

# **Ahsay Online Backup Manager v9**

## **Microsoft System State Backup and Restore Guide**

Ahsay Systems Corporation Limited

**27 January 2023**

# Copyright Notice

© 2023 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 (<http://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, Oracle Database, Java and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

OpenJDK is a registered trademark of Oracle America, Inc.

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](http://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.

Debian is a registered trademark of Software in the Public Interest, Inc.

Rocky is a registered trademark of Rocky Brands.

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	Version
25 January 2022	<ul style="list-style-type: none"><li>▪ Ch 1.2 – modified the system architecture diagram</li><li>▪ Ch. 2, 3, 4, &amp; 5 – updated the screenshots</li><li>▪ Ch. 2, 4, &amp; Appendix – updated the links</li></ul>	9.1.0.0
7 March 2022	<ul style="list-style-type: none"><li>▪ Ch 4.1 – updated note for Migrate Data</li></ul>	9.1.0.0
21 April 2022	<ul style="list-style-type: none"><li>▪ Ch 2.2 – updated the software requirement</li><li>▪ Ch. 4 &amp; 5 – updated the screenshots</li></ul>	9.1.2.43
27 January 2023	<ul style="list-style-type: none"><li>▪ Ch. 5.1 – updated restore instructions</li></ul>	9.5.2.0

# Table of Contents

<b>1</b>	<b>Overview.....</b>	<b>1</b>
1.1	What is this software? .....	1
1.2	System Architecture .....	2
<b>2</b>	<b>Preparing for Backup and Restore.....</b>	<b>3</b>
2.1	Hardware Requirement .....	3
2.2	Software Requirement.....	3
2.3	Antivirus Exclusion Requirement .....	3
2.4	AhsayOBM Installation .....	3
2.5	AhsayOBM Add-on Module Configuration .....	3
2.6	Backup Quota Requirement .....	4
2.7	Java Heap Size .....	4
2.8	License Requirement.....	4
2.9	Windows Requirements.....	5
2.10	Temporary Volume .....	6
2.11	Best Practices and Recommendations .....	8
2.12	Restore Considerations .....	11
<b>3</b>	<b>Configuring a MS Windows System Backup Set .....</b>	<b>12</b>
3.1	Configuring an MS Windows System State Backup Set .....	12
<b>4</b>	<b>Running a Backup .....</b>	<b>22</b>
4.1	Start a Manual Backup .....	22
4.2	Configure Backup Schedule for Automated Backup .....	25
<b>5</b>	<b>Restore with a Microsoft Windows System Backup Set .....</b>	<b>31</b>
5.1	Restore the System State Data .....	31
5.2	Apply the System State Data.....	37
<b>6</b>	<b>Contact Ahsay.....</b>	<b>46</b>
6.1	Technical Assistance.....	46
6.2	Documentation .....	46
	<b>Appendix.....</b>	<b>47</b>
	Appendix A Cloud Storage as Backup Destination: .....	47

# 1 Overview

## 1.1 What is this software?

Ahsay brings you specialized client backup software, namely AhsayOBM, to provide a set of tools to protect your Microsoft System State. This includes backup feature, that leverages Microsoft's native WBAdmin command-line tool (<http://go.microsoft.com/fwlink/?LinkId=140216>) for Windows Server 2008 and newer releases, and recovery feature.

System state backup and restore operations include all system state data, and you cannot choose to backup or restore individual components due to dependencies among the system state components.

System state data is comprised of the following files:

- Boot files, including the system files, and all files protected by Windows File Protection (WFP)
- Active Directory (on a domain controller only)
- SYSVOL (on a domain controller only)
- Certificate Services (on certification authority only)
- Cluster database (on a cluster node only)
- Component Services Class registration database
- Performance counter configuration information
- Microsoft Internet Information Services (IIS) meta directory (on an IIS server only)
- Registry

The size of a set of system state backup data is dependent on the role installed on the server.

Please refer to the following article for more details:

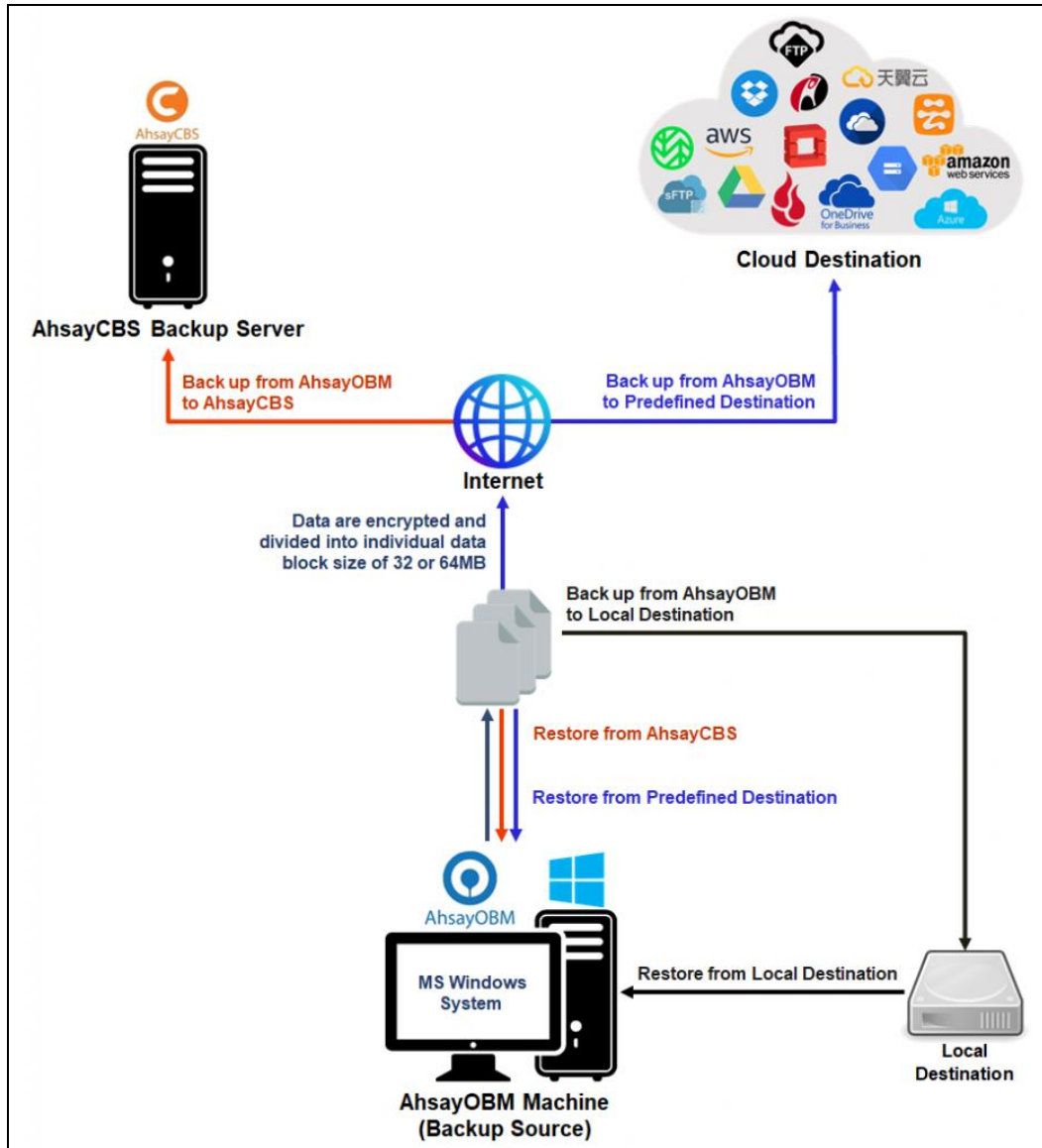
For Windows 2008 and newer releases:

<https://msdn.microsoft.com/en-us/library/windows/desktop/bb968830>

## 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 State 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 of MS Windows System State using the AhsayOBM as a client backup software.



## 2 Preparing for Backup and Restore

### 2.1 Hardware Requirement

To achieve the optimal performance when AhsayOBM is running on your machine, refer to the following link for the list of hardware requirements for AhsayOBM:

[FAQ: Ahsay Hardware Requirement List \(HRL\) for version 9.1 or above](#)

### 2.2 Software Requirement

Make sure the operating system where you need the Windows System State to be backed up is compatible with the AhsayOBM. Refer to the following link for the list of compatible operating systems and application versions.

[FAQ: Ahsay Software Compatibility List \(SCL\) for version 9.1 or above](#)

#### NOTE

OBM v9 support for System State recovery will need OBM v9.1.2.42 or later, earlier v9 versions are not supported.

### 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 State Backup** add-on module is enabled in your AhsayOBM user account. Please contact your service provider for more details.

The screenshot shows the AhsayOBM configuration interface. On the left is a sidebar with navigation links: User Profile, Backup Set, Settings, Report, Statistics, and Effective Policy. The main area has tabs for General, Backup Client Settings, Contact, User Group, Authentication, and Mobile Backup. The 'Backup Client Settings' tab is active, showing 'Backup Client' options (AhsayOBM User selected, AhsayACB User unselected) and a list of 'Add-on Modules'. The 'Windows System State Backup' module is checked and highlighted with a red box. Other modules include Microsoft Exchange Server, MySQL Database Server, Lotus Domino, Windows System Backup, VMware, Microsoft Exchange Mailbox, NAS - QNAP, Mobile (max. 10), Volume Shadow Copy, OpenDirect / Granular Restore, MariaDB Database Server, Microsoft SQL Server, Oracle Database Server, Lotus Notes, Hyper-V, ShadowProtect System Backup, NAS - Synology, Continuous Data Protection, In-File DeltaOnly apply to v8 or before, Office 365 Backup, and Deduplication.

## 2.6 Backup Quota Requirement

Make sure that your AhsayOBM user account has sufficient quota assigned to accommodate the storage for the system state backup for the new backup set and retention policy. Please contact your backup service provider for more details.

## 2.7 Java Heap Size

The default Java heap size setting of AhsayOBM is 2048MB. For Windows System State backup, it is highly recommended to increase the Java heap size setting to at least 4096MB to improve backup and restore performance. The actual heap size used will be dependent on amount of free memory available on the machine with AhsayOBM installed (machine that is running the backup).

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.



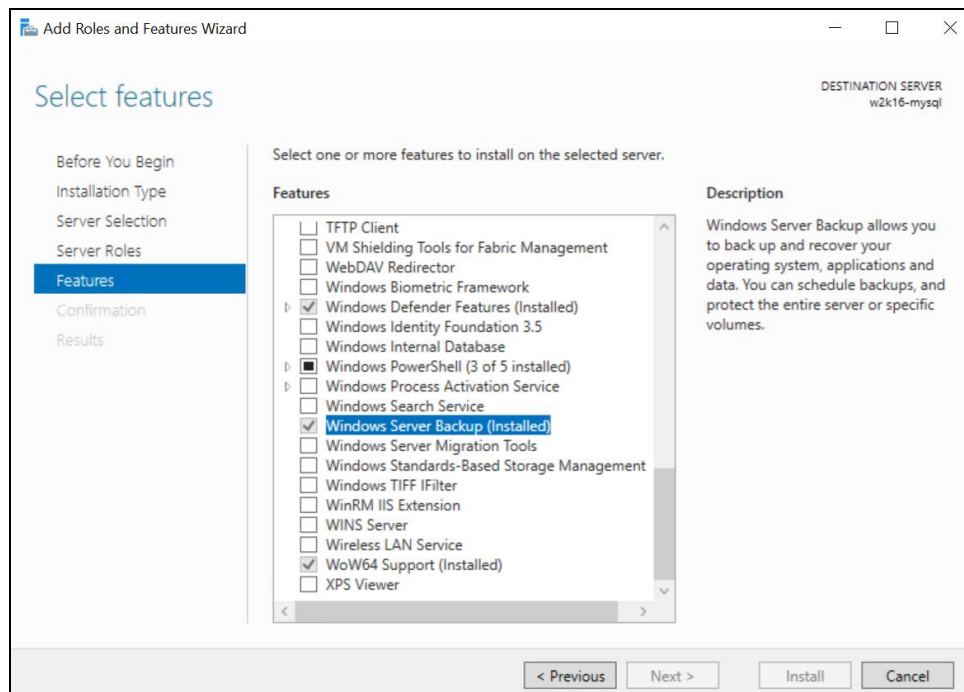
## 2.9 Windows Requirements

### 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

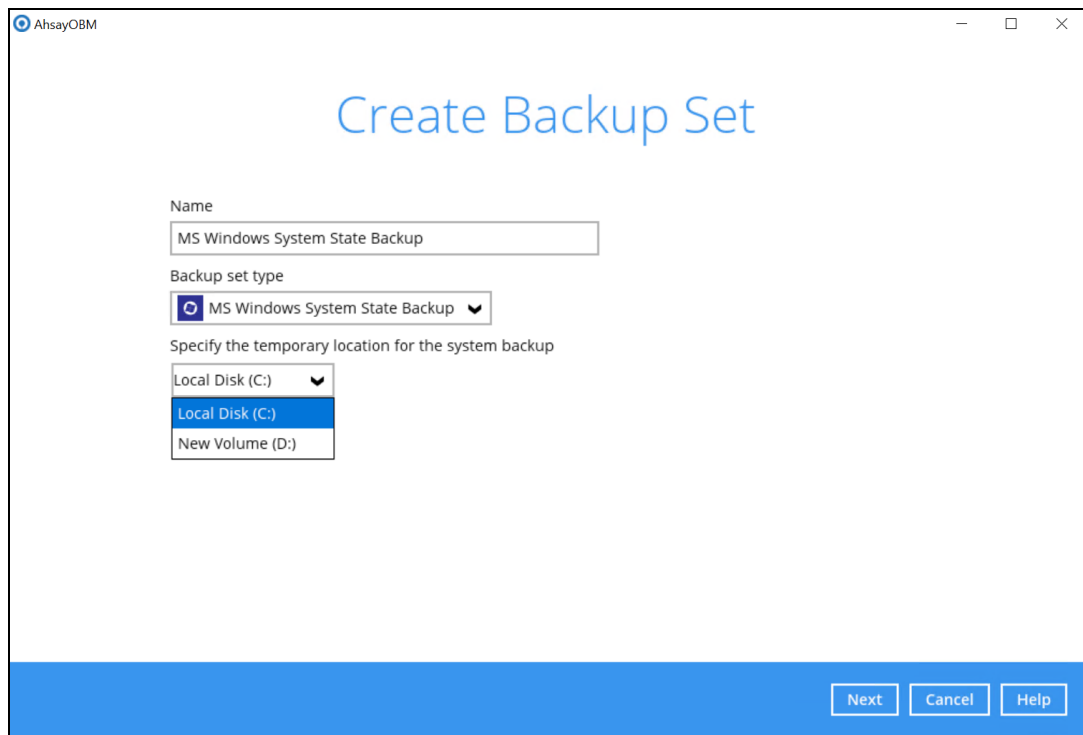
Ensure that you have the latest service packs installed. Updates to the Windows operating system improve its performance and resolve known issues with Windows Server Backup.

#### NOTE

- Windows XP Home is not supported for the system state backup and restore by AhsayOBM.
- As Windows XP and Windows 2003 are no longer supported by Microsoft anymore, Ahsay will provide best effort support.

