Ahsay Backup

Ahsay Online Backup Manager v7

VMware vCenter/ESXi Guest Virtual Machine Backup & Restore Guide

Ahsay Systems Corporation Limited

2 November 2017

www.ahsay.com

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

Copyright Notice

Trademarks

Disclaimer

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

Revision History

Date	Descriptions	Type of modification
15 July, 2016	First Draft	New
23 Aug, 2016	Modified Ch. 2.5	Modification
27 Sept, 2016	Modified Ch 6.1 with AhsayCBS added as backup destination; Ch 1 Overview section modified	Modification
3 Dec, 2016	Modified Ch 3.5 with new information on AhsayOBM NFS service	Modification
3 Feb 2017	Added instructions and screen shots for Encryption key handling in Ch. 6.1	New
5 Apr 2017	Updated Requirements in Ch.3; Updated info about supporting VMware v6.5: Added Ch.12 about restore in VMDK format; Added Encryption Type option in Ch. 6.1 Create a VMware VM Backup Set	New / Modified
31 May 2017	Added Ch.5 Granular restore section, added step in Create new backup set, added Granular restore sub-section in the Restore section, added step & screen shot of UUID request	New
23 Jun 2017	Updated Ch.4, Ch.5, Ch.7, Ch 14, Updated all granular screen shots	Modified
13 Jul 2017	Updated Ch.5, Ch.10, Ch.14, Updated all granular screen shots	Modified
26 Jul 2017	Updated Ch2.4 Granular Restore section; Updated Ch3.2 Software Requirement; Updated Ch3.4.6 Disk Space Available on Backup Client Computer (or the vCenter computer) ; Updated Ch14 Granular Restore steps order	New / Modified
18 August 2017	Modified Ch2.4 Features Comparison between VDDK and Non-VDDK Modes; Add License Specification to Ch3.3; Add Cloud Destination for comparison between Run Direct and Non-Run Direct in Ch3.5	New / Modified

11 October 2017	Modified Ch.5.1; Added note of restore using Windows File Explorer for Ch.14;	New/ Modified

Table of Contents

1 Overview

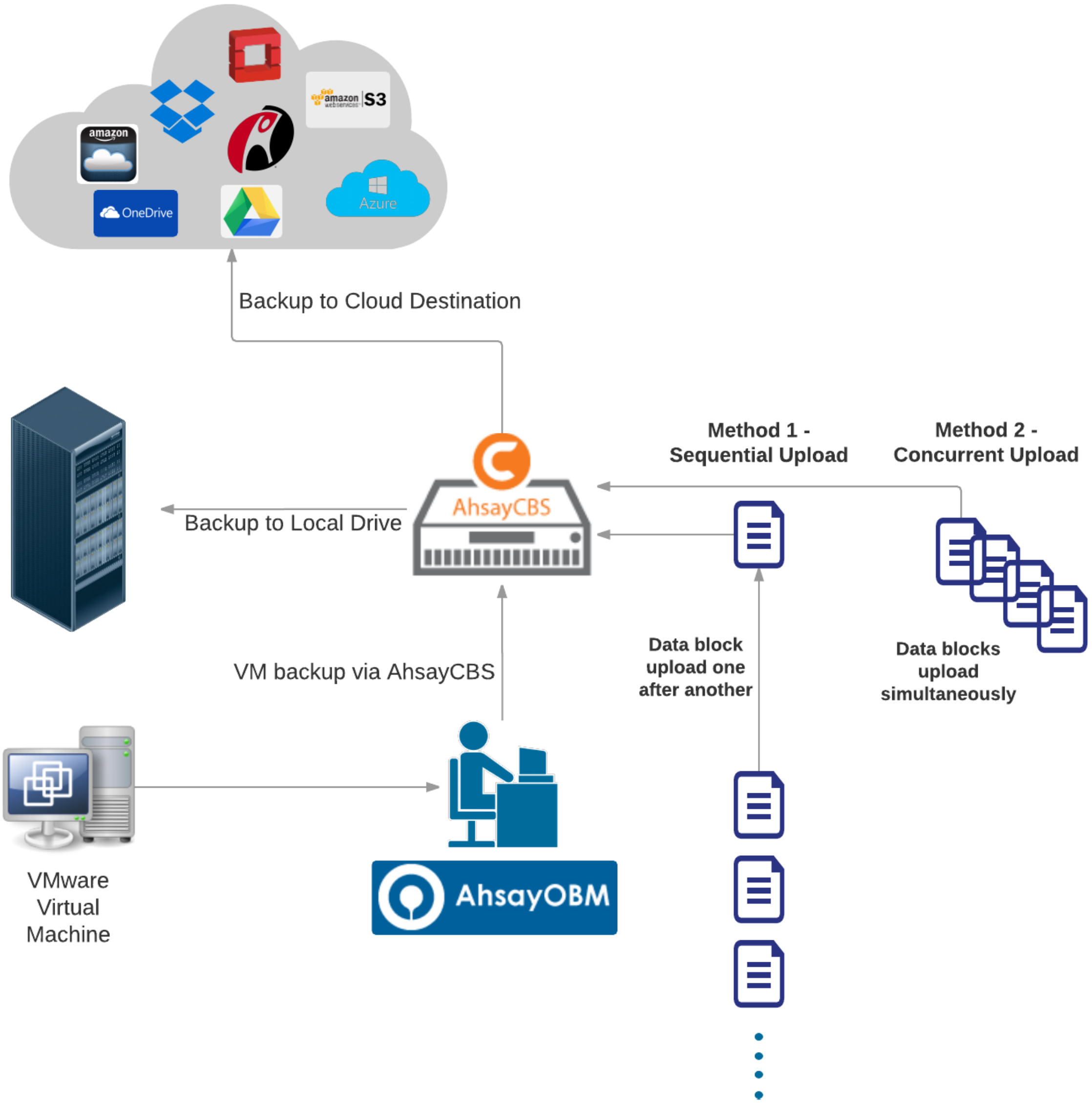
What is this software?

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

System Architecture

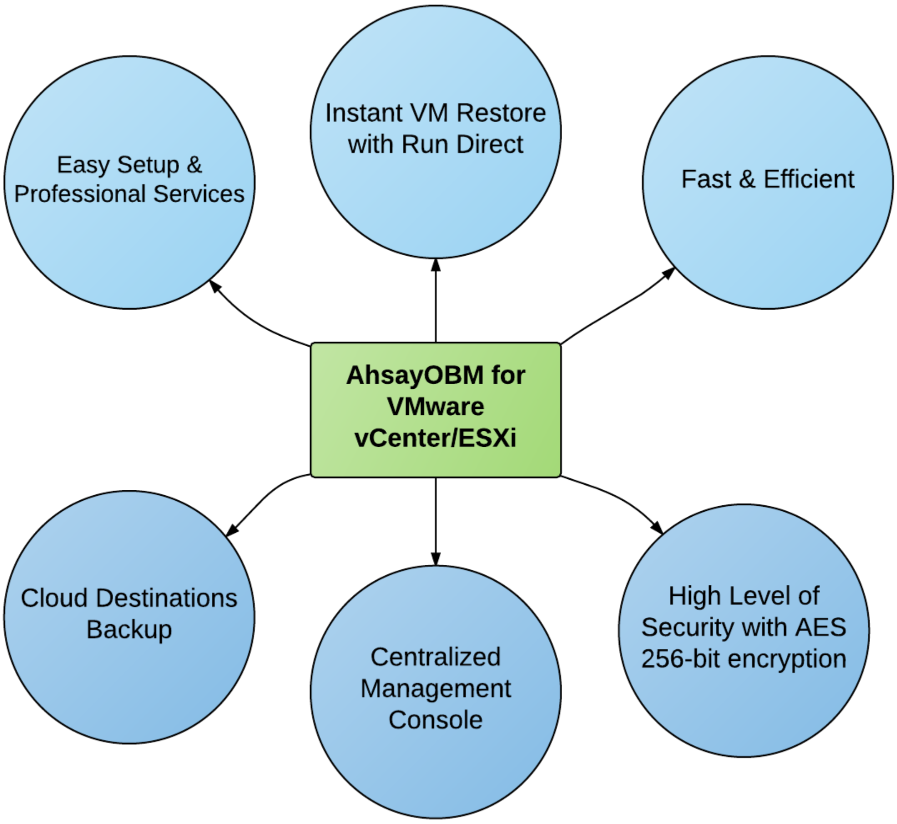
Below is the system architecture diagram illustrating the major elements involved in the backup process among the VMware server, AhsayOBM and AhsayCBS.

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



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

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



AhsayOBM for VMware vCenter/ESXi
Easy Setup & Professional Services
Instant VM Restore with Run Direct
Fast & Efficient
Cloud Destinations Backup
Centralized Management Console
High Level of Security with AES 256-bit encryption

Easy Setup & Professional Services

***Setup is a few clicks away* -** our enhanced AhsayOBM v7 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?

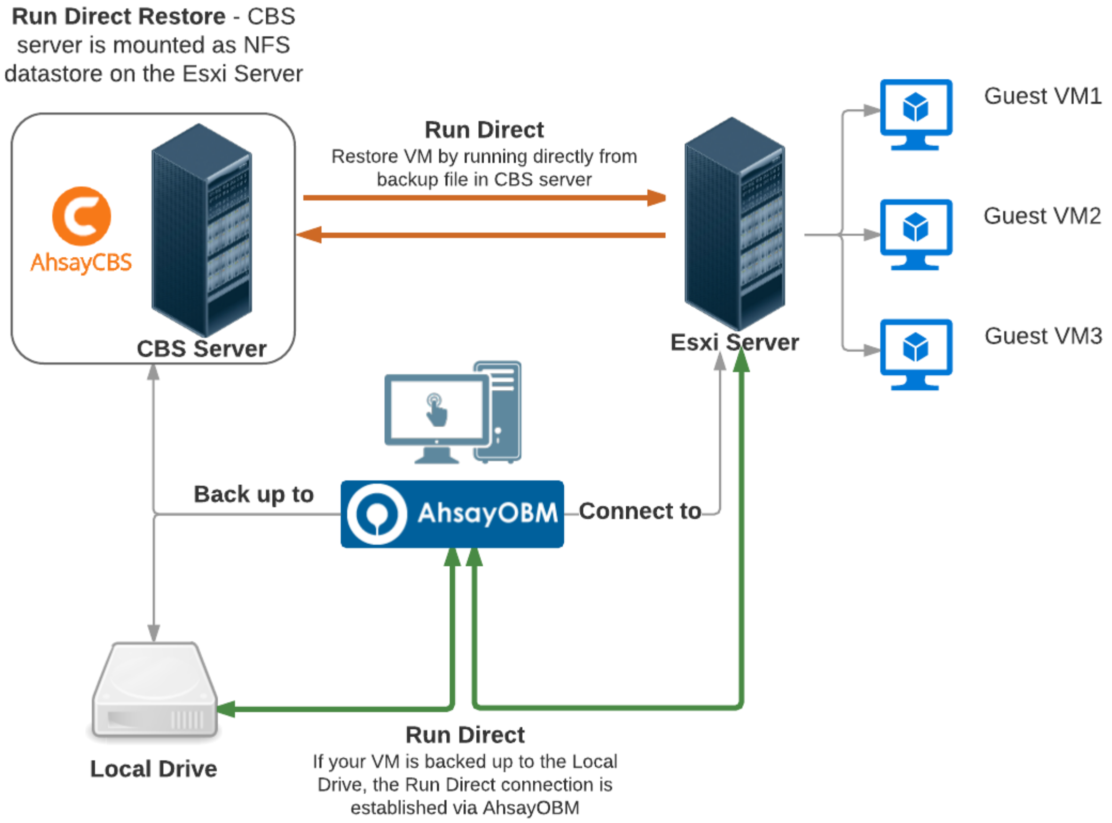
Run Direct is a feature introduced since AhsayOBM version 7.5.0.0, that helps reduce disruption and downtime of your production VMs.

Unlike normal VM restore procedure where a VM is extracted from backup files and copy 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 a NFS datastore from the VMware host, where the VM is run directly from the backup files.

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



Run Direct Restore - CBS server is mounted as NFS datastore on the Esxi Server
Run Direct
Restore VM by running directly from backup file in CBS server
AhsayCBS
CBS Server
Esxi Server
Guest VM1
Guest VM2
Guest VM3
Back up to
AhsayOBM
Connect to
Local Drive
Run Direct
If your VM is backed up to the Local Drive, the Run Direct connection is established via AhsayOBM

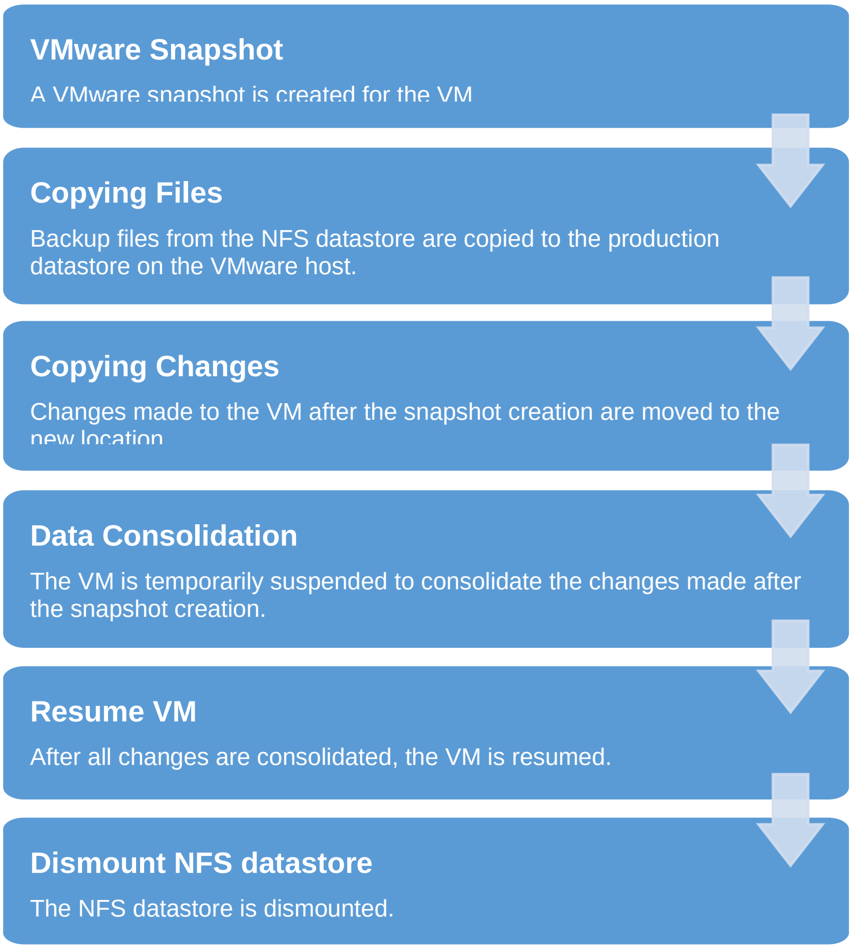
The restored virtual machine, at this stage (e.g. before the restore is finalized) is in a read-only state to preserve its integrity. All changes made to the virtual disks (e.g. operation within the guest virtual machine) are stored separately in transaction logs stored on the NFS datastore or the original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

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

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

Finalizing a VM Recovery (Migrating VM to permanent location)

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



VMware Snapshot

A VMware snapshot is created for the VM

Copying Files

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

Copying Changes

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

Data Consolidation

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

Resume VM

After all changes are consolidated, the VM is resumed.

Dismount NFS datastore

The NFS datastore is dismounted.

Note

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

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

Fast and Efficient

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

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

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

Centralized Management Console

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

- ***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 via the URL below.
- ***Backup User*** – configure backup settings, monitor backup and restore activities, and initiate a Run Direct activity.

Cloud Destinations Backup

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

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

* Available on computers with China or Hong Kong local settings

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

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

High Level of Security

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

- ***Un-hackable Encryption Key*** – to provide the best protection to your backup data, you can turn on the encryption feature which will be 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. You backup service provider can make it mandatory for you to upload the encryption key to the centralized management console, the encryption key will be uploaded in hashed format and will only be used when you request for a recovery.

What is the purpose of this document?

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

The document can be divided into 3 main parts.

Part 1: Preparing for VMware VM Backup & Restore

Understanding Backup Mode
Introduce the differences between Non-VDDK and VDDK backup modes

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

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

Part 2: Performing VMware VM Backup

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

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

Part 3: Performing VMware VM Restore

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

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

What should I expect from this document?

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

Who should read this document?

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

2 Understanding Backup Mode

Backup Mode

There are two backup modes available for VM backup:

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

Note

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

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

Non-VDDK Backup Mode

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

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

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

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

VDDK Backup Mode

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

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

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

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

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

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

Features Comparison between VDDK and Non-VDDK Modes

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

3 Requirements

Hardware Requirement

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

Software Requirement

Refer to the following article for the list of compatible operating systems and VMware platforms: FAQ: Ahsay Software Compatibility List (SCL) for version 7.3 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 (5250)

VMware vCenter / ESXi Server Requirements

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

ESXi / vCenter Patch Release

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

License Specification

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

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.

Root Account

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

Port Requirement

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

Note

Ports 443 and 902 are default ports for VMware.

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

Disk Space Available on Datastore

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

Maximum Virtual Disk Size

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

VMware Tools

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

Note

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

There are different types of quiescing mechanisms, according to the guest operating systems (e.g. Crash-consistent, File-system-consistent and Application-consist quiescing).

For more details, refer to the following VMware vSphere document: http://pubs.vmware.com/vsphere-60/index.jsp#com.vmware.vddk.pg.doc/vddkBkupVadp.9.6.html

ESXi/ESX Hosts and Virtual Machine Hardware Versions Compatibility

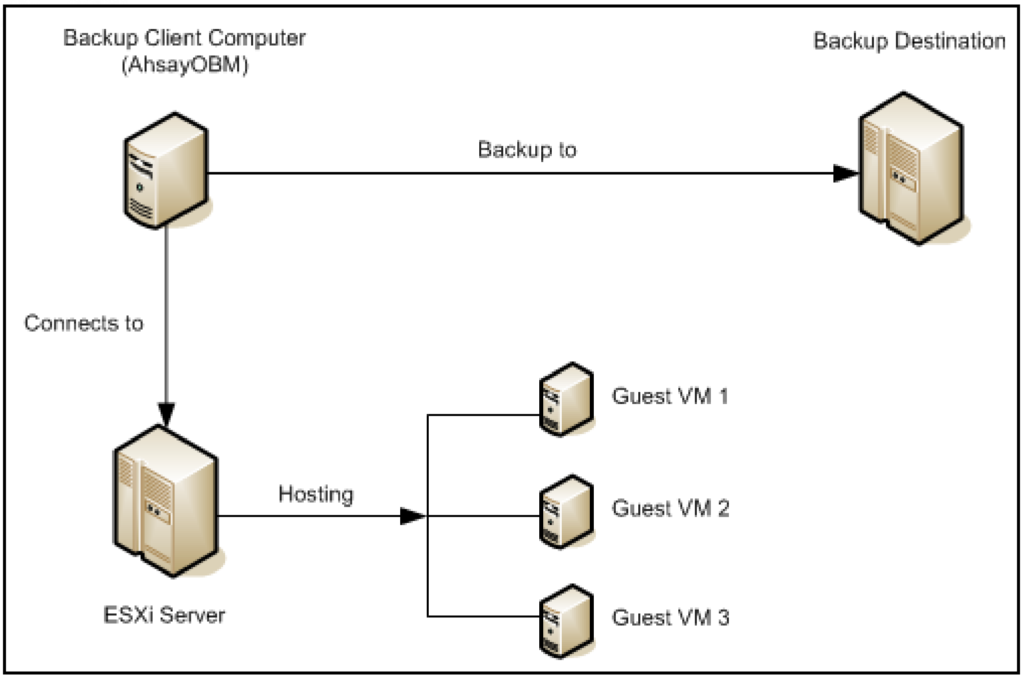
Refer to the link below for information on the supported and compatible virtual machine hardware versions in VMware vSphere.
ESXi/ESX hosts and compatible virtual machine hardware versions list (2007240)

Backup Client Computer Requirements

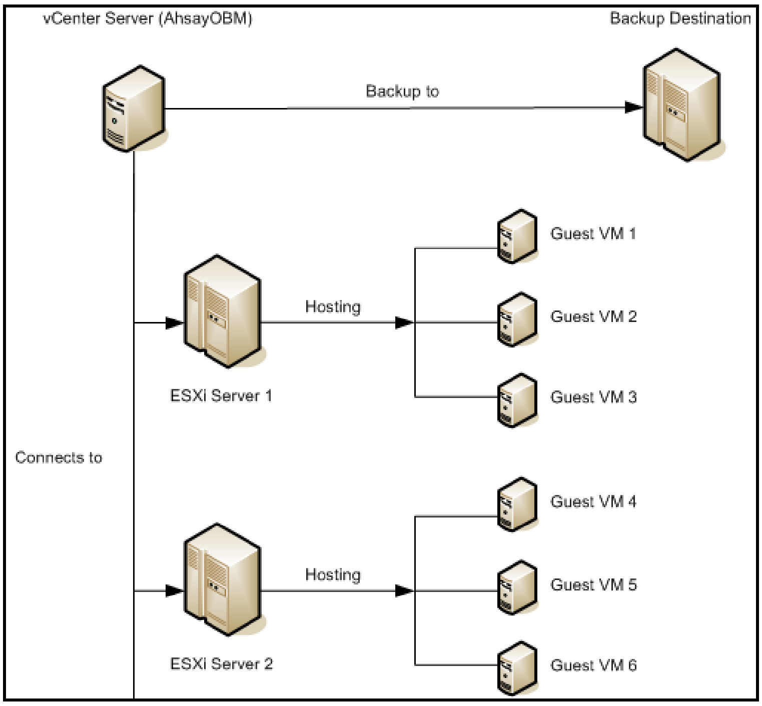
For backup of virtual machines on ESXi server (with no vCenter setup), a separate Backup Client Computer must be prepared for AhsayOBM to install on.

Important

AhsayOBM cannot be installed on an ESXi server directly.



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



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

Hardware and Software Requirement

Ensure that the hardware and software requirements are met by the Backup Client Computer or the vCenter computer.

Add-on Module Requirement

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

Backup Quota Requirement

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

Port Requirement

- For environment with firewall, the vCenter, ESXi hosts and Backup Client Computer must be able to communicate with each other.
- Make sure that ports 22, 80, 111, 443 and 902 allow outbound communication on the Backup Client Computer. Refer to the link below for details on port usage. https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1012382

Note

Ports 443 and 902 are default ports for VMware.

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

Backup Client Computer on Linux

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

Important

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

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

Sufficient disk space must be allocated on the Backup Client Computer (or the vCenter computer) for the temporary directory configured for the backup set, and the formula of calculation of disk space is like 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 take into account guest VM growth over time. It is recommended for fast growing guest VM the maximum free space required should be reviewed on regular basis to avoid potential backup problems.

Refer to the link below for details of the maximum free space required for temporary directory.
FAQ: Tips On How To Setup The Temporary Directory For Your Backup Set (#5247)

Windows OS Requirement for VDDK and Non-VDDK Modes Backup

Make sure AhsayOBM is installed on:

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

Run Direct Requirements

Run Direct is a feature introduced since AhsayOBM version 7.5.0.0, that helps reduce disruption and downtime of your production VMs.

For more details on Run Direct, refer to the chapter on Instant VM Restore with Run Direct.

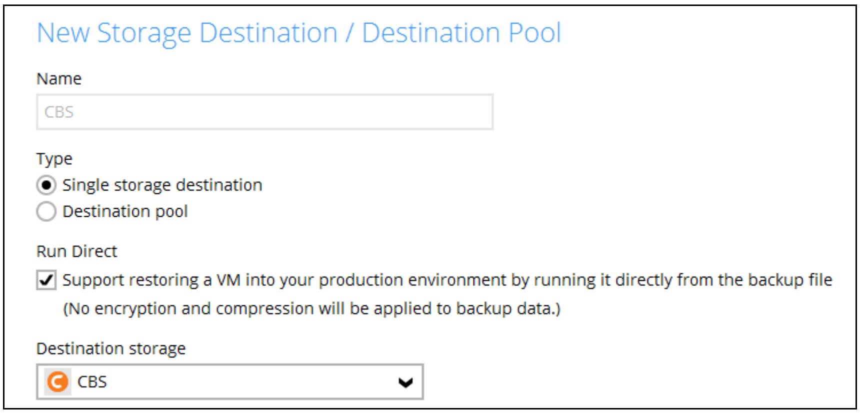
To utilize the Run Direct feature, ensure that the following requirements are met:

VDDK Backup Mode

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

Backup Destination Requirement

- When a Run Direct restore is performed, the backup destination containing the guest VM files is mounted on the VMware host as NFS datastore.
- Ensure that the following requirements are met by the backup destination of the VMware VM backup set:
  - **Destination Type** of the backup destination must be set to a **Single storage destination**.



New Storage Destination / Destination Pool

Name

CBS

Type

● Single storage destination

○ Destination pool

Run Direct

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

Destination storage

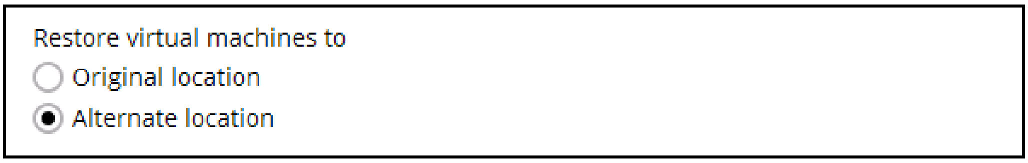
CBS

  - 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 form the backup files in the backup destination.
- **Operation System of the Backup Client Computer**

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

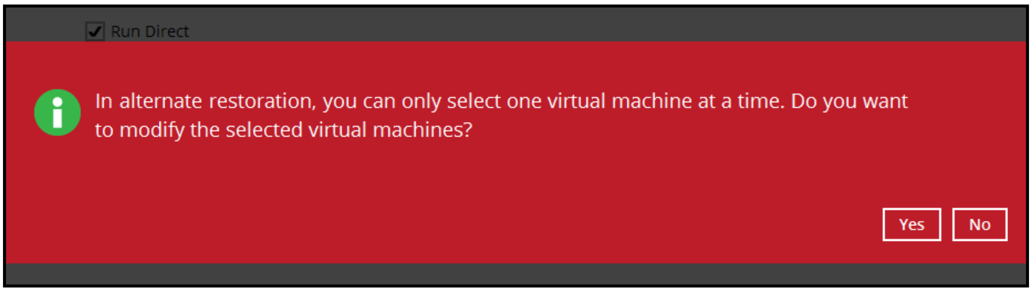
- **Restore to Alternate Location**
  - When performing a Run Direct restore to **Alternate Location**, only one VM can be selected per restore session.



Restore virtual machines to

○ Original location

● Alternate location



☑ Run Direct

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

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

- Dedicated NFS Service

Starting from AhsayOBM version 7.9.0.0, a dedicated AhsayOBM NFS Windows service is introduced to allow Run Direct session to continue even if the AhsayOBM user interface is closed.

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

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

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

VDDK Backup Mode Requirements

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

License Requirement

- The VMware vSphere Storage APIs, which are essential for VDDK backup mode, are included with the VMware vSphere Enterprise Standard, Enterprise and Enterprise Plus Edition: http://www.vmware.com/products/vsphere/features-storage-api

- Ensure that the license requirement is met.

Notes

- For VM on free version of ESXi without a Run Direct backup destination, backup will be performed in non-VDDK mode.
- For VM on free version of ESXi with a Run Direct backup destination, the following error message would be returned during a backup:
"Skip backing up Virtual Machine "name". Reason = "Run Direct is only support to VDDK backup mode"".

Changed Block Tracking (CBT) on VMs

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

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

Note

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

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

VMware Snapshot

VDDK backup mode does not support backup of virtual machine snapshot.

Virtual Machine State

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

Non-VDDK Backup Mode Requirements

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

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

4 Best Practices and Recommendations

Please consider the following recommendations:

- Use the latest version of AhsayOBM.

  The latest version of AhsayOBM should be installed on the staging machine or Backup Client Computer for VMware ESX/ESXi, or on the vCenter server.

  Always stay up-to-date when newer version of AhsayOBM is released. To get our latest product and company news through email, please subscribe to our mailing list: http://www.ahsay.com/jsp/en/home/subscribe_mail_list.jsp

- Install AhsayOBM on a physical staging machine

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

- VMware Tools

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

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

- Don’t 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 mode / CBT feature.

  The VDDK or CBT (Change Block Tracking) feature is supported on VMware ESXi/vCenter hosts with VMware Essentials License or above. The job of the CBT feature is keeping track of any data blocks which have changed since the last backup job. As the AhsayOBM via the vStorage API can quickly obtain this information it does not need to calculate it which requires time and resources, therefore the performance of incremental backups is much faster with CBT feature enabled.

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

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

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

  Refer to the following article for details on setting up the temporary directory FAQ: Tips On How To Setup The Temporary Directory For Your Backup Set

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

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

- Backup the guest VMs to more than one destination

  To provide maximum data protection and recovery flexibility you should consider 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 can be restored from another location.

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

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

  Refer to the following KB article for further instruction:
  http://wiki.ahsay.com/doku.php?id=public:5003_faq:how_do_i_modify_the_java_heap_size_setting_of_ahsayobm_or_ahsayacb&s[]=5003

5 Granular Restore Technology

What is Granular Restore Technology?

