Ahsay Backup

Ahsay Online Backup Manager v8

VMware vCenter/ESXi Guest Virtual Machine Backup & Restore Guide

Ahsay Systems Corporation Limited

11 October 2021

Copyright Notice

Trademarks

Disclaimer

Revision History

Date	Descriptions	Type of modification
30 July 2020	Modified the Limitation for Non-VDDK Backup Mode in Ch. 2.3.2; Modified the OS Requirements in Ch. 3.5.7 and Ch. 5.4.4; Modified the Periodic Data Integrity Check (PDIC) diagram in Ch. 8; Added Network Drive Requirements in Ch. 5.4.6; Added Limitations in Ch. 5.5; Modified Best Practices and Recommendations in Ch. 4	New / Modifications
23 September 2020	Added VDDK Backup Mode Requirements in Ch. 3.7.3; Modified the Overview on the Backup Process and Periodic Data Integrity Check (PDIC) diagrams in Ch. 8	New / Modifications
25 January 2021	Updated screenshot in Ch. 3.5.2; Updated login steps in Ch. 6; Updated PDIC diagram in Ch. 8; Updated Ch. 3.5.7; Updated Ch. 3.4.2	Modification
25 March 2021	Added VDDK API changes in Ch. 2.4; Updated screenshot in Ch. 7, 9 , 11, 12 , 13 and 14; Added vSAN backup requirement in Ch. 3.9; Added restoring VM in vSAN in Ch 15; Added cleanup of temporary files in Appendix	New / Modification
7 April 2021	Updated Ch. 8; Added sub-chapters for the detailed process diagrams in Ch. 8.1, 8.2, 8.2.1, 8.2.2 and 8.3	New / Modifications
19 April 2021	Added the different vSAN setups in Ch. 3.5; Added vSAN requirements and limitations in Ch. 3.8; Added limitations in Ch. 15	New
30 April 2021	Removed Ch. 2.3.3 and merged it with Ch. 2.3.1; Updated notes of PDIC in Ch. 8.1	Modification
23 July 2021	Updated the system architecture diagram in Ch. 1.2	Modification
11 October 2021	Updated login instructions in Ch. 6	Modifications

Table of Contents

1 Overview

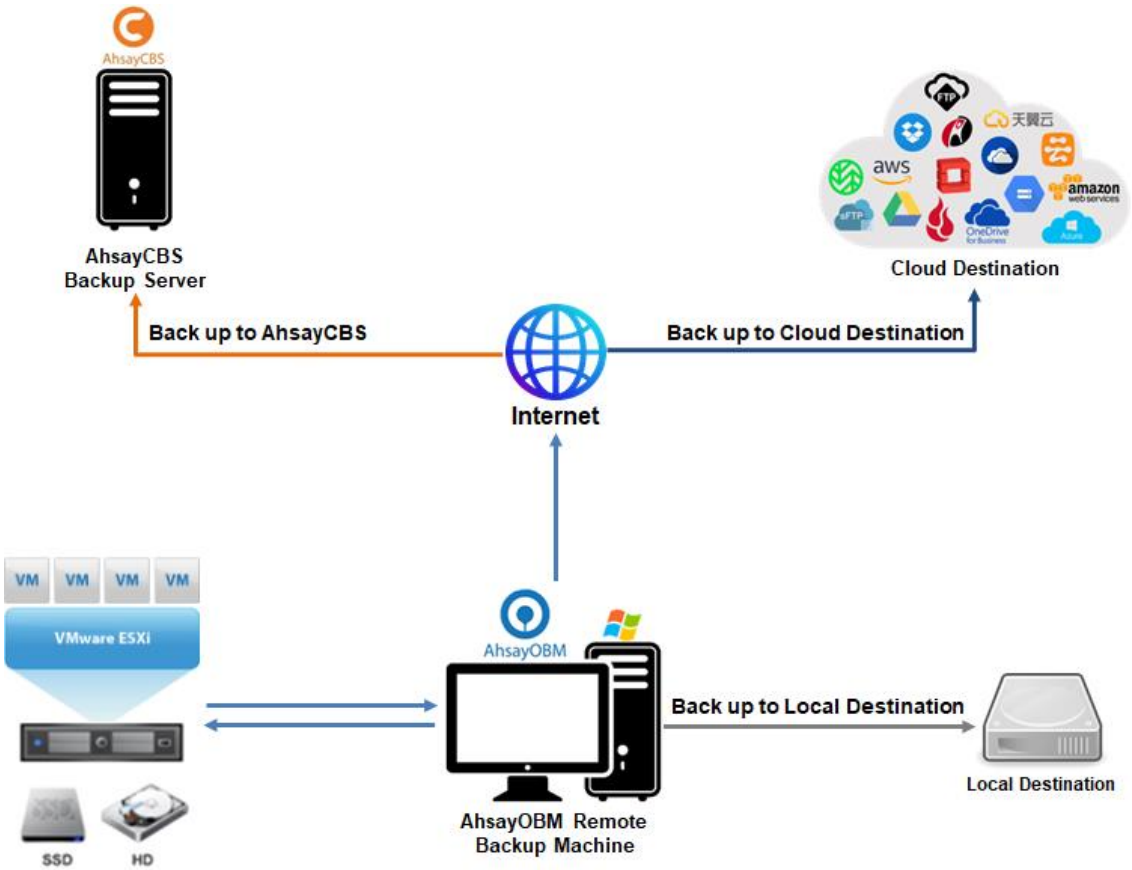
1.1 What is this software?

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

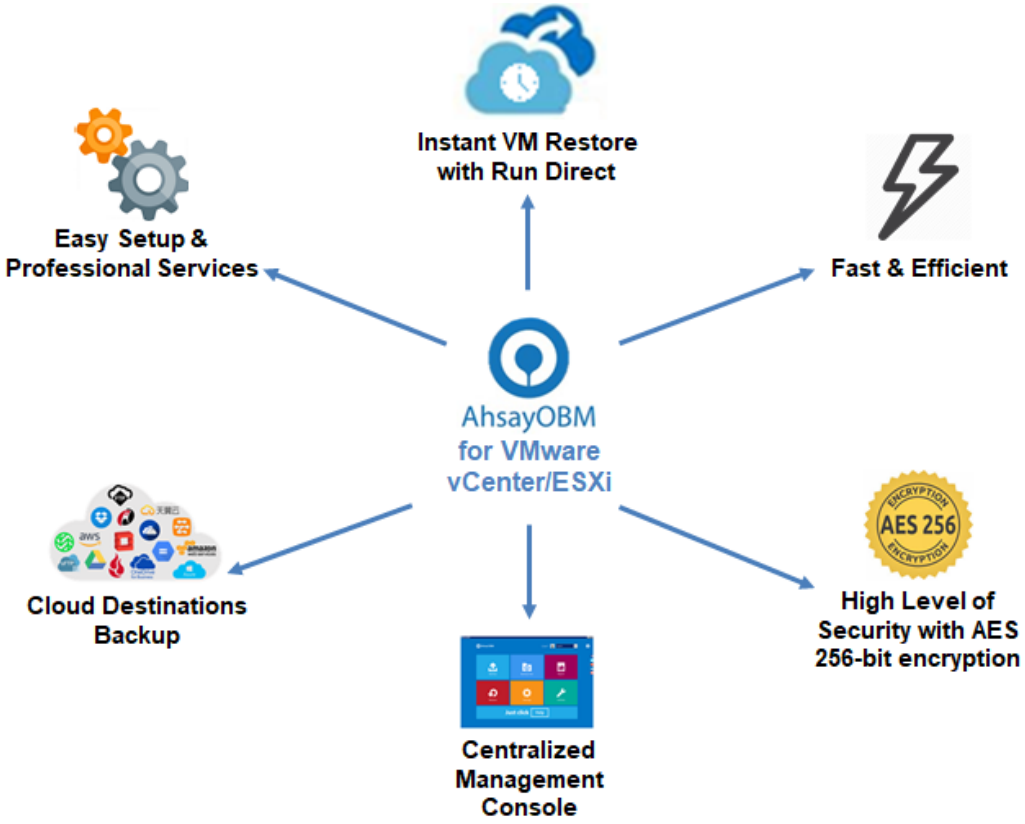
Below is the system architecture diagram illustrating the major elements involved in the backup process among the VMware server, AhsayOBM and AhsayCBS.

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

Professional Services

AhsayOBM Installation and Configuration Service

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

Valid Maintenance

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

Refer to our Professional Services webpage for further details and subscription.

Instant VM Restore with Run Direct

What is Run Direct?

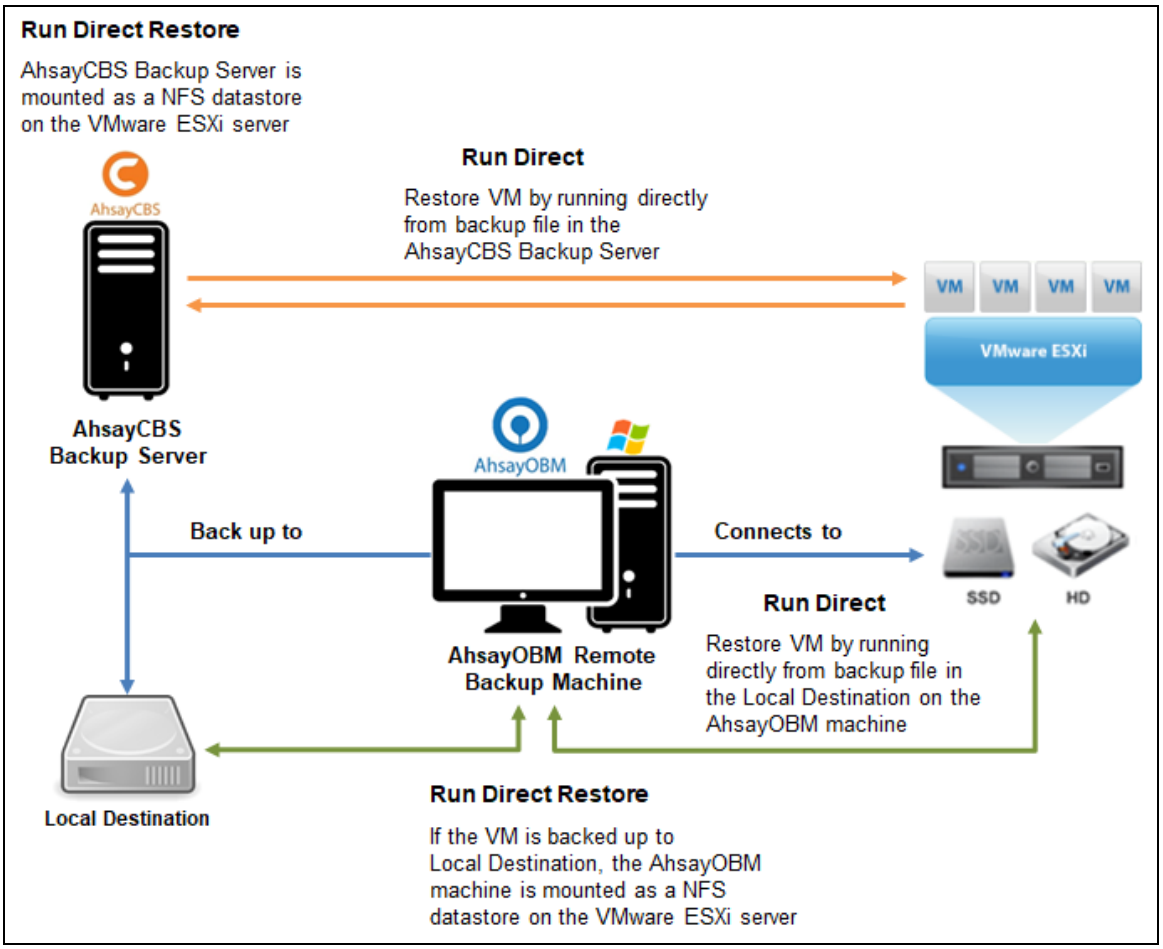
Run Direct is a feature that helps reduce disruption and downtime of your production VMs.

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

How does Run Direct work?

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

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



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

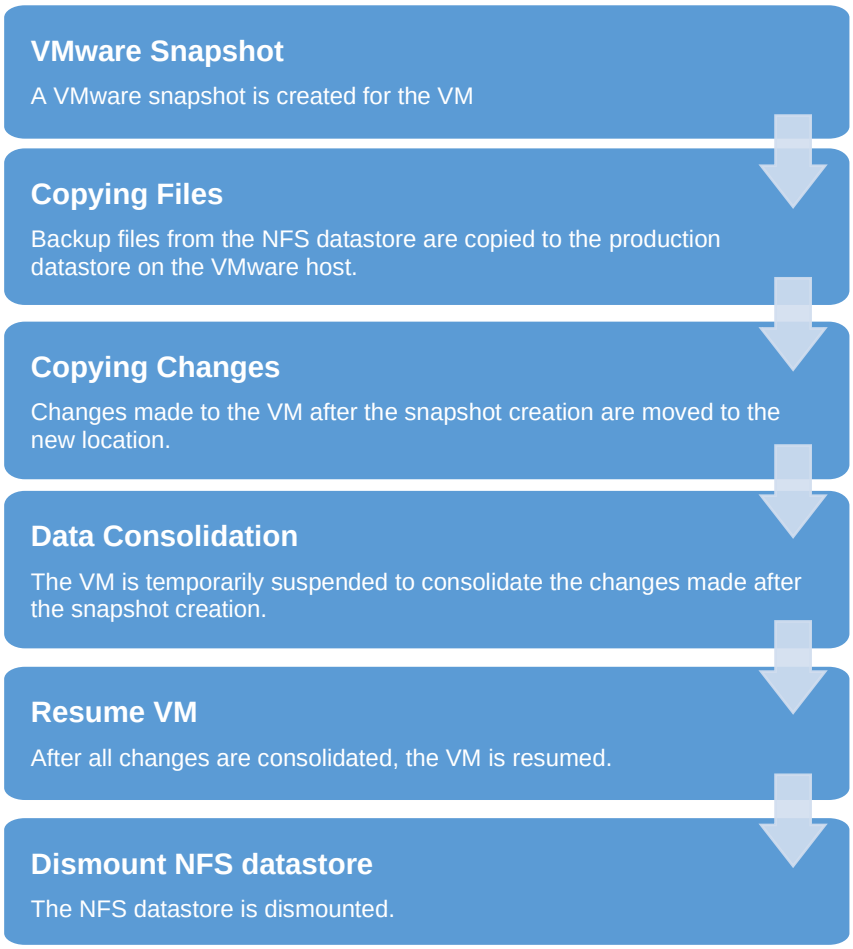
discarded, or the changes will be consolidated with the original virtual machine data when the restore is finalized.

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

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

Finalizing a VM Recovery (Migrating VM to permanent location)

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



NOTE

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

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

Fast and Efficient

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

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

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

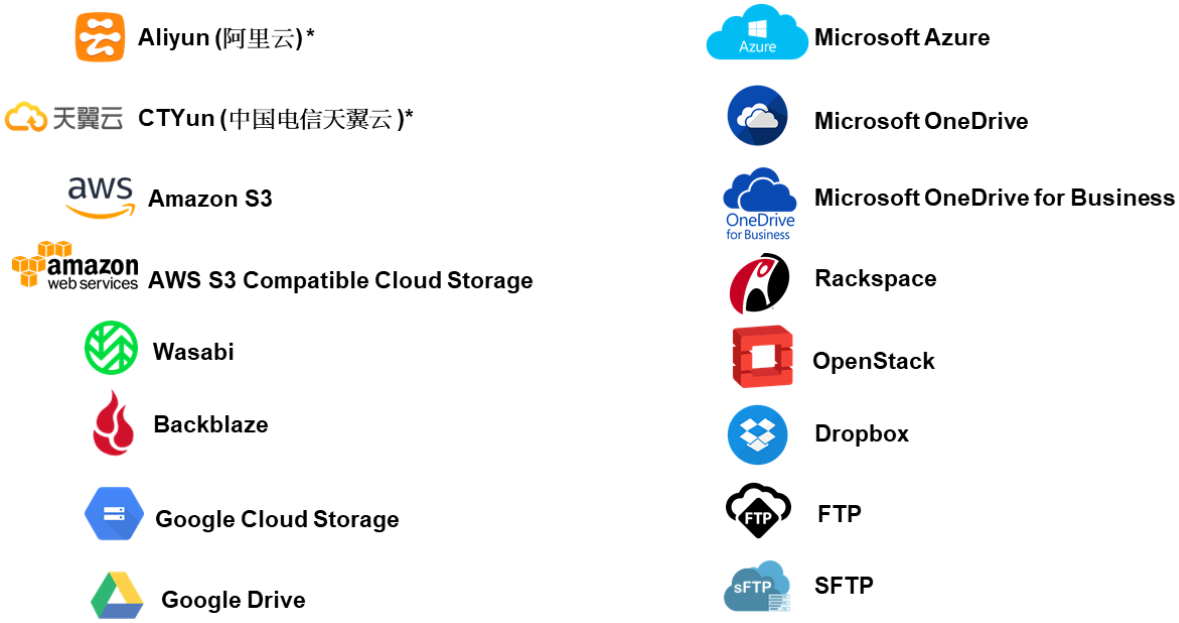
Centralized Management Console

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

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

Cloud Destinations Backup

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



* Available on computers with China or Hong Kong local settings

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

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

High Level of Security

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

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

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 differences between Non-VDDK and VDDK backup modes

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

Best Practices and Recommendations
Items recommended to pay attention to before backup and restore

Part 2: Performing VMware VM Backup

Creating a Backup Set
Log in to AhsayOBM and create backup set

Running a Backup Set
Run backup set & configure backup schedule for automated backup

Part 3: Performing VMware VM Restore

Restoring VM with Run Direct
Steps on performing a VM restore with Run Direct

Restoring VM without Run Direct
Steps on performing a VM restore without Run Direct

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 Modes

2.1 VMware Backup Modes

There are two backup modes available for VM backup:

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

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

The backup mode is chosen by AhsayOBM at the start of a backup according 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 Preparing for Backup and Restore.

2.1.1 Non-VDDK Backup Mode

For VM on free version of VMware hosts (except VMware vCenter/ESXi v7), and or if the backup machine where AhsayOBM is installed in a non-Windows operating system such as Linux or MacOS, then the backup is performed in non-VDDK mode. Backup in non-VDDK mode produces a backup chain that consists of a full file and a set of delta files:

- During the first backup, full files (e.g. virtual disk file (*.vmdk)) are created in the backup destination which is based on the provisioned size of the guest VM.
- During subsequent backups, if In-file delta - an AhsayOBM feature is employed to track only data blocks that have changed since the last backup, all changed data blocks are saved as incremental / differential delta files in the backup chain. The in-file delta generation is based on the provisioned size of the guest VM.

During a backup in non-VDDK mode, VM files are streamed to the Backup Client Computer for delta generation:

Pros	Free version of VMware ESXi is supported except VMware vCenter/ESXi v7.
Cons	Slower backup speed for subsequent backup compared to VDDK backup, as a result of the backup using the provisioned size for full and incremental backups instead of the actual used size. Run Direct is not supported.

2.1.2 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 compared to non-VDDK backup, as a result of backing up only the used size of your VM instead of the entire machine to enhance backup efficiency. This also helps with minimizing the storage size requirement and saving storage cost. Run Direct is supported.
Cons	Requires paid license, i.e. VMware Essentials License for usage of vSphere API. Requires VMFS5, VMFS6 or vSAN datastores to support full and incremental backups according to used size of the guest VM.

NOTE

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.

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

2.2 Features Comparison between VDDK and Non-VDDK Modes

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

2.3 VDDK and Non-VDDK Backup Mode Limitations

2.3.1 VDDK and Non-VDDK Backup Mode

- 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.

2.3.2 Non-VDDK Backup Mode

- VMware vCenter/ESXi 7 is only supported in Non-VDDK backup mode if the guest VM is powered off during a backup job.

- 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.

2.4 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. So starting with AhsayOBM v8.5.0.0 or above, Ahsay has decided to **temporarily revert to using VDDK 6 API** until the VDDK 7 API bus has been addressed by VMware.

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

- All new installation of AhsayOBM v8.5.0.0 or above
- AhsayOBM upgrades from v6, v7 or pre-v8.5.0.0 to v8.5.0.0 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 v8.5.0.0 or above. Once AhsayOBM is upgraded to v8.5.0.0 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 8.1 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 8.1 or above.

Refer to the following article for the list of compatible operating systems for Granular Restore:
FAQ: Ahsay Software Compatibility List (SCL) for Granular and OpenDirect Restore for version 8.1 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:
https://wiki.ahsay.com/doku.php?id=public:8014_suggestion_on_antivirus_exclusions

NOTE

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

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

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

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=displayKC&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

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

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

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

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

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

NOTE

Ports 443 and 902 are default ports for VMware.

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

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-consist 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.

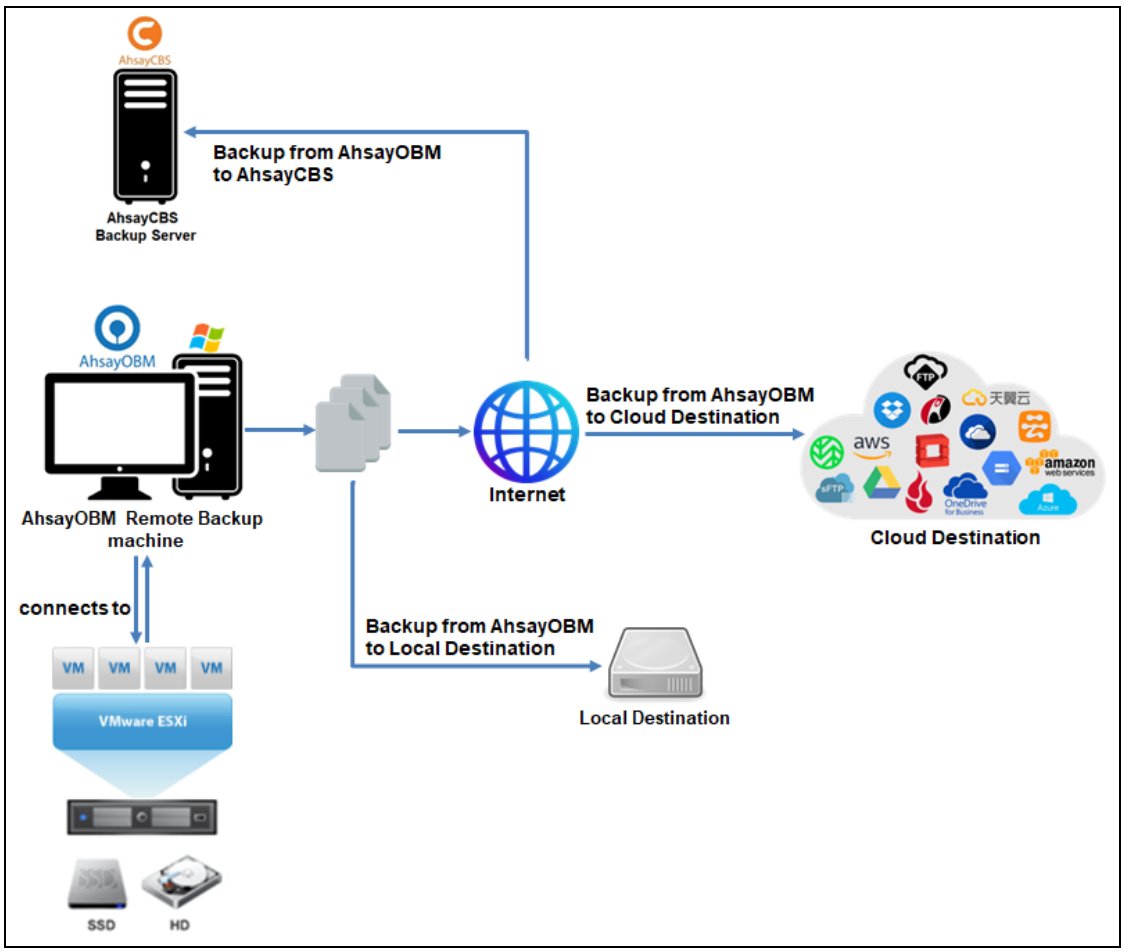
AhsayOBM installed on a Windows machine will allow support for VDDK backup mode, Run Direct, Granular Restore and vSAN Cluster.

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.



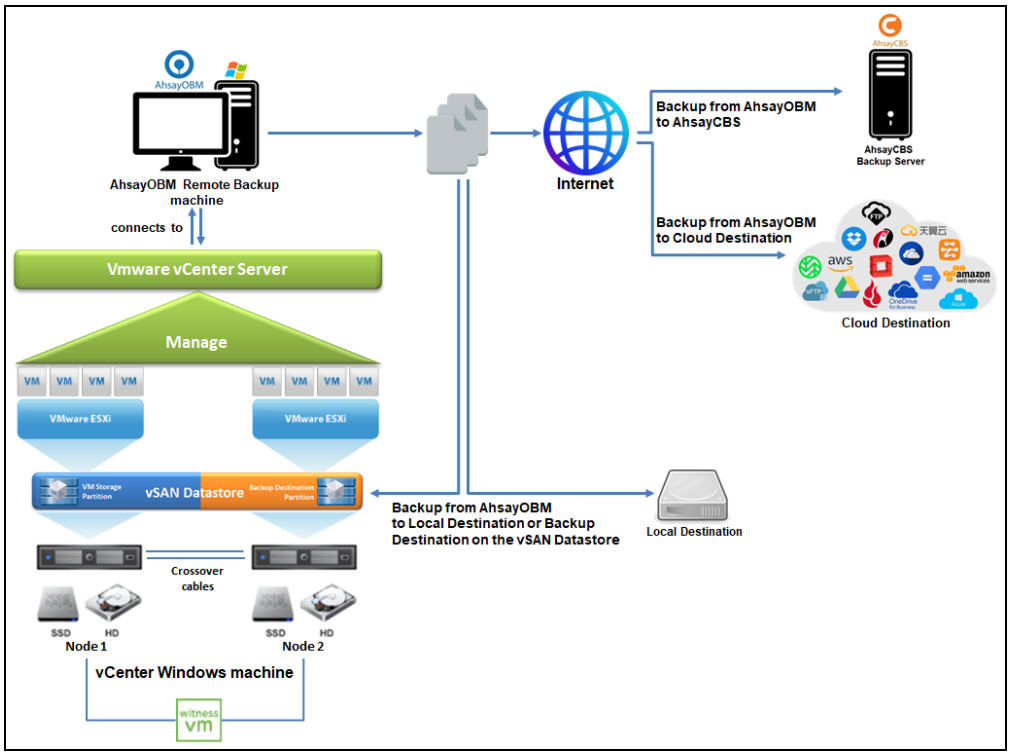
For environment with the following vSAN setup:

- Two Node vSAN Cluster
- Standard vSAN Cluster
- Stretched vSAN Cluster

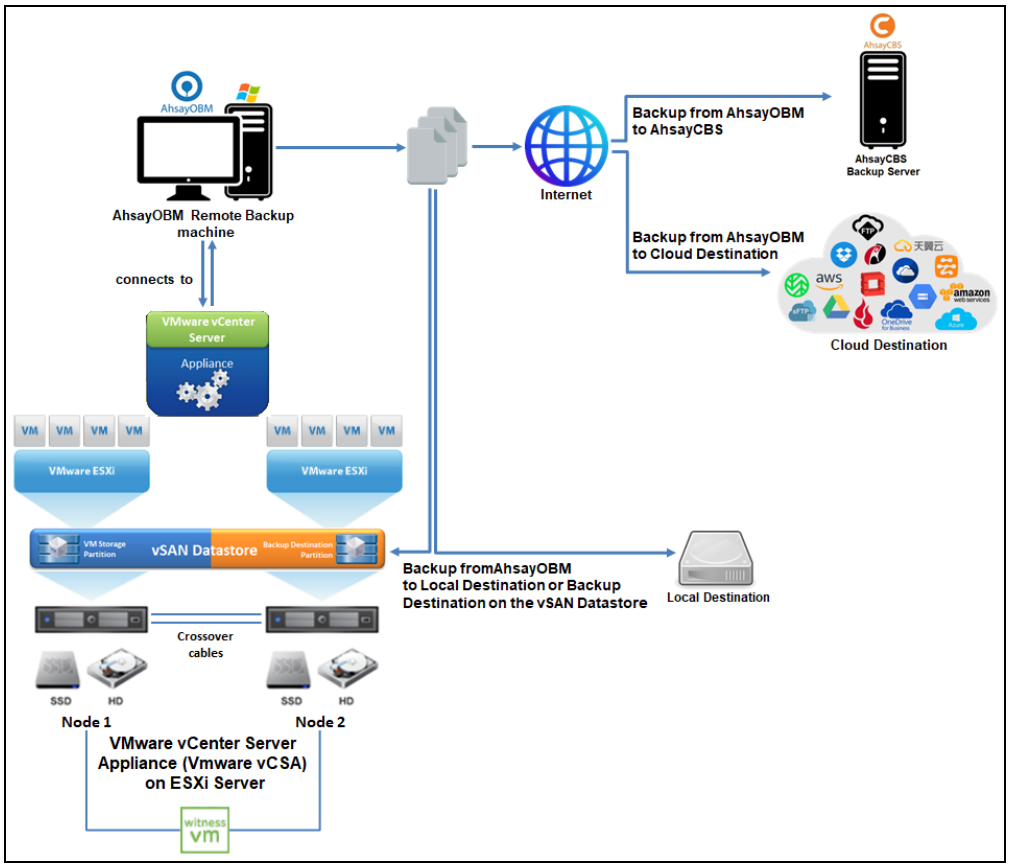
The AhsayOBM setup and deployment for Two Node and Standard vSAN Cluster are similar as they both are on one site.

The following are the two different setups using a 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.

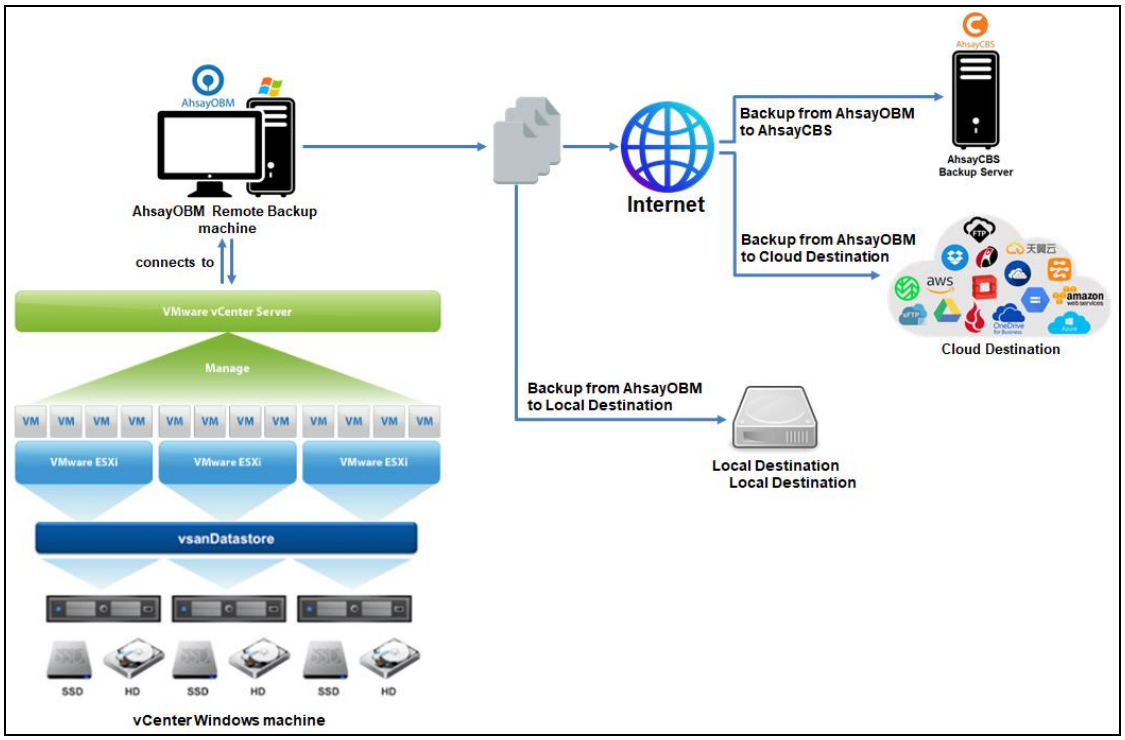


For VMware vCenter Server Appliance (vCSA) with Two Node vSAN Cluster setup, a separate Backup Client Computer must be prepared for AhsayOBM to be installed on.

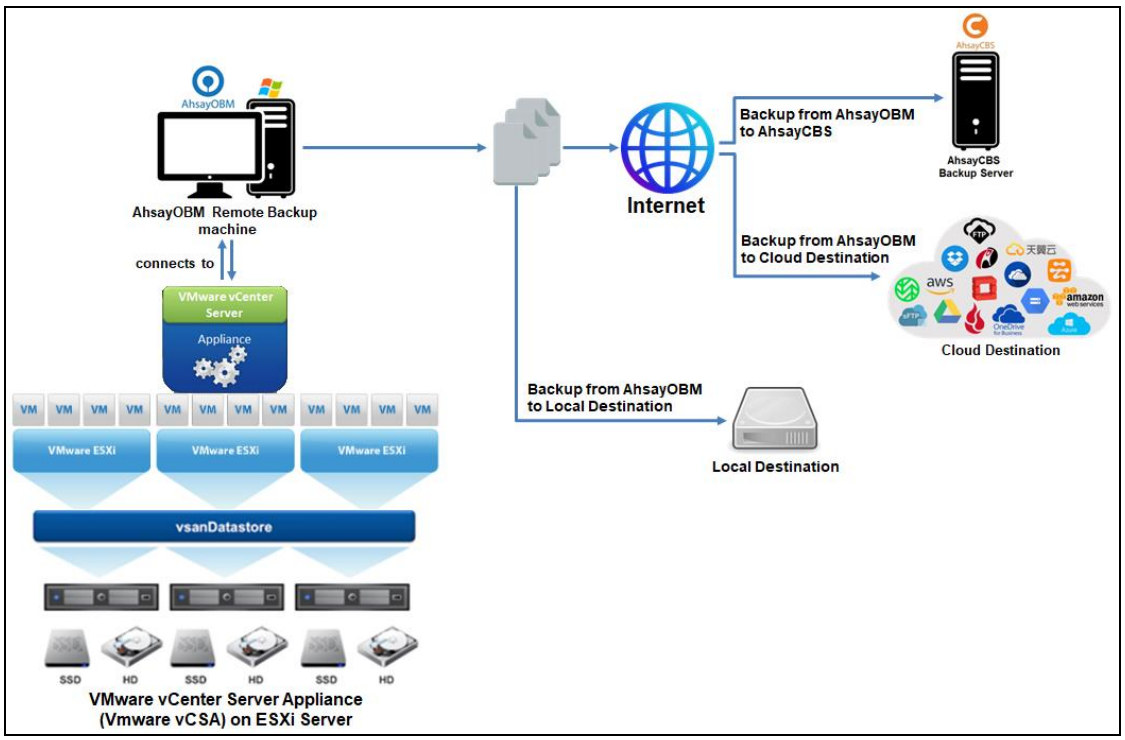


The following are the two different setups using a Standard vSAN Cluster:

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.

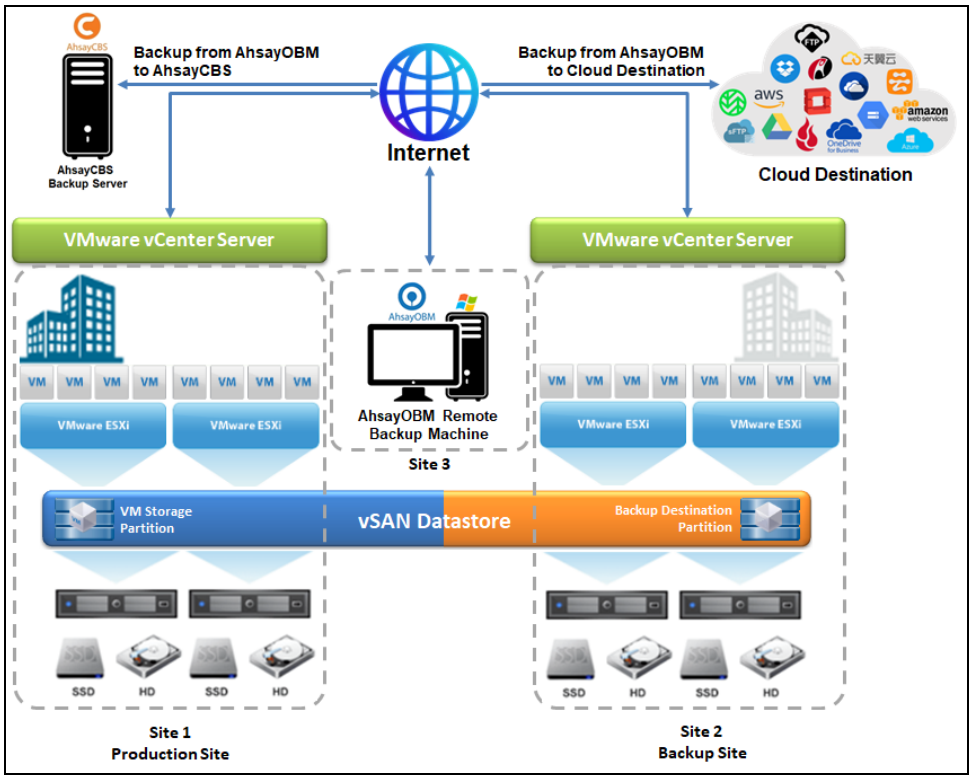


For VMware vCenter Server Appliance (vCSA) with Standard vSAN Cluster setup, a separate Backup Client Computer must be prepared for AhsayOBM to be installed on.

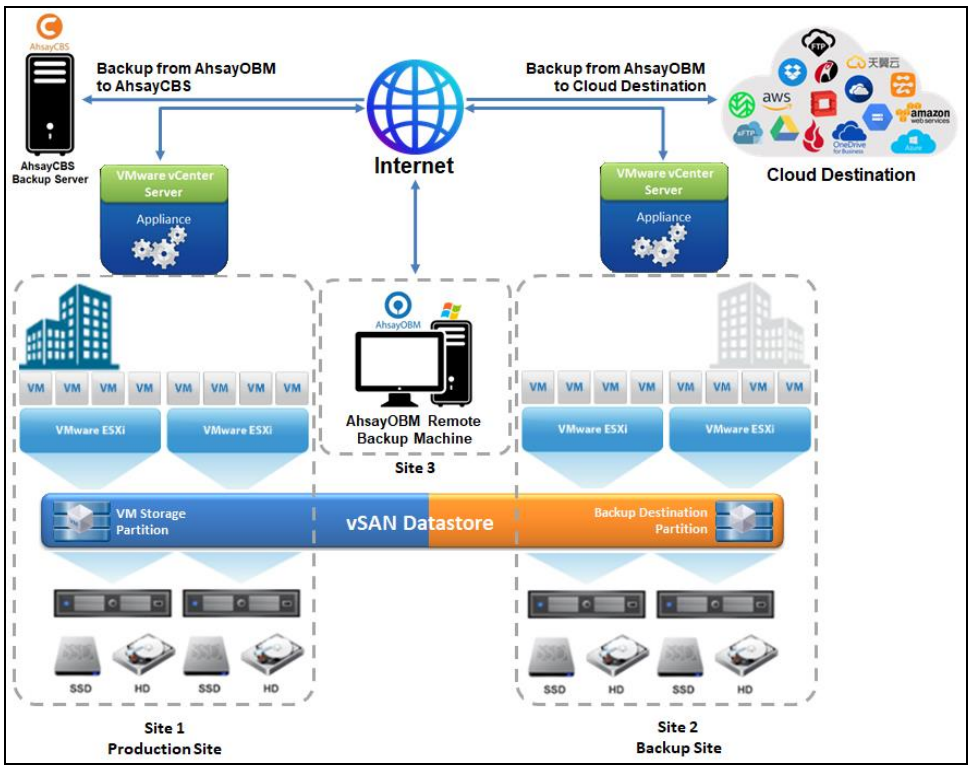


The following are the two different setups using a Stretched vSAN Cluster:

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.

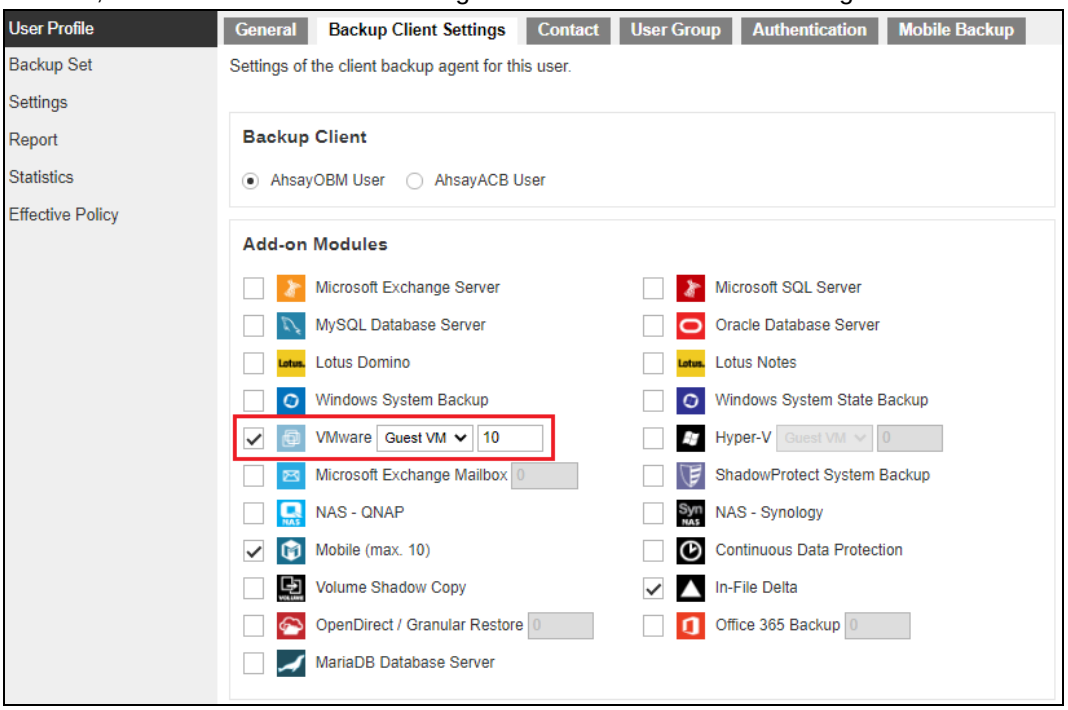


3.5.1 Hardware and Software Requirement

Ensure that the hardware and software requirements 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.



