



# Microsoft Hyper-V Guest Virtual Machine Backup & Restore Guide

**Disclaimer:**

QuikCloud Ltd 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 QuikCloud Ltd without prior notice to you.

## Contents

<i>What is this software?</i> .....	3
System Architecture.....	3
<i>Preparation and Prerequisites</i> .....	4
Antivirus Exclusions.....	4
QCBM .....	4
<i>Hyper-V Server Requirements</i> .....	6
<i>Hyper-V Backup Methods</i> .....	9
VM Snapshot.....	9
VM Snapshot Method requirements.....	9
Saved State.....	9
CBT Requirement.....	10
<i>Windows Server 2016 Requirement</i> .....	11
RCT Requirement.....	11
Guest VM Dependencies Requirements.....	11
Limitations .....	12
<i>Run Direct</i> .....	13
What is Granular Restore Technology? .....	14
Benefits of using Granular Restore .....	15
Requirements .....	16
License Requirements.....	16
Backup Quota Storage .....	16
Operating System.....	16
Temporary Directory Requirement .....	17
Available Spare Drive Letter.....	17
Network Requirements .....	17
Other Dependencies.....	17
Permissions .....	17
<i>Creating a Hyper-V Backup Set</i> .....	18
Non-Cluster Environment.....	18
Non-Run Direct Backup Set .....	20
Cluster Environment .....	23
Requirements.....	23
For Hyper-V Cluster backup sets.....	23
Run Direct Backup Set.....	23
Non Run Direct Backup Set .....	26



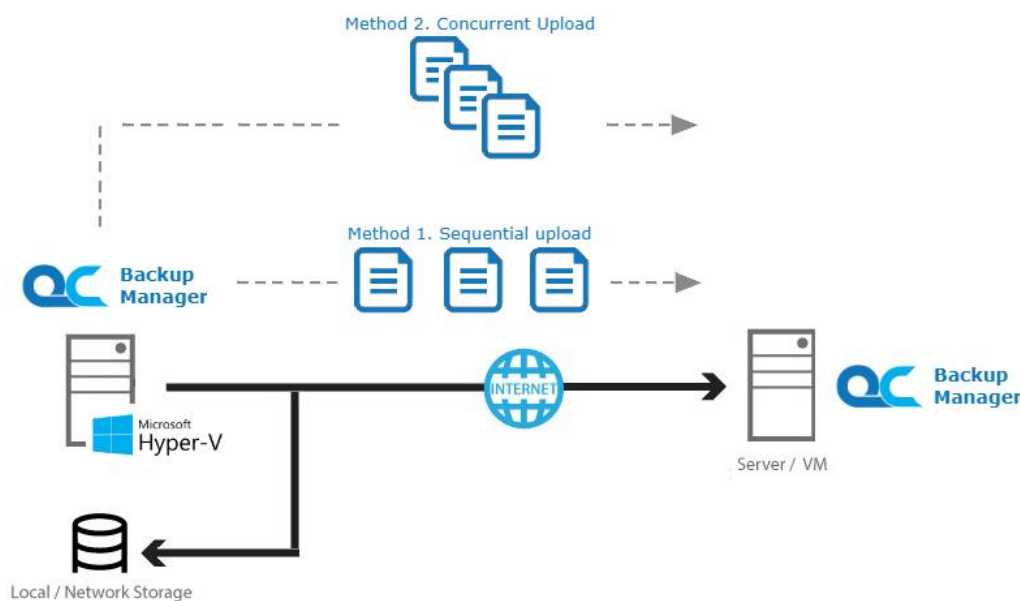
## What is this software?

QuikCloud brings you specialized client backup software, namely QCBM, to provide a comprehensive backup solution for your Hyper-V host machine backup. The Hyper-V module of QCBM provides you with a set of tools to protect Hyper-V host machine and guest VMs. This includes a machine backup feature and instant recovery feature (with the use of Run Direct technology), to ensure that mission critical machines are back up and running within minutes of a disaster.

## System Architecture

The following high-level system architecture diagram illustrates the major elements involved in the backup process of a Hyper-V host with QCBM.

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



## ***Preparation and Prerequisites***

Before any backup sets are created, you must ensure that the following has been met.

### ***Antivirus Exclusions***

To optimise performance of the QCBM client on Windows and to avoid conflict with your antivirus software. Please ensure the following paths are excluded from any real-time or scheduled scans.

- \Program Files\QCBM
- \Users\%user%\obm
- \%temp path location%

### ***QCBM***

1. QCBM is installed on the Hyper-V server. For Hyper-V Cluster environment QCBM is installed on all Cluster nodes.
2. The operating system account for setting up the Hyper-V / Hyper-V Cluster backup set must have administrator permission (e.g. administrative to access the cluster storage).
3. For Granular Restore, Windows User Account Control (UAC) must be disabled.
4. QCBM user account has sufficient Hyper-V add on modules or CPU sockets assigned. Hyper-V Cluster backup sets will require one QCBM license per node. (Please contact your backup service provider for details)
5. QCBM user account has sufficient quota assigned to accommodate the storage of the guest virtual machines. (Please contact your backup service provider for details).

Hyper-V guest virtual machines contain three types of virtual disks:      Fixed Hard Disk.

- Dynamic Hard Disk.
- Differencing Hard Disk.

