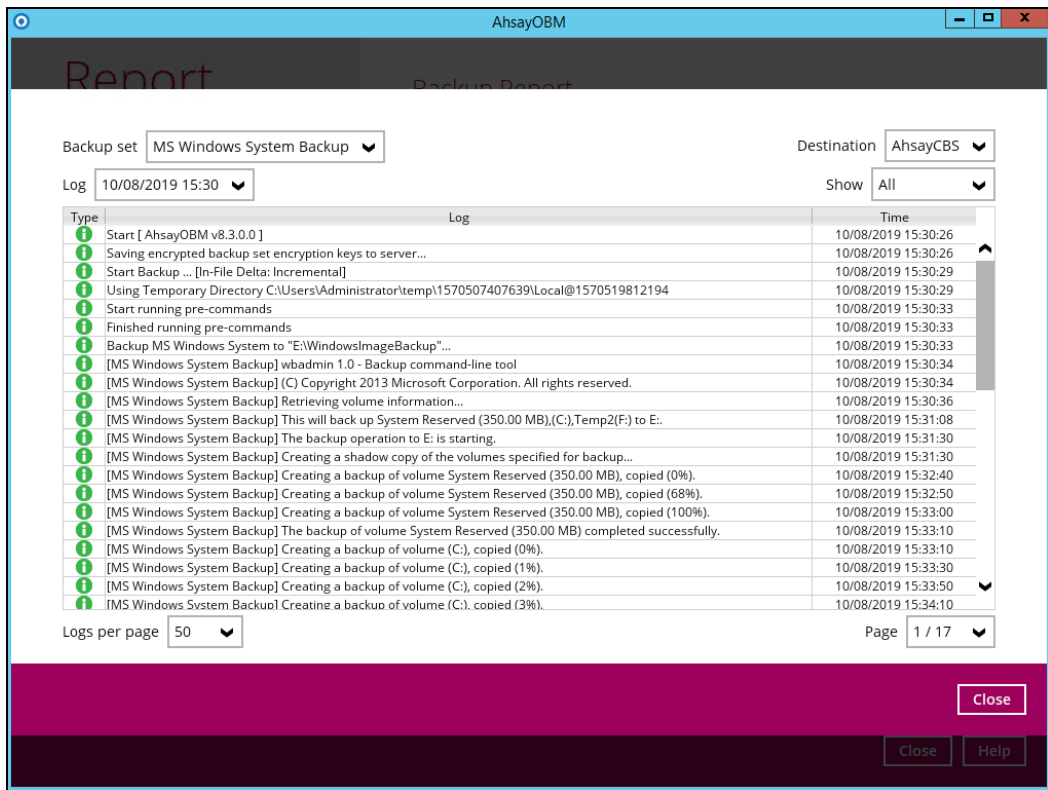


In this Backup Report screen, you can see the backup set with corresponding destination, completion date and time, and status.



Click the backup report and the summary of the backup will be displayed. You can also click the **View Log**, this will redirect you to the log summary of your backup.





You can also search for backup reports from a specific period of date. For example, we have the **From** date which is, **01 Oct 2019** and the **To** date which is, **8 Oct 2019**. Then click the **Go** button to generate the available reports.

From	To
01 ▼ Oct ▼ 2019 ▼	08 ▼ Oct ▼ 2019 ▼
Go	

If this is a valid range of dates then backup reports will be displayed unless there were no backup running on the specified dates. A message of **No records found** will also be displayed.

From	To
01 ▼ Oct ▼ 2019 ▼	05 ▼ Oct ▼ 2019 ▼
Go	

AhsayOBM

Report

- Backup
- Restore
- Usage

Backup Report

From: 01 Oct 2019 To: 05 Oct 2019

Backup set	Destination	Completion	Status
No records found			

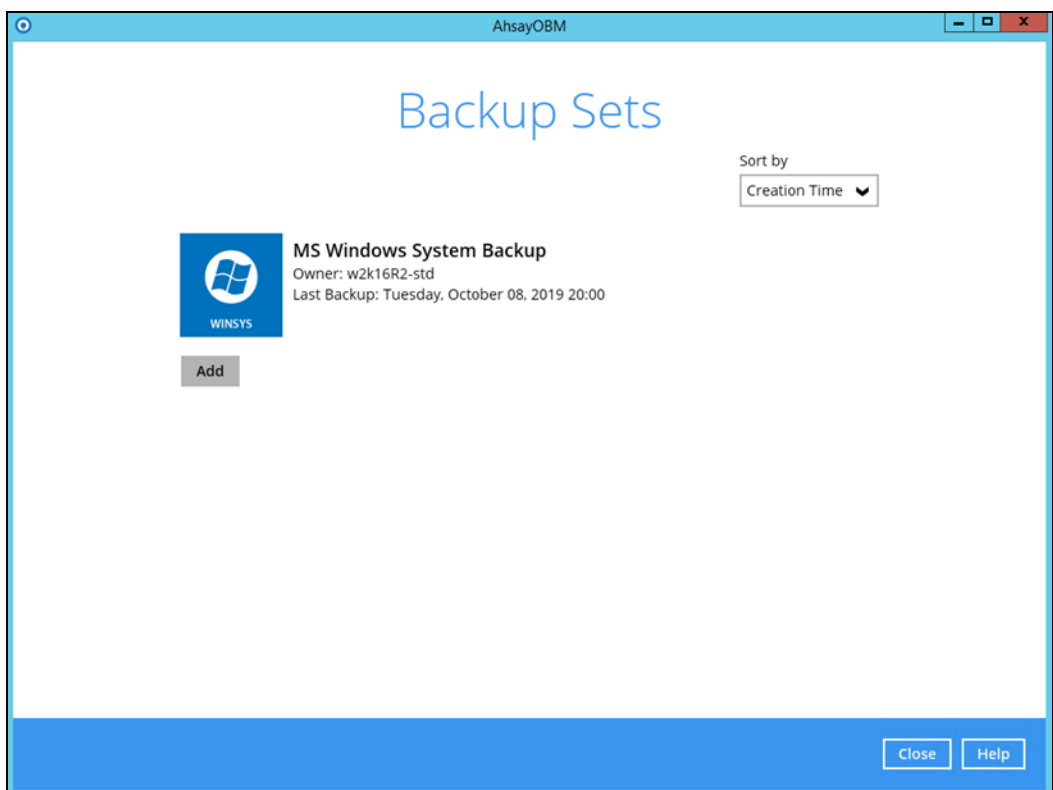
No. of records per page: 50 Page: -

8.2 Configure Backup Schedule for Automated Backup

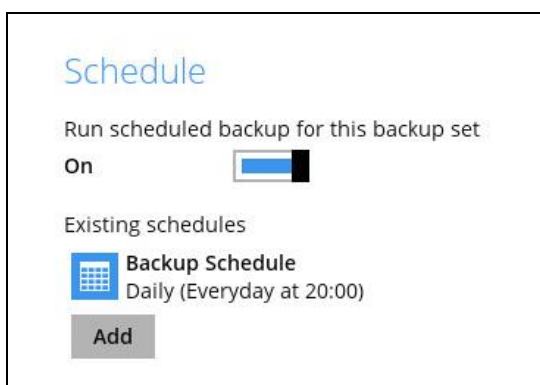
1. Click the **Backup Sets** icon on the main interface of AhsayOBM.



2. All backup sets will be listed. Select the backup set that you would like to create a backup schedule for.



3. Go to the **Backup Schedule** tab. If the **Run scheduled backup for this backup set** option is off, switch it **On**. Existing schedules will be listed if there is any. Click the **Add** button to add a new backup schedule.



4. The New Backup Schedule window will appear.

New Backup Schedule

Name
Daily-1

Type
Daily

Start backup
at 13:00

Stop
until full backup completed

Run Retention Policy after backup

5. In the New Backup Schedule window, configure the following backup schedule settings.

- **Name** – the name of the backup schedule.
- **Type** – the type of backup schedule. There are four (4) different types of backup schedule: Daily, Weekly, Monthly and Custom.
- **Daily** – the time of the day or interval in minutes/hours which the backup job will run.

New Backup Schedule

Name
Daily-1

Type
Daily

Start backup
at 15:41

Stop
until full backup completed

Run Retention Policy after backup

- **Weekly** – the day of the week and the time of the day or interval in minutes/hours which the backup job will run.

New Backup Schedule

Name
Weekly-1

Type
Weekly

Backup on these days of the week
 Sun Mon Tue Wed Thu Fri Sat

Start backup
at 23:00

Stop
until full backup completed

Run Retention Policy after backup

- **Monthly** - the day of the month and the time of that day which the backup job will run.

New Backup Schedule

Name
Monthly-1

Type
Monthly

Backup on the following day every month
 Day Last
 First Sunday

Start backup at
23:00 on the selected days

Stop
until full backup completed

Run Retention Policy after backup

- **Custom** – a specific date and the time of that date which the backup job will run.

New Backup Schedule

Name
Custom-1

Type
Custom

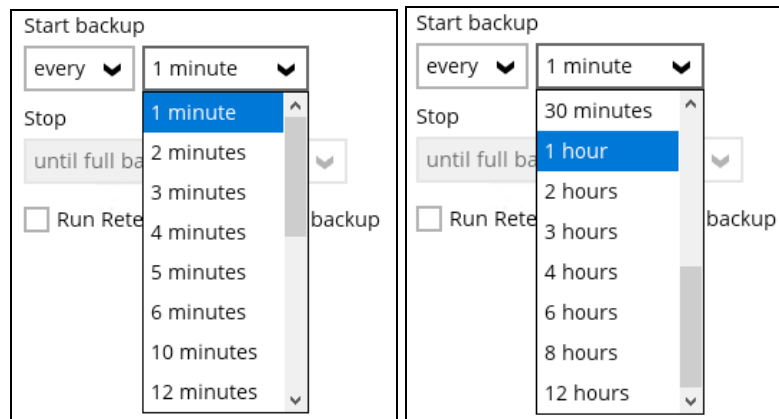
Backup on the following day once
2020 June 31

Start backup at
23:59

Stop
until full backup completed

Run Retention Policy after backup

- **Start backup** – the start time of the backup job.
 - **at** – this option will start a backup job at a specific time.
 - **every** – this option will start a backup job in intervals of minutes or hours.



- **Stop** – the stop time of the backup job. This only applies to schedules with start backup “at” and is not supported for periodic backup schedule (start backup “every”)
 - **until full backup completed** – this option will stop a backup job once it is complete. This is the configured stop time of the backup job by default.
 - **after (defined no. of hrs.)** – this option will stop a backup job after a certain number of hours regardless of whether the backup job has completed or not. This can range from 1 to 24 hrs.

The number of hours must be enough to complete a backup of all files in the backup set. For small files in a backup, if the number of hours is not enough to back up all files, then the outstanding files will be backed up in the next backup job. However, if the backup set contains large files, this may result in partially backed up files.

For example, if a backup has 100GB file size which will take approximately 15 hours to complete on your environment, but you set the “stop” after 10 hours, the file will be partially backed up and cannot be restored. The next backup will upload the files from scratch again.

The partially backed up data will have to be removed by running the data integrity check.

As a general rule, it is recommended to review this setting regularly as the data size on the backup machine may grow over time.

- **Run Retention Policy after backup** – if enabled, the AhsayOBM will run a retention policy job to remove files from the backup destination(s) which have exceeded the retention policy after performing a backup job. To save hard disk quote in the long run, it is recommended to enable this option.





As an example, the four types of backup schedules may look like the following:

Schedule

Run scheduled backup for this backup set

On

Existing schedules

-  **Daily-1**
Daily (Everyday at 15:41)
-  **Weekly-1**
Weekly - Saturday (Every week at 23:00)
-  **Monthly-1**
Monthly - The Last Day (Every month at 23:00)
-  **Custom-1**
Custom (07/01/2020 at 23:59)

6. Click **Save** to confirm your settings once done.

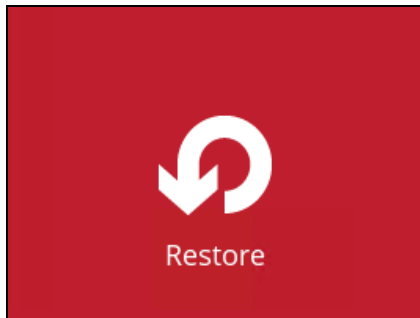
9 Restore with a MS Windows System Backup Set

9.1 Login to AhsayOBM

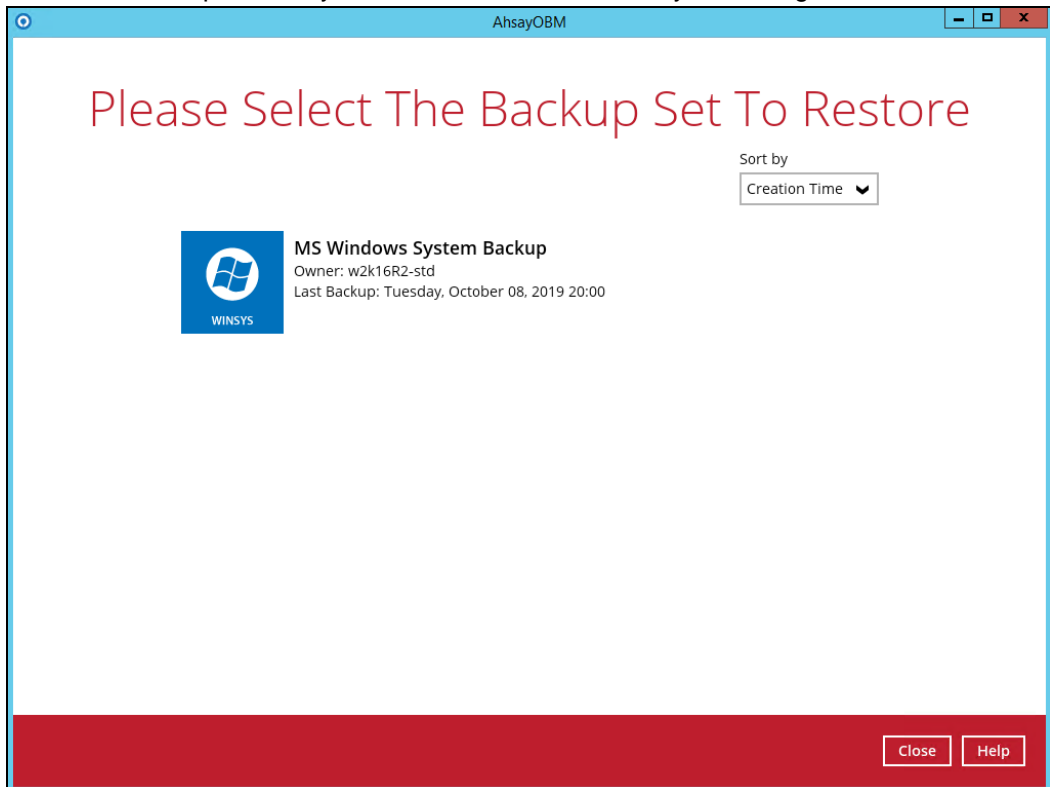
Login to the AhsayOBM application according to the instruction provided in the chapter on [Starting AhsayOBM](#).

9.2 Restore the System Image

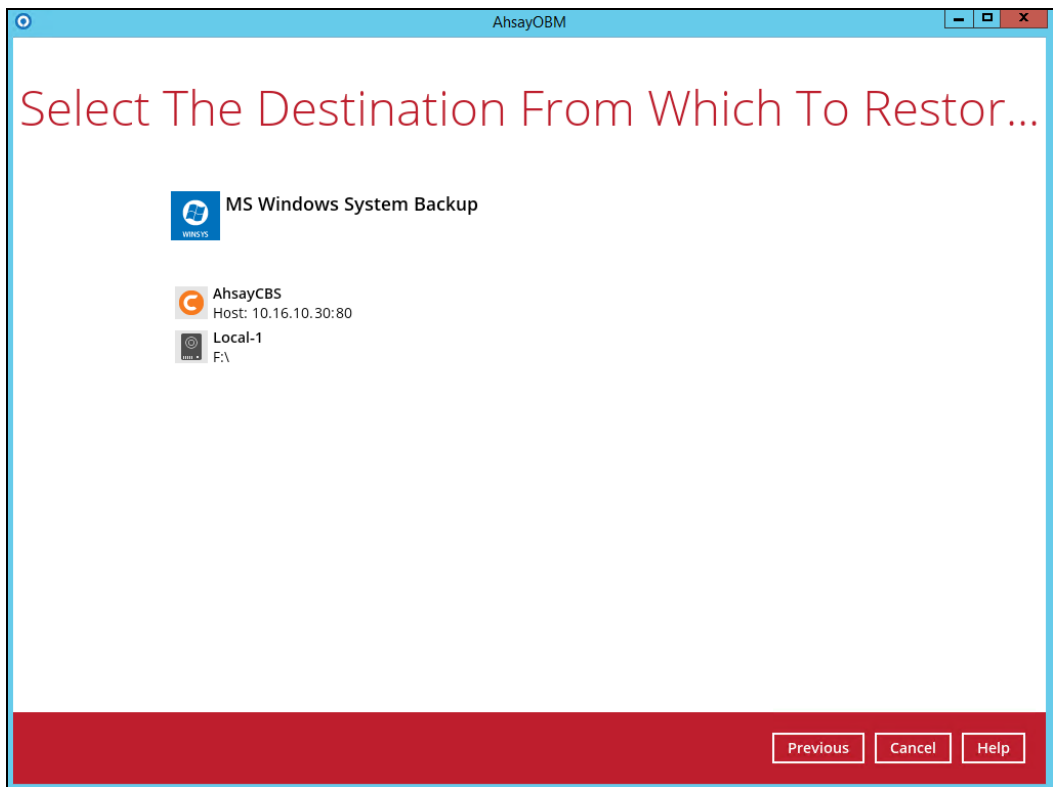
1. Click the **Restore** icon on the main interface of AhsayOBM.



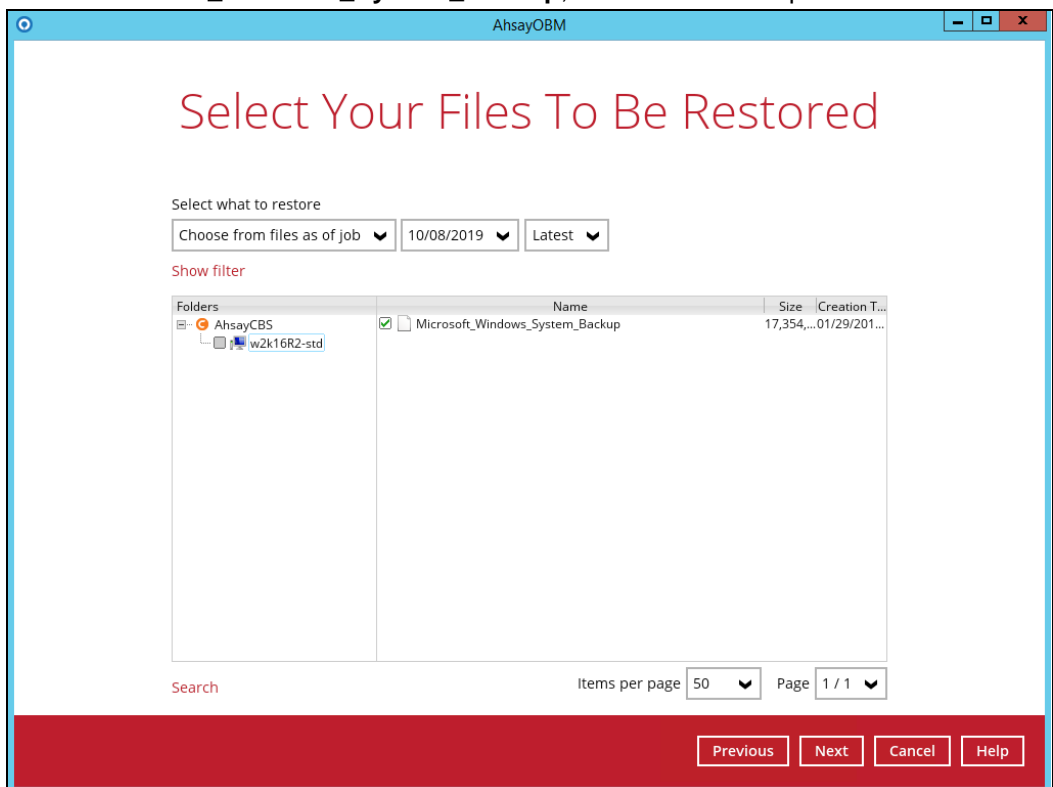
2. Select the backup set that you would like to restore the system image from.



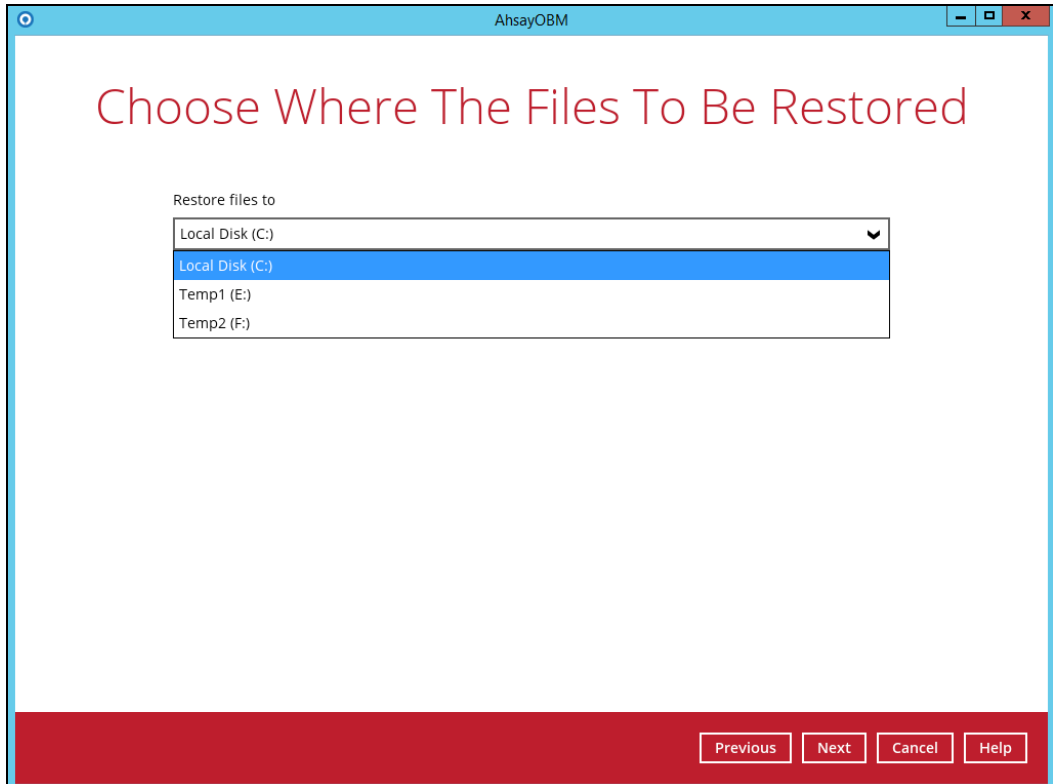
3. Select the backup destination that contains the system image that you would like to restore.



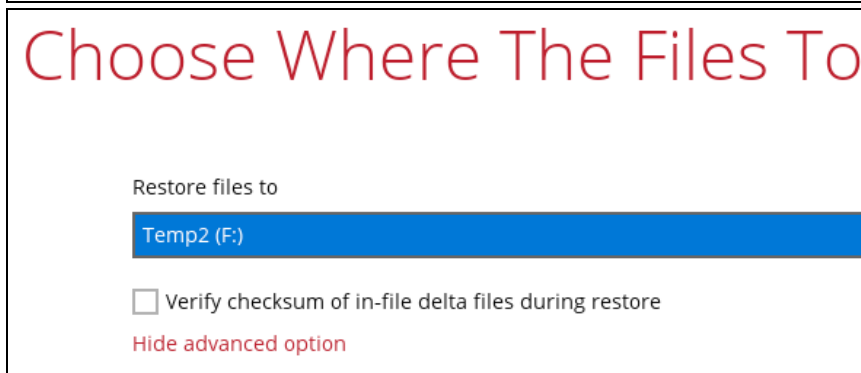
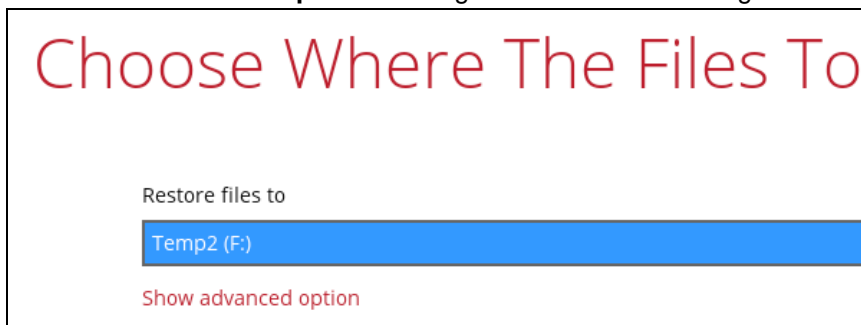
4. Select to restore from a specific backup job, or the latest job available from the **Select what to restore** drop down menu.
5. Select **Microsoft_Windows_System_Backup**, then click **Next** to proceed.