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 backup
  - VMware vCenter – calculated by the total number of guest VMs to backup
- 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. Just keep in mind to also include your future plans when making your decision. 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 link below for details on port usage:

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

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

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

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

NOTE

Ports 443 and 902 are default ports for VMware.

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

3.5.5 Backup Client Computer on Linux

For Backup Client Computer running on Linux operating system platform, 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 is 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 calculation of disk space is like the following:

(Total File Size * Delta Ratio) * number of backup destinations = **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.

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

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

3.5.7 Windows OS Requirement for VDDK and Non-VDDK Modes Backup

Make sure AhsayOBM is installed on:

- 64-bit Windows OS if you will back up VM data from VMware vCenter/ESXi 6.5 or above in VDDK mode. For VMware vCenter/ESXi 7 or above in VDDK mode, AhsayOBM must be installed on Windows version: Windows 2012 / Windows 2012 R2 / Windows 2016 (including versions 1709 and 1803) / Windows 2019.
- Either 32-bit or 64-bit Windows OS if you will back up VM data from VMware vCenter/ESXi 6.5 or 6.7 in Non-VDDK mode (Free VMware version).

NOTE

VMware vCenter/ESXi 7 is only supported in Non-VDDK backup mode if the VM is powered off during a backup job.

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 the chapter on 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 data directly from the backup files in the backup destination.

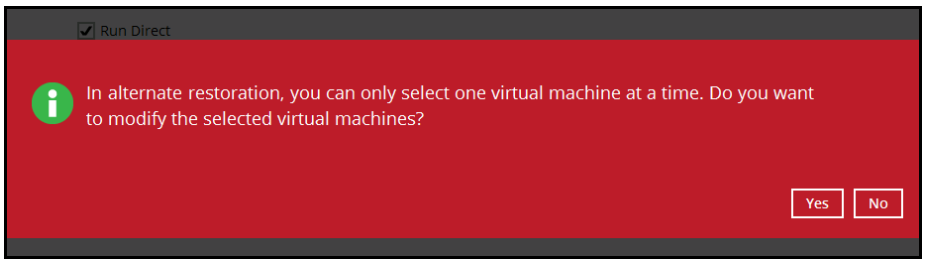
- Operation **System of the Backup Client Computer**

  - 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.

  - Consider creating 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 because 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 without a Run Direct backup destination, backup will be performed in non-VDDK mode.

For VM on free version of ESXi with a Run Direct backup destination, the following error message would be returned during a backup:
"Skip backing up Virtual Machine "name". Reason = "Run Direct is only support to VDDK backup mode"".

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

3.7.3 VMware CBT Known Issues

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@10.1.0.6:443(SSH: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.vmxf"...
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.

NOTE

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, however, backup sets which are upgraded from the previous versions are still supported.

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, 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

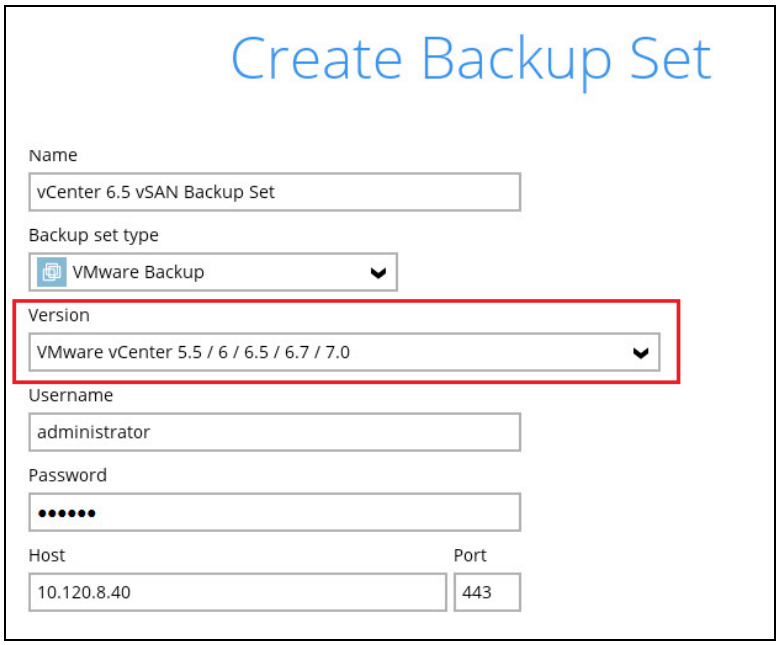
For VMs using vSAN datastore here are the requirements:

- 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. Here are the supported Windows operating systems:
  - Windows 7, 8, 8.1, 10
  - Windows 2012 x64 bit
  - Windows 2012 R2 x64 bit
  - Windows 2016 x64 bit
  - Windows 2019 x64 bit
- Backup set version must be VMware vCenter.



- 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 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.

4 Best Practices and Recommendations

Please consider the following recommendations:

- Use the latest version of AhsayOBM

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

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

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

  FAQ: Tips on how to setup the temporary directory for your backup set

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

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

- Backup the guest VMs to more than one destination

  To provide maximum data protection and recovery flexibility you should consider 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) if you are using non-VDDK backup mode.

  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 non-VDDK mode and or Granular restore, it is recommended to increase the Java heap size space to at least 4GB or above for optimal performance.

  Refer to the following KB article for further instruction:
  https://wiki.ahsay.com/doku.php?id=public:8011_faq:how_to_modify_the_java_heap_size_of_ahsayobc

- 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.

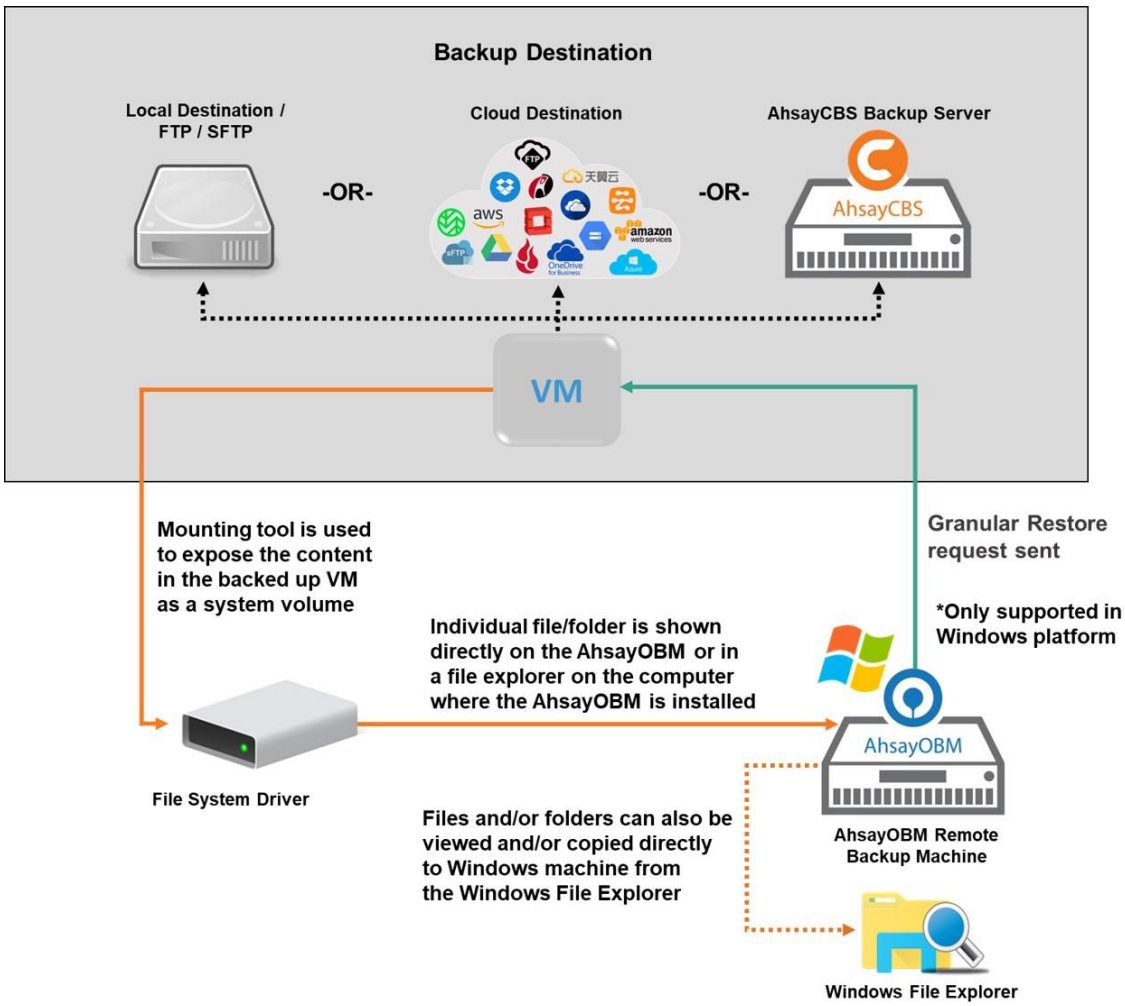
Granular restore is one of the available restore options for VMware ESXi/vCenter backup sets from AhsayOBM v8.1.0.0 or above. AhsayOBM makes use of granular restore technology to enable a file level restore from a virtual disk file (VDDK) of guest VM backup possible. It is particularly useful if you 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	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. ➢ **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. AhsayOBM must be installed on the following Windows Operating Systems:

Windows 2008 R2 SP1 or above	Windows 2012	Windows 2012 R2
Windows 2016	Windows 7 SP1 or above	Windows 8
Windows 8.1	Windows 10	Windows 2019

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

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

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

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 Logging in to AhsayOBM

Starting with AhsayOBM v8.5.0.0, there are several login scenarios depending on the setting of the account you are using. The different scenarios will be discussed below:

- Login without 2FA
- Login with 2FA using authenticator app
- Login with 2FA using Twilio

6.1 Login to AhsayOBM without 2FA

1. Log in to the AhsayOBM application user interface.

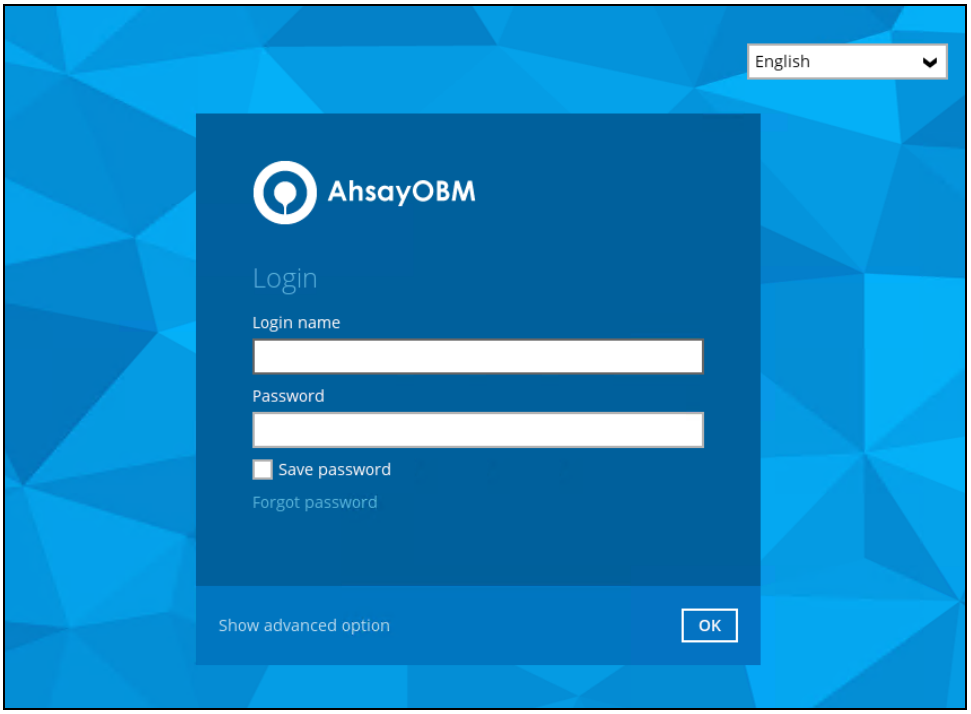
   For Backup Client Computer on Windows / Mac OS X, double-click the AhsayOBM desktop icon to launch the application.

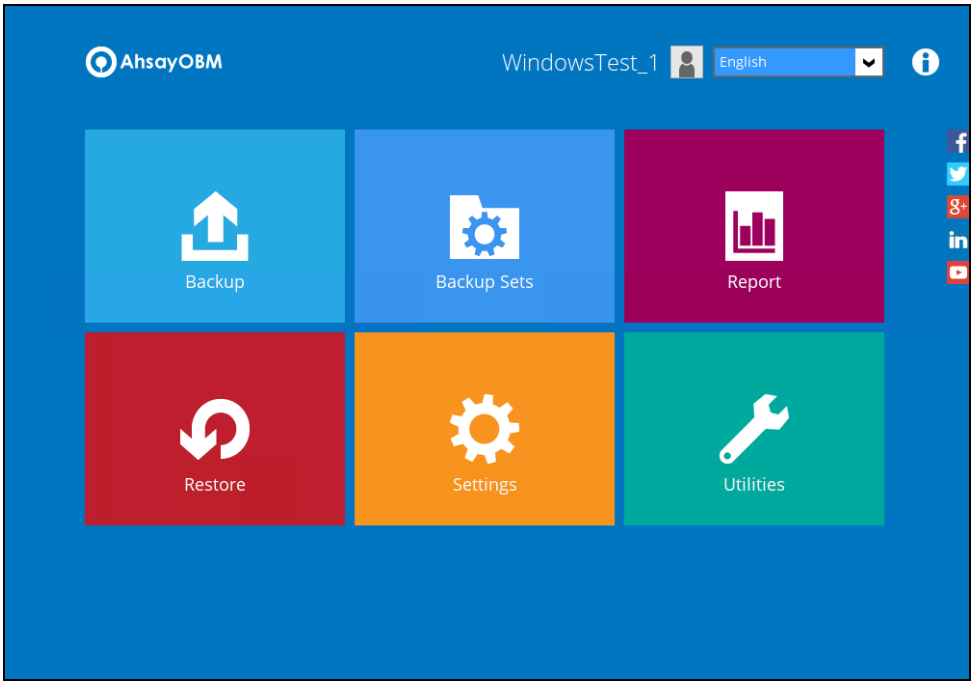
   For Backup Client Computer on Linux, enter the following command to launch the application user interface:

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

2. Enter the **Login name** and **Password** of your AhsayOBM account, then click **OK** to log in.

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



6.2 Login to AhsayOBM with 2FA using authenticator app

1. Log in to the AhsayOBM application user interface.

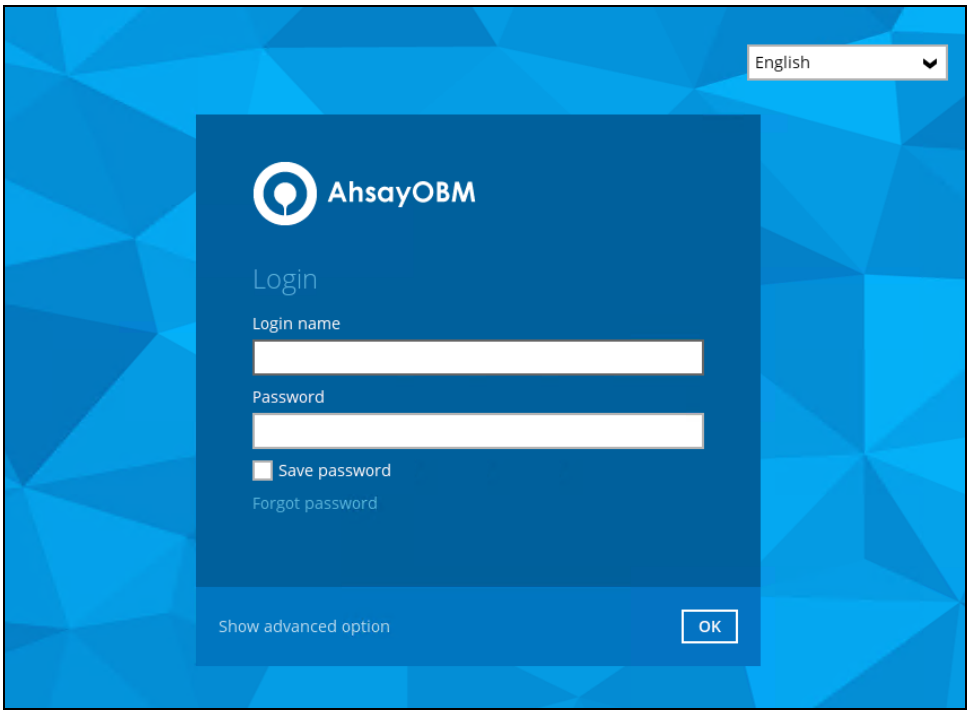
   For Backup Client Computer on Windows / Mac OS X, double-click the AhsayOBM desktop icon to launch the application.

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

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

2. Enter the **Login name** and **Password** of your AhsayOBM account, then click **OK** to log in.

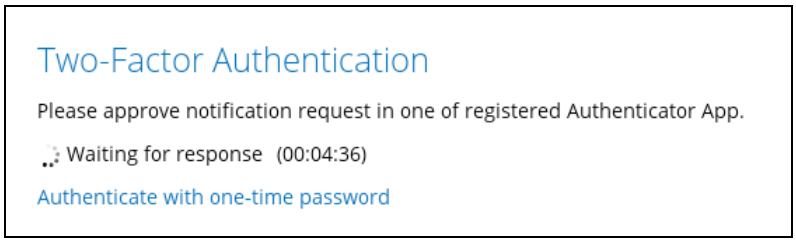
3. One of the two authentication methods will be displayed to continue with the login:

- Push Notification and TOTP when using Ahsay Mobile app
- TOTP only

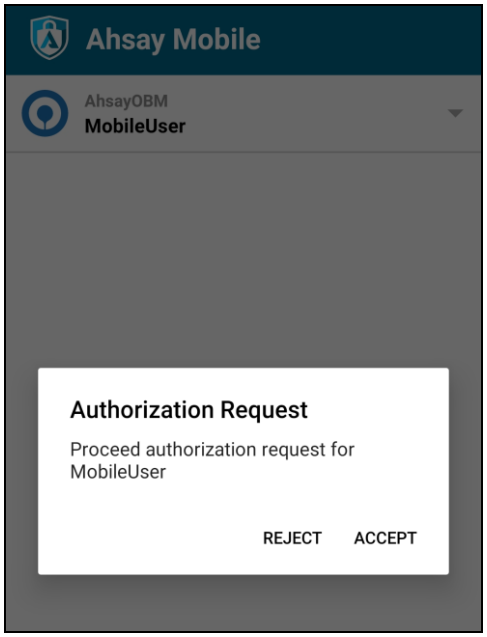
➢ If **Ahsay Mobile app** was configured to use Push Notification and TOTP, then there are two 2FA modes that can be used:

- Push Notification (default)

Push notification is the default 2FA mode. Accept the login request on Ahsay Mobile to complete the login.

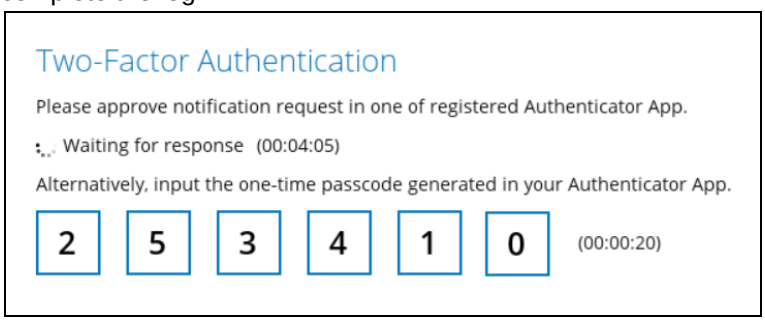


Example of the login request sent to the Ahsay Mobile app.

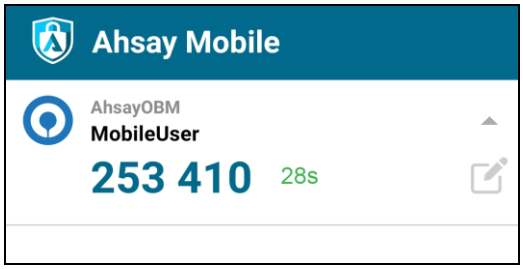


- TOTP

However, if push notification is not working or you prefer to use one-time passcode, click the Authenticate with one-time password link, then input the one-time passcode generated by Ahsay Mobile to complete the login.

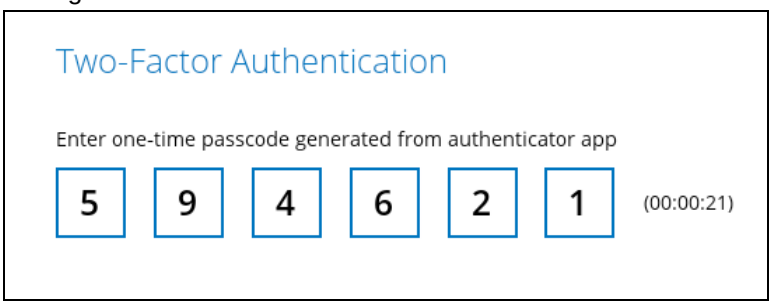


Example of the one-time passcode generated in the Ahsay Mobile app.

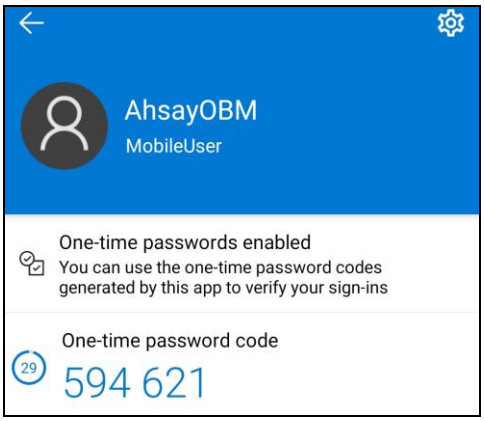


- TOTP only

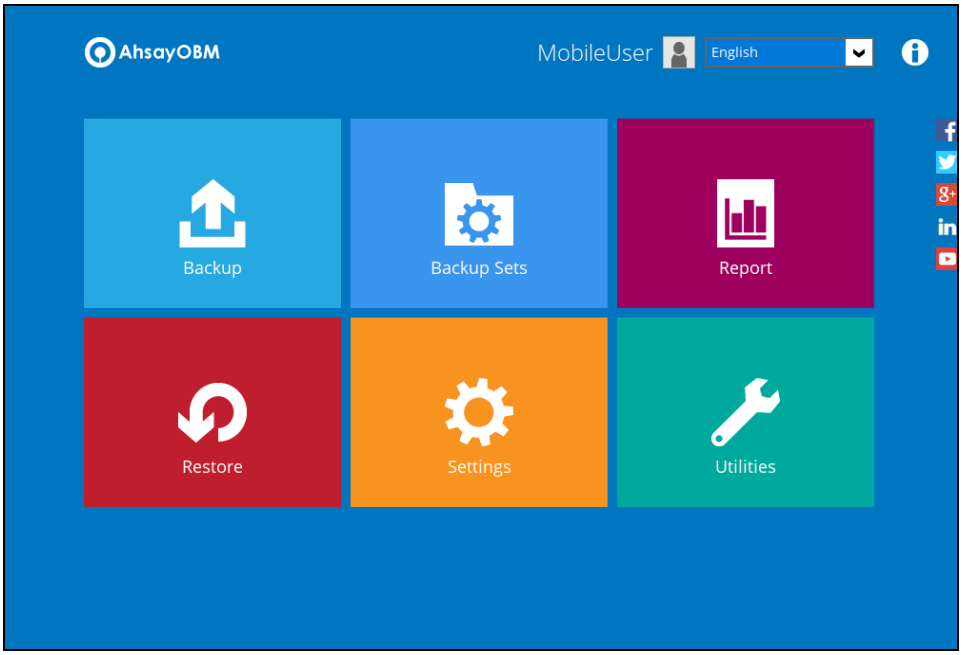
Enter the one-time passcode generated by the authenticator app to complete the login.



Example of the one-time passcode generated in the third-party authenticator app Microsoft Authenticator.



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



NOTE

If you have trouble logging in using the authenticator app, please refer to:

- Chapter 9 of the AhsayOBM Quick Start Guide for Windows
- Chapter 8 of the AhsayOBM Quick Start Guide for Mac
- Chapter 8 of the AhsayOBM Quick Start Guide for Linux (GUI)

6.3 Login to AhsayOBM with 2FA using Twilio

1. Log in to the AhsayOBM application user interface.

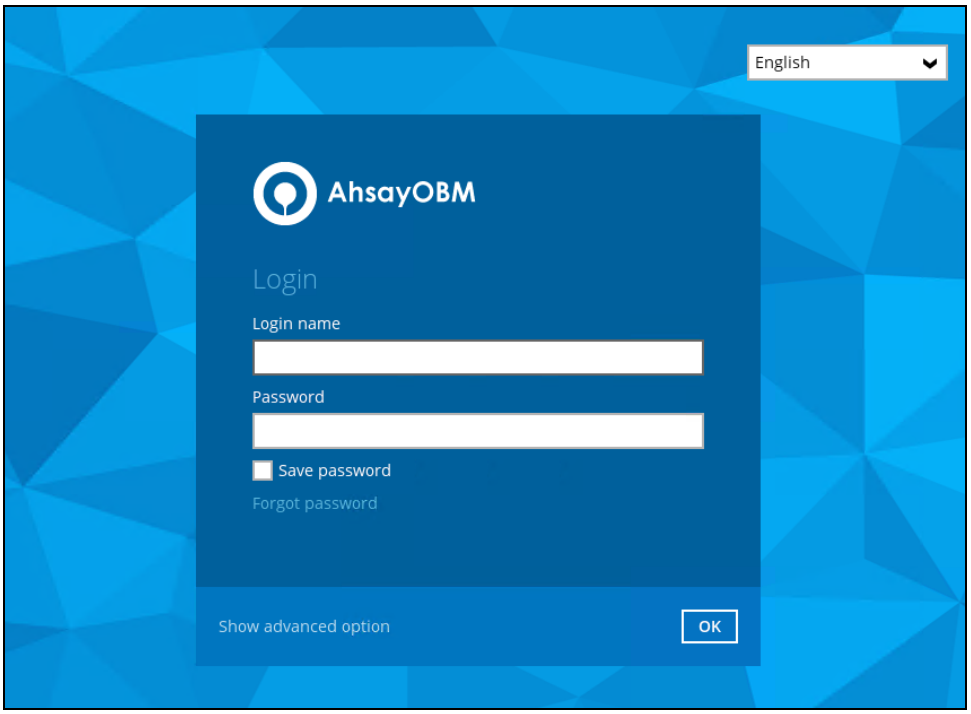
   For Backup Client Computer on Windows / Mac OS X, double-click the AhsayOBM desktop icon to launch the application.

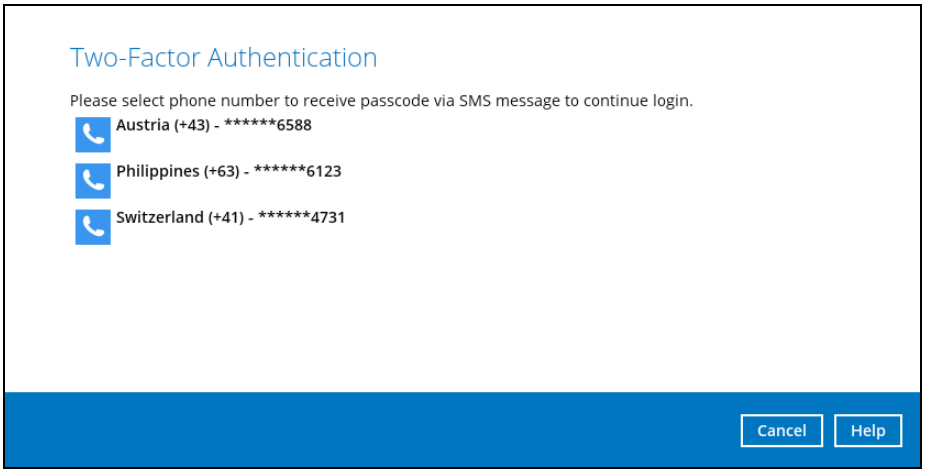
   For Backup Client Computer on Linux, enter the following command to launch the application user interface:

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

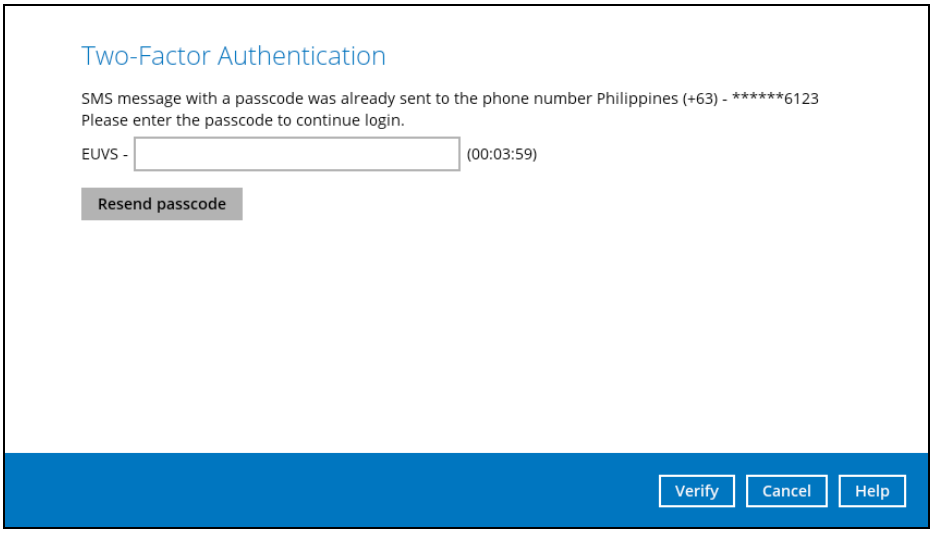
2. Enter the **Login name** and **Password** of your AhsayOBM account, then click **OK** to log in.

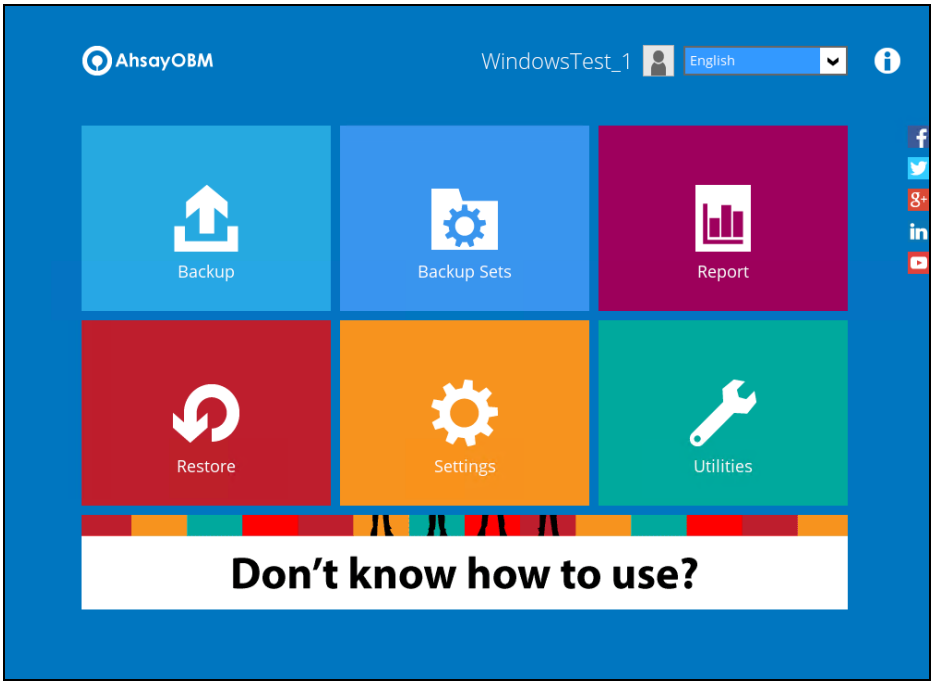
3. Select your phone number.



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

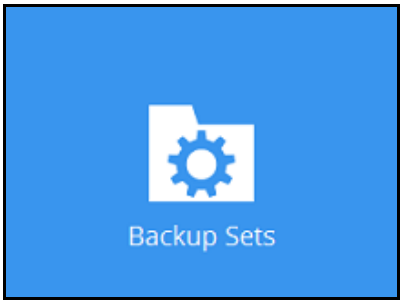


5. After successful login, the following screen will appear.



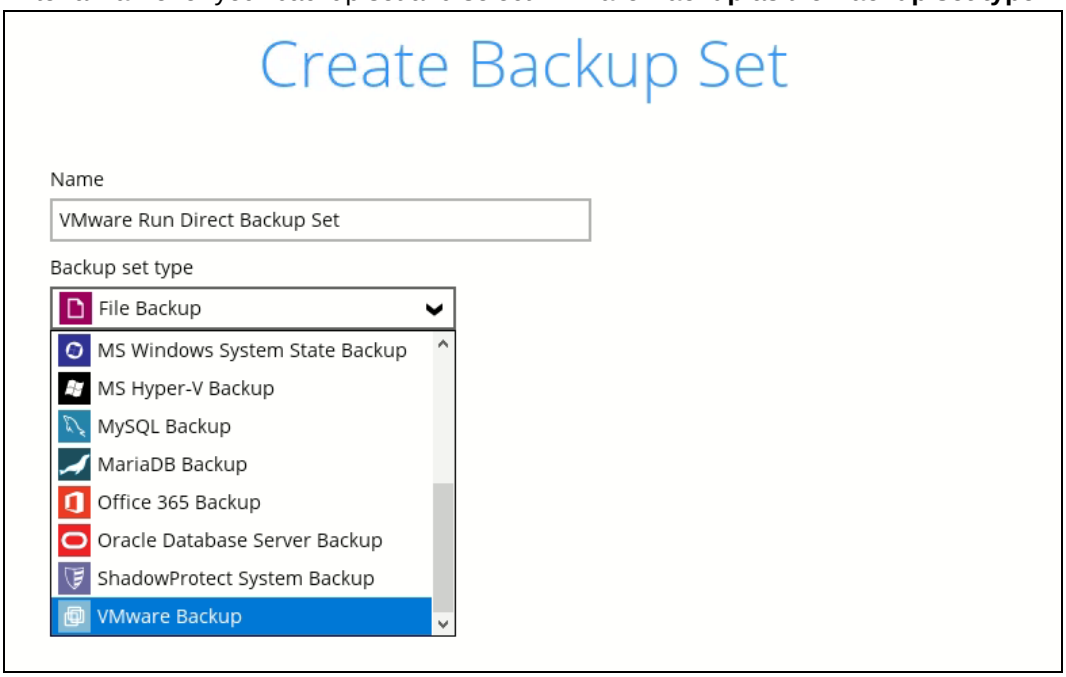
7 Creating a VMware VM Backup Set

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

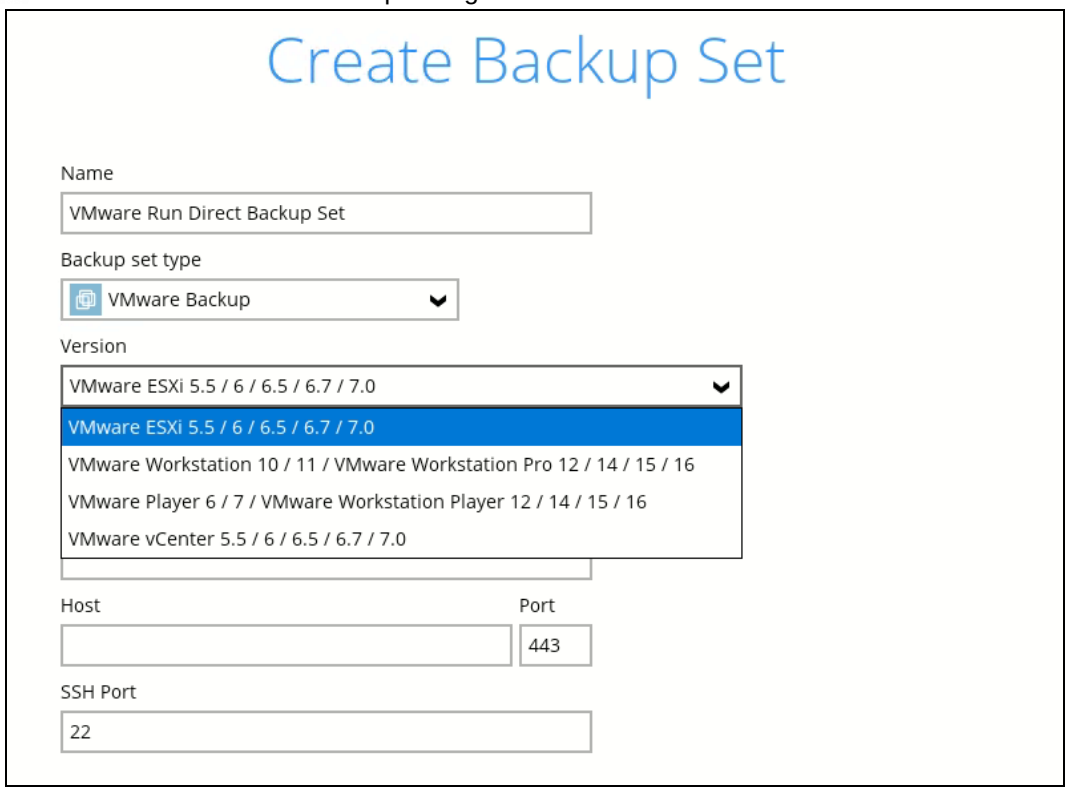


2. Create a VMware VM backup set by clicking the "+" icon next to **Add new backup set**.

3. Enter a **Name** for your backup set and select **VMware Backup** as the **Backup set type**.



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



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

  -OR-

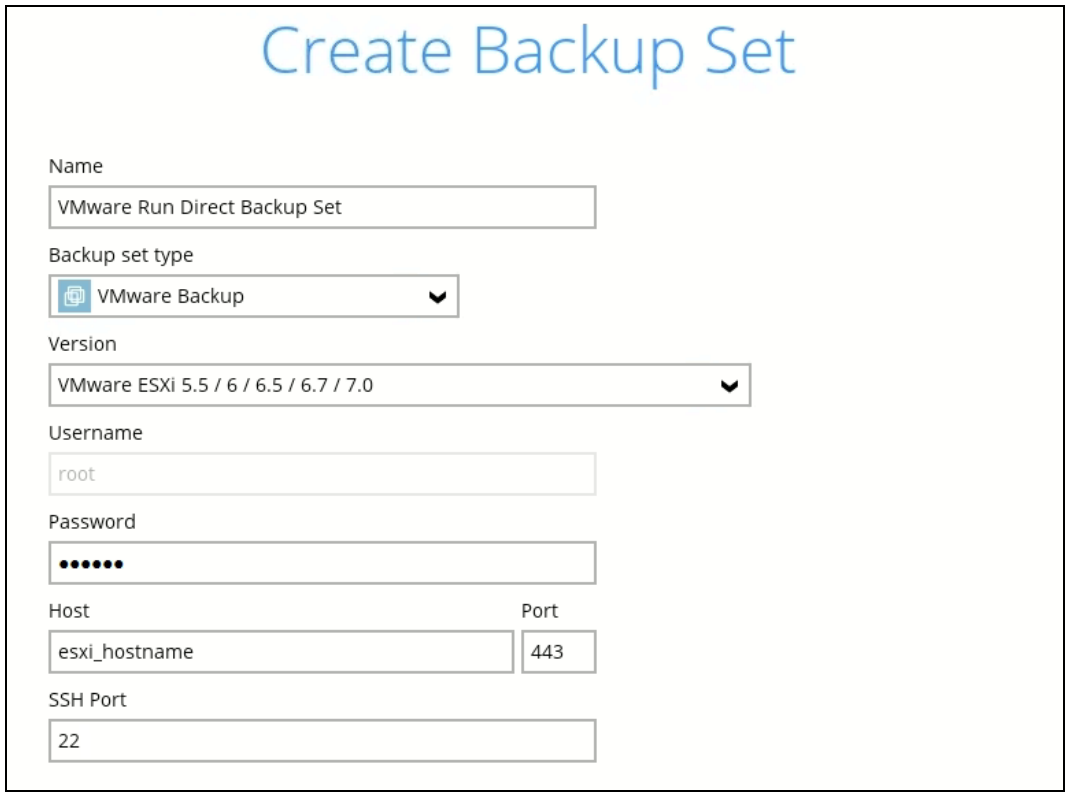
- Select **VMware vCenter 5.5 / 6 / 6.5 / 6.7 / 7.0** for a VMware vCenter backup set

NOTE

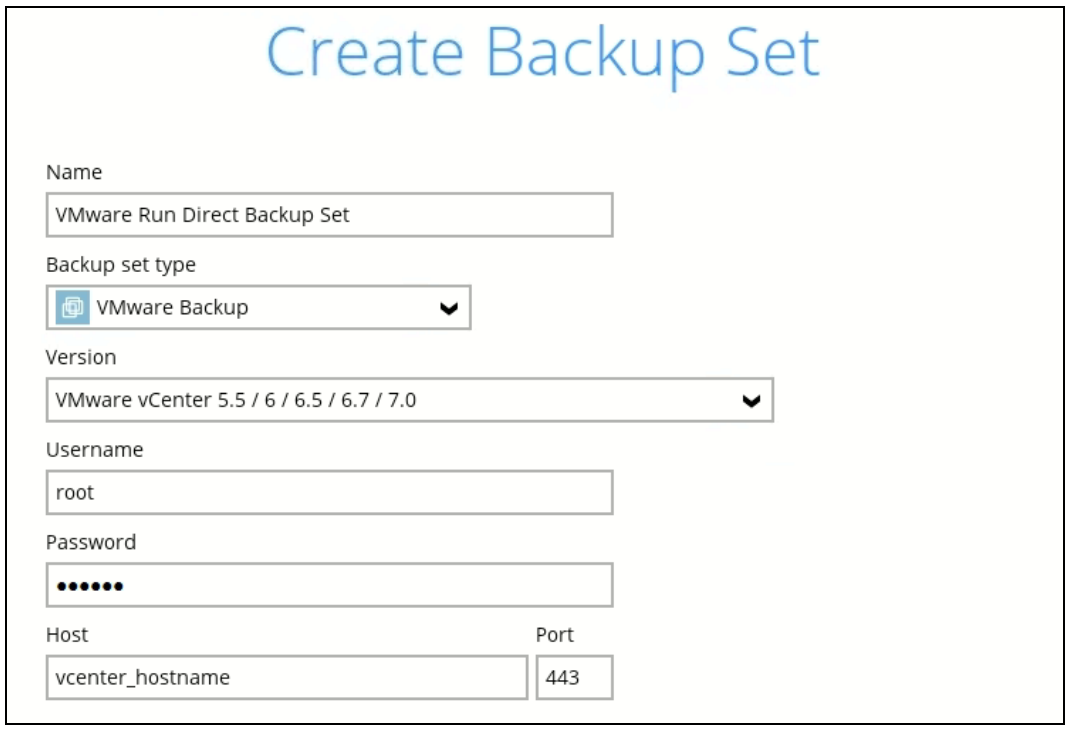
Refer to the following article for the list of compatible VMware platforms:

https://wiki.ahsay.com/doku.php?id=public:8001_faq:ahsay_software_compatibility_list_scl_for_version_8.1_or_above

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

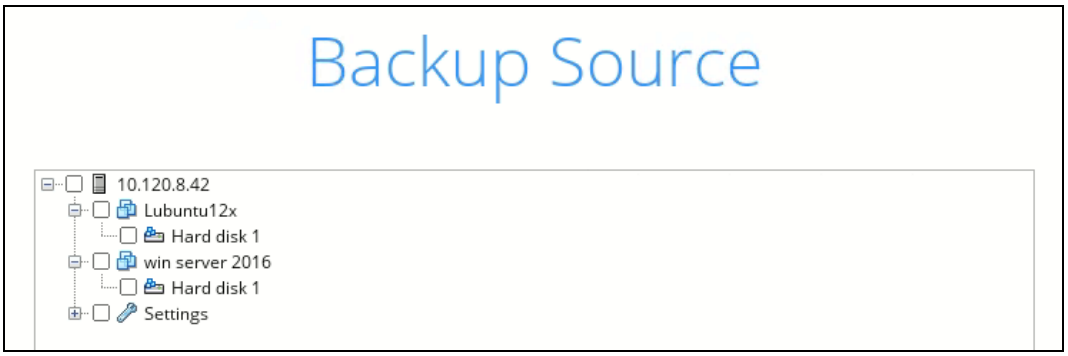


For a VMware vCenter backup set, enter the **Username** and **Password** of the administrator account, **Host**, and **Port** information of the vCenter server.