When QCBM backs up a Hyper-V guest virtual machines for an initial or subsequent full backup jobs:

- Using fixed Hard Disks it will back up the provisioned size, e.g. for a 500GB fixed virtual hard disk 500GB will be backed up to the storage designation.
  - Using Dynamic Hard Disk or Differencing Hard Disk it will back up the used size, e.g. for a 500GB fixed virtual hard disk, 20GB will be backed up to the storage designation if only 20GB are used.
6. Since version 7.13, the default Java heap size setting on QCBM is 2048MB, for Hyper-V backups it is highly recommended to increase the Java heap size setting to improve backup and restore performance. (The actual heap size is dependent on amount of free memory available on your Hyper-V server).

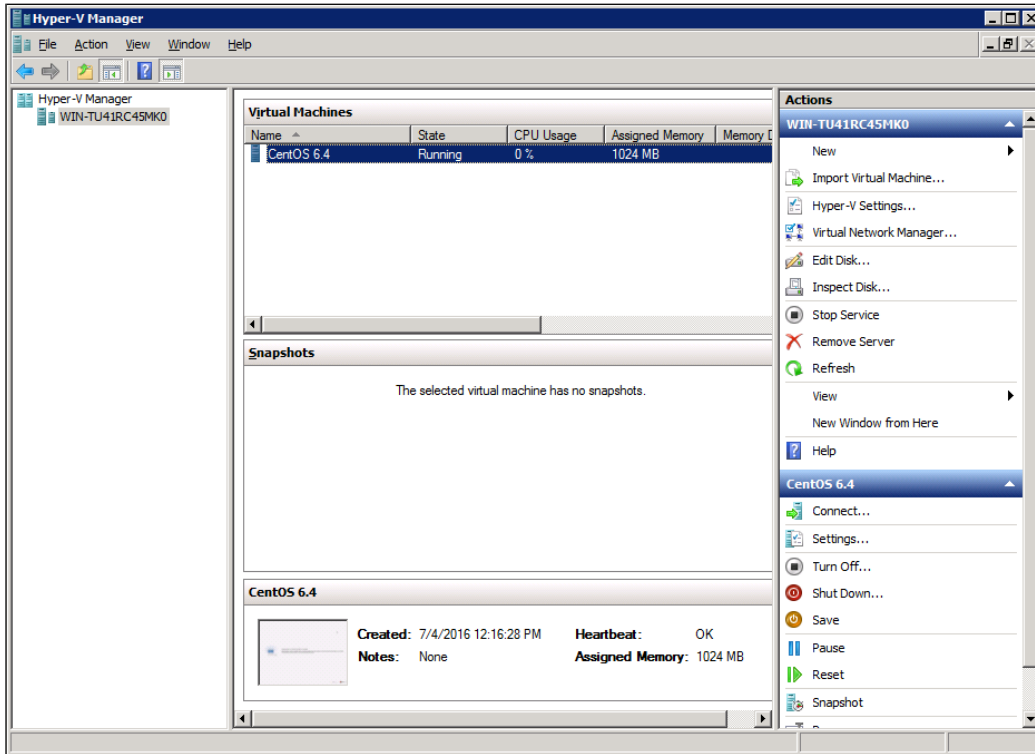
Delta generation of large VHD files is a memory intensive process; therefore, it is recommended that the Java heap size to be at least 2048MB - 4096MB. The actual required Java heap size is subject to various factors including files size, delta mode, backup frequency, etc.

7. For stand-alone Hyper-V server, QCBM uses the temporary folder for storing backup set index files and any incremental or differential delta files generated during a backup job. To ensure optimal backup / restore performance, it should be located on a local drive with plenty of free disk space. It should not be on the Windows system C:\ drive.  

Note: For Hyper-V server in Failover Cluster environment, the temporary folder must be set to a network shared path accessible to all cluster nodes, or a Cluster Shared Volume.
8. QCBM UI must be running when a guest virtual machine is started using Run Direct Restore or when migration process is running.
9. For local, mapped drive, or removable drive storage destinations with Run Direct enabled, the compression type will always be set to No Compression and data encryption is disabled to ensure optimal backup and restore performance. The backup set compression type and data encryption settings will only be applied to CBS, SFTP/FTP, or Cloud storage destinations.
10. For ease of restore it is recommended to back up the whole guest machine (all the virtual disks) rather than individual virtual disks.
11. Make sure NFS service has started for Run Direct to operate. If the backup destination is located on network drive, the logon must have sufficient permission to access the network resources.

## Hyper-V Server Requirements

1. The Hyper-V management tools are installed on the server. For Hyper-V Cluster environments Hyper-V management tools is installed on all Cluster nodes.



2. The Hyper-V services are started on the server. For Hyper-V Cluster environments the Hyper-V services are started on all Cluster nodes
3. The Microsoft Hyper-V VSS Writer is installed and running on the Hyper-V server and the writer state is Stable. This can be verified by running the vssadmin list writers command.

```
C:\Users\Administrator>vssadmin list writers
vssadmin 1.1 - Volume Shadow Copy Service administrative
command-line tool
.....
.....
.....
.....

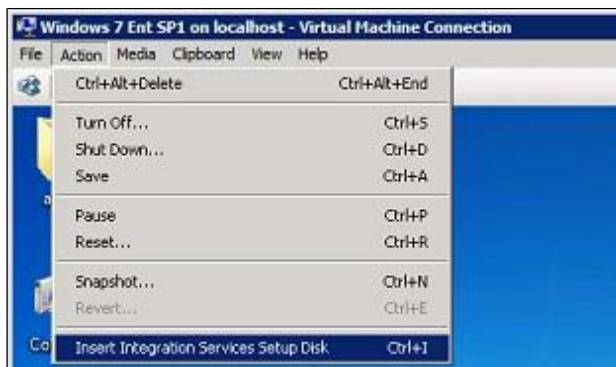
Writer name: 'Microsoft Hyper-V VSS Writer'
Writer Id: {66841cd4-6ded-4f4b-8f17-fd23f8ddc3de}
Writer Instance Id: {a51919e3-0256-4ecf-8530-
2f600de6ea68}
| State: [1] Stable Last error: No error
```

