# Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Us</td>
<td>4</td>
</tr>
<tr>
<td>About Product</td>
<td>4</td>
</tr>
<tr>
<td>Document Structure</td>
<td>4</td>
</tr>
<tr>
<td>Help &amp; Support</td>
<td>5</td>
</tr>
<tr>
<td>Deployment</td>
<td>5</td>
</tr>
<tr>
<td>Simple Deployment</td>
<td>5</td>
</tr>
<tr>
<td>Distributed Deployment</td>
<td>6</td>
</tr>
<tr>
<td>Components</td>
<td>6</td>
</tr>
<tr>
<td>Vembu BDR Backup Server</td>
<td>6</td>
</tr>
<tr>
<td>Storage Repository</td>
<td>7</td>
</tr>
<tr>
<td>Vembu Universal Explorer</td>
<td>7</td>
</tr>
<tr>
<td>System Requirements</td>
<td>7</td>
</tr>
<tr>
<td>BDR Backup Server</td>
<td>8</td>
</tr>
<tr>
<td>Supported Platform</td>
<td>9</td>
</tr>
<tr>
<td>Port Configuration</td>
<td>10</td>
</tr>
<tr>
<td>Naming Convention</td>
<td>10</td>
</tr>
<tr>
<td>Scalability and Infrastructure Sizing</td>
<td>10</td>
</tr>
<tr>
<td>Installation</td>
<td>14</td>
</tr>
<tr>
<td>Windows Installation</td>
<td>14</td>
</tr>
<tr>
<td>Case 1: Installing Vembu BDR Backup Server</td>
<td>14</td>
</tr>
<tr>
<td>Case 2: Uninstalling Vembu BDR Backup Server</td>
<td>23</td>
</tr>
<tr>
<td>Case 3: Installing Vembu Universal Explorer</td>
<td>25</td>
</tr>
<tr>
<td>Ubuntu Installation</td>
<td>28</td>
</tr>
<tr>
<td>Case 1: Installing Vembu BDR Backup Server</td>
<td>29</td>
</tr>
<tr>
<td>Case 2: Uninstalling Vembu BDR Backup Server</td>
<td>34</td>
</tr>
<tr>
<td>Login to Web GUI</td>
<td>35</td>
</tr>
<tr>
<td>Storage Pool Management</td>
<td>37</td>
</tr>
<tr>
<td>Storage Pools</td>
<td>38</td>
</tr>
<tr>
<td>Add/Manage Network Drive</td>
<td>40</td>
</tr>
<tr>
<td>Storage Calculator</td>
<td>41</td>
</tr>
<tr>
<td>Delete All Data</td>
<td>41</td>
</tr>
<tr>
<td>Credential Manager</td>
<td>43</td>
</tr>
<tr>
<td>Getting Started with Hyper-V Backup</td>
<td>45</td>
</tr>
<tr>
<td>Adding Hyper-V Server</td>
<td>46</td>
</tr>
<tr>
<td>Setup Hyper-V Backup Job</td>
<td>49</td>
</tr>
<tr>
<td>Step 1: Choose Host/VM Machine</td>
<td>49</td>
</tr>
<tr>
<td>Step 2: Guest Processing</td>
<td>55</td>
</tr>
<tr>
<td>Log Truncation and Guest OS Credentials</td>
<td>58</td>
</tr>
<tr>
<td>Step 3: Backup Scheduling</td>
<td>59</td>
</tr>
<tr>
<td>Step 4: Settings</td>
<td>61</td>
</tr>
<tr>
<td>Step 5: Review Configurations</td>
<td>69</td>
</tr>
<tr>
<td>Evaluation Cases</td>
<td>71</td>
</tr>
<tr>
<td>Case 1</td>
<td>72</td>
</tr>
<tr>
<td>Case 2</td>
<td>..........................................................</td>
</tr>
<tr>
<td>Case 3</td>
<td>..................................................................</td>
</tr>
<tr>
<td>Case 4</td>
<td>..................................................................</td>
</tr>
<tr>
<td>Manage Backup Job</td>
<td>..........................................................</td>
</tr>
<tr>
<td>Recovery</td>
<td>....................................................................</td>
</tr>
<tr>
<td>Manage Vembu Virtual Drive</td>
<td>..................................................................</td>
</tr>
<tr>
<td>Evaluation Cases</td>
<td>..........................................................</td>
</tr>
<tr>
<td>Case 1: Recover VM instantly on another virtual host</td>
<td>..........................................................</td>
</tr>
<tr>
<td>Case 2: Permanently restore backed up VM</td>
<td>..................................................................</td>
</tr>
<tr>
<td>Case 3: Recover a single file</td>
<td>..................................................................</td>
</tr>
<tr>
<td>Case 4: Instantly view/access files in a disk</td>
<td>..................................................................</td>
</tr>
<tr>
<td>Case 5: Restore VM as a file type of your choice</td>
<td>..................................................................</td>
</tr>
<tr>
<td>Case 6: Bare Metal Recovery</td>
<td>..................................................................</td>
</tr>
<tr>
<td>Reports</td>
<td>.....................................................................</td>
</tr>
<tr>
<td>Backup Job Report</td>
<td>..................................................................</td>
</tr>
<tr>
<td>Backup Status Report</td>
<td>..................................................................</td>
</tr>
<tr>
<td>Email Configuration</td>
<td>..................................................................</td>
</tr>
<tr>
<td>Case 1</td>
<td>..................................................................</td>
</tr>
<tr>
<td>Case 2</td>
<td>..................................................................</td>
</tr>
<tr>
<td>Image Integrity Report</td>
<td>..................................................................</td>
</tr>
<tr>
<td>VM Status Report</td>
<td>..................................................................</td>
</tr>
<tr>
<td>Quick VM Recovery</td>
<td>..................................................................</td>
</tr>
<tr>
<td>Portal Registration</td>
<td>..................................................................</td>
</tr>
<tr>
<td>Vembu BDR Suite Licensing</td>
<td>..................................................................</td>
</tr>
</tbody>
</table>
Evaluators Guide for Hyper-V Backup

About Us

From 2002, Vembu has been delivering simplified backup solutions through its portfolio of products to SMBs. Our flagship offering - Vembu BDR Suite is an all-in-one solution that addresses various backup, recovery, replication, and DR needs of your IT environment.

It caters to diverse and advanced use cases, thus ensuring business continuity at affordable pricing.

About Product

With Vembu VMBackup, you can backup your virtual environments such as: VMware and Hyper-V.

Some of the major features that make up Vembu VMBackup are:

- Agentless backup of all your VMs running on VMware and Hyper-V
- Replication of critical servers to a target ESXi host
- Multiple recovery options
- Extensive scheduling and retention settings
- Verified recoverability

Evaluator’s Guide for Hyper-V Backup

Document Structure

This document serves one purpose: To help you perform a hands-on evaluation of Vembu Hyper-V Backup.

A product is best experienced when it is used in your environment. But the hardest part is getting started with it. This evaluator's guide will help you use the key functionalities of the product and understand the diverse use cases that can be handled with it. Over the course of the document, you will be introduced to various features that are necessary to perform backup and recovery operations of your Hyper-V environment. You will get a sense of the usability and the performance of Vembu Hyper-V Backup only by testing out various scenarios.

To simplify the process of evaluation, we have introduced several evaluation cases, designed in such a way that by the end of the cases, you will have used every major option involved in protecting your Hyper-V environment. Each of the cases presents a scenario, the prerequisites to be met and the procedure to perform the exercise.

This guide is intended to provide various evaluation exercises for a complete product evaluation. Each product in Vembu BDR Suite has a separate user guide, where every aspect of
the product is explained in detail.

**Evaluator's Guide for Hyper-V Backup**

**Help & Support**

During the evaluation, if you are looking for further information or have any trouble, contact our 24/7 support at:

vembu-support@vembu.com

or call us at:

+1-512-256-8699 (US & Canada)
+44-203-793-8668 (United Kingdom)

You can find in-depth product documentation at
https://www.vembu.com/technical-documents/

You may find some of your questions already answered in our:

Knowledge Base:
https://www.vembu.com/support/knowledge-base/questions/

Community Forum:
https://www.vembu.com/community/questions/

You can find product demo videos and other tutorials at:

**Evaluator's Guide for Hyper-V Backup**

**Deployment**

- Simple Deployment
- Distributed Deployment

**Evaluator's Guide for Hyper-V Backup**

**Simple Deployment**

In this deployment scenario, you will require the following components:

1. Vembu BDR Backup Server
2. Backup Repository
3. Source Standalone Hyper-V Host/SMB server

- The Vembu BDR Backup Server is the core component for your backup infrastructure that lets you coordinate various functionalities through a single web console. The backup server is responsible for configuring & monitoring the backup jobs, managing the storage
When you configure a backup job from the Vembu BDR backup server, the VM data is directly processed from the Standalone Hyper-V/SMB server and then stored in the backup repository.

To follow the evaluation cases in this guide, it is sufficient to have one BDR backup server for this deployment.

**Evaluator’s Guide for Hyper-V Backup**

**Distributed Deployment**

In this deployment scenario, you will require the following components:

1. Vembu BDR Backup Server
2. Backup Repository
3. Source Hyper-V host

This architecture includes multiple distributed clients connected to a single backup server. Deploying multiple clients enables easier manageability and efficient data transfer from client to the server.

**Evaluator’s Guide for Hyper-V Backup**

**Components**

- Vembu BDR Backup Server
- Storage Repository
- Vembu Universal Explorer

**Evaluator’s Guide for Hyper-V Backup**

**BDR Backup Server**

- Vembu BDR Backup Server is a management server where you can perform backup operations and store all the backup data. It can be installed as a service in your Windows/Linux machines.

- You can do the following operations from the BDR Backup Server:
  - Configure Backups
  - Perform Restores
  - Manage Storage
  - View Reports
  - Native Tape Backup
  - Offsite Replication

- From Vembu BDR Backup Server, you can configure backups for:
  - VMware vSphere
  - Microsoft Hyper-V
  - Microsoft Windows
Evaluator’s Guide for Hyper-V Backup

Storage Repository

- All the backup data configured from Vembu BDR Backup Server is stored in the Storage Repository. Vembu BDR repository management has a hybrid volume manager that supports scalable and extendable backup storage of different storage media such as Local drives, NAS (NFS and CIFS) and SAN (iSCSI and FC).

- **VembuHIVE™** - Vembu has developed its own file system for storing your backup data. VembuHIVE can be thought of as a File System of File Systems with inbuilt version control, encryption, deduplication and inbuilt error correction. So, you can use any combination of storage devices such as NAS, SAN, and Directly Attached Storage as backup targets.

- **VembuHIVE** will analyze your backup data regardless of the environment (VMware, Hyper-V or Physical Server) and make use of the storage space. The backup data will be split and stored into several chunk files across the storage devices, ensuring optimum storage utilization.

**It has inbuilt:**
- Compression
- Encryption (AES-256 Bit encryption algorithm)
- Deduplication (Block-level deduplication applied in each backup job)
- Version controlling (Advanced forward & reverse incremental)

Evaluator’s Guide for Hyper-V Backup

Vembu Universal Explorer

Vembu Universal Explorer is a granular recovery tool that lets you perform item-level recovery from various Microsoft application backups such as Exchange, SQL, SharePoint and Active Directory.

You can perform:
- Granular restore of emails/mailboxes/Exchange stores from Microsoft Exchange
- Granular restore of Microsoft SQL databases and tables
- Document-level restore for Microsoft SharePoint
- User/ Domain level recovery for Microsoft Active Directory

Evaluator’s Guide for Hyper-V Backup

System Requirements

- **BDR Backup Server**
- **Supported Platform**
- **Port Configuration**
- **Naming Convention**
- **Scalability and Infrastructure Sizing**
# Evaluator’s Guide for Hyper-V Backup

## BDR Backup Server

| OS | • Windows Server 2019 Datacenter  
    | • Windows Server 2019 Standard  
    | • Windows Server 2019 Essential  
    | • Windows Server 2016 Datacenter  
    | • Windows Server 2016 Standard  
    | • Windows Server 2016 Essential  
    | • Windows Server 2012 R2 Datacenter  
    | • Windows Server 2012 R2 Standard  
    | • Windows Server 2012 R2 Essential  
    | • Windows Server 2012 Datacenter  
    | • Windows Server 2012 Standard  
    | • Windows Server 2012 Essential  
    | • Windows Server 2008 R2 Datacenter  
    | • Windows Server 2008 R2 Standard  
    | • Windows Server 2008 R2 Enterprise  
    | • Windows 10 Enterprise  
    | • Windows 10 Pro  
    | • Ubuntu LTS 18.04  
    | • Ubuntu LTS 16.04  
    | • Ubuntu LTS 14.04  
    | • Ubuntu LTS 12.04  |
| RAM | 8 GB (Minimum) and 16 GB (Recommended)  |
| CPU | 4 cores or 4 vCPUs (Minimum) and 8 cores or 8 vCPUs (Recommended)  
    | 64-bit Architecture  |
| Network | 1 Gbps & above. While replicating the on-site copy over WAN, 1 Mbps & above  |
| Browsers | • Internet Explorer 11 & above  
            | • Mozilla Firefox 28 & above  
            | • Google Chrome 34 & above  |

- The performance of the VMware and Hyper-V backups depends on the RAM & CPU availability of the BDR backup server.

Normally, 4 GB RAM will be utilized to run the BDR Backup Server and database services.
If only one backup job is active, then it will use the remaining memory (approx. 4 GB RAM). If two concurrent backups are active, then each backup job will use approx. 2 GB RAM. So, the memory utilization will be divided based on the active concurrent backup jobs.

We recommend you keeping approximately 500 MB RAM for each active backup job. If you want to run 8 concurrent backup jobs in your BDR backup server, you should assign 8 GB RAM (4 GB for BDR backup server and 4 GB to process the backup jobs). In order to avoid significant CPU usage during active backup progress, BDR backup server machine should be assigned with enough vCPUs or cores. Normally, one vCPU or core is enough to handle around 8 concurrent backup jobs activity (such as read/write). However, we recommend assigning a minimum of 4 cores/vCPUs for hassle-free usage.

Note: The above mentioned memory and CPU utilization are same for the BDR backup server (Windows & Ubuntu) deployed in physical and virtual environments.

Evaluator’s Guide for Hyper-V Backup

Supported Platform

Following are the virtual infrastructure platforms supported by Vembu VMBackup, with your respective supported versions listed:

<table>
<thead>
<tr>
<th>Virtual Infrastructure</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Platform</strong></td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Server 2016</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Server 2016 Core</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Server 2012 R2</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Server 2012 R2 Core</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Server 2012</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Server 2012 core</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Server 2008 R2</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Server 2008 R2 Core</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hypervisor</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows Hyper-V Server 2016</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Hyper-V Server 2012 R2 Core</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Hyper-V Server 2012</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Hyper-V Server 2008 R2</td>
<td></td>
</tr>
</tbody>
</table>

Following are the VM specifications and requirements supported by Vembu VMBackup:

<table>
<thead>
<tr>
<th>VM Specification</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtual Hardware</strong></td>
<td>Virtual hardware of all types and versions are supported, which includes support for Generation 2 VM hardware. Pass through virtual disks and shared VHDX that are connected to VMs are automatically skipped while taking snapshots for backups</td>
</tr>
</tbody>
</table>
Evaluator’s Guide for Hyper-V Backup

Port Configuration

Ports are an interface or gateway through which the applications communicate. The below section will cover the settings that are required for setting up your backup infrastructure components.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>32004</td>
<td>TCP</td>
<td>Port used for processing all Backup/Restore/Delete/Replication requests.</td>
</tr>
<tr>
<td>6060, 6061</td>
<td>HTTP, HTTPS</td>
<td>Port used for processing all Web Service requests.</td>
</tr>
<tr>
<td>32005</td>
<td>TCP</td>
<td>Port used for UI Communication.</td>
</tr>
<tr>
<td>42005</td>
<td>TCP</td>
<td>Port used for Vembu Integration service.</td>
</tr>
</tbody>
</table>

Evaluator’s Guide for Hyper-V Backup

Naming Conventions

- Any backup or replication job that is created in Vembu BDR Server should be named with the following rule:
  - Only [a-z][A-Z][0-9][ - _ ] characters are allowed in the backup/replication Name
  - Do not use the following reserved names for naming any backup/replication job:
    - CON, PRN, AUX, NUL, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, and LPT9.

To learn more about file/folder naming restrictions in Microsoft Windows, read the naming conventions column from the link mentioned below:
Naming Conventions - Microsoft

Evaluator’s Guide for Hyper-V Backup

Scalability & Infrastructure Sizing

| OS | Windows Server 2016 Datacenter |
- Windows Server 2016 Standard
- Windows Server 2016 Essential
- Windows Server 2012 R2 Datacenter
- Windows Server 2012 R2 Standard
- Windows Server 2012 R2 Essential
- Windows Server 2012 Datacenter
- Windows Server 2012 Standard
- Windows Server 2012 Essential
- Windows Server 2008 R2 Datacenter
- Windows Server 2008 R2 Standard
- Windows Server 2008 R2 Enterprise
- Windows 10 Enterprise
- Windows 10 Pro
- Ubuntu LTS 16.04
- Ubuntu LTS 14.04
- Ubuntu LTS 12.04

<table>
<thead>
<tr>
<th>RAM</th>
<th>8 GB (Minimum) and 16 GB (Recommended)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>4 cores or 4 vCPUs (Minimum) and 8 cores or 8 vCPUs (Recommended)</td>
</tr>
<tr>
<td></td>
<td>64-bit Architecture</td>
</tr>
<tr>
<td>Network</td>
<td>1 Gbps &amp; above. While replicating the on-site copy over WAN, 1 Mbps &amp; above</td>
</tr>
<tr>
<td>Browsers</td>
<td>Internet Explorer 11 &amp; above</td>
</tr>
<tr>
<td></td>
<td>Mozilla Firefox 28 &amp; above</td>
</tr>
<tr>
<td></td>
<td>Google Chrome 34 &amp; above</td>
</tr>
</tbody>
</table>

- The performance of the VMware and Hyper-V backups depends on the RAM & CPU availability of the BDR backup server.
- Normally, 4 GB RAM will be utilized to run the BDR backup agent and database services.
- If only one backup job is active, then it will use the remaining memory (approx. 4 GB RAM).
- If two concurrent backups are active, then each backup job will use approx. 2 GB RAM.