6. Select to restore the system image to a local volume or to a removable drive.



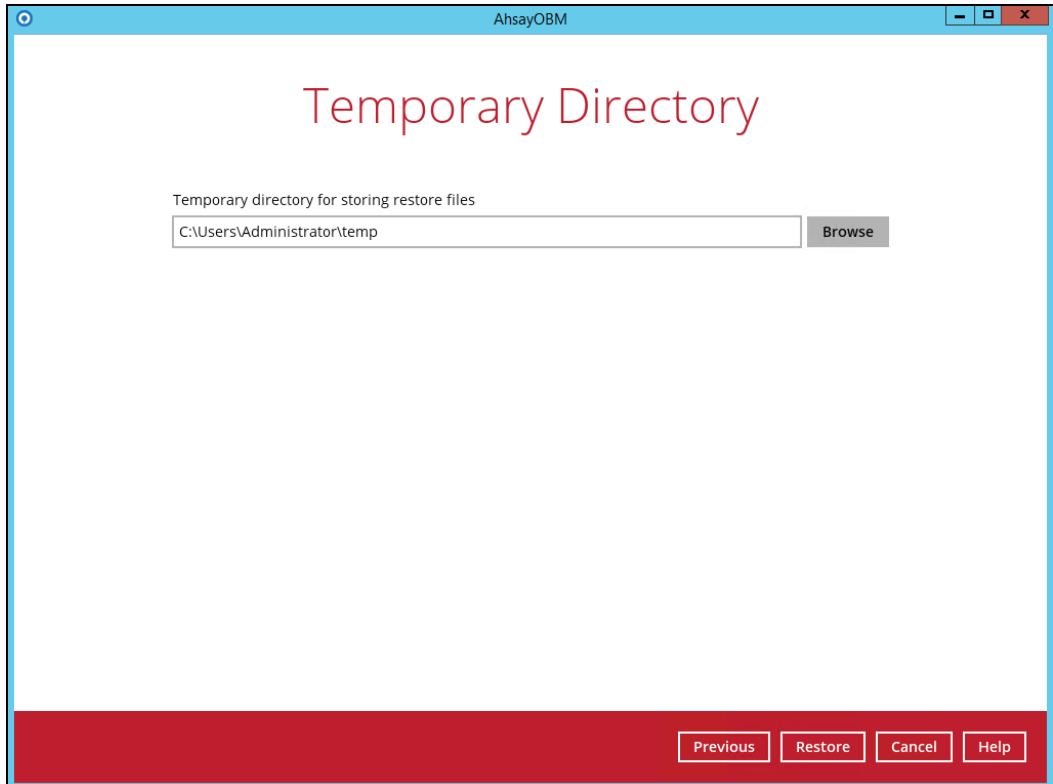
Click **Show advanced option** to configure other restore settings.



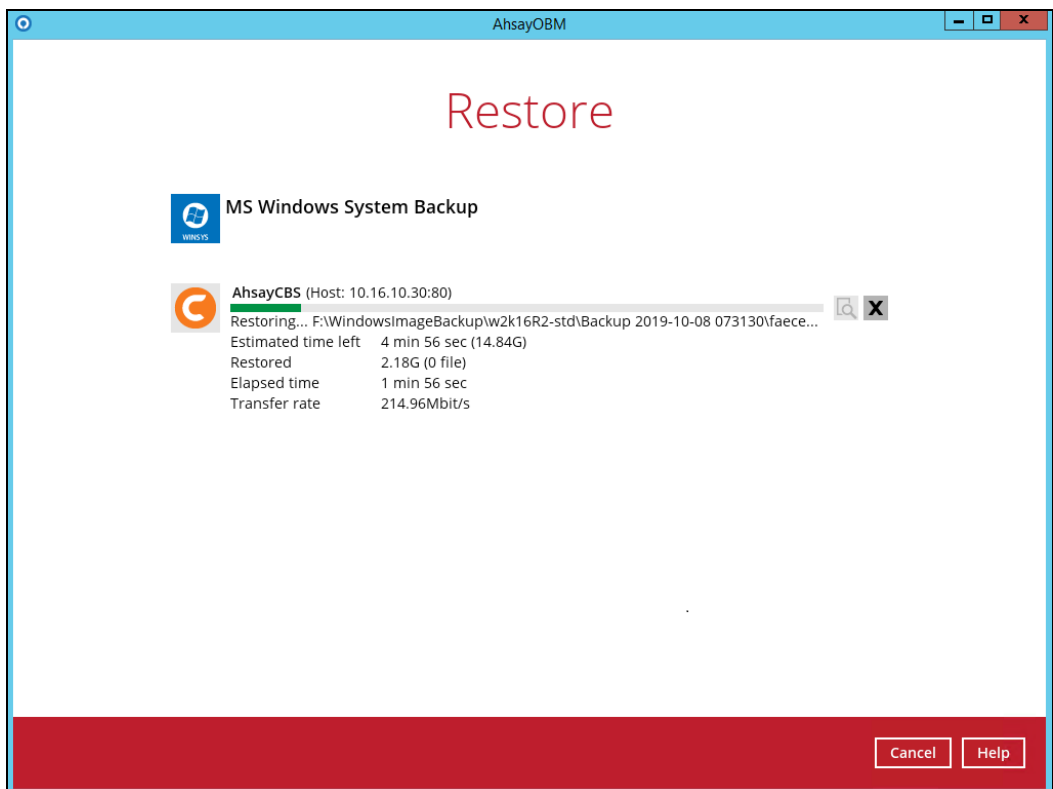
Verify checksum of in-file delta files during restore

By enabling this option, the checksum of in-file delta files will be verified during the restore process. This will check the data for errors during the restore process and create a data summary of the in-file delta files which will be included in the report.

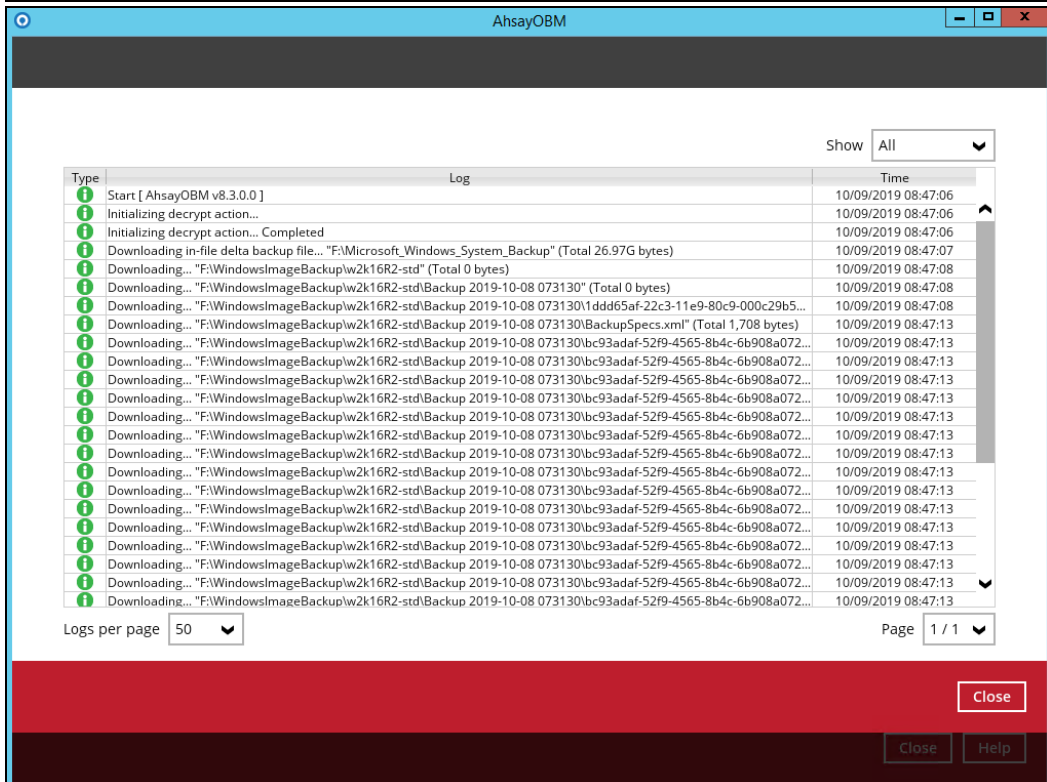
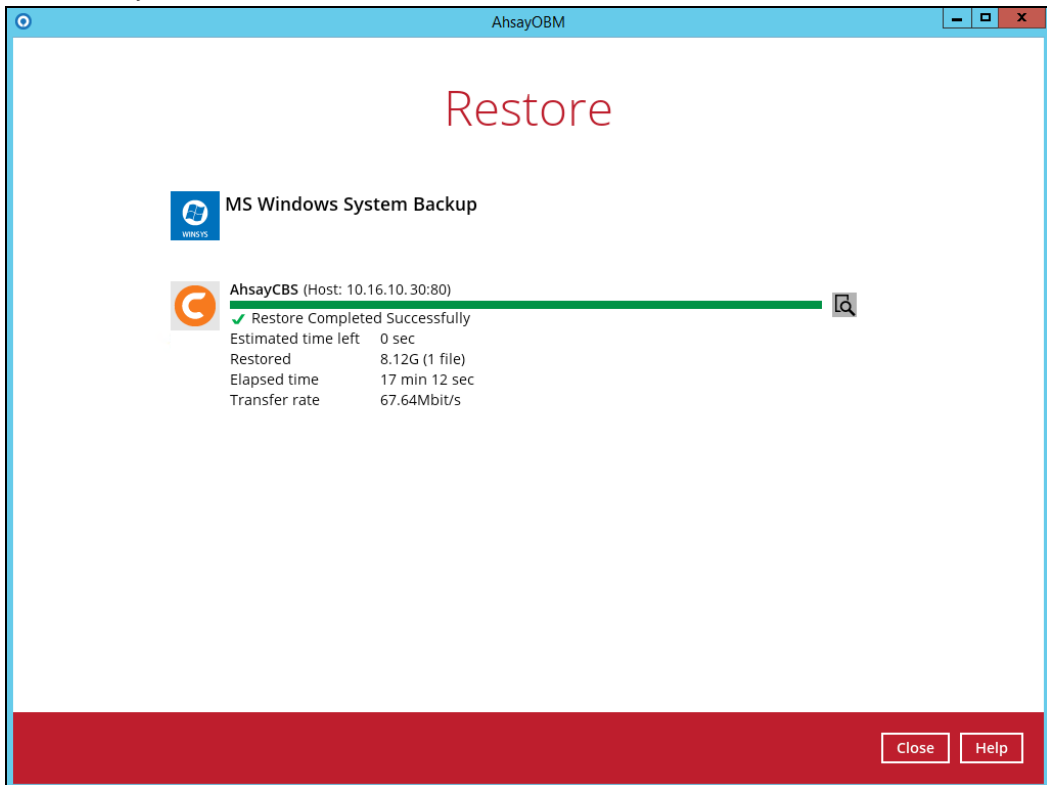
7. Select the temporary directory for storing temporary files.



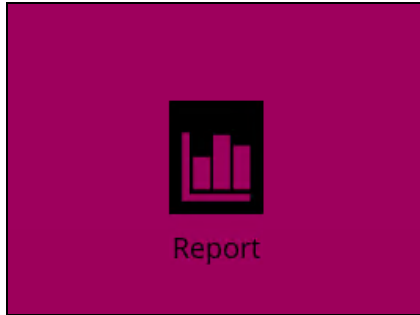
8. Click **Restore** to start the restoration.



9. The following screen is displayed when the system image files are restored successfully.



To view the report, go to the **Report > Restore**



In this Restore Report screen, you can see the backup set with corresponding destination, completion date and time, and status.

Backup set	Destination	Job	Status
MS Windows S...	AhsayCBS	Today 08:47	Completed

Click the restore report and the summary of the restoration will be displayed. You can also click the **View Log**, this will redirect you to the log summary of your backup.

Report

Backup

Restore

Usage

Restore Report

From: 02 Oct 2019 To: 09 Oct 2019 Go

Backup set	Destination	Job	Status
MS Windows System Backup	AhsayCBS	10/09/2019 08:47	Today 08:47 - 08:59 (CST)
		Status	✓ Completed successfully
		Downloaded files*	1 (17G)
<small>* Unit = No of files (Download size)</small>			
View log			

No. of records per page: 50 Page: 1 / 1

Close
Help

Report

Backup

Restore

Usage

Restore Report

Backup set: MS Windows System Backup

Log: 10/09/2019 08:47 Show: All

Type	Log	Time
Start [AhsayOBM v8.3.0.0]		10/09/2019 08:47:06
Initializing decrypt action...		10/09/2019 08:47:06
Initializing decrypt action... Completed		10/09/2019 08:47:06
Downloading in-file delta backup file... "F:\Microsoft_Windows_System_Backup" (Total 26.97G bytes)		10/09/2019 08:47:07
Downloading... "F:\WindowsImageBackup\w2k16R2-std\Backup 2019-10-08 073130" (Total 0 bytes)		10/09/2019 08:47:08
Downloading... "F:\WindowsImageBackup\w2k16R2-std\Backup 2019-10-08 073130\1ddd65af-22c3-11e9-80c9-000c29b5..." (Total 0 bytes)		10/09/2019 08:47:08
Downloading... "F:\WindowsImageBackup\w2k16R2-std\Backup 2019-10-08 073130\BackupSpecs.xml" (Total 1,708 bytes)		10/09/2019 08:47:13
Downloading... "F:\WindowsImageBackup\w2k16R2-std\Backup 2019-10-08 073130\bc93adaf-52f9-4565-8b4c-6b908a072..."		10/09/2019 08:47:13
Downloading... "F:\WindowsImageBackup\w2k16R2-std\Backup 2019-10-08 073130\bc93adaf-52f9-4565-8b4c-6b908a072..."		10/09/2019 08:47:13
Downloading... "F:\WindowsImageBackup\w2k16R2-std\Backup 2019-10-08 073130\bc93adaf-52f9-4565-8b4c-6b908a072..."		10/09/2019 08:47:13
Downloading... "F:\WindowsImageBackup\w2k16R2-std\Backup 2019-10-08 073130\bc93adaf-52f9-4565-8b4c-6b908a072..."		10/09/2019 08:47:13
Downloading... "F:\WindowsImageBackup\w2k16R2-std\Backup 2019-10-08 073130\bc93adaf-52f9-4565-8b4c-6b908a072..."		10/09/2019 08:47:13
Downloading... "F:\WindowsImageBackup\w2k16R2-std\Backup 2019-10-08 073130\bc93adaf-52f9-4565-8b4c-6b908a072..."		10/09/2019 08:47:13
Downloading... "F:\WindowsImageBackup\w2k16R2-std\Backup 2019-10-08 073130\bc93adaf-52f9-4565-8b4c-6b908a072..."		10/09/2019 08:47:13
Downloading... "F:\WindowsImageBackup\w2k16R2-std\Backup 2019-10-08 073130\bc93adaf-52f9-4565-8b4c-6b908a072..."		10/09/2019 08:47:13
Downloading... "F:\WindowsImageBackup\w2k16R2-std\Backup 2019-10-08 073130\bc93adaf-52f9-4565-8b4c-6b908a072..."		10/09/2019 08:47:13
Downloading... "F:\WindowsImageBackup\w2k16R2-std\Backup 2019-10-08 073130\bc93adaf-52f9-4565-8b4c-6b908a072..."		10/09/2019 08:47:13
Downloading... "F:\WindowsImageBackup\w2k16R2-std\Backup 2019-10-08 073130\bc93adaf-52f9-4565-8b4c-6b908a072..."		10/09/2019 08:47:13

Logs per page: 50 Page: 1 / 1

Close
Help

You can also search for restore reports from a specific period of date. For example, we have the **From** date which is, **01 Jan 2019** and the **To** date which is, **23 Jan 2019**. Then click the **Go** button to generate the available reports.

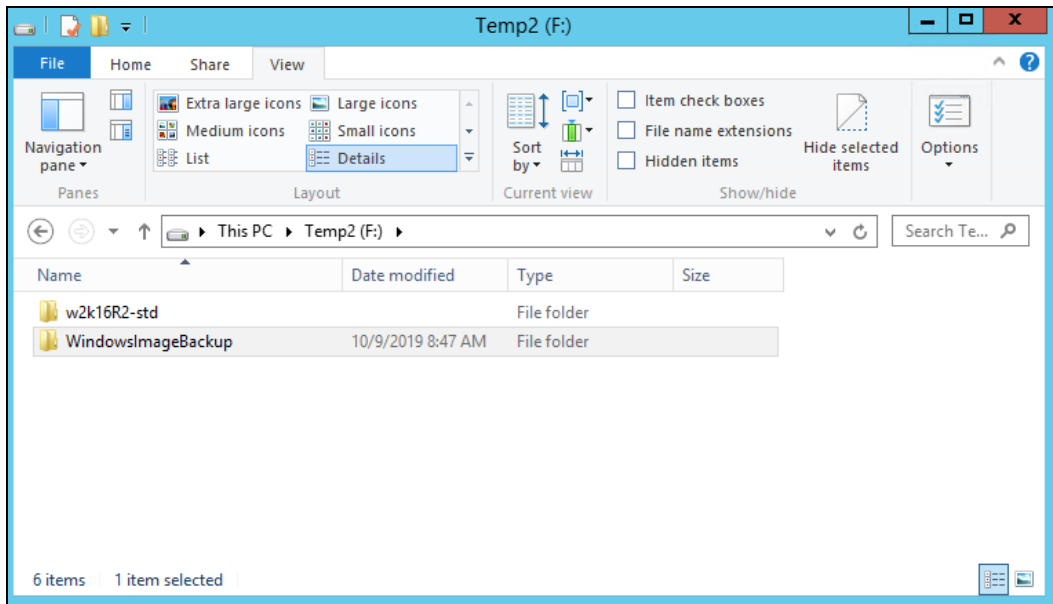
From		To					
01	Oct	2019	09	Oct	2019	Go	

If this is a valid range of dates then restore reports will be displayed unless there were no restoration running on the specified dates. A message of **No records found** will also be displayed.

From		To					
01	Oct	2019	05	Oct	2019	Go	

The screenshot shows the AhsayOBM web application interface. On the left is a sidebar with a 'Report' section containing 'Backup', 'Restore', and 'Usage' options. The main area is titled 'Restore Report' and contains a search form with 'From' and 'To' date pickers, a 'Go' button, and a table with columns for 'Backup set', 'Destination', 'Job', and 'Status'. Below the table, it displays 'No records found'. At the bottom, there are controls for 'No. of records per page' (set to 50) and 'Page' (set to -). A footer bar contains 'Close' and 'Help' buttons.

10. The restored system image files are stored in the **WindowsImageBackup** folder in the restore location.



Important: In addition to the system image files, the **WindowsImageBackup** folder includes catalog files that contain information about all backups in there up to the current backup, and Mediald, that contains the identifier for the backup storage location.

This information is required to perform a recovery. Do not alter the directory structure or delete any file / folder within the **WindowsImageBackup** folder.

11. Copy the **WindowsImageBackup** folder with its content to the server that you want to perform the restore for or copy the folder to a network drive that is accessible to the server that you want to perform the restore for.

WindowsImageBackup folder must be stored at the root level of a volume (e.g. top-most level), unless you are copying the folder to a network drive.

12. Continue to the next section of the guide.

9.3 Recovering Your Server

For server platforms such as Server 2008 / 2008 R2 / 2012 / 2012 R2, you can recover individual files, folders, volumes, application, application data, operating system, or full-system (bare-metal) with the following tools:

Tool	What you can recover
Recovery wizard (in Windows Server Backup)	Files, folders, volumes, application, and application data.
Windows setup disc / Windows Recovery Environment (Windows RE)	Operating system (critical volume), and full server recovery (all volumes).

Note: You can also perform the above tasks using `wbadmin` command. For the syntax of the command, refer to the following: <http://go.microsoft.com/fwlink/?LinkId=140216>

To determine what can be recovered from your restored system image, enter the following command in an elevated command prompt:

```
wbadmin get versions
[-backupTarget:<BackupTargetLocation> | <NetworkSharePath>]
```

Example (system image restored to G: volume):

```
C:\Users\Administrator>wbadmin get versions -backupTarget:g:
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2012 Microsoft Corporation. All rights reserved.

Backup time: 1/29/2019 10:29 AM
Backup target: 1394/USB Disk labeled Temp1 (E:)
Version identifier: 01/29/2019-02:29
Can recover: Volume(s), File(s), Application(s), Bare Metal
Recovery, System State
Snapshot ID: {f8cf57da-0c9d-453c-adbb-5f9a976c75c2}
```

For non-server platforms such as Windows 7 / 8 / 8.1 / 10, you can recover the full-system (bare-metal) with the following tools:

Tool	What you can recover
Advanced startup option (in safe mode)	Full system recovery.
Advanced startup option (Windows installation media)	Full system recovery.

Note: You can also perform the above tasks using `wbadmin` command. For the syntax of the command, refer to the following: <http://go.microsoft.com/fwlink/?LinkId=140216>

The following chapters in this guide contain instructions for:

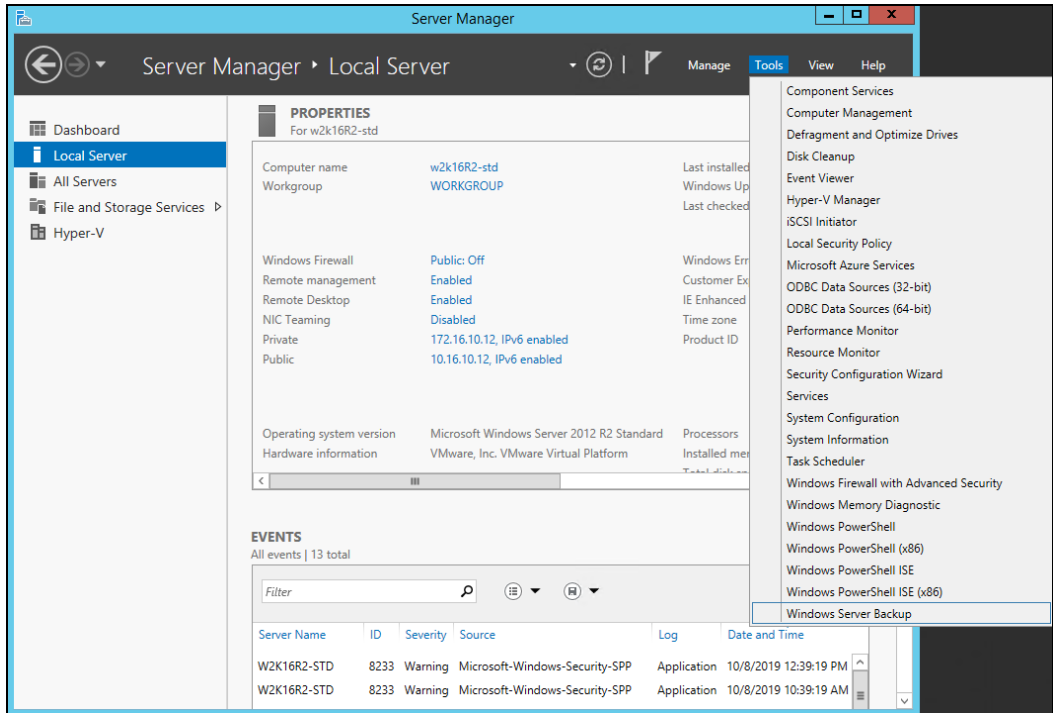
- ▶ [Recover Files and Folders](#)
- ▶ [Recover Application and Data](#)
- ▶ [Recover Volumes](#)
- ▶ [Recover the Operating System or Full System](#)
- ▶ [Recover the Full System \(Non-Server Platforms\)](#)

For instructions specific to recovering Active Directory Domain Services, refer to the following:
<http://go.microsoft.com/fwlink/?LinkId=143754>.

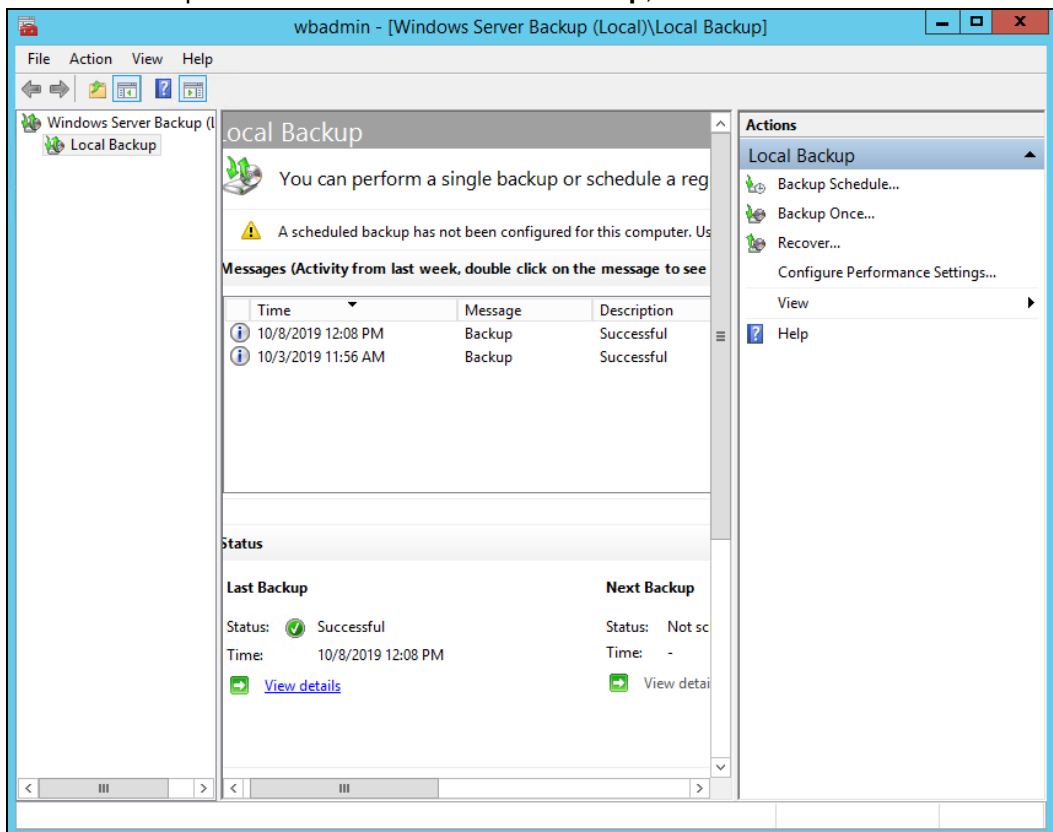
9.3.1 Recover Files and Folders

To recover files and folders using the Recovery Wizard in the Windows Server Backup user interface.