## 4. Integration Service

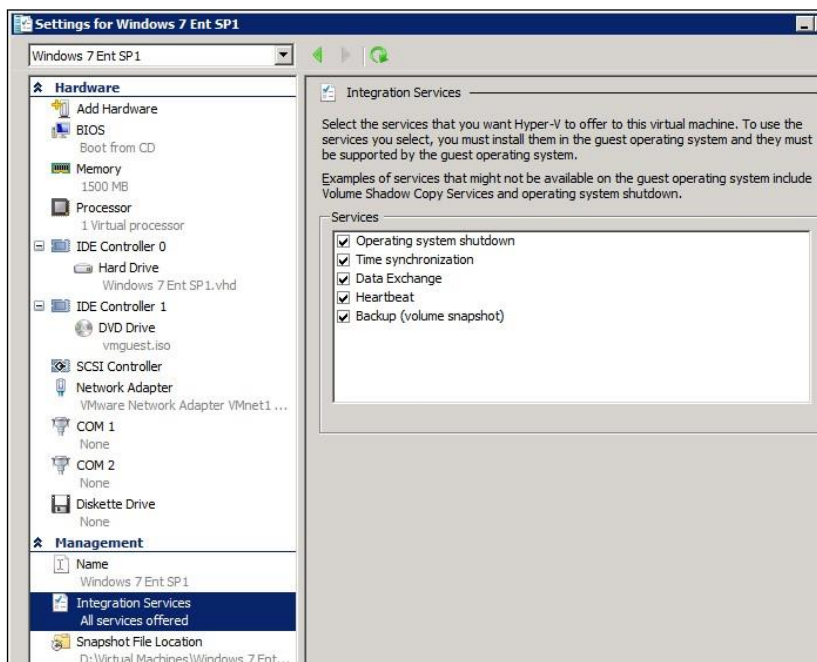
- i. If Integration services is not installed / updated on a guest virtual machine or the guest operating system is not supported by Integration Services, the corresponding virtual machine will be paused or go into a saved state during the snapshot process for both backup and restore, and resume when the snapshot is completed. Furthermore, the corresponding virtual machine uptime will also be reset to 00:00:00 in the Hyper-V Manager.
- ii. Installing or updating Integration Services guest virtual machine(s) may require a restart of the guest virtual machine to complete the installation.

- To install Integration Services.
- In Hyper-V Manager connect to the guest virtual machine and select Action > Insert Integration Services disk

Example: Windows 7 Enterprise guest

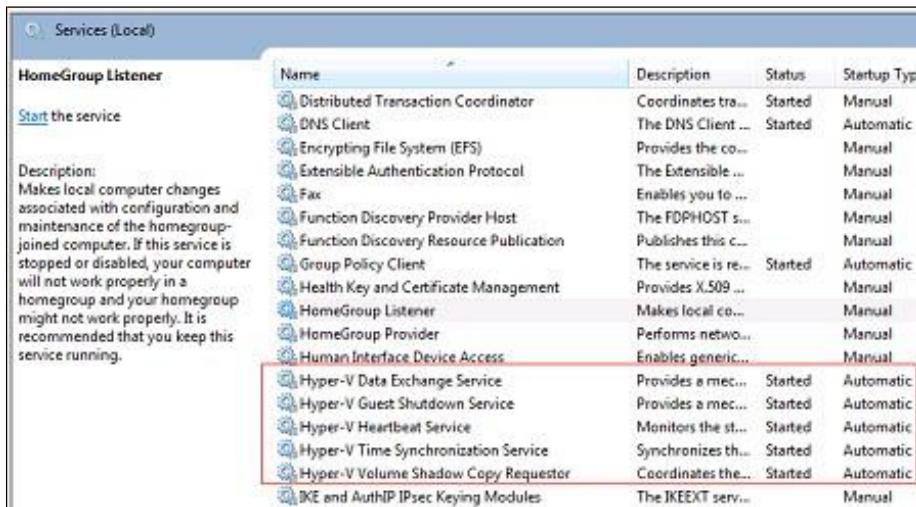


- If the guest operating system supports live virtual machines backup, the Backup (volume checkpoint) is enabled.





