

Ahsay Online Backup Manager v8

Microsoft Hyper-V Guest Virtual Machine Backup & Restore Guide

Ahsay Systems Corporation Limited

7 April 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. 7	New / Modification
15 May 2020	Modified the System Architecture diagram in Ch. 1.2; Reorganized the Requirements in Ch. 2; Added a diagram for Run Direct Restore in Ch. 3.2, and added diagrams for Non-Cluster and Cluster Environment in Chapters 6.1 and 6.2	New / Modifications
30 July 2020	Updated the Periodic Data Integrity Check (PDIC) diagram in Ch. 7; Added Best Practices and Recommendations in Ch. 2.19; Added Network Drive in Ch. 2.10; Modified Ch. 8.3 Configure Backup Schedule for Automated Backup	New / Modifications
23 September 2020	Updated the Limitations in Ch. 2.20; Modified the Overview on the Backup Process and Periodic Data Integrity Check (PDIC) diagrams in Ch. 7	Modifications
25 January 2021	Updated screenshots in Ch. 2.5; Updated login steps in Ch. 5; Updated the PDIC diagram in Ch. 7	Modifications
7 April 2021	Updated Ch. 7; Added sub-chapters for the detailed process diagrams in Ch. 7.1, 7.2, 7.2.1, 7.2.2 and 7.3	New / Modifications

Table of Contents

1	Overview.....	1
1.1	What is this software?	1
1.2	System Architecture.....	1
2	Preparing for Backup and Restore.....	2
2.1	Hardware Requirement	2
2.2	Software Requirement	2
2.3	Antivirus Exclusion.....	2
2.4	AhsayOBM Installation.....	2
2.5	License	2
2.5.1	Run Direct Restore	3
2.5.2	Granular Restore	3
2.6	Backup Quota	3
2.7	Java Heap Size.....	4
2.8	Permissions	4
2.9	Temporary Directory	4
2.9.1	For Hyper-V Server in Failover Cluster Environment	4
2.9.2	For Hyper-V Server in Non-Cluster Environment	4
2.10	Network Drive	4
2.11	Hyper-V Services	5
2.12	Hyper-V Backup Methods	9
2.12.1	VM Snapshot.....	10
2.12.2	Saved State.....	10
2.13	CBT Cluster Services.....	11
2.14	Windows Server 2016 and 2019 RCT Requirement.....	12
2.15	Hyper-V Cluster Setup	13
2.16	Guest VM Dependencies	13
2.17	Run Direct Restore	13
2.17.1	Supported Guest VM Operating System	13
2.17.2	NFS Service	14
2.17.3	For Restore to the Original Hyper-V Host	14
2.17.4	For Restore to a Different (Standby) Hyper-V Host.....	15
2.18	Granular Restore	16
2.18.1	Operating System.....	16
2.18.2	Available Spare Drive Letter	16
2.18.3	Network Requirements	16
2.18.4	Other Dependencies.....	17
2.19	Best Practices and Recommendations.....	17
2.20	Limitations.....	17

2.20.1	Run Direct Restore	18
2.20.2	Granular Restore	18
3	Run Direct.....	19
3.1	What is Run Direct?	19
3.2	How does Run Direct Restore work?	19
3.3	Benefits of using Run Direct Restore	21
4	Granular Restore Technology	22
4.1	What is Granular Restore Technology?.....	22
4.2	How does Granular Restore work?	23
4.3	Benefits of using Granular Restore	23
5	Starting AhsayOBM	26
5.1	Login to AhsayOBM with no 2FA	26
5.2	Login to AhsayOBM with 2FA using Twilio	28
5.3	Login to AhsayOBM with 2FA using Mobile Authentication	30
6	Creating a Hyper-V Backup Set	33
6.1	Non-Cluster Environment.....	33
6.1.1	Run Direct Backup Set	34
6.1.2	Non-Run Direct Backup Set.....	45
6.2	Cluster Environment.....	53
6.2.1	Run Direct Backup Set	55
6.2.2	Non-Run Direct Backup Set.....	64
7	Overview on the Backup Process	73
7.1	Periodic Data Integrity Check (PDIC) Process	74
7.2	Backup Set Index Handling Process	76
7.2.1	Start Backup Job	76
7.2.2	Completed Backup Job.....	77
7.3	Data Validation Check Process.....	78
8	Running Backup Jobs	79
8.1	Login to AhsayOBM.....	79
8.2	Start a Manual Backup.....	79
8.3	Configure Backup Schedule for Automated Backup	82
9	Restoring Hyper-V Guest Virtual Machines.....	87
	Restore Options	87
10	Run Direct Restore	89
10.1	Original Hyper-V Host	89
10.1.1	Start up a guest VM from Backup Destination without Auto Migration Enabled	89

10.1.2 Migrate Virtual Machine (Permanently Restore).....	93
10.1.3 Stop Run Direct Virtual Machines	95
10.1.4 Start up a guest VM from Backup Destination with Auto Migration Enabled	96
10.2 Different (Standby) Hyper-V Host.....	101
10.2.1 Start up a guest VM from Backup Destination without Auto Migration Enabled	101
10.2.2 Migrate Virtual Machine (Permanently Restore).....	105
10.2.3 Stop Run Direct Virtual Machines	108
10.2.4 Start up a guest VM from Backup Destination with Auto Migration Enabled	109
11 Non-Run Direct Restore	114
11.1 Original Hyper-V Host	114
11.1.1 Restore of Guest VM to the Original Hyper-V Host (Original Location) 114	
11.1.2 Restore of Guest VM to the Original Hyper-V Host (Alternate Location) 118	
11.2 Different (Standby) Hyper-V Host.....	122
Restore of a Guest VM to a Different (Standby) Hyper-V Host.....	122
11.3 Individual Virtual Disk Restore	127
Restore of an Individual Virtual Disk to Original/Different Guest VM	127
12 Granular Restore	133
Start Granular Restore	133
13 Contact Ahsay.....	141
13.1 Technical Assistance	141
13.2 Documentation.....	141

1 Overview

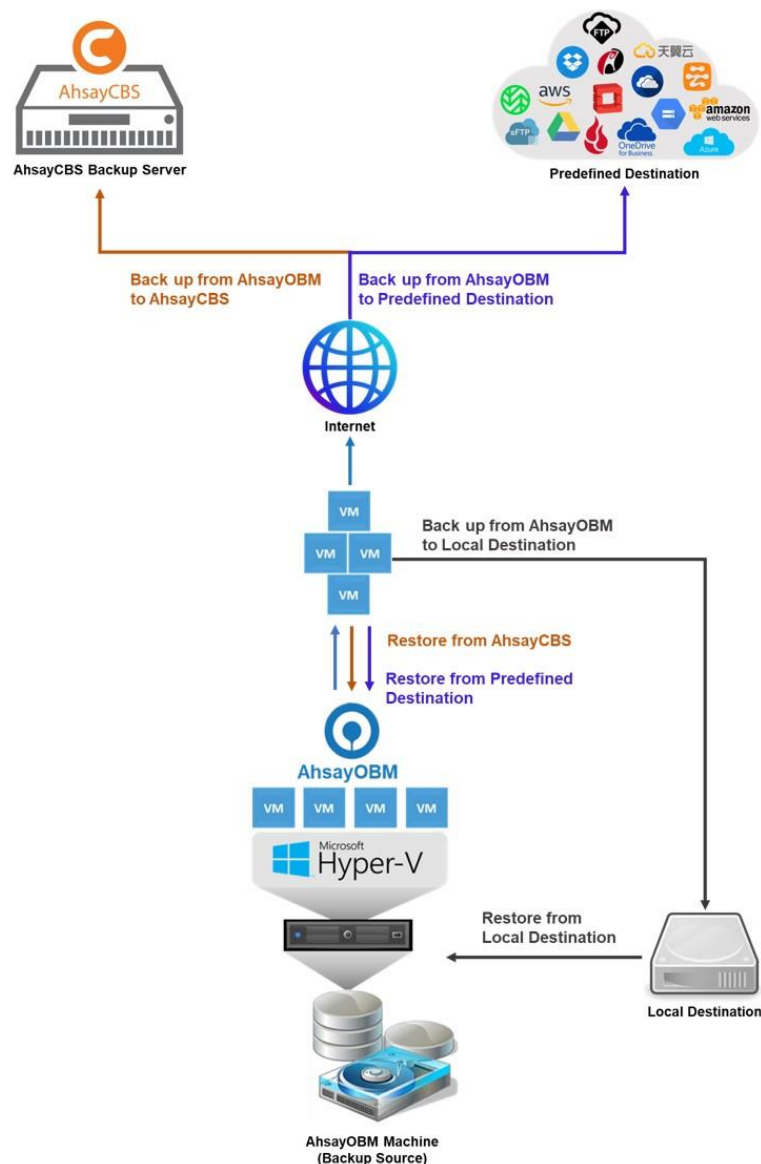
1.1 What is this software?

Ahsay brings you specialized client backup software, namely AhsayOBM, to provide a comprehensive backup solution for your Hyper-V host machine backup. The Hyper-V module of AhsayOBM provides you with a set of tools to protect Hyper-V host machine and guest VMs. This includes a machine backup feature and instant recovery feature (with the use of **Run Direct** technology), to ensure that mission critical machines are back up and running within minutes of a disaster.

1.2 System Architecture

The following high-level system architecture diagram illustrates the major elements involved in the backup process of a Hyper-V host with AhsayOBM and AhsayCBS.

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



2 Preparing for Backup and Restore

2.1 Hardware Requirement

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

2.2 Software Requirement

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

2.3 Antivirus Exclusion

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

https://wiki.ahsay.com/doku.php?id=public:8014_faq:suggestion_on_antivirus_exclusions

NOTE

The bJW.exe process is automatically added to Windows Defender exclusion list for Windows 10, 2016, and 2019 during installation / upgrade via installer or upgrade via AUA.

2.4 AhsayOBM Installation

The latest version of AhsayOBM must be installed on the Hyper-V server. For Hyper-V Cluster environment the latest version of AhsayOBM must be installed on all Cluster nodes.

2.5 License

AhsayOBM user account has sufficient Hyper-V add-on modules or CPU sockets assigned. Hyper-V Cluster backup sets will require one AhsayOBM license per node. For Hyper-V Cluster, the required number of CPU sockets must be equivalent to the total number of CPU sockets for all nodes.

The screenshot displays the 'Backup Client Settings' tab in the AhsayOBM interface. On the left, a sidebar lists navigation options: User Profile, 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 two sections: 'Backup Client' and 'Add-on Modules'. In the 'Backup Client' section, 'AhsayOBM User' is selected with a radio button. The 'Add-on Modules' section lists various services with checkboxes and input fields for configuration. The 'Hyper-V' module is checked and set to 10 Guest VMs. 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 (set to 10), MariaDB Database Server, Microsoft SQL Server, Oracle Database Server, Lotus Notes, Windows System State Backup, ShadowProtect System Backup, NAS - Synology, Continuous Data Protection, In-File Delta, and Office 365 Backup.

2.5.1 Run Direct Restore

Run Direct feature is already included with the basic Hyper-V add-on modules or CPU socket license. Contact your backup service provider for more details.

2.5.2 Granular Restore

An OpenDirect / Granular Restore add-on module license is required per backup set for this feature to work. Contact your backup service provider for more details.

The screenshot shows the 'Backup Client Settings' tab in the AhsayOBM interface. On the left is a sidebar with 'User Profile' selected. The main area has tabs for 'General', 'Backup Client Settings', 'Contact', 'User Group', 'Authentication', and 'Mobile Backup'. Under 'Backup Client Settings', it says 'Settings of the client backup agent for this user.' Below this, the 'Backup Client' section has two radio buttons: 'AhsayOBM User' (selected) and 'AhsayACB User'. The 'Add-on Modules' section contains two columns of modules, each with a checkbox and an input field for the number of VMs. The modules and their settings are: Microsoft Exchange Server (0), MySQL Database Server (0), Lotus Domino (0), Windows System Backup (0), VMware (Guest VM, 0), Microsoft Exchange Mailbox (0), NAS - QNAP (0), Mobile (max. 10) (checked), Volume Shadow Copy (0), OpenDirect / Granular Restore (10, checked), MariaDB Database Server (0), Microsoft SQL Server (0), Oracle Database Server (0), Lotus Notes (0), Windows System State Backup (0), Hyper-V (Guest VM, 10, checked), ShadowProtect System Backup (0), NAS - Synology (0), Continuous Data Protection (0), In-File Delta (0), and Office 365 Backup (0).

2.6 Backup Quota

AhsayOBM user account has sufficient quota assigned to accommodate the storage of the guest VMs. (Please contact your backup service provider for details).

Hyper-V guest VMs contain three types of virtual disks:

- Fixed Hard Disk.
- Dynamic Hard Disk.
- Differencing Hard Disk.

When AhsayOBM backs up a Hyper-V guest VMs for an initial or subsequent full backup jobs:

- Using fixed Hard Disks, it will back up the provisioned size, e.g. for a 500GB fixed virtual hard disk 500GB will be backed up to the storage designation.
- Using Dynamic Hard Disk or Differencing Hard Disk it will back up the used size, e.g. for a 500GB fixed virtual hard disk, 20GB will be backed up to the storage designation if only 20GB are used.

NOTE

As compression is not enabled for Granular backup sets, to optimize restore performance, the storage quota required will be higher than non-Granular backup sets. Contact your backup service provider for details.

2.7 Java Heap Size

The default Java heap size setting on AhsayOBM is 2048MB, for Hyper-V backups it is highly recommended to increase the Java heap size setting to improve backup and restore performance. (The actual heap size is dependent on amount of free memory available on your Hyper-V server).

Delta generation of large VHD files is a memory intensive process; therefore, it is recommended that the Java heap size to be at least 2048MB - 4096MB. The actual required Java heap size is subject to various factors including files size, delta mode, backup frequency, etc.

Refer to the following article for details:

https://wiki.ahsay.com/doku.php?id=public:8011_faq:how_to_modify_the_java_heap_size_of_ahsayobc&s%5b%5d

2.8 Permissions

The Windows login account used for installation and operation of the AhsayOBM client machine requires Administrator privileges.

The operating system account for setting up the Hyper-V / Hyper-V Cluster backup set must have administrator permission (e.g. administrative to access the cluster storage).

NOTE

For Granular Restore, Windows User Account Control (UAC) must be disabled.

2.9 Temporary Directory

For stand-alone Hyper-V server, AhsayOBM uses the temporary folder for storing backup set index files and any incremental or differential delta files generated during a backup job. To ensure optimal backup / restore performance, it should be located on a local drive with plenty of free disk space. It should not be on the **Windows System C:\ drive**.

2.9.1 For Hyper-V Server in Failover Cluster Environment

- Hyper-V Server 2008, 2008 R2, 2012, 2012 R2, the temporary directory must be set to a local drive of the Cluster Node.
- Hyper-V Server 2016 and 2019, the temporary directory must be set to the Cluster Shared Volume (CSV).

2.9.2 For Hyper-V Server in Non-Cluster Environment

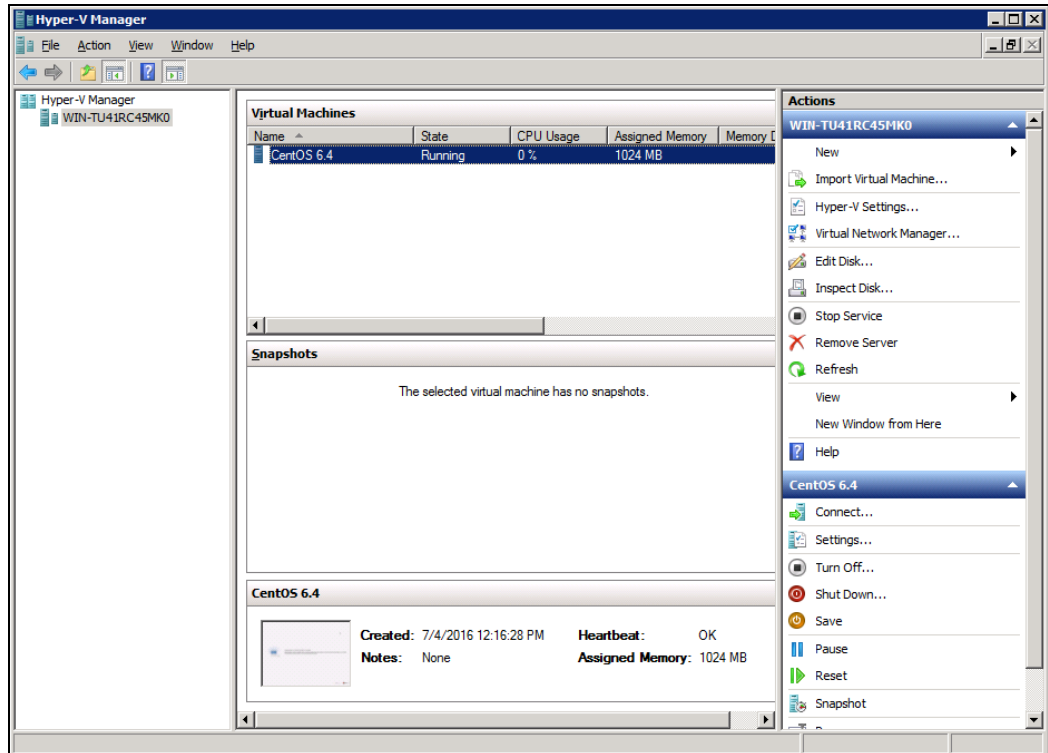
For **Hyper-V Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019** in a Non-Cluster environment, the temporary directory must be set to a local drive on the Hyper-V Server.

2.10 Network Drive

The login accounts for network drives must have read and write access permission to ensure that backup and restore would be successful.

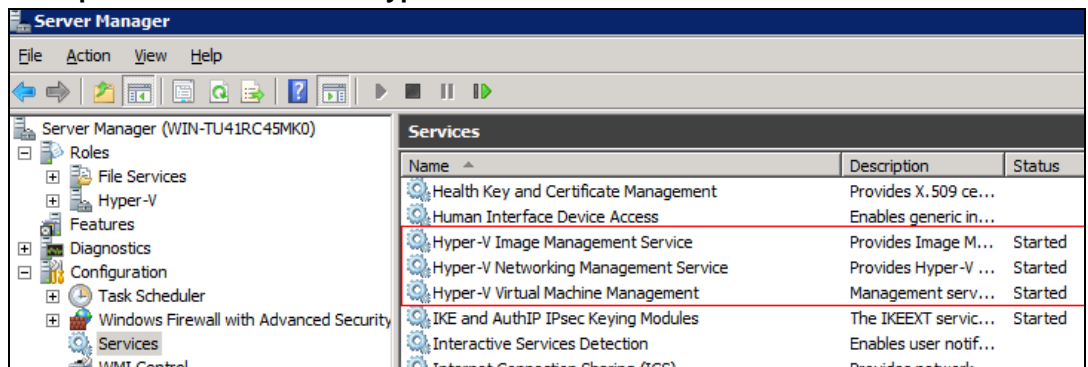
2.11 Hyper-V Services

1. The Hyper-V management tools are installed on the server. For Hyper-V Cluster environments Hyper-V management tools is installed on all Cluster nodes.



2. The Hyper-V services are started on the server. For Hyper-V Cluster environments the Hyper-V services are started on all Cluster nodes.

Example: Windows 2008 R2 Hyper-V



3. The **Microsoft Hyper-V VSS Writer** is installed and running on the Hyper-V server and the writer state is Stable. This can be verified by running the vssadmin list writers command.

Example:

```
C:\Users\Administrator>vssadmin list writers
vssadmin 1.1 - Volume Shadow Copy Service administrative
command-line tool
(C) Copyright 2001-2005 Microsoft Corp.
Writer name: 'Task Scheduler Writer'
Writer Id: {d61d61c8-d73a-4eee-8cdd-f6f9786b7124}
Writer Instance Id: {1bddd48e-5052-49db-9b07-b96f96727e6b}
State: [1] Stable
Last error: No error
```

Writer name: 'VSS Metadata Store Writer'
 Writer Id: {75dfb225-e2e4-4d39-9ac9-ffa9ff65ddf06}
 Writer Instance Id: {088e7a7d-09a8-4cc6-a609-ad90e75ddc93}
 State: [1] Stable
 Last error: No error

Writer name: 'Performance Counters Writer'
 Writer Id: {0badalde-01a9-4625-8278-69e735f39dd2}
 Writer Instance Id: {f0086dda-9efc-47c5-8eb6-a944c3d09381}
 State: [1] Stable
 Last error: No error

Writer name: 'System Writer'
 Writer Id: {e8132975-6f93-4464-a53e-1050253ae220}
 Writer Instance Id: {8de7ed2b-8d69-43dd-beec-5bfb79b9691c}
 State: [1] Stable
 Last error: No error

Writer name: 'SqlServerWriter'
 Writer Id: {a65faa63-5ea8-4ebc-9dbd-a0c4db26912a}
 Writer Instance Id: {1f668bf9-38d6-48e8-81c4-2df60a3fab57}
 State: [1] Stable
 Last error: No error

Writer name: 'ASR Writer'
 Writer Id: {be000cbe-11fe-4426-9c58-531aa6355fc4}
 Writer Instance Id: {01499d55-61da-45bc-9ale-76161065630f}
 State: [1] Stable
 Last error: No error

Writer name: 'Microsoft Hyper-V VSS Writer'
Writer Id: {66841cd4-6ded-4f4b-8f17-fd23f8ddc3de}
Writer Instance Id: {a51919e3-0256-4ecf-8530-2f600de6ea68}
State: [1] Stable
Last error: No error

Writer name: 'COM+ REGDB Writer'
 Writer Id: {542da469-d3e1-473c-9f4f-7847f01fc64f}
 Writer Instance Id: {7303813b-b22e-4967-87a3-4c6a42f861c4}
 State: [1] Stable
 Last error: No error

Writer name: 'Shadow Copy Optimization Writer'
 Writer Id: {4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f}
 Writer Instance Id: {d3199397-ec58-4e57-ad04-e0df345b5e68}
 State: [1] Stable
 Last error: No error

Writer name: 'Registry Writer'
 Writer Id: {afbab4a2-367d-4d15-a586-71dbb18f8485}
 Writer Instance Id: {25428453-2ded-4204-800f-e87204f2508a}
 State: [1] Stable
 Last error: No error

Writer name: 'BITS Writer'
 Writer Id: {4969d978-be47-48b0-b100-f328f07ac1e0}
 Writer Instance Id: {78fa3f1e-d706-4982-a826-32523ec9a305}
 State: [1] Stable
 Last error: No error

```

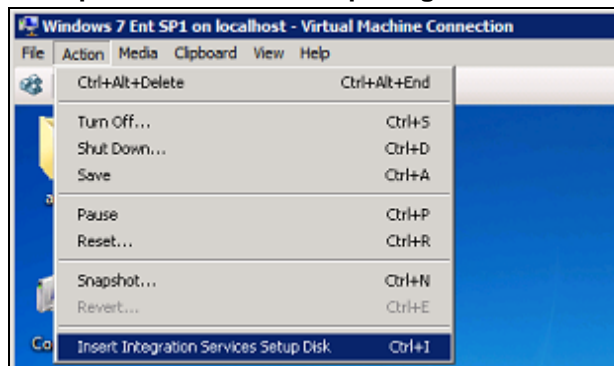
Writer name: 'WMI Writer'
Writer Id: {a6ad56c2-b509-4e6c-bb19-49d8f43532f0}
Writer Instance Id: {3efcf721-d590-4e50-9a37-845939ca51e0}
State: [1] Stable
Last error: No error

```

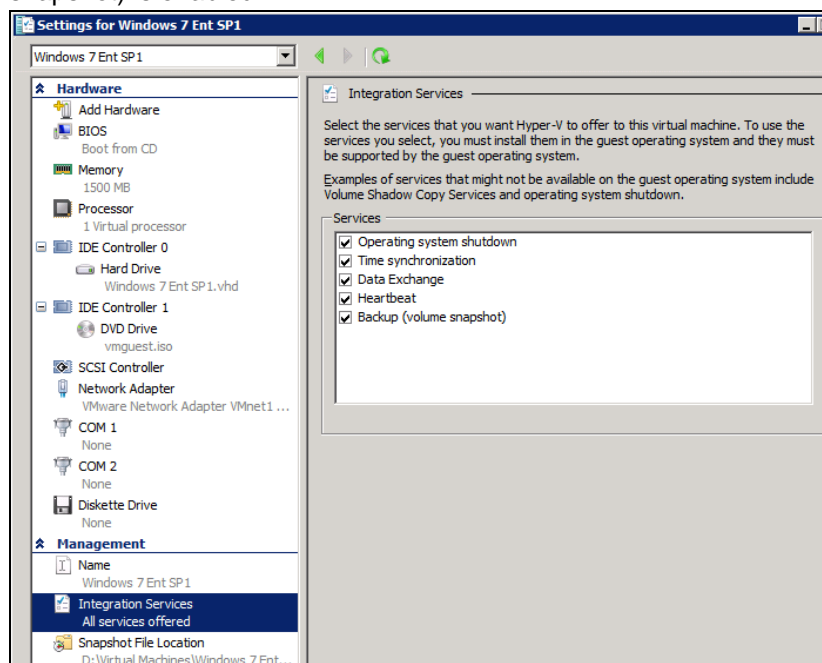
4. Integration Service

- i. If Integration services is not installed / updated on a guest VM or the guest operating system is not supported by Integration Services, the corresponding VM will be paused or go into a saved state during the snapshot process for both backup and restore, and resume when the snapshot is completed. Furthermore, the corresponding VM uptime will also be reset to 00:00:00 in the Hyper-V Manager.
- ii. Installing or updating Integration Services guest VM(s) may require a restart of the guest VM to complete the installation.
 - To install Integration Services
 - In Hyper-V Manager connect to the guest VM and select Action > Insert Integration Services Setup disk

Example: Windows 7 Enterprise guest



- If the guest operating system supports live VM backup, the Backup (volume snapshot) is enabled.



- The related Integration Services are running on the guest VM:

Example: Windows 7 Enterprise guest

Name	Description	Status	Startup Type
Distributed Transaction Coordinator	Coordinates tra...	Started	Manual
DNS Client	The DNS Client ...	Started	Automatic
Encrypting File System (EFS)	Provides the co...		Manual
Extensible Authentication Protocol	The Extensible ...		Manual
Fax	Enables you to ...		Manual
Function Discovery Provider Host	The FDPHOST s...		Manual
Function Discovery Resource Publication	Publishes this c...		Manual
Group Policy Client	The service is re...	Started	Automatic
Health Key and Certificate Management	Provides X.509 ...		Manual
HomeGroup Listener	Makes local co...		Manual
HomeGroup Provider	Performs netwo...		Manual
Human Interface Device Access	Enables generic...		Manual
Hyper-V Data Exchange Service	Provides a mec...	Started	Automatic
Hyper-V Guest Shutdown Service	Provides a mec...	Started	Automatic
Hyper-V Heartbeat Service	Monitors the st...	Started	Automatic
Hyper-V Time Synchronization Service	Synchronizes th...	Started	Automatic
Hyper-V Volume Shadow Copy Requestor	Coordinates the...	Started	Automatic
IKE and AuthIP IPsec Keying Modules	The IKEEXT serv...		Manual

Example: CentOS 6.4 Linux guest

To check if Linux Integration Services is running on the Linux guest:

```
# lsmod | grep hv

hv_netvsc          23667  0
hv_utils          7012   0
hv_storvsc        10022  2
hv_vmbus          91567  4
hv_netvsc,hv_utils,hid_hyperv,hv_storvsc

# ps -ef|grep hv
root      267      2  0 18:07 ?        00:00:00
[hv_vmbus_con/0]
root      268      2  0 18:07 ?        00:00:00
[hv_vmbus_ctl/0]
root      269      2  0 18:07 ?        00:00:00
[hv_vmbus_ctl/0]
root      270      2  0 18:07 ?        00:00:00
[hv_vmbus_ctl/0]
root      271      2  0 18:07 ?        00:00:00
[hv_vmbus_ctl/0]
root      272      2  0 18:07 ?        00:00:00
[hv_vmbus_ctl/0]
root      273      2  0 18:07 ?        00:00:00
[hv_vmbus_ctl/0]
root      274      2  0 18:07 ?        00:00:00
[hv_vmbus_ctl/0]
root      275      2  0 18:07 ?        00:00:00
[hv_vmbus_ctl/0]
root      276      2  0 18:07 ?        00:00:00
[hv_vmbus_ctl/0]
root      277      2  0 18:07 ?        00:00:00
[hv_vmbus_ctl/0]
root      1174     1  0 18:07 ?        00:00:00
/usr/sbin/hv_kvp_daemon
root      1185     1  0 18:07 ?        00:00:00
/usr/sbin/hv_vss_daemon
root      1332    1316  0 18:11 pts/0    00:00:00 grep hv
```

- Please refer to the following articles for further details on:
 - Considerations for backing up and restoring VMs
[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn798286\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn798286(v=ws.11))
 - Supported Windows Guest Operating Systems for Hyper-V in Windows Server 2012
[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn792028\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn792028(v=ws.11))
 - Supported Windows Guest Operating Systems for Hyper-V in Windows Server 2012 R2
[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn792027\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn792027(v=ws.11))
 - Supported Linux and FreeBSD VMs for Hyper-V on Windows
<https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/Supported-Linux-and-FreeBSD-virtual-machines-for-Hyper-V-on-Windows>
 - Supported CentOS and Red Hat Enterprise Linux VMs on Hyper-V
<https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/supported-centos-and-red-hat-enterprise-linux-virtual-machines-on-hyper-v>
 - Supported Ubuntu VMs on Hyper-V <https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/supported-ubuntu-virtual-machines-on-hyper-v>
 - Linux Integration Services Version 4.0 for Hyper-V
<https://rlevchenko.com/2015/08/18/linux-integration-services-version-4-0-for-hyper-v/>
 - Managing Hyper-V Integration Services
https://msdn.microsoft.com/en-us/virtualization/hyperv_on_windows/user_guide/managing_ics
 - Hyper-V on Window Server
<https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/hyper-v-on-windows-server>
- 5. For Hyper-V 2008 R2 server in order to use Run Direct restore feature the "**Microsoft Security Advisory 3033929**" security update must be installed.
 Please refer to the following KB article from Microsoft for further details:
<https://support.microsoft.com/en-us/kb/3033929>
- 6. For Run Direct Hyper-V Cluster backup sets the storage destination must be accessible by all Hyper-V nodes.
- 7. For Hyper-V Cluster backup sets, the guest VMs must be created and managed by the Failover Cluster Manager.

2.12 Hyper-V Backup Methods

AhsayOBM v8 supports two methods for Hyper-V guest VM backup, VM Snapshot and Saved State.

2.12.1 VM Snapshot

The VM snapshot method is the preferred backup option, as it supports live guest VM backups. This means guest VM will not be put into a saved state when a VSS snapshot is taken during a backup job. So, it will not affect the availability of any applications or services running on the guest VM every time a backup job is performed.

NOTE

If the VM Snapshot method cannot be used, AhsayOBM will automatically use the Saved State method.

1. The guest VM must be running.
2. Integration services must be enabled on the guest VM.
3. The Hyper-V Volume Shadow Copy Requestor service is running on the guest VM installed with Windows operating system. Please refer to the following article for further details: <https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/reference/integration-services#hyper-v-volume-shadow-copy-requestor>
4. For guest VMs installed with Linux / FreeBSD operating systems, the VSS Snapshot daemon is required for live backups, not all Linux / FreeBSD versions support live backup on Hyper-V. For example, only FreeBSD 11.1 supports live backup while for Ubuntu, version 14.04 LTS to 17.04 LTS supports live backups. Please refer to the following article for further details: <https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/supported-linux-and-freebsd-virtual-machines-for-hyper-v-on-windows>
5. The guest VM volumes must use a file system which supports the use of VSS snapshots, i.e. NTFS or ReFS.
6. The guest VMs snapshot file location must be set to the same volume in the Hyper-V host as the VHD file(s).
7. The guest VM volumes have to reside on basic disks. Dynamic disks cannot be used within the guest VM.

NOTE

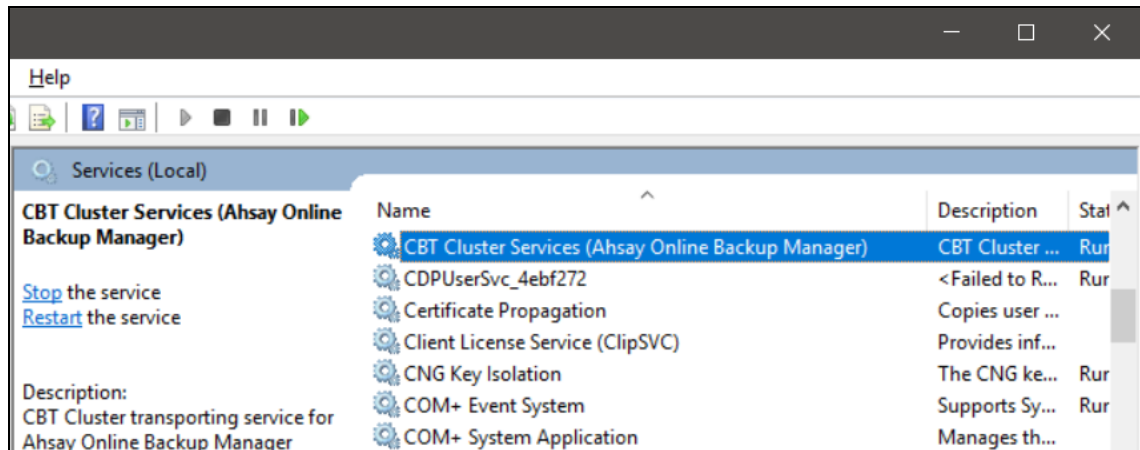
Some older Windows operating systems installed on guest VM's which do not support either Integration Services or the Hyper-V Volume Shadow Copy Requestor Service, will not support VM snapshot method, for example, Microsoft Windows 2000, Windows XP, or older Linux/FreeBSD versions.

2.12.2 Saved State

If any of the VM Snapshot method requirements cannot be fulfilled, AhsayOBM will automatically use the Save State method. When the Saved State method is used, the guest VM is placed into a saved state while the VSS snapshot is created (effectively shut down), and the duration is dependent on the size of VM and performance of Hyper-V host. The downside is it may affect the availability of any applications or services running on the guest VM every time a backup job is performed.

2.13 CBT Cluster Services

CBT Cluster Services (Ahsay Online Backup Manager) is installed and enabled upon installation / upgrade to version AhsayOBM v8.1.0.0 or above on Windows 2008/2008R2 or Windows 2012/2012R2.



1. **CBT (Changed Block Tracking)** Cluster Services is used to optimize incremental backups of VMs by keeping a log of the blocks of data that have changed since the previous snapshot making incremental backups much faster. When AhsayOBM performs a backup, CBT feature can request transmissions of only the blocks that changed since the last backup, or the blocks in use.

CBT service is supported on all the backup destinations for AhsayOBM.

2. CBT cluster service is only installed on Windows x64 machine.
3. Check if **CBTFilter** is enabled.

Example:

- i. This can be verified by running the net start CBTFilter command.

```
C:\Users\Administrator>net start CBTFilter
The requested service has already been started.

More help is available by typing NET HELPMSG 2182.
```

- ii. **NOTE:** For Windows Server 2008 R2, if the following error is displayed

```
C:\Users\Administrator>net start CBTFilter
System error 577 has occurred.

Windows cannot verify the digital signature for this file. A
recent hardware or software change might have installed a
file that is signed incorrect or damaged, or that might be
malicious software from an unknown source.
```

The issue may be related to the availability of SHA-2 code signing support for Windows Server 2008 R2 (<https://technet.microsoft.com/en-us/library/security/3033929>).

To resolve the issue, install the following patch from Microsoft
<https://www.microsoft.com/en-us/download/confirmation.aspx?id=46083>

Restart the affected server afterward for AhsayOBM to operate properly.

4. CBT Cluster Service and CBTFILTER will **NOT** be installed on Windows Server 2016 and 2019 where a built-in system called Resilient Change Tracking (RCT) will be used instead. For details of RCT, please refer to [Windows Server 2016 and 2019 RCT Requirement](#).
5. If a Windows Hyper-V 2008/2008 R2/2012/2012 R2 with AhsayOBM already installed is upgraded to Windows 2016/2019, it is recommended that both **CBT Cluster Service** and **CBTFILTER** should be uninstalled using the following batch files:

🔵 UninstallCBTClusterService.bat

```
C:\Program Files\AhsayOBM\bin>UninstallCBTClusterService.bat

C:\Program Files\AhsayOBM\bin>Service.exe

-r CBTCluster

Start to remove CBTCluster

Stopping CBTCluster.

CBTCluster stopped.

CBTCluster removed.
```

🔵 UninstallCBTClusterService.bat

```
C:\Program Files\AhsayOBM\bin>UninstallCBTFILTER.bat

C:\Program Files\AhsayOBM\bin>RUNASCMD64.EXE RUNDLL32.EXE
SETUPAPI.DLL,InstallHinfSection DefaultUninstall 132
D:\Program Files\AhsayOBM\bin\CBTFILTER.inf

execute RUNDLL32.EXE SETUPAPI.DLL,InstallHinfSection
DefaultUninstall 132 C:\Program
Files\AhsayOBM\bin\CBTFILTER.inf

run ShellExecuteEx runas RUNDLL32.EXE
SETUPAPI.DLL,InstallHinfSection DefaultUninstall 132
C:\Program Files\AhsayOBM\bin\CBTFILTER.inf

[2020-05-13-11-08-25] Execute return

"RUNDLL32.EXE SETUPAPI.DLL,InstallHinfSection
DefaultUninstall 132 C:\Program
Files\AhsayOBM\bin\CBTFILTER.inf" is executed successfully

exit code=0
```

2.14 Windows Server 2016 and 2019 RCT Requirement

1. AhsayOBM would not install CBT Cluster Services (Ahsay Online Backup Manager) but use the native built-in RCT (Resilient Change Tracking) feature of Windows server 2016 and 2019 instead.

2. The guest VM version in Hyper-V must be 8.0 or above.

Example:

- i. This can be verified by using Windows PowerShell.

```
get-VM | format-table name, version
```

```
PS C:\Users\Administrator> get-VM | format-table name, version
Name      Version
-----
lubuntu 8.0
```

- ii. If the version is not 8.0 or above, then the VM configuration version needs to be upgraded.

```
Update-VMversion <vmname>
```

```
PS C:\Users\Administrator> update-VMversion lubuntu
Confirm
Are you sure you want to perform this action?
Performing a configuration version update of "lubuntu" will prevent it from being migrated to or imported on previous
versions of Windows. This operation is not reversible.
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"):
```

Please refer to the following link of Microsoft for details about the VM version:

<https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/deploy/Upgrade-virtual-machine-version-in-Hyper-V-on-Windows-or-Windows-Server>

2.15 Hyper-V Cluster Setup

For Hyper-V Cluster backup sets:

1. The same version of AhsayOBM must be installed on all Hyper-V Cluster nodes.
2. All Hyper-V Cluster nodes must be running the same Windows version.
3. The same backup user account must be used for all nodes.
4. The same backup set must be used for all nodes
5. The backup schedule must be enabled on all Hyper-V Cluster nodes.

2.16 Guest VM Dependencies

To get full use of Hyper-V, install the appropriate linux-tools and linux-cloud-tools packages to install tools and daemons, e.g. VSS Snapshot Daemon, for use with VMs. Please refer to the following link for the details of requirements for Ubuntu relating to Hyper-V daemons:

<https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/supported-ubuntu-virtual-machines-on-hyper-v>

NOTE

For ease of restore, it is recommended to back up the whole VM (all the virtual disks) rather than individual virtual disks.

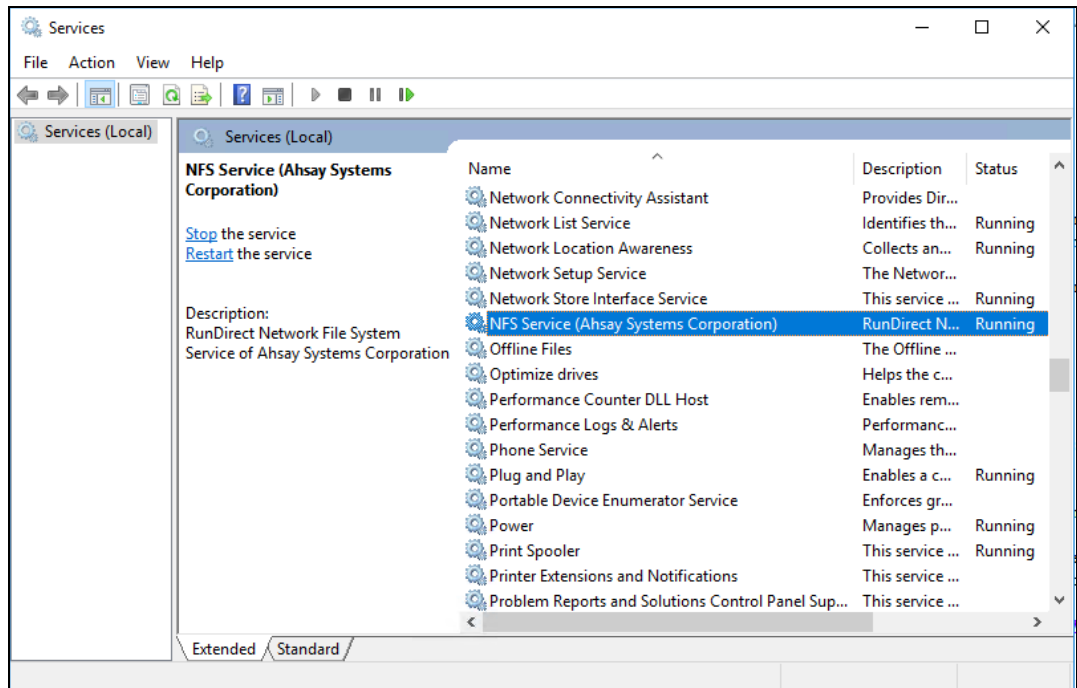
2.17 Run Direct Restore

2.17.1 Supported Guest VM Operating System

Guest VM running on Windows, Linux, and FreeBSD is supported for Run Direct Restore.

2.17.2 NFS Service

Make sure NFS service has started for Run Direct to operate. If the backup destination is located on network drive, the logon account must have sufficient permission to access the network resources.



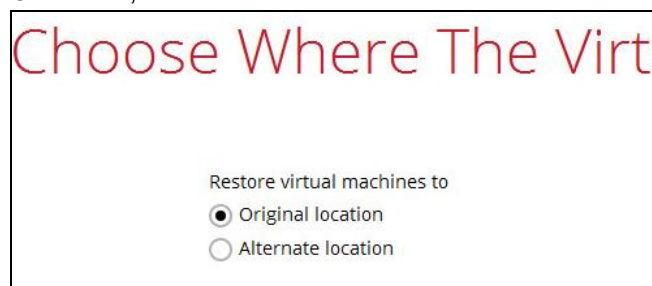
2.17.3 For Restore to the Original Hyper-V Host

- AhsayOBM UI must be running when a guest VM is started using Run Direct Restore or when migration process is running.
- For local, mapped drive, or removable drive storage destinations with Run Direct enabled, the compression type will always be set to No Compression and data encryption is disabled to ensure optimal backup and restore performance. The backup set compression type and data encryption settings will only be applied to CBS, SFTP/FTP, or Cloud storage destinations.
- Run Direct restore can only be performed on one guest VM at a time.
- Restored guest VMs using Run Direct containing a saved state will not automatically power on. The saved state must be manually deleted in Hyper-V Manager and the guest must be powered on manually.
- When a guest VM is started in a Run Direct instance is stopped any changes made within the guest environment will be lost, if the guest virtual is not migrated to the Hyper-V Server using the "Auto migrate after Run Direct is running" option.
- When a guest VM is started using Run Direct Restore, all backup jobs (manual and scheduled) for the related backup set will be skipped.

- When a guest VM is started using Run Direct Restore, the following features are not available for the backup set; Data Integrity Check, Space Freeing Up, and Delete Backup Data.

2.17.4 For Restore to a Different (Standby) Hyper-V Host

- AhsayOBM must be installed on the Hyper-V Host where you wish to restore the guest VM.
- The same AhsayOBM backup account must be used.
- For restore to an alternate Hyper-V Host with a different CPU architecture, the latest version of AhsayOBM client application must be installed.
- The correct encryption key is required if the backup set was created with the encryption key feature enabled.
- A guest VM backed up from a standalone Hyper-V host can only be restored to another standalone Hyper-V host. A guest VM backed up from a Hyper-V Cluster can only be restored to another Hyper-V Cluster.
- Guest VM backed up to local drive / mapped drive / removable drive on the original Hyper-V host can be restored to another Hyper-V host only if the new machine has access to the original drive(s).
- The network configuration and structure of the standby Hyper-V host must be same with the original Hyper-V host.
- For Hyper-V restore, it is highly recommended to increase the Java heap size setting to improve performance, especially on guest VM's with many incremental delta files. For further details, refer to [Ch. 2.7 Java Heap Size](#).
- For best restore performance, the temporary directory should be set to a local drive. Also, the temporary directory must have sufficient free disk space for the guest VM restore, for example, the restore of a 500GB guest VM with 30 incremental files of around 5GB each (500GB + 150GB (30 x 5GB)), the temporary directory will require at least 650GB of free space. For further details, refer to [Ch. 2.9 Temporary Directory](#).
- Restore guest VM to "Original Location" is possible only if the disk setup on the new Hyper-V host is the same as the original Hyper-V host, for example if the original guest VM was backed up on G: drive. Then restore to "Original location" can be selected if G: drive is setup on the new Hyper-V host. Otherwise, select "Alternate location".



- The Hyper-V management tools must be installed on the new Hyper-V host. For Hyper-V Cluster environments Hyper-V management tools must be installed on all Cluster nodes.

- The Hyper-V services must be started on the host. For Hyper-V Cluster environment, the Hyper-V services must be started on all Cluster nodes. For more details, refer to [Ch. 2.10 Hyper-V Services](#).
- **Microsoft Hyper-V VSS Writer** must be installed and running on the new Hyper-V host and the writer state must be Stable. This can be verified by running the vssadmin list writers command. For more details, refer to **number 3** of [Ch. 2.10 Hyper-V Services](#).

2.18 Granular Restore

2.18.1 Operating System

AhsayOBM must be installed on a 64-bit Windows machine as libraries for Granular only supports 64-bit Windows operating system. AhsayOBM must be installed on the following Windows Operating Systems:

Windows 2012	Windows 2012 R2	Windows 2016
Windows 8	Windows 8.1	Windows 10
Windows 2019		

Granular restore is supported on Hyper-V backup sets created and backed up using AhsayOBM installed on a Windows platform with the Granular Restore feature enabled on the backup set.

2.18.2 Available Spare Drive Letter

One spare drive letter must be available on the Windows machine for the granular restore process, as the VHD virtual disk is mounted on Windows as a logical drive. AhsayOBM will automatically take the next available drive letter in alphabetical order for the mounted virtual disk.

NOTE

1. The Windows drive letters A, B, and C are not used by granular restore.
2. The granular restore assigned drive letter(s) will be released once you exit from AhsayOBM UI.

2.18.3 Network Requirements

Recommended minimum network speed is **at least 100Mbps download speed**.

The network bandwidth requirements will increase in proportion to the size of the guest VM and or the incremental delta chain length to ensure optimal performance. Working with limited network bandwidth may severely affect the granular restore performance.

You can use an online network speed test website (e.g. www.speedtest.net) to get an idea of the actual bandwidth of the machine.

Recommendation

It is recommended that a local destination is added to the backup set for faster granular restore. Since granular restore of large guest VM from CBS server over the internet can be slow depending on network bandwidth and CBS server load.

2.18.4 Other Dependencies

The following dependencies are required for restore and therefore they are verified by AhsayOBM only when a granular restore is performed. Absence of these dependencies will not affect the backup job but would cause the granular restore to fail.

- Microsoft Visual C++ 2015 Redistributable (x86) / (x64)
<https://www.microsoft.com/en-us/download/details.aspx?id=48145>
- Update for Universal C Runtime in Windows
<https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows>

2.19 Best Practices and Recommendations

Please consider the following recommendations:

1. To ensure an optimal backup/restoration performance, it is highly recommended to set the temporary directory folder to a location with sufficient free disk space. It must be on another location other than Drive C: (e.g. Drive E:).
2. 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.

2.20 Limitations

1. Backup of VMs located on a SMB 3.0 shares is not supported.
2. Backup of guest VMs with pass-through disk (directly attached physical disk) is not supported. This is a Hyper-V limitation as the Microsoft Software Shadow Copy Provider cannot provide AhsayOBM with a VSS snapshot of pass-through disks which is required for a guest VM backup.

Although guest VM level backups are not possible, it is recommended to install AhsayOBM directly onto the guest VM to perform backups.

3. For backup of individual virtual disks, the restored VM does not support the reversion of previous snapshots, if the snapshot contains disks which are not previously backed up by AhsayOBM.
4. A guest VM can only be restored to the Hyper-V server with the same version, e.g. backup of a VM on Hyper-V 2012 R2 server cannot be restored to Hyper-V 2008 R2 Server or vice versa.
5. The VM will not start up if the virtual disk containing the guest operating system is not restored.
6. Restore of individual virtual disks is only supported using the **Restore raw file** option for a virtual disk with no snapshots.

NOTE

This will require modification of Hyper-V guest configuration files, and this only should be done if you have in-depth knowledge and understanding of Hyper-V, otherwise the guest VM may not startup properly.