- So, the memory utilization will be divided based on the active concurrent backup jobs. We recommend keeping approximately 500 MB RAM for each active backup job. If you want to run 8 concurrent backup jobs in your BDR backup server, you should assign 8 GB RAM (4 GB for BDR backup server and 4 GB to process the backup jobs).

- In order to avoid significant CPU usage during active backup progress, BDR backup server machine should be assigned with enough vCPUs or cores.
- Normally, one vCPU or core is enough to handle around 8 concurrent backup jobs’ activity (such as read/write). However, we recommend assigning a minimum of 4 cores/vCPUs for hassle-free usage.
**Note:** The Above mentioned memory and CPU utilization are same for the BDR backup server (Windows & Ubuntu) deployed in physical and virtual environments.

### Database Storage

- Make sure you have 10% free space available in the DB metadata storage target. For example, if you want to backup VMs with 2TB used data, after storage reduction, approximately 1TB data will be stored at storage targets. In this scenario, approximately 100GB free space would be required to store the metadata files.

### Storage Repositories

- You can use any NAS, SAN or Directly Attached Storage device to store the backup data. There are no limitations with any hardware vendor. So, we never recommend any specific hardware vendor.
- The performance of the backup job depends on the IOPS. So, you will get better backup performance, if you have higher IOPS.

**Note:** To calculate the required storage space for your environment, use [Vembu storage calculator](https://www.vembu.com/vembu-storage-calculator).

### Vembu VMBackup Sizing Table

The following tables illustrate how the VMware & Hyper-V backup performance parameters change depending upon the average data transfer rate.

#### Underlying Assumptions:

- The estimates provided below are not 'stretch estimates'; they are safe estimates and are more pessimistic than optimistic. Typical bottlenecks you should look out for are:
  - Bandwidth bottlenecks
  - Slowing down of data transfer due to low-performance switches/routers, etc.
  - The hard disk write speeds at the storage targets
  - CPU utilization by other non-related processes running on the BDR Backup Server

### Sizing Tables

#### BDR Backup Server Configuration

- **OS:** Windows 2012 R2 DC (Physical Machine)
- **RAM:** 16 GB
- **CPU:** Intel XEON CPU 2.10 GHz (4 cores)
- **Network:** 1 Gbps
- **BDR Version:** v3.9.1

#### Backup Environment

- **Hypervisor:** Microsoft Hyper-V
- **No. of VMs:** 1
- **VM data:** 2 TB
<table>
<thead>
<tr>
<th>Backup Type</th>
<th>VM Data Size</th>
<th>CPU Utilization</th>
<th>Memory Consumed</th>
<th>Total time taken to complete the backup</th>
<th>Transfer rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Backup</td>
<td>2 TB</td>
<td>22 %</td>
<td>3145 MB</td>
<td>383 Mins</td>
<td>803 Mbps</td>
</tr>
<tr>
<td>Incremental</td>
<td>55 GB</td>
<td>16.5 %</td>
<td>401 MB</td>
<td>11 Mins</td>
<td>751 Mbps</td>
</tr>
</tbody>
</table>

**Note:** The above measurements are taken for one backup job with one VM. So, if multiple concurrent backup jobs are active then it will share the memory and CPU. As stated earlier, each backup job will approximately require 500 MB RAM.

- It is important to note that there are no inherent scalability restrictions for a BDR backup server when it comes to the maximum number of simultaneous backups possible.
- If a larger number of backup jobs are simultaneously configured to a BDR backup server, then the only effect will be a corresponding degradation of performance in terms of time taken to complete the backup for all the backup jobs.
- The maximum number of backup jobs that can be supported by a single BDR backup server depends on:
  - The bandwidth of the network used
  - Time taken for each backup job
- For example, the above illustration assumes that backups are typically scheduled during 'non-office hours' (hence the 10 hour window); this is not always the case. Especially, if in case the backups can happen non-intrusively in the background while you do your regular work.

**Storage Device Throughput and Concurrent Writes:**

- The throughput of Storage devices (IDE/SCSI/SAS/NAS/SAN) are normally benchmarked based on maximum throughput achieved while performing sequential writes into the device.
- But when multiple VMs are backed up simultaneously to the BDR backup server, then the server will be concurrently writing the different files for different VMs onto the Storage device.

**Note:** When concurrent writes from multiple threads are being done, the throughput of the storage device determines the BDR backup server performance

- The reason storage devices do not perform well when multiple threads are writing to it concurrently is that the I/O seek that has to be done between writes from different threads can slow down the performance significantly.
- Hence, it is imperative that the storage device used to backup the data is of the highest quality and has the ability to scale and perform well when 100s of different threads write to the storage device concurrently.
Evaluator's Guide for Hyper-V Backup

Installation - Windows

- Windows Installation
- Ubuntu Installation

Evaluator's Guide for Hyper-V Backup

Windows Installation

- Case 1: Installing Vembu BDR Backup Server
- Case 2: Uninstalling Vembu BDR Backup Server
- Case 3: Installing Vembu Universal Backup Explorer

Evaluator's Guide for Hyper-V Backup

Installing Vembu Server

Prerequisites:

Refer system requirements for Vembu BDR backup server here - Vembu BDR backup server

Procedure:

Step 1: Getting started with the installation

Download the latest version of Vembu BDR Server for Windows and run the installer with administrator privileges. Begin the installation process by selecting Next from the welcome page.
Step 2: License Agreement

- 'Vembu BDR License Agreement' is the next step in the installation process, read the License Agreement carefully as it contains important information about your Rights, Restrictions, Obligations, Limitations, and Exclusions. Choose 'I accept the terms in the license agreement' option, else you cannot proceed with the installation.
Step 3: Installation Directory Customization:

- The next step in the installation wizard will allow you to customize the installation location of Vembu BDR backup server. The installation location consists of many application files such as conf files, exe files, bin files, and apache files.

Note: The default installation path is C:\Program Files\Vembu\Vembu BDR.

- Click the **Browse** option to select a different location for the Vembu BDR installation. Select the **Make New Folder** option if you want to create a new folder inside the installation location. The new folder by default will be created with the name VembuBDR. Once done selecting the installation location, click **OK** and select **Next** to proceed further with the installation.
Step 4: Default or Custom Installation Settings

- This step involves the option of either proceeding with the default configuration settings or customize them as desired. You can customize all the options in this page. The options are briefly explained below:

  - **Service Account** - If the account is a local or user account.
  - **Web Console User Name** - user name used to access the web console. By default it is admin.
  - **Web Console Password** - password for accessing the Vembu BDR backup server Web-Console. By default it is admin.
  - **Backup Port** - Backup Port acts as a common port for data transfer for backup schedules. By default, it is 32004
  - Click **Install** to proceed installation with default chosen settings or click the ‘**Let me customize the configurations**’ option and opt to customize settings.

**Note:** Make sure you have 1.2 GB of free space for installing Vembu BDR backup server.
Step 5: Specify the Windows logon user account

- If you have selected the Let me customize the configurations option in the previous steps, then proceed with the steps mentioned below.
- The next step is to specify the Windows logon user account under which Vembu BDR backup server would run. Select either Local System Account or User Account.
• If you select **User Account**, provide the Username and Password for that account.

**Note:** The user name should be in the DOMAIN\USERNAME format. Make sure the specified user account has enough privileges.

---

**Step 6: Configure PostgreSQL Data Location**

• The next step in Vembu BDR backup server installation is to select the drive to which PostgreSQL database will be stored. Default drive selection will be based on the maximum space available, however you can select a drive as per your requirement. When you select a drive as the storage, its total size and free size will be displayed adjacently.

• When you configure your storage repository make sure at least 10GB storage space is available. We generally do not recommend you selecting C:/ drive as the storage location since it is the OS drive and consists of important files. Click **Next** to proceed with the installation process.
Step 7: Configure Web Server Port:

- The next step in the wizard will allow you to configure port and Web-Console login configuration:
  - **WebServer port** - This is the port that will be in use when you access the Vembu BDR backup server Web-Console. The default port number used to access the web GUI is 6060. This can be changed to any available port number but it is recommended not to change unless you are an advanced user.

  You can configure a range of ports from the **Advanced Port Configurations** tab. The **ports** include:
  - Backup Server Port
  - UI Communication Port
  - HTTPS Port

- **User credentials for web console** (Default User Name: **admin** and Password: **admin**)
Each port's necessity is mentioned in the question mark near the respective text-box.

You can enable the HTTPS port which is used for accessing the Vembu BDR backup server web console in a secure manner. By default, the value is 6061. Selecting the Check Ports option will validate your entries provided and check if the ports are available. If the ports are not available, the comment 'not available' will be displayed. Click OK to close the tab and select Next to proceed with the installation process.
Step 8: Review Configuration

- Review the chosen configuration, and click **Install**. During installation, the following components are installed in your machine that is integral for the working of Vembu BDR backup server.
  - PostgreSQL
  - ODBC drivers (32-bit and 64-bit)
  - Web Server
  - Visual C++
- Verify the Destination folder location, Program folder location, and if Vembu BDR backup server will run as a service. Click **Install** option to begin the installation.

Step 9: Finish Setup Wizard

- The final step of the wizard after the installation will ask whether to:
  - Start Vembu BDR application - Vembu BDR backup server will be started immediately after this.
Open the Vembu BDR Web Console - this will open the Vembu BDR backup server Web-Console.

- Choose the appropriate option and click **Finish** to complete the installation process.

**Note**: Vembu BDR backup server is installed as a service and can be found in Services.msc page.

**Evaluator’s Guide for Hyper-V Backup**

**Uninstalling Vembu BDR Server**

**Prerequisites:**

- Vembu BDR server should already be installed in the machine
- The downloaded VembuBDR installer file should be available to directly perform a clean uninstallation

For clean uninstallation of Vembu BDR server in Windows machines, follow the below steps:

- From the Control Panel go to Programs and Features option, right click on **VembuBDR** and select the **Uninstall** option to proceed with clean uninstallation process
- In the pop-up window which alerts you to confirm proceeding with the uninstallation process, click **Yes**
You can witness Vembu BDR server being uninstalled from your machine.

Uninstallation is completed successfully but a few elements that are associated with Vembu BDR server will be removed only if you reboot your machine. Click Yes to reboot the machine or No to manually restart later.
Evaluator's Guide for Hyper-V Backup

Case 3: Installing Vembu Universal Explorer

Step 1: Getting started with the installation

- Download the installer file for Vembu Universal Explorer from here - Download Vembu Universal Explorer and run the installer with administrator privilege. Begin installing Vembu Universal Explorer by selecting Next in the installation wizard.

Step 2: Prerequisites and License Agreement

- The next window will check for the prerequisites for the installation in your machine and lists them along with download link for applications that are Uninstalled.
- You can download them right away, or check the I will install prerequisites later check-box
and install them later. Click Next to continue.

- Read and agree to Vembu Software License Agreement. Click Next to continue.

Step 3: Configure shortcut location
• The installation wizard will ask for folder name under which the setup will add program icons to the folder. In the next page, choose whether you need the shortcut and quick launch icons for the program and proceed. Click **Next** to proceed with the Vembu Universal Explorer installation process.

![Setup - Vembu Universal Explorer](image)

### Step 4: Review Selections

• The installation wizard will give a brief summary of the provided details, you can review it and proceed to install Vembu Universal Explorer by selecting the **Install** option.
Step 4: Completing Vembu Universal Explorer Installation

- Vembu Universal Explorer is installed successfully. If you want to start Vembu Universal Explorer Application after the setup closes, select the Start Vembu Universal Explorer Application check-box and click Finish.
Ubuntu Installation

- **Case 1: Installing Vembu BDR Backup Server**
- **Case 2: Uninstalling Vembu BDR Backup Server**

**Evaluator's Guide for Hyper-V Backup**

**Installing Vembu BDR Backup Server**

**Prerequisites:**

Refer system requirements for Vembu BDR [Here](#).

**To install Vembu BDR backup server on Linux machines follow the steps given below:**

Copy the download link from the following link: [Click here](#) and download the installer file using wget command and make sure you are a root user (use "sudo su" command to be a root user). You can download the installer to any Windows machine and move the installer to Linux machine using FTP/WinSCP.

1. Once you execute wget command you will have "VembuBDRSetup.sh" in the download location.

   ```
   root@vembu:/home/V40_Oct09# sh VembuBDRSetup.sh
   ```

2. Run the installer by using "sh" command. For ex: #sh VembuBDRSetup.sh. The installation process begins with the wizard displayed below, click Yes to proceed with the installation.

   ```
   Welcome to VembuBDR installation setup wizard.
   We will now take you through the VembuBDR installation process.
   VembuBDR is propriety software of Vembu and is licensed under its own terms which you are required to accept for this installation.
   If you would like to install VembuBDR, Please enter yes to proceed.
   Do you want to proceed [yes/no]:
   ```

3. The installer shows the License Agreement, read the License Agreement carefully as it contains important information about your Rights, Restrictions, Obligations, Limitations, and Exclusions. Enter "y" to proceed with your installation.
4. After initiating the installer, it will check for dependent packages and request for a confirmation from your side. Enter “y” to proceed further.

5. Please find the packages to be downloaded by Vembu BDR application here:
   - ODBC Driver (2.3.4)
   - PostgreSQL Connector (9.5.02)
   - Vembu BDR Server (4.0.1)
   - PostgreSQL RDBMS (9.6)

6. Specify the location to which the PostgreSQL files will be stored (you can proceed with the default choice). Vembu BDR will basically require 10% of the backup data storage for the internal metadata store. Hence please assess and configure a storage medium appropriate to the storage requirements. Ensure your drives have higher I/O performance. Specify the path and click Enter. We recommend you to use dedicated drive for this location instead of root volume. (Important STEP)

7. The next step in the installation is to specify the default port value for PostgreSQL. By default, the port number is 32010. The port number can be changed by proceeding with ‘y’.

   Note: You can enter the port value from 1024 to 65535. You cannot enter a port number that is below or beyond the allowed limit. You cannot proceed with a port value that is being used by another process.
8. Enter a valid port value and proceed. The installer will proceed to install Unix ODBC and PostgreSQL driver.

9. Click "Yes" install dependency packages of PostgreSQL.

10. Once done installing PostgreSQL, databases will be created and PostgreSQL will be restarted automatically.

11. In the next step, installer will begin downloading VembuBDR_4_0_0_DBN.zip file.

12. The Vembu BDR backup server build installation starts automatically after the download completes and will ask you to choose the type of installation. "Option 1" will Install Vembu BDR by creating a new Vembu BDR user account with root privileges. "Option 2" will install Vembu BDR in the current user and proceed with the installation. We recommend choosing Option 1.
13. If you have selected "Option 1" installer will create a new Vembu BDR user. If you have selected "Option 2" installer will install in the current user.

14. Once the user is created, it will ask to create a directory for the installation path. Enter "y" to proceed

15. Installer asks your permission to create repository. Enter "y" to create repository now or Enter "n" to create it after installing the backup server. If you want to create now press "y" and click Enter.

16. Once you click enter, installer will show the list of volumes present in your machine. Choose any volume by entering the corresponding number. Click the number and press Enter to continue (Example : Enter 1)
17. The repository will be created successfully and the installer asks for Vembu BDR Web Console Authentication as shown below. Provide the username and password through which you can access your Vembu BDR web console. By default, we recommend username as 'admin' and password as 'admin'. Press Enter to continue, Vembu BDR web console user will be created successfully.

```
Volumes with free space of 5GB or more
Mounted On   Total Space  Available Space
1  /         238G        212G
2  /media/vembutest/Storage1  229G        59G
3  /media/vembutest/Storage2  238G        218G
df: /run/user/1008/gvfs: Permission denied
df: /run/user/1008/gvfs: Permission denied
Please choose any one of volume
```

18. The installer asks you to change ports from default value. If you want to change click "y" else "n". By default, we recommend to click "n" and continue. Go through the usage of individual ports mentioned below.

- **Backup Server Port** is the port through which the installed Vembu VMBackup client will backup the data to the backup server. The default value is 32004.
- **UI Communication Port** is the port through which Vembu BDR Apache/PHP modules communicate with Vembu BDR to serve UI requests from the Vembu BDR Web Console. The default value is 32005.
- **HTTPS Port** is the port used to access the Vembu BDR Web Console in a secured manner. The default value is 6061.
- **Enable HTTPS** is the secure Web Console port through which you can access the Vembu BDR web console in a secure manner. You should enable "Enable HTTPS" option to edit this value. If you have enabled HTTPS option, you can access the Vembu BDR web console through https://localhost:6061
19. Once the installation is complete you will be asked to start Vembu BDR as Daemon process. If you have not started Vembu BDR as daemon process you can start using "sh startVembuBDR.sh" command and "sh stopVembuBDR" to stop Vembu BDR from the Vembu BDR installation location. If you want to start the immediately, enter "y" to proceed as shown below.

