# Table of contents

About Us .................................................................................................................. 5  
About Product ......................................................................................................... 5  
Document Structure ............................................................................................... 5  
Help and Support ..................................................................................................... 6  
Deployment ................................................................................................................ 6  
  Simple Deployment ................................................................................................. 6  
  Distributed Deployment .......................................................................................... 7  
Backup Components ................................................................................................. 7  
  Vembu BDR Backup Server .................................................................................... 7  
  Storage Repository ................................................................................................. 8  
  Vembu Universal Explorer ..................................................................................... 8  
System Requirements ............................................................................................... 8  
  Vembu BDR Backup Server ................................................................................... 9  
Supported Platform .................................................................................................. 10  
Port Configuration .................................................................................................... 11  
Naming Conventions ................................................................................................. 12  
Target/Source Host Permissions .............................................................................. 12  
Scalability and Infrastructure Sizing ......................................................................... 12  
Installation ................................................................................................................ 15  
  Windows Installation .............................................................................................. 15  
    Case 1: Installing Vembu BDR Server ................................................................. 16  
    Case 2: Uninstalling Vembu BDR Server ............................................................ 24  
    Case 3: Installing Vembu Universal Explorer .................................................... 26  
  Ubuntu Installation ................................................................................................. 29  
    Case 1: Installing Vembu BDR Server ................................................................. 30  
    Case 2: Uninstalling Vembu BDR Server ............................................................ 35  
Login to Web GUI ..................................................................................................... 36  
Storage Repository Setup .......................................................................................... 38  
  Add Storage Pools .................................................................................................. 41  
  Adding Network Drives .......................................................................................... 43  
  Storage Calculator ................................................................................................. 44  
  Delete All Data ....................................................................................................... 44  
Credential Manager .................................................................................................. 46  
Getting Started with VMware Backup ....................................................................... 48  
  Adding VMware Server ......................................................................................... 49  
  VMware Backup .................................................................................................... 51  
    Setup VMware Backup Job .................................................................................. 51  
      Step 1: Choose Host/VM Machine(s) ................................................................. 52  
      Step 2: Guest Processing .................................................................................... 57  
      Step 3: Configure Scheduling .......................................................................... 60  
      Step 4: Settings .................................................................................................. 61  
      Step 5: Review Configurations ......................................................................... 67  
Evaluation Case ........................................................................................................ 70
Case 2 ................................................................................................................. 194
Image Integrity ...................................................................................................... 196
VM Status ............................................................................................................. 199
Quick VM Recovery ............................................................................................... 200
Portal Registration ................................................................................................. 201
Vembu BDR Suite Licensing .................................................................................... 204
Evaluator's Guide for VMware 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.

Evaluator's Guide for VMware Backup

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
- Extensive scheduling and retention settings
- Replication of critical servers to a target ESXi host
- Multiple recovery options
- Verified recoverability

Evaluator's Guide for VMware Backup

Document Structure

- This document serves one purpose: To help you perform a hands-on evaluation of Vembu VMware 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, replication and recovery operations of your VMware environment. You will get a sense of the usability and the performance of Vembu VMware 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 VMware environment.
- Each of the cases presents a scenario, the prerequisites to be met and the procedure to perform the exercise. Only the information required to understand a feature and to perform a procedure is present in this guide.
- 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 VMware Backup

Help and 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/

You can ask a question in the Vembu Community forum:

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

You can find product demo videos and other tutorials at:

Evaluator's Guide for VMware Backup

Deployment

- Simple Deployment
- Distributed Deployment

Evaluator's Guide for VMware Backup

Simple Deployment

In this deployment scenario, you will require the following components:
1. Vembu BDR backup server
2. Backup Storage Repository
3. Source vCenter Server/ESXi host
4. Target vCenter Server/ESXi host (For replication scenario)
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 & replication jobs, Managing Storage Repository and other administration activities.

When you perform a backup or replication job from the Vembu BDR backup server, the VM data is directly processed from the vCenter Server/ESXi host 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 VMware Backup

Distributed Deployment

In this deployment scenario, you will require the following components:
1. Vembu BDR backup server
2. Vembu VMBackup client
3. Backup Storage Repository
4. Source ESXi host
5. Target ESXi host (For replication scenario)

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 VMware Backup

Backup Components

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

Evaluator’s Guide for VMware Backup

Vembu 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 Vembu 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 VMware 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.

**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)
- Automatic scale out functionality

**Evaluator's Guide for VMware 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 VMware Backup**

**System Requirements**

- [Vembu BDR Backup Server](#)
- [Supported Platform](#)
- [Port Configuration](#)
- [Naming Convention](#)
- [Target/Source Host Permissions](#)
- [Scalability and Infrastructure Sizing](#)
## Evaluator’s Guide for VMware Backup

### Vembu BDR Server

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Windows 10 Enterprise</td>
<td>Windows 10 Pro</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ubuntu LTS 18.04</td>
<td>Ubuntu LTS 16.04</td>
<td>Ubuntu LTS 14.04</td>
</tr>
</tbody>
</table>

<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>
</tbody>
</table>

| Network         | 1 Gbps & above. While replicating the on-site copy over WAN, 1 Mbps & above |

<table>
<thead>
<tr>
<th>Browsers</th>
<th>Internet Explorer 11 &amp; above</th>
</tr>
</thead>
<tbody>
<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 Vembu BDR backup server.

Normally, 4 GB RAM will be utilized to run the Vembu 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 allocating approximately 500 MB RAM for each active backup job. If you want to run 8 concurrent backup jobs in your Vembu BDR backup server, you should assign 8 GB RAM (4 GB for Vembu BDR backup server and 4 GB to process the backup jobs).
In order to avoid significant CPU usage during active backup progress, Vembu BDR backup server machine should be assigned with enough vCPUs or cores.
Normally, one vCPU or core is enough to handle 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 Vembu BDR backup server (Windows & Ubuntu) deployed in physical and virtual environments.

Evaluator's Guide for VMware 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>Platform</td>
<td></td>
</tr>
<tr>
<td>VMware vSphere 6.5</td>
<td></td>
</tr>
<tr>
<td>VMware vSphere 6.0</td>
<td></td>
</tr>
<tr>
<td>VMware vSphere 5.5</td>
<td></td>
</tr>
<tr>
<td>VMware vSphere 5.1</td>
<td></td>
</tr>
<tr>
<td>VMware vSphere 5.0</td>
<td></td>
</tr>
<tr>
<td>VMware vSphere 4.1</td>
<td></td>
</tr>
<tr>
<td>VMware vSphere 4.0</td>
<td></td>
</tr>
<tr>
<td>Hypervisor</td>
<td></td>
</tr>
<tr>
<td>ESX(i) 6.7</td>
<td></td>
</tr>
<tr>
<td>ESX(i) 6.5</td>
<td></td>
</tr>
<tr>
<td>ESX(i) 6.0</td>
<td></td>
</tr>
<tr>
<td>ESX(i) 5.5</td>
<td></td>
</tr>
<tr>
<td>ESX(i) 5.1</td>
<td></td>
</tr>
<tr>
<td>ESX(i) 5.0</td>
<td></td>
</tr>
<tr>
<td>ESX(i) 4.1</td>
<td></td>
</tr>
<tr>
<td>ESX 4.0</td>
<td></td>
</tr>
<tr>
<td>Management Server</td>
<td></td>
</tr>
<tr>
<td>vCenter Server 6.7</td>
<td></td>
</tr>
<tr>
<td>vCenter Server 6.5</td>
<td></td>
</tr>
<tr>
<td>vCenter Server 6.0</td>
<td></td>
</tr>
<tr>
<td>vCenter Server 5.5</td>
<td></td>
</tr>
<tr>
<td>vCenter Server 5.1</td>
<td></td>
</tr>
<tr>
<td>vCenter Server 5.0</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Virtual Hardware</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• The Virtual hardware of all types and versions are supported, which includes virtual disks larger than 2 TB and up to recent addition- 62TB VMDK</td>
</tr>
<tr>
<td></td>
<td>• VMware does not support snapshotting VMs with disks engaged in SCSI bus sharing; Such VMs are not supported by Vembu VMBackup.</td>
</tr>
<tr>
<td></td>
<td>• RDM virtual disks in physical mode, independent disks, and disks connected via in-guest iSCSI initiator are not supported and are skipped from processing automatically.</td>
</tr>
<tr>
<td></td>
<td>• Network shares and mount points targeted to 3rd party storage devices are also skipped as these volumes/disks are not visible in the VM configuration file.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OS</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• All VMware supported operating systems.</td>
</tr>
<tr>
<td></td>
<td>• Application-Aware processing support from Microsoft Windows 2003 SP1 and later.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Software</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• VMware Tools(optional) are required for Application-Aware processing and File-level restore from Microsoft Windows guest OS.</td>
</tr>
<tr>
<td></td>
<td>• All latest OS service packs and patches (required for Application-Aware processing)</td>
</tr>
</tbody>
</table>

---

**Evaluator’s Guide for VMware 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>443</td>
<td>HTTPS TCP</td>
<td>Port used for ESXi</td>
</tr>
</tbody>
</table>
Evaluators Guide for VMware 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 VMware Backup

Target/Source Host Permissions

- Root permissions on the source ESXi host
- Root or equivalent permissions on the Linux backup repository
- Write permission on the target folder and share
- If VMware vCenter Server is added to the backup infrastructure, an account that has administrator permissions is required. Instead of granting administrator permissions to the account, you can configure more granular permissions

Evaluator’s Guide for VMware Backup

Scalability & Infrastructure Sizing

<table>
<thead>
<tr>
<th>OS</th>
<th>Windows Server 2016 Datacenter</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Windows Server 2016 Standard</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2016 Essential</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 R2 Datacenter</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 R2 Standard</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 R2 Essential</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 Datacenter</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 Standard</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 Essential</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2 Datacenter</td>
</tr>
</tbody>
</table>
The performance of the VMware and Hyper-V backups depends on the RAM & CPU availability of the Vembu BDR backup server.

Normally, 4 GB RAM will be utilized to run the Vembu 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 Vembu BDR backup server, you should assign 8 GB RAM (4 GB for Vembu BDR backup server and 4 GB to process the backup jobs).

In order to avoid significant CPU usage during active backup progress, Vembu 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 Vembu 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](#).

### 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 Vembu 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**: v4.0.1

#### Backup Environment

- **Hypervisor**: VMware vSphere
- **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 Vembu 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 Vembu 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 Vembu 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 Vembu 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 Vembu BDR backup server’s 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 VMware Backup**

**Installation**

- [Windows Installation](#)
- [Ubuntu Installation](#)

**Evaluator’s Guide for VMware Backup**

**Windows Installation**

- [Case 1: Installing Vembu BDR Server](#)
- [Case 2: Uninstalling Vembu BDR Server](#)
- [Case 3: Installing Vembu Universal Explorer](#)
Evaluator's Guide for VMware 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.

![Browse For Folder](image)

**Note:** Make sure you have 1.2 GB of free space for installing Vembu BDR backup server.

### 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.
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.

![Vembu Backup & Disaster Recovery](image)

**Configuration Finished**

The installer has finished configuring Vembu BDR on this computer.

Click finish to exit installer.

- Start Vembu BDR application
- Open the Vembu BDR Web Console.

---

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

---

**Evaluator’s Guide for VMware 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 VMware 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.

### 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 Server**
- **Case 2: Uninstalling Vembu BDR Server**

**Evaluator's Guide for VMware Backup**

**Installing Vembu BDR 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 proprietary 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.

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: **HTTPS Port** 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.

Evaluated Guide for VMware Backup

Uninstalling Vembu BDR 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)
Proceding with option 1 will delete and uninstall existing VembuBDR instances. If you wish to continue, click yes.

Proceding 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 VMware Backup**

**Login to Web GUI - Vembu BDR**

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

- Entering the URL: [https://localhost:6061](https://localhost:6061) (or)
- [https://<IP_Address_of_Machine>:6060](https://<IP_Address_of_Machine>:6060) (or)
- Via shortcut icon created in the desktop
- Via web console option the tray icon
If you login to Vembu BDR web console after a fresh installation, you will be asked to choose the Time Zone in which the backup/replication reports are to be generated based on the configured time zone. 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.

(UTC+05:30) 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 once you have assigned the Vembu BDR ID. The Vembu BDR ID will be updated successfully and you will be redirected 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.

**Note:**
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.

**To check the version of Vembu BDR backup server**
- Open the web browser and type the following URL:
  - localhost:6060/readme.html (or) IP Address:6060/readme.html

<table>
<thead>
<tr>
<th>About VembuBDR Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Name</td>
</tr>
<tr>
<td>Build Name</td>
</tr>
<tr>
<td>Build Version</td>
</tr>
<tr>
<td>Build Number</td>
</tr>
<tr>
<td>Previous Version</td>
</tr>
<tr>
<td>Installation Date</td>
</tr>
<tr>
<td>VembuBDR Mode of Installation</td>
</tr>
<tr>
<td>VembuBDR Application Type</td>
</tr>
<tr>
<td>VembuBDR Installation Path</td>
</tr>
<tr>
<td>Small &amp; Medium Businesses and Remote / Branch offices edition</td>
</tr>
</tbody>
</table>

**Evaluator's Guide for VMware Backup**

**Storage Pool Management**
- Storage pool management option lets you manage and configure drives into separate storage pools for storing the backup data. Vembu BDR has a new file system that halts
backup for nothing and once the storage pool gets filled, you can extend the storage by using the edit option. New volumes can be added 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 choose the **Storage Pool** option.
- If it is a fresh installation, you must configure a storage pool before you begin scheduling your backup jobs. Select the **Click here** option or **Add** option to configure storage pool. Provide a storage pool name and select any set of volumes from the list of available storage volumes. Click **Save**. The space available and the backup location when that particular volume is selected as a storage pool will be displayed. Click **Next**.