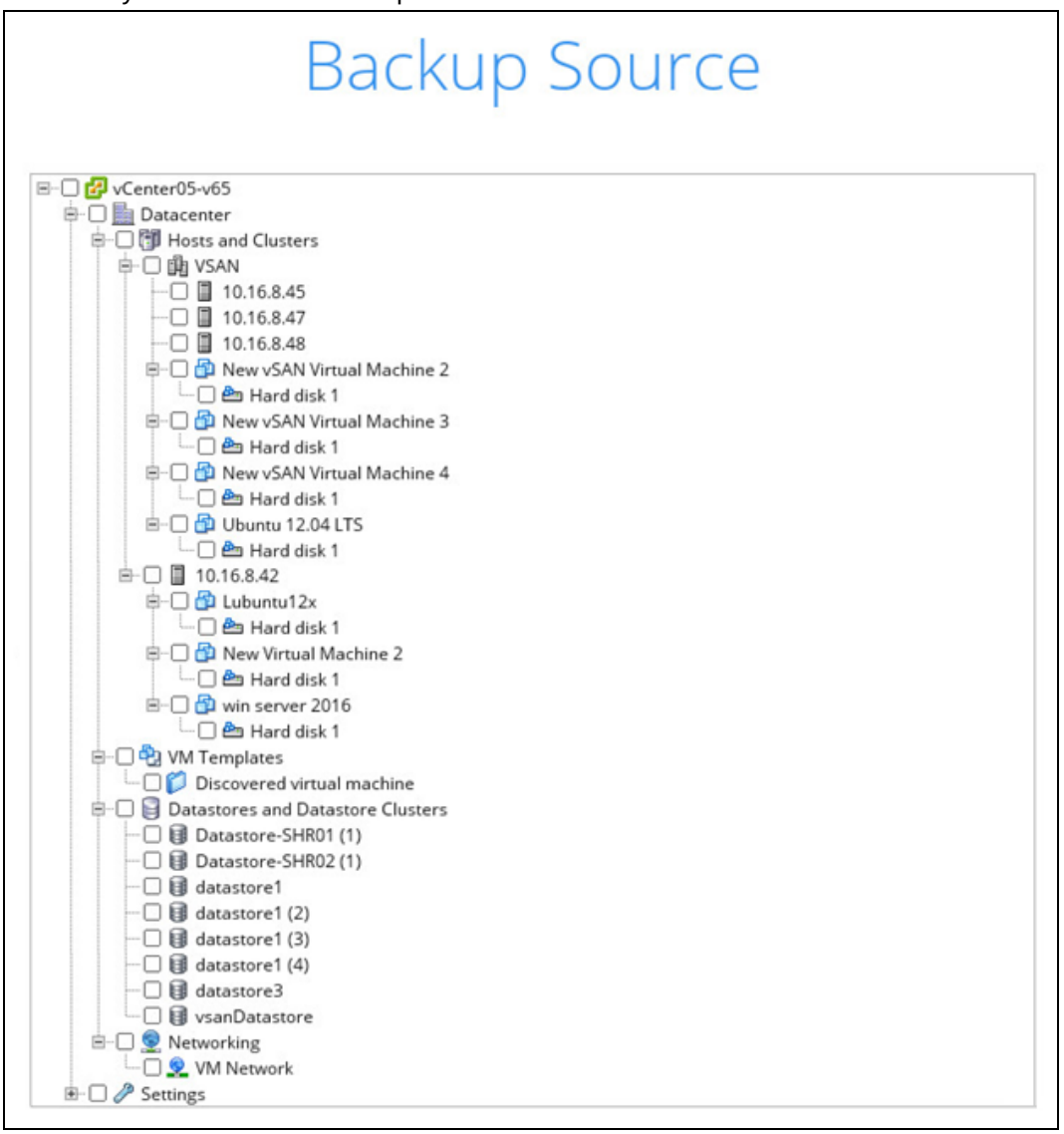


Click **Next** to proceed when you have finished entering all necessary information.

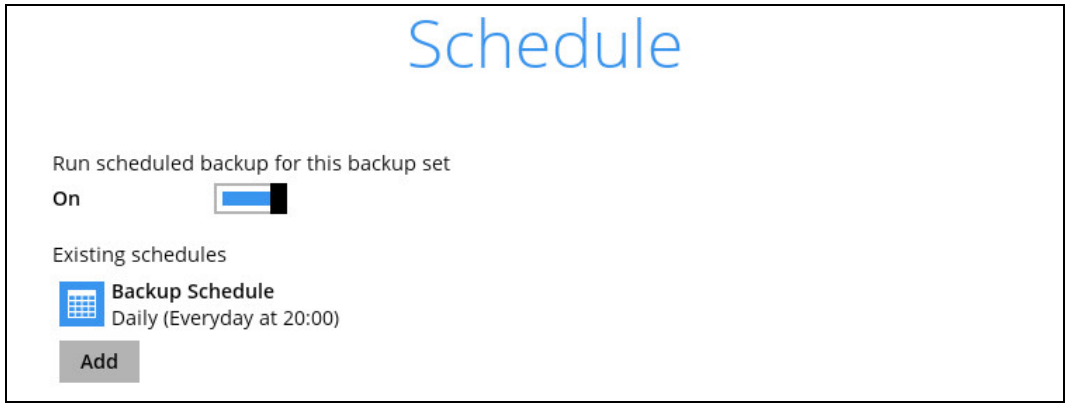
6. For VMware ESXi backup set, select the settings, virtual machines or individual virtual disks that you would like to backup.



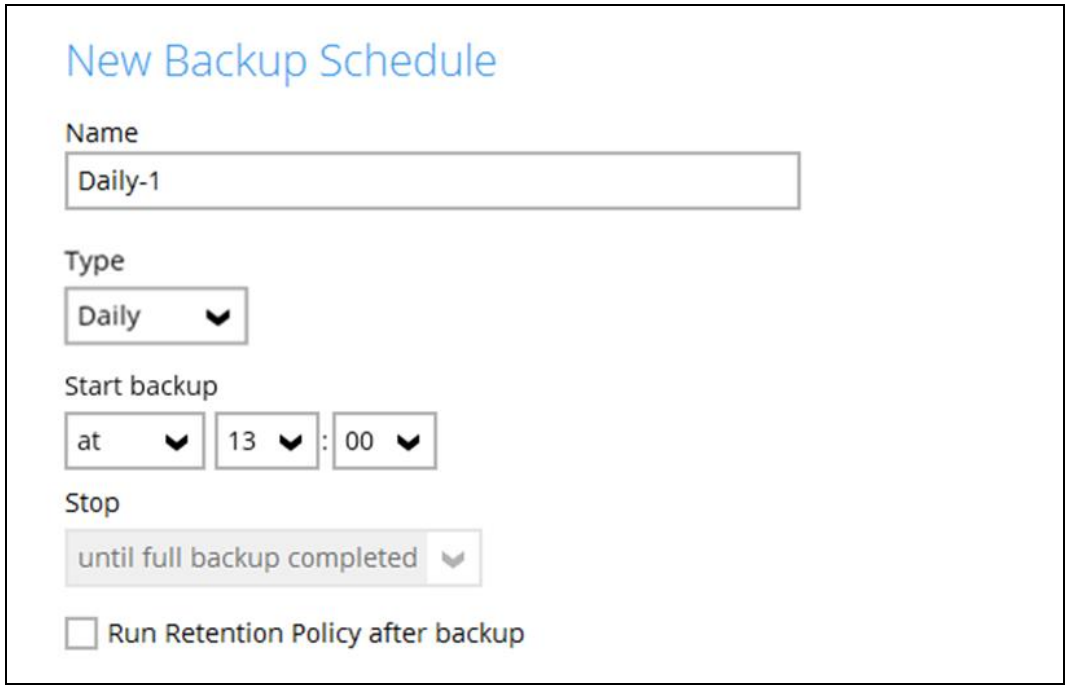
For VMware vCenter backup set, select the settings, virtual machines or individual virtual disks that you would like to backup.



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



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



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

NOTE

For details about the options from the dropdown menus, please refer to Configure Backup Schedule for Automated Backup.

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

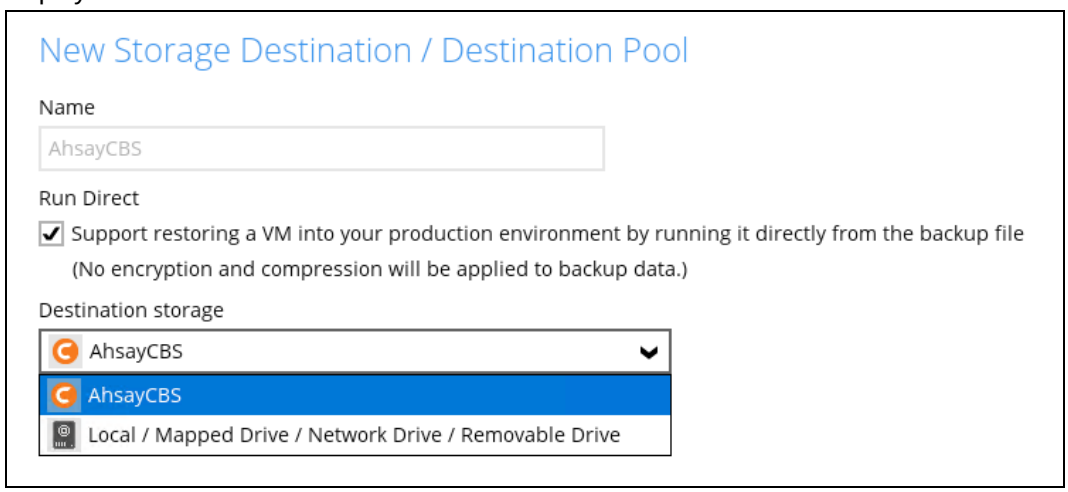
Select the appropriate option from the **Backup mode** dropdown menu.

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

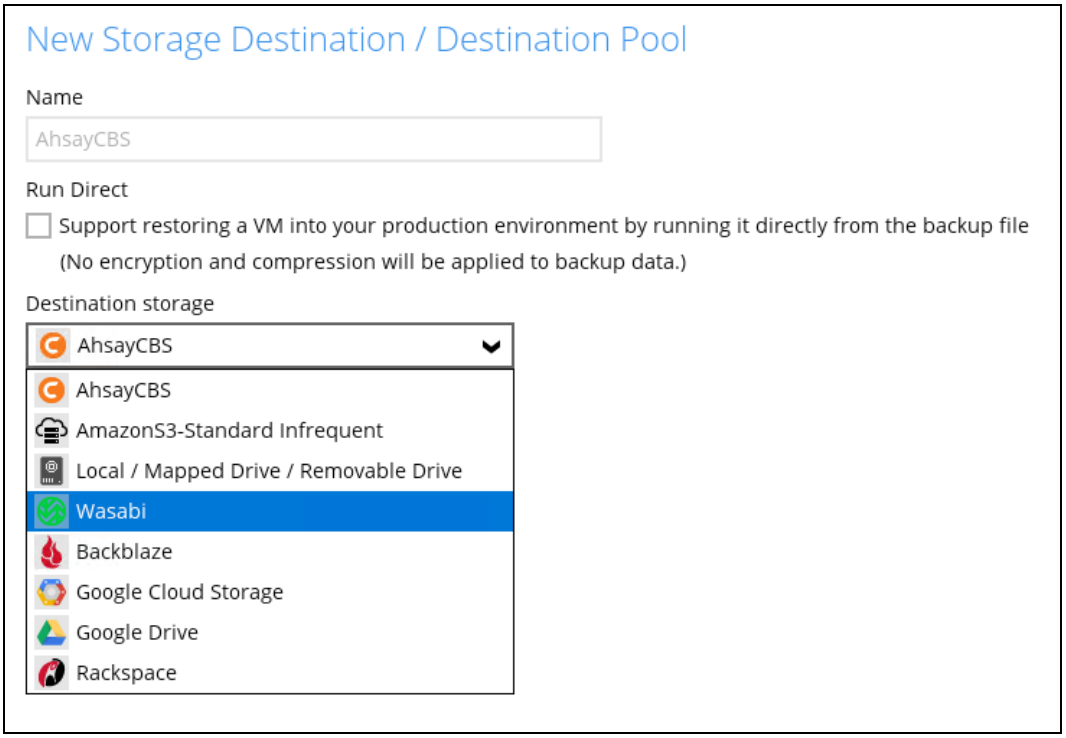
To select a backup destination for the backup data storage, click the "**+**" icon next to **Add new storage destination / destination pool**.

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

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



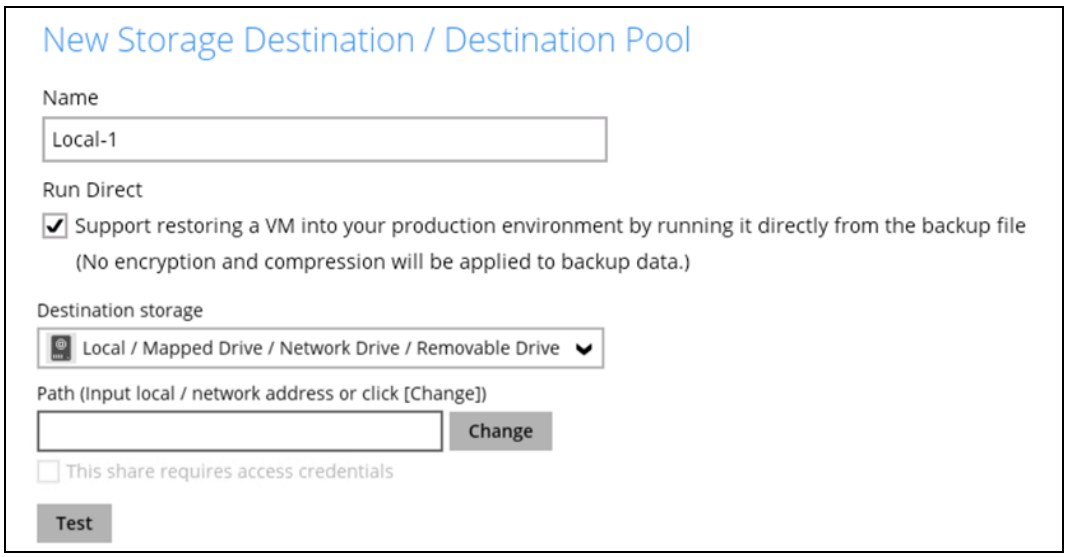
To get a list of other available destinations, unselect the Run Direct option.



NOTE

- Further to the above settings, there are also other requirements for the Run Direct feature, refer to the chapter on Run Direct Requirement for more details.
- The actual number of available destinations may be different. Please contact your backup service provider for details.
- For more details on Backup Destination, refer to the following article for details: https://wiki.ahsay.com/doku.php?id=public:8002_faq:faq_on_backup_destination

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



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

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

NOTE

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

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

Click **Next** to proceed.

NOTE

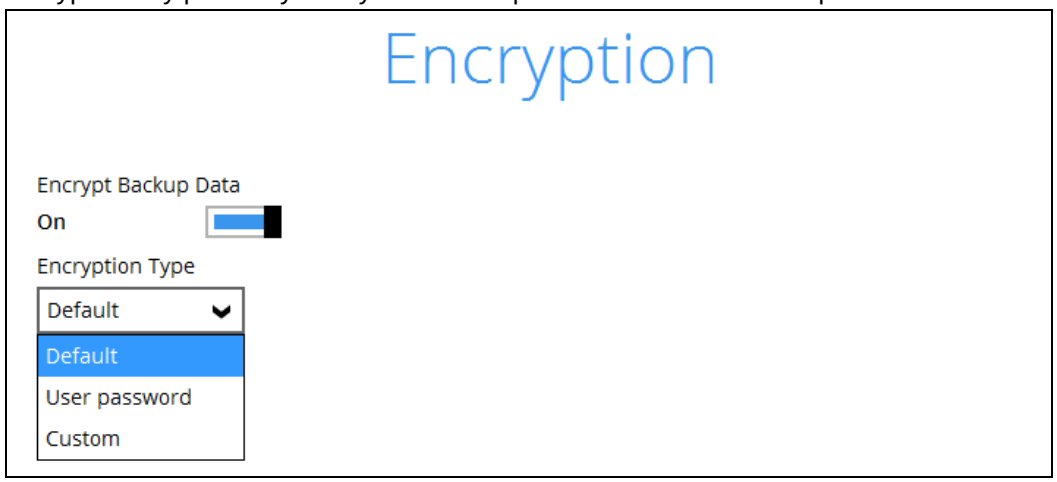
If you have enabled the Granular Restore or Run Direct restore feature, backup data will not be compressed and encrypted to optimize the restore performance, therefore you can skip to step 14.

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.

12. 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.

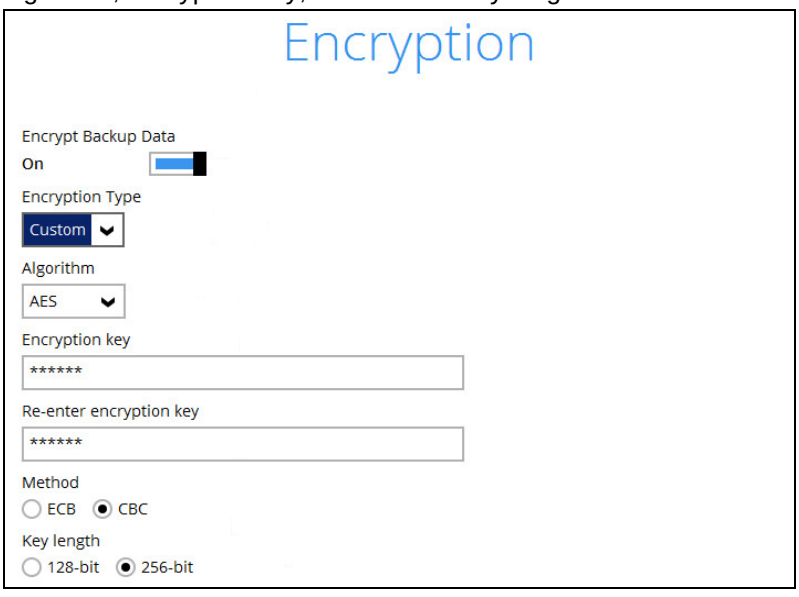


NOTE

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

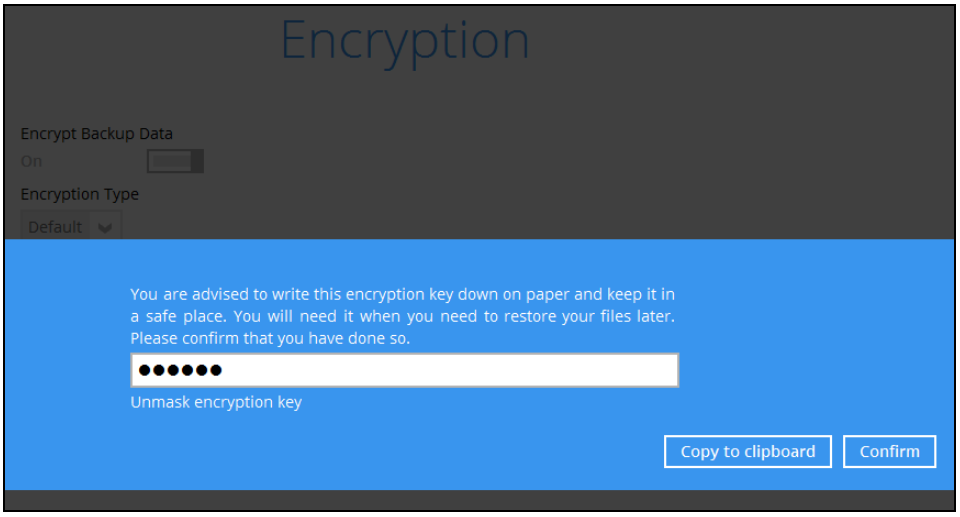
You can choose from one of the following three Encryption Type options:

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



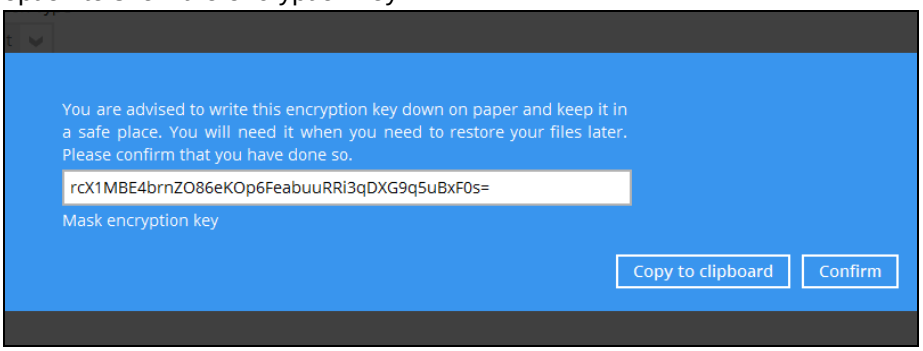
Click **Next** when you are done setting.

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



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

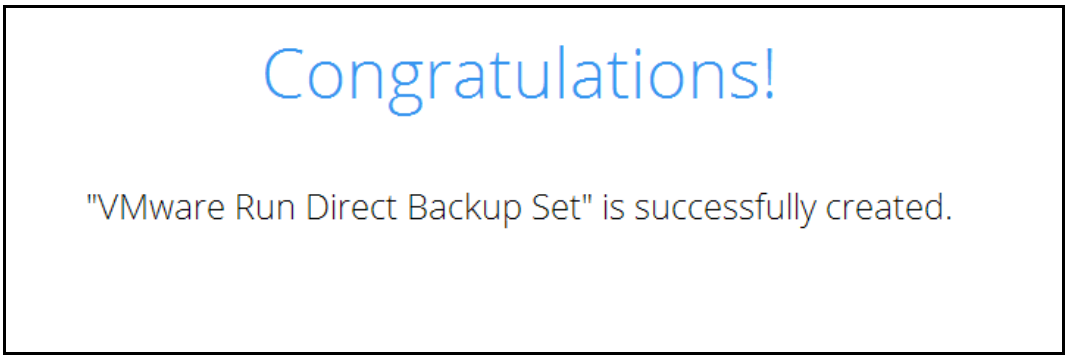
- **Unmask encryption key** – The encryption key is masked by default. Click this option to show the encryption key.



- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.

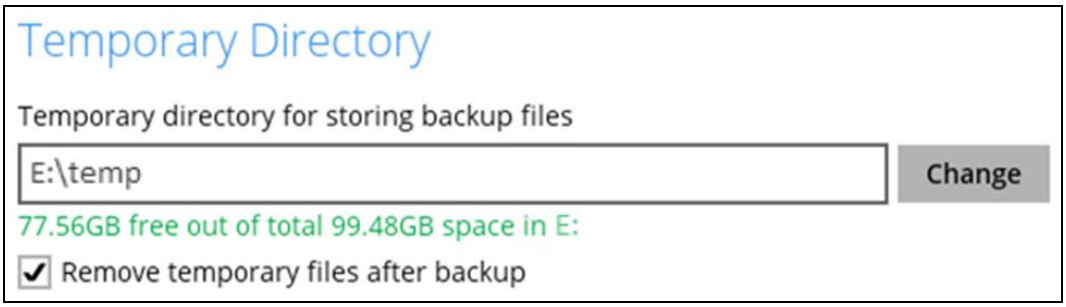
- **Confirm** – Click to exit this pop-up window and proceed to the next step.

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



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

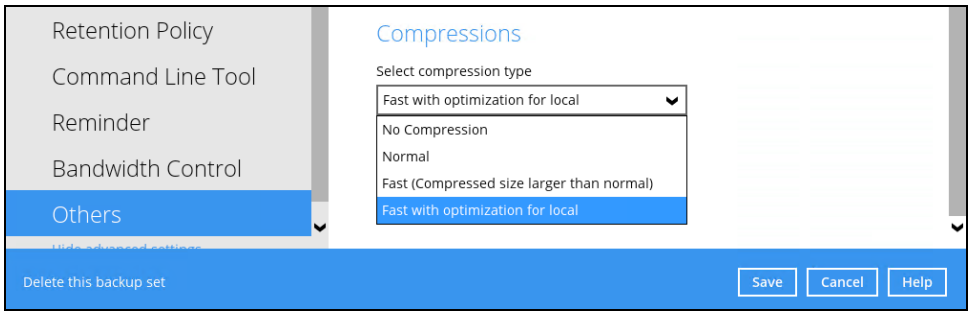
16. Based on Best Practices and Recommendations, it is highly recommended to set the **temporary directory** to another location other than Drive C: (e.g. Drive E:). To do this, go to **Backup Sets > Others > Temporary Directory** and click the **Change** button to browse for another location.



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

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

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



NOTE

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

8 Overview on the Backup Process

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.

- Periodic Data Integrity Check (PDIC) Process **(Step 3)**
- Backup Set Index Handling Process
  - Start Backup Job **(Step 5)**
  - Completed Backup Job **(Step 14)**
- Data Validation Check Process **(Step 12)**

8.1 Periodic Data Integrity Check (PDIC) Process

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

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

PDIC schedule = ***%BackupSetID% modulo 5***
or
%BackupSetID% mod 5

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

0	**Monday**
1	**Tuesday**
2	**Wednesday**
3	**Thursday**
4	**Friday**

NOTE: The PDIC schedule cannot be changed.

Example:

Backup set ID: 1594627447932

Calculation: 1594627447932 mod 5 = ***2***

2	**Wednesday**

In this example:

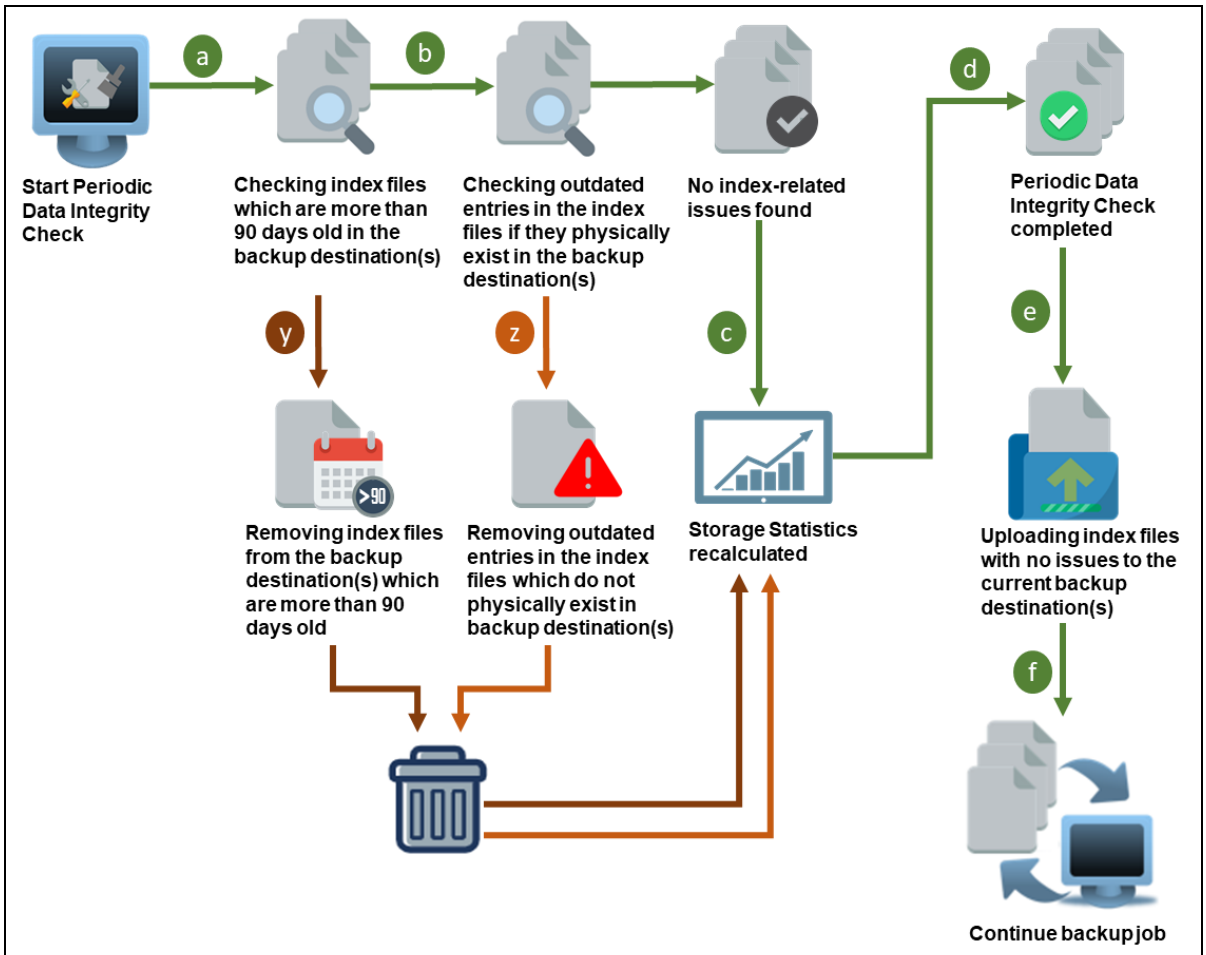
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

NOTE

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

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

1. If AhsayOBM was upgraded to v8.5 (or above) from an older version v6, v7, or pre-8.3.6.0 version. In this case, the PDIC job will run on the first backup job after upgrade.
2. If backup jobs for a backup set are not run on a regular daily backup schedule (for example: on a weekly or monthly schedule), then the PDIC job will run if it detects that the previous PDIC job was run more than 7 days ago.
3. Every time a data integrity check (DIC) is run, the latest PDIC run date is reset, the next PDIC job will run after 7 days.
4. The PDIC job will not run if there are no files in both the data and retention areas. For example: a newly created backup set with no backup job history or a backup set where all the data has been deleted using the Delete Backup Data feature.
5. The PDIC job will not run on a backup set which contains any data which is still in v6 format. It will only run if all v6 data format on a backup set has undergone data migration to v8 block format.



a Check the index files in the backup destination(s) to determine if they were more than 90 days old.
- ➔ If **YES**, proceed to y
- ➔ If **NO**, proceed to b

b Check the outdated entries in the index files for files and/or folders if they physically exist in the backup destination(s).
- ➔ If **YES**, proceed to c
- ➔ If **NO**, proceed to z

c Storage Statistics for Data area and Retention area usage will be recalculated.

d Periodic Data Integrity check is completed.

e Index files with no issues will be uploaded to the current backup destination(s).

f The backup job process will continue.

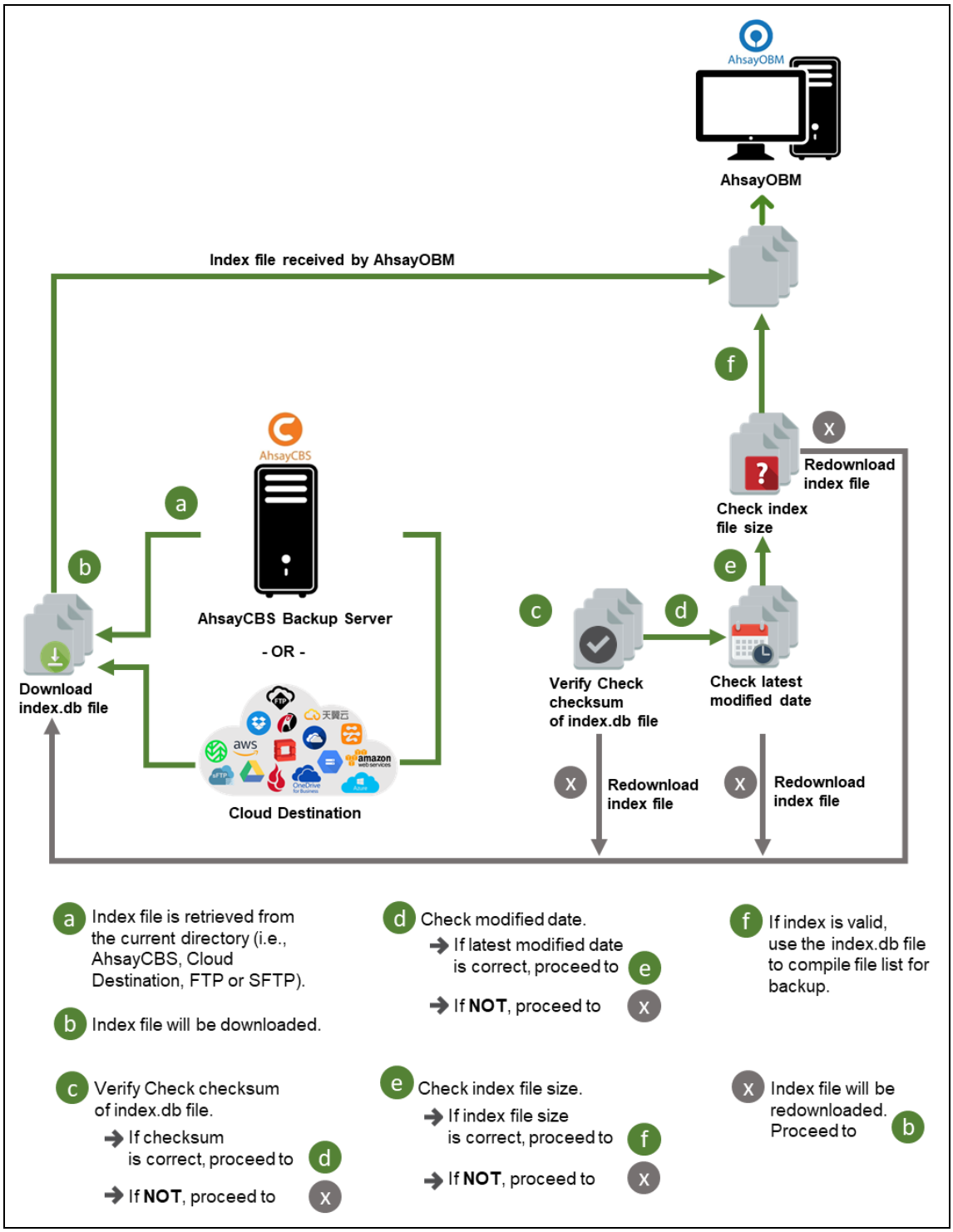
y Index files which are more than 90 days old will be removed from the backup destination(s).

z Outdated entries in the index files for files and/folders which do not physically exist in backup destination(s) will be removed.

