

Ahsay Online Backup Manager v9

VMware vCenter/ESXi Guest Virtual Machine Backup & Restore Guide

Ahsay Systems Corporation Limited

27 January 2023

Copyright Notice

© 2023 Ahsay Systems Corporation Limited. All rights reserved.

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

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

Trademarks

Ahsay, Ahsay Cloud Backup Suite, Ahsay Online Backup Suite, Ahsay Offsite Backup Server, Ahsay Online Backup Manager, Ahsay A-Click Backup, Ahsay Replication Server, Ahsay BackupBox Firmware, Ahsay Universal Backup System and Ahsay NAS Client Utility, Ahsay Mobile are trademarks of Ahsay Systems Corporation Limited.

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

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

Dropbox is a registered trademark of Dropbox Inc.

Google Cloud Storage, Google Drive, Google Authenticator, and Android are registered trademarks of Google Inc.

Wasabi Hot Cloud Storage is a registered trademark of Wasabi Technologies Inc.

Backblaze B2 Cloud Storage is a registered trademark of Backblaze Inc.

MariaDB is a registered trademark of MariaDB Corporation AB.

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

Microsoft Windows, Microsoft Exchange Server, Microsoft SQL Server, Microsoft Hyper-V, Microsoft Azure, OneDrive, OneDrive for Business, Microsoft Authenticator, and Microsoft Office 365 are registered trademarks of Microsoft Corporation.

Oracle, Oracle Database, Java and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

OpenJDK is a registered trademark of Oracle America, Inc.

Rackspace and OpenStack are registered trademarks of Rackspace US, Inc.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo and JBoss are registered trademarks of Red Hat, Inc. www.redhat.com in the U.S. and other countries.

Linux is a registered trademark of Linus Torvalds in the U.S. and other countries.

Ubuntu is a registered trademark of Canonical Ltd.

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

Rocky is a registered trademark of Rocky Brands.

ShadowProtect is a registered trademark of StorageCraft Technology Corporation.

VMware ESXi, vCenter, and vSAN are registered trademarks of VMware, Inc.

All other product names are registered trademarks of their respective owners.

Disclaimer

Ahsay Systems Corporation Limited will not have or accept any liability, obligation or responsibility whatsoever for any loss, destruction or damage (including without limitation consequential loss, destruction or damage) however arising from or in respect of any use or misuse of reliance on this document. By reading and following the instructions in this document, you agree to accept unconditionally the terms of this Disclaimer and as they may be revised and/or amended from time to time by Ahsay Systems Corporation Limited without prior notice to you.

Revision History

Date	Descriptions	Version
7 March 2022	<ul style="list-style-type: none">▪ Ch. 7.1 – added Migrate Data▪ Ch. 2.1 – added Non-VDDK end of support	9.1.0.0
3 November 2022	<ul style="list-style-type: none">▪ Ch. 6 – added instructions on how to enable CBT	9.1.0.0
27 January 2023	<ul style="list-style-type: none">▪ Ch. 9, 10, 11, 12 and 13 – updated restore instructions	9.5.2.0

Table of Contents

1	Overview.....	1
1.1	What is this software?	1
1.2	System Architecture.....	1
1.3	Why should I use AhsayOBM to back up my VMware vCenter/ESXi?.....	2
1.4	What is the purpose of this document?	7
1.5	What should I expect from this document?.....	8
1.6	Who should read this document?	8
2	Understanding VMware Backup Mode.....	9
2.1	Non-VDDK Backup Mode End of Support	9
2.2	VMware Backup Mode	9
	VDDK Backup Mode	9
2.3	Features of VDDK Backup Mode	10
2.4	VDDK Backup Mode Limitations	11
2.5	VDDK API Changes.....	12
3	Requirements.....	13
3.1	Hardware Requirement	13
3.2	Software Requirement	13
3.3	Antivirus Exclusion Requirement.....	13
3.4	VMware vCenter / ESXi Server Requirements	13
	3.4.1 ESXi / vCenter Patch Release	13
	3.4.2 License Specification	13
	3.4.3 ESXi Shell Access	14
	3.4.4 SSH.....	14
	3.4.5 Root Account	14
	3.4.6 Port Requirement.....	14
	3.4.7 Disk Space Available on Datastore	14
	3.4.8 VMware Tools.....	14
	3.4.9 ESXi Hosts and Virtual Machine Hardware Versions Compatibility	15
3.5	Backup Client Computer Requirements	15
	3.5.1 Hardware and Software Requirement	20
	3.5.2 Add-on Module Requirement	20
	3.5.3 Backup Quota Requirement.....	21
	3.5.4 Port Requirement.....	21
	3.5.5 Backup Client Computer on Linux.....	21
	3.5.6 Disk Space Available on Backup Client Computer (or the vCenter computer)	22
	3.5.7 Windows OS Requirement for VDDK Mode	22
3.6	Run Direct Requirements	22
	3.6.1 VDDK Backup Mode.....	22

3.6.2	Backup Destination Requirement.....	22
3.7	VDDK Backup Mode Requirements	24
3.7.1	License Requirement.....	24
3.7.2	Changed Block Tracking (CBT) on VMs	24
3.7.3	VMware CBT Known Issues	25
3.7.4	VMware Snapshot	26
3.7.5	Virtual Machine State.....	26
3.7.6	File Name Requirement.....	26
3.7.7	Restore Requirement.....	26
3.8	vSAN Backup and Restore	27
3.8.1	Requirements	27
3.8.2	Limitations	28
4	Best Practices and Recommendations.....	29
5	Granular Restore Technology	32
5.1	What is Granular Restore Technology?.....	32
5.2	How does Granular Restore work?	33
5.3	Benefits of using Granular Restore	34
5.4	Requirements	35
5.4.1	Supported Backup Modules.....	35
5.4.2	License Requirements	35
5.4.3	Backup Quota Storage	35
5.4.4	Operating System.....	36
5.4.5	Temporary Directory Requirement.....	36
5.4.6	Network Drive Requirements	36
5.4.7	Available Spare Drive Letter	36
5.4.8	Network Requirements	36
5.4.9	Other Dependencies.....	37
5.4.10	Permissions.....	37
5.5	Limitations.....	37
	Enhanced Network Drive Support	37
6	Creating a VMware VM Backup Set.....	38
7	Running a Backup	49
7.1	Start a Manual Backup.....	49
7.2	Configure Backup Schedule for Automated Backup	55
8	Restore Methods.....	60
9	Method 1 - Restoring a Virtual Machine with Run Direct.....	62
9.1	Running Direct Restore via AhsayOBM.....	62
9.2	Verifying Run Direct Restore Connection	69
9.3	Manage Run Direct VM.....	71
9.3.1	Finalize VM Restore	71

9.3.2	Stop Run Direct VM	72
9.4	Run Direct Restore via User Web Console	74
10	Method 2 - Restoring a Virtual Machine without Run Direct	76
	VM Restore without Run Direct	76
11	Method 3 - Restoring a Virtual Machine in Raw File (VMDK Format)	82
	Restoring a VM in VMDK format	82
12	Method 4 – Granular Restore	88
	Requirements and Limitations	88
13	Method 5 - Restoring a Virtual Machine on vSAN	97
13.1	Restore with Run Direct	98
13.1.1	Restore from vSAN datastore to vSAN datastore.....	98
13.1.2	Restore from vSAN datastore to VMFS datastore.....	104
13.1.3	Restore from VMFS datastore to vSAN datastore.....	111
13.2	Restore without Run Direct	118
13.2.1	Restore from vSAN datastore to vSAN datastore.....	118
13.2.2	Restore from vSAN datastore to VMFS datastore.....	123
13.2.3	Restore from VMFS datastore to vSAN datastore.....	129
14	Contact Ahsay	135
14.1	Technical Assistance	135
14.2	Documentation.....	135
Appendix	136
	How to clean up the temporary files on VMware Host when Run Direct terminates unexpectedly	136

1 Overview

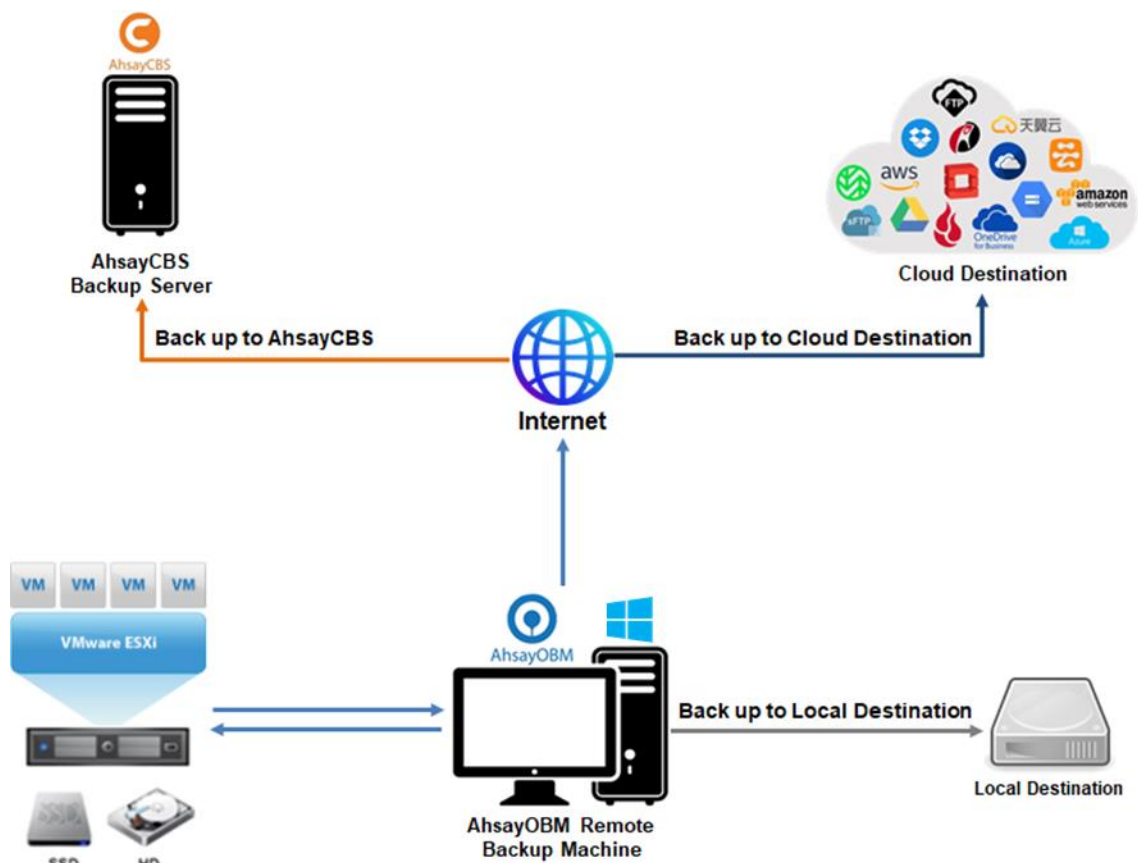
1.1 What is this software?

Ahsay brings you specialized client backup software, namely AhsayOBM, to provide a comprehensive backup solution for your 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.

1.2 System Architecture

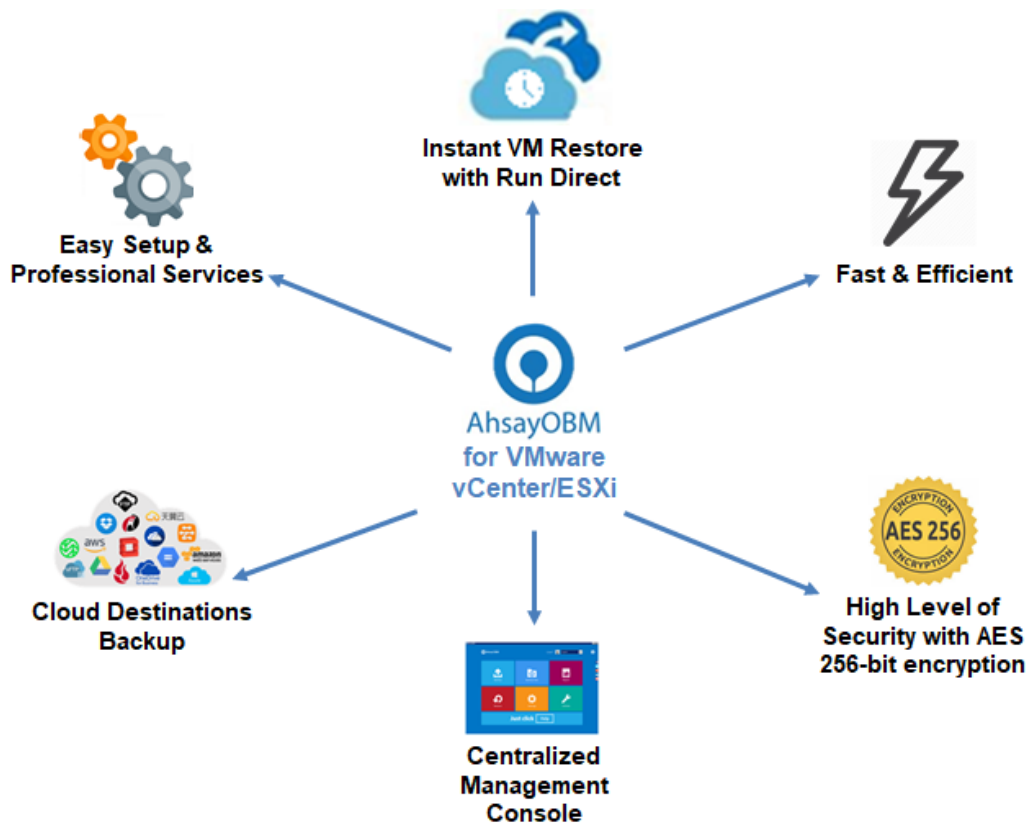
Below is the system architecture diagram illustrating the major elements involved in the backup process among the VMware server, AhsayOBM and AhsayCBS.

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.



1.3 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 where we can help make your backup experience a better one.



Easy Setup & Professional Services

Setup is a few clicks away - our enhanced AhsayOBM v9 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?

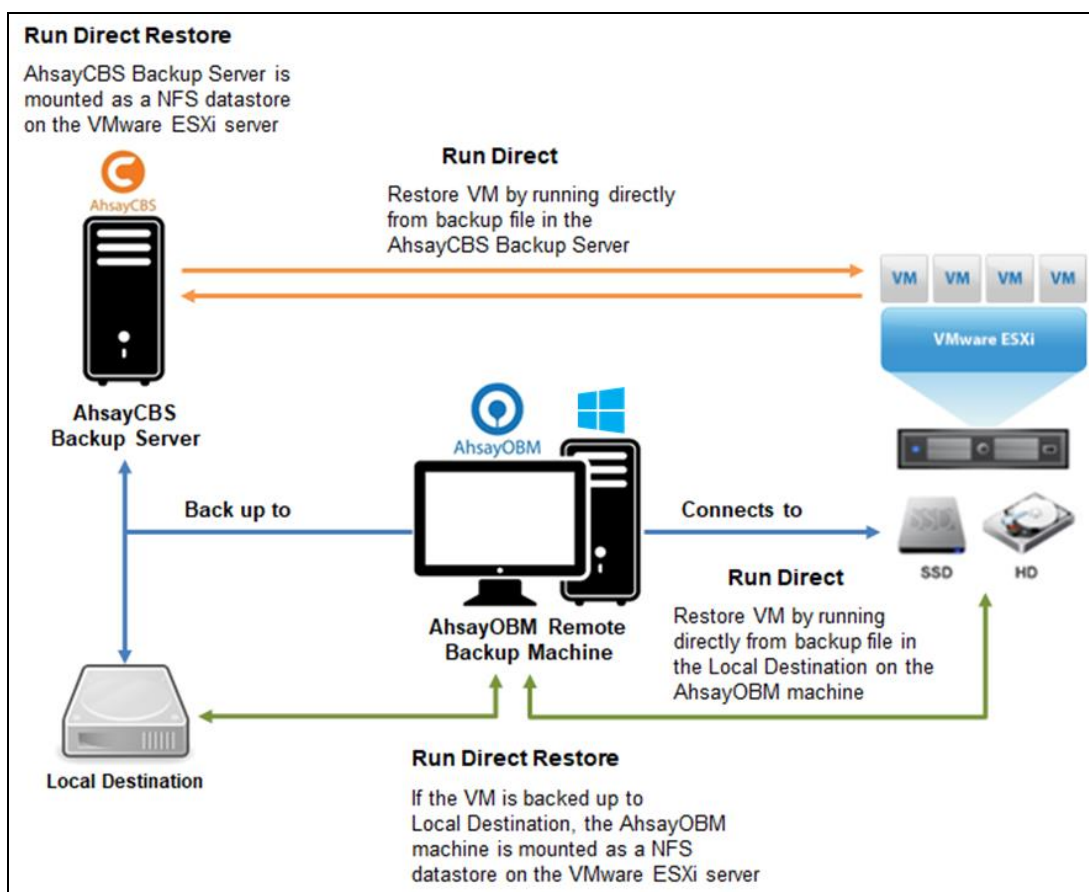
Run Direct is a feature that helps reduce disruption and downtime of your production VMs.

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).



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:

VMware Snapshot

A VMware snapshot is created for the VM.

Copying Files

Backup files from the NFS datastore are copied to the production datastore on the VMware host.

Copying Changes

Changes made to the VM after the snapshot creation are moved to the new location.

Data Consolidation

The VM is suspended temporarily to consolidate the changes made after the snapshot creation.

Resume VM

After all changes are consolidated, the VM is resumed.

Dismount NFS Datastore

The NFS datastore is dismounted.

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.

- ❶ **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.
- ❷ **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 [AhsayCBS v9 Administrator's Guide](#).

- ❶ **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 [AhsayCBS v9 User's Guide](#).
- ❷ **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 *		Microsoft Azure
	CTYun *		Microsoft OneDrive
	Amazon S3		Microsoft OneDrive for Business
	AWS S3 Compatible Cloud Storage		Rackspace
	Wasabi		OpenStack
	Backblaze		Dropbox
	Google Cloud Storage		FTP
	Google Drive		SFTP

* Available on computers with China or Hong Kong local settings

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

- ❶ **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.
- ❷ **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.

- ❶ **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.

1.4 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 VDDK backup mode

Requirements

Hardware, software, VMware server, Client Backup Computer, Run Direct, and VDDK backup mode Requirements

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

1.5 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.

1.6 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 VMware Backup Mode

2.1 Non-VDDK Backup Mode End of Support

Starting with AhsayOBM v9 or above, **Non-VDDK backup mode is no longer supported** in VMware backups and ONLY VDDK backup mode is supported.

Therefore, **FILE mode is also no longer supported** in VMware Backup set type.

VMware backup sets created in AhsayOBM v8.5.4.x with AhsayCBS v9 can still be run in non-VDDK backup mode. However, if the AhsayOBM v8.5.4.x is upgraded to AhsayOBM v9 or above with AhsayCBS v9, VMware backup sets in non-VDDK backup mode will fail to back up.

Therefore, if the VMware backup set will continue to run backup jobs in non-VDDK backup mode, it is recommended to NOT upgrade to AhsayOBM v9 and continue using AhsayOBM v8.5.4.x.

For more details, refer to the following article:

[FAQ: VMware Non-VDDK Backup Mode in AhsayOBM v9](#)

2.2 VMware 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 to the license key on the VMware host, the operating system of the backup machine where the AhsayOBM is installed, as well as other requirements outlined in [Chapter 3 Requirements](#).

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 backups.

Pros

Faster backup speed for subsequent backups, 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.

Run Direct is supported.

Cons	<p>Requires paid license, i.e. VMware Essentials License for usage of vSphere API.</p> <p>Requires VMFS5, VMFS6 or vSAN datastores to support full and incremental backups according to used size of the guest VM.</p>
-------------	--

<p style="text-align: center;">NOTE</p> <p>In VDDK backup mode, if the guest VM is located on an NFS datastore, the full backup will be performed using provisioned size of the guest VM.</p>
--

Further to the VMware license requirement described above, there are other requirements for VMware VM backup in VDDK backup mode. Refer to [Chapter 3 Requirements](#) for details.

2.3 Features of VDDK Backup Mode

	VDDK (CBT)
Full Backup	Used data size of guest
Incremental / Differential	Generated by VMware Host using CBT
Storage Size	Uses less storage quota
Storage Cost	Lower storage cost
Backup Speed	Faster backup speed due to smaller data size
Run Direct Support	YES
Restore from VDDK to VMDK format	YES
Granular Restore	YES
AhsayOBM on Windows Platform	YES
AhsayOBM on Non-Windows Platform	NO
Backup and Restore to vSAN Cluster	YES

2.4 VDDK Backup Mode Limitations

- Guest VMs with RDM (Raw Device Mapping) disks, or iSCSI initiator are not supported. As VMware is not able to create a snapshot of raw, RDM disks or iSCSI disks.

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

- Guest VMs with raw disks are not supported. As VMware is not able to create a snapshot of raw disks.

To perform a backup of the guest VM, it must either be powered off before the backup job or alternatively install AhsayOBM directly onto the guest VM to perform backups.

- Backup of guest VM snapshots are not supported.
- Backup of guest VM state (e.g. power on state / suspend state) is not supported.
- If a guest VM has virtual hard disks larger than 2 TB, VMware snapshot operations can take much longer to finish, therefore backups may take longer.
- Guest VMs setup with PCI vSphere DirectPath I/O devices are not supported. As VMware is not able to create a snapshot of these devices.

The guest VMs must be powered off before a backup can be made.

- All independent disks both persistent and non-persistent are not supported. As VMware does not support snapshots of independent disks when the guest VM is powered on.

To perform a backup of the guest VM, it must either be powered off before the backup job or alternatively install AhsayOBM directly onto the guest VM to perform backups.

NOTE

Backup of suspended guest VMs with independent disks are also not supported.

- Guest VMs configured with bus sharing are not supported. As VMware does not support snapshots of this type of configuration.

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

2.5 VDDK API Changes

VDDK 7 API implemented in AhsayOBM v8.3.4.0 to v8.3.6.x was found to cause issues on some VMware ESXi/vCenter v6, v6.5, v6.7, and v7 backup sets running in VDDK mode, related to both backup and restore. Ahsay has decided to **temporarily revert to using VDDK 6 API** until the VDDK 7 API bug has been addressed by VMware.

Until further notice, VDDK 6 API will be used for:

- All new installation of AhsayOBM v9.1.0.0 or above
- AhsayOBM upgrades from v6, v7 or pre-v9.1.0.0 to 9.1.0.0 or above

Affected existing AhsayOBM version with VDDK 7 API: AhsayOBM v8.3.4.0 to 8.3.6.x

Affected VMware versions: VMware ESXi/vCenter v6, v6.5, v6.7 and v7 backup sets running in VDDK backup mode.

To address the issues of clients with VMware VDDK mode backup sets on affected AhsayOBM versions, it is strongly advised to immediately upgrade to AhsayOBM v9.1.0.0 or above. Once AhsayOBM is upgraded to v9.1.0.0 or above, the existing VMware ESXi/vCenter v6, v6.5, v6.7, and v7 backup jobs will resume running without any further configuration or intervention needed.

3 Requirements

3.1 Hardware Requirement

Refer to the following article for the list of hardware requirements for AhsayOBM:

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

3.2 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 9.1 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 on version 9.1 or above](#)

3.3 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:

[FAQ: Suggestion on antivirus exclusions to improve performance of Ahsay software on Windows](#)

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.

3.4 VMware vCenter / ESXi Server Requirements

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

3.4.1 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>)

3.4.2 License Specification

- Paid License (VMware Essentials License or above): VMware ESXi and vCenter v5.5, v6, v6.5, v6.7 and v7
- Free License: VMware ESXi v5.5, v6, v6.5, v6.7

NOTE

For backup of VMware vCenter/ESXi 7 hosts using a Free License key or if the AhsayOBM is installed on a non-Windows staging machine such as macOS or Linux/FreeBSD, the guest VMs must be powered off.

3.4.3 ESXi Shell Access

- ❶ 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>
- ❷ Consult with VMware support representatives if you are unsure on the process.

3.4.4 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=displayKnowledgeArticle&externalId=8375637

3.4.5 Root Account

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

3.4.6 Port Requirement

- ❶ For environment with firewall, the vCenter, ESXi servers and Backup Client Computer must be able to communicate with each other.
- ❷ Ensure that ports 22, 80, 111, 443 and 902 allow outbound communication on the vCenter and ESXi servers. Refer to the links 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.

3.4.7 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.

3.4.8 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-consistent quiescing).

3.4.9 ESXi 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 hosts and compatible virtual machine hardware versions list \(2007240\)](#)

3.5 Backup Client Computer Requirements

In the following VMware setup:

- ▶ Standalone VMware ESXi Server
- ▶ VMware vCenter Server
 - ◉ Windows VMware vCenter Server
 - ◉ VMware vCenter Server Appliance (vCSA)

For backup of virtual machines on VMware vCenter/ESXi Server, it is recommended a separate Backup Client Computer (staging machine) must be prepared for AhsayOBM to be installed on.

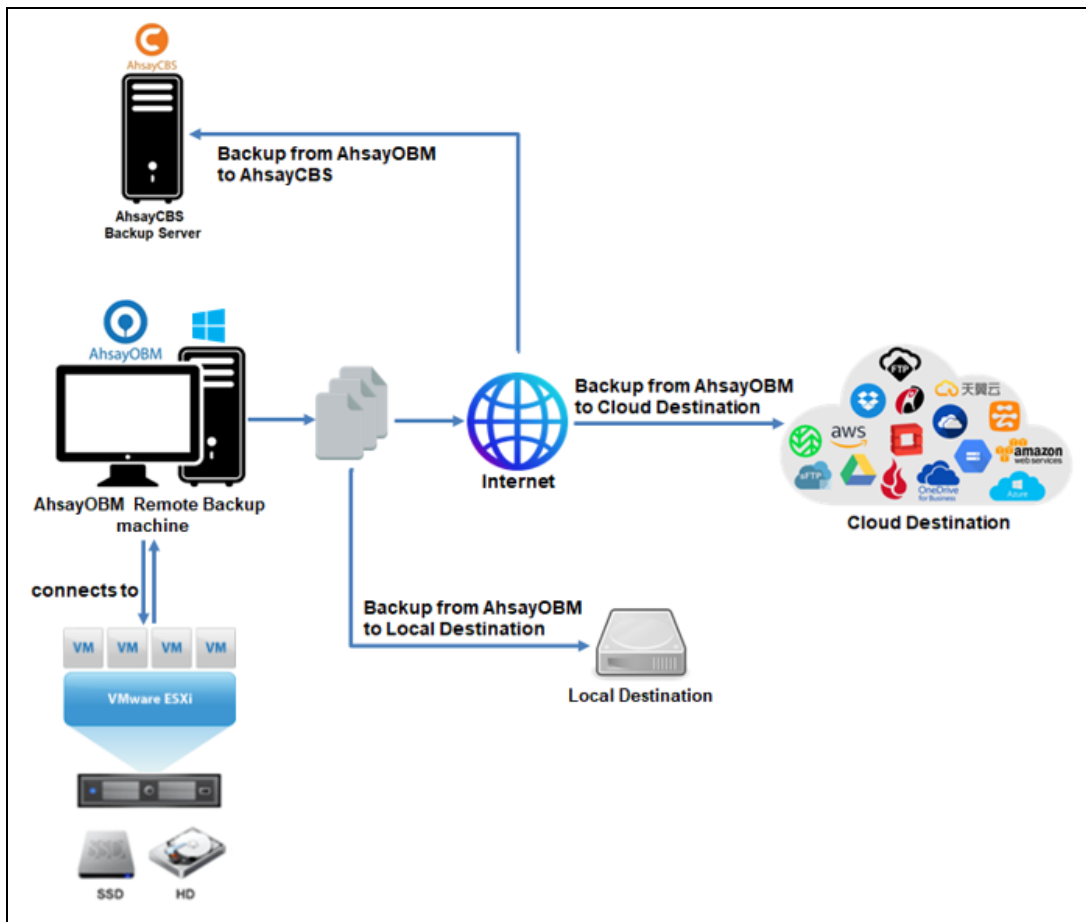
AhsayOBM installed on a Windows machine will allow support for VDDK backup mode, Run Direct, Granular Restore and vSAN Cluster.

However, for Standalone VMware ESXi Server and VMware vCenter Server Appliance (vCSA), AhsayOBM can be installed on either a Linux (GUI) or MacOS machine but VDDK backup mode, Run Direct, Granular Restore and vSAN Cluster are not supported on these platforms.

IMPORTANT

AhsayOBM cannot be directly installed on a VMware ESXi server or VMware vCenter Server Appliance (vCSA).

AhsayOBM is installed on a remote backup machine which connects to the standalone VMware ESXi server. The backup is saved either on AhsayCBS, a local destination on the AhsayOBM remote backup machine or to a cloud destination.



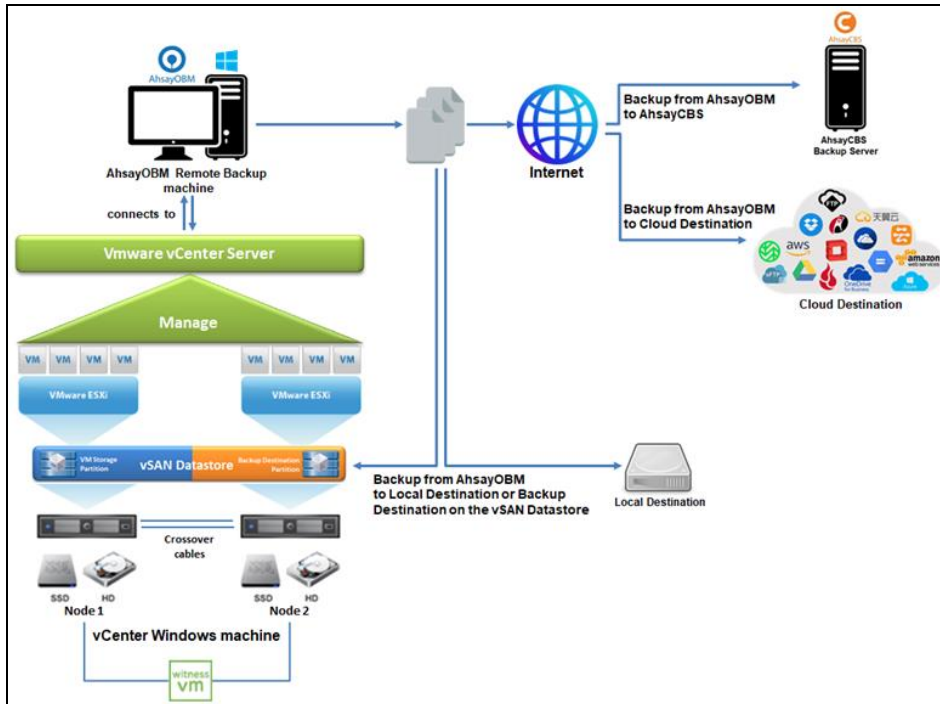
For environment with the following vSAN setups, the AhsayOBM setup and deployment for **Two Node** and **Standard vSAN Cluster** are similar as they both are on one site.