**Note:** Only [a-z][A-Z][0-9][ - _ ] characters are allowed in the storage pool name.
When you have added more than one storage pool, you can choose any storage pool as your default storage pool. You can modify the default storage pool by enabling Set as default option alongside the respective storage pool you wish to set as default. If a particular storage pool is made as default pool the backups that occur after this will be stored in the new default storage pool only. The increments of the old backups will be stored in the previously configured default pool.

- You can add network volumes using the click here option or Manage Network Drive option available in the Network Volume section.
- Click here to go to Add Network Drive page.
- Click here to learn about Storage Pools.
- Click here to Calculate your Storage Space Requirements.
- Click here for steps to Reset Vembu BDR to Fresh Installation state.
Evaluator’s Guide for VMware 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.

    ![Storage Pool Management](image)

- 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.

### Add Storage Pool

- **Name of the Pool**: Default_Rpo
- **Make it as Default Pool**: Yes

#### Choose Volumes

<table>
<thead>
<tr>
<th>Storage Volumes</th>
<th>Space Usage</th>
<th>Backup Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>F:\</td>
<td>99.37 GB / 99.7 GB</td>
<td>F:\storage</td>
</tr>
<tr>
<td>G:\</td>
<td>10.64 GB / 10.95 GB</td>
<td>G:\storage</td>
</tr>
</tbody>
</table>

- **Size of the Pool**: 99.37 GB

- 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 VMware Backup**

**Manage Network Drives**

This option lets you add, delete network drives which will be listed along with a separate drive letter and can be configured for the storage location.

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

- Go to **Management** tab and select **Storage Pool** option. In the Network Volume section select the **Click here** option or **Manage Network Drive** option.

**Add & Manage Network drives:**

To add a network drive, provide the following attribute details:

- **Drive Name:** Provide a drive letter/name for network drive to be added.
- **Drive Path:** Network path of the drive to be added.
  
  Ex: `\<MACHINE_NAME OR IP_ADDRESS>\<SHARE_NAME>`

- **Username & Password** - If the network drive requires login authentication provide the username and password to authenticate drive addition.

- You can add ‘n’ number of network drives and manage it via **Manage Network Drives** page.

- An added network drive can be edited, click the **edit** icon from the Actions section and from the Mapped Drive Settings pop-up window, change the Username and Password.
Note: You cannot edit the Drive Name and Drive Path.

- A network drive added can be deleted if not required, with delete option alongside the drives added.

Evaluator's Guide for VMware Backup

Storage Calculator

Users with large data centers and high data traffic can 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 the link below to calculate your storage space requirements:

Vembu Storage Calculator

Evaluator's Guide for VMware Backup

Delete All Data

This option will allow you to completely wipe out your backup server data and reset Vembu BDR to fresh installation state.

- From the Management tab, select Storage Pool option and select Delete All.
The Delete All Data window will be displayed as shown below.

- To proceed with the deletion process, 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 Submit.

Note: 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. Once the delete process is notified with a success note, you have to manually delete the folder.
On proceeding with **I agree**, all the data will be removed and Vembu BDR will reset to a fresh installation state.

**Note:** Delete the 'Hyper-V / Windows Server' backup proxy entries manually from the BDR Server web console page ("Backup->Microsoft Hyper-V" for Hyper-V and Backup->Windows Server" for Windows Server. Also, remove 'VembuIntegrationService' on the respective "Hyper-V / Windows Server" host from 'Control Panel->Programs and Features'.

### Evaluator's Guide for VMware Backup

#### Credential

- 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 a backup or replication job (While adding server/physical machine/tape)**

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 a backup or replication 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**: the 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**: 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.
- 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 VMware Backup

Adding VMware Server

You need to add a source VMware Server before you begin configuring your VMware backup. The VMware Server can be a vCenter Server or an ESXi Host.

Prerequisites:
- The VMware Server should be of Licensed Edition
- The VMware Server should be of ESXi 4.0 & above and vCenter 4.0 & above

Procedure:
- From the Backup tab, select VMware vSphere. You will be taken to the Add VMware vCenter Server or ESXi host page.

Add the vCenter Server/ESXi Host by providing the following:
- Hostname/ IP Address: Enter the Hostname or IP address of the vCenter Server/ESXi host you wish to backup.
- You can add new credentials or select existing credentials. Click here to read more.
- 443: Port used for communication between the host and the Vembu BDR backup server.
Note:

- Vembu VMBackup does not support VMware backup for ESXi free versions because these versions do not support VMware APIs that are required for agentless backup
- Backing up encrypted VMs is not supported for vSphere host v6.7
- VM backup may fail with “VMware Modular exception error” in case of ESXi compatibility/permission issue with respect to vCenter

- Vembu BDR server communicates with the VMware server using the port that is set. By default it is set to 443. You can modify this port number in case you have configured a different port number for vCenter/ESXi communication. Click Save.
- Once the VMware Server is added, it will be available in the Manage Servers page. Click the Backup Now option to configure your backup schedule (or)
- Navigate to the Backup tab and click VMware vSphere. You can Edit or Delete the added VMware Servers in this list.

The Following details can be edited in an already added VMware Host

- You can select a different credential or add a new credential
• If you want to remove a particular VMware Server, click the Delete option. A pop-up window with the message "Are you sure you want to remove the host?" will appear. Click OK to delete your VMware Server.

Evaluator’s Guide for VMware Backup

VMware Backup

• Setup VMware Backup Job
• Evaluation Case
• Recovery
• Manage Backup Job

Evaluator’s Guide for VMware Backup

Setup VMware Backup Job

• Click the Backup option from the added VMware Server. You will be taken to backup configuration page where you can begin configuring your VMware backup schedule. Before you begin the backup process, you must configure a storage repository, else you will get the alert "You have not configured storage location. Please configure storage location before scheduling your backup. Click OK to redirect to Storage Pool Management page."

• There are 5 major steps involved in VMware backup. They are:
  o Choose Host/VMs machine(s)
  o Guest Processing
  o Configure Scheduling
  o Settings
Step 1: Choose Host/VM Machine(s)

- The first step in your VMware backup process is to choose the virtual machines that are to be backed up. From the list of VMs available select the required VMs for the backup process.
- If you have added a vCenter Server, all the ESXi hosts under that server and all the VMs under that ESXi host will be listed for backup.
- If you have added an ESXi host, all the VMs in that host will be listed with checkboxes.
- 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, type the name of the VM that is to be backed up and click the search icon.

**Note:** In a backup job where an entire host is backed up, if you add any new VM to that host, the new VM will be backed up in the next schedule.

- If you have selected an ESXi host for the backup schedule, you might want to exclude a specific set of VMs from the backup process. Such VMs can be excluded using VM(s)/Disk(s) exclusion option.

**Note:** Incase you haven't selected any VM for the backup and proceed with VM(s)/Disk(s) Exclusion you will get the message: Select the desired VMs or Host.

**VM Exclusion**

- Upon choosing the VM(s)/Disk(s) Exclusion option, you will get the pop-up window displayed below. Choose Exclude VM(s) tab.
Click **Select VM(s)** option which will list the VMs that are to be excluded from this backup schedule. Click **Add** option, this will add the VM to the Exclude VM list.

You can add more VMs to be excluded from the backup job by choosing **Select VM(s)** option or Remove an already excluded VM by selecting the **Remove VM Exclusion** option in the Actions tab. Click **Save** once you are done excluding the VMs from your backup schedule.
Disk Exclusion

- You can exclude a particular Disk type either at host level or VM level using Disk Exclusion option. Under Exclude Disk(s) tab, you will find the configured host(s) listed.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type of disk excluded</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.102.147</td>
<td>No Disk Excluded</td>
<td></td>
</tr>
</tbody>
</table>

Select the Edit Disk Exclusion option under the Actions tab to assign global disk exclusion rule for VMs under a chosen host. Edit Disk Exclusion tab will have the following exclusion rules:

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

No Disk Excluded: If you are configuring this option, none of the disks will be excluded from the backup schedule. By default 'No disks excluded' option will be selected.

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: 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 three options available are IDE, SATA and SCSI. Click Add once you have selected the disks to be excluded and click Save.

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.
Once you save the settings you will be alerted with the message “VM's/Disk's Exclusion configuration details saved successfully”.

- Disk exclusion can be configured for individual VMs. Select the VMs that have to backed up and click the **VM(s)/Disk(s) Exclusion** option.
- The VMs that you have configured for the backup will be listed, select the type of disk to be excluded. From the Actions tab, select **Edit Disk Exclusion** option.

- Select the **Edit Disk Exclusion** option under the Actions tab to assign global disk exclusion rule for VMs under a chosen host. Edit Disk exclusion tab will have following exclusion rules:
  - No Disk Excluded
  - Include only System Disks for Backup. Exclude Others (typically Disk 0:0)
  - Select type of Disk to exclude
No Disk Excluded: If you are configuring this option, none of the disks will be excluded. By default, No disks excluded option will be selected.

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: 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 exclude in each disk type. The three options available are IDE, SATA and SCSI. Click Add once you have selected the disks to be excluded and click Save.

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.

- Once you save the settings you will get the message "VM's/Disk's Exclusion configuration details saved successfully".
Step 2: Guest Processing

- The second step in the backup process is to configure Application Aware Settings. This feature provides data consistency for the applications (MS Exchange Server, MS SQL Server, MS SharePoint Server, MS Active Directory) that reside in the VM.
- During the backup process, the writers that are available will be checked if they are stable or not. Only if they are in a stable state the backup will proceed. This ensures a consistent database snapshot. Consistent database snapshot will be created by quiescing the applications using Microsoft VSS API.

Note: By default, Application Aware settings will be disabled.

- Select the Enable Application Aware Processing option. You can customize Application Aware configurations at Host/VM Level. Select the Click here option 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 - if you are configuring application aware settings at host level, the IP address of the host will be displayed. If you are configuring application aware settings at VM level, the name of the VM will be displayed.
  - VSS Writer Status - displays if the VSS writer status is required, ignored or disabled based on your selection.
  - Log Truncation Status - displays if 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.

<table>
<thead>
<tr>
<th>Manage Application Aware Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Add" /> <img src="image" alt="Edit" /> <img src="image" alt="Remove" /></td>
</tr>
</tbody>
</table>

- You can configure Application Aware rules for your entire ESXi host or the individual VMs residing in that ESXi host. Click the checkbox next to the entity name option, this will select all the entities. If you want to select individual entities, select the required entity (Host/VM) and click the **Edit** option.

**Note:** Make sure VMware Tools are running in Guest OS

- The Appaware Settings page will be displayed. You can configure the Application-aware processing configurations. Three options will be available:
  - **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.

- **Transaction log processing**: You can configure two options from this section:
  - **Truncate the transaction logs**: This option will purge the transaction logs and saves the space consumed by the application transaction logs.
  - **Disable Log Transactions**: The log transactions will be disabled and truncation won't happen.

**Note**: If **Disable Application processing** option is selected in Application-aware processing section, then transaction log processing will not be applicable.

- If you have selected a host for the backup process but want to set different Application aware rules for individual VMs, select the **+Add** option. This will open the Appaware settings page. Expand the host further by choosing the **+** option and select the VM to which different Application Aware rules must be set. Click the **Add** option. The selected VM will be added and displayed in the Customize settings page. Click the **Edit** option and edit the Application aware rules for the added VMs.

**Note**: Appaware backups is not supported for VM(s) with Desktop OS, 32 bit Guest OS.

- You can remove the VMs that you have added to the list by selecting the **x Remove** option. Click **Save** once you are done configuring the Application Aware Settings and click **Next** to proceed to the Credentials page.
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.

Evaluator's Guide for VMware Backup

Step 3: Configure Scheduling

- The Configure Scheduling option defines the frequency of your backup job. You can configure the backup schedules by choosing between Run Every/Run Daily/Run Weekly options.
- Select Run Every option if you want to run your VMware backup at regular intervals on a specific day(s). The time frame ranges from 15 minutes to 12 hours a day on specific days a week. By default, all the days in the week will be selected. If you don’t want to run your backup on all days, manually select the days in which you want to run the backup.
- If you want to run your backup every day, select Run Daily option and configure the time period in which your VMware backup has to occur.
- If you want to run your backup every week on a specific day and time, choose the Run Weekly option. Select the time frame and day in which you want to run the backup.

Note: By default, Run Every option will be selected for the backup schedule.
Additional Full Backups (Optional)

- In an enterprise environment, configuring a backup job with one full backup followed by incremental forever is not a recommended practice. There may arise a requirement wherein you need to schedule full backups frequently. Depending on the schedule of your backup, your 'incremental backups' can become quite big themselves.
- Running full backups frequently may sometimes lead to storage space consumption, due to which Vembu has developed an option to retain the number of Additional Full Backups.

Select the **Enable** Additional Full Backups option. For Run Every, Run Daily backups, the Additional Full Backup settings will allow you to configure Daily/Weekly/Monthly Additional Full Backups. If you have configured your backup to Run Weekly, then you can select Monthly Additional Full Backup option only.

You can specify the count for the maximum number of full backups to be retained. For example, when you set the count as 4 for retaining the full backups in the backup server, the latest 4 versions of the full backup will be maintained at all times. The default value for full backup retention is 2 and the retention count ranges from '01' to '99'.

**Note:** By default, Additional Full Backup will be disabled.

**Store a maximum of full backups:**

- You can limit the number of full backups to be retained with 'Store a maximum of' option.
- For example, If you need only 6 months data to be retained, it is recommended 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 and the incremental associated with that will be deleted.
- Once done configuring the backup schedule, click **Next** to configure retention policies for your backup.

**Note:** You can set the option with Store a maximum of till 99 Additional Full Backups for the scheduled backup

**Evaluator’s Guide for VMware Backup**

**Step 4: Settings**

In the Settings page, you can configure the following:
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:**

- 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.
- There are two types of retention:
  - 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 increments 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.