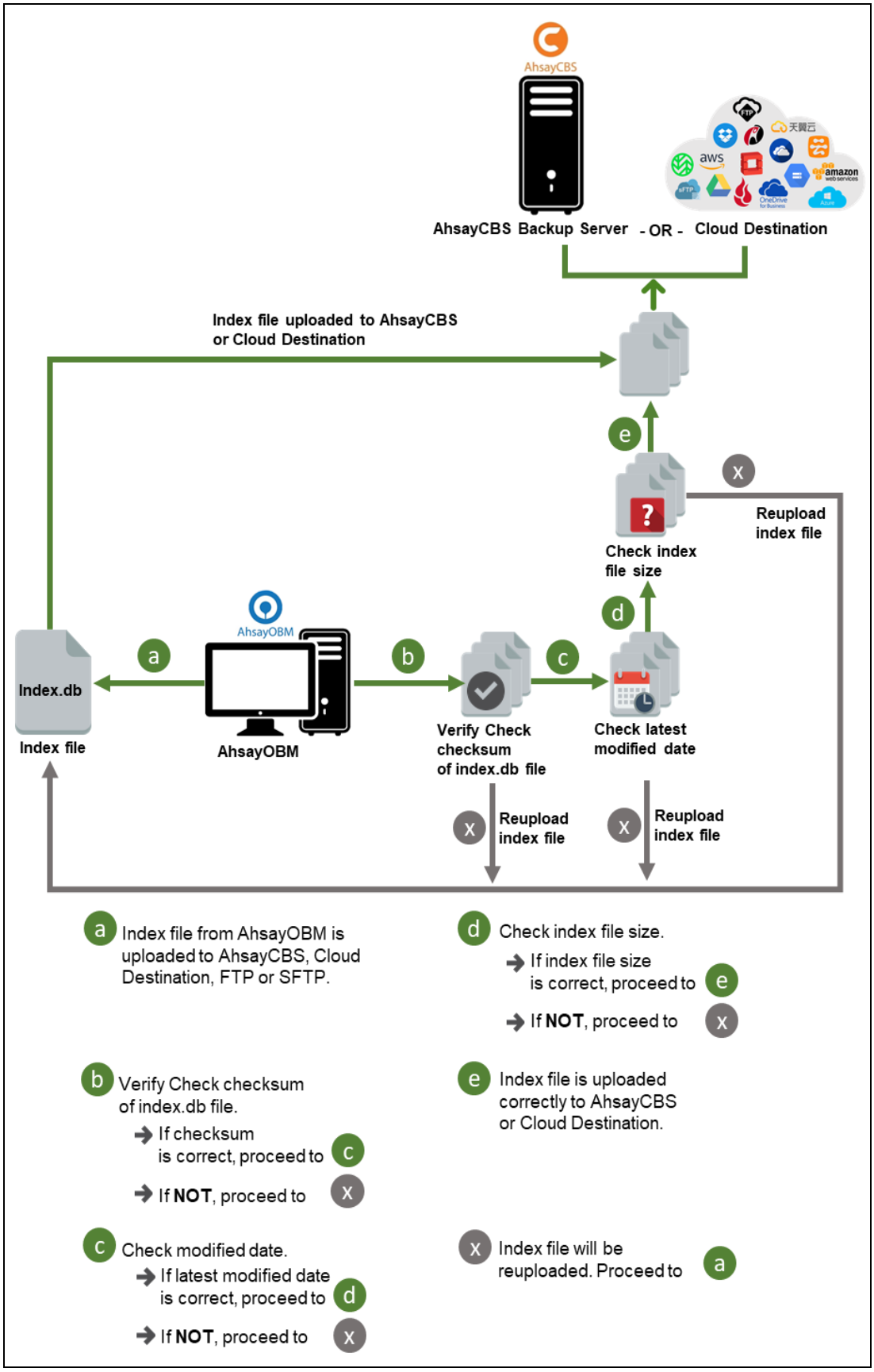
8.2 Backup Set Index Handling Process

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

8.2.1 Start Backup Job

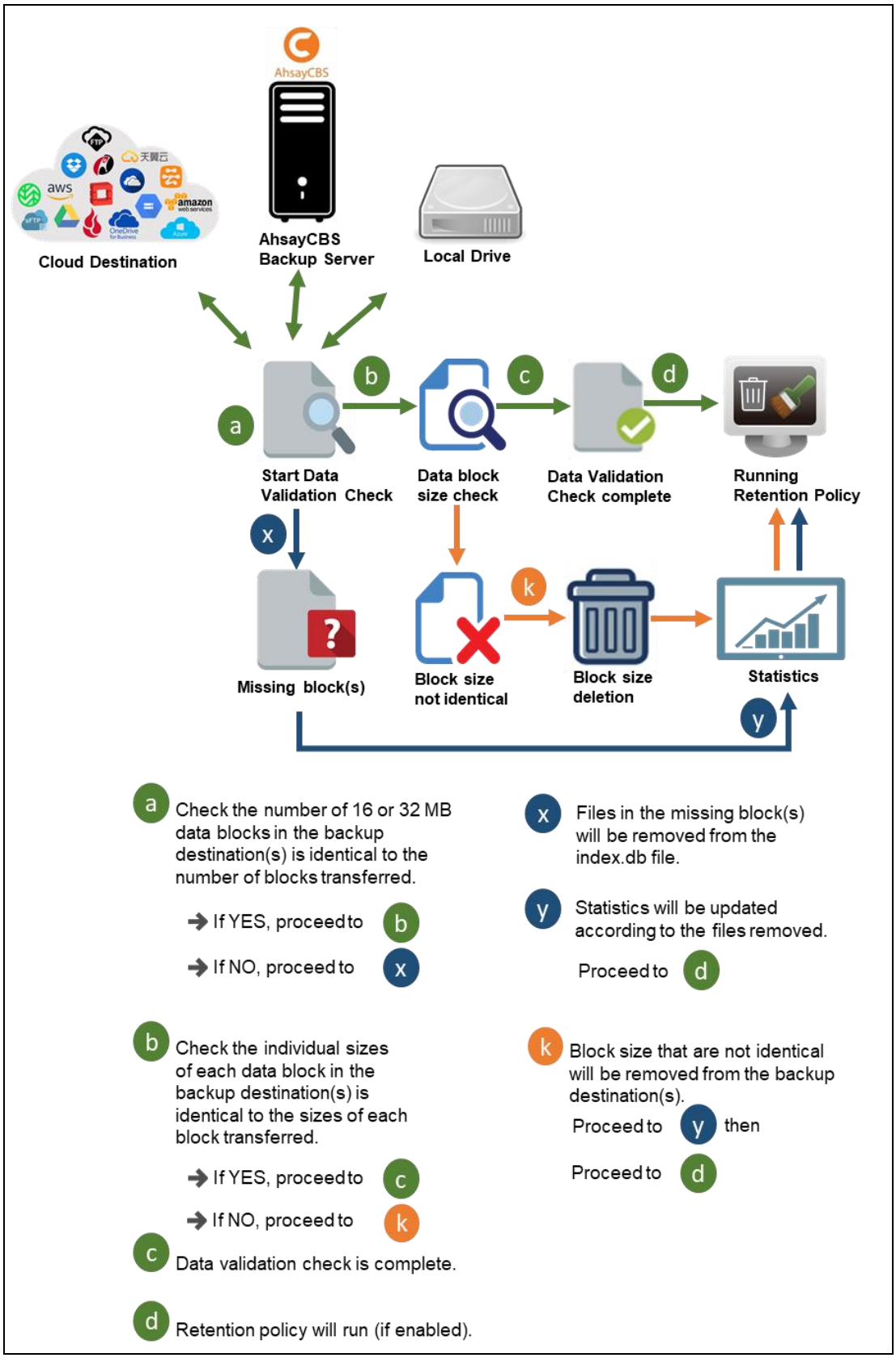


8.2.2 Completed Backup Job



8.3 Data Validation Check Process

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



9 Running a Backup

9.1 Start a Manual Backup

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

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

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

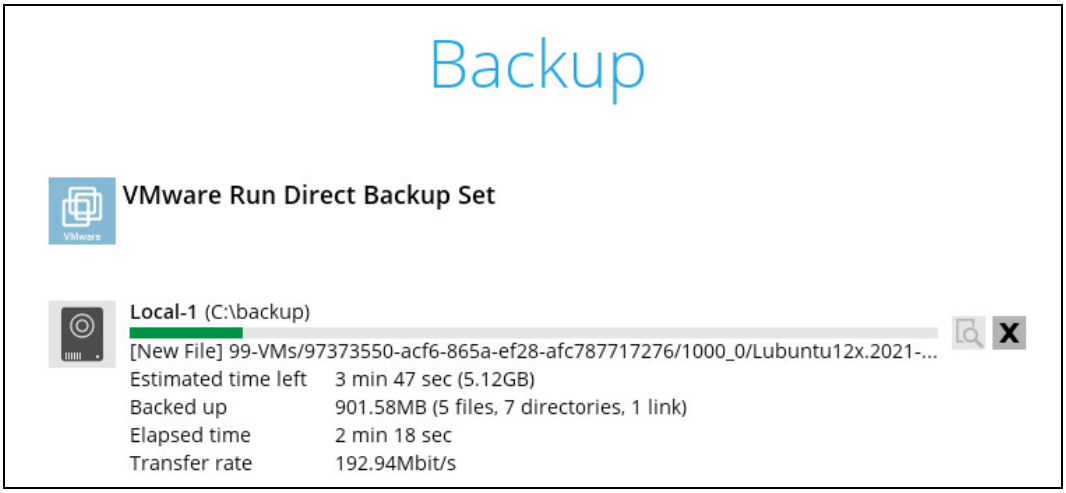
4. When advanced options are shown, it is recommended that you tick the checkbox next to **Run Retention Policy after backup** in the Retention Policy section at the bottom. This will help you save hard disk quota in the long run. In the In-File Delta type section, the

following three options are available:

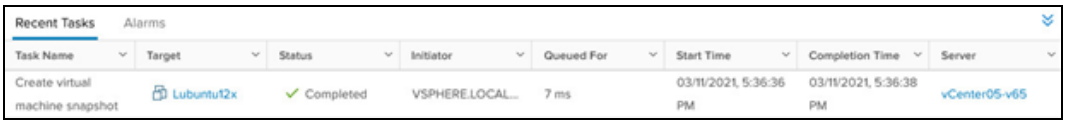
- **Full** – A full backup captures all the data that you want to protect. When you run a backup job for the first time, AhsayOBM will run a full backup regardless of the in-file delta setting.
- **Differential** – A differential backup captures only the changes made as compared with the last uploaded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

Click **Backup** to start the backup.

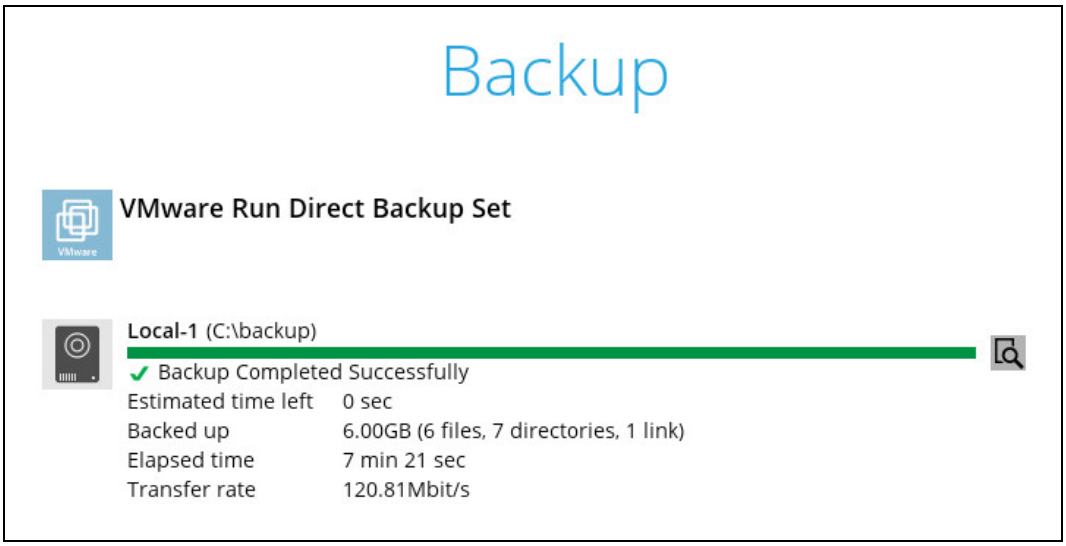
5. Click Backup to start the backup job. The status will be shown.



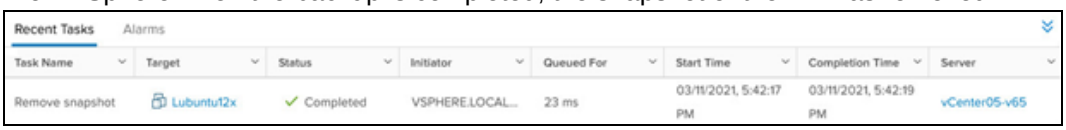
Another way of checking the progress of the backup is from vSphere. The backup has started when a snapshot of the vm was created.



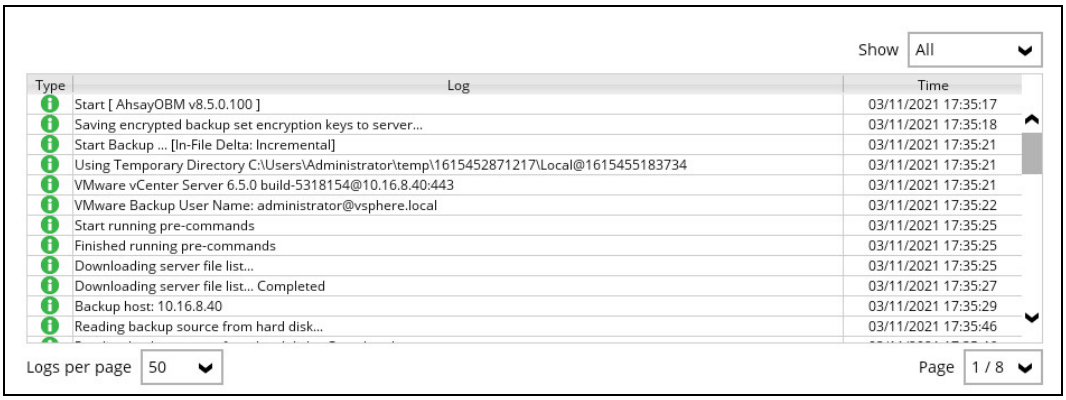
6. When the backup is completed, the progress bar will be green in color and the message "Backup Completed Successfully" will appear.



From vSphere when the backup is completed, the snapshot of the vm was removed.

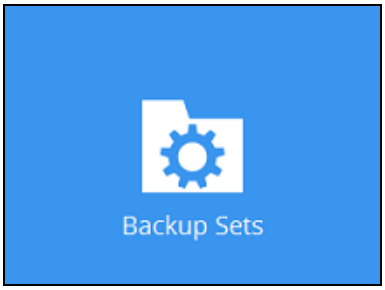


7. You can click the **View** icon on the right hand side to check the log. A window will pop up to show the log. Click **Close** to exit the pop-up window.



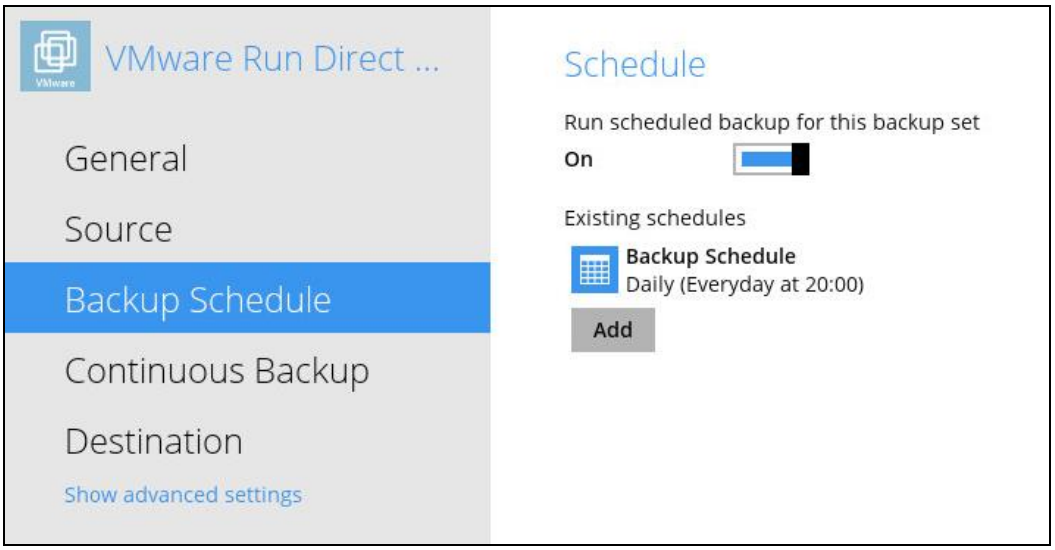
9.2 Configure Backup Schedule for Automated Backup

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

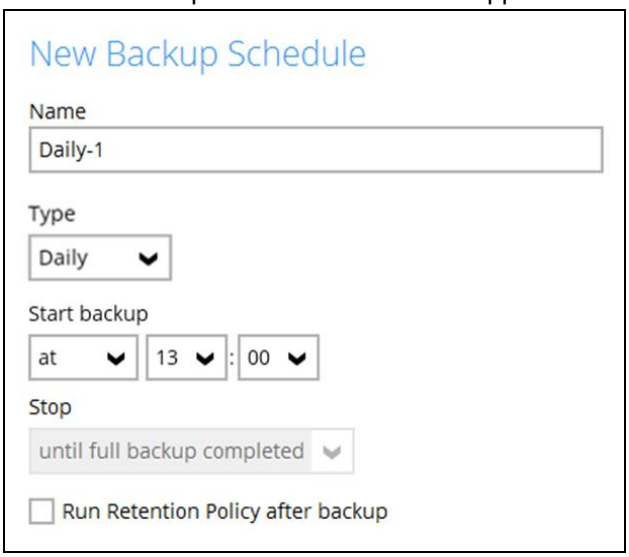


2. All backup sets will be listed. Select the backup set that you would like to create a backup schedule for.

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

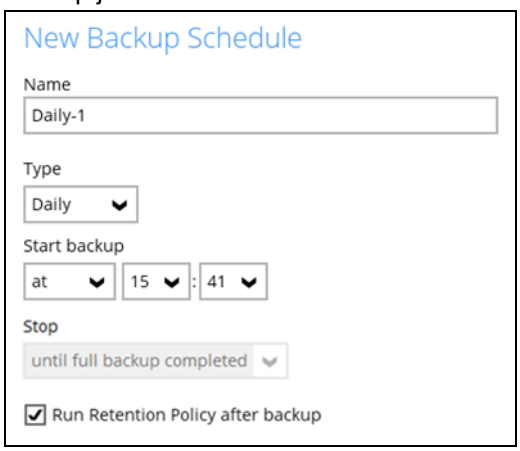


4. The New Backup Schedule window will appear.

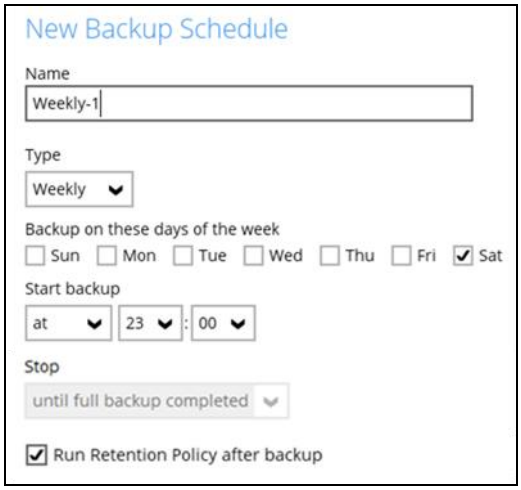


5. In the New Backup Schedule window, configure the following backup schedule settings.

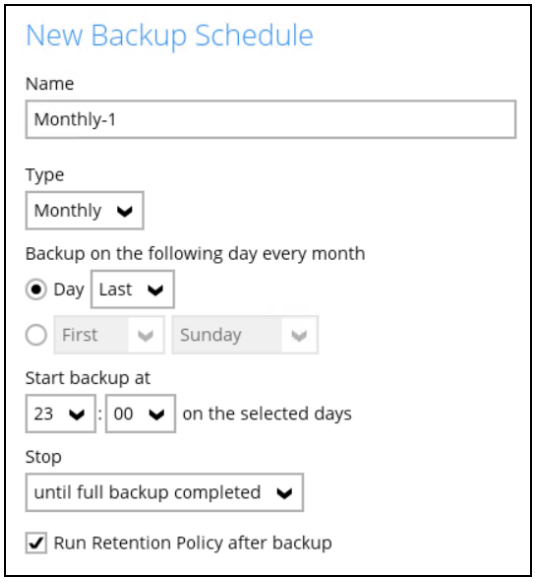
- **Name** – the name of the backup schedule.
- **Type** – the type of backup schedule. There are four (4) different types of backup schedule: Daily, Weekly, Monthly and Custom.
  - **Daily** – the time of the day or interval in minutes/hours which the backup job will run.



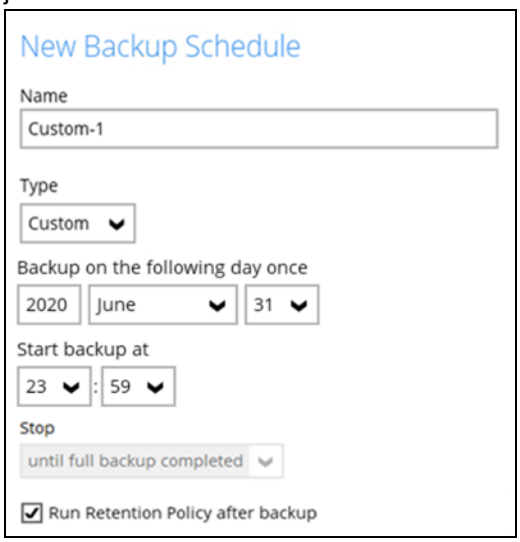
  - **Weekly** – the day of the week and the time of the day or interval in minutes/hours which the backup job will run.



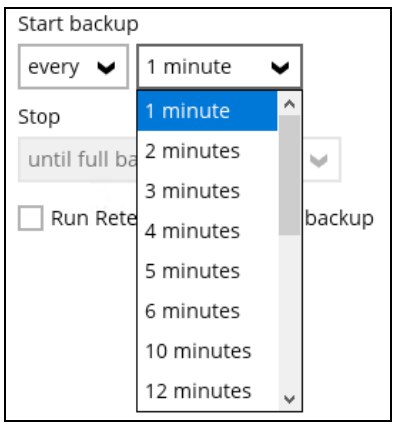
- **Monthly** – the day of the month and the time of that day which the backup job will run.

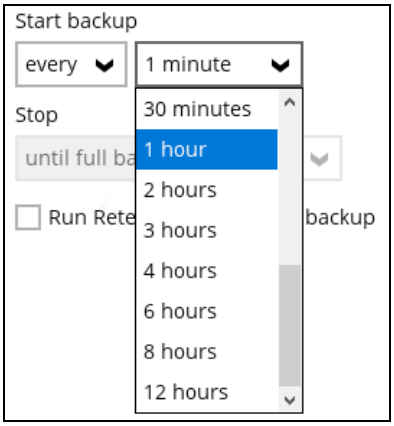


- **Custom** – a specific date and the time of that date which the backup job will run.

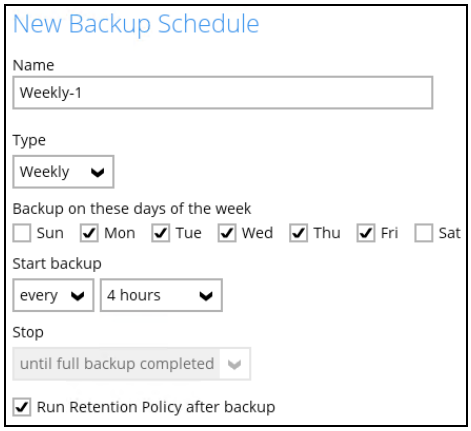


- **Start backup** – the start time of the backup job.
  - **at** – this option will start a backup job at a specific time.
  - **every** – this option will start a backup job in intervals of minutes or hours.





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



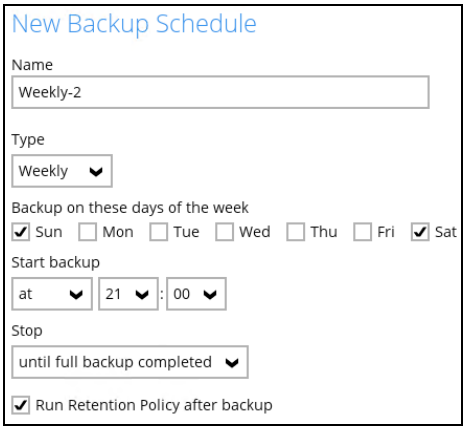


Figure 1.1 ***Figure 1.2***

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

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

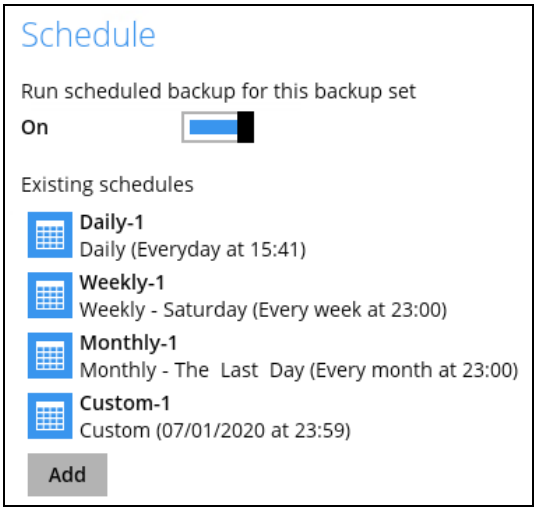
- **Stop** – the stop time of the backup job. This only applies to schedules with start backup "at" and is not supported for periodic backup schedule (start backup "every")
  - **until full backup completed** – this option will stop a backup job once it is complete. This is the configured stop time of the backup job by default.
  - **after (defined no. of hrs.)** – this option will stop a backup job after a certain number of hours regardless of whether the backup job has completed or not. This can range from 1 to 24 hrs.
    - The number of hours must be enough to complete a backup of all files in the backup set. For small files in a backup, if the number of hours is not enough to back up all files, then the outstanding files will be backed up in the next backup job. However, if the backup set contains large files, this may result in partially backed up files.
    - For example, if a backup has 100GB file size which will take approximately 15 hours to complete on your environment, but you set

the “stop” after 10 hours, the file will be partially backed up and cannot be restored. The next backup will upload the files from scratch again.

- The partially backed up data will have to be removed by running the data integrity check.
- As a general rule, it is recommended to review this setting regularly as the data size on the backup machine may grow over time.

- **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:



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

10 Restore Methods

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

Method 1 - Restoring a Virtual Machine with Run Direct
Introduction
This restore method can power up a VM instantly by running it directly from the backup files in the backup destination.
Pros
➢ Fast Recovery ➢ Minimize VM server down time so as minimizing impact on your business
Cons
➢ Changes made to the running VM during Run Direct power up process will be lost when the VM is powered down if not committed to the VM by completing a successful migration.

Method 2 - Restoring a Virtual Machine without Run Direct
Introduction
This is the conventional restore method where VM data is restored from the backup destination to the original VM host, another datastore of the original VMware host or another VMware host.
Pros
➢ Complete VM restore can be done in one take; no data migration needed afterwards
Cons
➢ Recovery time could be long if the VM size is large ➢ Long VM server down time may cause greater impact on your business

Method 3 - Restoring a Virtual Machine in Raw File (VMDK Format)
Introduction
If you wish to restore the VM to another VMware host (ESXi server) directly without using AhsayOBM
Pros
➢ You can manually restore the VM to another VMware host (ESXi server) off-site without having to use AhsayOBM as the restore channel
Cons
➢ Restore procedures are relatively complicated

Method 4 – Granular Restore
Introduction
AhsayOBM makes use of granular restore technology to enable a file level restore from a virtual disk file (VHD) of guest VM backup possible. It is particularly useful if you only need to restore individual file(s) from a guest VM, which would normally take a long time to restore and then power up before you can gain access to the files on the virtual disks. Granular restore gives you a fast and convenient way to recover individual files on a guest VM. For more details about Granular Restore, refer to the Granular Restore section.
Pros
➢ File level restore and access to files, without having boot up or to restore the entire Guest VM. ➢ Pin-point file restore to save time and promote efficiency ➢ Only one backup set required as opposed to the traditional restore method where two backup sets are required for file level restore
Cons
➢ No encryption and compression for backup set

11 Method 1 - Restoring a Virtual Machine with Run Direct

11.1 Login to AhsayOBM

Log in to the AhsayOBM application according to the instructions provided in the chapter on Starting AhsayOBM.

11.2 Running Direct Restore via AhsayOBM

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

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

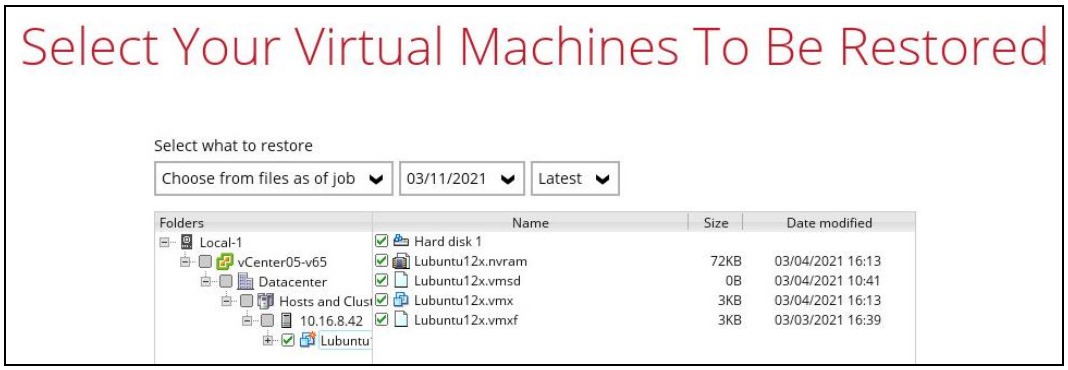
3. Select the backup destination that contains the VM that you would like to restore.

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

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

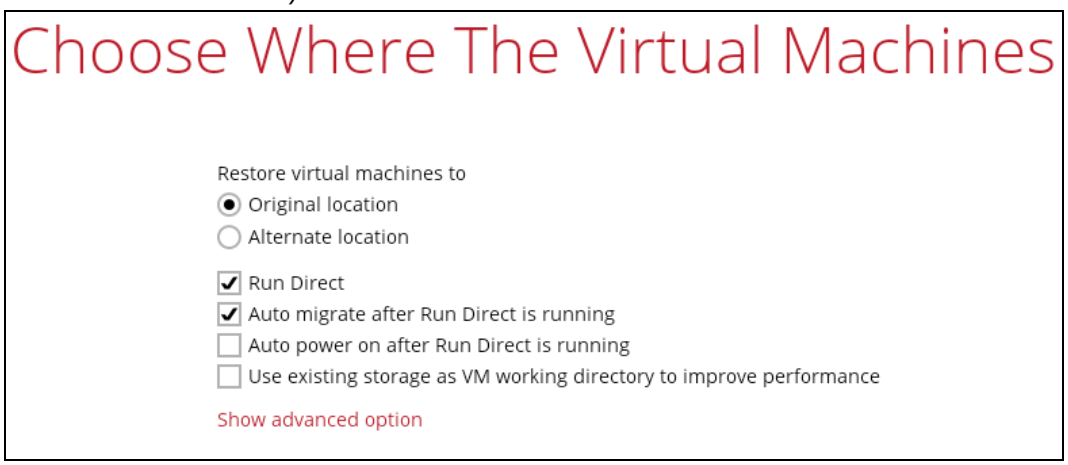
IMPORTANT

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

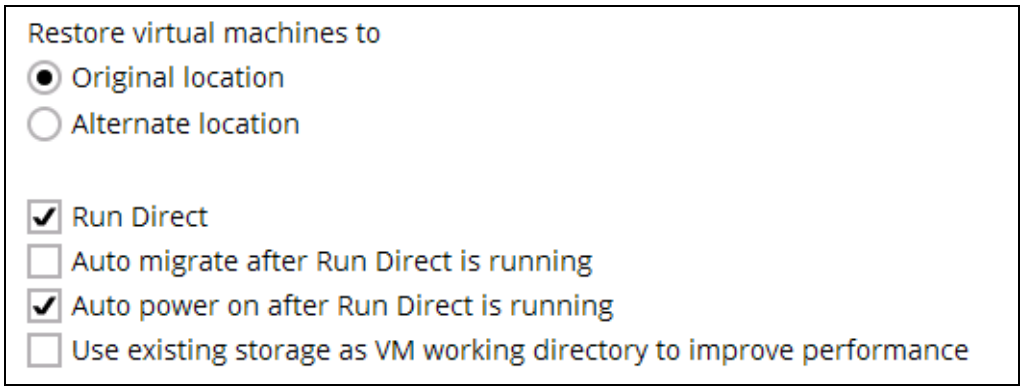


If you wish to restore the VM to another VMware host (ESXi server), you can restore the VM in raw file format, where the .vmdk disk format file will be included, by clicking the **Restore raw file** button at the bottom left corner. Refer to the steps in Restoring VM in VMDK format.

6. 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).



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



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

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

  NOTE

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

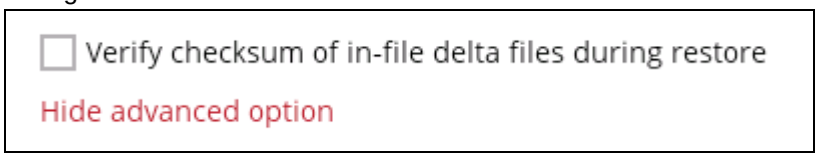
- **Auto power on after Run Direct is running**

  Enable this option to power up the virtual machine automatically, after Run Direct is running for the VM.

- **Use existing storage as VM working directory to improve performance**

  Enable this option to enhance performance of the restored VM. Click **Next** to proceed when you are done with the settings.

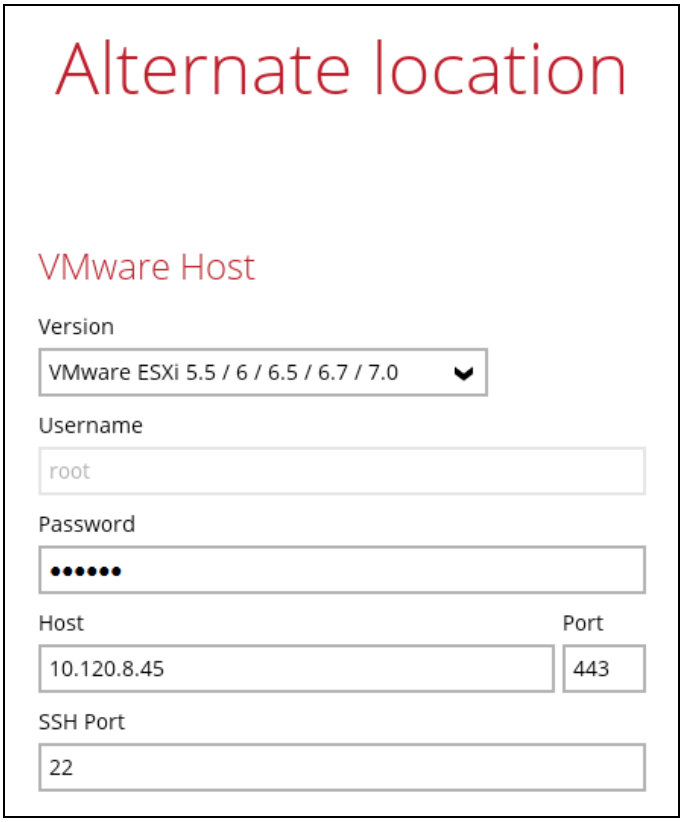
8. Click Show advanced option if you want to enable Verify checksum of in-file delta files during restore.



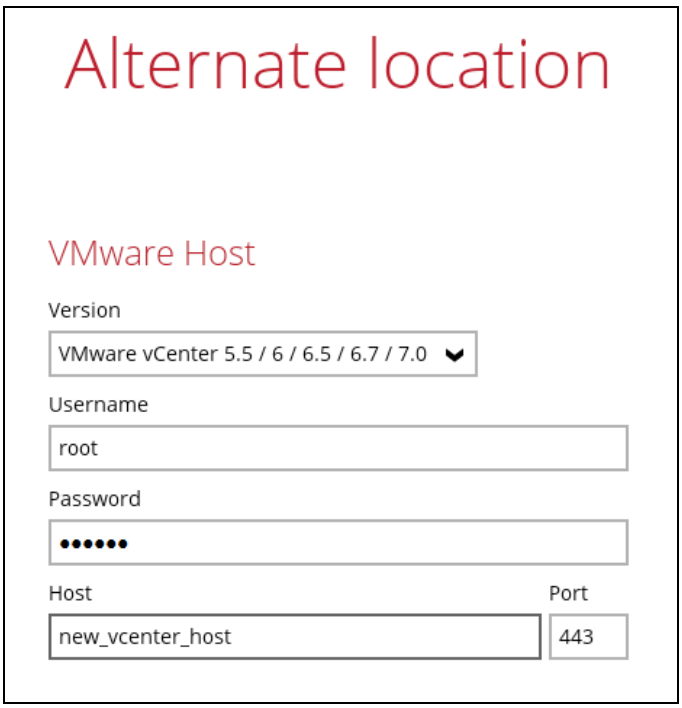
9. This step applies only for restoring to **Alternate location**. For restoring to **Original location**, skip to step 10.

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

   - For restoration to another VMware host (ESXi server), select **Version VMware ESXi 5.5 / 6 / 65 / 6.7 / 7.0**, then enter the **Password** of the root account, **Host**, **Port** and **SSH Port** of the new / original host.



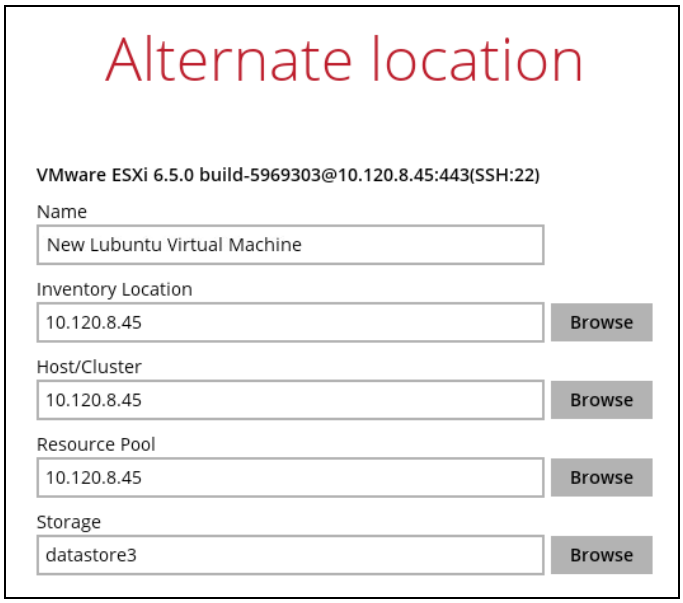
- For restoration to another VMware host (vCenter server), enter the **Username** and **Password** of the administrator account, **Host**, and **Port** information of the new / original vCenter server.

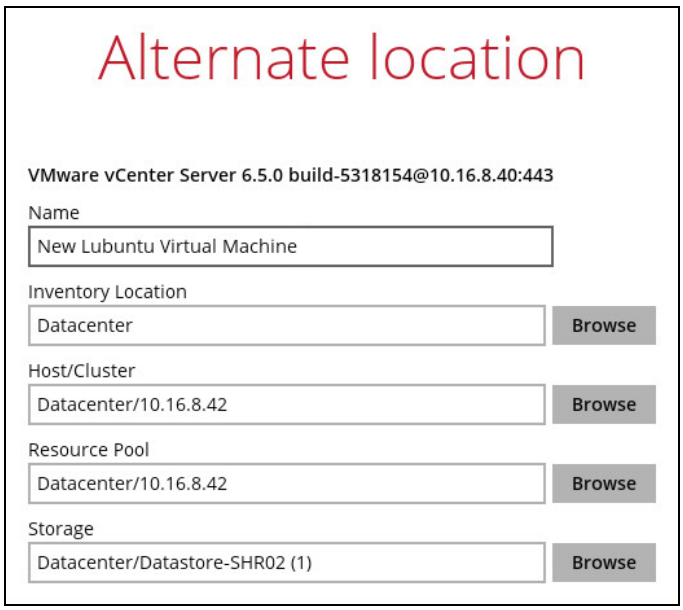


Press **Next** to proceed when you are done with the settings.

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

the VM to be restored to.



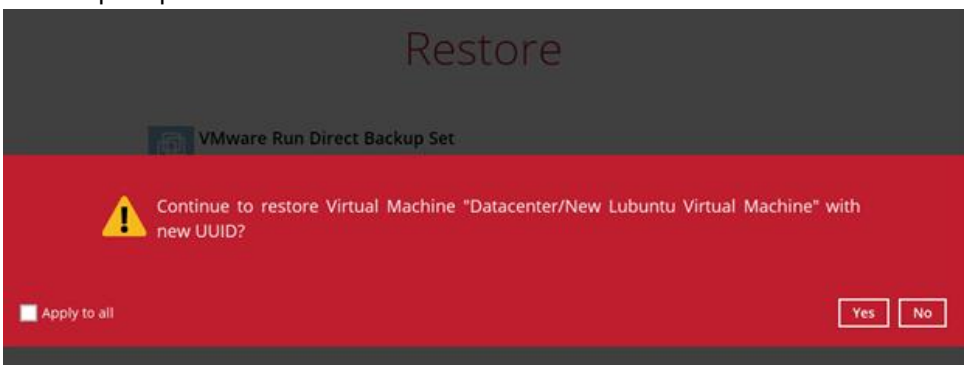


Click **Next** to proceed when you are done with the settings.

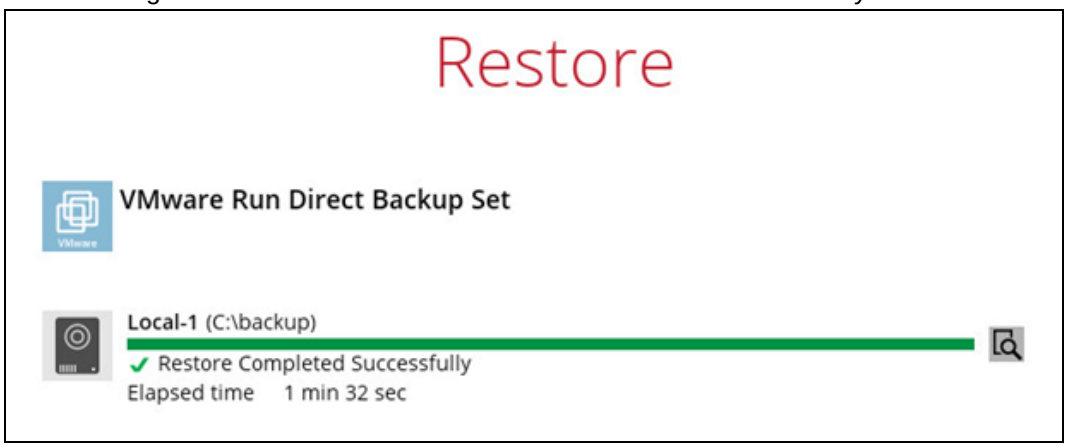
10. Select the temporary directory for storing temporary files, then click **Restore** to start the restoration.

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

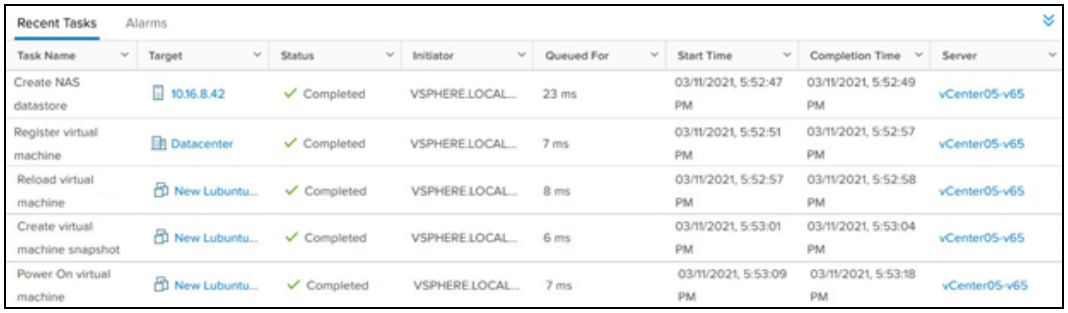
- Restoring guest VM to another VMware host, since each virtual machine is automatically assigned a universally unique identifier (UUID), a new UUID must be created when you restore the guest VM to another host. It is not possible to have two identical UUID running at the same time, so make sure to click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



12. 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.



NOTE

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

11.3 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

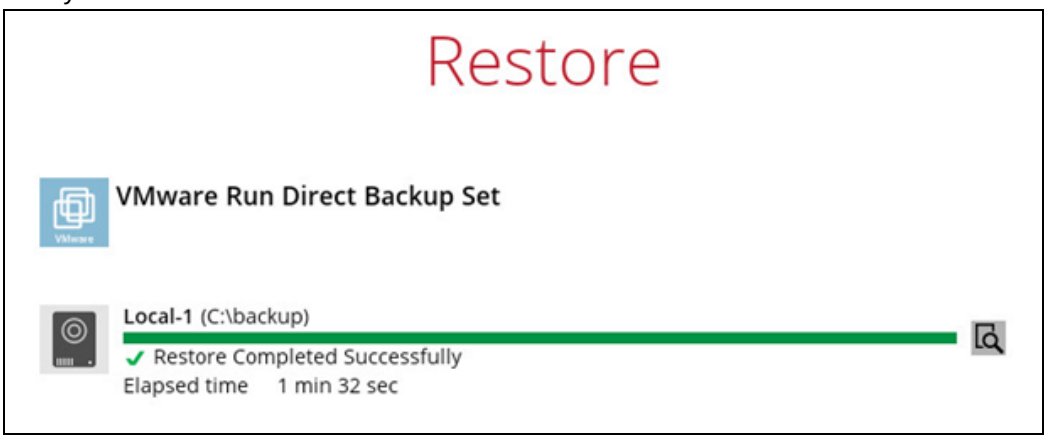
Mount VM on VMware Host
The NFS datastore is mounted on the VMware Host

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.

