



Ahsay Online Backup Manager v8

Microsoft System State 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. 4	New / Modification
30 July 2020	Added Periodic Backup Schedule in Ch. 3; Modified Periodic Data Integrity Check (PDIC) diagram in Ch. 6; Added Ch. 8.3 Configure Backup Schedule for Automated Backup	New / Modifications
23 September 2020	Updated Overview Backup Process and PDIC in Ch. 6	Modifications
25 January 2021	Updated screenshot in Ch. 2.5; Updated login steps in Ch. 5; Updated PDIC diagram in Ch. 6	Modifications
7 April 2021	Updated Ch. 6; Added sub-chapters for the detailed process diagrams in Ch. 6.1, 6.2, 6.2.1, 6.2.2 and 6.3	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	2
1.3	About this document	3
1.3.1	Document Main Part	3
1.3.2	What should I expect from this document?	3
1.3.3	Who should read this document?	3
2	Preparing for Backup and Restore	4
2.1	Hardware Requirement	4
2.2	Software Requirement	4
2.3	Antivirus Exclusion Requirement	4
2.4	AhsayOBM Installation	4
2.5	AhsayOBM Add-on Module Configuration	4
2.6	Backup Quota Requirement	5
2.7	Java Heap Size	5
2.8	License Requirement	5
2.9	Windows Requirement	5
2.10	Temporary Volume	8
3	Best Practices and Recommendations	10
4	Restore Consideration	13
5	Logging in to AhsayOBM	14
5.1	Login to AhsayOBM without 2FA	14
5.2	Login to AhsayOBM with 2FA using authenticator app	16
5.3	Login to AhsayOBM with 2FA using Twilio	19
6	Overview on the Backup Process	21
6.1	Periodic Data Integrity Check (PDIC) Process	22
6.2	Backup Set Index Handling Process	24
6.2.1	Start Backup Job	24
6.2.2	Completed Backup Job	25
6.3	Data Validation Check Process	26
7	Windows XP and Windows Server 2003	27
7.1	Configuring a MS Windows System State Backup Set	27
7.2	Start a Manual Backup	36
7.3	Restore the System State Data	40
7.4	Apply the System State Data	45
8	Windows Server 2008 and Newer Releases	51
8.1	Configuring a MS Windows System State Backup Set	51

8.2	Start a Manual Backup	60
8.3	Configure Backup Schedule for Automated Backup	62
8.4	Restore the System State Data.....	67
8.5	Apply the System State Data	73
9	Contact Ahsay	82
9.1	Technical Assistance	82
9.2	Documentation	82
Appendix	83
Appendix A	Cloud Storage as Backup Destination:	83

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 XP and Windows Server 2003:

<https://msdn.microsoft.com/en-us/library/windows/desktop/aa381498>

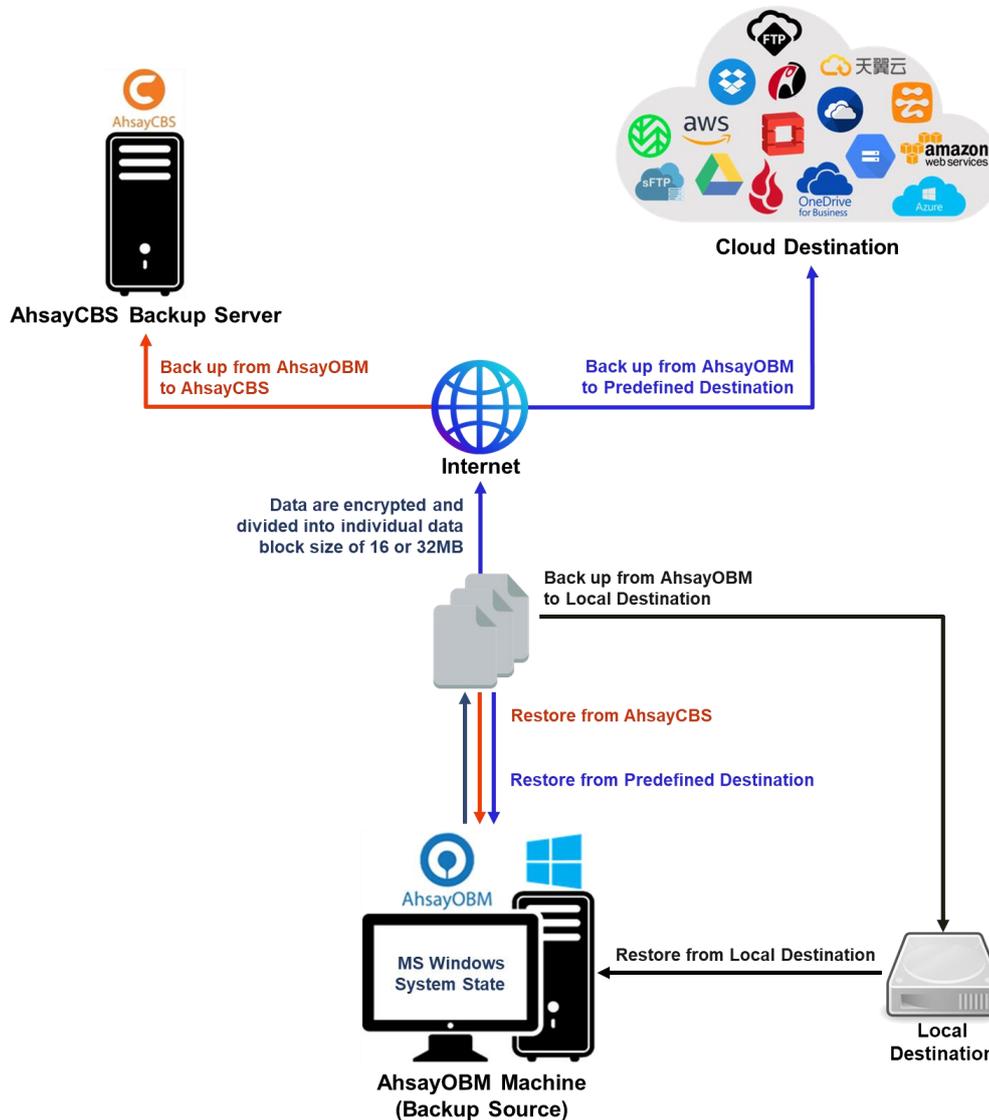
For Windows 2008 and newer releases:

<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.



1.3 About this document

1.3.1 Document Main Part

This document contains information that are essential for understanding the MS Windows System State backup and recovery process.

The document can be divided into three (3) main parts:

Part 1: Preparing for Microsoft System State Backup & Restore

Requirements and Limitation

Requirements on hardware & software for installation and limitation

Best Practice and Recommendation

Items recommended to pay attention to before backup and restore

Part 2: Performing Microsoft System State Backup

Starting AhsayOBM

Login to AhsayOBM

Creating a Backup Set

Create a backup set using AhsayOBM

Running a Backup Set

Run a backup set using the AhsayOBM

Part 3: Restoring Microsoft System State Backup

Restoring a Backup Set using AhsayOBM

Restore a backup using the AhsayOBM and User Web Console

1.3.2 What should I expect from this document?

After reading through this documentation, you can expect to have sufficient knowledge to set up your system to backup Microsoft System State on AhsayOBM, as well as to carry out an end-to-end backup and restore process.

1.3.3 Who should read this document?

This documentation is intended for backup administrators and IT professionals who are responsible for the Microsoft System State backup and restore.

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

The screenshot displays the 'Backup Client Settings' configuration page in AhsayOBM. The interface includes a sidebar with navigation options: Backup Set, Settings, Report, Statistics, and Effective Policy. The main content area is titled 'Settings of the client backup agent for this user.' and contains the following sections:

- Backup Client:** Radio buttons for 'AhsayOBM User' (selected) and 'AhsayACB User'.
- Add-on Modules:** A grid of checkboxes for various backup modules. The 'Windows System State Backup' module is checked and highlighted with a red rectangular box.

Module Name	Enabled
Microsoft Exchange Server	<input type="checkbox"/>
MySQL Database Server	<input type="checkbox"/>
Lotus Domino	<input type="checkbox"/>
Windows System Backup	<input type="checkbox"/>
VMware	<input type="checkbox"/>
Microsoft Exchange Mailbox	<input type="checkbox"/>
NAS - QNAP	<input type="checkbox"/>
Mobile (max. 10)	<input checked="" type="checkbox"/>
Volume Shadow Copy	<input checked="" type="checkbox"/>
OpenDirect / Granular Restore	<input type="checkbox"/>
MariaDB Database Server	<input type="checkbox"/>
Microsoft SQL Server	<input checked="" type="checkbox"/>
Oracle Database Server	<input type="checkbox"/>
Lotus Notes	<input type="checkbox"/>
Windows System State Backup	<input checked="" type="checkbox"/>
Hyper-V	<input type="checkbox"/>
ShadowProtect System Backup	<input type="checkbox"/>
NAS - Synology	<input type="checkbox"/>
Continuous Data Protection	<input type="checkbox"/>
In-File Delta	<input checked="" type="checkbox"/>
Office 365 Backup	<input type="checkbox"/>

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.

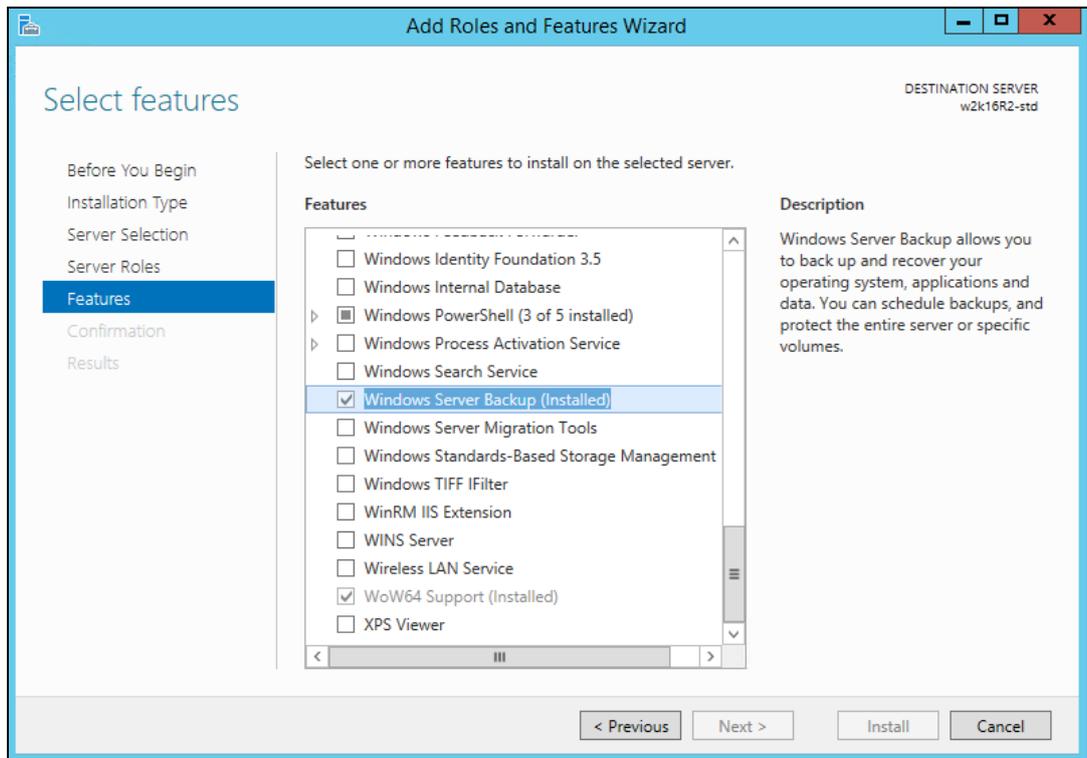
2.9 Windows Requirement

▶ 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.

- **NTBackup**

NTBackup must be installed on the computer to be backed up.

This can be confirmed either by searching if `ntbackup.exe` is found under `C:\WINDOWS`, or running the following command in an administrative command prompt:

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\support>ntbackup
```

You can verify if ntbacup is installed or not by the following interface pop out or not.



• **System Volume**

The system volume must be formatted with NTFS.

• **Latest Service Packs from Microsoft**

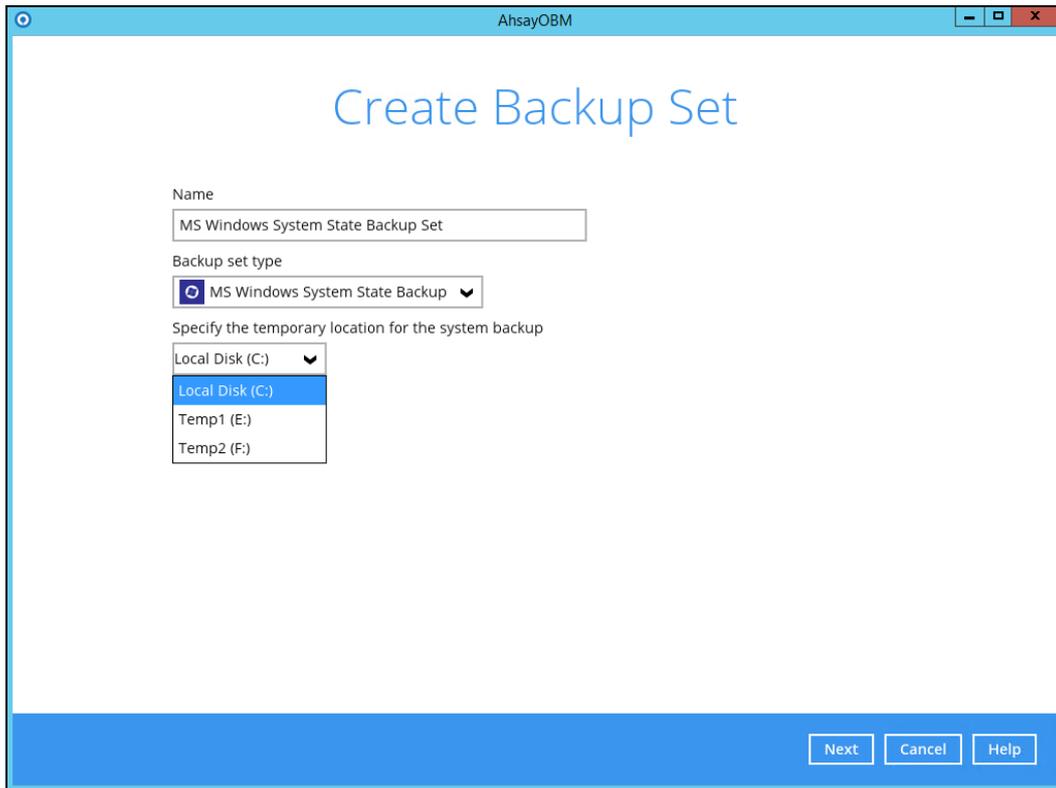
Ensure that you have the latest service packs installed. Updates to the Windows operating system improve its performance and resolve known issues with Windows Server Backup.

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 for backup and restore for these 2 Windows platforms.

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](#)

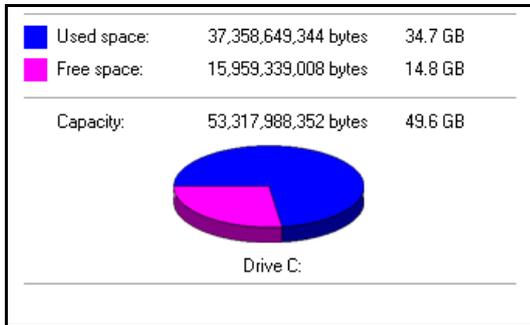
⦿ Disk Space Available in Temporary Storage Location

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 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 E:).

The screenshot shows the configuration window for a Microsoft Windows System State backup. The 'General' tab is selected, and the 'Specify the temporary location for the system backup' dropdown is set to 'Temp1 (E:)', which is highlighted as the recommended configuration.

NOTE

Kindly noted that 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.

4 Restore Consideration

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>

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:

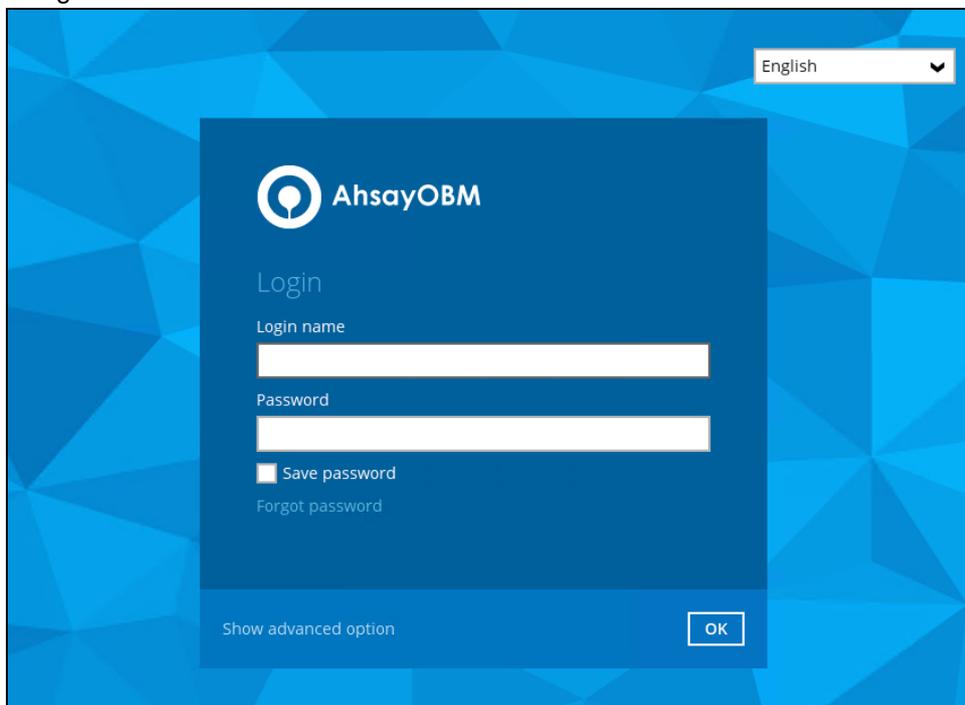
- [Login without 2FA](#)
- [Login with 2FA using authenticator app](#)
- [Login with 2FA using Twilio](#)

5.1 Login to AhsayOBM without 2FA

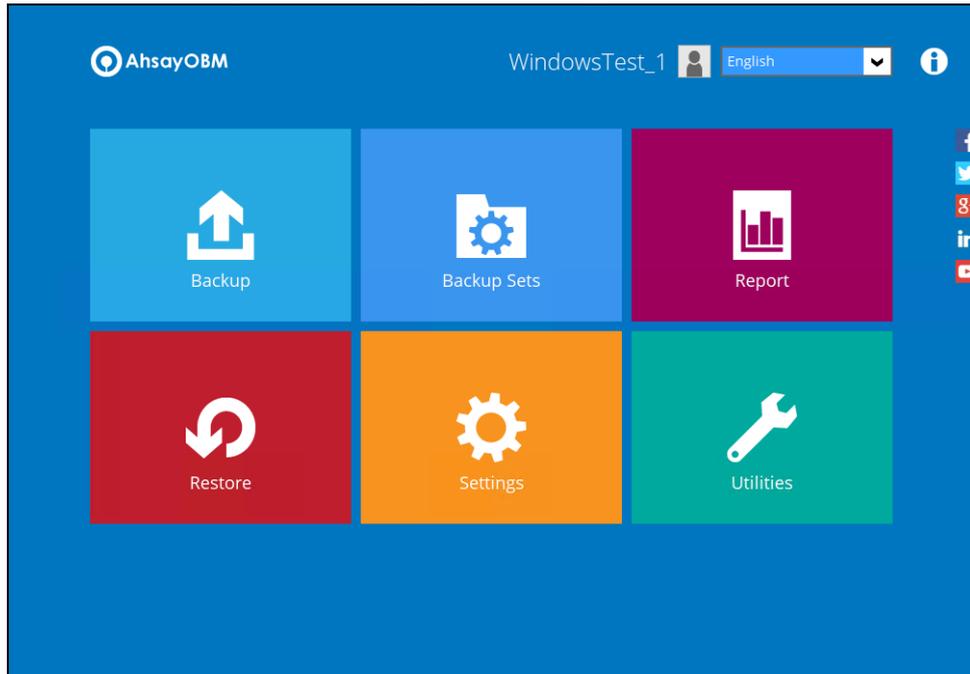
1. Log in to the AhsayOBM application user interface. Double-click the AhsayOBM desktop icon to launch the application.



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'. 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 labeled 'Forgot password'. At the bottom left, there is a link labeled '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 screen. It features a blue background with a white AhsayOBM logo and the text 'AhsayOBM'. Below the logo, the word 'Login' is displayed. There are two input fields for '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.

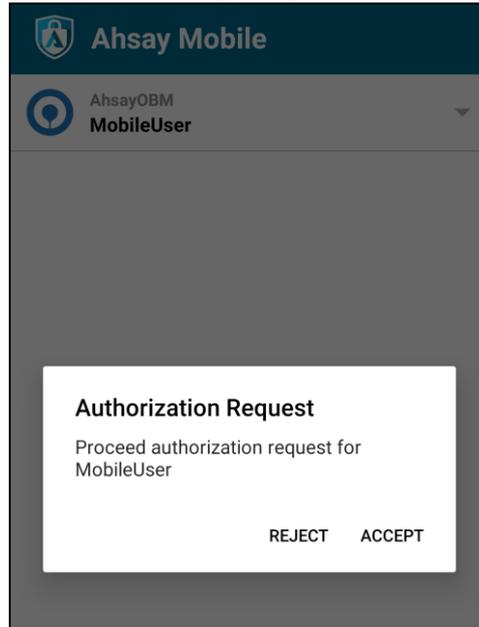
Two-Factor Authentication

Please approve notification request in one of registered Authenticator App.

⌚ Waiting for response (00:04:36)

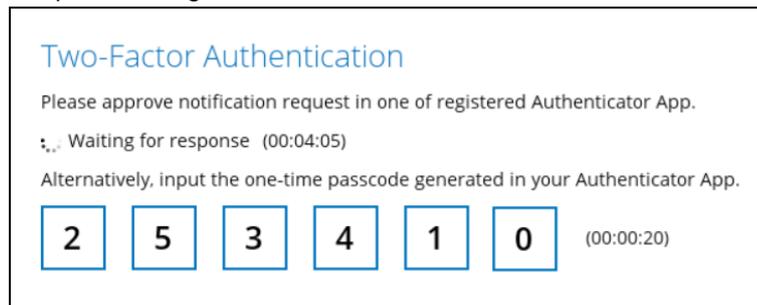
[Authenticate with one-time password](#)

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

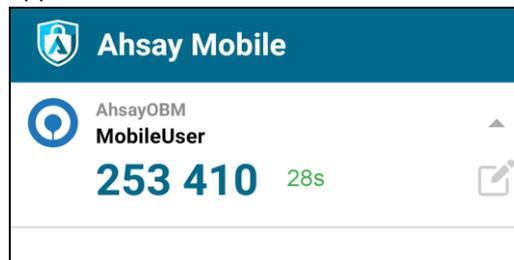


- TOTP

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.

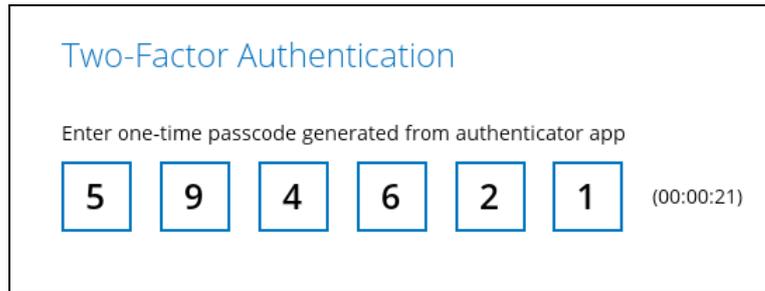


Example of the one-time passcode generated in the Ahsay Mobile app.

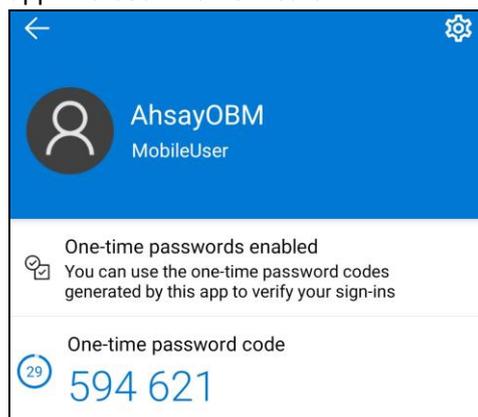


➤ TOTP only

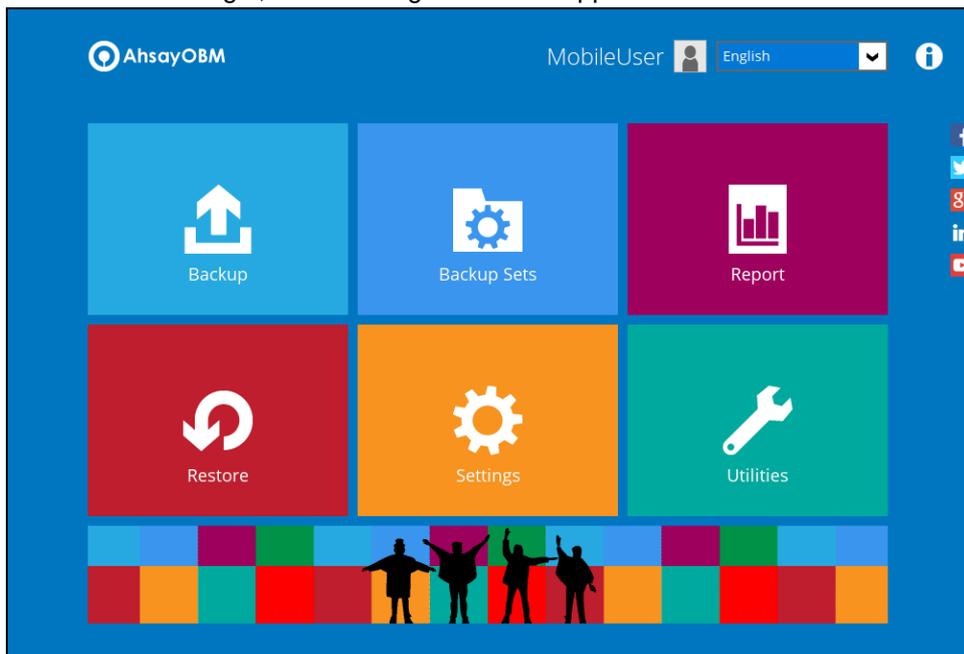
Enter the one-time passcode generated by the authenticator app to complete the login.



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 dialog box. It has a blue background with a white login form in the center. The form includes the AhsayOBM logo and name, a 'Login' heading, and two input fields for 'Login name' and 'Password'. There is a 'Save password' checkbox and 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. Select your phone number.

The image shows the Two-Factor Authentication dialog box. It has a white background with a blue header 'Two-Factor Authentication'. Below the header, it says 'Please select phone number to receive passcode via SMS message to continue login.' There are three radio button options: '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

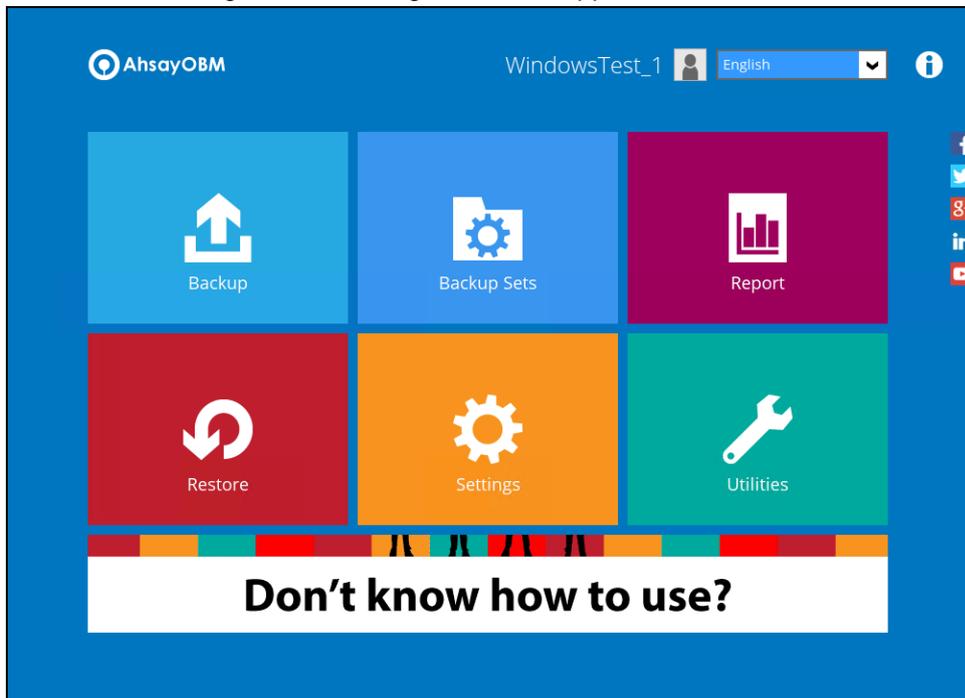
SMS message with a passcode was already sent to the phone number Philippines (+63) - *****6123
Please enter the passcode to continue login.

EUVS - (00:03:59)

[Resend passcode](#)

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

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



6 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 \(Step 11\)](#)



6.1 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 mod 5 = 2

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

In this example:

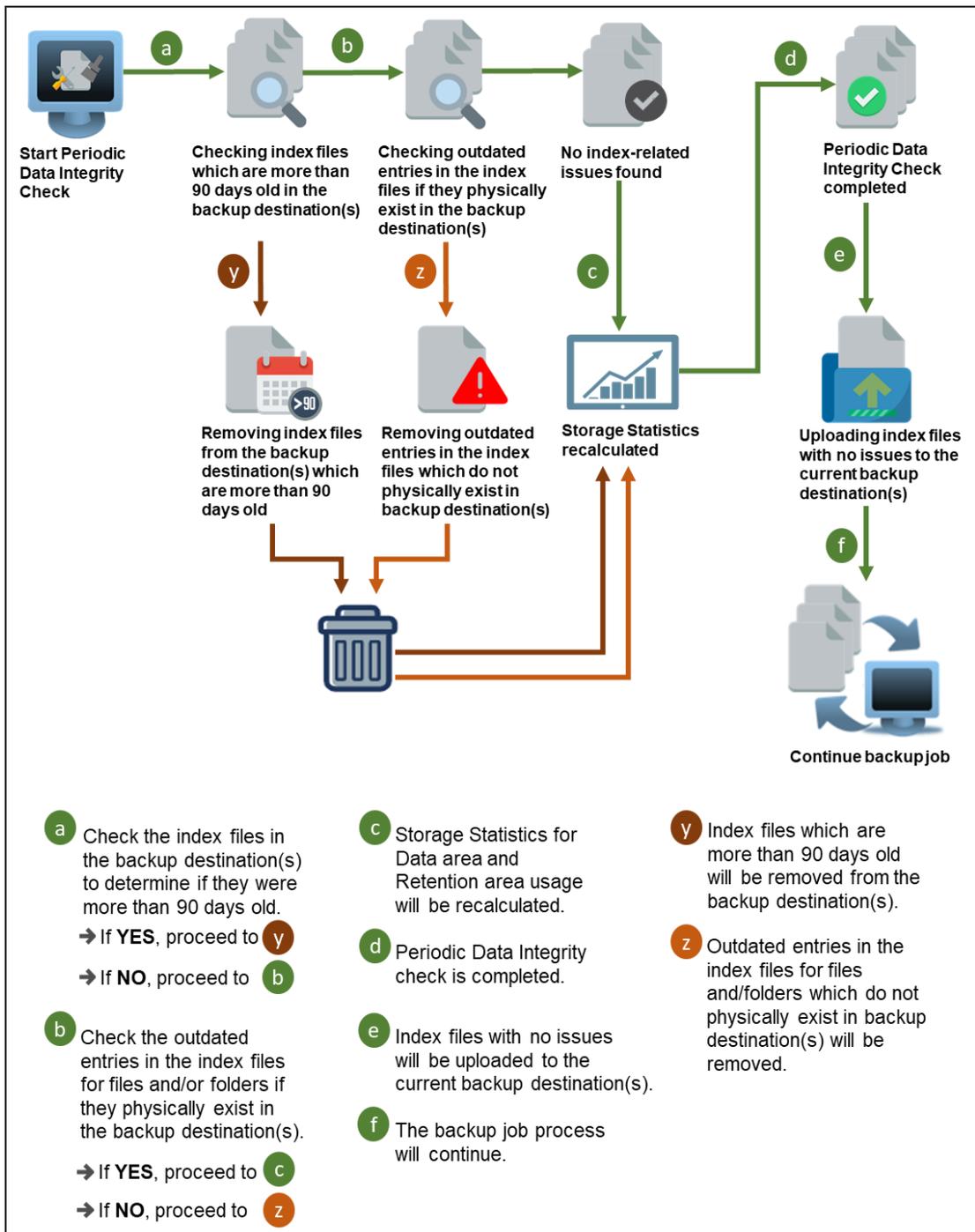
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

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:

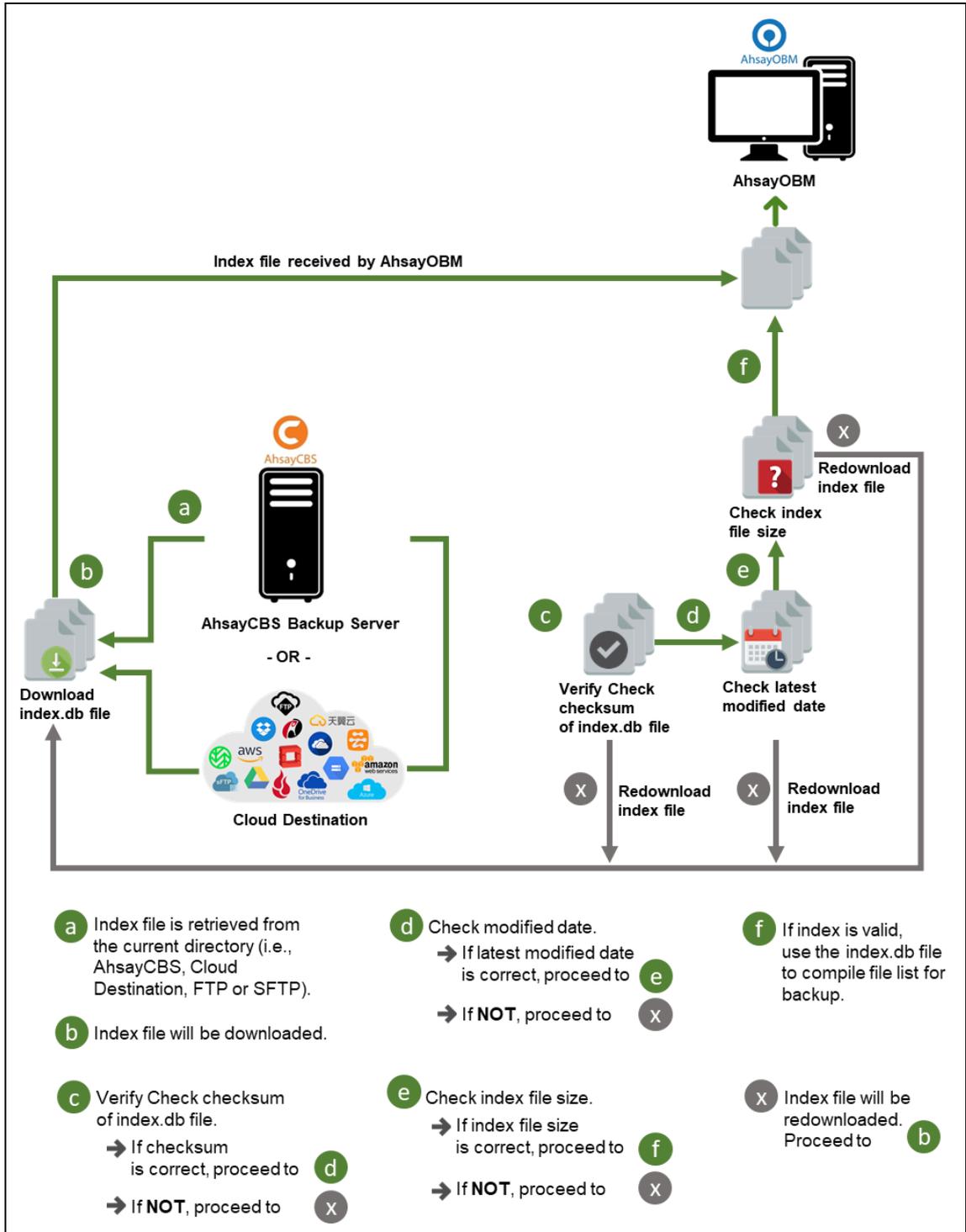
1. If AhsayOBM was upgraded to v8.5 (or above) from an older version v6, v7, or pre-8.3.6.0 version. In this case, the PDIC job will run on the first backup job after upgrade.
2. If backup jobs for a backup set are not run on a regular daily backup schedule (for example: on a weekly or monthly schedule),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



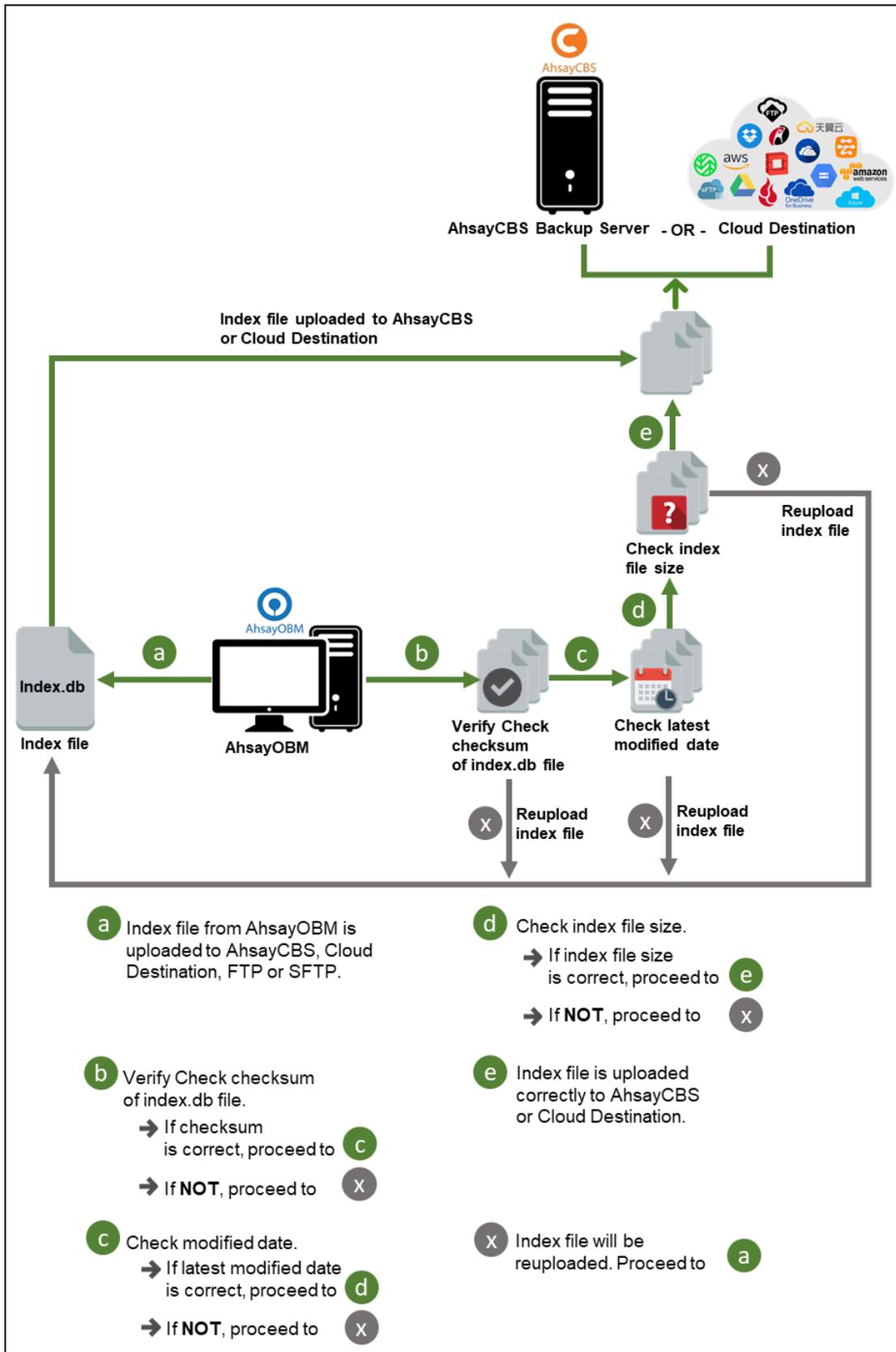
6.2 Backup Set Index Handling Process

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.

6.2.1 Start Backup Job

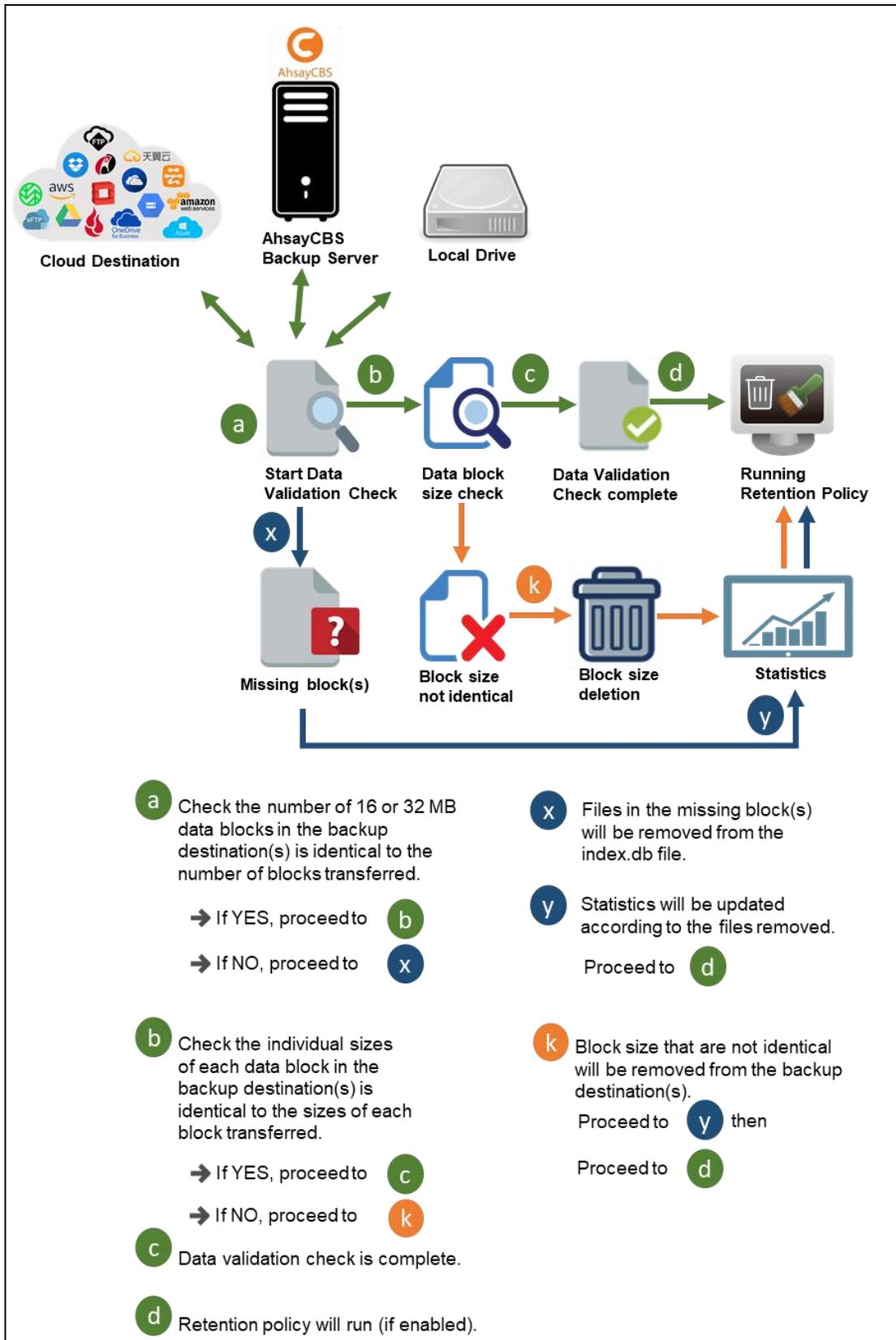


6.2.2 Completed Backup Job



6.3 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.

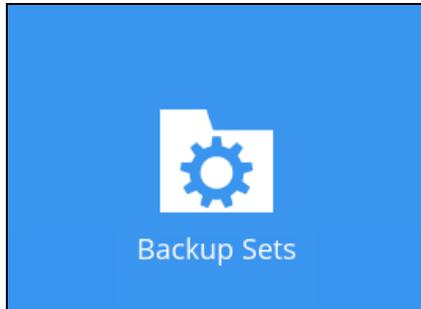


7 Windows XP and Windows Server 2003

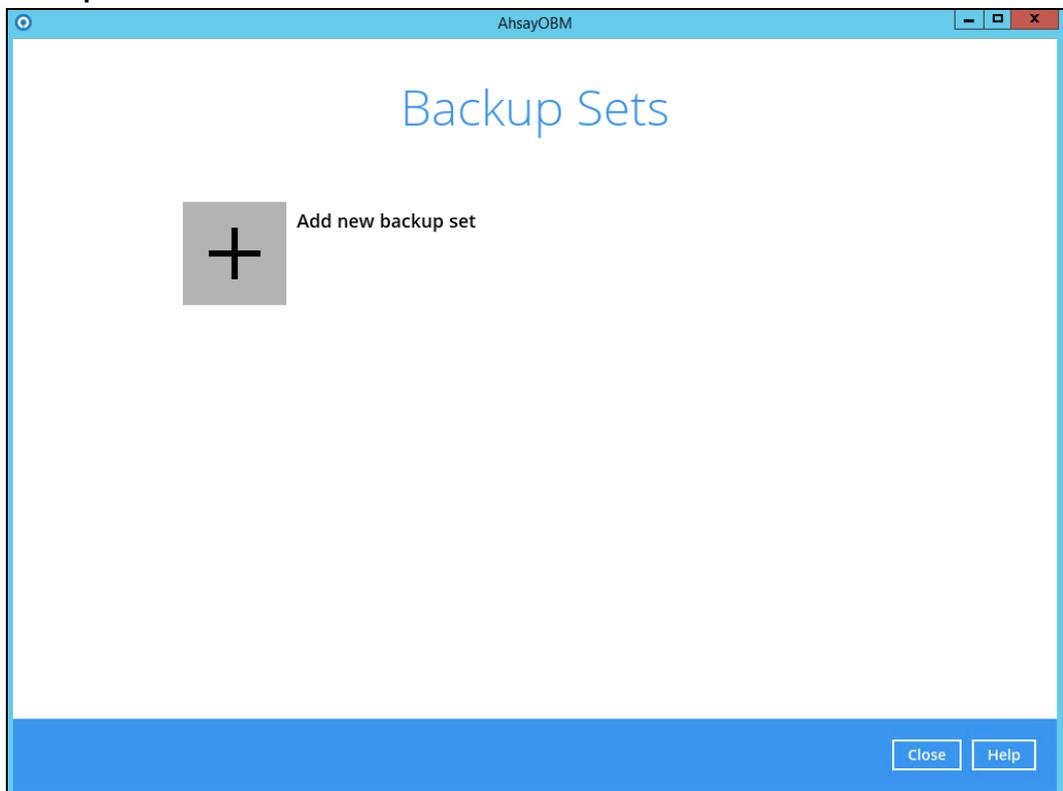
7.1 Configuring a MS Windows System State Backup Set

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 Set

Backup set type
MS Windows System State Backup

Specify the temporary location for the system backup
Temp1 (E:)

Next Cancel Help

AhsayOBM

Create Backup Set

Name
MS Windows System State Backup Set

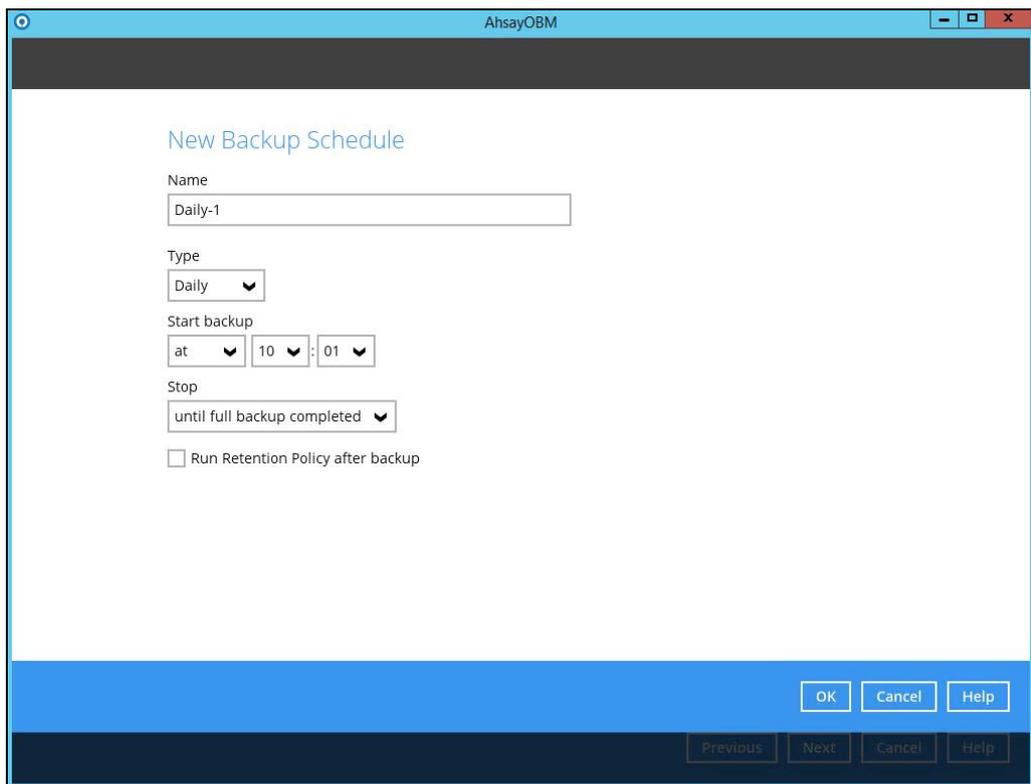
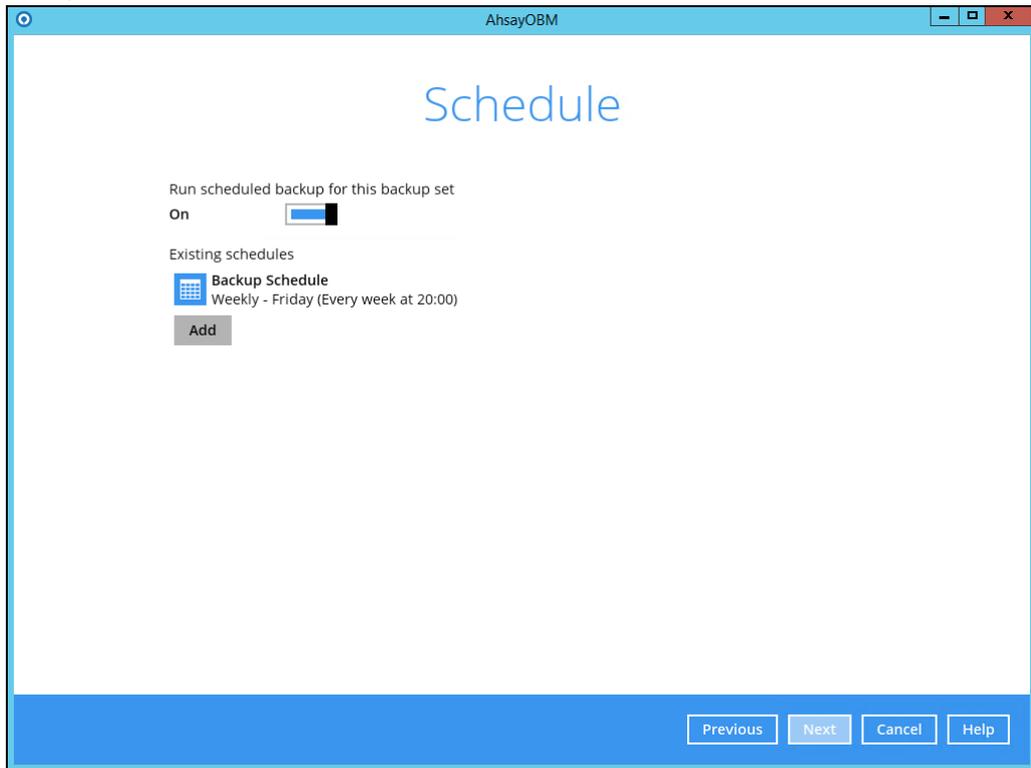
Backup set type
MS Windows System State Backup

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

Next Cancel Help

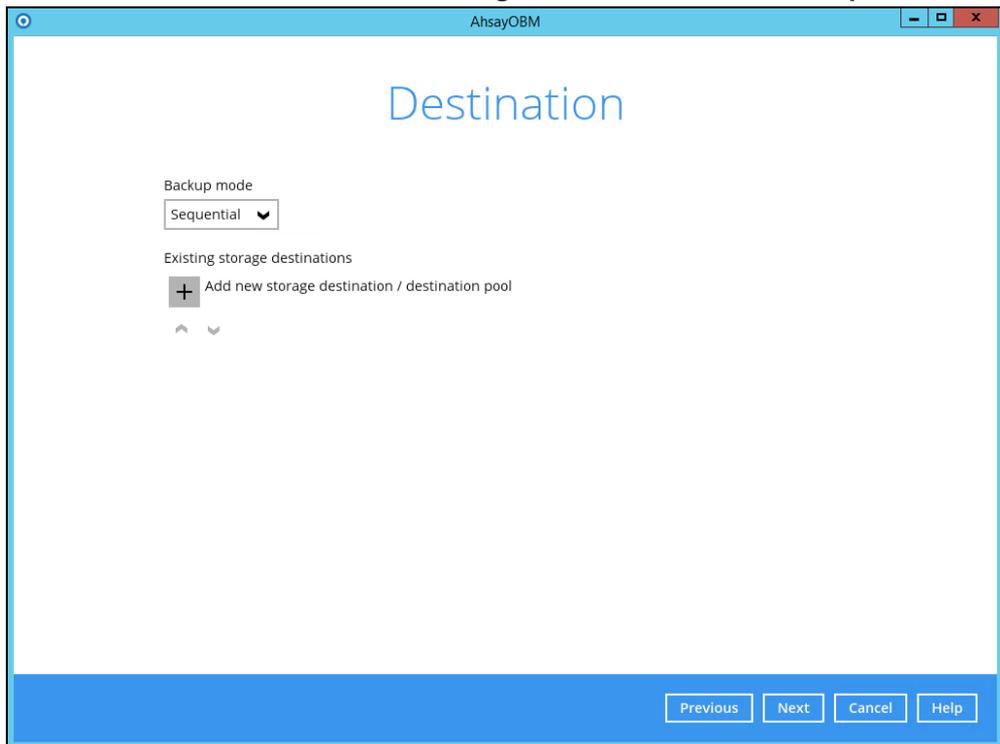
4. In the **Schedule** window, configure a backup schedule for backup job to run automatically at your specified time interval.

As you can see, there's already a default Backup Schedule which is set weekly, every Friday around 20:00PM. Click **Add** to add a new schedule.



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

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



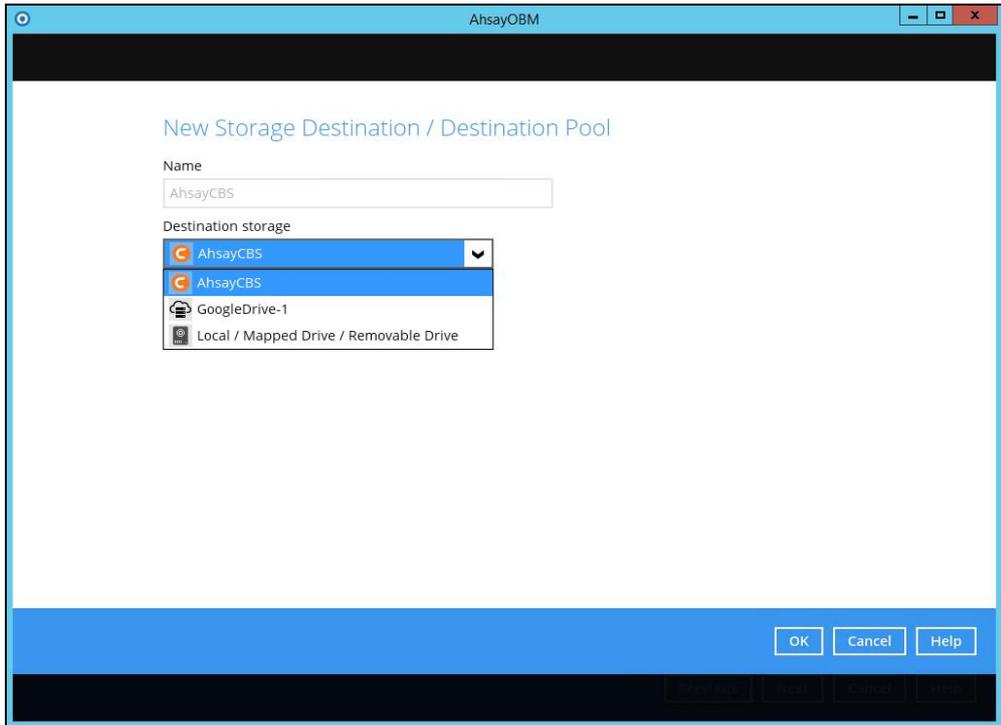
NOTE

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

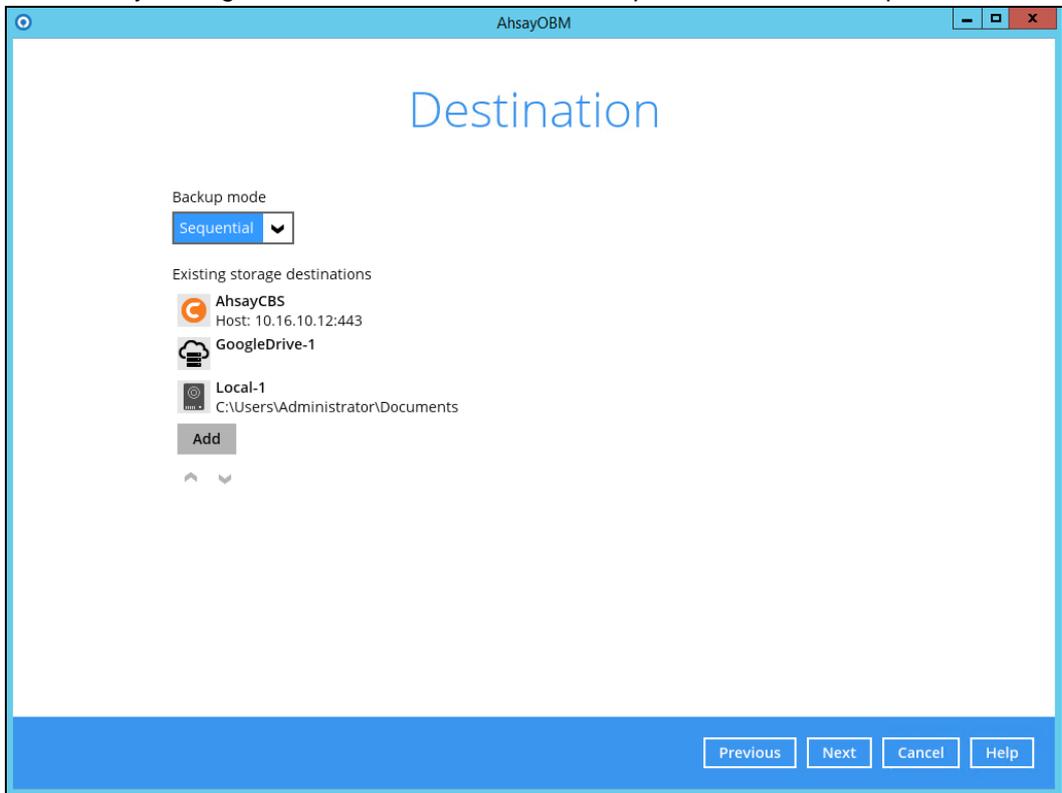
[FAQ: Frequently Asked Questions on Backup Destination](#)

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

- Select the **Destination storage**.



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.

7. 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.

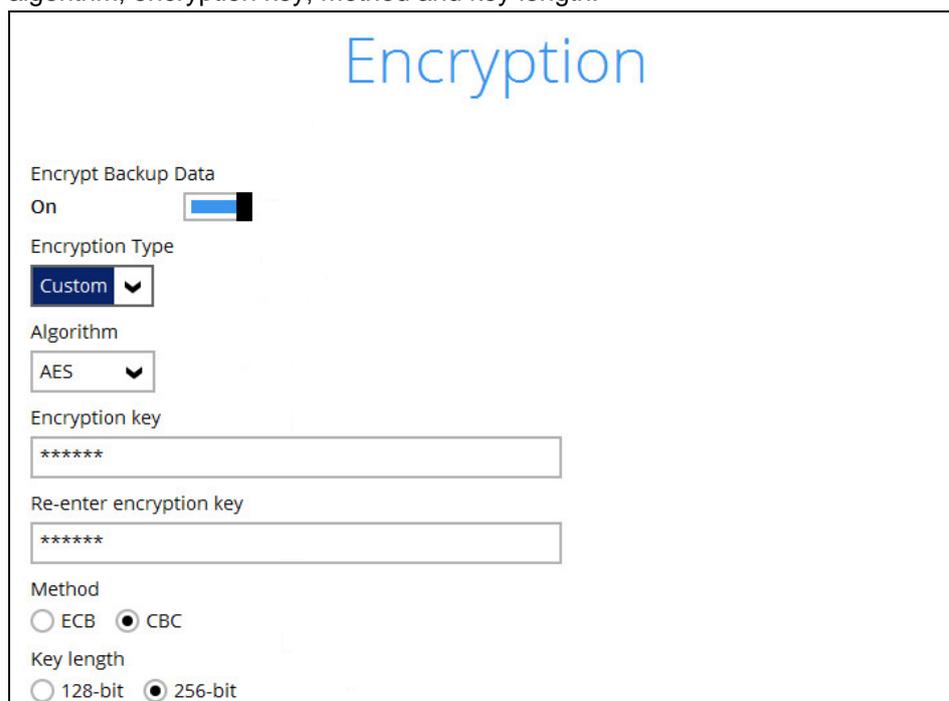


The screenshot shows the 'Encryption' window with the following settings:

- Encrypt Backup Data:** On (checkbox checked)
- Encryption Type:** Default (dropdown menu open, showing options: Default, User password, Custom)

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.



The screenshot shows the 'Encryption' window with the following settings:

- Encrypt Backup Data:** On (checkbox checked)
- Encryption Type:** Custom (dropdown menu)
- Algorithm:** AES (dropdown menu)
- Encryption key:** [*****] (text input field)
- Re-enter encryption key:** [*****] (text input field)
- Method:** ECB CBC
- Key length:** 128-bit 256-bit

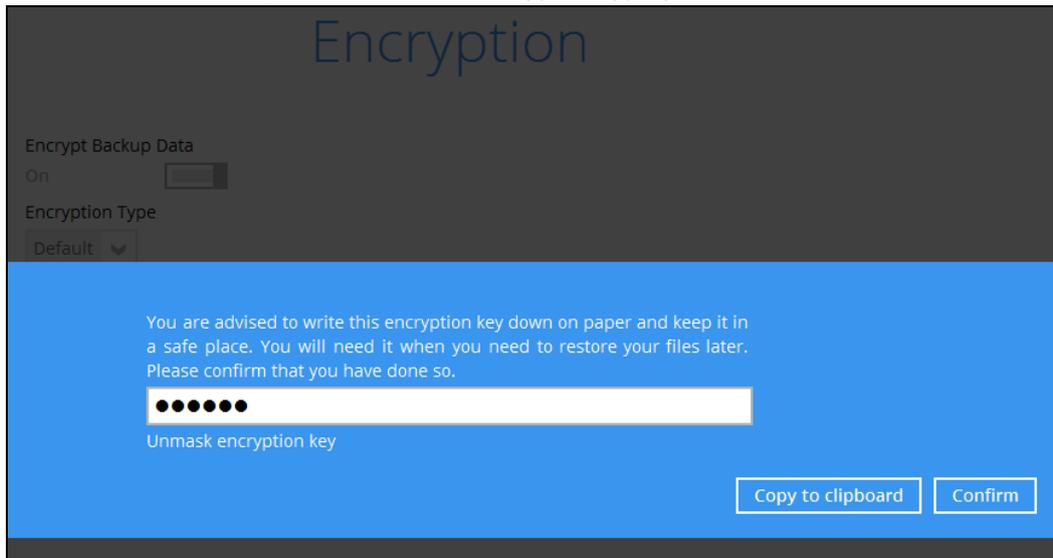
NOTE

For best practice on managing your encryption key, refer to this link:

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

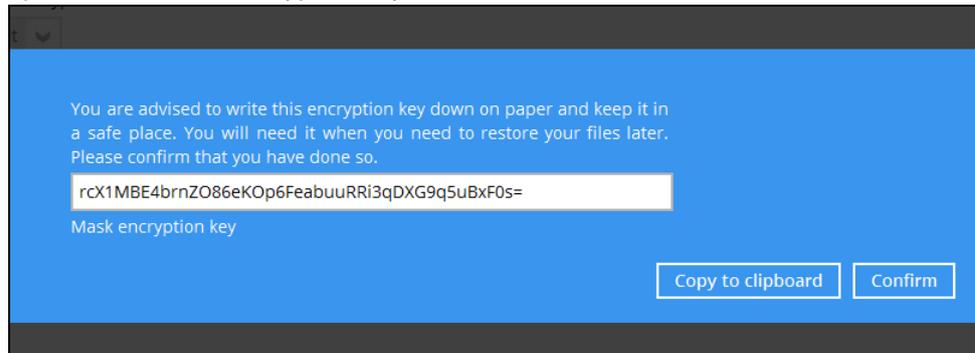
Click **Next** when you are done setting.

8. 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.



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.
9. If you have enabled the **Schedule** feature in the previous step, the following window will be shown. 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.

AhsayOBM

Windows User Authentication

Domain Name (e.g. Ahsay.com) / Host Name
child.csv2012.local

User name
Administrator

Password
●●●●●●●●

Previous Next Cancel Help

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

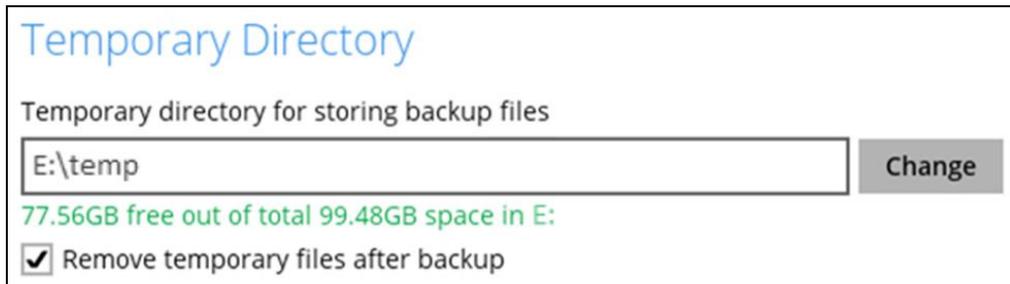
AhsayOBM

Congratulations!

"MS Windows System State Backup Set" is successfully created.

Backup now Close

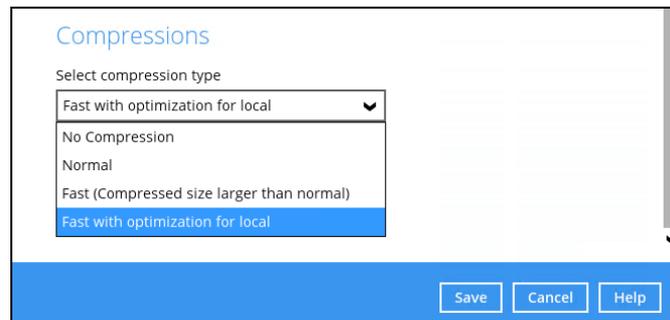
11. Based on [Best Practices and Recommendations](#), it is highly recommended to set the temporary directory to another location other than Drive C: (e.g. Drive E:). To do this, go to **Backup Sets > Others > Temporary Directory** and click the **Change** button to browse for another location.



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

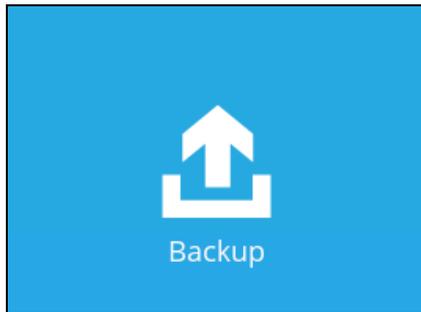
Go to **Others > Compressions**, then select from the following:

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

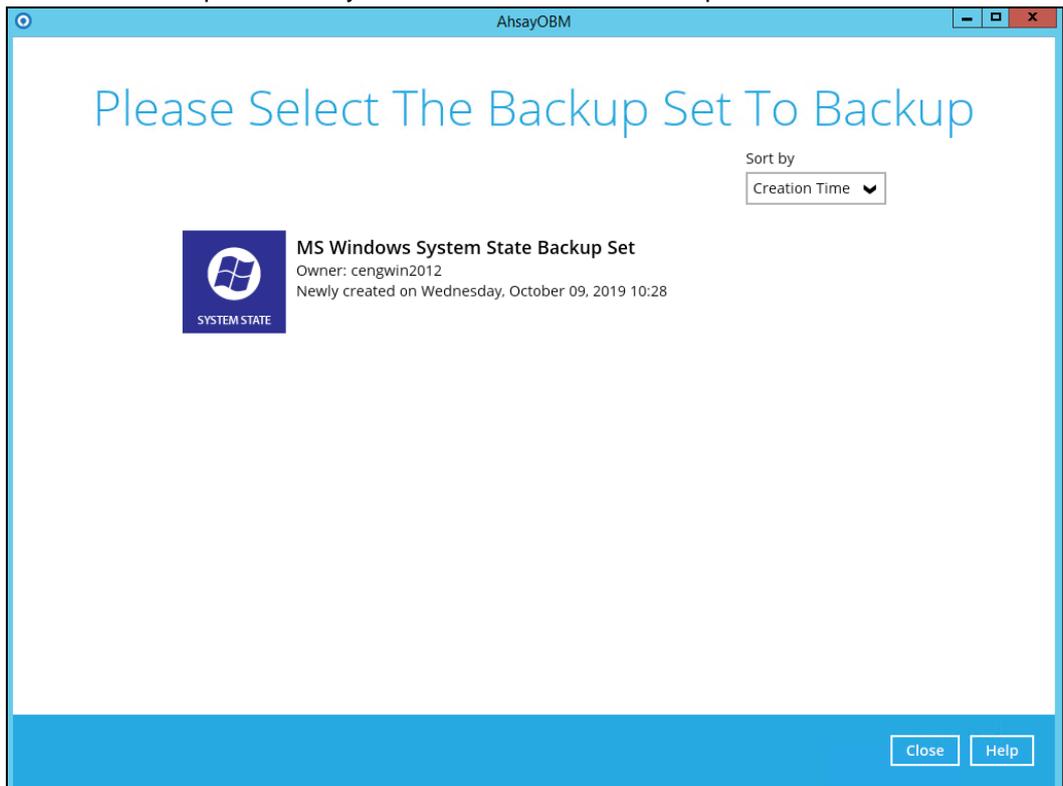


7.2 Start a Manual Backup

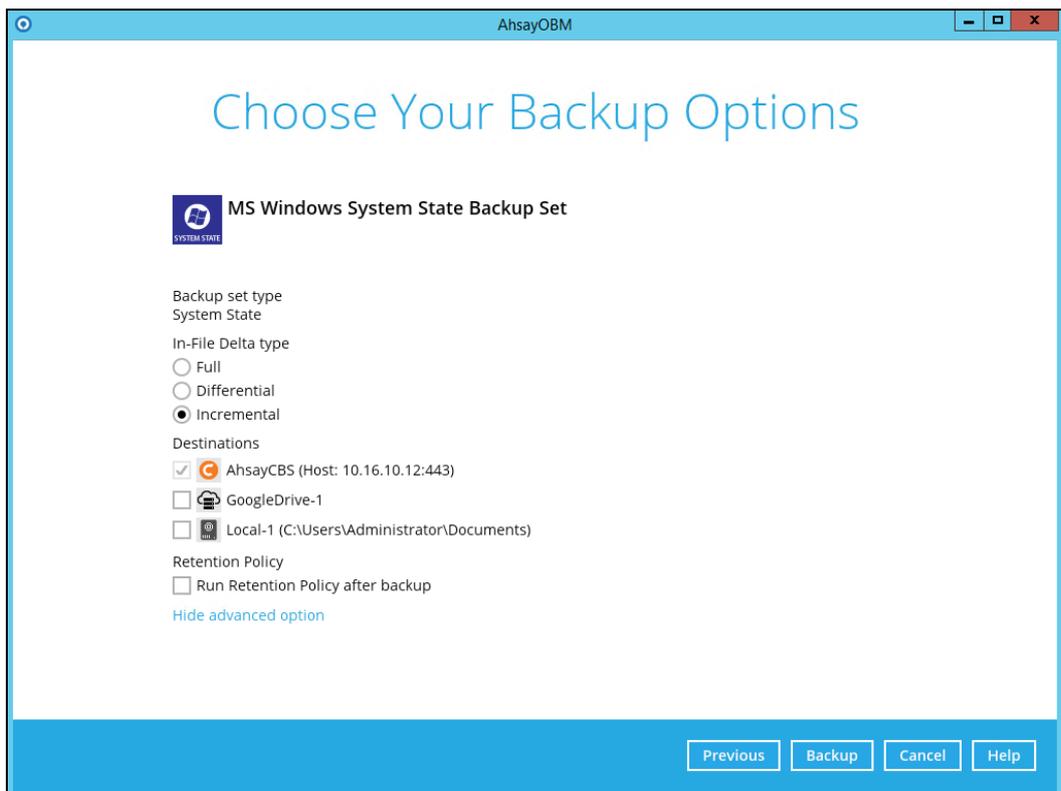
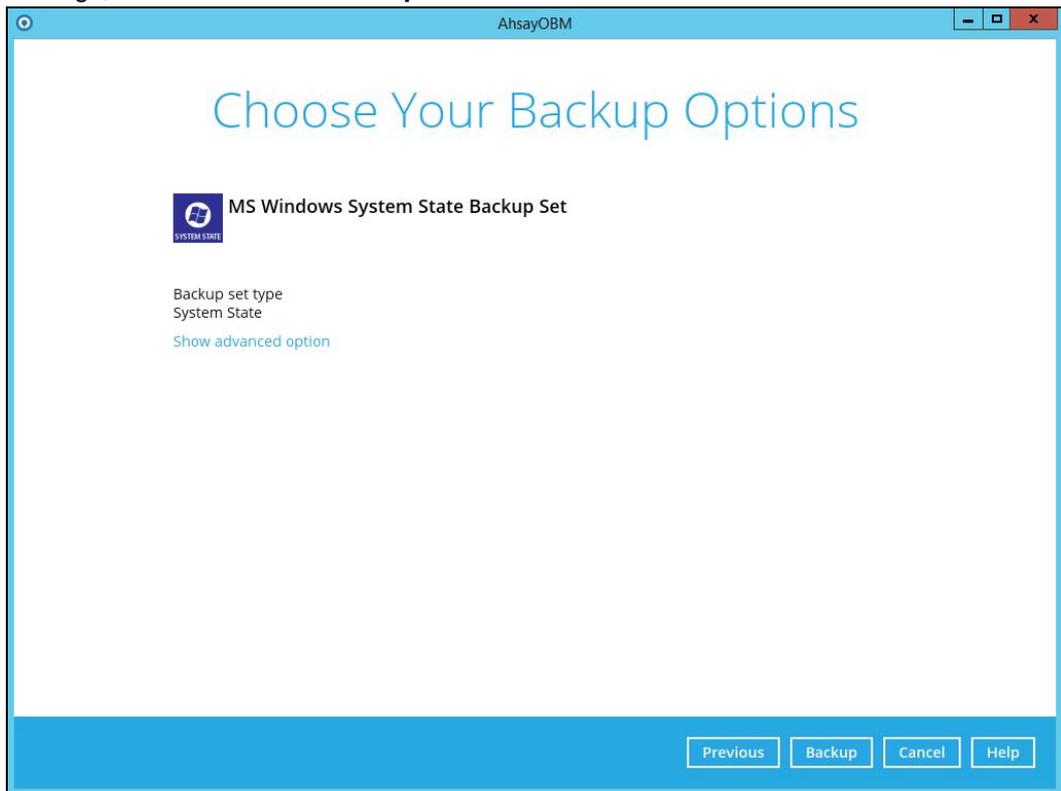
1. Click the **Backup** icon on the main interface of AhsayOBM.



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

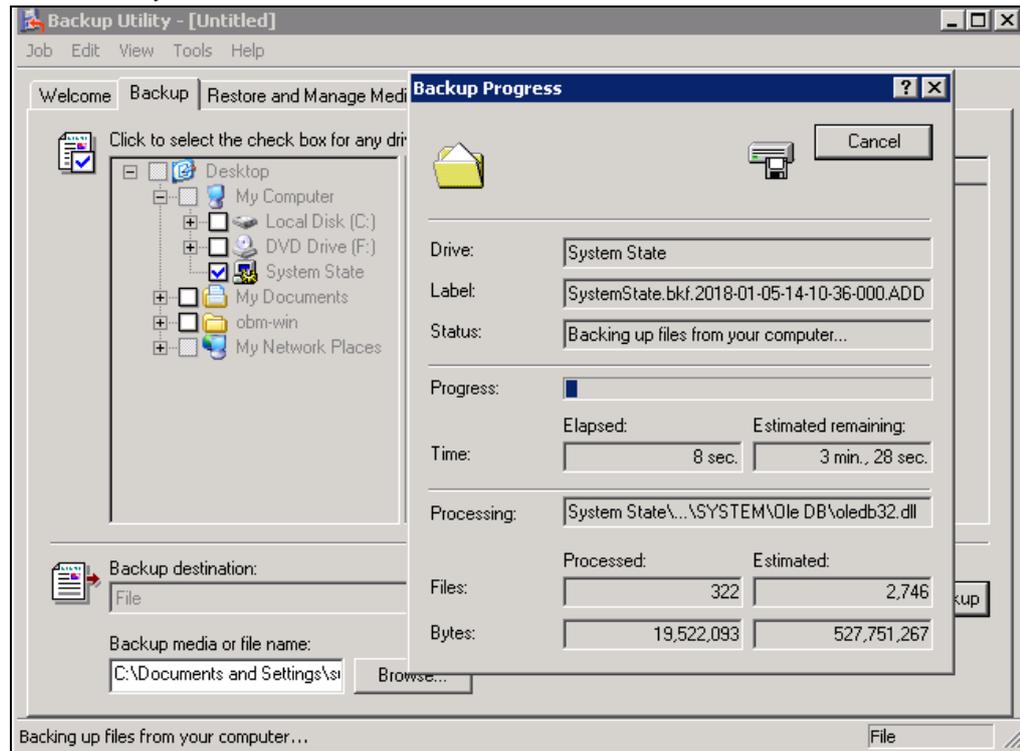


3. If you would like to modify the In-File Delta type, Destinations and Retention Policy Settings, click **Show advanced option**.



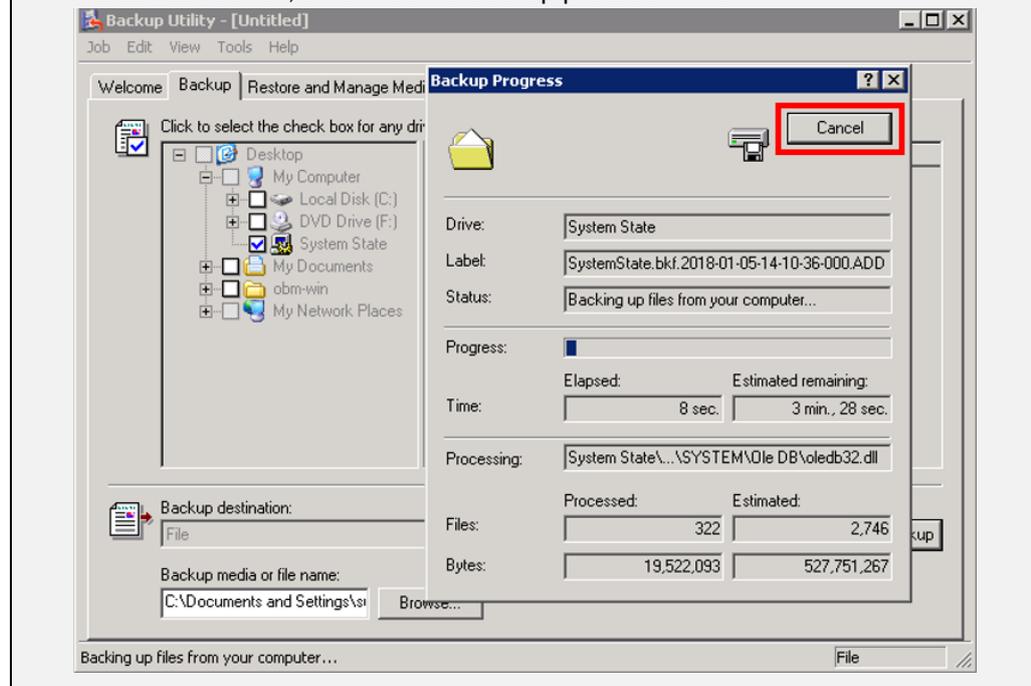
4. Click **Backup** to start the backup job. The NTBackup interface will be displayed temporarily when creating the system state .bkf file. The window will close

automatically afterward.

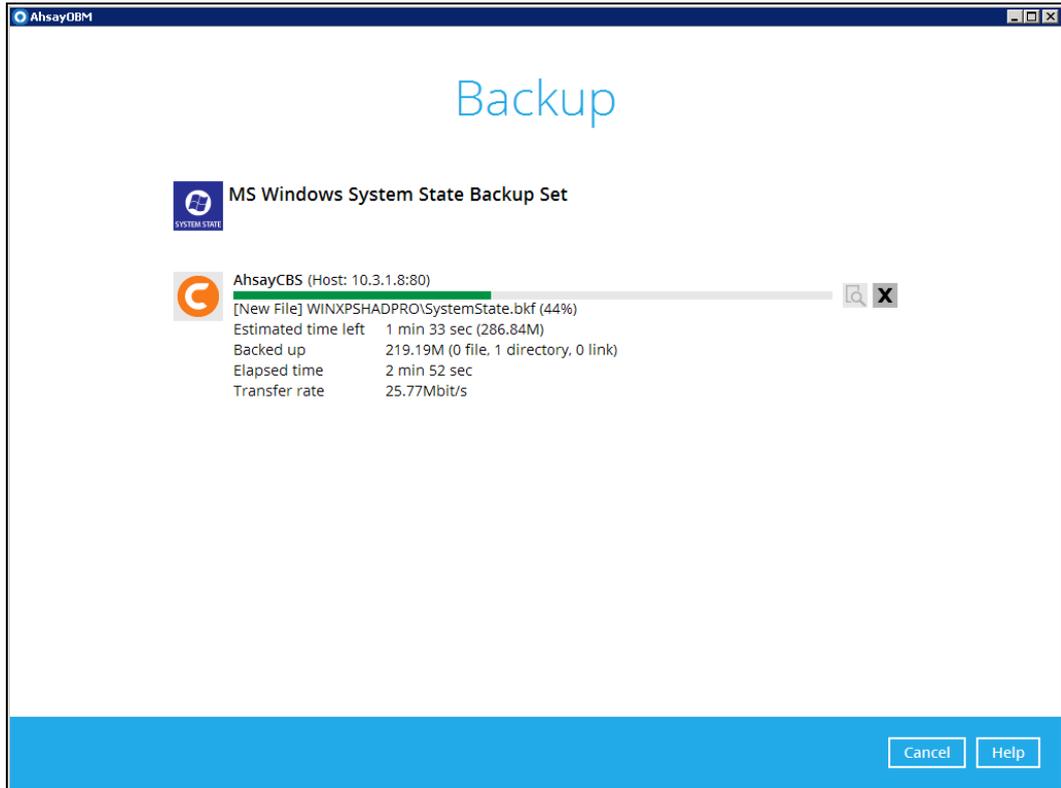


NOTE

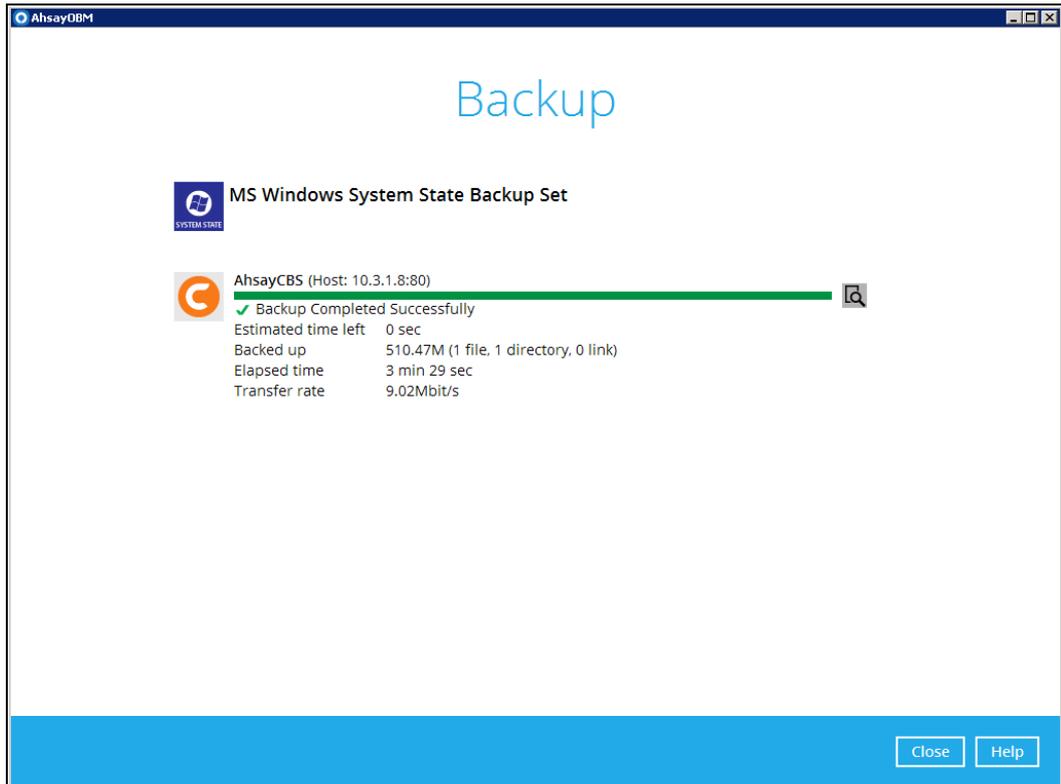
- Kindly noted that the NTBackup interface will only be displayed during manual backup process, it will NOT be shown during a scheduled backup or a continuous backup.
- During the process of creating the system state .bkf file, please do **NOT** click on the **Cancel** button, otherwise the backup process will fail.



5. AhsayOBM wil start to backup the system state .bkf file.



6. The following screen is displayed when the system state data are backed up successfully.

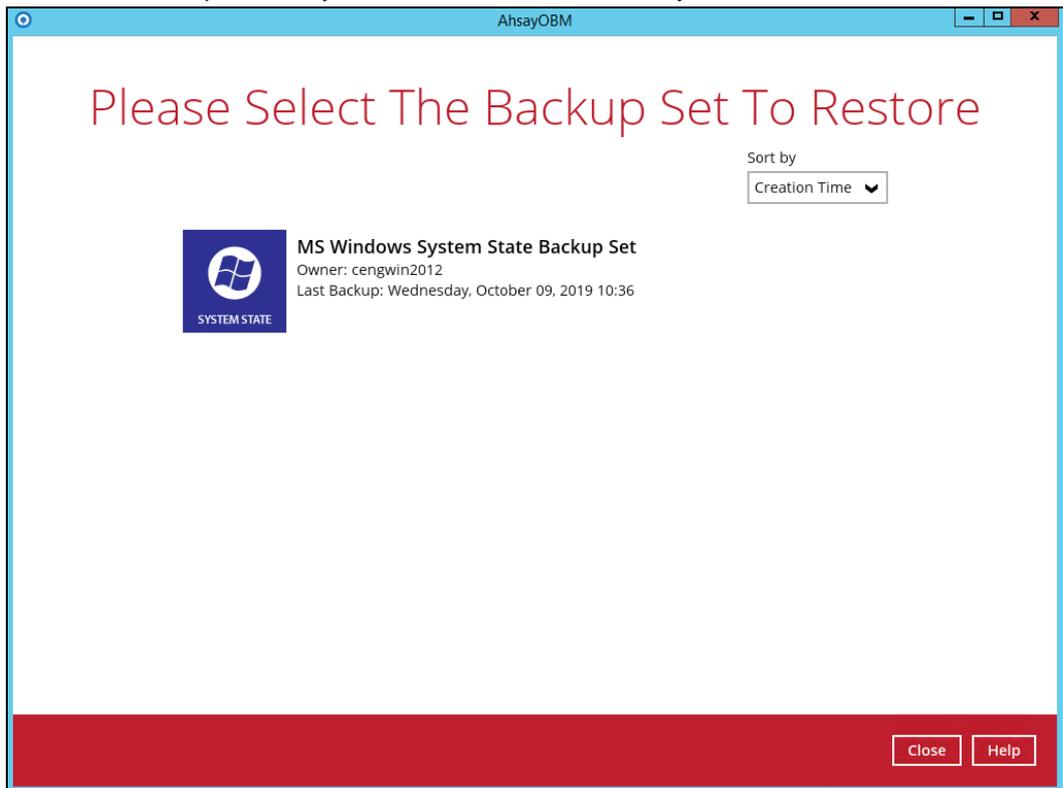


7.3 Restore the System State Data

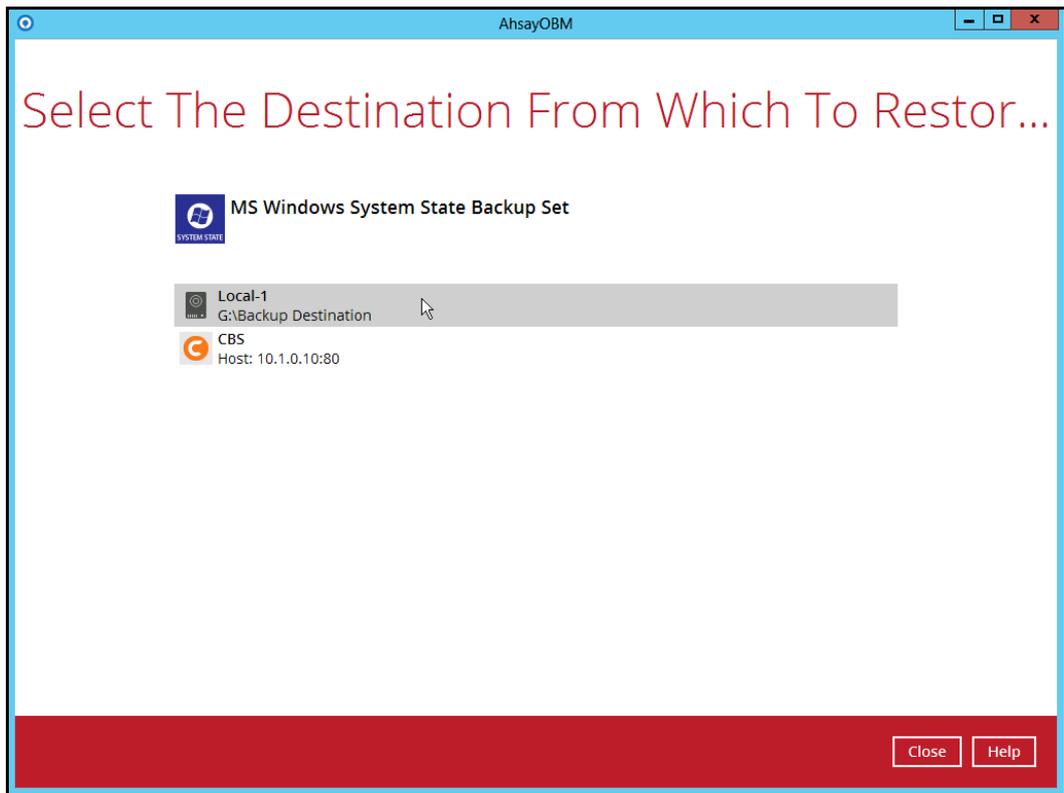
1. Click the **Restore** icon on the main interface of AhsayOBM.



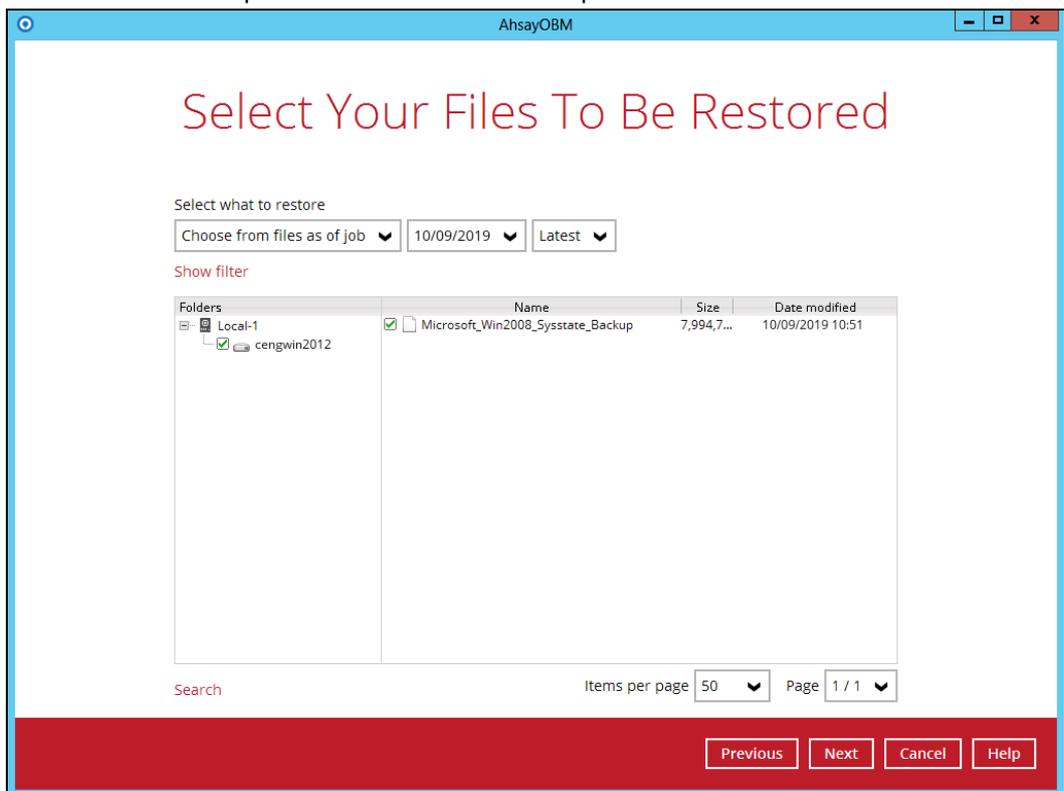
2. Select the backup set that you would like to restore the system state data from.



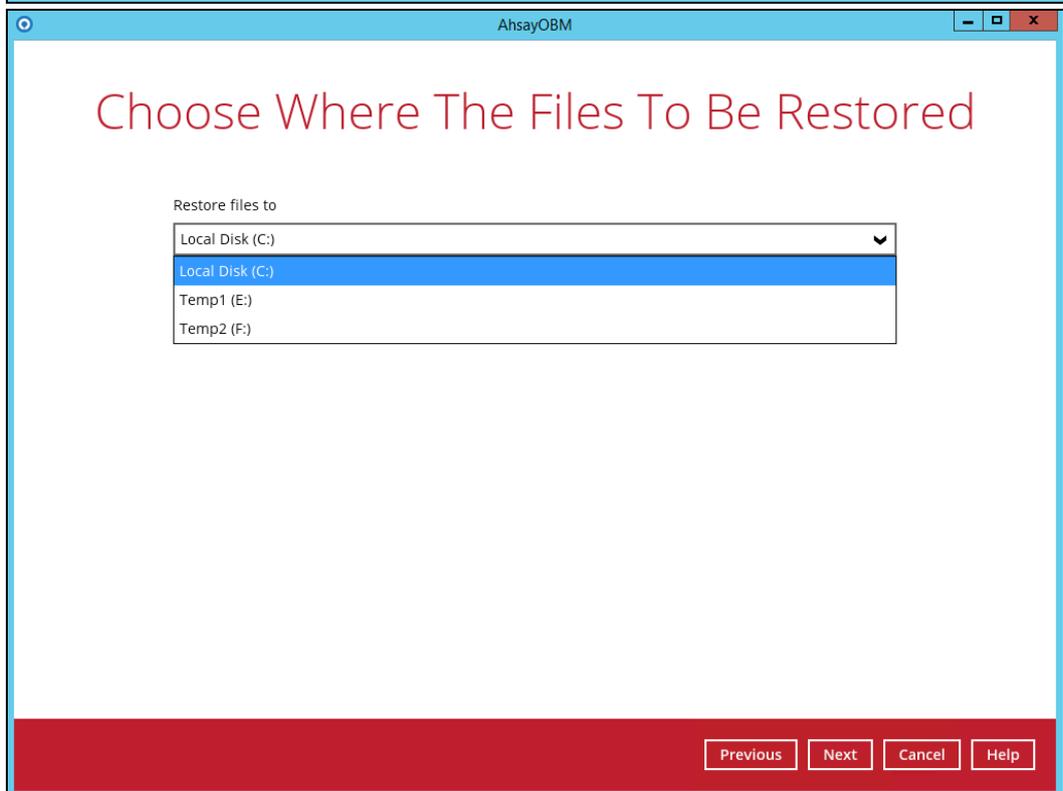
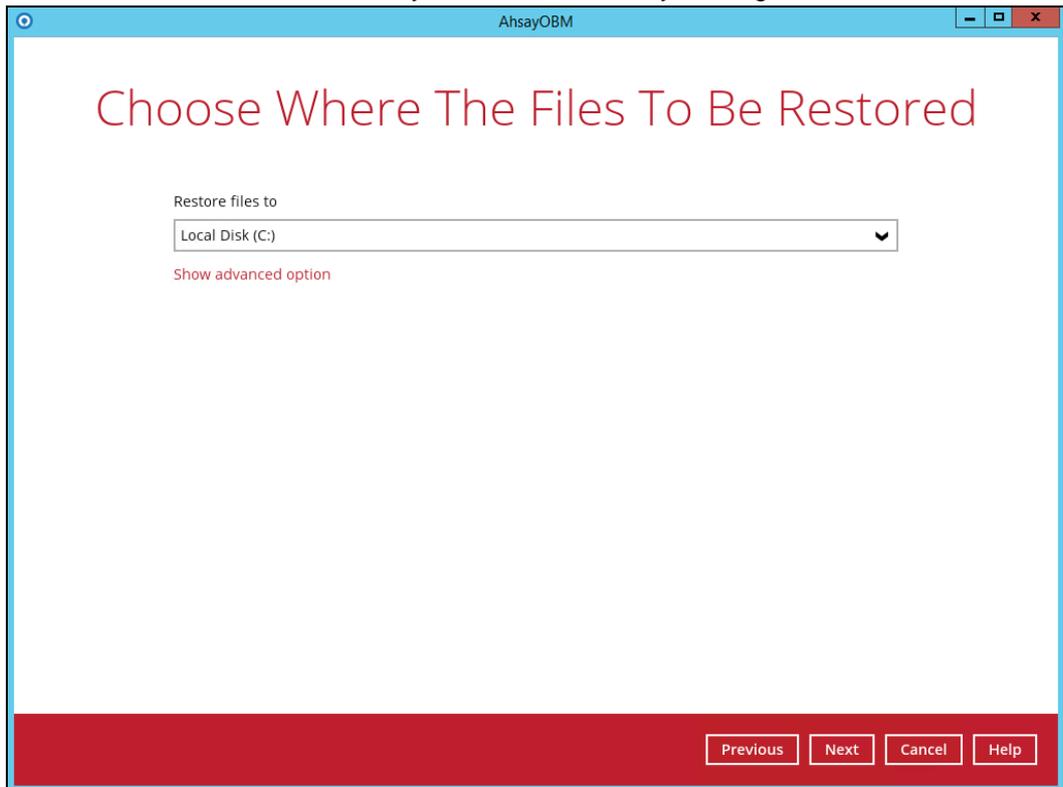
3. Select the backup destination that contains the system state data that you would like to restore.



4. 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.



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



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

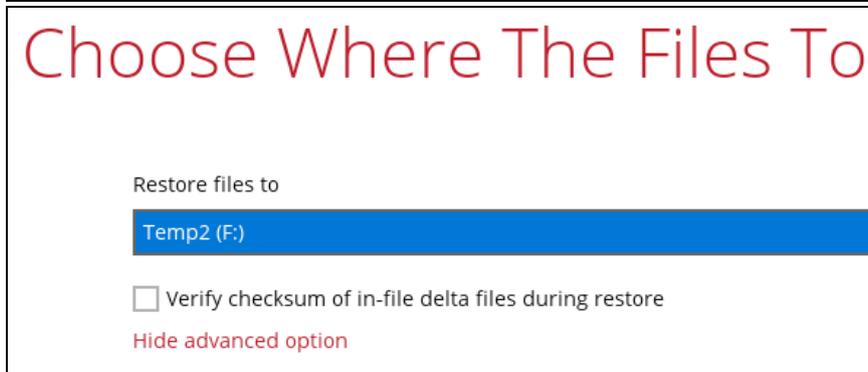


Choose Where The Files To

Restore files to

Temp2 (F:)

Show advanced option



Choose Where The Files To

Restore files to

Temp2 (F:)

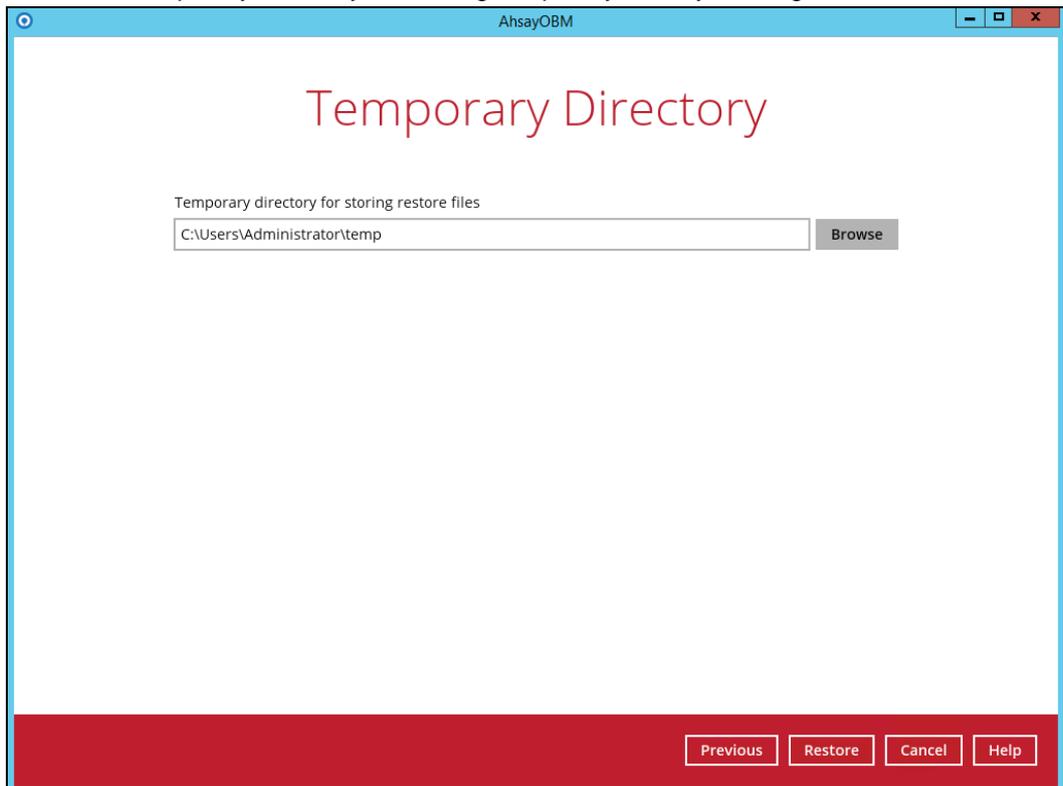
Verify checksum of in-file delta files during restore

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.

6. Select the temporary directory for storing temporary files by clicking **Browse**.



Temporary Directory

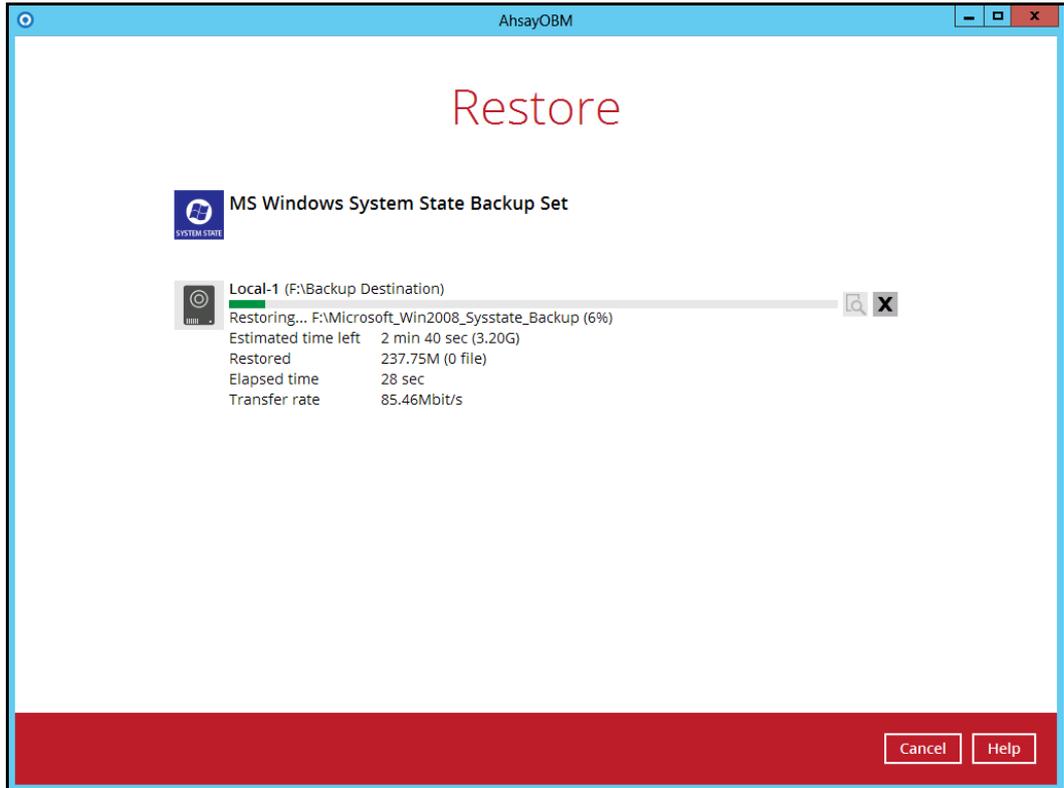
Temporary directory for storing restore files

C:\Users\Administrator\temp

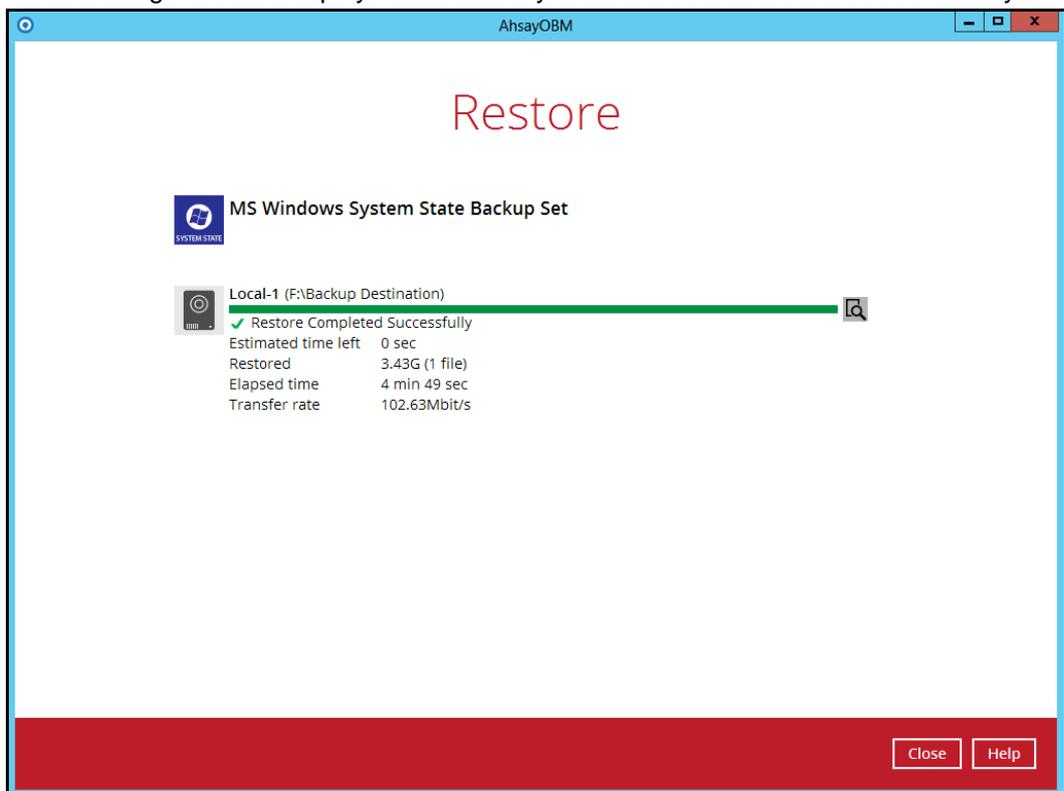
Browse

Previous Restore Cancel Help

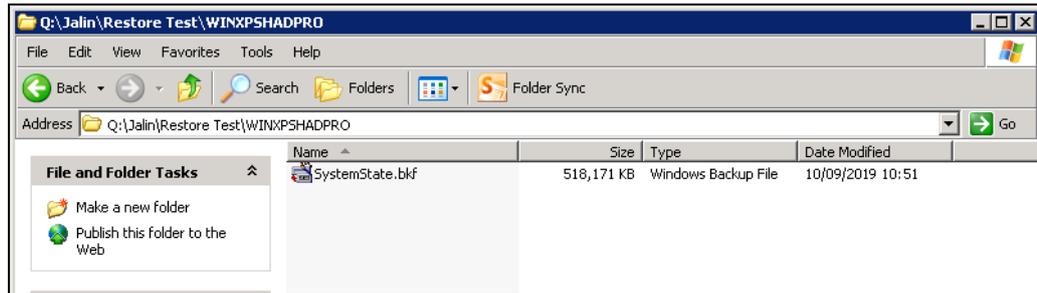
7. Click **Restore** to start the restoration.



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



9. The restored system state data is stored in the “hostname” folder in the restore location.

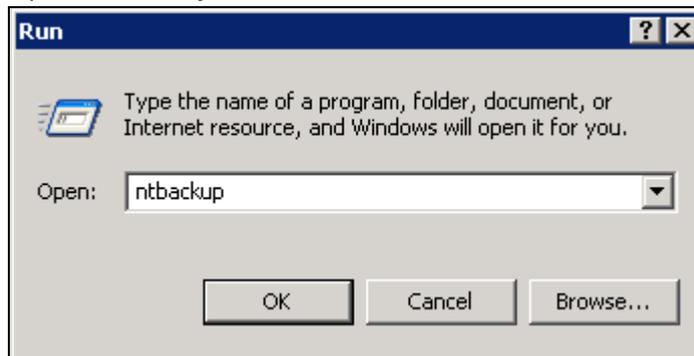


10. Continue to the next section of the guide.

7.4 Apply the System State Data

Before you begin, please make sure that the system state data restored with AhsayOBM are copied to a local disk or in a remote shared folder.

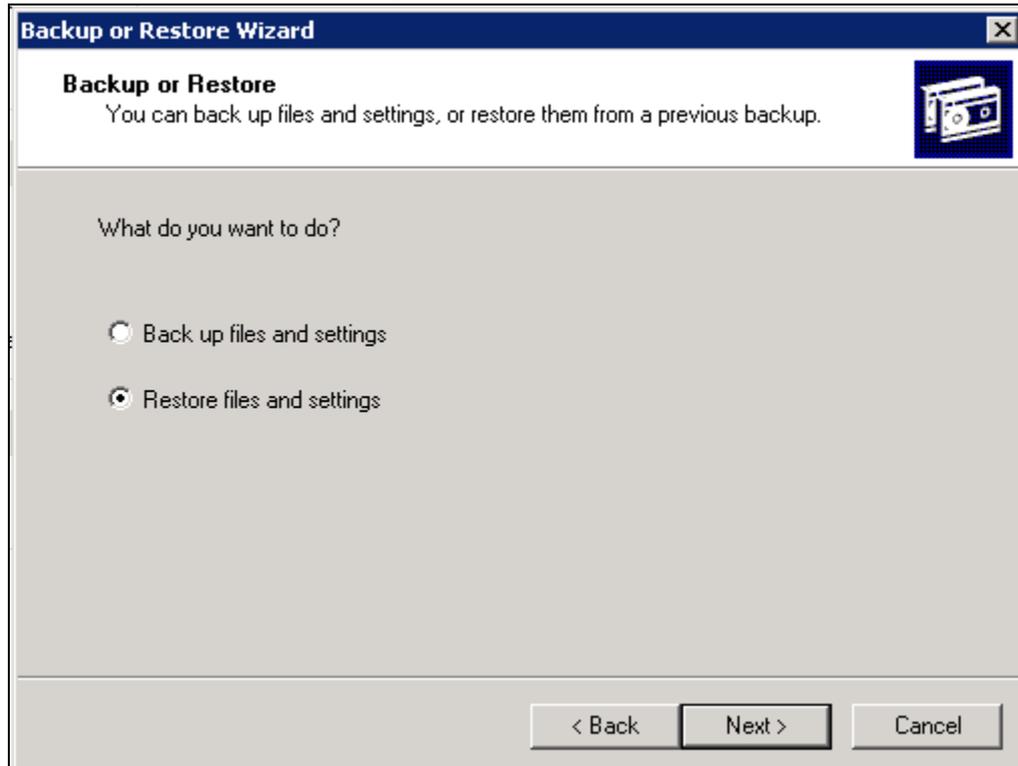
1. Open **NTBackup**. In the Windows Start menu, click **Run...** and type in **ntbackup**.



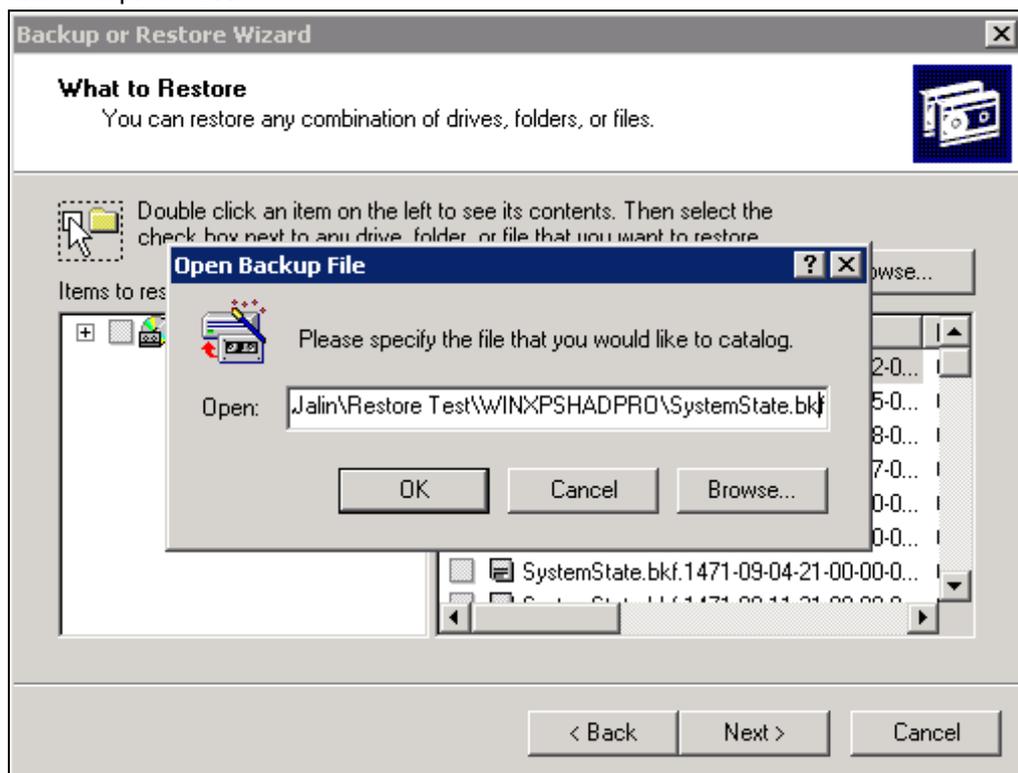
2. Click **Next** to proceed.



3. Choose **Restore file and settings** and click **Next** to proceed.

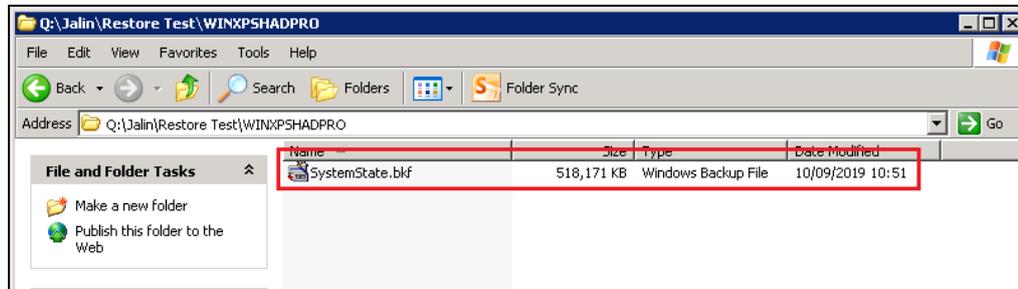
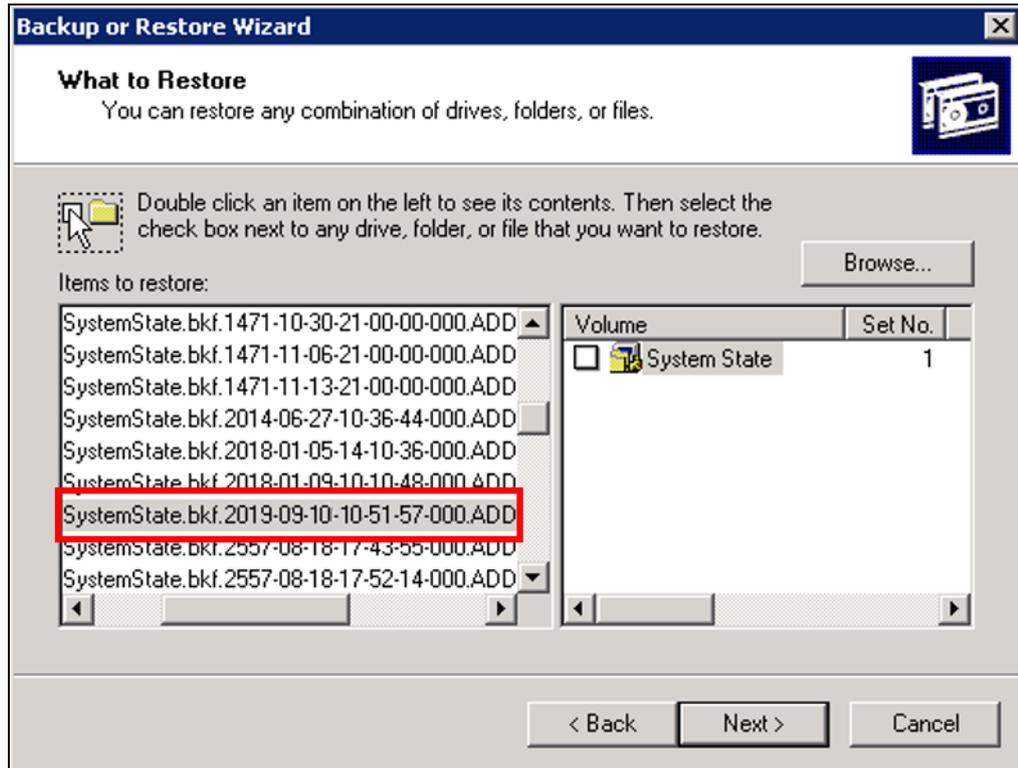


4. Click **Browse** to choose the **SystemState.bkf** file, which is restored via AhsayOBM, and then press **OK**.

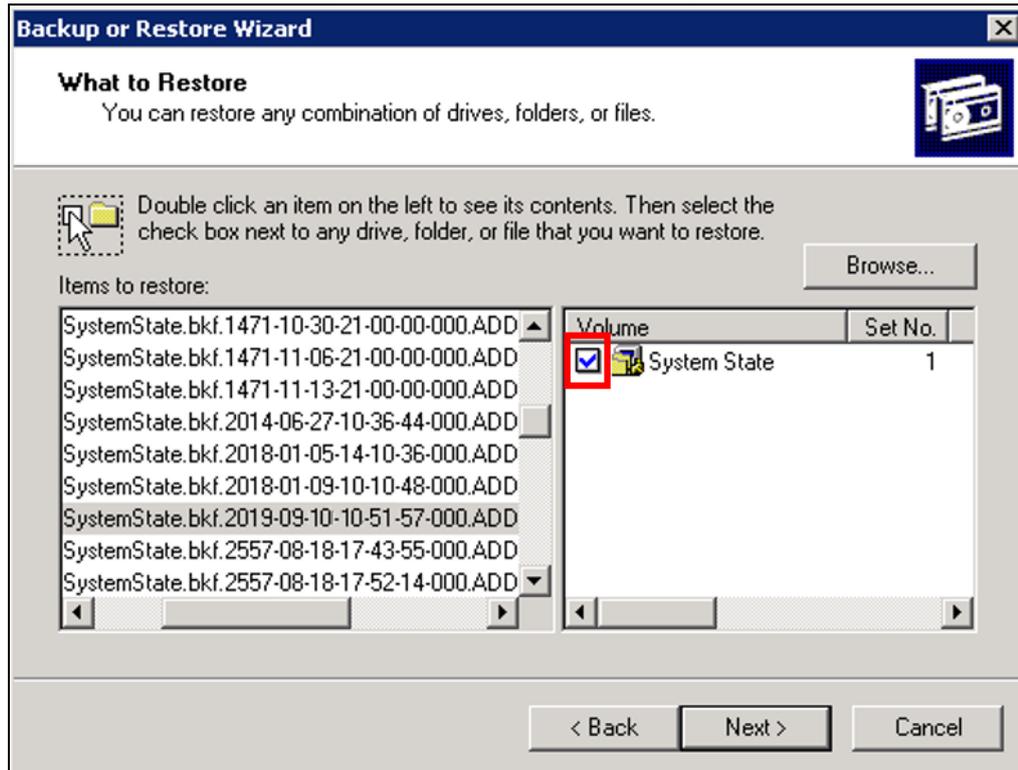


5. Expand the file tree from the left panel and select the corresponding System State file according to the file restored previously. You can refer to the restored file in the restored destination. The correct SystemState.bkf file should be the one with the most

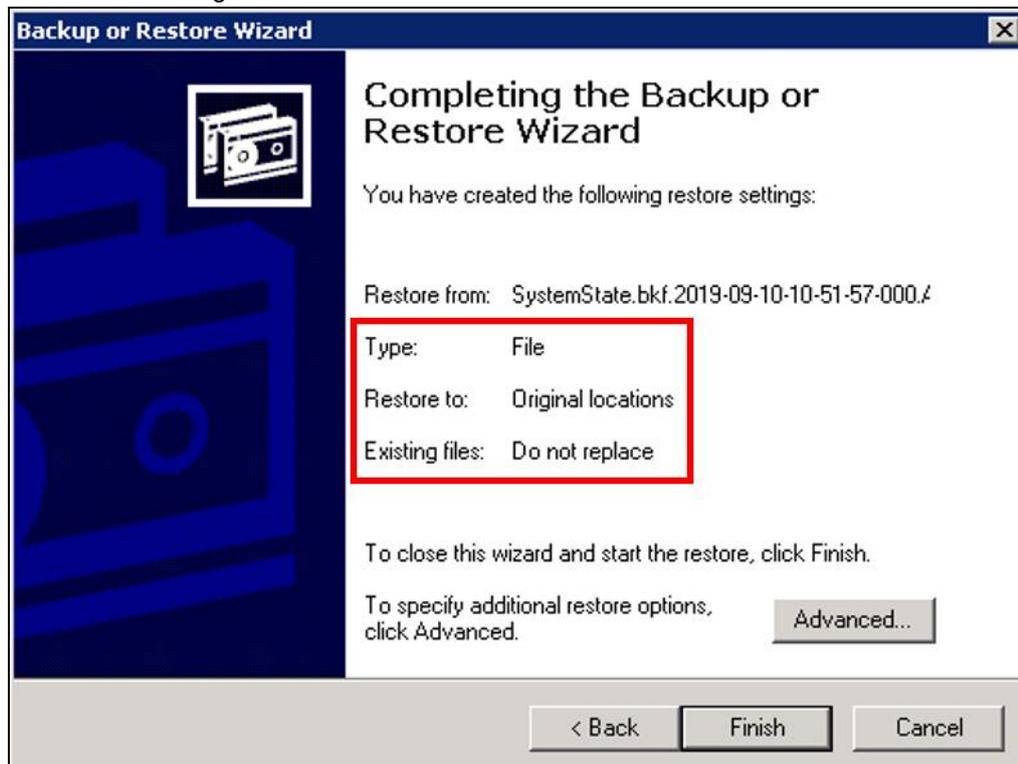
updated modification time as the file in restored destination.



6. Check the box in front of **System State** and click **Next** to proceed.



7. Review the settings.

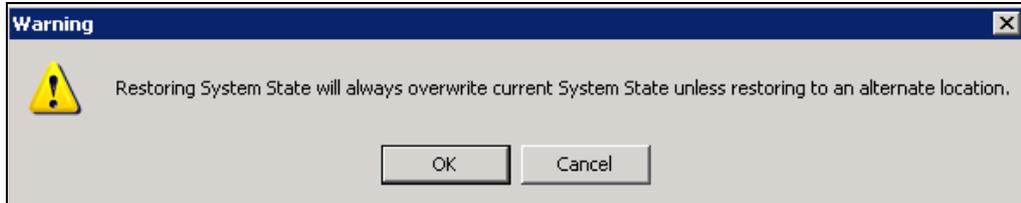


- If you don't want to change any settings, click **Finish** to begin the restore process with default setting.
- If you want to change any of the advanced restore options, such as restoring security and junction point data, click **Advanced...** to modify the settings. Please

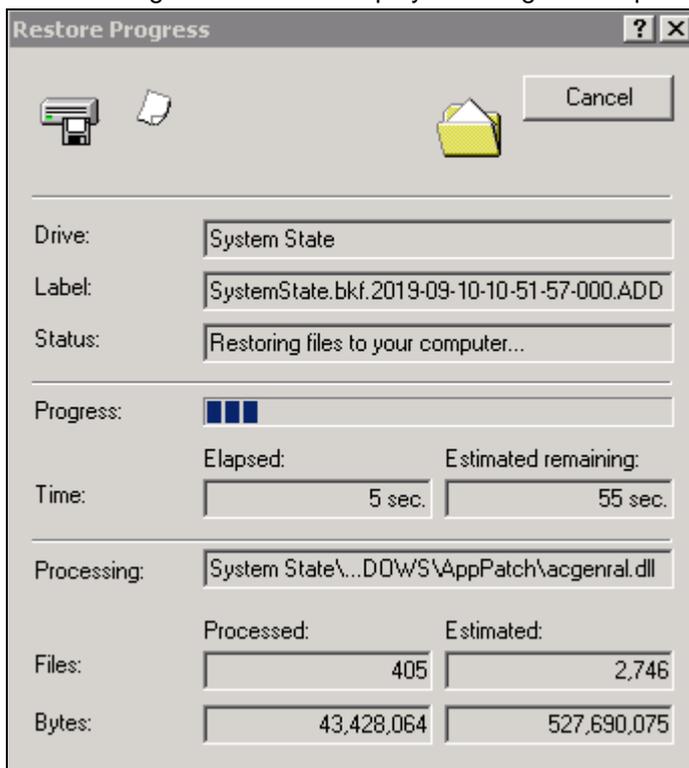
refer to the following article for more details: <https://msdn.microsoft.com/en-us/library/cc875820.aspx>

When you are done setting advanced restore option, click **Finish** to begin the restore.

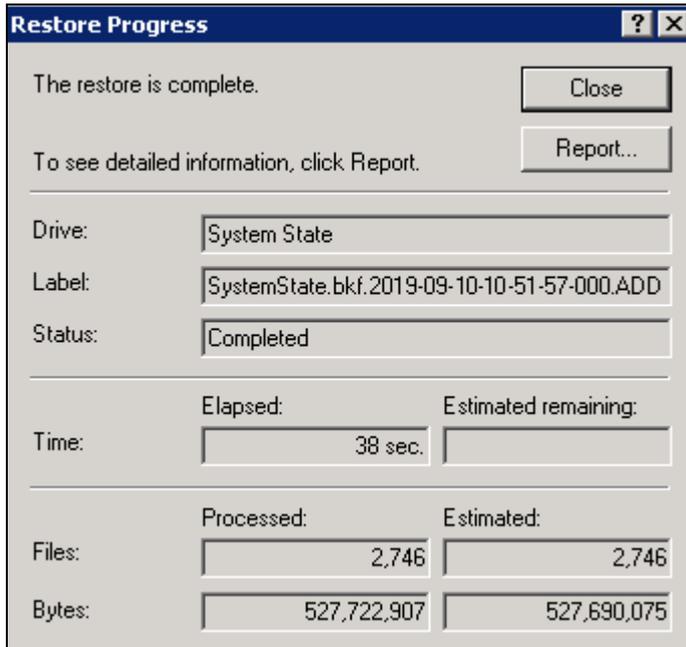
8. Click **Yes** to confirm and start the restore process.



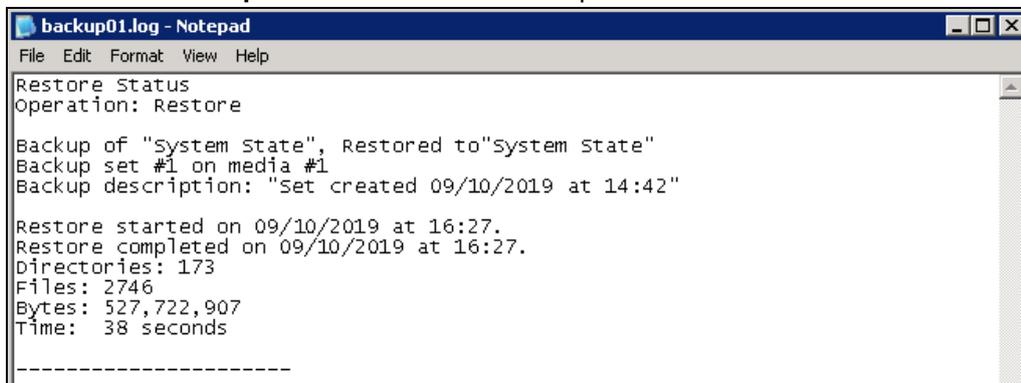
9. The following screen will be displayed during restore process.



10. The following screen will be displayed when the restore process is completed.

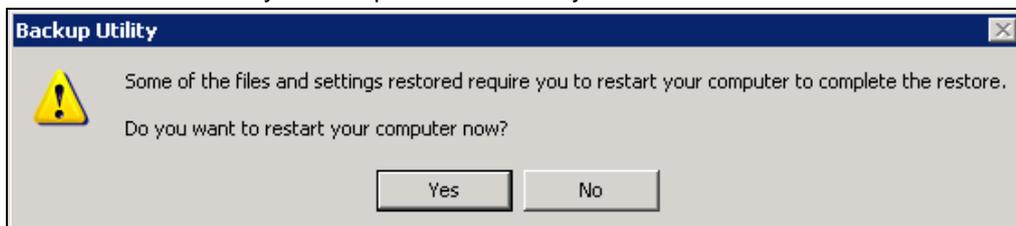


11. You can click on **Report...** to view the restore report.



Or click **Close** to finish the restore process.

A restart must be performed after the system state restoration, and you are suggested to click **Yes** to restart your computer immediately.

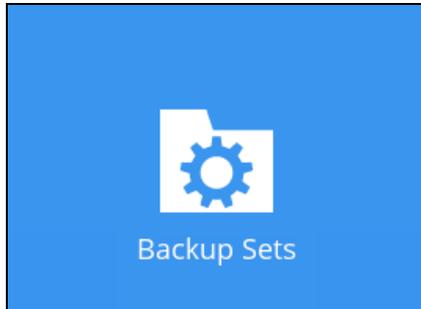


8 Windows Server 2008 and Newer Releases

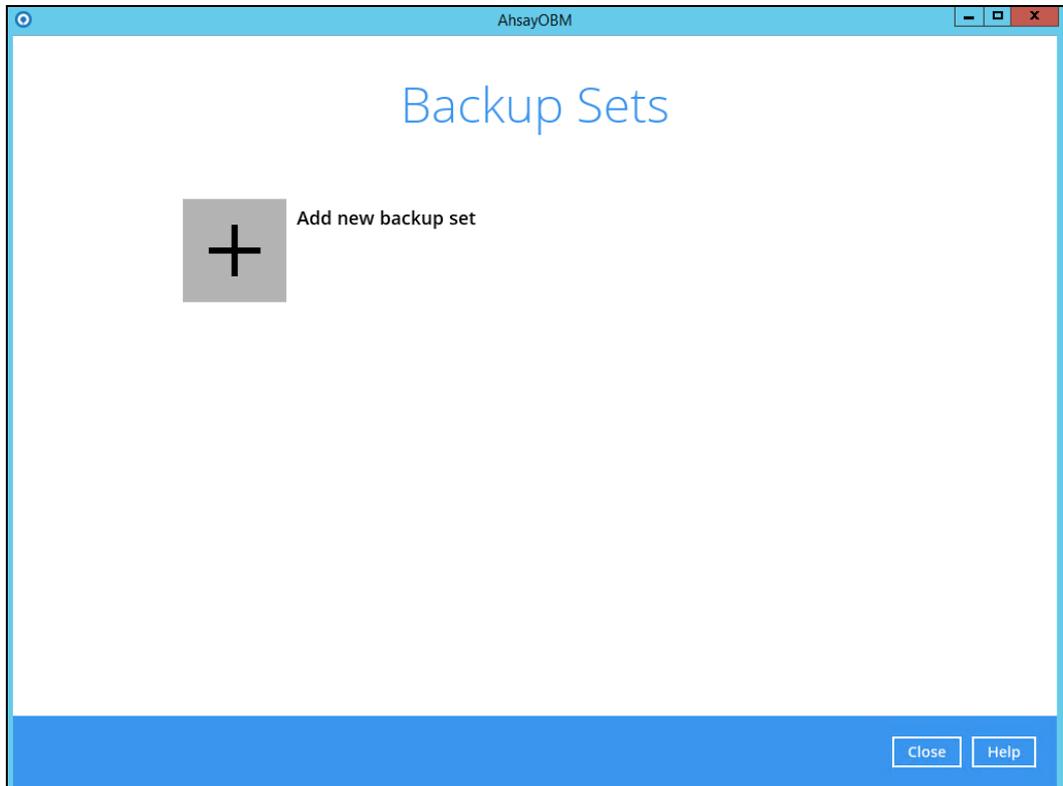
8.1 Configuring a MS Windows System State Backup Set

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 Set

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

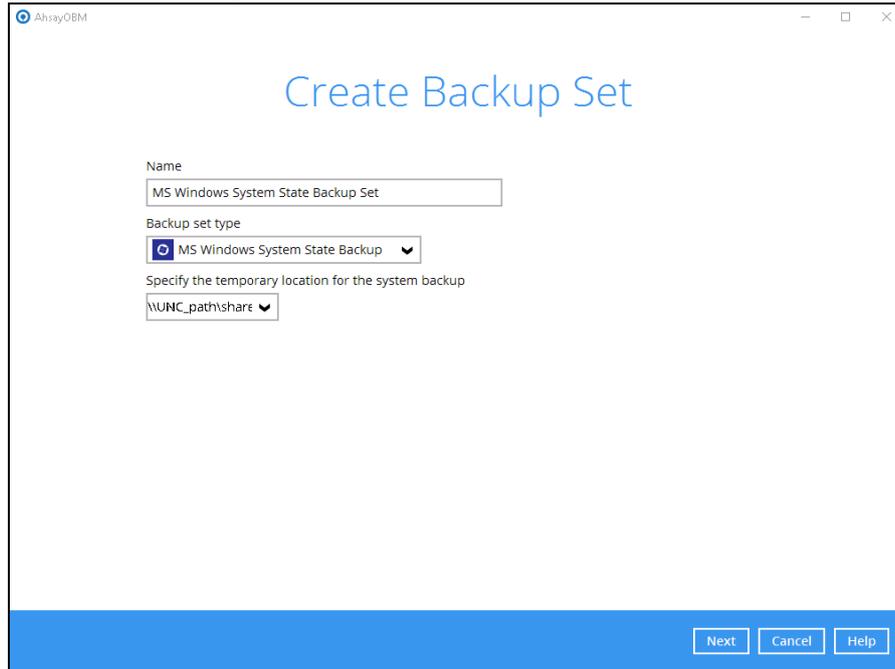
Name
MS Windows System State Backup Set

Backup set type
MS Windows System State Backup

Specify the temporary location for the system backup
Local Disk (C:)
Local Disk (C:)
Volume 1 (E:)
Volume 2 (F:)

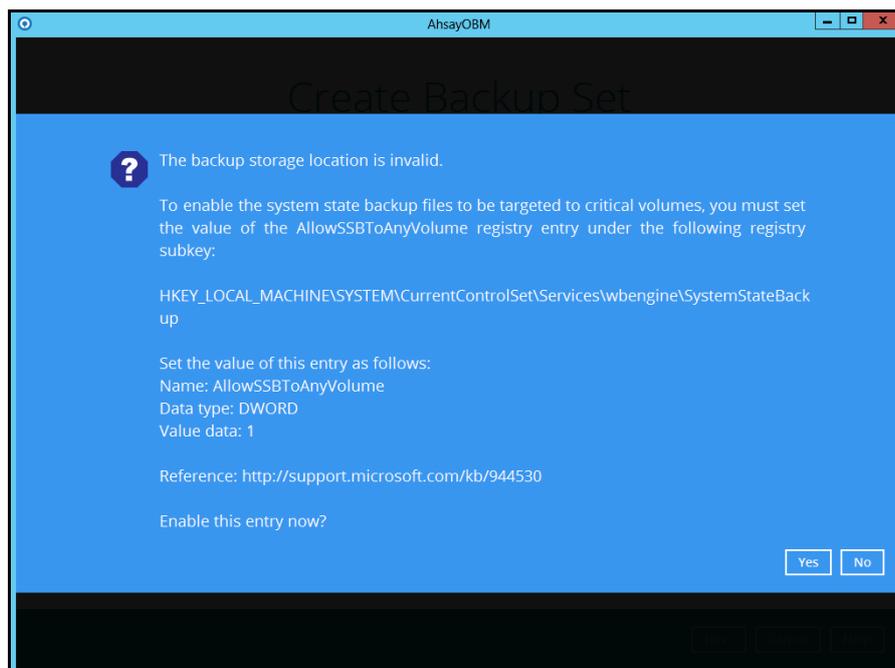
Next Cancel Help

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:



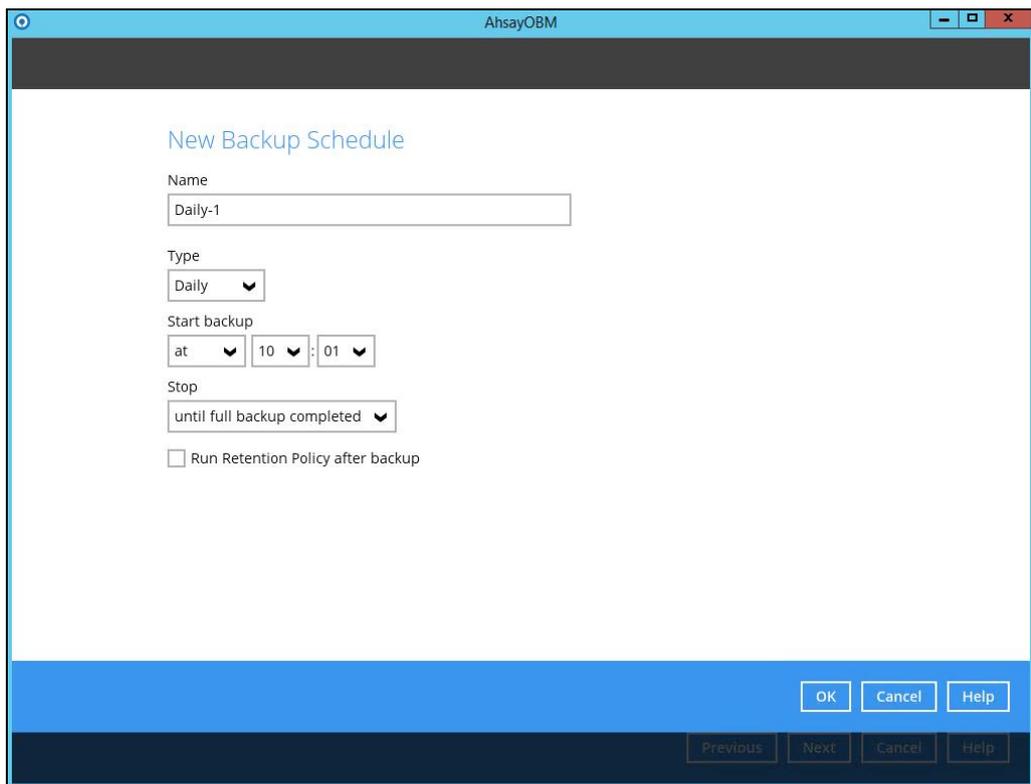
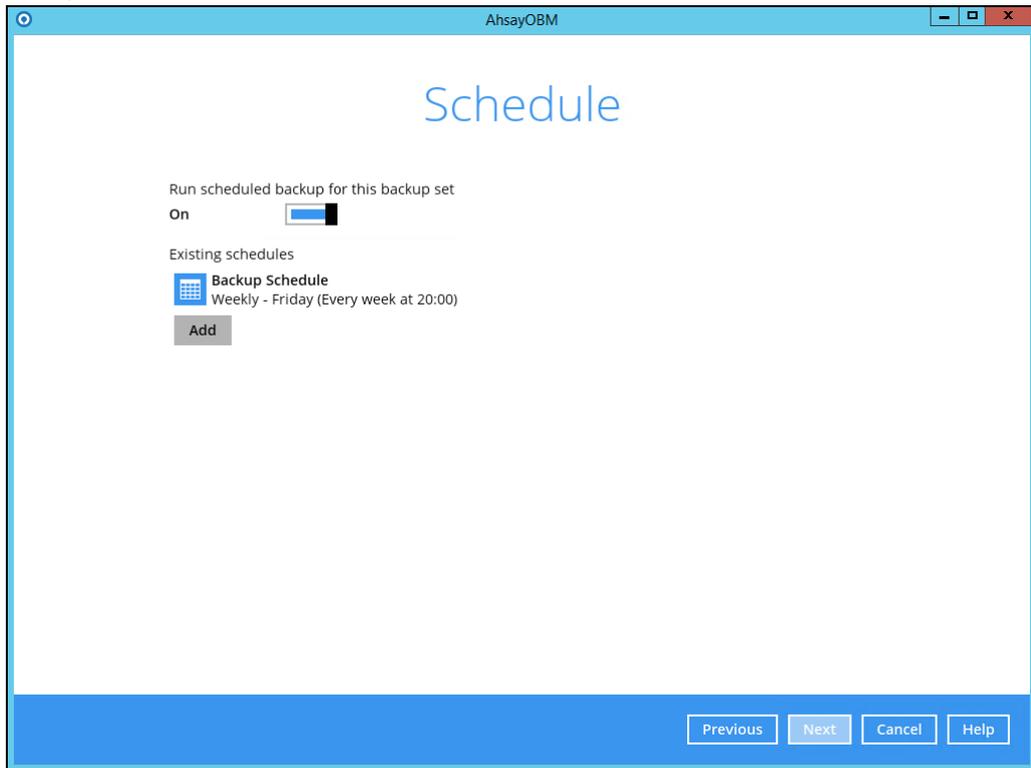
Click **Yes** for AhsayOBM to enable the registry entry, or click **No**, then change the storage location setting to another location.

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](#)

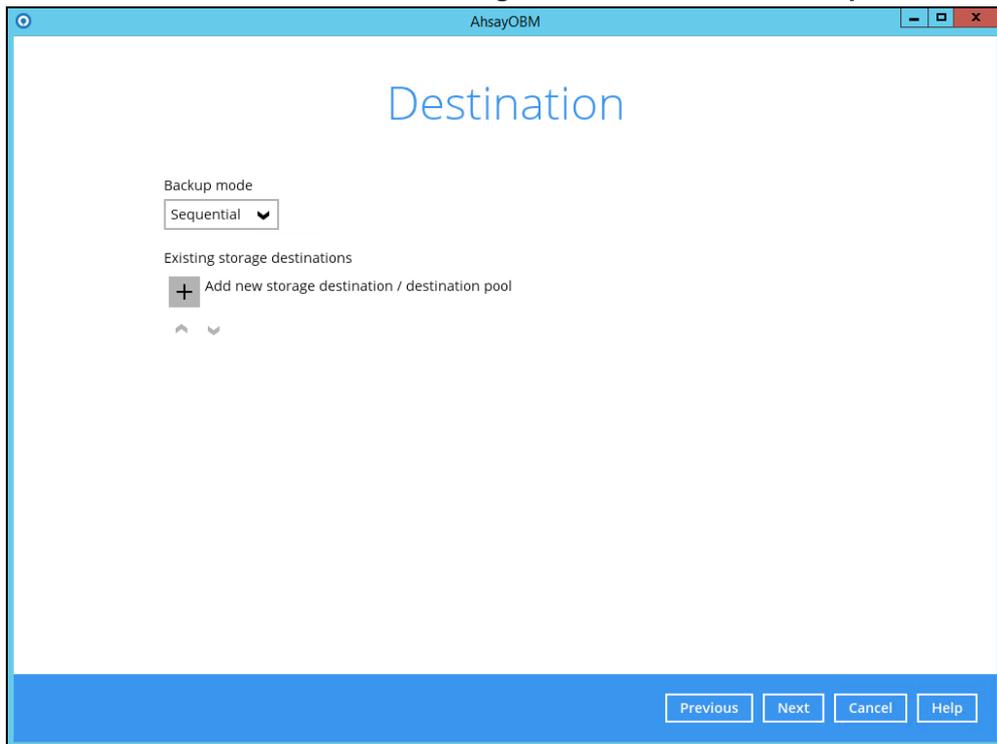
5. In the **Schedule** window, configure a backup schedule for backup job to run automatically at your specified time interval.

As you can see there's already a default Backup Schedule which is set weekly, every Friday around 20:00PM. Click **Add** to add a new schedule.



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

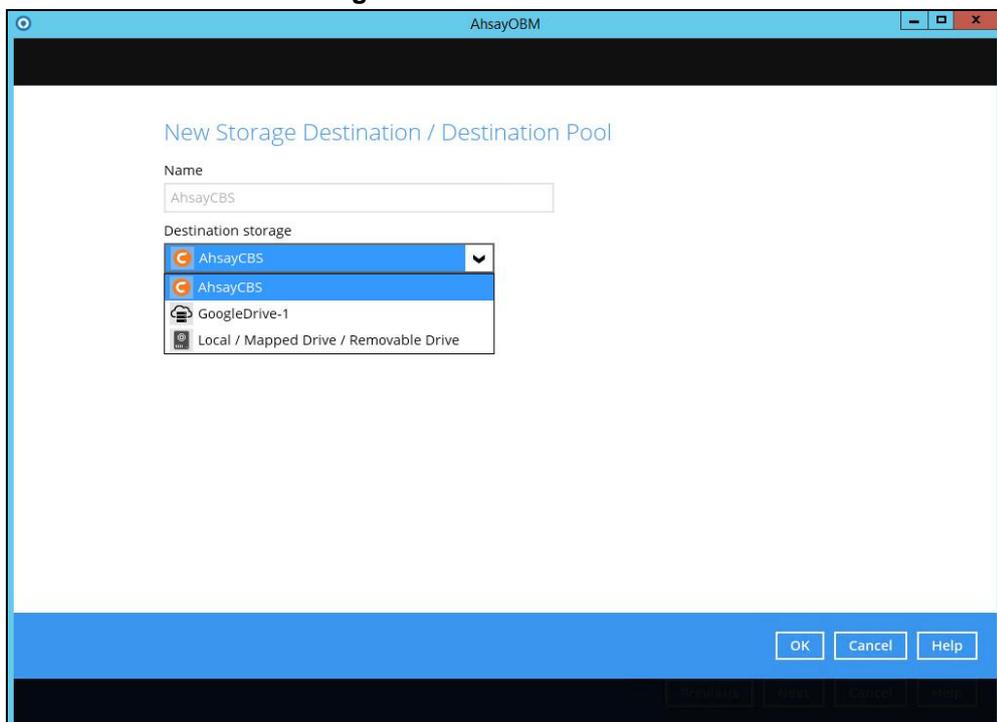
6. In the **Destination** menu, select a backup destination where the backup data will be stored. Click **+** next to **Add new storage destination / destination pool**.



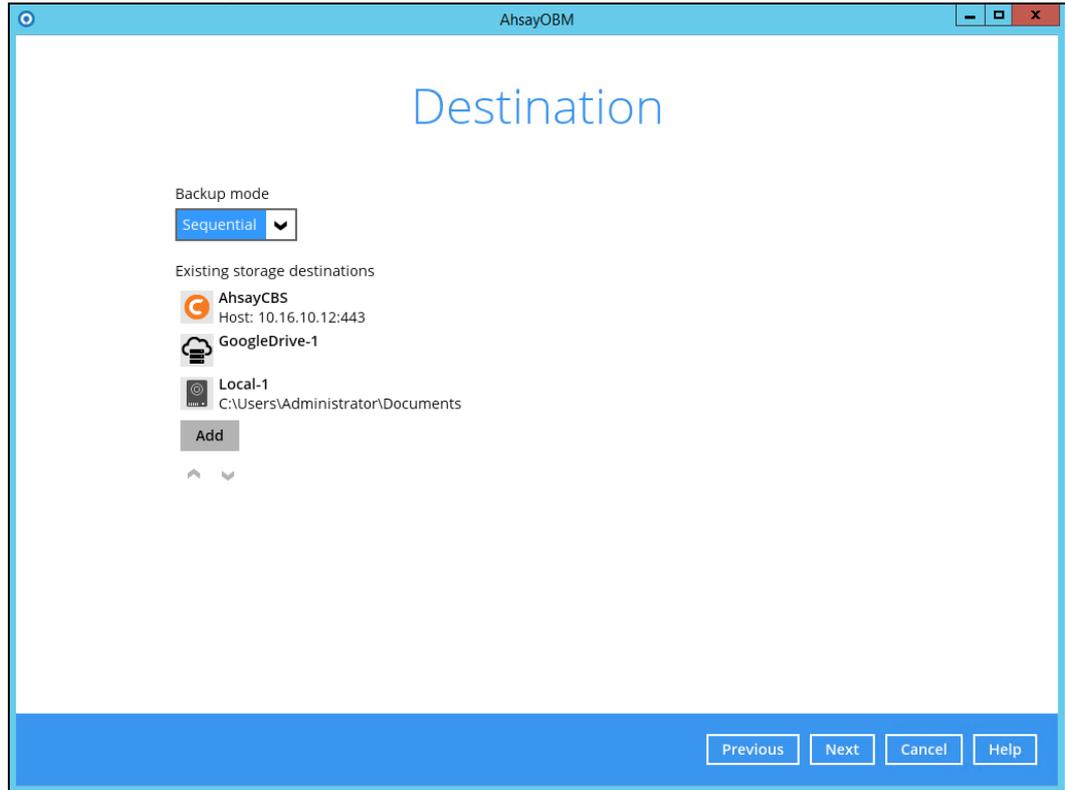
Note: For more details on Backup Destination, refer to this link: [FAQ: Frequently Asked Questions on Backup Destination](#)

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**.

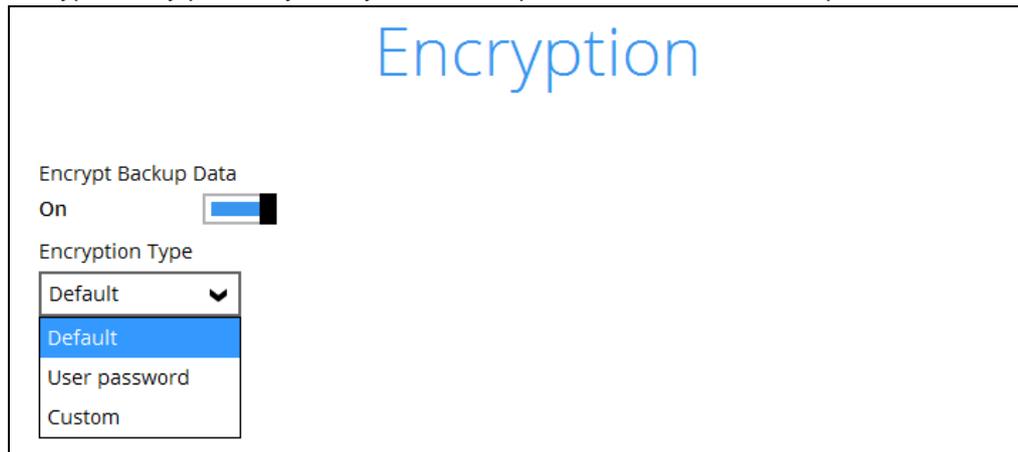


Continue by adding another destination for the backup set or click **Next** to proceed.



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.

The screenshot shows the 'Encryption' settings page. At the top, the word 'Encryption' is displayed in a large blue font. Below it, there are several settings:

- Encrypt Backup Data:** A toggle switch is set to 'On'.
- Encryption Type:** A dropdown menu is set to 'Custom'.
- Algorithm:** A dropdown menu is set to 'AES'.
- Encryption key:** A text input field containing seven asterisks (*****).
- Re-enter encryption key:** A text input field containing seven asterisks (*****).
- Method:** Two radio buttons are present: 'ECB' (unselected) and 'CBC' (selected).
- Key length:** Two radio buttons are present: '128-bit' (unselected) and '256-bit' (selected).

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.

The screenshot shows a confirmation pop-up window titled 'Encryption'. The background is dark grey, and the main content area is blue. At the top, the word 'Encryption' is displayed in a large blue font. Below it, there are several settings:

- Encrypt Backup Data:** A toggle switch is set to 'On'.
- Encryption Type:** A dropdown menu is set to 'Default'.

The main body of the pop-up contains the following text:

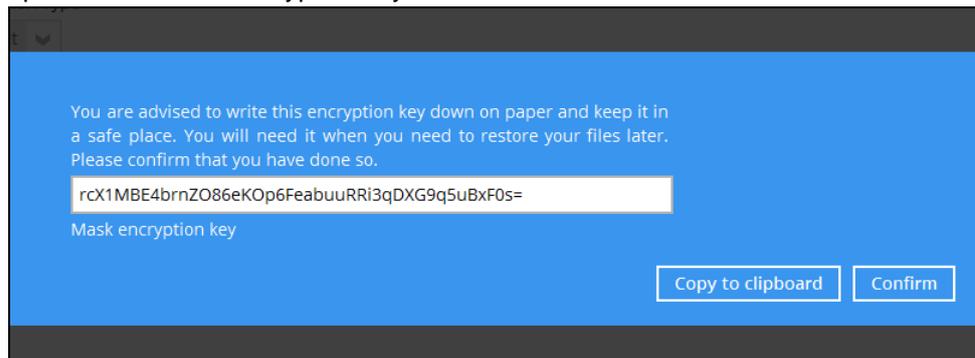
You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.

Below the text is a text input field containing seven asterisks (*****). Below the input field is the text 'Unmask encryption key'.

At the bottom right of the pop-up, there are two buttons: 'Copy to clipboard' and 'Confirm'.

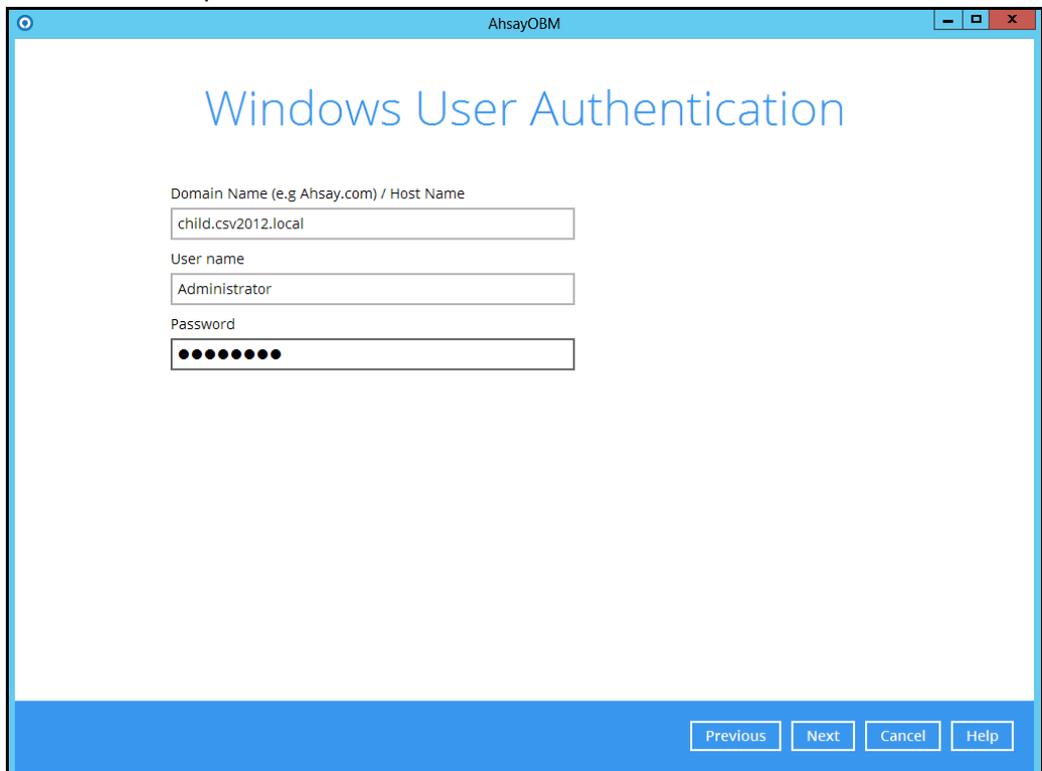
The pop-up window has the following three options to choose from:

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

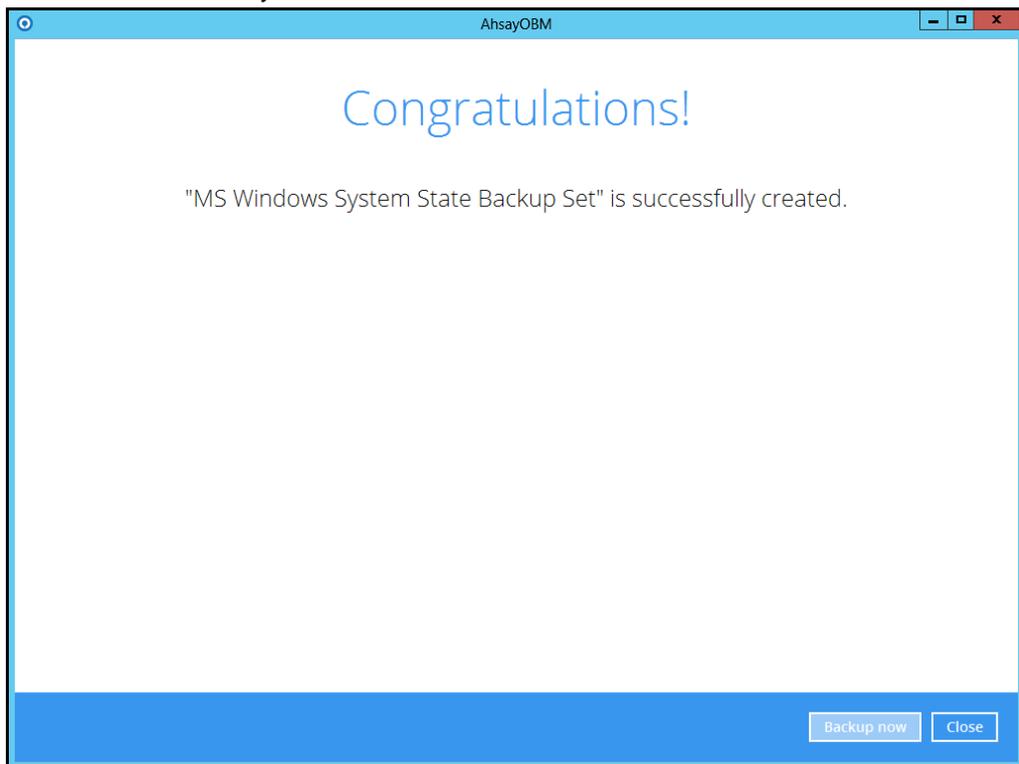


- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.
- **Confirm** – Click to exit this pop-up window and proceed to the next step.

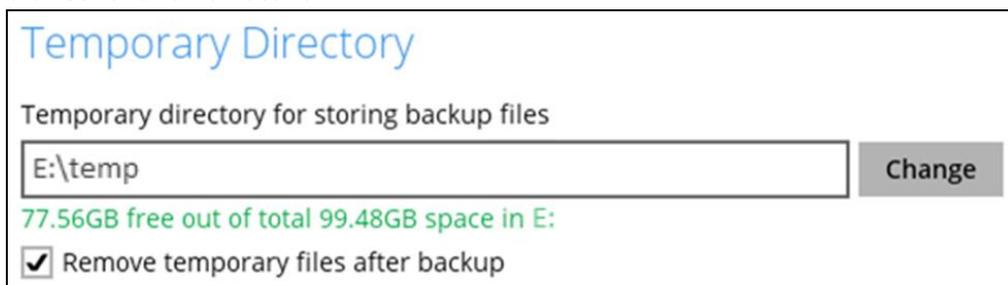
10. If you have enabled the **Schedule** feature in the previous step, the following window will be shown. Enter the **Domain Name / Host Name** of the computer, **User Name** and **Password** of the Windows account that will be running the backup. Click **Next** to create the backup set.



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



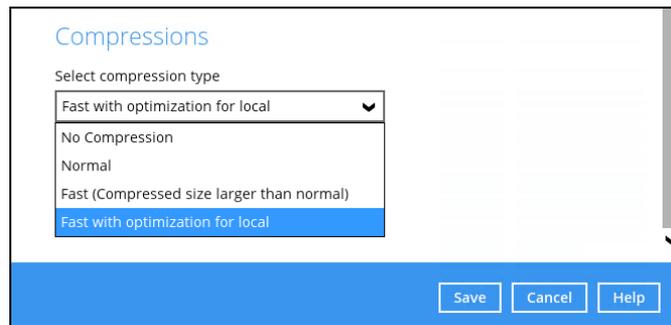
12. Based on [Best Practices and Recommendations](#), it is highly recommended to set the temporary directory to another location other than Drive C: (e.g. Drive E:). To do this, go to **Backup Sets > Others > Temporary Directory** and click the **Change** button to browse for another location.



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

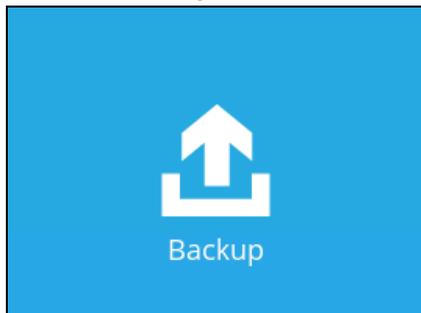
Go to **Others > Compressions**, then select from the following:

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

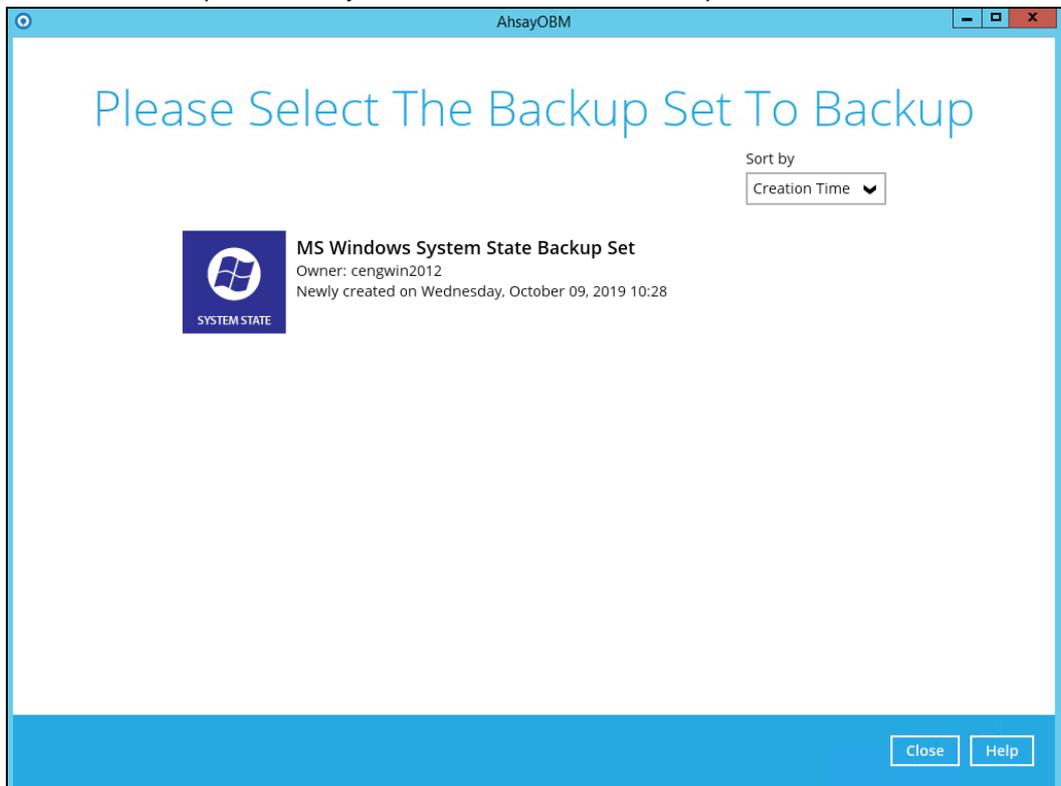


8.2 Start a Manual Backup

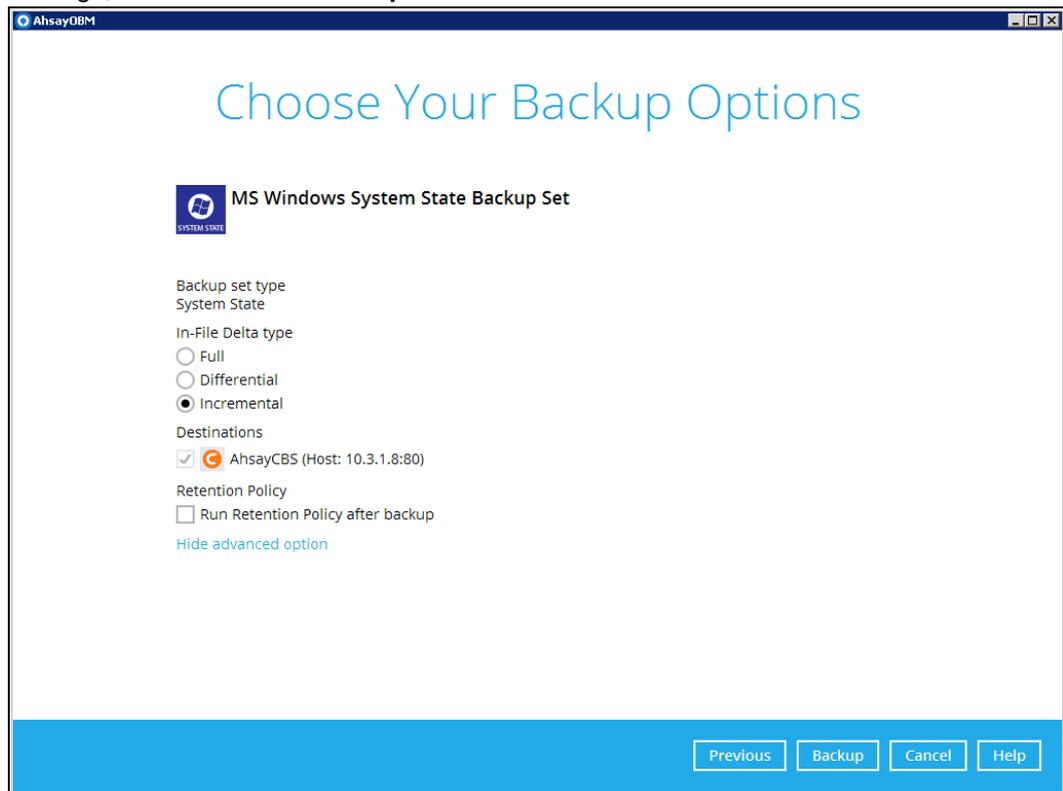
1. Click the **Backup** icon on the main interface of AhsayOBM.



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

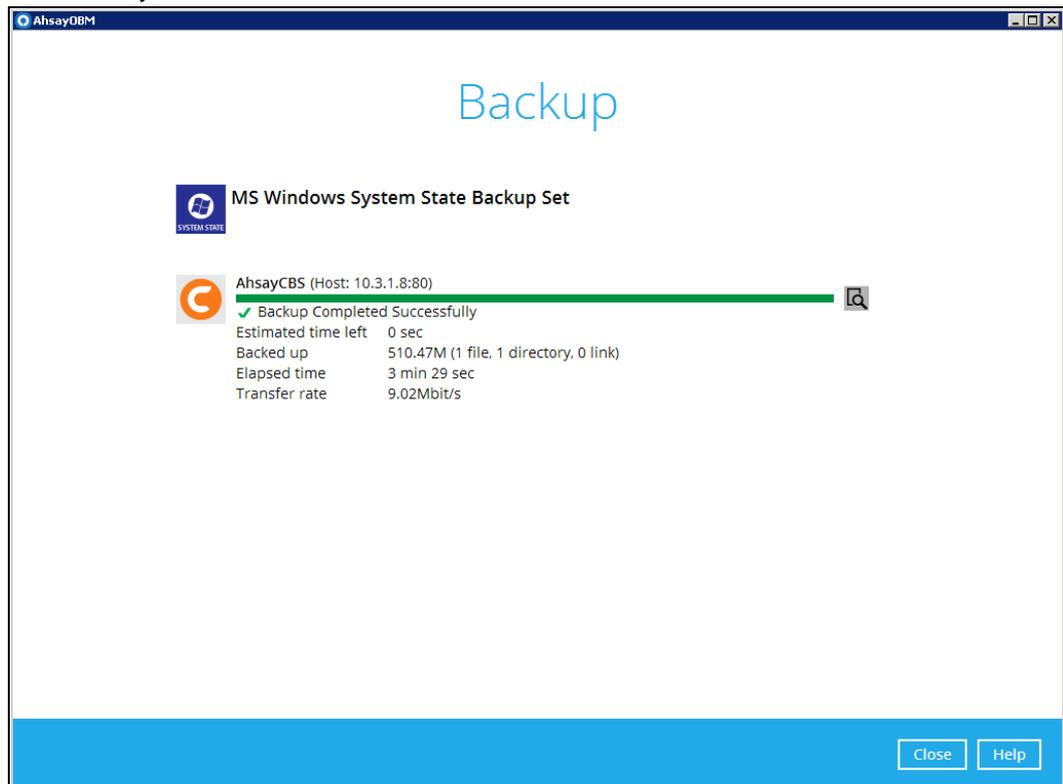


3. If you would like to modify the In-File Delta type, Destinations and Retention Policy Settings, click **Show advance option**.



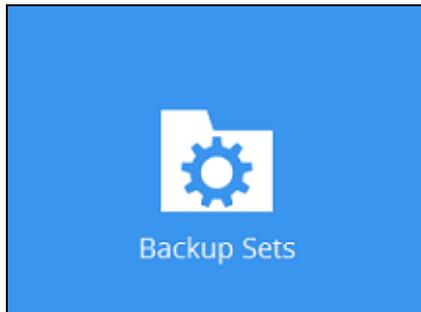
Click **Backup** to start the backup job.

4. The following screen is displayed when the system state data are backed up successfully.

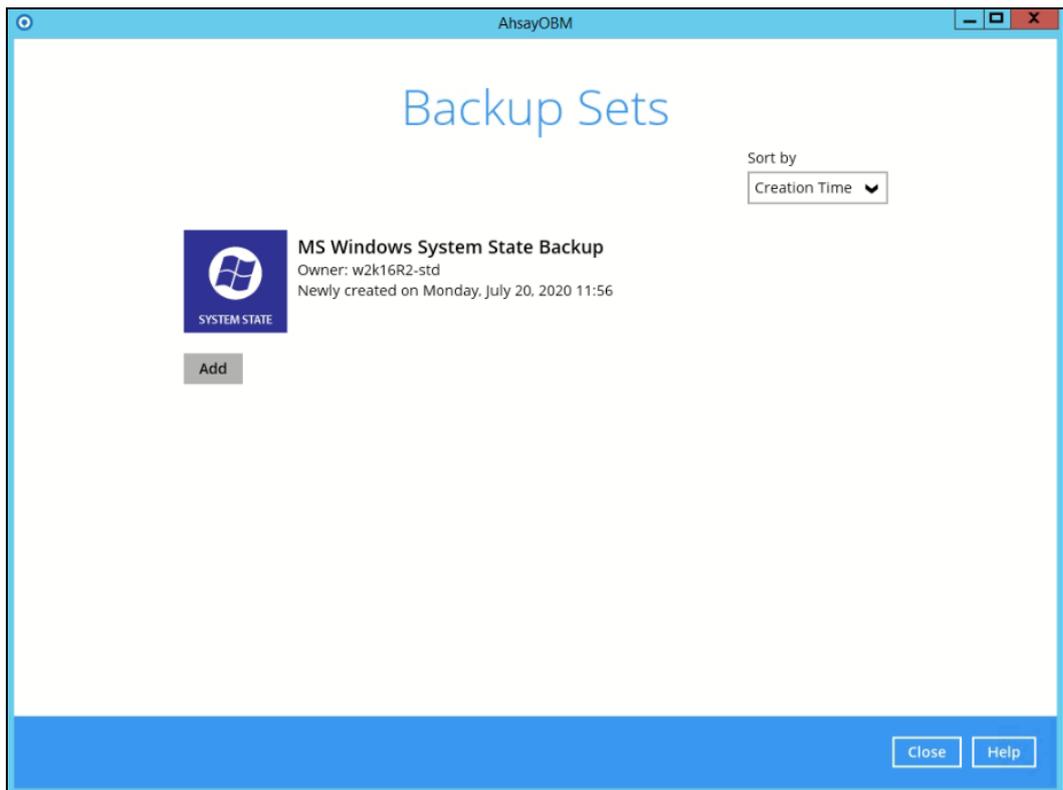


8.3 Configure Backup Schedule for Automated Backup

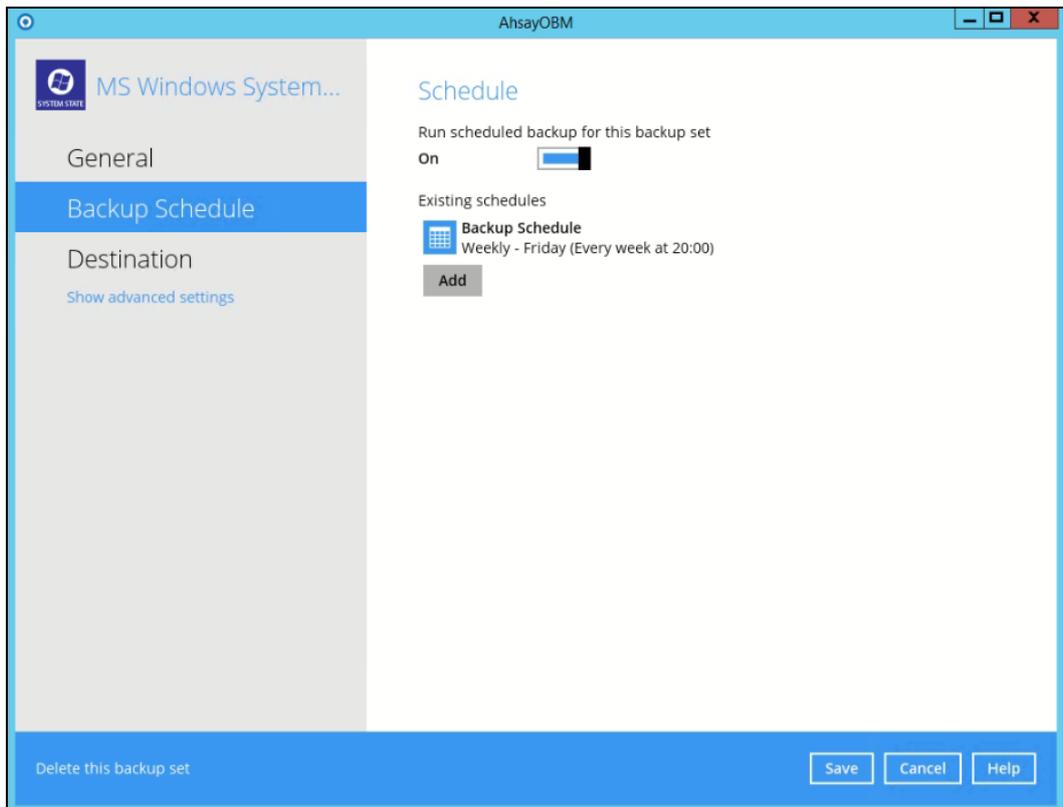
1. Click the **Backup Sets** icon on the main interface of AhsayOBM.



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 schedule will be listed by default. Click the **Add** button to add a new backup schedule.



- The New Backup Schedule window will appear.

New Backup Schedule

Name

Type

Start backup
 :

Stop

Run Retention Policy after backup

- 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.

- **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

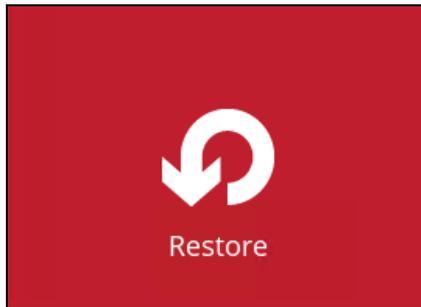
Existing schedules

-  **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)

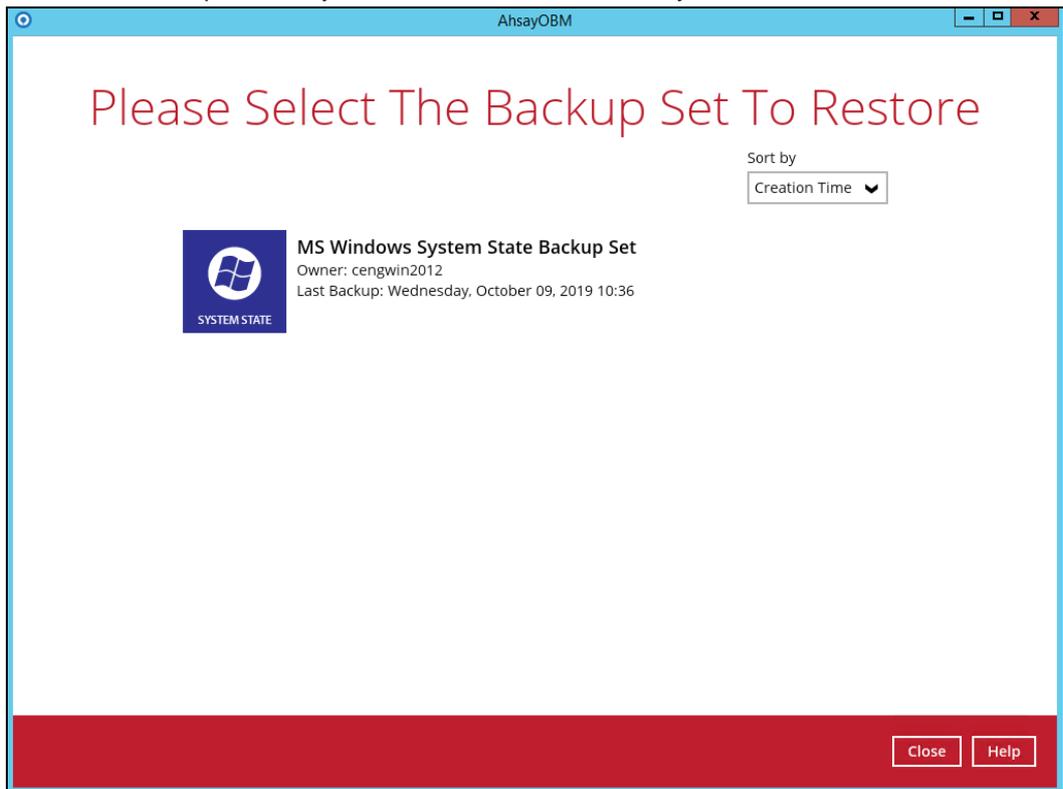
6. Click **Save** to confirm your settings once done.

8.4 Restore the System State Data

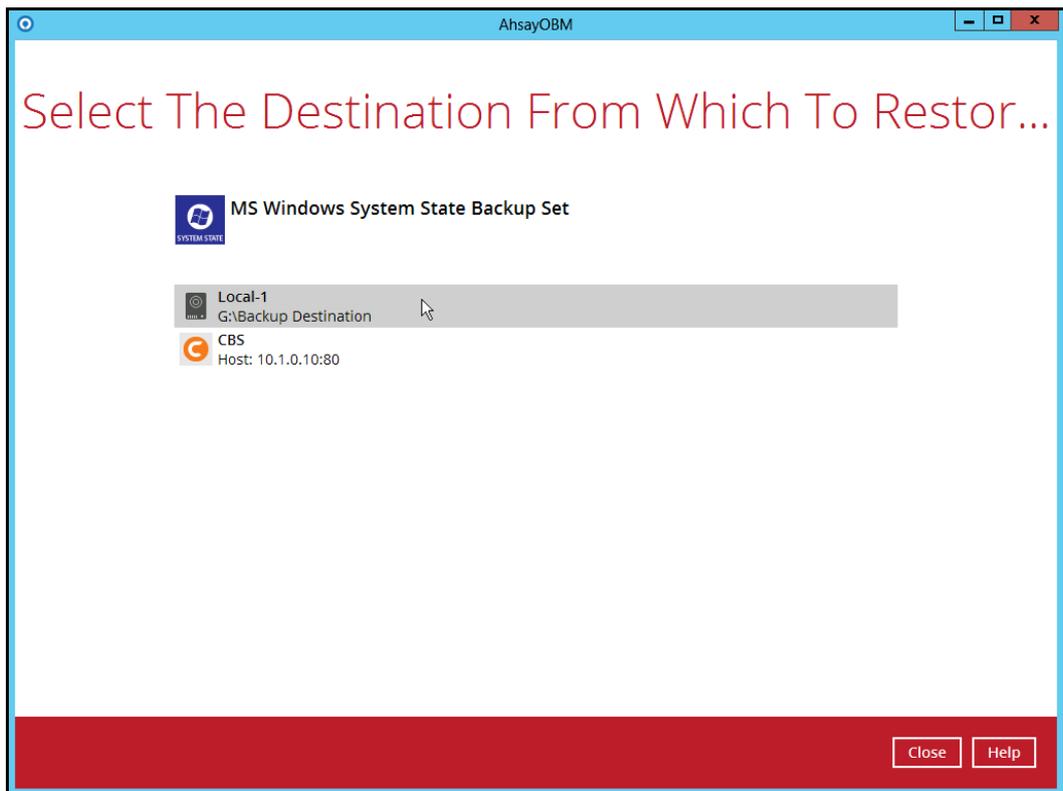
1. Click the **Restore** icon on the main interface of AhsayOBM.



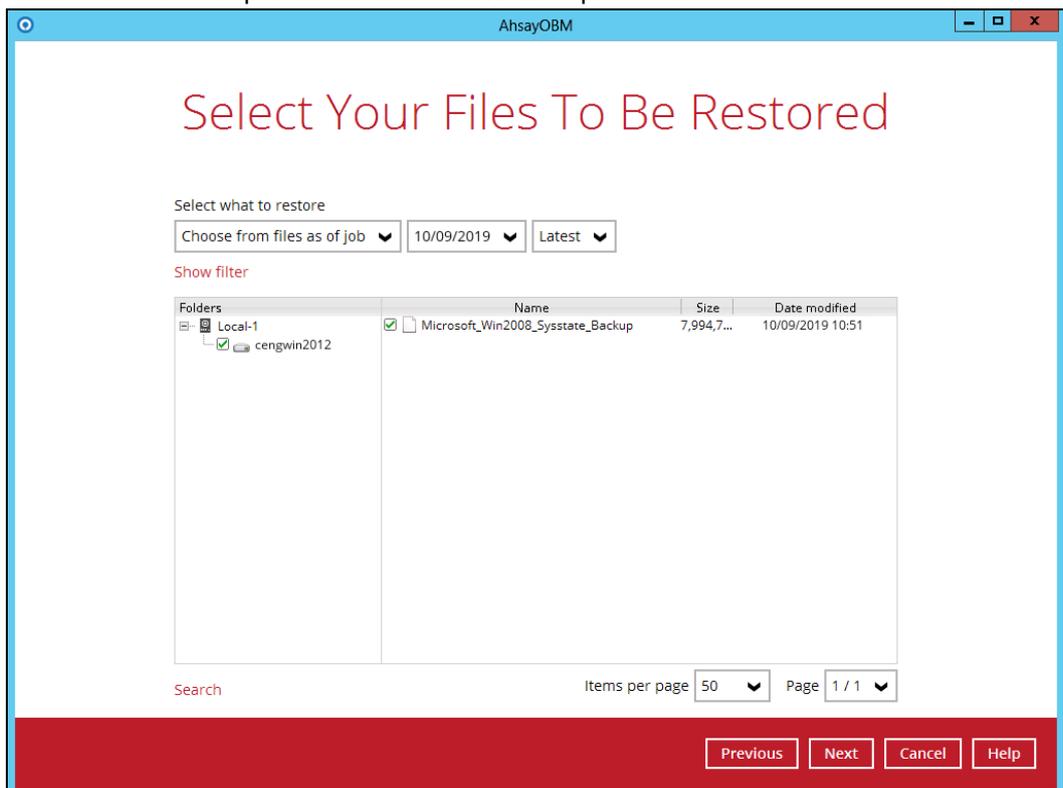
2. Select the backup set that you would like to restore the system state data from.



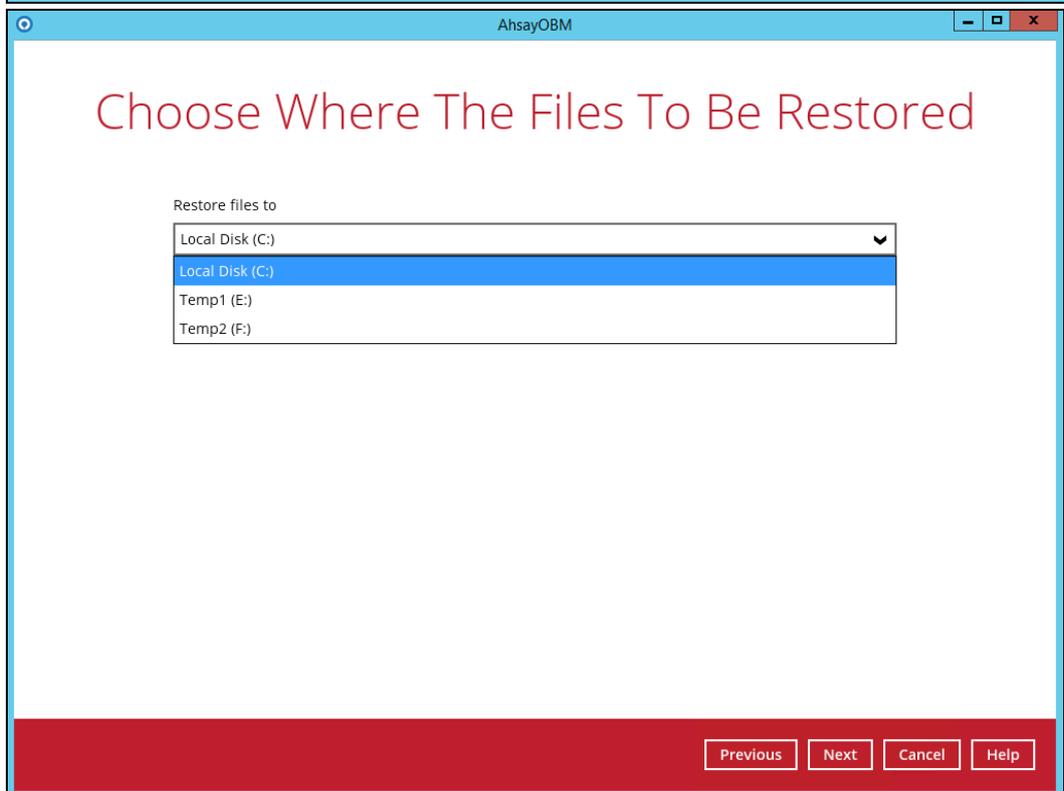
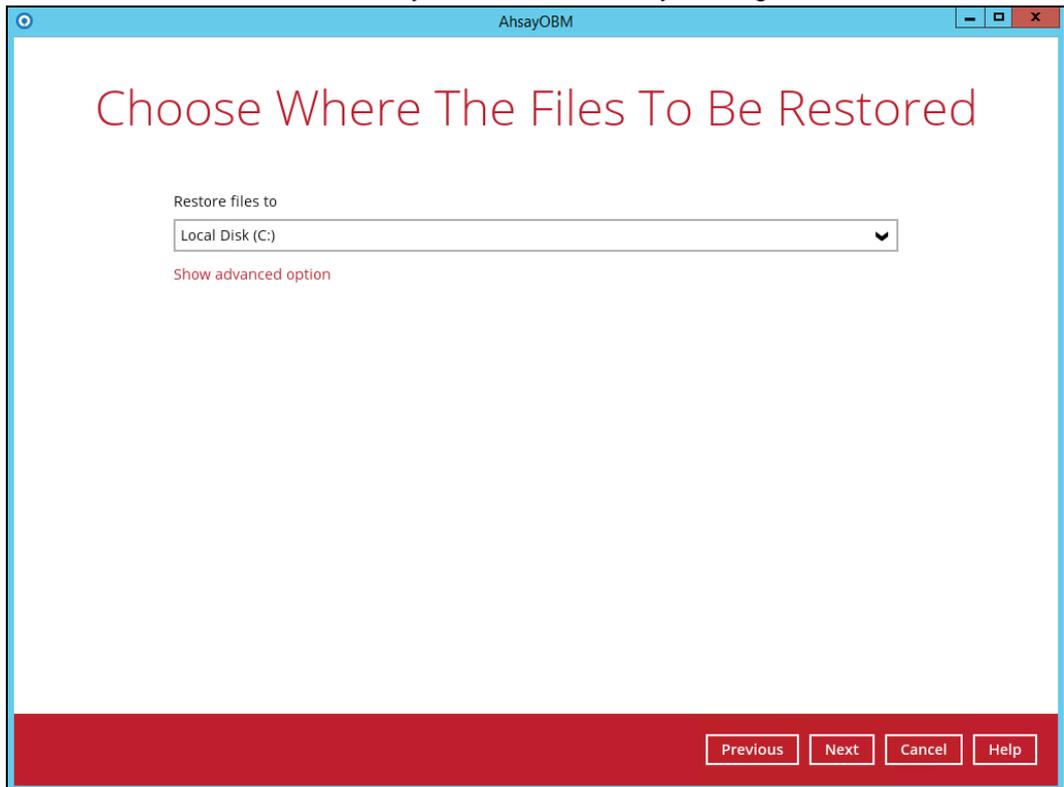
3. Select the backup destination that contains the system state data that you would like to restore.



4. 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.



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



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

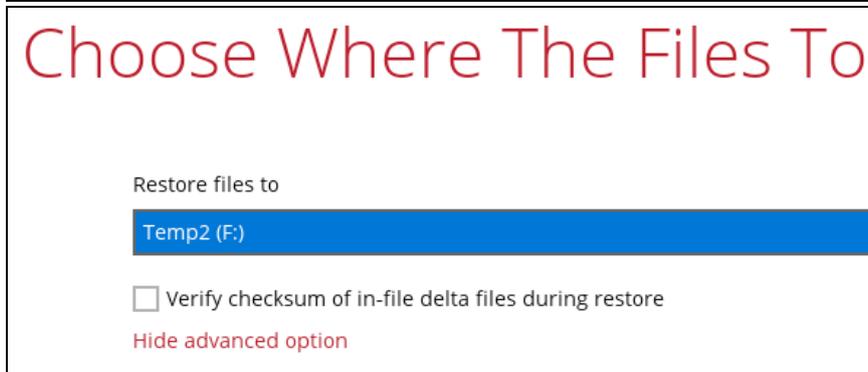


Choose Where The Files To

Restore files to

Temp2 (F:)

Show advanced option



Choose Where The Files To

Restore files to

Temp2 (F:)

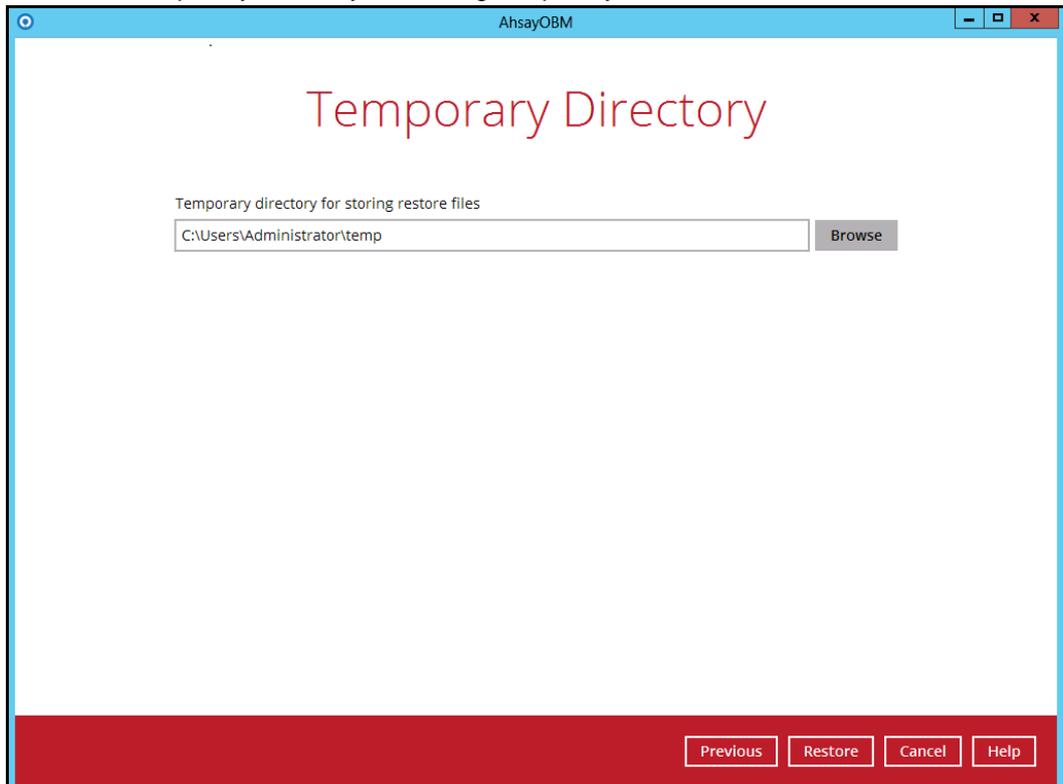
Verify checksum of in-file delta files during restore

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.

6. Select the temporary directory for storing temporary files.



AhsayOBM

Temporary Directory

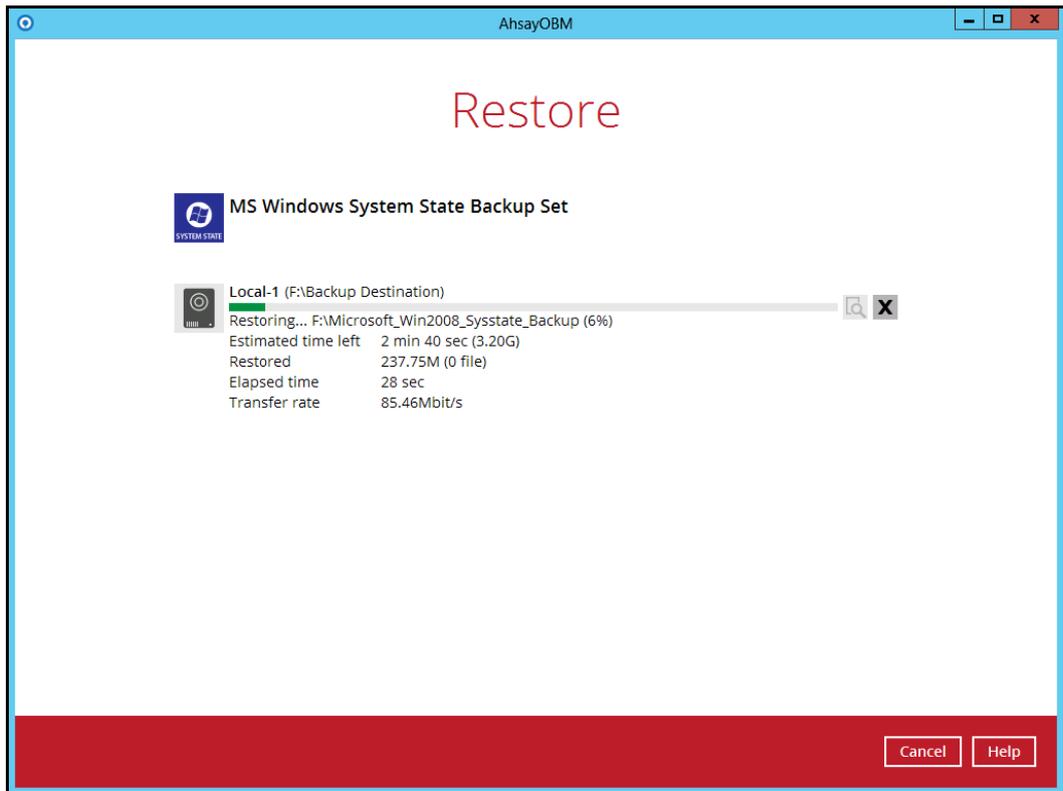
Temporary directory for storing restore files

C:\Users\Administrator\temp

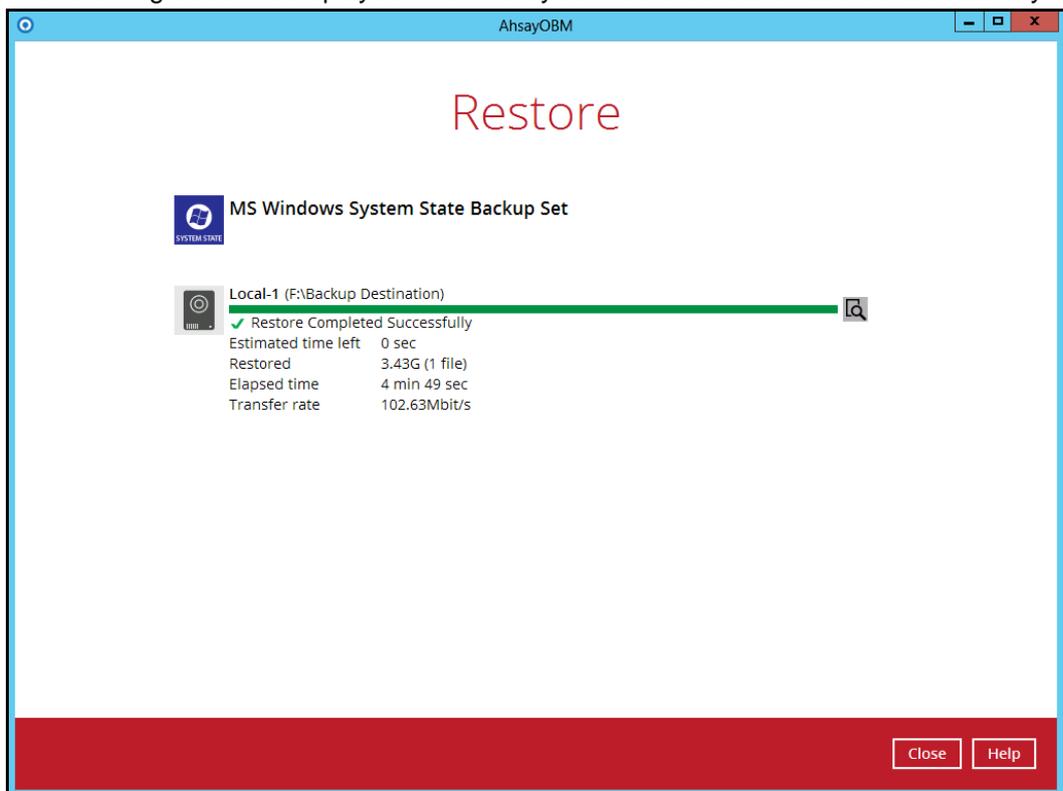
Browse

Previous Restore Cancel Help

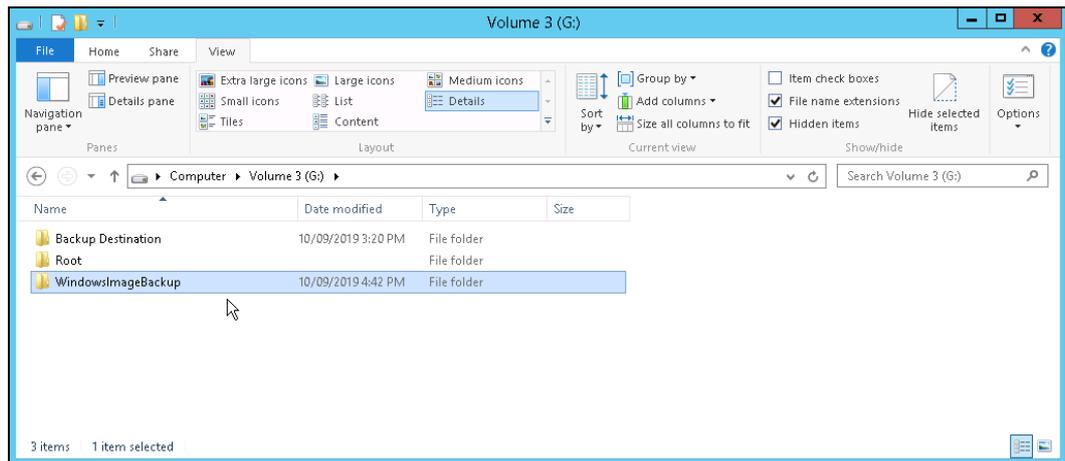
7. Click **Restore** to start the restoration.



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



- The restored system state data are stored in the **WindowsImageBackup** folder in the restore location.



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 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

- 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.

- Continue to the next section of the guide.

8.5 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>}]
```

