

Ahsay Online Backup Manager v8

VMware vCenter/ESXi Guest Virtual Machine Backup & Restore Guide

Ahsay Systems Corporation Limited

9 May 2019

Copyright Notice

© 2019 Ahsay Systems Corporation Limited. All rights reserved.

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

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

Trademarks

Ahsay, Ahsay Cloud Backup Suite, Ahsay Online Backup Suite, Ahsay Offsite Backup Server, Ahsay Online Backup Manager, Ahsay A-Click Backup, Ahsay Replication Server, Ahsay BackupBox Firmware, Ahsay Universal Backup System, 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
9 May 2019	Updated wiki links in Ch. 3, 4 and 7; Updated screen shots in Ch. 7, 9, 11, 12, 13 and 14	Modified

Table of Contents

1 Overview	1
What is this software?	1
System Architecture	1
Why should I use AhsayOBM to back up my VMware vCenter/ESXi?	2
What is the purpose of this document?	7
What should I expect from this document?	7
Who should read this document?	7
2 Understanding Backup Mode	8
Backup Mode	8
Non-VDDK Backup Mode	8
VDDK Backup Mode	8
Features Comparison between VDDK and Non-VDDK Modes	9
3 Requirements	10
Hardware Requirement	10
Software Requirement	10
Antivirus Exclusion Requirement	10
VMware vCenter / ESXi Server Requirements	10
ESXi / vCenter Patch Release	10
License Specification	10
ESXi Shell Access	10
SSH	11
Root Account	11
Port Requirement	11
Disk Space Available on Datastore	11
Maximum Virtual Disk Size	11
VMware Tools	11
ESXi/ESX Hosts and Virtual Machine Hardware Versions Compatibility	12
Backup Client Computer Requirements	12
Hardware and Software Requirement	13
Add-on Module Requirement	13
Backup Quota Requirement	13
Port Requirement	13
Backup Client Computer on Linux	14
Disk Space Available on Backup Client Computer (or the vCenter computer)	14
Windows OS Requirement for VDDK and Non-VDDK Modes Backup	14
Run Direct Requirements	15
VDDK Backup Mode	15

Backup Destination Requirement	15
VDDK Backup Mode Requirements	16
License Requirement.....	16
Changed Block Tracking (CBT) on VMs	17
VMware Snapshot	18
Virtual Machine State	18
File Name Requirement.....	18
Non-VDDK Backup Mode Requirements.....	18
4 Best Practices and Recommendations.....	19
5 Granular Restore Technology	21
What is Granular Restore Technology?.....	21
How does Granular Restore work?	22
Benefits of using Granular Restore	22
Requirements.....	24
Supported Backup Modules.....	24
License Requirements.....	24
Backup Quota Storage	24
Operating System.....	24
Temporary Directory Requirement.....	24
Available Spare Drive Letter	24
Network Requirements	24
Other Dependencies.....	25
Permissions.....	25
6 Starting AhsayOBM	26
Login to AhsayOBM	26
7 Creating a VMware VM Backup Set.....	27
8 Overview on Backup Process.....	37
9 Running a Backup	38
Start a Manual Backup.....	38
Configure Backup Schedule for Automated Backup	40
10 Restore Methods.....	43
11 Method 1 - Restoring a Virtual Machine with Run Direct.....	45
Login to AhsayOBM	45
Running Direct Restore via AhsayOBM.....	45
Verifying Run Direct Restore Connection	51
Manage Run Direct VM.....	53
Finalize VM Restore	54

Stop Run Direct VM.....	55
Run Direct Restore via User Web Console	56
12 Method 2 - Restoring a Virtual Machine without Run Direct	58
Login to AhsayOBM	58
VM Restore without Run Direct	58
13 Method 3 - Restoring a Virtual Machine in Raw File (VMDK Format)	64
Restoring a VM in VMDK format	64
14 Method 4 – Granular Restore.....	70
Requirements and Limitations	70
15 Contact Ahsay.....	79
Technical Assistance	79
Documentation	79

1 Overview

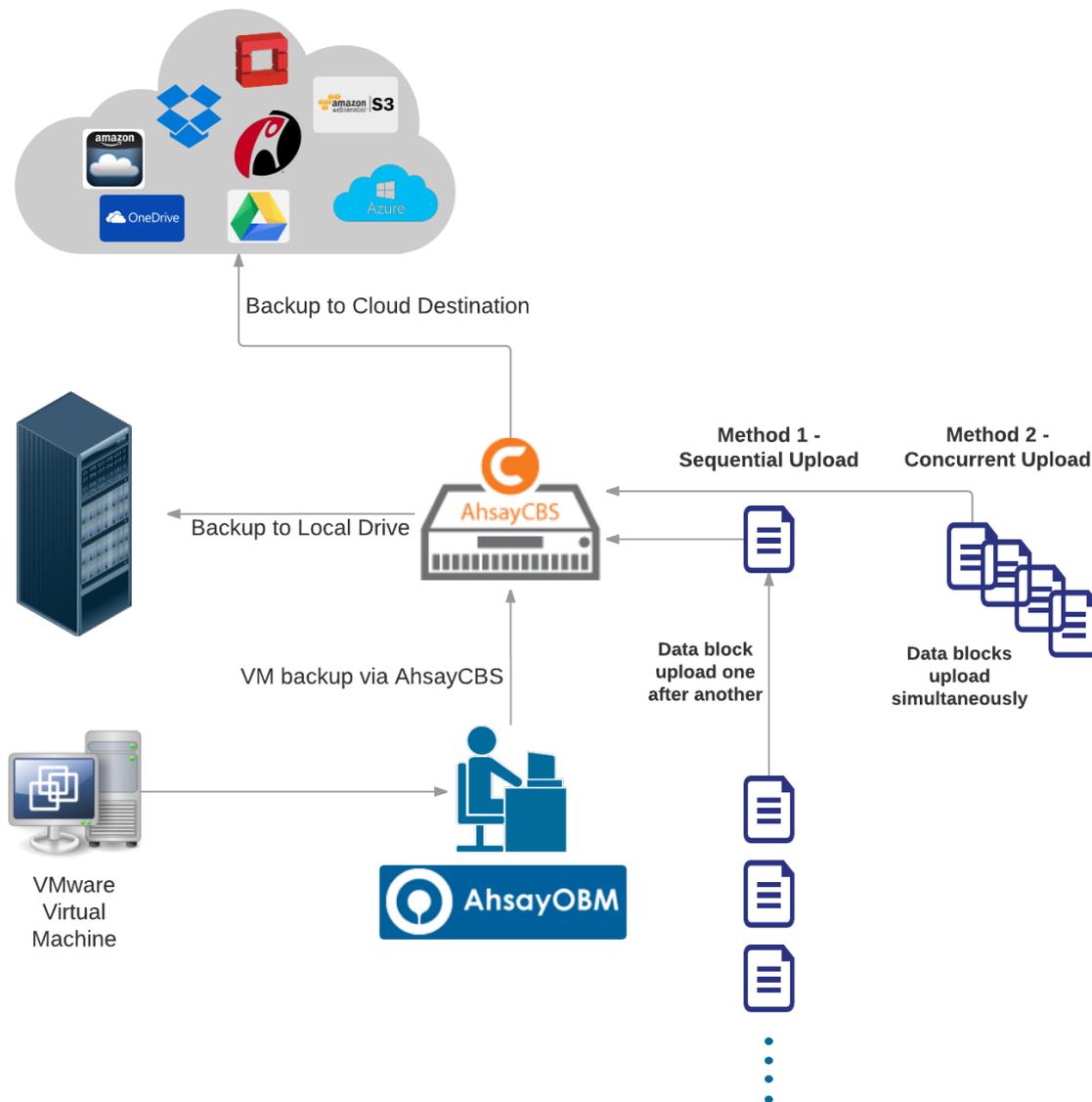
What is this software?

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

System Architecture

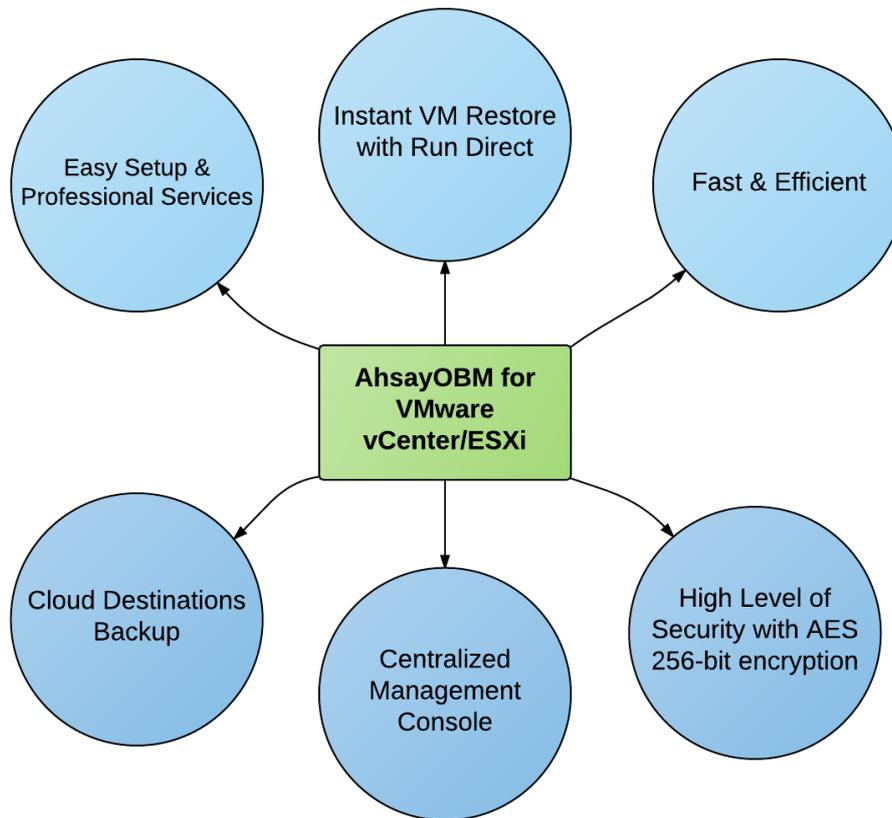
Below is the system architecture diagram illustrating the major elements involved in the backup process among the VMware server, AhsayOBM and AhsayCBS.

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.



Why should I use AhsayOBM to back up my VMware vCenter/ESXi?

We are committed to bringing you a comprehensive VMware backup solution with AhsayOBM. Below are some key areas we can help making your backup experience a better one.



Easy Setup & Professional Services

Setup is a few clicks away - our enhanced AhsayOBM v8 can be easily downloaded and installed in just a few clicks. The refined user interface also provides user-friendly instructions to guide you through installation, configuration, backup and restore. The intuitive setup procedures together with instructions in this user guide makes the software installation and operations easy even for layman users. That being said, if you do run into any problems during setup, we are here to help out. Visit the URL below for details on technical assistance.

<https://www.ahsay.com/jsp/en/contact/kbQuestion.jsp>

Professional Services

AhsayOBM Installation and Configuration Service

If you would like to save the time of reading through this document for setup, we have introduced this service to take care of all the installation and setup for you. On top of the installation and setup services, we also have a whole series of premium after-sales services to provide you with the best user experiences possible.

Valid Maintenance

Our Valid Maintenance provides you with professional and timely customer support along the way. You are entitled to the Valid Maintenance for free during the first year of your service subscription, and recurring annual fee at 20% of your annual subscription fee.

Refer to our [Professional Services](#) webpage for further details and subscription.



Instant VM Restore with Run Direct

What is Run Direct?

Run Direct is a feature that helps reduce disruption and downtime of your production VMs.

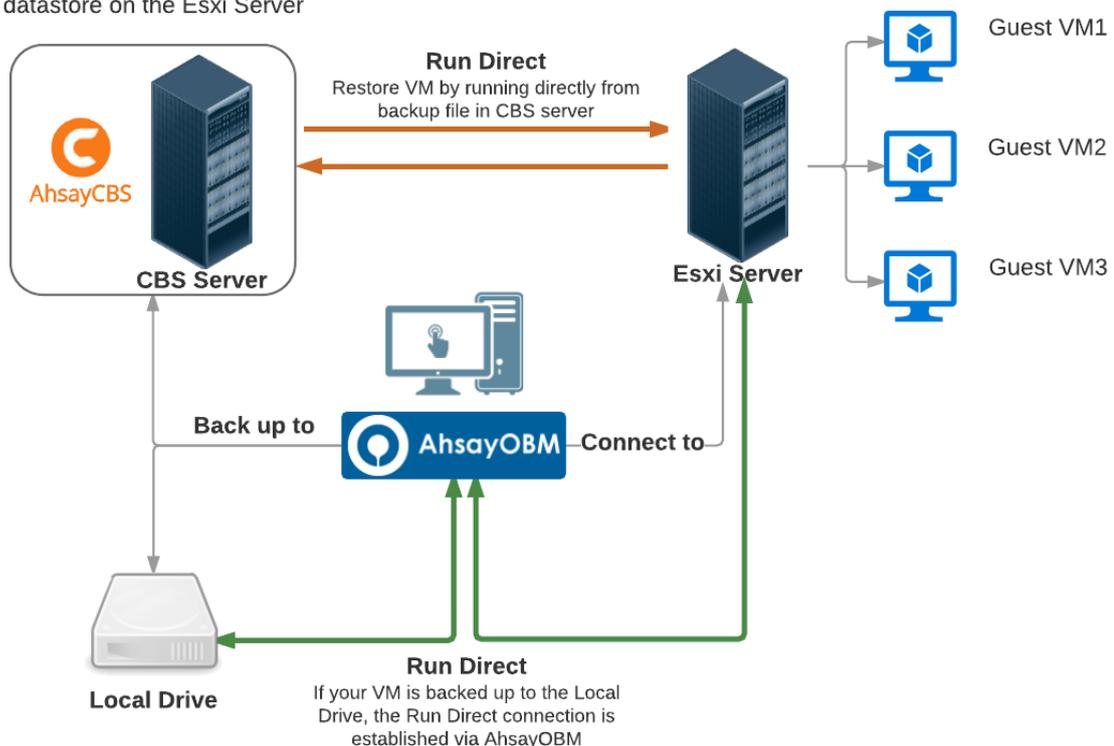
Unlike normal VM restore procedure where a VM is extracted from backup files and copied to the production storage, which can take hours to complete. Restore with Run Direct can instantly power up a VM by running it directly from the backup files in the backup destination and the VM can be put into production.

How does Run Direct work?

When a Run Direct restore is performed, the backup destination is mounted as an NFS datastore from the VMware host, where the VM is run directly from the backup files.

The backup destination can either be the AhsayCBS server or a local drive that can connect with AhsayOBM. Initiating a Run Direct from the AhsayCBS (also known as agentless restore) will trigger a connection directly with the VMware host (ESXi server and the direction shown in orange indicator below), while initiating the same action on the AhsayOBM requires the connection to route through the OBM (shown in green indication below).

Run Direct Restore - CBS
server is mounted as NFS
datastore on the Esxi Server



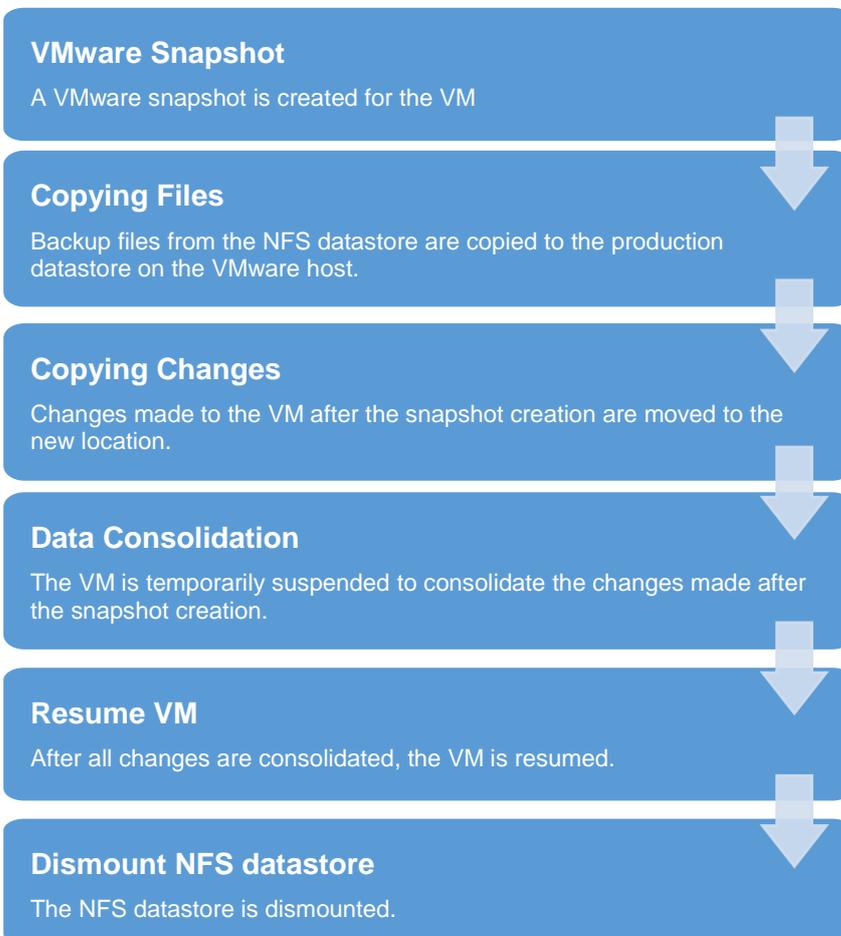
The restored virtual machine, at this stage (e.g. before the restore is finalized) is in a read-only state to preserve its integrity. All changes made to the virtual disks (e.g. operation within the guest virtual machine) are stored separately in transaction logs stored on the NFS datastore or the original datastore, depending on the setting selected. These changes are discarded when Run Direct is stopped, where the restored VM 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.

Settings Differences between Run Direct and Non-Run Direct Backup Set on VMware

	Run Direct Backup Set	Non-Run Direct Backup Set
Encryption	NO	YES
Compression	NO	YES
VDDK (CBT)	YES	YES
AhsayCBS	YES	YES
Local Destination	YES	YES
Cloud Destination	NO	YES

Finalizing a VM Recovery (Migrating VM to permanent location)

To finalize recovery of a VM, you will still need to migrate it to a permanent location on the VMware host. The following steps are taken when you finalize a Run Direct restore:



NOTE

For vCenter VM backup set, provided that the vMotion feature of the vCenter set is working properly, the VM will not be suspended during the data consolidation.

For more details on how to setup a VMware VM backup set with Run Direct, refer to the chapter on [Configuring a VMware VM Backup Set](#).



Fast and Efficient

We understand that backup could be a time and resources consuming process, which is why AhsayOBM is designed with advanced technologies to make backup a fast and efficient process.

We also understand that you may wish to run backup at a specified time interval of your choice, that's why we also allow you to set your own backup schedules so that you can take full control of the time when to perform backup.

- **Multi-threading** – this technology utilizes the computing power of multiple CPU cores for creating multiple backup and restore threads to produce fast backup and restore performance.
- **Block Level Incremental Backup** – this technology breaks down the backup files into multiple blocks and only the changed blocks will be backed up each time.



Centralized Management Console

Our enriched features on the centralized web console offers you a one-stop location for monitoring and managing your backup and restore, whether you are a system administrator or backup user. Below is an overview of what you can do with it depending on your role. For more details regarding the setup and operations of the centralized management console, refer to the [administrator guide](#).

- **System Administrator** – full control over the user accounts and their backup and restore activities, as well as all system related settings. For more details regarding the centralized management console, refer to the [user guide](#).
- **Backup User** – configure backup settings, monitor backup and restore activities, and initiate a Run Direct activity.



Cloud Destinations Backup

To offer you with the highest flexibility of backup destination, you can now back up server data to a wide range of cloud storage destinations. Below is a list of supported cloud destinations.

Aliyun (阿里云) *	CTYun (中国电信天翼云) *	Amazon S3	Amazon Cloud Drive
Google Cloud Storage	Google Drive	OneDrive	Microsoft OneDrive / OneDrive for Business
Rackspace	OpenStack	Microsoft Azure	Dropbox
FTP	SFTP	AWS S3 Compatible Cloud Storage	

* Available on computers with China or Hong Kong local settings

Cloud backup gives you **two major advantages**:

- **Multi-destination Backup for Extra Protection** – you can now back up your VM to both local drive and cloud destination. While local drive backup gives you the convenience of faster backup and restore as a result of the locally resided infrastructure, you can take a further step to utilize the cloud backup to give you an extra layer of protection in the event of a local drive corruption, where you will still be able to retrieve data from the cloud destination.
- **Eliminate Hardware Investment** – with the increasingly affordable cloud storage cost, you can deploy on cloud platform and utilize cloud storage as your centralized data repository, or simply expand your cloud storage as a backup destination without having to invest on hardware.



