Ahsay™ Ahsay Backup

Ahsay Online Backup Manager v7

Microsoft Hyper-V Guest Virtual Machine Backup & Restore Guide

Ahsay Systems Corporation Limited

2 November 2017

A wholly owned subsidiary of
Ahsay Backup Software Development Company Limited
HKEx Stock Code: 8290

Copyright Notice

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, Ahsay NAS Client Utility are trademarks of Ahsay Systems Corporation Limited.

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

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

Dropbox is registered trademark of Dropbox Inc.

Google Cloud Storage and Google Drive are registered trademarks of Google Inc.

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

Microsoft, Windows, Microsoft Exchange Server, Microsoft SQL Server, Microsoft Hyper-V, Microsoft Azure, One Drive and One Drive for Business 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, Oracle 10g, Oracle 11g 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.

ShadowProtect is registered trademark of StorageCraft Technology Corporation.

VMware, ESX, ESXi, vCenter 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
20 Sept 2016	First Draft	New
25 Sept 2016	Ch. 1.3	Modified
23 Nov 2016	Ch. 1.4, 2, 5.1.2, 5.2.1	Modified
27 Jan 2017	Ch. 1.3, 2	Modified
3 Feb 2017	Added instructions and screen shots for Encryption key handling in Ch. 5; added new limitation in Ch. 2	New
5 Apr 2017	Added Overview section; revised requirements in Ch.2; content restructured in Ch.9 & added steps for restore VM to another host; Added Encryption Type option in Ch. 5.1 & Ch. 5.2	New & Modified
31 May 2017	Added Ch.4 Granular restore section, added step in Create new backup set, added Granular restore sub-section in the Restore section	New
20 Jun 2017	Updated Ch.4, Ch. 9, Ch. 12, Updated all granular screen shots	Modified
13 Jul 2017	Updated Ch.4, Ch. 9, Ch. 12, Updated all granular screen shots	Modified
6 October 2017	Updated Ch.2.4; Added CBT Requirement for Ch.2.5; Added Windows Server 2016 Requirement for Ch.2.6; updated Limitations for Ch.2.7; Updated Ch.4.1; Updated Ch.12; Added note of restore using Windows File Explorer for Ch.12; Added Ch.2.5 Hyper-V Backup Methods	New/ Modified

Table of Contents

1 Overview

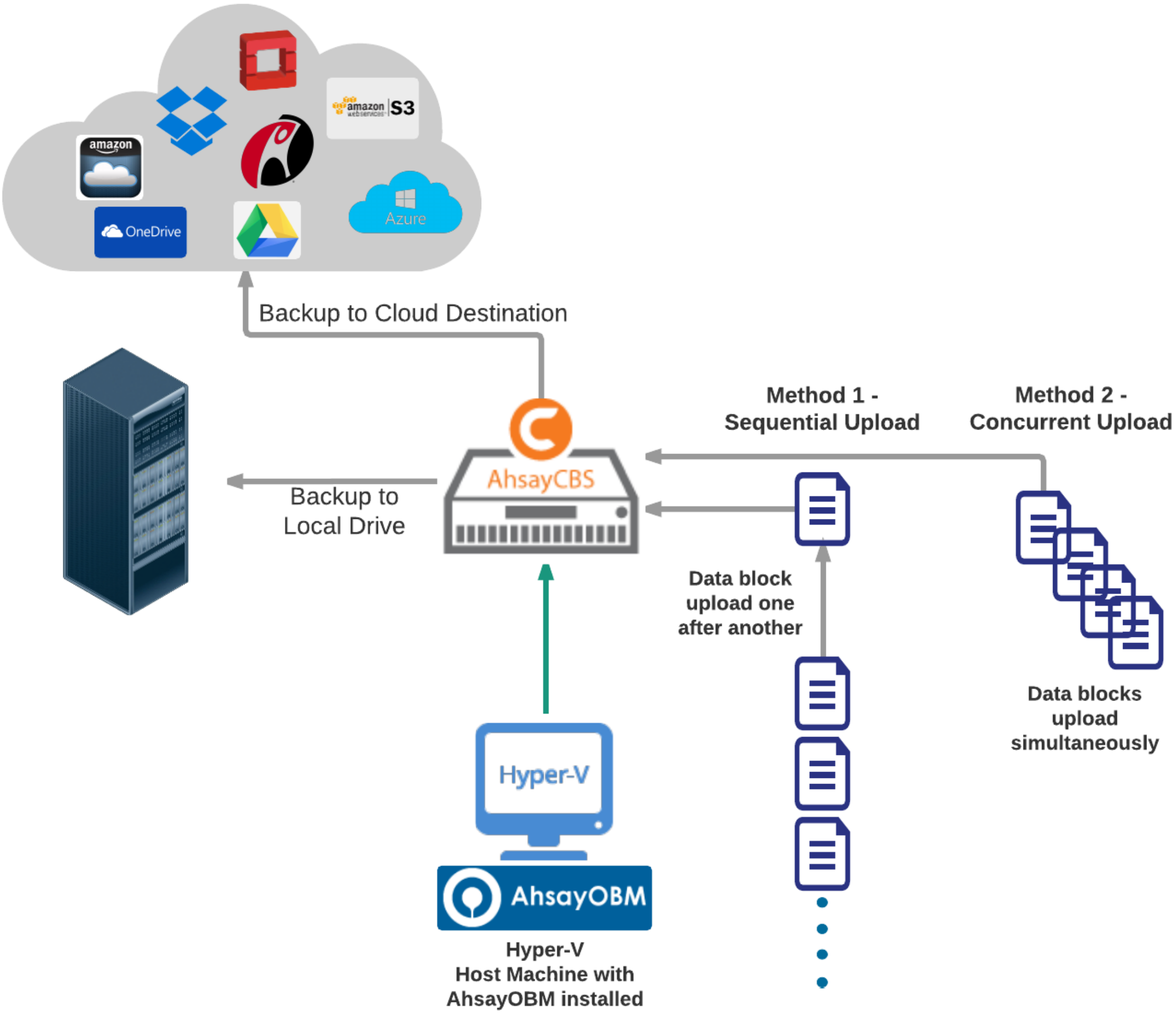
What is this software?

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 virtual machines. 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.

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

Hardware Requirement

Refer to the following article for the list of hardware requirements for AhsayOBM:
FAQ: Ahsay Hardware Requirement List (HRL) for version 7.3 or above

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 7.3 or above

AhsayOBM

1. AhsayOBM is installed on the Hyper-V server. For Hyper-V Cluster environment AhsayOBM is installed on all Cluster nodes.

2. 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).

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

4. 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. (Please contact your backup service provider for details)

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

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

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

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

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

6. The default Java heap size setting on AhsayOBM is 1024MB, 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 increased to 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 KB article for details:
https://forum.ahsay.com/viewtopic.php?f=206&t=14117

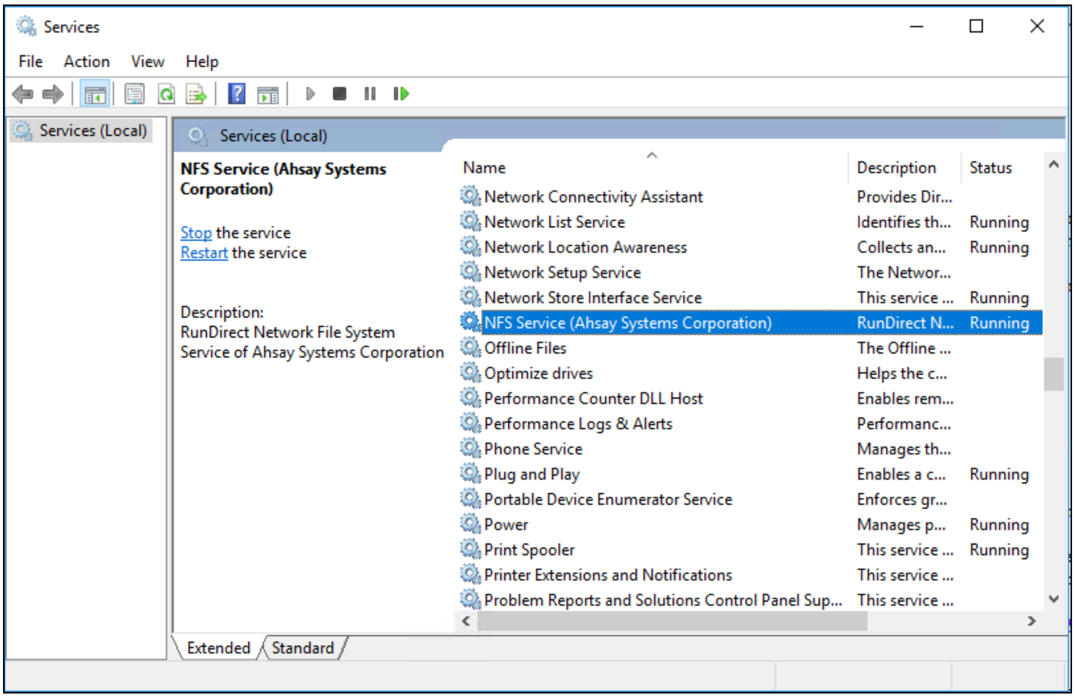
7. AhsayOBM uses the temporary folder for storing backup set index files and any incremental or differential delta files generated during a backup job. To ensure optimal backup/restore performance, it should be located on a local drive with plenty of free disk space. **It should not be on the Windows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

8. AhsayOBM UI must be running when a guest virtual machine is started using Run Direct Restore or when migration process is running.

9. 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.

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

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



NFS Service (Ahsay Systems Corporation)

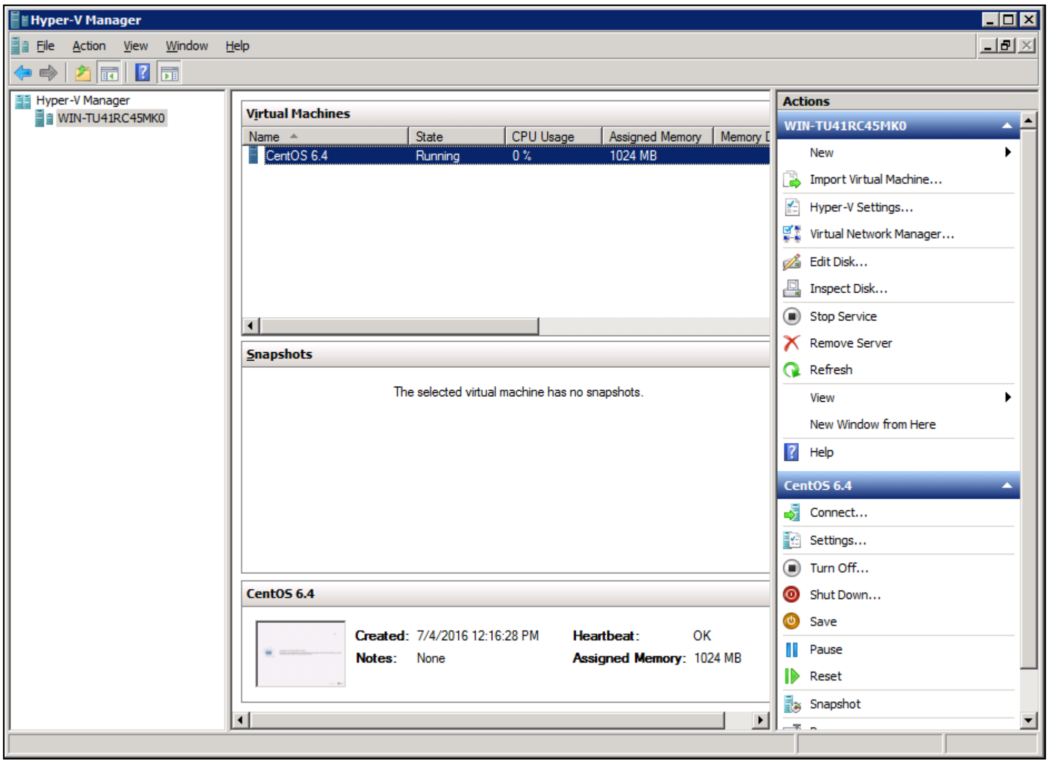
Stop the service
Restart the service

Description:
RunDirect Network File System Service of Ahsay Systems Corporation

Name	Description	Status
Network Connectivity Assistant	Provides Dir...	
Network List Service	Identifies th...	Running
Network Location Awareness	Collects an...	Running
Network Setup Service	The Networ...	
Network Store Interface Service	This service ...	Running
NFS Service (Ahsay Systems Corporation)	RunDirect N...	Running
Offline Files	The Offline ...	
Optimize drives	Helps the c...	
Performance Counter DLL Host	Enables rem...	
Performance Logs & Alerts	Performanc...	
Phone Service	Manages th...	
Plug and Play	Enables a c...	Running
Portable Device Enumerator Service	Enforces gr...	
Power	Manages p...	Running
Print Spooler	This service ...	Running
Printer Extensions and Notifications	This service ...	
Problem Reports and Solutions Control Panel Sup...	This service ...	

Hyper-V Server Requirement

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.

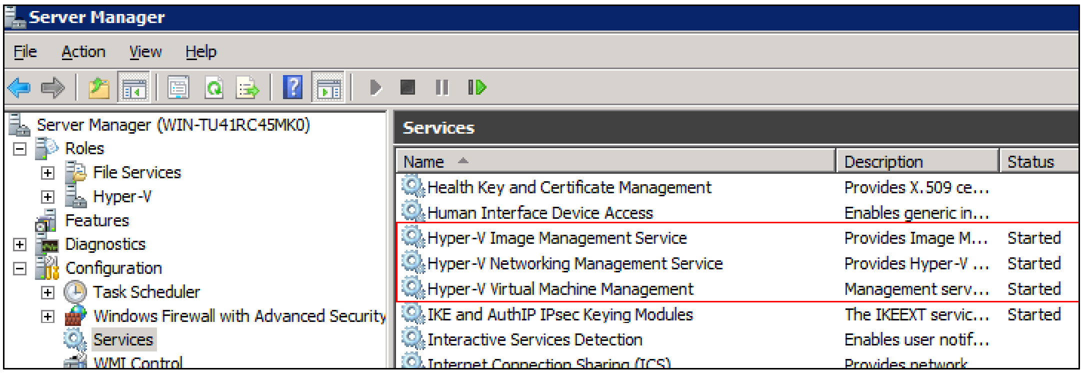


Name	State	CPU Usage	Assigned Memory	Memory [
CentOS 6.4	Running	0 %	1024 MB	

The selected virtual machine has no snapshots.

Created: 7/4/2016 12:16:28 PM **Heartbeat:** OK
Notes: None **Assigned Memory:** 1024 MB

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



Name	Description	Status
Health Key and Certificate Management	Provides X.509 ce...	
Human Interface Device Access	Enables generic in...	
Hyper-V Image Management Service	Provides Image M...	Started
Hyper-V Networking Management Service	Provides Hyper-V ...	Started
Hyper-V Virtual Machine Management	Management serv...	Started
IKE and AuthIP IPsec Keying Modules	The IKEEXT servic...	Started
Interactive Services Detection	Enables user notif...	
Internet Connection Sharing (ICS)	Provides network	

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-ffaff65ddf06}
   Writer Instance Id: {088e7a7d-09a8-4cc6-a609-ad90e75ddc93}
   State: [1] Stable
   Last error: No error

Writer name: 'Performance Counters Writer'
   Writer Id: {0bada1de-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-9a1e-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
```

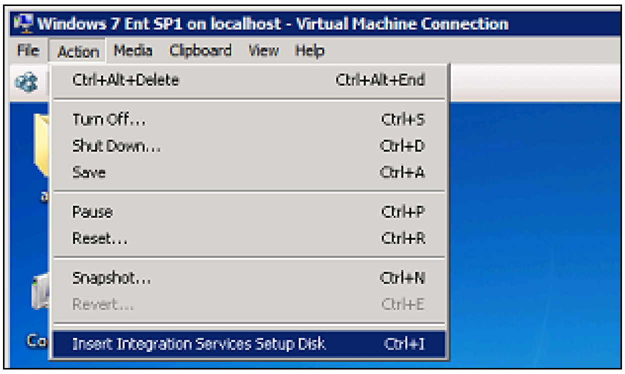
4. Integration Service

i. If Integration services is not installed / updated on a guest virtual machine or the guest operating system is not supported by Integration Services, the corresponding virtual machine will be paused or go into a saved stated during the snapshot process for both backup and restore, and resume when the snapshot is completed. Furthermore, the corresponding virtual machine uptime will also be reset to 00:00:00 in the Hyper-V Manager.

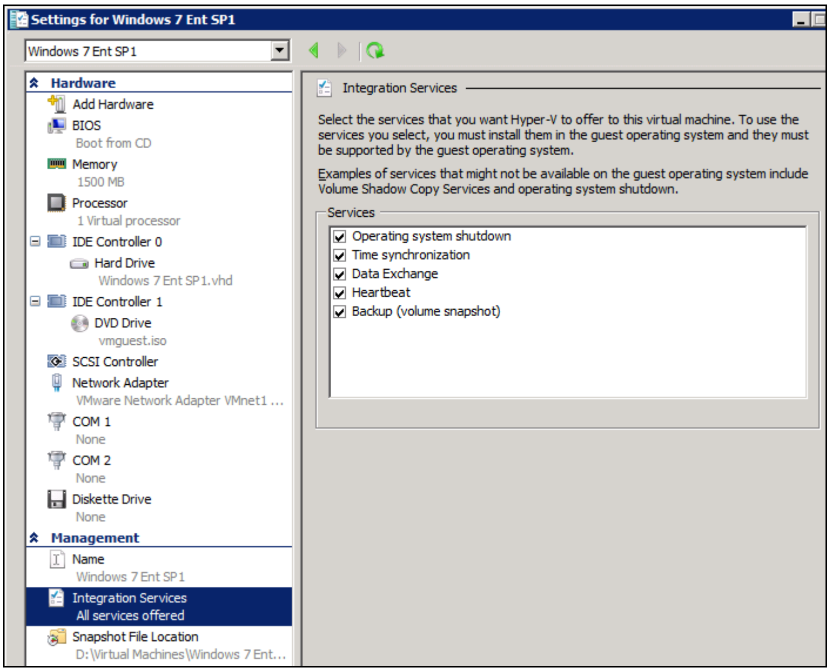
ii. Installing or updating Integration Services guest virtual machine(s) may require a restart of the guest virtual machine to complete the installation.

- To install Integration Services
- In Hyper-V Manager connect to the guest virtual machine and select Action > Insert Integration Services disk

Example: Windows 7 Enterprise guest



- If the guest operating system supports live virtual machine backup the Backup (volume checkpoint) is enabled.



BIOS
Boot from CD
Memory
1500 MB
Processor
1 Virtual processor
IDE Controller 0
Hard Drive
Windows 7 Ent SP1.vhd
IDE Controller 1
DVD Drive
vmguest.iso
SCSI Controller
Network Adapter
VMware Network Adapter VMnet1 ...
COM 1
None
COM 2
None
Diskette Drive
None
Name
Windows 7 Ent SP1
Integration Services
All services offered
Snapshot File Location
D:\Virtual Machines\Windows 7 Ent...

Integration Services

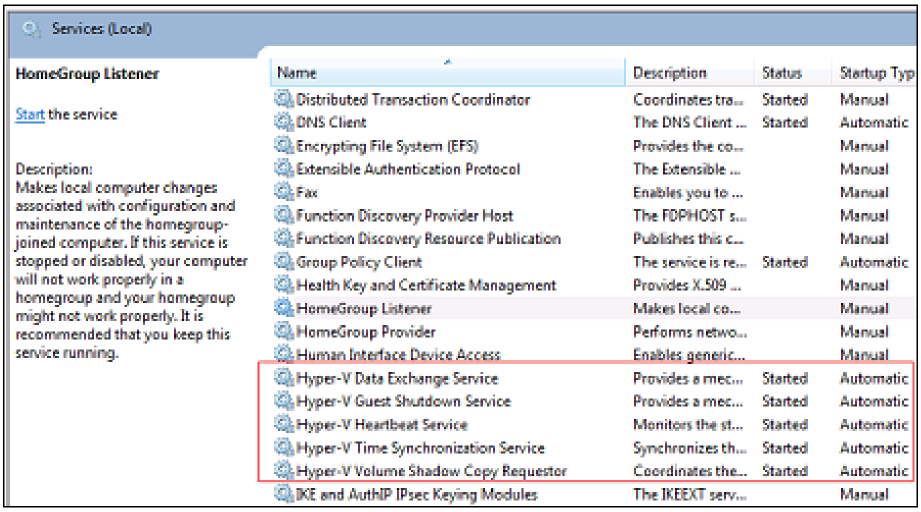
Select the services that you want Hyper-V to offer to this virtual machine. To use the services you select, you must install them in the guest operating system and they must be supported by the guest operating system.

Examples of services that might not be available on the guest operating system include Volume Shadow Copy Services and operating system shutdown.

Services
- ☑ Operating system shutdown
- ☑ Time synchronization
- ☑ Data Exchange
- ☑ Heartbeat
- ☑ Backup (volume snapshot)

- The related Integration Services are running on the guest virtual machine:

Example: Windows 7 Enterprise guest



Services (Local)

HomeGroup Listener

Start the service

Description:
Makes local computer changes associated with configuration and maintenance of the homegroup-joined computer. If this service is stopped or disabled, your computer will not work properly in a homegroup and your homegroup might not work properly. It is recommended that you keep this service running.

Name	Description	Status	Startup Typ
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 virtual machines https://technet.microsoft.com/en-us/library/dn798286.aspx
  - Supported Windows Guest Operating Systems for Hyper-V in Windows Server 2012 https://technet.microsoft.com/en-us/library/dn792028(v=ws.11).aspx
  - Supported Windows Guest Operating Systems for Hyper-V in Windows Server 2012 R2 https://technet.microsoft.com/en-us/library/dn792027(v=ws.11).aspx
  - Supported Linux and FreeBSD virtual machines for Hyper https://technet.microsoft.com/library/dn531030.aspx
  - Linux Integration Services Version 4.0 for Hyper-V https://www.microsoft.com/en-us/download/details.aspx?id=46842
  - Managing Hyper-V Integration Services https://msdn.microsoft.com/en-us/virtualization/hyperv_on_windows/user_guide/managing_ics

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 virtual machines must be created and managed by the Failover Cluster Manager.

Hyper-V Backup Methods

AhsayOBM v7 supports two methods for Hyper-V guest VM backup, VM Snapshot and Saved State.

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.

VM Snapshot Method Requirements

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, for example NTFS.

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

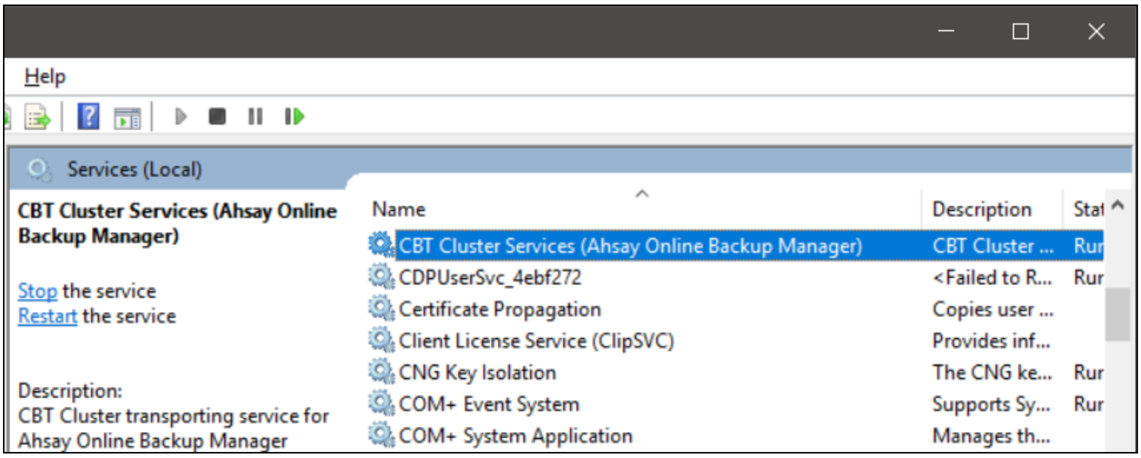
Some older Windows operating systems installed on guest VM's which do not support either Integration Services or the Hyper-V Volume Shadow Copy Requestor Service, will not support VM snapshot method, for example, Microsoft Windows 2000, Windows XP, or older Linux/FreeBSD versions.

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 Huper-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.

CBT Requirement

Since AhsayOBM version 7.9.0.0, a new service **CBT Cluster Services (Ahsay Online Backup Manager)** is installed and enabled upon installation / upgrade to version AhsayOBM v7.9.0.0 or above.



CBT Cluster Services (Ahsay Online Backup Manager)

Stop the service
Restart the service

Description:
CBT Cluster transporting service for Ahsay Online Backup Manager

Name	Description	Stat
CBT Cluster Services (Ahsay Online Backup Manager)	CBT Cluster ...	Rur
CDPUserSvc_4ebf272	<Failed to R...	Rur
Certificate Propagation	Copies user ...	
Client License Service (ClipSVC)	Provides inf...	
CNG Key Isolation	The CNG ke...	Rur
COM+ Event System	Supports Sy...	Rur
COM+ System Application	Manages th...	

1. CBT (**Changed Block Tracking**) is used to optimize incremental backups of virtual machines 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.

> **Note**
>
> From version 7.15.0.0 onwards, CBT service is supported on all the backup destinations for AhsayOBM instead of only RunDirect related local destination.

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 where a built-in system called Resilient Change Tracking (RCT) will be used instead. For details of RCT, please refer to Windows Server 2016 RCT Requirement.

Windows Server 2016 Requirement

RCT Requirement

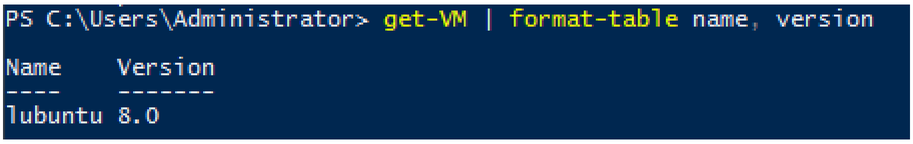
1. From v7.15.0.0 onwards AhsayOBM would not install CBT Cluster Services (Ahsay Online Backup Manager) but use the native built-in RCT (Resilient Change Tracking) feature of Windows server 2016 instead.

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

   Example:

   i. This can be verified by using Windows PowerShell.

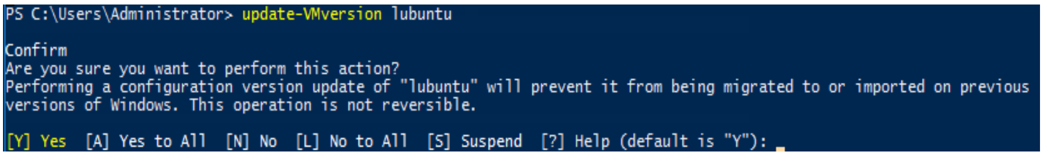
```
get-VM | format-table name, version
```