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

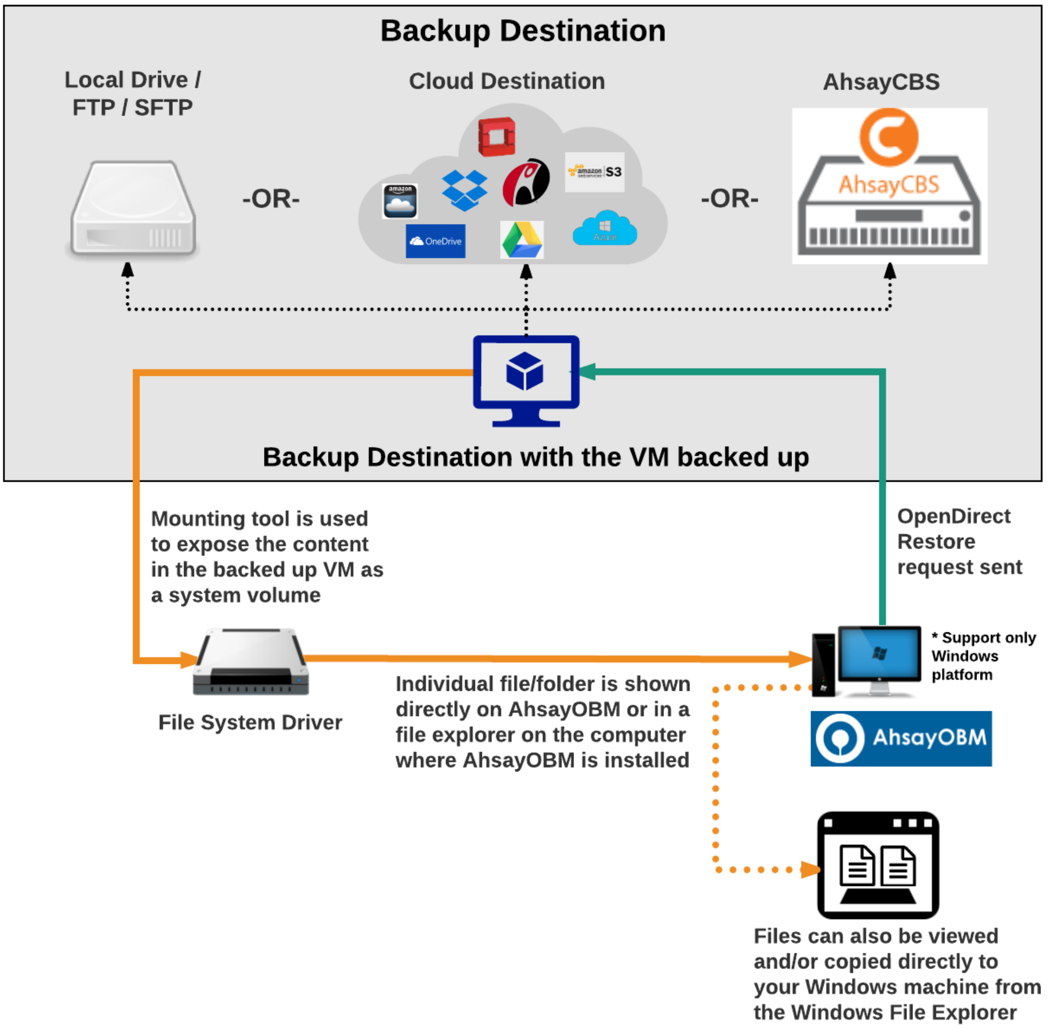
Granular restore is one of the available restore options for VMware ESXi/vCenter backup sets from AhsayOBM v7.13.0.0 or above. AhsayOBM makes use of granular restore technology to enable a file level restore from a virtual disk file (VDDK) of guest VM backup possible. It is particularly useful if you only need to restore individual file(s) from a guest VM which would normally a long time to restore and then startup before you can gain access the files on the virtual disks. Granular restore gives you a fast and convenient way to recover individual files on a guest VM.

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

IMPORTANT

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

How does Granular Restore work?


Backup Destination
Local Drive / FTP / SFTP
Cloud Destination
AhsayCBS
-OR-
-OR-
AhsayCBS
OneDrive
S3
Backup Destination with the VM backed up
Mounting tool is used to expose the content in the backed up VM as a system volume
OpenDirect Restore request sent
* Support only Windows platform
File System Driver
Individual file/folder is shown directly on AhsayOBM or in a file explorer on the computer where AhsayOBM is installed
AhsayOBM
Files can also be viewed and/or copied directly to your Windows machine from the Windows File Explorer

Benefits of using Granular Restore

Comparison between Granular Restore and Traditional Restore.

Granular Restore	
Introduction	
Granular restore allows you to quickly mount virtual disk(s) directly from the backup file of a guest VM, so that individual files from virtual disk(s) can be exposed via the file explorer on AhsayOBM, or to be copied from the file explorer on to a 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 required an additional AhsayOBM installation on the guest VM environment, with Granular Restore feature, only one backup set is required. ➢ **Fewer CAL (Client Access License) required -** you will only need one AhsayOBM CAL to perform guest VM, Run Direct, and Granular restore. ➢ **Less storage space required -** as you only need to provision storage for one backup set. ➢ **Less backup time required** - As only one backup job needs to run. ➢ **Less time spent on administration** - As there are fewer backup sets to maintain.
Cons	
No Encryption and Compression	To ensure optimal restore performance, the backup of the guest VM will **NOT** be encrypted and compressed, therefore, you may have to take this factor in consideration when using this restore method.

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

Requirements

Supported Backup Modules

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

License Requirements

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

Backup Quota Storage

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

Operating System

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

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

Temporary Directory Requirement

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

Available Spare Drive Letter

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

Note

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

Network Requirements

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

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

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

Other Dependencies

The following dependencies are restore related and therefore they will be checked by AhsayOBM only when granular restore is performed. Absence of these elements will not affect the backup job but would cause the restore to fail.

- Microsoft Visual C++ 2015 Redistributable (x86) / (x64)
  https://www.microsoft.com/en-us/download/details.aspx?id=48145

- Update for Universal C Runtime in Windows
  https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows

- **For Windows 7 and Windows Server 2008 R2 only**

  Microsoft Security Advisory 3033929
  https://technet.microsoft.com/en-us/library/security/3033929.aspx

Permissions

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

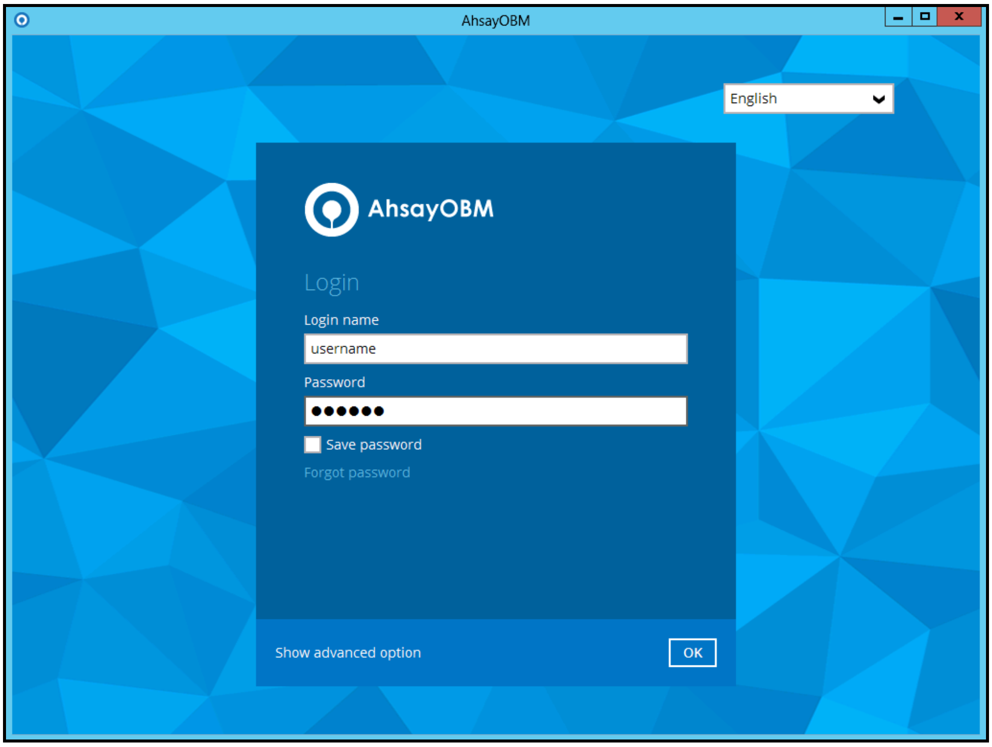
- For Granular Restore, Windows User Account Control (UAC) must be disabled.

6 Starting AhsayOBM

Login to AhsayOBM

1. Login to the AhsayOBM application user interface.

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



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

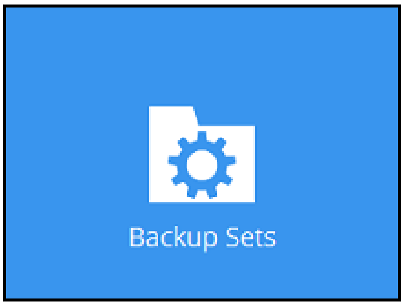
```
# sh /usr/local/obm/bin/RunOBC.sh &
```

2. Enter the **Login name** and **Password** of your AhsayOBM account.

3. Click **OK** afterward to login to AhsayOBM.

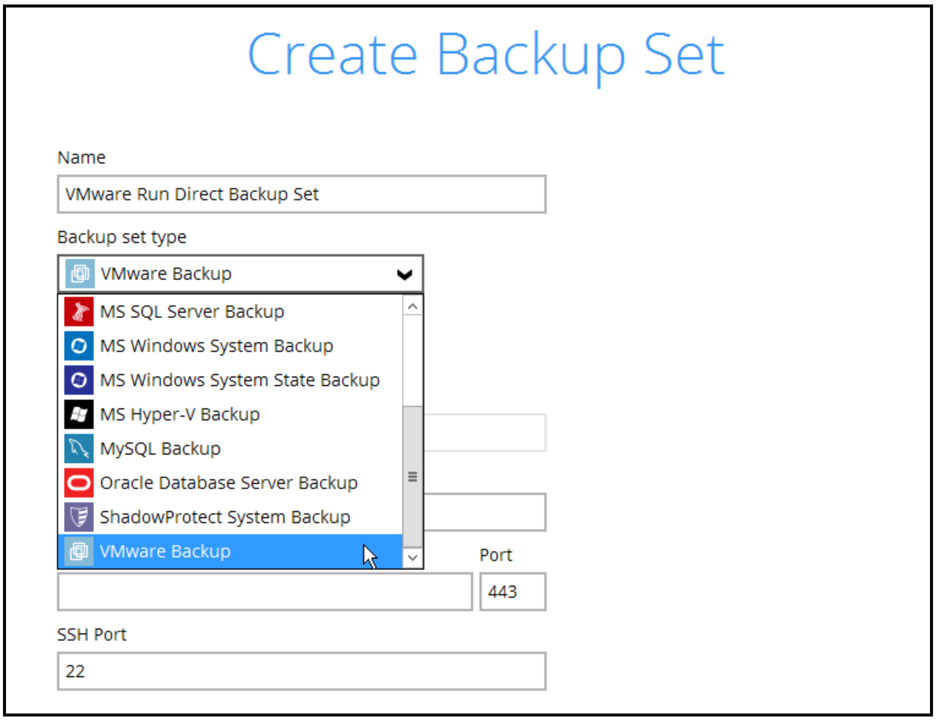
7 Creating a VMware VM Backup Set

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



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

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



Create Backup Set

Name: VMware Run Direct Backup Set

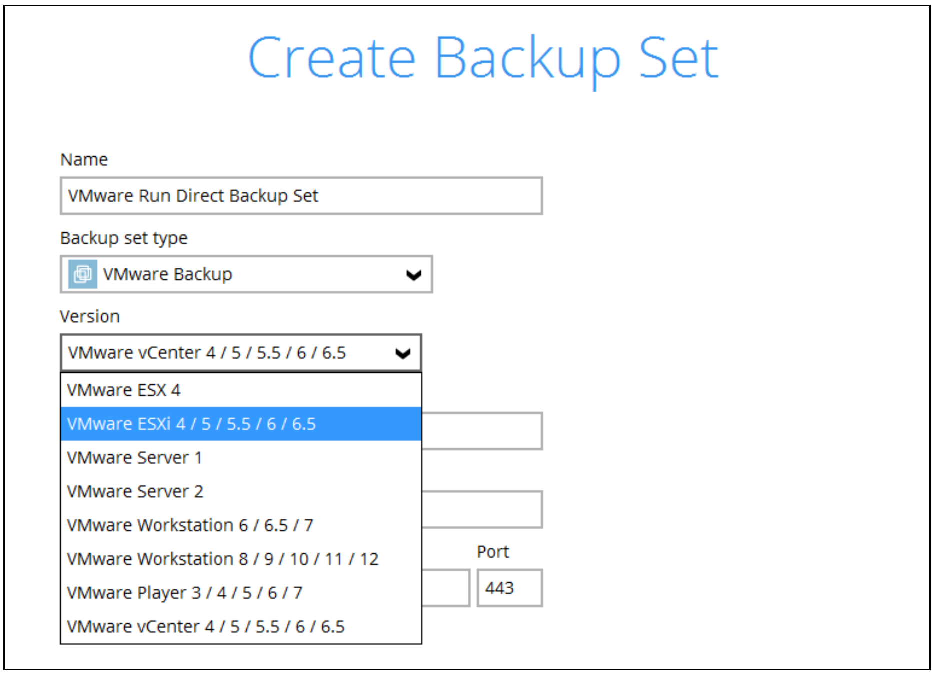
Backup set type: VMware Backup

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

Port: 443

SSH Port: 22

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



Create Backup Set

Name

VMware Run Direct Backup Set

Backup set type

VMware Backup

Version

VMware vCenter 4 / 5 / 5.5 / 6 / 6.5

- VMware ESX 4
- VMware ESXi 4 / 5 / 5.5 / 6 / 6.5
- VMware Server 1
- VMware Server 2
- VMware Workstation 6 / 6.5 / 7
- VMware Workstation 8 / 9 / 10 / 11 / 12
- VMware Player 3 / 4 / 5 / 6 / 7
- VMware vCenter 4 / 5 / 5.5 / 6 / 6.5

Port

443

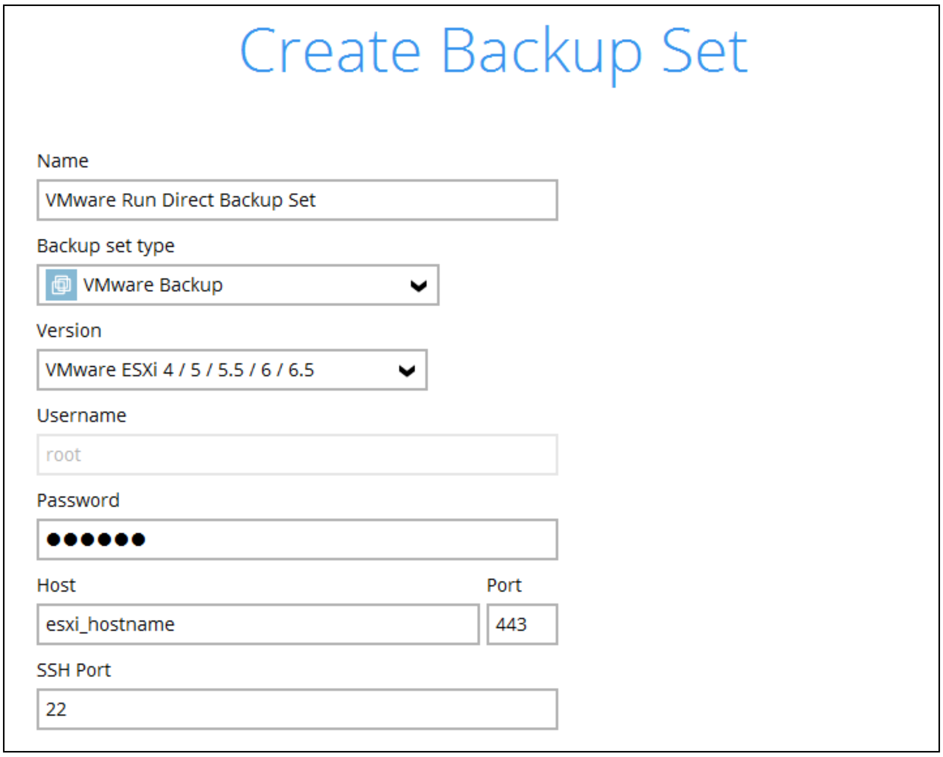
- Select **VMware ESXi 4 / 5 / 5.5 / 6 / 6.5** for a VMware ESXi backup set

-OR-

- Select **VMware vCenter 4 / 5 / 5.5 / 6 / 6.5** for a VMware vCenter backup set

Note: *Refer to the following KB article for the list compatible VMware platforms:* *http://wiki.ahsay.com/doku.php?id=public:5047_faq:frequently_asked_questions_about_ahsayobm_installation_on_synology_nas_devices&s[]=5047*

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



Create Backup Set

Name

VMware Run Direct Backup Set

Backup set type

VMware Backup

Version

VMware ESXi 4 / 5 / 5.5 / 6 / 6.5

Username

root

Password

●●●●●●

Host

esxi_hostname

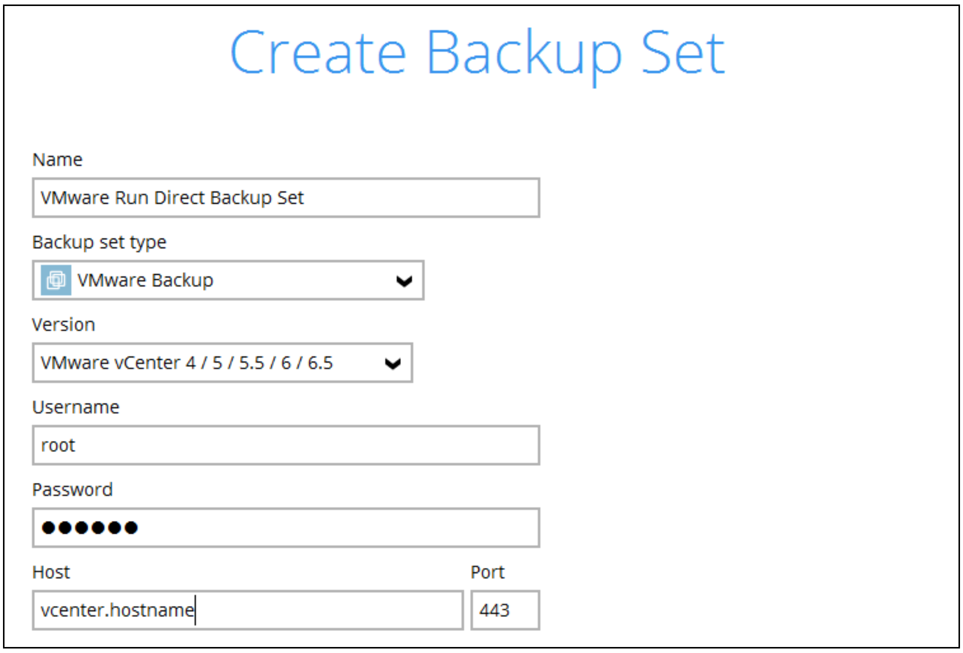
Port

443

SSH Port

22

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



Create Backup Set

Name: VMware Run Direct Backup Set

Backup set type: VMware Backup

Version: VMware vCenter 4 / 5 / 5.5 / 6 / 6.5

Username: root

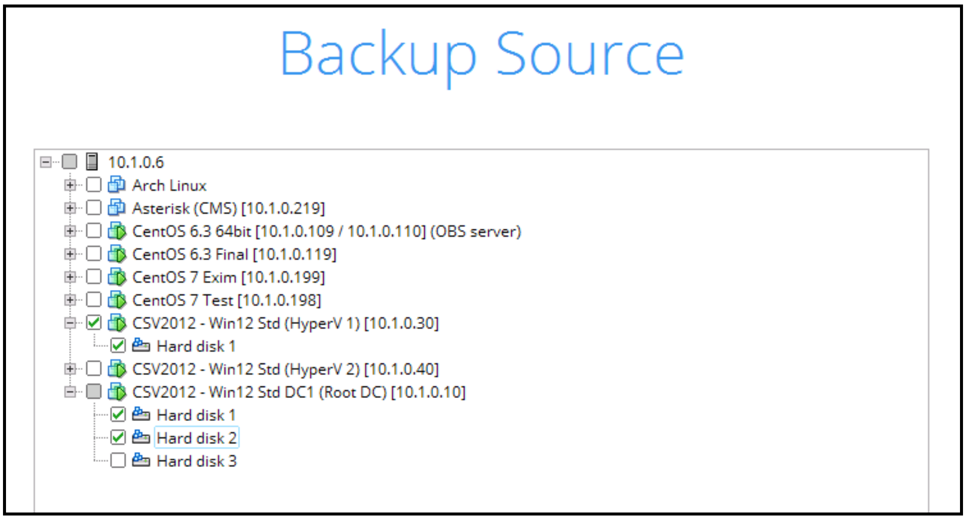
Password: ●●●●●●

Host: vcenter.hostname

Port: 443

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

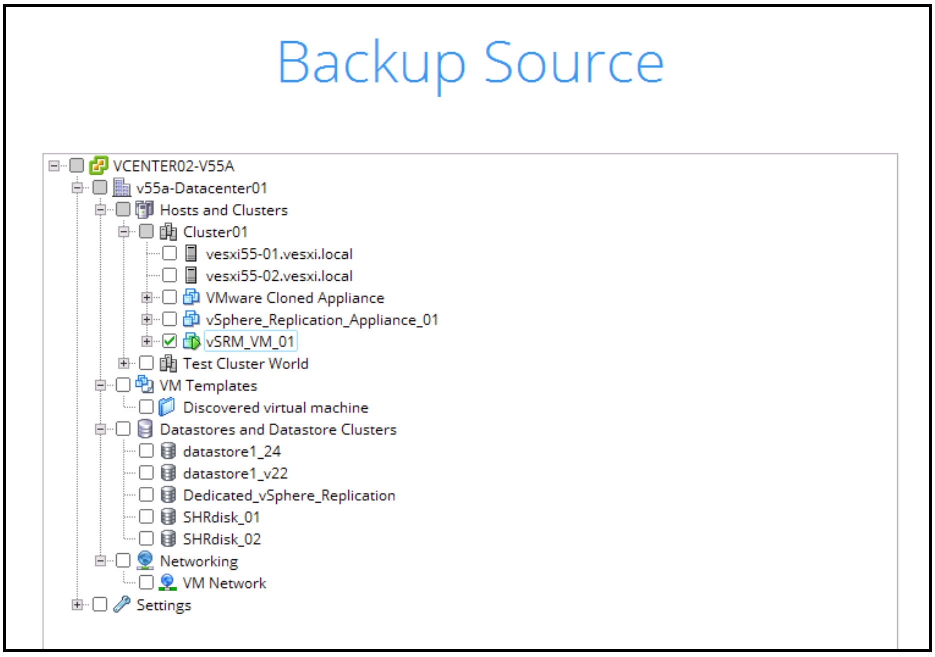
6. For VMware ESXi backup set, select the virtual machines or individual virtual disks that you would like to backup.



Backup Source

```
□ 10.1.0.6
  □ Arch Linux
  □ Asterisk (CMS) [10.1.0.219]
  □ CentOS 6.3 64bit [10.1.0.109 / 10.1.0.110] (OBS server)
  □ CentOS 6.3 Final [10.1.0.119]
  □ CentOS 7 Exim [10.1.0.199]
  □ CentOS 7 Test [10.1.0.198]
  ☑ CSV2012 - Win12 Std (HyperV 1) [10.1.0.30]
    ☑ Hard disk 1
  □ CSV2012 - Win12 Std (HyperV 2) [10.1.0.40]
  □ CSV2012 - Win12 Std DC1 (Root DC) [10.1.0.10]
    ☑ Hard disk 1
    ☑ Hard disk 2
    □ Hard disk 3
```

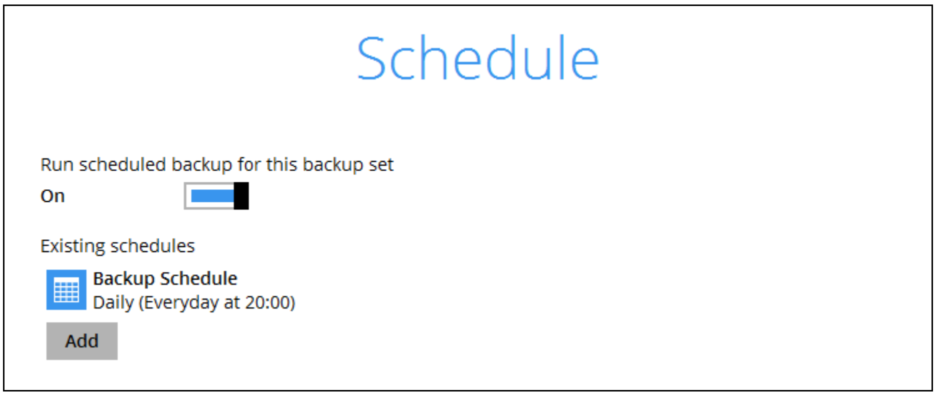
For VMware vCenter backup set, select the settings, virtual machines or individual virtual disks that you would like to backup.



Backup Source

```
⊟ □ VCENTER02-V55A
   ⊟ □ v55a-Datacenter01
      ⊟ □ Hosts and Clusters
         ⊟ □ Cluster01
               □ vesxi55-01.vesxi.local
               □ vesxi55-02.vesxi.local
            ⊞ □ VMware Cloned Appliance
            ⊞ □ vSphere_Replication_Appliance_01
            ⊞ ☑ vSRM_VM_01
         ⊞ □ Test Cluster World
      ⊟ □ VM Templates
            □ Discovered virtual machine
      ⊟ □ Datastores and Datastore Clusters
            □ datastore1_24
            □ datastore1_v22
            □ Dedicated_vSphere_Replication
            □ SHRdisk_01
            □ SHRdisk_02
      ⊟ □ Networking
            □ VM Network
   ⊞ □ Settings
```

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.



Schedule

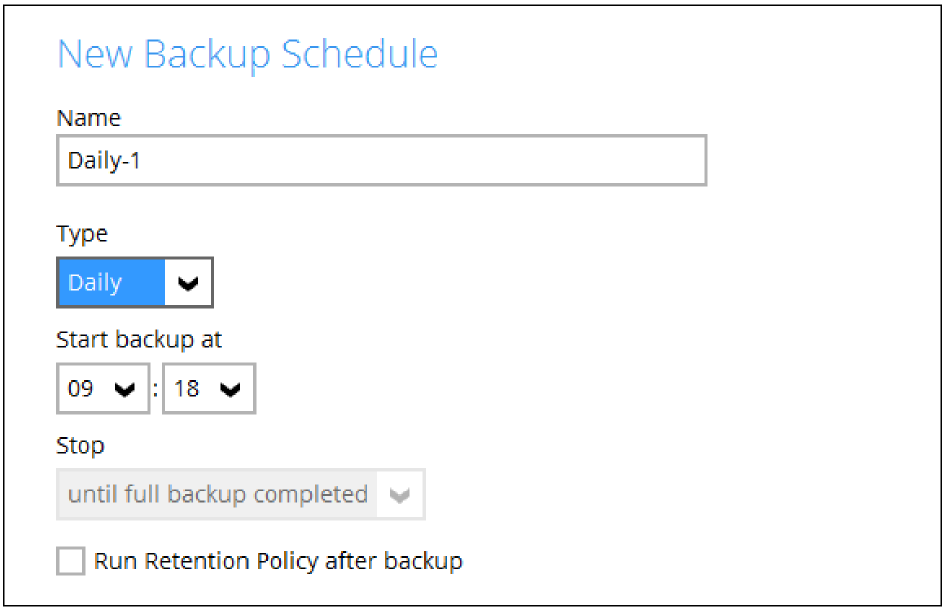
Run scheduled backup for this backup set

On

Existing schedules

Backup Schedule
Daily (Everyday at 20:00)

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 finsihed confgured a backup schedule.



New Backup Schedule

Name: Daily-1

Type: Daily

Start backup at: 09 : 18

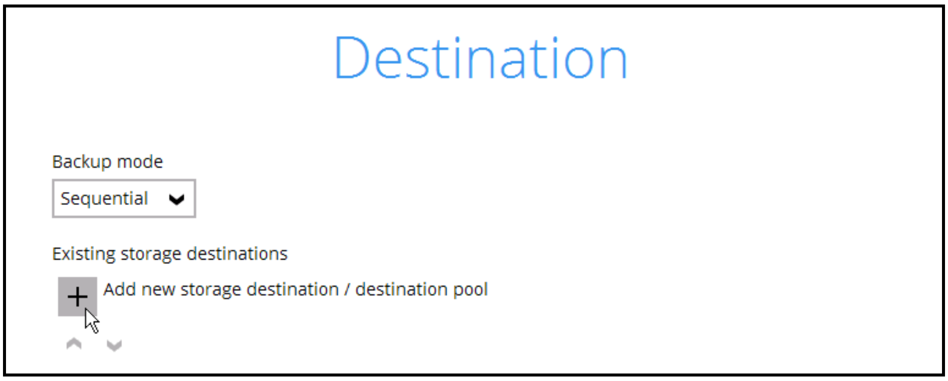
Stop: until full backup completed

□ Run Retention Policy after backup

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

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

8. In the Destination menu, select a backup destination where the backup data will be stored. Click the "**+**" icon next to **Add new storage destination / destination pool**.



