vembu

Evaluators Guide for Windows Server Backup

vmware PARTNER TECHNOLOGY ALLIANCE

Microsoft GOLD CERTIFIED Partner

NetApp Alliance Partner

Hewlett Packard Enterprise

amazon web services | Partner Network TECHNOLOGY PARTNER

redhat. TECHNOLOGY PARTNER

Backup & Disaster Recovery for Virtual and Physical Data Centers

Table of contents

Evaluator's Guide for Windows Servers and Workstations

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 Windows Servers and Workstations

About Product

With Vembu ImageBackup, you can backup your Physical Windows Servers and Workstations including the Operating System, Files/Folders and Applications for SMBs (Small and Medium Businesses) and Enterprises.

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

- Configure all your physical servers and workstations(desktops and laptops) directly from the Vembu BDR Server.
- Extensive scheduling and retention settings
- Multiple recovery options
- Bare Metal Recovery
- Automated Backup Verifications

Evaluator's Guide for Windows Servers and Workstations

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 Windows Servers and Workstations

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/

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

You can find product demo videos and other tutorials at:
https://www.vembu.com/product-videos/

Evaluator's Guide for Windows Servers and Workstations

Deployment

Evaluator's Guide for Windows Servers and Workstations

Simple Deployment

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

1. Vembu BDR backup server
2. Backup Repository
3. Microsoft Windows Server/Workstation

The Vembu BDR backup server is the core component for your backup infrastructure that lets you coordinate various functionalities through a single web console. The backup server is responsible for Configuring & Monitoring the backup jobs, Managing Storage Repository and other administration activities.

When you perform Backup job from the Vembu BDR backup server, the physical Windows Server backup data is directly processed from the Microsoft Windows host and then stored in the backup repository.

To follow the evaluation cases in this guide, it is sufficient to have only the BDR Backup Server for this deployment.

Evaluator's Guide for Windows Servers and Workstations

Backup Components

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

Evaluator's Guide for Windows Servers and Workstations

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 Windows Servers and Workstations

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 Windows Servers and Workstations

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 Windows Servers and Workstations

System Requirements

- Vembu BDR Backup Server
- Port Configuration
- Naming Conventions

Evaluator's Guide for Windows Servers and Workstations

Vembu BDR Server

OS	• Windows Server 2019 Datacenter • Windows Server 2019 Standard • Windows Server 2019 Essential • Windows Server 2016 Datacenter • Windows Server 2016 Standard • Windows Server 2016 Essential

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

- The performance of the VMware and Hyper-V backups depends on the RAM & CPU availability of the 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 Windows Servers and Workstations

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.

Port	Protocol	Use
32004	TCP	Port used for processing all Backup/Restore/Delete/Replication requests.
6060, 6061,4545	HTTP,HTTPS	Port used for processing all Web Service requests.
32005	TCP	Port used for UI Communication.
42005	TCP	Port used for Communication between Vembu Integration Service and Vembu BDR Server

Evaluator's Guide for Windows Servers and Workstations

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 Windows Servers and Workstations

Installation

- Windows Installation
- Ubuntu Installation

Evaluator's Guide for Windows Servers and Workstations

Windows Installation

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

Evaluator's Guide for Windows Servers and Workstations

Installing Vembu Server

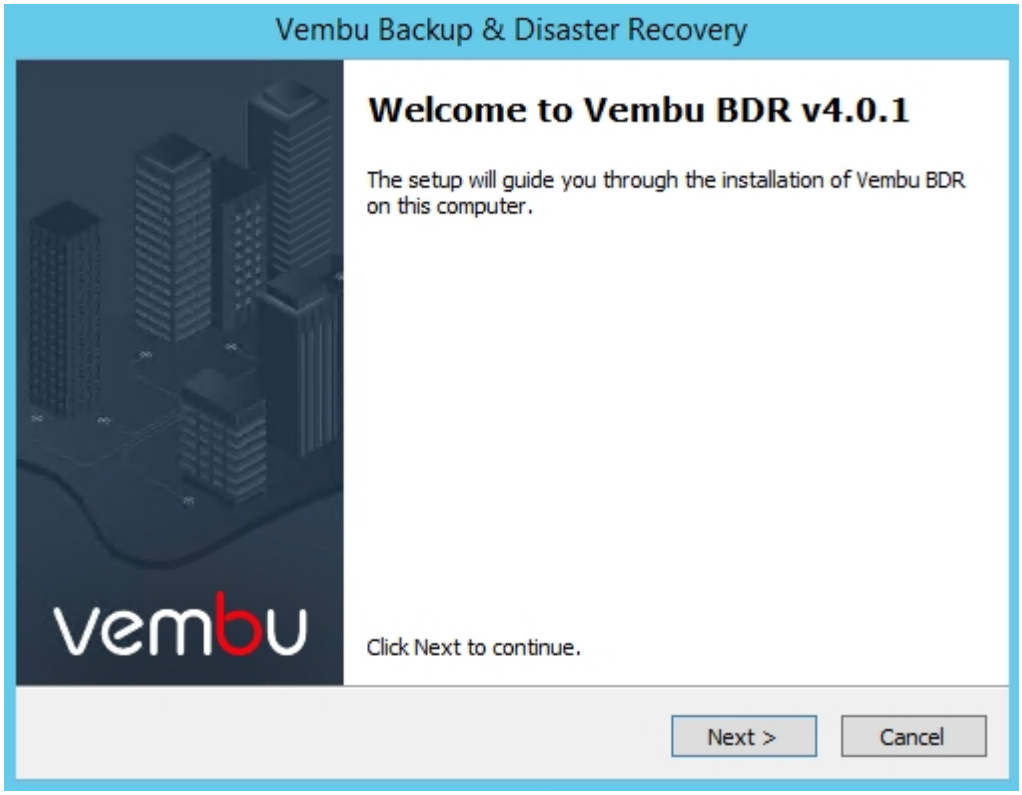
Prerequisites:

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

Procedure:

Step 1: Getting started with the installation

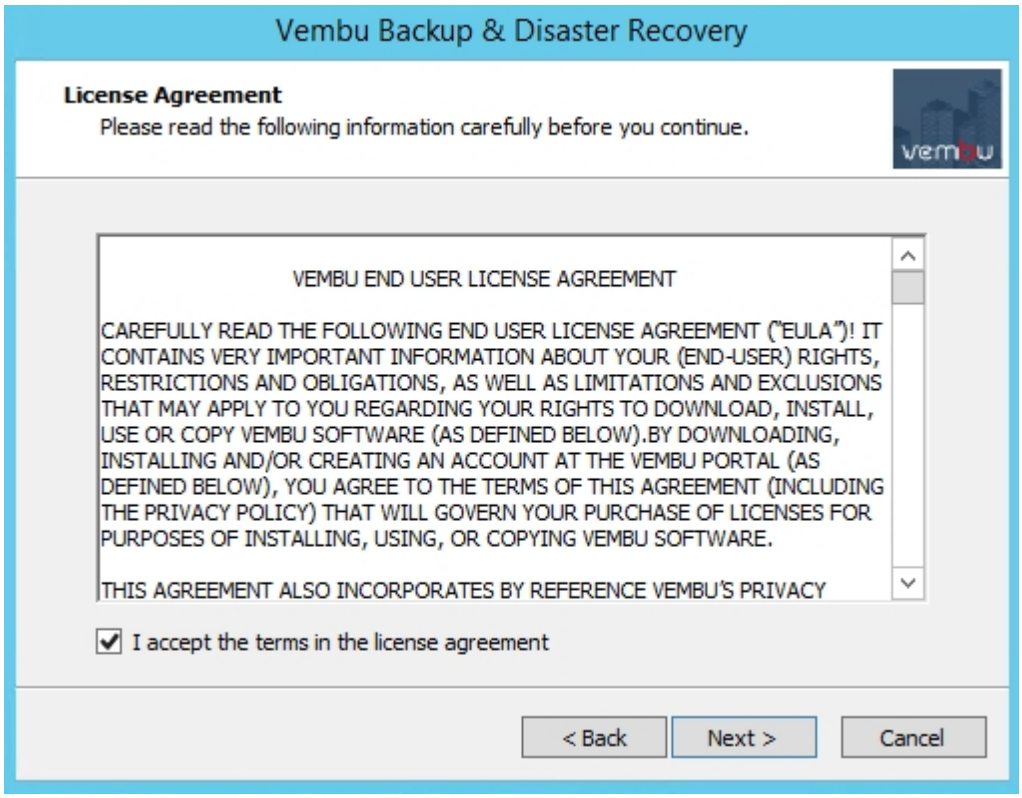
Download the latest version of Vembu BDR Server for Windows and run the installer with administrator privileges. Begin the installation process by selecting **Next** from the welcome page.



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**

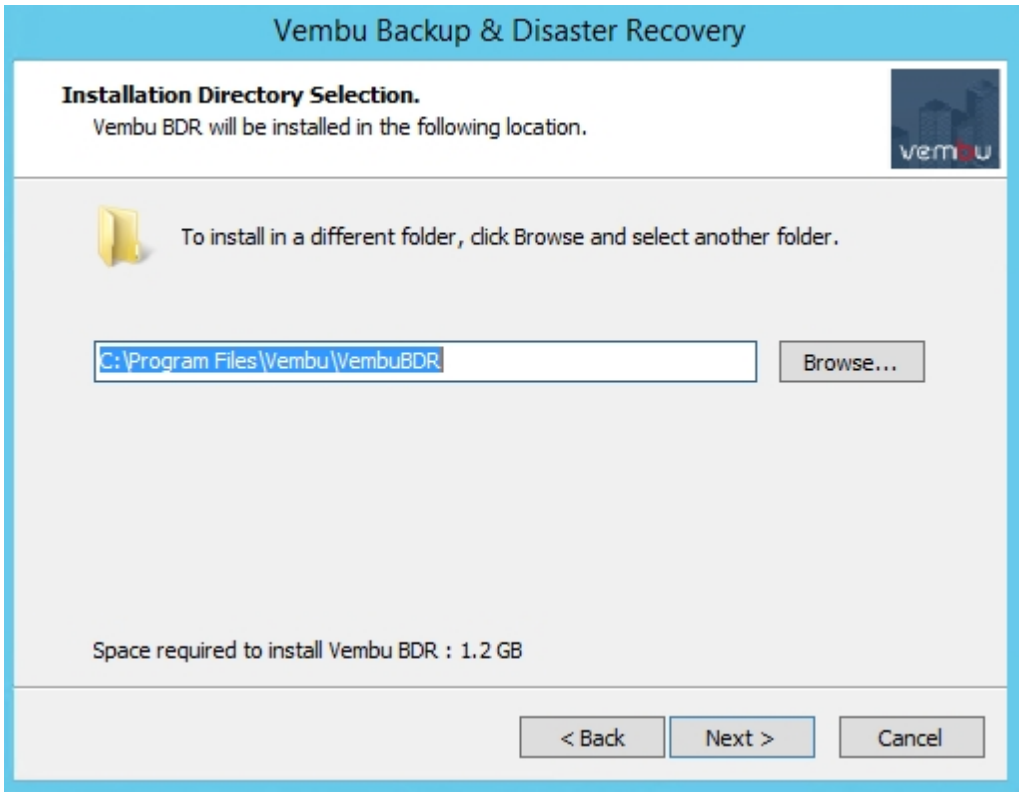
license agreement' option, else you cannot proceed with the installation.



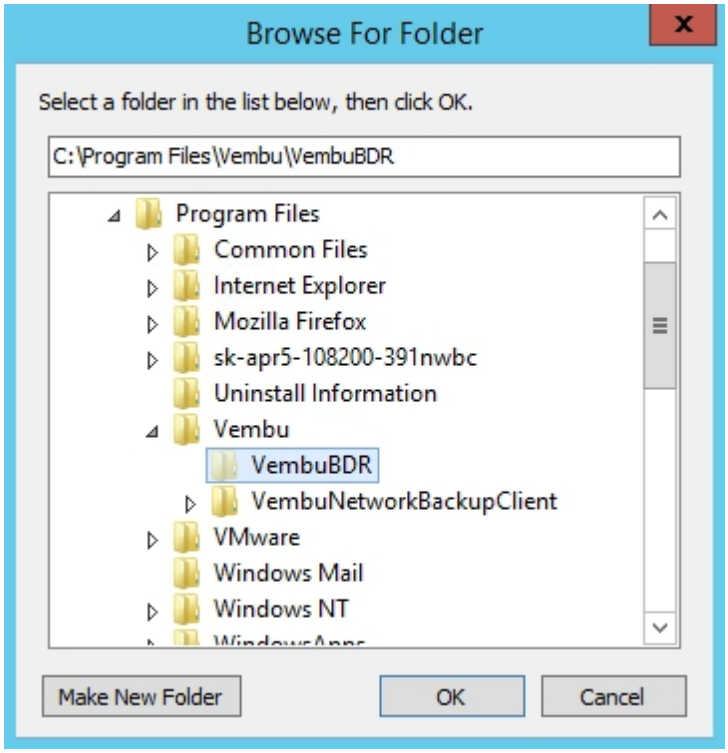
Step 3: Installation Directory Customization:

- 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.



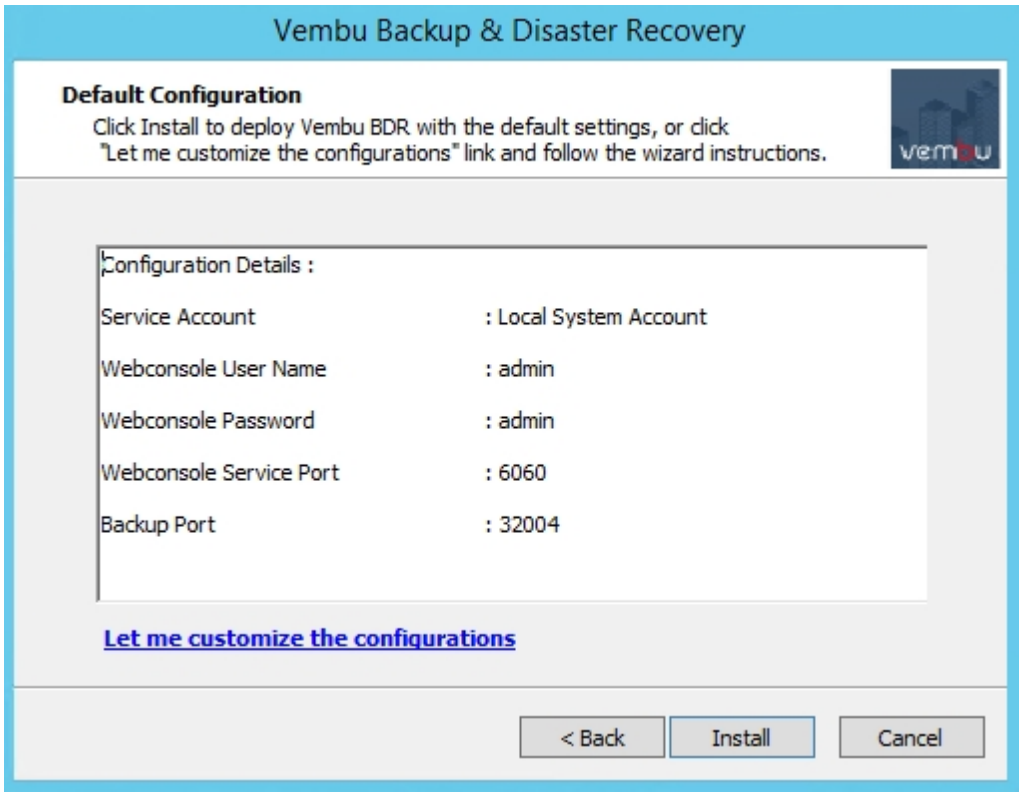
- Click the **Browse** option to select a different location for the Vembu BDR installation. Select the **Make New Folder** option if you want to create a new folder inside the installation location. The new folder by default will be created with the name VembuBDR. Once done selecting the installation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



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

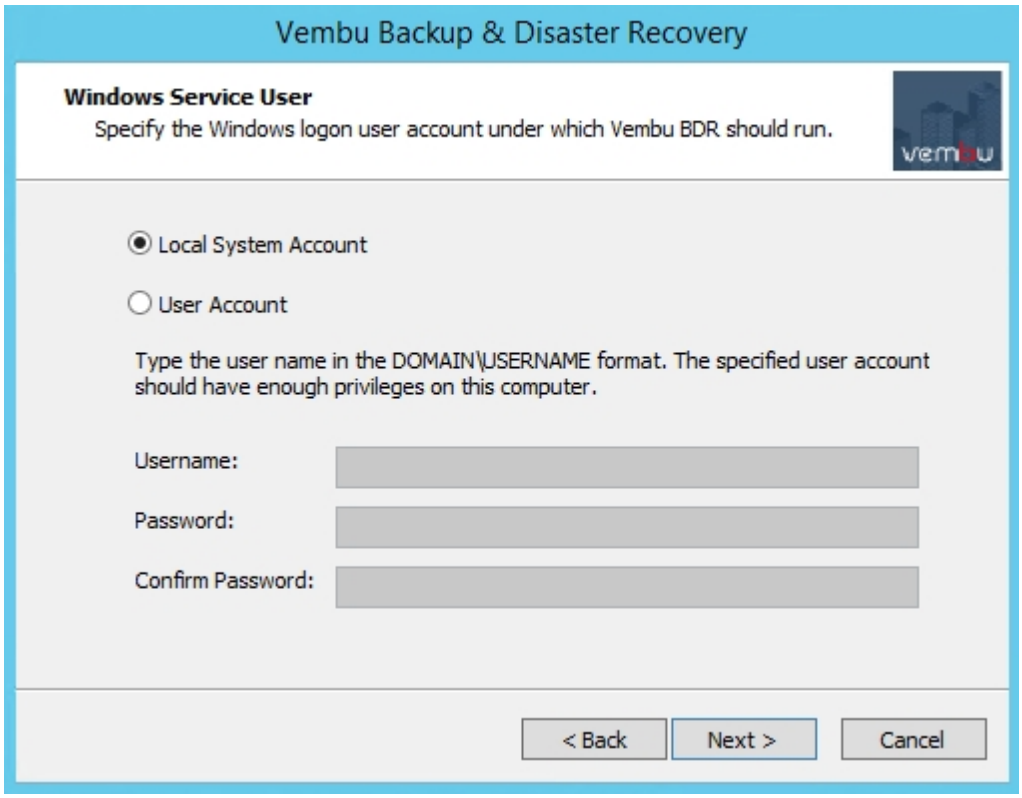
Step 4: Default or Custom Installation Settings

- 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.



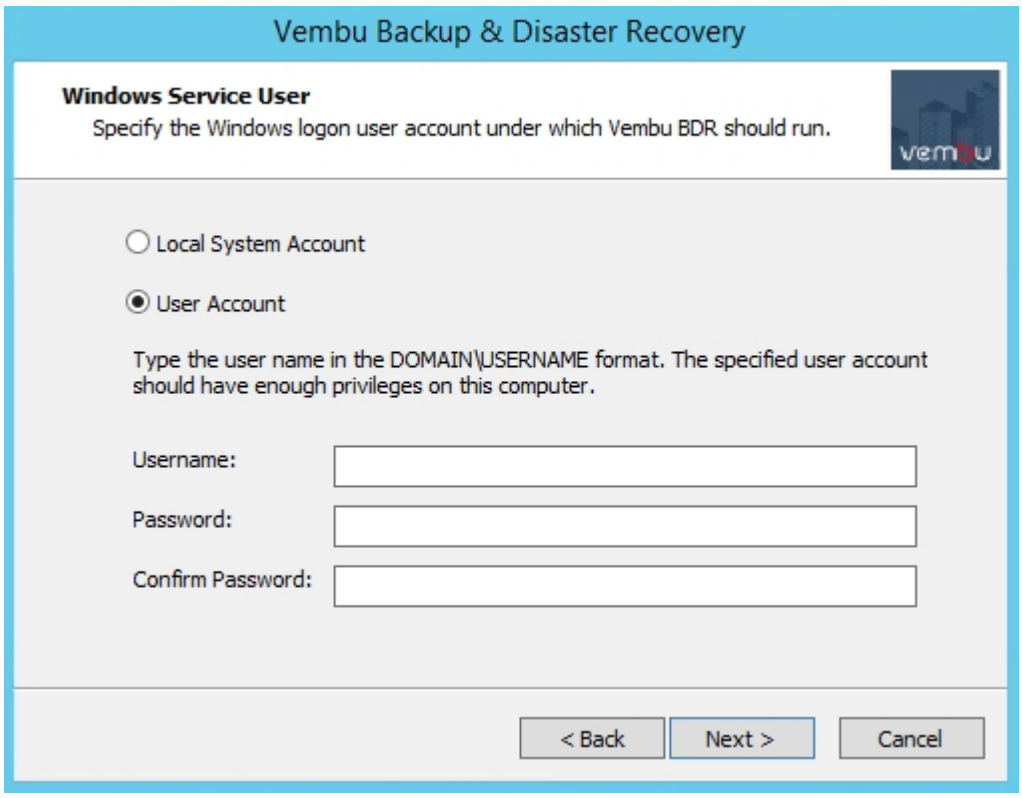
Step 5: Specify the Windows logon user account

- 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.

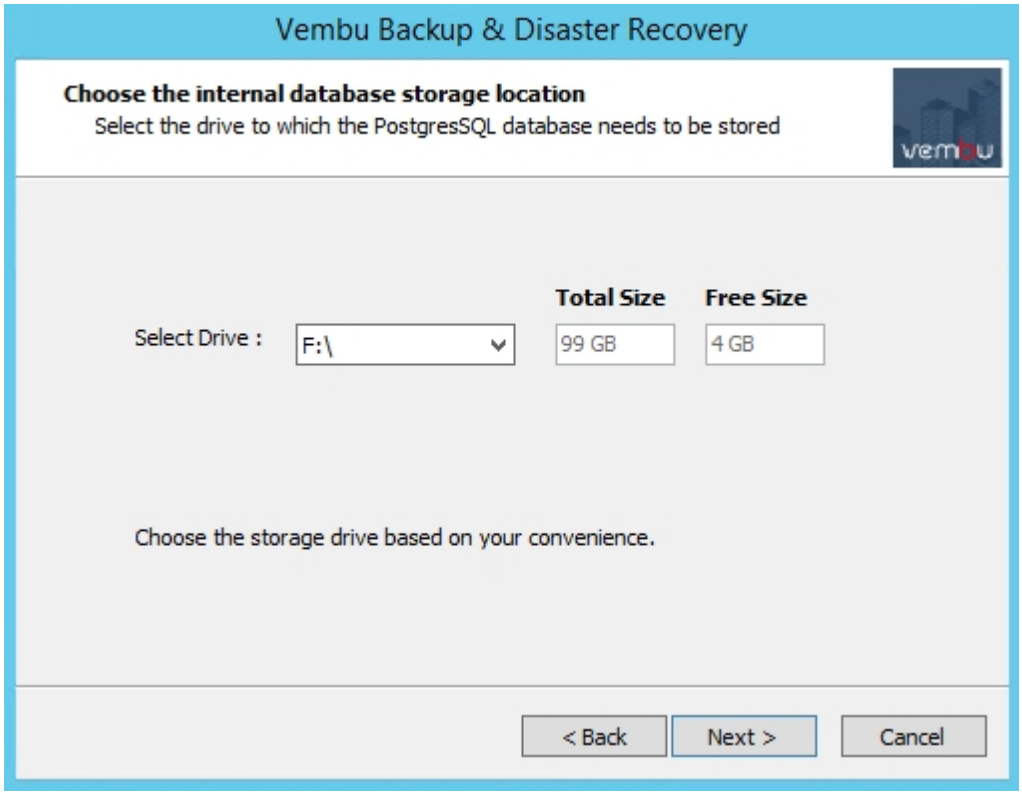
Note: The user name should be in the DOMAIN\USERNAME format. Make sure the specified user account has enough privileges.



- Click **Next** to proceed further with the installation process

Step 6: Configure PostgreSQL Data Location

- The next step in Vembu BDR backup server installation is to select the drive to which PostgreSQL database will be stored. Default drive selection will be based on the maximum space available, however you can select a drive as per your requirement. When you select a drive as the storage, its total size and free size will be displayed adjacently.
- When you configure your storage repository make sure at least 10GB storage space is available. We generally do not recommend you selecting C:/ drive as the storage location since it is the OS drive and consists of important files. Click **Next** to proceed with the installation process.



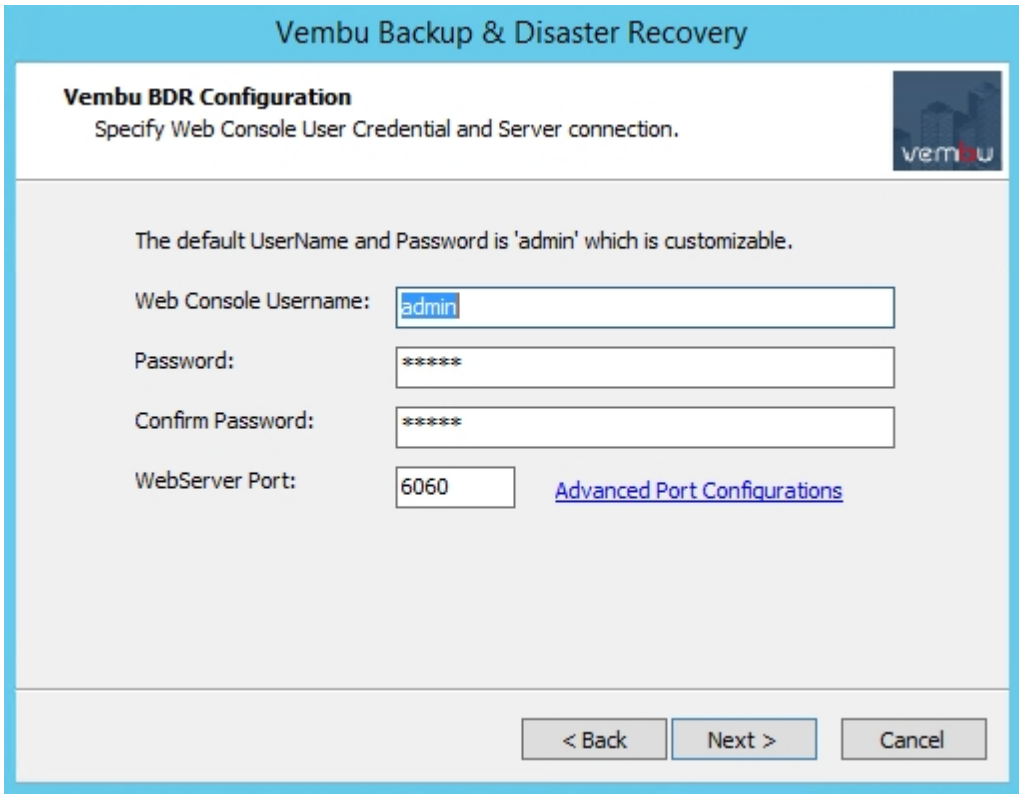
Step 7: Configure Web Server Port:

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

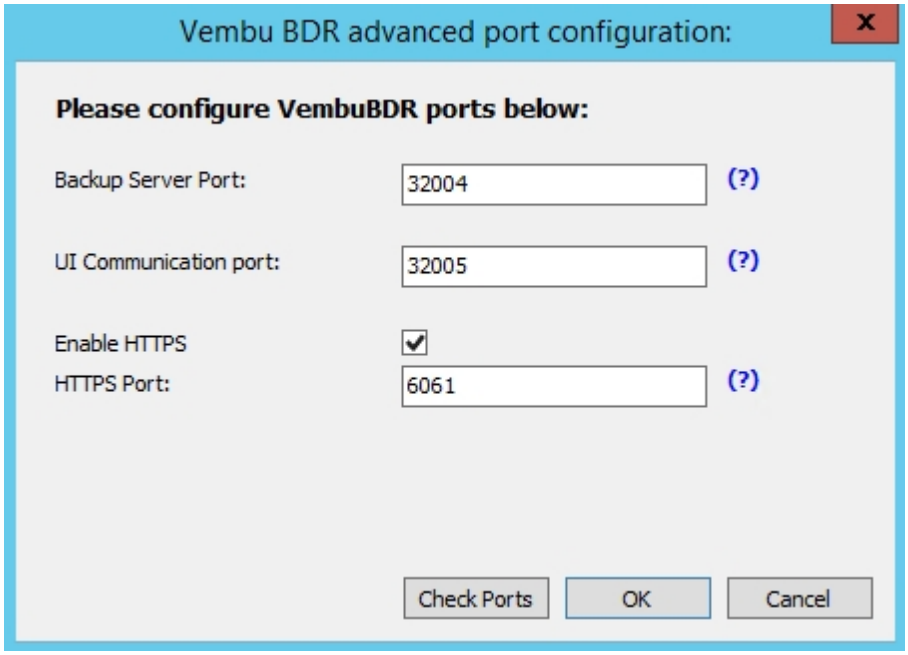
You can configure a range of ports from the **Advanced Port Configurations** tab. The **ports** include:

- Backup Server Port
- UI Communication Port
- HTTPS Port

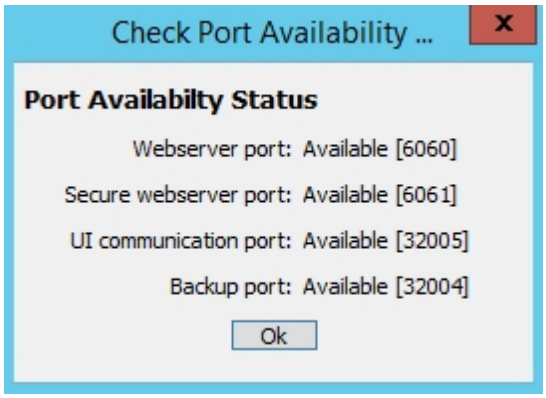
- User credentials for web console (Default User Name: **admin** and Password: **admin**)



- Each port's necessity is mentioned in the question mark near the respective text-box.

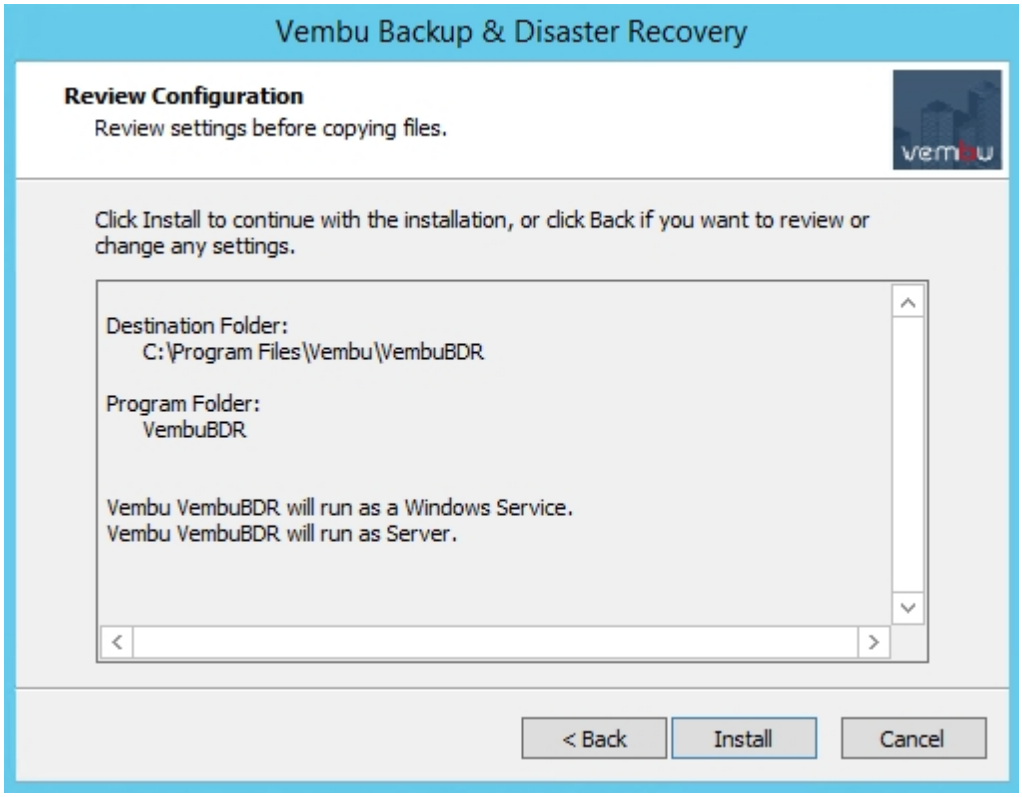


- You can enable the HTTPS port which is used for accessing the Vembu BDR backup server web console in a secure manner. By default, the value is 6061. Selecting the **Check Ports** option will validate your entries provided and check if the ports are available. If the ports are not available, the comment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



Step 8: Review Configuration

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

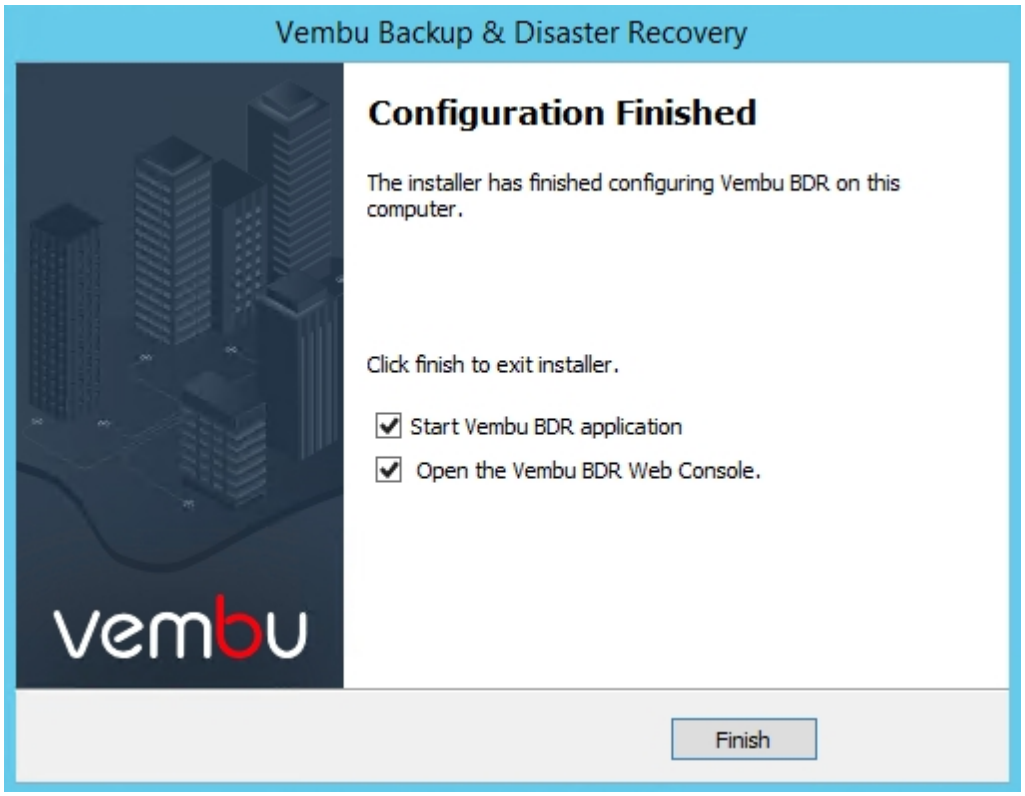


Step 9: Finish Setup Wizard

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

- Open the Vembu BDR Web Console - this will open the Vembu BDR backup server Web-Console.

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



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

Evaluator's Guide for Windows Servers and Workstations

Uninstalling Vembu BDR Server

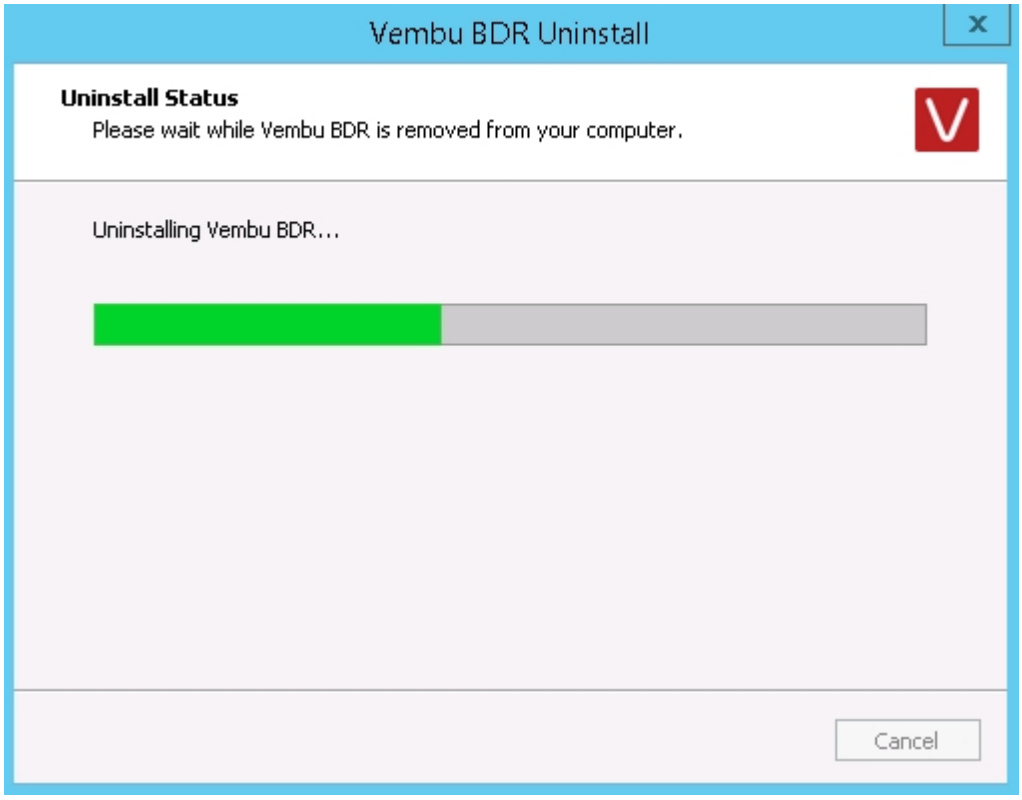
Prerequisites:

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

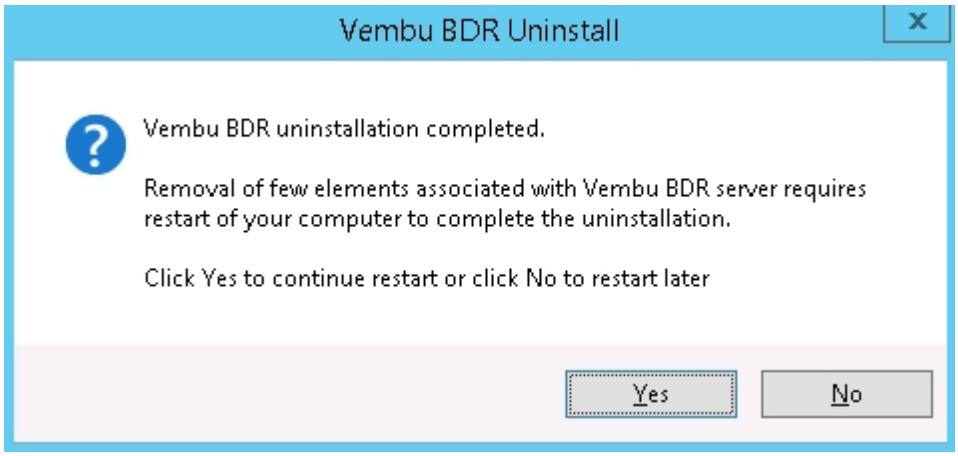
For clean uninstallation of Vembu BDR server in Windows machines, follow the below steps:

- From the Control Panel go to Programs and Features option, right click on **VembuBDR** and select the **Uninstall** option to proceed with clean the uninstallation process.
- In the pop-up window which alerts you that you are 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.



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)

```
|=============================================================================================================|
|      1. Uninstall and Remove VembuBDR                                                                       |

|      2.Uninstall and Remove all the existing VembuBDR, PostgreSQL services [Clean Uninstallation]  |

|=============================================================================================================|
```

- Proceeding with option 1 will delete and uninstall existing VembuBDR instances. If you wish to continue, click **yes**.

```
Enter your choice[ 1 / 2 ] :1
This will uninstall and delete existing VembuBDR instances
Would you like to continue anyway ? Click Yes to continue. Or Click No to use the existing setup[y/n]: y
```

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

```
Enter your choice[ 1 / 2 ] :2
This will uninstall and delete all the existing VembuBDR, PosgreSQL services and its data.
Click Yes to continue. Or Click No to use the existing setup.[y/n]: y
```

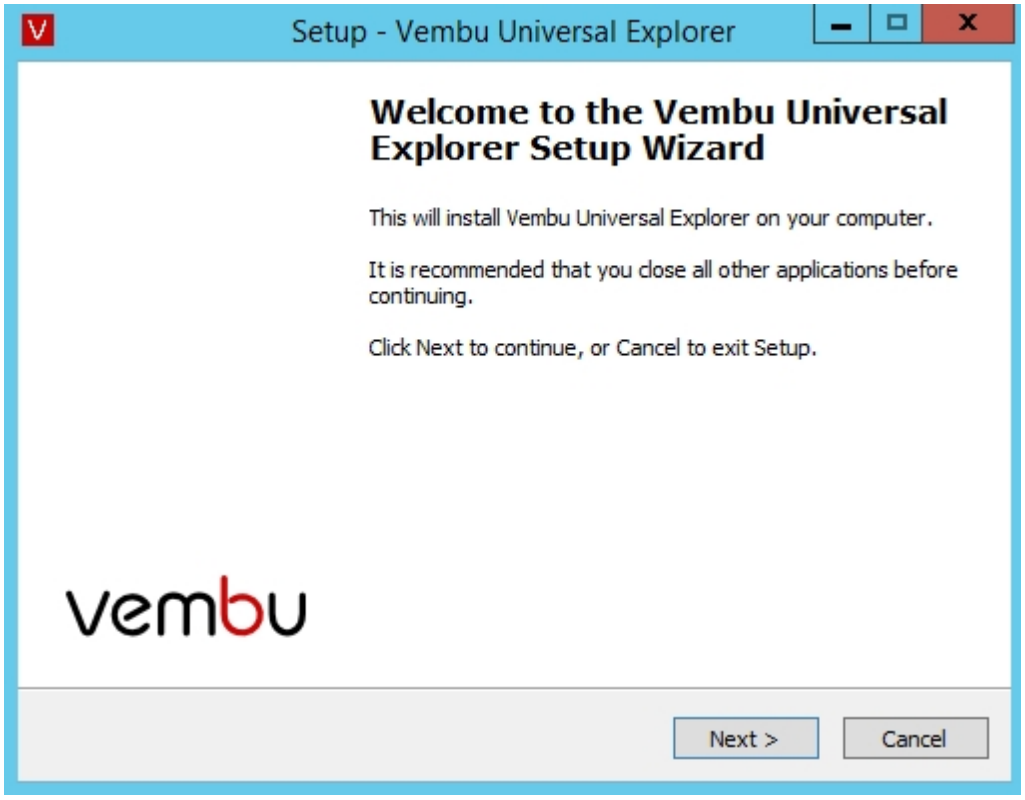
- VembuBDR will be uninstalled successfully.

Evaluator's Guide for Windows Servers and Workstations

Installing Vembu Universal Explorer

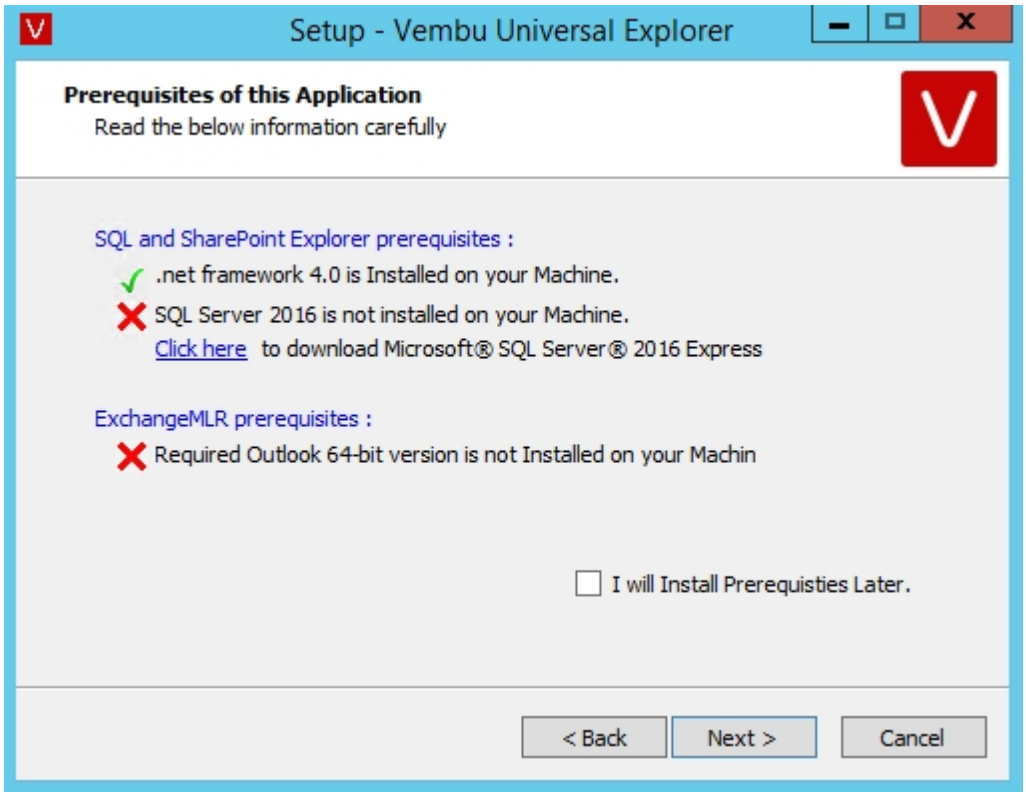
Step 1: Getting started with the installation

- 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.

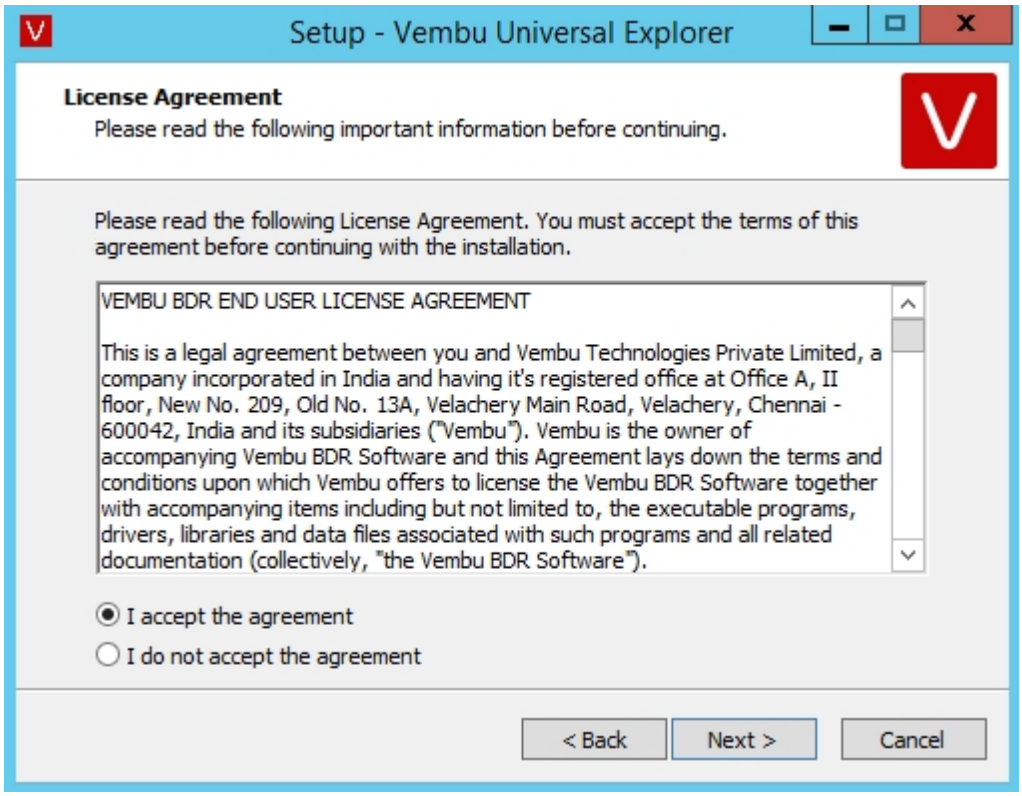


Step 2: Prerequisites and License Agreement

- 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.