- [Two Node vSAN Cluster](#)
- [Standard vSAN Cluster](#)
- [Stretched vSAN Cluster](#)

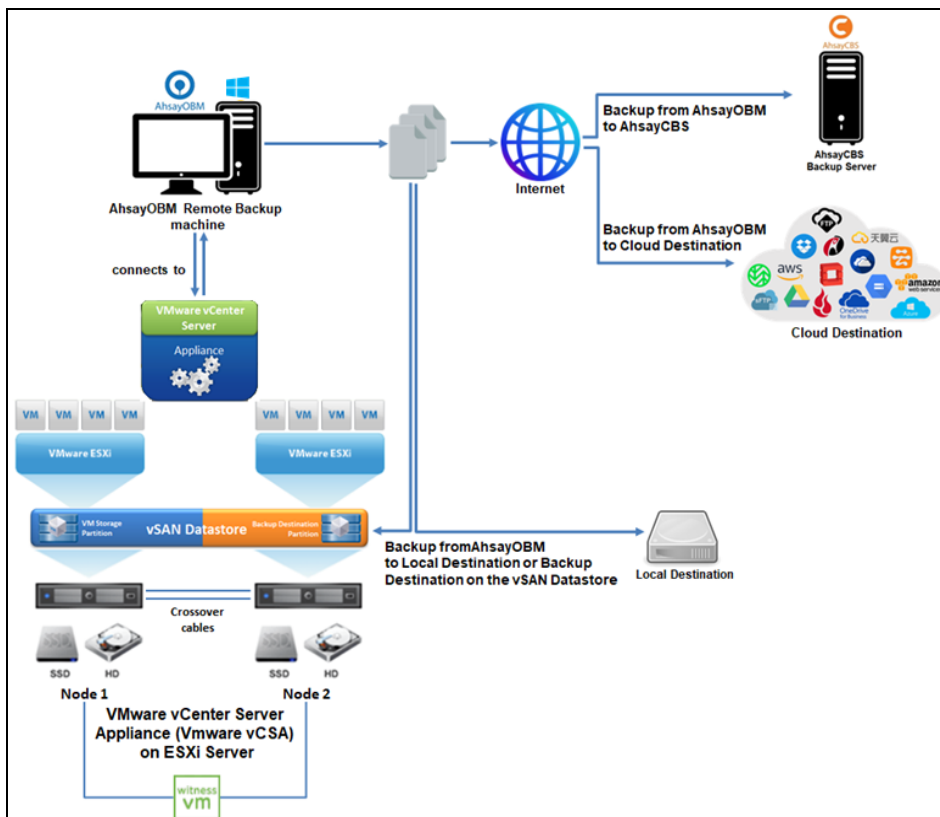
The following are the two different types of setups for each vSAN Cluster.

Two Node vSAN Cluster:

For environment with Windows vCenter Server with Two Node vSAN Cluster setup, a separate Backup Client Computer must be prepared for AhsayOBM to be installed on.

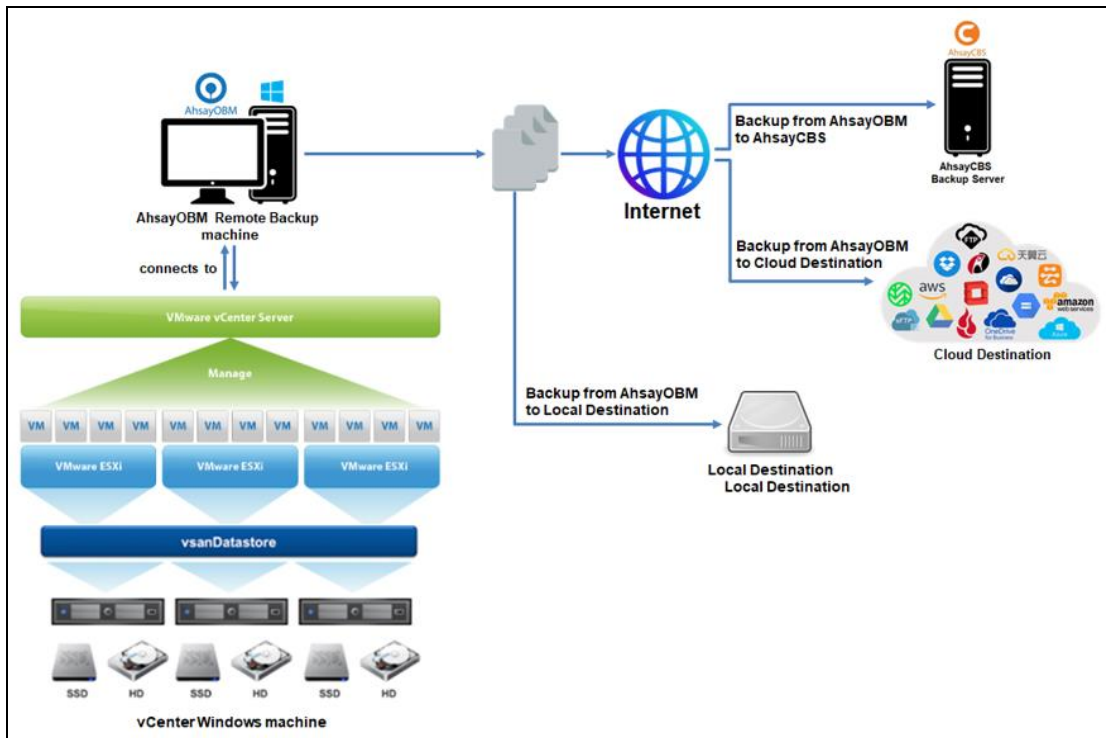


For VMware vCenter Server Appliance (vCSA) with Two Node vSAN Cluster setup, a separate Backup Client Computer must be prepared for AhsayOBM to be installed on.

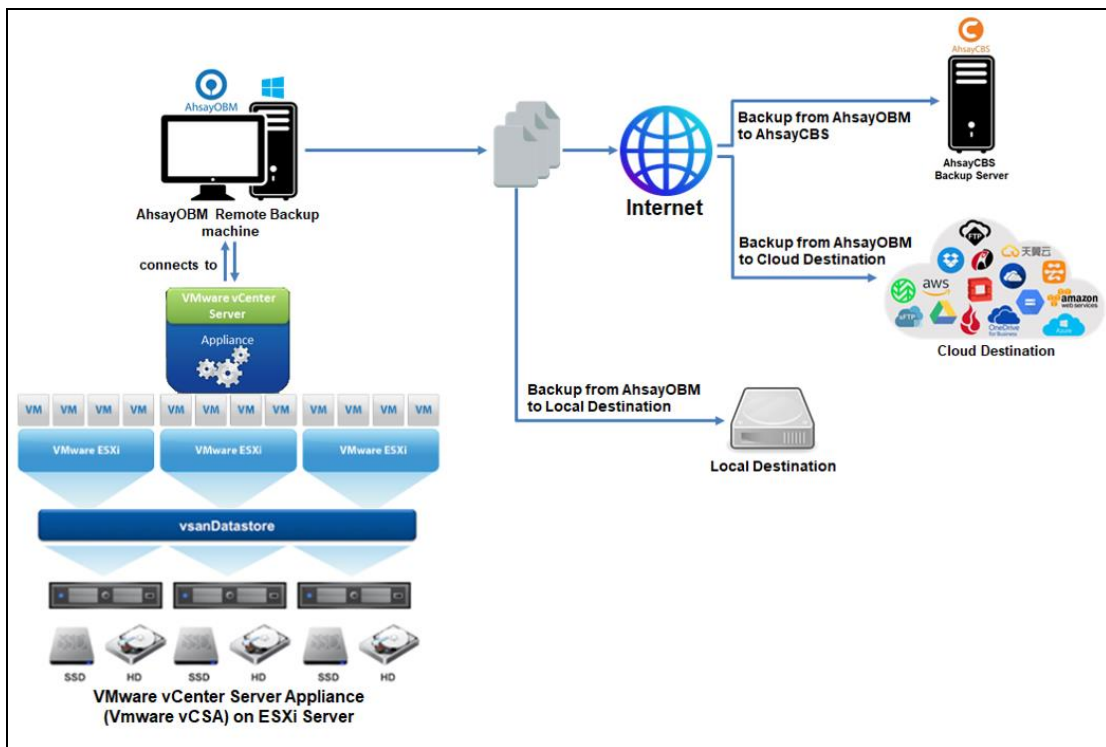


Standard vSAN Cluster:

For environment with Windows vCenter Server with Standard vSAN Cluster setup, a separate Backup Client Computer must be prepared for AhsayOBM to be installed on.

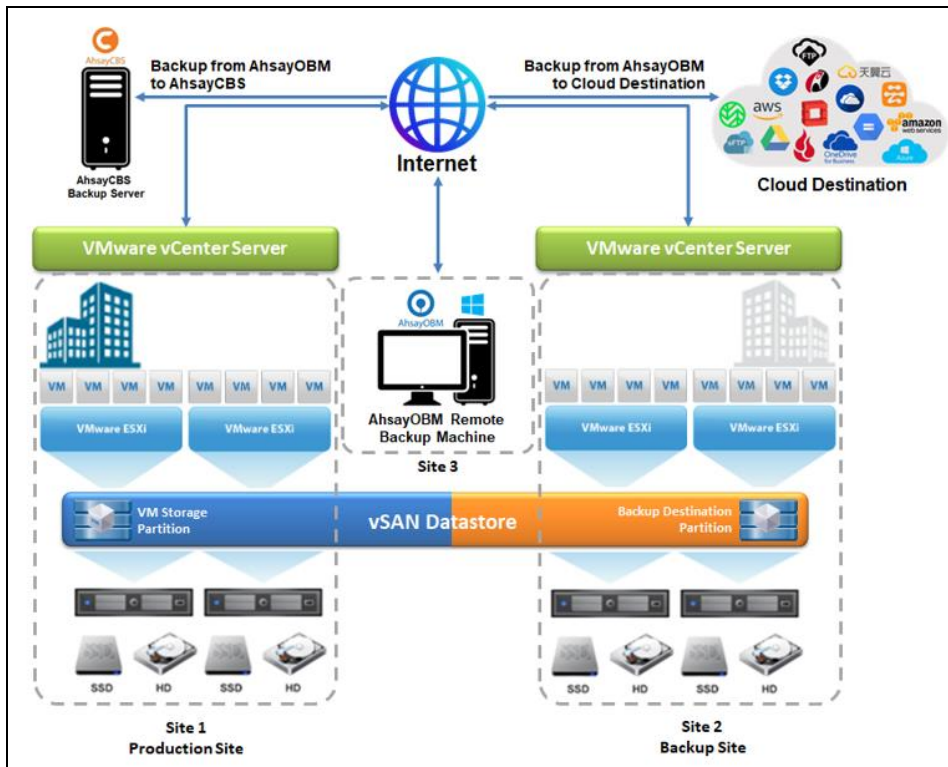


For VMware vCenter Server Appliance (vCSA) with Standard vSAN Cluster setup, a separate Backup Client Computer must be prepared for AhsayOBM to be installed on.

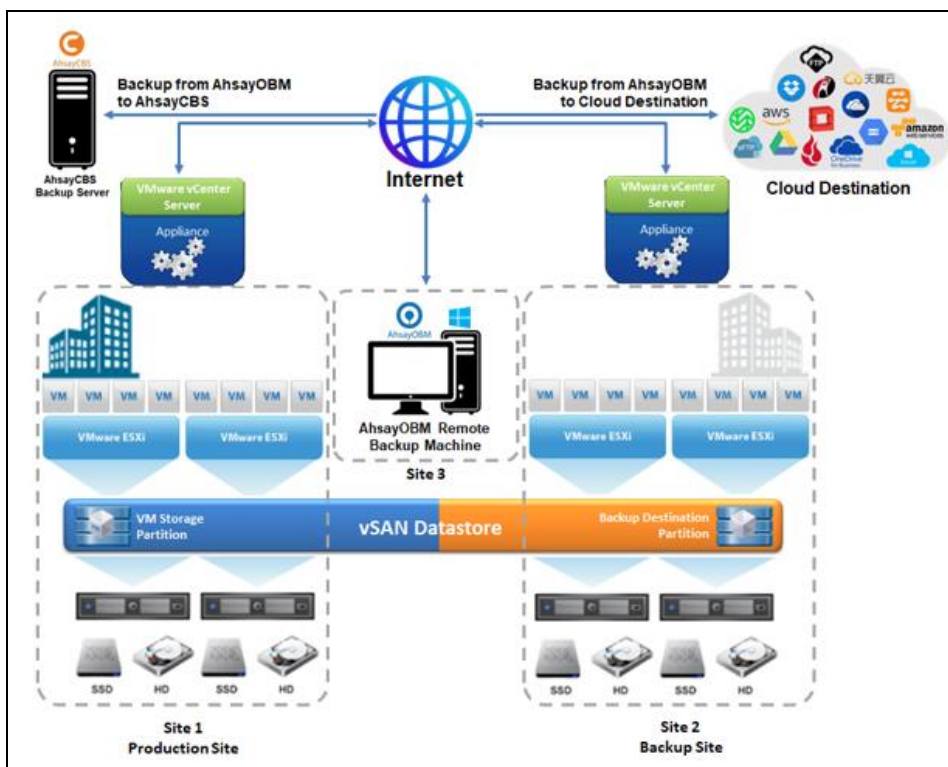


Stretched vSAN Cluster:

For environment with Windows vCenter Server with Stretched vSAN Cluster setup, a separate Backup Client Computer on a third location connected to the production site using internet connection must be prepared for AhsayOBM to be installed on.



For VMware vCenter Server Appliance (vCSA) with Stretched vSAN Cluster setup, a separate Backup Client Computer on a third location connected to the production site using internet connection must be prepared for AhsayOBM to be installed on.



3.5.1 Hardware and Software Requirement

Ensure that the **Hardware** and **Software Requirements** on [Chapter 3 Requirements](#) are met by the Backup Client Computer or the vCenter computer.

3.5.2 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 VM / socket license is assigned.

The screenshot shows the 'Backup Client Settings' tab in the AhsayOBM interface. The 'Backup Client' section is active, showing the 'AhsayOBM User' selected. Under 'Add-on Modules', the 'VMware' module is checked and highlighted with a red box. It shows 'Guest VM' as the license type and '10' as the count. Other modules like Microsoft Exchange Server, MySQL Database Server, Lotus Domino, Windows System Backup, Microsoft Exchange Mailbox, NAS - QNAP, Mobile (max. 10), Volume Shadow Copy, OpenDirect / Granular Restore, MariaDB Database Server, Microsoft SQL Server, Oracle Database Server, Lotus Notes, Windows System State Backup, Hyper-V, ShadowProtect System Backup, NAS - Synology, Continuous Data Protection, In-File DeltaOnly apply to v8 or before, Office 365 Backup, and Deduplication are also listed with their respective checkboxes and license counts.

There are 2 types of license models that you can choose from:

▶ Per Guest VM license

- ◉ VMware ESXi Standalone – calculated by the total number of guest VMs to back up
- ◉ VMware vCenter – calculated by the total number of guest VMs to back up

▶ Per Socket license

- ◉ VMware ESXi Standalone – calculated based on the total number of physical CPU or sockets for the ESXi machine
- ◉ VMware vCenter – calculated based on the total number of physical CPU or sockets for all VMware ESXi machines under the vCenter environment

To decide which license model is best for you, you must determine the total number of VMs and/or physical CPU that you will be using. Consider the following scenarios:

- ▶ You have 1 physical CPU in the ESXi machine with 20 VMs. In this scenario, it would be best to use the per socket license since you will only need 1 license for the physical CPU versus the 20 licenses if you will use the per guest VM license.

- You have 10 physical CPUs under a vCenter environment but only have 5 VMs running. In this case, a per guest VM license would be better than the per socket license.

It depends on the situation that will determine which license model is best to use. Keep in mind to also include your future plans regarding your VMware backup when deciding about which license to use. Contact your backup service provider for more details.

3.5.3 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.

3.5.4 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 links 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.

3.5.5 Backup Client Computer on Linux

For Backup Client Computer running on Linux operating system platform, the Graphical User Interface (GUI) environment (e.g. GNOME or KDE) must be installed to support selection of guest VMs in backup source.

IMPORTANT

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

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

Sufficient disk space must be allocated on the Backup Client Computer (or the Windows vCenter server if AhsayOBM is installed on this machine) for the temporary directory configured for the backup set, and the formula for the calculation of disk space is as follows:

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

NOTE

The calculation is based on the current guest VM size, and it does not consider 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.

3.5.7 Windows OS Requirement for VDDK Mode

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.
- For VMware vCenter/ESXi 7 or above, AhsayOBM must be installed on Windows version: Windows 2012 / Windows 2012 R2 / Windows 2016 (including versions 1709 and 1803) / Windows 2019.

3.6 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 [Instant VM Restore with Run Direct](#).

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

3.6.1 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.

3.6.2 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**

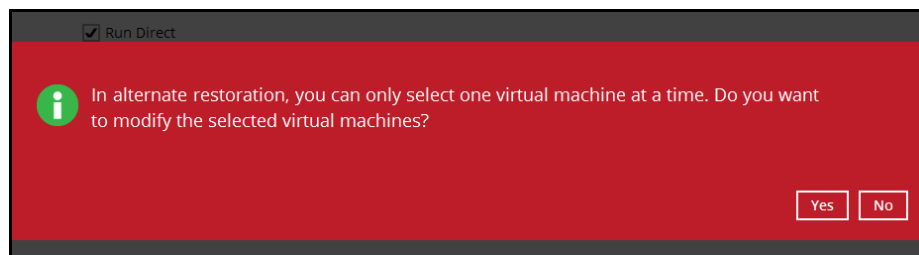
- When performing a Run Direct restore to **Alternate Location**, only one VM can be selected per restore session.



Restore virtual machines to

☐ Original location

☒ Alternate location



☒ Run Direct

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

Yes No

- Consider creating a 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.

3.7 VDDK Backup Mode Requirements

AhsayOBM supports VDDK backup mode (Virtual Disk Development Kit) for ESXi and vCenter setup. The backup speed is enhanced as the generation of the delta file of the VM are performed directly by the 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 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 as VDDK backup mode is only supported on Windows platform.

3.7.1 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 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"."

3.7.2 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 vSAN volume, VMFS volume backed by SAN, iSCSI, local disk, or an 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.

WARNING

Once you run the AhsayOBM CBT enabled backup job on a VM with VMware CBT setting enabled, going forward you should not disable VMware CBT. The backup will fail if you disable CBT from VMware, even though AhsayOBM CBT setting is enabled.

3.7.3 VMware CBT Known Issues

Although AhsayOBM v8.3.4.0 or above no longer supports the creation of new VMware backup set for VMware vCenter/ESXi v5.0 and v5.1, backup sets which are upgraded from the previous AhsayOBM versions can continue to run with applicable fix.

For VMware vCenter/ESXi v5.0, v5.1, v5.5 and v6.0, there is a known Changed Block Tracking (CBT) bug which can sometimes return incorrect changed sectors on a guest VM. As the CBT is used by the AhsayOBM for VDDK backup modes, it affects the integrity of both incremental and differential backups.

NOTE

For VMware vCenter/ESXi 5.0, v5.1, and v5.5, refer to <https://kb.vmware.com/s/article/2090639>.

For VMware vCenter/ESXi v6.0, refer to <https://kb.vmware.com/s/article/2136854>.

If a VMware backup is performed on any of the affected versions (i.e. v5.0, v5.1, v5.5 and v6.0), even if it was upgraded to a later version, it will be impossible for the AhsayOBM to restore the guest VMs due to the CBT bug, even though all backup jobs are recorded as successful by the AhsayOBM.

As part of the backup job, AhsayOBM will automatically check if the VMware version is affected by the VMware CBT bug. If the problematic VMware version detected is related to the affected version (i.e. v5.0, v5.1, v5.5 and v6.0), then the AhsayOBM will show a warning in the backup report indicating that the VMware host is affected by the CBT bug:

Backup Logs

No.	Type	Timestamp	Log
1	start	2020/09/07 17:08:13	Start [AhsayOBM v8.3.6.0]
2	info	2020/09/07 17:08:17	Using Temporary Directory D:\Temp\1599457814938\Local\1599457922832
3	info	2020/09/07 17:08:17	VMware ESXi 5.1.0 build-1157734@10.1.0.6:443SSH:22)
4	warn	2020/09/07 17:08:17	Current backup source includes ESXi server(s) which could sometimes return incorrect changed sectors (KB2090639). Please upgrade the following ESXi server(s) to the fixed build to avoid backup incorrect backup data: [Name:localhost.localdomain (VMware ESXi 5.1.0 build-1157734), FixedBuildNo:2323236]. Reference: VMware ESXi 5.0.x, 5.1.x and 5.5.x (https://kb.vmware.com/s/article/2090639) and VMware ESXi 6.0.x (https://kb.vmware.com/s/article/2136854)
5	info	2020/09/07 17:08:17	VMware Backup User Name: root
6	info	2020/09/07 17:08:20	Start running pre-commands
7	info	2020/09/07 17:08:20	Finished running pre-commands
8	info	2020/09/07 17:08:23	Download valid index files from backup job "Current" to "D:\Temp\1599457814938\Local\1599457922832\index".
9	info	2020/09/07 17:08:25	Backup host: 10.1.0.6
10	info	2020/09/07 17:11:06	Backup virtual machine (VDDK Mode): Arch Linux
11	info	2020/09/07 17:11:28	Spooling file "Arch Linux/Arch Linux.nvram"...
12	info	2020/09/07 17:11:30	Spooling file "Arch Linux/Arch Linux.vmsd"...
13	info	2020/09/07 17:11:31	Spooling file "Arch Linux/Arch Linux.vmx"...
14	info	2020/09/07 17:11:33	Spooling file "Arch Linux/Arch Linux.vmx"...
15	info	2020/09/07 17:11:35	Taking snapshot of virtual machine "Arch Linux"...
16	info	2020/09/07 17:11:37	Backup snapshot created successfully. Virtual Machine = "Arch Linux"
17	info	2020/09/07 17:31:52	Removing backup snapshot from virtual machine "Arch Linux"...
18	info	2020/09/07 17:31:52	Backup snapshot removed successfully. Virtual Machine = "Arch Linux"
19	info	2020/09/07 17:31:52	Backing up virtual machine "Arch Linux" Completed

Current backup source includes ESXi server(s) which could sometimes return incorrect changed sectors (KB2090639).

Please upgrade the following ESXi server(s) to the fixed build to avoid backup incorrect backup data: [Name:localhost.localdomain (VMware ESXi 5.1.0 build-1157734), FixedBuildNo:2323236]. Reference: VMware ESXi 5.0.x, 5.1.x and 5.5.x (<https://kb.vmware.com/s/article/2090639>) and VMware ESXi 6.0.x (<https://kb.vmware.com/s/article/2136854>)

To resolve this problem, it is strongly recommended to perform the following steps:

1. Apply the VMware patch or upgrade the VMware vCenter/ESXi.
2. Perform a full backup of the affected guest VMs.

3.7.4 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.

3.7.5 Virtual Machine State

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

3.7.6 File Name Requirement

If the file name of the virtual machine contains the following special characters, the 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>

3.7.7 Restore Requirement

For VMware ESXi restore, the virtual machine must be restored to a VMware ESXi host with the same VMFS datastore version.

For example, the backup of the virtual machine was done on a VMware ESXi host with a **VMFS5 datastore** in VDDK backup mode but is restored to a VMware ESXi host using a **VMFS6 datastore** and vice versa.

NOTE

This limitation does not apply to VMware vCenter backup sets.

3.8 vSAN Backup and Restore

3.8.1 Requirements

For VMs using vSAN datastore here are the requirements:

- Supported vSAN setups for AhsayOBM v8.5.0.118 or above
 - Two Node vSAN Cluster
 - Standard vSAN Cluster
 - Stretched vSAN Cluster
- VMware vSAN version with corresponding vCenter and ESXi compatible version

vSAN version	vCenter version	ESXi version
5.5	5.5 or later	5.5 or later
6.0	6.0 or later	6.0 or later
6.1	6.0 or later	6.0 or later
6.2	6.0 or later	6.0 or later
6.5	6.5 or later	6.5 or later
6.6	6.5 or later	6.5 or later
6.6.1	6.5 or later	6.5 or later
6.7	6.7 or later	6.7 or later
7.0	7.0 or later	7.0 or later

- AhsayOBM must be installed on a supported Windows operating system as vSAN backup and restore is only supported on Windows platform.

Refer to the following article for the list of the supported Windows operating system:

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

- Backup set version must be VMware vCenter.

Create Backup Set

Name
vCenter 6.5 vSAN Backup Set

Backup set type
VMware Backup

Version
VMware vCenter 5.5 / 6 / 6.5 / 6.7 / 7.0

Username
administrator

Password
.....

Host
10.120.8.40

Port
443

- Only VDDK backup mode is supported for VMs in vSAN datastore.
- VMware vMotion must be enabled on the vCenter and ESXi servers for Run Direct to support live migration.
- For Stretched vSAN Cluster, the AhsayOBM staging machine must be located on another site aside from the VMware Center production and backup sites.

3.8.2 Limitations

- Backup and restore of guest VMs on a Stretched vSAN Cluster will be slower since it will be dependent on the internet connection between the AhsayOBM staging machine and the VMware vCenter server compared with a non-Stretched vSAN Cluster backup and restore which is using a LAN connection.
- Run Direct restore may not be possible for Stretched vSAN Cluster since AhsayOBM is located on another site.

The VMware vCenter server will have to power on and manage the VM, which is stored on a backup destination on the AhsayOBM staging machine through an internet connection.

4 Best Practices and Recommendations

Please consider the following recommendations:

- Use the latest version of AhsayOBM (v9.1 or above).

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

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

<https://www.ahsay.com/rss/technical-updates.rss>

- 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).

It is highly recommended to set the temporary directory folder to another location with sufficient free disk space other than Drive C: (e.g. Drive E:).

- 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 storing 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 VM can be restored from another location.

- Consider increasing the Java memory allocation setting for AhsayOBM (Java heap space) as more memory is required for in-file delta generation, which is performed by AhsayOBM, depending on the provisioned size of the guest VMs. A relatively large Java heap size may be required, i.e. 4GB, 6GB, 8GB etc.

If you are using Granular restore, it is recommended to increase the Java heap size space to at least 4GB or above for optimal performance.

Refer to this link for more details about the modification of the java heap size setting for AhsayOBM:

[FAQ: How to modify the Java heap size setting of AhsayOBM / AhsayACB](#)

- It is highly recommended to back up the whole VM instead of individual disk for backup of virtual machine with snapshot.
- Consider performing routine recovery test to ensure your backup is setup and performed properly.
- Consider disabling 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)
- For backups using vCenter Server Appliance (vCSA) on VMware ESXi server, a separate Backup Client Computer must be prepared for the AhsayOBM to be installed on, which can connect to the vCenter Server Appliance (vCSA) through a LAN.
- Periodic Backup Schedule

The periodic backup schedule should be reviewed regularly to ensure that the interval is sufficient to handle the data volume on the machine. Over time, data usage pattern may

change on a production server, i.e. the number of new files created, the number of files which are updated/deleted, and new users may be added etc.

Consider the following key points to efficiently handle backup sets with periodic backup schedule.

- ◉ Hardware – to achieve optimal performance, compatible hardware requirements is a must. Ensure you have the backup machine's appropriate hardware specifications to accommodate frequency of backups,
 - so that the data is always backed up within the periodic backup interval
 - so that the backup frequency does not affect the performance of the production server
- ◉ Network – make sure to have enough network bandwidth to accommodate the volume of data within the backup interval.
- ◉ Retention Policy - also make sure to consider the Retention Policy settings and Retention Area storage management which can grow because of the changes in the backup data for each backup job.

5 Granular Restore Technology

5.1 What is Granular Restore Technology?

AhsayOBM Granular Restore Technology enables the recovery of individual files from a guest VM without booting up or restoring the whole guest VM first.

