

Online Backup Manager v7

# VMware vCenter/ESXi Guest Virtual Machine Backup & Restore Guide

11 September 2017

## Copyright Notice

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

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

## Trademarks

All product names are registered trademarks of their respective owners.

## Disclaimer

THE SUPPLIER 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 THE SUPPLIER without prior notice to you.

## Revision History

<b>Date</b>	<b>Descriptions</b>	<b>Type of modification</b>
15 July, 2016	First Draft	New
23 Aug, 2016	Modified Ch. 2.5	Modification
27 Sept, 2016	Modified Ch 6.1 with CBS added as backup destination; Ch 1 Overview section modified	Modification
3 Dec, 2016	Modified Ch 3.5 with new information on OBM 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

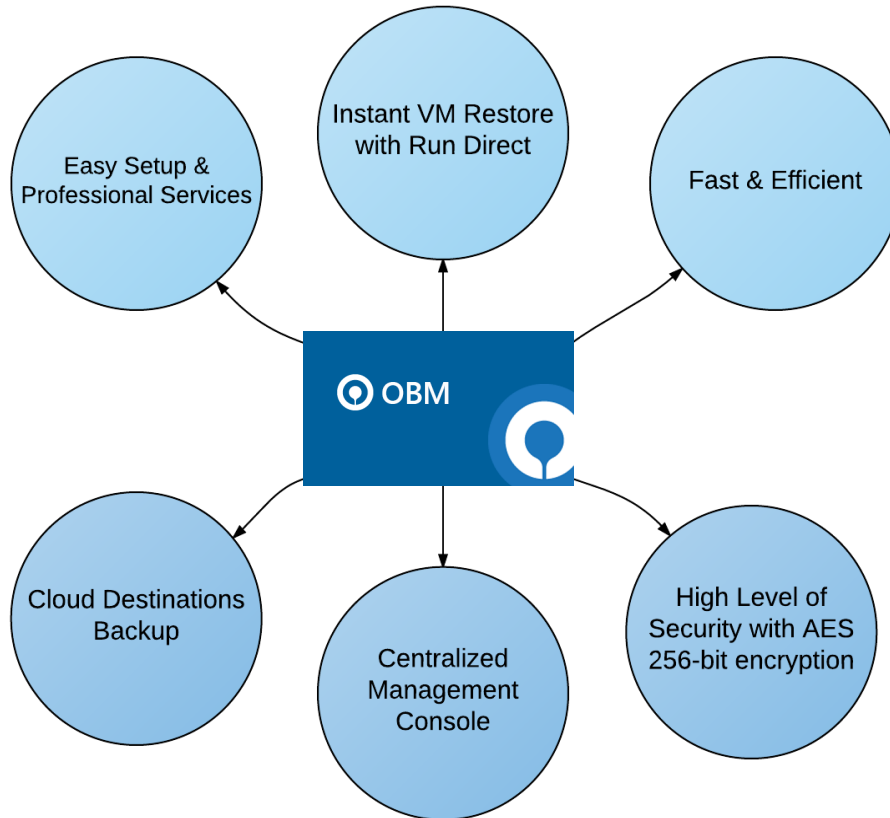
# Table of Contents

Why should I use OBM to back up my VMware vCenter/ESXi?.....	1
What is the purpose of this document? .....	5
What should I expect from this document? .....	5
<b>1 Understanding Backup Mode .....</b>	<b>6</b>
Backup Mode .....	6
Non-VDDK Backup Mode.....	6
VDDK Backup Mode .....	6
Features Comparison between VDDK and Non-VDDK Modes.....	7
<b>2 Requirements .....</b>	<b>8</b>
Hardware Requirement .....	8
Software Requirement .....	8
VMware vCenter / ESXi Server Requirements .....	8
ESXi / vCenter Patch Release .....	8
ESXi Shell Access .....	8
Root Account.....	8
Port Requirement .....	8
Disk Space Available on Datastore.....	8
Maximum Virtual Disk Size .....	9
VMware Tools .....	9
ESXi/ESX Hosts and Virtual Machine Hardware Versions Compatibility .....	9
Backup Client Computer Requirements .....	9
Hardware and Software Requirement.....	10
Add-on Module Requirement.....	11
Backup Quota Requirement .....	11
Port Requirement .....	11
Backup Client Computer on Linux .....	11
Disk Space Available on Backup Client Computer (or the vCenter computer) ..	11
Windows OS Requirement for VDDK and Non-VDDK Modes Backup .....	11
Run Direct Requirements .....	12
VDDK Backup Mode.....	12
Backup Destination Requirement .....	12
VDDK Backup Mode Requirements .....	14
License Requirement.....	14
Changed Block Tracking (CBT) on VMs .....	14
VMware Snapshot .....	15
Virtual Machine State .....	15
Non-VDDK Backup Mode Requirements.....	15
<b>3 Best Practices and Recommendations .....</b>	<b>16</b>

<b>4</b>	<b>Starting OBM</b> .....	<b>18</b>
	Login to OBM.....	18
<b>5</b>	<b>Creating a VMware VM Backup Set</b> .....	<b>19</b>
<b>6</b>	<b>Overview on Backup Process</b> .....	<b>29</b>
<b>7</b>	<b>Running a Backup</b> .....	<b>30</b>
	Start a Manual Backup.....	30
	Configure Backup Schedule for Automated Backup .....	33
<b>8</b>	<b>Restore Methods</b> .....	<b>37</b>
<b>9</b>	<b>Method 1 - Restoring a Virtual Machine with Run Direct</b> .....	<b>39</b>
	Login to OBM.....	39
	Running Direct Restore via OBM .....	39
	Verifying Run Direct Restore Connection .....	45
	Manage Run Direct VM.....	47
	Finalize VM Restore .....	48
	Stop Run Direct VM.....	48
<b>10</b>	<b>Method 2 - Restoring a Virtual Machine without Run Direct</b> .....	<b>50</b>
	Login to OBM.....	50
	VM Restore without Run Direct .....	50
<b>11</b>	<b>Method 3 - Restoring a Virtual Machine in Raw File (VMDK Format)</b> .....	<b>55</b>
	Restoring a VM in VMDK format .....	55

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

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



### Easy Setup & Professional Services

**Setup is a few clicks away** - our enhanced OBM 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.



## Instant VM Restore with Run Direct

### *What is Run Direct?*

Run Direct is a feature introduced since OBM 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 restore a VM by running it directly from the backup files in the backup destination. Administrator can troubleshoot on the failed virtual machine, while users are back in production with minimal disruption.

### *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.

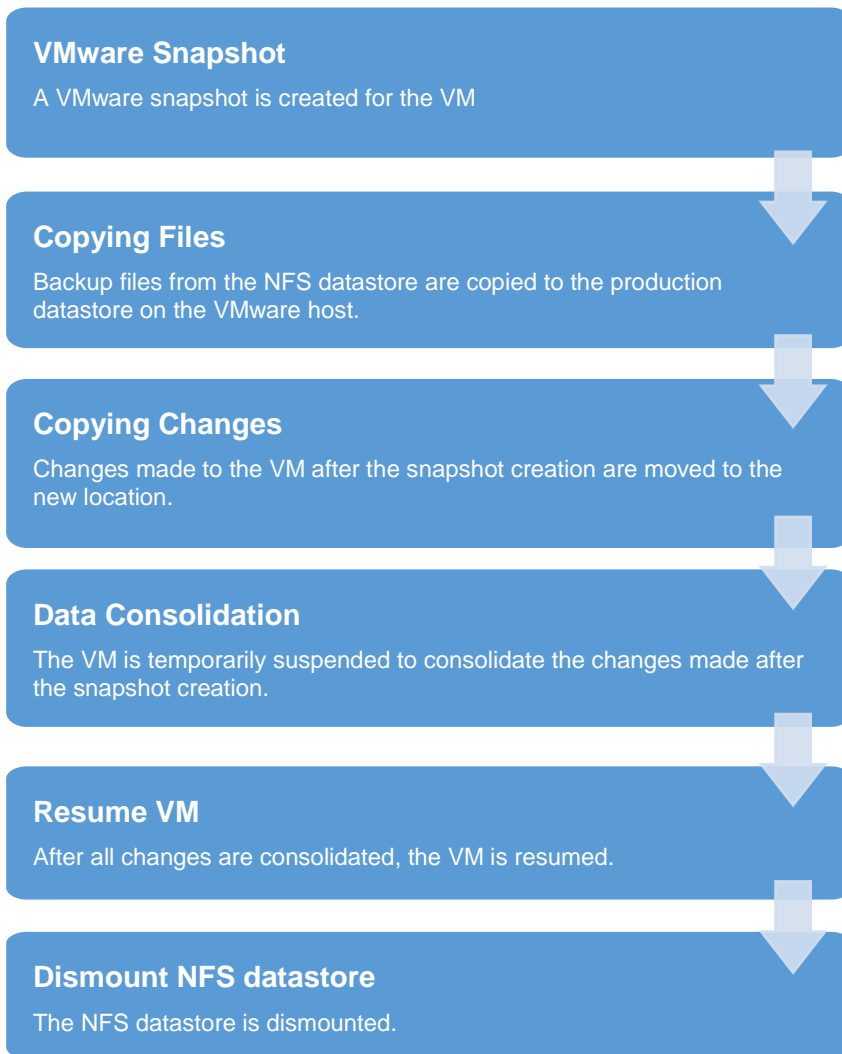
The restored virtual machine, at this stage (e.g. before the restore is finalized) is in a read-only state to preserve its integrity. All changes made to the virtual disks (e.g. operation within the guest virtual machine) are stored separately in transaction logs stored on the NFS datastore or the original 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
<b>Encryption</b>	NO	YES
<b>Compression</b>	NO	YES
<b>VDDK (CBT)</b>	YES	YES
<b>CBS</b>	NO	YES
<b>Local Destination</b>	YES	YES

### *Finalizing a VM Recovery (Migrating VM to permanent location)*

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



**Note**

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

Beside disaster recovery scenario, the Run Direct restore feature is also useful for recovery test or quick recovery of data on archived VM. Instead of restoring a VM on the production storage, run a VM directly from the backup files, to confirm on the backup, or quickly recover a file within an archived virtual machine that no longer exists on the VMware host.

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 OBM 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.



## Flexible Backup Destinations

- **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.



## High Level of Security

We understand your VM may contain sensitive information that requires protection, which 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 by default encrypt the backup data locally with AES 256-bit truly randomized encryption key.

## 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 OBM 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 OBM, as well as to carry out an end-to-end backup and restore process.

# 1 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, OBM must be installed on a supported Windows operating system platform.

The backup mode is chosen by OBM 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 OBM 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:

<b>Pros</b>	Free version of ESXi is supported.
<b>Cons</b>	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 (\*.l.vddk) in the backup chain.

During a subsequent backup in VDDK mode, OBM 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.

<b>Pros</b>	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.
<b>Cons</b>	VMware license requirement 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

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

## 2 Requirements

### Hardware Requirement

Refer to the following article for the list of hardware requirements for OBM: [FAQ: 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: Software Compatibility List \(SCL\) for version 7.3 or above](#).

### 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>)

#### 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

OBM 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-consistent quiescing).

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

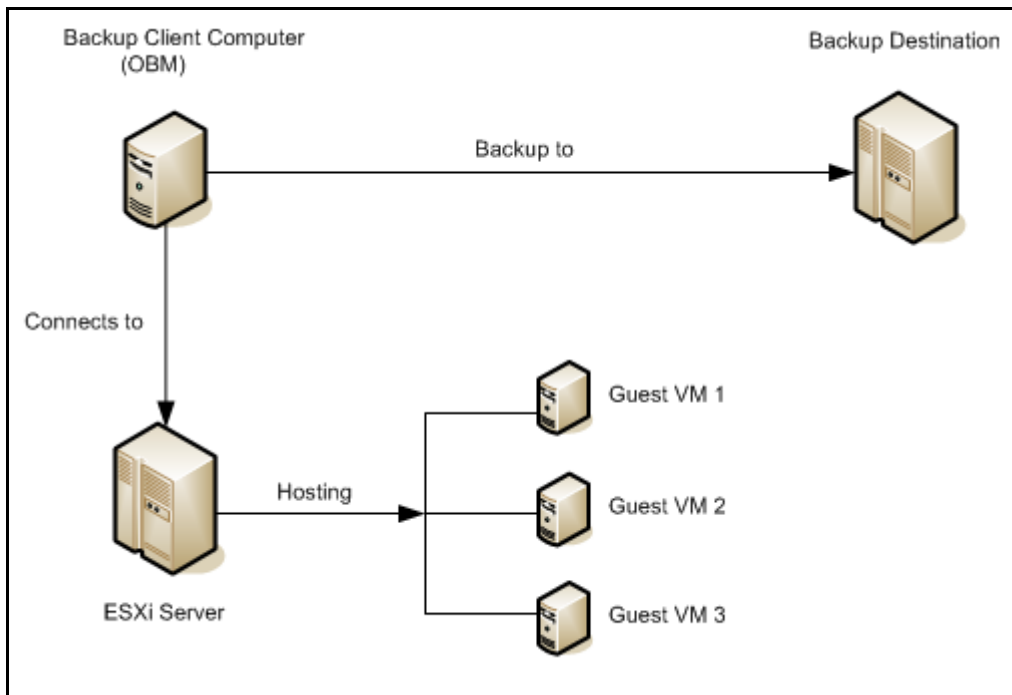
[ESXi/ESX hosts and compatible virtual machine hardware versions list \(2007240\)](#)

### Backup Client Computer Requirements

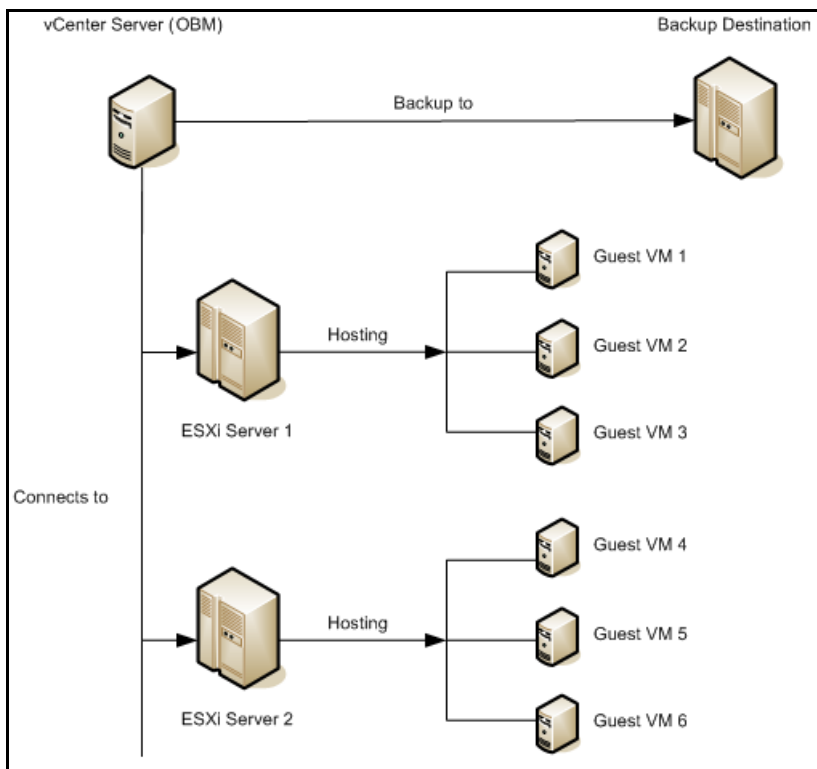
For backup of virtual machines on ESXi server (with no vCenter setup), a separate Backup Client Computer must be prepared for OBM to be installed on.