```
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 need to upgrade the virtual machine configuration version.

```
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 virtual machine 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

Guest VM Dependencies Requirements

To get full use of Hyper-V, install the appropriate linux-tools and linux-cloud-tools packages to install tools and daemons, i.e. VSS Snapshot Daemon, for use with virtual machines. 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-linux-and-freebsd-virtual-machines-for-hyper-v-on-windows

Limitations

1. Backup of guest machines located on a SMB 3.0 shares is not supported.

2. Backup of virtual machine with pass through disk (directly attached physical disk) is not supported.

3. For backup of individual virtual disks, the restored virtual machine does not support the reversion of previous snapshots, if the snapshot contains disks which are not previously backed up by AhsayOBM.

4. A guest virtual machine can only be restored to the Hyper-V server with the same version, i.e. backup of a guest on Hyper-V 2012 R2 server cannot be restored to Hyper-V 2008 R2 Server or vice versa.

5. The guest virtual machine 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.

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

Note

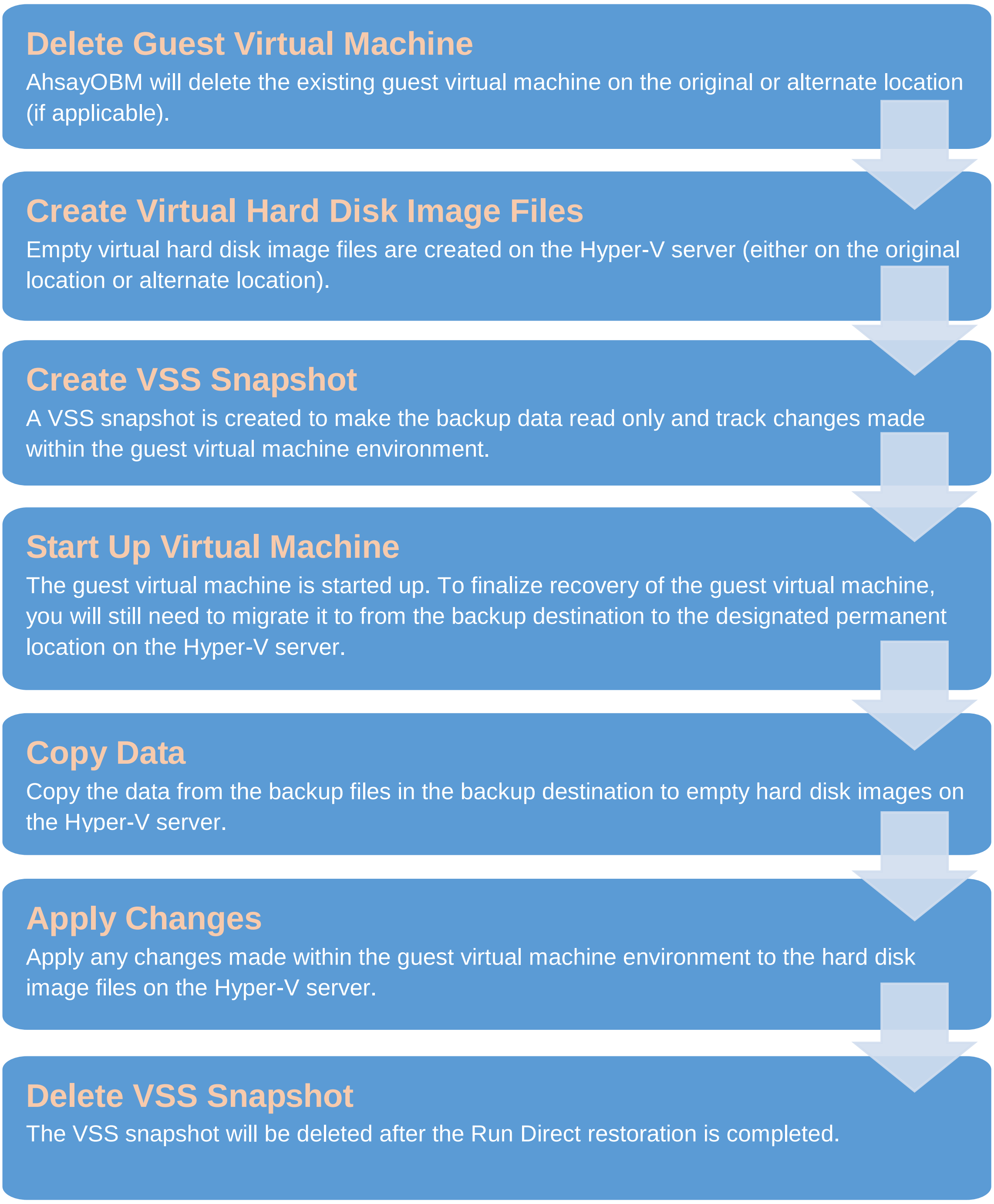
This will require modification of Hyper-V guest configuration files, and this only should be done if you have in-depth knowledge and understanding of Hyper-V, otherwise the guest virtual machine may not startup properly.

3 Run Direct

Hyper-V Run Direct is a recovery feature introduced in AhsayOBM version v7.5.0.0, it helps to reduce disruption and downtime of your production guest virtual machines.

Unlike normal recovery procedures where the guest virtual machine(s) 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 virtual machine by running it directly from the backup file in the backup destination; this process can be completed in minutes.

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



Delete Guest Virtual Machine

AhsayOBM will delete the existing guest virtual machine 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 virtual machine environment.

Start Up Virtual Machine

The guest virtual machine is started up. To finalize recovery of the guest virtual machine, you will still need to migrate it to 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 virtual machine 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 virtual machine, 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 virtual machine) 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 virtual machine will be removed and all changes will be discarded, or the changes will be consolidated with the original virtual machine data when the restore is finalized.

For more details on Run Direct restore options, refer to Restore Options.

4 Granular Restore Technology

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.

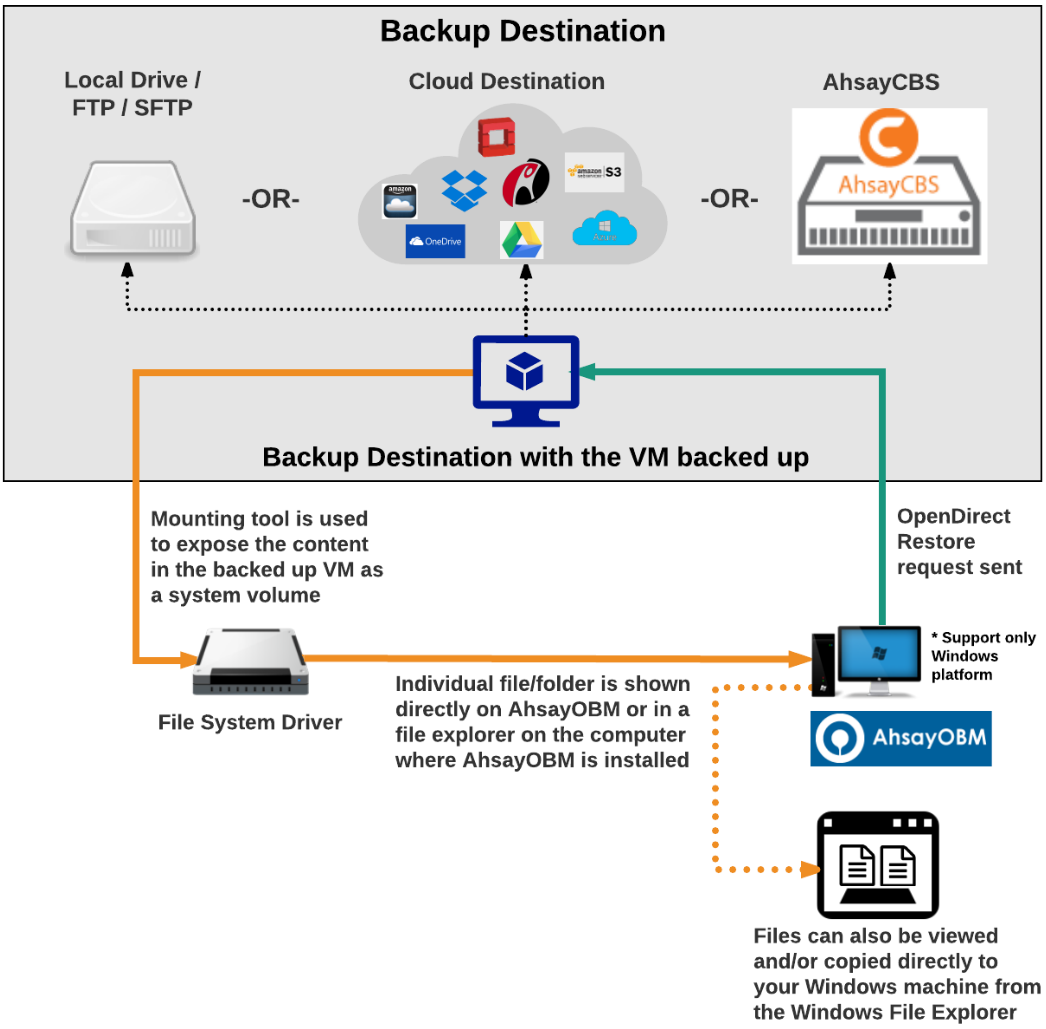
Granular restore is one of the available restore options for Hyper-V backup sets from AhsayOBM v7.13.0.0 or above. AhsayOBM makes use of granular restore technology to enable a file level restore from a virtual disk file (VHD) of guest VM backup possible. It is particularly useful if you only need to 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 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 virtual machine. 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, i.e. 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.

How does Granular Restore work?


Backup Destination
Local Drive / FTP / SFTP
-OR-
Cloud Destination
-OR-
AhsayCBS
Backup Destination with the VM backed up
Mounting tool is used to expose the content in the backed up VM as a system volume
OpenDirect Restore request sent
File System Driver
Individual file/folder is shown directly on AhsayOBM or in a file explorer on the computer where AhsayOBM is installed
* Support only Windows platform
AhsayOBM
Files can also be viewed and/or copied directly to your Windows machine from the Windows File Explorer

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	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 required an additional AhsayOBM installation on the guest VM environment, with Granular Restore feature, only one backup set is required. ➢ **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 make 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 to either to the original VM location or another a 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 Encryption	Guest VM is encrypted and compressed, therefore is in smaller file size, and encrypted before being uploaded to the backup destination.
Cons	
Slower	As the entire guest VM has to be restored before you can access any it’s

Recovery	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 CAL (client access licenses) are required.

Requirements

Supported Backup Modules

Granular restore is supported on Hyper-V backup sets created and backed up using AhsayOBM v7.13.0.0 or above installed on a Windows platform with the Granular Restore feature enabled on the backup set.

License Requirements

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.

Backup Quota Storage

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.

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

Temporary Directory Requirement

The temporary Directory Folder should have at least the same available size as the guest VM to be restored and should be located on a local drive to ensure optimal performance.

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.

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.

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

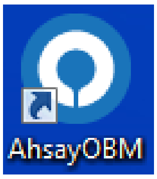
Permissions

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

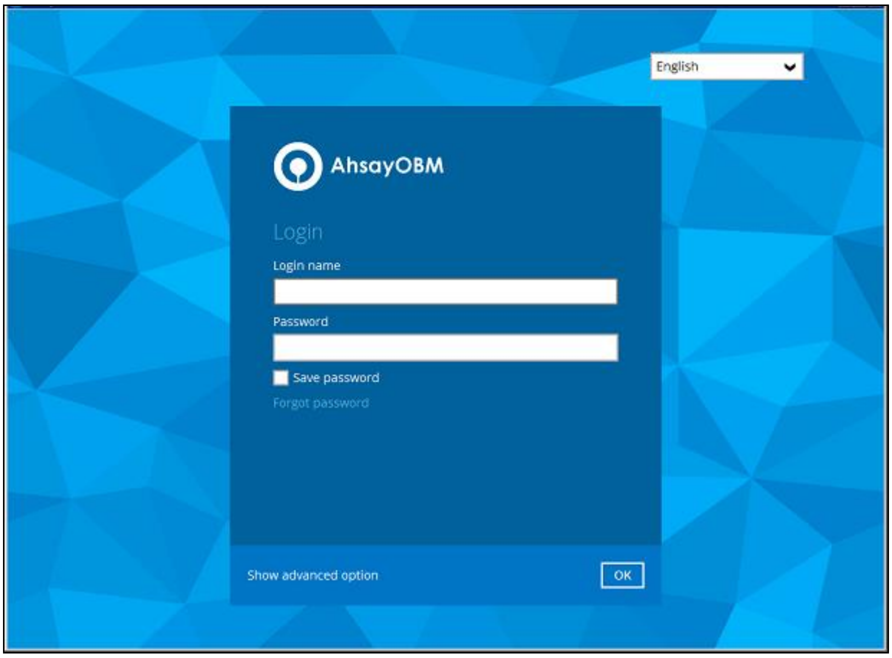
5 Starting AhsayOBM

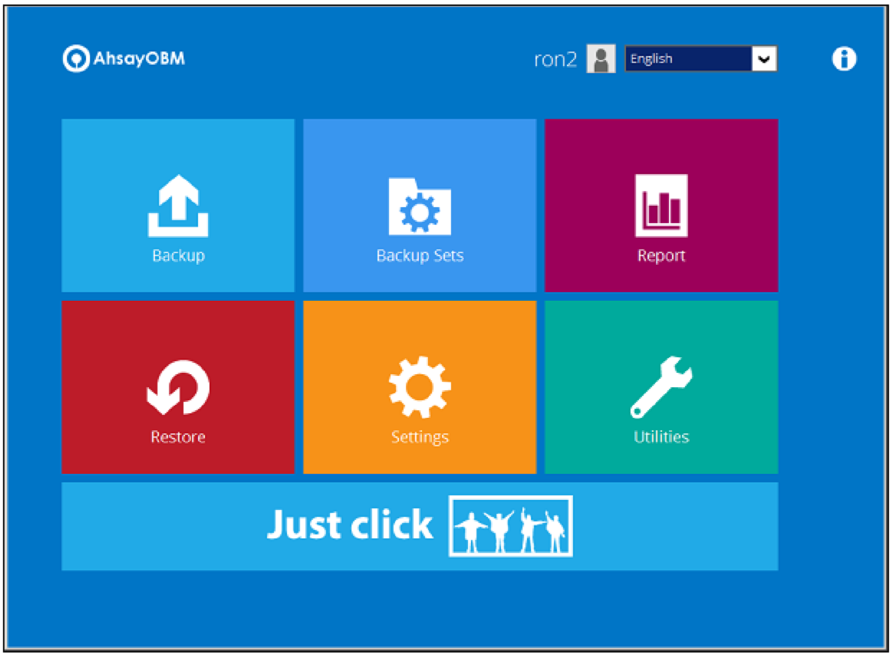
Login to AhsayOBM

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.



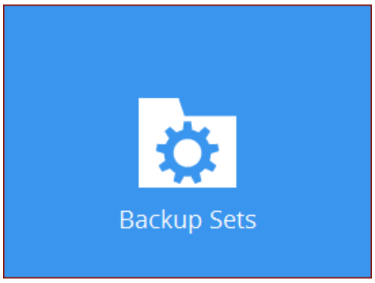


6 Creating a Hyper-V Backup Set

Non-Cluster Environment

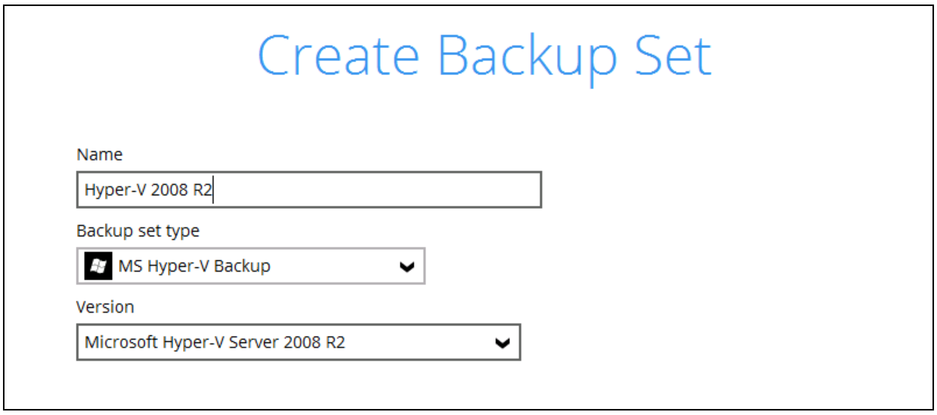
Run Direct Backup Set

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** and name your new backup set then click **Next** to proceed.



Create Backup Set

Name

Hyper-V 2008 R2

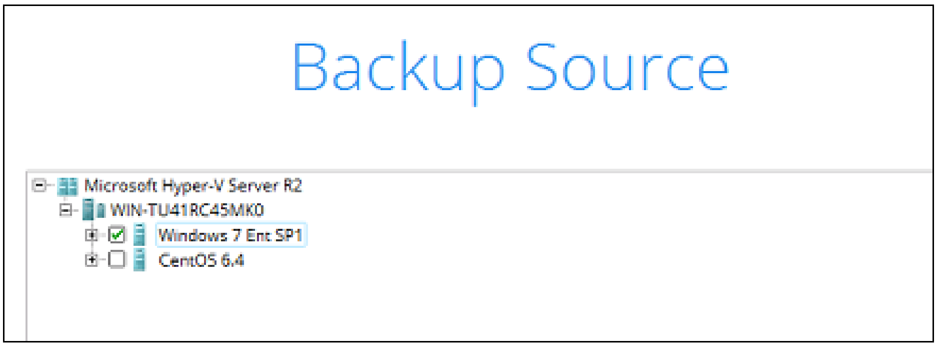
Backup set type

MS Hyper-V Backup

Version

Microsoft Hyper-V Server 2008 R2

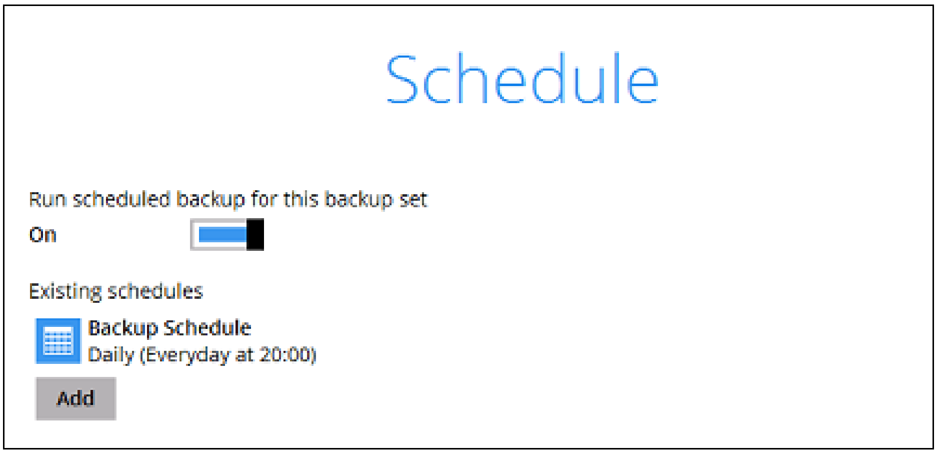
4. In the Backup Source menu, select the guest virtual machines you would like to backup. Click **Next** to proceed.



Backup Source

Microsoft Hyper-V Server R2
WIN-TU41RC45MK0
☑ Windows 7 Ent SP1
□ CentOS 6.4

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



Schedule

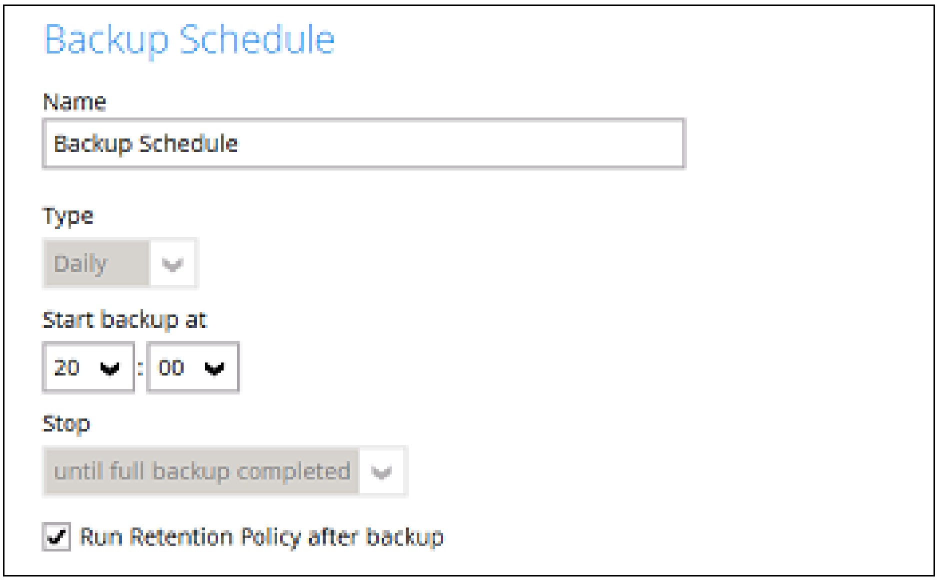
Run scheduled backup for this backup set

On

Existing schedules

Backup Schedule
Daily (Everyday at 20:00)

Click **Add** to add a new schedule or double click on the existing schedule to change the values. Click **Next** to proceed when you are done setting.



Backup Schedule

Name: Backup Schedule

Type: Daily

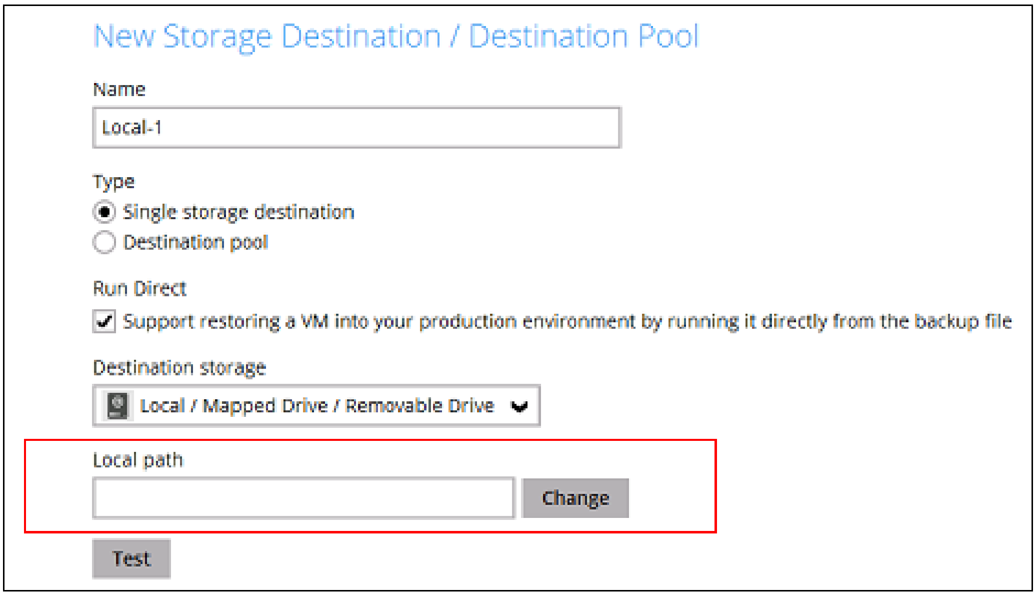
Start backup at: 20 : 00

Stop: until full backup completed

☑ Run Retention Policy after backup

***Note:** The default backup schedule is daily backup at 22:00, the backup job will run until completion and the retention policy job will be run immediately after the backup job*.

6. Select the backup storage destination.



