vinchin

VINCHIN BACKUP & RECOVERY V7.2

Admin User Guide

2023/10

成都云祺科技有限公司
Chengdu Vinchin Technology Co.,Ltd.

vmware PARTNER TECHNOLOGY ALLIANCE
redhat TECHNOLOGY PARTNER
CITRIX Partner Independent Software Vendor

Table of Contents

Introduction 7

Product Overview 7

Supported Environments 8

VM Backup 8

Server Backup 8

Database Backup 8

File Backup 9

NAS Backup 9

Getting Started 10

System Login 10

Change Password 10

System License 13

Storage Repository 14

Direct Attached Storages (DAS) 14

Add Disk Partition 15

Add Local Disk 15

Add Local Directory 16

Add Logical Volume 16

Network Attached Storages (NAS) 17

NFS Share 17

CIFS Share 17

Storage Area Network (SAN) Storages 18

Fibre Channel (FC) 18

iSCSI 19

Offsite Storage 19

Cloud Object Storages 20

Add Amazon S3 Cloud Object Storage 20

Add Microsoft Azure Blob Storage 20

Add Alibaba Object Storage Service (OSS) 21

Add Huawei Object Storage Service (OBS) 21

Add Tencent Cloud Object Storage (COS) 22

Add Ceph S3-compatible Object Storage 22

Add Wasabi Hot Cloud Storage 22

Add MinIO Object Storage 23

Import Backups 23

Manage Storages 24
VM Backup 25
Preparation for VM Backup 25
Install VM Backup Plugin 25
Add Virtual Infrastructure 38
Overview of VM Backup Features 51
Backup Methods 51
Backup Data Reduction 52
Backup Data Encryption 52
Retention Policy 53
Data Transmission 54
Incremental Mode 56
Create VM Backup Job 58
Step 1. Select VMs to Backup 58
Step 2. Select Backup Destination 60
Step 3. Configure Backup Strategies 61
Step 4. Review and Confirm Job Settings 72
VM Backup Job Management 72
VM Backup Data Management 73
View Backup Data 73
Retention Tags 74
Delete Backup Data 75
VM Restore 76
Full VM Restore 76
Create Full VM Restore Job 76
Restore Job Operations 80
Instant VM Restore 81
Create Instant VM Restore Job 81
Instant Restore Job Management 83
Live Migration 84
Granular VM Restore 86
Create Granular Restore Job 86
Granular Restore Job Operations 86
V2V Migration 88
V2V Migration Licensing 88
Supported Platforms 88
Conditions and Limitations 88
V2V Migration with Full VM Restore 89
V2V Migration with Instant VM Restore 89
Physical Backup 90

Preparation for Physical Backup 90
Deploy Agents for Linux Server 90
Deploy Agents for Windows Server 91
Agent Auto Deployment 94
Add Physical Backup Agent 98
License Physical Backup Agents 98
File Backup 99
Create File Backup Job 99
File Backup Data 105
File Restore 106
SQL Server Database Backup 109
Preparation SQL Server Backup 109
Create SQL Server Backup Job 110
Create SQL Server Restore Job 114
SQL Server Backup Data 117
MySQL Database Backup 118
Preparation for MySQL Backup 118
Create MySQL Backup Job 120
Create MySQL Restore Job 124
MySQL Backup Data 127
Oracle Database Backup 128
Preparation for Oracle Backup 128
Create Oracle Backup Job 130
Create Oracle Restore Job 134
Oracle Backup Data 137
PostgreSQL Database Backup 138
Preparation for PostgreSQL Backup 138
Create PostgreSQL Backup Job 139
Create PostgreSQL Restore Job 143
PostgreSQL Backup Data 145
MariaDB Database Backup 147
Preparation for MariaDB Backup 147
Create MariaDB Backup Job 148
Create MariaDB Restore Job 152
MariaDB Backup Data 154
Server Backup 156
Preparation for Server Backup 156
Create Server Backup Job 156
Server Backup Data 161
Preparation for Server Restore 162
Create Server Restore Job 165

NAS Backup 167
Preparation for NAS Backup 167
Add NAS Shares 167
License NAS Shares 167
Create NAS Backup Job 168
Step 1: Backup Source 168
Step 2: Backup Destination 169
Step 3: Advanced Strategy 169
Step 4: Review & Confirm 171
NAS Backup Job Management 171
NAS Backup Data 171
View Backup Data 172
Retention Tags 172
Delete Backup Data 173
Create NAS Restore Job 173
Step 1: Restore Point 173
Step 2: Restore Destination 174
Step 3: Restore Strategy 174
Step 4: Review & Confirm 175
Backup Copy 176
Prerequisites of Backup Copy 176
Onsite Backup Copy 176
Offsite Backup Copy 176
VM Copy 177
Create VM Copy Job 177
VM Copy Retrieve 180
VM Copy Data 182
File Copy 183
Create File Copy Job 183
File Copy Retrieve 185
File Copy Data 187
Database Copy 187
Create Database Copy Job 187
Database Copy Retrieve 188
Database Copy Data 188
Server Copy 188
Create Server Copy Job 189
Server Copy Retrieve 189
Server Copy Data 189
NAS Copy 189

Create NAS Copy Job 190
NAS Copy Retrieve 190
NAS Copy Data 190
Backup Archive 191
Create Archive Job 191
Step 1: Archive Source 191
Step 2: Primary Strategy 191
Step 3: Advanced Strategy 192
Step 4: Review & Confirm 193
Archive Job Management 193
Archive Retrieve 195
Step 1: Retrieve Source 195
Step 2: Retrieve Destination 195
Step 3: Retrieve Strategy 195
Step 4: Review & Confirm 196
Archive Data 197
Backup Verification 198
Create Verification Lab 198
Step 1: Basic Info 198
Step 2: Target Host 198
Step 3: Isolated Network 199
Step 4: Review & Confirm 199
Create Verification Job 200
Step 1: Verification Source 200
Step 2: Verification Lab 201
Step 3: Verification Strategy 201
Step 4: Review & Confirm 201
Verification Job Management 202
Resources 204
Virtual Infrastructure 204
Virtual Platform 204
Cloud Platform 205
LAN-Free 205
Backup Proxy 209
Agents 210
NAS Shares 210
Storage 210
Backup Node 210
Strategy Templates 211

System 212
System Settings 212
Network Settings 212
Time Settings 215
Notifications 216
Security Settings 218
Restart & Shutdown 220
Upgrade 221
Data Visualization 222
System Tools 223
Configuration Backup 227
User Management 231
Users 231
Groups 232
Roles 233
Domain Server 235
Account Settings 236
User Information 236
Change Password 236
Lock Screen 237
About 237
Logout 237
Informational 238
Home 238
Monitor Center 239
Jobs 239
Alerts 241
Logs 242
Reports 244
System 246
System Monitor 246
System Info 248

Introduction

Product Overview

Vinchin Backup & Recovery is an ease-of-use, secure and reliable data protection and disaster recovery solution designed to support multiple virtualizations, physical and NAS backup.

Its VM backup is agentless and image-based, all VM backups are taken from the hypervisor level. For physical servers, by implementing manual or automated agent deployment, files, databases and the entire operating system of physical Windows and Linux server can be easily backed up.

Main Features:

- **VM Backup**: agentless, Image-based hypervisor level backup for up to 15 mainstreams virtualization.
- **VM Restore:** various VM restore options including Full Restore, Instant Restore, Granular Restore and V2V Migration to guarantee your business continuity.
- **File Backup and Restore**: file backup and restore for various Windows editions and Linux distributions.
- **Database Backup and Restore**: backup MS SQL Server, Oracle Database, MySQL Database, PostgreSQL and MariaDB databases with application-consistent abilities, and restore to original host or new host.
- **Backup Copy**: copy VM backups, file backups, database backups, server backups and NAS backups to a secondary storage or secondary location for disaster recovery.
- **Backup Archive**: archive VM backups to cloud object storages for long-term data retention and data protection laws and regulations compliance.
- **Backup Encryption**: protect all backups from unauthorized access.
- **Storage Protection**: keep backups safe from ransomware and other malwares.
- **Agentless V2V Migration**: Support agentless V2V migration(bidirectional migration) between any two virtualizations among the 15 virtual platforms supported by Vinchin.

Supported Environments

VM Backup

- VMware vSphere: 5.5, 6.0, 6.5, 6.7, 7.0(U1, U2, U3), 8.0(U1, U2)
- Microsoft Hyper-V Server: 2012R2, 2016, 2019, 2022, Windows 8.1 (Desktop), Windows 10 (Desktop), Windows 11 (Desktop)
- Microsoft Hyper-V on Windows Server: 2012 R2, 2016, 2019,2022
- Citrix XenServer: 6.5, 7.x
- Citrix Hypervisor: 8.0, 8.1, 8.2
- XCP-ng: 7.4, 7.5, 7.6, 8.0, 8.1, 8.2
- RHV: 4.0, 4.1, 4.2, 4.3, 4.4
- oVirt: 4.0, 4.1, 4.2, 4.3, 4.4, 4.5
- OpenStack: Mitaka and later versions + Ceph/NetApp/Promise(as production storage)
- Sangfor HCI: 5.8.1, 5.8.2, 5.8.3, 5.8.5, 5.8.6, 5.8.7R1, 5.8.8, 6.0.1, 6.0.1R1, 6.2.0, 6.3.0, 6.7.0, 6.7.0R2, 6.8.0, 6.8.0R1
- Oracle Linux Virtualization Manager (OLVM): 4.3, 4.4
- Huawei FusionCompute (KVM): 6.5.1, 8.0.0, 8.0.1
- H3C UIS: E0606, E0611, E0716, E0720, E0721, E0750
- H3C CAS: E0506, E0526, E0530, E0535, E0706, E0709, E0710, E0718, E0730
- ZStack: 3.5, 3.7, 3.8, 3.9, 3.10, 4.0.1, 4.3.0, 4.3.28, 4.4.16, 4.5.1, 4.7.11
- Proxmox VE: 7.2, 7.4, 8.0

Server Backup

- Windows Desktop: Windows XP, Windows 7, Windows 8, Windows 10, Windows 11
- Windows Server: Server 2003, Server 2008, Server 2012, Server 2016, Server 2019, Server 2022
- RHEL (Red Hat Enterprise Linux): 6, 7, 8
- CentOS Linux: 6, 7, 8
- Debian: 8.11 to 9.13

Notice

Only 64-bit operating systems are supported for server backup.

Database Backup

Supported databases and versions.

- Oracle Database (Windows and Linux): 11g, 12c, 18c, 19c, 20c, 21c
- MS SQL Server (Windows): 2008, 2012, 2014, 2016, 2017, 2019, 2022
- MySQL (Linux): 5.6, 5.7, 8.0, 8.0.26, 8.0.28
- PostgreSQL (Linux): 12, 13, 14

- Postgres Pro (Linux): 13.10, 14.5, 14.7
- MariaDB (Linux): 10.5 to 10.10.2

Supported database deployments.

- Oracle database deployment: Standalone, Real Application Clusters (RAC)
- MS SQL Server deployment: Standalone, Failover Cluster, Always On availability groups
- MySQL deployment: Standalone
- PostgreSQL deployment: Standalone
- MariaDB deployment: Standalone

File Backup

- Windows Desktop: Windows XP, Windows 7, Windows 8, Windows 10
- Windows Server: Server 2003, Server 2008, Server 2012, Server 2016, Server 2019, Server 2022
- RHEL (Red Hat Enterprise Linux): 6, 7, 8
- CentOS Linux: 6, 7, 8
- Debian Linux: 8.11, 9.6, 9.13
- Ubuntu Linux: 14.04, 16.04, 18.04, 20.04, 22.04

Notice

Only 64-bit operating systems are supported for file backup.

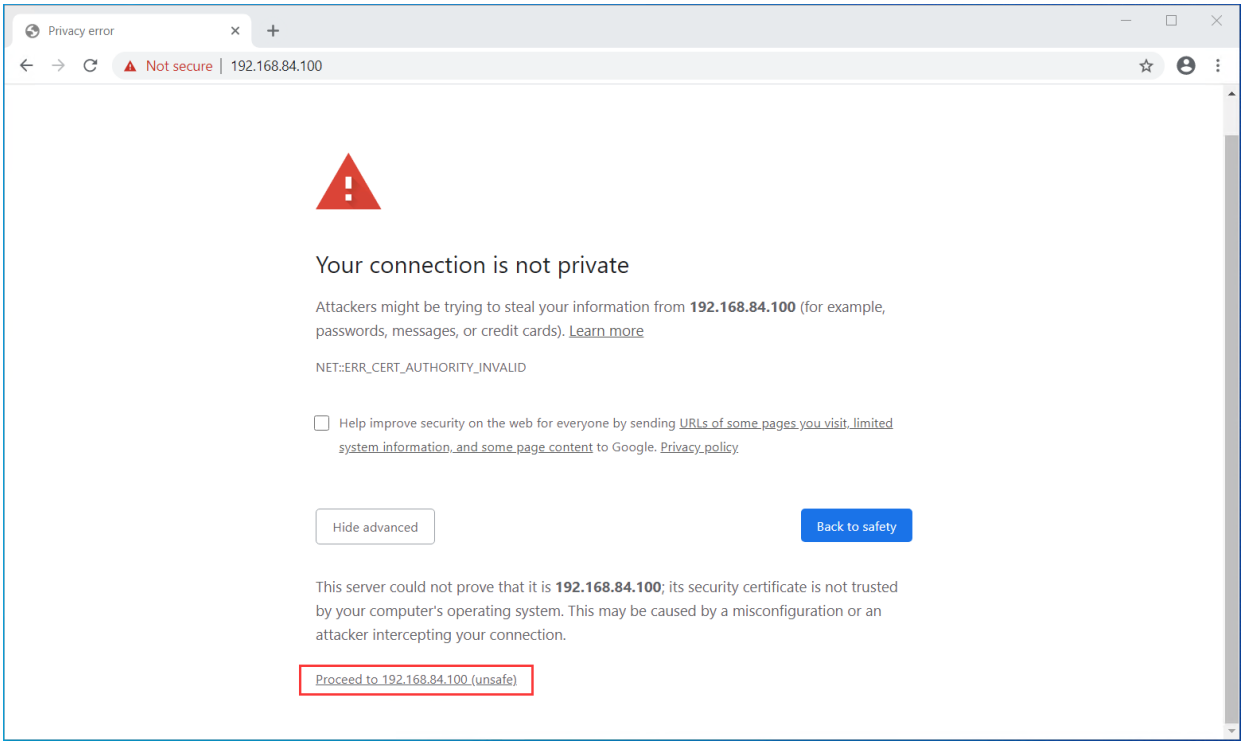
NAS Backup

- CIFS: v2.0, v3.0
- NFS: v3.0, v4.0, v4.1

Getting Started

System Login

To open Vinchin Backup Server web console, it is recommended to use Google Chrome web browser. In the browser address bar, enter the IP address that you have assigned to the Backup Server during installation. You'll probably see the below "**You connection is not private**" warning message.



Please click on **Advanced** button to show advanced options. Then click on "**Proceed to xxx.xxx.xxx.xxx (unsafe)**" to open the web console of Vinchin Backup Server.

If MacOS, please click on **Advanced** button, then type "thisisunsafe" directly on the warning screen to open the web console.

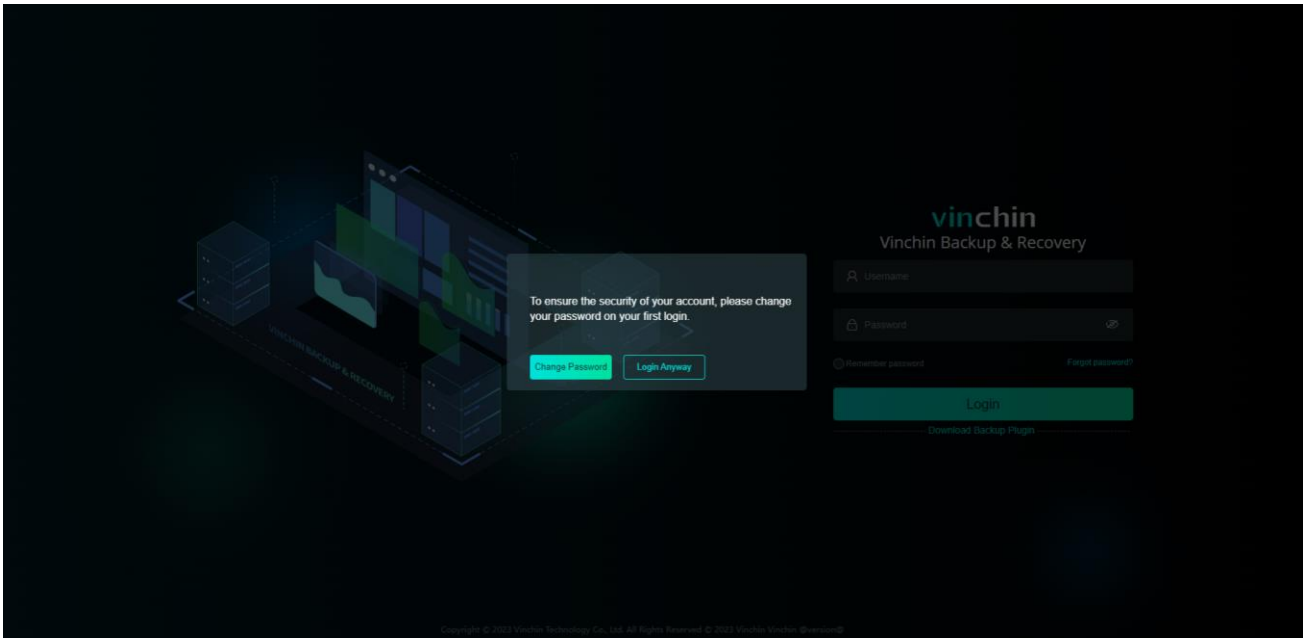
On the login screen of Vinchin Backup & Recovery, please use the below default credentials to log in.

Username: **admin**

Password: **123456**

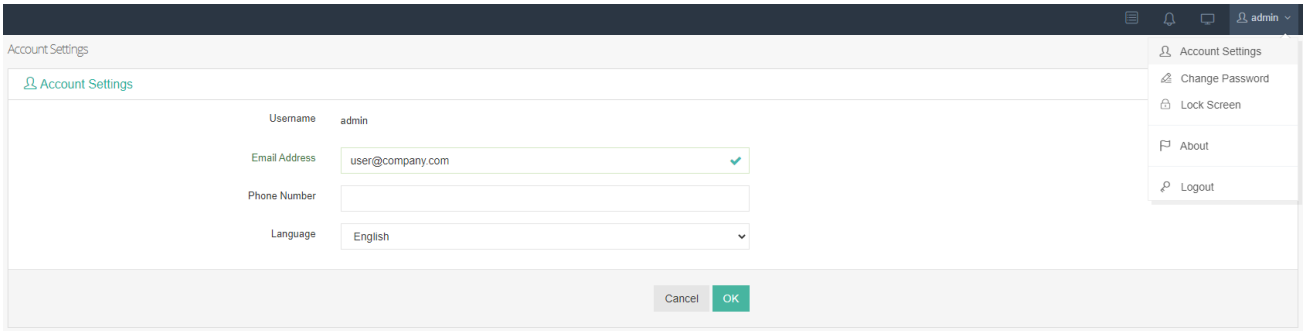
Change Password

For the safety of Vinchin Backup Server, please change the default administrator password right after your first-time login. It will remind you to change the password or you can keep the default password and direct login. If you skip password reset step, the password can be manually changed from **admin** > **Change Password** screen.



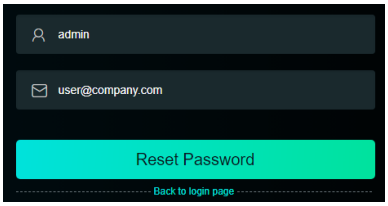
It's recommended to use combination of uppercase and lowercase letters, numbers, and special characters as the new password.

To prevent losing your password, it's also recommended to configure your email in the **Account Settings** for Vinchin Backup & Recovery being able to send you password reset email to reset your password.



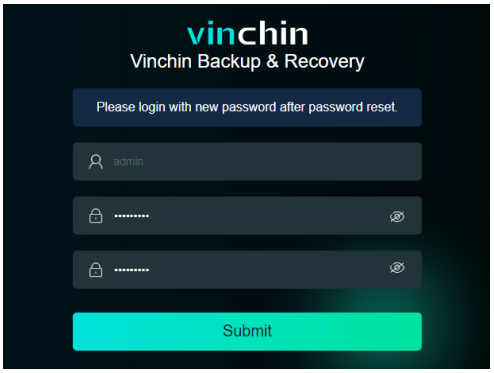
Sending password reset email requires enabling the mail services on the Vinchin backup server, please refer to Notifications to setup mail services.

If you had enabled mail services and associated your user account with your email address, when you forgot your password, on the login screen you could click on **Forget password**, then provide your username and email address and click on **Reset Password** to reset your password via a password reset email.



If the user name and the email address match, then the password reset email will be sent.

When you had received the password reset email, please copy the password reset URL and paste in the browser address bar to reset your password.

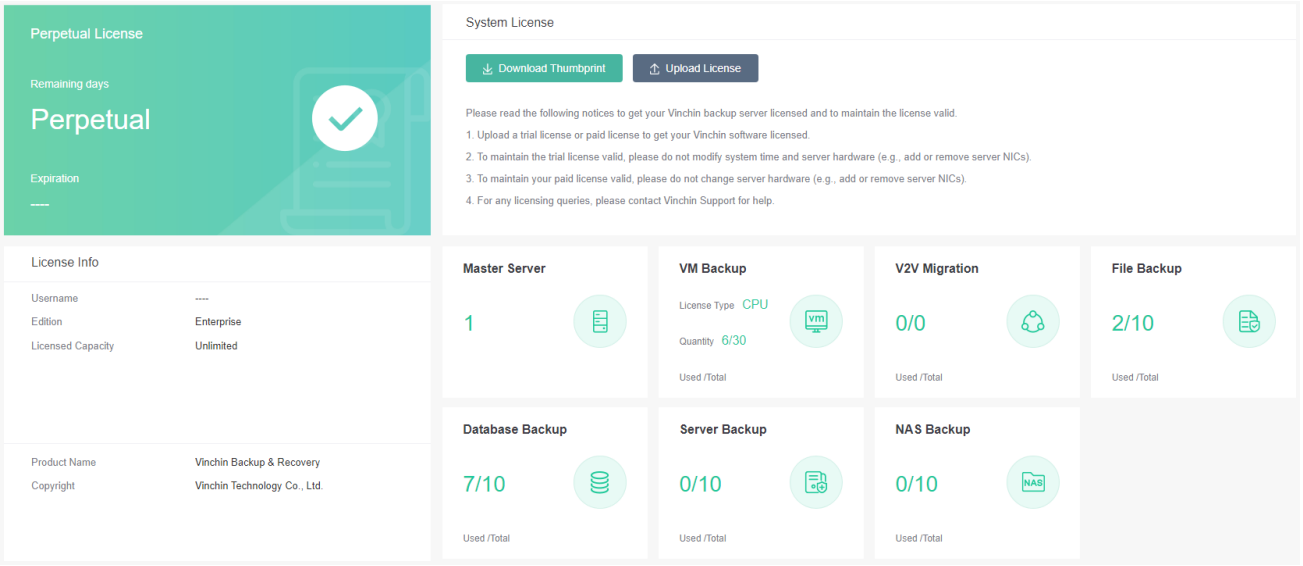


Please make sure you use the password reset URL in the same LAN in which your PC could open the web console of Vinchin backup server.

The password reset URL only valid for 5 minutes, if it's expired, please apply for a new password reset email.

System License

When you have registered to download Vinchin Backup & Recovery, a 60-day full featured trial license key will be sent to you via the email you provided, after the installation, please open Vinchin Backup & Recovery web console and go to **System** > **System License** page to upload the trial license key to get the software licensed for evaluation. If you wish to buy a paid license for Vinchin Backup & Recovery, please contact our sales team. Once you had received the paid license and uploaded to Vinchin Backup & Recovery, your system license page should look like below.



The number of licensed feature modules will be given in “used/licensed” format. The actual license info depends on the order you have placed.

Storage Repository

In Vinchin Backup & Recovery, storages are used for 3 objectives:

- Backup
- Backup Copy
- Backup Archive

Adding a backup storage is essential before you can create any backup jobs.

Backup copy storage is required when you want to copy your backups to a secondary storage or a remote location.

Backup archive storage, usually a more cost-effective storage media which is needed when you want to archive your VM backup data for long-term retention purpose.

Once a storage's objective has been settled, it cannot be used for other purpose, e.g., a backup storage can only be used for backup, it cannot be used for backup copy or backup archive.

The supported storage types/protocols and storage objectives are as showing below.

Storage Types/Objectives	**Backup**	**Backup Copy**	**Backup Archive**
Disk Partition	Yes	Yes	Yes
Local Disk	Yes	Yes	Yes
Local Directory	Yes	Yes	Yes
Logical Volume	Yes	Yes	Yes
Channel (FC)	Yes	Yes	Yes
iSCSI	Yes	Yes	Yes
NFS Share	Yes	Yes	Yes
CIFS Share	Yes	Yes	Yes
Off-site Storage	No	Yes, backup copy only	no
Cloud Object Storage	No	No	Yes, backup archive only

The storages are added and managed from **Resources** > **Storage** page.

Direct Attached Storages (DAS)

The storge devices attached directly to Vinchin Backup & Recovery including:

- Disk Partition
- Local Disk
- Local Directory
- Logical Volume

These storage devices can be used as storage repository to store your backup data, backup copy data and archive data.

Add Disk Partition

An unmounted disk partition on the Vinchin backup server or backup node can be used as backup, backup copy or backup archive storage.

To add a disk partition as Vinchin storage.

1. Select **Disk Partition** in the **Storage Type** dropdown list.
2. Select the node (if any) from the **Node IP/Domain** dropdown list on which the disk partition resides in.
3. Wait for the scanning process of the disk partition, when it presents in the **Storage Resources** list, please select it.
4. In the **Name** field, give the storage a custom name for identification.
5. Select from **Backup**, **Copy** or **Archive** according for which purpose the storage will be used.
6. Setup storage usage alert as per your requirements.
7. Click on **OK** to add the storage.

If the disk partition was once been used by Vinchin and which contains backup data, you will get a dialog asking either to import the backups or to format the storage.

If those backups are no longer useful, you can choose to format it, and Vinchin will erase everything then make new filesystem on the disk partition. It will take a while depending on the storage size and performance, please do not leave the page and wait patiently for the process to be completed.

If you choose to import the backups, Vinchin will not touch the backups and the disk partition filesystem, as for how to manage the imported backups, please refer to Import Backups.

For a fresh new disk partition or disk partition contains data which is unrecognizable by Vinchin, you will get a dialog asking to format the storage, please make sure you had made backup of the data on the disk partition, otherwise everything will be erased!

Add Local Disk

An unpartitioned or unmounted local disk on the Vinchin backup server or backup node can be used as backup, backup copy or backup archive storage.

To add a local disk as Vinchin storage.

1. Select **Local Disk** in the **Storage Type** dropdown list.
2. Select the node (if any) from the **Node IP/Domain** dropdown list on which the disk partition resides in.
3. Wait for the scanning process of the local disk, when it presents in the **Storage Resources** list, please select it.
4. In the **Name** field, give the storage a custom name for identification.
5. Select from **Backup**, **Copy** or **Archive** according for which purpose the storage will be used.
6. Setup storage usage alert as per your requirements.
7. Click on **OK** to add the storage.

If the local disk was once been used by Vinchin and which contains backup data, you will get a dialog asking either to import the backups or to format the storage.

If those backups are no longer useful, you can choose to format it, and Vinchin will erase everything then make new filesystem on the disk. It will take a while depending on the storage size and performance, please do not leave the page and wait patiently for the process to be completed.

If you choose to import the backups, Vinchin will not touch the backups and the disk filesystem, as for how to

manage the imported backups, please refer to Import Backups.
For a fresh new local disk or disk contains data which is unrecognizable by Vinchin, you will get a dialog asking to format the storage, please make sure you had made backup of the data on the disk, otherwise everything will be erased!

Add Local Directory

A local directory on the Vinchin backup server or backup node filesystem can be used as backup, backup copy or backup archive storage.
To add local directory as Vinchin storage.
1. Select **Local Directory** in the **Storage Type** dropdown list.
2. Select the node (if any) from the **Node IP/Domain** dropdown list on which the disk partition resides in.
3. Type the directory path which you wish to use in the **Directory Path** field. The directory path should be an existing directory, otherwise it will fail to add storage.
4. In the **Name** field, give the storage a custom name for identification.
5. Select from **Backup**, **Copy** or **Archive** according for which purpose the storage will be used.
6. Setup storage usage alert as per your requirements.
7. Click on **OK** to add the storage.

If the directory was once been used as Vinchin storage and which contains backup data, you'll get a dialog asking either to import the backups or not.
If you choose to add storage without importing old backups, Vinchin will skip the backups and add the directory as storage, the old backups will still reside in the directory but unable to be managed or used for restoration from Vinchin web console.
If you choose to add storage and import the old backups, after adding storage and importing backups, you'll be able to manage the old backups or use the backups for restoration purpose from Vinchin web console.

Add Logical Volume

An unmounted logical volume on the Vinchin backup server or backup node can be used as backup, backup copy or backup archive storage.
To add a logical volume as Vinchin storage.
1. Select **Logical Volume** in the **Storage Type** dropdown list.
2. Select the node (if any) from the **Node IP/Domain** dropdown list on which the disk partition resides in.
3. Wait for the scanning process of the logical volume, when it presents in the **Storage Resources** list, please select it.
4. In the **Name** field, give the storage a custom name for identification.
5. Select from **Backup**, **Copy** or **Archive** according for which purpose the storage will be used.
6. Setup storage usage alert as per your requirements.
7. Click on **OK** to add the storage.

If the logical volume was once been used by Vinchin and which contains backup data, you will get a dialog asking either to import the backups or to format the storage.
If those backups are no longer useful, you can choose to format it, and Vinchin will erase everything then make new filesystem on the disk partition. It will take a while depending on the storage size and performance, please do not

leave the page and wait patiently for the process to be completed.
If you choose to import the backups, Vinchin will not touch the backups and the filesystem, as for how to manage the imported backups, please refer to Import Backups.

Network Attached Storages (NAS)

NFS Share

Before adding the NFS share as Vinchin storage, make sure Vinchin server/node has read and write permissions to the NFS share, otherwise you'll fail to add the NFS share.
To add an NFS storage to Vinchin server or node.
1. Select **NFS Share** in the **Storage Type** dropdown list.
2. Select the node (if any) from the **Node IP/Domain** dropdown list on which you wish the NFS share to be added to.
3. Type the NFS share path in the **Shared Folder** field. The path format should be "nas_server_ip:/path/directory" (without quotes), e.g., 192.168.1.10:/path/directory.
4. In the **Name** field, give the storage a custom name for identification.
5. Select from **Backup**, **Copy** or **Archive** according for which purpose the storage will be used.
6. Setup storage usage alert as per your requirements.
7. Click on **OK** to add the storage.
By default, Vinchin will connect to the NFS share using NFS protocol version 3.0, if your NFS server runs other protocol versions, please click on config the mount params and type the protocol version in the **Mount Params** field, e.g., "vers=2.0" (without quotes). If any other parameters required, please also specify them here and separate each with a coma.
Adding an NFS share to Vinchin, the existing data in the NFS share will remain unmodified, but it is not recommended to share the same NFS directory with other services and applications, it might impact on the backup and restore efficiencies.

CIFS Share

Before adding the CIFS share as Vinchin storage, make sure Vinchin server/node has read and write permissions to the CIFS share, otherwise you'll fail to add the CIFS share.
To add an CIFS share to Vinchin server or node.
1. Select **CIFS Share** in the **Storage Type** dropdown list.
2. Select the node (if any) from the **Node IP/Domain** dropdown list on which you wish the CIFS share to be added to.
3. Type the CIFS share path in the **Shared Folder** field. The path format should be "//nas_server_ip/path/directory" (without quotes), e.g., //192.168.1.10/path/directory.
4. Provide the CIFS share user credentials in **Username** and **Password** fields.
5. In the **Name** field, give the storage a custom name for identification.
6. Select from **Backup**, **Copy** or **Archive** according for which purpose the storage will be used.
7. Setup storage usage alert as per your requirements.

8. Click on **OK** to add the storage.

By default, Vinchin will connect to the CIFS share using SMB protocol version 3.0, if your CIFS server runs other protocol versions, please click on config the mount params and type the protocol version in the **Mount Params** field, e.g., "vers=2.0" (without quotes). If any other parameters required, please also specify them here and separate each with a coma.

Adding an CIFS share to Vinchin, the existing data in the CIFS share will remain unmodified, but it is not recommended to share the same CIFS directory with other services and applications, it might impact on the backup and restore efficiencies.

Storage Area Network (SAN) Storages

Fibre Channel (FC)

To add Fibre Channel (FC) storage to Vinchin server/node as backup, copy or archive storage. Make sure your Vinchin server/node is a physical machine which has an FC HBA interface card and have been connected to the FC SAN.

1. Select **Fibre Channel (FC)** in the **Storage Type** dropdown list.
2. Select the node (if any) from the **Node IP/Domain** dropdown list on which the FC LUN you wish to add to.
3. Wait for the scanning process of the FC HBA card, when it presents in the **Fibre Channel** list, please use the WWPN to map the target FC LUN to Vinchin from the storage server (if you haven't done this yet).
4. When done step 3, please refresh the page and repeat step 1 and 2.
5. In **Storage Resource** you should see the mapped FC LUN presented, please verify if the FC LUN is intended to be used as Vinchin storage and then select it.
6. In the **Name** field, give the storage a custom name for identification.
7. Select from **Backup**, **Copy** or **Archive** according for which purpose the storage will be used.
8. Setup storage usage alert as per your requirements.
9. Click on **OK** to add the storage.

If the FC LUN was once been used by Vinchin and which contains backup data, you will get a dialog asking either to import the backups or to format the storage.

If those backups are no longer useful, you can choose to format it, and Vinchin will erase everything then make new filesystem on the FC LUN. It will take a while depending on the storage size and performance, please do not leave the page and wait patiently for the process to be completed.

If you choose to import the backups, Vinchin will not touch the backups and the FC LUN filesystem, as for how to manage the imported backups, please refer to Import Backups.

For a fresh new FC LUN or FC LUN contains data which is unrecognizable by Vinchin, you will get a dialog asking to format the storage, please make sure you had made backup of the data on the FC LUN, otherwise everything will be erased!

iSCSI

To add iSCSI storage to Vinchin server/node as backup, copy or archive storage. Make sure your Vinchin server/node is connected to the IP SAN.

1. Select **iSCSI** in the **Storage Type** dropdown list.
2. Select the node (if any) from the **Node IP/Domain** dropdown list on which the iSCSI LUN you wish to add to.
3. Copy the IQN of the Vinchin server/node from the **iSCSI Name** field, please use the IQN to map the target iSCSI LUN to Vinchin from the storage server (if you haven't done this yet).
4. When done step 3, please type the IP address of the storage server in the **iSCSI Server** field and click on **Scan Target** button to scan the iSCSI LUN mapped to Vinchin server/node.
5. Wait for the scanning process to be completed and you'll see the iSCSI LUN presented in the **Target LUN** list. Please verify if the iSCSI LUN is intended to be used as Vinchin storage and then select it.
6. In the **Name** field, give the storage a custom name for identification.
7. Select from **Backup**, **Copy** or **Archive** according for which purpose the storage will be used.
8. Setup storage usage alert as per your requirements.
9. Click on **OK** to add the storage.

If the iSCSI LUN was once been used by Vinchin and which contains backup data, you will get a dialog asking either to import the backups or to format the storage.

If those backups are no longer useful, you can choose to format it, and Vinchin will erase everything then make new filesystem on the iSCSI LUN. It will take a while depending on the storage size and performance, please do not leave the page and wait patiently for the process to be completed.

If you choose to import the backups, Vinchin will not touch the backups and the disk partition filesystem, as for how to manage the imported backups, please refer to Import Backups.

For a fresh new iSCSI LUN or iSCSI LUN contains data which is unrecognizable by Vinchin, you will get a dialog asking to format the storage, please make sure you had made backup of the data on the iSCSI LUN, otherwise everything will be erased!

Offsite Storage

To add an offsite copy storage, please go to **Resources** > **Storage** page and do as follows.

1. Click on **Add** button.
2. In **Storage Type** dropdown list, select **Off-site Storage**.
3. In the IP Address field, type the IP address of the remote site Vinchin server. As for the default port number, if modification is required, please contact Vinchin Support for help, otherwise please do not modify it.
4. In the **Username** and **Password** fields, type the web admin credentials of the remote site Vinchin server.
5. In the **Name** field, give the storage a custom name for identification.
6. An offsite storage is used for offsite backup copy only, so, the **Storage Usage** is set to **Copy** by default and cannot be changed.
7. Optionally setup the **Storage Alert** as per your requirement.
8. Click on **OK** to add the offsite copy storage.

If the offsite storage contains backup data, you will get a dialog asking either to import the backups or not.

Check the **Import Backups** checkbox to import the existing backup copy data, as for how to manage the imported backups, please refer to Import Backups.

If you don't want to import the backup copy data, click on OK button to add the offsite storage directly without importing any data. The existing backup copy data on the offsite storage will not be visible on primary Vinchin server web console, those data should be managed on the remote Vinchin server web console.

Cloud Object Storages

Cloud Object Storages are used to archive your VM backups for long-term retention purpose. The object storages supported by Vinchin Backup & Recovery are as follows.

- Amazon S3 Cloud Object Storage
- Microsoft Azure Blob Storage
- Alibaba Object Storage Service (OSS)
- Huawei Object Storage Service (OBS)
- Tencent Cloud Object Storage (COS)
- Wasabi Hot Cloud Storage
- MinIO Object Storage
- Ceph S3-compatible Object Storage

Add Amazon S3 Cloud Object Storage

To add Amazon S3 Cloud Object storage as a backup archive target, please do as follows.

1. In **Storage Type** dropdown list select **Cloud Object Storage**.
2. In **Vendor** dropdown list select **AWS S3**.
3. In the **Region** dropdown list select a location of the datacenter where you want your data to be saved.
4. The **Service Endpoint** field is optional, if you need to specify the service endpoint URL, and if it's SSL enabled, please enable **SSL Certificate** option, and input the URL without "https://".
5. In the **Access Key** field, enter the access key ID of your Amazon S3 account.
6. In the **Secret Key** field, enter the secret access key of your Amazon S3 account.
7. In the **Bucket** field, enter the storage bucket name then click on **Scan Bucket** to obtain the existing folders within the bucket.
8. In **Folder** dropdown list, select a folder to be used or click on manually enter a folder name then enter a new folder name to be created and used.
9. Give the storage a name for identification in the **Name** field.
10. Cloud object storages are currently used for backup archive only, so the **Storage Usage** is set as **Archive** by default and cannot be changed.
11. Set a limitation of maximum storage space allowed to be used in the **Quota** field.

Add Microsoft Azure Blob Storage

To add Microsoft Azure Blob storage, please do as follows.

1. In the **Storage Type** dropdown list, select **Cloud Object Storage**.
2. In the **Vendor** dropdown list, select **Azure**.
3. In the **Connection String** field, enter the connection string for your Azure storage account. The connection string

should look similar to:

```
DefaultEndpointsProtocol=https;AccountName=storagesample;AccountKey=<account-key>
```

4. In the **Container** field, enter a container name and click on **Scan Container** to obtain the existing folders in the container.
5. Give the storage a name for identification in the **Name** field.
6. Cloud object storages are currently used for backup archive only, so the **Storage Usage** is set as **Archive** by default and cannot be changed.
7. Set a limitation of maximum storage space allowed to be used in the **Quota** field.

Add Alibaba Object Storage Service (OSS)

To add Alibaba OSS as a backup archive target, please do as follows.
1. In **Storage Type** dropdown list select **Cloud Object Storage**.
2. In **Vendor** dropdown list select **Alibaba Cloud**.
3. In the **Region** dropdown list select a location of the datacenter where you want your data to be saved.
4. In the **Access Key** field, enter the access key ID of your Alibaba cloud account.
5. In the **Secret Key** field, enter the secret access key of your Alibaba cloud account.
6. In the **Bucket** field, enter the storage bucket name then click on **Scan Bucket** to obtain the existing folders within the bucket.
7. In **Folder** dropdown list, select a folder to be used or click on manually enter a folder name then enter a new folder name to be created and used.
8. Give the storage a name for identification in the **Name** field.
9. Cloud object storages are currently used for backup archive only, so the **Storage Usage** is set as **Archive** by default and cannot be changed.
10. Set a limitation of maximum storage space allowed to be used in the **Quota** field.

Add Huawei Object Storage Service (OBS)

To add Huawei OBS as a backup archive target, please do as follows.
1. In **Storage Type** dropdown list select **Cloud Object Storage**.
2. In **Vendor** dropdown list select **Huawei Cloud**.
3. In the **Region** dropdown list select a location of the datacenter where you want your data to be saved.
4. In the **Access Key** field, enter the access key ID of your Huawei cloud account.
5. In the **Secret Key** field, enter the secret access key of your Huawei cloud account.
6. In the **Bucket** field, enter the storage bucket name then click on **Scan Bucket** to obtain the existing folders within the bucket.
7. In **Folder** dropdown list, select a folder to be used or click on manually enter a folder name then enter a new folder name to be created and used.
8. Give the storage a name for identification in the **Name** field.
9. Cloud object storages are currently used for backup archive only, so the **Storage Usage** is set as **Archive** by default and cannot be changed.
10. Set a limitation of maximum storage space allowed to be used in the **Quota** field.

Add Tencent Cloud Object Storage (COS)

To add Tencent COS as a backup archive target, please do as follows.
1. In **Storage Type** dropdown list select **Cloud Object Storage**.
2. In **Vendor** dropdown list select **Tencent Cloud**.
3. In the **Region** dropdown list select a location of the datacenter where you want your data to be saved.
4. In the **Access Key** field, enter the access key ID of your Tencent cloud account.
5. In the **Secret Key** field, enter the secret access key of your Tencent cloud account.
6. In the **Bucket** field, enter the storage bucket name then click on Scan Bucket to obtain the existing folders within the bucket.
7. In **Folder** dropdown list, select a folder to be used or click on manually enter a folder name then enter a new folder name to be created and used.
8. Give the storage a name for identification in the **Name** field.
9. Cloud object storages are currently used for backup archive only, so the **Storage Usage** is set as **Archive** by default and cannot be changed.
10. Set a limitation of maximum storage space allowed to be used in the **Quota** field.

Add Ceph S3-compatible Object Storage

To add Ceph S3 Object storage as a backup archive target, please do as follows.
1. In **Storage Type** dropdown list select **Cloud Object Storage**.
2. In **Vendor** dropdown list select **Ceph S3**.
3. In the **Service Endpoint** field, enter the URL of the Ceph S3 service endpoint URL with format "IP_address:port_number" (without quotes) or "domain:port_number" (without quotes), and if it's SSL enabled, please enable **SSL Certificate** option, and input the URL without "https://".
4. In the **Access Key** field, enter the access key ID of your Ceph S3 account.
5. In the **Secret Key** field, enter the secret access key of your Ceph S3 account.
6. In the **Bucket** field, enter the storage bucket name then click on **Scan Bucket** to obtain the existing folders within the bucket.
7. In **Folder** dropdown list, select a folder to be used or click on manually enter a folder name then enter a new folder name to be created and used.
8. Give the storage a name for identification in the **Name** field.
9. Cloud object storages are currently used for backup archive only, so the **Storage Usage** is set as **Archive** by default and cannot be changed.
10. Set a limitation of maximum storage space allowed to be used in the **Quota** field.

Add Wasabi Hot Cloud Storage

To add Wasabi Hot Cloud Storage as a backup archive target, please do as follows.
1. In **Storage Type** dropdown list select **Cloud Object Storage**.
2. In **Vendor** dropdown list select **Wasabi**.
3. In the **Region** dropdown list select a location of the datacenter where you want your data to be saved.

4. In the **Access Key** field, enter the access key ID of your Wasabi cloud account.
5. In the **Secret Key** field, enter the secret access key of your Wasabi cloud account.
6. In the **Bucket** field, enter the storage bucket name then click on **Scan Bucket** to obtain the existing folders within the bucket.
7. In **Folder** dropdown list, select a folder to be used or click on manually enter a folder name then enter a new folder name to be created and used.
8. Give the storage a name for identification in the **Name** field.
9. Cloud object storages are currently used for backup archive only, so the **Storage Usage** is set as **Archive** by default and cannot be changed.
10. Set a limitation of maximum storage space allowed to be used in the **Quota** field.

Add MinIO Object Storage

To add MinIO Object storage as a backup archive target, please do as follows.
1. In **Storage Type** dropdown list select **Cloud Object Storage**.
2. In **Vendor** dropdown list select **MinIO**.
3. In the **Service Endpoint** field, enter the URL of the MinIO service endpoint URL with format "IP_address:port_number" (without quotes) or "domain:port_number" (without quotes), and if it's SSL enabled, please enable **SSL Certificate** option, and input the URL without "https://".
4. In the **Access Key** field, enter the access key ID of your MinIO account.
5. In the **Secret Key** field, enter the secret access key of your MinIO account.
6. In the **Bucket** field, enter the storage bucket name then click on **Scan Bucket** to obtain the existing folders within the bucket.
7. In **Folder** dropdown list, select a folder to be used or click on manually enter a folder name then enter a new folder name to be created and used.
8. Give the storage a name for identification in the **Name** field.
9. Cloud object storages are currently used for backup archive only, so the **Storage Usage** is set as **Archive** by default and cannot be changed.
10. Set a limitation of maximum storage space allowed to be used in the **Quota** field.

Import Backups

For the storages to be added, if once they had been used by Vinchin Backup & Recovery, no matter for backup, copy or archive purpose, the data should still remain on them. When you try to add them again, the data will be automatically recognized by Vinchin Backup Server.
The imported backup data should be assigned to a user from the **Resources** > **Storage** page by clicking on the **Manage Imported Backups** button. By selecting the corresponding backup job, and click on **Assign** button, you are able to assign the backup data to the selected user from the popup dialog.
If you only import the data without assigning to any user, those data will not be visible to anyone.
Once the backup data had been assigned to a user, the user will be able to see the backup data and create restore jobs with those data.
If the imported backups are VM backups, to create a VM restore job please do it on **VM Backup** > **Restore** page.
If the imported backups are file backups, to create a file restore job please do it on **Physical Backup** > **File Backup** >

Restore page.
If the imported backups are database backups, to create a database restore job please do it on **Physical Backup** > **Database Backup** > **Restore** page.
If the imported backups are server backups, to create a server restore job please do it on **Physical Backup** > **Server Backup** > **Restore** page.
If the imported backups are NAS backups, to create a NAS restore job please do it on **NAS Backup** > **Restore** page.

Manage Storages

All storages added to Vinchin backup server or node can be managed from Vinchin backup server web console, from the **Resources** > **Storage** page.
By selecting a storage and click on **Edit** button, you are able to edit specific settings of the selected storage.
By selecting a storage and click on **Delete** button, you are able to delete this storage from Vinchin backup server or node. But if there's any existing job using this storage, it is not allowed to be deleted. Please first stop and delete the corresponding job then delete the storage.
No matter the storage is used for backup, copy or archive purpose, the data on the storage will not be deleted. Once you add that storage again, Vinchin will detect the data and give you option to import those data. But the corresponding job cannot be resumed to run upon the imported data. For more information of importing backups, please refer to Import Backups.