High Level of Security

We understand your VM may contain sensitive information that requires to be protected, that is why your backup data will be encrypted with the highest level of security measure.

- **Un-hackable Encryption Key** – to provide the best protection to your backup data, you can turn on the encryption feature which will default encrypt the backup data locally with AES 256-bit truly randomized encryption key.
- **Encryption Key Recovery** – Furthermore, we have a backup plan for you to recover your encryption key in case you have lost it. Your backup service provider can make it mandatory for you to upload the encryption key to the centralized management console, the encryption key will be uploaded in hashed format and will only be used when you request for a recovery.

What is the purpose of this document?

This document aims at providing all necessary information for you to get started with setting up your system for VMware VM backup and restore, followed by step-by-step instructions on creating backup set, running backup job and restoring backed up data.

The document can be divided into 3 main parts.

Part 1: Preparing for VMware VM Backup & Restore

Understanding Backup Mode

Introduce the differences between Non-VDDK and VDDK backup modes

Requirements

Requirements on hardware, software, VMware server, Client Backup Computer, Run Direct, and Non-VDDK/VDDK backup modes

Best Practices and Recommendations

Items recommended to pay attention to before backup and restore

Part 2: Performing VMware VM Backup

Creating a Backup Set

Log in to AhsayOBM and create backup set

Running a Backup Set

Run backup set & configure backup schedule for automated backup

Part 3: Performing VMware VM Restore

Restoring VM with Run Direct

Steps on performing a VM restore with Run Direct

Restoring VM without Run Direct

Steps on performing a VM restore without Run Direct

What should I expect from this document?

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

Who should read this document?

This documentation is intended for backup administrators and IT professionals who are responsible for the VMware VM backup and restore.

2 Understanding Backup Mode

Backup Mode

There are two backup modes available for VM backup:

- **Non-VDDK backup mode**
- **VDDK backup mode**

NOTE

For VDDK backup mode, AhsayOBM must be installed on a supported Windows operating system platform.

The backup mode is chosen by AhsayOBM at the start of a backup, according on the license level of the VMware host, as well as other requirements outlined in [Preparing for Backup and Restore](#).

Non-VDDK Backup Mode

For VM on free version of VMware hosts, backup is performed in non-VDDK mode. Backup in non-VDDK mode produces a backup chain that consists of a full file and a set of delta files:

- During the first backup, full files (e.g. virtual disk file (*.vmdk)) are created in the backup destination.
- During subsequent backup, In-file delta - an AhsayOBM feature is employed, to track only data blocks that have change since the last backup. All changed data blocks are saved as incremental / differential delta files in the backup chain.

During a subsequent backup in non-VDDK mode, VM files are streamed to the [Backup Client Computer](#), for delta generation:

Pros	Free version of ESXi is supported.
Cons	Slower backup speed for subsequent backup compared to VDDK backup, as a result of having the entire VM backed up every time regardless of the actual used size.

VDDK Backup Mode

For VM on VMware host on Enterprise Standard, Enterprise and Enterprise Plus Edition, backup is performed in VDDK mode. Backup in VDDK mode produces a backup chain that consists of a full VDDK file and a set of VDDK incremental files.

- During the first backup, full files (*.F.vddk) are created in the backup destination.
- During subsequent backup, Changed Block Tracking (CBT) - a VMware native feature (<https://kb.vmware.com/kb/1020128>) is employed, to identify disk sectors altered since the last backup. Altered blocks are saved as incremental VDDK file (*.I.vddk) in the backup chain.

During a subsequent backup in VDDK mode, AhsayOBM queries CBT through VADP (vSphere APIs for Data Protection) to request for transmission of all altered blocks since the last backup.

As there is no need to stream the VM files to the [Backup Client Computer](#) for delta generation, backup in VDDK mode will greatly enhance the speed of subsequent backup.

Pros	Faster backup speed for subsequent backups compared to non-VDDK backup, as a result of backing up only the used size of your VM instead of the entire machine to enhance backup efficiency. This also helps with minimizing the storage size requirement and saving storage cost.
Cons	Require paid license, i.e. VMware Essentials License for usage of vSphere API.

Further to the VMware license requirement described above, there are other requirements for VMware VM backup in VDDK backup mode. Refer to the chapter on [Preparing for Backup and Restore](#) for details.

Features Comparison between VDDK and Non-VDDK Modes

	VDDK (CBT)	Non-VDDK
Full Backup	Used data size of guest	Provisioned data size of guest
Incremental / Differential	Generated by VMware Host using CBT	Generated by AhsayOBM on the staging machine using in-file delta
Storage Size	Uses less storage quota	Uses more storage quota
Storage Cost	Lower storage cost	Higher storage cost
Backup Speed	Faster backup speed due to smaller data size	Slower backup speed due to larger data size
Run Direct Support	YES	NO
Restore from VDDK to VMDK format	YES	NO
Granular Restore	YES	YES
AhsayOBM on Windows Platform	YES	YES
AhsayOBM on Non Windows Platform	NO	YES

3 Requirements

Hardware Requirement

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

Software Requirement

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

Refer to the following article for the list of compatible operating systems for Granular Restore: [FAQ: Ahsay Software Compatibility List \(SCL\) for Granular and OpenDirect Restore](#)

Antivirus Exclusion Requirement

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

http://wiki.ahsay.com/doku.php?id=public:8014_suggestion_on_antivirus_exclusions

NOTE

For AhsayOBM version 8.1 or above, the bJW.exe process is automatically added to Windows Defender exclusion list for Windows 10 and 2016, during installation / upgrade via installer or upgrade via AUA.

VMware vCenter / ESXi Server Requirements

For backup of virtual machines on vCenter / ESXi servers, make sure the following requirements are met.

ESXi / vCenter Patch Release

Make sure that the latest supported patch release is installed on the vCenter / ESXi hosts to prevent critical issue, such as corruption to change tracking data in certain situation (<https://kb.vmware.com/kb/2090639>)

License Specification

- Paid License (VMware Essentials License or above): VMware ESXi and vCenter v5, v5.5, v6 , v6.5 and v6.7
- Free License: VMware ESXi v5, v5.5, v6 , v6.5 and v6.7

ESXi Shell Access

- ESXi Shell access must be enabled on the ESXi servers. Refer to the following VMware KB article for instruction: <https://kb.vmware.com/kb/2004746>
- Consult with VMware support representatives if you are unsure on the process.

SSH

SSH must be enabled on the hypervisor (ESXi Server). To enable root SSH login on an ESXi host, please follow the below instructions from VMware.

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=8375637

Root Account

AhsayOBM requires root account access to the ESXi server to perform backup and restore.

Port Requirement

- For environment with firewall, the vCenter, ESXi servers and Backup Client Computer must be able to communicate with each other.
- Ensure that ports 22, 80, 111, 443 and 902 allow outbound communication on the vCenter and ESXi servers. Refer to the link below for details on port usage:

<https://kb.vmware.com/s/article/2012773>

<https://kb.vmware.com/s/article/2106283>

<https://kb.vmware.com/s/article/2039095>

<https://kb.vmware.com/s/article/2131180>

NOTE

Ports 443 and 902 are default ports for VMware.

If these have been changed from the default in your VMware environment, the firewall requirements will change accordingly.

Disk Space Available on Datastore

Sufficient disk space must be allocated on the datastore (e.g. 1.2 x size of the largest virtual machine selected for backup), where the virtual machine(s) for backup are located.

Maximum Virtual Disk Size

- For VMware ESXi version 5.1 and earlier, the maximum size of a virtual disk to be backup cannot exceed 1.98 TB (or less, depending the block size setting of the datastore).
- Details - <http://kb.vmware.com/kb/1003565>

VMware Tools

VMware Tools are used to quiesce VMs prior to backing them up. To create consistent backup for your VMs on Windows platforms, ensure that VMware Tools are installed, and up-to-date on all VMs to be backup.

NOTE

Quiescing is a process that ensures that the disk data is in a state suitable for backups to reduce the possibility of data corruption upon restore. This is especially important for transactional-based applications running on VMs like MS SQL Server.

There are different types of quiescing mechanisms, according to the guest operating systems (e.g. Crash-

consistent, File-system-consistent and Application-consist quiescing).

ESXi/ESX Hosts and Virtual Machine Hardware Versions Compatibility

Refer to the link below for information on the supported and compatible virtual machine hardware versions in VMware vSphere.

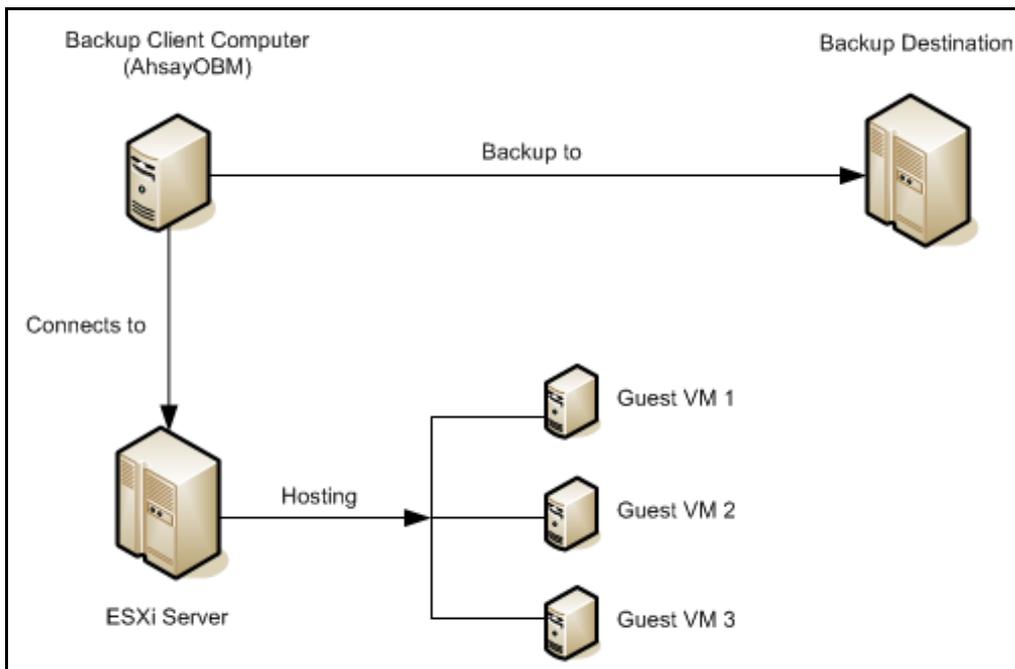
[ESXi/ESX hosts and compatible virtual machine hardware versions list \(2007240\)](#)

Backup Client Computer Requirements

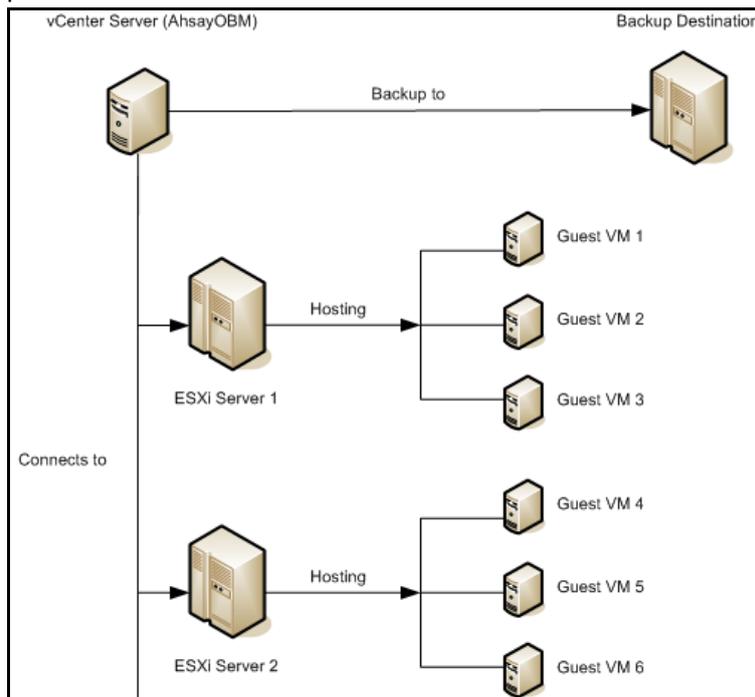
For backup of virtual machines on ESXi server (with no vCenter setup), a separate Backup Client Computer must be prepared for AhsayOBM to install on.

IMPORTANT

AhsayOBM cannot be installed on an ESXi server directly.



For environment with vCenter setup, AhsayOBM is installed on the vCenter computer for best performance.



Ensure that the following requirements are met by the Backup Client Computer or the vCenter computer:

Hardware and Software Requirement

Ensure that the [hardware](#) and [software requirements](#) are met by the Backup Client Computer or the vCenter computer.

Add-on Module Requirement

Make sure that the VMware VM backup add-on module is enabled for your AhsayOBM user account, and that sufficient number of guest / socket is assigned. Contact your backup service provider for more details.

Backup Quota Requirement

Make sure that your AhsayOBM user account has sufficient quota assigned to accommodate the storage for the guest virtual machines. Contact your backup service provider for details.

Port Requirement

- For environment with firewall, the vCenter, ESXi hosts and Backup Client Computer must be able to communicate with each other.
- Make sure that ports 22, 80, 111, 443 and 902 allow outbound communication on the Backup Client Computer. Refer to the link below for details on port usage:

<https://kb.vmware.com/s/article/2012773>

<https://kb.vmware.com/s/article/2106283>

<https://kb.vmware.com/s/article/2039095>

<https://kb.vmware.com/s/article/2131180>

NOTE

Ports 443 and 902 are default ports for VMware.

If these have been changed from the default in your VMware environment, the firewall requirements will change accordingly.

Backup Client Computer on Linux

For Backup Client Computer running on Linux operating system platform, Graphical User Interface (GUI) environment (e.g. GOME or KDE) must be installed.

IMPORTANT

Run Direct restore, VDDK backup mode and Granular Restore is not supported for Backup Client Computer on Linux / Mac OS X platforms.

Disk Space Available on Backup Client Computer (or the vCenter computer)

Sufficient disk space must be allocated on the Backup Client Computer (or the vCenter computer) for the temporary directory configured for the backup set, and the formula for calculation of disk space is like the following:

$(\text{Total File Size} * \text{Delta Ratio}) * \text{number of backup destinations} = \text{Maximum Free Space Required}$

NOTE

The calculation is based on the current guest VM size, and it does not take into account guest VM growth over time. It is recommended for fast growing guest VM the maximum free space required should be reviewed on a regular basis to avoid potential backup problems.

Refer to the link below for details of the maximum free space required for temporary directory.

[FAQ: Tips On How To Setup The Temporary Directory For Your Backup Set \(#5247\)](#)

Windows OS Requirement for VDDK and Non-VDDK Modes Backup

Make sure AhsayOBM is installed on:

- 64-bit Windows OS if you will back up VM data from VMware vCenter/ESXi 6.5 or above in VDDK mode.
- Either 32-bit or 64-bit Windows OS if you will back up VM data from VMware vCenter/ESXi 6.5 or above in Non-VDDK mode (Free VMware version).

Run Direct Requirements

Run Direct is a feature that helps reduce disruption and downtime of your production VMs.

For more details on Run Direct, refer to the chapter on [Instant VM Restore with Run Direct](#).

To utilize the Run Direct feature, ensure that the following requirements are met:

VDDK Backup Mode

Run Direct restore is only supported for virtual machine that is backed up in VDDK mode. Make sure that the [VDDK backup mode requirements](#) are met.

Backup Destination Requirement

- ▶ When a Run Direct restore is performed, the backup destination containing the guest VM files is mounted on the VMware host as NFS datastore.
- ▶ Ensure that the following requirements are met by the backup destination of the VMware VM backup set:
 - Destination must be accessible to the VMware host.
 - Destination must have sufficient disk space available for the Run Direct restore. There should be 1.5 x total provisioned size of all VMs selected for backup.
 - For Run Direct restore of 1 VM with provisioned size of 100GB, there should be 150GB (e.g. 1.5 x 100GB) of free space available in the Destination.

▶ No Compression and Encryption

Data backed up to a Run Direct enabled destination is not compressed or encrypted to optimize restore performance as Run Direct will make the VM restored by running the data directly from the backup files in the backup destination.

▶ Operation System of the Backup Client Computer

- Run Direct restore is only supported by AhsayOBM installation on Windows.
- To utilize the Run Direct feature, make sure that AhsayOBM is installed on a supported Windows platform.

▶ Restore to Alternate Location

- When performing a Run Direct restore to **Alternate Location**, only one VM can be selected per restore session.

Restore virtual machines to

Original location

Alternate location

Run Direct

 In alternate restoration, you can only select one virtual machine at a time. Do you want to modify the selected virtual machines?

- Consider to create separate VMware VM backup set for each VM that you intend to perform Run Direct restore (e.g. VMs that you may restore to alternate location).

- **Dedicated NFS Service**

A dedicated AhsayOBM NFS Windows service is introduced to allow Run Direct session to continue even if the AhsayOBM user interface is closed.

By default, the AhsayOBM NFS service is started as Local System, which does not have sufficient permission to access any network resources (e.g. the AhsayOBM NFS service does not have sufficient permission to access the VM backup files on network drive).

Make sure that the **Log on** setting of the **Ahsay Online Backup Manager NFS Service** is configured with an account with sufficient permission to access the network backup destination where the backed up VM data are stored.

1. Under Control Panel, open Administrative Tools then Services.
2. Right click on Ahsay Online Backup Manager NFS Service, select the Log on tab.
3. Select the **This Account** option.
4. Enter the login credentials of an account with sufficient permission.
5. Restart the service afterward.

VDDK Backup Mode Requirements

AhsayOBM supports VDDK backup mode (Virtual Disk Development Kit) for ESX/ESXi and vCenter setup. The backup speed is enhanced because the generation of the delta file of the VM are performed directly by the ESX/ESXi or vCenter itself. With VDDK backup mode, the following are supported:

- Backup / restore of the resource pool and 'roles' settings, and support of restoration to another name or alternate location on the ESX/ESXi platform.
- VM hardware version upgrade, change tracking option and change tracking data option when a new backup set is created.
- Add or remove VM hard disk without uploading the existing hard disk again on the vCenter backup.

For VDDK backup mode, AhsayOBM must be installed on a supported Windows operating system platform.

License Requirement

- The VMware vSphere Storage APIs, which are essential for VDDK backup mode, are included with the VMware vSphere Enterprise Standard, Enterprise and Enterprise Plus Edition.
- Ensure that the license requirement is met.

NOTE

For VM on free version of ESXi without a Run Direct backup destination, backup will be performed in non-VDDK mode.

For VM on free version of ESXi with a Run Direct backup destination, the following error message would be returned during a backup:

"Skip backing up Virtual Machine "name". Reason = "Run Direct is only support to VDDK backup"

mode”.

Changed Block Tracking (CBT) on VMs

CBT must be enabled for the VM to be backed up in VDDK mode. Make sure that the following requirements are met:

- The VM must be hardware version 7 or later.
- The VM must have zero (0) snapshots when CBT is enabled.
- The virtual disk must be located on a VMFS volume backed by SAN, iSCSI, local disk, or a NFS volume.

NOTE

For virtual disk on VMFS, the initial backup (e.g. full file backup) will be of size similar to used size; while for virtual disk on NFS, the initial backup will be of the provisioned size.

- RDM (Raw Device Mapping) in physical compatibility mode is not supported.
- The virtual disk must not be in Independent Mode (Persistent or Nonpersistent).

NOTE

Once the backup job executed on a VM with change block tracking option enabled by the VDDK, please do not turn off this option in the VM for consequent backup jobs. If you need to disable this option, you are suggested to create a new backup set with this option disabled.

VMware Snapshot

VDDK backup mode does not support backup of [virtual machine snapshot](#).

For backup of individual virtual disk, 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.

Virtual Machine State

VDDK backup mode does not support backup of virtual machine state (e.g. power on state / suspend state).

File Name Requirement

If the file name of the virtual machine contains the following special characters, https access to the virtual machine's files will fail:

` ^ ~ = ; ! / ([] { } @ \$ \ & # % +

This is due to the percent-encoding specified in the URL standard is not supported for ESXi based HTTP(S) file access. To resolve the issue, please rename the corresponding file to avoid special characters. For instructions on renaming a virtual machine, please refer to the following knowledge base article from VMware: <https://kb.vmware.com/s/article/2031763>

Non-VDDK Backup Mode Requirements

For VM that cannot be backed up in VDDK mode, non-VDDK backup mode will be used instead.