Evaluator's Guide for Hyper-V Backup

Uninstalling Vembu BDR Backup server - Linux

For clean uninstallation of Vembu BDR server in linux machines, follow the below steps:

- Login to Linux machine with root privilege.
- Change the directory path to Vembu BDR installation location.
- Run following command to proceed uninstallation: sh uninstall.sh

```
root@vembu:/home/vembubdr/Vembu/VembuBDR# sh uninstall.sh
```

- Running the above command will provide two options to choose between:
  - Uninstall Vembu BDR server or
  - Perform clean uninstallation(Vembu BDR and PostgreSQL)
• Proceeding with option 1 will delete and uninstall existing VembuBDR instances. If you wish to continue, click yes.

• Proceeding with option 2 will uninstall and delete all existing VembuBDR, PostgreSQL services and its data. If you wish to continue, click yes.

• VembuBDR will be uninstalled successfully.

**Evaluator's Guide for Hyper-V Backup**

**Login to Web GUI - Vembu BDR**

You can log in to Vembu BDR web UI via the following options:

- Via shortcut icon created in the desktop
- Via web console option the tray icon
• User who login after a fresh installation will be required to choose the **time zone** in which they want their **backup/replication** reports to be generated.

• Choose the required **Time Zone** and click **Save** option.

**Time Zone**

*Select your timezone from the below list Vembu BDR uses this timezone for display purpose through the application.*

(LKT+05:39) Chennai, Kolkata, Mumbai, New Delhi

**Mon 19 Nov 2018 20:51:42**

• The next step is to enter a unique **Vembu BDR ID**. The ID should be globally unique as it is with this ID that each installation of Vembu BDR is identified.

**Vembu BDR ID**

*The Vembu BDR ID specified here should be unique. We recommend to use machineName.domainName as the Vembu BDR ID since it is globally unique.*

Enter Unique Vembu BDR ID

• Click the **Update** option to assign the Vembu BDR ID. The Vembu BDR ID will be updated successfully and you will be directed to the storage pool management page. Configure a storage pool to begin with your backup process.

**Note**: It is recommended to give machine name.domain name as Vembu BDR ID since it should be globally unique.

The following characters are permitted as part of the ID:

[ A-Z][a-z][0-9][ - _ ] Your ID must not start or end with special characters and it must be between 1-50 characters in length.
Troubleshooting:

- If there seems to be an issue existing in accessing web GUI, check if the server/client service is running in Services.
- Also, check whether VembuBDR WebServer service is running.

Evaluator's Guide for Hyper-V Backup

Storage Pool Management

Storage pool management page allows you to manage and configure drives into separate storage pools for storing backup data. Vembu BDR has a new file system that halts backup and once a storage pool gets filled, you can extend storage by edit option where you can add new volumes to an already created storage pool.

Note: Vembu BDR repository management has a hybrid volume manager that supports scalable and extendable backup storage of different storage media such as Local drives, NAS(NFS and CiFS) and SAN(iSCSI and FC).

- From the Management Tab select Storage Pool Management
• Users can add network volumes using 'Add network drive' option in settings.

• Click here to learn about Storage Pools.
• Click here to go to Add Network Drive page.
• Click here to Calculate your Storage Space Requirements.
• Click here for steps to Reset Vembu BDR to Fresh Installation state.

Evaluators Guide for Hyper-V Backup

Storage Pools

• Storage Pools are used to aggregate the space available from different volumes and utilize them as a single storage for specific backups.

![Image of Storage Pool Management interface]

• The backup storage configured after the installation will act as a default pool

**Note:** Backup cannot be configured until the default storage pool is configured.

• You can add new volumes to create a pool for storing your backups. You can create 'n' number of storage pools, wherein 'n' number of volumes can be added to form a pool.
• Physical and network shared volumes can be combined together to form a pool. A single volume can be added to multiple pools.
• Backups configured from a standalone client will only be stored in default storage repository of backup server.
• You can choose the storage pool for backups during backup configuration itself when the backup is configured from a client on the server.

**Note:** If a storage volume has free space less than 5GB, it cannot be added as a storage repository.

Steps to create Storage Pool:

• **Add Storage Pool:** To create a new storage pool, click the Add Storage Pool option. Give
the storage pool a name and select any set of volumes from the list of available storage volumes. Enter the storage pool name, this name will be listed in the available storage pools for the backups

**Note:** Only [a-z][A-Z][0-9][ - _ ] characters are allowed in the storage pool name.

- **Choose Volumes:** In the choose volume section, you will have three sections namely: Storage Volume, Space Usage & Backup Location
  - **Storage Volume** - The list of drives added in the machine. Enable the checkbox if you want to select the drive for a pool.
  - **Space Usage** - The total space and the available space of each drives in the machine.
  - **Backup Location** - The storage location or path for each volumes where the backup data will be stored.

**Note:** It is not recommended to choose OS Partition as Storage repository.

<table>
<thead>
<tr>
<th>Choose Volumes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Storage Volumes</strong></td>
</tr>
<tr>
<td>F: \</td>
</tr>
<tr>
<td>C: \</td>
</tr>
</tbody>
</table>

- The list of storage volumes with its used size and backup location are displayed. You can select the required drives for the pool.
- Once all the details are provided, click **Save**. The new pool that is created will be displayed in the list of storage pools.
You can expand the storage pool size by adding Volumes. Use the **Edit** option with respect to that storage pool.

**Note**: If the backup data is available in the pool, it cannot be deleted. The storage pool can be deleted only if the pool does not contain any backup data.

**Evaluator’s Guide for Hyper-V Backup**

**Add/Manage Network Drives**

Network Drive or Mapped Drive option allows users to add and delete network drives that are within the same network. The drives that are added will then be listed in the storage volumes list along with a separate drive letter which can be utilised as a backup storage. If your storage pool is running out of storage to store the backup data, then you have an option to add network drives into the pool.

**Note**: Mapped network drives are not supported when Vembu BDR server runs in local logon account. Change logon user with administrator privileged user in service management console and then proceed to configure Network drive.

1. Go to **Management** tab and select **Storage Pool** option. Click on **Manage Network Drive** option.

To add a network drive, one must provide following attribute details:

- **Drive Name**- Provide a drive letter/name for network drive to be added

  **Note**: Drive name must be a single alpha character: A-Z or a-z. Do not give drive name which is already present in your local machine

- **Drive Path**- Network path of the drive to be added. Enter the Target Host’s UNC path where the data will get stored and make sure the shared Drive/Volume has enough space.

  **Ex**: `\<MACHINE_NAME OR IP_ADDRESS>\<SHARE_NAME>`

You can enter the shared path as single Drive or Volume letter and make sure the shared path you have mentioned has Full access.
• **Username & Password** - If network drive requires login authentication provide the username and password to authenticate drive addition.

• A user can add 'n' number of network drives and can manage it via 'Manage network drives' page.

2. Once done providing details, click 'Save' to add network drive.

• The added drives listed can also be deleted using the 'Delete' option if no longer required.

---

**Evaluator's Guide for Hyper-V Backup**

**Storage Calculator**

Users with large data centers and high data traffic can now calculate their storage space requirements with Vembu Storage calculator. The calculation will be made based on the type of job a user opts for along with recovery points and the average data traffic ratio. We implement a custom compression method that reduces storage space to a vast ratio difference compared to source data size.

Click below to calculate your storage space requirements:

[Vembu Storage Calculator](#)

---

**Evaluator's Guide for Hyper-V Backup**

**Delete All Data**

This option lets you to wipe out your server data and reset Vembu BDR Server to a fresh installation state.

• Click the **Management** tab and select **Storage Pool**, you can view **Delete All** option.
• The **Delete all data** window will be displayed as shown below.

![Image of Delete All Data window]

**Delete All Data**

This process will wipe out all your backed up data references from this Server and this will not have any impact on trial period. To continue deletion, type the following text exactly in the below textbox.

```
I wish to delete storage repositories folder manually
```

Enter the text

- I understand and thereby acknowledge that this function will cause irrecoverable data loss

**Note:** At the end of this process, backed up data will be temporarily renamed as "sgstorage-TIMESTAMP" in the Storage Repository location and you have to **delete it manually**.

- In order to proceed with the deletion process, you must type the phrase "**I wish to delete storage repositories folder manually**" as mentioned in the window. Please note that the command is case-sensitive and the phrase should be typed as given.
- Select the checkbox to acknowledge the deletion and click **I agree** option.
- Once you click on 'I agree' all the backup server data will be wiped out and Vembu BDR will be reset to a fresh installation state.
- Proceeding with the delete option will not auto-delete the backed up data, but will rename the **sgstorage** folder with the timestamp of deletion period in the configured storage location. If sgstorage is present in all the drives in a machine, each sgstorage folder will be renamed with a timestamp of deletion period.
- Once the delete process is notified with a success note, you have to manually delete the folder.
Credential Manager

- Credential Manager allows you to create, save, and manage user credentials when you add servers and physical machines. Credential Manager accumulates the records of the user credentials and allows communication with the respective backup infrastructure. There are no limitations on the number of credentials that can be added.

Credentials can be added in three ways:
- From the Credential Management page
- Before configuring the backup job (While adding server/physical machine)
- While scheduling the backup job

1. From the Credential Management page

From the Management tab select Credential option. The Credential Management page will be displayed. The following details will be available in this page:
- Credential UserName
- Credential Description
- Last edited time
- Edit - edit the given username/password/description combination in the database, which can be used if you have changed the password
Click the **Add Credentials** option to create a new credential into the record. Provide the following:

- **User Name**: the domain name or user name of the host or server that is to be added
- **Password**: the specific password for the mentioned host or server that is to be added
- **Description**: the text which acts as a hint or a possible description of the credential that is recorded in the database and could be used further for other possible credentials.

2. **Before configuring the backup job (While adding server/physical machine)**

When you are adding a new server/physical machine you can add a new credential. Click the **Add Credentials** option and provide the following:

- **User Name**: Enter the hostname or IP address of the host to which the backup must proceed.
- **Password**: The specific password for the mentioned host or server
- **Description**: the text which acts as a hint or a possible description of the credential that is recorded in the database and could be used further for other possible credentials.
You can either add a new credential or select an already added credential from the Select Credentials drop down list.

3. While scheduling the backup job

When you are adding machines to which you are enabling Application Aware consistency, you can add a new credential. Click the +Add Credentials option and provide the following:

- **User Name**: User name of the Guest OS machine to which you are enabling Application Aware process.
- **Password**: The specific password of the Guest OS machine.
- **Description**: A hint or possible description of the credential that is recorded in the database and could be used further for other possible credentials.
- In case you have previously added credentials, select the particular description from the Select Credentials drop down list. Once done click Save.

---

Evaluator's Guide for Hyper-V Backup

Getting started with Hyper-V Backup

- **Adding Hyper-V Server**
- **Setup Hyper-V Backup Job**
- **Evaluation Cases**
Evaluators Guide for Hyper-V Backup

Adding Hyper-V Server

You need to add a source Hyper-V Server before you begin configuring your Hyper-V backup. The Hyper-V Server can be a Standalone Hyper-V Host or SMB server.

Procedure:

- To add your Hyper-V server with Vembu BDR, click on Add Hyper-V Server option

- You can choose 'Hyper-V Cluster' or 'Standalone Hyper-V Host' or 'SMB Host' as server type

- On selecting Standalone Hyper-V Host you need to provide the login Hyper-V Host credentials, it also asks you to confirm whether you are using the SMB server as storage for the VMs
  - If 'Yes' - Users will be redirected to the next page to provide SMB credentials
  - If 'No' - Server addition will be completed with Saving the credentials'
  - Port number 42005 will be used for the communication between Vembu Integration Service and Vembu BDR Server

You can connect your host with Vembu BDR server through following combinations in Hostname/IP Address section:
- Hostname - Enter the Hostname alone
- Host name can be added using FQDN(Fully qualified domain name) ie., machine_name.domain_name
- 192.xxx.xxx.xxx - Enter only the IP address

For Username the following formats:
- Username - Enter the username alone
- Username@domain
- Domain\Username
Choosing SMB Host will direct you to Add SMB Host credentials page, where you need to provide SMB Host credential. Once done providing it, hit Add Host to add Hyper-V server.

Choosing Hyper-V Cluster Host will direct you to Add Hyper-V Cluster credentials page, where you need to provide Cluster host credential. Once done providing it, hit Add Host to add Hyper-V Cluster.
- Once you have added the Hyper-V server, the list of Hyper-V servers added will be shown.
- From the list of servers added, Click the **Backup** option to configure a new backup job.

![Evaluators Guide for Hyper-V Backup](image)

- **Rescan** option installs the VembuIntegrationService agent automatically in the Hyper-V host, which is mandatory to proceed with the backup. Once you click the **Rescan** button you will get alert message, to scan and install the VembuIntegrationService on the target machine, Click **Ok** to install.

  Scan and install the VembuIntegrationService on the target machine

  ![Scan and install the VembuIntegrationService on the target machine](image)

- In the **Status** column, you can view the current progress while you rescan. You can also edit the host credential details using the **Edit** button.

![Update Host Details](image)

- **Agent information report** gives you the stage-wise report of the VIS agent installation. Click the reports icon to view the Machine Name, Version, Installed time, Status, Remarks. Further expand it to view the installation start and end time.
Note: Virtual machines without Hyper-V Integration Services installed will remain in a saved state while the VSS snapshot is created.

For application consistency VM backup, the Guest Machine should be installed with the latest Hyper-V integration services. VMs with checkpoints (*.AVHD & *.AVHDx) will not be backed up. To perform the backup, checkpoints need to be removed.

- If you want to remove a particular Hyper-V Server, click the **Remove** option. A pop-up window with the message “Are you sure you want to remove the host 192.168.102.120?” will appear. Click **OK** to delete your Hyper-V Server

---

**Evaluator’s Guide for Hyper-V Backup**

**Setup Hyper-V Backup Job**

- Click the **Backup** option from the added Hyper-V Server. You will be taken to backup configuration page where you can begin configuring your Hyper-V Backup schedule.

- There are 5 major steps involved in Hyper-V backup. They are:
  - Choose Host/VMs machine(s) for backup
  - Guest processing
  - Backup Scheduling
  - Settings
  - Review Selections

**Evaluators Guide for Hyper-V Backup**

**Choose machine(s) you wish to configure**

In this section you can select VM(s) for the new backup job,

- You can configure either host level backup job or can select any specific set of VMs to be backed up. Choose the entire or list of VMs you wish to backup and proceed
- You can search a specific **VM/Host/Cluster** easily using the search feature
- If you have chosen a host level backup and after the completion of the initial full backup, if you have added any new VM(s) to the backed up host, then the new VM(s) will be added to backup job from next backup schedules
If you have chosen a Cluster VM for backup then the hierarchy of Cluster host and the nodes will be represented as shown below,

VM(s)/Disk(s) Exclusion

This options allows you to Exclude the VM(s) and the Disk(s) in a VM from the backup job. On selecting Host-level backup, you might wish to exclude some specific set of VMs from getting backed up. Such VMs can be excluded using VM(s)/Disk(s) exclusion option. If you have configured multiple VM(s), then you can exclude the Disk(s) in the VM using this feature

VM Exclusion

Click 'VM(s)/Disk(s) Exclusion' option, you will get a popup as shown below
Choose 'Exclude VM(s)' tab

To exclude a virtual machine from a configured host-level backup, click 'select VM' and choose the VMs to be excluded and click 'Exclude'

Once added, save the exclusion settings

You can add/delete a VM from the backup job's exclusion list whenever required by editing the backup job

Note: Changes made in VM exclusion settings will be taken into effect immediately with next schedule.

Disk Exclusion

Click 'VM(s)/Disk(s) Exclusion' option, you will get a popup as shown below

Choose 'Exclude Disk(s)' tab
• Disk exclusion can be either enabled at host-level or can be configured at VM level

**Host level Disk Exclusion:*** This exclusion type is possible when you opt to configure the host level backup job. Under 'Exclude Disk(s)' tab, you will find the configured host(s) listed

![Image](image1.png)

- You can choose 'Edit Disk Exclusion' option, to assign global disk exclusion rule for VMs under a chosen host. Edit Disk exclusion tab will have following exclusion rules:
  - No disks Excluded
  - Include only System Disks for Backup. Exclude Others (typically 0:0)
  - Select type of Disk to exclude

*Note: By default, No disks excluded option will be selected.*

**No Disks Excluded**: By default, No disk Excluded option will be selected. This backs up the complete VM without excluding any disks. i.e., No disk will be excluded

**Include only System Disks for Backup. Exclude Others**: This option allows you to include only the System Disks Generally (0:0) (i.e) the disk that contains the machine configuration and OS files and excludes all the other disks.

**Select type of Disk to exclude**: This option allows you to select the type of disks to be excluded from the VM(s), such as IDE, SCSI by selecting the checkboxes and the selected disks will get excluded from the backup.

![Image](image2.png)

- Opting for the third option of selecting disk type will list all available disk types for VMs in Hyper-V
• User can choose the disk(s) to be excluded in each disk type

![Edit Disk Exclusion](image)

- No Disk Excluded
- Include only System Disks for Backup. Exclude Others (typically Disk 0:0)
- Select type of Disk to exclude

![Exclusion Settings Table](image)

- IDE
  - IDE 0:0
  - IDE 0:1
  - IDE 1:0
  - IDE 1:1

- SCSI

• Once done assigning disk exclusion rule, click 'Confirm' and save the exclusion settings

**VM level Disk Exclusion** - This exclusion type can be configured in both host level and VM level backup job. Under 'Exclude Disk(s)' tab, you will find the list of configured VM(s).