#### Important

OBM cannot be installed on an ESXi server directly.



For environment with vCenter setup, OBM should be 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 OBM 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 OBM 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&cm\\_d=displayKC&externalId=1012382](https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cm_d=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 and VDDK backup mode 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 (e.g. 120% x provisioned size of the largest virtual machine selected for backup).

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

Make sure OBM is installed on:



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

## Run Direct Requirements

Run Direct is a feature introduced since OBM 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 ESXi 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**.

The screenshot shows the configuration for a new storage destination. The name is 'CBS'. The type is 'Single storage destination'. The 'Run Direct' checkbox is checked, indicating support for restoring a VM directly from the backup file. The destination storage is set to 'CBS'.

- ◉ Destination must be accessible to the ESXi host.
- ◉ Destination must have sufficient disk space available for the backup operation. There should be 1.5 x total provisioned size of all VMs selected for backup.
- ◉ For backup 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.

## ▶ Operation System of the Backup Client Computer

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

## ▶ Restore to Alternate Location

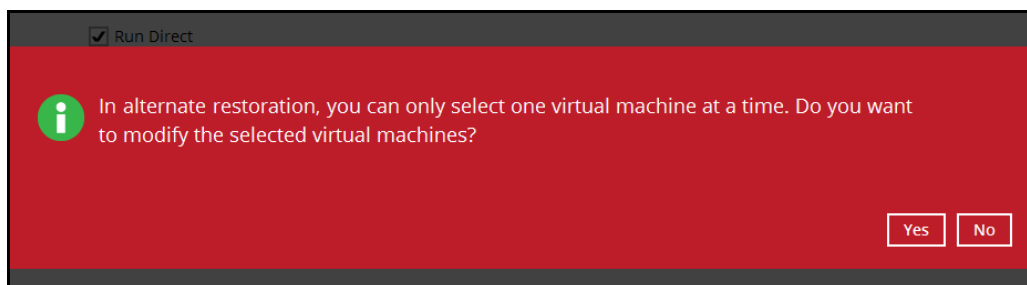
- ◉ When performing a Run Direct restore to **Alternate Location**, only one VM can be selected per restore session.



Restore virtual machines to

Original location

Alternate location



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

## ▶ **Dedicated NFS Service**

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

By default, the OBM NFS service is started as Local System, which does not have sufficient permission to access any network resources (e.g. the OBM 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 **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 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, OBM 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.

### 3 Best Practices and Recommendations

Please consider the following recommendations:

- Use the latest version of OBM.

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

- Install OBM on a physical staging machine

For best backup and restore performance, it is highly recommended that OBM 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 OBM to quiesce the guest VMs prior to backing them up to create consistent backup for your VMs

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

- Don't use a guest VM as a staging machine.

Although installing OBM 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 OBM 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).

- ▶ 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 OBM (Java heap space) if you are using non-VDDK mode backup.

If you are using non-VDDK mode, 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:

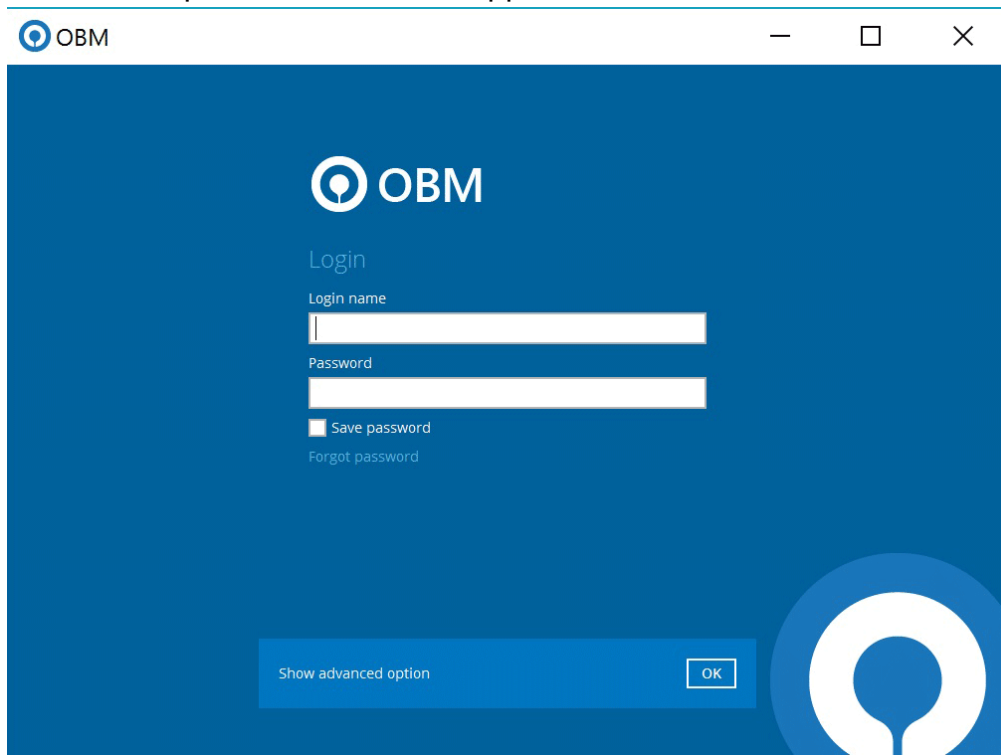
<http://portal.vsl-net.com/backup/v7/FAQ/5003.pdf>