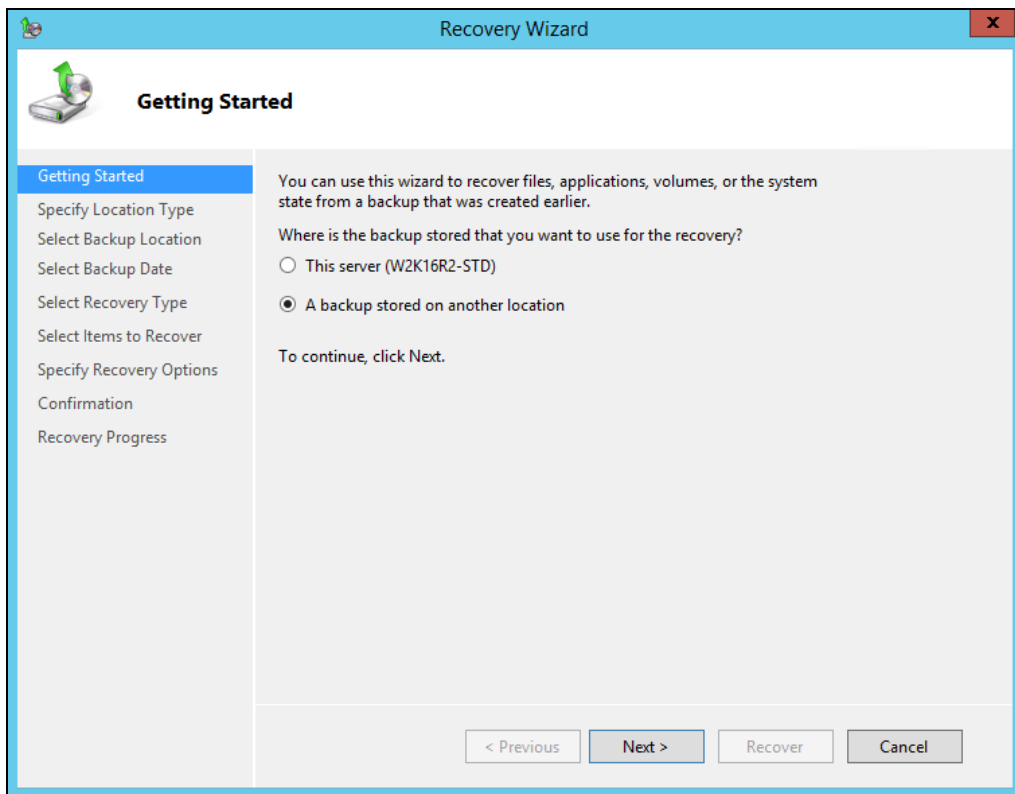
1. Open **Windows Server Backup** from **Administrative Tools** or **Server Manager**.



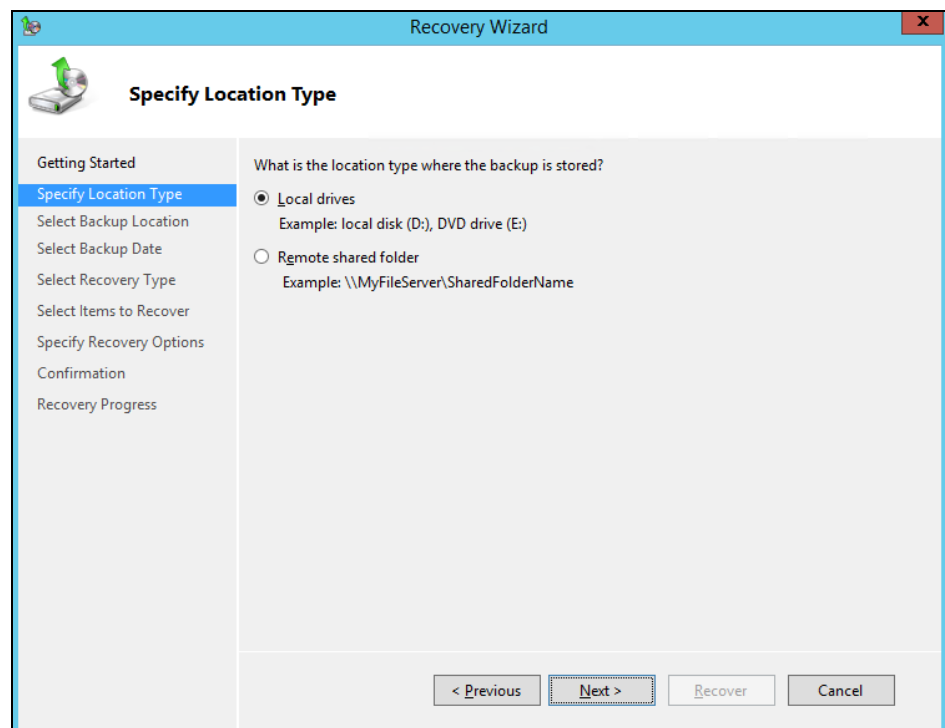
2. In the **Actions** panel under **Windows Server Backup**, click **Recover...**



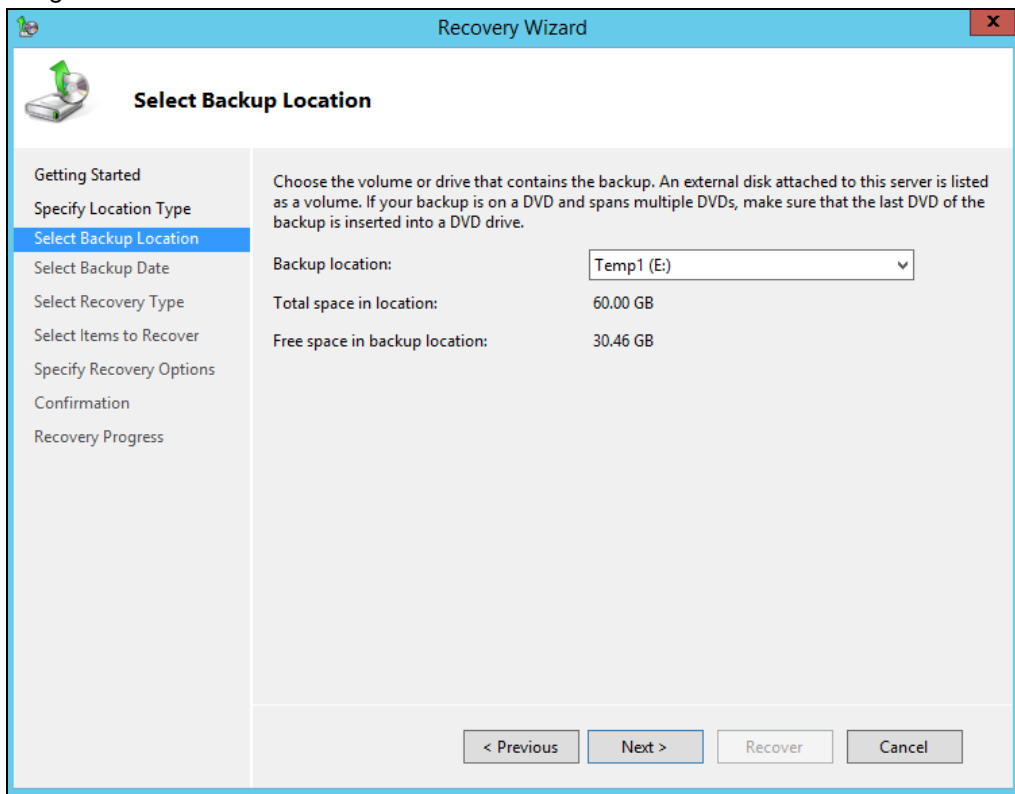
3. On the **Getting Started** page, select **A backup stored on another location**, then click **Next**.



4. On the **Specify Location Type** page, select
 - Click **Local drives** if the system image was copied to a local volume on the server.
 - Click **Remote shared folder**, if the system image was copied to a network path accessible to this server.

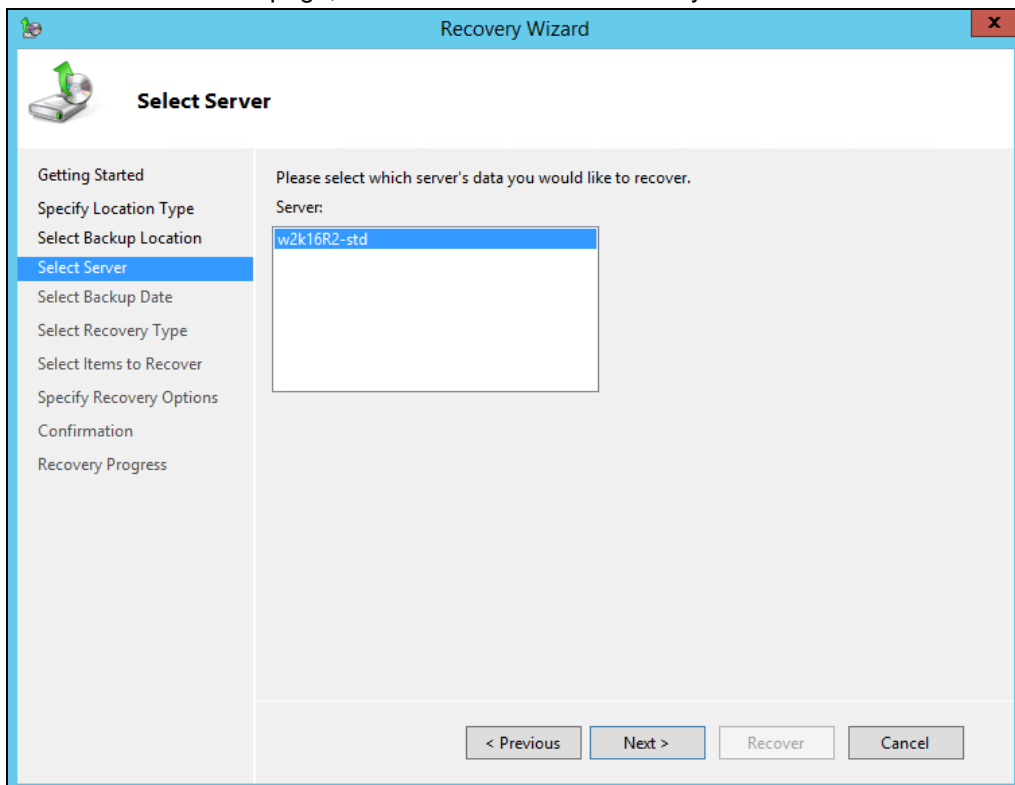


5. On the **Select Backup Location** page, select the volume that contains the system image file.

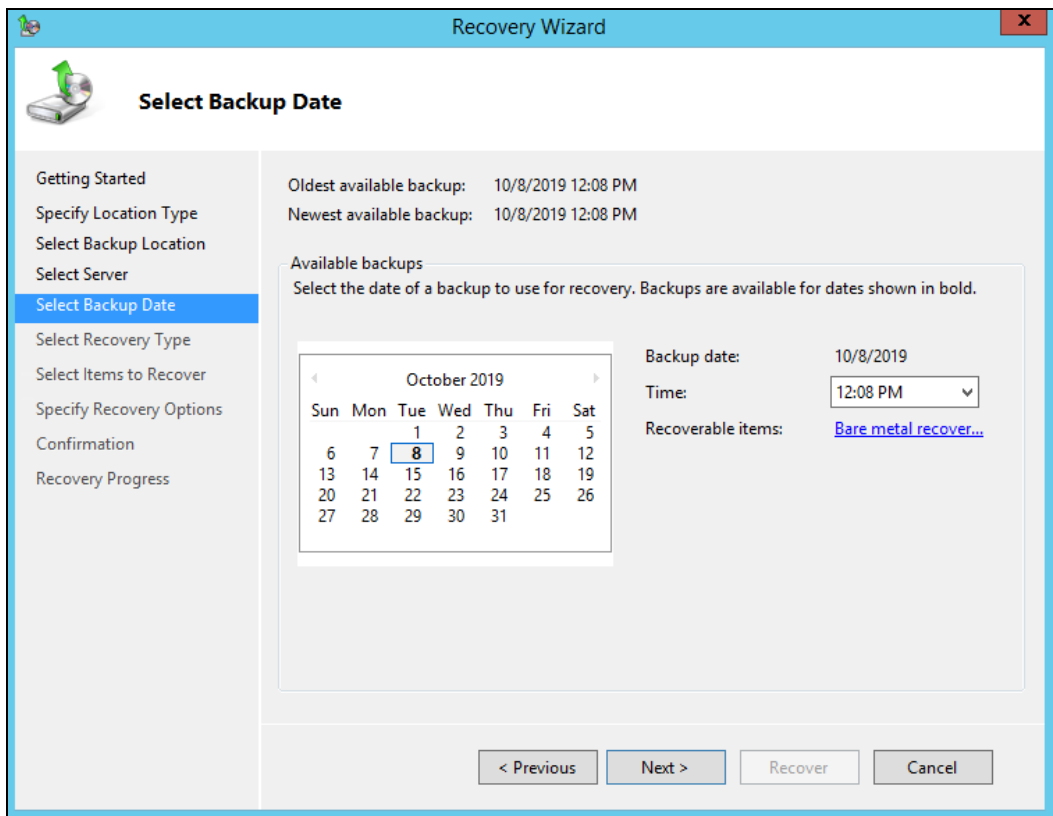


Note: Assuming that the **WindowsImageBackup** folder was copied to the following **F:\WindowsImageBackup**

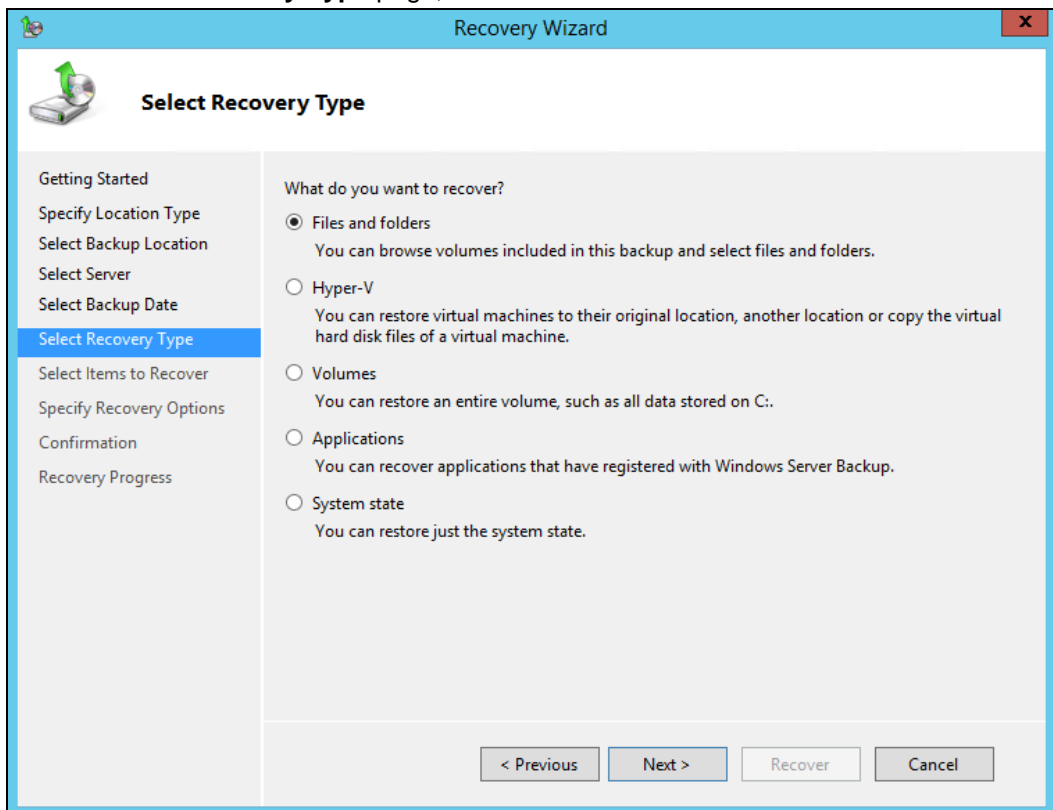
6. On the **Select Server** page, select the server whose data you want to recover.



- On the **Select Backup Date** page, select the point in time of the backup you want to restore from.

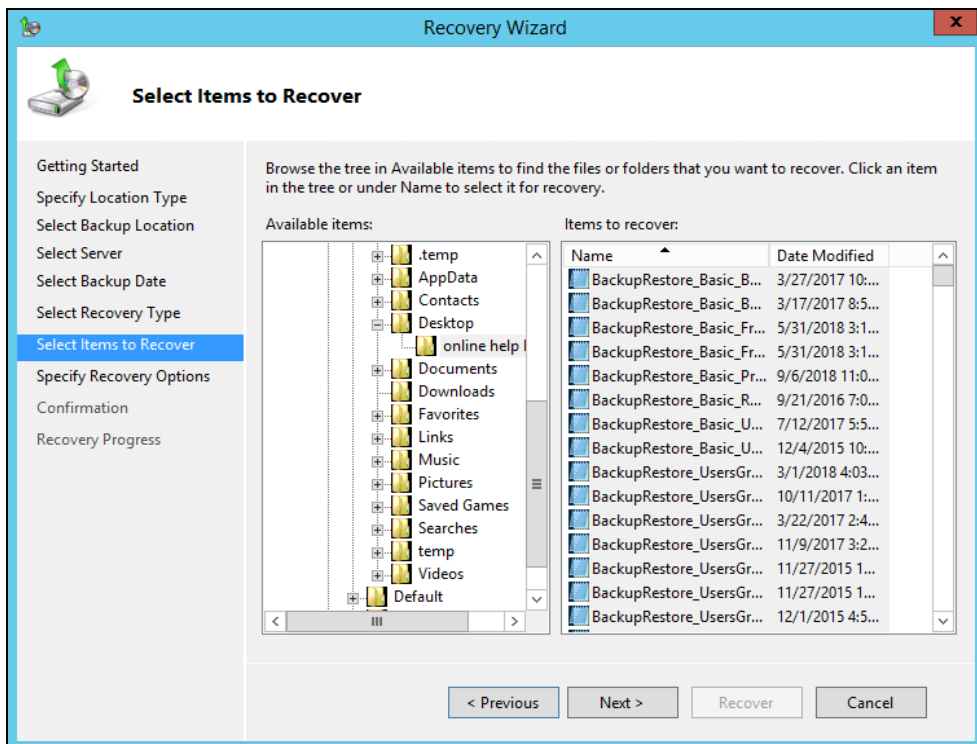


- On the **Select Recovery Type** page, click **Files and folders**.



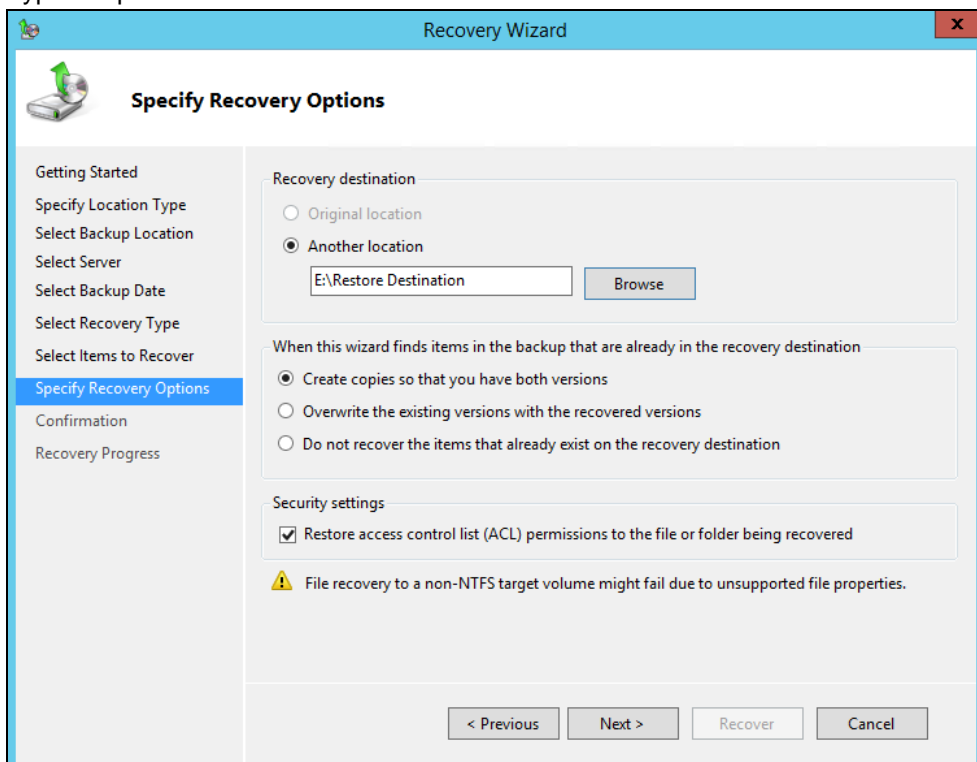
- On the **Select Items to Recover** page, under **Available items**, expand the list until the folder you want is visible.

Click a folder to display the contents in the adjacent pane, click each item that you want to restore.



- On the **Specify Recovery Options** page, under **Recovery destination**, select **Alternate location**.

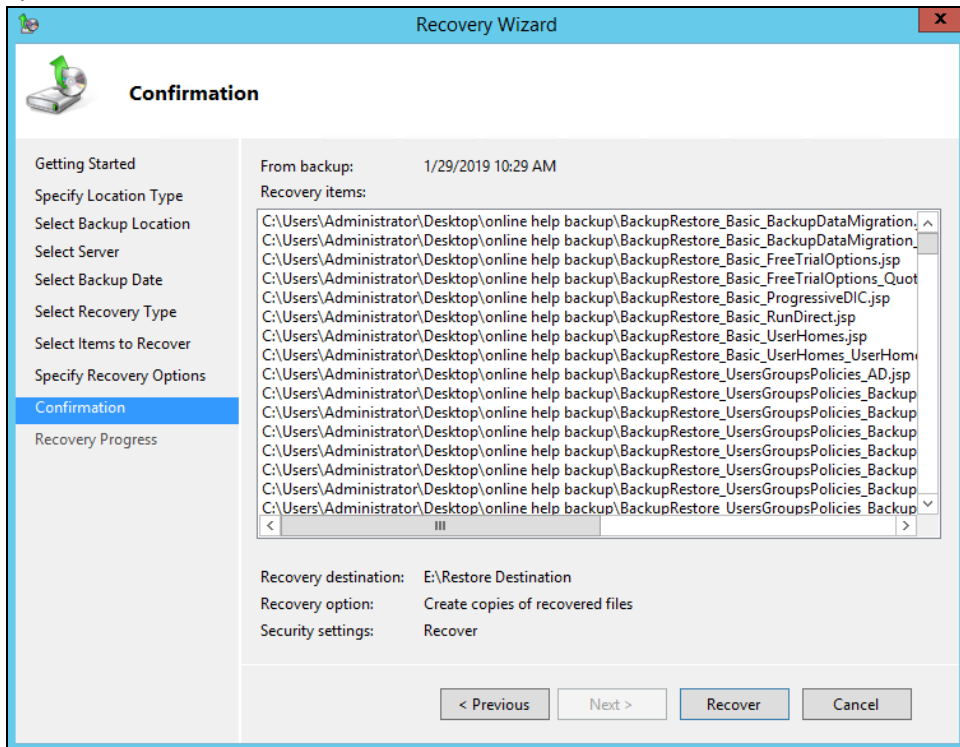
Type the path to the location or click **Browse** to select it.



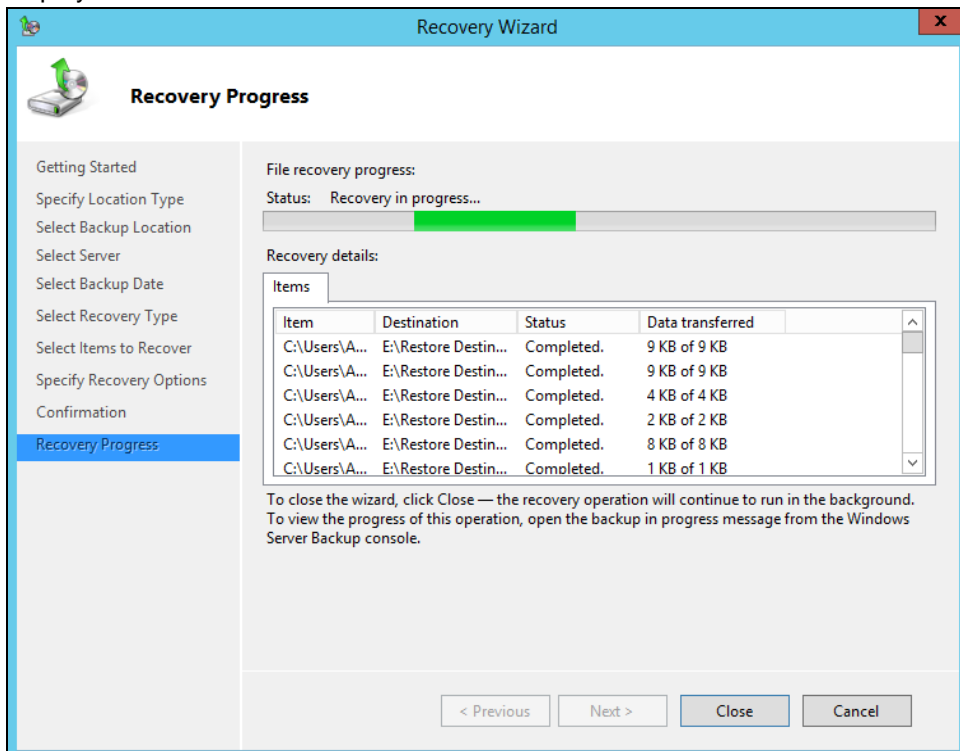
Modify the **When this wizard finds items in the backup that are already in the recovery destination** setting, and the **Security settings** if necessary.