If it's a host level backup job, you can assign both host level exclusion rule as well as assign exclusion rule for individual VMs by adding VMs to be configured using **Select VM(s)** option.

- Choose 'Edit Disk Exclusion' option alongside a VM to configure disk exclusion rule for the selected VM. Edit Disk exclusion tab will have following exclusion rules:
  - No disks Excluded
  - Include only System Disks for Backup. Exclude Others (typically 0:0)
  - Select type of Disk to exclude

**Note:** By default, No disks excluded option will be selected.
**No Disks Excluded**: By default, No disk Excluded option will be selected. This backs up the complete VM without excluding any disks. i.e. No disk will be excluded.

**Include only System Disks for Backup. Exclude Others**: This option allows you to include only the System Disks Generally (0:0) (i.e) the disk that contains the machine configuration and OS files and excludes all the other disks.

**Select type of Disk to exclude**: This option allows you to select the type of disks to be excluded from the VM(s), such as IDE, SCSI by selecting the checkboxes and the selected disks will get excluded from the backup.

- Opting for the third option of selecting disk type will list all available disk types for VMs in Hyper-V
- User can choose the disk(s) to be excluded in each disk type
- Once done assigning disk exclusion rule, click 'Confirm' and save the exclusion settings
You can also add/delete a disk to/from exclusion list, whenever required by editing the backup job.

**Note:** Changes made in disk exclusion settings will be applied only when an additional full backup is scheduled.

### Evaluators Guide for Hyper-V Backup

### Guest Processing - Application-Aware Hyper-V Backups

Application-Aware is a feature available for Hyper-V environments handling high-end application servers. Microsoft Exchange Server, SQL Server, Active Directory, SharePoint are some of the data sensitive applications that require prior steps to be taken before configuring a backup, for data consistency.

**How it works**

Enabling application-aware process, Vembu BDR server will keep constant communication with Microsoft VSS that ensures all pending application transactions are either committed or rolled back before proceeding with the VM snapshots for backup. This ensures backup data stays uncorrupted for restore.

When the application-aware option is disabled, it will put the backup under risk and even further lead to corrupted data during disaster recovery. For business-continuity, it is recommended to have application aware option enabled for VMs that have data-sensitive applications.

In Vembu BDR, Hyper-V backups utilize Microsoft VSS writers to take application-consistent...
backups (MS SQL, MS Exchange) and truncate exchange log files to free up space.

**Prerequisites**

To perform application-aware image processing, the Guest Machine (running MS Exchange server, MS SQL Server, MS SharePoint Server, MS Active Directory) should be installed with latest Hyper-V integration services.

**Steps for Guest processing:**

**Step 1:** Click the toggle button to **Enable Application Aware Processing** option.

**Step 2:** You can customize Application Aware configurations at Host/VM Level. Select **Click here** to customize the global configuration settings at Host/VM level. The Manage Application Aware settings pop up window will be displayed.

The following options will be available in this page:

- **Host/VM level entity** - Displays the Host name/IP address. If you are configuring application aware settings at VM level, the name of the VM will be displayed.
- **VSS Writer Status** - Whether the VSS writer status is required, ignored or disabled based on your selection.
- **Log Truncation Status** - Displays whether the log truncation status is enabled or disabled. If **Truncate the transaction log** option is selected, the log status will be enabled. If the **Disable Log Transactions** is selected, log truncation status will be disabled.
You can configure Application Aware rules for your entire Hyper-V host or individual VMs. Click the check-box next to the entity name, this will select all the entities. If you want to select individual entities, select the required entity (Host/VM) and click the **Edit** option.

**Step 3: Application aware settings**

- The Appaware Settings page will be displayed. You can configure the Application-aware processing configurations.
  - **Require successful application processing**: Choosing this option lets Vembu BDR track the application consistency and trigger the backup process, only when all the VSS writers in the VM are in a stable state. You can stop the backup if any of the application writers say for Eg MS SQL writer is not in a stable state or if the VSS writers were not processed successfully after the snapshot.
  - **Ignore application processing failures**: This option, lets Vembu BDR trigger the backup job when it is scheduled, despite the success/failure of application processed. It will not process the Application VSS writers and ignores the writer's status. By default, we do not recommend this option as it may lead to data inconsistency of the applications in the backup.
  - **Disable Application processing**: Application Aware will be disabled for the selected entity.
Truncate Transaction logs

**Step 1:** To truncate the transaction logs, Click the Radio button alongside **Truncate the transaction logs** option

- Enabling this option lets Vembu BDR truncate the exchange server logs before initiating the backup process. It purges and commits log files along with the .edb files and reduce storage space consumed

**Step 2:** If you have selected **Disable Log Transactions** the log transactions will be disabled and truncation won't happen. Click **save** to save the application aware settings.
Guest OS Credentials

- You can select previously added guest OS credentials by choosing the Select Credentials drop down list.
- Click here to learn about adding new guest OS credentials.
- Save and proceed with Next to configure backup schedule.

Evaluators Guide for Hyper-V Backup

Configure Backup Scheduling

You can configure the backup schedules flexibly based on the requirement. The backup job can
be scheduled from Hourly/Daily/Weekly options.

- If you want your data to be backed up frequently you can go with Run every schedule option. Here you can configure the backup to run in hourly basis. Use the checkboxes to select the days on which you want to backup your data

- Run daily option executes the backup job at specific time daily, Using the fields next to the option you can set your preferable time at which the backup job should run daily

- If you want to run the backup job on specific days at a specific time you can select Run weekly option

- Select your desired backup scheduling using the respective fields and proceed with the backup configuration

**Additional Full Backups**

In an enterprise environment, configuring a backup job with one full backup and forever incremental is not a recommended practice. You can configure additional full backups periodically and that can be automated with our additional backup option.

- If needed, enable the additional full backup option and select your additional full backup scheduling. If not needed, you can directly switch to step 4

- You can select the time, day and month using its respective fields and click Next to proceed with backup settings

**Additional Full Backups can be configured by following the order of scheduling:**

**Run Every**

If you have selected Run Every backup schedule, then you will be allowed to configure the additional full backups on Daily or Weekly or Monthly basis.

- Daily at a specific time
- Weekly on specific days at specific time
- Monthly at a specific time on the specific days of the weekdays for the selected months
For example, 9 am on First Sunday of January, Feb, March

**Run Daily**

If you have selected **Run Daily** backup schedule, you will be allowed to configure the additional full backups on **Daily or Weekly or Monthly** basis.

- Daily at a specific time
- Weekly on specific days at specific time
- Monthly at a specific time on the specific days of the weekdays for the selected months

**Run Weekly**

If you have selected **Run Weekly** backup schedule, you can configure the additional full backup on specific days of the **Month**, at particular time.

- Monthly at a specific time on the specific days of the weekdays for the selected months

For example, 9am on First Sunday of January, February, March, April, May, June

**Store maximum of**

Users can also limit the number of full backups to be retained with 'Store a maximum of' option.

For example, If a user needs only 6 months data to be retained, we recommend to configure monthly full backups with maximum full backup count set at 6. This way, when the 7th month's full backup completes successfully - the 1st month's additional full backup will be deleted.

---

**Evaluator's Guide for Hyper-V Backup**

**Settings**

In the Settings page, you can configure the following:

- Retention Policies
- Storage Repository
- Backup Encryption

All these three settings are **optional** with each option set to a default action. For example:
- Not enabling retention will result in forever incremental backups
- By default, the storage pool configured for the backup job is the default repository (Default_Repo)
- The backup data stored in your repository will be encrypted using the system generated password

**Configure Retention Policy**

The retention policy allows you to retain the backups of multiple versions of files at the backup server. When configuring the retention policy for your backup job various aspects should be considered such as storage consumption and backup consistency. By retaining multiple version of backup files you can restore their desired version of backup when required. Vembu BDR provides forever incremental backups, where you can have ‘n’ number of incremental. The retention count denotes the count for retaining the backup versions in the storage repositories.

Vembu provides two types of retention for Hyper-V backups:
- Basic retention
- Advanced retention (GFS)

**Basic retention:**

Basic retention in Vembu is a collection of every day’s merge. If basic retention is enabled then every day’s incrementals will be merged together to form a daily merge. By default, the daily merge will occur on the 3rd day from the day you have configured your backup.

For example, if you have configured a backup on Tuesday (Day 1) then the daily merge will occur on successful completion of first incremental on Thursday (Day 3).

**Working with Basic Retention - Daily merge**

Let us assume that you have configured "Keep Last 3 daily merge recovery points".

- The backup is configured on Day 1 with backup scheduled to run every hour. Vembu BDR will now backup the data in the regular intervals based on the configuration scheduled.

- When the first incremental of Day 3 runs successfully, then every incremental that had
taken place on Day 1 will get merged as a single recovery point and be marked as **Daily merge** (D)

Similarly, on Day 4, the incrementals of Day 2 will be consolidated as a single restore point and repeats the same for 5th Day and 6th Day.

As per the requirement, you need daily merge restore points of the latest 3 days alone. In this case, after the 6th day's successful incremental backup, the daily merged recovery point becomes 4 which exceeds the configured merge count.

So, the daily merge of Day 1 will be synthetically merged with the daily merge of Day 2 making it a single restore point. This process repeats regularly to retain the 3 daily merge restore points.

- So after the completion of one-week backup schedule, you will have 3 daily merged restore points with all the latest incrementals (2nd, 3rd and 4th Day Merged points)

- Now you have the 3 daily restore points available. This process will continue to maintain the latest 3 daily merged data available at all times

**Note:** The Basic Retention option will be available only if you are scheduling backup for hourly and daily schedules. In case you want to schedule for weekly incremental, opt for Advanced Retention (GFS).

### Advanced (GFS Retention)

The Multilevel GFS retention reduces the time taken to restore backed up machines and most importantly reduces consumption of storage space. Using advanced retention settings you can ensure that the backups will not fill up your storage space. It also helps avoid long chains of incrementals, ensuring consistency of backup data and allow you to meet the requirements of your long-term retention policy.

GFS retention policy is otherwise known as Grandfather-Father-son retention, it is an advanced version of basic retention which consists of multiple retention cycles for your backup data. GFS retention merges incremental backups on a daily, weekly and monthly basis. In this retention policy daily merge is called as Son, weekly merge as Father and monthly merge as Grandfather.

- **Daily Merge**
- **Weekly Merge**
- **Monthly Merge**

The above merge process will run based on a defined hierarchy with Daily Merge first followed by Weekly and Monthly Merge. Daily Merge is the same process that takes place in Basic retention.

### Working with Advanced retention - Daily, Weekly and Monthly merge

When you configure Advanced retention policy for your backup job it will start from the daily merge process.

- **Daily merge**
If you have selected only the daily merge process then you will have a collection of daily merge incremental data marked as \((d)\).

**Scenario 1: Advance retention policy enabled only Daily merge.**

- On the successful completion of the 3rd days first incremental backup, the 1st day incrementals will get merged together to form a daily merge recovery point marked as \((d)\).
- Similarly, on 4th day, the incrementals of 2nd day will be consolidated as a single restore point and so on for 5th Day and 6th Day.
- This process continues to maintain the daily merge recovery point.

**Weekly merge**

If you have selected only the weekly merge process then you will have a collection of weekly merge incremental data marked as \((w)\).

**Scenario 2: Advance retention policy enabled Daily merge and Weekly merge.**

If you have configured to merge the daily merged incrementals upto sunday.

The daily merge process takes place for the following week till Sunday. Once Sunday's first incremental backup get completed successfully, all the daily merged incremental backup upto sunday gets merged together as Weekly merge. It retains the single timestamp version of weekly merged data marked as \((w)\).

**Monthly merge**

If you have selected only the monthly merge process then you will have a collection of monthly merged incremental data marked as \((m)\).

**Scenario 3: Advanced retention policy enabled to retain Daily, Weekly and Monthly merge data**

- If you have selected all the three daily, weekly and monthly then each merge process will get initiated on the user-specified day.
- If you have configured the weekly merge on Sunday. Once after the first successful incremental on Sunday all the daily merge backups from last Monday will be merged together and marked as **Weekly merge (W)**
- The daily merge process will continue and next Sunday you will be having another weekly merge with all the previous weeks daily merge.
- Now with the completion of the **Weekly merge**, the merge of Daily and Weekly process will continue to take place until the configuration of Monthly merge arrives on you specified day of the month (**First Week Wednesday**)

**Note:** You have configured the monthly merge to take place on First week wednesday

- Once the incremental of **First Week's Wednesday** is completed, the monthly merge process will start. It will merge all the daily and weekly merge along with the incrementals that took place before the First Week Wednesday as a **single monthly merge point**.
When you want to restore a month's backup data, this monthly restore point will be available for restore.

Steps to configure the retention policy

- Click the Enable retention checkbox to set the **Basic retention**. By default, it is configured to keep the last 3 days of daily recovery points and at the maximum of 99 daily merge recovery points can be kept at the backup server.

- To configure the advanced retention option, click the **Advanced retention** option. You can either choose Daily merge or Weekly merge or Monthly merge. You can also select all the three options together using its respective fields.

Storage Repository

Storage Repository lets you configure and manage drives into separate storage pools for storing your backup data. If the storage repository for the backups gets filled or running out of space, then you can extend your storage by adding new volumes to an already created storage pool.

**Note**: Vembu BDR repository management has a hybrid volume manager that supports scalable and extendable backup storage of different storage media such as Local drives, NAS (NFS and CIFS) and SAN (iSCSI and FC).

If the storage pool gets filled, you will be alerted with the message in the notification bell.

Storage pool

Storage Pools are used to aggregate the space available from different volumes and utilise them as a single storage for specific backups.

- The backup storage configured during installation will act as a **Default Repo**. In case if the backup storage is not configured during installation, you have to create default pool from the ‘Settings’ page while configuring backup or from the ‘Storage Management’ page of BDR server.

**Note**: You cannot trigger any backup until he configures the default storage pool.
You can create 'n' number of storage pools, whereas 'n' number of volumes can also be added to form a pool.

A single volume can be added to multiple pools. New volumes can also be added to create a pool for storing your backups.

Physical and network shared volumes can be combined together to form a pool.

**Steps to create Storage pool while configuring backup**

- In the Storage Repository section, **default repo** is chosen by default, you can change the pool by adding new Storage pool.

  - If the storage repo is already added during installation, the **available pool space** for the chosen Storage repo will be listed below the Storage Repository option.

  - **Add Storage Pool:** To create a new storage pool, click the 'Add Storage Pool' option. Give a Storage Pool name and select any set of volumes from the list of available Storage Volumes.

  - **Storage Pool Name:** Enter the storage pool name, which will be listed in the available storage pools for the backups.

    **Note:** Only [a-z][A-Z][0-9][ - _ ] characters are allowed in the storage pool name.

  - **Choose Volumes:** In the choose volume section, you will have three parts Storage Volume, Space Usage, Backup Location.

    - **Storage Volume** - The list of drives added in the machine. Enable the checkbox if you want to select the drive for a pool.
      - **Space Usage** - The total space and the available space of the each drives in the machine.
      - **Backup Location** - The storage Location or path for each Volumes, where the backup data will be stored.

    **Note:** If you select C drive for storage pool, you will be alerted with a message "It is not recommended to choose OS partition as Storage repository. Please change if you select OS drive for Storage pool."
If you select any of the Volumes in the machine, then its available storage space will be displayed at the bottom near the 'Size of the Pool' option. The Size of the pool is displayed accordingly with the number of volumes added to the pool.

You can modify the default storage pool by enabling 'Make it as default pool' option alongside respective storage pool they wish to set default. If a particular storage pool is made as default pool, then the backups that are freshly configured will be stored in a newly set default pool. But, the increments of the old backups will now be stored in the previously configured default pool.

You can also add network volumes using 'Add network drive' option in Storage management page.

Encryption Setting

Encrypting data is important because it prevents information from being accessed and exploited by some unauthorized users during data transfer. Encryption securely protects our data from hackers, intruders, criminals and is a component of security.

Backups configured under Vembu BDR can be encrypted with a user-defined password which can be provided during backup configuration. A user can choose between system generated password or from the list of user-defined passwords.

Steps to ‘Enable Encryption’ while configuring backups:

1. Proceed with the backup configuration of your choice till backup 'Scheduling' and proceed with Next to Settings Page.
2. You have an option to 'Enable Encryption', enable the checkbox.
3. A user can choose a password of their choice between System-generated password or from the list of user-defined passwords.

**Note:** By default, Vembu uses the system-generated password to encrypt backups even if Encryption is disabled. You can opt for a custom password for extended data protection and you will be required to provide it during recovery. Opting to the custom password will disable integrity check from being performed automatically. It is recommended to perform Quick VM Recovery periodically to ensure data integrity.

**System Generated Password**

The selected files and folders will be encrypted using AES algorithm with a 256-bit encryption key automatically generated by Vembu BDR Server.

You can also create a new password by proceeding with 'Add Password' option. Provide password of your choice along with a password hint. With the help of the encryption hint, you can easily identify the required password and click **Save** button.

**Rules for Password and Hint to be inserted:**

- Password and its hint should not be the same to avoid security issues. encryption hint should be at least 6 characters and not more than 25 characters. Encryption hints are unique and no two passwords can have the same encryption hint.
- Password length should be at least 6 characters and not more than 16 characters. It should contain a minimum of one alphabet, a number and a special character.
- Vembu BDR suite uses industry standard AES - 256 encryption algorithm to encrypt the backup data.