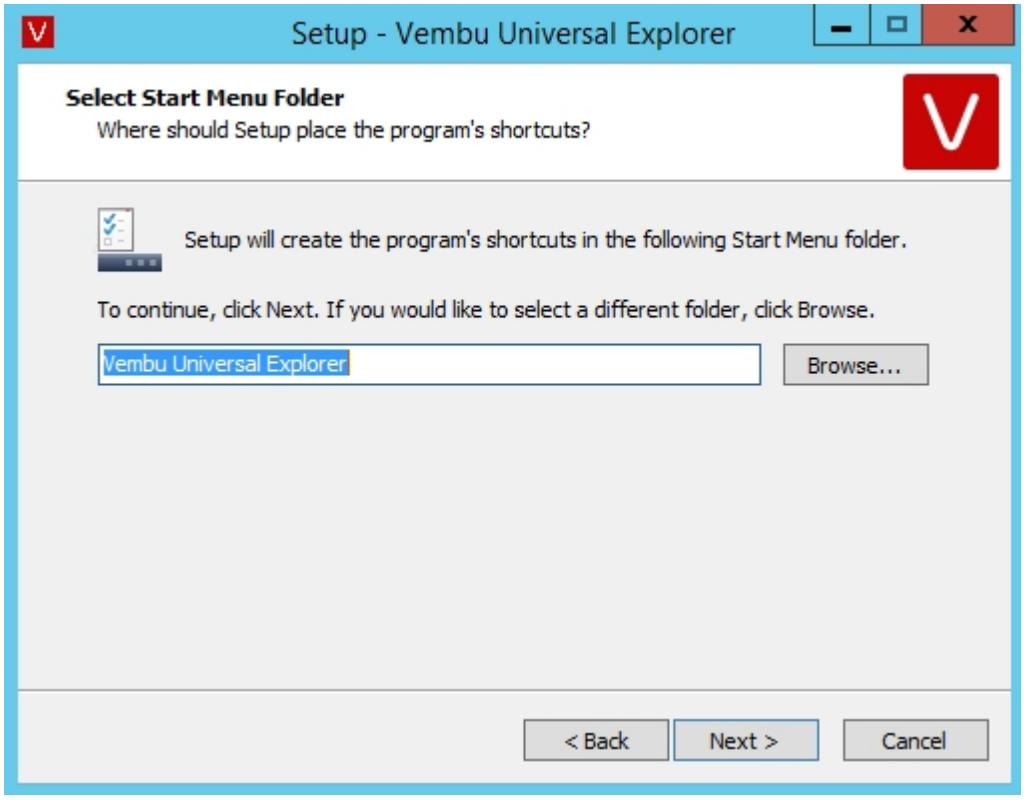
- Read and agree to Vembu Software License Agreement. Click **Next** to continue.



Step 3: Configure shortcut location

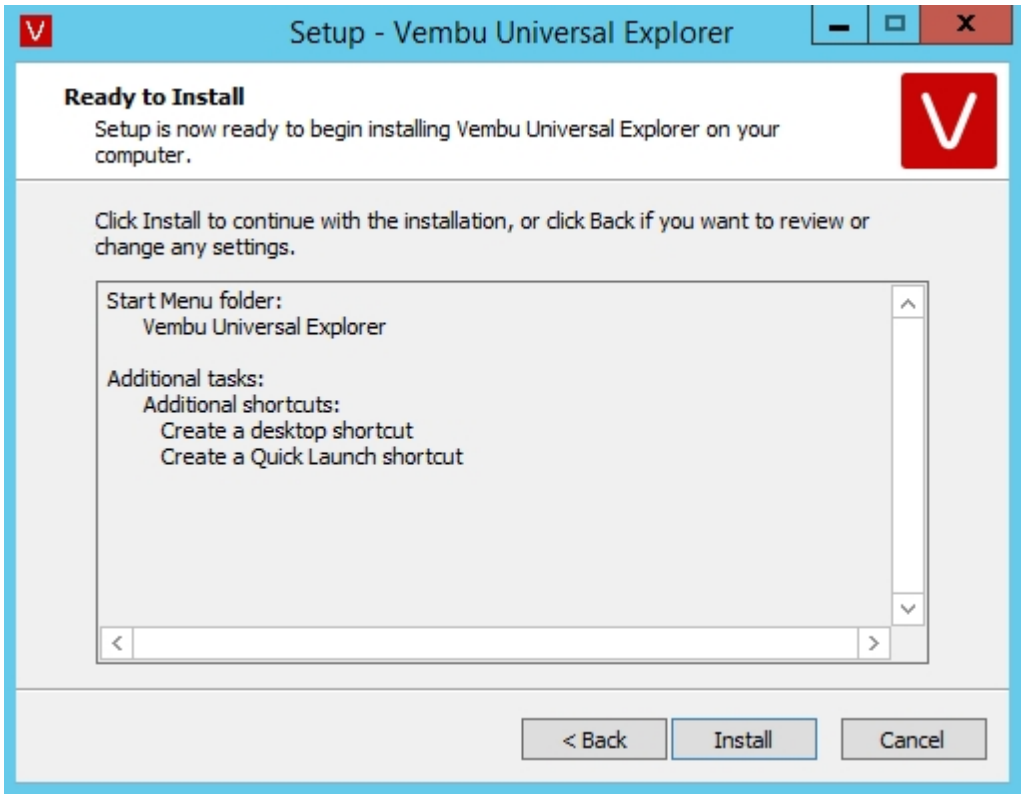
- The installation wizard will ask for folder name under which the setup will add program icons to the folder. In the next page, choose whether you need the shortcut and quick

launch icons for the program and proceed. Click **Next** to proceed with the Vembu Universal Explorer installation process.



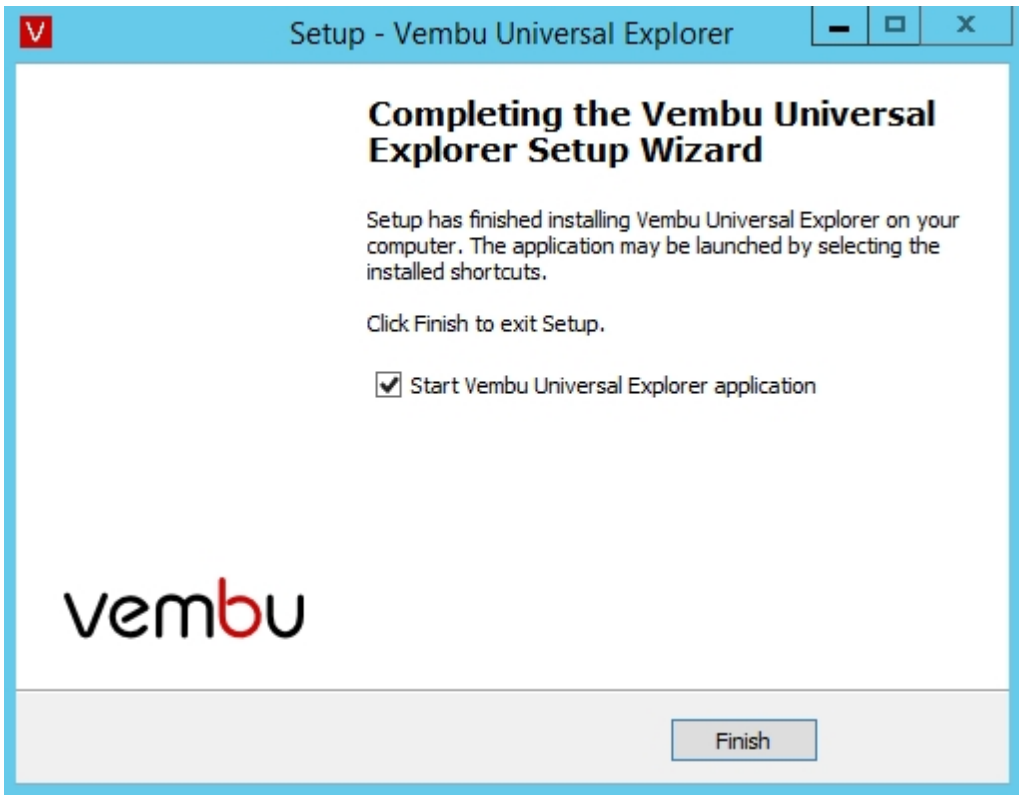
Step 4: Review Selections

- 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**.



Evaluator's Guide for Windows Servers and Workstations

Ubuntu Installation

Evaluator's Guide for Windows Servers and Workstations

Installing Vembu BDR Server

Prerequisites:

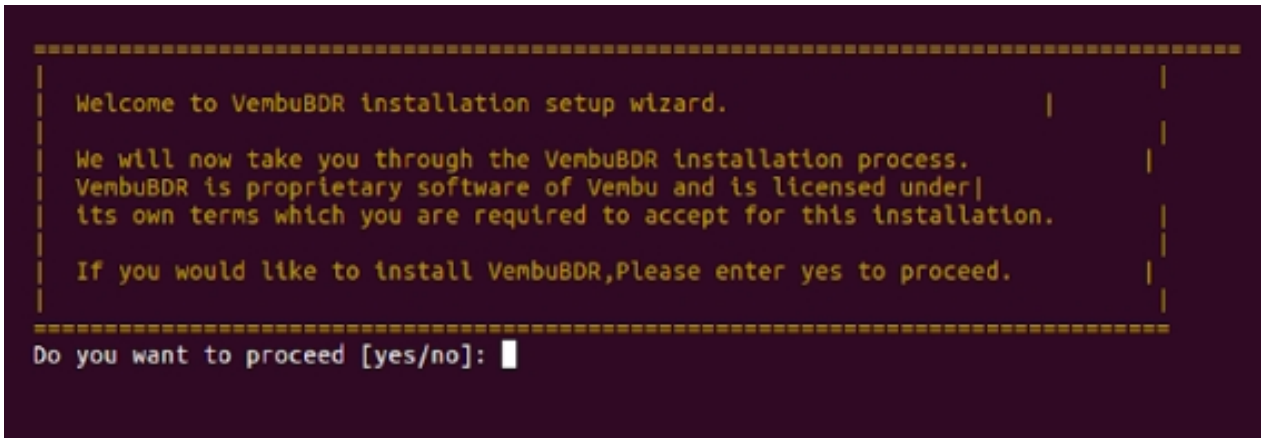
Refer system requirements for Vembu BDR Here

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

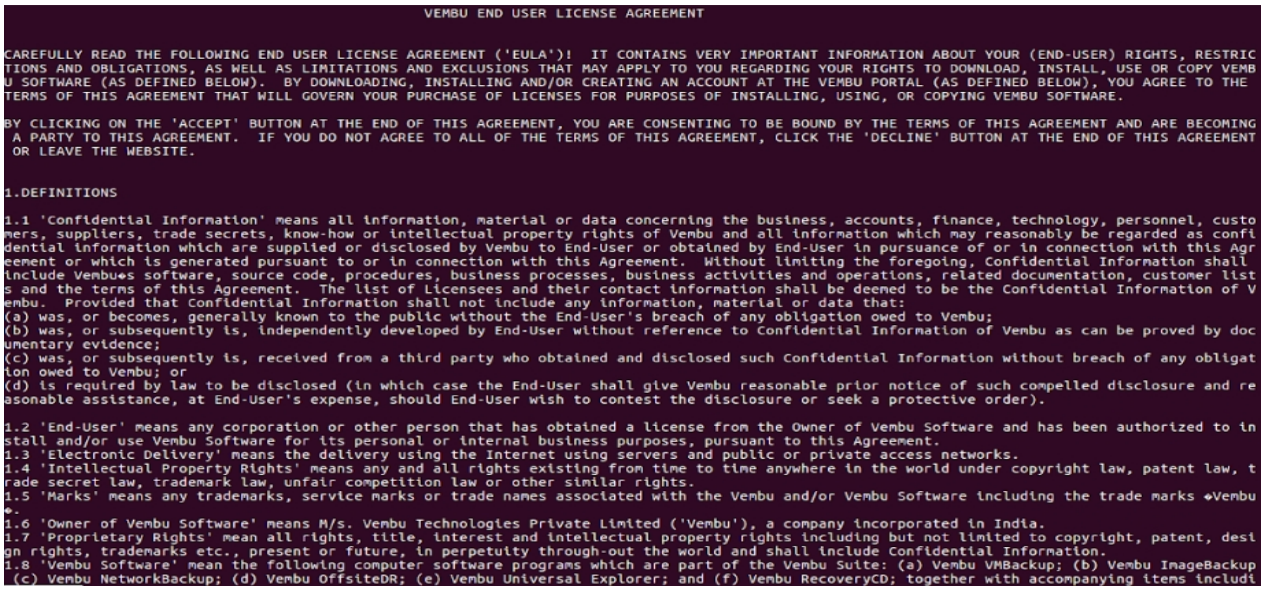
Copy the download link from the following link: Click here and download the installer file using wget command and make sure you are a root user (use “sudo su” command to be a root user). You can download the installer to any Windows machine and move the installer to Linux machine using FTP/WinSCP.

1. Once you execute wget command you will have “**VembuBDRSetup.sh**” in the download location.

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.

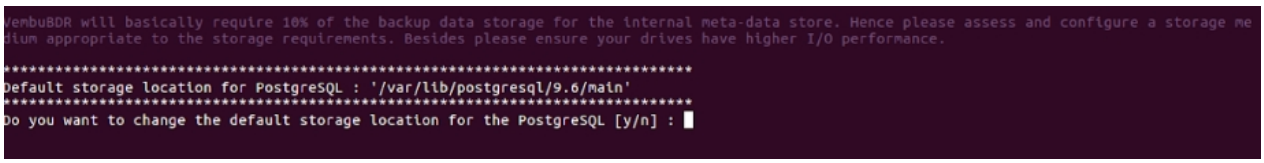


3. The installer shows the License Agreement, read the License Agreement carefully as it contains important information about your Rights, Restrictions, Obligations, Limitations, and Exclusions. Enter “**y**” to proceed with your installation.



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.

```
********************************************************************************
Default storage location for PostgreSQL : '/var/lib/postgresql/9.6/main'
********************************************************************************
Do you want to change the default storage location for the PostgreSQL [y/n] : n
********************************************************************************
Default port for PostgreSQL : '32010'
********************************************************************************
Do you want to change the default port for the PostgreSQL [y/n] : n
********************************************************************************
********************************************************************************
```

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.

```
********************************************************************************
Installing Unix ODBC and Postgresql driver please wait....
odbc configurations for postgresql is in progress.

********************************************************************************
 Test Connectivity between "ODBC-driver" and \PostGreSQL-Server"
********************************************************************************
********************************************************************************
#########################Installing_unixodbc  finished##########################
********************************************************************************
###############Installing postgresql database please wait#######################
********************************************************************************
```

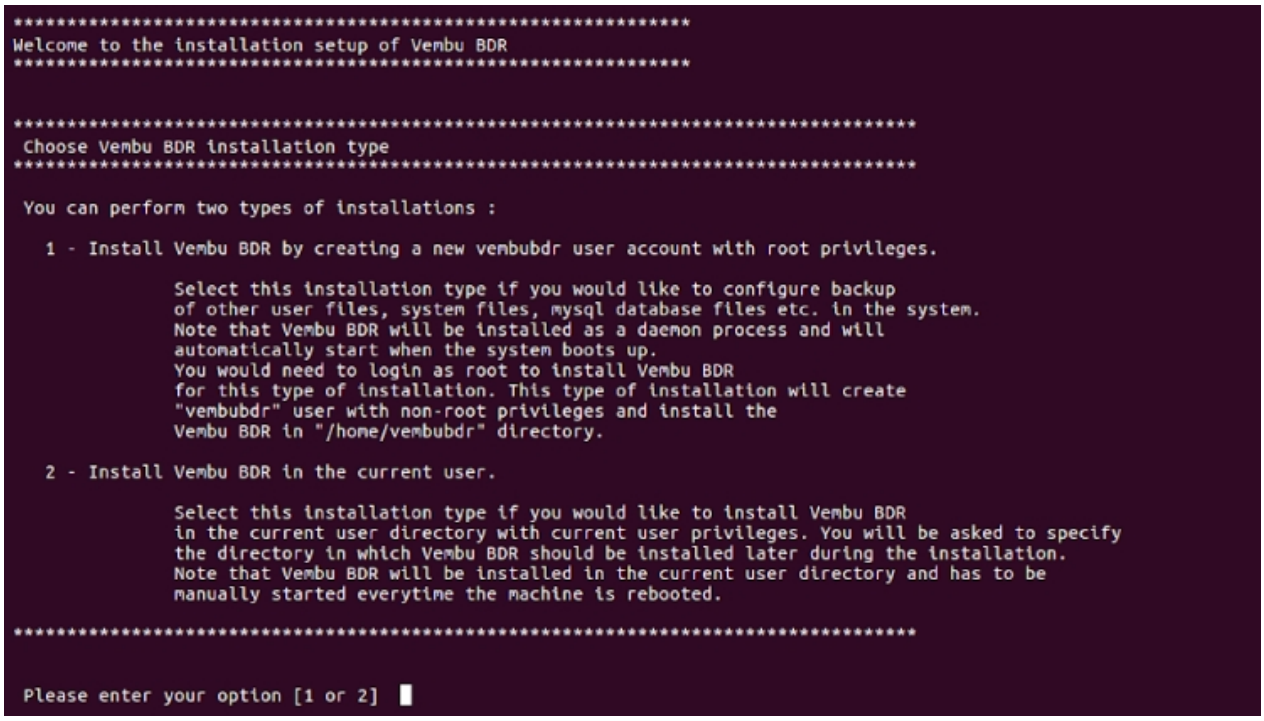
10. Once done installing PostgreSQL, databases will be created and PostgreSQL will be restarted automatically.

```
ALTER ROLE
CREATE DATABASE
```

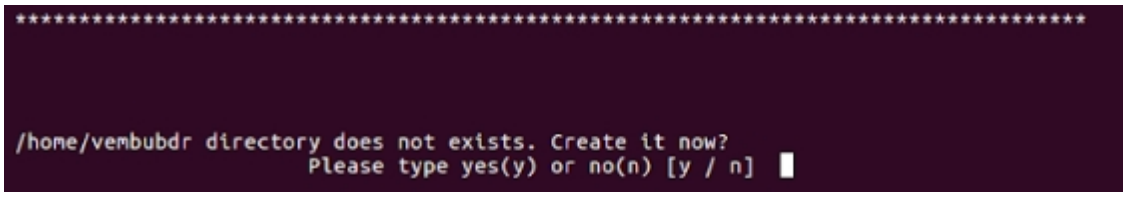
11. In the next step, installer will begin downloading VembuBDR_4_0_0_DBN.zip file.

```
               ##################################################
                VembuOffsiteDR 4.0.1 Server installation
               ##################################################

 Downloading VembuOffsiteDR Now....

Sg-DebianUbuntu-64bit
--2019-04-25 13:58:57--  http://192.168.100.125/builds/VembuProducts/BDRSuite/4-0-1/15-04-2019-20-37/ServerClientBuilds/VembuOffsiteDR_4_0_1_DB
N.zip
Connecting to 192.168.100.125:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 225255559 (215M) [application/zip]
Saving to: 'VembuOffsiteDR_4_0_1_DBN.zip'

VembuOffsiteDR_4_0_1_DBN.zip        100%[===================================================================>] 214.82M  77.9MB/s    in 2.8s

2019-04-25 13:58:59 (77.9 MB/s) - 'VembuOffsiteDR_4_0_1_DBN.zip' saved [225255559/225255559]
```

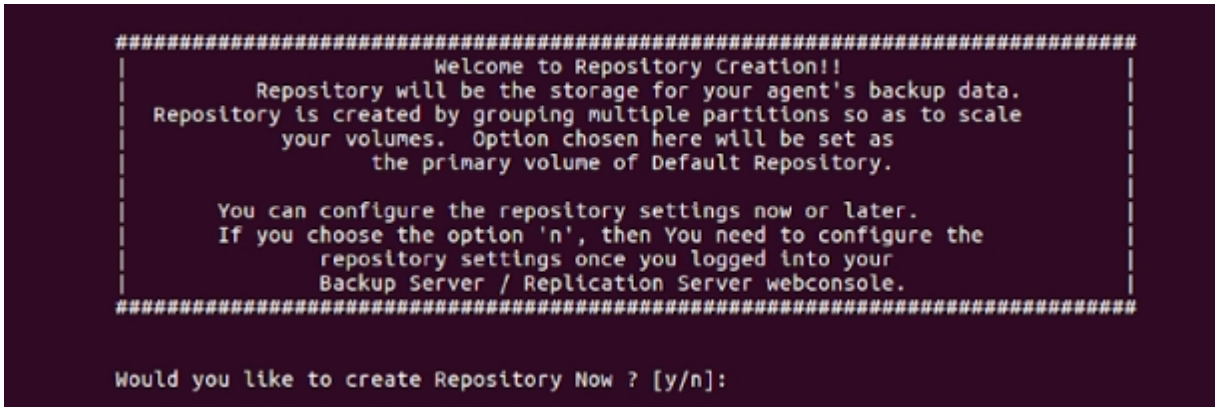
12. The Vembu BDR backup server build installation starts automatically after the download completes and will ask you to choose the type of installation. “Option 1” will Install Vembu BDR by creating a new Vembu BDR user account with root privileges. “Option 2” will install Vembu BDR in the current user 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)

```
Volumes with free space of 5GB or more

       Mounted On              Total Space     Available Space
1      /                       230G            212G
2      /media/vembutest/Storage1                       229G            59G
3      /media/vembutest/Storage2                       230G            218G
df: /run/user/108/gvfs: Permission denied
df: /run/user/1000/gvfs: Permission denied

Please choose any one of volume
```

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.

```
############################ Configured Repository Details ############################

       Repository Name :       Default_Repo
       Volume Path     :       /media/vembutest/Storage2/sgstorage/Default_Repo

#####################################################################################

 You have configured the default repository.
#################### Default Repository configured successfully ####################


 *************************************************************************************

 Vembu BDR Web Console Authentication

 Enter Username and password for Vembu BDR Web Console.
 This is required while starting the Vembu BDR Web Console.


 Enter Username :  admin


 Enter Password :

 Re-type Password :

Vembu BDR Web Console user created.

 *************************************************************************************
```

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

```
**********************************************************************
Backup Server Port is used by Vembu BDR to connect the server. UI Communication Port
is used for communication between Vembu BDR Web console and Vembu BDR Application.
You can configure these ports manually.
By default the value of
  1. Backup Server Port is 32004
  2. UI Communication Port is 32005.
**********************************************************************

Do you want to change these ports from default value [y/n]
```

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.

```
Vembu BDR has been successfully installed!
*******************************************************************************

Installation Details:
*********************

Installation Directory                  : /home/vembubdr
Apache Port                             : 6060

Default Repository Configuration
Repository Name                         : Default_Repo
Storage Path                            : /media/vembutest/Storage2/sgstorage/Default_Repo

Script to start Vembu BDR       : /home/vembubdr/Vembu/VembuBDR/startVembuBDR.sh
Script to stop Vembu BDR        : /home/vembubdr/Vembu/VembuBDR/stopVembuBDR.sh
Vembu BDR Web Console URL    : https://vembu:6061


Vembu BDR installed as daemon process in /etc/init.d/vembubdr
Do you want to start Vembu BDR as daemon process now ? Please type Yes(y) or No(n): [ y / n ]
```

Evaluator's Guide for Windows Servers and Workstations

Uninstalling Vembu BDR Server

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)

```
|=============================================================================================================|
|      1. Uninstall and Remove VembuBDR                                                                       |
|      2.Uninstall and Remove all the existing VembuBDR, PostgreSQL services [Clean Uninstallation]  |
|=============================================================================================================|
```

- Proceeding with option 1 will delete and uninstall existing VembuBDR instances. If you wish to continue, click **yes**.

```
Enter your choice[ 1 / 2 ] :1
This will uninstall and delete existing VembuBDR instances
Would you like to continue anyway ? Click Yes to continue. Or Click No to use the existing setup[y/n]: y
```

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

```
Enter your choice[ 1 / 2 ] :2
This will uninstall and delete all the existing VembuBDR, PosgreSQL services and its data.
Click Yes to continue. Or Click No to use the existing setup.[y/n]: y
```

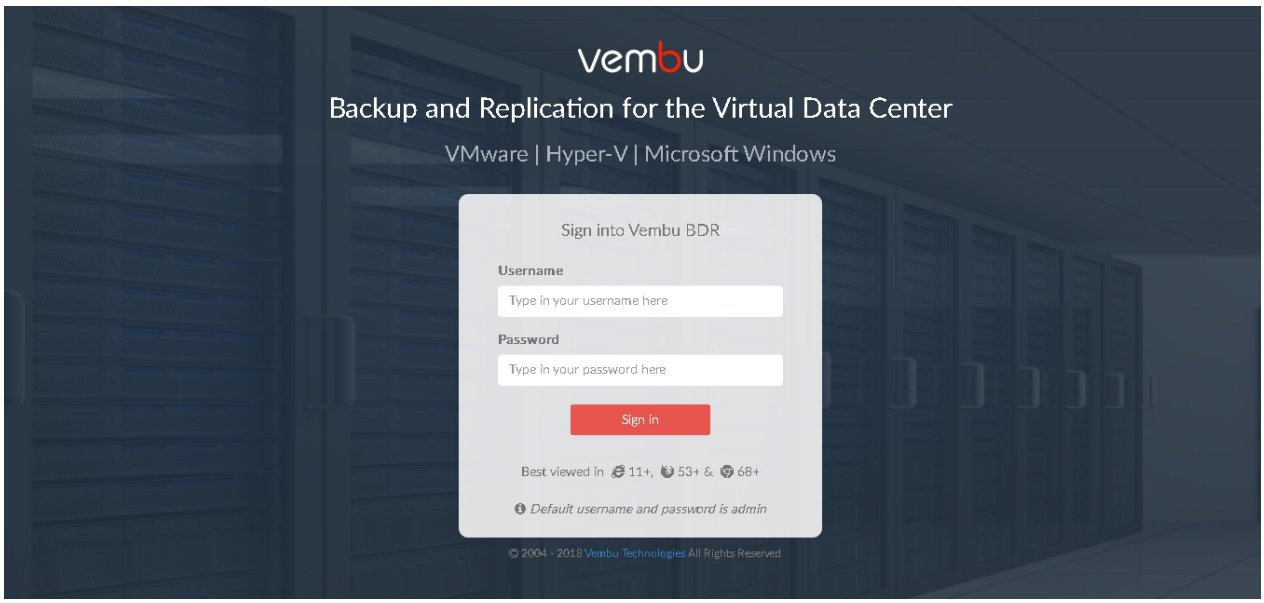
- VembuBDR will be uninstalled successfully.

Evaluator's Guide for Windows Servers and Workstations

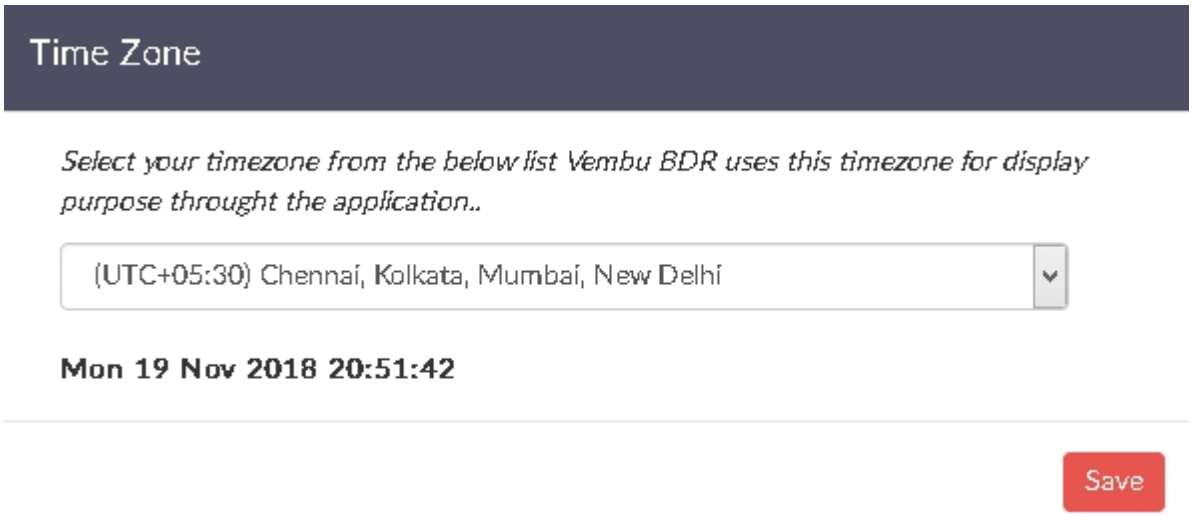
Login to Web GUI - Vembu BDR

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

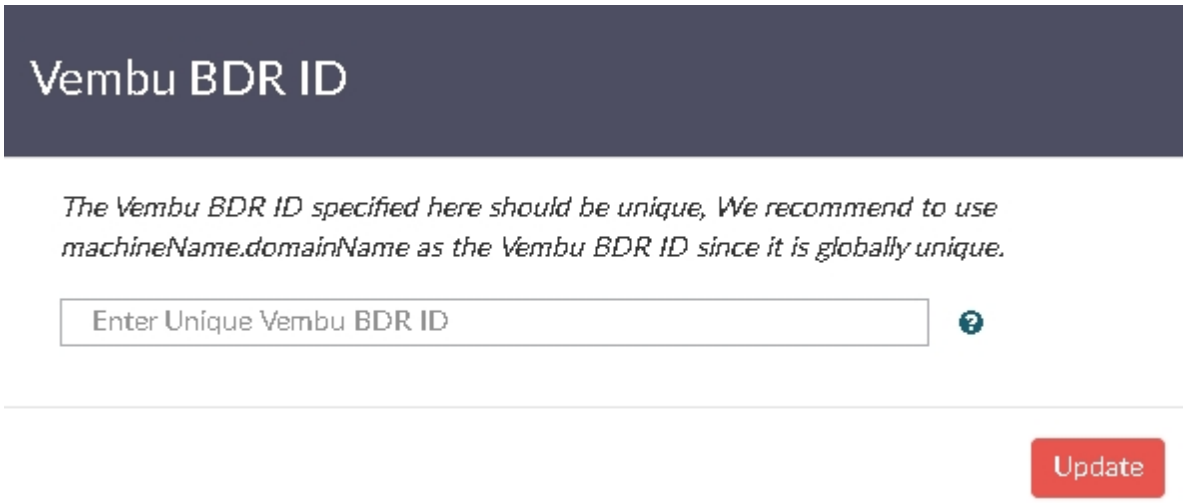
- Entering the URL: https://localhost:6061 (or)
- **https://<IP_Address_of_Machine>:6060 (or)**
- **https://<IP_Address_of_Machine>:6061 (secured port) in browser**
- Via **shortcut icon** created in the desktop
- Via web console option the **tray icon**



- 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.



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



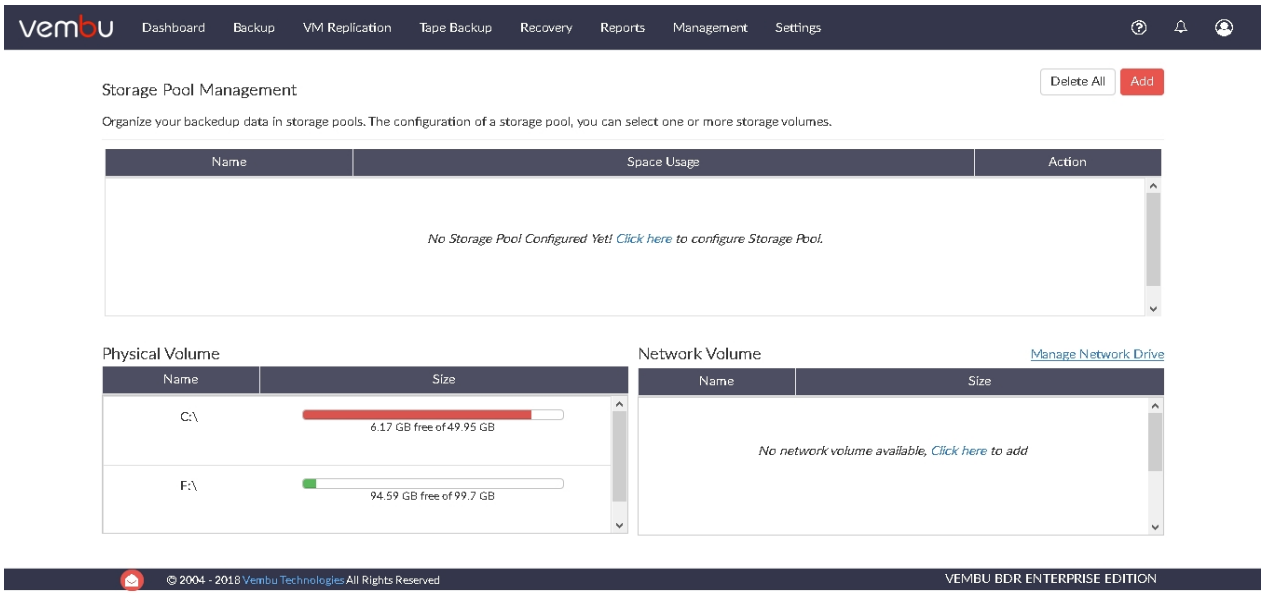
- Click the **Update** option once you have assigned the Vembu BDR ID. The Vembu BDR ID will be updated successfully and you will be redirected to the storage pool management page. Configure a storage pool to begin with your backup process.

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

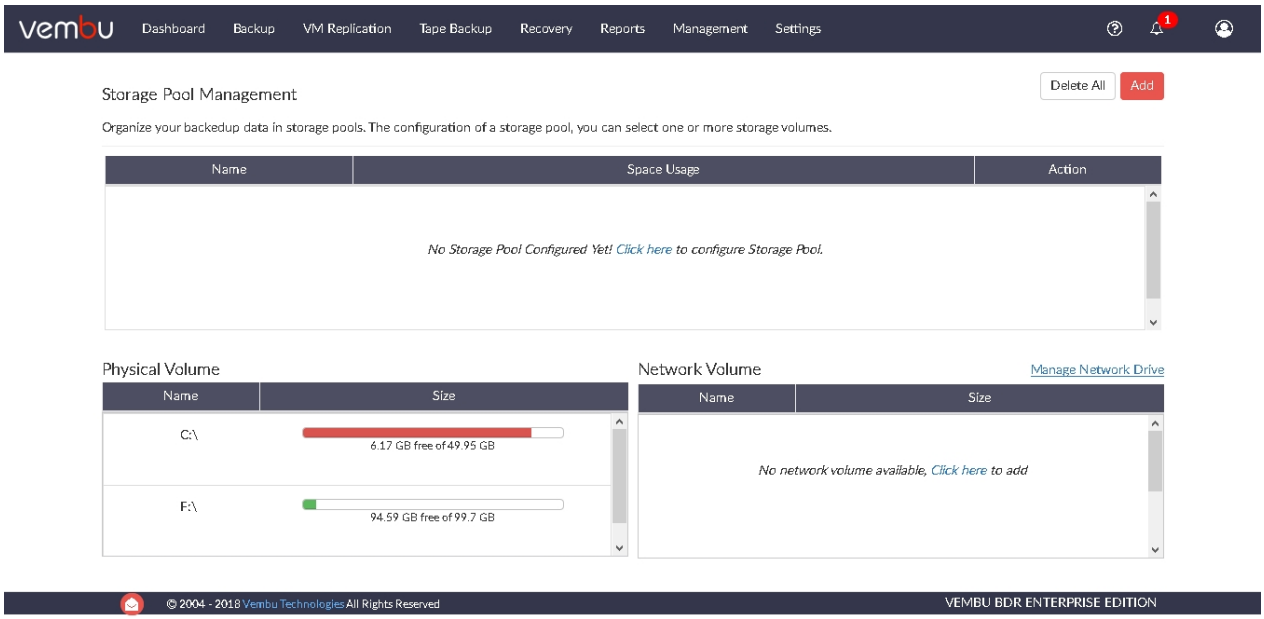
About VembuBDR Installation	
OS Name	Windows 2012 R2
Build Name	VembuBDRSetup (3).exe
Build Version	4.0.1
Build Number	4012019041520
Previous Version	0
Installation Date	Thursday 25-Apr-2019 02:00:20
VembuBDR Mode of Installation	Server
VembuBDR Application Type	Service
VembuBDR Installation Path	C:\Program Files\Vembu\VembuBDR
Small & Medium Businesses and Remote / Branch offices edition	

Evaluator's Guide for Windows Servers and Workstations

Storage Pool Management

- Storage 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

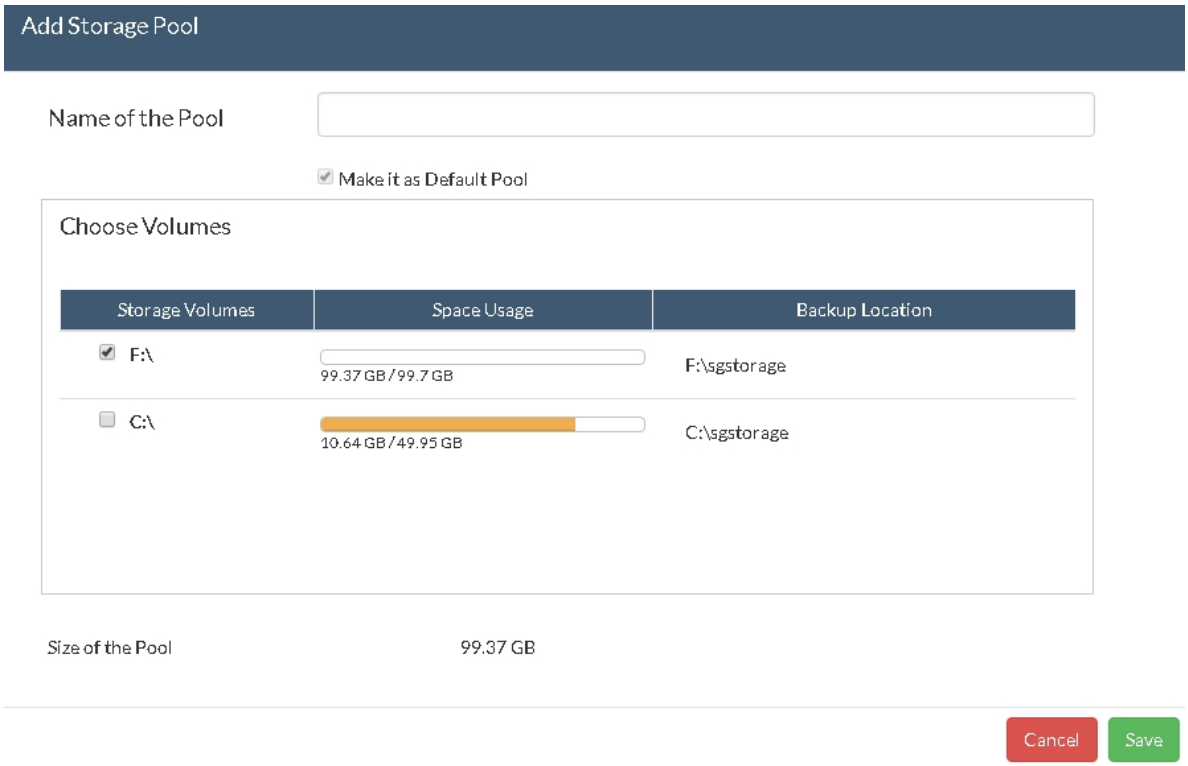
nothing and once the storage pool gets filled, you can extend the storage by using the edit option. New volumes can be added to an already created storage pool.



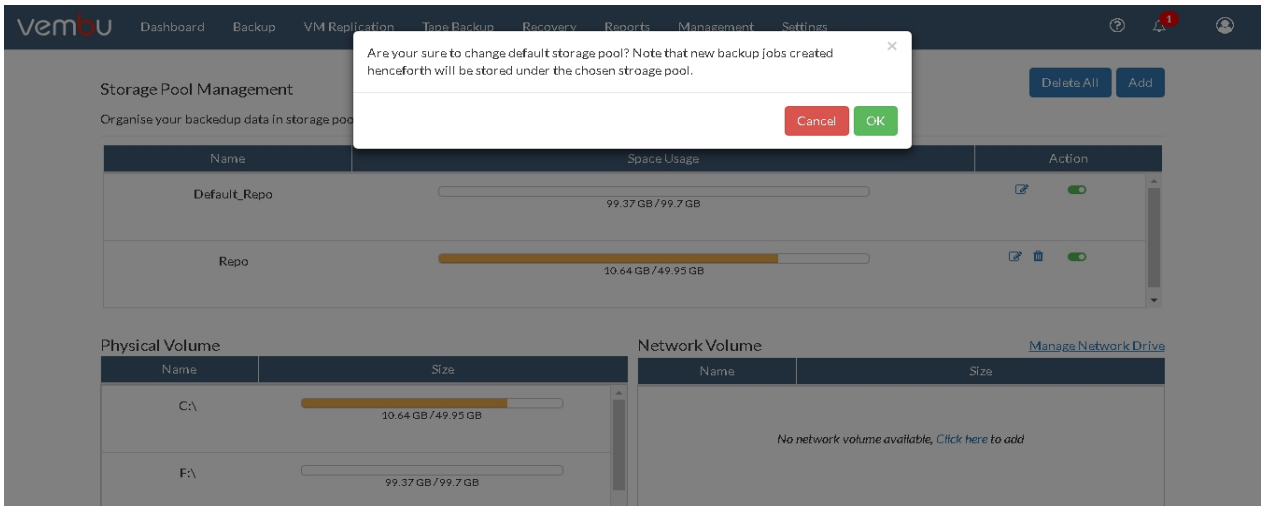
Note: Vembu BDR repository management has a hybrid volume manager that supports scalable and extendable backup storage of different storage media such as Local drives, NAS(NFS and CiFS) and SAN(iSCSI and FC).

- 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.



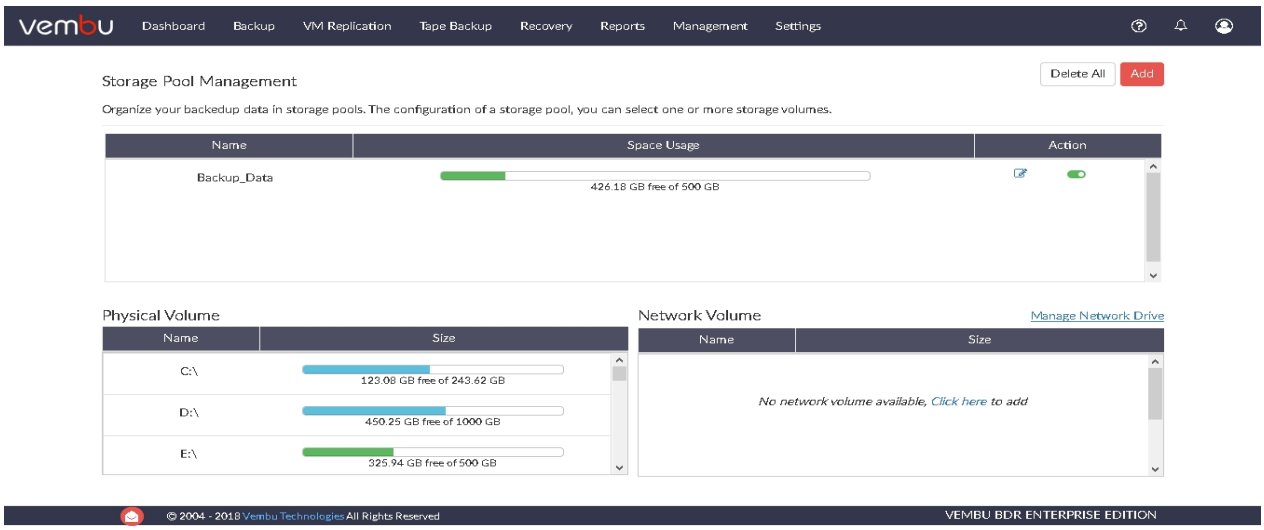
- You can add network volumes using the **click here** option or **Manage Network Drive** option available in the Network Volume section.

- 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 Windows Servers and Workstations

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 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

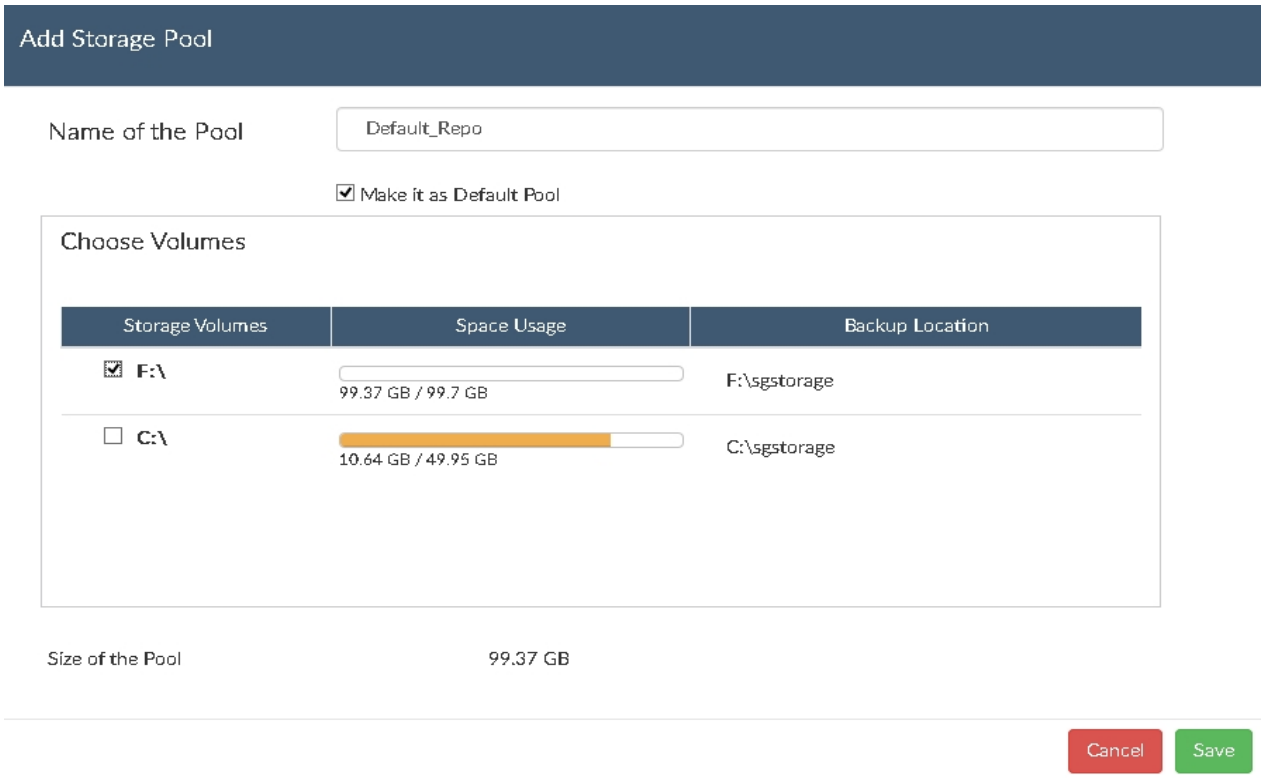
Note: Only [a-z][A-Z][0-9][- _] characters are allowed in the storage pool name.

- **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

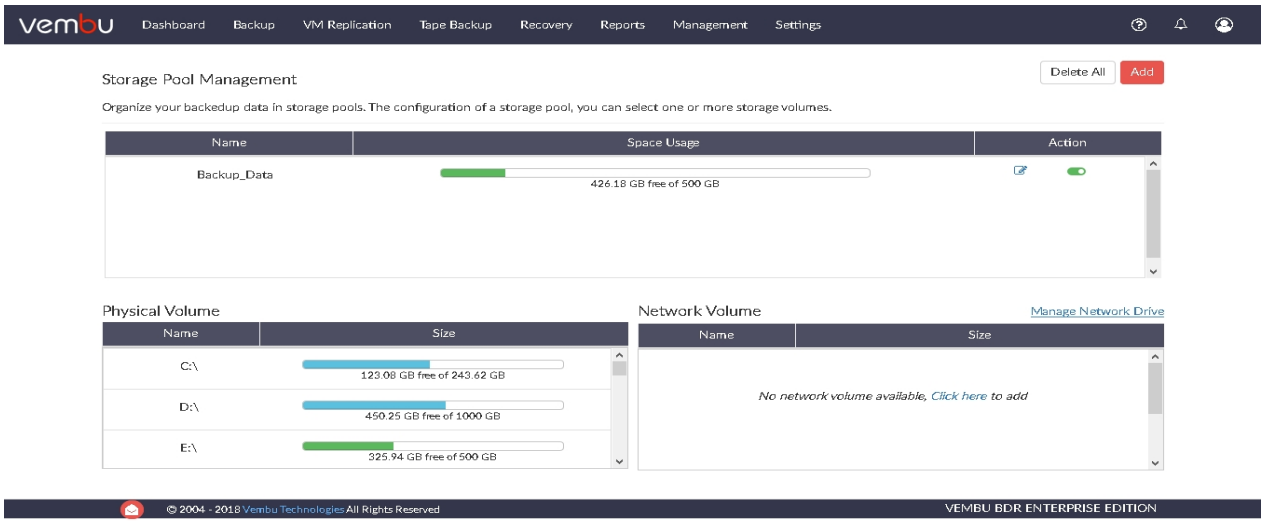
you want to select the drive for a pool.