7. Replication must be disabled for the VM selected for backup, otherwise there may be following error occurring during backup job:

Failed to backup virtual machine "guest_guid", Reason = "Failed to take VM snapshot. Error = [CreateVirtualSystemSnapshotV2] Error="The method call failed." (32775)".

Please refer to the following link for more details:

https://wiki.ahsay.com/doku.php?id=public:5349_failed_to_backup_hyperv_virtual_machine_with_replication_enabled

2.20.1 Run Direct Restore

- Run Direct Restore of VM containing .VHDS shared virtual disk(s) is not supported.

2.20.2 Granular Restore

- Granular restore does not support the mounting of virtual disks, if the disk itself is encrypted, for example using Windows Bitlocker or other third-party security features.
- If any folders or files on a virtual disk are encrypted these files/folder cannot be restored. For example, if the "Encrypt contents to secure data" is selected in Advanced attributes.
- The mounting of Linux/Unix file systems from virtual disk file is currently not available due to limitations of the file system drivers.
- Granular restore can only be performed on one guest VM at a time with no limitation on number of virtual disk than can be mounted on the guest VM. However, only files/folders from one virtual disk can be retrieved at a time.
- Windows User Account Control (UAC) must be disabled to apply granular restore.

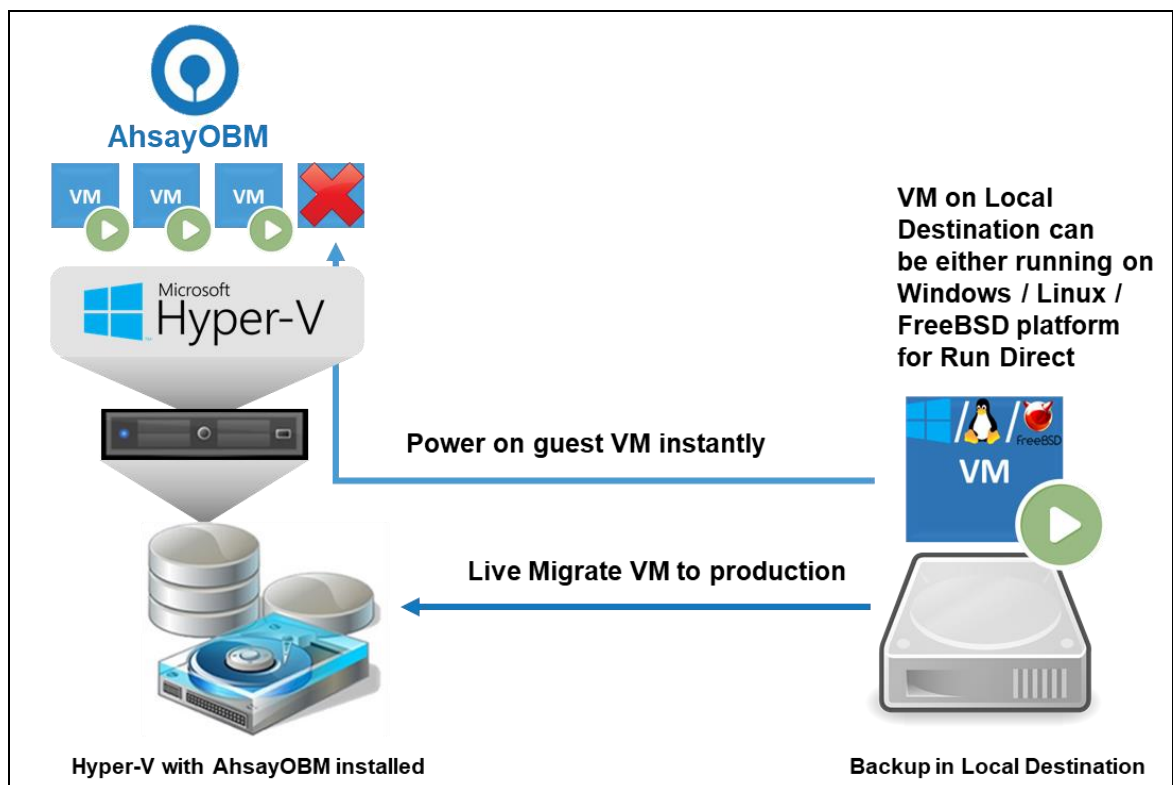
3 Run Direct

3.1 What is Run Direct?

Hyper-V Run Direct is a recovery feature helps to reduce disruption and downtime of your production guest VMs.

Unlike normal recovery procedures where the guest VMs are restored from the backup destination and copied to production storage which can take hours to complete, restore with Run Direct can instantly boot up a guest VM by running it directly from the backup file in the backup destination; this process can be completed in minutes.

3.2 How does Run Direct Restore work?



When a production guest VM suffers a fatal outage, the system administrator can log in to AhsayOBM on the Hyper-V server and initiate a Run Direct Restore request to start up the backup copy of the affected guest VM. The guest VM is instantly powered on from the backup in the Local Destination and can be put into production in minutes.

The guest VM on the Local Destination is then migrated to the designated permanent location on the Hyper-V server while it is running.

NOTE

Guest VMs that runs on Windows, Linux, or FreeBSD operating systems is supported for Run Direct Restore.

The following steps are taken when a Run Direct restore is initiated:

Delete Guest Virtual Machine

AhsayOBM will delete the existing guest VM on the original or alternate location (if applicable).

Create Virtual Hard Disk Image Files

Empty virtual hard disk image files are created on the Hyper-V server (either on the original location or alternate location).

Create VSS Snapshot

A VSS snapshot is created to make the backup data read only and track changes made within the guest VM environment.

Start Up Virtual Machine

The guest VM is started up. To finalize recovery of the guest VM, you will still need to migrate it from the backup destination to the designated permanent location on the Hyper-V server.

Copy Data

Copy the data from the backup files in the backup destination to empty hard disk images on the Hyper-V server.

Apply Changes

Apply any changes made within the guest VM environment to the hard disk image files on the Hyper-V server.

Delete VSS Snapshot

The VSS snapshot will be deleted after the Run Direct restoration is completed.

The restored VM, at this stage (e.g. before the restore is finalized) is in a read-only state to avoid unexpected changes. All changes made to the virtual disks (e.g. operation within the guest VM) are stored in a VSS snapshot created for the Run Direct restore. These changes are discarded when Run Direct is stopped, where the restored guest VM will be removed and all changes will be discarded, or the changes will be consolidated with the original VM data when the restore is finalized.

For more details on Run Direct restore options, refer to [Restore Options](#).

3.3 Benefits of using Run Direct Restore

With Run Direct Restore, you can start up the guest VM directly from the backup file in minutes, without restoring the guest VM to the Hyper-V server. The guest VM can then be put into production already immediately, while it has been restored (live migration) to the Hyper-V server.

4 Granular Restore Technology

4.1 What is Granular Restore Technology?

AhsayOBM granular restore technology enables the recovery of individual files from a guest VM without booting up or restoring the whole guest VM first.

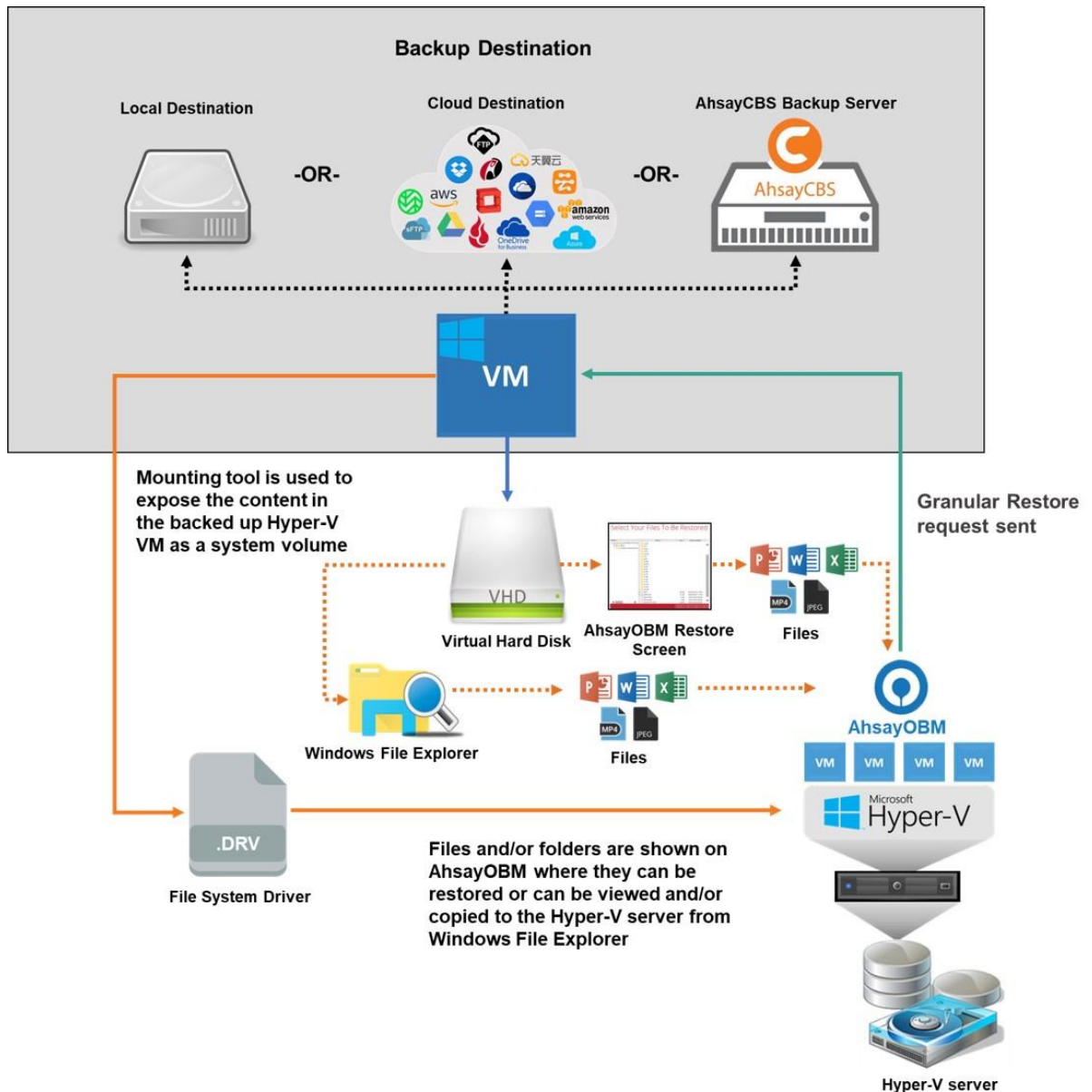
Granular restore is one of the available restore options for Hyper-V backup sets. AhsayOBM makes use of granular restore technology to enable a file level restore from a virtual disk file (VHD) of guest VM backup possible. It is particularly useful if you only need to restore individual file(s) from a guest VM which would normally take a long time to restore and then startup before you can gain access to the files on the virtual disks. Granular restore gives you a fast and convenient way to recover individual files from a guest VM.

During the granular restore process, the virtual disks of the guest VM can be mounted on the Windows machine as a local drive. This will allow the individual files on the virtual disks to be viewed via the file explorer within AhsayOBM or from the Windows File Explorer on the Windows machine you are performing the restore on, without having to restore the entire VM. Granular restore can only mount virtual disks if the guest VM is running on a Windows Platform and it is supported for all backup destinations, e.g. AhsayCBS, Cloud storage, or Local/Network drives. The mounting of Linux/Unix file systems from virtual disk file is currently not available due to limitations of the file system drivers.

IMPORTANT

Granular restore requires an additional OpenDirect / Granular restore add-on module license to work. Contact your backup service provider for further details.

4.2 How does Granular Restore work?



4.3 Benefits of using Granular Restore

Comparison between Granular Restore and Traditional Restore

Granular Restore
Introduction
Granular restore allows you to quickly mount virtual disk(s) directly from the backup file of a guest VM, so that individual files from virtual disk(s) can be exposed via the file explorer on AhsayOBM, or to be copied from the file explorer on to a 32 bit or 64 bit Windows machine you are performing the restore.
Pros

Restore of Entire Guest VM Not Required	Compared to a traditional restore where you have to restore the entire guest VM first, before you can access any individual files/folders, granular restore allows you to view and download individual files, without having to restore the entire guest VM first.
Ability to Restore Selected Files	In some cases, you may only need to restore a few individual file(s) from the guest VM, therefore, granular restore gives you a fast, convenient, and flexible tool to restore selected file(s) from a guest VM quickly.
Only One Backup Set Required	<p>With traditional restore methods, if you wish to restore individual file(s) from a guest VM, you will have to create two different backup sets; a Hyper-V guest VM backup set and a separate file backup set for the file(s) you wish to restore. You will require an additional AhsayOBM installation on the guest VM environment, with Granular Restore feature, only one backup set is required.</p> <ul style="list-style-type: none"> ➤ Fewer CAL (Client Access License) required - you will only need one AhsayOBM CAL to perform guest VM, Run Direct, and Granular restore. ➤ Less storage space required - as you only need to provision storage for one backup set. ➤ Less backup time required - As only one backup job needs to run. ➤ Less time spent on administration - As there are fewer backup sets to maintain.
Cons	
No Encryption and Compression	To ensure optimal restore performance, the backup of the guest VM will NOT be encrypted and compressed, therefore, you may have to take this factor in consideration when using this restore method.

Traditional Restore	
Introduction	
The traditional restore method for guest VMs, restores the entire backup files either to the original VM location or another standby location. The files or data on the guest VM can only be accessed once the guest VM has been fully recovered and booted up.	
Pros	
Backup with Compression and	Guest VM is encrypted and compressed, therefore is in a smaller file size, and encrypted before being uploaded to the backup destination.

Encryption	
Cons	
Slower Recovery	As the entire guest VM has to be restored before you can access any of its file(s) or data, the restore time could be long if the guest VM size is large.
Two Backup Sets and CALs Required	If you only wish to restore individual files from VM, two separate backup sets are required, one for the VM image and the other for the individual files, and therefore two CALs (client access licenses) are required.

5 Starting 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:

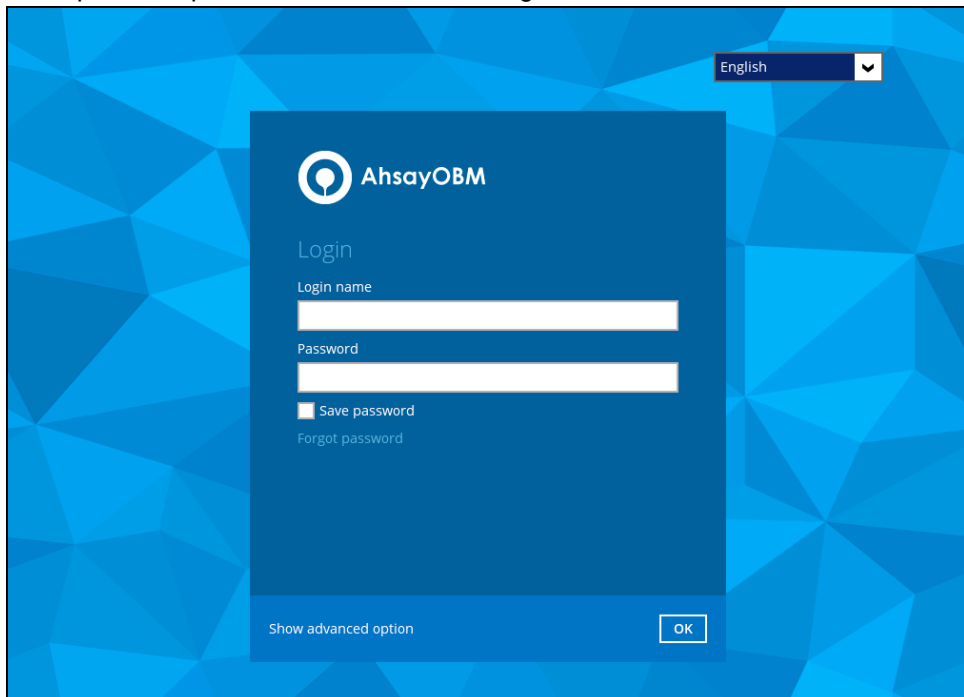
- [Login with no 2FA](#)
- [Login with 2FA using Twilio](#)
- [Login with 2FA using Mobile Authentication](#)

5.1 Login to AhsayOBM with no 2FA

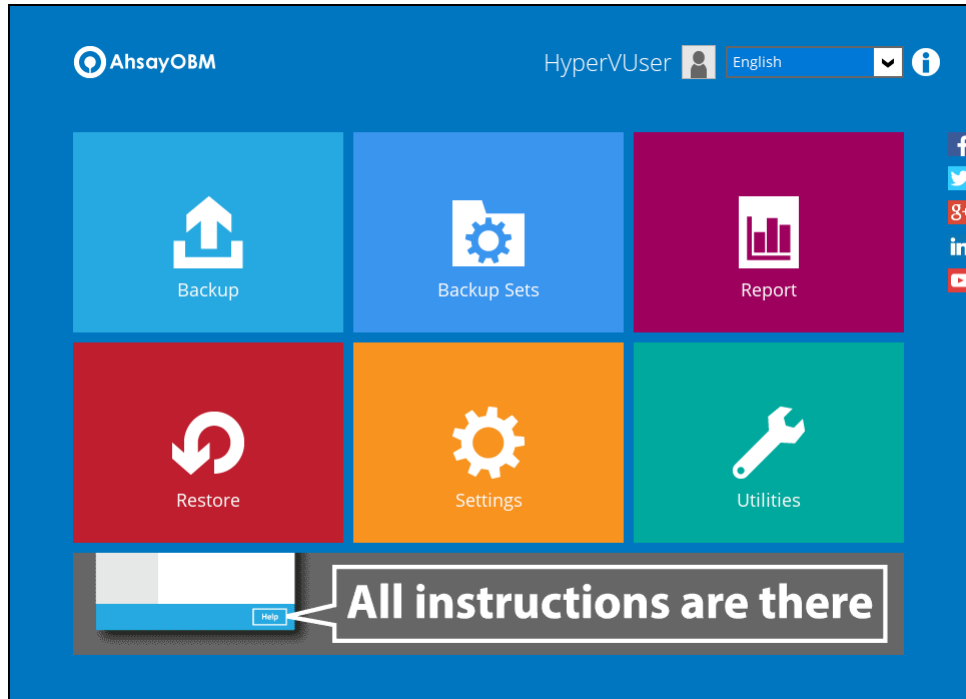
1. A shortcut icon of AhsayOBM should have been created on your Windows desktop after installation. Double click the icon to launch the application.



2. Enter the login name and password of your AhsayOBM account provided by your backup service provider, then click **OK** to login.



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



5.2 Login to AhsayOBM with 2FA using Twilio

1. A shortcut icon of AhsayOBM should have been created on your Windows desktop after installation. Double click the icon to launch the application.



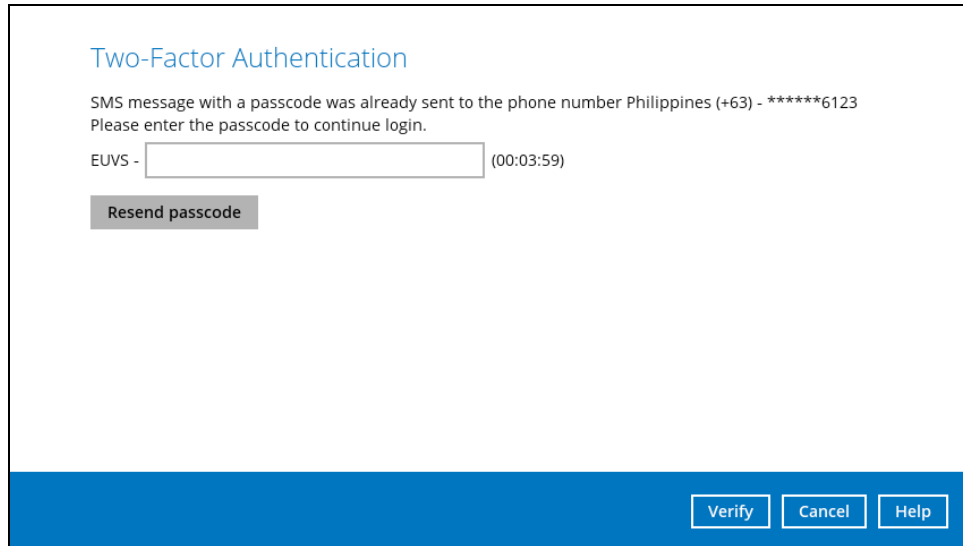
2. Enter the login name and password of your AhsayOBM account provided by your backup service provider, then click **OK** to login.

The AhsayOBM login screen. It has a blue background with a geometric pattern. In the center is a dark blue login box. The box contains the AhsayOBM logo and the word 'Login'. Below this are two input fields: 'Login name' and 'Password'. There is a checkbox for 'Save password' and a link for 'Forgot password'. At the bottom of the box are two buttons: 'Show advanced option' and 'OK'. In the top right corner of the screen, there is a language dropdown menu set to 'English'.

3. Select your phone number.

The Two-Factor Authentication screen. It has a white background. At the top, it says 'Two-Factor Authentication'. Below that, it says 'Please select phone number to receive passcode via SMS message to continue login.' There are three phone icons with corresponding numbers: 'Austria (+43) - *****6588', 'Philippines (+63) - *****6123', and 'Switzerland (+41) - *****4731'. At the bottom right, there are two buttons: 'Cancel' and 'Help'.

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



Two-Factor Authentication

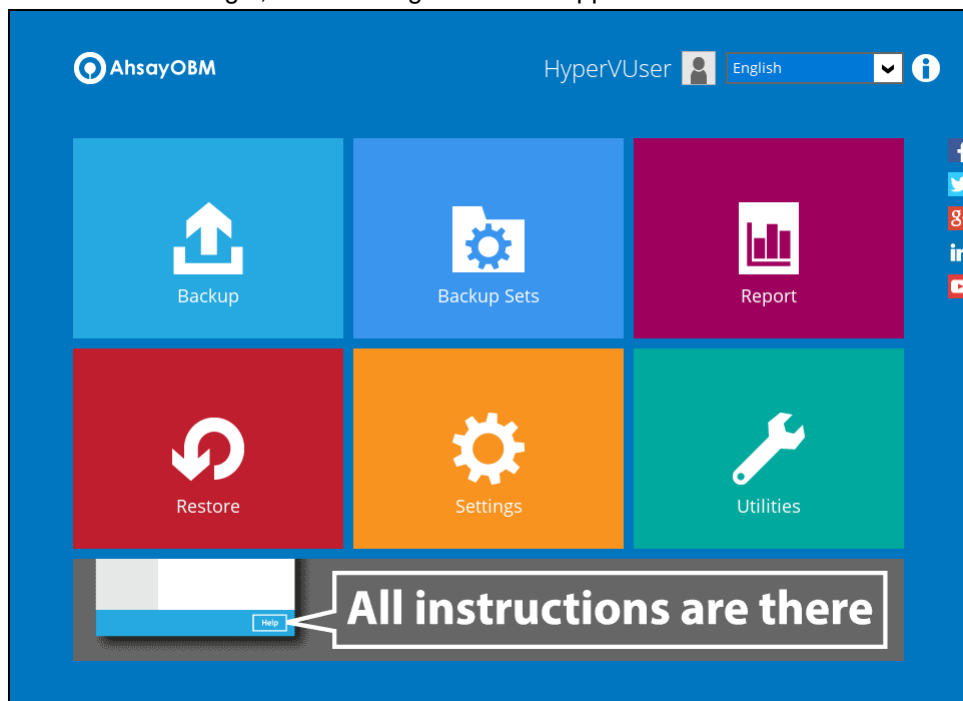
SMS message with a passcode was already sent to the phone number Philippines (+63) - *****6123
Please enter the passcode to continue login.

EUVS - (00:03:59)

[Resend passcode](#)

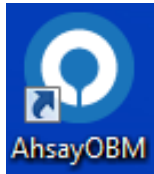
[Verify](#) [Cancel](#) [Help](#)

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

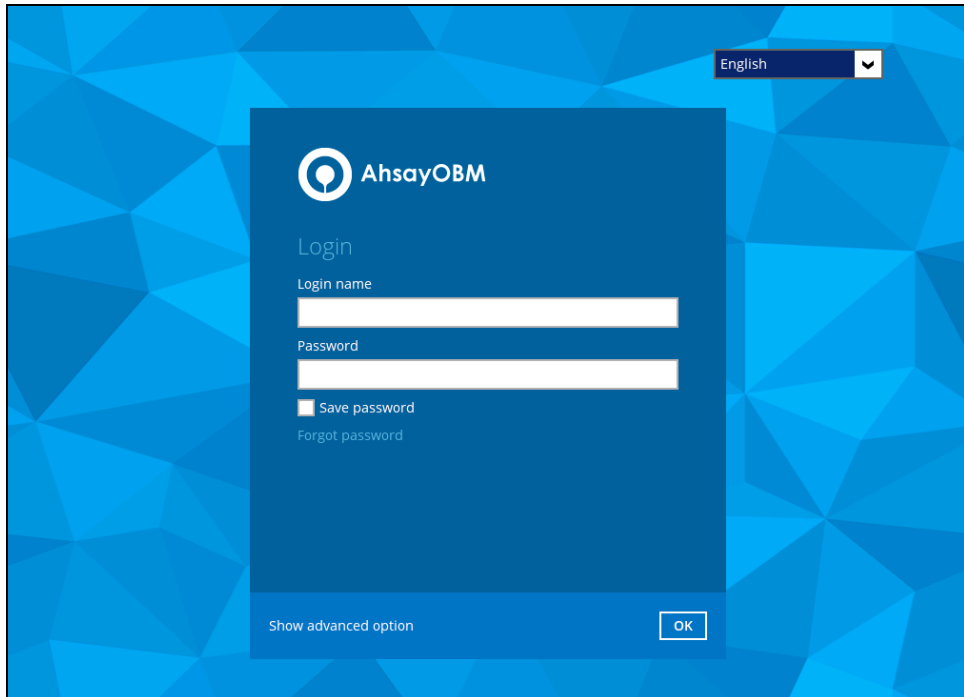


5.3 Login to AhsayOBM with 2FA using Mobile Authentication

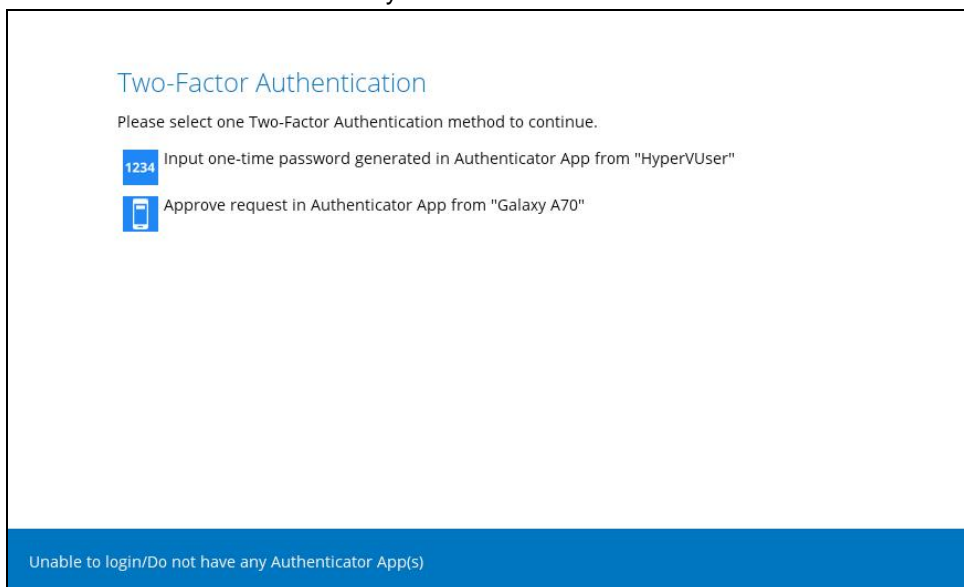
1. A shortcut icon of AhsayOBM should have been created on your Windows desktop after installation. Double click the icon to launch the application.



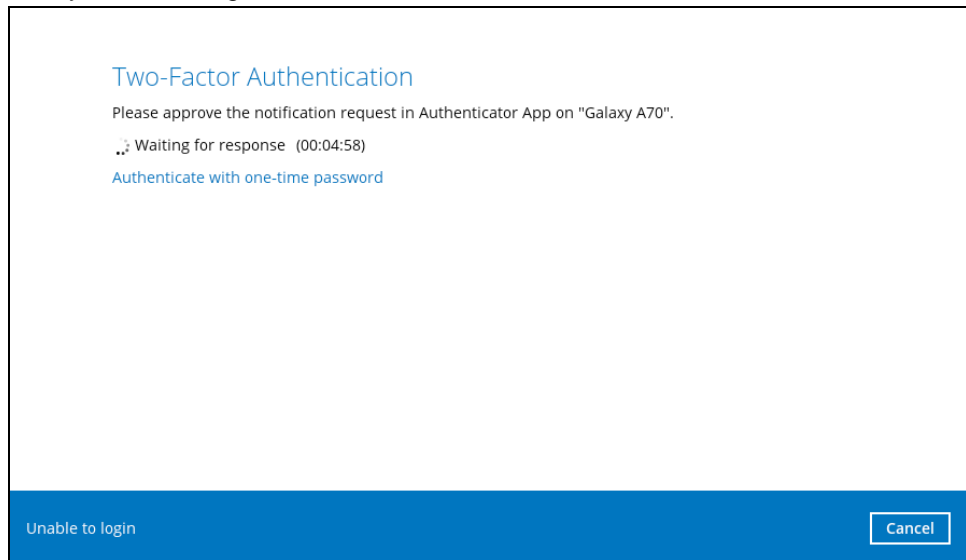
2. Enter the login name and password of your AhsayOBM account provided by your backup service provider, then click **OK** to login.



3. Click the authentication method you want to use.

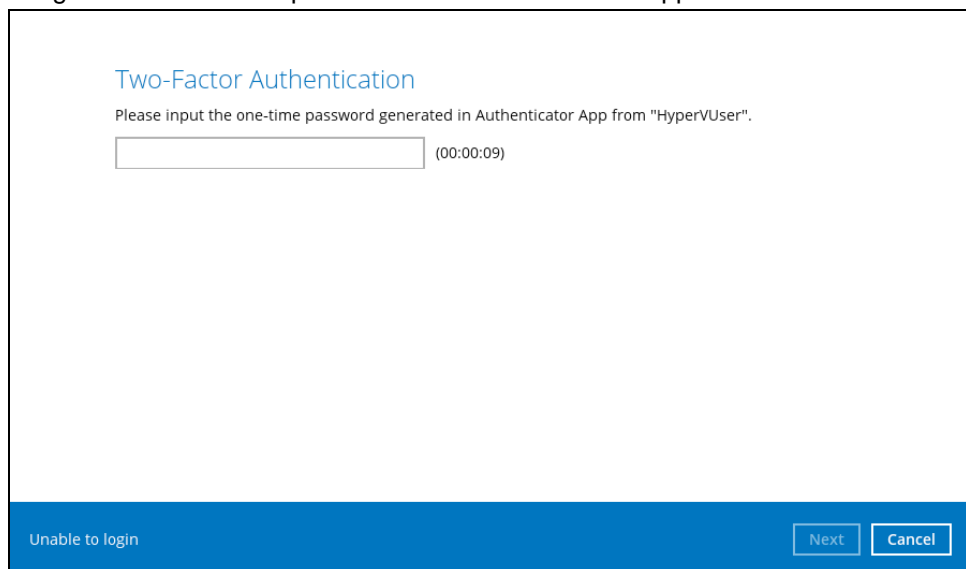


4. If **“Approve request in Authenticator App”** is selected, approve the request in Ahsay Mobile to login.



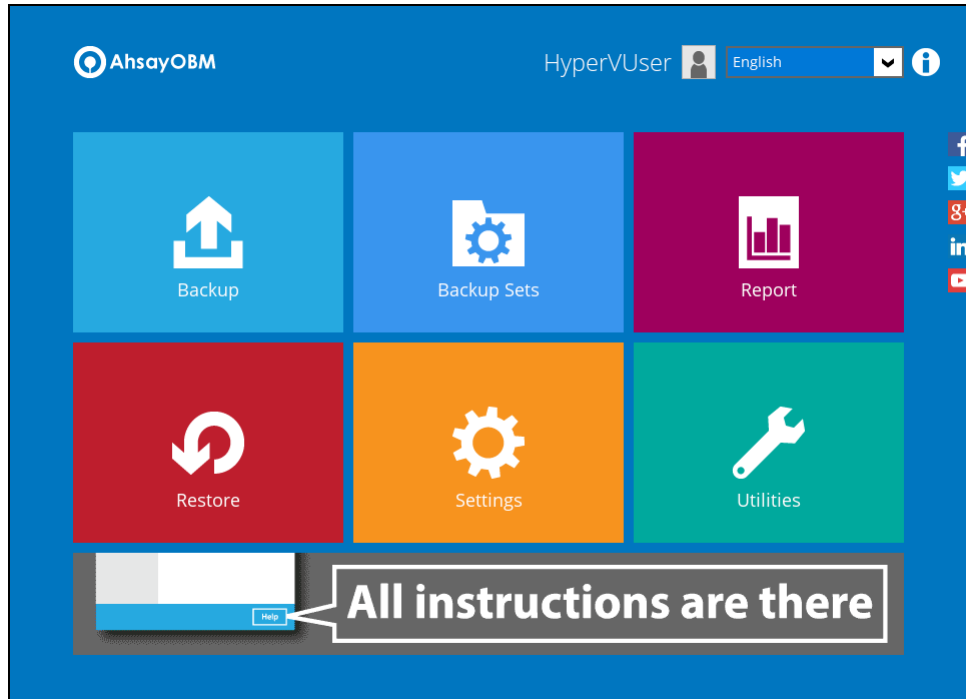
The screenshot shows a 'Two-Factor Authentication' dialog box. The title is 'Two-Factor Authentication' in blue. Below the title, it says 'Please approve the notification request in Authenticator App on "Galaxy A70".' There is a loading spinner icon followed by 'Waiting for response (00:04:58)'. A blue link 'Authenticate with one-time password' is present. At the bottom, there is a blue bar with the text 'Unable to login' on the left and a 'Cancel' button on the right.

- If **“Input one-time password generated in Authenticator App”** is selected, enter the generated one-time password in the authenticator app and click **Next**.



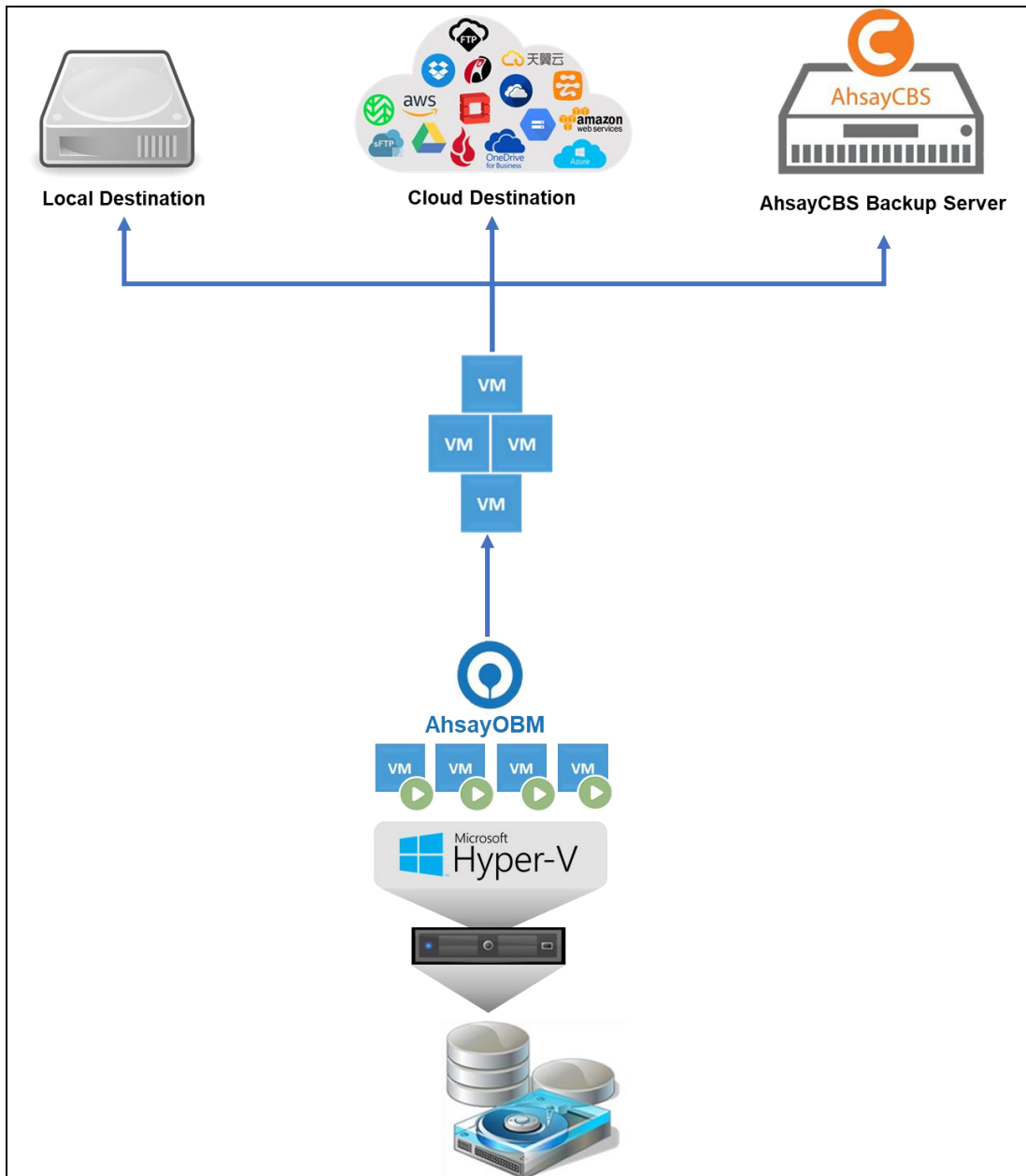
The screenshot shows a 'Two-Factor Authentication' dialog box. The title is 'Two-Factor Authentication' in blue. Below the title, it says 'Please input the one-time password generated in Authenticator App from "HyperVUser".' There is a text input field followed by a timer '(00:00:09)'. At the bottom, there is a blue bar with the text 'Unable to login' on the left and 'Next' and 'Cancel' buttons on the right.

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



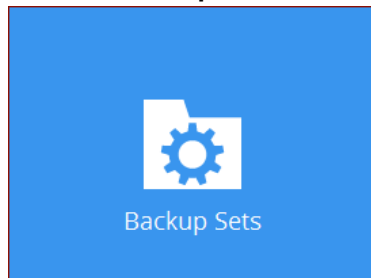
6 Creating a Hyper-V Backup Set

6.1 Non-Cluster Environment



6.1.1 Run Direct Backup Set

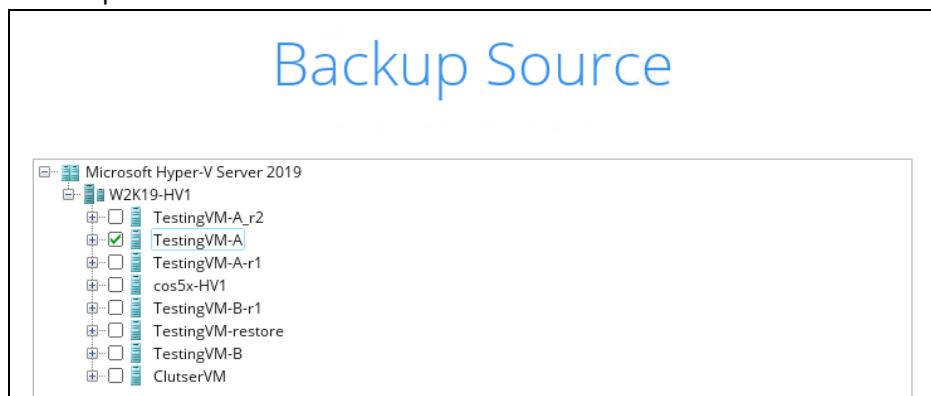
1. Click the **Backup Sets** icon on the main interface of AhsayOBM.



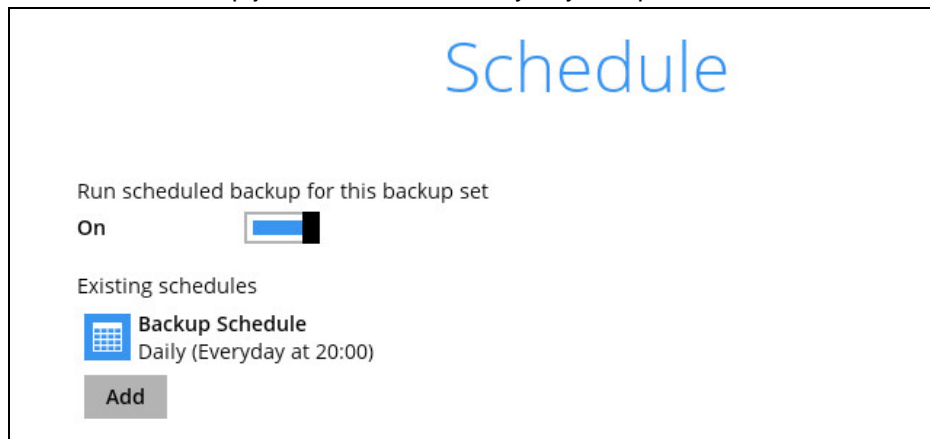
2. Create a new backup set by clicking the "+" icon or **Add** button to create new backup set.
3. Select the **Backup set type** and name your new backup set then click **Next** to proceed.

A screenshot of the "Create Backup Set" dialog box in AhsayOBM. The dialog has a title bar with "AhsayOBM" and standard window controls. The main area has the title "Create Backup Set" in blue. Below it are three input fields: "Name" with the text "MS Hyper-V 2019 Non Cluster", "Backup set type" with a dropdown menu showing "MS Hyper-V Backup", and "Version" with a dropdown menu showing "Microsoft Hyper-V Server 2019". At the bottom right are three buttons: "Next", "Cancel", and "Help".

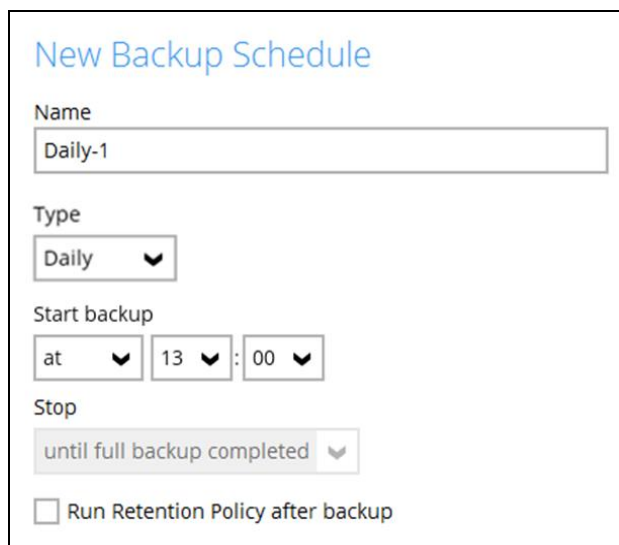
4. In the Backup Source menu, select the guest VM(s) you would like to backup. Click **Next** to proceed.



5. In the Schedule window, the **Run scheduled backup for this backup set** is turned on by default. You may edit the existing backup schedule, or you may create a new schedule for backup job to run automatically at your specified time interval.

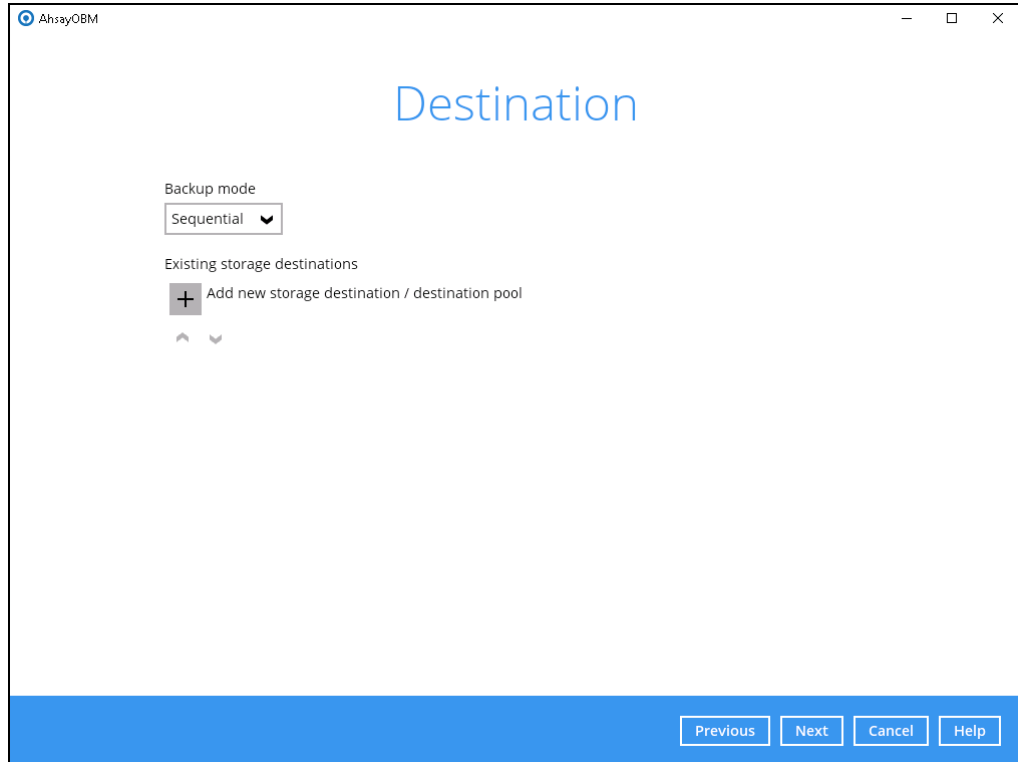



Click **Add** to add a new schedule.

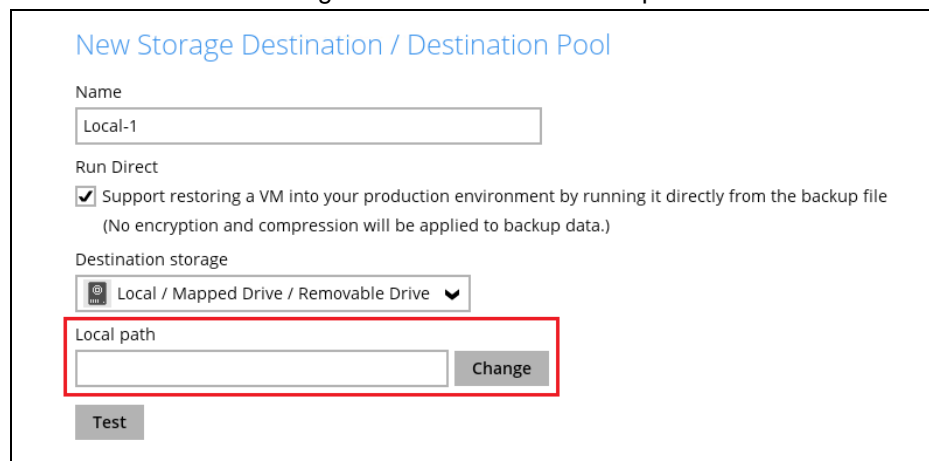


Click **OK** when you are done setting. Then click **Next** to proceed.

6. Select the backup storage destination.



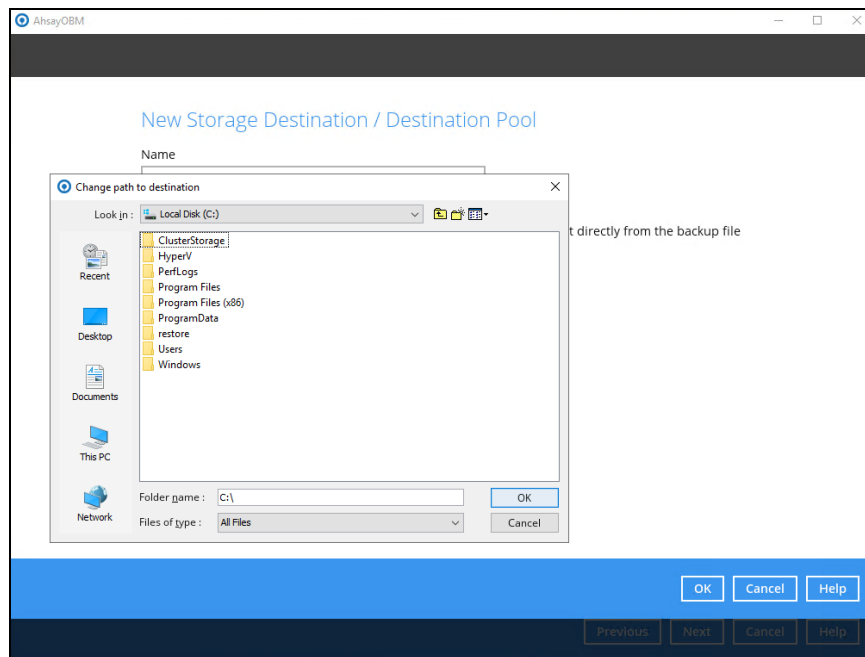
Click  to add new storage destination / destination pool.