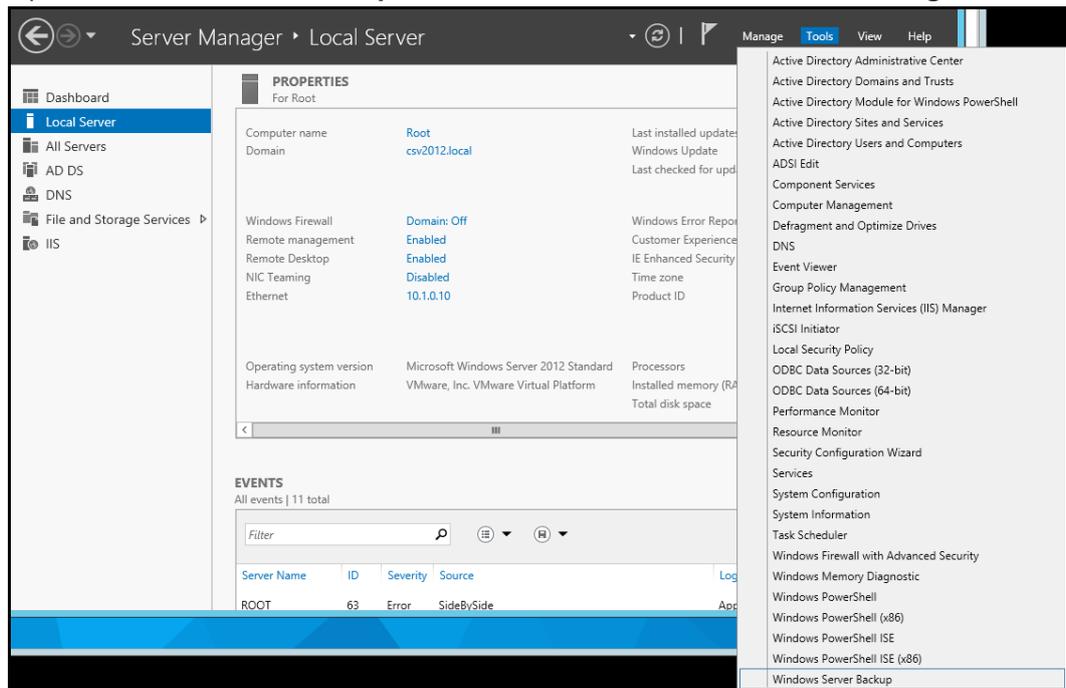
Example (system state restored to G: volume):

```
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: 10/09/2019 1:46 PM  
Backup target: 1394/USB Disk labeled Volume 3 (G:)  
Version identifier: 10/09/2019-05:46  
Can recover: Volume(s), File(s), Application(s), Bare Metal  
Recovery, System State  
Snapshot ID: {feb9079c-9459-4034-908f-7b5a9b0bb1e5}
```