- Independent Disk (Persistent or Non-persistent)
- Independent disk can only be backed up if the VM is shutdown during a backup. If the VM is started up during the backup, all independent disks selected for backup cannot be backed up.

4 Best Practices and Recommendations

Please consider the following recommendations:

- Use the latest version of AhsayOBM

Install the latest version of AhsayOBM on the staging machine or Backup Client Computer for backup of VM hosted on a VMware ESX/ESXi server, or on the vCenter server.

Always stay up-to-date when newer version of AhsayOBM is released. To get our latest product and company news through email, please subscribe to our newsletter:

<https://www.ahsay.com/jsp/en/contact/ahsay-contact.jsp>

- Install AhsayOBM on a physical staging machine

For best backup and restore performance, it is highly recommended that AhsayOBM is installed on a server grade staging machine or backup client computer with sufficient memory and processing power. As guest VM can be very large, during backups and restore this may involve the compression & encryption of large amounts of data, which can be very resource intensive.

- VMware Tools

Make sure the latest version of VMware Tools is installed on each guest VM selected for backup. VMware Tools is used by AhsayOBM to quiesce the guest VMs prior to backing them up to create consistent backup for your VMs

Quiescing is a process that ensures that the disk data is in a state suitable for backups to reduce the possibility of data corruption upon restore. This is especially important for transaction-based applications running on VMs like MS SQL Server, MS Exchange etc. There are different types of quiescing mechanisms, according to the guest operating systems (e.g. Crash-consistent, File-system-consistent and Application-consistent quiescing).

- Do not use a guest VM as a staging machine

Although installing AhsayOBM on a guest VM as a staging machine is possible, the backup and restore will work as on a physical staging machine. This setup is actually inefficient and can lead to possible performance bottlenecks on the VMware host server, as in a VMware host the virtualization layer separates guest VM OS layer and the VMware host physical hardware layer.

As the guest VM operating system does not have direct access to physical hardware where the data resides, a backup agent installed inside the guest VM must go through the virtualization layer to access the guest virtual machine data.

- Use the VDDK backup mode / CBT feature

The CBT (Change Block Tracking) feature, which is required for backup in VDDK mode, is supported by VM host with VMware Essentials License (or other paid licenses). The CBT feature, which is utilized for tracking changes of data blocks since the last backup can be done quickly and directly on the VM host. Therefore, the performance of incremental backups is much faster with VDDK backup mode.

Another advantage of VDDK mode is the amount of data backed up is relatively smaller. The used data size of the guest VM is backed up instead of the provisioned size, so the storage cost of these backups will be less.

- The temporary directory of a VMware VM backup set is set to a local volume, and not to a network volume (e.g. to improve I/O performance).

However, the temporary directory should not be set to the system volume (e.g. where the operating system is installed).

Refer to the following article for details on setting up the temporary directory:

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

- Plan your backup schedules carefully to minimize any performance impact on the VMware host.

To avoid concentrated disk I/O on the VMware host datastores which will have a negative performance impact on the guest VMs residing on these datastores, you should schedule your backups to limit the number of concurrent VM backups on a host and shared datastores. Hosts typically share the same datastores in virtual environments, and bottlenecks caused by too many simultaneous VM backups on a single datastore will affect all hosts that have VMs running on that datastore.

- Backup the guest VMs to more than one destination

To provide maximum data protection and recovery flexibility you should consider to store your guest VM backups in multiple backup destinations, ideally both onsite and offsite locations. Onsite locations on local or network drives will enable very quick recovery even for large guest VMs. While offsite locations will ensure that if there is a site outage, the guest can be restored from another location.

- Consider to increase the Java memory allocation setting for AhsayOBM (Java heap space) if you are using non-VDDK backup mode.

If you are using non-VDDK mode and or Granular restore, it is recommended to increase the Java heap size space to at least 2GB or above for optimal performance.

Refer to the following KB article for further instruction:

http://wiki.ahsay.com/doku.php?id=public:8011_faq:how_to_modify_the_java_heap_size_of_ahsayobc

- It is highly recommended to backup the whole VM instead of individual disk for backup of virtual machine with snapshot.
- Consider to perform routine recovery test to ensure your backup is setup and performed properly.
- Consider to disable the memory snapshot or quiesce guest options when taking snapshot for VMware VM backup, to shorten the time required for the process.
 - Snapshot the virtual machine's memory
 - Quiesce guest file system (Needs VMware Tools installed)

5 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.

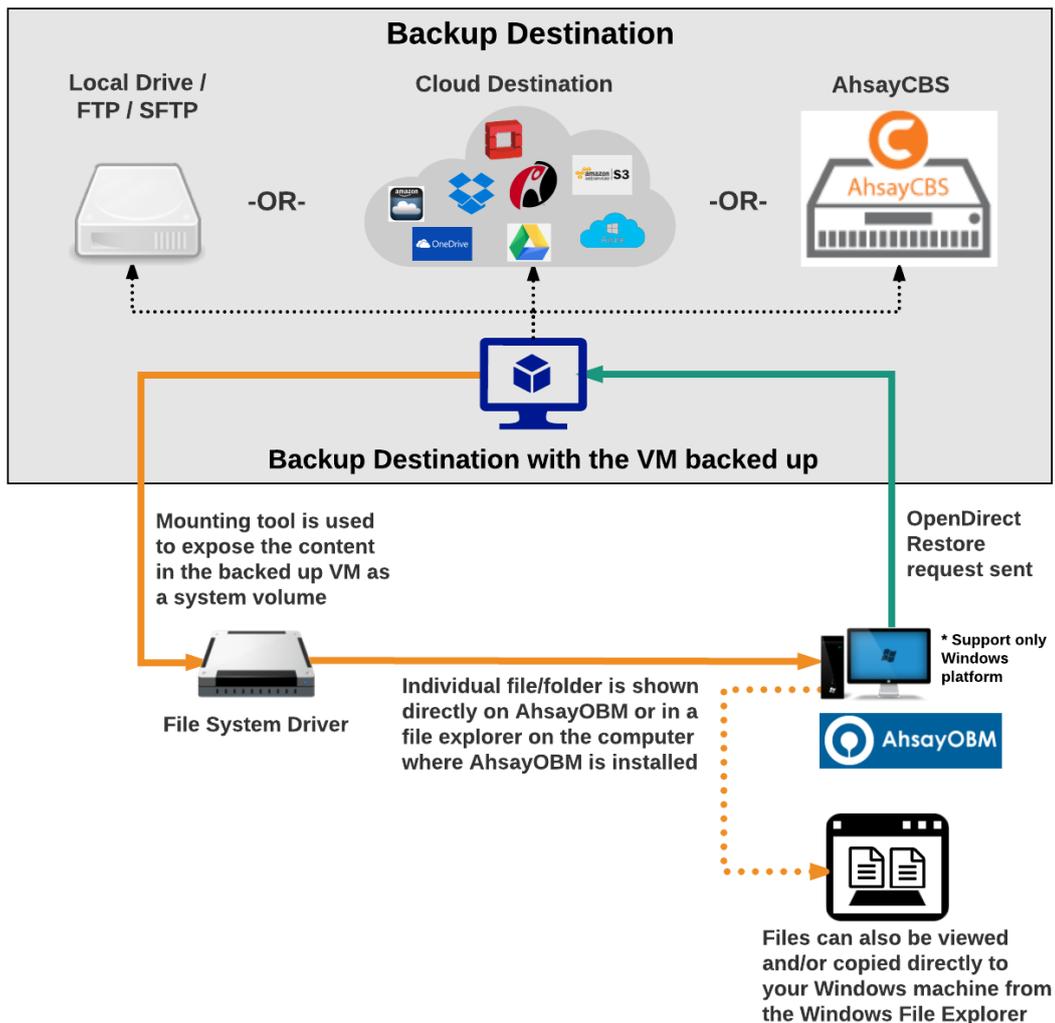
Granular restore is one of the available restore options for VMware ESXi/vCenter backup sets from AhsayOBM v8.1.0.0 or above. AhsayOBM makes use of granular restore technology to enable a file level restore from a virtual disk file (VDDK) of guest VM backup possible. It is particularly useful if you only need to restore individual file(s) from a guest VM which would normally take a long time to restore and then startup before you can gain access to the files on the virtual disks. Granular restore gives you a fast and convenient way to recover individual files on 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?



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 64 bit Windows machine you are performing the restore.	
Pros	
Restore of Entire Guest VM Not Required	Compared to a traditional restore where you have to restore the entire guest VM first, before you can access any individual files/folders, granular restore allows you to view and download individual files, without having to restore the entire guest VM first.

Ability to Restore Selected Files	In some cases, you may only need to restore a few individual file(s) from the guest VM, therefore, granular restore gives you a fast, convenient, and flexible tool to restore selected file(s) from a guest VM quickly.
Only One Backup Set Required	<p>With traditional restore methods, if you wish to restore individual file(s) from a guest VM, you will have to create two different backup sets; a VMware guest VM backup set and a separate file backup set for the file(s) you wish to restore. You will require an additional AhsayOBM installation on the guest VM environment, with Granular Restore feature, only one backup set is required.</p> <ul style="list-style-type: none"> ➤ Fewer CAL (Client Access License) required - you will only need one AhsayOBM CAL to perform guest VM, Run Direct, and Granular restore. ➤ Less storage space required - as you only need to provision storage for one backup set. ➤ Less backup time required - As only one backup job needs to run. ➤ Less time spent on administration - As there are fewer backup sets to maintain.
Cons	
No Encryption and Compression	To ensure optimal restore performance, the backup of the guest VM will NOT be encrypted and compressed, therefore, you may have to take this factor in consideration when using this restore method.

Traditional Restore	
Introduction	
The traditional restore method for guest VMs, restores the entire backup files to either the original VM location or another standby location. The files or data on the guest VM can only be accessed once the guest VM has been fully recovered and booted up.	
Pros	
Backup with Compression and Encryption	Guest VM is encrypted and compressed, therefore is in smaller file size, and encrypted before being uploaded to the backup destination.
Cons	
Slower Recovery	As the entire guest VM has to be restored before you can access any of its file(s) or data, the restore time could be long if the guest VM size is large.
Two Backup Sets and CALs Required	If you only wish to restore individual files from VM, two separate backup sets are required, one for the VM image and the other for the individual files, and therefore two CAL (client access licenses) are required.

Requirements

Supported Backup Modules

Granular restore is supported on VMware backup sets created and backed up using AhsayOBM v8.1.0.0 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 for VMware ESXi/VCenter. AhsayOBM must be installed on the following Windows Operating Systems:

Windows 2008 R2 SP1 or above	Windows 2012	Windows 2012 R2
Windows 2016	Windows 7 SP1 or above	Windows 8
Windows 8.1	Windows 10	

Temporary Directory Requirement

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 VDDK 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

The Windows drive letters A, B, and C are not used by granular restore.

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 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 restore related and therefore they will be checked by AhsayOBM only when granular restore is performed. Absence of these elements will not affect the backup job but would cause the 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>
- **For Windows 7 and Windows Server 2008 R2 only**
Microsoft Security Advisory 3033929
<https://docs.microsoft.com/en-us/securityupdates/securityadvisories/2015/3033929>

Permissions

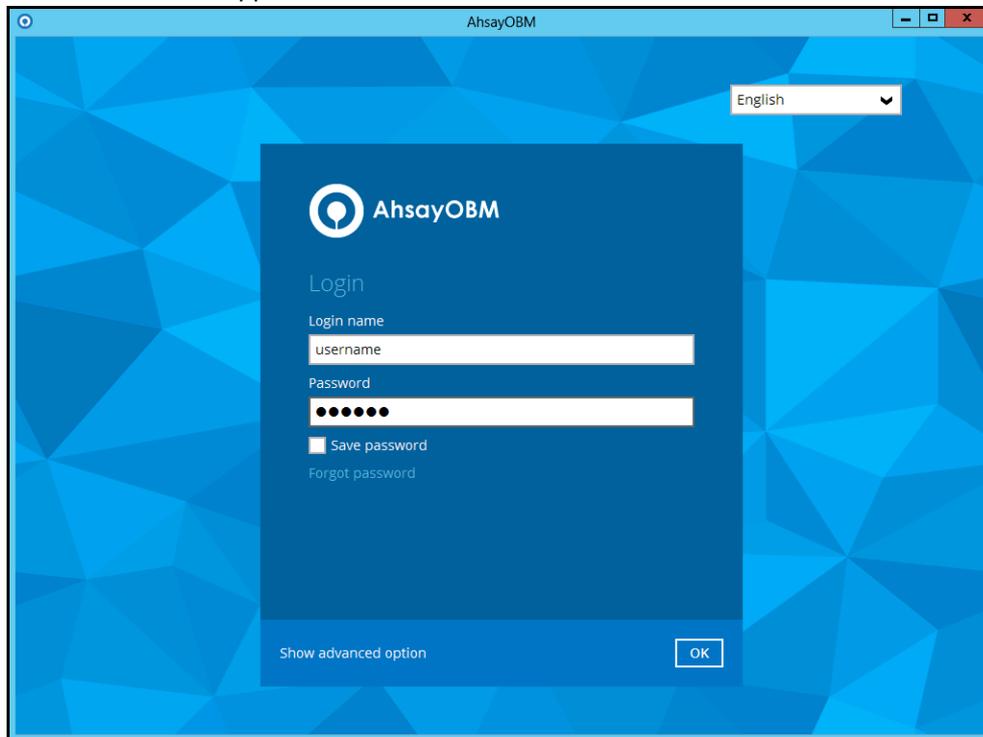
- The Windows login account used for installation and operation of the AhsayOBM client machine requires Administrator privileges.
- For Granular Restore, Windows User Account Control (UAC) must be disabled.

6 Starting AhsayOBM

Login to AhsayOBM

1. Login to the AhsayOBM application user interface.

For Backup Client Computer on Windows / Mac OS X, double click the AhsayOBM desktop icon to launch the application.



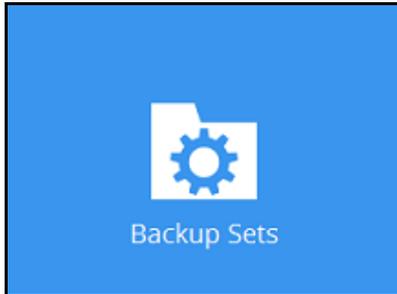
For Backup Client Computer on Linux, enter the following command to launch the application user interface:

```
# sh /usr/local/obm/bin/RunOBC.sh &
```

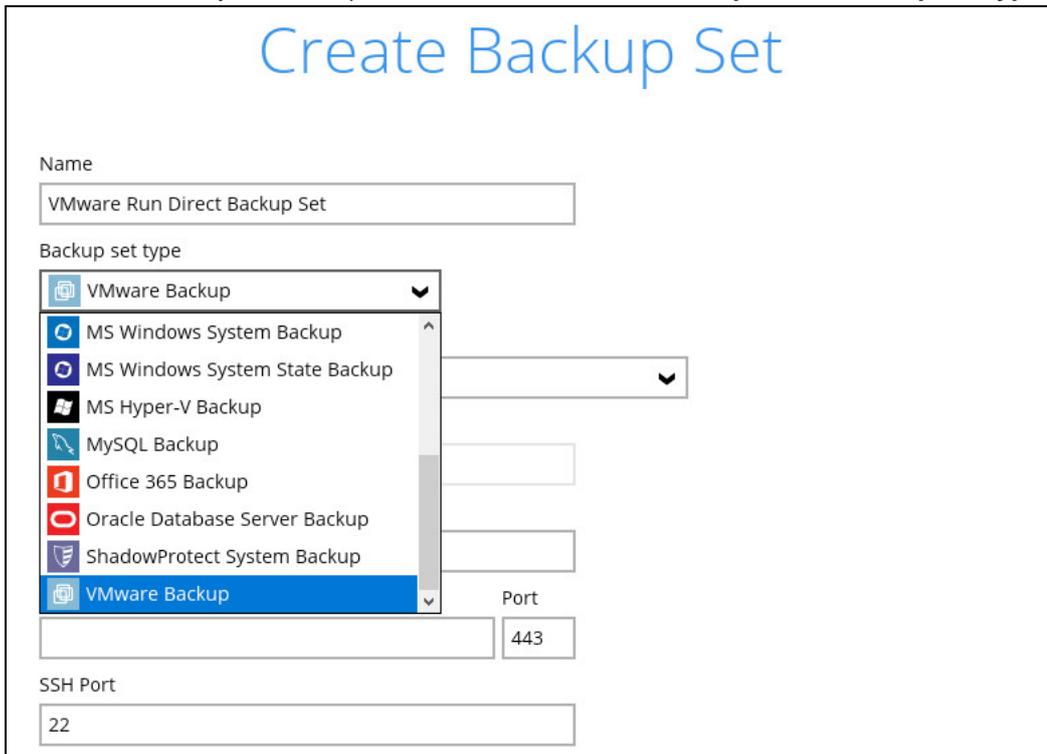
2. Enter the **Login name** and **Password** of your AhsayOBM account.
3. Click **OK** afterward to login to AhsayOBM.

7 Creating a VMware VM Backup Set

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



2. Create a VMware VM backup set by clicking the “+” icon next to **Add new backup set**.
3. Enter a **Name** for your backup set and select **VMware Backup** as the **Backup set type**.



Create Backup Set

Name
VMware Run Direct Backup Set

Backup set type

- VMware Backup
- MS Windows System Backup
- MS Windows System State Backup
- MS Hyper-V Backup
- MySQL Backup
- Office 365 Backup
- Oracle Database Server Backup
- ShadowProtect System Backup
- VMware Backup

Port
443

SSH Port
22

4. Select the **Version** of the corresponding host:

Create Backup Set

Name

Backup set type

Version

VMware ESXi 5 / 5.5 / 6 / 6.5 / 6.7

VMware ESXi 5 / 5.5 / 6 / 6.5 / 6.7

VMware Workstation 10 / 11 / VMware Workstation Pro 12 / 14 / 15

VMware Player 6 / 7 / VMware Workstation Player 12 / 14 / 15

VMware vCenter 5 / 5.5 / 6 / 6.5 / 6.7

Host Port

SSH Port

- Select **VMware ESXi 5 / 5.5 / 6 / 6.5 / 6.7** for a VMware ESXi backup set
- OR-**
- Select **VMware vCenter 5 / 5.5 / 6 / 6.5 / 6.7** for a VMware vCenter backup set

NOTE: Refer to the following article for the list of compatible VMware platforms:
http://wiki.ahsay.com/doku.php?id=public:8001_faq:ahsay_software_compatibility_list_scl_for_version_8.1_or_above

5. Enter the VMware host and access information. For a VMware ESXi backup set, enter the **Password** of the root account, **Host**, **Port** and **SSH Port** information of the ESXi host.

Create Backup Set

Name

Backup set type

Version

Username

Password

Host Port

SSH Port

For a VMware vCenter backup set, enter the **Username** and **Password** of the administrator account, **Host**, and **Port** information of the vCenter server.