**Working:**

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).

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. will backup the data in 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. This recovery point will be marked as Daily merge (D).
- Similarly, on Day 4, the increments of Day 2 will be consolidated as a single restore point and the process will repeat 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.
- The daily merge of Day 1 will be 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.
- After the completion of one-week backup schedule, you will have 3 daily merged restore points with all the latest increments (2nd, 3rd and 4th Day Merged points). This process will continue to maintain the latest 3 daily merged data available at all times.

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

Advanced (GFS Retention):

- GFS otherwise known as Grandfather-Father-Son is an advanced version of basic retention which consists of multiple retention options for your backup data. The Multilevel GFS reduces the time taken to restore backed up machines and reduces the size of image files in the storage location. It helps in avoiding the formation of long chains of increments and allows you to meet the requirements of your retention policy.

GFS consists of three types of Merge:

- Daily Merge
- Weekly Merge
- Monthly Merge

Scenario 1: Advanced Retention policy enabled only Daily merge.

- On the successful completion of the 3rd days first incremental backup, the 1st day increments will get merged together to form a daily merge recovery point marked as (d).
- Similarly, on 4th day, the increments 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 increments till 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 up to 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 Daily, Weekly and Monthly merge, each merge process will get initiated on the user-specified day.
• If you have configured Weekly merge on Sunday, 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.
• 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 the user 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 increments 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.

**Note:** Daily Merge and Weekly Merge option is applicable for Run Every and Run Daily frequency. If you have configured Run Weekly for the backup schedule, you can select Monthly Merge option alone.

**Note:** By default, Retention will not be enabled. If enabled, Basic Retention will be selected.

---

**Storage Repository**

• Storage Repository is a management page that lets you manage and configure drives into separate storage pools for storing your backup data. Vembu BDR has a new file system that halts backup once a storage pool gets filled, you can expand 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).

**Storage Pools**

- Storage Pools are used to aggregate the space available from different volumes and utilize them as a single storage for specific backups.
- The backup storage that is configured during BDR server installation will act as a **Default Repository**.

Note: You cannot trigger any backup until a default pool is configured.

- You can add new volumes to create a pool for storing your backups. ‘n’ number of storage pools can be created and there are no restrictions on the volumes that 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 be stored in default storage repository of the 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.

**Steps to create Storage Pool:**

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

  - If the Storage Repository is already added during installation, the **Available Pool Space** for the chosen Repository 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. 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** - 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.

- 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 you wish to set default. If a particular storage pool is made as default pool the backups that occur after this will be stored in the newly configured default storage pool. But, the increments of the old backups will be stored in the previously configured default pool.

- **Click Save** once you have configured the storage pool.

### Encryption Setting

Backups configured from the Vembu BDR server can be encrypted with a user-defined password. Vembu BDR server encrypts each and every block instead of the encrypting the backup as a whole. This will secure your data using the AES-256 bit encryption algorithm.
Steps to add Encryption Password:

- To encrypt your backup, select the **Enable Encryption** checkbox. You can add your own password or encrypt the backup with a System Generated Password.
- To create a new password, click **Add Password**. Provide password of your choice along with a password hint and click **Save**.
- The newly created password will be available in the drop-down list. With the help of the encryption hint, you can identify the required password.

**Note:** By default, Vembu VMware backup uses the system-generated password to encrypt backups even if Encryption is disabled. You can opt to 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.

**Note:** Password and its hint should not be the same to avoid security issues. The 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.

- Once you have completed configuring the Encryption Password, Click **Save**. Click the **Clear** option if you want to clear out the Password and Encryption hint. Click **Next** to review your configurations.

**Note:** By default, Encryption Setting will be disabled.

Step 5: Review Configurations

- The last step in your VMware backup 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 configurations provided and enter an appropriate name for the backup schedule.
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 will be redirected to the **List All Jobs** page once you complete configuring the backup job. Verify the progress of your backup in the **Overall Progress Window**. To view the backup progress window, select the arrow mark in the **Status** section.
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.
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.

Warning: Are you sure you want to abort this backup VMwareTestBackup?

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

Evaluator's Guide for VMware Backup

Evaluation Case

- In this section, we have covered 4 evaluation cases that will guide you through the various features and configuration options available in VMware 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

- Configure a job to backup an entire ESXi host or vCenter Server
- Turn off Application Aware Settings
- 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

The steps that are mentioned below will guide you to create a backup job. Follow the steps to carry out the evaluation case.

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

- Since our requirement is to backup the **entire ESXi host**, select the source ESXi 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.

*Note:* If you have added a vCenter Server, the entire vCenter Server cannot be selected for the backup. The individual ESXi hosts under that vCenter Server will be displayed, select the required ESXi hosts or the VMS in that host for the backup schedule.

*Note:* If a specific ESXi host is a part of High Availability Cluster, backups of that specific host will continue even during a disaster.

Step 2: 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 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 VMware 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, 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:
  o Host/VM(s) Details
  o Scheduling Details
  o Retention Settings
  o Storage Pool & Encryption Settings
• Enter a backup job name.

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.

• The evaluation case requires to Enable the Run this backup job immediately after configuration, enable the option. 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.
Case 2

- Configure a backup job to backup only particular VMs from the source ESXi host
- Enable Application Aware processing and log truncation for specific VMs
- 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.

Procedure:

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

- In this page, the vCenter Server and the ESXi hosts under that vCenter will be displayed. Click the (+) near each ESXi host to expand the list further. According to the evaluation case, only particular VMs are to be backed up and not the entire ESXi host.
- Select the required VMs for the backup schedule and click Next to proceed with the backup schedule.
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 and select Click here option.

By default in the Appaware Settings pop-up window, the Require successful application processing and Truncate the transaction log option will be selected. Click Save.
- 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’s 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.

Note: 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 VMware backup job.
- Click **Next** to proceed with the backup schedule.

Note: By default, Vembu VMware Backup uses the system-generated password to encrypt backups even if Encryption is disabled. You can opt to 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.

**Step 7: Review Configurations**

- The last step in your VMware 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 complete the backup schedule configuration.

```
Evaluator's Guide for VMware Backup

Case 3

- Configure a job to backup an entire ESXi host and exclude a VM and a Disk from the host
- Enable Application Aware settings and ignore Application Processing Failures for an entire host
- 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
- Backup incremental forever
- Add a new storage pool for the backup job and make it as default pool
- Add a new password to encrypt the backup
```
You must perform the basic steps that are involved in creating a backup job to execute the evaluation case as mentioned above. Follow the steps that are explained below to execute the case.

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

- In this page, the vCenter Server and the ESXi hosts in the vCenter will be displayed. Click the (+) near each ESXi host to expand the list further. According to the evaluation case, you need to **backup the entire host and exclude a VM and a disk**.
- Select the ESXi host that you wish to backup.

- **Click VM(s)/Disk(s) Exclusion option.** You need to exclude a VM and a Disk. Since we have selected an entire ESXi 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 three options available are IDE, SATA 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 and select the **Click here** option to open the Manage Application Aware Settings page.
From the Manage Application Aware Settings page, select the checkbox near the ESXi host and click the **Edit** option.

In the Appaware settings page, select the **Ignored application processing failures** option and click **Save**.
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 VMware backup **Every Week of Monday** by 09:00PM 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 **backup incremental forever**, 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.

**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 VMware 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.
Case 4

- Edit the backup job and add a VM to the backup schedule
- Turn off Application Aware Settings for specific VMs under a host
- 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.

**Note:** You cannot edit a backup when it is in progress.

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: Turn Off Application Aware Settings

- 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.
- The evaluation case involves disabling the Application Aware Settings, disable the **Enable Application Aware Processing** option.
- Click **Next** to proceed editing 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 VMware 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 VMware 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:** Recovering a 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:** Attach a disk to another VM
- **Case 6:** Restore VM as a file type of your choice
- **Case 7:** Bare Metal Recovery

From the Vembu BDR server, select the 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

Selecting the **Restore** icon will allow you to configure your restore along with the options listed below:

**Restore**

- Selecting this option will lead you to select the restore type

**Note:** The Restore symbol is hidden or greyed-out due to following reasons.

- If the backup selected for restore is currently in backup progress.
- If the replication process is active for the backup that is selected for restore.
- If the full backup of the selected backup job fails to complete.
If the backup selected for restore is already processing a Restore job at that moment.

**Virtual mount**
- You can instantly mount your backup data virtually in the VembuVirtualDrive from where you can access your backup in different file formats such as: IMG, VHD, VHDX, VMDK. Click Yes from the pop-up window to mount your backup data.

**Mount Backup - Appaware_push_check**

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

- Once done with the requirement, unmount backup data. This will resume the backup job, so that increments will run as per schedule.

**Unmount Backup - Appaware_push_check**

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?

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 you can suspend the replication process

- **Persistent Boot Delete** - Persistent data can be restored using restore options if needed. The Persistent data is indicated with a (+P) sign alongside timestamps of backup versions. Such persistent data can be deleted using the 'Persistent boot delete' option. The option lets you choose the timestamp of persistent data to be deleted. 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 the deletion process.
**Note:** Deleting persistent data process is not permitted when the backup is virtually mounted

- **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

- **Offsite Replication** - If offsite replication is configured, an option to perform replication instantly will be available

Are you sure you want to replicate this job **SmallVM** now?

- **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
  - Offsite Copy Report

Select the **More** tab to view further details on the report. You will get the pop-up image displayed below.
From the drop-down list in the right top pane, select Full Backups option. You can delete your full backup by selecting the full backup timestamp version and the delete icon.

**Vembu Virtual Drive (NFS Share)**

Vembu Virtual Drive is an exclusive feature of VembuBDR server, that allows instant 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 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 your 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 be mounted in disk management to access file level backup data.

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

- Go to Management tab, and choose Virtual Drive option. This page lists all image backups stored in backup server. You can virtual mount any backup data which you wish to instant access.
To virtual mount a backup data, click the **Mount** option alongside specific backup job to be accessed.

You can access the backup data by viewing VembuVirtualDrive displayed in My Computer. Once done with requirement, unmount data by selecting the **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 the 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 to save NFS settings.

### Enable NFS Service on Linux Screenshot

![Enable NFS Service on Linux Screenshot](image)

**Note:** 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.

### Enable NFS Service on Windows Screenshot

![Enable NFS Service on Windows Screenshot](image)
**Evaluators Guide for VMware Backup**

**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 "Vembu NFS as Share in "Folder" field
3. Then provide a name for that datastore e.g. 192.168.10.10/Vembu/NFS

Now ESXi hosts will direct access to the backed up image/path/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>VMware_Test</td>
<td>192.168.100.79</td>
<td>VM</td>
<td>Mount</td>
</tr>
</tbody>
</table>

- NFS share service allows you to add VembuVirtualDrive as a NFS datastore in ESXi servers.

**Note:** Before enabling NFS service in Vembu Virtual Drive, make sure Microsoft or other third party NFS services are disabled for uninterrupted service.

**Evaluator's Guide for VMware Backup**

**Evaluation Case**

- There are 7 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 VMware Backup**

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

- In some scenarios, you might require instant access to your VMs or Physical Machines after a crash. **Quick VM Recovery** provides that option.
- **Quick VM Recovery** restores your VMware VMs instantly by reading the backup data in encrypted state from the storage repositories. Once the data is read, Vembu proceeds to create VHD, VHDX, VMDK, and IMG disks in the VembuVirtualDrive without occupying any physical storage. By using this VMDK, VHD file present in the Vembu Virtual Drive, Vembu creates a VM in the ESXi host/Hyper-V instantly. When the VM is booted and in a ready to use state, the changes that occur after this will be stored in a separate virtual disk file.
- **Quick VM Recovery** ensures minimal downtime and RTO less than 15 minutes.

You can choose to boot your backed up VM in any of the following hypervisors:

- VMware (Available in both Windows and Linux servers as an alternate software for instant
boot)

- Hyper-V (Default software chosen for Windows and available only on Windows Backup servers)
- KVM (Default software selected for Linux and available only on Linux servers)

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**

- Select the restore version for the restore process. The restore version is created based on the end time of the backup (i.e. the date and time when the backup process scheduled is completed), this is named as *Recovery points*. The full backup and incremental backup timestamps are listed with the latest backup version as a parent node and old backup version further sub-nodes. You can fall back to the required timestamp whenever needed to recover the backed up data.
- If you have configured *Additional full backups*, then separate restore version timestamp is created for each full backups with another tree structure.
- If the restore timestamp version is denoted with symbols (d), (w), (m), (+P) at the end, indicates that the Daily Merge (d), Weekly Merge (w), Monthly Merge (m), and Persistent boot changes (+P) process has taken place on the version. Here (d), (w), (m) restore version specifies the merge process has done on the recovery point and Persistent boot changes (+P) specifies the Quick VM Recovery process has been done for that version.
- If you select Restore version timestamp with (+P), you have to enable *Include persistent boot changes in restore* option to include the changes done during the previous boot restore process. If you don't enable the checkbox, then the changes will not be included in the selected recovery process.
- You can select the full backup timestamp for restore as well as the individual incremental timestamp version for the restore process. On selecting the full backup recovery point, only the data of full backup version is restored.

**Note:** You can enable only one timestamp for restore at a time.
• Select the restore version and click **Next** to proceed to select restore data.

**Note**: If you have backed up multiple VMs, you can restore only one VM at a time using Quick VM Recovery option.

**Step 3: Choose the Restore Data**

• Once you are done selecting the restore version, the next step is to select the Restore data. From the drop down list, select the VM that is going to be recovered.
• You can search for a particular VM from the search tab. Click **Next** to proceed to configure 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
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."

- Proceed to select the **Target Datastore**. If the added VMware Server is an ESXi host, select the **Target Datastore** from the list of datastores present in that host. If the added server is a vCenter Server, select the target ESXi Server and the target datastore.