Destination

Backup mode: Sequential

Existing storage destinations

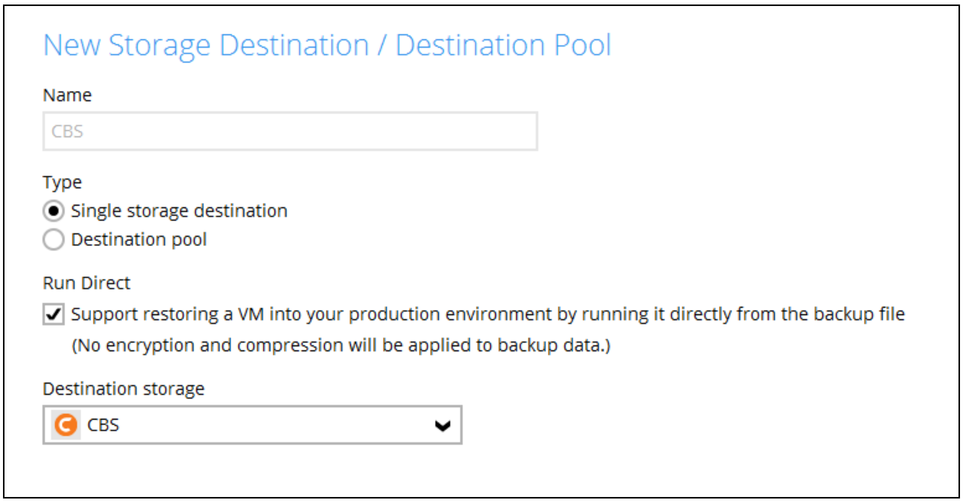
Select the appropriate option from the **Backup mode** dropdown menu.

- **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 storage type.

- **Single storage destination** – the entire backup will be uploaded to one single destination you selected under the **Destination storage** drop-down list. By default, the destination storage is selected as **CBS**.



New Storage Destination / Destination Pool

Name

CBS

Type

● Single storage destination

○ Destination pool

Run Direct

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

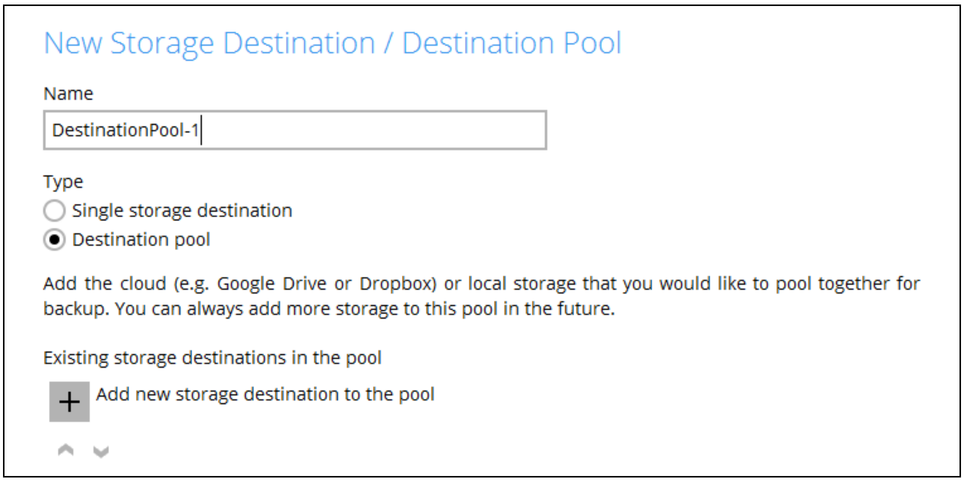
Destination storage

CBS

Run Direct

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

- **Destination pool** – the backup will be spread over on the destinations you have selected. Enter a **Name** for the destination pool and then click the **+** icon next to **Add new storage destination to the pool** to select the desired destinations.



New Storage Destination / Destination Pool

Name

DestinationPool-1

Type

○ Single storage destination

● Destination pool

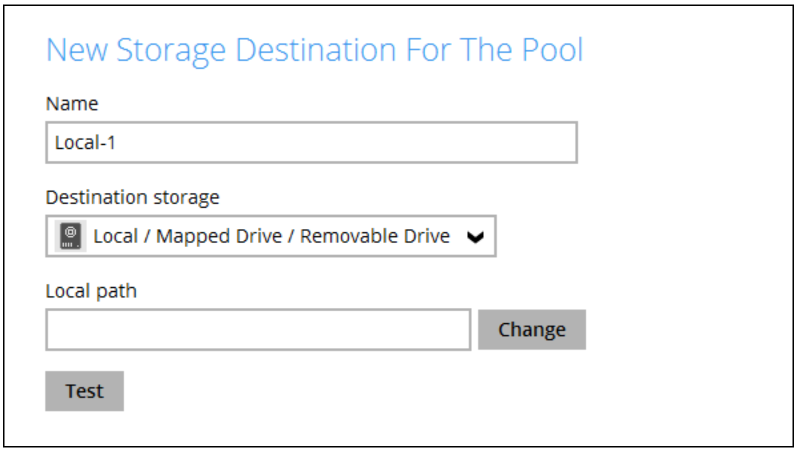
Add the cloud (e.g. Google Drive or Dropbox) or local storage that you would like to pool together for backup. You can always add more storage to this pool in the future.

Existing storage destinations in the pool

+ Add new storage destination to the pool

You can choose a storage combination of the Local/Mapped drive/Removable Drive, Cloud storage or FTP.

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



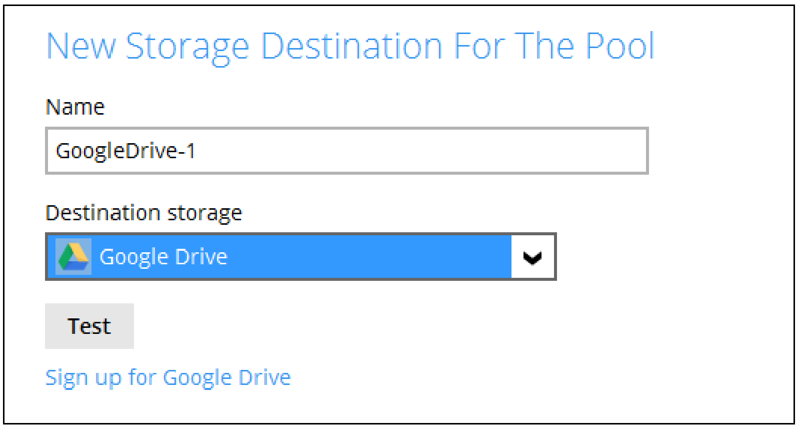
New Storage Destination For The Pool

Name: Local-1

Destination storage: Local / Mapped Drive / Removable Drive

Local path:

- If you have chosen the Cloud Storage, click **Test** to log in to the corresponding cloud storage service.

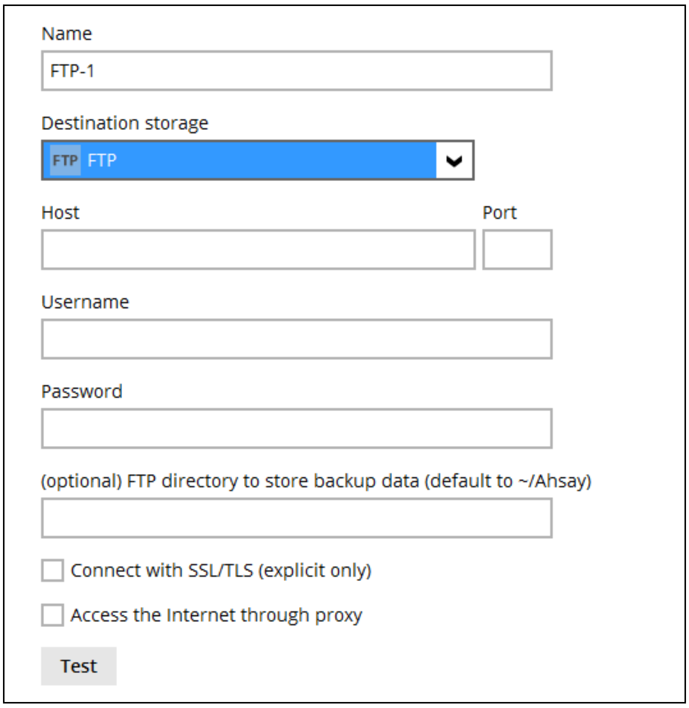


New Storage Destination For The Pool

Name: GoogleDrive-1

Destination storage: Google Drive

- If you have chosen the FTP as the destination, enter the the Host, Username and Password details.



Name: FTP-1

Destination storage: FTP

Host

Port

Username

Password

(optional) FTP directory to store backup data (default to ~/Ahsay)

□ Connect with SSL/TLS (explicit only)

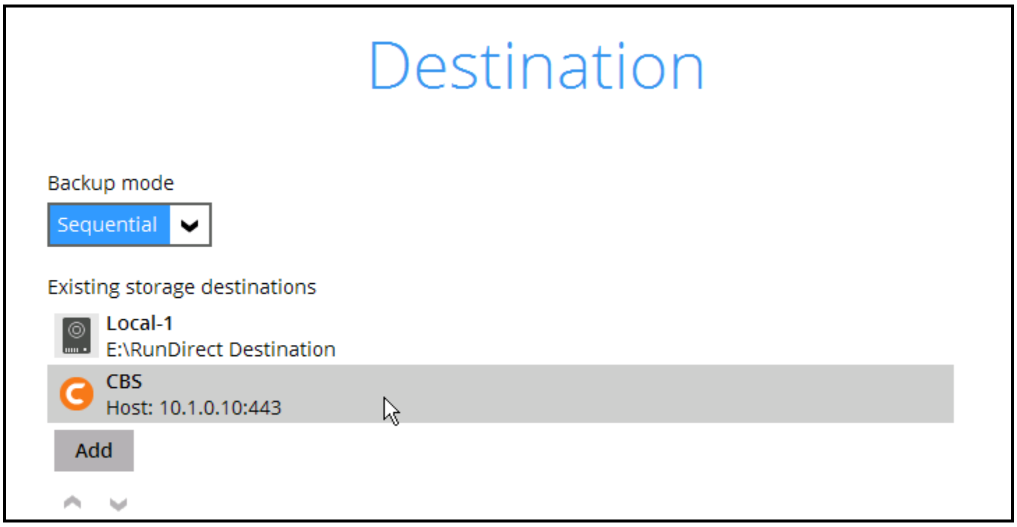
□ Access the Internet through proxy

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

Note

For more details on Backup Destination, refer to the following KB article for details: http://wiki.ahsay.com/doku.php?id=public:5026_faq:frequently_asked_questions_on_backup_destination&s[]=5026

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



Destination

Backup mode

Sequential

Existing storage destinations

Local-1
E:\RunDirect Destination

CBS
Host: 10.1.0.10:443

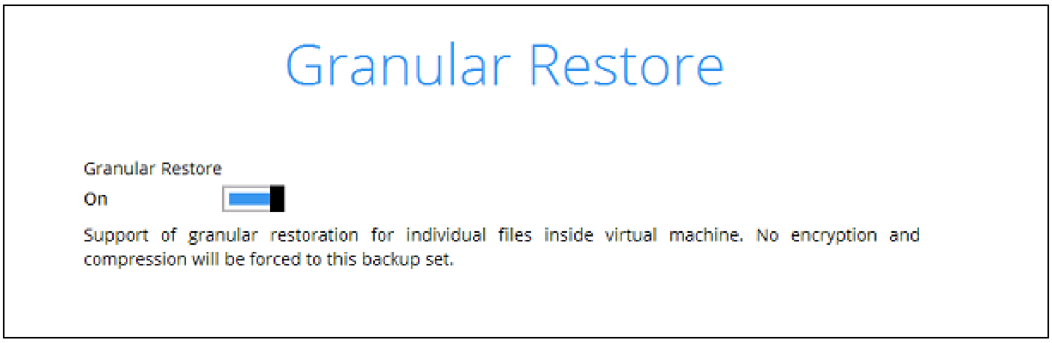
Add

Note

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

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

    Click **Next** to proceed.



Granular Restore

Granular Restore

On

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

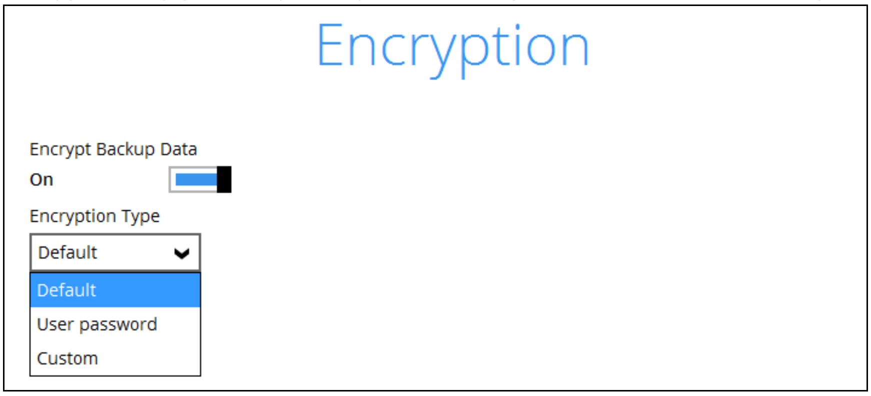
Notes

1. Once the Granular Restore feature is enabled and the backup set is saved, it is NOT possible to disable it afterwards, and vice versa. If you wish to change the Granular Restore settings, a new backup set will have to be created.
2. It is possible to enable both Granular Restore and Run Direct restore on the same backup set. However, AhsayOBM will only allow either Granular Restore or Run Direct restore to run, but not both to run concurrently.

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

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

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



Encryption

Encrypt Backup Data: On

Encryption Type: Default

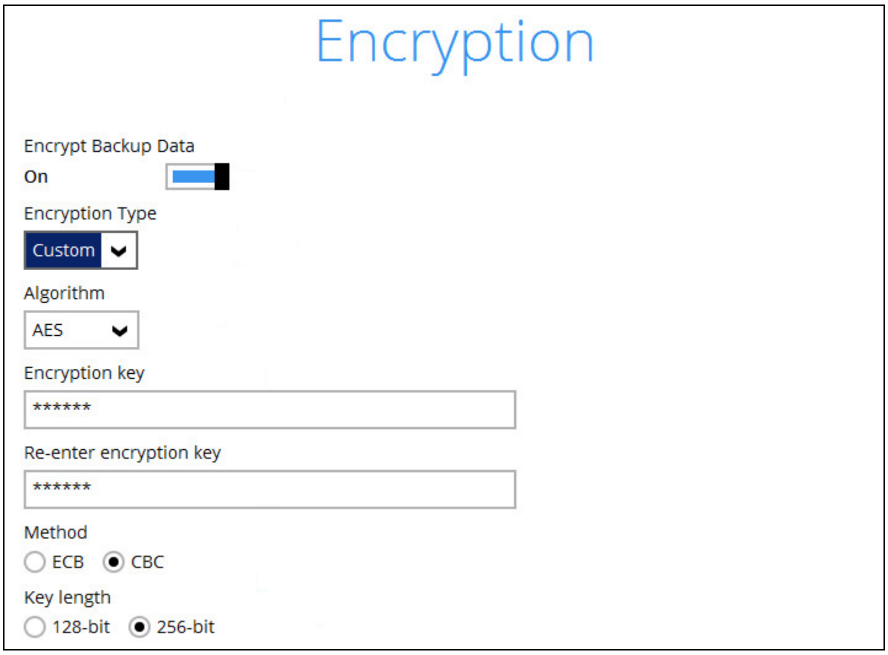
Note

For best practice on managing your encryption key, refer to the following KB article.
http://wiki.ahsay.com/doku.php?id=public:5034_best_practices_for_managing_encryption_key_on_ahsayobm_or_ahsayacb_version_7&s[]=5034

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

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

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



Encryption

Encrypt Backup Data

On

Encryption Type

Custom

Algorithm

AES

Encryption key

******

Re-enter encryption key

******

Method

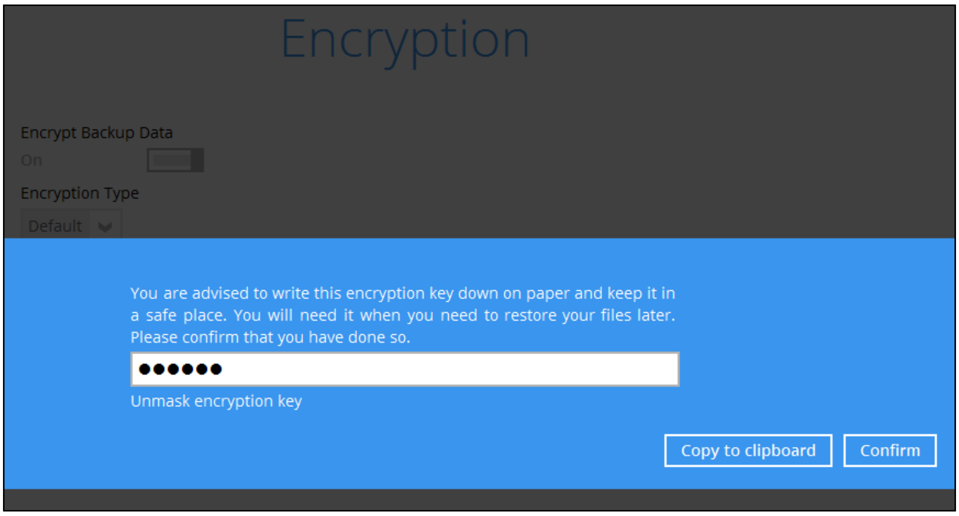
○ ECB ● CBC

Key length

○ 128-bit ● 256-bit

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.



Encryption

Encrypt Backup Data

On

Encryption Type

Default

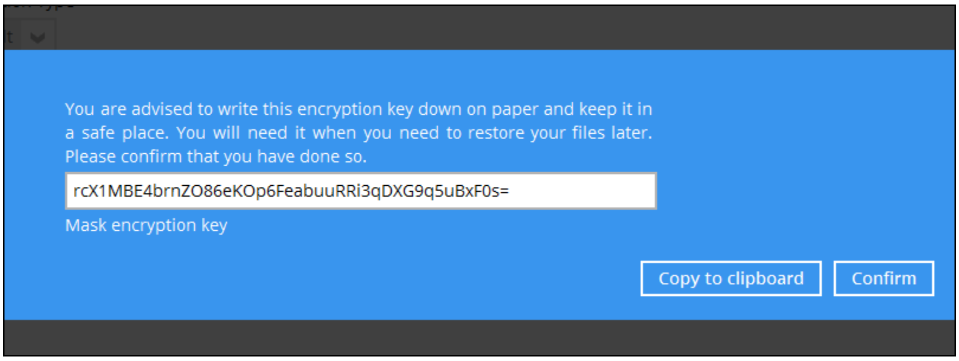
You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.

●●●●●●

Unmask encryption key

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

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



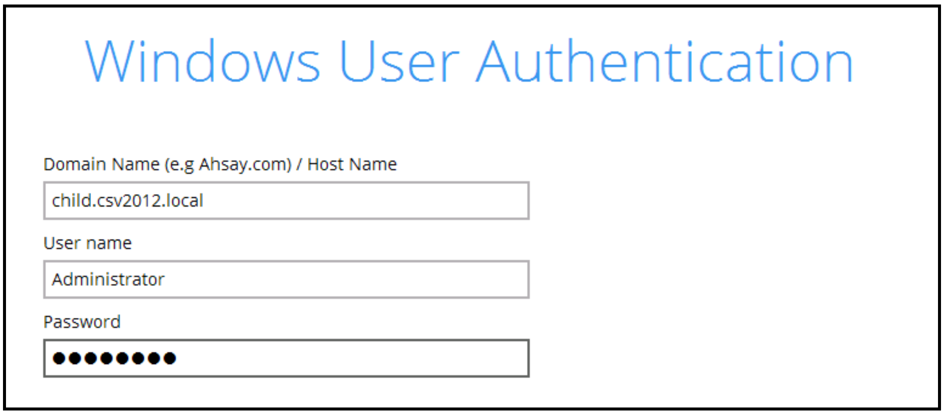
You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.

rcX1MBE4brnZO86eKOp6FeabuuRRi3qDXG9q5uBxF0s=

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

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

14. Enter the Windows login credentials used by AhsayOBM to authenticate the scheduled or continuous backup.



Windows User Authentication

Domain Name (e.g Ahsay.com) / Host Name: child.csv2012.local

User name: Administrator

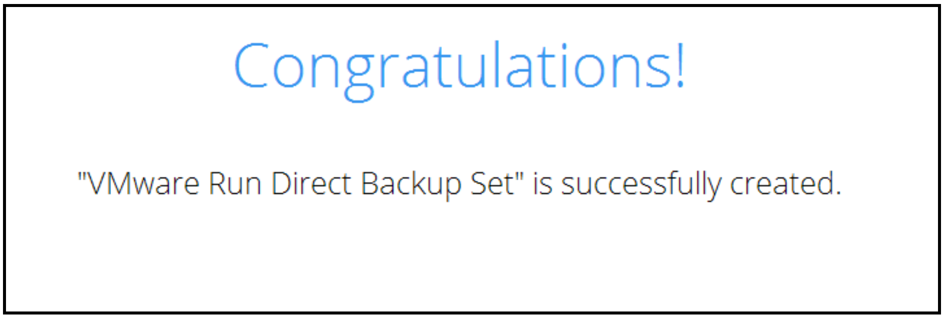
Password: ●●●●●●●●

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

Note

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

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



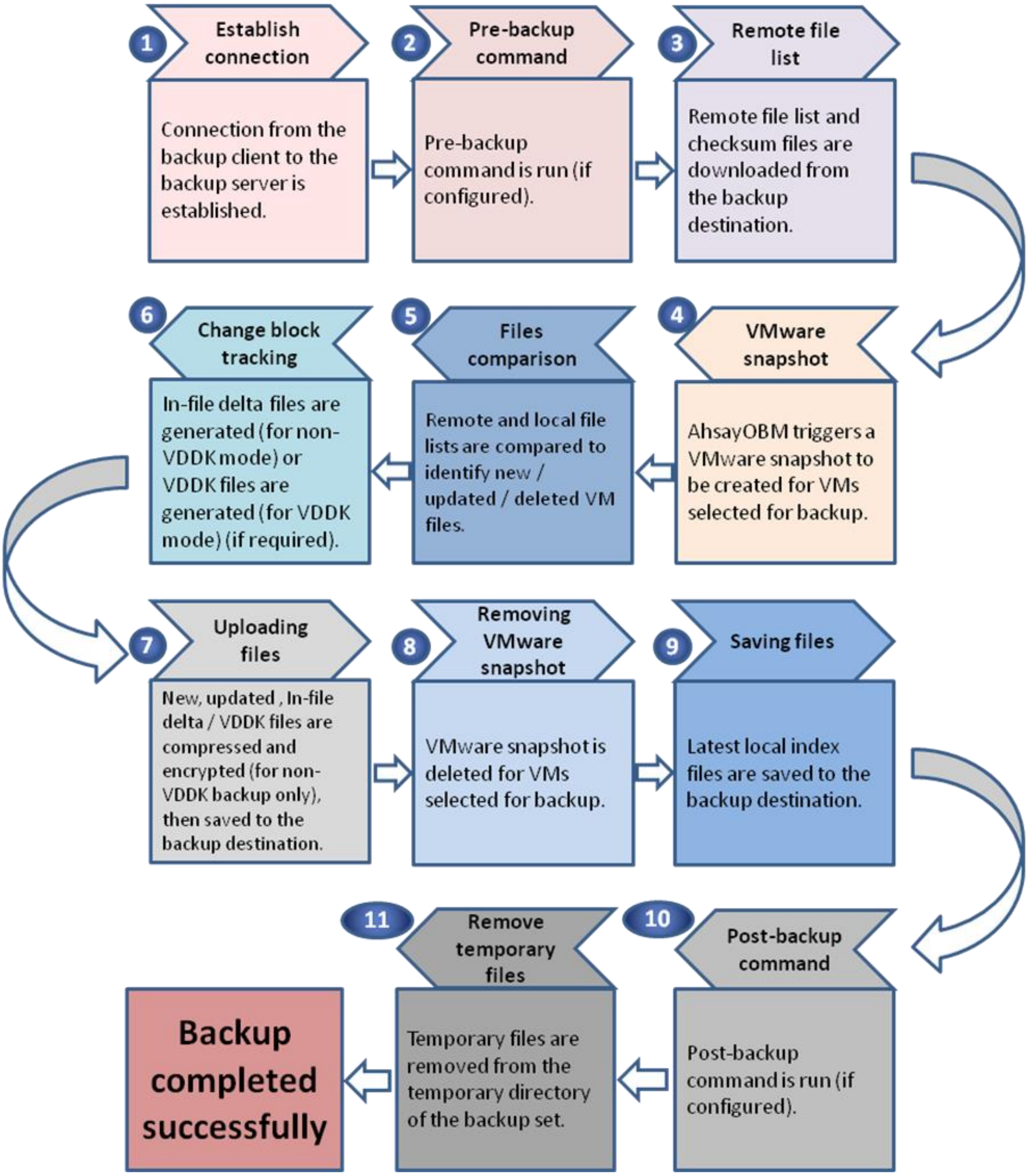
Congratulations!

"VMware Run Direct Backup Set" is successfully created.

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

8 Overview on Backup Process

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



1 Establish connection

Connection from the backup client to the backup server is established.

2 Pre-backup command

Pre-backup command is run (if configured).

3 Remote file list

Remote file list and checksum files are downloaded from the backup destination.

4 VMware snapshot

AhsayOBM triggers a VMware snapshot to be created for VMs selected for backup.

5 Files comparison

Remote and local file lists are compared to identify new / updated / deleted VM files.

6 Change block tracking

In-file delta files are generated (for non-VDDK mode) or VDDK files are generated (for VDDK mode) (if required).

7 Uploading files

New, updated , In-file delta / VDDK files are compressed and encrypted (for non-VDDK backup only), then saved to the backup destination.

8 Removing VMware snapshot

VMware snapshot is deleted for VMs selected for backup.

9 Saving files

Latest local index files are saved to the backup destination.

10 Post-backup command

Post-backup command is run (if configured).

11 Remove temporary files

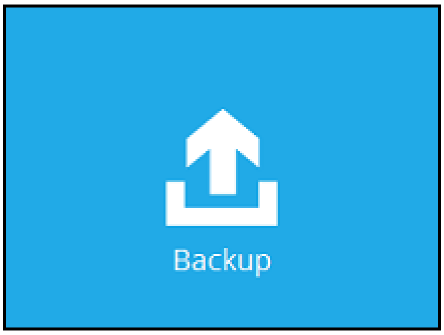
Temporary files are removed from the temporary directory of the backup set.

Backup completed successfully

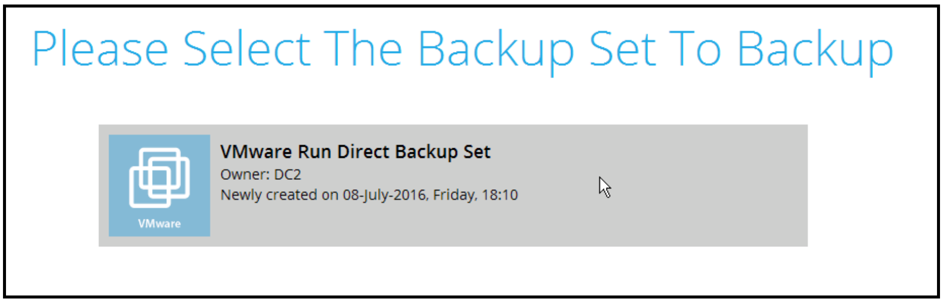
9 Running a Backup

Start a Manual Backup

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



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

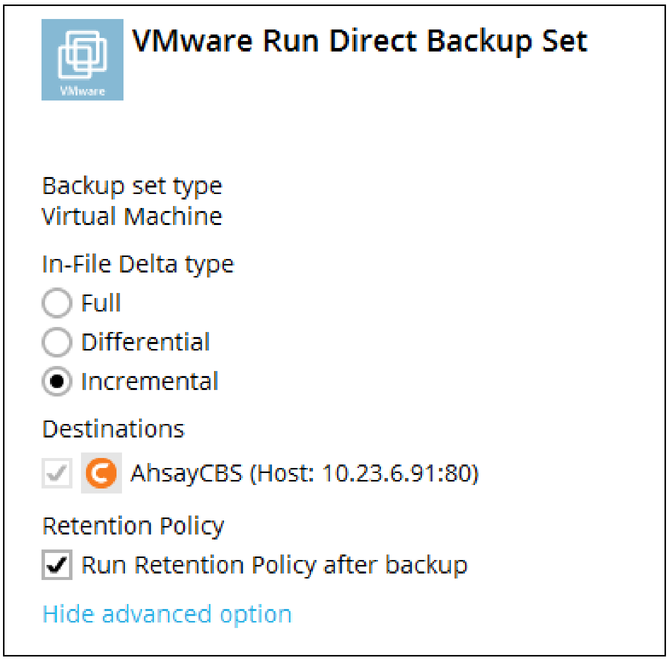


Please Select The Backup Set To Backup

VMware Run Direct Backup Set
Owner: DC2
Newly created on 08-July-2016, Friday, 18:10

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:



VMware Run Direct Backup Set

Backup set type
Virtual Machine

In-File Delta type
○ Full
○ Differential
● Incremental

Destinations
☑ AhsayCBS (Host: 10.23.6.91:80)

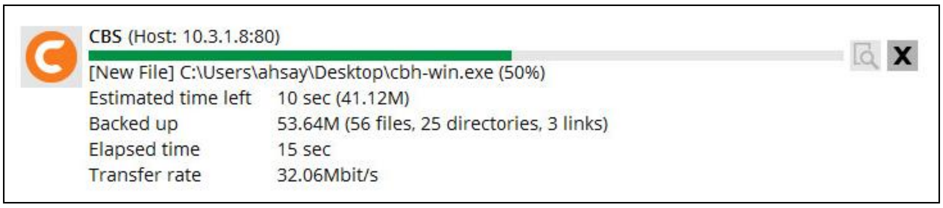
Retention Policy
☑ Run Retention Policy after backup

Hide advanced option

- **Full** – A full backup captures all the data that you want to protect. When you run a backup job for the first time, AhsayOBM will run a full backup regardless of the in-file delta setting.
- **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.