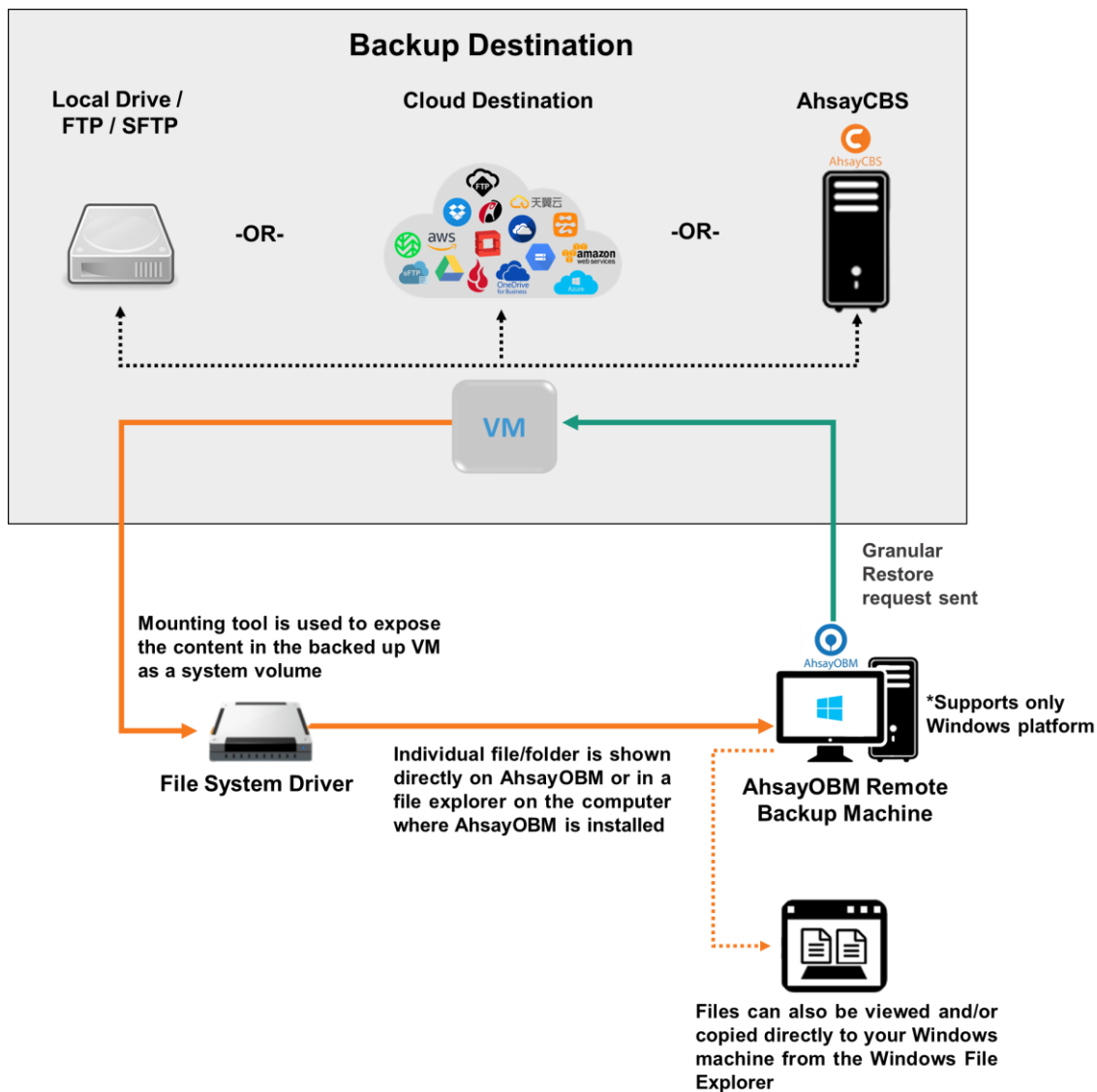
Granular restore is one of the available restore options for VMware ESXi/vCenter backup sets from AhsayOBM v8.1.0.0 or above. AhsayOBM makes use of Granular Restore technology to enable a file level restore from a virtual disk file (VDDK) of guest VM backup possible. It is particularly useful if you 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.

5.2 How does Granular Restore work?



5.3 Benefits of using Granular Restore

Comparison between Granular Restore and Traditional Restore.

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

5.4 Requirements

5.4.1 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.

5.4.2 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.

5.4.3 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.

5.4.4 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. Refer to the following article for the list of compatible operating system for Granular Restore:

[FAQ: Ahsay Software Compatibility List \(SCL\) for Granular and OpenDirect Restore on version 9.1 or above](#)

For VMware ESXi/vCenter 7 backups, AhsayOBM must be installed on the following Windows version:

Windows Server 2012	Windows Server 2019
Windows Server 2012 R2	Windows Server 2022
Windows 2016 (including versions 1709 and 1803)	

5.4.5 Temporary Directory Requirement

The temporary directory folder should have at least the same available size as the guest VM to be restored and should be located on a local drive to ensure optimal backup/restore performance.

5.4.6 Network Drive Requirements

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

5.4.7 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.

5.4.8 Network Requirements

The 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.

5.4.9 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/security-updates/securityadvisories/2015/3033929>

5.4.10 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.
- For Granular Restore (OpenDirect), it is required to log in as the real Windows administrator and not any other user with admin role or with elevated admin account permission. The real administrator account will be the one with the security identifier (SID) "**S-1-5-21domain-500**".

NOTE

For more information about security identifiers in Windows OS, refer to the following article:

<https://support.microsoft.com/en-us/help/243330/well-known-security-identifiers-in-windows-operating-systems>

5.5 Limitations

Enhanced Network Drive Support

- For network drives which have not been already setup or mapped in Windows.
- Temporary folder location is not supported with individual login credentials but can still be setup separately using existing Windows User Authentication login.
- It also does not support Pre-Backup and Post-Backup Commands.
- Not supported on "Restore Raw file" and "Restore to local computer" options.

6 Creating a VMware VM Backup Set

1. Log in to the AhsayOBM application user interface.

For instructions on how to log in, please refer to [Chapter 8](#) of the **AhsayOBM v9 Quick Start Guide for Windows**.

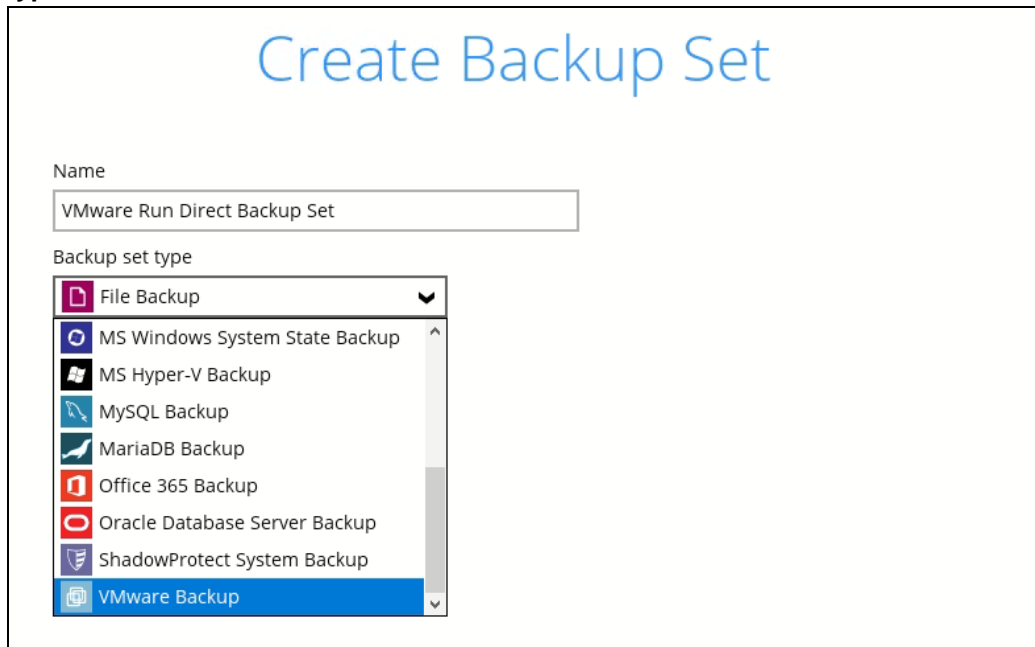
For Backup Client Computer on Linux, enter the following command to launch the application user interface:

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

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



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

A screenshot of the "Create Backup Set" form. The title "Create Backup Set" is at the top in blue. Below it, there is a "Name" label and a text input field containing "VMware Run Direct Backup Set". Underneath is a "Backup set type" label and a dropdown menu. The dropdown menu is open, showing a list of backup types: File Backup, MS Windows System State Backup, MS Hyper-V Backup, MySQL Backup, MariaDB Backup, Office 365 Backup, Oracle Database Server Backup, ShadowProtect System Backup, and VMware Backup. The "VMware Backup" option is highlighted in blue at the bottom of the list.

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

Create Backup Set

Name

Backup set type

Version

VMware ESXi 5.5 / 6 / 6.5 / 6.7 / 7.0

VMware ESXi 5.5 / 6 / 6.5 / 6.7 / 7.0

VMware Workstation 10 / 11 / VMware Workstation Pro 12 / 14 / 15 / 16

VMware Player 6 / 7 / VMware Workstation Player 12 / 14 / 15 / 16

VMware vCenter 5.5 / 6 / 6.5 / 6.7 / 7.0

Host Port

SSH Port

- Select **VMware ESXi 5.5 / 6 / 6.5 / 6.7 / 7.0** for a VMware ESXi backup set
- OR-
- Select **VMware vCenter 5.5 / 6 / 6.5 / 6.7 / 7.0** for a VMware vCenter backup set

NOTE

Refer to the following article for the list of compatible VMware platforms:

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

6. 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
VMware Run Direct Backup Set

Backup set type
VMware Backup

Version
VMware ESXi 5.5 / 6 / 6.5 / 6.7 / 7.0

Username
root

Password
•••••

Host
esxi_hostname

Port
443

SSH Port
22

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

Create Backup Set

Name
VMware Run Direct Backup Set

Backup set type
VMware Backup

Version
VMware vCenter 5.5 / 6 / 6.5 / 6.7 / 7.0

Username
Administrator

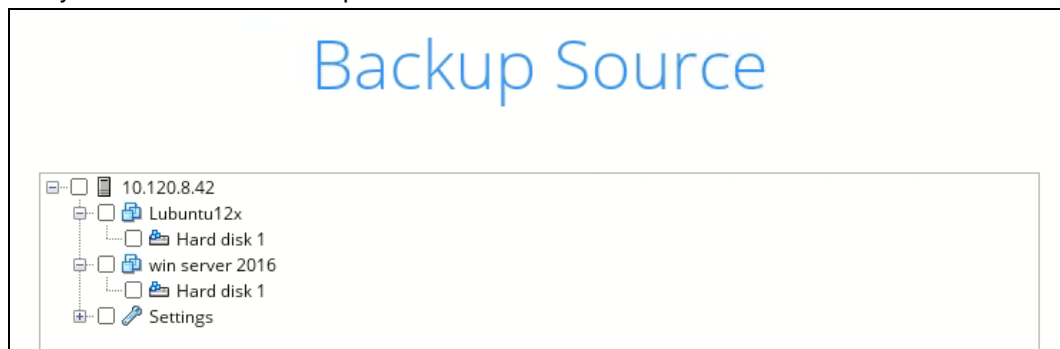
Password
•••••

Host
vCenter03-v6

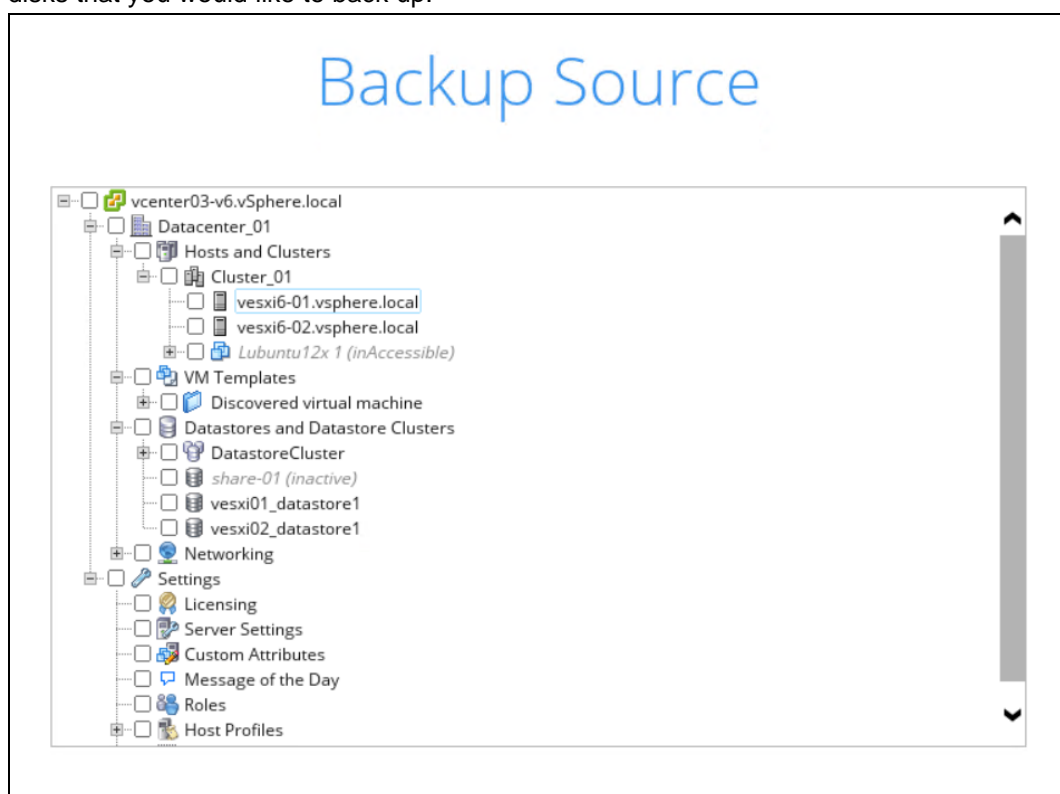
Port
443

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

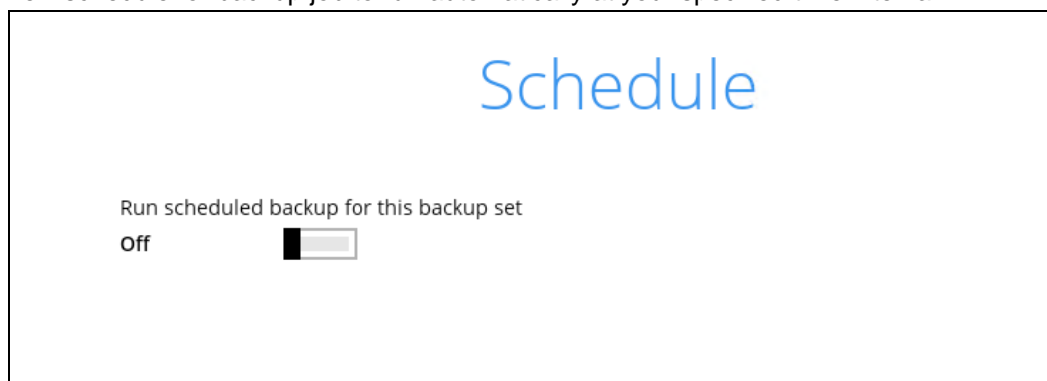
7. For VMware ESXi backup set, select the settings, virtual machines or individual virtual disks that you would like to back up.



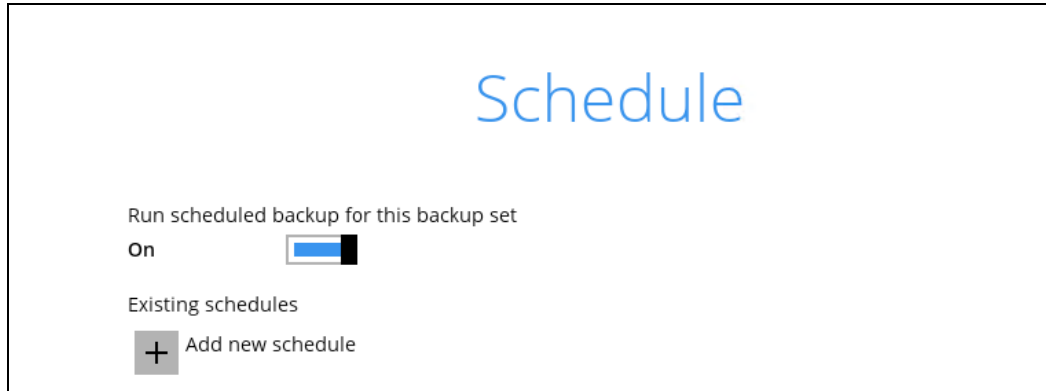
For a VMware vCenter backup set, select the settings, virtual machines or individual virtual disks that you would like to back up.



8. In the **Schedule** window, you may edit the existing backup schedule, or you may create a new schedule for backup job to run automatically at your specified time interval.



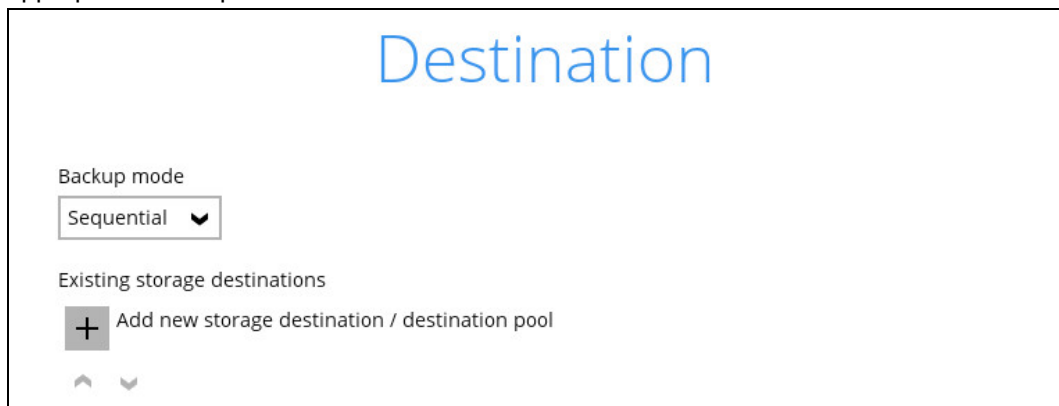
Click the “+” button to add a new schedule.



The 'Schedule' window displays the title 'Schedule' in blue. Below it, the text 'Run scheduled backup for this backup set' is followed by a toggle switch labeled 'On', which is currently turned on. Underneath, the text 'Existing schedules' is shown above a list area. At the bottom left of the list area is a grey button with a white plus sign and the text 'Add new schedule'.

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

9. In the **Destination** window, click the the **Backup mode** drop-down menu to select the appropriate backup mode.



The 'Destination' window displays the title 'Destination' in blue. Below it, the text 'Backup mode' is followed by a drop-down menu currently showing 'Sequential'. Underneath, the text 'Existing storage destinations' is shown above a list area. At the bottom left of the list area is a grey button with a white plus sign and the text 'Add new storage destination / destination pool'. Below this button are two small, faint upward and downward arrow icons.

- **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**.

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

To utilize the Run Direct feature for your VMs recovery, enable the **Run Direct** option (default). When the Run Direct option is enabled, the two supported Run Direct destinations are displayed.

New Storage Destination / Destination Pool

Name
AhsayCBS

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

Destination storage
AhsayCBS
AhsayCBS
Local / Mapped Drive / Network Drive / Removable Drive

To get a list of other available destinations, unselect the **Run Direct** option.

New Storage Destination / Destination Pool

Name
AhsayCBS

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

Destination storage
AhsayCBS
AhsayCBS
AmazonS3-Standard Infrequent
Local / Mapped Drive / Removable Drive
Wasabi
Backblaze
Google Cloud Storage
Google Drive
Rackspace

NOTE

- Further to the above settings, there are also other requirements for the Run Direct feature. Refer to the [Chapter 3.6 Run Direct Requirements](#) for more details.
- The actual number of available destinations may be different. Please contact your backup service provider for details.
- For more details on the Backup Destination, refer to the following article:
[FAQ: Frequently Asked Questions on Backup Destination](#)

If you have chosen the Local/Mapped Drive/Network Drive/Removable Drive option, you can change the **Name** of the storage. Click **Change** to browse to a directory path where the backup data will be stored. The path must be accessible to the VMware vCenter or ESXi host.

New Storage Destination / Destination Pool

Name

Local-1

Run Direct

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

Destination storage

Local / Mapped Drive / Network Drive / Removable Drive



Path (Input local / network address or click [Change])

Change

☐ This share requires access credentials

Test

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

11. You can add multiple storage destination if you wish. The backup data will be uploaded to all the storage 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

Local-1

C:\backup

AhsayCBS

Host: 10.3.121.17:80

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).

12. If you wish to enable the granular restore feature, make sure you turn on the **Granular Restore** switch in this menu. Refer to [Chapter 12 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.

NOTE

If you have enabled the Granular Restore or Run Direct restore feature, the backup data will not be compressed and encrypted to optimize the restore performance. Therefore, you can skip to **step 14**.

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 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.

13. 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

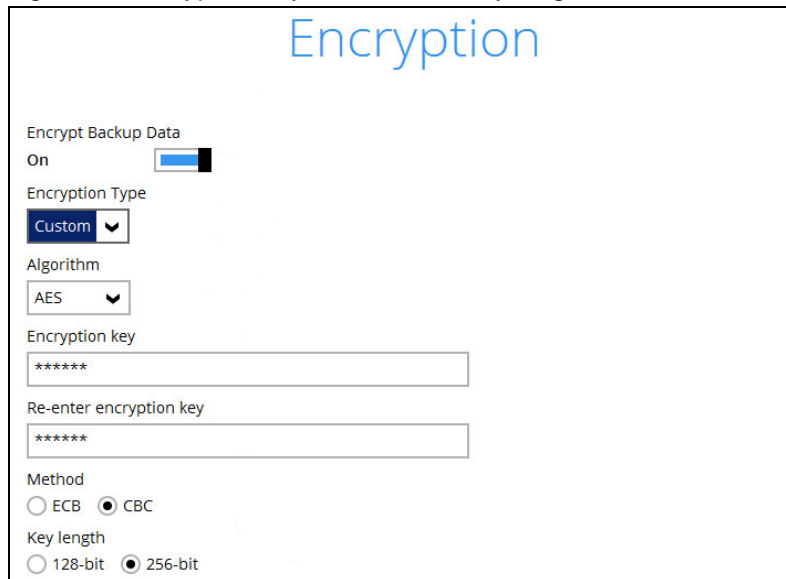
NOTE

For best practices on managing your encryption key, refer to the following article:

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

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

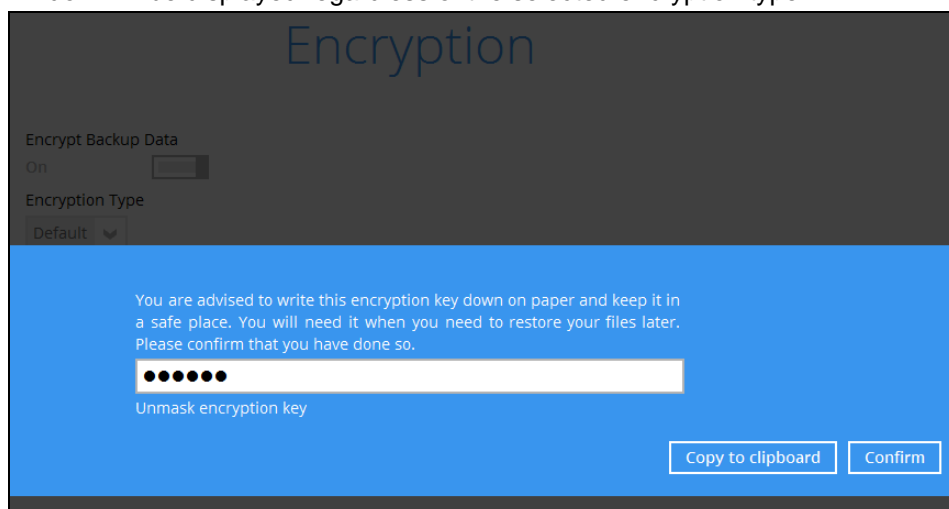
- **Default** – an encryption key with 44 alphanumeric characters will be randomly generated by the system
- **User password** – the encryption key will be the same as the login password of your AhsayOBM at the time when this backup set is created. Please be reminded that if you change the AhsayOBM login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



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

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

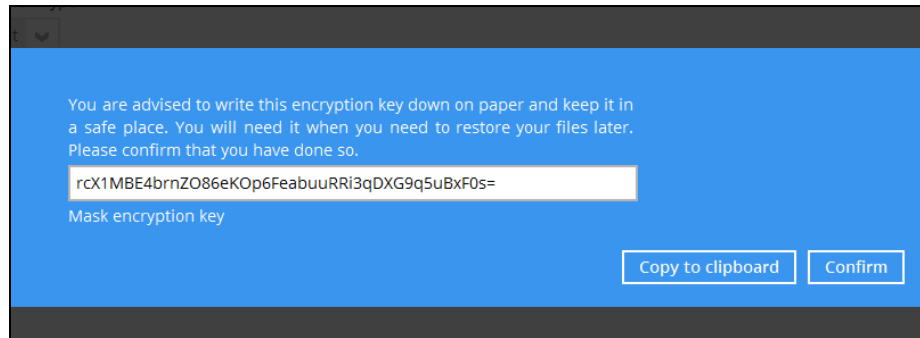
If you have enabled the Encryption Key feature in the previous step, the following pop-up window will be displayed regardless of the selected encryption type.



The screenshot shows a confirmation pop-up window titled 'Encryption'. The background is dark grey. The title 'Encryption' is in blue. Below it, the 'Encrypt Backup Data' toggle is set to 'On'. The 'Encryption Type' dropdown menu is set to 'Default'. The main content area has a blue background. It contains the text: 'You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.' Below this text is a text input field containing '*****'. Below the input field is the text 'Unmask encryption key'. At the bottom right, there are two buttons: 'Copy to clipboard' and 'Confirm'.

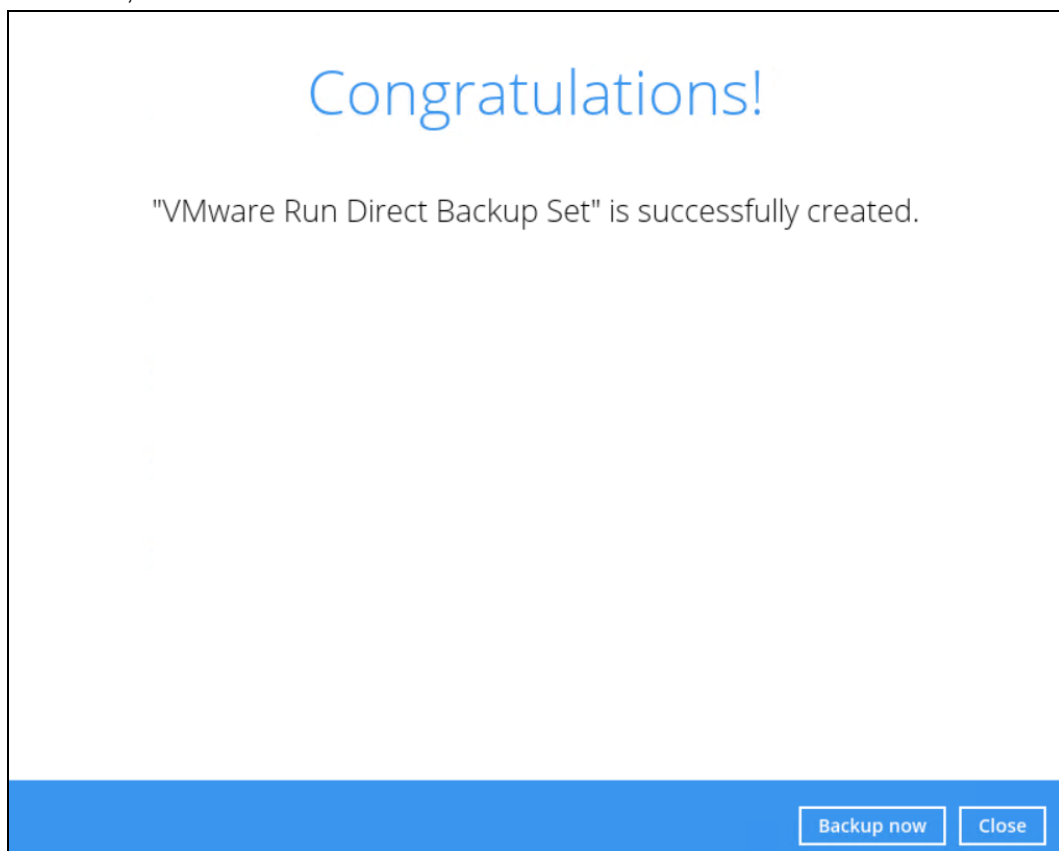
The pop-up window has the following three options to choose from:

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

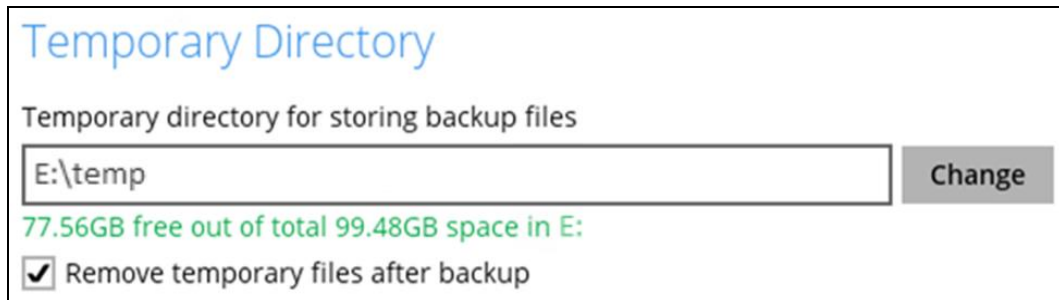


- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.
- **Confirm** – Click to exit this pop-up window and proceed to the next step.

14. Backup set created. Click **Backup now** if you wish to run a backup for this backup set. Otherwise, click the **Close** button.

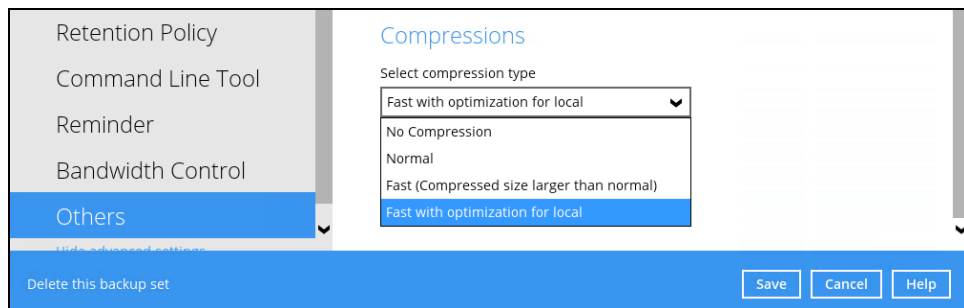


15. Based on [Best Practices and Recommendations](#), it is highly recommended to set the **temporary directory** to another location other than Drive C: (e.g. Drive E:). To do this, go to **Backup Sets > Others > Temporary Directory** and click the **Change** button to browse for another location.