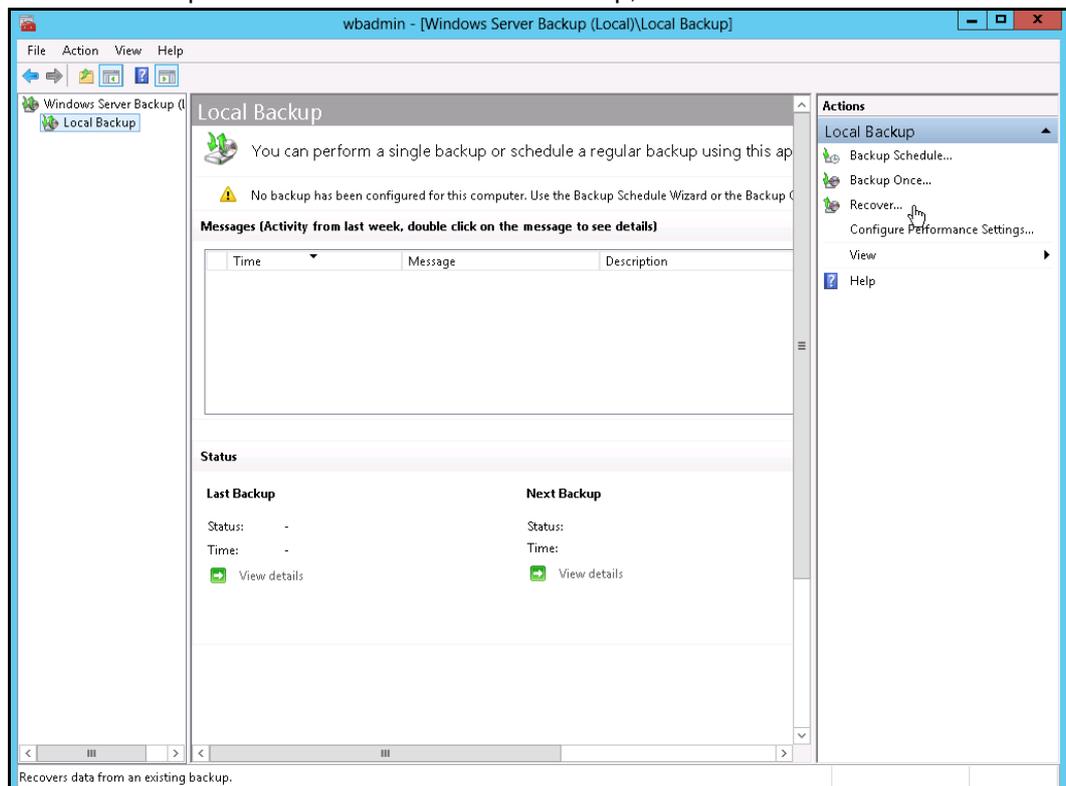
Note: File and folder recovery is not possible from a system state backup performed on Windows Server 2008.