## 4 Starting OBM

### Login to OBM

1. Login to the OBM application user interface.

For Backup Client Computer on Windows / Mac OS X, double click the OBM 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 &
```

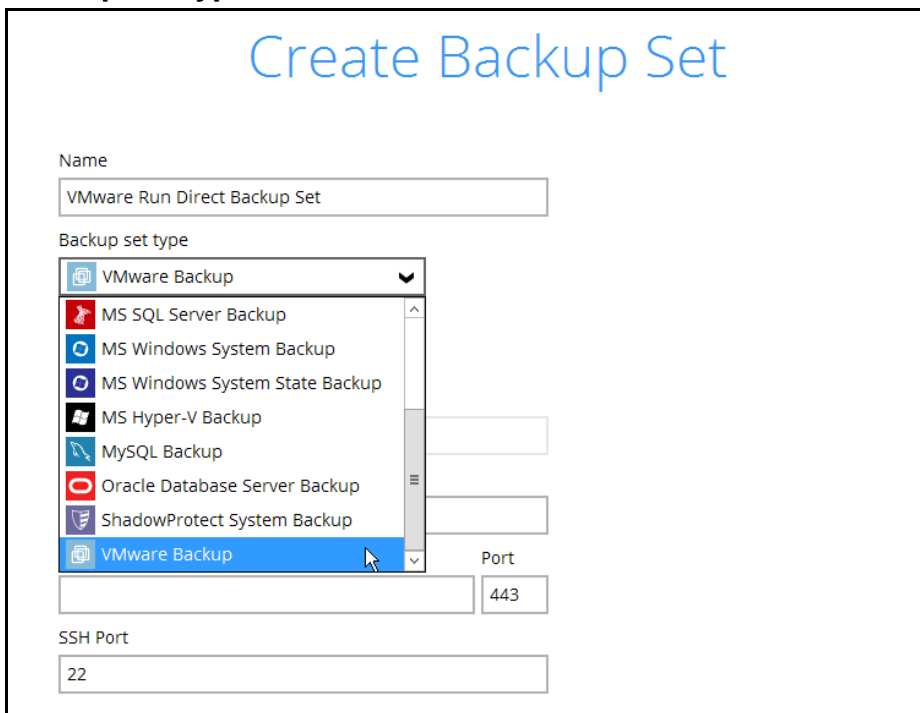
2. Enter the **Login name** and **Password** of your OBM account.
3. Click **OK** afterward to login to OBM.

## 5 Creating a VMware VM Backup Set

1. In the OBM 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**.

A screenshot of the "Create Backup Set" form. The title "Create Backup Set" is at the top in blue. Below it, there are several input fields and a dropdown menu. The "Name" field contains "VMware Run Direct Backup Set". The "Backup set type" dropdown menu is open, showing a list of backup types: VMware Backup (selected), MS SQL Server Backup, MS Windows System Backup, MS Windows System State Backup, MS Hyper-V Backup, MySQL Backup, Oracle Database Server Backup, and ShadowProtect System Backup. To the right of the dropdown, there are two empty input fields. Below the dropdown, there is a "Port" field containing "443". At the bottom, there is an "SSH Port" field containing "22".



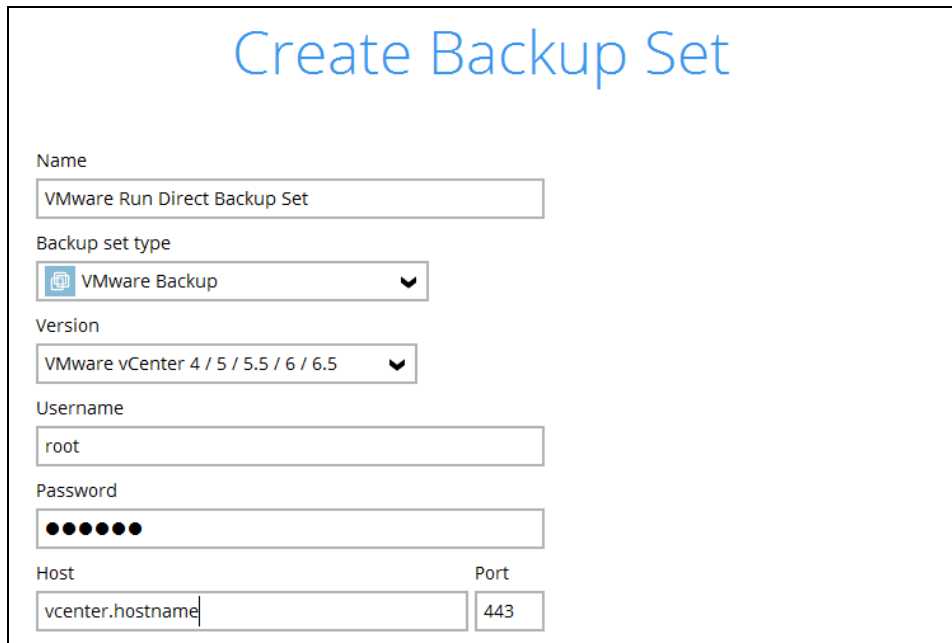
4. Select the **Version** of the corresponding host:

The screenshot shows the 'Create Backup Set' form. The 'Name' field contains 'VMware Run Direct Backup Set'. The 'Backup set type' is set to 'VMware Backup'. The 'Version' dropdown menu is open, showing options: 'VMware vCenter 4 / 5 / 5.5 / 6 / 6.5', 'VMware ESX 4', 'VMware ESXi 4 / 5 / 5.5 / 6 / 6.5' (highlighted), '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', and 'VMware vCenter 4 / 5 / 5.5 / 6 / 6.5'. The 'Port' field contains '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
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.

The screenshot shows the 'Create Backup Set' form. The 'Name' field contains 'VMware Run Direct Backup Set'. The 'Backup set type' is set to 'VMware Backup'. The 'Version' dropdown menu is closed, showing 'VMware ESXi 4 / 5 / 5.5 / 6 / 6.5'. The 'Username' field contains 'root'. The 'Password' field is masked with dots. The 'Host' field contains 'esxi\_hostname', the 'Port' field contains '443', and the 'SSH Port' field contains '22'.

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

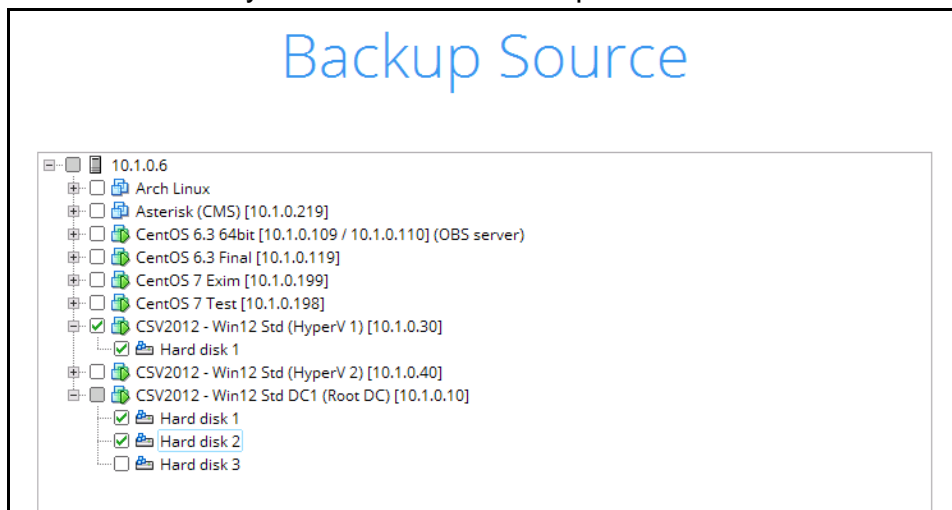


The screenshot shows a 'Create Backup Set' configuration window. The title is 'Create Backup Set' in blue. The form contains the following fields:

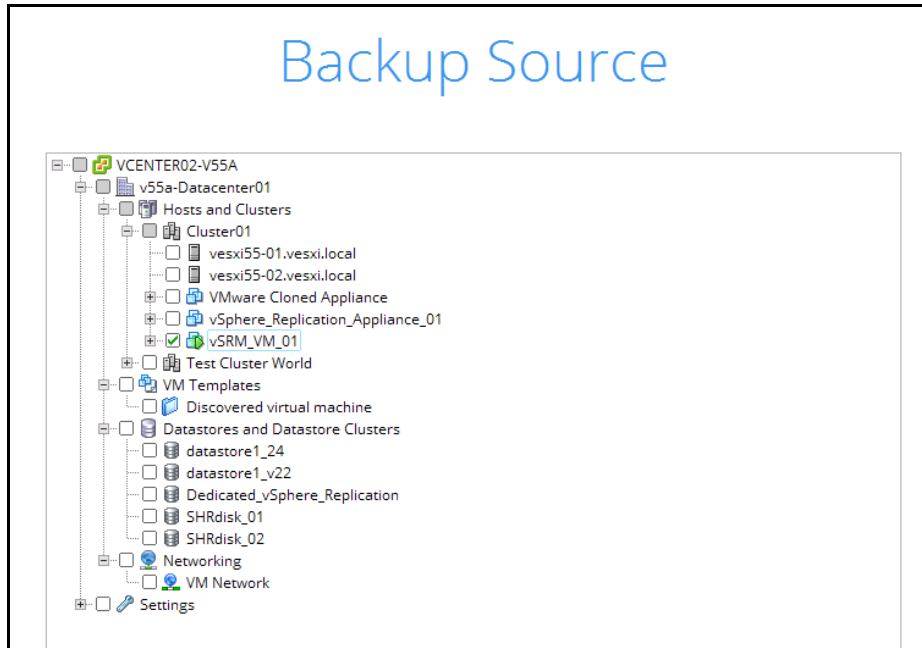
- Name:** VMware Run Direct Backup Set
- Backup set type:** VMware Backup (selected from a dropdown menu)
- Version:** VMware vCenter 4 / 5 / 5.5 / 6 / 6.5 (selected from a dropdown menu)
- Username:** root
- Password:** A password field with six black dots for masking.
- Host:** vcenter.hostname
- Port:** 443

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

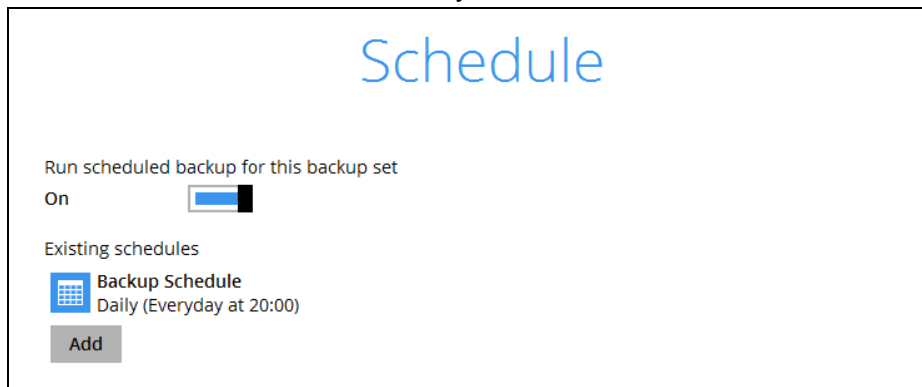
6. For VMware ESXi backup set, select the virtual machines or individual virtual disks that you would like to backup.



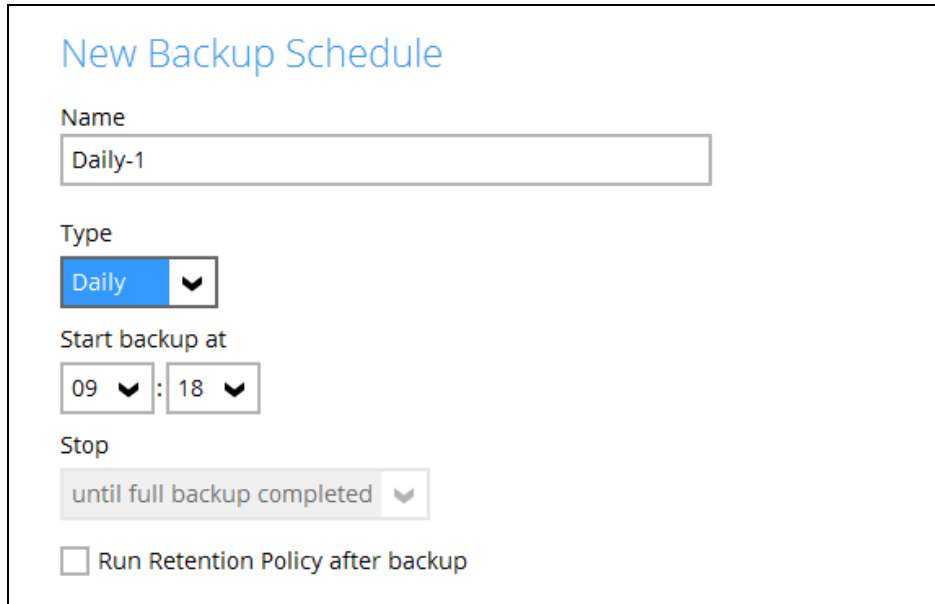
For VMware vCenter backup set, select the settings, virtual machines or individual virtual disks that you would like to backup.



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



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



**New Backup Schedule**

Name  
Daily-1

Type  
Daily

Start backup at  
09 : 18

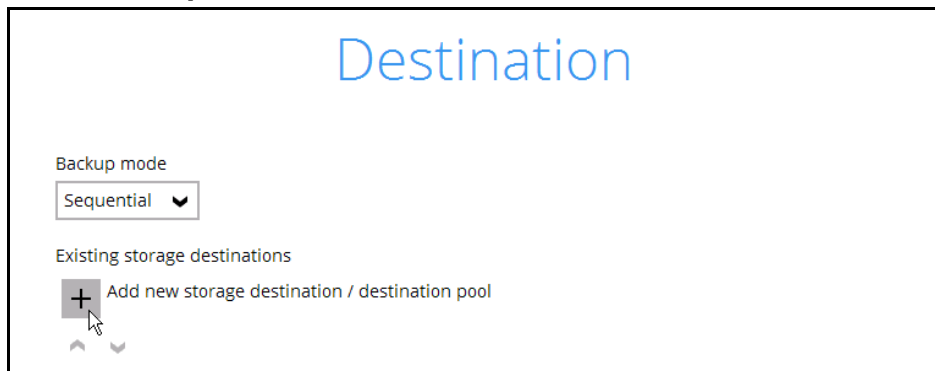
Stop  
until full backup completed

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  
+ Add new storage destination / destination pool

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

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

#### 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

Type  
 Single storage destination  
 Destination pool

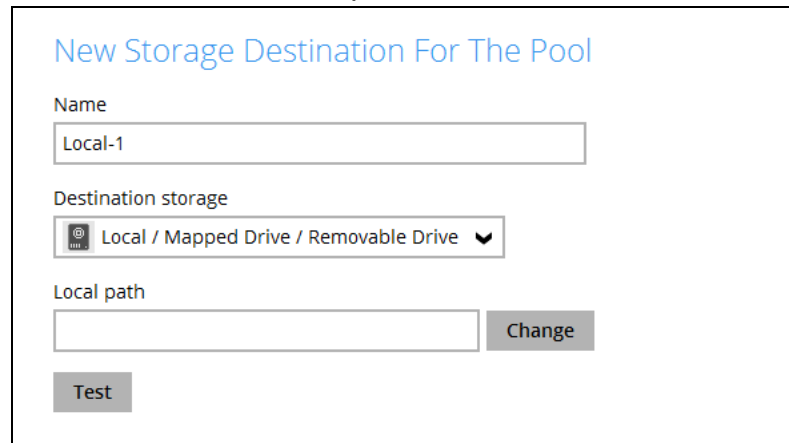
Add the cloud (e.g. Google Drive or Dropbox) or local storage that you would like to pool together for backup. You can always add more storage to this pool in the future.

Existing storage destinations in the pool  
 Add new storage destination to the pool

^ v