16. Optional: Select your preferred **Compression** type. Go to **Others > Compressions**, then select from the following:

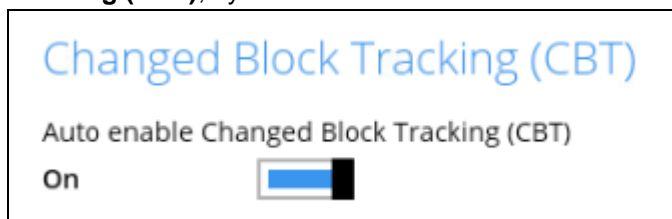
- No Compression
- Normal
- Fast (Compressed size larger than normal)
- Fast with optimization for local



NOTE

The Normal, Fast, or Fast with optimization for local compression types will not be applied to Run Direct enabled destinations.

17. Optional: Check if Changed Block Tracking is enabled. Go to **Others > Changed Block Tracking (CBT)**, by default it is enabled.



7 Running a Backup

7.1 Start a Manual Backup

The following steps are performed during a VMware VM backup job. For an overview of the detailed process for Steps 3, 5, 12, and 14, please refer to the following chapters of the **AhsayOBM v9 Quick Start Guide for Windows**.

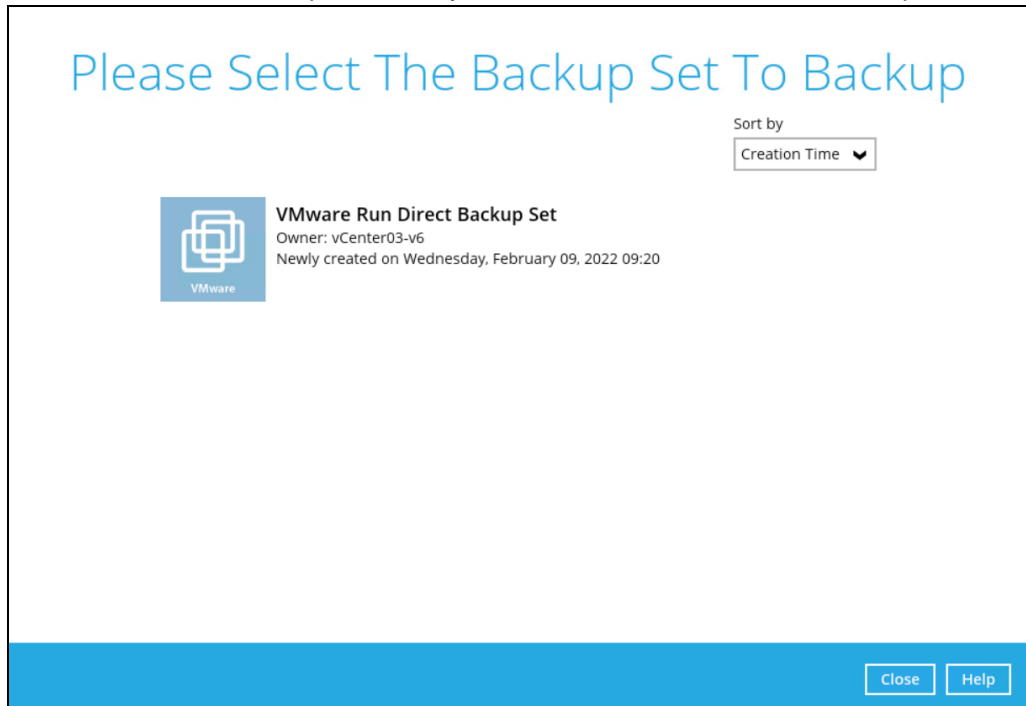
- ▶ Periodic Data Integrity Check (PDIC) Process (**Step 3**) – [Chapter 12.1](#)
- ▶ Backup Set Index Handling Process
 - Start Backup Job (**Step 5**) – [Chapter 12.2.1](#)
 - Completed Backup Job (**Step 14**) – [Chapter 12.2.2](#)
- ▶ Data Validation Check Process (**Step 12**) – [Chapter 12.3](#)



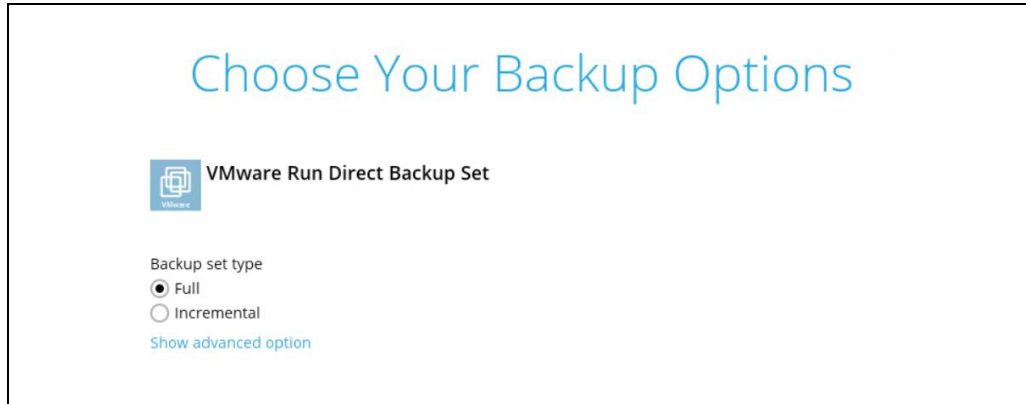
1. Click the **Backup** icon on the main interface of AhsayOBM.




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



3. Choose a backup set type (i.e., Full or Incremental).



Choose Your Backup Options

 VMware Run Direct Backup Set

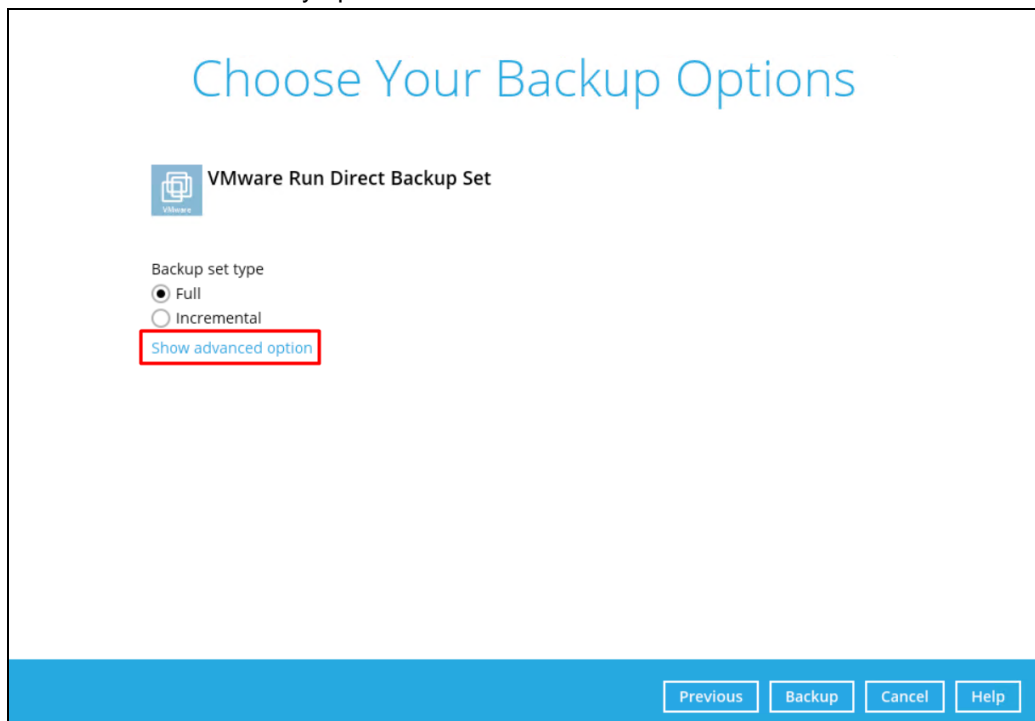
Backup set type

☒ Full


☐ Incremental

[Show advanced option](#)

- **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.
 - **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).
4. Click the **Show advanced option** in case you want to modify the Destinations, Migrate Data and Retention Policy options.



Choose Your Backup Options

 VMware Run Direct Backup Set

Backup set type

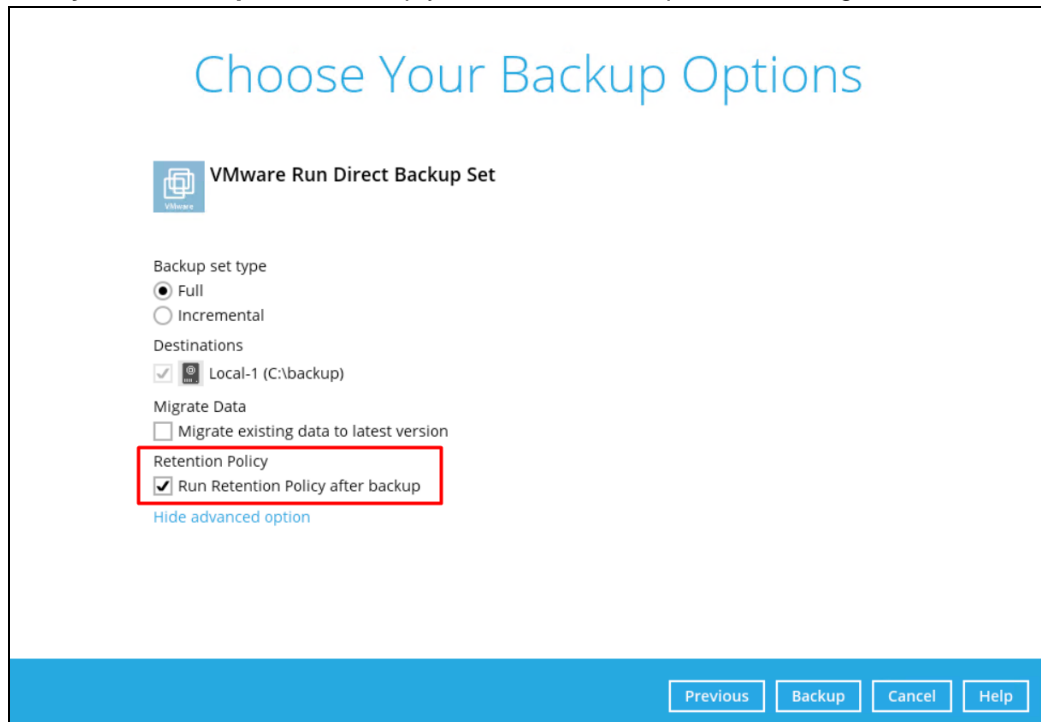
☒ Full

☐ Incremental

[Show advanced option](#)

[Previous](#) [Backup](#) [Cancel](#) [Help](#)

5. When the advanced options are shown, it is recommended to enable the **Run Retention Policy after backup**. This will help you save hard disk quota in the long run.



Choose Your Backup Options

VMware Run Direct Backup Set

Backup set type

☒ Full

☐ Incremental

Destinations

☒ Local-1 (C:\backup)

Migrate Data

☐ Migrate existing data to latest version

Retention Policy

☒ Run Retention Policy after backup

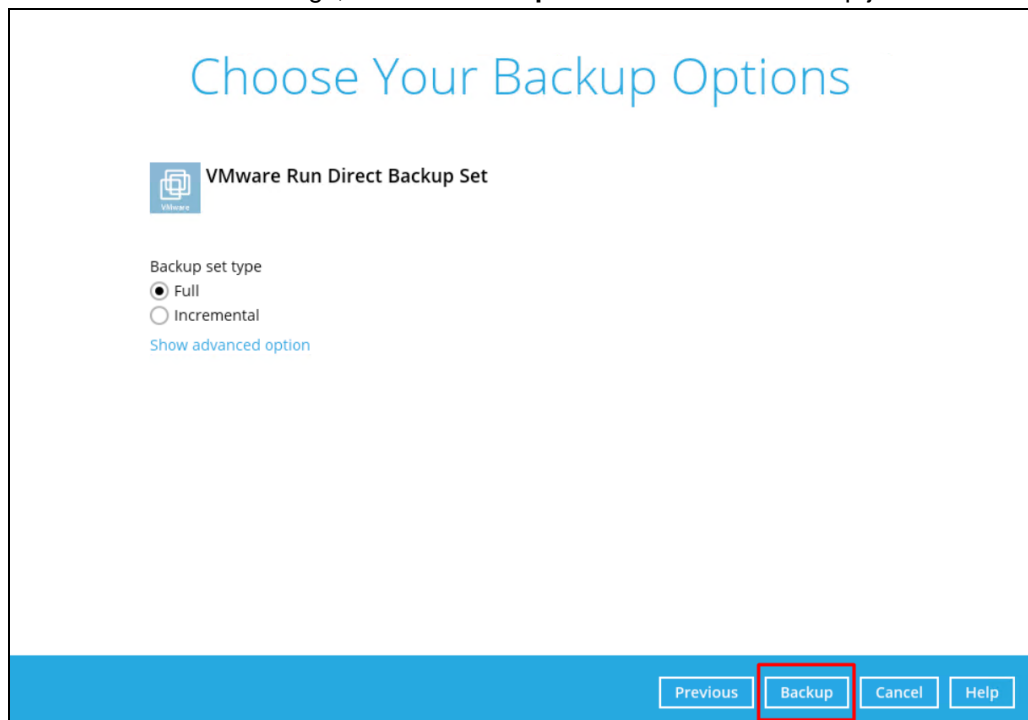
[Hide advanced option](#)

Previous Backup Cancel Help

NOTE

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

6. Once done with the settings, click the **Backup** button to start the backup job.



Choose Your Backup Options

VMware Run Direct Backup Set

Backup set type

☒ Full


☐ Incremental


[Show advanced option](#)

Previous Backup Cancel Help

7. The status of the backup job will be shown.

Backup

**VMware Run Direct Backup Set**

**Local-1 (C:\backup)**



[New File] 99-VMs/97373550-acf6-865a-ef28-afc787717276/1000_0/Lubuntu12x.2021-...

Estimated time left 3 min 47 sec (5.12GB)

Backed up 901.58MB (5 files, 7 directories, 1 link)


Elapsed time 2 min 18 sec

Transfer rate 192.94Mbit/s





Another way of checking the progress of the backup is from vSphere. The backup has started when a Snapshot of the VM was created.

Recent Tasks		Alarms						
Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time	Server	
Create virtual machine snapshot	Lubuntu12x	Completed	VSPHERE.LOCAL...	7 ms	03/11/2021, 5:36:36 PM	03/11/2021, 5:36:38 PM	vCenter05-v65	

8. The following screen will be displayed to indicate that the backup job is successfully completed. You may click the  button to check for the backup log.

Backup

**VMware Run Direct Backup Set**

**Local-1 (C:\backup)**


Backup Completed Successfully

Estimated time left 0 sec

Backed up 6.00GB (6 files, 7 directories, 1 link)

Elapsed time 7 min 21 sec

Transfer rate 120.81Mbit/s



Show All

Type	Log	Time
1	Start [AhsayOBM v9.1.0.0]	02/09/2022 14:00:54
1	Saving encrypted backup set encryption keys to server...	02/09/2022 14:00:54
1	Start Backup ... Full [Deduplication: enabled, Deduplication scope: All files within the same backup set, Migrate Delta...	02/09/2022 14:00:57
1	Using Temporary Directory C:\Users\Administrator\obm\temp\1644385928819\Local@1644386009953	02/09/2022 14:00:57
1	VMware vCenter Server 6.0.0 build-9313458@vCenter03-v6:443	02/09/2022 14:00:58
1	VMware Backup User Name: Administrator	02/09/2022 14:00:58
1	Start running pre-commands	02/09/2022 14:00:58
1	Finished running pre-commands	02/09/2022 14:00:58
1	Downloading server file list...	02/09/2022 14:00:58
1	Downloading server file list... Completed	02/09/2022 14:00:58
1	Backup host: vCenter03-v6	02/09/2022 14:01:00
1	Reading backup source from hard disk...	02/09/2022 14:01:07
1	Reading backup source from hard disk... Completed	02/09/2022 14:01:07
1	[New Directory]... 01-Datacenters	02/09/2022 14:01:08
1	[New Directory]... 01-Datacenters/02-Datacenter_01	02/09/2022 14:01:08
1	[New Directory]... 01-Datacenters/50-Settings	02/09/2022 14:01:08
1	[New Directory]... 01-Datacenters/02-Datacenter_01/10-host	02/09/2022 14:01:08
1	[New Directory]... 01-Datacenters/02-Datacenter_01/20-vm	02/09/2022 14:01:08
1	[New Directory]... 01-Datacenters/02-Datacenter_01/30-datastore	02/09/2022 14:01:08
1	[New Directory]... 01-Datacenters/02-Datacenter_01/40-network	02/09/2022 14:01:08

Logs per page 50


Page 1 / 2

Close

Close

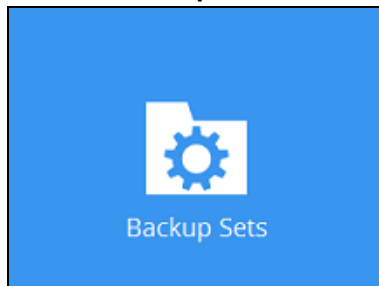
Help

From vSphere, the Snapshot of the VM will be removed when the backup is completed.

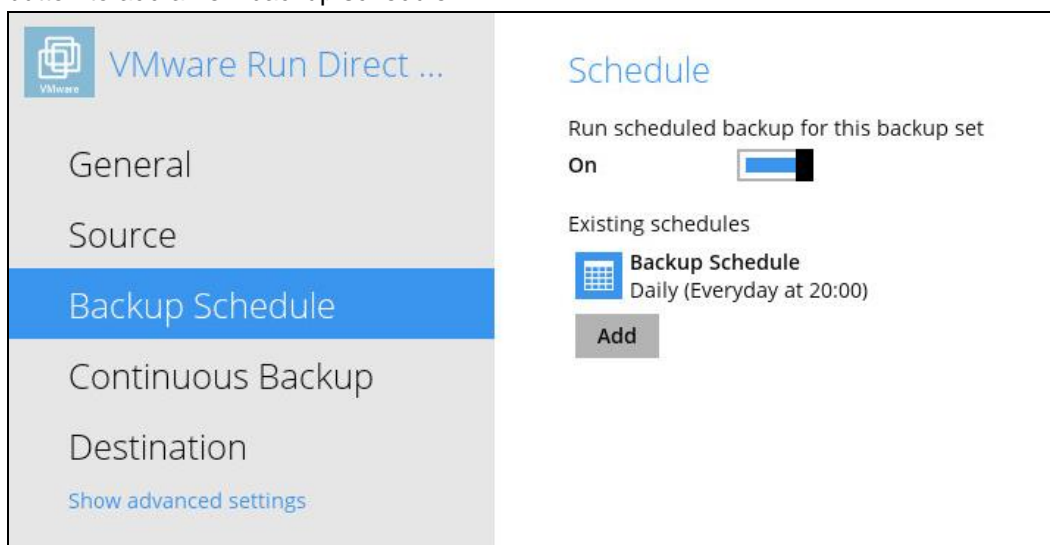
Recent Tasks		Alarms						
Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time	Server	
Remove snapshot	 Ubuntu12x	✓ Completed	VSPHERE.LOCAL...	23 ms	03/11/2021, 5:42:17 PM	03/11/2021, 5:42:19 PM	vCenter05-v65	

7.2 Configure Backup Schedule for Automated Backup

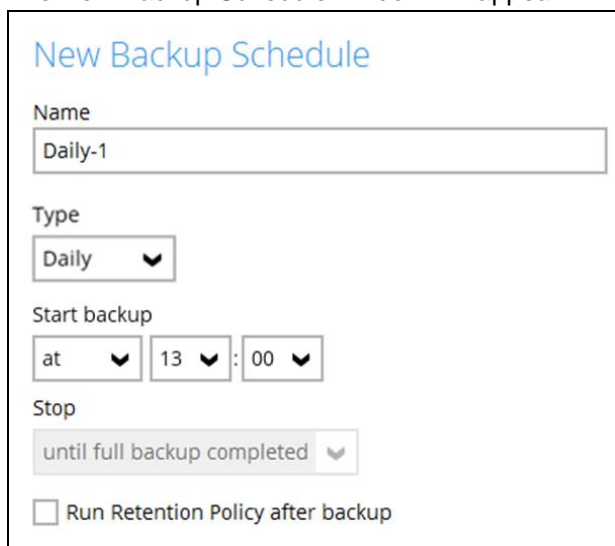
1. Click the **Backup Sets** icon on the AhsayOBM main interface.



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 schedule will be listed if there is any. Click the **Add** button to add a new backup schedule.



4. The New Backup Schedule window will appear.



New Backup Schedule

Name
Daily-1

Type
Daily

Start backup
at 13:00

Stop
until full backup completed

☐ Run Retention Policy after backup

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

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

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

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

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

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

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

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

New Backup Schedule

Name
Monthly-1

Type
Monthly

Backup on the following day every month

☒ Day Last

☐ First Sunday

Start backup at
23 : 00 on the selected days

Stop
until full backup completed

☒ Run Retention Policy after backup

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

New Backup Schedule

Name
Custom-1

Type
Custom

Backup on the following day once

2020 June 31

Start backup at
23 : 59

Stop
until full backup completed

☒ Run Retention Policy after backup

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

Start backup
every 1 minute

Stop
until full backup completed

☐ Run Retention Policy after backup

1 minute
2 minutes
3 minutes
4 minutes
5 minutes
6 minutes
10 minutes
12 minutes

Start backup
every 1 minute

Stop
until full backup completed

☐ Run Retention Policy after backup

30 minutes
1 hour
2 hours
3 hours
4 hours
6 hours
8 hours
12 hours

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

New Backup Schedule

Name
Weekly-1

Type
Weekly

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

Start backup
every 4 hours

Stop
until full backup completed

☒ Run Retention Policy after backup

Figure 1.1

New Backup Schedule

Name
Weekly-2

Type
Weekly

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

Start backup
at 21:00

Stop
until full backup completed

☒ Run Retention Policy after backup

Figure 1.2

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

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

- ❏ **Stop** – the stop time of the backup job. This only applies to schedules with start backup “at” and is not supported for periodic backup schedule (start backup “every”)
- ❏ **until full backup completed** – this option will stop a backup job once it is complete. This is the configured stop time of the backup job by default.
- ❏ **after (defined no. of hrs.)** – this option will stop a backup job after a certain number of hours regardless of whether the backup job has completed or not. This can range from 1 to 24 hrs.

The number of hours must be enough to complete a backup of all files in the backup set. For small files in a backup, if the number of hours is not enough to back up all files, then the outstanding files will be backed up in the next backup job. However, if the backup set contains large files, this may result in partially backed up files.

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

The partially backed up data will have to be removed by running the Data Integrity Check.


As a general rule, it is recommended to review this setting regularly as the data size on the backup machine may grow over time.

- ❏ **Run Retention Policy after backup** – if enabled, the AhsayOBM will run a Retention Policy job to remove files from the backup destination(s) which have exceeded the Retention Policy after performing a backup job. To save hard disk quote in the long run, it is recommended to enable this option.





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


Schedule

Run scheduled backup for this backup set

On 

Existing schedules

-  **Daily-1**
Daily (Everyday at 15:41)
-  **Weekly-1**
Weekly - Saturday (Every week at 23:00)
-  **Monthly-1**
Monthly - The Last Day (Every month at 23:00)
-  **Custom-1**
Custom (07/01/2020 at 23:59)



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

8 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 [Chapter 12 Granular Restore](#).

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

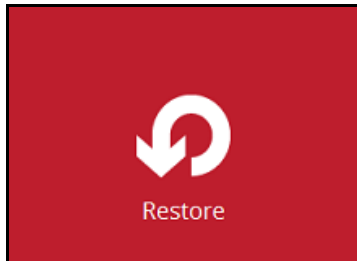
Cons

- No encryption and compression for backup set

9 Method 1 - Restoring a Virtual Machine with Run Direct

9.1 Running Direct Restore via AhsayOBM

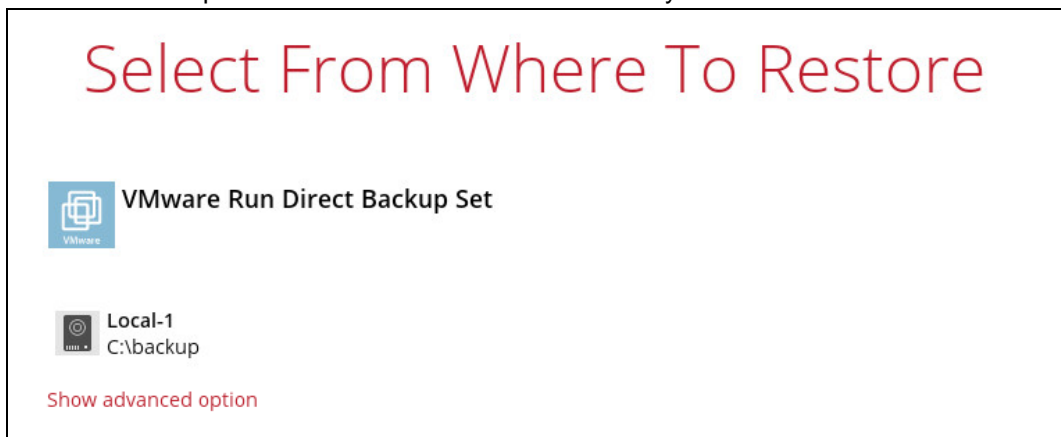
1. Click the **Restore** icon on the main interface of AhsayOBM.



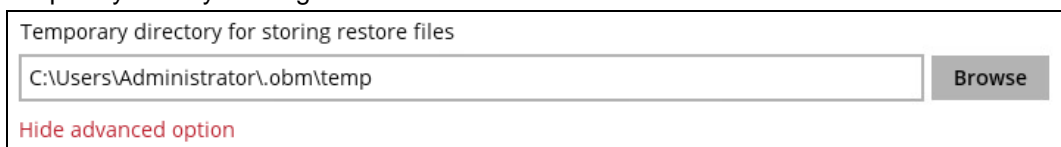
2. Select the backup set that you would like to restore the VM from.



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



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



4. If the Granular Restore is enabled in the backup set, the following screen will be displayed. Select the restore mode. Otherwise, proceed to the next step.

Please Choose A Restore Mode

Restore mode


☒ Restore virtual machines

☐ Restore individual files inside virtual machine (Granular Restore)

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

☐ Show backup job(s) outside retention

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

 All backup jobs will be shown, including the backup jobs which have been deleted. Some of the data may not be restorable. Do you wish to continue?

Yes No

6. 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 Restored

Select what to restore

Choose from files as of job Latest ☐ Show backup job(s) outside retention

Folders	Name	Size	Date modified
Local-1	Hard disk 1		
vCenter05-v65	Lubuntu12x.nvram	72KB	03/04/2021 16:13
Datacenter	Lubuntu12x.vmsd	0B	03/04/2021 10:41
Hosts and Clusters	Lubuntu12x.vmx	3KB	03/04/2021 16:13
10.16.8.42	Lubuntu12x.vmx	3KB	03/03/2021 16:39
Lubuntu			

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 [Restoring a VM in VMDK format](#).

7. 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).

Choose Where The Virtual Machines

Restore virtual machines to

☒ Original location

☐ Alternate location

☒ Run Direct

☒ 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

[Show advanced option](#)

8. 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:

Restore virtual machines to

☒ Original location

☐ Alternate location

☒ Run Direct

☐ 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

⦿ **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.

9. Click the **Show advanced option** if you would like to enable **Verify checksum of in-file delta files during restore**.

☒ Run Direct
☒ 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
[Show advanced option](#)

☐ Verify checksum of in-file delta files during restore
[Hide advanced option](#)

10. This step applies only for restoring to **Alternate location**. For restoring to **Original location**, skip to step 11.

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 / 6 / 6.5 / 6.7 / 7.0**, 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 / 6 / 6.5 / 6.7 / 7.0

Username
root

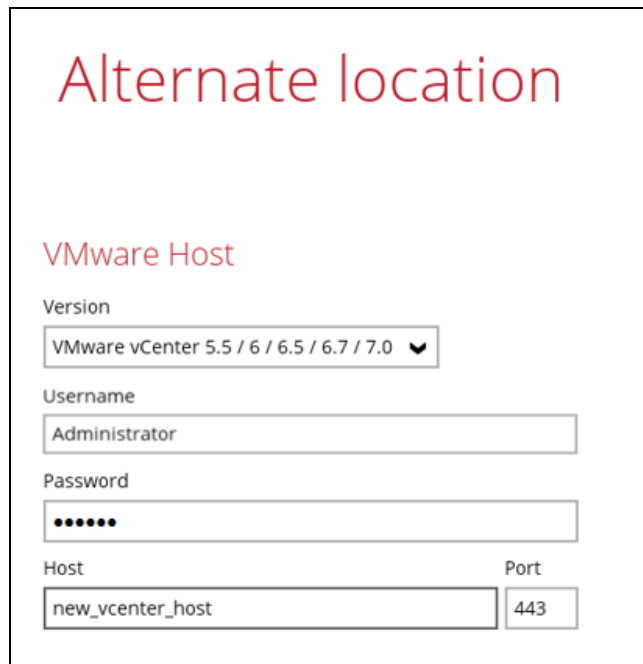
Password
.....

Host
10.120.8.45

Port
443

SSH Port
22

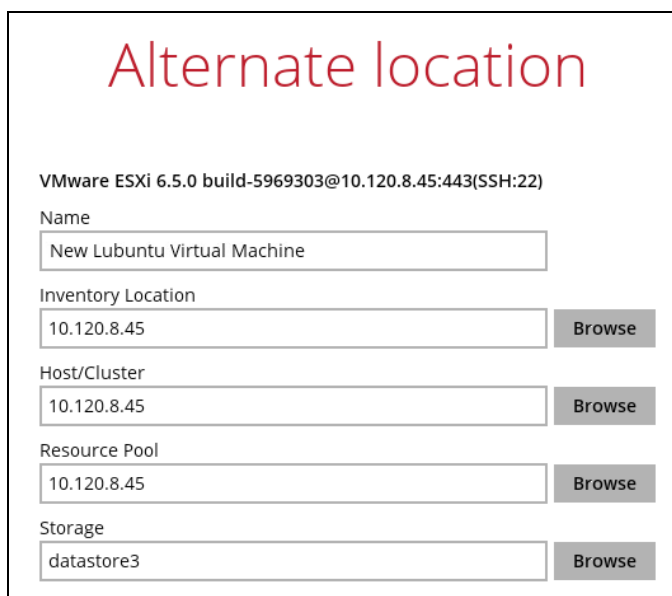
- For restoration to another VMware host (vCenter server), enter the **Username** and **Password** of the administrator account, **Host**, and **Port** information of the new / original vCenter server.