- Provide a VM Name. This is the name with which your VM will be created in the datastore you have configured.

- Enable the **Power on VM automatically** option if you want your restored VM to be powered ON automatically. Click **Next** to proceed with the restore process.
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:
Evaluators Guide for VMware Backup

- Backup Schedule
- User Name
- Current File
- Total Files
- Transfer Rate
- Files Restored

**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.

![Abort Restore](image)

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

![Abort Restore](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.
Case 2: Permanently restore backed up VM

- If you want to permanently restore your VMs either to the same host or to a different virtual host, it can be done through the Live Recovery to ESXi Server option. The VMs will be restored into the data store that is present in the storage repositories.
- Once the restore process begins, Vembu utilizes any one of the following VMware data transport modes depending upon the configurations you provide for restoring the VM data. The modes are as follows:
  - HotAdd mode
  - Direct SAN mode
  - Network mode
- Vembu will restore your VMs through HotAdd mode if your BDR Backup server is employed as a Virtual Machine in the ESXi host. Once the Full VM Recovery process begins, the VM data will be restored by attaching an empty disk either to BDR Backup server or to your VMBackup proxy. After the data transfer to the attached disk is completed, the disk will be reattached to the VMs that are restored.
- Vembu will restore your VM data through Direct SAN mode if your BDR Backup server, ESXi host, and VM Datastore are deployed in a SAN Environment. Vembu will start the data transfer through SAN mode by utilizing FC SAN or iSCSI SAN for transferring the VM data.
- When you transfer data through LAN, Vembu uses NBD (Network Block Device) and NBDSSL (Secure NBD) as the transport mode for data transfer. The VM data will be transported to the ESXi host or vCenter server through a TCP/IP connection. The difference between NBD and NBDSSL mode is that the data transfer will be encrypted between the virtual host and the BDR Backup Server in NBDSSL mode.

**Procedure:**

**Step 1: Choose the Restore Type**
Click the **Recovery** tab and select the **restore** icon near the VMware backup that is to be restored. Select **Live Recovery to ESXi Server** as the Restore type and click **Next**.

**Step 2: Choose the Restore Version**

- The next step will be to choose the restore version (time-stamp) of your backup data. The latest restore version will be at the top of the tree followed by the older restore versions. If the time-stamp consists of the Persistent data (+P) option and you restore that version, all the changes you have made in the VM will be restored. The restore version also consists of (d)- daily merge, (w)- weekly merge and (m)- monthly merge.
- The restore version is created based on the end time of the backup (i.e the date and time when the backup process scheduled is completed), this is named as Recovery points. The full backup and incremental backup timestamps are listed with the latest backup version as a parent node and old backup version further sub-nodes. You can fall back to the required timestamp to recover the backed up data.
- Select the **Include persistent boot changes** in the restore option if you want to restore your backup data along with the changes made.

**Note:** The 'Include persistent boot changes in restore' option will be available only if you are restoring the time-stamp with (+P)

- Select the restore version and proceed to select restore data.
Step 3: Choose the Restore Data

- Once you are done selecting the restore version, the next step is to select the Restore data. You can select the entire VM or select individual disks under that VM for the restore process.
- You can search for a particular VM from the search tab. Click Next to proceed to configure restore options.

Step 4: Configure Restore Options

While configuring the Live Recovery restore option, you can customize the options for your hardware configurations for the target VM. You can customize the configurations details for the target VM such as:

- Changing the memory
- No. of CPUs
- No of Cores Per Socket
- Virtual Machine Disk provision types
- Network

- If you have backed up more than one VM, while restoring you can select a single server to which the VM will be restored. Click the Select Target Server option and select the server to which the VMs will be restored or if you want to restore your VMs to individual servers,
click the **Select Target Server** option in the Host Name section.

- Select the required server from the **Servers** drop down list or add a new server using the **Add VMware Server** option. Provide the Hostname/IP Address of the server and select a credential from the **Select Credentials** drop down list. You can add a new credential using the **Add Credentials** option. [Click here](#) to read more on adding credentials.

![Target Server Details](image)

**Add Server**

- **Hostname / IP Address**
- **Select Credentials**
- **Add Credentials**
- **443**
- **Add**
- **Cancel**

- If you have added a vCenter Server select the following:
  - Select the ESXi Host
  - Select the Target Datastore
  - Enter the Target VM Name

- If you have added an ESXi host, enter the following details:
  - Select Target Datastore
  - Enter Target VM Name

- Click the **More** option near the target VM name and configure the settings. Auto filled values will be taken from source VM configurations.

- While restoring, you can choose different disk types. The disks that have been backed up
will be listed, choose the respective disks that are required disk type. The types are:
- Thin
- Thick [Eager Zeroed]
- Thick [Lazy Zeroed]

- You can customize your CPU and memory settings. The maximum and minimum values is based on the target ESXi server's configuration. You cannot provide a value that exceeds the maximum supported value. For example, ESXi server Version 4.0 supports max CPU Sockets upto 8 while ESXi server version 6.5 supports upto 128. Make sure you provide the value within the maximum and minimum value range displayed, else the message "Provided value for memory is not in the specified range" will pop-up, similar for CPU settings.

- Check whether you have selected the same configurations that are applicable in the target server also, else the message "VM(s) selected for restore is incompatible with the selected target server. Please select different target server" will appear. Refer this link: https://kb.vmware.com/s/article/2051652

Note: If you enter the same VM name, the message name "VM with same name already exists in selected host. Please enter different VM name" will pop-up.

- Click Next to review your configurations

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

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
  - Target Server IP address
  - Target Datastore
  - Target VM Name
• Verify all the details and click **Restore Now**. This will trigger the Live Recovery to ESXi Server process.

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
- User Name
- Current File
- Total Files
- Transfer Rate
- Files Restored

**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.

Abort Restore - VMwareBackup_Test

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

- 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?

OK  Cancel

Evaluator's Guide for VMware Backup

Case 3: Recover a single file

- Sometimes, you might 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.

- To handle such scenarios Vembu offers File Level Recovery which allows you to restore files and folders of your choice from the backed up VM. Once you configure the restore location and trigger the restore process you can find your backup files in the specified location within minutes.

Step 1: Choose the Restore Type

- Click the Recovery tab and select the restore icon near the VMware 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 next step will be to choose the restore version (time-stamp) of your backup data. The latest restore version will be at the top of the tree followed by the older restore versions. If the time-stamp consists of the Persistent data (+P) option and you restore that version, all the changes you have made in the VM will be restored. The restore version also consists of (d)- daily merge, (w)- weekly merge and (m)- monthly merge.

- The restore version is created based on the end time of the backup (i.e. the date and time when the backup process scheduled is completed), this is named as Recovery points. The full backup and incremental backup timestamps are listed with the latest backup version as a parent node and old backup version further sub-nodes. You can fall back to the required timestamp to recover the backed up data.

- Select the Include persistent boot changes in the restore option if you want to restore your backup data along with the changes made.

Note: The Include persistent boot changes in restore option will be available only if you are restoring the time-stamp with (+P)

Step 3: Choose the Restore Data

- Once you are done selecting the restore version, the next step is to select the Restore data. A tree listing backed up VMs along with its disks will be displayed. Click (+) to explore the
virtual machine further from the web based console instead of opening the machine and accessing the files. On further expansion the respective files and folders will be listed. Select the specific files and folders that have to be restored. Click **Next** to proceed to configure restore option.

**Note:** Vembu supports File Level Restore only for NTFS File System. If there is an error while listing VM(s)/Disk(s)/Volume(s), check if Vembu Storage volume is corrupted/ chunk files are not available.

---

**Step 4: Configure Restore Options**

- The next step is to select whether you want to compress your restore data. Select the **Enable** option for compressing your restore data.
- You can encrypt the compressed data by selecting the **Encrypt Restored files for Zip process** option. Provide the encryption password and configure the restore location where the files are to be restored. 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 which the data will be restored.
- Once the restore is complete, go to the restore location to access the Zip folder. Enter the corresponding password to access the Zip file. The compressed data will be available and can be downloaded from the Restore Reports page.

**Note:**

The password you enter should satisfy the following conditions:

1. Password should contain only the characters [a-z] [A-Z] [0-9]
2. Password should contain at least 6 characters and at most 12 characters
3. Password should not contain spaces or other special characters

- Click **Next** to proceed to review your configurations.
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
  - Target restore location
- Verify all the details and click Restore Now.

- You will be redirected to the recovery page. In 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
  - User Name
  - Current File
  - Total Files
  - Transfer Rate
  - Files Restored
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.
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.

**Step 1: Choose the Restore Type**

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

**Step 2: Choose the Restore Version**

- The next step will be to choose the restore version (time-stamp) of your backup data. The latest restore version will be at the top of the tree followed by the older restore versions. If the time-stamp consists of the Persistent data (+P) option and you restore that version, all the changes you have made in the VM will be restored. The restore version also consists of (d)- daily merge, (w)- weekly merge and (m)- monthly merge.
• The restore version is created based on the end time of the backup (i.e. the date and time when the backup process scheduled is completed), this is named as Recovery points. The full backup and incremental backup timestamps are listed with the latest backup version as a parent node and old backup version further sub-nodes. You can fall back to the required timestamp to recover the backed up data.

• Select the **Include persistent boot changes** in the restore option if you want to restore your backup data along with the changes made.

• Select the restore version and click **Next** to proceed to select restore data.

**Note:** The 'Include persistent boot changes in restore' option will be available only if you are restoring the time-stamp with (+P)

![Screenshot of the restore version selection page](image)

**Note:** If the backup is mounted unmount the backup from Recovery page and then proceed with the restore process.

**Step 3: Choose the Restore Data**

• Once you are done selecting the restore version, the next step is to select the Restore data. Select the disk that has to be mounted in the disk management for the restore process.

• You can search for a particular VM from the search tab. Click **Next** to proceed to review your configurations.

**Note:** You cannot mount more than one disk simultaneously. Choosing multiple disks for mount process will display error message "User allowed to restore only one disk at a time. If you choose multiple disks, previous selection should be ignored."
Step 4: 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
- Verify all the details and click Restore Now. This will trigger the Disk Management Mount process.

**Note:** Once done with the requirement, unmount backup data. This will resume the backup job, so that increments will run as per schedule.

- You will be redirected to the recovery page. In 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
  - User Name
  - Current File
  - Total Files
  - Transfer Rate
  - Files Restored
Note: To enhance the restore performance, close the restore progress window and open it occasionally to check the restore progress.

- Open the VembuVirtualDrive folder. You can find your backup data mounted in various formats.

Case 5: Attach a disk to another VM

- **Disk Level Recovery** allows you to restore an individual disk from the VM that is backed up. The disk will be restored to the target VM and will be attached so that it can be accessed from that target VM.
- In some cases, you can also attach the restored disk to your original VM in case of any disaster. Once the disks are attached to the target VM, you will be alerted to manually reboot the VM so that the configurations get updated.
Step 1: Choose the Restore Type

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

![Image]

Step 2: Choose the Restore Version

- The next step will be to choose the restore version (time-stamp) of your backup data. The latest restore version will be at the top of the tree followed by the older restore versions. If the time-stamp consists of the Persistent data (+P) option and you restore that version, all the changes you have made in the VM will be restored. The restore version also consists of (d)- daily merge, (w)- weekly merge and (m)- monthly merge.
- The restore version is created based on the end time of the backup (i.e. the date and time when the backup process scheduled is completed), this is named as Recovery points. The full backup and incremental backup timestamps are listed with the latest backup version as a parent node and old backup version further sub-nodes. You can fall back to the required timestamp to recover the backed up data.
- Select the Include persistent boot changes in the restore option if you want to restore your backup data along with the changes made.
- Select the restore version and proceed to select restore data.

**Note:** The 'Include persistent boot changes in restore' option will be available only if you are restoring the time-stamp with (+P)
Step 3: Choose the Restore Data

- Once you are done selecting the restore version, the next step is to select the Restore data. Select the disk that is to be restored. You can search for a particular VM from the search tab. Click Next to proceed with the restore process.

Step 4: Configure Restore Options

- The next step is to configure the target server details. Select whether the target server is an ESXi host or a vCenter Server.
- If the target server is a vCenter Server, select the vCenter Server details and enter the following:
  - Select ESXi Host
  - Select the Target VM Name to which the disk is to be attached
  - Select Target Datastore

- If the target server is an ESXi host, add the ESXi host details and do the following:
  - Select the Target VM Name to which the disk is to be attached
  - Select Target Datastore
If the VMware Server is not listed in the drop-down list, add the ESXi host or vCenter Server through the Add VMware Server option. Provide the target server Hostname/IP address, select the credentials from the Select Credentials drop-down list or add a new credential using the Add Credentials option. Click here to read more on adding credentials.

Configure the Port number, by default the value is 443. Click Add to add the VMware Server.

Once done providing the details, Click Next to proceed to review your configurations.

Note: The target virtual machine will be powered off for performing disk restore.

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
- Verify all the details and click **Restore Now**.

- You will be redirected to the recovery page. In 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
  - User Name
  - Current File
  - Total Files
  - Transfer Rate
  - Files Restored
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.

![Abort Restore - VMwareBackup_Test](image1)

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

- 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.