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

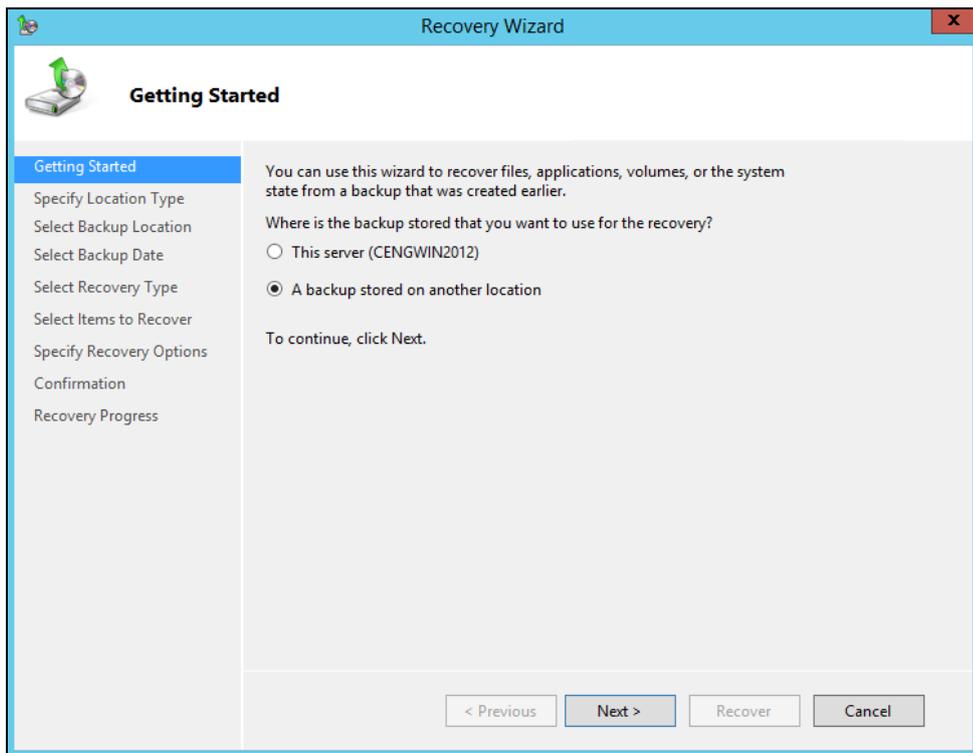
1. Open **Windows Server Backup** from **Administrative Tools** or **Server Manager**.