VM Backup

Preparation for VM Backup

Install VM Backup Plugin

Install Hyper-V Backup Plugin

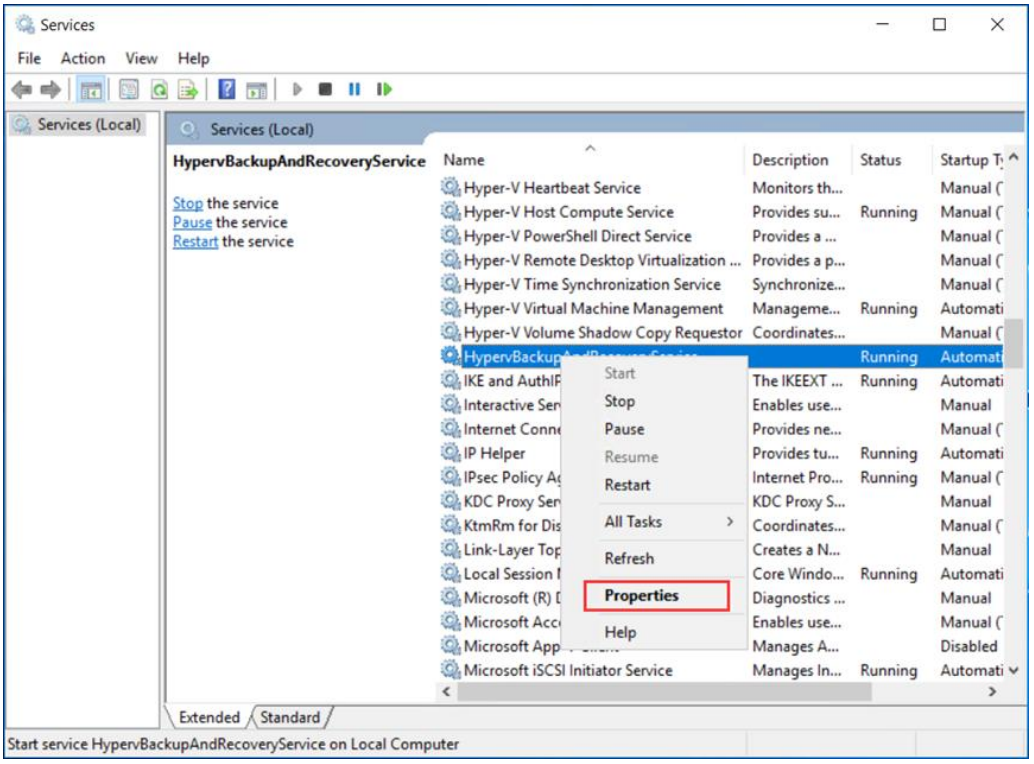
Download Backup Plugin

The Hyper-V VM backup plugins can be downloaded from the login screen of Vinchin backup server's web console.
1. By clicking on **Download Backup Plugin**, you'll see the download options.
2. In **Type** dropdown list, select **VM Backup Plugin** option.
3. In **Platform** dropdown list, select **Microsoft Hyper-V**.
4. Click on **Download** button to download the installer.

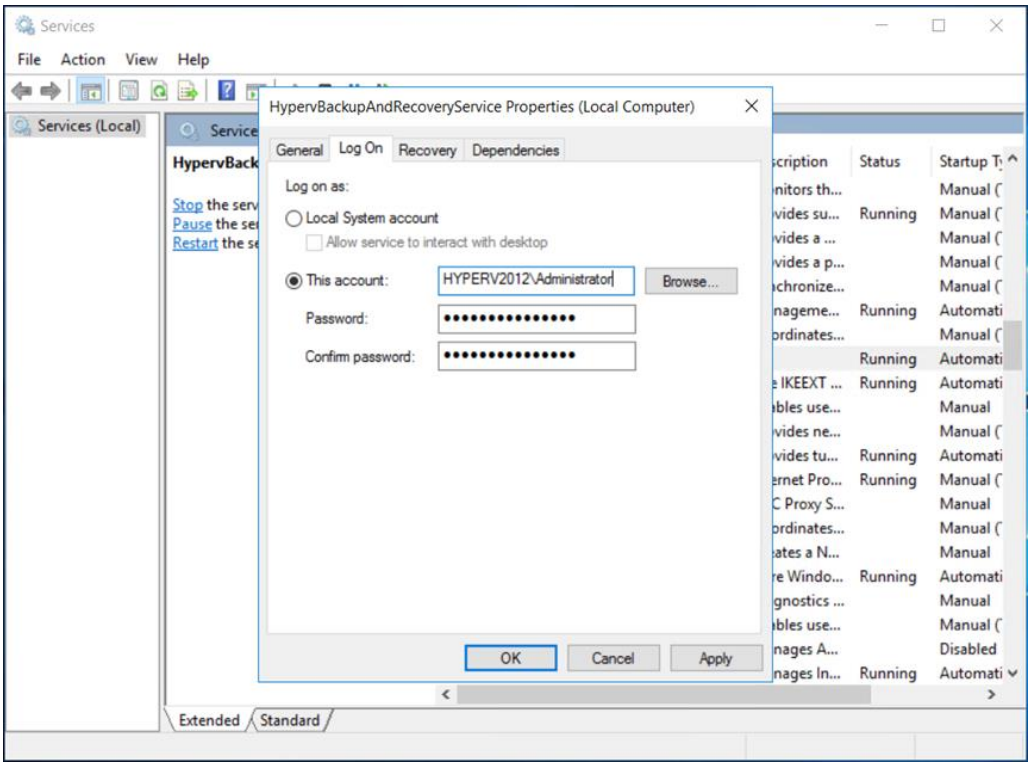
Install on Windows Server with Desktop Experience

The VM backup plugin for Hyper-V should be installed on all the Hyper-V hosts (Standalone, Failover Cluster and SCVMM), please upload the backup plugin installer to all the hosts for installation.
1. Right click the installer and run the installer with administrator privileges (In SCVMM environment, please use SCVMM domain user to install the backup plugin on both Hyper-V host and SCVMM server).
2. When you see the installation wizard, click on **Quick Install** to begin the installation process.

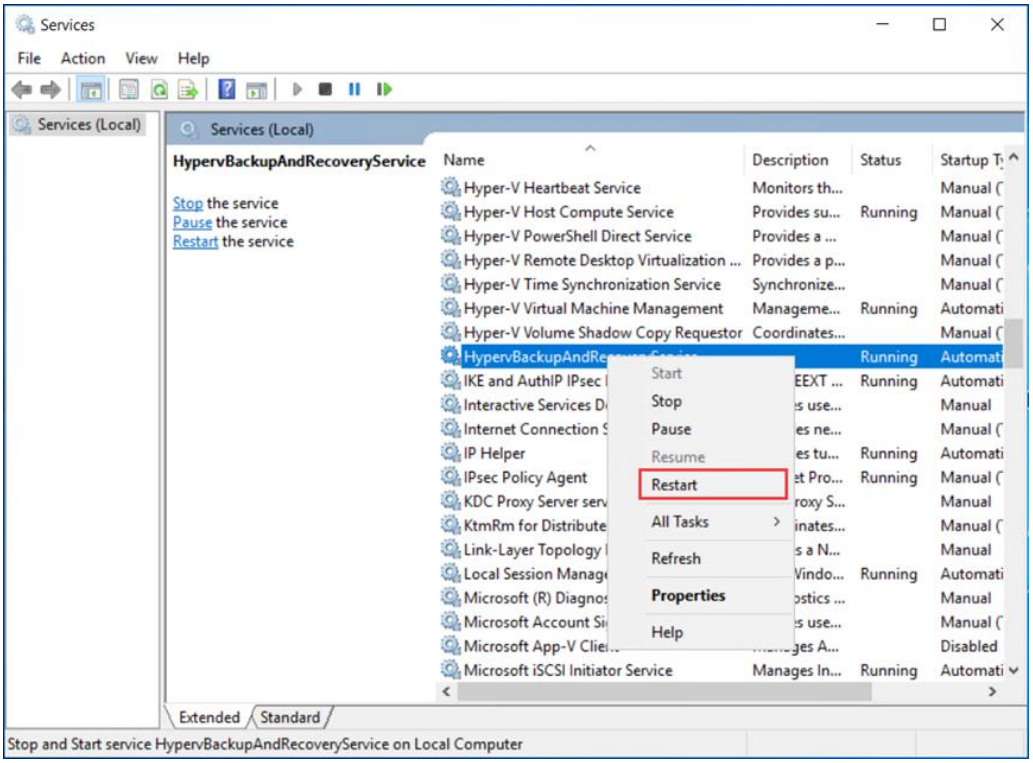
In case of a **Failover Cluster environment,** you also need to modify the backup plugin service's login permission as a domain user with local administrator privileges, and then restart the backup plugin services. To do this, please continue the following steps.
1. Right click the Start icon, select Run, type `services.msc` in the Run box and press Enter to open the Windows Services Manager.
2. Find the `HypervBackupAndRecoveryService` in the Services manager, right click on this service and select Properties.



3. In the property settings dialog, select Log On and set a domain user with local administrator privileges as the below example.



4. When done, apply the changes and restart the service.



Install on Windows Server Core in Silent Mode

If you are running Hyper-V natively on host hardware or within the Windows Server Core, you can install the backup plugin in silent mode.

To copy the installer to the Hyper-V host or Windows Server, you can use a USB flash drive to copy the installer to the Hyper-V host or Windows Server Core.

Or you can share the installer from your Windows PC, then from the Hyper-V host or Windows Server Core command lines to copy the installer.

To copy the shared installer, please first use the below command to establish a connection to the Windows PC.

```
net use \\ip_of_windows_pc\ipc$ pass /user:username
```

'ip_of_windows_pc' should be the exact IP address of the Windows PC which shares the installer.

'pass' should be the password of the Windows PC user.

'username' should be the username sharing the installer on the Windows PC.

Then use below command to copy the backup plugin installer to the Hyper-V host or Windows Server Core.

```
copy \\ip_of_windows_pc\foler\file_name1 \path\file_name2
```

'ip_of_windows_pc' should be the exact IP address of the Windows PC which shares the installer.

'folder_name1' should be the exact backup plugin installer file name.

'path' should be the full path on Hyper-V host or Windows Server Core where you want to save the installer.

'file_name2' can be a new file name or you can type the original file name to be saved on the Hyper-V host or Windows Server Core.

To install the backup plugin, please go to the directory where you copied the installer, then use the below command to install.

```
vinchin-hyper-v-agent.windows.7.0.0.xxx.exe /verysilent
```

Where 'xxx' should be the exact version number of the downloaded backup plugin installer.

After installation, please check the backup plugin service connection status using below command.

```
netstat -a
```

If you got active TCP connection on port 29200 and 29201 as shown below, then the backup plugin is successfully installed and services are up running.

```
  TCP    0.0.0.0:29200          WIN-L2MSB093K5D:0      LISTENING
  TCP    0.0.0.0:29201          WIN-L2MSB093K5D:0      LISTENING
```

Install Citrix Hypervisor Backup Plugin

Download Backup Plugin

The Citrix Hypervisor (XenServer) VM backup plugins can be downloaded from the login screen of Vinchin backup server's web console.

1. By clicking on **Download Backup Plugin**, you'll see the download options.
2. In **Type** dropdown list, select **VM Backup Plugin** option.
3. In **Platform** dropdown list, select **Citrix XenServer/Citrix Hypervisor**.
4. In the **Version** dropdown list, select the exact version of your Citrix Hypervisor (XenServer).
5. Click on **Download** button to download the installer.

Install Backup Plugin

The VM backup plugin for Citrix Hypervisor (XenServer) should be installed on the Citrix Hypervisor (XenServer) pool master host and the slave hosts, please upload the backup plugin installer to all the hosts for installation.

After the installer is uploaded, please install it from the Citrix Hypervisor (XenServer) hosts' command line interface (CLI) by using the below command.

```
rpm -i vxe-backup-agent-xxx.x86_64.rpm
```

Where the 'xxx' should be the version number same as the actual downloaded installer.

Please make sure you upload and install the backup plugin installer on all the Citrix Hypervisor (XenServer) hosts.

Notice

The backup plugin should NOT be installed on the Citrix Hypervisor (XenServer) guest OS.

Uninstall Backup Plugin

In order to reinstall the backup plugin or to install a newer version of backup plugin, you need to first uninstall the existing backup plugin.

To uninstall Vinchin backup plugin for Citrix Hypervisor (XenServer), please run the below command.

```
rpm -e vxe-backup-agent
```

Notice

If the Citrix Hypervisor (XenServer) backup plugin gets uninstalled without reinstallation or installing a newer version of backup plugin, your VM backup jobs will fail!

Install XCP-ng Backup Plugin

Download Backup Plugin

The XCP-ng VM backup plugin can be downloaded from the login screen of Vinchin backup server's web console.

1. By clicking on **Download Backup Plugin**, you'll see the download options.
2. In **Type** dropdown list, select **VM Backup Plugin** option.
3. In **Platform** dropdown list, select **XCP-ng**.
4. In the **Version** dropdown list, select the exact version of your XCP-ng virtual platform.
5. Click on **Download** button to download the installer.

Install Backup Plugin

The VM backup plugin for XCP-ng should be installed on the XCP-ng pool master host and also the slave hosts, please upload the backup plugin installer to all the hosts for installation.

After the installer is uploaded, please install it from the XCP-ng hosts' command line interface (CLI) by using the below command.

```
rpm -i vxe-backup-agent-xxx.x86_64.rpm
```

Where the 'xxx' should be the version number same as the actually downloaded installer.

Please make sure you upload and install the backup plugin installer on all the XCP-ng hosts.

Notice

The backup plugin should NOT be installed on the XCP-ng guest OS.

Uninstall XCP-ng Backup Plugin

In order to reinstall the backup plugin or to install a newer version of backup plugin, you need to first uninstall the existing backup plugin.

To uninstall Vinchin backup plugin for XCP-ng, please run the below command.

```
rpm -e vxe-backup-agent
```

Notice

If the XCP-ng backup plugin gets uninstalled without reinstallation or installing a newer version of backup plugin, your VM backup jobs will fail!

Install oVirt Backup Plugin

Download Backup Plugin

The oVirt VM backup plugin can be downloaded from the login screen of Vinchin backup server's web console.

1. By clicking on **Download Backup Plugin**, you'll see the download options.
2. In **Type** dropdown list, select **VM Backup Plugin** option.
3. In Platform dropdown list, select Red Hat Virtualization (RHV)/oVirt.
4. In the Version dropdown list, select the exact version of your oVirt virtual platform.
5. Click on Download button to download the installer.

Notice

If you are running oVirt 4.4.7 or newer versions, backup plugin is not required to be installed.

Install Backup Plugin

The VM backup plugin for oVirt should be installed on all the oVirt hosts, please upload the backup plugin installer to all the hosts for installation.

After the installer is uploaded, please install it from the oVirt hosts' command line interface (CLI) by using the below command.

```
yum install vinchin-stack-patch-cloud-xxx.x86_64.rpm
```

Where the 'xxx' should be the version number same as the actually downloaded installer.

Please make sure you upload and install the backup plugin installer on all the oVirt hosts.

Notice

1. The backup plugin for oVirt must be installed with yum command instead of rpm command.

2. Please DO NOT install the backup plugin on the oVirt engine!

Uninstall oVirt Backup Plugin

In order to reinstall the backup plugin or to install a newer version of backup plugin, you need to first uninstall the existing backup plugin.

To uninstall Vinchin backup plugin for oVirt, please run the below command.

```
rpm -e vinchin-stack-patch-cloud
```

Notice

If the oVirt backup plugin gets uninstalled without reinstallation or installing a newer version of backup plugin, your VM backup jobs will fail!

Install RHV Backup Plugin

Download Backup Plugin

The RHV VM backup plugin can be downloaded from the login screen of Vinchin backup server's web console.

1. By clicking on **Download Backup Plugin**, you'll see the download options.
2. In **Type** dropdown list, select **VM Backup Plugin** option.
3. In **Platform** dropdown list, select **Red Hat Virtualization (RHV)/oVirt**.
4. In the **Version** dropdown list, select the exact version of your RHV virtual platform.
5. Click on **Download** button to download the installer.

Notice

If you are running RHV 4.4.7 or newer versions, backup plugin is not required to be installed.

Install Backup Plugin

The VM backup plugin for RHV should be installed on all the RHV hosts, please upload the backup plugin installer to all the hosts for installation.

After the installer is uploaded, please install it from the RHV hosts' command line interface (CLI) by using the below command.

```
yum install vinchin-stack-patch-cloud-xxx.x86_64.rpm
```

Where the 'xxx' should be the version number same as the actually downloaded installer.

Please make sure you upload and install the backup plugin installer on all the RHV hosts.

Notice:

1. The backup plugin for RHV must be installed with yum command instead of rpm command.

2. Please DO NOT install the backup plugin on the RHV engine!

Uninstall RHV Backup Plugin

In order to reinstall the backup plugin or to install a newer version of backup plugin, you need to first uninstall the existing backup plugin.

To uninstall Vinchin backup plugin for RHV, please run the below command.

```
rpm -e vinchin-stack-patch-cloud
```

Notice

If the RHV backup plugin gets uninstalled without reinstallation or installing a newer version of backup plugin, your VM backup jobs will fail!

Install OLVM Backup Plugin

Download Backup Plugin

The OLVM VM backup plugin can be downloaded from the login screen of Vinchin backup server's web console.

1. By clicking on **Download Backup Plugin**, you'll see the download options.
2. In **Type** dropdown list, select **VM Backup Plugin** option.
3. In **Platform** dropdown list, select **Oracle Linux Virtualization Manager (OLVM)**.
4. In the **Version** dropdown list, select the exact version of your OLVM virtual platform.
5. Click on **Download** button to download the installer.

Notice

If you are running OLVM 4.4.8 or newer versions, backup plugin is not required to be installed.

Install Backup Plugin

The VM backup plugin for OLVM should be installed on all the OLVM hosts, please upload the backup plugin installer to all the hosts for installation.

After the installer is uploaded, please install it from the OLVM hosts' command line interface (CLI) by using the below command.

```
yum install vinchin-stack-patch-cloud-xxx.x86_64.rpm
```

Where the 'xxx' should be the version number same as the actually downloaded installer.

Please make sure you upload and install the backup plugin installer on all the OLVM hosts.

Notice

1. The backup plugin for OLVM must be installed with yum command instead of rpm command.

2. Please DO NOT install the backup plugin on the RHV engine!

Uninstall OLVM Backup Plugin

In order to reinstall the backup plugin or to install a newer version of backup plugin, you need to first uninstall the existing backup plugin.

To uninstall Vinchin backup plugin for OLVM, please run the below command.

```
rpm -e vinchin-stack-patch-cloud
```

Notice

If the OLVM backup plugin gets uninstalled without reinstallation or installing a newer version of backup plugin, your VM backup jobs will fail!

Install Sangfor HCI Backup Plugin

Download Backup Plugin

The Sangfor HCI VM backup plugin can be downloaded from the login screen of Vinchin backup server's web console.

1. By clicking on **Download Backup Plugin**, you'll see the download options.
2. In **Type** dropdown list, select **VM Backup Plugin** option.
3. In **Platform** dropdown list, select **Sangfor HCI**.
4. In the **Version** dropdown list, select the exact version of your Sangfor HCI virtual platform.
5. Click on **Download** button to download the installer.

Install Backup Plugin

The VM backup plugin for Sangfor HCI should be installed on all the Sangfor hosts, please upload the backup plugin installer to all the hosts for installation.

After the installer is uploaded, please install it from the Sangfor hosts' command line interface (CLI) .

1. By using the below command to decompress the .tar.gz package.

```
tar -zvxf vinchin-kvm-backup-patch-xxx-Debian.7-x86_64.tar.gz
```

Where the 'xxx' should be the version number same as the actually downloaded installer.

2. Enter the backup plugin package folder.

```
cd vinchin-kvm-backup-patch-xxx-Debian.7-x86_64
```

Where the 'xxx' should be the version number same as the installer package's version number.

3. Install with the below command.

```
./kvm_backup_patch_install
```

Please make sure you upload and install the backup plugin installer on all the Sangfor HCI hosts.

Uninstall Backup Plugin

In order to reinstall the backup plugin or to install a newer version of backup plugin, you need to first uninstall the existing backup plugin.

To uninstall Vinchin backup plugin for Sangfor HCI, please run the below command from Sangfor HCI host CLI.

```
./kvm_backup_patch_uninstall
```

The uninstall command should be executed from the folder decompressed from the installer package.

Notice

If the Sangfor HCI backup plugin gets uninstalled without reinstallation or installing a newer version of backup plugin, your VM backup jobs will fail!

Install H3C Backup Plugin

Download Backup Plugin

The H3C UIS/CAS VM backup plugin can be downloaded from the login screen of Vinchin backup server's web console.

1. By clicking on **Download Backup Plugin**, you'll see the download options.
2. In **Type** dropdown list, select **VM Backup Plugin** option.
3. In **Platform** dropdown list, select **H3C UIS/CAS**.
4. In the **Version** dropdown list, select the exact version of your H3C virtual platform.
5. Click on **Download** button to download the installer.

Install Backup Plugin

The VM backup plugin for H3C should be installed on all the H3C hosts, please upload the backup plugin installer to all the hosts for installation.

After the installer is uploaded, please install it from the H3C hosts' command line interface (CLI) .

1. By using the below command to decompress the .tar.gz package.

```
tar -zvxf vinchin-kvm-backup-patch-xxx-x86_64.tar.gz
```

Where the 'xxx' should be the version number same as the actually downloaded installer.

2. Enter the backup plugin package folder.

```
cd vinchin-kvm-backup-patch-xxx-x86_64
```

Where the 'xxx' should be the version number same as the installer package's version number.

3. Install with the below command.

```
./kvm_backup_patch_install
```

Please make sure you upload and install the backup plugin installer on all the H3C hosts.

Uninstall Backup Plugin

In order to reinstall the backup plugin or to install a newer version of backup plugin, you need to first uninstall the existing backup plugin.

To uninstall Vinchin backup plugin for H3C, please run the below command from H3C host CLI.

```
./kvm_backup_patch_uninstall
```

The uninstall command should be executed from the folder decompressed from the installer package.

Notice

If the H3C backup plugin gets uninstalled without reinstallation or installing a newer version of backup plugin, your VM backup jobs will fail!

Install ZStack Backup Plugin

Download Backup Plugin

The ZStack VM backup plugin can be downloaded from the login screen of Vinchin backup server's web console.

1. By clicking on **Download Backup Plugin**, you'll see the download options.
2. In **Type** dropdown list, select **VM Backup Plugin** option.
3. In **Platform** dropdown list, select **ZStack Cloud**.
4. In the **Version** dropdown list, select the exact version of your ZStack virtual platform.
5. Click on **Download** button to download the installer.

Install Backup Plugin

The VM backup plugin for ZStack should be installed on all the ZStack hosts, please upload the backup plugin installer to all the hosts for installation.

After the installer is uploaded, please install it from the ZStack hosts' command line interface (CLI) .

Enter the directory where you uploaded the backup plugin, and then use below command to install the backup plugin.

```
yum install vinchin-stack-patch-cloud-xxx-1.el7.x86_64.rpm
```

Where the ‘xxx’ should be the version number same as the actual downloaded installer.

Please make sure you upload and install the backup plugin installer on all the ZStack hosts.

Uninstall Backup Plugin

In order to reinstall the backup plugin or to install a newer version of backup plugin, you need to first uninstall the existing backup plugin.

To uninstall Vinchin backup plugin for ZStack, please run the below command from ZStack host CLI.

```
rpm -e vinchin-stack-patch-cloud
```

The uninstall command should be executed from the folder decompressed from the installer package.

Notice

If the ZStack backup plugin gets uninstalled without reinstallation or installing a newer version of backup plugin, your VM backup jobs will fail!

Install Proxmox VE Backup Plugin

Download Backup Plugin

The Proxmox VE VM backup plugins can be downloaded from the login screen of Vinchin backup server's web console.

1. By clicking on **Download Backup Plugin**, you'll see the download options.
2. In **Type** dropdown list, select **VM Backup Plugin** option.
3. In **Platform** dropdown list, select **Proxmox VE**.
4. In the **Version** dropdown list, select the exact version of your Proxmox VE.
5. Click on **Download** button to download the installer.

Install Backup Plugin

The VM backup plugin for Proxmox VE should be installed on the Proxmox VE pool master host and the slave hosts, please upload the backup plugin installer to all the hosts for installation.

After the installer is uploaded, please install it from the Proxmox VE hosts' command line interface (CLI) by using the below command:

```
dpkg -i vinchin-stack-patch-cloud-xxx.Ubuntu.x86_64.deb
```

Where the 'xxx' should be the version number same as the actual downloaded installer.

Please make sure you upload and install the backup plugin installer on all the Proxmox VE hosts.

Uninstall Backup Plugin

In order to reinstall the backup plugin or to install a newer version of backup plugin, you need to first uninstall the existing backup plugin.

To uninstall Vinchin backup plugin for Proxmox VE, please run the below command from Proxmox VE host CLI.

```
dpkg -P vinchin-stack-patch-cloud
```

The uninstall command should be executed from the folder decompressed from the installer package.

Notice

If the Proxmox VE backup plugin gets uninstalled without reinstallation or installing a newer version of backup plugin, your VM backup jobs will fail!

Install OpenStack Backup Plugin

Download Backup Plugin

The OpenStack VM backup plugin can be downloaded from the login screen of Vinchin backup server's web console.
1. By clicking on **Download Backup Plugin**, you'll see the download options.
2. In **Type** dropdown list, select **VM Backup Plugin** option.
3. In **Platform** dropdown list, select **OpenStack**.
4. In the Version dropdown list, select the exact version of your OpenStack virtual platform.
Cloud (RHEL) is for OpenStack on Red Hat Enterprise Linux, the downloaded backup plugin installer shoud be a .rpm package.
Cloud (UBUNTU) is for OpenStack on Ubuntu Linux, the downloaded backup plugin installer should be a .deb package.
Docker (RHEL) is for OpenStack containerized with Docker on Red Hat Enterprise Linux, the downloaded backup plugin installer should be a .rpm package.
Docker (UBUNTU) is for OpenStack containerized with Docker on Ubuntu Linux, the downloaded backup plugin installer should be a .deb package.
5. Click on **Download** button to download the installer.

Install Backup Plugin

The VM backup plugin for OpenStack should be installed on all the controller nodes, if the controller nodes can SSH log in to the compute nodes without using a password, then you don't have to install backup plugin on the compute nodes, otherwise, the backup plugin should also be installed on all the compute nodes.
Please upload the backup plugin installer to all the hosts for installation.
After the installer is uploaded, please install it from the OpenStack hosts' command line interface (CLI).
Cloud (RHEL) install with the below command.

```
rpm -i vinchin-stack-patch-cloud-xxx.x86_64.rpm
```

Cloud (UBUNTU) install with the below command.

```
sudo dpkg -i vinchin-stack-patch-cloud-xxx.Ubuntu.x86_64.deb
```

Docker (RHEL) install with the below command.

```
rpm -i vinchin-stack-patch-docker-xxx.x86_64.rpm
```

Docker (UBUNTU) install with the below command.

```
sudo dpkg -i vinchin-stack-patch-docker-xxx.Ubuntu.x86_64.deb
```

Please make sure you upload and install the backup plugin installer on all the OpenStack hosts.

Uninstall Backup Plugin

In order to reinstall the backup plugin or to install a newer version of backup plugin, you need to first uninstall the

existing backup plugin.

To uninstall Vinchin backup plugin for OpenStack, please run the below command from OpenStack host CLI.

Cloud (RHEL) uninstall with the below command.

```
rpm -e vinchin-stack-patch-cloud
```

Cloud (UBUNTU) uninstall with the below command.

```
sudo dpkg -r vinchin-stack-patch-cloud
```

Docker (RHEL) uninstall with the below command.

```
rpm -e vinchin-stack-patch-docker
```

Docker (UBUNTU) uninstall with the below command.

```
sudo dpkg -r vinchin-stack-patch-docker
```

Notice

If the OpenStack backup plugin gets uninstalled without reinstallation or installing a newer version of backup plugin, your VM backup jobs will fail!

Add Virtual Infrastructure

VMware vShpere

Add VMware vSphere Virtual Platform

To add VMware vCenter server or standalone ESXi host to Vinchin, follow the steps below.
1. Go to **Resources** > **Virtual Infrastructure** > **Virtual Platform** page.
2. Click on **Add** button.
3. In the **Platform** dropdown list, select **VMware vSphere**.
4. In the **IP/Domain** field, specify the IP address or domain name of the vCenter server, or if it's a standalone ESXi host, please specify the IP address or domain name of the standalone ESXi host that you wish to add.
5. In the **Username** and **Password** fields, specify credentials of the vCenter server or standalone ESXi host.
6. In the **Name** field, specify a custom name for this newly added virtual platform.
7. Click on **OK** to add the VMware virtual platform.

Notice
Please make sure Vinchin backup server can access the VMware virtual platform on ports 443 and 902, otherwise you will not be able to add virtual platform or perform VM backup.

License VMware Virtual Platform for Backup

Once you had successfully added the VMware virtual platform to Vinchin backup server, in the **Virtual Platform List**, the VMware virtual platform will be listed.
If your license type is "Per CPU Sockets", the VMware virtual platform will be **Unlicensed** state, at this moment you are unable to create any backup job for the VMware VMs.
To get the VMware virtual platform licensed for backup, please do as follows.
1. Click on the **License** button.
2. In the **Host Licensing** dialog, select all hosts of the VMware virtual platform.
3. Click on **License** button to get the VMware hosts Licensed for VM backup.
Once the VMware virtual platform gets licensed, you are now able to create backup jobs for the VMware VMs.

Add Hyper-V Virtual Platform

To add Hyper-V virtual platform to Vinchin, follow the below steps.
1. Go to **Resources** > **Virtual Infrastructure** > **Virtual Platform** page.
2. Click on **Add** button.
3. In the **Platform** dropdown list, select **Microsoft Hyper-V**.
4. In the **Type** dropdown list select the deployment type of you Hyper-V.
5. In the **IP/Domain** field, enter the SCVMM server IP if your Hyper-V virtual platform is managed by a SCVMM management server; enter the cluster IP if your Hyper-V virtual platform is deployed as Failover Cluster; enter the IP address of the Hyper-V server or Windows Server with Hyper-V Role, if it's a standalone deployment.
6. In the **Username** field, enter the domain user with administrator permissions of the SCVMM server and all other hosts if your Hyper-V virtual platform is managed by a SCVMM management server; enter the domain user with local administrator permissions of all clustered hosts if it's a failover clustering environment; enter the administrator username if it's a standalone deployment.
7. In the **Password** field enter the corresponding password of the username you specified above.
8. In the **Name** field, specify a custom name for this newly added virtual infrastructure.
9. Click on **OK** to add the Hyper-V virtual platform.

Notice
Please make sure Vinchin backup server can access the Hyper-V virtual platform on port 29200 and 29201, otherwise you will not be able to add virtual platform or perform VM backup.

License Hyper-V Virtual Platform for Backup

Once you had successfully added the Hyper-V virtual platform to Vinchin backup server, in the **Virtual Platform List**, the Hyper-V virtual platform will be listed.
If your license type is "Per CPU Sockets", the Hyper-V virtual platform will be Unlicensed state, at this moment you are unable to create any backup job for the Hyper-V VMs.
To get the Hyper-V virtual platform licensed for backup, please do as follows.
1. Click on the **License** button.
2. In the **Host Licensing** dialog, select all hosts of the Hyper-V virtual platform.
3. Click on **License** button to get the Hyper-V hosts licensed for VM backup.
Once the Hyper-V virtual platform gets licensed, you are now able to create backup jobs for the VMs.

Citrix Hypervisor

Add Citrix Virtual Platform

To add Citrix Hypervisor (XenServer) virtual platform to Vinchin, follow the below steps.

1. Go to **Resources** > **Virtual Infrastructure** > **Virtual Platform** page.
2. Click on **Add** button.
3. In the **Platform** dropdown list, select **Citrix XenServer/Citrix Hypervisor**.
4. In the **IP/Domain** field, specify the IP address or domain name of the Citrix pool master.
5. In the **Username** and **Password** fields, specify credentials of the pool master host.
6. In the **Name** field, specify a custom name for this newly added virtual infrastructure.
7. Click on **OK** to add the Citrix Hypervisor (XenServer) virtual platform.

Notice

Please make sure Vinchin backup server can access the Citrix virtual platform on port 80, 443 and 29202, otherwise you will not be able to add virtual platform or perform VM backup.

License Citrix Virtual Platform for Backup

Once you had successfully added the Citrix Hypervisor (XenServer) virtual platform to Vinchin backup server, in the **Virtual Platform List**, the Citrix Hypervisor (XenServer) virtual platform will be listed.

If your license type is "Per CPU Sockets", the Citrix Hypervisor (XenServer) virtaul platform will be Unlicensed state, at this moment you are unable to create any backup job for the Citrix VMs.

To get the Citrix virtual platform licensed for backup, please do as follows.

1. Click on the **License** button.
2. In the **Host Licensing** dialog, select all hosts of the Citrix Hypervisor (XenServer) virtual platform.
3. Click on **License** button to get the Citrix Hypervisor (XenServer) hosts autorized for VM backup.

Once the Citrix virtual platform gets licensed, you are now able to create backup jobs for the Citrix VMs.

XCP-ng

Add XCP-ng Virtual Platform

To add XCP-ng virtual platform to Vinchin, follow the below steps.

1. Go to **Resources** > **Virtual Infrastructure** > **Virtual Platform** page.
2. Click on **Add** button.
3. In the **Platform** dropdown list, select **XCP-ng**.
4. In the **IP/Domain** field, specify the IP address or domain name of the XCP-ng pool master.
5. In the **Username** and **Password** fields, specify credentials of the pool master host.
6. In the **Name** field, specify a custom name for this newly added virtual platform.

7. Click on **OK** to add the XCP-ng virtual platform.

Notice

Please make sure Vinchin backup server can access the XCP-ng virtual platform on port 80, 443 and 29202, otherwise you will not be able to add virtual platform or perform VM backup.

License XCP-ng Virtual Platform for Backup

Once you had successfully added the XCP-ng virtual platform to Vinchin backup server, in the **Virtual Platform List**, the XCP-ng virtual platform will be listed.

If your license type is "Per CPU Sockets", the XCP-ng virtual platform will be Unlicensed state, at this moment you are unable to create any backup job for the XCP-ng VMs.

To get the XCP-ng virtual platform licensed for backup, please do as follows.

1. Click on the **License** button.
2. In the **Host Licensing** dialog, select all hosts of the XCP-ng virtual platform.
3. Click on **License** button to get the XCP-ng hosts Licensed for VM backup.

Once the XCP-ng virtual platform gets licensed, you are now able to create backup jobs for the XCP-ng VMs.

oVirt

Add oVirt Virtual Platform

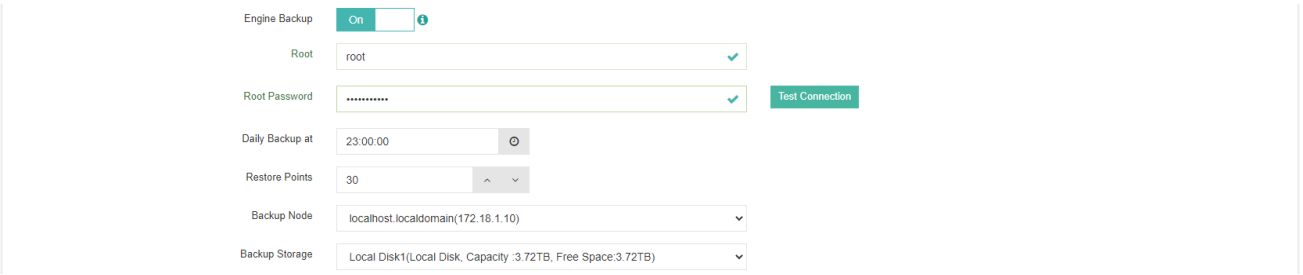
To add oVirt virtual platform to Vinchin, follow the steps below.

1. Go to **Resources** > **Virtual Infrastructure** > **Virtual Platform** page.
2. Click on **Add** button.
3. In the **Platform** dropdown list, select **oVirt**.
4. In the **IP/Domain** field, specify the IP address or domain name of the oVirt engine.
5. For the **Username** field, there are 2 circumstances.

- If you are running oVirt version 4.5.0 or older versions, or if you had upgraded from older versions to 4.5.1 or newer, default username is “admin” and it should be used with the “internal” domain, so you should type “admin@internal” here.
- If it's a fresh new installation of oVirt 4.5.1 or newer version, Keycloak is configured as a default SSO provider for oVirt Engine, you should use “admin@ovirt@internalsso” as the username.

6. In the **Password** field, please type in the password for oVirt engine admin user.
7. In the **Name** field, specify a custom name for this newly added virtual platform.
8. As for **Engine Backup**, it is optional, it can be used to backup the oVirt engine metadata.

To enable engine backup, you need to use root permission of the oVirt engine.



With the above settings, Vinchin Backup & Recovery will automatically backup oVirt engine at 11pm every day, and 30 backups will be saved for restore purpose.

9. Click on **OK** to add the oVirt virtual platform.

Notice

Please make sure Vinchin backup server can access the oVirt virtual platform on port 443, 29203 and 29204, otherwise you will not be able to add virtual platform or perform VM backup.

License oVirt Virtual Platform for Backup

Once you had successfully added the oVirt virtual platform to Vinchin backup server, in the **Virtual Platform List**, the oVirt virtual platform will be listed.

If your license type is "Per CPU Sockets", the oVirt virtual platform will be in Unlicensed state, at this moment you are unable to create any backup job for the oVirt VMs.

To get the oVirt virtual platform licensed for backup, please do as follows.

1. Click on the **License** button.
2. In the **Host Licensing** dialog, select all hosts of the oVirt virtual platform.
3. Click on **License** button to get the oVirt hosts licensed for VM backup.

Once the oVirt virtual platform gets licensed, you are now able to create backup jobs for the oVirt VMs.

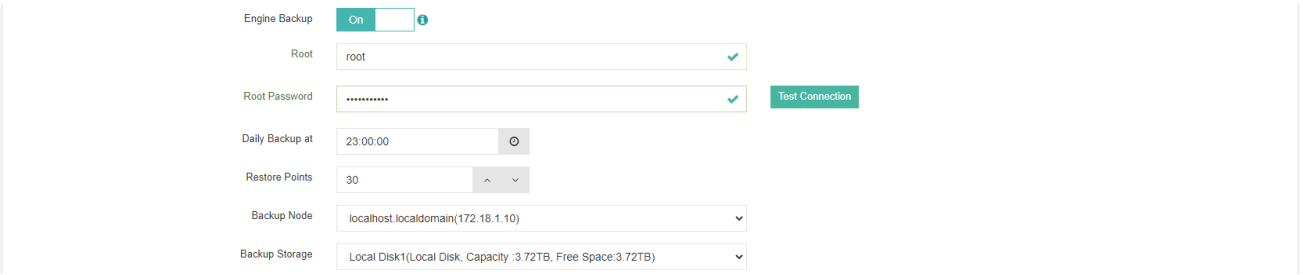
Red Hat Virtualization (RHV)

Add RHV Virtual Platform

To add RHV virtual platform to Vinchin, follow the steps below.

1. Go to **Resources** > **Virtual Infrastructure** > **Virtual Platform** page.
2. Click on **Add** button.
3. In the **Platform** dropdown list, select **Red Hat Virtualization (RHV)**.
4. In the **IP/Domain** field, specify the IP address or domain name of the RHV engine.
5. In the **Username** field, the default username is “admin” and it should be used with the “internal” domain, so you should probably type “admin@internal” here.
6. In the **Password** field, please type in the password for RHV engine admin user.
7. In the **Name** field, specify a custom name for this newly added virtual platform.
8. As for **Engine Backup**, it is optional, it can be used to backup the RHV engine metadata.

To enable engine backup, you need to use root permission of the RHV engine.



With the above settings, Vinchin Backup & Recovery will automatically backup RHV engine at 11pm every day, and 30 backups will be saved for restore purpose.

8. Click on **OK** to add the RHV virtual platform.

Notice

Please make sure Vinchin backup server can access the RHV virtual platform on port 443, 29203 and 29204, otherwise you will not be able to add virtual platform or perform VM backup.

License RHV Virtual Platform for Backup

Once you had successfully added the RHV virtual platform to Vinchin backup server, in the **Virtual Platform List**, the RHV virtual platform will be listed.

If your license type is "Per CPU Sockets", the RHV virtual platform will be Unlicensed state, at this moment you are unable to create any backup job for the RHV VMs.

To get the RHV virtual platform licensed for backup, please do as follows.

1. Click on the **License** button.
2. In the **Host Licensing** dialog, select all hosts of the RHV virtual platform.
3. Click on **License** button to get the RHV hosts licensed for VM backup.

Once the RHV virtual platform gets licensed, you are now able to create backup jobs for the RHV VMs.

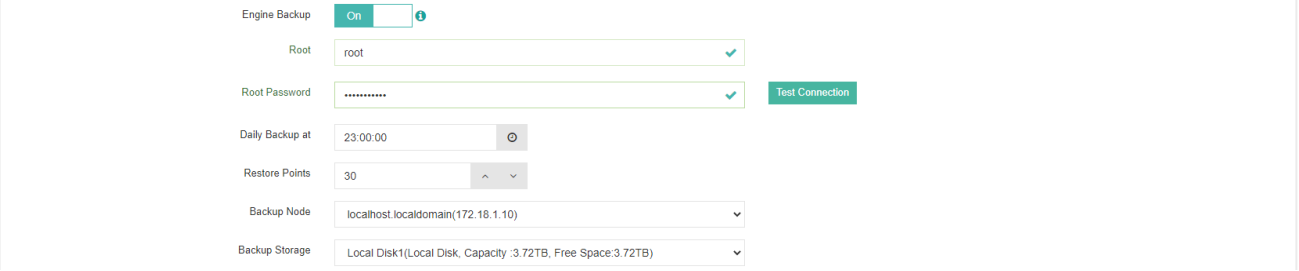
Oracle Linux Virtualization Manager (OLVM)

Add OLVM Virtual Platform

To add OLVM virtual platform to Vinchin, follow the steps below.

1. Go to **Resources** > **Virtual Infrastructure** > **Virtual Platform** page.
2. Click on **Add** button.
3. In the **Platform** dropdown list, select **Oracle Linux Virtualization Manager (OLVM)**.
4. In the **IP/Domain** field, specify the IP address or domain name of the OLVM engine.
5. In the **Username** field, the default username is “admin” and it should be used with the “internal” domain, so you should probably type “admin@internal” here.
6. In the **Password** field, please type in the password for OLVM engine admin user.
7. In the **Name** field, specify a custom name for this newly added virtual platform.
8. As for **Engine Backup**, it is optional, it can be used to backup the OLVM engine metadata.

To enable engine backup, you need to use root permission of the OLVM engine.



With the above settings, Vinchin Backup & Recovery will automatically backup OLVM engine at 11pm every day, and 30 backups will be saved for restore purpose.

8. Click on **OK** to add the OLVM virtual platform.

Notice

Please make sure Vinchin backup server can access the OLVM virtual platform on port 443, 29203 and 29204, otherwise you will not be able to add virtual platform or perform VM backup.

License OLVM Virtual Platform for Backup

Once you had successfully added the OLVM virtual platform to Vinchin backup server, in the **Virtual Platform List**, the OLVM virtual platform will be listed.

If your license type is "Per CPU Sockets", the OLVM virtual platform will be Unlicensed state, at this moment you are unable to create any backup job for the OLVM VMs.

To get the OLVM virtual platform licensed for backup, please do as follows.

1. Click on the **License** button.
2. In the **Host Licensing** dialog, select all hosts of the OLVM virtual platform.
3. Click on **License** button to get the OLVM hosts licensed for VM backup.

Once the OLVM virtual platform gets licensed, you are now able to create backup jobs for the OLVM VMs.

Sangfor HCI

Add Sangfor HCI Virtual Platform

To add Sangfor HCI virtual platform to Vinchin, follow the below steps.

1. Go to **Resources** > **Virtual Infrastructure** > **Virtual Platform** page.
2. Click on **Add** button.
3. In the **Platform** dropdown list, select **Sangfor HCI**.
4. In the **IP/Domain** field, specify the IP address of the Sangfor HCI master node, or if it's cluster deployment, the virtual IP of the cluster must be used here.
5. In the **Username** and **Password** fields, specify credentials of the super admin user.
6. In the **Name** field, specify a custom name for this newly added virtual platform.
7. Click on **OK** to add the Sangfor HCI virtual platform.

If you are running Sangfor HCI 6.3 or higher versions, please enable SSH port from Sangfor HCI web console on the **System** -> **Port Management** page.

And if you had enabled **Allow SSH Access by IP Address** option, please add Vinchin backup server's IP address into the **IP Address** list at the bottom of this page. Otherwise Vinchin will fail to backup the UEFI boot mode VMs.

Notice

Please make sure Vinchin backup server can access the Sangfor HCI virtual platform on port 443, 29203 and 29204, otherwise you will not be able to add virtual platform or perform VM backup.

License Sangfor HCI Virtual Platform for Backup

Once you had successfully added the Sangfor HCI virtual platform to Vinchin backup server, in the **Virtual Platform List**, the Sangfor HCI virtual platform will be listed.

If your license type is "Per CPU Sockets", the Sangfor HCI virtaul platform will be Unlicensed state, at this moment you are unable to create any backup job for the Sangfor HCI VMs.

To get the Sangfor HCI virtual platform licensed for backup, please do as follows.

1. Click on the **License** button.
2. In the **Host Licensing** dialog, select all hosts of the Sangfor HCI virtual platform.
3. Click on **License** button to get the Sangfor HCI hosts licensed for VM backup.

Once the Sangfor HCI virtual platform gets licensed, you are now able to create backup jobs for the VMs.

Huawei FusionCompute

Add Huawei FusionCompute Virtual Platform

To add Huawei FusionCompute virtual platform to Vinchin, follow the below steps.

1. Go to **Resources** > **Virtual Infrastructure** > **Virtual Platform** page.
2. Click on **Add** button.
3. In the **Platform** dropdown list, select **Huawei FusionCompute (KVM)**.
4. In the **IP/Domain** field, specify the IP address and port number of the FusionCompute Virtual Resource Manager (VRM) server in format "server_ip:7443" without quotes. E.g., 172.18.5.202:7443.
5. In the **Username** field, the northbound interface authentication account should be used, the default username used by FusionCompute is "gesysman".
6. In the **Password** field, please type in the northbound interface authentication account password.
7. In the **Name** field, specify a custom name for this newly added virtual platform.
8. Click on **OK** to add the Huawei FusionCompute virtual platform.

Notice

Please make sure Vinchin backup server can access the Huawei FusionCompute virtual platform on port 7443, 35000~35020, otherwise you will not be able to add virtual platform or perform VM backup.

License Huawei FusionCompute Virtual Platform for Backup

Once you had successfully added the Huawei FusionCompute virtual platform to Vinchin backup server, in the **Virtual Platform List**, the virtual platform will be listed.
If your license type is "Per CPU Sockets", the Huawei FusionCompute virtaul platform will be Unlicensed state, at this moment you are unable to create any backup job for the Huawei FusionCompute VMs.
To get the Huawei FusionCompute virtual platform licensed for backup, please do as follows.
1. Click on the **License** button.
2. In the **Host Licensing** dialog, select all hosts of the Huawei FusionCompute virtual platform.
3. Click on **License** button to get all the hosts licensed for VM backup.
Once the Huawei FusionCompute virtual platform gets licensed, you are now able to create backup jobs for the Huawei FusionCompute VMs.

H3C

Add H3C Virtual Platform

To add H3C virtual platform to Vinchin, follow the below steps.
1. Go to **Resources** > **Virtual Infrastructure** > **Virtual Platform** page.
2. Click on **Add** button.
3. In the **Platform** dropdown list, select **H3C UIS/CAS**.
4. In the **IP/Domain** field, specify the IP address and port number of the H3C CVM server in format "server_ip:8080" without quotes.
5. In the **Username** and **Password** fields, specify credentials of the administrator.
6. In the **Name** field, specify a custom name for this newly added virtual platform.
7. Click on **OK** to add the H3C virtual platform.