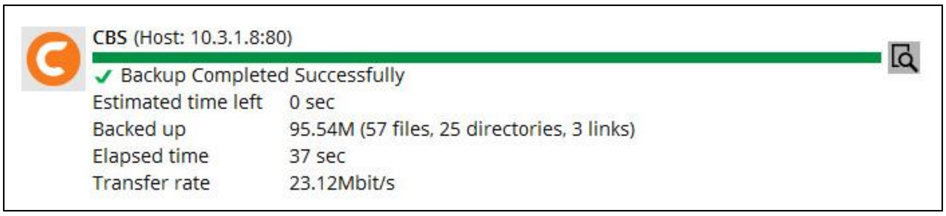


CBS (Host: 10.3.1.8:80)

[New File] C:\Users\ahsay\Desktop\cbh-win.exe (50%)

Estimated time left	10 sec (41.12M)
Backed up	53.64M (56 files, 25 directories, 3 links)
Elapsed time	15 sec
Transfer rate	32.06Mbit/s

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

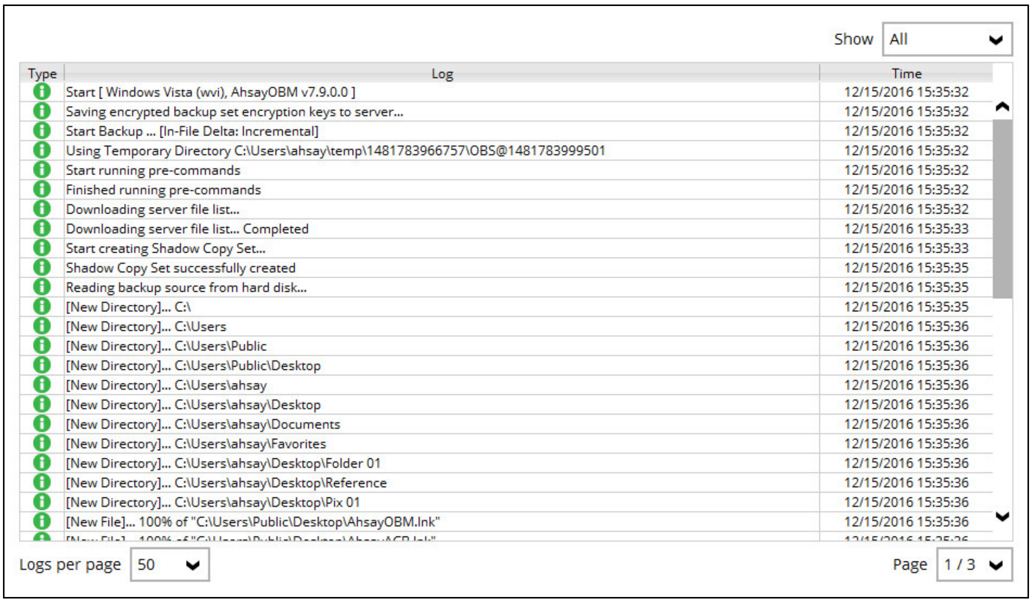


CBS (Host: 10.3.1.8:80)

✓ Backup Completed Successfully

Estimated time left	0 sec
Backed up	95.54M (57 files, 25 directories, 3 links)
Elapsed time	37 sec
Transfer rate	23.12Mbit/s

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.



Show: All

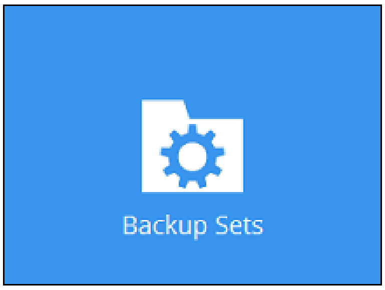
Type	Log	Time
ⓘ	Start [Windows Vista (wvi), AhsayOBM v7.9.0.0]	12/15/2016 15:35:32
ⓘ	Saving encrypted backup set encryption keys to server...	12/15/2016 15:35:32
ⓘ	Start Backup ... [In-File Delta: Incremental]	12/15/2016 15:35:32
ⓘ	Using Temporary Directory C:\Users\ahsay\temp\1481783966757\OBS@1481783999501	12/15/2016 15:35:32
ⓘ	Start running pre-commands	12/15/2016 15:35:32
ⓘ	Finished running pre-commands	12/15/2016 15:35:32
ⓘ	Downloading server file list...	12/15/2016 15:35:32
ⓘ	Downloading server file list... Completed	12/15/2016 15:35:33
ⓘ	Start creating Shadow Copy Set...	12/15/2016 15:35:33
ⓘ	Shadow Copy Set successfully created	12/15/2016 15:35:35
ⓘ	Reading backup source from hard disk...	12/15/2016 15:35:35
ⓘ	[New Directory]... C:\	12/15/2016 15:35:35
ⓘ	[New Directory]... C:\Users	12/15/2016 15:35:36
ⓘ	[New Directory]... C:\Users\Public	12/15/2016 15:35:36
ⓘ	[New Directory]... C:\Users\Public\Desktop	12/15/2016 15:35:36
ⓘ	[New Directory]... C:\Users\ahsay	12/15/2016 15:35:36
ⓘ	[New Directory]... C:\Users\ahsay\Desktop	12/15/2016 15:35:36
ⓘ	[New Directory]... C:\Users\ahsay\Documents	12/15/2016 15:35:36
ⓘ	[New Directory]... C:\Users\ahsay\Favorites	12/15/2016 15:35:36
ⓘ	[New Directory]... C:\Users\ahsay\Desktop\Folder 01	12/15/2016 15:35:36
ⓘ	[New Directory]... C:\Users\ahsay\Desktop\Reference	12/15/2016 15:35:36
ⓘ	[New Directory]... C:\Users\ahsay\Desktop\Pix 01	12/15/2016 15:35:36
ⓘ	[New File]... 100% of "C:\Users\Public\Desktop\AhsayOBM.lnk"	12/15/2016 15:35:36
ⓘ	[New File]... 100% of "C:\Users\Public\Desktop\AhsayACB.lnk"	12/15/2016 15:35:36

Logs per page: 50

Page: 1 / 3

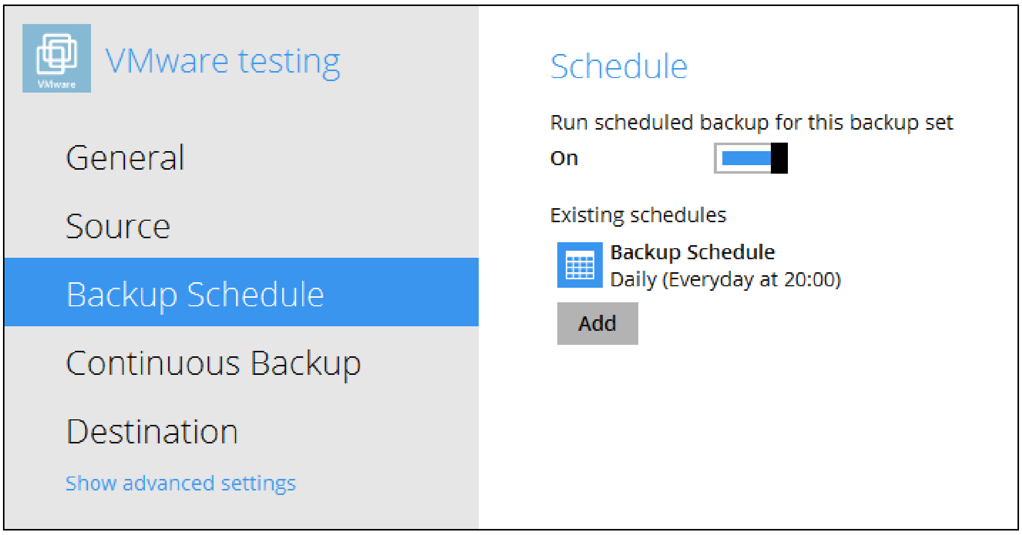
Configure Backup Schedule for Automated Backup

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.



Schedule

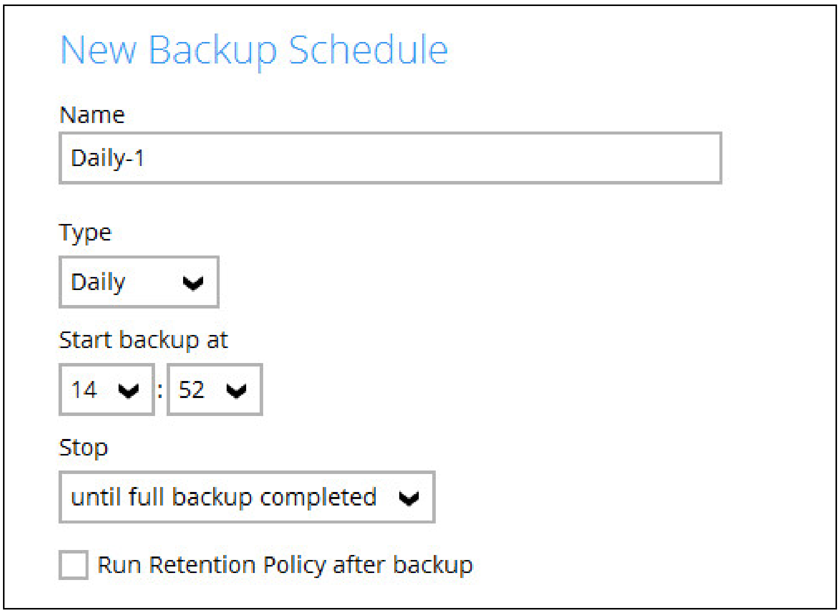
Run scheduled backup for this backup set

On

Existing schedules

Backup Schedule
Daily (Everyday at 20:00)

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



New Backup Schedule

Name: Daily-1

Type: Daily

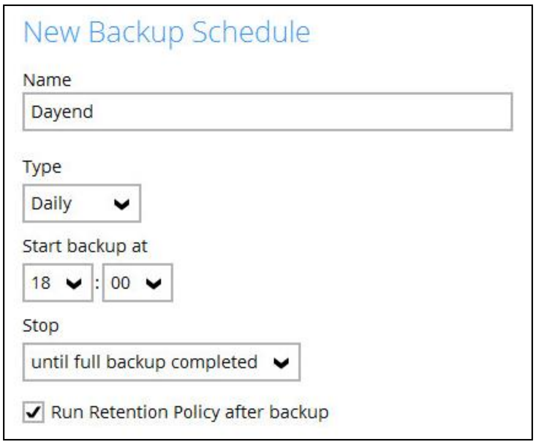
Start backup at: 14 : 52

Stop: until full backup completed

☐ Run Retention Policy after backup

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

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



New Backup Schedule

Name: Dayend

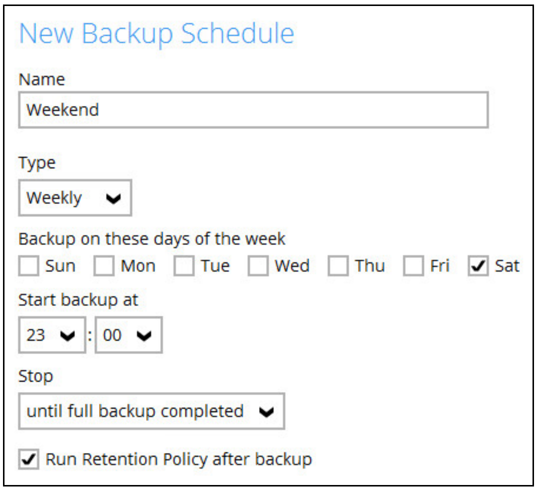
Type: Daily

Start backup at: 18 : 00

Stop: until full backup completed

☑ Run Retention Policy after backup

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



New Backup Schedule

Name: Weekend

Type: Weekly

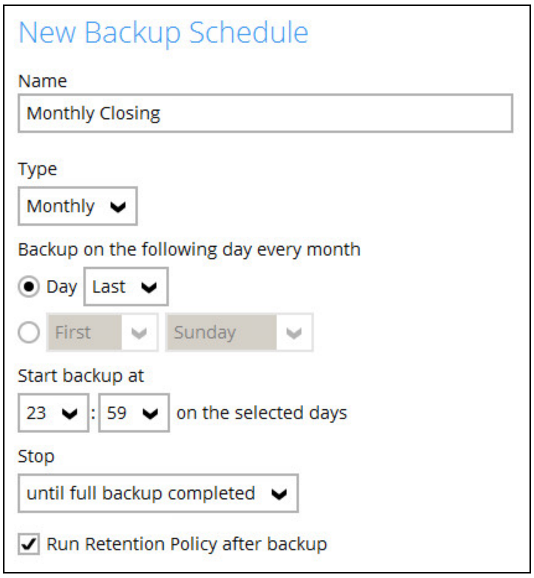
Backup on these days of the week: □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri ☑ Sat

Start backup at: 23 : 00

Stop: until full backup completed

☑ Run Retention Policy after backup

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



New Backup Schedule

Name: Monthly Closing

Type: Monthly

Backup on the following day every month

● Day Last

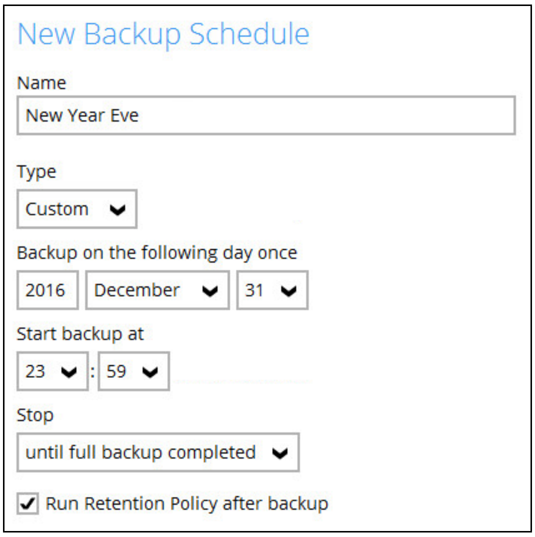
○ First Sunday

Start backup at: 23 : 59 on the selected days

Stop: until full backup completed

☑ Run Retention Policy after backup

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



New Backup Schedule

Name

New Year Eve

Type

Custom

Backup on the following day once

2016 December 31

Start backup at

23 : 59

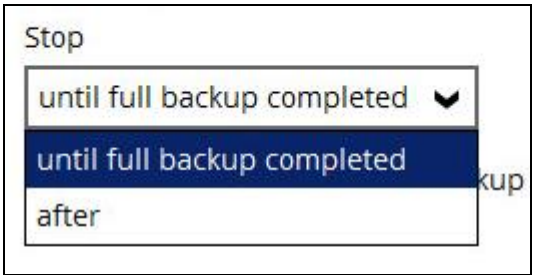
Stop

until full backup completed

☑ Run Retention Policy after backup

The **Stop** dropdown menu offers two options:

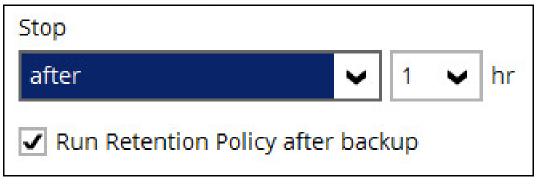
- **until full backup completed** – in case you prefer a complete backup



Stop

until full backup completed

- **after [how many] hr** – in case you prefer the backup job to stop after a certain number of hours regardless of whether or not the backup job is complete

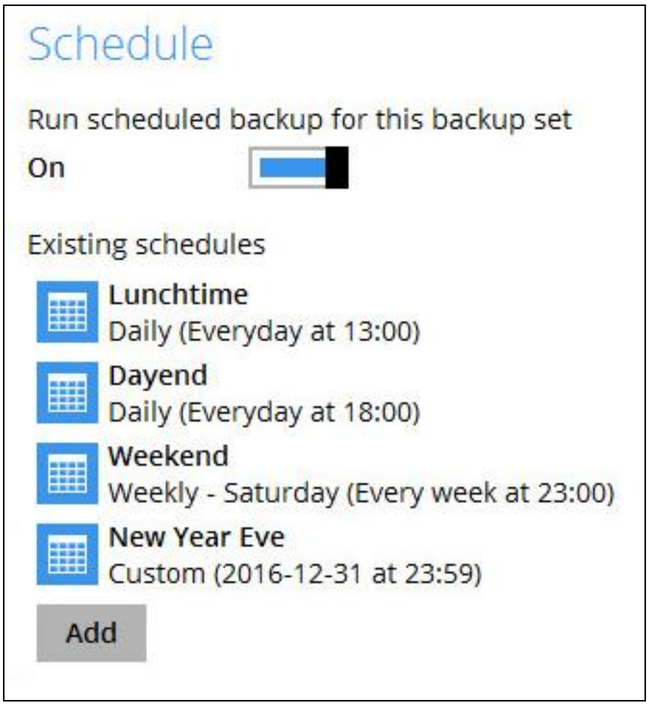


Stop

after 1 hr

☑ Run Retention Policy after backup

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



Schedule

Run scheduled backup for this backup set

On

Existing schedules

Lunchtime
Daily (Everyday at 13:00)

Dayend
Daily (Everyday at 18:00)

Weekend
Weekly - Saturday (Every week at 23:00)

New Year Eve
Custom (2016-12-31 at 23:59)

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

10 Restore Methods

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

Method 1 - Restoring a Virtual Machine with Run Direct

Introduction

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

Pros

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

Cons

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

Method 2 - Restoring a Virtual Machine without Run Direct

Introduction

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

Pros

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

Cons

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

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

Introduction

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

Pros

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

Cons

- Restore procedures are relatively complicated

Method 4 – Granular Restore

Introduction

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

For more details about Granular Restore, refer to the Granular Restore section.

Pros

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

Cons

- No encryption and compression for backup set

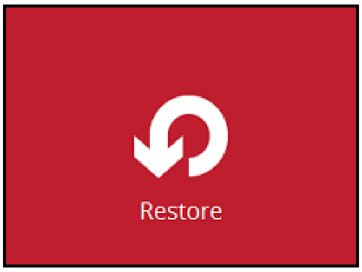
11 Method 1 - Restoring a Virtual Machine with Run Direct

Login to AhsayOBM

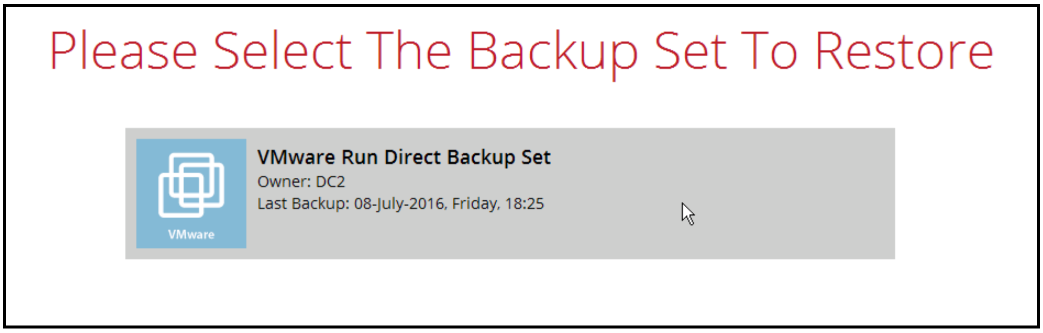
Log in to the AhsayOBM application according to the instructions provided in the chapter on Starting AhsayOBM.

Running Direct Restore via AhsayOBM

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



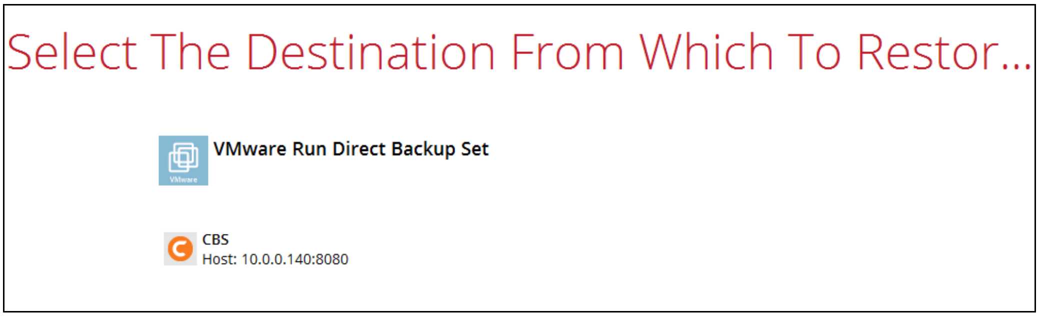
2. Select the backup set that you would like to restore the VM from.



Please Select The Backup Set To Restore

VMware Run Direct Backup Set
Owner: DC2
Last Backup: 08-July-2016, Friday, 18:25

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

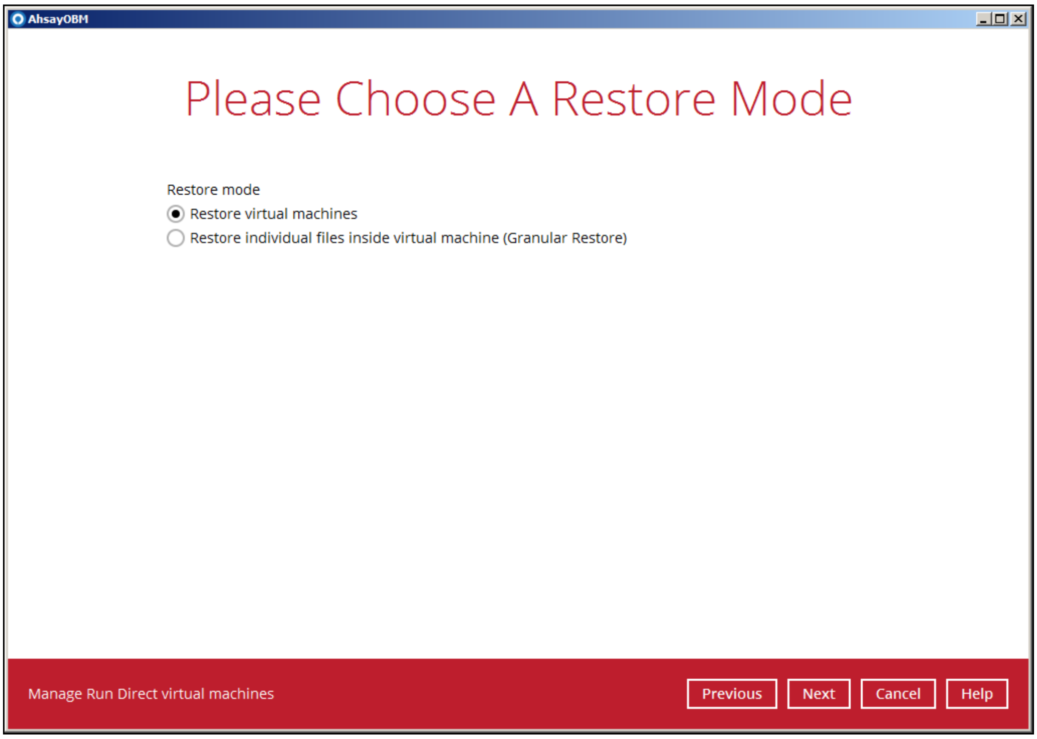


Select The Destination From Which To Restor...

VMware Run Direct Backup Set

CBS
Host: 10.0.0.140:8080

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



Please Choose A Restore Mode

Restore mode

● Restore virtual machines

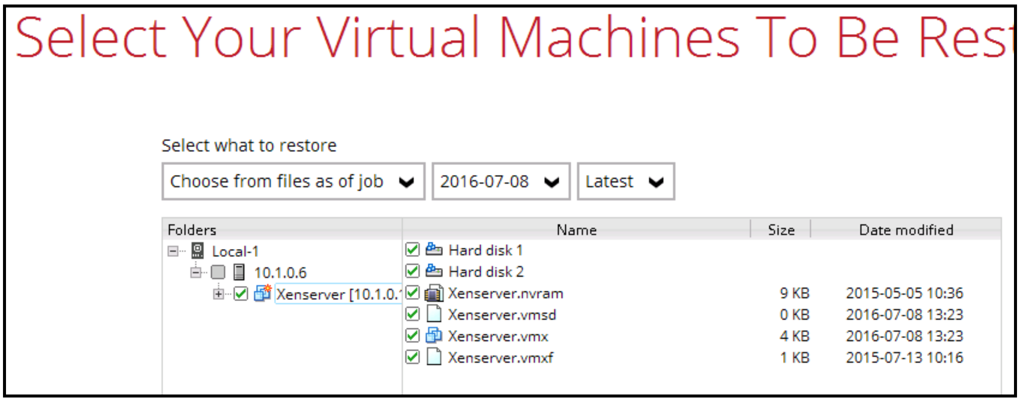
○ Restore individual files inside virtual machine (Granular Restore)

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

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

Important

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



Select Your Virtual Machines To Be Res

Select what to restore

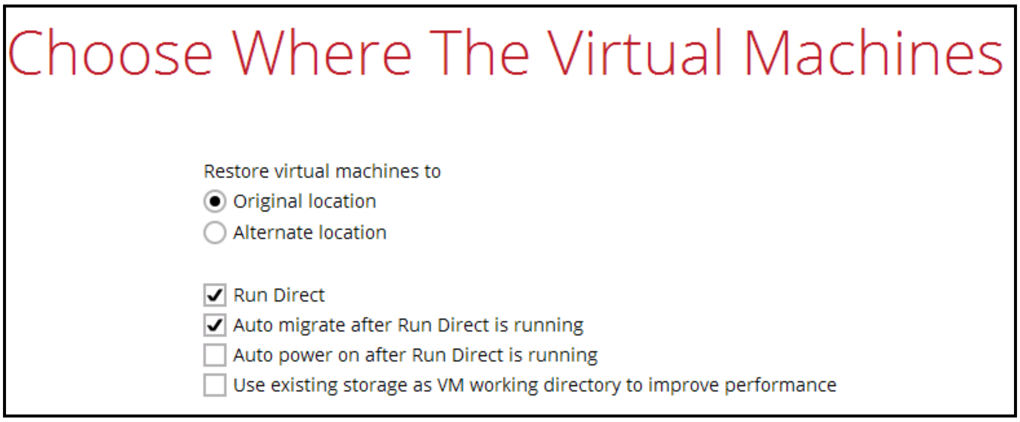
Choose from files as of job | 2016-07-08 | Latest

Folders	Name	Size	Date modified
⊟ Local-1	☑ Hard disk 1		
⊟ □ 10.1.0.6	☑ Hard disk 2		
⊞ ☑ Xenserver [10.1.0.'	☑ Xenserver.nvram	9 KB	2015-05-05 10:36
	☑ Xenserver.vmsd	0 KB	2016-07-08 13:23
	☑ Xenserver.vmx	4 KB	2016-07-08 13:23
	☑ Xenserver.vmxf	1 KB	2015-07-13 10:16

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

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

another VMware host).


Choose Where The Virtual Machines

Restore virtual machines to

● Original location

○ Alternate location

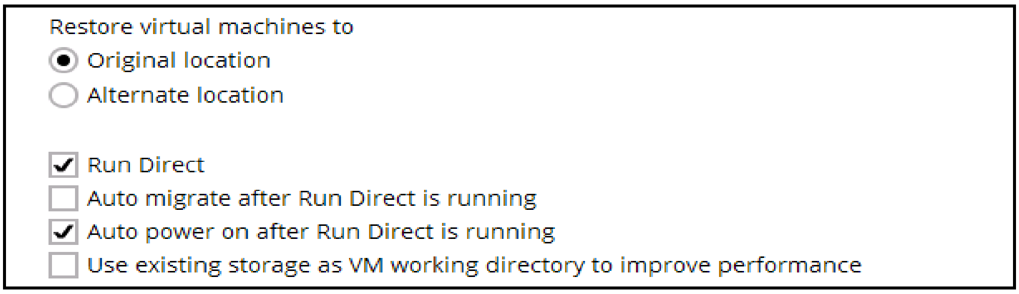
☑ Run Direct

☑ Auto migrate after Run Direct is running

□ Auto power on after Run Direct is running

□ Use existing storage as VM working directory to improve performance

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


Restore virtual machines to

● Original location

○ Alternate location

☑ Run Direct

□ Auto migrate after Run Direct is running

☑ Auto power on after Run Direct is running

□ Use existing storage as VM working directory to improve performance

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

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

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

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

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

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

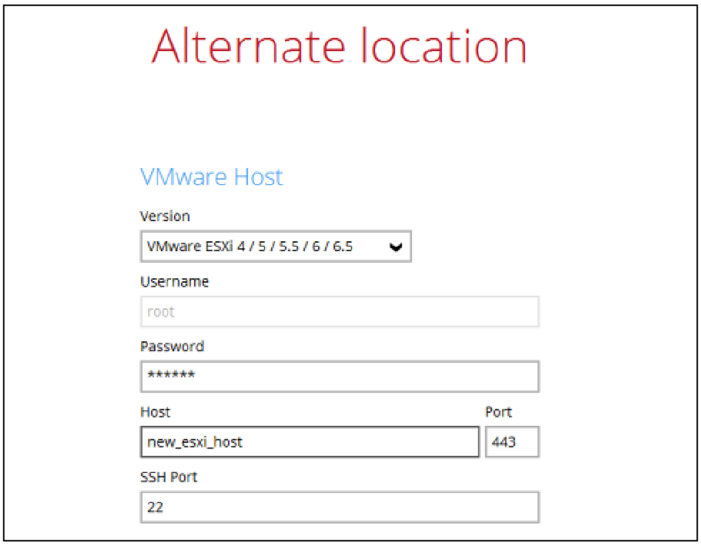
  Enable this option to enhance performance of the restored VM. Click **Next** to proceed when you are done with the settings.