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

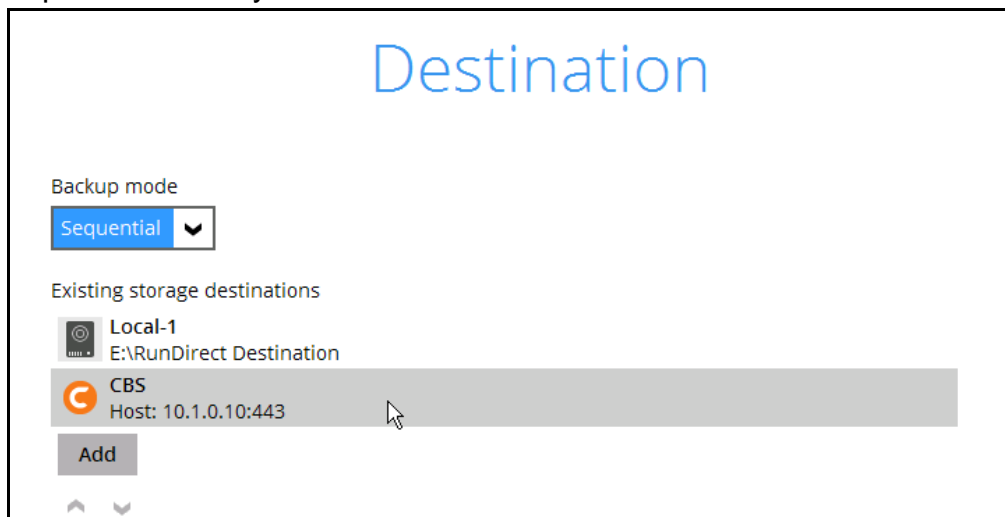
- If you have chosen the Local/Mapped Drive/Removable Drive option, click **Change** to browse to a directory path where backup data will be stored. The path must be accessible to the ESXi host.



The screenshot shows a configuration window titled "New Storage Destination For The Pool". It contains the following fields and controls:

- Name:** A text input field containing "Local-1".
- Destination storage:** A dropdown menu with a server icon and the text "Local / Mapped Drive / Removable Drive".
- Local path:** A text input field that is currently empty, followed by a "Change" button.
- Test:** A button located below the local path field.

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.



The screenshot shows a configuration window titled "Destination". It contains the following elements:

- Backup mode:** A dropdown menu with "Sequential" selected.
- Existing storage destinations:** A list of two destinations:
  - Local-1:** E:\RunDirect Destination
  - CBS:** Host: 10.1.0.10:443
- Add:** A button to add a new destination.
- Ordering:** Up and down arrow icons at the bottom of the list to reorder destinations.

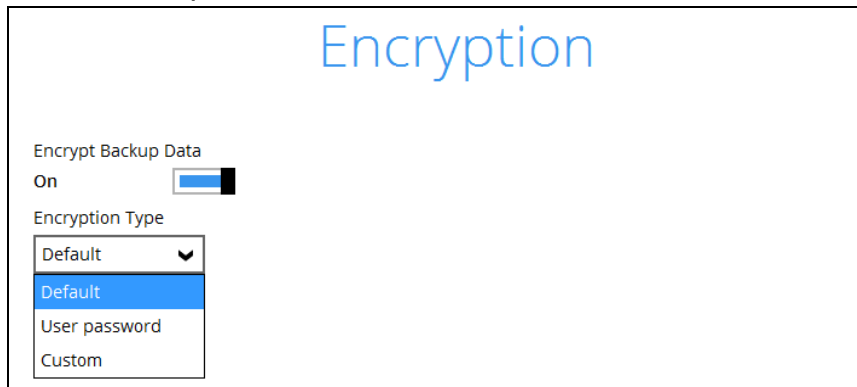
### Note

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).

Click **Next** to proceed.

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

most secure protection.

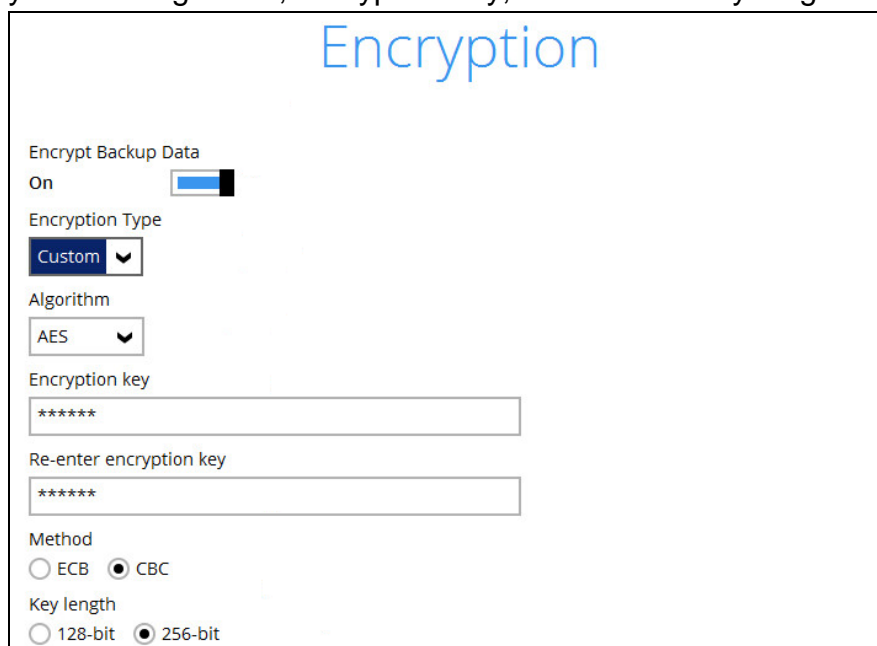


The screenshot shows the 'Encryption' settings page. At the top, the word 'Encryption' is displayed in a large blue font. Below it, there are two main sections. The first section is 'Encrypt Backup Data', which has a toggle switch set to 'On'. The second section is 'Encryption Type', which has a dropdown menu currently showing 'Default'. The dropdown menu is open, showing three options: 'Default' (highlighted in blue), 'User password', and 'Custom'.

**WARNING:** If a note of the encryption key is NOT taken, and the key is LOST, the data will be irretrievable. We recommend changing the DEFAULT encryption key to something memorable.

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

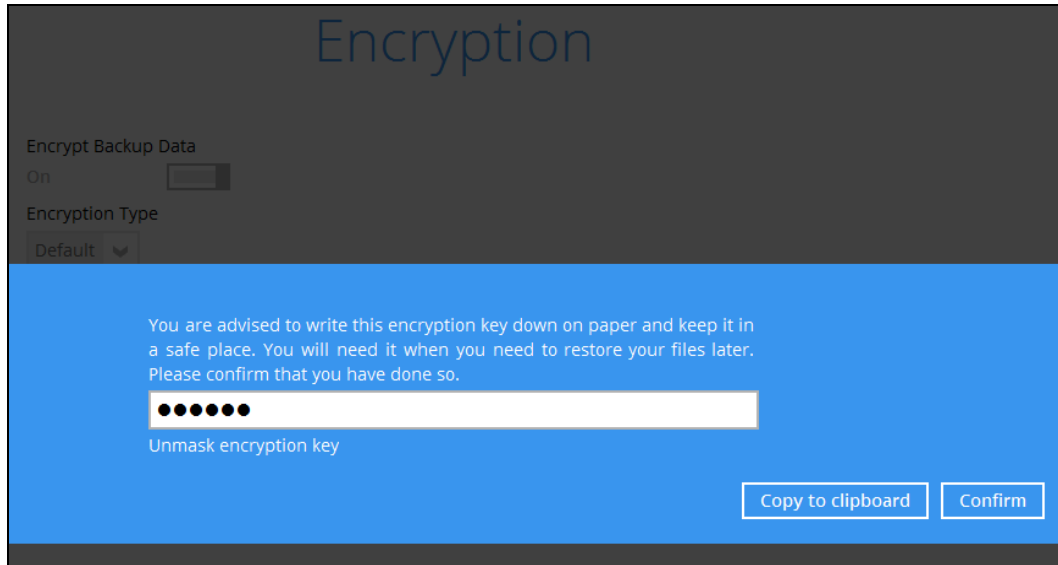
- **Default** – an encryption key with 44 alpha numeric characters will be randomly generated by the system
- **User password** – the encryption key will be the same as the login password of your OBM at the time when this backup set is created. Please be reminded that if you change the OBM login password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



The screenshot shows the 'Encryption' settings page with the 'Custom' option selected. The 'Encrypt Backup Data' toggle is still 'On'. The 'Encryption Type' dropdown is now set to 'Custom'. Below this, there are several more settings: 'Algorithm' is set to 'AES'; 'Encryption key' and 'Re-enter encryption key' are both input fields containing asterisks (\*\*\*\*\*); 'Method' has two radio buttons, 'ECB' and 'CBC', with 'CBC' selected; and 'Key length' has two radio buttons, '128-bit' and '256-bit', with '256-bit' selected.

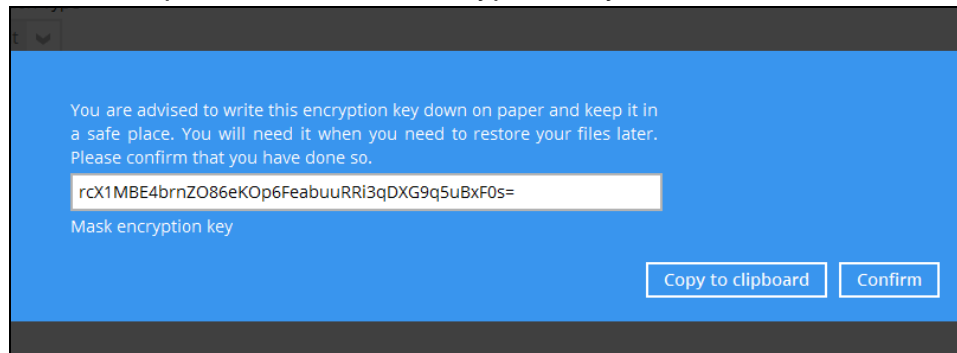
Click **Next** when you are done setting.

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



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

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

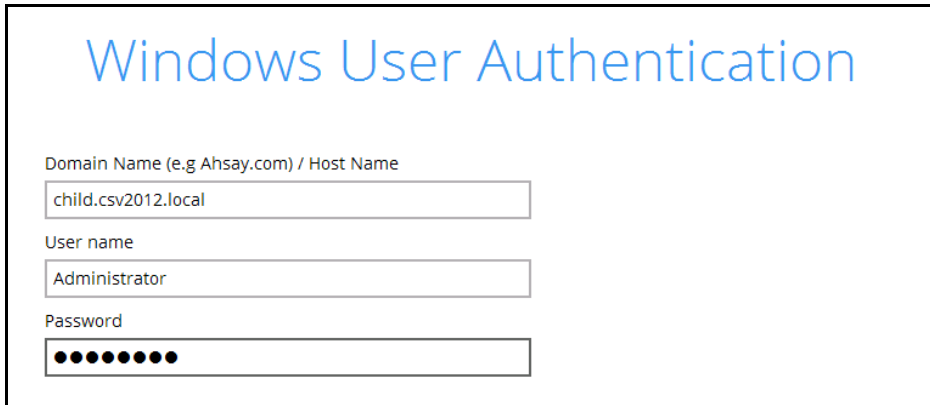


- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.
- **Confirm** – Click to exit this pop-up window and proceed to the next step.

**WARNING:** If a note of the encryption key is NOT taken, and the key is LOST, the data will be irretrievable. We recommend changing the DEFAULT encryption key to something memorable.



13. Enter the Windows login credentials used by OBM to authenticate the scheduled or continuous backup.



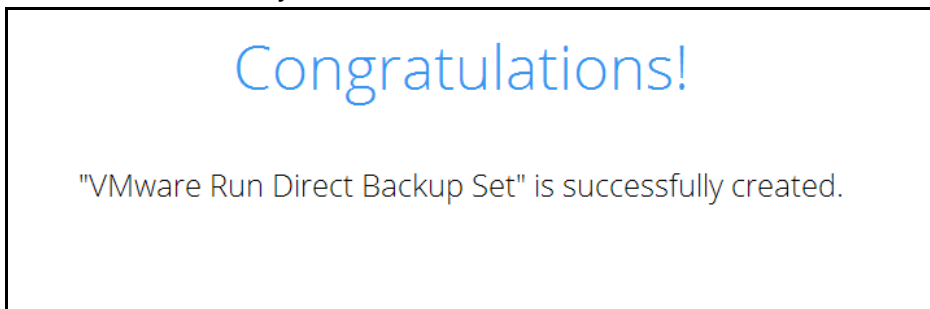
The screenshot shows a dialog box titled "Windows User Authentication" in blue text. Below the title are three input fields: "Domain Name (e.g Ahsay.com) / Host Name" with the text "child.csv2012.local", "User name" with the text "Administrator", and "Password" with a masked password represented by ten black dots.