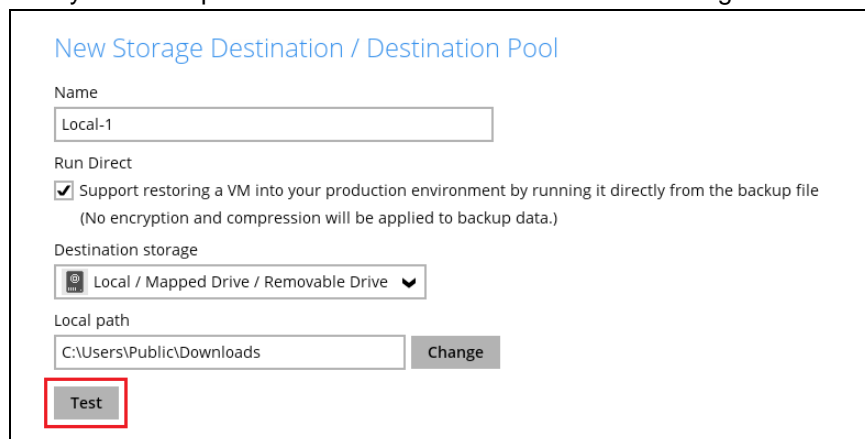
NOTE

1. For Hyper-V backup sets by default the **Run Direct** feature is enabled.
2. For Run Direct enabled backup sets, the storage destination is restricted to Local/ Mapped Drive/ Removable Drive.

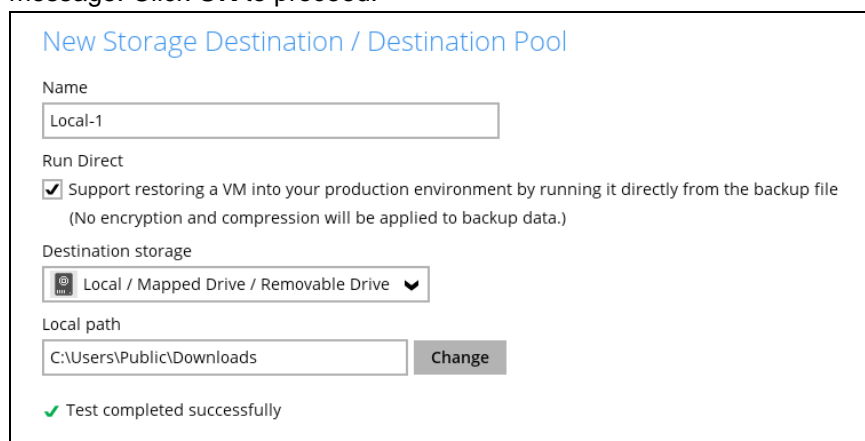
- i. Click on **Change** to select the storage destination a Local/ Mapped Drive/ Removable Drive.



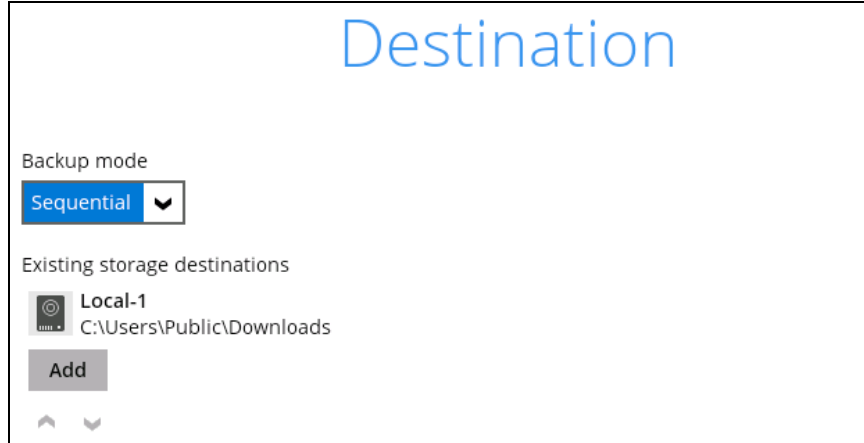
- ii. After selecting the storage destination click on the **Test** button to verify if AhsayOBM has permission to access the folder on the storage destination.



- iii. Once the test is finished AhsayOBM will display “**Test completed successfully**” message. Click **OK** to proceed.

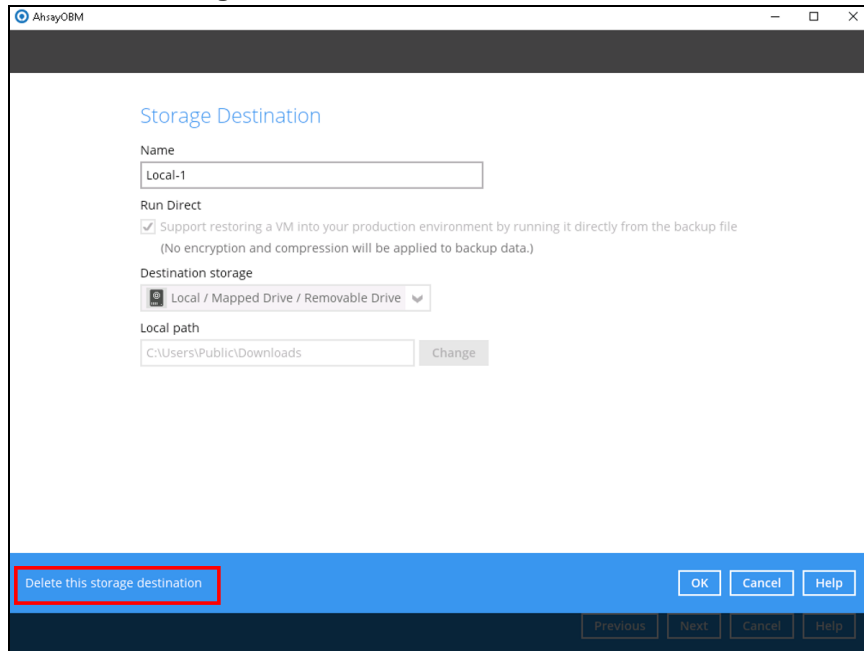


- iv. To add extra storage destination click **Add**, otherwise Click **Next** to proceed.



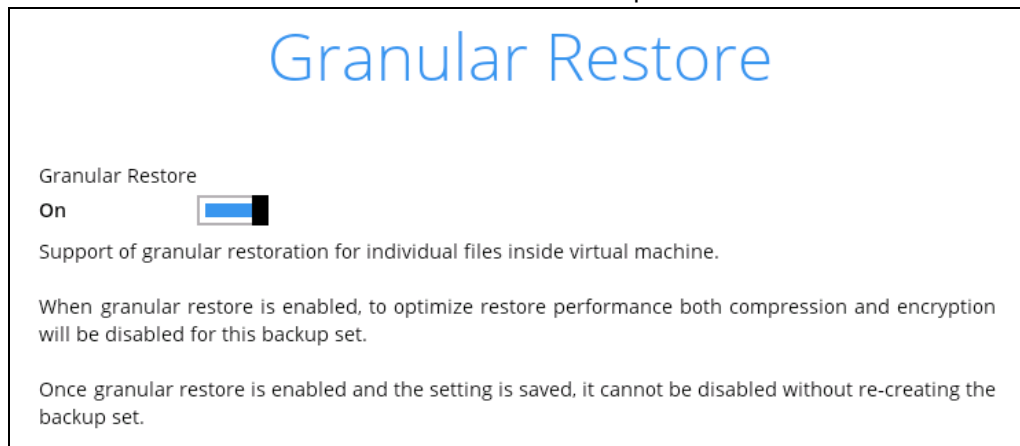
The 'Destination' screen displays the 'Backup mode' set to 'Sequential'. Under 'Existing storage destinations', there is one entry named 'Local-1' with the path 'C:\Users\Public\Downloads'. An 'Add' button is located below the list, and up/down arrows are at the bottom left.

If you want to delete the existing destination, double click the destination and click **Delete this storage destination** at the lower left corner.



The 'Storage Destination' configuration window shows the 'Name' as 'Local-1'. The 'Run Direct' checkbox is checked. The 'Destination storage' dropdown is set to 'Local / Mapped Drive / Removable Drive'. The 'Local path' is 'C:\Users\Public\Downloads'. At the bottom left, the 'Delete this storage destination' button is highlighted with a red box. At the bottom right, there are 'OK', 'Cancel', and 'Help' buttons.

7. If you wish to enable the granular restore feature, make sure you turn on the **Granular Restore** switch in this menu. Click **Next** to proceed.



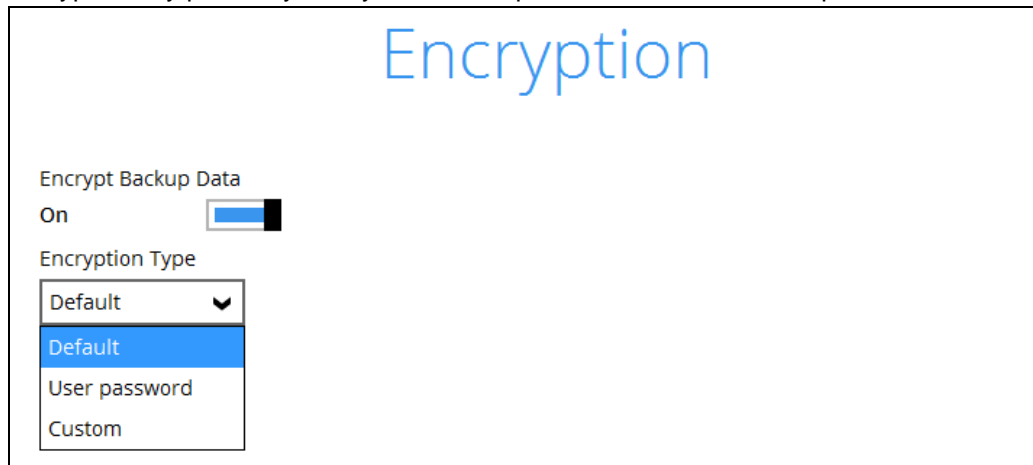
The 'Granular Restore' screen features a toggle switch for 'Granular Restore' which is currently turned 'On'. Below the switch, it states: 'Support of granular restoration for individual files inside virtual machine.' A note explains: 'When granular restore is enabled, to optimize restore performance both compression and encryption will be disabled for this backup set.' Another note states: 'Once granular restore is enabled and the setting is saved, it cannot be disabled without re-creating the backup set.'

NOTES

1. Once the Granular Restore feature is enabled and the backup set is saved, it is **NOT** possible to disable it afterwards, and vice versa. If you wish to change the Granular Restore settings, a new backup set will have to be created.
2. It is possible to enable both Granular Restore and Run Direct restore on the same backup set. However, AhsayOBM will only allow either Granular Restore or Run Direct restore to run, but not both to run concurrently.
3. Granular Restore requires an additional OpenDirect / Granular restore add-on module license to work. Contact your backup service provider for further details.
4. When Granular Restore is enabled, to optimize restore performance both compression and encryption will be disabled for this backup set.
5. Granular Restore might not be available, this depends on your backup service provider settings. Contact your backup service provider for more information.

8. **IMPORTANT:** If you have enabled the Granular restore or Run Direct restore feature, the backup data will not be compressed and encrypted to optimize the restore performance, therefore you can skip to step 10.

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



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

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

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

Encryption

Encrypt Backup Data
On ☒

Encryption Type
Custom ▼

Algorithm
AES ▼

Encryption key

Re-enter encryption key

Method
☐ ECB ☒ CBC

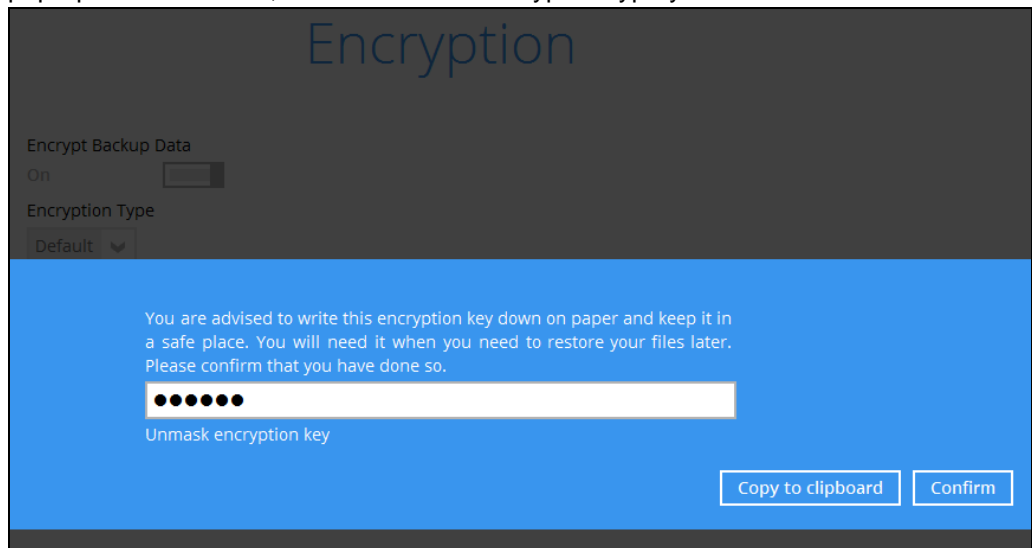
Key length
☐ 128-bit ☒ 256-bit

NOTE

- For best practice on managing your encryption key, refer to the following article.
https://wiki.ahsay.com/doku.php?id=public:8015_faq:best_practices_for_managing_encryption_key
- For local, mapped drive, or removable drive storage destinations with Run Direct enabled the compression type will be set **No Compression** and data encryption is **disabled** to ensure optimal backup and restore performance. The backup set compression type and data encryption settings will only be applied to CBS, SFTP/FTP, or Cloud storage destinations for the backup set.

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

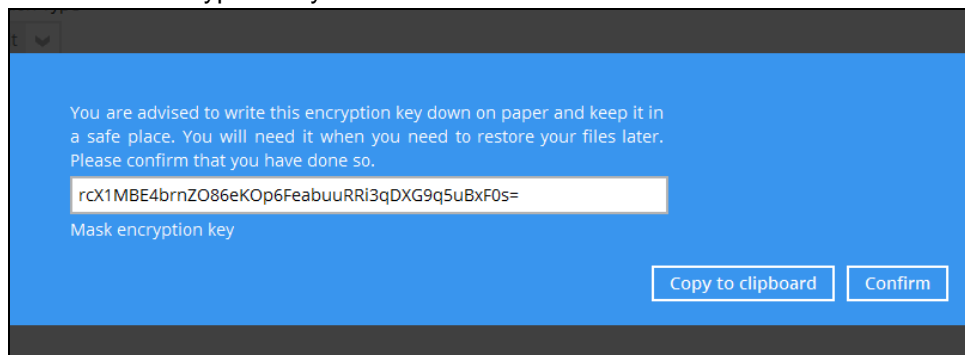
9. If you have enabled the Encryption Key feature in the previous step, the following pop-up window shows, no matter which encryption type you have selected.



The screenshot shows a pop-up window titled "Encryption". At the top, it says "Encrypt Backup Data" with a toggle switch set to "On". Below that, "Encryption Type" is set to "Default". The main body of the window is blue and contains the 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 this text is a text input field containing seven black dots, representing a masked encryption key. Below the input field is the label "Unmask encryption key". At the bottom right, there are two buttons: "Copy to clipboard" and "Confirm".

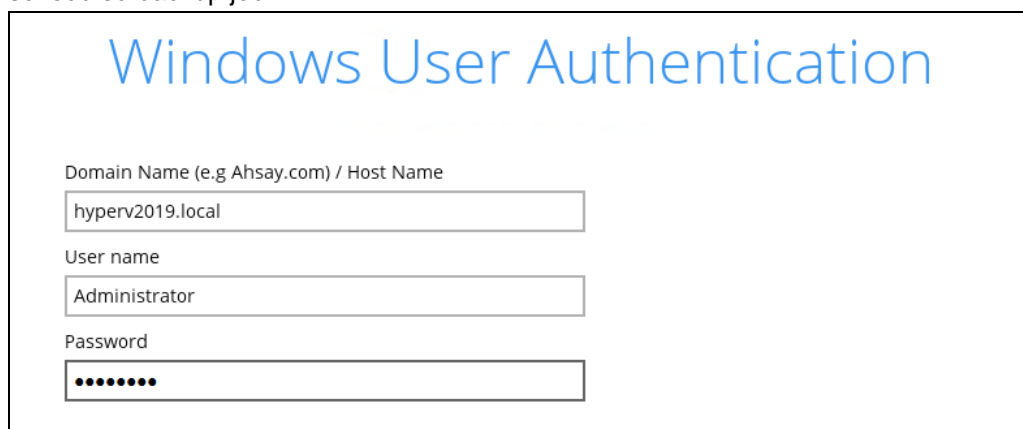
The pop-up window has the following three options to choose from:

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



This screenshot shows the same pop-up window as before, but the encryption key is now unmasked. The text input field contains the alphanumeric string "rcX1MBE4brnZO86eKOp6FeabuuRRI3qDXG9q5uBxF0s=". Below the input field is the label "Mask encryption key". The "Copy to clipboard" and "Confirm" buttons remain at the bottom right.

- **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 Windows login credentials used by AhsayOBM to authenticate the scheduled backup job.

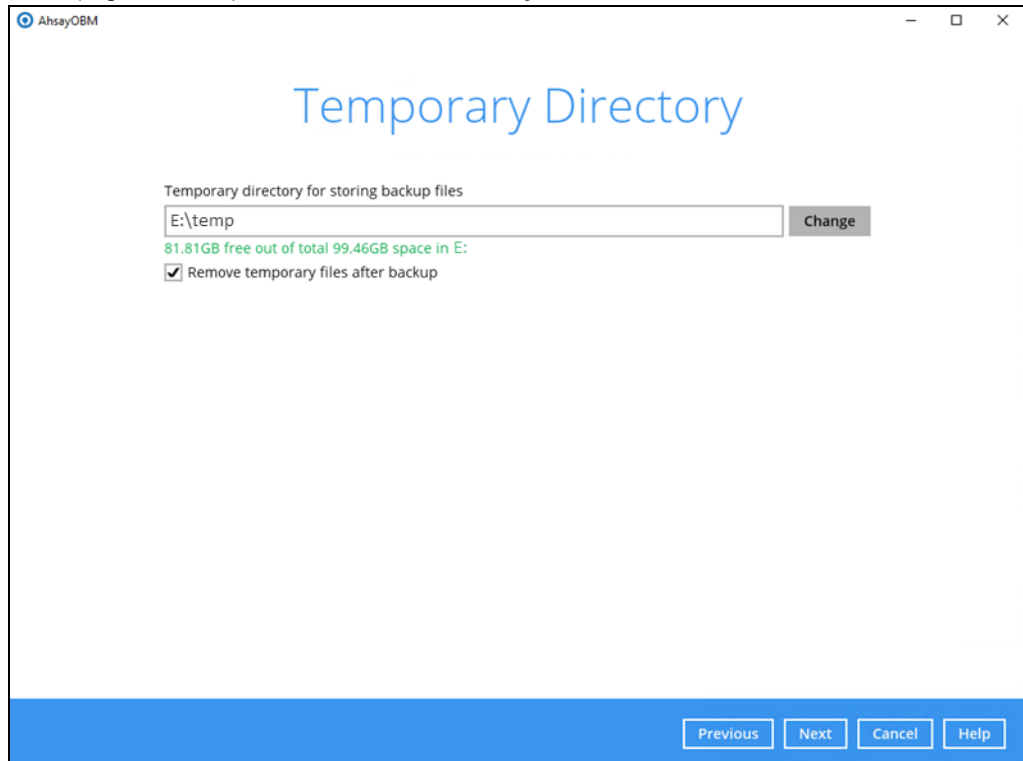


The screenshot shows a "Windows User Authentication" form. It has a title "Windows User Authentication" in blue. Below the title, there are three input fields: "Domain Name (e.g Ahsay.com) / Host Name" with the value "hyperv2019.local", "User name" with the value "Administrator", and "Password" with a masked password represented by seven black dots.

NOTE

If the backup schedule is turned off for the backup set the Windows User Authentication screen will be automatically skipped. The Windows User Authentication login credentials can be added or updated post backup set creation.

11. Select the temporary directory for storing temporary files, and then click **Next** to finish the setting. Upon creation of backup set, the temporary directory is set to `C:\Users\Administrator\obm\temp` by default. For optimal backup and/or restore performance, temporary directory location should be changed to other available drive (e.g. drive E:\) and not on **Windows System C:\ drive**.

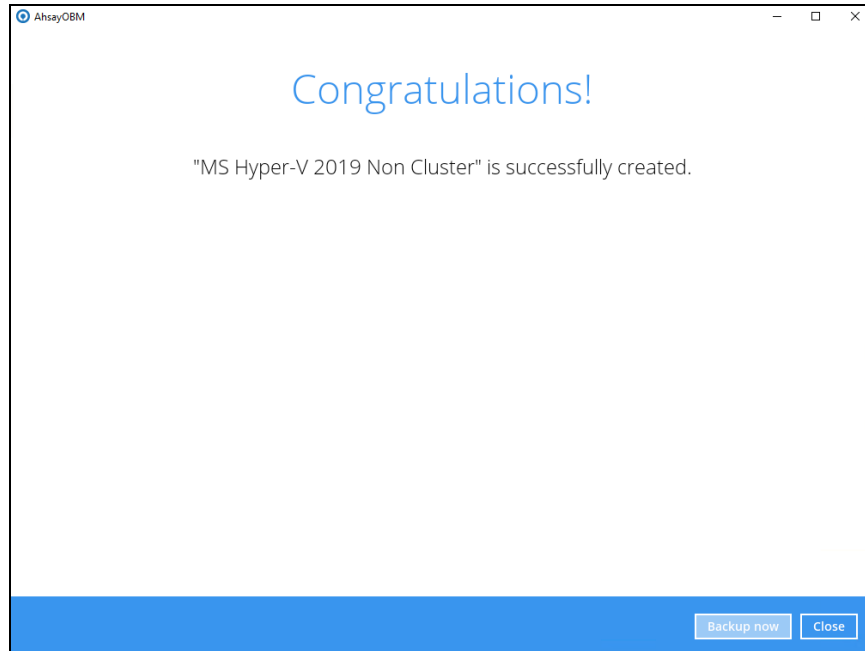


Refer to [Chapter 2.9](#) of this document for details on the temporary directory requirement. To know more about how to set up the temporary directory location, refer to the following KB article:

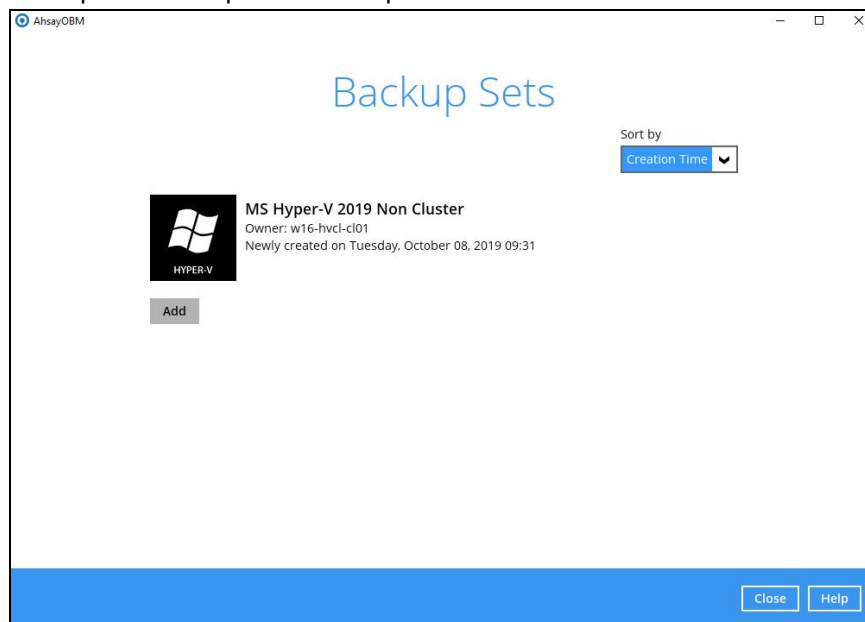
[FAQ: Tips on how to set up the temporary directory for your backup set](#)

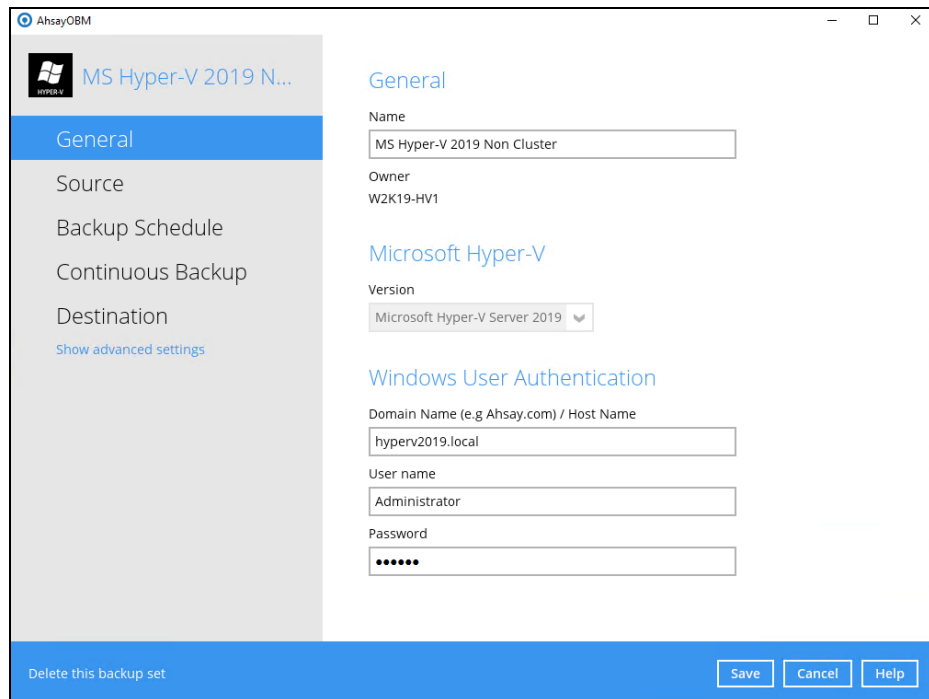
12. Backup set created.

- i. To start a manual backup job, click on **Backup now**.



- ii. To verify the backup set settings, click on **Close** and then click on the Hyper-V backup set to complete the setup.

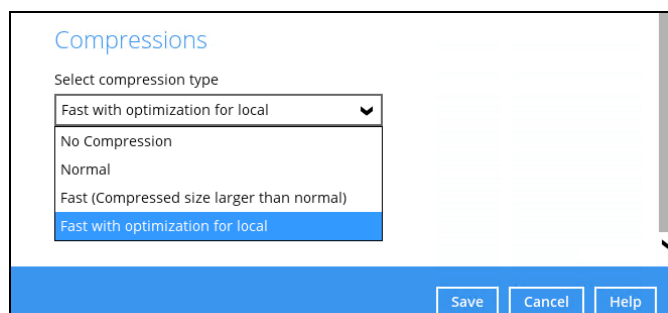




13. Optional: Select your preferred **Compression** type. By default, the compression type is Fast with optimization for local.

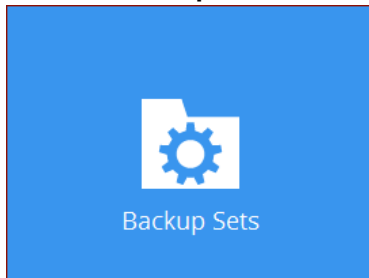
Go to **Others > Compressions**, then select from the following:

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

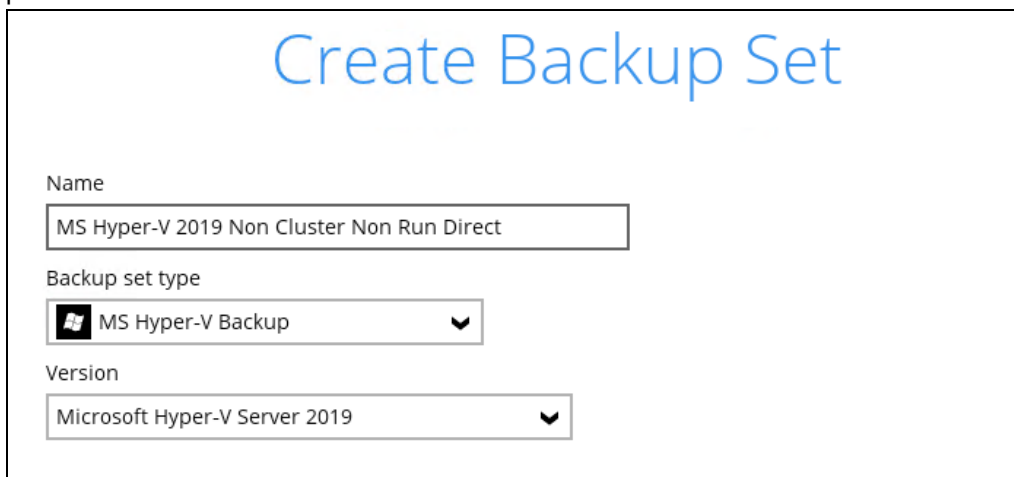


6.1.2 Non-Run Direct Backup Set

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

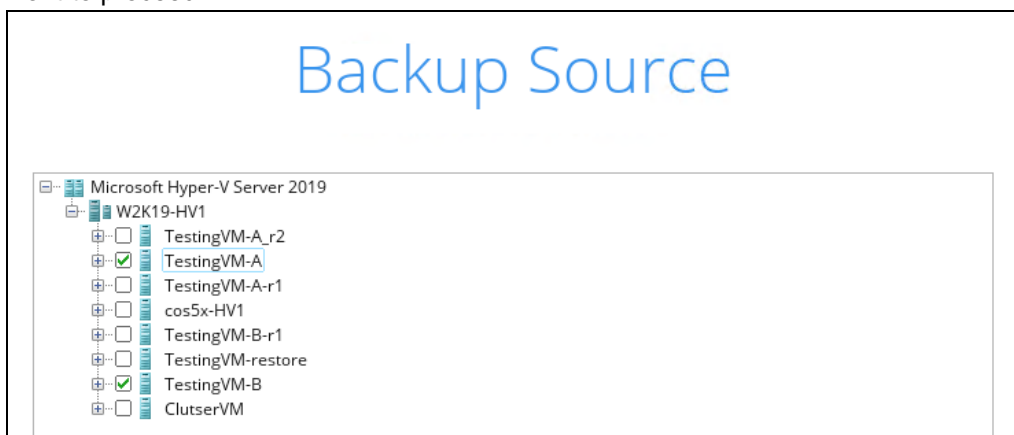


2. Create a new backup set by clicking the “+” icon next to **Add new backup set**.
3. Select the **Backup set type** and name your new backup set then click **Next** to proceed.



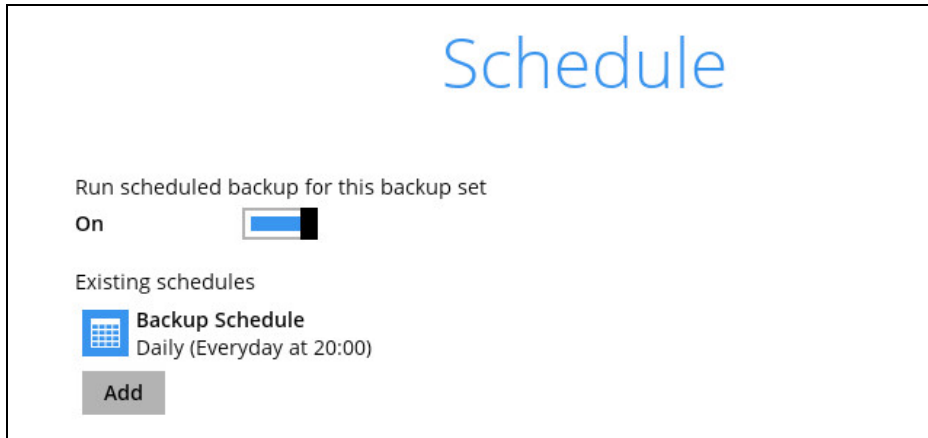
NOTE: AhsayOBM will automatically detect the Hyper-V version installed on the host.

4. In the Backup Source menu, select the guest VM(s) you would like to backup. Click **Next** to proceed.

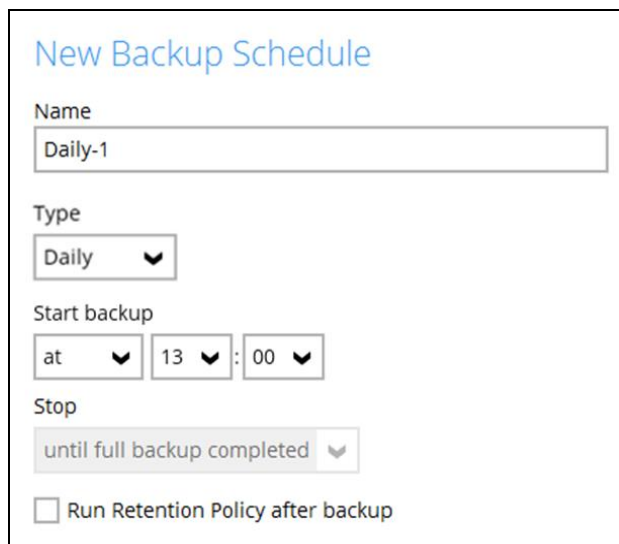


5. In the Schedule window, the **Run scheduled backup for this backup set** is turned on by default. You may edit the existing backup schedule, or you may create a new

schedule for backup job to run automatically at your specified time interval.

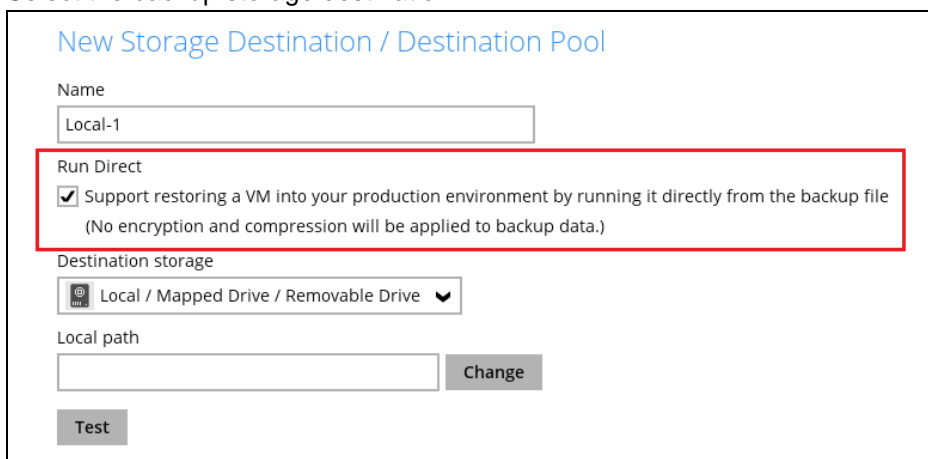


Click **Add** to add a new schedule.



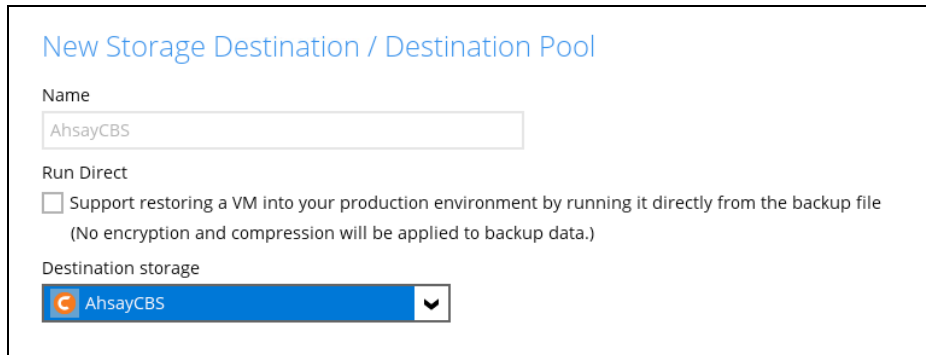
Click **OK** when you are done setting. Then click **Next** to proceed.

6. Select the backup storage destination.



NOTE: For Hyper-V backup sets, the default setting is for **Run Direct** to be enabled and the storage destination is either a **Local, Mapped Drive, or Removable Drive**.

To select a cloud, sftp/ftp, or CBS as a storage destination un-select **Run Direct** setting and select your desired cloud, sftp/ftp, or CBS as a storage destination. Click **OK** to proceed when you are done.



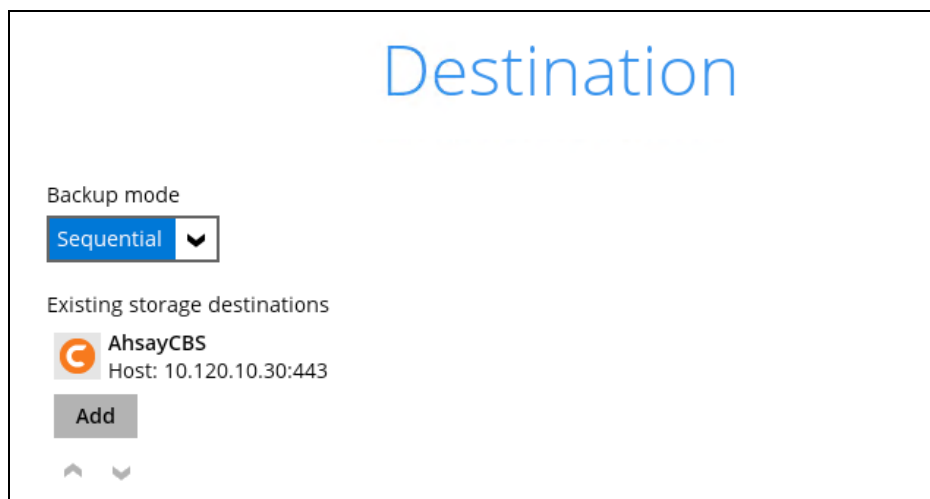
New Storage Destination / Destination Pool

Name
AhsayCBS

Run Direct
☐ Support restoring a VM into your production environment by running it directly from the backup file
(No encryption and compression will be applied to backup data.)

Destination storage
AhsayCBS

7. Click **Add** to add additional storage destination or click **Next** to proceed when you are done.



Destination

Backup mode
Sequential

Existing storage destinations

AhsayCBS
Host: 10.120.10.30:443

Add

8. If you wish to enable the Granular restore feature, make sure you turn on the **Granular Restore** switch in this menu. Click **Next** to proceed.



Granular Restore

Granular Restore
On

Support of granular restoration for individual files inside virtual machine.

When granular restore is enabled, to optimize restore performance both compression and encryption will be disabled for this backup set.

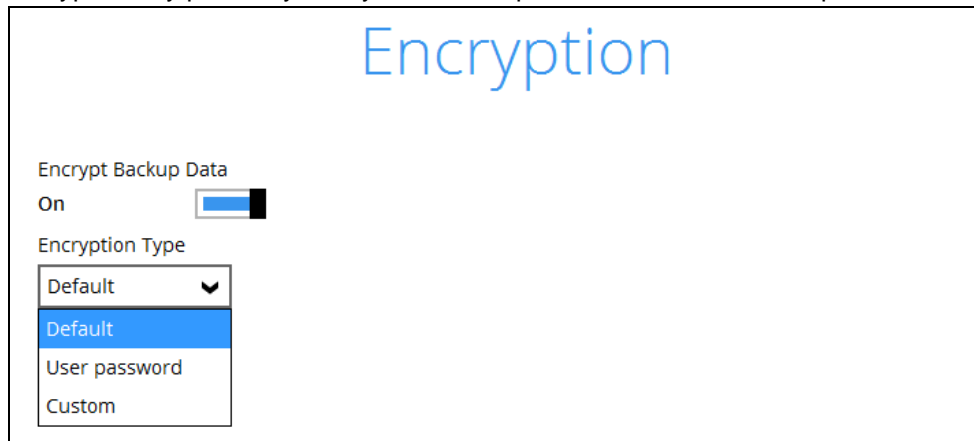
Once granular restore is enabled and the setting is saved, it cannot be disabled without re-creating the backup set.

NOTES

1. Once the Granular Restore feature is enabled and the backup set is saved, it is **NOT** possible to disable it afterwards, and vice versa. If you wish to change the Granular Restore settings, a new backup set will have to be created.
2. It is possible to enable both Granular Restore and Run Direct restore on the same backup set. However, AhsayOBM will only allow either Granular Restore or Run Direct restore to run, but not to run concurrently.
3. Granular Restore requires an additional OpenDirect / Granular Restore add-on module license to work. Contact your backup service provider for further details.
4. Granular Restore might not be available, this depends on your backup service provider settings. Contact your backup service provider for more information.

9. **IMPORTANT:** If you have enabled the Granular restore or Run Direct restore feature, backup data will not be compressed and encrypted to optimize the restore performance, therefore you can skip to step 11.

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.



Encryption

Encrypt Backup Data
On ☒

Encryption Type
Default ▼
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' settings window. At the top, the title 'Encryption' is displayed in blue. Below it, the 'Encrypt Backup Data' toggle is set to 'On'. The 'Encryption Type' dropdown is set to 'Custom'. The 'Algorithm' dropdown is set to 'AES'. The 'Encryption key' field contains seven asterisks. The 'Re-enter encryption key' field also contains seven asterisks. The 'Method' section has two radio buttons: 'ECB' (unselected) and 'CBC' (selected). The 'Key length' section has two radio buttons: '128-bit' (unselected) and '256-bit' (selected).

NOTE

- For best practice on managing your encryption key, refer to the following article.
https://wiki.ahsay.com/doku.php?id=public:8015_faq:best_practices_for_managing_encryption_key
- For local, mapped drive, or removable drive storage destinations with Run Direct enabled the compression type will be set **No Compression** and data encryption is **disabled** to ensure optimal backup and restore performance. The backup set compression type and data encryption settings will only be applied to CBS, SFTP/FTP, or Cloud storage destinations for the backup set.

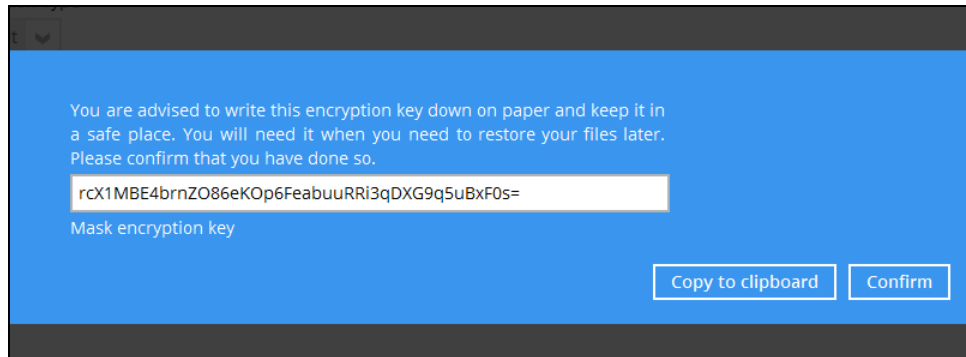
Click **Next** when you are done setting.

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

The screenshot shows a confirmation pop-up window titled 'Encryption'. It has a dark grey header with the title in blue. The body is light blue. It contains the 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 this text is a field with seven asterisks. At the bottom, there are two buttons: 'Copy to clipboard' and 'Confirm'.

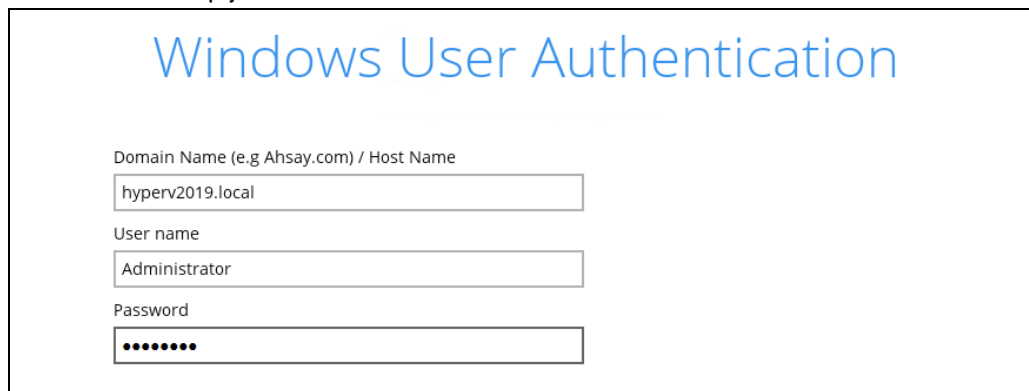
The pop-up window has the following three options to choose from:

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



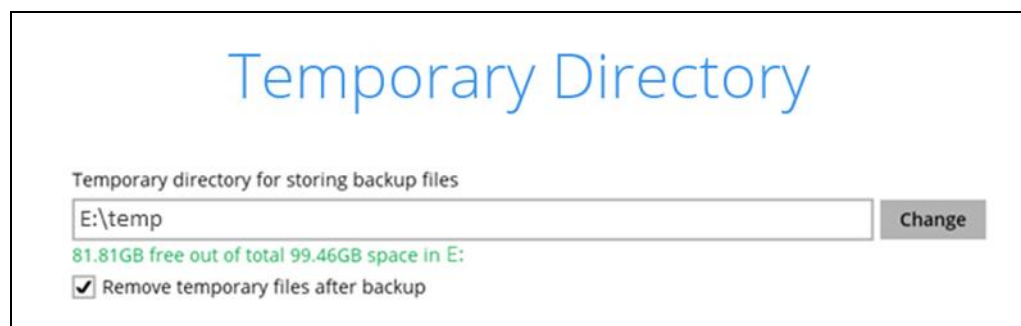
- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.
- **Confirm** – Click to exit this pop-up window and proceed to the next step.

11. Enter the Windows login credentials used by AhsayOBM to authenticate the scheduled backup job.



NOTE: If the backup schedule is turned off for the backup set the Windows User Authentication screen will be automatically skipped. The Windows User Authentication login credentials can be added or update post backup set creation.

12. Select the temporary directory for storing temporary files, and then click **Next** to finish the setting. Upon creation of backup set, the temporary directory is set to `C:\Users\Administrator\obm\temp` by default. For optimal backup and/or restore performance, temporary directory location should be changed to other available drive (e.g. drive E:\) and not on **Windows System C:\ drive**.

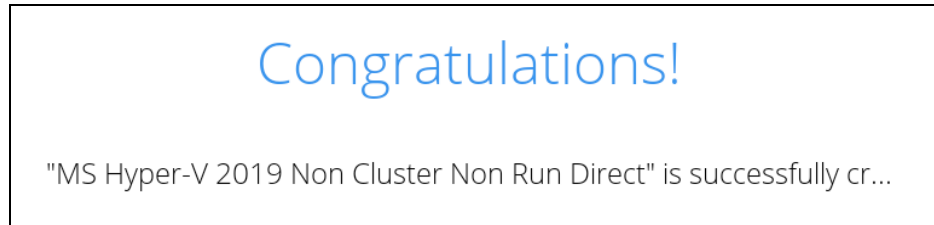


Refer to [Chapter 2.9](#) of this document for details on the temporary directory requirement. To know more about how to set up the temporary directory location, refer to the following KB article:

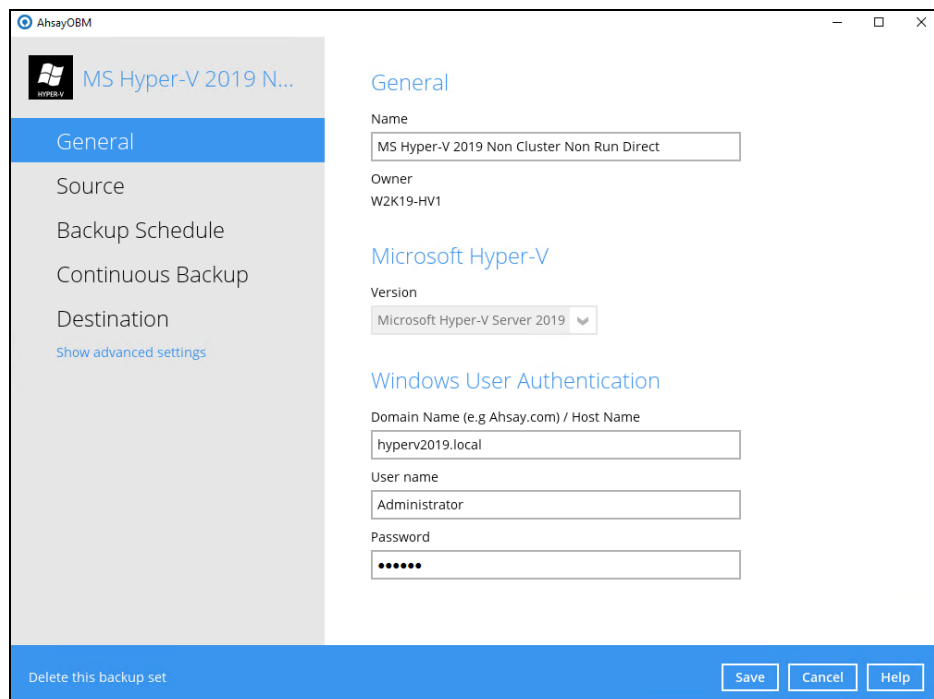
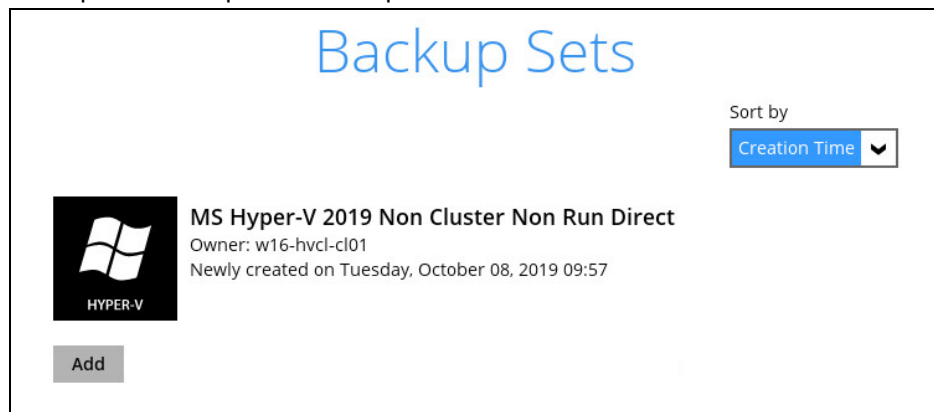
[FAQ: Tips on how to set up the temporary directory for your backup set](#)

13. Backup set created.

i. To start a manual backup job, click on **Backup now**.