The screenshot shows a dialog box titled "Alternate location" in red. Below the title is a section header "VMware Host" in red. The form contains the following fields: "Version" with a dropdown menu showing "VMware vCenter 5.5 / 6 / 6.5 / 6.7 / 7.0"; "Username" with a text input field containing "Administrator"; "Password" with a text input field containing six dots; "Host" with a text input field containing "new_vcenter_host"; and "Port" with a text input field containing "443".

Click **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.



The screenshot shows a dialog box titled "Alternate location" in red. Below the title is the text "VMware ESXi 6.5.0 build-5969303@10.120.8.45:443(SSH:22)". The form contains the following fields: "Name" with a text input field containing "New Lubuntu Virtual Machine"; "Inventory Location" with a text input field containing "10.120.8.45" and a "Browse" button; "Host/Cluster" with a text input field containing "10.120.8.45" and a "Browse" button; "Resource Pool" with a text input field containing "10.120.8.45" and a "Browse" button; and "Storage" with a text input field containing "datastore3" and a "Browse" button.

Alternate location

VMware vCenter Server 6.5.0 build-5318154@10.16.8.40:443

Name

New Lubuntu Virtual Machine

Inventory Location

Datacenter

Browse

Host/Cluster

Datacenter/10.16.8.42

Browse

Resource Pool

Datacenter/10.16.8.42

Browse

Storage

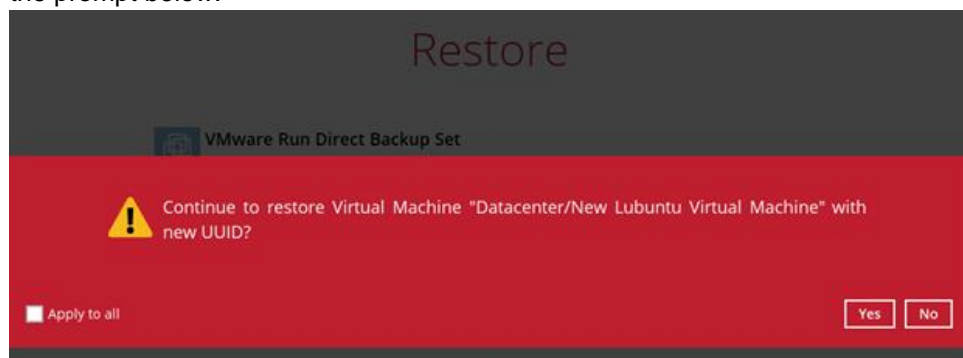
Datacenter/Datastore-SHR02 (1)

Browse

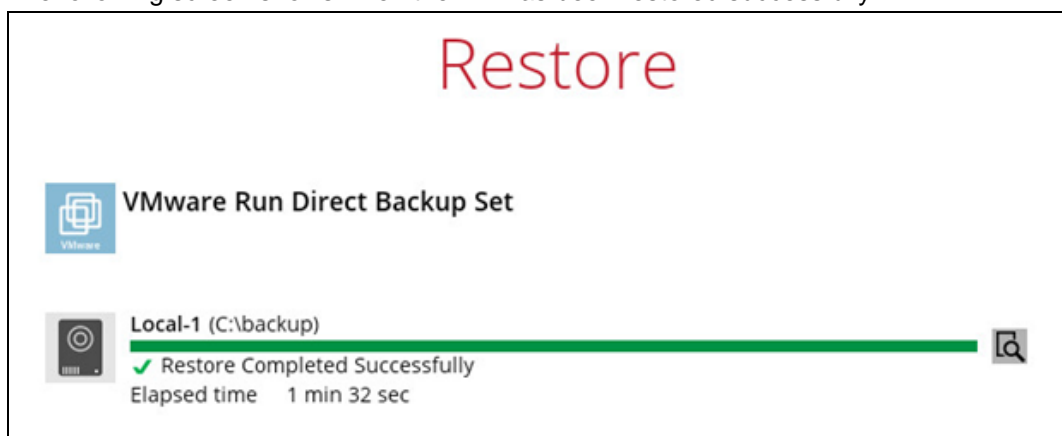
Click **Restore** to proceed when you are done with the settings.

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

- 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.



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



Another way of checking the progress of the restore is from vSphere. The restore has started when a NAS datastore was created, and it is completed when the virtual machine is powered on.

Recent Tasks		Alarms							
Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time	Server		
Create NAS datastore	10.16.8.42	✓ Completed	VSPHERE.LOCAL...	23 ms	03/11/2021, 5:52:47 PM	03/11/2021, 5:52:49 PM	vCenter05-v65		
Register virtual machine	Datacenter	✓ Completed	VSPHERE.LOCAL...	7 ms	03/11/2021, 5:52:51 PM	03/11/2021, 5:52:57 PM	vCenter05-v65		
Reload virtual machine	New Lubuntu...	✓ Completed	VSPHERE.LOCAL...	8 ms	03/11/2021, 5:52:57 PM	03/11/2021, 5:52:58 PM	vCenter05-v65		
Create virtual machine snapshot	New Lubuntu...	✓ Completed	VSPHERE.LOCAL...	6 ms	03/11/2021, 5:53:01 PM	03/11/2021, 5:53:04 PM	vCenter05-v65		
Power On virtual machine	New Lubuntu...	✓ Completed	VSPHERE.LOCAL...	7 ms	03/11/2021, 5:53:09 PM	03/11/2021, 5:53:18 PM	vCenter05-v65		

NOTE

In cases when Run Direct restore encounters an error or AhsayOBM crashes during a Run Direct restore, temporarily files are remained on the VMware Host. These temporary files must be manually cleaned. For instructions on how to do this, please refer to the [Appendix](#).

9.2 Verifying Run Direct Restore Connection

When a Run Direct restore is initiated, the following steps are taken at the backend.

Create NAS datastore

The backup destination is turned into a NFS (also known as NAS) datastore.

Mount VM on VMware Host

The NFS datastore is mounted on the VMware Host.

Create Virtual Machine Snapshot

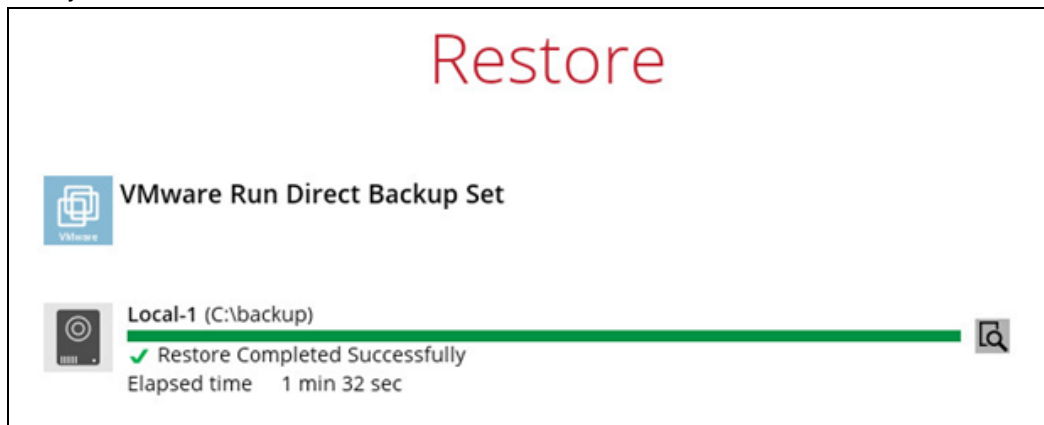
A snapshot of the virtual machine is created. All changes made while Run Direct is taking place will be stored temporarily in this snapshot, and the changes will not be committed to the virtual machine until a migration is done.

Power on Virtual Machine

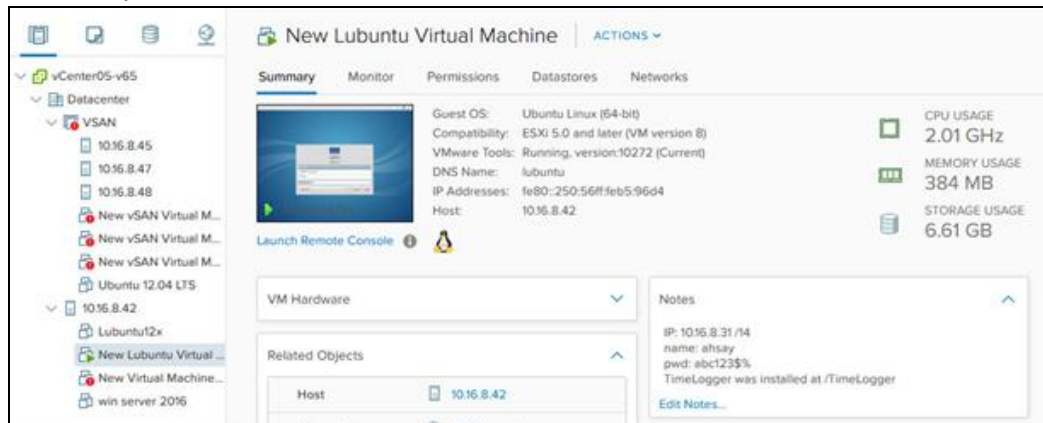
The virtual machine is being powered on so it can be run directly from the backup files.

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

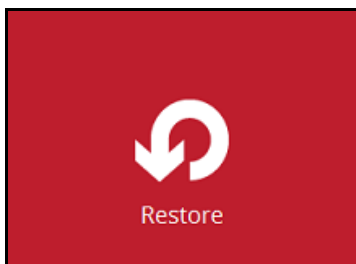
Do not exit from the AhsayOBM application when a Run Direct restored VM is still running. Run Direct must be stopped (e.g. by finalizing recovery of the VM or stopping the VM) before exiting AhsayOBM.

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.

9.3 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.



9.3.1 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.

Run Direct Virtual Machine

Source information

Backup set	VMware Run Direct Backup Set
Destination	Local-1
Job	Latest
From	Datacenter/Lubuntu12x
Creation Time	2021-03-11 17:53:20

Migration Information

VMware vCenter Server 6.5.0 build-5318154@10.16.8.40:443

Name
New Lubuntu Virtual Machine

Storage
Datacenter/Datastore-SHR02 (1) Browse

Stop Run Direct Previous Migrate Virtual Machine Cancel Help

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.

9.3.2 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.

Select Run Direct Virtual Machine

 **VMware Run Direct Backup Set**
New Lubuntu Virtual Machine (Datacenter/New Lubuntu Virtual Machine)

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

Run Direct Virtual Machine

Source information

Backup set	VMware Run Direct Backup Set
Destination	Local-1
Job	Latest
From	Datacenter/Lubuntu12x
Creation Time	2021-03-11 17:53:20

Migration Information

VMware vCenter Server 6.5.0 build-5318154@10.16.8.40:443

Name

Storage

[Stop Run Direct](#)

3. Click **Yes** to proceed.

 Stop Run Direct virtual machine?

NOTES

1. When the Auto Migrate option is selected, there will be no Stop Run Direct option available. As once the auto migration is completed, the guest VM will have been fully restored to the VMware Host and will be running and managed under the VMware Host environment. Therefore, the Run Direct VM instance will no longer exist as a result.
2. The "Stop Run Direct" link is only present if you run a Run Direct restore without auto migrate selected.

9.4 Run Direct Restore via User Web Console

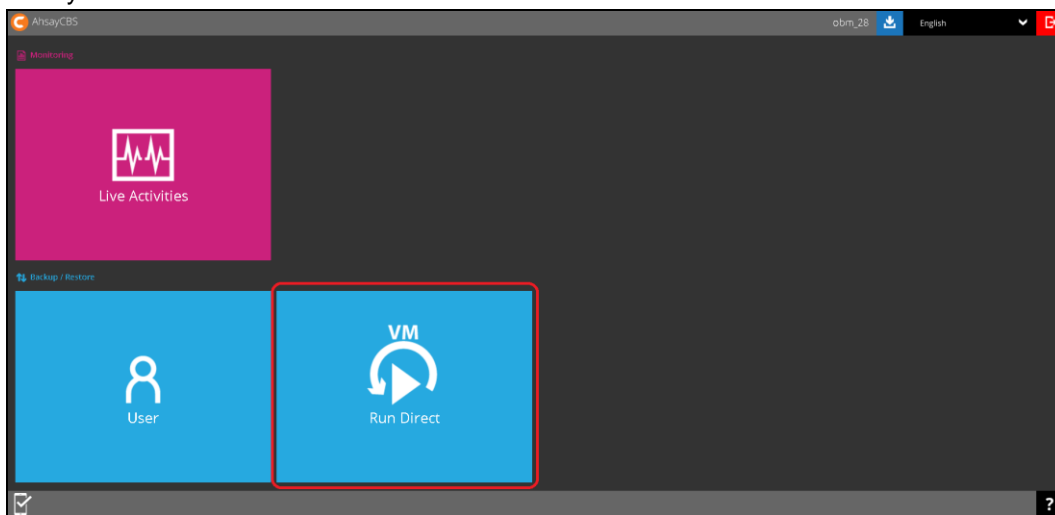
Besides using the AhsayOBM, you can utilize the AhsayCBS User Web Console to initiate a Run Direct restore (also known as Agentless Restore).

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 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 v9 User's 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 Specific Backup Job

Start Run Direct

Restore file of job 2021-02-04-10-12-00

10.120.8.42

☒ win server 2016

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
2021-02-04 11:13:42	info	Preparing for Run Direct...
2021-02-04 11:13:43	info	Use target storage as VM working directory. Reason = "Delta disk format of virtual disks is not supported by datastore."
2021-02-04 11:13:50	info	Mount datastore "cbs-RunDirect (10.16.10.11:cbsRunDirect)"...

Run Direct



<input type="checkbox"/>	Running	Backup Set	Host	Name	Progress	Start time
<input type="checkbox"/>	No	VMware Run Direct Backup Set	10.120.8.42	New Virtual Machine		2021-02-04 11:13:20

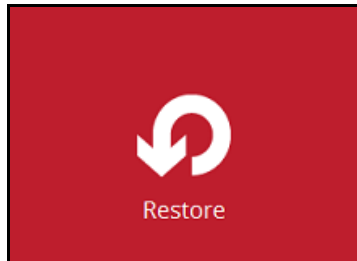
NOTE

In cases when Run Direct restore encounters an error, temporary files will remain on the VMware Host. These temporary files must be manually cleaned. For instructions on how to do this please refer to the [Appendix](#).

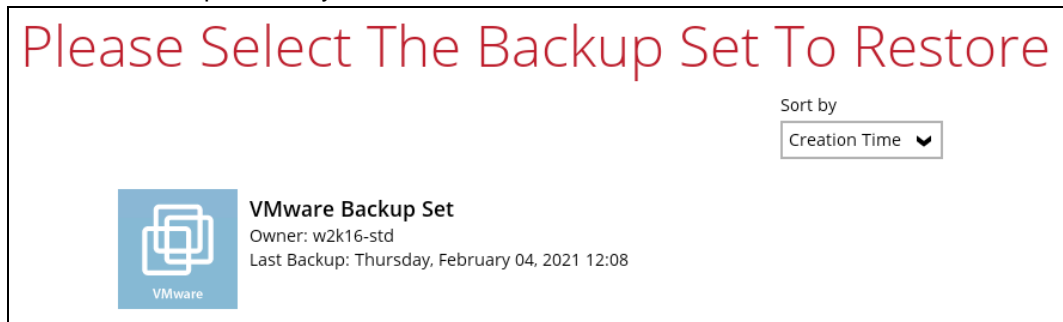
10 Method 2 - Restoring a Virtual Machine without Run Direct

VM Restore without Run Direct

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



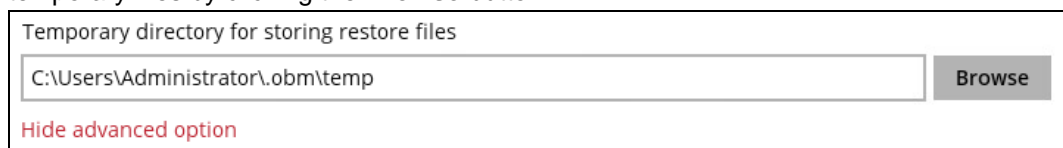
2. Select the backup set that you would like to restore the VM from.



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



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



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

☐ Show backup job(s) outside retention

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



All backup jobs will be shown, including the backup jobs which have been deleted. Some of the data may not be restorable. Do you wish to continue?

Yes

No

5. Select to restore VM from a specific backup job, or the latest job available from the **Select what to restore** drop down menu. Then select the virtual machine that you would like to restore.

Select Your Virtual Machines To Be Restored

Select what to restore

Choose from files as of job 02/04/2021 Latest ☐ Show backup job(s) outside retention

Folders	Name	Size	Date modified
AhsayCBS	Hard disk 1		
10.120.8.42	win server 2016.nvram	8KB	02/04/2021 12:06
win server 2016	win server 2016.vmsd	0B	02/04/2021 12:06
	win server 2016.vmx	3KB	02/04/2021 11:24

☐ Restore raw file

Items per page 50 Page 1 / 1

Previous

Next

Cancel

Help

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).

Choose Where The Virtual Machines To Be ...

Restore virtual machines to

☒ Original location

☐ Alternate location

☐ Run Direct

[Show advanced option](#)

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

Choose Where The Virtual Machines To Be ...

Restore virtual machines to

- ☒ Original location
☐ Alternate location

☐ Run Direct

Show advanced option

☐ 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.
- i. 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 / 6 / 6.5 / 6.7 / 7.0**, 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 / 6 / 6.5 / 6.7 / 7.0

Username

root

Password

.....

Host

10.120.8.42

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.



The screenshot shows a dialog box titled "Alternate location" in red. Below the title is a section header "VMware Host" in red. The form contains the following fields: "Version" with a dropdown menu showing "VMware vCenter 5.5 / 6 / 6.5 / 6.7 / 7.0"; "Username" with a text input field containing "Administrator"; "Password" with a text input field containing seven dots; "Host" with a text input field containing "new_vcenter_host"; and "Port" with a text input field containing "443".

Click **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.



The screenshot shows a dialog box titled "Alternate location" in red. Below the title is the text "VMware ESXi 6.5.0 build-4564106@10.120.8.42:443(SSH:22)". The form contains the following fields: "Name" with a text input field containing "New Virtual Machine"; "Inventory Location" with a text input field containing "10.120.8.42" and a "Browse" button; "Host/Cluster" with a text input field containing "10.120.8.42" and a "Browse" button; "Resource Pool" with a text input field containing "10.120.8.42" and a "Browse" button; and "Storage" with a text input field containing "Datastore-SHR01" and a "Browse" button.

Alternate location

VMware vCenter Server 6.0.0 build-9313458@10.16.8.25:443

Name

New Virtual Machine

Inventory Location

Datacenter_01

Browse

Host/Cluster

Browse

Resource Pool

Browse

Storage

Browse

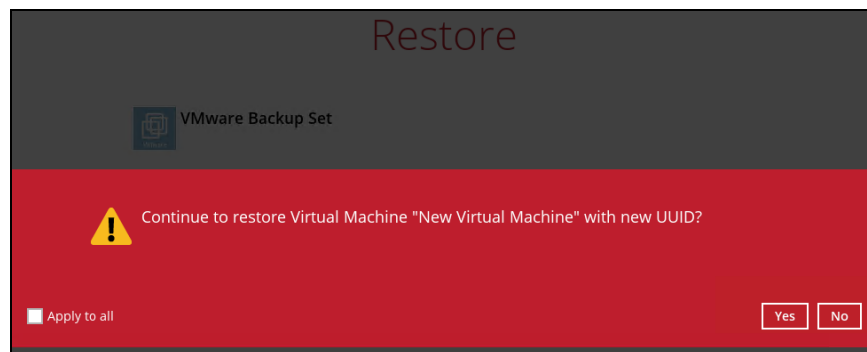
NOTE

For VMware ESXi backup sets, when restoring a guest VM to either different datastore on the original VMware ESXi host or different VMware ESXi host, make sure the datastore is formatted in the same VMFS version.

For example if the guest VM was originally backed up from a VMware host using VMFS5 datastore, then it must be restored back to a VMFS5 datastore. Restoring the guest VM to a VMFS6 datastore will not work.


The limitation does not apply to VMware vCenter backup sets.


9. Click **Restore** to proceed.
10. When restoring your guest VM, different messages will be prompted depending on your selected location.
 - 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.





11. The status of the restore job will be displayed.

Restore



VMware Backup Set


AhsayCBS (Host: 10.16.10.11:80)


Restoring... C:\Users\Administrator\temp\RestoreSet\1611738972751\win server 201...
 Estimated time left 3 min 35 sec (5.14GB)
 Restored 4.14GB (3 files)
 Elapsed time 8 min 51 sec
 Transfer rate 102.24Mbit/s


Aside from AhsayOBM, you can also check the status of the restore job from the vSphere interface. You can see that the restore started in the task “Make Directory”, and the restore was completed in the “Reconfig VM” task.


Recent tasks							
Task	Target	Initiator	Queued	Started	Result	Comple...	
Reconfig VM	 New Virtual ...	root	02/04/2021 ...	02/04/2021 14:32:36	✓ Completed succ...	02/04/2021 ...	^
Nfc Random Access...	None	root	02/04/2021 ...	02/04/2021 14:20:37	✓ Completed succ...	02/04/2021 ...	
Find By Inventory P...	None	root	02/04/2021 ...	02/04/2021 14:20:36	✓ Completed succ...	02/04/2021 ...	
Register VM	vm	root	02/04/2021 ...	02/04/2021 14:20:33	✓ Completed succ...	02/04/2021 ...	
Refresh Datastore S...	Datastore-SHR02	root	02/04/2021 ...	02/04/2021 14:20:28	✓ Completed succ...	02/04/2021 ...	
Create Virtual Disk	[Datastore-SHR0...	root	02/04/2021 ...	02/04/2021 14:20:27	✓ Completed succ...	02/04/2021 ...	
Make Directory	None	root	02/04/2021 ...	02/04/2021 14:20:26	✓ Completed succ...	02/04/2021 ...	v

12. The following screen will be displayed when the VM has been restored successfully.

Restore


VMware Backup Set


AhsayCBS (Host: 10.16.10.11:80)



✓ Restore Completed Successfully
 Estimated time left 0 sec
 Restored 9.28GB (4 files)
 Elapsed time 16 min 17 sec
 Transfer rate 81.65Mbit/s

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.

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

Restoring a VM in VMDK format

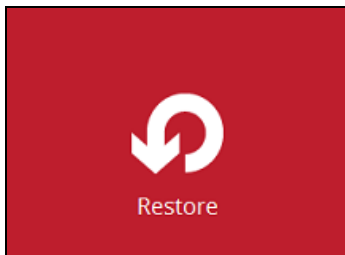
Restoring a VM in VMDK format is used to enable guest VMs that are backed up in VDDK mode to be restored in VMDK raw file format. This feature is useful if you wish to restore the backed up VM to another VMware host (ESXi server) even without using the AhsayOBM.

IMPORTANT

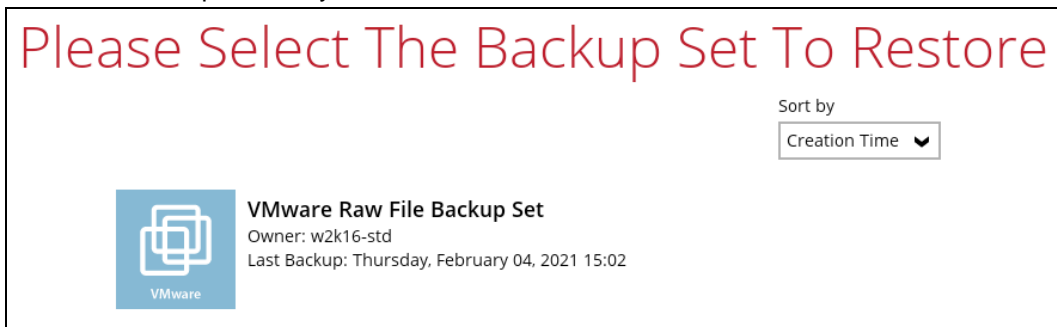
Restoring guest VMs from VDDK to VMDK format only supports backup sets that are created in AhsayOBM. Backup sets created with AhsayOBM before v7.9.0.0, or VMware VDDK backup sets migrated from v6 are **NOT** supported.

Follow the steps below for details.

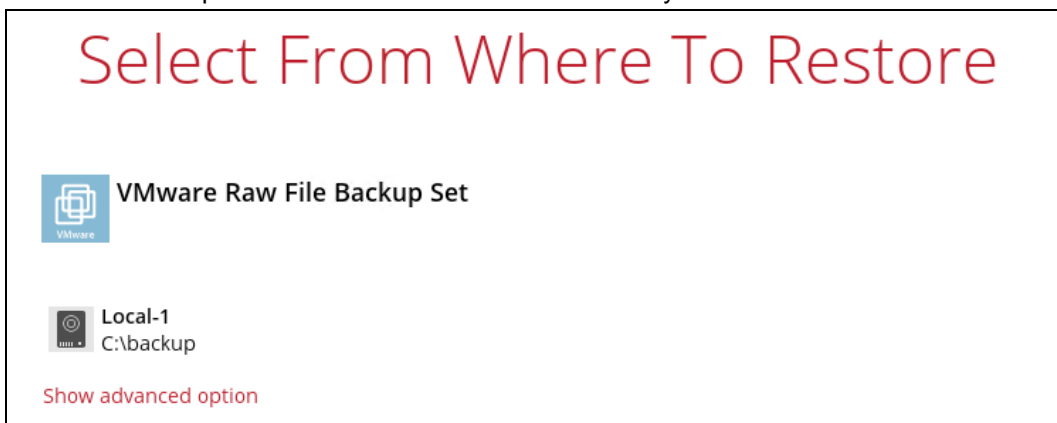
1. Click the **Restore** icon on the main interface of AhsayOBM.



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.



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

Temporary directory for storing restore files

C:\Users\Administrator\obm\temp

Browse

Hide advanced option

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

☐ Show backup job(s) outside retention

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

?

All backup jobs will be shown, including the backup jobs which have been deleted. Some of the data may not be restorable. Do you wish to continue?

YesNo

5. Select to restore VM from a specific backup job, or the latest job available from the **Select what to restore** drop down menu. 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 VMs to restore in .vmdk format.

Select Your Virtual Machines To Be Restored

Select what to restore

Choose from files as of job02/04/2021Latest☐ Show backup job(s) outside retention

Folders

Local-1

10.120.8.42

Lubuntu12x

Hard disk 1

Lubuntu12x.nvram

Lubuntu12x.vmsd

Lubuntu12x.vmx

Lubuntu12x.vmx

Name	Size	Date modified
Hard disk 1	72KB	02/03/2021 16:40
Lubuntu12x.nvram	0B	02/03/2021 16:40
Lubuntu12x.vmsd	3KB	02/03/2021 16:40
Lubuntu12x.vmx	3KB	01/29/2021 16:27

☒ Restore raw file

Items per page50Page1 / 1

PreviousNextCancelHelp

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

Choose Where The Virtual Machines To Be ...

Restore virtual machines to

C:\restored

Browse

Show advanced option

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

Choose Where The Virtual Machines To Be ...

Restore virtual machines to

C:\restored

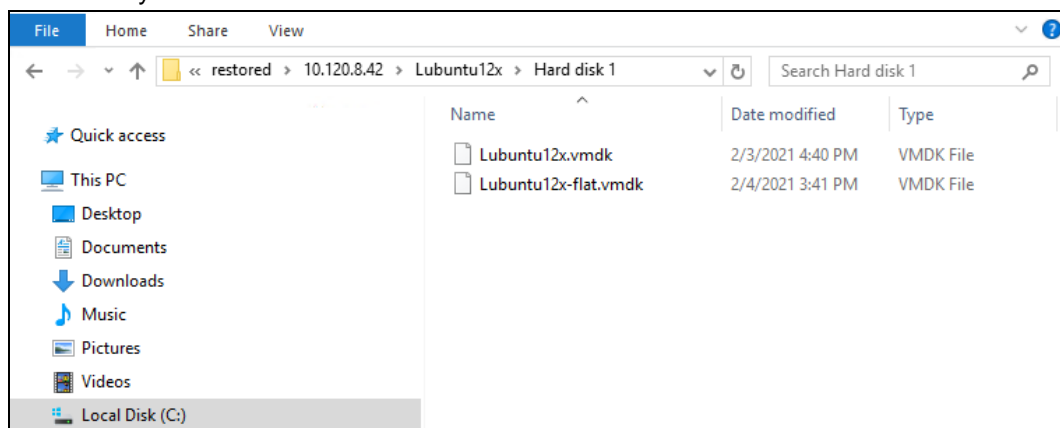
Browse

Show advanced option

☒ Verify checksum of in-file delta files during restore

Hide advanced option

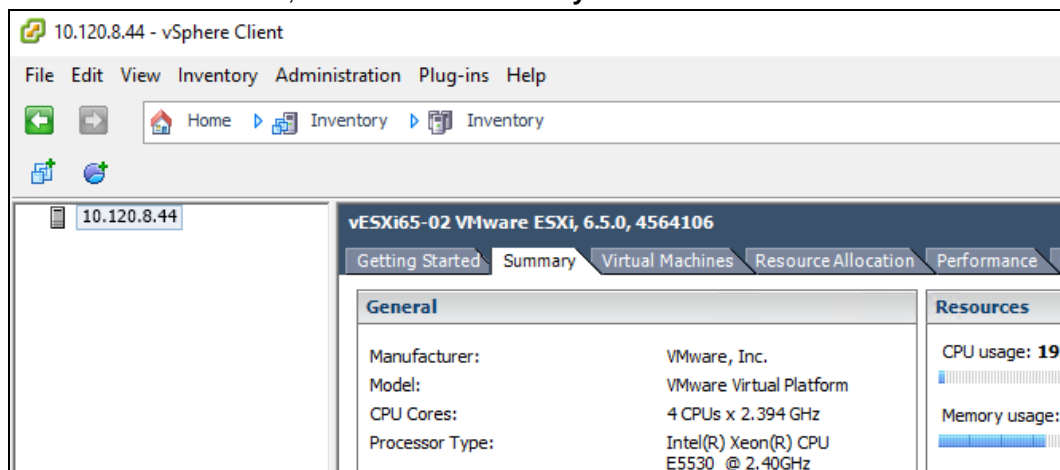
8. Click **Restore** to start the VM restore process.
9. Open the folder where you have the VM restored. Check whether the .vmdk file has been successfully restored.