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 4 / 5 / 5.5 / 6 / 6.5**, then enter the **Password** of the root account, **Host**, **Port** and

SSH Port of the new / original host.



Alternate location

VMware Host

Version

VMware ESXi 4 / 5 / 5.5 / 6 / 6.5

Username

root

Password

******

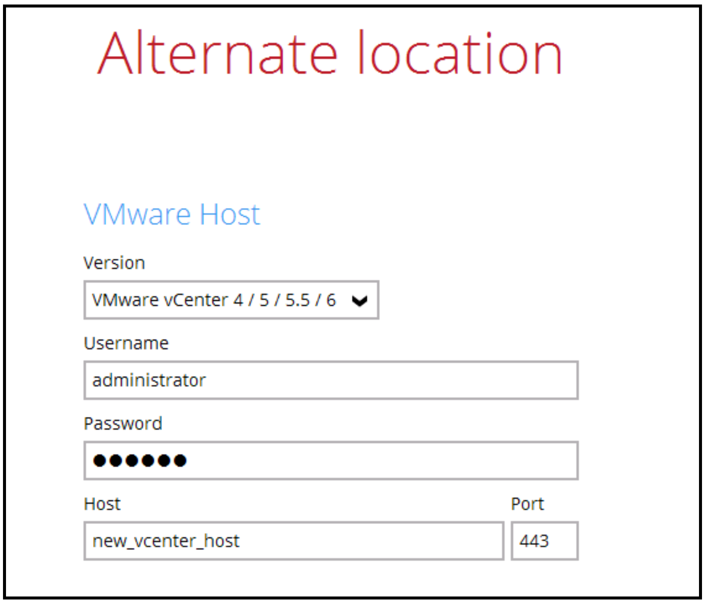
Host: new_esxi_host

Port: 443

SSH Port

22

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



Alternate location

VMware Host

Version

VMware vCenter 4 / 5 / 5.5 / 6

Username

administrator

Password

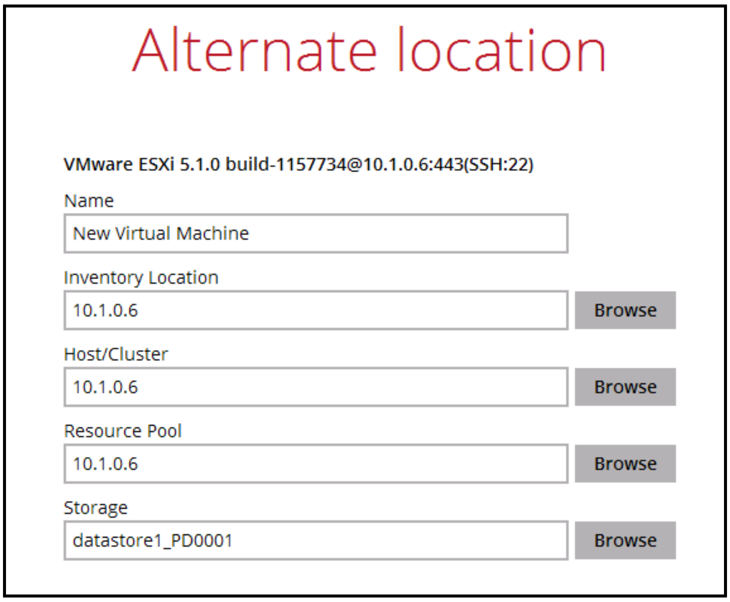
●●●●●●

Host: new_vcenter_host

Port: 443

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

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



Alternate location

VMware ESXi 5.1.0 build-1157734@10.1.0.6:443(SSH:22)

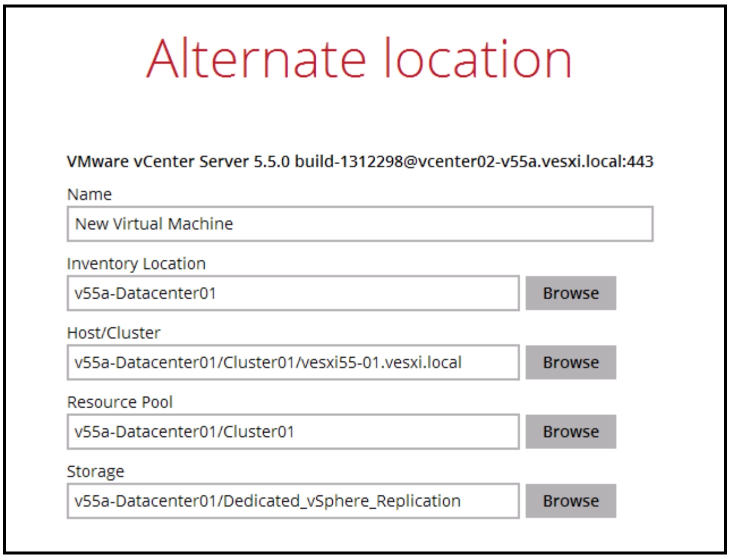
Name: New Virtual Machine

Inventory Location: 10.1.0.6

Host/Cluster: 10.1.0.6

Resource Pool: 10.1.0.6

Storage: datastore1_PD0001



Alternate location

VMware vCenter Server 5.5.0 build-1312298@vcenter02-v55a.vesxi.local:443

Name: New Virtual Machine

Inventory Location: v55a-Datacenter01

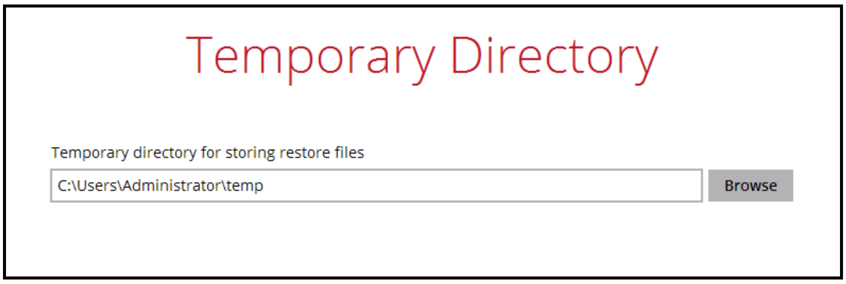
Host/Cluster: v55a-Datacenter01/Cluster01/vesxi55-01.vesxi.local

Resource Pool: v55a-Datacenter01/Cluster01

Storage: v55a-Datacenter01/Dedicated_vSphere_Replication

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.

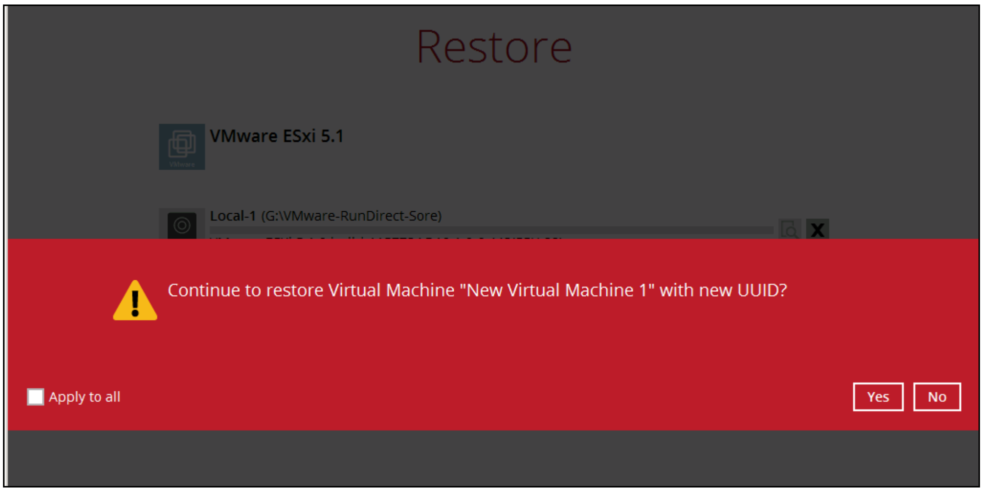


Temporary Directory

Temporary directory for storing restore files: C:\Users\Administrator\temp

11. When restoring your guest VM to another VMware host, the following message will be prompted. 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 because it is not possible to have two identical UUID running at the same time.

Therefore, make sure you click **Yes** when you see the prompt below.



Restore

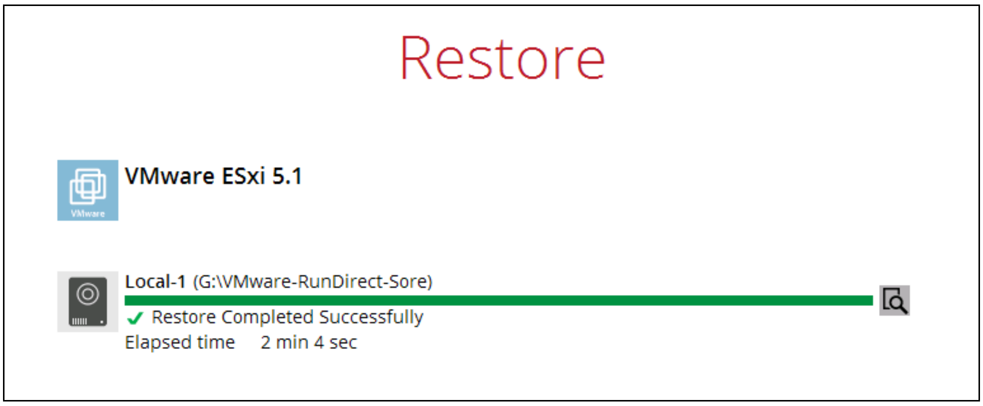
VMware ESXi 5.1

Local-1 (G:\VMware-RunDirect-Sore)

Continue to restore Virtual Machine "New Virtual Machine 1" with new UUID?

□ Apply to all

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



Restore

VMware ESXi 5.1

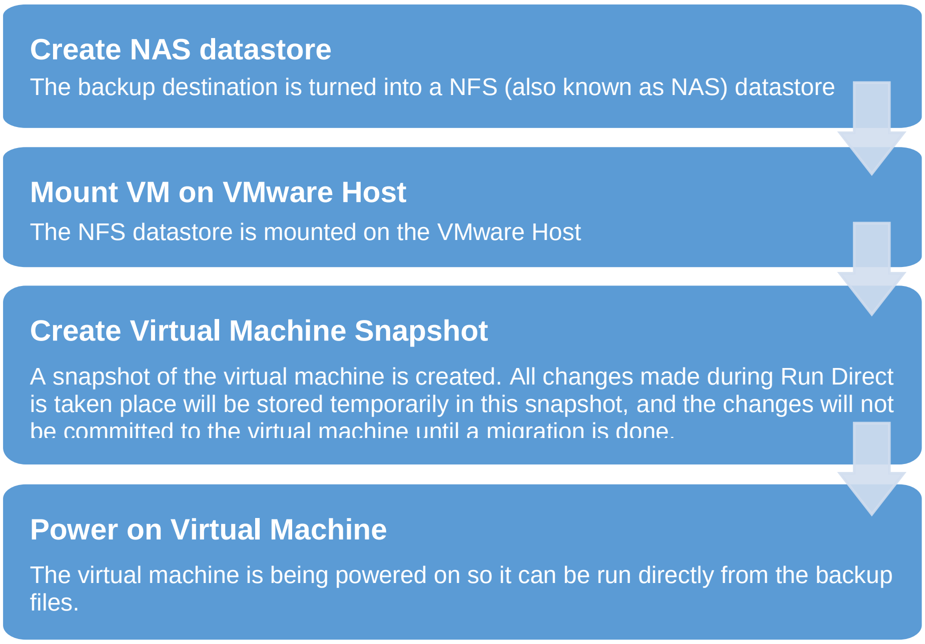
Local-1 (G:\VMware-RunDirect-Sore)

✓ Restore Completed Successfully

Elapsed time 2 min 4 sec

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

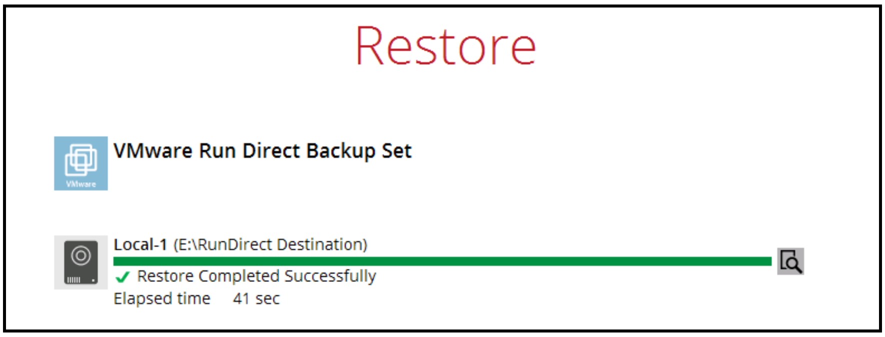
A snapshot of the virtual machine is created. All changes made during Run Direct is taken place will be stored temporarily in this snapshot, and the changes will not be committed to the virtual machine until a migration is done.

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.



Restore

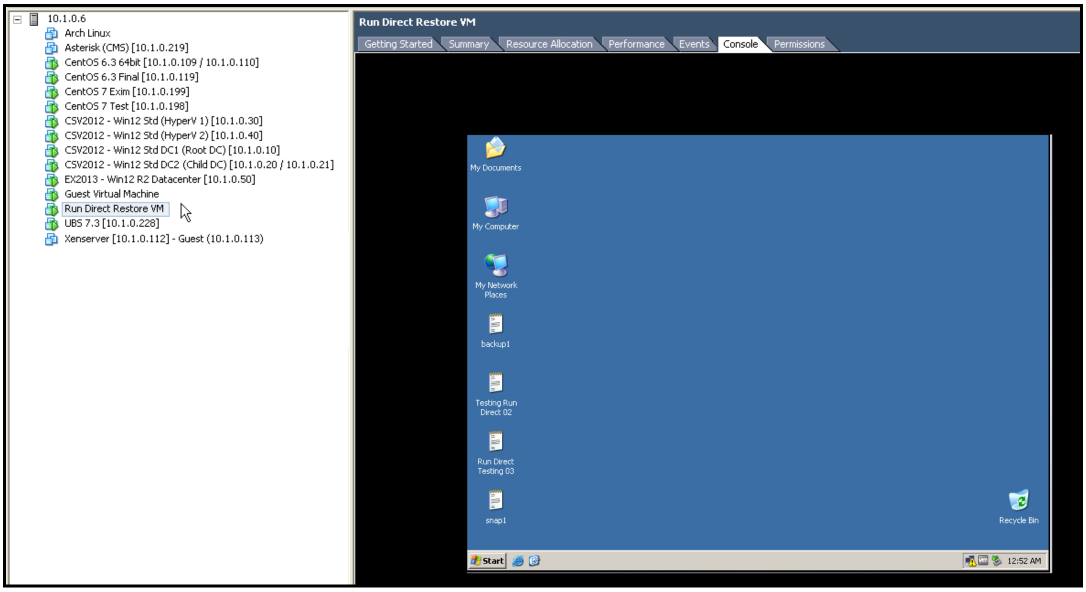
VMware Run Direct Backup Set

Local-1 (E:\RunDirect Destination)

✓ Restore Completed Successfully

Elapsed time 41 sec

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


10.1.0.6
Arch Linux
Asterisk (CMS) [10.1.0.219]
CentOS 6.3 64bit [10.1.0.109 / 10.1.0.110]
CentOS 6.3 Final [10.1.0.119]
CentOS 7 Exim [10.1.0.199]
CentOS 7 Test [10.1.0.198]
CSV2012 - Win12 Std (HyperV 1) [10.1.0.30]
CSV2012 - Win12 Std (HyperV 2) [10.1.0.40]
CSV2012 - Win12 Std DC1 (Root DC) [10.1.0.10]
CSV2012 - Win12 Std DC2 (Child DC) [10.1.0.20 / 10.1.0.21]
EX2013 - Win12 R2 Datacenter [10.1.0.50]
Guest Virtual Machine
Run Direct Restore VM
UBS 7.3 [10.1.0.228]
Xenserver [10.1.0.112] - Guest (10.1.0.113)
Run Direct Restore VM
Getting Started
Summary
Resource Allocation
Performance
Events
Console
Permissions
My Documents
My Computer
My Network Places
backup1
Testing Run Direct 02
Run Direct Testing 03
snap1
Recycle Bin
Start
12:52 AM

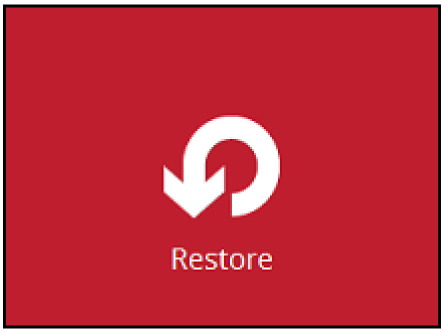
Notes

- Do not exit from the AhsayOBM application when a Run Direct restored VM is still running. Run Direct must be stopped (e.g. by finalizing recovery of the VM or stopping the VM) before exiting AhsayOBM.
- When the restored VM is starting up, there may be an error screen prompted to alert you that Windows was not shut down properly. This message shows as a result of the VM’s runtime status not being backed up. You may simply select to start up Windows as normal to proceed with the startup.

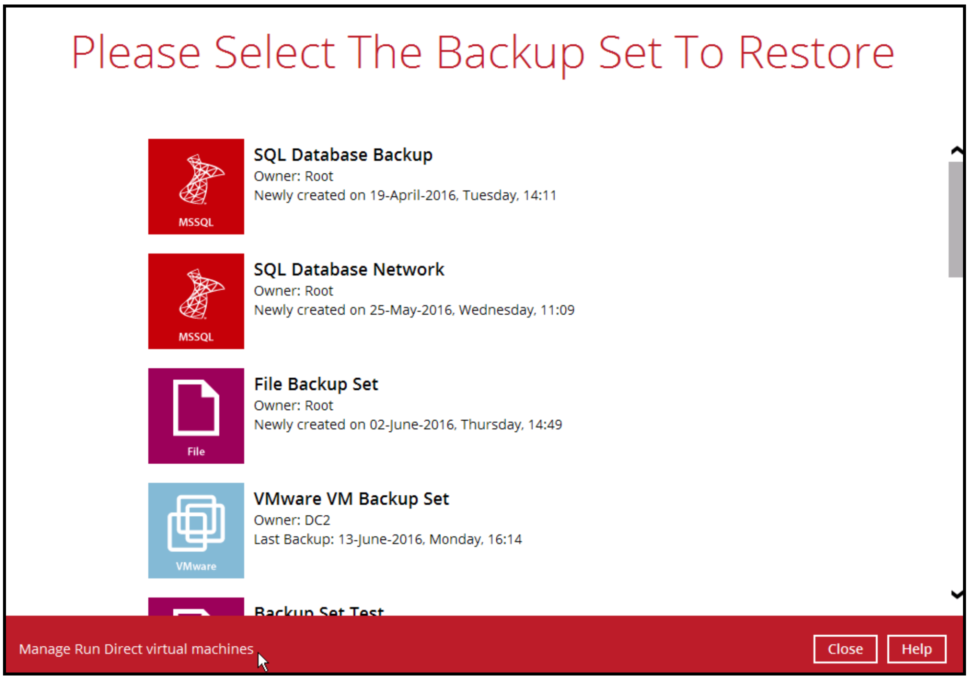
Manage Run Direct VM

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

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



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



Please Select The Backup Set To Restore

SQL Database Backup
Owner: Root
Newly created on 19-April-2016, Tuesday, 14:11

SQL Database Network
Owner: Root
Newly created on 25-May-2016, Wednesday, 11:09

File Backup Set
Owner: Root
Newly created on 02-June-2016, Thursday, 14:49

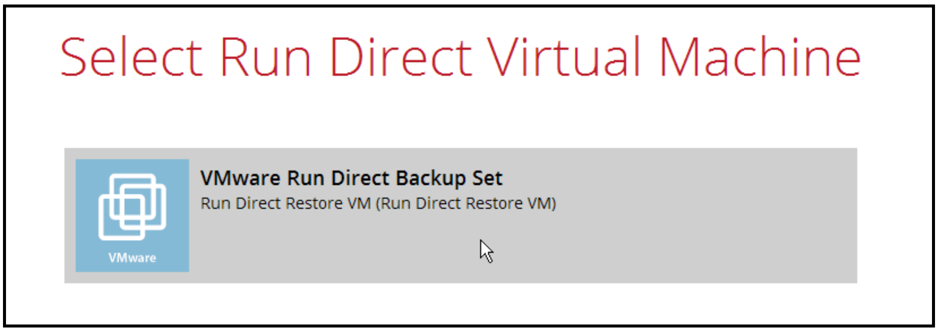
VMware VM Backup Set
Owner: DC2
Last Backup: 13-June-2016, Monday, 16:14

Backup Set Test

Finalize VM Restore

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

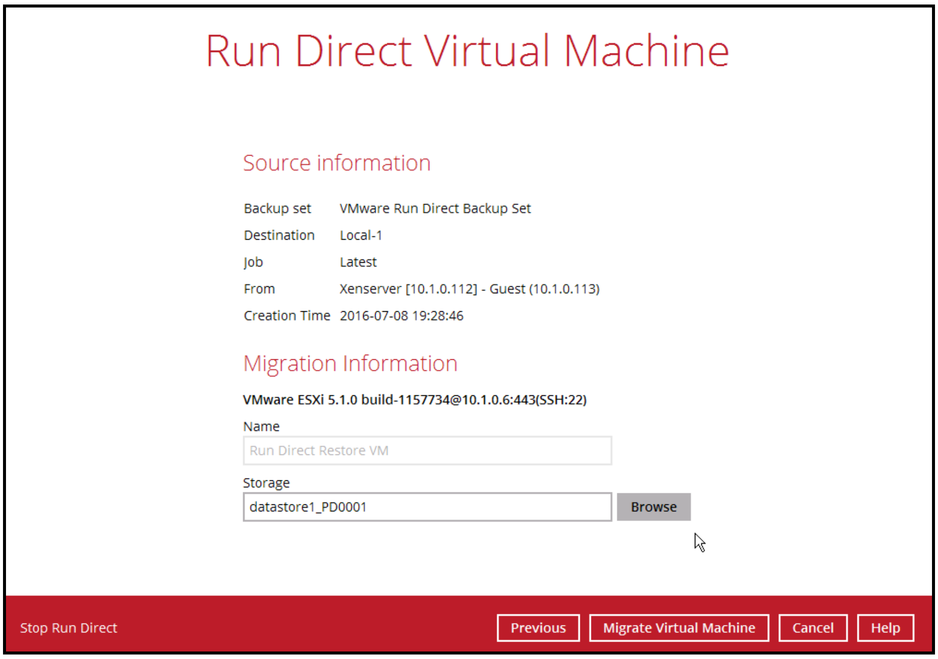
1. Select the backup set which contains the Run Direct VM that you would like to finalize.



Select Run Direct Virtual Machine

VMware Run Direct Backup Set
Run Direct Restore VM (Run Direct Restore VM)

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



Run Direct Virtual Machine

Source information

Backup set VMware Run Direct Backup Set
Destination Local-1
Job Latest
From Xenserver [10.1.0.112] - Guest (10.1.0.113)
Creation Time 2016-07-08 19:28:46

Migration Information

VMware ESXi 5.1.0 build-1157734@10.1.0.6:443(SSH:22)

Name
Run Direct Restore VM

Storage
datastore1_PD0001

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

Note

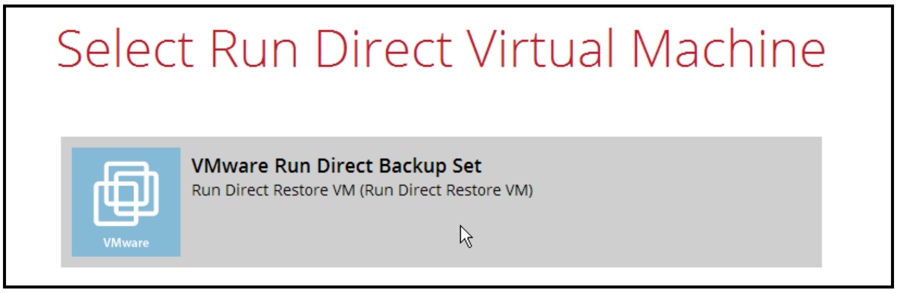
For VM on ESXi host, the VM may be suspended temporarily during the migration process. The downtime of the VM should be minimal.

Stop Run Direct VM

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

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

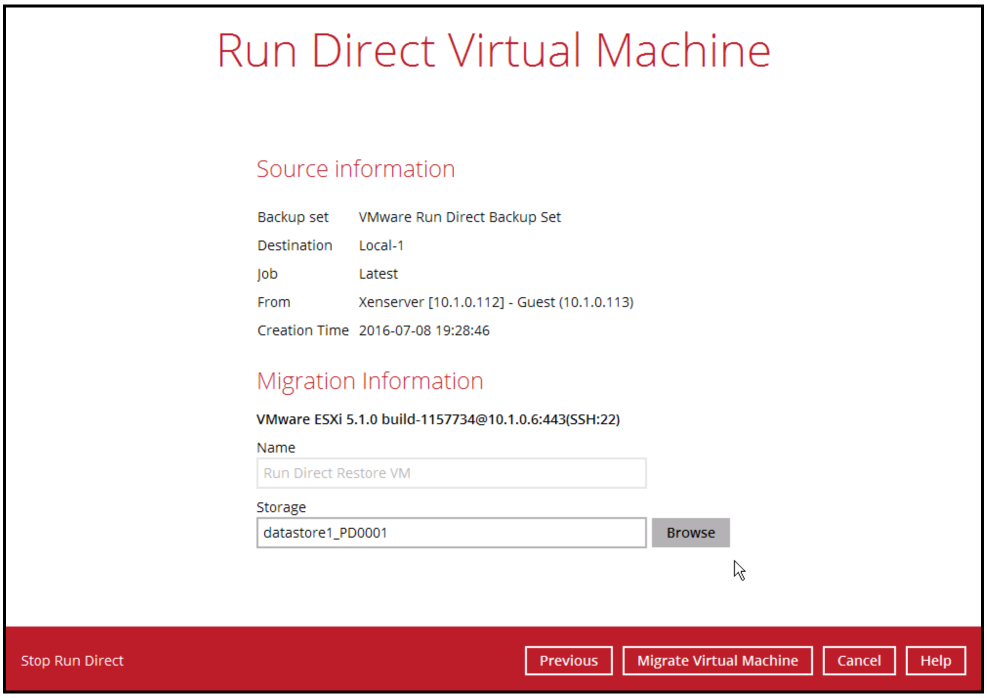
Alternatively, select the backup set which contains the VM that you would like to stop.



Select Run Direct Virtual Machine

VMware Run Direct Backup Set
Run Direct Restore VM (Run Direct Restore VM)

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



Run Direct Virtual Machine

Source information

Backup set VMware Run Direct Backup Set
Destination Local-1
Job Latest
From Xenserver [10.1.0.112] - Guest (10.1.0.113)
Creation Time 2016-07-08 19:28:46

Migration Information

VMware ESXi 5.1.0 build-1157734@10.1.0.6:443(SSH:22)

Name
Run Direct Restore VM

Storage
datastore1_PD0001

Run Direct Restore via User Web Console

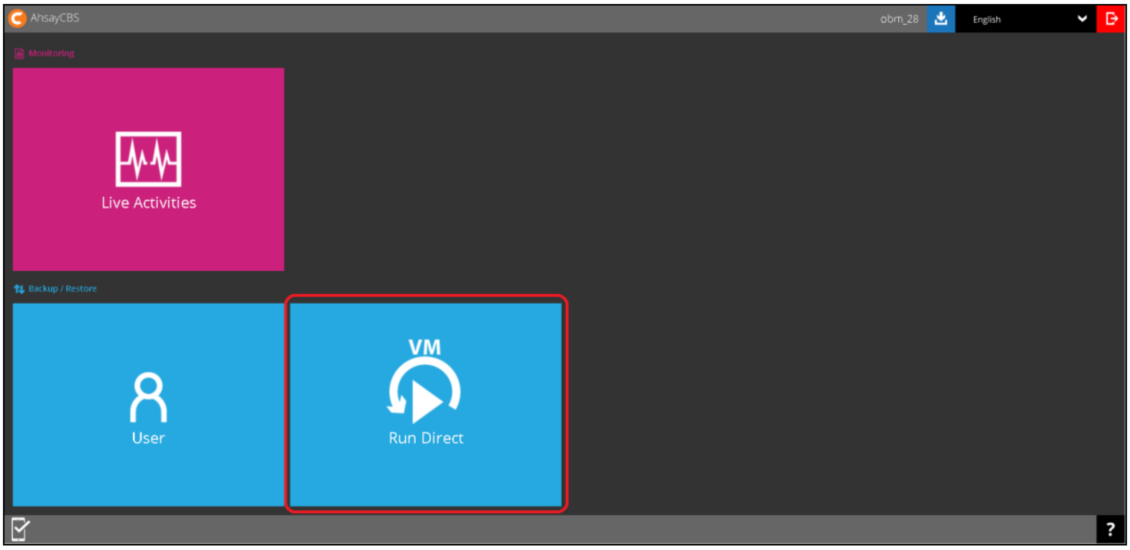
Besides using the AhsayOBM, you can now utilize the AhsayCBS User Web Console to initiate a run direct restore (also known as Agentless Restore) which is supported since AhsayCBS version 7.9.0.0.