- **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.



- 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 Windows Servers and Workstations

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.

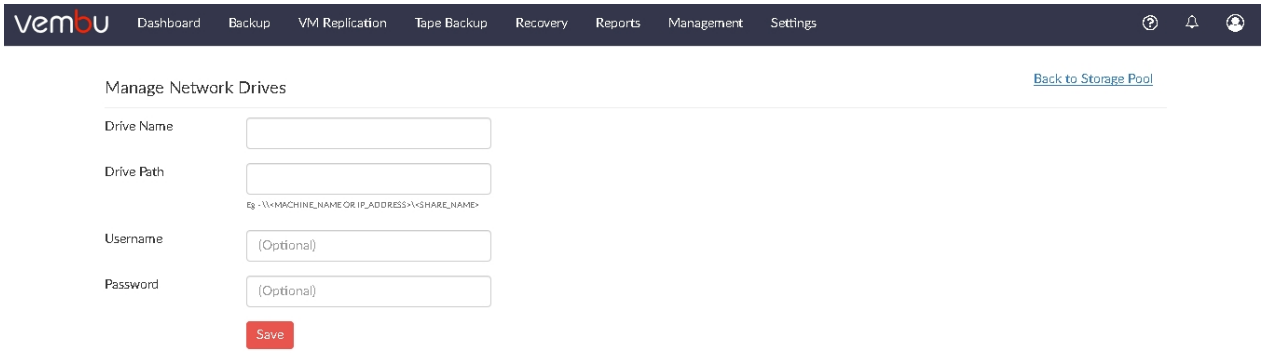
Note: Mapped Network Drives are not supported when Vembu BDR server runs in local logon account. Change logon user with administrator privilege user in service management console and then proceed to configure network drive.

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

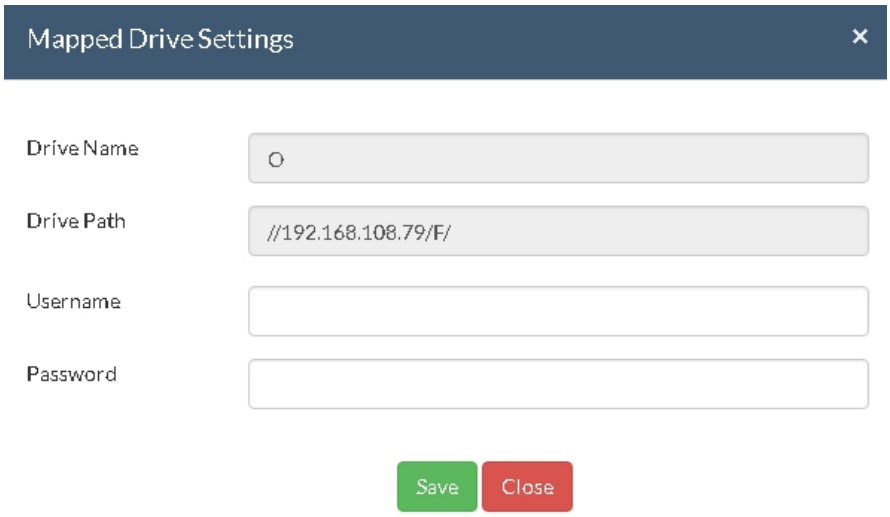
Add & Manage Network drives:

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>

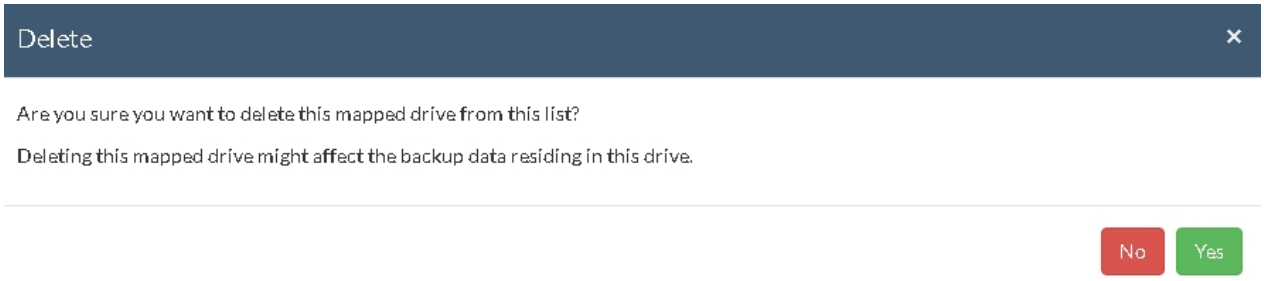


- **Username & Password-** If the network drive requires login authentication provide the username and password to authenticate drive addition.
- You can add 'n' number of network drives and manage it via **Manage Network Drives** page.
- An added network drive can be edited, click the **edit** icon 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 Windows Servers and Workstations

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:

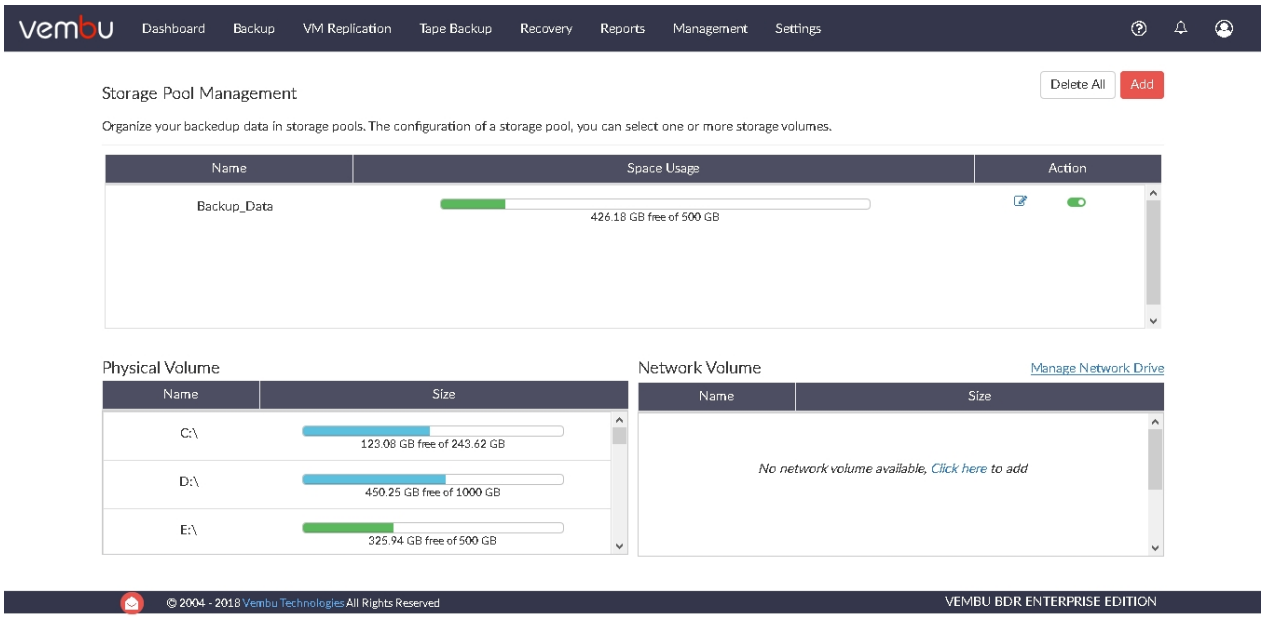
Vembu Storage Calculator

Evaluator's Guide for Windows Servers and Workstations

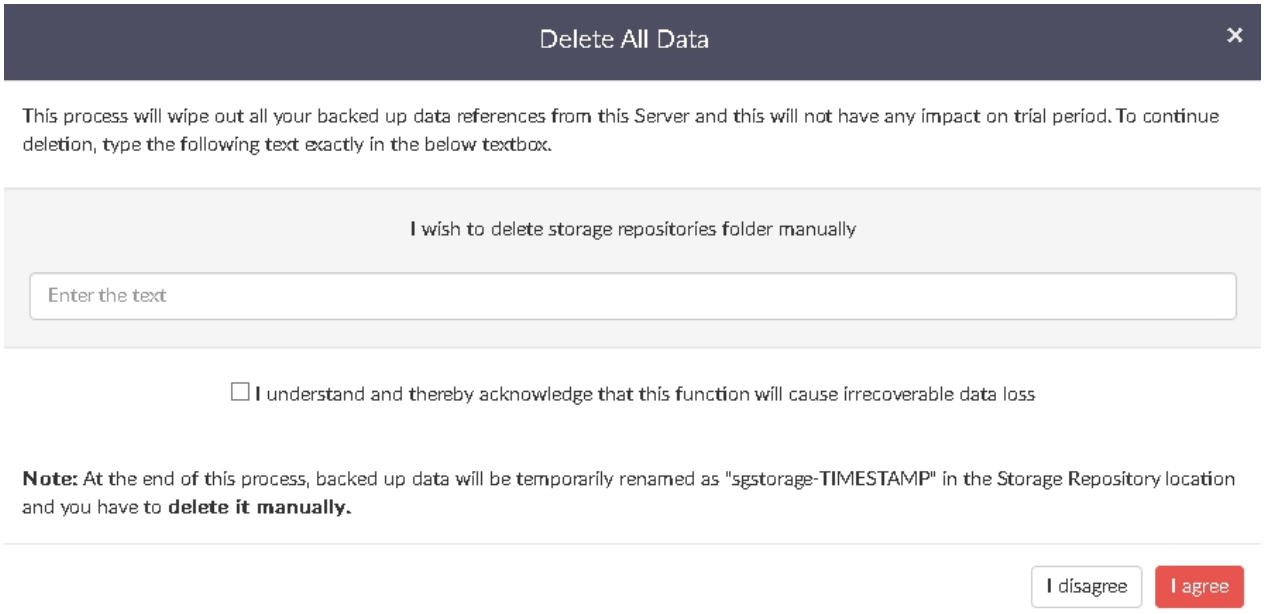
Delete All Data

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 Windows Servers and Workstations

Getting started with Windows Server and Workstation Backup

- Adding Microsoft Windows Server
- Installing Vembu ImageBackup Driver
- Setup Image Backup Job
- Evaluation Case
- Recovery
- Manage Backup Job

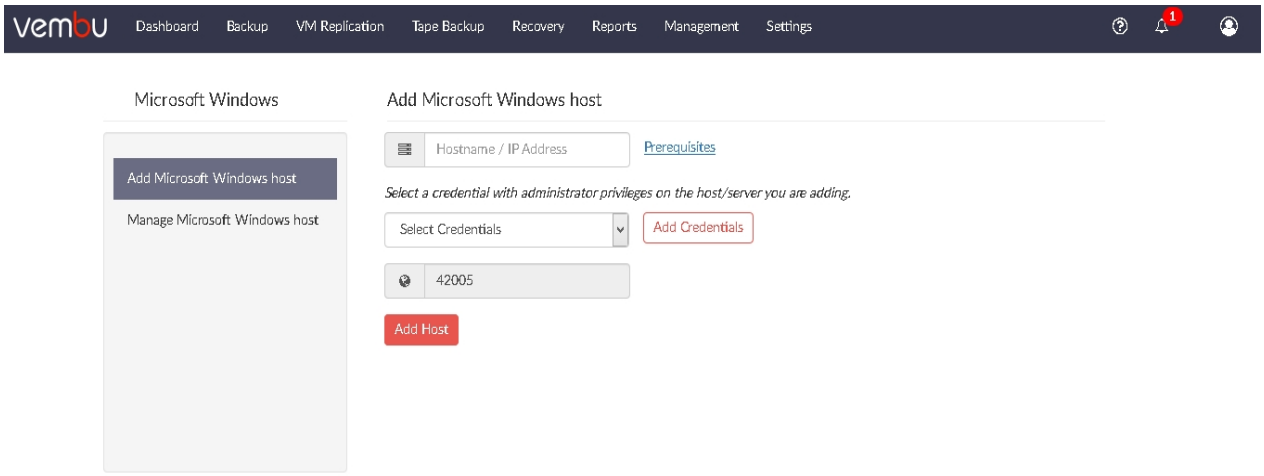
Evaluator's Guide for Windows Servers and Workstations

Adding Microsoft Windows Server

You need to add a Windows Server host or Workstation before you configure a backup job.

Procedure:

- From the **Backup** tab, click **Microsoft Windows**. You must add a Windows Server before you begin configuring the backup schedule.



Step 2: Add Microsoft Windows Server/Workstation server by providing **'Hostname/IP Address** and its login credentials.

Note: You can add as many Windows Server host into the Vembu BDR Server whenever required.

- **Hostname/ IP Address:** Enter the hostname or IP address of the hostname for which you have to proceed with the backup
- **User Name:** Enter the username of the specific host
- **Password:** The password of the host or IP Address
- **42005:** Port used for communication between **Vembu Integration Service** and Vembu BDR Server

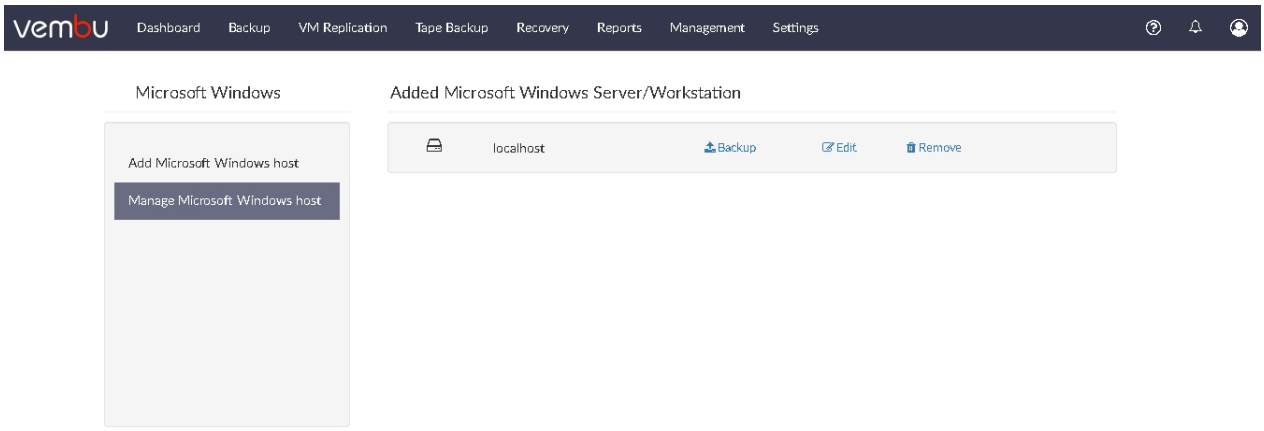
The Hostname can be added using FQDN(Fully qualified domain name) ie., machine_name.domain_name. You can connect your host with Vembu BDR server through following combinations in Hostname/IP Address section:

- **Hostname** - Enter the Hostname alone
- **Hostname@Domain name** - Enter the hostname followed by @ and domainname
- **Domain name/Hostname** - Enter the domain name followed backslash (/) and the hostname
- **192.xxx.xxx.xxx** - Enter only the IP address

Step 3: VembuBDR server communicates with the Microsoft Windows Server using the port that is set to **42005** as default. You can modify this port number as per your port number availability.

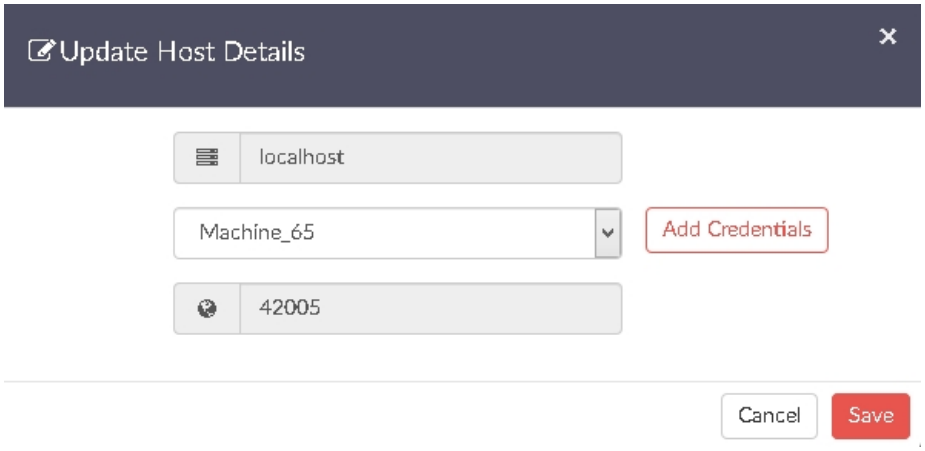
Step 4: Click **Save** once you have provided the credentials.

Note: If you have provided an invalid Hostname/IP address, the following alert message will be displayed "**Unable to connect the remote Windows Machine. Please check network connection settings."**

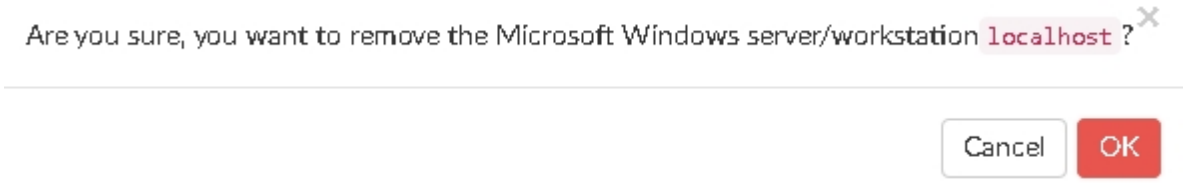


The Following details can be edited in an already added VMware Host

- You can select a different credential or add a new credential



- If you want to remove a particular Windows Server, click the **Remove** option. A pop-up window with the message **"Are you sure, you want to remove the Microsoft Windows server/workstation 192.xxx.xxx.xxx?"** will appear. Click **OK** to delete your Microsoft Windows Server.



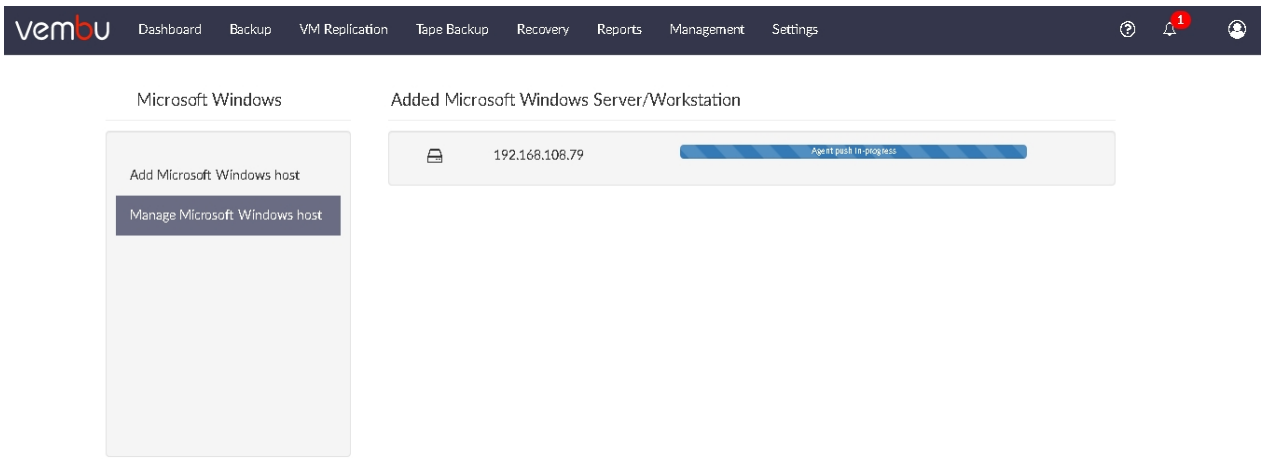
- Vembu BDR server pushes **VIS - Vembu Integration Service** on to the added target machine.
- Vembu Integration Services**:** VIS acts as an agent in the target machine in which the data present in the machine has to be backed up. Vembu Integration Service reads the data from the added machine and lists the disks and drives in the Vembu BDR server for backup.
- If there is any problem while connecting **Vembu Integration Services**, read KB article

Evaluator's Guide for Windows Servers and Workstations

Installing Vembu ImageBackup Driver

Vembu ImageBackup driver is installed to read and fetch information regarding the disks and volumes in the added target machine. It tracks the changes that has happened between the backup schedules. To track the changes, the driver creates a file named **bitmap.dat** in the backup volumes.

- You will be requested to install **Vembu ImageBackup driver** to list the disks and drives for configuring the backup job.
- Once the link is clicked, the driver installation will start automatically. After the driver is installed successfully, the target machine will be rebooted to update the driver installed and for the creation of the registry.
- After the machine restarts, login to the added target machine for the configured registry details to be applied in the machine so that Vembu BDR server will list the disks and volumes of the target machine.
- Log in to Vembu BDR server and proceed to configure the backup job. Navigate and click **Backup** tab and choose **Microsoft Windows**
- Click the **Backup** option near the respective Windows server.



Evaluator's Guide for Windows Servers and Workstations

Setup Vembu ImageBackup Job

Click **Backup** corresponding to the added server in the **List of Added Servers** and you will be taken to backup configuration page.

There are 5 major steps involved in configuring Vembu Image Backup. They are listed below:

- Choose disk/drive(s)
- Guest Processing
- Configure Schedule
- Settings
- Review Configurations

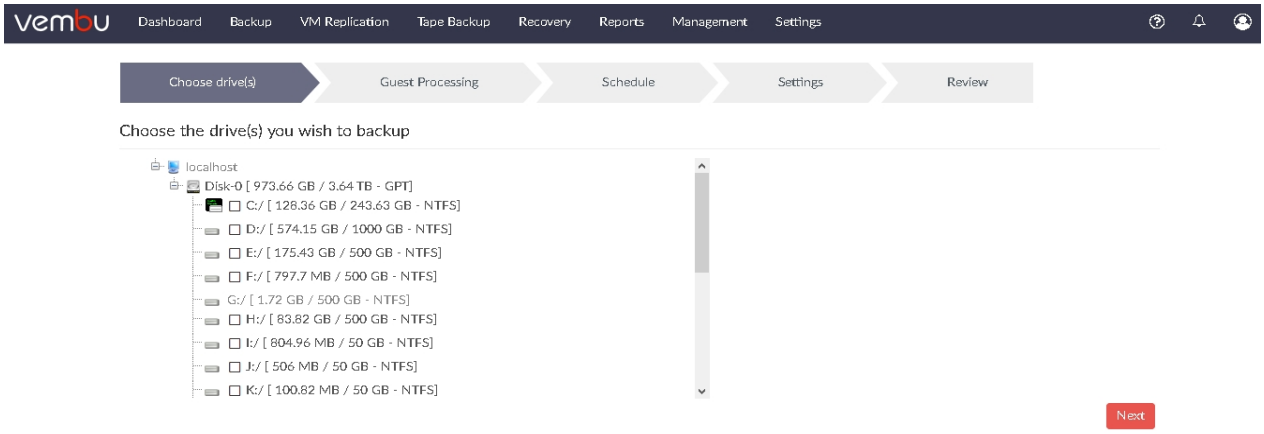
Evaluator's Guide for Windows Servers and Workstations

Step 1: Choose Drive(s)

- From the selected host, disks and drives will be displayed with its **available space, full**

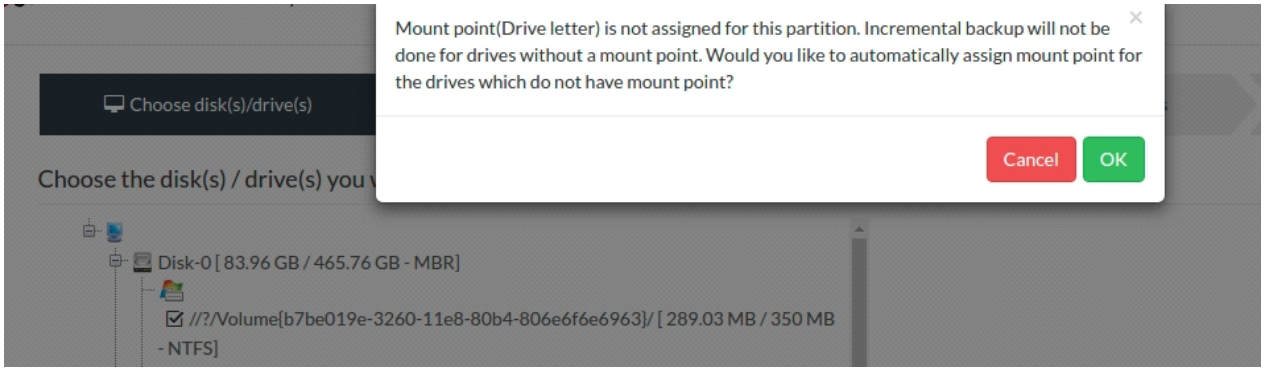
space and the type of disk. You can select the drives from the disk to backup. Click **Next** to proceed with the backup process.

- The drives(Volumes) that are already backed up will be greyed out and is not eligible for backup.
- If you have chosen drives from different disks for backup, the backup will progress in ascending order of disks. **For Example:** In a 3 disk setup, the backup progress will be in following order: Drives from Disk 0 will be backed up first, followed by drives from Disk 1 which is then concluded by drives from Disk 2.
- You can choose the drives to be backed up by selecting the check boxes. Once done selecting, click **Next** to proceed with the backup process.



Mount Point

- Vembu BDR server assigns a mount point to the volumes that do not have volume **Mount point or drive letter** assigned. This is required as the volume without mount point cannot be scheduled for incremental backup. The Driver letter will be applied automatically on refreshing the page



Note:

- Disk image backup is supported for single digit disks(Disk 0, Disk 1,...Disk 9) and is not supported for two digit-disks, for example, Disk10, Disk11 and so on
- It is recommended to include boot partition (System Reserved) in the backup to make the backed up image bootable on restore
- The drives that are already backed up cannot be backed up further. It can be edited through Edit backup jobs
- The disk/volume cannot be configured for the backup process due to any of the below mentioned reasons:

1) If the volume has already been configured for backup.
2) Disk is ReFS/FAT/exFAT formatted.
3) If the volume is compressed using NTFS Compression.
4) If the Volume is NTFS folder mounted.

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).
- 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.

Enabling Application Aware processing option, gives you two choices:

- **Require successful application processing:** Choosing this option lets Vembu BDR track the application consistency and triggers the backup process, only when all the VSS writers 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.

Note: If any applications are running and you have selected "Ignore application processing failures" option, then the application in the backup might not be consistent while restoring.

Truncate the transaction logs:

- Enabling this option lets Vembu BDR truncate the Exchange Server logs before initiating the backup process. It purges and commits log files along with the .edb files. This avoids the disk space consumed by the application transaction logs.

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

VMware Guest Credentials:

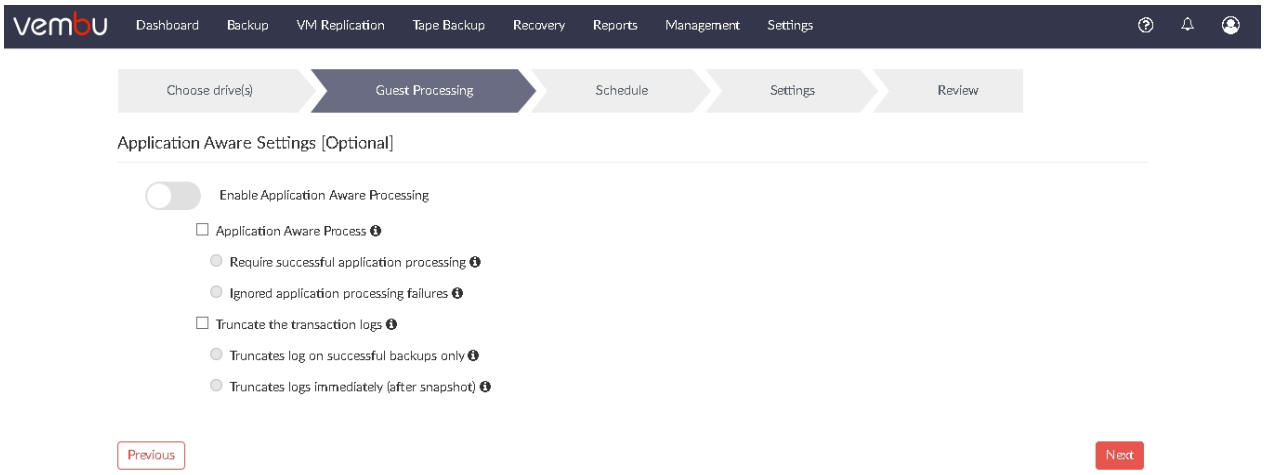
- To perform Application Aware Image processing, login credentials of guest machines are required. The writer status will be checked using the Guest tool. The details of the writer's status will be fetched for the backup process.

- Three steps are involved in this process.
  - Select the desired Server and select the virtual machine to which you wish to enable Application Aware backups.
  - Provide the login credentials of the virtual machine and save it.
  - Now scheduling backup will have Application Aware options enabled.

Note: You must select at least a VM to enable Application Aware.

- You can add a new Guest credential using the **Add New VMware Guest Credential** option. If you wish to clear out all the configured Guest Credential Settings, select the **Clear all the VMware Guest Credential Settings.** Click **Next** to proceed configuring your backup schedule.

Note: Application Aware backup is not supported for 32 bit Guest OS



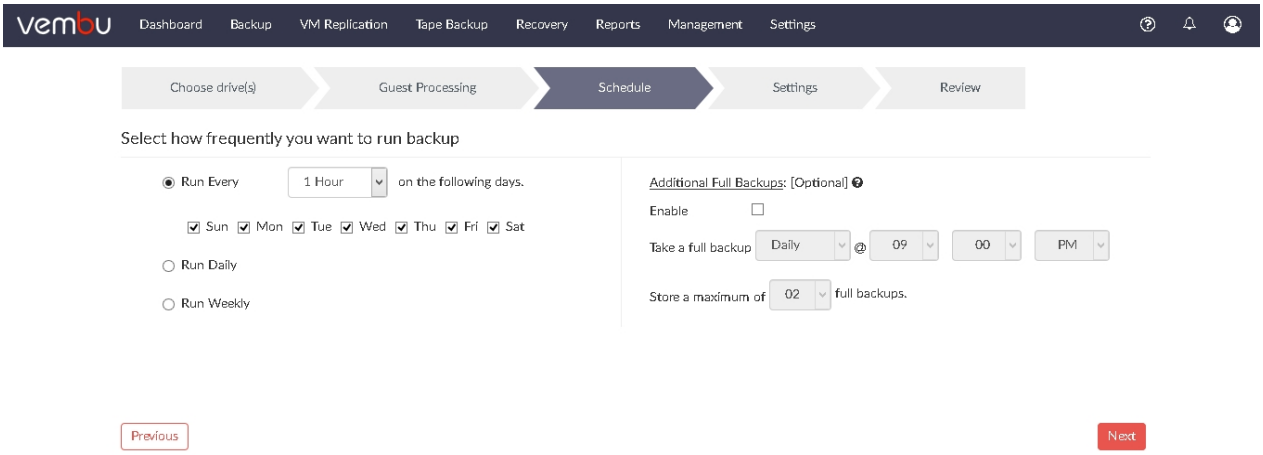
Note: It is recommended to enable the truncate logs option. Since the continuous growing of transactional logs leads to rapid consumption of storage space and the database modifications seems difficult when more log data is in the disk space on your drive.

Evaluator's Guide for Windows Servers and Workstations

Step 3: Configure Scheduling

- The Configure Scheduling option defines the frequency of your Disk Image 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 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 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.

Configuring Additional Full Backup:

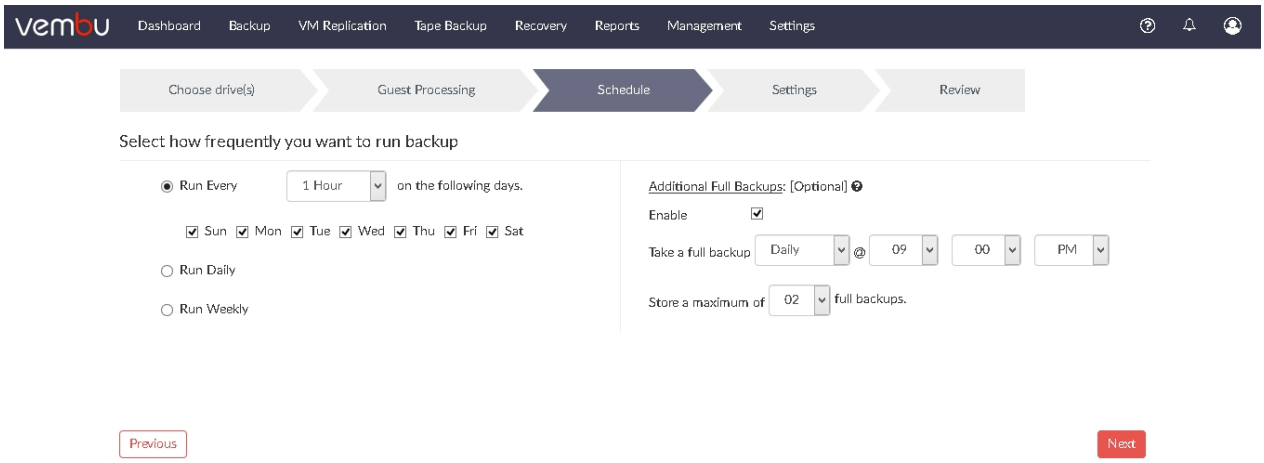
- Select the **Enable** Additional Full Backups option. For Run Every, Run Daily backups, the Additional Full Backup settings will allow you to configure Daily/Weekly/Monthly Additional Full Backups. If you have configured your backup to Run Weekly, then you can select Monthly Additional Full Backup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

You can also 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.

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



- Once done configuring the backup schedule, click **Next** to configure retention policies for your backup.

Evaluator's Guide for Windows Servers and Workstations

Step 4: Settings

In the Settings page, you can configure the following:

- Retention Policies
- Storage Repository
- Backup Encryption

All these three settings are **optional** with each option set to a default action. For example:

- Not enabling retention will result in forever incremental backups
- By default, the storage pool configured for the backup job is the default repository(Default_Repo)
- The backup data stored in your repository will be encrypted using the system generated password.

Configure Retention Policy:

- 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.

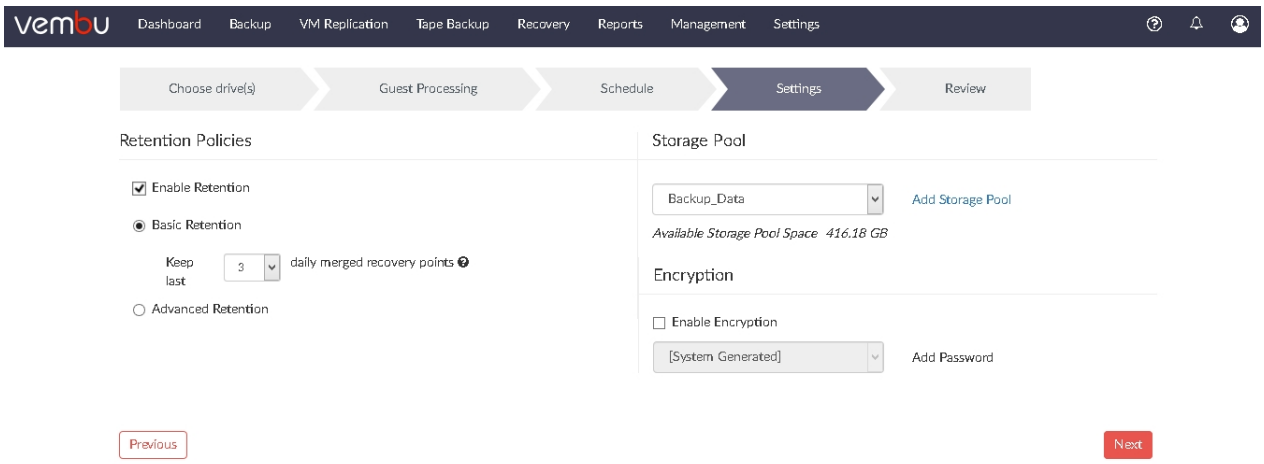
Working:

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

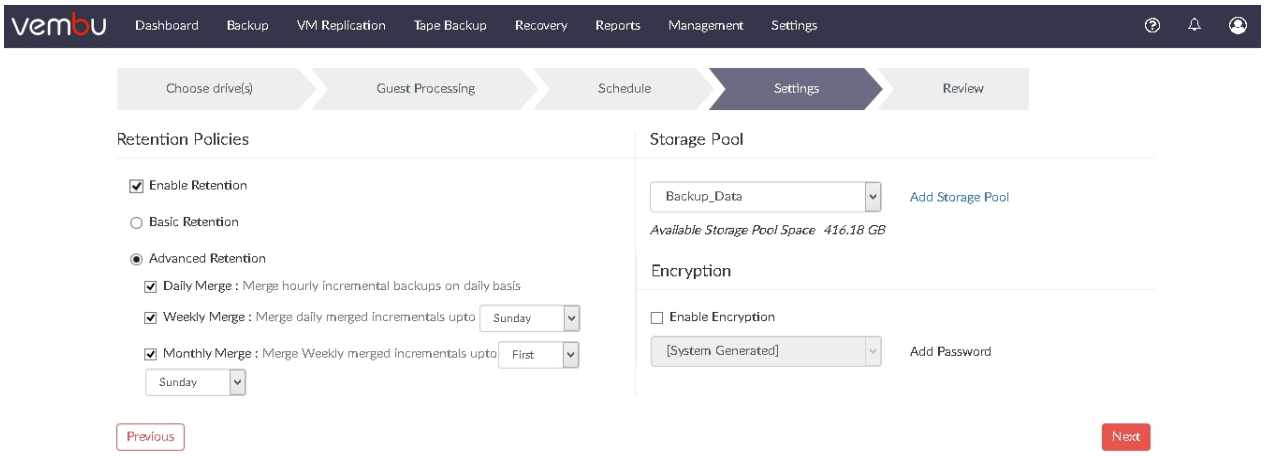
- If you have selected Daily, Weekly and Monthly merge, each merge process will get initiated on the user-specified day.
- If you have configured Weekly merge on Sunday, after the first successful incremental on Sunday all the daily merge backups from last Monday will be merged together and marked as 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

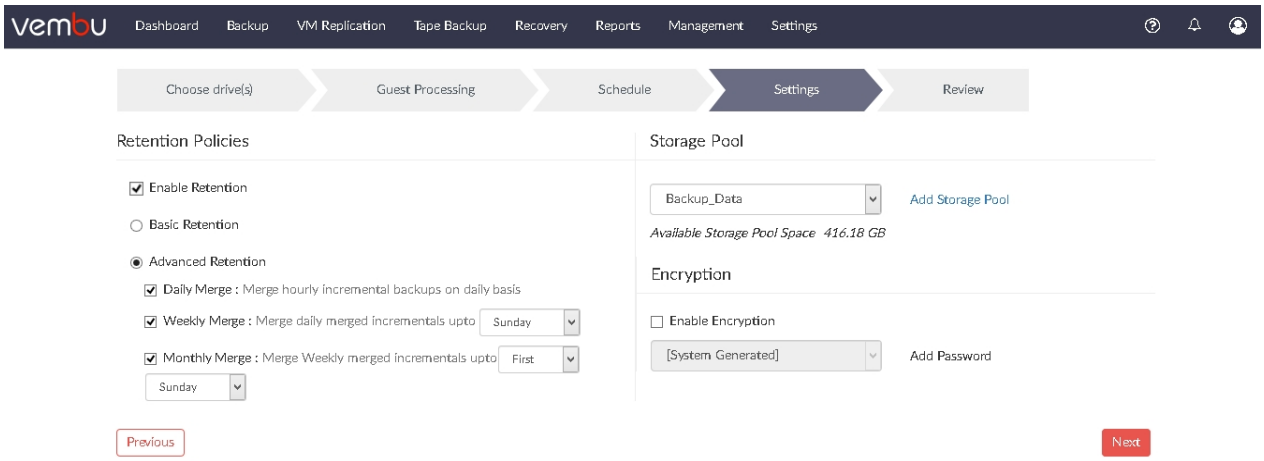
- Storage Pools are used to aggregate the space available from different volumes and utilize them as a single storage for specific backups.
- The backup storage that is configured during BDR server installation will act as a **Default Repository**.

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

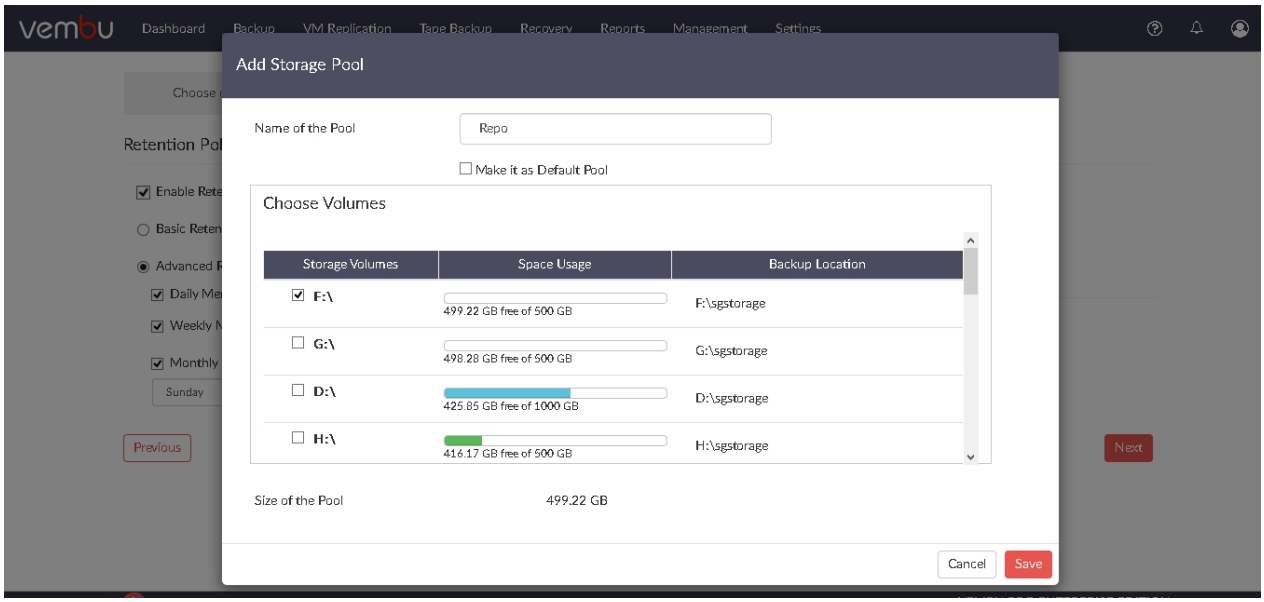
- **Add Storage Pool:** To create a new storage pool, click the **Add Storage Pool** option. Give a Storage Pool name and select any set of volumes from the list of available Storage Volumes. Enter the storage pool name, this name will be listed in the available storage pools for the backups

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, 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.

- 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. Choose the password and click **Next**.

Note: By default, Vembu 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.

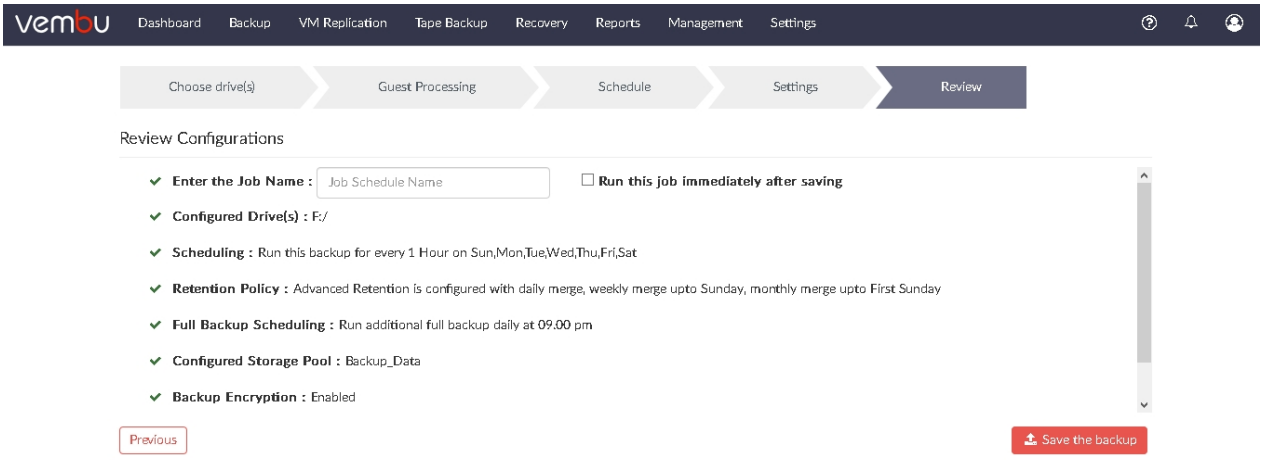
- Once you have completed configuring the Encryption Password, Click **Save**. Click the **Clear** option if you want to clear out the Password and Encryption hint.

Note: By default, Encryption Setting will be disabled.

Step 5: Review Configurations

- The last step in your backup process 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 drives/ disks**- The Drives/Disks 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:

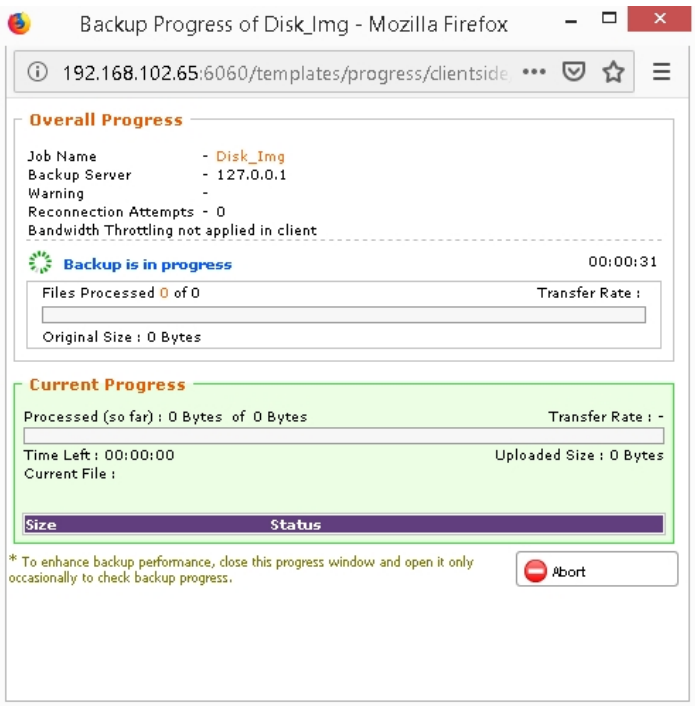
Progress Details:

- 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.