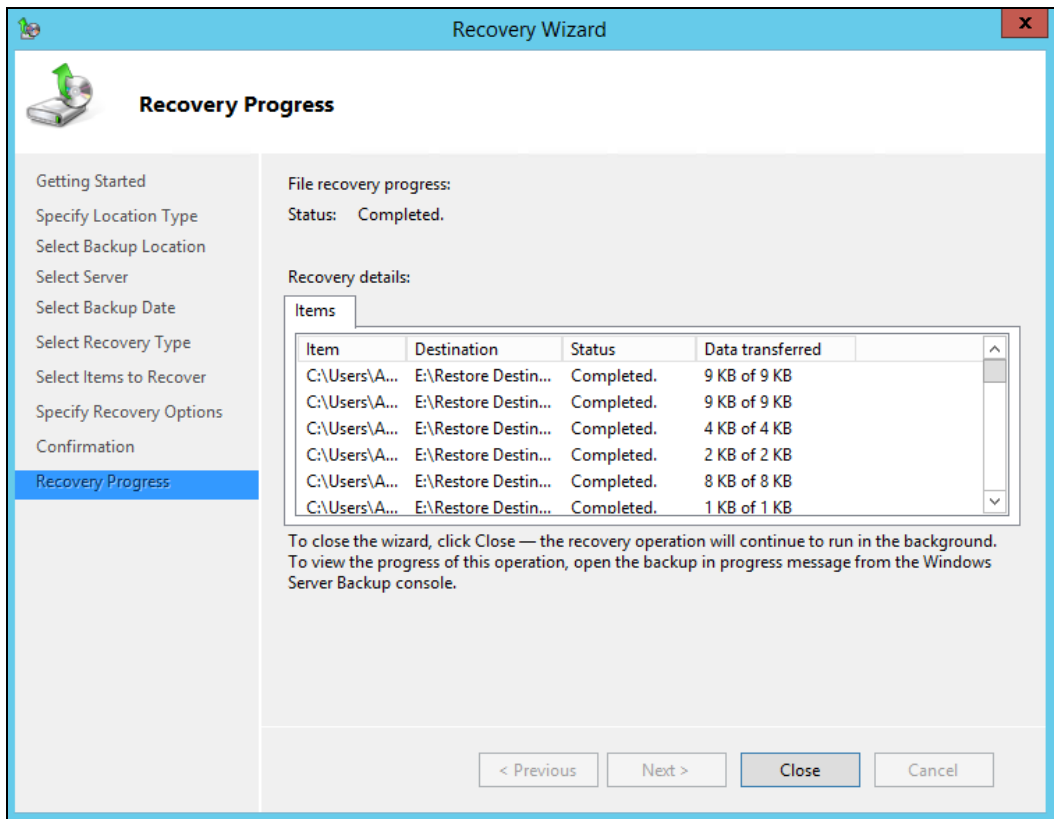
Click **Next** to proceed.

- On the **Confirmation** page, review the details, and then click **Recover** to restore the specified items.



- On the **Recovery progress** page, the status and result of the recovery operation is displayed.

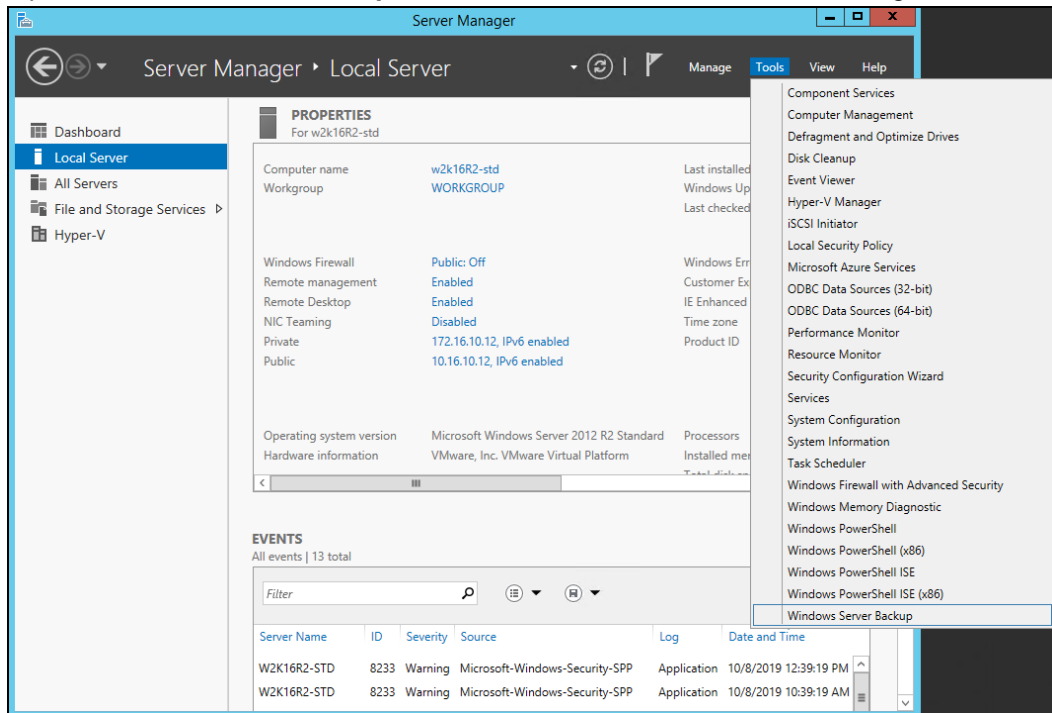




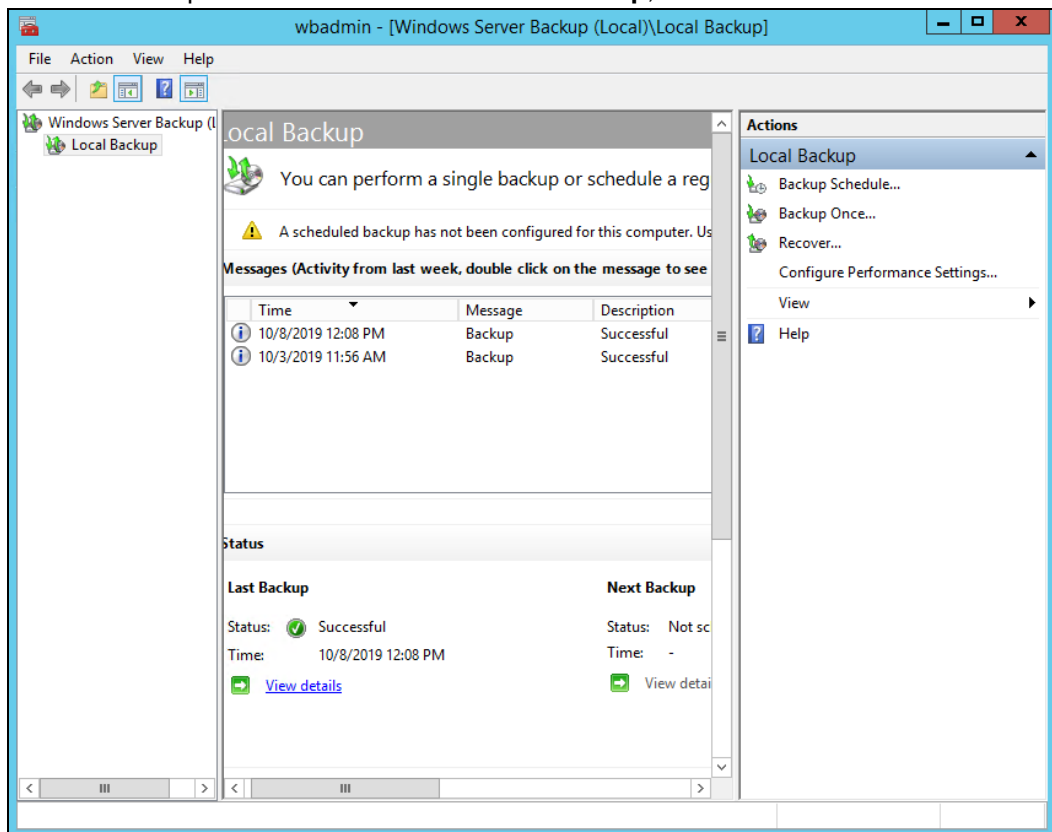
9.3.2 Recover Applications and Data

To recover application and data using the Recovery Wizard in the Windows Server Backup user interface.

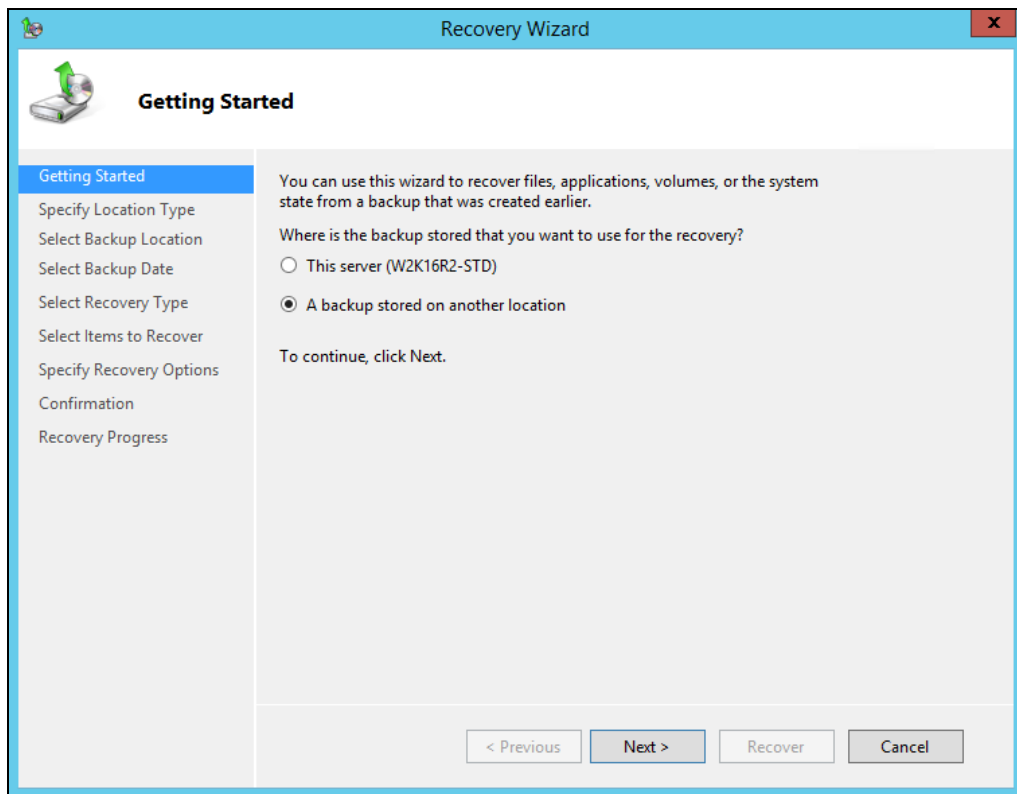
1. Open **Windows Server Backup** from Administrative Tools or Server Manager.



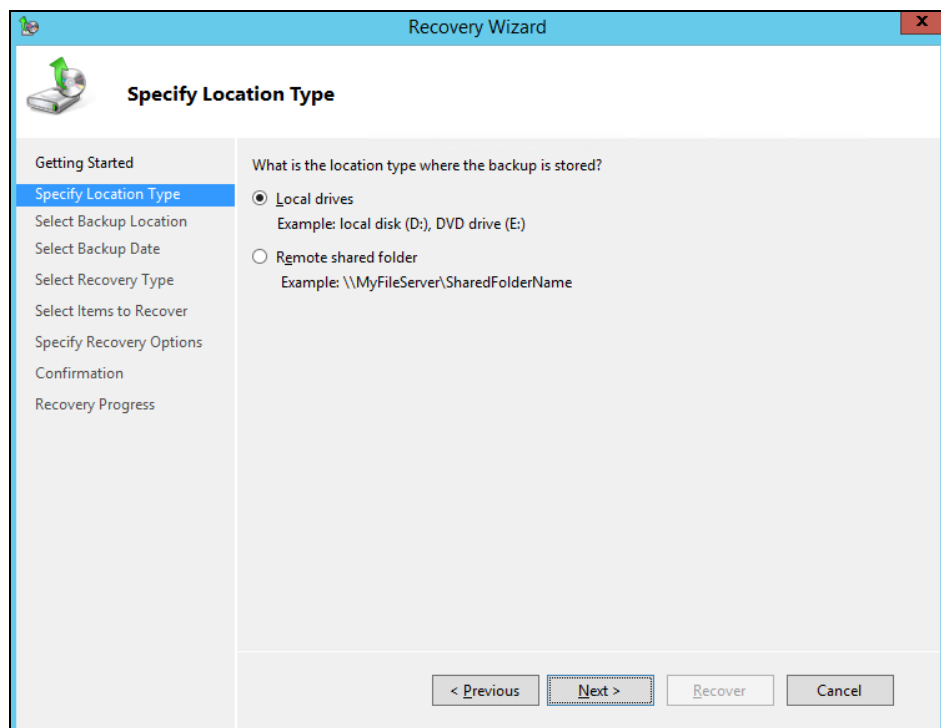
2. In the **Actions** panel under **Windows Server Backup**, click **Recover...**



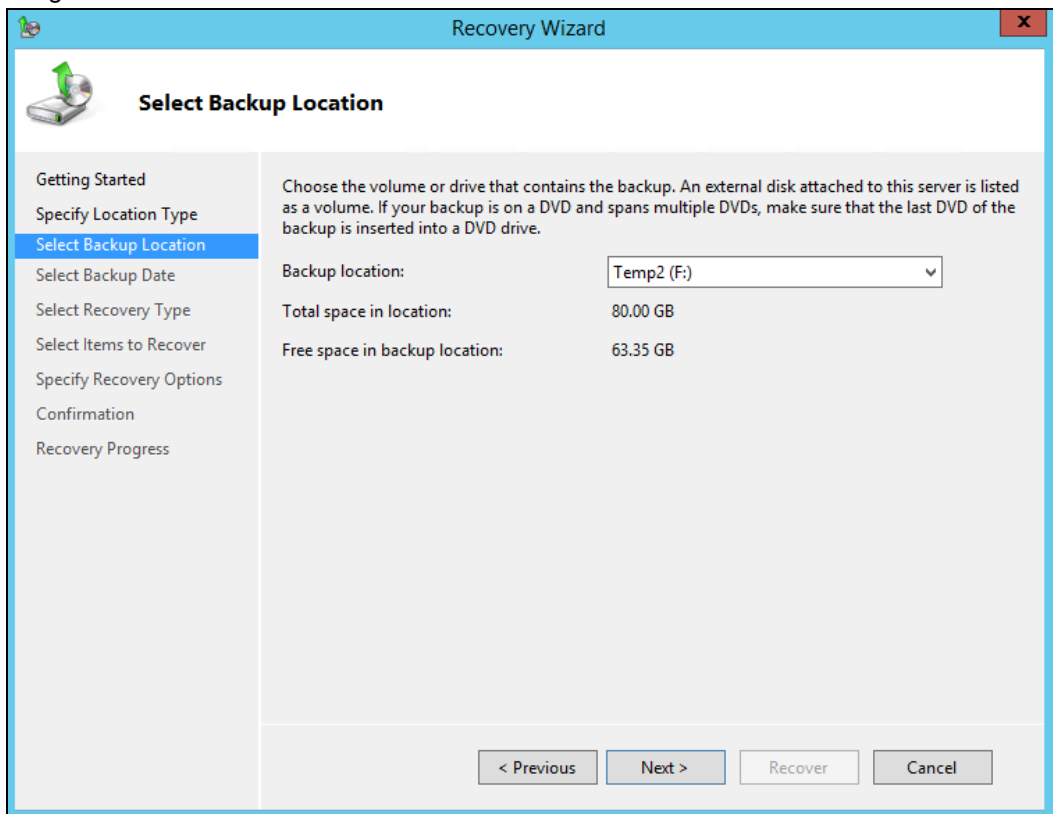
3. On the **Getting Started** page, select **A backup stored on another location**, then click **Next**.



4. On the **Specify Location Type** page, select
 - Click **Local drives** if the system image was copied to a local volume on the server.
 - Click **Remote shared folder**, if the system image was copied to a network path accessible to this server.

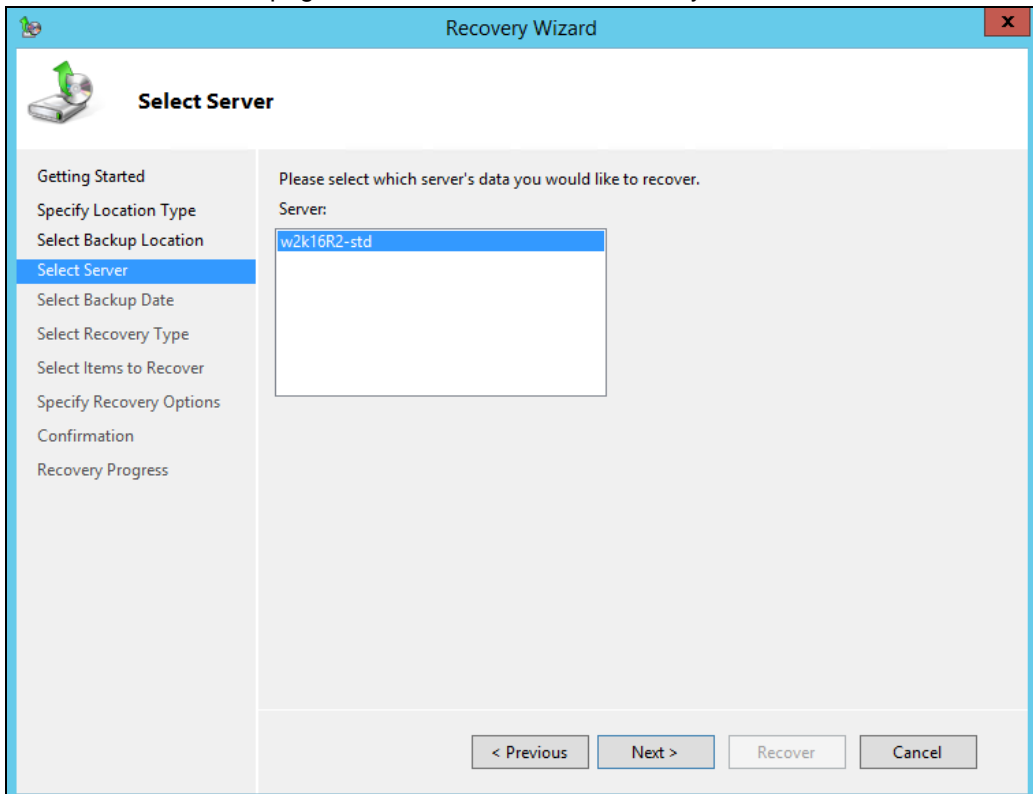


5. On the **Select Backup Location** page, select the volume that contains the system image file.

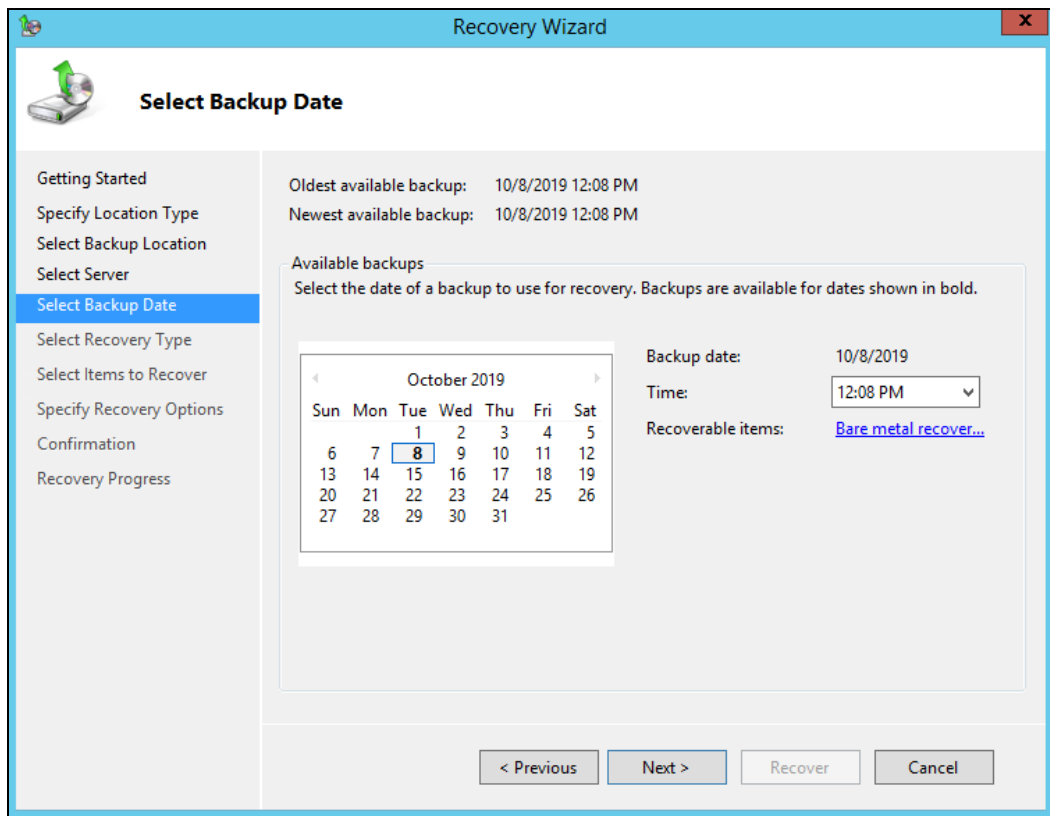


Note: Assuming that the *WindowsImageBackup* folder was copied to the following *F:\WindowsImageBackup*

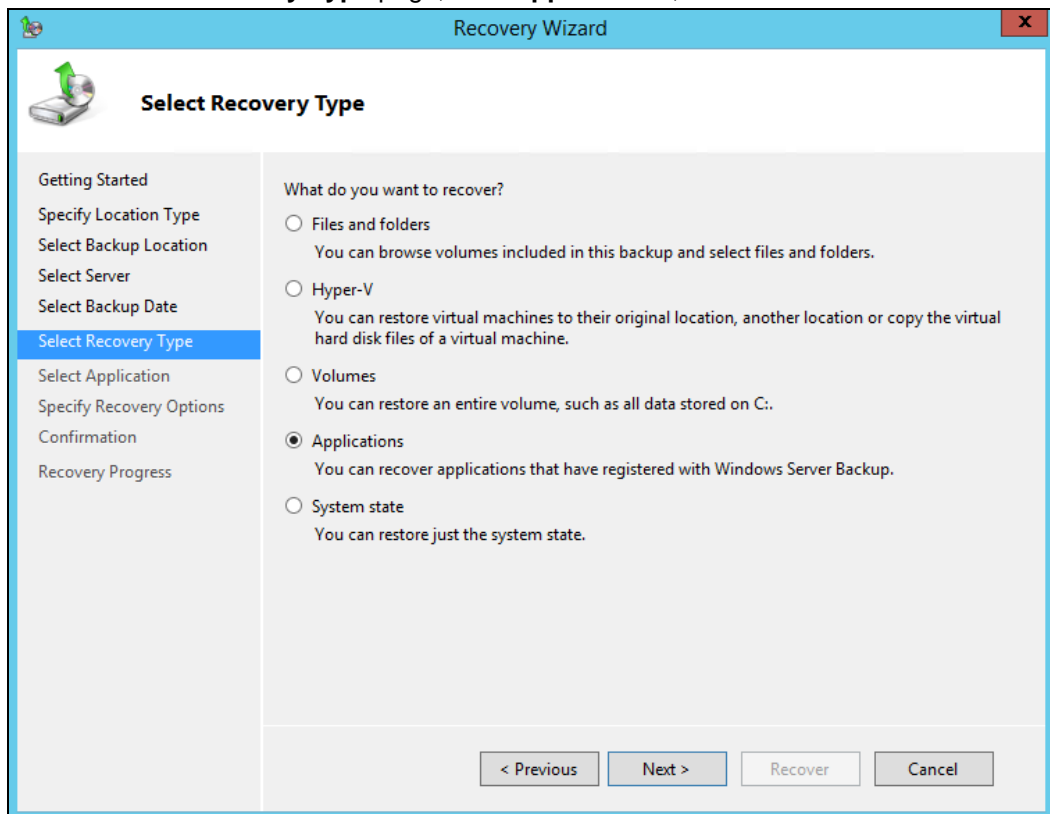
6. On the **Select Server** page, select the server whose data you want to recover.