A newly created password will be available in the drop-down list, choose it and proceed with 'Next' to review the backup configuration.

---

**Evaluator's Guide for Hyper-V Backup**

**Review Configurations**

This page shows the entire configuration of the recent backup to be processed, where a final view of the whole backup settings is displayed such as the configured Host/VM's, scheduling information, retention policies, given backup storage server and encryption settings.

If there are any changes to be made in the configured settings you can review here and alter the settings by navigating to the previous steps by clicking 'Previous' option.

- You will be asked to provide an *unique name* for the backup configured. The unique name given in the Enter the Job Name field will help you identify the specific backup job that you have configured among other backups in the recovery page.

- The following details will be available in this page:
  - **Configured Host/VM(s)** - The Host/VM you have configured for the backup process.
  - **Scheduling** - Frequency of your backup schedule.
  - **Retention Policy** - The settings you have configured in retention.
  - **Full Backup Scheduling** - Full Backup schedule frequency.
  - **Configured Storage Pool** - The name of the storage pool you have configured.
  - **Backup Encryption** - Status of the encryption, whether enabled or disabled.
  - **Encryption Hint** (Applicable only if encryption is enabled).

- You have the option of running the backup job immediately after saving the backup. If you want your backup job to be triggered immediately after you save the backup, irrespective of the backup schedule you have configured, select the **Run this job immediately after saving** option.
- Click **Save the backup** option once all the configurations are reviewed. On saving the backup, you will be prompted to confirm to proceed further. Click **OK** to complete the
backup progress

**Note:** There are few rules to be followed for specifying job name. They are

- Only [a-z][A-Z][0-9][ - _ ] characters are allowed in the job name. Other Special Characters are not allowed in the job name.
- The job name should not be more than 26 characters.

**Progress Details:**

- You can verify the progress of your backup in the **Overall Progress** window. To view the backup progress window, Go to **Backup** tab and press **List All Jobs** option, Click on the triangle mark in the **Status** section. The overall progress of your backup along with details is listed below.

The overall backup progress page consists of the details listed below:

- **Job Name** - Name of your backup job
- **Backup Server** - The IP address of the backup server to which the backup is currently processing
- **Warning** - Warning for the backup job if any
- **Reconnection Attempts** - The count of the times Vembu client attempted to reconnect to
the backup server

- **Bandwidth Throttling** - Whether bandwidth throttling is applied in the client or not
- **Transfer Rate** - Rate at which the backup data is transferred to your backup server. (Bytes, KB, MB, GB)
- **Original Size of the file** - The actual size of your backup file
- **Time Left** - Time remaining for your backup to complete
- **Current File** - The name of the current disk which is being backed up
- **The configured backup Volume with its Size and Status** of the backup progress is displayed in the bottom of the window.

**Abort** - You can abort your backup if not required, from the **Abort (-)** option available in the progress window. You will get a popup window as shown below. Click **OK** to Abort your backup.

192.168.108.79:5060 says

The backup will be aborted immediately and no further data will be transferred to the backup server during this backup schedule. However the backup will resume at the next scheduled time. Do you wish to proceed?

[OK] [Cancel]

You can also abort your backup from the List Jobs page. Click the X mark in the status section. Click **Yes** from the warning window to abort your backup.

[Abort Backup]

[Warning: Are you sure you want to abort this backup hyper-v ?]

[No] [Yes]

**Note:** To enhance your backup performance, close the progress window and open it occasionally to check backup progress.

**Evaluator’s Guide for Hyper-V Backup**

**Evaluation Cases**

- In this section, we have covered 4 evaluation cases that will guide you through the various features and configuration options available in Hyper-V backup. By the end of the evaluation case, you would have used every option while configuring your backup job. You will create and edit backups that suit diverse use cases.
- During the evaluation scenarios, you will get familiar with the product using the feature overview, procedure and guidelines provided.

- [Case 1](#)
- [Case 2](#)
• **Case 3**
• **Case 4**

**Evaluator’s Guide for Hyper-V Backup**

**Case 1**

- Configure a job to backup an entire Standalone Hyper-V host or SMB Server
- Schedule the backup job to run every 1 hour on all days except Sunday
- Keep last 5 daily merged recovery points
- Change the Storage Pool
- Run the backup job immediately after saving

Configuring a backup job for the above case will guide you through the basic steps involved in creating a backup job. Follow the procedure mentioned below to execute the case.

**Step 1: Choose the virtual machine(s) for backup**

- Since our requirement is to backup the entire Standalone Hyper-V host, select the source Hyper-V host check box. This option will select all the VMs under that particular host for the backup process. Click **Next** to proceed further in the backup configuration.

**Step 2: Configure backup schedule**

Configuring the backup schedule has three options to choose from:

- **Run Every** - Run the backup at regular intervals on specific day(s)
- **Run Daily** - Run the backup every day in a specific time frame
- **Run Weekly** - Run the backup on particular days of the week at a specific time period

- As per the evaluation case, the backup job has to be scheduled **every 1 hour on all days except Sunday**. Select **Run Every** option and choose **1 Hour** as the time frequency for the backup. Select all the days except **Sunday**. Click **Next** to proceed further in the backup configuration.
Step 3: Configure Retention Policy

While configuring the Retention Policies for your Hyper-V backup, you will have two options to configure from:

- Basic Retention
- Advanced Retention

- The evaluation case requires you to keep the last 5 daily merged recovery points, so proceed with Basic Retention.
- Select Enable Retention option. By default, Basic Retention will be enabled.
- From the keep last daily merged recovery points drop-down list, choose the value as 5. Click Next to proceed further in the backup configuration.

Note: By default, retention is not enabled and incremental backups will run forever.

Step 4: Configure Storage Repository

- The next step will be to change the storage repository from Default_Repo. If you have already added a storage pool, select it from the drop down list. Else, click the Add Storage Pool option.
- Click Save once you have configured the storage repository.
Step 5: Review Configurations

The Review page lets you review your configurations before you proceed to trigger the backup. Verify the following:

- Host/VM(s) Details
- Scheduling Details
- Retention Settings
- Storage Pool & Encryption Settings

- Enter a backup job name.

**Note:** There are few rules to be followed for specifying job name. Only `[a-z][A-Z][0-9][-_]` characters are allowed in the job name. Other Special Characters are not allowed in the job name. The job name should not be more than 26 characters.

- The evaluation case requires you to enable the *Run this backup job immediately after configuration*. Your backup job will now be triggered immediately after you save the backup, irrespective of the backup schedule configured.
- Click *Save the backup* to complete the backup schedule configuration.

Evaluator's Guide for Hyper-V Backup
Case 2

- Configure a backup job to backup only particular VMs from the source Hyper-V host
- Disable the Application Aware processing
- Run the backup job every day at 09:00 PM
- Take an additional full backup on the First Wednesday of every month
- Merge the daily recovery points on Sunday of every week
- Add a new storage pool for the backup job
- Encrypt the backup job with System Generated password

Configuring a backup job for the above case will guide you through the steps involved in creating a backup job. Follow the procedure mentioned below to execute the evaluation case.

Step 1: Choose the virtual machine(s) you wish to backup

- In this page, all the VMs under Standalone Hyper-V host will be displayed. According to the evaluation case, only particular VMs are to be backed up and not the entire Hyper-V host
- Select the required VMs for the backup schedule and click Next to proceed with the backup schedule

Step 2: Disable the Application aware

- According to the evaluation case, Disable the application aware processing option. By default the option is disabled
- Click Next to proceed to with the backup schedule
Step 3: Configure the backup schedule

Configuring the backup schedule has three options to choose from:

- **Run Every** - Run the backup at regular intervals on specific day(s)
- **Run Daily** - Run the backup everyday in a specific time frame
- **Run Weekly** - Run the backup on particular days of the week at a specific time period

According to the evaluation case, backup must **Run Daily at 09:00 PM**. Select the **Run Daily** option from the drop down list and configure the time to **09:00 PM**

*Note: By default the time selected for Run Daily will be 09:00 PM*

The next step is to configure an **Additional Full Backup on the First Wednesday of every month**.

Select the frequency of the Additional Full Backup. You can take an Additional Full Backup Daily, Weekly or Monthly.

- Enable Additional Full Backup and select **Monthly** from the Take a full backup drop down list
- Choose when the full backup has to run every month. There are two drop down list which specifies which day of the month and the days of the week
- Choose **First** and **Wednesday**. By default all the months will be selected for the backup
Step 4: Configure retention policy

- You can choose the number of backup versions to be retained in the storage repositories by selecting the retention count. Retention is aimed at optimizing the storage utilization while adhering to your organization backup policy.
- Enable Retention option and select Advanced Retention option since the evaluation case involves merging the daily recovery points on Sunday of every week.
- As the backup has been scheduled to Run Daily, only two options will be listed under Advanced Retention:
  - Weekly Merge - Merge all daily merged recovery points every week
  - Monthly Merge - Merge all daily merged recovery points every month
- Select Weekly Merge. Choose Sunday as the day of the week as to when the merge has to take place.

Note: By default, retention is not enabled and incremental backups will run forever.

Step 5: Configure Storage Repository

- The next step will be add a new storage repository for the backup schedule. Click the Add Storage Pool option. Give the storage pool a name and select the storage volume. Click Save once you have completed configuring the storage repository.
Note: It is not recommended to choose OS Partition as Storage repository. Only [a-z][A-Z][0-9][ - _ ] characters are allowed in the Storage Pool Name.

Step 6: Configure Encryption

- Backups configured from the Vembu BDR Server can be encrypted with a user-defined password.
- Select Enable Encryption option. By default System Generated option will be selected for your Hyper-V backup job.
- Click Next to proceed with the backup schedule.

Step 7: Review Configurations

- The last step in your Hyper-V backup configuration is to review the configurations you have selected. Enter a backup schedule name. Vembu BDR Server supports creating
multiple backup schedules each with its own configuration. The backup schedule name will uniquely identify the backup. While restoring your backup data, you need to choose the data to be restored using its schedule name.

- Review the following
  - Host/VM(s) Details
  - Scheduling Details
  - Retention Settings
  - Storage Pool & Encryption Settings

**Note:** There are few rules to be followed for specifying job name. Only `[a-z][A-Z][0-9][ - _ ]` characters are allowed in the job name. Other Special Characters are not allowed in the job name. The job name should not be more than 26 characters.

- Click **Save the backup** to complete the backup schedule configuration.

Evaluator's Guide for Hyper-V Backup

**Case 3**

- Configure a job to backup an entire Standalone Hyper-V host and exclude a VM and a Disk from the host
- Enable Truncate the transaction logs
- Run the backup job on Monday of every week at 09:00 PM
- Take an Additional Full Backup on the Last Sunday of every month and store a maximum of 3 additional full backups
- Disable retention policy
- Add a new storage pool for the backup job and make it as default pool
- Add a new password to encrypt the backup

Configuring a backup job for the above case will guide you through the basic steps involved in creating a backup job. Follow the procedure mentioned below to execute the case.

**Step 1: Choose the machine(s) you wish to configure**

- In this page, all the VM's under Standalone Hyper-V host will be displayed. According to the evaluation case, you need to **backup the entire host and exclude a VM and a disk**.
- Select the entire Hyper-V host using the check-box.
• Click **VM(s)/Disk(s) Exclusion** option. You need to exclude a VM and a Disk. Since we have selected an entire Hyper-V host for backup, all the VMs under that host will be selected for the backup. Select the VM you need to exclude from the list and click **Add**.

• The excluded VM will be listed in the Exclusion Settings page. If you need to remove the exclusion and add the VM to the backup schedule, click **Remove VM Exclusion**.
To exclude a disk from the backup schedule, click **Exclude Disk(s)** tab and click the **Edit Disk Exclusion** option.

There are three types of disk exclusion available:

- **No Disk Excluded** - No disks will be excluded. This is the default condition.
- **Include only System Disks for Backup. Exclude Others (typically Disk 0:0)** - This option will include the OS Disks for backup and exclude others. The disk with the number 0:0 will be included for the backup schedule regardless of the Disk type.
- **Select type of Disk to exclude** - opting for this option will allow you to select the type of the disk that has to be excluded from the backup schedule. Select the disk(s) that have to be excluded in each disk type. The two options available are IDE and SCSI. Click **Add** once you have selected the disks to be excluded and click **Save**.

The excluded disk will be listed in the Exclusion settings page. If you need to edit the disk exclusion, click **Edit Disk Exclusion**.

**Note:** Removal of already configured exclusion rules will have effect only from next additional full backup. It will not have effect on current full backup.

---

**Step 2: Configure Guest Processing**

- Application Aware feature provides data consistency for the applications (MS Exchange Server, MS SQL Server, MS SharePoint Server, MS Active Directory) that reside in the VM.
- Enable the **Application aware processing** option, Click the link to customize the settings and in the application aware settings page select **Truncate the transaction logs**.
- On selecting this option lets Vembu BDR truncate the exchange server logs before initiating the backup process. It purges and commits log files along with the .edb files and reduce storage space consumed.

**Note:** To perform application-aware image processing, the Guest Machine (running MS Exchange server, MS SQL Server, MS SharePoint Server, MS Active Directory) should be
installed with latest Hyper-V integration services.

---

**Step 3: Configure the backup schedule**

Configuring the backup schedule has three options to choose from:

- **Run Every** - Run the backup at regular intervals on specific day(s)
- **Run Daily** - Run the backup everyday in a specific time frame
- **Run Weekly** - Run the backup on particular days of the week at a specific time period

- The evaluation case involves to schedule Hyper-V backup Every Week of Monday by 09:00 PM select Run Weekly option. Select Monday and set the time at 09:00 PM.
The next step is to configure **Additional Full Backup for Last Sunday every month**.

Enable the **Additional Full Backups** option. Since the backup is scheduled to ‘Run Weekly’ you can configure Additional Full Backups for **Monthly** alone.

Configure when the Additional Full Backup has to run every month. There are two options you should select:
- The first drop down list specifies the day of the month the backup must run: **First**, **Second**, **Third**, **Fourth** and **Last**. Select **Last**
- The second drop down lists the days of the week. Choose **Sunday**

You have to retain a **maximum of 3 additional full backups**. From the **Store a maximum of** check box select **3**. Click **Next** to proceed with the backup schedule.

**Step 4: Configure the Retention Policy**

- You can choose the number of backup versions to be retained in the storage repositories by selecting the retention count. Retention is aimed at optimizing the storage utilization while adhering to your organization’s backup policy.
- Since this evaluation case requires you to **disable retention policy, do not enable retention**.
Note: By default, retention is not enabled and incremental backups will run forever.

Step 5: Configure Storage Repository

- The next step will be to change the storage repository from Default_Repo. Click the Add Storage Pool option to add a new storage pool. Give the storage pool a name and select the required volumes.
- The evaluation case involves making this storage pool as default pool. Click the Make it as Default Pool option. This storage pool will now be configured as the default storage pool. Click Save and select Next to proceed with the evaluation case.

Note: It is not recommended to choose OS Partition as Storage repository. Only [a-zA-Z][0-9][ - _ ] characters are allowed in the Storage Pool Name.

Step 6: Configure Encryption

- Backups configured from the Vembu BDR Server can be encrypted with a user-defined
password.
- Select **Enable Encryption** option. To create a new password, click on **Add Password**. Provide password of your choice along with a password hint and click **Save**.
- Newly created password will be available in the drop-down list. With the help of the encryption hint, you can easily identify the required password. Choose the password and click **Next**.

**Note:** Opting to the custom password will disable integrity check from being performed automatically. It is recommended to perform Quick VM Recovery periodically to ensure data integrity.

**Note:** Password and its hint should not be the same to avoid security issues.
Password should contain at least a character, a number and a special character [ ! @ # $ % ^ & * ].
Encryption hint should be at least 6 characters and not more than 25 characters.
Encryption hints are unique and no two passwords can have the same encryption hint.

**Step 7: Review Configurations**
- The last step in your Hyper-V backup configuration is to review the configurations you have selected. Enter a Backup Schedule Name. Vembu BDR Server supports creating multiple backup schedules each with its own configuration. The backup schedule name will uniquely identify the backup. While restoring your backup data, you need to choose the data to be restored using its schedule name.
- Review the following
  - Host/VM(s) Details
  - Scheduling Details
  - Retention Settings
  - Storage Pool & Encryption Settings

**Note:** There are few rules to be followed for specifying job name.
They are: Only [a-z][A-Z][0-9][ - _ ] characters are allowed in the job name.
Other Special Characters are not allowed in the job name.
The job name should not be more than 26 characters.
- Click **Save the backup** to save the backup schedule.
Evaluator's Guide for Hyper-V Backup

Case 4

- Edit the backup job and add a VM to the backup schedule
- Disable Application aware processing option
- Change the backup schedule to Run Weekly on Monday 09:00 PM
- Change the maximum number of full backups to be retained to 7 and run the additional full backup after saving the configuration
- Enable Retention and configure Advanced Retention
- Run the backup job immediately after saving the configuration

Editing a backup job for the above case will guide you through the basic steps involved in editing a backup job. The aim of this evaluation case is to let you know, the list of options which can be edited in an already configured backup schedule. Follow the procedure mentioned below to execute the case.

Step 1: Adding a VM to the backup schedule

- From the List All Jobs page, click the More option and select 'Edit' option
- From the list of VMs displayed, add a particular VM to the backup schedule
- You can choose the VMs to be backed up by selecting the checkboxes present near the VM. You can search for a particular VM in the Search VM checkbox. Click Next to proceed with the backup schedule.
Step 2: Disable the Application aware processing

- Application Aware feature provides data consistency for the applications (MS Exchange server, MS SQL Server, MS SharePoint Server, MS Active Directory) that reside in the VM.
- Disable Application aware processing option.
- Click Next to proceed with the backup schedule.