## 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 two (2) drives in total, Local Disk C: and New Volume D:

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](#)

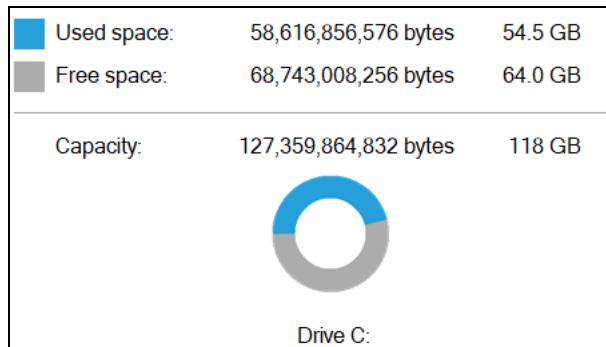
## • Disk Space Available in Temporary Storage Location

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

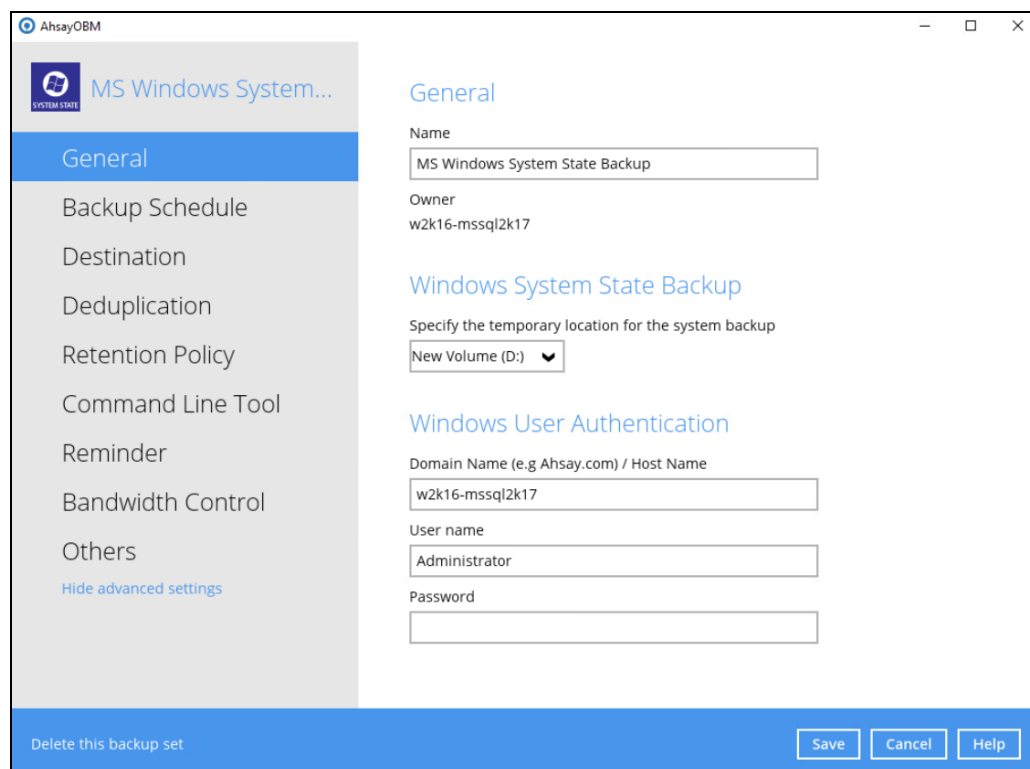
This limitation does not apply to Windows 8 or newer releases of Windows platforms.

## 2.11 Best Practices and Recommendations

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

### Temporary Directory Folder Location

For best performance, it is recommended that the temporary storage location of a MS Windows System State 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 D:).



#### NOTE

For Windows Server 2008 or newer releases, the restriction on temporary volume ([Ch 2.10](#)) must also be considered.

### 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

### Backup Frequency

MS Windows System State 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 to identify those flaws.

## • **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.

## • **Restore to Alternate Computer**

You can restore a system state backup to the same physical computer from which the system state 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 state 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>

## 📌 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.

- ⦿ 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.
- ⦿ Network – make sure to have enough network bandwidth to accommodate the volume of data within the backup interval.
- ⦿ 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.

## 2.12 Restore Considerations

Please consider the following before performing a MS System State 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>


## 3 Configuring a MS Windows System Backup Set

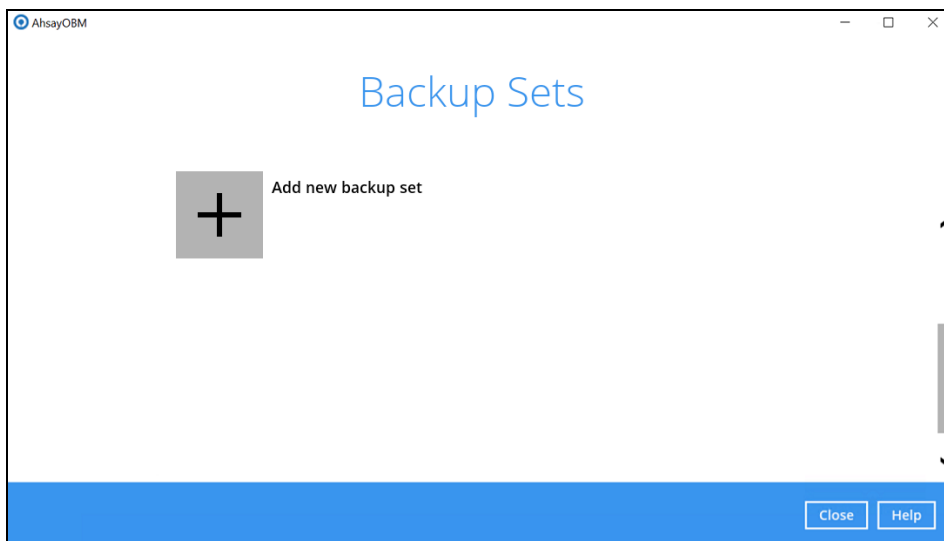
### 3.1 Configuring an MS Windows System State Backup Set

Create the MS Windows System State backup set using following steps.

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

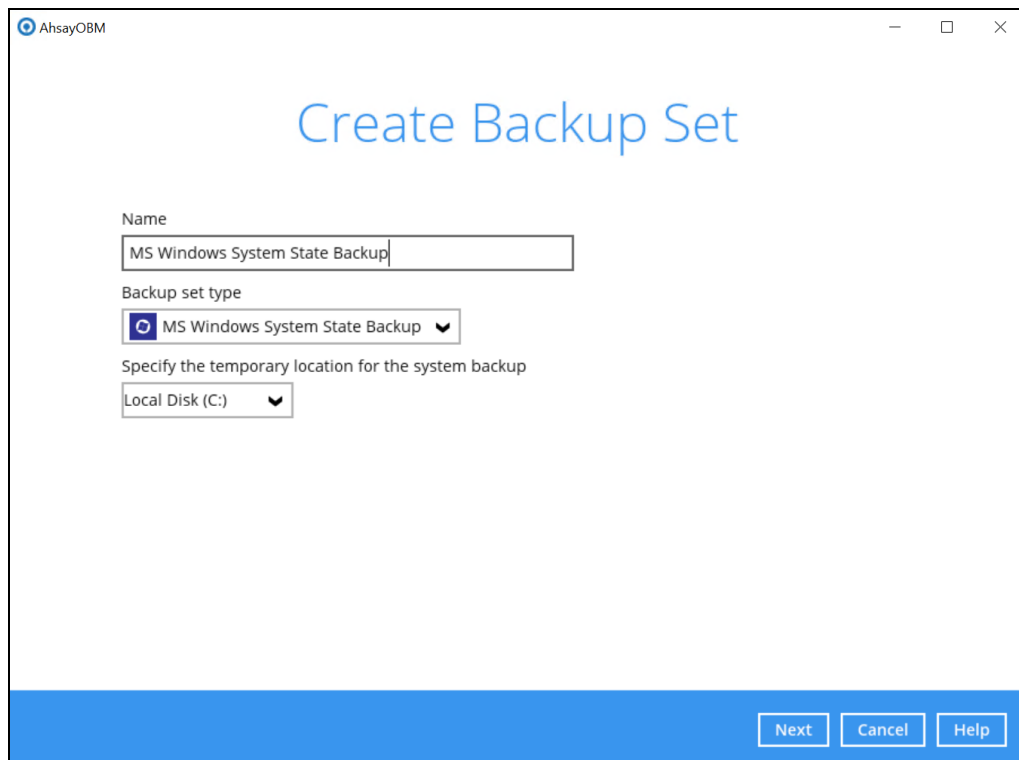


2. Create a MS Windows System State backup set by clicking  next to **Add new backup set**.





3. Select **MS Windows System State Backup** as the **Backup set type**, enter a **Name** for your backup set, and specify a **Temporary Location** for your back up. Click **Next** to proceed.



AhsayOBM

## Create Backup Set

Name  
MS Windows System State Backup

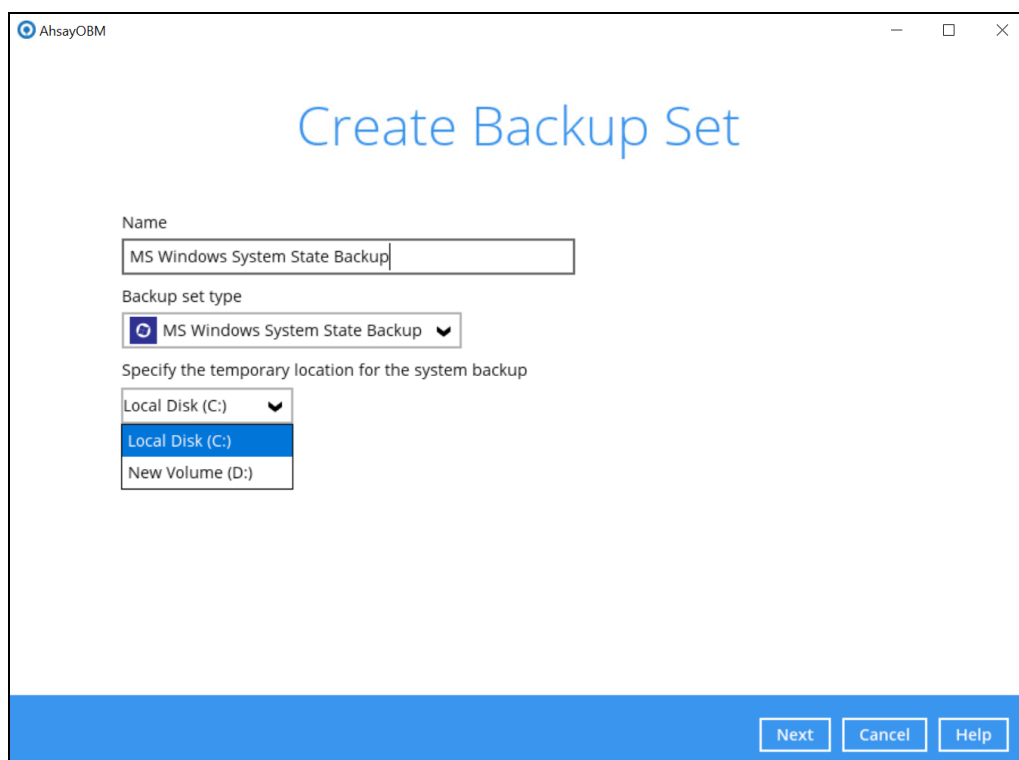
Backup set type  
MS Windows System State Backup

Specify the temporary location for the system backup  
Local Disk (C:)

Next Cancel Help

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

Select a local volume from the dropdown menu.



AhsayOBM

## Create Backup Set

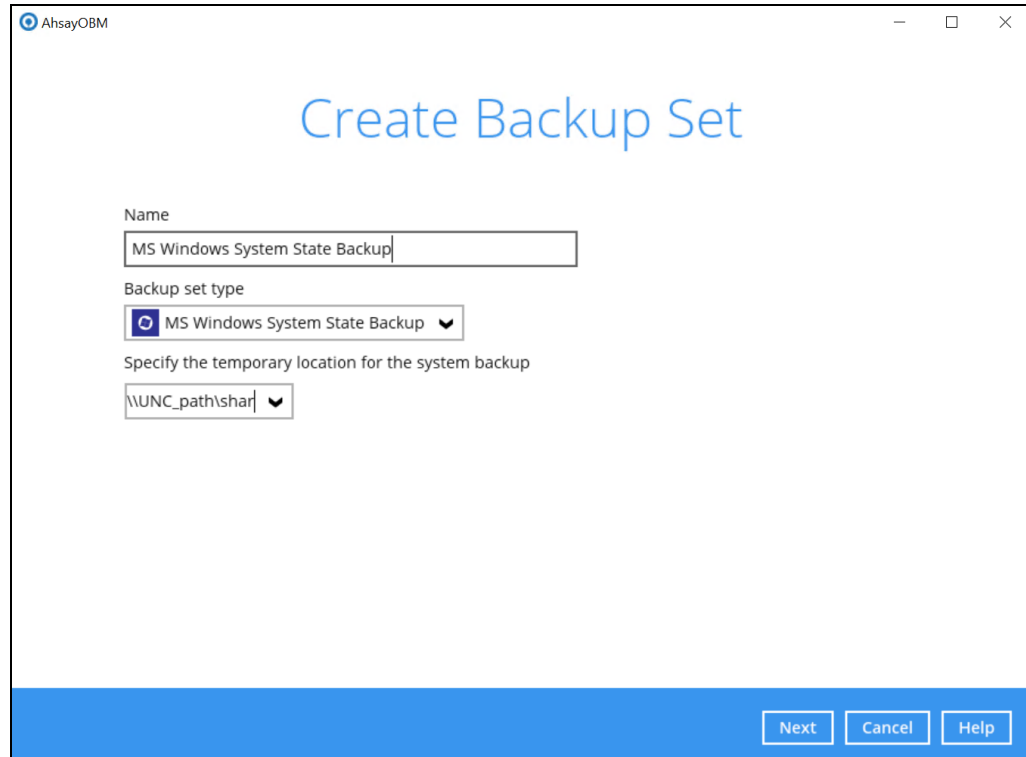
Name  
MS Windows System State Backup

Backup set type  
MS Windows System State Backup

Specify the temporary location for the system backup  
Local Disk (C:)  
Local Disk (C:)  
New Volume (D:)

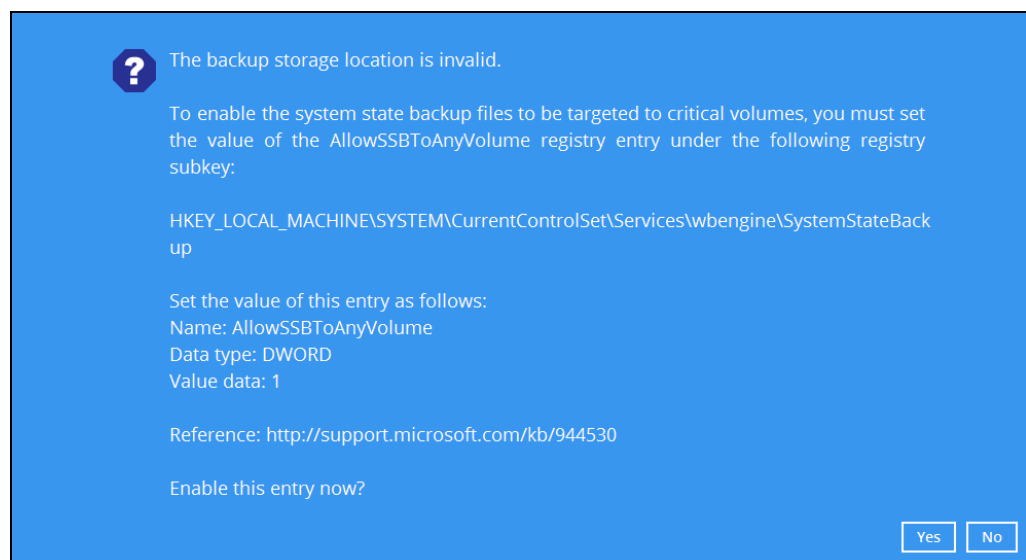
Next Cancel Help

**OR** enter the UNC path to a network volume that is accessible to the client computer.



**Note:** For Windows 2008 Server, the temporary storage location cannot be set to a network path.

**Note:** If the storage location is set to a critical volume (e.g. system volume), the following message will be displayed:



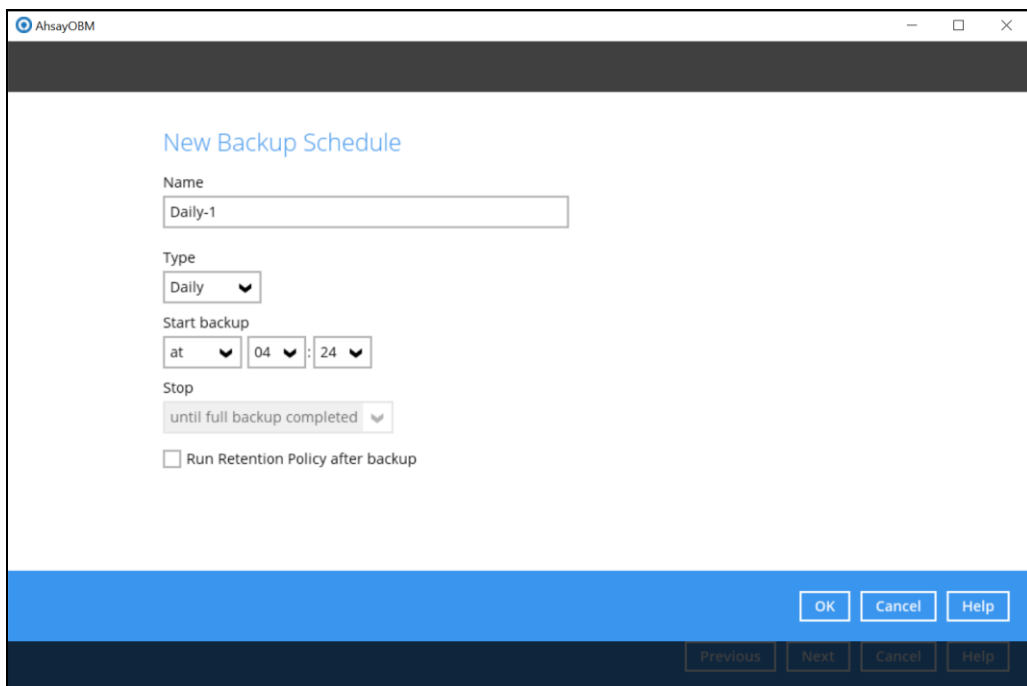
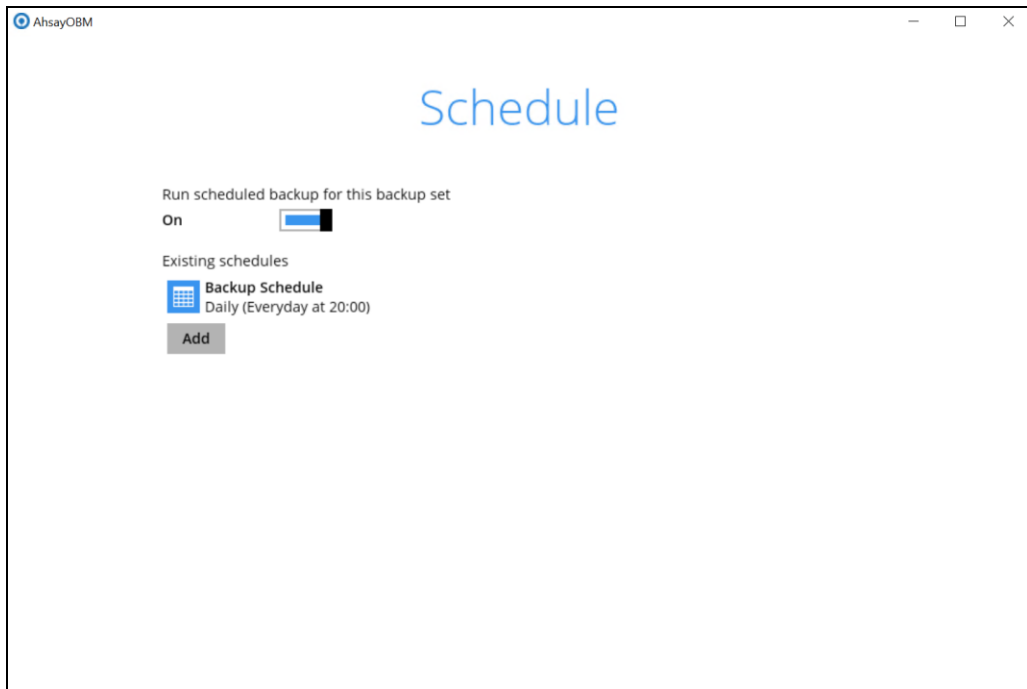
Click **Yes** for AhsayOBM to enable the registry entry, or click **No**, then change the storage location setting to another location.

Refer to the following link for the details on the restriction:


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

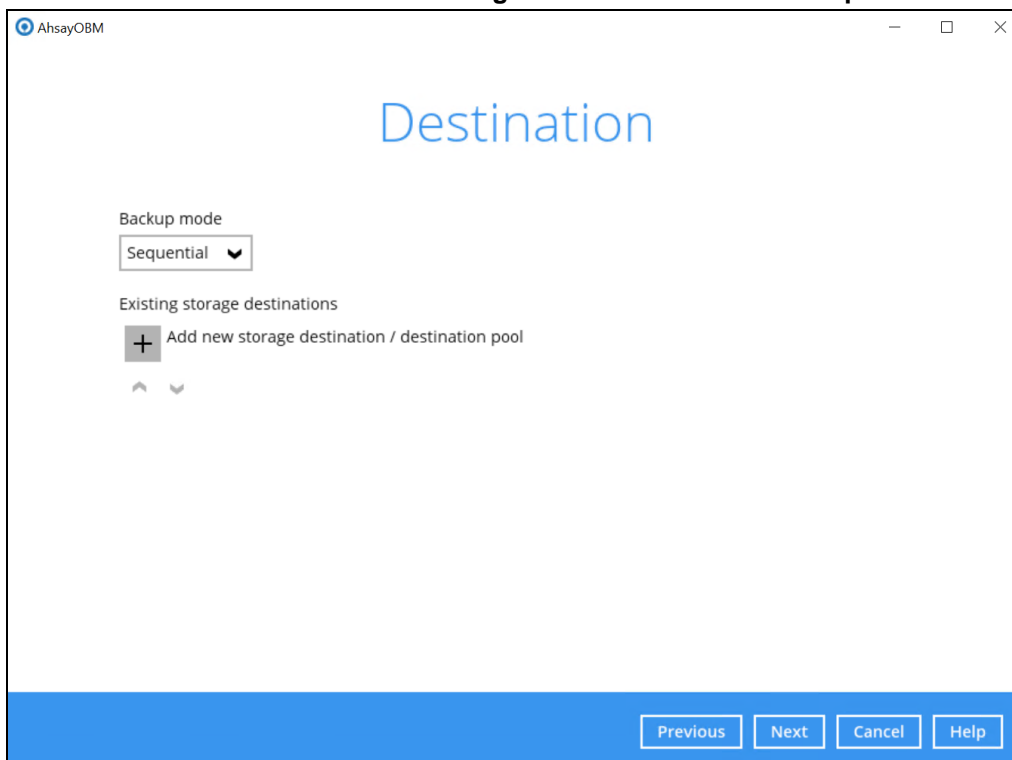
5. In the **Schedule** window, configure a backup schedule for backup job to run automatically at your specified time interval.

Click **Add** to add a new schedule.



Click **OK** to continue, and then click **Next** to proceed afterward.

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



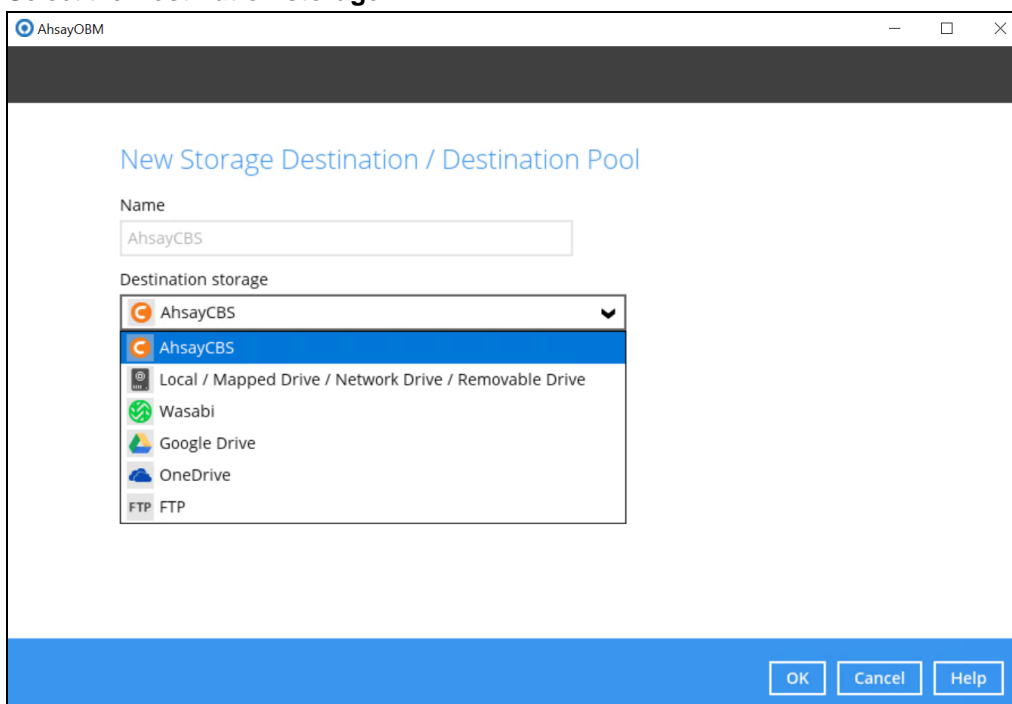
The screenshot shows the 'Destination' configuration window in AhsayOBM. The title bar says 'AhsayOBM'. The main heading is 'Destination'. Below it, there is a 'Backup mode' dropdown menu set to 'Sequential'. Under 'Existing storage destinations', there is a plus icon and the text 'Add new storage destination / destination pool'. At the bottom right, there are four buttons: 'Previous', 'Next', 'Cancel', and 'Help'.

**Note:** For more details on Backup Destination, refer to this link:

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

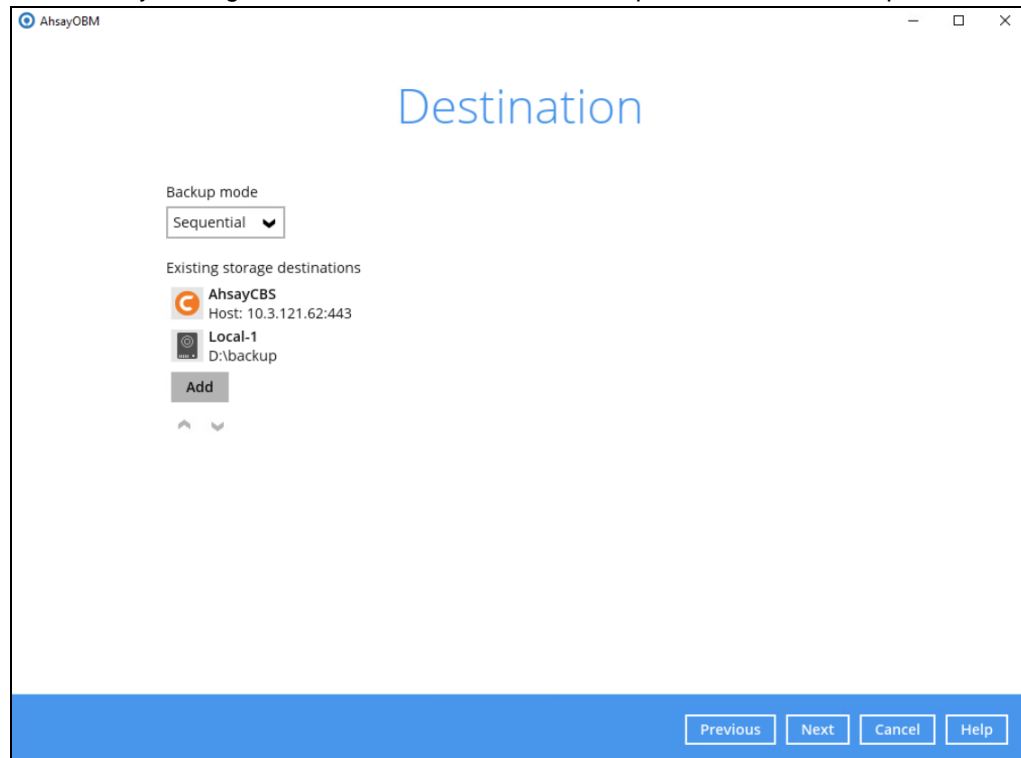
For more details on configuration of cloud storage as backup destination, refer to the [Appendix A](#) section in this guide.

7. Select the **Destination storage**.



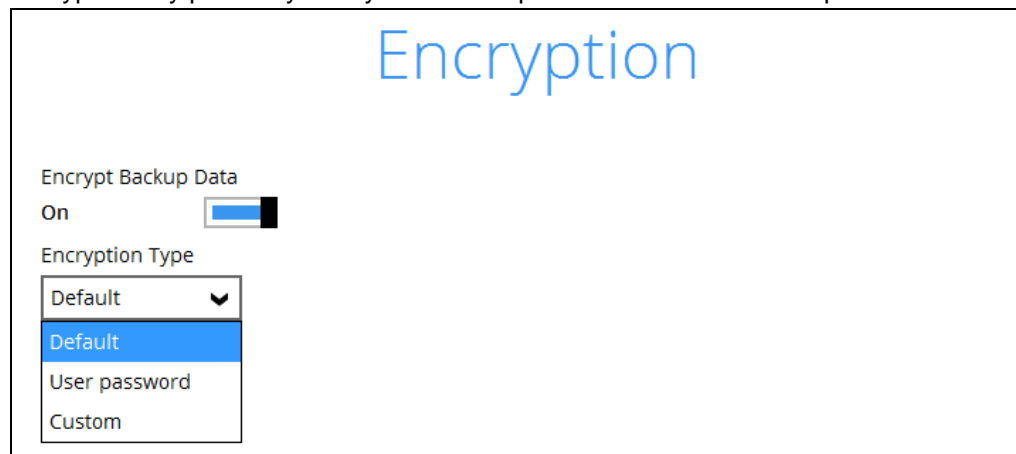
The screenshot shows the 'New Storage Destination / Destination Pool' configuration window in AhsayOBM. The title bar says 'AhsayOBM'. The main heading is 'New Storage Destination / Destination Pool'. Below it, there is a 'Name' text box containing 'AhsayCBS'. Under 'Destination storage', there is a dropdown menu with the following options: 'AhsayCBS' (selected), 'AhsayCBS', 'Local / Mapped Drive / Network Drive / Removable Drive', 'Wasabi', 'Google Drive', 'OneDrive', and 'FTP'. At the bottom right, there are three buttons: 'OK', 'Cancel', and 'Help'.

Continue by adding another destination for the backup set or click **Next** to proceed.



