VMware Backup Set

AhsayOBM allows you to back up individual Guest virtual machines (VMs) on your VMware hosts with our VMware Backup Set. VMware Guest VM backup module of AhsayOBM provides you with a set of tools to perform hot backup of your running VMs in VMware environment.

When you need to restore a VM, besides restoring the whole VM image, you can also utilize the built-in Run Direct feature to spin-up the VM in minutes without the need to restore the whole VM first. Moreover, our Granular Restore feature allows you to mount the virtual disks in a backed up VM and restore individual files within the VM without the need to spin-up the VM first.

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.

Instant VM Restore with Run Direct

What is Run Direct?

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

How does Run Direct work?

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

The backup destination can either be the AhsayCBS server or a local drive that can connect with AhsayOBM. Initiating a Run Direct from the AhsayCBS (also known as agentless restore) will trigger a connection directly with the VMWare host (ESXi server and the direction shown in orange indicator

below), while initiating the same action on the AhsayOBM requires the connection to route through the OBM (shown in green indication below).

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

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:

1). VMware Snapshot

A VMware snapshot is created for the VM

2). Copying Files

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

3). Copying Changes

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

4). Data Consolidation

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

5). Resume VM

After all changes are consolidated, the VM is resumed.

6). Dismount NFS datastore

The NFS datastore is dismounted.

> 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.

Backup Mode

There are two backup modes available for VM backup:

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 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.

Pro	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.
Con	Require paid license, i.e. VMware Essentials License for usage of vSphere API.

Non-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 (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:

Pro	Free version of ESXi is supported.
Con	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.

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

Requirements

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.

License Specification

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

ESXi Shell Access

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

SSH

SSH must be enabled on the hypervisor (ESXi Server). To enable root SSH login on an ESXi host, please follow this instructions from VMware: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=8375637

Root Account

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

Port Requirement

For environment with firewall, the vCenter, ESXi servers and Backup Client Computer must be able to communicate with each other.

Ensure that ports 22, 80, 111, 443 and 902 allow outbound communication on the vCenter and ESXi servers. Refer to the link below for details on port usage:
https://kb.vmware.com/s/article/2012773 https://kb.vmware.com/s/article/2106283
https://kb.vmware.com/s/article/2039095 https://kb.vmware.com/s/article/2131180

> Ports 443 and 902 are default ports for VMware. If these have been changed from the default in your VMware environment, the firewall requirements will change accordingly.