Step 3: Edit the Backup Schedule

Configuring the backup schedule has three options to choose from:

- **Run Every** - Run the backup at regular intervals on specific day(s)
- **Run Daily** - Run the backup everyday in a specific time frame
- **Run Weekly** - Run the backup on particular days of the week at a specific time period

- Since the evaluation case involves to run the backup weekly on Monday 09:00PM, select Run Weekly option and Monday as the day for the backup. Configure the time to 09:00PM which is the default time set.
Step 4: Edit the Additional Full Backup Settings

- The evaluation case involves changing the maximum number of full backups to be retained count to 7 and to Run the Additional Full Backup after saving the configuration.
- From the Store a maximum of full backups drop down list, change the value to 7 and select the Run the Additional Full Backup after saving the configuration check-box. Additional Full Backup will be triggered once this backup schedule is saved.
- Click Next to proceed with the backup schedule.

Step 5: Edit the Retention Settings

- You can choose the number of backup versions to be retained in the storage repositories by selecting the retention count. Retention is aimed at optimizing the storage utilization while adhering to your organizations backup policy.
- Since this evaluation case requires you to enable retention and configure advanced retention, select the Enable Retention option.
- As you have configured Run Weekly as the backup schedule, you can only configure monthly merge option in Advanced Retention. Select a time frame for the merge process and click Next to continue scheduling your backup.
Step 6: Review Configurations

- The last step in your Hyper-V backup configuration is to review the configurations you have edited. Vembu BDR Server supports creating multiple backup schedules each with its own configuration.

- Review the following
  - Host/VM(s) Details
  - Backup Schedule Details
  - Additional Full Backup Schedule
  - Retention Settings

- The evaluation case involves to run the backup immediately after you save this schedule, select the **Run this job immediately after saving** option. Your backup job will be triggered immediately after you save the backup, irrespective of the backup schedule configured.

- Click **Save the backup** to run your backup job.

You cannot edit the following options:

- Backup Encryption
- Encryption Hint
- Storage Repository
Job Name

Evaluators Guide for Hyper-V Backup

Manage Backup Job

- Click Backup icon to list the backup jobs
- The list of backup jobs configured from that particular client machine will be listed along with options to edit, suspend/resume, run/abort, delete the backup job
- Users can also view the Plugin type and historical report of a particular backup job

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Job Name</th>
<th>Host Name</th>
<th>Next Schedule Time</th>
<th>Suspend/Resume</th>
<th>Run Now</th>
<th>Status</th>
<th>Reports</th>
<th>More</th>
</tr>
</thead>
<tbody>
<tr>
<td>hyperv</td>
<td>localhost</td>
<td>192.168.102.203</td>
<td>Tue 27 Nov 2018 10:24 PM</td>
<td>✔️</td>
<td>idle</td>
<td></td>
<td>📊</td>
<td></td>
</tr>
<tr>
<td>2node</td>
<td>192.168.102.203</td>
<td>-</td>
<td>✔️</td>
<td>-</td>
<td></td>
<td>📊</td>
<td></td>
<td></td>
</tr>
<tr>
<td>case</td>
<td>192.168.102.203</td>
<td>-</td>
<td>✔️</td>
<td>-</td>
<td></td>
<td>📊</td>
<td></td>
<td></td>
</tr>
<tr>
<td>loc</td>
<td>localhost</td>
<td>-</td>
<td>✔️</td>
<td>-</td>
<td></td>
<td>📊</td>
<td></td>
<td></td>
</tr>
<tr>
<td>google</td>
<td>192.168.102.203</td>
<td>-</td>
<td>✔️</td>
<td>-</td>
<td></td>
<td>📊</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Suspend or Resume

- This option lets a user suspend and resume a configured backup job.
- A suspended backup job will not run schedules as per its configuration, until or unless it is resumed.

Run Now

- The Run now option is used to execute the backup job immediately.
- If run now is triggered in midst of scheduled interval, then the next schedule interval will be calculated from the time of the recent backup job.

Note: If a backup job is triggered in midst of scheduled interval with run now, then the next backup schedule will be triggered

Abort

- This option is used to abort a backup job that is currently in progress.

View

- This option allows you to view the saved configuration of any specific backup job.
Click the **edit** option to edit the backup job
Click the **List Backups** option to navigate to the list backup jobs page
In this page user can also create a new backup job, on clicking **Create New** button you will be prompted with the below pop-up to create a new backup job.

**Edit**

- This option allows you to edit the configuration of an already scheduled backup job.
- Edit option allows you to completely reconfigure the backup job being edited. (i.e) User can:
  - Add/remove VMs.
  - Reconfigure the schedule frequency, retention policies, additional backups and application-aware options of the backup job.
- Once done, review the edited configuration and save it.

**Delete**

- This option is used to delete the backup job, if no longer required.
- Proceeding with this option, will ask for deletion confirmation and click **yes** to confirm the deletion of backup job.
Evaluator's Guide for Hyper-V Backup

Recovery

Vembu allows you to restore your backup data from the Vembu BDR Server using multiple recovery options. With the need for different recovery options for different scenarios, Vembu offers restore cases as follows:

- **Case 1**: Recover VM instantly on another virtual host
- **Case 2**: Permanently restore backed up VM
- **Case 3**: Recover a single file
- **Case 4**: Instantly view/access files in a disk
- **Case 5**: Restore VM as a file type of your choice
- **Case 6**: Bare Metal Recovery

- Go to Recovery tab.
- Backups configured from various client machines to the server, will be listed for recovery, along with below-listed options:
  - Restore
  - Virtual mount
  - Persistent Boot delete
  - Delete
  - Full backup delete
  - Replication actions
  - Status
  - Reports
Virtual mount

- This option lets you instant mount backup data virtually where users can access backup in different file formats such as: IMG, VHD, VHDX, VMDK.

Mount Backup - VMCNoEncrypt

Are you sure you want to Mount the backup data in the Virtual drive?

Yes

Unmount Backup - VMCNoEncrypt

Backup image might be in use by recovery options such as Quick VM recovery or Disk Management Mount. Do you still want to unmount the backup from VirtualDrive?

Yes

To learn about how to manage Virtual Drive: Click Here

Replication actions

This option will be available only if the OffsiteDR replication is enabled. If enabled you will be provided with two options, Replicate now and Suspend.
- Replicate now option will allow you to trigger the OffsiteDR replication immediately
- Using the suspend option user can suspend the replication process
Persistent Boot delete

During each instant boot and instant file recovery session, a change in backup data will take place which then is saved as **Persistent Instant boot data**.

- Persistent data can be restored using restore options, if needed. The Persistent data will be listed with a (+p) sign alongside timestamps of backup versions.
- The persistent data can also be deleted if not required, using the 'Persistent Boot delete' option.
- This option allows user to choose the timestamp of persistent data to be deleted.
- User will also be required to confirm the deletion by selecting the checkbox 'Are you sure you want to delete the selected version related persistent boot data from the repository location permanently?' to proceed with deletion process.

```
Delete Persistent backup data of VM for this backup - VMC-UserGen
```

- **Delete** - There are two types of delete available in the restore page:
  - Delete - Delete the backup entry and data from the server
  - Full Backup Delete - Delete the latest full backup

Full backup delete

- If you have configured the additional full backup option you will have multiple versions of full backups. **Full backup delete** option allows you to delete the full backup
- Once you Click **Full backup delete** you will be navigated to backup report page where you can view multiple versions of full backup.
- Select the Full backup timestamp version you wish to delete. Click the delete icon.

```
```

- **Status** - Indicates whether a restore job is active or not.
• **Reports** - You can find various reports for the backup job such as:
  - Backup Report
  - Restore Report
  - Merge Report
  - Deleted Backup Report

**Evaluator’s Guide for Hyper-V Backup**

**Vembu Virtual Drive**

Vembu Virtual Drive is an exclusive feature of VembuBDR server, that allows user to instantly access backup data. With the help of VembuHIVE file system, Vembu Virtual Drive virtual mount backup data and allow instant access for users.

Vembu Virtual Drive will be installed during the installation of Vembu BDR Server and does not occupy any storage space in the hard drive. When you wants to access or is in need of certain files instantly, the backup data can be mounted from the BDR Server and can be accessed in the Vembu Virtual Drive. Once the required data is available in the virtual drive, you can take a copy of it separately.

Vembu Virtual Drive will make following file format types available for any image-based backups mounted in it:

- VHD
- VMDK
- VHDX
- VMDK-Flat
- RAW image files

These files can be used based on user requirements. For example, a VHD file can be mounted in Hyper-V or a VMDK file can be mounted in a ESXi server or a RAW image file can be mounted in KVM to create a virtual machine. VHD file can also be mounted in disk management to access file level backup data.

**Manage Vembu Virtual Drive (NFS Share)**

- Click the **Management** tab and select **Virtual Drive**

This page lists all image backups stored in backup server and user can virtual mount any backup data he wish to instant access.
To virtual mount a backup data, user have to click 'Mount' option alongside specific backup job to be accessed.

User can now have access to backup data by viewing VembuVirtualDrive displayed in My Computer.

Once done with requirement, user can unmount data by clicking on 'Unmount' option.

### Enable NFS Service on Vembu Virtual Drive

- Vembu Virtual Drive can be shared within a network area by enabling NFS service on Vembu Virtual Drive.
- NFS service for Vembu Virtual Drive is available on both Linux and Windows servers.

**Note:** For enabling NFS feature in Linux servers, it is necessary to have NFS kernel server installed in Backup Server machine. You can install NFS Service by using “apt-get install nfs-kernel-server” command. You need to run VembuBDR with root/administrator privileges in order to save NFS settings.

### Enable NFS Service on Linux - Sample image

#### Vembu Virtual Drive - NFS Share Settings

Enable NFS service on Vembu Virtual Drive

---

For enabling NFS feature, it is necessary to have NFS kernel server installed in Backup Server machine. You can install NFS Service by using “apt-get install nfs-kernel-server” command. You need to run VembuBDR with root/administrator privileges in order to save the NFS setting.

---

You can now attach and access Vembu VirtualDrive in ESXi® Server as a NFS datastore using the below steps.

1. Provide DNS Name/IP Address of Backup Server in "Server" field
2. Provide "VembuVirtualDrive" as Share in "Folder" field
3. Then provide a name for that datastore

Example: \192.168.10\home\vembudrive\Vembu\VembuBDR\Vembu\VirtualDrive

Now ESXi® hosts get direct access to the backed up image files(Raw VMDK) hence you can recover the backed up virtual machines.

### List of backups available for virtual drive mount/unmount

<table>
<thead>
<tr>
<th>Backup Name</th>
<th>Client Name</th>
<th>Plugin Type</th>
<th>Virtual Mount Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>server-1</td>
<td>aliagamai-360linuxxxx</td>
<td>vms</td>
<td>Mount</td>
</tr>
</tbody>
</table>

### Enable NFS Service on Windows - Sample image

#### Virtual Drive Management

NFS Share Settings

Enable NFS service on Vembu Virtual Drive

---

You can now attach and access Vembu VirtualDrive in ESXi® Server as a NFS datastore using the below steps.

1. Provide DNS Name/IP Address of Backup Server in "Server" field
2. Provide "VembuVirtualDrive" as Share in "Folder" field
3. Then provide a name for that datastore

Example: \192.168\10\home\vembudrive\Vembu\VembuBDR\Vembu\VirtualDrive

Now ESXi® hosts get direct access to the backed up image files(Raw VMDK) hence you can recover the backed up virtual machines.

### List of backups to virtual drive mount/unmount

<table>
<thead>
<tr>
<th>Backup Name</th>
<th>Client Name</th>
<th>Plugin Type</th>
<th>Virtual Mount Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMC-borDef</td>
<td>win138412br02</td>
<td></td>
<td>Mount</td>
</tr>
<tr>
<td>VMCDev001</td>
<td>win138412br02</td>
<td></td>
<td>Unmount</td>
</tr>
<tr>
<td>VMC-borDef</td>
<td>win138412br02</td>
<td></td>
<td>Unmount</td>
</tr>
</tbody>
</table>
NFS share service allows user to add VembuVirtualDrive as a NFS datastore in ESXi servers.

**Note:** Before enabling NFS service on Vembu Virtual Drive, please make sure Microsoft or any other third party NFS services is disabled to ensure uninterrupted service.

**Evaluator’s Guide for Hyper-V Backup**

**Evaluation Case**

- There are 6 cases listed under this section along with their procedures that will help you perform the restore operations. By the end of the cases, you will have used every recovery option and restored your backup VM data in various forms addressing different use cases.
- Although there are multiple recovery options, there are some common prerequisites to be met, for you to perform the recovery.

**Prerequisites**

- To perform a restore operation, you must have a VM that has been backed up successfully at least once
- The VM to be restored should not be undergoing backup or replication process at the time of restore

**Evaluator’s Guide for Hyper-V Backup**

**Case 1: Recovering a VM instantly on another virtual host**

**Quick VM Recovery** option allows you to instantly access the backup image as ready state VM in their production environment with minimal downtime (i.e) Minimal downtime and business continuity secured by making VMs instantly available. Quick VM recovery gives 3 choices of instant boot software to users:

- VMware (Available in both Windows and Ubuntu servers as an alternate software for instant boot)
- Hyper-V (Default chosen software for Windows and available only on Windows servers)
- KVM (Default chosen software for Ubuntu and available only on Ubuntu servers)

- During any disaster, Users would like to bring back their critical VM’s immediately into production host. As previously said, Quick VM recovery gives a user the privilege to access their backup data instantly. Using Quick VM recovery user can boot their virtual machine into different virtual environments such as VMware, Hyper-V and KVM
- Moreover, Users can directly boot the VM into their native host or to any virtual platform and check whether the Guest OS and application are working properly

**Procedure**

**Step 1: Choose the Restore Type**

- Click the **Recovery** tab and select the VM that is to be restored. Select **Quick VM Recovery** as the Restore type and click **Next**.
Step 2: Choose the Restore Version

The restore version is created based on the time period (i.e., the date and time) when the backup process is configured, where the full backup and incremental backup timestamp is viewed in form of hierarchical tree structure. You can select the full backup timestamp for restore as well as the individual incremental timestamp version for restore process. On selecting the full backup version, only the data of full backup version is restored.

- The regular routine of restore process is of selecting the timestamp version they wish to restore and click Next to proceed.
- On selecting the restore point, its appropriate data to be restored is displayed.

Step 3: Choose the Restore Data

In the restore data section, select the VM that you want to restore.

To select the restore data expand the host node. You will be allowed to select only one VM for the restore at a time.

- If you have configured only a single VM in this backup then it will display the backed up VM for restore.
- If you have configured an entire host in this backup, then it will list all the VM’s under the host in a tree structure. You can select the VM that you want to recover from the list.
- You can enter the VM name for quick search in the search field.
Once you have selected the VM, Click **Next** to proceed with restore options.

**Step 4: Select the Software for Quick VM Recovery**

- The next step will be to choose the environment in which the Quick VM Recovery is to be performed.
- Depending upon the target hypervisor where the VM needs to be booted, the restore options vary.
- In the Quick VM Recovery drop down list select any one from the following:
  - VMware
  - Hyper-V
  - KVM

**Restoring to a target VMware Server:**

- Select VMware from the drop-down list and the target VMware Server in which the VM is to be booted. If the target VMware Server is not displayed in the drop down list, click **Add VMware Server** option. Enter the Hostname/ IP Address of the VMware Server, select a credential from the list or add a new credential using the **Add Credentials** option.
- To know more about adding credentials, [Click here](#). Click **Add** to save the provided credentials.

**Note:** If you configure a port number that is already taken, you will get the message: "Network connection timed out. Invalid VMware Server IP or Invalid Port."
If you have entered an ESXi host IP, then you will be asked to select the target datastore location.

- In the Target datastore field, list of datastore available in the ESXi host will be listed select the target datastore using the drop down list

If you have entered the vCenter server address, then you will be asked to select the Target ESXi host in which you want to restore the VM

- In the target ESXi host field, select the target ESXi host using the drop down list. Once you have selected the ESXi host you will be asked to select the target datastore

**Note:** If the added server is a vCenter Server, select the **Target Host Name** from the list of ESXi hosts.

- In the Target datastore field, list of datastore available in the ESXi host will be listed select the target datastore using the drop down list

In the **VM name** field you can change the virtual machine name to identify the VM in the Target ESXi host or vCenter. You can also specify whether the VM should be powered ON automatically in the Target ESXi host or vCenter server after the completion of recovery.
**Evaluators Guide for Hyper-V Backup**

**Note:** Only [a-z][A-Z][0-9][ - _ ] characters are allowed in the VM name to be created.

### Restoring to a target Hyper-V Host

- From the Quick VM Recovery drop down list, select **Hyper-V**.
- Allocate the Startup RAM that is used for booting the VM. Click **Next** to proceed with the restore process.

**Note:** If you assign a higher physical memory (RAM) than the free memory currently available on your server the Quick Recovery may fail.

### Restore to a KVM Host:

- From the Quick VM Recovery drop down list, select **KVM**
- Allocate the Startup RAM that is used for booting the VM. Click **Next** to proceed with the restore process.