**Note:** Multiple backup destinations can be configured for a single backup set.

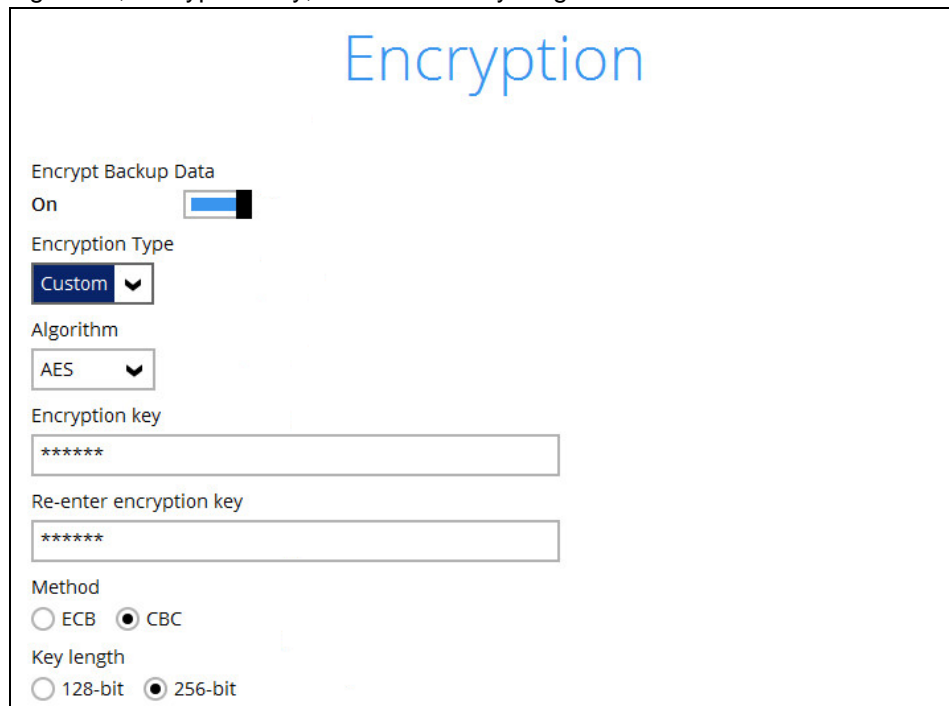
8. In the Encryption window, the default **Encrypt Backup Data** option is enabled with an encryption key preset by the system which provides the most secure protection.



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  
\*\*\*\*\*

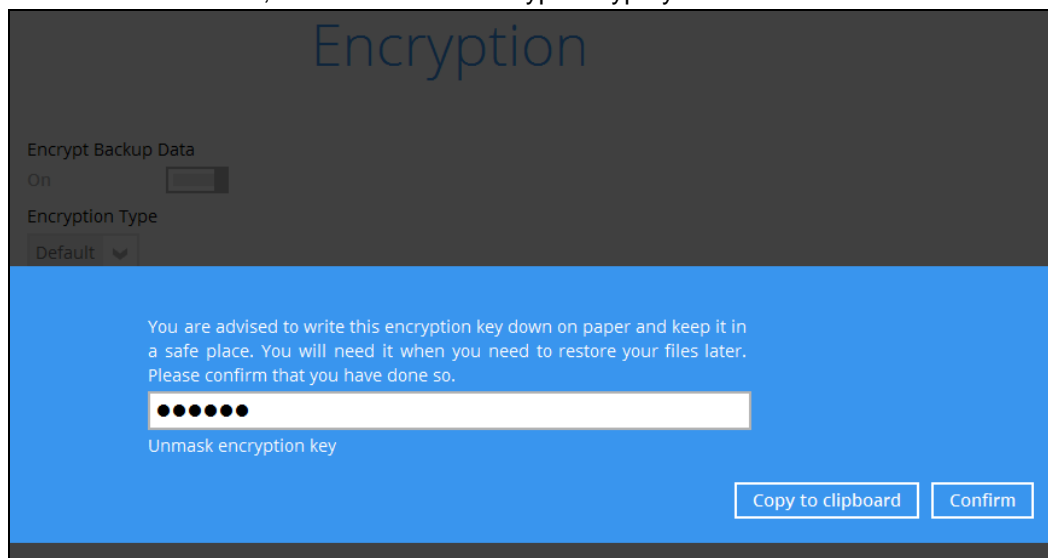
Method  
☐ ECB ☒ CBC

Key length  
☐ 128-bit ☒ 256-bit

**Note:** For best practice on managing your encryption key, refer to this link:  
[FAQ: Best practices for managing encryption key for AhsayOBM or AhsayACB](#)

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

9. If you have enabled the **Encryption** feature in the previous step, the following pop-up window will be shown, 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.

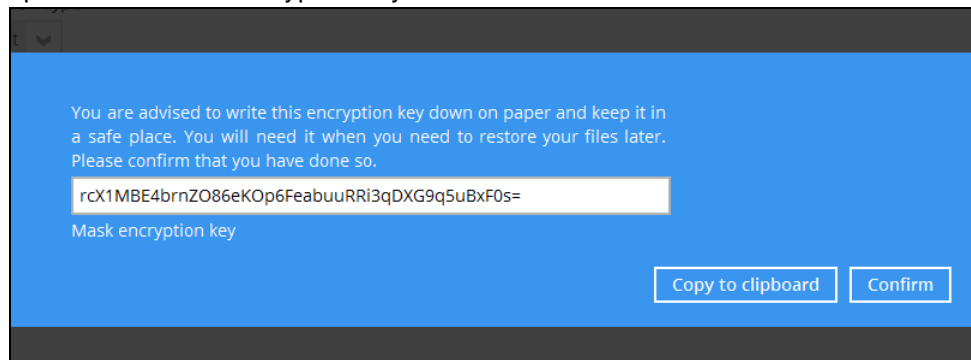
●●●●●●

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.

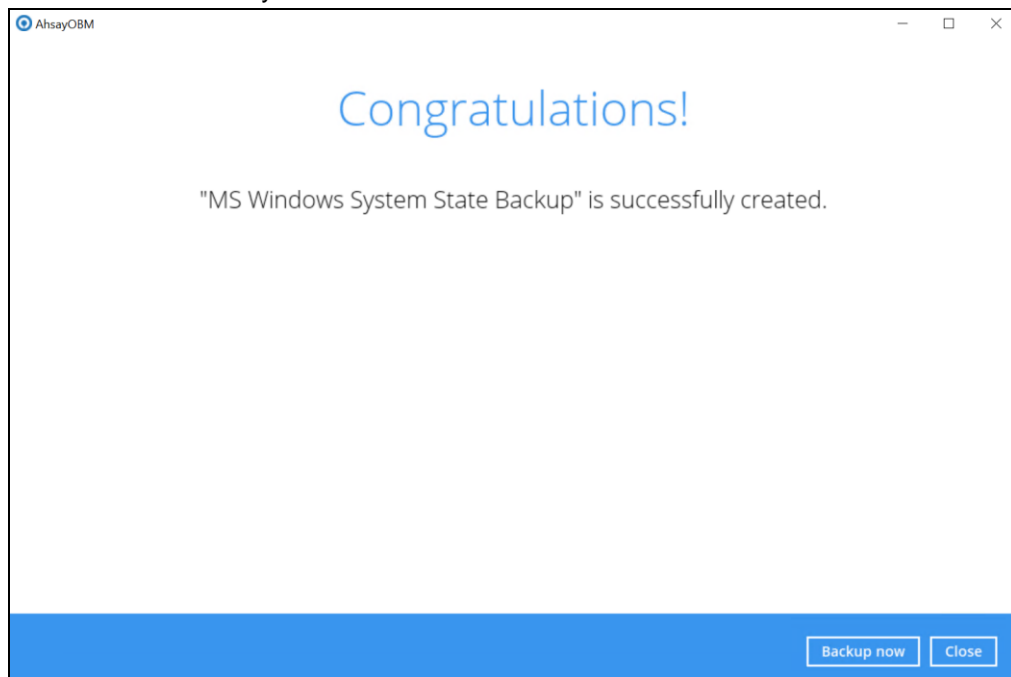


- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.
- **Confirm** – Click to exit this pop-up window and proceed to the next step.

10. Enter the **Domain Name / Host Name** of the computer, **User Name** and **Password** of the Windows account that will be running the backup. Click **Next** to create the backup set.

A window titled "AhsayOBM" with a blue header. The main title is "Windows User Authentication". Below it are three input fields: "Domain Name (e.g Ahsay.com) / Host Name" with the value "w2k16-mssql2k17", "User name" with the value "Administrator", and "Password" which is empty. At the bottom right are four buttons: "Previous", "Next", "Cancel", and "Help".

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



12. 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.

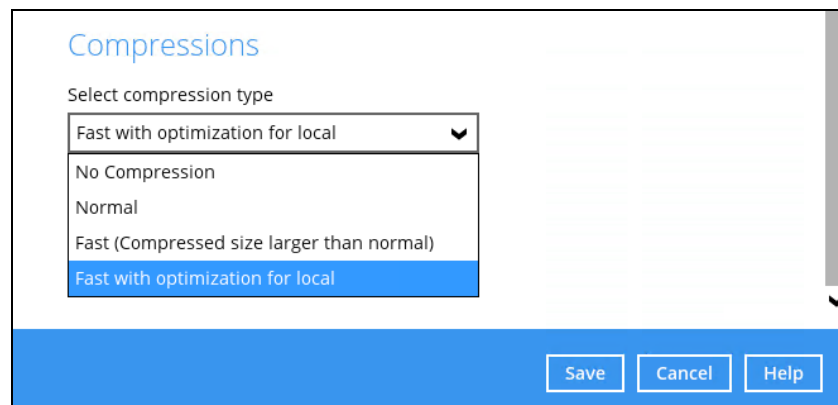




13. Optional: Select your preferred **Compression** type. By default, the compression type is Fast with optimization for local.

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

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



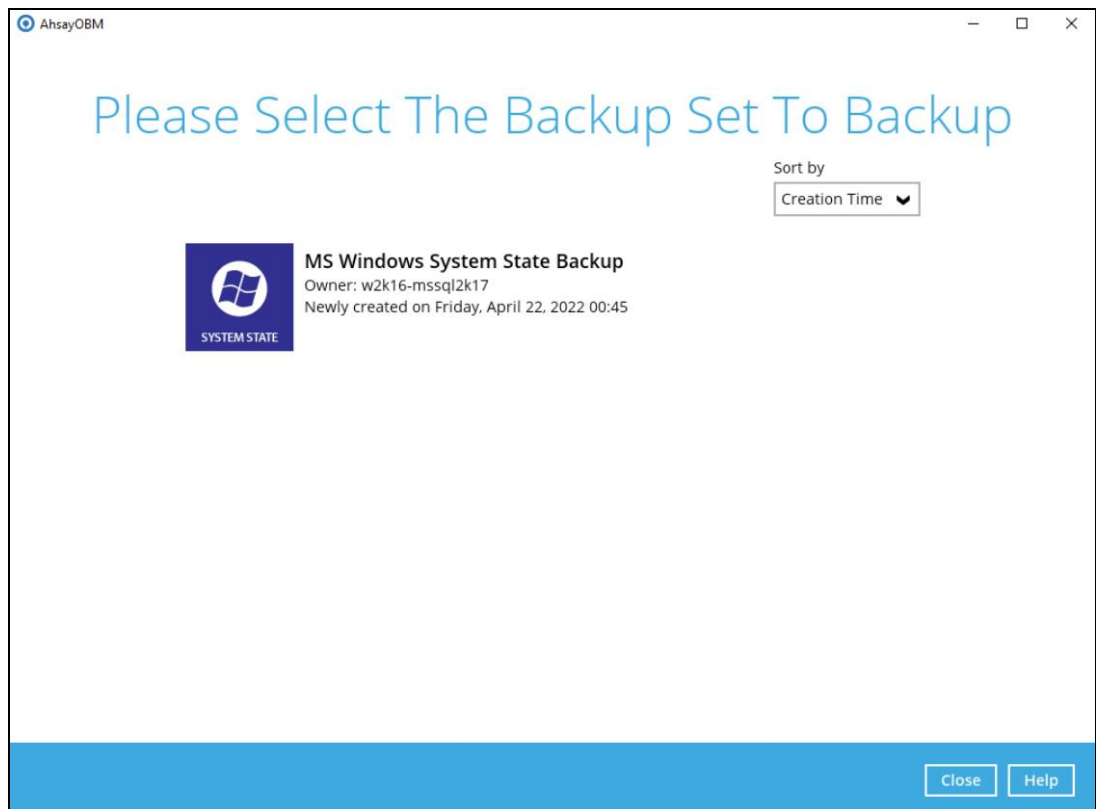
## 4 Running a Backup

### 4.1 Start a Manual Backup

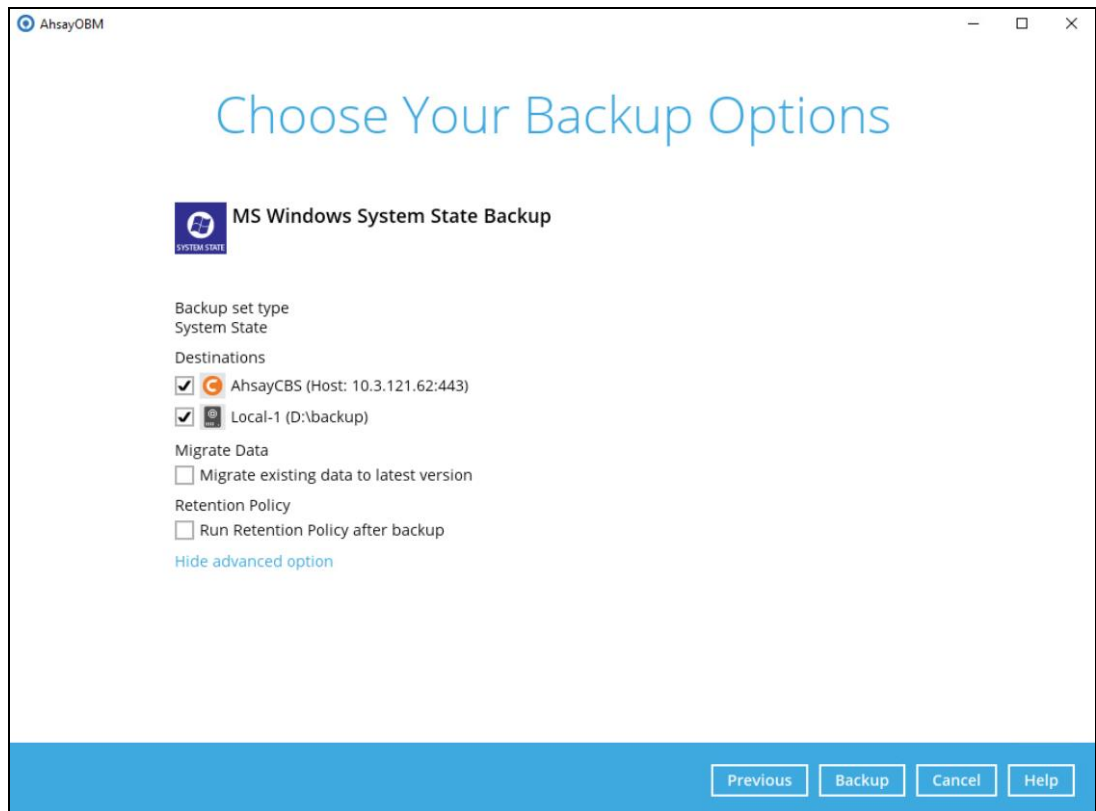
1. Click the **Backup** icon on the main interface of AhsayOBM.



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



3. If you would like to modify the Destinations, Migrate Date, and Retention Policy settings, click **Show advanced option**.