New Storage Destination / Destination Pool

Name

Local-1

Type

● Single storage destination

○ Destination pool

Run Direct

☑ Support restoring a VM into your production environment by running it directly from the backup file

Destination storage

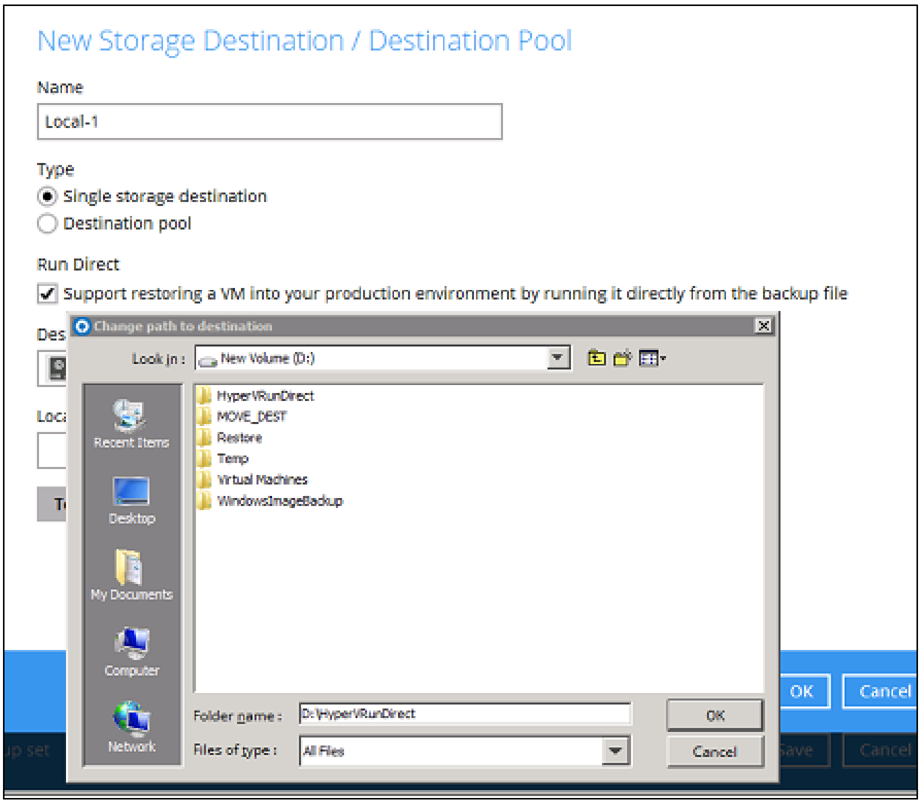
Local / Mapped Drive / Removable Drive

Local path

Note

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

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



New Storage Destination / Destination Pool

Name

Local-1

Type

● Single storage destination

○ Destination pool

Run Direct

☑ Support restoring a VM into your production environment by running it directly from the backup file

Change path to destination

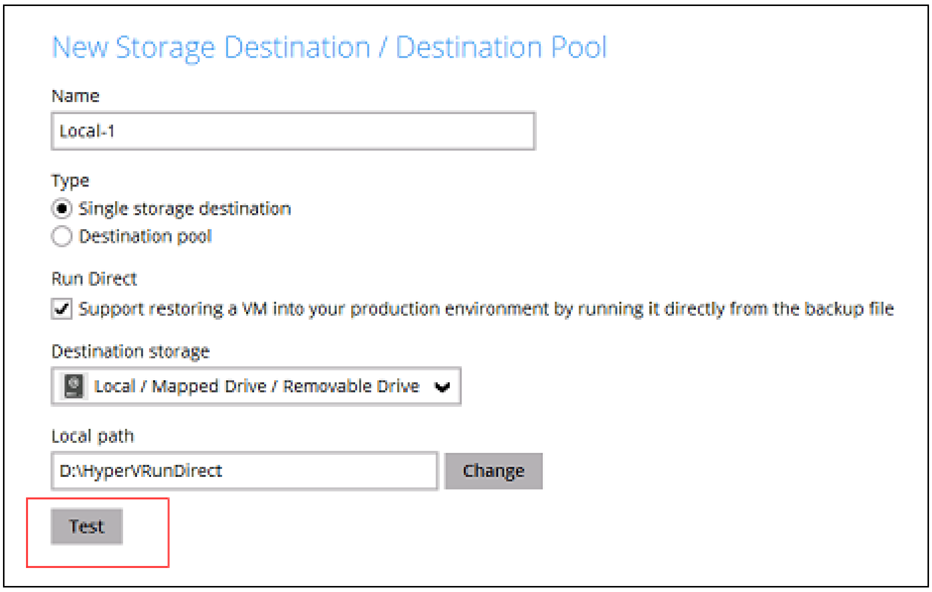
Look in : New Volume (D:)

HyperVRunDirect
MOVE_DEST
Restore
Temp
Virtual Machines
WindowsImageBackup

Folder name : D:\HyperVRunDirect

Files of type : All Files

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

Type

● Single storage destination

○ Destination pool

Run Direct

☑ Support restoring a VM into your production environment by running it directly from the backup file

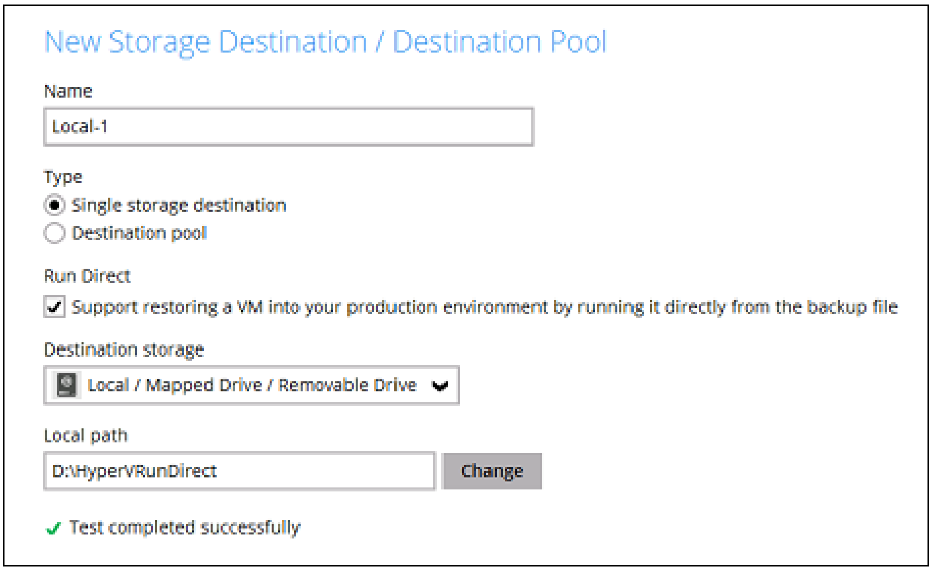
Destination storage

Local / Mapped Drive / Removable Drive

Local path

D:\HyperVRunDirect

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

Type

● Single storage destination

○ Destination pool

Run Direct

☑ Support restoring a VM into your production environment by running it directly from the backup file

Destination storage

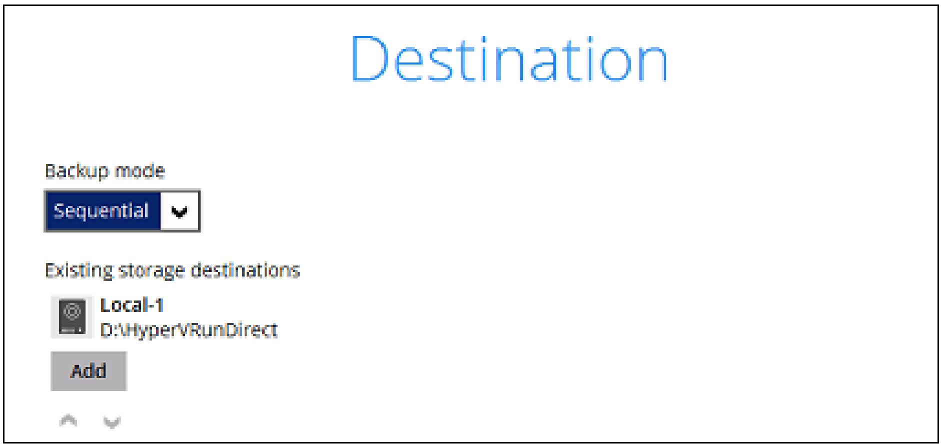
Local / Mapped Drive / Removable Drive

Local path

D:\HyperVRunDirect

✓ Test completed successfully

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



Destination

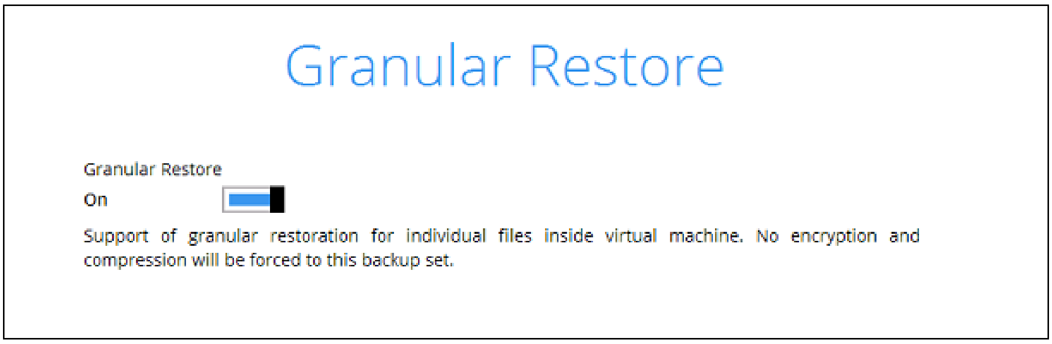
Backup mode

Sequential

Existing storage destinations

Local-1
D:\HyperVRunDirect

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.



Granular Restore

Granular Restore

On

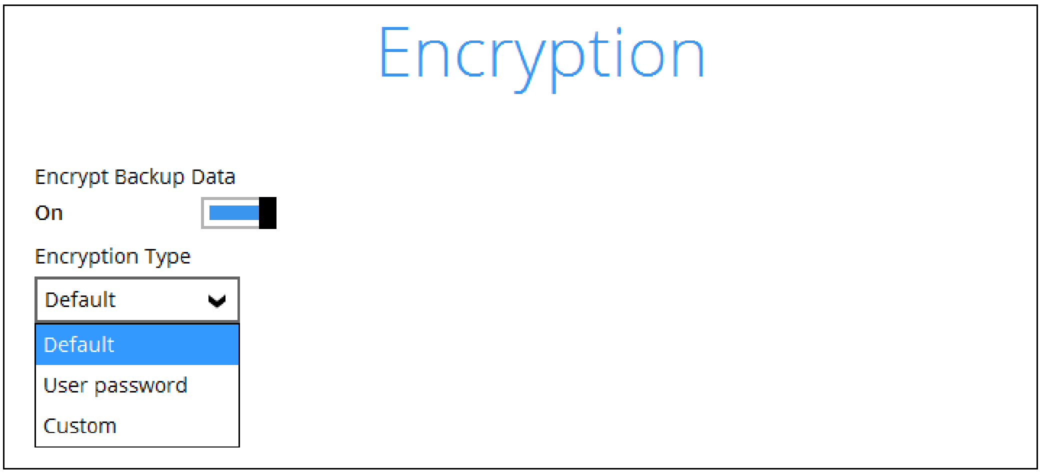
Support of granular restoration for individual files inside virtual machine. No encryption and compression will be forced to this backup set.

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.

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.



Encryption

Encrypt Backup Data

On

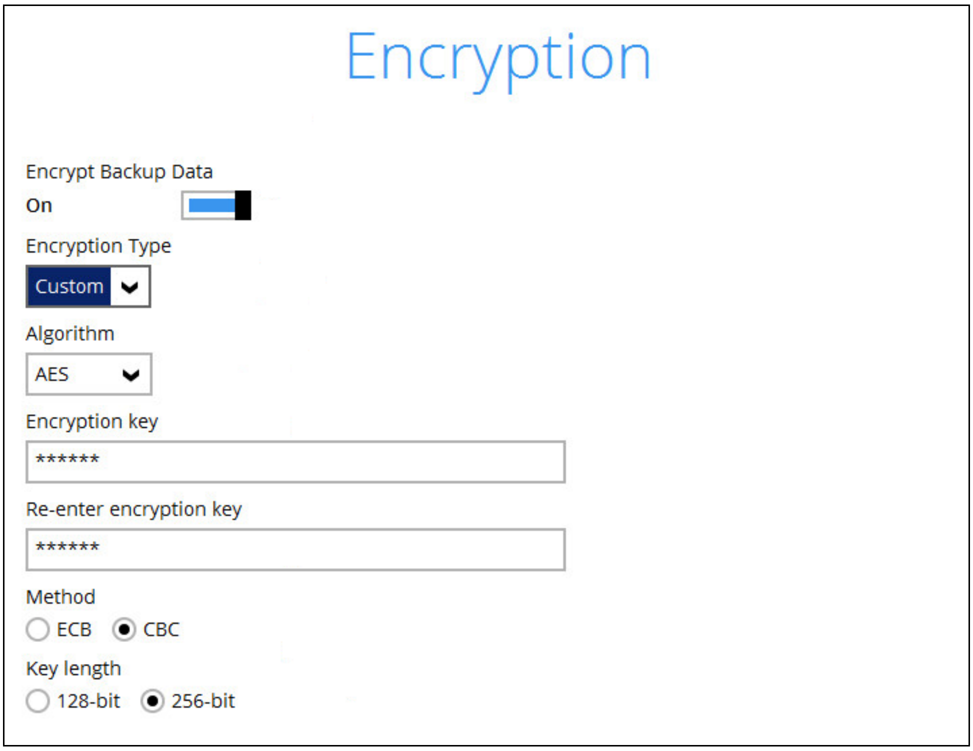
Encryption Type

Default

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

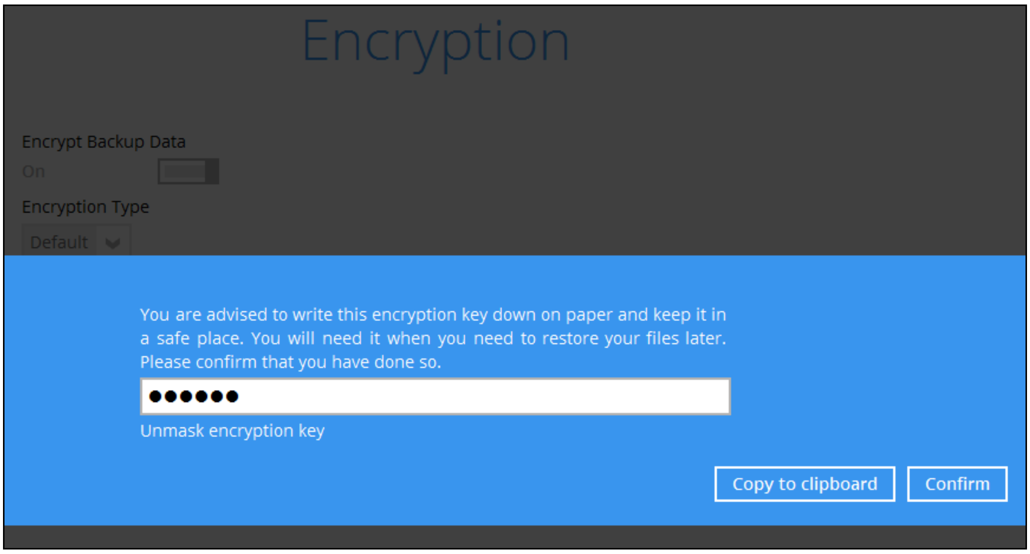
Notes:

1. For best practice on managing your encryption key, refer to the following KB article. https://forum.ahsay.com/viewtopic.php?f=169&t=14090

2. For local, mapped drive, or removable drive storage destinations with Run Direct enabled the compression type will a 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.



Encryption

Encrypt Backup Data

On

Encryption Type

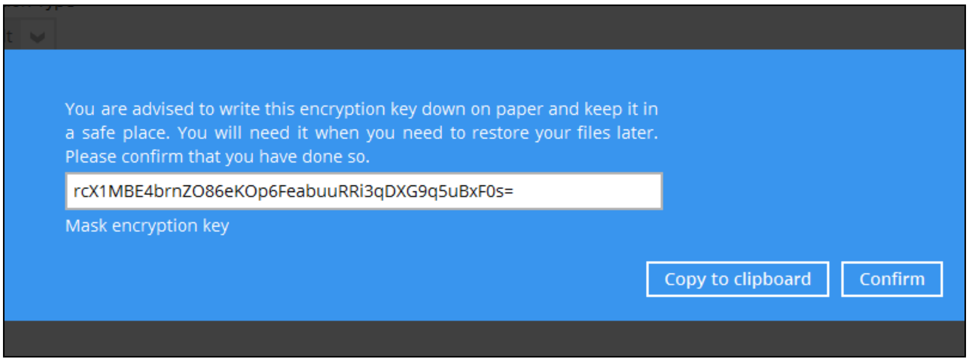
Default

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

●●●●●●

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.



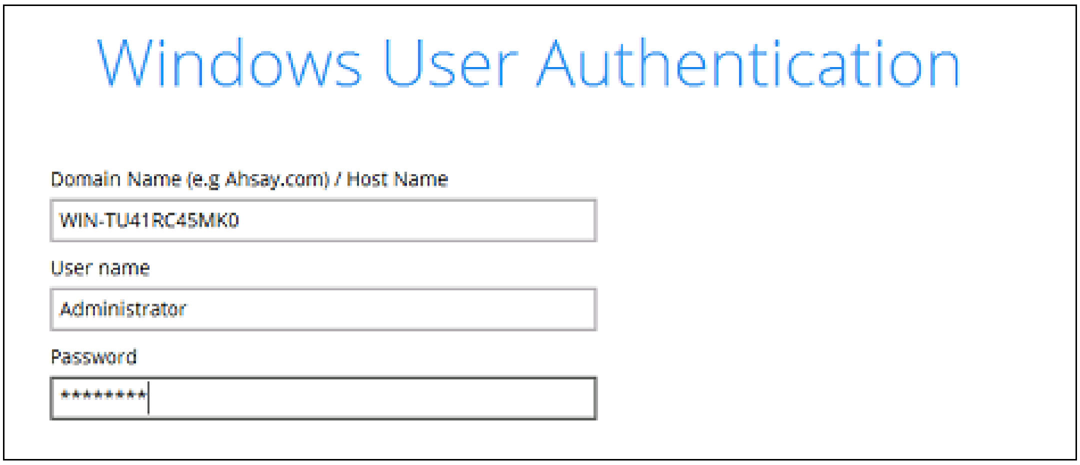
You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.

rcX1MBE4brnZO86eKOp6FeabuuRRi3qDXG9q5uBxF0s=

- **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 or continuous backup job.



Windows User Authentication

Domain Name (e.g Ahsay.com) / Host Name: WIN-TU41RC45MK0

User name: Administrator

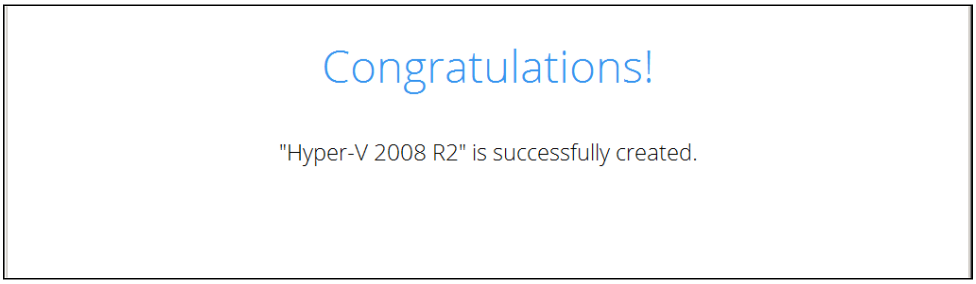
Password: ********

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. **Backup set created.**

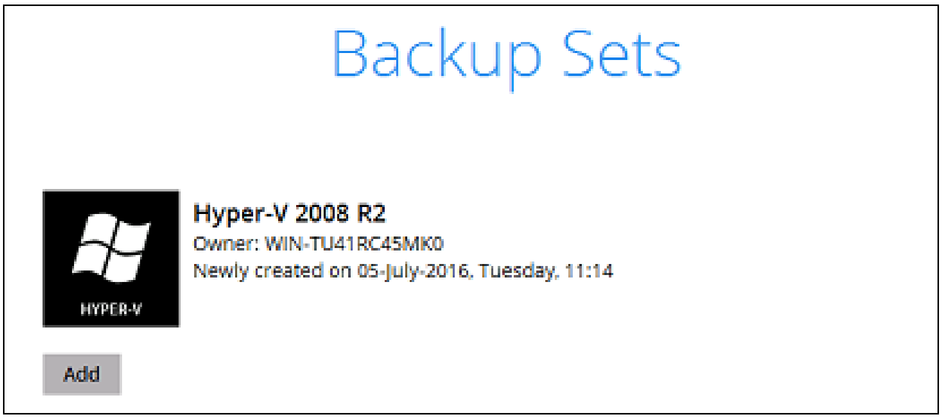
    i. To start a manual backup job click on **Backup now.**



Congratulations!

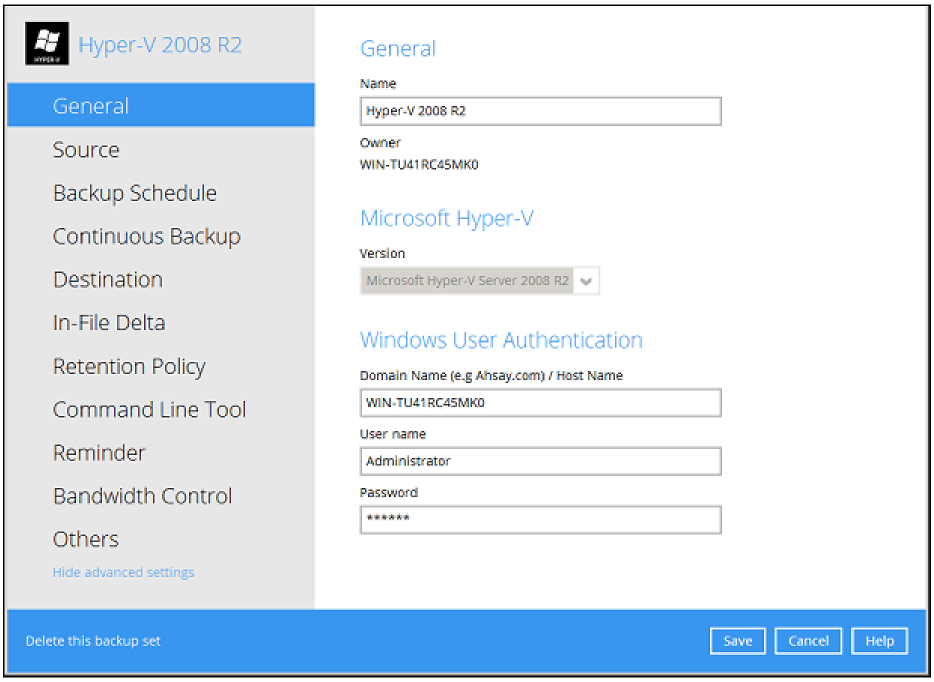
"Hyper-V 2008 R2" is successfully created.

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



Backup Sets

Hyper-V 2008 R2
Owner: WIN-TU41RC45MK0
Newly created on 05-July-2016, Tuesday, 11:14



General

Name: Hyper-V 2008 R2

Owner: WIN-TU41RC45MK0

Microsoft Hyper-V

Version: Microsoft Hyper-V Server 2008 R2

Windows User Authentication

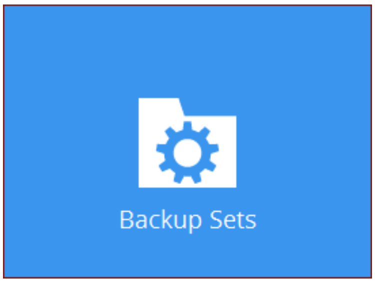
Domain Name (e.g Ahsay.com) / Host Name: WIN-TU41RC45MK0

User name: Administrator

Password: ******

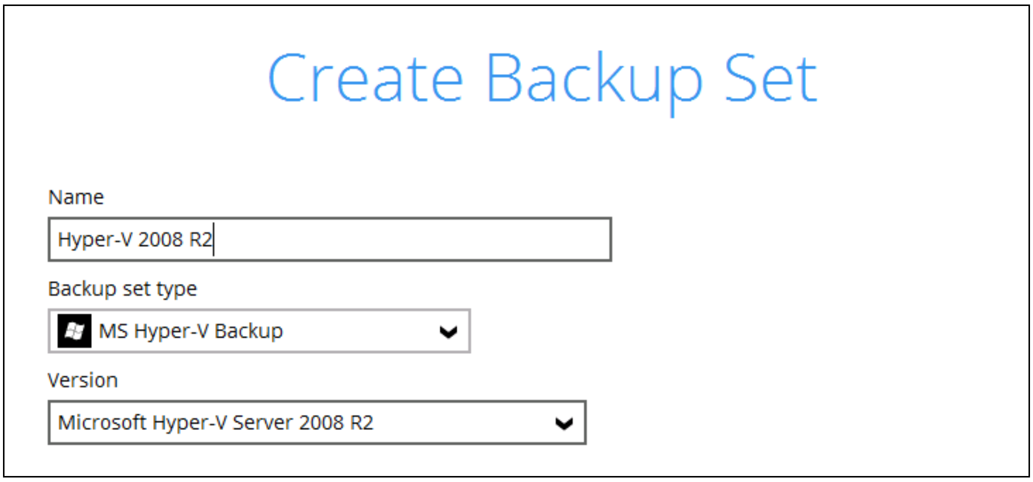
Non Run Direct Backup Set

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.



Create Backup Set

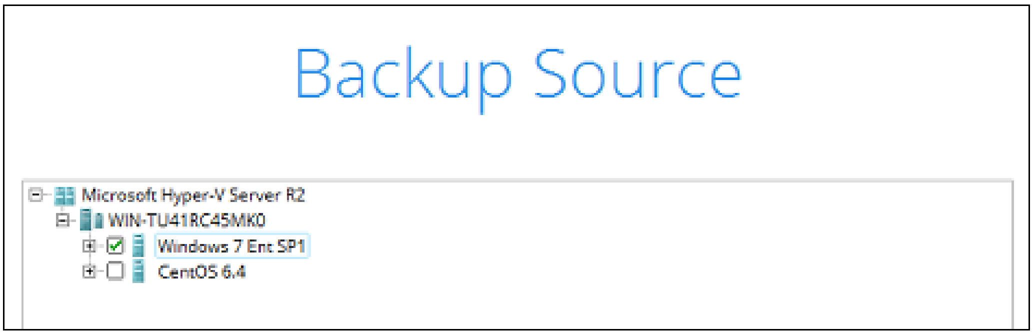
Name: Hyper-V 2008 R2

Backup set type: MS Hyper-V Backup

Version: Microsoft Hyper-V Server 2008 R2

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

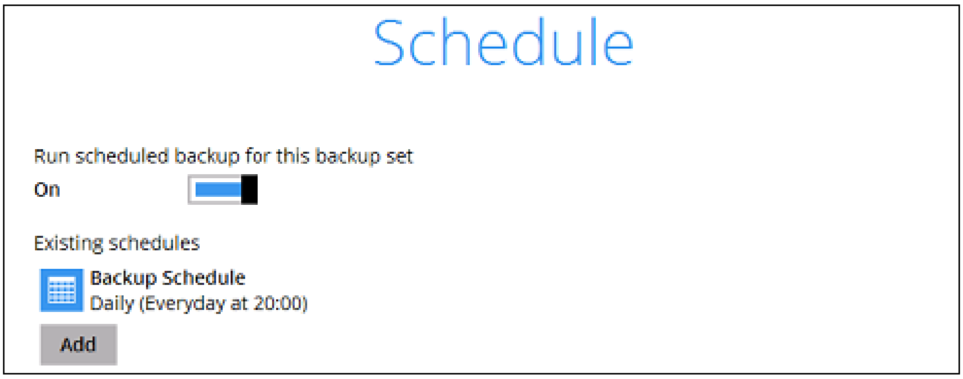
4. In the Backup Source menu, select the guest virtual machines you would like to backup. Click **Next** to proceed.



Backup Source

- Microsoft Hyper-V Server R2
  - WIN-TU41RC45MK0
    - ☑ Windows 7 Ent SP1
    - □ CentOS 6.4

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



Schedule

Run scheduled backup for this backup set

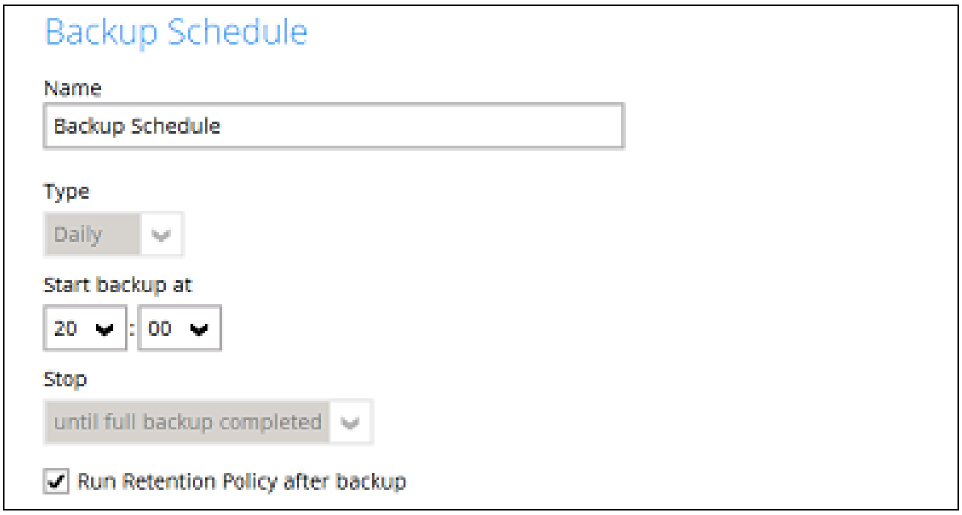
On

Existing schedules

Backup Schedule
Daily (Everyday at 20:00)

Add

Click **Add** to add a new schedule or double click on the existing schedule to change the values. Click **Next** to proceed when you are done setting.



Backup Schedule

Name: Backup Schedule

Type: Daily

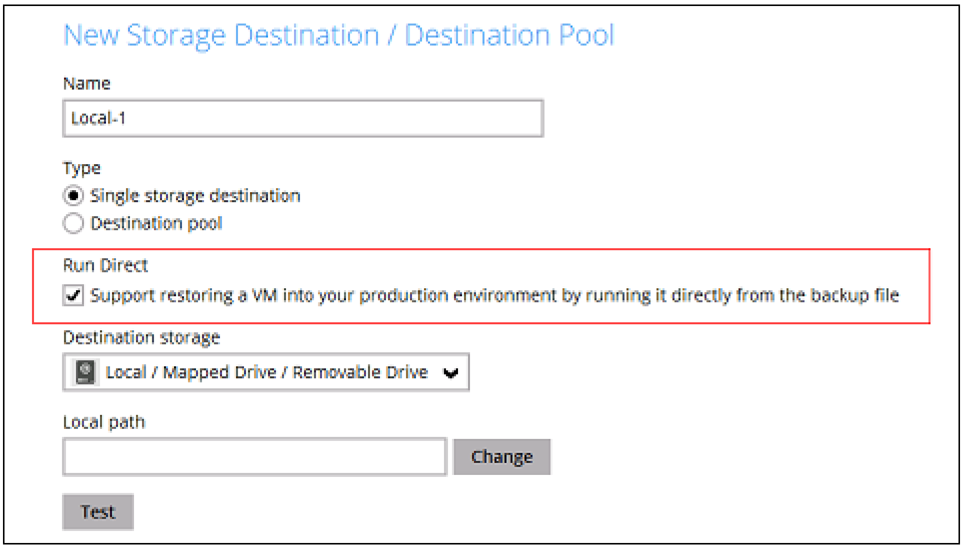
Start backup at: 20 : 00

Stop: until full backup completed

☑ Run Retention Policy after backup

Note: *The default backup schedule is daily backup at 22:00 with the backup job will run until completion and the retention policy job will be run immediately after the backup job*.

6. Select the backup storage destination.



New Storage Destination / Destination Pool

Name: Local-1

Type

● Single storage destination

○ Destination pool

Run Direct

☑ Support restoring a VM into your production environment by running it directly from the backup file

Destination storage: Local / Mapped Drive / Removable Drive

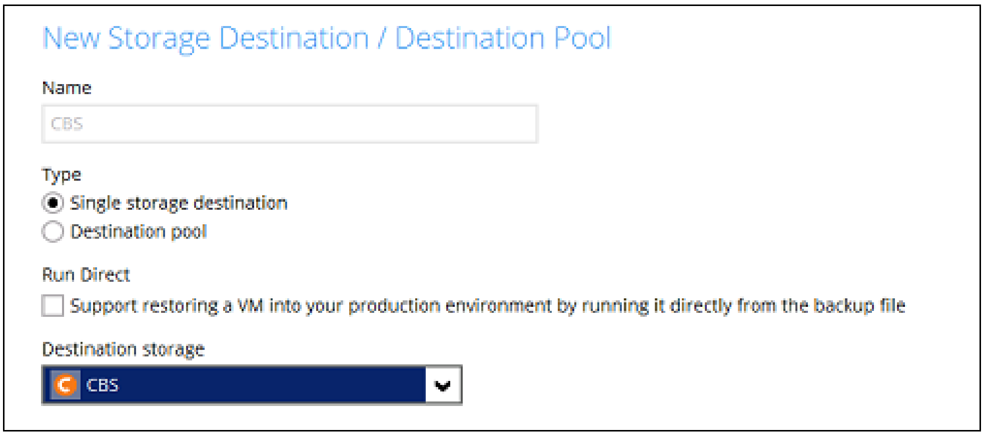
Local path:

Change

Test

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

CBS

Type

● Single storage destination

○ Destination pool

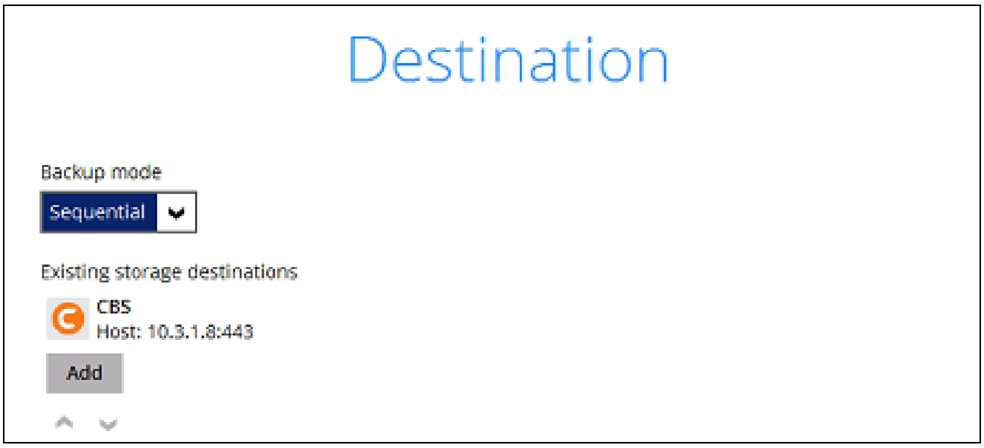
Run Direct

□ Support restoring a VM into your production environment by running it directly from the backup file

Destination storage

CBS

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



Destination

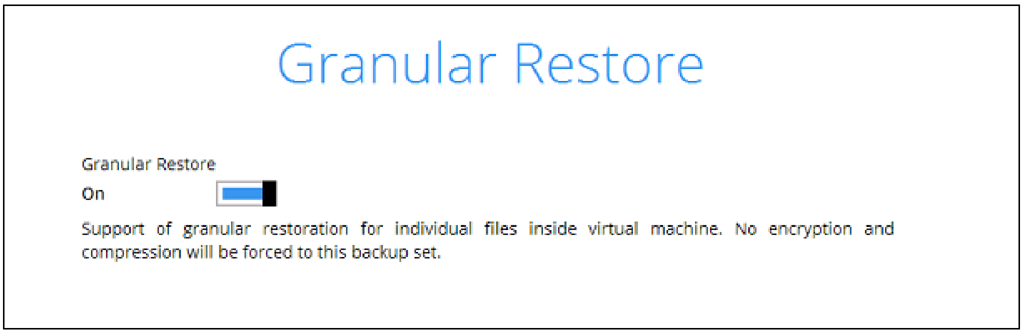
Backup mode

Sequential

Existing storage destinations

CBS
Host: 10.3.1.8:443

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

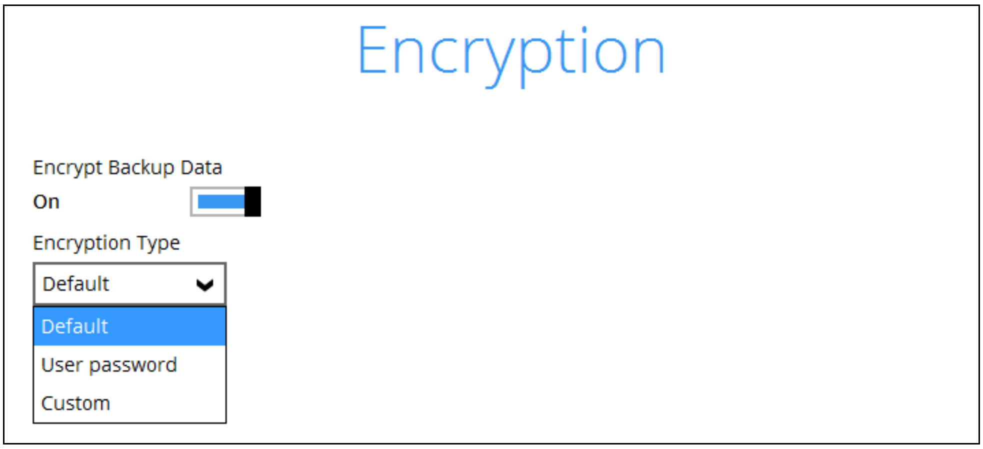
Support of granular restoration for individual files inside virtual machine. No encryption and compression will be forced to this backup set.

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.

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

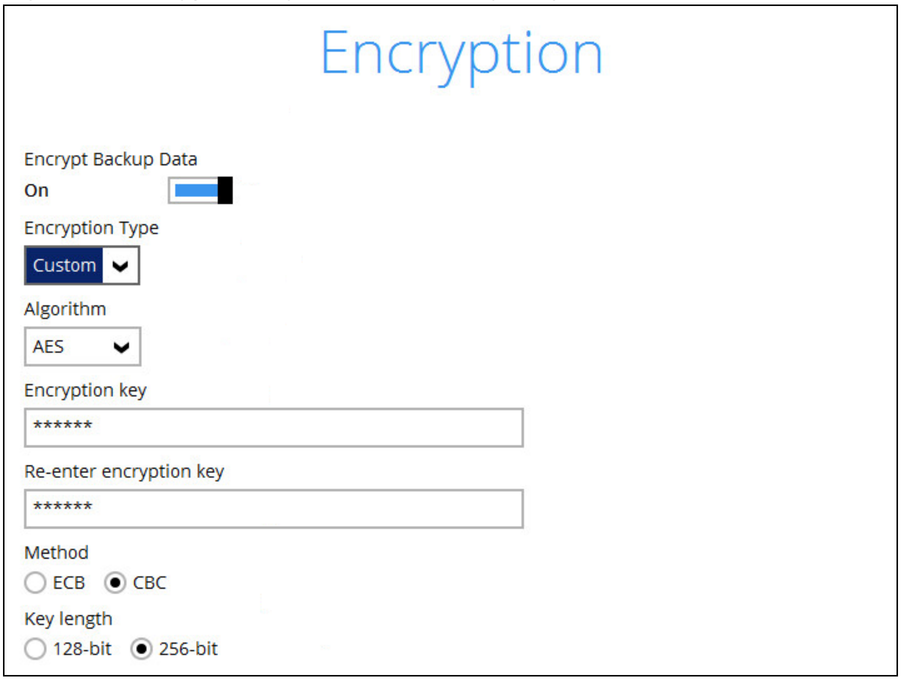
On

Encryption Type

Default

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

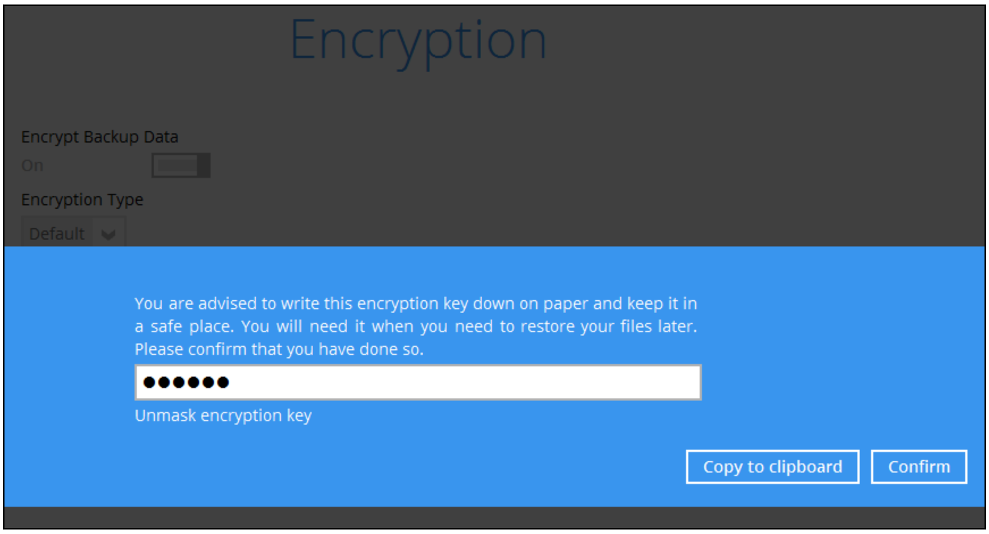
Notes:

i. *For best practice on managing your encryption key, refer to the following KB article. https://forum.ahsay.com/viewtopic.php?f=169&t=14090*

ii. *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.

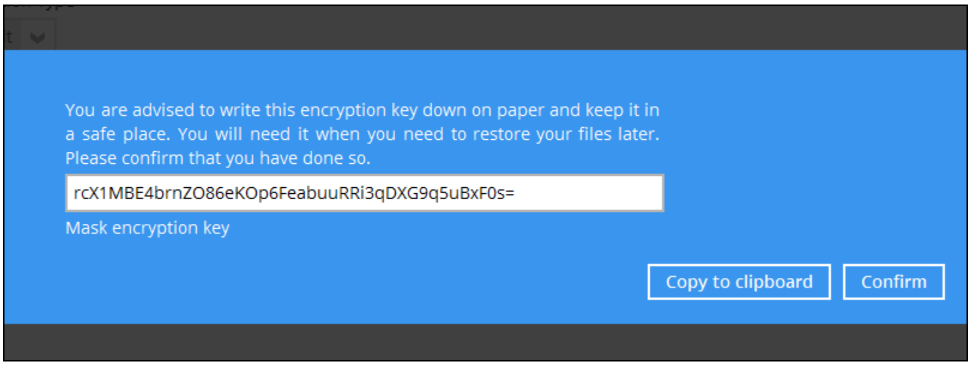


You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.

●●●●●●

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.



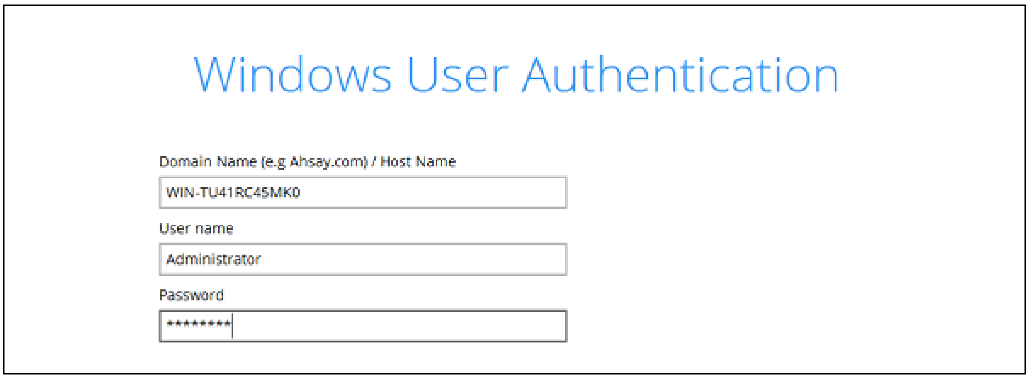
You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.

rcX1MBE4brnZO86eKOp6FeabuuRRi3qDXG9q5uBxF0s=

- **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.



Windows User Authentication

Domain Name (e.g Ahsay.com) / Host Name: WIN-TU41RC45MK0