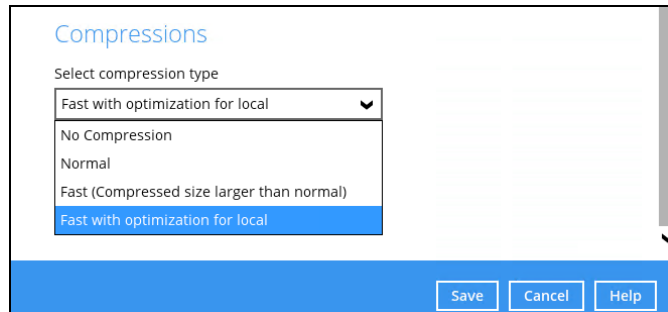
ii. To verify the backup set settings, click on Close and then click on the Hyper-V backup set to complete the setup.



14. 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



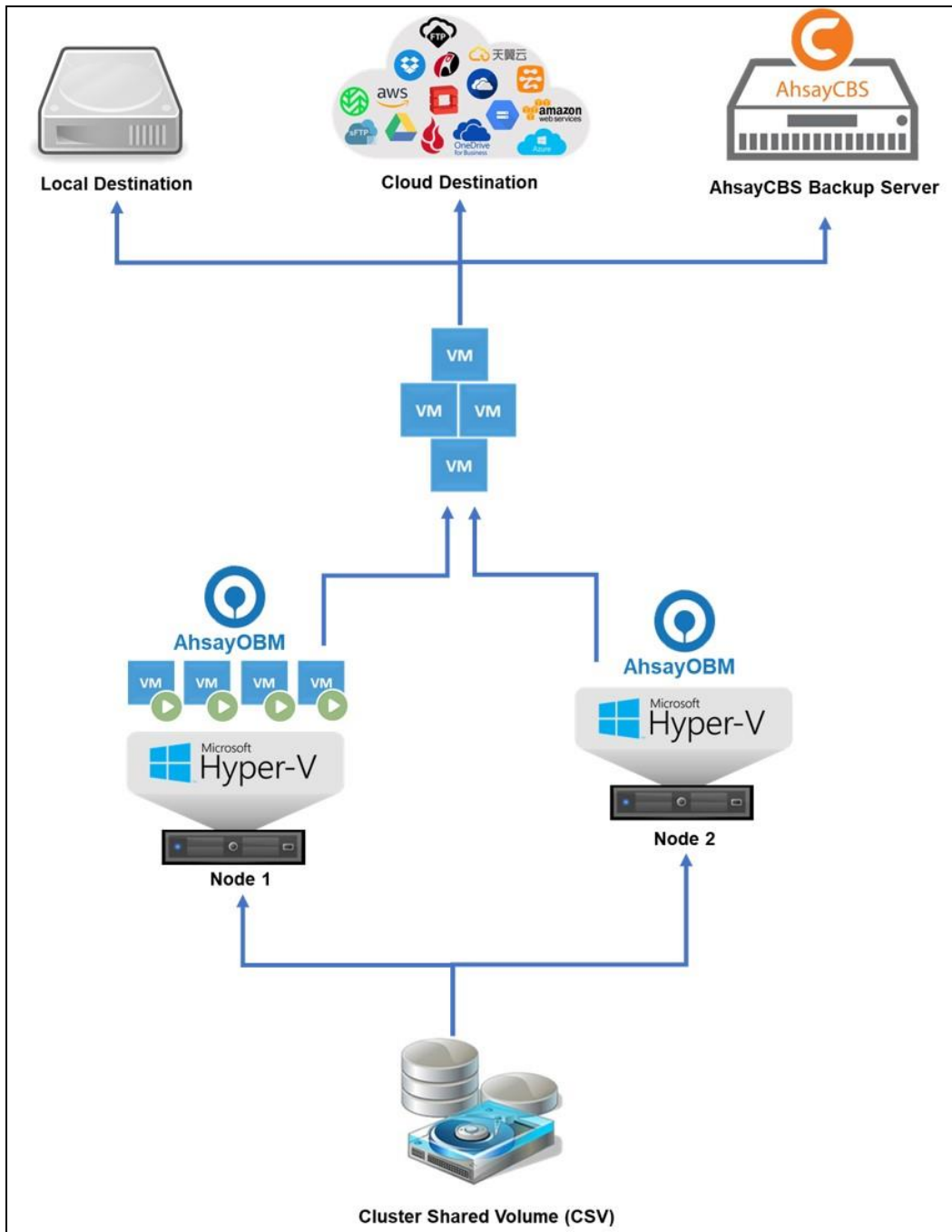
6.2 Cluster Environment

There are two (2) types of configuration in a Hyper-V Cluster Setup:

- **Active/Passive**
- **Active/Active**

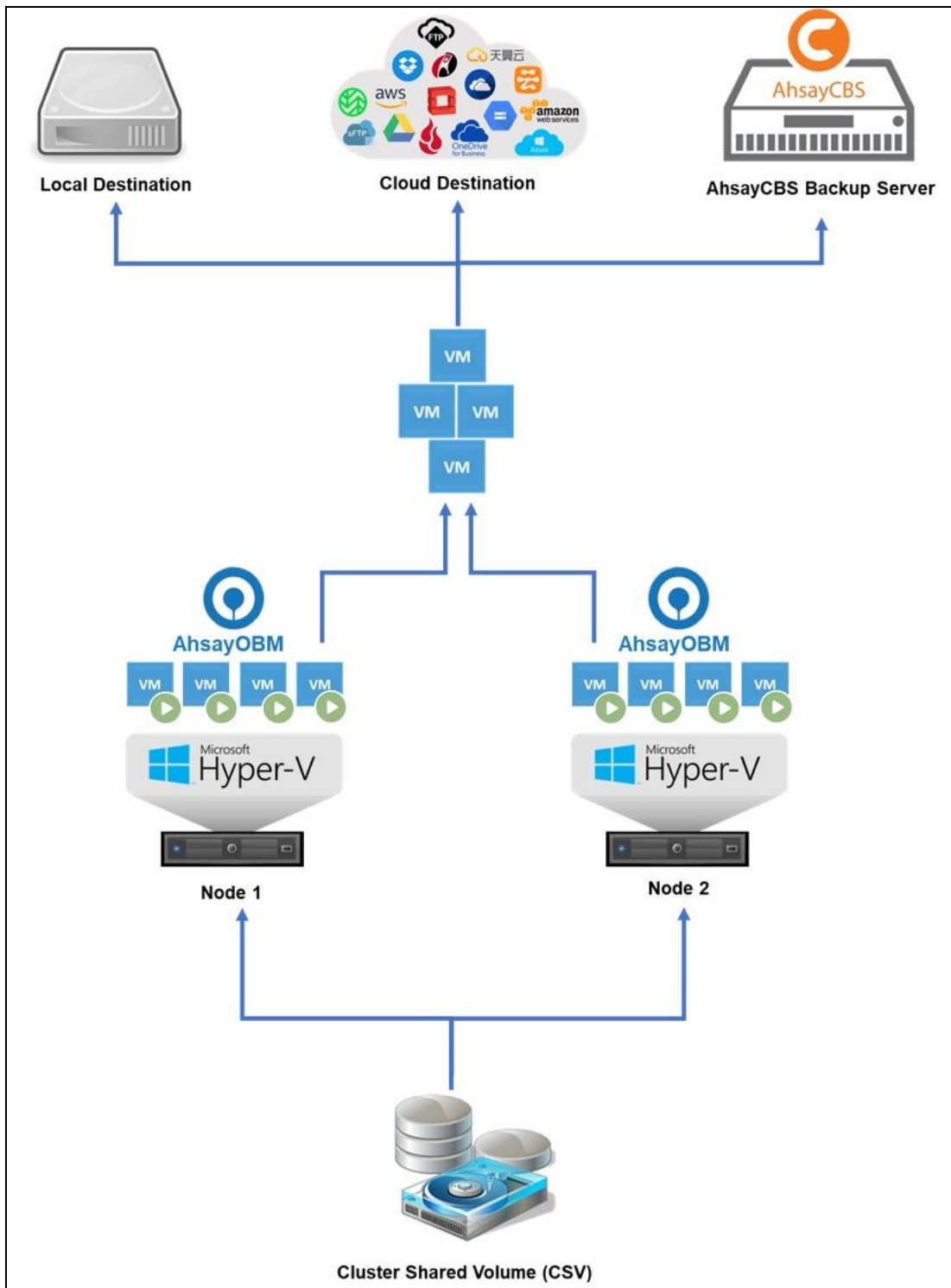
Active/Passive

In an Active/Passive configuration, there is at least one node in the cluster which is idle or not running any VM or resources.



Active/Active

In an Active/Active configuration, all VMs are running in all nodes.

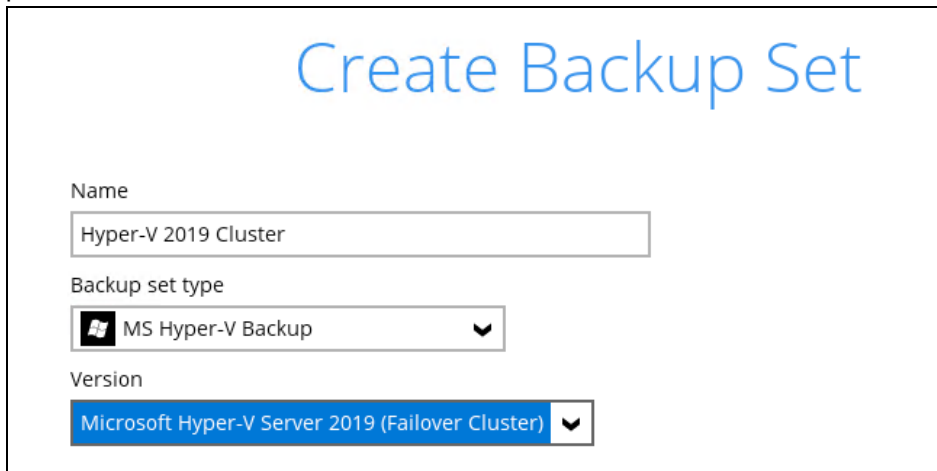


6.2.1 Run Direct Backup Set

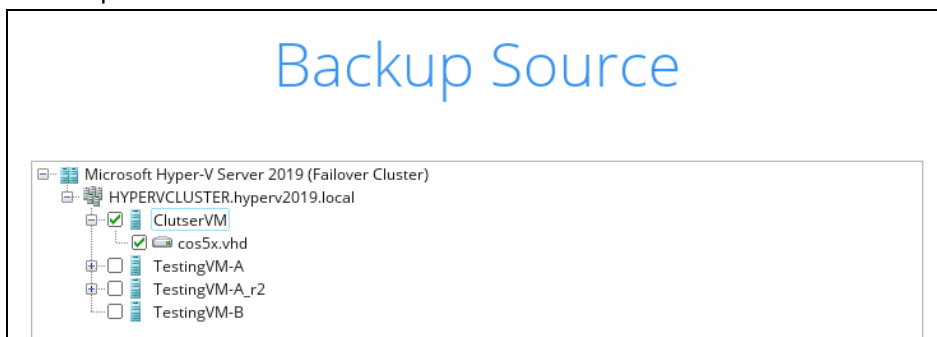
1. Click the Backup **Sets** icon on the main interface of AhsayOBM



2. Create a new backup set by clicking the “+” icon or **Add** button to created new backup set.
3. Select the **Backup set type** MS Hyper-V Backup, Version **Microsoft Hyper-V Server 2019 (Failover Cluster)**, and name your new backup set then click **Next** to proceed.



4. In the Backup Source menu, select the guest VM(s) you would like to backup. Click **Next** to proceed.




5. In the Schedule window, the **Run scheduled backup for this backup set** is turned on by default. You may edit the existing backup schedule, or you may create a new schedule for backup job to run automatically at your specified time interval.

Schedule

Run scheduled backup for this backup set

On 

Existing schedules

 **Backup Schedule**
Daily (Everyday at 20:00)

Add

Click on **Add** if you want to add a new schedule.

New Backup Schedule

Name

Daily-1

Type

Daily ▼

Start backup

at ▼ 13 ▼ : 00 ▼

Stop

until full backup completed ▼

☐ Run Retention Policy after backup

Click **OK** when you are done setting. Then click **Next** to proceed.

6. Click on **+** to add the destination.

Destination

Backup mode

Sequential ▼

Existing storage destinations

+ Add new storage destination / destination pool



7. Select the backup storage destination.

New Storage Destination / Destination Pool

Name
Local-1

Run Direct
☒ Support restoring a VM into your production environment by running it directly from the backup file
(No encryption and compression will be applied to backup data.)

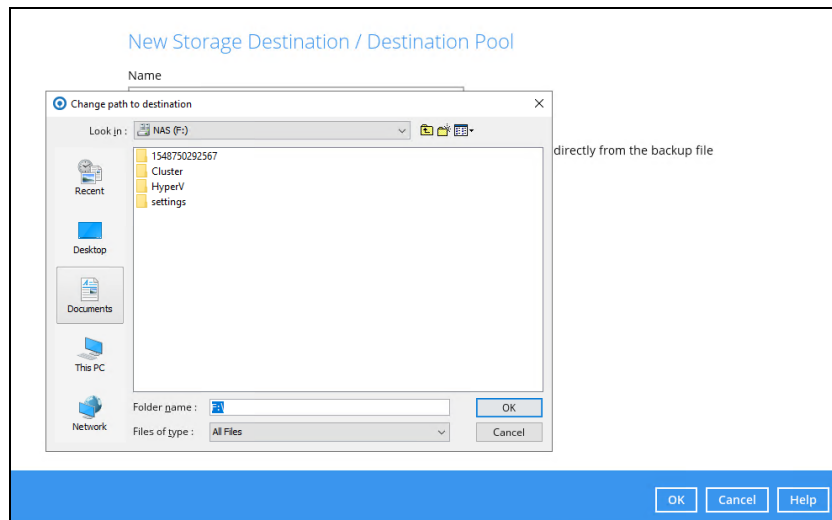
Destination storage
Local / Mapped Drive / Removable Drive

Local path
Change

Test

NOTE: For Hyper-V backup sets by the default the **Run Direct** feature is enabled.

- i. Click on Change to select the storage destination a Local, Mapped Drive, or Removable Drive.



- ii. After selecting the storage destination click on the Test button to verify if AhsayOBM has permission to access the folder on the storage destination.

New Storage Destination / Destination Pool

Name
Local-1

Run Direct
☒ Support restoring a VM into your production environment by running it directly from the backup file
(No encryption and compression will be applied to backup data.)

Destination storage
Local / Mapped Drive / Removable Drive ▼

Local path
F:\ Change

Test

- iii. Once the test is finished AhsayOBM will display “Test completed successfully” message. Click **OK** to proceed.

New Storage Destination / Destination Pool

Name
Local-1

Run Direct
☒ Support restoring a VM into your production environment by running it directly from the backup file
(No encryption and compression will be applied to backup data.)

Destination storage
Local / Mapped Drive / Removable Drive ▼

Local path
F:\ Change

✓ Test completed successfully

NOTE: For Hyper-V Cluster backup set with Run Direct enabled please ensure all nodes have access to the **Local, Mapped Drive, or Removable Drive** destination storage.

- iv. To add extra storage destinations click **Add**, otherwise Click **Next** to proceed.

Destination

Backup mode
Sequential ▼

Existing storage destinations

Local-1
F:\

Add

⌵ ⌶

8. If you wish to enable the Granular Restore feature, make sure you turn on the **Granular Restore** switch in this menu. Click **Next** to proceed.

Granular Restore

Granular Restore
On ☒

Support of granular restoration for individual files inside virtual machine.

When granular restore is enabled, to optimize restore performance both compression and encryption will be disabled for this backup set.

Once granular restore is enabled and the setting is saved, it cannot be disabled without re-creating the backup set.

NOTES

1. Once the Granular Restore feature is enabled and the backup set is saved, it is **NOT** possible to disable it afterwards, and vice versa. If you wish to change the Granular Restore settings, a new backup set will have to be created.
2. It is possible to enable both Granular Restore and Run Direct restore on the same backup set. However, AhsayOBM will only allow either Granular Restore or Run Direct restore to run, but not to run concurrently.
3. Granular Restore requires an additional OpenDirect / Granular restore add-on module license to work. Contact your backup service provider for further details.
4. Granular Restore might not be available, this depends on your backup service provider settings. Contact your backup service provider for more information.

9. **IMPORTANT:** If you have enabled the Granular restore or Run Direct restore feature, backup data will not be compressed and encrypted to optimize restore performance, therefore you can skip to step 10.

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

Encryption

Encrypt Backup Data
On ☒

Encryption Type

Default

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.

Encryption

Encrypt Backup Data
On ☒

Encryption Type
Custom ▼

Algorithm
AES ▼

Encryption key

Re-enter encryption key

Method
☐ ECB ☒ CBC

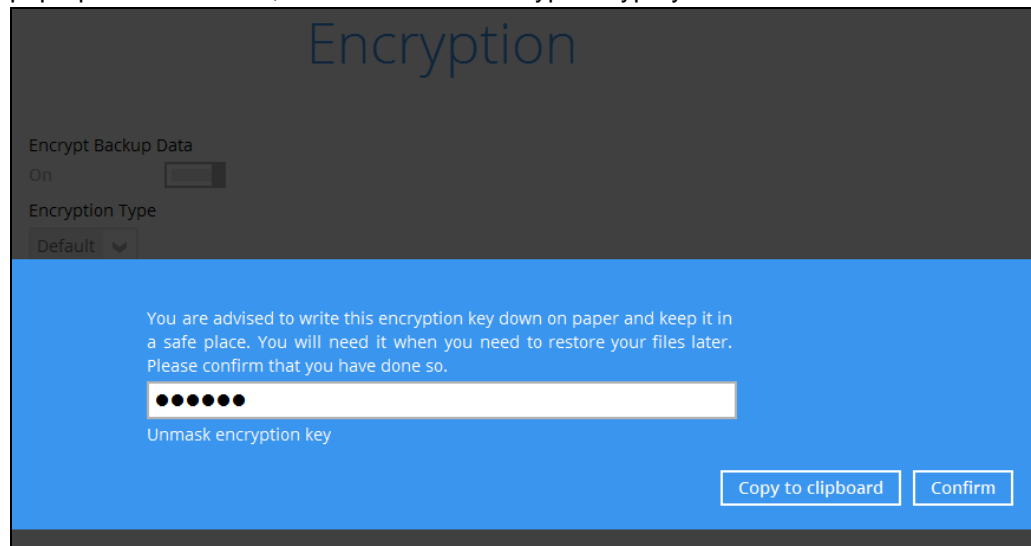
Key length
☐ 128-bit ☒ 256-bit

NOTE

- For best practice on managing your encryption key, refer to the following article.
https://wiki.ahsay.com/doku.php?id=public:8015_faq:best_practices_for_managing_encryption_key
- For local, mapped drive, or removable drive storage destinations with Run Direct enabled the compression type will be set **No Compression** and data encryption is **disabled** to ensure optimal backup and restore performance. The backup set compression type and data encryption settings will only be applied to CBS, SFTP/FTP, or Cloud storage destinations for the backup set.

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

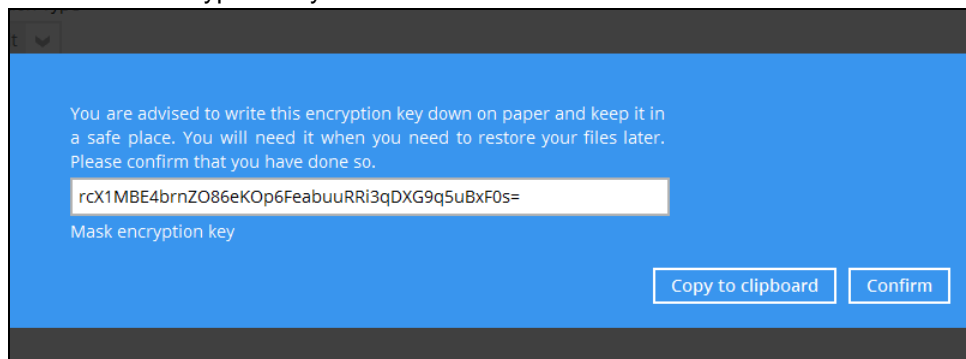
10. If you have enabled the Encryption Key feature in the previous step, the following pop-up window shows, no matter which encryption type you have selected.



The screenshot shows a dark-themed window titled "Encryption". It has a section for "Encrypt Backup Data" with a toggle switch set to "On" and a dropdown for "Encryption Type" set to "Default". Below this is a blue area with 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." A text box contains masked characters "●●●●●●". Below the text box is the label "Unmask encryption key". At the bottom right are two buttons: "Copy to clipboard" and "Confirm".

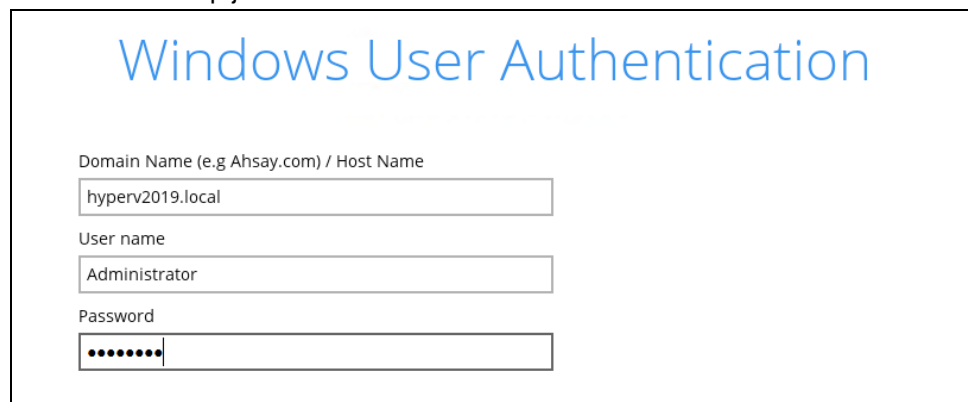
The pop-up window has the following three options to choose from:

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



The screenshot shows the same "Encryption" window, but the text box now displays the unmasked encryption key: "rcX1MBE4brnZO86eKOp6FeabuuRRI3qDXG9q5uBxF0s=". Below the text box is the label "Mask encryption key". The "Copy to clipboard" and "Confirm" buttons remain at the bottom right.

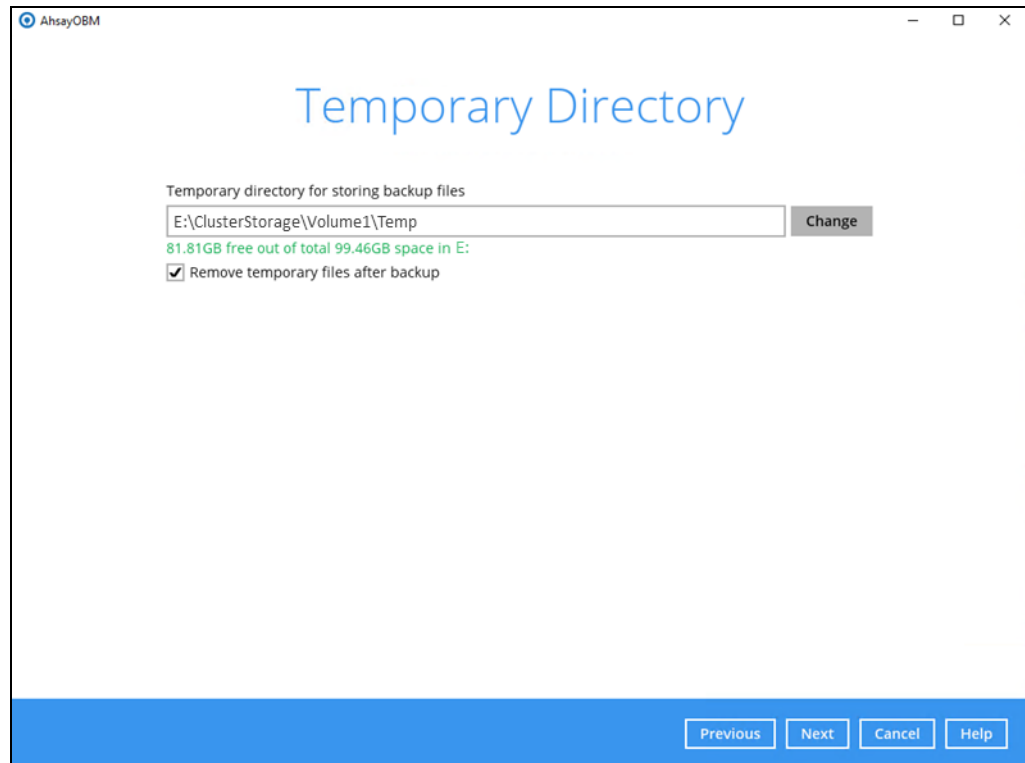
- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.
 - **Confirm** – Click to exit this pop-up window and proceed to the next step.
11. Enter the Windows login credentials used by AhsayOBM to authenticate the scheduled backup job.



The screenshot shows a light blue window titled "Windows User Authentication". It contains three input fields: "Domain Name (e.g Ahsay.com) / Host Name" with the value "hyperv2019.local", "User name" with the value "Administrator", and "Password" with masked characters "●●●●●●".

NOTE: If the backup schedule is turned off for the backup set the Windows User Authentication screen will be automatically skipped. The Windows User Authentication login credentials can be added or updated post backup set creation.

12. Configure a temporary directory for the backup set, then click **Next** to finish the setting. Upon creation of backup set, the temporary directory is set to `C:\Users\Administrator\obm\temp` by default. For optimal backup and/or restore performance, temporary directory location should be changed to other available drive (e.g. drive E:\) and not on **Windows System C:\ drive** or a drive which is accessible to all nodes in the cluster, i.e. Cluster Shared Volume.



AhsayOBM

Temporary Directory

Temporary directory for storing backup files

E:\ClusterStorage\Volume1\Temp Change

81.81GB free out of total 99.46GB space in E:

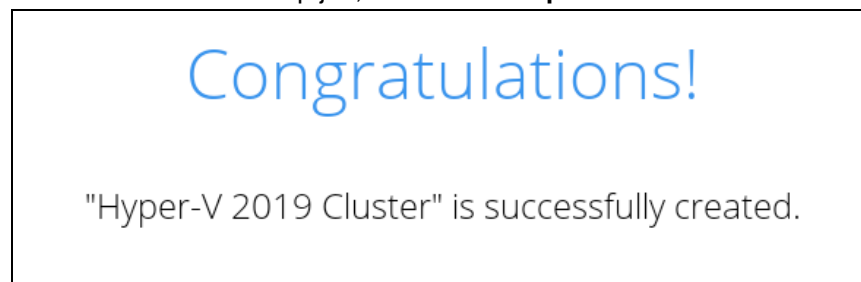
☒ Remove temporary files after backup

Previous Next Cancel Help

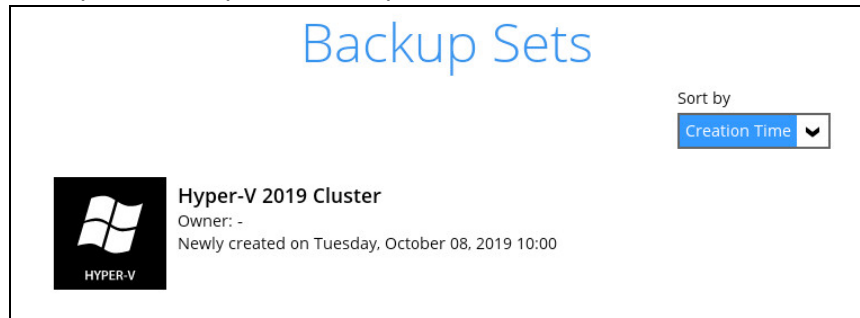
Refer to [Chapter 2.9](#) of this document for details on the temporary directory requirement. To know more about how to set up the temporary directory location, refer to the following KB article:

[FAQ: Tips on how to set up the temporary directory for your backup set](#)

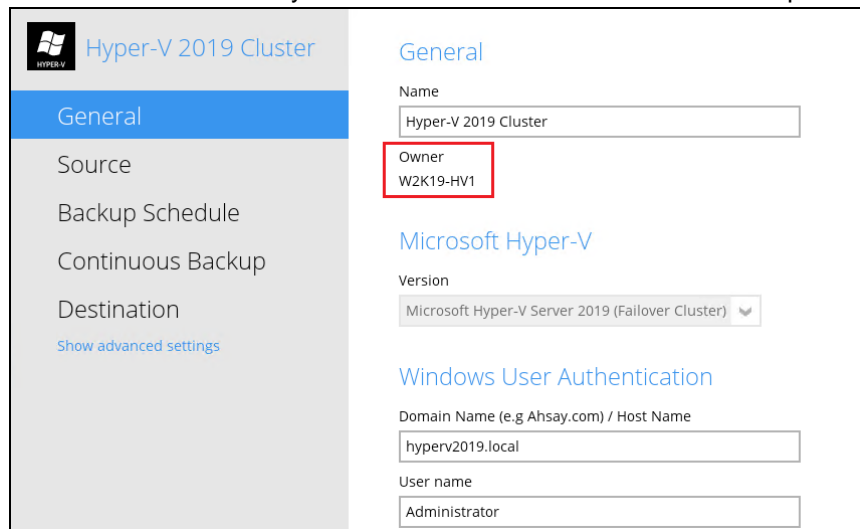
13. Backup set created.
 - i. To start a manual backup job, click on **Backup now**.



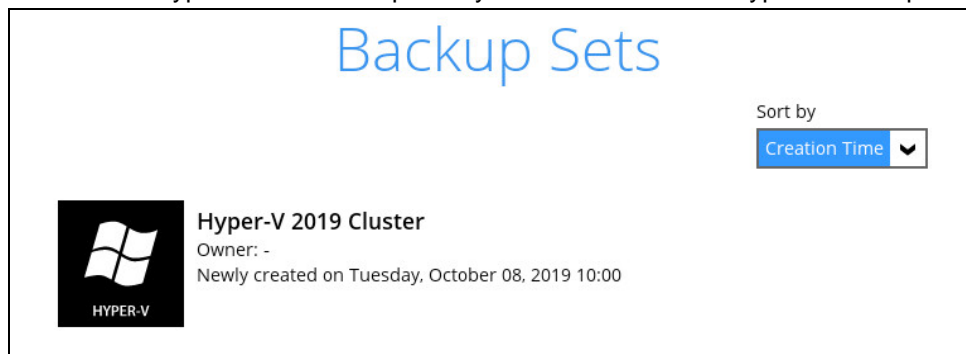
- ii. To verify the backup set settings, click on Close and then click on the Hyper-V backup set to complete the setup.



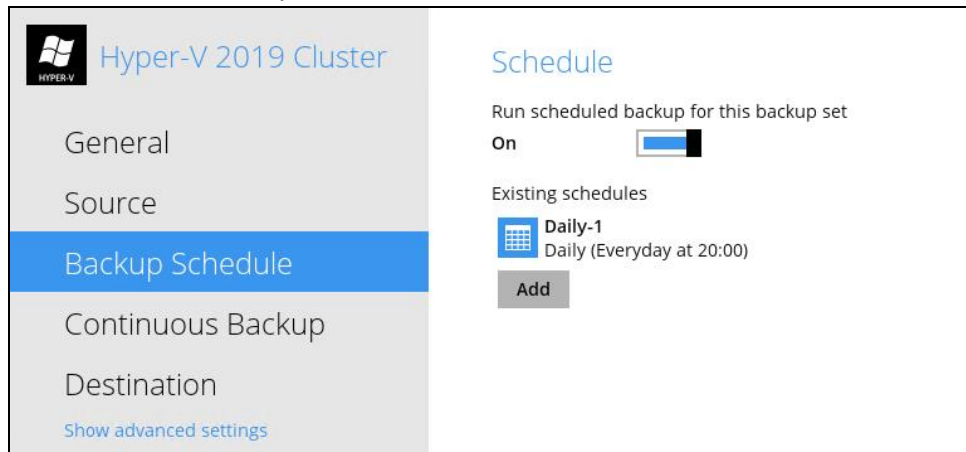
- iii. Go to **General** and verify if the node has been added to the backup schedule.



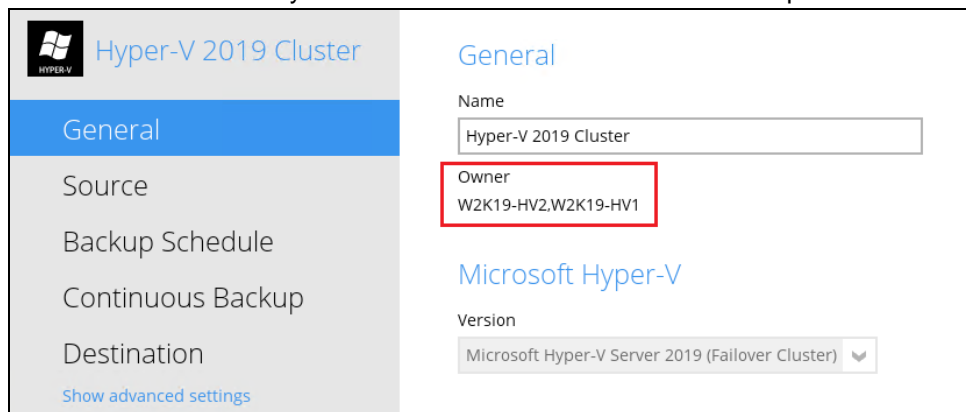
14. On the next Hyper-V node startup AhsayOBM and select the Hyper-V backup set.



15. Go to **Backup schedule** and enable the **Run schedule backup for this backup set** and set the backup schedule time and click on **Save** when finished.



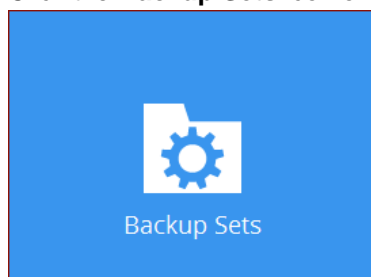
16. Go to **General** and verify if the node has been added to the backup schedule.



17. Repeat steps 14 to 16 for all Hyper-V Cluster nodes.

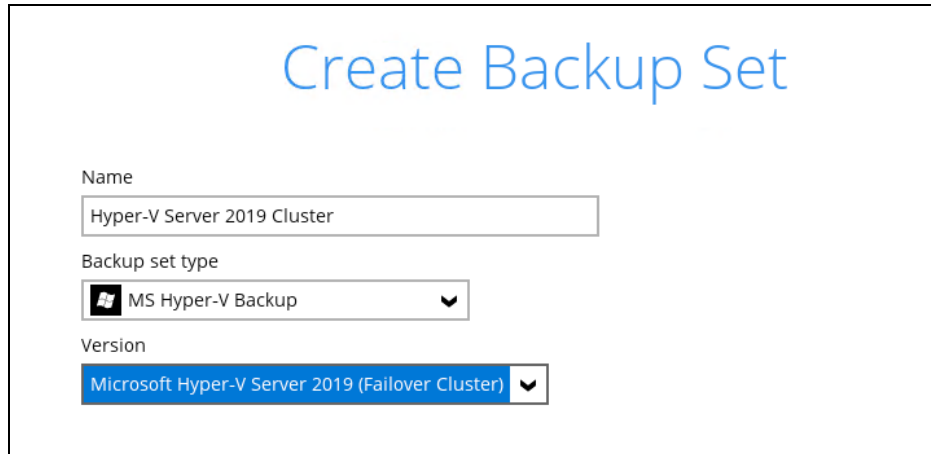
6.2.2 Non-Run Direct Backup Set

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

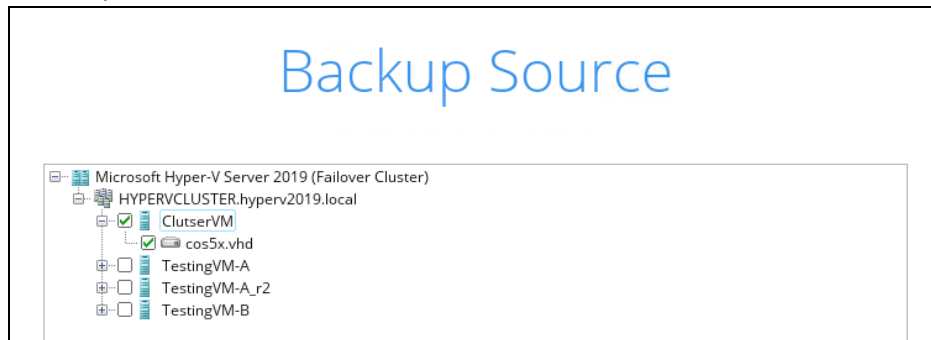


2. Create a new backup set by clicking the “+” icon or **Add** button to created new backup set.
3. Select the **Backup set type** MS Hyper-V Backup, Version **Microsoft Hyper-V Server 2012 R2 (Failover Cluster)**, and name your new backup set then click **Next**

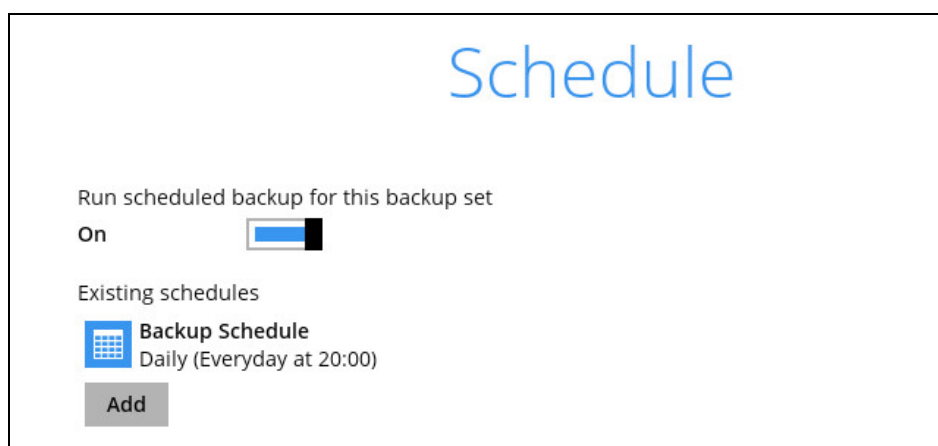
to proceed.



4. In the Backup Source menu, select the guest VM(s) you would like to backup. Click **Next** to proceed.



5. In the Schedule window, the **Run scheduled backup for this backup set** is turned on by default. You may edit the existing backup schedule, or you may create a new schedule for backup job to run automatically at your specified time interval.



Click on **Add** if you want to add a new schedule.

New Backup Schedule

Name
Daily-1

Type
Daily

Start backup
at 13 : 00

Stop
until full backup completed

☐ Run Retention Policy after backup

Click **OK** when you are done setting. Then click **Next** to proceed.

- Select the backup storage destination. To select a cloud, SFTP/FTP, or CBS as a storage destination un-select **Run Direct** setting and select your desired cloud, SFTP/FTP, or CBS as a storage destination. Click **OK** to proceed when you are done.

New Storage Destination / Destination Pool

Name
AhsayCBS

Run Direct
☐ Support restoring a VM into your production environment by running it directly from the backup file
(No encryption and compression will be applied to backup data.)

Destination storage
AhsayCBS

- Click **Add** to add additional storage destination or click **Next** to proceed when you are done.

Destination

Backup mode
Sequential

Existing storage destinations

AhsayCBS
Host: 10.120.10.30:443

Add

^ v

8. If you wish to enable the Granular Restore feature, make sure you turn on the **Granular Restore** switch in this menu. Click **Next** to proceed.

Granular Restore

Granular Restore
On ☒

Support of granular restoration for individual files inside virtual machine.

When granular restore is enabled, to optimize restore performance both compression and encryption will be disabled for this backup set.

Once granular restore is enabled and the setting is saved, it cannot be disabled without re-creating the backup set.

NOTES

1. Once the Granular Restore feature is enabled and the backup set is saved, it is **NOT** possible to disable it afterwards, and vice versa. If you wish to change the Granular Restore settings, a new backup set will have to be created.
2. It is possible to enable both Granular Restore and Run Direct restore on the same backup set. However, AhsayOBM will only allow either Granular Restore or Run Direct restore to run, but not to run concurrently.
3. Granular Restore requires an additional OpenDirect / Granular restore add-on module license to work. Contact your backup service provider for further details.
4. Granular Restore might not be available, this depends on your backup service provider settings. Contact your backup service provider for more information.

9. **IMPORTANT:** If you have enabled the Granular Restore or Run Direct restore feature, backup data will not be compressed and encrypted to optimize restore performance, therefore you can skip to step 11.

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.

Encryption

Encrypt Backup Data
On ☒

Encryption Type

Default

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.

Encryption

Encrypt Backup Data
On ☒

Encryption Type
Custom ▼

Algorithm
AES ▼

Encryption key

Re-enter encryption key

Method
☐ ECB ☒ CBC

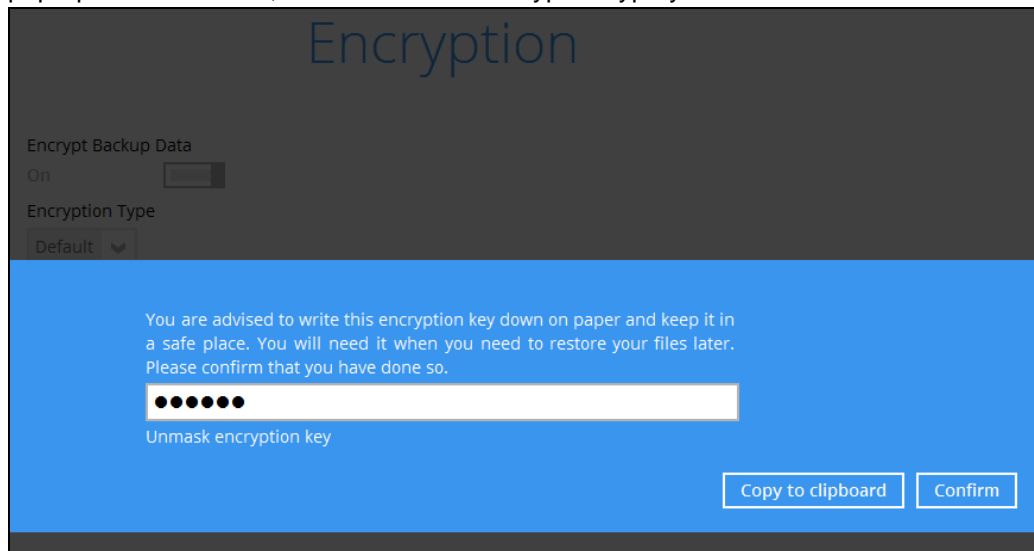
Key length
☐ 128-bit ☒ 256-bit

NOTE

- For best practice on managing your encryption key, refer to the following article.
https://wiki.ahsay.com/doku.php?id=public:8015_faq:best_practices_for_managing_encryption_key
- For local, mapped drive, or removable drive storage destinations with Run Direct enabled the compression type will be set **No Compression** and data encryption is **disabled** to ensure optimal backup and restore performance. The backup set compression type and data encryption settings will only be applied to CBS, SFTP/FTP, or Cloud storage destinations for the backup set.

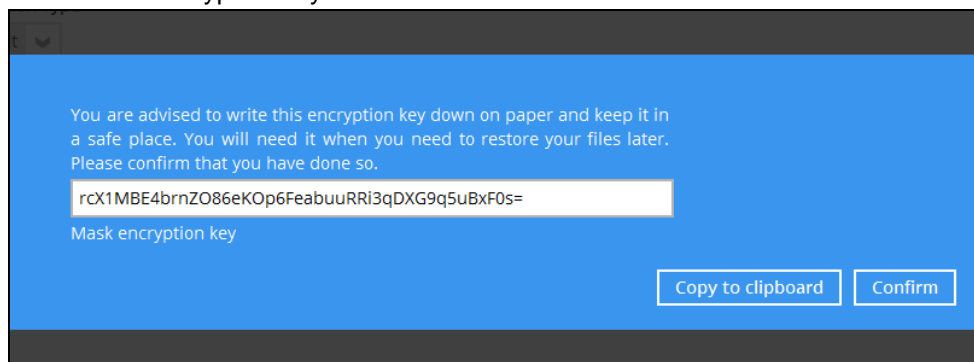
Click **Next** when you are done setting.

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



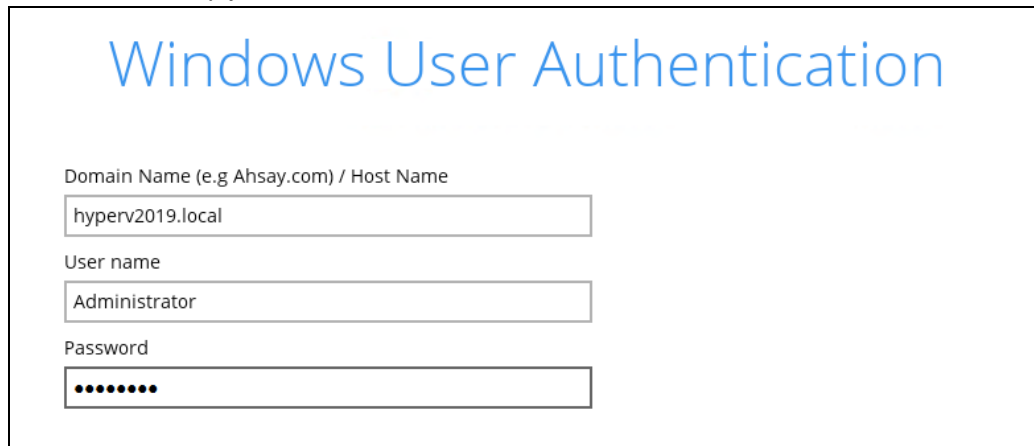
The pop-up window has the following three options to choose from:

- **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.

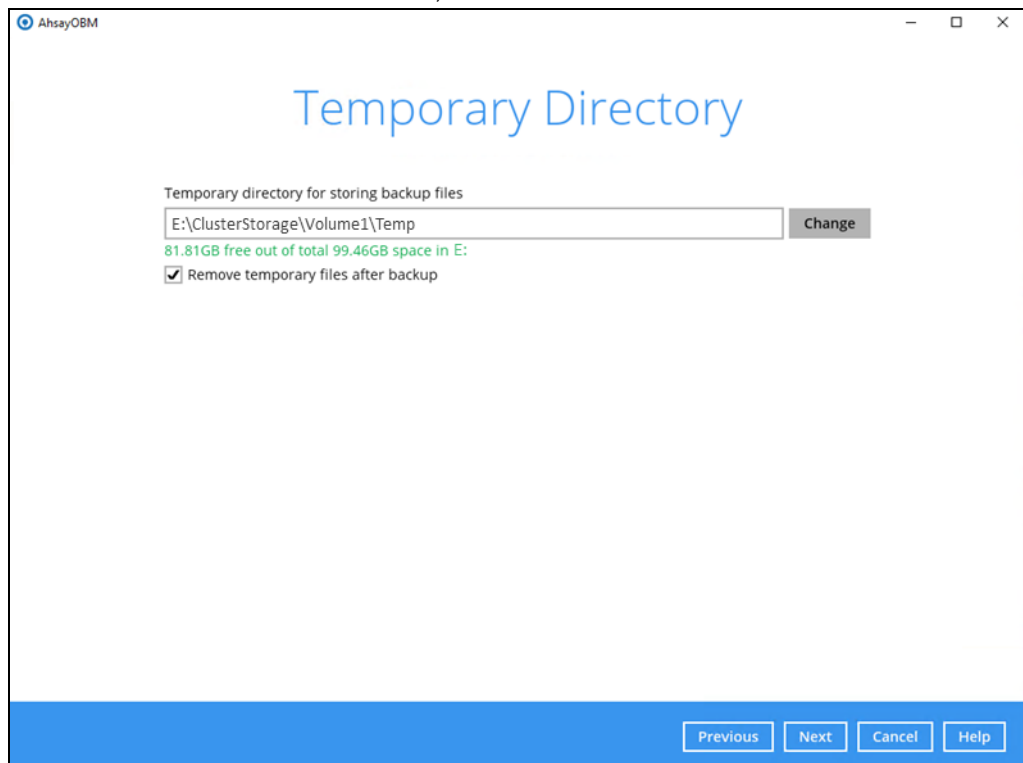
11. Enter the Windows login credentials used by AhsayOBM to authenticate the scheduled backup job.