Create Backup Set

Name

Backup set type

Version

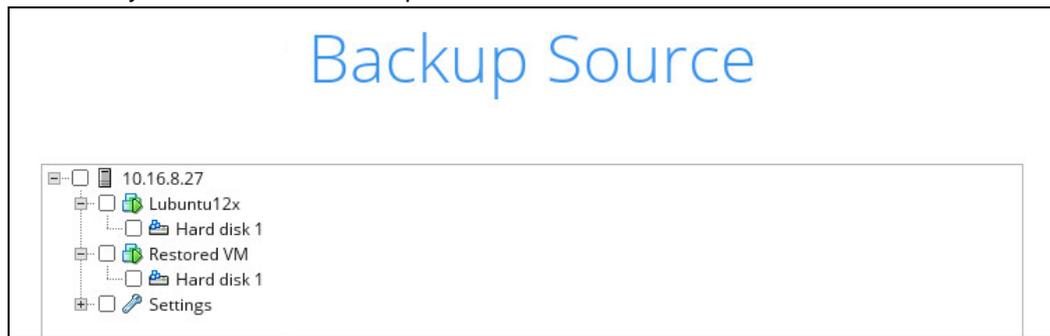
Username

Password

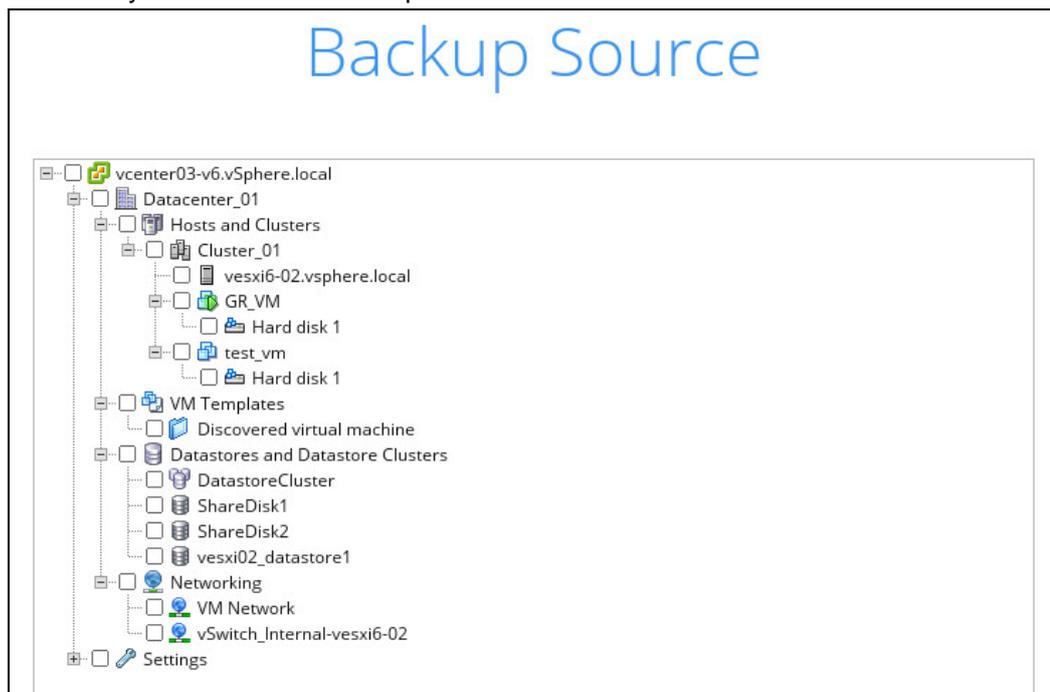
Host Port

Click **Next** to proceed when you have finished entering all necessary information.

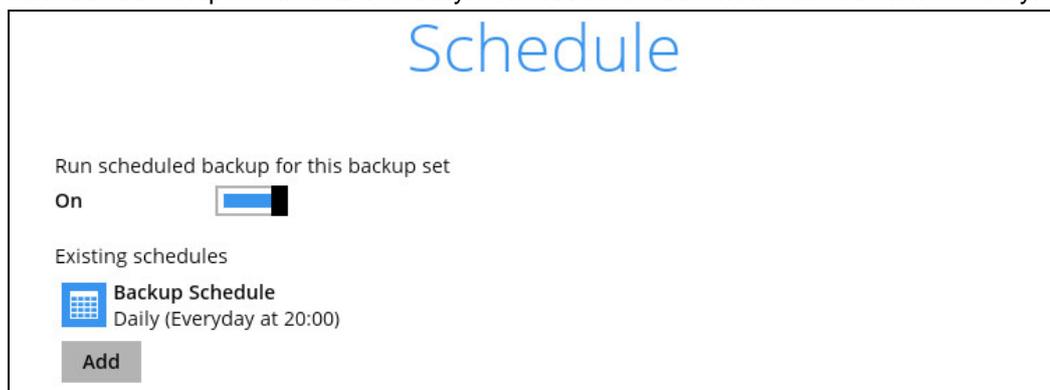
6. For VMware ESXi backup set, select the settings, virtual machines or individual virtual disks that you would like to backup.



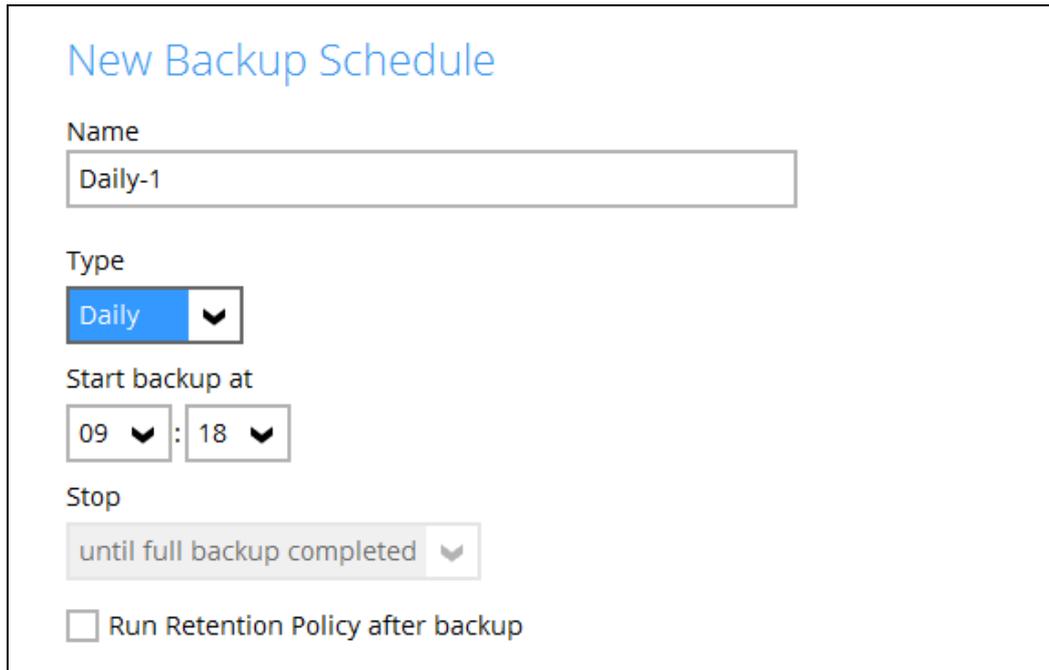
- For VMware vCenter backup set, select the settings, virtual machines or individual virtual disks that you would like to backup.



7. In the Schedule menu, configure a backup schedule for backup job to run automatically at your specified time interval. By default, this feature is turned on with a predefined scheduled backup to run at 20:00 daily. Click **Add** to add a new schedule if necessary.



If you will configure a scheduled backup, define the backup schedule details in the New Backup Schedule section as shown below. Click **OK** when you have finished configuring the backup schedule.



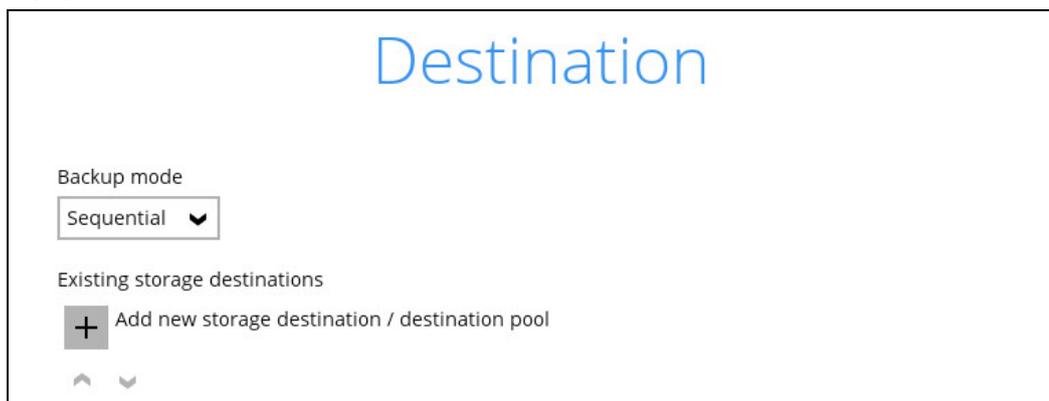
The screenshot shows a form titled "New Backup Schedule". It contains the following fields and options:

- Name:** A text input field containing "Daily-1".
- Type:** A dropdown menu with "Daily" selected.
- Start backup at:** Two time selection fields showing "09" and "18".
- Stop:** A dropdown menu with "until full backup completed" selected.
- Run Retention Policy after backup

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

Note: For details about the options from the dropdown menus, please refer to [Configure Backup Schedule for Automated Backup](#).

8. In the Destination menu, select the appropriate option from the **Backup mode** dropdown menu.



The screenshot shows a form titled "Destination". It contains the following fields and options:

- Backup mode:** A dropdown menu with "Sequential" selected.
- Existing storage destinations:** A section with a "+" icon and the text "Add new storage destination / destination pool".
- Up and down arrow icons below the "Add new storage destination" button.

Select the appropriate option from the **Backup mode** dropdown menu.

- **Sequential** (default value) – run backup jobs to each backup destination one by one
- **Concurrent** – run backup jobs to all backup destinations at the same time

To select a backup destination for the backup data storage, click the "+" icon next to **Add new storage destination / destination pool**.

9. In the New Storage Destination / Destination Pool menu, select the **Destination storage**.

New Storage Destination / Destination Pool

Name

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

Destination storage

Run Direct

1. To utilize the Run Direct feature for your VMs recovery, enable the **Run Direct** option. The Run Direct option is only available for single storage destination, and is enabled by default.
2. Further to the above settings, there are also other requirements for the Run Direct feature, refer to the chapter on [Run Direct Requirement](#) for more details.

If you have chosen the Local/Mapped Drive/Removable Drive option, you can change the Name then click **Change** to browse to a directory path where backup data will be stored. The path must be accessible to the ESXi host.

New Storage Destination / Destination Pool

Name

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

Destination storage

Local path

Click **OK** to proceed when you are done with the settings.

NOTE

For more details on Backup Destination, refer to the following article for details:
http://wiki.ahsay.com/doku.php?id=public:8002_faq:faq_on_backup_destination

10. You can add multiple storage destination if you wish. The backup data will be uploaded to all the destinations you have selected in this menu in the order you added them. Press the   icon to alter the order. Click **Next** to proceed when you are done with the selection.

Destination

Backup mode
Sequential ▼

Existing storage destinations

-  **AhsayCBS**
Host: 10.90.10.12:443
-  **Local-1**
C:\rdbackup

Add

NOTE

Multiple backup destinations can be configured for a single backup set (e.g. one destination with Run Direct enabled, and another with Run Direct disabled).

11. If you wish to enable the granular restore feature, make sure you turn on the **Granular Restore** switch in this menu. Refer to [Granular Restore](#) section for further details on this feature.

Click **Next** to proceed.

Granular Restore

Granular Restore
On

Support of granular restoration for individual files inside virtual machine.

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

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

Notes

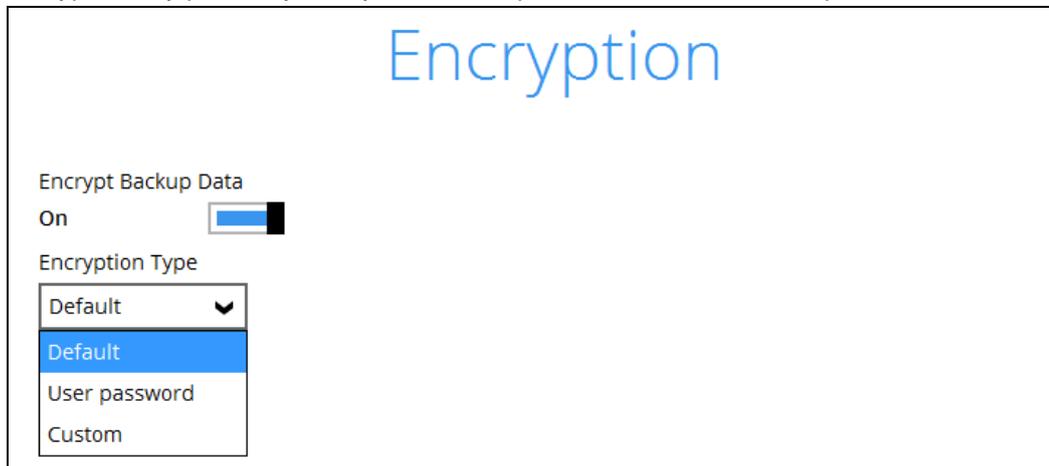
Once the Granular Restore feature is enabled and the backup set is saved, it is NOT possible to disable it afterwards, and vice versa. If you wish to change the Granular Restore settings, a new backup set will have to be created.

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.

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

12. **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 14.

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



Encryption

Encrypt Backup Data
On

Encryption Type
Default ▼
Default
User password
Custom

NOTE

For best practice on managing your encryption key, refer to the following article.
http://wiki.ahsay.com/doku.php?id=public:8015_faq:best_practices_for_managing_encryption_key

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

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

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

The screenshot shows the 'Encryption' settings window. At the top, the word 'Encryption' is displayed in a large blue font. Below it, there are several settings: 'Encrypt Backup Data' is set to 'On' with a blue toggle switch; 'Encryption Type' is set to 'Custom' in a dropdown menu; 'Algorithm' is set to 'AES' in a dropdown menu; 'Encryption key' and 'Re-enter encryption key' are both masked with '*****' in text input fields; 'Method' has 'CBC' selected with a radio button, while 'ECB' is unselected; 'Key length' has '256-bit' selected with a radio button, while '128-bit' is unselected.

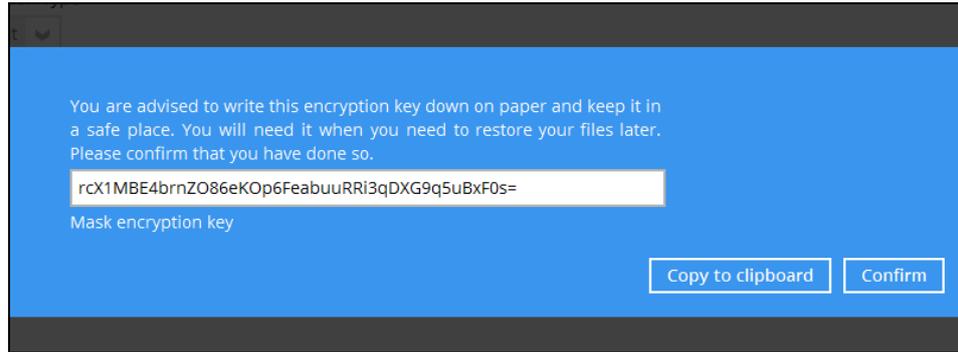
Click **Next** when you are done setting.

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

The screenshot shows a confirmation pop-up window titled 'Encryption'. The background is dark grey. The text inside reads: 'You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.' Below this text is a text input field containing six black dots. Underneath the field is the text 'Unmask encryption key'. At the bottom right, there are two buttons: 'Copy to clipboard' and 'Confirm'.

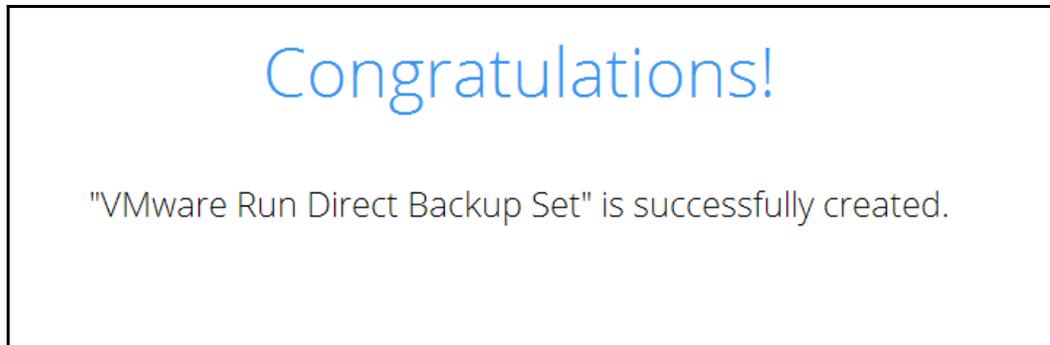
The pop-up window has the following three options to choose from:

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



- **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.

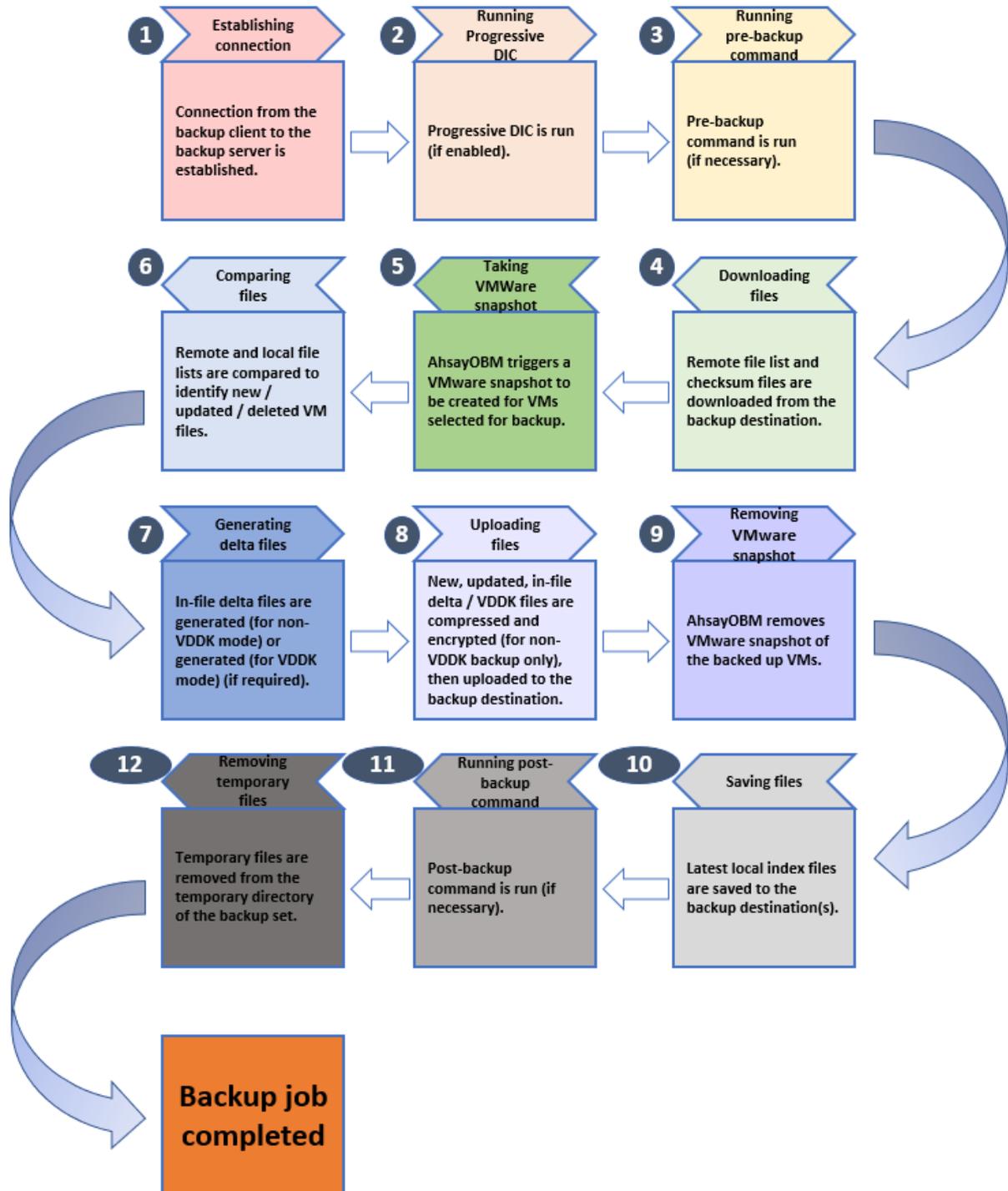
14. The following screen is displayed when the new VMware VM backup set is created successfully.



15. Click the **Backup now** button if you wish to run a backup for this backup set now.

8 Overview on Backup Process

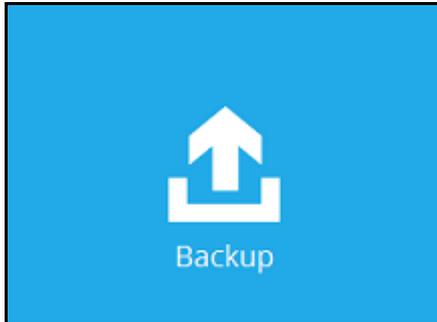
The following steps are performed during a VMware VM backup job.