**Note:** If you assign a higher physical memory (RAM) than the free memory currently available on your server the Quick Recovery may fail.
Step 5: Review Configurations

- The final step in this restore process is to review the configurations you have selected.
- Check the following:
  - Restore type
  - Restore version
  - VM machine selected for restore
  - Booting Software
  - Target Server IP address
  - Target Datastore
  - Target VM Name
- Verify all the details and click Restore Now. This will trigger the Quick VM Recovery restore process.

Note: Once done with requirement, shutdown and turn off VM before unmounting backup data. This will resume backup job, so that incremental will run as per schedule.

- You will be redirected to the recovery page. From the status tab click the arrow mark which will open the restore progress window.
- The following details will be available in the restore progress page:
  - Backup Schedule
<table>
<thead>
<tr>
<th>Evaluators Guide for Hyper-V Backup</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
</tr>
<tr>
<td>Current File</td>
</tr>
<tr>
<td>Total Files</td>
</tr>
<tr>
<td>Transfer Rate</td>
</tr>
<tr>
<td>Files Restored</td>
</tr>
</tbody>
</table>

- **Note**: To enhance the restore performance, close the restore progress window and open it only occasionally to check the restore progress.

- You have the option of aborting the restore process. From the Recovery page click the **Abort Server Side Restore** option, this will open a pop-up window as displayed below. Click **Yes** to abort the restore.

  **Abort Restore - VMwareBackup_Test**

  The restore operation for this backup schedule will be aborted now. Do you wish to proceed?

  ![Abort Restore pop-up](image)

- Or open the restore progress window and click the **Abort (-)** option which will open a pop-up window displayed below. Click **OK** to abort the restore process.

  ![Abort Restore pop-up](image)
Evaluator’s Guide for Hyper-V Backup

Case 2: Permanently restore backed up VM

With Live Recovery to Hyper-V server option, users can restore the virtual machine to the same or different Hyper-V server. Live recovery to Hyper-V server is a permanent recovery process where the backed up virtual machine will be permanently restored to the Target Hyper-V server.

Procedure

Step 1: Choose the Restore Type

- Click the Recovery tab and select the restore icon near the Hyper-V backup that is to be restored. Select Live Recovery to Hyper-V Server as the Restore type and click Next.

Step 2: Choose the Restore version

The restore version is created based on the time period (i.e. the date and time) when the backup process is configured, where the full backup and incremental backup timestamp is viewed in form of hierarchical tree structure. You can select the full backup timestamp for restore as well as the individual incremental timestamp version for restore process. On selecting the full backup version, only the data of full backup version is restored.

- The regular routine of restore process is of selecting the timestamp version they wish to restore and click Next to proceed
- On selecting the restore point, its appropriate data to be restored is displayed
Step 3: Choose the Restore Data

In the restore data section, select the VM that you want to restore.

To select the restore data expand the host node. You will be allowed to select a single VM or multiple VM's for the restore at a time.

- If you have configured only a single VM in this backup then it will display the backed up VM for restore
- If you have configured an entire host in this backup, then it will list all the successfully backed up VM's under the host in a tree structure. You can select the VM's that you want to recover from the list
- You can also enter the VM name for quick search in the search field

Once you have selected the restore data, Click Next to proceed with restore options.

Step 4: Select the Restore options

This step allows you to set the restore settings for the Live recovery. You will be asked to enter or select the target server details
You will be asked to provide the target host details for the VM recovery (i.e.) To select the Target Host using the drop-down list in order to permanently restore the VM in the target Hyper-V host.

If you want to restore the VM to a new target host apart from the list, then manually enter the IP address/Host name of target Hyper-V server.

If you have selected the existing target host, then the target host credentials details will be automatically chosen from the drop-down list.

If it's a new Hyper-V host, then Click Add credentials and enter the target host credentials in the respective fields of the credentials manager pop-up window and save the host credentials.
• Now select the **Credentials** from the list and click the **Test Connectivity** option to check the connection between the Vembu BDR Backup server and Target host.

• This option allows you to check whether the **Vembu Integration Service** agent is installed in the Target Hyper-V host or not. If the VIS agent is installed you will get an alert window stating 'Vembu Integration Service' agent is already installed on the remote host. Click **ok** to proceed with the restore.
If the VIS agent is not installed, you will be asked to install the agent, click OK to install the VIS agent to proceed with the restore.

You need to allocate the RAM size for the VM (By default, set to 2 GB)

Choose a location where VHD/VHDX file (required for live recovery) will be downloaded

Note: Make sure the provided location have read/write access.

Click Next to proceed with the restore

Note: Incremental will not continue after performing Live Migration for the particular Guest
Live restore to Windows Server 2008 R2 and Windows Server 2012 is not supported for Generation 2 Guest Machines. Live Restore will proceed the restores with Default Configuration, the VM level settings such as Virtual Switch etc, will not be restored.

**Step 5: Review the restore settings**

- Once done configuring the recovery job, the final step will be to review all your configurations before proceeding to trigger the restore. The page list the Restore type, Selected restore version, Selected VM(s), Target location, Restore format

- Once done reviewing, click **Restore Now** to proceed with **Live Recovery to Hyper-V Server**
- You will be redirected to the recovery page once the restore process is completed
- You can view the status of the Restore from the 'Status' option. Once you click the inverted triangle, the below page will be displayed

The following details will be available in the Restore Progress Page window

- **Backup Schedule:** The Backup schedule name mentioned by you for indicating the backup during restore progress
- **Client Name:** The name of the client from which the backup process is initiated
- **Total Files:** The number of files present in the selected backup
- **Transfer Rate:** Speed of the restore process
- **Bytes transferred:** Rate at which the backup data is restored (Bytes, KB, MB, GB)
- **Files Restored:** Number of files restored during the process of recovery
- **Time Left:** Time remaining for the restore to complete
- **Abort:** You can abort your restore if not required from the 'Abort' (-) option available in that window. You will get a pop up as shown below. Click **Ok** to Abort your Restore
- **Suspend:** You can suspend your restore if not required from the Suspend option available in that window. You will get a pop up as shown below. Click **Ok** to Suspend your Restore
You have the option of aborting the restore process. From the Recovery page click the Abort Server Side Restore option, this will open a pop-up window as displayed below. Click Yes to abort the restore.

![Abort Restore - case](image)

The restore operation for this backup schedule will be aborted now. Do you wish to proceed?

No  Yes

Or Open the restore progress window and click the Abort (-) option which will open a pop-up window displayed below. Click OK to abort the restore process.

Evaluator's Guide for Hyper-V Backup

Case 3: Recover a single file

- Sometimes, you may want to restore specific VM data instead of restoring the entire VM data. The source VM may consist of data which might be needed later. As VM Recovery will happen as a whole (Entire VM Restore), some users do not prefer to restore the entire VM data as it occupies space and utilizes network bandwidth.
- In different restore scenarios user expect different restore options to perform their tasks. File Level Recovery option allows the user to instantly restore the individual files and folders present in the VMs that are backed up using Vembu BDR Server
- User can browse and select the individual files and folders from the backed up VM for restore instead restoring an entire VM or physical machine, which eventually saves restore time and makes the files easier to access

Procedure
Step 1: Choose the Restore Type

- Click the **Recovery** tab and select the restore icon near the Hyper-V backup that is to be restored. Select **File Level Recovery** as the Restore type and click **Next** to proceed with the restore process.

Step 2: Choose the Restore Version

- The restore version is created based on the time period (i.e. the date and time) when the backup process is configured, where the full backup and incremental backup timestamp is viewed in form of hierarchical tree structure. You can select the full backup timestamp for restore as well as the individual incremental timestamp version for restore process. On selecting the full backup version, only the data of full backup version is restored.
- The regular routine of restore process is of selecting the timestamp version they wish to restore and click **Next** to proceed.
- On selecting the restore point, its appropriate data to be restored is displayed.

Step 3: Choose the Restore Data

- A tree listing backed up VMs along with its disks which on further expansion will list respective files and folders in it. Select specific files and folders you want to restore.
- Once done selecting files/folders, proceed to choose restore location.
Evaluators Guide for Hyper-V Backup

Note: File level recovery is supported only for Windows virtual machines with NTFS Filesystems

Step 4: Configure the Restore Options

You can restore the file as a compressed zip file by selecting “Enable Compression” option. In addition, you can also enable encryption for the zip file by selecting “Encrypt Compressed data” option and by providing a password for the zip file to secure from unauthorized access.

- After the completion of restore to access the file in the Zip folder, Goto the restore location and user can access the file in the zip folder by entering the password set
- The compressed data can be available and can be downloaded in the Restore Reports
- Disabling Compression is applied when there is no limitation in the local network bandwidth and if required space is available in the destination location.

Note: Password should contain only the characters [a-z] [A-Z] [0-9]
Password should contain at least 6 characters and at most 12 characters
Password should not contain any spaces or other special characters

Select Restore Location

The target restore location can either be a local drive on the backup server or any network shared drive that you have mapped with Vembu BDR server. The restore can be directed to the network shared location.

- Click the Browse icon in the right of the restore location and choose the stipulated drive to where the data has to be restored
Step 5: Review the Restore Settings

- Once done configuring the recovery job, the final step will be to review all your configurations before proceeding to trigger the restore. The page lists the Restore type, Selected restore version, Target location.

- Once done reviewing, Click **Restore Now** to proceed with File Level Recovery.
- You will be redirected to the recovery page once the restore process is completed.
- You can view the status of the Restore from the 'Status' option. Once you click the inverted triangle, the below page will be displayed.

The following details will be available in the Restore Progress Page window:

- **Backup Schedule**: The Backup schedule name mentioned by the user for indicating the backup during restore progress.
- **Client Name**: The name of the client from which the backup process is initiated.
- **Total Files**: The number of files present in the selected backup.
- **Transfer Rate**: Speed of the restore process.
- **Bytes transferred**: Rate at which the backup data is restored (Bytes, KB, MB, GB).
- **Files Restored**: Number of files restored during the process of recovery.
- **Time Left**: Time remaining for the restore to complete.
- **Abort**: You can abort your restore if not required from the 'Abort' (-) option available in that window. You will get a pop up as shown below. Click **Ok** to Abort your Restore.
- **Suspend:** You can suspend your restore if not required from the Suspend option available in that window. You will get a pop up as shown below. Click **Ok** to Suspend your Restore.

![Suspend pop-up](image)

- You have the option of aborting the restore process. From the Recovery page click the **Abort Server Side Restore** option, this will open a pop-up window as displayed below. Click **Yes** to abort the restore.

![Abort pop-up](image)

- Or open the restore progress window and click the **Abort (-)** option which will open a pop-up window displayed below. Click **OK** to abort the restore process.

192.168.102.58:5060 says

The restore operation for this backup schedule will be aborted now. Do you wish to proceed?

![Abort pop-up](image)

**Evaluator's Guide for Hyper-V Backup**
Case 4: Instantly view/access files in a disk

- There may be situations in which you may want to access your backup data instantly, without having to restore the entire backup. Disk Management Mount option will be helpful in such scenarios. You can auto attach your backup data to the disk management and find your backup data available in the VembuVirtualDrive in various file formats such as IMG, VHD, VHDX, and VMDK.
- When the backup data is attached to disk management, the files will be created virtually by mounting the backup data. This restore type will be helpful in times of disk corruption. The restored virtual disk can be can be attached to any VM later.

Procedure

Step 1: Choose the Restore Type

- Click the Recovery tab and select the restore icon near the Hyper-V backup that is to be restored. Select Disk Management Mount as the Restore type and click Next.

Step 2: Choose the Restore Version

The restore version is created based on the time period (i.e the date and time) when the backup process is configured, where the full backup and incremental backup timestamp is viewed in form of hierarchical tree structure. You can select the full backup timestamp for restore as well as the individual incremental timestamp version for restore process. On selecting the full backup version, only the data of full backup version is restored.

- The regular routine of restore process is of selecting the timestamp version they wish to restore and click Next to proceed.
- On selecting the restore point, its appropriate data to be restored is displayed
**Note:** You can enable only one timestamp for restore at a time.

**Step 3: Choose the Restore Data**

In restore data section, select the data you need to restore.

- In this section you cannot select the entire VM for restore but you may have multiple disks in the virtual machine, so you can expand the VM node and select the particular disk file that you need to mount in disk management for restore

On selecting the restore data, you will be directed to review your restore configurations.

**Note:** You cannot mount more than one disk simultaneously. Choosing multiple disks for mount process will pop-out an Error message “User allowed to restore only one disk at a time. If you choose multiple disks, previous selection should be ignored.”

**Step 4: Configure the Restore Settings**

Once done configuring restore options, proceed to review configuration. The page list the Restore type, Selected restore version, Selected VM Machines(s) for restore.
Once done reviewing all the selected settings for restore, Click ‘Restore Now’ option to initiate the restore progress.

- Open the VembuVirtualDrive folder. You can find your backup data mounted in various formats.
Evaluator's Guide for Hyper-V Backup

Case 5: Restore VM as a file type of your choice

- Using Download VM Files option, you can download the backup data in multiple file formats such as VHD, VMDK, VHDX, VMDK-Flat and RAW. So that the different file formats can be used for the virtual mount process and creation of the virtual machines in different virtual environments when required.
- Taking offsite copies in various format allow users to boot backup data across various:
  - Virtual environments (Oracle Box, KVM, Hyper-V, VMware vSphere, VMware player etc.,)
  - Physical environments (Desktops and Workstations)
- Also, reconstruction of physical servers is also possible with this offline backup copies.

Procedure

Step 1: Choose the Restore Type

- Click the Recovery tab and select the restore icon near the Hyper-V backup that is to be restored. Select Download as the Restore type and click Next to proceed with the restore process.

Step 2: Choose the Restore Version

The restore version is created based on the time period (i.e the date and time) when the backup process is configured, where the full backup and incremental backup timestamp is viewed in form of hierarchical tree structure. You can select the full backup timestamp for restore as well as the individual incremental timestamp version for restore process. On selecting the full backup version, only the data of full backup version is restored.

- The regular routine of restore process is of selecting the timestamp version they wish to restore and click Next to proceed
- On selecting the restore point, its appropriate data to be restored is displayed

Note: You can enable only one timestamp for restore at a time.
Step 3: Choose the Restore data

In the restore data section, disks present in the backup VM will be listed in a hierarchical formation.

- You can select the disk or exclude the disks for restore. For example if your backed up VM has multiple disks under it, you can either select all the disks or select only the disks that you need to restore.
- You can view the individual volumes/drives under the disk by expanding the node but you are not allowed to select only the volumes/drives for restore.
- Click Next to proceed with restore options.

Step 4: Configure the Restore Options

The target restore location can either be a local drive on the backup server or any network shared drive that you have mapped with Vembu BDR server. The restore can be directed to the network shared location.

- Click the Browse tab in the right of the restore location and choose the stipulated drive to where the data has to be restored.

Note: Flat VMDK restore is not supported for Generation2 Guest OSes with more than 2TB disk.
Step 5: Review the restore settings

Once done configuring the Recovery job, the final step will be to review all your configurations before proceeding to trigger the Restore. The page list the Restore type, Selected restore version, selected disks/drives for restore, target location and type of disk format.

- Once done reviewing all the chosen settings for restore, Click ‘Restore Now’ option to initiate the restore progress.
- You will be redirected to the recovery page once the restore process is completed.
- You can view the status of the Restore from the 'Status' option. Once you click the inverted triangle, the below page will be displayed.

The following details will be available in the Restore Progress Page window

- **Backup Schedule**: The Backup schedule name mentioned by you for indicating the backup during restore progress
- **Client Name**: The name of the client from which the backup process is initiated
- **Total Files**: The number of files present in the selected backup
- **Transfer Rate**: Speed of the restore process
- **Bytes transferred**: Rate at which the backup data is restored (Bytes, KB, MB, GB)
- **Files Restored**: Number of files restored during the process of recovery
- **Time Left**: Time remaining for the restore to complete
**Abort**: You can abort your restore if not required from the 'Abort' (-) option available in that window. You will get a pop up as shown below. Click **Ok** to Abort your Restore

**Suspend**: You can suspend your restore if not required from the Suspend option available in that window. You will get a pop up as shown below. Click **Ok** to Suspend your Restore

---

**Note**: To enhance the restore performance, close the restore progress window and open it occasionally to check the restore progress.

---

**You have the option of aborting the restore process.** From the Recovery page click the **Abort Server Side Restore** option, this will open a pop-up window as displayed below. Click **Yes** to abort the restore.

---

**Or open the restore progress window and click the **Abort** (-) option which will open a pop-up window displayed below. Click **OK** to abort the restore process.**

---

192.168.102.58:6060 says

The restore operation for this backup schedule will be aborted now. Do you wish to proceed?

---

[Options: **No**, **Yes**]
Case 6: Bare Metal Recovery

Bare Metal Recovery (BMR) allows you to restore the Physical Window Servers, Desktops and Laptops from the scratch. This Restoration process brings back the system to its last-known stable state before the disaster or system crash.

Note: Dissimilar hardware is not supported

Procedure

The backed up Image file is downloaded from Vembu BDR Server and restore process is performed using Vembu Recovery CD which can be restored to the source hardware or new hardware. Bare Metal Recovery (BMR) is prone to lesser error as human intervention is minimized.

Follow the below steps to perform Physical Recovery for Image backups using Recovery CD:

Step 1 - Download VHD:

- Proceed with Download under Recovery options and choose VHD as your virtual disk format - [Click Here](#) to know the step by step process to download.