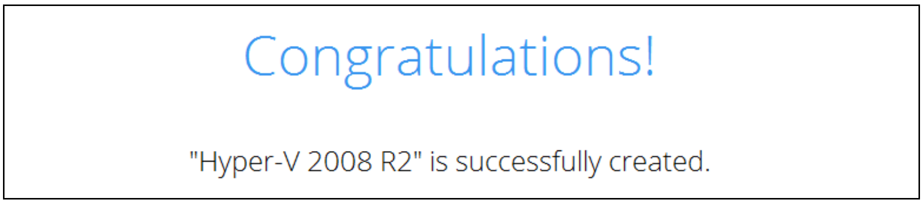
User name: Administrator

Password: ********

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. **Backup set created.**

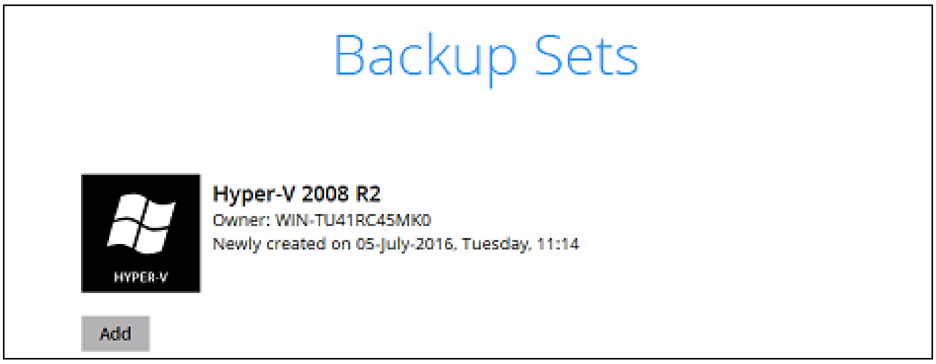
    i. To start a manual backup job click on **Backup now**.



Congratulations!

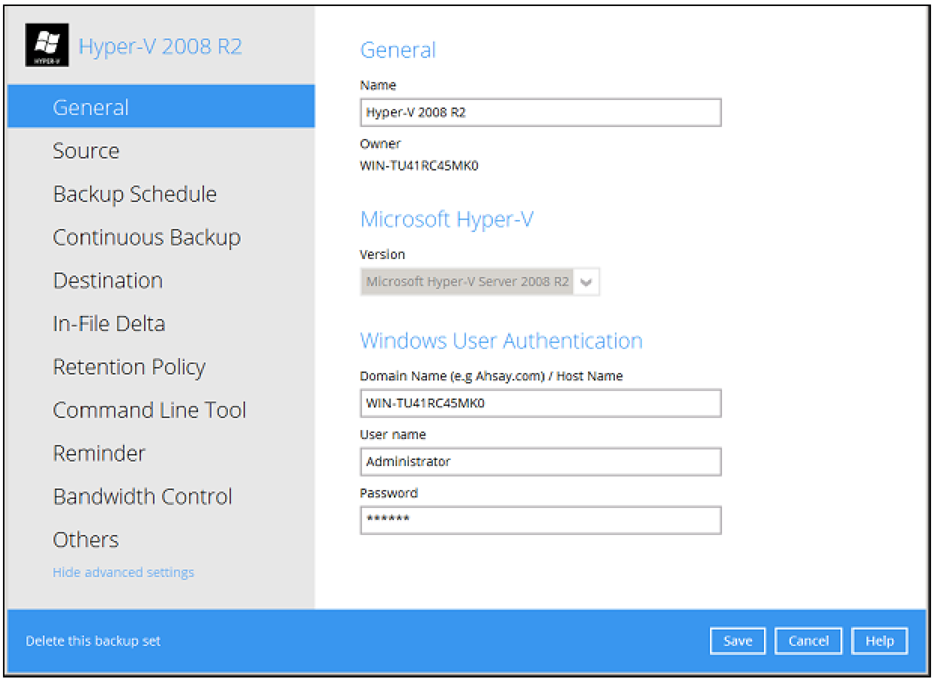
"Hyper-V 2008 R2" is successfully created.

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



Backup Sets

Hyper-V 2008 R2
Owner: WIN-TU41RC45MK0
Newly created on 05-July-2016, Tuesday, 11:14



General

Name

Hyper-V 2008 R2

Owner

WIN-TU41RC45MK0

Microsoft Hyper-V

Version

Microsoft Hyper-V Server 2008 R2

Windows User Authentication

Domain Name (e.g Ahsay.com) / Host Name

WIN-TU41RC45MK0

User name

Administrator

Password

******

Cluster Environment

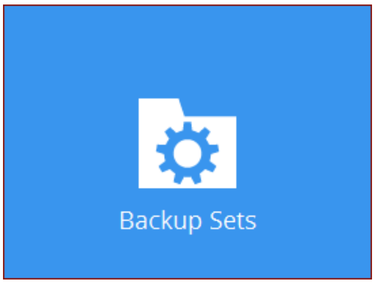
Requirements

For Hyper-V Cluster backup sets:

1. The same version of AhsayOBM must be installed on all Hyper-V Cluster nodes.
2. The same backup user account must be used.
3. The backup schedule must be enabled on all Hyper-V Cluster nodes.

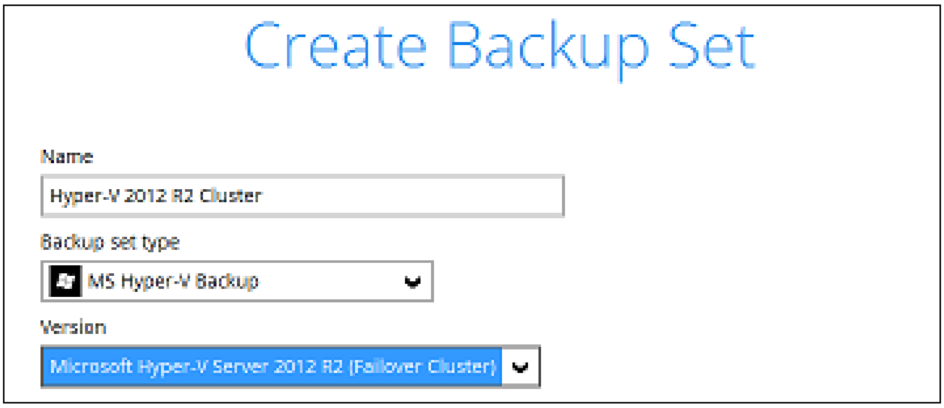
Run Direct Backup Set

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.



Create Backup Set

Name

Hyper-V 2012 R2 Cluster

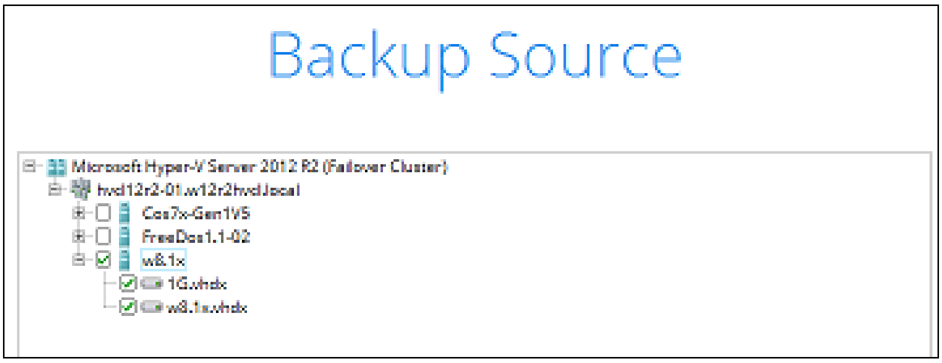
Backup set type

MS Hyper-V Backup

Version

Microsoft Hyper-V Server 2012 R2 (Failover Cluster)

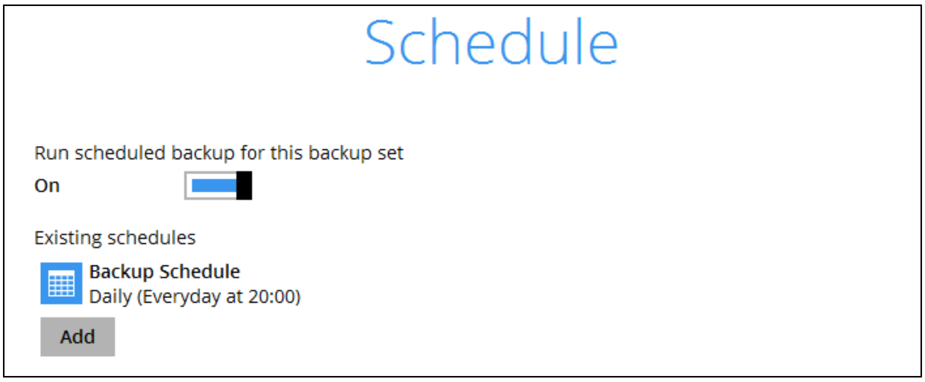
4. In the Backup Source menu, select the guest virtual machines you would like to backup. Click **Next** to proceed.



Backup Source

- Microsoft Hyper-V Server 2012 R2 (Failover Cluster)
  - hvd12r2-01.w12r2hvd.local
    - □ Cos7x-Gen1VS
    - □ FreeDos1.1-02
    - ☑ w8.1x
      - ☑ 1G.vhdx
      - ☑ w8.1x.vhdx

5. Click **Add** to add a new schedule or double click on the existing schedule to change the values. Click **Next** to proceed when you are done setting.



Schedule

Run scheduled backup for this backup set

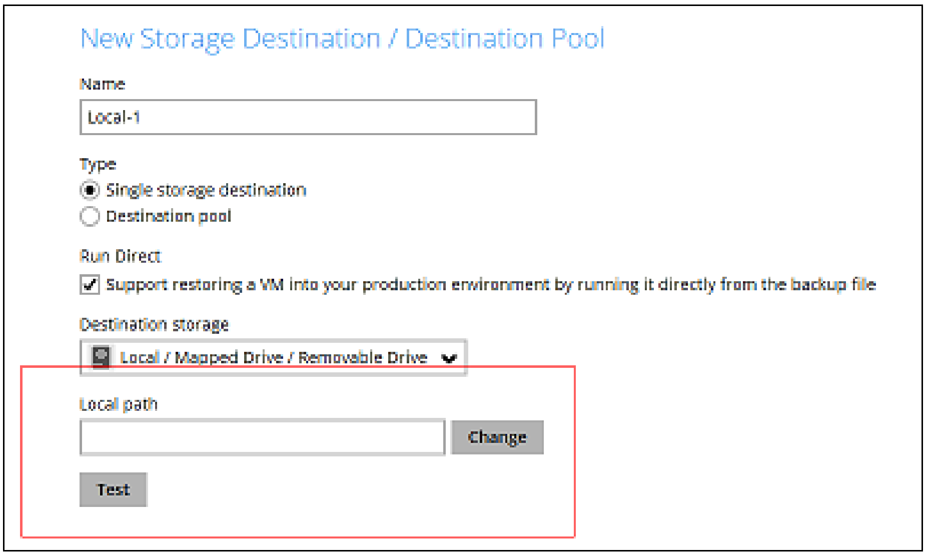
On

Existing schedules

Backup Schedule
Daily (Everyday at 20:00)

Note: *The default backup schedule is daily backup at 22:00 with the backup job will run until completion and the retention policy job will be run immediately after the backup job*.

6. Select the backup storage destination.



New Storage Destination / Destination Pool

Name

Local-1

Type

● Single storage destination

○ Destination pool

Run Direct

☑ Support restoring a VM into your production environment by running it directly from the backup file

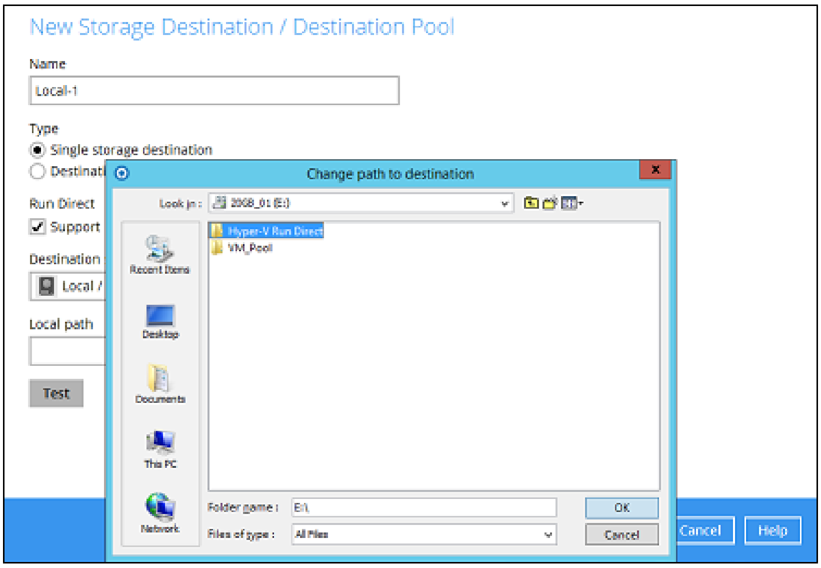
Destination storage

Local / Mapped Drive / Removable Drive

Local path

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.



New Storage Destination / Destination Pool

Name

Local-1

Type

● Single storage destination

○ Destinati

Run Direct

☑ Support

Destination

Local /

Local path

Change path to destination

Look in : 2008_01 (E:)

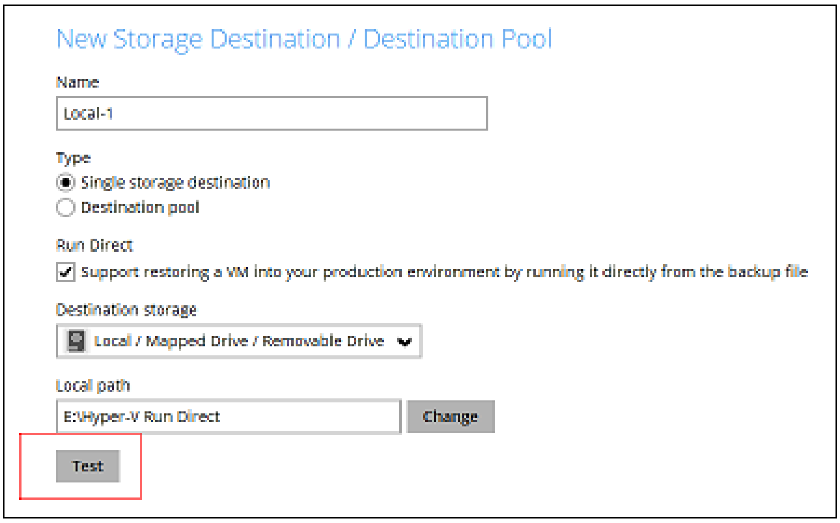
Hyper-V Run Direct

VM_Pool

Folder name : E:\

Files of type : All Files

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

Type

● Single storage destination

○ Destination pool

Run Direct

☑ Support restoring a VM into your production environment by running it directly from the backup file

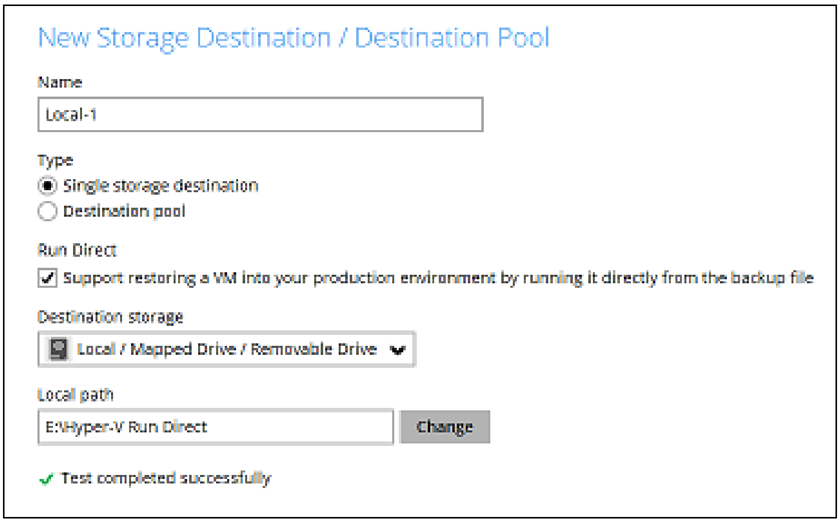
Destination storage

Local / Mapped Drive / Removable Drive

Local path

E:\Hyper-V Run Direct

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

Type

● Single storage destination

○ Destination pool

Run Direct

☑ Support restoring a VM into your production environment by running it directly from the backup file

Destination storage

Local / Mapped Drive / Removable Drive

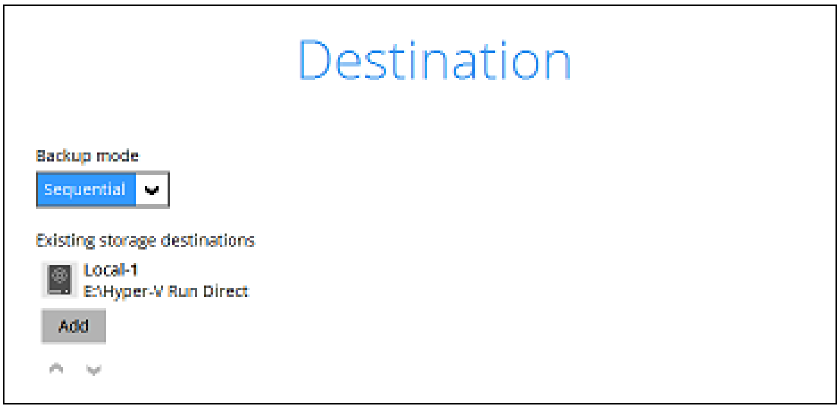
Local path

E:\Hyper-V Run Direct

✓ 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

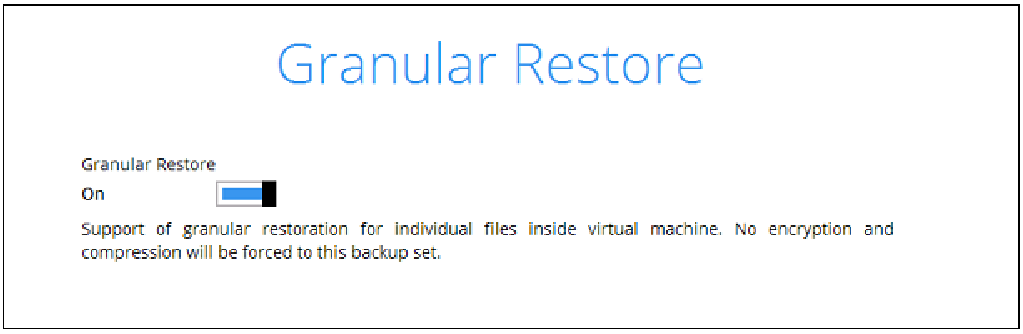
Backup mode

Sequential

Existing storage destinations

Local-1
E:\Hyper-V Run Direct

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.



Granular Restore

Granular Restore

On

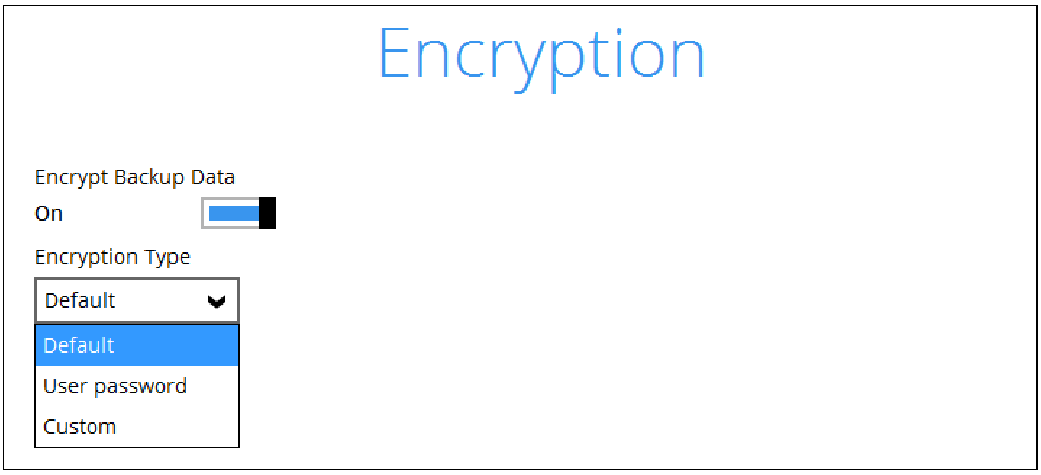
Support of granular restoration for individual files inside virtual machine. No encryption and compression will be forced to this backup set.

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.

8. **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

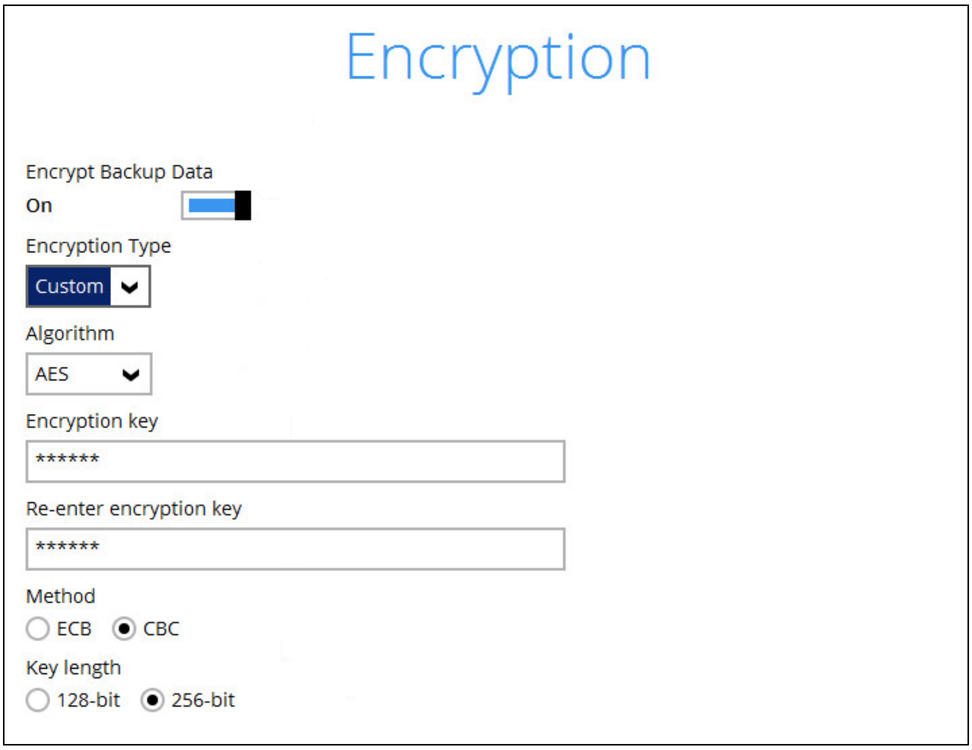
Encryption Type

Default

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

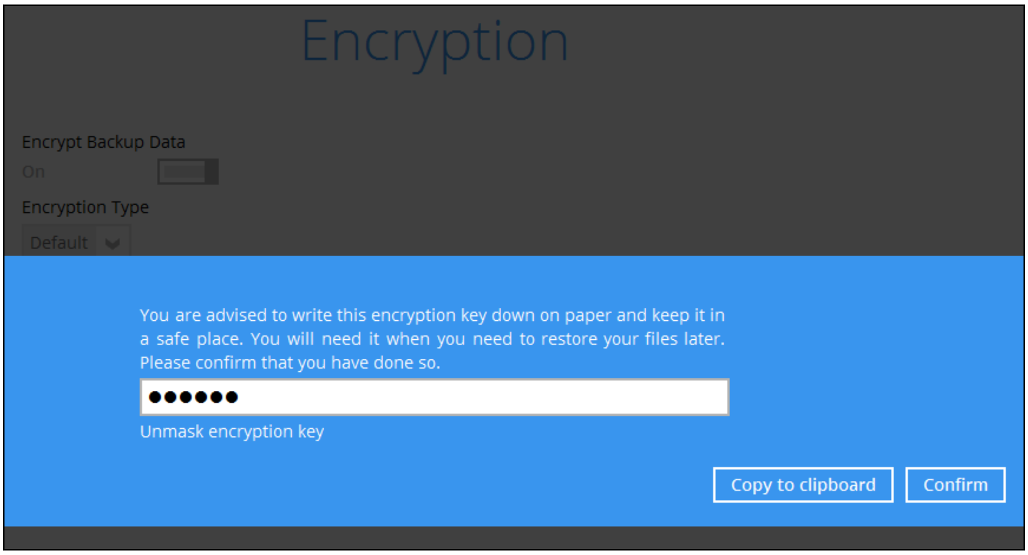
Notes:

i. *For best practice on managing your encryption key, refer to the following KB article. https://forum.ahsay.com/viewtopic.php?f=169&t=14090*

ii. *For local, mapped drive, or removable drive storage destinations with Run Direct enabled the compression type will always 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.



Encryption

Encrypt Backup Data
On

Encryption Type
Default

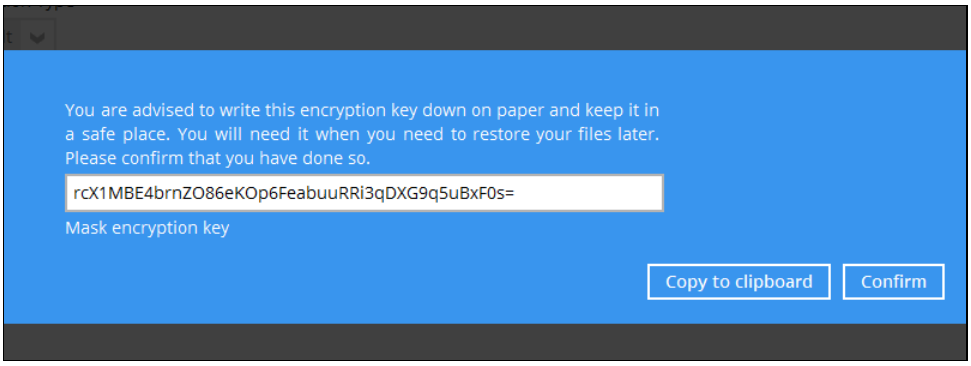
You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.

●●●●●●

Unmask encryption key

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.



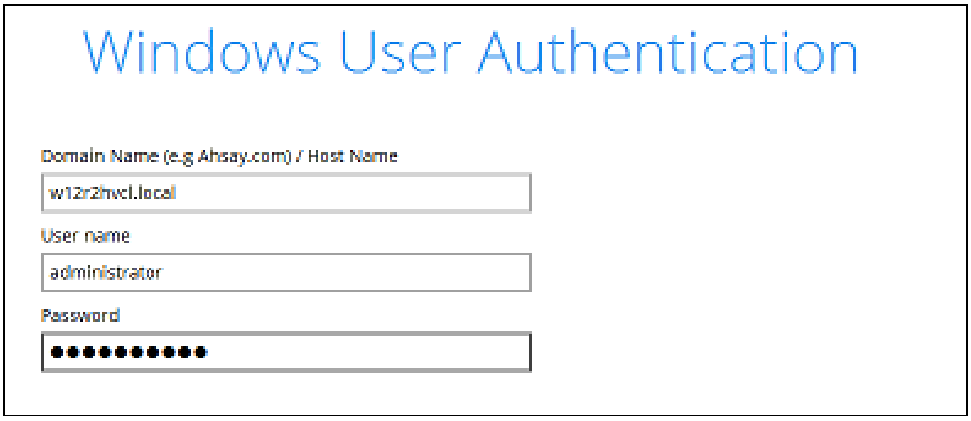
You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.

rcX1MBE4brnZO86eKOp6FeabuuRRi3qDXG9q5uBxF0s=

- **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 or continuous backup job.



Windows User Authentication

Domain Name (e.g Ahsay.com) / Host Name: w12r2hvcl.local

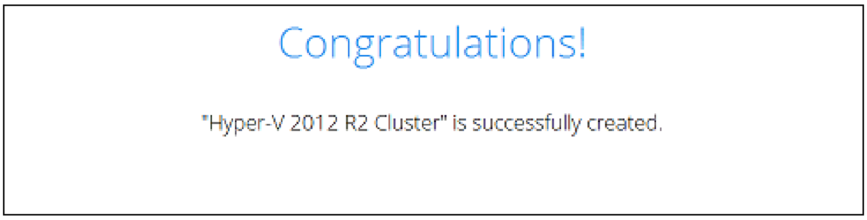
User name: administrator

Password: ●●●●●●●●●●

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.*

11. **Backup set created.**

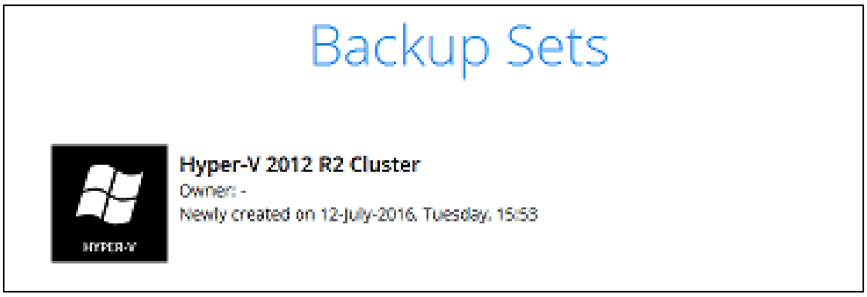
    i. To start a manual backup job click on **Backup now.**



Congratulations!

"Hyper-V 2012 R2 Cluster" is successfully created.

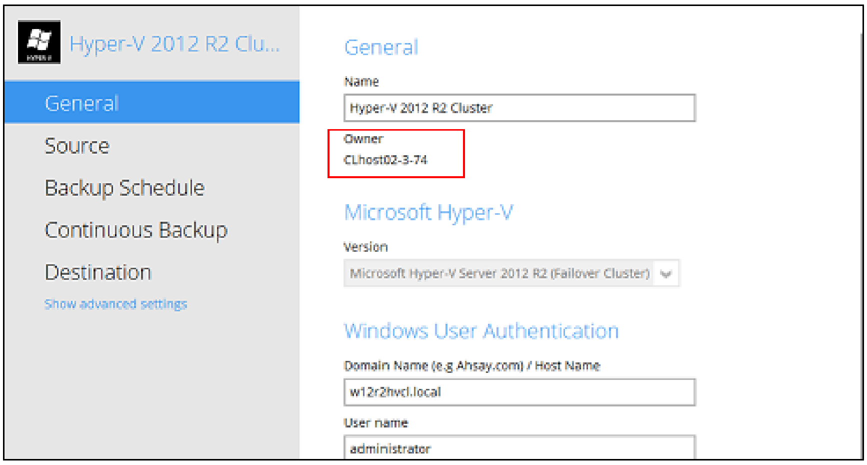
ii. To verify the backup set settings click on Close and then click on the Hyper-V backup set to complete the setup.



Backup Sets

Hyper-V 2012 R2 Cluster
Owner: -
Newly created on 12-July-2016, Tuesday, 15:53

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



General

Name: Hyper-V 2012 R2 Cluster

Owner: CLhost02-3-74

Microsoft Hyper-V

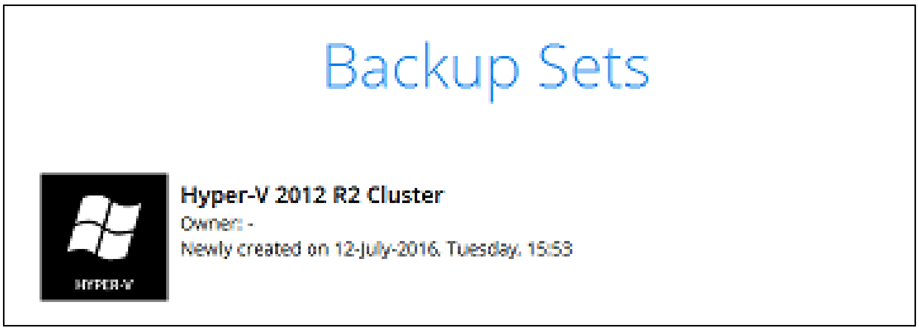
Version: Microsoft Hyper-V Server 2012 R2 (Failover Cluster)

Windows User Authentication

Domain Name (e.g Ahsay.com) / Host Name: w12r2hvcl.local

User name: administrator

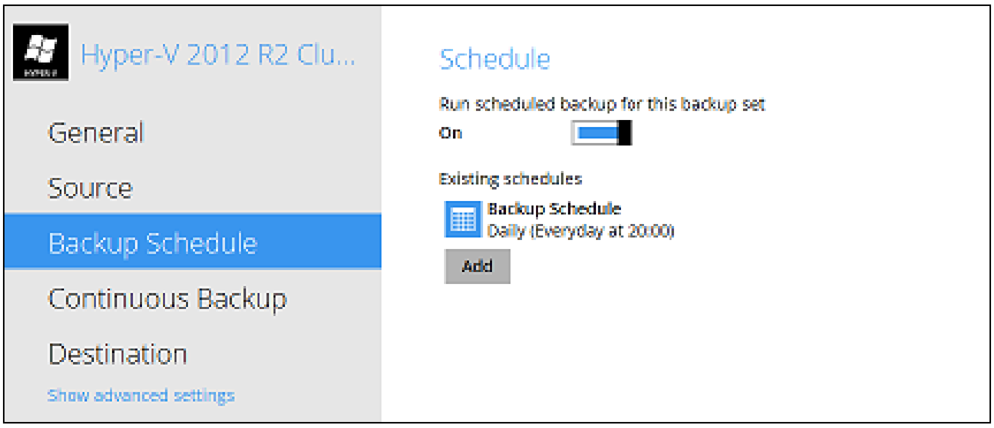
iv. On the next Hyper-V node startup AhsayOBM and select the Hyper-V backup set.



Backup Sets

Hyper-V 2012 R2 Cluster
Owner: -
Newly created on 12-July-2016, Tuesday, 15:53

12. 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.



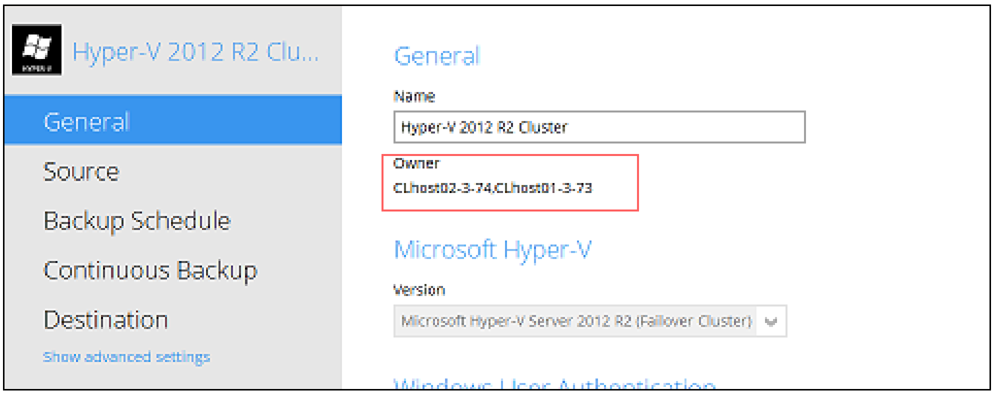
Schedule

Run scheduled backup for this backup set: On

Existing schedules

Backup Schedule
Daily (Everyday at 20:00)

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



Name: Hyper-V 2012 R2 Cluster

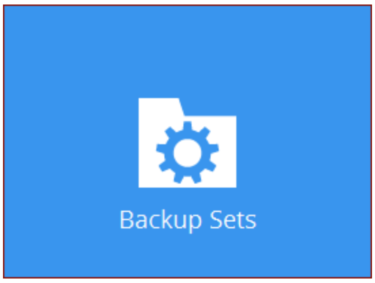
Owner: CLhost02-3-74,CLhost01-3-73

Version: Microsoft Hyper-V Server 2012 R2 (Failover Cluster)

14. Repeat steps 11 to 12 for all Hyper-V Cluster nodes.

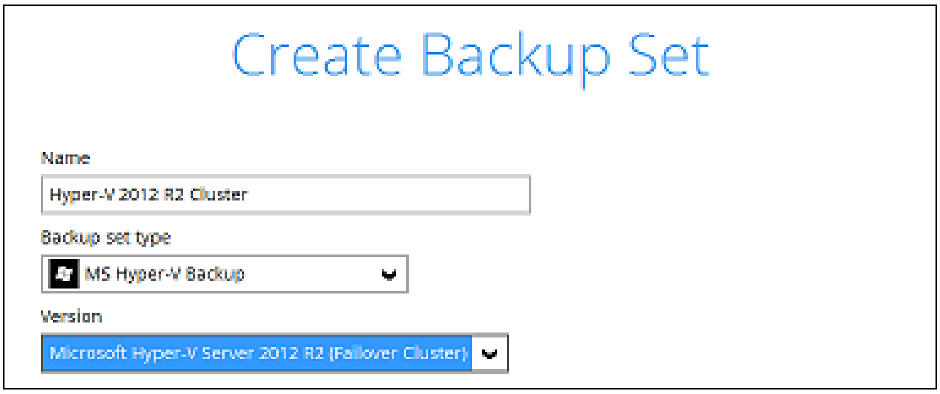
Non Run Direct Backup Set

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.



Create Backup Set

Name

Hyper-V 2012 R2 Cluster

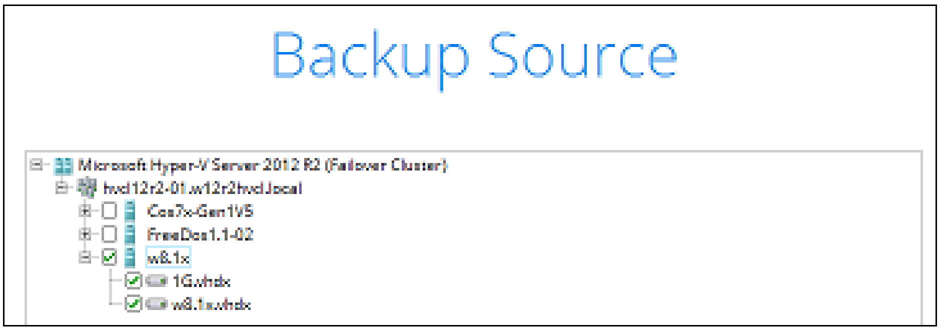
Backup set type

MS Hyper-V Backup

Version

Microsoft Hyper-V Server 2012 R2 (Failover Cluster)

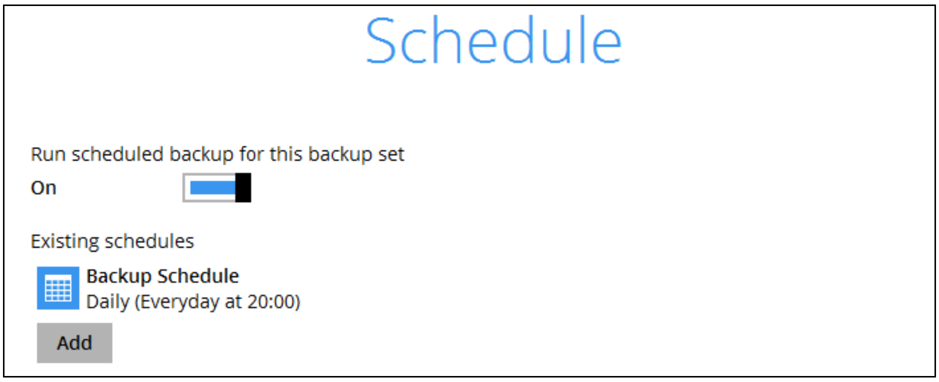
4. In the Backup Source menu, select the guest virtual machines you would like to backup. Click **Next** to proceed.



Backup Source