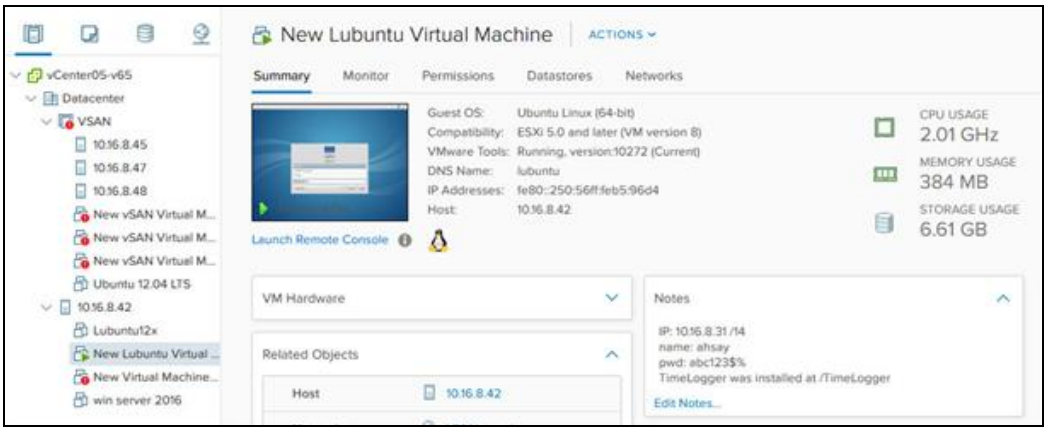
Power on Virtual Machine
The virtual machine is being powered on so it can be run directly from the backup files.

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.

11.4 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.

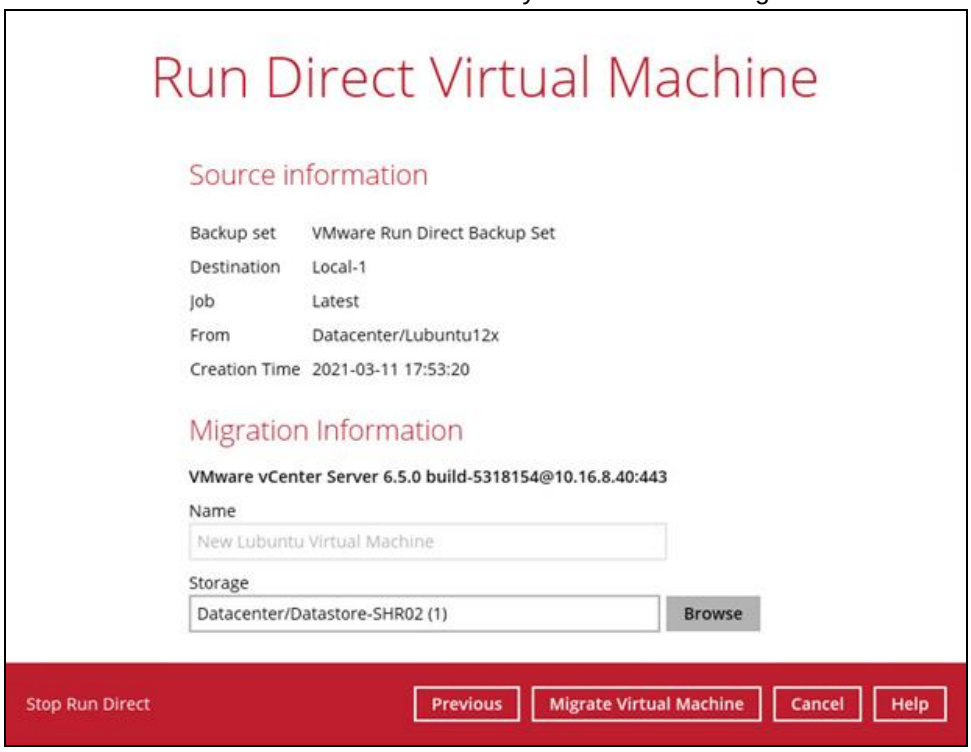
2. Click **Manage Run Direct virtual machines** to manage all Run Direct virtual machines.

11.4.1 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.



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.

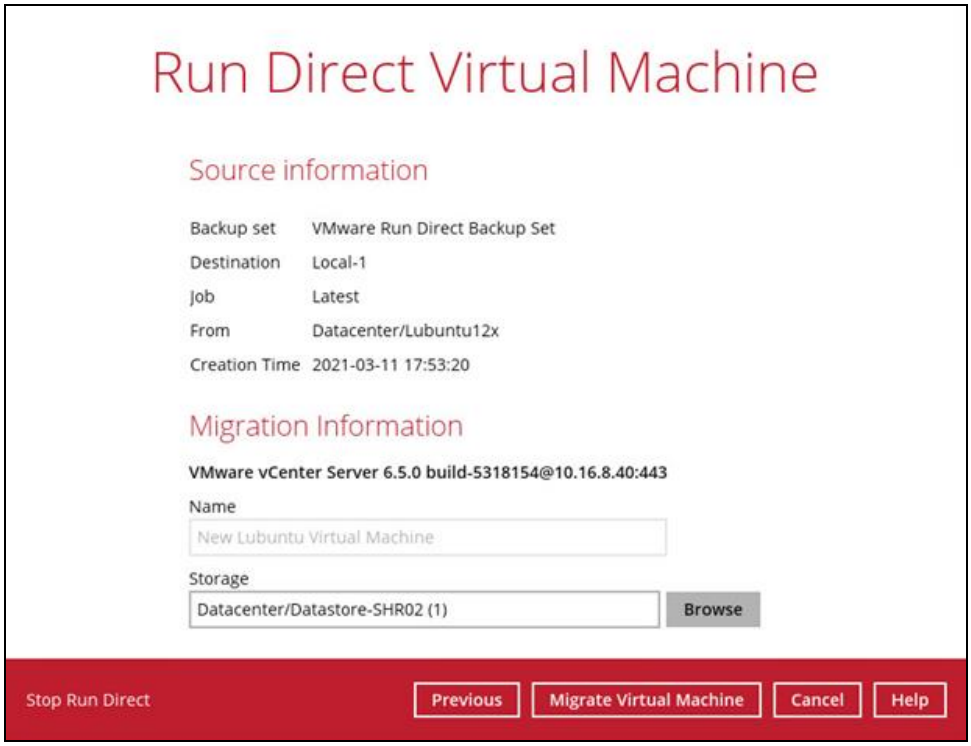
11.4.2 Stop Run Direct VM

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.

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



3. Click **Yes** to proceed.

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.

11.5 Run Direct Restore via User Web Console

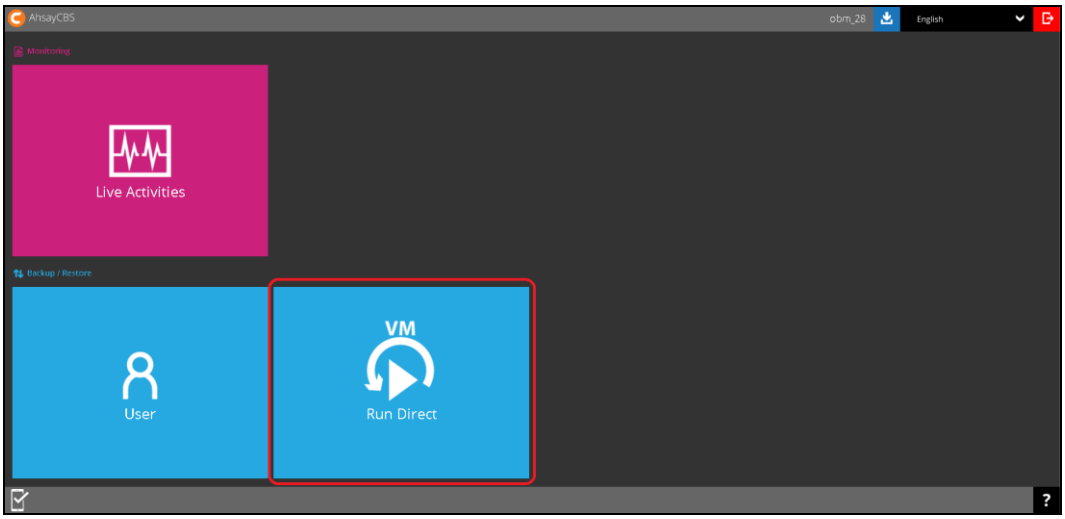
Besides using the AhsayOBM, you can now utilize the AhsayCBS User Web Console to initiate a run direct restore (also known as Agentless Restore).

Why use the User Web Console?

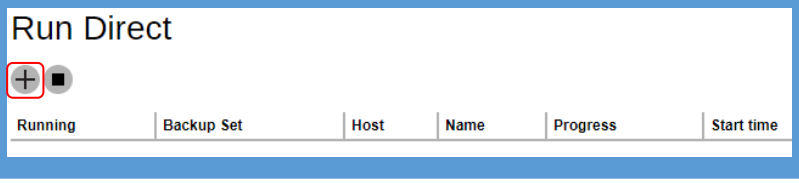
Unlike starting a Run Direct restore on AhsayOBM which you have to be physically with the client backup agent, you can now access the User Web Console to perform the same action as long as you have Internet connection and a web browser.

How to do it?

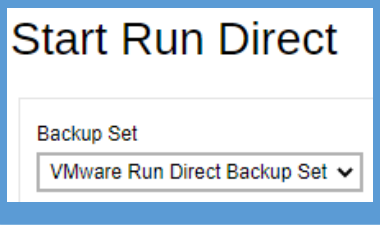
In the AhsayCBS User Web Console landing page, click on the Run Direct icon to start a run direct restore. For details on the operations, please refer to the AhsayCBS User Guide. The steps below give you a high-level overview of how a Run Direct is initiated on the AhsayCBS User Web Console.



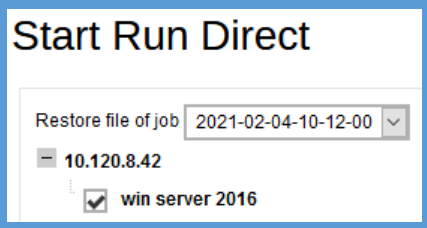
Start a Run Direct Session



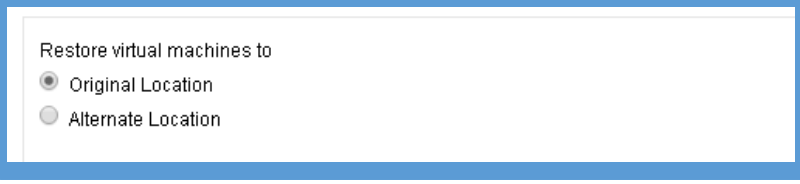
Select the Backup Set



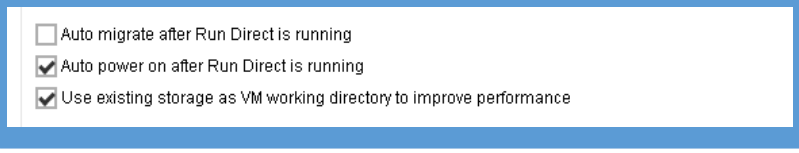
Select Specific Backup Job



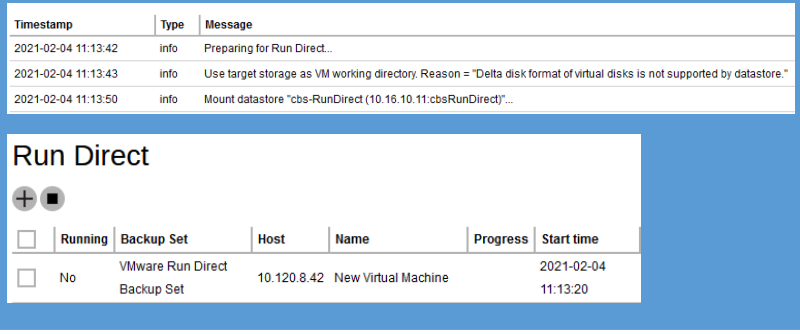
Select Restore Destination



Configure the Run Direct Options



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)"...

NOTE

In cases when Run Direct restore encounters an error, temporarily files are left behind on the VMware Host. These temporary files must be manually cleaned. For instructions on how to do this please refer to the Appendix.

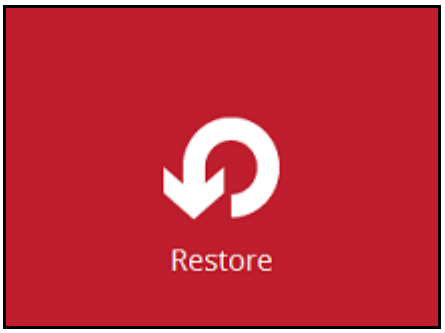
12 Method 2 - Restoring a Virtual Machine without Run Direct

12.1 Login to AhsayOBM

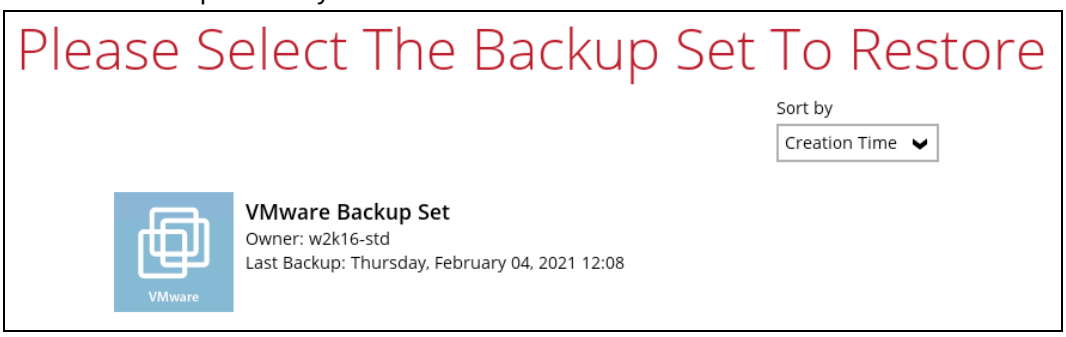
Login to the AhsayOBM application according to the instruction provided in the chapter on Starting AhsayOBM.

12.2 VM Restore without Run Direct

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



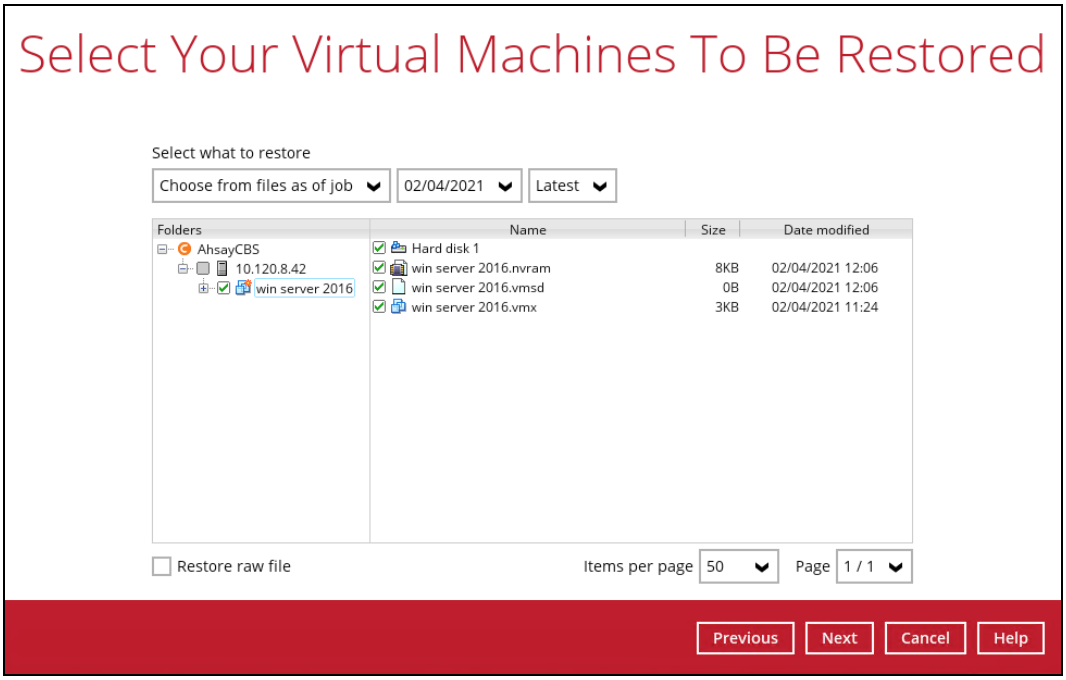
2. Select the backup set that you would like to restore the VM from.



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

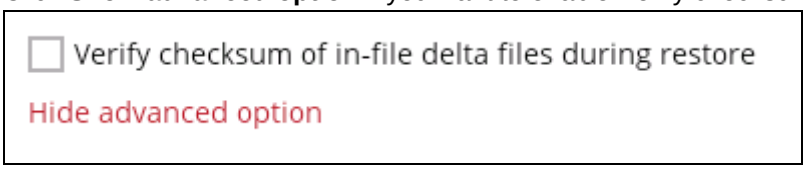
4. Select to restore VM from a specific backup job, or the latest job available from the **Select what to restore** drop down menu.

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



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

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

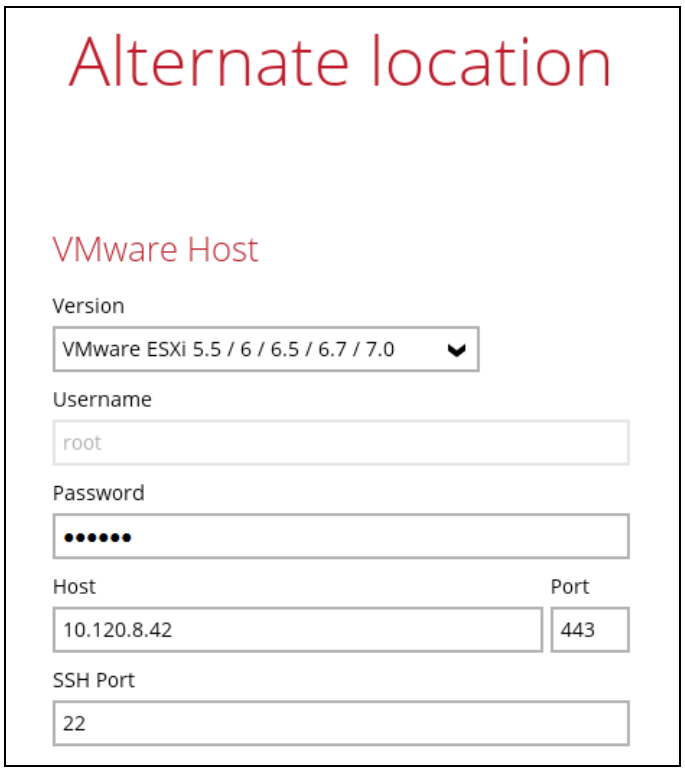


8. Click **Next** to proceed.

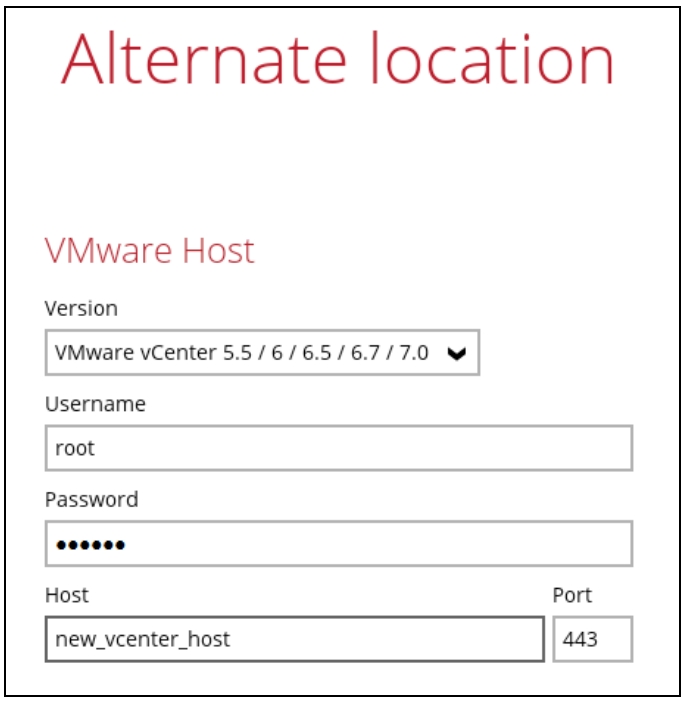
9. This step applies only for restoring to **Alternate location**. For restoring to **Original location**, skip to step 10.

   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.



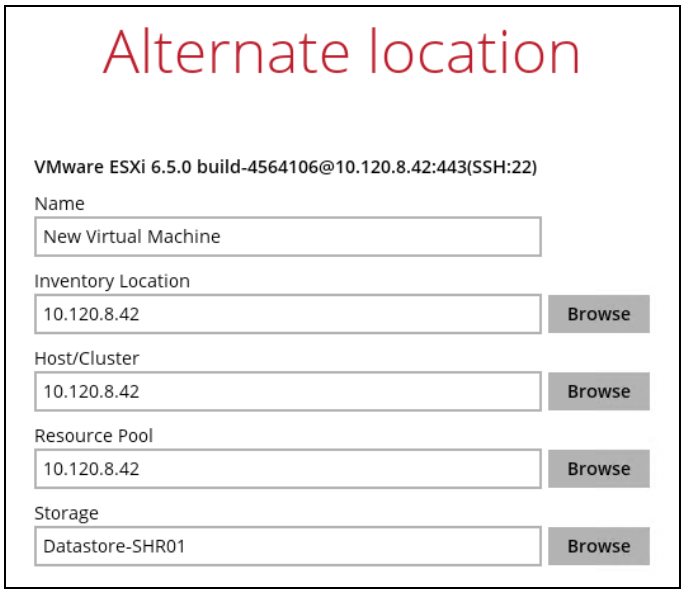
- For restoration to another VMware host (vCenter server), enter the **Username** and **Password** of the administrator account, **Host**, and **Port** information of the new / original vCenter server.

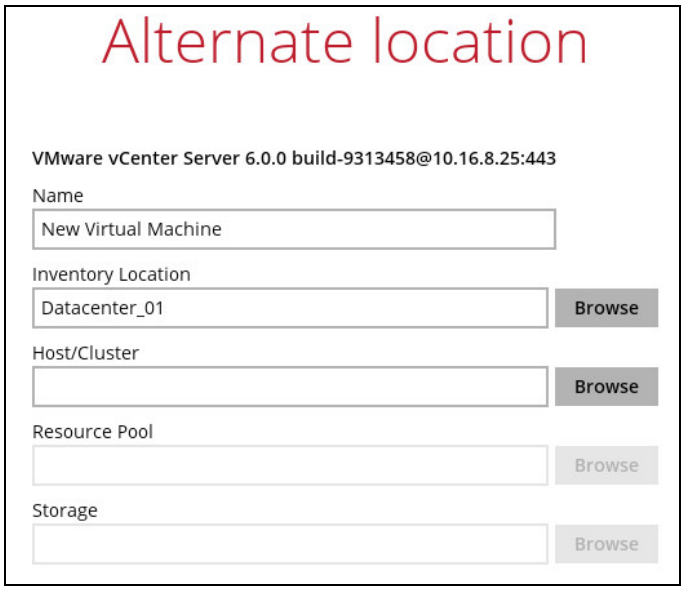


Click **Next** to proceed when you are done with the settings.

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

like the VM to be restored to.





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

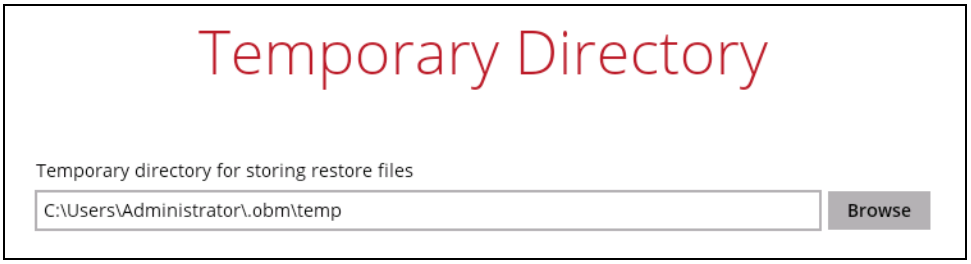
NOTE

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.

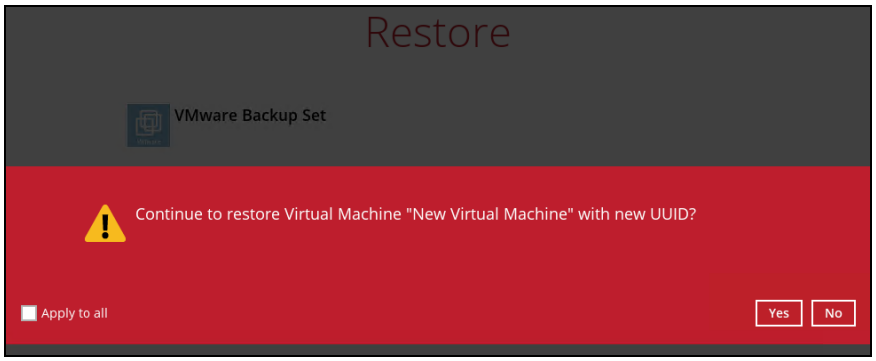
The limitation does not apply to VMware vCenter backup sets.

10. Select the temporary directory for storing temporary files.

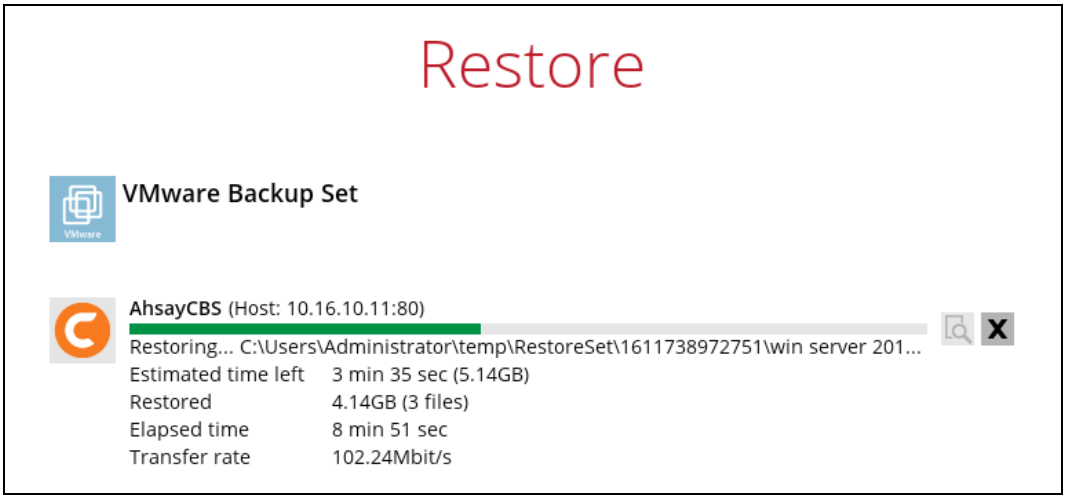


11. When restoring your guest VM, different messages will be prompted depending on your selected location.

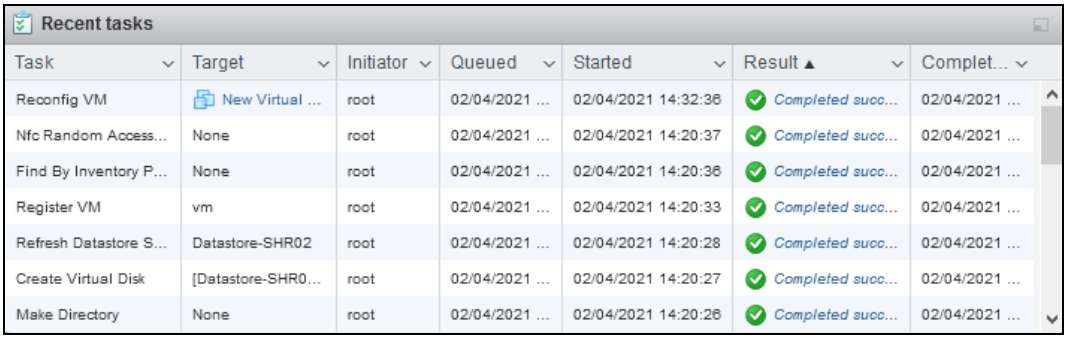
- Restoring to another VMware host, since each virtual machine is automatically assigned a universally unique identifier (UUID), a new UUID must be created when you restore the guest VM to another host. It is not possible to have two identical UUID running at the same time so make sure to click **Yes**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



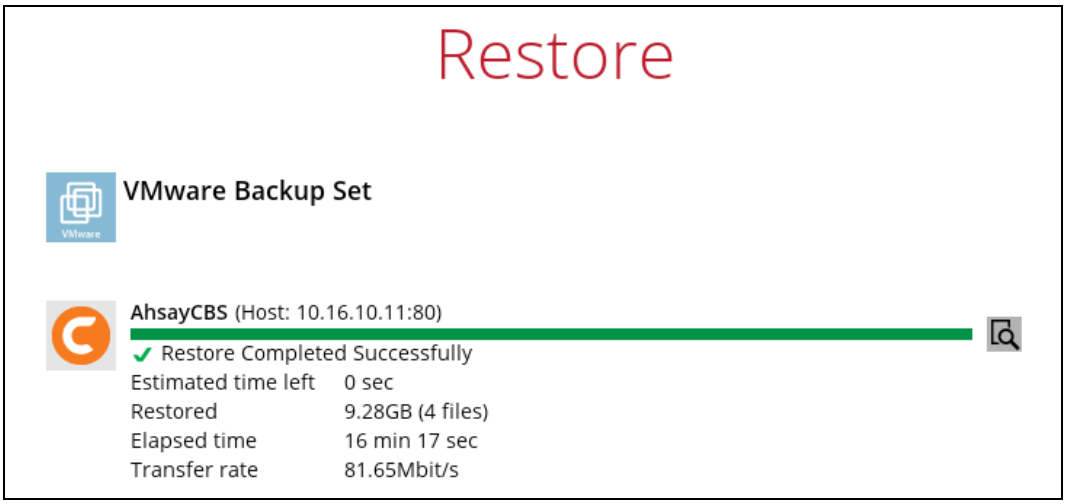
12. The status of the restore job will be displayed.



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



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



NOTE

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

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

Restoring a VM in VMDK format

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

IMPORTANT

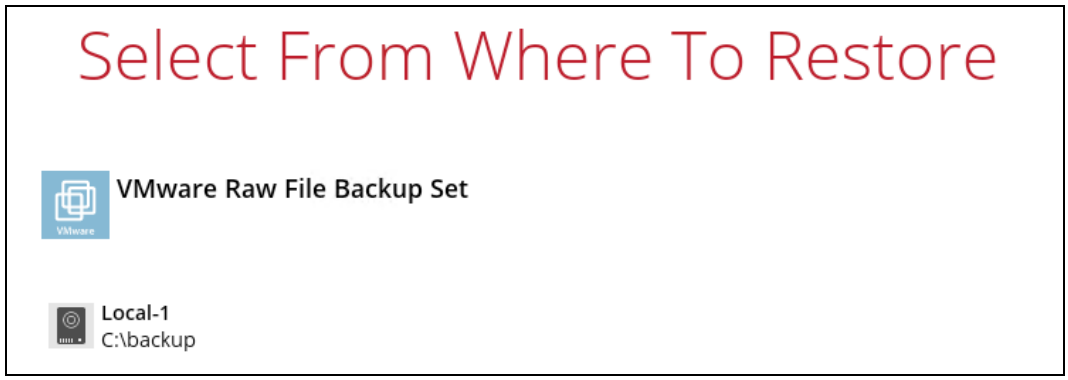
Restoring guest VMs from VDDK to VMDK format only supports backup sets that are created in AhsayOBM. Backup sets created with AhsayOBM before v7.9.0.0, or VMware VDDK backup sets migrated from v6 are **NOT** supported.

Follow the steps below for details.

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

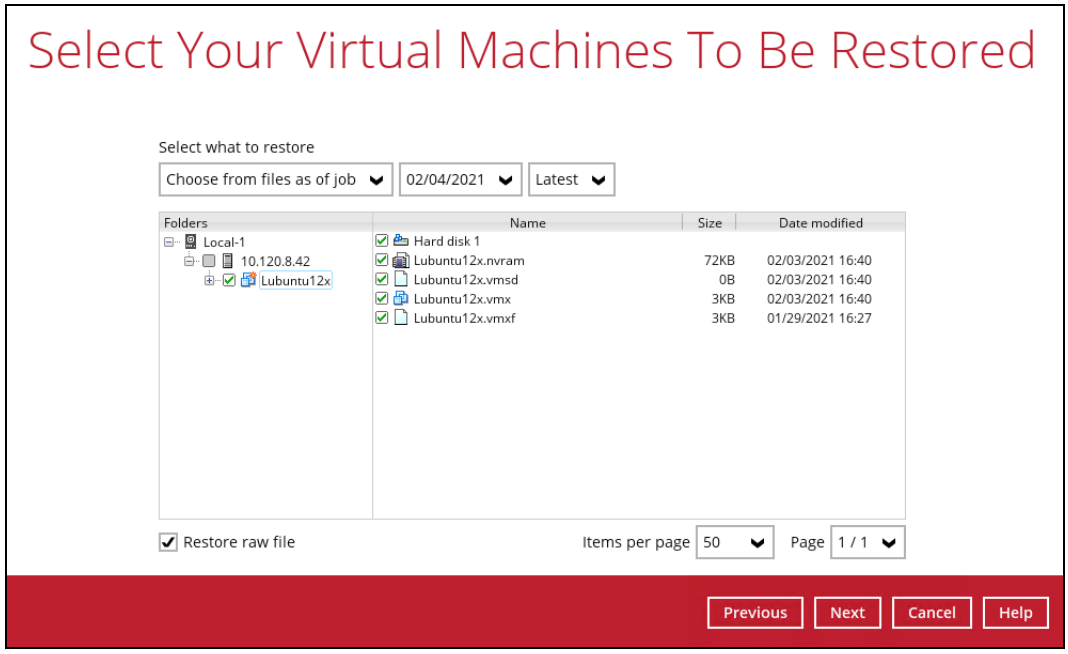
2. Select the backup set that you would like to restore the VM from.

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



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

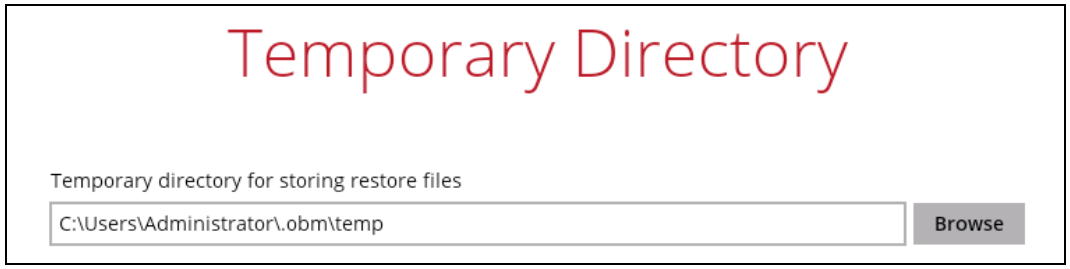
5. Select the virtual machine that you would like to restore in .vmdk format, then click the **Restore raw file** checkbox at the bottom left corner. It is possible to select multiple VM to restore in .vmdk format.



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

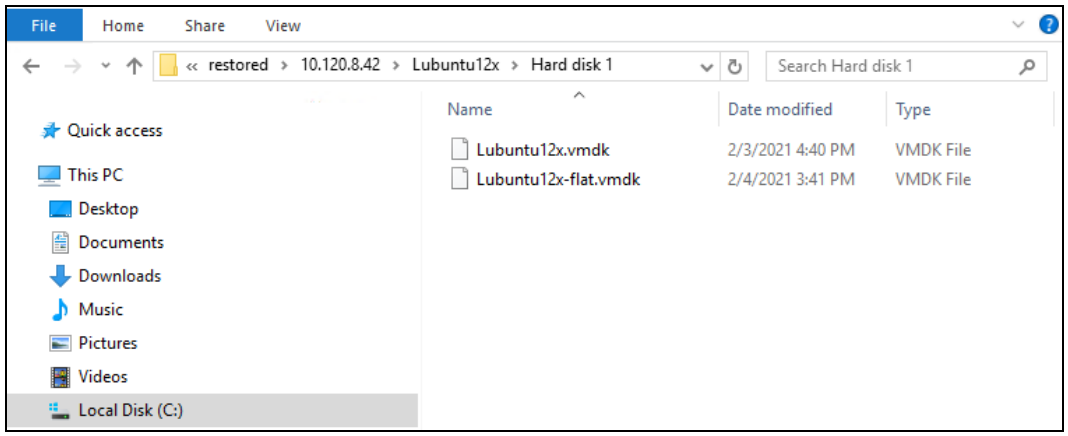
7. Click **Show advanced** option if you want to enable the Verify checksum of in-file delta files.

8. Select a temporary directory for storing restore files.

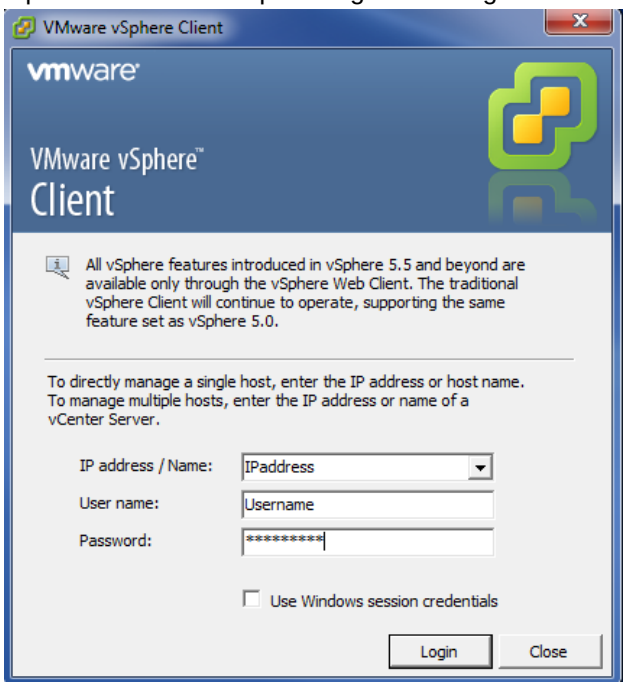


9. Click **Restore** to start the VM restore.

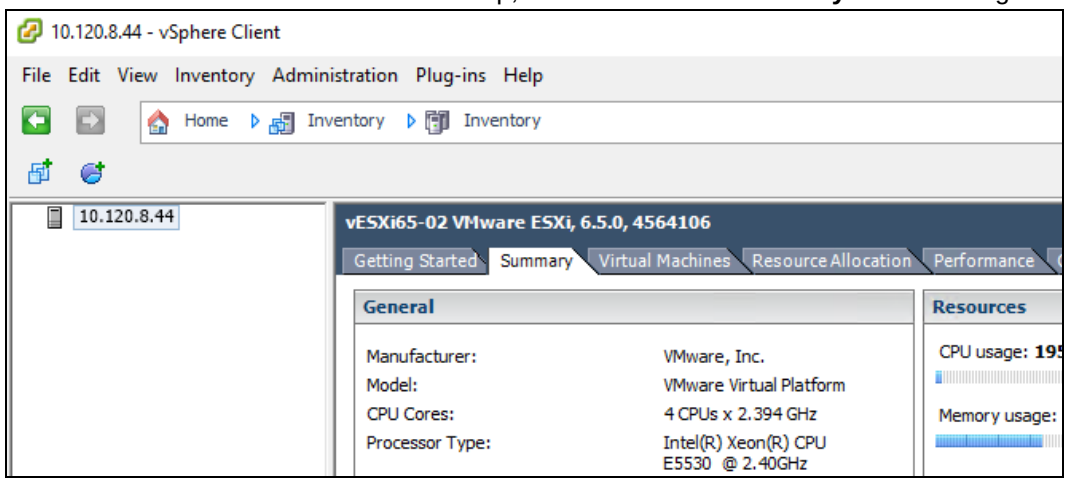
10. Open the folder where you have the VM restored. Check whether the .vmdk file has been successfully restored.



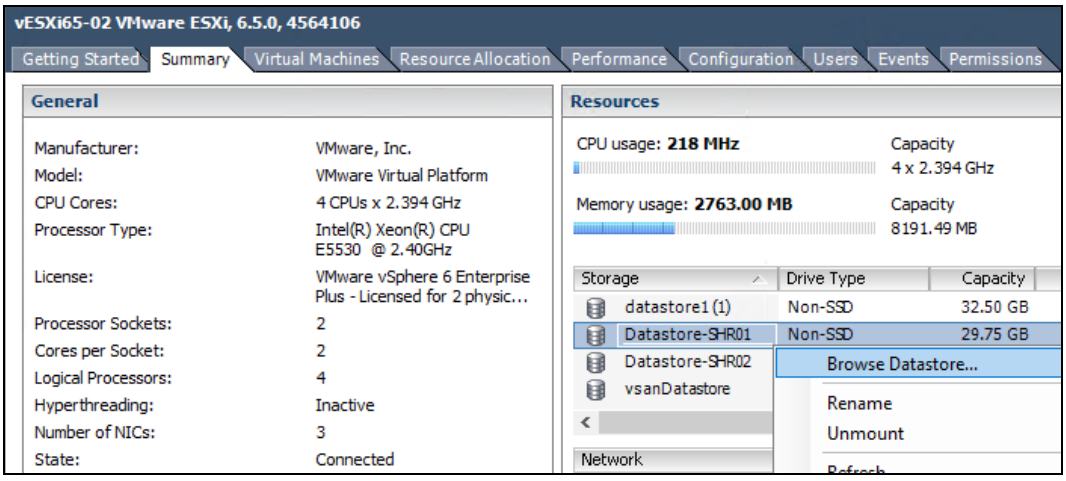
11. Open the VMware vSphere agent and log in to the ESXi server you wish to restore the VM to.



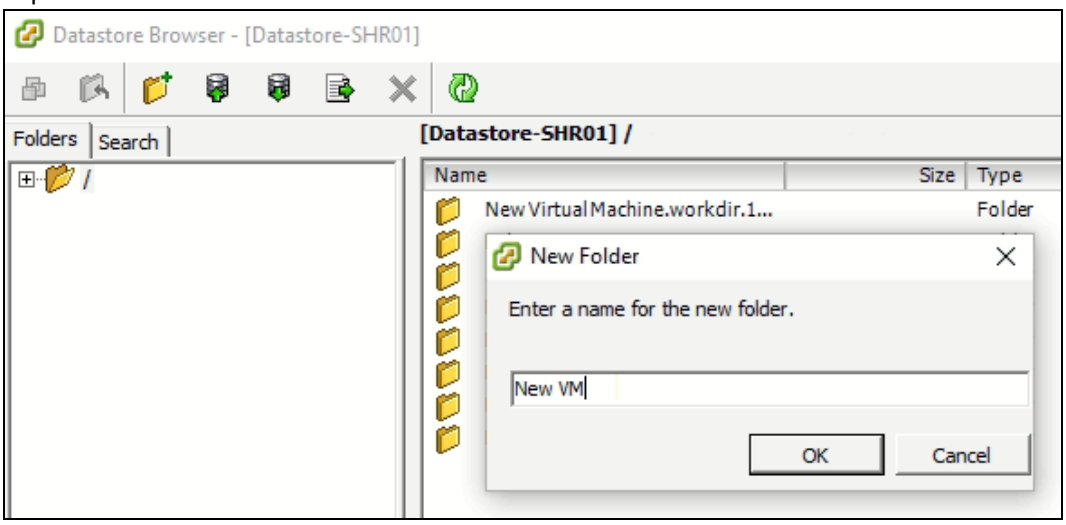
12. Click on the VM machine's name at the top, then look for the **Summary** tab on the right.