Notice
Please make sure Vinchin backup server can access the H3C virtual platform on port 443, 29203 and 29204, otherwise you will not be able to add virtual platform or perform VM backup.

License H3C Virtual Platform for Backup

Once you had successfully added the H3C virtual platform to Vinchin backup server, in the **Virtual Platform List**, the H3C virtual platform will be listed.
If your license type is "Per CPU Sockets", the H3C virtual platform will be Unlicensed state, at this moment you are unable to create any backup job for the H3C VMs.
To get the H3C virtual platform licensed for backup, please do as follows.
1. Click on the **License** button.
2. In the **Host Licensing** dialog, select all hosts of the H3C virtual platform.
3. Click on **License** button to get the H3C hosts licensed for VM backup.

Once the H3C virtual platform gets licensed, you are now able to create backup jobs for the H3C VM instance.

ZStack Cloud

Add ZStack Cloud Virtual Platform

To add ZStack virtual platform to Vinchin, follow the below steps.
1. Go to **Resources** > **Virtual Infrastructure** > **Virtual Platform** page.
2. Click on **Add** button.
3. In the **Platform** dropdown list, select **ZStack Cloud**.
4. In the **IP/Domain** field, specify the IP address and port number of the ZStack management node in format "node_ip:8080" without quotes.
5. In the **Username** and **Password** fields, specify credentials of the administrator.
6. In the **Name** field, specify a custom name for this newly added virtual infrastructure.
7. Click on **OK** to add the ZStack Cloud virtual platform.

Notice
Please make sure Vinchin backup server can access the ZStack virtual platform on port 443, 29203 and 29204, otherwise you will not be able to add virtual platform or perform VM backup.

Authorize ZStack Virtual Platform for Backup

Once you had successfully added the ZStack virtual platform to Vinchin backup server, in the **Virtual Platform List**, the ZStack virtual platform will be listed.
If your license type is "Per CPU Sockets", the ZStack virtual platform will be Unlicensed state, at this moment you are unable to create any backup job for the ZStack VM instances.
To get the ZStack virtual platform licensed for backup, please do as follows.
1. Click on the **License** button.
2. In the **Host Licensing** dialog, select all hosts of the ZStack virtual platform.
3. Click on **License** button to get the ZStack hosts licensed for VM backup.
Once the ZStack virtual platform gets licensed, you are now able to create backup jobs for the ZStack VM instances.

Proxmox VE

Add Proxmox VE Virtual Platform

To add Proxmox VE virtual platform to Vinchin, follow the below steps.
1. Go to **Resources > Virtual Infrastructure > Virtual Platform** page.
2. Click on Add button.

3. In the Platform dropdown list, select Proxmox VE.
4. In the IP/Domain field, specify the IP address and port number of the Proxmox VE server in format "server_ip:8006" without quotes.
5. In the Username and Password fields, specify credentials of the administrator.
6. In the Name field, specify a custom name for this newly added virtual platform.
7. Click on OK to add the Proxmox VE virtual platform.

Notice

Please make sure Vinchin backup server can access the Proxmox VE virtual platform on port 443, 29203 and 29204, otherwise you will not be able to add virtual platform or perform VM backup.

License Proxmox VE Virtual Platform for Backup

Once you had successfully added the Proxmox VE virtual platform to Vinchin backup server, in the Virtual Platform List, the Proxmox VE virtual platform will be listed.
If your license type is "Per CPU Sockets", the Proxmox VE virtual platform will be Unlicensed state, at this moment you are unable to create any backup job for the Proxmox VE VMs.
To get the Proxmox VE virtual platform licensed for backup, please do as follows.
1. Click on the License button.
2. In the Host Licensing dialog, select all hosts of the Proxmox VE virtual platform.
3. Click on License button to get the Proxmox VE hosts licensed for VM backup.
Once the Proxmox VE virtual platform gets licensed, you are now able to create backup jobs for the VMs.

OpenStack

Add OpenStack Cloud Platform

To add OpenStack cloud platform to Vinchin backup server, please do as follows.
1. Go to **Resources** > **Virtual Infrastructure** > **Cloud Platform** page.
2. Click on **Add** button.
3. In the **Platform** dropdown list, select **OpenStack**.
4. In the **IP/Domain Name** field, please enter the `kolla_internal_vip_address` or the `kolla_internal_fqdn`.
5. By turning the **Advanced Settings** option on, you can configure the endpoint API from **Public**, **Admin** or **Internal**. For the port number, please use the default port number, otherwise you need to check the keystone identity services to determine the port number. For the **Domain**, please enter the Keystone domain which the project belongs to.
8. In the **Username** and **Password** fields, enter the credentials for the project admin.
9. In the **Name** field, specify a custom name for this newly added virtual infrastructure.
10. Click on **OK** to add OpenStack virtual platform.

License OpenStack Cloud Platform for Backup

Once OpenStack cloud platform has been successfully added, it will be listed in the **Cloud Platform List**.
If you are running Vinchin Backup & Recovery with the free trial license, the OpenStack virtaul platform will be in Unlicensed state, at this moment you are unable to create any backup job for the VM instances.
To get the OpenStack virtual platform licensed for backup, please do as follows.
1. Click on the **License** button.
2. In the **Host Licensing** dialog, select all hosts of the OpenStack cloud platform.
3. Click on **License** button to get the OpenStack hosts licensed for VM backup.
Once the OpenStack virtual platform gets licensed, you are now able to create backup jobs for the VM instances.

Notice
The recommended license model of Vinchin Backup & Recovery to backup OpenStack cloud platform is "Per VM License", if you wish to use the "Per VM License", please contact your Vinchin account manager or contact Vinchin Support Team for help.

Overview of VM Backup Features

This section contains the following topics:

- Backup Methods
- Backup Data Reduction
- Backup Data Encryption
- Retention Policy
- GFS Retention
- Data Transmission
- Incremental Mode

Backup Methods

With Vinchin Backup & Recovery, you can schedule Full Backup, Incremental Backup, Differential Backup and Forever Incremental Backup to protect your VMs.

Full Backup

The full backup is the most complete type of backup, it will create a full copy of the data assets to the backup repository. It is considered the simplest way for backup and recovery, but at the same time, it is the most storage space occupation and time-consuming backup method. As a result, it is either scheduled with longer backup intervals or shorter retention time.

Incremental Backup

Incremental backup is a backup method which backs up the new and changed data since the previous backup (full or incremental). Usually, it requires a full backup to be taken in longer time intervals, and then run the incremental backups in shorter time intervals.

Differential Backup

Differential backup is the backup method which backs up the new and changed data since the previous full backup.

Forever Incremental Backup

Forever Incremental backup will start with an initial full backup and then runs incremental backups without any further full backups. In other words, it always backs up the new and changed data blocks comparing to the previous backup.

Backup Data Reduction

Vinchin Backup & Recovery provides multiple methods, such as Data deduplication, Data compression and BitDetector (a unique feature in Vinchin Backup & Recovery), to reduce the size of stored backups.
This section contains the following topics:

- Data Deduplication
- Data Compression
- BitDetector

Data Deduplication

Data deduplication is a method for reducing backup size. With data deduplication enabled, Vinchin Backup & Recovery reduce the amount of backup data stored by eliminating duplicated and zeroed data blocks and storing only the unique data blocks. It's a built-in functionality and do not require storage server support.

Data Compression

Data compression a method for reducing backup size. With data compression enabled, compress backup data in specific block size to save backup storage space. Utilizes the high efficiency LZO compression algorithm, compression ratio can be more than 50%. It's a built-in functionality and do not require storage server support.

BitDetector

BitDetector is a Vinchin unique feature for VM backup, it is a feature set which consists of exclude the following items from backing up.

- Swap file blocks
- Deleted file blocks
- unpartitioned spaces and partition gaps

BitDetector currently works on NTFS filesystem, with BitDetector, all the above-mentioned data of the Windows VMs will be excluded from backing up. Except data deduplication and compression, it is another important feature which helps reducing the backup data size.

Backup Data Encryption

Backup data encryption, is a feature designed to protect your backup data from unauthorized access.
When it’s enabled, the backup data will be encrypted and then written into backup storage, a password can be used to secure the backups. When restoring those data, password verification is required before restoration.

Retention Policy

Short-term Retention

Retention policy defines the number of restore points or number of days to keep your backup data. Specify the restore points/days Vinchin Backup & Recovery will purge the obsolete
points/days from backup storage, keep the latest restore points/days.

- **Differential backup job**: Each differential restore point depends on the previous full restore point. When retention policy has been triggered, Vinchin Backup & Recovery will start deleting the earliest differential restore points, when all the differential restore points between the first and the second full restore points had been deleted, and when retention policy has been triggered for the next time, the first full restore point will be deleted.
- **Incremental backup job**: When the retention policy of an incremental backup job has been triggered, Vinchin Backup & Recovery will try to merge the first incremental restore point with the full restore point on the first backup chain, the full restore point will step forward and the first incremental restore point will be gone. It will run the same process until all incremental restore points had been merged with the first full restore point. After that when the retention policy had been triggered for the next time, the first full restore point will be deleted, and then the second backup chain becomes the first and the restore point merging process goes on the same way
- **Forever incremental backup job**: Different from incremental backup, forever incremental backup will only create one backup chain for each VM included in the job, when retention policy has been triggered, Vinchin Backup & Recovery will merge the first incremental restore point with the only full restore point at the beginning of the backup chain, and the timestamp of the full restore point will keep stepping forward each time when the incremental restore point had been merged.

Warning

If you select Retention Mode as Number of Days, please be cautious of while Vinchin Backup & Recovery have been powered off for several days (over retention days), retention policy will trigger while you start Vinchin Backup & Recovery. The data will be expired and deleted.

Long-term (GFS) Retention

GFS retention, also as known as Grandfather-Father-Son retention. It is a long-term data retention policy which allows you to retain your VM backups for longer period of time using a minimal amount of storage resource. Vinchin Backup & Recovery implemented GFS retention to retain the following backups for different periods of time respectively:

- Weekly full backup
- Monthly full backup
- Yearly full backup

For the weekly full backup, you can specify a day of the week on which the full backup is supposed to be created, and specify for how long (how many weeks) to be retained. Then Vinchin Backup & Recovery will start to wait and tag the first coming full backup of the week. The tagged full backup will be retained for the specified number of

weeks, and the general short-term retention policy will not purge the tagged weekly full backup until the tag is expired. As for the monthly and yearly full backups, GFS retention works the same way.
GFS retention policy can be configured during the VM backup job creation process, when the job started to run regularly according to its schedule. The specific backups will also be tagged automatically as per your configurations.
The tagged full backups (restore points) can be seen on the **VM Backup** > **Backup Data** page, the tags can be added or removed manually on the same page if needed, but GFS retention only works with full backups (full restore points).
GFS retention works independently with the general short-term retention policy, so you can implement both general and GFS retention policies in a VM backup job. Additionally, for some specific backups, you can manually tag them with the forever retention tag to keep them in the backup storage permanently.

Data Transmission

Vinchin offers various data transmission options for users to perform VM backup. Users can choose flexibly from the following transmission options based on user demands and the actual virtual and backup infrastructure deployments.

- LAN
- LAN Encrypted
- LAN-free
- HotAdd
- NBD
- ImageIO
- Backup Proxy
- Transmission Network

LAN

The local area network (LAN) can be the production network or a dedicated network for transmission. With this option chosen, VM data will be transferred using the TCP/IP connection between the source virtual platform and the target backup storage.

Encrypted Transmission

When VM data is being transmitted over the network, Vinchin Backup & Recovery will encrypt the transmission path to guarantee the data is not compromised during backup and restore processes.

LAN-free

For virtual infrastructures with central storage servers, system administrators usually use a storage area network, to improve data storage efficiency, redundancy, and flexibility.
To backup virtual machines within this kind of virtual infrastructure, users can use the existing SAN for virtual

machine backup and recovery. It is also called LAN-free backup.
The benefits of implementing LAN-Free backup and recovery are as follows:

- The backup and recovery data flows will only go through the SAN without passing it through the hosts and production network.
- Minimize the impact on critical business operations.
- The highly efficient backup and recovery process can minimize possible business downtime.
- More backup job sessions can be scheduled for shorter RPOs.

Backup data can be transferred from the production storage area to the backup storage area directly via SAN using Fibre Channel (FC), Internet SCSI (iSCSI), or NFS protocols.
To transfer via SAN (LAN-free), you need to add a LAN-free path from the **Resources** > **Virtual Infrastructure** > **LAN-free** page first.

HotAdd

HotAdd is a VMware ESXi server capability which enables the VM virtual disks to be directly attached to the backup server VM, the backup server VM can then read data blocks from/to the virtual disks directly bypassing the hypervisor's (VMware ESXi) TCP/IP stack.
Vinchin Backup & Recovery provides 2 ways to utilize HotAdd transport for VMware vShpere virtual machine backup.
1. If your Vinchin backup server is installed as a VM within the VMware ESXi cluster, you can directly enable HotAdd transport mode.
2. If your Vinchin backup server is installed on a physical machine, to be able to utilize HotAdd transport functionality, you need to install Vinchin backup proxy as a VM within the VMware ESXi cluster.

Notice
HotAdd only works with SCSI disks but not IDE disks.

NBD

Network Block Device (NBD) is a network protocol allows Vinchin Backup & Recovery to access block devices of the VMs over the network for backup and restore activities.
Currently, NBD transport protocol is supported with Huawei FusionCompute virtual platform.

ImageIO

Vinchin Backup & Recovery use ImageIO API perform full or incremental backups for VM without temporary snapshots. With the implementation of ImageIO API, you can use CBT for incremental backups, and also no backup plugin installation required.
ImageIO API is applicable with the following virtual platforms:

- RedHat Virtualization version ≧ 4.4.7
- oVirt version ≧ 4.4.7
- OLVM ≧ 4.4.8

Backup Proxy

Vinchin backup proxy is an optional backup infrastructure component dedicated for VMware virtual platform, it can utilize the HotAdd technology of the ESXi server for efficient VM backup.
If you are backing up your VMware virtual platform through LAN, and your Vinchin backup server is installed on a physical machine, you can choose to install a Vinchin backup proxy VM on the ESXi cluster for implementation of HotAdd backup.
If your Vinchin backup server is installed as a VM on the ESXi cluster, then Vinchin backup proxy installation is not required, because the backup proxy functionality is already built-in on the Vinchin backup server VM.

Transmission Network

Transmission network is set for eliminate the impact on business-critical services while in backup. If you have a separated network (e.g., storage network) for VM backup, please specify the network address in the **Transmission Network** field in “network/prefix_length” format, e.g., 172.16.0.0/16.
Backup over a transmission network is applicable with the following virtual platforms:

- VMware vSphere
- Citrix Hypervisor (XenServer)
- Red Hat Virtualization (RHV)
- oVirt
- Oracle Linux Virtualization Manager (OLVM)
- Sangfor HCI
- ZStack Cloud
- H3C CAS/UIS

Incremental Mode

Changed Block Tracking (CBT)

CBT (Changed Block Tracking) is an incremental backup technology built-in in the virtual platforms for a quicker VM incremental backup process and smaller size of backup data. As a result, it can reduce the amount of time incremental backup takes, and reduces the storage space by saving the new and changed data only.
Vinchin Backup & Recovery now had implemented CBT support for:

- VMware vSphere
- Citrix Hypervisor (XenServer 7.3 and higher)
- XCP-ng
- RHV (4.4.7 or newer)
- oVirt (4.4.7 or newer)
- OLVM (4.4.8 or newer)
- Huawei FusionCompute (KVM)

SpeedKit

SpeedKit is a unique feature introduced by Vinchin for high-efficiency VM incremental backups. It is an alternative incremental backup technology to those hypervisors do not have CBT implementations yet. Currently SpeedKit can be used for incremental backups of the following virtual platforms:

- Citrix XenServer (version below 7.3)
- Red Hat Virtualization (version below 4.4.7)
- oVirt (version below 4.4.7)
- Oracle Linux Virtualization Manager (version below 4.4.8)
- OpenStack
- Sangfor HCI
- Proxmox VE

When SpeedKit is applied to an incremental backup job, there will be a snapshot kept in the datastore for each of the VMs included in the backup job. This is for rapid calculation of the data changes of the VM disks.

Ordinary

Ordinary incremental mode can be used when the virtual platform does not have CBT implementation or users do not want to use SpeedKit as the incremental mode. Ordinary incremental mode will take longer time to calculate the increments of the VM data than CBT and SpeedKit.

Change Incremental Mode

Incremental mode of an existing VM backup job can be changed if required. To change the incremental mode, simply stop and edit the job. In step 3 of the job editing wizard, click on the **Advanced Strategy** tab, in the **Incremental Mode** dropdown list, please select another incremental mode then save the modification.

Changing of the incremental mode will result in the next incremental backup downgrade to full backup. If changing from **SpeedKit** to **CBT** or **Ordinary** mode, the reserved VM snapshot will be cleared on the next run of the job.

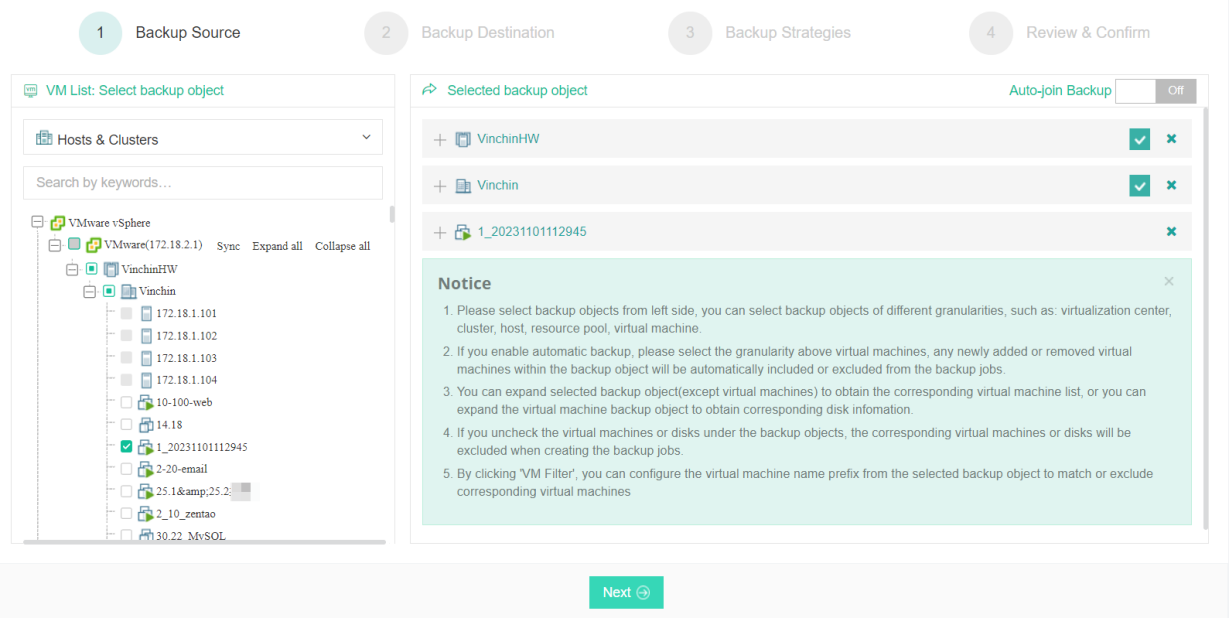
Create VM Backup Job

To create a VMware vSphere backup job, you can get started from the **VM Backup** > **Virtual Machines** page by selecting target VM(s) and then click on **Create new job**, or you can get started from **VM Backup** > **Backup** page.
The New Backup Job wizard for VMware vSphere opens. Please complete the wizard as instructed in the sections below:

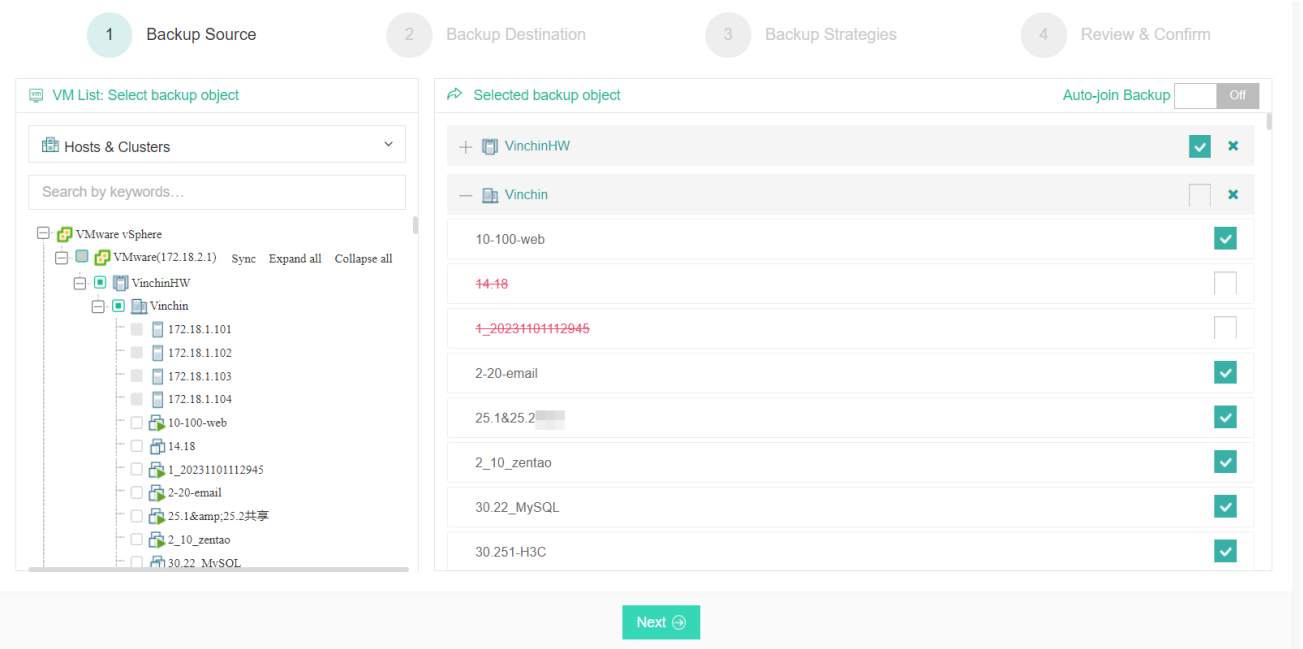
Step 1. Select VMs to Backup
Step 2. Select Backup Destination
Step 3. Configure Backup Strategies
Step 4. Review and Confirm Job Settings

Step 1. Select VMs to Backup

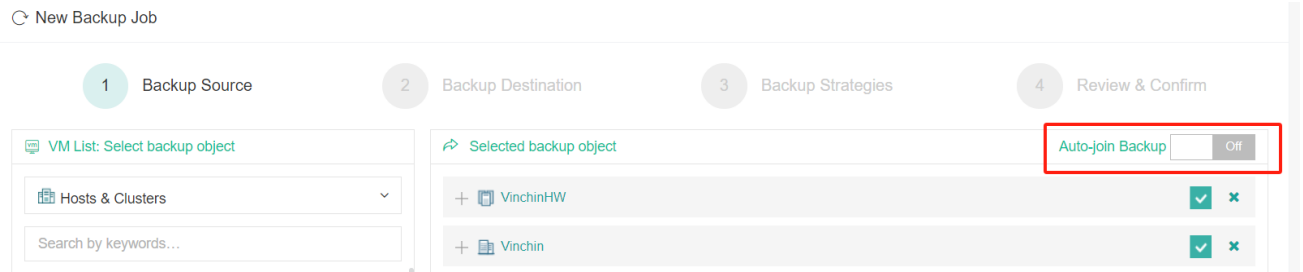
To get started on creating a VM backup job, you can either do it from **VM Backup** > **Virtual Machines** page or from the **VM Backup** > **Backup** page.
On the **VM Backup** > **Virtual Machines** page, you can view all the VMs from all virtual platforms which you've connected to Vinchin backup server. And you can choose to add VM(s) to existing backup job or create a new backup job from here.
By clicking on **Options** of a specific VM and choose **Add to existing job**, or by selecting multiple VMs and click on **Add to existing job** button on the top of the VM list, you can directly add a single VM or multiple VMs to an existing VM backup job.
By clicking on **Options** of a specific VM and choose **Create new job**, or by selecting multiple VMs and click on **Create new job** button on the top of the VM list, you will start a wizard of creating a new VM backup job.
Besides selecting VMs from the **VM Backup** > **Virtual Machines** page to start creating a new VM backup job, you can also do it on **VM Backup** > **Backup** page.
Please follow the below steps to create a new VM backup job.
Select backup objects of different granularities, it can be virtualization center, cluster, host, resource pool, virtual machine. The selected backup object(s) will be listed in the Selected backup object column.



By default, all virtual machines of the selected backup object will be all backed up, if you wish to exclude certain virtual machines of certain object from backing up, please click on the object to expand it in the Selected backup object list, the virtual machines of the object will be shown. By either selecting the virtual machine or not, you can choose to whether to back up the virtual machine or not.

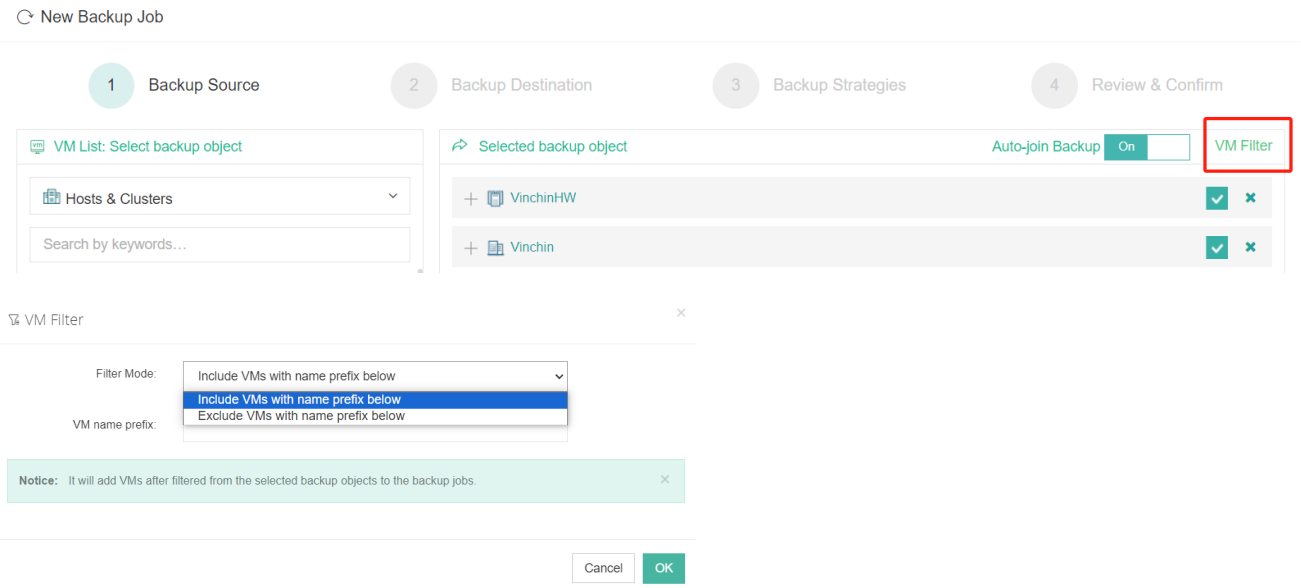


If you enable **Auto-join backup**, please select the granularity above virtual machines, any newly added or removed virtual machines within the backup object will be automatically included or excluded from the backup jobs.



If there's VM not showing in the selected backup object column, please click on **Sync** button to update and sync the VM list to Vinchin backup server.

By clicking '**VM Filter**', you can configure the virtual machine name prefix from the selected backup object to match or exclude the corresponding VMs. There are two filter modes: **Include VMs with name prefix below** and **Exclude VMs with name prefix below.**



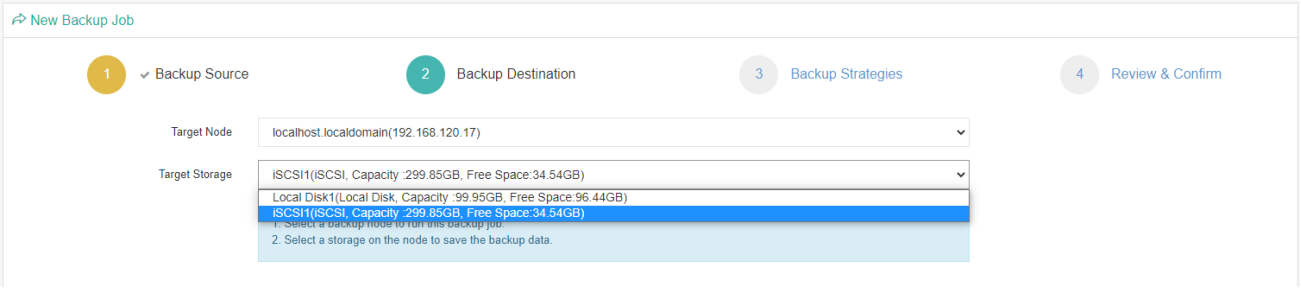
After adding the target VM(s), please click on **Next** button to continue.

Note

You can only add VMs from the same virtual platform into a same job, if you have multiple virtual platforms, please create new jobs for the virtual platforms separately.

Step 2. Select Backup Destination

A backup destination (backup storage) should be associated with this backup job.



In the **Target Node** dropdown list, you can select a backup node on which you want the backup data to be processed and stored.

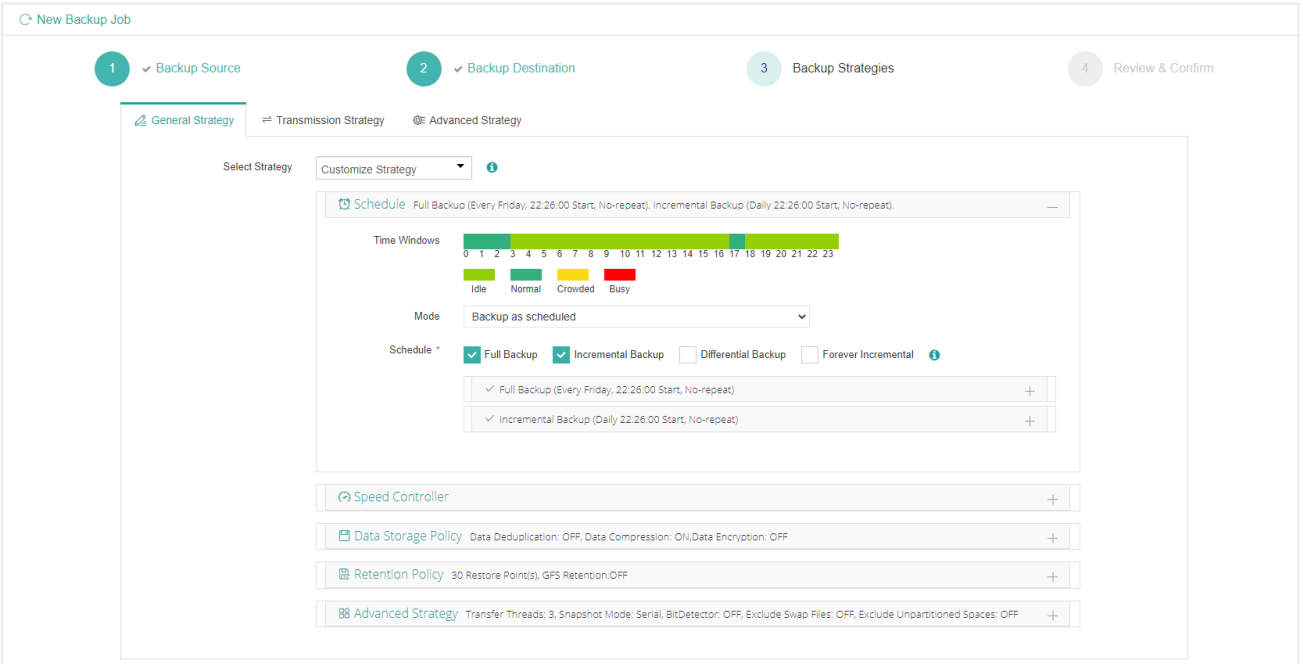
In the **Target Storage** dropdown list, the storages which belong to the selected backup node can be selected.

When done selecting the backup storage, please click on **Next** button to continue.

Step 3. Configure Backup Strategies

General Strategy

Under the **General Strategy** tab, you can setup the backup Time Schedule, Speed Controller, Data Storage Policy, Retention Policy and some other advanced options.



In the **Select Strategy** dropdown list, you can select a preconfigured strategy template, if you had created strategy templates, otherwise choose **Customize Strategy**. For how to create strategy templates, please refer to Strategy Templates.

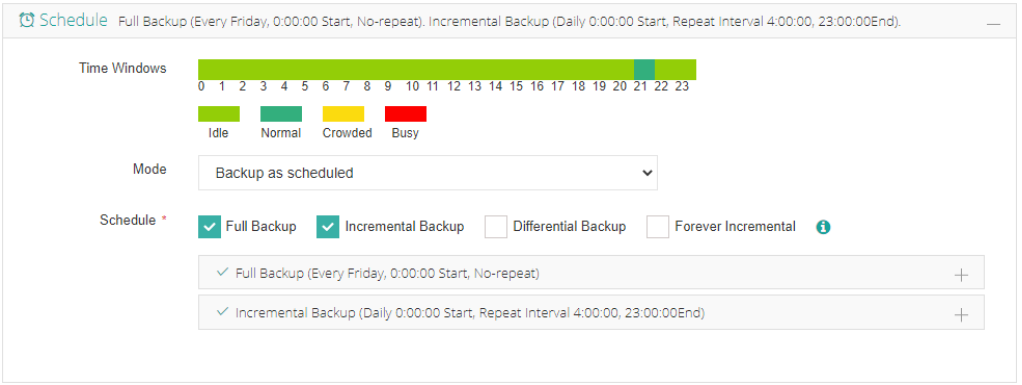
To determine the backup window of this job, the **Time Windows** indicator can be a reference for you to determine in which time window the job should be scheduled.

In the **Time Schedule** field, you can configure the time schedule of the backup job, you can configure the job as a **Backup as Scheduled** job or a **Once-off Backup** job.

For a once-off backup job, the job will only run for once, and only full backup will be performed. You only have to appoint a time of when to start the backup job in the **Start Time** field.

For a scheduled backup job, you can schedule full backup only, full with incremental combination, full with differential combination and forever incremental backup methods.

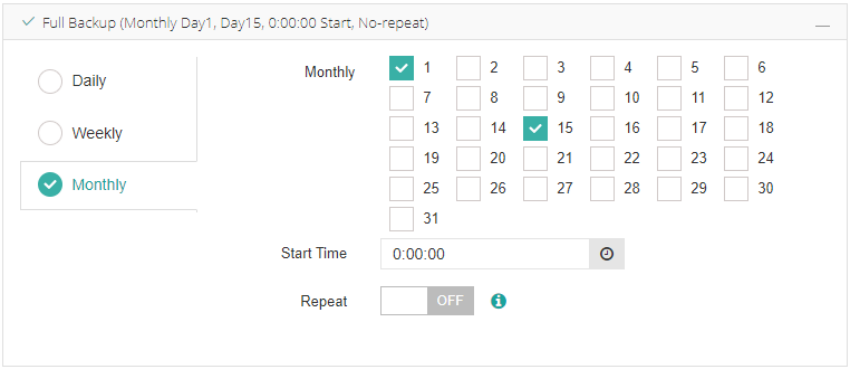
Here we take full with incremental as an example.



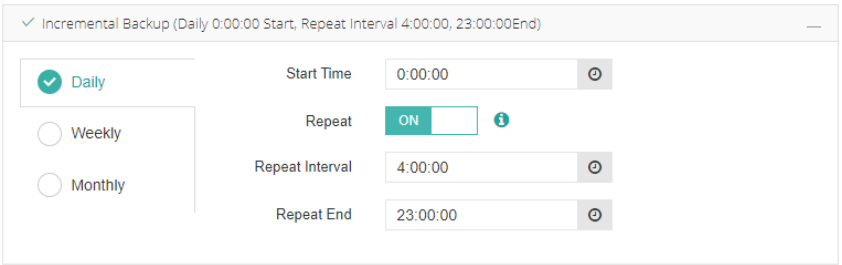
Vinchin backup server will suggest a time to start the backup job, please change the start time if needed. When the start time of a full backup is overlapped with an incremental backup, full backup will be taken at first priority, and the incremental backup will be taken on the next scheduled start time.

If you want to customize the schedules according to your requirements, you can click on the + icon to expand and customize the settings for either full backups or incremental backups.

For example, you can schedule full backups twice a month without repeating.

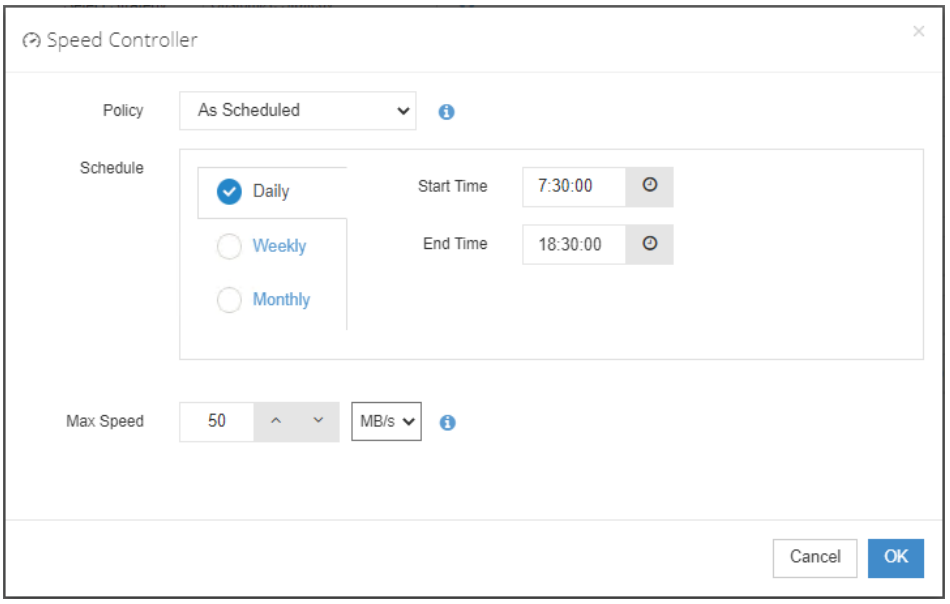


Then configure several incremental backups each day, by default incremental backup will run only for once each day, to run incremental backups several times a day, you can enable the **Repeat** option.



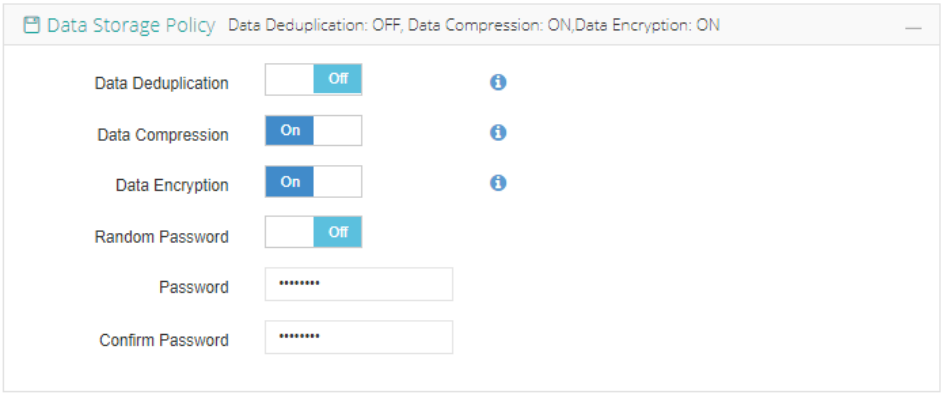
In the above example, full backups will run on day 1 and day 15 of each month, incremental backups will start to run at 0:00 every day and repeat every 4 hours till 23:00 of the day. This is just an example, you should configure the schedules per your requirements based on your actual virtual environments.

After configuring the time schedules of the backups, next you can configure the **Speed Controller**, the speed controller settings are optional, only if the backup jobs will bring network or I/O overload to your production environment, you can configure the speed controller accordingly.



The speed controller policy can be configured as **Permanent** or **As Scheduled**.

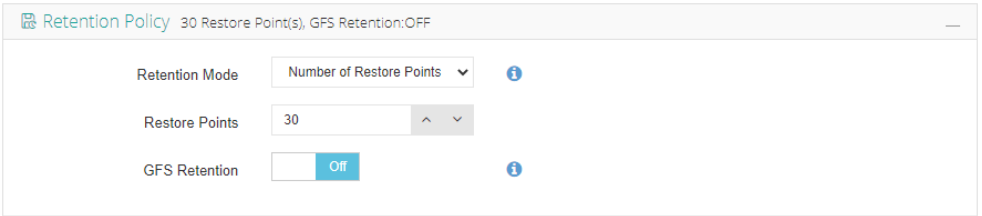
Data Storage Policy including **Deduplication**, **Compression** and **Encryption** of the backup data.



By enabling **Data Deduplication** and **Data Compression**, you can save the bandwidth and storage resources for transmitting and storing the backup data.

By enabling **Data Encryption**, the backup data will be encrypted and then stored into the backup storage. A password needs to be specified to secure the data encryption, when creating a VM restore job, password verification is required to perform VM restore.

Retention Policy can be used to define how much/long the backup data to be reserved in the backup storage, you can either define the retention policy with **Number of Restore Points** or **Number of Days** mode. Additionally, you can activate the advanced **GFS Retention** for your VM backups to apply long-term retention policy of some specific full restore points.



If you choose the retention policy as number of restore points, Vinchin Backup Server will save the specified number of restore points (for each VM included in the backup job), if you choose number of days, Vinchin Backup Server will

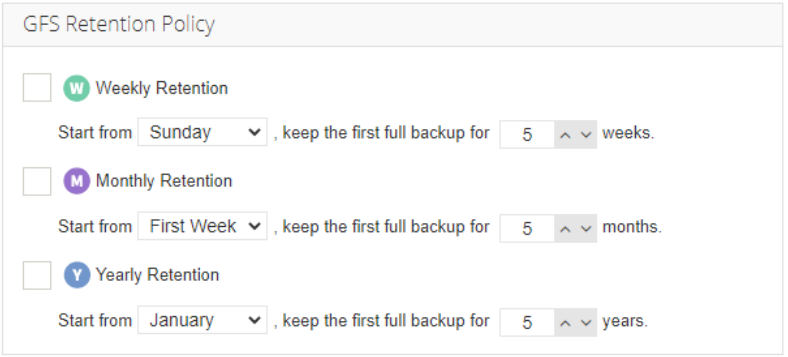
save the restore points within the specified number of days (for each VM included in the backup job), the older restore points will be deleted or merged to comply with the retention policy.

For the backup jobs with full backup schedules only, Vinchin Backup server will delete the older backup restore points directly to comply with the retention policy.

For the incremental backup jobs, to comply with the retention policy, Vinchin backup server will merge the first full backup with the following incremental backup restore points to comply with the retention policy. If it's a forever incremental backup job, Vinchin backup server will always merge backup restore points. If there are full backups to be taken regularly, then the first full backup will be merged with the incremental backup restore points between the first and the second full backup restore points one by one, when there's no incremental backup between the first and the second full backup, the first full backup restore point will be deleted at the next run of the job.

For differential backup jobs, Vinchin backup server will delete the first differential backup restore point to comply with the retention policy, if all differential backup restore points between the first and the second full backup restore points had been deleted, the first full backup restore point will be deleted at the next run of the job.

If you wish to apply long-term data retention with GFS, please switch the **GFS Retention** option on and then configure the **Weekly Retention**, **Monthly Retention** and **Yearly Retention** policies accordingly.



For **Weekly Retention**, please select a day of the week from which the full restore point will be generated and specify how many weeks you wish the weekly full backup to be reserved.

For example, if **Sunday** is selected, Vinchin backup server will tag the full restore point of each Sunday with a "**W**" tag. If there's no full restore point generated on Sunday, it will start waiting and tagging the first coming full restore point of the week. The tagged full restore point will be kept for the specified number of weeks.

To be able to turn on weekly GFS retention, you should at least configure the full backup schedules to run on weekly basis.

For **Monthly Retention**, please select the first or the last week of the month from which the full restore point is coming from and specify how many months you wish the monthly full backup to be reserved.

For example, if **First Week** is selected, Vinchin backup server will tag the first coming full restore point from the first week of each month with a "**M**" tag. The tagged full restore point will be kept for the specified number of months.

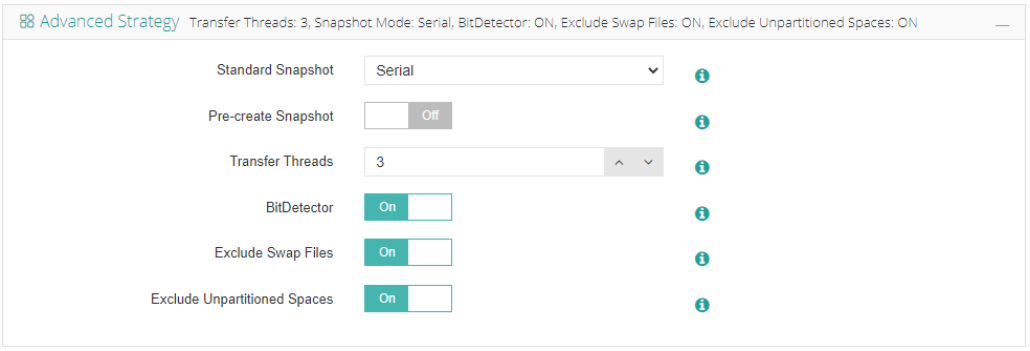
To be able to turn on monthly GFS retention, you should at least configure the full backup schedules to run on weekly basis.

For **Yearly Retention**, please select a month of the year from which the full restore point is coming from and specify how many years you wish the yearly full backup to be reserved.

For example, if **January** is selected, Vinchin backup server will tag the first coming full restore point from each January with a "**Y**" tag. The tagged full restore point will be kept for the specified number of years.

To be able to turn on yearly GFS retention, you should at least configure the full backup schedules to run on monthly basis.

Advanced Strategy contains some advanced options for the VM backup job.



Standard Snapshot can be configured if the backup job includes multiple VMs, and it can be configured as **Serial** or **Parallel**. If serial, the snapshots will be taken one by one. If parallel, the snapshot requests will be simultaneously sent to the virtual platform. It's not recommended to set parallel snapshot, as it may cause the production environment overload.

Pre-create Snapshot can be enabled to create the next VM's disk snapshot while the previous VM is being transferred to the backup storage.

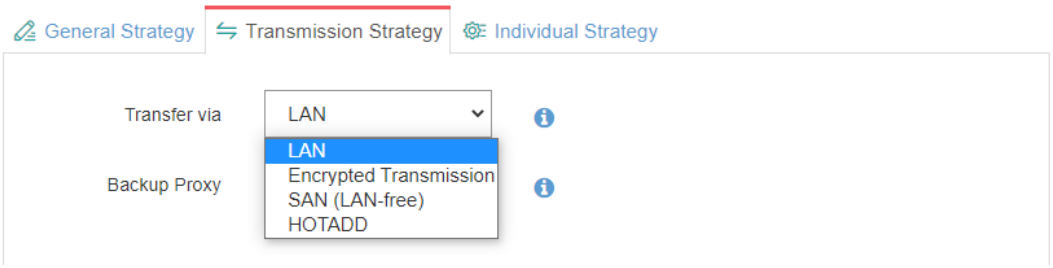
By specifying the number of **Transfer Threads**, you can enable multithreaded transmission to improve the processing speed of the backup job. The default value for multithreaded transmission is 3, even if you can set the value from 1 to 8, but usually 3 threads will be enough.