The screenshot shows the 'Choose Your Backup Options' window in AhsayOBM. The title bar says 'AhsayOBM'. The main heading is 'Choose Your Backup Options'. Below it is a section for 'MS Windows System State Backup' with a 'SYSTEM STATE' icon. The settings are as follows:

- Backup set type: System State
- Destinations:
  - ☒ AhsayCBS (Host: 10.3.121.62:443)
  - ☒ Local-1 (D:\backup)
- Migrate Data:
  - ☐ Migrate existing data to latest version
- Retention Policy:
  - ☐ Run Retention Policy after backup

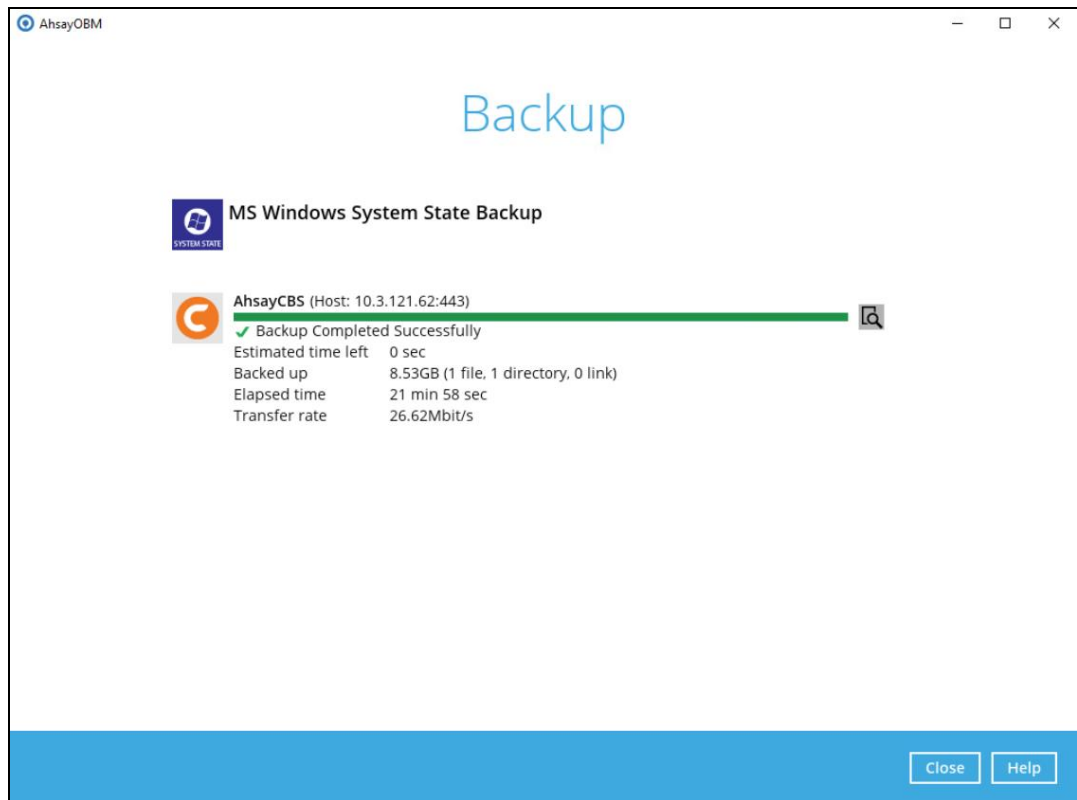
At the bottom, there is a link 'Hide advanced option' and four buttons: 'Previous', 'Backup', 'Cancel', and 'Help'.

Click **Backup** to start the backup job.

#### NOTE

The **Migrate Data** option will only be displayed if Deduplication is enabled for the backup set. When the Migrate Data option is enabled, the existing data will be migrated to the latest version during a backup job. This option is disabled by default. Backup job(s) for backup sets with Migrate Data enabled may take longer to finish. For more information about this feature, refer to [Ahsay CBS v9 New Features Supplemental document](#).

4. The following screen is displayed when the System State data are backed up successfully.

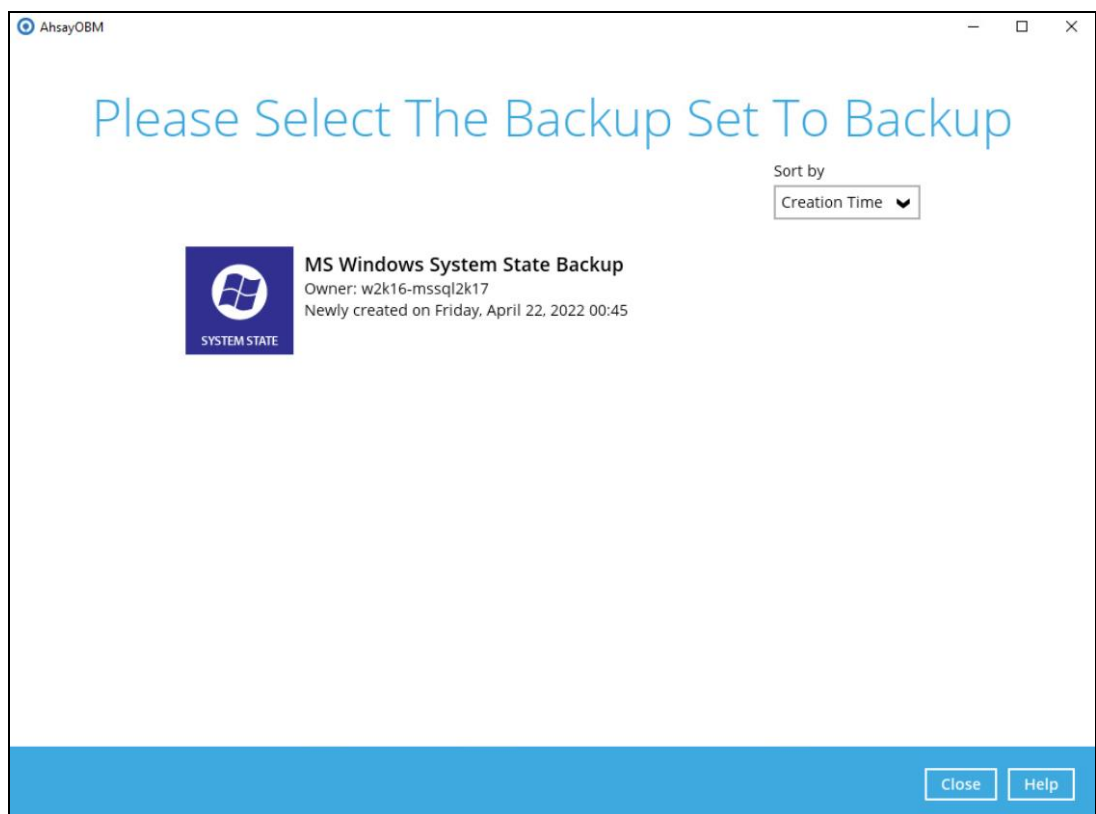


## 4.2 Configure Backup Schedule for Automated Backup

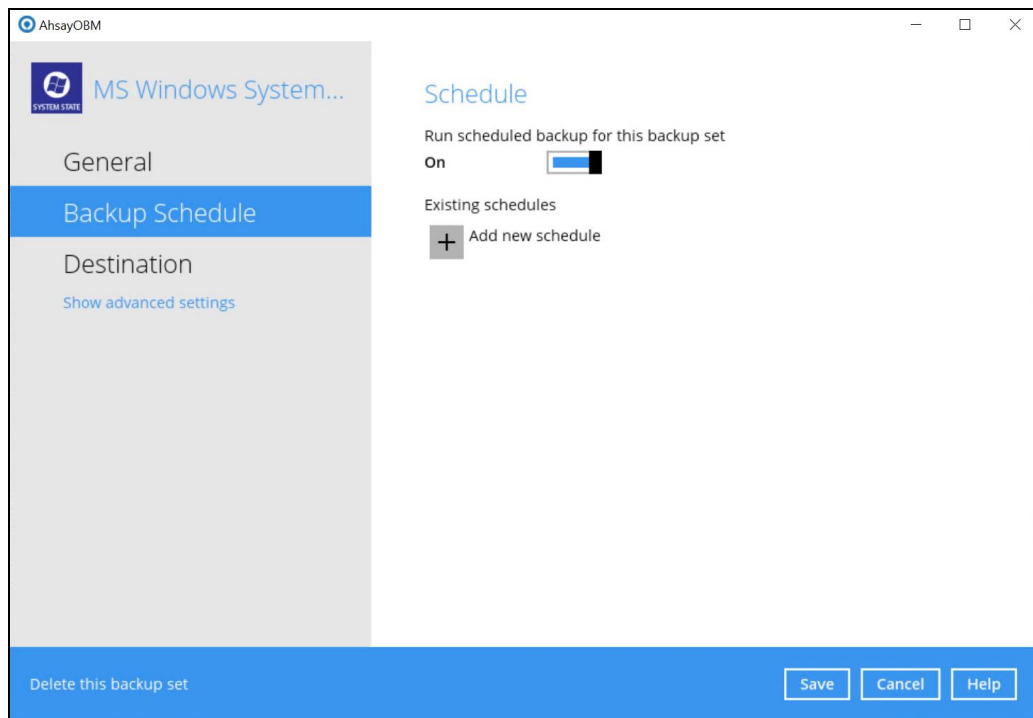
1. Click the **Backup Sets** icon on the main interface of AhsayOBM.



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



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



- The New Backup Schedule window will appear.

The 'New Backup Schedule' window contains the following fields and options:

- Name:** A text input field containing 'Daily-1'.
- Type:** A dropdown menu with 'Daily' selected.
- Start backup:** A time selection interface with 'at' selected, followed by a dropdown showing '13' and another dropdown showing '00'.
- Stop:** A dropdown menu with 'until full backup completed' selected.
- Run Retention Policy after backup:** An unchecked checkbox.

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

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

The screenshot shows the 'New Backup Schedule' window with the following settings:

- Name:** Daily-1
- Type:** Daily (selected from a dropdown menu)
- Start backup:** at 15:41 (selected from dropdowns)
- Stop:** until full backup completed (selected from a dropdown menu)
- ☒ Run Retention Policy after backup

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

The screenshot shows the 'New Backup Schedule' window with the following settings:

- Name:** Weekly-1
- Type:** Weekly (selected from a dropdown menu)
- Backup on these days of the week:** Sun, Mon, Tue, Wed, Thu, Fri, ☒ Sat
- Start backup:** at 23:00 (selected from dropdowns)
- Stop:** until full backup completed (selected from a dropdown menu)
- ☒ 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

2022 December ▼ 22 ▼

Start backup at  
11 ▼ : 15 ▼

Stop  
until full backup completed ▼

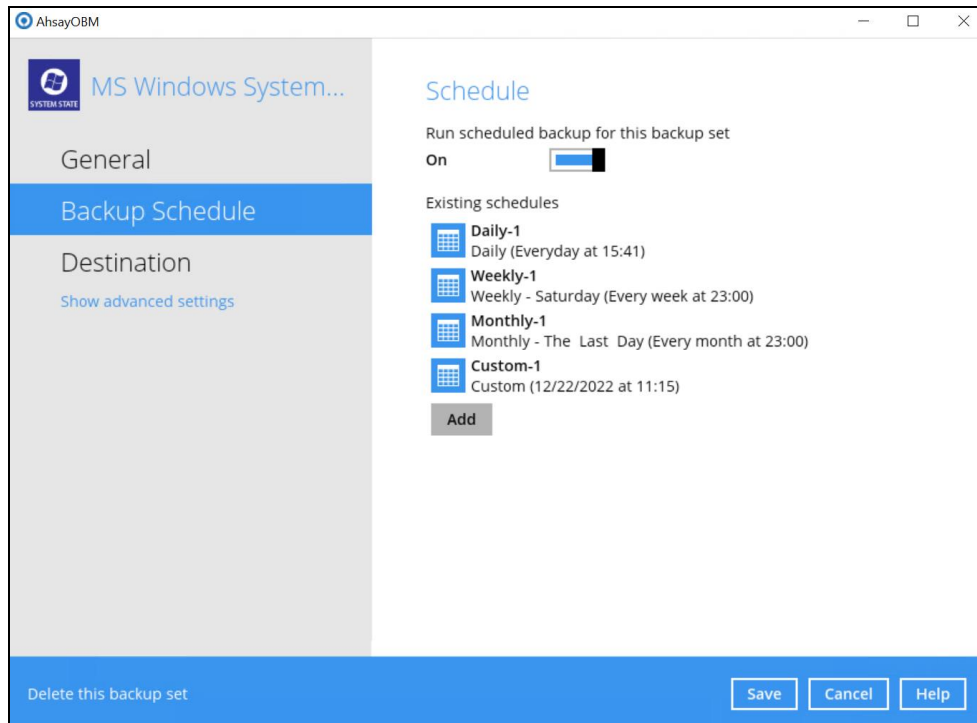
☐ Run Retention Policy after backup



- **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.

- ❶ **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 quota in the long run, it is recommended to enable this option.
- ❷ As an example, the four types of backup schedules may look like the following:

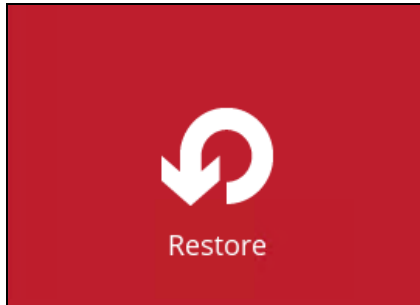


Click **Save** to confirm your settings once done.

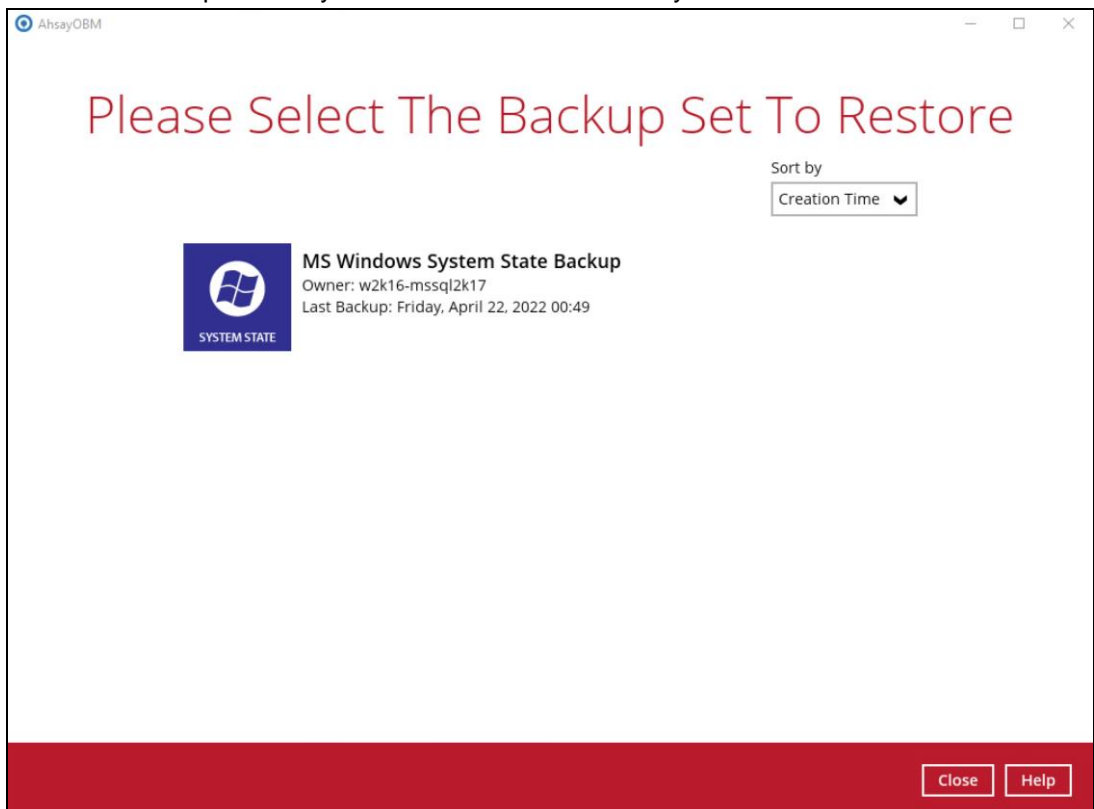
## 5 Restore with a Microsoft Windows System Backup Set