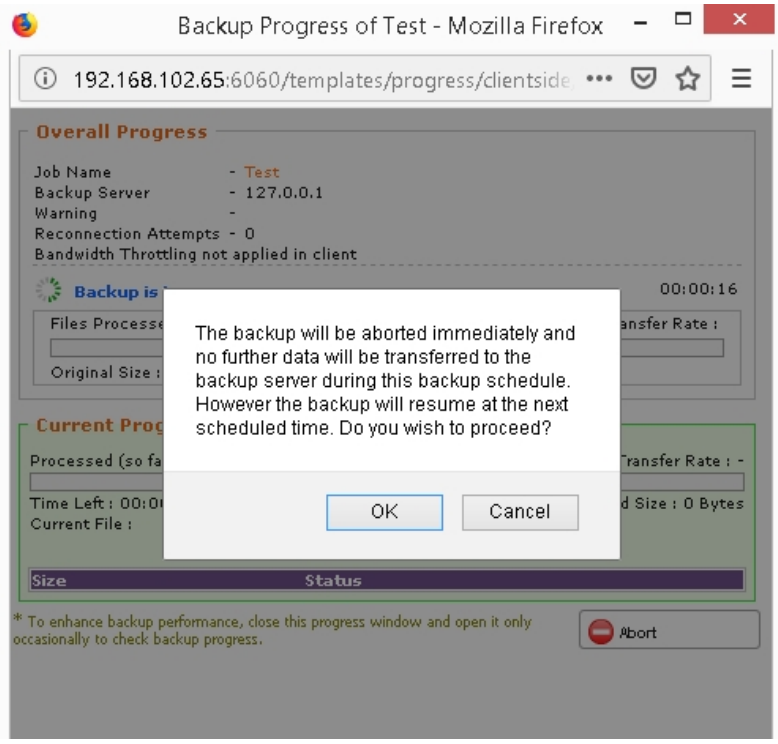
- **Job Name** - Name of your backup job entered
- **Backup Server** - The backup server to which the backup is currently processing
- **Warning** - Warning for the backup job if any
- **Reconnection Attempts -** The count of the times Vembu client attempted to reconnect to the backup server
- **Bandwidth 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 listed 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 pop up as shown below. Click **OK** to Abort your

backup

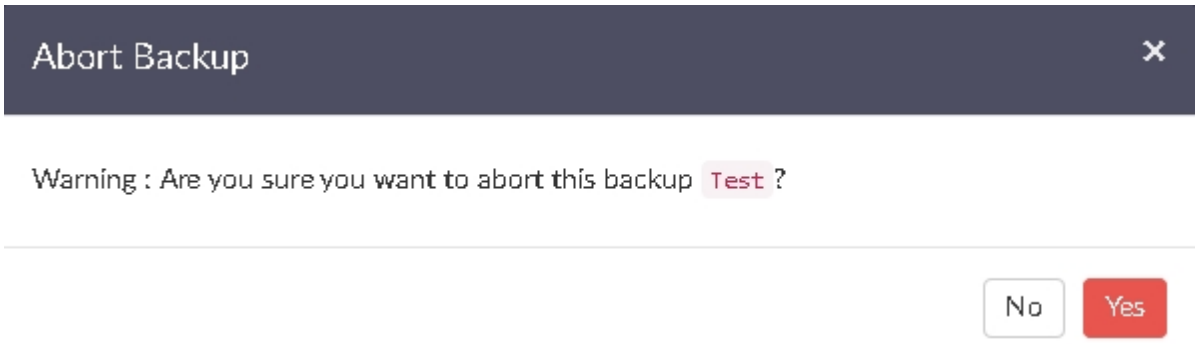
Thus, backup progress is witnessed and can be verified once it is completed successfully.



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.



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

Evaluator's Guide for Windows Servers and Workstations

Evaluation Case:

There are 4 evaluation cases detailed below that will guide you through the various features and configuration options available in the Vembu ImageBackup. By the end of all the cases, you will have used every option available in the product and created backups that suit diverse use cases.

During the evaluation scenarios, you will get familiar with the product using the feature overview, procedure, and guidelines provided.

- Case 1
- Case 2
- Case 3
- Case 4

Evaluator's Guide for Windows Servers and Workstations

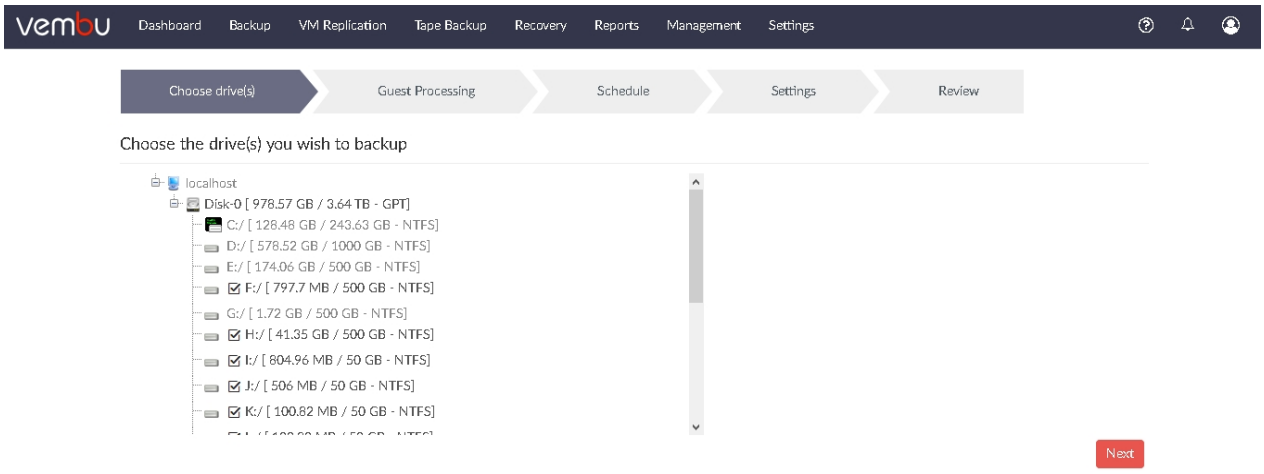
Case 1

- Configure a job to backup all the drives in the added Windows Server
- Enable Application Aware processing and truncate log on successful backups only
- Schedule the backup job to run every 1 hour on all days except Sunday
- Keep last 5 daily merged recovery points
- Run the backup job immediately after configuration

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

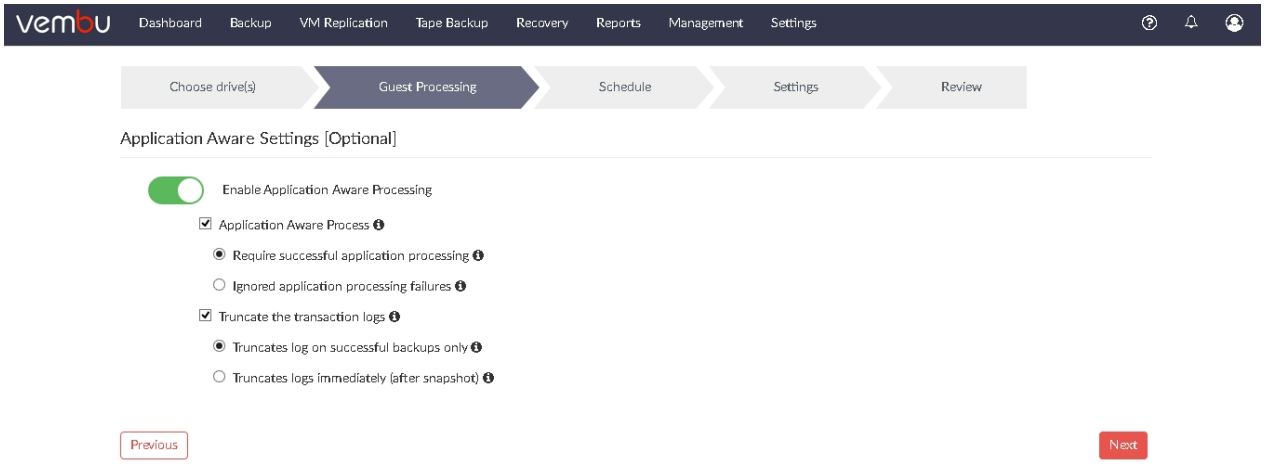
Step 1: Choose the drive(s) for backup

- Since the scenario involves backing up the entire drives that are added in the windows server, select the check box of all drives. Click **Next** to proceed with the backup schedule.



Step 2: Configure Guest Processing

- Enable **Application Aware Settings** option. When you enable the option it will match the requirement of the evaluation case (Default Action). Click **Next** to proceed with the backup schedule.

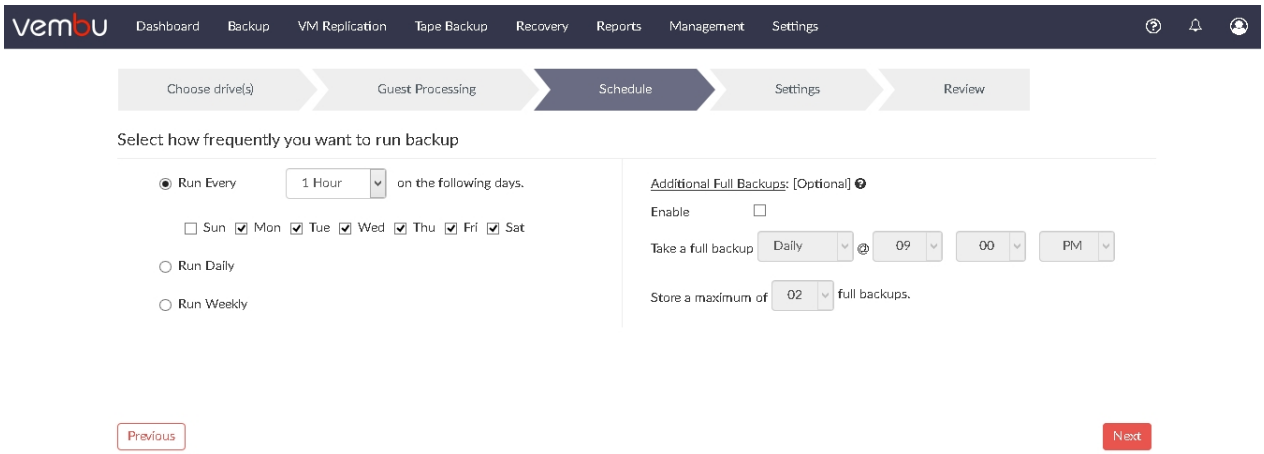


Step 3: Configure the backup schedule

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 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 chose **1 Hour** as the time frequency for the backup. By default all the days will be selected, ignore Sunday by removing the tick mark from the checkbox. Click **Next** to proceed further in the backup configuration.



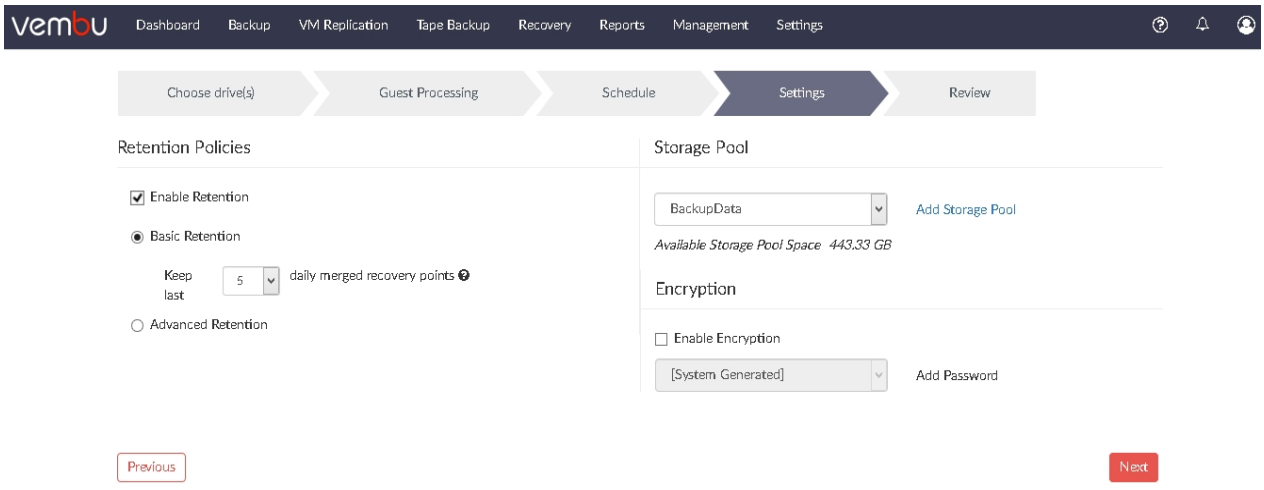
Step 4: Configure Retention Policy

While configuring the Retention Policies for your 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.** Select the **Enable Retention** checkbox and select **Basic Retention** (Default Action). The default value chosen for the daily merged recovery points is 3, change it to **5**. Click **Next** to proceed further in the backup configuration.

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



Step 5: Review Configurations

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

- Configured Drive(s)
- Backup Schedule
- Application Aware Settings
- Retention Policies
- Configured Storage Pool

- Encryption Settings

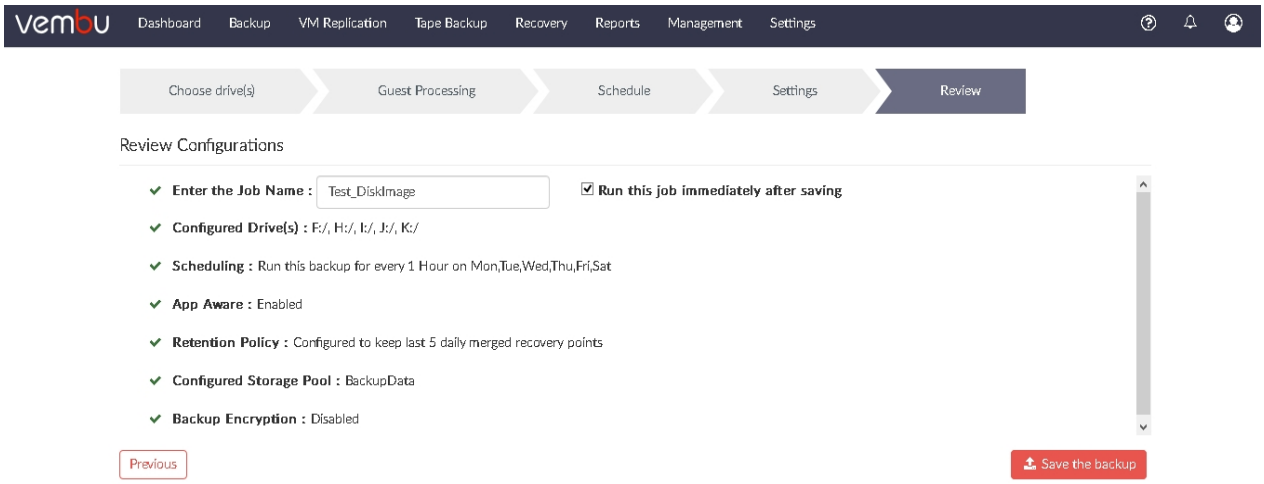
- Enter a backup job name.

Note:

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

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

- The evaluation case requires to "**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.
- Once done reviewing your selections, click **Save the backup** and **OK** from the pop-up window to complete the configuration.



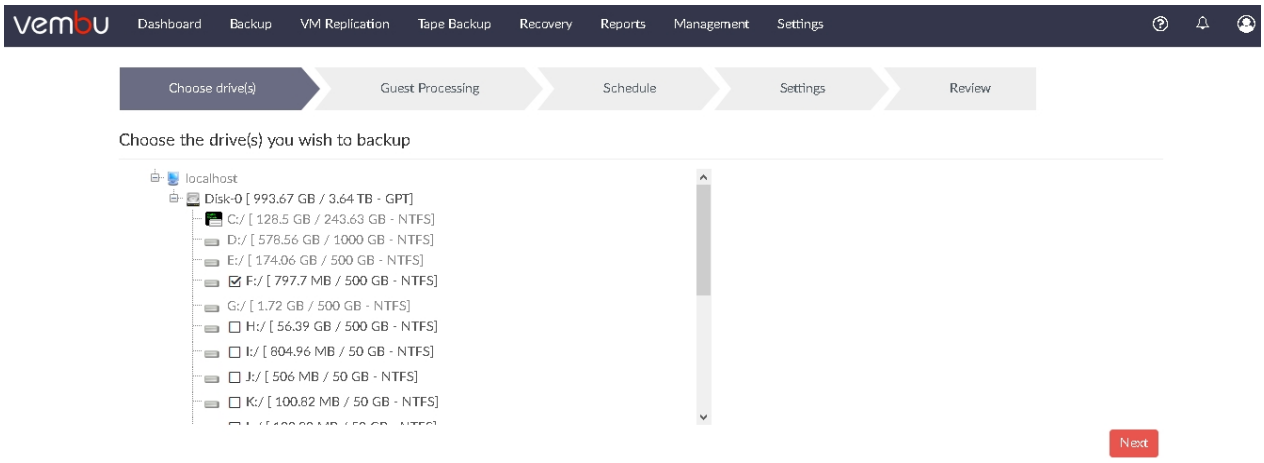
Evaluator's Guide for Windows Servers and Workstations

Case 2

- Configure a job to backup only particular drives
- Enable Application Aware processing and truncate logs immediately for the backup
- 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
- Change the storage pool
- Encrypt the backup job with System Generated password

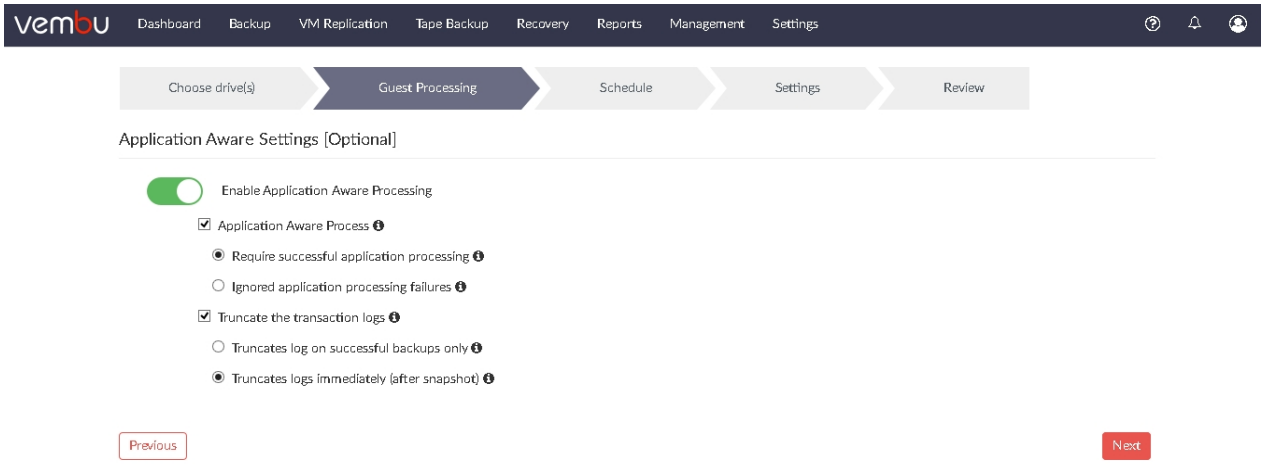
Step 1: Choose the drive(s) you wish to backup

- As per the evaluation case, only certain drives are to be backed up from host. Select the drives required for the backup and click **Next** to proceed with the backup schedule.



Step 2: Configure Guest Processing

- The next step is to configure Application Aware Settings. Enable the **Application Aware Processing** option. Select the **Require successful application processing** option and **Truncate logs immediately** option. Click **Next** to proceed 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**.

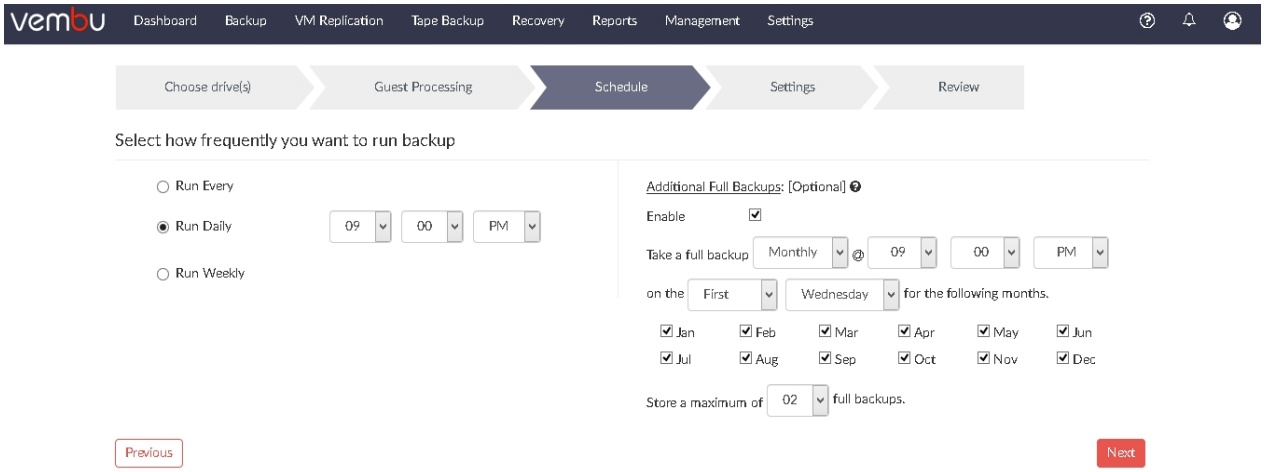
Note: By default the time selected for Run Daily will be 09:00 PM

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



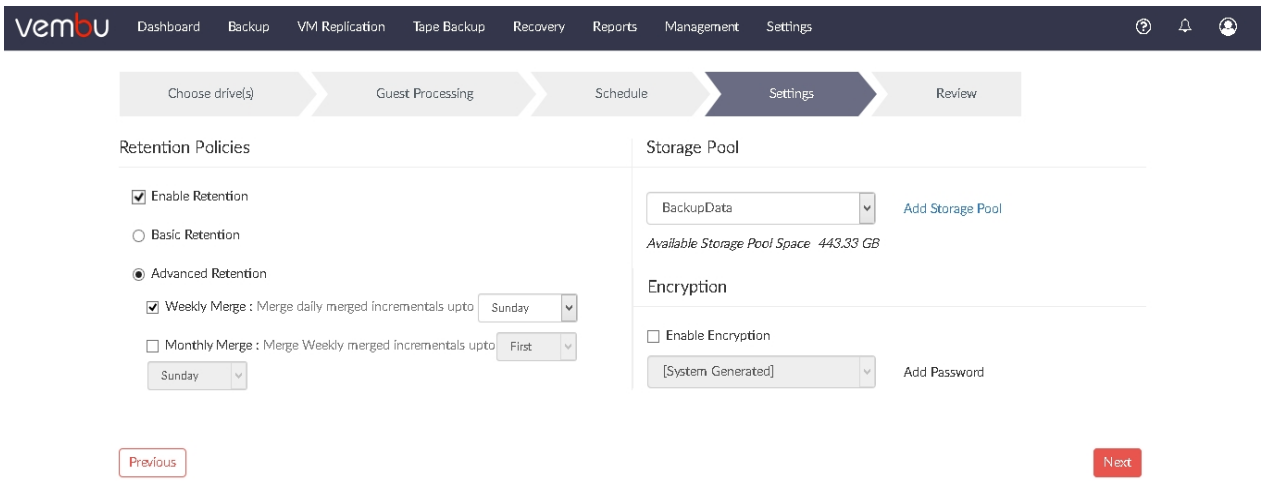
Step 4: Configure retention policy

- The next step in the backup process is to configure retention settings. Select the **Enable Retention** option and choose **Advanced Retention** as this case involves merge of daily merged recovery points.

Since the backup scheduled 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

- Your restore points have to merge every Sunday according to the given scenario. Select **Weekly Merge**. Choose **Sunday** from the list of days in a week for the merge process to occur.



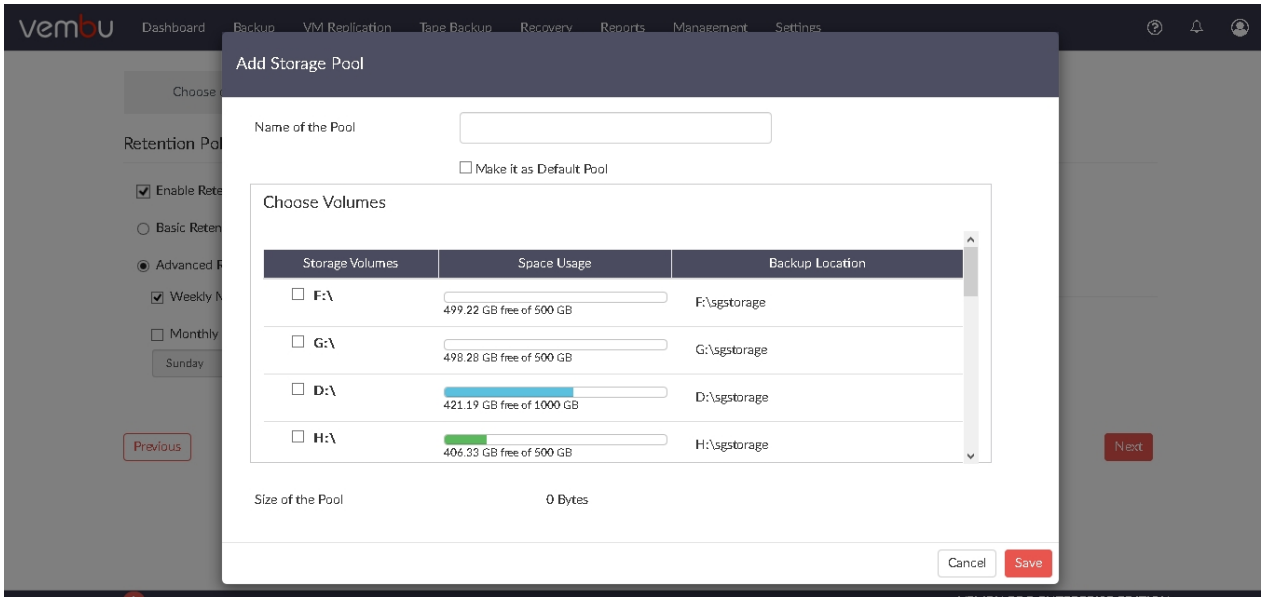
Note: By default, retention is not enabled and incremental backups will run forever.

Step 5: Configure Storage Repository

- The next step is to 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: Only [a-z][A-Z][0-9][- _] characters are allowed in the Storage Pool Name.

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

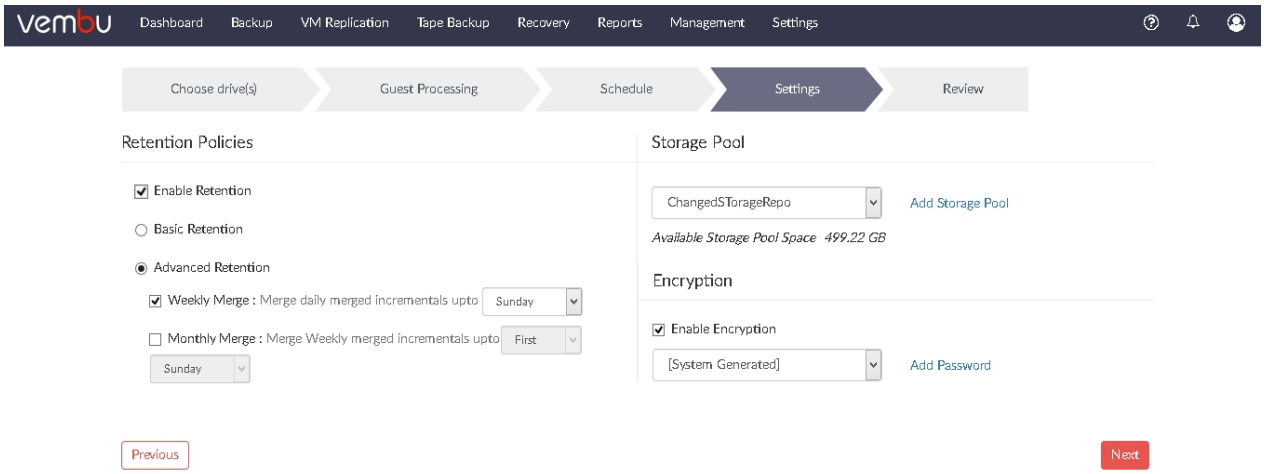


Step 6: Configure Encryption

- Backups configured from the Vembu BDR server can be encrypted with a user-defined password.
- Select the **Enable Encryption** option. By default **System Generated** option will be selected for your backup job.

System Generated Password:

- The selected files and folders will be encrypted using AES algorithm with a 256-bit encryption key automatically generated by Vembu BDR Server. Click **Next** to proceed with the backup schedule.



Note: By default, Vembu BDR 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

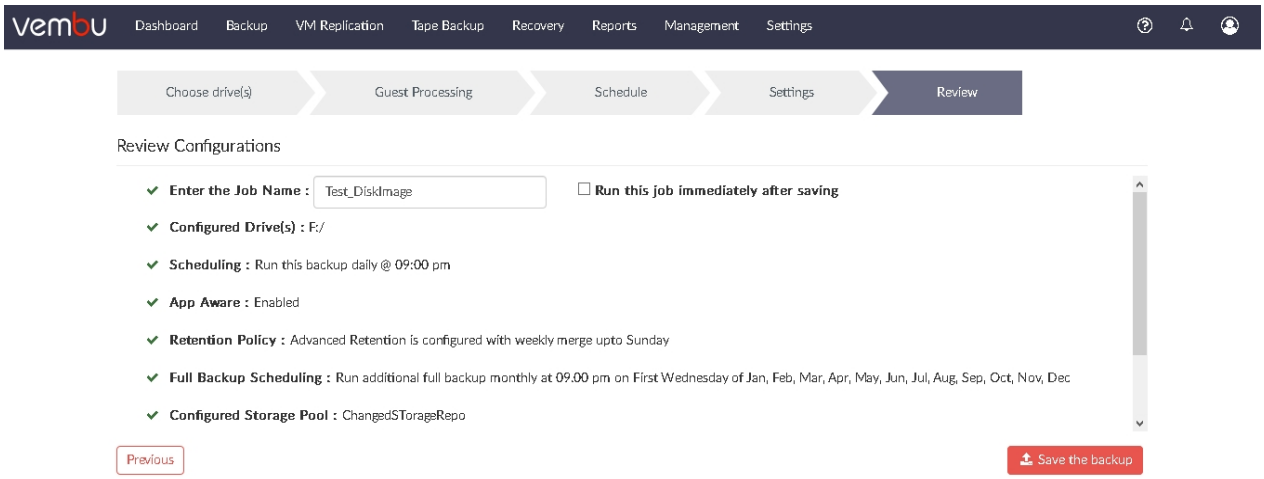
- Enter a backup schedule name. Vembu BDR server supports creating multiple backup schedules each with its own configuration. The backup schedule name will uniquely identify the backup. While restoring your backup data, you need to choose the data to be restored using its schedule name.
- Review the following
    - Drive(s) Configured
    - Scheduling Details
    - Application Aware Process Settings
    - Retention Settings
    - Full Backup Scheduling
    - 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.

- Once done reviewing your selections, click **Save the backup** and **OK** from the pop-up window to complete the configuration.



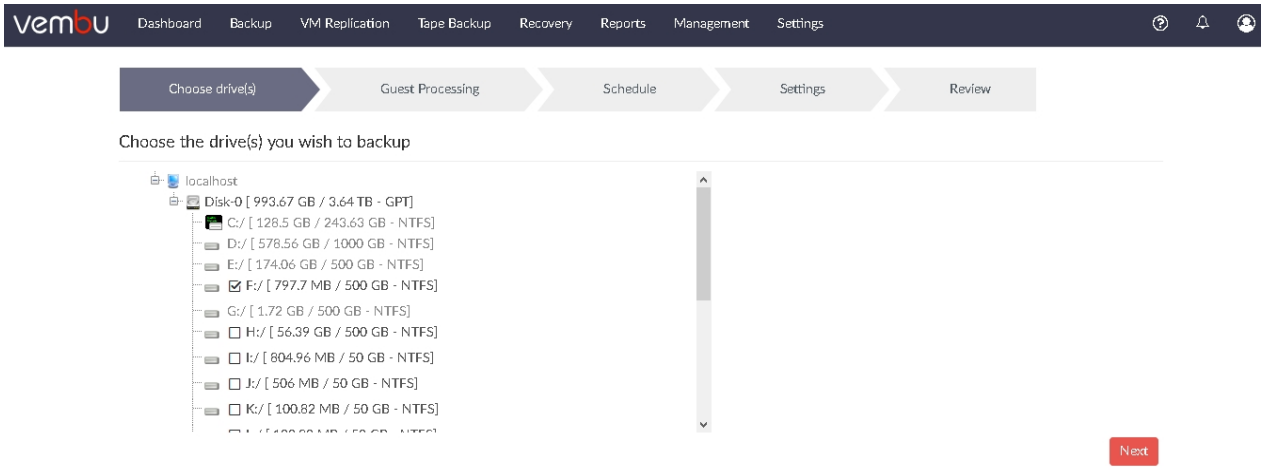
Evaluator's Guide for Windows Servers and Workstations

Case 3

- Configure a job to backup specific disks/drives
- Enable Application Aware processing settings, ignore application processing failures and truncate logs immediately for the backup
- Run the backup job on Monday of every week at 09:00 PM
- Take Additional Full Backup on the Last Sunday of every month and store a maximum of 3 Additional Full Backup
- Disable Retention Policy
- Add a new storage pool for the backup job and make it the default pool
- Add a new password to encrypt the backup

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

- Select the specific disk/drive(s) that is to be backed up and click Next to proceed with the backup schedule.

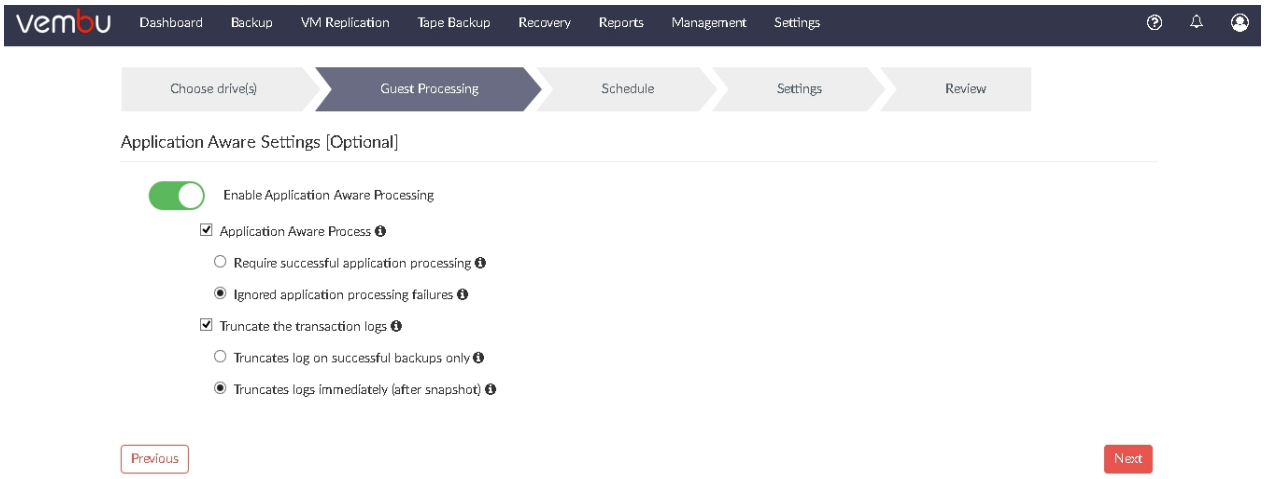


Step 2: Configure Guest Processing

- 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

machine.

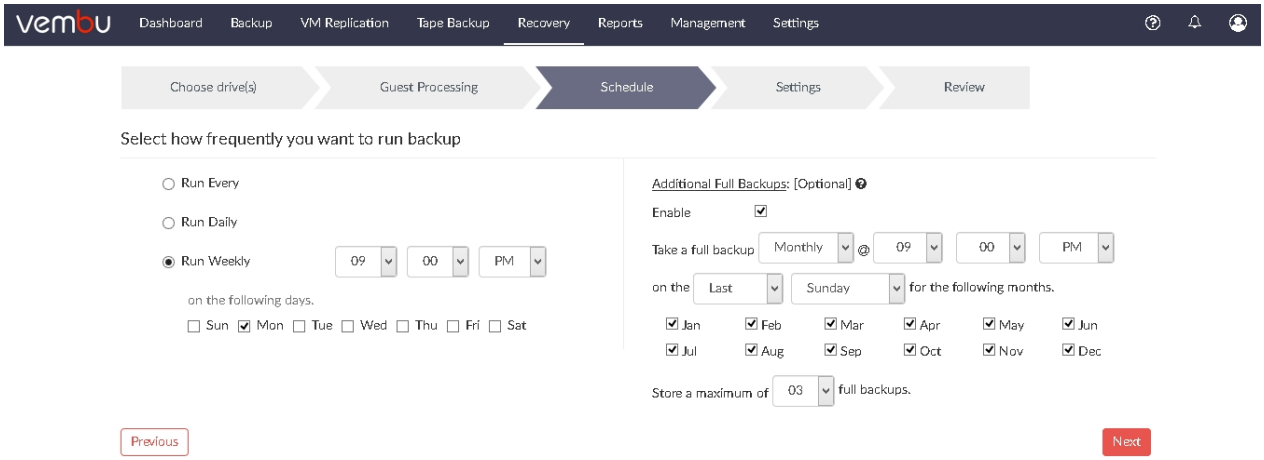
- Enable **Application Aware Processing** option and select the **Ignored application processing failures** option. When Ignore Successful Application Processing is selected Vembu BDR will trigger the backup job when it is scheduled, despite the success/failure of application processed. It will not process the Application VSS writers and ignores the writer's status. From the truncate transaction logs section, select **Truncate logs immediately** option. Click **Next** to proceed with the backup schedule.



Step 3: Configure the backup schedule

- The evaluation case involves to schedule your backup **Every Week of Monday** by **09:00PM** select **Run Weekly** option. Select **Monday** and set the time at **09:00 PM**.
- Enable **Additional Full Backups**. In this case, an additional full backup must run on the Last Sunday every month. Select the frequency of Additional Full Backup. Choose when the full backup has to run every month. There are two options that help you configure this:
  - The first drop down has the which day of the month the backup has to run by allowing you to choose from **First**, **Second**, **Third**, **Fourth** and **Last**. Select **Last**
  - The second drop down lists the days of the week. Choose **Sunday**

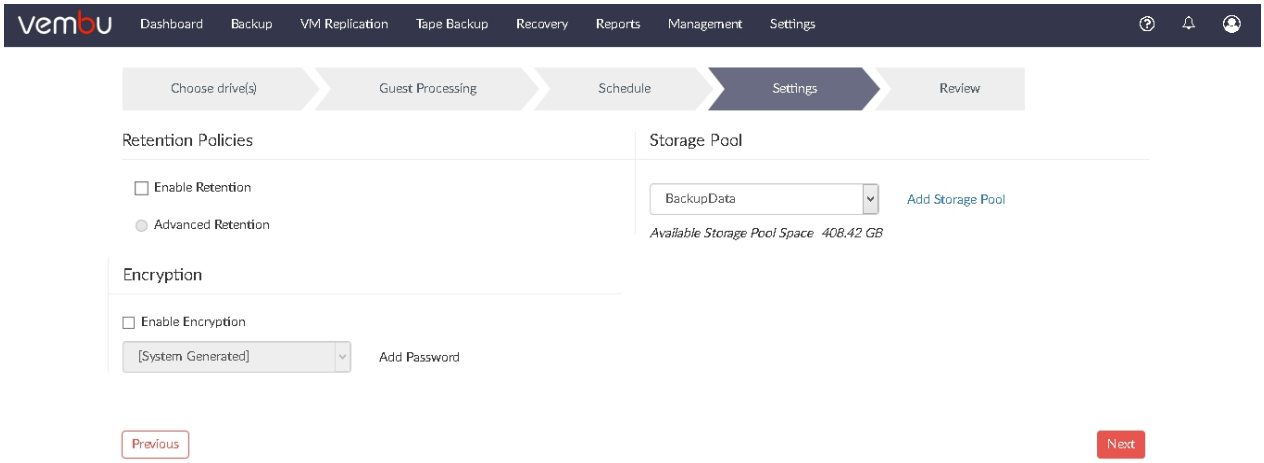
- You have to retain only a maximum of 3 additional full backups. Select the drop down box next to **Store a maximum of** and select **3**. Click **Next** to proceed with the backup schedule.



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 organizations backup policy.
- Since this evaluation case requires you to disable Retention policy, **do not enable retention**.

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

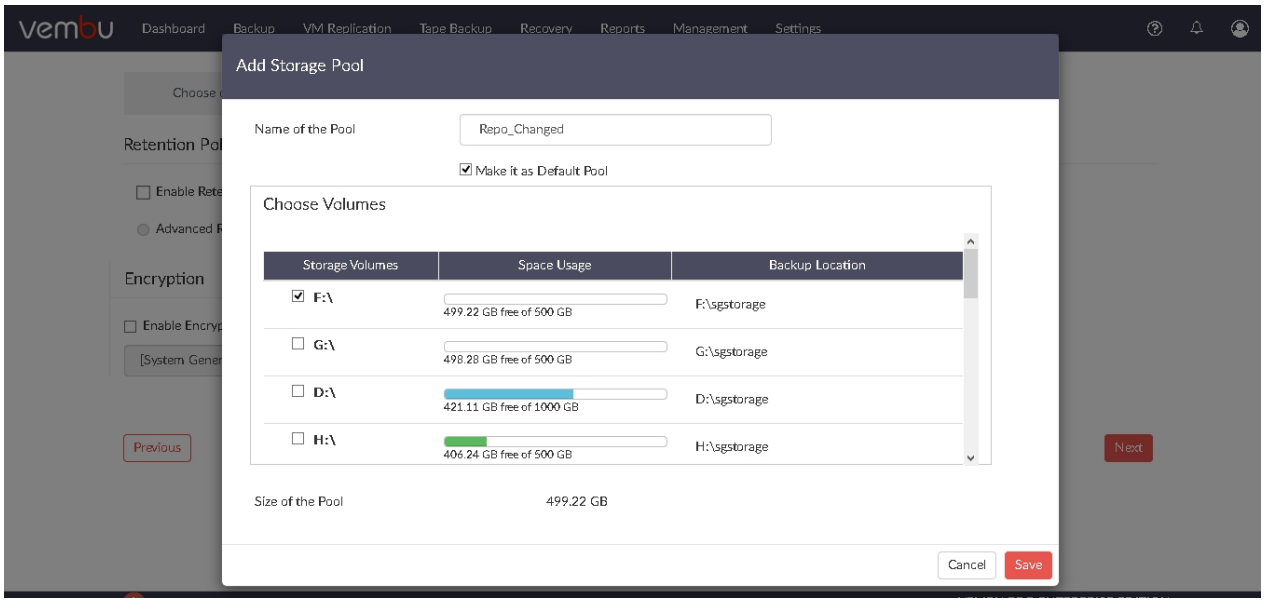


Step 5: Configure Storage Repository

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

Note: Only [a-z][A-Z][0-9][- _] characters are allowed in the Storage Pool Name.

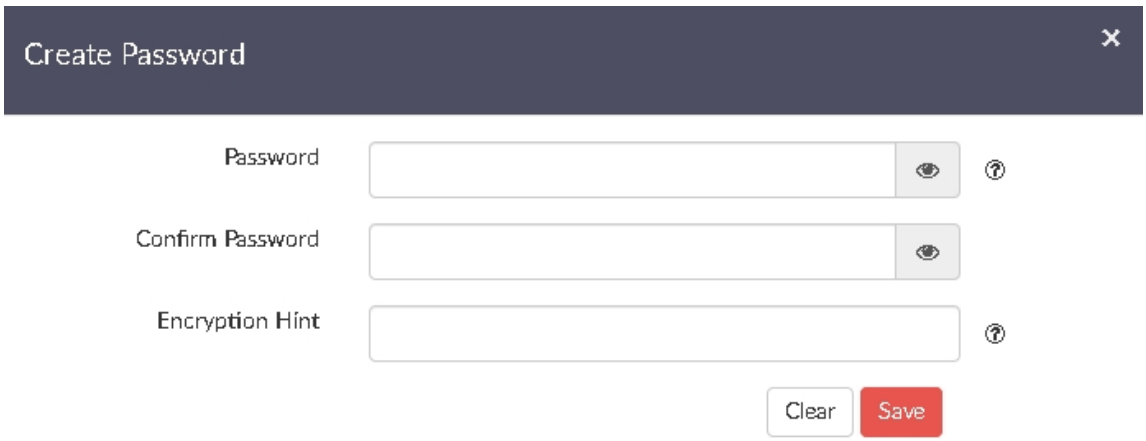
Note: It is not recommended to choose OS Partition as Storage repository.



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

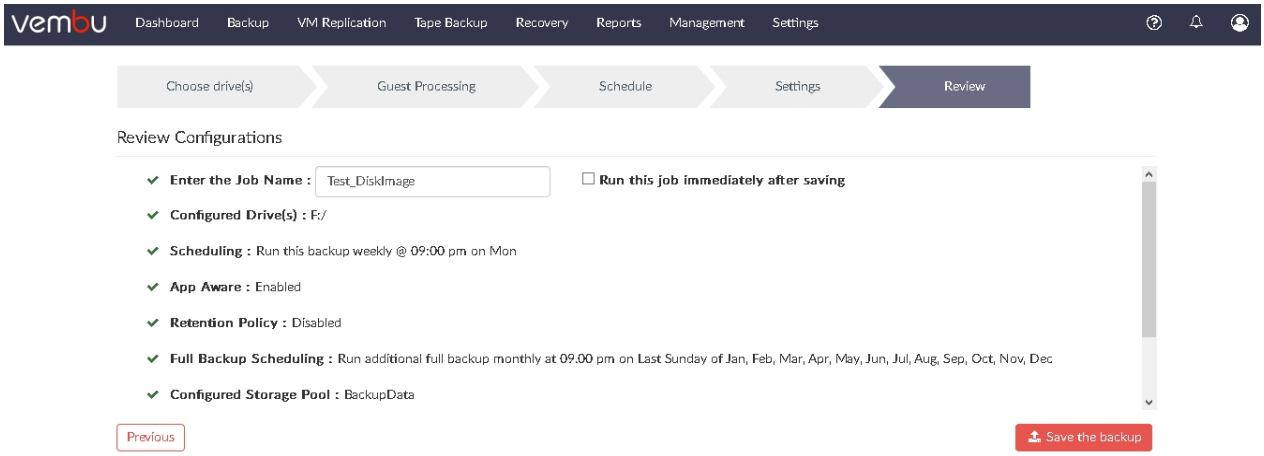
- The last step in your backup configuration is to review the configurations you have selected. Enter a Backup Schedule Name. Vembu BDR Server supports creating multiple backup schedules each with its own configuration. The backup schedule name will uniquely identify the backup. While restoring your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

Note:

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

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

- Click **Save the backup** and click **OK** from pop-up window to begin the backup.



Evaluator's Guide for Windows Servers and Workstations

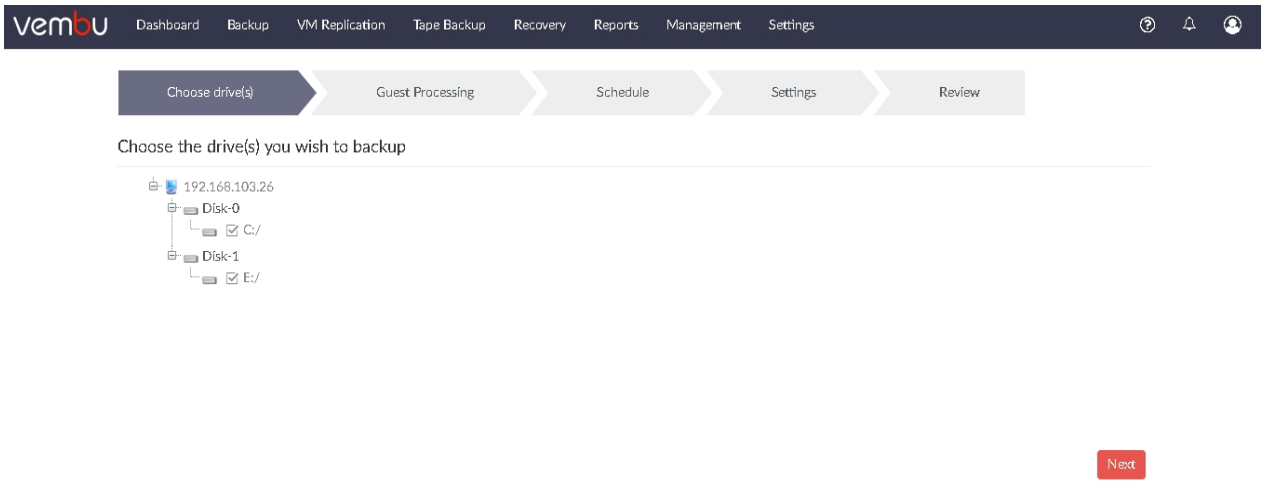
Case 4

- Edit the backup job
- Turn off Application Aware Settings
- Change the backup schedule to Run Weekly on Monday 09:00 PM
- Change the maximum number of full backups to be retained to 7 and run the Additional Full Backup after saving the configuration
- Enable Retention and configure Advanced Retention
- Run the backup job immediately after saving the configuration.