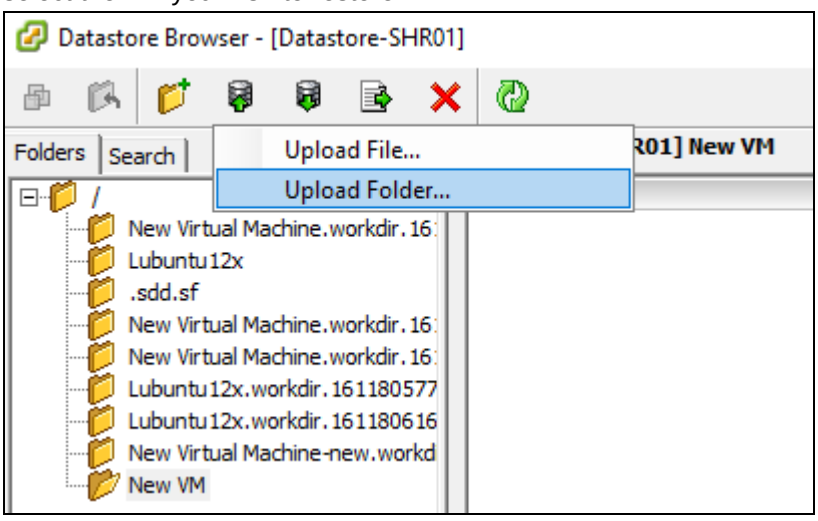
13. Right click on the Datastore where you wish to deploy the restored VM to, then click Browse Datastore.



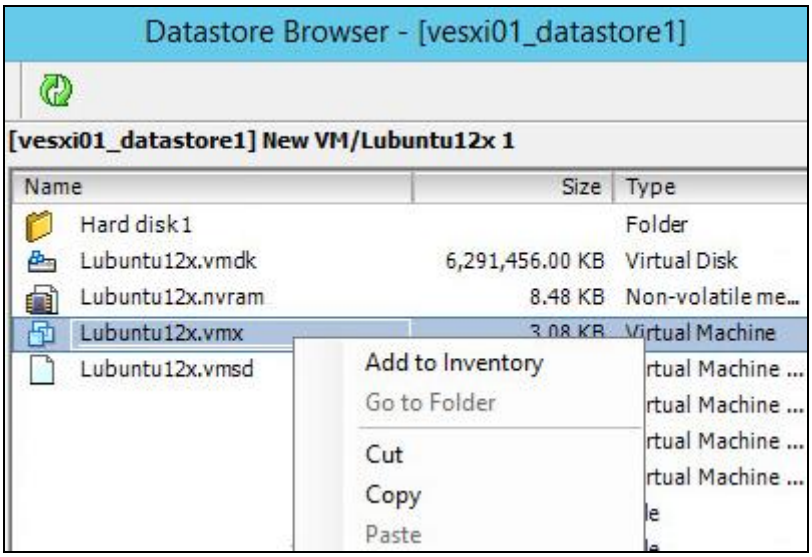
14. Right click on the right panel to open a new folder for uploading the VM you are going to import.



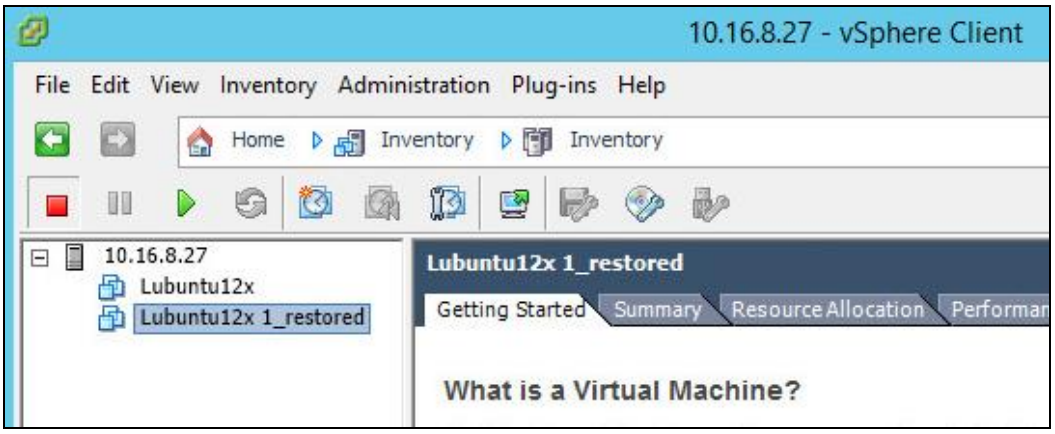
15. Open the newly created folder then click the Upload Folder option at the top menu bar to select the VM you wish to restore.



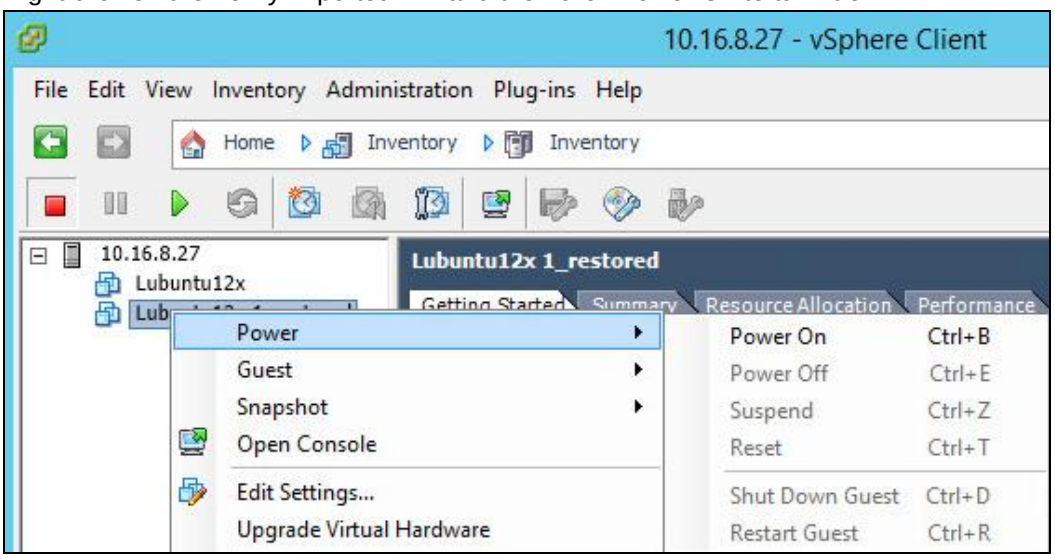
16. Open the folder you have just uploaded, then right click on the .vmx file and click on **Add to Inventory**.



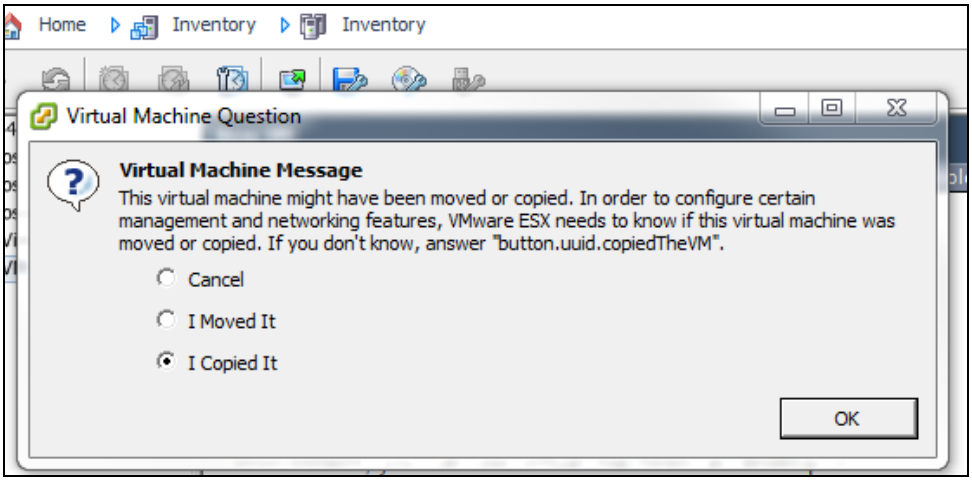
17. Follow the screen prompts and name the imported VM and confirm the resource pool. You should see the imported VM display on the left on the main page of vSphere if the VM has been successfully imported to the ESXi server.



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



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



14 Method 4 – Granular Restore

IMPORTANT

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

- Microsoft Visual C++ 2015 Redistributable (x86) / (x64)
  https://www.microsoft.com/en-us/download/details.aspx?id=48145
- Update for Universal C Runtime in Windows
  https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows
- Microsoft Security Advisory 3033929 (for Windows 7 and Windows Server 2008 R2)
  https://technet.microsoft.com/en-us/library/security/3033929.aspx

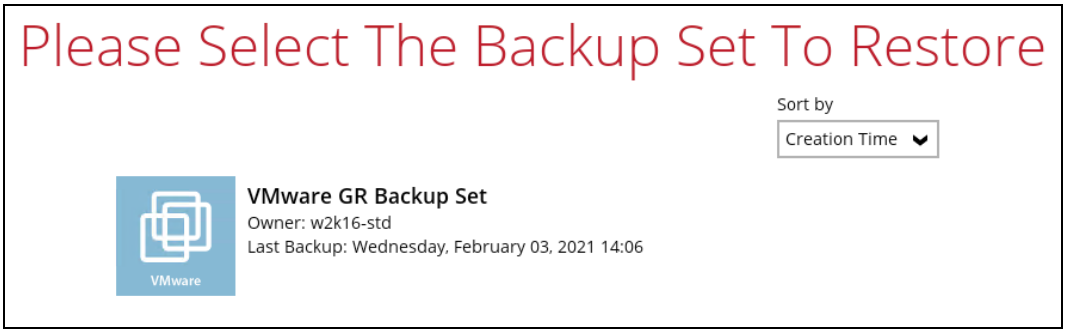
Requirements and Limitations

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

Start Granular Restore

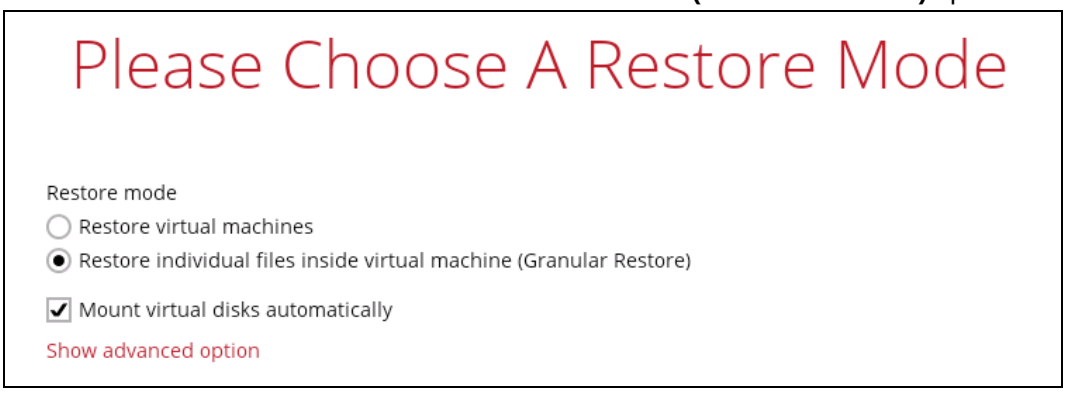
1. Click the **Restore** icon on the main interface of AhsayOBM.

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



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

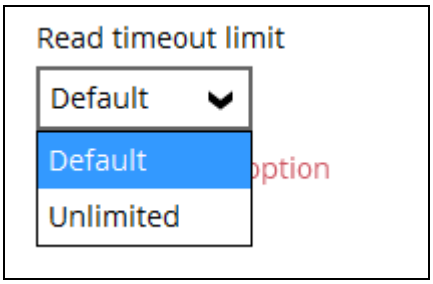
4. Select to the **Restore individual files in virtual machine (Granular Restore)** option.



NOTE

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

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



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

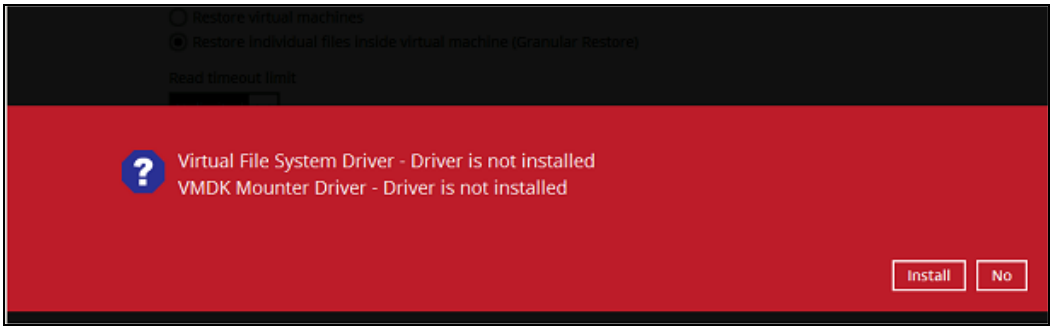
- **Default** – This setting should be suitable for guest VMs located on a local, removable, or network drive. The time out value is 15 seconds.
- **Unlimited** – the connection will not time out when this is selected. This selection is recommended when:
  - Backup destination is a cloud stroage.
  -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

NOTE

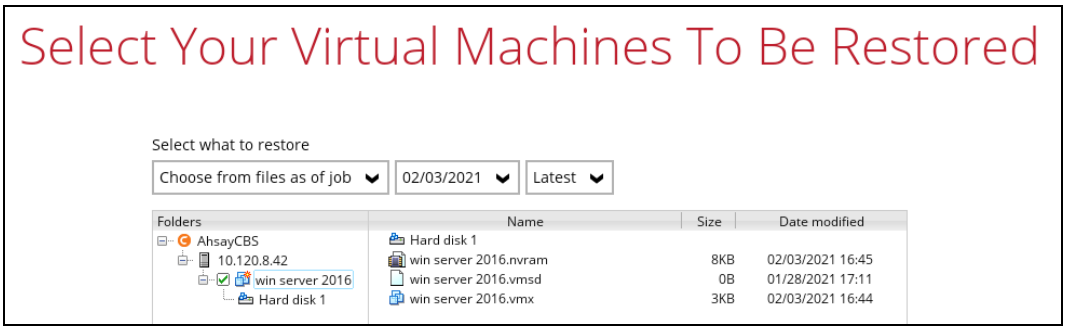
If in doubt or unsure about the guest VM size or network stability, it is recommended to use **Unlimited**.

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

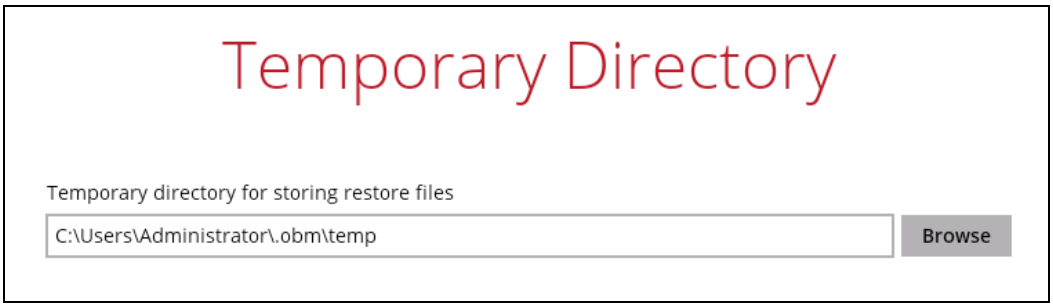
5. The following screen will be shown when you perform Granular Restore for a backup set on this machine for the first time only. Make sure you click **Install** to confirm starting the installation of the drivers on this machine. Clicking **No** will exit the restore process.



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



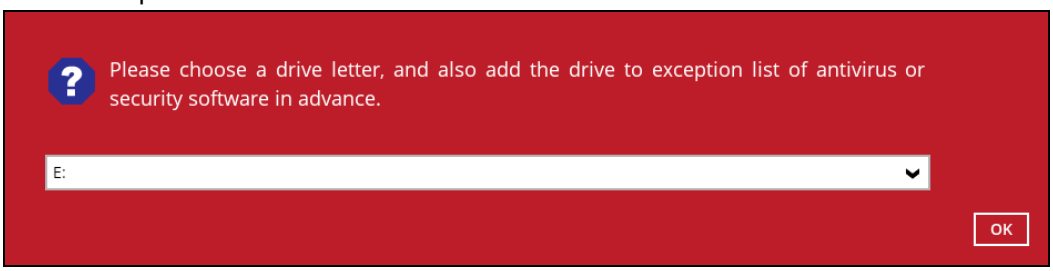
7. Select a temporary directory for storing restore files, then click **Restore** to start the Granular Restore.



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

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

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



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

Otherwise, all the virtual disks will be automatically mounted.

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

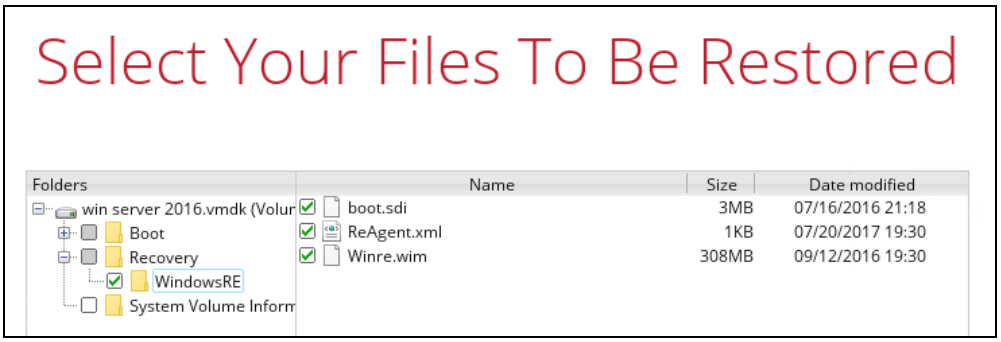
There are two options to restore individual files from here.

Option 1: Restore Using AhsayOBM File Explorer

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

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

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

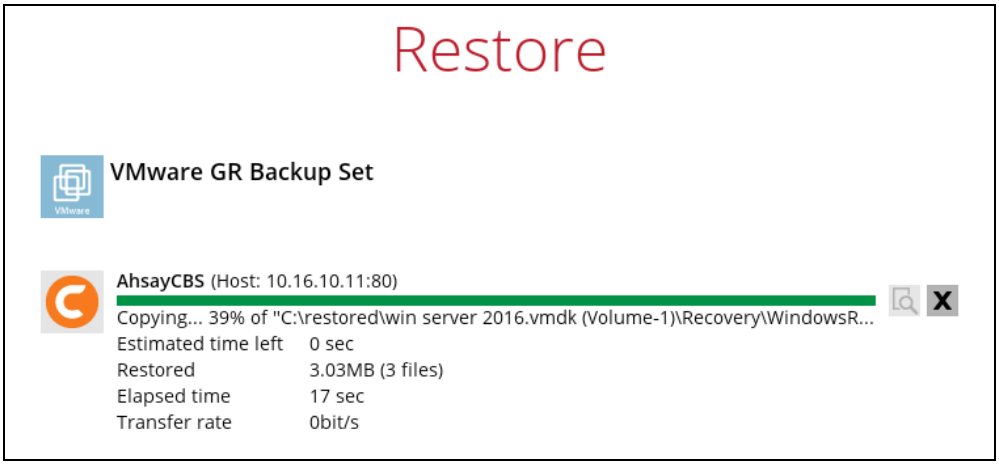


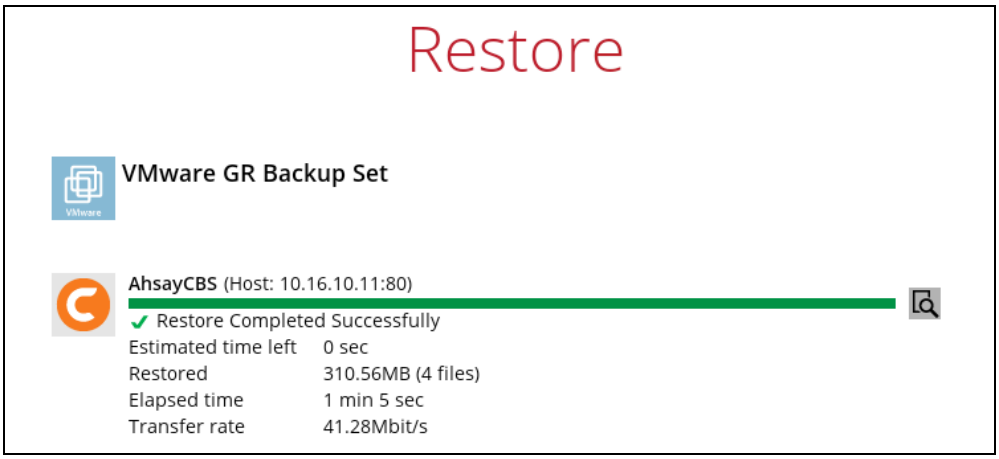
NOTE

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

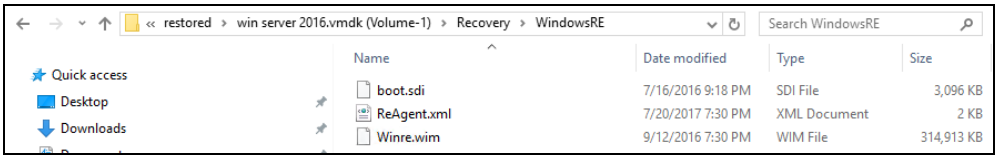
ii. Select a path where you wish the files to be restored to, then click **Restore**.

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





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



Option 2: Restore Using Windows File Explorer

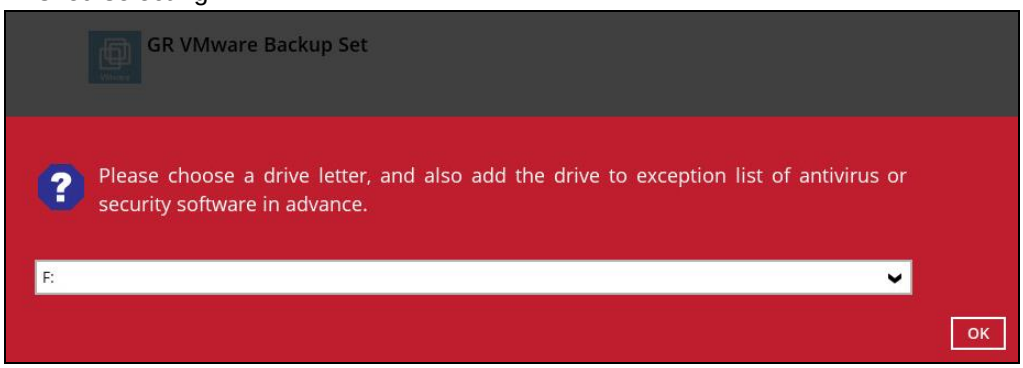
This method allows you to browse through the files from the mounted virtual disk through the Windows File Explorer on the machine where you have AhsayOBM installed on.

NOTE

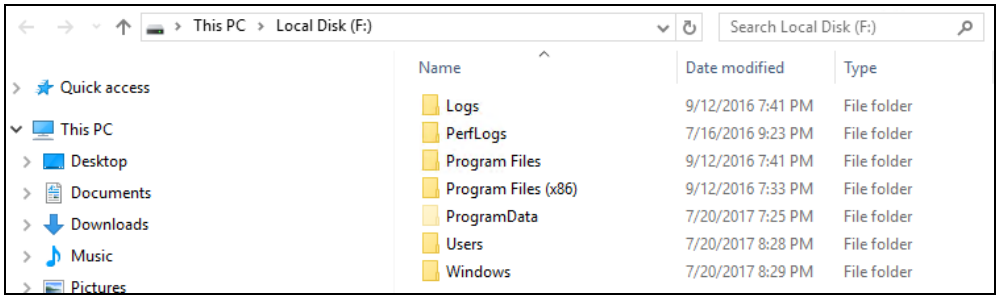
Granular restore of VMware backup sets performed using Windows File Explorer:

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

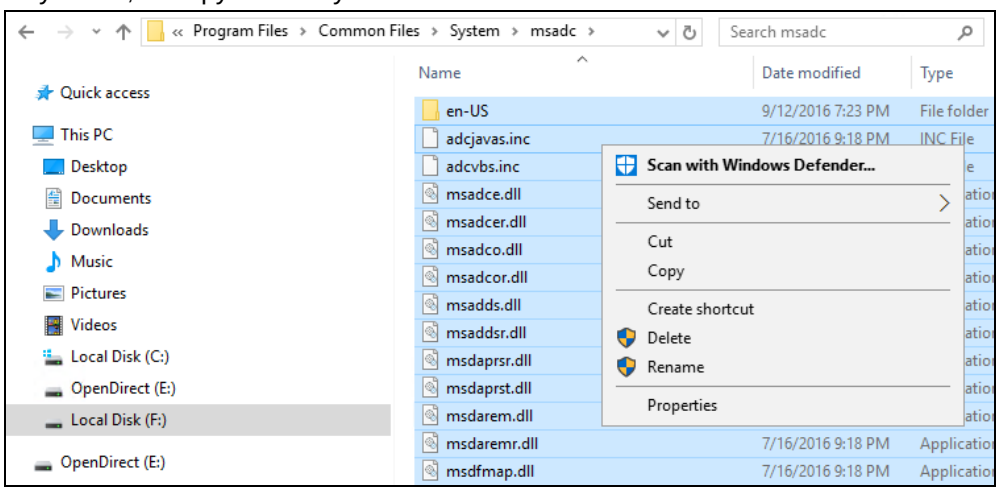
i. Click  and then you will be prompted to select a driver letter where you wish the mounted backup image to be mapped on your machine, click **OK** when you have finished selecting.



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



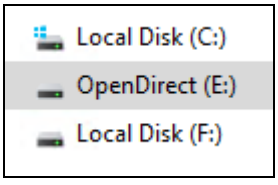
iii. You can now click on the files to view them directly from here, which will be in read-only mode, or copy them to your local machine.



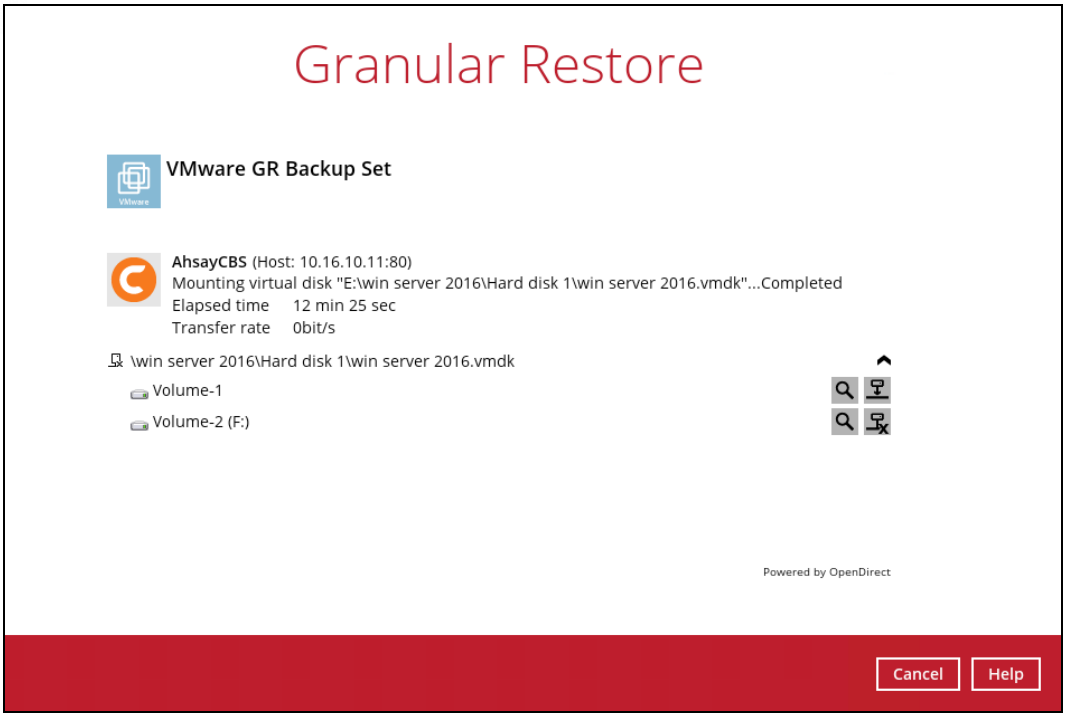
NOTE

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

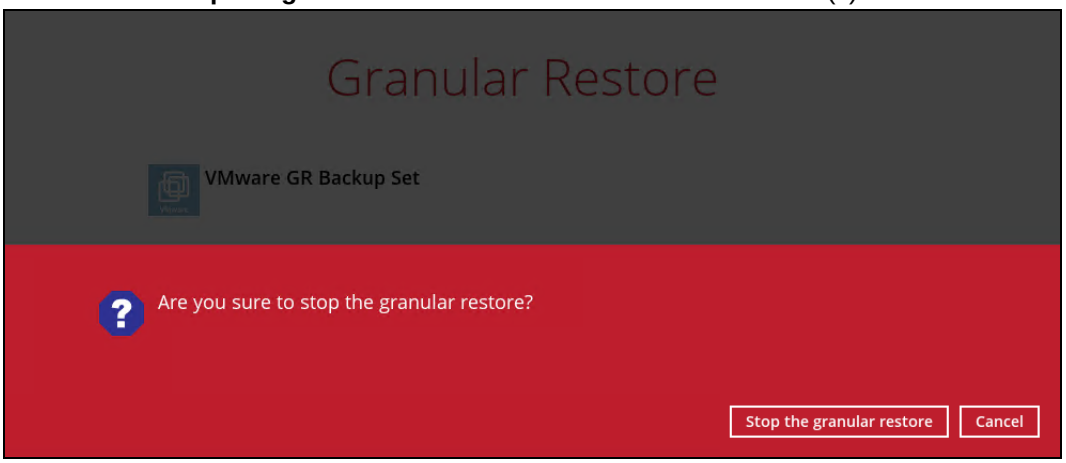
iv. The mounted drive letter cannot be ejected from the Windows File Explorer, and it will only be closed when you exit AhsayOBM.



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



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



IMPORTANT

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

15 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 without Run Direct
  - Restore backup from vSAN datastore to vSAN datastore
  - Restore backup from vSAN datastore to VMFS datastore
  - Restore backup from VMFS datastore to vSAN datastore
- Restore with Run Direct
  - Restore backup from vSAN datastore to vSAN datastore
  - Restore backup from vSAN datastore to VMFS datastore
  - Restore backup from VMFS datastore to vSAN datastore

LIMITATIONS

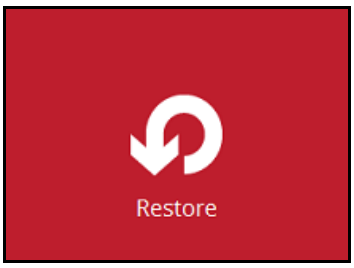
- Restore of guest VMs on a Stretched vSAN Cluster will be slower.

  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.

15.1 Restore a backup from vSAN datastore to vSAN datastore without Run Direct

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

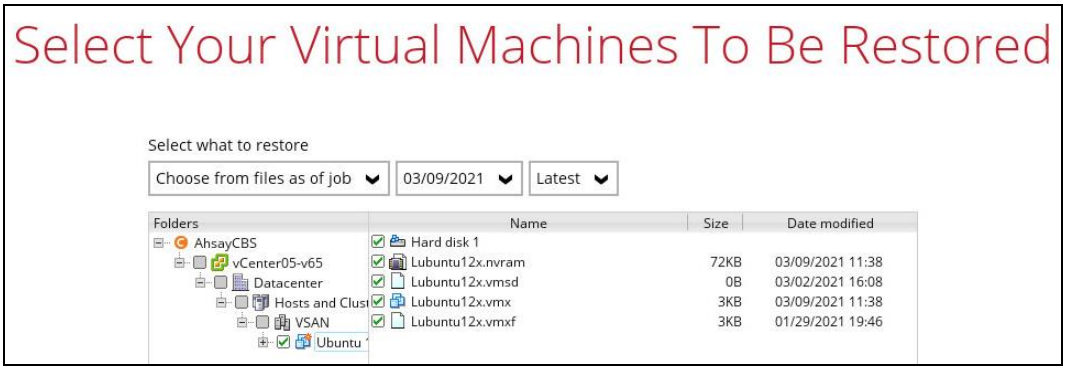


2. Select the backup set that you would like to restore the VM from.

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

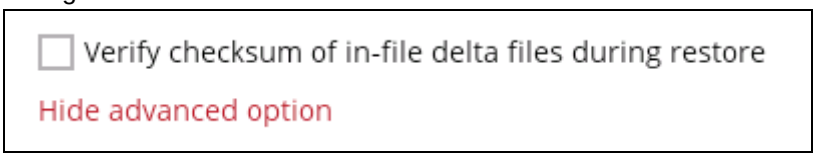
4. If Granular Restore is enabled in the backup set this screen will be displayed, select the restore mode. Otherwise proceed to the next step.

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



6. Select to restore the VM to the **Original location**. If the backup set has **Run Direct** enabled, by default it will be enabled here. Uncheck **Run Direct** to disable it.

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

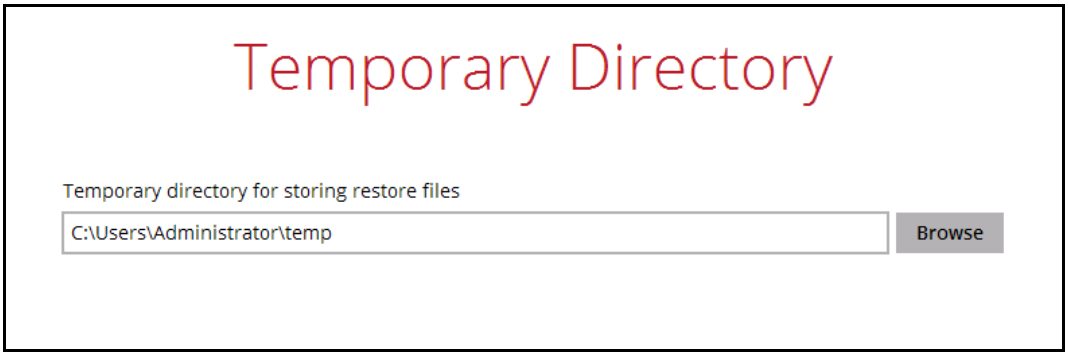


NOTE

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

Click **Next** to proceed.

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



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

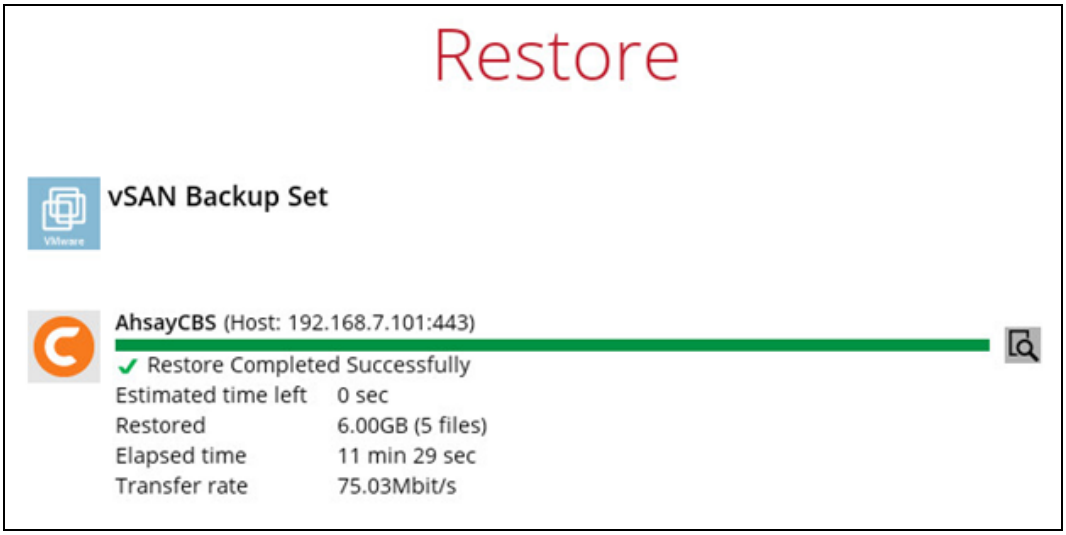
- Restoring guest VM to original location, this message will only be displayed if the original guest VM exists on the datastore. Click **Yes** to proceed.

- 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.

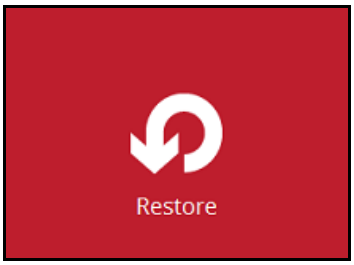
- Another way of checking the progress of the restore is from vSphere. The restore has started when the virtual machine was unregistered. And it is completed when the virtual machine was reconfigured.

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



15.2 Restore a backup from vSAN datastore to VMFS datastore without Run Direct

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

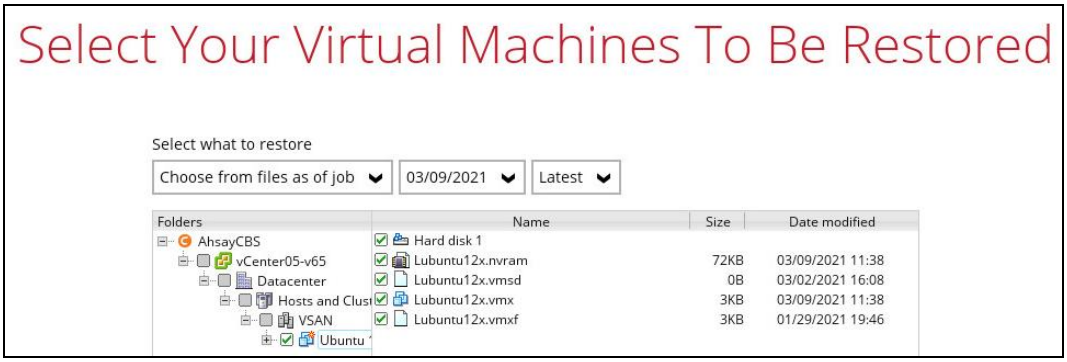


2. Select the backup set that you would like to restore the VM from.

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

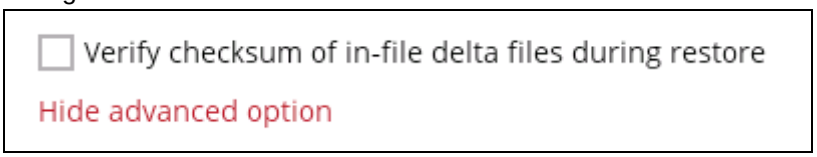
4. If Granular Restore is enabled in the backup set this screen will be displayed, select the restore mode. Otherwise proceed to the next step.

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



6. 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, by default it will be enabled here. Uncheck **Run Direct** to disable it.

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

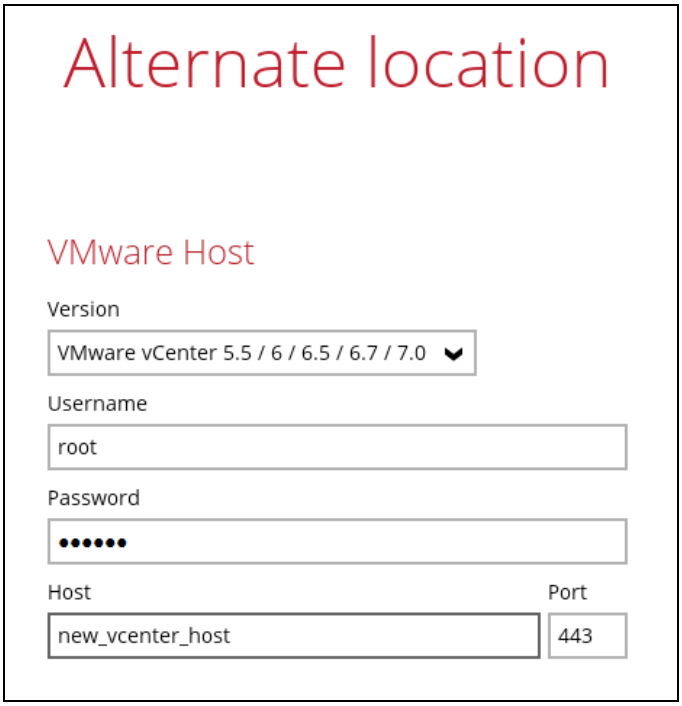


NOTE

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

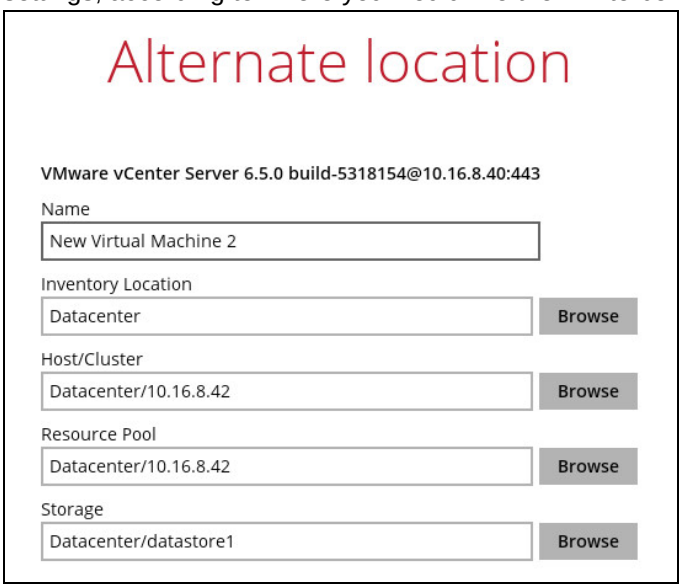
8. This step applies only for restoring to **Alternate location**.