```
⊟ Microsoft Hyper-V Server 2012 R2 (Failover Cluster)
  ⊟ hvd12r2-01.w12r2hvd.local
    ⊞ □ Cos7x-Gen1VS
    ⊞ □ FreeDos1.1-02
    ⊟ ☑ w8.1x
        ☑ 1G.vhdx
        ☑ w8.1x.vhdx
```

5. Click **Add** to add a new schedule or double click on the existing schedule to change the values. Click **Next** to proceed when you are done setting.



Schedule

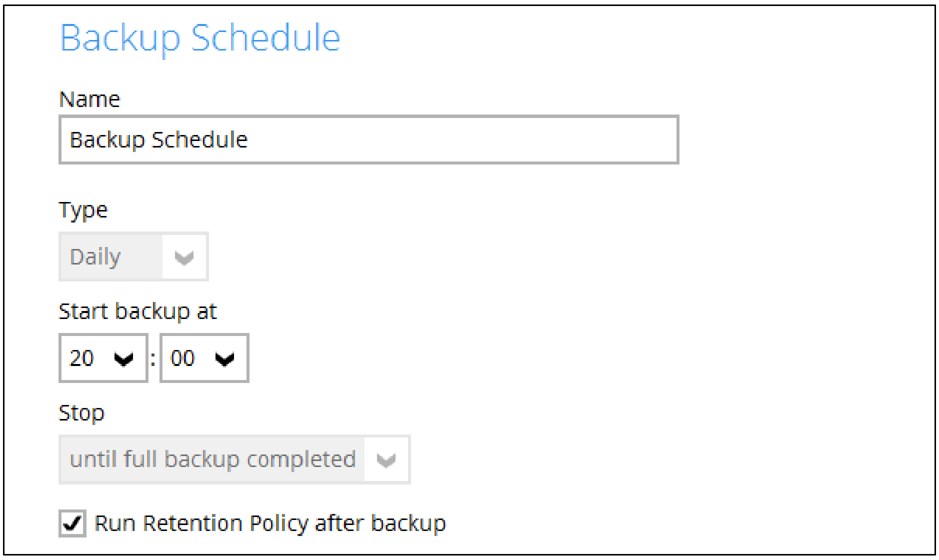
Run scheduled backup for this backup set

On

Existing schedules

Backup Schedule
Daily (Everyday at 20:00)

Click **Add** to add a new schedule or double click on the existing schedule to change the values. Click **Next** to proceed when you are done setting.



Backup Schedule

Name

Backup Schedule

Type

Daily

Start backup at

20 : 00

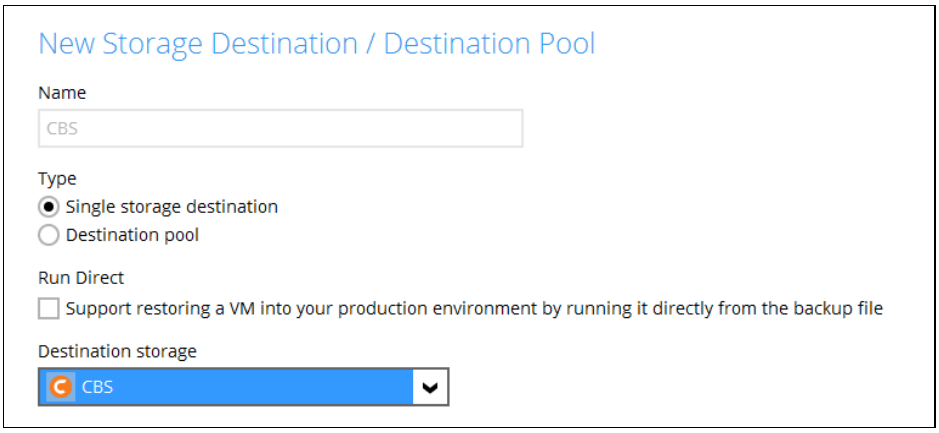
Stop

until full backup completed

☑ Run Retention Policy after backup

Note: *The default backup schedule is daily backup at 22:00 with the backup job will run until completion and the retention policy job will be run immediately after the backup job.*

6. 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

CBS

Type

● Single storage destination

○ Destination pool

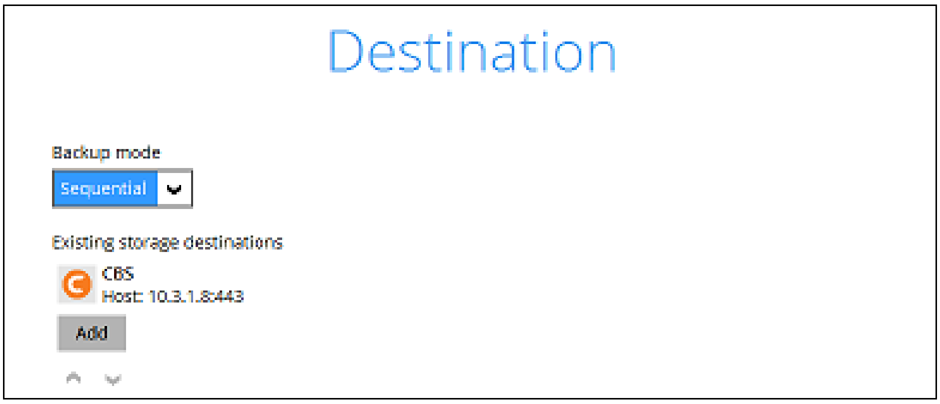
Run Direct

□ Support restoring a VM into your production environment by running it directly from the backup file

Destination storage

CBS

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



Destination

Backup mode

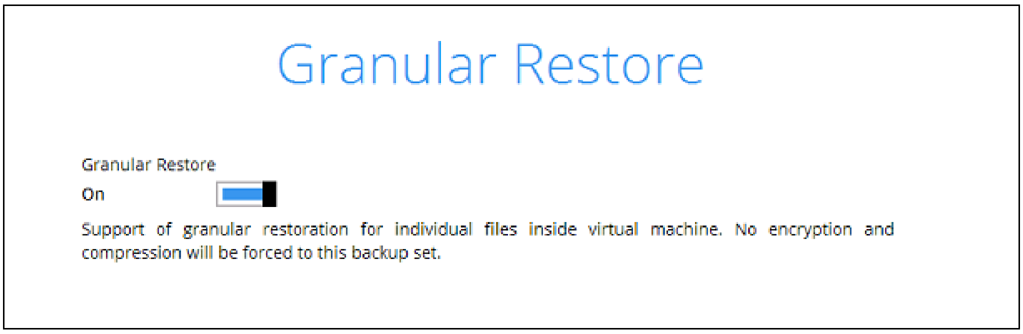
Sequential

Existing storage destinations

CBS

Host: 10.3.1.8:443

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

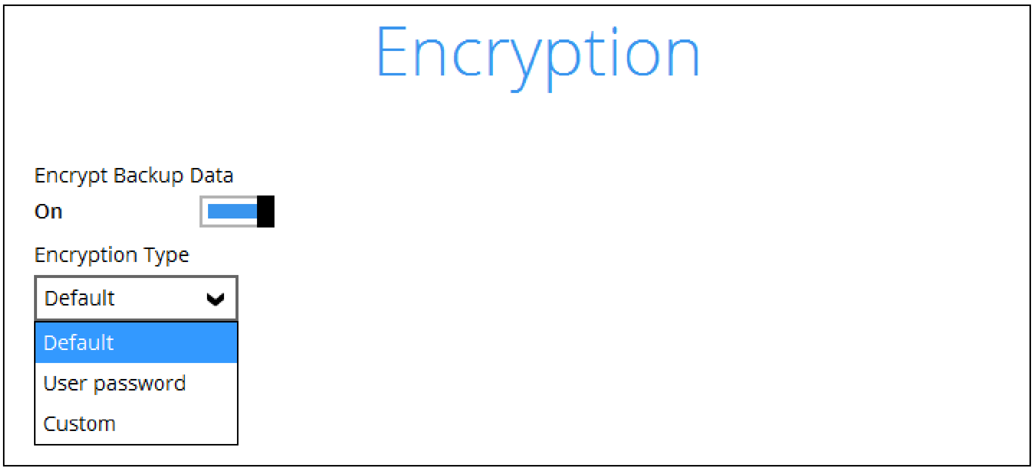
Support of granular restoration for individual files inside virtual machine. No encryption and compression will be forced to this backup set.

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.

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

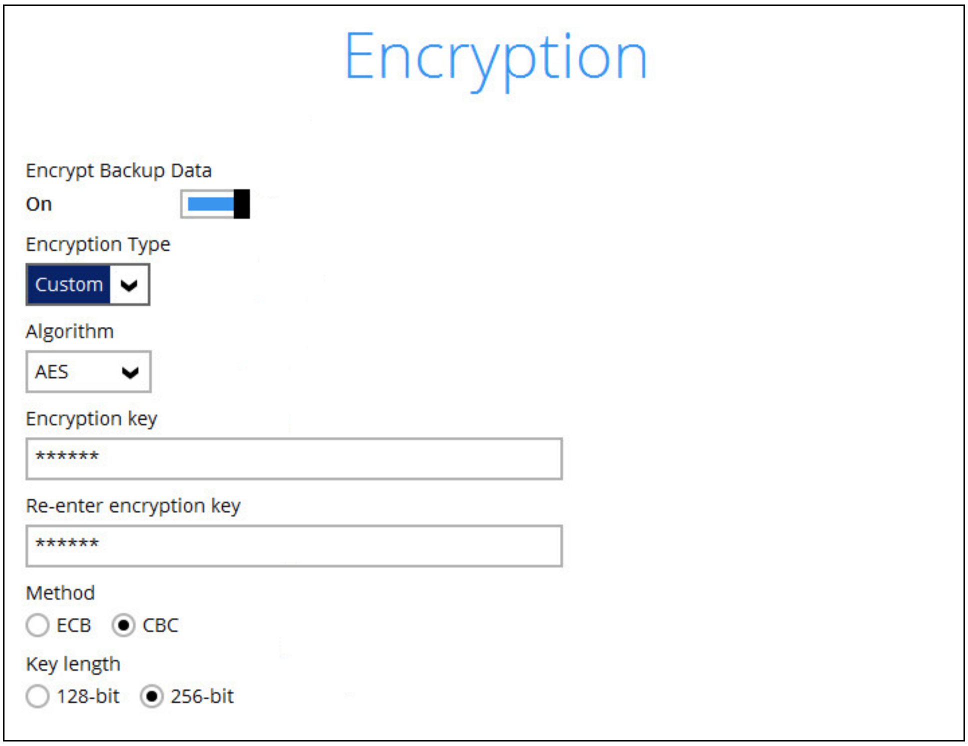
Encryption Type

Default

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

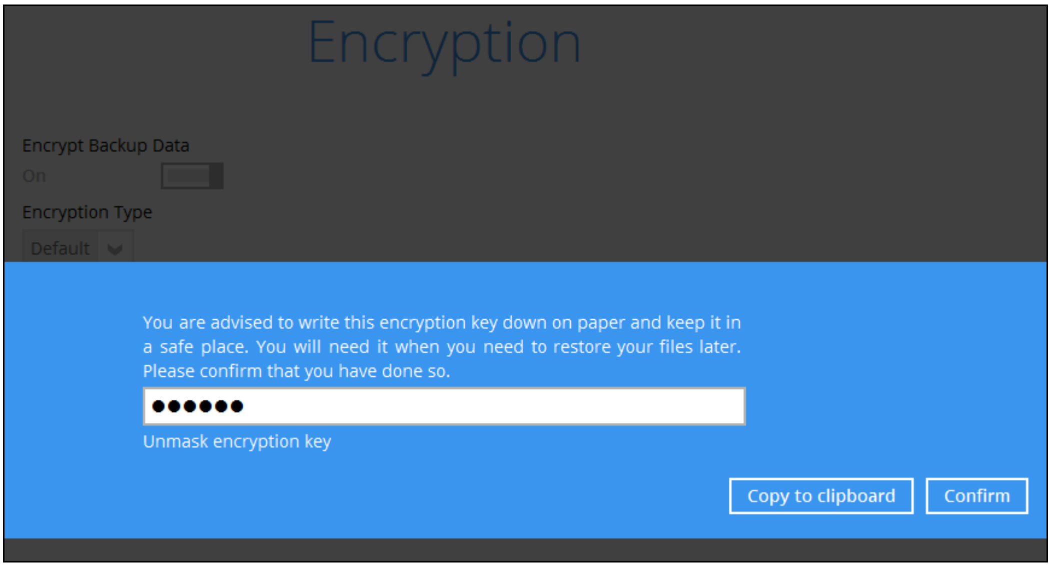
Notes:

i. For best practice on managing your encryption key, refer to the following KB article. https://forum.ahsay.com/viewtopic.php?f=169&t=14090

ii. For local, mapped drive, or removable drive storage destinations with Run Direct enabled the compression type will always 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.

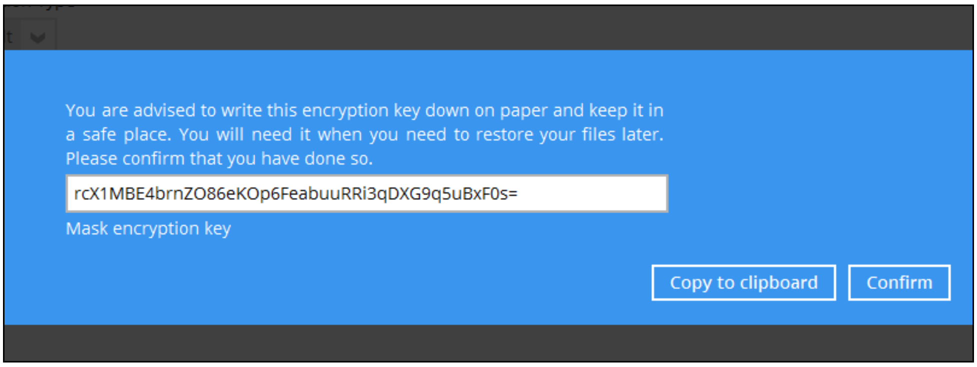


You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.

●●●●●●

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.



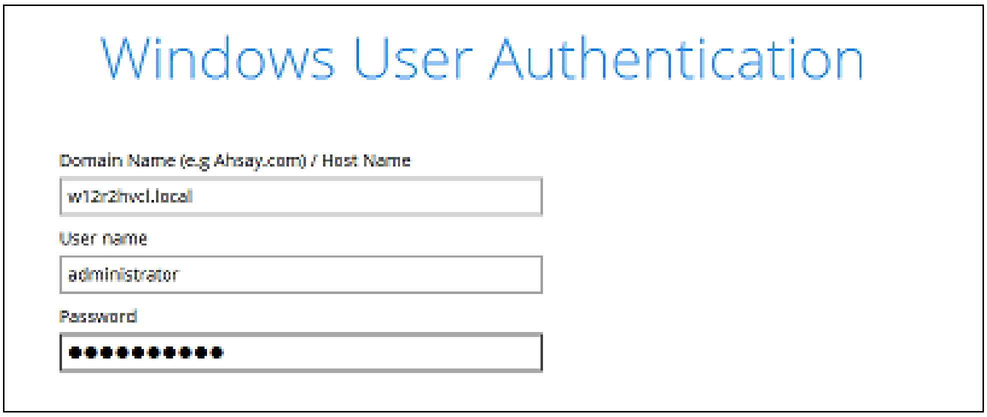
You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.

rcX1MBE4brnZO86eKOp6FeabuuRRi3qDXG9q5uBxF0s=

- **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.



Windows User Authentication

Domain Name (e.g Ahsay.com) / Host Name: w12r2hvcl.local

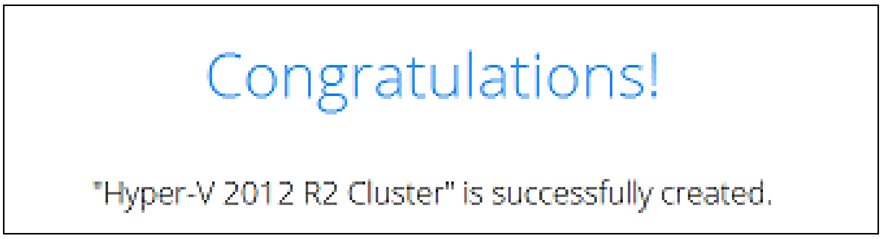
User name: administrator

Password: ●●●●●●●●●●●

***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. **Backup set created.**

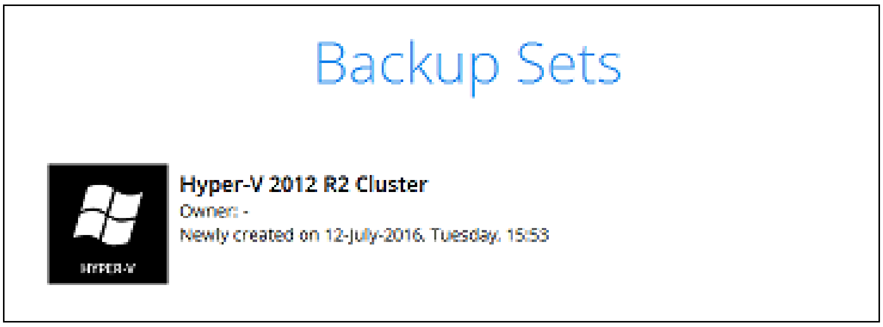
    i. To start a manual backup job click on **Backup now.**



Congratulations!

"Hyper-V 2012 R2 Cluster" is successfully created.

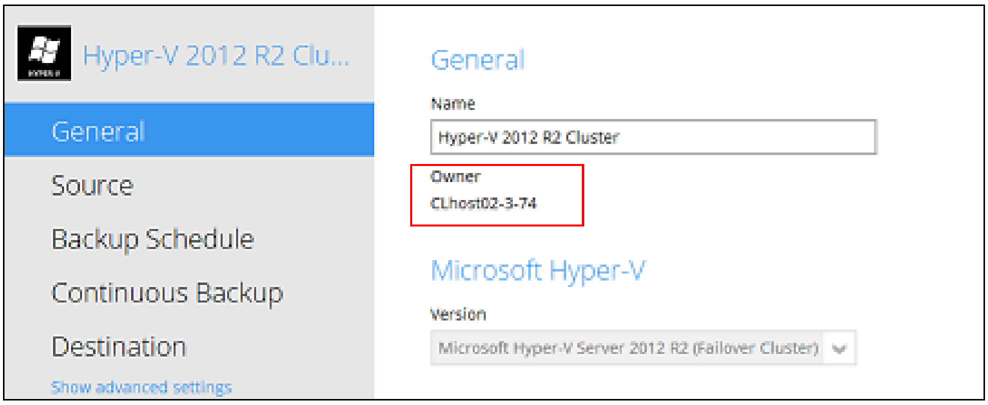
    ii. To verify the backup set settings click on Close and then click on the Hyper-V backup set to complete the setup.



Backup Sets

Hyper-V 2012 R2 Cluster
Owner: -
Newly created on 12-July-2016, Tuesday, 15:53

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



General

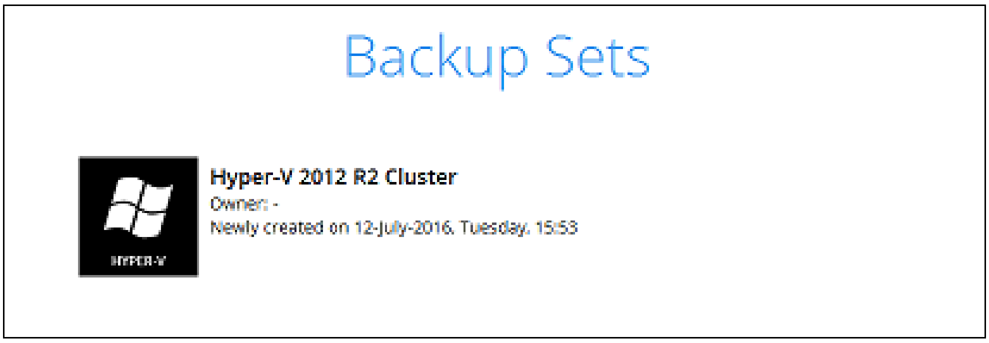
Name: Hyper-V 2012 R2 Cluster

Owner: CLhost02-3-74

Microsoft Hyper-V

Version: Microsoft Hyper-V Server 2012 R2 (Failover Cluster)

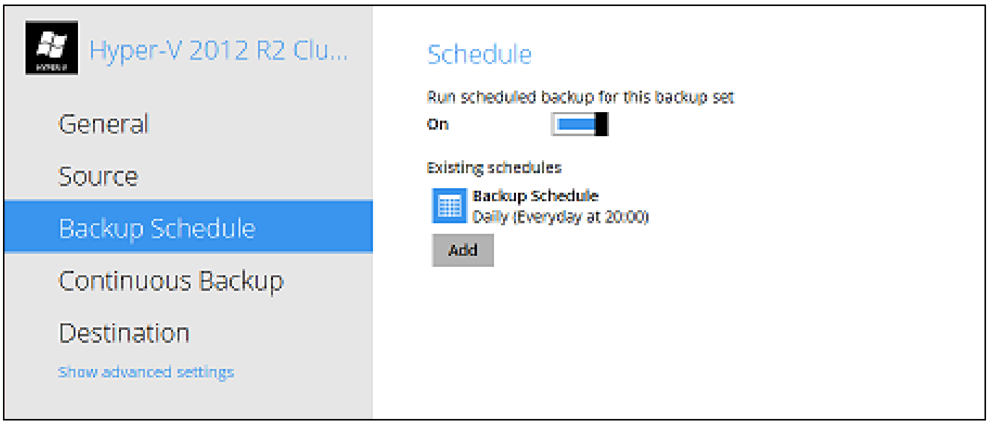
14. On the next Hyper-V node startup AhsayOBM and select the Hyper-V backup set.



Backup Sets

Hyper-V 2012 R2 Cluster
Owner: -
Newly created on 12-July-2016, Tuesday, 15:53

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.

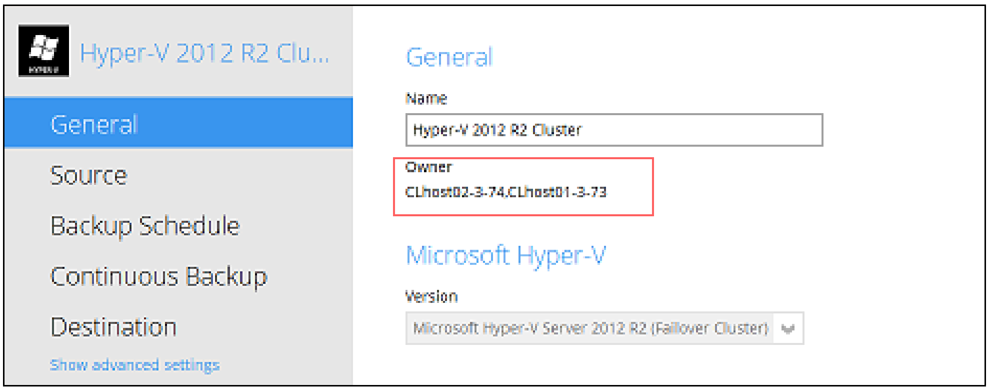


Schedule

Run scheduled backup for this backup set
On

Existing schedules
Backup Schedule
Daily (Everyday at 20:00)

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



General

Name
Hyper-V 2012 R2 Cluster

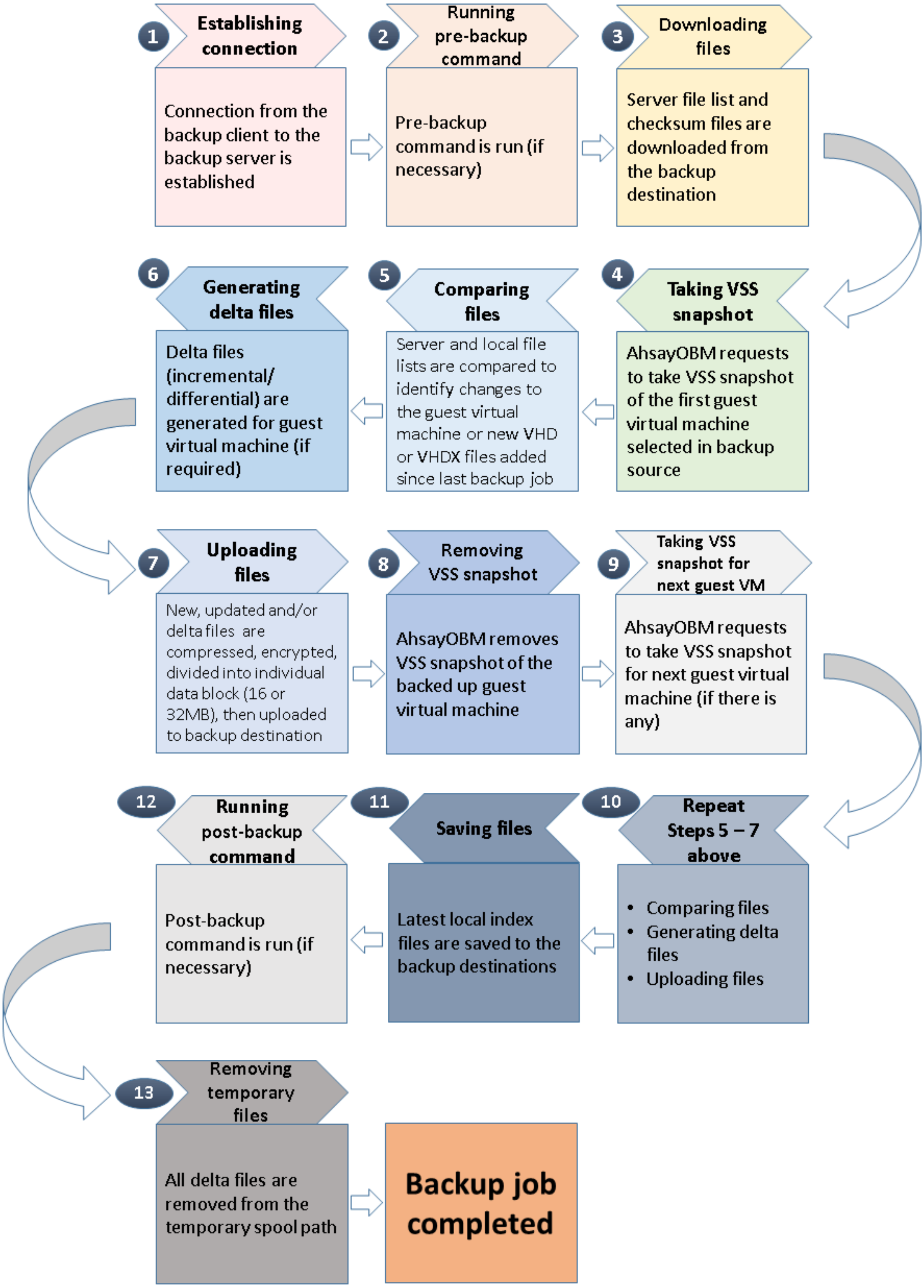
Owner
CLhost02-3-74,CLhost01-3-73

Microsoft Hyper-V

Version
Microsoft Hyper-V Server 2012 R2 (Failover Cluster)

17. Repeat steps 13 to 15 for all Hyper-V Cluster nodes.

7 Overview on the Backup Process



1 **Establishing connection**

Connection from the backup client to the backup server is established

2 **Running pre-backup command**

Pre-backup command is run (if necessary)

3 **Downloading files**

Server file list and checksum files are downloaded from the backup destination

4 **Taking VSS snapshot**

AhsayOBM requests to take VSS snapshot of the first guest virtual machine selected in backup source

5 **Comparing files**

Server and local file lists are compared to identify changes to the guest virtual machine or new VHD or VHDX files added since last backup job

6 **Generating delta files**

Delta files (incremental/ differential) are generated for guest virtual machine (if required)

7 **Uploading files**

New, updated and/or delta files are compressed, encrypted, divided into individual data block (16 or 32MB), then uploaded to backup destination

8 **Removing VSS snapshot**

AhsayOBM removes VSS snapshot of the backed up guest virtual machine

9 **Taking VSS snapshot for next guest VM**

AhsayOBM requests to take VSS snapshot for next guest virtual machine (if there is any)

10 **Repeat Steps 5 – 7 above**

- Comparing files
- Generating delta files
- Uploading files

11 **Saving files**

Latest local index files are saved to the backup destinations

12 **Running post-backup command**

Post-backup command is run (if necessary)

13 **Removing temporary files**

All delta files are removed from the temporary spool path

Backup job completed

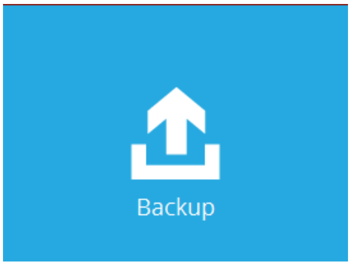
8 Running Backup Jobs

Login to AhsayOBM

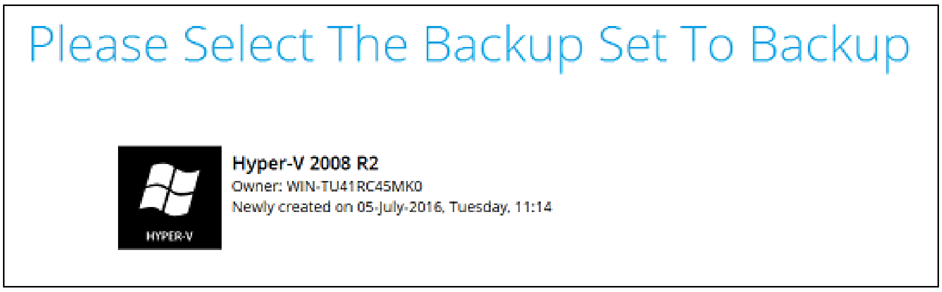
Login to the AhsayOBM application according to the instructions in Chapter 3.1

Start a Manual Backup

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



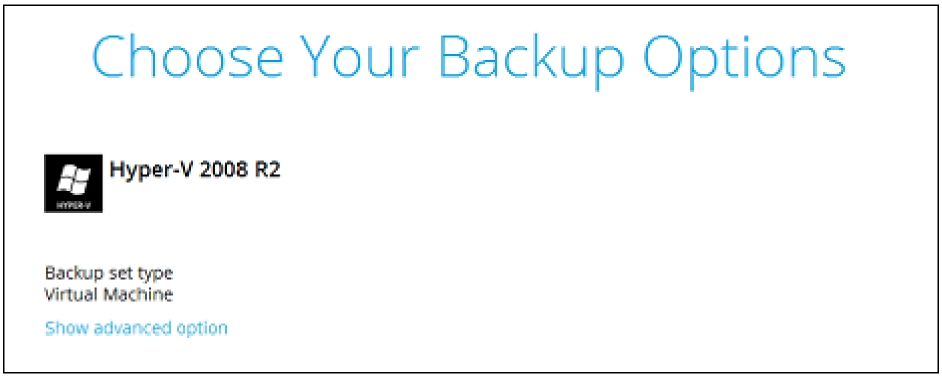
2. Select the Hyper-V backup set which you would like to start a manual backup.



Please Select The Backup Set To Backup

Hyper-V 2008 R2
Owner: WIN-TU41RC45MK0
Newly created on 05-July-2016, Tuesday, 11:14

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

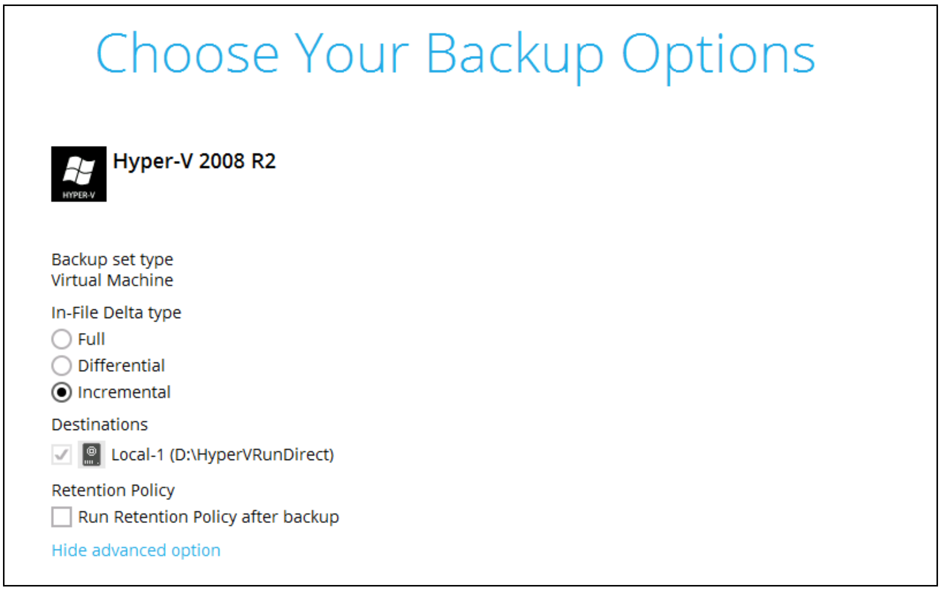


Choose Your Backup Options

Hyper-V 2008 R2

Backup set type
Virtual Machine

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



Choose Your Backup Options

Hyper-V 2008 R2

Backup set type
Virtual Machine

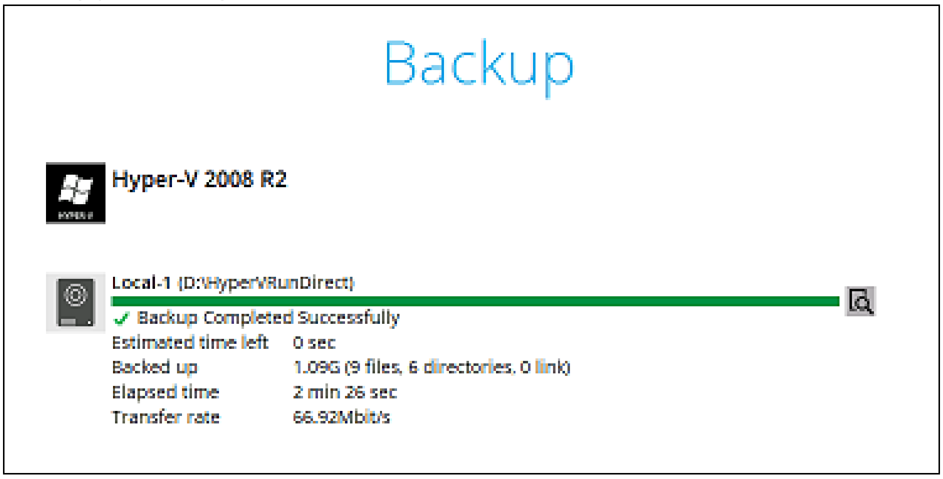
In-File Delta type
○ Full
○ Differential
● Incremental

Destinations
☑ Local-1 (D:\HyperVRunDirect)

Retention Policy
□ Run Retention Policy after backup

Hide advanced option

5. Backup job is completed.



Backup

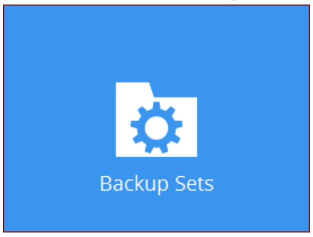
Hyper-V 2008 R2

Local-1 (D:\HyperVRunDirect)
✓ Backup Completed Successfully

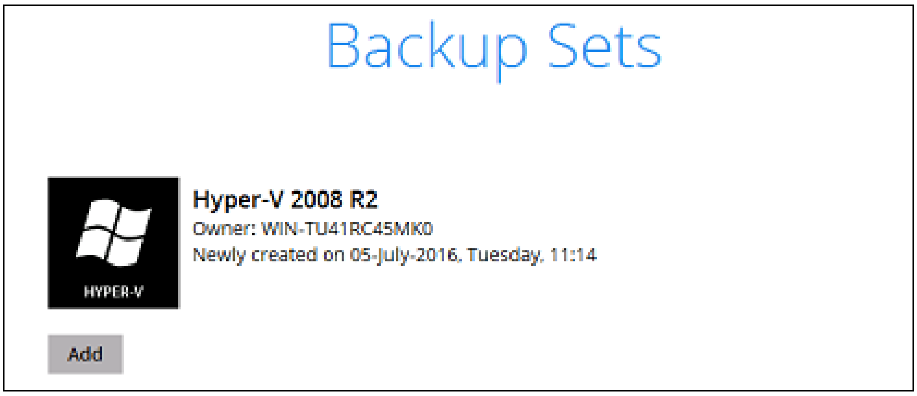
Estimated time left	0 sec
Backed up	1.09G (9 files, 6 directories, 0 link)
Elapsed time	2 min 26 sec
Transfer rate	66.92Mbit/s

Configure Backup Schedule for Automated Backup

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

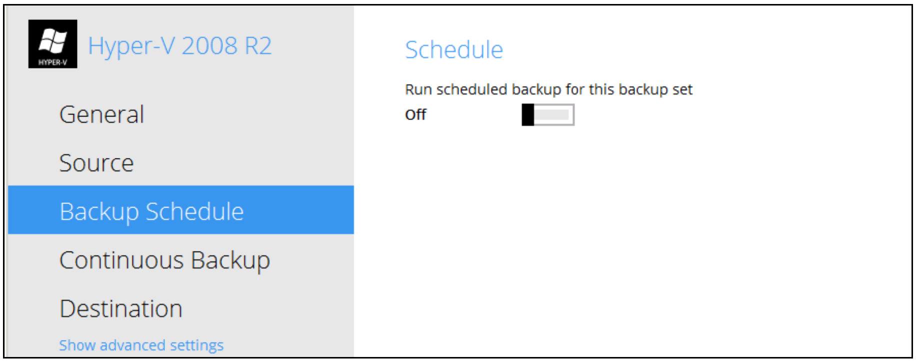


2. Select the backup set that you would like to create a backup schedule for.


Backup Sets

Hyper-V 2008 R2
Owner: WIN-TU41RC45MK0
Newly created on 05-July-2016, Tuesday, 11:14

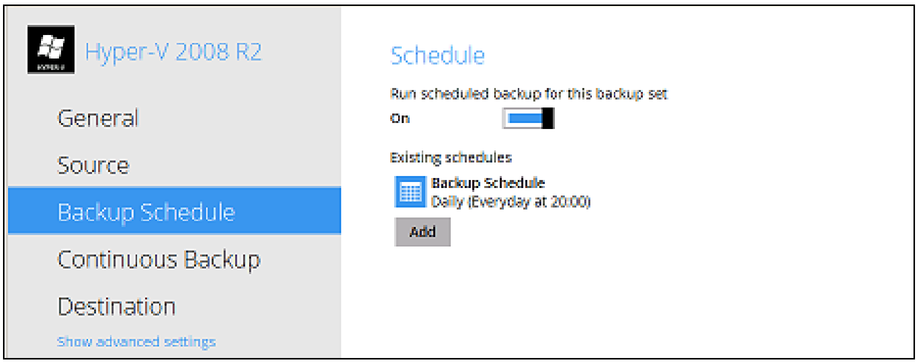
3. Click Backup Schedule.



Schedule

Run scheduled backup for this backup set
Off

4. Then create a new backup schedule by clicking on the **Run scheduled backup for this backup set**. Set this to **On.**



Schedule

Run scheduled backup for this backup set
On

Existing schedules
Backup Schedule
Daily (Everyday at 20:00)

Click **Add** to add a new schedule or double click on the existing schedule to change the existing values. Click **Save** to proceed when you are done setting.

Note: *The default backup schedule is daily backup at 22:00 with the backup job will run until completion and the retention policy job will be run immediately after the backup job*.

9 Restoring Hyper-V Guest Virtual Machines

Restore Options

There are two major types of restore options, namely Run Direct Restore and Non Run Direct Restore.

Run Direct Restore
Start up the guest virtual machine directly from the backup file without restoring the guest virtual machine to the Hyper-V server.
Type 1 – 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.
Type 2 – Start up a guest VM from Backup Destination with Auto Migration Enabled
To start up the guest virtual machine directly from the backup file and then start restoring the guest virtual machine files to the Hyper-V server. VM data will start migrating without the need trigger a manual migration. Any changes made during the Run Direct instance will also be committed to the Hyper-V server as well.

Non Run Direct Restore
Conventional restore method where AhsayOBM will restore the guest virtual machine files to the Hyper-V server
Type 1 – Restore to the same Hyper-V server
For this type of restore, you can choose from one of the following restore methods. ➢ Restore the entire guest VM to the original location ➢ Restore the entire guest VM to another drive or folder on the same Hyper-V server ➢ Restore individual virtual disk to original/different guest virtual machine
Type 2 – Restore backed up guest VM to another Hyper-V server on a different host
You need to have the same version of Hyper-V server together with AhsayOBM installed on the machine where you wish to restore the guest virtual machine. Refer to the steps in Initiate Restore of VM to another Hyper-V Server on Different Host for details.

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 a long time to restore and then boot up before you can gain access 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

Requirements and Limitations

1. Restored guest virtual machines 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.

2. For Run Direct enabled backup sets the storage destination is restricted to Local, Mapped Drive, or Removable Drive.

3. When a guest virtual machine 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.

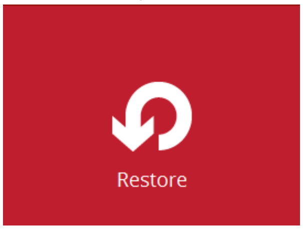
4. When a guest virtual machine is started using Run Direct Restore all backup jobs (manual, scheduled, and continuous) for the related backup set will be skipped.

5. When a guest virtual machine 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.

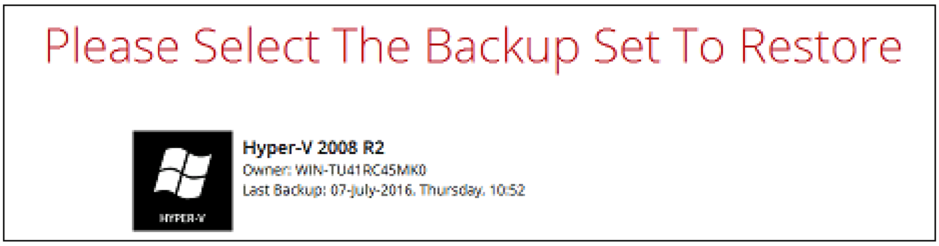
Start up a guest VM from Backup Destination without Auto Migration Enabled

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

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



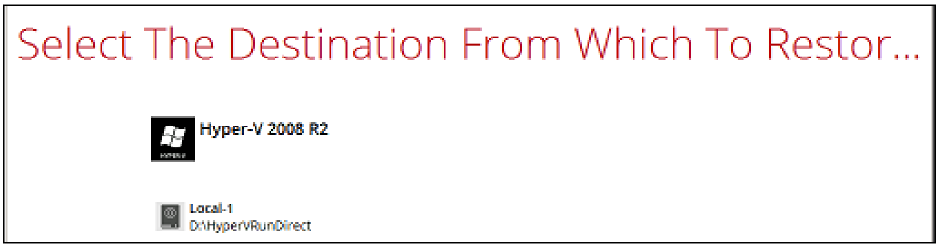
2. Select the backup set that you would like to restore the guest virtual machine from.



Please Select The Backup Set To Restore

Hyper-V 2008 R2
Owner: WIN-TU41RC45MK0
Last Backup: 07-July-2016, Thursday, 10:52

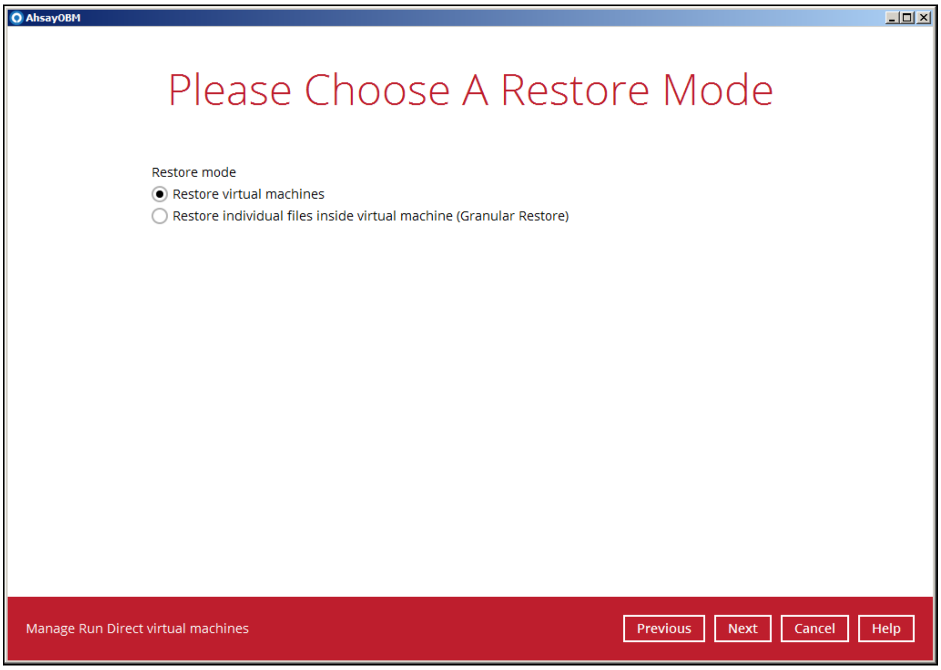
3. Select the local, mapped drive, or removable drive storage destination that contains Hyper-V guest VM that you would like to restore.



Select The Destination From Which To Restor...

Local-1
D:\HyperVRunDirect

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



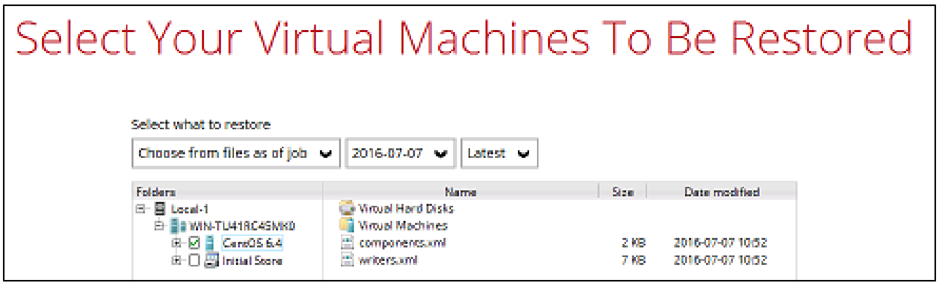
Please Choose A Restore Mode

Restore mode

● Restore virtual machines

○ Restore individual files inside virtual machine (Granular Restore)

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.



Select Your Virtual Machines To Be Restored

Select what to restore

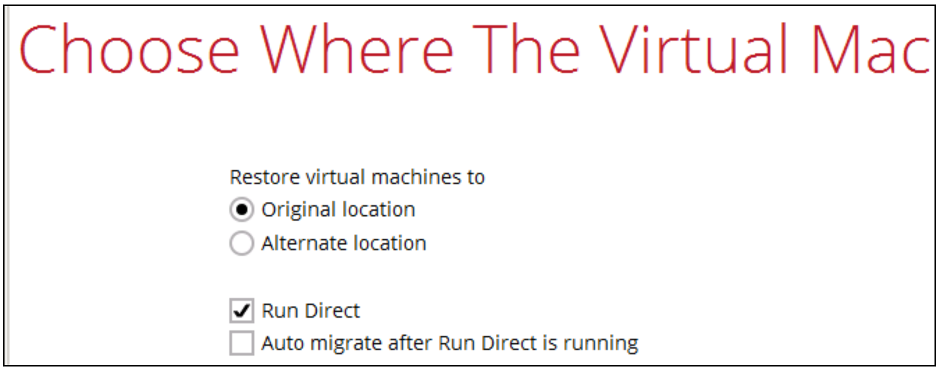
Choose from files as of job | 2016-07-07 | Latest

Folders

- ⊟ Local-1
  - ⊟ WIN-TU41RC4SMK0
    - ⊞ ☑ CentOS 6.4
    - ⊞ □ Initial Store

Name	Size	Date modified
Virtual Hard Disks		
Virtual Machines		
components.xml	2 KB	2016-07-07 10:52
writers.xml	7 KB	2016-07-07 10:52

6. Select to restore the Hyper-V guest VM to the Original location and then select **Run Direct** click **Next** to proceed.



Choose Where The Virtual Mac

Restore virtual machines to

● Original location

○ Alternate location

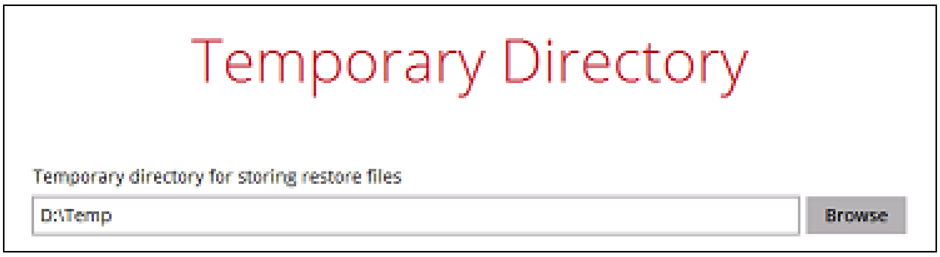
☑ Run Direct

□ Auto migrate after Run Direct is running

Note

Restore to an Alternate location can only be performed on one guest virtual machine at a time.

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



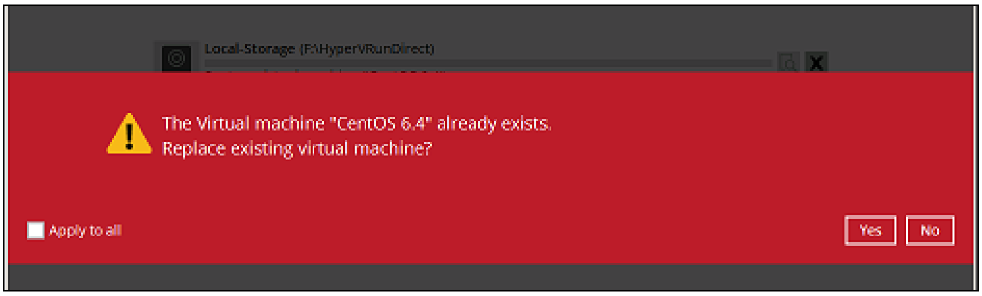
Temporary Directory

Temporary directory for storing restore files

D:\Temp

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

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

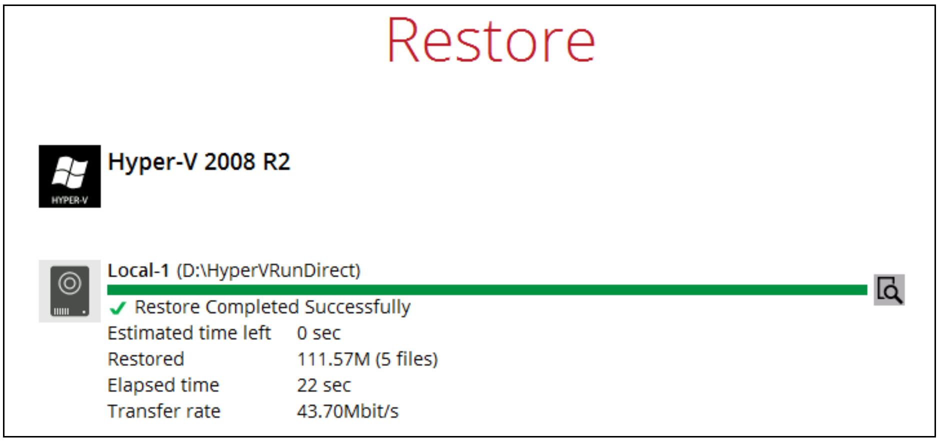


Local-Storage (F:\HyperVRunDirect)

The Virtual machine "CentOS 6.4" already exists.
Replace existing virtual machine?

□ Apply to all

8. After the Hyper-V guest virtual machine has been restored, you will see the following screen.



Restore

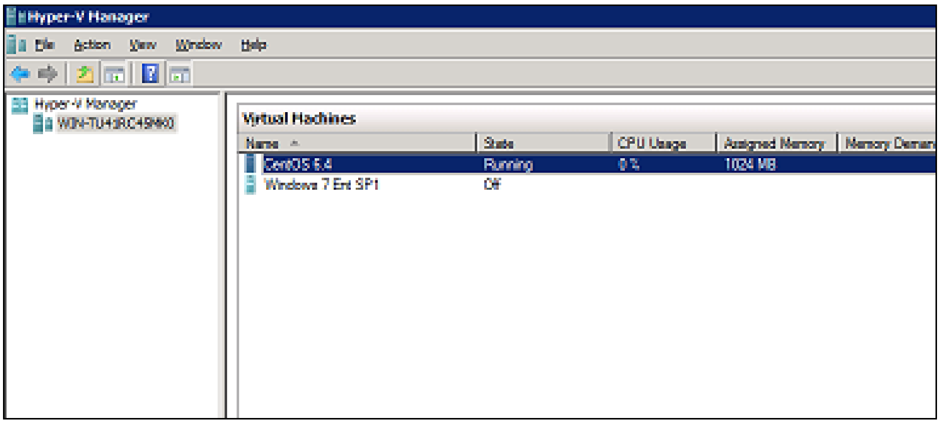
Hyper-V 2008 R2

Local-1 (D:\HyperVRunDirect)

✓ Restore Completed Successfully

Estimated time left	0 sec
Restored	111.57M (5 files)
Elapsed time	22 sec
Transfer rate	43.70Mbit/s

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

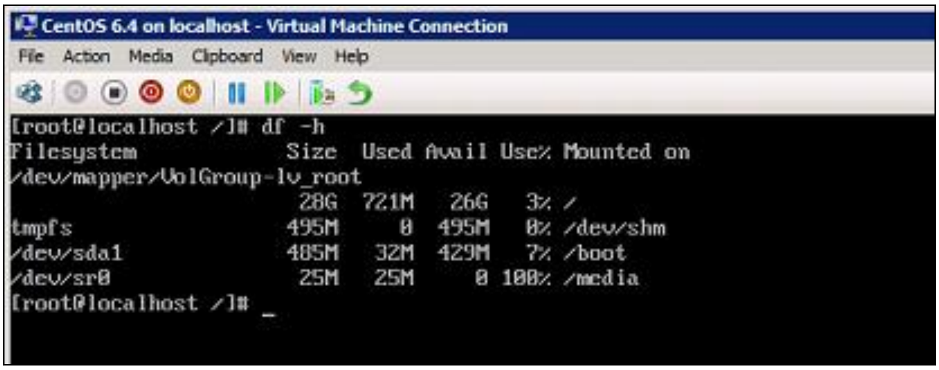


Virtual Machines

Name	State	CPU Usage	Assigned Memory	Memory Deman
CentOS 6.4	Running	0 %	1024 MB	
Windows 7 Ent SP1	Off			

10. Connect to the guest virtual machine to verify if is running correctly.

Example: Linux guest



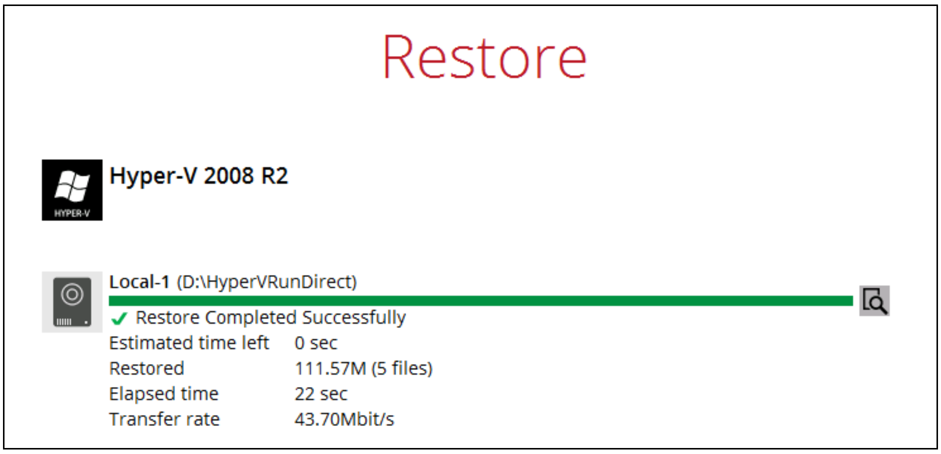
CentOS 6.4 on localhost - Virtual Machine Connection
File Action Media Clipboard View Help