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

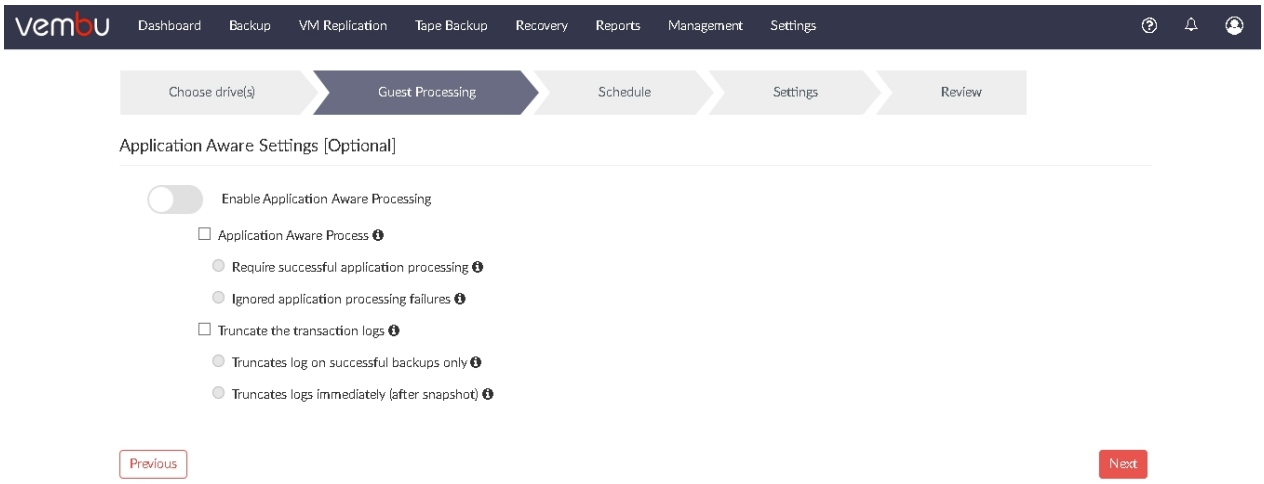
Step 1: Editing the backup schedule

- From the List All Jobs page, click the **More** option and select **Edit** option.
- The list of backed up Drives under disks are displayed. Click **Next** to proceed.



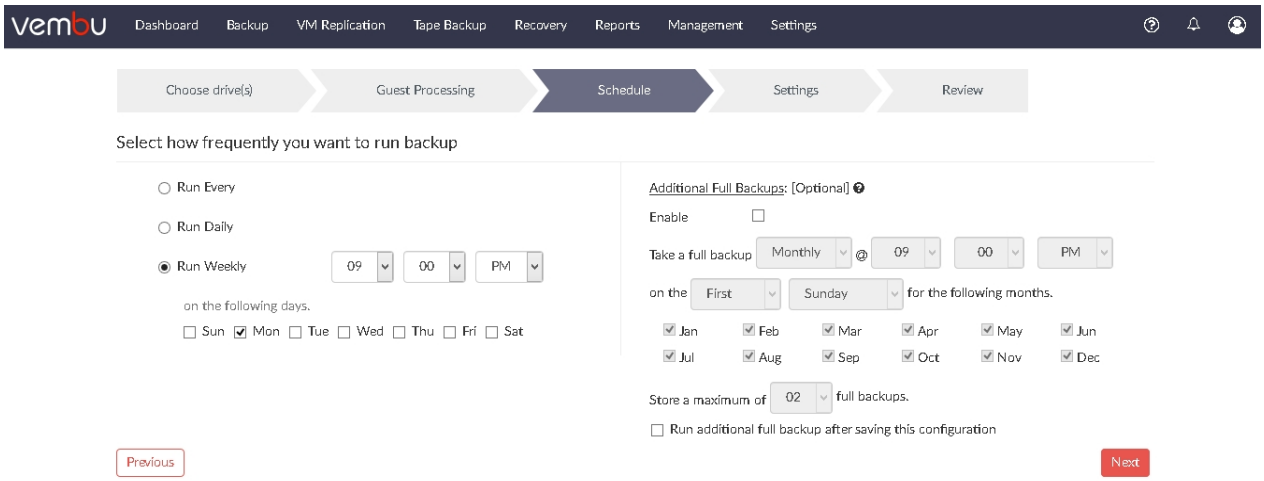
Step 2: Turn Off Application Aware Settings

- The evaluation case involves disabling the Application Aware Settings, disable the **Application Aware Process** Check-box.
- Click **Next** to proceed editing the backup schedule.



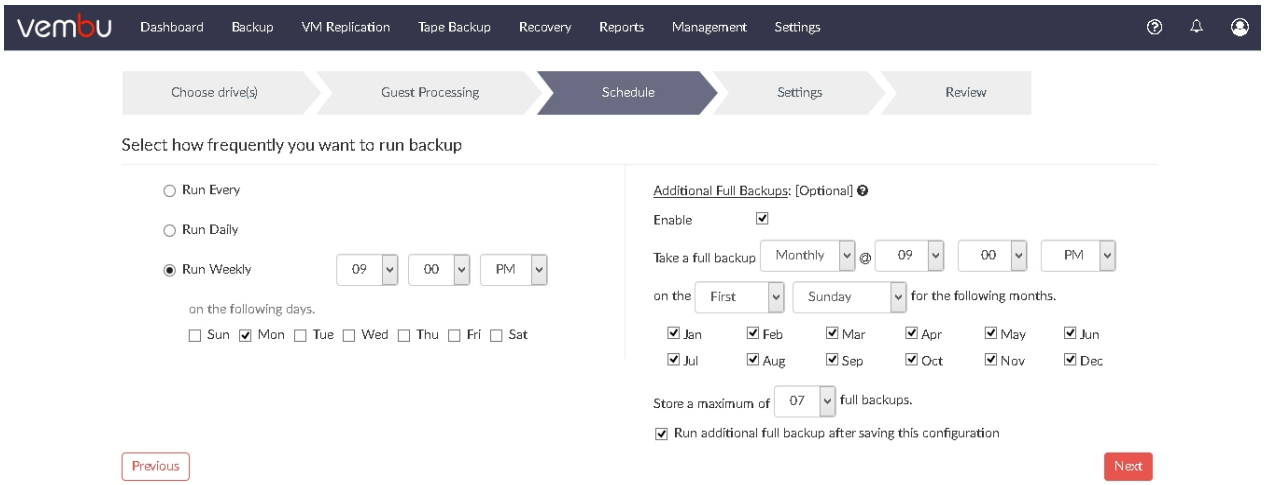
Step 3: Edit the Backup Schedule

- The evaluation case involves to run the backup **Run 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.



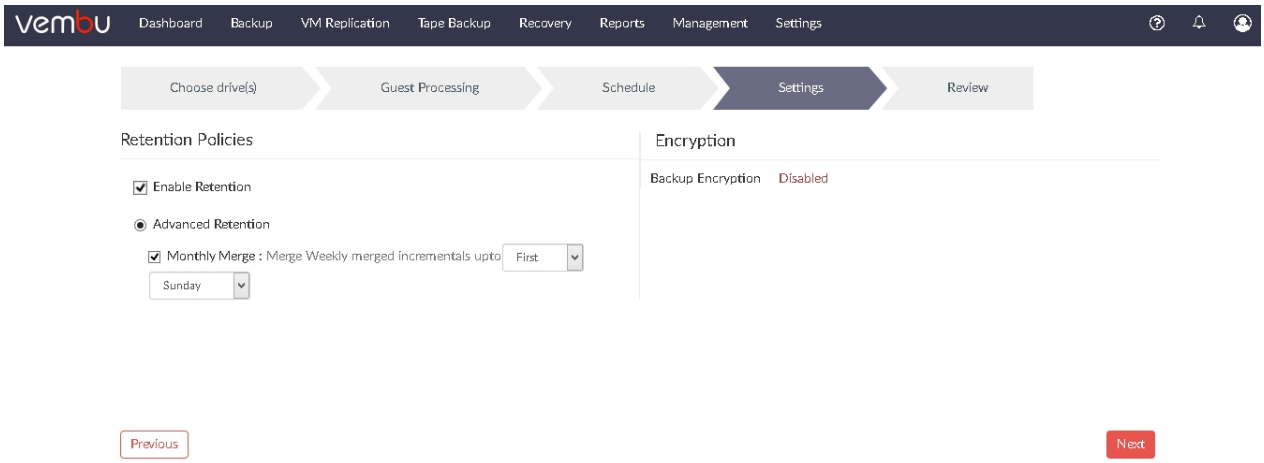
Step 4: Edit the Additional Full Backup Settings

- 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 "**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.



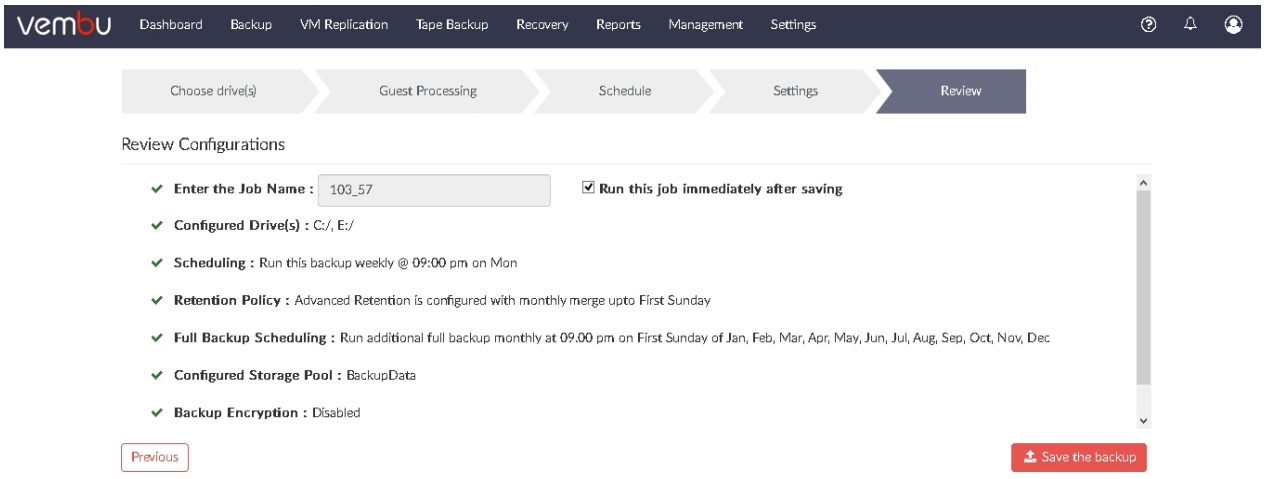
Step 5: Edit the Retention Settings

- 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 specific day in a month for the merge process and click **Next** to continue configuring your backup.



Step 6: Review Configurations

- The last step in your 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
    - Drives/Disk(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:

- Add Disks/Drives
- Backup Encryption
- Encryption Hint
- Storage Repository
- Job Name

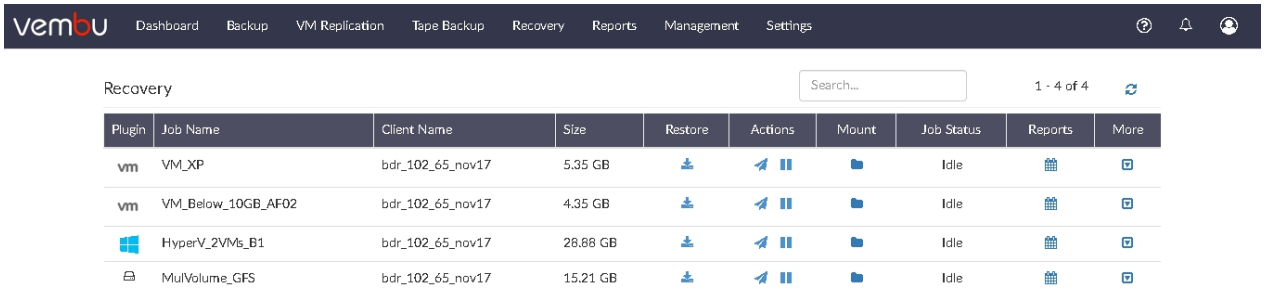
Evaluator's Guide for Windows Servers and Workstations

Recovery

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

- Case 1: Recover VM instantly on another virtual host
- Case 2: Restoring individual disk/drive to another disk/drive
- Case 3: Recover a single file
- Case 4: Instantly view/access files in a disk
- Case 5: Restore Physical Machine as a file type of your choice
- Case 6: Bare Metal Recovery

- 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



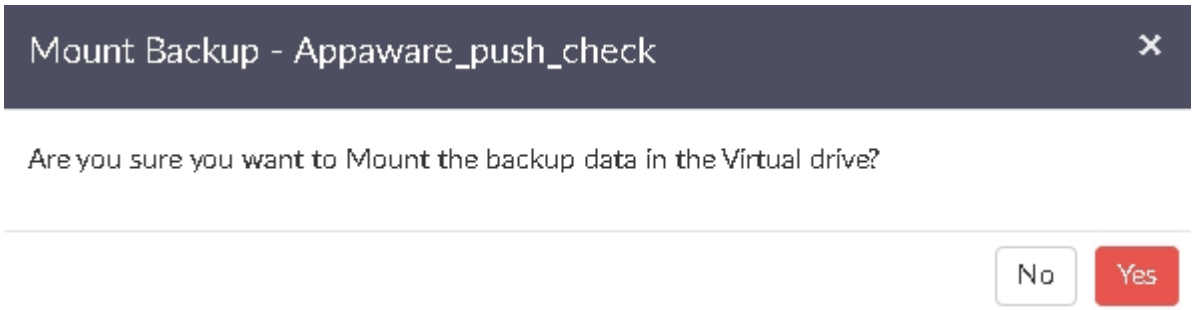
Selecting the **Recovery** tab will allow you to configure your restore along with the options listed below:

Restore

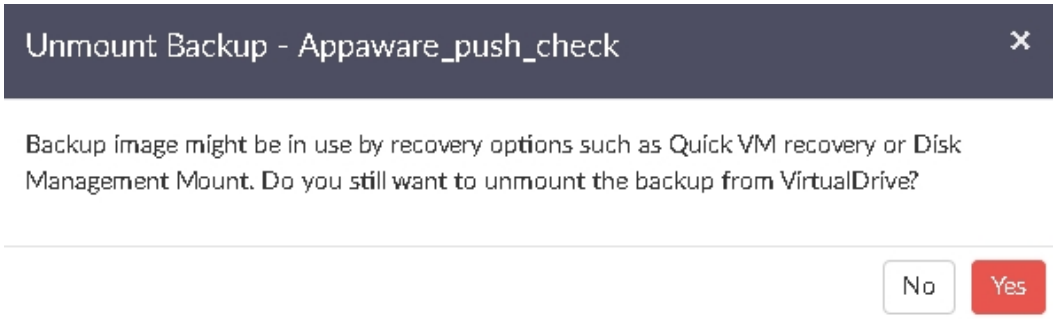
- Selecting this option will lead you to select the restore type

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.



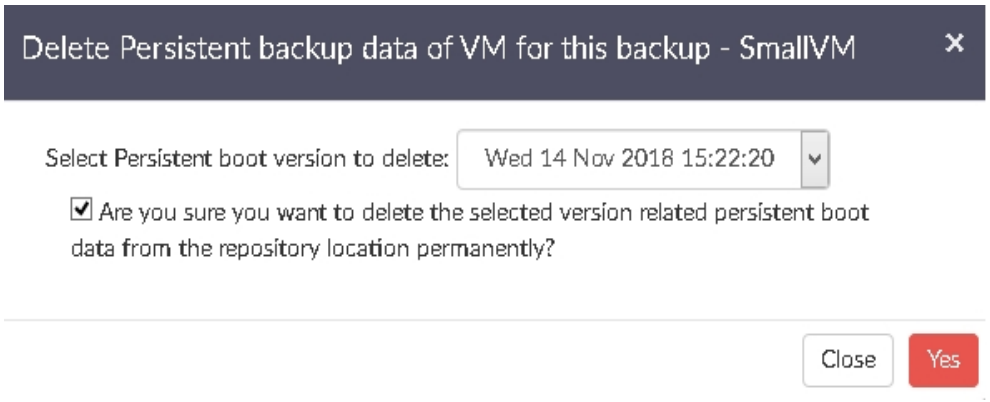
- Once done with the requirement, unmount backup data. This will resume the backup job, so that increments will run as per schedule.



To learn about how to manage Virtual Drive: **Click Here**

Note: The Restore symbol is hidden or greyed-out due to following reasons.
o If the backup selected for restore is currently in backup progress.
o If the replication process is active for the backup that is selected for restore.
o If the full backup of the selected backup job fails to complete.
o If the backup selected for restore is already processing a Restore job at that moment.

- **Proceed to Persistent boot delete:**
  During each instant boot(Quick VM recovery) and instant file recovery session, a change in backup data will take place which is saved as **Persistent Instant boot data.**
  - Persistent data can be restored using restore options if needed. The Persistent data is indicated with a **(+P) sign** alongside timestamps of backup version.
  - Such persistent data can be deleted using the **'Persistent boot delete'** option, if it is not required.
  - 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.

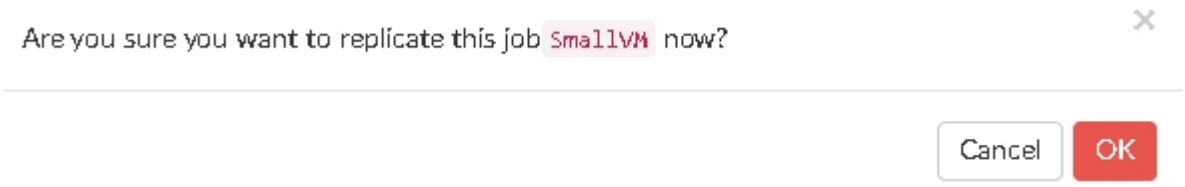


Delete

There are two types of delete available in the restore page:

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

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



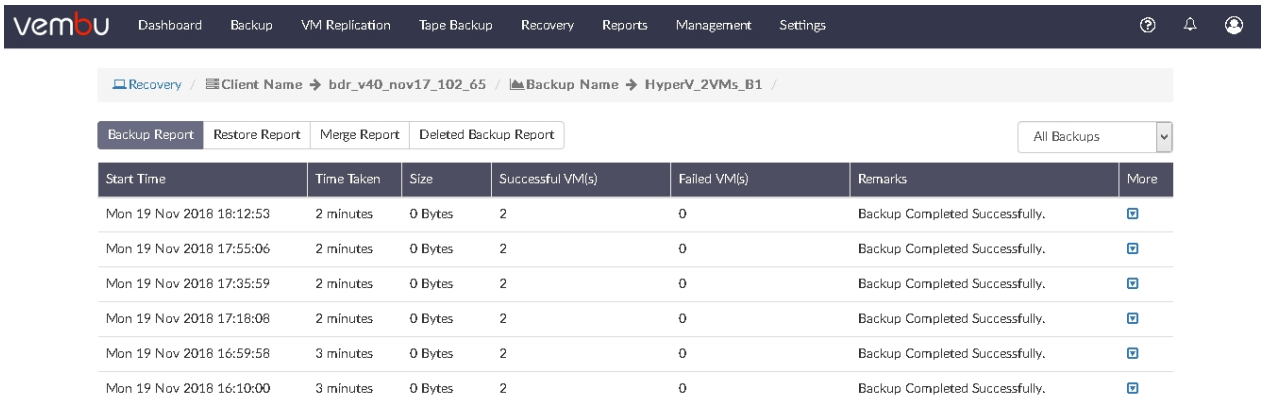
- **Replication actions**

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**.

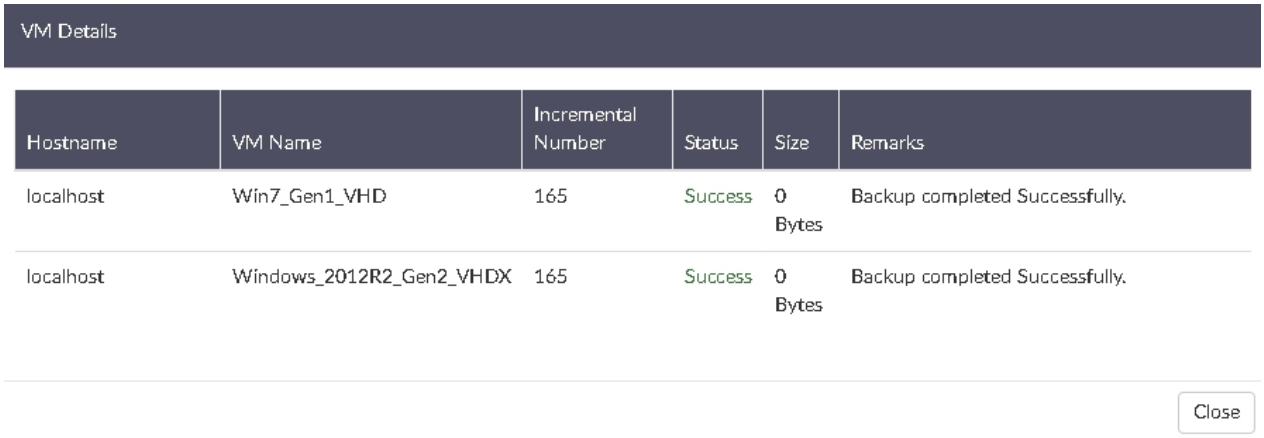
- **Replicate now** option will allow you to trigger the OffsiteDR replication immediately
- Using the **suspend** option you can suspend the replication process

- **Status**
  Indicates whether a backup job is running at any given time

- **Reports**
  You can find various reports for the backup job such as:
    - Backup Report
    - Restore Report
    - Merge Report
    - Deleted Backup Report



- Select the **More** tab to view further details on the report.



- From the drop-down list in the right top pane, select Full Backups option. You can delete your full backup by selecting the **Delete** icon.

Evaluator's Guide for Windows Servers and Workstations

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.

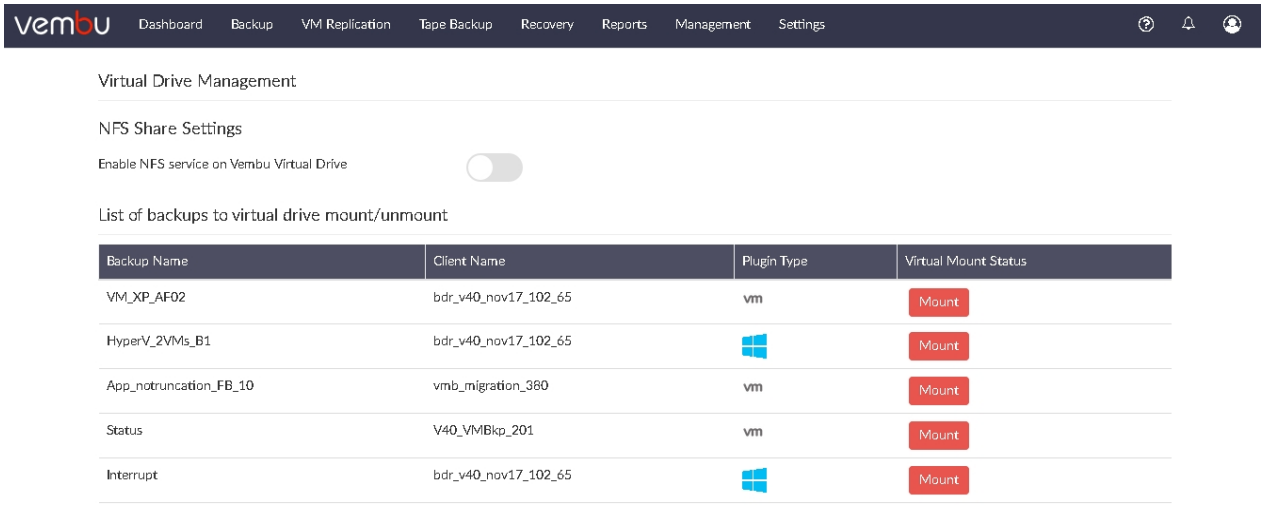
Vembu Virtual Drive will make following file format types available for any image based backups mounted in it:

- 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, select **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.



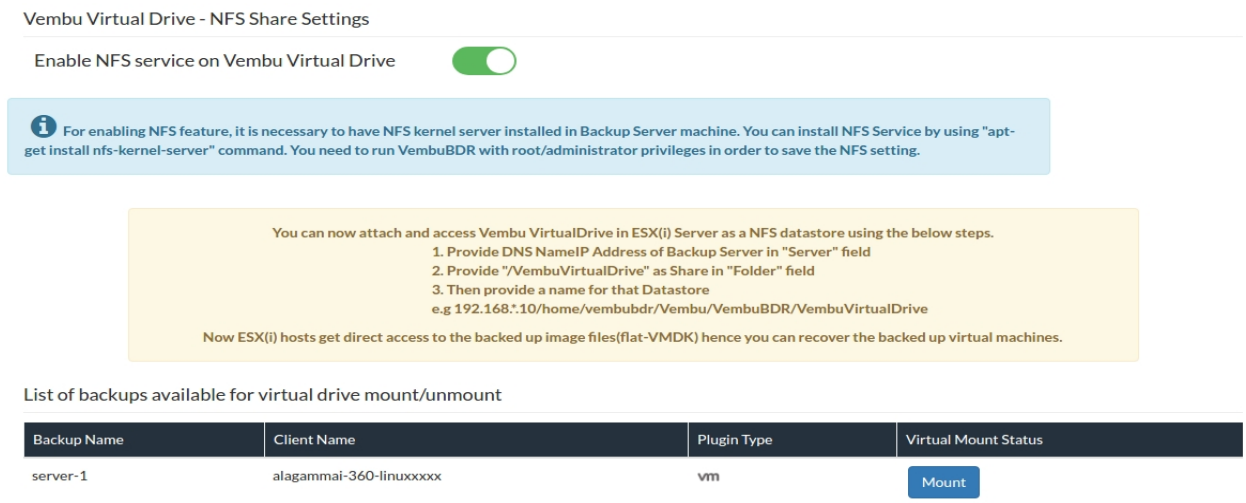
- To virtual mount a backup data, click the **Mount** option alongside specific backup job to be accessed.
- You can access the backup data by viewing VembuVirtualDrive displayed in My Computer. Once done with requirement, unmount data by selecting the **Unmount** option.

Enable NFS Service on Vembu Virtual Drive

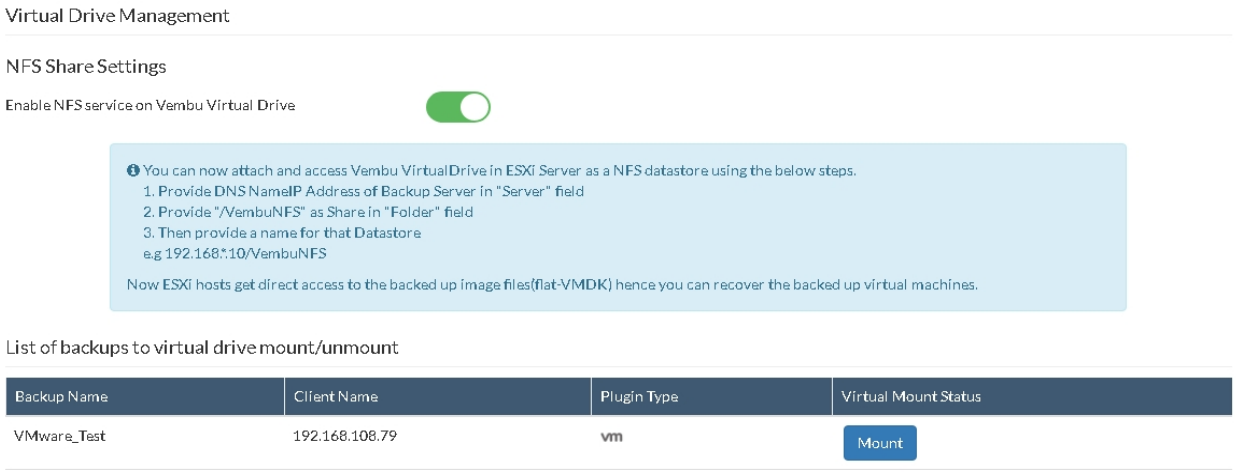
- Vembu Virtual Drive can be shared within a network area by enabling NFS service on Vembu Virtual Drive.
- NFS service for Vembu Virtual Drive is available on both Linux and Windows servers.

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 Windows Screenshot



- 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 Windows Servers and Workstations

Evaluation Case

There are 6 cases listed under this section along with their procedures that will help you perform the restore operations. By the end of the cases, you will have used every recovery option and restored your backup 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 restore operations, you must have a backup data that has been backed up successfully at least once
- The data to be restored should not be undergoing backup or replication process at the time

of restore

Evaluator's Guide for Windows Servers and Workstations

Case 1: Recovering a VM instantly on another virtual host

- In some scenarios, you might require instant access to your Physical Machines or VMs after a crash. **Quick VM Recovery** provides that option.
- Quick VM Recovery restores your Physical Machines 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:

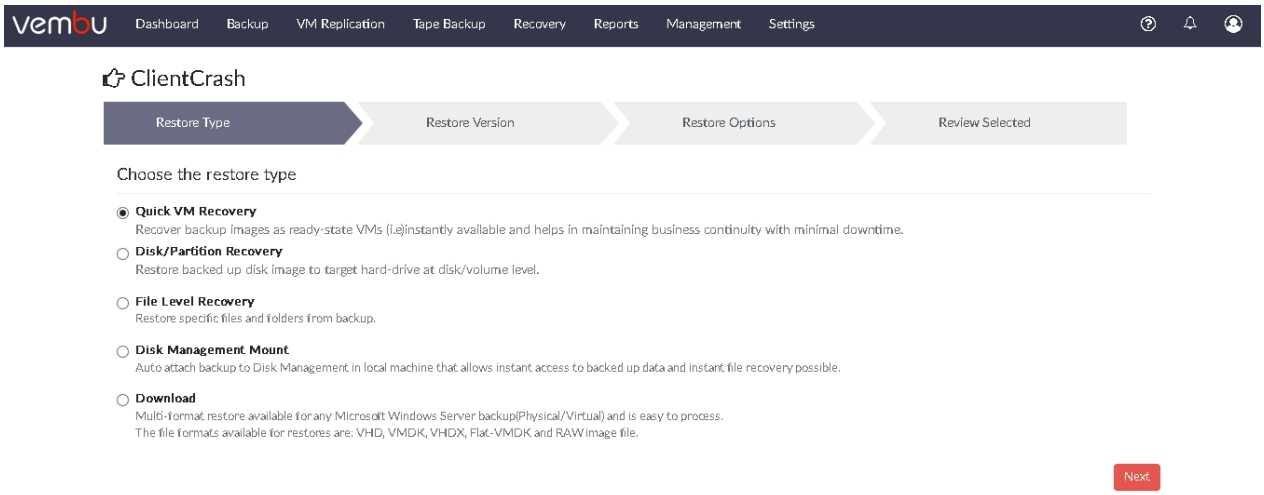
- VMware (Available in both Windows and Linux servers as an alternate software for instant boot)
- Hyper-V (Default software chosen for Windows and available only on Windows Backup servers)
- KVM (Default software selected for Linux and available only on Linux servers)

Note: Quick VM Recovery is only possible, if the backed up disk is a System bootable disk

Procedure

Step 1: Choose the Restore Type

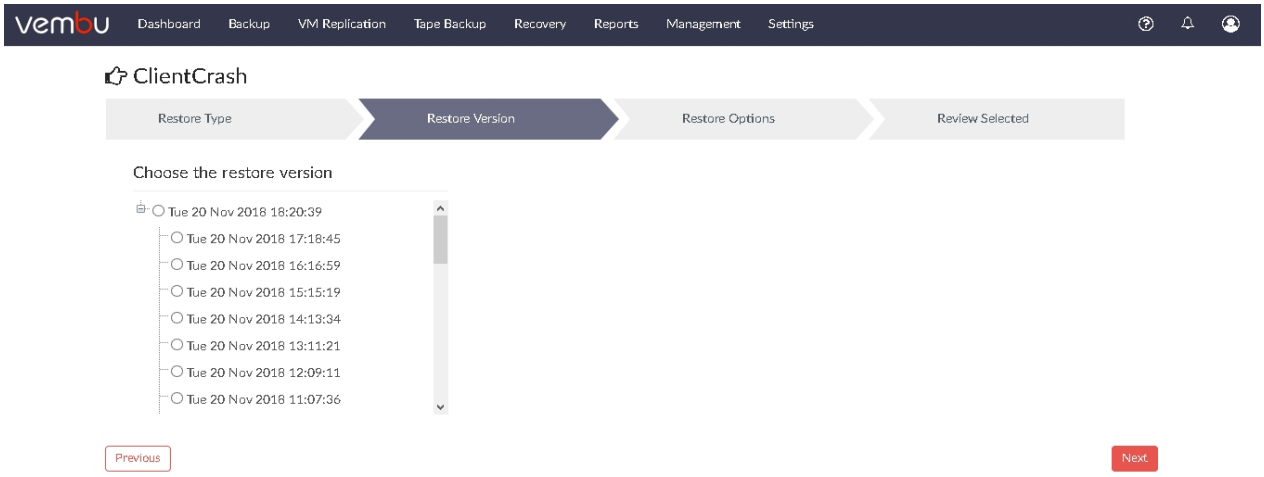
- Login to Vembu BDR server installed in a Windows/Ubuntu machine environment and click the **Recovery** tab. Select the desired backup job that has to be restored and choose **Quick VM Recovery** as the restore type.
- Click **Next** to proceed with restore process.



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.

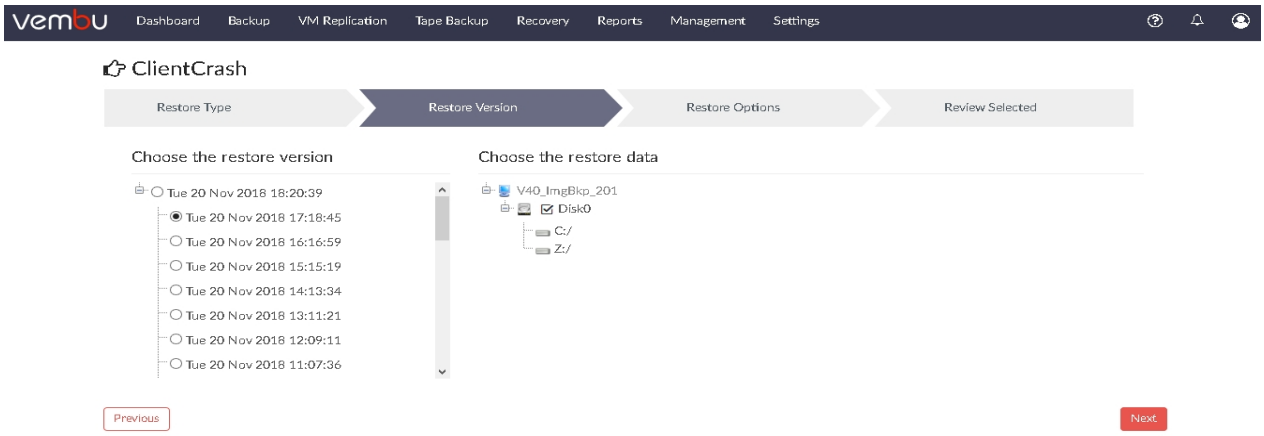
Note: You can enable only one timestamp for restore at a time.



Step 3: Choose the Restore Data

- In the restore data section, select the disk that you want to restore. You will be allowed to select only bootable drive for the restore in Quick VM recovery. If you have configured disks with multiple drives for backup, you cannot recover all the drives in the disk using Quick VM Recovery.
- Once you have selected the restore data, click **Next** to proceed with restore process.

Note: Only drives which have System-bootable OS in the backup will be displayed for Quick VM Recovery.



Step 4: Select the Software for Quick VM Recovery

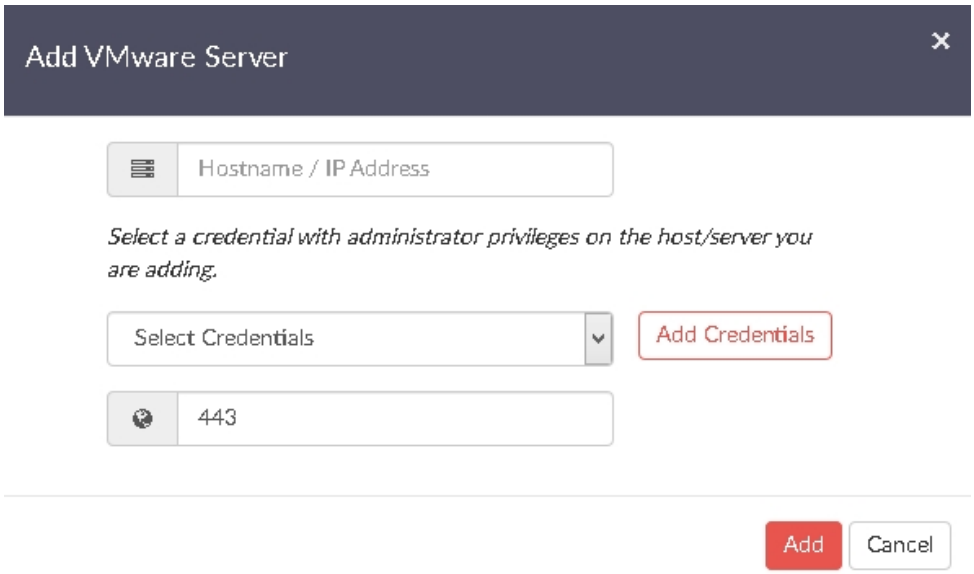
- The next step will be to choose the environment in which the Quick VM Recovery is to be performed.Depending upon the target hypervisor where the VM needs to be booted, the restore options vary.

In the Quick VM Recovery drop down list select any one from the following:

- VMware
- Hyper-V
- KVM

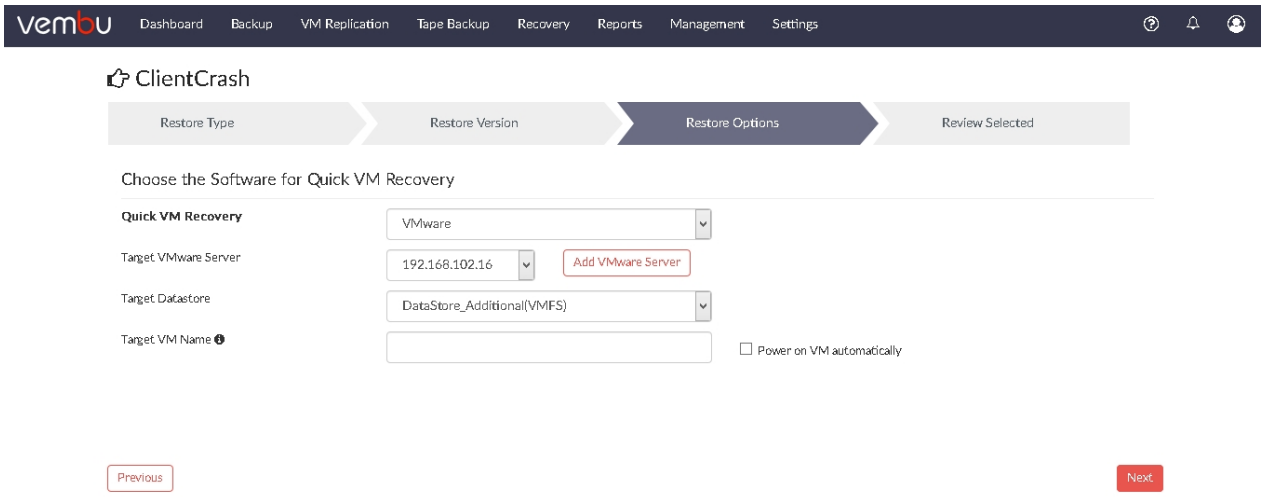
Restore to a target VMware Server:

- Select VMware from the drop-down list and the target VMware Server in which the booting must take place. 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. Click **Add** to to save the provided credentials.

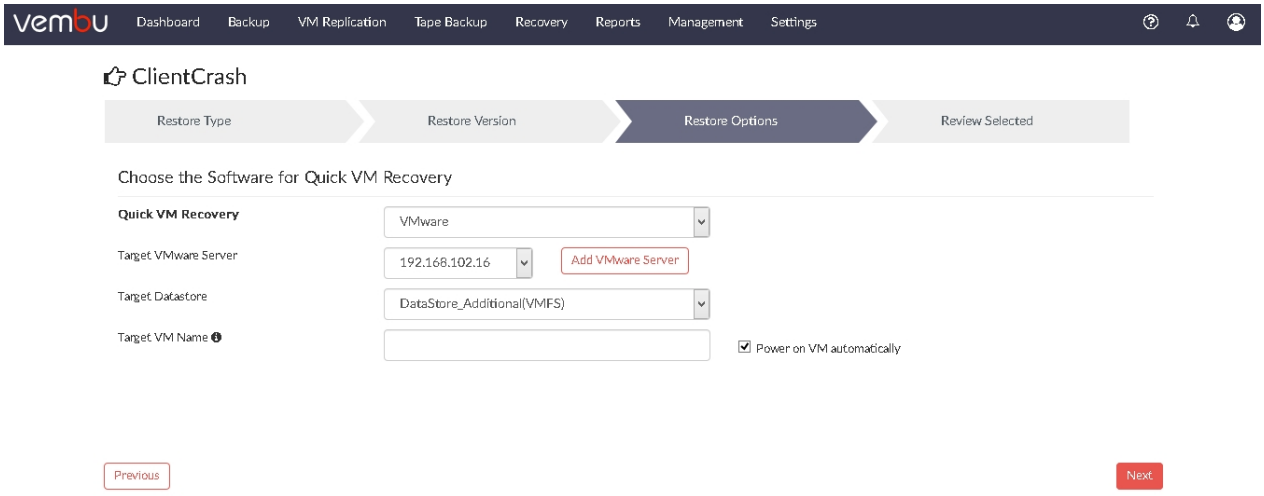


Note: If the added server is a vCenter Server, select the **Target Host Name** from the list of ESXi hosts.

Note: If you configure a port number that is already taken, you will get the message: "Network connection timed out. Invalid VMware Server IP or Invalid Port."



- If you have entered an ESXi host IP, then you will be asked to select the target datastore location.
- In the **Target Datastore** field, the available datastore in the ESXi host will be listed. Using the drop-down list, select the target datastore to which the VM will be added.
- If you have entered the **vCenter Server** address, then you have to select the **Target ESXi host IP address** in which you want to restore the VM.



- In the **Target ESXi Server** field, select the target ESXi host using the drop-down list. Once you have selected the ESXi host, specify the **Target Datastore** from the list of datastores available under the ESXi host
- Provide a **VM Name.** This is the name with which your VM will be created in the datastore you have configured. Enter the unique VM name, that you can identify easily in the selected target host.

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

- 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. Once you are

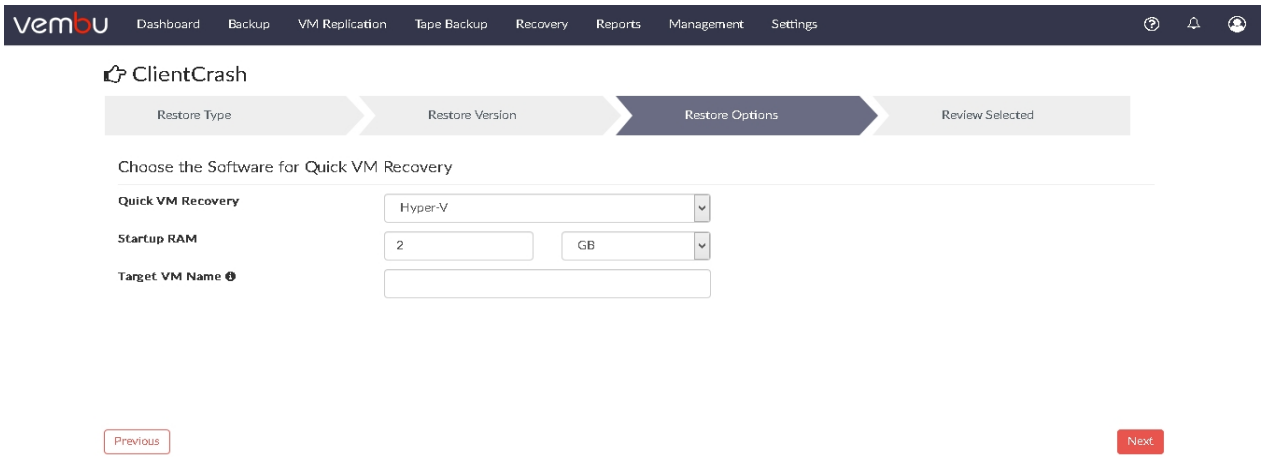
done with the restore options, click **Next** to proceed with Review selected window.

Note: 6 GB RAM will be assigned by default for VMs booted via VMware ESXi in Quick VM Recovery

Restore to a Hyper-V Host:

- You can choose the software as Hyper-V (For Windows servers). On selecting Hyper-V as your booting software, the default **RAM size chosen is 2 GB** which can be modified based on your requirement.
- Once you have configured the restore options, Click **Next** to review your configurations.

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

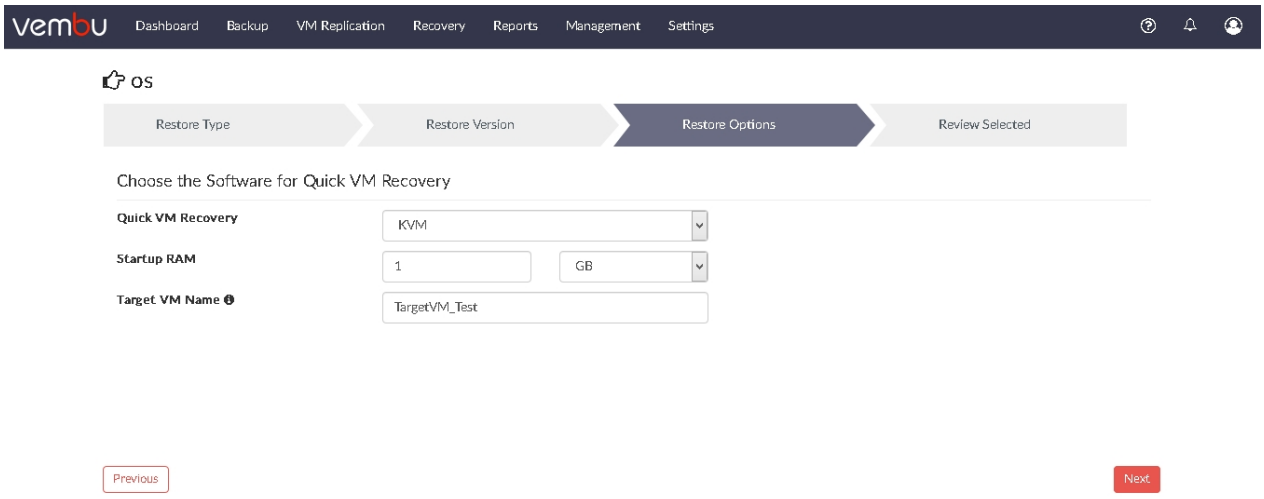


Restore to a KVM Host:

- Choose the software for Quick VM Recovery as **KVM** (For Ubuntu servers). On selecting KVM as your boot software, the default RAM size chosen is **2GB** which can be modified based on your requirement.

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

- Once you have configured the restore options, Click **Next** to review your configurations.

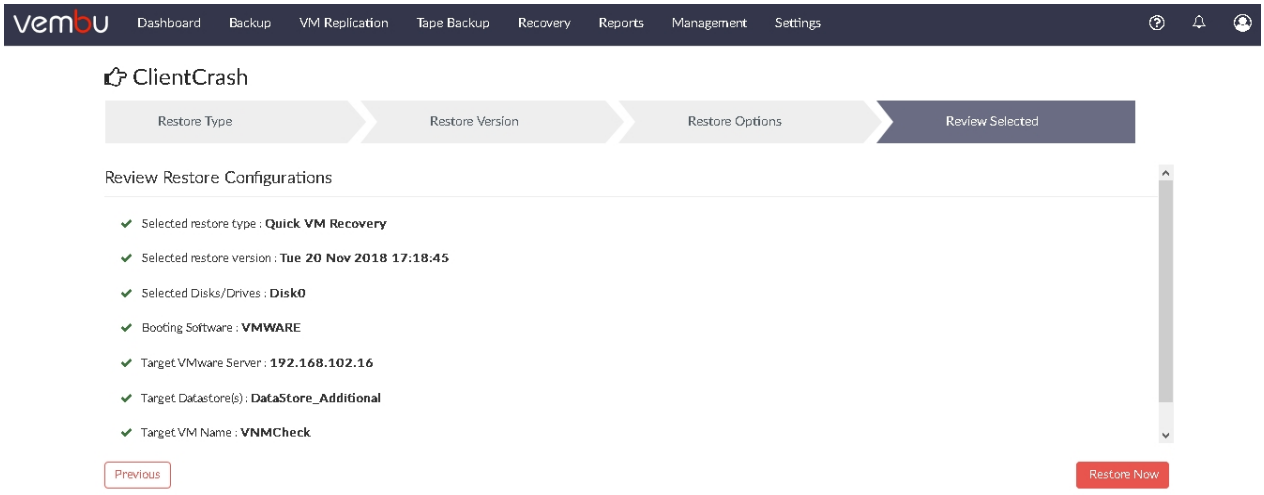


Limitations:

- If the KVM has EFI boot, the boot process will not occur in Quick VM Recovery.
- If the backed up Disk Size is more than 2TB, then boot process is not possible.