- The related Integration Services are running on the guest virtual machine:  
Example: Windows 7 enterprise guest



- Please refer to the following articles for further details on:
  - Considerations for backing up and restoring virtual machines  
<https://technet.microsoft.com/en-us/library/dn798286.aspx>
  - Supported Windows Guest Operating Systems for Hyper-V in Windows Server 2012  
[https://technet.microsoft.com/en-us/library/dn792028\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn792028(v=ws.11).aspx)
  - Supported Windows Guest Operating Systems for Hyper-V in Windows Server 2012 R2  
[https://technet.microsoft.com/en-us/library/dn792027\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn792027(v=ws.11).aspx)
  - Supported Linux and FreeBSD virtual machines for Hyper-V  
<https://technet.microsoft.com/library/dn531030.aspx>
  - Linux Integration Services Version 4.0 for Hyper-V  
<https://www.microsoft.com/en-us/download/details.aspx?id=46842>
  - Managing Hyper-V Integration Services  
[https://msdn.microsoft.com/en-us/virtualization/hyperv\\_on\\_windows/user\\_guide/managing\\_ics](https://msdn.microsoft.com/en-us/virtualization/hyperv_on_windows/user_guide/managing_ics)

5. For Hyper-V 2008 R2 server in order to use Run Direct restore feature the "Microsoft Security Advisory 3033929" security update must be installed.

Please refer to the following KB article from Microsoft for further details:  
<https://support.microsoft.com/en-us/kb/3033929>

6. For Run Direct Hyper-V Cluster backup sets the storage destination must be accessible by all Hyper-V nodes.
7. For Hyper-V Cluster backup sets the guest virtual machines must be created and managed by the Failover Cluster Manager.



## Hyper-V Backup Methods

QCBM v7 Supports two methods for Hyper-V guest VM backup, VM Snapshot and Saved State.

### VM Snapshot

The VM snapshot method is the preferred backup option, as it supports live guest VM backups. This means guest VM will not be put into a saved state when a VSS snapshot is taken during a backup job. So, it will not affect the availability of any applications or services running on the guest VM every time a backup job is performed.

**Note: if the VM Snapshot method cannot be used, the QCBM will automatically use the Saved State method.**

### VM Snapshot Method requirements

1. The guest VM must be running.
2. Integration services must be enabled on the guest VM.
3. The Hyper-V Volume Shadow Copy Requestor service is running on the guest VM installed with Windows operating system. Please refer to the following article for further details: <https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/reference/integration-services#hyper-v-volume-shadow-copy-requestor>
4. For guest VMs installed with Linux / FreeBSD operating systems, the VSS Snapshot daemon is required for live backups, not all Linux / FreeBSD versions support live backup on Hyper-V. For example, only FreeBSD 11.1 supports live backup while for Ubuntu, version 14.04 LTS to 17.04 LTS supports live backups. Please refer to the following article for further details: <https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/supported-linux-and-freebsd-virtual-machines-for-hyper-v-on-windows>
5. The guest VM volumes must use a file system which supports the use of VSS snapshots, for example NTFS.
6. The guest VMs snapshot file location must be set to the same volume in the Hyper-V host as the VHD file(s).
7. The guest VM volumes have to reside on basic disks. Dynamic disks cannot be used within the guest VM.

**Note: Some older Windows operating systems installed on guest VM's which do not support either Integration Services or the Hyper-V Volume Shadow Copy Requestor Service, will not support VM snapshot method, for example, Microsoft Windows 2000, Windows XP, or older Linux/FreeBSD versions**

### Saved State

If any of the VM Snapshot method requirements cannot be fulfilled, QCBM will automatically use the Save State method. When the Saved State method is used, the guest VM is placed into a saved state while the VSS snapshot is created (effectively shut down), and the duration is dependent on the size of VM and performance of Hyper-V host. The downside is it may affect the availability of any applications or services running on the guest VM every time a backup job is performed.



## **CBT Requirement**

Since QCBM version 7.9.0.0, a new service **CBT Cluster Services (QuikCloud Backup Manager)** is installed and enabled upon installation / upgrade to version QCBM v7.9.0.0 or above.

1. CBT (Changed Block Tracking) is used to optimize incremental backups of virtual machines by keeping a log of the blocks of data that have changed since the previous snapshot making incremental backups much faster. When QCBM performs a backup, CBT feature can request transmissions of only the blocks that changed since the last backup, or the blocks in use.
2. CBT cluster service is only installed on Windows x64 machine.
3. Check if **CBTFilter** is enabled.

To confirm this run the following

```
C:\Users\Administrator>net start CBTFilter  
  
The requested service has already been started.  
  
More help is available by typing NET HELPMSG 2182.
```

*For Windows 2008 R2. If the following error message is displayed*

```
C:\Users\Administrator>net start CBTFilter  
System error 577 has occurred.  
  
Windows cannot verify the digital signature for this file. A recent hardware or software change might have installed a file that is signed incorrect or damaged, or that might be malicious software from an unknown source.
```

*The issue may be related to the availability of SHA-2 code signing support for Windows 2008 R2 <https://technet.microsoft.com/en-us/library/security/3033929>*

*To resolve the issue, install the following patch from Microsoft <https://www.microsoft.com/en-us/download/confirmation.aspx?id=46083>*

*Restart the affected server after for QCBM to operate properly.*

4. CBT Cluster Service and CBTFilter will NOT be installed on Windows Server 2016 where a built-in system called Resilient Change Tracking (RCT) will be used instead. For details of RCT, please refer to Windows Server 2016 RCT Requirement.



## Windows Server 2016 Requirement

### RCT Requirement

1. From version 7.15.0.0 onwards QCBM would not install CBT Cluster Services (QuikCloud Backup Manager) but use the native built-in RCT (Resilient Change Tracking) feature of Windows server 2016 instead.
2. The guest virtual machine version in Hyper-V must be 8.0 or above.