```
[root@localhost /]# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/VolGroup-lv_root
                       28G  721M   26G   3% /
tmpfs                 495M     0  495M   0% /dev/shm
/dev/sda1             485M   32M  429M   7% /boot
/dev/sr0               25M   25M     0 100% /media
[root@localhost /]# _
```

Migrate Virtual Machine (Permanently Restore)

To permanently restore the guest virtual machine 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 guest machine is already running.

1. After starting up the guest machine from the backup destination. Click on **Close.**



Restore

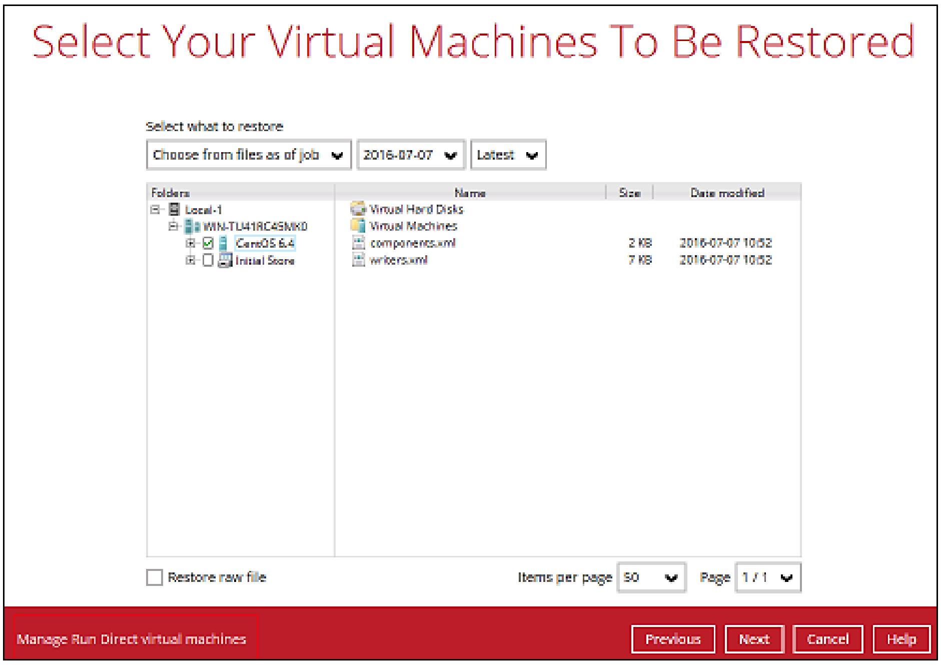
Hyper-V 2008 R2

Local-1 (D:\HyperVRunDirect)

✓ Restore Completed Successfully

Estimated time left	0 sec
Restored	111.57M (5 files)
Elapsed time	22 sec
Transfer rate	43.70Mbit/s

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 | 2016-07-07 | Latest

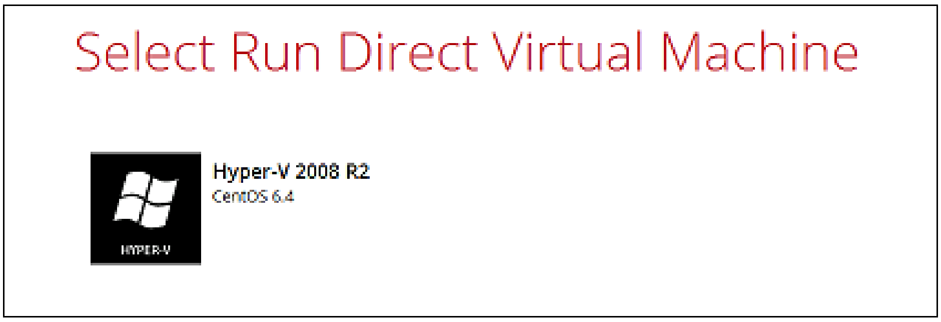
Folders:
- ⊟ Local-1
  - ⊟ WIN-TU41RC4SMK0
    - ⊞ ☑ CentOS 6.4
    - ⊞ ☐ Initial Store

Name	Size	Date modified
Virtual Hard Disks		
Virtual Machines		
components.xml	2 KB	2016-07-07 10:52
writers.xml	7 KB	2016-07-07 10:52

☐ Restore raw file

Items per page 50 | Page 1 / 1

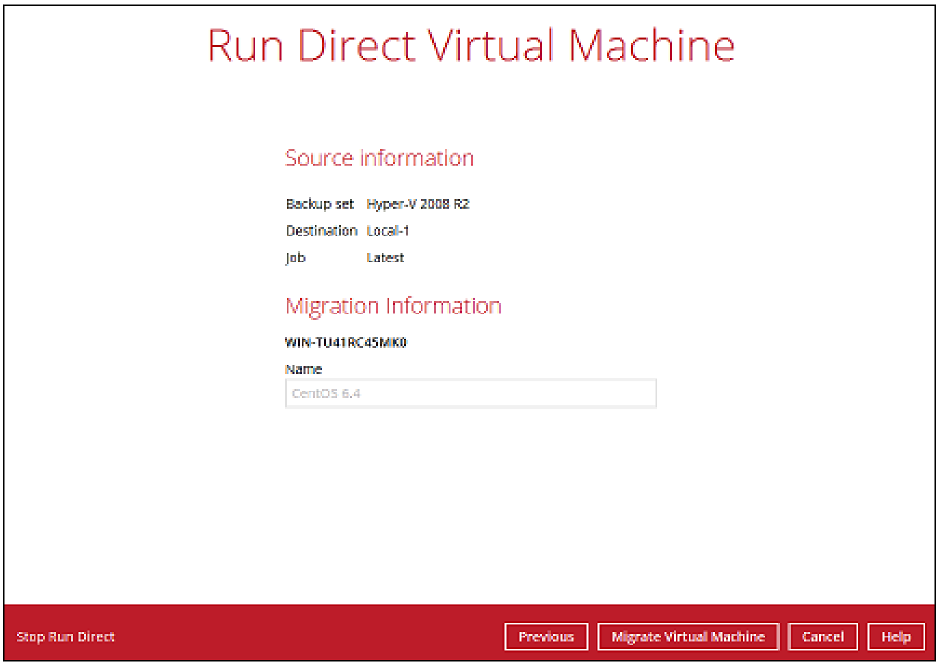
3. Click on the guest virtual machine.



Select Run Direct Virtual Machine

Hyper-V 2008 R2
CentOS 6.4

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



Run Direct Virtual Machine

Source information

Backup set Hyper-V 2008 R2
Destination Local-1
Job Latest

Migration Information

WIN-TU41RC45MK0

Name

CentOS 6.4

Note

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

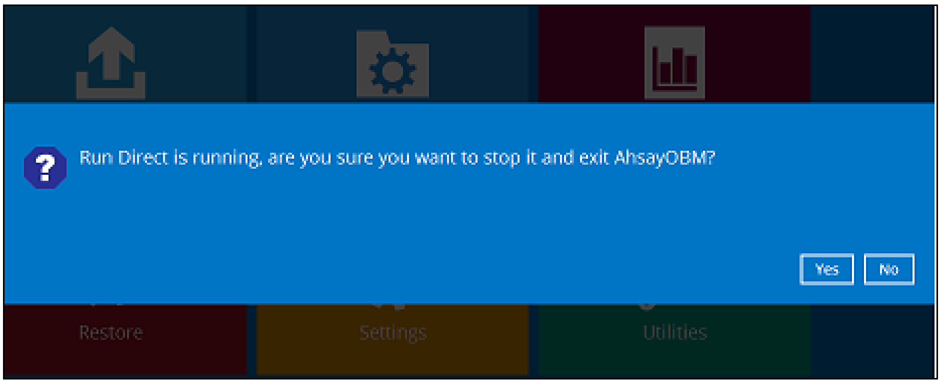
The guest virtual machine can be used during the migration process. Any changes made in the guest virtual machine environment is saved in transaction logs and will be applied when the migration process is completed.

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

Stop Run Direct Virtual Machines

To stop running guest virtual machines started up using Run Direct can be done by either:

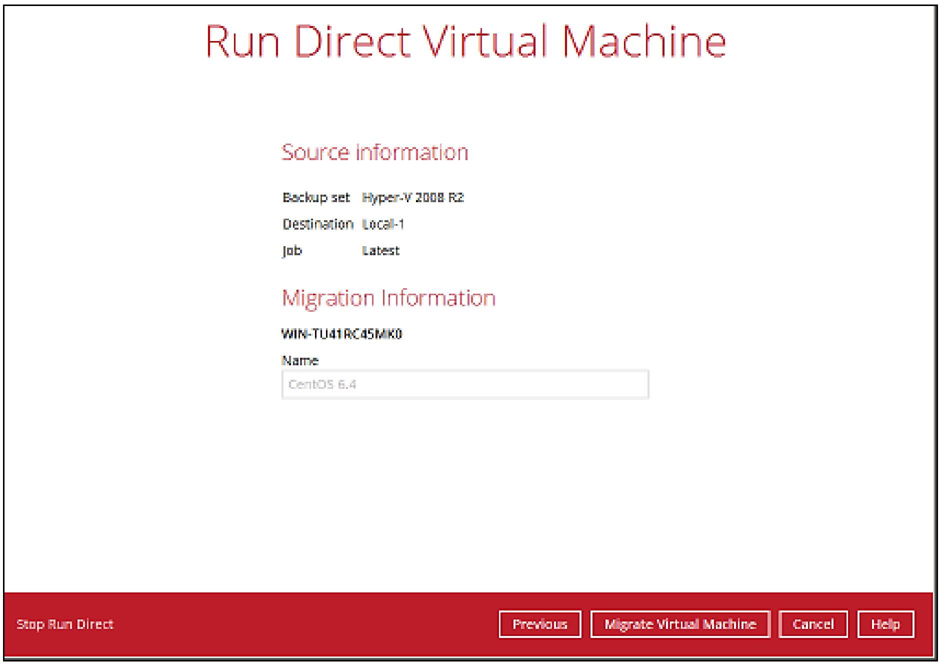
- Quitting AhsayOBM



Run Direct is running, are you sure you want to stop it and exit AhsayOBM?

-OR-

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



Run Direct Virtual Machine

Source information

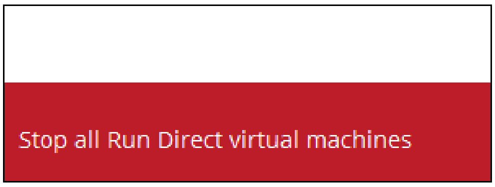
Backup set Hyper-V 2008 R2
Destination Local-1
Job Latest

Migration Information

WIN-TU41RC45MK0

Name
CentOS 6.4

Click on **Stop all Run Direct virtual machines.**



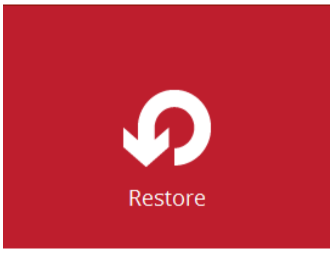
Note

When a guest virtual machine 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.

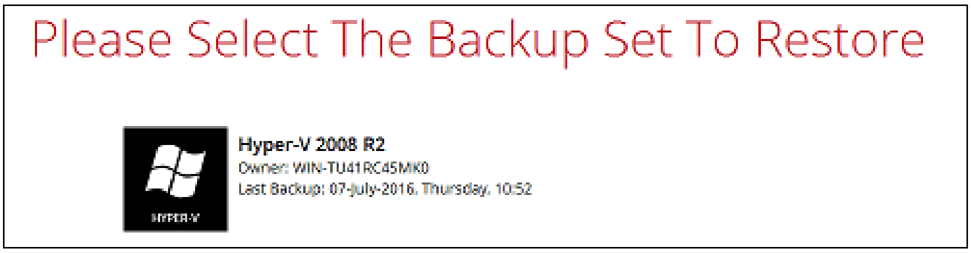
Start up a guest VM from Backup Destination with Auto Migration Enabled

Start up the Run Direct Restore

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



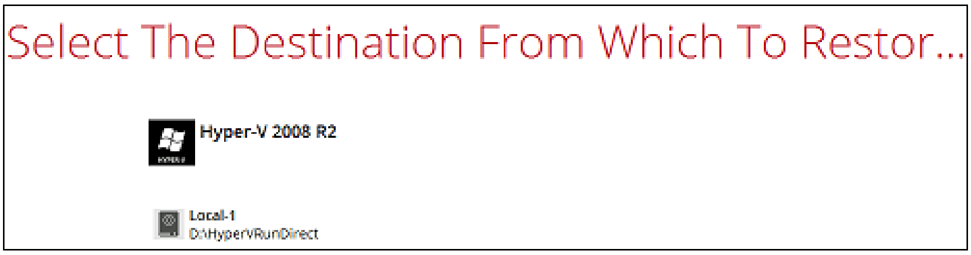
2. Select the backup set that you would like to restore the guest virtual machine from.



Please Select The Backup Set To Restore

Hyper-V 2008 R2
Owner: WIN-TU41RC45MK0
Last Backup: 07-July-2016, Thursday, 10:52

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

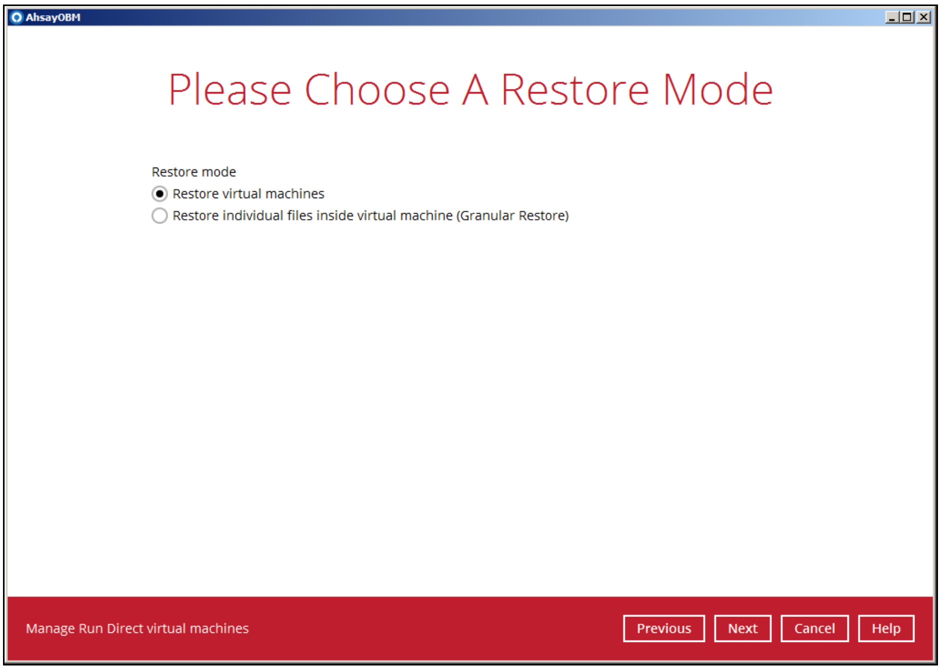


Select The Destination From Which To Restor...

Hyper-V 2008 R2

Local-1
D:\HyperVRunDirect

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

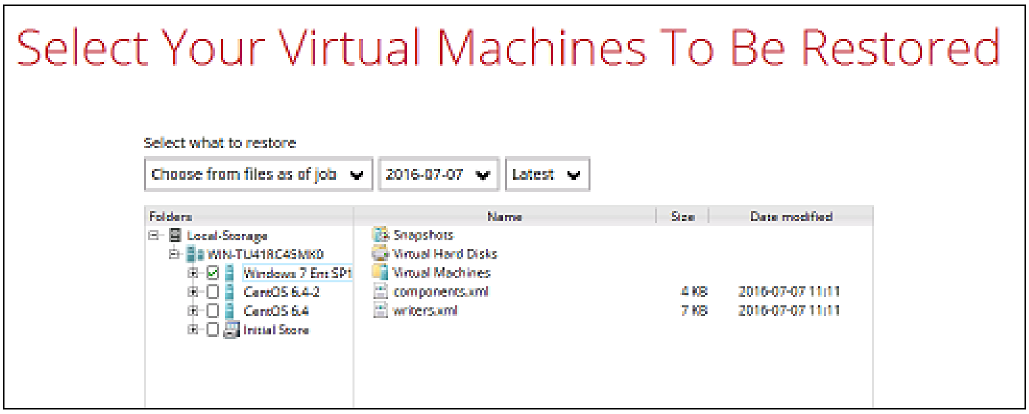


Please Choose A Restore Mode

Restore mode
● Restore virtual machines
○ Restore individual files inside virtual machine (Granular Restore)

Manage Run Direct virtual machines

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.



Select Your Virtual Machines To Be Restored

Select what to restore

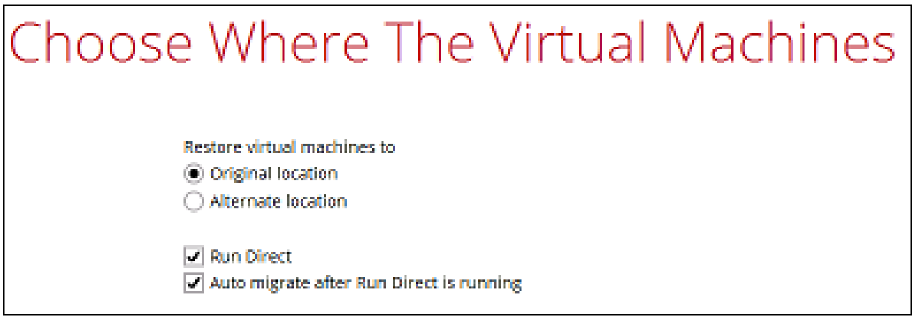
Choose from files as of job ▾ 2016-07-07 ▾ Latest ▾

Folders

- ⊟ Local-Storage
  - ⊟ WIN-TU41RC45MK0
    - ⊞ ☑ Windows 7 Ent SP1
    - ⊞ □ CentOS 6.4-2
    - ⊞ □ CentOS 6.4
    - ⊞ □ Initial Store

Name	Size	Date modified
Snapshots		
Virtual Hard Disks		
Virtual Machines		
components.xml	4 KB	2016-07-07 11:11
writers.xml	7 KB	2016-07-07 11:11

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



Choose Where The Virtual Machines

Restore virtual machines to

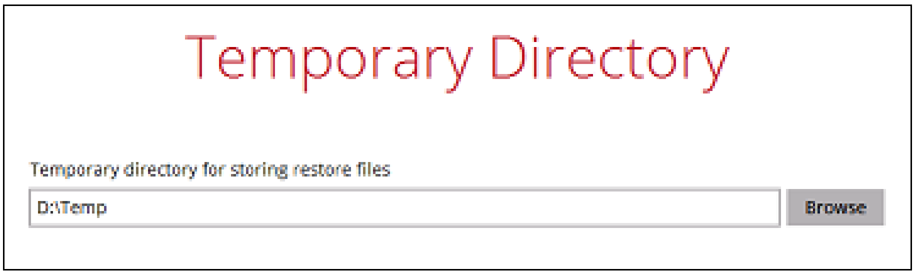
● Original location

○ Alternate location

☑ Run Direct

☑ Auto migrate after Run Direct is running

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



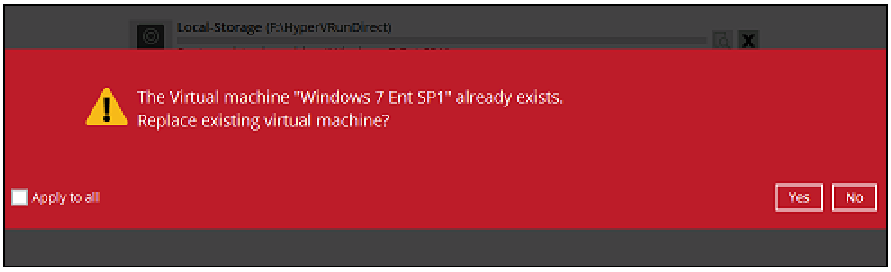
Temporary Directory

Temporary directory for storing restore files

D:\Temp

8. If the guest virtual machine selected to be restore already exists on the Hyper-V server AhsayOBM will prompt to confirm overwriting of the existing guest.

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

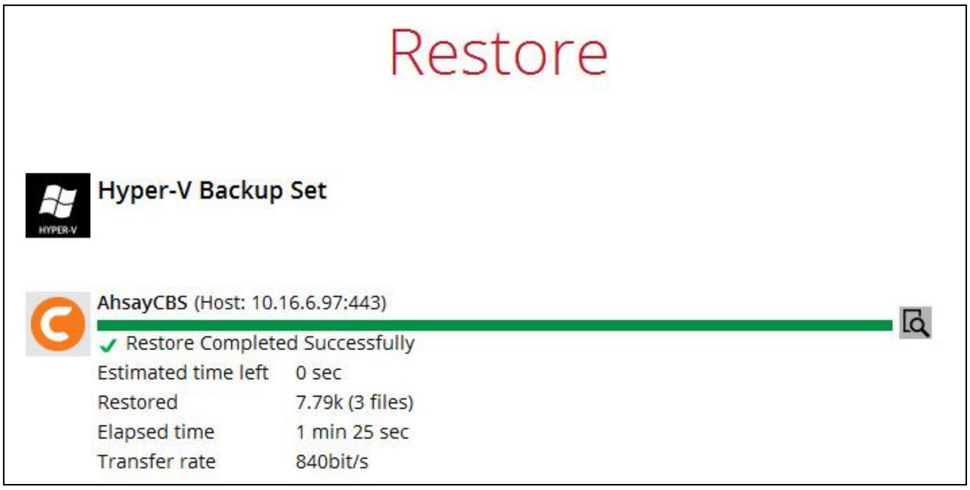


Local-Storage (F:\HyperVRunDirect)

The Virtual machine "Windows 7 Ent SP1" already exists.
Replace existing virtual machine?

□ Apply to all

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



Restore

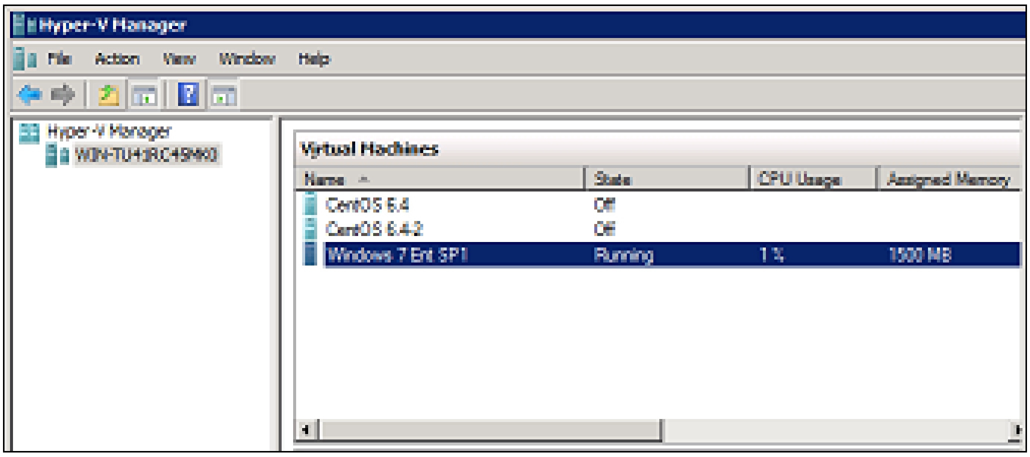
Hyper-V Backup Set

AhsayCBS (Host: 10.16.6.97:443)

✓ Restore Completed Successfully

Estimated time left	0 sec
Restored	7.79k (3 files)
Elapsed time	1 min 25 sec
Transfer rate	840bit/s

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



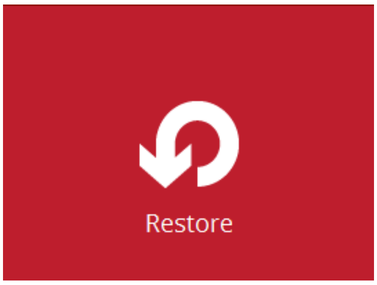
Virtual Machines

Name	State	CPU Usage	Assigned Memory
CentOS 6.4	Off		
CentOS 6.4-2	Off		
Windows 7 Ent SP1	Running	1 %	1500 MB

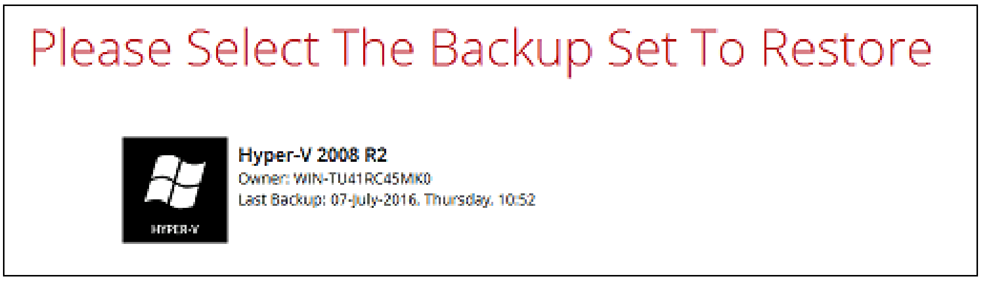
11 Non-Run Direct Restore

Initiate Restore of Guest Virtual Machine to the Original Hyper-V Server Location

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



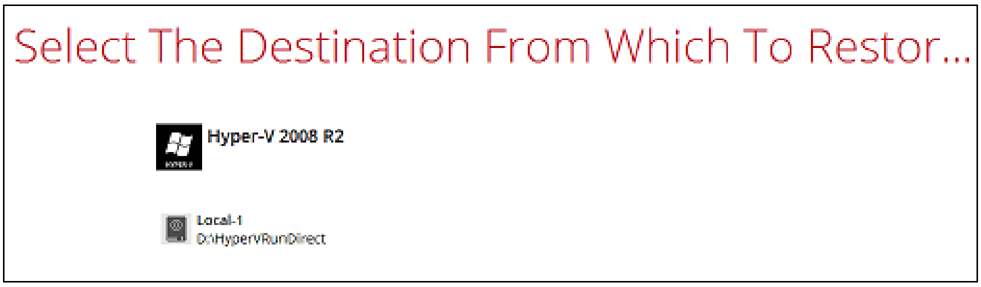
2. Select the backup set that you would like to restore the guest virtual machine from.



Please Select The Backup Set To Restore

Hyper-V 2008 R2
Owner: WIN-TU41RC45MK0
Last Backup: 07-July-2016, Thursday, 10:52

3. Select the drive storage destination that contains Hyper-V guest virtual machine that you would like to restore.



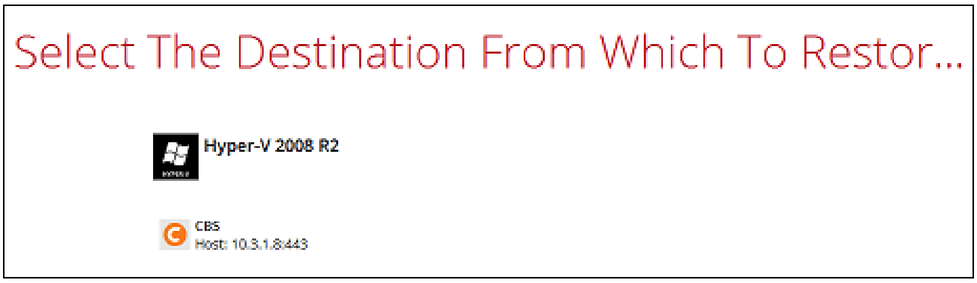
Select The Destination From Which To Restor...

Hyper-V 2008 R2

Local-1
D:\HyperVRunDirect

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

5. **Example: Restore from AhsayCBS**

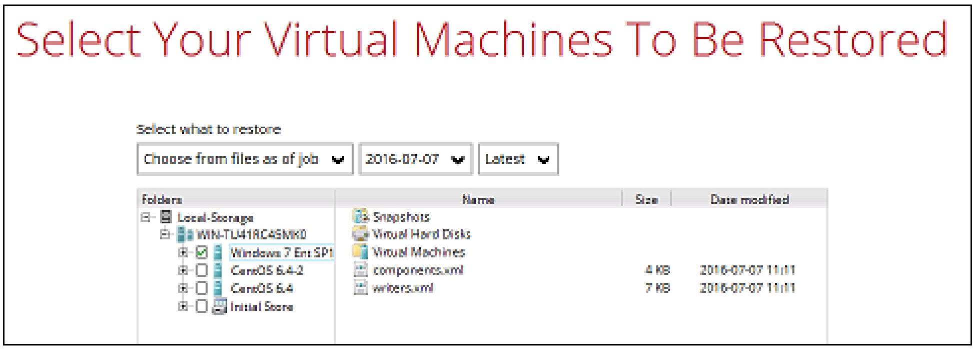


Select The Destination From Which To Restor...

Hyper-V 2008 R2

CBS
Host: 10.3.1.8:443

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. Click **Next** to proceed.



Select Your Virtual Machines To Be Restored

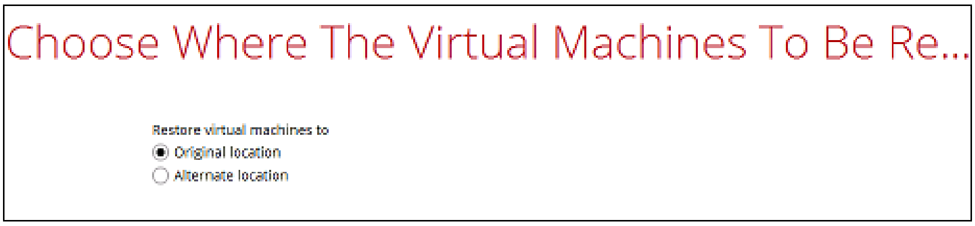
Select what to restore

Choose from files as of job ⌄ | 2016-07-07 ⌄ | Latest ⌄

Folders
- ⊟ Local-Storage
  - ⊟ WIN-TU41RC4SMK0
    - ⊞ ☑ Windows 7 Ent SP1
    - ⊞ □ CentOS 6.4-2
    - ⊞ □ CentOS 6.4
    - ⊞ □ Initial Store

Name	Size	Date modified
Snapshots		
Virtual Hard Disks		
Virtual Machines		
components.xml	4 KB	2016-07-07 11:11
writers.xml	7 KB	2016-07-07 11:11

7. Select to restore the Hyper-v guest to the Original location, or to an Alternate location. Uncheck the box of Run then click **Next** to proceed.



Choose Where The Virtual Machines To Be Re...

Restore virtual machines to

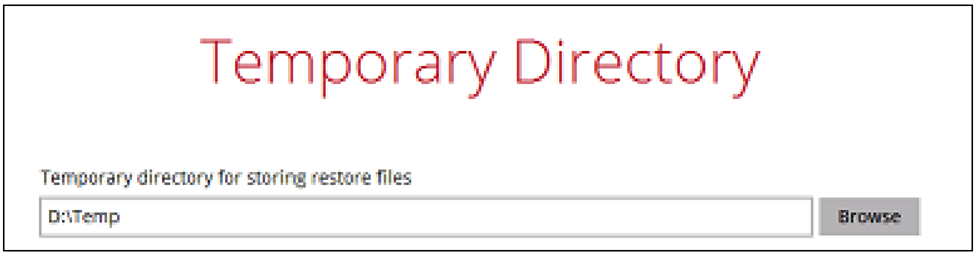
● Original location

○ Alternate location

Note

Restore to an Alternate location can only be performed on one guest virtual machine at a time.

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



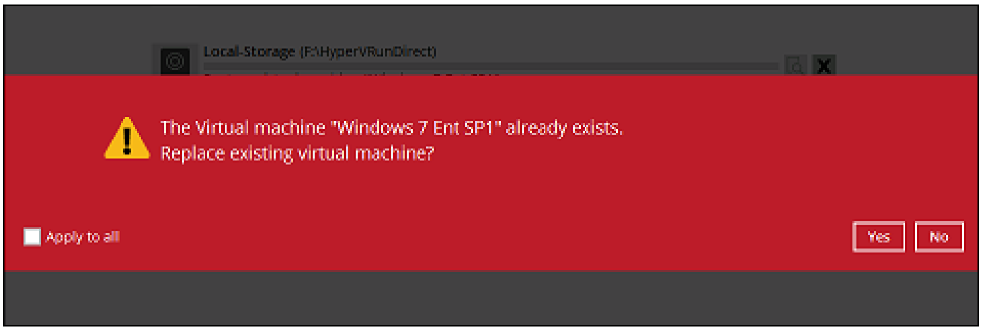
Temporary Directory

Temporary directory for storing restore files

D:\Temp

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

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

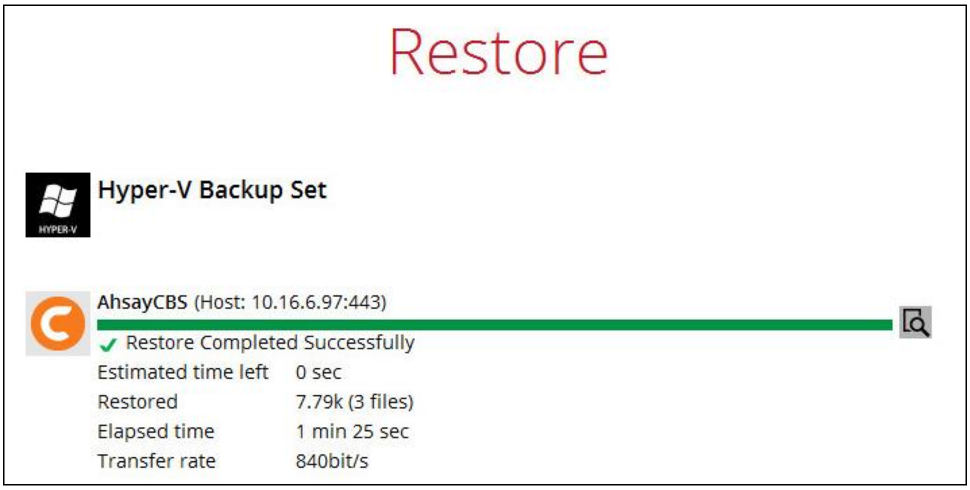


Local-Storage (F:\HyperVRunDirect)

The Virtual machine "Windows 7 Ent SP1" already exists.
Replace existing virtual machine?

□ Apply to all

10. After the Hyper-V guest virtual machine has been restored.



Restore

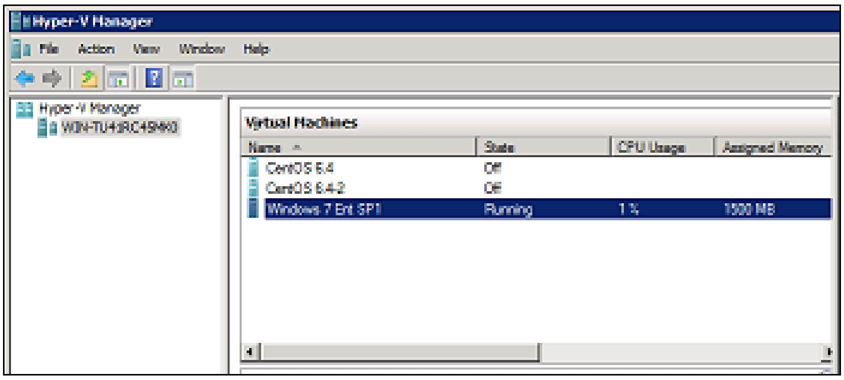
Hyper-V Backup Set

AhsayCBS (Host: 10.16.6.97:443)

✓ Restore Completed Successfully

Estimated time left	0 sec
Restored	7.79k (3 files)
Elapsed time	1 min 25 sec
Transfer rate	840bit/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 virtual machine.



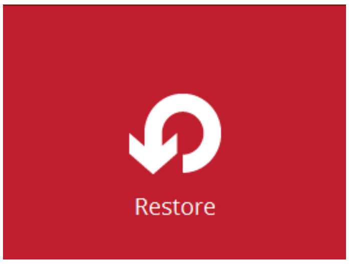
Virtual Machines

Name	State	CPU Usage	Assigned Memory
CentOS 6.4	Off		
CentOS 6.4-2	Off		
Windows 7 Ent SP1	Running	1 %	1500 MB

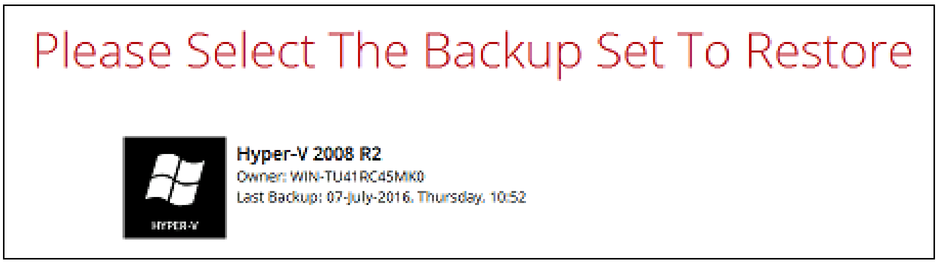
Initiate Restore of an Individual Virtual Disk to Original/Different Guest Virtual Machine

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

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



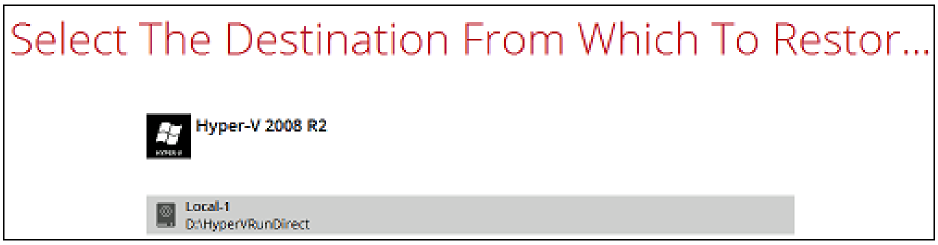
2. Select the backup set that you would like to restore the guest virtual machine from.



Please Select The Backup Set To Restore

Hyper-V 2008 R2
Owner: WIN-TU41RC45MK0
Last Backup: 07-July-2016, Thursday, 10:52

3. Select the drive storage destination that contains Hyper-V guest virtual machine that you would like to restore.

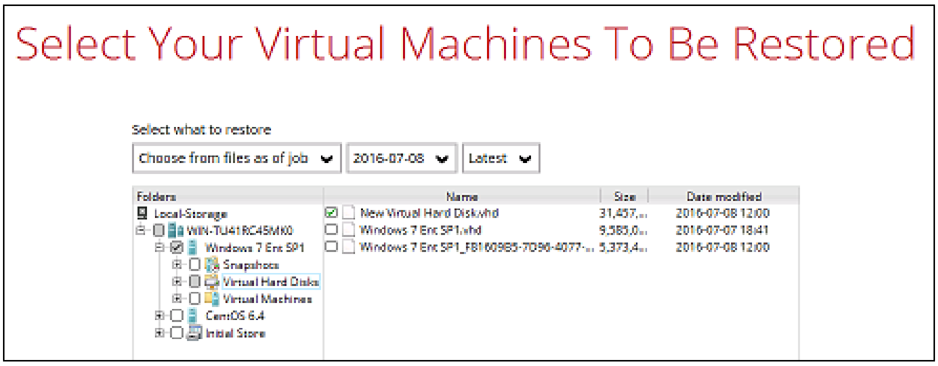


Select The Destination From Which To Restor...