9 Running a Backup

Start a Manual Backup

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



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



3. If you would like to modify the In-File Delta type, Destinations and Retention Policy Settings, click **Show advanced option**.
4. When advanced options are shown, it is recommended that you tick the checkbox next to **Run Retention Policy after backup** in the Retention Policy section at the bottom. This will help you save hard disk quota in the long run. In the In-File Delta type section, the following three options are available:



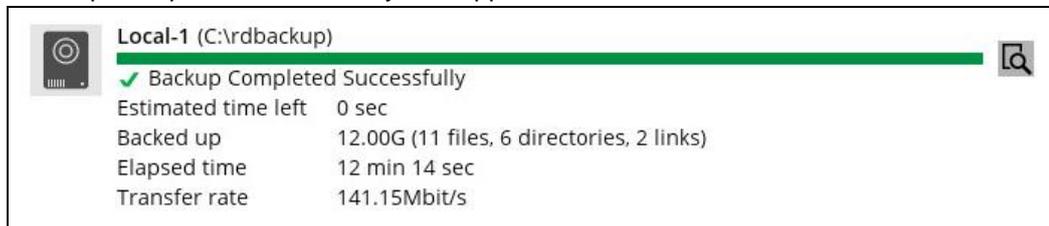
- **Full** – A full backup captures all the data that you want to protect. When you run a backup job for the first time, AhsayOBM will run a full backup regardless of the in-file delta setting.
- **Differential** – A differential backup captures only the changes made as compared with the last uploaded full file only (i.e. changes since the last full backup, not since the last differential backup).
- **Incremental** – An incremental backup captures only the changes made as compared with the last uploaded full or delta file (i.e. changes since the last incremental backup).

Click **Backup** to start the backup.

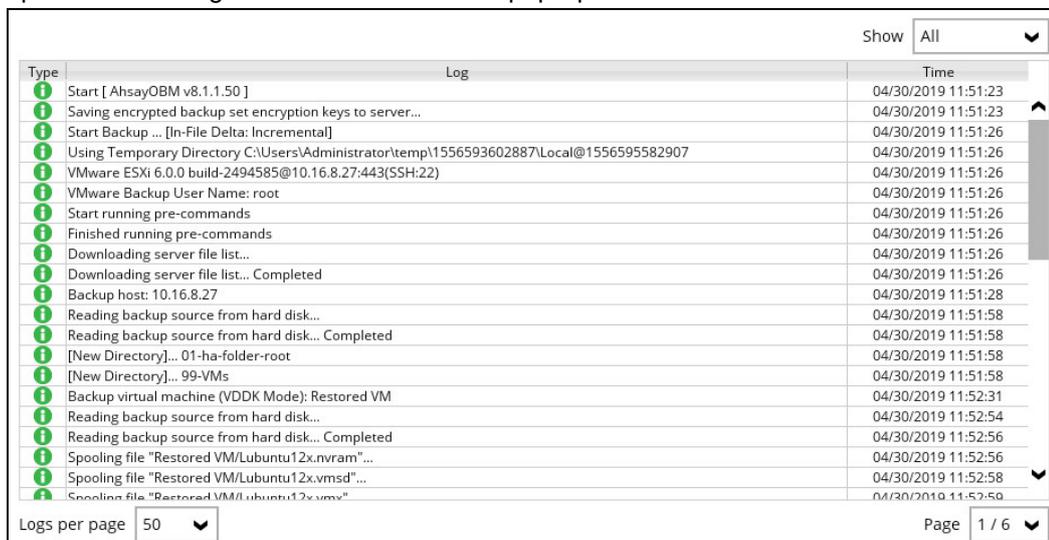
5. Click Backup to start the backup job. The status will be shown.



6. When the backup is completed, the progress bar will be green in color and the message “Backup Completed Successfully” will appear.

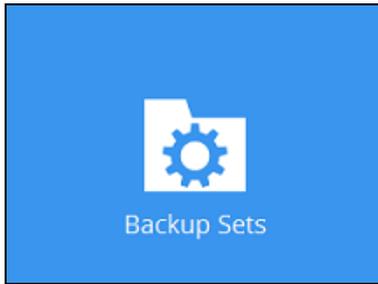


7. You can click the **View** icon on the right hand side to check the log. A window will pop up to show the log. Click **Close** to exit the pop-up window.

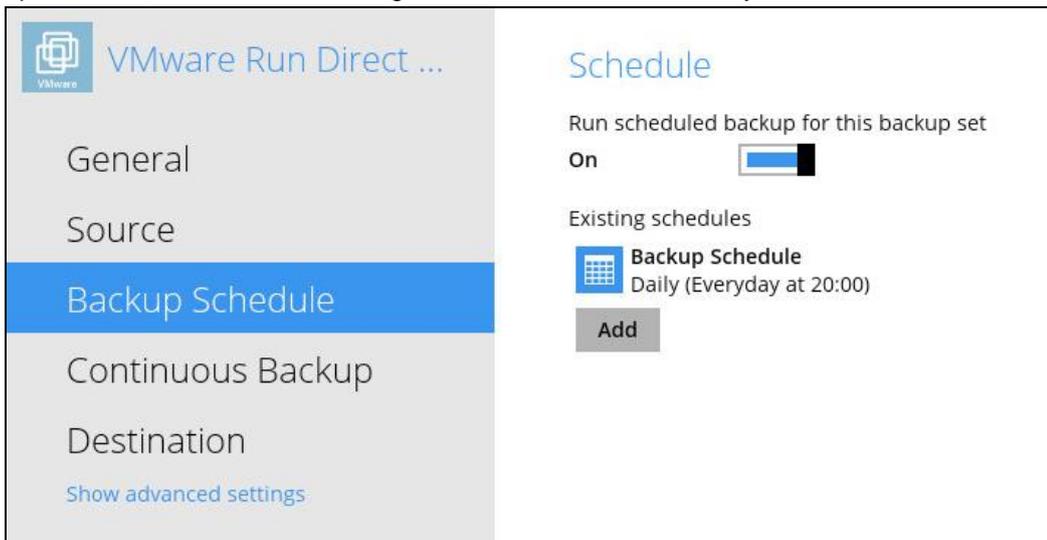


Configure Backup Schedule for Automated Backup

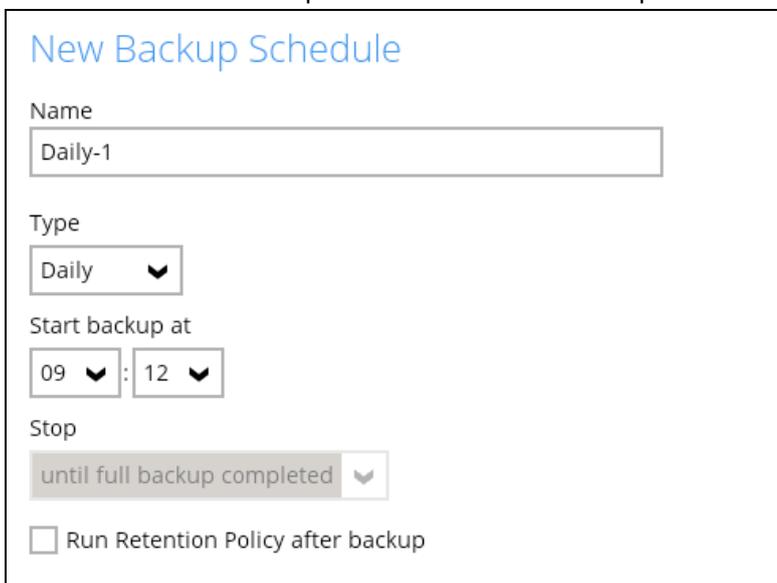
1. Click the Backup Sets icon on the AhsayOBM main interface.



2. All backup sets will be listed. Select the backup set that you would like to create a backup schedule for.
3. Go to the **Backup Schedule** tab. If the **Run scheduled backup for this backup set** option is off, switch it **On**. Existing schedules will be listed if any.



4. Click **Add** to add a backup schedule. The New Backup Schedule window will appear.

The "New Backup Schedule" window contains the following fields:

- Name:** A text input field containing "Daily-1".
- Type:** A dropdown menu with "Daily" selected.
- Start backup at:** Two dropdown menus for time selection, showing "09" and "12".
- Stop:** A dropdown menu with "until full backup completed" selected.
- Run Retention Policy after backup

5. In the New Backup Schedule window, you can configure your backup schedule settings. To save hard disk quota in the long run, it is recommended that you tick the checkbox next to **Run Retention Policy after backup** at the bottom. The rest of the setting options will vary by which option you choose from the **Type** dropdown menu:

⊙ **Daily** – when to start the backup job

New Backup Schedule

Name
Dayend

Type
Daily

Start backup at
18 : 00

Stop
until full backup completed

Run Retention Policy after backup

⊙ **Weekly** – which day of the week and what time that day to start the backup job

New Backup Schedule

Name
Weekend

Type
Weekly

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

Start backup at
23 : 00

Stop
until full backup completed

Run Retention Policy after backup

⊙ **Monthly** – which day of the month and what time that day to start the backup job

New Backup Schedule

Name
Monthly Closing

Type
Monthly

Backup on the following day every month
 Day Last
 First Sunday

Start backup at
23 : 00 on the selected days

Stop
until full backup completed

Run Retention Policy after backup

- **Custom** – which particular date to start a one-off backup job

New Backup Schedule

Name

Type

Backup on the following day once

Start backup at
 :

Stop

Run Retention Policy after backup

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

Schedule

Run scheduled backup for this backup set

On

Existing schedules

- Dayend**
Daily (Everyday at 18:00)
- Weekend**
Weekly - Saturday (Every week at 23:00)
- Monthly Closing**
Monthly - The Last Day (Every month at 23:00)
- New Years Eve**
Custom (31/12/2019 at 23:59)

6. Click **Save** to confirm your settings when you are done with the settings.

10 Restore Methods

There are four methods to restore your backed up virtual machine.

Method 1 - Restoring a Virtual Machine with Run Direct

Introduction

This restore method can power up a VM instantly by running it directly from the backup files in the backup destination.

Pros

- Fast Recovery
- Minimize VM server down time so as minimizing impact on your business

Cons

- Changes made to the running VM during Run Direct power up process will be lost when the VM is powered down if not committed to the VM by completing a successful migration.

Method 2 - Restoring a Virtual Machine without Run Direct

Introduction

This is the conventional restore method where VM data is restored from the backup destination to the original VM host, another datastore of the original VMware host or another VMware host.

Pros

- Complete VM restore can be done in one take; no data migration needed afterwards

Cons

- Recovery time could be long if the VM size is large
- Long VM server down time may cause greater impact on your business

Method 3 - Restoring a Virtual Machine in Raw File (VMDK Format)

Introduction

If you wish to restore the VM to another VMware host (ESXi server) directly without using AhsayOBM

Pros

- You can manually restore the VM to another VMware host (ESXi server) off-site without having to use AhsayOBM as the restore channel

Cons

- Restore procedures are relatively complicated

Method 4 – [Granular Restore](#)

Introduction

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 power up before you can gain access to the files on the virtual disks. Granular restore gives you a fast and convenient way to recover individual files on a guest VM.

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

Pros

- File level restore and access to files, without having boot up or to restore the entire Guest VM.
- Pin-point file restore to save time and promote efficiency
- Only one backup set required as opposed to the traditional restore method where two backup sets are required for file level restore

Cons

- No encryption and compression for backup set

11 Method 1 - Restoring a Virtual Machine with Run Direct

Login to AhsayOBM

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

Running Direct Restore via AhsayOBM

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



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



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

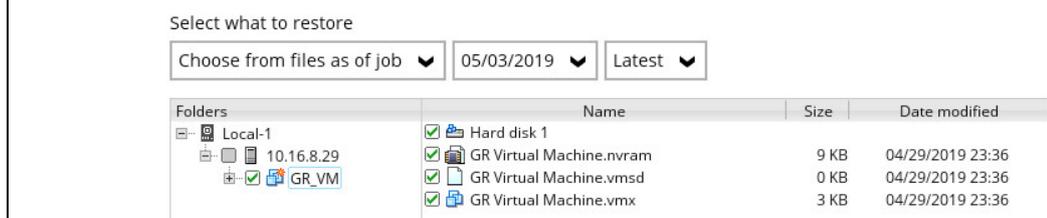


4. Select the virtual machine that you would like to restore.

Important

When performing a Run Direct restore to **Alternate Location**, only one VM can be selected per restore session.

Select Your Virtual Machines To Be Res

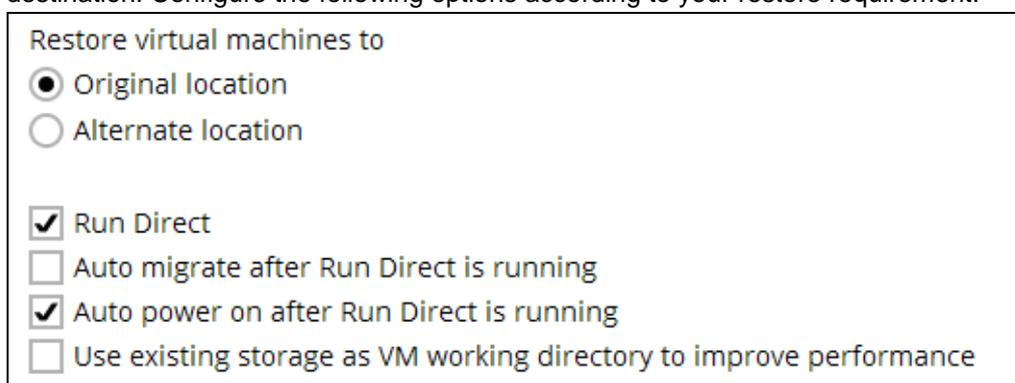


If you wish to restore the VM to another VMware host (ESXi server), you can restore the VM in raw file format, where the .vmdk disk format file will be included, by clicking the **Restore raw file** button at the bottom left corner. Refer to the steps in [Appendix Restoring VM in VMDK format](#).

5. Select to restore the VM to its **Original location** (to the original VMware host and datastore), or to an **Alternate location** (to another datastore of the original VMware host or another VMware host).



6. Enable the **Run Direct** option to run the VM directly from the backup files in the backup destination. Configure the following options according to your restore requirement:



- **Auto migrate after Run Direct is running**

Enable this option to auto migrate the VM to a permanent location on the original VMware host \ another datastore of the original VMware host \ another VMware host, according to the **Restore virtual machines to** option.

NOTE

This will finalize the recovery of the VM; The migration will be performed after the VM is powered on.

- ⦿ **Auto power on after Run Direct is running**
Enable this option to power up the virtual machine automatically, after Run Direct is running for the VM.
- ⦿ **Use existing storage as VM working directory to improve performance**
Enable this option to enhance performance of the restored VM. Click **Next** to proceed when you are done with the settings.

7. Click Show advanced option if you want to enable Verify checksum of in-file delta files during restore.

Verify checksum of in-file delta files during restore

Hide advanced option

8. This step applies only for restoring to **Alternate location**. For restoring to **Original location**, skip to step 9.

Enter the VMware host and access information of where you would like the VM to be restored to.

- ⦿ For restoration to another VMware host (ESXi server), select **Version VMware ESXi 5 / 5.5 / 6 / 6.5 / 6.7**, then enter the **Password** of the root account, **Host**, **Port** and **SSH Port** of the new / original host.

Alternate location

VMware Host

Version
VMware ESXi 5 / 5.5 / 6 / 6.5 / 6.7

Username
root

Password
•••••

Host
10.16.8.29

Port
443

SSH Port
22

- For restoration to another VMware host (vCenter server), enter the **Username** and **Password** of the administrator account, **Host**, and **Port** information of the new / original vCenter server.

Alternate location

VMware Host

Version
VMware vCenter 5 / 5.5 / 6 / 6.5 / 6.7 ▼

Username
root

Password

Host
new_vcenter_host

Port
443

Press **Next** to proceed when you are done with the settings.

Enter a new **Name** for the VM, then **Browse** to modify the **Inventory Location**, **Host/Cluster**, **Resource Pool** and **Storage** settings, according to where you would like the VM to be restored to.

Alternate location

VMware ESXi 6.0.0 build-5050593@10.16.8.29:443(SSH:22)

Name
New Virtual Machine

Inventory Location
10.16.8.29 **Browse**

Host/Cluster
10.16.8.29 **Browse**

Resource Pool
10.16.8.29 **Browse**

Storage
vesxi02_datastore1 **Browse**

Alternate location

VMware vCenter Server 6.0.0 build-9313458@10.16.8.25:443

Name

Inventory Location

Host/Cluster

Resource Pool

Storage

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

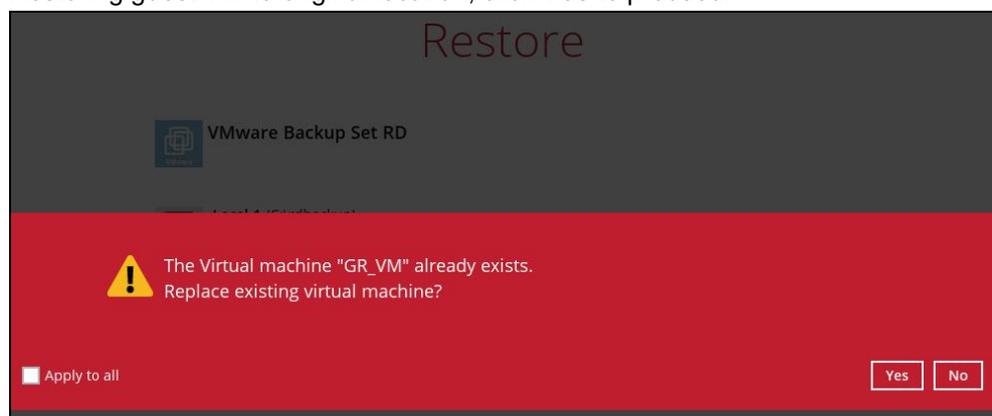
9. Select the temporary directory for storing temporary files, then click **Restore** to start the restoration.

Temporary Directory

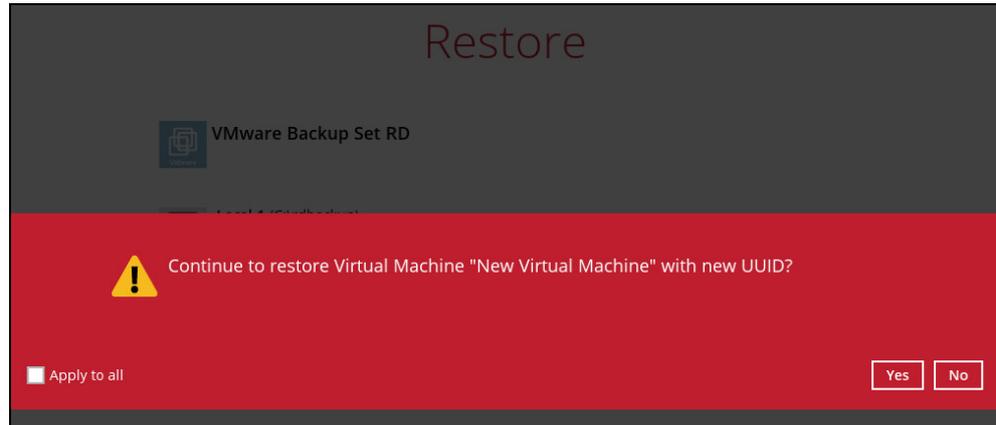
Temporary directory for storing restore files

10. When restoring your guest VM, different messages will be prompted depending on the selected location.

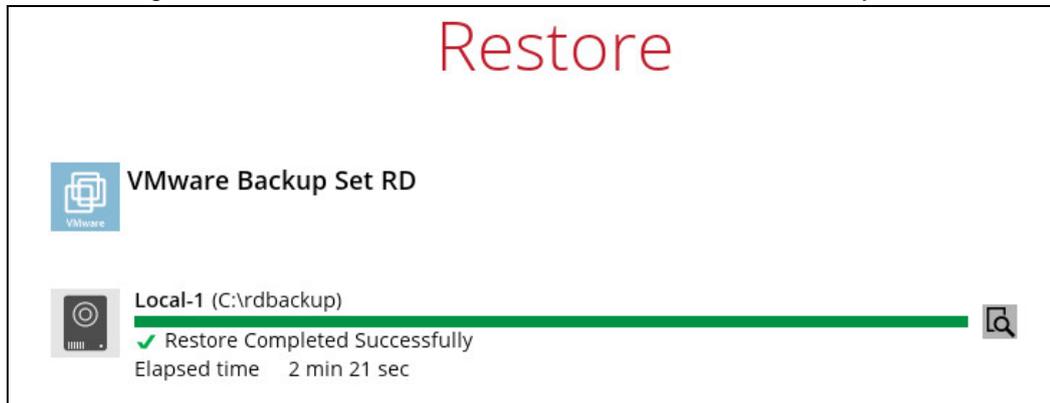
- Restoring guest VM to original location, click **Yes** to proceed.