### 5.1 Restore the System State Data

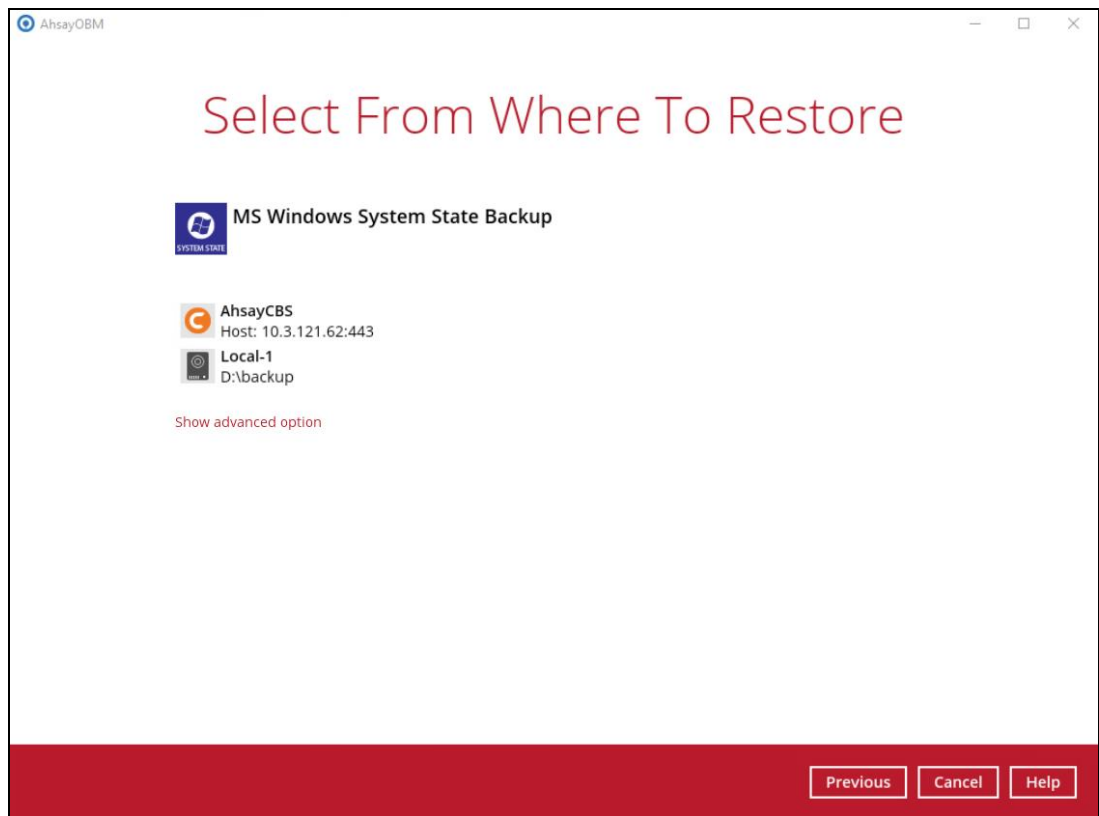
1. Click the **Restore** icon on the main interface of AhsayOBM.



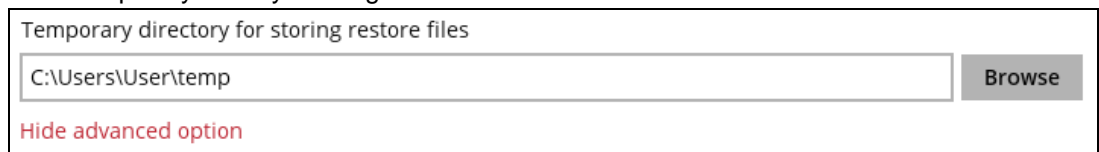
2. Select the backup set that you would like to restore the system state data from.



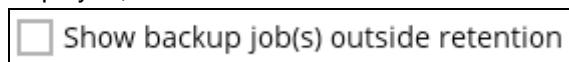
3. Select the backup destination that contains the system state data that you would like to restore.



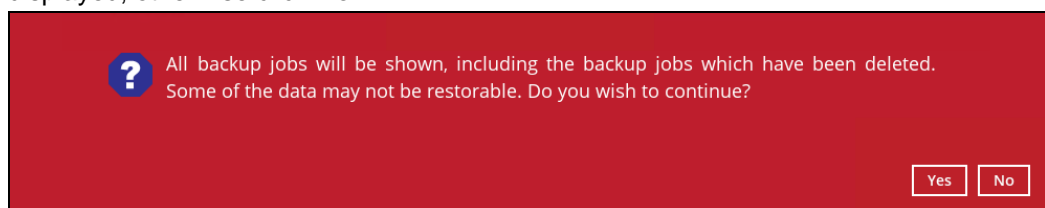
You may configure the **Temporary directory for storing restore files** by clicking **Show advanced option**. This will allow you to select the directory that will be used to store temporary files by clicking the **Browse** button.



4. Tick **Show backup job(s) outside retention** if you want all backup jobs to be displayed, even the deleted ones.



Once ticked, this message will be displayed. Click **Yes** if you want all backup jobs to be displayed, otherwise click **No**.



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

The screenshot shows the 'Select Your Files To Be Restored' window in AhsayOBM. The window has a title bar with the AhsayOBM logo and standard window controls. The main heading is 'Select Your Files To Be Restored' in a large, red, sans-serif font. Below the heading, there is a section titled 'Select what to restore'. This section contains a dropdown menu labeled 'Choose from files as of job' with a downward arrow, a date dropdown set to '04/22/2022', a 'Latest' dropdown, and a checkbox labeled 'Show backup job(s) outside retention'. Below this is a red link 'Show filter'. The main area is a table with columns: 'Folders', 'Name', 'Size', and 'Date modified'. The 'Folders' column shows a tree view with 'AhsayCBS' expanded, containing 'w2k16-mssql2k17'. The 'Name' column shows 'Microsoft\_Win2008\_Sysstate\_Backup' with a green checkmark icon. The 'Size' column shows '8.53GB' and the 'Date modified' column shows '04/22/2022 01:00'. At the bottom of the table area, there is a 'Search' label, 'Items per page' set to '50', and 'Page' set to '1 / 1'. The bottom of the window has a red bar with four buttons: 'Previous', 'Next', 'Cancel', and 'Help'.

6. Select the location to restore the system state data to by clicking the arrow down icon.

The screenshot shows the 'Choose Where The Files To Be Restored' window in AhsayOBM. The window has a title bar with the AhsayOBM logo and standard window controls. The main heading is 'Choose Where The Files To Be Restored' in a large, red, sans-serif font. Below the heading, there is a section titled 'Restore files to'. This section contains a dropdown menu showing 'Local Disk (C:)' with a downward arrow. Below this is a red link 'Show advanced option'. The bottom of the window has a red bar with four buttons: 'Previous', 'Restore', 'Cancel', and 'Help'.

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

## Choose Where The Files To

Restore files to

New Volume (D:)

Show advanced option

## Choose Where The Files To

Restore files to

New Volume (D:)

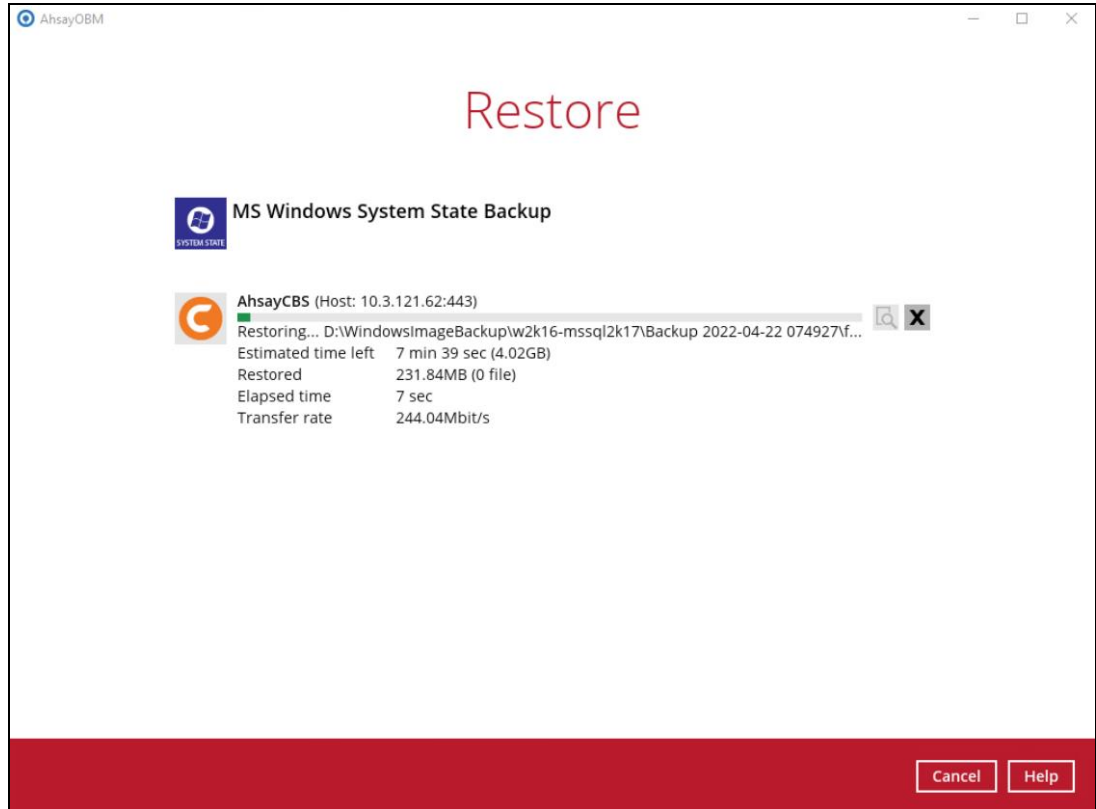
☐ Verify checksum of in-file delta files during restore

Hide advanced option

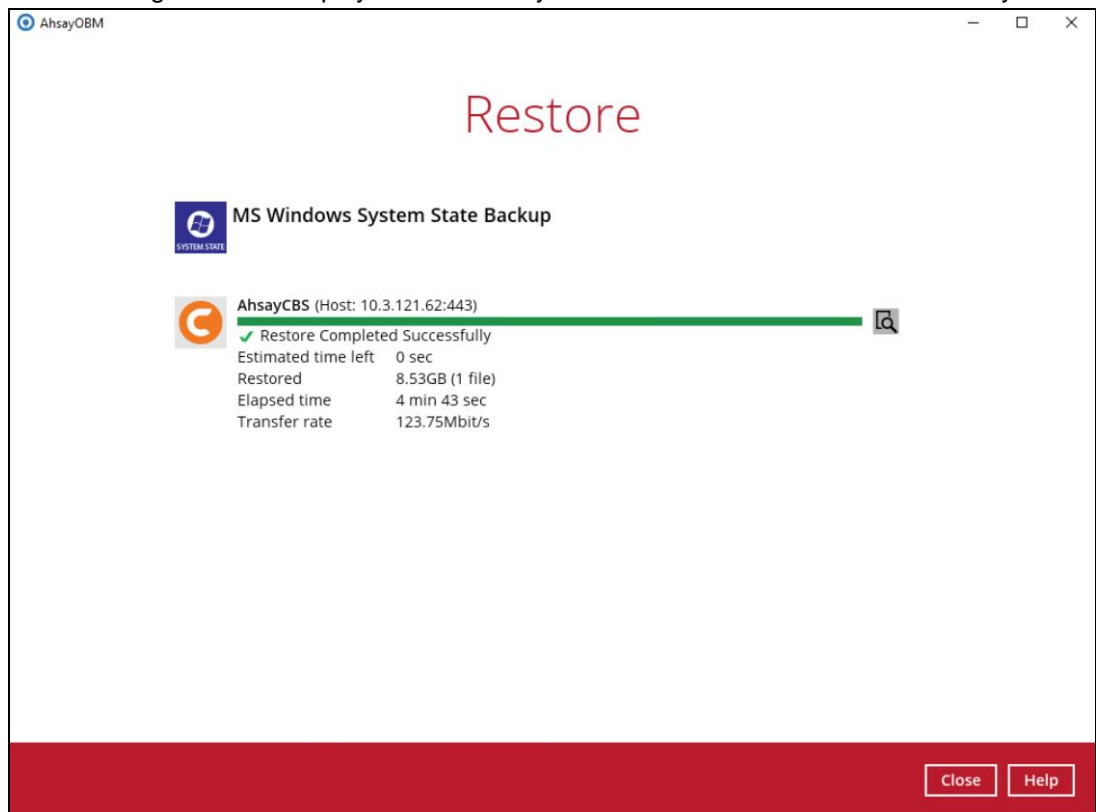
🔍 **Verify checksum of in-file delta files during restore**

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.

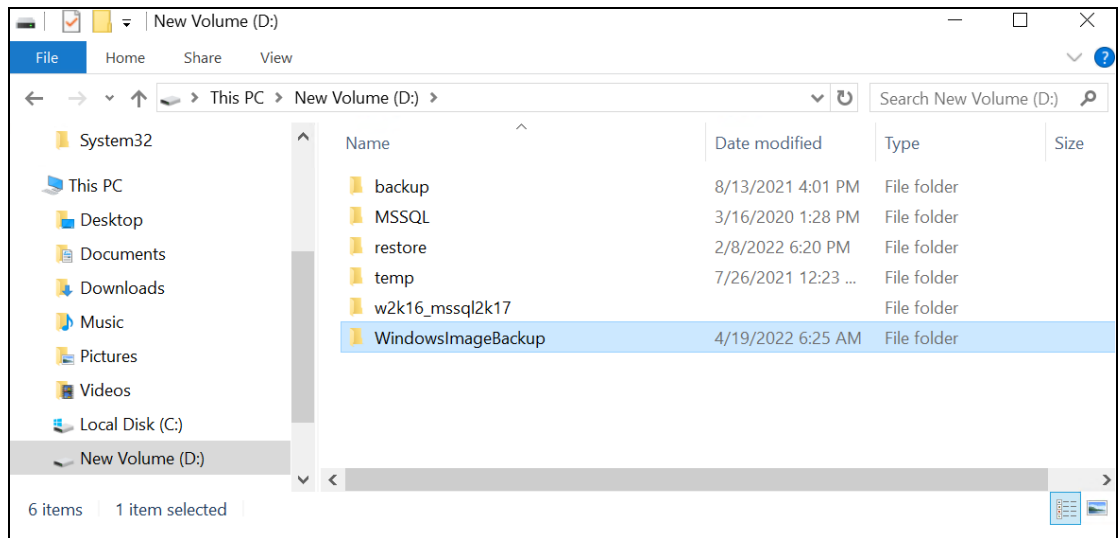
7. Click **Restore** to start the restoration.



8. The following screen is displayed when the system state data is restored successfully.



9. Go to the restore location you have selected and copy the file to the server that you want to perform the restore for, or to a network drive that is accessible to the server.



**Important:** In addition to the system state data, the **WindowsImageBackup** folder includes catalog files that contain information about all backups in there up to the current backup, and MediaId, 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.

10. Copy the **WindowsImageBackup** folder and its content to the server that you want to perform the restore for, or to a network drive that is accessible to the server.