The screenshot shows a dialog box titled "Windows User Authentication". It contains three input fields: "Domain Name (e.g Ahsay.com) / Host Name" with the value "hyperv2019.local", "User name" with the value "Administrator", and "Password" which is masked with dots. The dialog box has a light blue header and a white body.

NOTE: If the backup schedule is turned off for the backup set the Windows User Authentication screen will be automatically skipped. The Windows User Authentication login credentials can be added or update post backup set creation.

12. Configure a temporary directory for the backup set, then click **Next** to finish the setting. Upon creation of backup set, the temporary directory is set to `C:\Users\Administrator\obm\temp` by default. For optimal backup and/or restore performance, temporary directory location should be changed to other available drive (e.g. drive E:\) and not on **Windows System C:\ drive** or a drive which is accessible to all nodes in the cluster, i.e. Cluster Shared Volume.



The screenshot shows a window titled "Temporary Directory" from the AhsayOBM application. It features a text input field for the "Temporary directory for storing backup files" containing the path "E:\ClusterStorage\Volume1\Temp". To the right of the input field is a "Change" button. Below the input field, a green status message reads "81.81GB free out of total 99.46GB space in E:". A checkbox labeled "Remove temporary files after backup" is checked. At the bottom of the window, there is a blue bar containing four buttons: "Previous", "Next", "Cancel", and "Help".

Refer to [Chapter 2.9](#) of this document for details on the temporary directory requirement. To know more about how to set up the temporary directory location, refer to the following KB article:

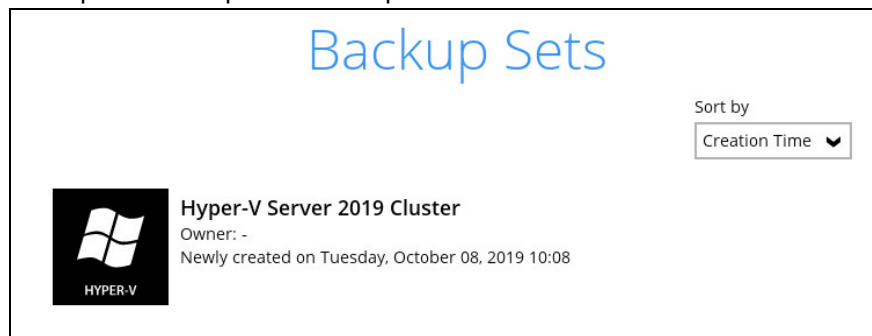
[FAQ: Tips on how to set up the temporary directory for your backup set](#)

13. **Backup set created.**

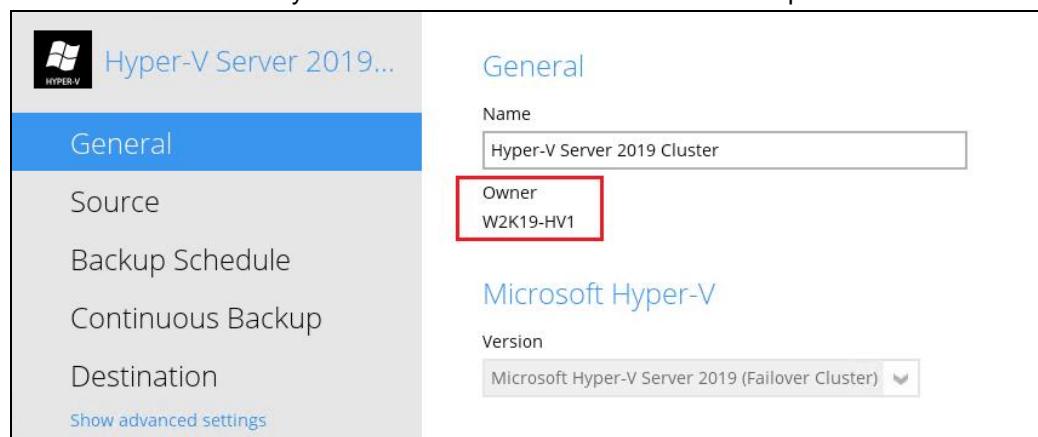
- i. To start a manual backup job, click on **Backup now**.



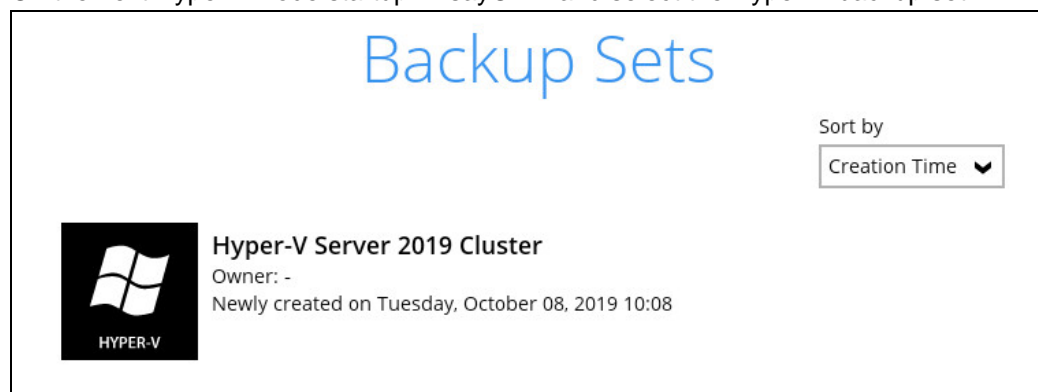
- ii. To verify the backup set settings, click on Close and then click on the Hyper-V backup set to complete the setup.



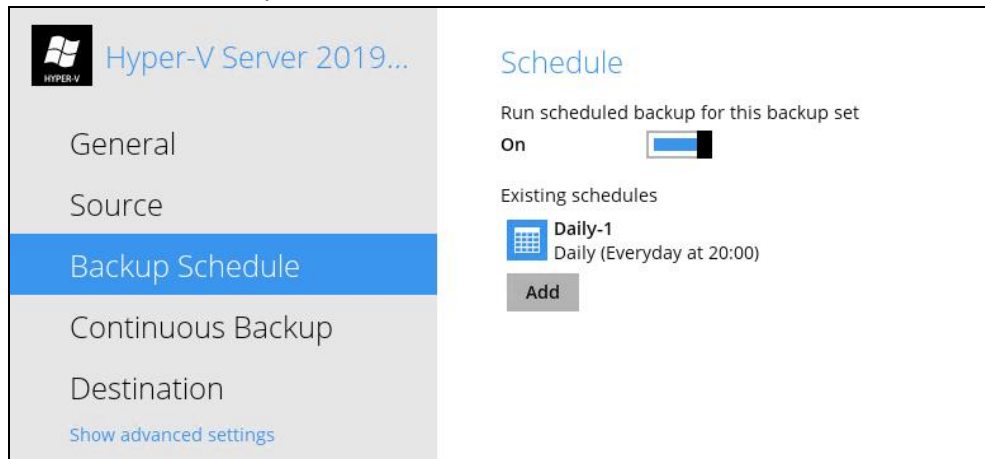
14. Go to **General** and verify if the node has been added to the backup schedule.



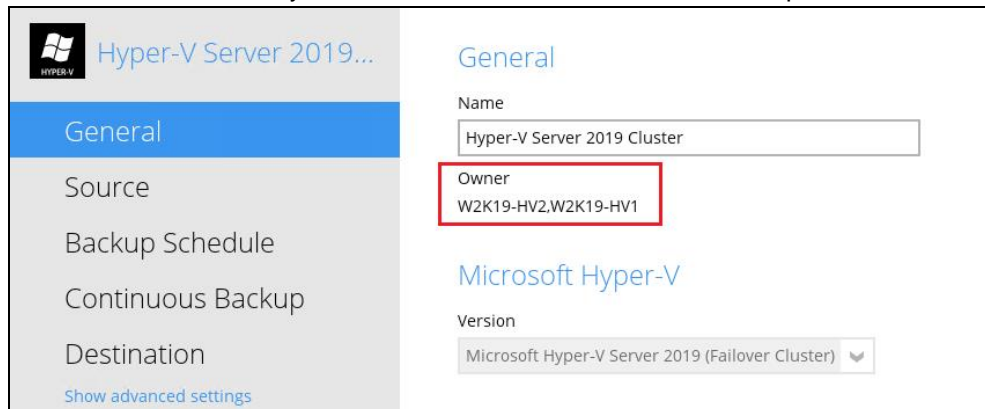
15. On the next Hyper-V node startup AhsayOBM and select the Hyper-V backup set.



16. Go to **Backup schedule** and enable the **Run schedule backup for this backup set** and set the backup schedule time and click on **Save** when finished.



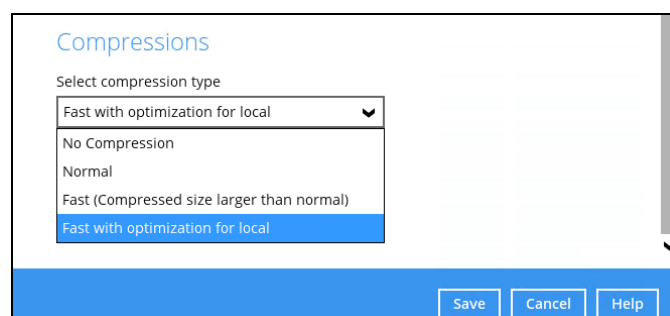
17. Go to **General** and verify if the node has been added to the backup schedule.



18. Repeat steps 15 to 17 for all Hyper-V Cluster nodes.
19. Optional: Select your preferred **Compression** type. By default, the compression type is Fast with optimization for local.

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

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



7 Overview on the Backup Process

The following steps are performed during a Hyper-V backup job. For an overview of the detailed process for Steps 3, 5, 14, and 16, please 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 \(Step 16\)](#)
- ▶ [Data Validation Check Process \(Step 14\)](#)



7.1 Periodic Data Integrity Check (PDIC) Process

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

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

PDIC schedule = %BackupSetID% modulo 5

or

%BackupSetID% mod 5

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

0	Monday
1	Tuesday
2	Wednesday
3	Thursday
4	Friday

NOTE: The PDIC schedule cannot be changed.

Example:

Backup set ID: 1594627447932

Calculation: $1594627447932 \bmod 5 = 2$

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

In this example:

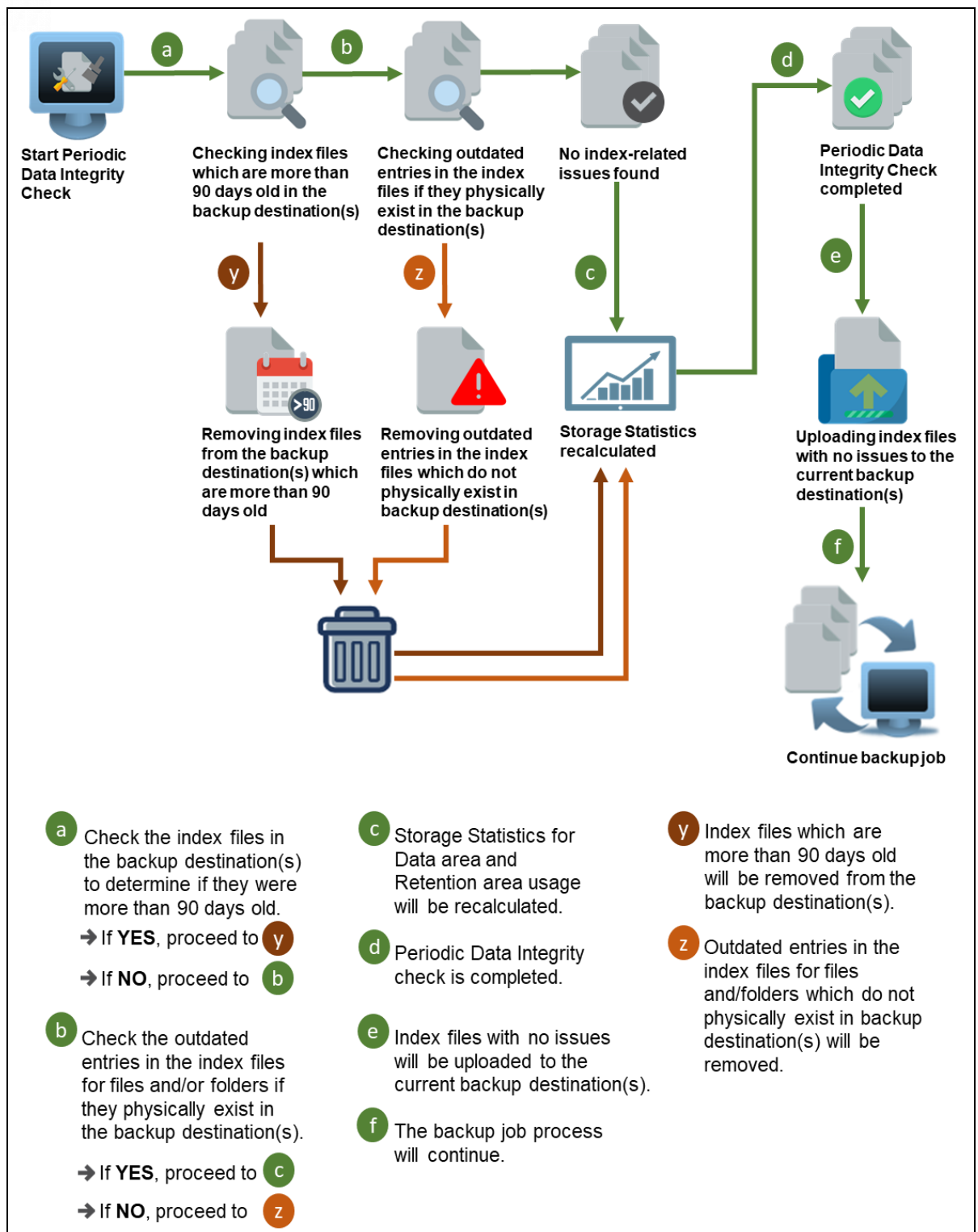
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

NOTE

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

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

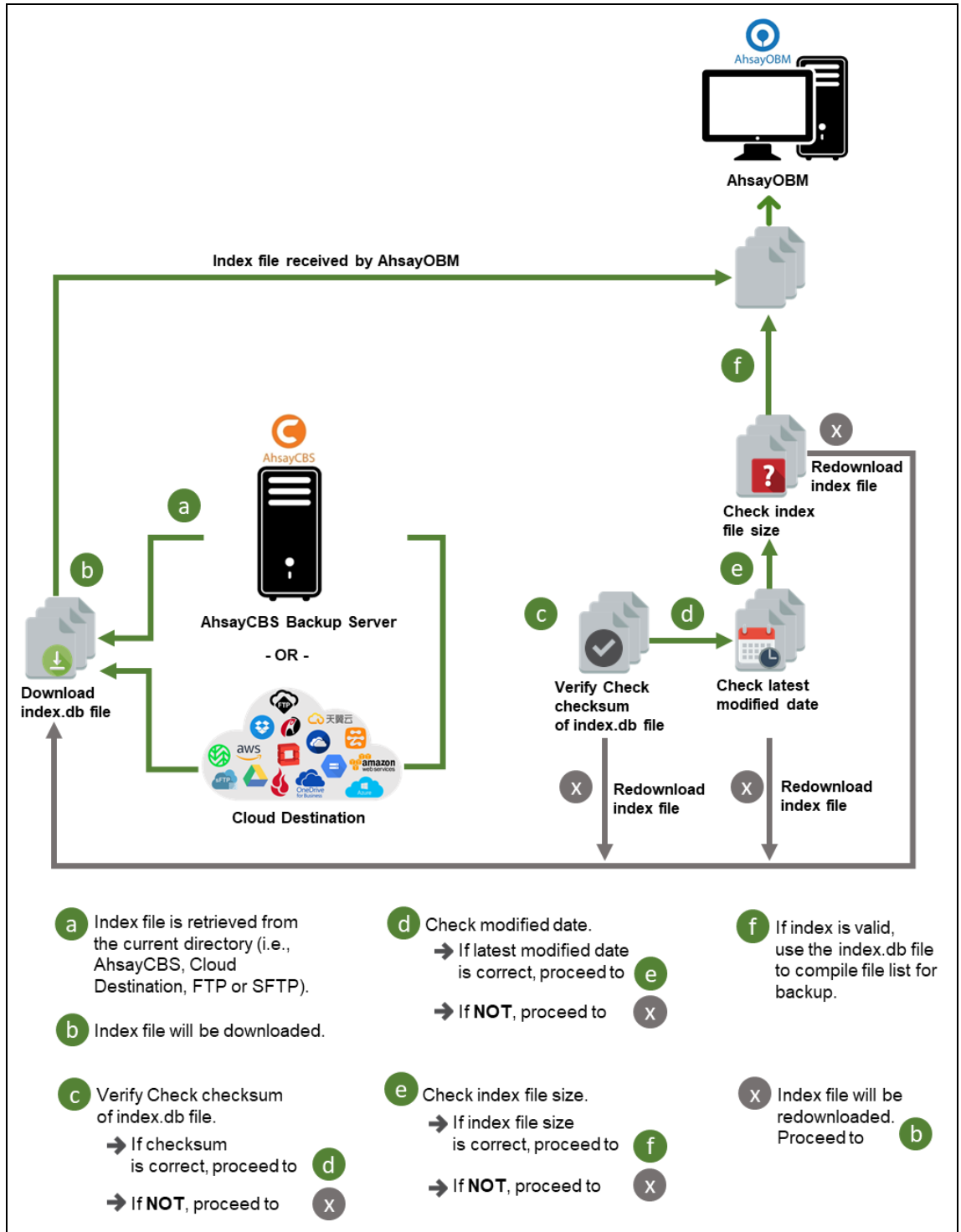
1. If AhsayOBM was upgraded to v8.5 (or above) from an older version v6, v7, or pre-8.3.6.0 version. In this case, the PDIC job will run on the first backup job after upgrade.
2. If backup jobs for a backup set are not run on a regular daily backup schedule (for example: on a weekly or monthly schedule),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



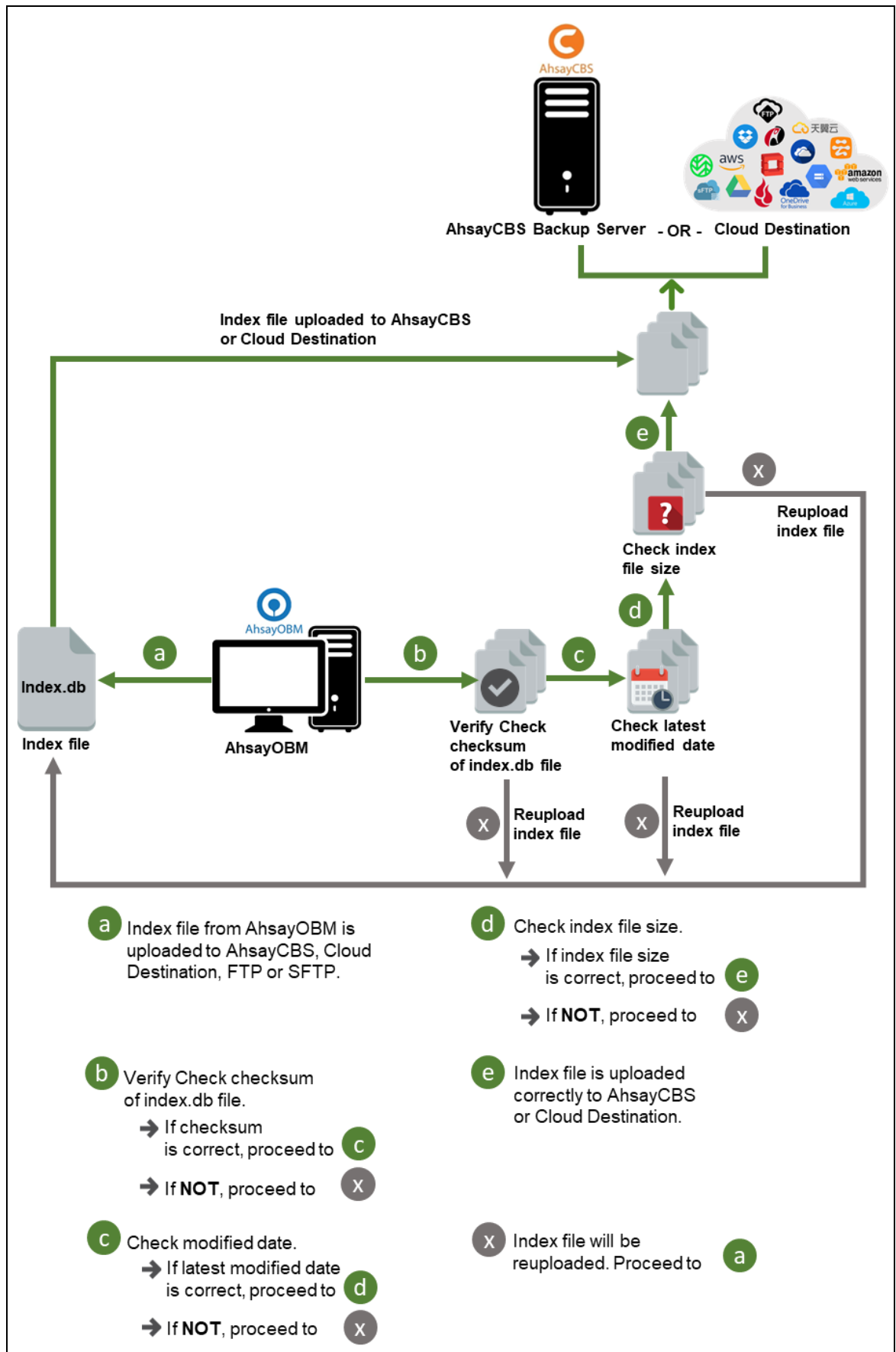
7.2 Backup Set Index Handling Process

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

7.2.1 Start Backup Job

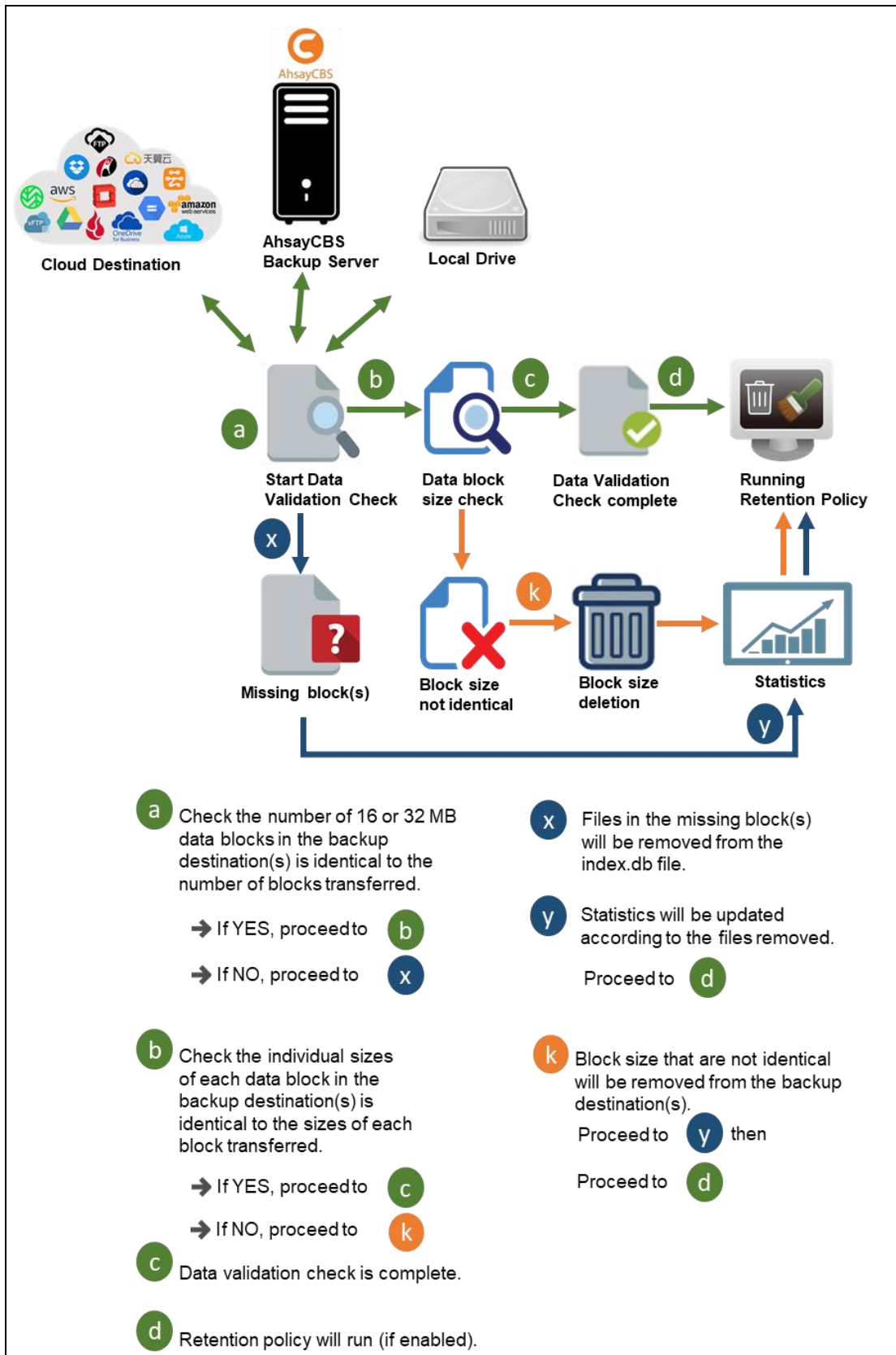


7.2.2 Completed Backup Job



7.3 Data Validation Check Process

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



8 Running Backup Jobs

8.1 Login to AhsayOBM

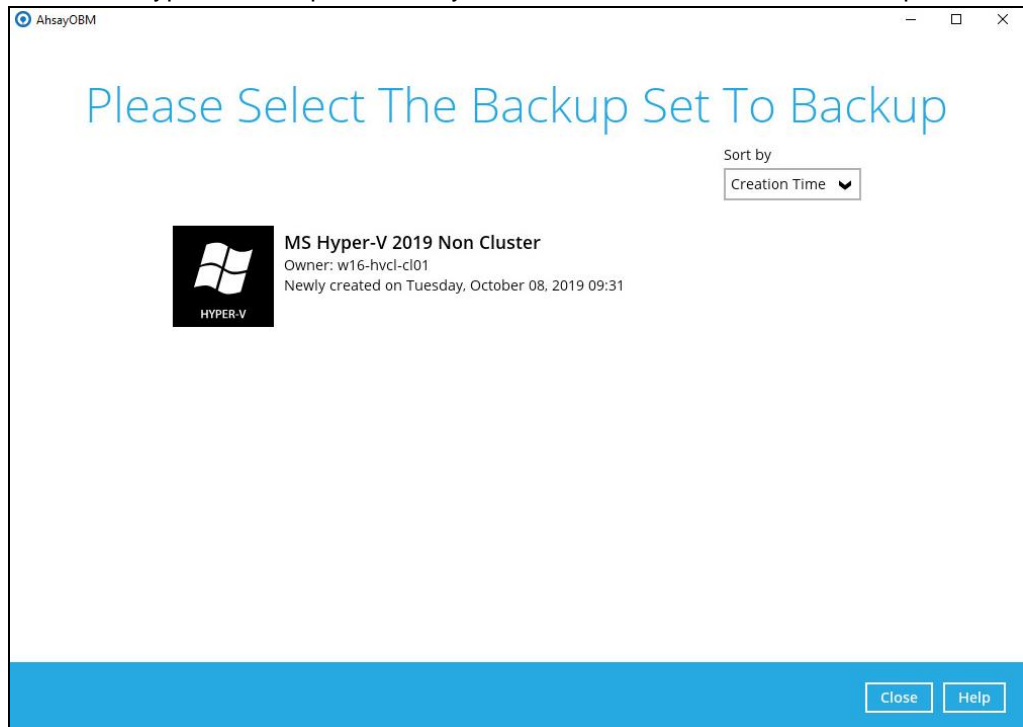
Log in to the AhsayOBM application according to the instructions in [Chapter 5](#).

8.2 Start a Manual Backup

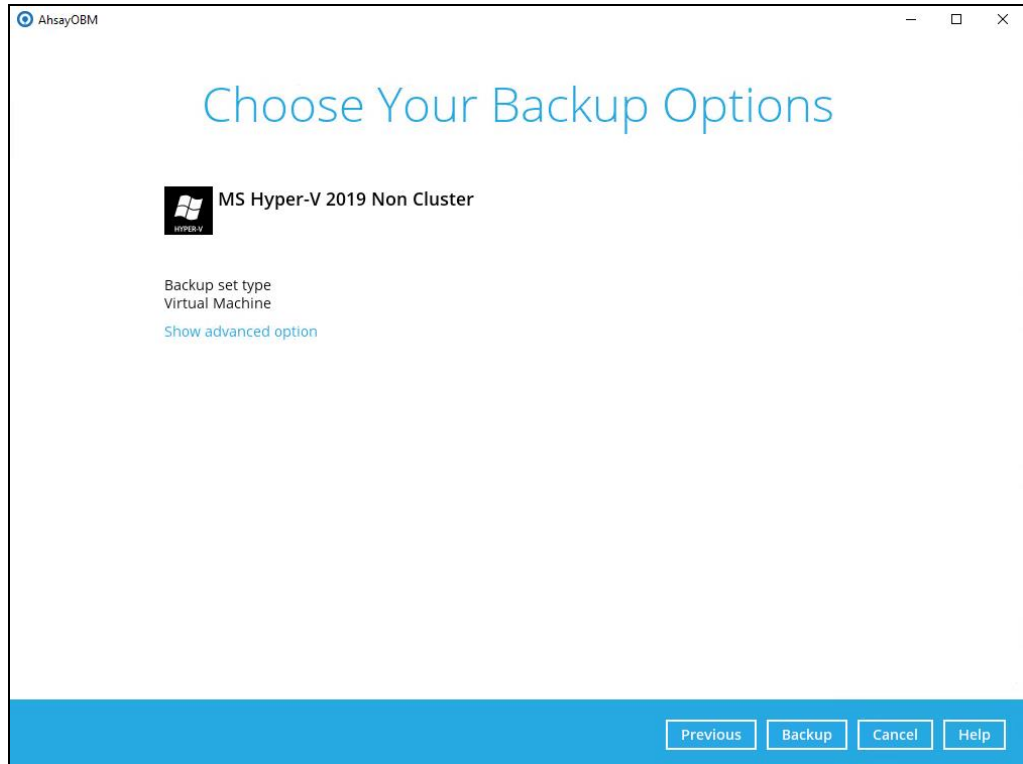
1. Click the Backup icon on the main interface of AhsayOBM.



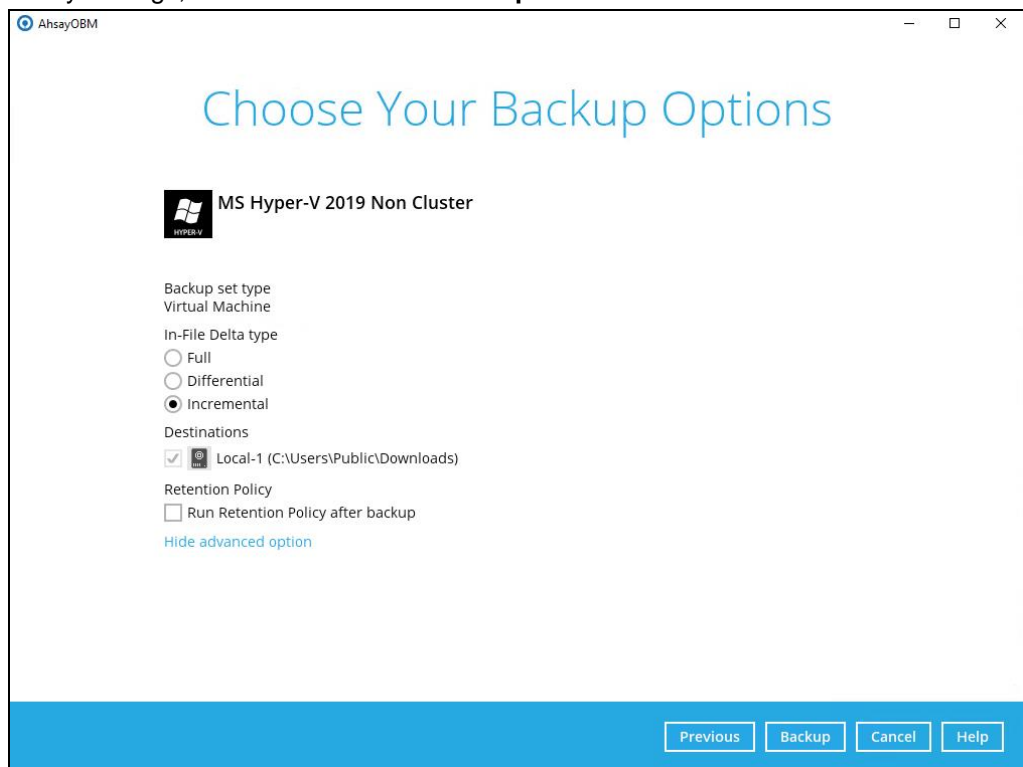
2. Select the Hyper-V backup set which you would like to start a manual backup.



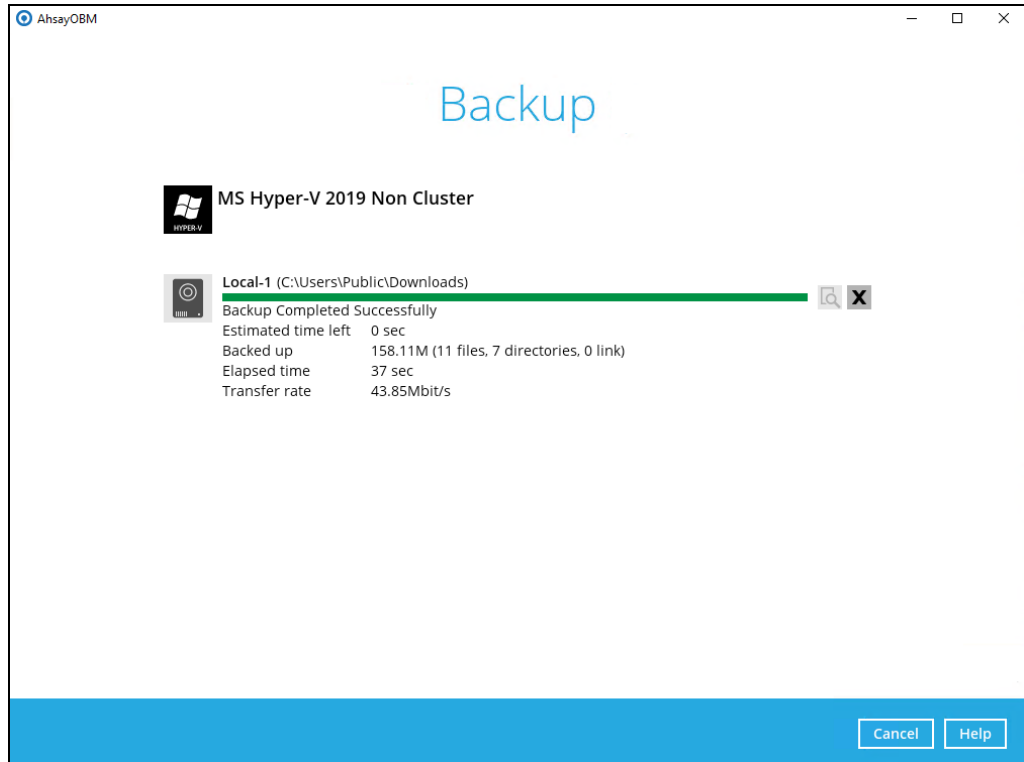
3. Click on **Backup** to start the backup job.



4. If you would like to modify the In-File Delta type, Destinations, or Run Retention Policy settings, click on **Show advanced option**.

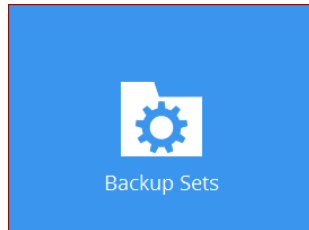


5. Backup job is completed.

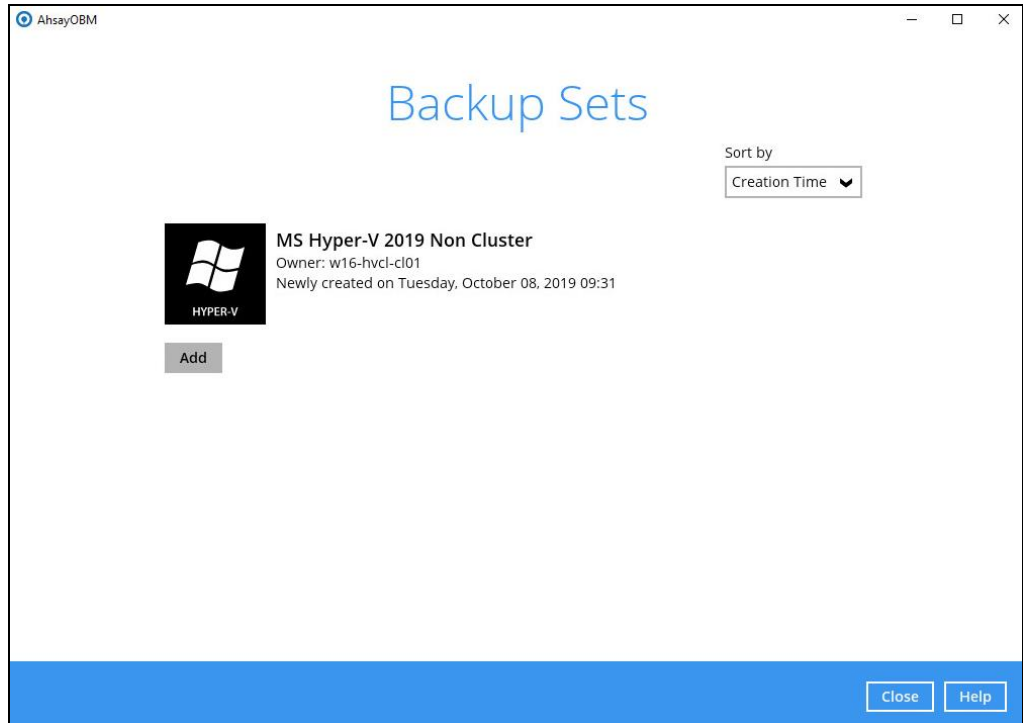


8.3 Configure Backup Schedule for Automated Backup

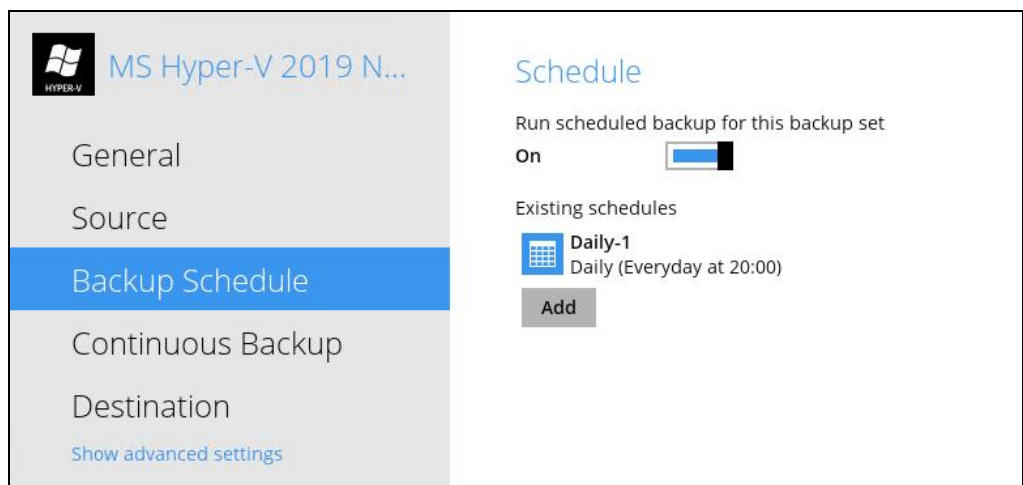
1. Click on the **Backup Sets** icon on the AhsayOBM main interface.



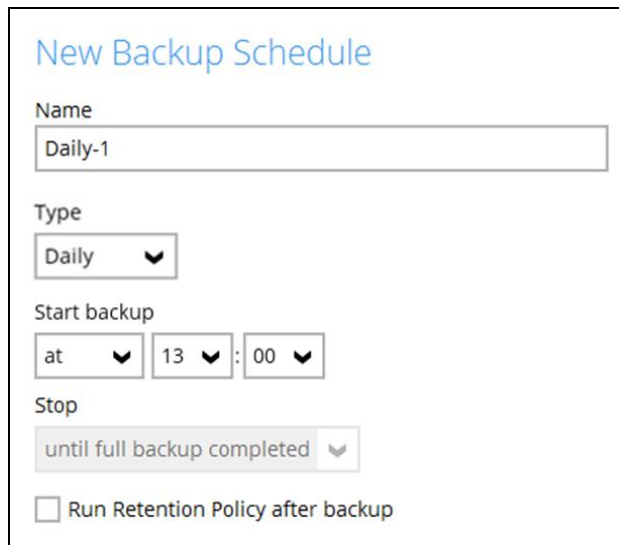
2. Select the backup set that you would like to create a backup schedule for.



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



4. The New Backup Schedule window will appear.



New Backup Schedule

Name
Daily-1

Type
Daily ▼

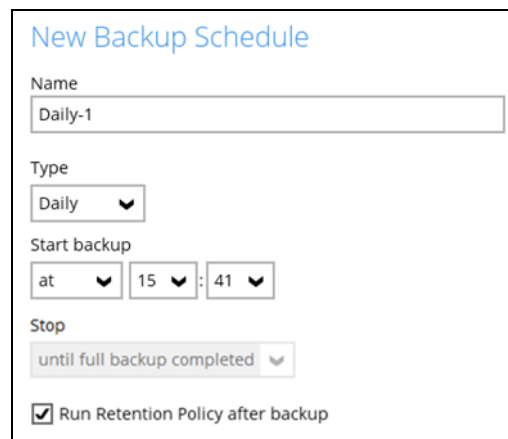
Start backup
at ▼ 13 ▼ : 00 ▼

Stop
until full backup completed ▼

☐ Run Retention Policy after backup

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

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



New Backup Schedule

Name
Daily-1

Type
Daily ▼

Start backup
at ▼ 15 ▼ : 41 ▼

Stop
until full backup completed ▼

☒ Run Retention Policy after backup

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

New Backup Schedule

Name
Weekly-1

Type
Weekly

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

Start backup
 at 23 : 00

Stop
 until full backup completed

☒ Run Retention Policy after backup

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

New Backup Schedule

Name
Monthly-1

Type
Monthly

Backup on the following day every month
☒ Day Last
☐ First Sunday

Start backup at
 23 : 00 on the selected days

Stop
 until full backup completed

☒ Run Retention Policy after backup

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

New Backup Schedule

Name
Custom-1

Type
Custom

Backup on the following day once
 2020 June 31

Start backup at
 23 : 59

Stop
 until full backup completed

☒ Run Retention Policy after backup

• **Start backup** – the start time of the backup job.

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

Here is an example of a backup set that has a periodic and normal backup schedule.

Figure 1.1

Figure 1.2

Figure 1.1 – Periodic backup schedule runs every 4 hours from Monday – Friday during business hours

Figure 1.2 – Normal backup schedule runs at 21:00 or 9:00 PM on Saturday and Sunday on weekend non-business 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.

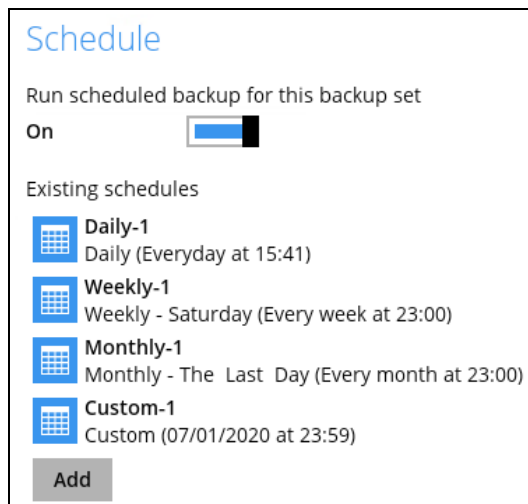
For example, if a backup has 100GB file size which will take approximately 15 hours to complete on your environment, but you set the “stop” after 10 hours, the file will be partially backed up and cannot be restored. The next backup will upload the files from scratch again.

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 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:



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

9 Restoring Hyper-V Guest Virtual Machines

Restore Options

There are three major types of restore options, namely Run Direct Restore, Non-Run Direct Restore and Granular Restore.

Run Direct Restore
Start up the guest VM directly from the backup file without restoring the guest VM to the Hyper-V server.
Type 1 – Original Hyper-V Host
<p>Start up a guest VM from Backup Destination without Auto Migration Enabled -- The guest VM data will not migrate to the destination until you manually trigger this action by following the steps in Migrate Virtual Machine (Permanently Restore). If manual migration is not performed, any changes made during the Run Direct instance will NOT be committed to backup files.</p> <p>Start up a guest VM from Backup Destination with Auto Migration Enabled -- To start up the guest VM directly from the backup file and then start restoring the guest VM files to the Hyper-V server. VM guest will start migrating without the need to trigger a manual migration. Any changes made during the Run Direct instance will also be committed to the Hyper-V server as well.</p>
Type 2 – Different (Standby) Hyper-V Host
<p>Run Direct restore guest VM to a standby Hyper-V host is supported.</p> <p>This restore option allows you to restore your backed up guest VM to another Hyper-V host, for example: if your original Hyper-V host is down and you need to restore your production guest VM's to a standby Hyper-V host.</p> <p>Start up a guest VM from Backup Destination without Auto Migration Enabled -- The guest VM data will not migrate to the destination until you manually trigger this action by following the steps in Migrate Virtual Machine (Permanently Restore). If manual migration is not performed, any changes made during the Run Direct instance will NOT be committed to backup files.</p> <p>Start up a guest VM from Backup Destination with Auto Migration Enabled -- To start up the guest VM directly from the backup file and then start restoring the guest VM files to the Hyper-V server. VM data will start migrating without the need to trigger a manual migration. Any changes made during the Run Direct instance will also be committed to the Hyper-V server as well.</p>
Non-Run Direct Restore
Conventional restore method where AhsayOBM will restore the guest VM files to the Hyper-V server.

Type 1 – Original Hyper-V Host

Restore of a Guest VM to the Original Hyper-V Host (Original Location) -- This option will restore guest VM to original location which contains the backed up guest VM.

Restore of a Guest VM to the Original Hyper-V Host (Alternate Location) -- This feature will restore any guest VM to another location (a different disk or folder) on the same Hyper-V host.

Type 2 – Different (Standby) Hyper-V Host

Restore of a Guest VM to a different (Standby) Hyper-V Host -- This restore option allows you to restore your backed up guest VM to another Hyper-V host, for example: if your original Hyper-V host is down and you need to restore your production guest VM's to a standby Hyper-V host.

Type 3 – Individual Virtual Disk Restore

Restore of an Individual Virtual Disk to Original/ Different Guest VM -- The Restore raw file feature is used to the restore of an individual virtual disk to the original or a different guest VM.

Granular Restore

AhsayOBM makes use of granular restore technology to enable a file level restore from a virtual disk file (VHD) of guest VM backup possible. It is particularly useful if you only need to restore individual file(s) from a guest VM, which would normally take a long time to restore and then boot up before you can gain access to the files on the virtual disks. Granular restore gives you a fast and convenient way to recover individual files on a guest VM.

For more details about Granular Restore, refer to the [Granular Restore](#) section.

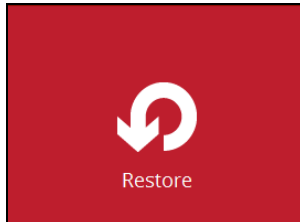
10 Run Direct Restore

10.1 Original Hyper-V Host

10.1.1 Start up a guest VM from Backup Destination without Auto Migration Enabled

Follow the steps below to start up the guest VM directly from the backup files.

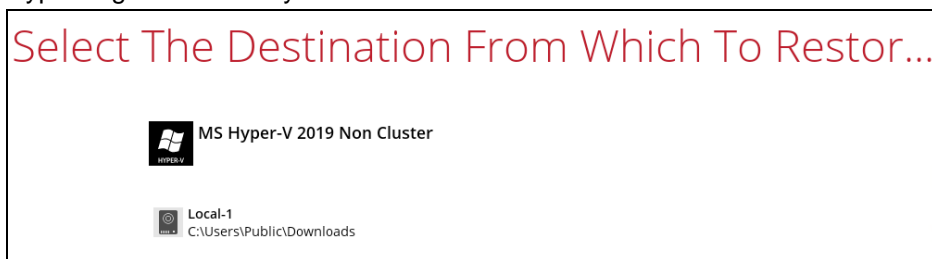
1. In the AhsayOBM main interface, click the Restore icon.