- Restoring guest VM to another VMware host, since each virtual machine is automatically assigned a universally unique identifier (UUID), a new UUID must be created when you restore the guest VM to another host. It is not possible to have two identical UUID running at the same time, so make sure to click **Yes** when you see the prompt below.

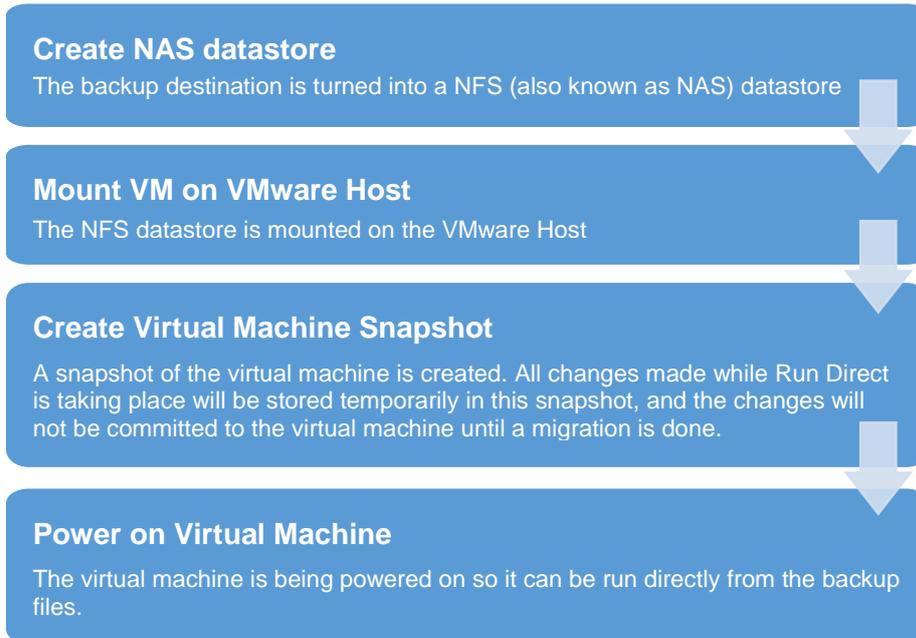


11. The following screen shows when the VM has been restored successfully.



Verifying Run Direct Restore Connection

When a run direct restore is initiated, the following steps are taken at the backend.

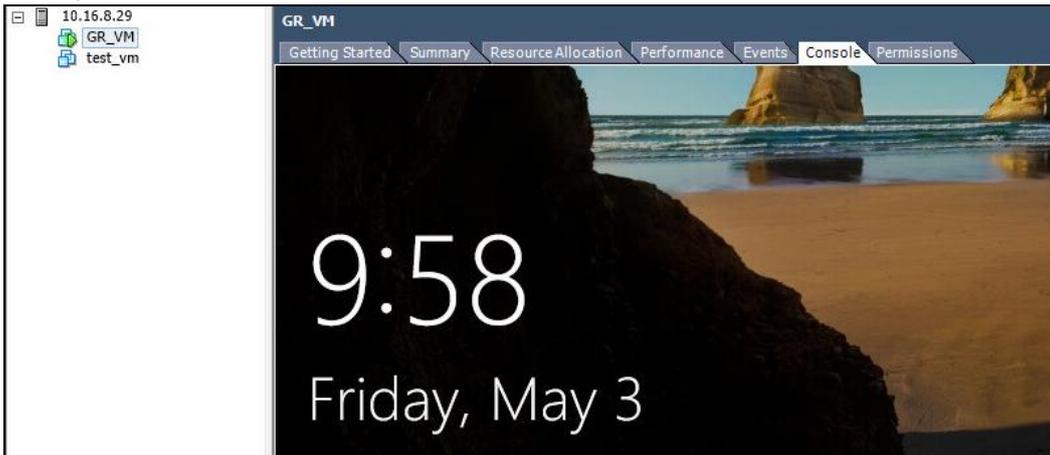


Check the following items to verify if the run direct restore connection has been established between the backup destination and the VMware host.

- The following screen with the text **Restore Completed Successfully** displayed in your AhsayOBM.



- You should also be able to see the restored VM being run directly from the backup files in the backup destination.



NOTE

Do not exit from the AhsayOBM application when a Run Direct restored VM is still running. Run Direct must be stopped (e.g. by finalizing recovery of the VM or stopping the VM) before exiting AhsayOBM.

When the restored VM is starting up, there may be an error screen prompted to alert you that Windows was not shut down properly. This message shows as a result of the VM's runtime status not being backed up. You may simply select to start up Windows as normal to proceed with the startup.

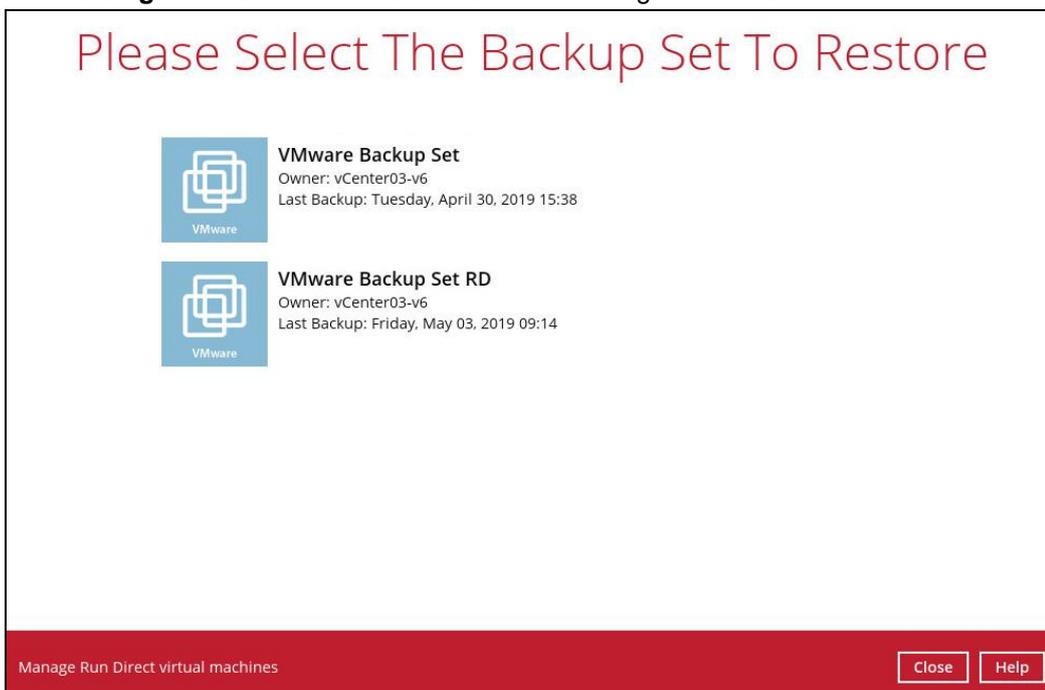
Manage Run Direct VM

Manage a Run Direct restored virtual machine, by finalizing the VM recovery (e.g. migrating it to a permanent location on the VMware host), or stop the virtual machine when it is no longer needed.

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



2. Click **Manage Run Direct virtual machines** to manage all Run Direct virtual machines.



Finalize VM Restore

To finalize recovery of a VM, migrate it to a permanent location on the VMware host:

1. Select the backup set which contains the Run Direct VM that you would like to finalize.



2. Click **Browse** to select the datastore where you would like to migrate the VM to.



3. Click **Migrate Virtual Machine** to start the migration process.

NOTE

For VM on ESXi host, the VM may be suspended temporarily during the migration process. The downtime of the VM should be minimal.

Stop Run Direct VM

To stop all virtual machines, or individual virtual machine that is running with the Run Direct feature:

1. Click **Stop all Run Direct virtual machines** to stop all VMs that are currently running with the Run Direct option.

Alternatively, select the backup set which contains the VM that you would like to stop.



2. Click **Stop Run Direct** to stop the VM.



3. Click **Yes** to proceed.



Run Direct Restore via User Web Console

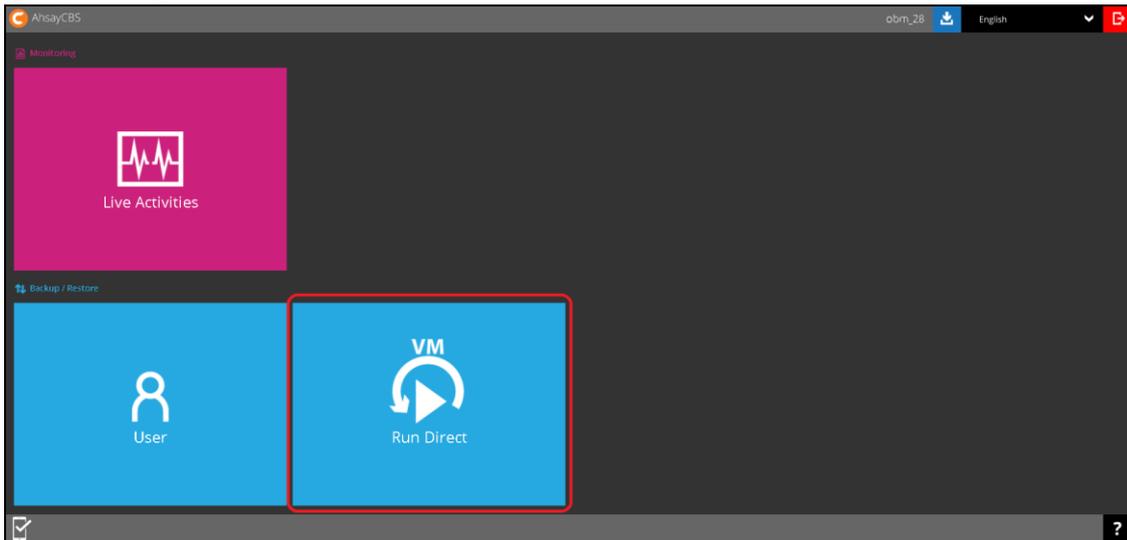
Besides using the AhsayOBM, you can now utilize the AhsayCBS User Web Console to initiate a run direct restore (also known as Agentless Restore).

Why use the User Web Console?

Unlike starting a Run Direct restore on AhsayOBM which you have to be physically with the client backup agent, you can now access the User Web Console to perform the same action as long as you have Internet connection and a web browser.

How to do it?

In the AhsayCBS User Web Console landing page, click on the Run Direct icon to start a run direct restore. For details on the operations, please refer to the [AhsayCBS User Guide](#). The steps below give you a high level overview of how a Run Direct is initiated on the AhsayCBS User Web Console.



Start a Run Direct Session

Run Direct



Running	Backup Set	Host	Name	Progress	Start time
---------	------------	------	------	----------	------------

Select the Backup Set

Start Run Direct

Backup Set

VMware Web RD Backup Set

Select Specific Backup Job

Start Run Direct

Restore file of job 2019-05-03-16-18-46

10.16.8.29

New Virtual Machine

Select Restore Destination

Restore virtual machines to

- Original Location
- Alternate Location

Configure the Run Direct Options

- Auto migrate after Run Direct is running
- Auto power on after Run Direct is running
- Use existing storage as VM working directory to improve performance

Run Direct Begins with Status Display

Timestamp	Type	Message
2019-06-23 08:00:36	info	"10.16.8.29" already exists.
2019-06-23 08:00:43	info	Powering off virtual machine "Lubuntu14_386"...
2019-06-23 08:00:47	info	Removing virtual machine "Lubuntu14_386" from the inventory...
2019-06-23 08:00:49	info	Preparing for Run Direct...



<input type="checkbox"/>	Running	Backup Set	Host	Name	Progress
<input type="checkbox"/>	No	VMware Web RD Backup Set	10.16.8.29		

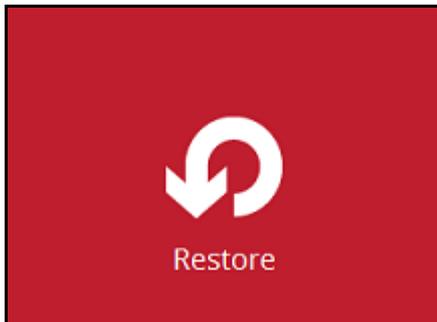
12 Method 2 - Restoring a Virtual Machine without Run Direct

Login to AhsayOBM

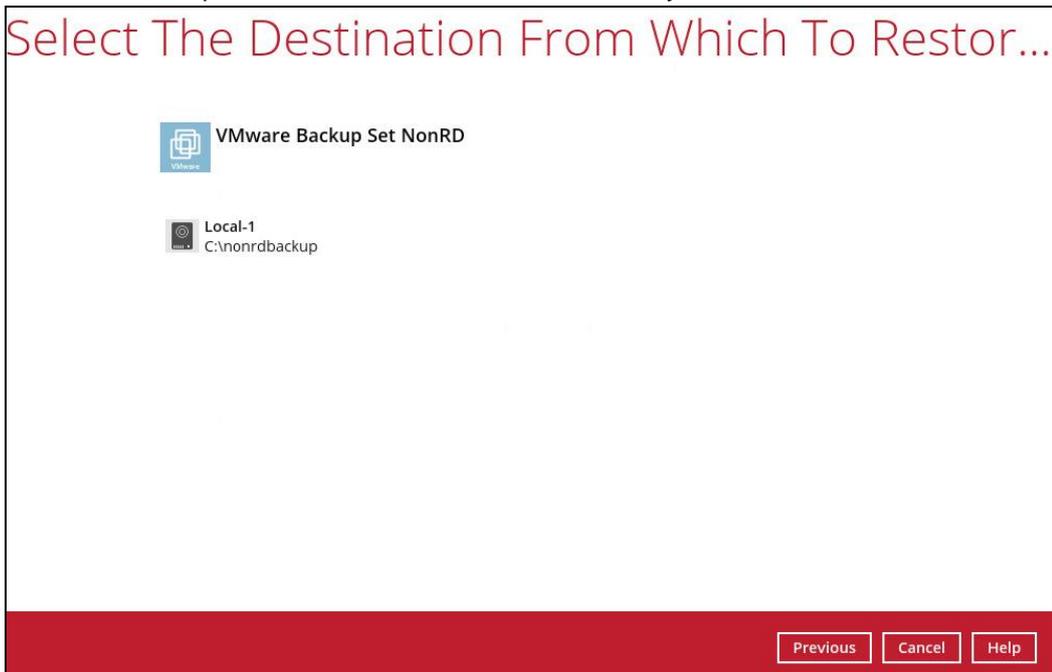
Login to the AhsayOBM application according to the instruction provided in the chapter on [Starting AhsayOBM](#).

VM Restore without Run Direct

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

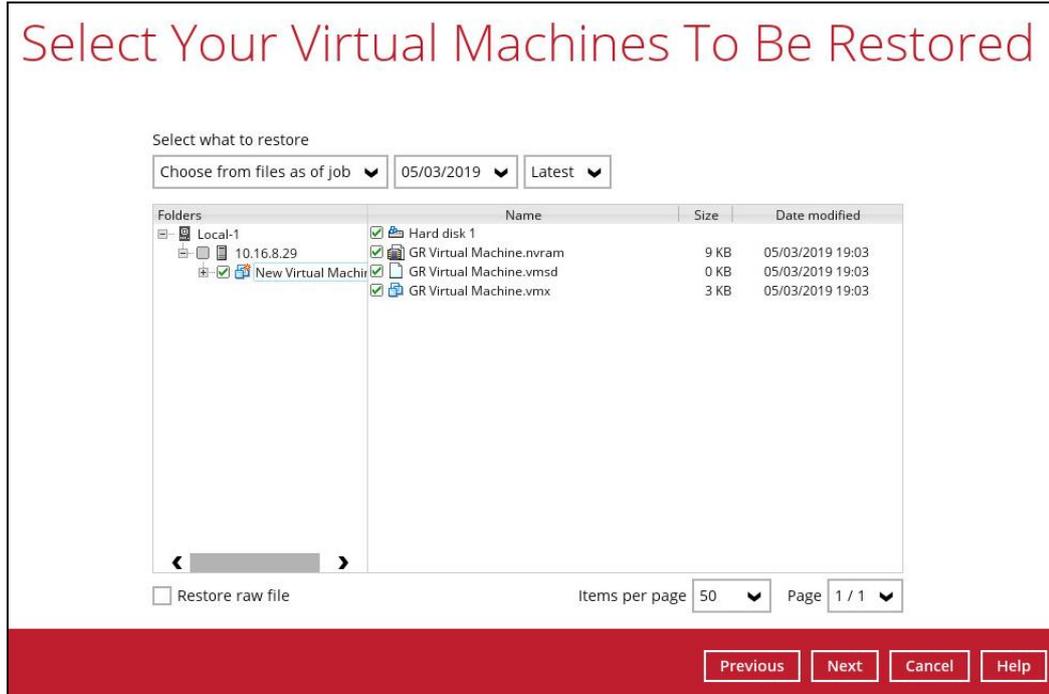


2. Select the backup set that you would like to restore the VM from.
3. Select the backup destination that contains the VM that you would like to restore.



4. Select to restore VM from a specific backup job, or the latest job available from the **Select what to restore** drop down menu.

5. Select the virtual machine that you would like to restore.



6. Select to restore the VM to its **Original location** (to the original ESXi host and datastore), or to an **Alternate location** (to a different VMware host or to another datastore).



7. Click **Show advanced option** if you want to enable Verify checksum of in-file delta files.



8. Click **Next** to proceed.
9. This step applies only for restoring to **Alternate location**. For restoring to **Original location**, skip to step 10.
- Enter the VMware host and access information of where you would like the VM to be restored to.
 - For restoration to another VMware host (ESXi server), select **Version VMware ESXi 5 / 5.5 / 6 / 6.5 / 6.7**, then enter the **Password** of the root

account, **Host**, **Port** and **SSH Port** of the new / original host.

Alternate location

VMware Host

Version
VMware ESXi 5 / 5.5 / 6 / 6.5 / 6.7 ▼

Username
root

Password

Host Port
new_esxi_host 443

SSH Port
22

- For restoration to another VMware host (vCenter server), enter the **Username** and **Password** of the administrator account, **Host**, and **Port** information of the new / original vCenter server.

Alternate location

VMware Host

Version
VMware vCenter 5 / 5.5 / 6 / 6.5 / 6.7 ▼

Username
root

Password

Host Port
new_vcenter_host 443

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

- ii. Enter a new **Name** for the VM, then **Browse** to modify the **Inventory Location**, **Host/Cluster**, **Resource Pool** and **Storage** settings, according to where you would like the VM to be restored to.

Alternate location

VMware ESXi 6.0.0 build-5050593@10.16.8.29:443(SSH:22)

Name

Inventory Location
 Browse

Host/Cluster
 Browse

Resource Pool
 Browse

Storage
 Browse

Alternate location

VMware vCenter Server 6.0.0 build-9313458@10.16.8.25:443

Name

Inventory Location
 Browse

Host/Cluster
 Browse

Resource Pool
 Browse

Storage
 Browse

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

- 10. Select the temporary directory for storing temporary files.