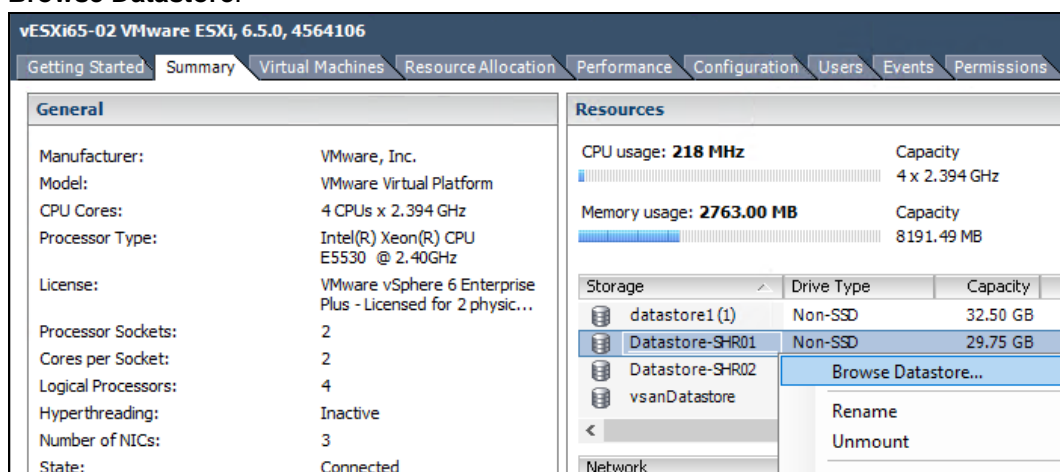
10. Open the VMware vSphere agent and log in to the ESXi server where you wish to restore the VM to.



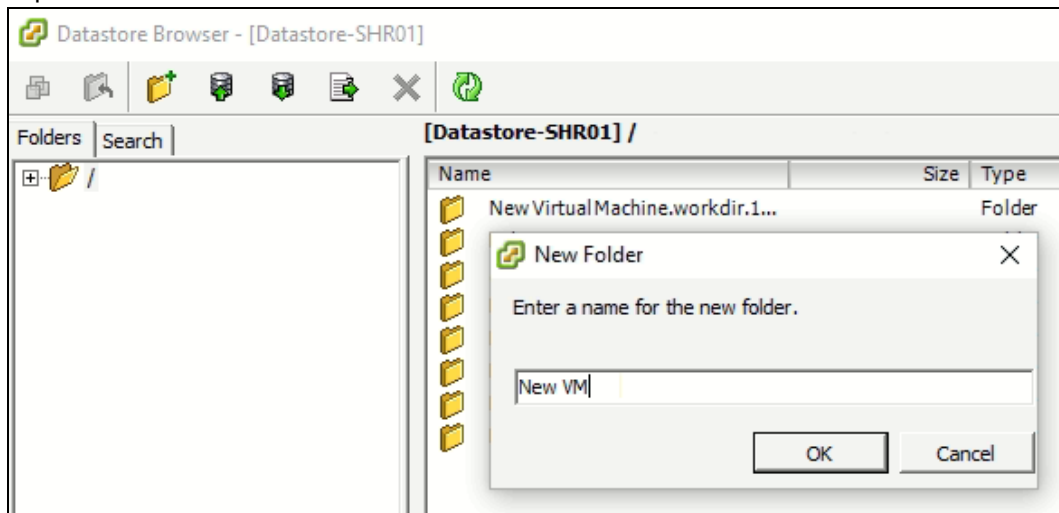
11. Click on the VM's name, then click the **Summary** tab.



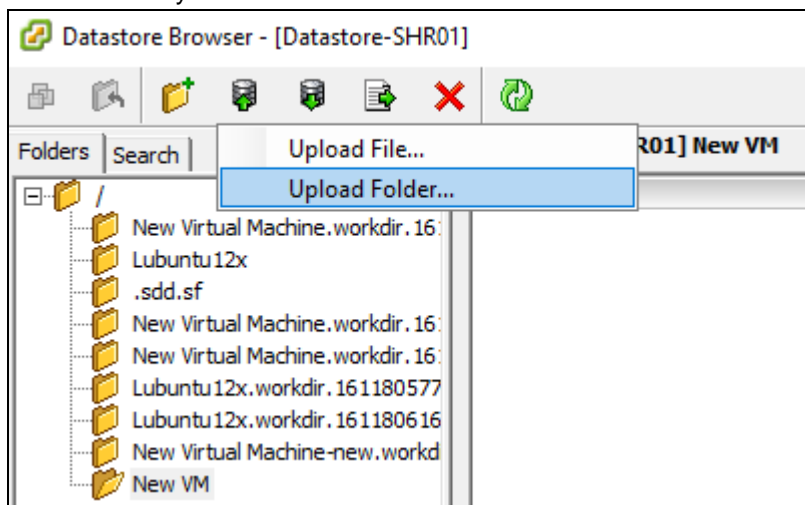
12. Right-click on the Datastore where you wish to deploy the restored VM to, then select **Browse Datastore**.



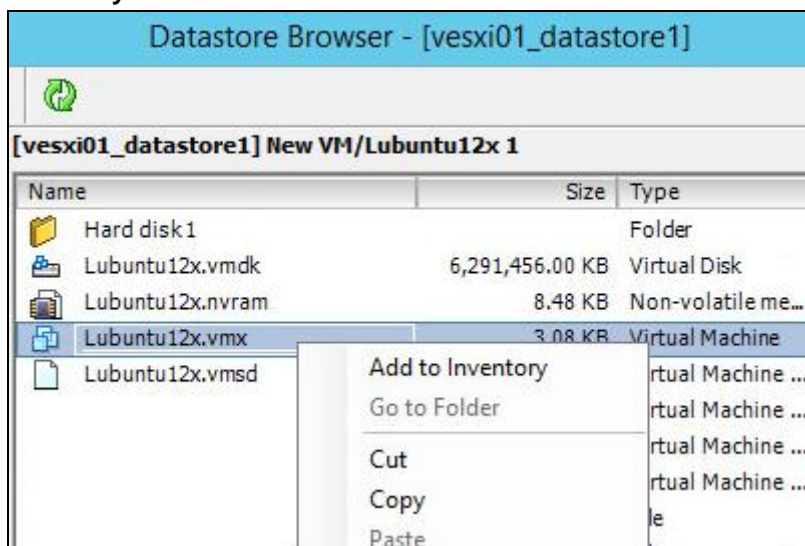
13. Right-click on the right panel to open a new folder for uploading the VM you are going to import.



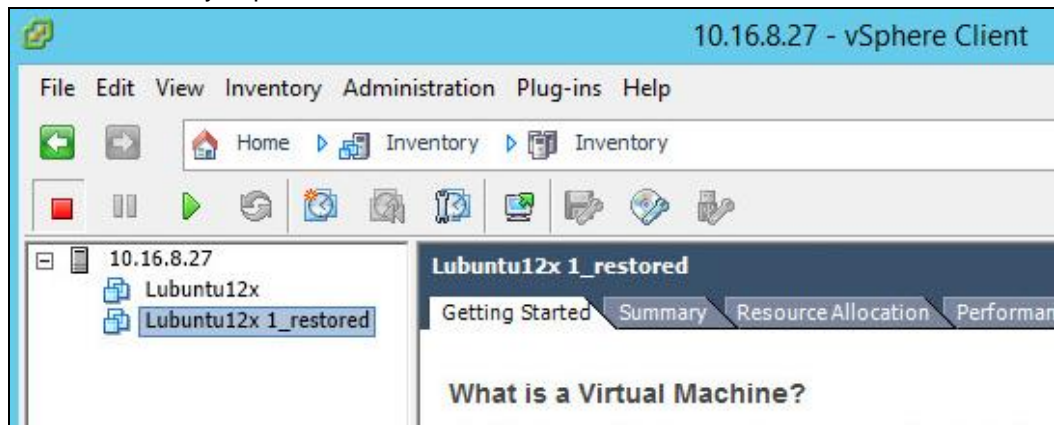
14. Open the newly created folder then select the **Upload Folder** option at the top menu bar to select the VM you wish to restore.



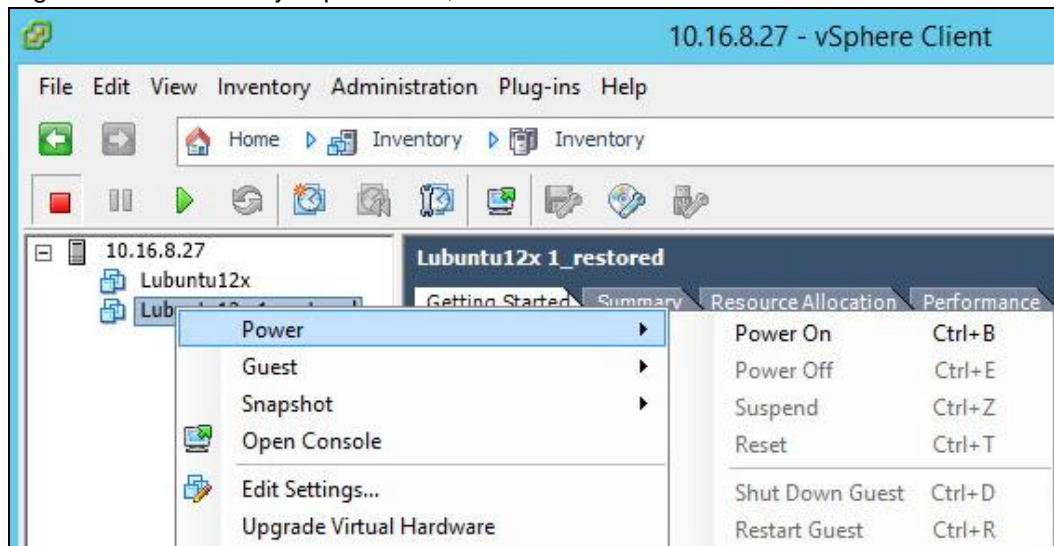
15. Open the folder you have just uploaded, then right-click on the .vmx file and click **Add to Inventory**.



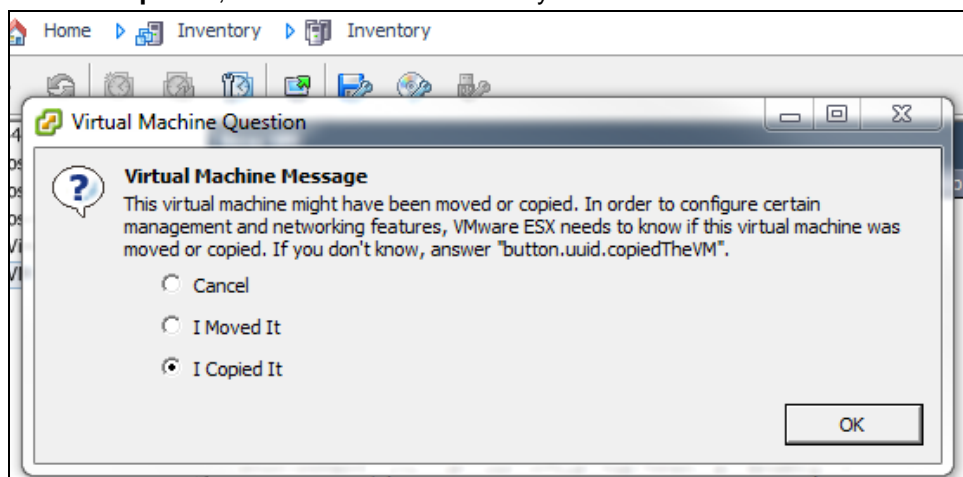
16. Follow the screen prompts, then name the imported VM and confirm the resource pool. You should see the imported VM displayed on the left of the main page of vSphere if the VM has been successfully imported to the ESXi server.



17. Right-click on the newly imported VM, then click **Power > Power On** to turn it on.



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



12 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.

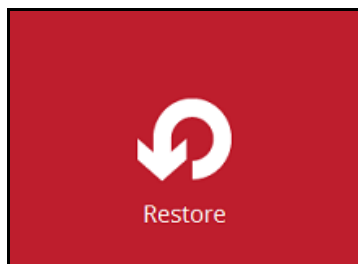
- Microsoft Visual C++ 2015 Redistributable (x86) / (x64)
<https://www.microsoft.com/en-us/download/details.aspx?id=48145>
- Update for Universal C Runtime in Windows
<https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows>
- Microsoft Security Advisory 3033929 (for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

Please Select The Backup Set To Restore

Sort by
Creation Time ▼

**VMware GR Backup Set**
Owner: w2k16-std
Last Backup: Wednesday, February 03, 2021 14:06

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

Select From Where To Restore

**VMware GR Backup Set**

**AhsayCBS**
Host: 10.16.10.11:80

Show advanced option

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

Temporary directory for storing restore files

C:\Users\Administrator\.obm\temp

Browse

Hide advanced option

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

Please Choose A Restore Mode

Restore mode

☐ Restore virtual machines

☒ Restore individual files inside virtual machine (Granular Restore)

☒ Mount virtual disks automatically

Show advanced option

NOTE

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

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

Read timeout limit

Default

Default

Unlimited

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.

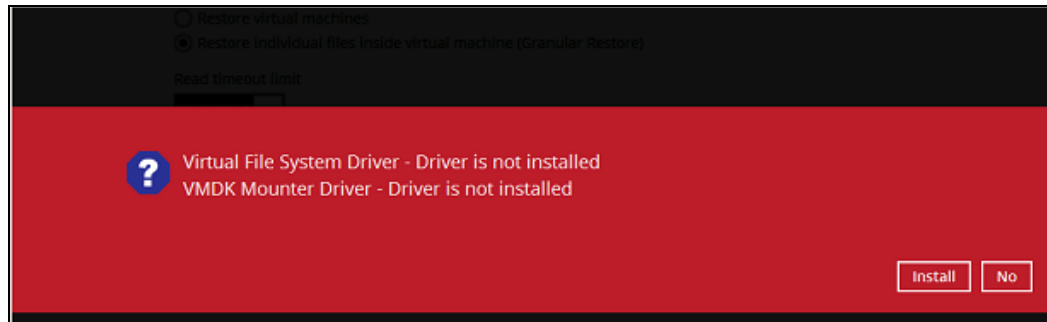
- **Default** – This setting should be suitable for guest VMs located on a local, removable, or network drive. The time out value is 15 seconds.
- **Unlimited** – The connection will not time out when this is selected. This selection is recommended when:
 - Backup destination is a cloud storage.
 - AhsayCBS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

NOTE

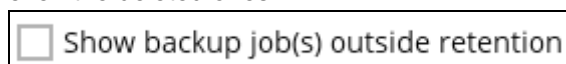
If in doubt or unsure about the guest VM size or network stability, it is recommended to use **Unlimited**.

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

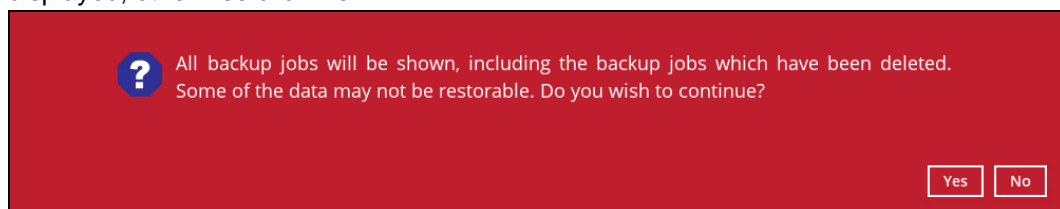
5. The following screen will be shown when you perform Granular Restore for a backup set on this machine for the first time only. Make sure you click **Install** to confirm starting the installation of the drivers on this machine. Clicking **No** will exit the restore process.



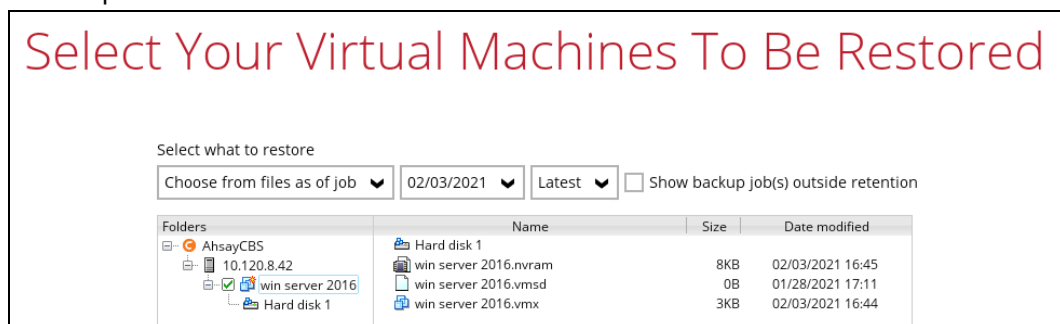
6. Tick **Show backup job(s) outside retention** if you want all backup jobs to be displayed, even the deleted ones.



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



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

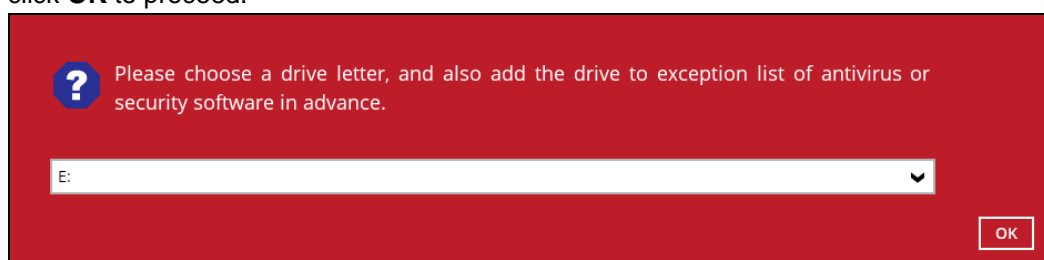


8. The following screen will be displayed when the virtual disk(s) are in the process of being prepared for mounting on the AhsayOBM machine.



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.



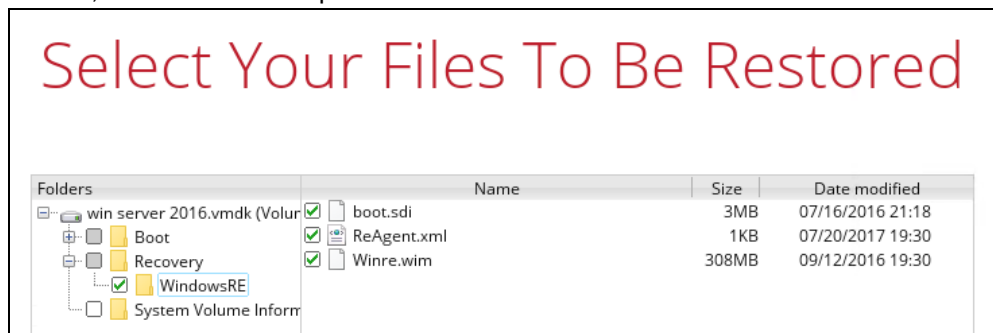
There are two options to restore individual files from here.

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**.


Choose Where The Files To Be Restored

Restore files to

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

Restore

**VMware GR Backup Set**

**AhsayCBS (Host: 10.16.10.11:80)**

✓ Restore Completed Successfully

Estimated time left 0 sec

Restored 310.56MB (4 files)

Elapsed time 1 min 5 sec

Transfer rate 41.28Mbit/s

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

restored > win server 2016.vmdk (Volume-1) > Recovery > WindowsRE					Search WindowsRE
		Name	Date modified	Type	Size
★ Quick access		boot.sdi	7/16/2016 9:18 PM	SDI File	3,096 KB
Desktop		ReAgent.xml	7/20/2017 7:30 PM	XML Document	2 KB
Downloads		Winre.wim	9/12/2016 7:30 PM	WIM File	314,913 KB


Option 2: Restore Using Windows File Explorer

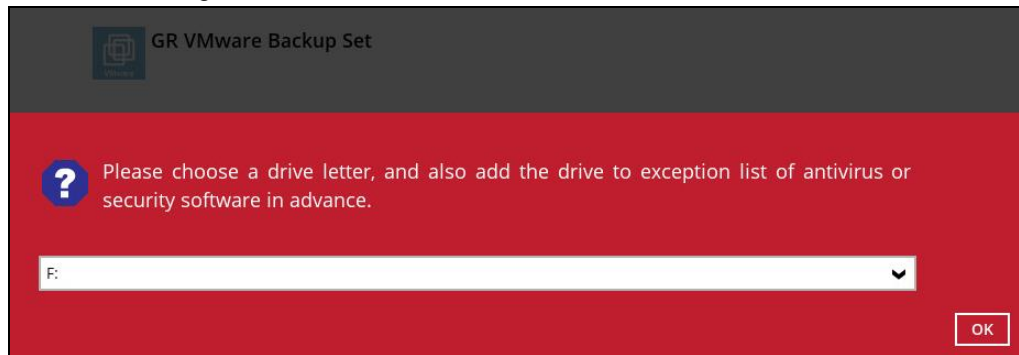
This method allows you to browse through the files from the mounted virtual disk through the Windows File Explorer on the machine where you have AhsayOBM installed on.

NOTE

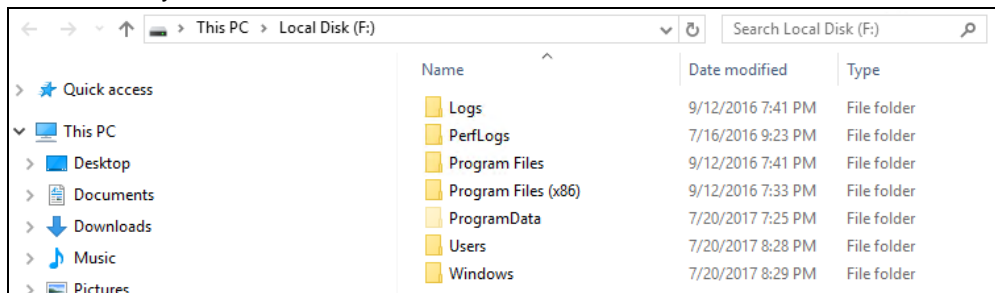
Granular restore of VMware backup sets performed using Windows File Explorer:

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.

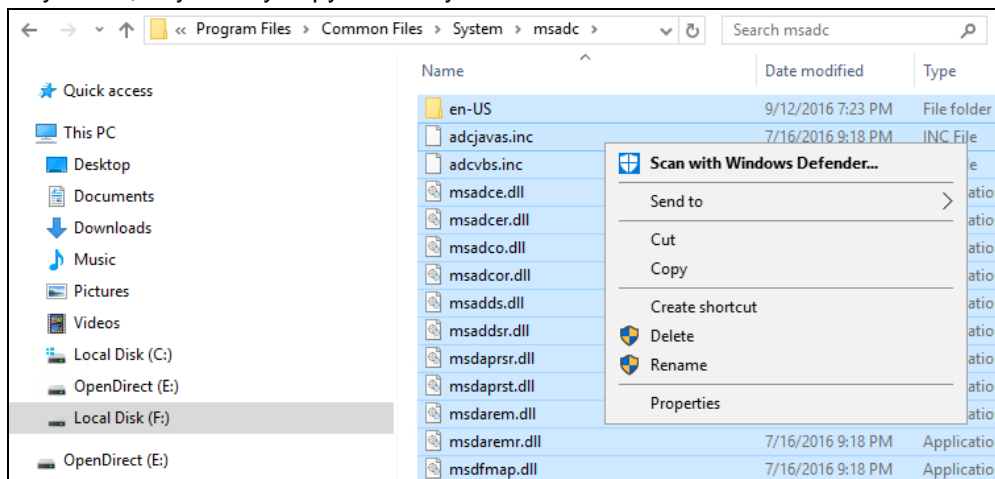
- i. Click  and then you will be prompted to select a drive letter where you wish the mounted backup image to be mapped on your machine, click **OK** when you have finished selecting.



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



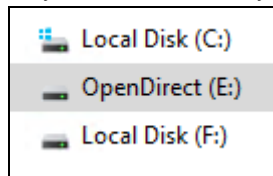
- iii. You can now click on the files to view them directly from here, which will be in read-only mode, or you may copy them to your local machine.



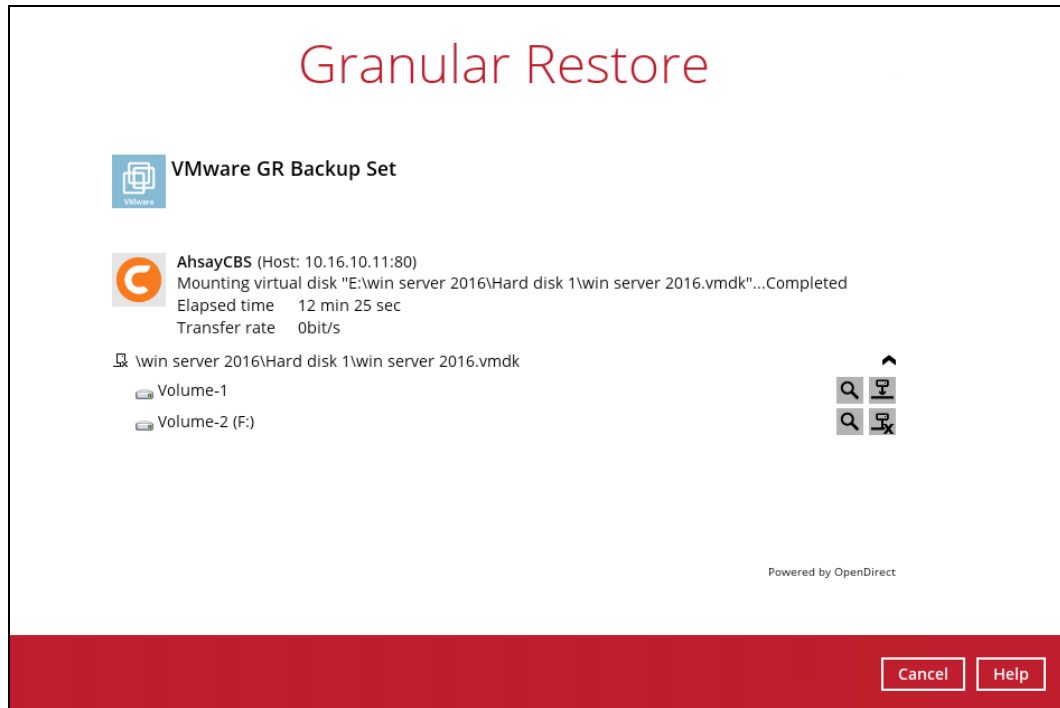
NOTE

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.

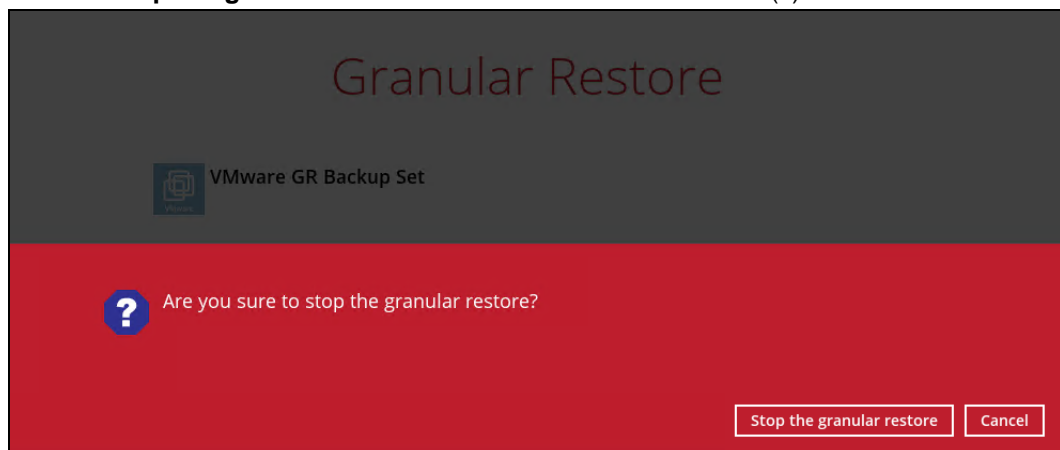
- iv. The mounted drive letter cannot be ejected from the Windows File Explorer, and it will only be closed when you exit AhsayOBM.



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



13. Click on **Stop the granular restore** and unmount the virtual disk(s).



IMPORTANT

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

13 Method 5 - Restoring a Virtual Machine on vSAN

There are three supported restore scenarios for normal and Run Direct restore of VMs on a vSAN Cluster. Each scenario will be discussed below.

• Restore with Run Direct

- [Restore from vSAN datastore to vSAN datastore](#)
- [Restore from vSAN datastore to VMFS datastore](#)
- [Restore from VMFS datastore to vSAN datastore](#)

• Restore without Run Direct

- [Restore from vSAN datastore to vSAN datastore](#)
- [Restore from vSAN datastore to VMFS datastore](#)
- [Restore from VMFS datastore to vSAN datastore](#)

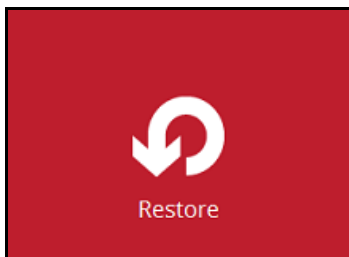
LIMITATIONS

- Restore of guest VMs on a Stretched vSAN Cluster will be slower.
Since it will be dependent on the internet for connection between the AhsayOBM staging machine and the VMware vCenter server compared with a non-Stretched vSAN Cluster backup and restore which is using a LAN connection.
- Run Direct restore may not be possible for Stretched vSAN Cluster since AhsayOBM is located on another site.
The VMware vCenter server will have to power on and manage the VM, which is stored on a backup destination on the AhsayOBM staging machine through an internet connection.