Example:

This can be verified by using Windows PowerShell.

```
get-VM | format-table name, version
```

```
PS C:\Users\Administrator> get-VM | format-table name, version
Name      Version
----      -
lubuntu   8.0
```

If the version is not 8.0 or above, then need to upgrade the virtual machine configuration version.

```
Update-VMversion <vmname>
```

```
PS C:\Users\Administrator> update-VMversion lubuntu
Confirm
Are you sure you want to perform this action?
Performing a configuration version update of "lubuntu" will prevent it from being migrated to or imported on previous
versions of Windows. This operation is not reversible.
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"):
```

Please refer to the following link of Microsoft for details about virtual machine version:

<https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/deploy/Upgrade-virtual-machine-version-in-Hyper-V-on-Windows-or-Windows-Server>

### Guest VM Dependencies Requirements

To get full use of Hyper-V, install the appropriate linux-tools and linux-cloud-tools packages to install tools and daemons, e.g. VSS Snapshot Daemon, for use with virtual machines. Please refer to the following link for the details of requirements for Ubuntu relating to Hyper-V daemons:

<https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/supported-linux-and-freebsd-virtual-machines-for-hyper-v-on-windows>



## ***Limitations***

1. Backup of guest machines located on a SMB 3.0 shares is not supported.
2. Backup of virtual machine with pass through disk (directly attached physical disk) is not supported.
3. For backup of individual virtual disks, the restored virtual machine does not support the reversion of previous snapshots, if the snapshot contains disks which are not previously backed up by QCBM.
4. A guest virtual machine can only be restored to the Hyper-V server with the same version e.g. backup of a guest on Hyper-V 2012 R2 server cannot be restored to Hyper-V 2008 R2 Server or vice versa.
5. The guest virtual machine will not start up if the virtual disk containing the guest operating system is not restored.
6. Run Direct Restore of VM containing VHDS shared virtual disk(s) is not supported.
7. Restore of individual virtual disks is only supported using the Restore raw file option for a virtual disk with no snapshots.
8. Replication must be disabled for the VM selected for backup, otherwise there may be following error occurring during backup job:
  - For QCBM pre-v7.15.6.55: Failed to backup virtual machine "guest\_guid"., Reason= "A parameter cannot be found that matches parameter name 'vmid'.
  - For QCBM v7.15.6.55 or above: Failed to backup virtual machine "guest\_guid"., Reason = "Failed to take VM snapshot. Error = [CreateVirtualSystemSnapshotV2] Error="The method call failed." (32775)".

## Run Direct

Hyper-V Run Direct is a recovery feature introduced in QCBM version 7.5.0.0, it helps to reduce disruption and downtime of your production guest virtual machines.

Unlike normal recovery procedures where the guest virtual machine(s) are restored from the backup destination and copied to production storage, which can take hours to complete. Restore with Run Direct can instantly boot up a guest virtual machine by running it directly from the backup file in the backup destination; this process can be completed in minutes.

The following steps are taken when a Run Direct restore is initiated:

### Delete Guest Virtual Machine

QCBM will delete the existing guest virtual machine on the original or alternate location (if applicable).

### Create Virtual Hard Disk Image Files

Empty virtual hard disk image files are created on the Hyper-V server (either on the original location or alternate location).

### Create VSS Snapshot

A VSS snapshot is created to make the backup data read only and track changes made within the guest virtual machine environment.

### Start Up Virtual Machine

The guest virtual machine is started up. To finalize recovery of the guest virtual machine, you will still need to migrate it to from the backup destination to the designated permanent location on the Hyper-V server.

### Copy Data

Copy the data from the backup files in the backup destination to empty hard disk images on the Hyper-V server.

### Apply Changes

Apply any changes made within the guest virtual machine environment to the hard disk image files on the Hyper-V server.

### Delete VSS Snapshot

The VSS snapshot will be deleted after the Run Direct restoration is completed.



## **What is Granular Restore Technology?**

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

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

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



## Benefits of using Granular Restore

Comparison between Granular Restore and Traditional Restore

Granular Restore	
<b>Introduction</b>	
<p>Granular restore allows you to quickly mount virtual disk(s) directly from the backup file of a guest VM, so that individual files from virtual disk(s) can be exposed via the file explorer on QCBM, or to be copied from the file explorer on to a 32bit or 64bit Windows machine you are performing the restore.</p>	
<b>Pros</b>	
<b>Restore of Entire Guest VM Not Required</b>	<p>Compared to a traditional restore where you must restore the entire guest VM first, before you can access any individual files/folders, granular restore allows you to view and download individual files, without having to restore the entire guest VM first.</p>
<b>Ability to Restore Selected Files</b>	<p>In some cases, you may only need to restore a few individual file(s) from the guest VM, therefore, granular restore gives you a fast, convenient, and flexible tool to restore selected file(s) from a guest VM quickly.</p>
<b>Only One Backup Set Required</b>	<p>With traditional restore methods, if you wish to restore individual file(s) from a guest VM, you will have to create two different backup sets; a Hyper-V guest VM backup set and a separate file backup set for the file(s) you wish to restore. You will require an additional QCBM installation on the guest VM environment, with Granular Restore feature, only one backup set is required.</p> <ul style="list-style-type: none"><li>➤ <b>Fewer CAL (Client Access License) required</b> - you will only need one QCBM CAL to perform guest VM, Run Direct, and Granular restore.</li><li>➤ <b>Less storage space required</b> - as you only need to provision storage for one backup set.</li><li>➤ <b>Less backup time required</b> - As only one backup job needs to run.</li><li>➤ <b>Less time spent on administration</b> - As there are fewer backup sets to maintain.</li></ul>
<b>Cons</b>	
<b>No Encryption and Compression</b>	<p>To make ensure optimal restore performance, the backup of the guest VM will <b>NOT</b> be encrypted and compressed, therefore, you may have to take this factor in consideration when using this restore method.</p>



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

### ***Requirements***

Supported Backup Modules

Granular restore is supported on Hyper-V backup sets created and backed up using QCBM version 7.13.0.0 or above installed on a Windows platform with the Granular Restore feature enabled on the backup set.