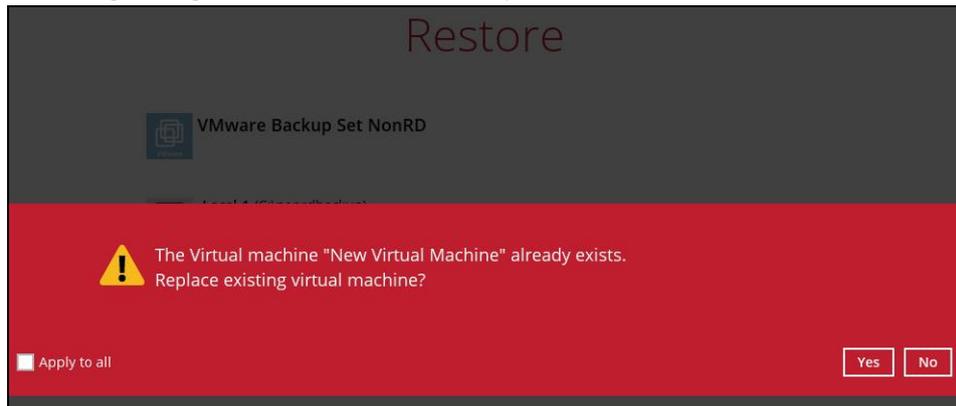
Temporary Directory

Temporary directory for storing restore files

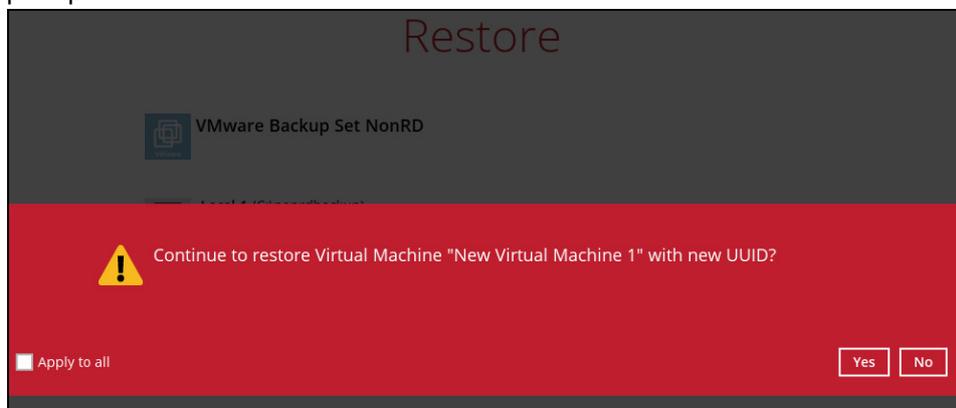
Browse

11. When restoring your guest VM, different messages will be prompted depending on your selected location.

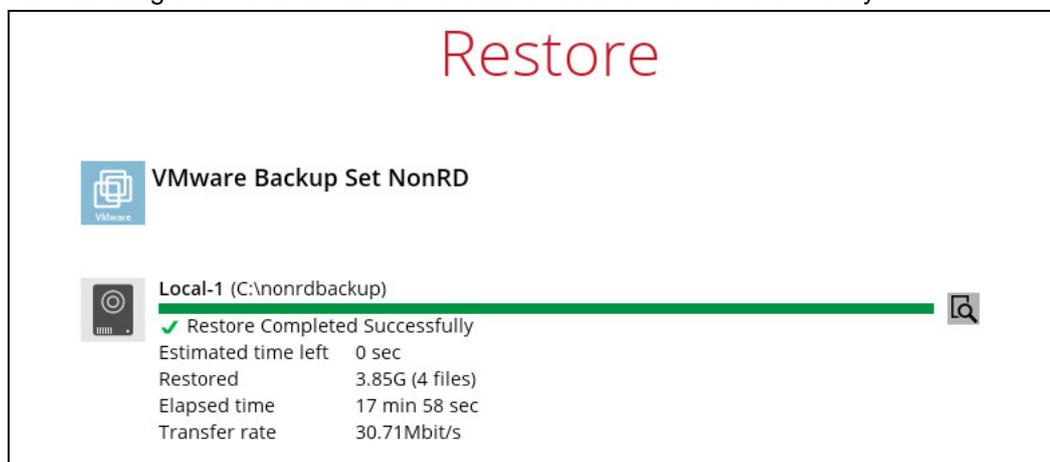
- Restoring to original location, click **Yes** to proceed.



- Restoring to another VMware host, since each virtual machine is automatically assigned a universally unique identifier (UUID), a new UUID must be created when you restore the guest VM to another host. It is not possible to have two identical UUID running at the same time so make sure to click **Yes** when you see the prompt below.



12. The following screen shows when the VM has been restored successfully.



NOTE

When the restored VM is starting up, there may be an error screen prompted to alert you that Windows was not shut down properly. This message shows as a result of the VM's runtime status not being backed up. You may simply select to start up Windows as normal to proceed with the startup.

13 Method 3 - Restoring a Virtual Machine in Raw File (VMDK Format)

Restoring a VM in VMDK format

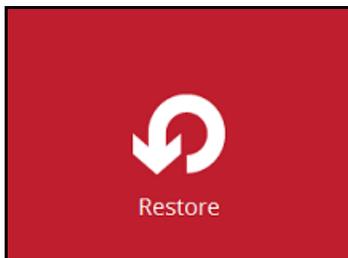
We have introduced a new feature to enable guest VMs that are backed up in VDDK mode to be restored in VMDK raw file format. This feature is useful if you wish to restore the backed up VM to another VMware host (ESXi server) even without using the AhsayOBM.

IMPORTANT

Restoring guest VMs from VDDK to VMDK format only supports backup sets that are created in AhsayOBM. Backup sets created with AhsayOBM before v7.9.0.0, or VMware VDDK backup sets migrated from v6 are **NOT** supported.

Follow the steps below for details.

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



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

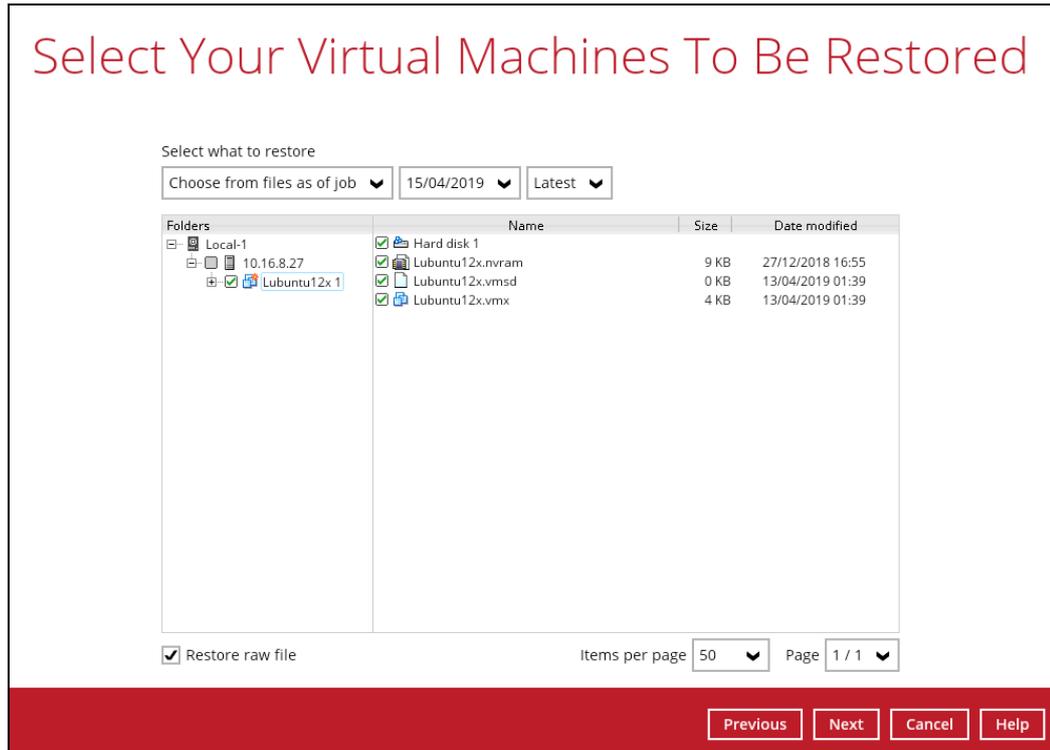


3. Select the backup destination that contains the VM that you would like to restore.



4. Select to restore VM from a specific backup job, or the latest job available from the **Select what to restore** drop down menu.
5. Select the virtual machine that you would like to restore in .vmdk format, then click the **Restore raw file** checkbox at the bottom left corner. It is possible to select multiple VM to

restore in .vmdk format.



6. Select a location where you wish to restore the VM to. Click **Browse** to select a location and then click **Next** to confirm.



7. Click **Show advanced** option if you want to enable the Verify checksum of in-file delta files.

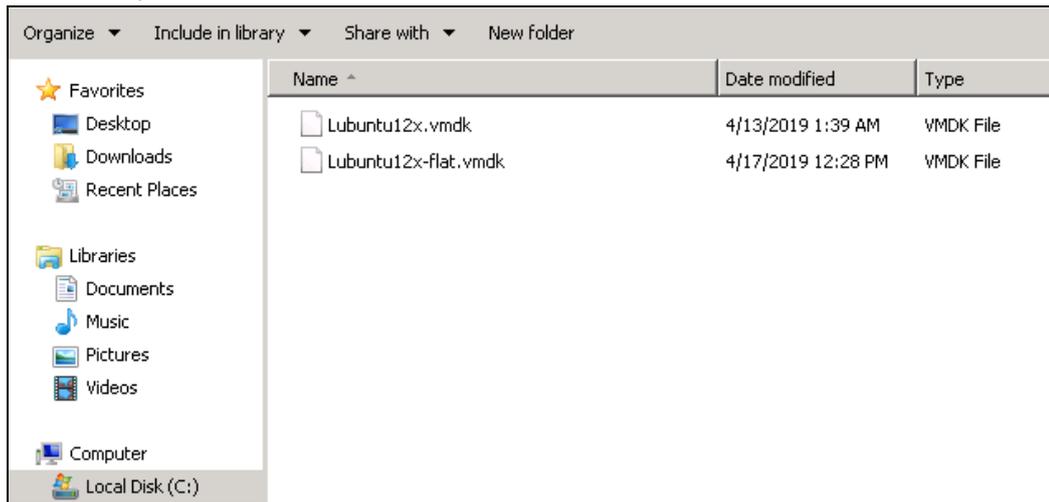


8. Select a temporary directory for storing restore files.



9. Click **Restore** to start the VM restore.

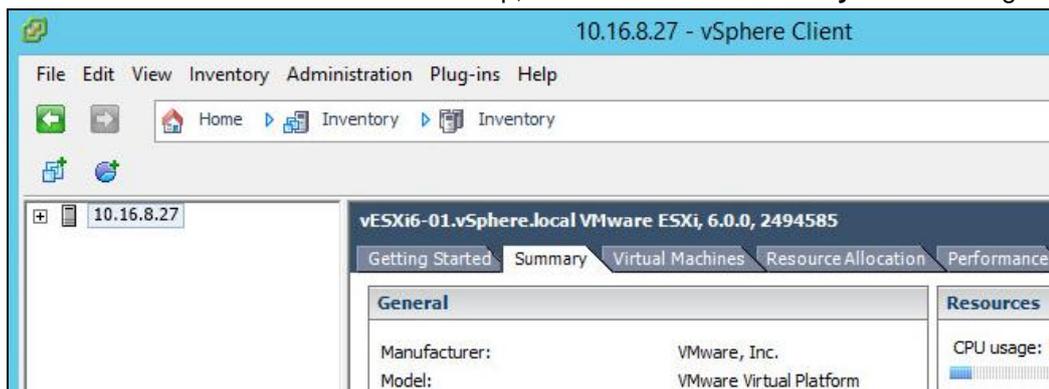
10. Open the folder where you have the VM restored. Check whether the .vmdk file has been successfully restored.



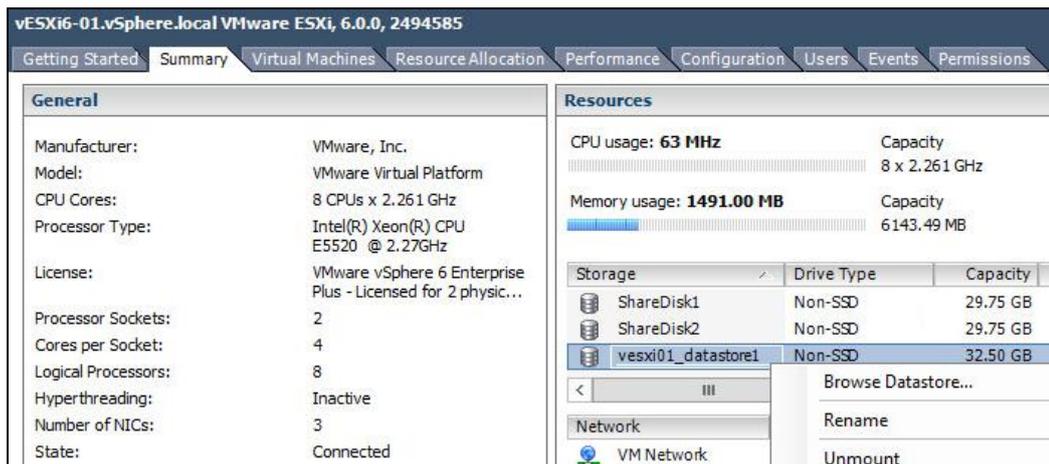
11. Open the VMware vSphere agent and log in to the ESXi server you wish to restore the VM to.



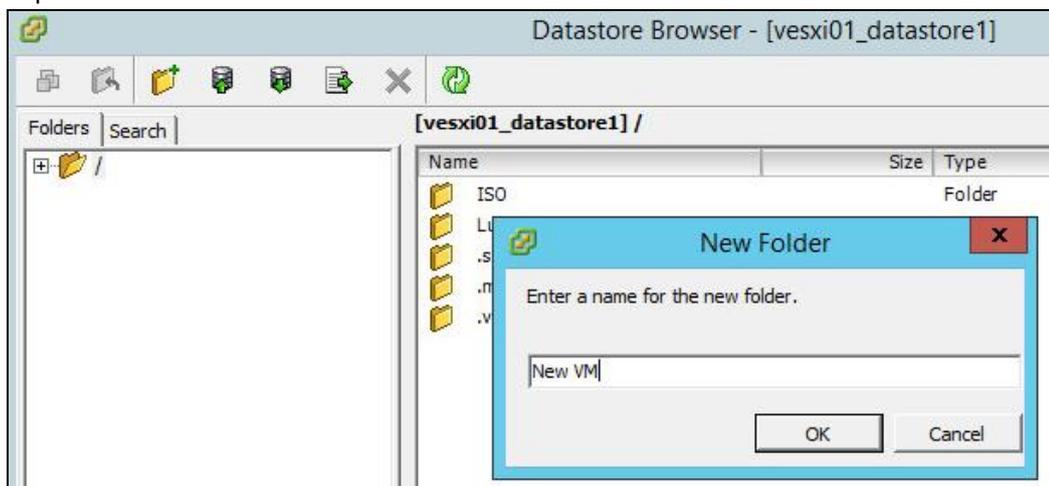
12. Click on the VM machine's name at the top, then look for the **Summary** tab on the right.



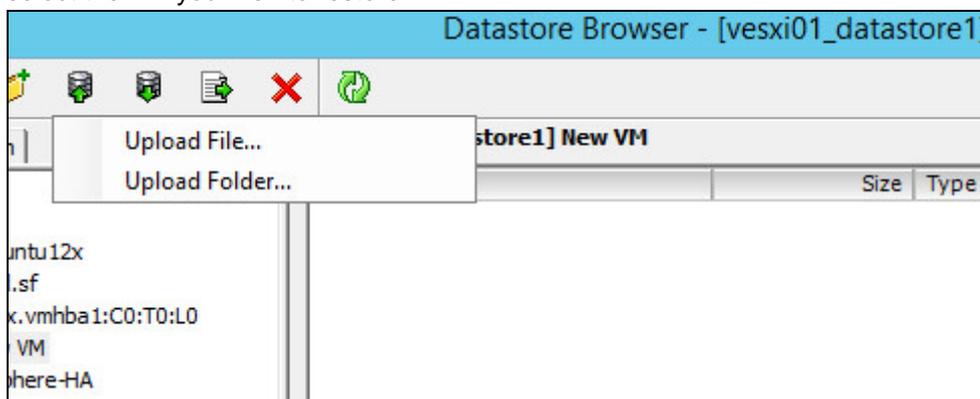
- Right click on the Datastore where you wish to deploy the restored VM to, then click Browse Datastore.



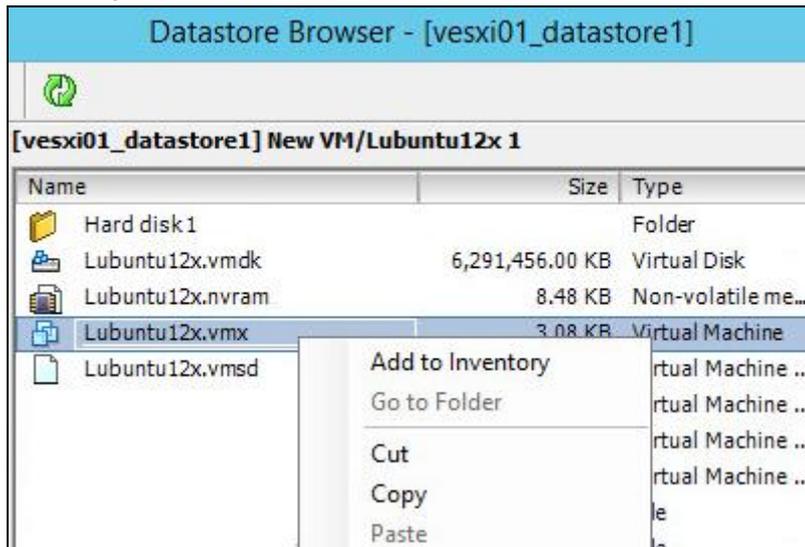
- Right click on the right panel to open a new folder for uploading the VM you are going to import.



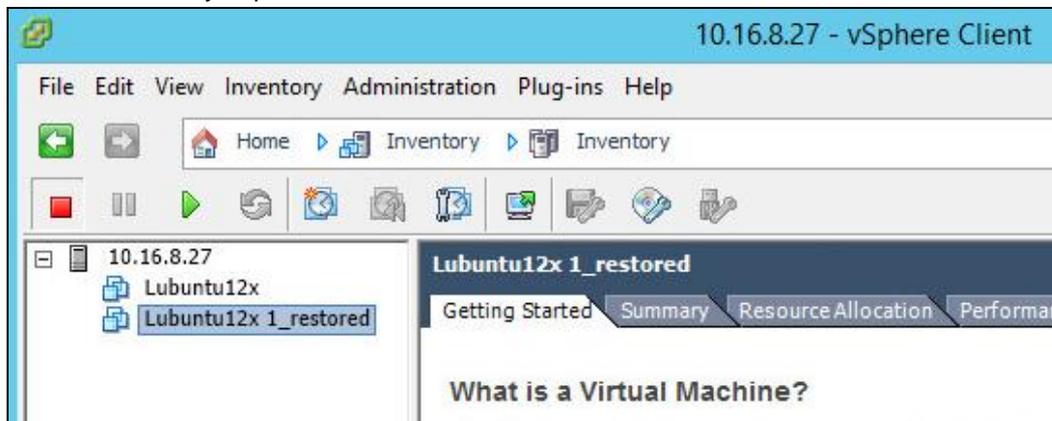
- Open the newly created folder then click the Upload Folder option at the top menu bar to select the VM you wish to restore.



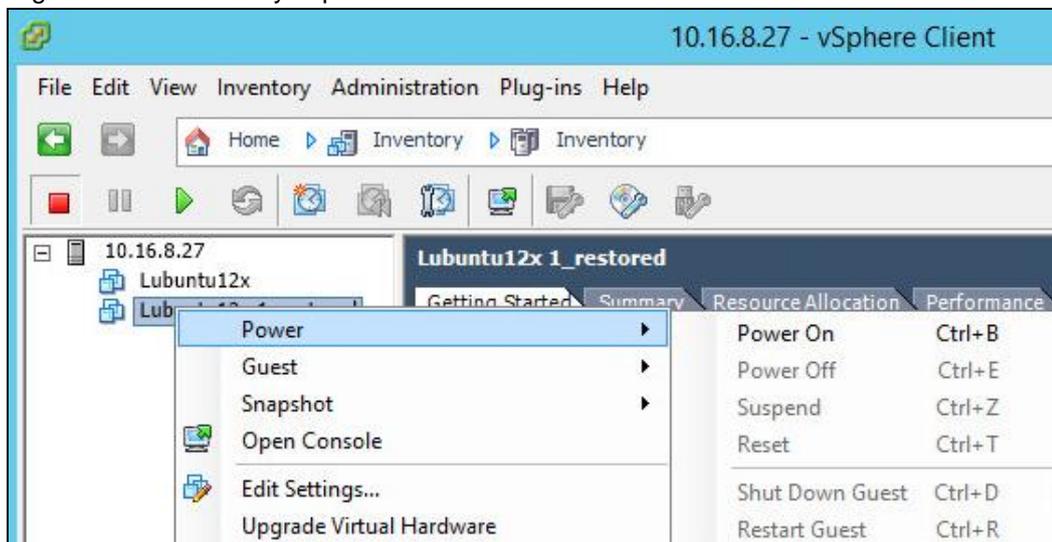
- Open the folder you have just uploaded, then right click on the .vmx file and click on **Add to Inventory**.