   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.

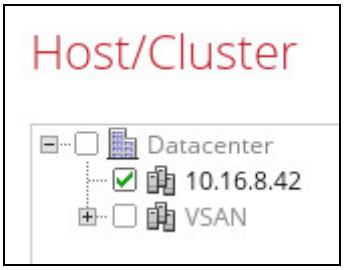


Press **Next** to proceed when you are done with the settings.

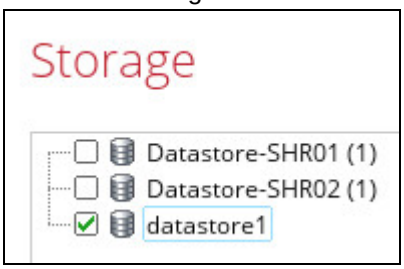
Enter a new **Name** for the VM, then **Browse** to modify the **Host/Cluster** and **Storage** settings, according to where you would like the VM to be restored to.



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

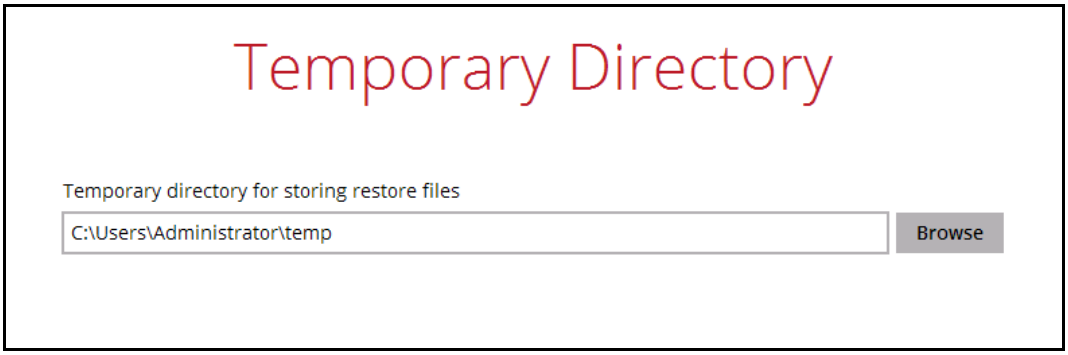


Select the storage.



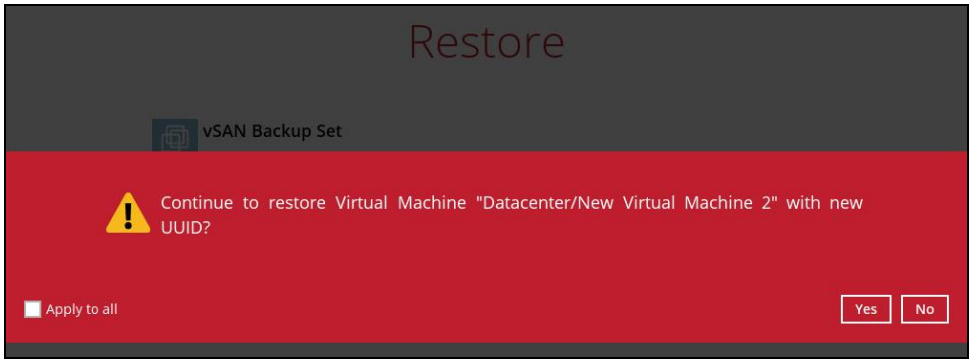
Click **Next** to proceed when you are done with the settings.

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

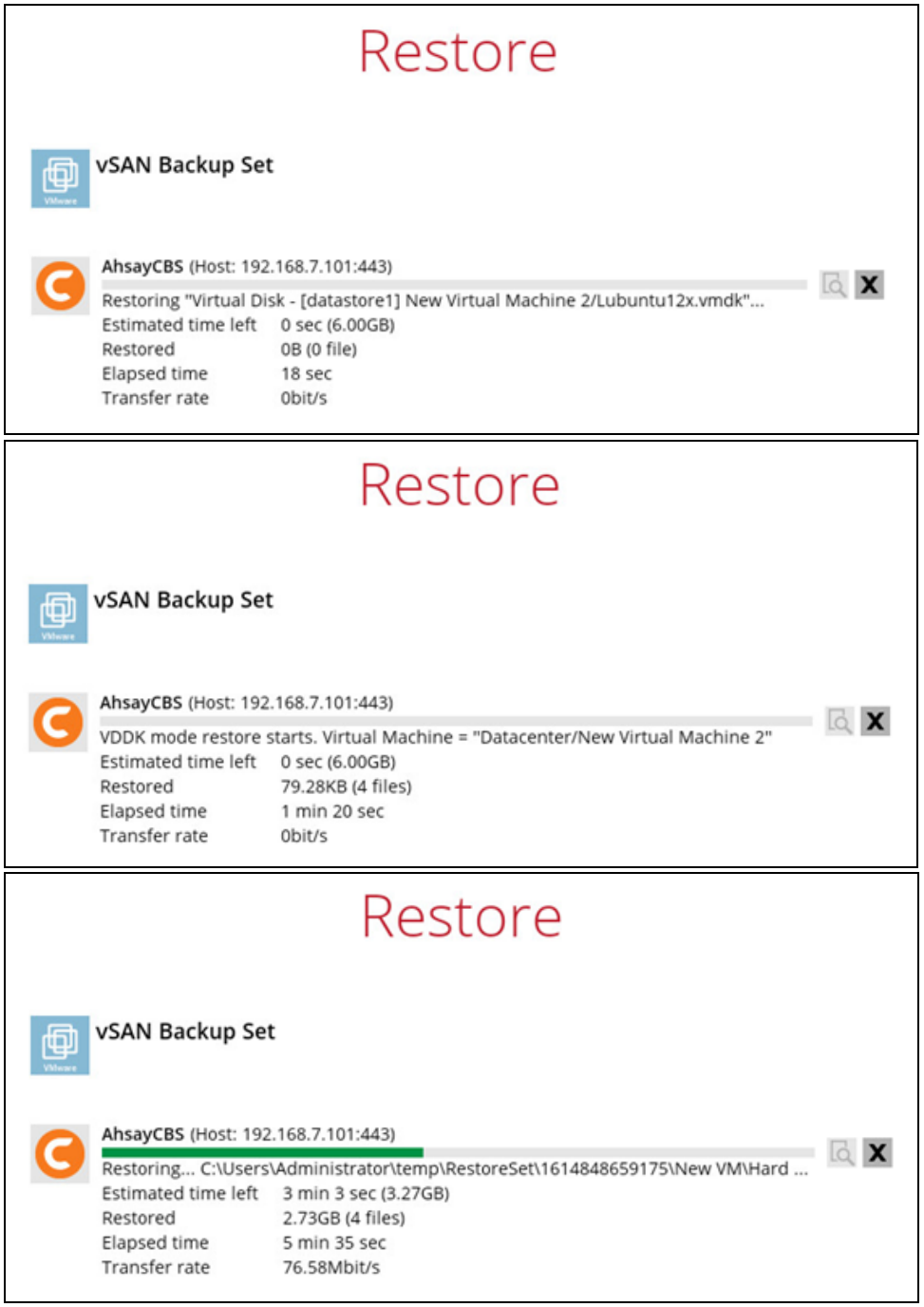


10. When restoring your guest VM, different messages will be prompted depending on the selected location.

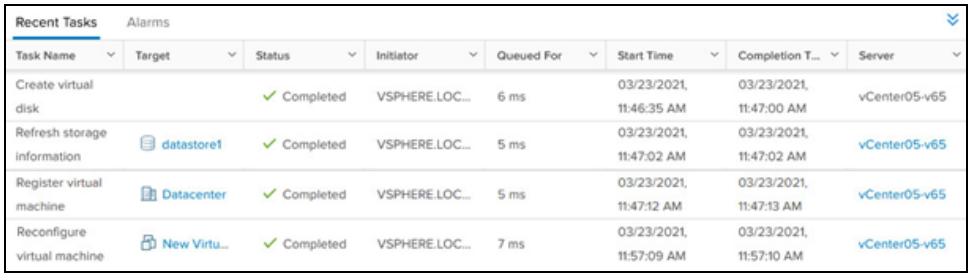
- Restoring guest VM to another VMware host, since each virtual machine is automatically assigned a universally unique identifier (UUID), a new UUID must be created when you restore the guest VM to another host. It is not possible to have two identical UUID running at the same time, so make sure to click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



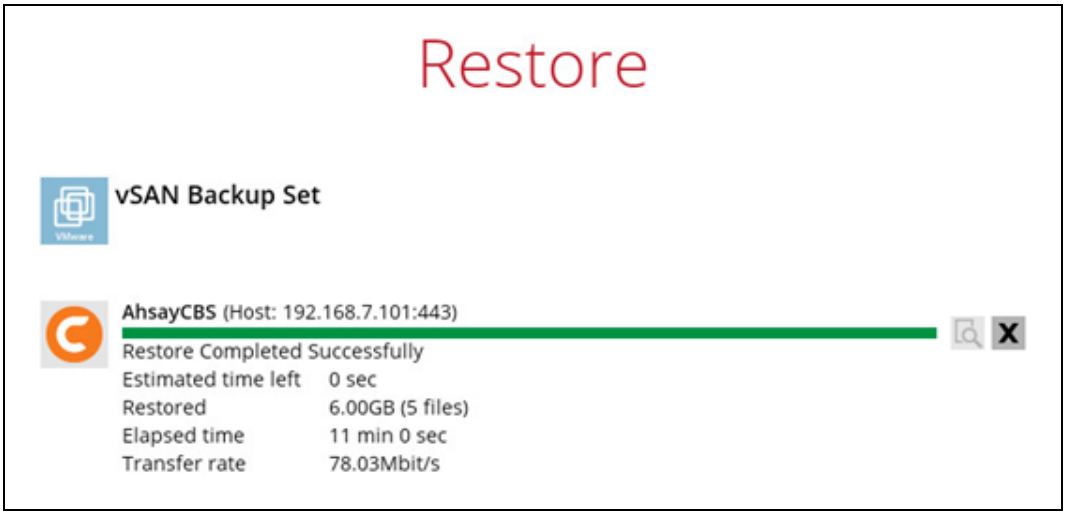
- The progress of the restore can be seen from the status bar.



- 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.



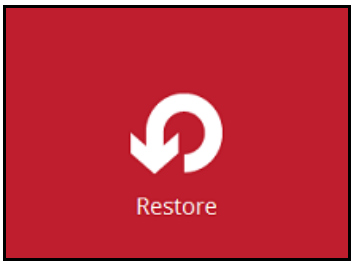
11. The following screen shows when the VM has been restored successfully.



.

15.3 Restore a backup from VMFS datastore to vSAN datastore without Run Direct

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

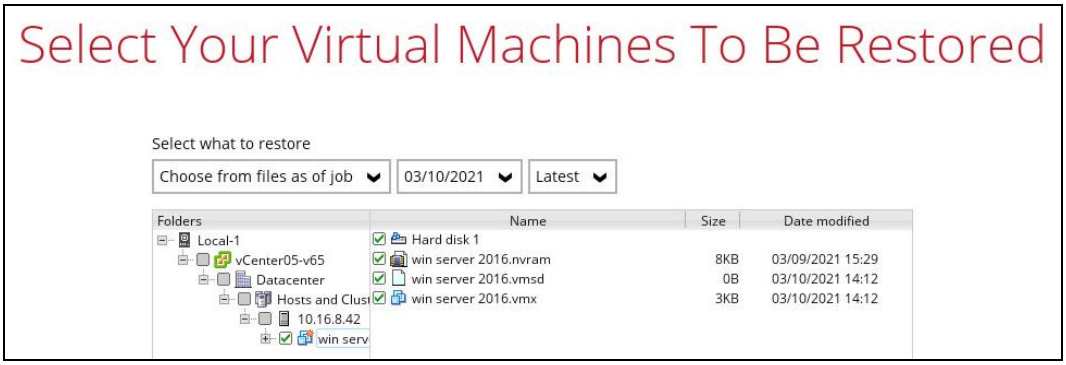


2. Select the backup set that you would like to restore the VM from.

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

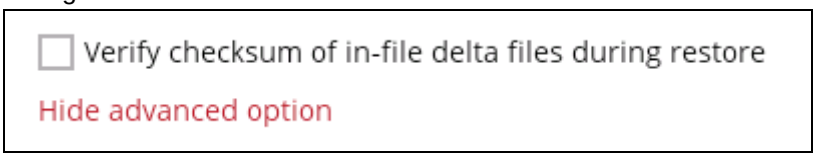
4. If Granular Restore is enabled in the backup set this screen will be displayed, select the restore mode. Otherwise proceed to the next step.

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



6. 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, by default it will be enabled here. Uncheck **Run Direct** to disable it.

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

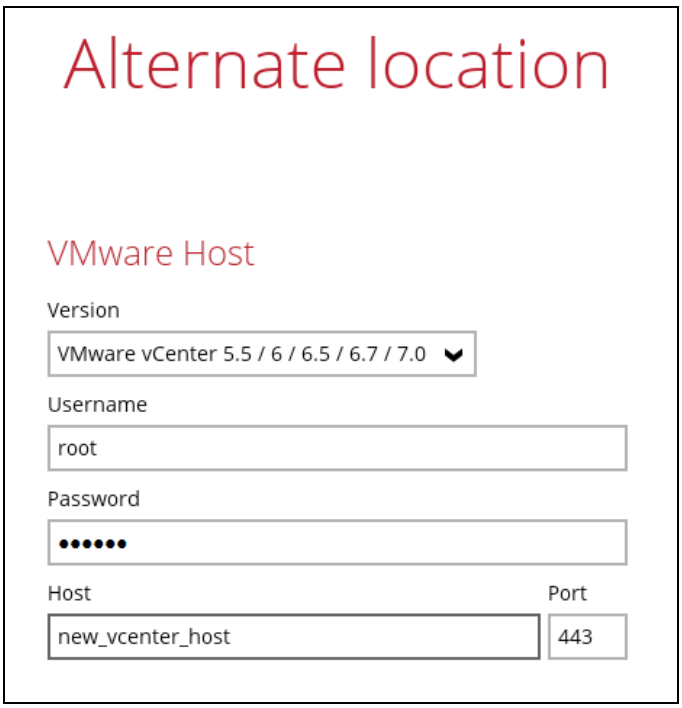


NOTE

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

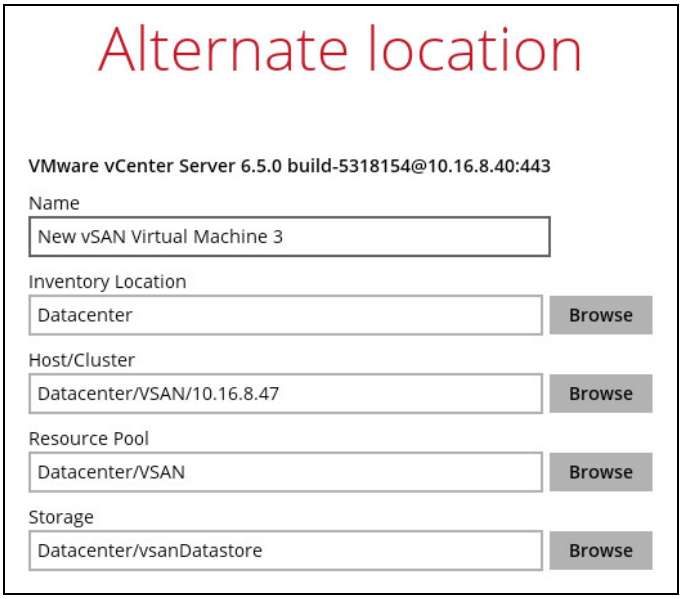
8. This step applies only for restoring to **Alternate location**.

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.



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

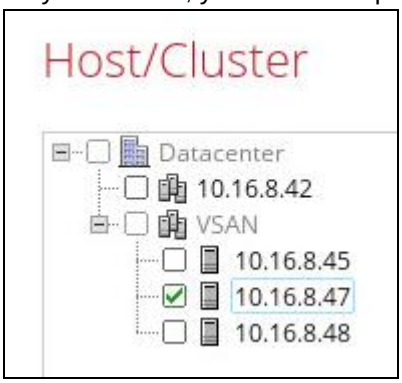
Enter a new **Name** for the VM, then **Browse** to modify the **Host/Cluster** and **Storage** settings to select the alternate vSAN datastore, according to where you would like the VM to be restored to.



NOTE

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

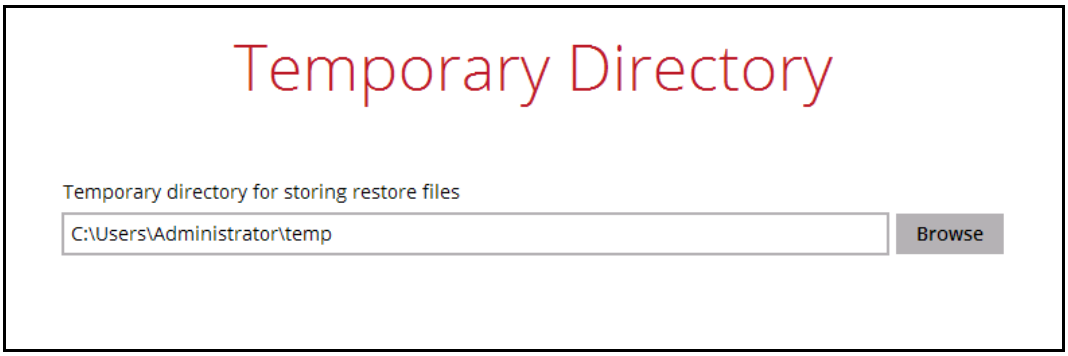
As you can see, you need to expand the vSAN to be able to select the host.



Select the vSAN storage.

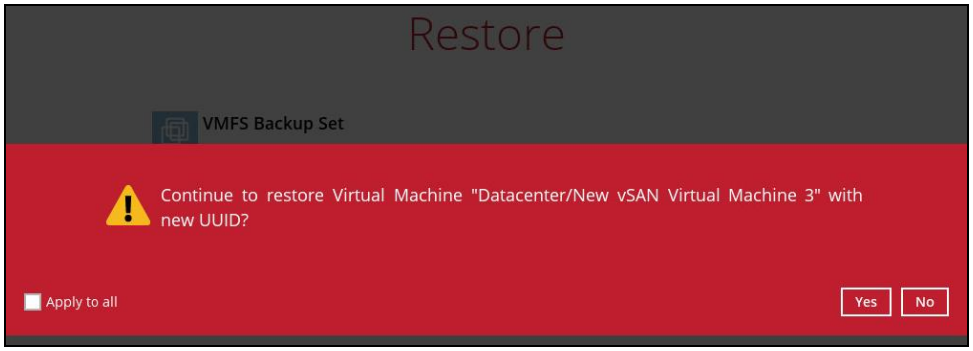
Click **Next** to proceed when you are done with the settings.

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

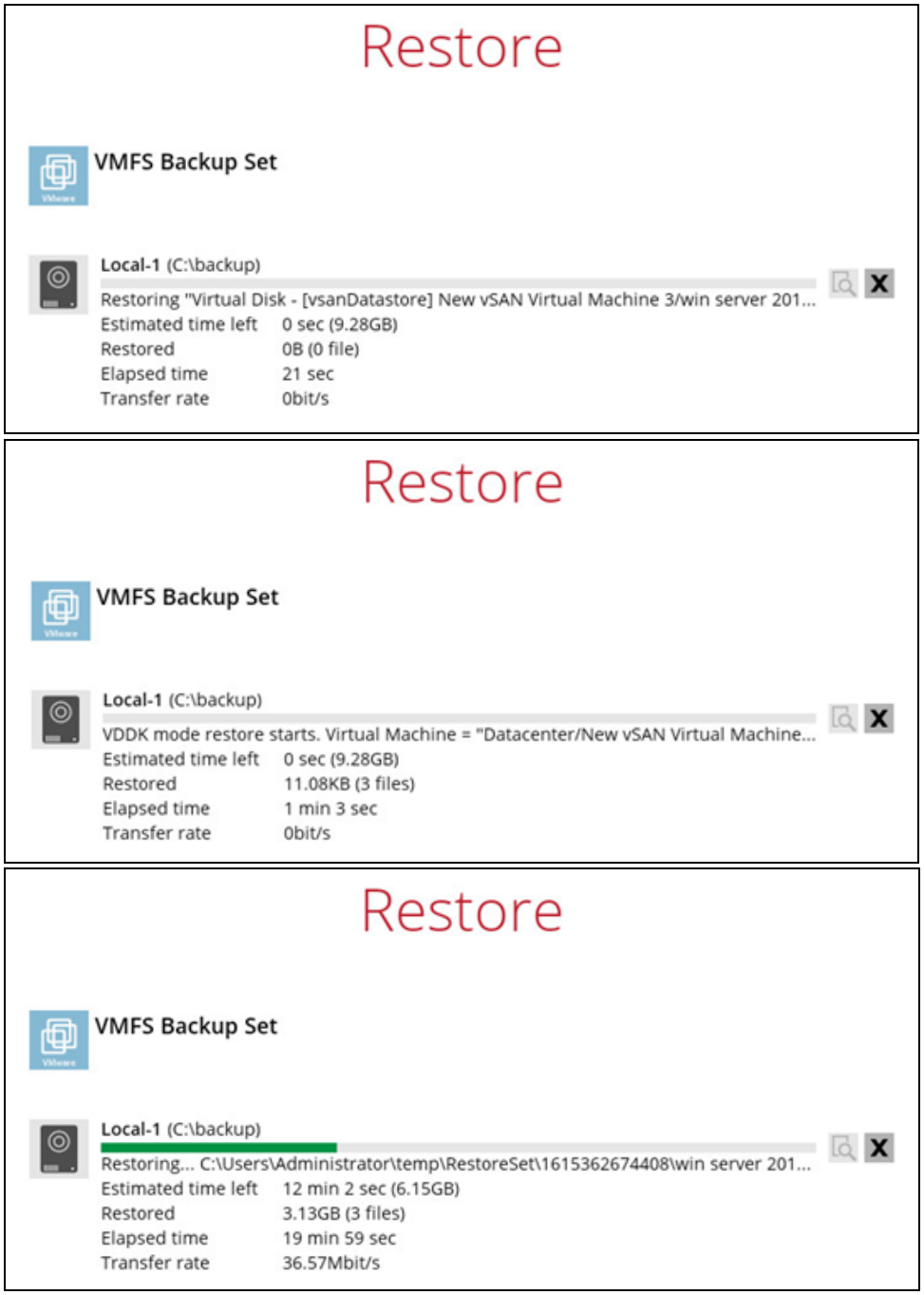


10. When restoring your guest VM, different messages will be prompted depending on the selected location.

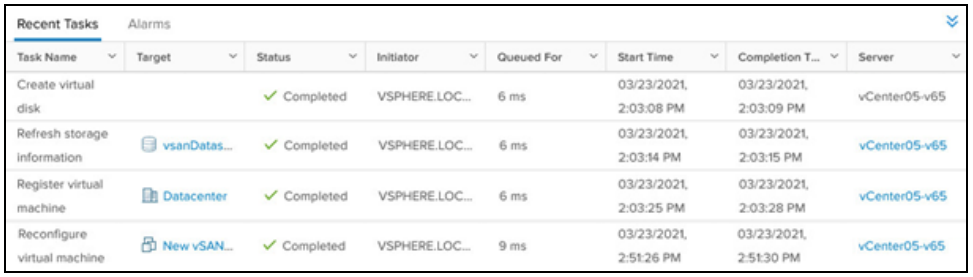
- Restoring guest VM to another VMware host, since each virtual machine is automatically assigned a universally unique identifier (UUID), a new UUID must be created when you restore the guest VM to another host. It is not possible to have two identical UUID running at the same time, so make sure to click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



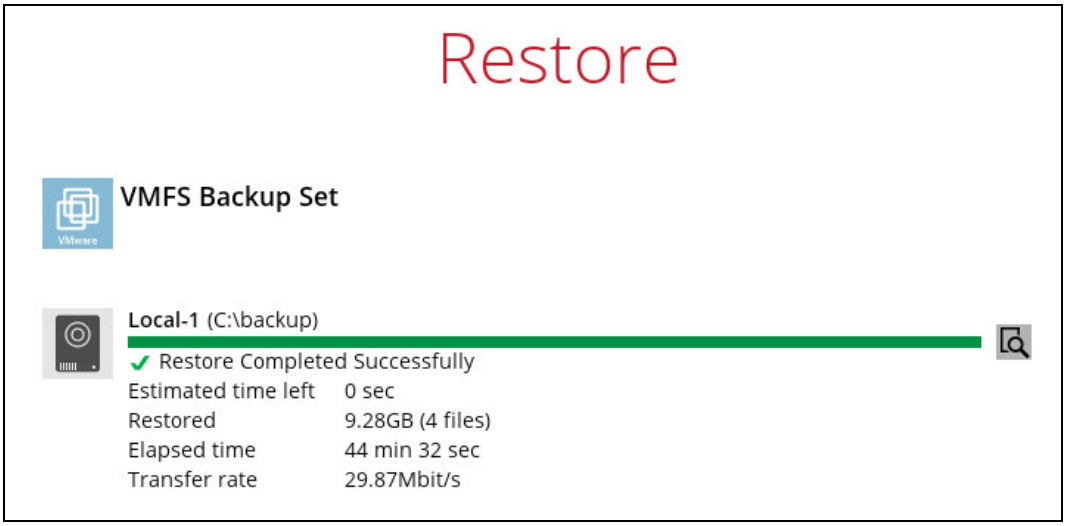
- The progress of the restore can be seen from the status bar.



- 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.



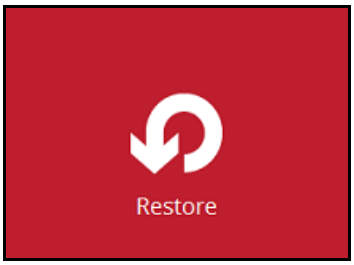
11. The following screen shows when the VM has been restored successfully.



.

15.4 Restore a backup from vSAN datastore to vSAN datastore with Run Direct

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



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

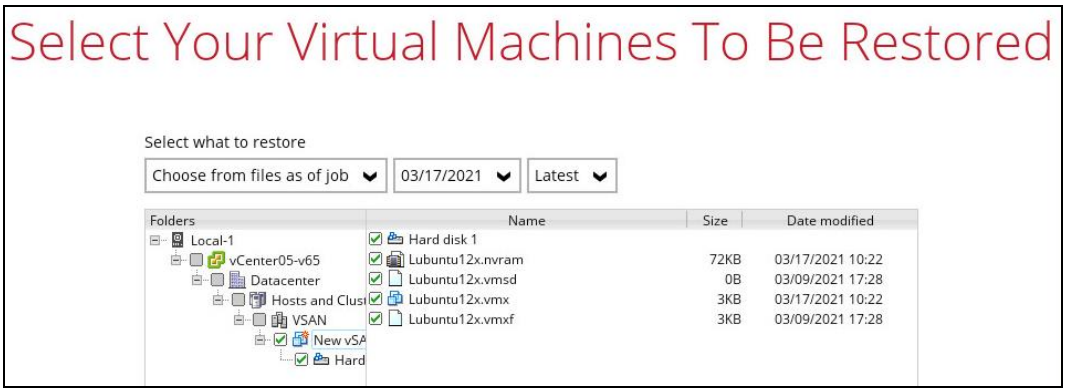
3. Select the backup destination that contains the VM that you would like to restore.

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

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

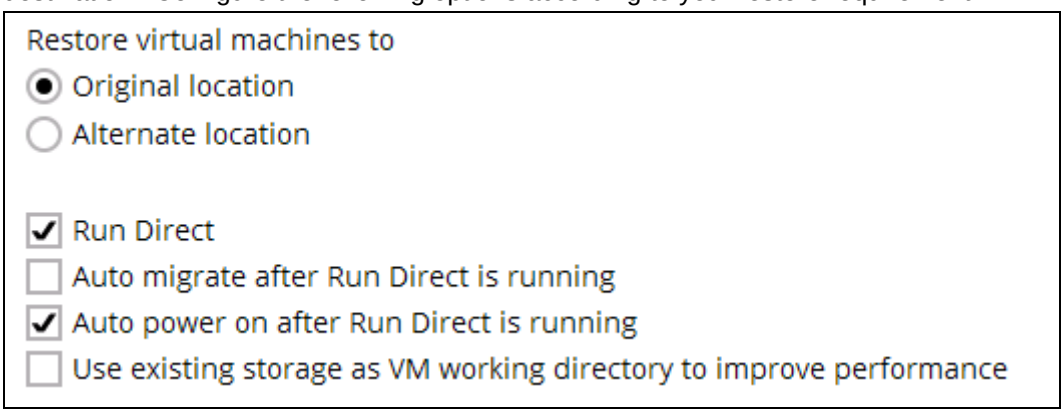
IMPORTANT

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



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

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



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

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

NOTE

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

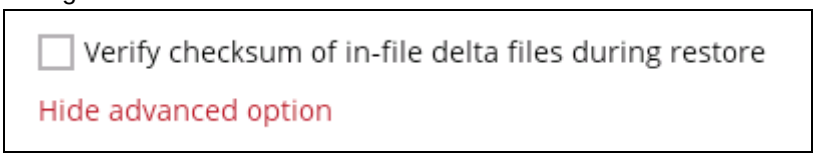
- **Auto power on after Run Direct is running**

  Enable this option to power up the virtual machine automatically, after Run Direct is running for the VM.

- **Use existing storage as VM working directory to improve performance**

  Enable this option to enhance performance of the restored VM.

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

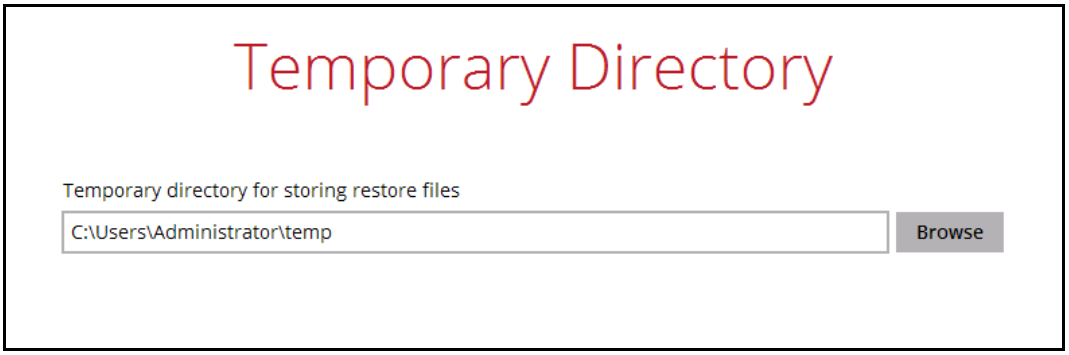


NOTE

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.

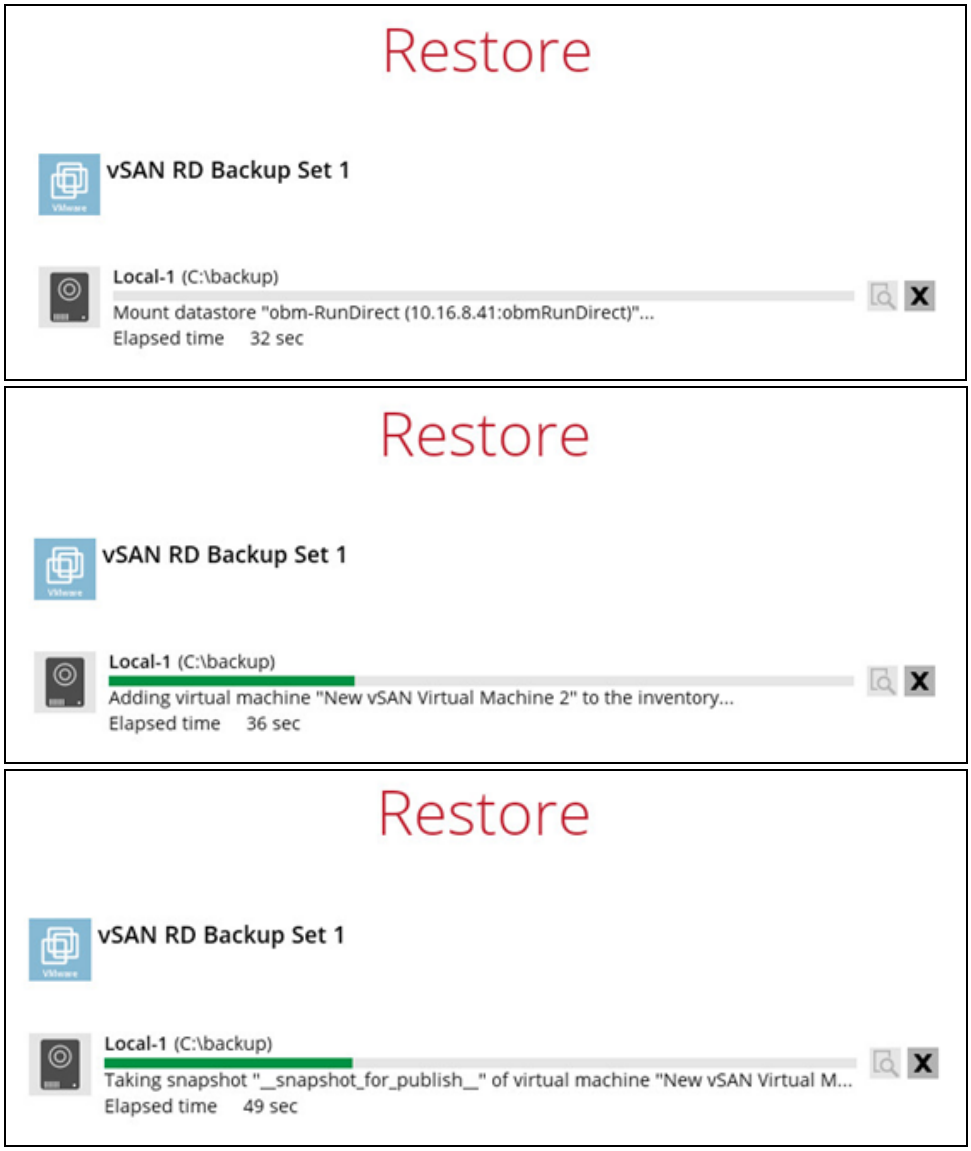
9. Select the temporary directory for storing temporary files, then click **Restore** to start the restoration.



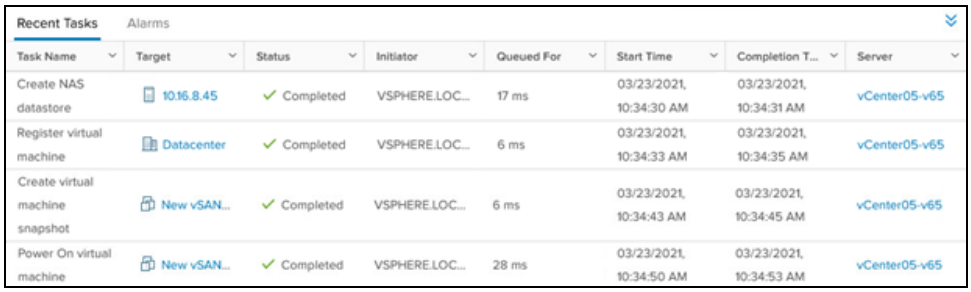
10. When restoring your guest VM, different messages will be prompted depending on the selected location.

- 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.

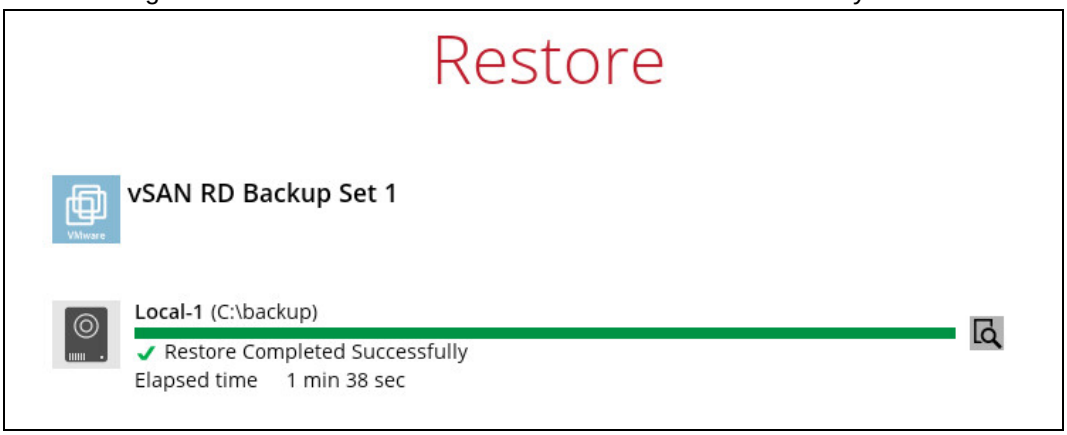
- The progress of the restore can be seen from the status bar.



- 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.



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

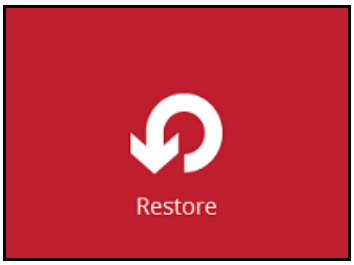


NOTE

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

15.5 Restore a backup from vSAN datastore to VMFS datastore with Run Direct

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



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

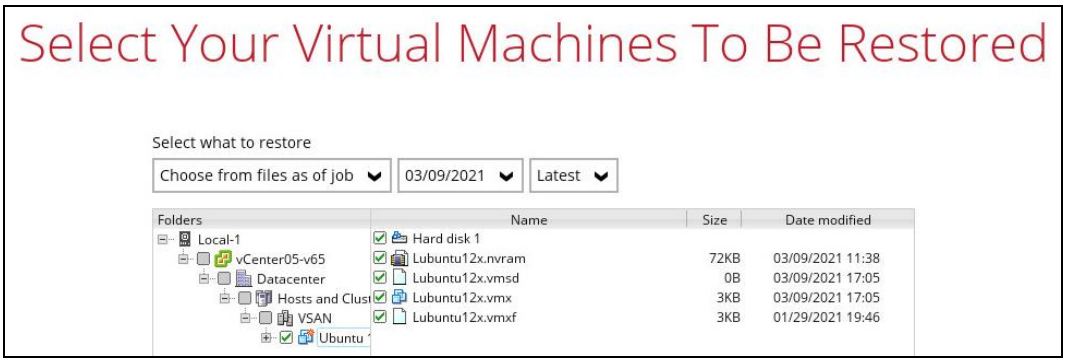
3. Select the backup destination that contains the VM that you would like to restore.

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

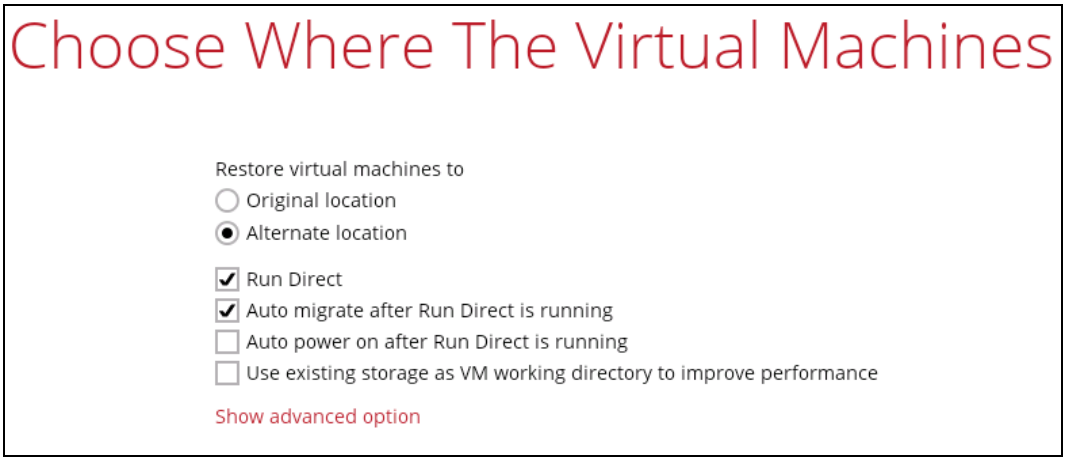
5. Select the virtual machine that you would like to restore.

IMPORTANT

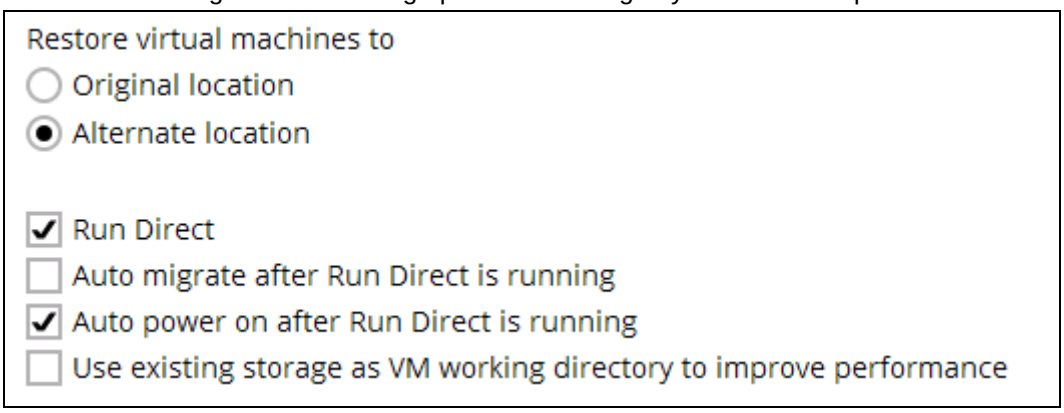
When performing a Run Direct restore to **Alternate Location**, only one VM can be selected per restore session.