Disk Space Available on Datastore

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

Maximum Virtual Disk Size

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

http://kb.vmware.com/kb/1003565

VMware Tools

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

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

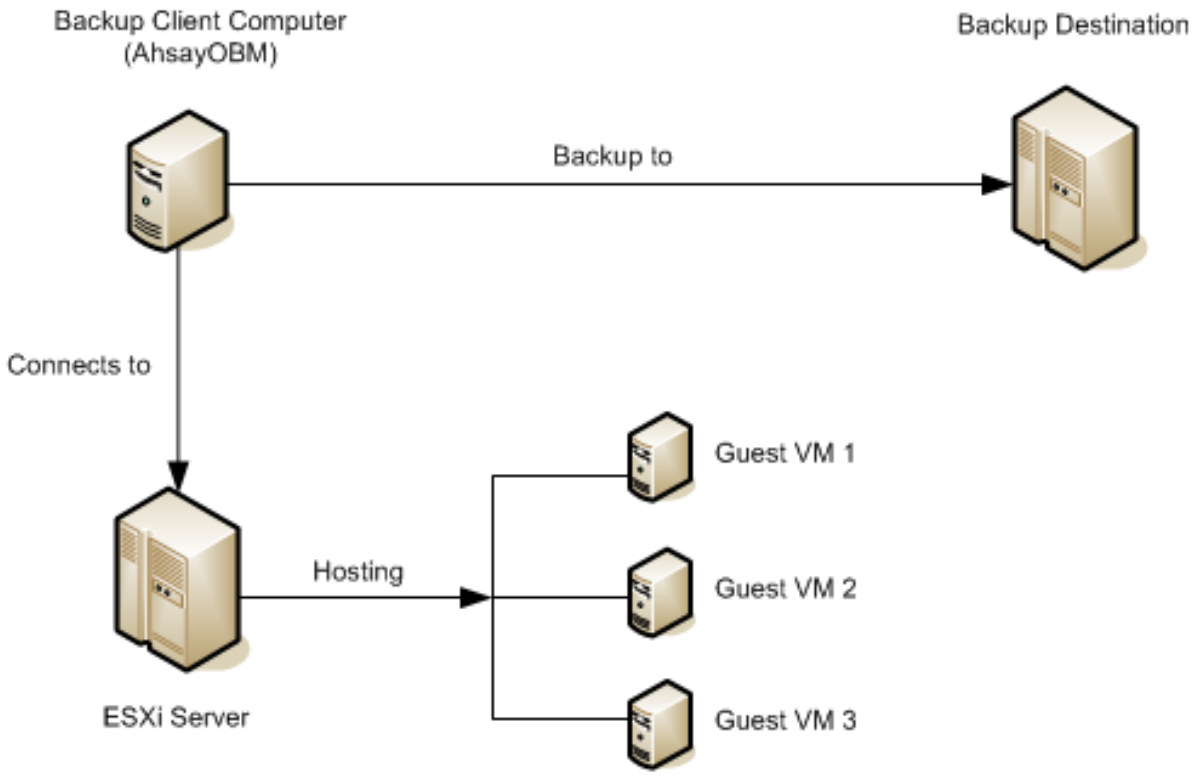
ESXi/ESX Hosts and Virtual Machine Hardware Versions Compatibility

Refer to this link 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)