### ***License Requirements***

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

### ***Backup Quota Storage***

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

### ***Operating System***

QCBM must be installed on a 64bit Windows machine as libraries for Granular only supports 64bit Windows operating system. QCBM must be installed on the following Windows Operating Systems:

Windows 2012  
Windows 8

Windows 2012 R2  
Windows 8.1

Windows 2016  
Windows 10



### **Temporary Directory Requirement**

For Hyper-V 2008 and 2012 in both Non-Cluster and Cluster environment, the temporary directory must be set to a local drive.

For Hyper-V 2016 or above in a Non-Cluster environment, the temporary directory can be set to a local drive, network drive or a cluster storage.

For Hyper-V 2016 or above in a Cluster environment, the temporary directory must be set to a network drive or cluster storage accessible to all cluster members.

The temporary directory should have at least the same available size as the guest VM to be restored.

### *Available Spare Drive Letter*

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

### Note

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

### **Network Requirements**

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

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

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

### **Other Dependencies**

The following dependencies are required for restore and therefore they are verified by QCBM only when a granular restore is performed. Absence of these dependencies will not affect the backup job but would cause the granular restore to fail.

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

### **Permissions**

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

## Creating a Hyper-V Backup Set

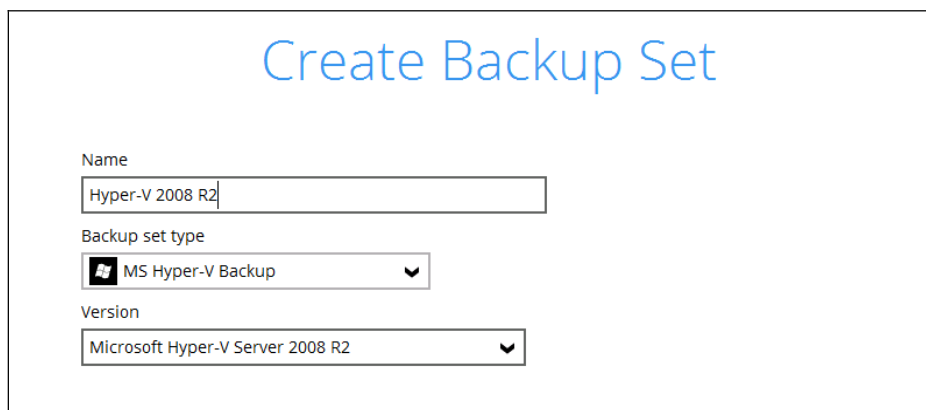
### Non-Cluster Environment

Run Direct Backup Set

1. Click the Backup Sets icon on the main interface of QCBM.



2. Create a new backup set by clicking the "+" icon or **Add** button to create a new backup set.
3. Select the Backup set type and name your new backup set then click Next to proceed

A screenshot of the "Create Backup Set" form. The title "Create Backup Set" is at the top. Below it are three input fields: "Name" with the text "Hyper-V 2008 R2", "Backup set type" with a dropdown menu showing "MS Hyper-V Backup", and "Version" with a dropdown menu showing "Microsoft Hyper-V Server 2008 R2".

4. In the Backup Source menu, select the guest virtual machines you would like to backup. Click **Next** to proceed.

A screenshot of the "Backup Source" menu. The title "Backup Source" is at the top. Below it is a tree view showing the backup source structure: "Microsoft Hyper-V Server R2" expanded to show "WIN-TU41RC45MK0", which is expanded to show "Windows 7 Ent SP1" (checked) and "CentOS 6.4" (unchecked).

5. In the Schedule menu, you can configure a backup schedule for backup job to run automatically at your specified time interval.

**Note:** The default backup schedule is daily backup at 22:00, the backup job will run until completion and the retention policy job will be run immediately after the backup job.

## 6. Select the backup destination

New Storage Destination / Destination Pool

Name  
Local-1

Type  
 Single storage destination  
 Destination pool

Run Direct  
 Support restoring a VM into your production environment by running it directly from the backup file

Destination storage  
Local / Mapped Drive / Removable Drive

Local path  
Change

Test

### Note

- For Hyper-V backup sets by the default the Run Direct feature is enabled.
  - For Run Direct enabled backup sets, the storage destination is restricted to Local, Mapped Drive, or Removable Drive.
7. After selecting the storage destination click on the Test button to verify if QCBM has permission to access the folder on the storage destination.
  8. Once the test is finished QCBM will display “Test completed successfully” message. Click OK to proceed.
  9. If you wish to enable the granular restore feature, make sure you turn on the Granular Restore switch in this menu. Click Next to proceed.