Step 2 - Install Windows AIK/ADK and Prepare Vembu Recovery CD Builder:

- To do Bare-Metal recovery using Vembu Recovery CD, download and install Windows AIK or ADK:
  - Click on following link to download Windows AIK: [Click Here](#)
  - Click on following link to download Windows ADK: [Click Here](#)
- Once Windows AIK/ADK is installed, download Vembu Recovery CD: [Click Here to Download](#)
- You will have Vembu Recovery CD in both 32-bit and 64-bit zip formats, download accordingly based on requirement. Now unzip the downloaded file and run RecoverCDBuilder with administrator privileges. You will get a window opened as displayed below.
Step 2 - Create Vembu Recovery ISO file:

- Read the Service Provider License Agreement carefully and click Agree. The next step is the VembuBDR Recovery CD Builder. The image is displayed below.

Note: When you have RAID and additional drivers to be set up in the machine to be recovered, such drivers can be bundled with Vembu Recovery CD using 'Additional Driver' option.
In this window, AIK/ADK location will be auto-filled, the target location is the location where you want to store ISO. Click Build to start creating an ISO file. You can monitor the progress of ISO creation.

- Once done, the ISO file will be available in the Target location you have entered.

Step 3 - Burn ISO file to a CD/DVD:
- Insert a blank CD in CD/DVD drive and burn the created ISO file in CD by right-clicking over ISO file and choosing the option 'Burn Disk Image'. Windows Disk Image Burner will open, choose the CD/DVD drive and click **Burn** to start burning process.

![Windows Disc Image Burner](image)

- You can monitor progressing of the burning process.

**Step 4 - Boot via CD/DVD and Run Vembu BDR Recovery Console:**

- Once the burn process completes, the CD will be auto ejected. Reinsert CD and reboot machine to BIOS settings. Change the boot priority and set CD/DVD as a primary boot device and click **Save** and **Exit**. VembuBDR recovery console will be opened as displayed below. Click **Next** to continue.
Step 5 - Accept Software License Agreement:

- Read the Software License Agreement carefully, click **Accept** and proceed with **Next**.
Step 6 - Initialize Disk/Partition Recovery:

- You will have the option to select a task from the below list:
  - Recover entire Disk or Partition
  - Set BCD Boot configuration
  - VMware Driver installation
Since we have to do physical recovery, proceed with 'Recover entire disk or partition' option and click Next.

Step 7 - Choose Source file and disk/partition to be restored:

- You will be directed to recovery page, where you will be required to provide details for following options:
  - Browse and select the file which you need to recover.
  - Browse and select the backup configuration file.
  - Select the disk/drive you wish to restore from the following list.
Once done choosing respective requirements, click Next to proceed.
Step 8 - Choose Target Disk/Drive:

- In next window, you will be required to select target disk/drive to which recovery will be performed. Once done selecting the target, click Next.

**Note:** The selected disk/drive will be formatted and only the recovered data will be available. Make sure you don't have any important data on target disk/drive.
• The recovery process will be initiated and once it is completed successfully, you can find your recovered data in the target disk/drive selected.

Evaluator's Guide for Hyper-V Backup

Reports

• Vembu offers three types of reports in the Vembu BDR Server web console delivering extensive information about the backup/restore jobs and their statuses.
• There is also an option which when configured delivers reports that you require, directly to your inbox on a regular basis.

  • Backup Job Report
  • Backup Status Report
  • Image Integrity Report
  • VM Status Report

Evaluator's Guide for Hyper-V Backup

Backup Job Report

Backup Job Report will display historical reports of the specific backup that is selected.

  • Go to the Recovery tab.
  • This page lists all the backup jobs configured to the server where you can see a report option alongside every backup job.
  • Click on Reports
    o Backup report
- Users can also filter the reports to view the status of full backups alone (excluding incremental).

**Evaluator’s Guide for Hyper-V Backup**

**Backup Status Report**

Backup Status Report lists all the backup jobs that are configured and its status. From the Reports tab select 'Backup Status Report' option.

- **Success** - Backup job completed successfully
- **Failure** - Backup job failed due to an error. The reason for the backup failure will be listed in the report
- **Missed** - When there is an error in the connection between the server and the target
- **Suspended** - When the backup schedule is skipped because the backup job is in a suspended state
- **Partial** - This message appears when the entire data is not backed up

- Along with the backup status, other information listed are Status, Client Name, Job Name, Schedule Type, Next Schedule Time, Remarks
• Clicking on a particular report will further expand the report and display details such as: Backup Start Time, Backup End Time and Plugin Type

• In the Backup Status Report page, you will have three tabs: Last 24 hours report, Latest Backup job status, Schedule email report

**Last 24 Hours Report**
The Last 24 Hours Report lists the backup statuses of all the backup jobs that occurred in the last 24 hours.

**Latest Backup Job Status**
The second tab, Latest Backup Status, lists the status of the latest backup job across all timestamps.

**Note:** By default, the backup status of the latest backup jobs from the last 24 hours will be listed

**Schedule Email report**

• Users can also send custom filtered reports by providing a sender Email address.
• And can choose a custom filter saved or add a new filter based on requirement.
• And choose schedules when to send:
  o Daily by specifying a time period.
  o Or choose weekly and specify a weekday and time period.

**Filter report**

Filter option lets you add custom filters wherein you can apply a filter of your choice for ease of view.
• The backup filter includes different status to choose from: missed, suspended, failed, successfully completed, partially completed.
Filters can also be applied based on duration. Provide the custom data range, apart from ranging between last 1-30 days.

Click View Report option to view the report immediately based on the filter you have configured. Click the Save & View Report to save the filter you have configured and then view the report.

Evaluator’s Guide for Hyper-V Backup

Email Configuration

- This section consists of 2 evaluation cases which will guide you in configuring the email reports.
- By the end of the cases, you will have used every option in the email reports section. This will help in addressing different use cases.

Evaluation Cases:
- [Case 1]
- [Case 2]

Evaluator’s Guide for Hyper-V Backup

Case 1

- Configure SMTP server settings and add your Email in the BDR console to send the Integrity Check report to your inbox.

Prerequisites

- This evaluation case requires you to have a backup job that has been successful
- The bootable disk should be present in the backup data to perform boot test

Procedure:
Step 1: Enable Email Configuration

- To configure open the Settings tab, choose Email and Configure option.
- By default, Email Configuration option will be disabled, Enable the Email Notifications option.

Step 2: Configure SMTP Server Settings

Enter the following details in order to setup the email ID:

- **SMTP Server** - The SMTP server using which the email reports will be sent
- **SMTP Server Port Number** - The port used by the SMTP Server. The default port number configured is 25

If your SMTP Server requires authentication, enable the This SMTP Server Requires Authentication checkbox and enter the following details:

- **Username & Password** - Login credentials of the email
- **Authentication Type** - Choose an authentication protocol among the following: PLAIN, LOGIN, CRAM-MD5, AUTO, ANONYMOUS, NTLM
- **SMTP Secure Protocol** - If a secure protocol is to be used, choose SSL or TLS, else choose NONE
- **Sender Email ID** - The email ID from which the report will be sent. You have the option of testing the Mail Server using the Test Mail Server option. Provide the Mail ID and select Send Test E-mail option.

![SMTP Server Configuration](image)

Step 3: Select Email Reports

- You can use the same email ID for receiving all the reports, but according to the evaluation case, only the Integrity Check reports is required.
- Select the Use different email ID for each report option and select Integrity Check.
- Enter the email ID to which the report has to be sent. Click Save.
Evaluator's Guide for Hyper-V Backup

Case 2

- Schedule a report that is emailed to your inbox every Monday at 09:00 AM. The report should list all the Suspended and Successfully completed backup schedules in the last 2 days.

Prerequisites

- This evaluation case requires you to have backup jobs that have been successful and backup jobs that have been suspended
- This evaluation can show you proper results for your understanding only if you run the backup job multiple times a day for at least 2 days
- The email ID that is going to be configured should be already added in the Email Configuration Settings. Refer the previous evaluation case for information on how to add an email.

Procedure:

Step 1: Configure Email

- Go to Reports tab and click Backup Status Report.
- Click on Schedule Email Report and enable the Email Report option.
- Enter your email ID in the Email Recipient text box.
Step 2: Configure Schedule

- In the Scheduling section, you will have two options to configure from:
  - Daily
  - Weekly On

- As per the evaluation case, you have to schedule a report to be emailed to your inbox every Monday at 09:00 AM. So, select Weekly On, select the day as Monday and set the time to 09:00 AM.

Step 3: Configure Filter

- Click the Add Filter option and enter the following details:
  - Filter Name - Name of the filter
  - Filter Status - According to evaluation case, the report should list all the Suspended and Successfully completed backup schedules in the last 2 days. So, select the Suspended and Successfully completed checkboxes
  - Filter by duration - Select Last 2 days
Click **Save** for saving the configured filter and click **Save** in the email schedule page.

**Evaluator’s Guide for Hyper-V Backup**

**Image Integrity Report**

- The Image Integrity Report verifies the recoverability of the backup job. It confirms if the backup data is mountable and provides boot image of the most recent backup. This ensures that the backup is in a readily-bootable state.

**Note:** All the image based backup jobs are listed and the jobs that get a "-" under the boot column cannot be verified.

- Along with the boot and mount results, you can find other details such as: backup name, plugin, client name, host name, machine name, disk name and scheduled time.
- **Mount Test** - The backup data is mounted in the disk management and a Tick appears when the mount process is successful.
- **Boot Test** - The VM is booted in the target host and a screenshot of the booted VM is available across each backup job. You can find the booted image by clicking on the Camera icon.

**Note**: Boot Check is not applicable for Data Partition.

You can configure a filter for this report by selecting the filter icon and enter the following details:
- **Client Name** - Name of the client
- **Backup Name** - The name of the backup job
- **Filter Status** - All, Success, Failed

- Click **Apply** after configuring the filter report. Click **Reset** to clear all the selections.
Evaluator’s Guide for Hyper-V Backup

VM Status Report

VM status report gives the user the centralized report page of all VM’s that are configured for backup. It allows user to view the detailed backup reports of virtual machines configured from both ESXi or Hyper-V Host.

This Reports will be generated separately for individual virtual machines that are configured for backup - VM Name, Host Name, Status, Plugin, Last Success, Last Schedule, Size.

<table>
<thead>
<tr>
<th>Plugin</th>
<th>VM Name</th>
<th>Host Name</th>
<th>Last Schedule</th>
<th>Status</th>
<th>Last Recovery</th>
<th>More</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test1</td>
<td>localhost</td>
<td></td>
<td>Tue 27 Nov 2018 16:09:48</td>
<td></td>
<td>Tue 27 Nov 2018 16:09:48</td>
<td></td>
</tr>
<tr>
<td>Cluster01</td>
<td>192.168.102.200</td>
<td></td>
<td>Tue 27 Nov 2018 16:02:39</td>
<td></td>
<td>Tue 27 Nov 2018 16:02:39</td>
<td></td>
</tr>
<tr>
<td>Small VM_21_13...</td>
<td>localhost</td>
<td></td>
<td>Mon 26 Nov 2018 23:00:10</td>
<td></td>
<td>Mon 26 Nov 2018 23:00:10</td>
<td></td>
</tr>
<tr>
<td>2008 R2 VM_22_1...</td>
<td>localhost</td>
<td></td>
<td>Sat 24 Nov 2018 16:25:08</td>
<td></td>
<td>Sat 24 Nov 2018 16:25:08</td>
<td></td>
</tr>
<tr>
<td>Small VM</td>
<td>localhost</td>
<td></td>
<td>Sat 24 Nov 2018 14:11:28</td>
<td></td>
<td>Sat 24 Nov 2018 14:11:28</td>
<td></td>
</tr>
</tbody>
</table>

- **Plugin** - Plugin Type of the backup job
- **VM Name** - Name of the VM
- **Host Name** - IP address of the virtual host
- **Last Recovery** - The recent successful VM recovery
- **Last Schedule** - The recent schedule of the VM backup job

- Selecting the More option will display the details mentioned below: **Backup Name**, **Incremental Number**, **Time Taken**, **Start Time**, **Size**, **Status** and **Remarks**
Evaluator’s Guide for VMware Backup

Quick VM Recovery Report

- This report provides detailed information on the Quick VM Recovery for the VMware and Hyper-V Plugins that are scheduled from the Vembu BDR backup server.
- From the Reports tab, select Quick VM Recovery option. This page consists of the following details:
  - Plugin: The plugin type whether VMware or Hyper-V
  - VM Name: The VM Name along with the timestamp used. The VM Name will be the name you have provided while configuring the Quick VM Recovery schedule.
  - Recovery Point: The timestamp that is used for the recovery.
  - Start Time: The time the Quick VM Recovery is initiated.
  - End Time: The time the VM is unmounted. (unmount option is triggered from Vembu BDR UI)
  - Target Hypervisor: The IP address of the target host configured for the restore process (ESXi or Hyper-V host).
  - Remarks: Remarks about the restore schedule.

- Using the Search option, you can search the required VM from the list. Type the required VM name in the checkbox and the related VMs will be listed. Moving the cursor over the VM Name will list the full VM name along with the restore timestamp.
Evaluator's Guide for Hyper-V Backup

Portal Registration

- You must create a Vembu Portal Account to register your backup server with Vembu Portal. In Vembu Portal you can manage all your Vembu products and services.

Creating a Vembu Portal Account:
Vembu portal is an all-in-one hub spot for managing your registered Vembu products and services where you can get started. To register in Vembu portal, follow the steps given below:

- Go to portal.vembu.com and click Sign Up.
- Provide the following details to create your account:
  - Company Name
  - First Name and Last Name
  - Email ID
  - Contact Number
  - Country and State
- Once done providing the requested details click Sign Up to register.
- A verification Email will be sent to the registered Email ID. Kindly check your Inbox(Spam folder, if not found in Inbox) for verification email and click Verify my email address option. If the button doesn't work copy-paste the link given below the 'Verify' button in your browser.
Welcome To Vembu Portal

Vembu Portal is an all-in-one portal where you can register for Vembu products & services.

Hi,

Welcome to Vembu Technologies and thanks for registering for a Vembu Portal account. You can purchase and manage your licenses for Vembu Products and Services from logging into your Vembu Portal account.

In order to complete your email verification process, please click the "Verify my email address" button below.

Verify my email address

Your Vembu Portal user name is: [redacted]

Email verification button not working?

If you are unable to click on the button above, you can complete your email verification by copying the below link and pasting it on your browser.

- You will be directed to a page with the registered Email ID and you will be requested to create a password for your account. Once done providing password, click **Activate**.

Vembu Portal account is now created successfully. Click **Login to Vembu Portal** option, provide the registered Email ID and password.
You can view the Vembu Portal Dashboard.

**Server Registration**

Once the Vembu Portal account is created
- Login to Vembu BDR web console.
- Go to **Management** tab and select **License** option.

**Registration Steps:**

- Click the **Register** option.
Provide Vembu account credentials in the pop-up shown and register the trial.

Once registered, you can check server registration by selecting the Run License Check option.

Evaluator’s Guide for Hyper-V Backup

Vembu BDR Suite Licensing

Vembu BDR Suite consists of three different types of editions with each edition introduced for a specific purpose. Get started with knowing the differences between the functionalities of these editions to make the best decision that fulfills the backup requirements of your business. Vembu also offers paid licenses for its customers which are of different types.

Perpetual License

- Perpetual licensing is a single time payment with which Vembu products can be used and
this license is applicable especially for IT admins and for all public sectors, Govt org and will be valid for a time period of 10 years from the date of issue.

- This includes all standard 24/7 FREE technical support for the first year and from the second year users need to pay AMC(Annual maintenance cost) which includes both standard technical support and maintenance. The AMC can be paid on the note of yearly or can be paid for multiple years as per the requirement.
- In perpetual licensing only primary on-premise backups can be done if you want to go for the Offsite you need to purchase license. The following will not be offered under perpetual licensing Vembu CloudDR, Vembu BDR360, Vembu OnlineBackup and Vembu SaaSBackup.

Subscription License

- The Subscription license will expire once your subscription period comes to an end, the users can pay up for annual or periodically. Users generally subscribe for a period of 1-5 years depending on their requirement. The subscription based license is applicable for everyone including the Service providers(SP).
- With Subscription licensing user will have a 24/7 standard technical support throughout the license period.

Note: For Desktop backups, you need to purchase support license separately.

- In the case of perpetual and subscription based licensing, the license will be generated for the number of VMware and Hyper-V host physical CPU sockets mentioned.
- There is no restriction for the number of VM’s running on the particular host.

FREE edition

- Post 30 days trial version, you can either opt to purchase the product or continue using the free edition.
- The free edition is equivalent to that of standard edition and in case of configuring a backup job you have minimal restrictions in features only.
- You can proceed the backup with any VM plugin (VMware/Hyper-V).
- Maximum of 3 VM’s can be selected in the Full featured free edition backup (Full backup and incremental backups).

Note: You can configure only one Full featured free edition backup job, other new backup jobs will proceed with Limited settings (or) you can delete the previously configured full featured backup job from the server and re-configure a new full featured backup job.

- If you configure a new backup then the backup will proceed with some restrictions, such as retention policy, additional full backups, etc., will not be supported for the Limited edition backups.
- Once free edition is activated, In Vembu VMBackup only the first backup will be sent as full featured backup and the other backups from the clients will be sent as limited edition backups.

Standard edition

- You can configure any number of backup jobs with Standard edition and in configuring a
backup job there are no feature restrictions, except VM replication and GFS retention.

**Enterprise edition**

- In Enterprise edition there are no feature restrictions, you can configure 'n' number of backups jobs and all the advanced features will be available for your backup job with this license.
- Check the edition-wise comparison of features [here](#)