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.

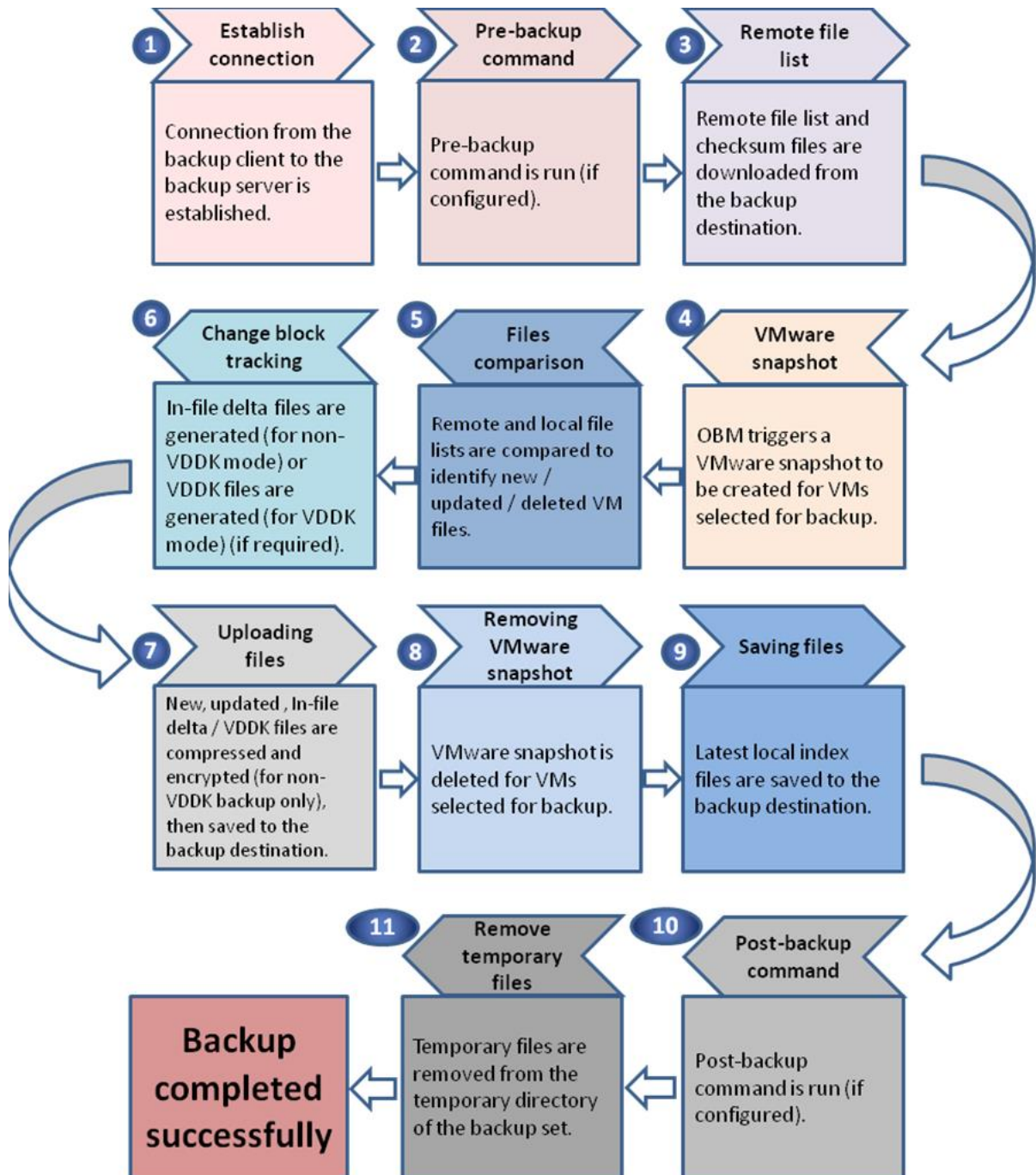
14. The following screen is displayed when the new VMware VM backup set is created successfully.



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

## 6 Overview on Backup Process

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



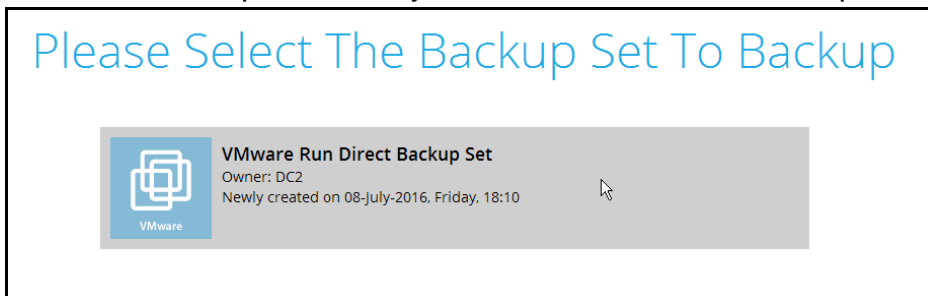
## 7 Running a Backup

### Start a Manual Backup

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




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



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

available:



### 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

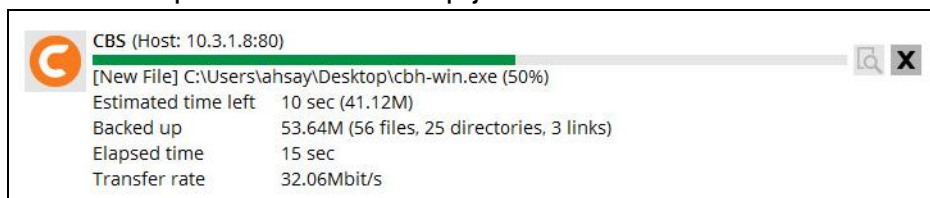
Run Retention Policy after backup

[Hide advanced option](#)

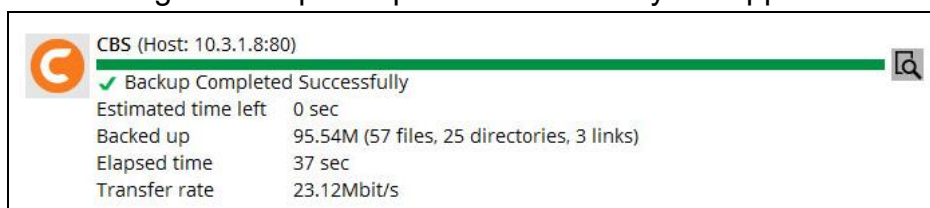
- **Full** – A full backup captures all the data that you want to protect. When you run a backup job for the first time, OBM will run a full backup regardless of the in-file delta setting.
- **Differential** – A differential backup captures only the changes made as compared with the last uploaded full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


Click **Backup** to start the backup.

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



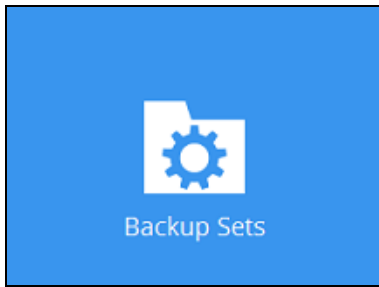
6. When the backup is completed, the progress bar will be green in color and the message "Backup Completed Successfully" will appear.



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

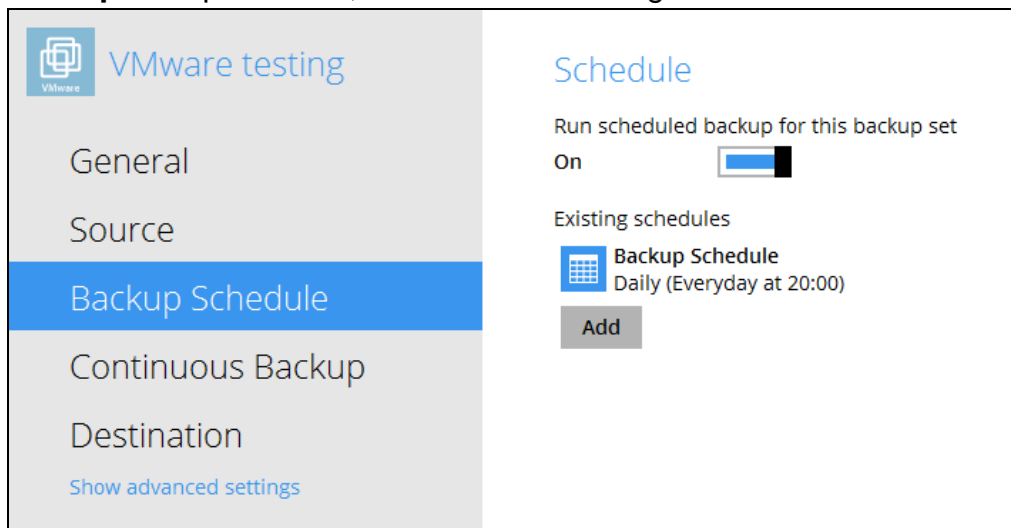
## Configure Backup Schedule for Automated Backup

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



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

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



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

The screenshot shows the 'New Backup Schedule' window. The title is 'New Backup Schedule'. Below the title, there is a text input field for 'Name' containing 'Daily-1'. Underneath is a dropdown menu for 'Type' set to 'Daily'. The 'Start backup at' section has two dropdown menus for time, showing '14' and '52'. The 'Stop' section has a dropdown menu set to 'until full backup completed'. At the bottom, there is a checkbox labeled 'Run Retention Policy after backup' which is currently unchecked.

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

The screenshot shows the 'New Backup Schedule' window. The title is 'New Backup Schedule'. Below the title, there is a text input field for 'Name' containing 'Dayend'. Underneath is a dropdown menu for 'Type' set to 'Daily'. The 'Start backup at' section has two dropdown menus for time, showing '18' and '00'. The 'Stop' section has a dropdown menu set to 'until full backup completed'. At the bottom, there is a checkbox labeled 'Run Retention Policy after backup' which is currently checked.

- ⦿ **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

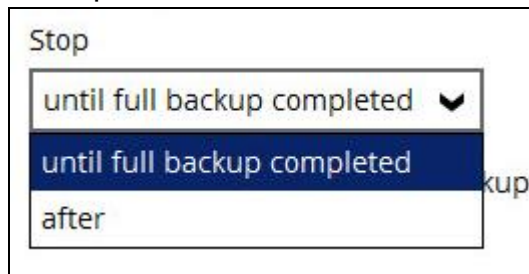
Stop  
until full backup completed

Run Retention Policy after backup

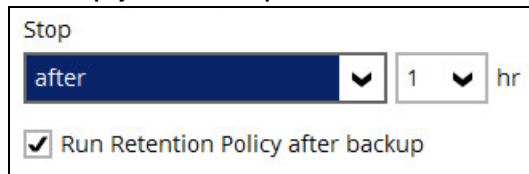


The **Stop** dropdown menu offers two options:

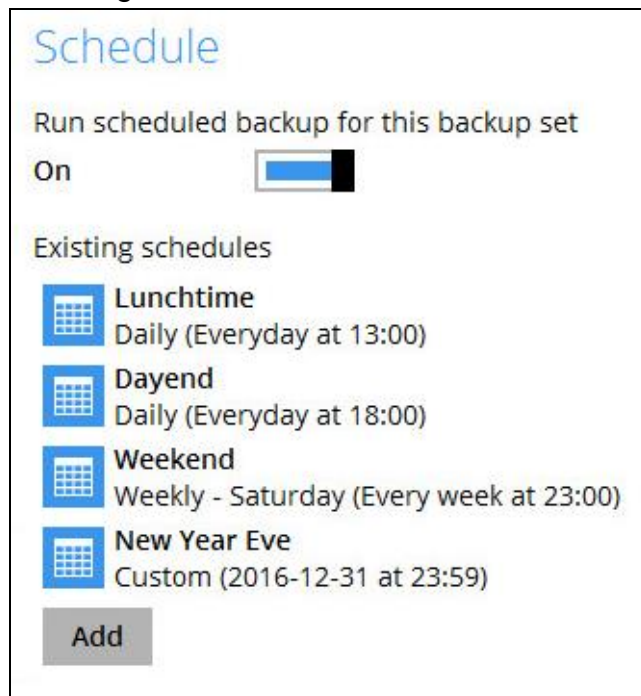
- ⦿ **until full backup completed** – in case you prefer a complete backup



- ⦿ **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



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



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

## 8 Restore Methods

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

### Method 1 - Restoring a Virtual Machine with Run Direct

#### Introduction

This restore method can instantly restore a VM by running it directly from the backup files in the backup destination. Administrator can troubleshoot on the failed virtual machine, while users are back in production with minimal disruption.

#### Pros

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

#### Cons

- Changes made during Run-Direct restore is not committed to the VM until it is migrated completely.

### 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 either the original VM location or an alternate location of your choice.

#### 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 larger
- 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 ESXi server directly without using OBM