![Restore Progress of Test_Restore - Mozilla Firefox](image2)

**Evaluator’s Guide for VMware Backup**

**Case 6: Restore VM as a file type of your choice**

- With **Download** option, you can download your backed up VM data as an offsite copy to a local destination. You can migrate your VMs across hypervisors (V2V) by downloading the file-format required for the target hypervisor. Backup data can be downloaded in various virtual disk formats which are mentioned below:
  - VHD
  - VHDX
  - VMDK
Step 1: Choose the Restore Type

- Click the Recovery tab and select the restore icon near the VMware 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 next step will be to choose the restore version (time-stamp) of your backup data. The latest restore version will be at the top of the tree followed by the older restore versions. If the time-stamp consists of the Persistent data (+P) option and you restore that version, all the changes you have made in the VM will be restored. The restore version also consists of (d)- daily merge, (w)- weekly merge and (m)- monthly merge.
- The restore version is created based on the end time of the backup (i.e the date and time when the backup process scheduled is completed), this is named as Recovery points. The full backup and incremental backup timestamps are listed with the latest backup version as a parent node and old backup version further sub-nodes. You can fall back to the required timestamp to recover the backed up data.
- Select the Include persistent boot changes in the restore option if you want to restore your backup data along with the changes made.
- Select the restore version and proceed to select restore data.

Note: The ‘Include persistent boot changes in restore’ option will be available only if you are restoring the time-stamp with (+P)
Step 3: Choose the Restore Data

- Once you are done selecting the restore version, the next step is to select the Restore data. Select the disk under the particular VM that is to be restored. You can search for a particular VM from the search tab. Click Next to proceed with the restore process.

Step 4: Configure the Restore Location and Virtual Disk Format

- The next step is to configure the restore location to which the files will be downloaded in the selected format. Make sure you have enough space in the restore location. The location can be a local drive or a network drive you have mapped using Vembu BDR server.
- From the Virtual Disk Format drop-down list, select the format in which you want to download your backup data. Click Next to review your restore configurations.
**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
  - Selected VM Machine
  - Target Location
  - Restore Format
- Verify all the details and click **Restore Now**.

You will be redirected to the recovery page. In 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
- User Name
- Current File
- Total Files
- Transfer Rate
Files Restored

**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.

![Abort Restore - VMwareBackup_Test](image)

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

- 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.
Case 7: 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](#)
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.
• 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 VMware Backup**

**Manage Backup Job**

- Once you have configured a backup job, you will be redirected to the List All Jobs page. This page acts as a central hub to all the backups and will list the backups that are configured to and from the Vembu BDR server.
- You will find the list of all the backup jobs you have configured, along with information such as:
  - Plugin type
  - Job Name - Name of the backup Job
  - Host Name - The IP address of the host from which the backup was configured
  - Next Schedule Time - The next occurrence of the backup
  - Suspend/Resume the backup - Suspend the backup and the job will not run until you manually resume
  - Run Now - This option will trigger the backup process immediately irrespective of the backup schedule.
  - Status of the backup - Whether the backup is in progress or idle state
  - Reports - backup report
  - Abort - Abort a backup job when it is in progress
  - Refresh
The More option consists of - View, Edit, and Delete the replication

View - You can view the following options:
- Machines configured for the backup along with the exclusion settings
- Backup Schedule Details
- Retention Configuration
- Advanced Configurations - Application Aware settings and Backup Encryption

You can create a new backup job by selecting the Create New option. The pop-up window displayed below will be available.

Edit - Reconfigure the entire backup job by changing
- VMs to be backed up
- Exclusion Settings
- Application Aware Process
- Schedule frequency
• **Delete** - Remove backup job and the data associated with it. You will get the pop-up displayed below. Click **Yes** to delete the backup job. You can go back to the List Backup jobs page by selecting List Backups option.

![Delete Backup](image)

*Warning:* The selected backup schedule and data will be deleted. Are you sure you want to delete this backup? "Appaware_push_check?"

---

**Note:** You cannot **Edit** a backup job while it is in progress.

---

**Evaluator’s Guide for VMware Backup**

---

**Getting Started with VMware Replication**

- Vembu offers VMware Replication, a feature with which you can replicate your VMs and create an exact copy of the production VM on another vCenter Server/ESXi host. The VMs that are replicated to the target host will be synchronized with the VM that is present in the source ESXi host.

- The target VMs are updated as only the changes that occur since the last backup in source VM will be copied to the target VM. The changes that happen will be tracked by Vembu Changed Block Tracking Driver (CBT).

- Through one replication job, you can replicate several VMs from the source to the target host. Even if your production VM goes down, you can immediately start your business operations by performing failover to replicated VM.

---

**Prerequisites:**
- The VMware Server should be of Licensed Edition

---

**Evaluator’s Guide for VMware Backup**

---

**Adding VMware Server**

---

**Setup VM Replication Job**

---

**Evaluation Case**

---

**Replica Failover and Failback**

---

**Manage VMware Replication Job**
The VMware Server should be of ESXi 4.0 & above and vCenter 4.0 & above

**Procedure:**

- From the **VM Replication** tab, select **VMware vSphere**. You will be taken to the Add VMware vCenter Server or ESXi host page.

![Add VMware vCenter Server or ESXi host page](image)

Add the vCenter Server/ESXi Host by providing the following:

- **Hostname/ IP Address**: Enter the Hostname or IP address of the vCenter Server/ESXi host you wish to replicate.
- You can add new credentials or select existing credentials. Click here to read more.
- **443**: Port used for communication between the host and the Vembu BDR backup server.

- Vembu BDR server communicates with the VMware server using the port that is set to 443 as default. You can modify this port number in case you have configured a different port number for vCenter/ESXi communication. Click **Save**.
- Once the VMware Server is added, it will be available in the Manage Servers page.
click **VM Replication** option to configure your replication schedule (or) Navigate to the **VM Replication** tab and click **VMware vSphere**. You can **Edit** or **Delete** the VMware Servers in this list.

<table>
<thead>
<tr>
<th>Type</th>
<th>Hostname</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>vm</td>
<td>192.168.102.16</td>
<td>Edit</td>
</tr>
<tr>
<td>vm</td>
<td>192.168.102.104</td>
<td>Edit</td>
</tr>
</tbody>
</table>

The Following details can be edited in an already added VMware Host
- You can select a different credential or add a new credential
- Port Number
- Add new credential

If you want to remove a particular VMware Server, click the **Delete** option. A pop-up window with the message "Are you sure you want to remove the host?" will appear. Click **OK** to delete your VMware Server.

*Note:*
- Encrypted VM Replication is not supported for vSphere host v6.7
- VM Replication may fail with 'VMware Modular Exception error' in case of ESXi compatibility/permission issue with respect to vCenter

**Evaluator’s Guide for VMware Backup**
Setup VM Replication Job

- Click the VM Replication option from the added VMware Server. You will be taken to the replication configuration page where you can begin configuring your VMware replication schedule.

There are 6 major steps involved in configuring a VMware Replication Job:
  - Choose Host/VM Machine(s)
  - Guest Processing
  - Configure Scheduling
  - Configure Target Replication Host
  - Configure Network Mapping and Re-IP Mapping
  - Review Configurations

Evaluator's Guide for VMware Backup

Step 1: Choose Host/VM Machine(s)

- The first step in your VMware Replication is to choose the virtual machines that are to be replicated. From the list of VMs available select the required VM for the replication process.

- If you had added a vCenter Server, all the ESXi hosts under that server and all the VMs under each ESXi host will be listed.

- If you had added an ESXi host, all the VMs in that host will be listed with checkboxes.

- You can choose the VMs to be replicated by selecting the checkboxes present near the VM.

- You can search for a particular VM in the Search VM checkbox, type the name of the VM that is to be replicated and click the search icon.

Note: In a replication job where an entire host is replicated, if you add any new VM to that host, the new VM will be replicated in the next schedule.

Note: Each replication job can have multiple VMs. For example, if you want to replicate an ESXi host which has 10 VMs, you can select the entire host as a single replication job. During the process, the VMs will be replicated one by one in the alphabetical order.

- If you have selected an ESXi host for replication, you might want to exclude a specific set of VMs from the replication process. Such VMs can be excluded using VM(s)/Disk(s) exclusion option.
Note: In case you haven't selected any VM for the replication and proceed with VM(s)/Disk(s) Exclusion you will get the message: Select the desired VMs or Host.

VM Exclusion

- Upon choosing the VM(s)/Disk(s) Exclusion option, you will get a pop-up displayed below. Choose 'Exclude VM(s)' tab.

Exclusion Settings

<table>
<thead>
<tr>
<th>Exclude VM(s)</th>
<th>Exclude Disk(s)</th>
<th>Select VM(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Name</td>
<td>Actions</td>
<td></td>
</tr>
</tbody>
</table>

- Click on 'Select VM(s)' option which will list the VMs that have to be excluded from this replication schedule. Click on 'Add' option which will add the VM to the Exclude VM list.

Selected VM(s) List

- You can add more VMs to be excluded from the replication job by choosing Select VM(s) option or remove an already excluded VM by selecting the Remove VM Exclusion option in the Actions tab. Click Save once you are done excluding the VMs from your replication schedule.
You can exclude a particular Disk type at host level or VM level using Disk Exclusion option. Under the Exclude Disk(s) tab, you will find the configured host(s) listed.

Select the Edit Disk Exclusion option under the Actions tab to assign global disk exclusion rule for VMs under a chosen host. Edit Disk exclusion tab will have following exclusion rules:

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

No Disk Excluded: If you are configuring this option, none of the disks will be excluded. By
default 'No disks excluded' option will be selected.

**Include only System Disks for Backup. Exclude Others(typically Disk 0:0):** This option will include the OS Disks for replication and exclude others. The disk with the number 0:0 will be included for the replication schedule regardless of the Disk type.

**Select type of Disk to exclude:** This option will allow you to select the type of the disk that has to be excluded from the replication schedule. Select the disk(s) that have to be excluded in each disk type. The three options available are IDE, SATA, and SCSI. Click Add once you have selected the disks to be excluded and click Save.

- Once you save the settings you will get the message "VM's/Disk's Exclusion configuration details saved successfully".

**VM Level Disk Exclusion:**
- Disk exclusion can be configured for individual VMs. Select the VMs that are to be replicated up and click the **VM(s)/Disk(s) Exclusion** option. The VMs that you have configured for the replication will be listed in this page, you have to select the type of disk to be excluded. From the Actions tab, select 'Edit Disk Exclusion' option.
Select the 'Edit Disk Exclusion' option under the Actions tab to assign global disk exclusion rule for VMs under a chosen host. Edit Disk exclusion tab will have following exclusion rules:

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

**No Disk Excluded**: If you are configuring this option, none of the disks will be excluded. By default 'No disks excluded' option will be selected.

**Include only System Disks for Backup. Exclude Others (typically Disk 0:0)**: This option will include the OS Disks for replication and exclude others. The disk with the number 0:0 will be included for the replication 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 replication schedule. Select the disk(s) that have to be excluded in each disk type. The three options available are IDE, SATA, and SCSI. Click Add once you have selected the disks to be excluded and click Save.

- Once you save the settings you will get the message "VM's/Disk's Exclusion configuration details saved successfully".
You cannot replicate VMs with names having special characters. They will fail with 'Modular Exception error'.

CD/DVD drives of virtual machines will not be replicated to the target host.

**Evaluator's Guide for VMware Backup**

**Step 2: Guest Processing**

- The second step in VMware Replication is to configure Application Aware Settings. This feature provides data consistency for the applications (MS Exchange Server, MS SQL Server, MS SharePoint Server, MS Active Directory) that reside in the VM. During the replication process, the writers that are available will be checked for stability. Only if they are in a stable state the replication will proceed. This ensures a consistent database snapshot. Consistent database snapshot will be created by quiescing the applications using Microsoft VSS API.
Note: By default, Application Aware settings will be disabled.

- Select the **Enable Application Aware Processing** option. You can customize Application Aware configurations at Host/VM Level. Select the **Click here** option 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 - if you are configuring application aware settings at host level, the IP address of the host will be displayed. If you are configuring application aware settings at VM level, the name of the VM will be displayed.
  - VSS Writer Status - displays if the VSS writer status is required, ignored or disabled based on your selection.
  - Log Truncation Status - displays if 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.

![Manage Application Aware Settings](image)

- You can configure Application Aware rules for your entire ESXi host or the individual VMs residing in that ESXi host. Click the checkbox next to the entity name option, this will select all the entities. If you want to select individual entities, select the required entity (Host/VM) and click the **Edit** option.

**Note:** Make sure VMware Tools are running in Guest OS

- The Appaware Settings page will be displayed. You can configure the Application-aware processing configurations. Three options will be available:
  - **Require successful application processing**: Choosing this option lets Vembu BDR track the application consistency and trigger the replication process, only when all
the VSS writers in the VM are in a stable state. You can stop the replication 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
  replication 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 replication.
- **Disable Application processing**: Application Aware will be disabled for the
  selected entity.

- **Transaction log processing**: You can configure two options from this section:
  - **Truncate the transaction logs**: This option will purge the transaction logs and saves
    the space consumed by the application transaction logs.
  - **Disable Log Transactions**: The log transactions will be disabled and truncation
    won't happen.

**Note**: If **Disable Application processing** option is selected in Application-aware processing
section, then transaction log processing will not be applicable.

- If you have selected a host for the replication process but want to set different Application
  aware rules for individual VMs, select the **Add** option. This will open the Appaware settings
  page. Expand the host further by choosing the + option and select the VM to which
  different Application Aware rules must be set. Click the **Add** option. The selected VM will
  be added and displayed in the Customize settings page. Click the **Edit** option and edit the
  Application aware rules for the added VMs.

**Note**: Appaware is not supported for VM(s) with Desktop OS, 32 bit Guest OS.
You can remove the VMs that you have added to the list by selecting the **Remove** option. Click **Save** once you are done configuring the Application Aware Settings and click **Next** to proceed to the Credentials page.

**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 replication schedule.

---

**Evaluator's Guide for VMware Backup**

**Step 3: Configure Scheduling**

- The Schedule option defines the frequency of your VMware replication job. You can configure the replication schedules by choosing between **Run Every**, **Run Daily**, and **Run Weekly** options.
- Select **Run Every** option if you want to run your VMware replication at regular intervals on specific day(s). The time frame ranges from 15 minutes to 12 hours a day on the specific days a week. By default, all the days in the week will be selected. If you don't want to run your replication on all the days, then manually select the days in which you want to run the replication.
- If you want to run your replication every day, select **Run Daily** option and configure the time period in which your VMware replication has to occur.
- If you want to run your replication every week on a specific day and time, choose the **Run Weekly** option. Select the time frame and day in which the VMware replication will run.
- Click **Next** when you have finished configuring the replication schedule.