Why using the User Web Console?

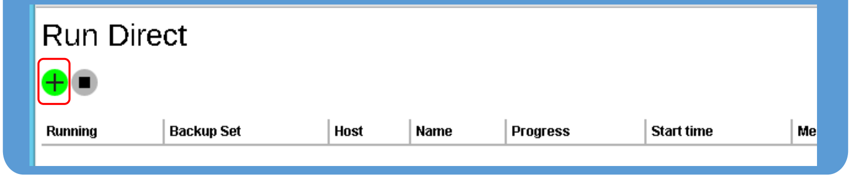
Unlike starting a Run Direct restore on AhsayOBM which you have to be physically with the client backup agent, you can now access the User Web Console to perform the same action as long as you have Internet connection and a web browser.

How to do it?

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



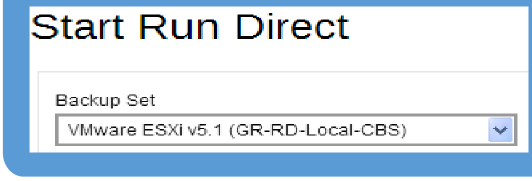
Start a Run Direct Session



Run Direct

Running	Backup Set	Host	Name	Progress	Start time	Me

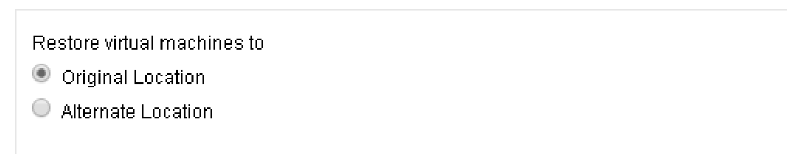
Select the Backup Set



Start Run Direct

Backup Set: VMware ESXi v5.1 (GR-RD-Local-CBS)

Select Restore Destination

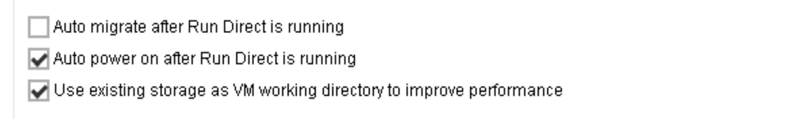


Restore virtual machines to

● Original Location

○ Alternate Location

Configure the Run Direct Options

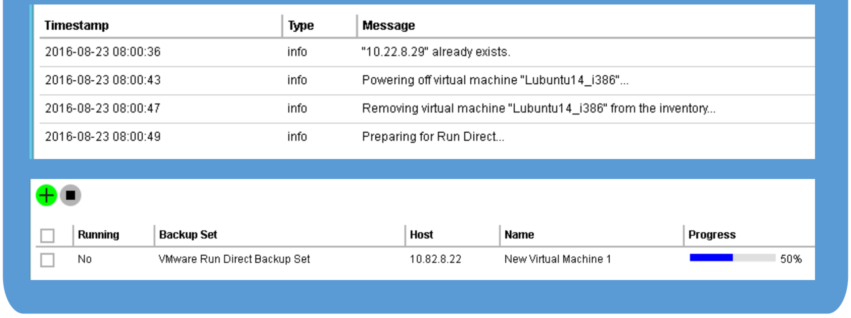


□ Auto migrate after Run Direct is running

☑ Auto power on after Run Direct is running

☑ Use existing storage as VM working directory to improve performance

Run Direct Begins with Status Display



Timestamp	Type	Message
2016-08-23 08:00:36	info	"10.22.8.29" already exists.
2016-08-23 08:00:43	info	Powering off virtual machine "Lubuntu14_i386"...
2016-08-23 08:00:47	info	Removing virtual machine "Lubuntu14_i386" from the inventory...
2016-08-23 08:00:49	info	Preparing for Run Direct...

⊕ ■

□	Running	Backup Set	Host	Name	Progress
□	No	VMware Run Direct Backup Set	10.82.8.22	New Virtual Machine 1	50%

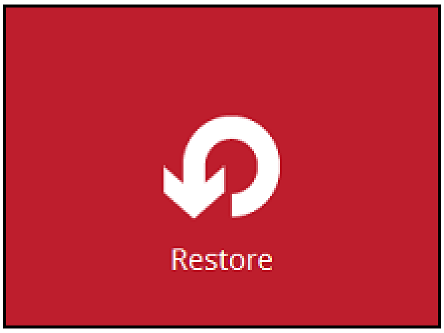
12 Method 2 - Restoring a Virtual Machine without Run Direct

Login to AhsayOBM

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

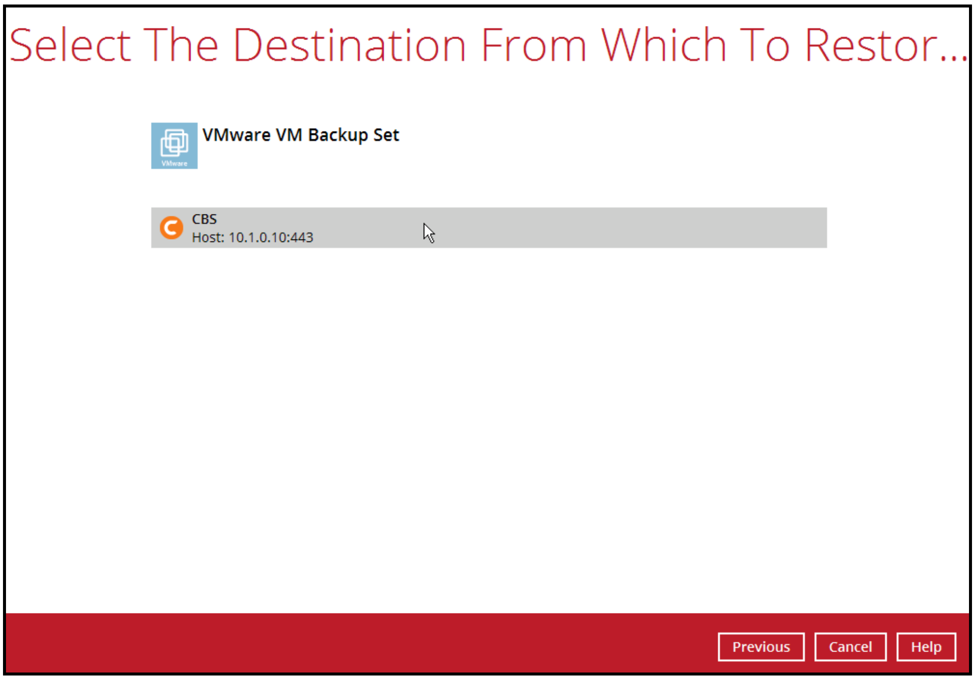
VM Restore without Run Direct

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



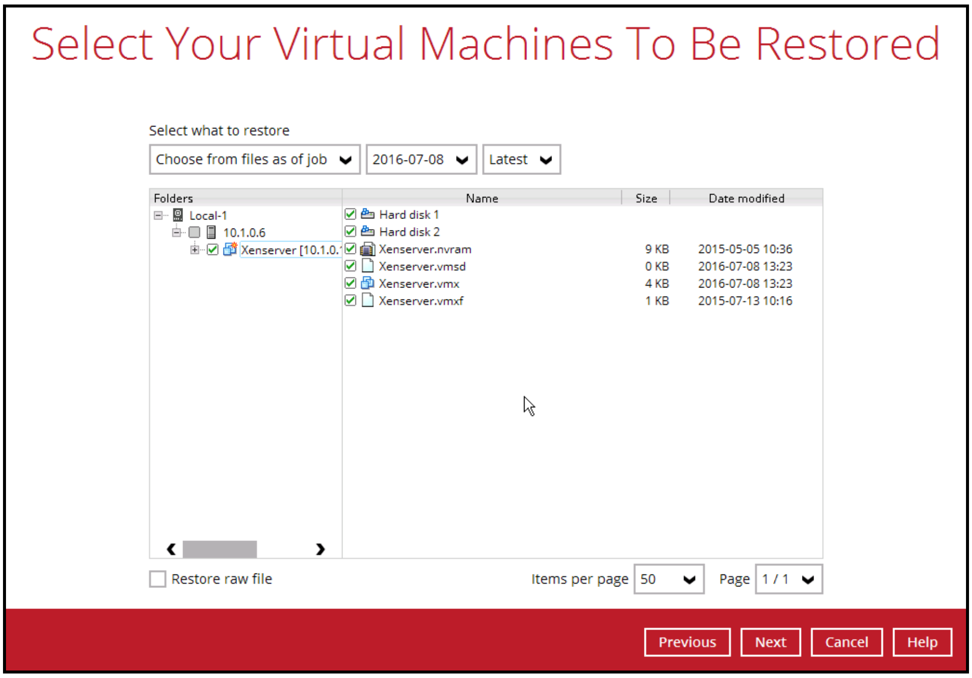
2. Select the backup set that you would like to restore the VM from.

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



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

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



Select Your Virtual Machines To Be Restored

Select what to restore

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

Folders

- Local-1
  - 10.1.0.6
    - ☑ Xenserver [10.1.0.1

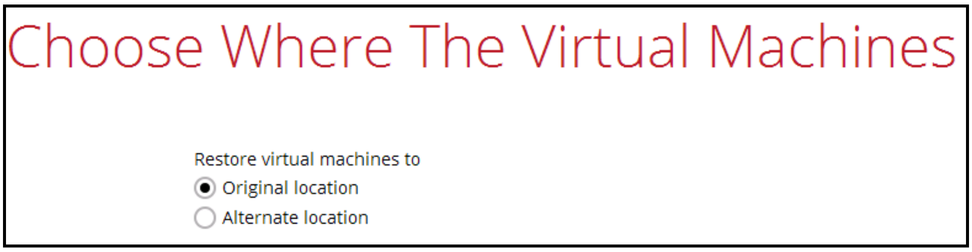
Name	Size	Date modified
☑ Hard disk 1		
☑ Hard disk 2		
☑ Xenserver.nvram	9 KB	2015-05-05 10:36
☑ Xenserver.vmsd	0 KB	2016-07-08 13:23
☑ Xenserver.vmx	4 KB	2016-07-08 13:23
☑ Xenserver.vmxf	1 KB	2015-07-13 10:16

□ Restore raw file

Items per page 50

Page 1 / 1

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



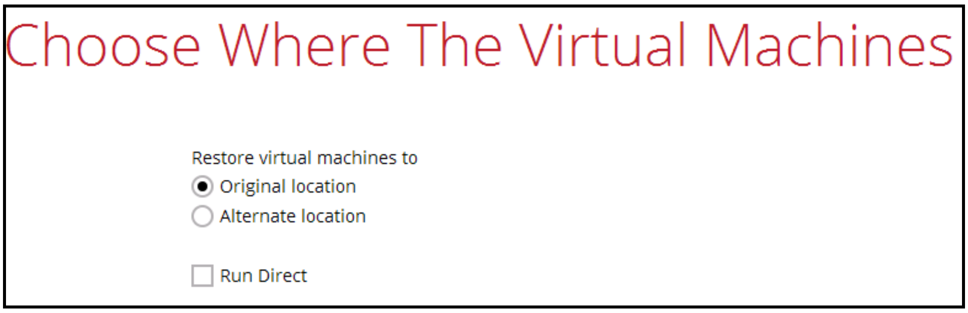
Choose Where The Virtual Machines

Restore virtual machines to

● Original location

○ Alternate location

7. Disable **Run Direct**.



Choose Where The Virtual Machines

Restore virtual machines to

● Original location

○ Alternate location

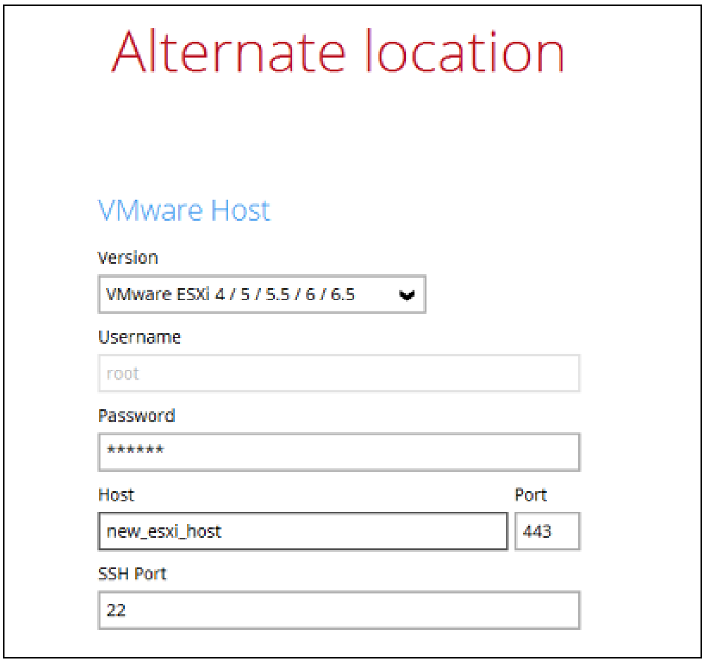
□ Run Direct

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 4 / 5 / 5.5 / 6**, **6.5**, then enter the **Password** of the root account, **Host**, **Port** and **SSH Port** of the new / original host.



Alternate location

VMware Host

Version: VMware ESXi 4 / 5 / 5.5 / 6 / 6.5

Username: root

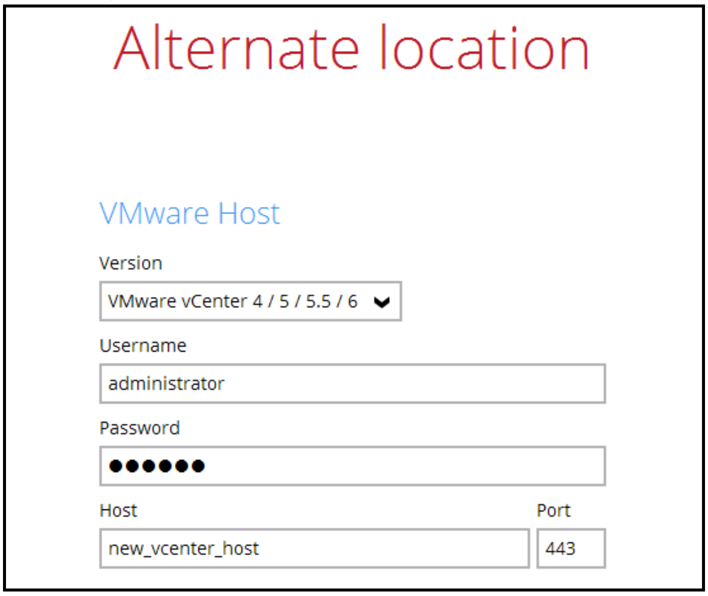
Password: ******

Host: new_esxi_host

Port: 443

SSH Port: 22

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



Alternate location

VMware Host

Version: VMware vCenter 4 / 5 / 5.5 / 6

Username: administrator

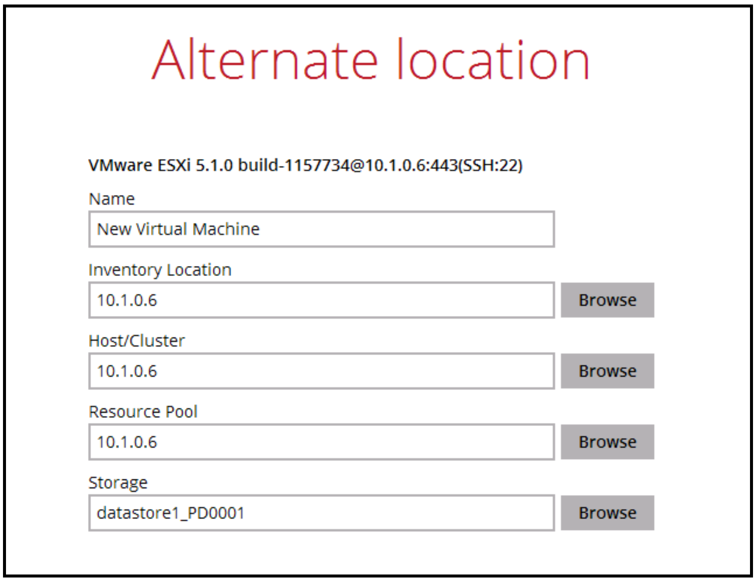
Password: ●●●●●●

Host: new_vcenter_host

Port: 443

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

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



Alternate location

VMware ESXi 5.1.0 build-1157734@10.1.0.6:443(SSH:22)

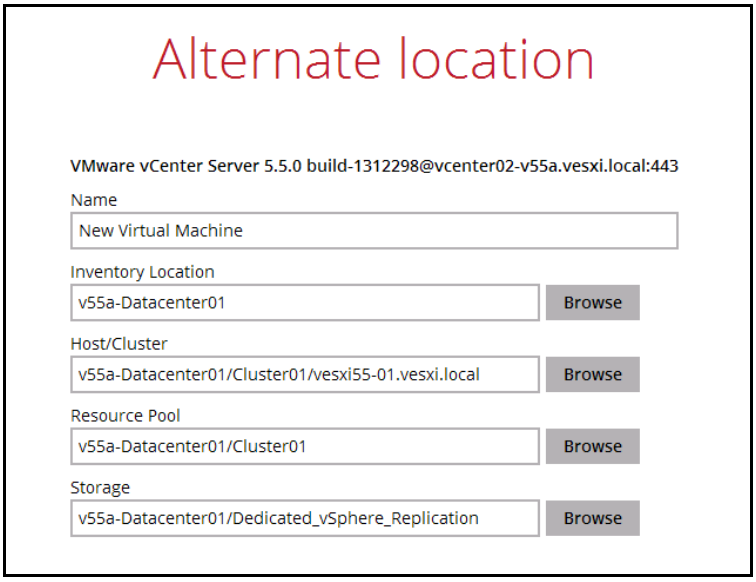
Name: New Virtual Machine

Inventory Location: 10.1.0.6

Host/Cluster: 10.1.0.6

Resource Pool: 10.1.0.6

Storage: datastore1_PD0001



Alternate location

VMware vCenter Server 5.5.0 build-1312298@vcenter02-v55a.vesxi.local:443

Name: New Virtual Machine

Inventory Location: v55a-Datacenter01

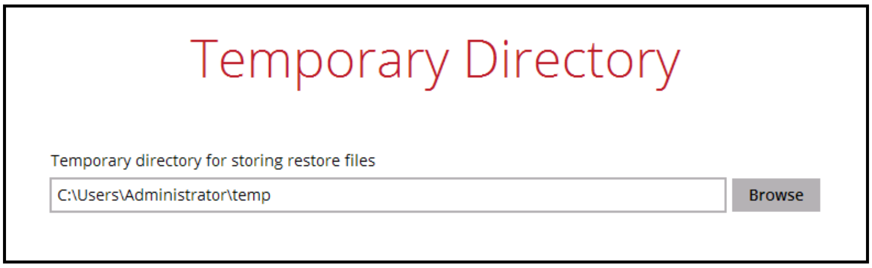
Host/Cluster: v55a-Datacenter01/Cluster01/vesxi55-01.vesxi.local

Resource Pool: v55a-Datacenter01/Cluster01

Storage: v55a-Datacenter01/Dedicated_vSphere_Replication

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

10. Select the temporary directory for storing temporary files.

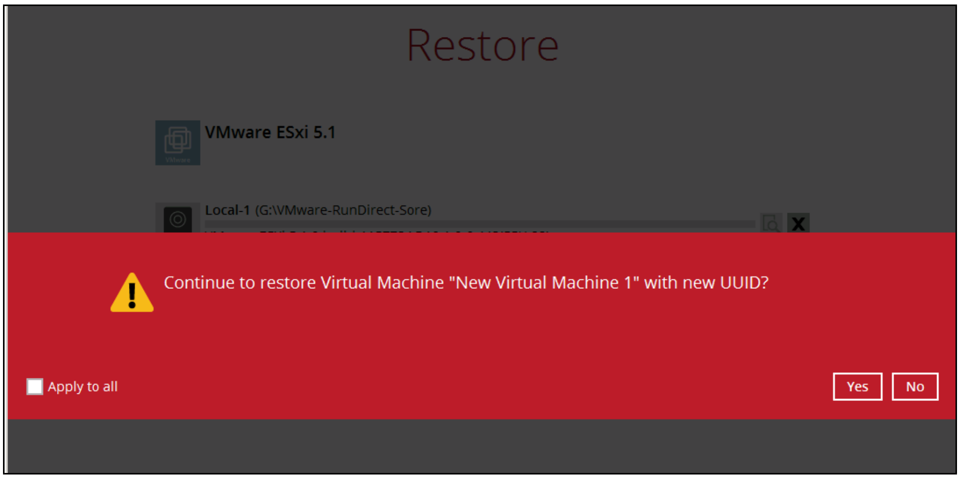


Temporary Directory

Temporary directory for storing restore files: C:\Users\Administrator\temp

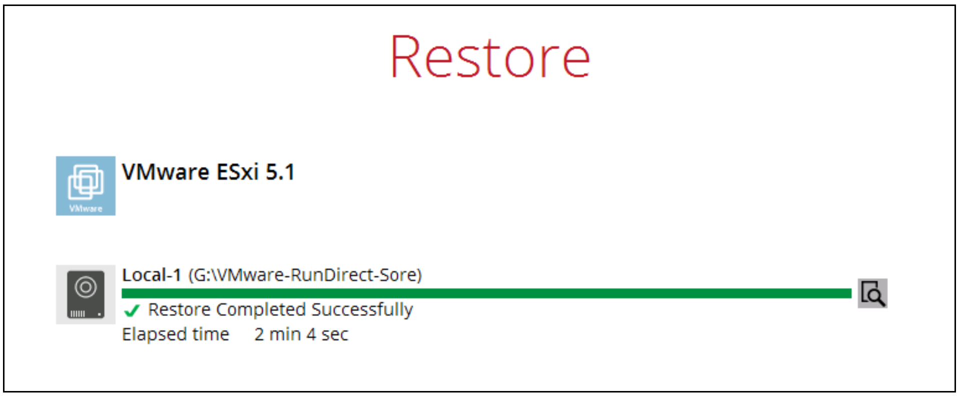
11. When restoring your guest VM to another VMware host, the following message will be prompted. Since each virtual machine is automatically assigned a universally unique identifier (UUID), a new UUID must be created when you restore the guest VM to another host because it is not possible to have two identical UUID running at the same time.

Therefore, make sure you click **Yes** when you see the prompt below.



Continue to restore Virtual Machine "New Virtual Machine 1" with new UUID?

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



✓ Restore Completed Successfully

Elapsed time 2 min 4 sec

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

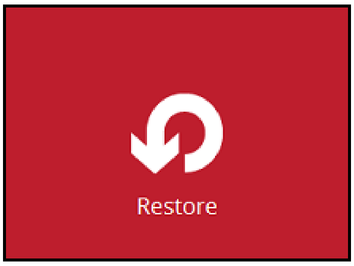
Since AhsayOBM v7.11.0.0, we have introduced a new feature to enable guest VMs that are backed up in VDDK mode to be restored in VMDK raw file format. This feature is useful if you wish to restore the backed up VM to another VMware host (ESXi server) even without using the AhsayOBM.

IMPORTANT

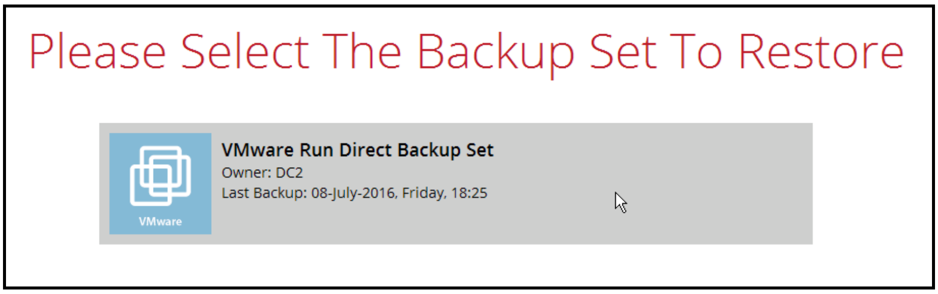
Restoring guest VMs from VDDK to VMDK format only supports backup sets that are created in AhsayOBM v7.9.0.0 or later version. Backup sets created with AhsayOBM before v7.9.0.0, or VMware VDDK backup sets migrated from v6 are **NOT** supported.

Follow the steps below for details.

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



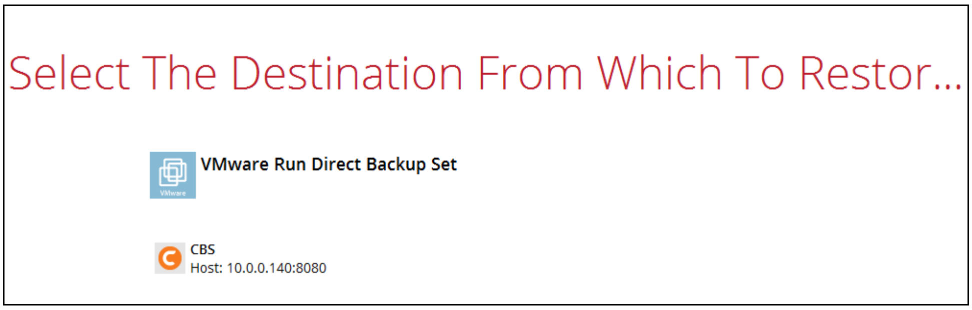
2. Select the backup set that you would like to restore the VM from.



Please Select The Backup Set To Restore

VMware Run Direct Backup Set
Owner: DC2
Last Backup: 08-July-2016, Friday, 18:25

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



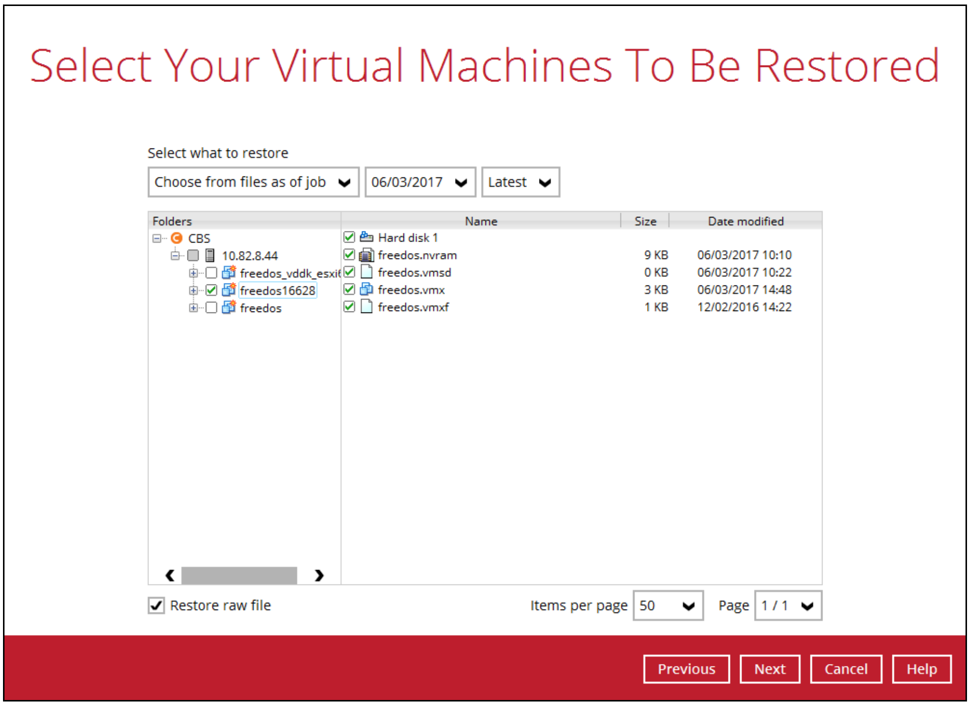
Select The Destination From Which To Restor...

VMware Run Direct Backup Set

CBS
Host: 10.0.0.140:8080

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.