#### Pros

- You can manually restore the VM to another ESXi server off-site without having to use OBM as the restore channel

**Cons**

- Restore procedures are relatively complicated

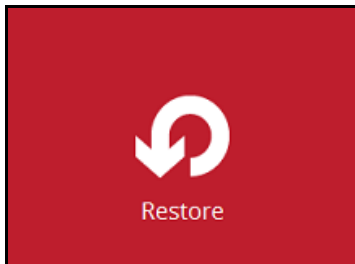
## 9 Method 1 - Restoring a Virtual Machine with Run Direct

### Login to OBM

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

### Running Direct Restore via OBM

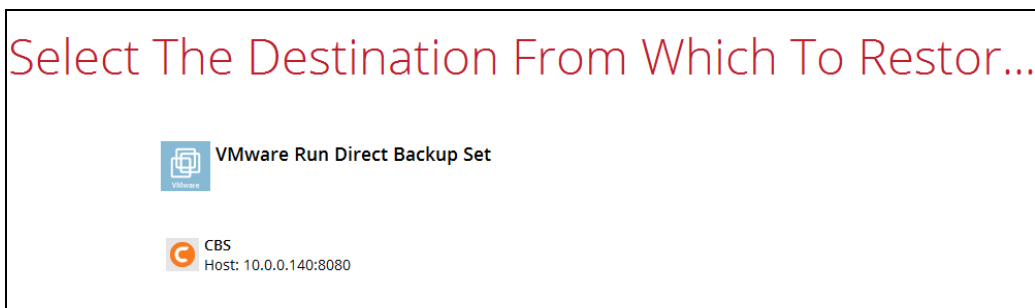
1. Click the **Restore** icon on the main interface of .



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.



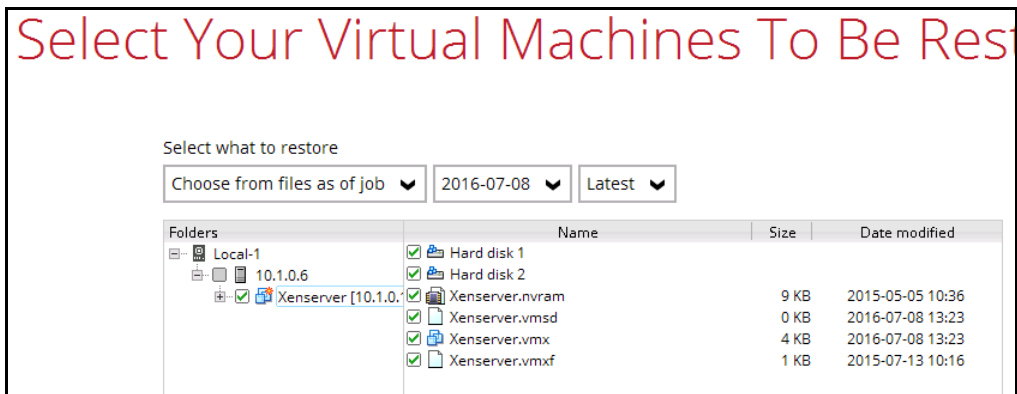
4. Select to restore VM from a specific backup job, or the latest job available from the **Select what to restore** drop down menu.

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

#### Important

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

per restore session.

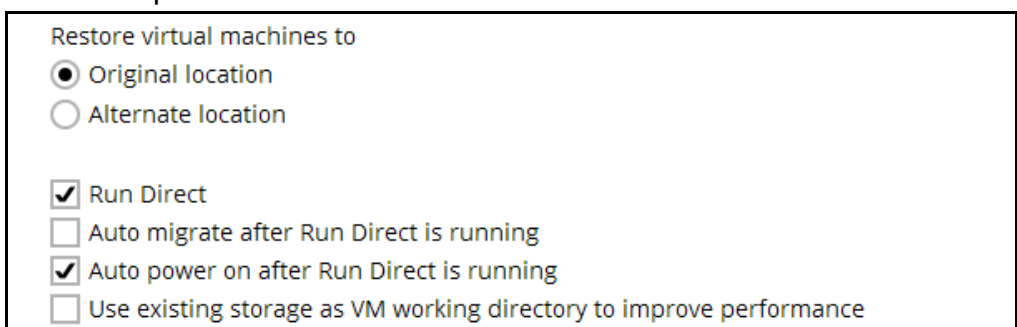


If you wish to restore the VM to another Esxi server, you can restore the VM in raw file format, where the .vmdk disk format file will be included, by clicking the **Restore raw file** button at the bottom left corner. Refer to the steps in [Appendix Restoring VM in VMDK format](#).

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



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



- Auto migrate after Run Direct is running**

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

**Note**

This will finalize the recovery of the VM; the migration will be performed right after Run Direct is running for the VM.

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

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

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

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

8. 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.

- i. For restoration to another VMware ESXi host, 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.

The screenshot shows a configuration window titled "Alternate location" in red text. Below the title is a blue heading "VMware Host". The form contains the following fields:

- Version:** A dropdown menu with the selected value "VMware ESXi 4 / 5 / 5.5 / 6 / 6.5".
- Username:** A text input field containing "root".
- Password:** A text input field containing "\*\*\*\*\*".
- Host:** A text input field containing "new\_esxi\_host".
- Port:** A text input field containing "443".
- SSH Port:** A text input field containing "22".

- ii. For restoration to another VMware vCenter setup, enter the **Password** of the administrator account, **Host**, and **Port** information

of the new / original vCenter server.

The screenshot shows a configuration window titled "Alternate location" in red text. Below the title, the section "VMware Host" is displayed in blue. The form includes the following fields:

- Version:** A dropdown menu showing "VMware vCenter 4 / 5 / 5.5 / 6".
- Username:** A text input field containing "administrator".
- Password:** A text input field with six black dots representing masked characters.
- Host:** A text input field containing "new\_vcenter\_host".
- Port:** A text input field containing "443".

- iii. Press **Next** to proceed when you are done with the settings.
- iv. Enter a new **Name** for the VM, then **Browse** to modify the **Inventory Location**, **Host/Cluster**, **Resource Pool** and **Storage** settings, according to where you would like the VM to be restored to.

The screenshot shows a configuration window titled "Alternate location" in red text. Below the title, the text "VMware ESXi 5.1.0 build-1157734@10.1.0.6:443(SSH:22)" is displayed. The form includes the following fields and buttons:

- Name:** A text input field containing "New Virtual Machine".
- Inventory Location:** A text input field containing "10.1.0.6" and a "Browse" button.
- Host/Cluster:** A text input field containing "10.1.0.6" and a "Browse" button.
- Resource Pool:** A text input field containing "10.1.0.6" and a "Browse" button.
- Storage:** A text input field containing "datastore1\_PD0001" and a "Browse" button.