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



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



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

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

NOTE

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

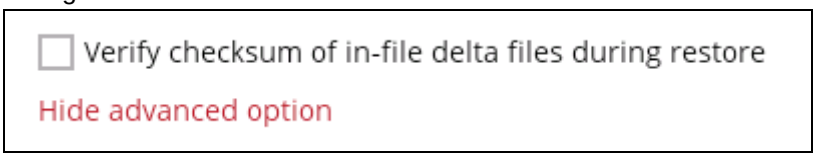
- **Auto power on after Run Direct is running**

  Enable this option to power up the virtual machine automatically, after Run Direct is running for the VM.

- **Use existing storage as VM working directory to improve performance**

  Enable this option to enhance performance of the restored VM.

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



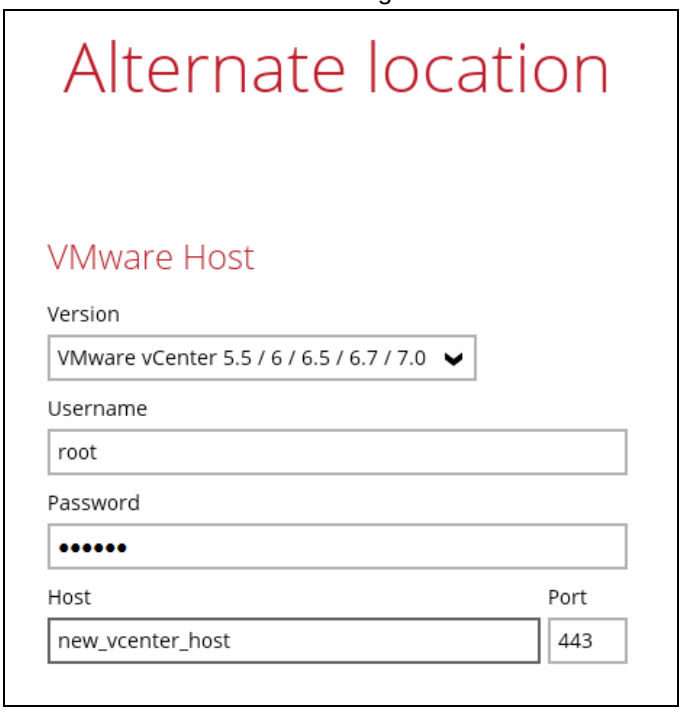
NOTE

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

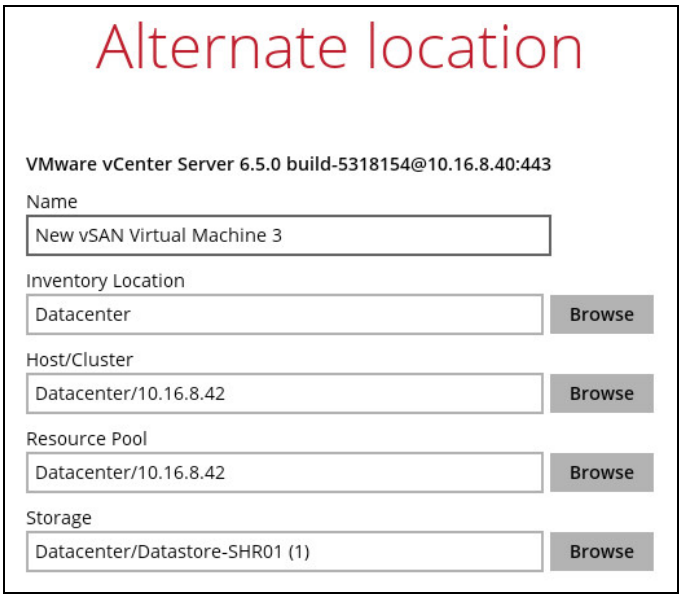
Click **Next** to proceed when you are done with the settings.

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

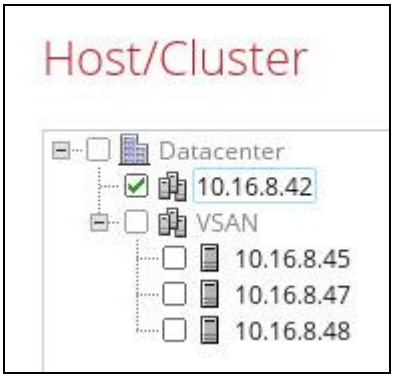
Enter the VMware host and access information of where you would like the VM to be restored to, enter the **Username** and **Password** of the administrator account, **Host**, and **Port** information of the new / original vCenter server.



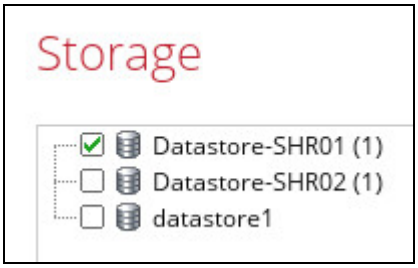
Enter a new **Name** for the VM, then **Browse** to modify the **Host/Cluster** and **Storage** settings, according to where you would like the VM to be restored to.



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

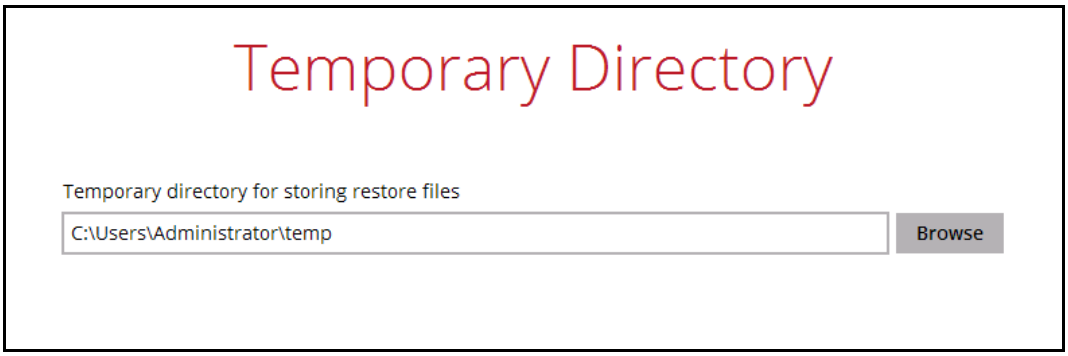


Select the storage.



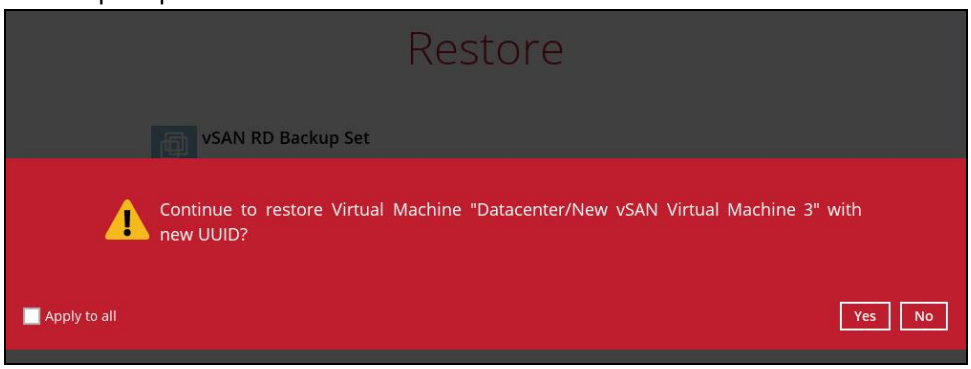
Press **Next** to proceed when you are done with the settings.

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

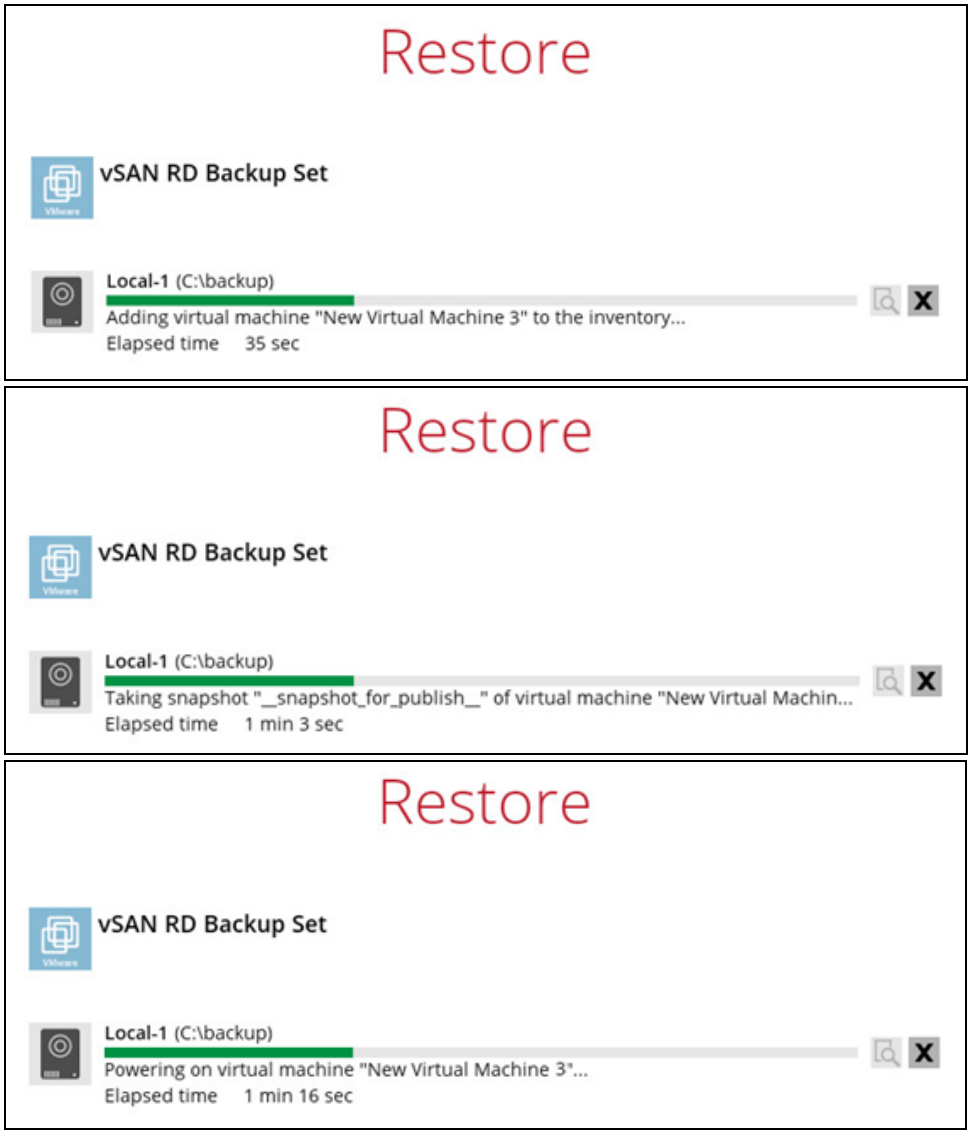


11. When restoring your guest VM, different messages will be prompted depending on the selected location.

- 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.

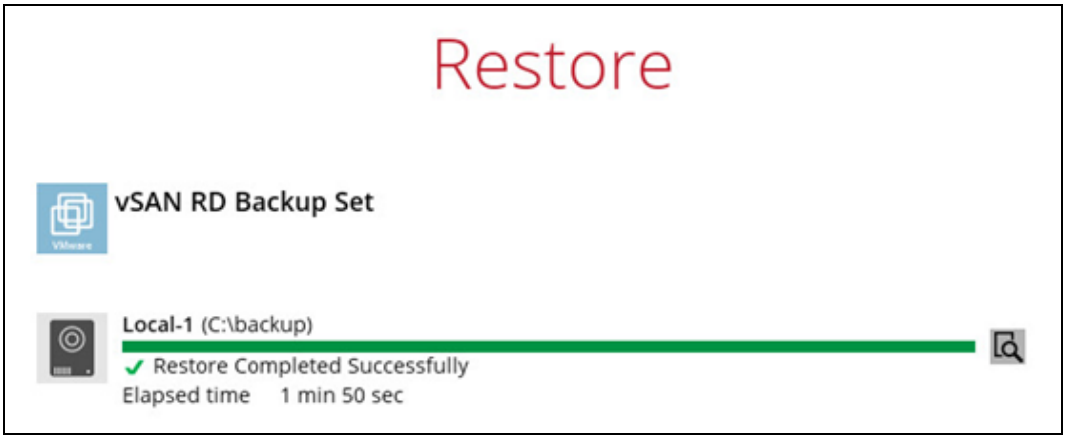


- Another way of checking the progress of the restore is from vSphere. The restore has started when a NAS datastore was created. And it is completed when the virtual machine was powered on.

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.

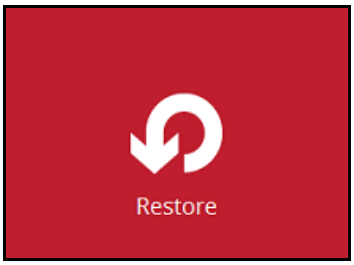


NOTE

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

15.6 Restore a backup from VMFS datastore to vSAN datastore with Run Direct

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



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

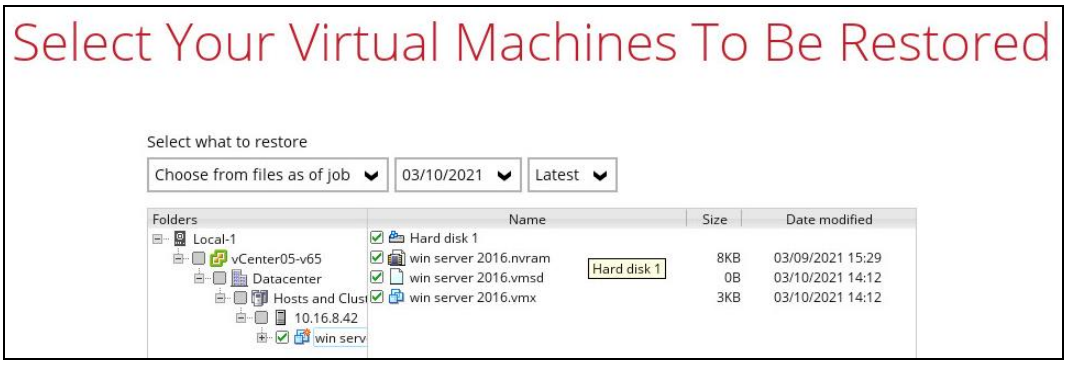
3. Select the backup destination that contains the VM that you would like to restore.

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

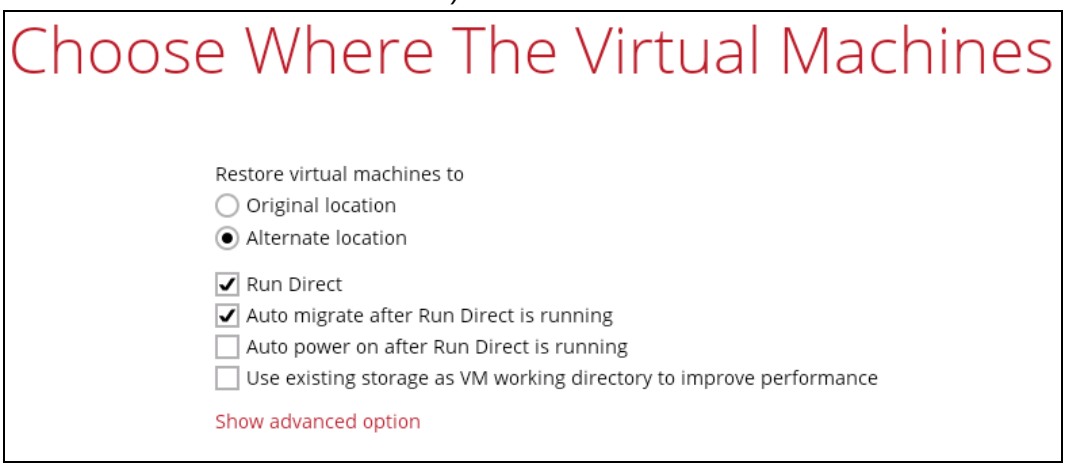
5. Select the virtual machine that you would like to restore.

IMPORTANT

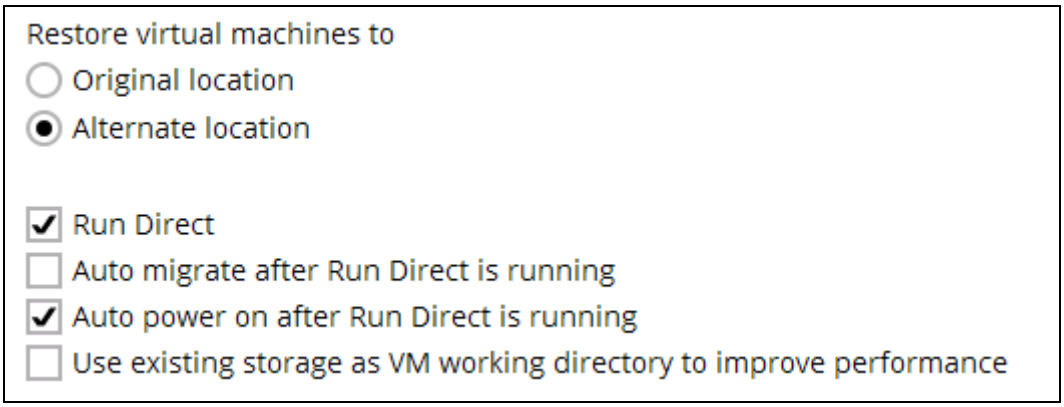
When performing a Run Direct restore to **Alternate Location**, only one VM can be selected per restore session.



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



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



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

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

NOTE

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

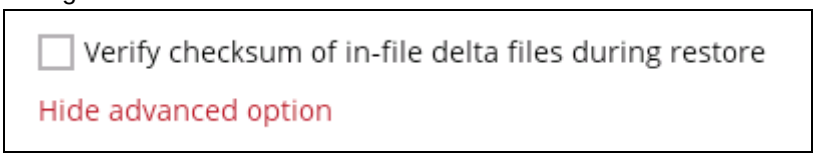
- **Auto power on after Run Direct is running**

  Enable this option to power up the virtual machine automatically, after Run Direct is running for the VM.

- **Use existing storage as VM working directory to improve performance**

  Enable this option to enhance performance of the restored VM.

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



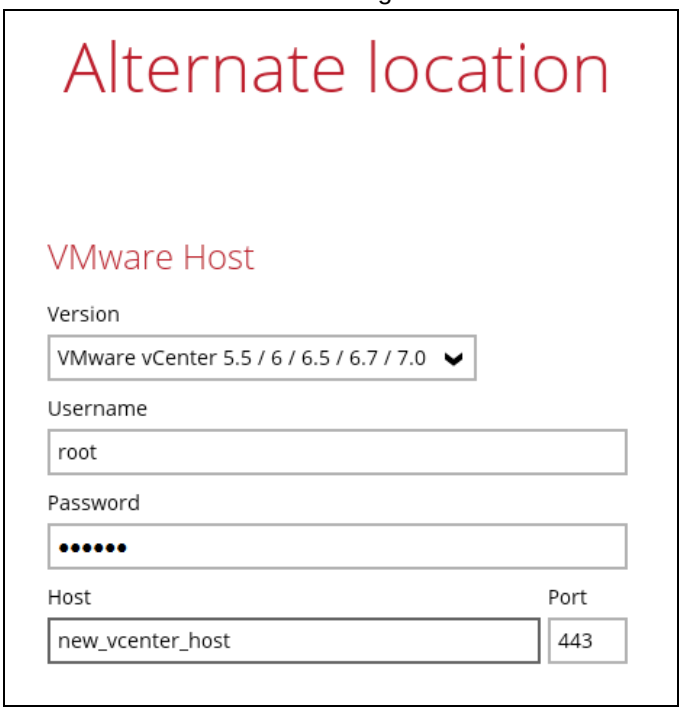
NOTE

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

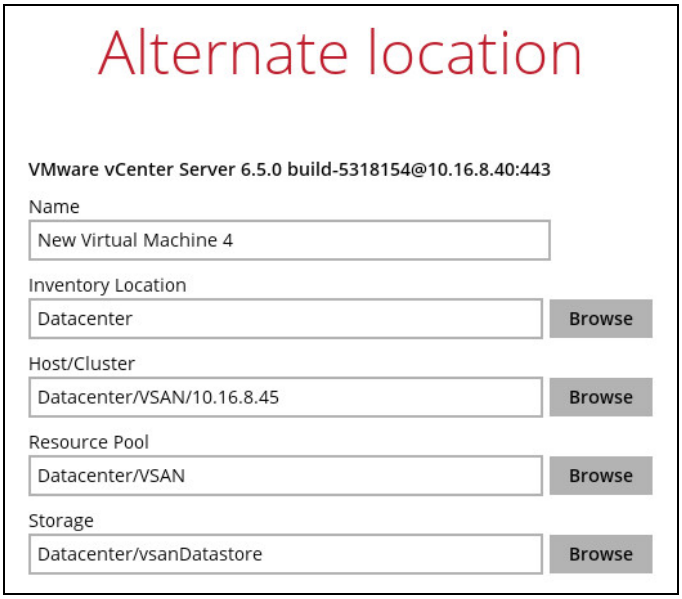
Click **Next** to proceed when you are done with the settings.

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.



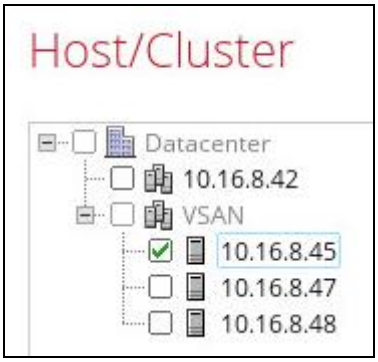
Enter a new **Name** for the VM, then **Browse** to modify the **Host/Cluster** and **Storage** settings to select the vSAN datastore, according to where you would like the VM to be restored to.



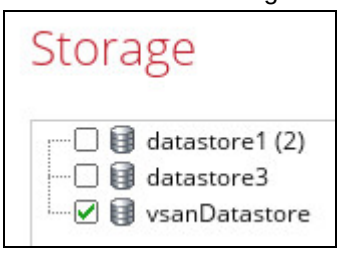
NOTE

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

As you can see, you need to expand the VSAN to be able to select the host.

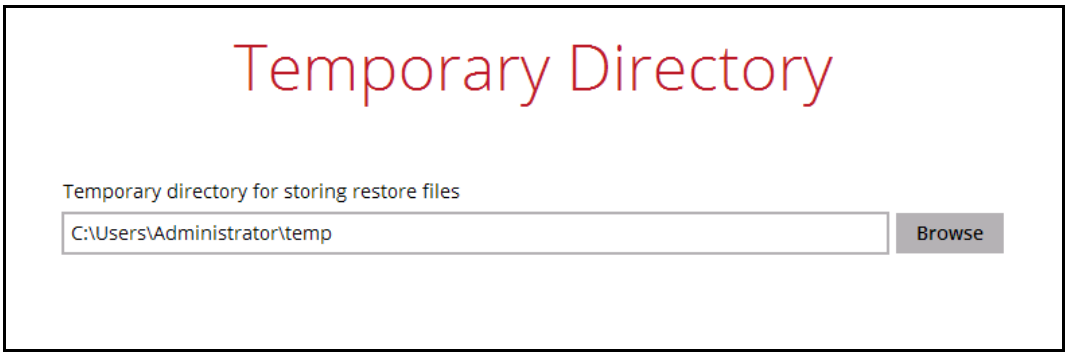


Select the vSAN storage.



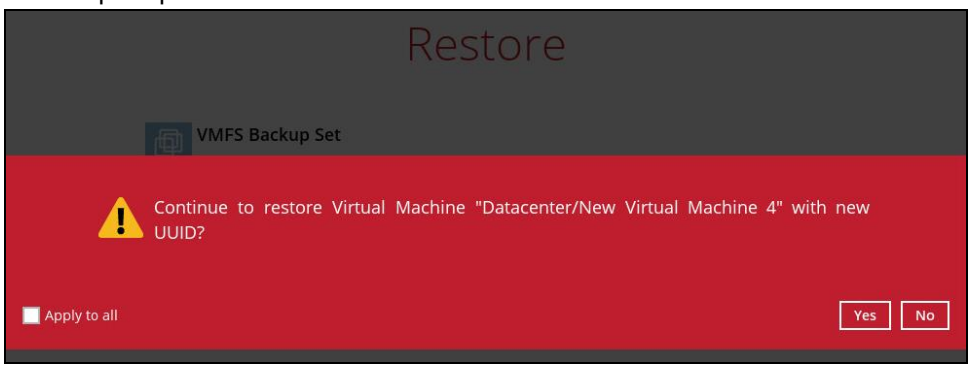
Press **Next** to proceed when you are done with the settings.

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

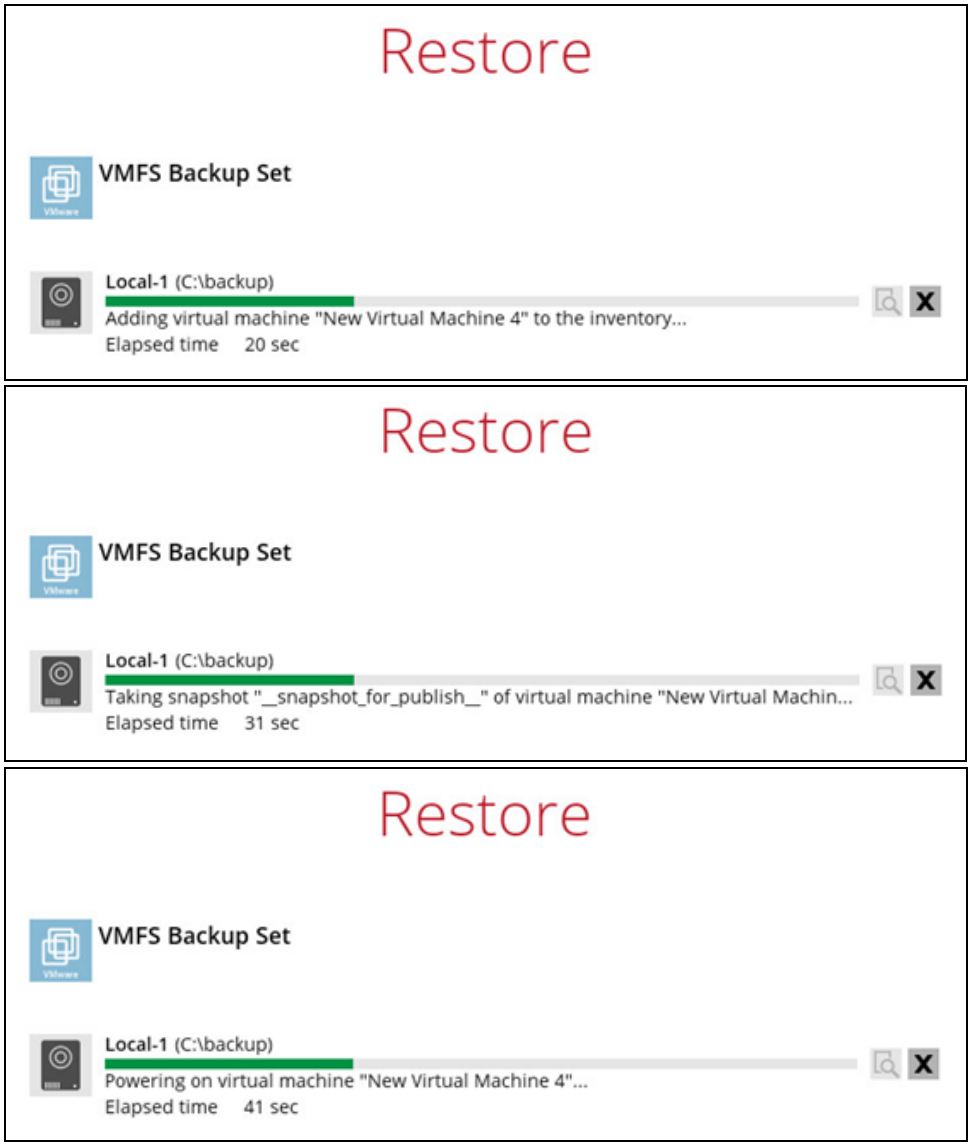


11. When restoring your guest VM, different messages will be prompted depending on the selected location.

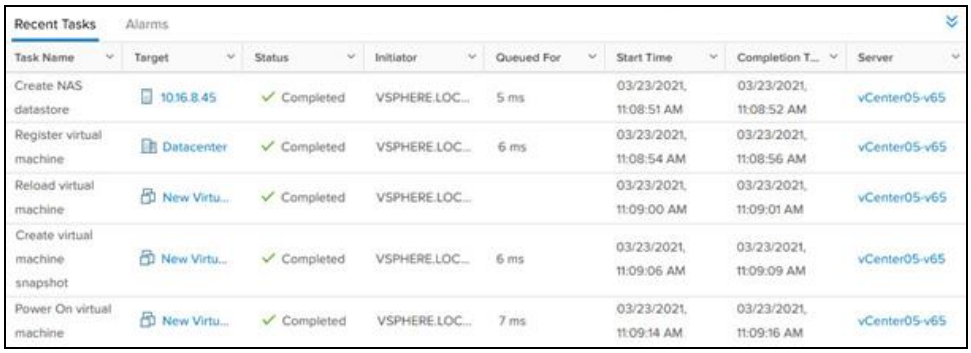
- Restoring guest VM to another VMware host, since each virtual machine is automatically assigned a universally unique identifier (UUID), a new UUID must be created when you restore the guest VM to another host. It is not possible to have two identical UUID running at the same time, so make sure to click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



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



- 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.



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

NOTE

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

16 Contact Ahsay

16.1 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/

16.2 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/

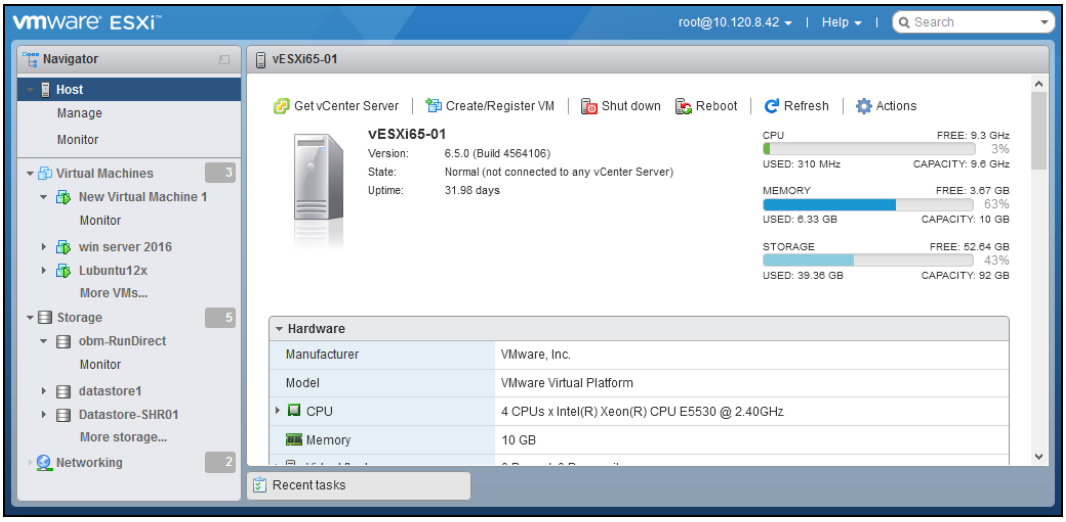
Please specify the specific document title as well as the change required/suggestion when contacting us.

Appendix

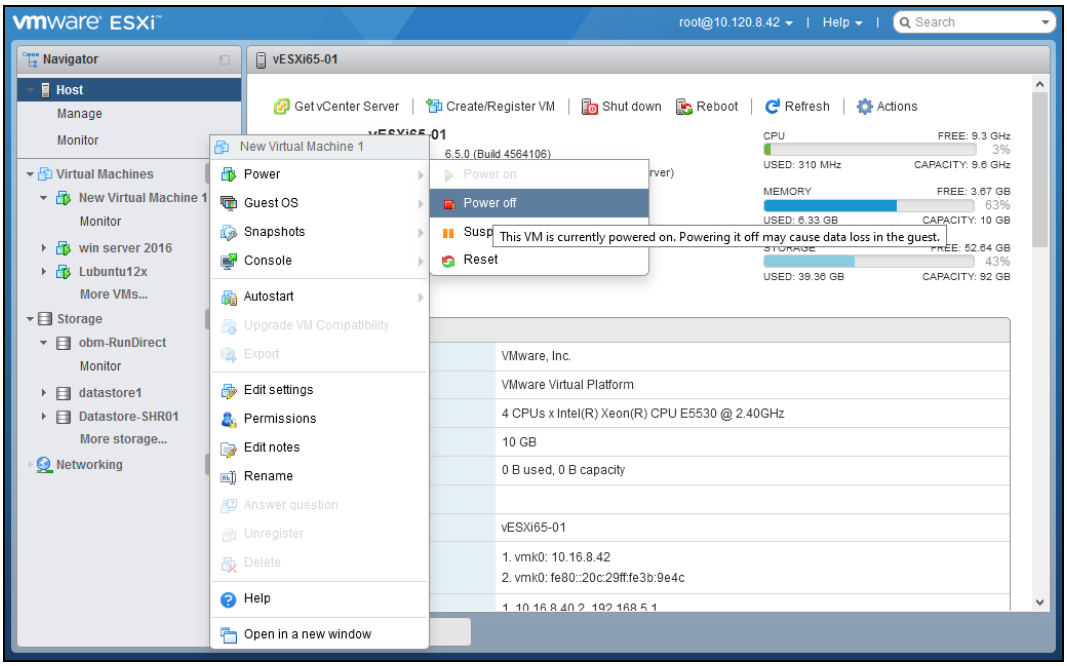
How to clean up the temporary files on VMware Host when Run Direct terminates unexpectedly

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:

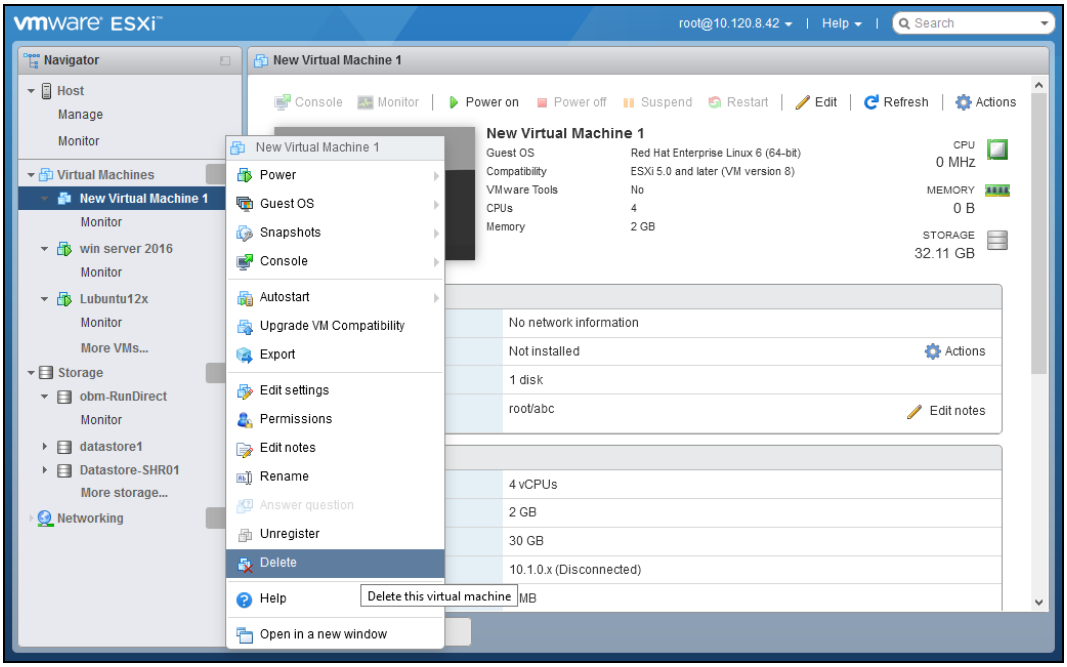
1. Open the vSphere Client or Web Client where the RunDirect VM is located.



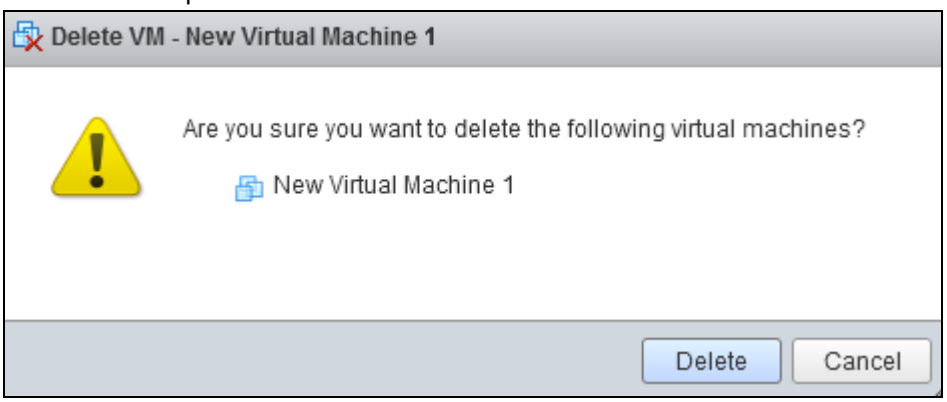
2. Right click the affected RunDirect VM, for example “New Virtual Machine 1” and select **Power off**.



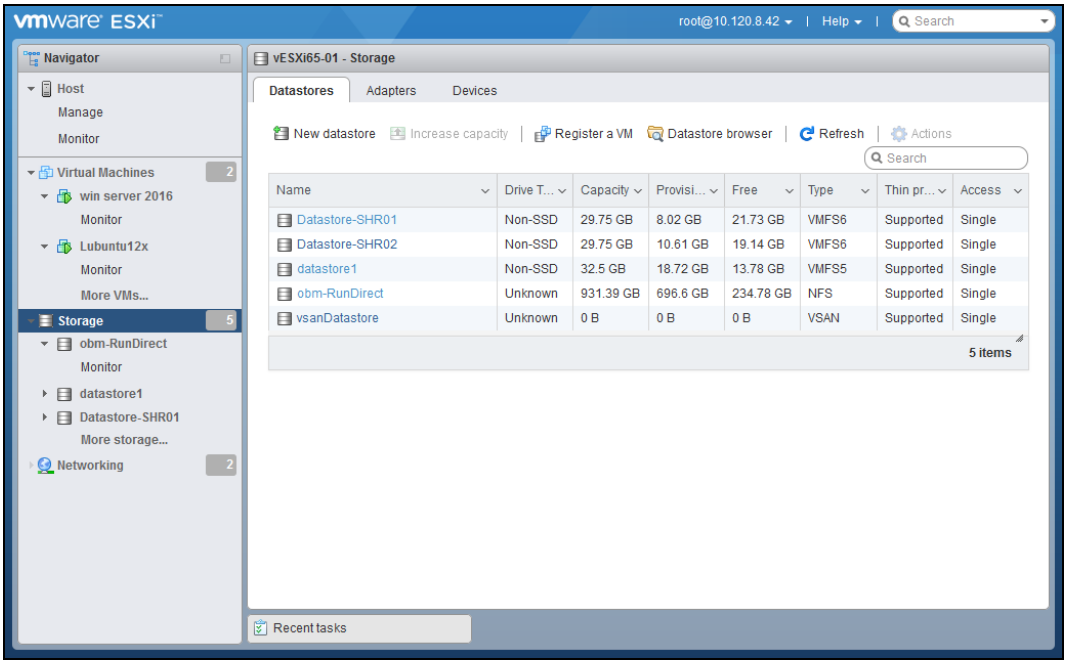
3. Right click the failed RunDirect VM, for example “New Virtual Machine 1” and select **Remove from Inventory** to remove the RunDirect VM or **Delete** to remove the RunDirect VM and temporary files remaining on the client machine if changes made on the RunDirect VM is not needed anymore.



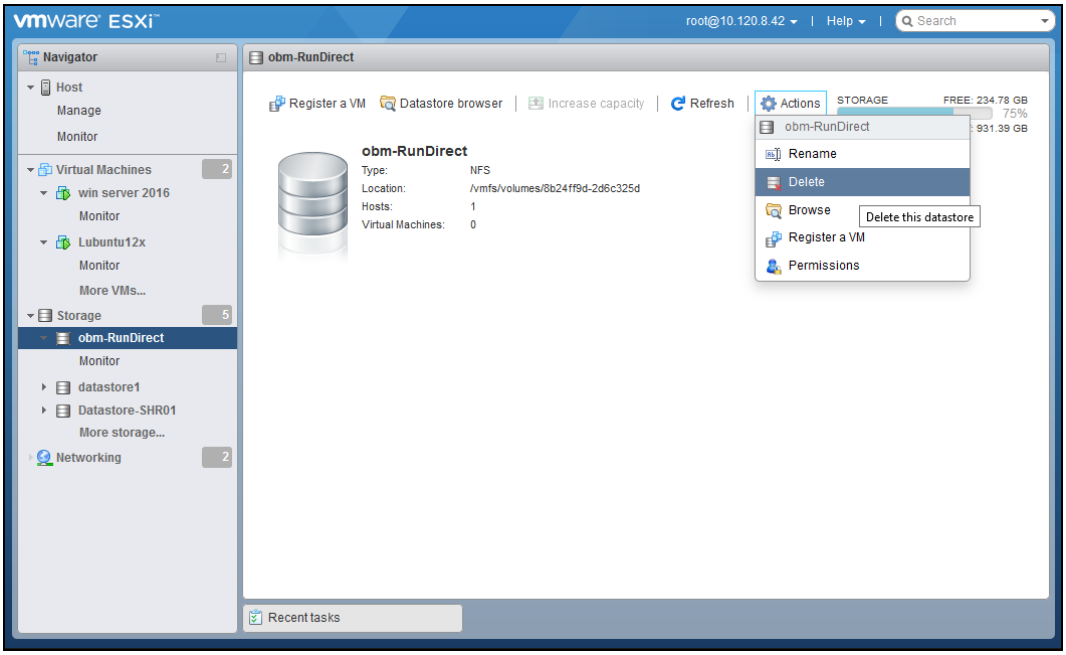
Click **Delete** to proceed.



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 and click **Actions** then **Delete** to remove the NFS datastore.



Click **Confirm** to delete the datastore.