BitDetector can be enabled to exclude the swap partitions and the unpartitioned spaces from the backup job.

Transmission Strategy

VMware vSphere

For VMware vSphere, the backup data can be transferred through LAN, Encrypted Transmission, SAN (LAN-free) or HOTADD. For more information of the data transmission methods, please refer to Data Transmission.



When you choose to transfer via **LAN** or **LAN (Encrypted Transmission)**, **Backup Proxy** can be used, as the backup proxy is installed on ESXi server you can utilize the HotAdd technology of the ESXi server for direct VMDK access.

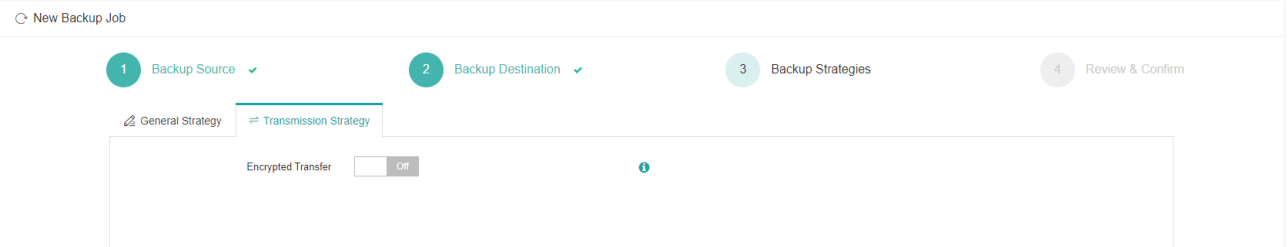
SAN (LAN-free) can be used to transfer the backup data from the storage area network. LAN-Free path needs to be configured, please refer to LAN-Free.

HOTADD can be used only if Vinchin Backup Server is installed on the ESXi server as a virtual machine.

Hyper-V

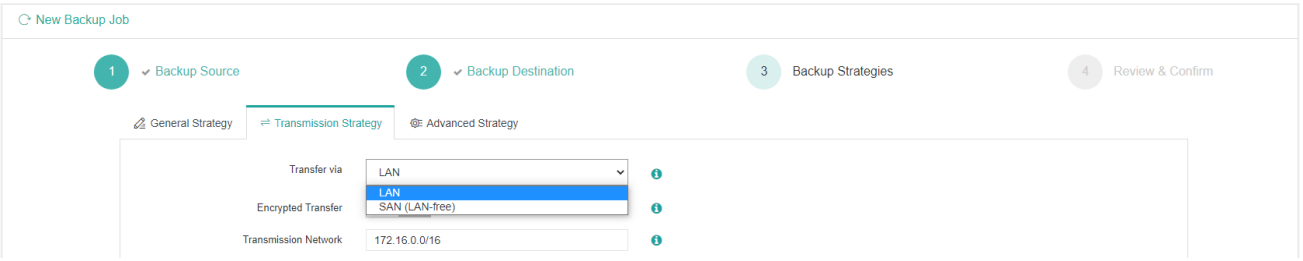
Currently the transmission of Hyper-V VM data can be only done through LAN.

For the data safety during backup process, users can enable **Encrypted Transfer** option.



Citrix Hypervisor (XenServer)

For Citrix Hypervisor (XenServer) the backup data can be transferred through LAN or through SAN (storage area network).



If you choose to do the backups over **LAN**, the backup data will be transferred via the production network. But if you have a separated network for VM backup, please specify the network address in the **Transmission Network** in "network/prefix_length" format, e.g., 172.16.0.0/16. And you can choose to either encrypt the transmission or not by turning **Encrypted Transfer** option on or off.

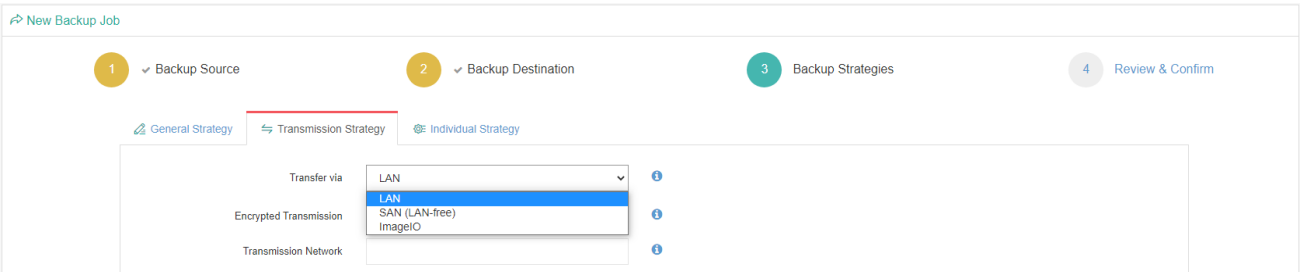
SAN (LAN-free) can be used to transfer the backup data from the storage area network. LAN-Free path needs to be configured in advance, please refer to LAN-free.

XCP-ng

The transmission strategies of XCP-ng are the same as Citrix Hypervisor (XenServer).

oVirt

For oVirt the backup data can be transferred through LAN, SAN (storage area network) or through LAN by using ImageIO API.



If you choose to do the backups over **LAN**, the backup data will be transferred via the production network. It requires a backup plugin installed on the oVirt compute nodes, if you haven't done this, please refer to Install oVirt Backup Plugin for more information.

SAN (LAN-free) can be used to transfer the backup data from the storage area network without the need to install a backup plugin. LAN-free path needs to be configured in advance, please refer to LAN-free.

ImageIO is supported with oVirt version 4.4.7 and above. If your oVirt version is (or above) 4.4.7 it's recommended

to use ImageIO, it does not require backup plugin installation and can support CBT as incremental backup mode. For more information, please refer to ImageIO.

If you have a separated LAN for VM backup, please specify the network address in the **Transmission Network** in "network/prefix_length" format, e.g., 172.16.0.0/16. And you can choose to either encrypt the transmission or not by turning **Encrypted Transmission** option on or off.

Red Hat Virtualization (RHV)

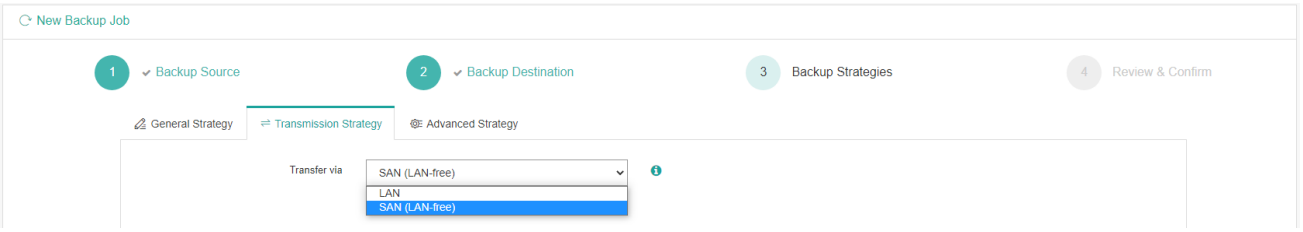
The transmission strategies for RHV are the same as oVirt.

Oracle Linux Virtualization Manager (OLVM)

The transmission strategies for OLVM are the same as oVirt.

OpenStack

For OpenStack, the backup data can be transferred through LAN or SAN.

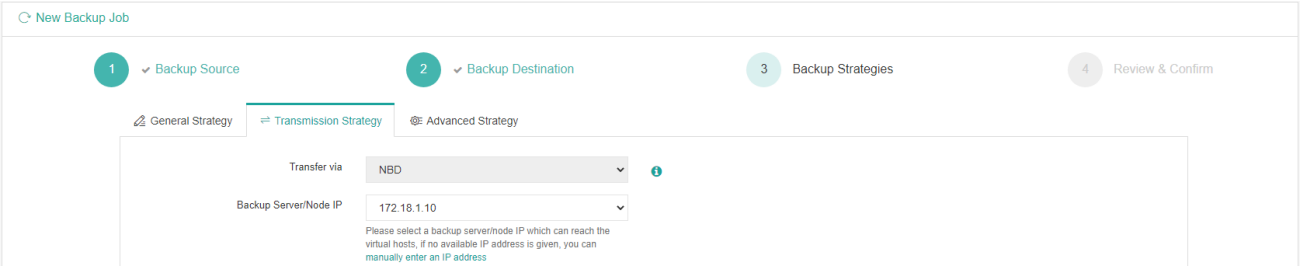


If running the backups through LAN, backup plugin must be installed on the controller and compute nodes.

If running the backups through LAN-free mode, your backend storage should be FC or Ceph. For FC SAN, LAN-free path needs to be configured in advance, please refer to LAN-free. For Ceph, Lan-free path configuration is not required, but users should configure Vinchin backup server being able to communicate with the Ceph storage network, pleases contact Vinchin support team for help on this specific configuration.

Huawei FusionCompute

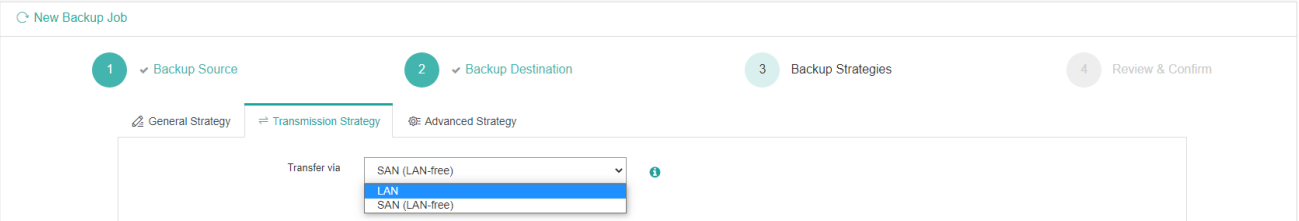
By default, the VM data will be transferred using NBD protocol through the LAN.



For **Backup Server/Node IP** option, if the backup server or node has multiple network connections, you can choose an IP address to establish the NBD connection for backup.

ZStack Cloud

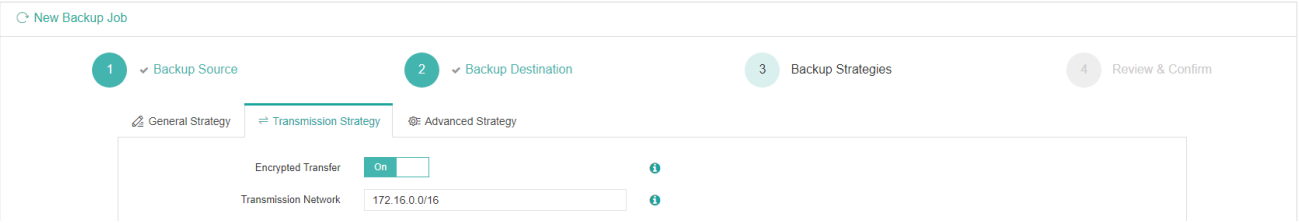
For ZStack Cloud, backup data can be transferred through LAN or SAN.



SAN (LAN-free) backup is only applicable when the backend storage of ZStack is Ceph, otherwise please select LAN.

H3C CAS/UIS

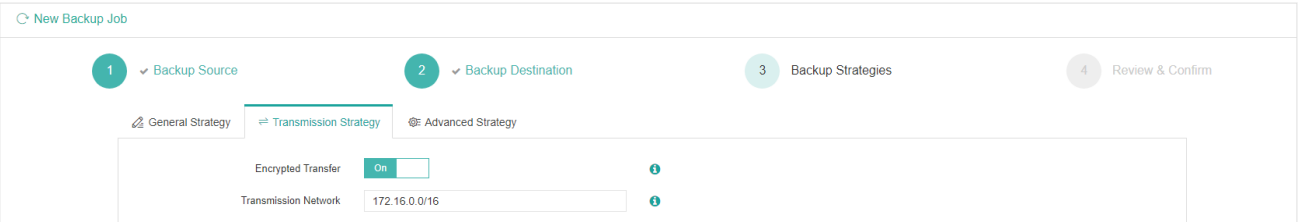
For H3C UIS/CAS, the backup data transmission goes through LAN by default, you can choose to either encrypt the backup data or not by turning the **Encrypted Transmission** on or off.



If you have a separated network for VM backup, please specify the network address in the **Transmission Network** field in “network/prefix_length” format, e.g., 172.16.0.0/16.

Sangfor HCI

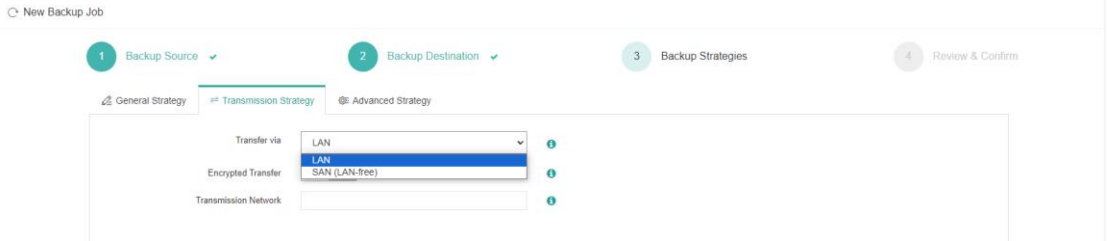
For Sangfor HCI, the backup data transmission goes through LAN by default, you can choose to either encrypt the backup data or not by turning the **Encrypted Transfer** on or off.



If you have a separated network for VM backup, please specify the network address in the **Transmission Network** field in “network/prefix_length” format, e.g., 172.16.0.0/16.

Proxmox VE

For Proxmox VE the backup data can be transferred through LAN or through SAN (storage area network).



If you choose to do the backups over **LAN**, the backup data will be transferred via the production network. But if you have a separated network for VM backup, please specify the network address in the **Transmission Network** in “network/prefix_length” format, e.g., 172.16.0.0/16. And you can choose to either encrypt the transmission or not

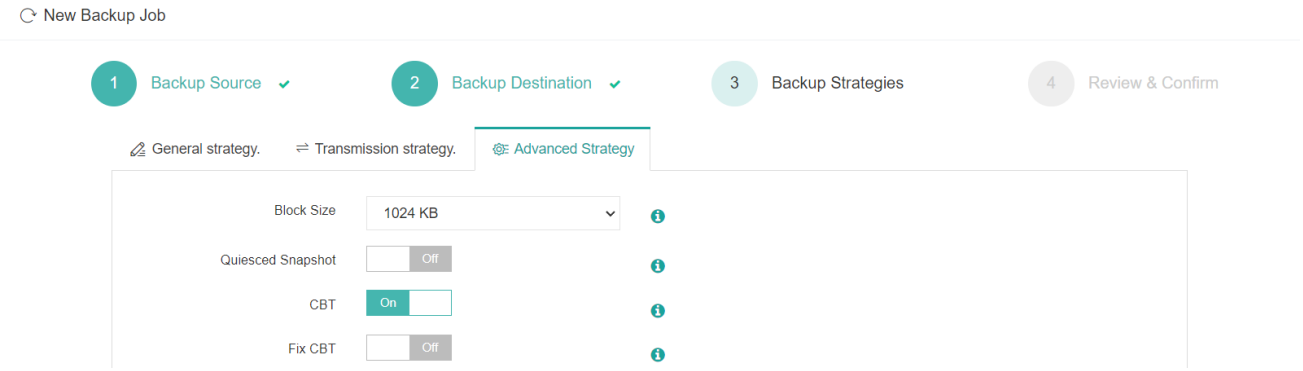
by turning **Encrypted Transfer** option on or off.

SAN (**LAN-free**) backup is only applicable when the backend storage of Proxmox VE are NFS, GlusterFS, LVM-Thin with iSCSI, LVM-Thin with FC, Ceph RBD, otherwise please select LAN.

Advanced Strategy

VMware vSphere

The advanced strategy settings for VMware vSphere are optional.



Block Size can be defined only for VMware vSphere virtual platform. When running the backup jobs, Vinchin Backup Server will perform deduplication and compression to the backup data per the defined block size.

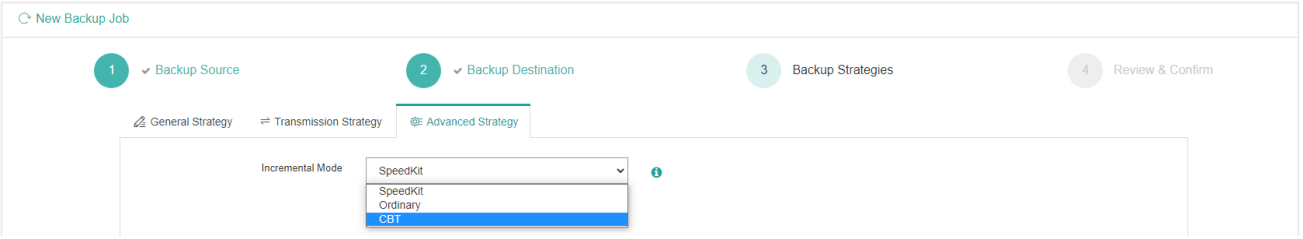
Quiesced Snapshot is configurable with VMware vSphere, when taking snapshot of the VMs to be backed up, if the VMs have VMware Tools installed, VMware Tools will process the VMs into a state suitable for backing up.

CBT (Changed Block Tracking) is a more advanced way to perform incremental backups than using SpeedKit or Ordinary mode. By default, CBT is enabled for VMware backup jobs. For more information about the incremental mode please refer to Incremental Mode.

Fix CBT can be enabled to fix CBT function if it is abnormal.

Citrix Hypervisor (XenServer)

The advanced strategy settings of Citrix Hypervisor (XenServer) are the incremental mode options.



If your Citrix is licensed as Premium Edition and the version is (or above) 7.3, **CBT** is the recommended incremental mode.

If your Citrix is licensed as Standard Edition and version below 7.3, **SpeedKit** is the recommended incremental mode. Otherwise choose **Ordinary** as the incremental mode.

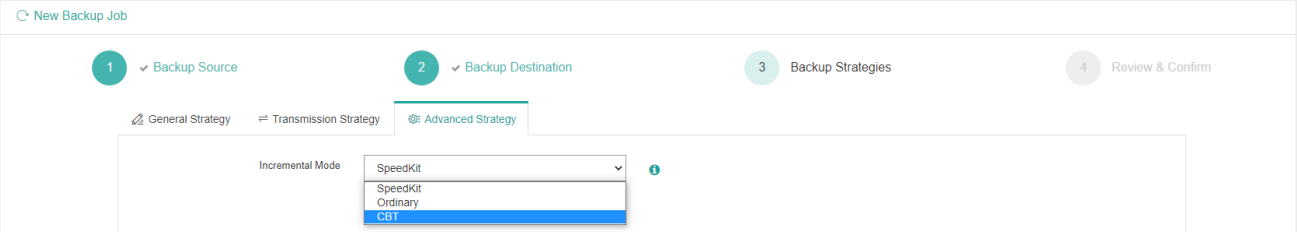
For more information of the incremental mode, please refer to Incremental Mode.

XCP-ng

The advanced strategies of XCP-ng are the same as Citrix Hypervisor (XenServer). But it's always recommended to use **CBT** as the incremental backup mode.

oVirt

The incremental mode options for backing up oVirt VMs can be configured under the advanced strategy settings.



If the backup data is configured to be transferred through LAN or SAN under the transmission strategy settings, the incremental mode is configurable between SpeedKit and Ordinary. If transferring through **ImageIO**, the incremental mode must be **CBT**, and vice versa.
For more information of the incremental modes, please refer to Incremental Mode.

Red Hat Virtualization (RHV)

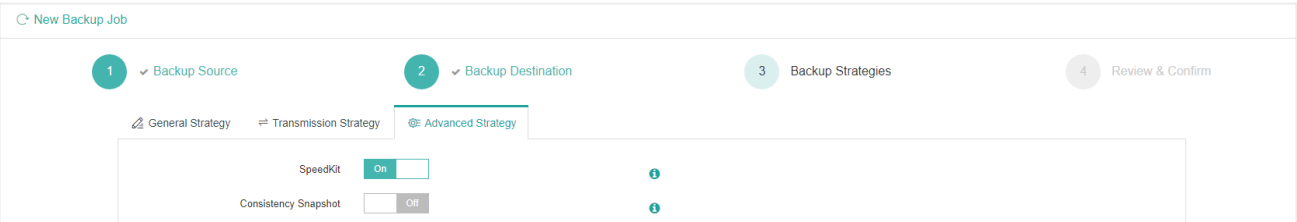
The advanced strategies for RHV are the same as oVirt.

Oracle Linux Virtualization Manager (OLVM)

The advanced strategies for OLVM are the same as oVirt.

OpenStack

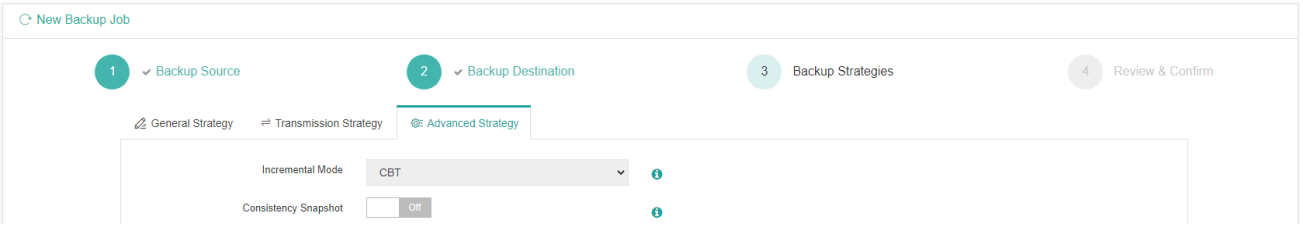
The advanced strategy settings for OpenStack VM backup including, **SpeedKit** and **Consistency Snapshot**.



SpeedKit is the default incremental mode for backing up OpenStack VMs, if disabled, Vinchin Backup & Recovery will perform VM backup in Ordinary incremental mode, the incremental backups will be slower.
For the **Consistency Snapshot** option, it guarantees the snapshots of all virtual disks of a VM to be taken at the same time.

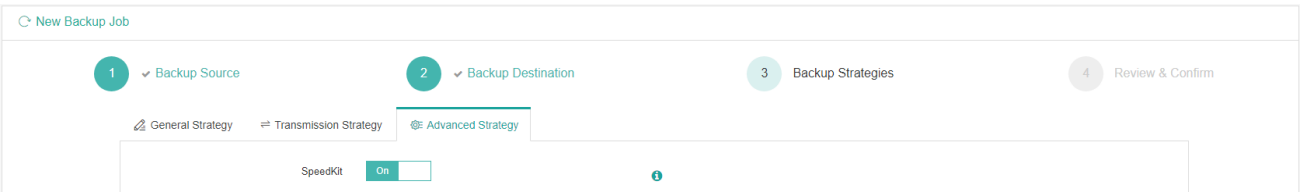
Huawei FusionCompute

The default **Incremental Mode** for backing up Huawei FusionCompute VMs is **CBT**. Besides, **Fix CBT** can be enabled to fix CBT function if it is abnormal.
Consistency Snapshot is used to ensure the VM data consistency when creating Huawei FusionCompute VM snapshots.



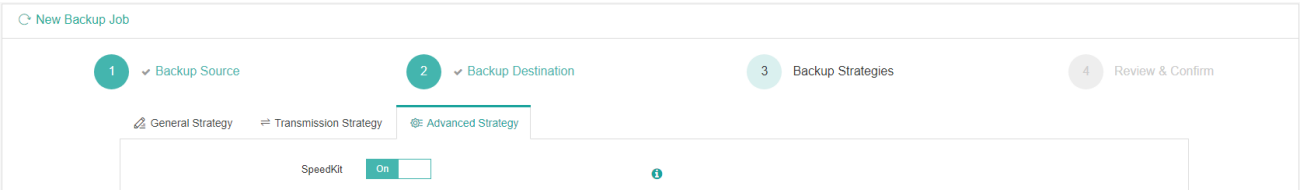
ZStack Cloud

The default incremental mode of backing up ZStack Cloud VMs is **SpeedKit**, it is recommended to keep it enabled for faster incremental backups, if turning it off, the next incremental backup will downgrade to full backup.



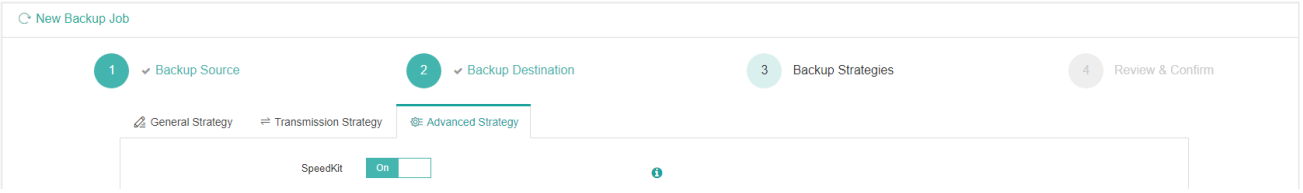
H3C CAS/UIS

The default incremental mode of backing up H3C CAS/UIS VMs is **SpeedKit**, it is recommended to keep it enabled for faster incremental backups, if turning it off, the next incremental backup will downgrade to full backup.



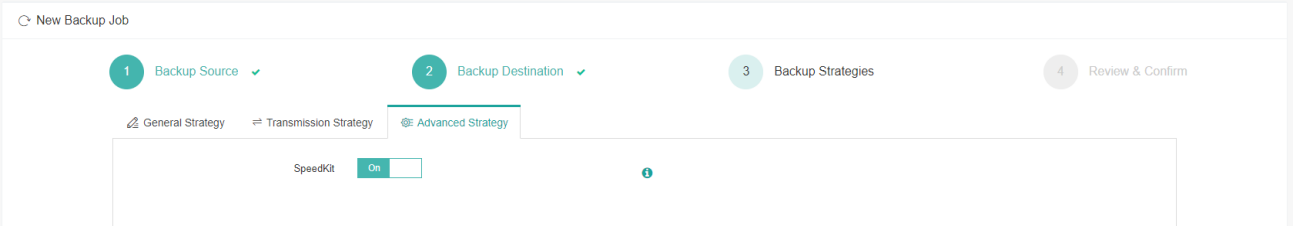
Sangfor HCI

The default incremental mode of backing up Sangfor HCI VMs is **SpeedKit**, it is recommended to keep it enabled for faster incremental backups, if turning it off, the next incremental backup will downgrade to full backup.



Proxmox VE

The default incremental mode of backing up Proxmox VE VMs is SpeedKit. It is recommended to keep it enabled for faster incremental backups. If you turn it off, the next incremental backup will be downgraded to full backup.

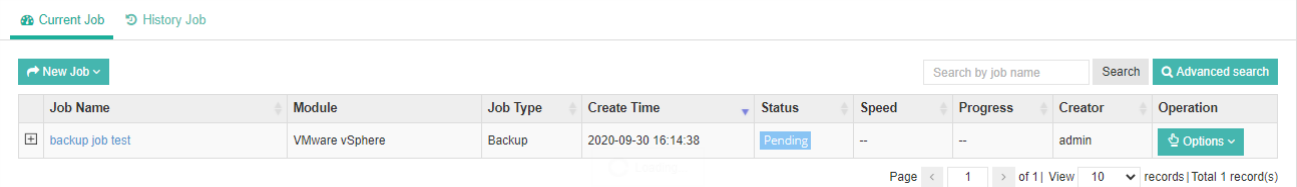


Step 4. Review and Confirm Job Settings

After completing the above-mentioned settings, you can review and confirm the settings in one screen.
A job name can be specified for identification of the VM backup jobs, and by clicking on the **Submit** button to confirm the settings and create the backup job.

VM Backup Job Management

After creating a new backup job, you can find it on the **Monitor Center** > **Jobs** page, under the **Current Job** tab.



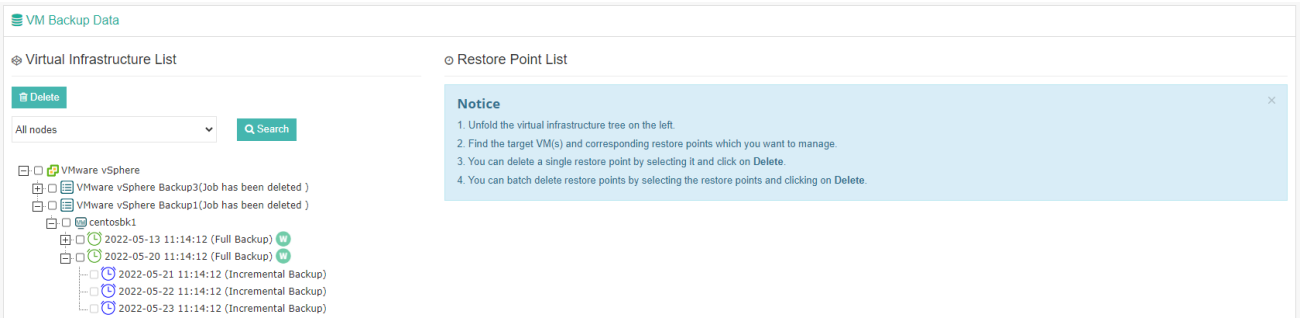
The status of the newly created job will usually be **Pending**, when the time condition matches the schedule, it will automatically run. And the status will change to Running, you can also see the transfer speed and job progress here within the job list. By clicking on the job name, you can check more detailed information on the **Job Detail** page.
For a scheduled backup job, after running one of the schedules, the status will change to Pending again and then wait for the next run.
For a once-off backup job, after running the job for once, it will be removed from the Current Job list. And you can find it from the History Job list.
For more information, please check the instructions on Monitor Center section.

VM Backup Data Management

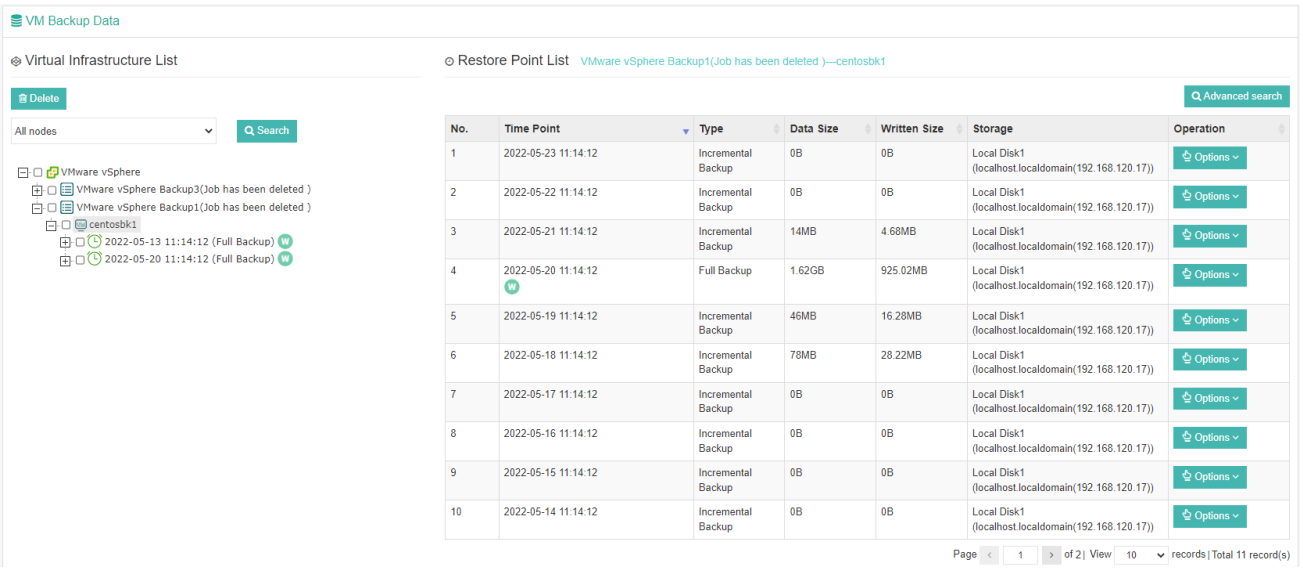
After running each VM backup job session, the VM backup data can be found and managed from **VM Backup** > **Backup Data** page.

View Backup Data

By default, all VM backups of all backup nodes from Vinchin backup infrastructure will be displayed, if you wish to view backups of a specific backup node, please select a node from the dropdown list.
The VM backup data is organized with a Virtual Platform -> Backup Job -> Virtual Machine -> Restore Point structure as shown below.



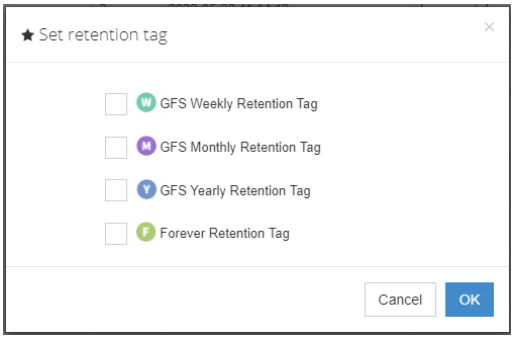
Each restore point is named with the timestamp of its creation and will be marked with its backup type. To view more information of the restore points, simply click on the VM name, all the restore points of the selected VM will be listed on the right side with more detailed information.



You can get more information like the actual data size, written size and the storage which is used to store the restore point data.
To search specific restore point(s), you can use the **Search** button on the left or use the **Advanced search** button top right of the **Restore Point List**.

Retention Tags

The purpose of using the retention tags is to avoid the short-term retention policy from purging some specific backups and keep them for a longer time period. There are 4 types of retention tags in Vinchin Backup & Recovery.
W: the weekly GFS retention tag (applicable for full backups).
M: the monthly GFS retention tag (applicable for full backups).
Y: the yearly GFS retention tag (applicable for full backups).
F: the forever retention tag (applicable for all types of backups).
The **W**, **M** and **Y** GFS retention tags can be either pre-configured in a VM backup job by enabling GFS retention to tag specific restore points automatically or can be manually set. While the **F** tag can only be manually set.
To manually set retention tags, please go to **VM Backup** > **Backup Data** page. By selecting a VM from a backup job, all the restore points will be listed on the right, find the restore point which you wish to set/unset retention tags and click **Options** button, and then select **Set Retention Tag**.



In the popup dialog you can set/unset retention tags for the selected restore point. GFS retention tags are only applicable for full restore points, forever retention tag is applicable for all types of restore points.
If GFS retention had been enabled in the backup job, the manually tagged restore points' retention time complies with the GFS retention time configured in the backup job. When the GFS retention tag exceeded the retention time defined in the VM backup job, the oldest tag will be removed and the corresponding restore point will be purged by the general retention policy.
If GFS retention is not enabled in the backup job, the manually tagged restore points will be reserved forever. As for the forever retention tag, once it has been set, the tagged restore point will be reserved forever.
For GFS retention tag, there can be only one full restore point tagged as weekly full backup of each week (same for the monthly and yearly retention tag). If there's already a full restore point had been tagged for the week, there will not be the second one to be tagged and it will fail to manually set the second GFS tag for the week (same for the monthly and yearly retention tag).
Forever retention tag works independently with the GFS retention tags, a restore can be tagged with GFS retention and forever retention tag at the same time, when the GFS retention tag expires, the forever retention tag will still remain and the restore point will be retained forever.

Delete Backup Data

We recommend configuring comprehensive retention policies for the VM backup jobs to automatically purge the out-of-date backups instead of manual deletion of the backup data. It is a highly risk operation by deleting the backup data manually. If you have to do this, please follow the below instructions.
To delete VM backup data, please go to **VM Backup** > **Backup Data** page. There are two approaches to perform the deletion, batch (or single) deletion of restore points from the left side tree view and single restore point deletion from the right side restore point list view.

Deleting restore point(s) from the tree view.
Please unfold the virtual infrastructure and the associated backup job, and unfold the VM which you wish to delete backup data from. Then select the restore point(s) you wish to be deleted and click on the **Delete** button on the top left of the tree view. You'll have to provide you password to confirm the deletion of selected restore point(s).
If it's a standalone full restore point, no incremental or differential restore points dependent on it, you can select and delete the standalone full restore point directly.
If it's a backup chain, formed by a full restore point and a series of incremental (or differential) restore points dependent on the full restore point, you can only delete the backup chain from the tree view.

Deleting restore point from the restore point list view.
Please select a VM from the left tree, the associated restore points will be listed on the right-side list view. By clicking on the **Options** button of a specific restore point and selecting **Delete** you are able to delete that single restore point, no matter it's full, incremental or differential.
If it's a standalone full restore point, no incremental restore points or differential restore points dependent on it, you can delete the standalone full restore point directly.
If it's a backup chain formed by a full restore point and a series or incremental restore points dependent on the full restore point, while deleting the incremental restore point in the end of the incremental chain, it will be directly deleted, if you delete any other restore point it will lead to data blocks merging with the next restore point. For example, you got an incremental backup chain, full on Monday, incremental on Tuesday and Wednesday, if you delete the incremental restore point of Tuesday, its data blocks will be merged with Wednesday incremental restore point. This mechanism can guarantee the backup data consistency.
If it's a backup chain formed by a full restore point and a series of differential restore points dependent on the full restore point, while deleting the full restore point is not allowed but you can delete the differential restore points, and there will not be data blocks merging required.

VM Restore

Vinchin Backup & Recovery provides comprehensive VM restore options for customers to recover their data assets or services in varies scenarios, in order to meet their requirements of data safety and business continuity.
The supported VM restore features are as follows.

- Full VM Restore
- Instant VM Restore
- Granular VM Restore
- V2V Migration

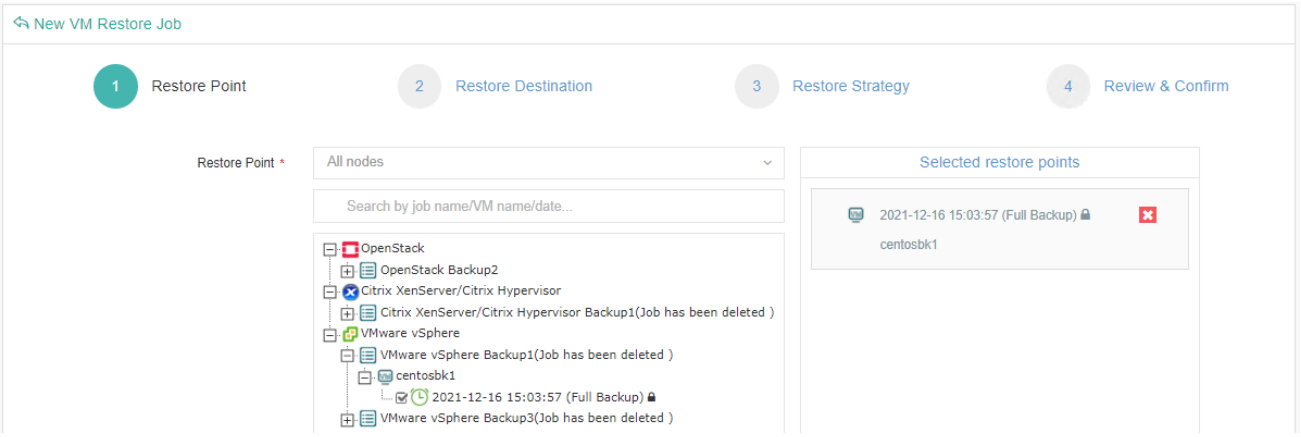
Full VM Restore

Create Full VM Restore Job

To restore a VM or a group of VMs, a restore job needs to be created, go to the **VM Backup** > **Restore** page. Please follow the below steps to create VM restore jobs.

Step 1: Select Restore Point

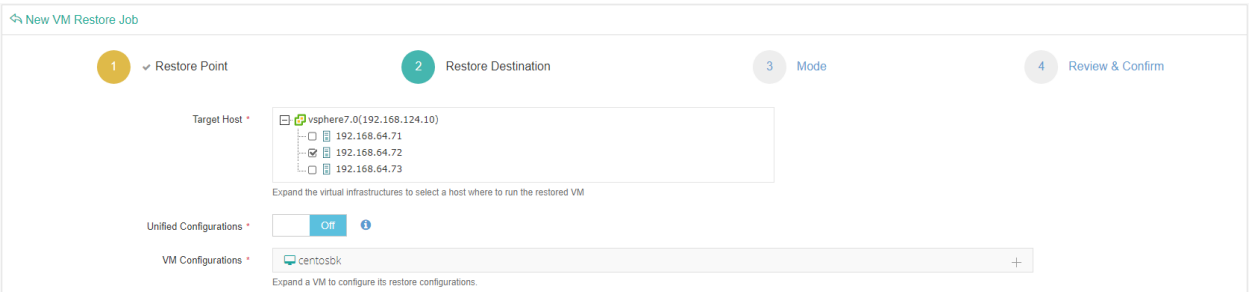
In the Restore Point dropdown list, select a backup node which stores the desired restore points.
Select a target VM restore point under your virtual infrastructure which you want to restore. You can quickly find the target restore point by searching the job name, VM name or the date of the restore point.



You can restore a group of VMs by selecting one of the restore points under each of the VMs. After selecting the desired restore point under virtual machine which you want to recover, click **Next** to continue.

Step 2: Restore Destination

In the Target Host list, select a target host where you want to run the restored VMs.



After restored, the VMs will run on the selected host.

Note

1. For OpenStack virtual platform, please select target project instead.

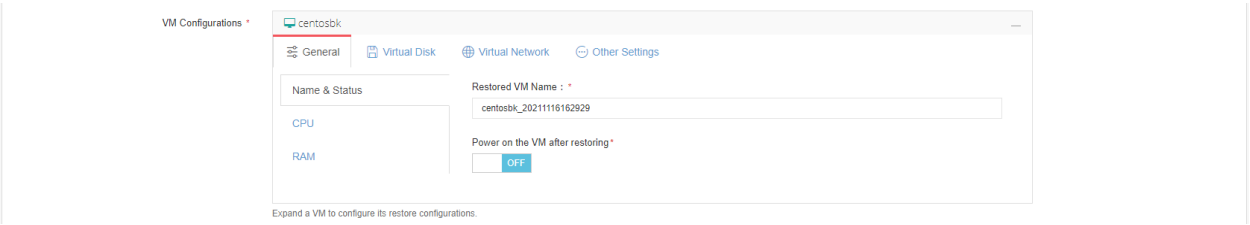
2. If the host is offline, you cannot select it as restore destination.

3. You can restore a VM to an unlicensed host.

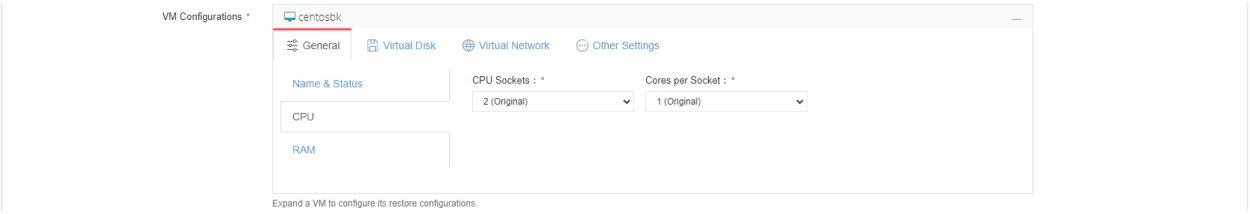
Unified Configurations: If you are restoring a group of VMs, enable this function you can set the storage, network, and choose whether to power on the target VMs after restoring.

VM Configurations: Here you can setup advanced restore options for specific VM(s) by clicking on the VM name, modifying the configurations of one VM will not affect the unified configurations of the other VMs if you had enabled **Unified Configurations** option.

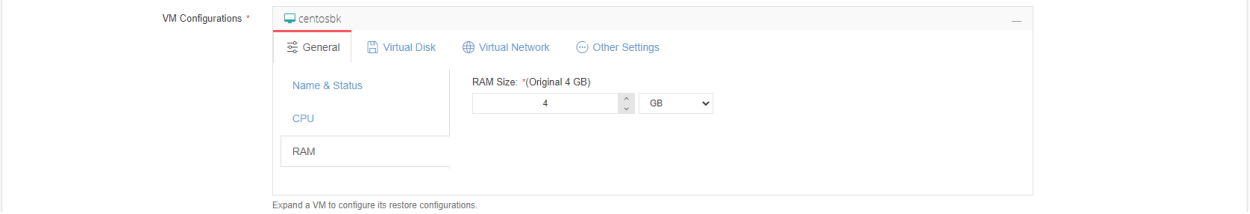
Name & Status: You can set a customized name for the VM to be restored and set its power status after restoring.



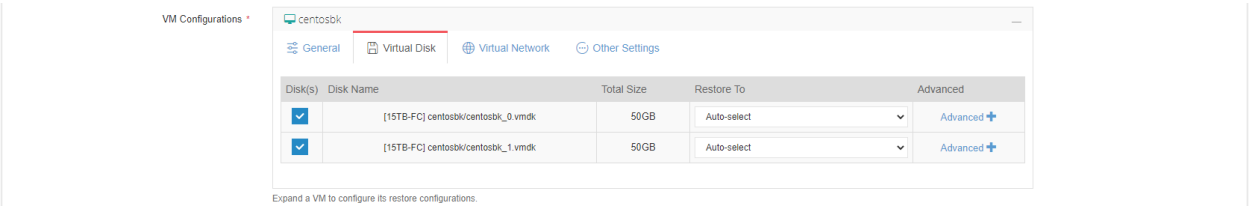
CPU: Here you are allowed to change the number of CPUs or CPU cores for the VM to be restored if necessary.



RAM: Here you are allowed to change the RAM size of the VM to be restored if necessary.



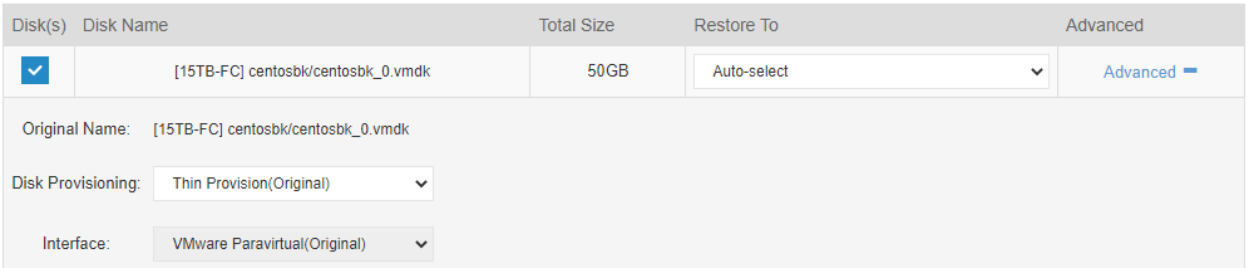
Virtual Disk: Virtual Disk settings are optional, you can proceed with the given default settings.



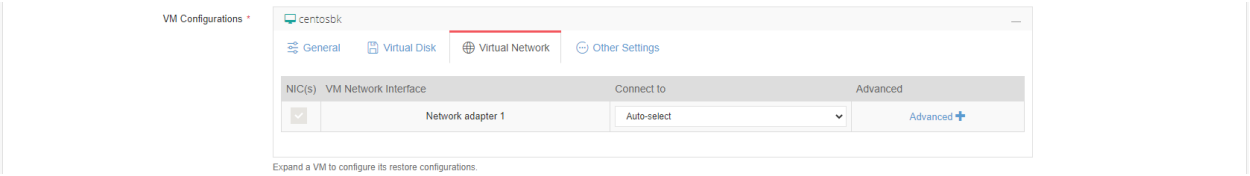
In the **Disk(s)** column, there are checkboxes for the VM virtual disks, when a VM has multiple disks, you can choose to restore specific disk(s) without having to restore all the disks of the VM. But if you don't restore the disk on which the operating system is installed, the restored VM will not be bootable, you need to re-install a new operating system or mount the restored disk to another VM to be able to access this virtual disk.