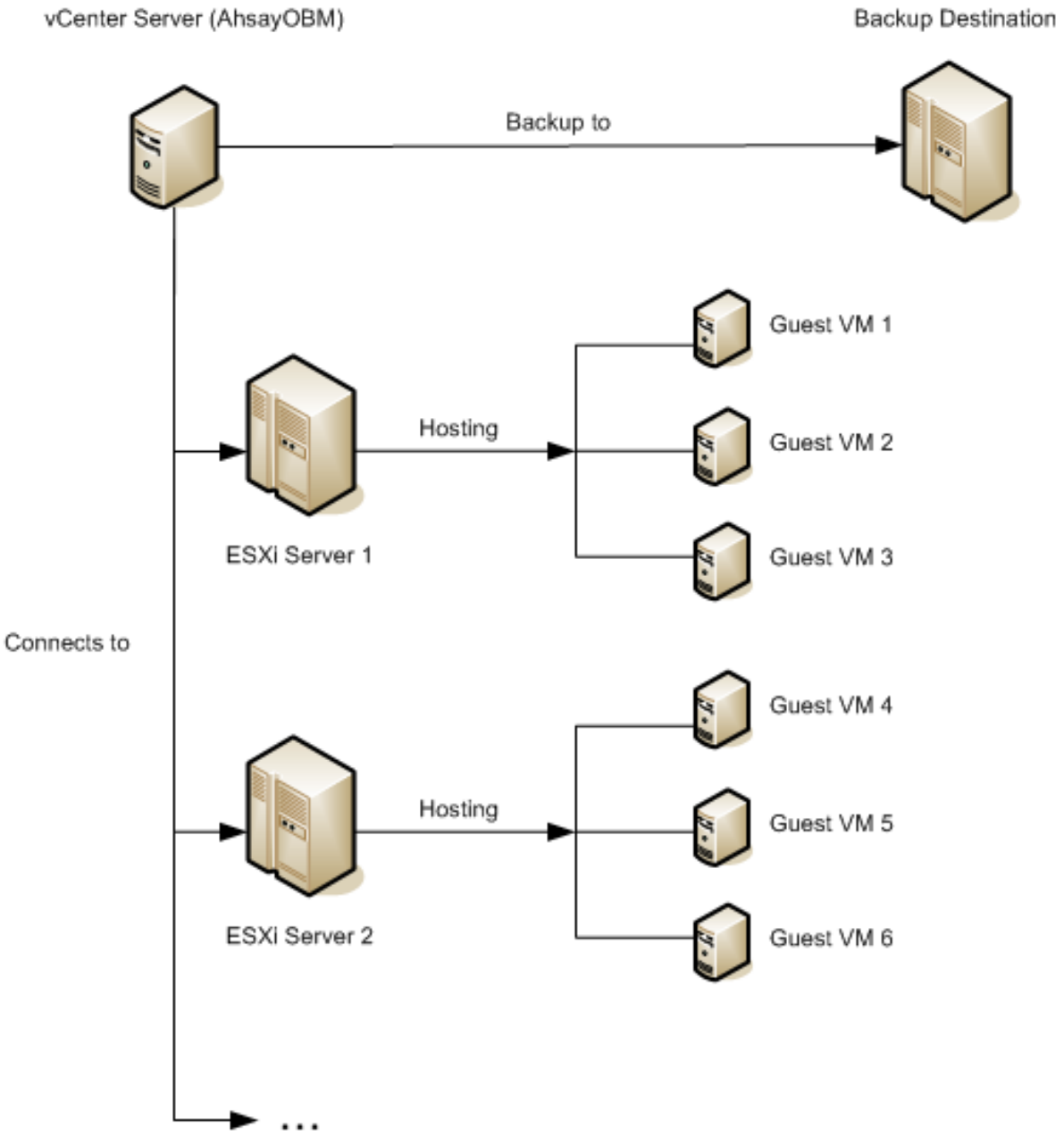
Backup Client Computer Requirements

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 Requirement

- Refer to this Hardware Requirement List for the list of hardware requirements for AhsayOBM.

Software Requirement

- Refer to this Software Compatibility List for Granular Restore in VMware backup sets.

Antivirus Exclusion Requirement

- To optimize performance of AhsayOBM on Windows, and to avoid conflict with your antivirus software, refer to this article for the list of processes and directory paths that should be

added to all antivirus software white-list / exclusion list.

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

Port Requirement

For environment with firewall, the vCenter, ESXi hosts and Backup Client Computer must be able to communicate with each other.

Make sure that ports 22, 80, 111, 443 and 902 allow outbound communication on the Backup Client Computer. Refer to the link below for details on port usage:
https://kb.vmware.com/s/article/2012773 https://kb.vmware.com/s/article/2106283
https://kb.vmware.com/s/article/2039095 https://kb.vmware.com/s/article/2131180

> 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.

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

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

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

(Total File Size * Delta Ratio) * number of backup destinations = Maximum Free Space Required

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

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

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).

Enabled Add-on Module in AhsayCBS

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.

Run Direct Requirements

Run Direct is a feature that helps reduce disruption and downtime of your production VMs. 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 (Virtual Disk Development Kit) for ESX/ESXi and vCenter setup. With VDDK mode, the backup speed is enhanced because the generation of the delta file of the VM are performed directly by the ESX/ESXi or vCenter itself. For being able to backup in VDDK mode, AhsayOBM must be installed on a supported Windows operating system platform.

License Requirement

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

> 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).

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

VMware Snapshot

VDDK backup mode does not support backup of virtual machine snapshot. For backup of individual virtual disk, the restored virtual machine does not support the reversion of previous snapshots, if the snapshot contains disks which are not previously backed up by AhsayOBM.

Virtual Machine State

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

File Name Requirement

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

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

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

Backup Destination

When a Run Direct restore is performed, the backup destination containing the guest VM files is mounted on the VMware host as NFS datastore.

Ensure that the following requirements are met by the backup destination of the VMware VM backup set:

- Destination must be accessible to the VMware host.
- Destination must have sufficient disk space available for the Run Direct restore. There should be 1.5 x total provisioned size of all VMs selected for backup.
- For Run Direct restore of 1 VM with provisioned size of 100GB, there should be 150GB (e.g. 1.5 x 100GB) of free space available in the Destination.