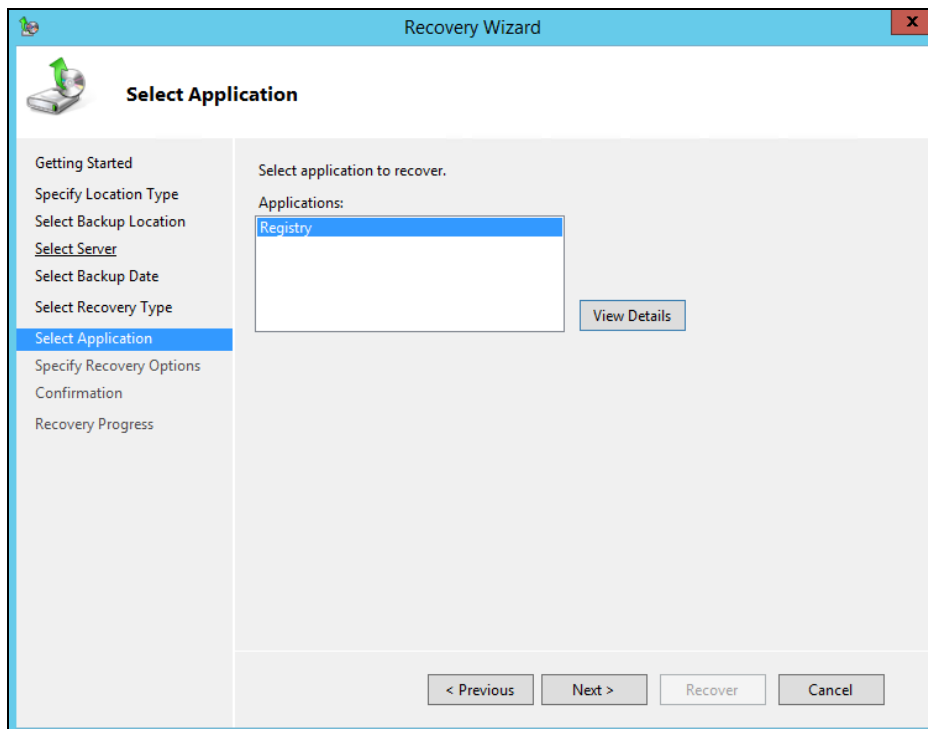
- On the **Select Backup Date** page, select the point in time of the backup you want to restore from



- On the **Select Recovery Type** page, click **Applications**, and then click **Next**.



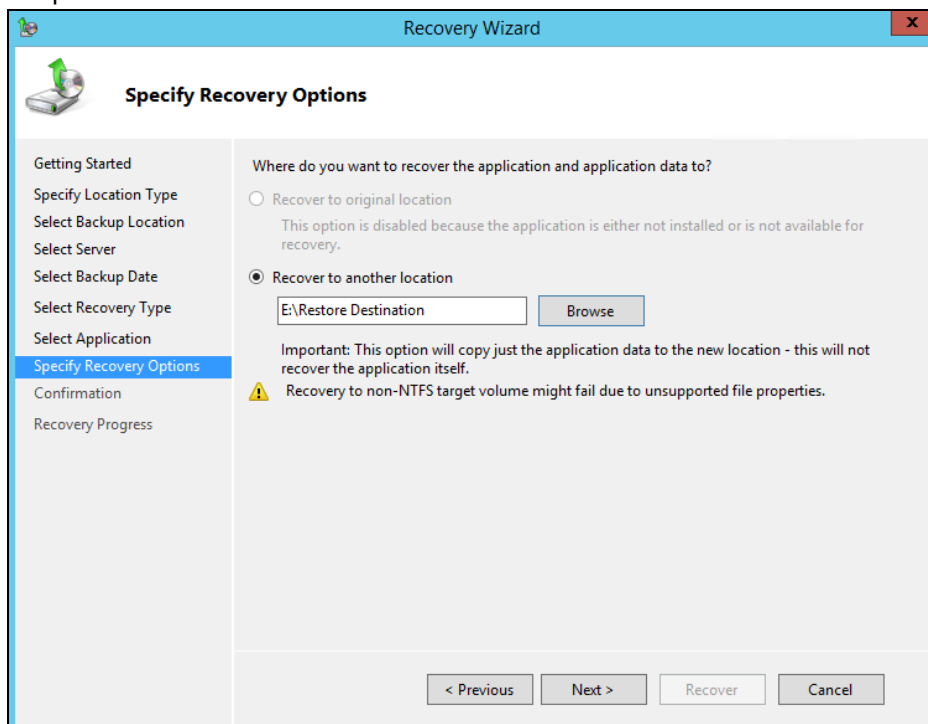
9. On the **Select Application** page, under **Applications**, click the application that you want to recover.



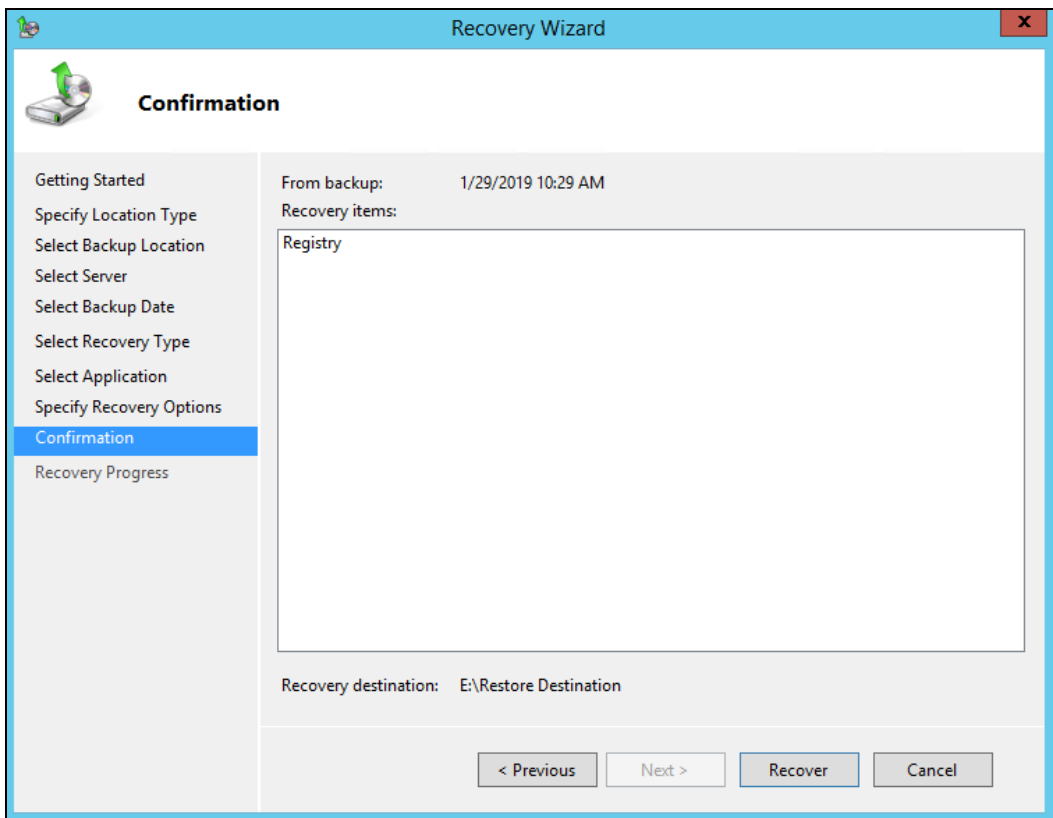
Note: If the backup that you are using is the most recent and the application you are recovering supports a "roll-forward" of the application database, you will see a check box labeled **Do not perform a roll-forward recovery of the application databases**.

Select this check box if you want to prevent Windows Server Backup from rolling forward the application database that is currently on your server.

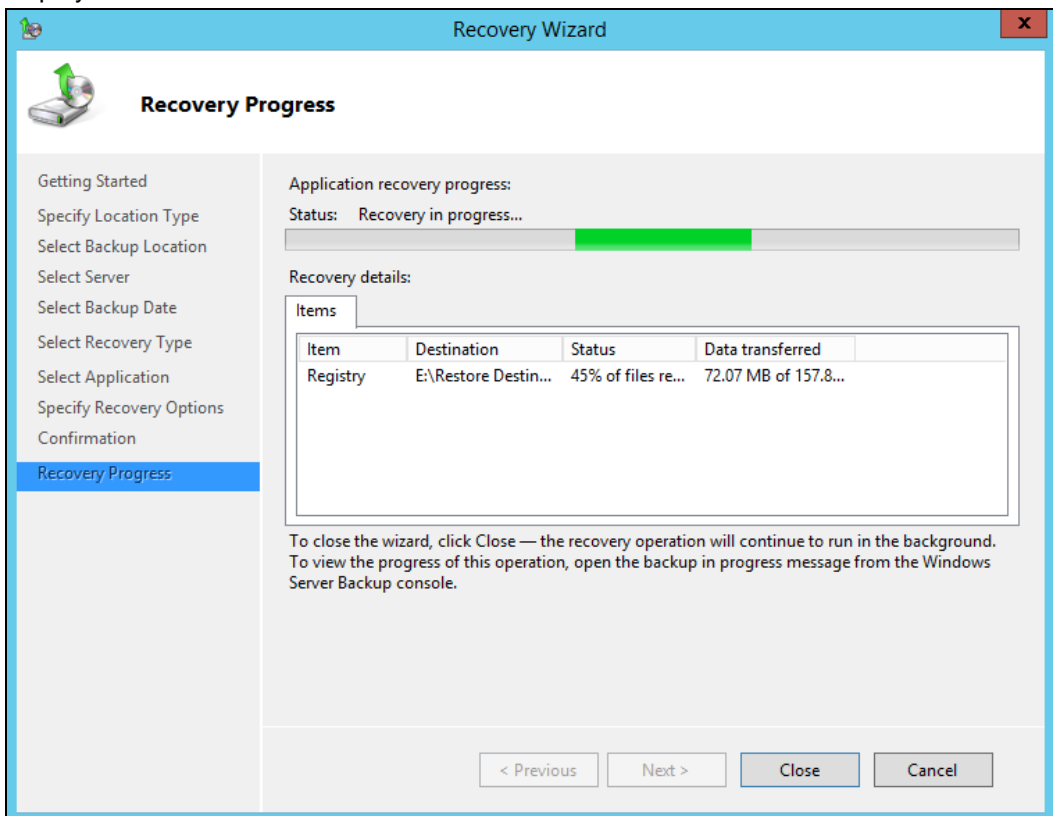
10. On the **Specify Recovery Options** page, select **Recover to another location**. Type the path to the location or click **Browse** to select it.

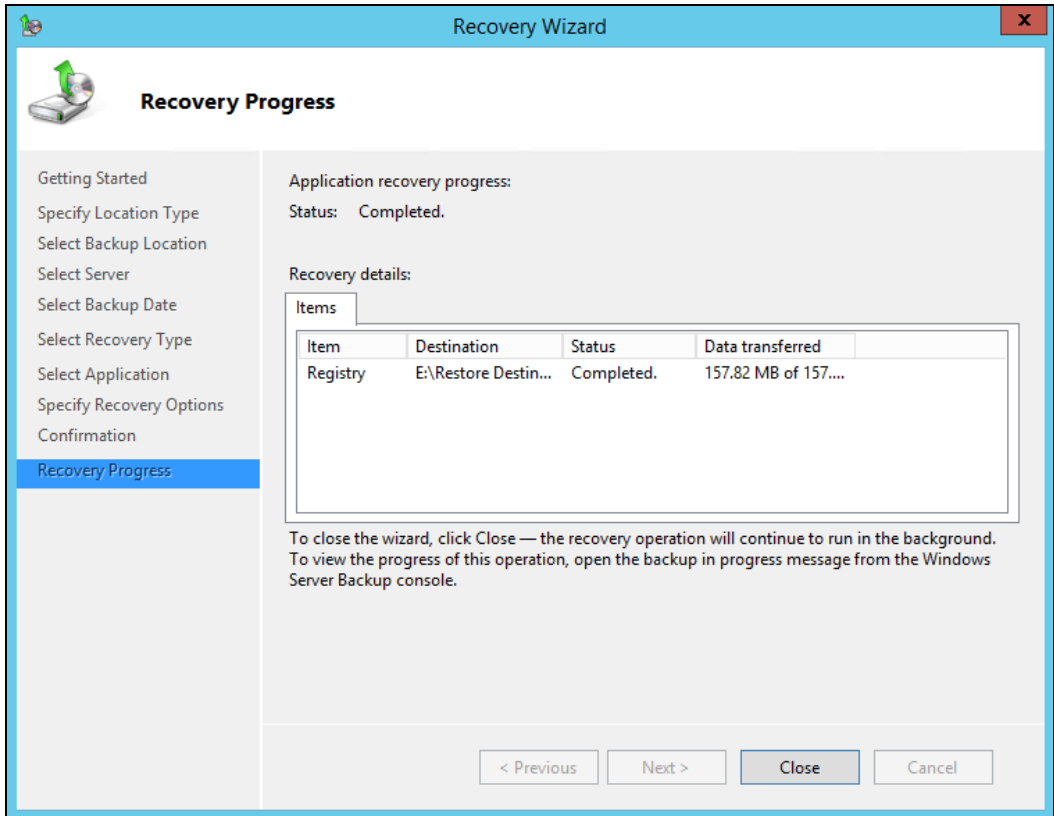


- On the **Confirmation** page, review the details, and then click **Recover** to restore the listed items.



- On the **Recovery progress** page, the status and result of the recovery operation is displayed.

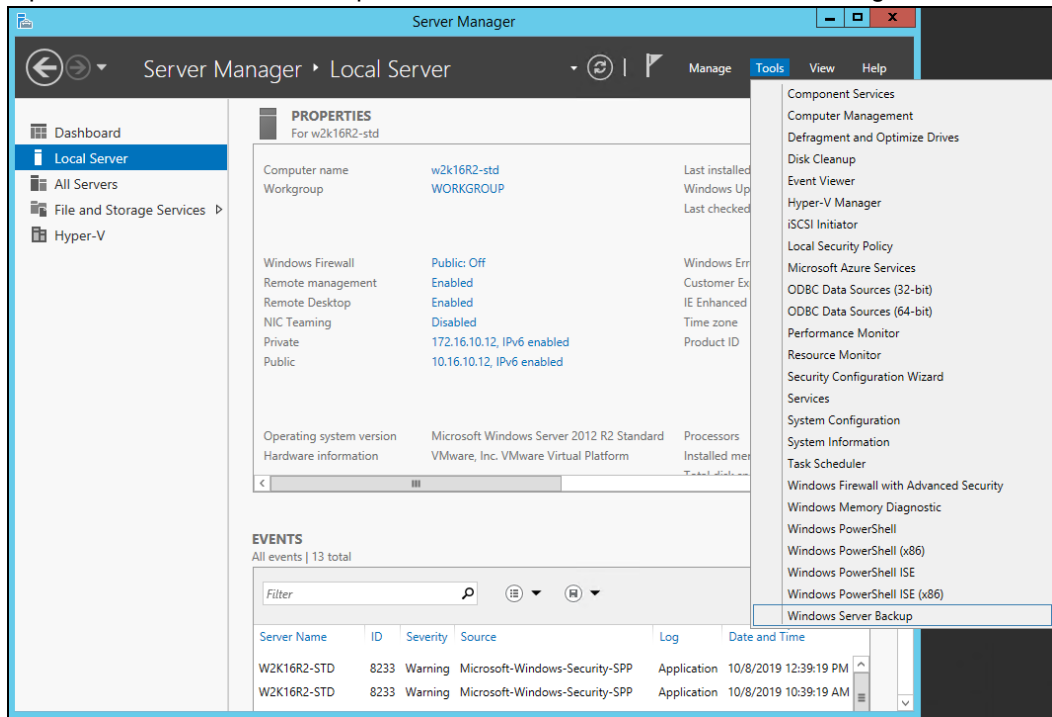




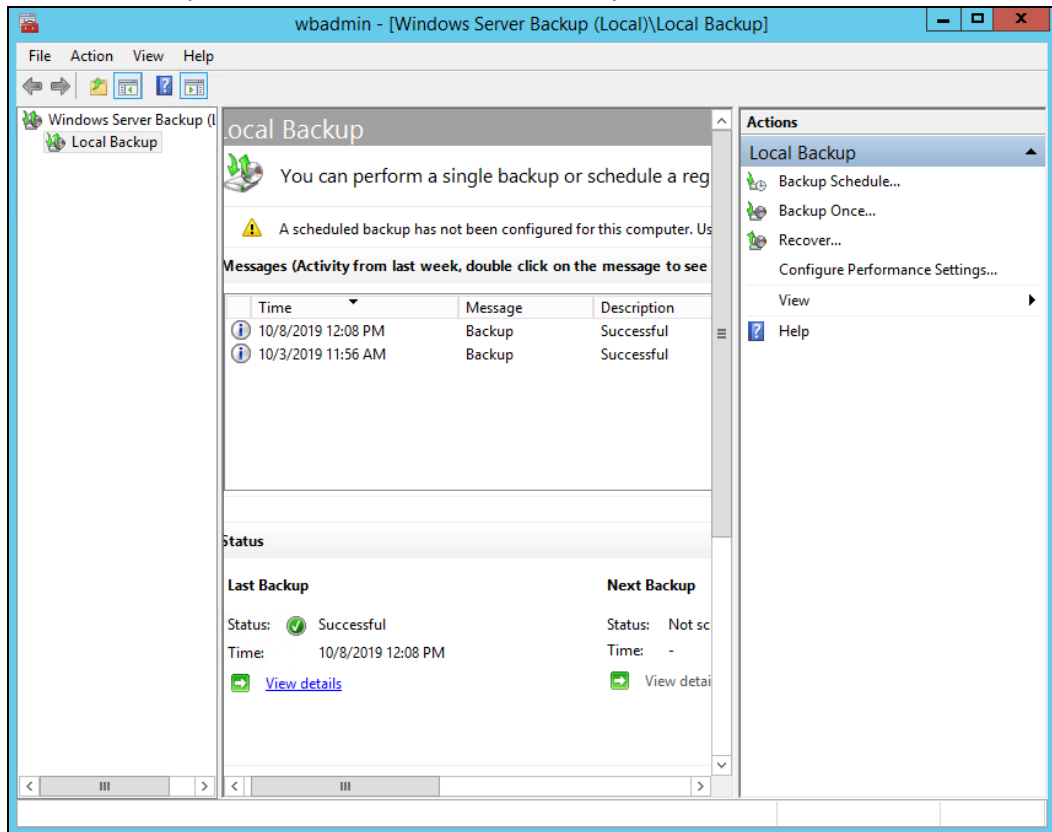
9.3.3 Recover Volumes

To recover volume using the Recovery Wizard in the Windows Server Backup user interface.

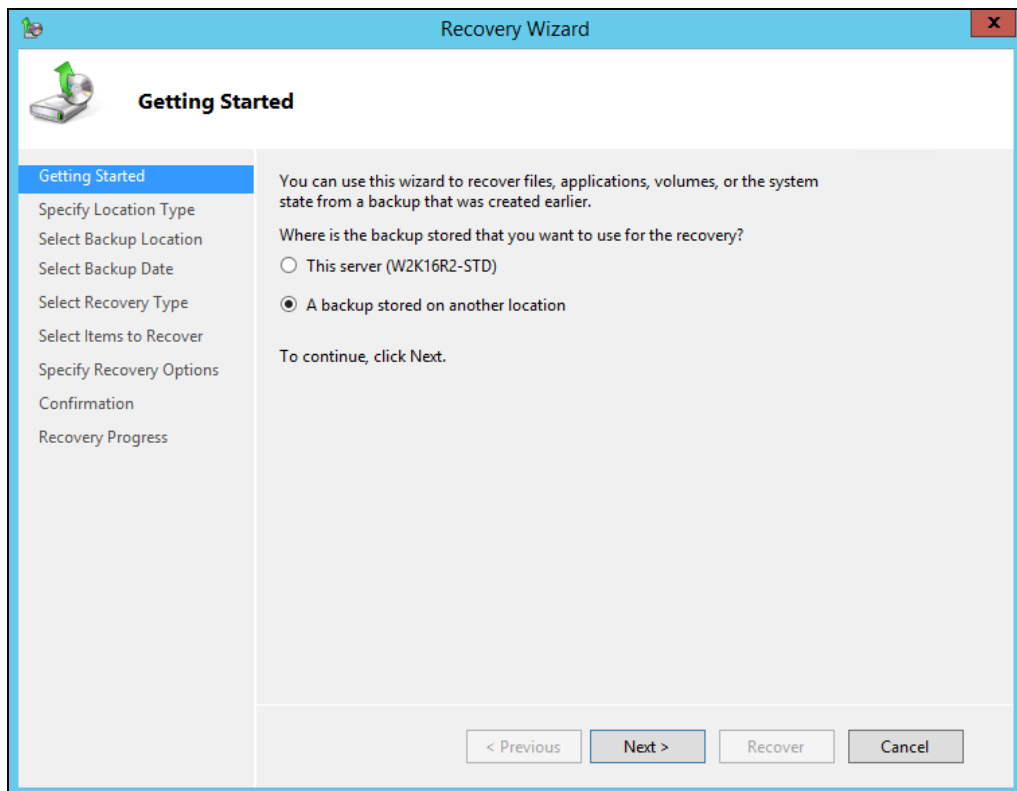
1. Open Windows Server Backup from Administrative Tools or Server Manager.



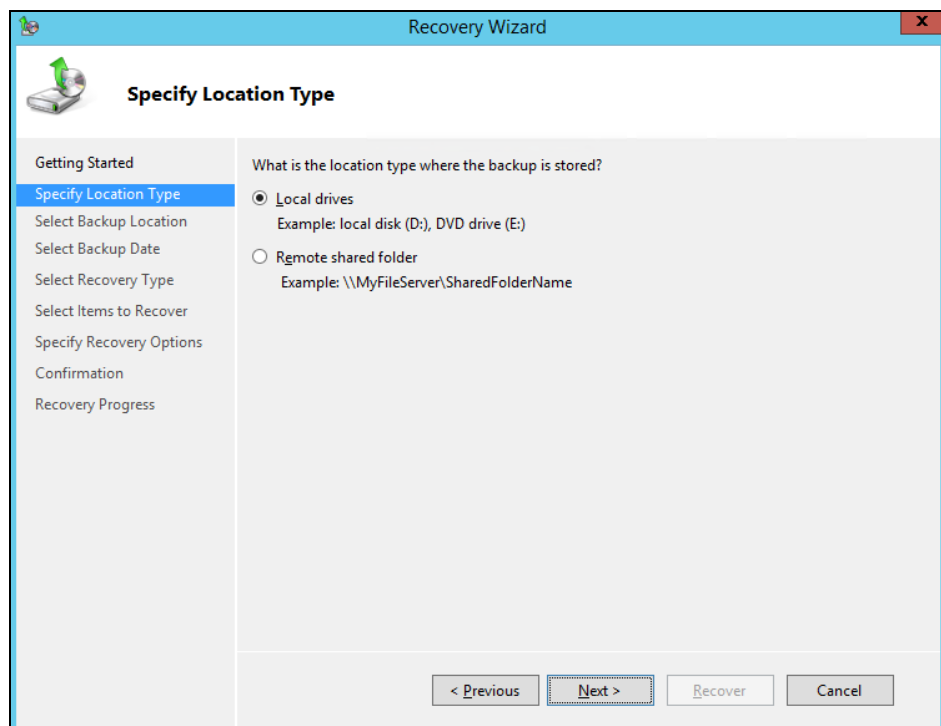
2. In the **Actions** panel under Windows Server Backup, click **Recover**.



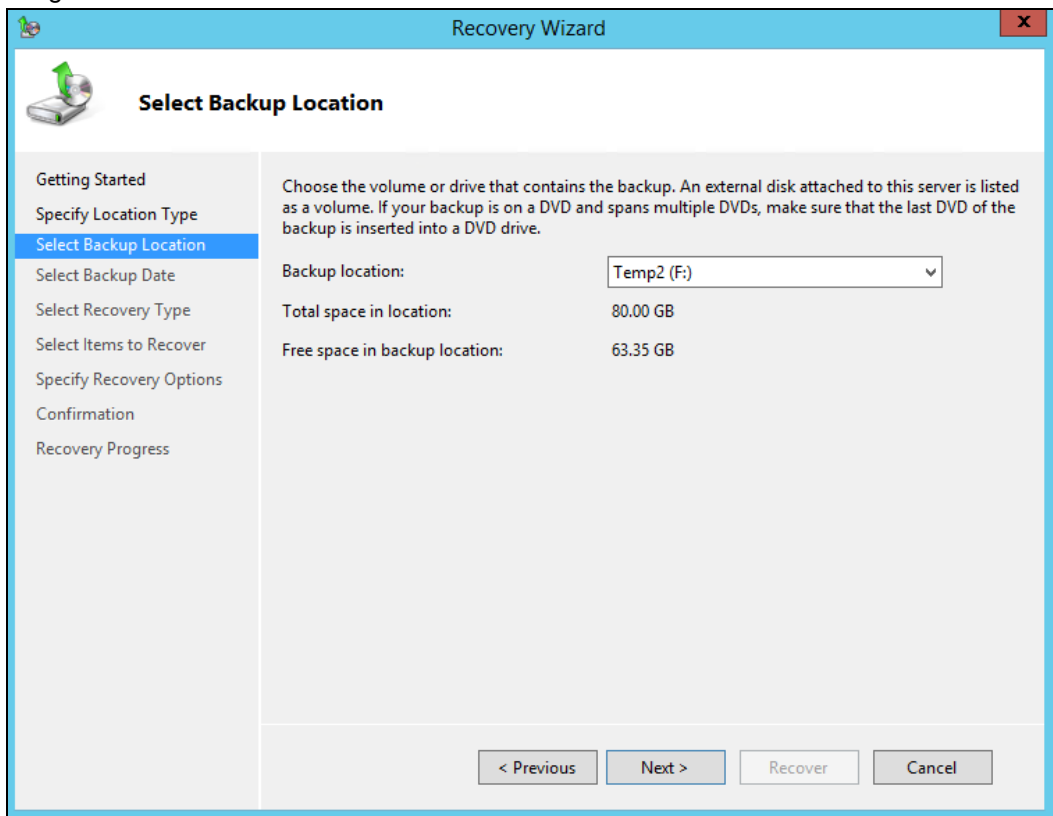
3. On the **Getting Started** page, select **A backup stored on another location**, then click **Next**.



4. On the **Specify Location Type** page, select
 - Click **Local drives** if the system image was copied to a local volume on the server.
 - Click **Remote shared folder**, if the system image was copied to a network path accessible to this server.