In **Restore To** column, you can select datastore to which the virtual disk will be restored. By default, Vinchin will automatically select a datastore to restore the VM virtual disk.

By clicking on **Advanced**, you can setup the disk provisioning options. But the virtual disk interface type cannot be configured, it should be kept as original interface type.

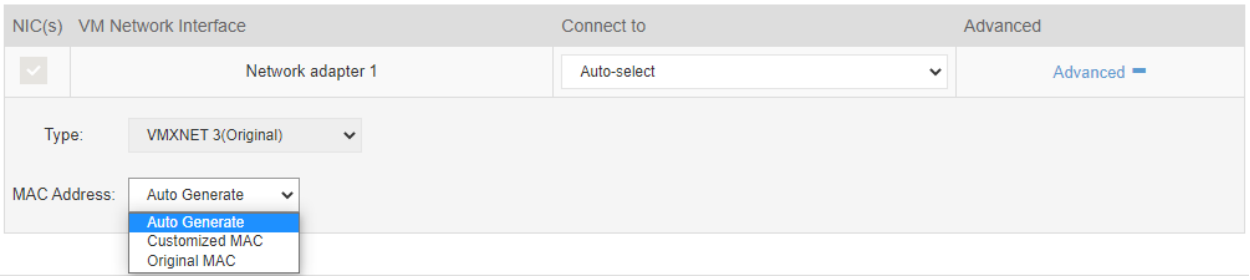


Virtual Network: Virtual Network settings are also optional. It allows you to select the virtual network to be connected to and the MAC address assignment of the restored VM.



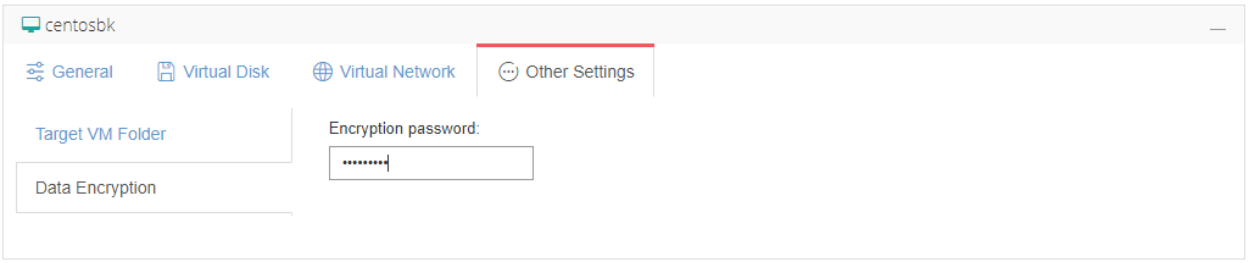
In the **Connect to** column, you can select a desired virtual network for specific virtual network interface of the VM, by default it will automatically select one from the available virtual networks.

By clicking on **Advanced**, you can setup the MAC address assignment for the virtual network interface.



By default, the virtual platform will auto generate a new MAC address for the VM, but you can also use the original MAC address or customize the VM MAC address if you prefer.

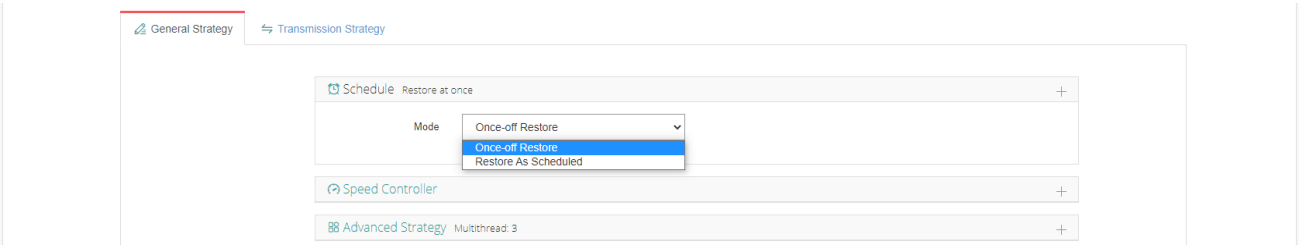
Other Settings: Currently, Other Settings option will not present to all VM restore job settings. This option will present for certain virtualizations for some additional configurations of the VM restore job.



If the VM backup data is encrypted (Data Encryption enabled in backup job), when restoring the VM you need to provide the data encryption password for verification under Other Settings tab, otherwise without the data encryption password, the VM cannot be restored.

Step 3: Restore Strategy

For the job schedule, you can configure the VM restore job as once-off restore or restore as scheduled.



If you choose **Once-off Restore**, the restore job will start running right after the job has been created. If you choose **Restore As Scheduled**, you need to set restore schedules. After this, the job will run as scheduled.

Notice

Only if you need to regularly restore the VM(s) to certain status from backups, you can choose to use Restore As Scheduled option, otherwise please use Once-off Restore.

For **Speed Controller**, it works the same principle as the VM backup jobs.

For **Advanced Strategy**, you can configure multithreading for the VM restore job, and it works the same principle as multithreading for the VM backup jobs.

For **Transmission Strategy**, please refer to Create VM Backup Job.

Step 4: Review & Confirm

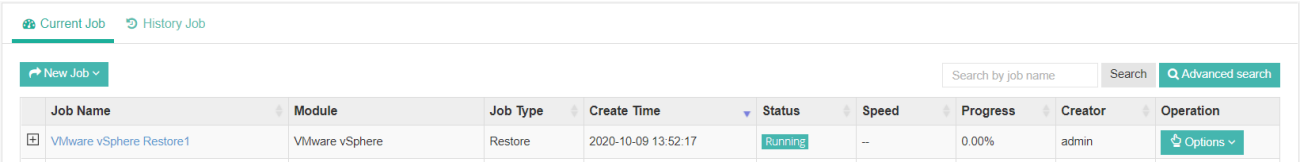
After finishing the above settings, you are able to review and confirm all settings here. Click **Submit** to confirm creating this job.

Notice

If this VM restore job is configured as "Restore now", it will start restoring the VM(s) right after the creation of this job.

Restore Job Operations

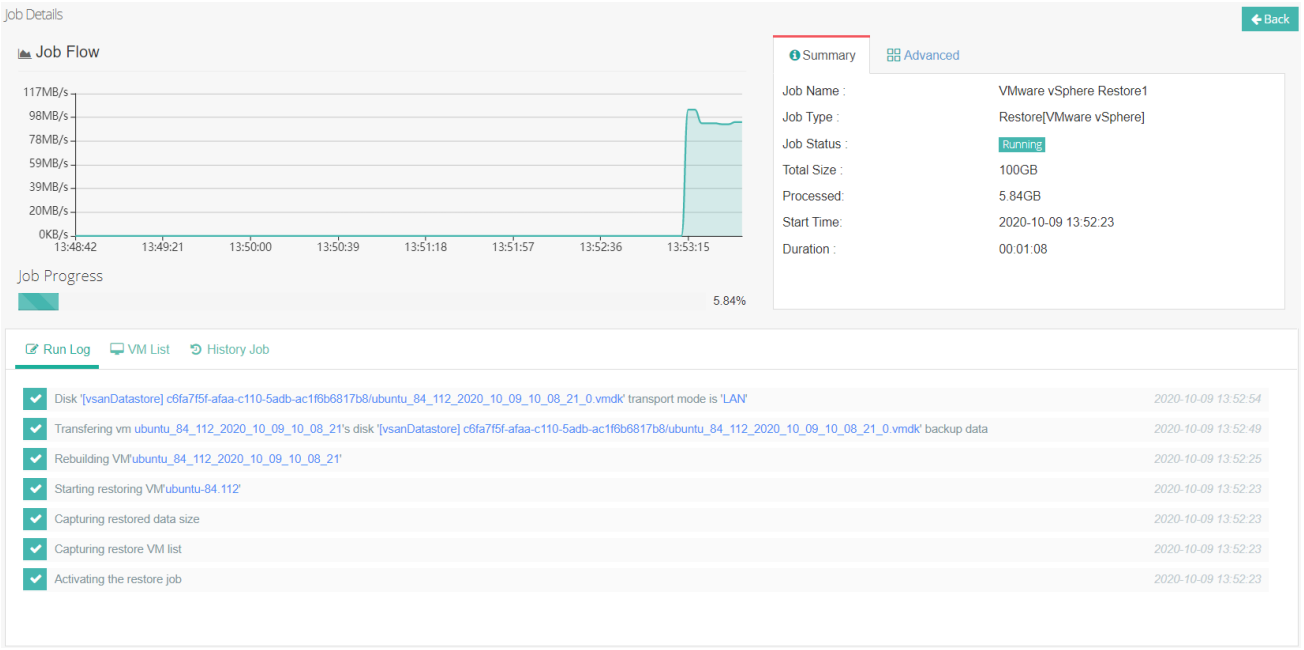
After creating a new restore job, you will be redirected to the **Monitor Center** > **Jobs** page, and you'll be able to see the VM restore job you created in the job list.



If the job is once-off restore, you should see the job in running status, if the job is supposed to "restore as scheduled", then you should see the job in pending status.

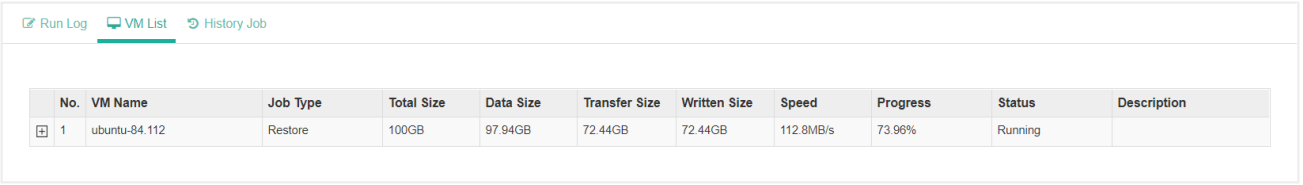
If you want to manually start the job, please click on **Options**, and then select **Start Job** to run it manually.

And by clicking on the job name and you'll be able to view the job details.



Run Log: The logs of the currently running restore job.

VM List: The list of VMs that will be restored by this job.



History Job: for a "Once-off Restore" job, this job will be auto-deleted after restoring completed and there will be no data to be displayed. If you've set "Restore as scheduled", you can review all the history running logs of this restore job.

Warning

During a restore process, do not power on the VM before the restore job is completed, otherwise the VM data will be damaged or lost.

Instant VM Restore

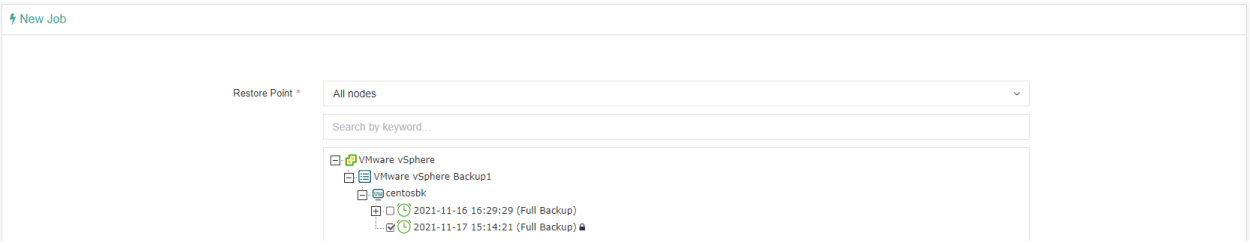
Instant VM Restore can be used in emergency situations to recover a VM within 1 min, minimizes the downtime of critical businesses. It can be very helpful in emergency situations to directly start a VM from its backup data, without the need to transfer backup data back to production storage then resume the VM.

Notice

Instant Restore is currently not supported with Microsoft Hyper-V and OpenStack virtual platforms.

Create Instant VM Restore Job

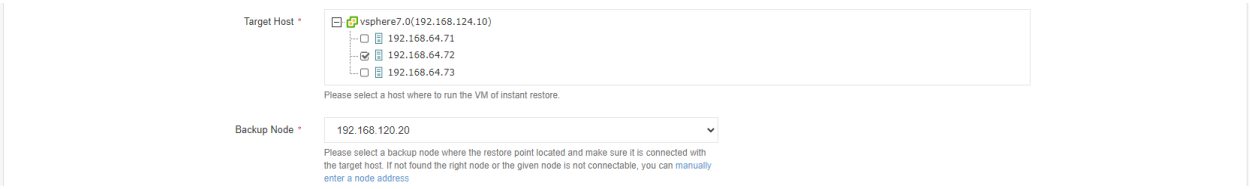
To create an Instant Restore job, please go to **VM Backup** > **Instant Restore** page, select a target VM restore point under your virtual platform which you want to recover to. You can quickly find the target restore point by specifying backup node and selecting Group by VMs or Group by Restore Points accordingly.



Notice

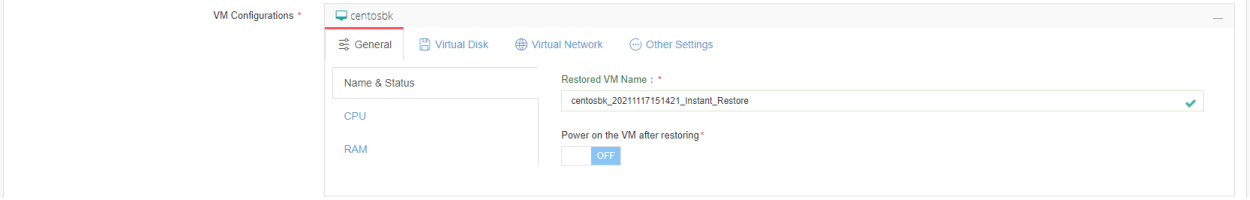
The restore point to be used for instant restore can be a full backup restore point, an incremental restore point or a differential restore point, but you can only select one restore point for each instant restore job.

Select a host as the restore destination where you want to run the instant restore VM, and select the backup node IP/domain where the backup storage is mounted.

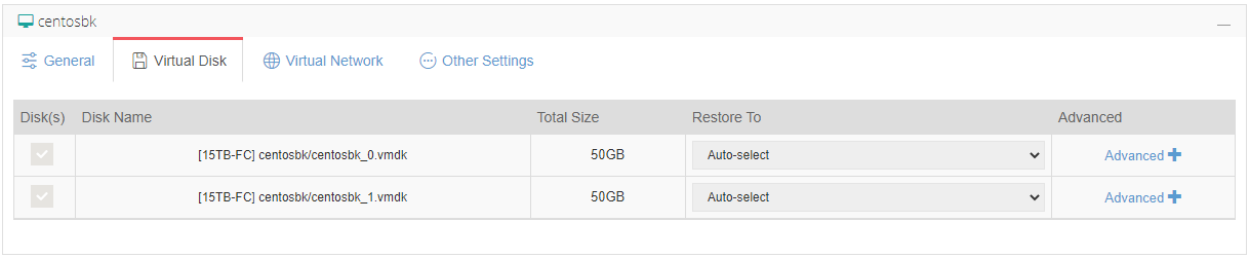


When a host is selected, in the VM configurations section it will show loading state, it will take a few seconds to request for the information of virtual platform resources.

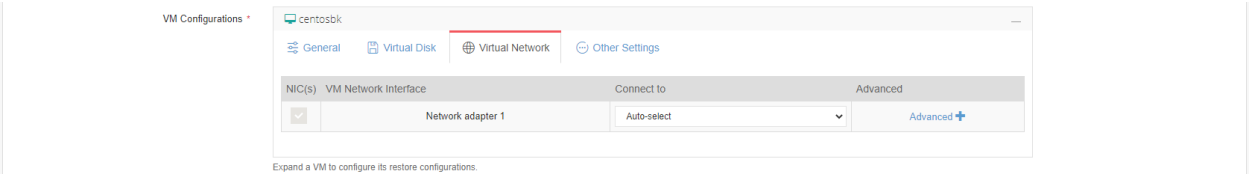
Under **General** tab, you are able to set VM name, power state, CPU and RAM size for the instant restore VM.



Under **Virtual Disk** tab, the virtual disk settings are view-only, because instant restore will use VM backup data to run the VM on virtual platform, no data transmission to virtual platform datastore will be involved at this stage, so virtual disk settings are temporarily not needed.

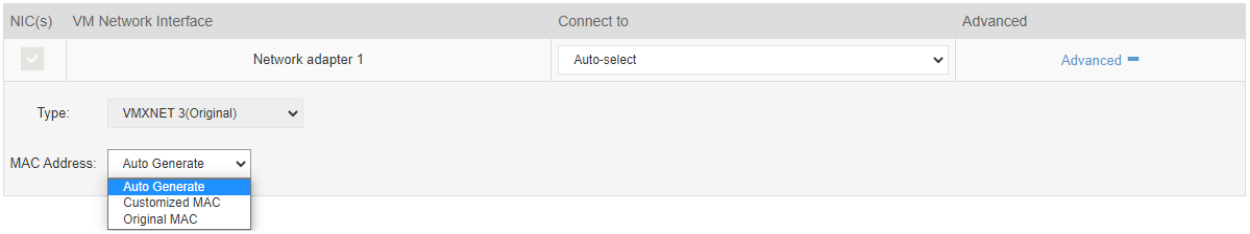


Virtual Network: It allows you to select the virtual network to be connected to and the MAC address assignment of the restored VM.



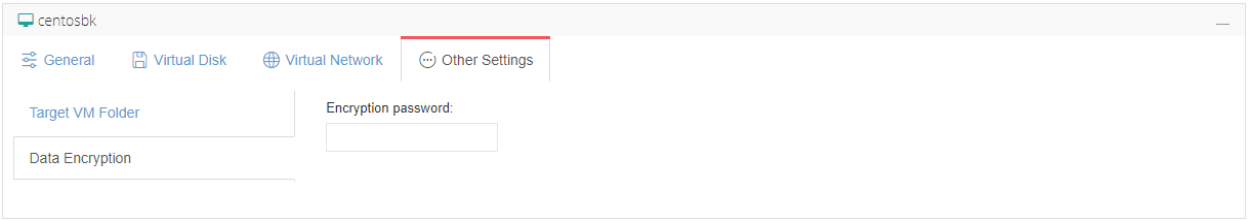
In the **Connect to** column, you can select a desired virtual network for specific virtual network interface of the VM, by default it will automatically select one from the available virtual networks.

By clicking on Advanced, you can setup the MAC address assignment for the virtual network interface.



By default, the virtual platform will auto generate a new MAC address for the VM, but you can also use the original MAC address or customize the VM MAC address if you prefer.

Other Settings: Currently, Other Settings option will not present to all VM restore job settings. This option will present for certain virtualizations for some additional configurations of the VM restore job.

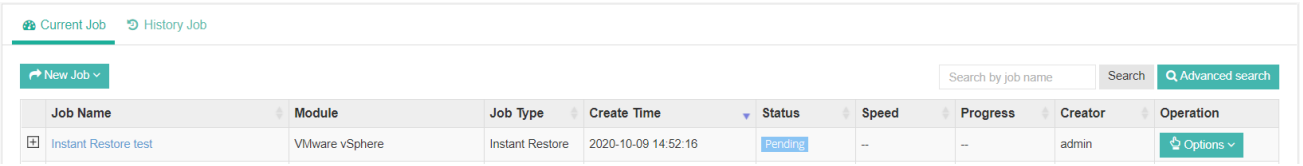


If the VM backup data is encrypted (Data Encryption enabled in backup job), when restoring the VM you need to provide the data encryption password for verification under Other Settings tab, otherwise without the data encryption password, the VM cannot be restored.

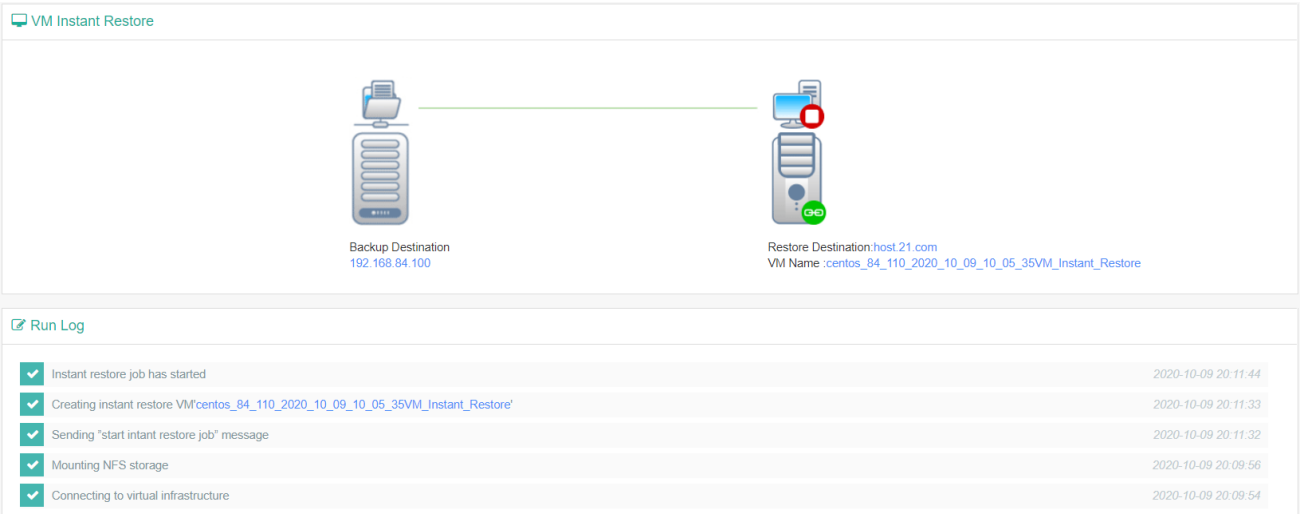
Once done, click on OK button to submit the creation of the instant restore job.

Instant Restore Job Management

After creating a new instant restore job, you will be redirected to the **Monitor Center** > **Jobs** page, and you'll be able to see the instant restore job you created in the job list.



To start the instant restore job, please click on **Options**, and then select **Start Job**. The job status will change to starting, it will take a while for the restore process to be completed, when the job status change to running, then the VM is restored. Now you click on the job name you'll see the instant restore job details.



The logs will display the instant recovery job progress. After the job is completed successfully, you can power on the restored VM from your virtual platform. If you have preset "Power on the VM after restoring", the VM will be powered on automatically.

The instant restore VM runs directly from Vinchin backup server storage, the original backup data will not be modified, the new data will be written into a cache area. It is recommended to perform a VM migration to migrate all VM data (original backup data and cache data) to the production storage of the virtual platform during the non-production hours, please refer to VM Migration to migrate the VM data back to production storage.

If the instant restore is just for verifying the backup data availability, and you want to delete the instant restore job, you can go back to the current job list and click **Options** of the running instant restore job and then select **Stop**, after the job has been stopped, then click **Options** again and select **Delete**.

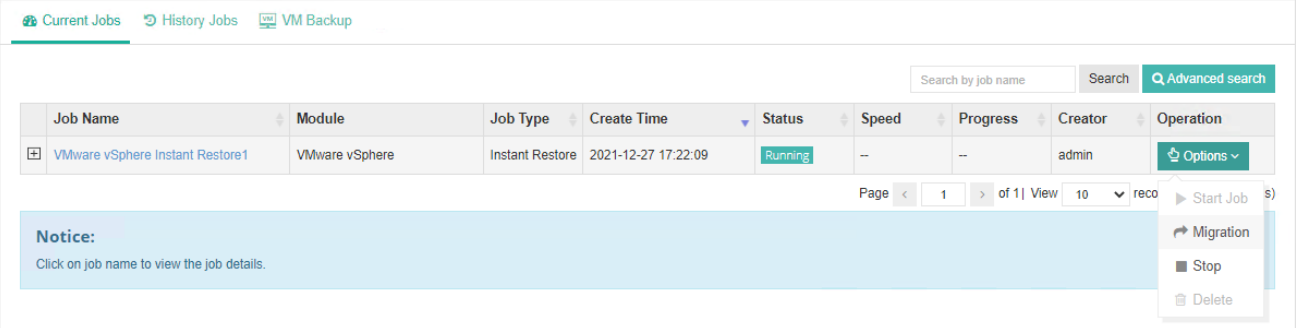
Warning

1. All the data of the instant restored VM is actually on Vinchin Backup Server/Node which is mounted to the selected host as NFS storage, if you delete the instant restore job, all the data of the restored VM will be deleted from the virtual platform host (including newly written data during the instant restore). If you need to reserve the restored VM and its newly written data, do not stop the job until you have migrated all data to the virtual platform host.

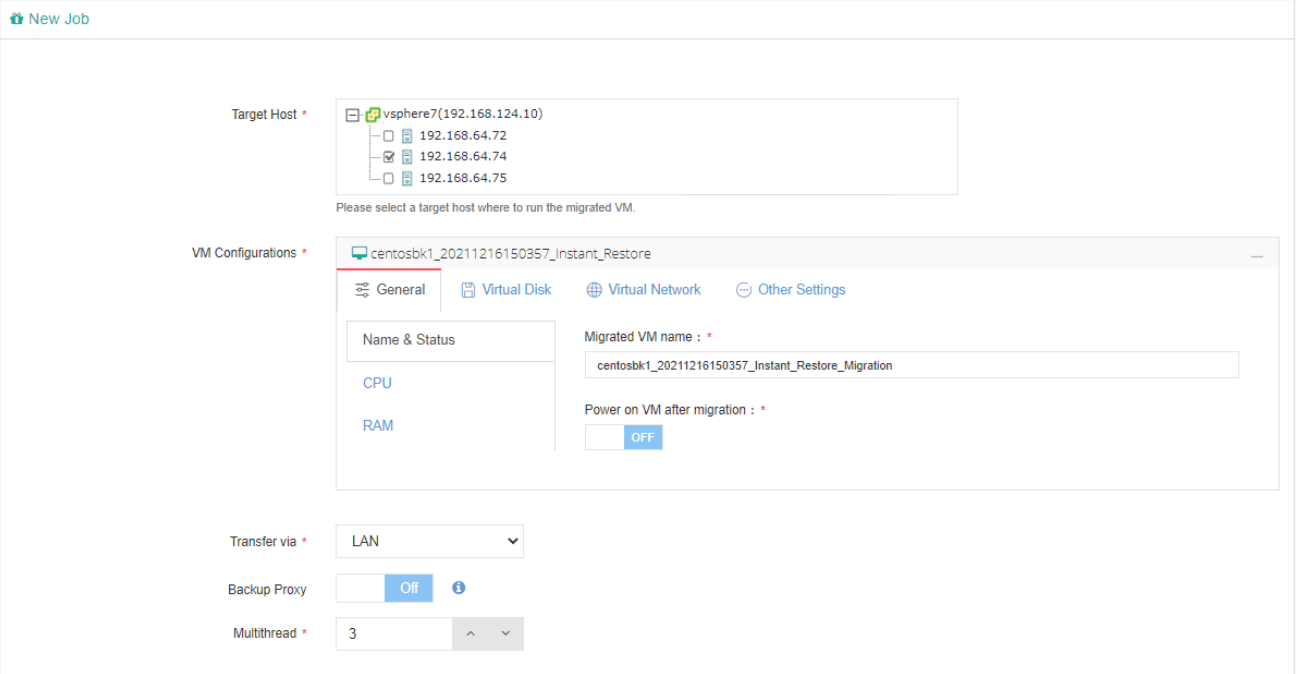
2. Do not create snapshot on the instant restore VM, or change any disk information. Otherwise, error will occur to the instant restore VM or it will crash.

Live Migration

Click on **Options** and then select **Migration** of the instant restore job with which you wish to perform VM migration.



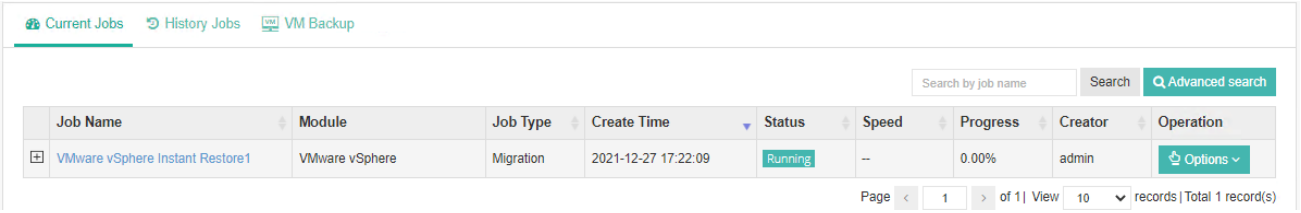
Select a host where to migrate the VM. Then you can rename the migrated VM and choose to whether power on it after migration, set virtual disk configurations, virtual network configurations for the VM. For more details of the VM Configurations please refer to Create VM Restore Job.



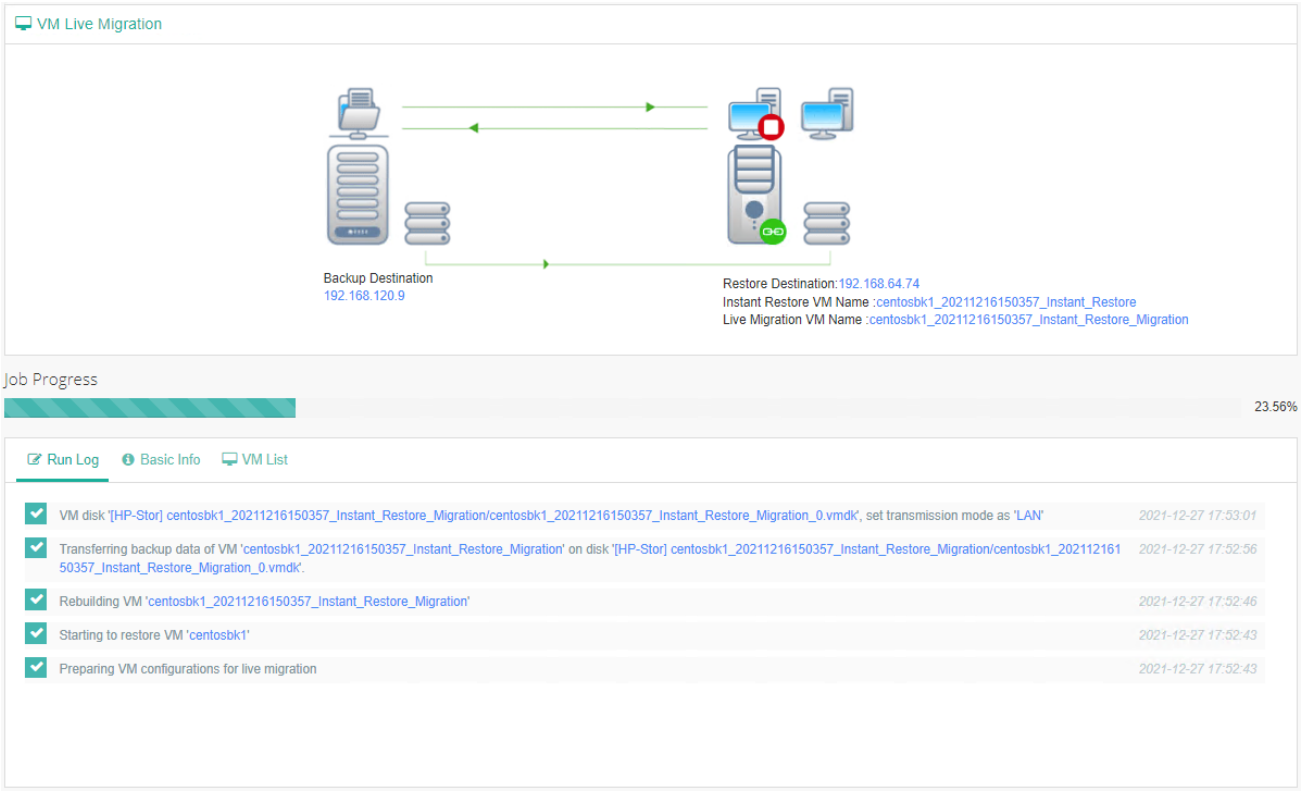
For the password verification, it's not required to perform VM migration, because password verification had already been done during VM instant restore job creation process.

You can also select transmission mode. For a detailed description of each transmission mode, please refer to Create VM Backup Job. And multithreaded transmission for VM migration is also applicable.

Click OK to start the migration job. And in the current job list, the job type will change from **Instant Restore** to **Migration**.



Click on the job name and you'll be able to view the detailed process of the VM migration.



After migration completed, the migration job will automatically change back to instant restore job, and this job is still in a running status. But the VM created by instant restore job will be powered off and the services will be taken over by the migrated VM. There will be around one minute of service down time, when Vinchin Backup Server tries to power off the instant restored VM and power on the migrated VM. If you didn't enable **Power on the VM after restoring** option, then you'll have to manually power it on.

Once VM migration is done, you are able to stop the instant restore job and delete it. All data including the cache data generated during the instant restore VM runtime will be all migrated to the production storage.

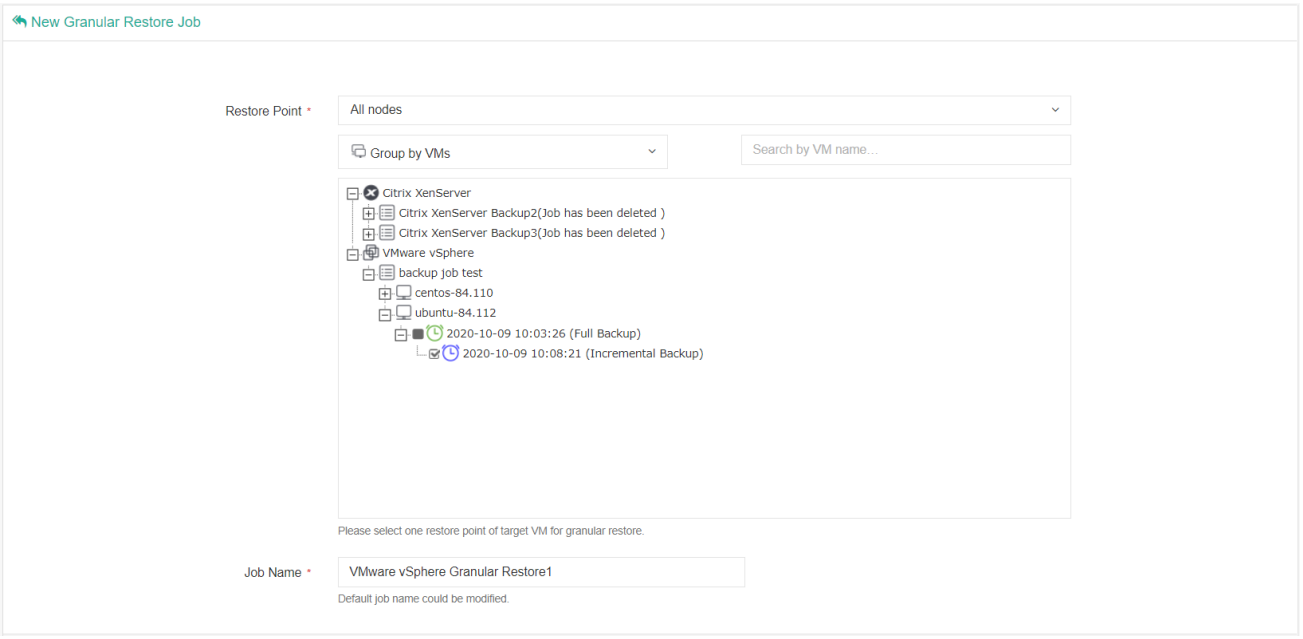
Notice

Do not power on the migrated VM before the whole process is successfully done, otherwise the VM migration will fail.

Granular VM Restore

Create Granular Restore Job

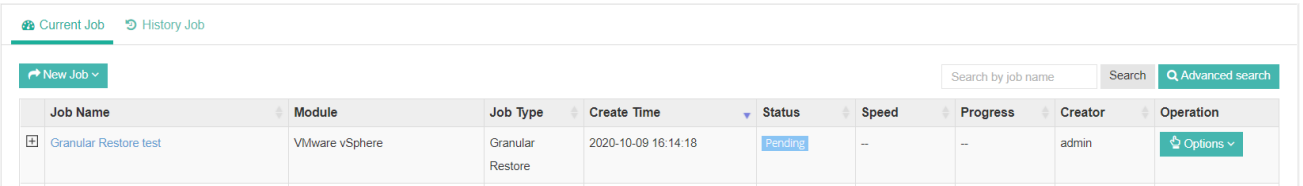
Granular Restore feature allows you to recover files or folders from the VM backup restore point, you don't have to restore the entire virtual machine for the purpose of recovering some files.
To create a granular restore job, please go to **VM Backup** > **Restore** > **Granular Restore** page, you will see all the available restore points under your virtual infrastructure.



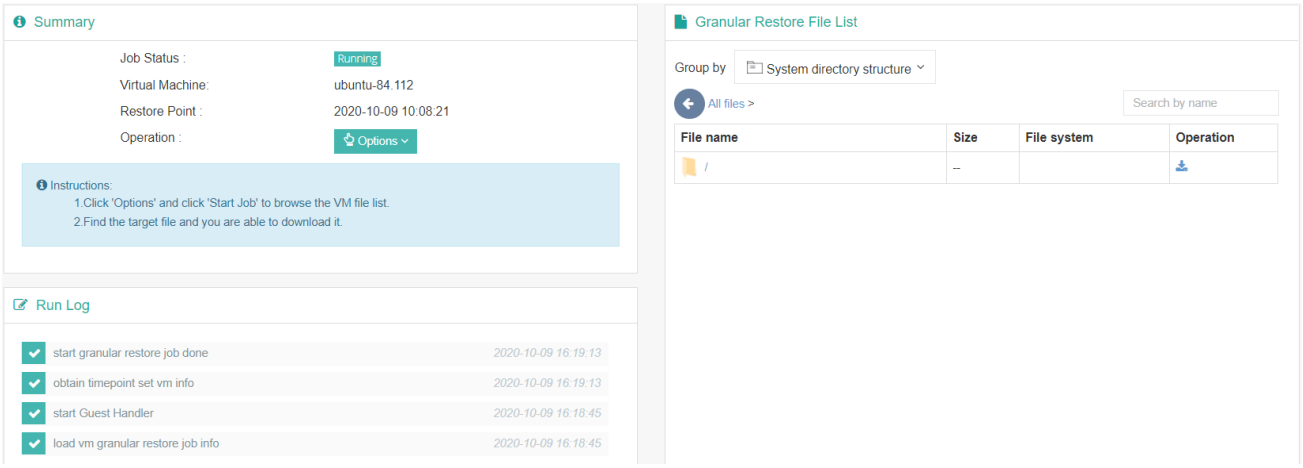
Select one restore point where you can find your target file. The restore point can be a full, an incremental or a differential restore point.
When done selecting the restore point, you may rename the granular restore job if necessary, then click on OK button to submit.

Granular Restore Job Operations

Once you finished creating the granular restore job, you'll be redirected to the **Monitor Center** > **Jobs** page. The newly created granular restore job will be listed in the current job list in pending status.

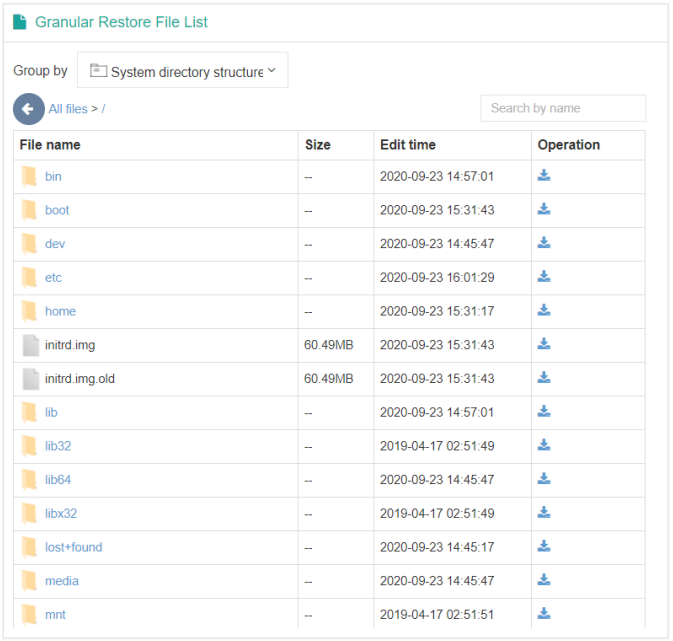


To run the granular restore job, please click on **Options**, then select **Start Job**. And the job status will change into preparing. The preparation process will take several seconds to several minutes depending on the VM size and the performance of Vinchin Backup Server hardware. After this, the status will change to running.
When you get running status, please click on the job name to browse the file list of the VM.



In the **Granular Restore File List** column, you are able to retrieve the desired files or folders. You can also organize the file list by system directory structure, physical disk device and LVM as per your convenience.

Enter the target directory, find the target files or folders and click on the button to download.



The downloaded files will be in the original format, while the downloaded folders will be a .tar.gz package, use the below command to decompress the package then you get all files of the target folder.

```
tar -zxvf foldername.tar.gz
```

Notice

Once you had done retrieving the files, please return to current job list, and stop the granular restore job. As if the granular restore job keeps running, certain system resources will always be occupied. And if the job is no longer needed, you can also delete the job from the current job list.

V2V Migration

V2V Migration Licensing

V2V Migration is a value-added feature which is available (also optional) on Vinchin Backup & Recovery Enterprise edition. It needs to be licensed separately based on the number of VMs you plan to migrate from one platform to another/other platforms.
The V2V Migration license will be counted by "per VM per restore" principle, which means for one VM, if you restore it to another virtual platform twice or to two different virtual platforms, 2 V2V Migration license counts will be consumed.

Supported Platforms

The following virtualizations are supported by Vinchin Backup & Recovery for V2V Migration.

- VMware vSphere
- Microsoft Hyper-V
- Red Hat Virtualization (RHV)
- oVirt
- Oracle Linux Virtualization Manager (OLVM)
- Citrix Hypervisor (formerly XenServer)
- XCP-ng
- OpenStack
- Huawei FusionCompute(KVM)
- H3C CAS/UIS
- Sangfor HCI
- Zstack
- Proxmox VE

Conditions and Limitations

V2V Migration involves converting a VM's configurations to a compatible version from one platform to another. And also involves disk format converting.
Due to the hypervisor and other technology differences between virtual platforms, Vinchin cross platform restore must comply with the below conditions.
Cross platform restore should comply with the restrictive conditions of the target virtualization platform, e.g., unsupported guest OS, unsupported hardware, etc.
Antivirus and other security software within the VMs might prevent drivers optimization processing, as a result, some application/software might not run properly after cross platform restore.
After cross platform restore, due to virtual hardware devices changing, hardware signature changing, there's possibility of application malfunction or license exception.

This situation is unavoidable and cannot be eliminated from Vinchin backup server side.
Due to the above-mentioned reasons, Vinchin cannot guarantee 100% success rate of all VM cross platform restores. There are possibilities of manual interaction and restore failures during cross platform restore. As a result, users should not abandon the original virtual platform before all VMs and data assets had been successfully restored to a new virtual platform.

V2V Migration with Full VM Restore

If your Vinchin Backup & Recovery has V2V Migration functionality enabled, and has multiple virtual platforms connected, when creating a VM restore job, you can directly select a different virtualization platform as the restore destination.
Refer to Full VM Restore to create a VM restore job for V2V Migration, in **Restore Destination**, step 2 of the job creation wizard, you can see all virtualization platforms connected to Vinchin. Expand the target virtualization and select a target host as the restore destination.
After the job is completed, the selected VM(s) will be restored to the target virtualization platform.

V2V Migration with Instant VM Restore

Vinchin Instant VM Restore feature allows you to use a VM's backup to run the VM directly on a different virtual platform. Within 15 seconds, the VM will be ready to start up on any desired platform. It ensures your core business continuity across virtual platforms in your hybrid virtualization environment.
If you have V2V Migration enabled with your Vinchin Backup & Recovery, when creating an instant VM restore job, you are allowed to select any virtual platform connected to Vinchin backup server. Please refer to Instant VM Restore to complete instant restore job configurations, in the **Target Host** field, please select a host from the target virtualization platform. Once the job is created and you click to start the job, you are able to access this VM and its services within 1 minute from the new virtual platform.
V2V Migration with instant restore runs the VM directly from backups resides in Vinchin backup server's storage repository. A live migration operation is required during non-production hours to migrate all backup data including the cache data generated during instant restore runtime to the new virtual platform datastore. Please refer to Live Migration to configure the migration settings, the migration should also be targeted to the new virtual platform.

Physical Backup

Preparation for Physical Backup

Physical backup of Vinchin Backup & Recovery is an agent-based backup functionality which can perform file level, application level (database) and volume level backups to meet the data protection needs of customers physical servers.
Before creating backup jobs for the file servers, database servers or the entire operating system of the physical servers, backup agents need to be deployed on the servers.

Deploy Agents for Linux Server

Download Backup Agent for Linux Server

Open the web console of Vinchin Backup & Recovery, on the login screen, click on **Download Backup Plugin** to show the agent download options.
In the **Type** dropdown list, please select **Physical Backup Agent** option.
In the **OS** dropdown list, please select the target Linux distribution.
Click on **Download** button to download the backup agent for the Linux servers.
The downloaded backup agent installer for Linux server should be a .tar.gz package. If you've downloaded it on a Windows desktop, please upload it to the Linux server which you wish to backup.

Install Backup Agent for Linux Server

Login to the command line interface (CLI) of the Linux server. Install the backup agent follow the steps below.
1. By using the below command to decompress the .tar.gz package.

```
tar -zvxf vinchin-backup-agent-xxx-x86_64.tar.gz
```

Where the 'xxx' should be the version number and Linux distribution same as the actually downloaded installer.

2. Enter the backup plugin package folder.

```
cd vinchin-backup-agent-xxx-x86_64
```

Where the 'xxx' should be the version number and Linux distribution same as the folder decompressed from the agent installer.

3. Install with the below command.

```
./agent_install
```

Once you execute the agent install command, the installation will begin, and during the installation process, you need to specify the agent connection mode and maybe required to specify the backup server IP based on connection mode you choose.

4. Choose the connection mode.

```
1) Server-to-client
2) Client-to-server
Please select connection mode [1,2] <default 2>:
```

Choose between 1 and 2 to determine “server to client” or “client to server” connection mode.

If 1 (input 1 and press enter), the agent will only be installed and will not connect to server, users will have to add the agent from Vinchin Backup & Recovery web console after the agent installation.

If 2 (directly press enter or input 2 and press enter), users will be asked to provide the Vinchin backup server IP for the agent being able to automatically connect to after the installation.

5. Specify backup server IP.

Only if the connection mode is 2, users will be asked to specify the backup server IP.

```
Please select connection mode [1,2] <default 2>:2
Please input backup server IP:172.18.1.10
```

Please enter Vinchin backup server IP then press enter.

6. Specify client/server listening port.

If the connection mode is 1, users will be asked to specify the client listening port. It’s not recommended to change the port number, please press enter to continue.

If the connection mode is 2, users will be asked to specify the server listening port. It’s not recommended to change the port number, please press enter to continue.

7. Specify client transport port.

It’s not recommended to change the client transport port, please press enter to confirm the installation.

Once the users completed the above settings, the installation will be done in a few seconds, if you had chosen connection mode 1 (server to client), after the agent installation, please open Vinchin Backup & Recovery web console to add the agent to Vinchin backup server, please refer to Add Physical Backup Agent.

Deploy Agents for Windows Server

Download Backup Agent for Windows Server

Open the web console of Vinchin Backup & Recovery on the target Windows server which you wish to backup, on the login screen, click on **Download Backup Plugin** to show the agent download options.

In the **Type** dropdown list, please select **Physical Backup Agent** option.

In the **OS** dropdown list, please select **Windows**.

Click on **Download** button to download the backup agent for the Windows servers.