### Notes

- *Once the Granular Restore feature is enabled and the backup set is saved, it is NOT possible to disable it afterwards, and vice versa. If you wish to change the Granular Restore settings, a new backup set will have to be created.*
  - *It is possible to enable both Granular Restore and Run Direct restore on the same backup set. However, QCBM will only allow either Granular Restore or Run Direct restore to run, but not both to run concurrently.*
  - *Granular Restore requires an additional OpenDirect / Granular restore add-on module license to work. Contact your backup service provider for further details.*
10. **IMPORTANT:** If you have enabled the Granular restore or Run Direct restore feature, the backup data will not be compressed and encrypted to optimize the restore performance, therefore you can skip to step 10.

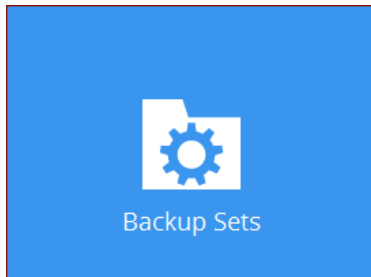
In the Encryption window, the default Encrypt Backup Data option is enabled with an encryption key preset by the system which provides the most secure protection

11. Enter the Windows login credentials used by QCBM to authenticate the scheduled or continuous backup job.
12. Backup Set Created



## Non-Run Direct Backup Set

1. Click the Backup Sets icon on the main interface of QCBM



2. Create a new backup set by clicking the “+” icon next to Add new backup set.
3. Select the Backup set type and name your new backup set then click Next to proceed.

### Note:

QCBM will automatically detect the Hyper-V version installed on the host. In the Backup Source menu, select the guest virtual machines you would like to backup. Click Next to proceed.

4. In the Backup Source menu, select the guest virtual machines you would like to backup. Click Next to proceed.
5. In the Schedule menu, you can configure a backup schedule for backup job to run automatically at your specified time interval.
6. Click Add to add a new schedule or double click on the existing schedule to change the values. Click Next to proceed when you are done setting.
7. Note: The default backup schedule is daily backup at 22:00 with the backup job will run until completion and the retention policy job will be run immediately after the backup job.
8. Select the backup storage destination.

### 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

Destination storage

Local path



**Note:**

For Hyper-V backup sets, the default setting is for Run Direct to be enabled and the storage destination is either a Local, Mapped Drive, or Removable Drive.

9. To select a cloud, sftp/ftp, or CBS as a storage destination un-select Run Direct setting and select your desired cloud, sftp/ftp, or CBS as a storage destination. Click OK to proceed when you are done.

New Storage Destination / Destination Pool

Name  
CBS

Type  
 Single storage destination  
 Destination pool

Run Direct  
 Support restoring a VM into your production environment by running it directly from the backup file

Destination storage

10. Click Add to an additional storage destination or click Next to proceed when you are done.
11. If you wish to enable the Granular restore feature, make sure you turn on the Granular Restore switch in this menu. Click Next to proceed.

**Notes:**

- Once the Granular Restore feature is enabled and the backup set is saved, it is **NOT** possible to disable it afterwards, and vice versa. If you wish to change the Granular Restore settings, a new backup set will have to be created.
  - It is possible to enable both Granular Restore and Run Direct restore on the same backup set. However, QCBM will only allow either
  - Granular Restore or Run Direct restore to run, but not both to run concurrently. Granular Restore requires an additional OpenDirect / Granular restore add-on module license to work. Contact your backup service provider for further details
12. **IMPORTANT:** If you have enabled the Granular restore or Run Direct restore feature, backup data will not be compressed and encrypted to optimize the restore performance, therefore you can skip to step 11.

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



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 QCBM at the time when this backup set is created. Please be reminded that if you change the QCBM 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.

Notes:

- For local, mapped drive, or removable drive storage destinations with Run Direct enabled the compression type will be set No Compression and data encryption is disabled to ensure optimal backup and restore performance. The backup set compression type and data encryption settings will only be applied to CBS, SFTP/FTP, or Cloud storage destinations for the backup set.

Click Next when you are done setting.

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.

13. Enter the Windows login credentials used by QCBM to authenticate the scheduled backup job.

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 update post backup set creation.

Backup set created.

Congratulations!

"Hyper-V 2008 R2" is successfully created.

# QUIK CLOUD

## Cluster Environment

### Requirements

For Hyper-V Cluster backup sets:

1. The same version of QCBM must be installed on all Hyper-V Cluster nodes.
2. The same backup user account must be used.
3. The backup schedule must be enabled on all Hyper-V Cluster nodes.

### Run Direct Backup Set

1. Click the Backup Sets icon on the main interface of QCBM
2. Create a new backup set by clicking the “+” icon or Add button to created new backup set.
3. Select the Backup set type MS Hyper-V Backup, Version Microsoft Hyper-V Server 2012 R2 (Failover Cluster), and name your new backup set then click Next to proceed.
4. In the Backup Source menu, select the guest virtual machines you would like to backup. Click Next to proceed.
5. Click Add to add a new schedule or double click on the existing schedule to change the values. Click Next to proceed when you are done setting.
6. Select the Storage destination