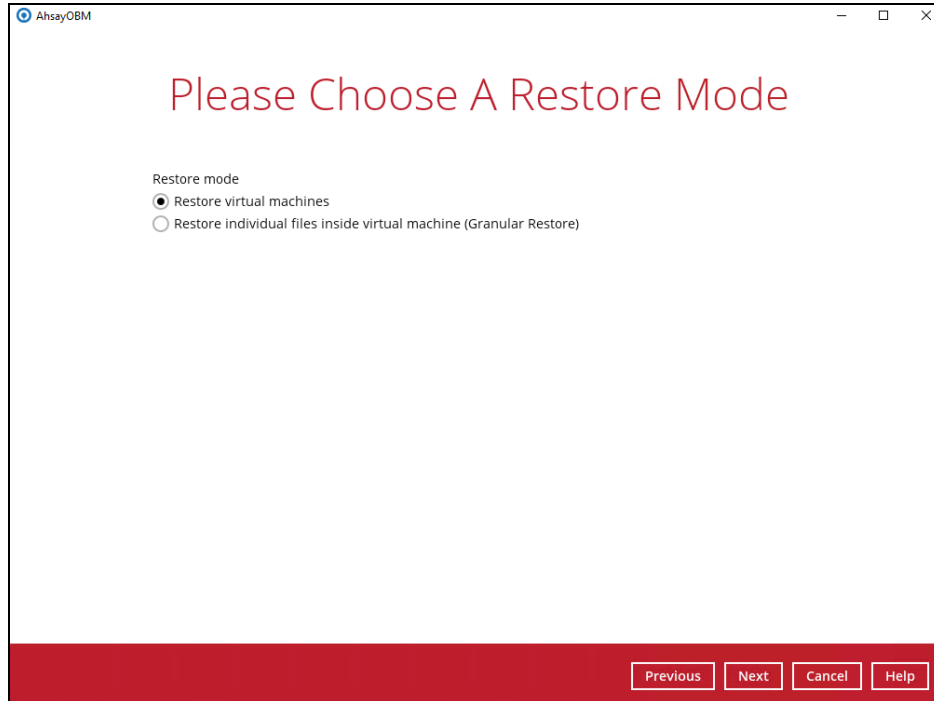
2. Select the backup set that you would like to restore the guest VM from.



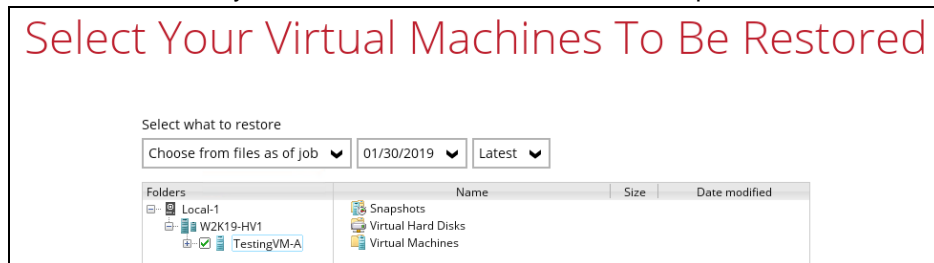
3. Select the local, mapped drive, or removable drive storage destination that contains Hyper-V guest VM that you would like to restore.



4. Select **Restore virtual machines** as the restore mode.



5. Select to restore the Hyper-V guest VM from a specific backup job then select the files or folders that you would like to restore. Click **Next** to proceed.



6. Select to restore the Hyper-V guest VM to the **Original location**, or to an **Alternate location**. Then select **Run Direct** and click **Next** to proceed.

- **Original location** – The Hyper-V guest VM will be restored to the same directory path which stores the backup source on the original Hyper-V host.



- **Alternate location** – The Hyper-V guest VM will be restored to the different directory path on the original Hyper-V host.

Choose Where The Virtual Machines To Be Re...

Restore virtual machines to

☐ Original location

☒ Alternate location

☒ Run Direct

☐ Auto migrate after Run Direct is running

[Show advanced option](#)

Click **Next** to proceed and the following values are needed to be updated:

i. **Virtual Machine Name**

ii. **Virtual Machines Directory Location** (guest configuration files)

iii. **Virtual Hard Disk Location** (new location for the guest VHD files)

Example:

i. Rename the restored guest VM to “**TestingVM-A-2**”

ii. Store the configuration files in the new location
“**C:\ClusterStorage\Volume1\VM\TestingVM-A\TestingVM-A_2**”

iii. Store the VHD files in the new location
“**C:\ClusterStorage\Volume1\VM\TestingVM-A\TestingVM-A_2**”

Alternate location

Virtual Machine Name

TestingVM-A-2

Virtual Machines Directory Location

C:\ClusterStorage\Volume1\VM\TestingVM-A\TestingVM-A_2 [Browse](#)

Virtual Hard Disk Location

C:\ClusterStorage\Volume1\VM\TestingVM-A\TestingVM-A_2 [Browse](#)

When the values have been updated click on **Next** to proceed.

7. Confirm the temporary directory path is correct and then click **Restore** to proceed.

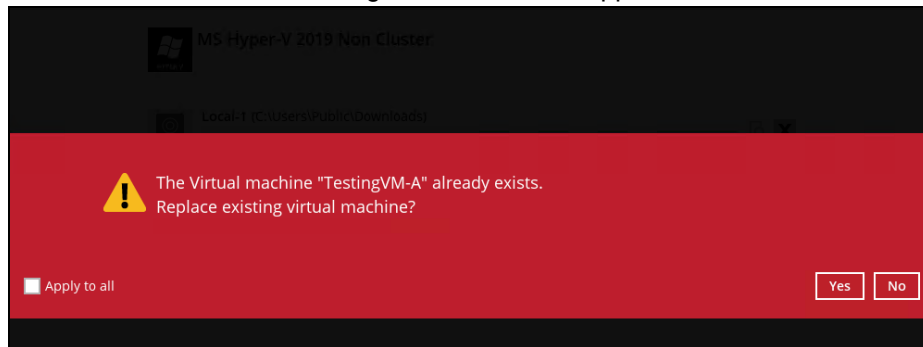
Temporary Directory

Temporary directory for storing restore files

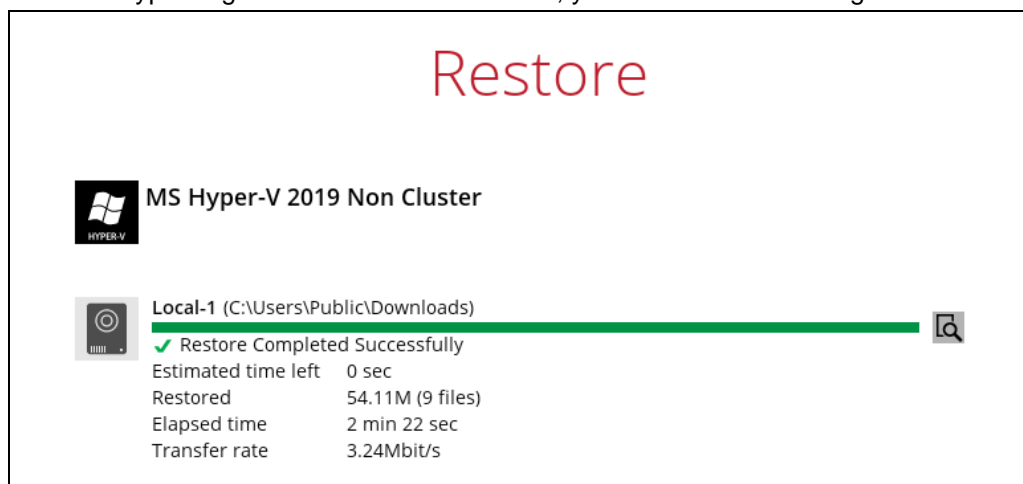
C:\Users\Administrator\.obm\temp [Browse](#)

8. If the guest VM selected to be restored already exists on the Hyper-V server, AhsayOBM will prompt to confirm overwriting of the existing guest.

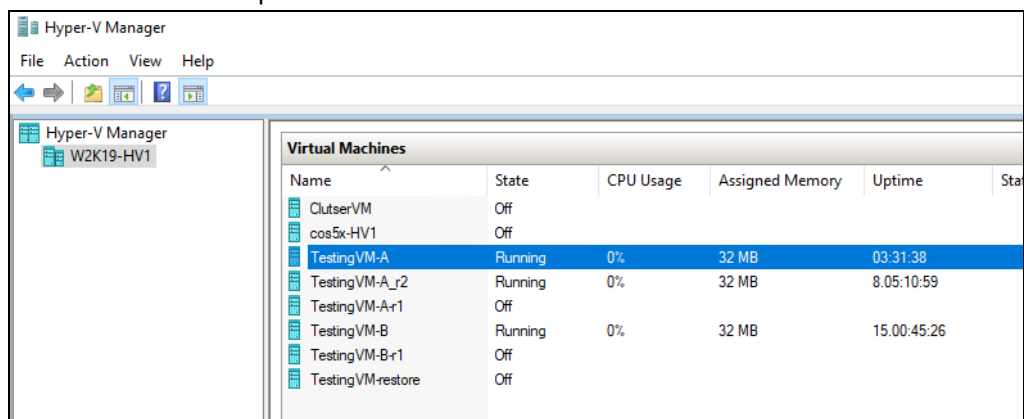
- **Yes** - the existing guest VM will be deleted from the Hyper-V server before the restore process starts.
- **No** - the restore of the current guest VM will be skipped.



9. After the Hyper-V guest VM has been restored, you will see the following screen.

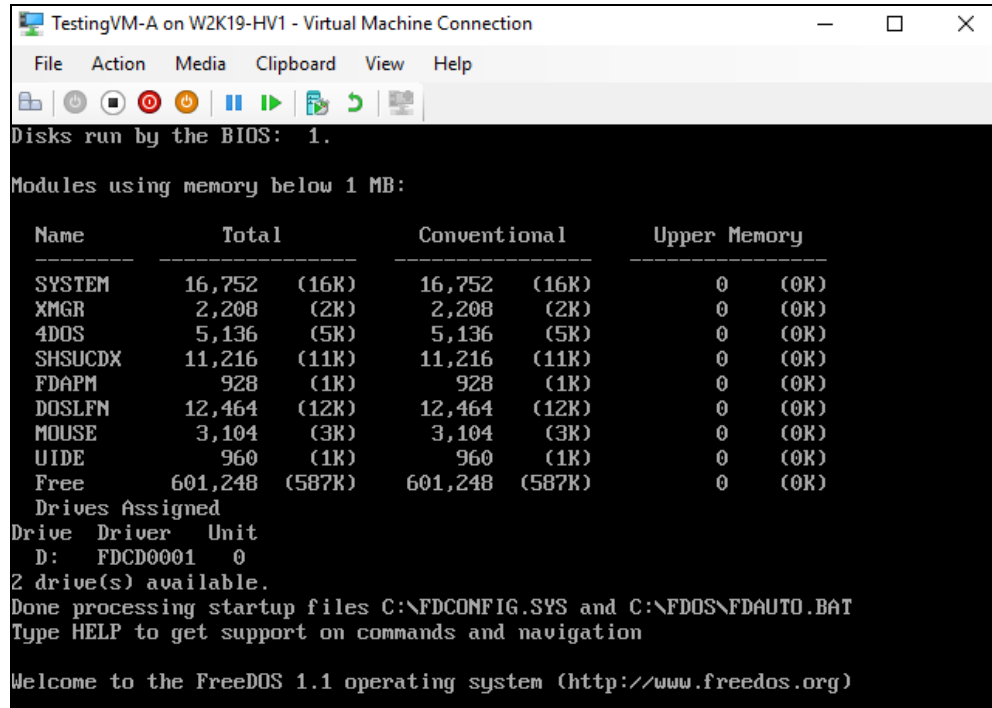


10. Go to the Hyper-V server and open the Hyper-V Manager to verify the guest VM has been restored and is powered on.



11. Connect to the guest VM to verify if is running correctly.

Example: FreeDOS

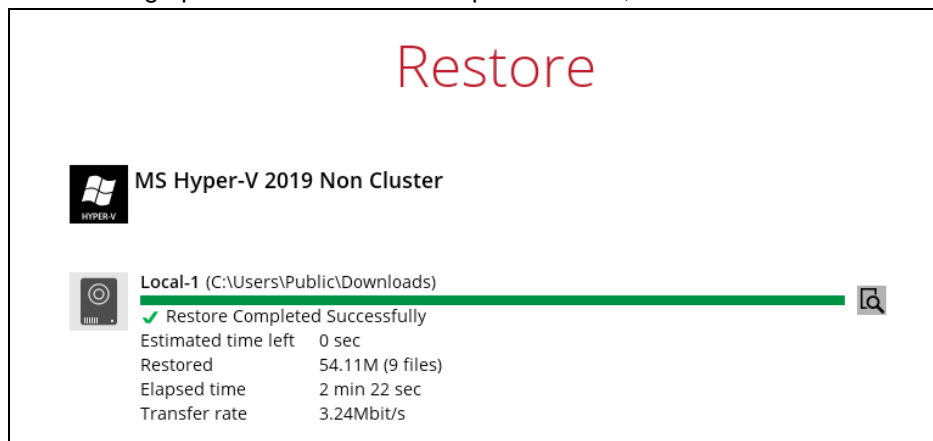


```
TestingVM-A on W2K19-HV1 - Virtual Machine Connection
File Action Media Clipboard View Help
Disks run by the BIOS: 1.
Modules using memory below 1 MB:
Name          Total          Conventional      Upper Memory
-----
SYSTEM        16,752 (16K)      16,752 (16K)      0 (0K)
XMGR           2,208 (2K)        2,208 (2K)        0 (0K)
4DOS           5,136 (5K)        5,136 (5K)        0 (0K)
SHSUCDX       11,216 (11K)      11,216 (11K)      0 (0K)
FDAPM           928 (1K)          928 (1K)          0 (0K)
DOSLFN       12,464 (12K)      12,464 (12K)      0 (0K)
MOUSE          3,104 (3K)        3,104 (3K)        0 (0K)
UIDE           960 (1K)          960 (1K)          0 (0K)
Free         601,248 (587K) 601,248 (587K)    0 (0K)
Drives Assigned
Drive Driver Unit
D: FDCD0001 0
2 drive(s) available.
Done processing startup files C:\FDCONFIG.SYS and C:\FDOS\FDAUTO.BAT
Type HELP to get support on commands and navigation
Welcome to the FreeDOS 1.1 operating system (http://www.freedos.org)
```

10.1.2 Migrate Virtual Machine (Permanently Restore)

To permanently restore the guest VM after starting up using the **Run Direct** option, you will still need to migrate it from the backup destination to the designated permanent location on the Hyper-V server using the **Migrate Virtual Machine** option. This process can be performed even when the VM is already running.

1. After starting up the VM from the backup destination, click **Close**.



2. Click on **Manage Run Direct virtual machines**.

Select Your Virtual Machines To Be Restored

Select what to restore

Choose from files as of job 01/30/2019 Latest

Folders	Name	Size	Date modified
Local-1	Snapshots		
W2K19-HV1	Virtual Hard Disks		
TestingVM-A	Virtual Machines		

☐ Restore raw file

Items per page 50 Page 1 / 1

Manage Run Direct virtual machines Previous Next Cancel Help

3. Click on the guest VM.

Select Run Direct Virtual Machine



MS Hyper-V 2019 Non Cluster
TestingVM-A

4. To permanently restore the guest VM, click on **Migrate Virtual Machine**.

Run Direct Virtual Machine

Source information

Backup set MS Hyper-V 2019 Non Cluster
Destination Local-1
Job Latest

Migration Information

W2K19-HV1
Name

Stop Run Direct Previous Migrate Virtual Machine Cancel Help

NOTE

AhsayOBM will begin migration of the guest VM from the backup destination to the Hyper-V Server.

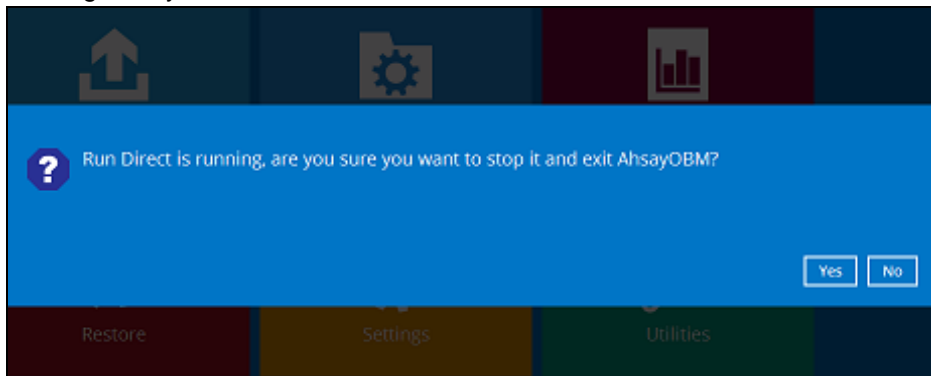
The guest VM can be used during the migration process. Any changes made in the guest VM environment is saved in transaction logs and will be applied when the migration process is completed.

When finalizing the restore, during the application of changes in transaction logs with the restored guest VM, the guest VM will be put into saved state temporarily. Once the changes have been applied, the guest VM resume.

10.1.3 Stop Run Direct Virtual Machines

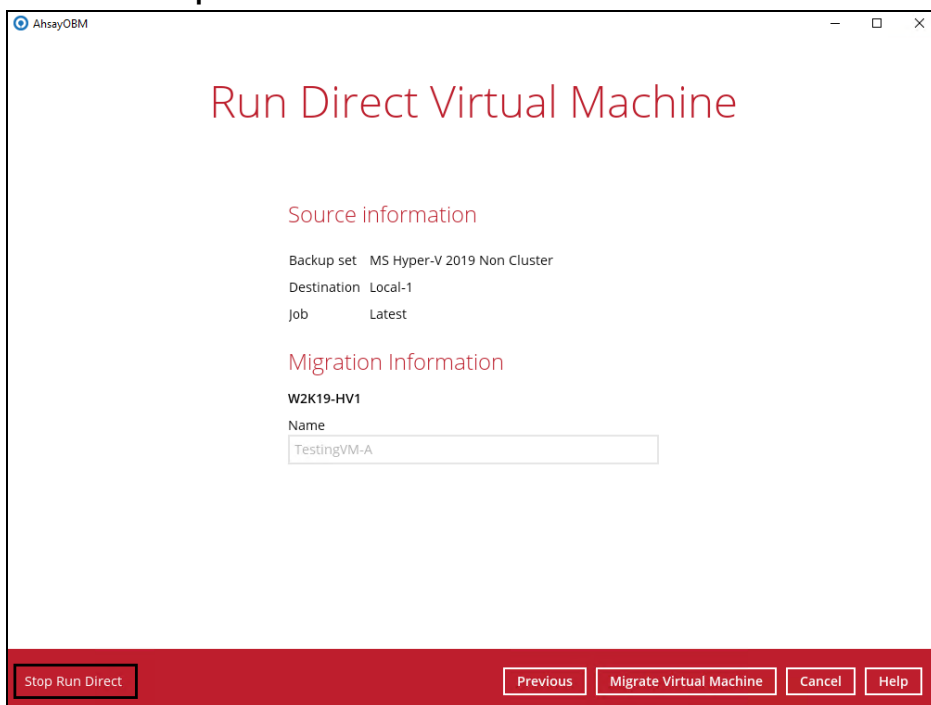
You can stop running guest VMs started up using Run Direct by either:

- Quitting AhsayOBM



-OR-

- Click on the **Stop Run Direct** button at the bottom left corner.



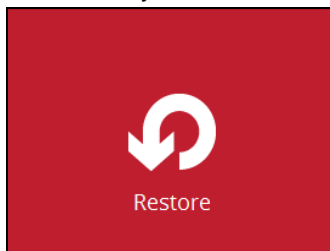
NOTES

1. When the Auto Migrate option is selected, there will be no Stop Run Direct option available. As once the auto migration is completed, the guest VM will have been fully restored to the Hyper-V Host and will be running and managed under the Hyper-V Host environment. Therefore, the Run Direct VM instance will no longer exist as a result.
2. The "Stop Run Direct" link only present if you run a Run Direct restore without auto migrate selected.
3. When a guest VM started in a Run Direct instance is stopped, any changes made within the guest environment will be lost, if the guest VM is not migrated to the Hyper-V Server using the "Auto migrate after Run Direct is running" option.

10.1.4 Start up a guest VM from Backup Destination with Auto Migration Enabled

Follow the steps below to start up the guest VM directly from the backup files.

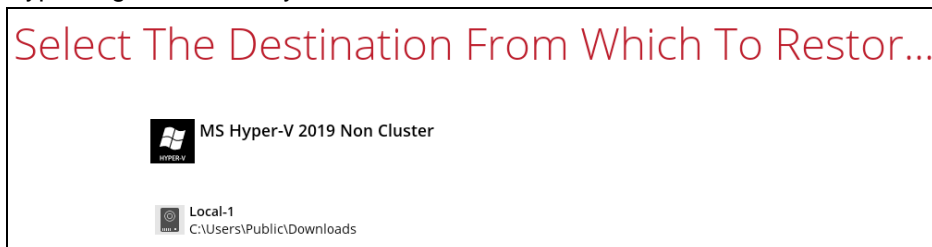
1. In the AhsayOBM main interface, click the **Restore** icon.



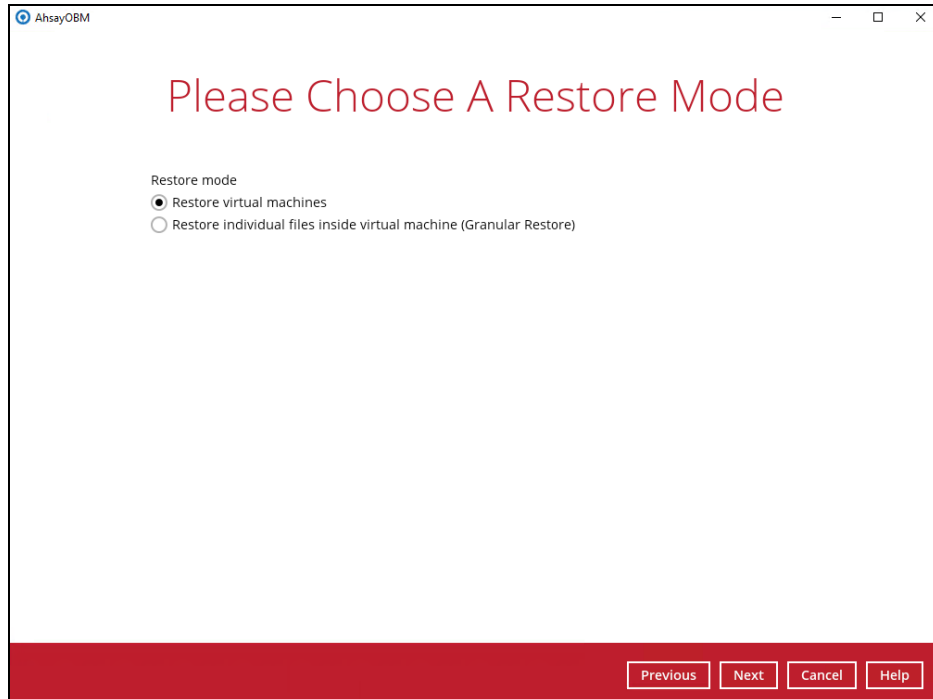
2. Select the backup set that you would like to restore the guest VM from.



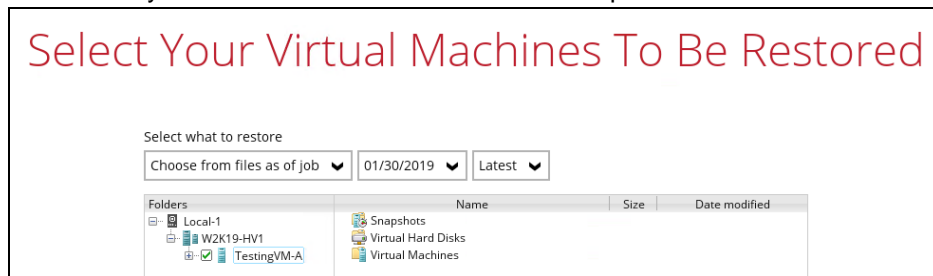
3. Select the local, mapped drive, or removable drive storage destination that contains Hyper-V guest VM that you would like to restore.



4. Select **Restore virtual machines** as the restore mode.

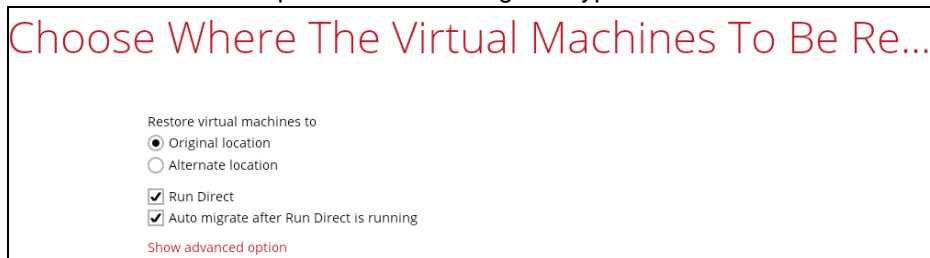


5. Select to restore the Hyper-V guest from a specific backup job then select the files or folders that you would like to restore. Click **Next** to proceed.



6. Select to restore the Hyper-V guest VM to the **Original location**, or to an **Alternate location**. Then select **Run Direct** and **Auto migrate after Run Direct is running** and click **Next** to proceed.

- ⦿ **Original location** – The Hyper-V guest VM will be restored to the same directory path which stores the backup source on the original Hyper-V host.



- **Alternate location** – The Hyper-V guest VM will be restored to the different directory path on the original Hyper-V host.

Choose Where The Virtual Machines To Be Re...

Restore virtual machines to

☐ Original location

☒ Alternate location

☒ Run Direct

☒ Auto migrate after Run Direct is running

Show advanced option

Click **Next** to proceed and the following values must be updated:

- Virtual Machine Name**
- Virtual Machines Directory Location** (guest configuration files)
- Virtual Hard Disk Location** (new location for the guest VHD files)

Example:

- Rename the restored guest VM to “**TestingVM-A_2**”
- Store the configuration files in the new location
“**C:\ClusterStorage\Volume1\VM\TestingVM-A\TestingVM-A_2**”
- Store the VHD files in the new location
“**C:\ClusterStorage\Volume1\VM\TestingVM-A\TestingVM-A_2**”

Alternate location

Virtual Machine Name

TestingVM-A_2

Virtual Machines Directory Location

C:\ClusterStorage\Volume1\VM\TestingVM-A\TestingVM-A_2 Browse

Virtual Hard Disk Location

C:\ClusterStorage\Volume1\VM\TestingVM-A\TestingVM-A_2 Browse

When the values have been updated click on **Next** to proceed.

- Confirm the temporary directory path is correct and then click **Restore** to proceed.

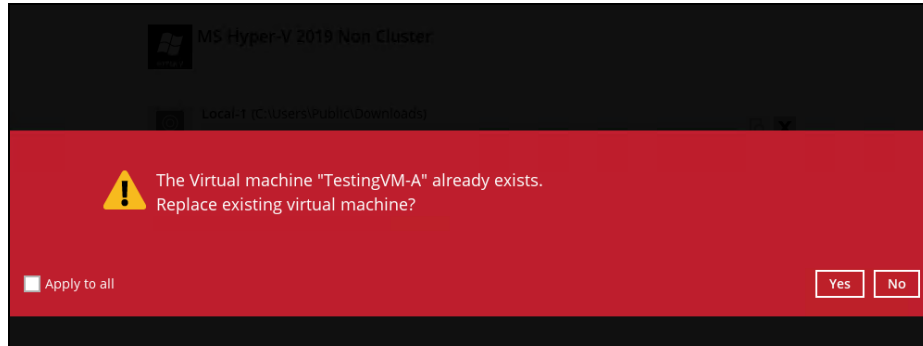
Temporary Directory

Temporary directory for storing restore files

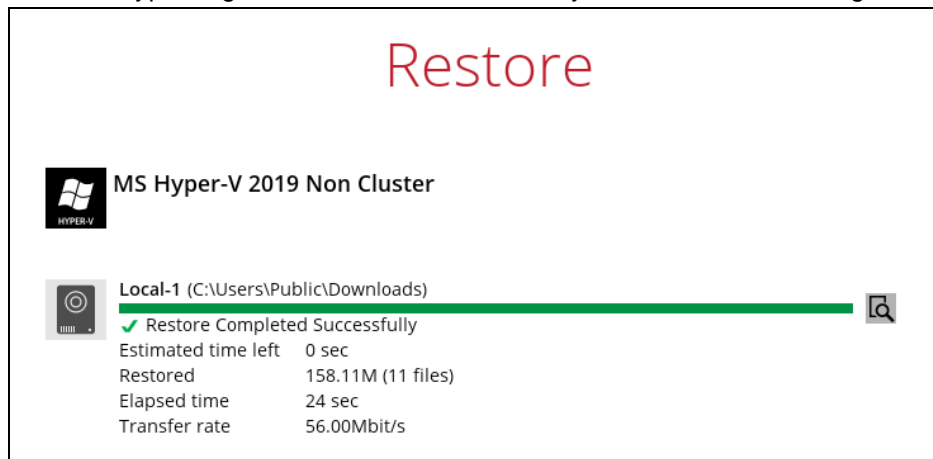
C:\Users\Administrator\obm\temp Browse

- If the guest VM selected to be restored already exists on the Hyper-V server AhsayOBM will prompt to confirm overwriting of the existing guest.
- **Yes** - the existing guest VM will be deleted from the Hyper-V server before the restore process starts.

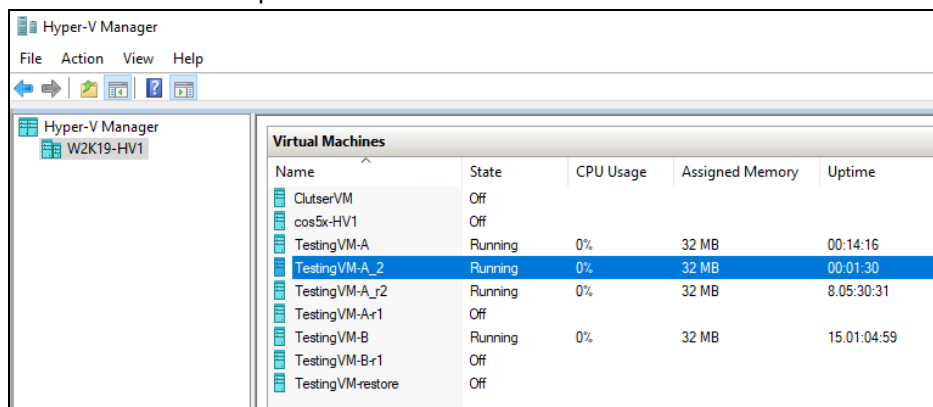
- **No** – the restore of the current guest VM will be skipped.



9. After the Hyper-V guest VM has been restored, you will see the following screen.

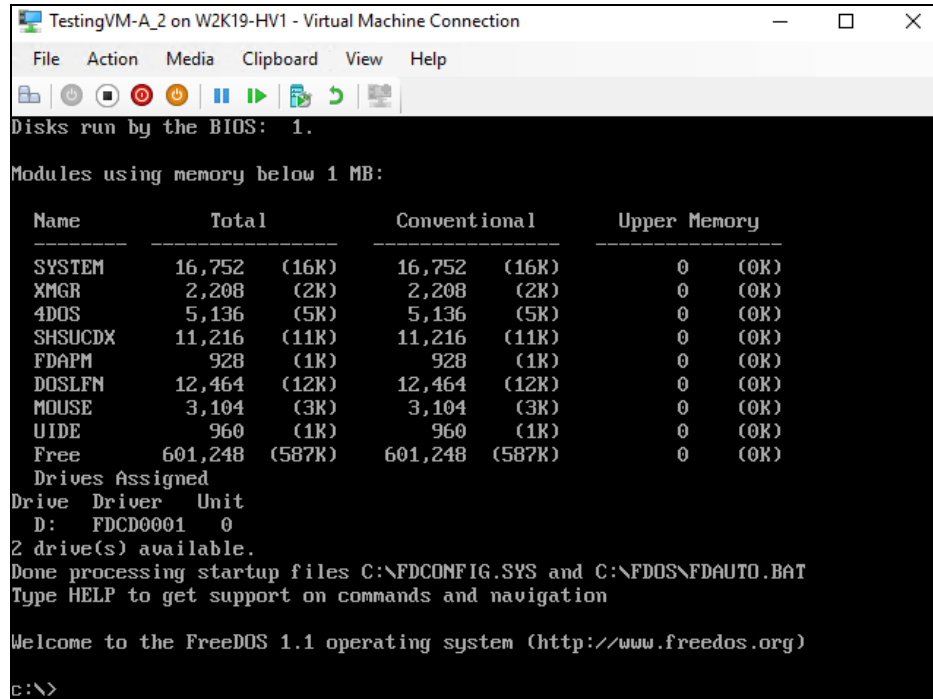


10. Go to the Hyper-V server and open the Hyper-V Manager to verify the guest has been restored and is powered on.



11. Connect to the guest VM to verify if it is running correctly.

Example: FreeDOS



```
TestingVM-A_2 on W2K19-HV1 - Virtual Machine Connection
File Action Media Clipboard View Help
Disks run by the BIOS: 1.
Modules using memory below 1 MB:
Name          Total          Conventional      Upper Memory
-----
SYSTEM        16,752 (16K)      16,752 (16K)        0 (0K)
XMGR           2,208 (2K)        2,208 (2K)          0 (0K)
4DOS           5,136 (5K)        5,136 (5K)          0 (0K)
SHSUCDX        11,216 (11K)      11,216 (11K)        0 (0K)
FDAPM           928 (1K)          928 (1K)            0 (0K)
DOSLFN         12,464 (12K)      12,464 (12K)        0 (0K)
MOUSE          3,104 (3K)        3,104 (3K)          0 (0K)
UIDE           960 (1K)          960 (1K)            0 (0K)
Free          601,248 (587K)  601,248 (587K)      0 (0K)
Drives Assigned
Drive Driver Unit
D:  FDCD0001  0
2 drive(s) available.
Done processing startup files C:\FDCONFIG.SYS and C:\FDOS\FDAUTO.BAT
Type HELP to get support on commands and navigation

Welcome to the FreeDOS 1.1 operating system (http://www.freedos.org)

c:\>
```

10.2 Different (Standby) Hyper-V Host

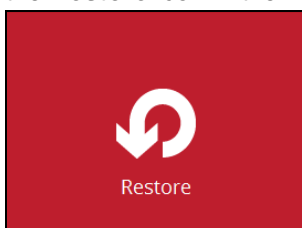
This restore option allows you to restore your backed up guest VM to another Hyper-V host, for example if your original Hyper-V host is down and you need to restore your production guest VM's to a standby Hyper-V host.

Please refer to the [Ch. 2.17.4 For Restore to a Different \(Standby\) Hyper-V Host](#) for the details about requirements and limitations for restoring Hyper-V guest VM to another Hyper-V host.

10.2.1 Start up a guest VM from Backup Destination without Auto Migration Enabled

Follow the steps below to start up the guest VM directly from the backup files.

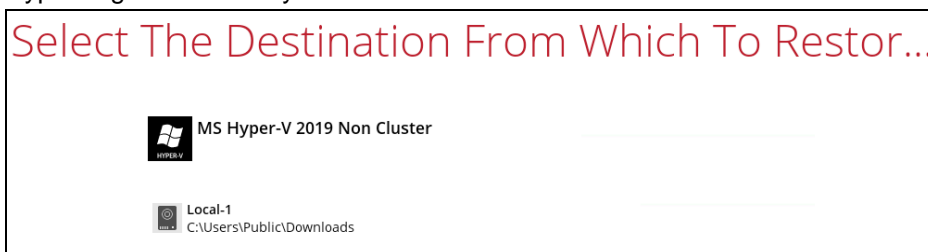
1. On the machine you wish to restore Hyper-V guest VM, launch AhsayOBM and click the **Restore** icon in the main interface.



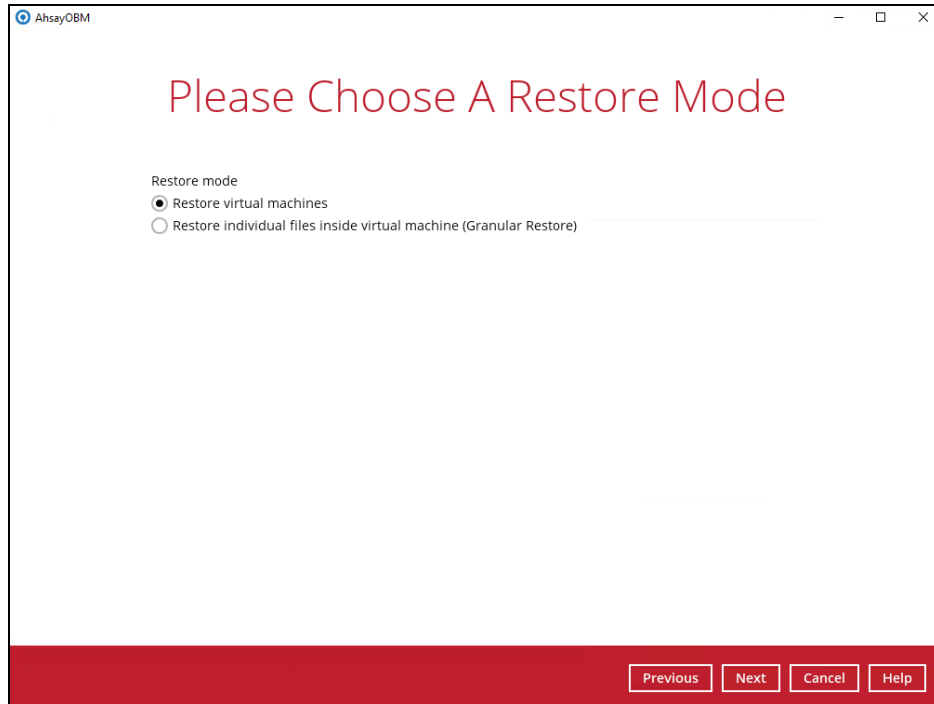
2. Select the backup set that you would like to restore the guest VM from.



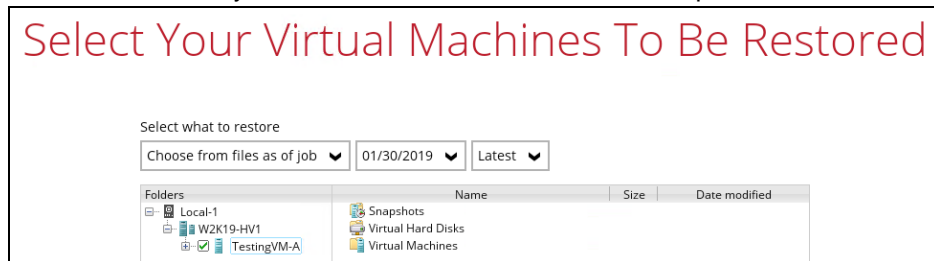
3. Select the local, mapped drive, or removable drive storage destination that contains Hyper-V guest VM that you would like to restore.



4. Select **Restore virtual machines** as the restore mode.

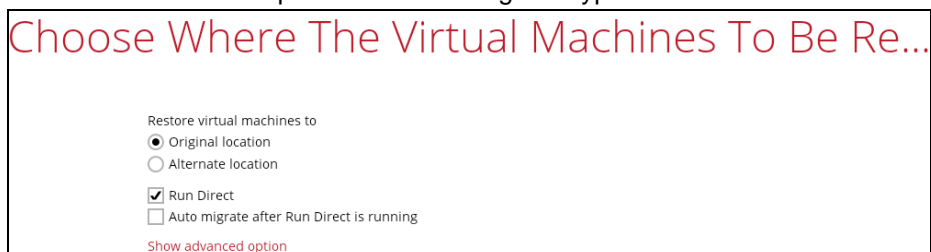


5. Select to restore the Hyper-V guest VM from a specific backup job then select the files or folders that you would like to restore. Click **Next** to proceed.



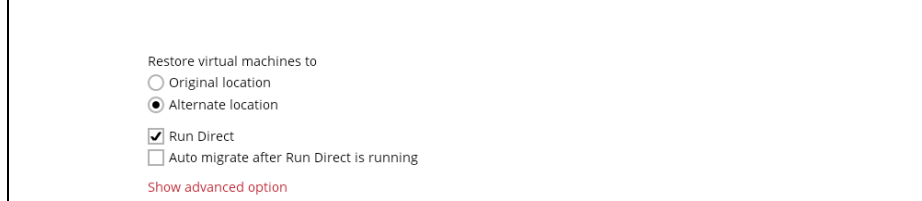
6. Select to restore the Hyper-V guest VM to the **Original location**, or to an **Alternate location**. Then select **Run Direct** and click **Next** to proceed.

- ⦿ **Original location** – The Hyper-V guest VM will be restored to the same directory path which stores the backup source on the original Hyper-V host.



- **Alternate location** - The Hyper-V guest VM will be restored to the different directory path on the original Hyper-V host.

Choose Where The Virtual Machines To Be Re...



Restore virtual machines to

☐ Original location

☒ Alternate location

☒ Run Direct

☐ Auto migrate after Run Direct is running

[Show advanced option](#)

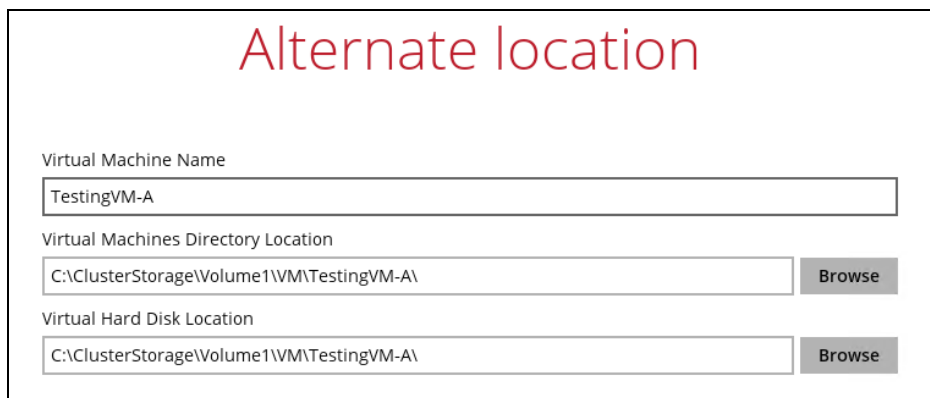
NOTE: For restore to an alternate Hyper-V Host with a different CPU architecture, the latest version of AhsayOBM client application must be installed.

Click **Next** to proceed and the following values are needed to update:

- Virtual Machine Name**
- Virtual Machines Directory Location** (guest configuration files)
- Virtual Hard Disk Location** (new location for the guest VHD files)

Example:

- Rename the restored guest VM to "**TestingVM-A**"
- Store the configuration files in the new location
"**C:\ClusterStorage\Volume1\VM\TestingVM-A**"
- Store the VHD files in the new location
"**C:\ClusterStorage\Volume1\VM\TestingVM-A**"



Alternate location

Virtual Machine Name

TestingVM-A

Virtual Machines Directory Location

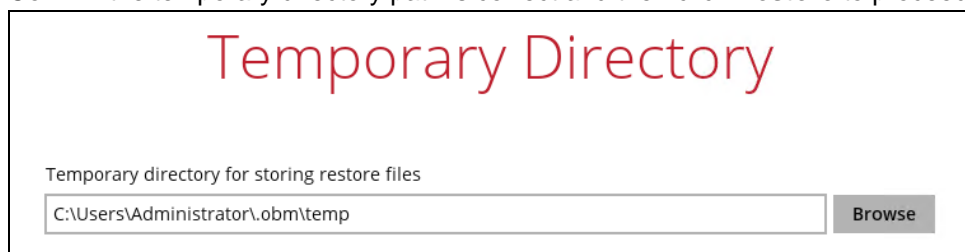
C:\ClusterStorage\Volume1\VM\TestingVM-A\ [Browse](#)

Virtual Hard Disk Location

C:\ClusterStorage\Volume1\VM\TestingVM-A\ [Browse](#)

When the values have been updated click on **Next** to proceed.

- Confirm the temporary directory path is correct and then click **Restore** to proceed.

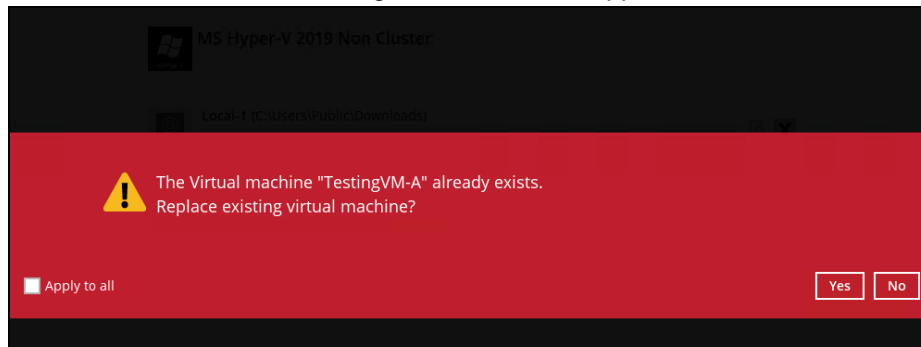


Temporary Directory

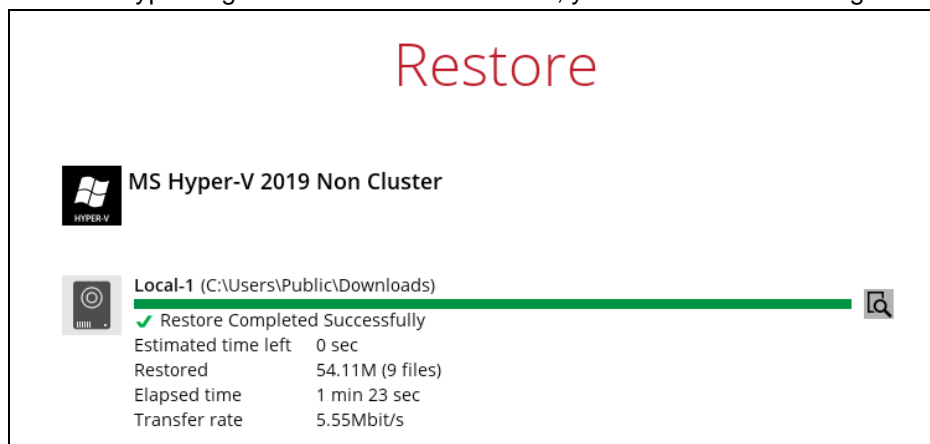
Temporary directory for storing restore files

C:\Users\Administrator\.obm\temp [Browse](#)

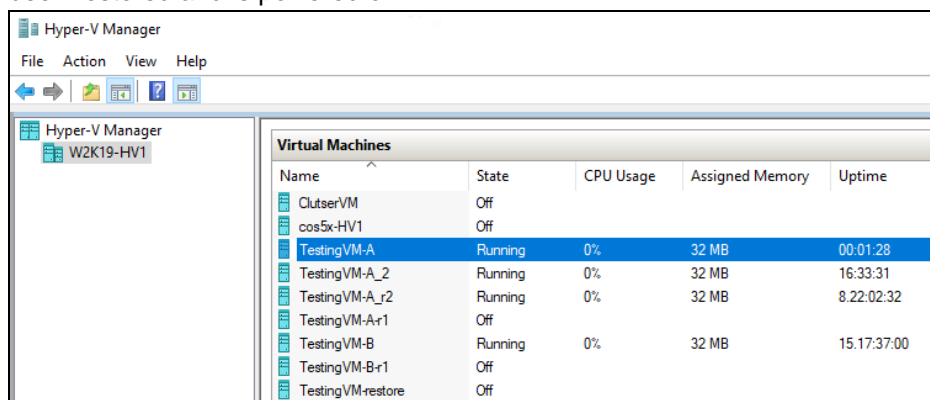
8. If the guest VM selected to be restored already exists on the Hyper-V server, AhsayOBM will prompt to confirm overwriting of the existing guest.
 - ⦿ **Yes** - the existing guest VM will be deleted from the Hyper-V server before the restore process starts.
 - ⦿ **No** – the restore of the current guest VM will be skipped.