## Alternate location

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

Name

Inventory Location

Host/Cluster

Resource Pool

Storage

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

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

## Temporary Directory

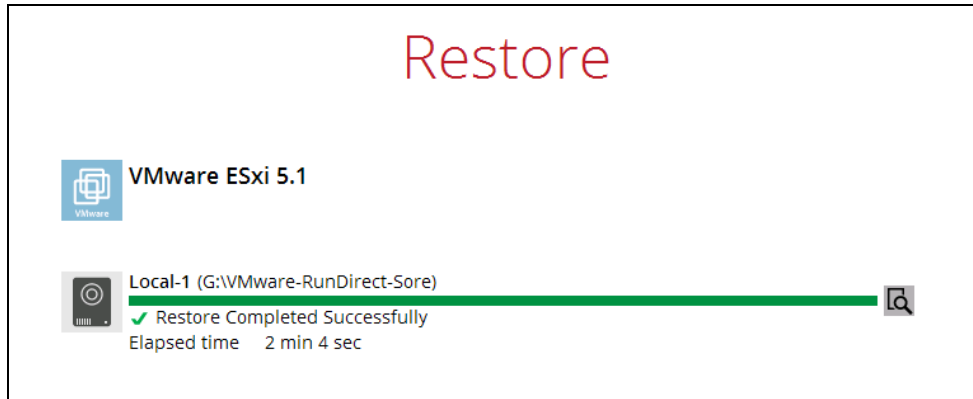
Temporary directory for storing restore files

10. When restoring your guest VM 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.



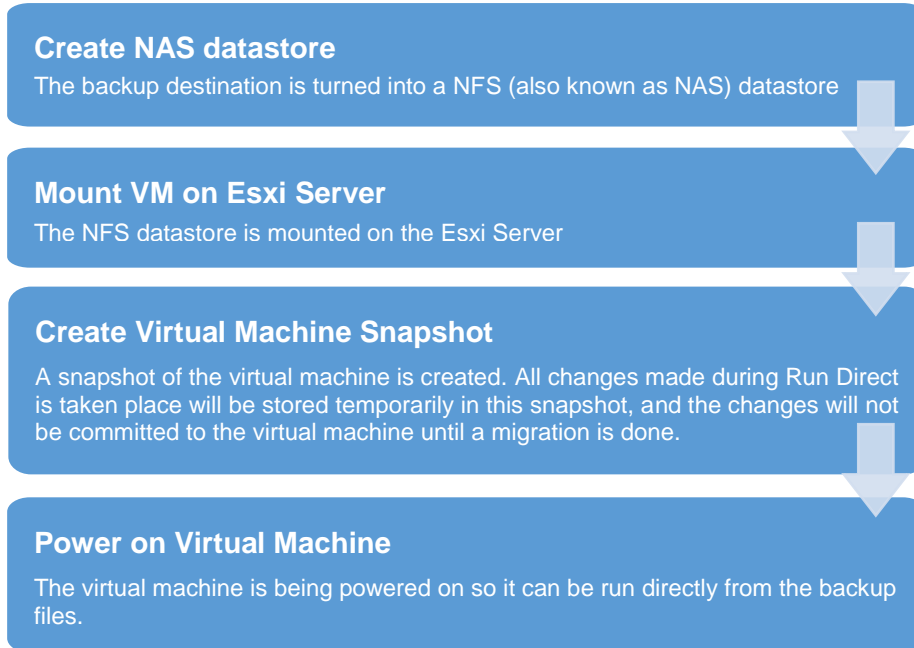


11. The following screen shows when the VM has been restored successfully.



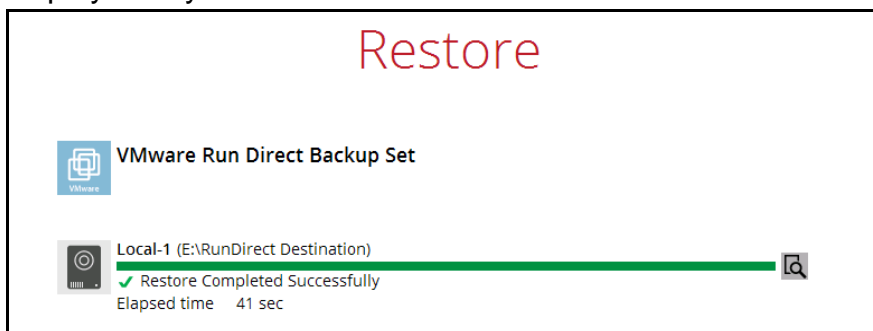
## Verifying Run Direct Restore Connection

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

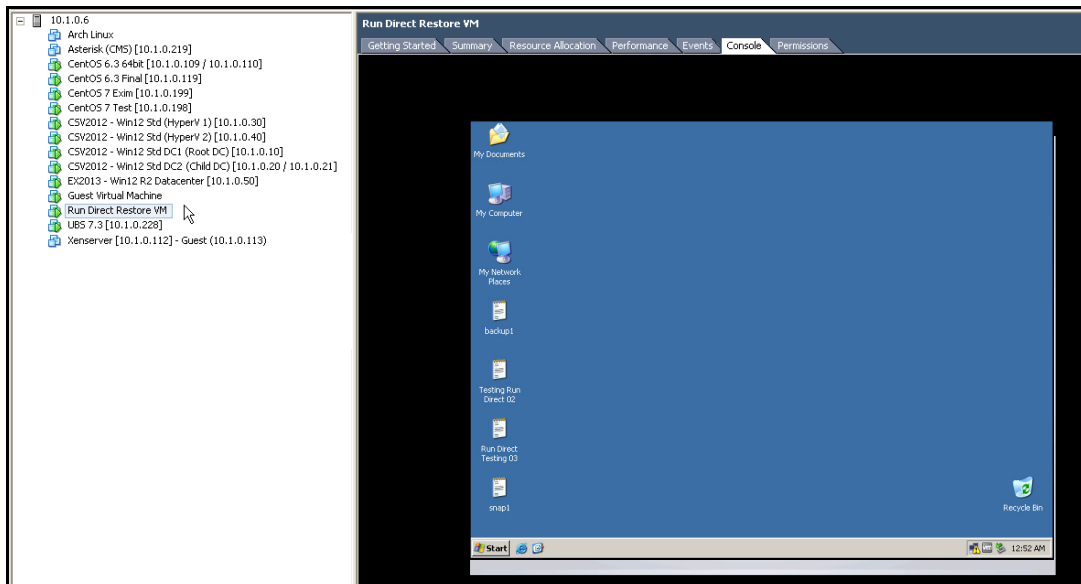


Check the following items to verify if the run direct restore connection has been established between the backup destination and the VMware host.

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



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



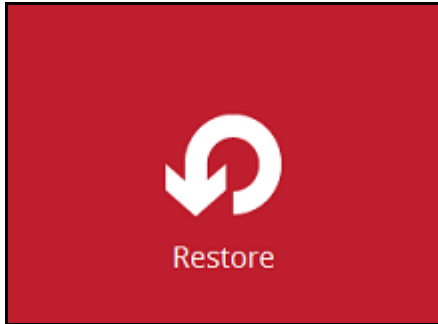
### Notes

- Do not exit from the OBM 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 OBM.
- 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.

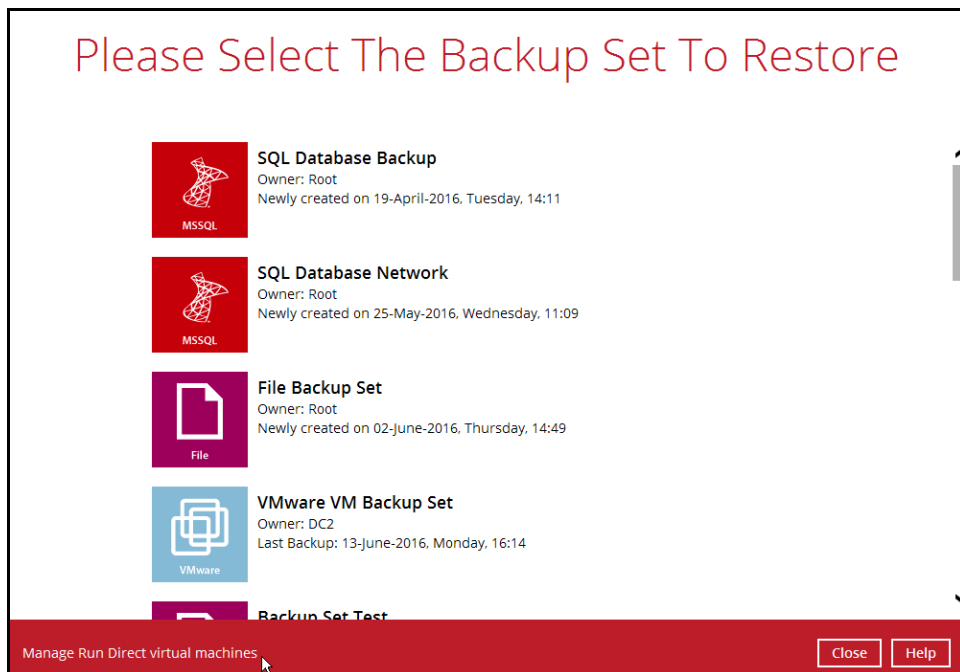
## Manage Run Direct VM

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 OBM.



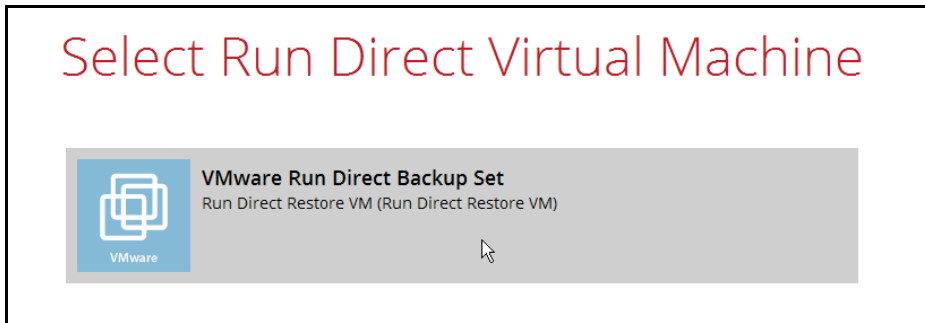
2. Click **Manage Run Direct virtual machines** to manage all Run Direct virtual machines.



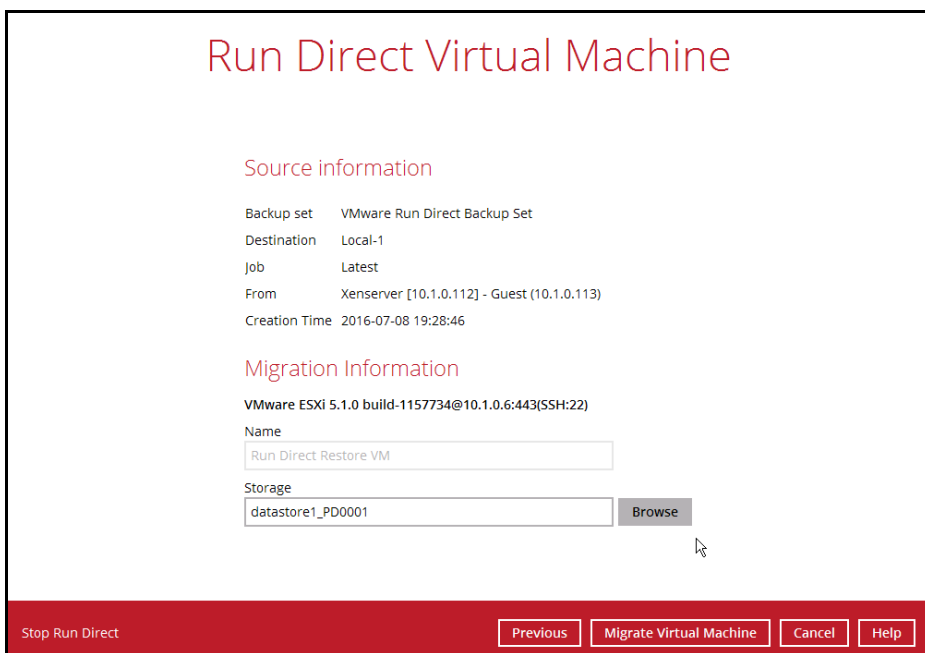
## Finalize VM Restore

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

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



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



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

### Note

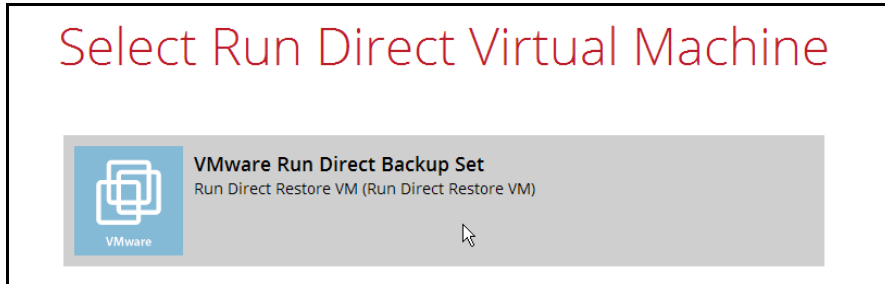
*For VM on ESXi host, the VM may be suspended temporarily during the migration process. The downtime of the VM should be minimal.*

## Stop Run Direct VM

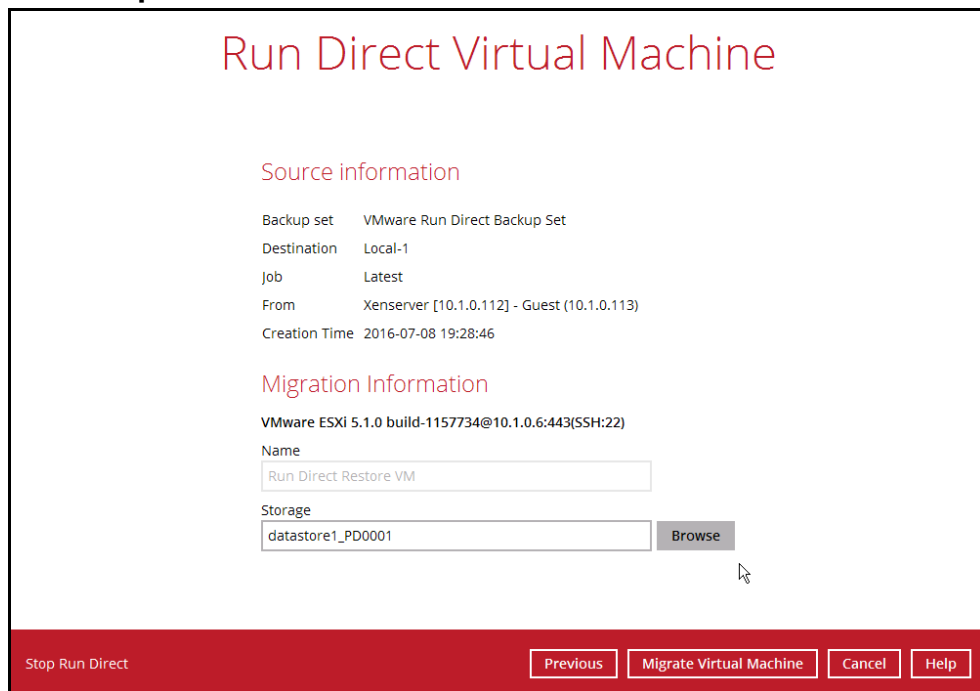
To stop all virtual machines, or individual virtual machine that is running with the Run Direct feature:

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

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



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



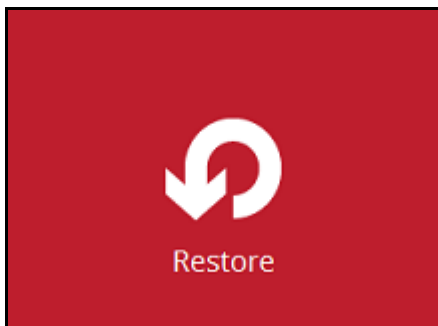
## 10 Method 2 - Restoring a Virtual Machine without Run Direct

### Login to OBM

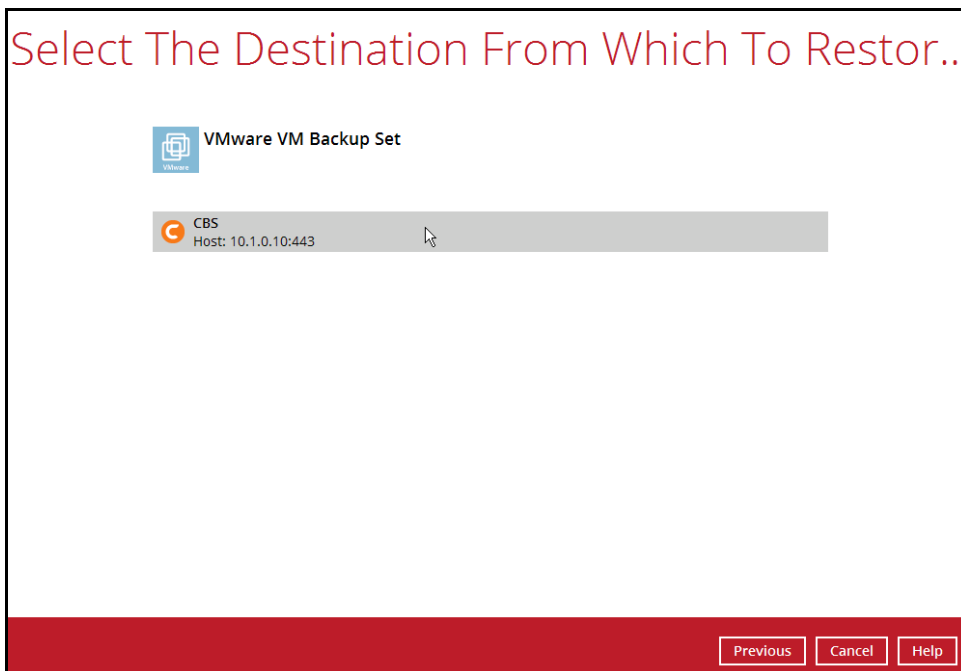
Login to the OBM application according to the instruction provided in the chapter on [Starting OBM](#).

### VM Restore without Run Direct

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

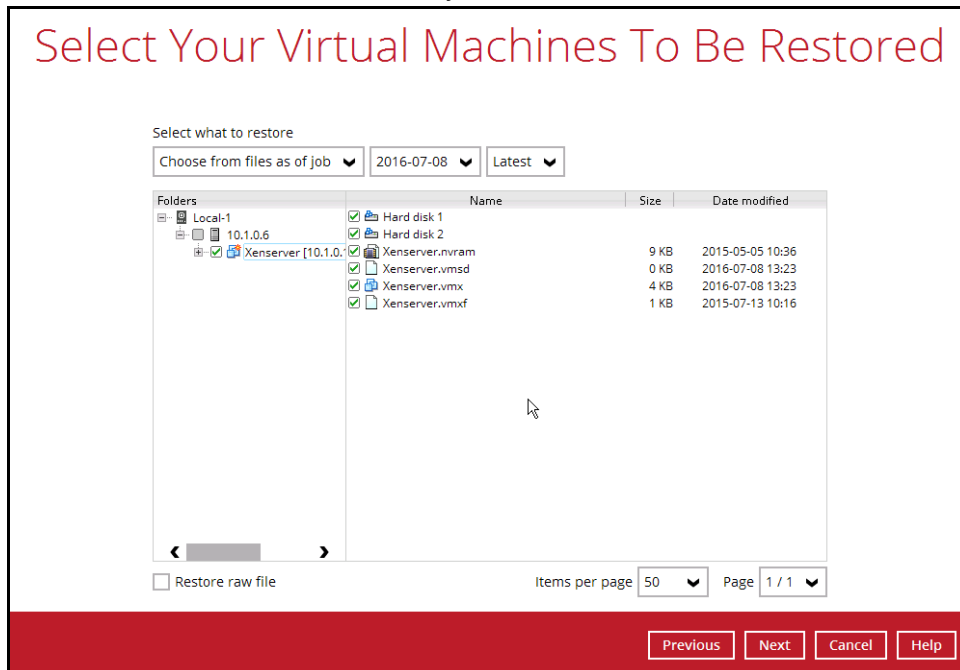


2. Select the backup set that you would like to restore the VM from.
3. Select the backup destination that contains the VM that you would like to restore.



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

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



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



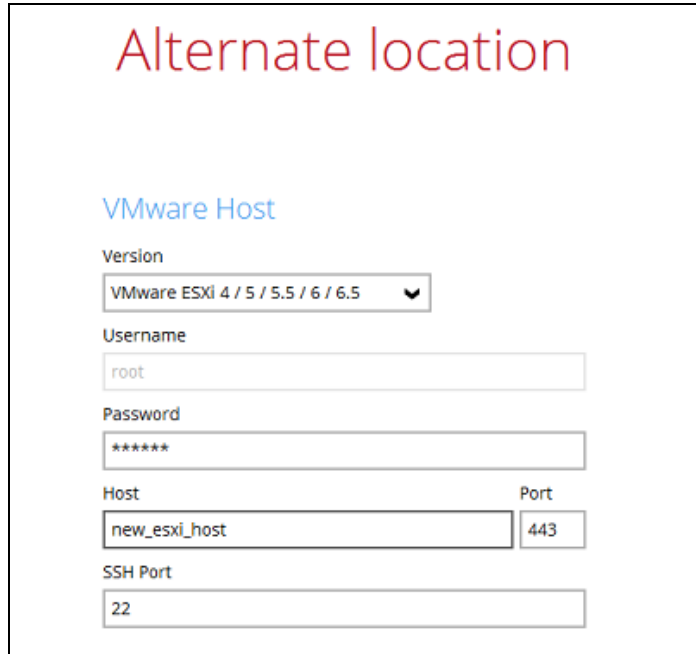
7. Disable **Run Direct**.



8. Click **Next** to proceed.



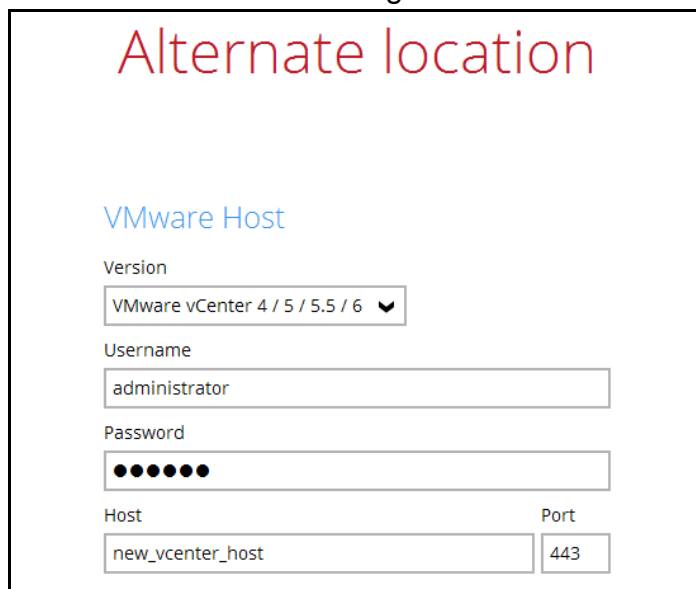
9. This step applies only for restoring to **Alternate location**. For restoring to **Original location**, skip to step 10.
- i. Enter the VMware host and access information of where you would like the VM to be restored to.
    - For restoration to another VMware ESXi host, select **Version VMware ESXi 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.



The screenshot shows a configuration window titled "Alternate location" in red text. Below the title is a section header "VMware Host" in blue. The form contains the following fields:

- Version:** A dropdown menu with the selected option "VMware ESXi 4 / 5 / 5.5 / 6 / 6.5".
- Username:** A text input field containing "root".
- Password:** A text input field containing "\*\*\*\*\*".
- Host:** A text input field containing "new\_esxi\_host".
- Port:** A text input field containing "443".
- SSH Port:** A text input field containing "22".

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