New Storage Destination / Destination Pool

Name  
Local-1

Type  
 Single storage destination  
 Destination pool

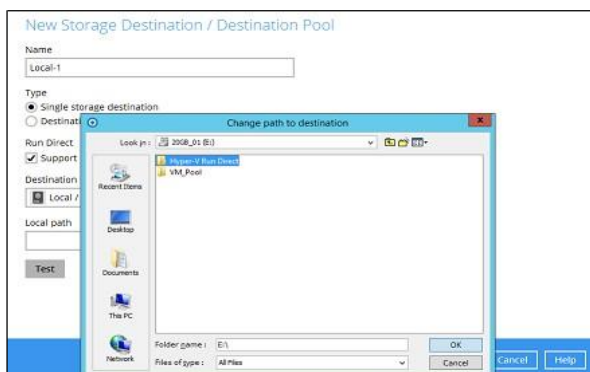
Run Direct  
 Support restoring a VM into your production environment by running it directly from the backup file

Destination storage  
Local / Mapped Drive / Removable Drive

Local path  
Change

Test

7. **Note:** For Hyper-V backup sets by the default the **Run Direct** feature is enabled
8. Click Change to select the storage destination a Local, Mapped Drive, or Removable Drive.







9. After selecting the storage destination click on the Test button to verify if QCBM has permission to access the folder on the storage destination

New Storage Destination / Destination Pool

Name  
Local-1

Type  
 Single storage destination  
 Destination pool

Run Direct  
 Support restoring a VM into your production environment by running it directly from the backup file

Destination storage  
Local / Mapped Drive / Removable Drive

Local path  
E:\Hyper-V Run Direct Change

Test

10. Once the test is finished QCBM will display “Test completed successfully” message. Click **OK** to proceed.

**Note:** For Hyper-V Cluster backup set with Run Direct enabled please ensure all nodes have access to the **Local, Mapped Drive, or Removable Drive** destination storage.

11. To add extra storage destinations click Add, otherwise Click Next to proceed
12. If you wish to enable the Granular Restore feature, make sure you turn on the Granular Restore switch in this menu. Click Next to proceed.

**Notes:**

- Once the Granular Restore feature is enabled and the backup set is saved, it is **NOT** possible to disable it afterwards, and vice versa. If you wish to change the Granular Restore settings, a new backup set will have to be created.
- It is possible to enable both Granular Restore and Run Direct restore on the same backup set. However, QCBM will only allow either Granular Restore or Run Direct restore to run, but not both to run concurrently.
- Granular Restore requires an additional OpenDirect / Granular restore add-on module license to work. Contact your backup service provider for further details.

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

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

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

**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 update post backup set creation



15. Configure a temporary directory for the backup set

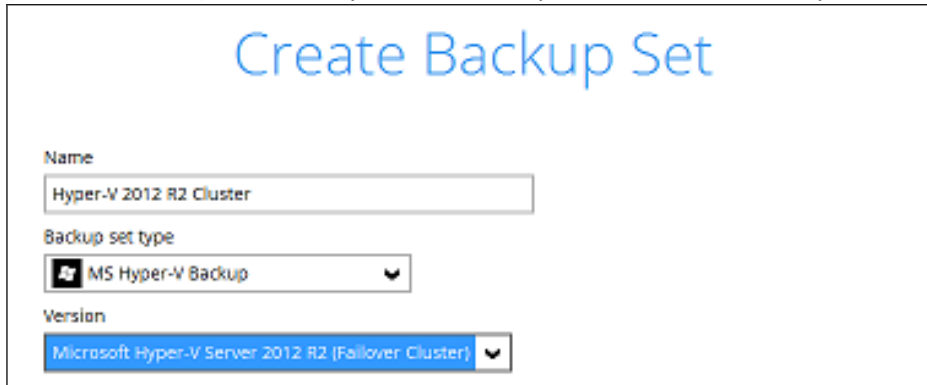
16. Backup Set created

Congratulations!

"Hyper-V 2012 R2 Cluster" is successfully created.

## Non Run Direct Backup Set

1. Click the Backup Sets icon on the main interface of QCBM
2. Create a new backup set by clicking the “+” icon or Add button to created new backup set.
3. Select the Backup set type MS Hyper-V Backup, Version Microsoft Hyper-V Server 2012 R2 (Failover Cluster), and name your new backup set then click Next to proceed.



4. In the Backup Source menu, select the guest virtual machines you would like to backup. Click Next to proceed.



5. Click Add to add a new schedule or double click on the existing schedule to change the values. Click Next to proceed when you are done setting.
6. Click Add to add a new schedule or double click on the existing schedule to change the values. Click Next to proceed when you are done setting.
7. **Note:**  
The default backup schedule is daily backup at 22:00 with the backup job will run until completion and the retention policy job will be run immediately after the backup job.
8. Select the backup storage destination. Select QCBS as a storage destination un-select Run Direct setting and select QCBS as a storage destination. Click OK to proceed when you are done
9. Click Add to an additional storage destination or click Next to proceed when you are done.



10. If you wish to enable the Granular Restore feature, make sure you turn on the Granular Restore switch in this menu. Click Next to proceed.



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

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.

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 QCBM at the time when this backup set is created. Please be reminded that if you change the QCBM 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.

**Notes:**

For local, mapped drive, or removable drive storage destinations with Run Direct enabled the compression type will always be set No Compression and data encryption is disabled to ensure optimal backup and restore performance. The backup set compression type and data encryption settings will only be applied to QCBS destination for the backup set.

Click Next when you are done setting.

12. Enter the Windows login credentials used by QCBM to authenticate the scheduled backup job.

**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 update post backup set creation.

13. Backup set created.



## Backup Overview