Hyper-V 2008 R2

Local-1
D:\HyperVRunDirect

4. 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 Your Virtual Machines To Be Restored

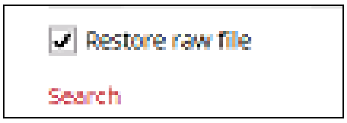
Select what to restore

Choose from files as of job | 2016-07-08 | Latest

Folders
- Local-Storage
  - ▣ WIN-TU41RC45MK0
    - ☑ Windows 7 Ent SP1
      - □ Snapshots
      - ▣ Virtual Hard Disks
      - □ Virtual Machines
    - □ CentOS 6.4
    - □ Initial Store

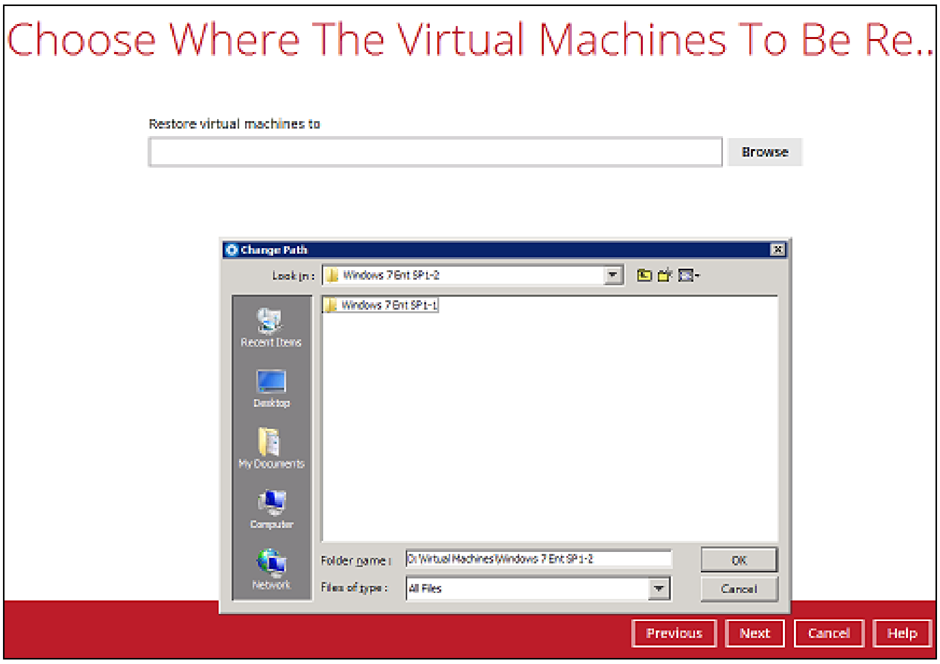
	Name	Size	Date modified
☑	New Virtual Hard Disk.vhd	31,457,...	2016-07-08 12:00
□	Windows 7 Ent SP1.vhd	9,585,0...	2016-07-07 18:41
□	Windows 7 Ent SP1_FB160985-7D96-4077-...	5,373,4...	2016-07-08 12:00

5. 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

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



Choose Where The Virtual Machines To Be Re..

Restore virtual machines to

Change Path

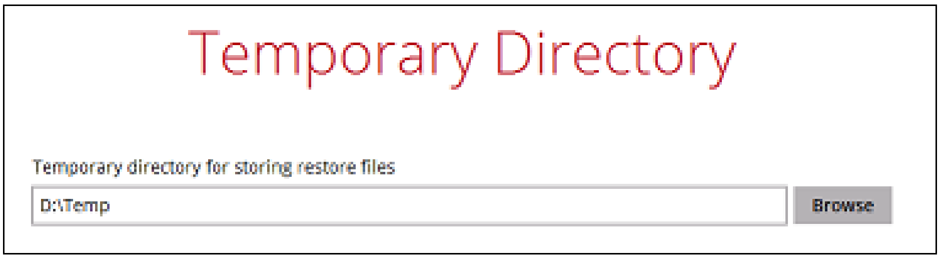
Look in: Windows 7 Ent SP1-2

Windows 7 Ent SP1-1

Folder name: D:\Virtual Machines\Windows 7 Ent SP1-2

Files of type: All Files

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

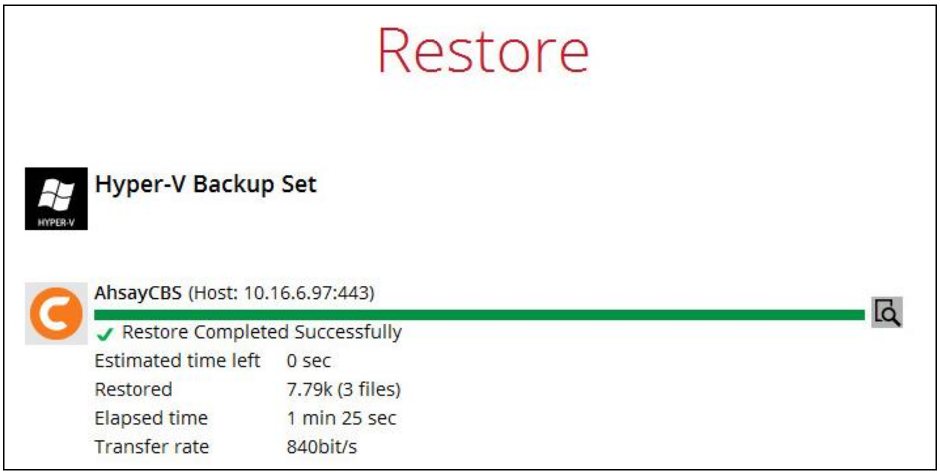


Temporary Directory

Temporary directory for storing restore files

D:\Temp

8. After the Hyper-V guest virtual machine has been restored.



Restore

Hyper-V Backup Set

AhsayCBS (Host: 10.16.6.97:443)

✓ Restore Completed Successfully

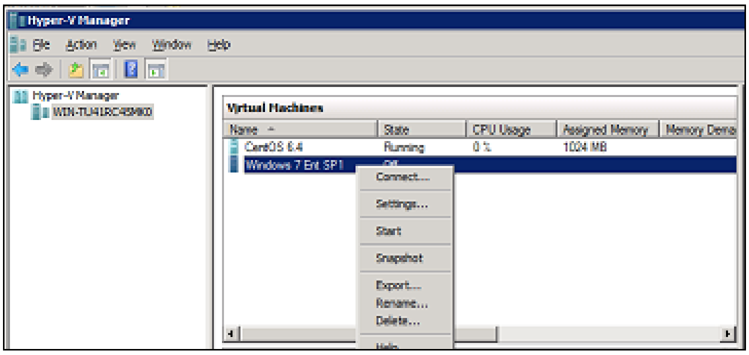
Estimated time left 0 sec

Restored 7.79k (3 files)

Elapsed time 1 min 25 sec

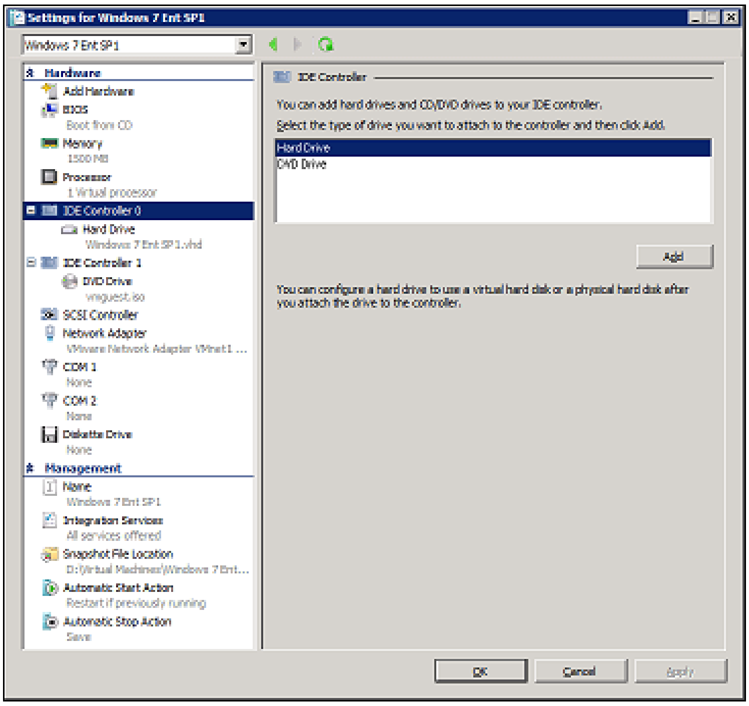
Transfer rate 840bit/s

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



Name	State	CPU Usage	Assigned Memory	Memory Dema
CentOS 6.4	Running	0 %	1024 MB	
Windows 7 Ent SP1	Off			

10. Select **Add** to add virtual disk to the guest virtual machine.

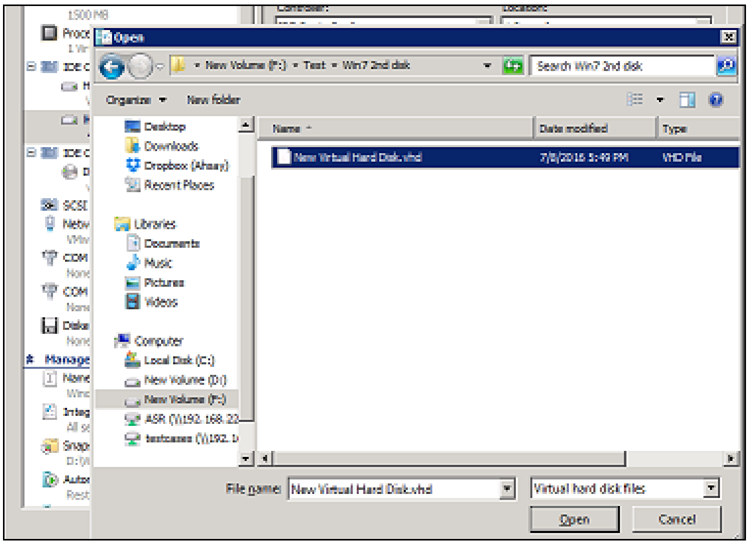


You can add hard drives and CD/DVD drives to your IDE controller.

Select the type of drive you want to attach to the controller and then click Add.

You can configure a hard drive to use a virtual hard disk or a physical hard disk after you attach the drive to the controller.

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

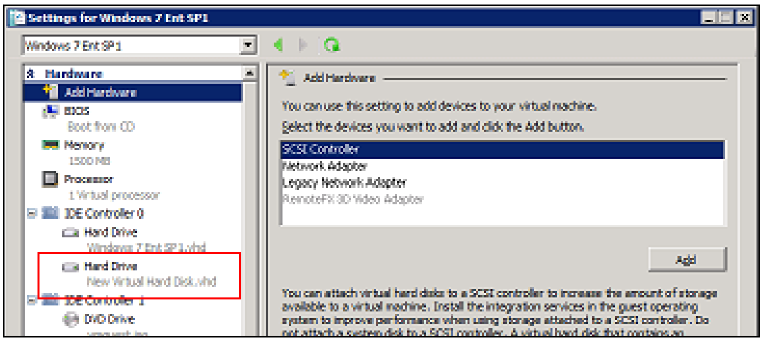


Name	Date modified	Type
New Virtual Hard Disk.vhd	7/8/2016 5:49 PM	VHD File

File name: New Virtual Hard Disk.vhd

Virtual hard disk files

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



You can use this setting to add devices to your virtual machine.

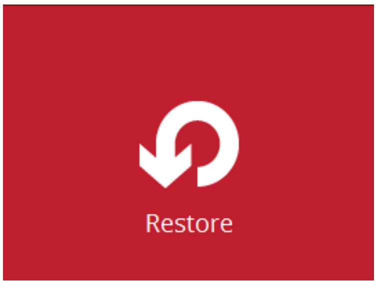
Select the devices you want to add and click the Add button.

You can attach virtual hard disks to a SCSI controller to increase the amount of storage available to a virtual machine. Install the integration services in the guest operating system to improve performance when using storage attached to a SCSI controller. Do not attach a system disk to a SCSI controller. A virtual hard disk that contains an

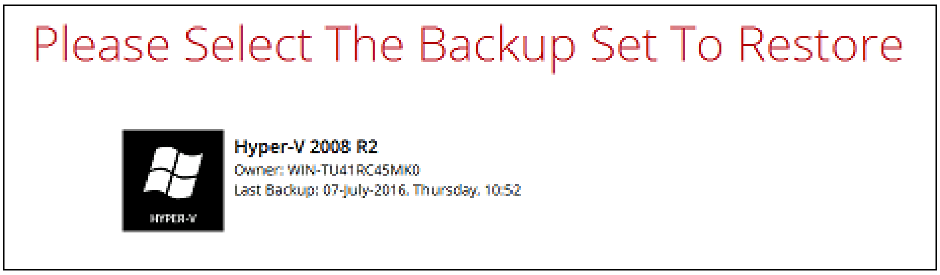
Initiate Restore of Guest Virtual Machine to an Alternate Location in the same Hyper-V Server Host

The restore to Alternate location is available for both Run Direct and Non-Run Direct backup sets, this feature will restore any guest virtual machine to another location (a different disk or folder) on the same Hyper-V server. The Restore to Alternate location can be used to restore only one guest virtual machine at any one time.

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



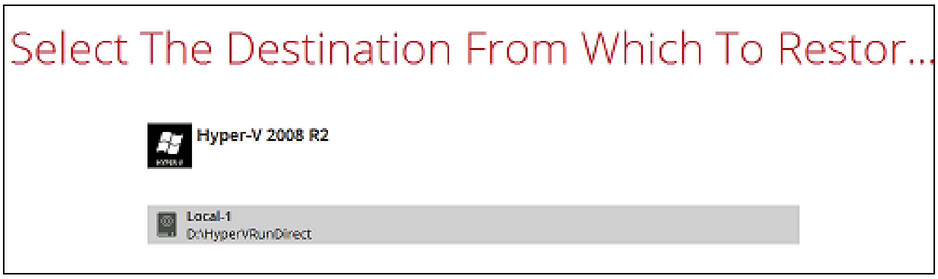
2. Select the backup set that you would like to restore the guest virtual machine from.



Please Select The Backup Set To Restore

Hyper-V 2008 R2
Owner: WIN-TU41RC45MK0
Last Backup: 07-July-2016, Thursday, 10:52

3. Select the drive storage destination that contains Hyper-V guest virtual machine that you would like to restore.

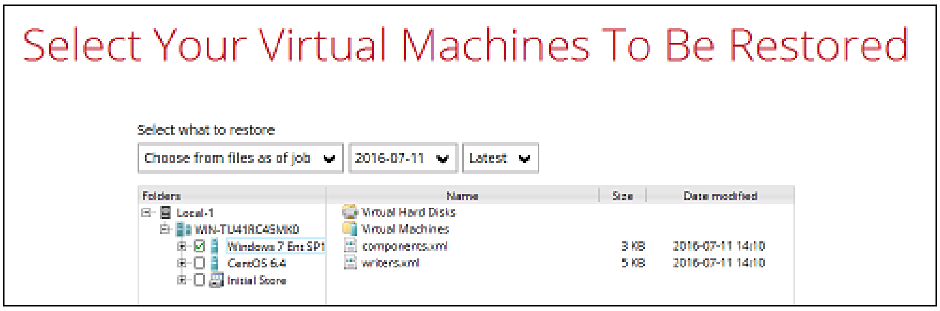


Select The Destination From Which To Restor...

Hyper-V 2008 R2

Local-1
D:\HyperVRunDirect

4. 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 Your Virtual Machines To Be Restored

Select what to restore

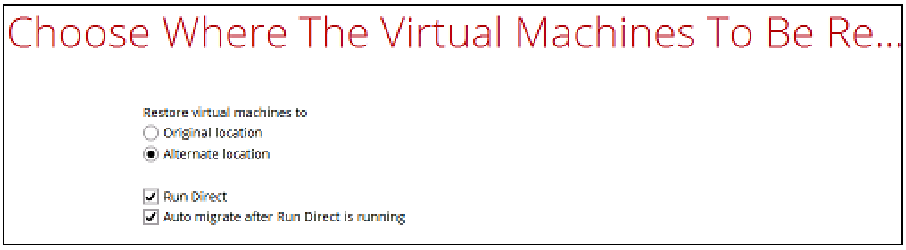
Choose from files as of job | 2016-07-11 | Latest

Folders:
- Local-1
  - WIN-TU41RC45MK0
    - ☑ Windows 7 Ent SP1
    - □ CentOS 6.4
    - □ Initial Store

Name	Size	Date modified
Virtual Hard Disks		
Virtual Machines		
components.xml	3 KB	2016-07-11 14:10
writers.xml	5 KB	2016-07-11 14:10

5. Select **Alternate location** and click **Next** to proceed.

Example: Restore a guest from using Run Direct with Auto Migration to another location.



Choose Where The Virtual Machines To Be Re...

Restore virtual machines to

○ Original location

● Alternate location

☑ Run Direct

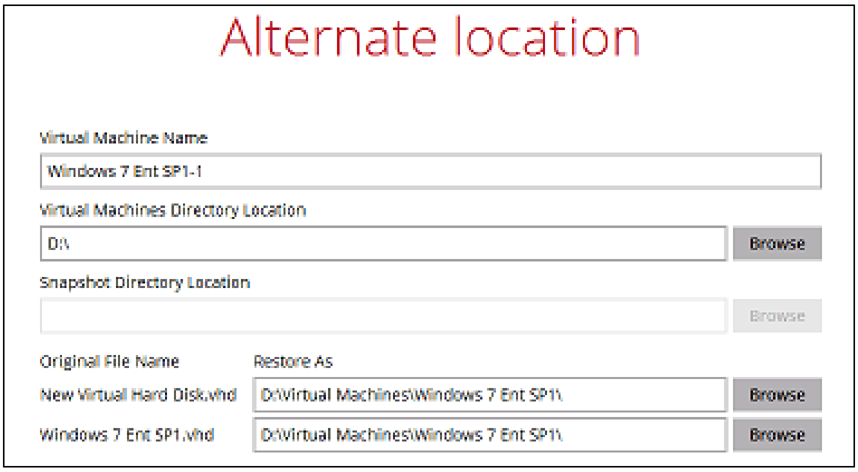
☑ Auto migrate after Run Direct is running

6. To restore the guest virtual machine to an Alternate location update the following values for:

   i. **Virtual Machine Name**

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

   iii. **Restore As (new location for the guest VHD files)**



Alternate location

Virtual Machine Name: Windows 7 Ent SP1-1

Virtual Machines Directory Location: D:\

Snapshot Directory Location:

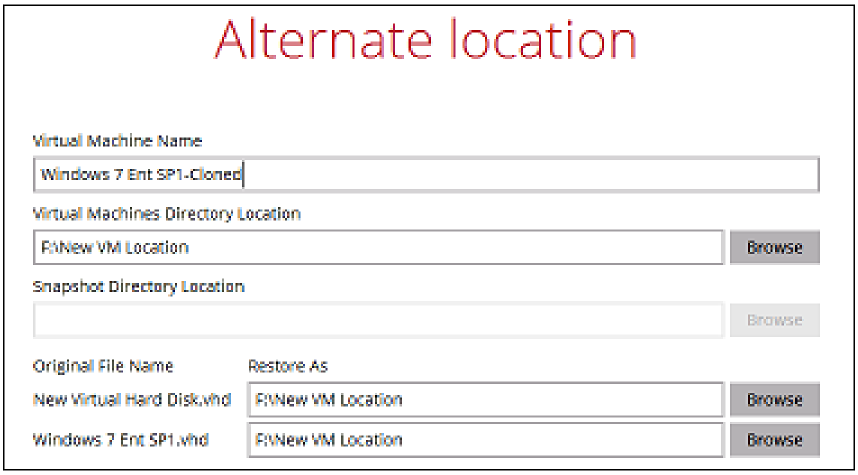
Original File Name	Restore As
New Virtual Hard Disk.vhd	D:\Virtual Machines\Windows 7 Ent SP1\
Windows 7 Ent SP1.vhd	D:\Virtual Machines\Windows 7 Ent SP1\

Example:

i. Rename the restored guest virtual machine to **Windows 7 Ent SP1-Cloned**

ii. Store the configuration files in the new location **F:\New VM Location**

iii. Store the VHD files files in the new location **F:\New VM Location**



Alternate location

Virtual Machine Name: Windows 7 Ent SP1-Cloned

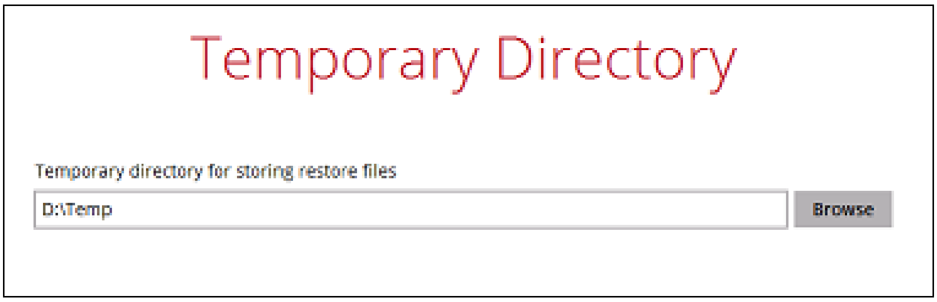
Virtual Machines Directory Location: F:\New VM Location

Snapshot Directory Location:

Original File Name	Restore As
New Virtual Hard Disk.vhd	F:\New VM Location
Windows 7 Ent SP1.vhd	F:\New VM Location

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.

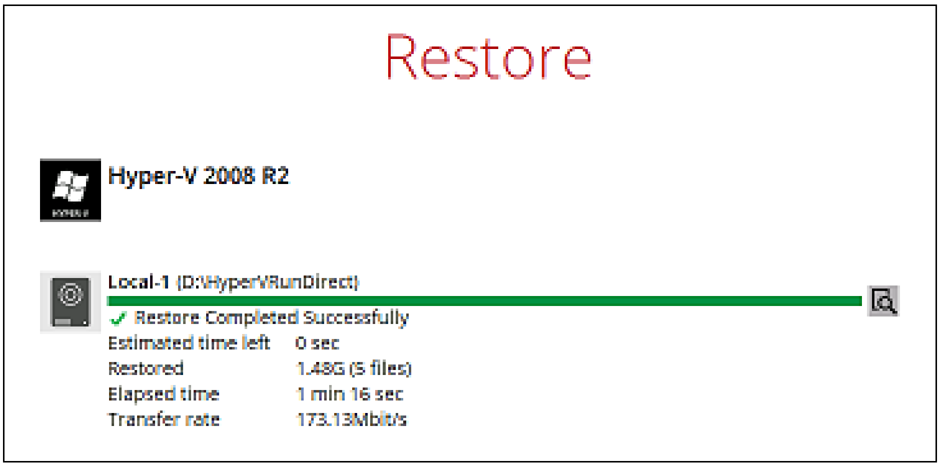


Temporary Directory

Temporary directory for storing restore files

D:\Temp

8. After the Hyper-V guest virtual machine has been restored successfully



Restore

Hyper-V 2008 R2

Local-1 (D:\HyperVRunDirect)

✓ Restore Completed Successfully

Estimated time left	0 sec
Restored	1.48G (5 files)
Elapsed time	1 min 16 sec
Transfer rate	173.13Mbit/s

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

Initiate Restore of Guest Virtual Machine to another Hyper-V Server (Different 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.

Requirements and Limitations:

1. AhsayOBM must be installed on the Hyper-V Host where you wish to restore the guest VM.

2. The same AhsayOBM backup account must be used.

3. The correct encryption key is required if the backup set was created with the encryption key feature enabled.

4. A guest virtual machine can only be restored to another Hyper-V server with the same version, i.e. backup of a guest on Hyper-V 2012 R2 server cannot be restored to Hyper-V 2008 R2 host or vice versa.

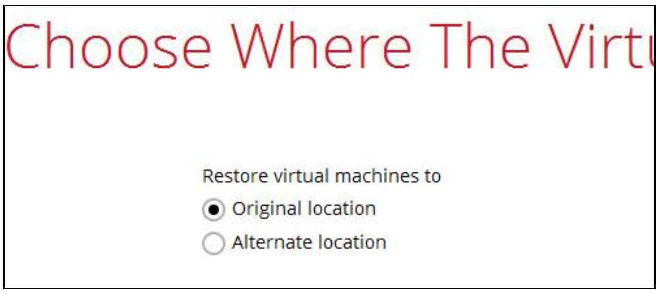
5. A guest virtual machine backed up from a standalone Hyper-V host can only be restored to another standalone Hyper-V host. A guest virtual machine backed up from a Hyper-V Cluster can only be restored to another Hyper-V Cluster.

6. Guest VMs 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).

7. The default Java heap size setting on AhsayOBM is 1024MB, for Hyper-V restore it is highly recommended to increase the Java heap size setting to improve performance. Especially guest VM's with many incremental delta files. (The actual heap size is dependent on amount of free memory available on your Hyper-V host).

8. The temporary directory should be set to a local drive for best restore performance. 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.

9. Restore guest VM's to original location is possible only if the disk setup on the new Hyper-V hosts 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".



Choose Where The Virtu

Restore virtual machines to

● Original location

○ Alternate location

10. The Hyper-V management tools are installed on the new Hyper-V host. For Hyper-V Cluster environments Hyper-V management tools is installed on all Cluster nodes.

11. The Hyper-V services are started on the host. For Hyper-V Cluster environment, the Hyper-V services are started on all Cluster nodes.

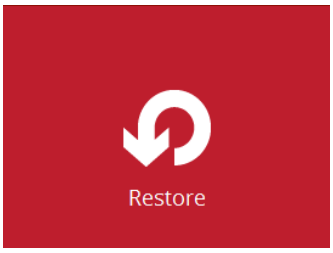
12. The **Microsoft Hyper-V VSS Writer** is installed and running on the new Hyper-V host and the writer state is Stable. This can be verified by running the vssadmin list writers command.

Example:

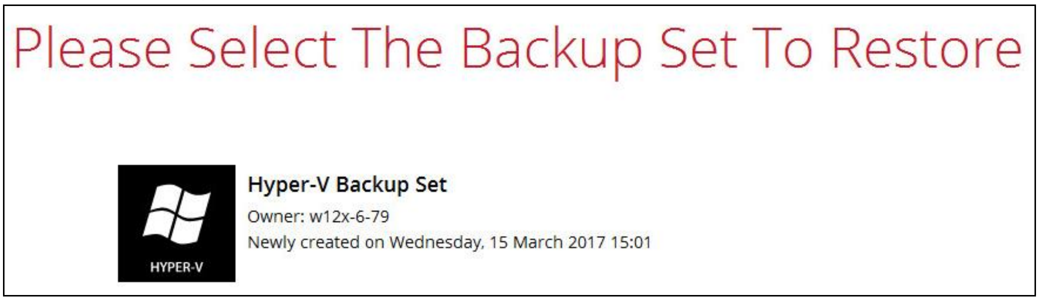
```
C:\Users\Administrator>vssadmin list writers
vssadmin 1.1 - Volume Shadow Copy Service administrative
command-line tool
(C) Copyright 2001-2005 Microsoft Corp.
Writer name: 'Task Scheduler Writer'
   Writer Id: {d61d61c8-d73a-4eee-8cdd-f6f9786b7124}
   Writer Instance Id: {1bddd48e-5052-49db-9b07-b96f96727e6b}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