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

11. Continue to the next section of the guide.



## 5.2 Apply the System State Data

Before you begin, make sure that the system state data restored with AhsayOBM are copied to a local disk (where you will perform the restore), or in a remote shared folder.

For Windows Server 2008 R2 or later, you can use the Recovery Wizard in Windows Server Backup or wbadmin command to recover the system state.

For Windows Server 2008, you can only use the wbadmin command to recover the system state.

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

Note: Refer to the following page for syntax of the Wbadmin command: <http://go.microsoft.com/fwlink/?LinkId=140216>

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

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

Example (system state restored to D: volume):

```
C:\Users\Administrator>wbadmin get versions -backupTarget:d:  
wbadmin 1.0 - Backup command-line tool  
(C) Copyright 2012 Microsoft Corporation. All rights reserved.  
  
Backup time: 04/19/2022 2:35 AM  
Backup target: 1394/USB Disk labeled Volume 3(D:)  
Version identifier: 04/19/2022-02:35  
Can recover: Volume(s), File(s), Application(s), Bare Metal Recovery,  
System State  
Snapshot ID: {feb9079c-9459-4034-908f-7b5a9b0bb1e5}
```

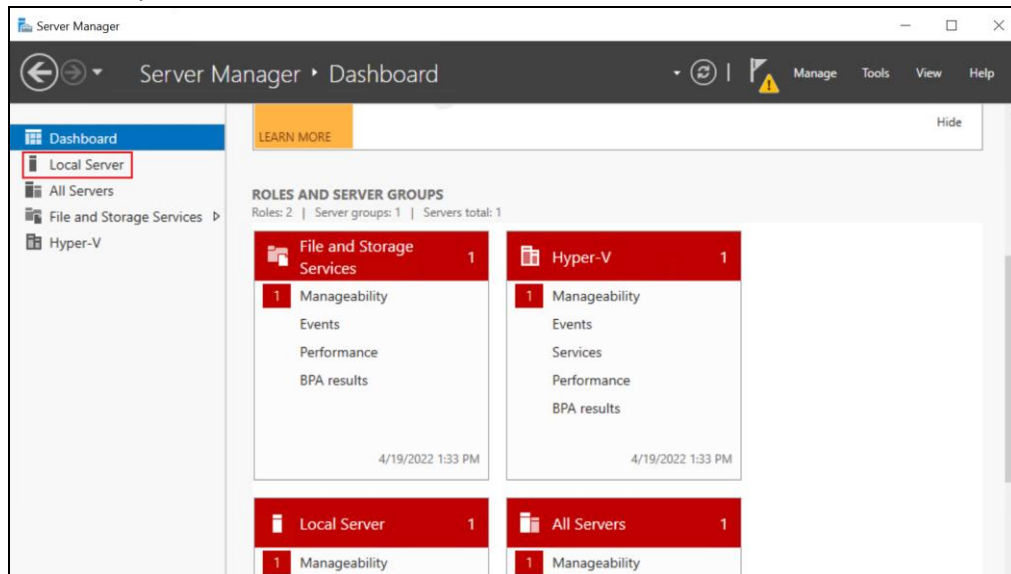
### NOTE

File and folder recovery are not possible from a system state backup performed on Windows Server 2008.

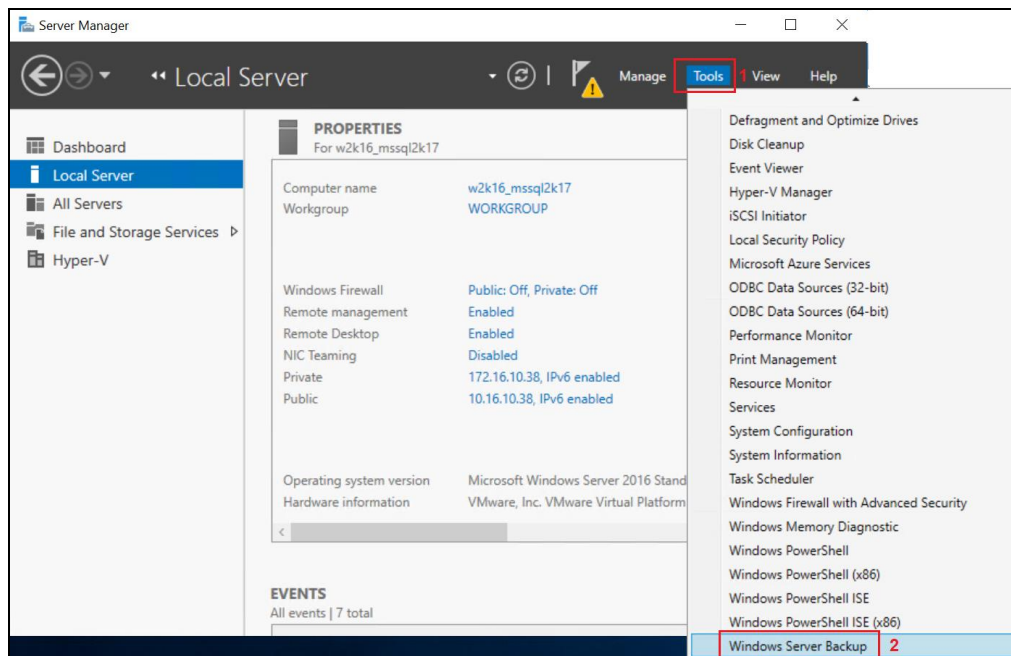
To recover the system state using the Windows Server Backup user interface.

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

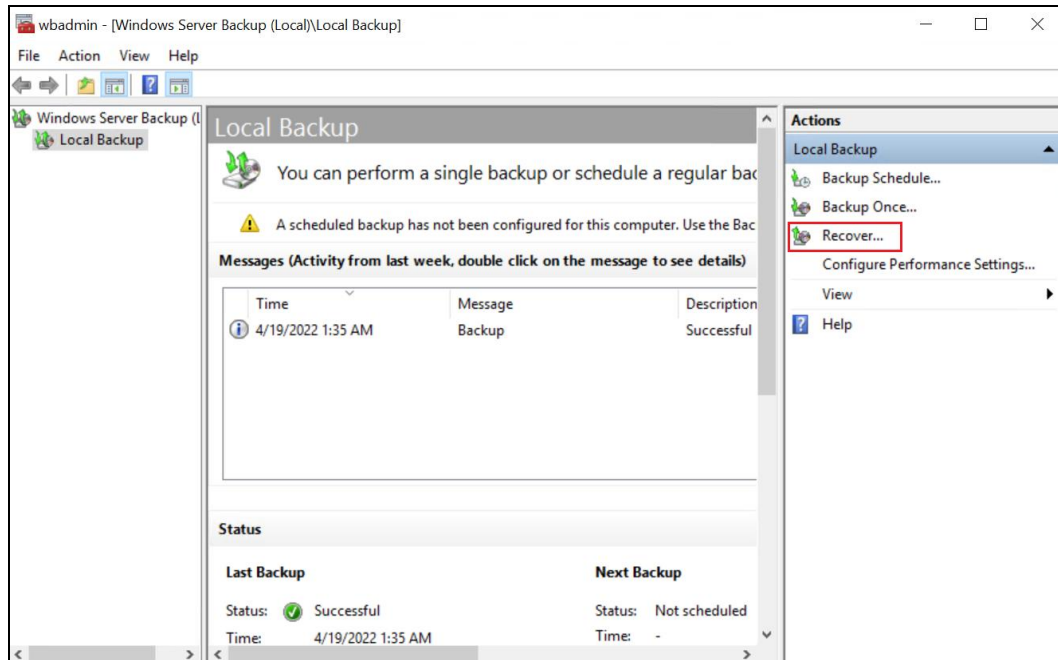
On the left panel, click **Local Server**.



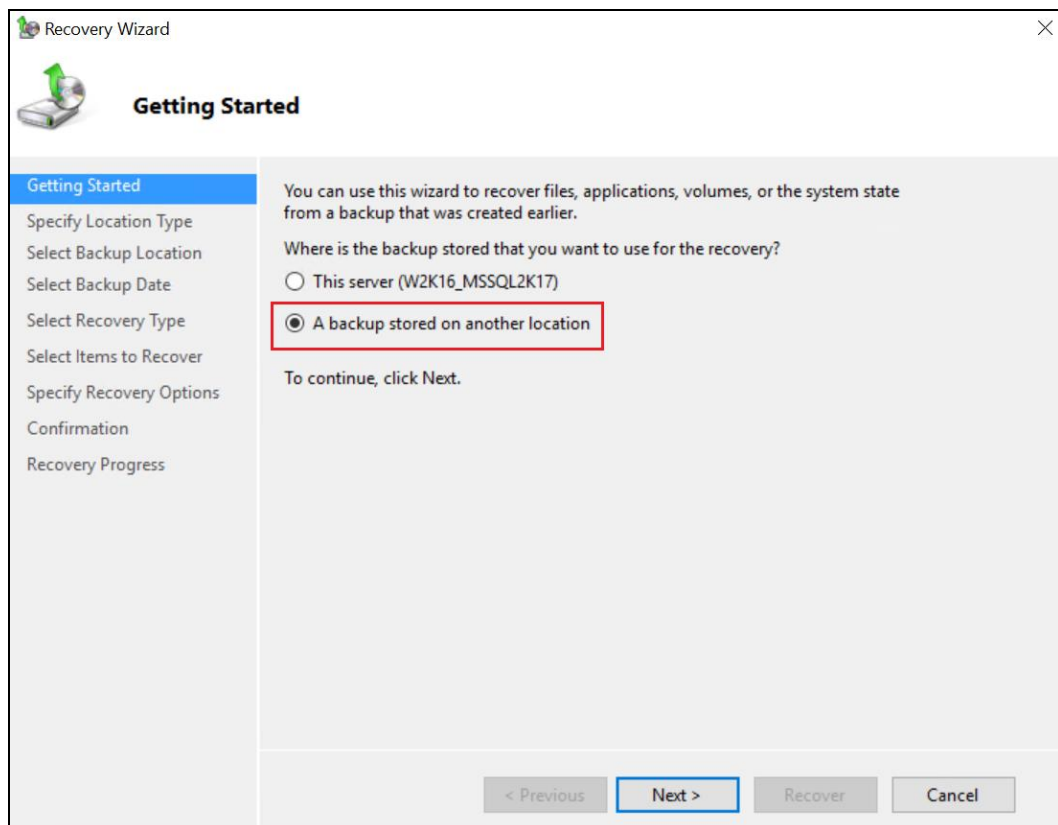
2. On the upper right corner of the **Local Server** page, click **Tools** and select **Windows Server Backup**.



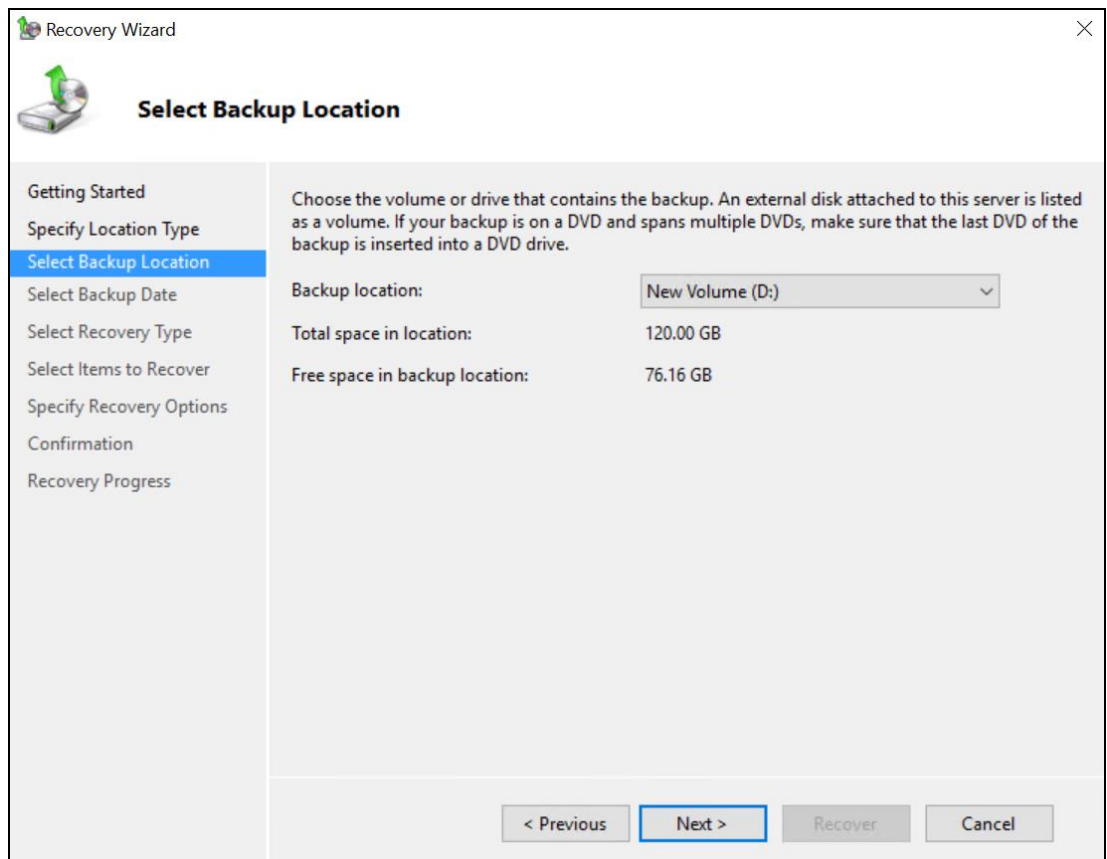
3. In the **Actions** panel under Windows Server Backup, click **Recover...**



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



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



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

D:\ **WindowsImageBackup**

Tap **Next**.

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

Recovery Wizard

### Select Server

Getting Started  
Specify Location Type  
Select Backup Location  
**Select Server**  
Select Backup Date  
Select Recovery Type  
Select Items to Recover  
Specify Recovery Options  
Confirmation  
Recovery Progress

Please select which server's data you would like to recover.

Server:

w2k16\_mssql2k17

< Previous   **Next >**   Recover   Cancel

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

Recovery Wizard

### Select Backup Date

Getting Started  
Specify Location Type  
Select Backup Location  
Select Server  
**Select Backup Date**  
Select Recovery Type  
Select Items to Recover  
Specify Recovery Options  
Confirmation  
Recovery Progress

Oldest available backup: 4/19/2022 1:35 AM  
Newest available backup: 4/19/2022 1:35 AM

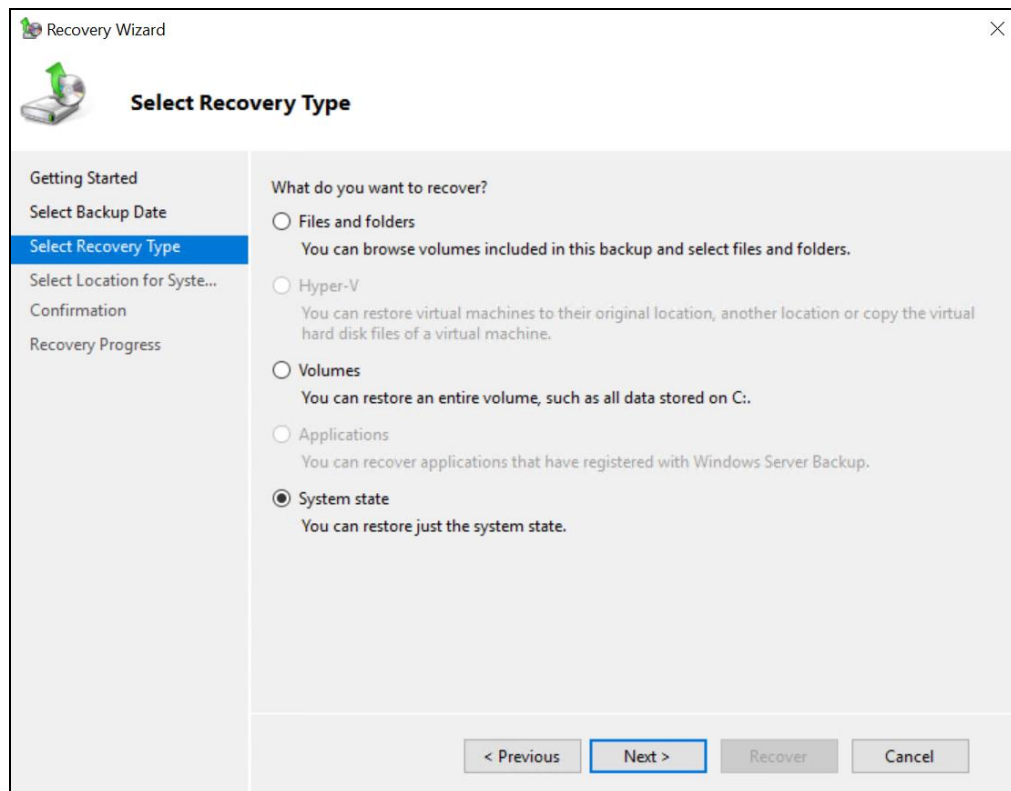
Available backups  
Select the date of a backup to use for recovery. Backups are available for dates shown in bold.