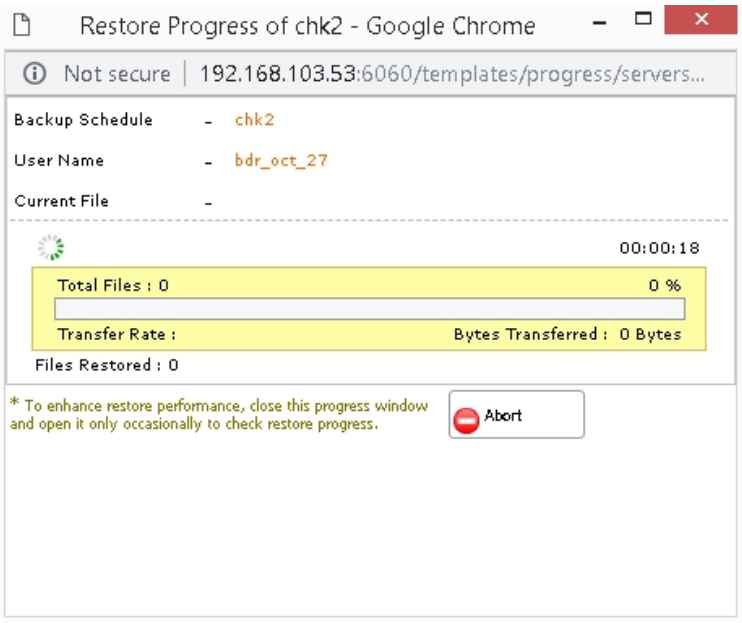
Step 5: Review Restore configurations

- Once done configuring the recovery job, the final step will be to review all your configurations before proceeding to trigger the Restore. Check the following:
    - Restore type
    - Restore version
    - Selected Disk/ Drive(s)
    - Booting software
    - Target VMware Server IP
    - Target Datastore
    - Target VM Name



- Once you have reviewed your selections, click **Restore Now** to begin the Quick VM Recovery process. You will be redirected to the recovery page once the restore process is completed.
- You can view the status of the Restore from the **Status** option. Once you click the inverted arrow mark, the below page will be displayed.

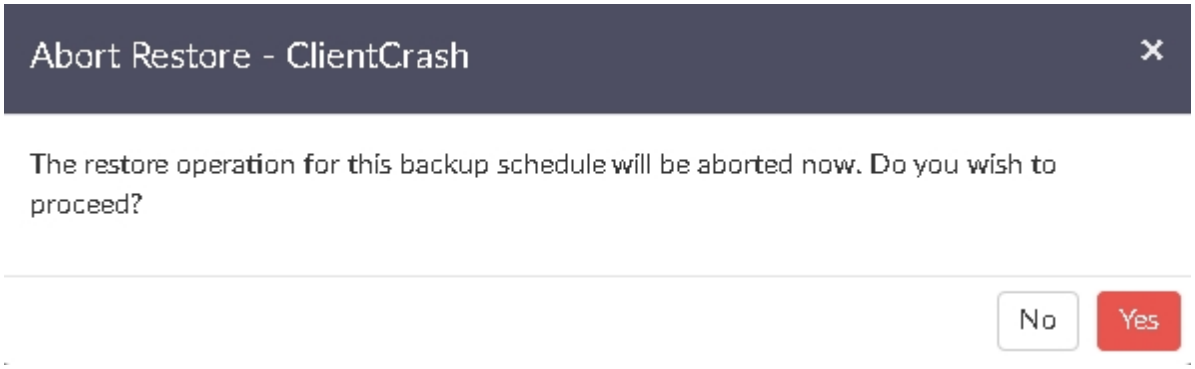
Note: Once done with requirement, shutdown and turn off VM before unmounting backup data. This will resume backup job, so that incremental will run as per schedule.



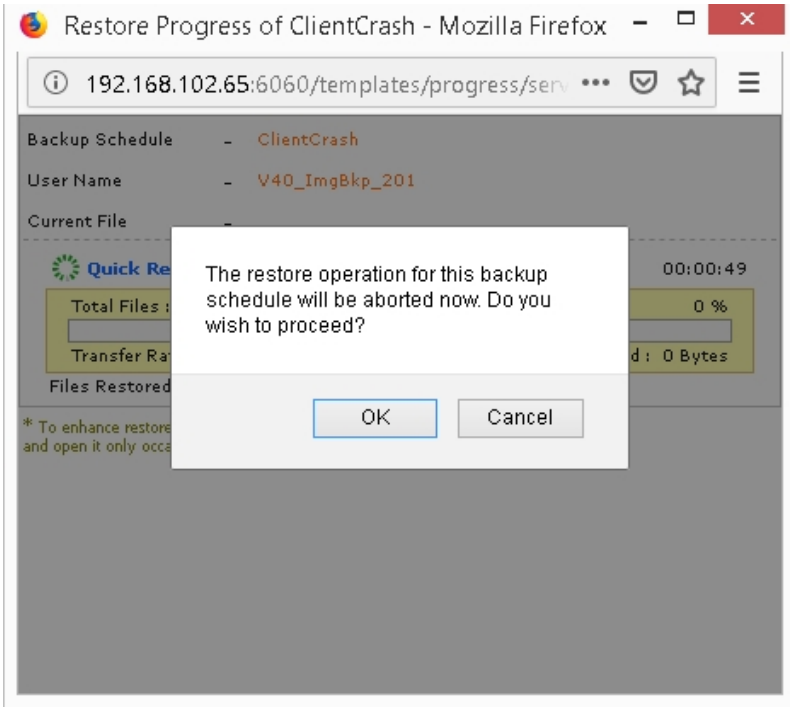
The following details will be available in the Restore Progress Page window

- **Backup Schedule**: The backup schedule name mentioned by the user for indicating the backup during restore progress.
- **Client Name:** The name of the client from which the backup process is initiated.
- **Total Files:** The number of disks/drives present in the selected backup.
- **Transfer Rate:** Speed at which the restore process
- **Bytes transferred:** Rate at which the backup data is restored (Bytes, KB, MB, GB)
- **Files Restored:** Number of disks/drives restored during the process of recovery
- **Time Left:** Time remaining for the restore to complete

- 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.



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

Evaluator's Guide for Windows Servers and Workstations

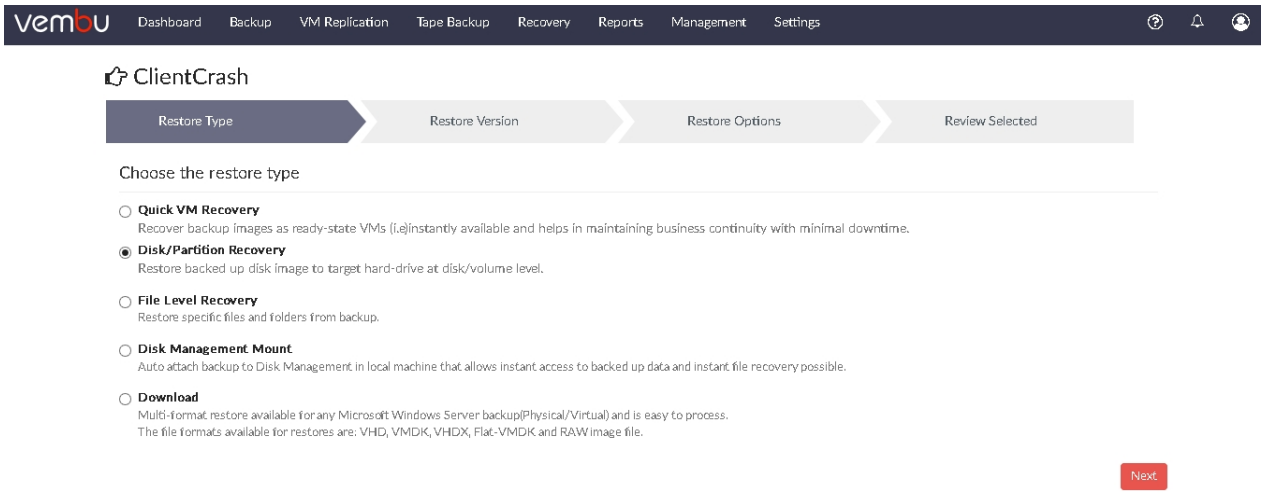
Case 2: Restoring individual disk/drive to another disk/drive

- **Disk/Partition Recovery** allows you to restore an individual disk/partition from the backed up physical machine. The disk/partition will be restored to the target machine and will be attached so that it can be accessed from that target machine.
- In some cases, you can also attach the restored disk to your original physical machine in case of any disaster. Once the disks are attached to the target machine, you will be alerted to manually reboot the machine so that the configurations get updated.

Procedure

Step 1: Choose the Restore Type

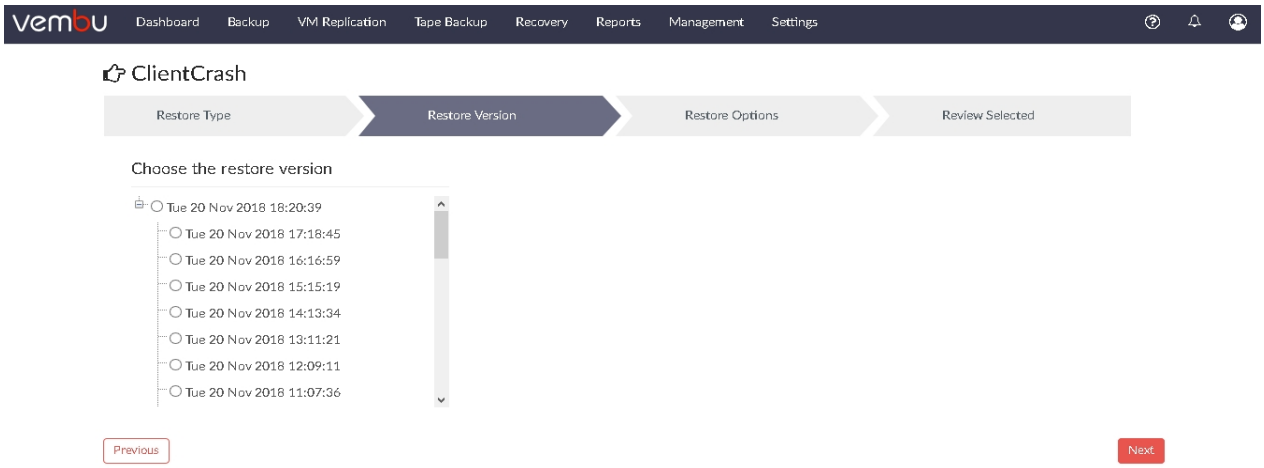
- Click the **Recovery** tab and select the **restore** icon near the Disk Image backup that is to be restored. Select **Disk/Partition Recovery** as the Restore type and click **Next** to proceed with the restore process.



Step 2: Choose the Restore Version

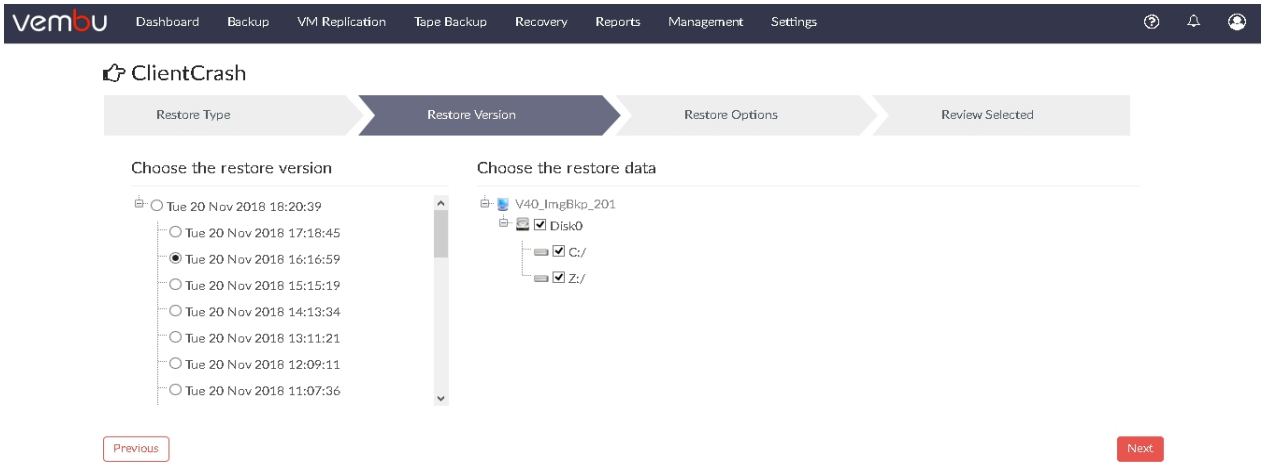
- Select the restore version for the restore process. The restore version is created based on the end time of the backup (i.e the date and time when the backup process scheduled is completed), this is named as **Recovery points**. The full backup and incremental backup timestamps are listed with the 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.



Step 3: Choose the Restore Data

- Select the backup data to be restored based on the requirement: at disk level or at the partition level. Once you have selected the restore data, click **Next** to proceed with restore process.

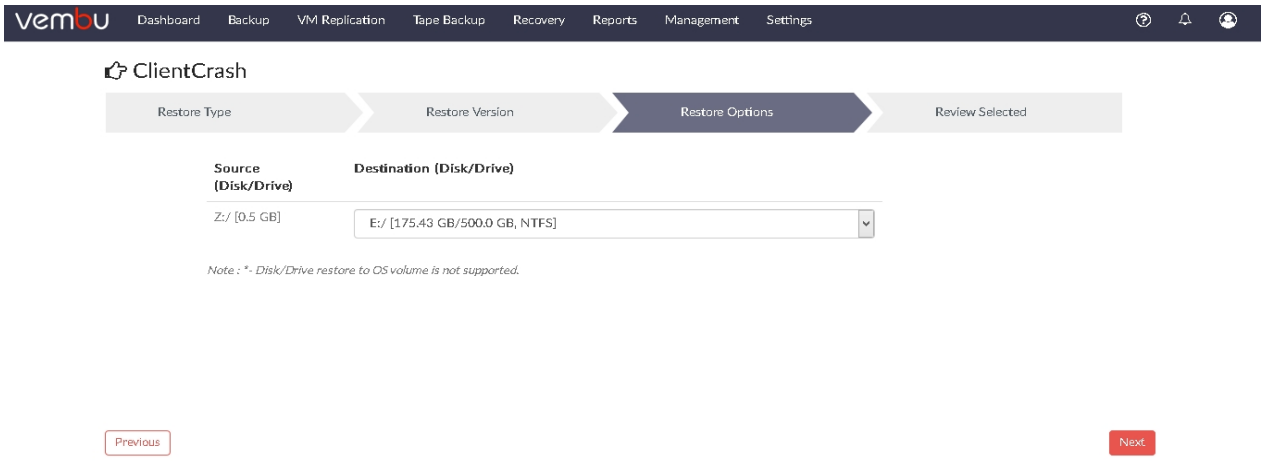


Step 4: Select Restore Options

Disk Level Recovery

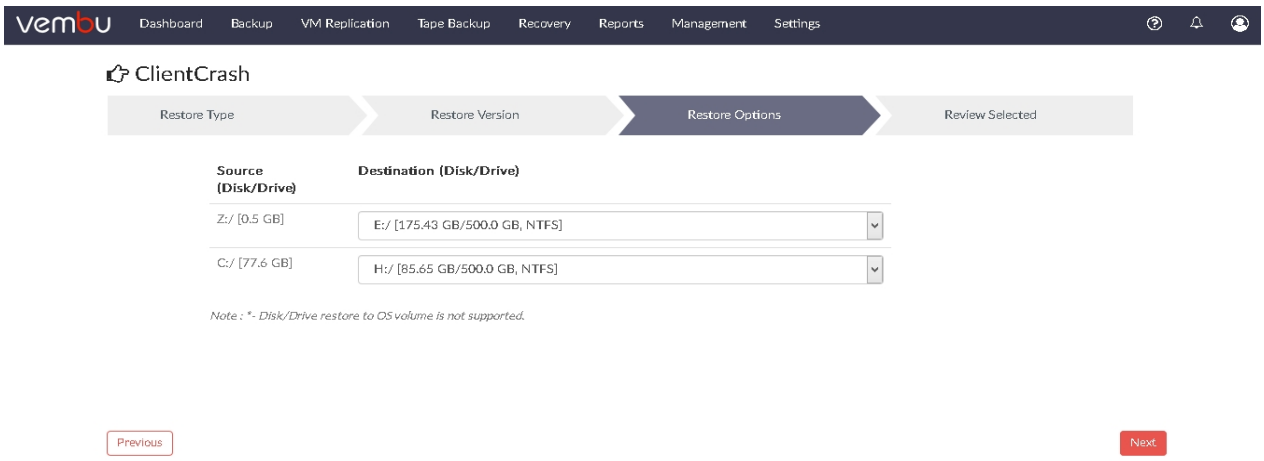
- If the data to be restored is selected at the disk level, you can choose from the list of disks available in the server machine.
- The destination disk chosen to perform restore will be displayed with its available storage space. The available space in the destination disk must be large enough to accommodate the backup data that is being recovered.

Note: Disk/ Drive restore to the OS volume is not supported.



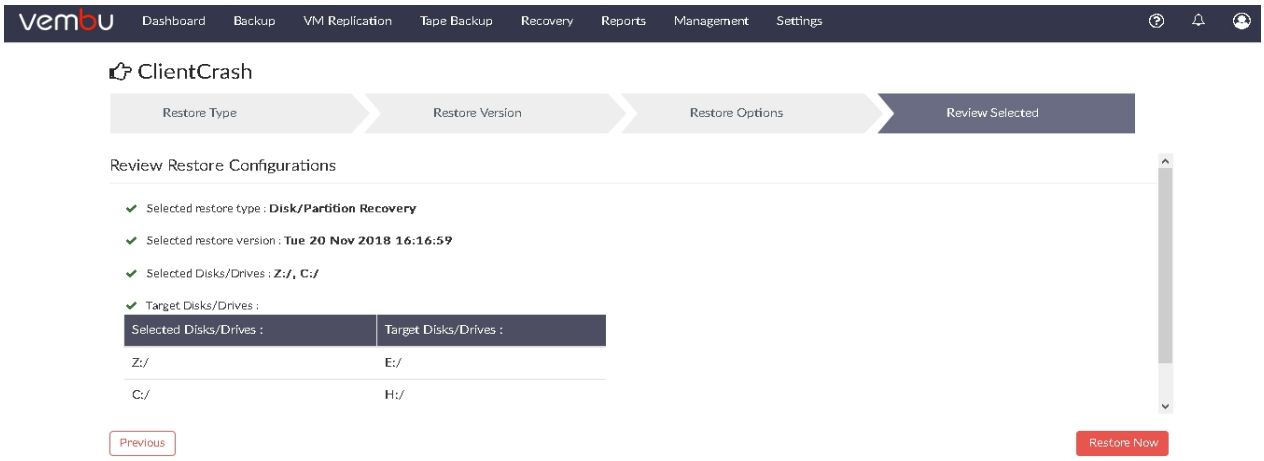
Partition Level Recovery

- If the data to be restored is selected at the partition level, you can choose from the list of partitions available in the server machine.The destination drive or volume chosen will be displayed with its total space, available space and the type of drive.
- Once done configuring the restore options click **Next** to review your selections.

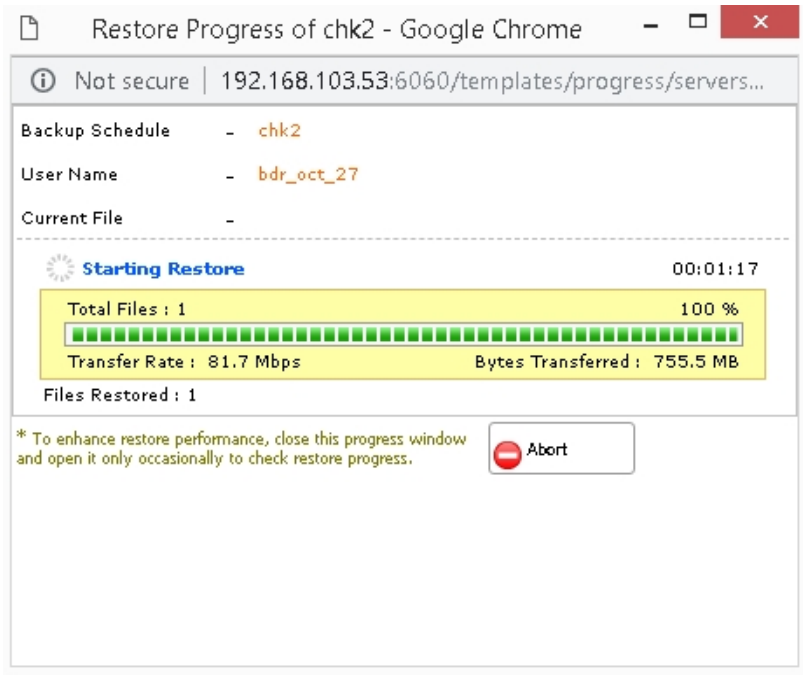


Step 5: Review Restore Configurations

- Once done configuring restore options, proceed to review configuration. The page will list the
  - Selected Restore type
  - Selected restore version
  - Selected disks/drives for restore
  - List of source and target Disks/Drives selected



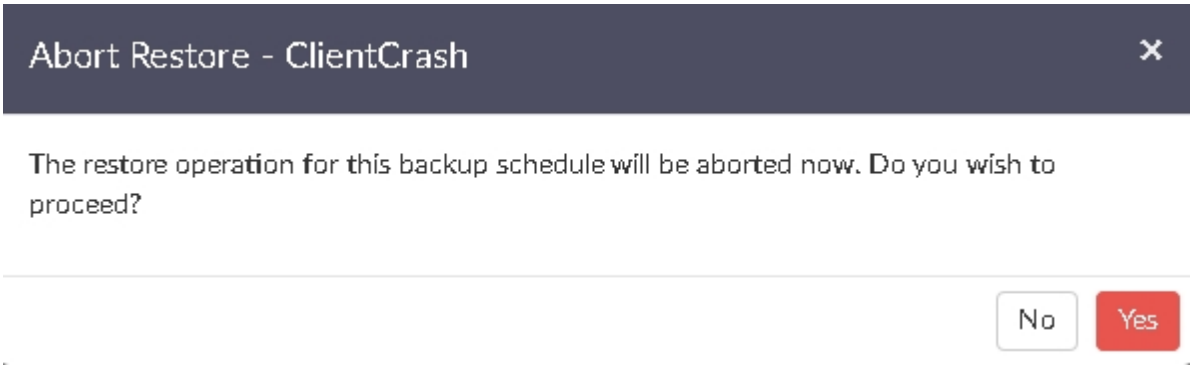
- Once you have reviewed your selections, click **Restore Now** to begin the restore. You will be redirected to the recovery page once the restore process is completed.
- You can view the status of the Restore from the **Status** option. Once you click the inverted arrow mark, the below page will be displayed.



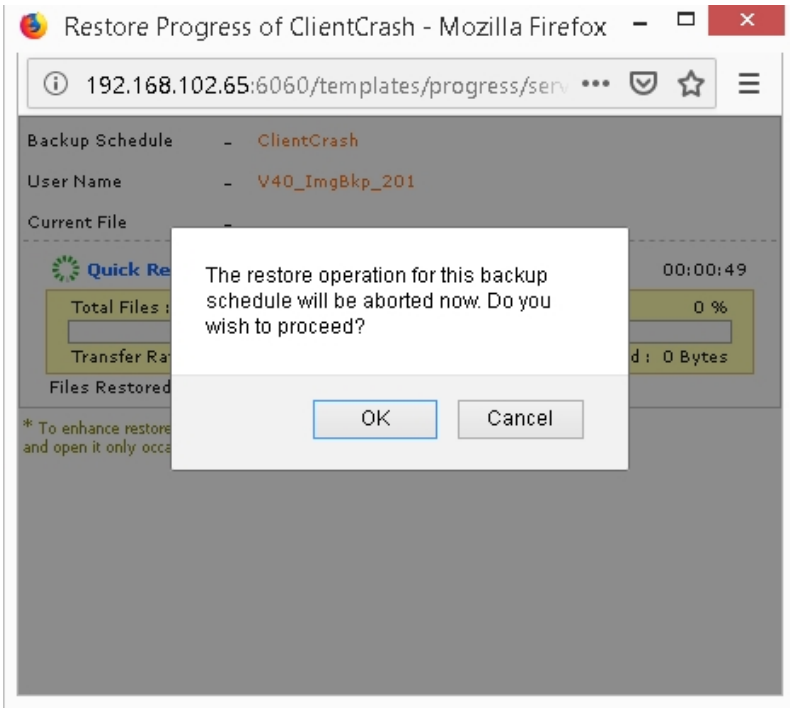
The following details will be available in the Restore Progress Page window

- **Backup Schedule**: The backup schedule name mentioned while creating a backup job.
- **Client Name:** The name of the client from which the backup process is initiated
- **Total Files:** The number of disk/Drives present in the selected backup
- **Transfer Rate:** Speed of the restore process
- **Bytes transferred:** Rate at which the backup data is restored (Bytes, KB, MB, GB)
- **Files Restored:** Number of Disk/Drives restored during the process of recovery
- **Time Left:** Time remaining for the restore to complete

- 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.



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

Tip: You must ensure the details about the target drive prior selection for Disk/Partition level Recovery

Limitations:

- For Dynamic Volumes, Partition Recovery is not supported
- Ensure that the Target Dynamic volumes are compatible with source dynamic volumes during recovery (For Example, source Dynamic mirror volumes can be restored only if the selected target volume is a Dynamic mirror)
- The destination drive or the target disk selected which is formatted to perform restore and cannot be recovered

Evaluator's Guide for Windows Servers and Workstations

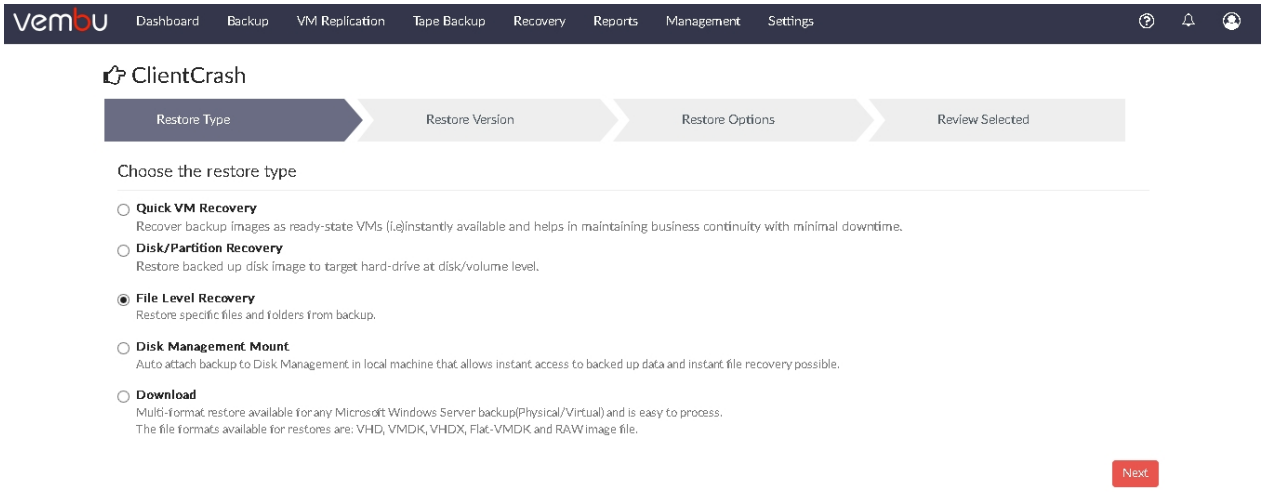
Case 3: Recover a single file

- Sometimes, you may want to restore specific files from a backed up physical machine instead of restoring the entire backup data. As Machine level Recovery will happen as a whole, some users do not prefer to restore the entire backup 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 physical machine. Once you configure the restore location and trigger the restore process you can find your backup files in the specified location within minutes.

Procedure

Step 1: Choose the Restore Type

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

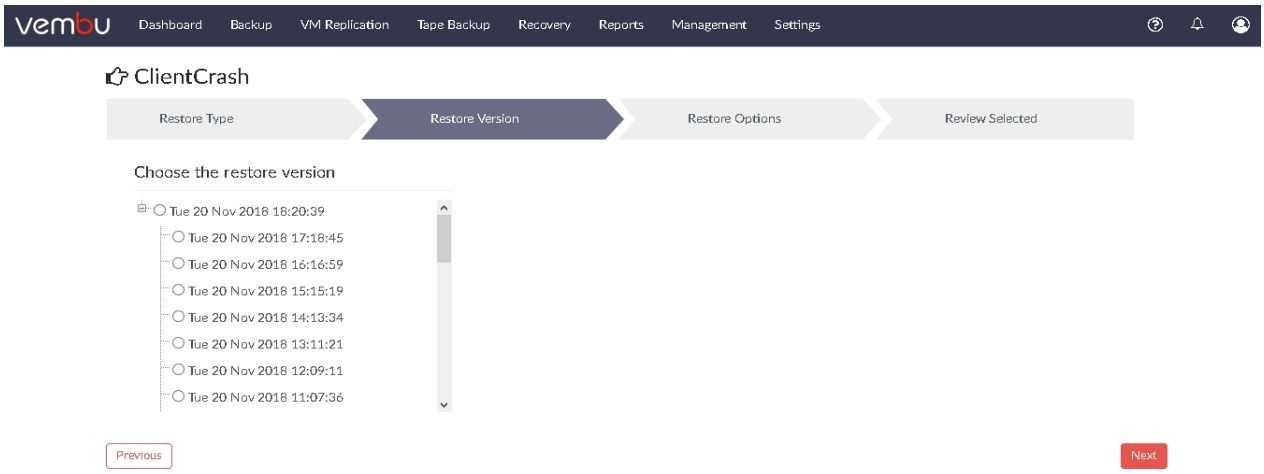


Step 2: Choose the Restore Version

- 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 select only one timestamp for restore at a time.



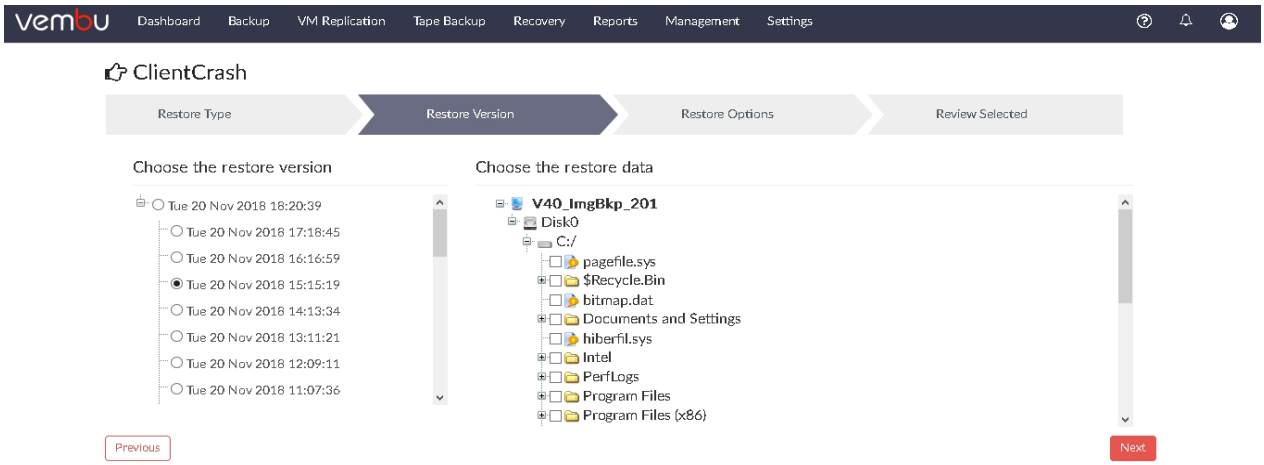
Step 3: Choose the Restore Data

- A tree listing backed up disks which on further expansion will list respective files and folders in it.
- You can select files and folders under different disks for restore.
- Select specific restore version of the files and folders you want to restore. Once done selecting files/folders, click **Next** to proceed with select restore location.

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 disks will be displayed. Click (+) to explore the disk 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 Disk(s)Volume(s), check if Vembu Storage volume is corrupted/ chunk files are not available



Step 4: Configure Restore Options

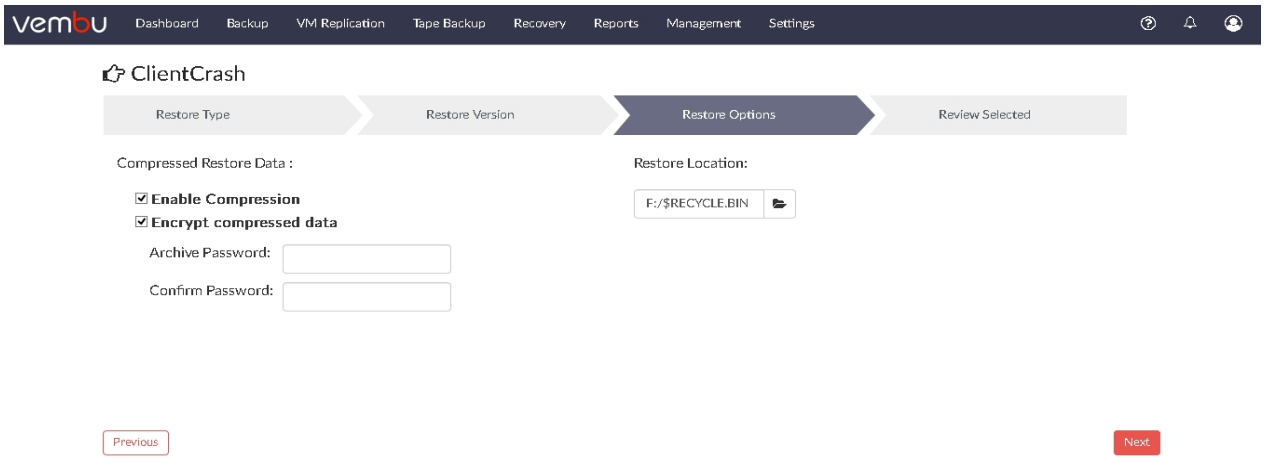
- The next step is to select whether you want to compress your restore data. Select the **Enable** option for compressing your restore data.
- You can encrypt the compressed data by selecting the **Encrypt Restored files for Zip process** option. Provide the encryption password and configure the restore 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

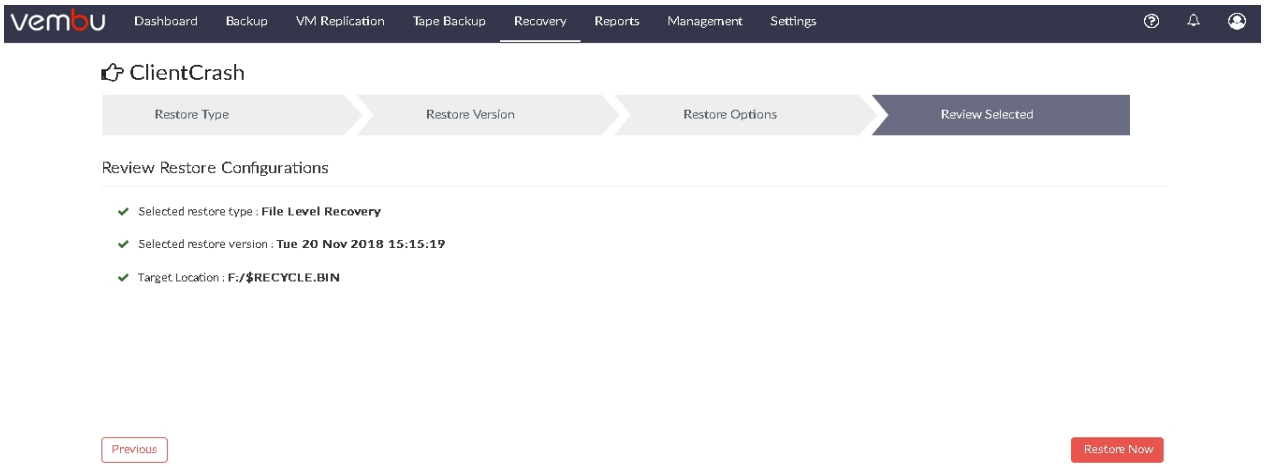
- Click **Next** to proceed to review your configurations.



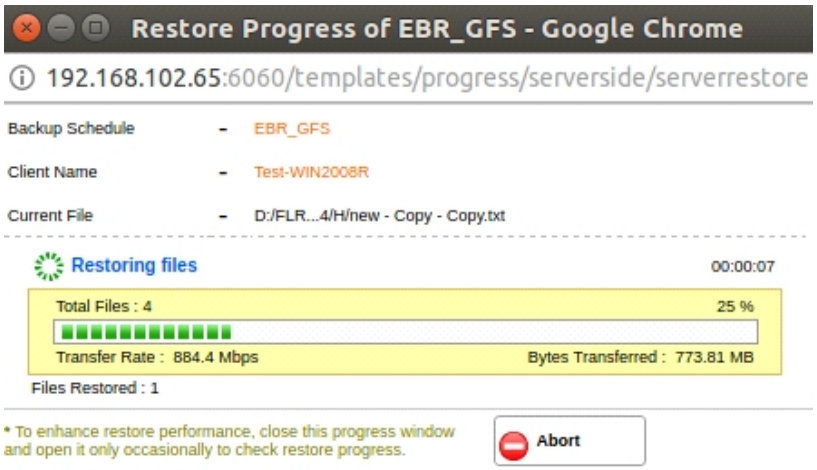
Step 5: Review Configurations

- 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.**

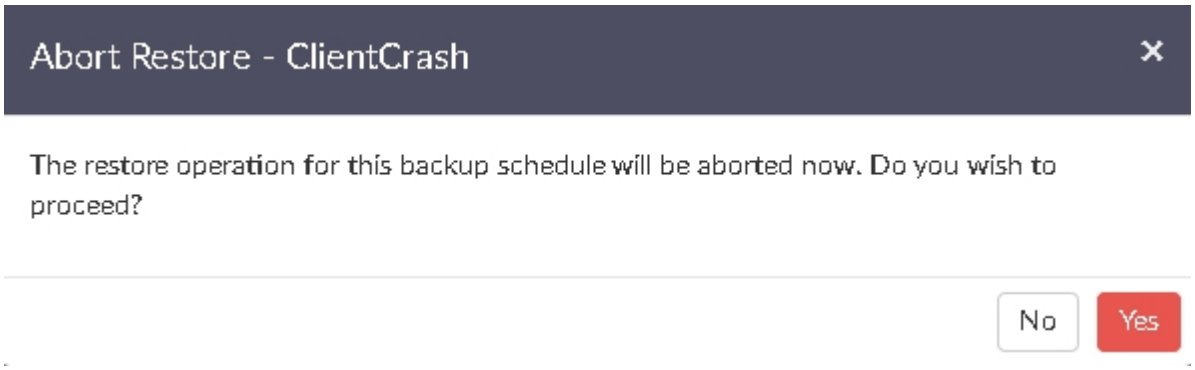


- You will be redirected to the recovery page. In the status tab click the arrow mark which will open the restore progress window.
- The following details will be available in the restore progress page:
  - Backup Schedule
  - User Name
  - Current File
  - Total Files
  - Transfer Rate
  - Files Restored

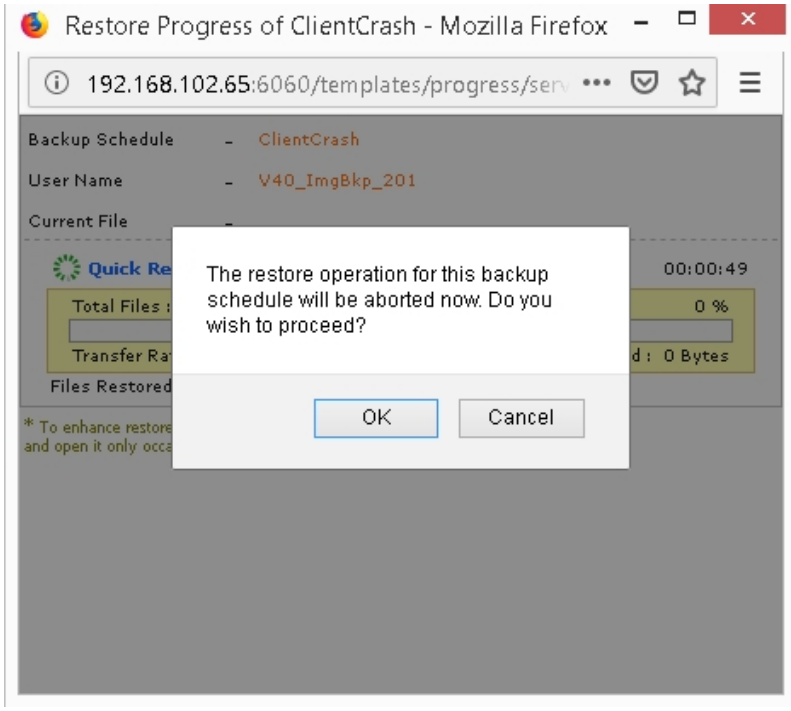


Note: To enhance the restore performance, close the restore progress window and open it occasionally to check the restore progress.

- 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.



Disk Management Mount

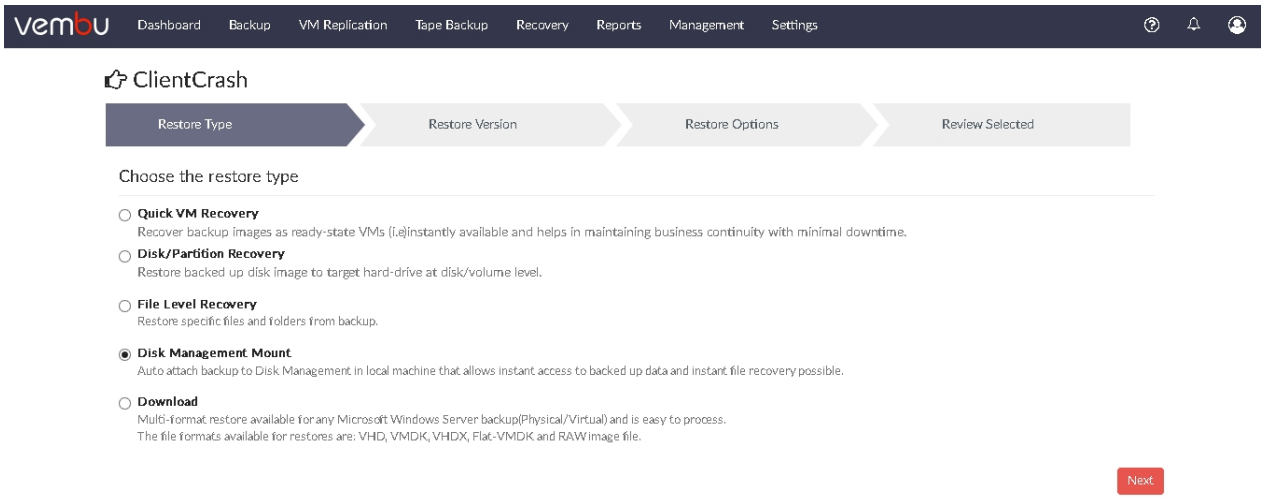
- There may be situations in which you may want to access your backup data instantly, without having to restore the entire backup. **Disk Management Mount** option will be helpful in such scenarios. You can auto attach your backup data to the disk management and find your backup data available in the 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 physical machine later.

Procedure

Step 1: Choose the Restore Type

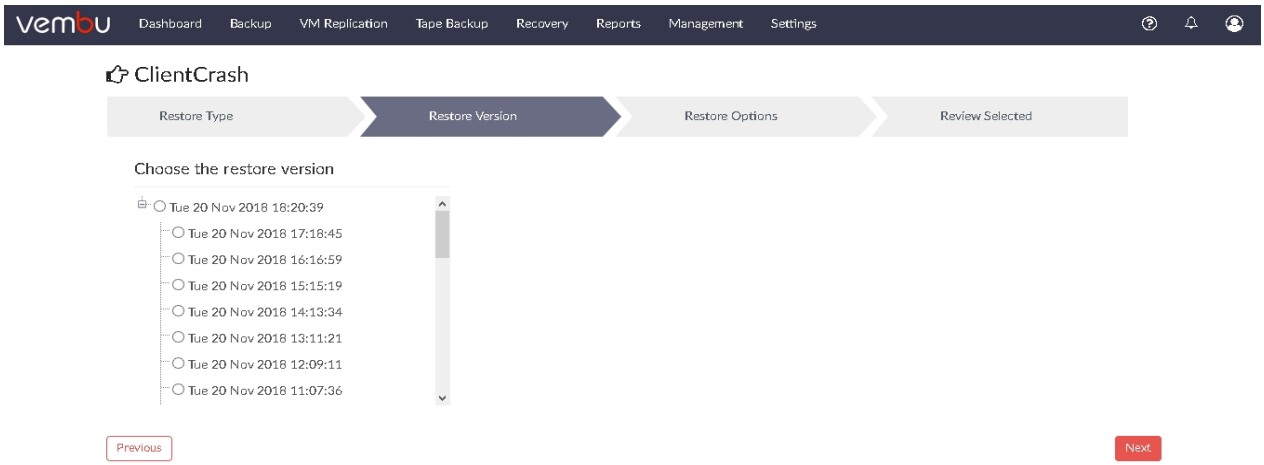
- Click the **Recovery** tab and select the **restore** icon near the Disk Image backup that is to be restored. Select **Disk Management Mount** as the Restore type and click **Next**.



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.
- Once done selecting the time-stamp version, click **Next** to configure the Restore data.

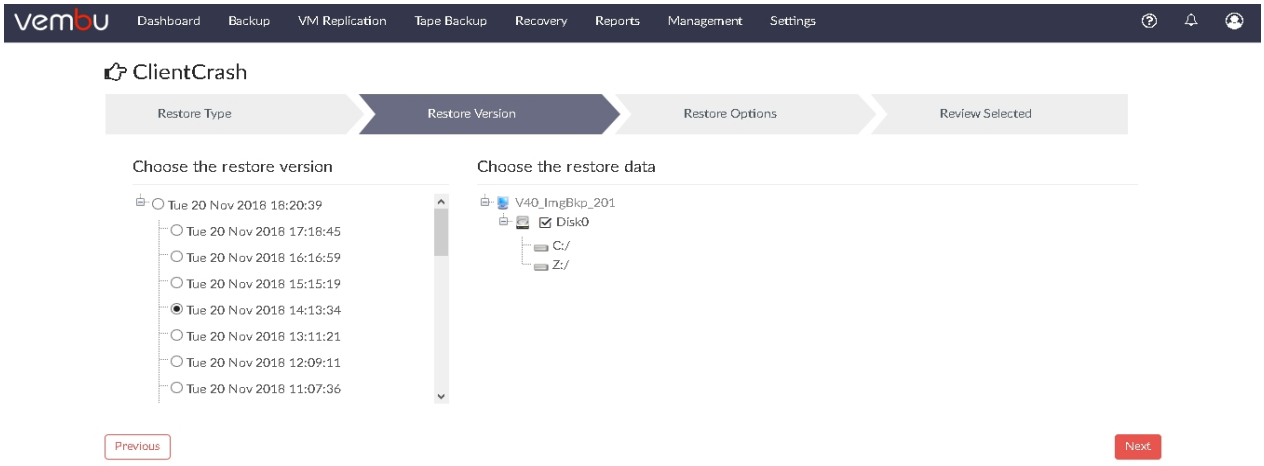
Note: You can select only one timestamp for restore at a time.