Writer name: 'VSS Metadata Store Writer'
   Writer Id: {75dfb225-e2e4-4d39-9ac9-ffaff65ddf06}
   Writer Instance Id: {088e7a7d-09a8-4cc6-a609-ad90e75ddc93}
   State: [1] Stable
   Last error: No error

Writer name: 'Performance Counters Writer'
   Writer Id: {0bada1de-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-9a1e-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
```

Steps

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



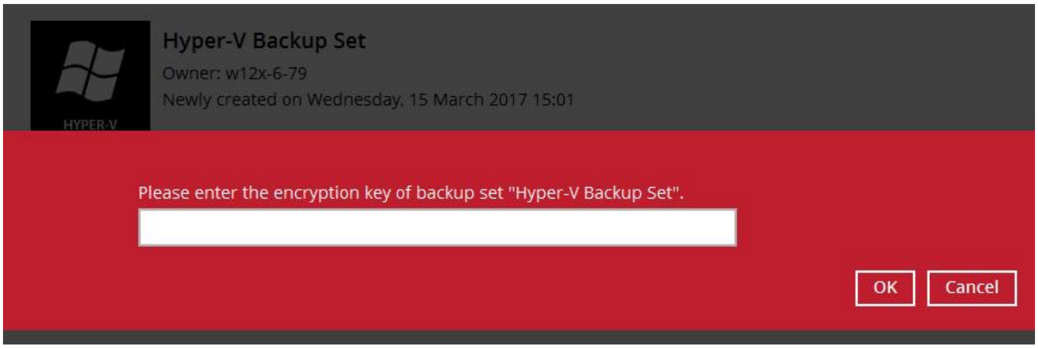
2. Select the backup set that you would like to restore the guest virtual machine from.



Please Select The Backup Set To Restore

Hyper-V Backup Set
Owner: w12x-6-79
Newly created on Wednesday, 15 March 2017 15:01

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.



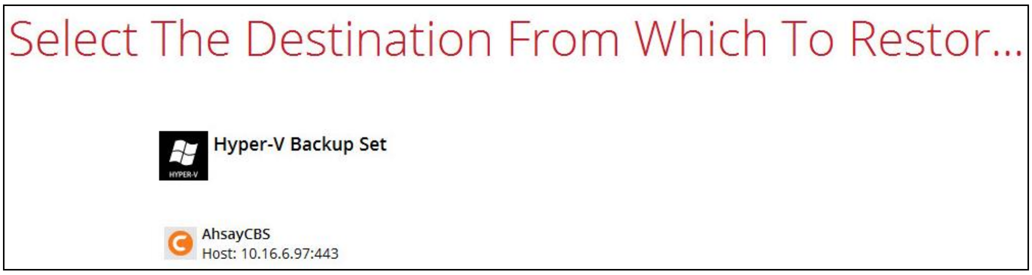
Hyper-V Backup Set

Owner: w12x-6-79

Newly created on Wednesday, 15 March 2017 15:01

Please enter the encryption key of backup set "Hyper-V Backup Set".

4. Select the drive storage destination that contains Hyper-V guest virtual machine that you would like to restore.



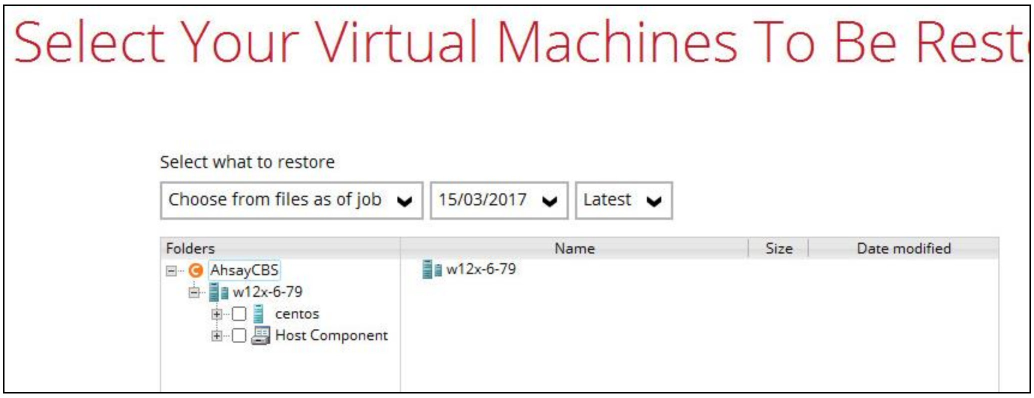
Select The Destination From Which To Restor...

Hyper-V Backup Set

AhsayCBS

Host: 10.16.6.97:443

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.



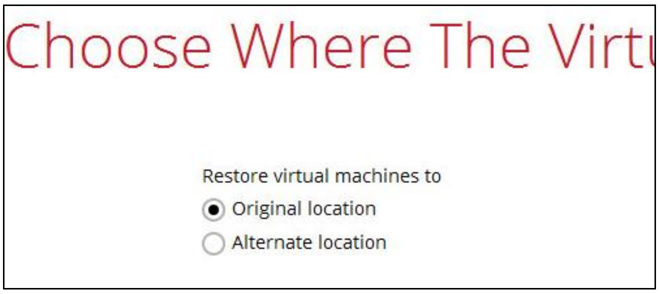
Select Your Virtual Machines To Be Rest

Select what to restore

Choose from files as of job | 15/03/2017 | Latest

Folders	Name	Size	Date modified
AhsayCBS w12x-6-79 □ centos □ Host Component	w12x-6-79		

6. Select to restore the Hyper-V guest to the Original location, or to an Alternate location, then click **Next** to proceed.



Choose Where The Virtu

Restore virtual machines to

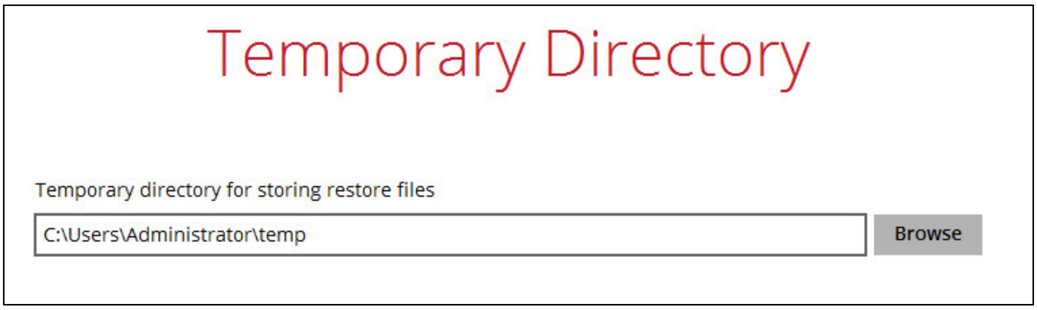
● Original location

○ Alternate location

Note

Restore to an Alternate location you can only be performed on one guest virtual machine at a time.

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



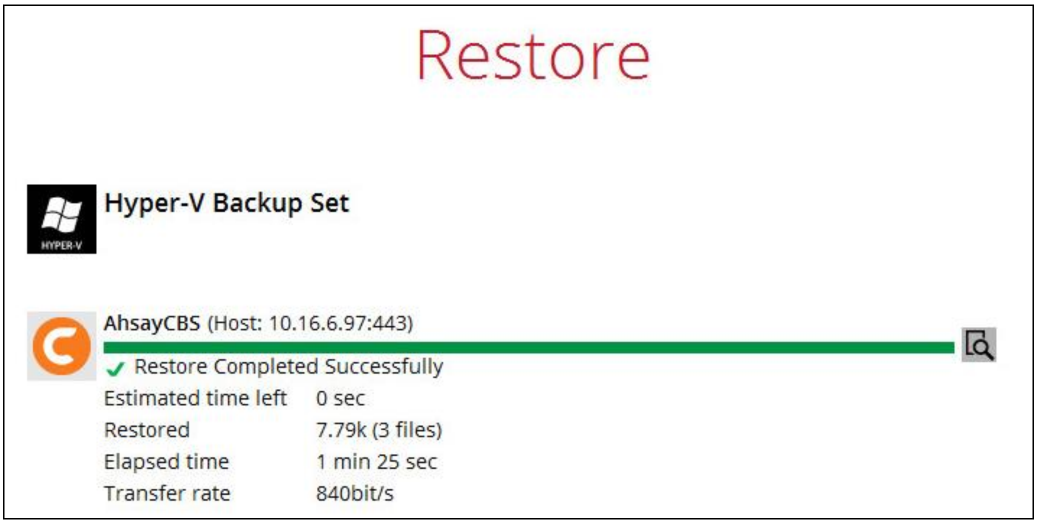
Temporary Directory

Temporary directory for storing restore files

C:\Users\Administrator\temp

8. Click **Restore** to start the restore process.

9. The following screen shows when the restore is completed.



Restore

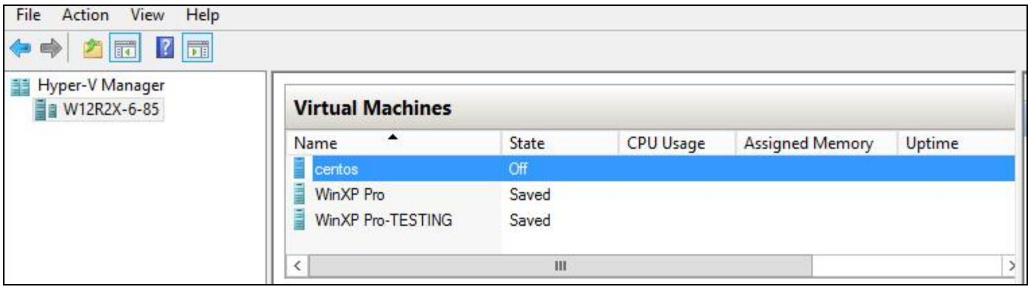
Hyper-V Backup Set

AhsayCBS (Host: 10.16.6.97:443)

✓ Restore Completed Successfully

Estimated time left	0 sec
Restored	7.79k (3 files)
Elapsed time	1 min 25 sec
Transfer rate	840bit/s

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



Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime
centos	Off			
WinXP Pro	Saved			
WinXP Pro-TESTING	Saved			

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

Requirements and Limitations

1. 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.

2. 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.

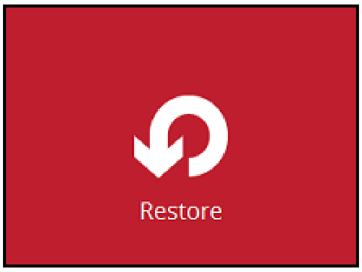
3. The mounting of Linux/Unix file systems from virtual disk file is currently not available due to limitations of the file system drivers.

4. 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.

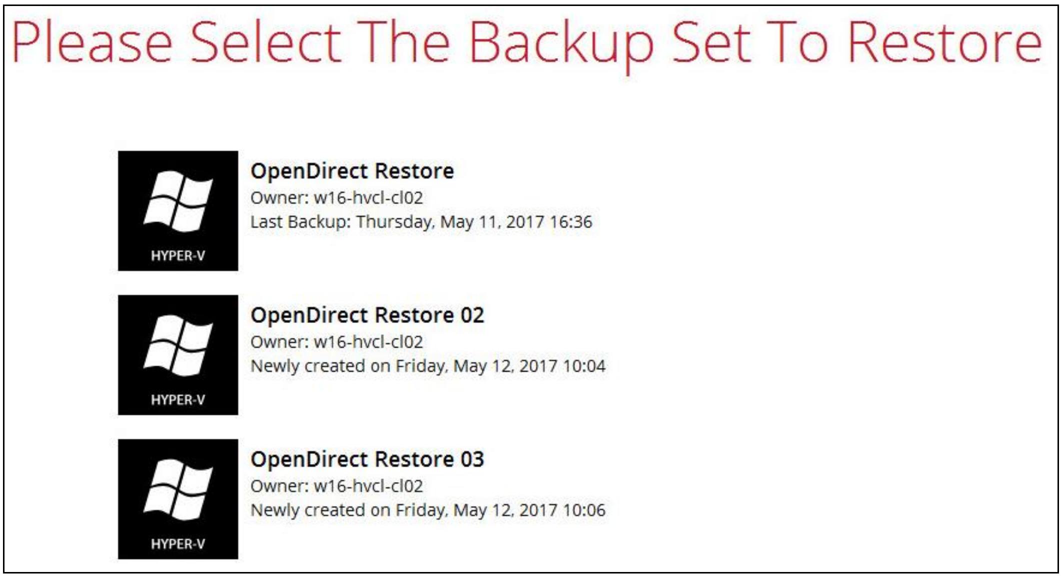
5. Windows User Account Control (UAC) must be disabled to apply granular restore.

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.



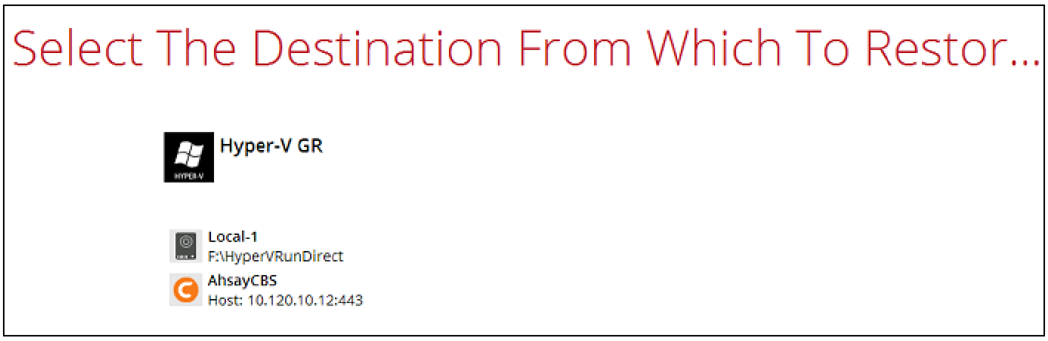
Please Select The Backup Set To Restore

OpenDirect Restore
Owner: w16-hvcl-cl02
Last Backup: Thursday, May 11, 2017 16:36

OpenDirect Restore 02
Owner: w16-hvcl-cl02
Newly created on Friday, May 12, 2017 10:04

OpenDirect Restore 03
Owner: w16-hvcl-cl02
Newly created on Friday, May 12, 2017 10:06

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



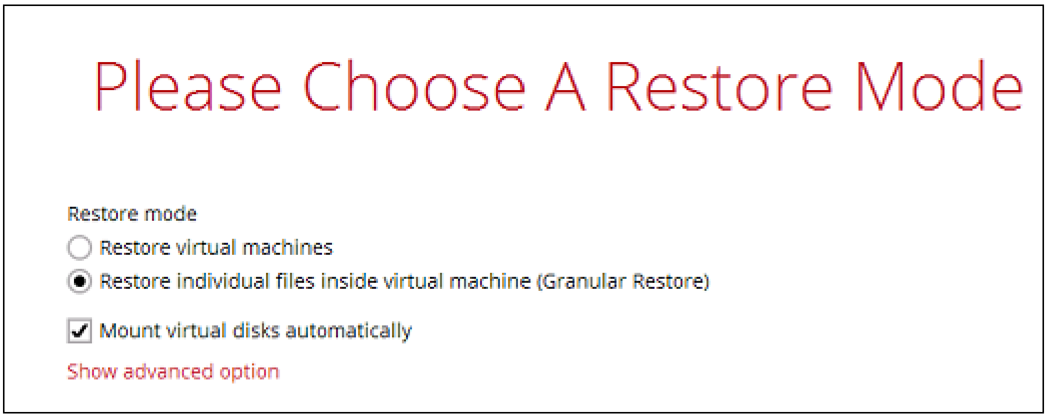
Select The Destination From Which To Restor...

Hyper-V GR

Local-1
F:\HyperVRunDirect

AhsayCBS
Host: 10.120.10.12:443

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


Please Choose A Restore Mode

Restore mode

○ Restore virtual machines

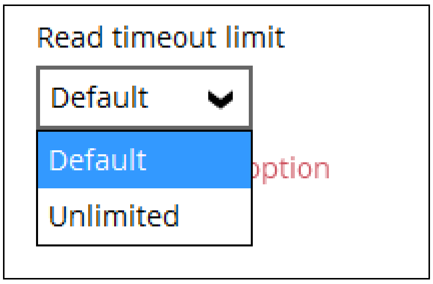
● Restore individual files inside virtual machine (Granular Restore)

☑ Mount virtual disks automatically

Note

The **Mount virtual disks automatically option** is selected by default. If the guest VM contains a 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

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

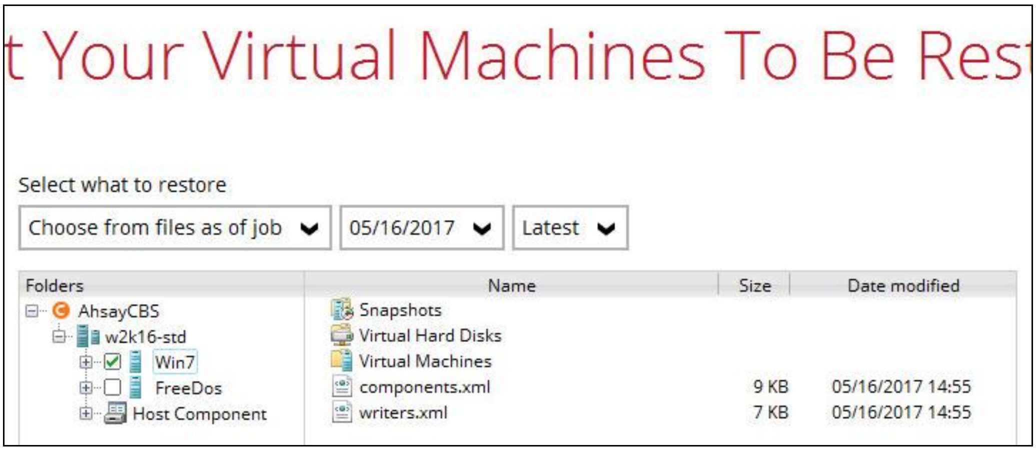
- **Default** – This setting should be suitable for guest VMs located on a local, removable, or network drive. The time out value is 15 seconds.
- **Unlimited** – the connection will not be time out when this is selected. This selection is recommended when:
  - Backup destination is a cloud stroage.
  - 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. Select the virtual machine that you would like to perform Granular Restore for, then click **Next** to proceed.



t Your Virtual Machines To Be Rest

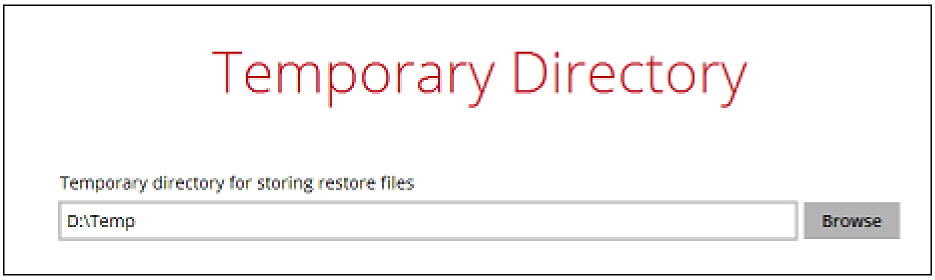
Select what to restore

Choose from files as of job | 05/16/2017 | Latest

Folders
- AhsayCBS
  - w2k16-std
    - ☑ Win7
    - □ FreeDos
    - Host Component

Name	Size	Date modified
Snapshots		
Virtual Hard Disks		
Virtual Machines		
components.xml	9 KB	05/16/2017 14:55
writers.xml	7 KB	05/16/2017 14:55

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

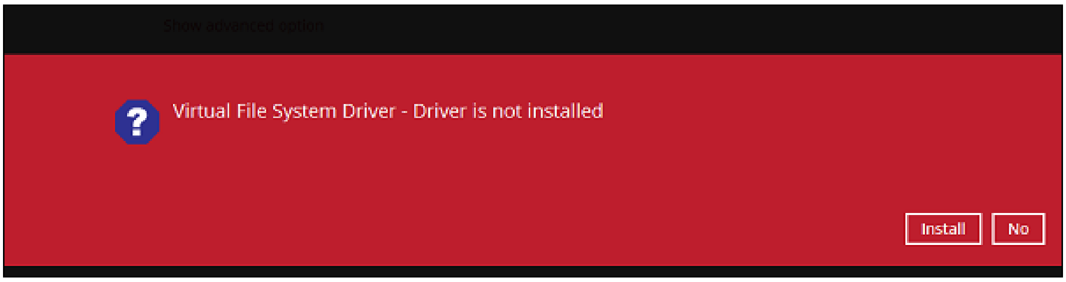


Temporary Directory

Temporary directory for storing restore files

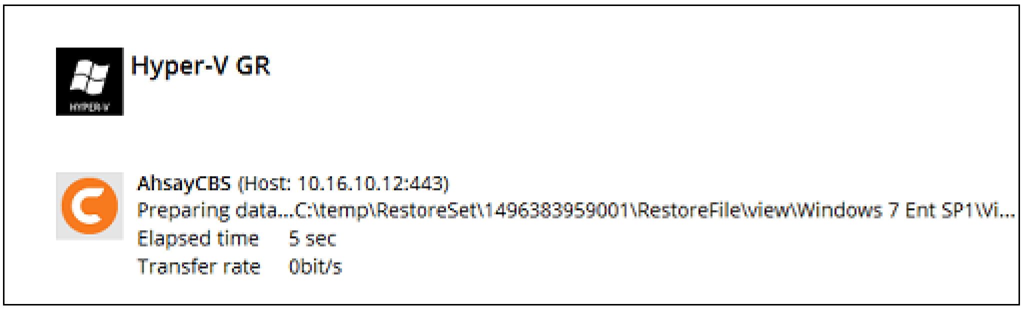
D:\Temp

7. The following screens show 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 t of the virtual disk on this machine. Clicking **No** will exit the restore process.



Virtual File System Driver - Driver is not installed

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

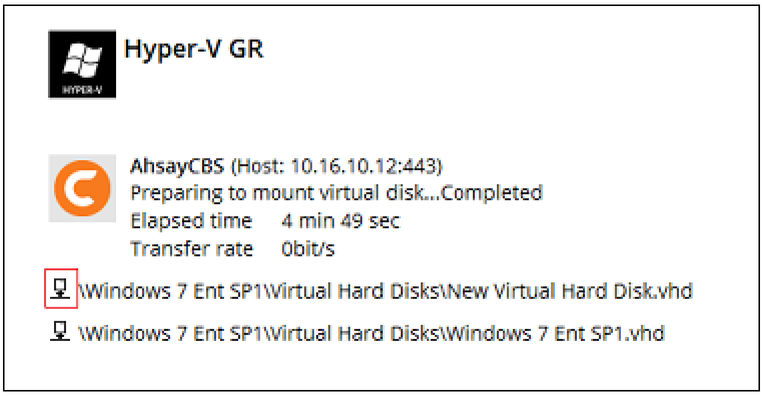


Hyper-V GR

AhsayCBS (Host: 10.16.10.12:443)
Preparing data...C:\temp\RestoreSet\1496383959001\RestoreFile\view\Windows 7 Ent SP1\Wi...
Elapsed time 5 sec
Transfer rate 0bit/s

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.

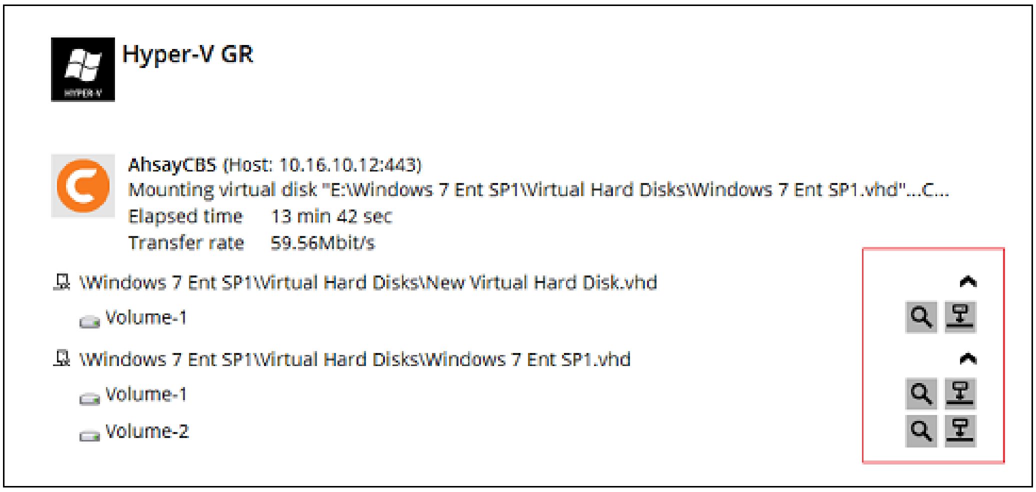


Hyper-V GR

AhsayCBS (Host: 10.16.10.12:443)
Preparing to mount virtual disk...Completed
Elapsed time 4 min 49 sec
Transfer rate 0bit/s

\Windows 7 Ent SP1\Virtual Hard Disks\New Virtual Hard Disk.vhd
\Windows 7 Ent SP1\Virtual Hard Disks\Windows 7 Ent SP1.vhd

Otherwise, the virtual disks will be automatically mounted.



Hyper-V GR

AhsayCBS (Host: 10.16.10.12:443)
Mounting virtual disk "E:\Windows 7 Ent SP1\Virtual Hard Disks\Windows 7 Ent SP1.vhd"...C...
Elapsed time 13 min 42 sec
Transfer rate 59.56Mbit/s

\Windows 7 Ent SP1\Virtual Hard Disks\New Virtual Hard Disk.vhd
Volume-1
\Windows 7 Ent SP1\Virtual Hard Disks\Windows 7 Ent SP1.vhd
Volume-1
Volume-2

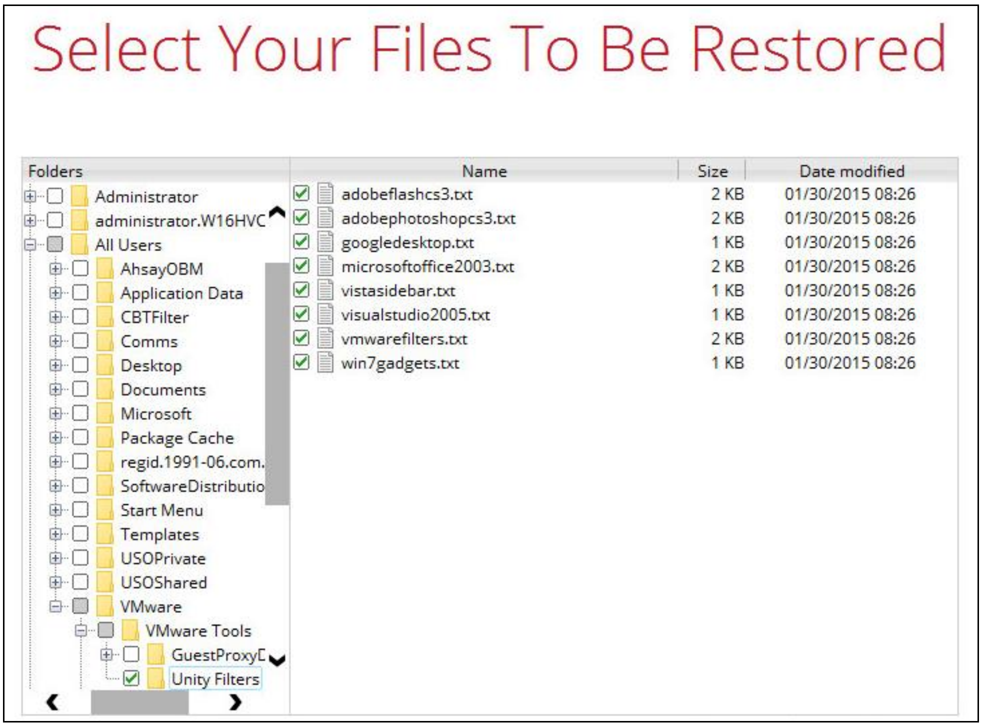
There are two options to restore individual files from here.

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.



Select Your Files To Be Restored

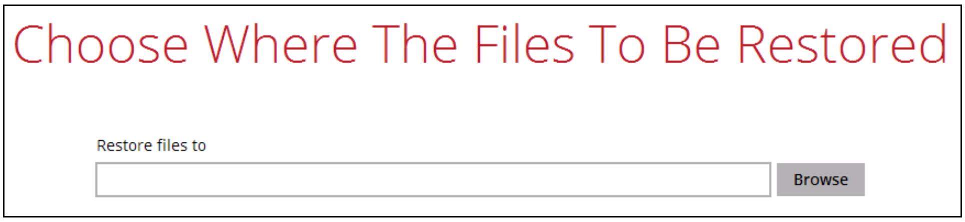
Folders
- ☐ Administrator
- ☐ administrator.W16HVC
- ▣ All Users
  - ☐ AhsayOBM
  - ☐ Application Data
  - ☐ CBTFilter
  - ☐ Comms
  - ☐ Desktop
  - ☐ Documents
  - ☐ Microsoft
  - ☐ Package Cache
  - ☐ regid.1991-06.com.
  - ☐ SoftwareDistributio
  - ☐ Start Menu
  - ☐ Templates
  - ☐ USOPrivate
  - ☐ USOShared
  - ▣ VMware
    - ▣ VMware Tools
      - ☐ GuestProxyD
      - ☑ Unity Filters

	Name	Size	Date modified
☑	adobeflashcs3.txt	2 KB	01/30/2015 08:26
☑	adobephotoshopcs3.txt	2 KB	01/30/2015 08:26
☑	googledesktop.txt	1 KB	01/30/2015 08:26
☑	microsoftoffice2003.txt	2 KB	01/30/2015 08:26
☑	vistasidebar.txt	1 KB	01/30/2015 08:26
☑	visualstudio2005.txt	1 KB	01/30/2015 08:26
☑	vmwarefilters.txt	2 KB	01/30/2015 08:26
☑	win7gadgets.txt	1 KB	01/30/2015 08:26

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.

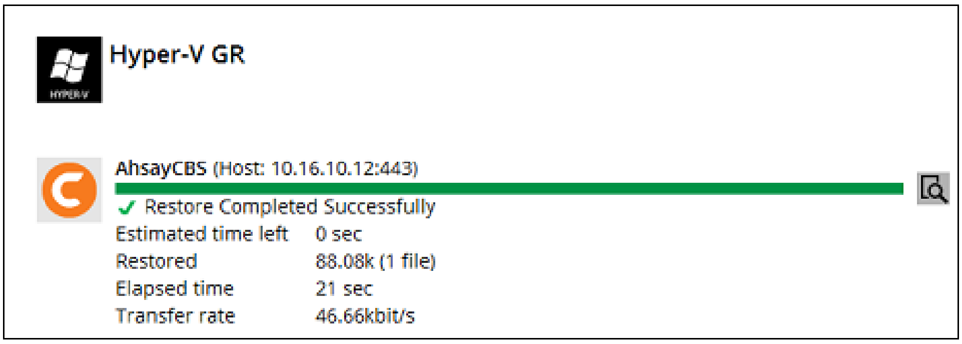
ii. Select a path where you wish the files to be restored to, then click **Restore**.



Choose Where The Files To Be Restored

Restore files to

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



Hyper-V GR

AhsayCBS (Host: 10.16.10.12:443)

✓ Restore Completed Successfully

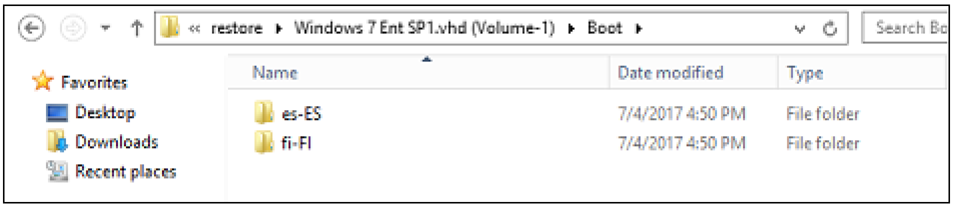
Estimated time left 0 sec

Restored 88.08k (1 file)

Elapsed time 21 sec

Transfer rate 46.66kbit/s

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



Name	Date modified	Type
es-ES	7/4/2017 4:50 PM	File folder
fi-FI	7/4/2017 4:50 PM	File folder

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

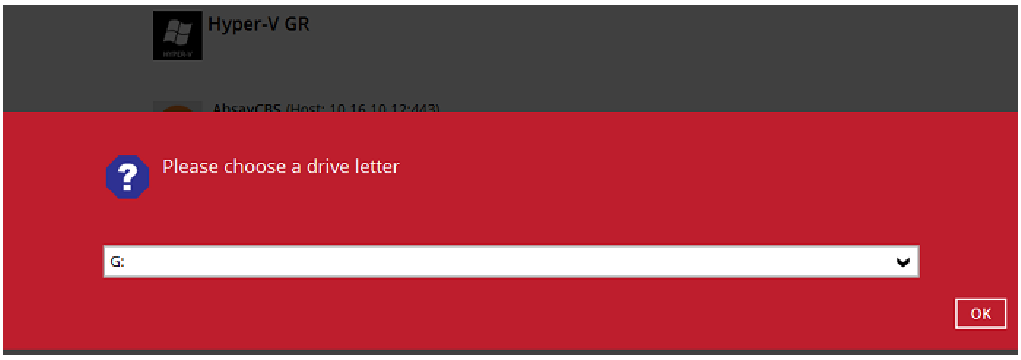
Granular restore of Hyper-V backup sets performed using Windows File Explorer :

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 AshayOBM.

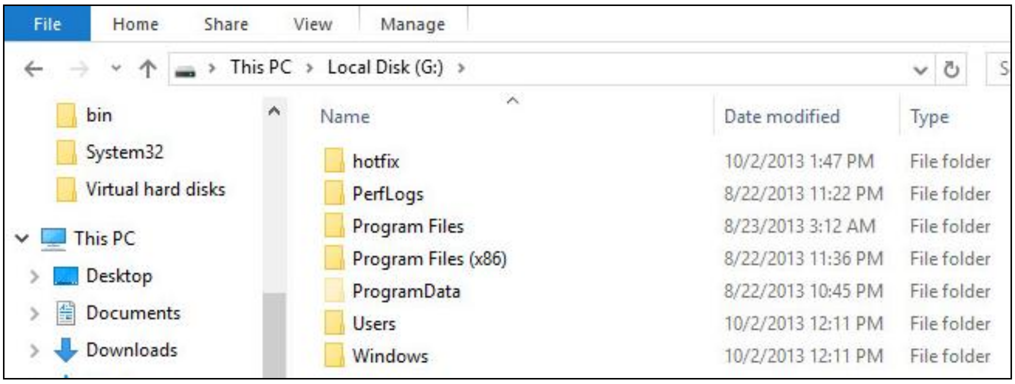
i. Click and then you will be prompted to select a driver letter where you wish the mounted image to be mapped on your machine, click **OK** when you have finished selection.



Please choose a drive letter

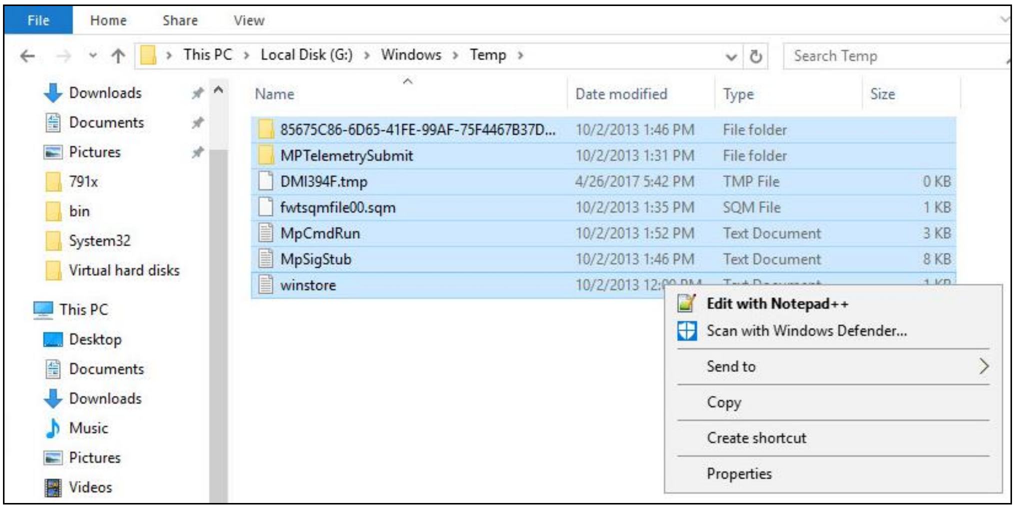
G:

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



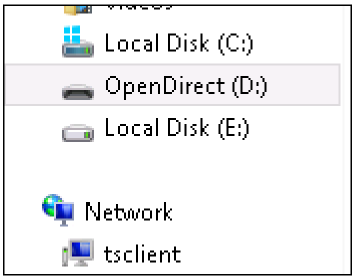
Name	Date modified	Type
hotfix	10/2/2013 1:47 PM	File folder
PerfLogs	8/22/2013 11:22 PM	File folder
Program Files	8/23/2013 3:12 AM	File folder
Program Files (x86)	8/22/2013 11:36 PM	File folder
ProgramData	8/22/2013 10:45 PM	File folder
Users	10/2/2013 12:11 PM	File folder
Windows	10/2/2013 12:11 PM	File folder

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.

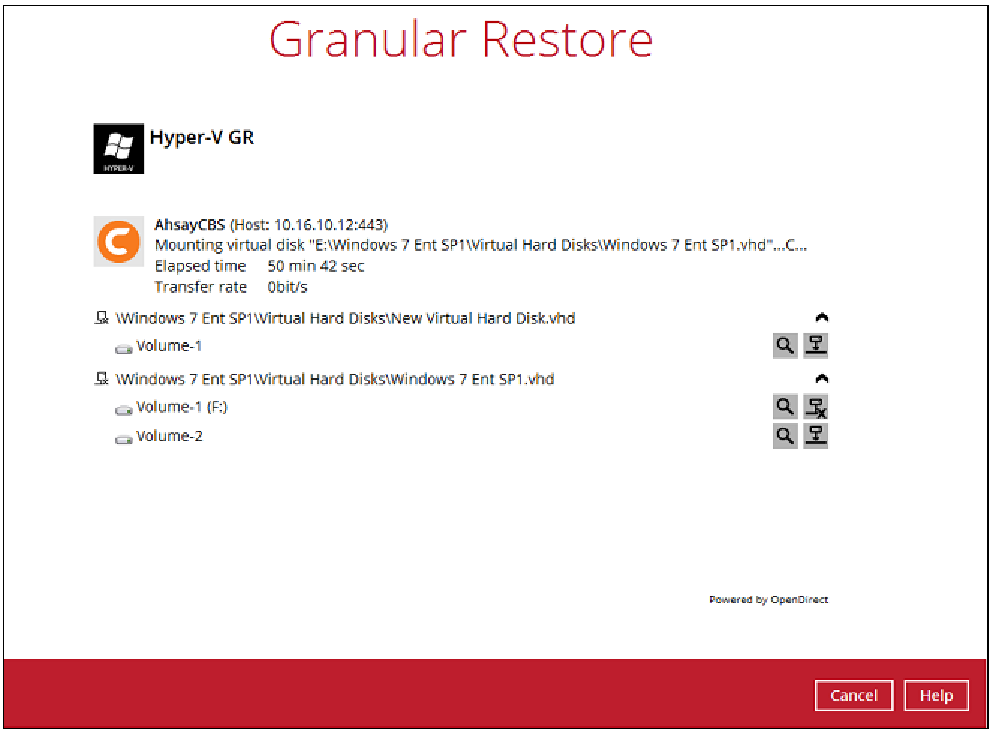


Name	Date modified	Type	Size
85675C86-6D65-41FE-99AF-75F4467B37D...	10/2/2013 1:46 PM	File folder	
MPTelemetrySubmit	10/2/2013 1:31 PM	File folder	
DMI394F.tmp	4/26/2017 5:42 PM	TMP File	0 KB
fwtsqmfile00.sqm	10/2/2013 1:35 PM	SQM File	1 KB
MpCmdRun	10/2/2013 1:52 PM	Text Document	3 KB
MpSigStub	10/2/2013 1:46 PM	Text Document	8 KB
winstore	10/2/2013 12:		

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



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



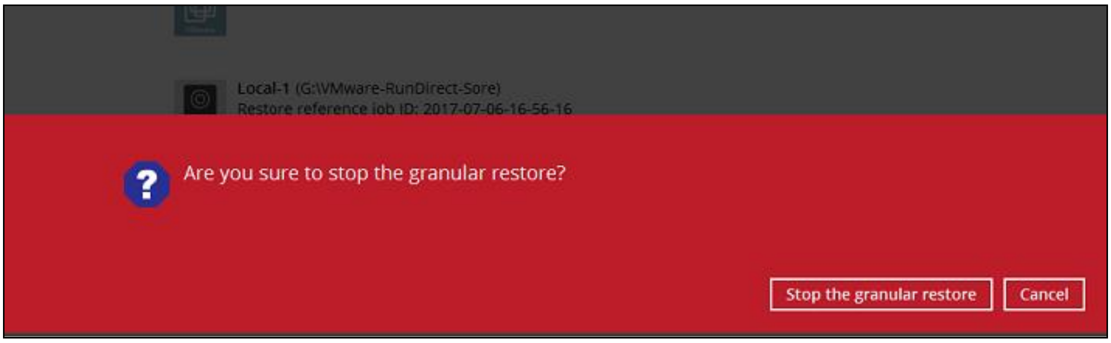
Granular Restore

Hyper-V GR

AhsayCBS (Host: 10.16.10.12:443)
Mounting virtual disk "E:\Windows 7 Ent SP1\Virtual Hard Disks\Windows 7 Ent SP1.vhd"...C...
Elapsed time 50 min 42 sec
Transfer rate 0bit/s

\Windows 7 Ent SP1\Virtual Hard Disks\New Virtual Hard Disk.vhd
Volume-1
\Windows 7 Ent SP1\Virtual Hard Disks\Windows 7 Ent SP1.vhd
Volume-1 (F:)
Volume-2

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



Local-1 (G:\VMware-RunDirect-Sore)
Restore reference job ID: 2017-07-06-16-56-16

Are you sure to stop the granular restore?

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

Technical Assistance

To contact Ahsay support representatives for technical assistance, visit the following website:
https://www.ahsay.com/jsp/en/contact/kbQuestion.jsp

Also use the Ahsay Knowledge Base for resource such as Hardware Compatibility List, Software Compatibility List, and other product information:
http://wiki.ahsay.com/doku.php?id=public:home

Documentation

Documentations for all Ahsay products are available at:
https://www.ahsay.com/jsp/en/home/index.jsp?pageContentKey=ahsay_downloads_documentation_guides

You can send us suggestions for improvements or report on issues in the documentation, by contacting us at:
https://www.ahsay.com/jsp/en/contact/kbQuestion.jsp

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