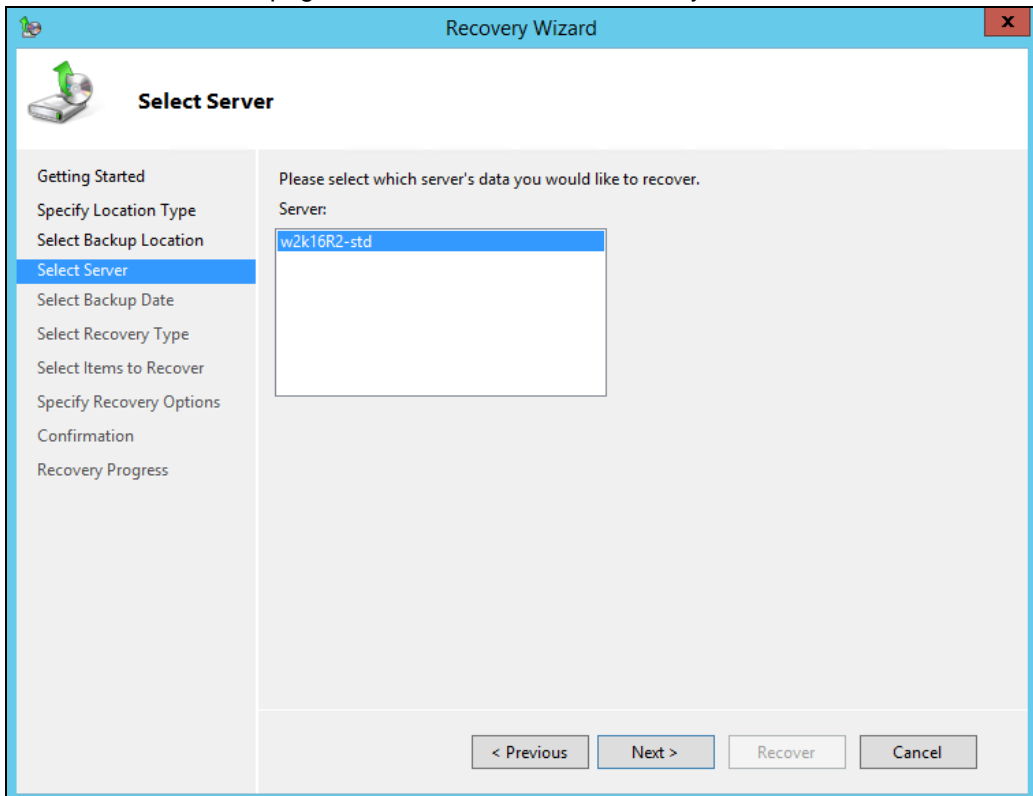


5. On the **Select Backup Location** page, select the volume that contains the system image file.

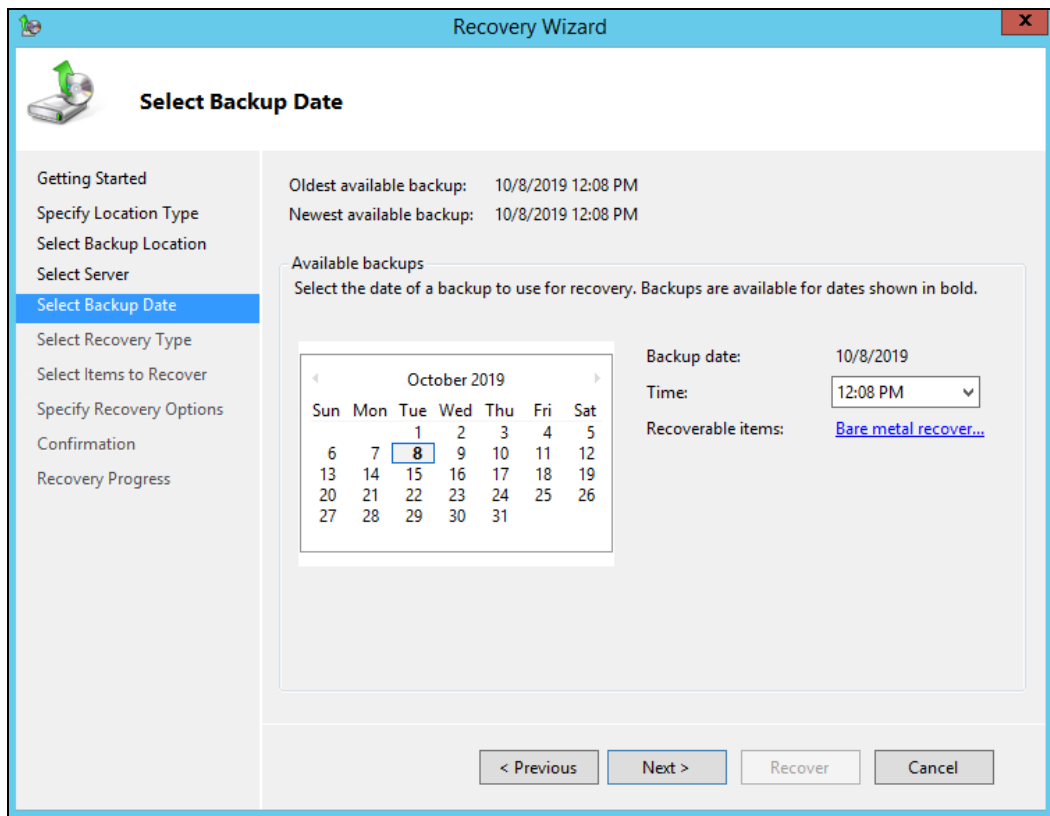


Note: Assuming that the *WindowsImageBackup* folder was copied to the following *F:\WindowsImageBackup*

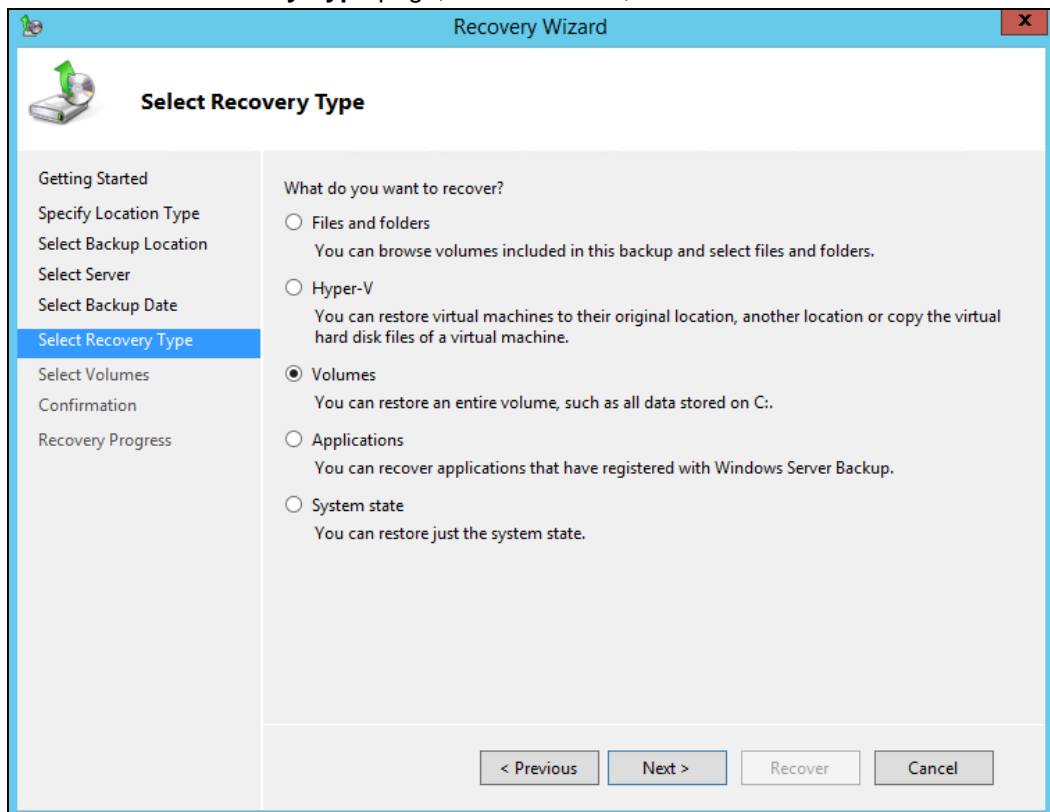
6. On the **Select Server** page, select the server whose data you want to recover.



- On the **Select Backup Date** page, select the point in time of the backup you want to restore from

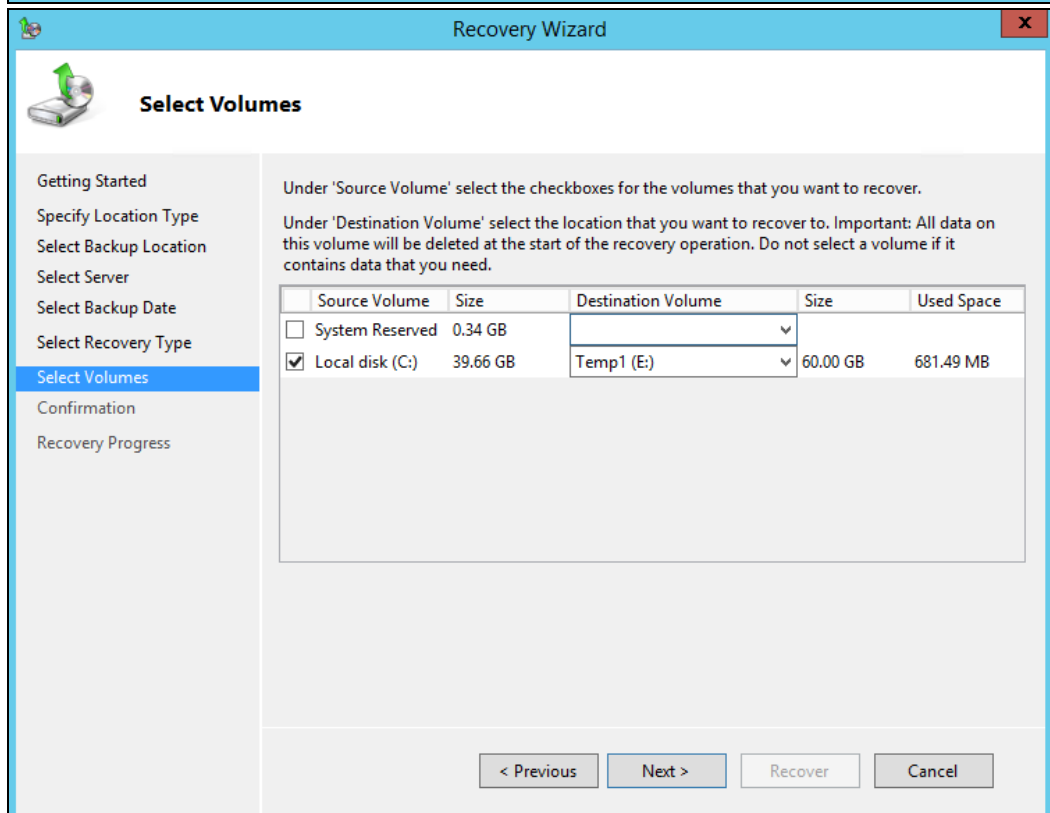
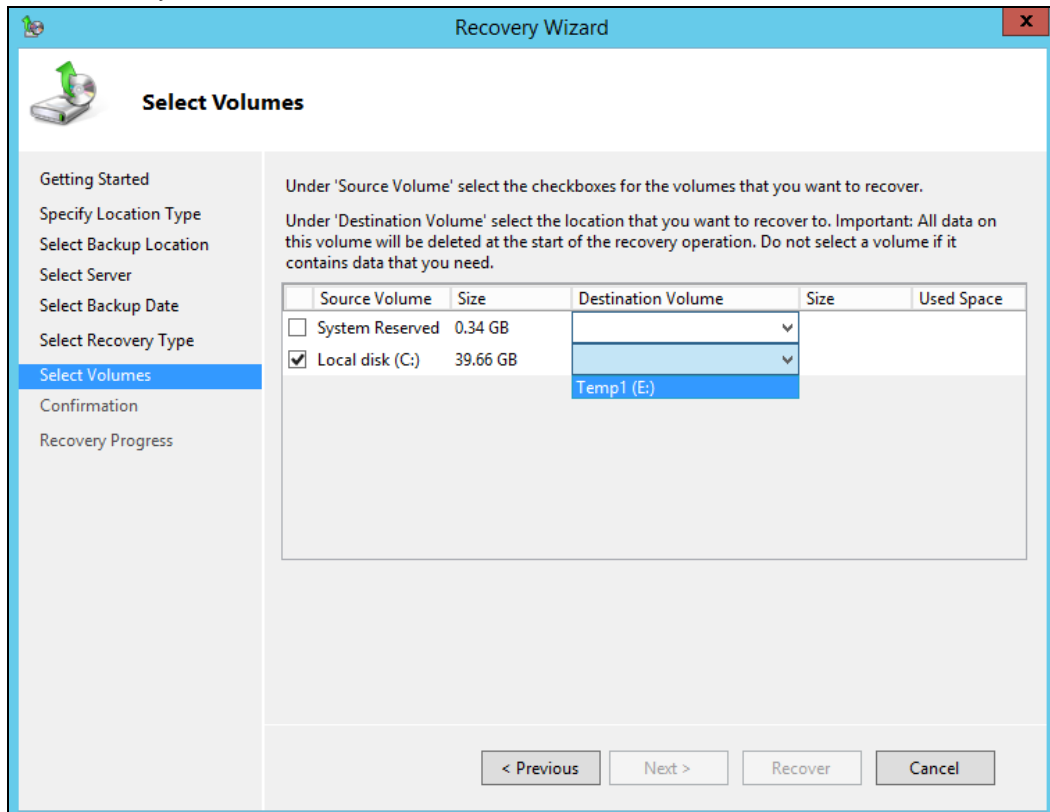


- On the **Select Recovery Type** page, click **Volumes**, and then click **Next**.

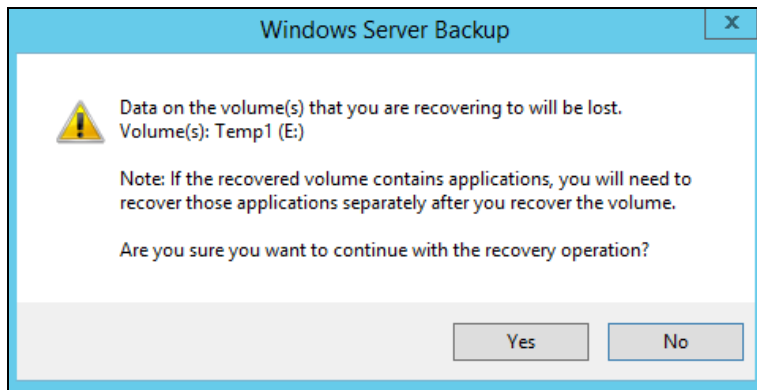


- On the **Select Volumes** page, select the check boxes associated with the volumes in the **Source Volume** column that you want to recover.

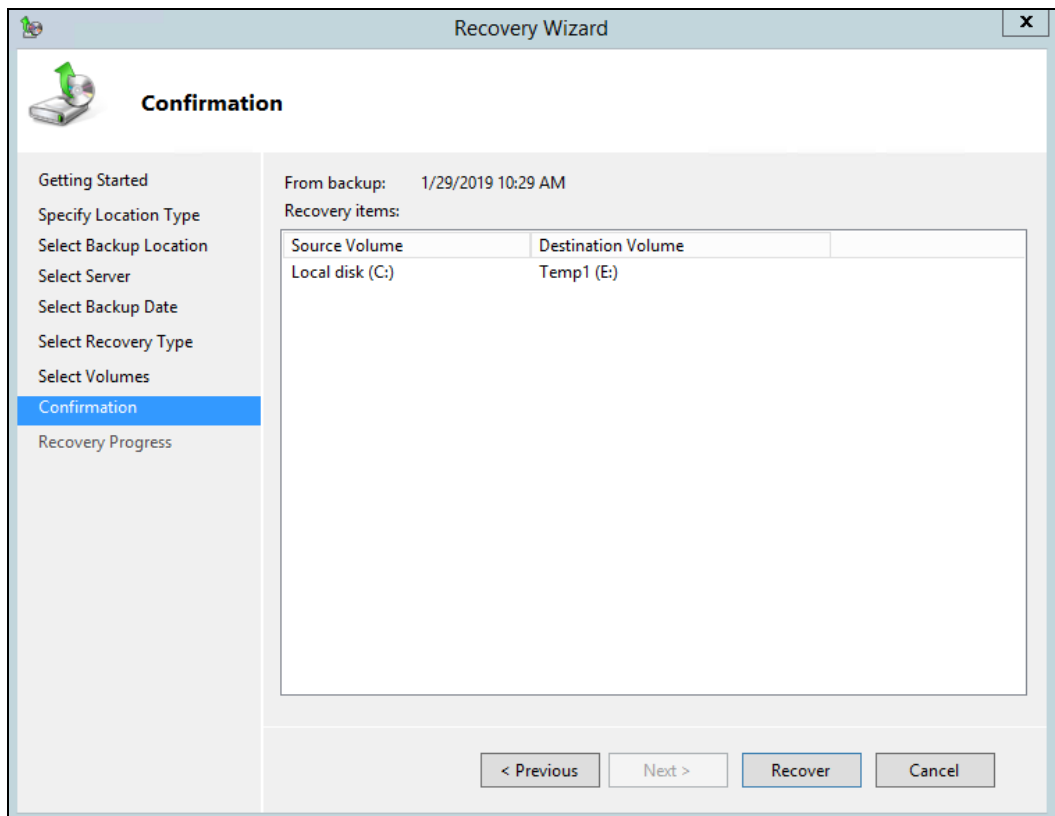
Then, from the associated dropdown list in the **Destination Volume** column, select the location that you want to recover the volume to.



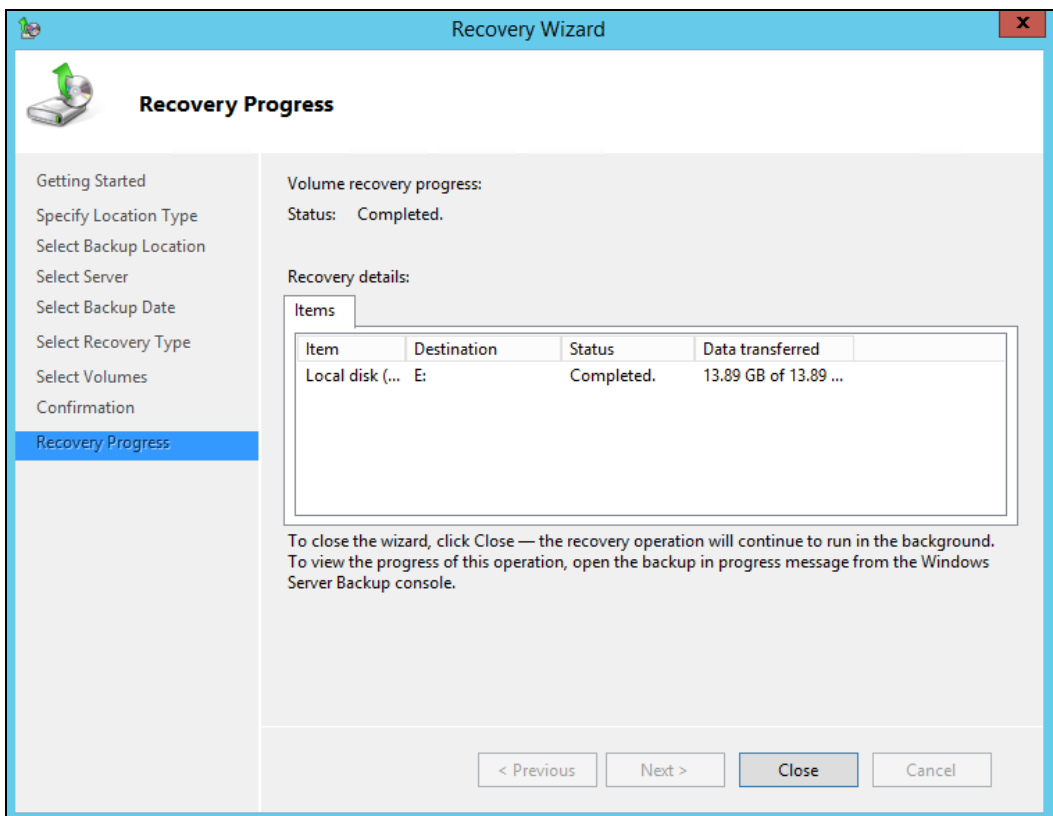
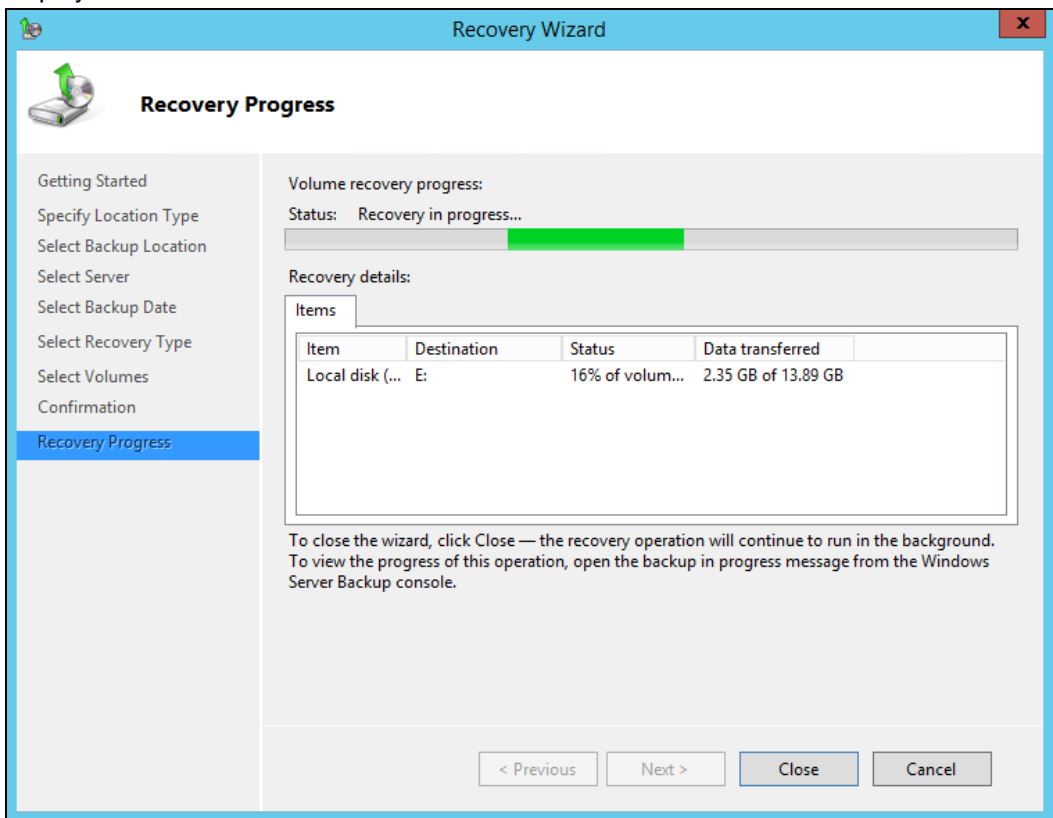
Important: Before clicking **Next** to continue, make sure that the destination volume is empty, or does not contain information that you will need later.



10. On the **Confirmation** page, review the details, and then click **Recover** to restore the volume.



- On the **Recovery progress** page, the status and result of the recovery operation is displayed.



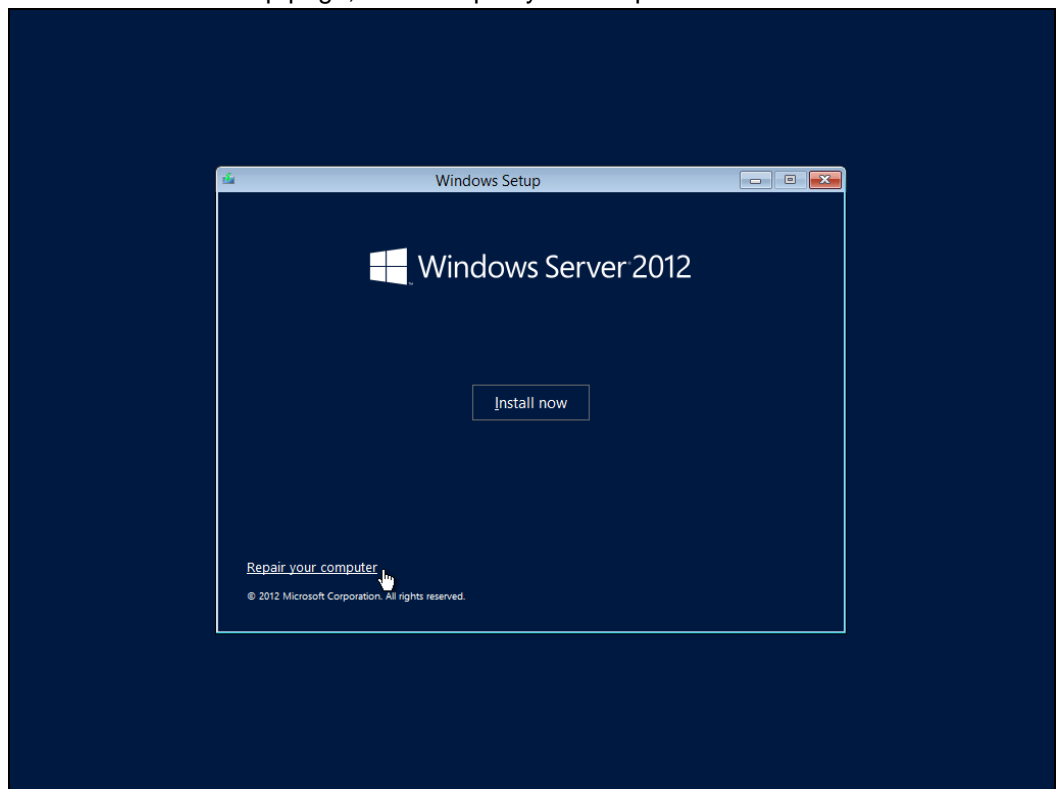
9.3.4 Recover Operating System or Full System

You can recover an operating system or full system by using Windows Recovery Environment, or by booting from a Windows setup disc.