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

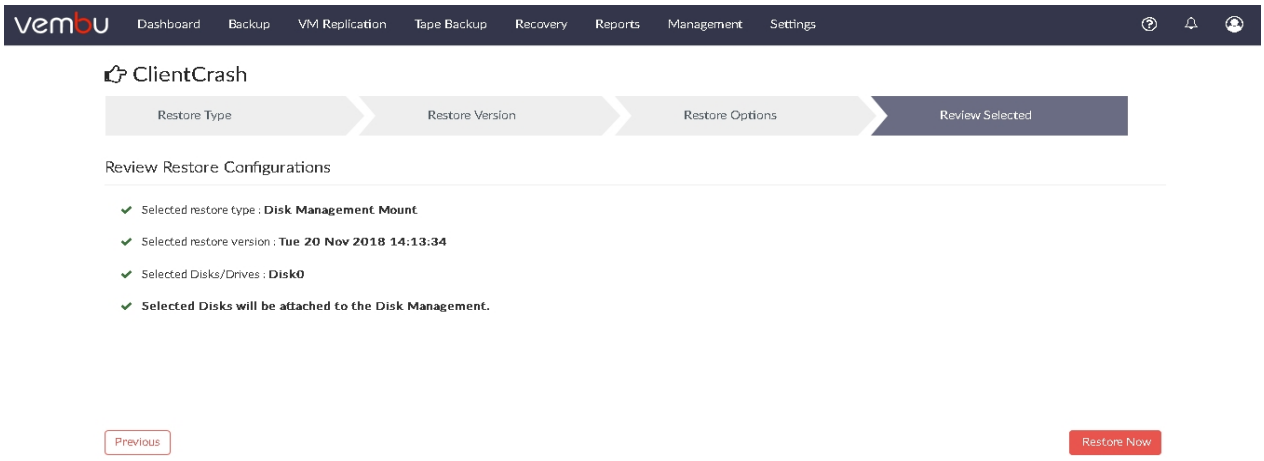
Note: You cannot mount more than one disk simultaneously. Choosing multiple disks for mount process will display error message “User allowed to restore only one disk at a time. If you choose multiple disks, previous selection should be ignored



Step 4: Review Configurations

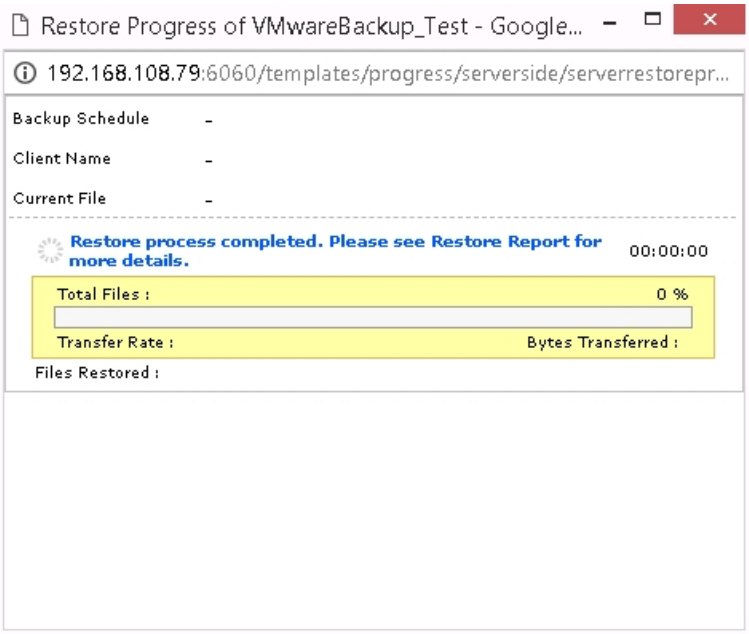
- The final step in this restore process is to review the configurations you have selected.
- Check the following:
  - Restore type
  - Restore version
  - Selected Disk/Drives

- Verify all the details and click **Restore Now.** This will trigger the Disk Management Mount process.



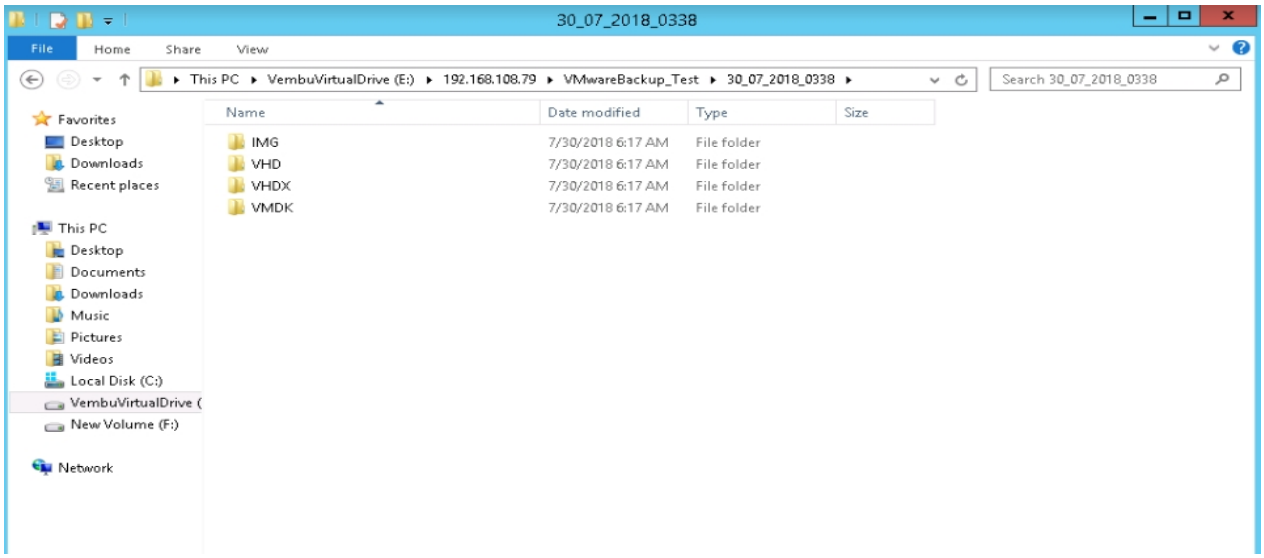
Note: Once done with the requirement, unmount backup data. This will resume the backup job, so that increments will run as per schedule.

- 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: The backup schedule name mentioned by the user for indicating the backup during restore progress
    - User Name
    - Current File
    - Total Files: The number of files present in the selected backup
    - Transfer Rate: Speed of the restore process
    - Bytes transferred: Rate at which the backup data is restored (Bytes, KB, MB, GB)
    - Files Restored: Number of files restored during the process of recovery
    - Time Left: Time remaining for the restore to complete



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.



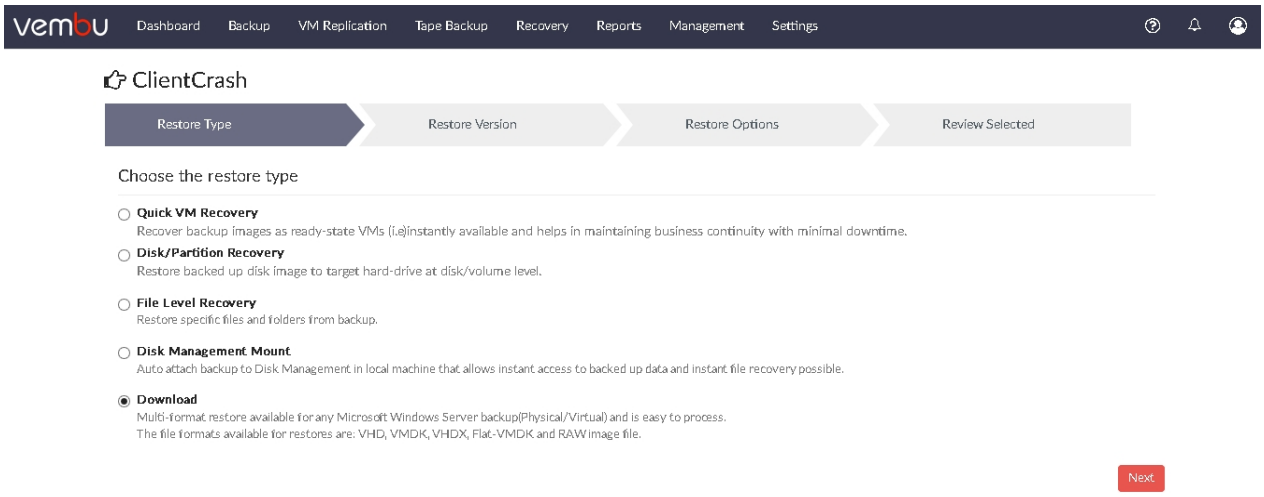
Case 5: Restore Physical Machine as a file type of your choice

- With **Download** option, you can download your backed up physical machine data as an offsite copy to a local destination. You can migrate your physical machines 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
    - Flat-VMDK
    - RAW image file

Procedure

Step 1: Choose the Restore Type

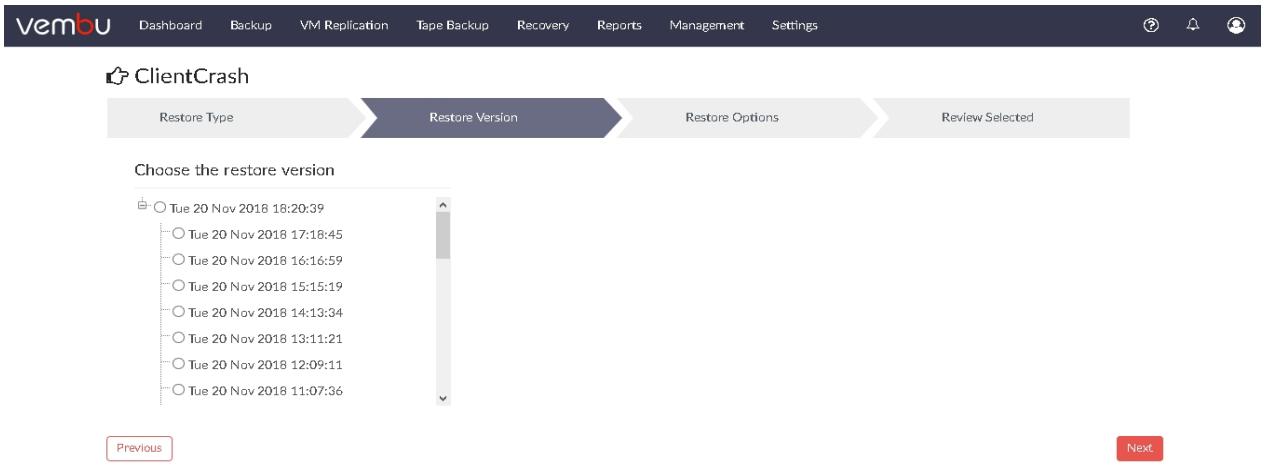
- Click the **Recovery** tab and select the **restore** icon near the Disk Image backup that is to be restored. Select **Download** as the Restore type and click **Next** to proceed with the restore process.



Step 2: Choose the Restore Version

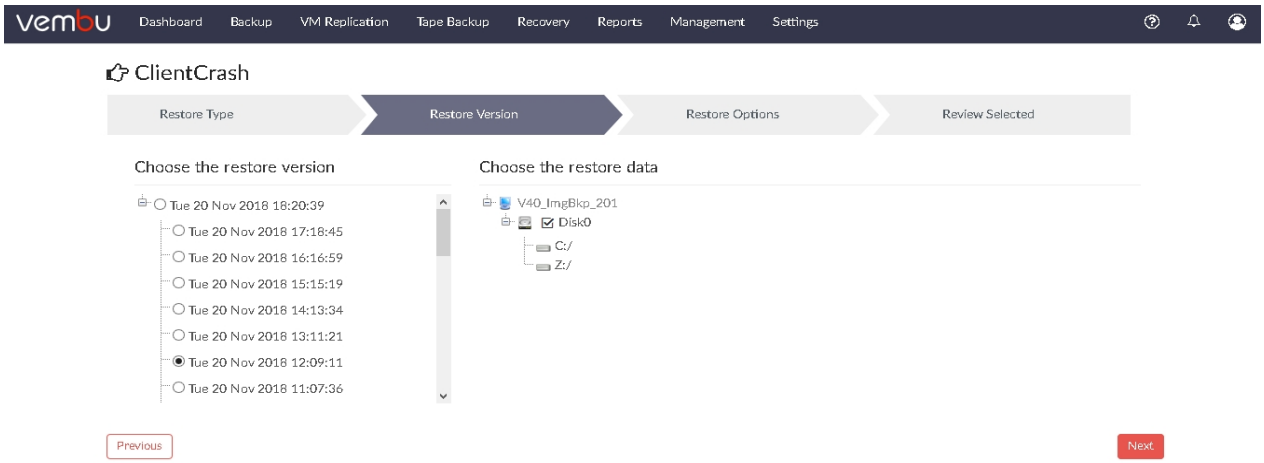
- Select the restore version for the restore process. The restore version is created based on the end time of the backup (i.e the date and time when the backup process scheduled is completed), this is named as **Recovery points**. The full backup and incremental backup timestamps are listed with the 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.
- Once done selecting the time-stamp version, click **Next** to configure the Restore data.

Note: You can select only one timestamp for restore at a time.



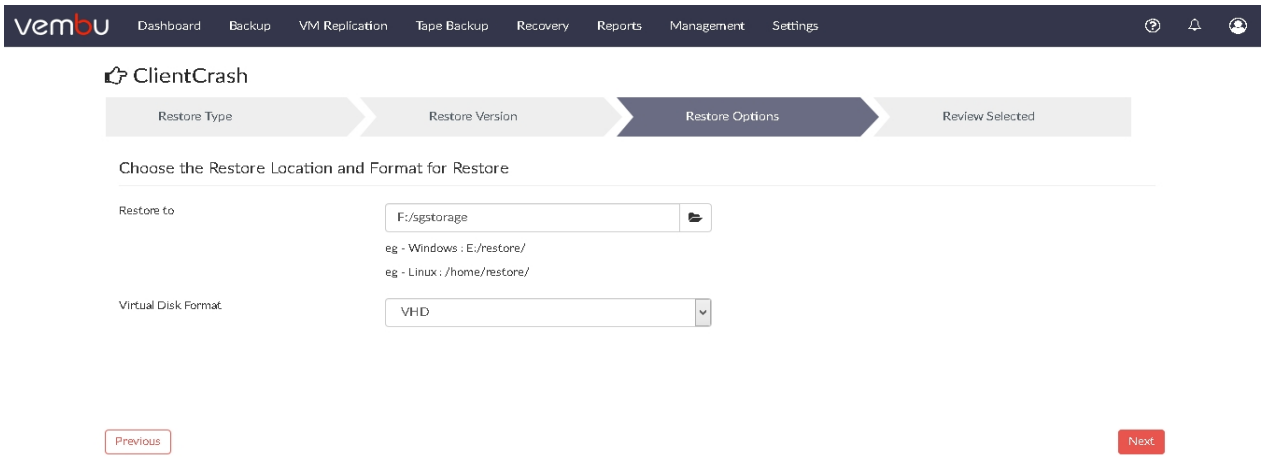
Step 3: Choose the Restore data

- The disks that are backed up will be listed in a structural order. If your backup has multiple disks under it, you can either select all the disks or select only the disks that you need to restore.
- You can view the individual volumes/drives under the disk by expanding the node. You are not allowed to select the volumes/drives under the disks for restore.
- 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.

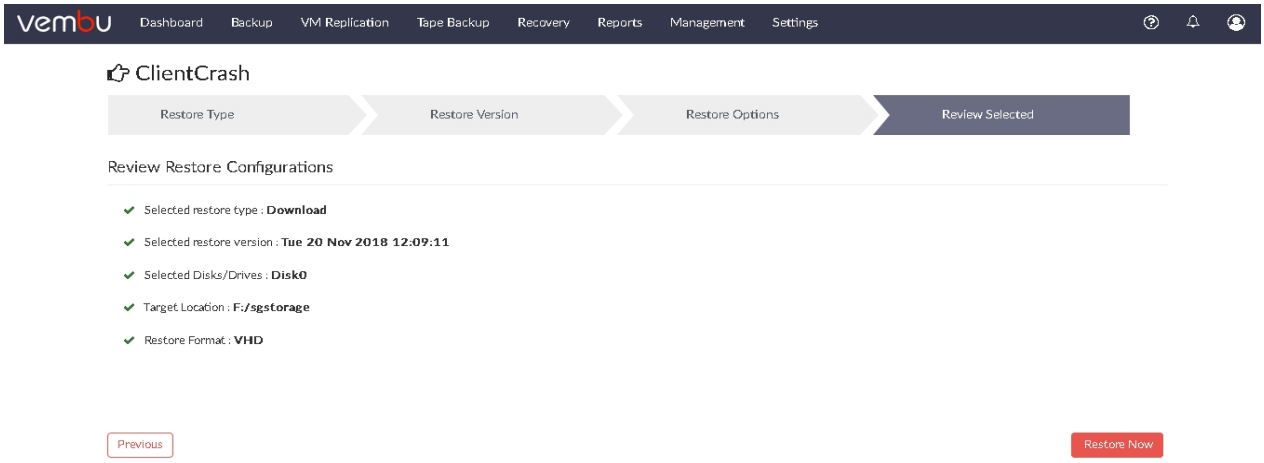


Note: Flat VMDK restore is not supported for Generation 2 Guest OSes with more than 2TB disk.

Step 5: Review Configurations

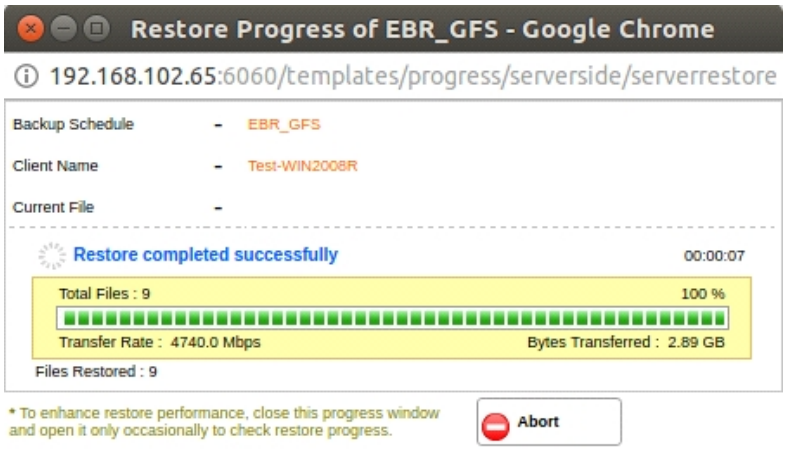
- The final step in this restore process is to review the configurations you have selected.
- Check the following:
  - Restore type
  - Restore version
  - Selected VM Machine
  - Target Location
  - Restore Format

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

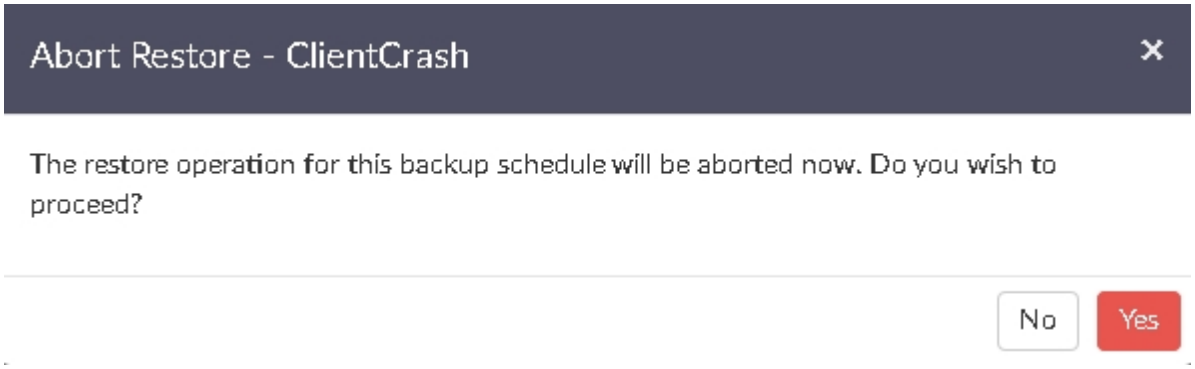


- You will be redirected to the recovery page. In the status tab click the arrow mark which will open the restore progress window.
- The following details will be available in the restore progress page:
  - Backup Schedule
  - User Name
  - Current File
  - Total Files
  - Transfer Rate

- Files Restored

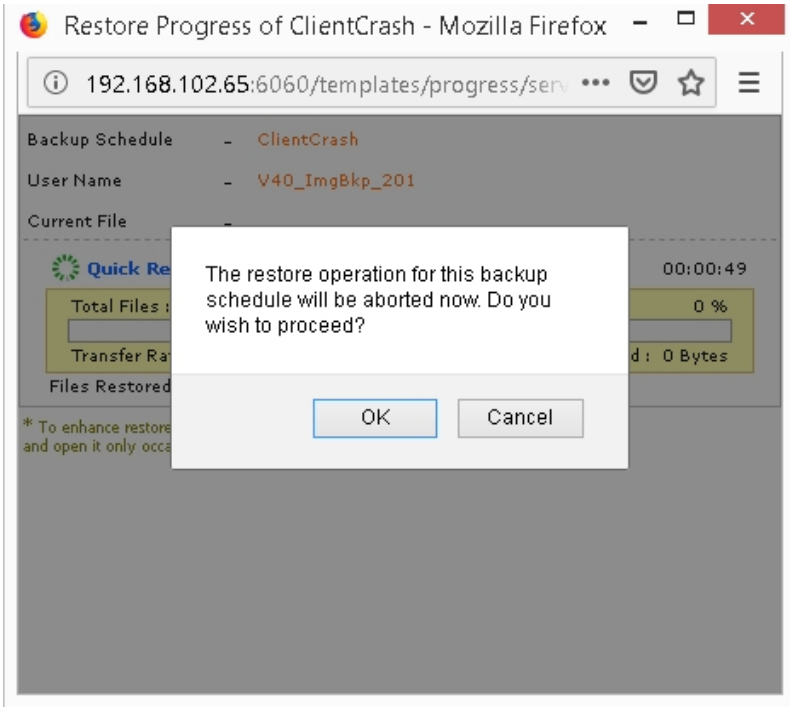


- You have the option of aborting the restore process. From the Recovery page click the **Abort Server Side Restore** option, this will open a pop-up window as displayed below. Click **Yes** to abort the restore.



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

- 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.



Note: You can download any other file format and use it to migrate your VMs to another hypervisor. This downloaded file can also be used for cross-platform migration.

Evaluator's Guide for Windows Servers and Workstations

Case 6: Bare Metal Recovery

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

Note: Dissimilar hardware is not supported

Procedure

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

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

Step 1 - Download VHD:

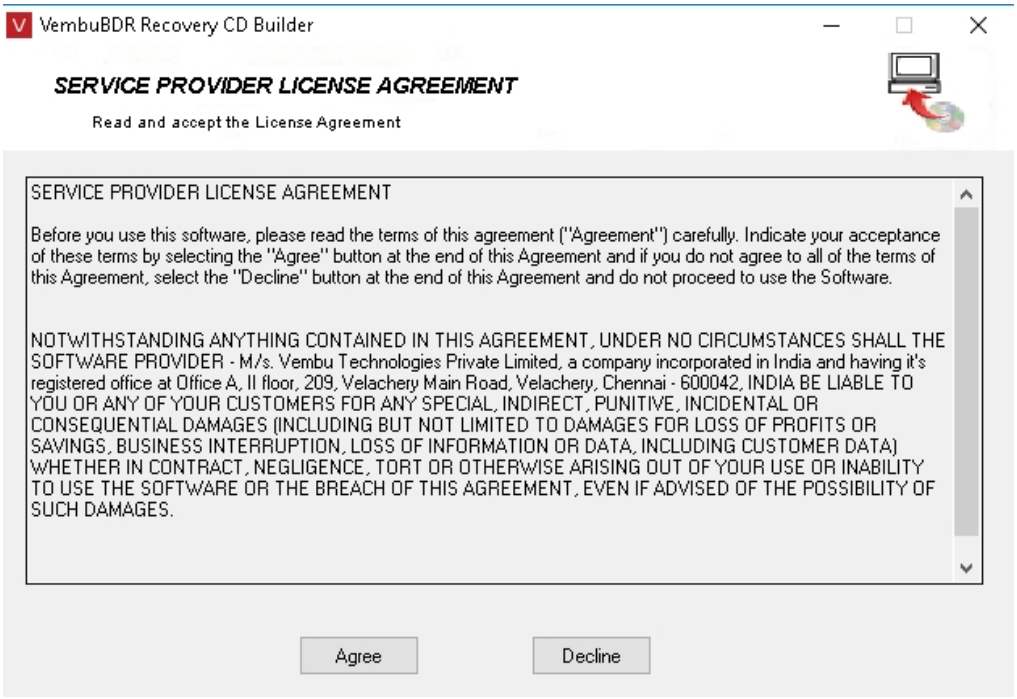
- Proceed with Download under Recovery options and choose VHD as your virtual disk format - Click Here to know the step by step process to download.

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

- To do Bare-Metal recovery using Vembu Recovery CD, download and install Windows AIK or ADK:

- Click on following link to download Windows AIK: Click Here
- Click on following link to download Windows ADK: Click Here

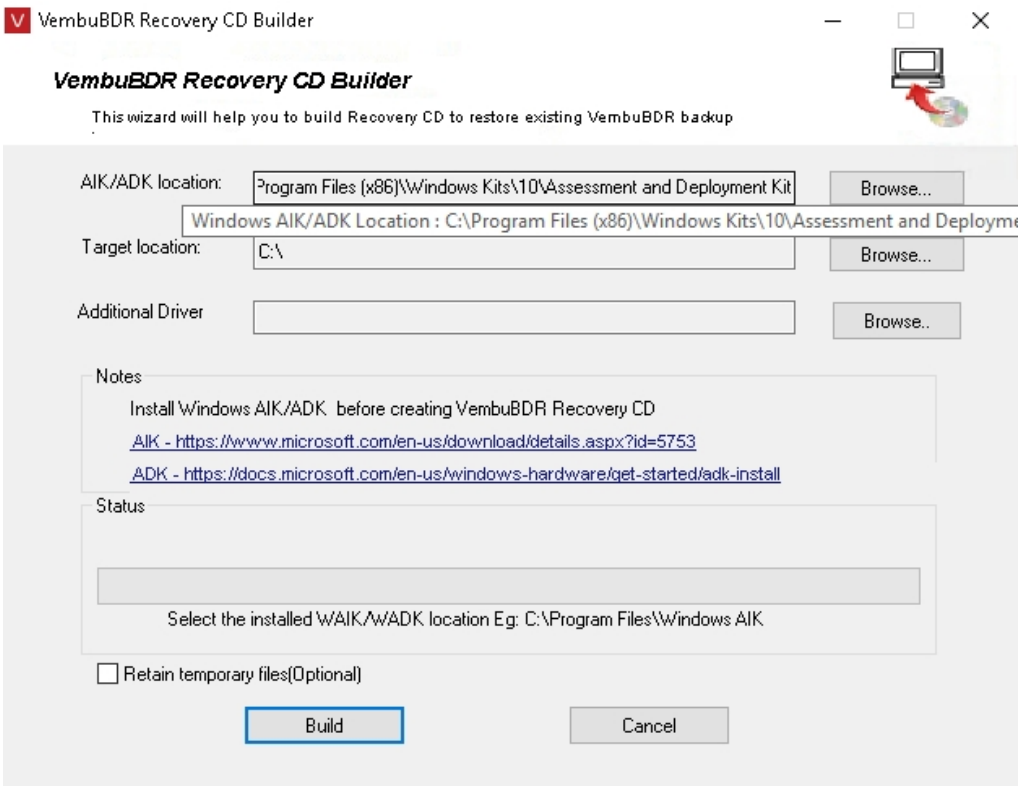
- Once Windows AIK/ADK is installed, download Vembu Recovery CD: Click Here to Download
- You will have Vembu Recovery CD in both 32-bit and 64-bit zip formats, download accordingly based on requirement. Now unzip the downloaded file and run RecoverCDBuilder with administrator privileges. You will get a window opened as displayed below.



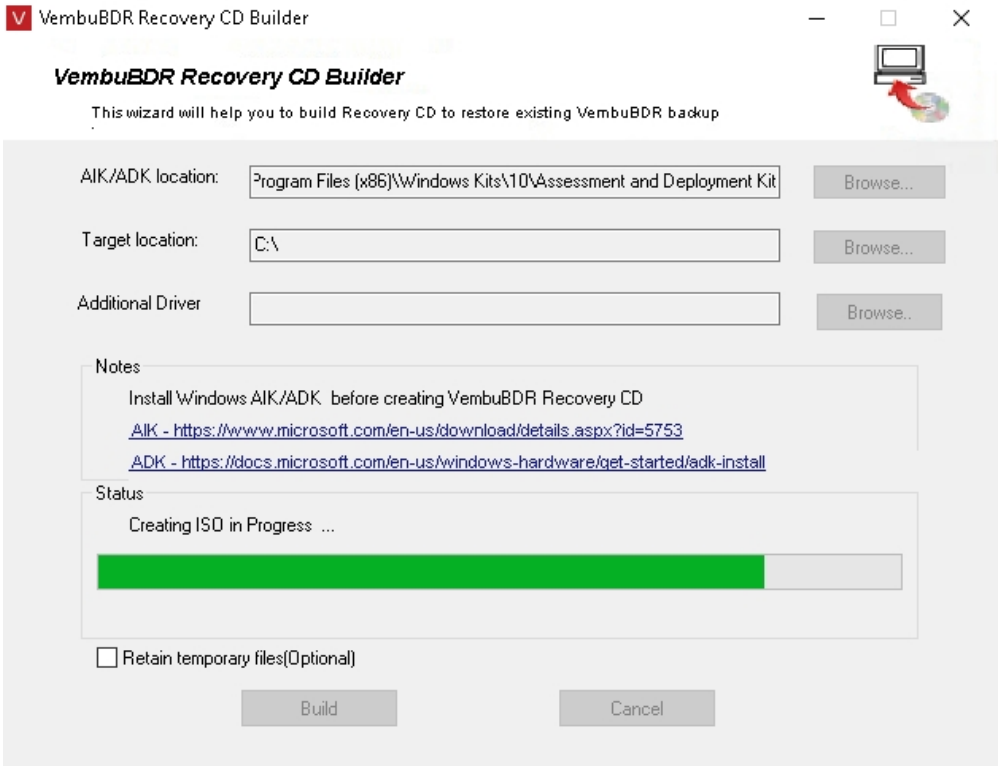
Step 2 - Create Vembu Recovery ISO file:

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

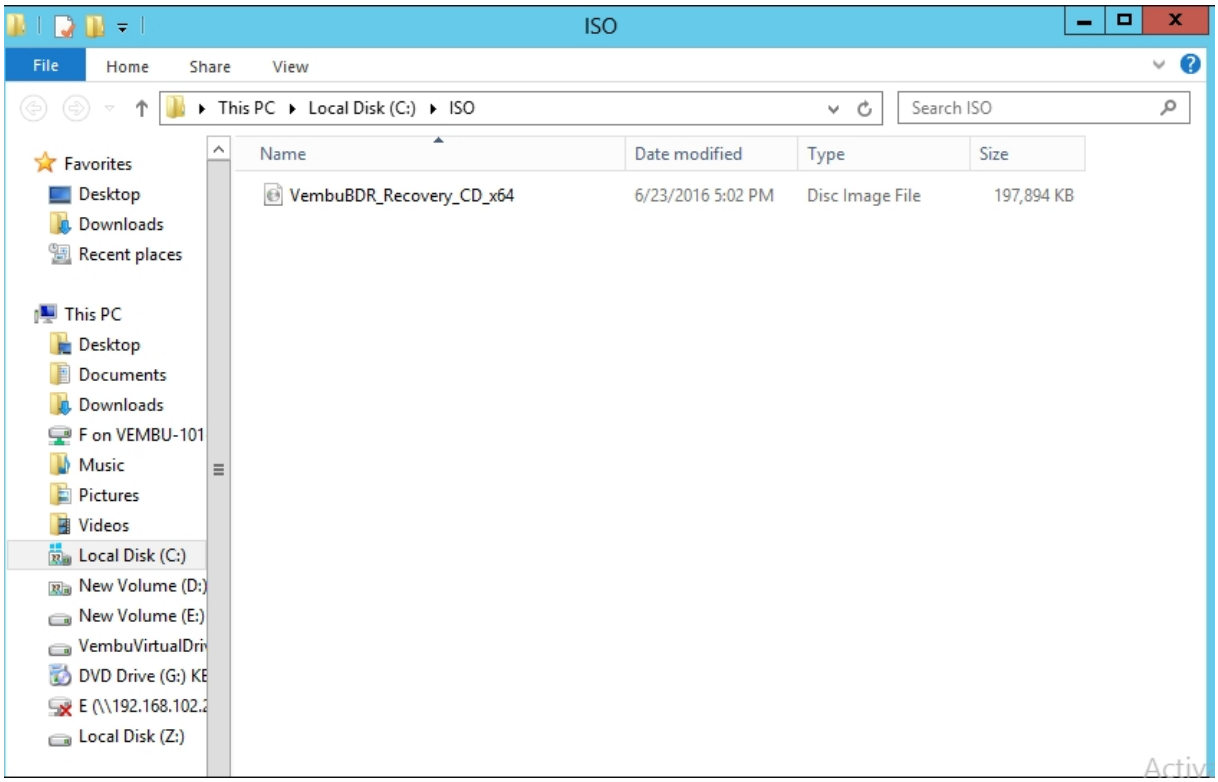
Note: When you have RAID and additional drivers to be set up in the machine to be recovered, such drivers can be bundled with Vembu Recovery CD using 'Additional Driver' option.



- In this window, AIK/ADK location will be auto-filled, the target location is the location where you want to store ISO. Click **Build** to start creating an ISO file. You can monitor the progress of ISO creation.

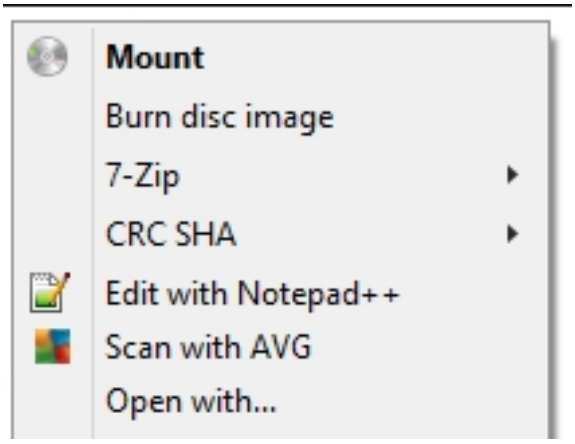


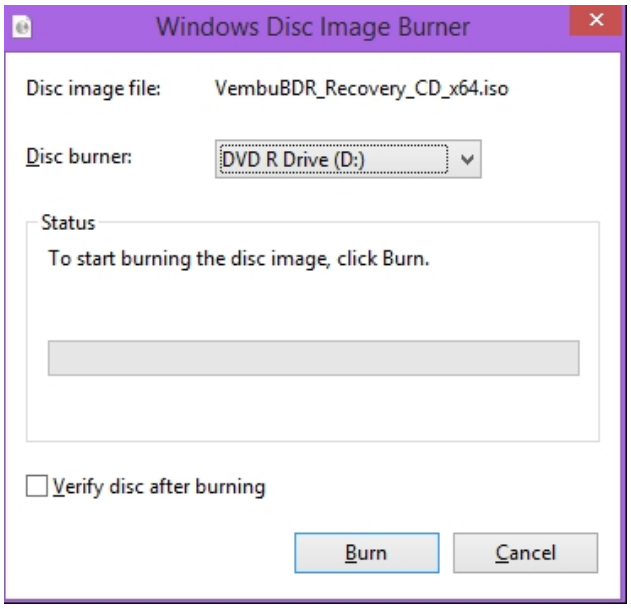
- Once done, the ISO file will be available in the Target location you have entered.



Step 3 - Burn ISO file to a CD/DVD:

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





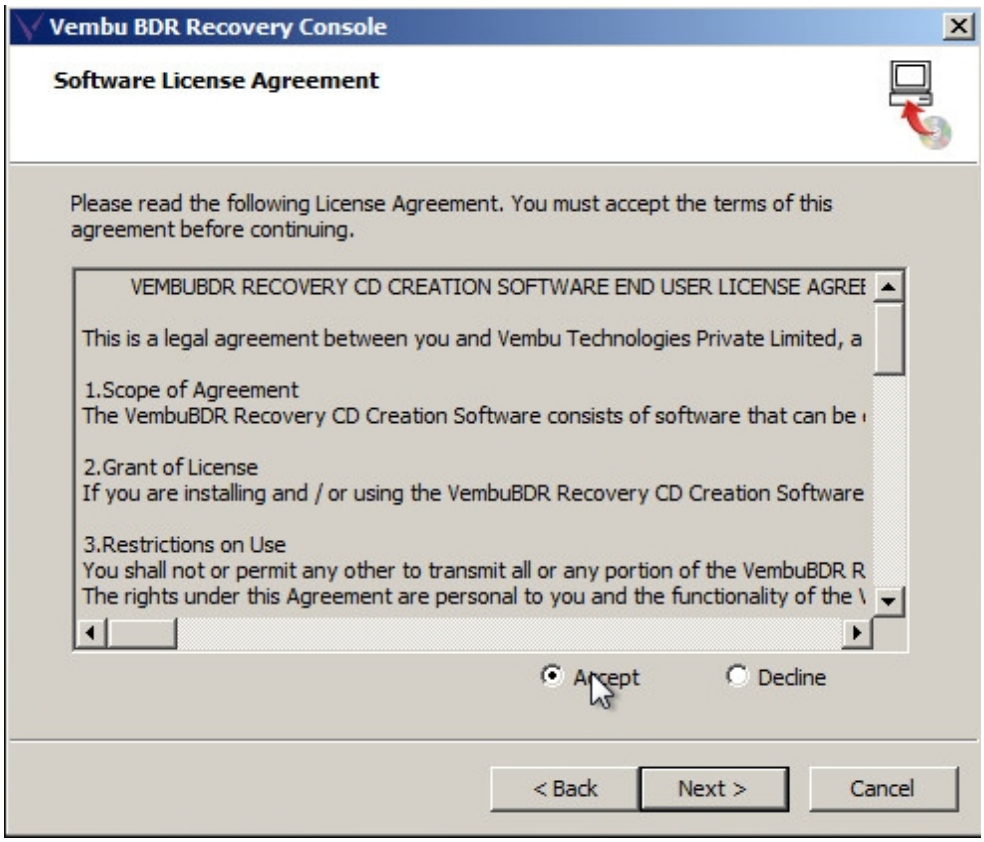
- You can monitor progressing of the burning process.

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:

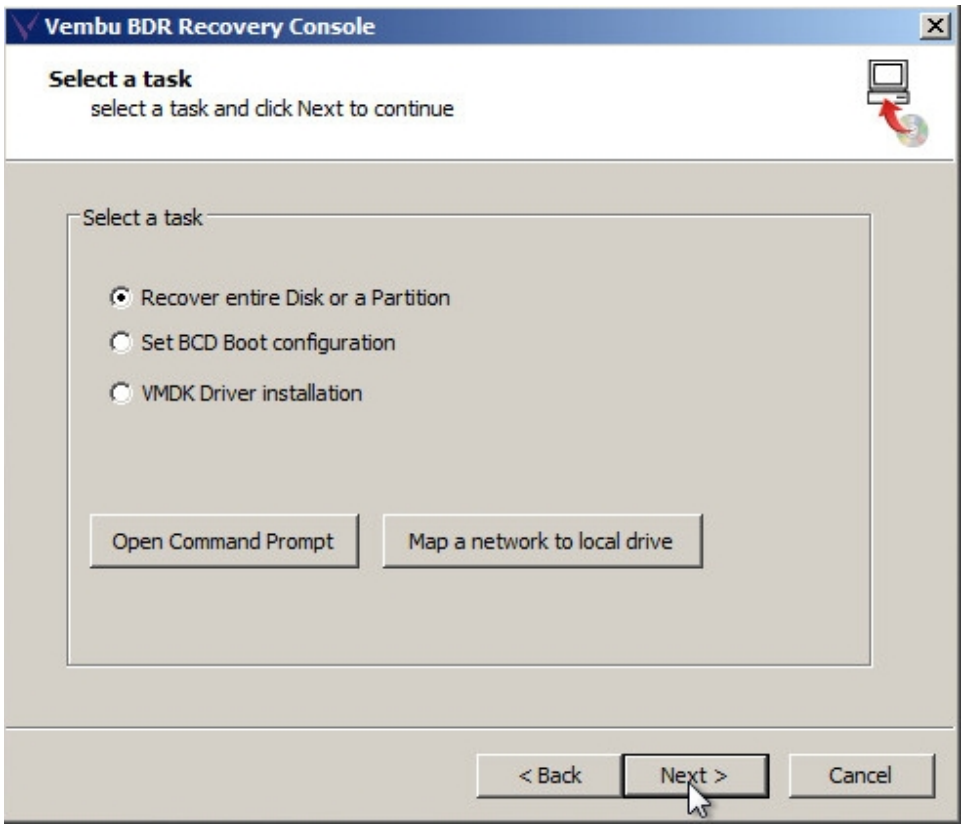
- Read the Software License Agreement carefully, click **Accept** and proceed with **Next.**



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

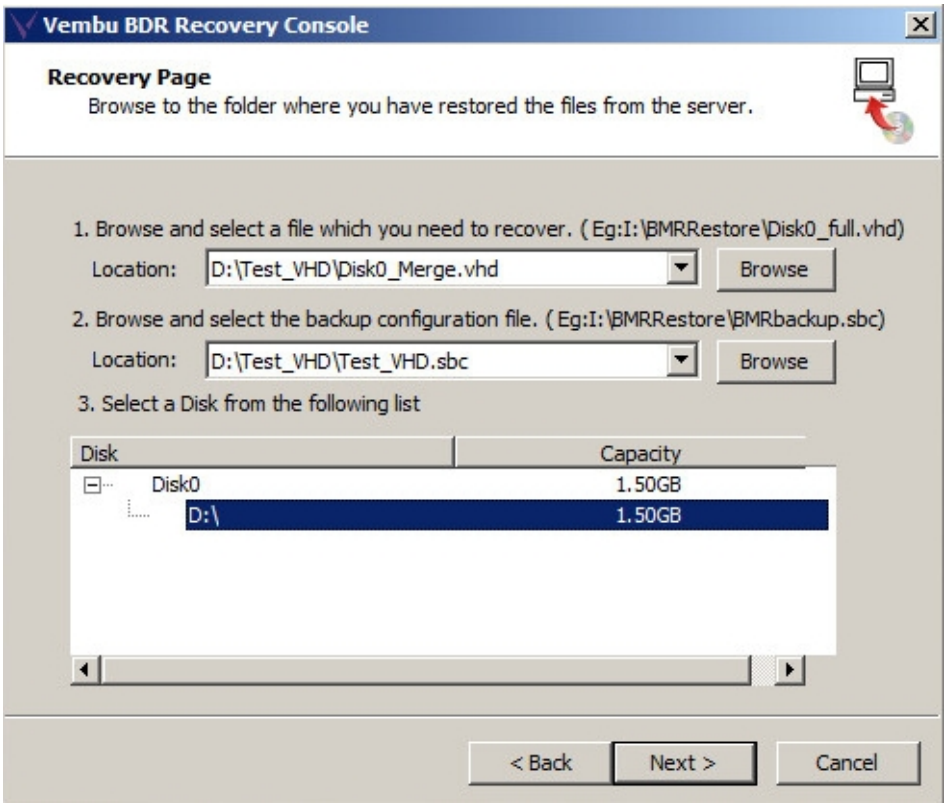
Since we have to do physical recovery, proceed with **'Recover entire disk or partition'** option and click **Next.**



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.

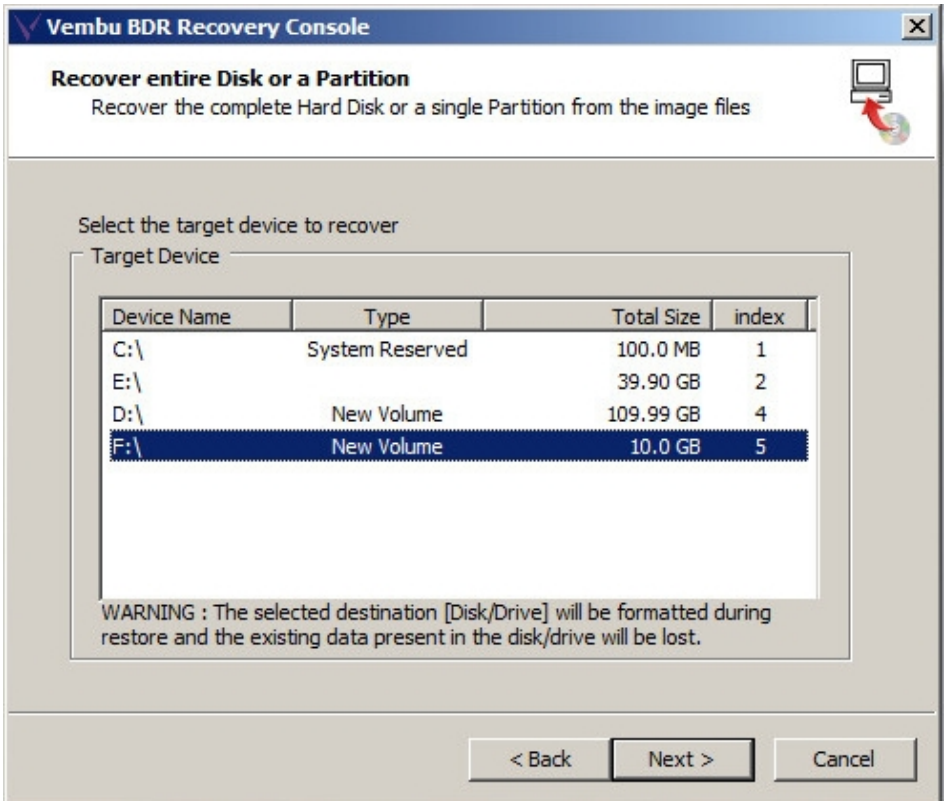
  Once done choosing respective requirements, click **Next** to proceed.



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.

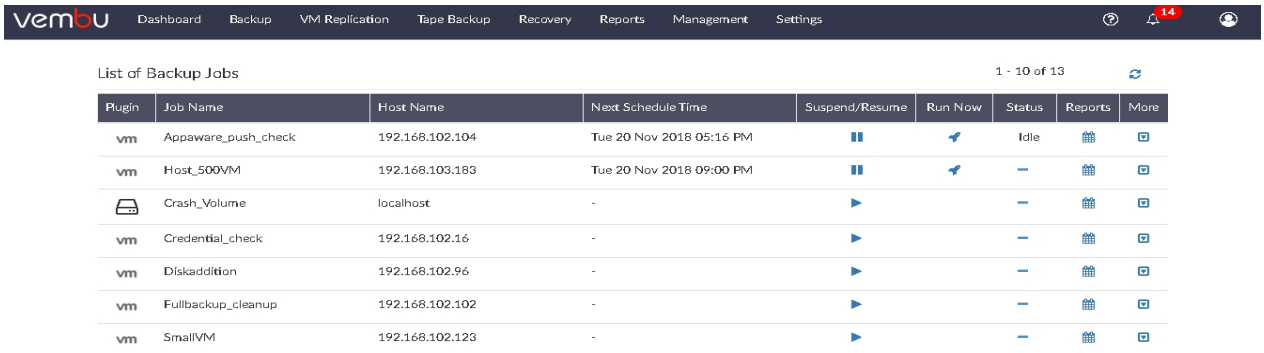


- The recovery process will be initiated and once it is completed successfully, you can find your recovered data in the target disk/drive selected.