Select Your Virtual Machines To Be Restored

Select what to restore

Choose from files as of job | 06/03/2017 | Latest

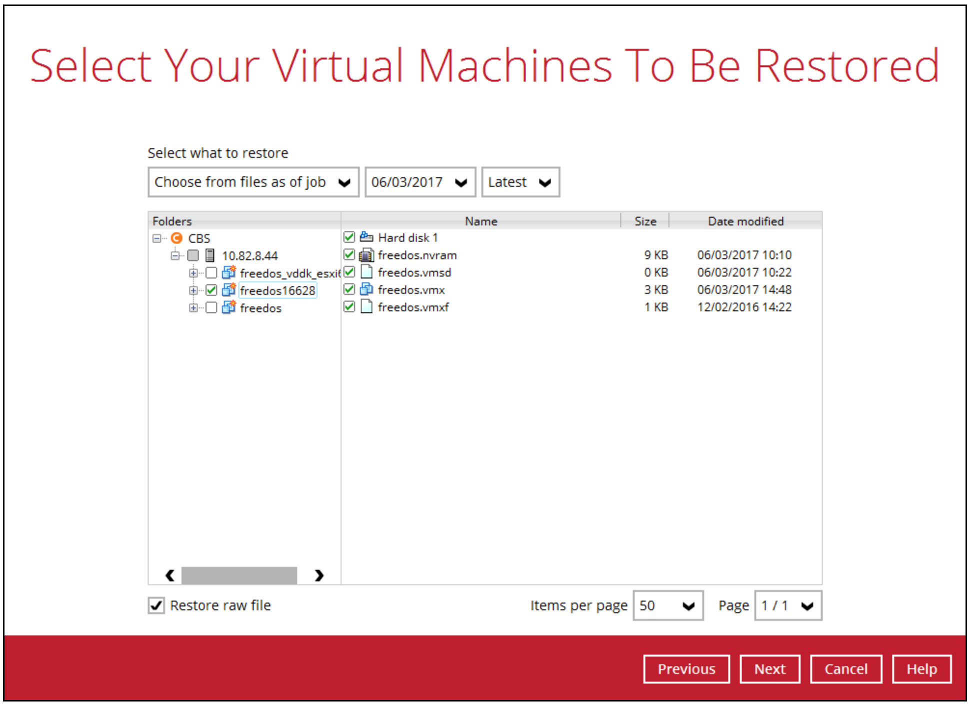
Folders:
- CBS
  - 10.82.8.44
    - □ freedos_vddk_esxi
    - ☑ freedos16628
    - □ freedos

Name	Size	Date modified
☑ Hard disk 1		
☑ freedos.nvram	9 KB	06/03/2017 10:10
☑ freedos.vmsd	0 KB	06/03/2017 10:22
☑ freedos.vmx	3 KB	06/03/2017 14:48
☑ freedos.vmxf	1 KB	12/02/2016 14:22

☑ Restore raw file

Items per page 50 Page 1 / 1

6. 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.



Select Your Virtual Machines To Be Restored

Select what to restore

Choose from files as of job | 06/03/2017 | Latest

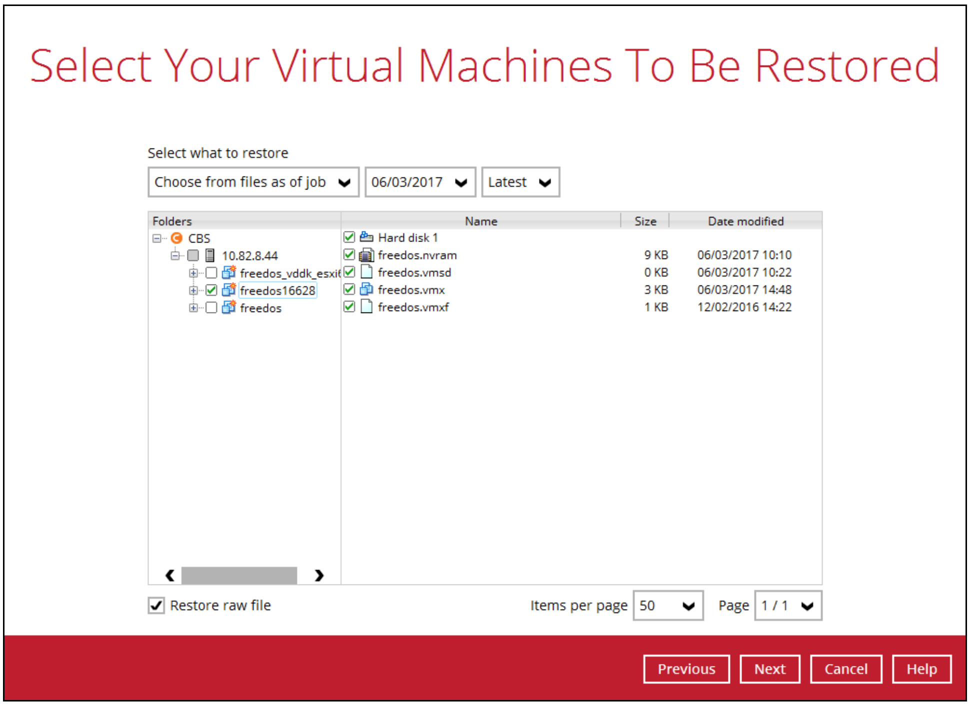
Folders:
- CBS
  - 10.82.8.44
    - □ freedos_vddk_esxi
    - ☑ freedos16628
    - □ freedos

Name	Size	Date modified
☑ Hard disk 1		
☑ freedos.nvram	9 KB	06/03/2017 10:10
☑ freedos.vmsd	0 KB	06/03/2017 10:22
☑ freedos.vmx	3 KB	06/03/2017 14:48
☑ freedos.vmxf	1 KB	12/02/2016 14:22

☑ Restore raw file

Items per page 50 Page 1 / 1

7. 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.



Select Your Virtual Machines To Be Restored

Select what to restore

Choose from files as of job | 06/03/2017 | Latest

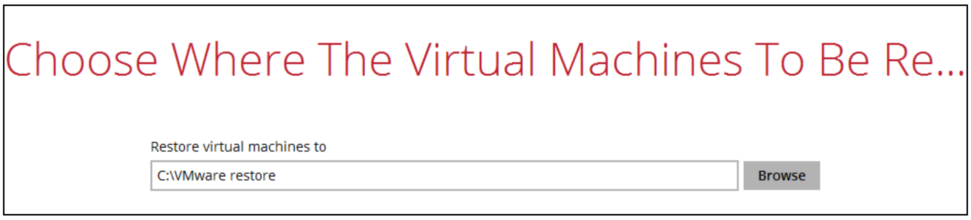
Folders
- CBS
  - 10.82.8.44
    - □ freedos_vddk_esxi6
    - ☑ freedos16628
    - □ freedos

Name	Size	Date modified
☑ Hard disk 1		
☑ freedos.nvram	9 KB	06/03/2017 10:10
☑ freedos.vmsd	0 KB	06/03/2017 10:22
☑ freedos.vmx	3 KB	06/03/2017 14:48
☑ freedos.vmxf	1 KB	12/02/2016 14:22

☑ Restore raw file

Items per page 50 Page 1 / 1

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

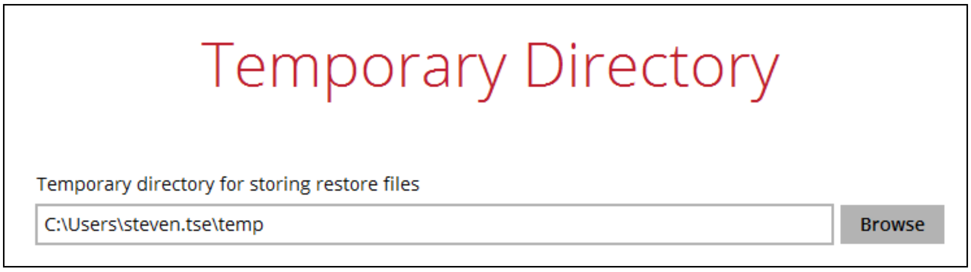


Choose Where The Virtual Machines To Be Re...

Restore virtual machines to

C:\VMware restore

9. Select a temporary directory for storing restore files.



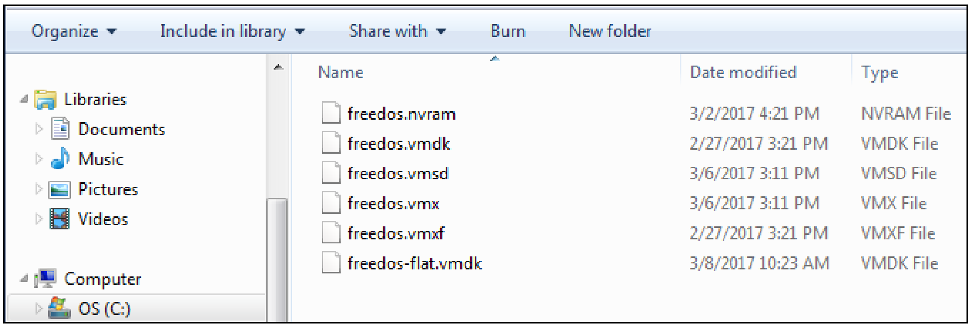
Temporary Directory

Temporary directory for storing restore files

C:\Users\steven.tse\temp

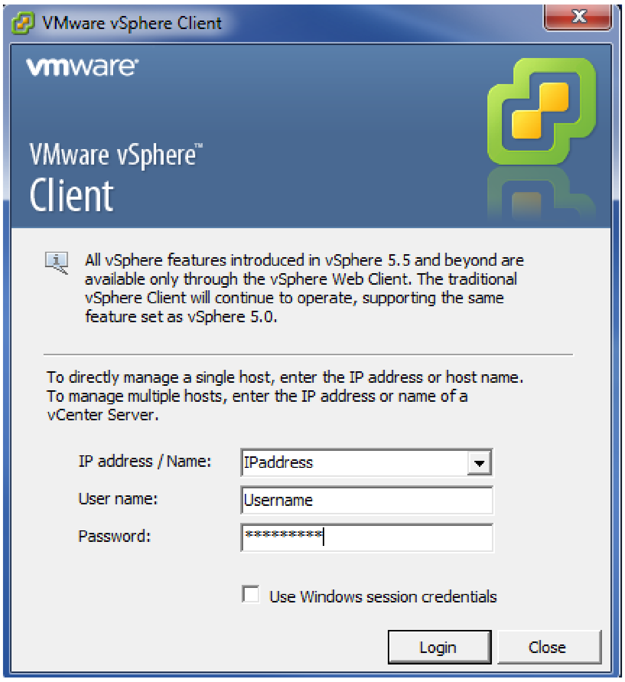
10. Click **Restore** to start the VM restore.

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



Name	Date modified	Type
freedos.nvram	3/2/2017 4:21 PM	NVRAM File
freedos.vmdk	2/27/2017 3:21 PM	VMDK File
freedos.vmsd	3/6/2017 3:11 PM	VMSD File
freedos.vmx	3/6/2017 3:11 PM	VMX File
freedos.vmxf	2/27/2017 3:21 PM	VMXF File
freedos-flat.vmdk	3/8/2017 10:23 AM	VMDK File

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



All vSphere features introduced in vSphere 5.5 and beyond are available only through the vSphere Web Client. The traditional vSphere Client will continue to operate, supporting the same feature set as vSphere 5.0.

To directly manage a single host, enter the IP address or host name. To manage multiple hosts, enter the IP address or name of a vCenter Server.

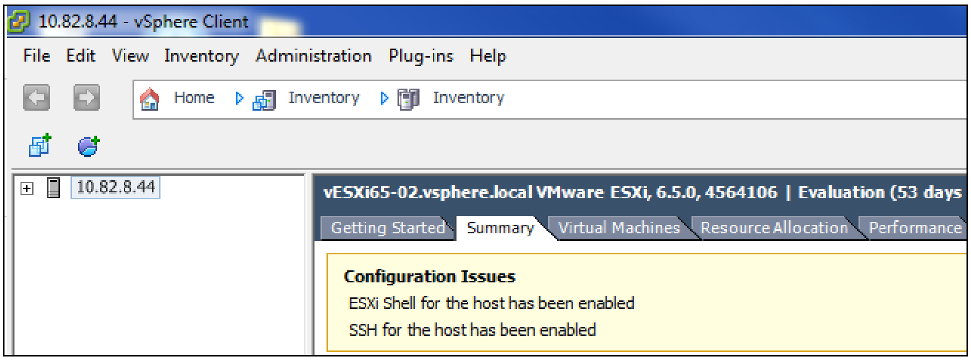
IP address / Name: IPaddress

User name: Username

Password: **********

□ Use Windows session credentials

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



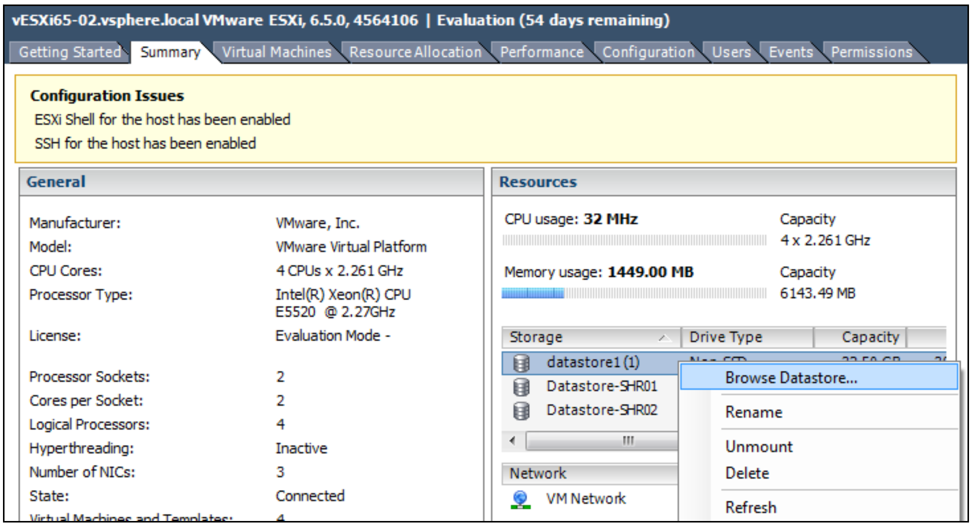
vESXi65-02.vsphere.local VMware ESXi, 6.5.0, 4564106 | Evaluation (53 days

Configuration Issues

ESXi Shell for the host has been enabled

SSH for the host has been enabled

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


vESXi65-02.vsphere.local VMware ESXi, 6.5.0, 4564106 | Evaluation (54 days remaining)

Configuration Issues
ESXi Shell for the host has been enabled
SSH for the host has been enabled

General

Manufacturer: VMware, Inc.
Model: VMware Virtual Platform
CPU Cores: 4 CPUs x 2.261 GHz
Processor Type: Intel(R) Xeon(R) CPU E5520 @ 2.27GHz
License: Evaluation Mode -
Processor Sockets: 2
Cores per Socket: 2
Logical Processors: 4
Hyperthreading: Inactive
Number of NICs: 3
State: Connected
Virtual Machines and Templates: 4

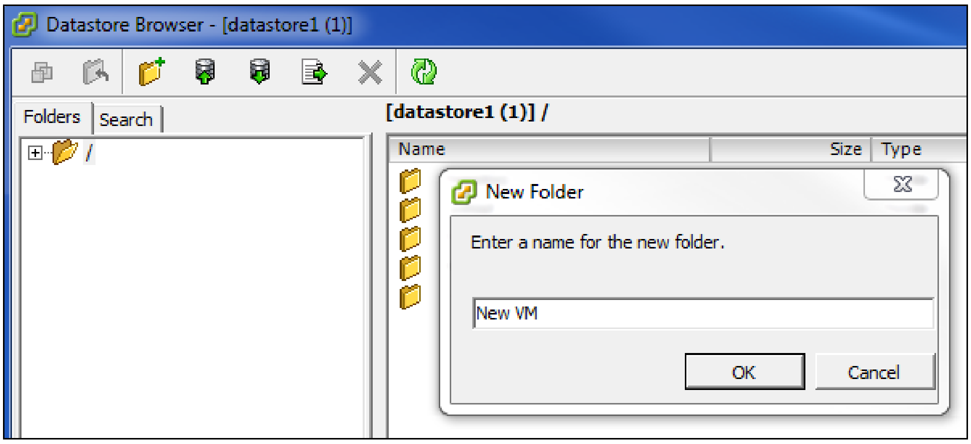
Resources

CPU usage: 32 MHz Capacity 4 x 2.261 GHz
Memory usage: 1449.00 MB Capacity 6143.49 MB

Storage	Drive Type	Capacity
datastore1 (1)		
Datastore-SHR01		
Datastore-SHR02		

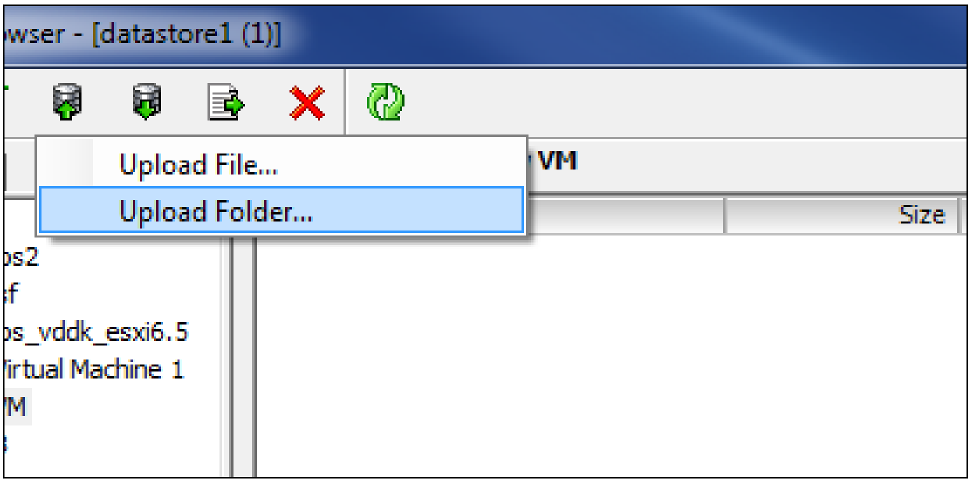
Network
VM Network

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

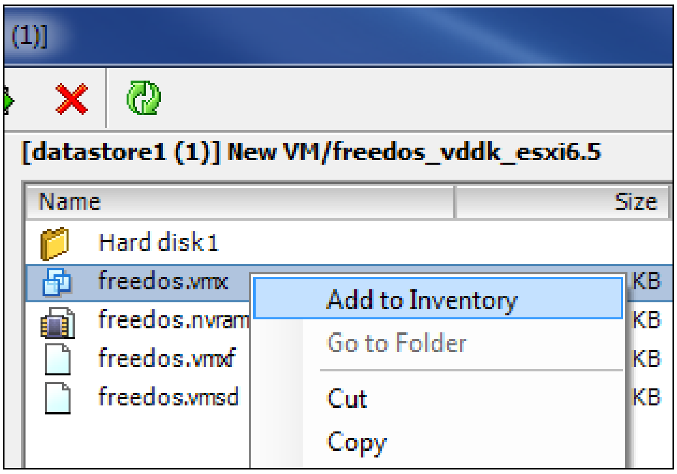

Datastore Browser - [datastore1 (1)]

New Folder
Enter a name for the new folder.
New VM

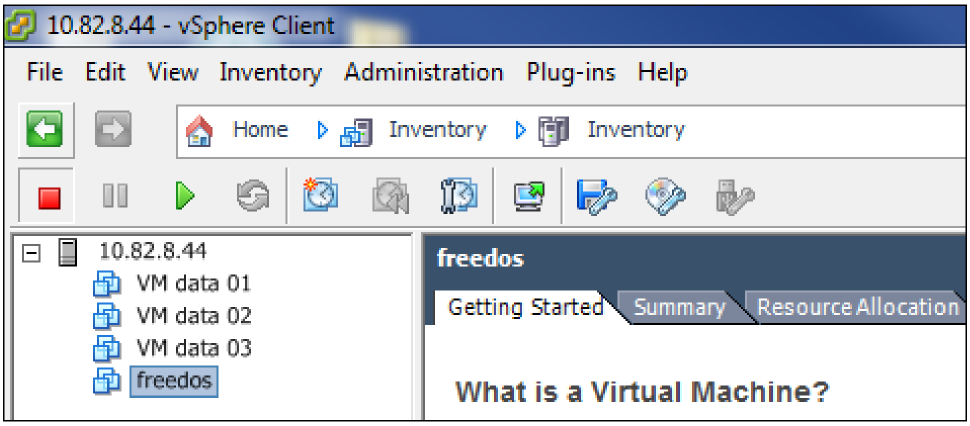
16. Open the newly created folder then click the Upload Folder option at the top menu bar to select the VM you wish to restore.


wser - [datastore1 (1)]

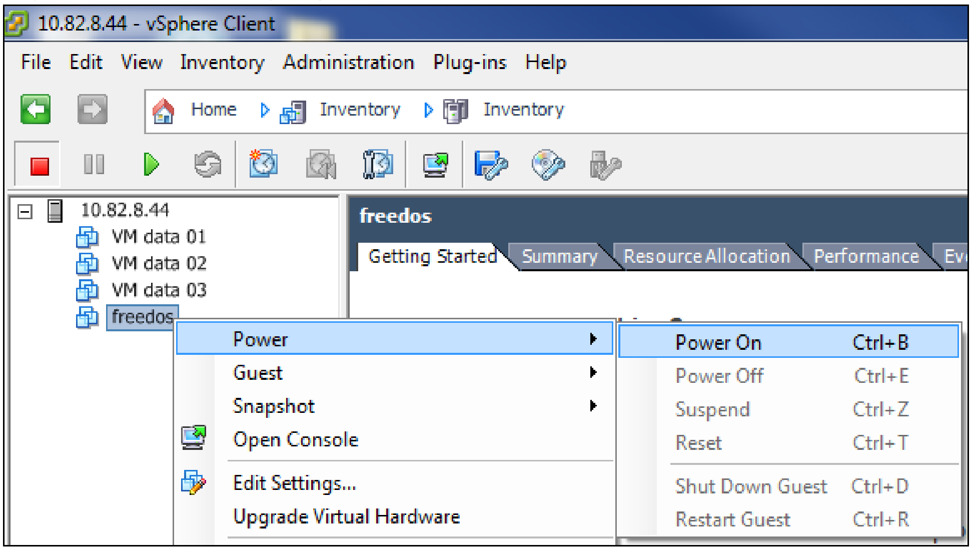
17. Open the folder you have just uploaded, then right click on the .vmx file and click on **Add to Inventory**.



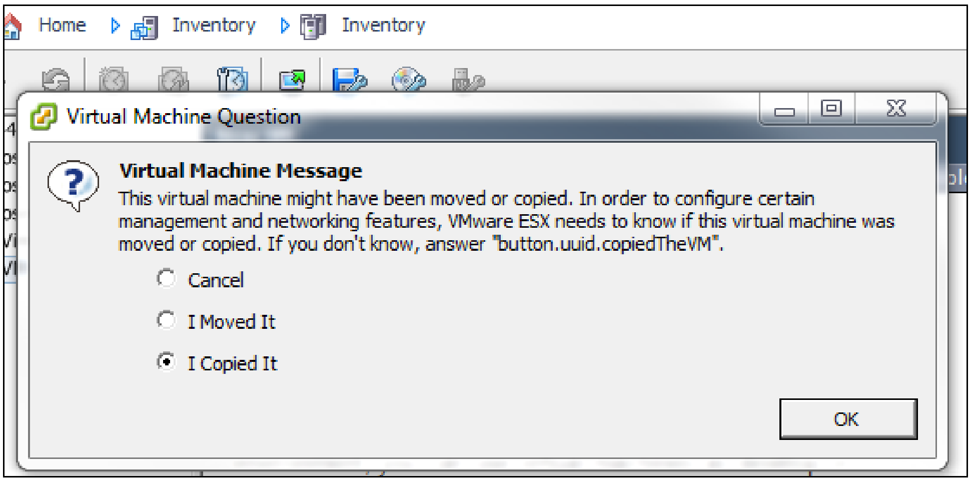
18. Follow the screen prompts and name the imported VM and confirm the resource pool. You should see the imported VM display on the left on the main page of vSphere if the VM has been successfully imported to the ESXi server.



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



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



Virtual Machine Message

This virtual machine might have been moved or copied. In order to configure certain management and networking features, VMware ESX needs to know if this virtual machine was moved or copied. If you don't know, answer "button.uuid.copiedTheVM".

○ Cancel

○ I Moved It

● I Copied It

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.

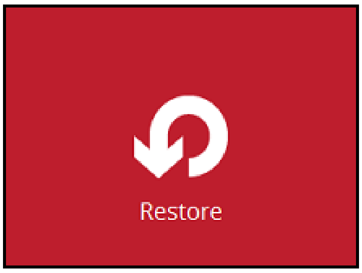
- Microsoft Visual C++ 2015 Redistributable (x86) / (x64)
  https://www.microsoft.com/en-us/download/details.aspx?id=48145
- Update for Universal C Runtime in Windows
  https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows
- Microsoft Security Advisory 3033929 (for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

Requirements and Limitations

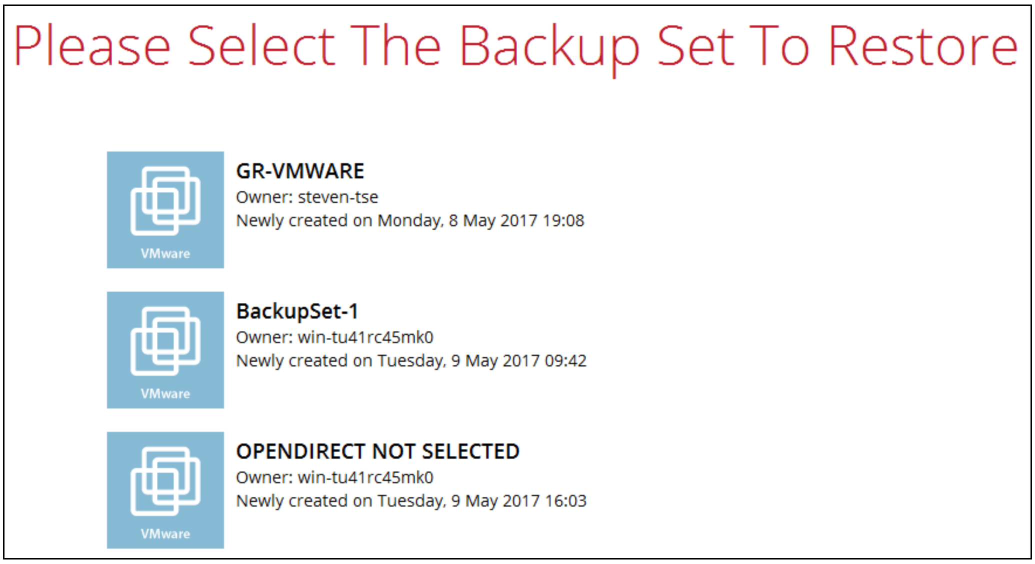
1. Granular restore does not support the mounting of virtual disks, if the disk itself is encrypted, for example using Windows Bitlocker or other third party security features.
2. If any folders or files on a virtual disk are encrypted, these files/folder cannot be supported with Granular Restore. For 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 than can be mounted on the guest VM, however, only files/ folders from one virtual disk can be retrieved at a time.
5. Windows User Account Control (UAC) must be disabled to apply granular restore.

Start Granular Restore

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



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



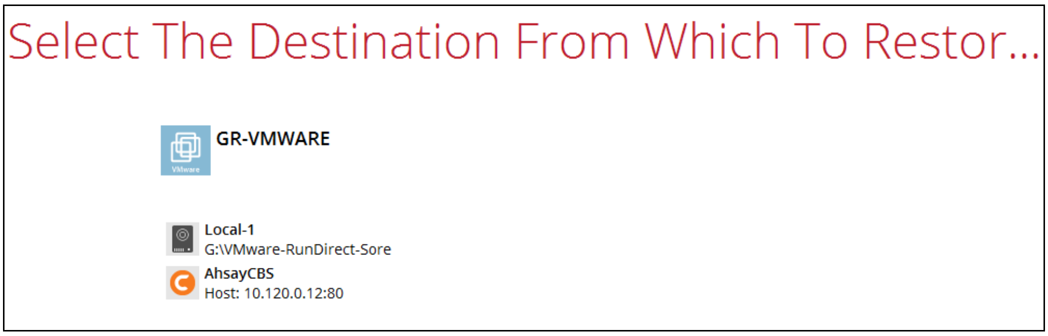
Please Select The Backup Set To Restore

GR-VMWARE
Owner: steven-tse
Newly created on Monday, 8 May 2017 19:08

BackupSet-1
Owner: win-tu41rc45mk0
Newly created on Tuesday, 9 May 2017 09:42

OPENDIRECT NOT SELECTED
Owner: win-tu41rc45mk0
Newly created on Tuesday, 9 May 2017 16:03

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



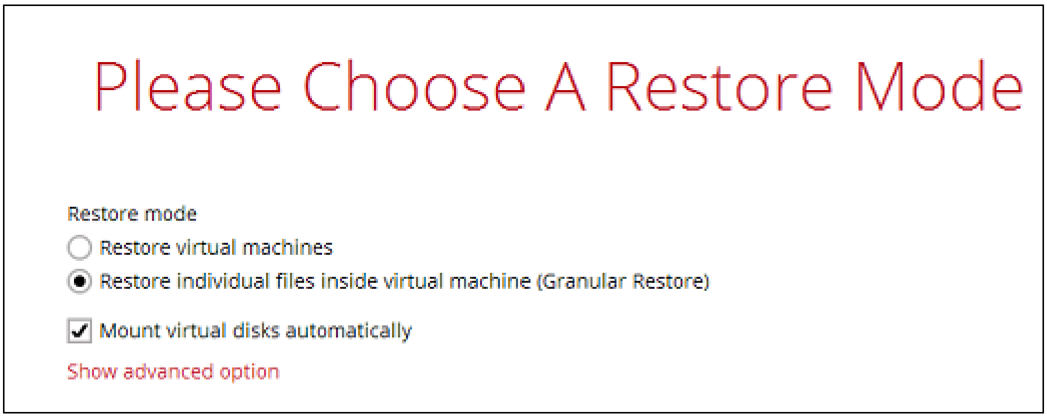
Select The Destination From Which To Restor...