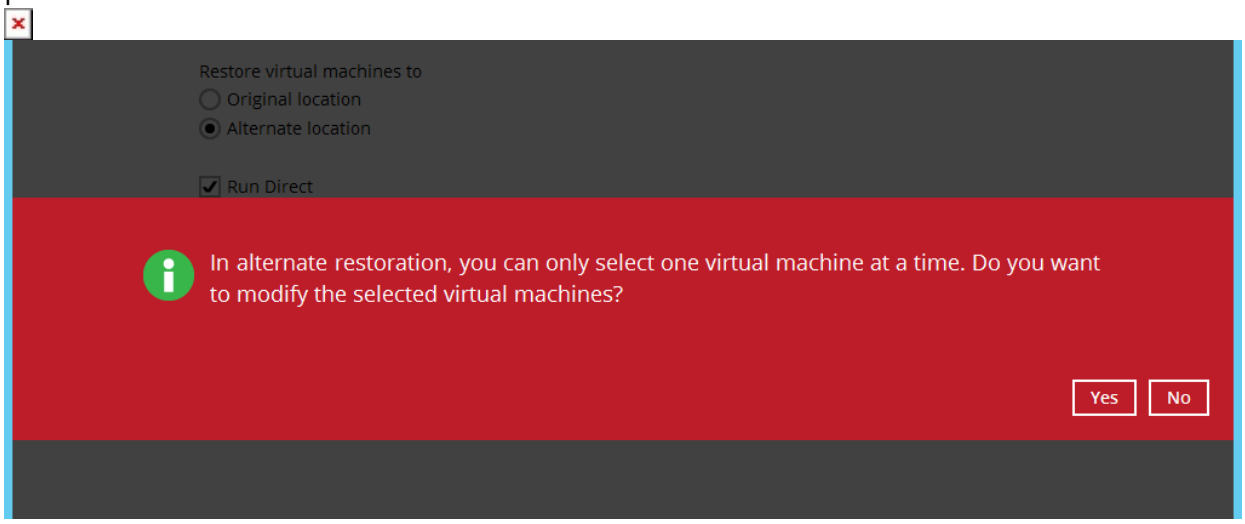
No Compression and Encryption - Data backed up to a Run Direct enabled destination is not compressed or encrypted to optimize restore performance as Run Direct will make the VM restored by running the data directly form the backup files in the backup destination.

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.



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

Dedicated NFS Service - A dedicated AhsayOBM NFS Windows service is introduced to allow Run Direct session to continue even if the AhsayOBM user interface is closed. By default, the AhsayOBM NFS service is started as Local System, which does not have sufficient permission to access any network resources (e.g. the AhsayOBM NFS service does not have sufficient permission to access the VM backup files on network drive). Make sure that the Log on setting of the Ahsay Online Backup Manager NFS Service is configured with an account with sufficient permission to access the network backup destination where the backed up VM data are stored.

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

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.

Best Practices and Recommendations

Please consider the following recommendations for running VMware backup:

Use the latest version of AhsayOBM

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

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

Install AhsayOBM on a physical staging machine

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

VMware Tools

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

Quiescing is a process that ensures that the disk data is in a state suitable for backups to reduce the possibility of data corruption upon restore. This is especially important for transaction-based applications running on VMs like MS SQL Server, MS Exchange etc. There are different types of

quiescing mechanisms, according to the guest operating systems (e.g. Crash-consistent, File-system-consistent and Application-consistent quiescing).

Do not use a guest VM as a staging machine

Although installing AhsayOBM on a guest VM as a staging machine is possible, the backup and restore will work as on a physical staging machine. This setup is actually inefficient and can lead to possible performance bottlenecks on the VMware host server, as in a VMware host the virtualization layer separates guest VM OS layer and the VMware host physical hardware layer. As the guest VM operating system does not have direct access to physical hardware where the data resides, a backup agent installed inside the guest VM must go through the virtualization layer to access the guest virtual machine data.

Use the VDDK backup mode / CBT feature

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

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

Proper use of Temporary Directory

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 this article for how to setup the temporary directory for your VMware backup set.