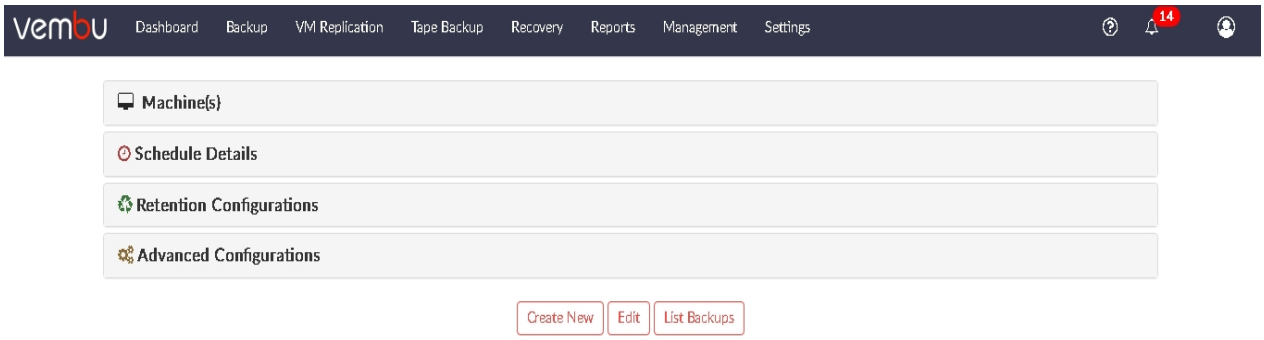
Evaluator's Guide for Windows Servers and Workstations

Manage Backup Job

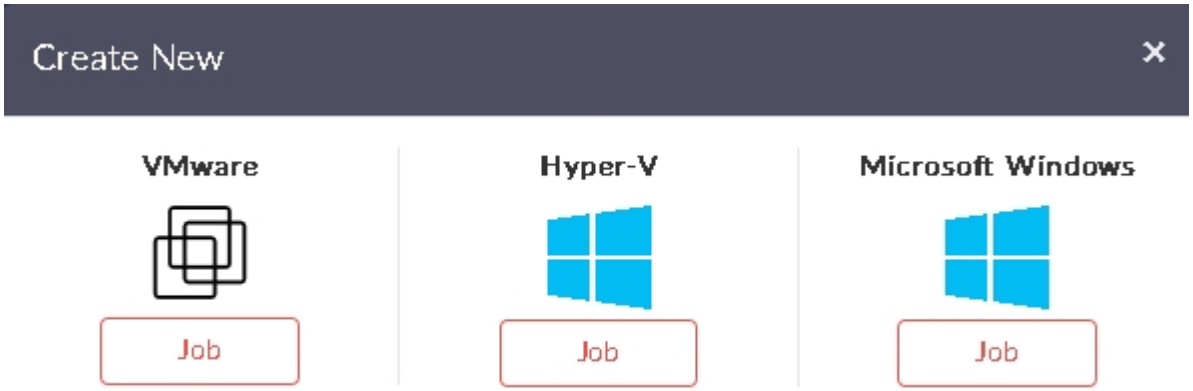
- Once you have configured a backup job, you will be redirected to the **List All Jobs** page. This page page acts as a central hub to all the backups and will list the backups that are configured to and from the Vembu BDR server.
- You will find the list of all the backup jobs you have configured, along 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



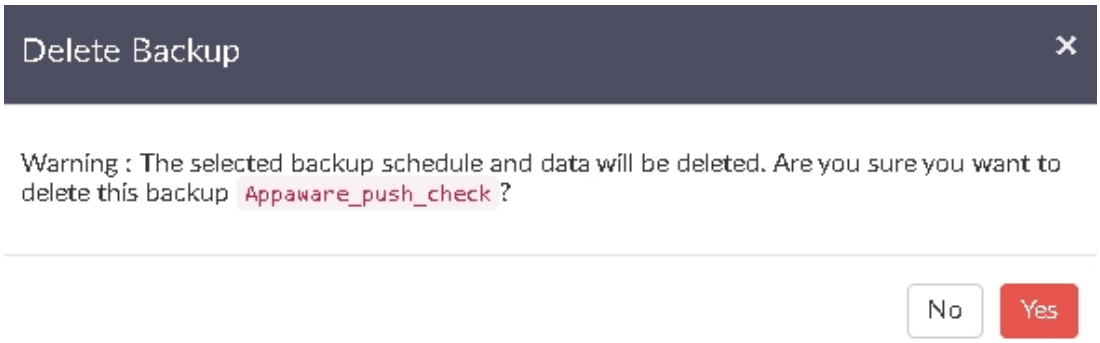
- You can create a new backup job by selecting the **Create New** option. The pop-up window displayed below will be avilable.



- **Edit** - Reconfigure the entire backup job by changing
  - VMs to be backed up
  - Exclusion Settings
  - Application Aware Process
  - Schedule frequency

- Additional Full Backup
- Retention Count

- **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.



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

Evaluator's Guide for Windows Servers and Workstations

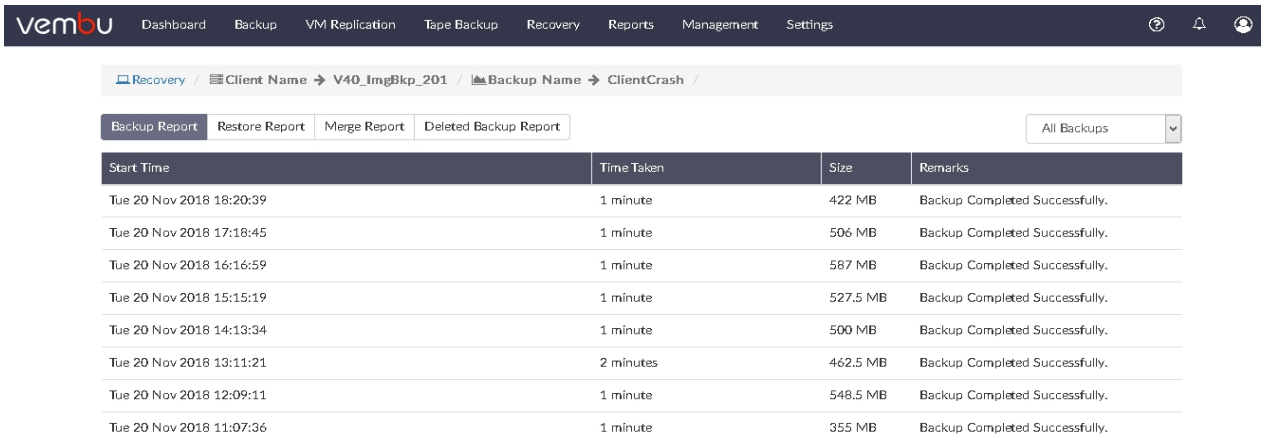
Reports

- Vembu offers three types of reports in the Vembu BDR Server web console delivering extensive information about the backup/restore jobs and their status.
- There is an option which when configured delivers reports that you require, directly to your inbox on a regular basis.
  - Backup Job
  - Backup Status
  - Image Integrity
  - Email Configuration Reports

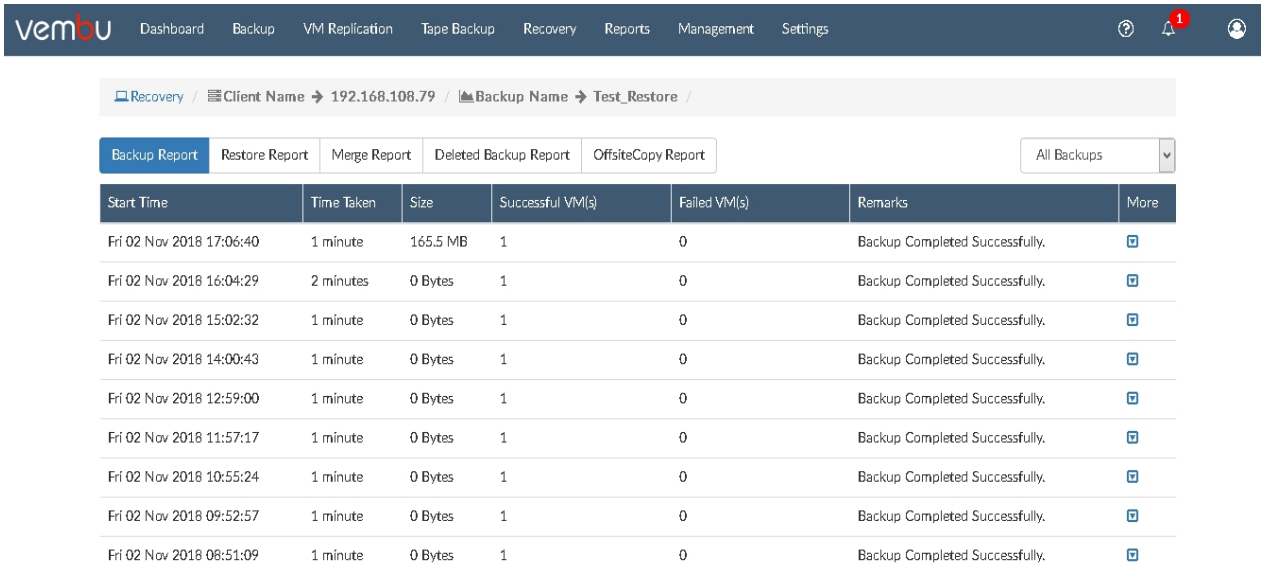
Evaluator's Guide for Windows Servers and Workstations

Backup Job Report

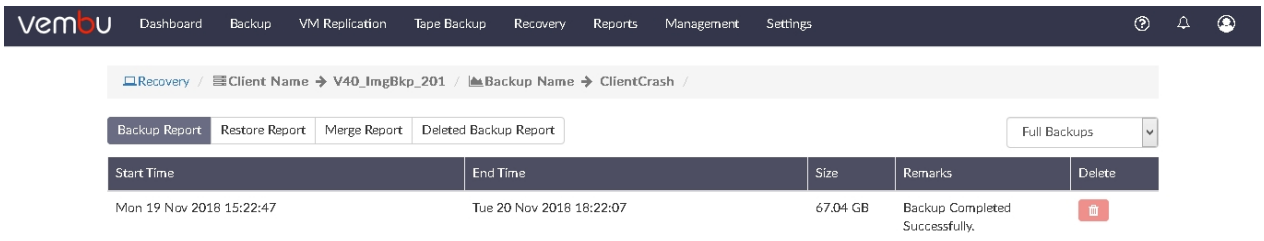
- Open the **Recovery** tab. This page lists all the backup jobs configured to the Vembu BDR server where you can see a report option alongside every backup job. Click the **Reports** icon.



- 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



- 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 Windows Servers and Workstations

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:

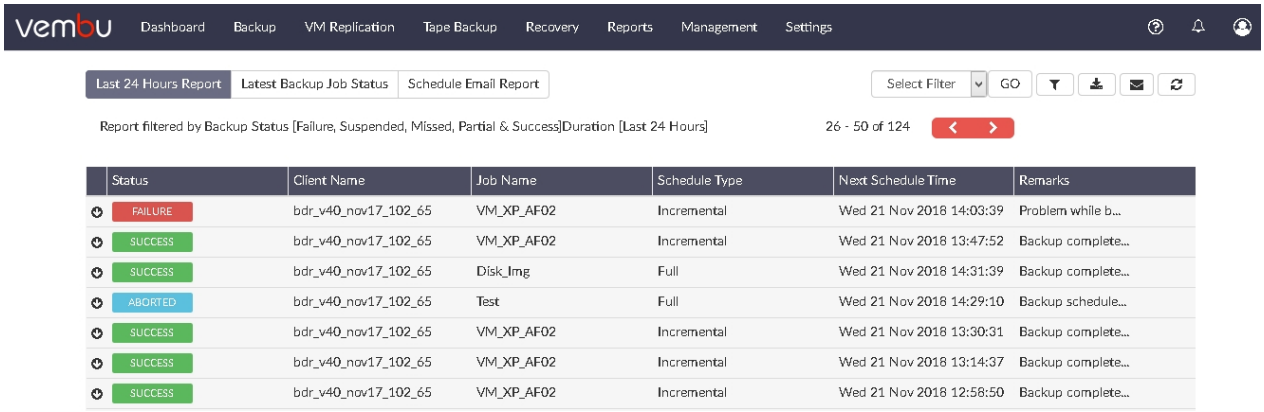
- **Successfully Completed** - Backup job completed successfully
- **Failed** - Backup job failed due to an error. The reason for the backup failure will be listed in the report
- **Missed** - When there is an error in the connection between the server and the target
- **Suspended** - When the backup 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
  - Plugin Type

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

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



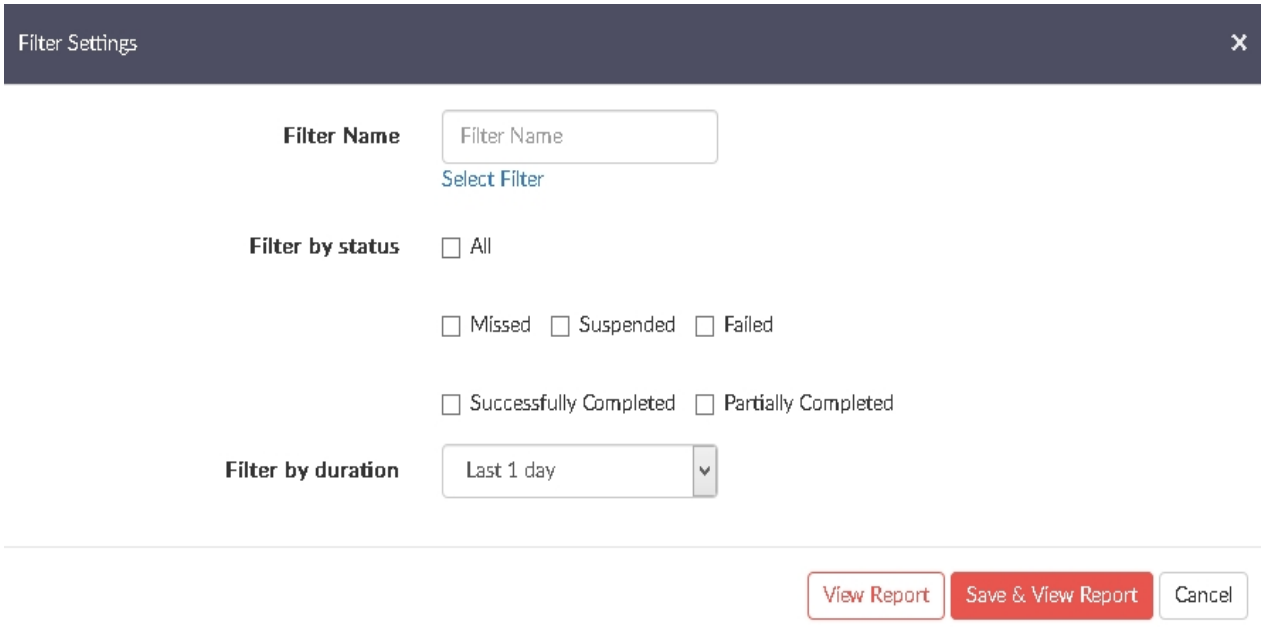
- The second tab, **Latest Backup Job Status**, lists the status of the latest backup job across all timestamps.

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

- 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:

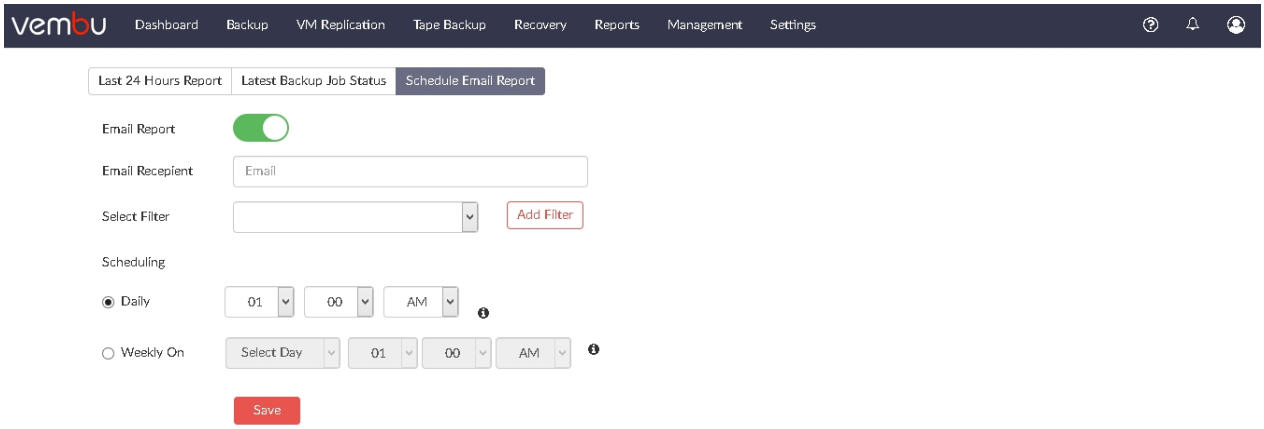
- Filter option lets you add custom filters wherein you can apply a filter of your choice for ease of view.
- The backup filter includes the following statuses to choose from: missed, suspended, failed, successfully completed, partially completed.
- Filters can also be applied based on duration. Provide the custom data range, apart from ranging between last 1-30 days.
- Click **View Report** option to view the report immediately based on the filter you have configured. Click the **Save & View Report** to save the filter you have configured and then view the report.



- 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

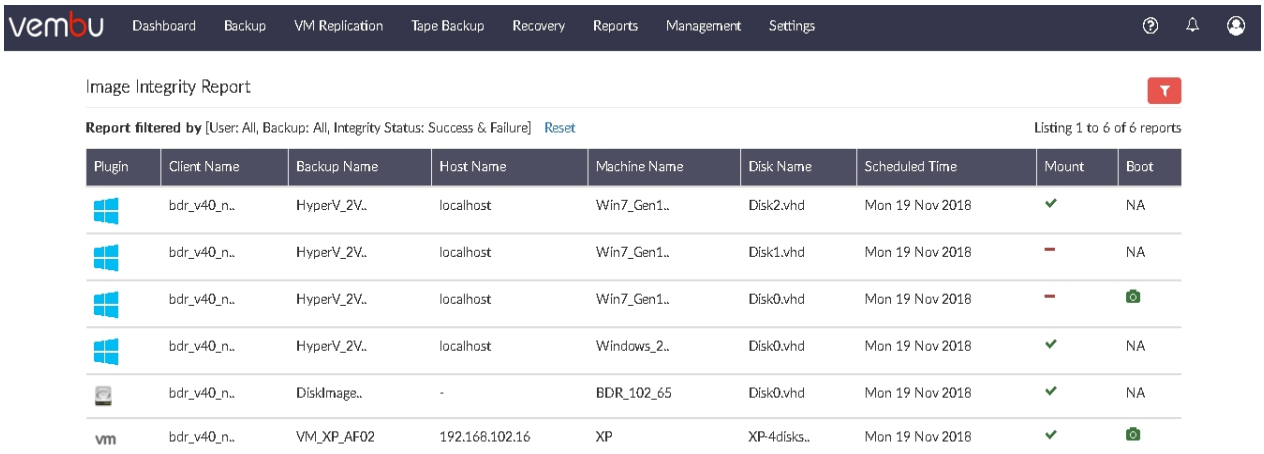
- Click **Save** option once you have provided the required details.



Evaluator's Guide for Windows Servers and Workstations

Image Integrity Report

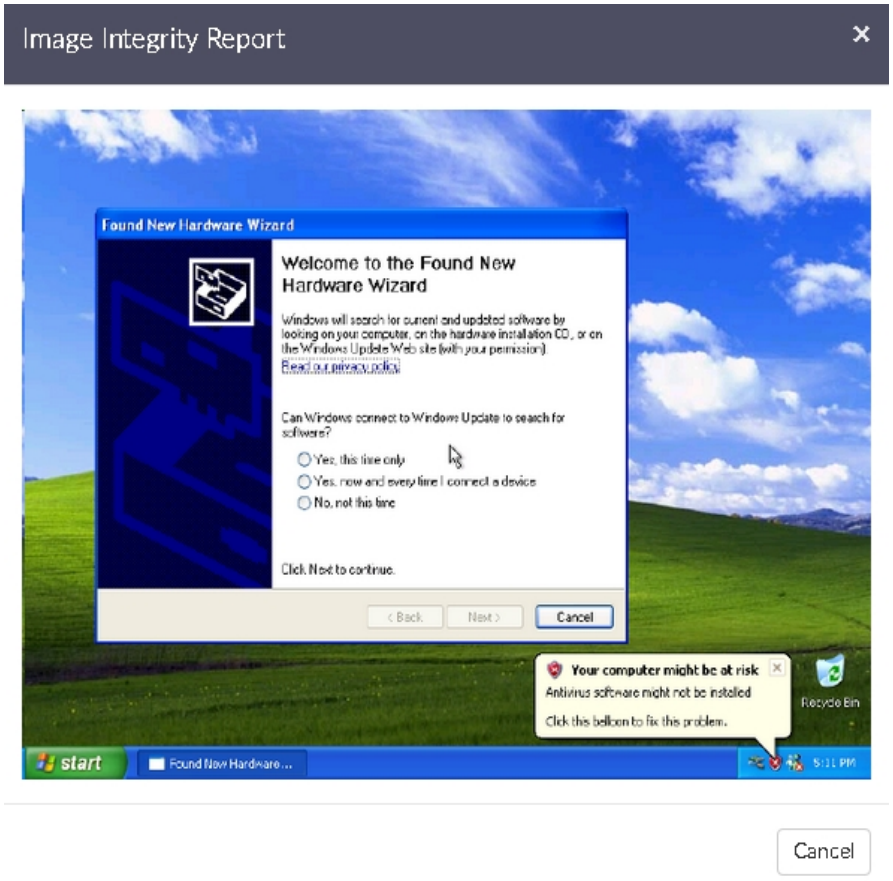
- The Image Integrity Report verifies the recoverability of the backup job. It confirms if the backup data is mountable and provides boot image of the most recent backup. This ensures that the backup is in a readily-bootable state.
- The Image Integrity check will take place once the first Incremental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



- 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:

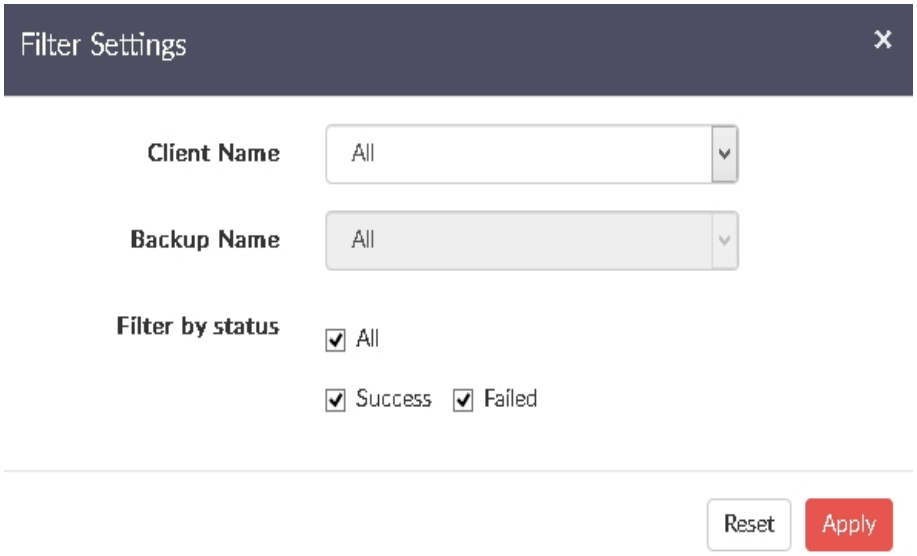
You can also configure **Email alert** for Image Integrity Report, you will receive a mail of Image Integrity report along with a boot image copy.

- 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.



Evaluator's Guide for Windows Servers and Workstations

Email Configuration Report

- 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 while configuring an Email Report. This will help in addressing different use cases.

Evaluation Cases:

- Case 1
- Case 2

Evaluator's Guide for Windows Servers and Workstations

Case 1

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

Prerequisites

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

Procedure

Step 1: Enable Email Configuration

- To configure open the **Management** tab, choose **Settings** - **Email Settings** and select the

Email Configuration option.

- By default, Email Configuration option will be disabled, Enable the **Change Email Configuration** option.

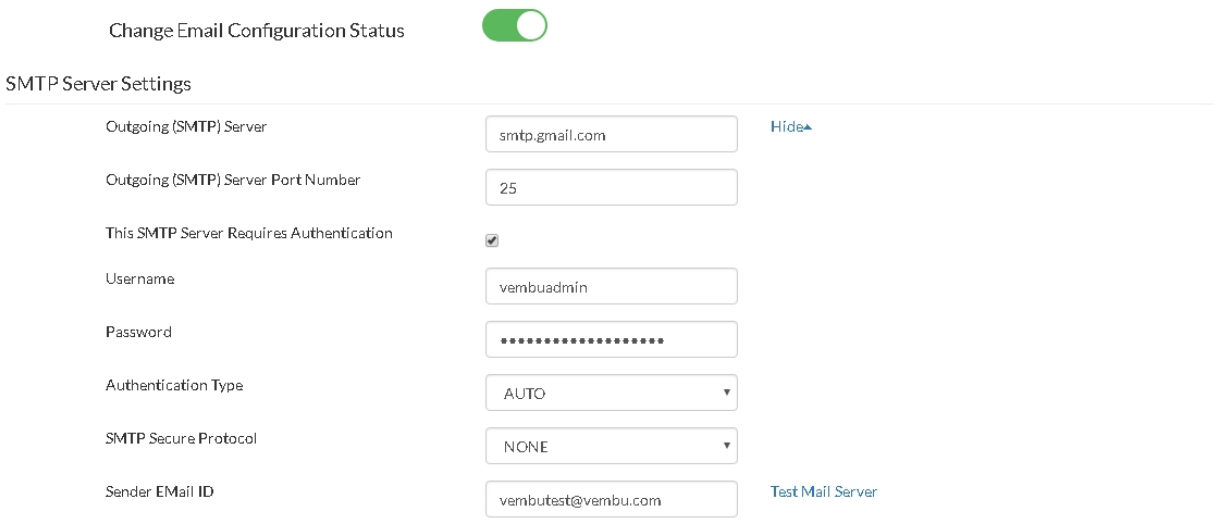
Step 2: Configure SMTP Server Settings

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

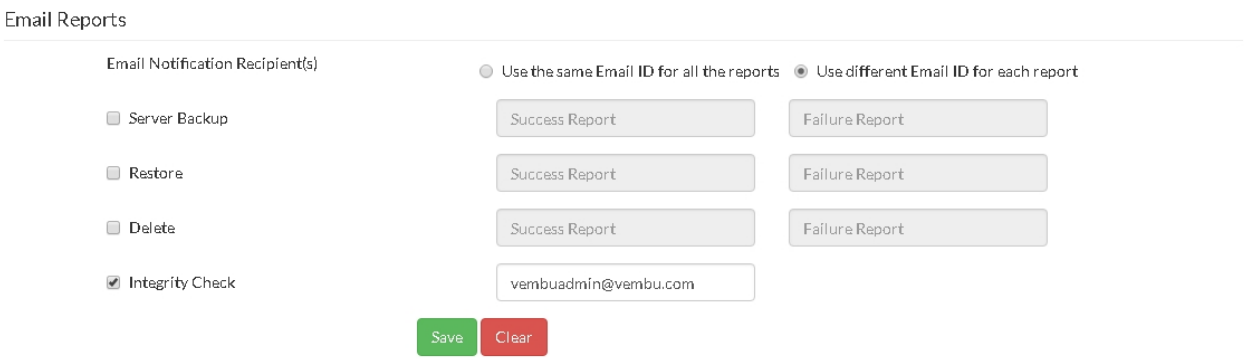
If your SMTP Server requires authentication, enable the **This SMTP Server Requires Authentication** checkbox and enter the following details:

- **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** - Provide 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. Enter 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 Windows Servers and Workstations

Case 2

- Schedule a report that has to be mailed to your inbox E**very Monday** at **09:00 AM**. The report should list all the **Suspended** and **Successfully** completed backup schedules in the **last 2 days**.

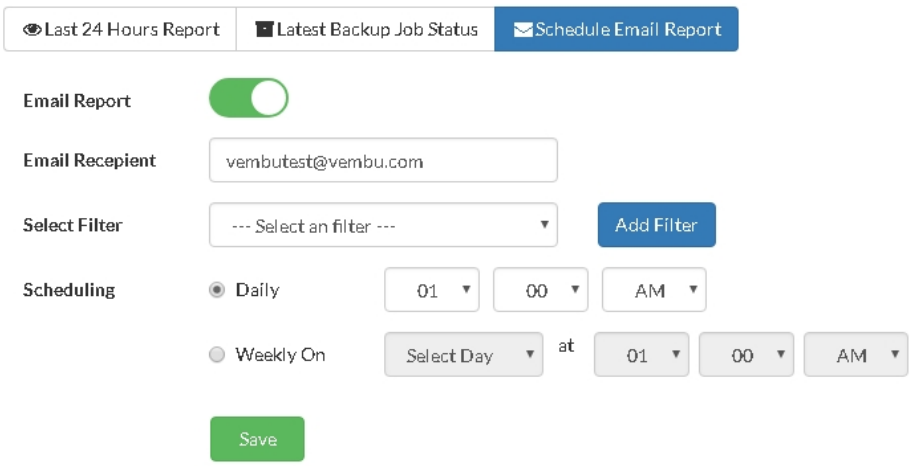
Prerequisites

- 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.



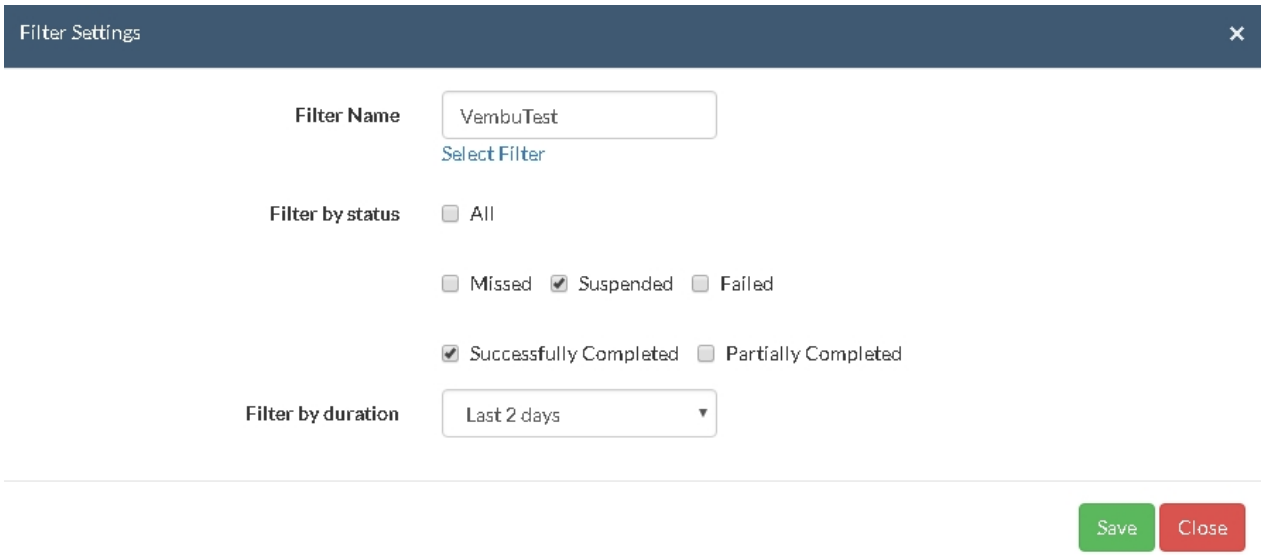
Step 2: Configure Schedule

- 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 that has to be mailed 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 then **Save** the email schedule page.

Evaluator's Guide for Windows Servers and Workstations

Portal Registration

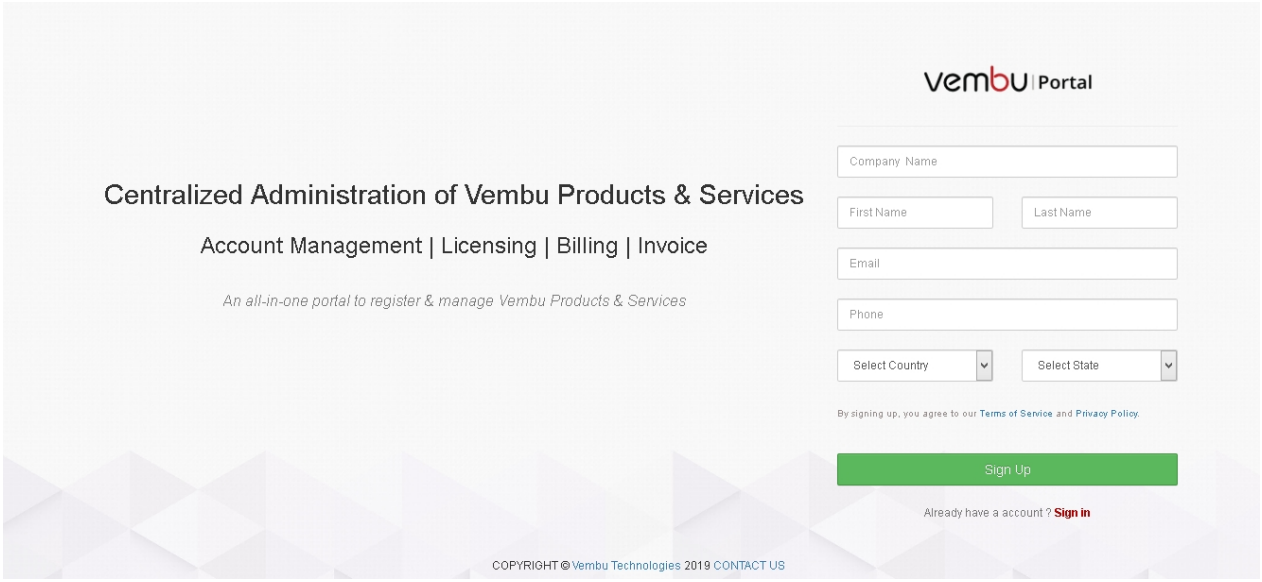
- You must create a Vembu Portal Account to register your backup server with Vembu Portal. Through the Vembu Portal you can manage all your Vembu products and services.

Creating a Vembu Portal Account:

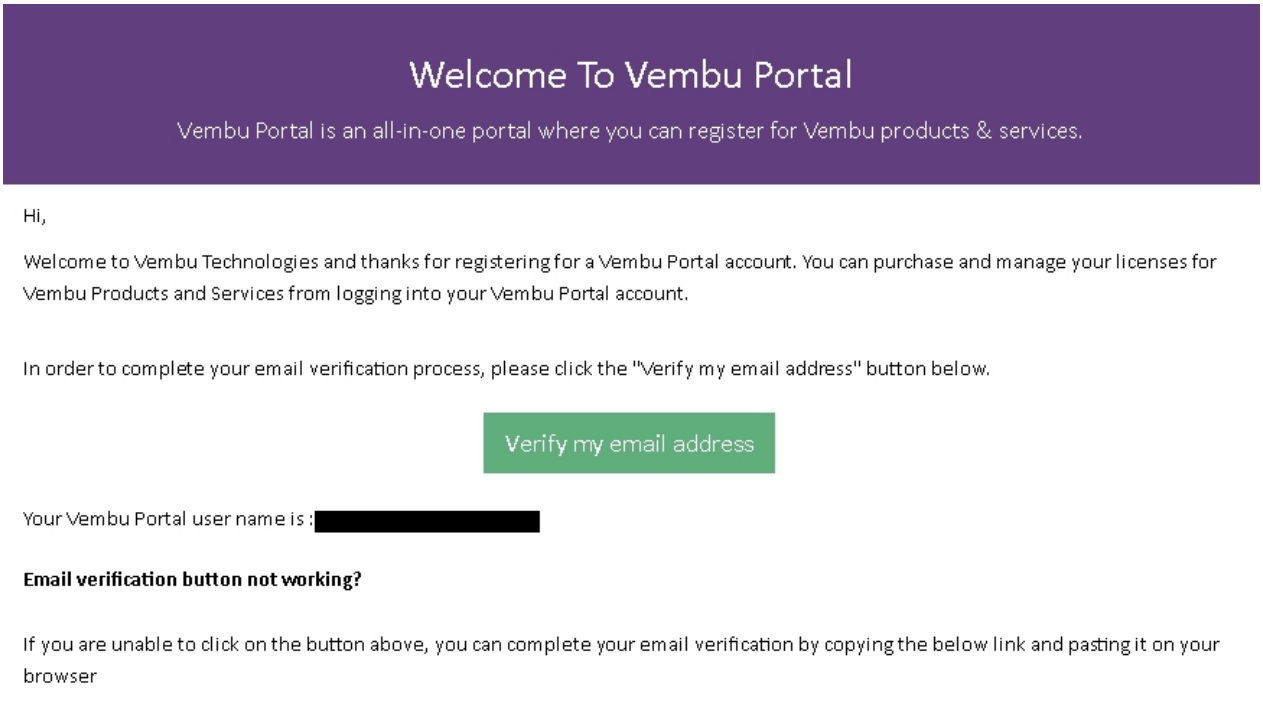
Vembu Portal is an all-in-one hub spot for managing your registered Vembu products and services where you can get started. To register in Vembu Portal, follow the steps given below:

- Open the URL - portal.vembu.com and click the **Sign Up** option.

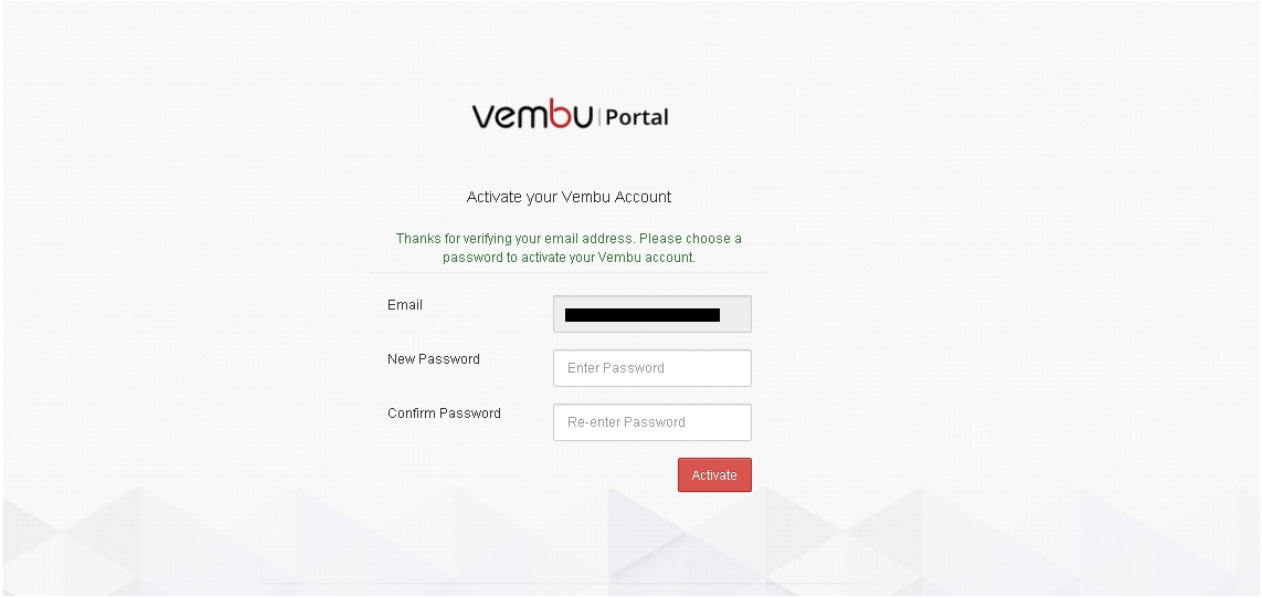
- Provide the following details to create your account:
  - Company Name
  - First Name and Last Name
  - E-Mail
  - Contact Number
  - Country and State



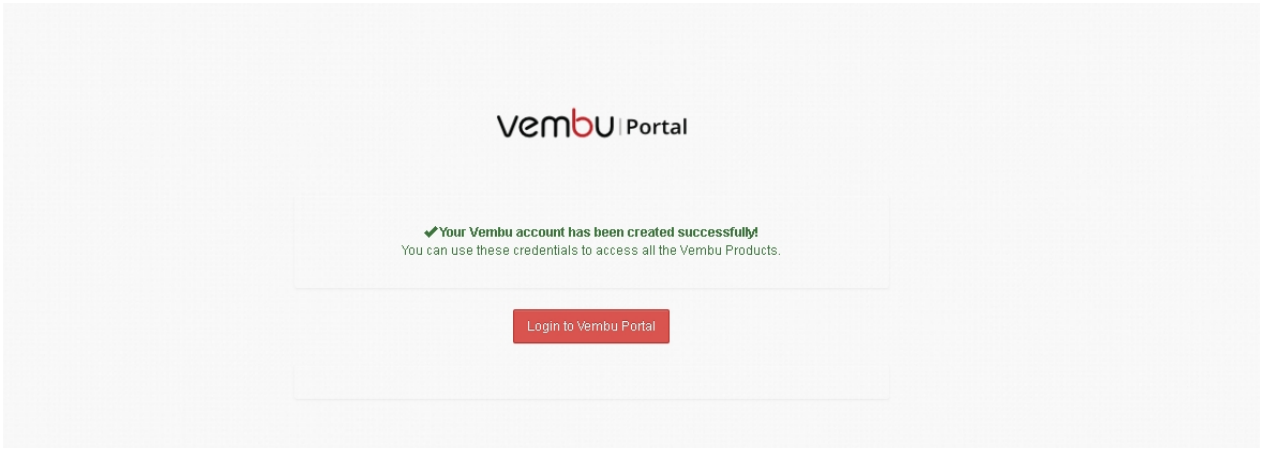
- Click the **Sign Up** option once you are done filling up the requested details.
- A verification E-Mail will be sent to the registered E-Mail ID. Check your Inbox or your Spam folder, if not found in Inbox) for the verification E-Mail and click **Verify my email address** option. If the button doesn't work copy-paste the link given below the 'Verify' button in your browser.



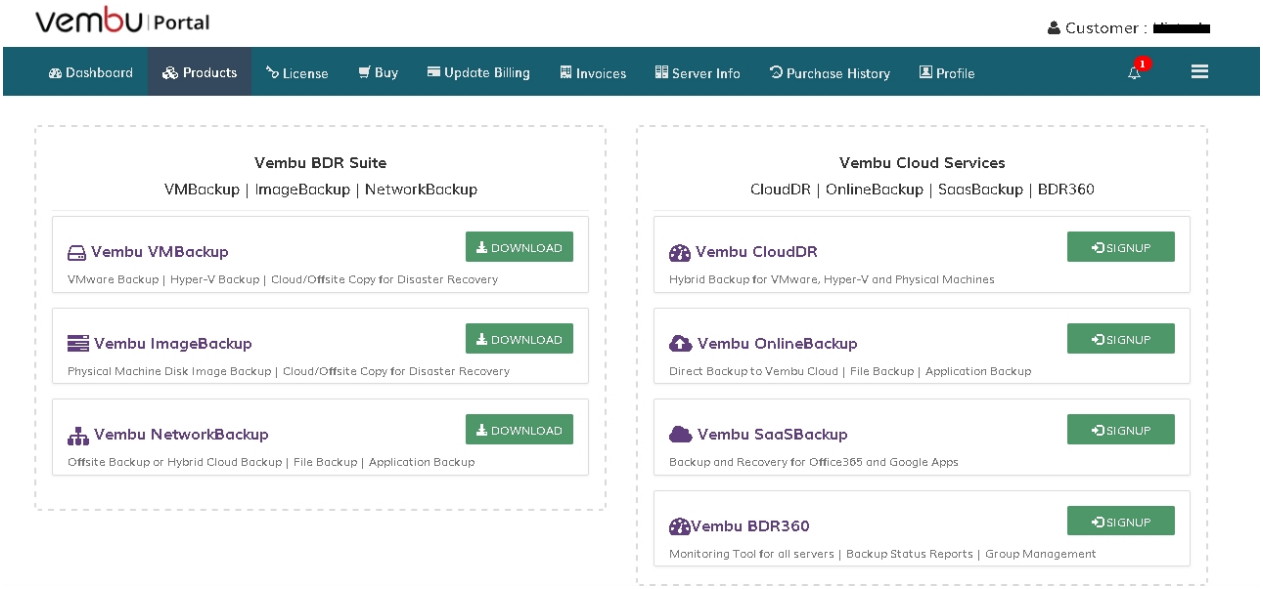
- You will be directed to a page with the registered E-Mail ID. You must create a password for your account. Enter the password of your choice and click **Activate**.



- 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.



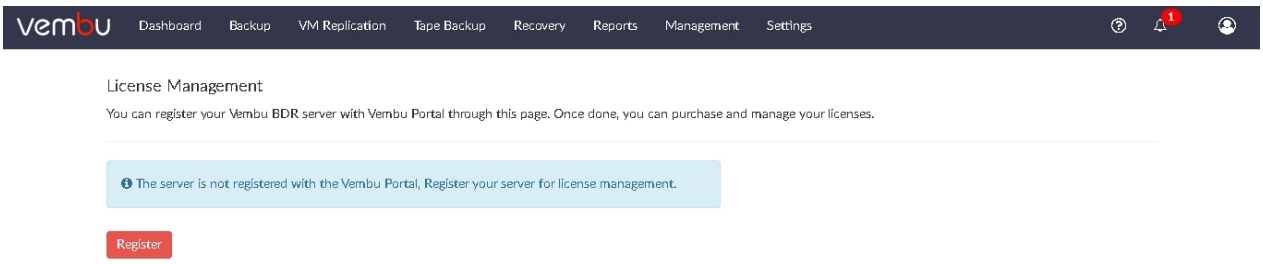
Server Registration

Once your Vembu Portal account is created

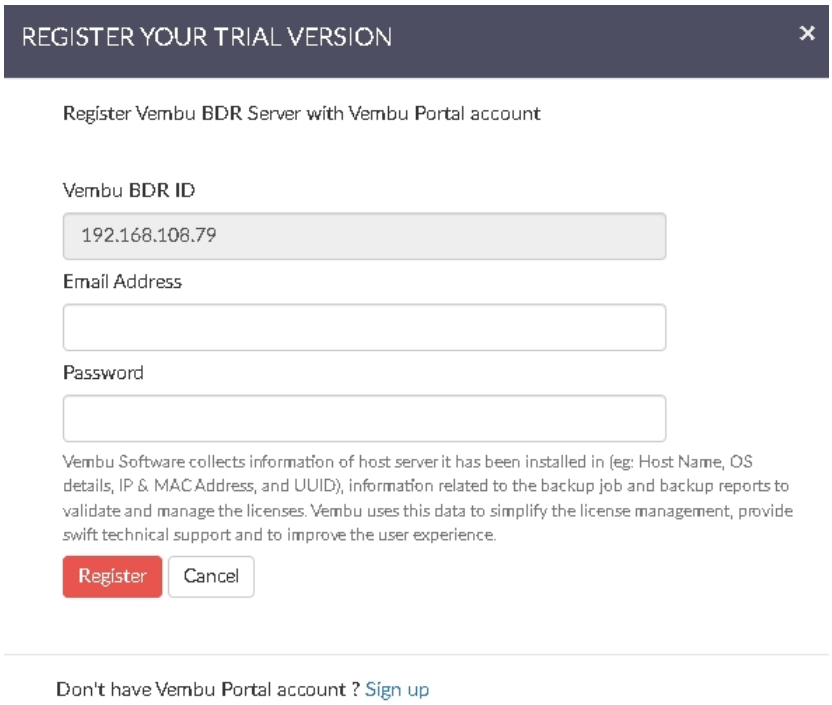
- Login to BDR Backup Server Web-Console.
- Go to **Management** tab and select the **License** option.

Registration Steps:

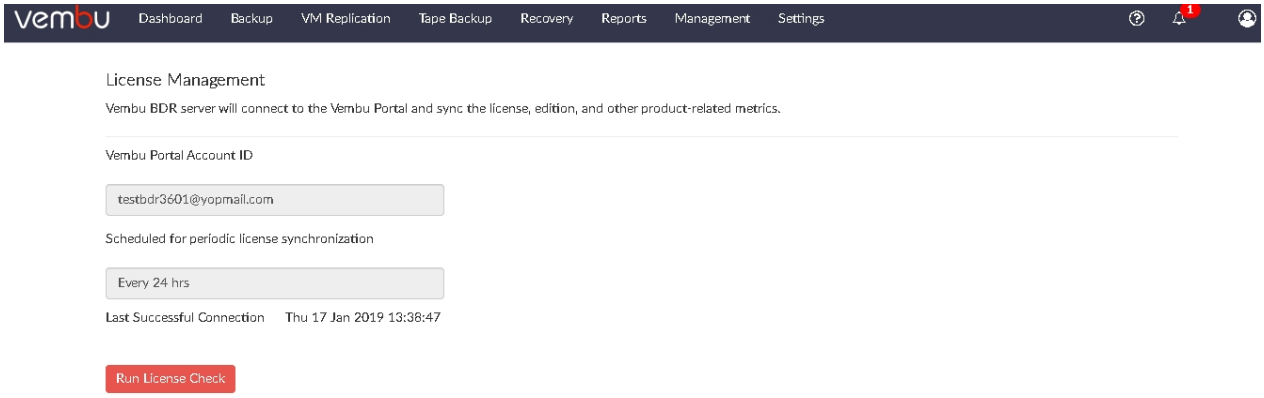
- In the License Management page, click the **Register** option.



- Provide the Email Address and Password in the pop-up shown and register the trial.



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



Evaluator's Guide for Windows Servers and Workstations

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.
- With above licensing models Vembu offers you FREE edition, Standard Edition and Enterprise edition.

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