9. After the Hyper-V guest VM has been restored, you will see the following screen.

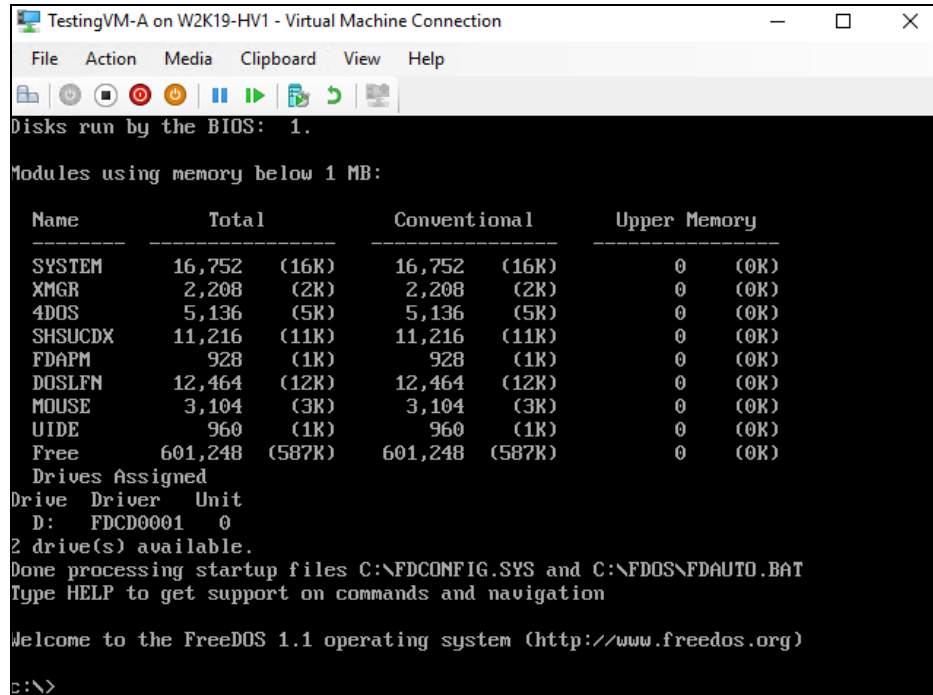


10. Go to the Hyper-V server and open the Hyper-V Manager to verify the guest VM has been restored and is powered on.



11. Connect to the guest VM to verify if is running correctly.

Example: FreeDOS

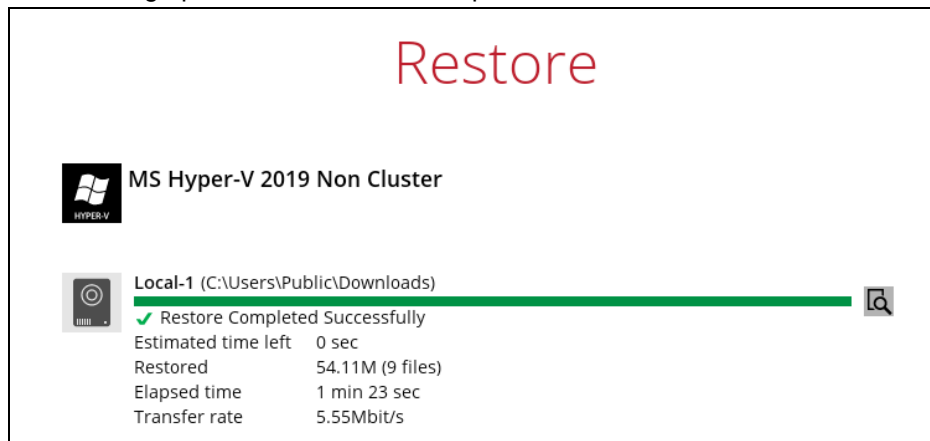


```
TestingVM-A on W2K19-HV1 - Virtual Machine Connection
File Action Media Clipboard View Help
Disks run by the BIOS: 1.
Modules using memory below 1 MB:
Name          Total          Conventional    Upper Memory
-----
SYSTEM        16,752 (16K)    16,752 (16K)    0 (0K)
XMGR           2,208 (2K)     2,208 (2K)     0 (0K)
4DOS           5,136 (5K)     5,136 (5K)     0 (0K)
SHSUCDX        11,216 (11K)    11,216 (11K)    0 (0K)
FDAPM           928 (1K)       928 (1K)       0 (0K)
DOSLFN        12,464 (12K)    12,464 (12K)    0 (0K)
MOUSE          3,104 (3K)     3,104 (3K)     0 (0K)
UIDE           960 (1K)       960 (1K)       0 (0K)
Free          601,248 (587K) 601,248 (587K) 0 (0K)
Drives Assigned
Drive Driver Unit
D: FDCD0001 0
2 drive(s) available.
Done processing startup files C:\FDCONFIG.SYS and C:\FDOS\FDAUTO.BAT
Type HELP to get support on commands and navigation
Welcome to the FreeDOS 1.1 operating system (http://www.freedos.org)
C:\>
```

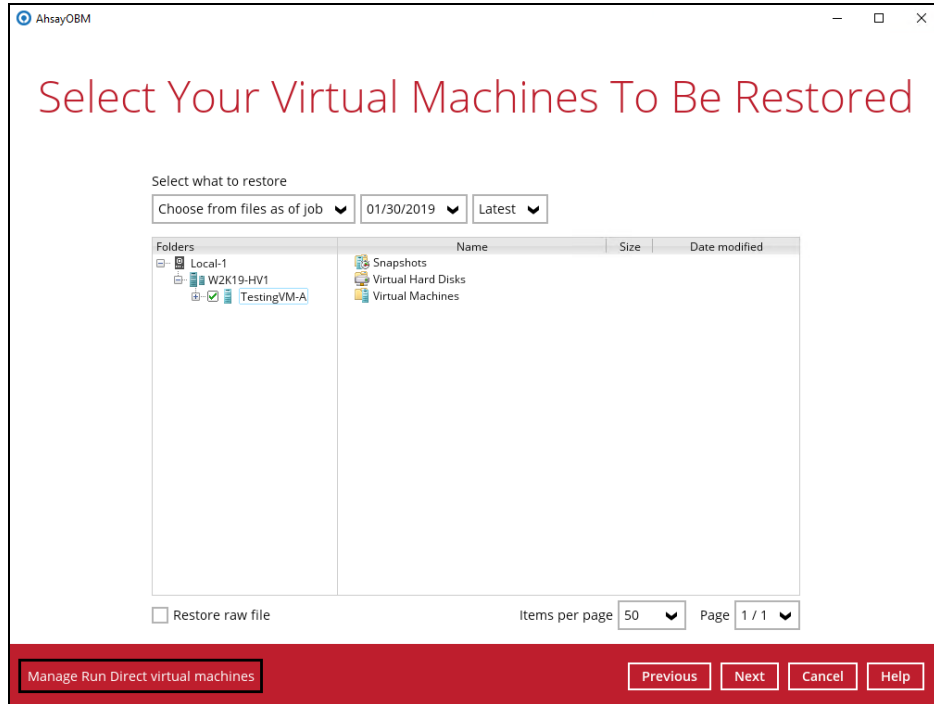
10.2.2 Migrate Virtual Machine (Permanently Restore)

To permanently restore the guest VM after starting up using the **Run Direct** option, you will still need to migrate it to from the backup destination to the designated permanent location on the Hyper-V server using the **Migrate Virtual Machine** option. This process can be performed even when the VM is already running.

1. After starting up the VM from the backup destination, click **Close**.



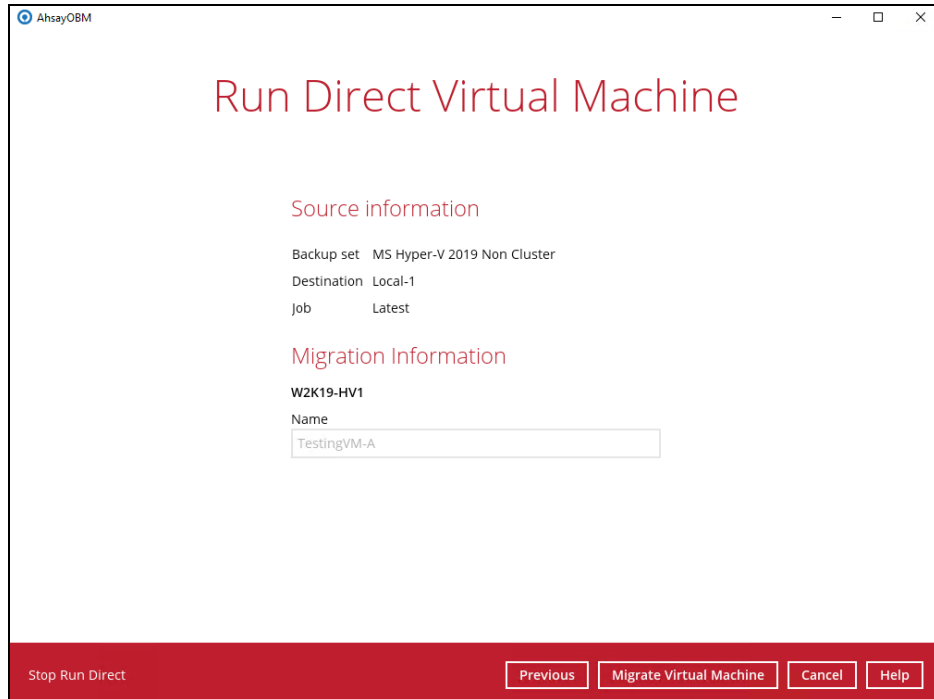
2. Click on **Manage Run Direct virtual machines**.



3. Click on the guest VM.



4. To permanently restore the guest VM, click on **Migrate Virtual Machine**.



The screenshot shows a window titled 'AhsayOBM' with the main heading 'Run Direct Virtual Machine' in red. Below this, there are two sections: 'Source information' and 'Migration Information'. The 'Source information' section displays 'Backup set: MS Hyper-V 2019 Non Cluster', 'Destination: Local-1', and 'Job: Latest'. The 'Migration Information' section shows 'W2K19-HV1' and a 'Name' field containing 'TestingVM-A'. At the bottom, there is a red bar with a 'Stop Run Direct' link on the left and four buttons: 'Previous', 'Migrate Virtual Machine', 'Cancel', and 'Help'.

NOTE

AhsayOBM will begin migration of the guest VM from the backup destination to the Hyper-V Server.

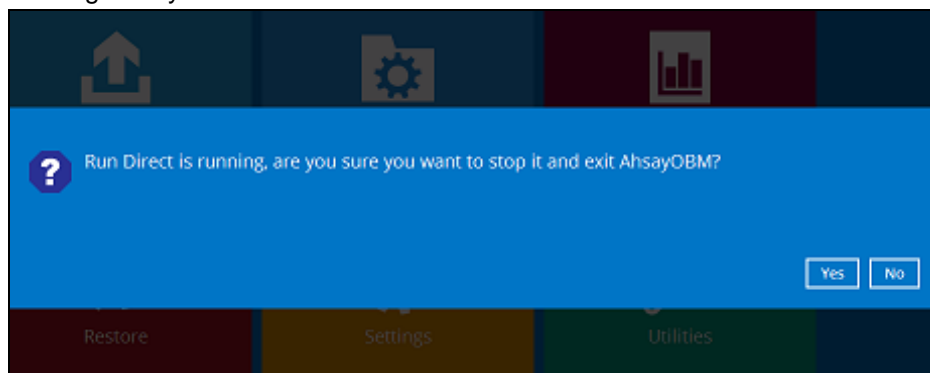
The guest VM can be used during the migration process. Any changes made in the guest VM environment is saved in transaction logs and will be applied when the migration process is completed.

When finalizing the restore, during the application of changes in transaction logs with the restored guest VM, the guest VM will be put into saved state temporarily. Once the changes have been applied, the guest VM will resume.

10.2.3 Stop Run Direct Virtual Machines

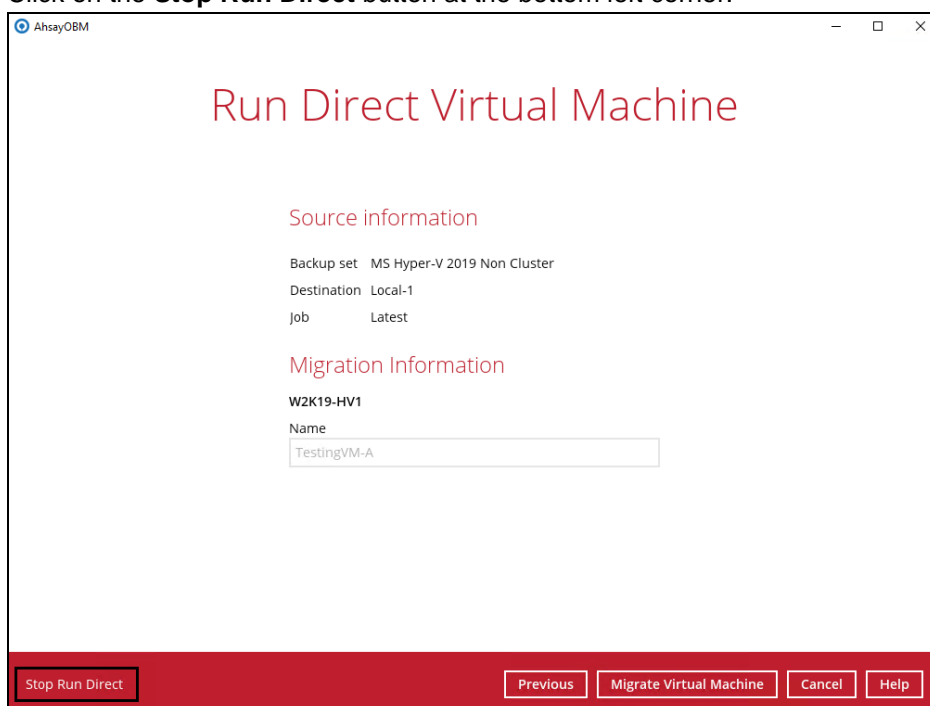
You can stop running guest VMs started up using Run Direct by either:

- ❶ Quitting AhsayOBM



-OR-

- ❷ Click on the **Stop Run Direct** button at the bottom left corner.



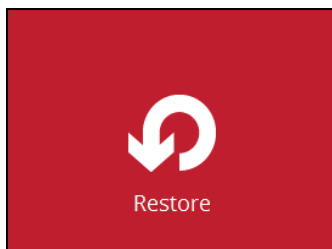
NOTES

1. When the Auto Migrate option is selected, there will be no Stop Run Direct option available. As once the auto migration is completed, the guest VM will have been fully restored to the Hyper-V Host and will be running and managed under the Hyper-V Host environment. Therefore, the Run Direct VM instance will no longer exist as a result.
2. The "Stop Run Direct" link only present if you run a Run Direct restore without auto migrate selected.
3. When a guest VM started in a Run Direct instance is stopped, any changes made within the guest environment will be lost, if the guest VM is not migrated to the Hyper-V Server using the "Auto migrate after Run Direct is running" option.

10.2.4 Start up a guest VM from Backup Destination with Auto Migration Enabled

Follow the steps below to start up the guest VM directly from the backup files.

1. On the machine you wish to restore Hyper-V guest VM, launch AhsayOBM and click the **Restore** icon in the main interface.



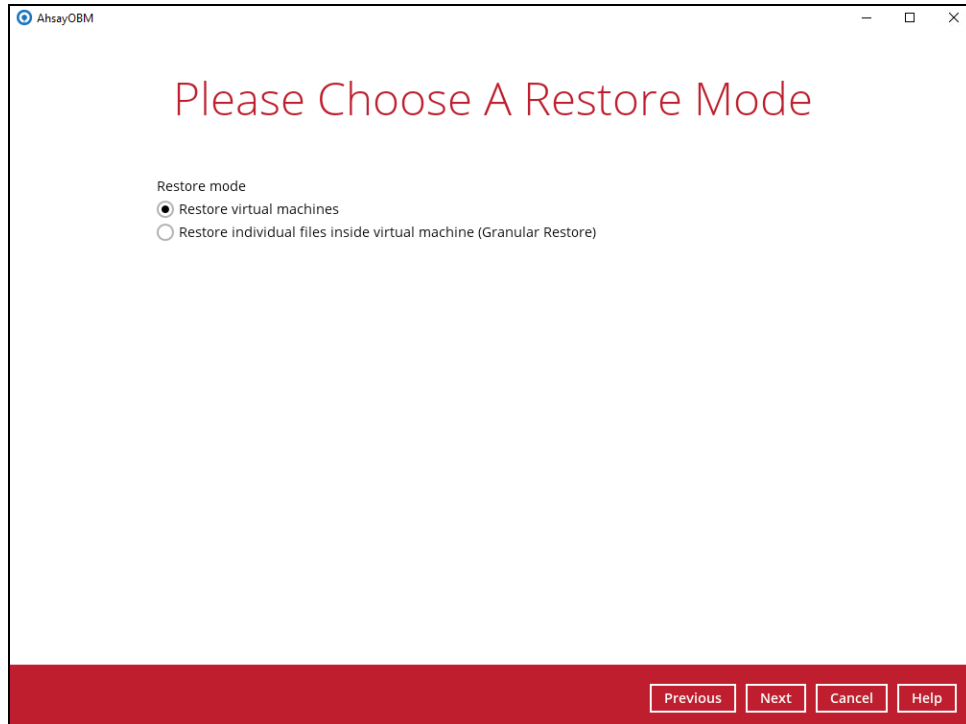
2. Select the backup set that you would like to restore the guest VM from.



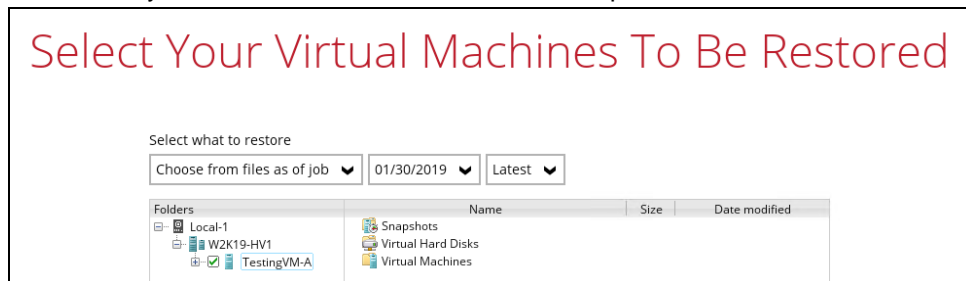
3. Select the local, mapped drive, or removable drive storage destination that contains Hyper-V guest VM that you would like to restore.



4. Select **Restore virtual machines** as the restore mode.



5. Select to restore the Hyper-V guest from a specific backup job then select the files or folders that you would like to restore. Click **Next** to proceed.



6. Select to restore the Hyper-V guest VM to the **Original location**, or to an **Alternate location**. Then select **Run Direct** and **Auto migrate after Run Direct is running** and click **Next** to proceed.

- ⦿ **Original location** – The Hyper-V guest VM will be restored to the same directory path which stores the backup source on the original Hyper-V host.



- **Alternate location** – The Hyper-V guest VM will be restored to a different directory path on the original Hyper-V host.

Choose Where The Virtual Machines To Be Re...

Restore virtual machines to

☐ Original location

☒ Alternate location

☒ Run Direct

☒ Auto migrate after Run Direct is running

[Show advanced option](#)

Click **Next** to proceed and the following values are needed to be update:

- Virtual Machine Name**
- Virtual Machines Directory Location** (guest configuration files)
- Virtual Hard Disk Location** (new location for the guest VHD files)

Example:

- Rename the restored guest VM to “**TestingVM-A-1**”
- Store the configuration files in the new location
“**C:\ClusterStorage\Volume1\VM\TestingVM-A-1**”
- Store the VHD files in the new location
“**C:\ClusterStorage\Volume1\VM\TestingVM-A-1**”

Alternate location

Virtual Machine Name

TestingVM-A-1

Virtual Machines Directory Location

C:\ClusterStorage\Volume1\VM\TestingVM-A-1

Virtual Hard Disk Location

C:\ClusterStorage\Volume1\VM\TestingVM-A-1

When the values have been updated click on **Next** to proceed.

7. Confirm the temporary directory path is correct and then click **Restore** to proceed.

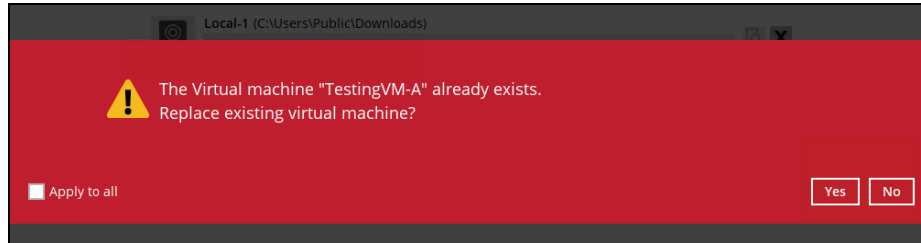
Temporary Directory

Temporary directory for storing restore files

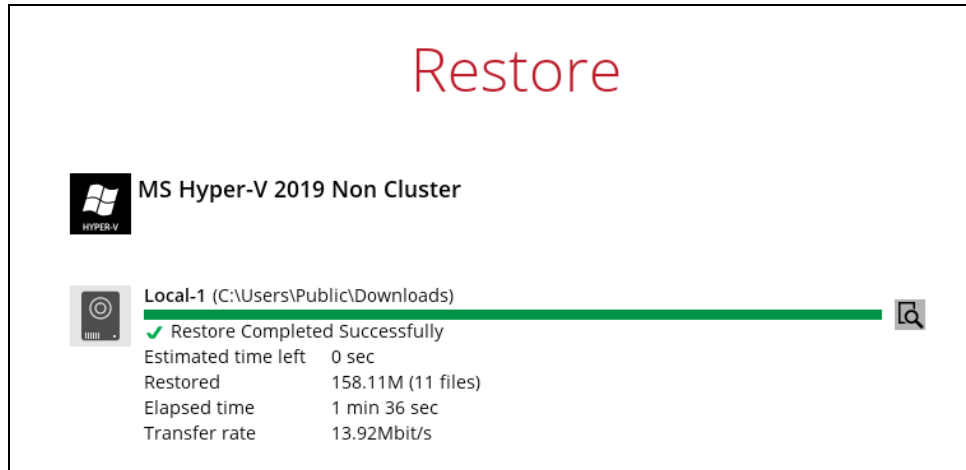
C:\Users\Administrator\obm\temp

8. If the guest VM selected to be restored already exists on the Hyper-V server AhsayOBM will prompt to confirm overwriting of the existing guest.
- **Yes** - the existing guest VM will be deleted from the Hyper-V server before the restore process starts.

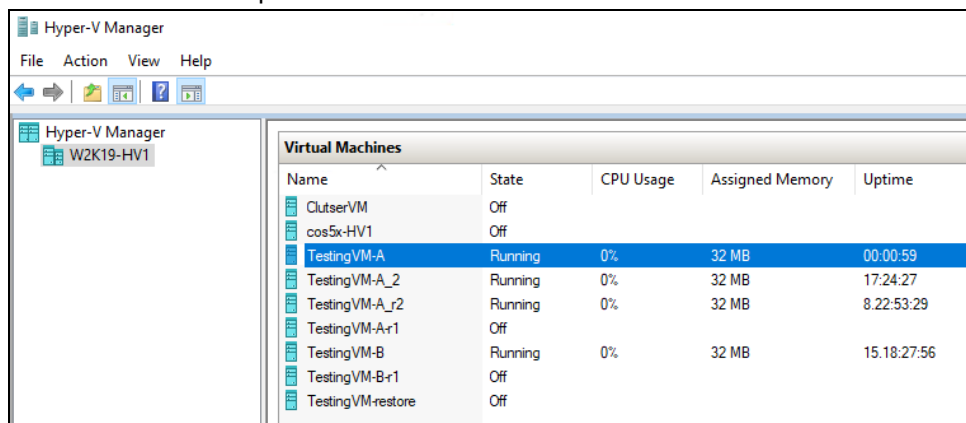
- **No** – the restore of the current guest VM will be skipped.



9. After the Hyper-V guest VM has been restored, you will see the following screen.



10. Go to the Hyper-V server and open the Hyper-V Manager to verify the guest has been restored and is powered on.



11. Connect to the guest VM to verify if it is running correctly.

Example: FreeDOS

```
TestingVM-A on W2K19-HV1 - Virtual Machine Connection
File Action Media Clipboard View Help
Disks run by the BIOS: 1.
Modules using memory below 1 MB:
Name          Total          Conventional      Upper Memory
-----
SYSTEM        16,752 (16K)      16,752 (16K)        0 (0K)
XMGR           2,208 (2K)        2,208 (2K)          0 (0K)
4DOS           5,136 (5K)        5,136 (5K)          0 (0K)
SHSUCDX        11,216 (11K)      11,216 (11K)        0 (0K)
FDAPM           928 (1K)          928 (1K)            0 (0K)
DOSLFN         12,464 (12K)      12,464 (12K)        0 (0K)
MOUSE          3,104 (3K)        3,104 (3K)          0 (0K)
UIDE            960 (1K)          960 (1K)            0 (0K)
Free          601,248 (587K)    601,248 (587K)      0 (0K)
Drives Assigned
Drive Driver Unit
D:  FDCD0001  0
2 drive(s) available.
Done processing startup files C:\FDCONFIG.SYS and C:\FDOS\FDAUTO.BAT
Type HELP to get support on commands and navigation

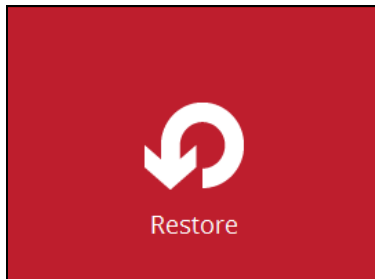
Welcome to the FreeDOS 1.1 operating system (http://www.freedos.org)
c:\>
```

11 Non-Run Direct Restore

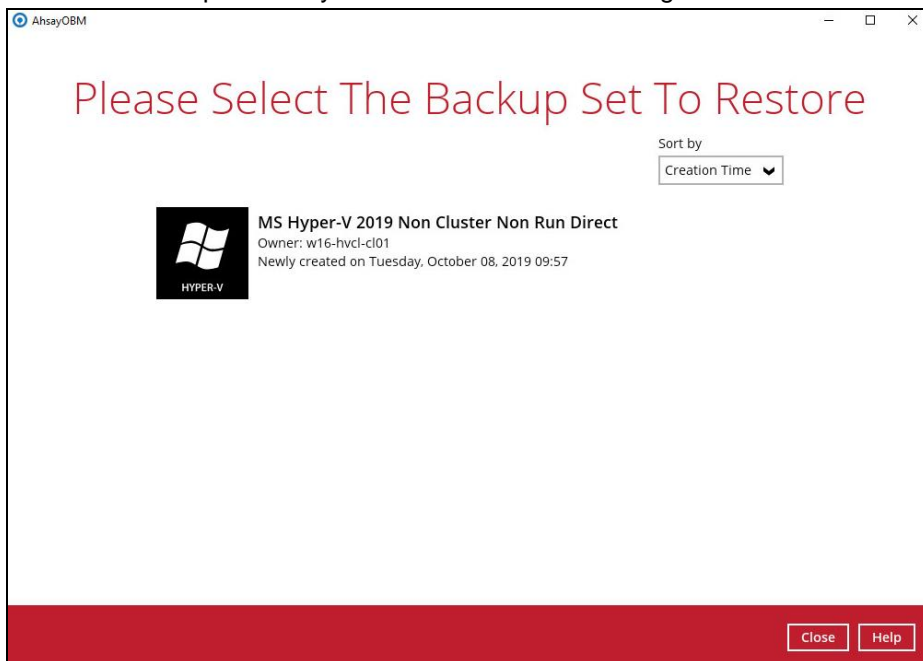
11.1 Original Hyper-V Host

11.1.1 Restore of Guest VM to the Original Hyper-V Host (Original Location)

1. In the AhsayOBM main interface, click the **Restore** icon.



2. Select the backup set that you would like to restore the guest VM from.

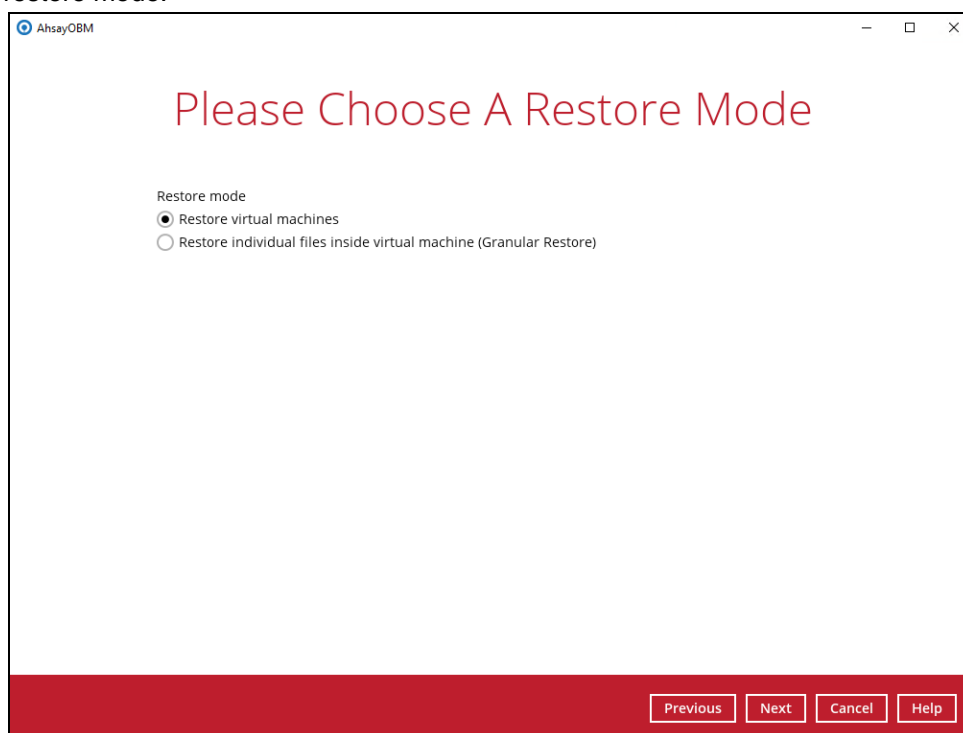


3. Select the CBS, cloud, SFTP/FTP or drive storage destination that contains Hyper-V guest VM that you would like to restore.

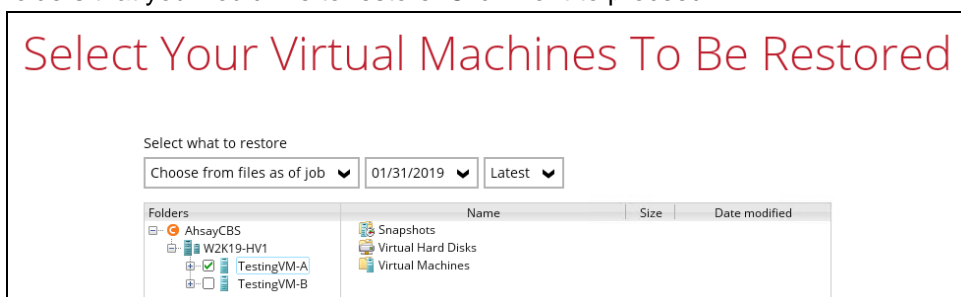
Example: Restore from AhsayCBS



4. If the backup set is created with **Run Direct** feature or **Granular Restore** feature enabled, the following step will show. Select **Restore virtual machines** as the restore mode.



5. Select to restore the Hyper-V guest from a specific backup job then select the files or folders that you would like to restore. Click **Next** to proceed.



6. Select to restore the Hyper-V guest VM to the **Original location**.

- ☒ For backup set without Run Direct feature enabled:



- For the backup set with Run Direct feature enabled, uncheck the box beside Run Direct and then click **Next** to proceed.

Choose Where The Virtual Machines To Be Re...

Restore virtual machines to

☒ Original location

☐ Alternate location

☐ Run Direct

[Show advanced option](#)

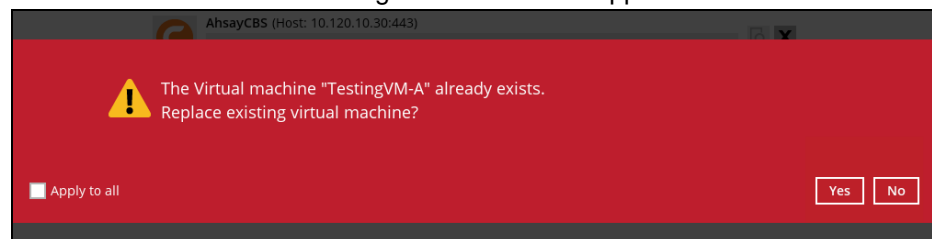
- Confirm the temporary directory path is correct and then click **Restore** to proceed.

Temporary Directory

Temporary directory for storing restore files

- If the guest VM selected to be restored already exists on the Hyper-V server AhsayOBM will prompt to confirm overwriting of the existing guest.

- Yes** - the existing guest VM will be deleted from the Hyper-V server before the restore process starts.
- No** – the restore of the current guest VM will be skipped.



- After the Hyper-V guest VM has been restored.

Restore

MS Hyper-V 2019 Non Cluster Non Run Direct

AhsayCBS (Host: 10.120.10.30:443)

✓ Restore Completed Successfully

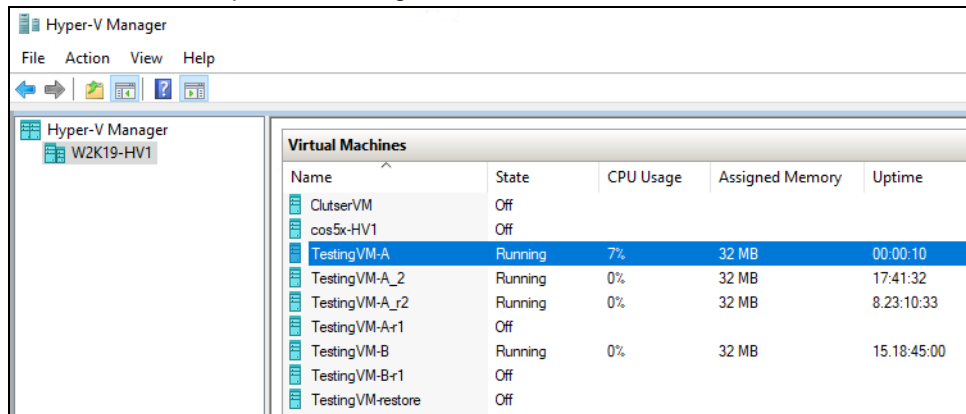
Estimated time left 0 sec

Restored 148.30M (11 files)

Elapsed time 1 min 12 sec

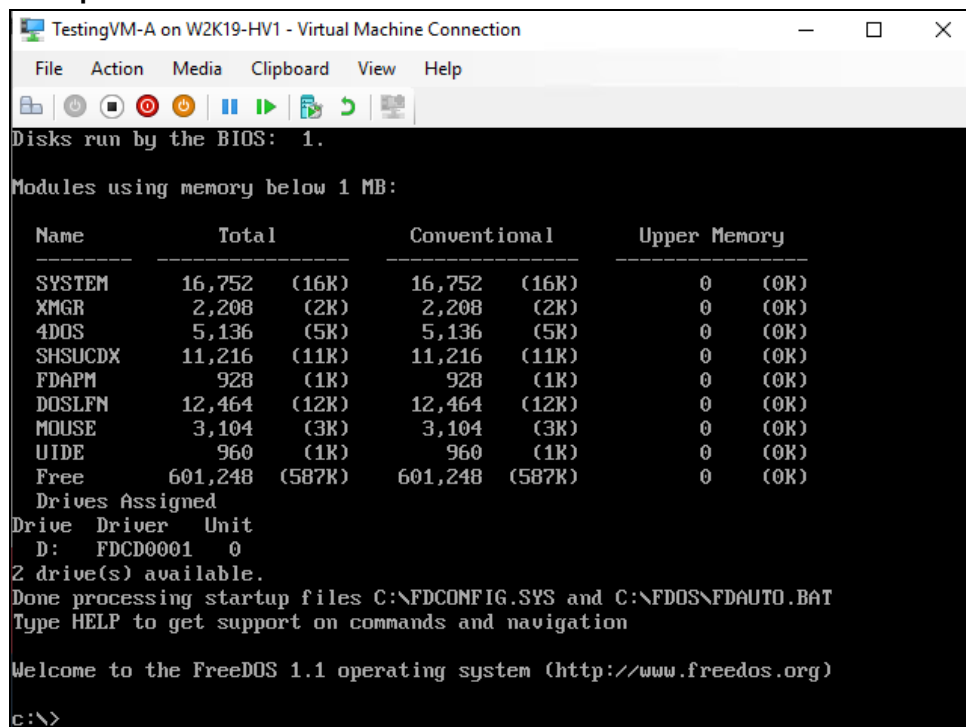
Transfer rate 17.49Mbit/s

10. Go to the Hyper-V server and open the Hyper-V Manager to verify the guest has been restored and power on the guest VM.



11. Connect to the guest VM to verify if it is running correctly.

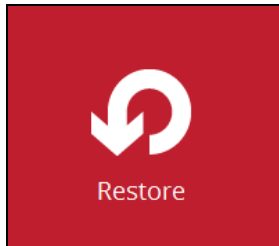
Example: FreeDOS



11.1.2 Restore of Guest VM to the Original Hyper-V Host (Alternate Location)

This feature will restore any guest VM to another location (a different disk or folder) on the same Hyper-V host. The Restore to Alternate location can be used to restore only one guest VM at any one time.

1. In the AhsayOBM main interface, click the **Restore** icon.



2. Select the backup set that you would like to restore the guest VM from.



3. Select the CBS, cloud, SFTP/FTP or drive storage destination that contains Hyper-V guest VM that you would like to restore.

Example: Restore from F:\ drive

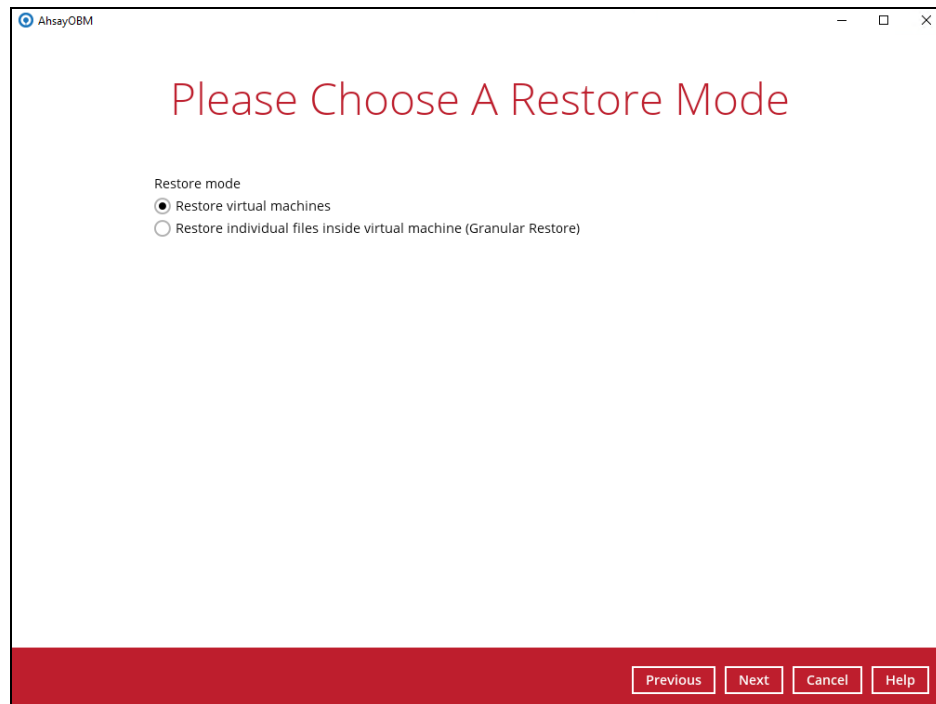


Example: Restore from AhsayCBS

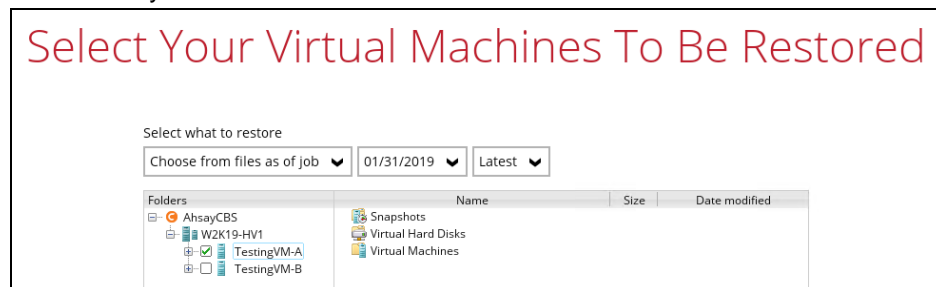


4. If the backup set is created with **Run Direct** feature or **Granular Restore** feature enabled, the following step will show. Select **Restore virtual machines** as the

restore mode.



5. Select to restore the Hyper-V guest from a specific backup job then select the files or folders that you would like to restore.

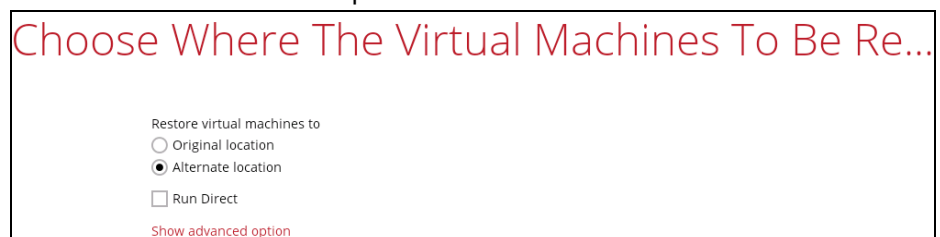


6. Select to restore the Hyper-V guest VM to the **Alternate location**.

- For backup set without Run Direct feature enabled:



- For the backup set with Run Direct feature enabled, uncheck the box of Run Direct and then click **Next** to proceed.



Click **Next** to proceed and the following values are needed to be updated:

- i. **Virtual Machine Name**
- ii. **Virtual Machines Directory Location** (guest configuration files)
- iii. **Virtual Hard Disk Location** (new location for the guest VHD files)

Example:

- i. Rename the restored guest VM to “**TestingVM-A-1**”
- ii. Store the configuration files in the new location
“**C:\ClusterStorage\Volume1\VM\TestingVM-A-1**”
- iii. Store the VHD files in the new location
“**C:\ClusterStorage\Volume1\VM\TestingVM-A-1**”

Alternate location

Virtual Machine Name	
<input style="width: 95%;" type="text" value="TestingVM-A-1"/>	
Virtual Machines Directory Location	
<input style="width: 95%;" type="text" value="C:\ClusterStorage\Volume1\VM\TestingVM-A-1"/>	<input type="button" value="Browse"/>
Virtual Hard Disk Location	
<input style="width: 95%;" type="text" value="C:\ClusterStorage\Volume1\VM\TestingVM-A-1"/>	<input type="button" value="Browse"/>

When the values have been updated click on **Next** to proceed.

7. When the values have been updated click on **Next** to proceed. Confirm the temporary directory path is correct and then click **Restore** to proceed.

Temporary Directory

Temporary directory for storing restore files	
<input style="width: 95%;" type="text" value="C:\Users\Administrator\obm\temp"/>	<input type="button" value="Browse"/>

8. The Hyper-V guest VM has been restored successfully.

Restore

MS Hyper-V 2019 Non Cluster Non Run Direct

AhsayCBS (Host: 10.120.10.30:443)

✓

Restore Completed Successfully

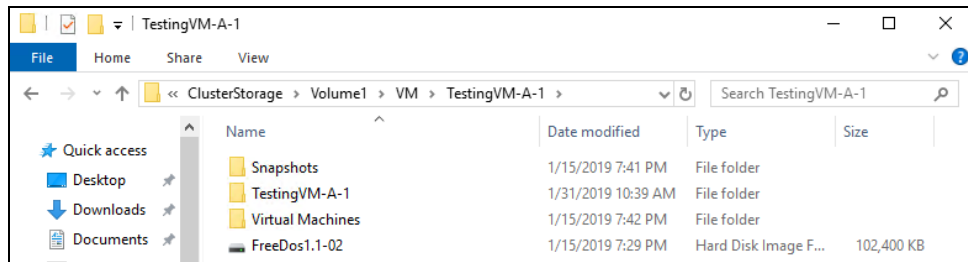
Estimated time left 0 sec

Restored 148.30M (11 files)

Elapsed time 22 sec

Transfer rate 56.27Mbit/s

9. Open Windows File Explorer and verify the guest has been restored to the new location.



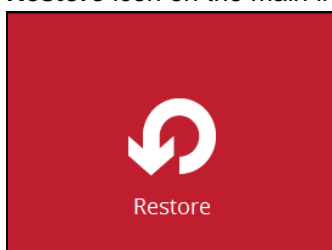
11.2 Different (Standby) Hyper-V Host

Restore of a Guest VM to a Different (Standby) Hyper-V Host

This restore option allows you to restore your backed up guest VM to another Hyper-V host, for example if your original Hyper-V host is down and you need to restore your production guest VM's to a standby Hyper-V host.

Please refer to the [Ch. 2.17.4 For Restore to a Different \(Standby\) Hyper-V Host](#) for the details about requirements and limitations for restoring Hyper-V guest VM to another Hyper-V host.

1. On the machine where you wish to restore the VM, launch AhsayOBM and click the **Restore** icon on the main interface.



2. Select the backup set that you would like to restore the guest VM from.



3. If encryption key was set at the time when the backup set was created, enter the encryption key when you see the following prompt.



4. Select the CBS, cloud, SFTP/FTP or drive storage destination that contains Hyper-V guest VM that you would like to restore.

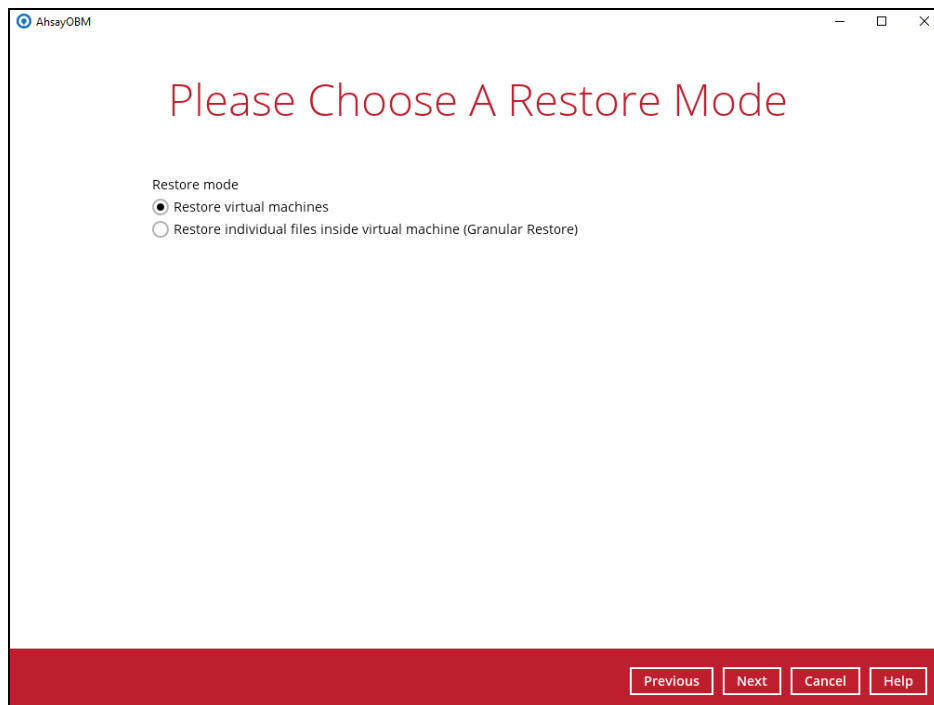
Example: Restore from F:\ drive



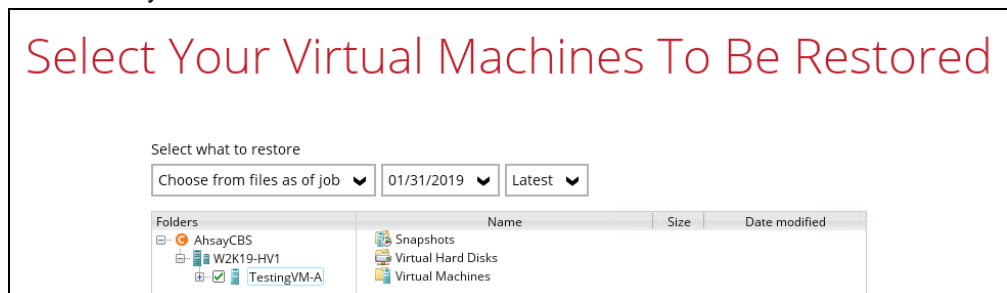
Example: Restore from AhsayCBS



5. If the backup set is created with **Run Direct** feature or **Granular Restore** feature enabled, the following step will show. Select **Restore virtual machines** as the restore mode.



6. Select to restore the Hyper-V guest from a specific backup job then select the files or folders that you would like to restore.



7. Select to restore the Hyper-V guest VM to the **Original location**, or to an **Alternate location**. Then click **Next** to proceed.

- ☒ **Original location** – The Hyper-V guest VM will be restored to the same directory path which stores the backup source on the original Hyper-V host.

- For backup set without Run Direct feature enabled:

Choose Where The Virtual Machines To Be Re...

Restore virtual machines to

☒ Original location

☐ Alternate location

Show advanced option

- For the backup set with Run Direct feature enabled, uncheck the box beside Run Direct and then click **Next** to proceed.

Choose Where The Virtual Machines To Be Re...

Restore virtual machines to

☒ Original location

☐ Alternate location

☐ Run Direct

Show advanced option

- **Alternate location** – The Hyper-V guest VM will be restored to the different directory path on the original Hyper-V host.

NOTE: For restore to an alternate Hyper-V Host with a different CPU architecture, the latest version of AhsayOBM client application must be installed.

- For backup set without Run Direct feature enabled:

Choose Where The Virtual Machines To Be Re...

Restore virtual machines to

☐ Original location

☒ Alternate location

Show advanced option

- For the backup set with Run Direct feature enabled, uncheck the box of Run Direct and then click **Next** to proceed.

Choose Where The Virtual Machines To Be Re...