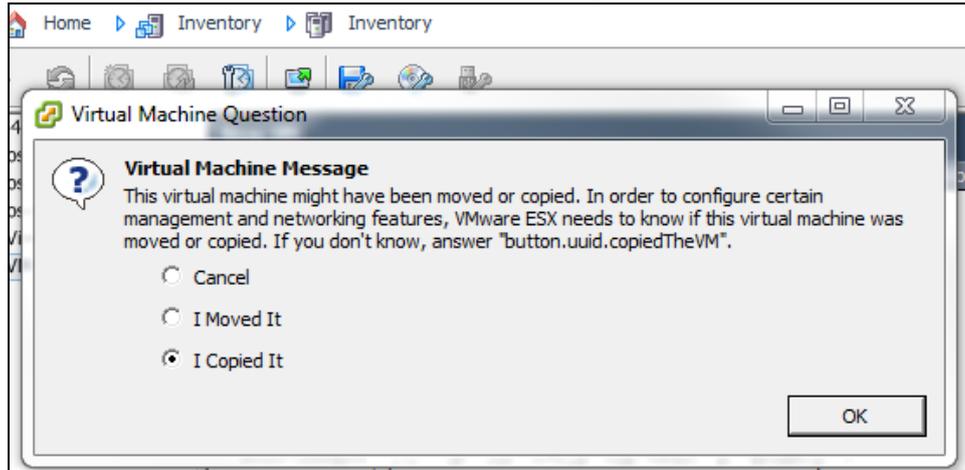
- Follow the screen prompts and name the imported VM and confirm the resource pool. You should see the imported VM display on the left on the main page of vSphere if the VM has been successfully imported to the ESXi server.



- Right click on the newly imported VM and then click Power On to turn it on.



19. Select **I Copied It** and then click **OK** to confirm if you see this screen.



14 Method 4 – 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.

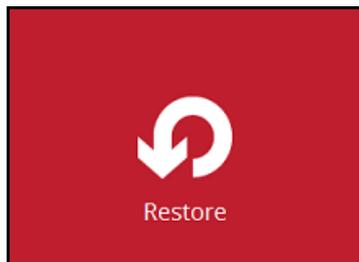
- Microsoft Visual C++ 2015 Redistributable (x86) / (x64)
<https://www.microsoft.com/en-us/download/details.aspx?id=48145>
- Update for Universal C Runtime in Windows
<https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows>
- Microsoft Security Advisory 3033929 (for Windows 7 and 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 supported with Granular Restore. 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 that 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.



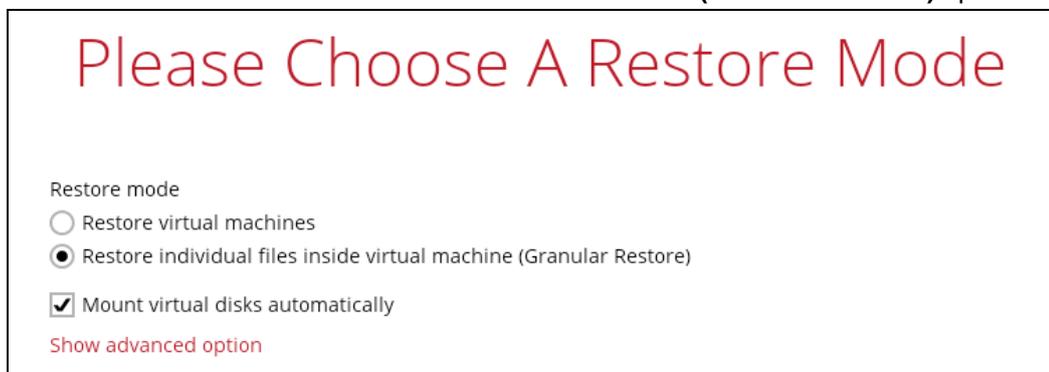
2. Select the backup set that you would like to restore the individual files from.



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



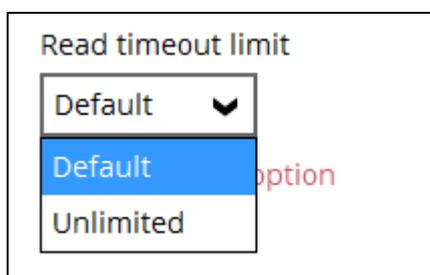
4. Select to the **Restore individual files in virtual machine (Granular Restore)** option.



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.



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

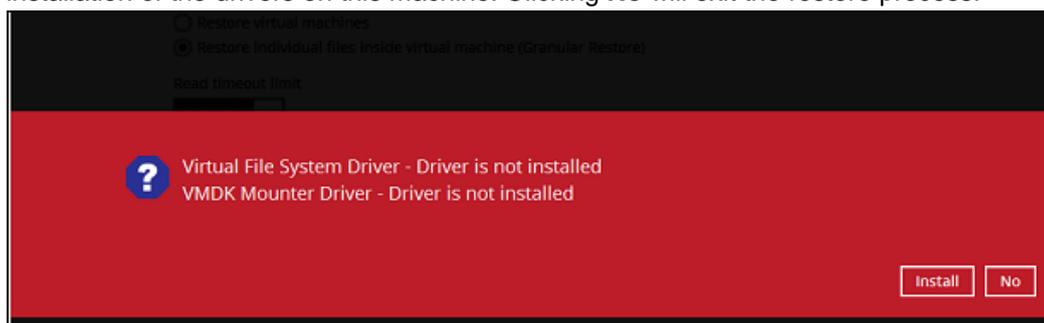
- **Default** – This setting should be suitable for guest VMs located on a local, removable, or network drive. The time out value is 15 seconds.
- **Unlimited** – the connection will not time out when this is selected. This selection is recommended when:
 - Backup destination is a cloud storage.
 - AhsayCBS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

NOTE

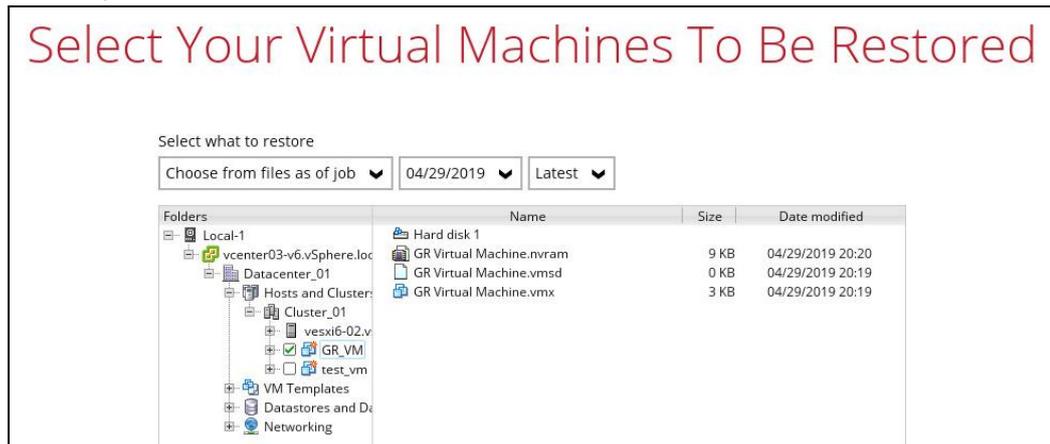
If in doubt or unsure about the guest VM size or network stability, it is recommended to use **Unlimited**.

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

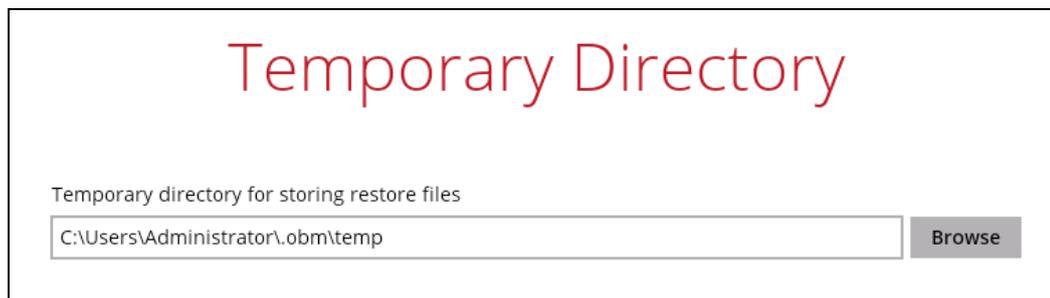
5. The following screen will be shown when you perform Granular Restore for a backup set on this machine for the first time only. Make sure you click **Install** to confirm starting the installation of the drivers on this machine. Clicking **No** will exit the restore process.



- Select the virtual machine that you would like to perform Granular Restore for, then click **Next** to proceed.



- Select a temporary directory for storing restore files, then click **Restore** to start the Granular Restore.

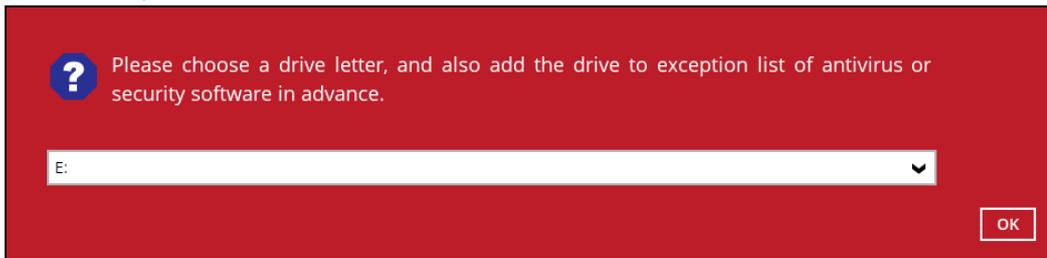


- When the virtual disk(s) are in the process of being prepared for mounting on the AhsayOBM machine, you will see the following screen.

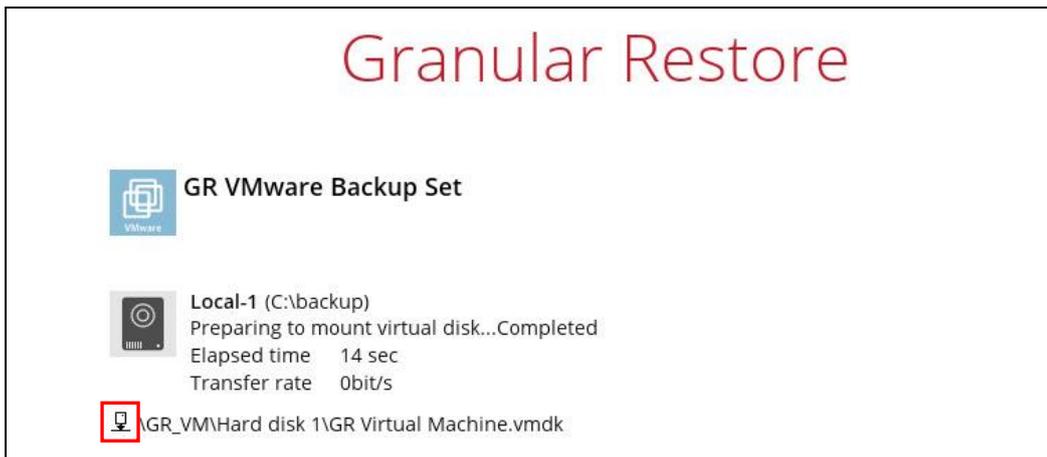


Please wait as the process could take some time depending on the size of the virtual disk, network bandwidth, and storage location.

9. Select the drive where you wish the mounted image to be mapped on your machine then click **OK** to proceed.



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



Otherwise, all the virtual disks will be automatically mounted.

11. When the virtual disk is mounted, you will see the following screen showing the information of the mounted virtual disk with the available volume shown.



There are two options to restore individual files from here.

Option 1: Restore Using AhsayOBM File Explorer

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

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

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



NOTE

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

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



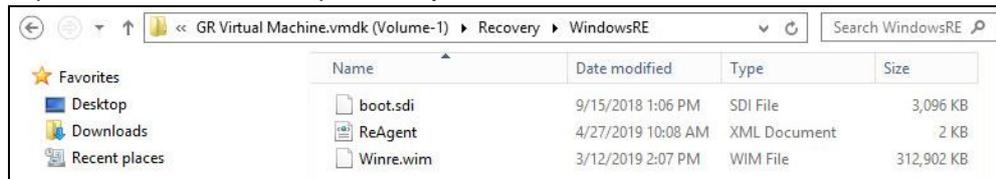
- iii. The following screen shows when the selected files have been restored to the defined destination.



Restore



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



Option 2: Restore Using Windows File Explorer

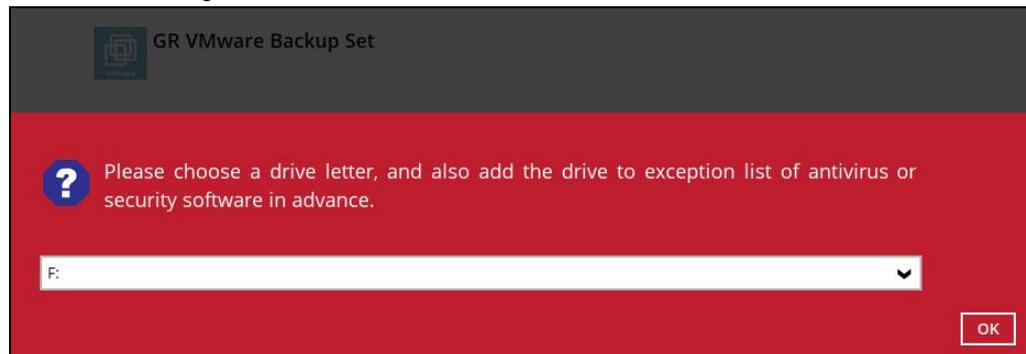
This method allows you to browse through the files from the mounted virtual disk through the Windows File Explorer on the machine where you have AhsayOBM installed on.

NOTE

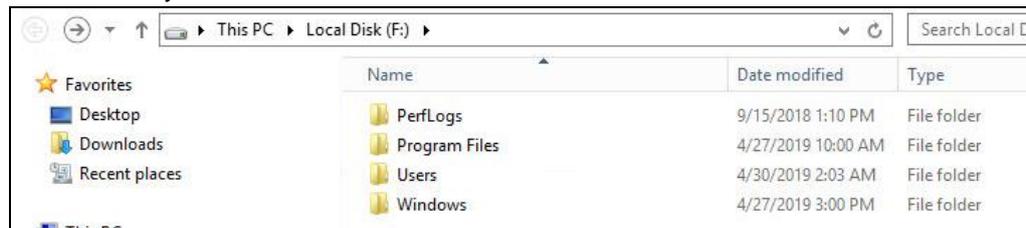
Granular restore of VMware backup sets performed using Windows File Explorer :

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

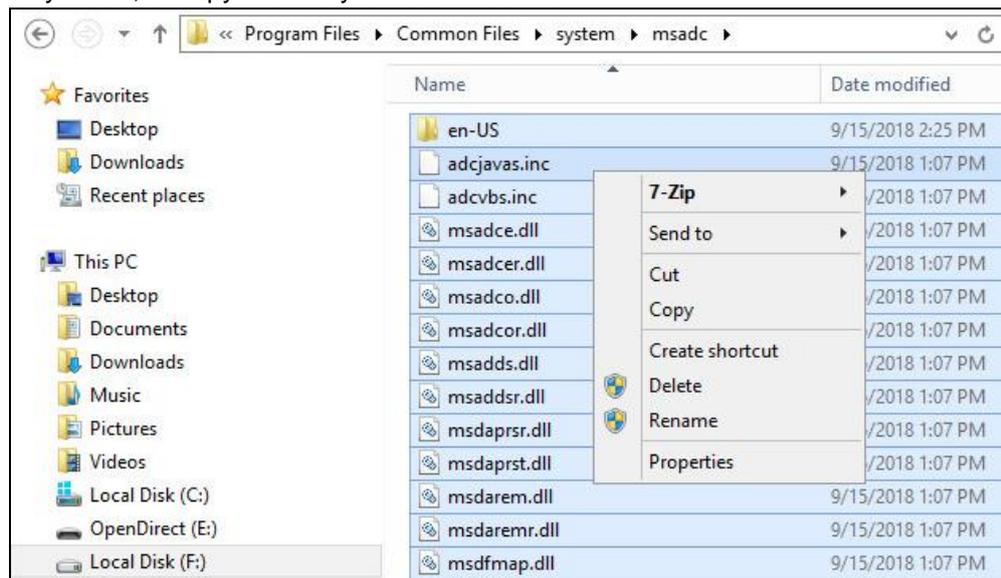
- i. Click  and then you will be prompted to select a drive letter where you wish the mounted backup image to be mapped on your machine, click **OK** when you have finished selecting.



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



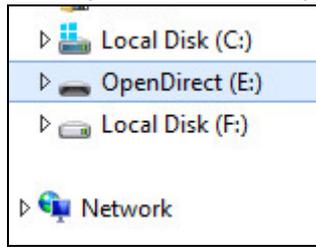
- iii. You can now click on the files to view them directly from here, which will be in read-only mode, or copy them to your local machine.



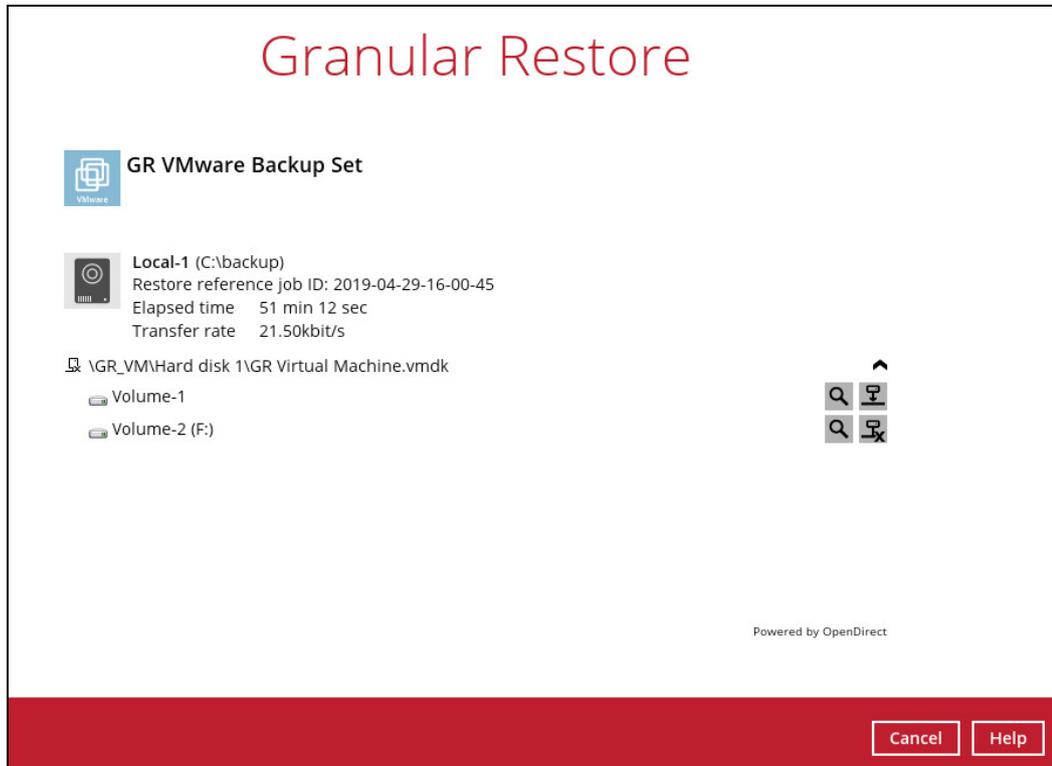
NOTE

Viewing the files directly is enabled only if the source application is already installed on the machine. i.e. "MS Word" must have already been installed for viewing the ".doc" file.

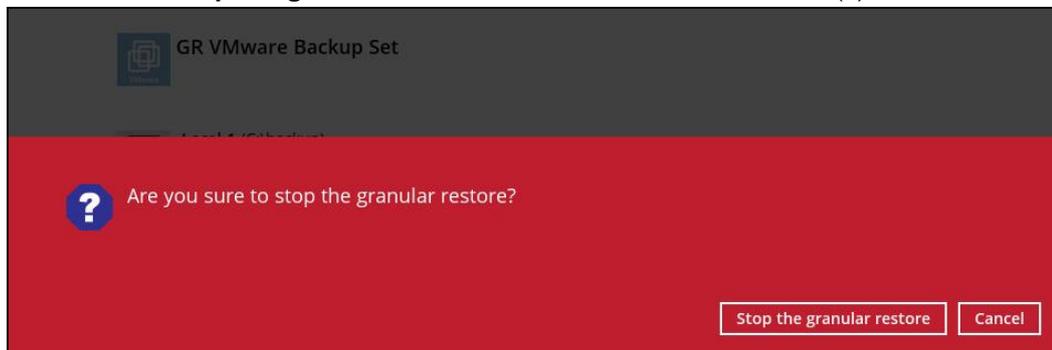
- iv. The mounted drive letter cannot be ejected from the Windows File Explorer, and it will only be closed when you exit AhsayOBM.



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



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



IMPORTANT

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

15 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.