**Note:** By default **Run Every** option will be selected for the replication schedule.
Evaluator's Guide for VMware Backup

Select how frequently you want to replicate:

- Run Every [ ]
- Run Daily [ ]
- Run Weekly [ ]

on the following days:
- Sun
- Mon
- Tue
- Wed
- Thu
- Fri
- Sat

[Previous] [Next]
Step 4: Configure Target Replication Host

- Choose the Target vCenter Server/ESXi host to which your source VMs data is to be replicated. If your target server is a **vCenter Server**, select the corresponding ESXi host and the datastore from the drop-down list. If your target server is an **vCenter Server**, select the datastore from the drop-down list.

- If you want to add the target VMware Server, click the **Add VMware Server** option. Provide the Hostname/IP address of the target Server. Incase you have previously added credentials for the target server, select it from the **Select Credentials** drop down list.
- To know more about adding credentials, **Click here**. If you have configured a different port number for the target server, change the port number manually and click **Add**.

- Vembu provides you an option to add a suffix name to your Source VM name. This is used to identify the VM in the target server as a replication job. By default, target VM replica will be given a suffix name as **Replica**, which can be edited. For Eg: If your Source VMs name is Vembu and Replica suffix name is Tech then your source VMs data will be replicated into a new VM in the Target Server named 'Vembu_Tech'.
Select retention count for replicated data, that is the number of replication versions that has to be maintained in the target host. For eg: if you configure the retention count to three, then the latest 3 versions of the replication will be maintained. By default, the value is ‘7’. Click **Next** to proceed further.

**Evaluator’s Guide for VMware Backup**

**Step 5: Configure Network Mapping and Re-IP Mapping**

**Network Mapping:**

- Network Mapping is the process of mapping or mirroring the source VM and Target VM. In your production or target environment, if you have configured different networks, network mapping feature will be helpful.
- If you configure two different types of networks in two different places your RTO and Business Continuity will be affected. To overcome this situation, Network Mapping utilizes the Power Replication feature. You must select the source and target networks that are to be mapped. For this process, Vembu BDR will maintain a table which consists of the networks that are mapped during each replication session. It will cross verify the source VM with the replicated VM and the network details are updated regularly. This process signifies a nil failure rate.

**Steps to configure source and target networks:**

- Enable the **Configure Networks** checkbox which is disabled by default
- Click the Search icon next to Source Network and select the network in which the source VM resides
- Click the Search icon next to Target Network and select the network to which the source VM has to be mapped
- Rules can be added in a similar manner for all the VMs configured for replication using the (+) icon present
- Once done, click **Next** to configure Re-IP mapping rules.

**Note:** By default, Network Mapping will be disabled.

**Note:** It is recommended to use the same network for the source and target hosts, as it saves time during replication and recovery.
Re-IP Mapping

- There may be situations in which you may use different types of IP schemes in source and target environments. During the replication process, the configurations of the source VM will be updated in the target VM.
- While performing Failover to the replica machine, the IP you have configured in the source may not be available in the target location. Re-IP Mapping in this situation will provide you various combinations of mapping rules to configure your replica. When you perform the Failover process, the replica machine registry will be updated with the IP rule that you have configured.

Follow the below steps to add a rule:

- Enable the Network Re-IP Mapping option. Click the Add Rule option which will open a pop-up window.
- Specify a Rule Name
- Enter the IP address and subnet mask of the source VM
- Enter the IP address, subnet mask and default gateway of the target VM
- Specify the preferred and alternate DNS server
- Click Save to save the Re-IP Mapping rule.
- You can edit an already configured rule using the edit option. You can also remove the added rule through the remove option.

Note:
- Linux VMs and GPT formatted disk VMs are not supported for Network Mapping and Re-IP Mapping.
- Re-IP Mapping will not work for Windows 7 Professional (32-bit) machine.
- Source VM’s VMXNET3 ethernet adapter configuration will not be replicated to the replica.
Step 6: Review Configurations

- The last step in your VMware replication configuration is to review the configurations you have selected. Enter a Replication Schedule Name. Vembu BDR server supports creating multiple replication schedules each with its own configuration. The replication schedule name will uniquely identify the replication. While restoring your replicated data, you need to choose the data to be restored using its schedule name.
- Review the configuration provided and enter an appropriate name for the replication schedule.
- The following details will be available in this page:
  - **Configured Host/VM(s)** - The Host/VM you have configured for the replication process
  - **Scheduling** - Frequency of your replication schedule
  - **Target Replication Host** - The IP address of the host to which you have configured the replication
  - **Network Mapping** - Whether Network Mapping is enabled or not
  - **Network Re-IP Mapping** - Whether Re-IP Mapping is enabled or not.
- You have the option of running the replication job immediately after saving the replication. If you want your replication job to be triggered immediately, irrespective of the replication schedule configured, select the **Run this job immediately after saving** option.
- Click **Save Replication** option once all the configurations are reviewed. On saving the replication, you will be prompted to confirm to proceed further. Click **Ok** to complete the replication 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 replication in the Overall Progress window. To view the backup progress window, Go to VM Replication tab and press List Jobs option, Click the arrow mark in the Status section.

Note: Resizing virtual disks in the primary site after initial replication will result in replication job failure permanently. You have to configure a new job to perform replication.

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

- **Job Name** - Name of your replication job
- **Backup Server** - The backup server to which the replication is currently processing
- **Warning** - Warning for the replication 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 replicated data is transferred to your backup server. (Bytes, KB, MB, GB)
- **Original Size of the file** - The actual size of your replication job
- **Time Left** - Time remaining for your replication to complete
- **Current File** - The name of the current disk that is being replicated

You have the option of aborting the replication schedule. From the List Jobs page in VM Replication tab, click the **Abort** option. This will open a pop-up window as displayed below. Click **Yes** to abort the replication.

---

**Note:** If the initial replication job fails intermittently, you have to delete the replica VM in the target site and create a new replication job.

---

You can abort your replication from the replication progress window. Click the **Abort** option, you will get a popup as shown below. Click **OK** to Abort the replication.

---

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

Evaluator's Guide for VMware Backup

Evaluation Case

- There are 4 evaluation cases explained below that will guide you through the various features and configuration options available in VMware Replication process. By the end of all the cases, you will have used every option available in the product and created replication schedules 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 VMware Backup

Case 1

- Configure a replication job to replicate an entire ESXi host or vCenter Server
- Enable Application Aware processing and log truncation for entire host
- Schedule the Replication to run every one hour on all the days except Wednesday
- Specify the IP and datastore of the target VMware Server and set the retention count to 7

Procedure:

Configuring a replication job for the above-mentioned configuration will take you through a basic and simple scenario. Follow the steps below:

**Step 1: Configure VM for the Replication Schedule**

- As per the evaluation case, we have to choose VM(s) from the VM list. Select the VMs from the ESXi host you wish to replicate and click **Next** to proceed with the evaluation case.
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 and select Click here option.

- By default in the Appaware Settings pop-up window, the Require successful application processing and Truncate the transaction log option will be selected. Click Save.
- Click Next to proceed to with the backup schedule.
Note: By default Application Aware Settings will not be enabled.

**Step 3: Configure Replication Schedule**

- Configuring the replication schedule has three options to choose from:
  - **Run Every** - Run the replication at regular intervals on specific day(s)
  - **Run Daily** - Run the replication every day in a specific time frame
  - **Run Weekly** - Run the replication on particular days of the week at a specific time period

- Since the evaluation case involves to **run the replication every hour on all the days except Wednesday**, select **Run Every** option. Configure the time to 1 Hour from the dropdown list and remove Wednesday from the selection.

**Note:** By default **Run Every** option will be selected and the time configured will be 1 Hour.

**Step 4: Configure Target Replication Server**

- Select the IP address of the target VMware Server from the VMware Server drop-down list.
- If the VMware Server you are adding is a vCenter Server, select the target ESXi host.
- Select the Datastore from the drop-down list
- Mention a replica suffix name. By default, the name is set as Replica.
- Set the retention count to 7 by selecting from the drop-down list. Click **Next** to review your replication configuration.
Step 5: Review Configurations

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

- Host/VM(s) Details
- Scheduling Details
- Target Replication Host Details

- Enter a replication job name and click **Save Replication** to complete VM Replication Schedule Configuration.

**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.

**Evaluator’s Guide for VMware Backup**

**Case 2**

- Configure a replication job to replicate only particular VMs from the source ESXi host
- Enable Application Aware processing and log truncation for specific VMs
- Schedule the replication to Run Everyday at 10:00 PM
- Specify the IP and datastore of the target VMware Server. Set the retention count to 3
- Enable Network Configuration and mention the IP addresses of the source and target networks to be mapped
- Enable the ‘Run this job immediately option.

Procedure:

Configuring a replication job for the above-mentioned case will take you through a basic scenario with a few changes. Follow the steps mentioned below:

**Step 1: Configure VM for the Replication Schedule**

- As per the evaluation case, select the entire ESXi host for the replication schedule. You must exclude a particular VM from the replication schedule.
- Click the **VM(s)/Disk(s) Exclusion** option. The exclusion Setting pop-up window will appear.
- Select the **Exclude VMs** tab and click on **Select VM(s)**. The ESXi host selected for the replication will be displayed. Expand it further and select the VM to be excluded. Click **Add** to exclude that VM from the replication schedule.

**Step 2: Configuring Application Aware Process**

- 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 and select **Click here** option.
Select the two VMs from the list in the Appaware Settings pop-up window and click the **Edit** option. The **Require successful application processing** and **Truncate the transaction log** option will be selected. Click **Save**.

Click **Next** to proceed to with the backup schedule.

---

**Step 3: Configure Replication Schedule**

- Configuring the replication schedule has three options to choose from:
  - **Run Every** - Run the replication at regular intervals on specific day(s)
  - **Run Daily** - Run the replication every day in a specific time frame
  - **Run Weekly** - Run the replication on particular days of the week at a specific time period

- The evaluation case involves to **schedule the replication everyday at 10:00 PM**, select
the Run Daily option and select 10:00 PM from the drop-down list. Click Next to proceed configure target replication host.

Step 4: Configure Target Replication Server

- Select the IP address of the target VMware Server from the VMware Server drop-down list.
- If the VMware Server you are adding is a vCenter Server, select the target ESXi host.
- Select the Datastore from the drop-down list
- Mention a replica suffix name. By default, the name is set as 'Replica'.
- Set the retention count to 3 by selecting from the drop-down list. Click Next to configure Network Mapping.

Step 5: Configure Network Mapping

- Enable the Configure Networks checkbox which is disabled by default
- Click on the Search icon next to Source Network and select the network in which the source VM resides
- Click on the Search icon next to Target Network and select the network to which the source VM has to be mapped
- Rules can be added in a similar manner for all the VMs configured for replication using the
Once done, click **Next** to Review your replication configurations.

**Note:** It is recommended to use the same network for the source and target hosts, as it saves time during replication and recovery

**Step 6: Review Configurations**

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

- Host/VM(s) Details
- Scheduling Details
- Target Replication Host Details
- Network Mapping enabled or not.

- Enter a replication job name. As per the evaluation case, select the **Run this job immediately after saving** option.

**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 Replication** to complete VM Replication Schedule Configuration.
Case 3

- Configure a replication job to replicate an entire ESXi host and exclude a Disk from a particular VM.
- Enable Application Aware settings and ignore Application Processing Failures for an entire host.
- Schedule the replication to run every Sunday at 10:00 PM.
- Specify the IP and datastore of the target VMware Server and set the retention count to 5.
- Enable Network Re-IP Mapping and add a rule.

**Procedure:**

Configuring a replication job for the above-mentioned configuration will take you through a basic scenario with a few advanced configurations. Follow the steps below:

**Step 1: Configure VM for the Replication Schedule**

- The first step will be to select the VMs that have to be replicated from the Configure VM(s) page. You can search for a particular VM from the Search VM tab.

- Once you have selected the VM for the schedule, select the **VM(s)/Disk(s) Exclusion** option.
• The exclusion Setting pop-up window will appear. According to the evaluation case, you have to exclude a disk from a particular VM. To exclude a disk from the backup schedule, click Exclude Disk(s) tab and click the Edit Disk Exclusion option in the Actions tab.

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

![](image1.png)

• The excluded disk will be listed in the Exclusion Settings page. If you need to edit the disk exclusion, click Edit Disk Exclusion. Click Save to save the exclusion setting. Once you save the settings, you will get the message "VM's/Disk's Exclusion configuration details saved successfully". Click Next to proceed to configure Application Aware process.

**Step 2: Configuring Application Aware Process**

• 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 and select Click here option.
Select the two VMs from the list in the Appaware Settings pop-up window and click the Edit option. Select the Ignored application processing failures option and click Save. Click Next to proceed with the backup schedule.

**Note:** By default Application Aware Settings will not be enabled.

**Step 3: Configure Replication Schedule**

- Configuring the replication schedule has three options to choose from:
  - **Run Every** - Run the replication at regular intervals on specific day(s)
  - **Run Daily** - Run the replication every day in a specific time frame
  - **Run Weekly** - Run the replication on particular days of the week at a specific time period

- As per the evaluation case you have to run the replication every Sunday at 10:00 PM. Select Run Weekly option and choose Sunday. From the drop-down box, configure the time to 10:00 PM. Click Next to configure target replication host.
Note: By default Run Every option will be selected and the time configured will be 1 Hour.