Restore virtual machines to

☐ Original location

☒ Alternate location

☐ Run Direct

Show advanced option

Click **Next** to proceed and the following values are needed to be updated:

- Virtual Machine Name**
- Virtual Machines Directory Location** (guest configuration files)
- Virtual Hard Disk Location** (new location for the guest VHD files)

Example:

- Rename the restored guest VM to **"TestingVM-A-3"**
- Store the configuration files in the new location
"C:\ClusterStorage\Volume1\VM\TestingVM-A\TestingVM-A-3"

- iii. Store the VHD files in the new location
"C:\ClusterStorage\Volume1\VM\TestingVM-A\TestingVM-A-3"

Alternate location

Virtual Machine Name

Virtual Machines Directory Location

Virtual Hard Disk Location

When the values have been updated click on **Next** to proceed.


8. Confirm the temporary directory path is correct and then click **Restore** to proceed.


Temporary Directory


Temporary directory for storing restore files


9. Click **Restore** to start the restore process.
10. The following screen shows when the restore is completed.

Restore


**MS Hyper-V 2019 Backup**

**AhsayCBS (Host: 10.120.10.30:443)**

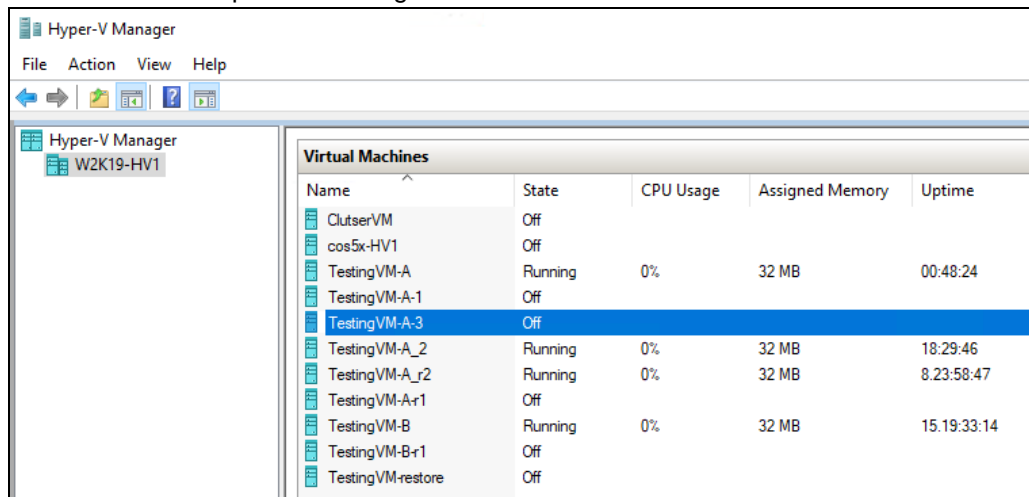


 **Restore Completed Successfully**

Estimated time left	0 sec
Restored	148.27M (11 files)
Elapsed time	26 sec
Transfer rate	49.38Mbit/s

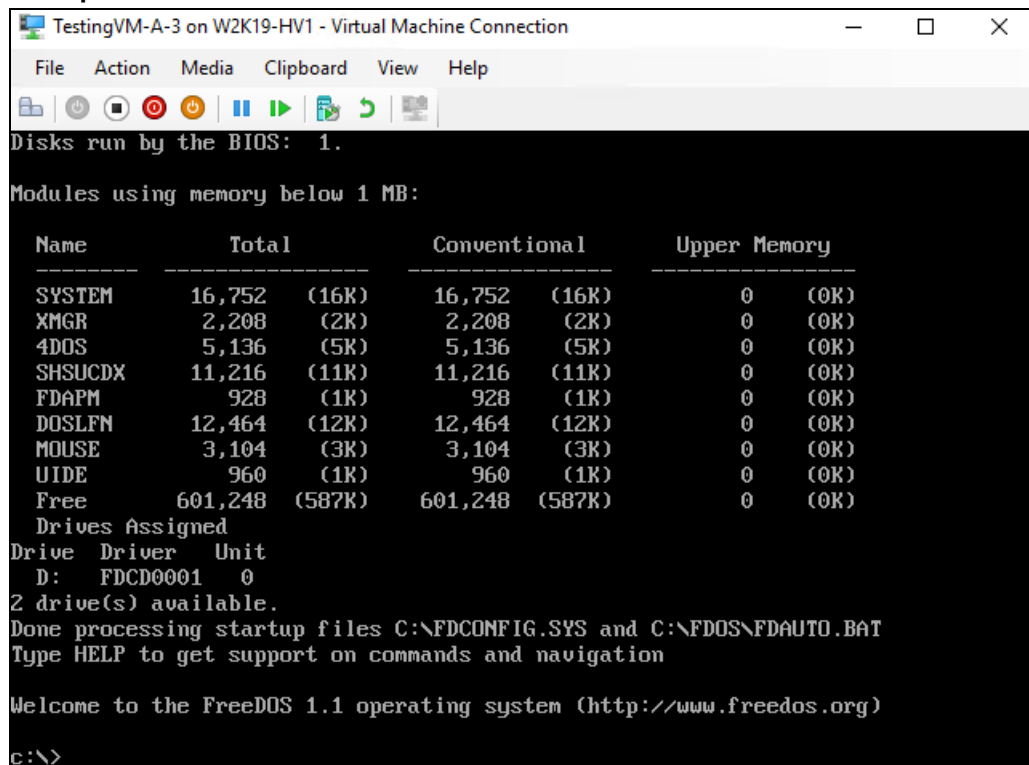


11. Go to the Hyper-V server and open the Hyper-V Manager to verify the guest has been restored and power on the guest VM.



12. Connect to the guest VM to verify if it is running correctly.

Example: FreeDOS

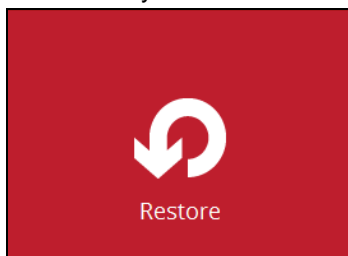


11.3 Individual Virtual Disk Restore

Restore of an Individual Virtual Disk to Original/Different Guest VM

The **Restore raw file** feature is used to the restore of an individual virtual disk to the original or a different guest VM.

1. In the AhsayOBM main interface, click the **Restore** icon.

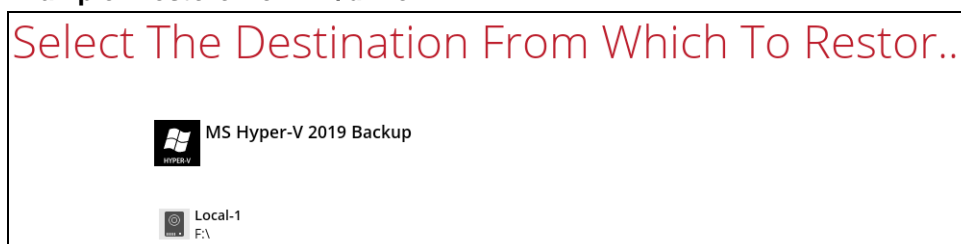


2. Select the backup set that you would like to restore the guest VM from.

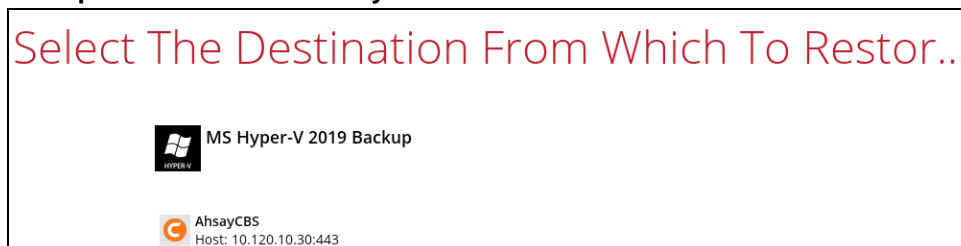


3. Select the CBS, cloud, SFTP/FTP or drive storage destination that contains Hyper-V guest VM that you would like to restore.

Example: Restore from F:\ drive

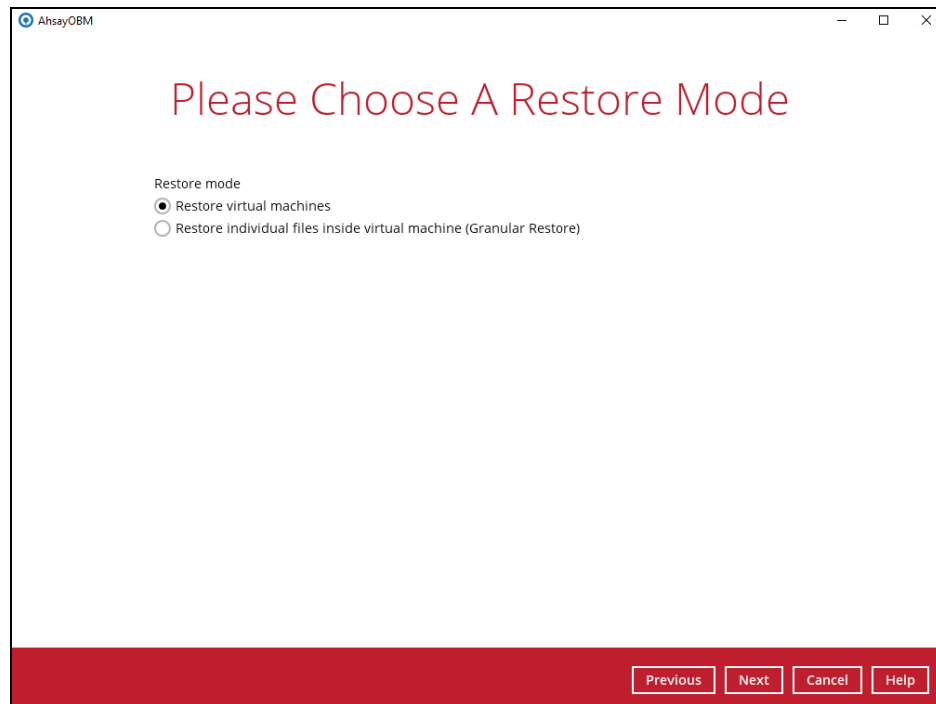


Example: Restore from AhsayCBS



4. If the backup set is created with **Run Direct** feature or **Granular Restore** feature enabled, the following step will show. Select **Restore virtual machines** as the

restore mode.



Please Choose A Restore Mode

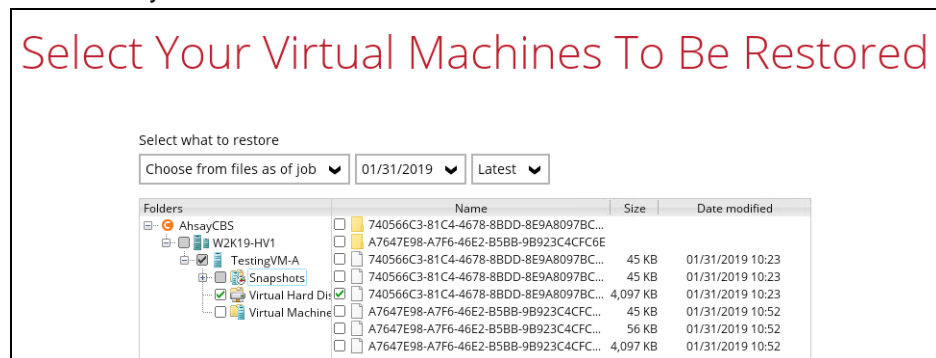
Restore mode

☒ Restore virtual machines

☐ Restore individual files inside virtual machine (Granular Restore)

Previous Next Cancel Help

5. Select to restore the Hyper-V guest from a specific backup job then select the files or folders that you would like to restore.

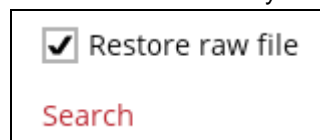


Select what to restore

Choose from files as of job 01/31/2019 Latest

Folders	Name	Size	Date modified
AhsayCBS	740566C3-81C4-4678-8BDD-8E9A8097BC...		
W2K19-HV1	A7647E98-A7F6-46E2-B5BB-9B923C4CFC6E		
TestingVM-A	740566C3-81C4-4678-8BDD-8E9A8097BC...	45 KB	01/31/2019 10:23
Snapshots	740566C3-81C4-4678-8BDD-8E9A8097BC...	45 KB	01/31/2019 10:23
Virtual Hard Disks	740566C3-81C4-4678-8BDD-8E9A8097BC...	4,097 KB	01/31/2019 10:23
Virtual Machine	A7647E98-A7F6-46E2-B5BB-9B923C4CFC...	45 KB	01/31/2019 10:52
	A7647E98-A7F6-46E2-B5BB-9B923C4CFC...	56 KB	01/31/2019 10:52
	A7647E98-A7F6-46E2-B5BB-9B923C4CFC...	4,097 KB	01/31/2019 10:52

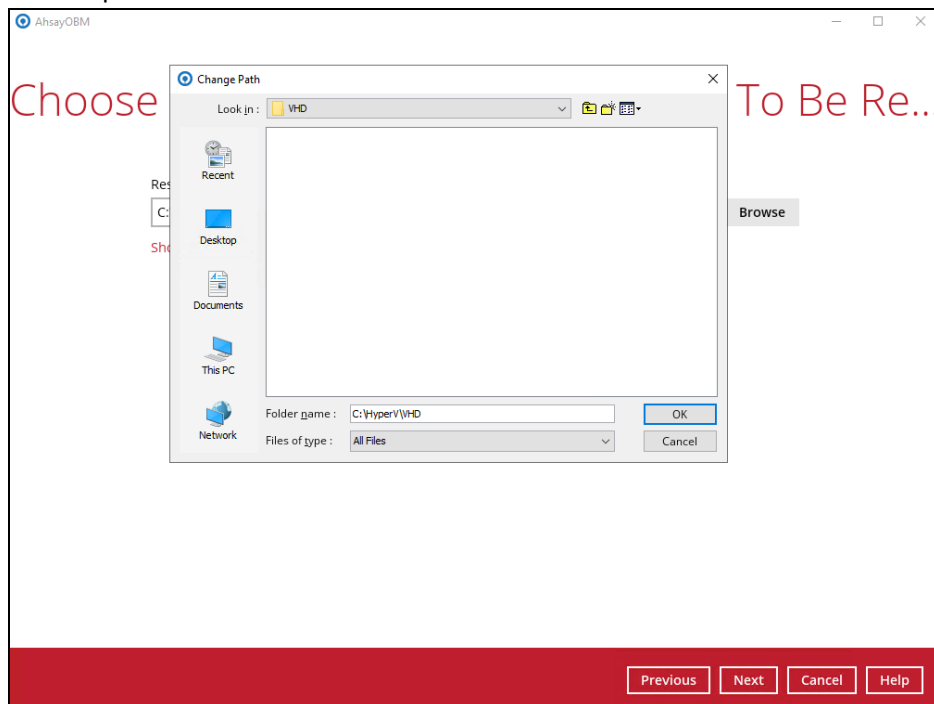
6. Then select the **Restore raw file** option and under the Virtual Hard Disks folder select the virtual disk you would like to restore. Click **Next** to proceed.



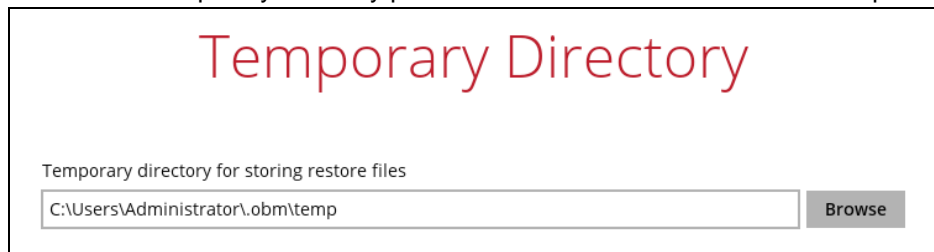
☒ Restore raw file

Search

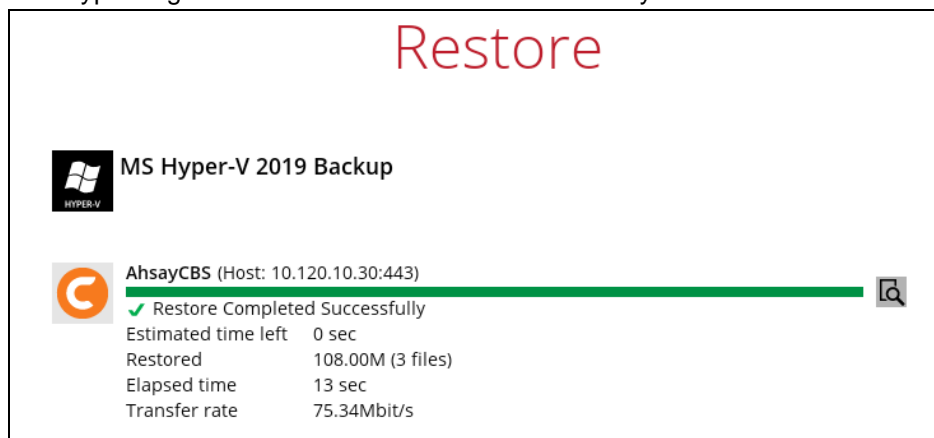
7. Select the location on the Hyper-V server you want to restore the virtual disk to. Click **Next** to proceed.



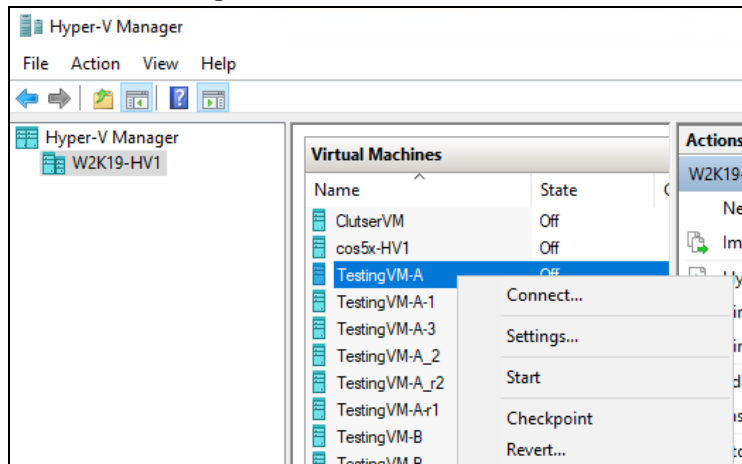
8. Confirm the temporary directory path is correct and then click **Restore** to proceed.



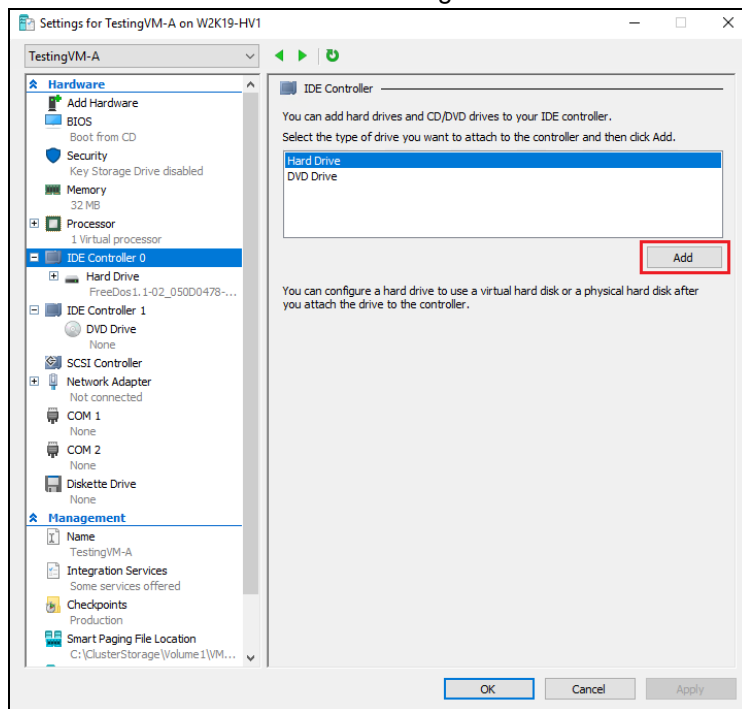
9. The Hyper-V guest VM has been restored successfully.



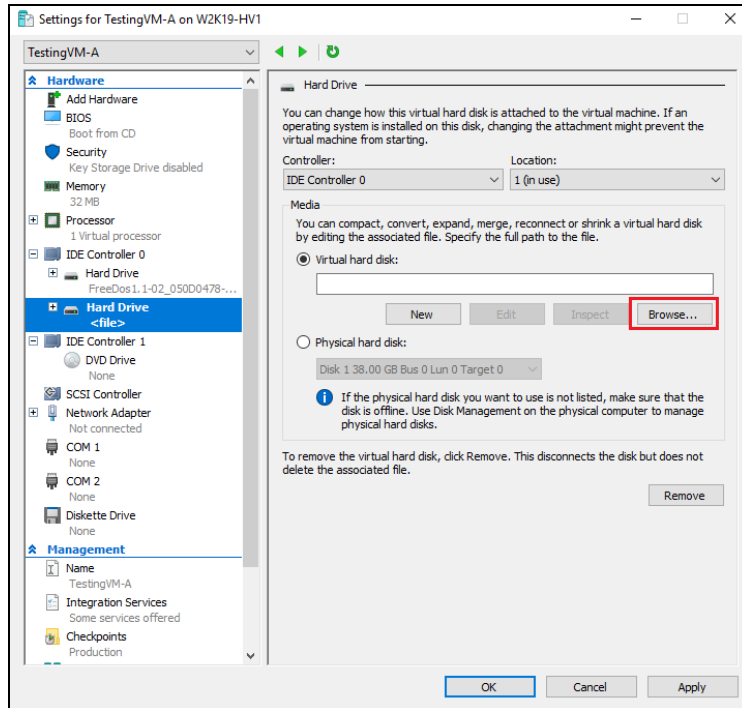
10. In Hyper-V Manager, right click on the guest VM you wish to add the virtual disk to and select **Settings**.



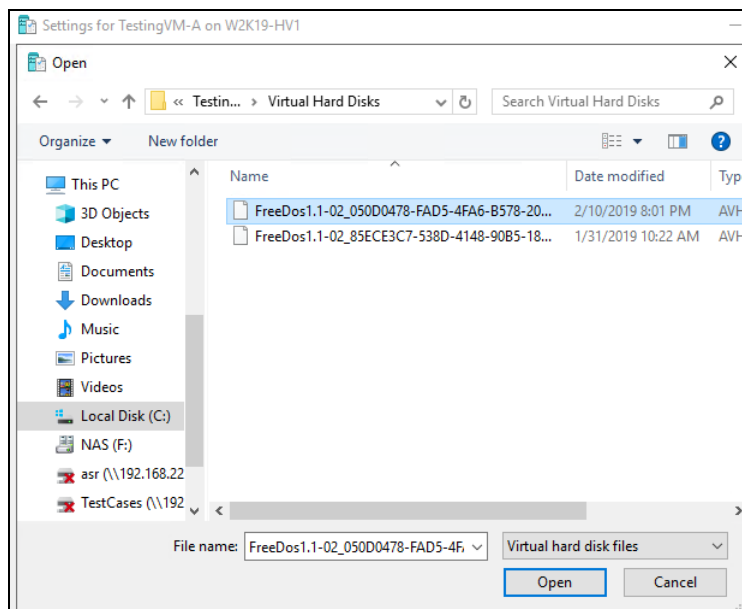
11. Select **Add** to add virtual disk to the guest VM.



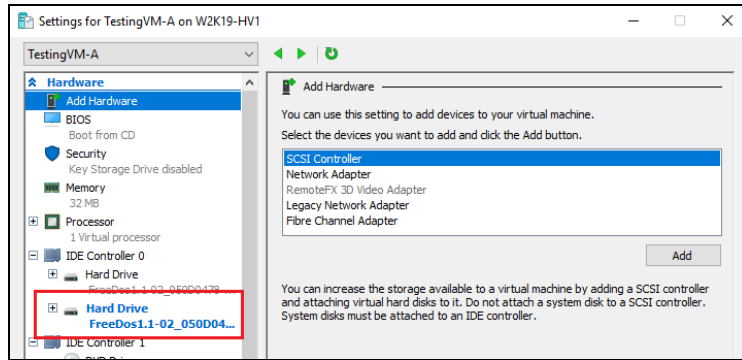
12. Click on Browse to choose the according vhd file.



13. Select the folder where the restore virtual disk is located.



14. **After the virtual disk is added.** Start the guest VM to confirm. Depending on the guest operating system there may be other configuration settings to be completed before the disk is available.



12 Granular Restore

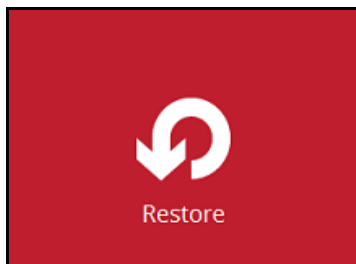
IMPORTANT

Before you proceed with the Granular Restore, make sure the following dependencies are fulfilled on the restore machine. Failure to do so may cause the granular restore to fail.

- Microsoft Visual C++ 2015 Redistributable (x86) / (x64)
<https://www.microsoft.com/en-us/download/details.aspx?id=48145>
- Update for Universal C Runtime in Windows
<https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows>
- Microsoft Security Advisory 3033929 (for Windows Server 2008 R2)
<https://technet.microsoft.com/en-us/library/security/3033929.aspx>

Start Granular Restore

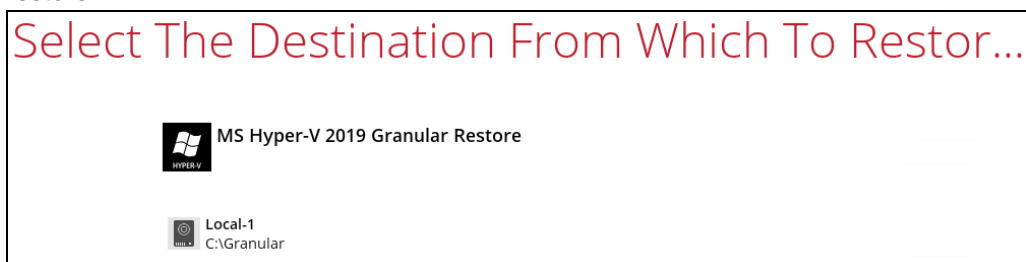
1. Click the **Restore** icon on the main interface of AhsayOBM.




2. Select the backup set that you would like to restore the individual files from.



3. Select the backup destination that contains the guest VM that you would like to restore.



4. Select the **Restore individual files in virtual machine (Granular Restore)** option.



Please Choose A Restore Mode

Restore mode

☐ Restore virtual machines

☒ Restore individual files inside virtual machine (Granular Restore)

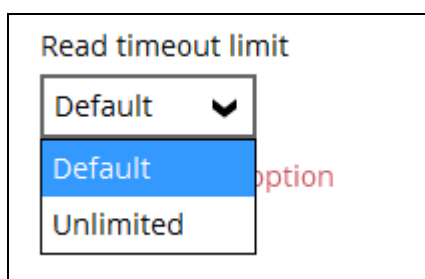
☒ Mount virtual disks automatically

[Show advanced option](#)

NOTE

The **Mount virtual disks automatically** option is selected by default. If the guest VM contains multiple virtual disks and you only require the restore of files from a single or certain virtual disk(s), then unselect this option to speed up the virtual disk mounting. Otherwise, granular restore will connect and mount all available virtual disks and this process could take longer.

You may select the **Read timeout limit** by clicking Show advanced option.



Read timeout limit

Default

Default

Unlimited

This selection defines the duration when the granular restore session will be disconnected if there is no response from the mounted VM.

- **Default** – This setting should be suitable for guest VMs located on a local, removable, or network drive. The time out value is 15 seconds.
- **Unlimited** – the connection will not be time out when this is selected. This selection is recommended when:
 - Backup destination is a cloud storage.
 - AhsayCBS over the Internet.
 - A large guest VM or guest VM with large incremental delta chain.

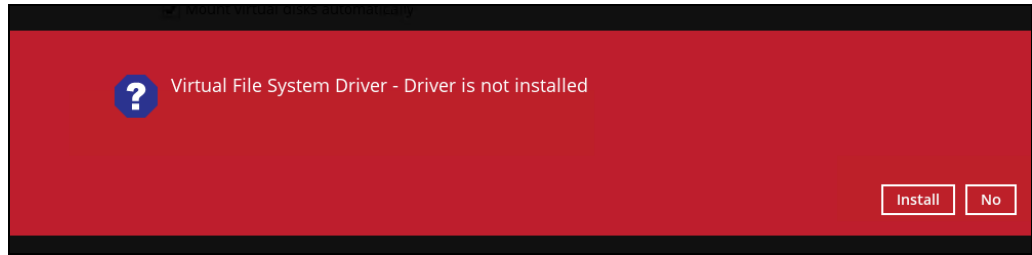
NOTE

If in doubt or unsure about the guest VM size or network stability, it is recommended to use **Unlimited**.

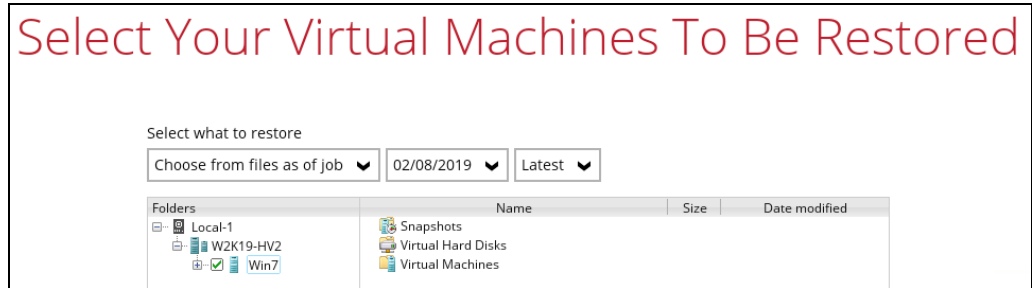
Click **Next** to proceed when you are done with the selection.

5. The following screen shows when you perform granular restore for a backup set on a machine for the first time only. Make sure you click **Yes** to confirm mounting of the

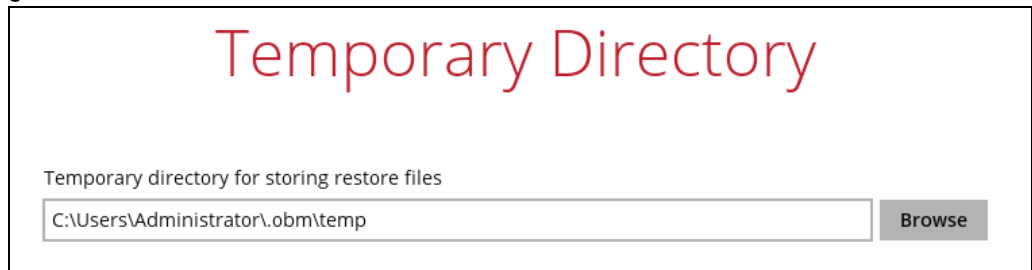
virtual disk on this machine. Clicking **No** will exit the restore process.



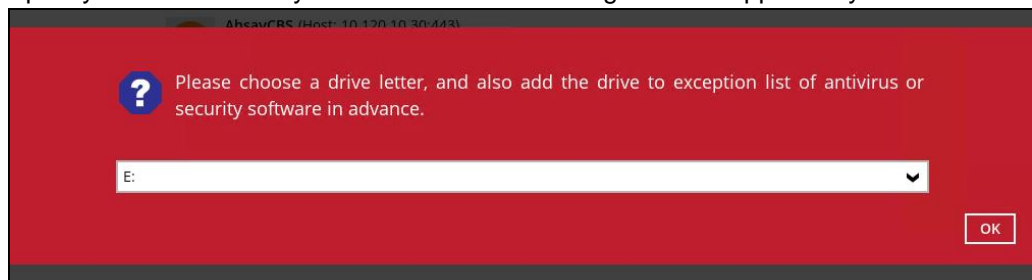
6. Select the VM that you would like to perform Granular Restore for, then click **Next** to proceed.



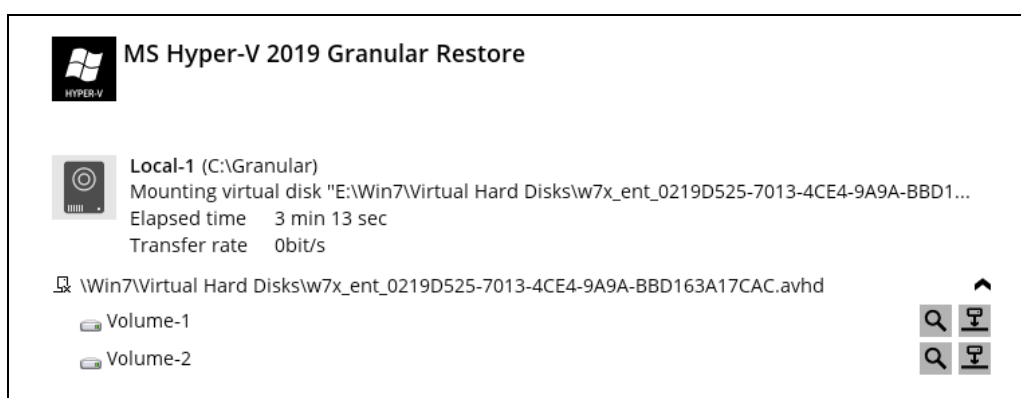
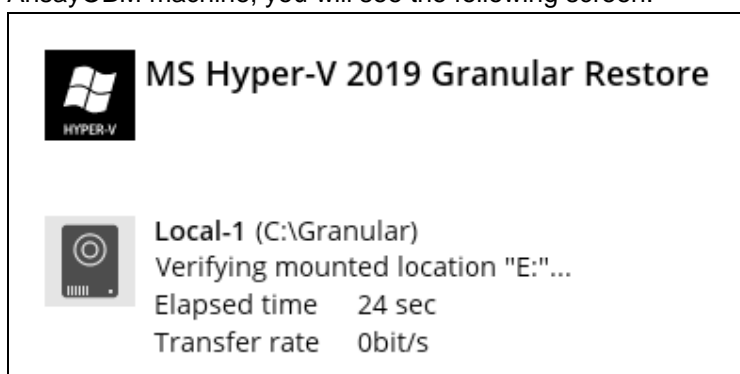
7. Select a temporary directory for storing restore files, then click Restore to start the granular restore.



8. Specify the drive where you wish the mounted image to be mapped on your machine.



When the virtual disk(s) are in the process of being prepared for mounting on the AhsayOBM machine, you will see the following screen.

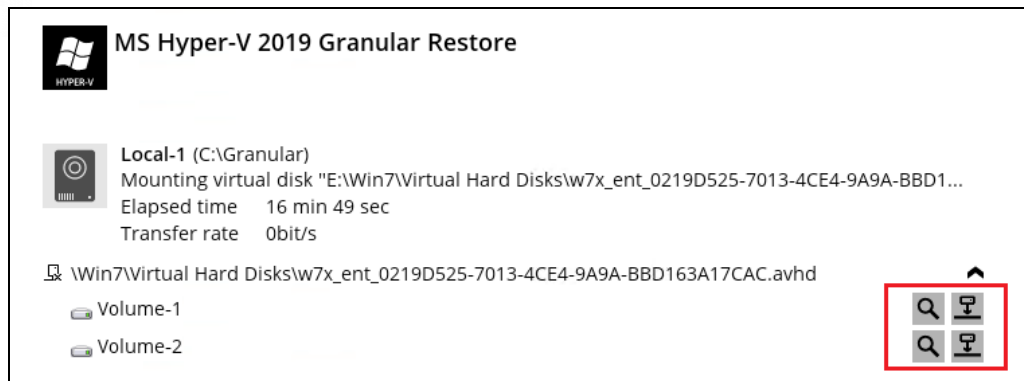


Please wait as the process could take some time depending on the size of the virtual disk, network bandwidth, and storage location.

9. If the **Mount virtual disks automatically** option is unselected, then click on the disk icon to mount the virtual disk you wish to restore files from.




Otherwise, the virtual disks will be automatically mounted.



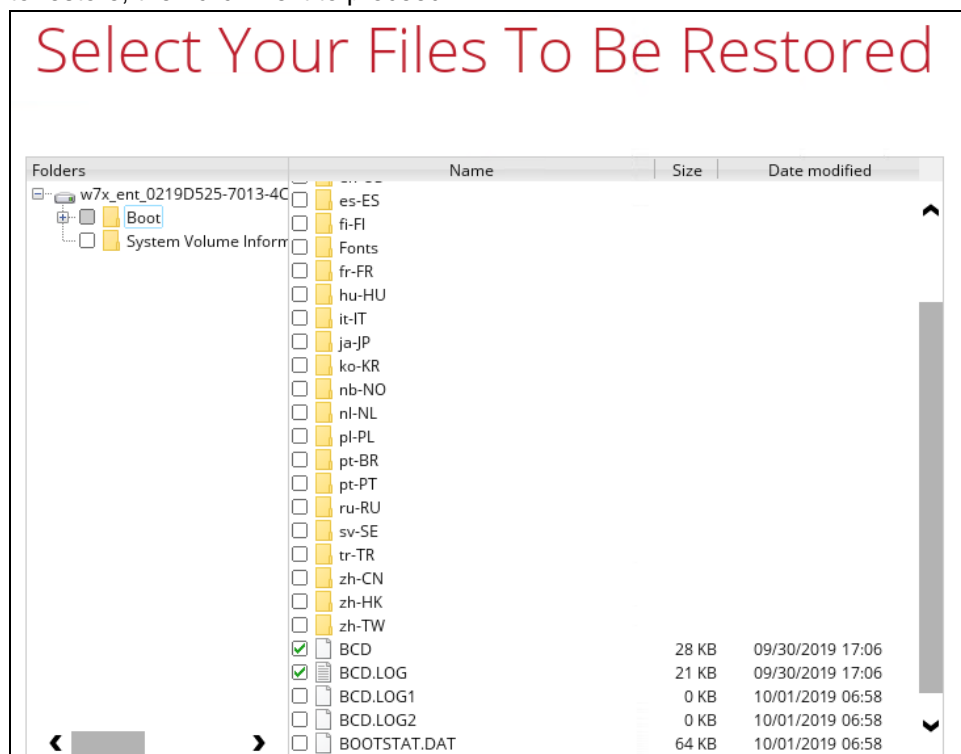
There are two options to restore individual files from here.

Option 1: Restore Using AhsayOBM File Explorer

This method allows you to use the file explorer in AhsayOBM to browse through the files from the mounted virtual disk and select files you wish to restore.

- i. Click  to browse the files in the mounted virtual disk. If there are multiple volumes in the guest VM, you can only select one volume to restore individual files at a time.

You will then see a file explorer menu as shown below. Select the file(s) you wish to restore, then click Next to proceed.



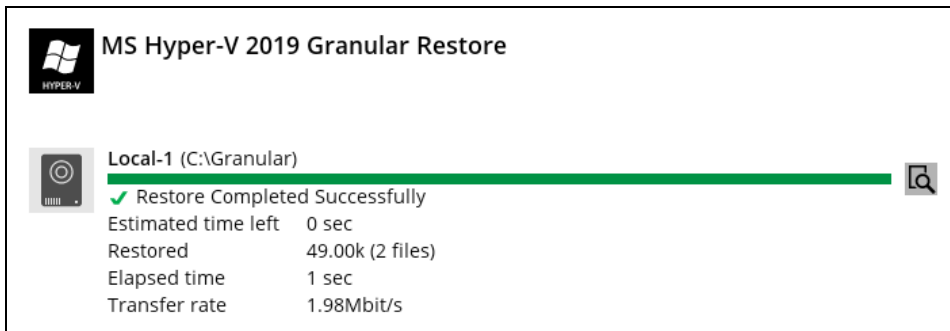
NOTE

Some system folder(s) / file(s) generated (e.g. System Volume Information) are only shown in the AhsayOBM File Explorer and will be not restored, therefore, those folder(s) / file(s) will not be shown in the mapped drive shown in step iv below.

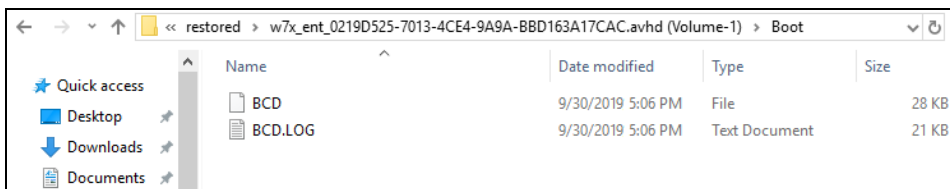
- ii. Select a path where you wish the files to be restored to, then click Restore.



- iii. The following screen shows when the selected files have been restored to the defined destination.



- iv. Open the defined restore path and you should be able to see the files being restored there.




Option 2: Restore Using Windows File Explorer

This method allows you to browse through the files from the mounted virtual disk through the file explorer on the machine where you have AhsayOBM installed on.

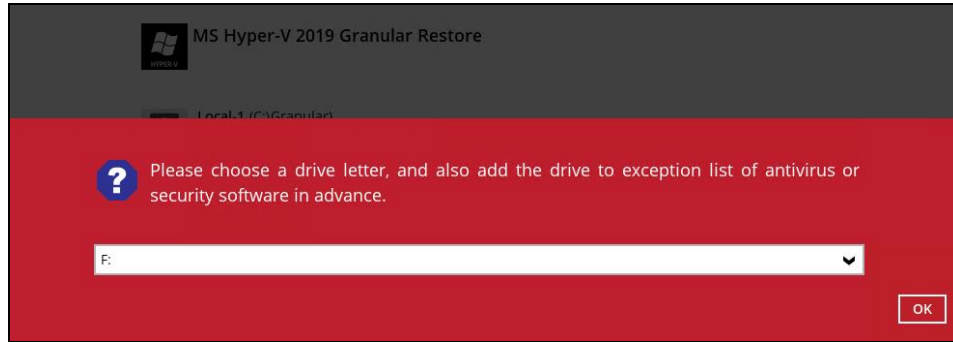
NOTE

Granular restore of Hyper-V backup sets performed using Windows File Explorer:

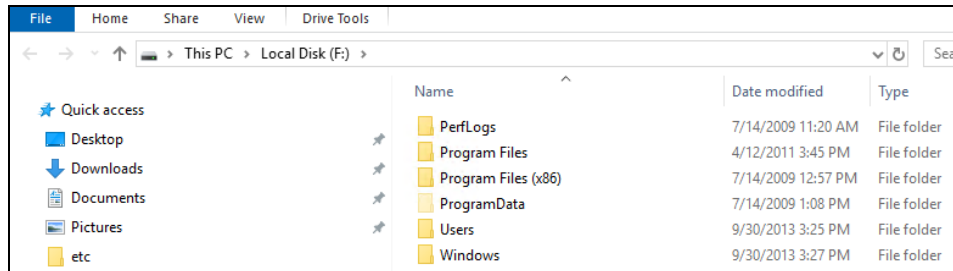
1. Will not show up on the **[Restore Status]** tab in **Live Activities** of the backup service provider AhsayCBS.
2. Will not generate restore reports on backup service provider AhsayCBS.
3. Will not generate restore log on AhsayOBM.

- i. Click  and then you will be prompted to select a driver letter where you wish the mounted image to be mapped on your machine, click **OK** when you have finished

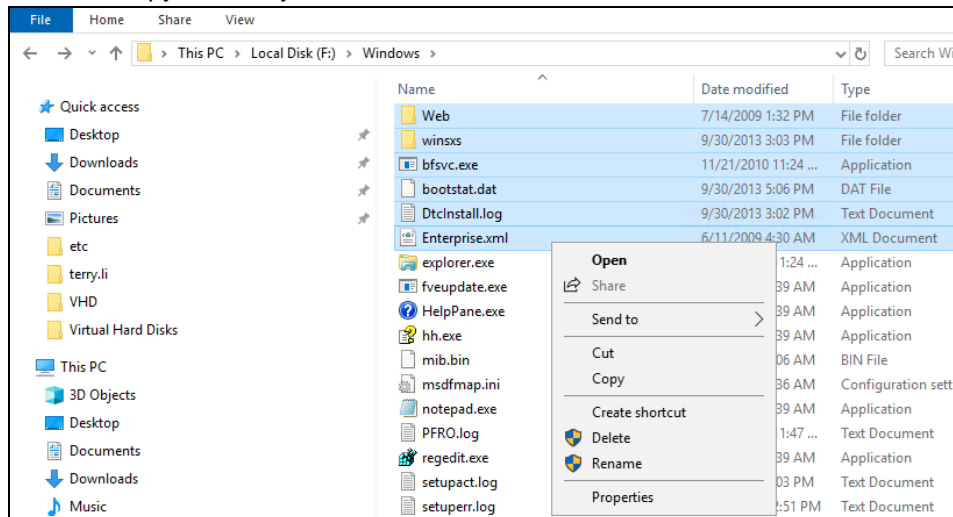
selecting.



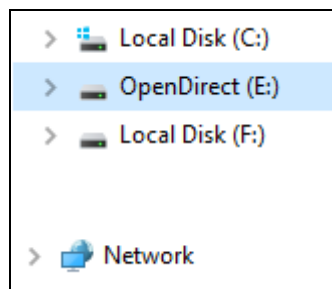
- ii. The selected drive letter will be mapped and prompted in the Windows Files Explorer with the files you wish to restore shown.



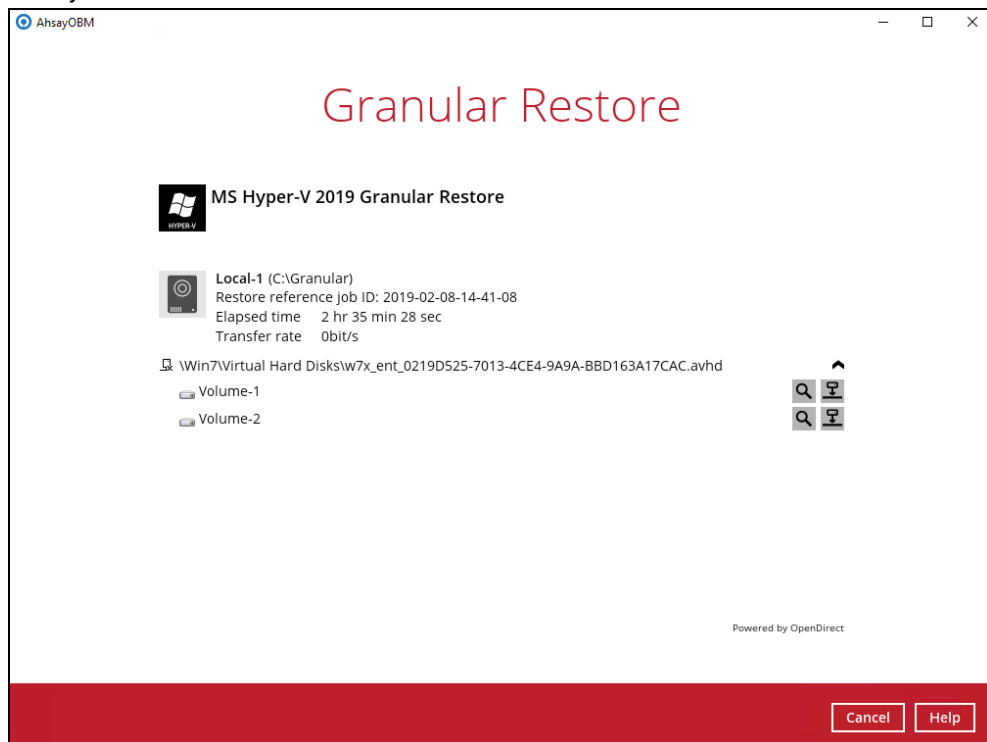
- iii. You can now click on the files to view them directly from here, which will be in read-only mode, or copy them to your local machine.



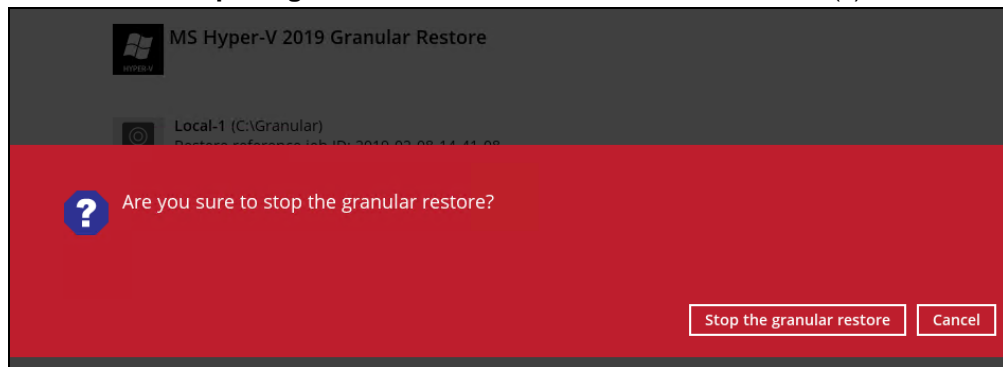
- iv. The mounted drive letter cannot be ejected from the Windows File Explorer, it will only be closed when you exit AhsayOBM.



10. When you have finished restoring the necessary files, you can go back to AhsayOBM and click on Cancel.



11. Then click on **Stop the granular restore** and unmount the virtual disk(s).



IMPORTANT

Due to the limitation of the virtual file system library, the mounted virtual disks will only be unmounted from your machine when you exit AhsayOBM.

13 Contact Ahsay

13.1 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/>

13.2 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.