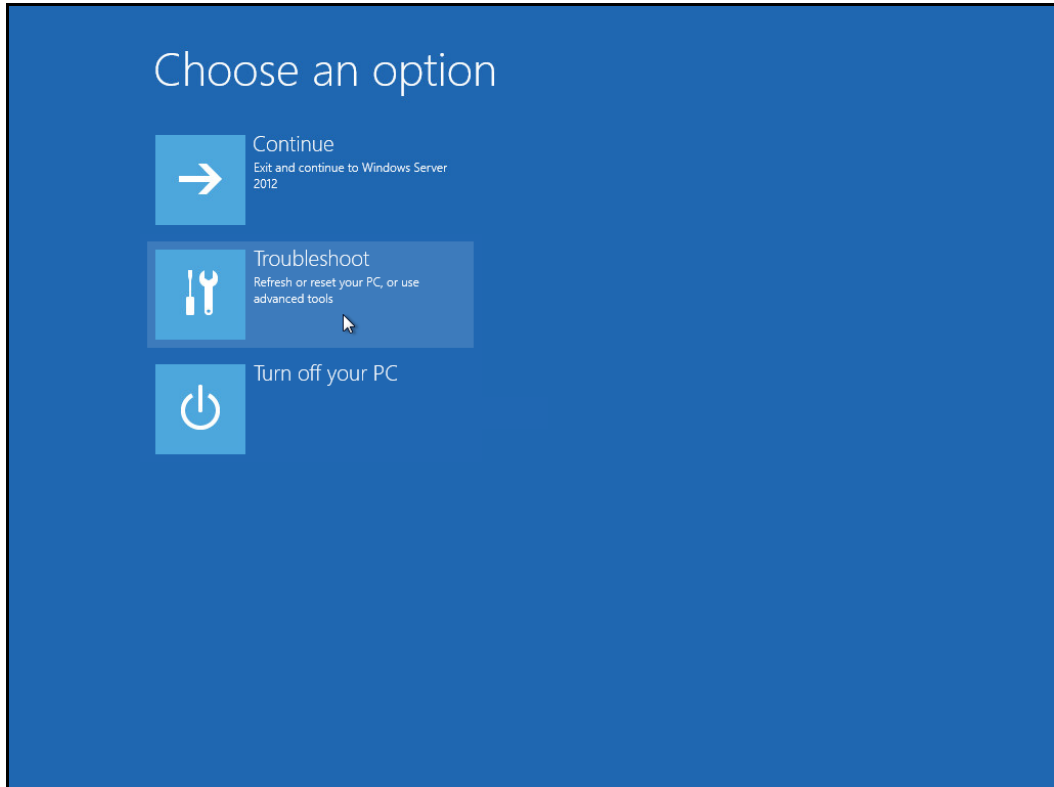
Note: For instructions specific to recovering Active Directory Domain Services, refer to the following: <http://go.microsoft.com/fwlink/?LinkId=143754>

To launch in Windows Recovery Environment, insert the Windows setup disc that has the same architecture of the system that you are recovering, into the CD / DVD drive and start or restart the computer. Press the required key to boot from the disc.

1. On the Windows Setup page, select Repair your computer.

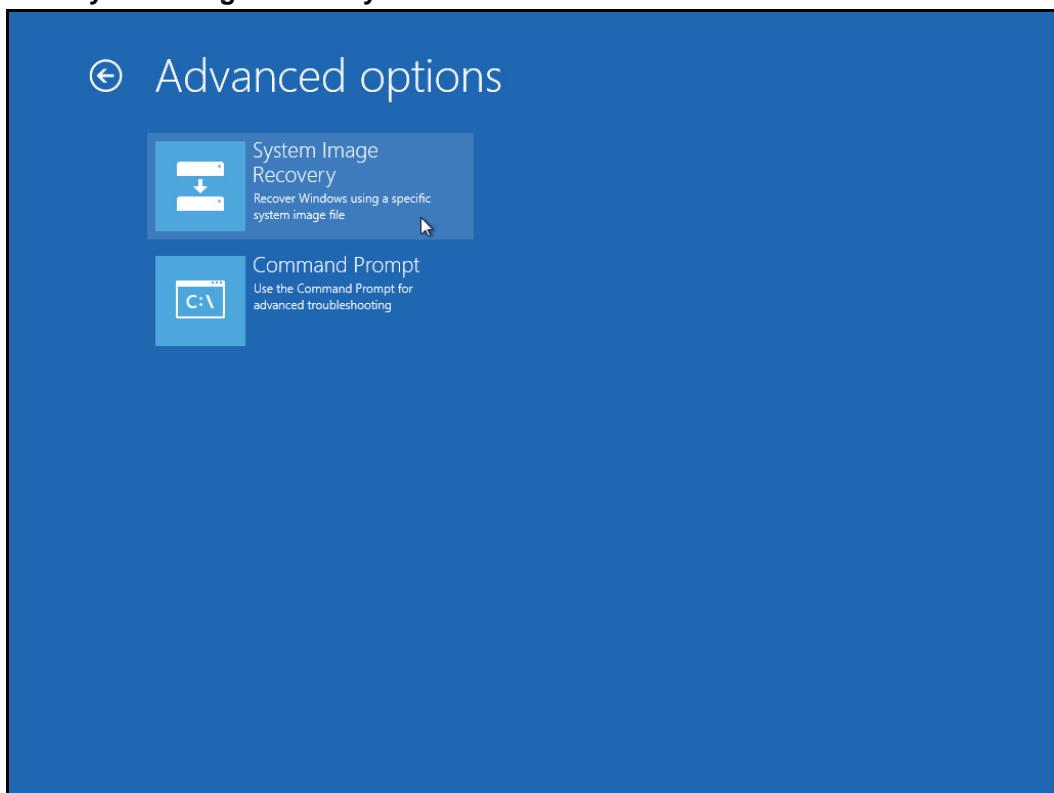


2. On the **Choose an option** page, click **Troubleshoot**.



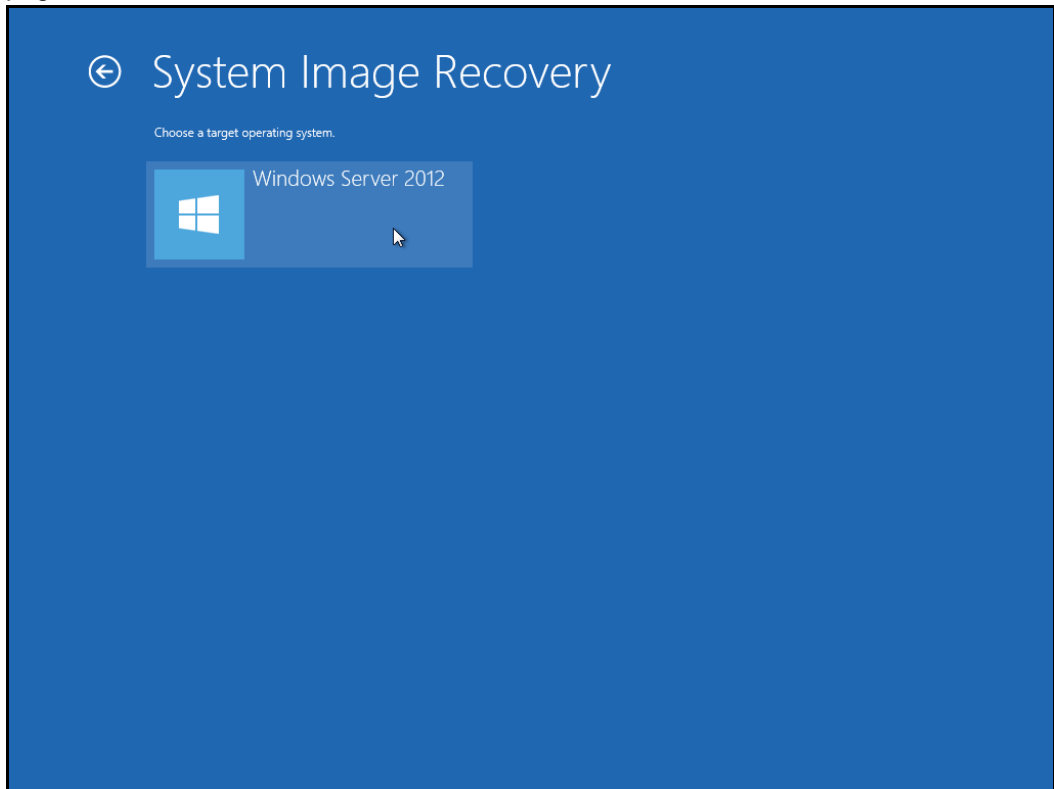
Note: This screen will only be displayed when you are recovering a Windows 2012 / 2012 R2 Server.

3. Click **System Image Recovery**.



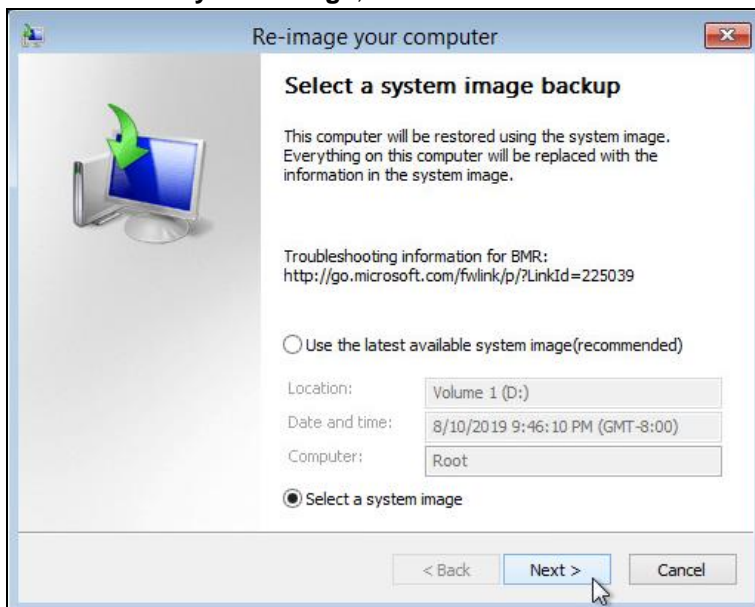
Note: This screen will only be displayed when you are recovering a Windows 2012 / 2012 R2 Server.

4. Confirm on the target operating system. This opens the **Re-image your computer** page.

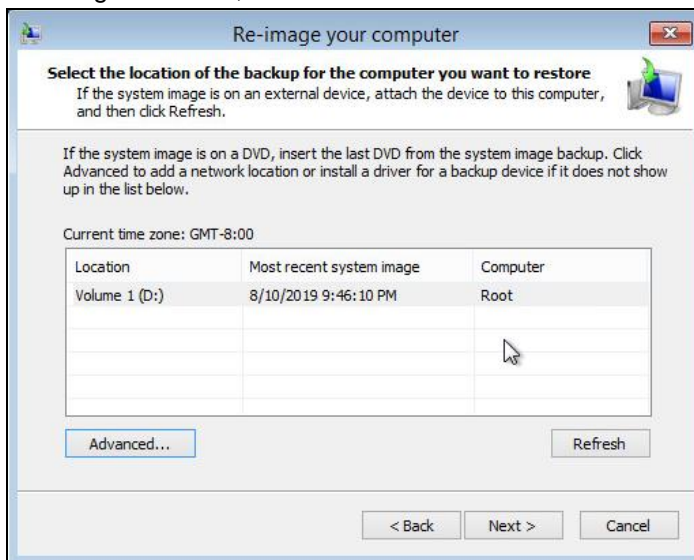


Note: This screen will only be displayed when you are recovering a Windows 2012 / 2012 R2 Server.

5. Click **Select a system image**, then click **Next**.



6. Select the location that contains the system image to restore from. If you do not see the image available, then



- Click **Advanced** and install the required driver for the removable drive to be accessed, if the system image was copied to a removable drive attached to the server.

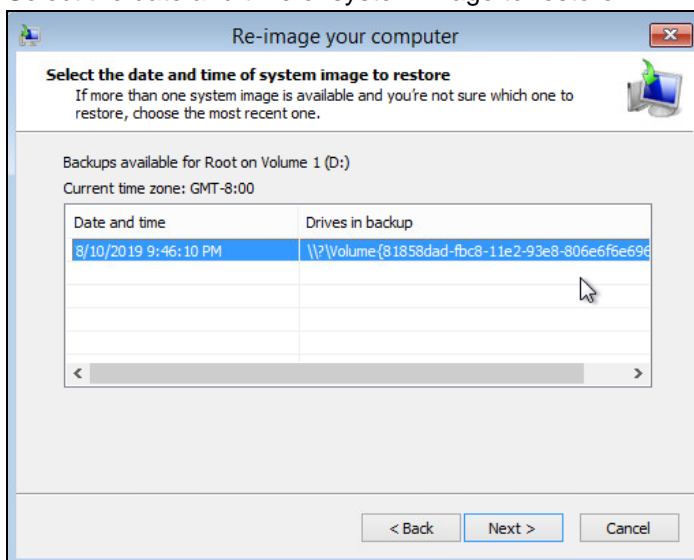
To install a driver, the driver must be located on the local system. You cannot install a driver from the network.

- Click **Advanced** and browse to the remote shared folder which contains the system image if the system image was copied to a network path.

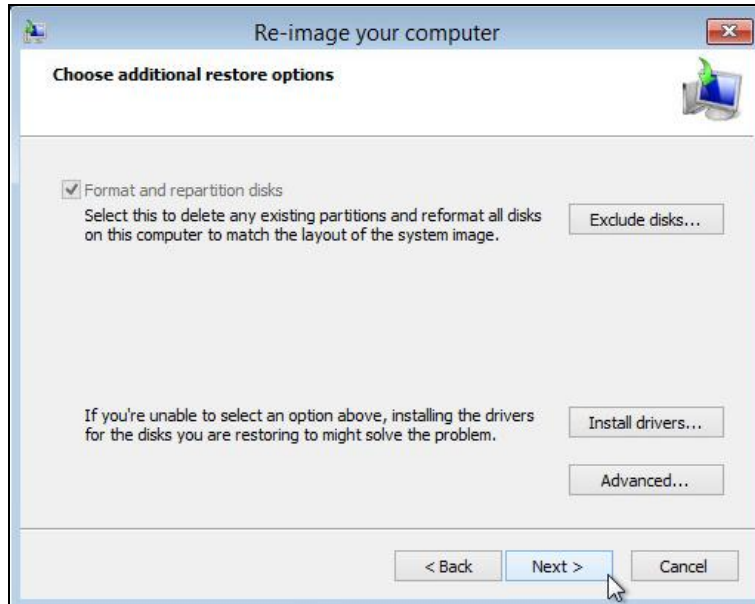
For domain environment, if the backup storage location is on a computer that is a member of that domain, then the computer containing the storage location should be on the IPsec boundary, to be accessible by non-domain computer.

When a computer boots into Windows Recovery Environment, it becomes a non-domain computer, therefore, cannot access the usual network shares. Only those computers that allow non-domain computers to access the share can be used as a backup storage location in this way.

7. Select the date and time of system image to restore.

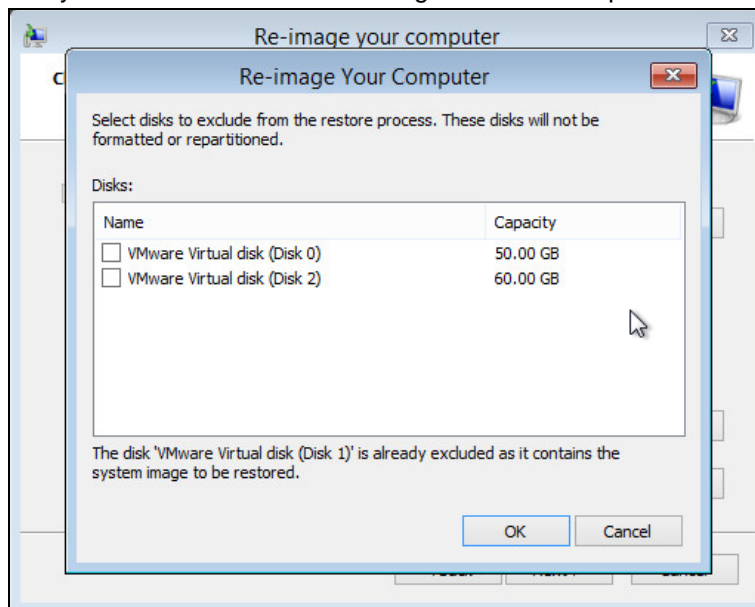


8. On the **Choose additional restore options** page



Select the **Format and repartition disks** check box to delete existing partitions and reformat the destination disks to be the same as the backup.

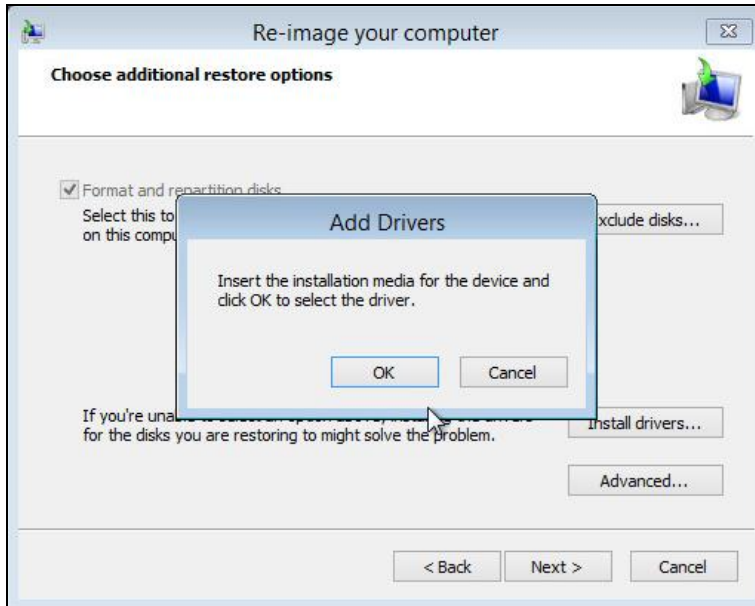
Click the **Exclude disks** button, then select the check boxes associated with any disks that you want to exclude from being formatted and partitioned.



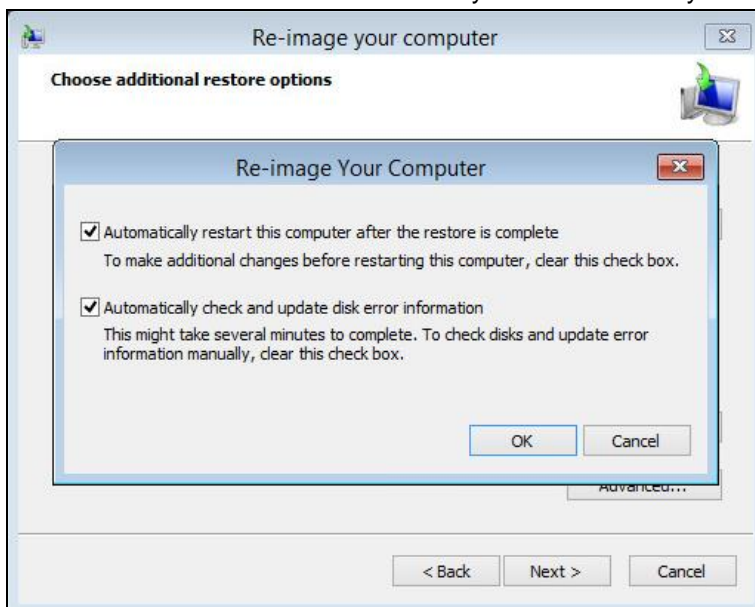
Note: The disk that contains the backup that you are using is automatically excluded.

Select the **Only restore system drives** check box (not displayed in screenshot) to perform an operating system only recovery (instead of a full system recovery).

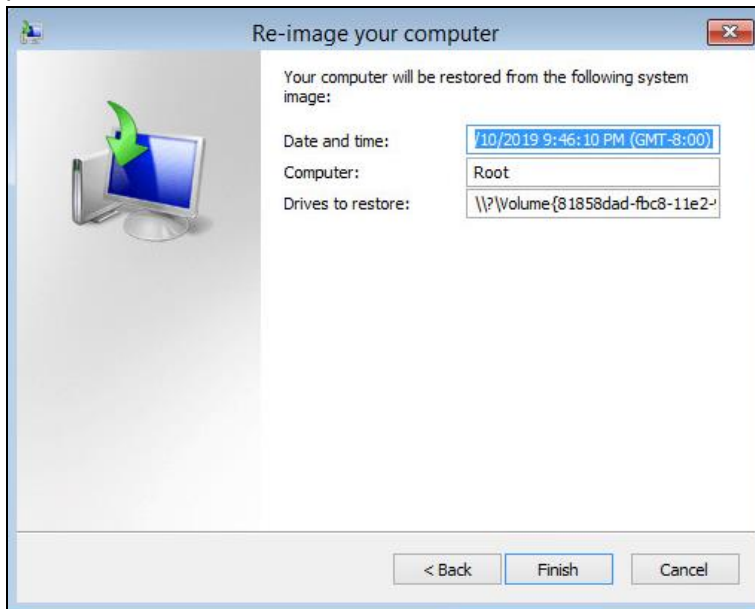
Click **Install drivers** to install device drivers for the hardware that you are recovering to.



Click **Advanced** to specify whether the computer is automatically restarted, and the disks are checked for errors immediately after the recovery.



9. Confirm the details for the restoration, and then click **Finish** to start the recovery process.



The recovery will succeed as long as all the critical volumes (e.g. volumes containing operating system components) are recovered.

If any data volume cannot be recovered, Windows will show a prompt with the unrecoverable volumes at the end of the recovery operation.

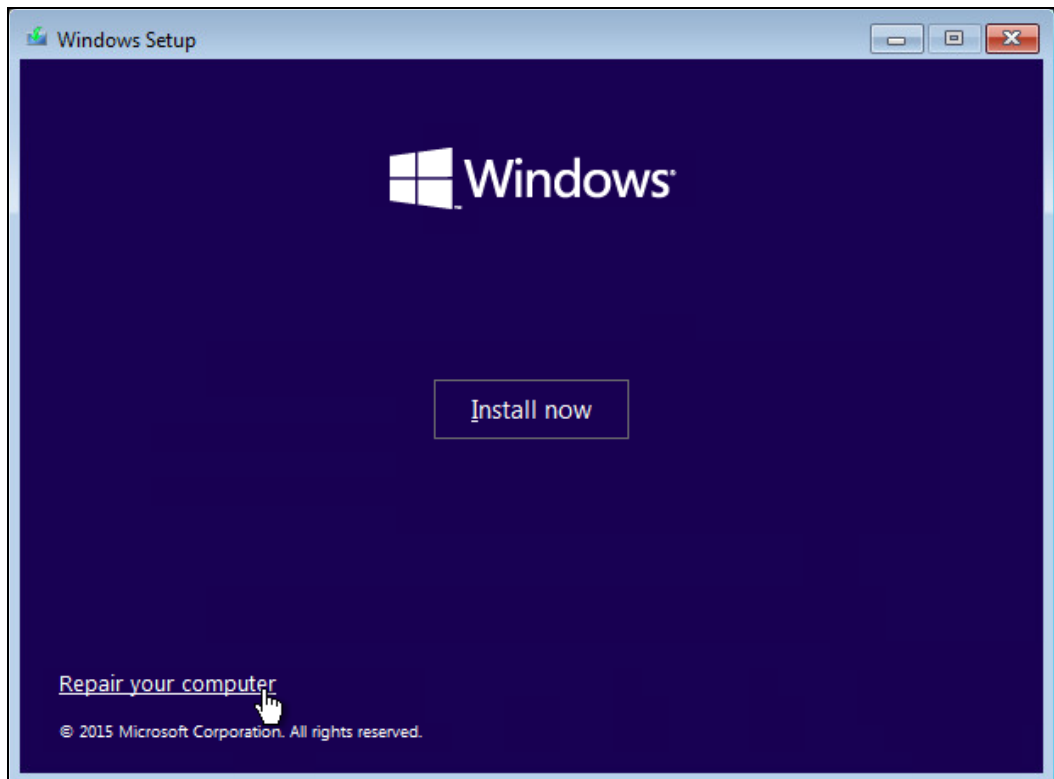
9.3.5 Recover a Full System (Non Server Platforms)

You can recover a full system using the advanced startup option by

- ▶ Booting from a Windows installation media

Insert the installation media that has the same architecture of the system that you are recovering and restart your computer. Press the required key to boot from the disc.

When you see the **Windows Setup** page, click **Next**, then click **Repair your computer**.