Step 4: Configure Target Replication Server

- Select the IP address of the target VMware Server from the VMware Server drop-down list.
- If the VMware Server you are adding is a vCenter Server, select the target ESXi host.
- Select the Datastore from the drop-down list.
- Mention a replica suffix name. By default, the name is set as 'Replica'.
- Set the retention count to 5 by selecting from the drop-down list. Click Next to proceed further with the evaluation case.

Step 5: Configure Re-IP Mapping

- The next step in the evaluation case is to Enable Network Re-IP Mapping and add a rule.
- Enable the Network Re-IP Mapping option and follow the below steps to add a rule.
  - Click the Add Rule option which will open a pop-up window.
  - Specify a Rule Name.
  - Enter the IP address and subnet mask of the source VM.
  - Enter the IP address, subnet mask and default gateway of the target VM.
  - Specify the preferred and alternate DNS server.
  - Click Save to save the configured Network Re-IP Mapping rule.
  - You can edit an already configured rule using the edit option. You can also remove
the added rule through the remove option.

```
<table>
<thead>
<tr>
<th>Networking Re-IP Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
</tr>
<tr>
<td>Source VM</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Subnet mask</td>
</tr>
<tr>
<td>Target VM</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Subnet mask</td>
</tr>
<tr>
<td>Default gateway</td>
</tr>
<tr>
<td>Preferred DNS server</td>
</tr>
<tr>
<td>Alternative DNS server</td>
</tr>
</tbody>
</table>
```

**Note:**
- Linux VMs and GPT formatted disk VMs are not supported for Network mapping and Re-IP mapping.
- Re-IP mapping will not work for Windows 7 Professional (32-bit) machine.
- Source VM’s VMXNET3 ethernet adapter configuration will not be replicated to the replica VM. IPv6 configuration is not supported for IP Re-mapping.
- To find the subnet mask, default gateway, preferred and alternate DNS server associated with your IP address, do the following:

**FOR WINDOWS:**
- Press ‘Win-R’, type "cmd" in the input box, then press **Enter**
- Type "ipconfig /all" at the command prompt, then press **Enter**
- The first address is the primary DNS server, and the next address is the secondary DNS server

**FOR LINUX**
- Launch a command line interface (This will vary depending on operating system distribution)
- In the resulting command line window or screen, type "ifconfig"
- Press **Enter**
- The location of the gateway address can be found by typing "netstat -r" at the command line
Note: Re-IP Mapping option is not supported for VM replication in Linux based backup Servers

- Click **Next** to proceed to review your Replication configurations.

### Step 6: Review Configurations

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

- Host/VM(s) Details
- Scheduling Details
- Target Replication Host Details
- Network Re-IP Mapping enabled or not.

- Enter a replication job name.

**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 Replication** to complete VM Replication Schedule Configuration.
Case 4

- Edit the replication job and add a VM to the replication schedule
- Turn off Application Aware Settings
- Change the replication schedule to Run Weekly on Monday 09:00PM
- Change the retention count to 4
- Enable Network Mapping
- Disable Re-IP Mapping
- Run the job immediately after saving

Procedure:

Editing a replication job for the above mentioned configuration will take you through a basic scenario with a few advanced configurations on how to edit a replication job and the options you can edit. Follow the steps below:

Step 1: Adding a VM to the replication schedule

- From the VM Replication tab, select List All Jobs option. Click More option and select Edit option
- In the choose the machine(s) page, add a particular VM to the replication schedule
- You can choose the VMs to be replicated 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 evaluation case.

Step 2: Configure Application Aware Process

- The next step will be to configure Application Aware Process. As per the evaluation case, you have to turn off the Application Aware Process. If you have selected Application Aware Process while configuring the replication schedule, it will be selected. Disable it and click Next to proceed further.
Note: By default, Application Aware Process will be disabled while configuring the replication job.

Step 3: Configure Replication Schedule

- Configuring the replication schedule has three options to choose from:
  - Run Every - Run the replication at regular intervals on specific day(s)
  - Run Daily - Run the replication every day in a specific time frame
  - Run Weekly - Run the replication on particular days of the week at a specific time period

- As per the evaluation case you have to change the replication schedule to Run Weekly on Monday 09:00 PM. The replication schedule that is already configured will be displayed. Select the Run Weekly option and day as Monday. Configure time period to 09:00 PM.

- Click Next to configure target replication host.

Step 4: Configure Target Replication Server

- While editing the Target Replication Server option, the only option you can edit is the retention count option. According to the evaluation change the retention count to 4 from the drop-down list.

- Click Next to proceed further with the evaluation case.
Step 5: Configure Network Mapping

- Enable the **Configure Networks** checkbox which will be disabled if you have not configured Network Mapping feature while scheduling the replication. Click the Search icon next to Source Network and select the network in which the source VM resides.
- Click the Search icon next to Target Network and select the network to which the source VM has to be mapped.
- Rules can be added in a similar manner for all the VMs configured for replication using the (+) icon present.
- Once done, click **Next** to proceed to configure Re-IP Mapping.

Step 6: Configure Re-IP Mapping

- According to the evaluation case, you have to disable Re-IP Mapping option. If you have enabled Re-IP Mapping while configuring the replication job, it will be selected. Disable the **Network Re-IP Mapping** option and click **Next** to review the configurations.
Step 7: Review Configurations

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

- Host/VM(s) Details
- Scheduling Details
- Target Replication Host Details
- Network Re-IP Mapping enabled or not

- Select the **Run this job immediately after saving** option. This option triggers the replication process immediately irrespective of the replication schedule you have configured.
- Choose whether to suspend the replication or not. Click **Save Replication** to complete VM Replication Schedule Configuration.

You cannot edit the following options:

- ESXi Host configured
- Datastore configured
- Replica Suffix Name
- Replication Job Name
Evaluator's Guide for VMware Backup

Replica Failover and Failback

- Sometimes businesses may require a substitute of the Virtual Machine that is being used for their business critical function in times of disaster. In this case they will want to avoid downtime and have the VM in a ready to use format so that their business keeps functioning. For the above mentioned scenario, Replication combined with Failover and FailBack is the process which meets their requirement.
- The section below will guide you through the various restoration scenarios available in the VMware Replication process.

Evaluator's Guide for VMware Backup

Failover

- Your primary server/VM has crashed due to a disaster
- Switch over to the replicated VM to continue with production

Procedure:

- When your source machine is down, you can use Failover process to switch the operations from the source VM to its replica in the target server. Once the Failover process is carried out, the replica machine will perform the role of the source machine. That is, the target VM will be powered ON with the same Network and IP configurations that was configured during the replication process.
- You can Failover the replica to any restore point available. If any data is added when the VM is in the Failover state, it will be maintained separately in a snapshot delta file.
- Select the VM Replication tab and choose Failover and Failback option. Click the Restore icon beside the required replication job.

![Failover and Failback](image)

- The next step is to select the restore type from the list. Select Failover as the restore type and click Next to proceed with the restore process.
Choose the restore type:

- **Failover**
  Switches the operations from original VM to its replica on the target host.
- **Finalize Failover**
  Finalizes the FailOver state of a replica by Undo FailOver/Permanent FailOver/FailBack options.
- **Finalize FailBack**
  Finalizes the FailBack state of a replica by Undo FailBack/Commit FailBack options.
- **File Level Recovery**
  Restores specific files and folders from VM Replica.

Choose the restore version from the tree. The restore version depends on the retention settings you have configured. Click **Next** to continue with the restore process.

The next step is to select the restore data for the restore. Select the VM(s) to be restored. You can search the required machine from the **Search VM** option. Click **Next** to continue further with the restore process.

The last step is to review your configurations before you perform the Failover process.
- Verify the following - VM(s) selected for the Failover, Restore Version configured. Once done verifying the selection, click **Failover** option. You will get a pop-up window to confirm the Failover process, click **OK** to begin the Failover.

![Failover](image)

- You will now be redirected to the Restore Progress page. Check the Client Name, Backup Name, Cand Progress status. Click the **Failover and FailBack** option to revert back to that page.

![Failover](image)

**Note:** The VM should not be manually powered on or powered on after the Failover as it may lead to data loss.

**Evaluator’s Guide for VMware Backup**

**Finalize Failover**

- Once you have performed the Failover process, you can finalize the Failover process. This option helps you finalize the failover process and let you decide whether to:
  - Revert to Source VM immediately
  - Completely switch from Source VM to replica VM
  - Rollback to the Source VM after a considerable amount of work done by the replica.

- Finalize Failover can be done based on the above scenarios as follows:
  - **Undo Failover**
  - **Permanent Failover**
- **Failback**
  
  The above listed options get enabled only after performing the Failover process.

**Procedure:**

Follow the steps given to finalize failover:

- Choose the **VM Replication** tab and select **Failover and Failback** option.

  ![Failover and Failback screenshot](image)

- Click the **Restore** icon across the replication job which you had recently failed over. From the restore type select **Finalize Failover** as the restore type and click **Next** to proceed.

  ![Finalize Failover screenshot](image)

- The next step is to select the restore data for the restore. Select the VM(s) to be restored. You can search the required machine from the **Search VM** option. Click **Next** to continue further with the restore process.
The next step is to select the Finalize type. Three options will be displayed which are explained below:

- **Undo Failover** - This option will revert the replica machine back to its original state (turned off state) before the failover was performed. That is all the changes (work data) made in target VM during failover period will be flushed and lost after undoing Failover.

- **Permanent Failover** - You can select this option if the source VM is not recoverable after a disaster. Finalizing failover will enable you to make the replica VM as the production machine permanently. The VM will be excluded from the replication schedule and further incrementals for the source VM will cease.

- **Failback** - This option allows you to revert from the target VM to the source VM completely with all the changes made after failing over. You can recover the replica VM to the same or different host and continue the operations of the production VM.
within the stipulated time and want to undo the Failover process, proceed with this type.

**Procedure:**

- Select **Undo Failover** from the Finalize Type and review the configurations by checking the selected VM(s) and the restoration type.
- Click **Undo Failover** to begin the restore process. Select **OK** from the pop-up window to confirm the Failover.

**Note:** The changes done in the target VM machine will be lost after undoing Failover

**Permanent Failover**

- If you have failed over to the replica VM after disaster and could not get your source VM running back up within the stipulated time, you can permanent the Failover process. The replica VM will be made the source VM permanently.

**Procedure:**

- Select **Permanent Failover** as the Finalize Failover type and review the configurations by checking the selected VM(s) and the restoration type.
- Click **Permanent Failover** to make the Failover process permanent. Select **OK** from the pop-up window to confirm the Failover.
Note: The replica VM will be excluded from the replication job after completion of Permanent Failover. The same should be configured again for replication.

Evaluator’s Guide for VMware Backup

Failback

- You have failed over to the replica VM after disaster and begin working on the replica VM. You got the source VM running within a week. Then use Failback option to Failback to the Source VM and begin working on it.

Procedure:

- From the Finalize Failover type, select Failback and click Next to continue further.
- You can restore to VMware Server or directly to the vCenter Server. If you want to add a VMware Server, click the +Add option and provide the required details. Enter the Hostname/IP Address and select a credential if you have already from the Select Credentials drop down list. Add a new credential by selecting the Add Credentials option. Click here to read more on credentials.
• Select the preferred option and specify the datastore and VM name of the source VM. Click **Next** to proceed to review your selection.

• Review your selection by checking the following:
  - Selected VMs
  - Failover Type
  - Target Server Name
  - Target Datastore
  - Target VM Name

• Click **Failback** option to begin the Failback. Select **OK** from the pop-up window to confirm the Failback.

**Note:** Failing back only the modified data after performing Failover is not supported

**Note:** If the Failback process fails intermittently, you have to delete the Failback VM in the target site and try again

**Evaluator’s Guide for VMware Backup**

**Finalize Failback**

• Once you have performed Failback to the source machine, you can finalize the failback job.
• This option helps you finalize the failback process and lets you decide whether to:
  o Revert back to failover state
  o Commit the failback job and start replicating the source VM.

• Finalize Failback can be configured based on the above scenarios as follows:
  o Undo FailBack
  o Commit Failback

**Note:** The options listed above will be enabled only if the Failback process is performed.

**Procedure:**

• Once the Failback process is completed successfully, you can finalize the Failback by following the below steps:

  • Click the VM Replication tab and select Failover and Failback option.
  • Click the Restore icon across the replication job which you had recently failed back. From the restore type, select Finalize Failback option and click Next to begin the Finalize Failback process.

  ![VM Replication Tab](image)

  Choose the restore type
  
  - Failover
    Switches the operations from original VM to its replica on the target host.
  - Finalize Failover
    Finalize the FailOver state of a replica by Undo FailOver/Permanent FailOver/Failback options.
  - Finalize FailBack
    Finalize the FailBack state of a replica by Undo FailBack/Commit FailBack options.
  - File Level Recovery
    Restore specific files and folders from VM Replica.

• The next step is to select the restore data for the restore. Select the VM(s) to be restored. You can search the required machine from the Search VM option. Click Next to continue further with the restore process.
The next step is to select the Finalize Failback type. Two options will be displayed which are explained below:

- **Undo Failback** - Undo Failback will revert the replica machine to the Failover state. You can recover the replica VM intact with all the changes made. If the source VM is not performing as expected, then you can avail this option.

- **Commit Failback** - If the source VM has been recovered properly and is functioning as expected after performing failback, then you can avail this option. It finalizes the Failback state and boots the source VM along with all the changes made.

**Evaluator's Guide for VMware Backup**

**Undo FailBack**

- You can revert the replica back to the Failover state if the Failback VM is not performing as per your requirements.

**Procedure:**

- From the Finalize Failback type, select **Undo Failback** and click **Next** to review your configurations by checking the selected VM(s) and the Finalize Failback type.
- Click **Undo Failback** to begin the process. Select **OK** from the pop-up window to confirm.
the Failback process.