GR-VMWARE

Local-1
G:\VMware-RunDirect-Sore

AhsayCBS
Host: 10.120.0.12:80

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



Please Choose A Restore Mode

Restore mode

○ Restore virtual machines

● Restore individual files inside virtual machine (Granular Restore)

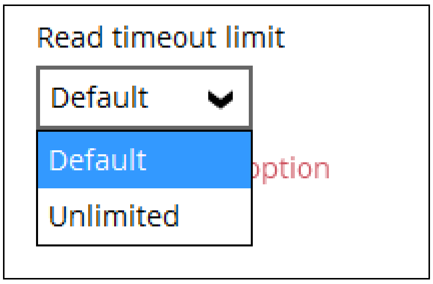
☑ Mount virtual disks automatically

Show advanced option

Note

The **Mount virtual disks automatically option** is selected by default. If the guest VM contains a multiple virtual disks and you only require the restore of files from a single or certain virtual disk(s), 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 time.

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



Read timeout limit

Default

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

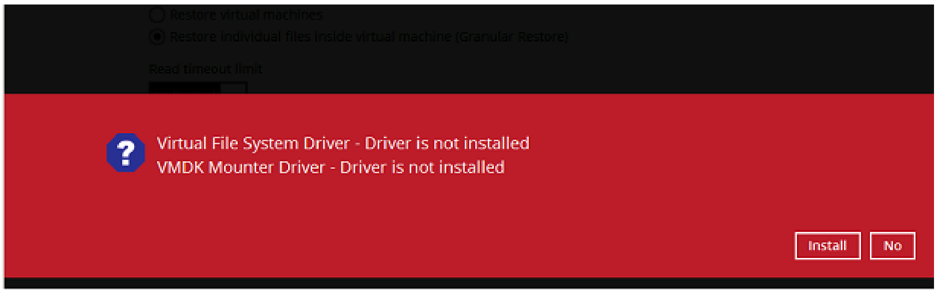
- **Default** – This setting should be suitable for guest VMs located on a local, removable, or network drive. The time out value is 15 seconds.
- **Unlimited** – the connection will not be time out when this is selected. This selection is recommended when:
  - Backup destination is a cloud stroage.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

Note

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

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

5. 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.

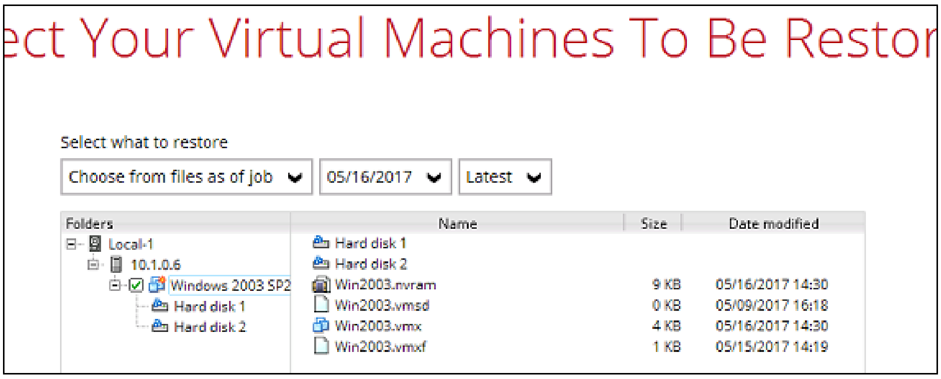


○ Restore virtual machines
● Restore individual files inside virtual machine (Granular Restore)

Read timeout limit

Virtual File System Driver - Driver is not installed
VMDK Mounter Driver - Driver is not installed

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



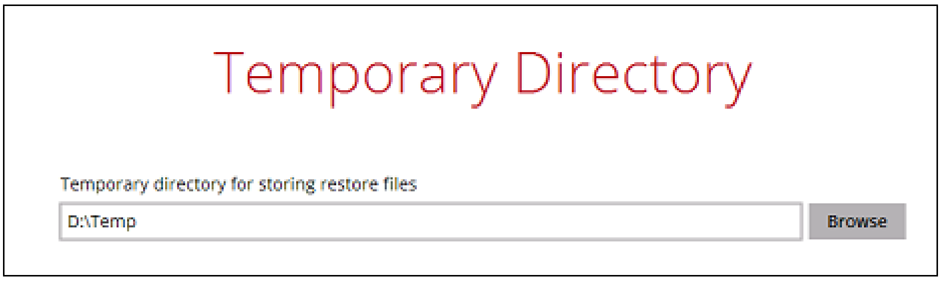
ect Your Virtual Machines To Be Restor

Select what to restore

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

Folders	Name	Size	Date modified
Local-1	Hard disk 1		
10.1.0.6	Hard disk 2		
☑ Windows 2003 SP2	Win2003.nvram	9 KB	05/16/2017 14:30
Hard disk 1	Win2003.vmsd	0 KB	05/09/2017 16:18
Hard disk 2	Win2003.vmx	4 KB	05/16/2017 14:30
	Win2003.vmxf	1 KB	05/15/2017 14:19

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

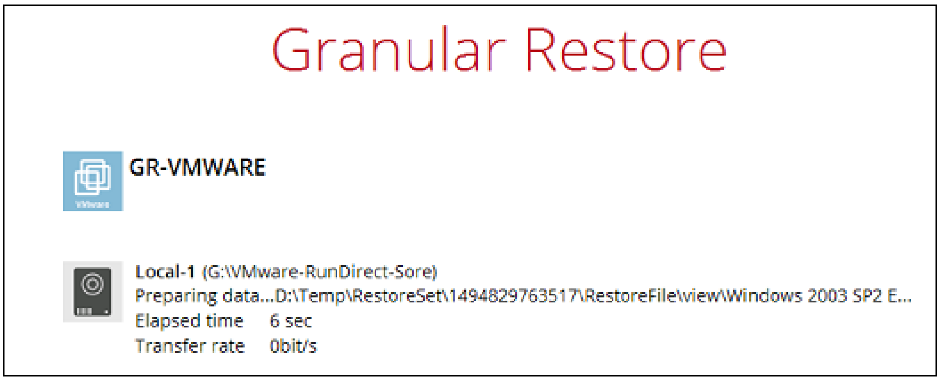


Temporary Directory

Temporary directory for storing restore files

D:\Temp

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.



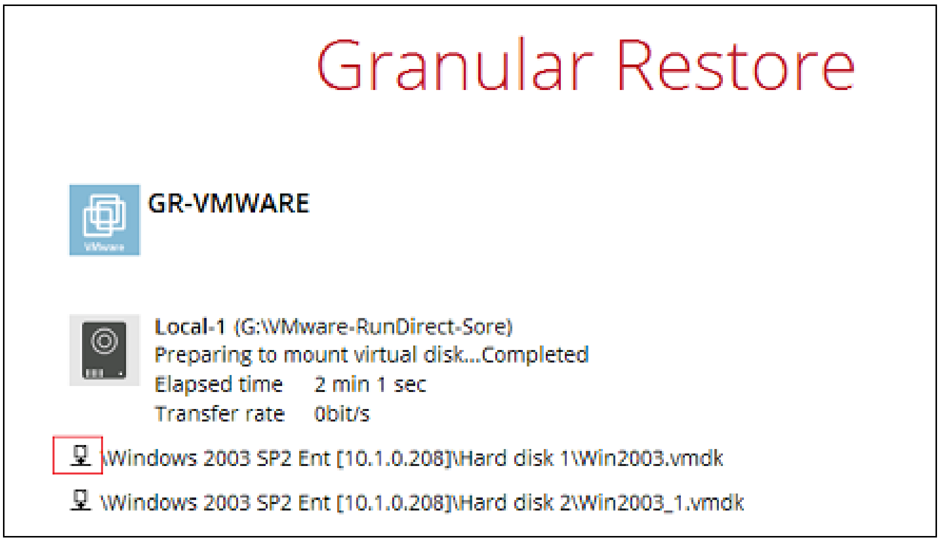
Granular Restore

GR-VMWARE

Local-1 (G:\VMware-RunDirect-Sore)
Preparing data...D:\Temp\RestoreSet\1494829763517\RestoreFile\view\Windows 2003 SP2 E...
Elapsed time 6 sec
Transfer rate 0bit/s

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

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



Granular Restore

GR-VMWARE

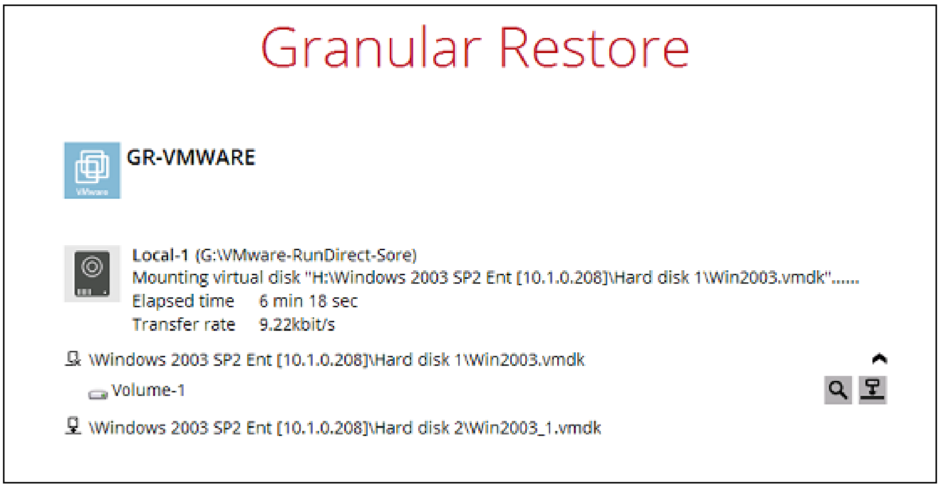
Local-1 (G:\VMware-RunDirect-Sore)
Preparing to mount virtual disk...Completed
Elapsed time 2 min 1 sec
Transfer rate 0bit/s

\Windows 2003 SP2 Ent [10.1.0.208]\Hard disk 1\Win2003.vmdk

\Windows 2003 SP2 Ent [10.1.0.208]\Hard disk 2\Win2003_1.vmdk

Otherwise, all the virtual disks will be automatically mounted.

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



Granular Restore

GR-VMWARE

Local-1 (G:\VMware-RunDirect-Sore)
Mounting virtual disk "H:\Windows 2003 SP2 Ent [10.1.0.208]\Hard disk 1\Win2003.vmdk"......
Elapsed time 6 min 18 sec
Transfer rate 9.22kbit/s

\Windows 2003 SP2 Ent [10.1.0.208]\Hard disk 1\Win2003.vmdk

Volume-1

\Windows 2003 SP2 Ent [10.1.0.208]\Hard disk 2\Win2003_1.vmdk

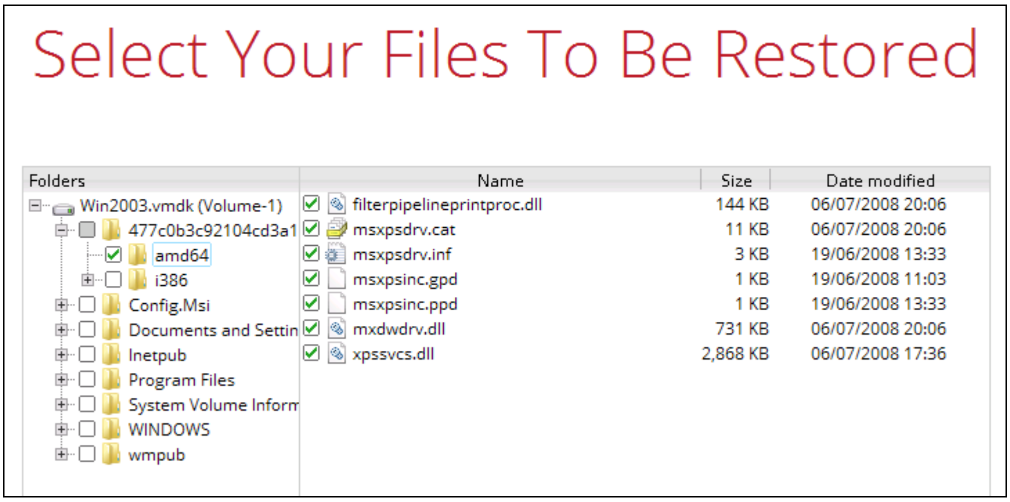
There are two options to restore individual files from here.

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.



Select Your Files To Be Restored

Folders

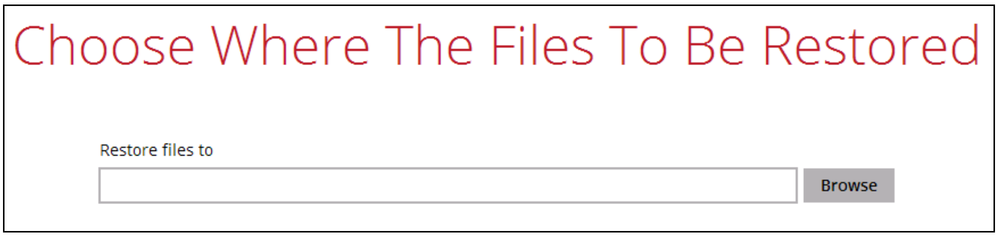
- ⊟ Win2003.vmdk (Volume-1)
  - ⊟ ▣ 477c0b3c92104cd3a1
    - ☑ amd64
    - ⊞ □ i386
  - ⊞ □ Config.Msi
  - ⊞ □ Documents and Settin
  - ⊞ □ Inetpub
  - ⊞ □ Program Files
  - ⊞ □ System Volume Inform
  - ⊞ □ WINDOWS
  - ⊞ □ wmpub

Name	Size	Date modified
☑ filterpipelineprintproc.dll	144 KB	06/07/2008 20:06
☑ msxpsdrv.cat	11 KB	06/07/2008 20:06
☑ msxpsdrv.inf	3 KB	19/06/2008 13:33
☑ msxpsinc.gpd	1 KB	19/06/2008 11:03
☑ msxpsinc.ppd	1 KB	19/06/2008 13:33
☑ mxdwdrv.dll	731 KB	06/07/2008 20:06
☑ xpssvcs.dll	2,868 KB	06/07/2008 17:36

Note

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

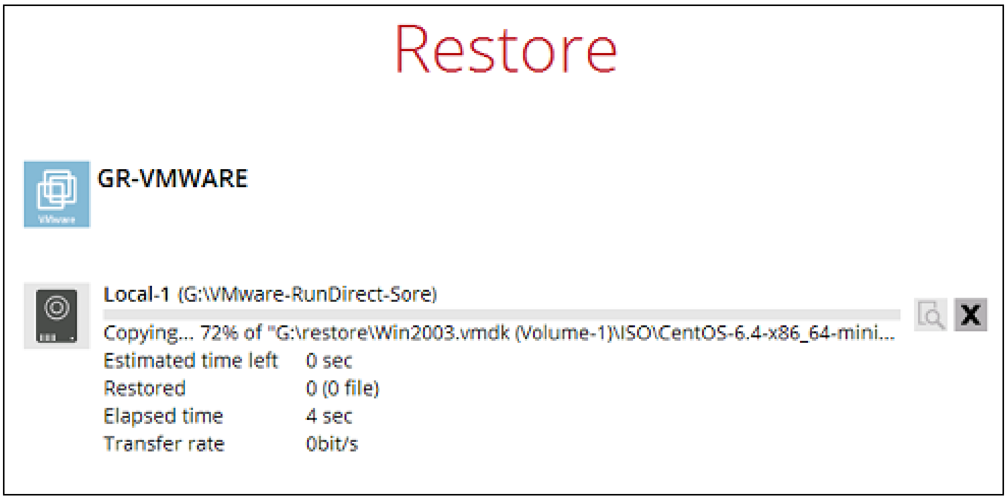
ii. Select a path where you wish the files to be restored to, then click **Restore**.



Choose Where The Files To Be Restored

Restore files to

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



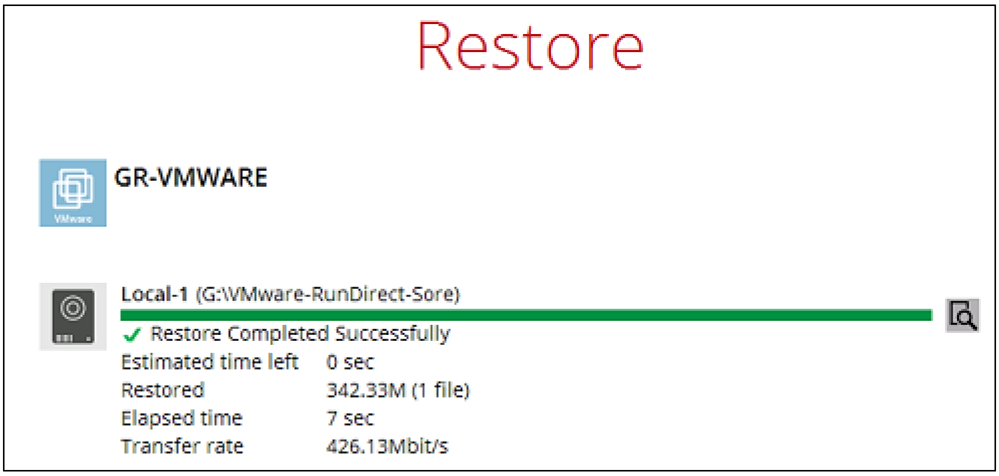
Restore

GR-VMWARE

Local-1 (G:\VMware-RunDirect-Sore)

Copying... 72% of "G:\restore\Win2003.vmdk (Volume-1)\ISO\CentOS-6.4-x86_64-mini...

Estimated time left	0 sec
Restored	0 (0 file)
Elapsed time	4 sec
Transfer rate	0bit/s



Restore

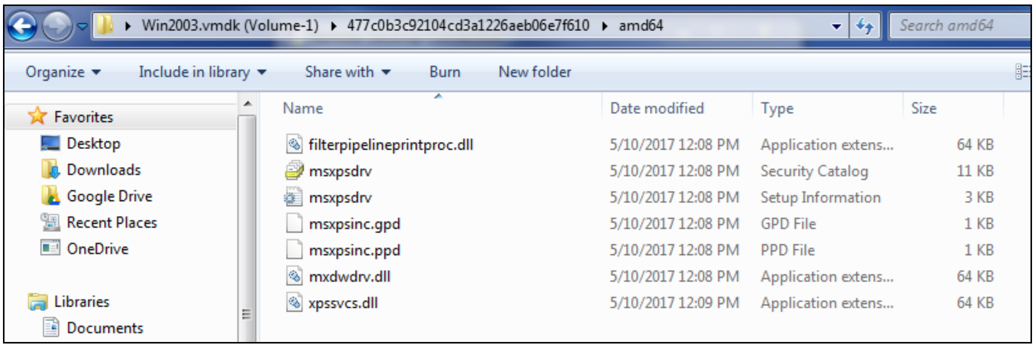
GR-VMWARE

Local-1 (G:\VMware-RunDirect-Sore)

✓ Restore Completed Successfully

Estimated time left	0 sec
Restored	342.33M (1 file)
Elapsed time	7 sec
Transfer rate	426.13Mbit/s

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



Name	Date modified	Type	Size
filterpipelineprintproc.dll	5/10/2017 12:08 PM	Application extens...	64 KB
msxpsdrv	5/10/2017 12:08 PM	Security Catalog	11 KB
msxpsdrv	5/10/2017 12:08 PM	Setup Information	3 KB
msxpsinc.gpd	5/10/2017 12:08 PM	GPD File	1 KB
msxpsinc.ppd	5/10/2017 12:08 PM	PPD File	1 KB
mxdwdrv.dll	5/10/2017 12:08 PM	Application extens...	64 KB
xpssvcs.dll	5/10/2017 12:09 PM	Application extens...	64 KB

Option 2: Restore Using Windows File Explorer

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

Note

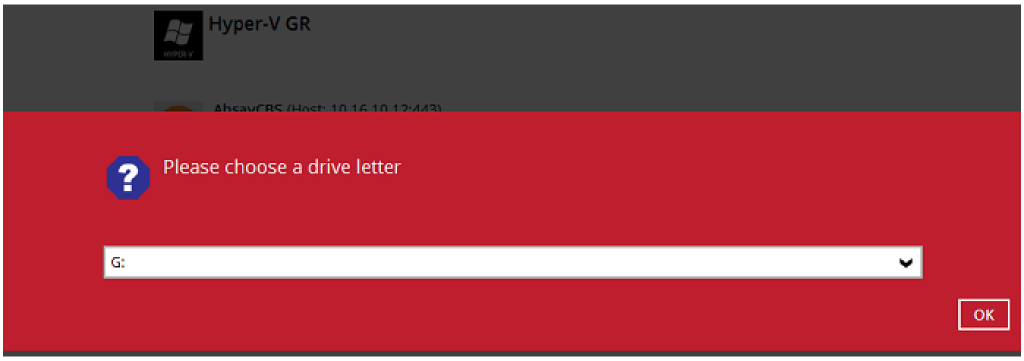
Granular restore of Hyper-V backup sets performed using Windows File Explorer :

1. Will not show up on the [**Restore Status**] tab in **Live Activities** of the backup service provider AhsayCBS.

2. Will not generate restore reports on backup service provider AhsayCBS.

3. Will not generate restore log on AhsayOBM.

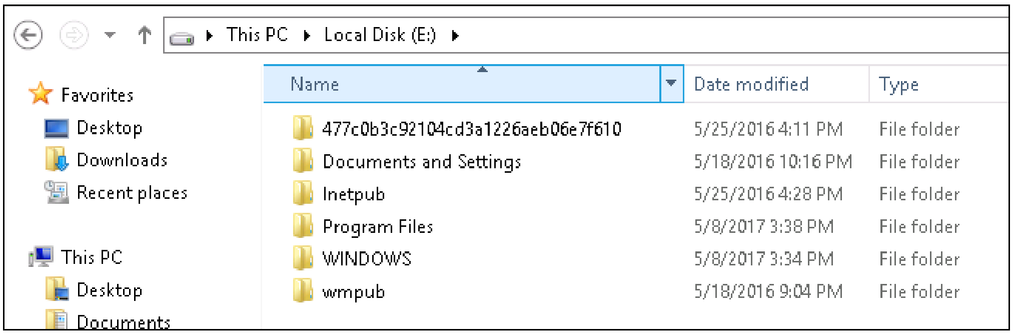
i. Click and then you will be prompted to select a driver letter where you wish the mounted backup image to be mapped on your machine, click **OK** when you have finished selection.



Please choose a drive letter

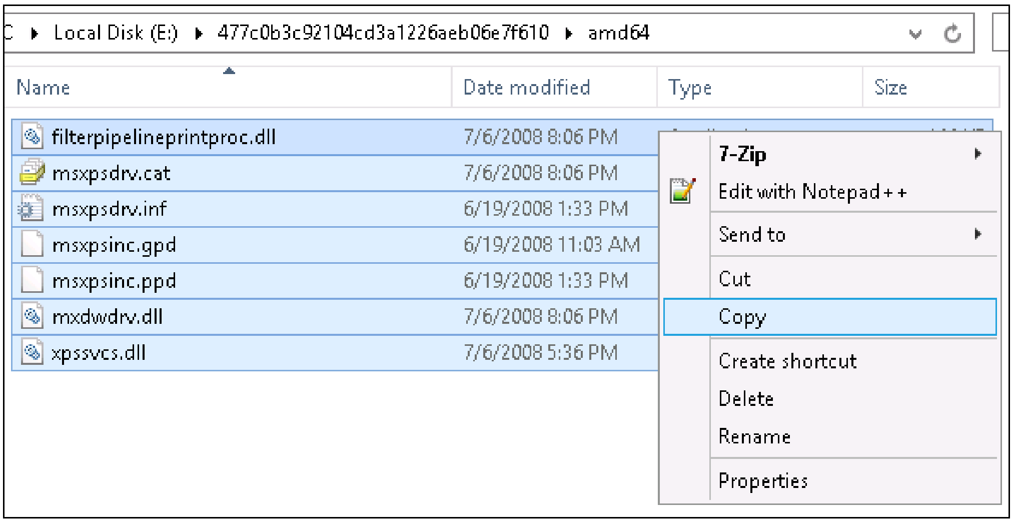
G:

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



Name	Date modified	Type
477c0b3c92104cd3a1226aeb06e7f610	5/25/2016 4:11 PM	File folder
Documents and Settings	5/18/2016 10:16 PM	File folder
Inetpub	5/25/2016 4:28 PM	File folder
Program Files	5/8/2017 3:38 PM	File folder
WINDOWS	5/8/2017 3:34 PM	File folder
wmpub	5/18/2016 9:04 PM	File folder

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

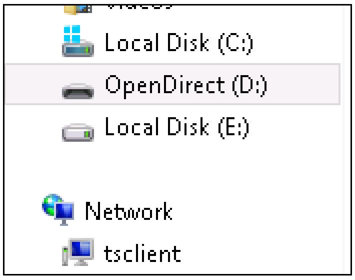


Name	Date modified	Type	Size
filterpipelineprintproc.dll	7/6/2008 8:06 PM		
msxpsdrv.cat	7/6/2008 8:06 PM		
msxpsdrv.inf	6/19/2008 1:33 PM		
msxpsinc.gpd	6/19/2008 11:03 AM		
msxpsinc.ppd	6/19/2008 1:33 PM		
mxdwdrv.dll	7/6/2008 8:06 PM		
xpssvcs.dll	7/6/2008 5:36 PM		

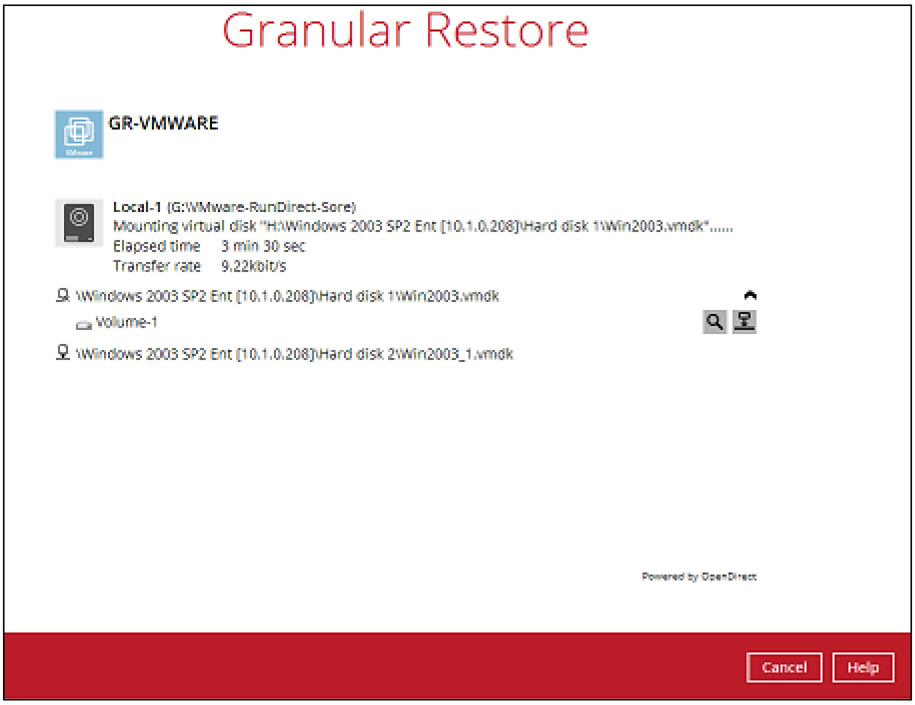
Note

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.



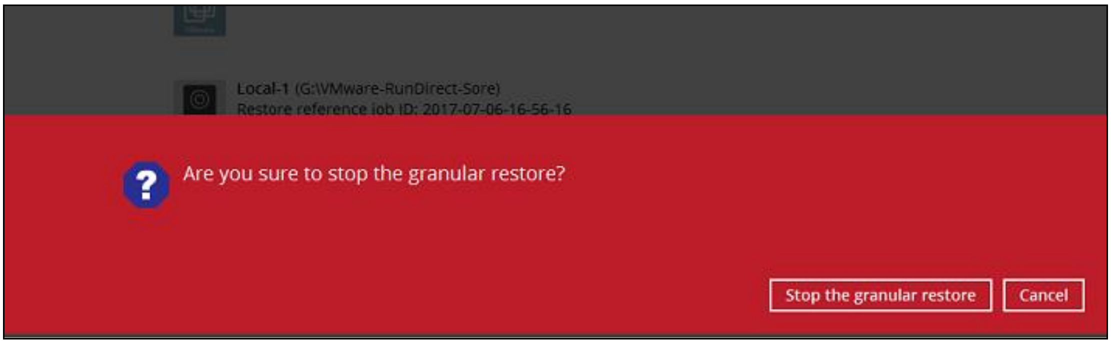
11. When you have finished restoring the necessary files, you can go back to AhsayOBM and click on **Cancel**.



Local-1 (G:\VMware-RunDirect-Sore)
Mounting virtual disk "H:\Windows 2003 SP2 Ent [10.1.0.208]\Hard disk 1\Win2003.vmdk"......
Elapsed time 3 min 30 sec
Transfer rate 9.22kbit/s

\Windows 2003 SP2 Ent [10.1.0.208]\Hard disk 1\Win2003.vmdk
Volume-1
\Windows 2003 SP2 Ent [10.1.0.208]\Hard disk 2\Win2003_1.vmdk

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



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

Are you sure to stop the granular restore?

IMPORTANT

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

15 Contact Ahsay

Technical Assistance

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

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

Documentation

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

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

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