The downloaded backup agent installer for Window should be a .exe package. If you’ve downloaded it on another Windows desktop, please upload it to the Windows server which you wish to backup.

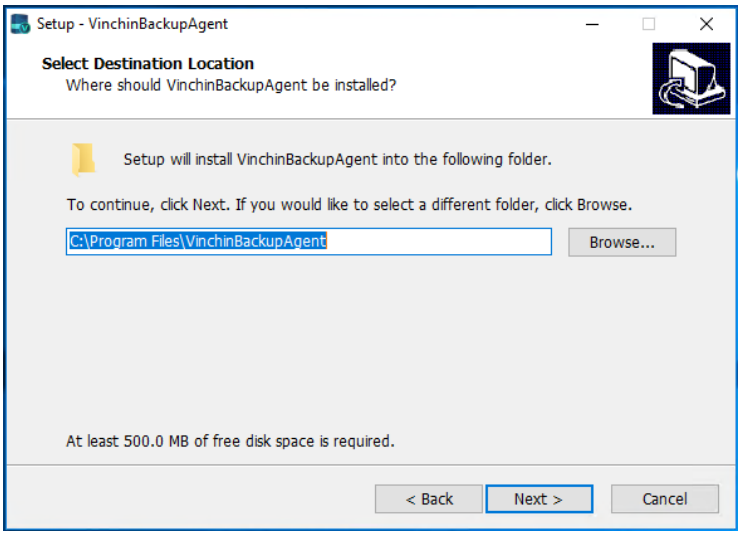
Install Backup Agent for Windows Server

Install the backup agent follow the steps below.

1. Run the backup agent installer with administrator permission by right clicking on the installer and select **Run as**

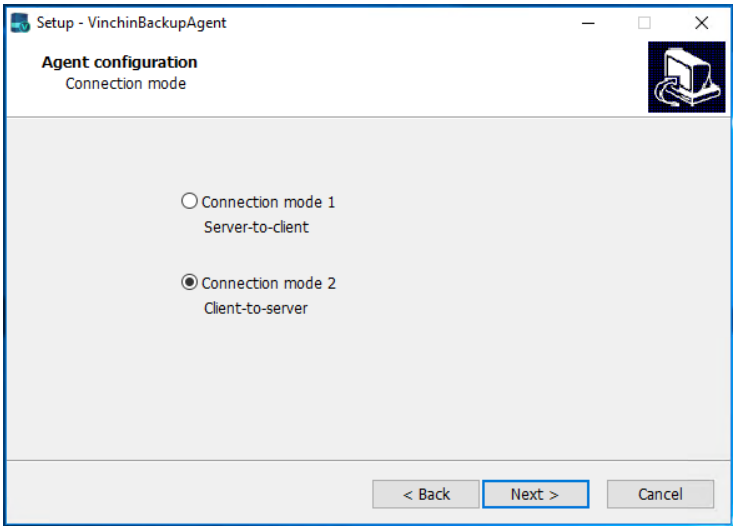
administrator.

2. Specify installation location.



It's recommended to install the backup agent in the default location.

3. Specify connection mode.

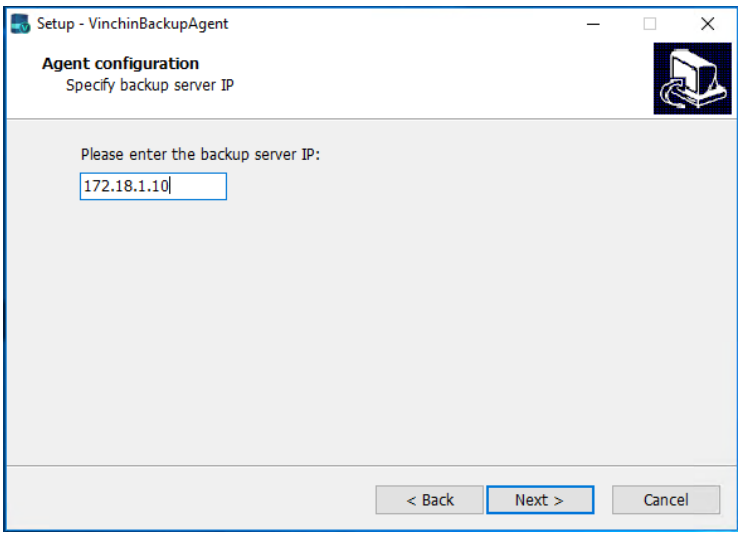


Choose between Connection mode 1 or 2 to determine "Server-to-client" or "Client-to-server" connection mode.

If Connection mode 1, the agent will only be installed and will not connect to server, users will have to add the agent from Vinchin Backup & Recovery web console after the agent installation.

If Connection mode 2, users will be asked to provide the Vinchin backup server IP for the agent being able to automatically connect to backup system after the installation.

4. Specify backup server IP.

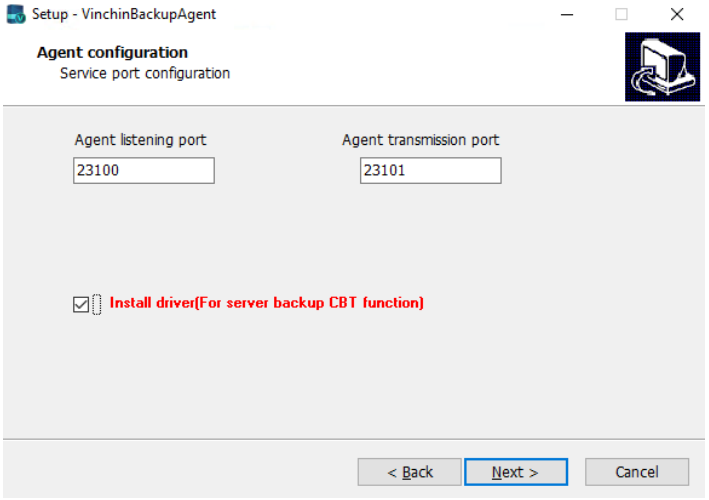


If you chose Connection mode 2, please enter the backup server IP address and click on next to continue.

5. Port configurations.

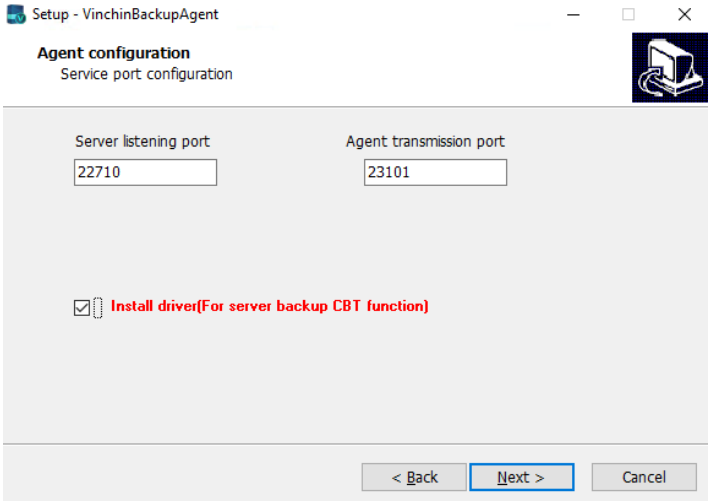
If Connection mode 1, users have to specify the Agent listening port and Agent transmission port.

Besides, you can select install driver If you want to turn on server backup CBT function for fast incremental backup.



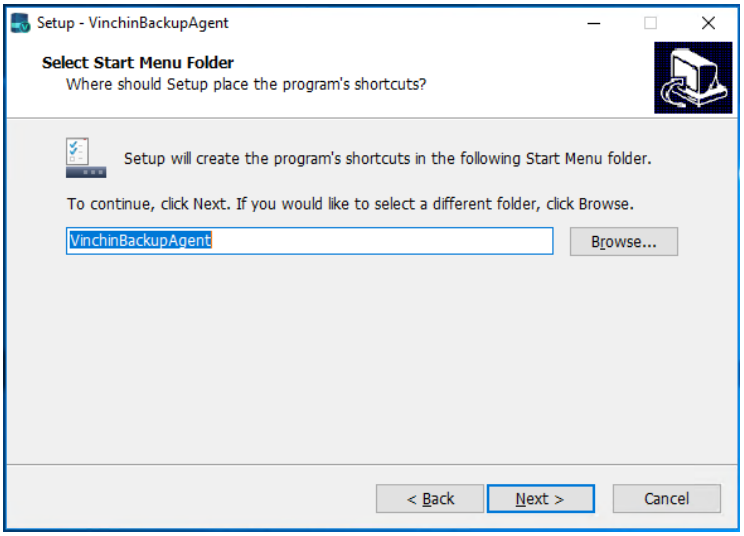
If Connection mode 2, users have to specify the server listening port and agent transmission port.

Besides, you can select install driver If you want to turn on server backup CBT function for fast incremental backup.



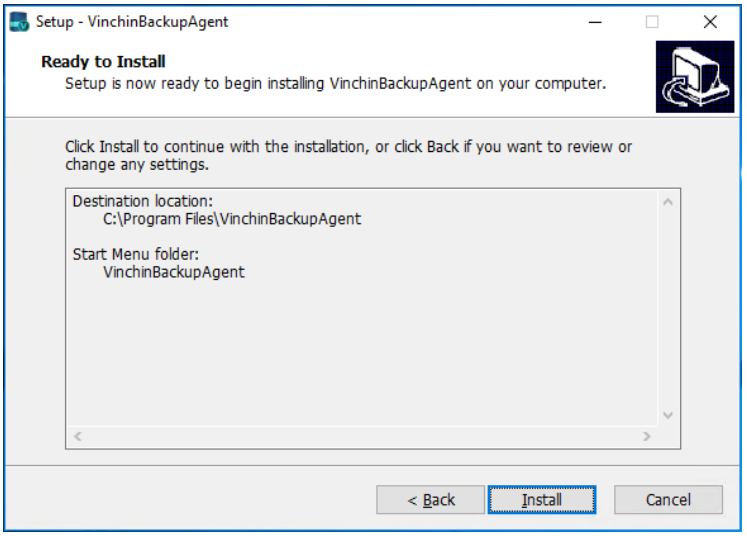
For both scenarios, it's always recommended to use the default port numbers.

6. Specify the start menu folder.



Please use the default folder and click on **Next** to continue.

7. Confirm installation.



If there's no issue with the installation location and the start menu folder, please click on **Install** to confirm the agent installation.

Once the installation is completed, please click on Finish to exist the agent installation wizard. If you had chosen Connection mode 1 (Server-to-client), after the agent installation, please open Vinchin Backup & Recovery web console to add the agent to Vinchin backup server, please refer to Add Physical Backup Agent.

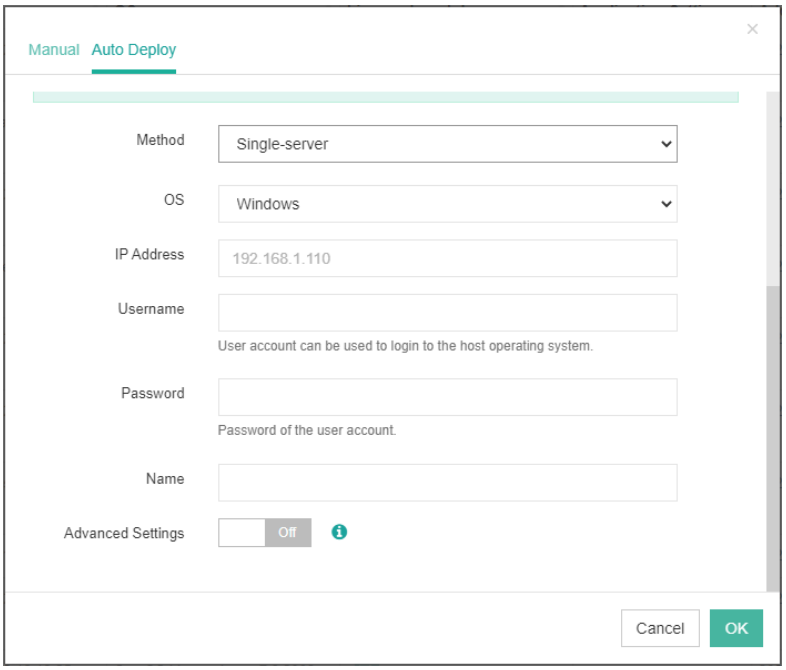
Agent Auto Deployment

Except manually download and install the backup agents for the Linux and Windows servers, users can also choose to auto deploy the agents. The agent auto deployment is supported with RHEL, CentOS, Ubuntu and Debian Linux distributions. For Windows, Windows Server 2008, 2012, 2016, 2019 and 2022 are supported. For Windows server 2003 and Windows desktop, agent auto deployment is not supported.

Agent auto deployment is suitable with the scenario which the backup server and the physical servers are in the same LAN. For other network environments, auto deployment might not work.

Manual

To deploy backup agent on a single Linux/Windows server, please go to **Resources** > **Agents** page. Click on **Add** button, and then in the pop-up dialog please select **Auto Deploy**.



In **Method** dropdown list, please select **Single-server**.

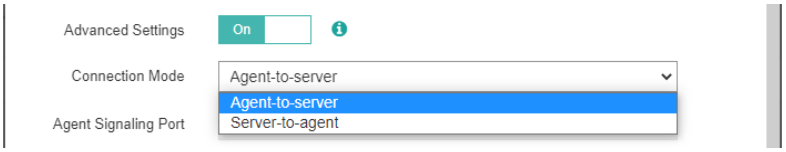
In the **OS** dropdown list, please select the physical server OS type.

In the IP Address field, please enter the IP address of the physical server for Vinchin backup server being able to connect and deploy backup agent.

In the **Username** and **Password** field, please provide the user credentials of root (if Linux) or administrator (if Windows). If with any other user accounts which lack of permissions, the agent deployment will fail.

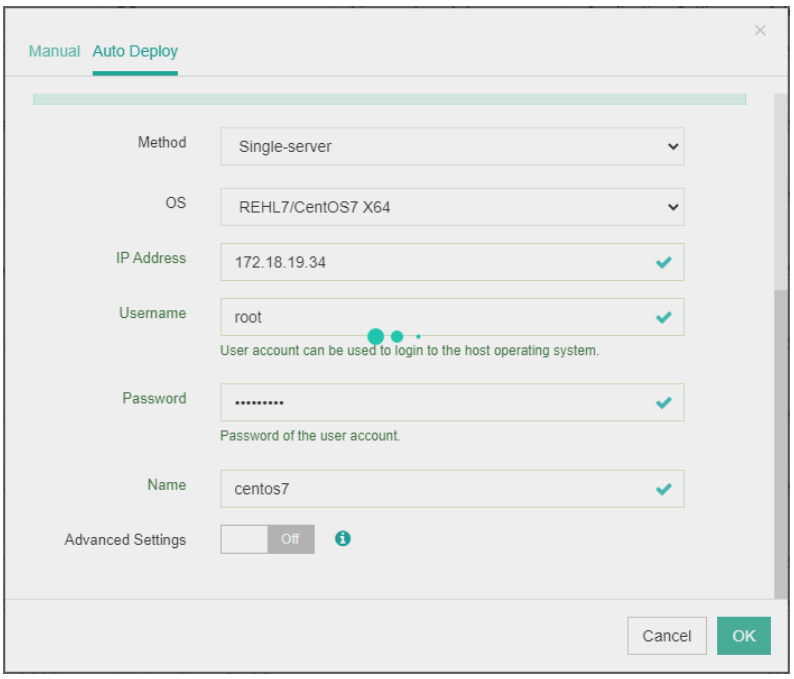
In the **Name** field, users can define a customized name for identification of the server agent.

The **Advanced Settings** are optional, it is used to configure the connection mode and signaling port or transmission port based on the connection mode you wish to use.



Usually, it's recommended to use the Agent-to-server mode, and leave the signaling and transmission ports as default.

Once done the configurations, click on **OK** to confirm adding the agent, Vinchin backup server will then try to connect with the specified server with provided user credentials and try to install the agent automatically.



While the screen is in loading state, please do not leave this page or refresh the page, otherwise it will fail to upload the agent installer to the server.

Once the uploading is done, the agent will be added in to the agent list, its status will be in “Offline(Deploying)” state. When the agent have been successfully deployed, the agent status will be changed to “Online(Deployed)”.

Import

For deploying physical backup agents on a large amount of physical servers, Vinchin provides batch import option for users to import the server list from a template file.

Please go to **Resources** > **Agents** page. Click on **Add** button, and then in the pop-up dialog please select **Auto Deploy**.

In the **Method** dropdown list, please select **Batch-import**.

Click on **Download template** to download the batch import template, a .xls file will be downloaded to your desktop, please edit this file with MS Excel.

In the **IP Address** column, please list the IP addresses of the servers which you wish to deploy backup agents.

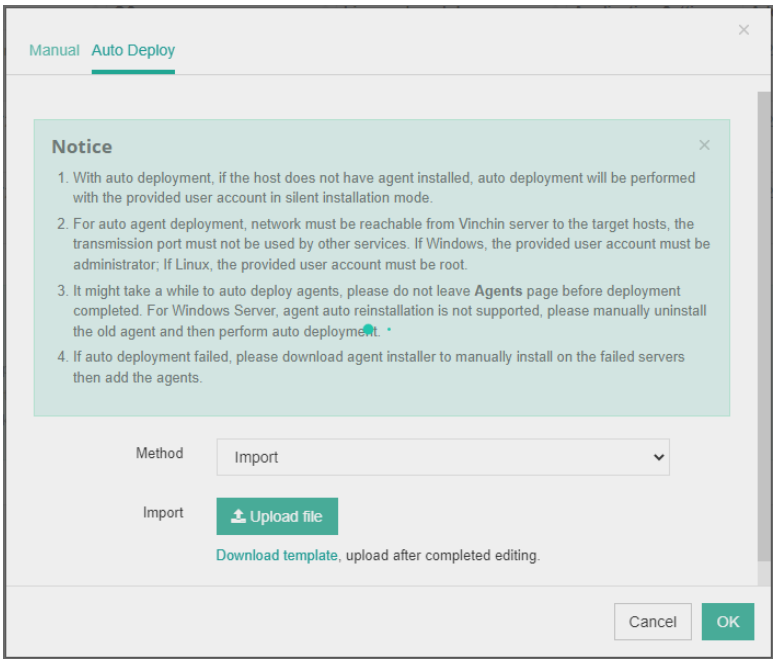
In the **Operating System** column, please specify the operating system type corresponding to the IP addresses.

In **User** and **Password** columns, please provide the user credentials, if Linux, please use root; if Windows, please user administrator.

In the **Alias** column, you can optionally define a customized name for each server for identification.

As for the **Connection Mode** and **Server Signaling Port**, it’s recommended to leave these 2 columns as default.

Once done editing the template file with all the server information, save the modifications and then upload it to batch import the server list for Vinchin backup server to batch deploy agents on those servers.



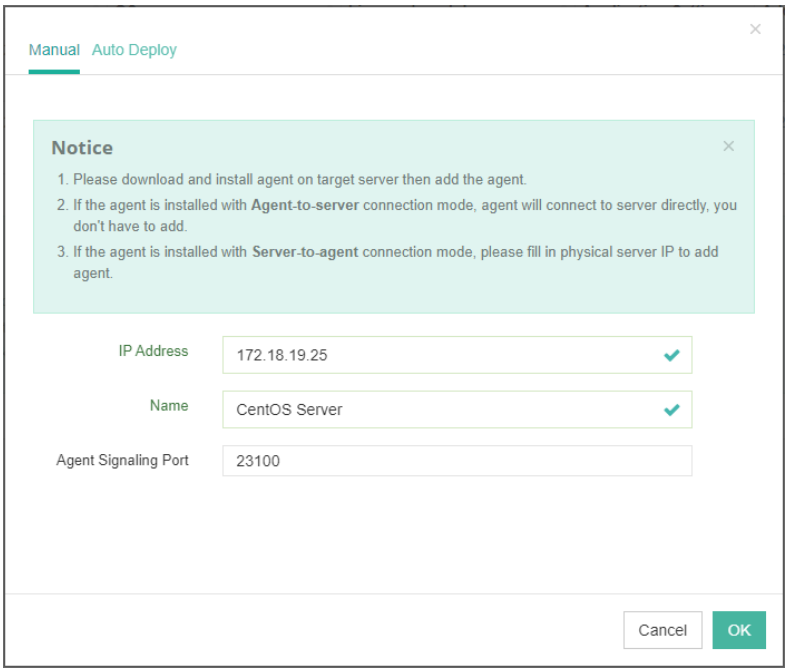
While the screen is in loading state, please do not leave this page or refresh the page, otherwise it will fail to upload the agent installer to the server.

Once the uploading is done, the agents will be added in to the agent list, agents' status will be in "Offline(Deploying)" state. When the agents have been successfully deployed, the agent status will be changed to "Online(Deployed)".

Add Physical Backup Agent

No matter for Linux or Windows backup agents, if the connection mode is 1 (Server-to-client), after the agent installation, users have to added the agents from Vinchin Backup & Recovery web console from **Resources** > **Agents** page.

Click on **Add** button to add the agent.

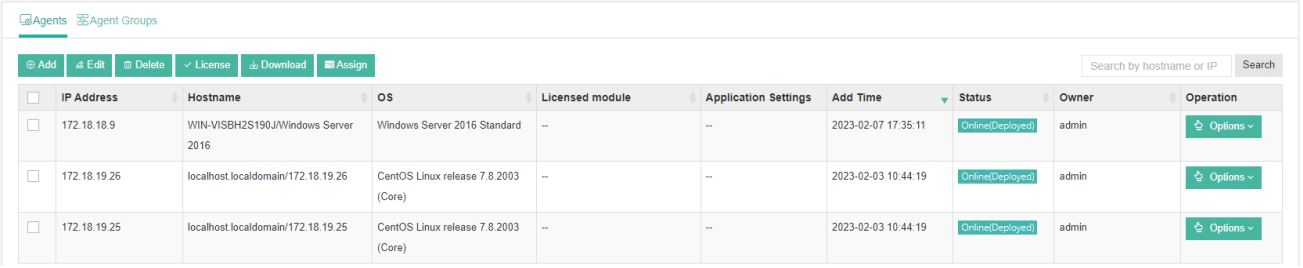


In the **IP Address** field, please input the IP of the Linux/Windows server which you had installed the agent with Server-to-client connection mode.

In the **Name** field, you can give it a name for identification.

As for the **Agent Signaling Port**, it's not recommended to change it, please leave it as default.

Once done, click **OK** to add the agent.

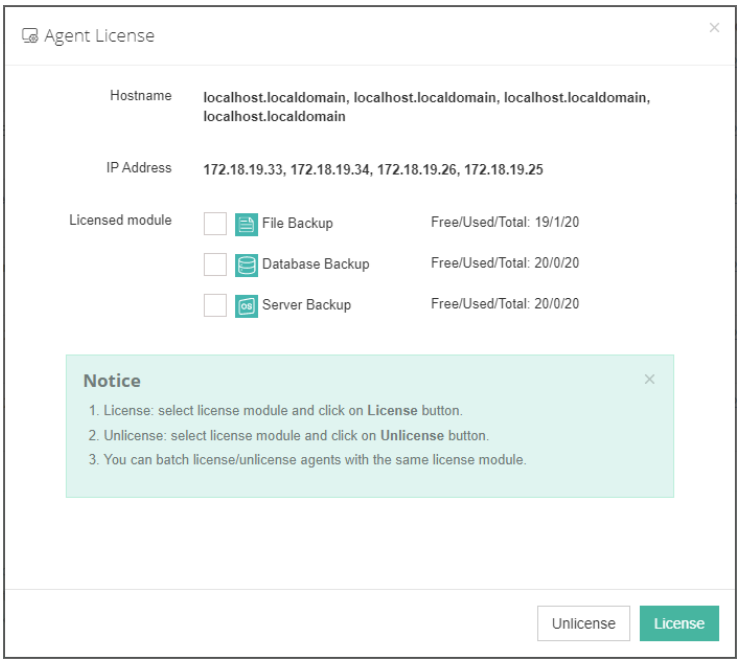


All agents connected to Vinchin backup server, no matter with Server-to-client or Client-to-server mode, will be all list on the **Resources** > **Agents** page.

License Physical Backup Agents

All physical backup agents connected to Vinchin backup server will be listed on the **Resources** > **Agents** page. Before users can perform file, database or server backup, the agents need to be licensed with corresponding license modules.

Select one or a group of physical backup agents and click on License button, you'll be able to enable backup of those agents.



The physical backup agents can be licensed with File Backup, Database Backup and Server Backup license modules. According to the workloads running on the physical server, please select corresponding module and then click on **License** button to get the agents licensed for backup.
To unlicense the agents, please also select the corresponding module and click on **Unlicense** button to get the agents unlicensed.

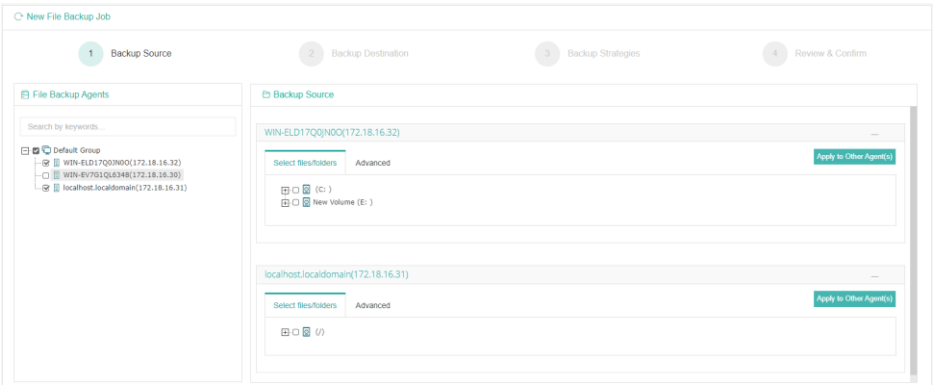
File Backup

Create File Backup Job

To create file backup jobs, please go to **Physical Backup** > **File Backup** > **Backup** page. There are 4 steps to create a file backup job.

Step 1: Backup Source

First you need to select the file backup agents from the **File Backup Agents** column for this backup job. It can be selected one or more file backup agents at the same time.

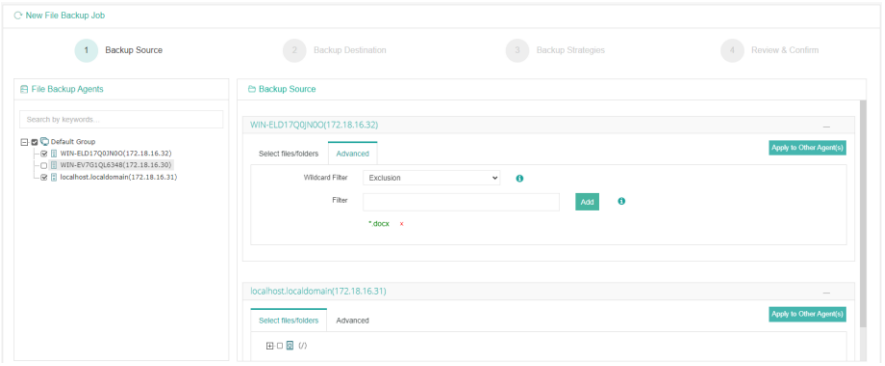


After selecting the file backup agents, click on **+** you can select files/folders you want to back up from the backup source column.

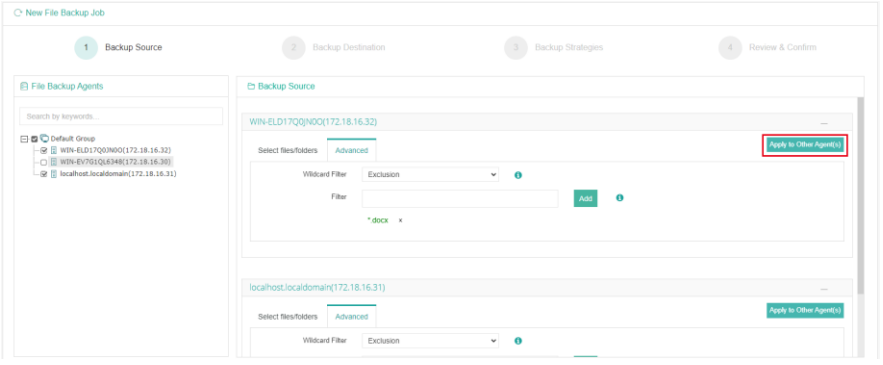
Then you can click on **Advanced,** the wildcard filter can be set.

Wildcard Filter including None, Exclusion and Inclusion. If you choose **None**, backup files/folders which you have selected won't use any filter. If you choose **Exclusion**, backup all files except the ones to be excluded by exclusion filters. If you choose **Inclusion**, only backup files which will be matched by the inclusion filters.

In the Filter field, type a filter rule e.g.: *.docx and click Add to add it; Multiple filters can be applied to a single backup job; '*' can match 0, 1 or multiple characters, '?' can only match 1 character.



After setting the wildcard filter, you can click on **Apply to Other Agent(s)** to apply the wildcard filter to other agent(s). Then click on **Next** to continue.



Step 2: Backup Destination

A backup destination (backup storage) should be associated with this backup job.

In the **Target Node** dropdown list, you can select a backup node on which you want the backup data to be

processed and stored.

In the **Target Storage** dropdown list, the storages which belong to the selected backup node can be selected. When done selecting the backup storage, please click on **Next** button to continue.

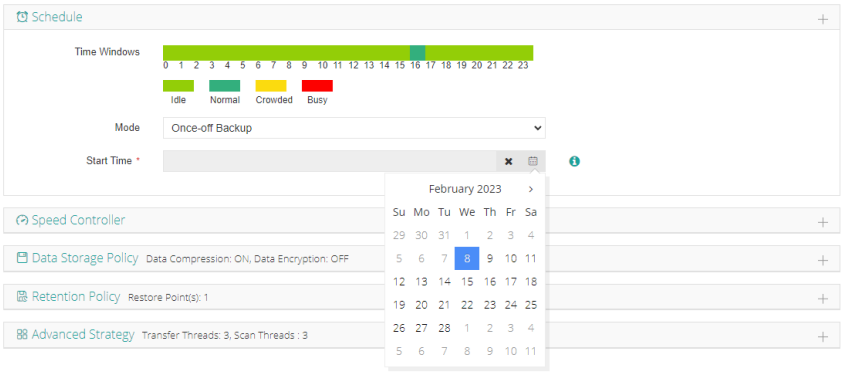
Step 3: Backup Strategies

Under the **General Strategy** tab, you can setup the backup Time Schedule, Speed Controller, Data Storage Policy, Retention Policy and Advanced Strategy.

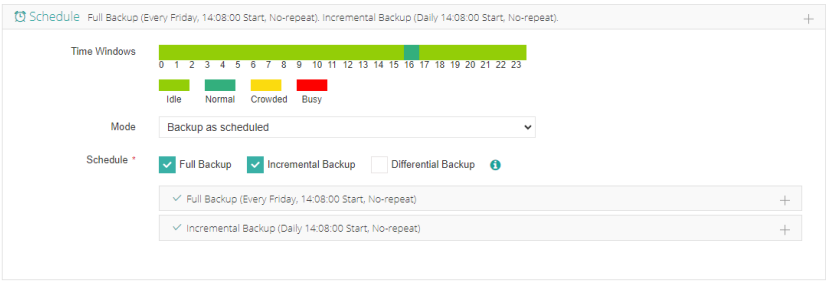
To determine the backup window of this job, the **Time Windows** indicator can be a reference for you to determine in which time window the job should be scheduled.

In the Time Schedule field, you can configure the time schedule of the backup job, you can configure the job as a **Backup as Scheduled** job or a **Once-off Backup** job.

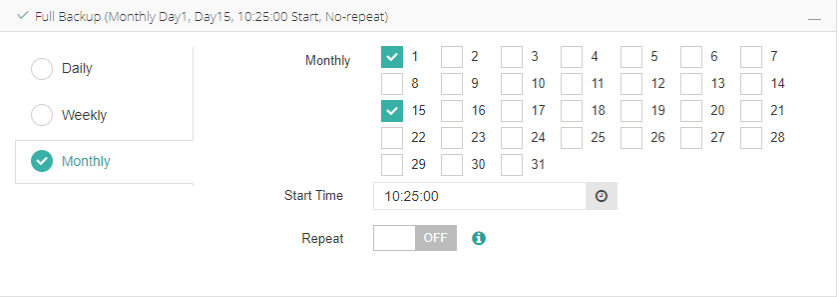
For a once-off backup job, the job will only run for once, and only full backup will be performed. You only have to appoint a time of when to start the backup job in the Time Schedule field.



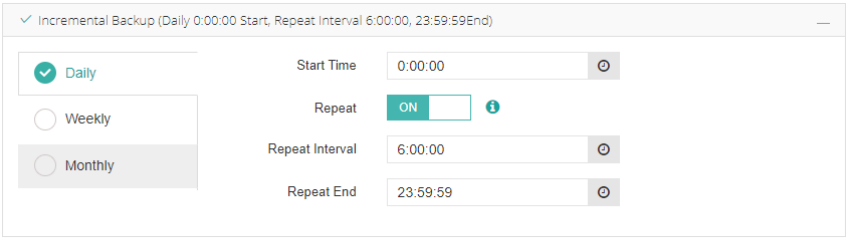
For Scheduled backup job, you can schedule Full Backup with Incremental Backup combination, Full Backup with Differential backup combination. Here we take Full Backup with Incremental Backup as an example.



By default, full backups will be scheduled on each Friday. And incremental backups will be scheduled each day (when the time point of a full backup is overlapped with an incremental backup, full backup will be taken, and the incremental backup with be taken on the next scheduled time point). This is the most commonly used strategy that we recommended. But if you want to customize the schedules according to your requirements, you can edit the settings for either full backups or incremental backups. For example, you can schedule full backups twice a month without repeating.



Then configure several incremental backups each day, by default incremental backup will run only for once each day, to run incremental backups several times a day, you can enable the **Repeat** option.



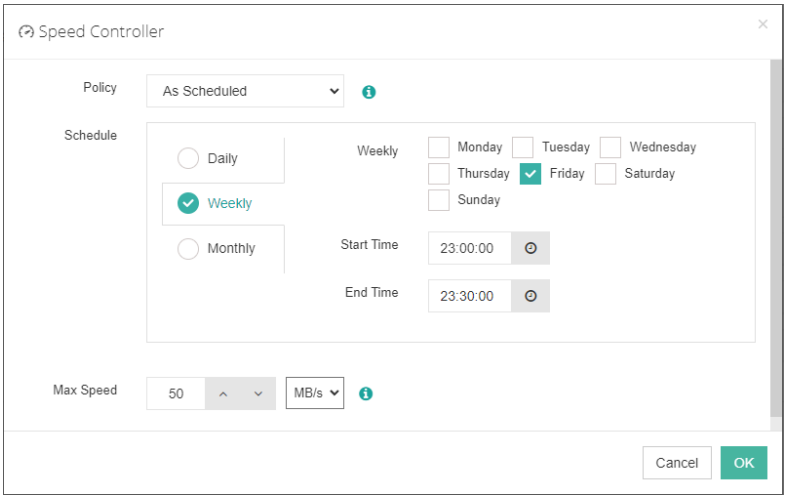
In the above example, full backups will run on day 1 and day 15 of each month, incremental backups will run every 6 hours each day. This is just an example, you should configure the schedules per your requirements based on your actual virtual environments.

Notice

1. It is recommended to run full backups on week basis and run incremental backups on daily basis.

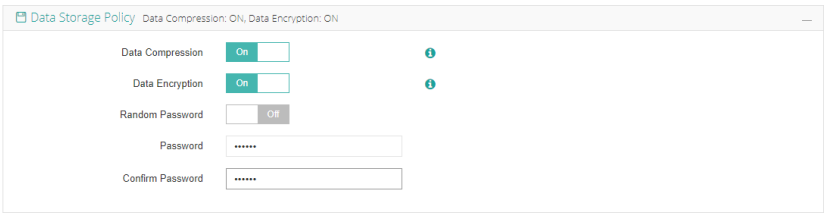
2. It is recommended to set the backup schedule to run at night or in the other nonproduction hours.

After configuring the time schedules of the backups, next you can configure the **Speed Controller**, the speed controller settings are optional, only if the backup jobs will bring network or I/O overload to your production environment, you can configure the speed controller accordingly.



The speed controller policy can be configured as **Permanent** or **As Scheduled**.

Data Storage Policy including **Compression** and **Encryption** of the backup data.



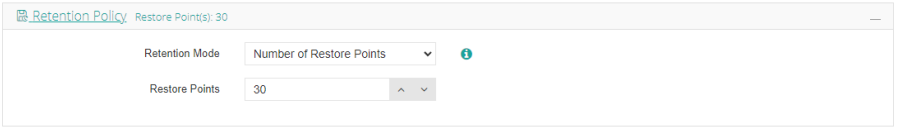
By enabling **Data Compression**, you can save the bandwidth and storage resources for transmitting and storing the backup data.

By enabling **Data Encryption**, the backup data will be encrypted and then stored into the backup storage. A password needs to be specified to secure the data encryption, when creating a VM restore job, password verification is required to perform VM restore.

Notice

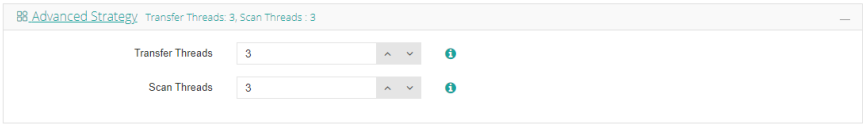
After configuring a custom encryption password, please keep the encryption password corresponding to the backup job safe. If you lose the encryption password, the backup data cannot be restored.

Retention Policy can be used to define how much/long the backup data to be reserved in the backup storage, you can either define the retention policy with **Number of Restore Points** or **Number of Days** mode.



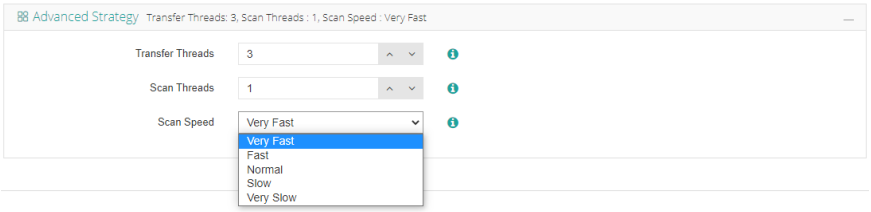
If you choose the retention policy as number of restore points, Vinchin Backup Server will save the specified number of restore points (the number of restore points is counted by full restore point), if you choose number of days, Vinchin Backup Server will save the restore points within the specified number of days, the older restore points will be deleted to comply with the retention policy.

Advanced Strategy contains transfer threads and scan threads. You can set 1 to 32 transfer/scan threads for a single backup job.



Increasing the number of threads can improve backup job efficiency, but multi-threading will occupy the resources of the file server, so the number of threads should be set reasonably according to the actual situation.

In order to eliminate the high efficiency backup impact on the performance of file server, users can set the transfer and scan thread number to 1. And when the scan thread has been set to 1, users also able to configure the scan speed.



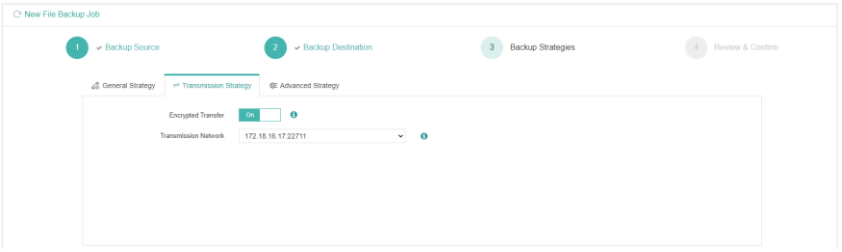
The scan speed can be configured with **Very Fast**, **Fast**, **Normal**, **Slow** and **Very Slow** options to balance the file

server performance and backup speed.

Under the **Transmission Strategy** tab, users can configure transmission options for file backup.

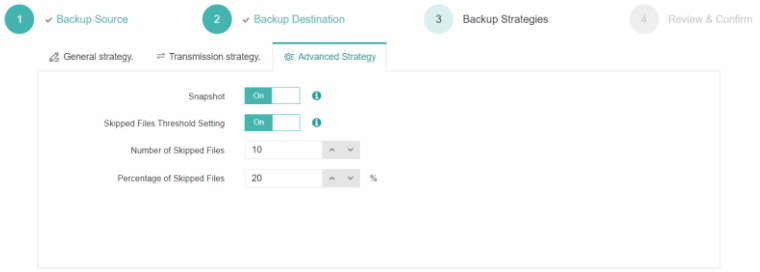
If you enable the **Encrypted Transfer**, backup data will be transferred through SSL protocol.

When multiple networks are configured, you can choose which network to backup, the premise is that the network is connected to the file server.



Under the **Advanced Strategy** tab, you can enable **Snapshot** to ensure file backup data consistency.

You can turn on **Skipped Files Threshold Setting** to setup the alert threshold. If the number or percentage of skipped files exceeds this threshold, the system will alert you.



Notice

To enable snapshot, you need to make sure there's sufficient disk space, if the free space is not enough for snapshot, the snapshot process might fail.

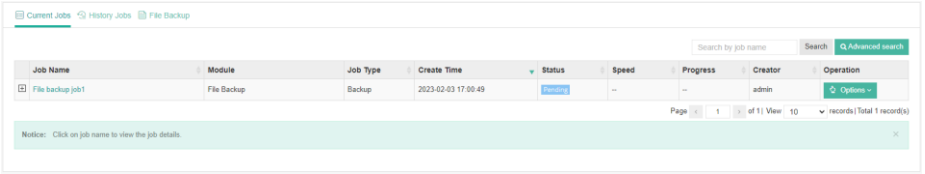
Step 4: Review & Confirm

After completing the above-mentioned settings, you are able to review and confirm the file backup job settings in one screen.

You can give this job a customized name then click on **Submit** to finish creating this file backup job.

File Backup Job Management

Once a file backup job had been created, you will be redirected to the **Monitor Center** > **Jobs** page.



The newly created file backup job will be in pending status, the operations which can be done to the file backup job is similar with the VM backup jobs, you can schedule on, start, stop, edit or delete the job from the current job list.

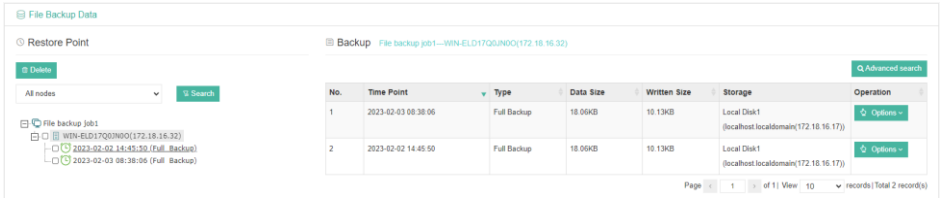
File Backup Data

The file backup data can be managed from **Physical Backup > File Backup** > **Backup Data** page.

View Backup Data

By default, all file backups of all backup nodes from Vinchin backup agents will be displayed, if you wish to view backups of a specific backup node, please select a node from the dropdown list.
The file backup data is organized with a file backup job -> file server -> restore point structure as shown below.

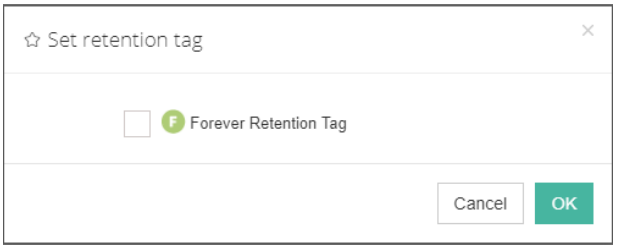
Each restore point is named with the timestamp of its creation and will be marked with its backup type. To view more information of the restore points, simply click on the file server name, all the restore points of the selected file server will be listed on the right with more detailed information.



You can get more information like the actual data size, written size and the storage which is used to store the file backup data.
To search specific restore point(s), you can use the **Search** button on the left or use the **Advanced search** button at the right side of the restore point list.

Retention Tags

The purpose of using the retention tags is to avoid the general retention policy from purging some specific backups and keep them for a longer time period.
For file backup data, you can set **F**: forever retention tag for the full restore points (incremental restore points does not support setting retention tag). The **F** tag can only be manually set. To manually set retention tags, please go to **Physical Backup > File Backup** > **Backup Data** page. By selecting a file server from a backup job, all the restore points will be listed on the right, find the restore point which you wish to set/unset retention tags and click **Options** button, and then select **Set Retention Tag**.



Check the **Forever Retention Tag** option and click **OK** to set the retention tag, once a the restore point has a forever retention tag set, it will be kept permanently until users unset the tag.

Delete Backup Data

We recommend configuring comprehensive retention policy for the file backup jobs to automatically purge the out-of-date backups instead of manual deletion of the backup data. It is a highly risk operation by deleting the backup data manually. If you have to do this, please follow the below instructions.

To delete File backup data, please go to **Physical Backup > File Backup** > **Backup Data** page. There are two approaches to perform the deletion.

From the left side tree view, by selecting a full restore point (incremental or differential restore points cannot be selected) and clicking on the **Delete** button to delete the backups, the dependent incremental or differential restore points will be deleted along with the full restore point.

From the right side table view, click on **Options** of a full restore point and select **Delete**, the selected full restore point will be deleted and the incremental or differential restore points will be deleted as well.

No matter how you perform the backup deletion, you need to provide your login password to confirm the deletion, once the data had been deleted, it's unrecoverable!

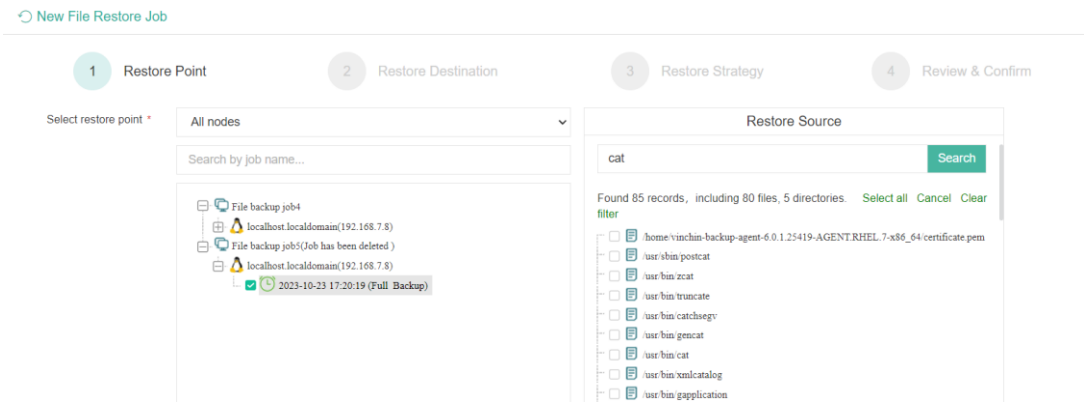
File Restore

To restore files from file backup restore points, please go to **Physical Backup > File Backup** > **Restore** page. There are 4 steps to restore files from the file backup restore points.

Step 1: Restore Point

First you need to select a backup agent and a desired restore point from the **Select Restore Point** column.

Then select the desired files/folders from the **Restore Source** column. You can choose select directories and search under selected directories for more precise and efficient recovery to save your time.



When done selecting files/folders, click on **Next** button to continue.