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

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

Backup the guest VMs to more than one destination

To provide maximum data protection and recovery flexibility you should consider to store your guest

VM backups in multiple backup destinations, ideally both onsite and offsite locations. Onsite locations on local or network drives will enable very quick recovery even for large guest VMs. While offsite locations will ensure that if there is a site outage, the guest can be restored from another location.

Proper Java memory allocation

Consider to increase the Java memory allocation setting for AhsayOBM (Java heap space) if you are using non-VDDK backup mode. If you are using non-VDDK mode and or Granular restore, it is recommended to increase the Java heap size space to at least 2GB or above for optimal performance. Refer to this KB article for how to modify Java heap size for your AhsayOBM client.

Backup whole VM

It is highly recommended to backup the whole VM instead of individual disk for backup of virtual machine with snapshot.

Routine recovery test

Consider to perform routine recovery test to ensure your backup is setup and performed properly.

Disable the memory snapshot or quiesce guest options

Consider to disable the memory snapshot or quiesce guest options when taking snapshot for VMware VM backup, to shorten the time required for the process.

- Snapshot the virtual machine's memory
- Quiesce guest file system (Needs VMware Tools installed)

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. Click here to read the details.

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

Documentation

- VMware Backup and Restore Guide

FAQs

- How to create a VMware backup set to be used with the Run Direct feature?
- How to instantly startup a VMware virtual machine with the Run Direct feature (with migration)?
- How to instantly startup a VMware virtual machine with the Run Direct feature (without migration)?

Issues

- Incorrect error message 'Another backup job is still running' is displayed (VMware VM backup)
- VMware VM backup job cannot run to completion (for backup set with backup schedule disabled)
- Guest virtual machines are not listed in AhsayOBM backup source when creating a VMware Workstation backup set
- "Cannot connect SSH, please check the SSH settings" error when creating a backup set on a VMware ESXi 6.0 Update 2 host
- VMware VM cannot start up properly with Operation System not found error (Run Direct restore failing when the backup destination is located on a network drive)
- When perform a VMware Run Direct restore on AhsayOBM the following error is shown “The NFS Service on this machine is not started or not functioning properly. This service is required for VM Run Direct.
- "Cannot connect SSH, please check the SSH settings" error when creating a backup set on a VMware ESXi host
- Unable to find vmrun.exe in "‘C:\Program Files (x86)\VMware\VMware Player’ or ‘C:\Program Files (x86)\VMware\VMware VIX’” when creating a VMware Workstation BackupSet
- ISSUE:"The specified virtual machine could not be found." warning is shown on VMware Workstation scheduled backup job
- ISSUE:"Reason = "UUID conflict on Virtual Machine." error is shown on VMware ESXi backup job
- VMware ESXi scheduled backup job missed with 'Current license or ESXi version prohibits execution' error
- VMware ESXi/vCenter VDDK mode backup job ends with "Error=Snapshot not taken since the state of the virtual machine has not changed since the last snapshot operation."
- “Hostname cannot be empty” error is shown when starting VMware Run Direct restore from AhsayCBS web console
- ISSUE:"Failed to restore "New Virtual Machine". Reason = "Fail to set entity permission. Error=Unknown error from class "com.vmware.vim25.UserNotFound" when restoring a guest VM to another VMware ESXi host
- ISSUE:"No backup set can start Run Direct" message shown when initiating a VMware ESXi/vCenter Run Direct restore on AhsayCBS user web console
- "IP address "xxx.xxx.xxx.xxx" of the VirtualCenter server managing this host. Please either connect this host through it or disconnect this host from it." error is shown when creating a VMware ESXi backup set
- "[CloudException.ConnectFailedExpt[SFtpManager.login] Failed to access SFTP" error when

create VMware ESXi backup set
- ISSUE:"Falied to list file (the media is write protected" when mounting a VMware ESXi/vCenter Window 10 guest VM virtual disk using Granular Restore
- "Access is denied" error when restoring files/folders using Granular Restore