13.1 Restore with Run Direct

13.1.1 Restore from vSAN datastore to vSAN datastore

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



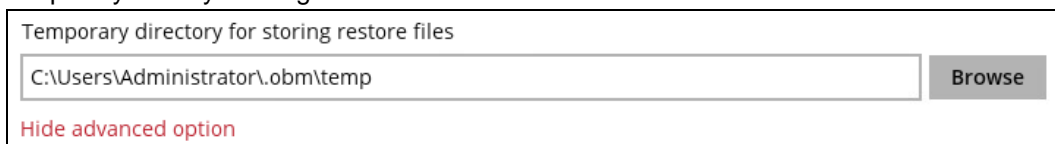
2. Select the backup set that you would like to restore the VM from.



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



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



4. If Granular Restore is enabled in the backup set this screen will be displayed, select the restore mode. Otherwise proceed to the next step.

Please Choose A Restore Mode

Restore mode


☒ Restore virtual machines

☐ Restore individual files inside virtual machine (Granular Restore)

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

☐ Show backup job(s) outside retention

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

 All backup jobs will be shown, including the backup jobs which have been deleted. Some of the data may not be restorable. Do you wish to continue?

Yes No

6. 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 Restored

Select what to restore

Choose from files as of job 03/17/2021 Latest ☐ Show backup job(s) outside retention

Folders	Name	Size	Date modified
Local-1	Hard disk 1		
vCenter05-v65	Lubuntu12x.nvram	72KB	03/17/2021 10:22
Datacenter	Lubuntu12x.vmsd	0B	03/09/2021 17:28
Hosts and Clusters	Lubuntu12x.vmx	3KB	03/17/2021 10:22
VSAN	Lubuntu12x.vmx	3KB	03/09/2021 17:28
New vSAN			
Hard			

7. Select to restore the VM to the **Original location**.

Choose Where The Virtual Machines

Restore virtual machines to

☒ Original location

☐ Alternate location

☒ Run Direct

☐ 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

Show advanced option

8. 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:

Restore virtual machines to

☒ Original location

☐ Alternate location

☒ Run Direct

☐ 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

• **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.

9. Click **Show advanced option** if you would like to enable **Verify checksum of in-file delta files during restore**.

Choose Where The Virtual Machines

Restore virtual machines to

☒ Original location
☐ Alternate location

☒ Run Direct
☐ 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

Show advanced option

☐ Verify checksum of in-file delta files during restore


Hide advanced option


NOTE

If this option is enabled this will result in additional restore time depending on the number of delta files.

10. Click **Restore** to proceed.
11. When restoring your guest VM, different messages will be prompted depending on the selected location.
- Restoring guest VM to original location, this message will only be displayed if the original guest VM exists on the datastore. Click **Yes** to proceed.

Restore

 vSAN RD Backup Set 1

 The Virtual machine "Datacenter/New vSAN Virtual Machine 2" already exists.
Replace existing virtual machine?

☐ Apply to all

Yes **No**

- The progress of the restore can be seen from the status bar.

Restore

 **vSAN RD Backup Set 1**

 **Local-1 (C:\backup)**
Mount datastore "obm-RunDirect (10.16.8.41:obmRunDirect)"...
Elapsed time 32 sec


Restore

 **vSAN RD Backup Set 1**


 **Local-1 (C:\backup)**
Adding virtual machine "New vSAN Virtual Machine 2" to the inventory...
Elapsed time 36 sec


Restore

 **vSAN RD Backup Set 1**









 **Local-1 (C:\backup)**
Taking snapshot "__snapshot_for_publish_" of virtual machine "New vSAN Virtual M...
Elapsed time 49 sec

Restore

 **vSAN RD Backup Set 1**

 **Local-1 (C:\backup)**
Powering on virtual machine "New vSAN Virtual Machine 2"...
Elapsed time 57 sec

Another way of checking the progress of the restore is from vSphere. The restore has started when a NAS datastore was created, and it is completed when the virtual machine was powered on.

Recent Tasks		Alarms						
Task Name	Target	Status	Initiator	Queued For	Start Time	Completion T...	Server	
Create NAS datastore	 10.16.8.45	 Completed	VSPHERE.LOC...	17 ms	03/23/2021, 10:34:30 AM	03/23/2021, 10:34:31 AM	vCenter05-v65	
Register virtual machine	 Datacenter	 Completed	VSPHERE.LOC...	6 ms	03/23/2021, 10:34:33 AM	03/23/2021, 10:34:35 AM	vCenter05-v65	
Create virtual machine snapshot	 New vSAN...	 Completed	VSPHERE.LOC...	6 ms	03/23/2021, 10:34:43 AM	03/23/2021, 10:34:45 AM	vCenter05-v65	
Power On virtual machine	 New vSAN...	 Completed	VSPHERE.LOC...	28 ms	03/23/2021, 10:34:50 AM	03/23/2021, 10:34:53 AM	vCenter05-v65	

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

Restore

vSAN RD Backup Set 1

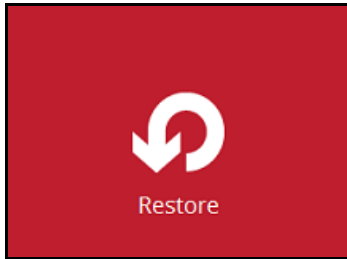
Local-1 (C:\backup)
✓ Restore Completed Successfully
 Elapsed time 1 min 38 sec

NOTE

In cases when Run Direct restore encounters an error or AhsayOBM crashes during a Run Direct restore, temporarily files are remained on the VMware Host. These temporary files must be manually cleaned. For instructions on how to do this, please refer to the [Appendix](#).

13.1.2 Restore from vSAN datastore to VMFS datastore

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



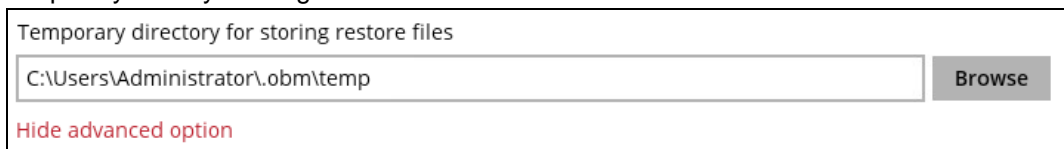
2. Select the backup set that you would like to restore the VM from.



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



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



4. If Granular Restore is enabled in the backup set, the following screen will be displayed. Select the restore mode. Otherwise, proceed to the next step.

Please Choose A Restore Mode

Restore mode


☒ Restore virtual machines

☐ Restore individual files inside virtual machine (Granular Restore)

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

☐ Show backup job(s) outside retention

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

 All backup jobs will be shown, including the backup jobs which have been deleted. Some of the data may not be restorable. Do you wish to continue?

Yes No

6. 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 Restored

Select what to restore

Choose from files as of job 03/09/2021 Latest ☐ Show backup job(s) outside retention

Folders	Name	Size	Date modified
Local-1	Hard disk 1		
vCenter05-v65	Lubuntu12x.nvram	72KB	03/09/2021 11:38
Datacenter	Lubuntu12x.vmsd	0B	03/09/2021 17:05
Hosts and Clus	Lubuntu12x.vmx	3KB	03/09/2021 17:05
VSAN	Lubuntu12x.vmx	3KB	01/29/2021 19:46
Ubuntu			

7. Select to restore the VM to an **Alternate location** (to another datastore on the original VMware host or another VMware host).

Choose Where The Virtual Machines

Restore virtual machines to

☐ Original location

☒ Alternate location

☒ Run Direct

☒ 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

Show advanced option

8. 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:

Restore virtual machines to

☐ Original location

☒ Alternate location

☒ Run Direct

☐ 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

• **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.

9. Click **Show advanced option** if you would like to enable **Verify checksum of in-file delta files during restore**.

Choose Where The Virtual Machines

Restore virtual machines to

☐ Original location

☒ Alternate location

☒ Run Direct

☒ 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

Show advanced option

☐ Verify checksum of in-file delta files during restore

Hide advanced option

NOTE

If this option is enabled this will result in additional restore time depending on the number of delta files.

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

10. This step applies only for restoring to **Alternate location**.

Enter the VMware host and access information of where you would like the VM to be restored to, then 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 / 6 / 6.5 / 6.7 / 7.0 ▼

Username

Administrator

Password

•••••

Host

new_vcenter_host

Port

443

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

Alternate location

VMware vCenter Server 6.5.0 build-5318154@10.16.8.40:443

Name

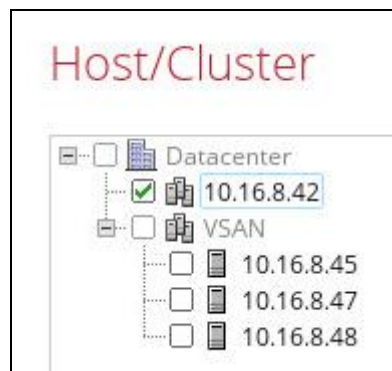
Inventory Location

Host/Cluster

Resource Pool

Storage

Select the host where the VM will be restored, make sure to select a host not on the vSAN cluster.



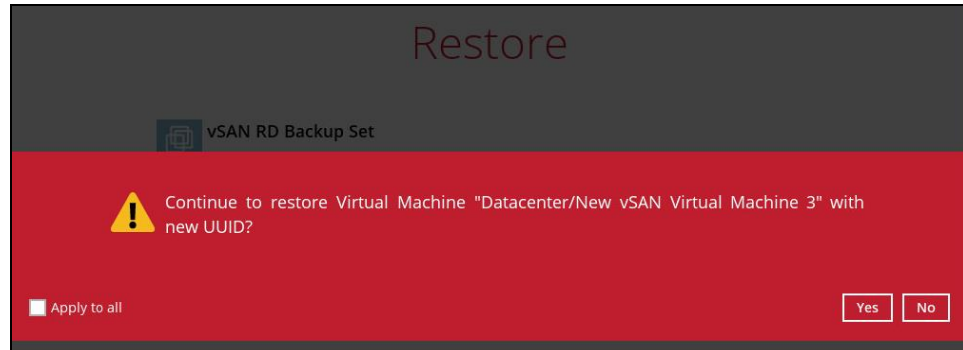
Select the storage.



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

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

- 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.



- The progress of the restore can be seen from the status bar.



Restore



vSAN RD Backup Set















Local-1 (C:\backup)

Powering on virtual machine "New Virtual Machine 3"...

Elapsed time 1 min 16 sec

Another way of checking the progress of the restore is from vSphere. The restore has started when a NAS datastore was created. And it is completed when the virtual machine was powered on.

Recent Tasks		Alarms						
Task Name	Target	Status	Initiator	Queued For	Start Time	Completion T...	Server	
Create NAS datastore	 10.16.8.42	 Completed	VSPHERE.LOC...	18 ms	03/23/2021, 10:48:34 AM	03/23/2021, 10:48:38 AM	vCenter05-v65	
Remove datastore	 obm-RunD...	 Completed	VSPHERE.LOC...	6 ms	03/23/2021, 10:45:31 AM	03/23/2021, 10:45:31 AM	vCenter05-v65	
Register virtual machine	 Datacenter	 Completed	VSPHERE.LOC...	11 ms	03/23/2021, 10:48:40 AM	03/23/2021, 10:48:59 AM	vCenter05-v65	
Reload virtual machine	 New Virtu...	 Completed	VSPHERE.LOC...	9 ms	03/23/2021, 10:49:01 AM	03/23/2021, 10:49:05 AM	vCenter05-v65	
Create virtual machine snapshot	 New Virtu...	 Completed	VSPHERE.LOC...	8 ms	03/23/2021, 10:49:10 AM	03/23/2021, 10:49:15 AM	vCenter05-v65	
Power On virtual machine	 New Virtu...	 Completed	VSPHERE.LOC...	7 ms	03/23/2021, 10:49:18 AM	03/23/2021, 10:49:55 AM	vCenter05-v65	

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

Restore



vSAN RD Backup Set



Local-1 (C:\backup)

✓ Restore Completed Successfully

Elapsed time 1 min 50 sec

NOTE

In cases when Run Direct restore encounters an error or AhsayOBM crashes during a Run Direct restore, temporarily files are remained on the VMware Host. These temporary files must be manually cleaned. For instructions on how to do this please refer to the [Appendix](#).

13.1.3 Restore from VMFS datastore to vSAN datastore

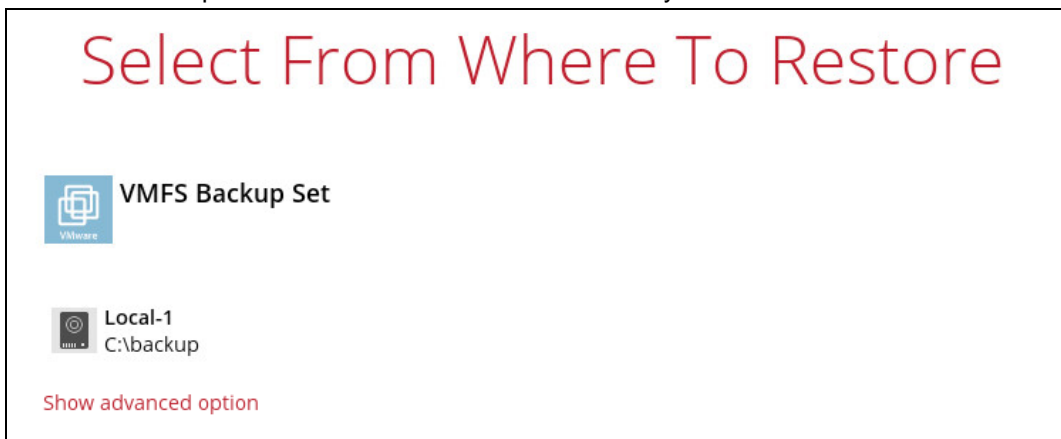
1. Click the **Restore** icon on the main interface of AhsayOBM.



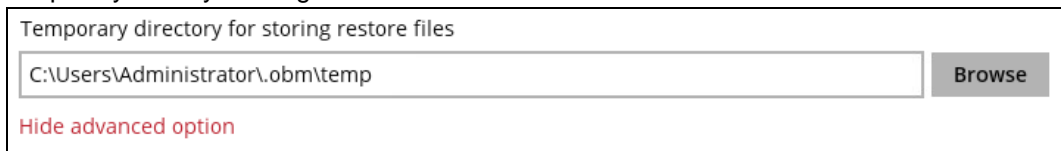
2. Select the backup set that you would like to restore the VM from.



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



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



4. If Granular Restore is enabled in the backup set, the following screen will be displayed. Select the Restore mode. Otherwise, proceed to the next step.

Please Choose A Restore Mode

Restore mode


☒ Restore virtual machines

☐ Restore individual files inside virtual machine (Granular Restore)

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

☐ Show backup job(s) outside retention

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

 All backup jobs will be shown, including the backup jobs which have been deleted. Some of the data may not be restorable. Do you wish to continue?

6. 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 Restored

Select what to restore

Choose from files as of job 03/10/2021 Latest ☐ Show backup job(s) outside retention

Folders	Name	Size	Date modified
Local-1	<input checked="" type="checkbox"/> Hard disk 1		
vCenter05-v65	<input checked="" type="checkbox"/> win server 2016.nvram	8KB	03/09/2021 15:29
Datacenter	<input checked="" type="checkbox"/> win server 2016.vmsd	0B	03/10/2021 14:12
Hosts and Clusters	<input checked="" type="checkbox"/> win server 2016.vmx	3KB	03/10/2021 14:12
10.16.8.42			
win serv			

7. Select to restore the VM to an **Alternate location** (to another datastore on the original VMware host or another VMware host).

Choose Where The Virtual Machines

Restore virtual machines to

☐ Original location

☒ Alternate location

☒ Run Direct

☒ 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

Show advanced option

8. 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:

Restore virtual machines to

☐ Original location

☒ Alternate location

☒ Run Direct

☐ 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

• **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.

9. Click **Show advanced option** if you would like to enable **Verify checksum of in-file delta files during restore**.

Choose Where The Virtual Machines

Restore virtual machines to

☐ Original location

☒ Alternate location

☒ Run Direct

☒ 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

Show advanced option

☐ Verify checksum of in-file delta files during restore

Hide advanced option

NOTE

If this option is enabled, this will result in additional restore time depending on the number of delta files.

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

10. This step applies only for restoring to **Alternate location**.

Enter the VMware host and access information of where you would like the VM to be restored to, 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 / 6 / 6.5 / 6.7 / 7.0 ▼

Username

Administrator

Password

•••••

Host

new_vcenter_host

Port

443

Enter a new **Name** for the VM, then **Browse** to modify the **Host/Cluster** and **Storage** settings to select the vSAN datastore, according to where you would like the VM to be restored to.

Alternate location

VMware vCenter Server 6.5.0 build-5318154@10.16.8.40:443

Name

Inventory Location

Host/Cluster

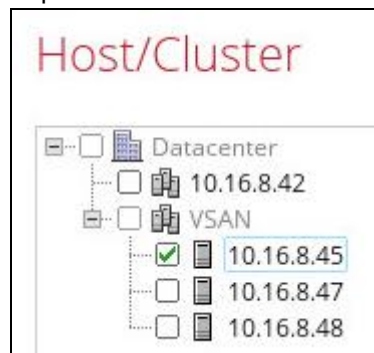
Resource Pool

Storage

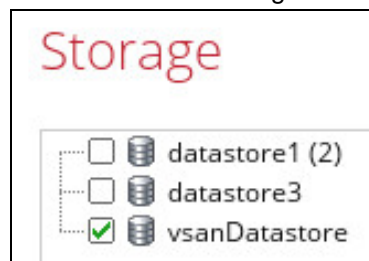
NOTE

It is important to select the vSAN cluster where the VM will be restored even if it is in the same vCenter.

Expand the VSAN to select the host



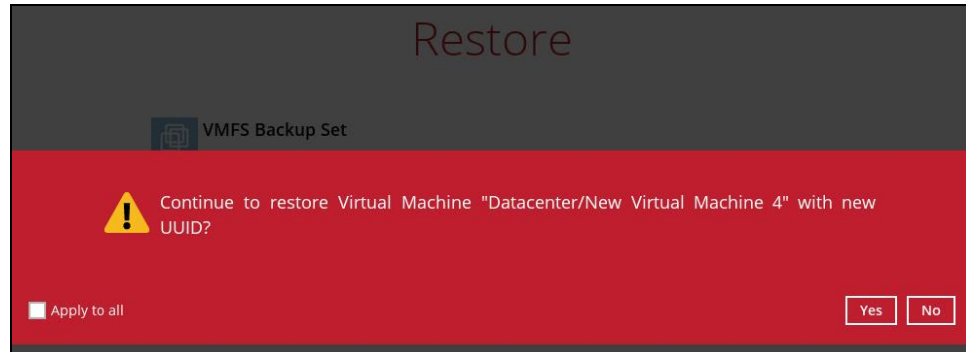
Select the vSAN storage.



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

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

- 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.



- The progress of the restore can be seen from the status bar.



Restore



VMFS Backup Set













Local-1 (C:\backup)

Powering on virtual machine "New Virtual Machine 4"...

Elapsed time 41 sec



Another way of checking the progress of the restore is from vSphere. The restore has started when a NAS datastore was created, and it is completed when the virtual machine was powered on.

Recent Tasks		Alarms					
Task Name	Target	Status	Initiator	Queued For	Start Time	Completion T...	Server
Create NAS datastore	 10.16.8.45	 Completed	VSPHERE.LOC...	5 ms	03/23/2021, 11:08:51 AM	03/23/2021, 11:08:52 AM	vCenter05-v65
Register virtual machine	 Datacenter	 Completed	VSPHERE.LOC...	6 ms	03/23/2021, 11:08:54 AM	03/23/2021, 11:08:56 AM	vCenter05-v65
Reload virtual machine	 New Virtu...	 Completed	VSPHERE.LOC...		03/23/2021, 11:09:00 AM	03/23/2021, 11:09:01 AM	vCenter05-v65
Create virtual machine snapshot	 New Virtu...	 Completed	VSPHERE.LOC...	6 ms	03/23/2021, 11:09:06 AM	03/23/2021, 11:09:09 AM	vCenter05-v65
Power On virtual machine	 New Virtu...	 Completed	VSPHERE.LOC...	7 ms	03/23/2021, 11:09:14 AM	03/23/2021, 11:09:16 AM	vCenter05-v65

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

Restore



VMFS Backup Set



Local-1 (C:\backup)

Restore Completed Successfully

Elapsed time 47 sec



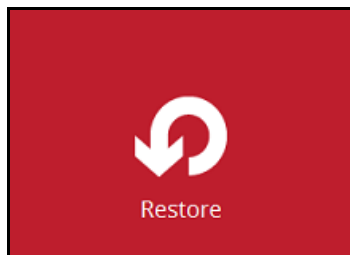
NOTE

In cases when Run Direct restore encounters an error or AhsayOBM crashes during a Run Direct restore, temporarily files are remained on the VMware Host. These temporary files must be manually cleaned. For instructions on how to do this, please refer to the [Appendix](#).

13.2 Restore without Run Direct

13.2.1 Restore from vSAN datastore to vSAN datastore

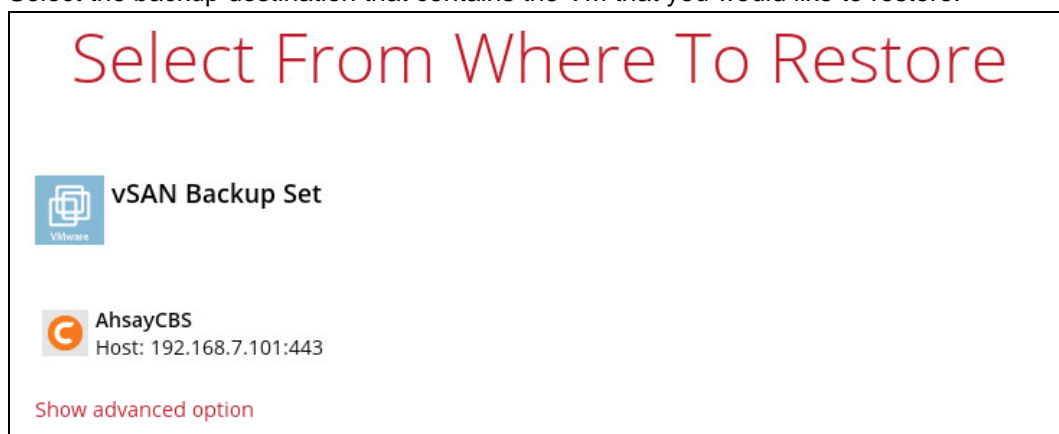
1. Click the **Restore** icon on the main interface of AhsayOBM.



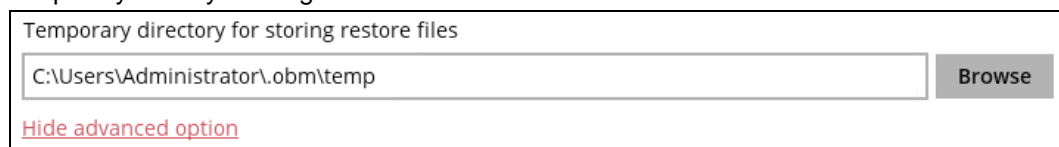
2. Select the backup set that you would like to restore the VM from.



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



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



4. If Granular Restore is enabled in the backup set this screen will be displayed, select the restore mode. Otherwise proceed to the next step.

Please Choose A Restore Mode

Restore mode


☒ Restore virtual machines

☐ Restore individual files inside virtual machine (Granular Restore)

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

☐ Show backup job(s) outside retention

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

 All backup jobs will be shown, including the backup jobs which have been deleted. Some of the data may not be restorable. Do you wish to continue?

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

Select Your Virtual Machines To Be Restored

Select what to restore

Choose from files as of job 03/09/2021 Latest ☐ Show backup job(s) outside retention

Folders	Name	Size	Date modified
AhsayCBS	Hard disk 1		
vCenter05-v65	Lubuntu12x.nvram	72KB	03/09/2021 11:38
Datacenter	Lubuntu12x.vmsd	0B	03/02/2021 16:08
Hosts and Clusters	Lubuntu12x.vmx	3KB	03/09/2021 11:38
VSAN	Lubuntu12x.vmx	3KB	01/29/2021 19:46
Ubuntu			

7. Select to restore the VM to the **Original location**. If the backup set has Run Direct enabled, the **Run Direct** option will be enabled by default. Disable the **Run Direct** option.

Choose Where The Virtual Machines

Restore virtual machines to

☒ Original location

☐ Alternate location

☐ Run Direct

Show advanced option

8. Click **Show advanced option** if you would like to enable **Verify checksum of in-file delta files during restore**.

Choose Where The Virtual Machines

Restore virtual machines to

☒ Original location

☐ Alternate location

☐ Run Direct

[Show advanced option](#)

☐ Verify checksum of in-file delta files during restore

[Hide advanced option](#)

NOTE

If this option is enabled this will result in additional restore time depending on the number of delta files.

9. Click **Restore** to proceed.
10. When restoring your guest VM, different messages will be prompted depending on the selected location.
- Restoring guest VM to original location. This message will only be displayed if the original guest VM exists on the datastore. Click **Yes** to proceed.

Restore

 vSAN Backup Set

 The Virtual machine "Datacenter/Discovered virtual machine/Ubuntu 12.04 LTS" already exists.
Replace existing virtual machine?

☐ Apply to all

[Yes](#) [No](#)

- The progress of the restore can be seen from the status bar.

This step will only be shown if the original guest VM exists on the datastore.

Restore

 **vSAN Backup Set**

 **AhsayCBS (Host: 192.168.7.101:443)**

Delete Virtual Disk "[datastore3] New VM/Lubuntu12x.vmdk"

Estimated time left 0 sec (6.00GB)

Restored 0B (0 file)

Elapsed time 47 sec

Transfer rate 0bit/s

Restore

 **vSAN Backup Set**

 **AhsayCBS (Host: 192.168.7.101:443)**

Restoring "Virtual Disk - [datastore3] New VM/Lubuntu12x.vmdk"...

Estimated time left 0 sec (6.00GB)

Restored 0B (0 file)

Elapsed time 1 min 27 sec

Transfer rate 0bit/s

Restore

 **vSAN Backup Set**

 **AhsayCBS (Host: 192.168.7.101:443)**

VDDK mode restore starts. Virtual Machine = "Datacenter/Discovered virtual machin..."

Estimated time left 0 sec (6.00GB)

Restored 79.28KB (4 files)

Elapsed time 2 min 8 sec

Transfer rate 0bit/s

Restore



vSAN Backup Set



AhsayCBS (Host: 192.168.7.101:443)

Restoring... C:\Users\Administrator\temp\RestoreSet\1614848659175\New VM\Hard ...

Estimated time left 1 min 24 sec (1.60GB)

Restored 4.40GB (4 files)

Elapsed time 8 min 37 sec

Transfer rate 81.13Mbit/s

Another way of checking the progress of the restore is from vSphere. The restore has started when the virtual machine was unregistered, and it is completed when the virtual machine was reconfigured.

Recent Tasks								
Task Name	Target	Status	Initiator	Queued For	Start Time	Completion T...	Server	
Unregister virtual machine	Ubuntu 12...	✓ Completed	VSPHERE.LOC...	10 ms	03/23/2021, 3:59:52 PM	03/23/2021, 3:59:53 PM	vCenter05-v65	
Delete virtual disk		✓ Completed	VSPHERE.LOC...	6 ms	03/23/2021, 4:01:26 PM	03/23/2021, 4:01:26 PM	vCenter05-v65	
Delete file	datastore3	✓ Completed	VSPHERE.LOC...	5 ms	03/23/2021, 4:01:49 PM	03/23/2021, 4:01:49 PM	vCenter05-v65	
Create virtual disk		✓ Completed	VSPHERE.LOC...	11 ms	03/23/2021, 4:02:08 PM	03/23/2021, 4:02:34 PM	vCenter05-v65	
Refresh storage information	datastore3	✓ Completed	VSPHERE.LOC...	10 ms	03/23/2021, 4:02:47 PM	03/23/2021, 4:02:47 PM	vCenter05-v65	
Register virtual machine	Discover...	✓ Completed	VSPHERE.LOC...	10 ms	03/23/2021, 4:02:49 PM	03/23/2021, 4:02:50 PM	vCenter05-v65	
Reconfigure virtual machine	Ubuntu 12...	✓ Completed	VSPHERE.LOC...	8 ms	03/23/2021, 4:13:08 PM	03/23/2021, 4:13:09 PM	vCenter05-v65	

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

Restore



vSAN Backup Set



AhsayCBS (Host: 192.168.7.101:443)

✓ Restore Completed Successfully

Estimated time left 0 sec

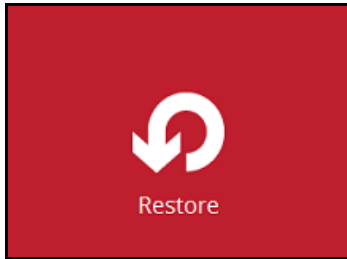
Restored 6.00GB (5 files)

Elapsed time 11 min 29 sec

Transfer rate 75.03Mbit/s

13.2.2 Restore from vSAN datastore to VMFS datastore

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.

Please Select The Backup Set To Restore

Sort by
Creation Time ▼

 **vSAN Backup Set**
Owner: vCenter05-v65
Last Backup: Tuesday, March 09, 2021 16:53

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

Select From Where To Restore

 **vSAN Backup Set**

 **AhsayCBS**
Host: 192.168.7.101:443

Show advanced option

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

Temporary directory for storing restore files

C:\Users\Administrator\obm\temp Browse

Hide advanced option

4. If Granular Restore is enabled in the backup set, the following screen will be displayed. Select the Restore mode. Otherwise, proceed to the next step.

Please Choose A Restore Mode

Restore mode


☒ Restore virtual machines

☐ Restore individual files inside virtual machine (Granular Restore)

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

☐ Show backup job(s) outside retention

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

 All backup jobs will be shown, including the backup jobs which have been deleted. Some of the data may not be restorable. Do you wish to continue?

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

Select Your Virtual Machines To Be Restored

Select what to restore

Choose from files as of job 03/09/2021 ☐ Show backup job(s) outside retention

Folders	Name	Size	Date modified
AhsayCBS	Hard disk 1	72KB	03/09/2021 11:38
vCenter05-v65	Lubuntu12x.nvram	0B	03/02/2021 16:08
Datacenter	Lubuntu12x.vmsd	3KB	03/09/2021 11:38
Hosts and Clusters	Lubuntu12x.vmx	3KB	01/29/2021 19:46
VSAN	Lubuntu12x.vmx		
Ubuntu			

7. Select to restore the VM to an **Alternate location** (to another datastore on the original VMware host or another VMware host). If the backup set has Run Direct enabled, the **Run Direct** option will be enabled by default. Disable the **Run Direct** option.