Notice

If the file backup data had been encrypted, when selecting the restore point, you'll be asked to provide the

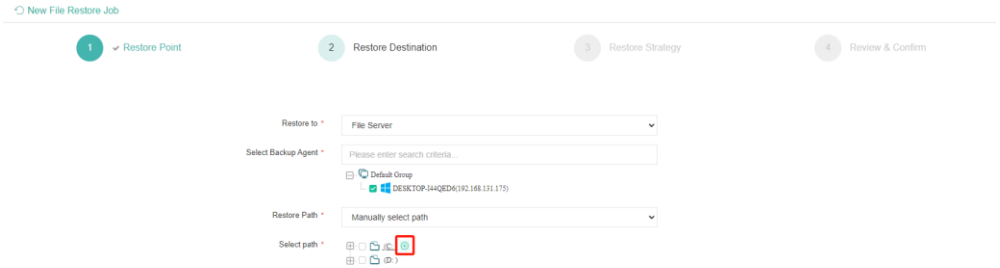
encryption password. Only if you provide the correct encryption password then you can continue to restore the files with the encrypted file backups.

Step 2: Restore Destination

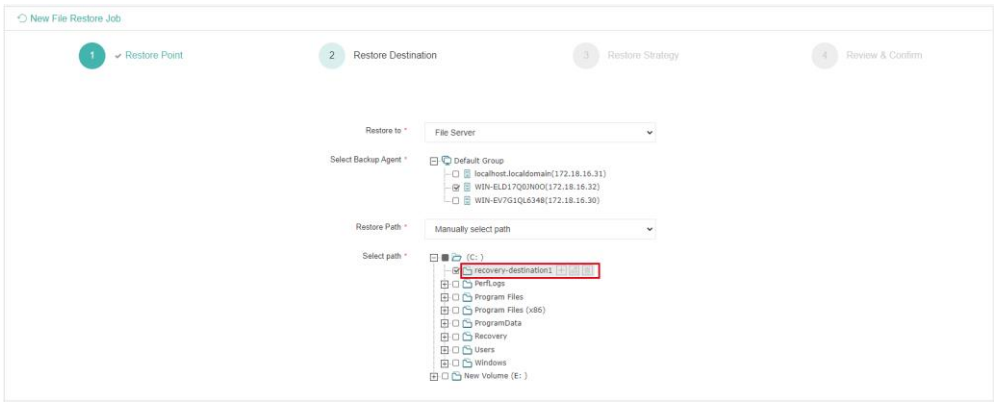
First you need to specify the destination for the selected files/folders to be restored to File server or NAS server.

Then please select the backup agent. You can search agent name for quick match selection. If the **Restore Path** is selected as “Manually select path”, check the specified disk/folder to restore the data to the corresponding path.

As shown in the figure below, hover the mouse over ‘(C:)’ and click the ‘**+**’ on the right can create a new folder.



The defult name of the new folder is “recovery-destination1”, which can be modified or deleted. For windows system, the file name cannot contain ‘< > / \ | : * ?’.



If the **Restore Path** is selected as “Recover to the original path”, the data will be overwritten and restored to the original path, all files with the same name under the original path will be overwritten and restored, and the newly created files will be kept unmodified.

Then please click on **Next** to continue.

Notice

Only when the recovery source and destination are of the same operating system can the recovery path be selected as ‘Restore to the original path’.

Step 3: Restore Strategy

The restore strategies including Speed Controller, Transfer Threads, Encrypted Transfer and Transmission Network, these options are with the same principle as when you setup the file backup job.

Step 4: Review & Confirm

After finishing the above settings, you are able to review and confirm all settings here. Click Submit to confirm creating this job.

Once the job has been created, you'll be redirected to the **Monitor Center** > **Jobs** page.

As the file restore job is by default to be executed right after the creation of the job, so it will run automatically, when you see it in the current job list, it should be in running status already, and once completed, the job will be automatically deleted from the current job list.

After this you can browse the restored files/folders from the selected file server/NAS server and the selected path.

SQL Server Database Backup

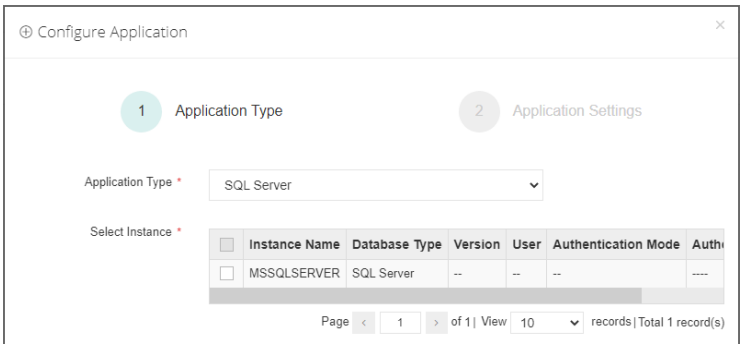
Preparation SQL Server Backup

After the installation of Vinchin physical backup agent on SQL Server database server, users have to license the agent with database backup module.

When done installation and licensing, please open Vinchin Backup Server web console and go to **Resources** > **Agents** page, find the target agent, click on **Options** and then select **Application** to configure application settings for database backup.

Click on **Configure Application** button to configure the application settings.

In the **Application Type** dropdown list, please select **SQL Server**.

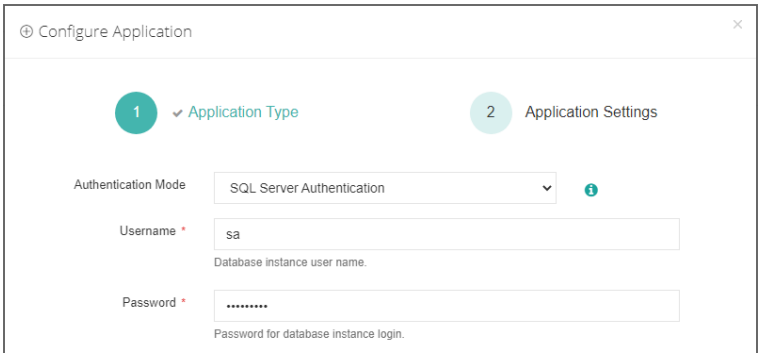


Select the SQL Server instance and click on **Next**.

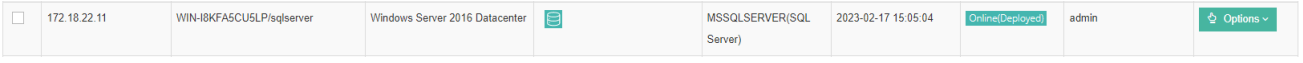
There are two authentication modes, **Windows Authentication** and **SQL Server Authentication.**

If select **Windows Authentication**, agent will use the user which you logged in to connect the SQL Server database, when running database backup.

If select **SQL Server Authentication**, in the popup dialog, fill the **Username** and **Password** that database you want to use.



When SQL Server application is successfully configured, in the agents list, you should see the agent look like below.



Now you should be able to create backup jobs for the SQL Server database server.

Notice

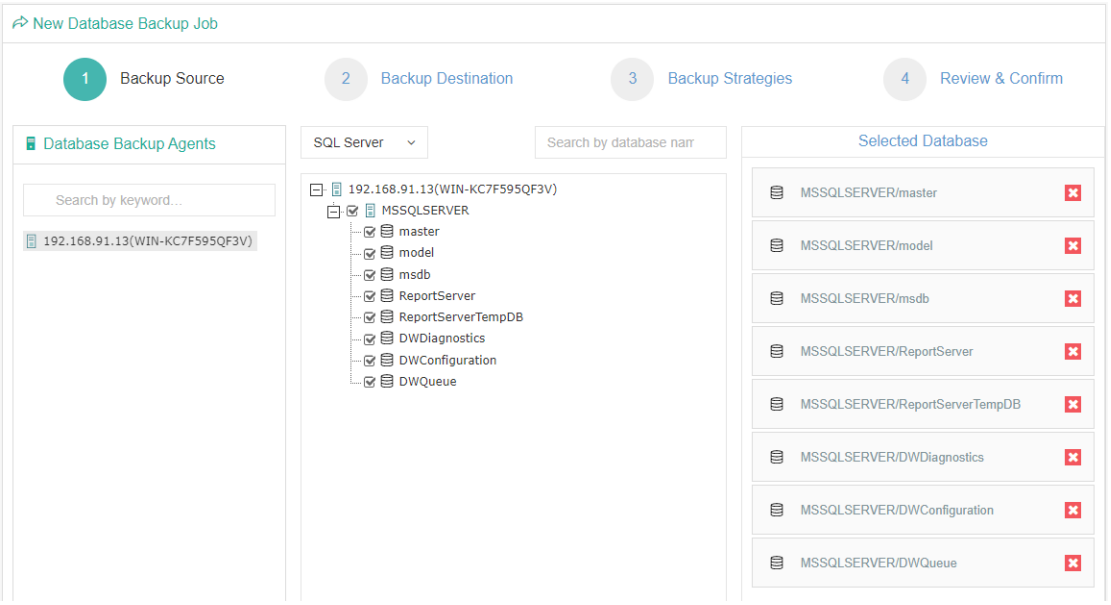
*Whichever authentication mode you select, please ensure that the user must have database **sysadmin** permissions.*

Create SQL Server Backup Job

To create SQL Server database backup jobs, please go to **Physical Backup** > **Database Backup** > **Backup** page. There are 4 steps to create a database backup job.

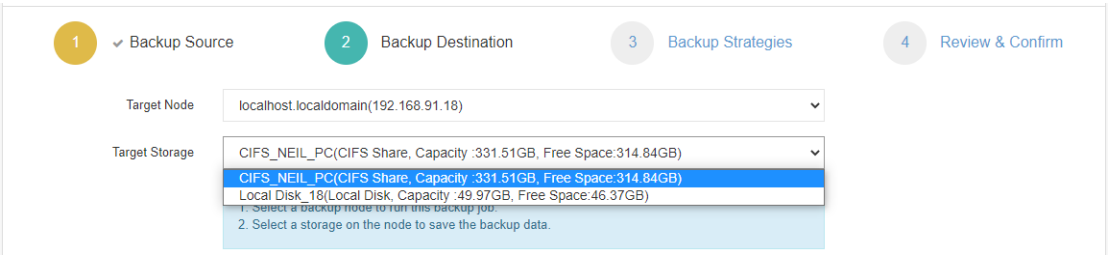
Step 1: Backup Source

First select database backup agent from left column, then expend SQL Server instance and select the databases which need to be backed up.



Step 2: Backup Destination

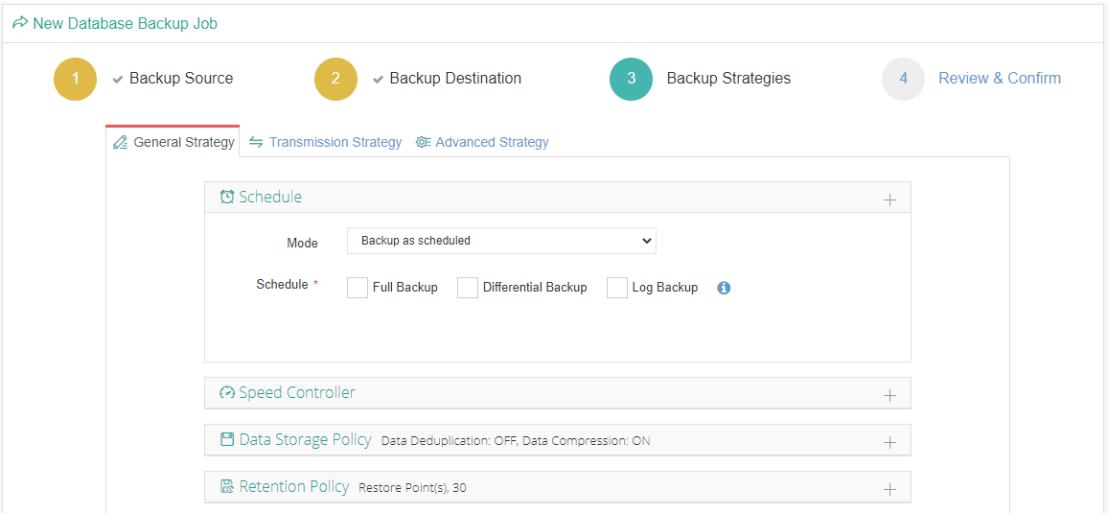
A backup destination (backup storage) should be associated with this backup job.



In the **Target Node** dropdown list, you can select a backup node on which you want the backup data to be processed and stored.
In the **Target Storage** dropdown list, the storages belong to the selected backup node can be selected.
When done selecting the backup storage, please click on **Next** button to continue.

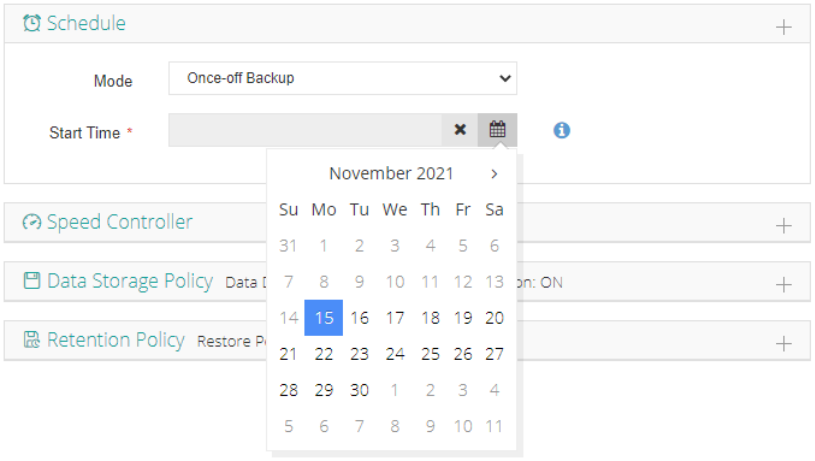
Step 3: Backup Strategies

In the General Strategy it including Schedule, Speed Controller, Data Storage Policy and Retention Policy.



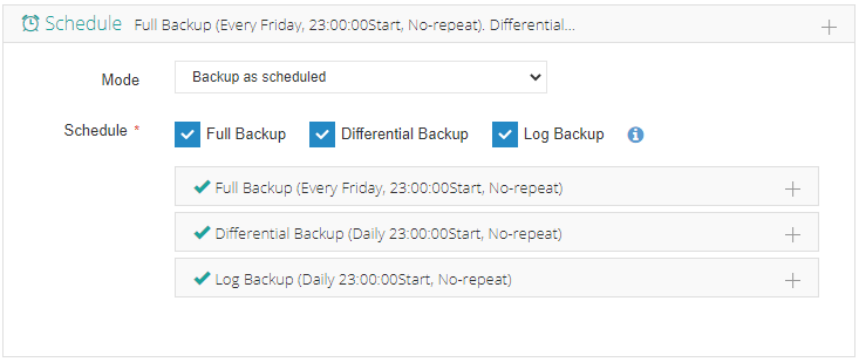
In the Schedule field, you can configure the time schedule of the backup job, you can configure the job as a **Backup as Scheduled** job or a **Once-off Backup** job.

For a once-off backup job, the job will only run for once, and only full backup will be performed. You only have to appoint a time of when to start the backup job, in the Time Schedule field.

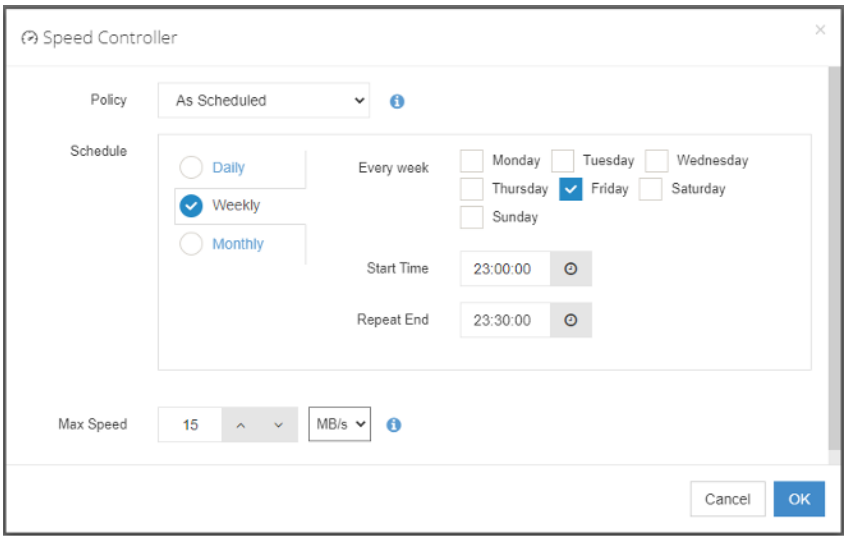


For a backup as scheduled job, you can schedule Full Backup, Differential Backup and Log Backup.

Here we take these three Backup as an example. Please set the backup mode and backup schedule as per your actual demands, then please click on **Next** to continue.

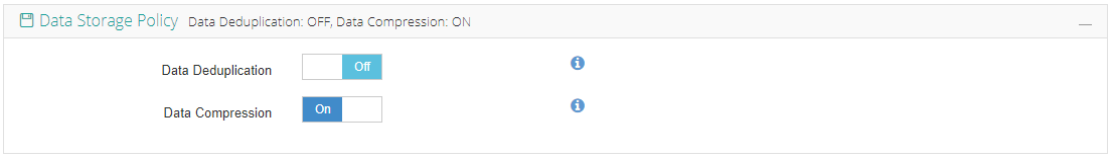


Speed Controller is optional. It can be used to limit the transmission speed during database backup if needed. The speed controller policy can be configured as either As Scheduled or Permanent. An As Scheduled policy can be configured to limit the backup speed on Daily, Weekly and Monthly basis.



A Permanent policy will always limit the backup speed within the specified Max Speed.

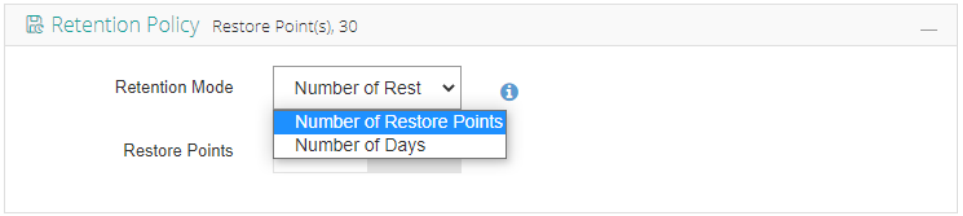
There are 2 options in Data Storage Policy section, Data Deduplication and Data Compression. By enabling these 2 options, the backup data will be deduplicated and compressed before saving into backup storage.



For the retention policy of the database backup, there are 2 retention mode, retain the database backups according to **Number of Restore Points** or **Number of Days**.

For the retention mode **Number of Restore Points**, the restore points will be counted by full restore points, including the differential backups and log backups dependent on this full backup.

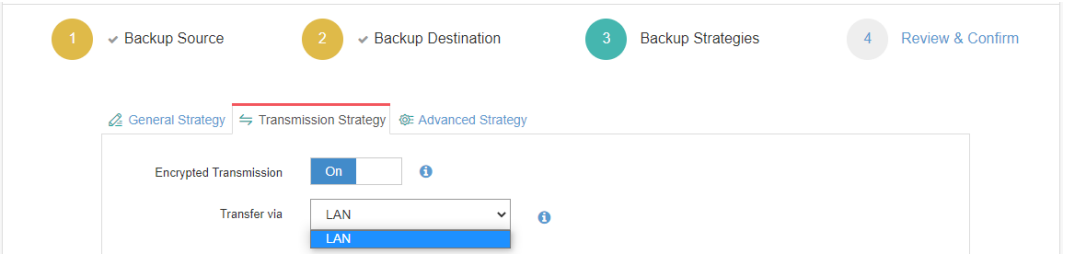
For retention mode **Number of Days**, Vinchin Backup Server will save the restore points within the specified number of days.



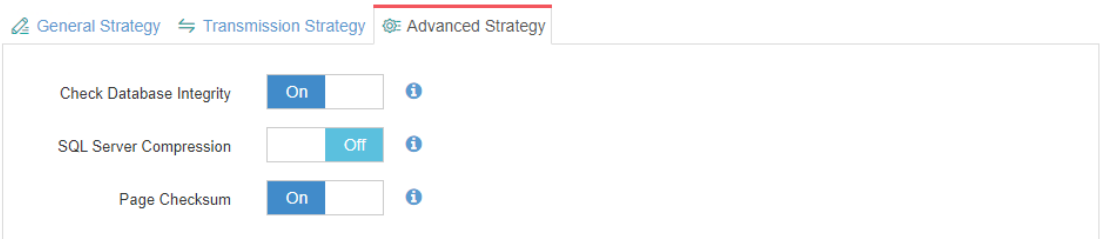
When the retention policy is triggered, the outdated restore points will be purged to comply with the retention policy.

In the transmission Strategy, you can choose to enable **Encrypted Transmission** for data safety.

The backup data will be transferred through LAN by default.



Advanced Strategy including Check Database Integrity, SQL Server Compression and Page Checksum.



Check database integrity function is to check database integrity and physical errors before the database backup job start.

SQL Server Compression is provided by SQL Server to reduce data transfer, data backup time and saves backup storage.

Page Checksum is used to verify the backup data during the transmission to avoid data damage.

Notice

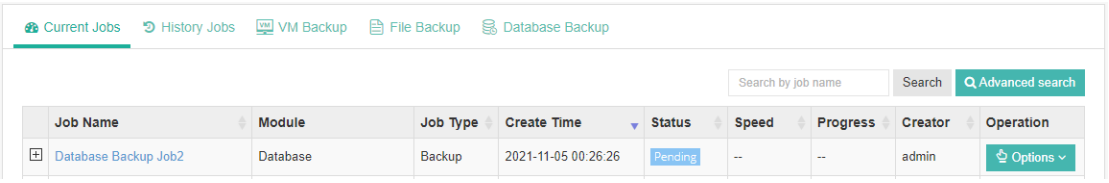
Between General Strategy Compressed Transfer and Advanced Strategy SQL Server Compression prefer only enable Compressed Transfer in general strategy. SQL Server Compression will use more CPU and memories.

Step 4: Review & Confirm

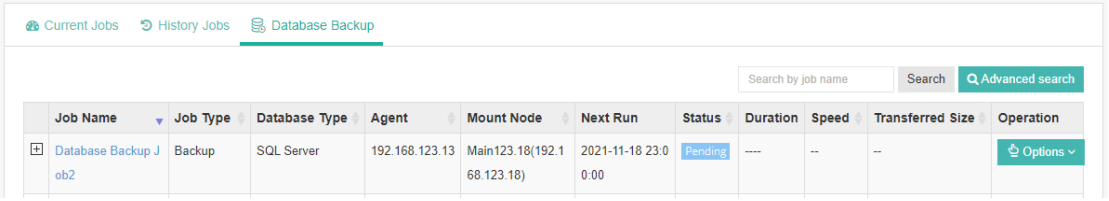
After completing the settings mentioned above, you can review and confirm the settings in one screen.
A job name can be specified for identification of the database backup job, and by clicking on the Submit button to create the backup job.

SQL Server Backup Job Management

Once a database backup job had been created, you will be redirected to the **Monitor Center** > **Jobs** page.



The status of the newly created job will usually be **Pending**, when the time condition matches the schedule, it will automatically run. And the status will change to Running, you can also see the transfer speed here within the job list.
Besides the Current Job list, there's a dedicated tab to show database backup jobs. More detailed information of database backup jobs, including database type, database agent info, backup node, next run time and some more detailed information dedicated for database backup will be given.



By clicking on the job name, you can check more detailed information on the **Job Detail** page.
For a scheduled backup job, after running one of the schedules, the status will change to Pending again and then wait for the next run.
For a once-off backup job, after running the job for once, it will be removed from the Current Job list. And you can find it from the History Job list.

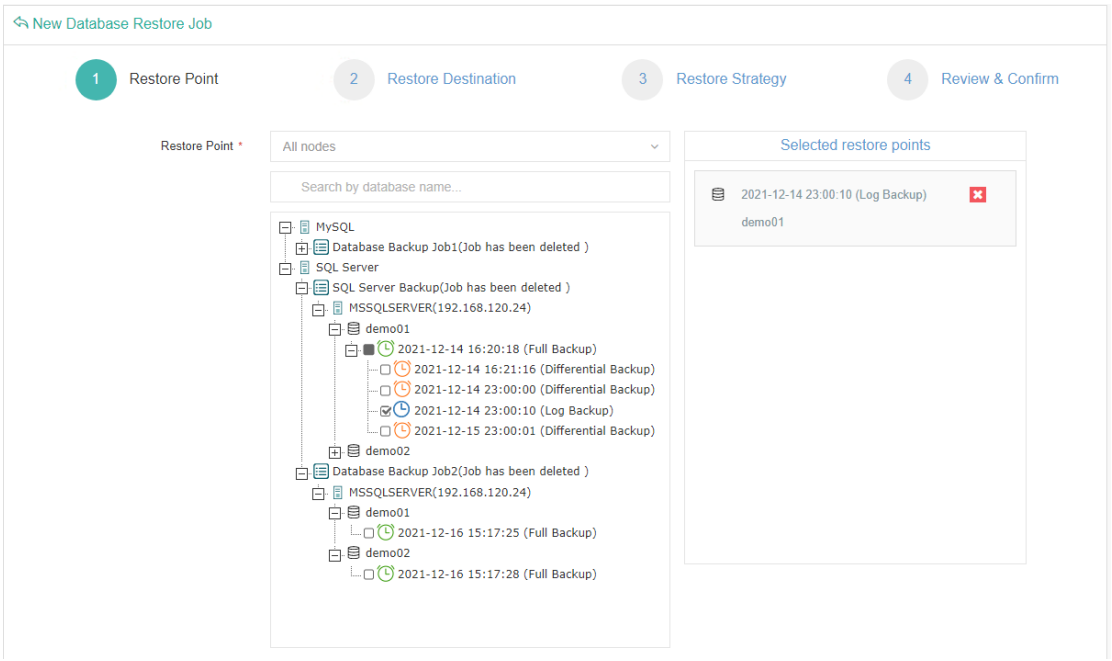
Create SQL Server Restore Job

To restore databases from database backup restore points, please go to **Database Backup** > **Restore** page. There are 4 steps to restore databases from the database backup restore points.

Step 1: Restore Point

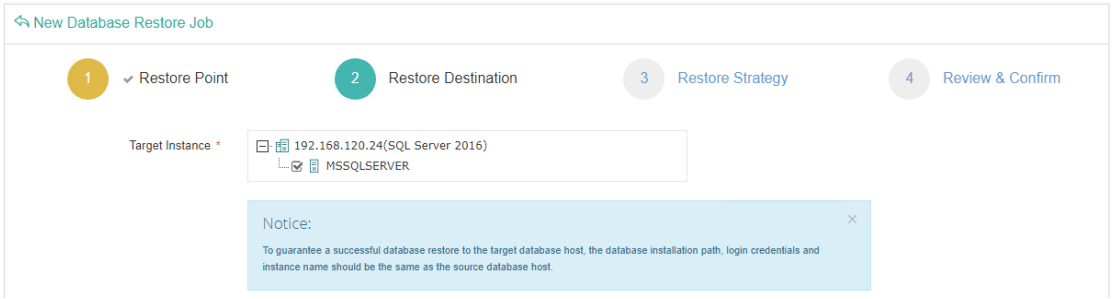
In the Restore Point dropdown list, select a backup node which stores the desired restore points.
Select a target database restore point under your database which you want to restore. You can quickly find the target restore point by searching the job name, database name or the date of the restore point. One restore job can

only select one restore point.



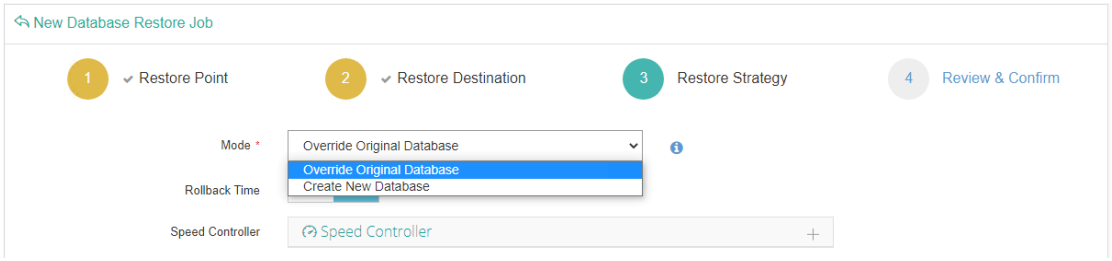
Step 2: Restore Destination

After selecting the desired restore point, please select the target database instance on which you wish to restore.

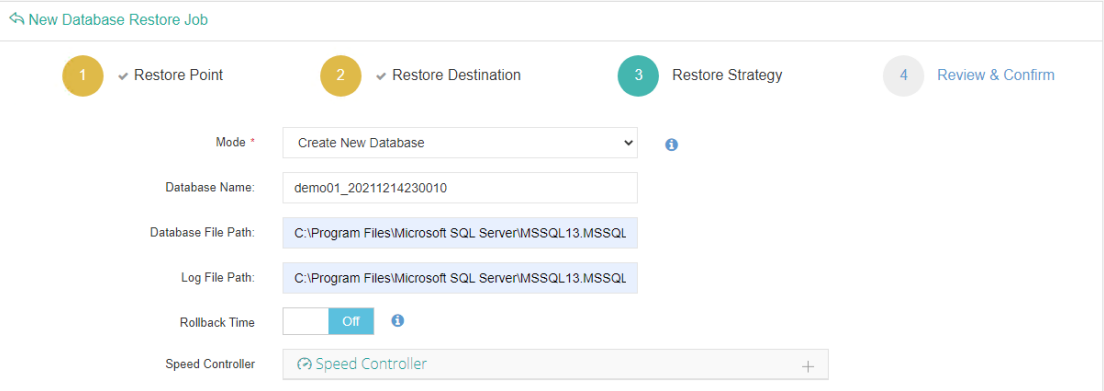


Step 3: Restore Strategy

There are 2 options for database restore, Override Original Database and Create New Database. If you want to use the Override Original Database restore, please pay attention to this mode, it will directly override the database. It is recommended to use the Create New Database restore to first restore the data to a new path to verify the data then perform override original database restore.

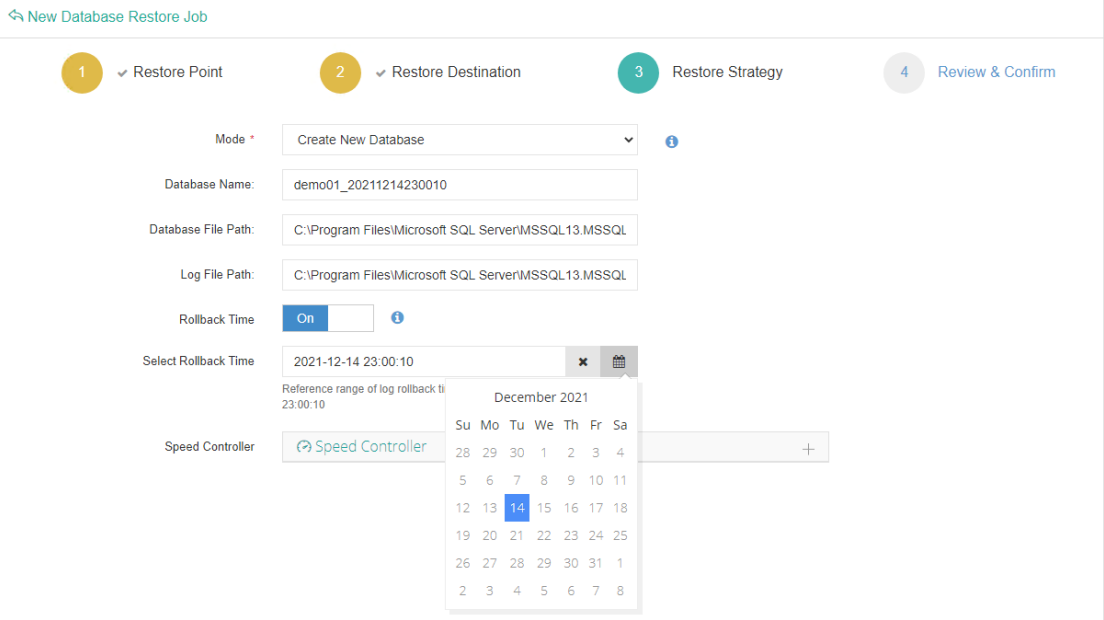


Select Create New Database need to edit database name, database file path, log file path. The path must be correct and have enough free disk space, the path will be automatically created during restore process.



Rollback Time: only if you had selected a log backup restore point to restore, you are allowed to perform transaction rollback restore. If you disable rollback time it will restore to the latest time point (time point of when the selected backup was taken) by default.

You can select the rollback time in second level within the reference range of log rollback time, so you can rollback the database to the state of any desired time point.



Same as database backup, while restoring databases, you can also configure speed controller to limit the database restore speed accordingly.

Step 4: Review & Confirm

After completing the above mentioned settings, you are able to review and confirm the settings in one screen.

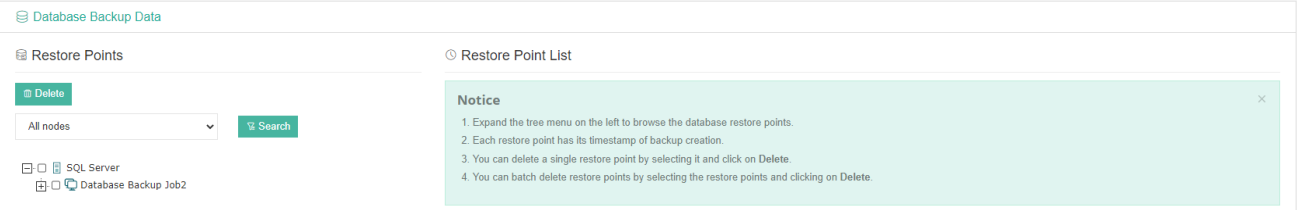
Once the job has been created, you'll be redirected to the **Monitor Center** > **Jobs** page.

As the database restore job is by default to be executed right after the creation of the job, so it will run automatically, when you see it in the current job list, it should be in running status already, and once completed, the job will be automatically deleted from the current job list.

After this you can browse the restored job from History Jobs. Your restored data will be found in the path you configured during creating the restore job.

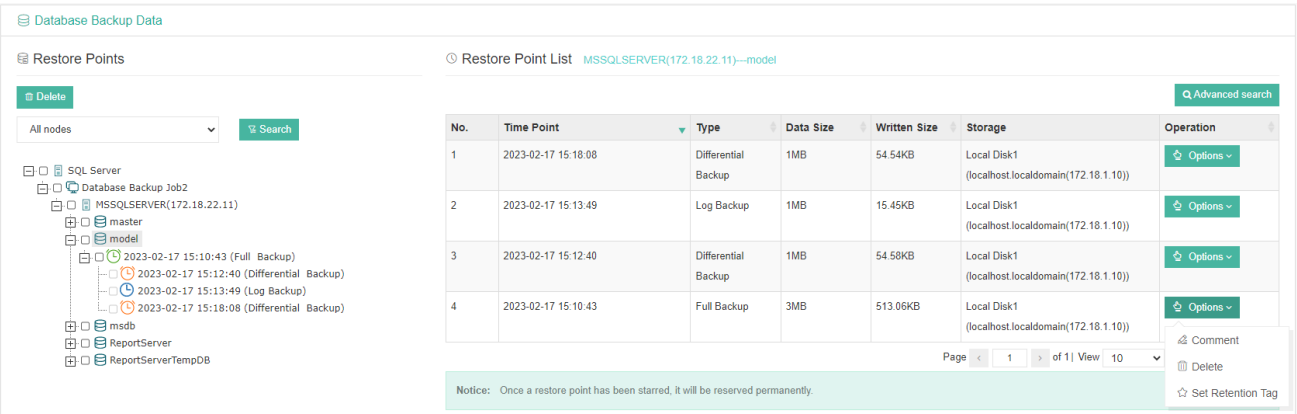
SQL Server Backup Data

The database backup data can be managed from **Physical Backup** > **Database Backup** > **Backup Data** page.



If you want to delete a restore point or multiple restore points, you can first select target restore point(s) from the left tree view, and click on the **Delete** button. The differential backup and log backup cannot be deleted independently, they will be deleted along with the dependent full backup.

When deleting backup data, you need to provide your login password to confirm the deletion, once deleted the data will be unrecoverable.



For the restore point list in the right column, you need to select a database in the left tree menu to view all restore points of the selected database. Information like backup type, data size, written backup size and storage will be given.

You can add comments to the full backups, differential backups and the log backups, and set retention tags for the full restore point to keep the full backup and its dependent incremental and log backups to not be deleted by retention policy.

A full restore point can be also deleted from the Restore Point List by clicking on Options and then select Delete, the dependent differential and log backups will be deleted along with the full restore point.

MySQL Database Backup

Preparation for MySQL Backup

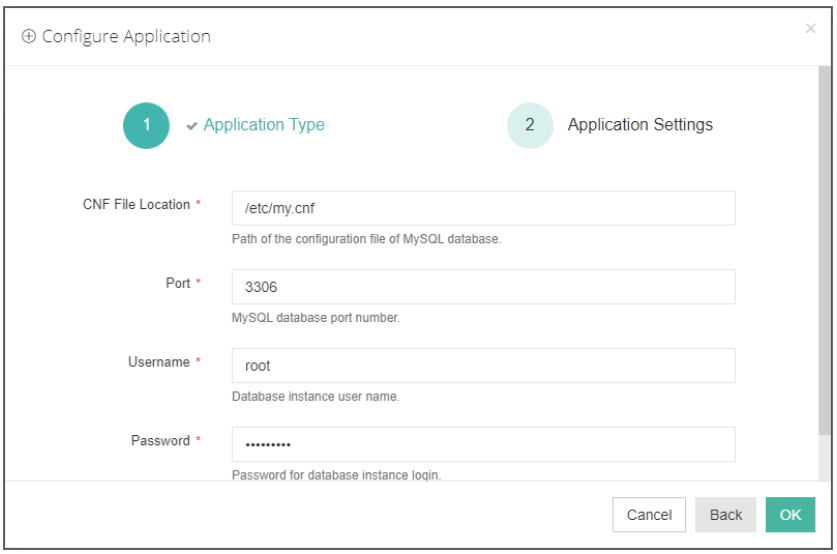
After the installation of Vinchin physical backup agent on MySQL database server, users have to license the agent with database backup module.

When done installation and licensing, please open Vinchin Backup Server web console and go to **Resources** > **Agents** page, find the target agent, click on **Options** and then select **Application** to configure application settings for database backup.

Click on **Configure Application** button to configure the application settings.

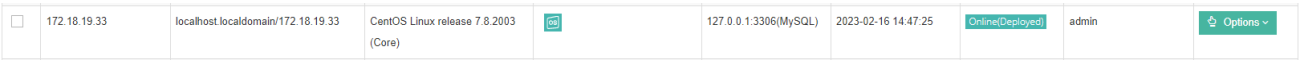
In the **Application Type** dropdown list, please select **MySQL** and then click on **Next**.

In the Applications Settings screen, please configure the following settings.



In the **CNF File Location** field, please type in the file path of MySQL cnf file. Leave the Port number with default value and provide database administrator username and password, click on OK to complete the application configuration.

When MySQL application is successfully configured, in the agents list, you should see the agent look like below.

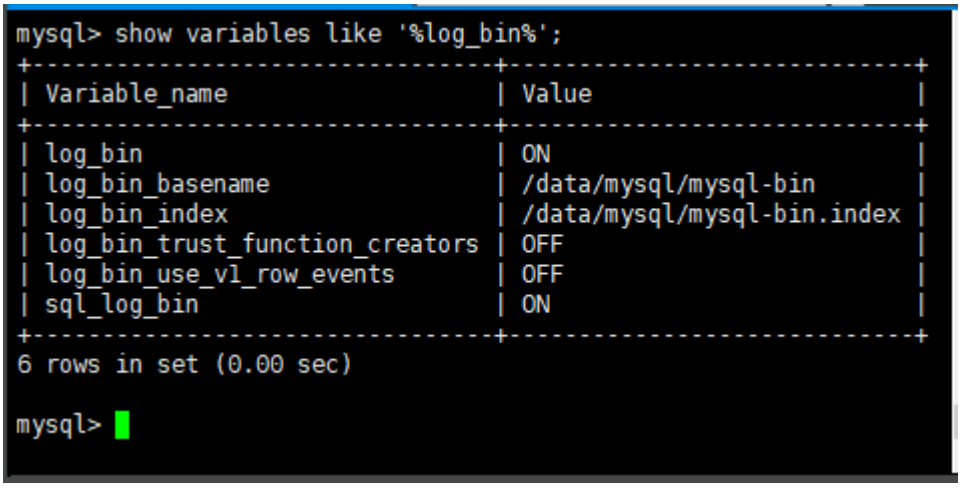


Now you should be able to create backup jobs for the MySQL database server.

If you want to run MySQL log backup, MySQL database needs binary logging enabled. You can check with below command from MySQL database command line interface.

```
show variables like '%log_bin%';
```

If you got log_bin value as on, which means binary logging is enabled.

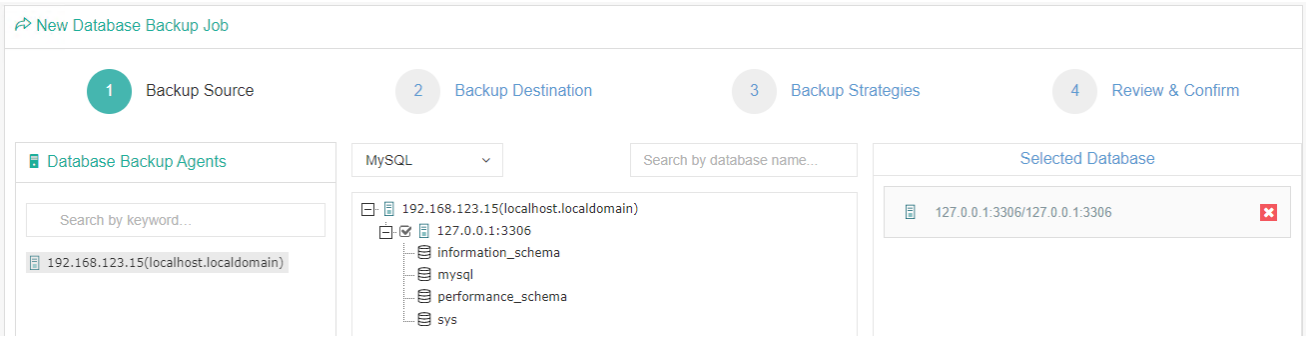


If binary logging is not enabled, it needs the database administrator to enable it.

Create MySQL Backup Job

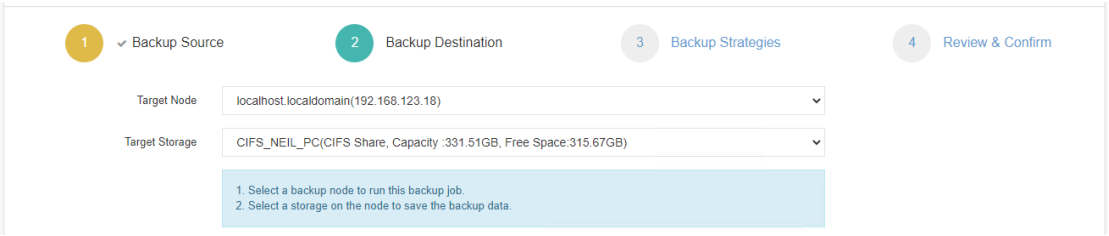
Step 1: Backup Source

First select backup source from left column, then select MySQL database instance you wish to backup, in the right column will show which instance you selected, click on next to step 2.



Step 2: Backup Destination

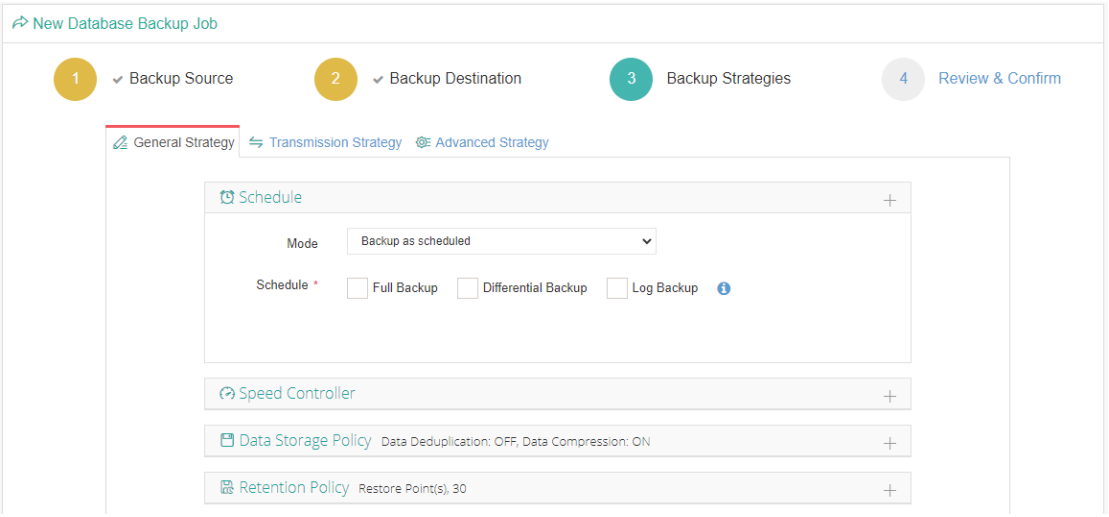
A backup destination (backup storage) should be associated with this backup job.



In the **Target Node** dropdown list, you can select a backup node on which you want the backup data to be processed and stored.
In the **Target Storage** dropdown list, the storages belong to the selected backup node can be selected.

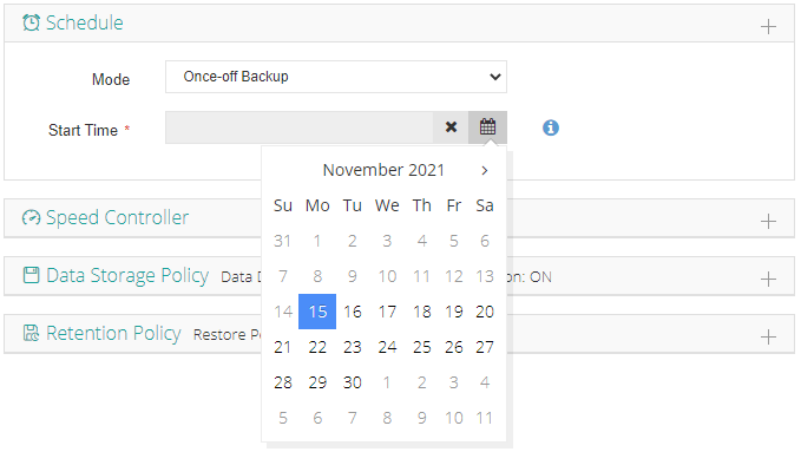
Step 3: Backup Strategies

In the General Strategy it including Schedule, Speed Controller, Data Storage Policy and Retention Policy.



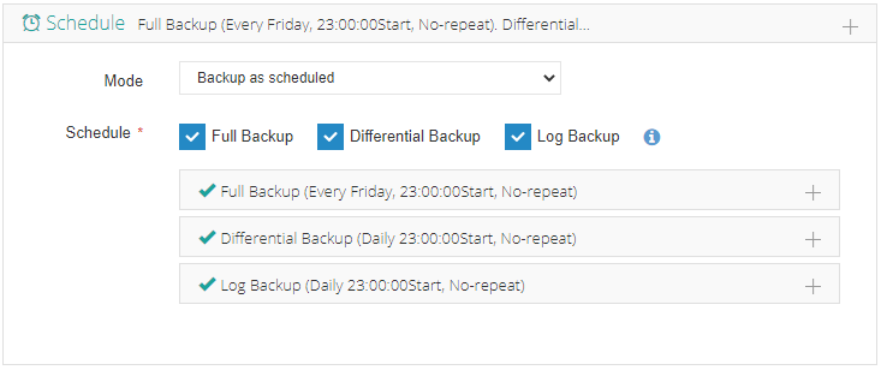
In the Schedule field, you can configure the time schedule of the backup job, you can configure the job as a **Backup as Scheduled** job or a **Once-off Backup** job.