**Commit Failback**

- If your source VM is fully functional after failing back and you want to continue the replication schedule, finalize the failback process by committing the failback and continue working on the source VM.

**Procedure:**

- From the Finalize Failback type, select **Commit Failback** and click **Next** to review your configurations by checking the selected VM(s) and the Finalize Failback type.
- Click **Commit Failback** to begin the process. Select **OK** from the pop-up window to confirm the Failback process.

**Note:** If the Failback process fails intermittently, you have to delete the Failback VM in the target site and try again.

**Note:** The replica VM will be excluded from the replication job after completion of Commit Failback. The same should be configured again for replication.
File Level Recovery

- If you require only specific files and folders to work, recover those particular files and folders alone to your source VM using File Level Recovery.

Procedure:

- From the VM Replication tab and select Failover and Failback option.
- Click the Restore icon across the replication job from which you want to restore files and click Next. From the restore types available, select File Level Recovery option and click Next to begin the restore process.

Choose the restore type

- Failover
  Switch the operation from the original VM to its replica on the target host.
- Finalize Failover
  Finish the failover state of a replica by Undo Failover/Permanent Failover/Failback options.
- Failover Failback
  Finish the failover state of a replica by Undo Failover/Concrete Failback options.
- File Level Recovery
  Restore specific files and folders from VM Replica.

- Choose the restore version from the tree. The restore version depends on the retention settings you have configured. Click Next to continue with the restore process.

Choose the restore version

- [Date]: [34 Nov 2019 11:16:07]

- The next step is to configure the restore data for the restore. The ESXi hosts/VMs added will be displayed. Expand the list and select the files to be restored. You can select multiple files from multiple machines in a single recovery job. Once done selecting the required files for the restore click Next to proceed with the restore process.
**Note:** FLR is not supported for Non-Windows OS machines, System volumes and Dynamic RAID volumes.

- Configure the restore location by selecting the folder icon. From the pop-up window which displays the list of drives, choose the required location by expanding the tree and click **Ok**.

- The last step is to review the configurations you have selected for the restore process. Check the Selected Version, Target Location and click **Download** option to begin the restore process.
Evaluator's Guide for VMware Backup

Manage VMware Replication Job

- Once you have configured a replication job, you will be redirected to the List Jobs page or select VM Replication tab and click List Jobs option. This page acts as a central hub to all the replication jobs and will list the replication jobs configured along with the below mentioned information:
  - Plugin type
  - Job Name - Name of the replication Job
  - Host Name - The IP address of the host from which the replication was configured
  - Next Schedule Time - The next occurrence of the replication
  - Suspend/Resume the replication - Suspend the replication job and the job will not run until you manually resume
  - Run Now - To run the replication immediately irrespective of the schedule configured.
  - Status of the backup - The state of the replication job.
  - Reports - replication report
  - Abort - Abort a replication job when it is in progress
  - Refresh

- The More option consists of - View, Edit, and Delete the replication
- View - You can view the following options:
  - Machines configured for the replication along with the exclusion settings
  - Replication Schedule Details
  - Retention Configuration
  - Target DR Server Details
  - Network Mapping
  - Re-IP Mapping
  - Advanced Configurations - Application Aware

- You can create a new VMware Replication job by selecting the Create New option. You can further edit this replication schedule by selecting the Edit option. You can go back to the List Jobs page by selecting the List Replicas option.
• **Edit** - Reconfigure the entire replication job by changing
  o VMs to be replicated
  o Schedule frequency
  o Retention Count
  o Network Mapping
  o Re-IP Mapping

• **Delete** - Remove replication job and the data associated with it. You will get the pop-up window displayed below. Click Yes to delete the replication job.

![Delete Replication](image)

Warning: The selected replication schedule and data will be deleted. Are you sure you want to delete this replication? ReplicationFix?

---

**Evaluator’s Guide for VMware 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.

The Reports are:

- [Backup Job Report](#)
- [Backup Status Report](#)
- [Image Integrity Report](#)
- [VM Status Report](#)
- [Quick VM Recovery Report](#)
Evaluator’s Guide for VMware Backup

Backup Job Report

- Open the Recovery tab. This page lists all the backup jobs configured to the Vembu BDR server where you can see a report option alongside every backup job. Click the Reports icon.

- In this page, you can view historical reports of the specific backup chosen where the following reports will be listed:
  - Backup Report
  - Restore Report
  - Merge Report
  - Deleted Backup Report
  - Offsite Copy Report

- You can filter the reports to view status of full backups alone (excluding incrementals).
- Select the More tab to view further details on the report. You will get the pop-up image displayed below.
From the drop-down list in the right top pane, select **Full Backups** option. You can delete your full backup by selecting the full backup timestamp version and the **delete** icon.

**Evaluator's Guide for VMware Backup**

**Backup Status Report**

- Backup Status Report lists all the backup jobs that are configured and their statuses. From the **Reports** tab select **Backup Status** option.

The backup status is split into the following:

- **Successfully Completed** - Backup job completed successfully
- **Failed** - 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
- **Partially Completed** - When a part of the backup data configured could not be backed up

Along with the backup status, other information are listed such as:

- 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
• In the Backup Status Report page, you will have three tabs.
  o Last 24 Hours Report
  o Latest Backup Job Status
  o Schedule Email Report

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

<table>
<thead>
<tr>
<th>Status</th>
<th>Client Name</th>
<th>Job Name</th>
<th>Schedule Type</th>
<th>Next Schedule Time</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUCCESS</td>
<td>lab_v40_nov17_102_65</td>
<td>Dic trigger</td>
<td>Incremental</td>
<td>Mon Nov 2018 20:02:04</td>
<td>Backup complete.</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>NVBiq_nov17_201</td>
<td>SubFolder</td>
<td>Incremental</td>
<td>Mon Nov 2018 20:44:47</td>
<td>No new modified.</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>V40_09Msgs_201</td>
<td>Test</td>
<td>Incremental</td>
<td>Mon Nov 2018 20:27:00</td>
<td>Backup complete.</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>V40_NVBiq_201</td>
<td>Status</td>
<td>Full</td>
<td>Mon Nov 2018 20:23:57</td>
<td>Problem while b.</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>NVBiq_nov17_201</td>
<td>STD Filter</td>
<td>Full</td>
<td>Mon Nov 2018 20:01:56</td>
<td>Backup complete.</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>NVBiq_nov17_201</td>
<td>SubFolder</td>
<td>Incremental</td>
<td>Mon Nov 2018 19:44:50</td>
<td>Backup complete.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Status</th>
<th>Client Name</th>
<th>Job Name</th>
<th>Schedule Type</th>
<th>Next Schedule Time</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUCCESS</td>
<td>lab_v40_nov17_102_65</td>
<td>Dic trigger</td>
<td>Incremental</td>
<td>Mon Nov 2018 20:02:04</td>
<td>Backup complete.</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>NVBiq_nov17_201</td>
<td>SubFolder</td>
<td>Incremental</td>
<td>Mon Nov 2018 20:44:47</td>
<td>No new modified.</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>V40_09Msgs_201</td>
<td>Test</td>
<td>Incremental</td>
<td>Mon Nov 2018 20:27:00</td>
<td>Backup complete.</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>V40_NVBiq_201</td>
<td>Status</td>
<td>Full</td>
<td>Mon Nov 2018 20:23:57</td>
<td>Problem while b.</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>NVBiq_nov17_201</td>
<td>STD Filter</td>
<td>Full</td>
<td>Mon Nov 2018 20:01:56</td>
<td>Backup complete.</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>NVBiq_nov17_201</td>
<td>SubFolder</td>
<td>Incremental</td>
<td>Mon Nov 2018 19:44:50</td>
<td>Backup complete.</td>
</tr>
</tbody>
</table>

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

• You can configure filters for both the reports by clicking the Filter icon on the top-right of the page. You can download any of the reports with or without a filter as CSV files.

Filter Option:

• Filter option lets you add custom filters wherein you can apply a filter of your choice for ease of view.
• The backup filter includes the following statuses to choose from: missed, suspended, failed,
- 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.

The third tab, **Schedule Email Report**, will allow you to email reports periodically to your inbox. Enable the **Email Reports** option and provide the following:
- Email recipient
- Filter selection
- Adding Filter
- Schedule

Click **Save** option once you have provided the required details.

**Evaluator’s Guide for VMware Backup**

**Evaluation Case**

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

**Evaluation Case:**

- **Case 1**
- **Case 2**

**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 **Change Email Configuration** option.

**Step 2: Configure SMTP Server Settings**

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

- **Outgoing SMTP Server** - The SMTP server using which the email reports will be sent
- **Outgoing 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.
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 VMware 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.

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.

The Image Integrity check will take place once the first Incremental schedule is completed. From that time, after 24 hours the Image Integrity check will take place for your backup.
before the upcoming schedule

- To view the Image Integrity Report, open the Reports tab and select the Image Integrity option.

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Client Name</th>
<th>Backup Name</th>
<th>Host Name</th>
<th>Machine Name</th>
<th>Disk Name</th>
<th>Scheduled Time</th>
<th>Mount</th>
<th>Boot</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware</td>
<td>hyper-V_2K</td>
<td>localhost</td>
<td>Win-2_Gen1</td>
<td>Disk2Shared</td>
<td>Mar 19 Nov 2018</td>
<td>✔</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>VMware</td>
<td>hyper-V_2K</td>
<td>localhost</td>
<td>Win-7_Gen1</td>
<td>Disk1Shared</td>
<td>Mar 19 Nov 2018</td>
<td>✔</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>VMware</td>
<td>hyper-V_2K</td>
<td>localhost</td>
<td>Win-7_Gen1</td>
<td>Disk2Shared</td>
<td>Mar 19 Nov 2018</td>
<td>✔</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>VMware</td>
<td>WIndows_2K</td>
<td>localhost</td>
<td>Win-2_Gen1</td>
<td>Disk2Shared</td>
<td>Mar 19 Nov 2018</td>
<td>✔</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>VMware</td>
<td>VM_XP_4GQ</td>
<td>192.168.102.16</td>
<td>XP</td>
<td>Disk2Shared</td>
<td>Mar 19 Nov 2018</td>
<td>✔</td>
<td>NA</td>
<td></td>
</tr>
</tbody>
</table>

- The Image Integrity Report page lists backup details such as:
  - **Plugin used**: The Plugin type of the backup (VMware, Hyper-V or Disk Image)
  - **Client Name**: The Client machine name or agent name from which the backup is configured
  - **Backup Name**: The name of the backup provided during the configuration of the backup
  - **Host Name**: The name of the host in which the data is backed up to the backup server
  - **Machine Name**: The name of the machine for which the backup is configured
  - **Disk Name**: The name of the disk
  - **Scheduled Time**: The time when the Image Integrity check took place. Only the recent integrity check report is displayed here
  - **Mount**: The option ensures the backed up disks in each VM/physical machines are mountable. The backup data is mounted in the disk management and a tick symbol appears when the mount process is successful
  - **Boot**: This process makes sure the bootability of the OS disk to use into a new machine. The VM is booted in the target host and a screenshot of the booted VM is available alongside each backup job. You can find the booted image by clicking the Camera icon
  - For Non-OS disks, mount test can be performed and boot test will be tagged NA(Not Applicable).

- An example of a boot image is displayed below:
Note:

You can also configure **Email alert** for Image Integrity Report, you will receive a mail of Image Integrity report along with a boot image copy.

- The jobs that gets a "-" under the boot column cannot be verified.
- Boot Check is not applicable for Data Partition (i.e) it is only applicable for OS installed drive

You can configure filter for this report by selecting the filter icon and the following options:

- 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.
VM Status Report

- The VM Status Report lists the status of all the VM backup jobs with information such as:
  - Plugin - Plugin Type of the backup job
  - VM Name - Name of the VM
  - Host Name - IP address of the virtual host
  - Last Success - The recent successful VM backup
  - Last Schedule - The recent schedule of the VM backup job
  - Size - Size of the backup job

- From the Reports tab, select VM Status option.

- Selecting the More option will display the details mentioned below:
  - Status
  - Backup Name
  - Incremental Number
  - Start Time
  - Time Taken
  - Size
  - Remarks
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 VMware Backup

Portal Registration

- You must create a Vembu Portal Account to register your backup server with Vembu Portal. Through the 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:

- Open the URL - portal.vembu.com and click the Sign Up option.
- Provide the following details to create your account:
  - Company Name
  - First Name and Last Name
  - E-Mail
  - Contact Number
  - Country and State

- Click the Sign Up option once you are done filling up the requested details.
- A verification E-Mail will be sent to the registered E-Mail ID. Check your Inbox or your Spam folder, if not found in Inbox) for the verification E-Mail 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 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.

- 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 E-Mail ID. You must create a password for your account. Enter the password of your choice and click Activate.

- Your Vembu Portal account will be created successfully. Click Login to Vembu Portal option and login using the registered E-Mail ID and password.
You can view the Vembu Portal Dashboard, an image of the Vembu Portal Dashboard is displayed below.

Server Registration

Once your Vembu Portal account is created
- Login to BDR Backup Server Web-Console.
- Go to Management tab and select the License option.

Registration Steps:
- In the License Management page, click the Register option.
• Provide the Email Address and Password in the pop-up shown and register the trial.

REGISTRATION TRIAL VERSION

Register Vembu BDR Server with Vembu Portal account

Vembu BDR ID:

192.168.109.79

Email Address

Password

Vembu Software collects information of host server it has been installed in (e.g. Host Name, OS details, IP & MAC Address, and UUID), information related to the backup job and backup reports to validate and manage the licenses. Vembu uses this data to simplify the license management, provide sufit technical support and to improve the user experience.

Register Cancel

Don't have Vembu Portal account? Sign up

• Once you have registered, you can check the Server Registration by selecting the Run License Check option.

Evaluator's Guide for VMware 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 you backup job with this license.
- Check the edition-wise comparison of features [here](#)