Backup date: 4/19/2022  
Time: 1:35 AM  
Recoverable items: [System state](#)

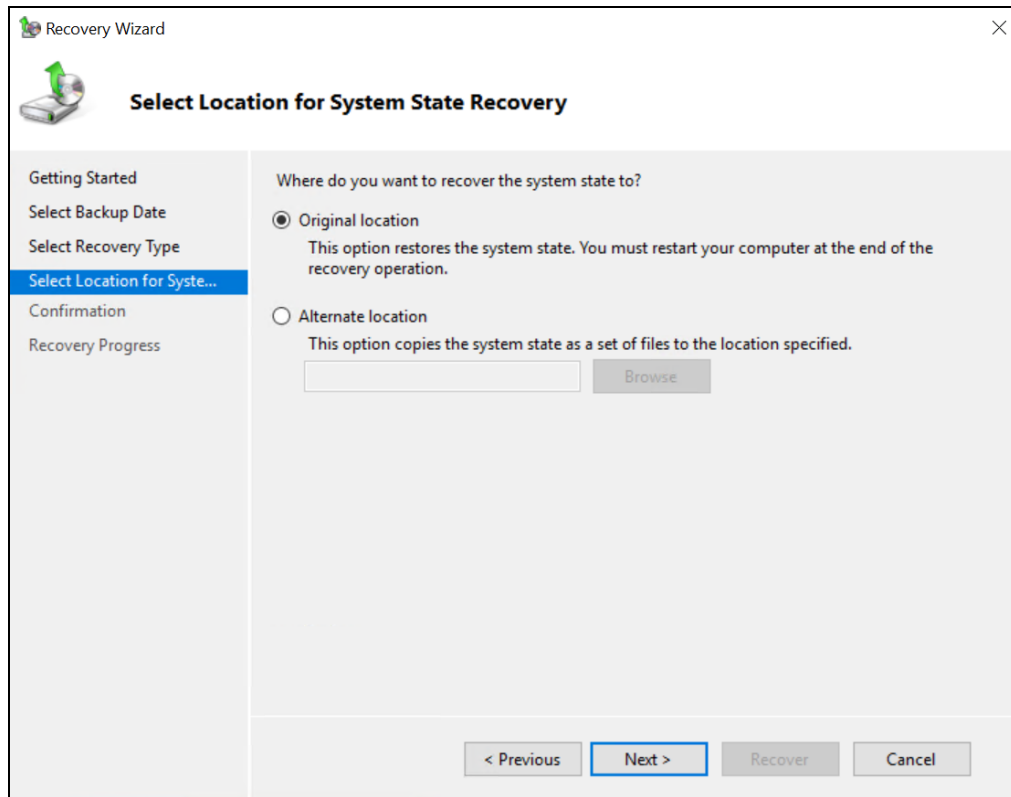
Sun	Mon	Tue	Wed	Thu	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	<b>19</b>	<b>20</b>	21	22	23
24	25	26	27	28	29	30

< Previous   **Next >**   Recover   Cancel

8. On the **Select Recovery Type** page, select **System state**. Click **Next**.



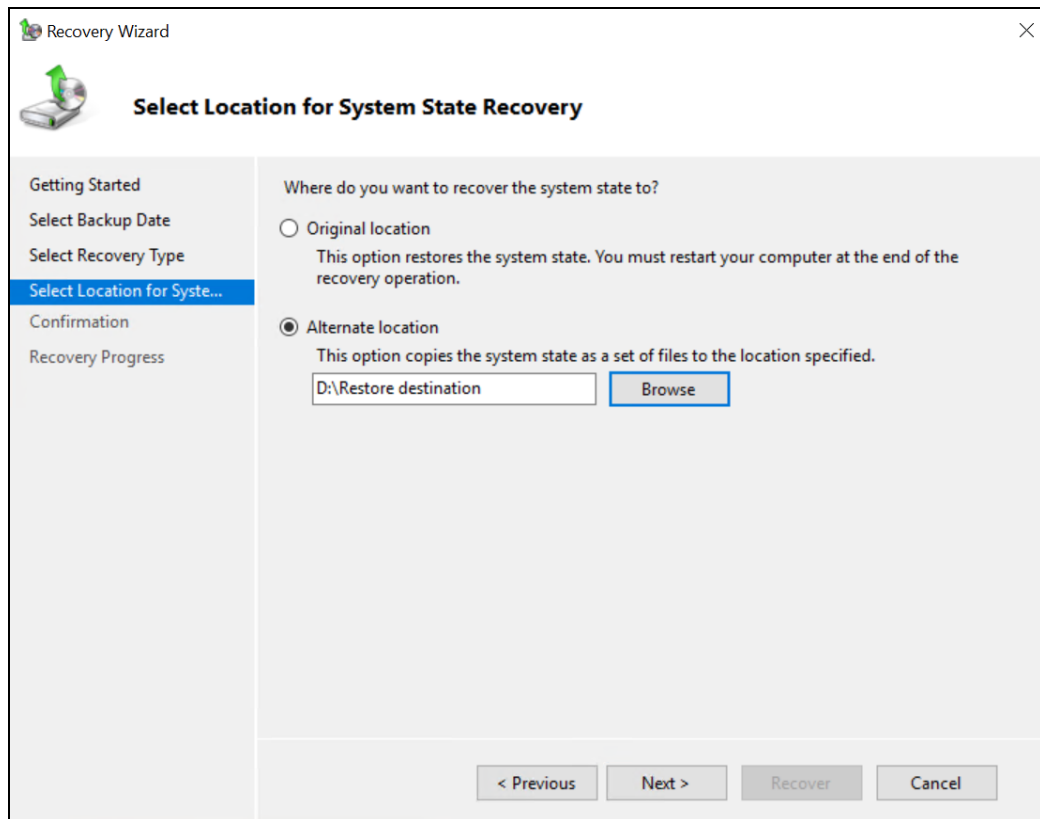
9. On the **Select Location for System State Recovery** page, select
- **Original location**, to restore the system state to the same physical computer from which the system state backup was created
- Or
- **Alternate location**, to restore a copy of the system state as a set of files.



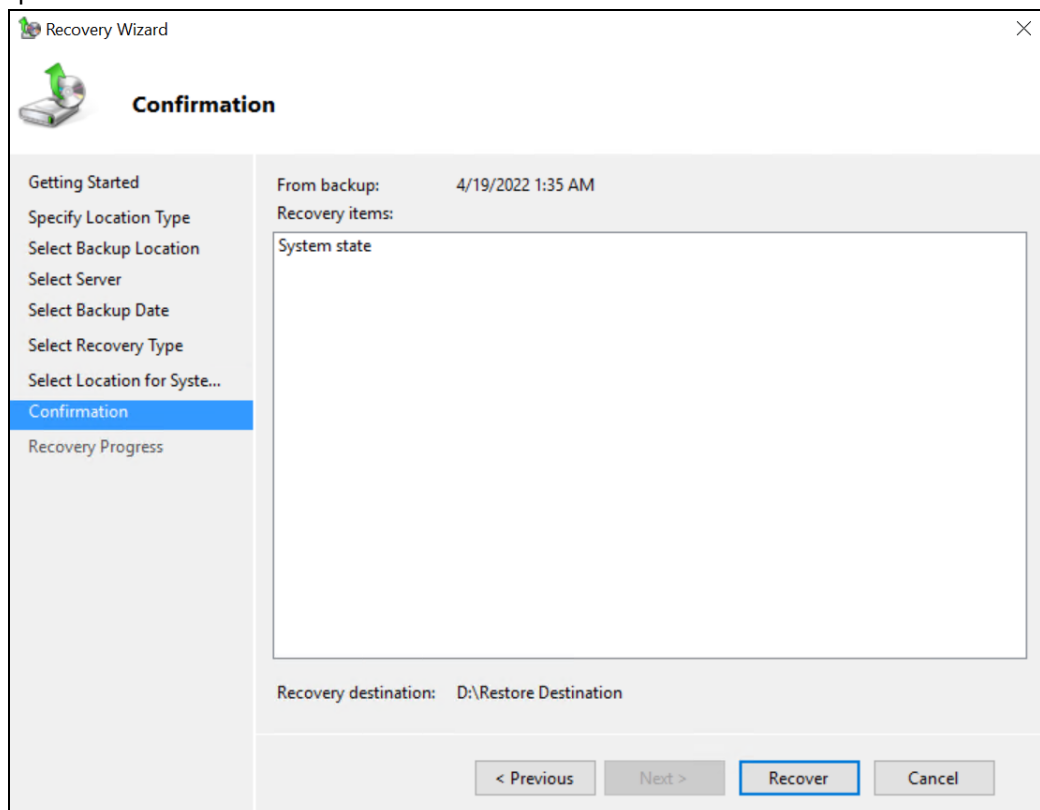
**Note:** The options displayed are different for system state containing Active Directory Domain Services.

You will also need to start the server in Directory Services Restore Mode (DSRM) to restore system state data containing Active Directory Domain Services.

For instructions specific to recovering system state to Active Directory server, see <http://go.microsoft.com/fwlink/?LinkId=143754>

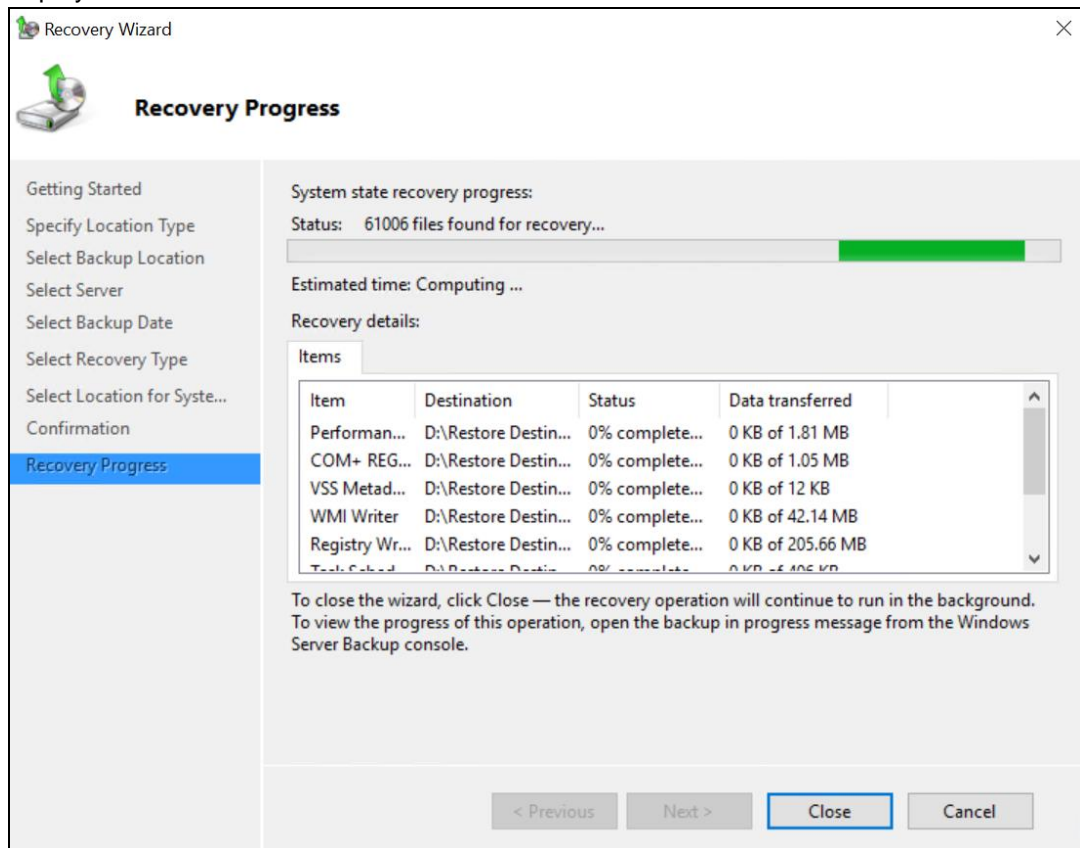


10. On the **Confirmation** page, review the details, and then click **Recover** to restore the specified items.





11. On the **Recovery progress** page, the status and result of the recovery operation are displayed.



**Important:** For restore to **Original location**, the system state recovery cannot be stopped once it is started, or the system could become unbootable.

## 6 Contact Ahsay

### 6.1 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/>

### 6.2 Documentation

Documentations for all Ahsay products are available at:

[https://www.ahsay.com/jsp/en/downloads/ahsay-downloads\\_documentation\\_guides.jsp](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.

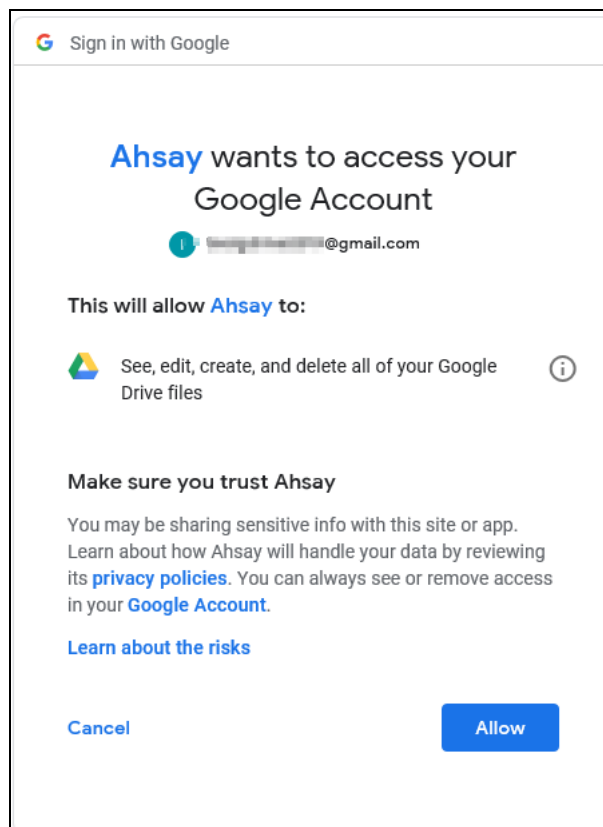
## Appendix

### Appendix A Cloud Storage as Backup Destination:

For most cloud storage provider (e.g. Dropbox, Google Drive ... etc.), you need to allow access 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](#)