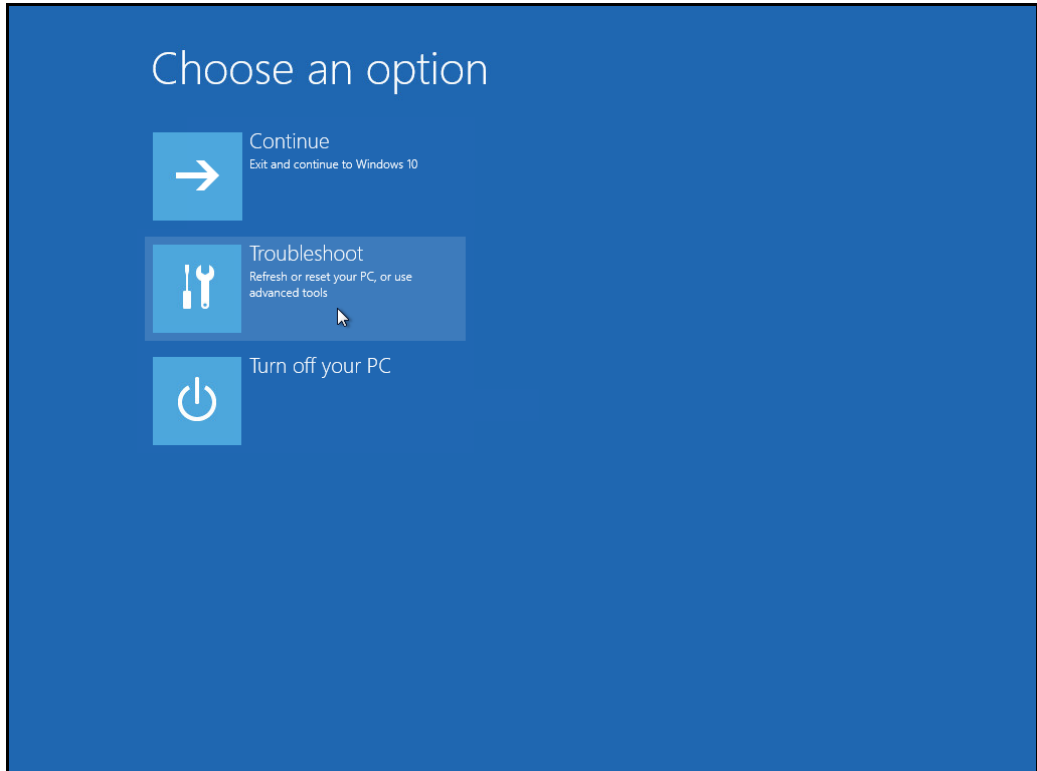


- ▶ Starting Windows in safe mode

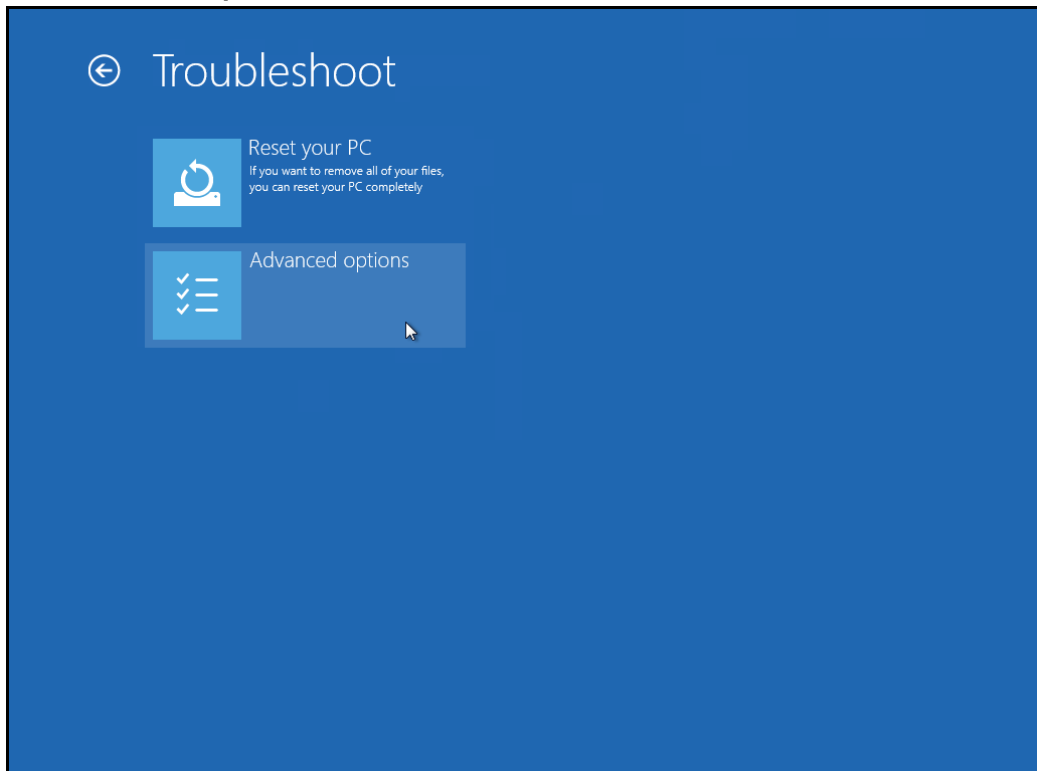
Press the **Power** button at the Windows login screen, in the Start menu, or in the Setting screen. Then press and hold the SHIFT key on the keyboard and click **Restart**.

Once you are in the Startup Option menu, perform the following steps.

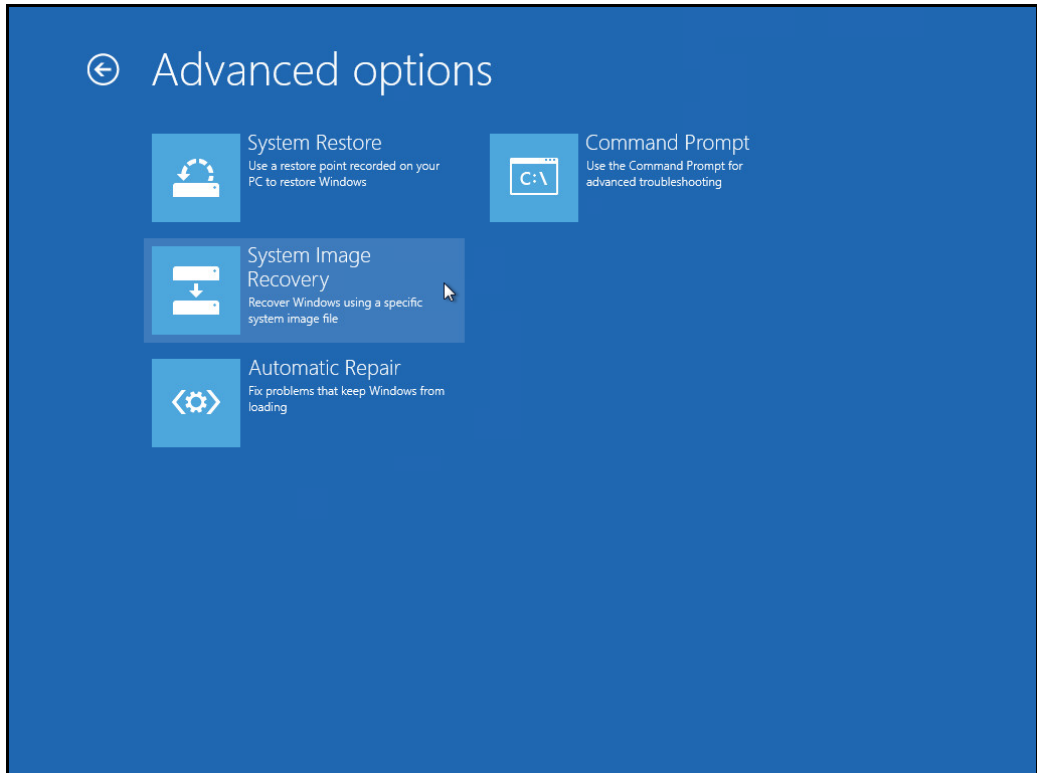
1. Click **Troubleshoot**.



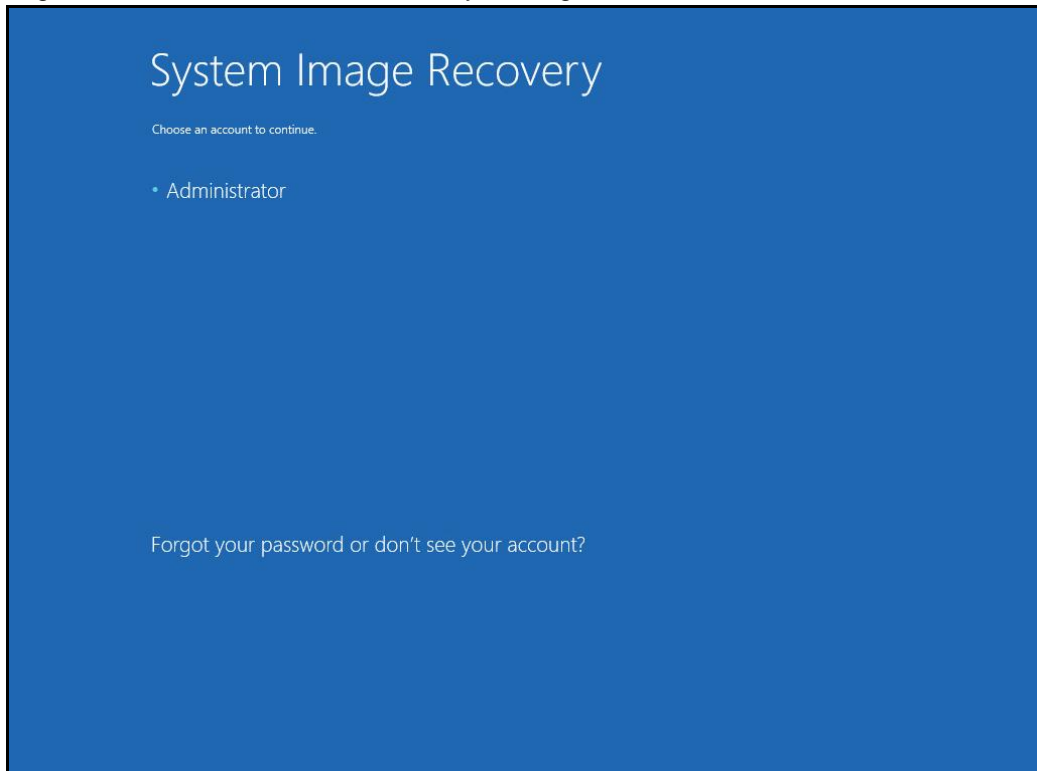
2. Click **Advanced options**.



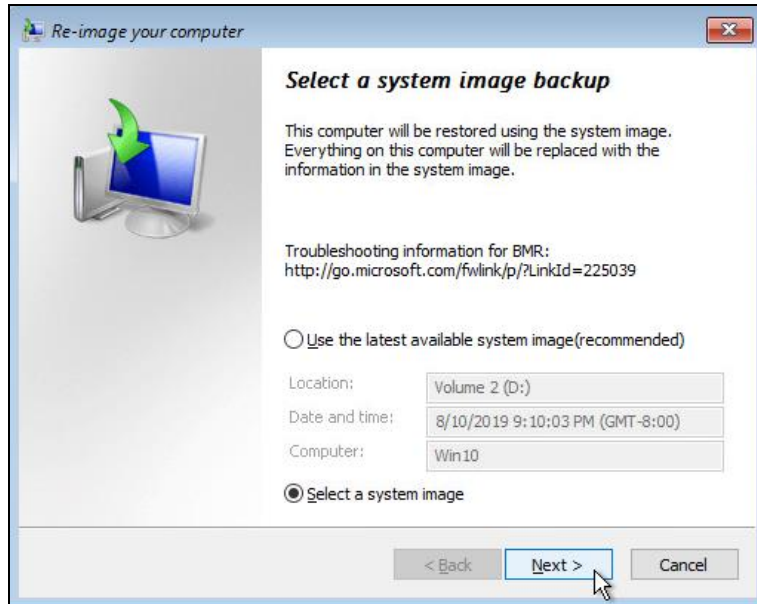
3. Click **System Image Recovery**.



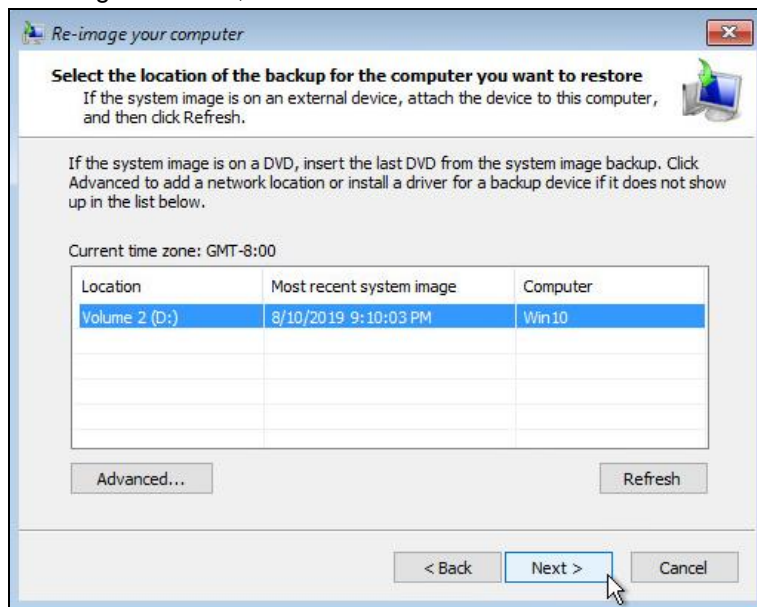
4. Login with an administrative account, by clicking on **Administrator**.



- Click **Select a system image**, then click **Next**.



- Select the location that contains the system image to restore from. If you do not see the image available, then



- Click **Advanced** and install the required driver for the removable drive to be accessed, if the system image was copied to a removable drive attached to the server.

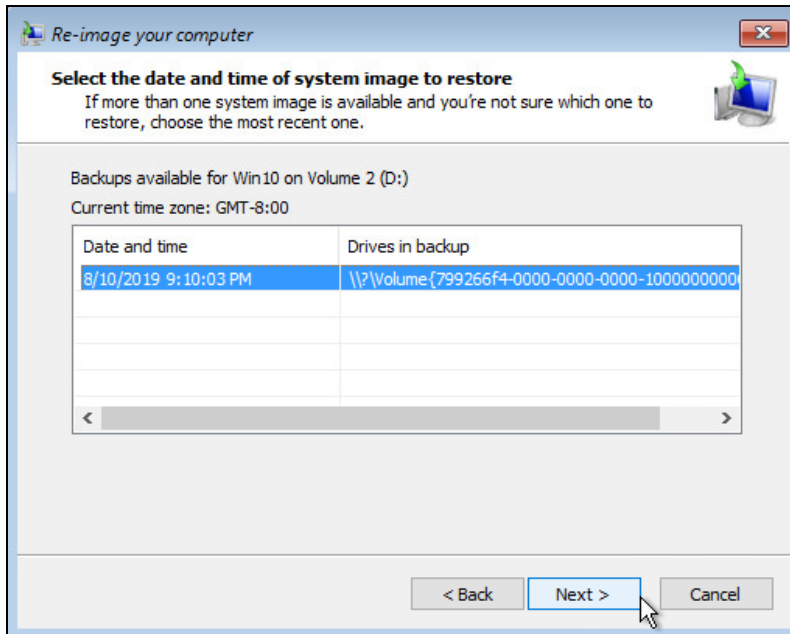
To install a driver, the driver must be located on the local system. You cannot install a driver from the network.

- Click **Advanced** and browse to the remote shared folder which contains the system image if the system image was copied to a network path.

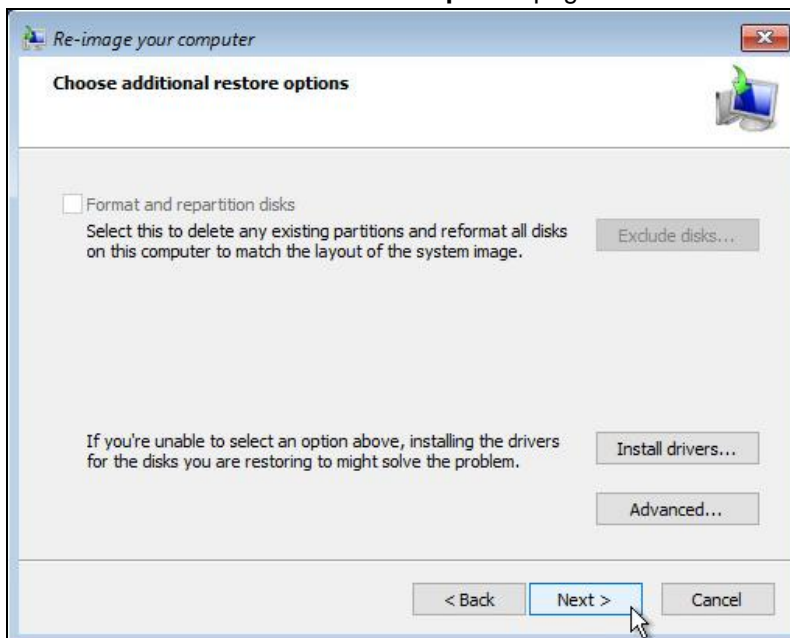
For domain environment, if the backup storage location is on a computer that is a member of that domain, then the computer containing the storage location should be on the IPsec boundary, to be accessible by non-domain computer.

When a computer boots into Windows Recovery Environment, it becomes a non-domain computer, therefore, cannot access the usual network shares. Only those computers that allow non-domain computers to access the share can be used as a backup storage location in this way.

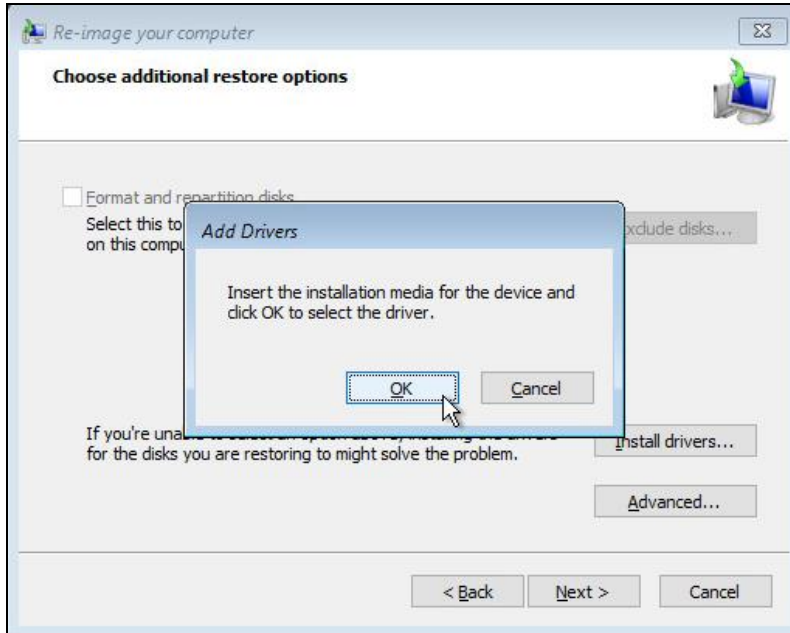
7. Select the date and time of system image to restore.



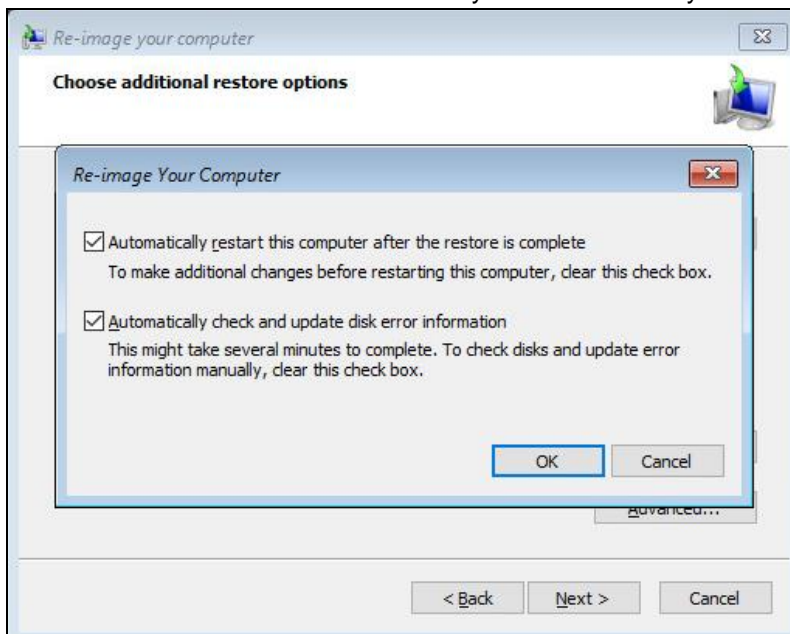
8. On the **Choose additional restore options** page.



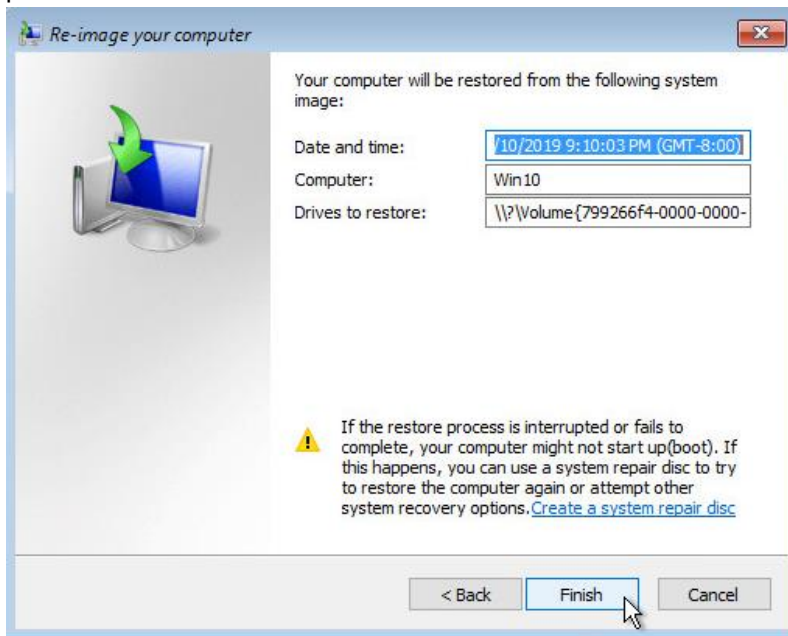
Click **Install drivers** to install device drivers for the hardware that you are recovering to.



Click **Advanced** to specify whether the computer is automatically restarted, and the disks are checked for errors immediately after the recovery.



9. Confirm the details for the restoration, and then click **Finish** to start the recovery process.



Important: Do not interrupt the restore process.

The recovery will succeed as long as all the critical volumes (e.g. volumes containing operating system components) are recovered.

10 Contact Ahsay

10.1 Technical Assistance

To contact Ahsay support representatives for technical assistance, visit the Partner Portal:
<https://www.ahsay.com/partners/>

Also use the Ahsay Wikipedia for resource such as Hardware Compatibility List, Software Compatibility List, and other product information:
<https://wiki.ahsay.com/>

10.2 Documentation

Documentations for all Ahsay products are available at:
https://www.ahsay.com/jsp/en/downloads/ahsay-downloads_documentation_guides.jsp

You can send us suggestions for improvements or report on issues in the documentation by contacting us at:
<https://www.ahsay.com/partners/>

Please specify the specific document title as well as the change required/suggestion when contacting us.

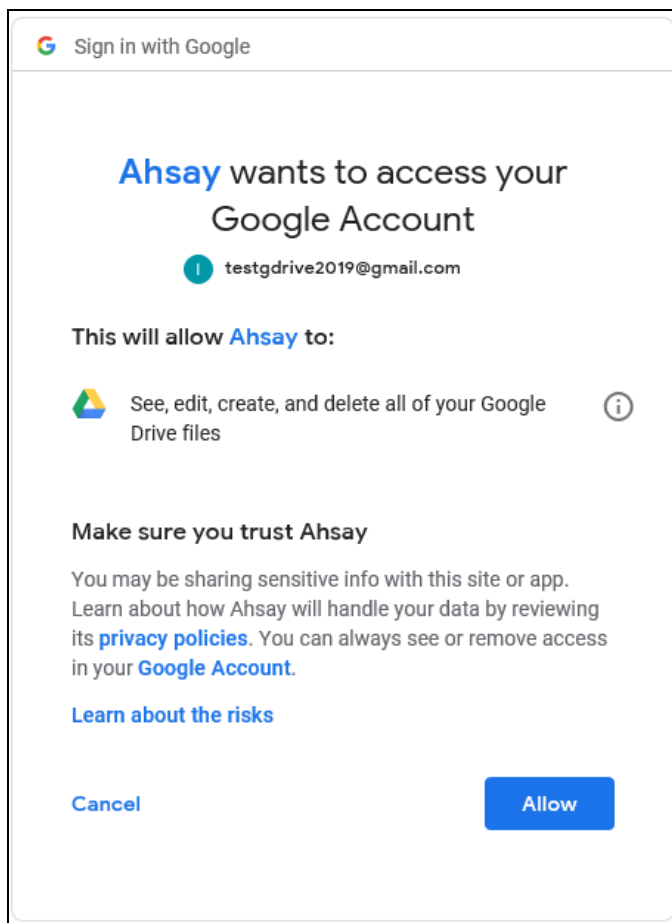
Appendix

Appendix A Cloud Storage as Backup Destination:

For most cloud storage provider (e.g. Dropbox, Google Drive ... etc.), you need to allow AhsayOBM to access the cloud destination. Click OK / Test, you will be prompted to login to the corresponding cloud service.

Important: The authentication request will be opened in a new tab / window on the browser, ensure that the pop-up tab / window is not blocked (e.g. pop-up blocker in your browser).

Click Allow to permit AhsayOBM to access the cloud storage:



Enter the authentication code returned in AhsayOBM to complete the destination setup.

Note: A backup destination can be set to a supported cloud storage, backup server, FTP / SFTP server, network storage, or local / removable drive on your computer.

Multiple backup destinations can be configured for a single backup set. In fact, it is recommended for you to setup at least 2 backup destinations for your backup set.

For more details on backup destination, for example which cloud service providers are supported, destination type, or limitation, you can refer to this link:

[FAQ: Frequently Asked Questions on Backup Destination](#)