The screenshot shows a configuration window titled "Alternate location" in red text. Below the title is a section header "VMware Host" in blue. The form contains the following fields:

- Version:** A dropdown menu with the selected option "VMware vCenter 4 / 5 / 5.5 / 6".
- Username:** A text input field containing "administrator".
- Password:** A text input field containing "●●●●●●".
- Host:** A text input field containing "new\_vcenter\_host".
- Port:** A text input field containing "443".

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

- iii. 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

Inventory Location  
 **Browse**

Host/Cluster  
 **Browse**

Resource Pool  
 **Browse**

Storage  
 **Browse**

**Alternate location**

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

Name

Inventory Location  
 **Browse**

Host/Cluster  
 **Browse**

Resource Pool  
 **Browse**

Storage  
 **Browse**

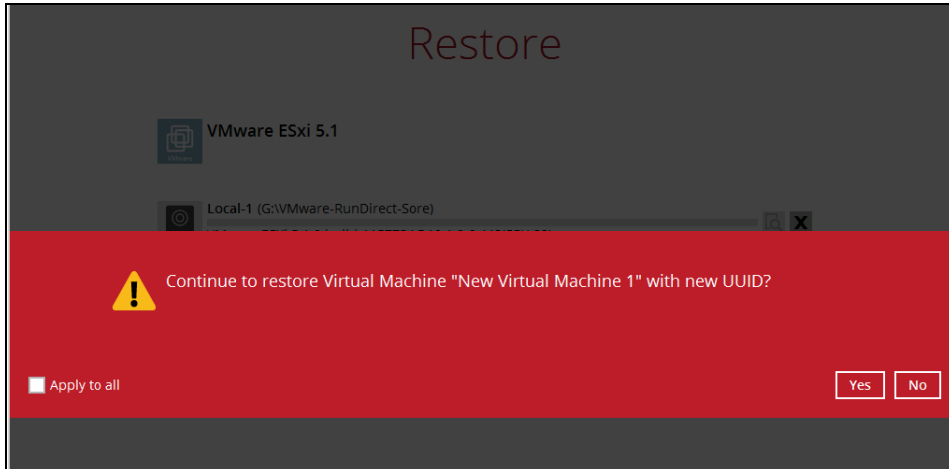
- iv. Click **Next** to proceed when you are done with the settings.
10. Select the temporary directory for storing temporary files.

**Temporary Directory**

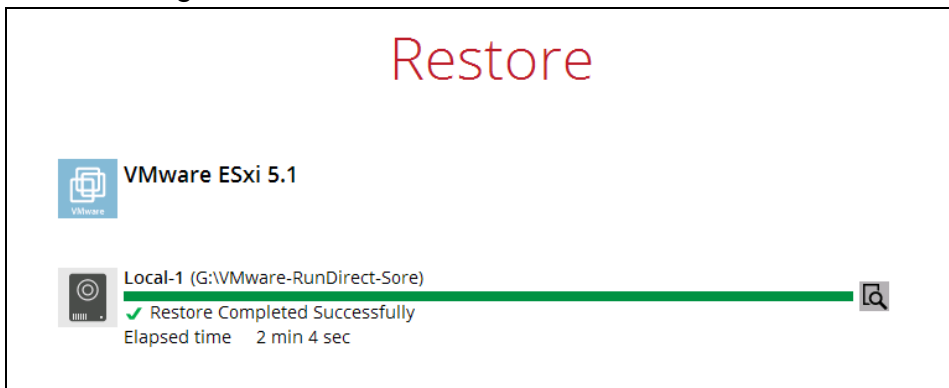
Temporary directory for storing restore files

**Browse**

11. When restoring your guest VM 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.



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



### Note

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

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

### Restoring a VM in VMDK format

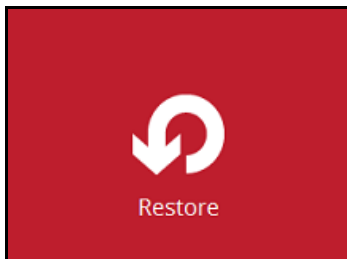
Since OBM v7.11.0.0, we have introduced a new feature to enable guest VMs that are backed up in VDDK mode to be restored in VMDK raw file format. This feature is useful if you wish to restore the backed up VM to another ESXi server even without using the OBM.

#### IMPORTANT

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

Follow the steps below for details.

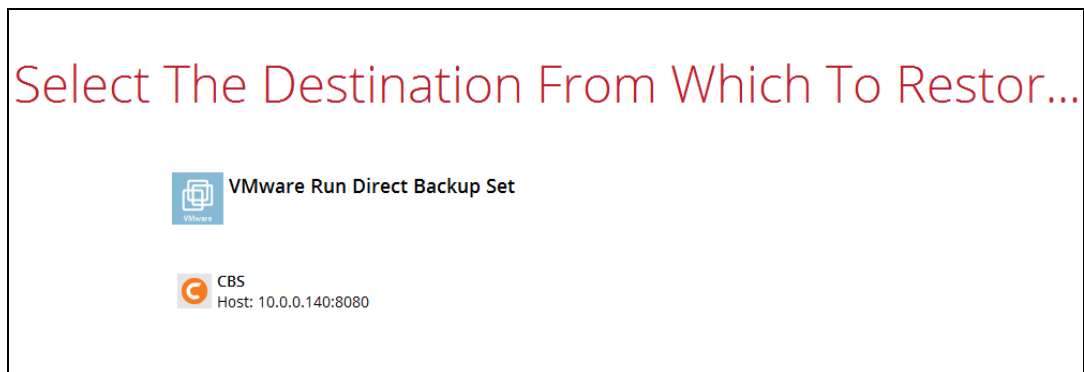
1. Click the **Restore** icon on the main interface of OBM.



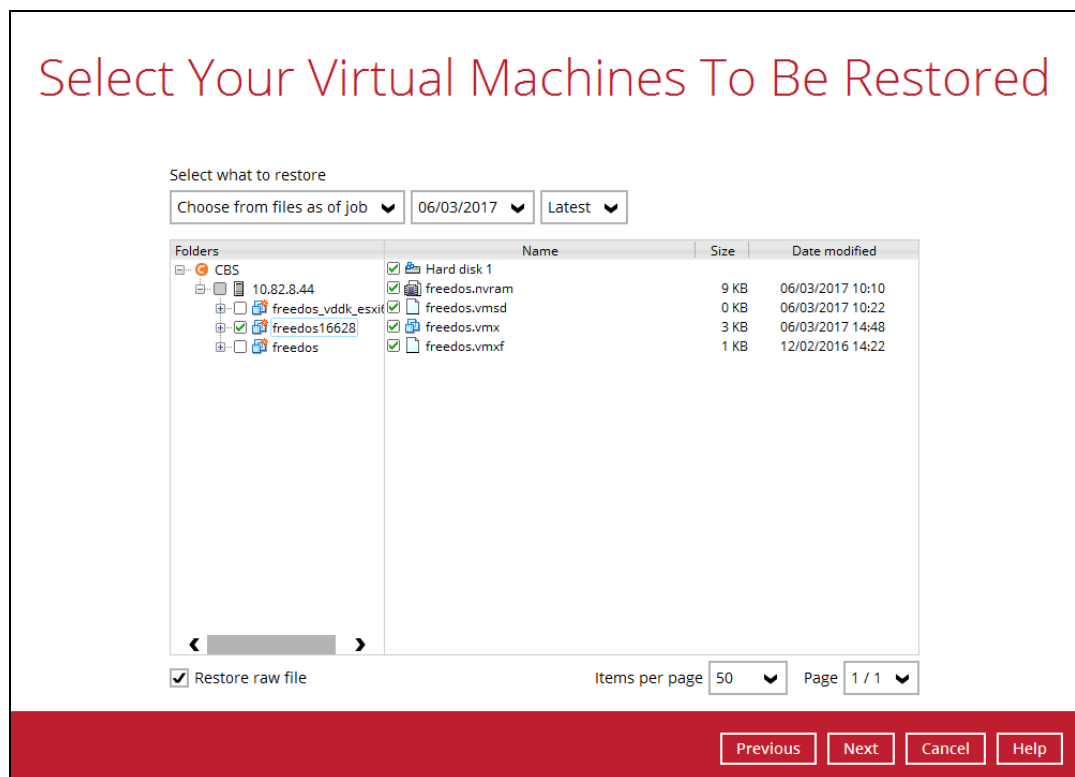
2. Select the backup set that you would like to restore the VM from.



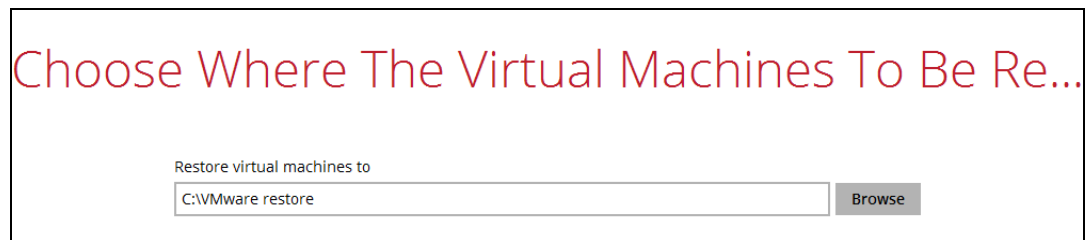
3. Select the backup destination that contains the VM that you would like to restore.



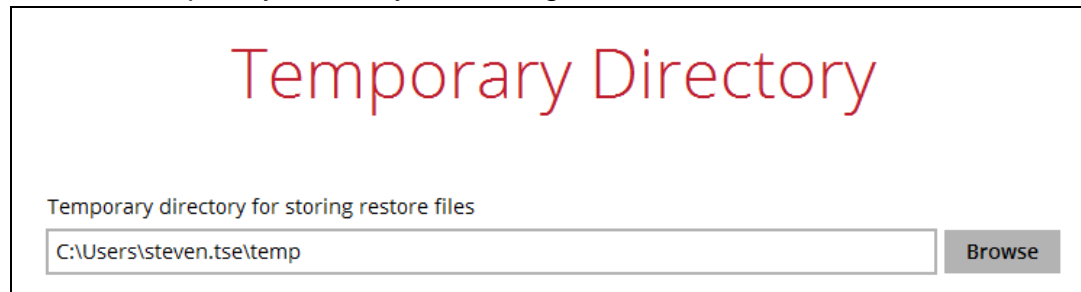
4. Select to restore VM from a specific backup job, or the latest job available from the **Select what to restore** drop down menu.
5. Select the virtual machine that you would like to restore in .vmdk format, then click the **Restore raw file** checkbox at the bottom left corner. It is possible to select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



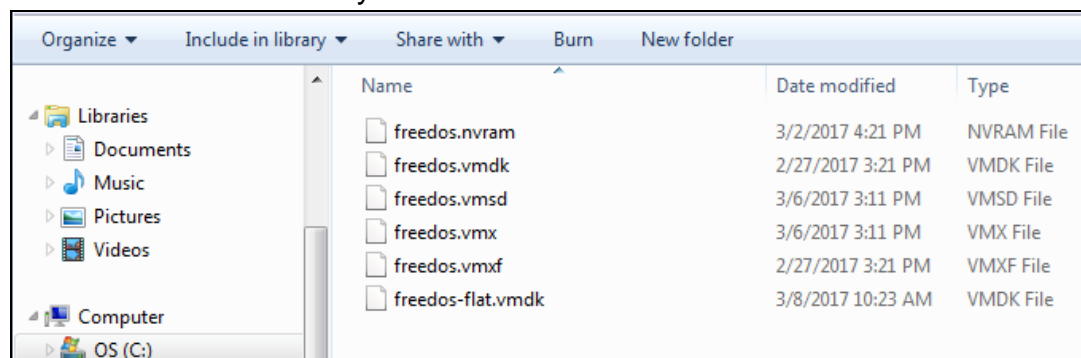
6. Select a location where you wish to restore the VM to. Click **Browse** to select a location and then click **Next** to confirm.



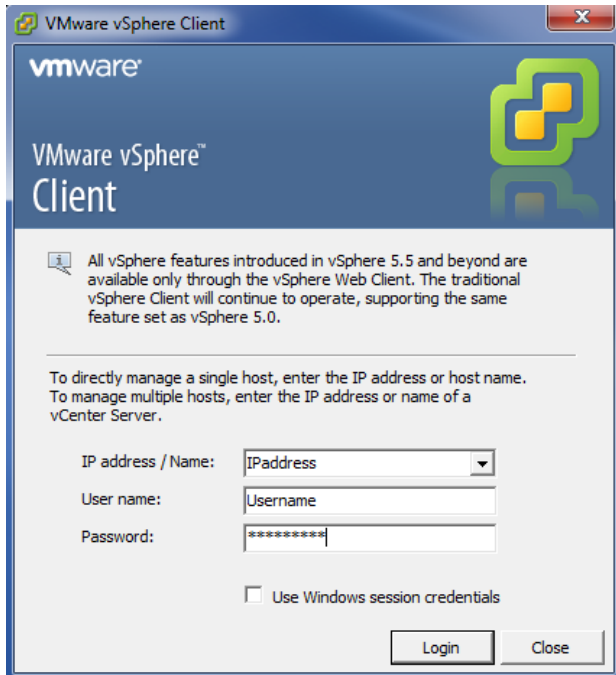
7. Select a temporary directory for storing restore files.



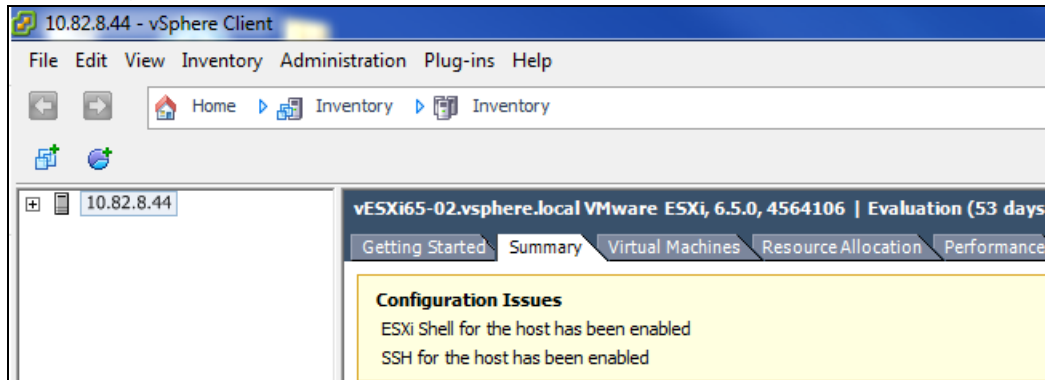
8. Click **Restore** to start the VM restore.
9. Open the folder where you have the VM restored. Check whether the .vmdk file has been successfully restored.



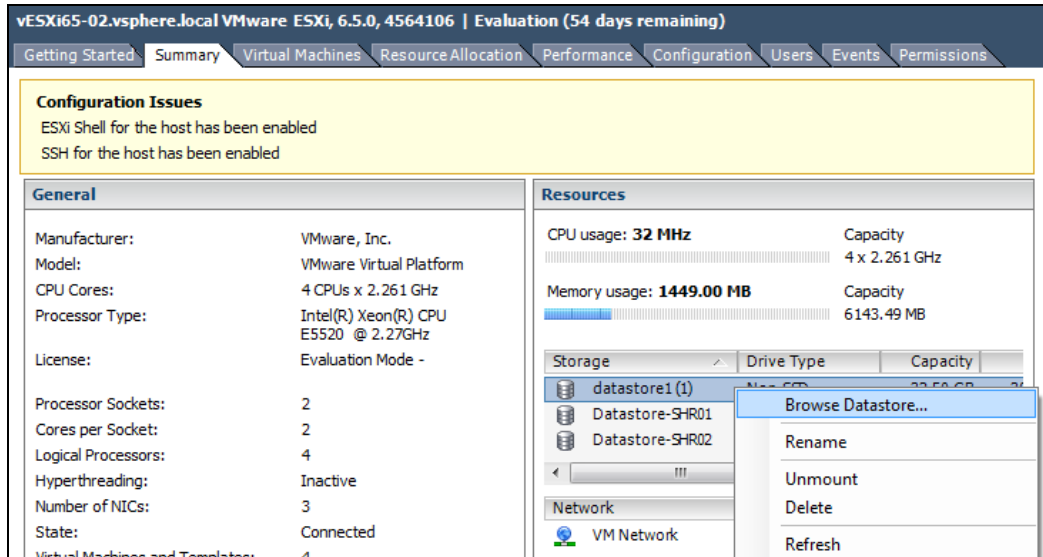
10. Open the VMware vSphere agent and log in to the Esxi server you wish to restore the VM to.



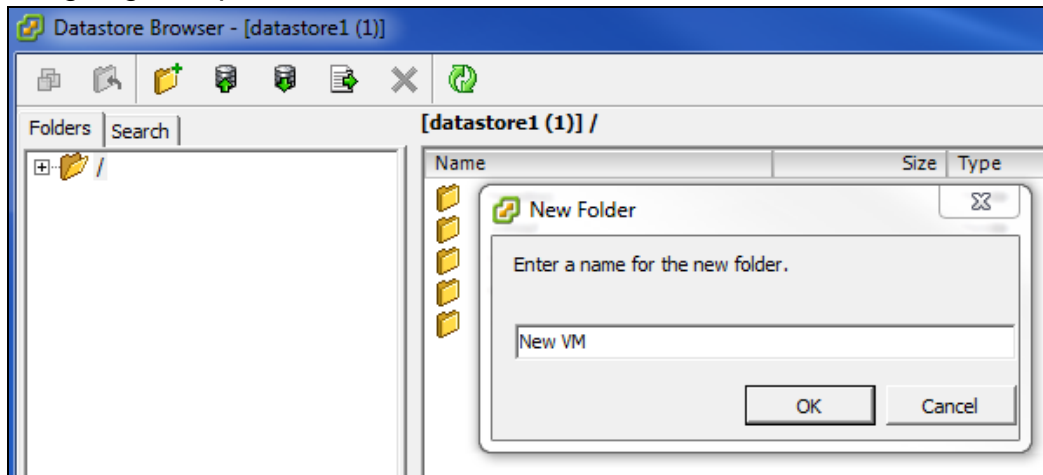
11. Click on the VM machine's name at the top, then look for the **Summary** tab on the right.



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

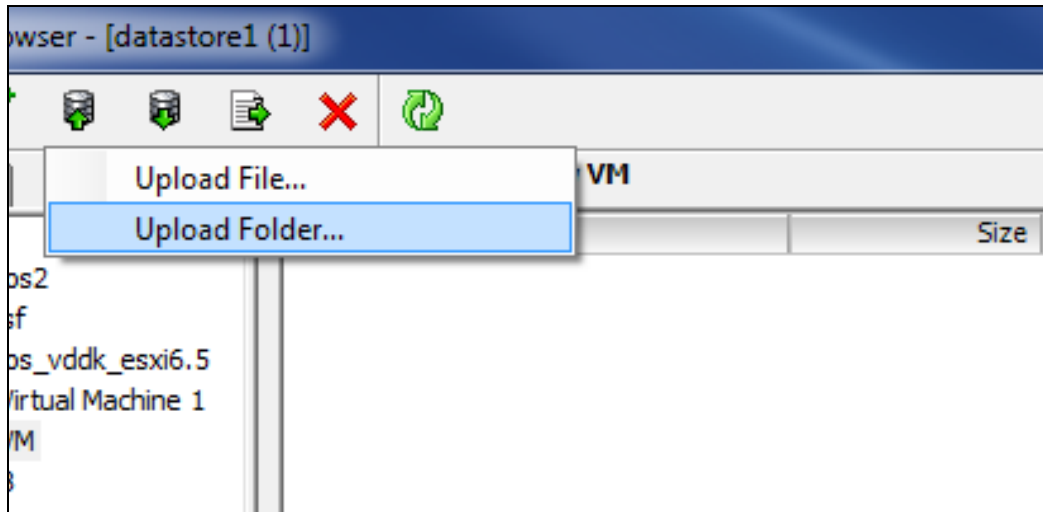


- Right click on the right panel to open a new folder for uploading the VM you are going to import.

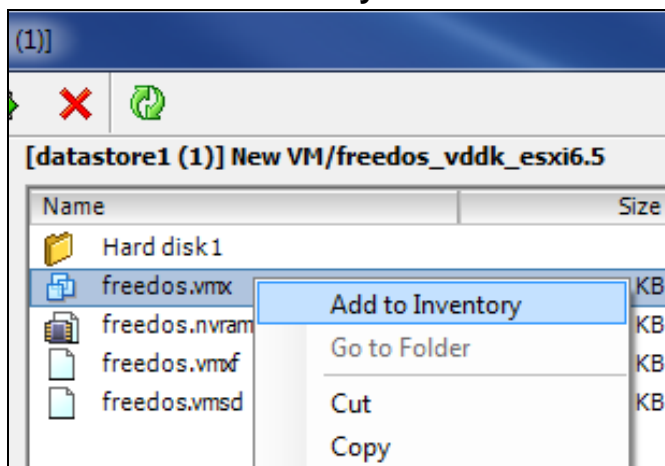




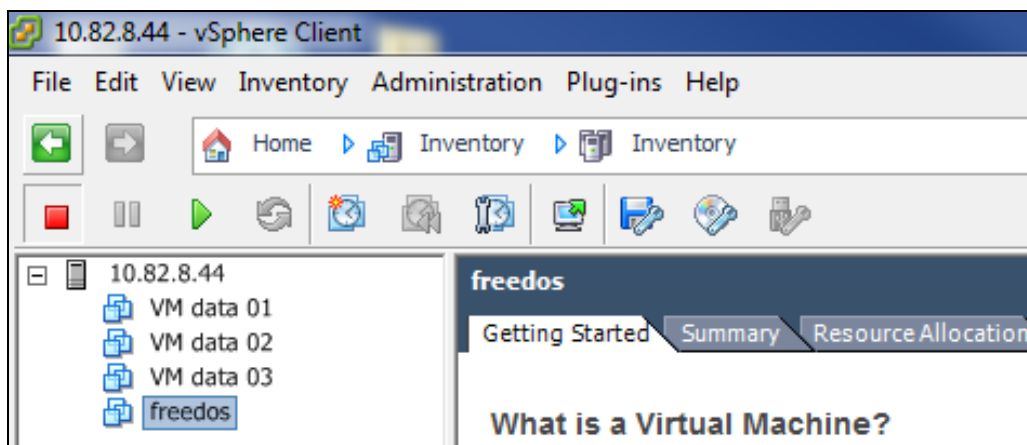
14. Open the newly created folder then click the Upload Folder option at the top menu bar to select the VM you wish to restore.



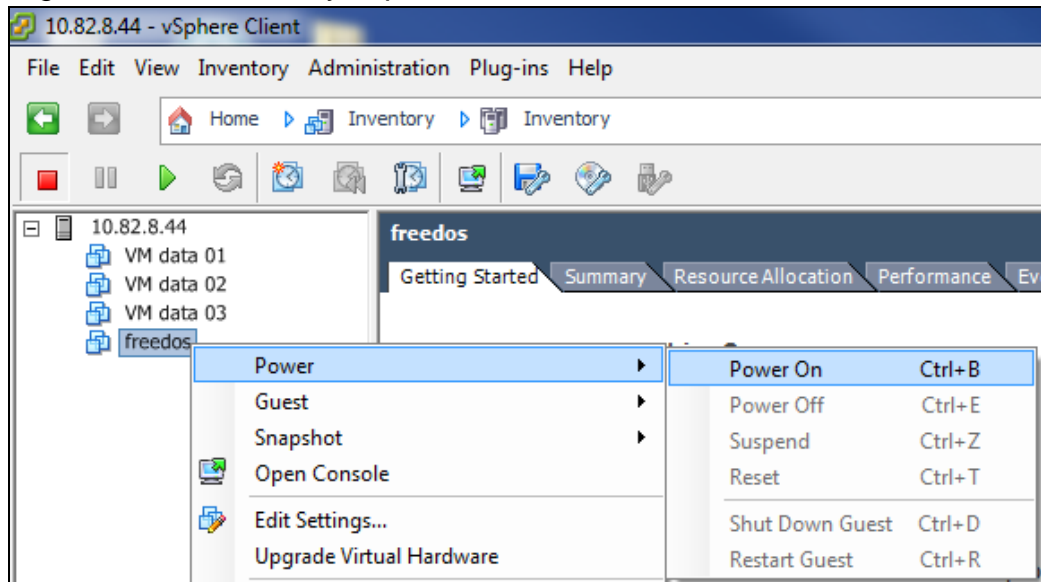
15. Open the folder you have just uploaded, then right click on the .vmx file and click on **Add to Inventory**.



16. 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.



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



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