Choose Where The Virtual Machines

Restore virtual machines to

☐ Original location

☒ Alternate location

☐ Run Direct

Show advanced option

8. Click **Show advanced option** if you would like to enable **Verify checksum of in-file delta files during restore**.

Choose Where The Virtual Machines

Restore virtual machines to

☒ Original location

☐ Alternate location

☐ Run Direct

Show advanced option

☐ Verify checksum of in-file delta files during restore

Hide advanced option

NOTE

If this option is enabled this will result in additional restore time depending on the number of delta files.

9. This step applies only for restoring to **Alternate location**.

Enter the VMware host and access information of where you would like the VM to be restored to, then 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 / 6 / 6.5 / 6.7 / 7.0 ▼

Username

Administrator

Password

.....

Host Port

new_vcenter_host 443

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

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

Alternate location

VMware vCenter Server 6.5.0 build-5318154@10.16.8.40:443

Name

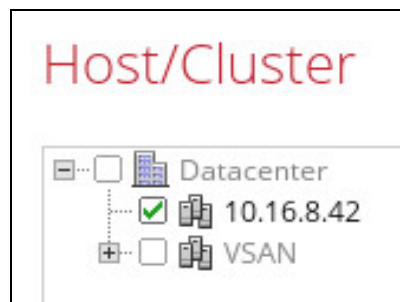
Inventory Location

Host/Cluster

Resource Pool

Storage

Select the host where the VM will be restored. Make sure to select a host not on the vSAN cluster.



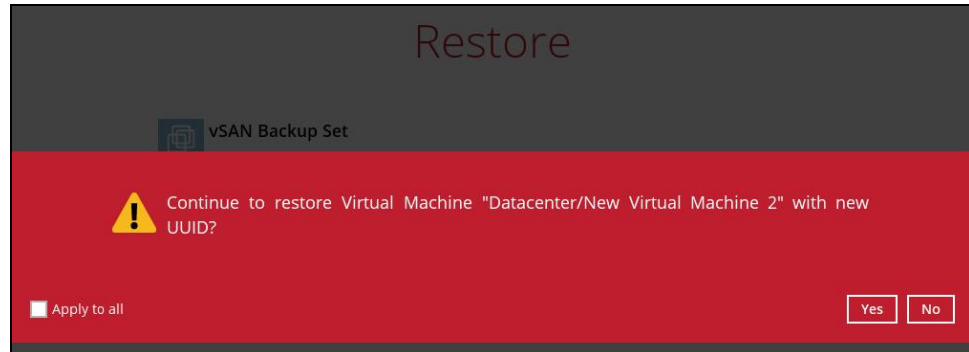
Select the storage.



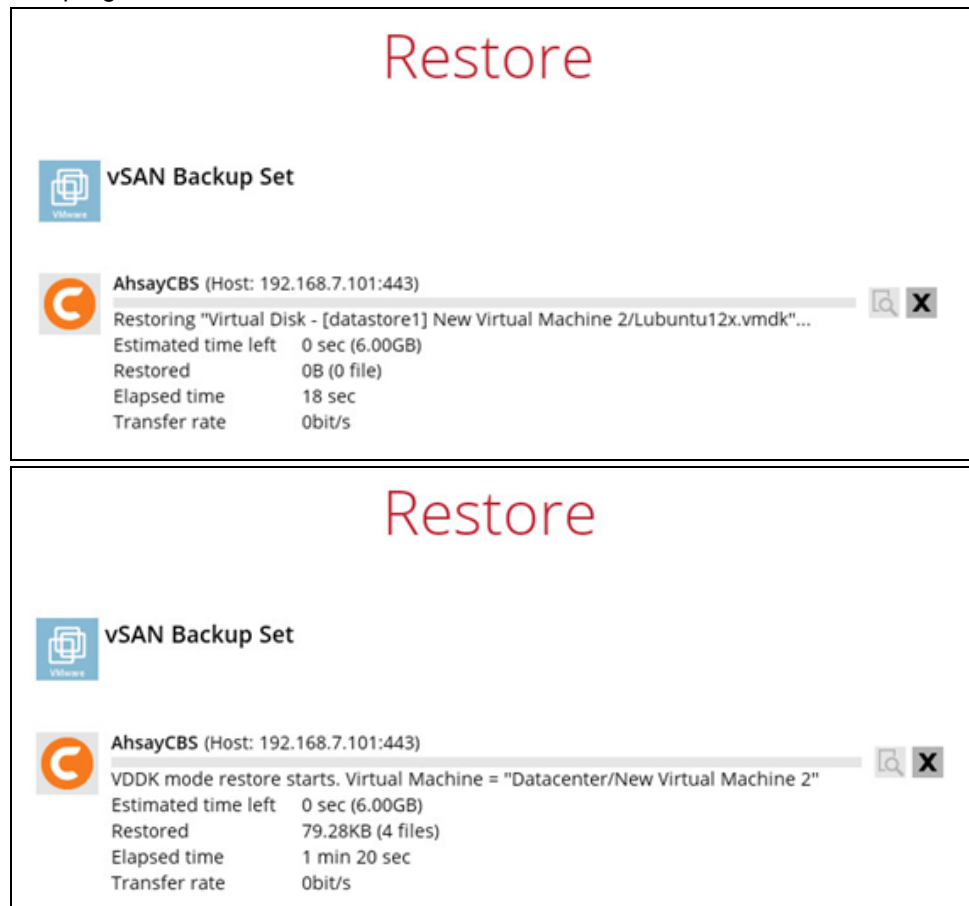
Click **Restore** to proceed when you are done with the settings.

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

- 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.



- The progress of the restore can be seen from the status bar.



Restore



vSAN Backup Set



AhsayCBS (Host: 192.168.7.101:443)

Restoring... C:\Users\Administrator\temp\RestoreSet\1614848659175\New VM\Hard ...

Estimated time left 3 min 3 sec (3.27GB)

Restored 2.73GB (4 files)

Elapsed time 5 min 35 sec

Transfer rate 76.58Mbit/s

Another way of checking the progress of the restore is from vSphere. The restore has started when a virtual disk was created, and it is completed when the virtual machine was reconfigured.

Recent Tasks		Alarms							
Task Name	Target	Status	Initiator	Queued For	Start Time	Completion T...	Server		
Create virtual disk		✓ Completed	VSPHERE.LOC...	6 ms	03/23/2021, 11:46:35 AM	03/23/2021, 11:47:00 AM	vCenter05-v65		
Refresh storage information	datastore1	✓ Completed	VSPHERE.LOC...	5 ms	03/23/2021, 11:47:02 AM	03/23/2021, 11:47:02 AM	vCenter05-v65		
Register virtual machine	Datacenter	✓ Completed	VSPHERE.LOC...	5 ms	03/23/2021, 11:47:12 AM	03/23/2021, 11:47:13 AM	vCenter05-v65		
Reconfigure virtual machine	New Virtu...	✓ Completed	VSPHERE.LOC...	7 ms	03/23/2021, 11:57:09 AM	03/23/2021, 11:57:10 AM	vCenter05-v65		

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

Restore



vSAN Backup Set



AhsayCBS (Host: 192.168.7.101:443)

Restore Completed Successfully

Estimated time left 0 sec

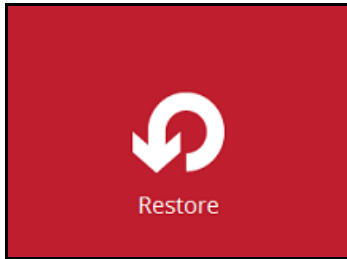
Restored 6.00GB (5 files)

Elapsed time 11 min 0 sec

Transfer rate 78.03Mbit/s

13.2.3 Restore from VMFS datastore to vSAN datastore

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



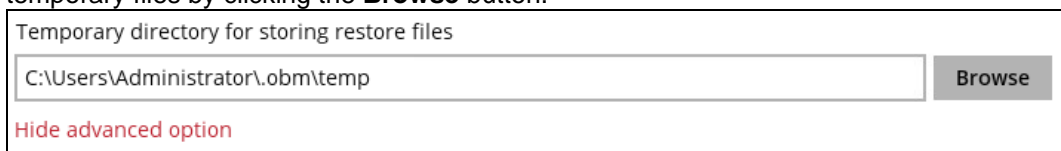
2. Select the backup set that you would like to restore the VM from.



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



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



4. If Granular Restore is enabled in the backup set, the following screen will be displayed. Select the Restore mode. Otherwise, proceed to the next step.

Please Choose A Restore Mode

Restore mode


☒ Restore virtual machines

☐ Restore individual files inside virtual machine (Granular Restore)

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

☐ Show backup job(s) outside retention

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

 All backup jobs will be shown, including the backup jobs which have been deleted. Some of the data may not be restorable. Do you wish to continue?

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

Select Your Virtual Machines To Be Restored

Select what to restore

Choose from files as of job 03/10/2021 Latest ☐ Show backup job(s) outside retention

Folders	Name	Size	Date modified
Local-1	Hard disk 1		
vCenter05-v65	win server 2016.nvram	8KB	03/09/2021 15:29
Datacenter	win server 2016.vmsd	0B	03/10/2021 14:12
Hosts and Clusters	win server 2016.vmx	3KB	03/10/2021 14:12
10.16.8.42			
win serv			

7. Select to restore the VM to an **Alternate location** (to another datastore on the original VMware host or another VMware host). If the backup set has Run Direct enabled, the **Run Direct** option will be enabled by default. Disable the **Run Direct** option.

Choose Where The Virtual Machines

Restore virtual machines to

☐ Original location

☒ Alternate location

☐ Run Direct

Show advanced option

8. Click **Show advanced option** if you would like to enable **Verify checksum of in-file delta files during restore**.

Choose Where The Virtual Machines

Restore virtual machines to

☐ Original location

☒ Alternate location

☐ Run Direct

Show advanced option

☐ Verify checksum of in-file delta files during restore

Hide advanced option

NOTE

If this option is enabled this will result in additional restore time depending on the number of delta files.

9. This step applies only for restoring to **Alternate location**.

Enter the VMware host and access information of where you would like the VM to be restored to, 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 / 6 / 6.5 / 6.7 / 7.0 ▼

Username

Administrator

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 **Host/Cluster** and **Storage** settings to select the alternate vSAN datastore, according to where you would like the VM to be restored to.

Alternate location

VMware vCenter Server 6.5.0 build-5318154@10.16.8.40:443

Name

Inventory Location

Host/Cluster

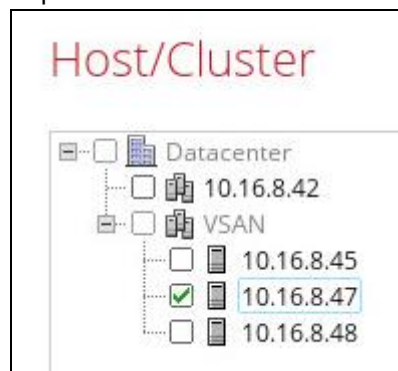
Resource Pool

Storage

NOTE

It is important to select the vSAN cluster where the VM will be restored even if it is in the same vCenter.

Expand the vSAN to be able to select the host.



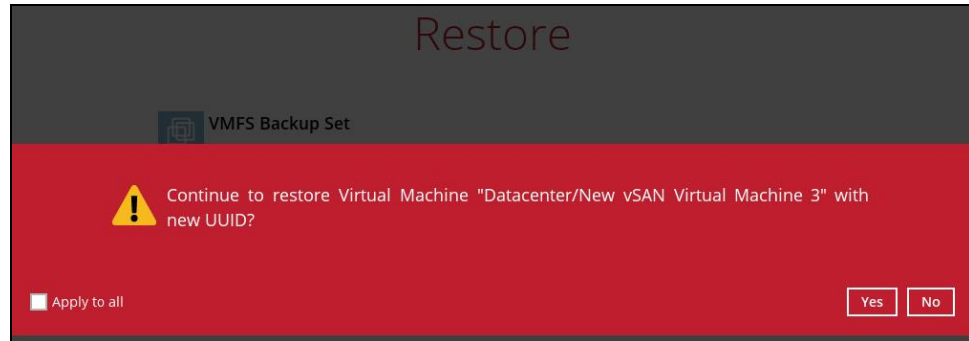
Select the vSAN storage.



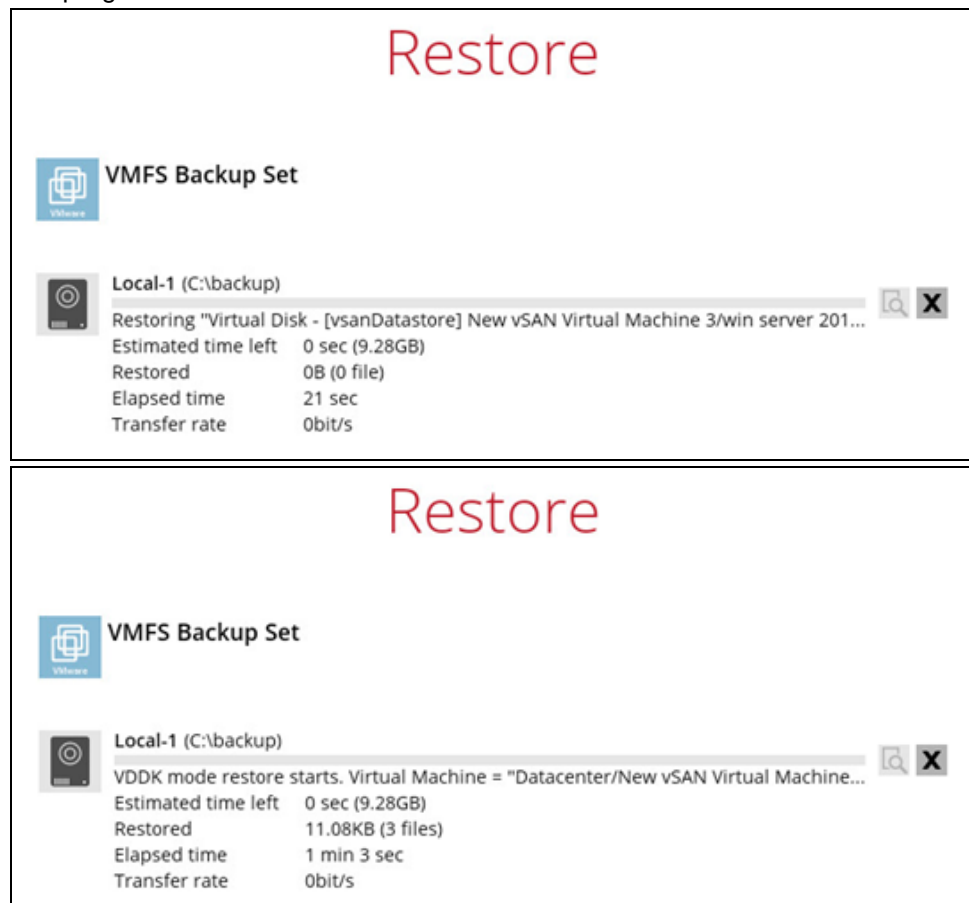
Click **Restore** to proceed when you are done with the settings.

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

- 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.



- The progress of the restore can be seen from the status bar.



Restore



VMFS Backup Set



Local-1 (C:\backup)

Restoring... C:\Users\Administrator\temp\RestoreSet\1615362674408\win server 201...




Estimated time left 12 min 2 sec (6.15GB)

Restored 3.13GB (3 files)

Elapsed time 19 min 59 sec

Transfer rate 36.57Mbit/s

Another way of checking the progress of the restore is from vSphere. The restore has started when a virtual disk was created, and it is completed when the virtual machine was reconfigured.

Recent Tasks		Alarms						
Task Name	Target	Status	Initiator	Queued For	Start Time	Completion T...	Server	
Create virtual disk		✔ Completed	VSPHERE.LOC...	6 ms	03/23/2021, 2:03:08 PM	03/23/2021, 2:03:09 PM	vCenter05-v65	
Refresh storage information	 vsanDatas...	✔ Completed	VSPHERE.LOC...	6 ms	03/23/2021, 2:03:14 PM	03/23/2021, 2:03:15 PM	vCenter05-v65	
Register virtual machine	 Datacenter	✔ Completed	VSPHERE.LOC...	6 ms	03/23/2021, 2:03:25 PM	03/23/2021, 2:03:28 PM	vCenter05-v65	
Reconfigure virtual machine	 New vSAN...	✔ Completed	VSPHERE.LOC...	9 ms	03/23/2021, 2:51:26 PM	03/23/2021, 2:51:30 PM	vCenter05-v65	

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

Restore



VMFS Backup Set



Local-1 (C:\backup)

✓ Restore Completed Successfully

Estimated time left 0 sec

Restored 9.28GB (4 files)

Elapsed time 44 min 32 sec

Transfer rate 29.87Mbit/s

14 Contact Ahsay

14.1 Technical Assistance

To contact Ahsay support representatives for technical assistance, visit the Partner Portal:
<https://www.ahsay.com/partners/>

Also use the Ahsay Wikipedia for resource such as Hardware Compatibility List, Software Compatibility List, and other product information:
<https://wiki.ahsay.com/>

14.2 Documentation

Documentations for all Ahsay products are available at:
https://www.ahsay.com/jsp/en/downloads/ahsay-downloads_documentation_guides.jsp

You can send us suggestions for improvements or report on issues in the documentation by contacting us at:
<https://www.ahsay.com/partners/>

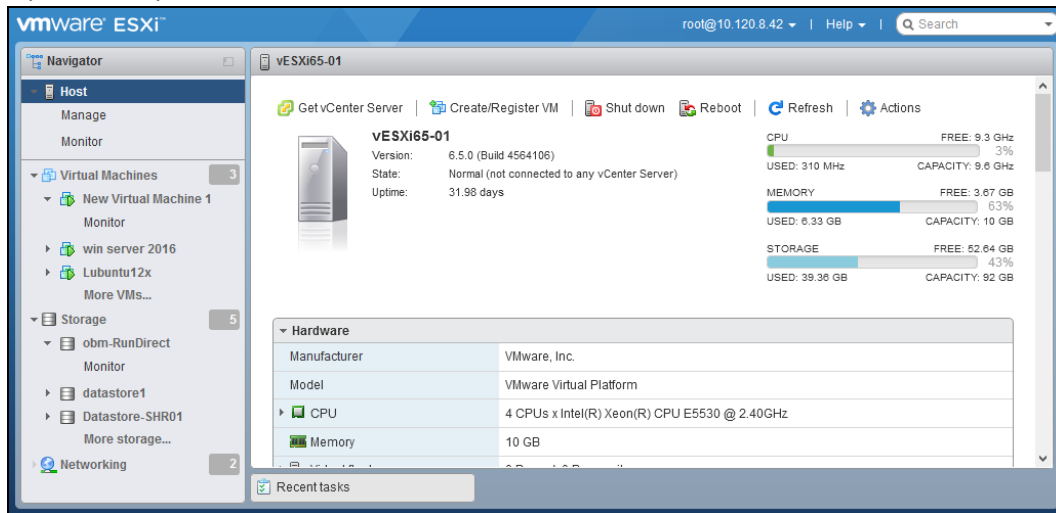
Please specify the specific document title as well as the change required/suggestion when contacting us.

Appendix

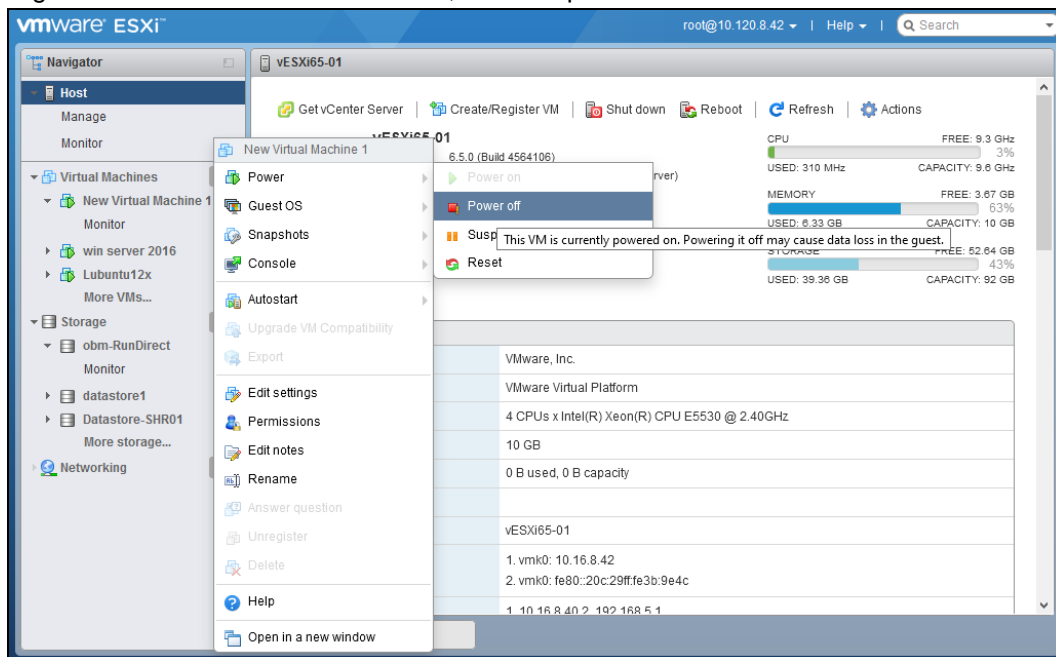
How to clean up the temporary files on VMware Host when Run Direct terminates unexpectedly

When Run Direct encounters a restore error or AhsayOBM crashes during Run Direct restore which leave behind settings on the VMware host, the temporary RunDirect files on the VMware Host must be cleaned manually. Follow the steps below on how to do this:

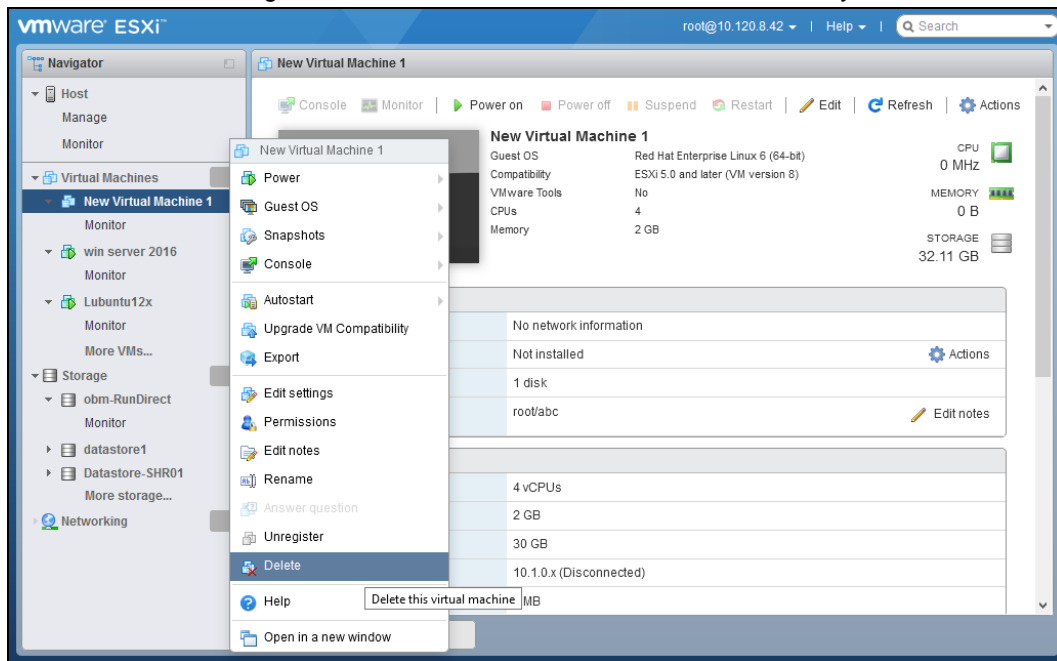
1. Open the vSphere Client or Web Client where the RunDirect VM is located.



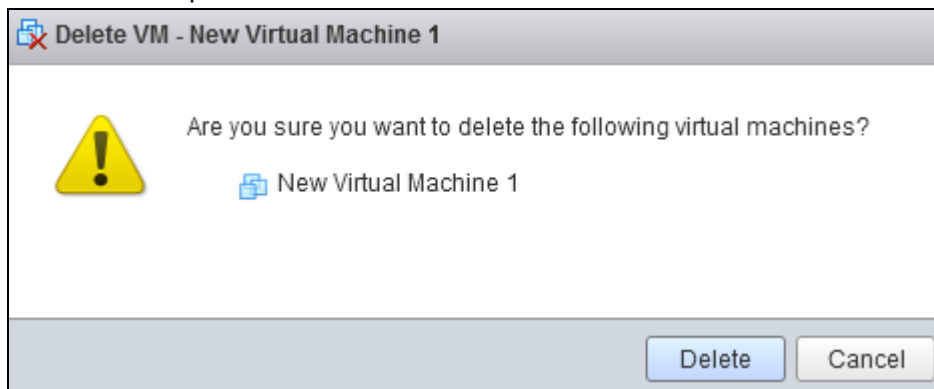
2. Right click the affected RunDirect VM, for example “New Virtual Machine 1” and select **Power off**.



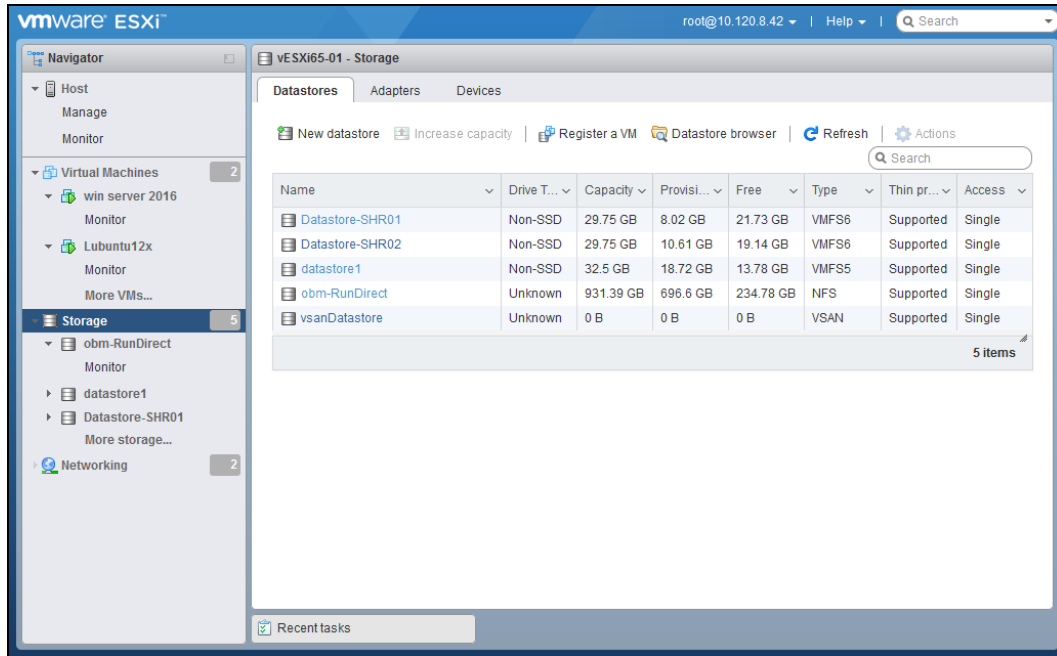
3. Right-click the failed RunDirect VM, for example “New Virtual Machine 1” and select **Remove from Inventory** or **Delete** to remove the RunDirect VM and temporary files remaining on the client machine if changes made on the RunDirect VM is not needed anymore.



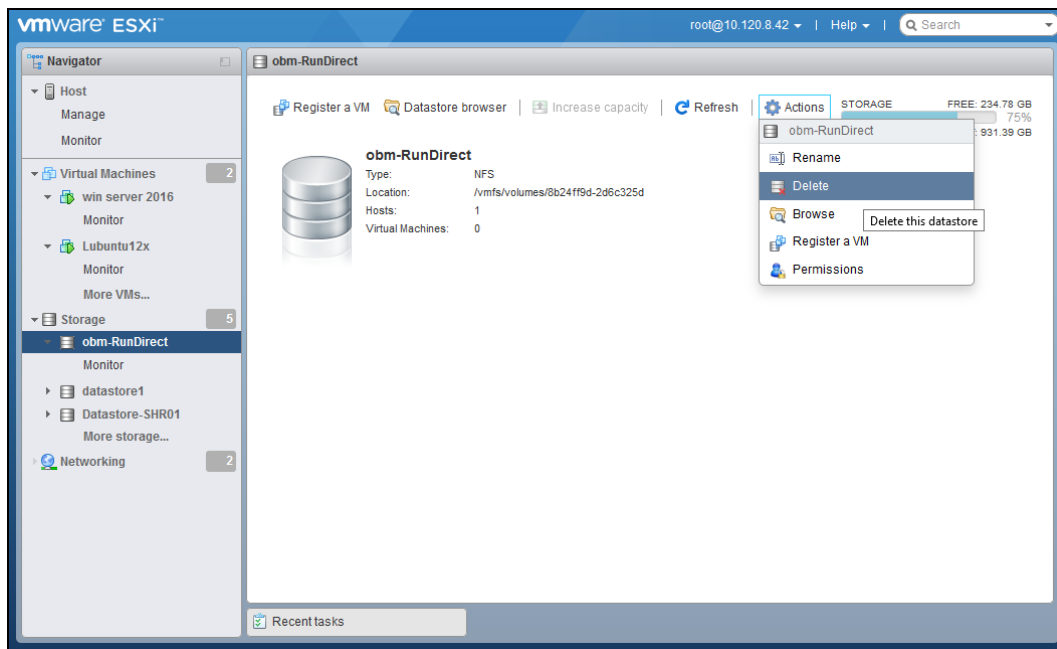
Click **Delete** to proceed.



4. Go to the storage list of ESXi server where NFS server is mounted.



5. Click the NFS datastore with name “obm-RunDirect” or similar name, then click **Actions** and **Delete** to remove the NFS datastore.



Click **Confirm** to delete the datastore.