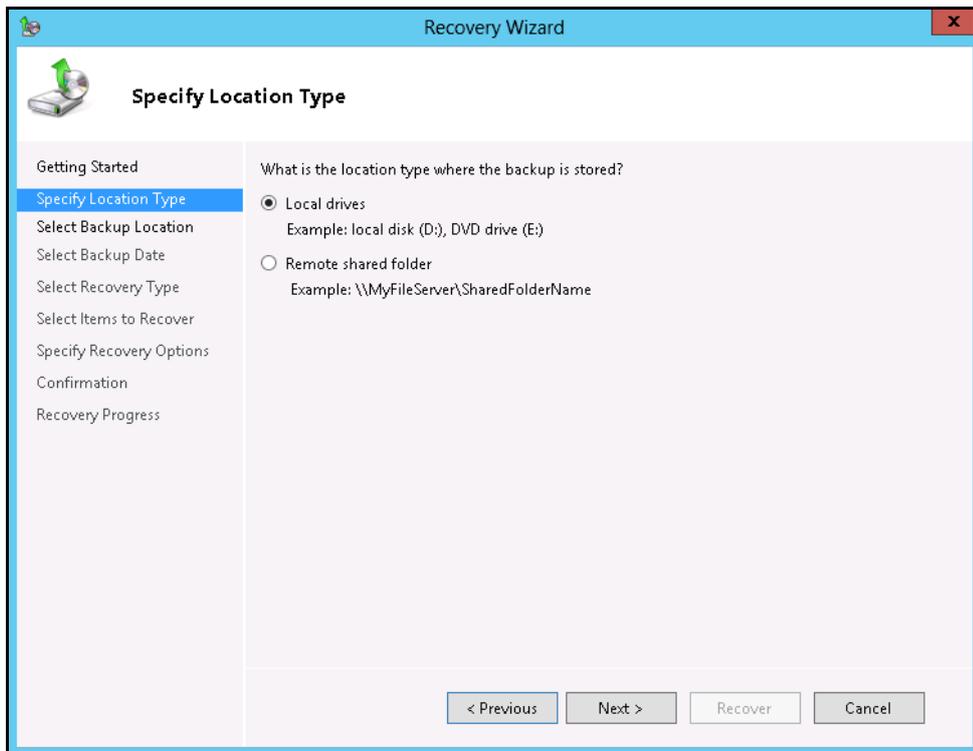
2. In the **Actions** panel under Windows Server Backup, click **Recover...**



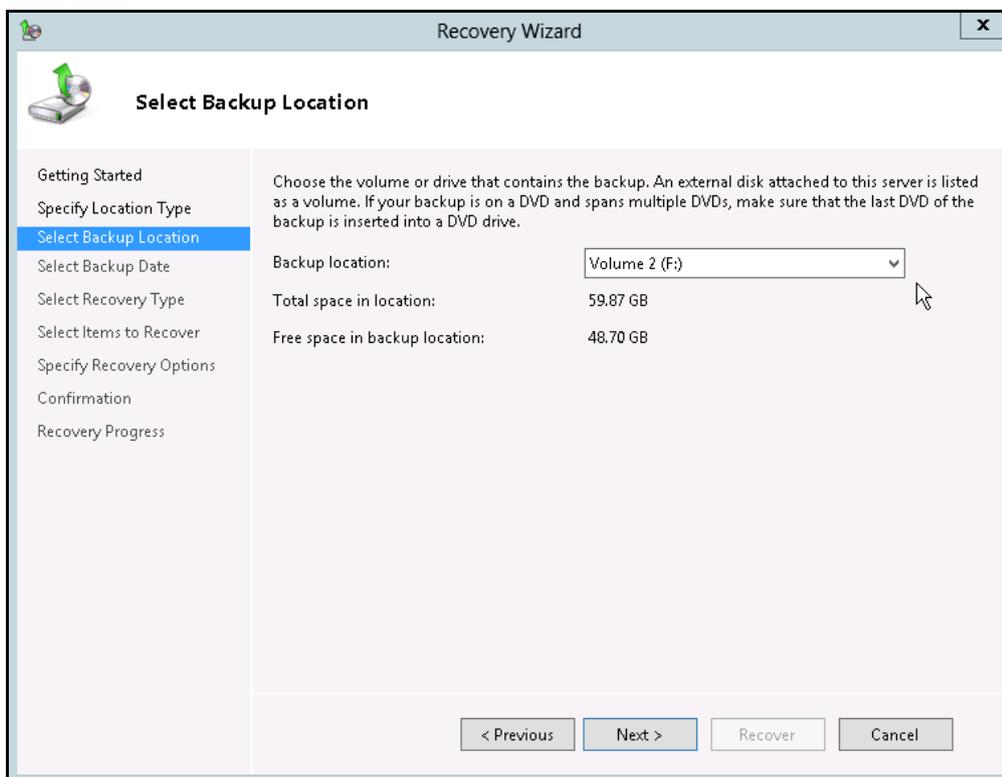
3. On the **Getting Started** page, select **A backup stored on another location**, then click **Next**.



4. On the **Specify Location Type** page, select
 - Click **Local drives**, if the system 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.

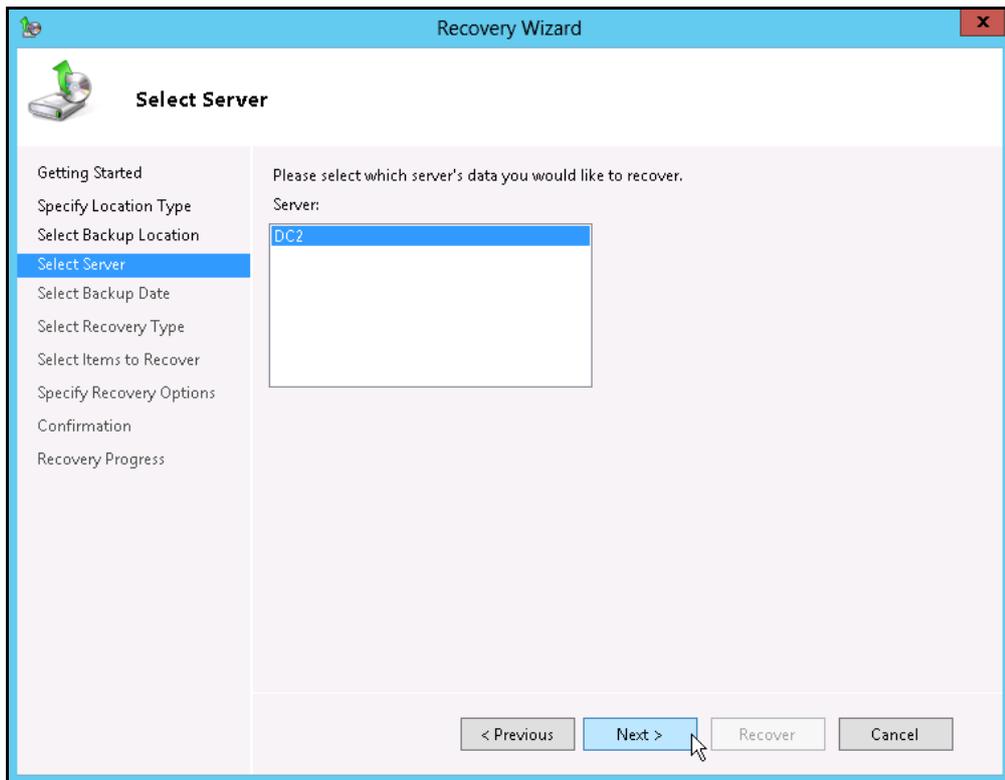


5. On the **Select Backup Location** page, select the volume that contains the system state data.

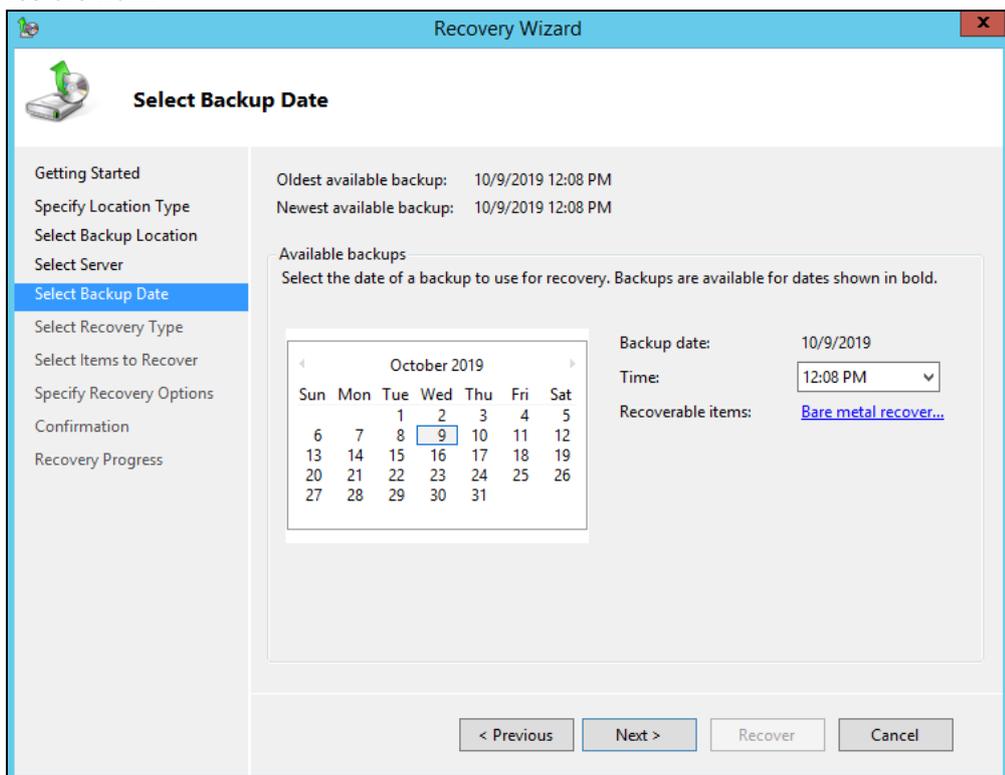


Note: Assuming that the **WindowsImageBackup** folder was copied to the following
F:\WindowsImageBackup

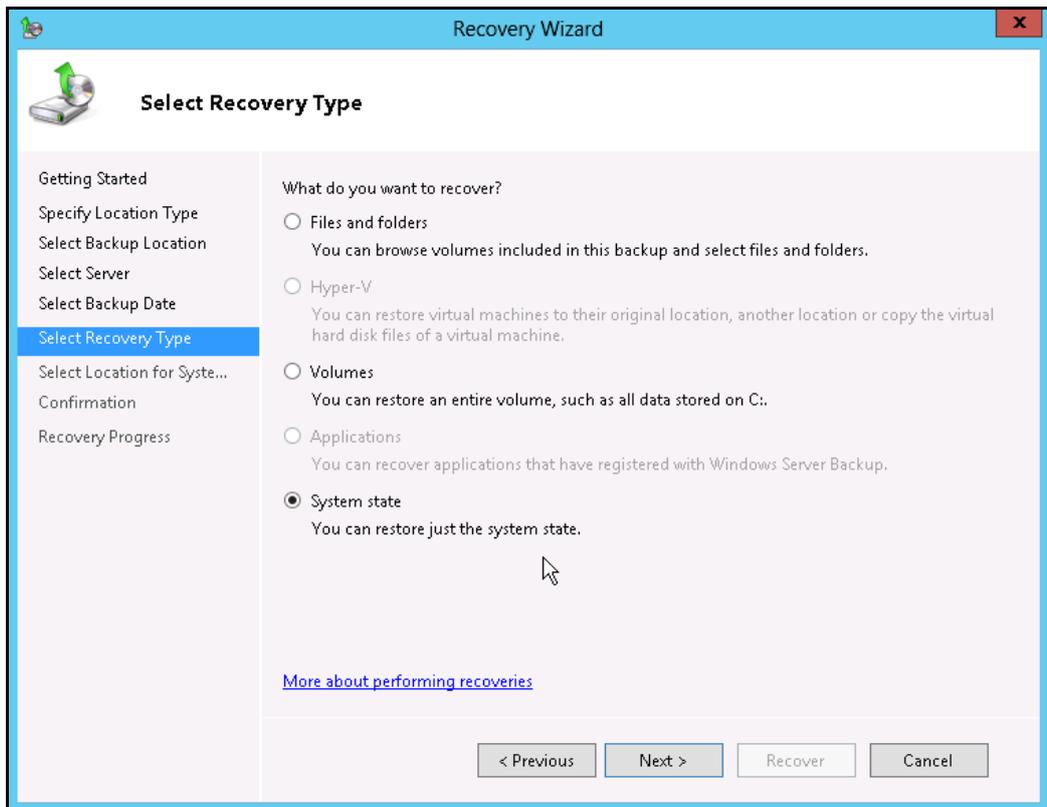
6. On the **Select Server** page, select the server whose data you want to recover.



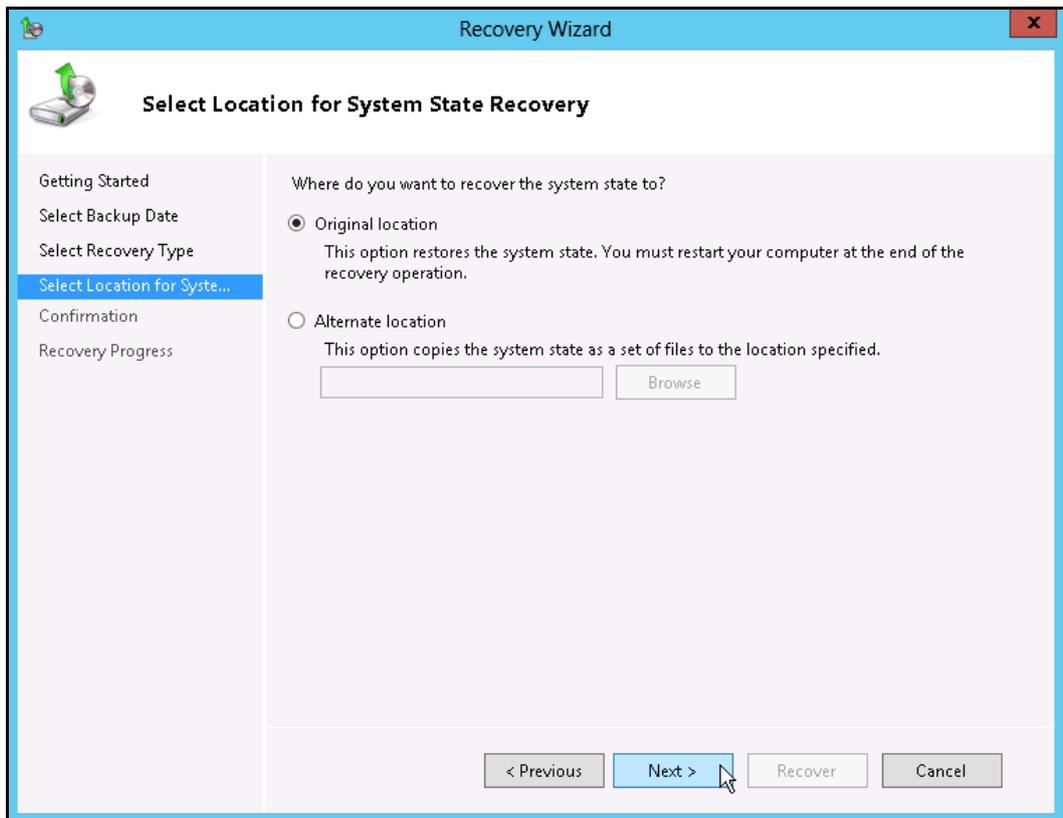
7. On the **Select Backup Date** page, select the point in time of the backup you want to restore from.



8. On the **Select Recovery Type** page, click **System state**.



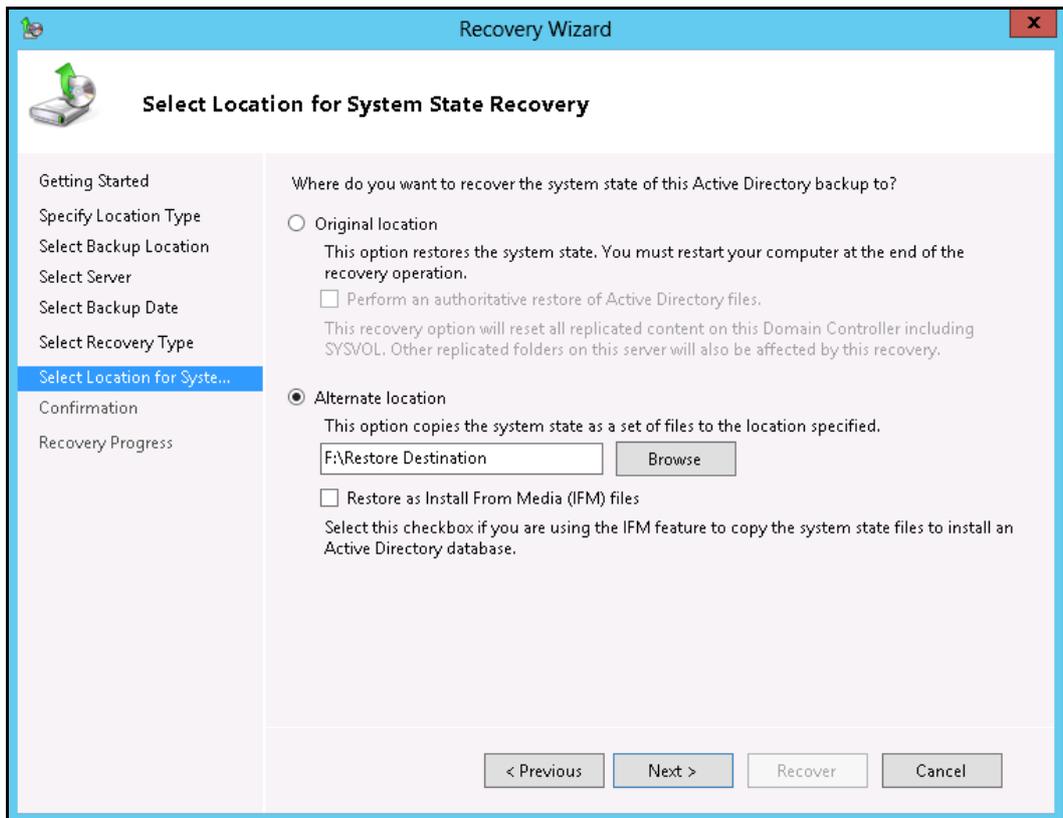
9. On the **Select Location for System State Recovery** page, select
- **Original location**, to restore the system state to the same physical computer from which the system state backup was created
- Or
- **Alternate location**, to restore a copy of the system state as a set of files.



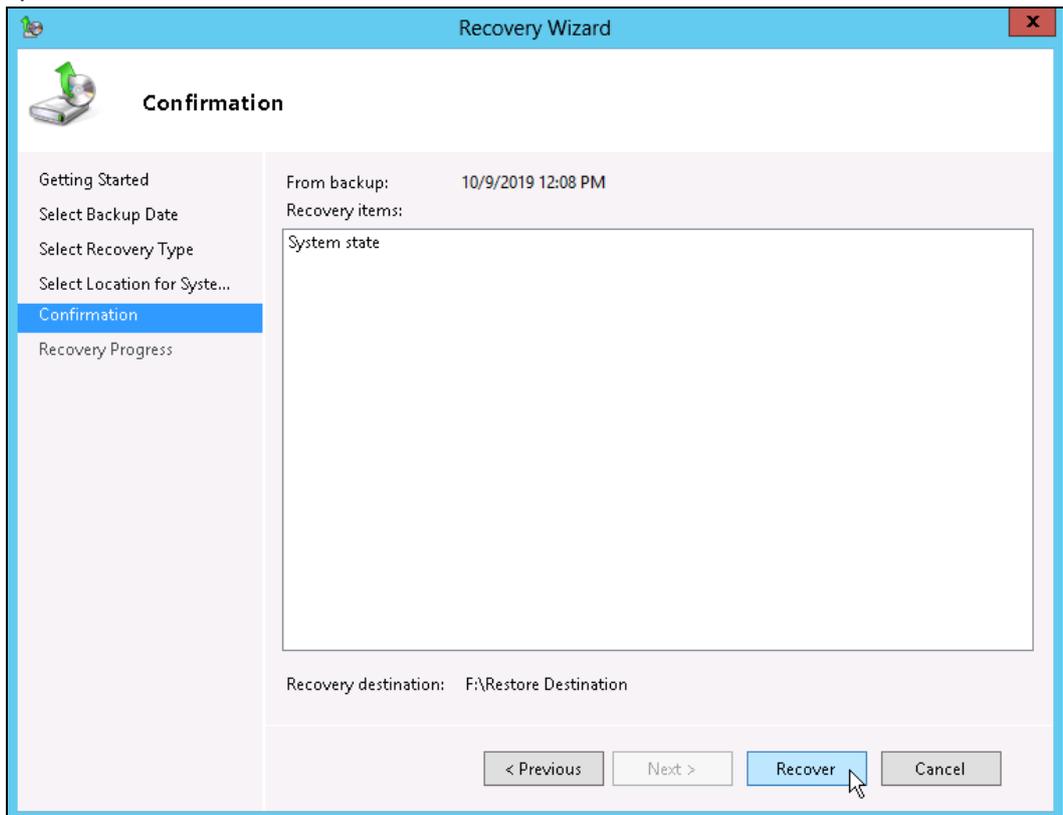
Note: The options displayed are different for system state containing Active Directory Domain Services.

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

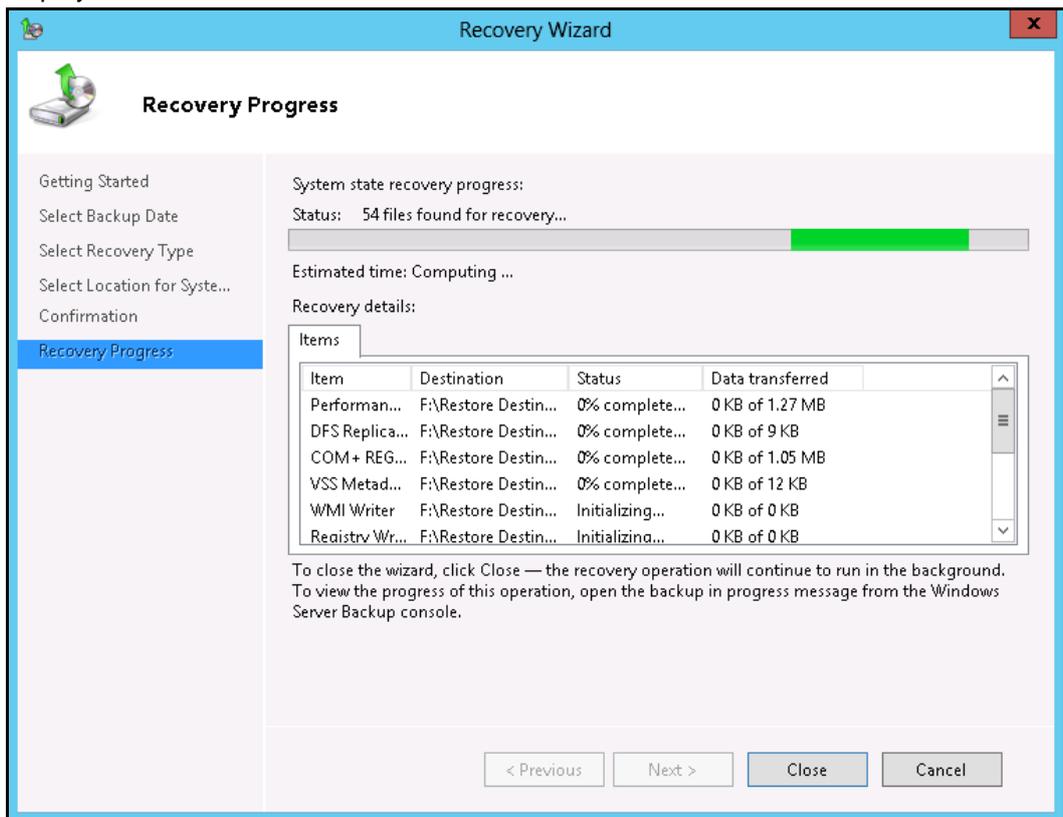
For instructions specific to recovering system state to Active Directory server, see <http://go.microsoft.com/fwlink/?LinkId=143754>



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 is displayed.



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

9 Contact Ahsay

9.1 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/>

9.2 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.

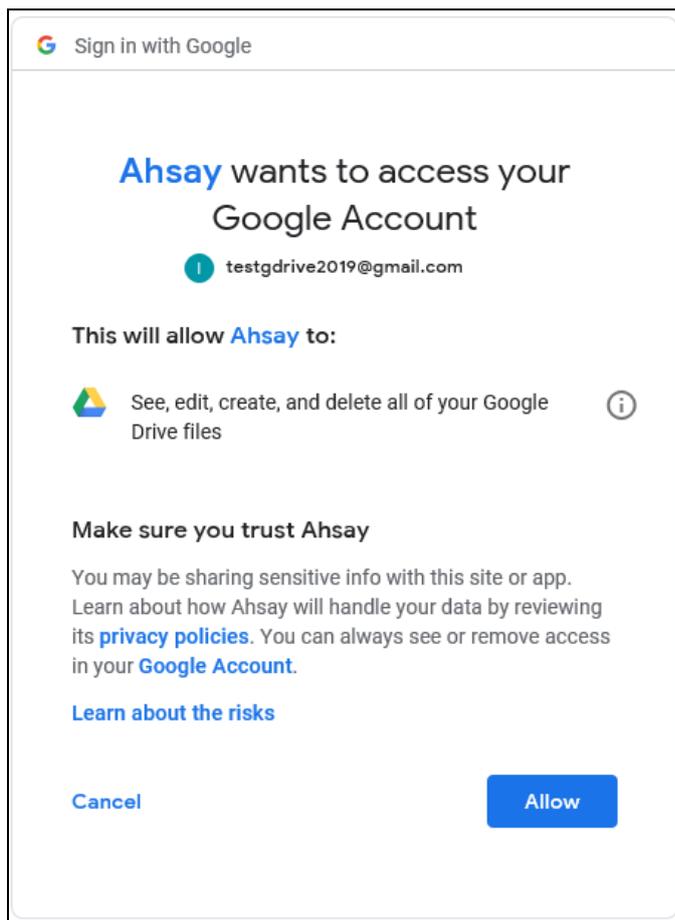
Appendix

Appendix A Cloud Storage as Backup Destination:

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