For a once-off backup job, the job will only run for once, and only full backup will be performed. You only have to appoint a time of when to start the backup job, in the Time Schedule field.



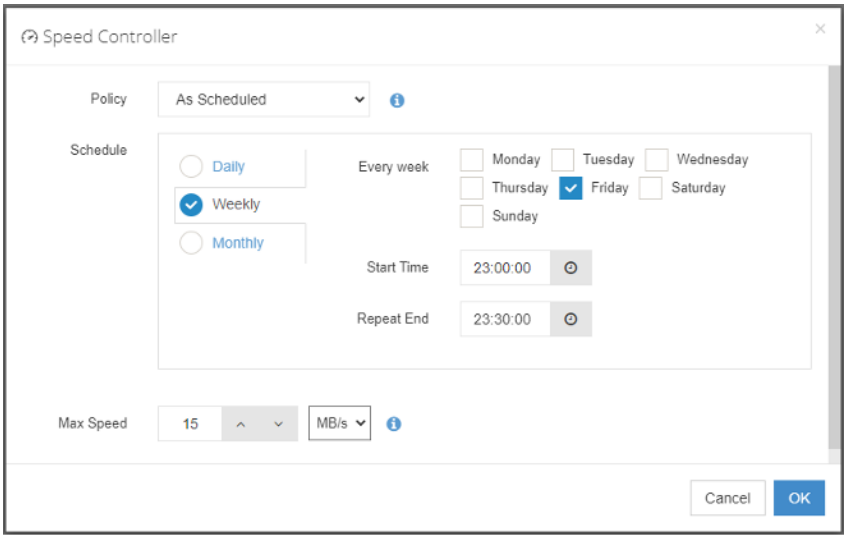
For backup job type, you can schedule Full Backup, Incremental Backup and Log Backup.

Here we take these three Backup as an Example. Please set the backup mode and backup schedule as per your actual demands, then please click on **Next** to continue.



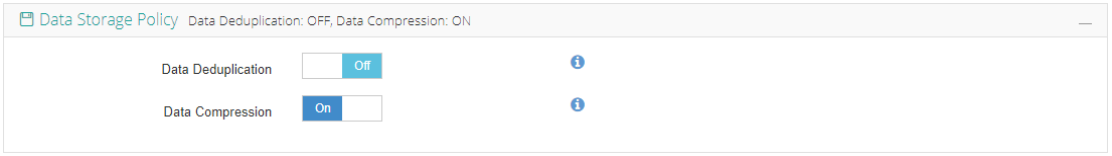
Speed Controller is optional. It can be used to limit the transmission speed during database backup if needed.

The speed controller policy can be configured as either As Scheduled or Permanent. An As Scheduled policy can be configured to limit the backup speed on Daily, Weekly and Monthly basis.



A Permanent policy will always limit the backup speed within the specified Max Speed.

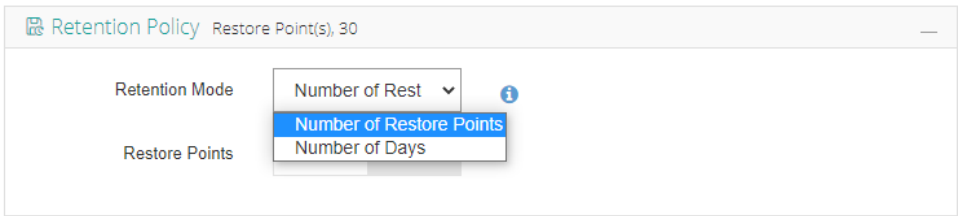
There are 2 options in Data Storage Policy section, Data Deduplication and Data Compression. By enabling these 2 options, the backup data will be deduplicated and compressed before saving into backup storage.



For the retention policy of the database backup, there are 2 retention mode, retain the database backups according to **Number of Restore Points** or **Number of Days**.

For the retention mode **Number of Restore Points**, the restore points will be counted by full restore points, including the incremental backups and log backups dependent on this full backup.

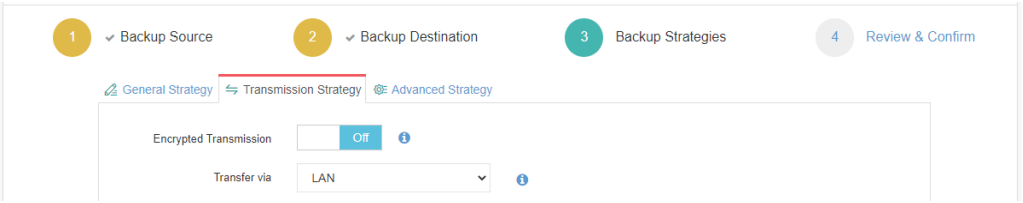
For retention mode **Number of Days**, Vinchin Backup Server will save the restore points within the specified number of days.



When the retention policy is triggered, the outdated restore points will be purged to comply with the retention policy.

In the transmission Strategy, you can choose to enable **Encrypted Transmission** for data safety.

The backup data will be transferred through LAN by default.



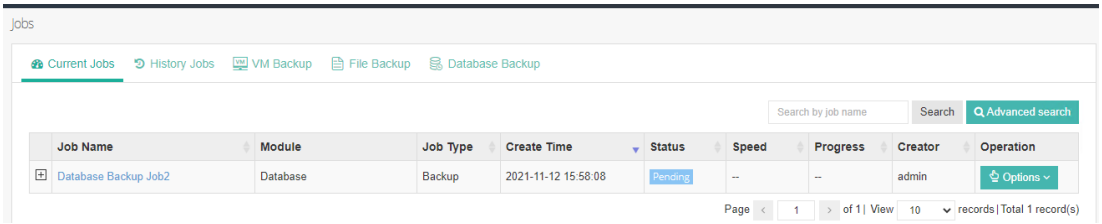
Step 4: Review & Confirm

After completing the above-mentioned settings, you are able to review and confirm the settings in one screen.

A job name can be specified for identification of the database backup job, and by clicking on the Submit button to create the backup job.

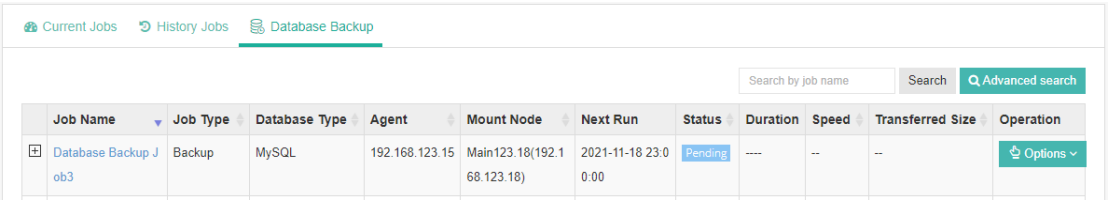
MySQL Backup Job Management

Once a database backup job had been created, you will be redirected to the **Monitor Center** > **Jobs** page.



The status of the newly created job will usually be **Pending**, when the time condition matches the schedule, it will automatically run. And the status will change to Running, you can also see the transfer speed here within the job list.

Besides the Current Job list, there's a dedicated tab to show database backup jobs. More detailed information of database backup jobs, including database type, database agent info, backup node, next run time and some more detailed information dedicated for database backup will be given.



By clicking on the job name you can check more detailed information on the **Job Detail** page.

For a scheduled backup job, after running one of the schedules, the status will change to Pending again and then wait for the next run.

For a once-off backup job, after running the job for once, it will be removed from the Current Job list. And you can find it from the History Job list.

Create MySQL Restore Job

There are two methods to recover MySQL database, **Override Original Database** and **Redirect Restore to New Path**. For **Override Original Database** restore, MySQL database needs to be shutdown. For example:

```
systemctl stop mysqld
```

And an empty temporary directory needs to be created and should be granted with mysql user permission for storing cache data during restoration process. For example:

```
mkdir /data
chown -R mysql:mysql /data
```

All data in the original data directory (datadir) needs to be cleared before restoration, it's recommended to rename the original data directory and create a new directory with the original data directory name, and it needs to be granted with mysql user permission, for example:

```
cd /var/lib/
mv mysql mysql.bk
mkdir mysql
chown -R mysql:mysql mysql
```

Notice

1. The above operations should be done by the MySQL database admin.

2. The temporary directory is recommended to be created on the same partition as original data directory.

2. For the datadir, it's configured in the my.cnf file, database admin should perform the above operations according to the actual environment.

For **Redirect Restore to New Path**, a temporary directory and a new data directory need to be created and need to be granted with mysql user permissions, for example:

```
mkdir /data
chown -R mysql:mysql /data
mkdir /data1
chown -R mysql:mysql /data1
```

Notice

1. Redirect Restore to New Path does not require shutdown MySQL database services.

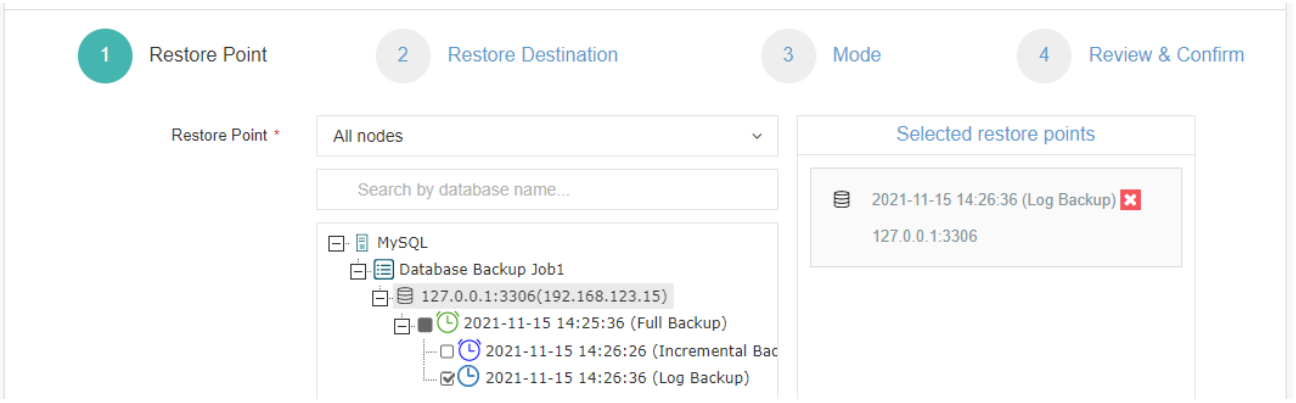
2. The restored data will be saved in the new data directory, database admin can use the restored data to create new database or modify the my.cnf file to start MySQL database from the new data directory.

To restore databases from database backup restore points, please go to **Database Backup** > **Restore** page. There are 4 steps to restore databases from the database backup restore points.

Step 1: Restore Point

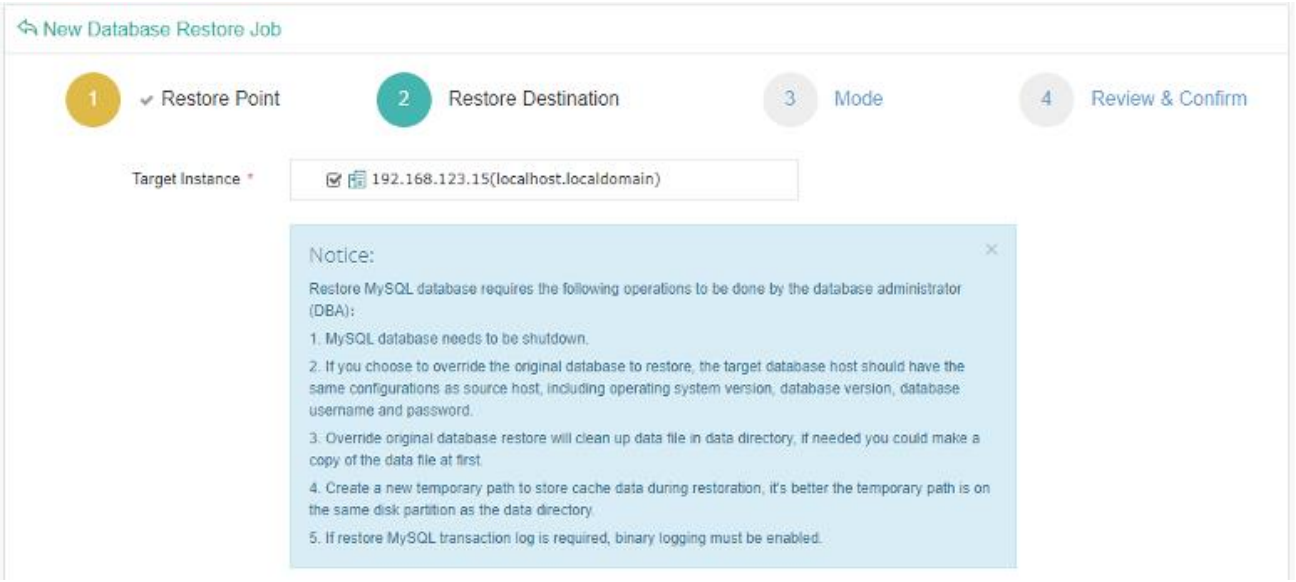
In the Restore Point dropdown list, select a backup node which stores the desired restore points.

Select a target database restore point under your database which you want to restore. You can quickly find the target restore point by searching the job name, database name or the date of the restore point. One restore job only can select one restore point.



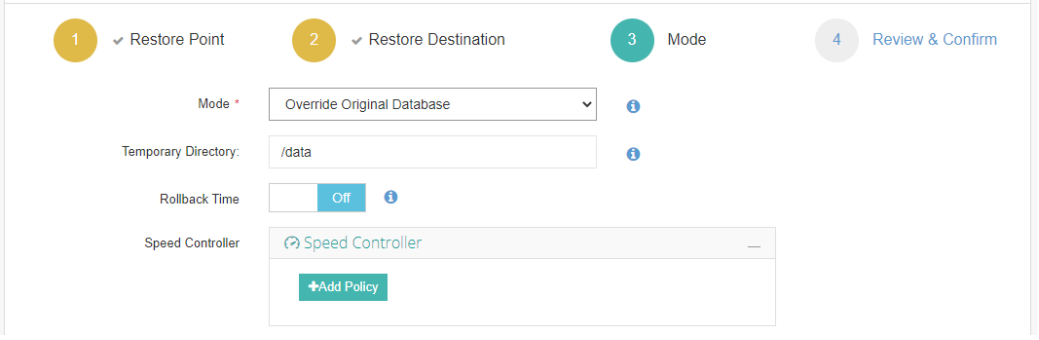
Step 2: Restore Destination

After selecting restore point, select **Target Instance** to restore.

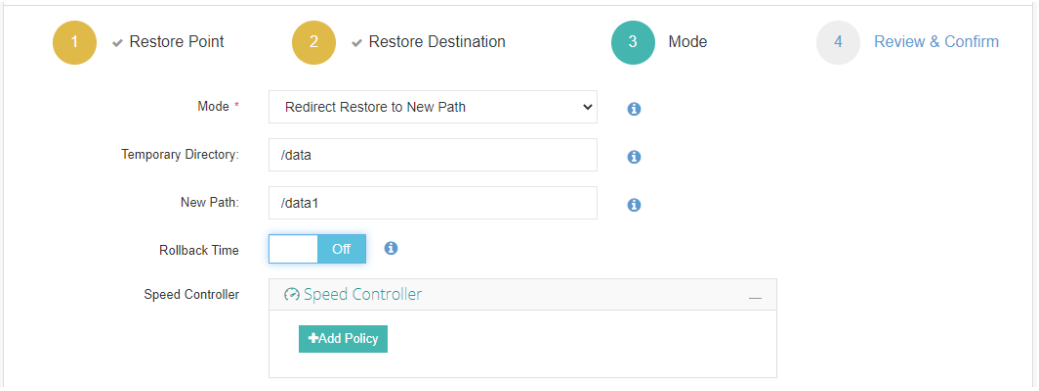


Step 3: Restore Strategy

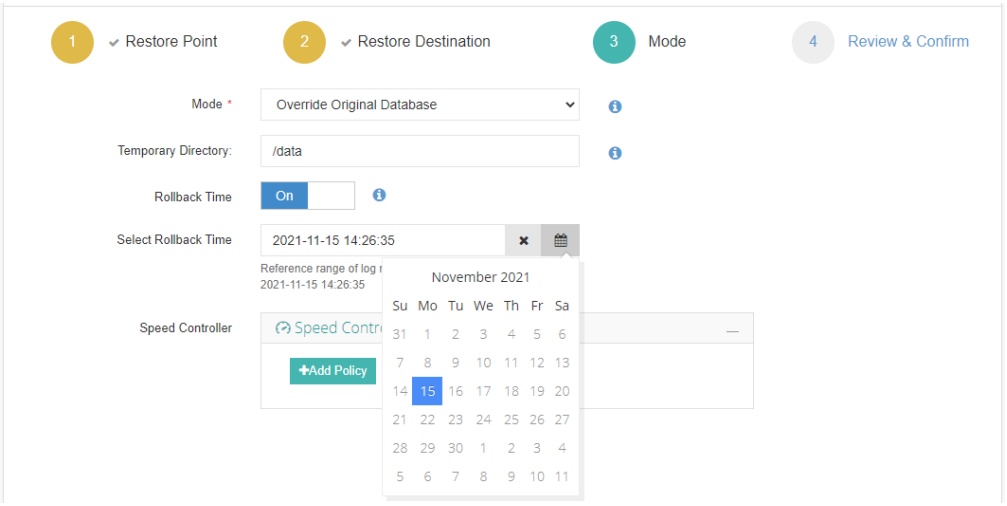
For **Override Original Database** restore, fill in the temporary directory path.



For **Redirect Restore the New Path** restore, fill in the temporary directory path and the new data directory path.



Rollback time: if you had selected log backup restore point, you are able to rollback MySQL database state within the given time range.



If you disable rollback time it will by default restore to the latest time point of the backup when it's been taken.
Same as database backup, while restoring databases, you can also configure **Speed Controller** to limit the database restore speed accordingly.

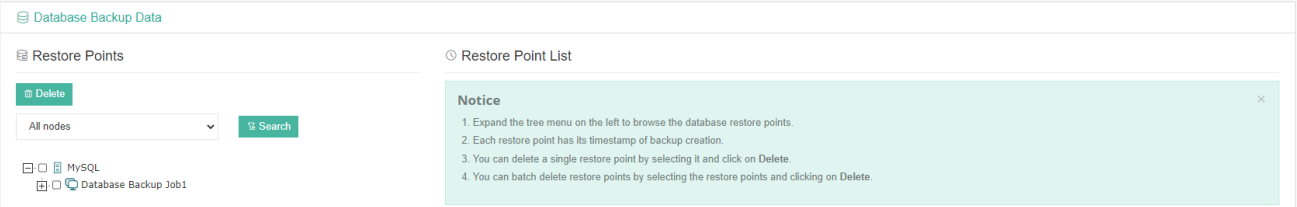
Step 4: Review&Confirm

After completing the above-mentioned settings, you are able to review and confirm the settings in one screen.
Once the job has been created, you'll be redirected to the **Monitor Center** > **Jobs** page.
As the database restore job is by default to be executed right after the creation of the job, so it will run automatically, when you see it in the current job list, it should be in running status already, and once completed, the job will be automatically deleted from the current job list.
After this you can browse the restored job from History Jobs. Your restored data will be found in the path you configured during creating the restore job.

Notice
If you use log backup point to override original database, MySQL service will auto restart, no need to manually start MySQL service.

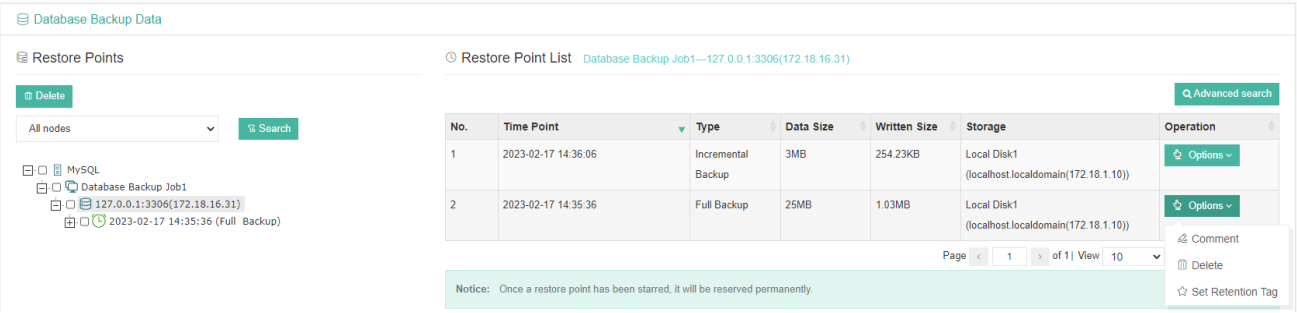
MySQL Backup Data

The database backup data can be managed from **Physical Backup** > **Database Backup** > **Backup Data** page.



If you want to delete a restore point or multiple restore points, you can first select target restore point(s) from the left tree view, and click on the **Delete** button. The incremental backup and log backup cannot be deleted individually, they will be deleted along with the dependent full backup.

When deleting backup data, you need to provide your login password to confirm the deletion, once deleted the data will be unrecoverable.



For the restore point list in the right column, you need to select a database in the left tree menu to view all restore points of the selected database. Information like backup type, data size, written backup size and storage will be given.

You can add comments to the full backups, incremental backups and the log backups, and set retention tags for the full restore point to keep the full backup and its dependent incremental and log backups to not be deleted by retention policy.

A full restore point can be also deleted from the Restore Point List by clicking on Options and then select Delete, the dependent incremental and log backups will be deleted along with the full restore point.

Oracle Database Backup

Preparation for Oracle Backup

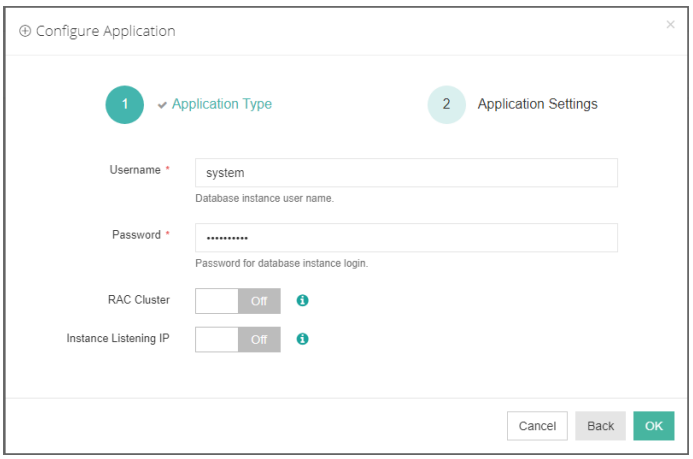
After the installation of Vinchin physical backup agent on Oracle database server, users have to license the agent with database backup module.

When done installation and licensing, please open Vinchin Backup Server web console and go to **Resources** > **Agents** page, find the target agent, click on **Options** and then select **Application** to configure application settings for database backup.

Click on **Configure Application** button to configure the application settings.

In the **Application Type** dropdown list, please select **Oracle**.

The database instances of Oracle will be listed in the **Select Instance** field. For standalone Oracle database server, select the database instance and click on **Next** button to get the instance authenticated for backup.



It's recommended to grant sysdba permission to the system user, then use system user to backup Oracle database.

The user to be used to backup Oracle database must have dba and sysdba permissions. You can login to oracle database use below commands to check user permissions.

Check if GRANTED_ROLE = DBA by using command:

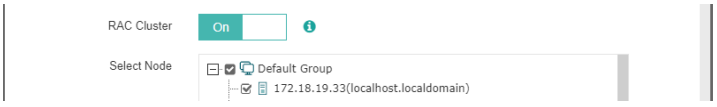
```
select * from dba_role_privs where grantee='username';
```

Check if SYSDBA = TRUE by using command:

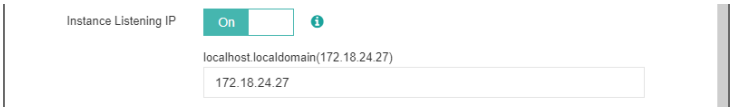
```
select * from v$pwfile_users where username='username';
```

For RAC cluster, database backup agent needs to be installed on each of the cluster nodes, then add all nodes (backup agents) to Vinchin backup server.

To enable RAC cluster, turn the **RAC Cluster** option on, and in the **Select Node** field, select all the other nodes of the RAC cluster.

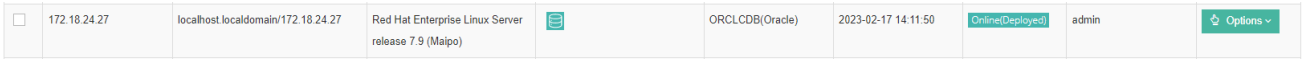


For the **Instance Listening IP**, if the backup server or the database server is on the Internet, this option needs to be turned on.



The IP address of the database instance where the agent is installed must be provided here. When done the above settings, click on **OK**.

When Oracle application is successfully configured, in the agents list, you should see the agent look like below.



Now you should be able to create backup jobs for the Oracle database server.

Notice

1. If database server is Linux, the database backup agent needs to use 2 service ports: 23100 and 23101. On the database server firewall, these 2 ports need to be opened for Vinchin backup server.

2. To add RAC Cluster, database backup agent needs to be installed on all the cluster nodes, and all nodes (agents) need to be added to Vinchin.

3. Choose one Oracle database agent to do Instance Authentication for the RAC cluster.

4. To back up the Oracle RAC cluster environment, run the show all command on the RMAN command line to check whether the control file snapshot is set to the shared storage.

5. Only one backup job needs to be created for one of the RAC cluster node.

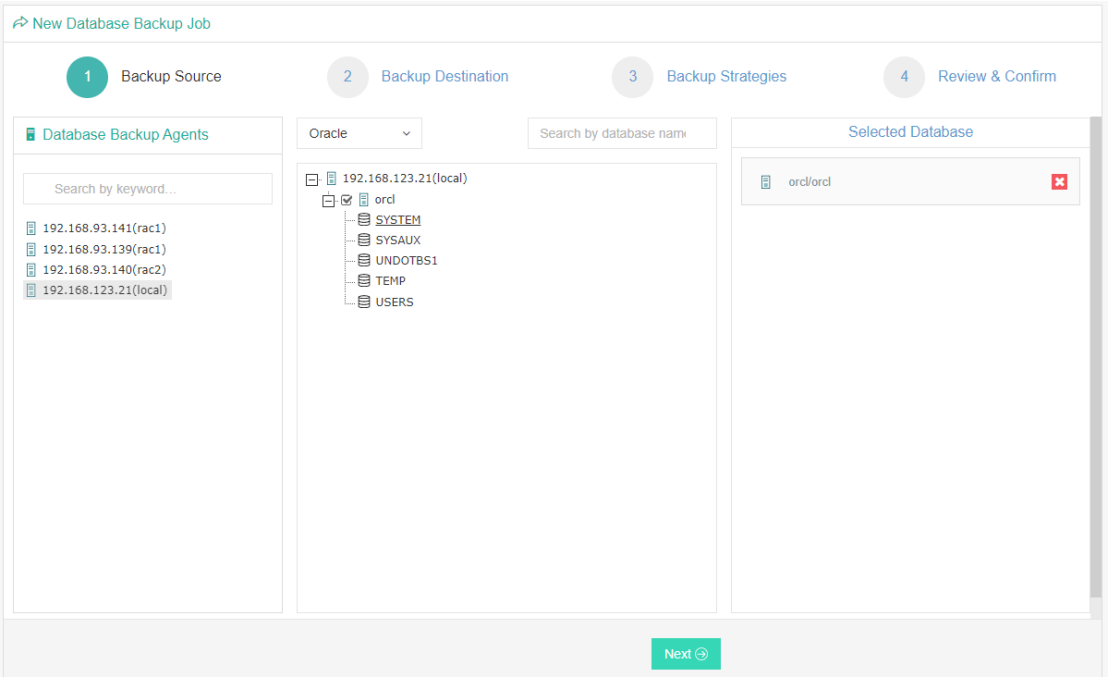
6. If one or some of the RAC cluster node fail, backup will be performed on other node, there's no need to modify the backup job under such situation.

7. Archivelog mode needs to be enabled with the database instance before taking backups.

Create Oracle Backup Job

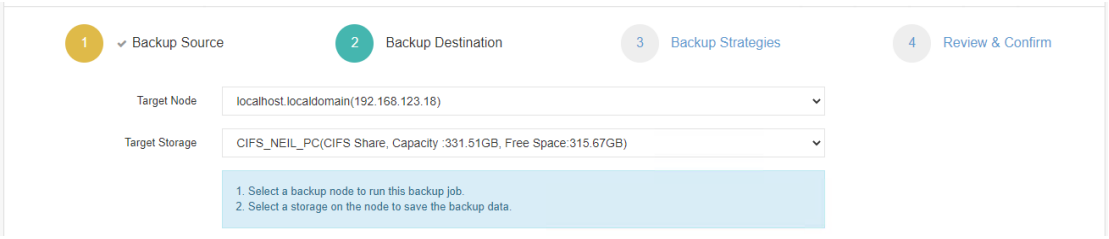
Step 1: Backup Source

First you need to select a target host from the left column, then select Oracle database instance you wish to backup, in the right column will show the instance you select. Click on next to step 2.



Step 2: Backup Destination

A backup destination (backup storage) should be associated with this backup job.

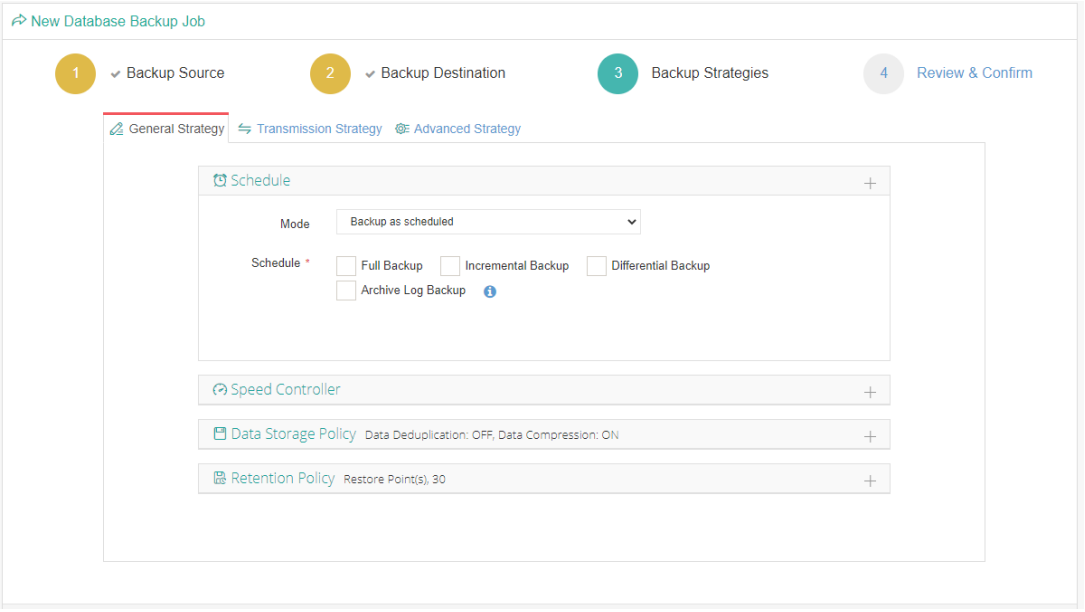


In the **Target Node** dropdown list, you can select a backup node on which you want the backup data to be processed and stored.

In the **Target Storage** dropdown list, the storages belong to the selected backup node can be selected.

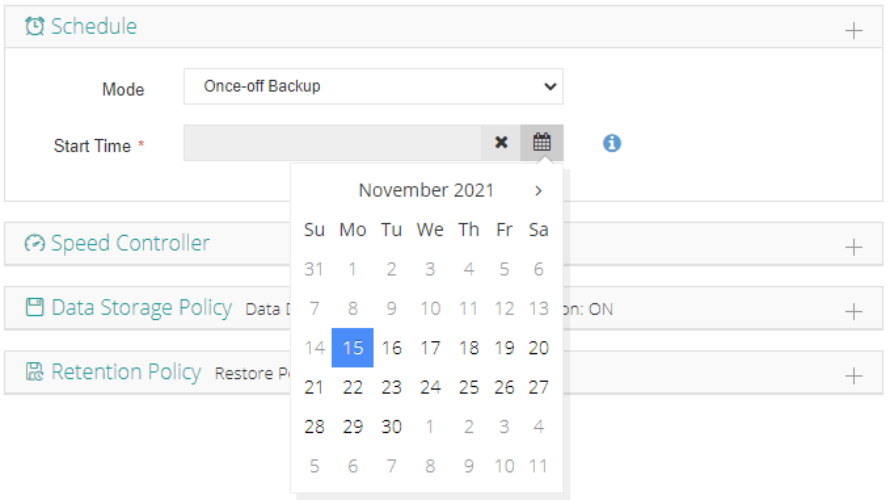
Step 3: Backup Strategies

In the General Strategy it including Schedule, Speed Controller, Data Storage Policy and Retention Policy.

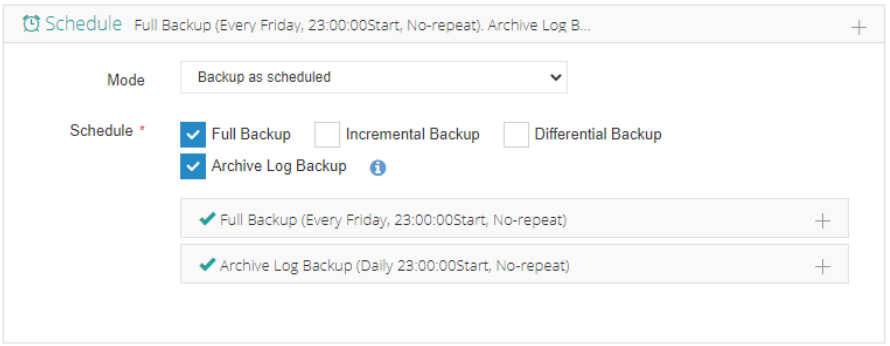


In the Schedule field, you can configure the time schedule of the backup job, you can configure the job as a **Backup as Scheduled** job or a **Once-off Backup** job.

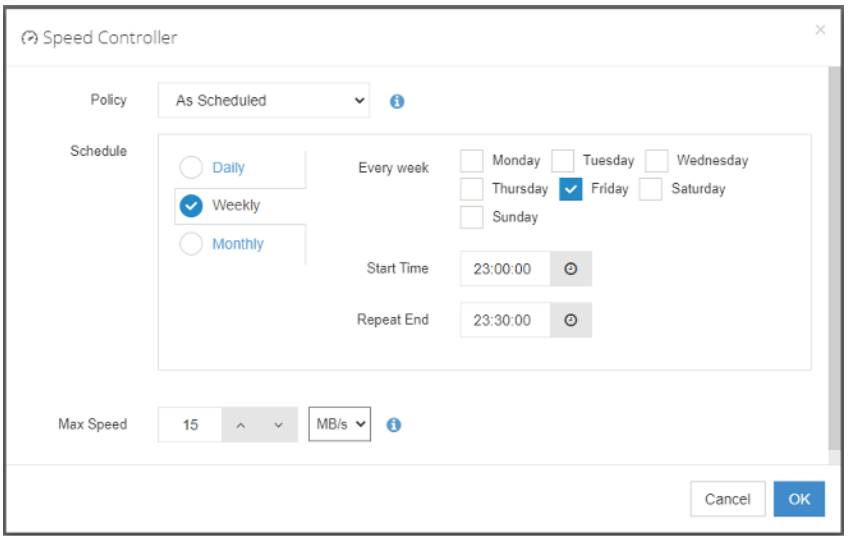
For a once-off backup job, the job will only run for once, and only full backup will be performed. You only have to appoint a time of when to start the backup job, in the Start Time field.



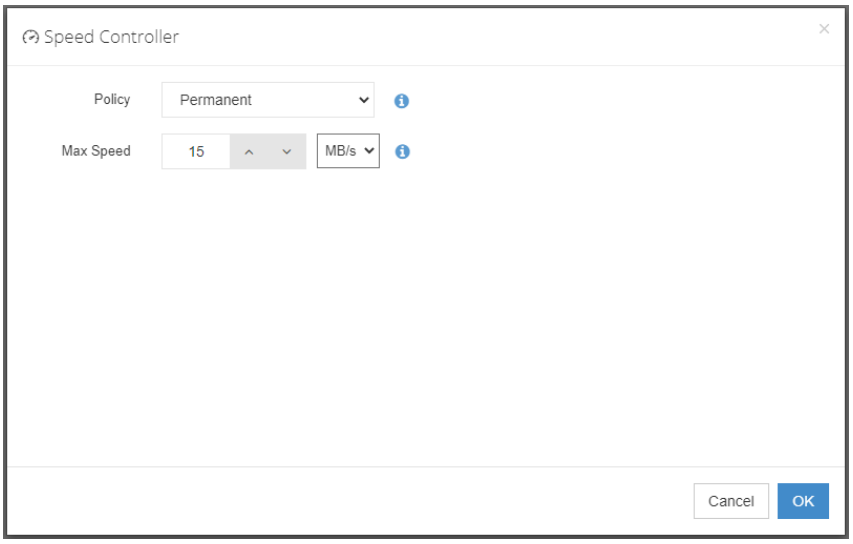
For backup job type, you can schedule Full Backup, Incremental Backup, Differential Backup and Archive Log Backup. For Oracle database must have **Full Backup** and **Archive Log Backup**. Please set the backup mode and backup schedule as per your actual demands, then please click on **Next** to continue.



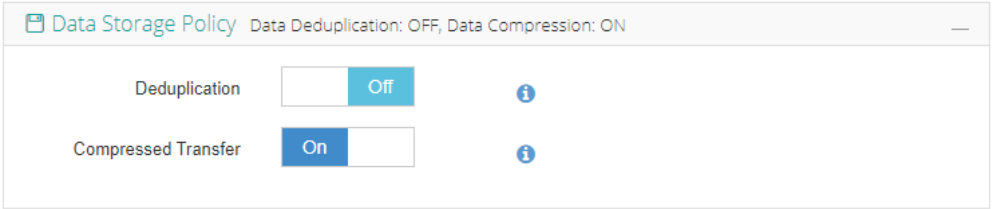
Speed Controller is optional. It can be used to limit the transmission speed during database backup if needed.
The speed controller policy can be configured as either As Scheduled or Permanent. An As Scheduled policy can be configured to limit the backup speed on Daily, Weekly and Monthly basis.



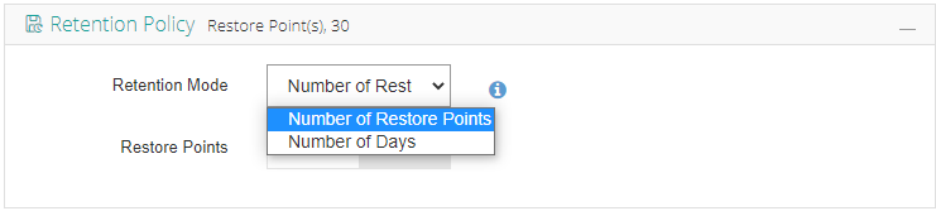
A Permanent policy will always limit the backup speed within the specified Max Speed.



There are 2 options in Data Storage Policy section, Data Deduplication and Data Compression. By enabling these 2 options, the backup data will be deduplicated and compressed before saving into backup storage.



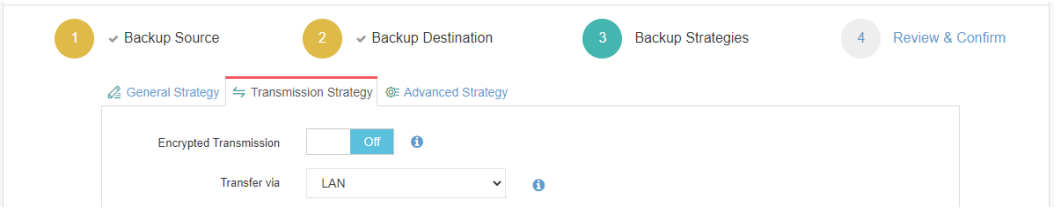
For the retention policy of the database backup, there are 2 retention mode, retain the database backups according to **Number of Restore Points** or **Number of Days**.
For the retention mode **Number of Restore Points**, the restore points will be counted by full restore points, including the differential backups and log backups dependent on this full backup.
For retention mode **Number of Days**, Vinchin Backup Server will save the restore points within the specified number of days.



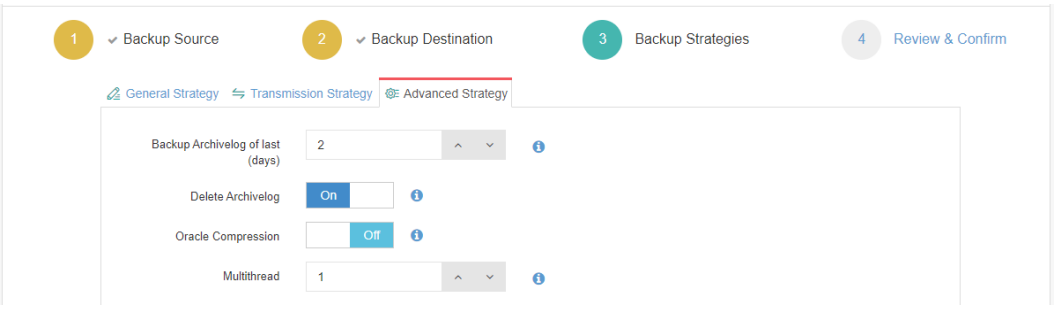
When the retention policy is triggered, the outdated restore points will be purged to comply with the retention policy.

In the transmission Strategy, you can choose to enable **Encrypted Transmission** for data safety.

The backup data will be transferred through LAN by default.



Advanced Strategy allows you to configure Backup Archivelog of last (days), Delete Archivelog, Oracle Compression and Multithreaded transmission.



Backup archivelog of last(days): The default value of the recent archivinglog days is associated with the frequency of archiving log backup set in the schedule policy. e.g. if Archive Log Backup set to Daily, default is 2 days. If Archive Log backup set to every week, default is 8 days. If Archive Log Backup set to Monthly, default is 31.

Delete Archivelog: enabled delete archivelog can delete backed up archivelog file from database server, reclaim archive space from the database server. If disabled this option, database admin needs manually delete archivelog files.

Oracle Compression: provide by Oracle to reduce data transfer, data backup time and save backup storage, disabled by default.

Multithread: backup data will be transferred over multiple channels to improve the backup speed. The default value is 1, and the maximum value is 6.

Notice

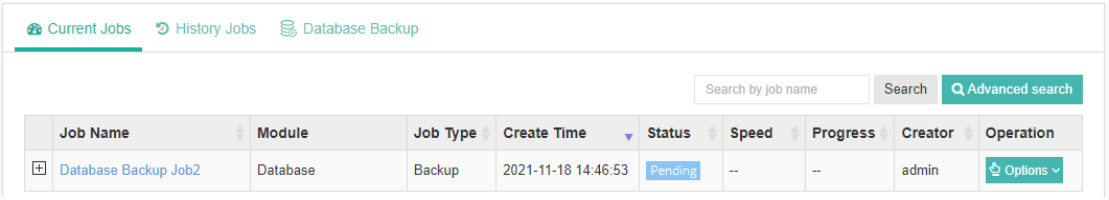
If Delete Archivelog is disabled, DBA must manually delete archivelog files regularly, otherwise, production database crash may occur once space is fulfilled with archive log files. It is recommended to enable this function.

Step 4: Review & Confirm

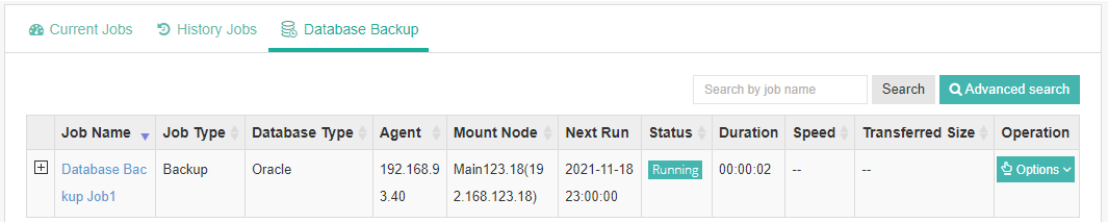
After completing the above mentioned settings, you are able to review and confirm the settings in one screen.
A job name can be specified for identification of the database backup jobs, and by clicking on the Submit button to confirm the creation of the backup job.

Oracle Backup Job Management

Once a database backup job had been created, you will be redirected to the **Monitor Center** > **Jobs** page.



The status of the newly created job will usually be **Pending**, when the time condition matches the schedule, it will automatically run. And the status will change to Running, you can also see the transfer speed here within the job list.
Besides the Current Job list, there's a dedicated tab to show database backup jobs. More detailed information of database backup jobs, including database type, database agent info, backup node, next run time and some more detailed information dedicated for database backup will be given.



By clicking on the job name you can check more detailed information on the **Job Detail** page.
For a scheduled backup job, after running one of the schedules, the status will change to Pending again and then wait for the next run.
For a once-off backup job, after running the job for once, it will be removed from the Current Job list. And you can find it from the History Job list.

Create Oracle Restore Job

Before starting to restore Oracle database, there are some configurations need DBA to check.
Target recovery database server needs database backup agent installed, and if it's Linux system, the service ports: 23100 and 23101 need to be opened to Vinchin backup server.
Target Oracle database instance needs to be shutdown, and static listener registration needs to be configured in listener.ora file.
Archivelog mode needs to be enabled with the target Oracle database server. You can check status by login to sqlplus and using below command.

```
archivelog list;
```

Check if **Automatic archival** status is **Enabled**, if not please configure this by DBA.

Check whether the database instance can be connected by using below command. In standalone environment.

```
rman target=username/password@instancename
```

In RAC cluster, use below command.

```
rman target=username/password@publicIP:1521/instancename
```

If connection fails, the restore job will fail, please contact DBA to fix it.

If **Override Original Database** restore to another database server, it requires the target database server configurations should be the same as the source database server, including operating system, database version, installation path and instance name. Please be careful to use override original database function.

If **Restore to New Path**, the database path will be automatically changed to the new path specified during the restore process. After restoration, DBA can just start the database services directly from the new path.

Notice

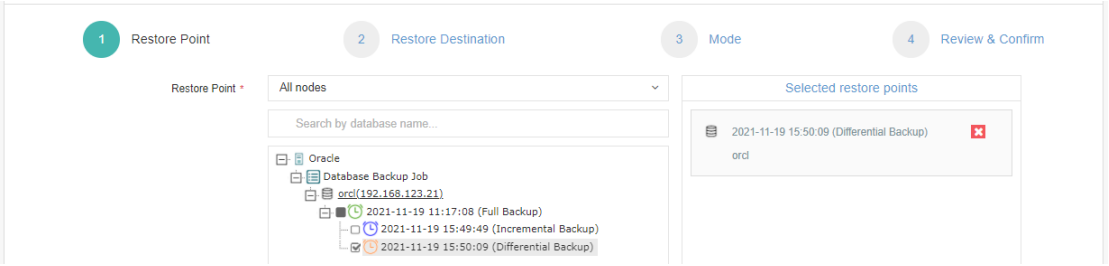
Restore to New Path does not work with Oracle RAC, because the database path will only change on the RAC node which the restore job is associated to, other nodes will not be changed. If you use Restore to New Path with Oracle RAC, it will cause Oracle RAC exception!

To restore databases from database backup restore points, please go to **Physical Backup** > **Database Backup** > **Restore** page. There are 4 steps to restore databases from the database backup restore points.

Step 1: Restore Point

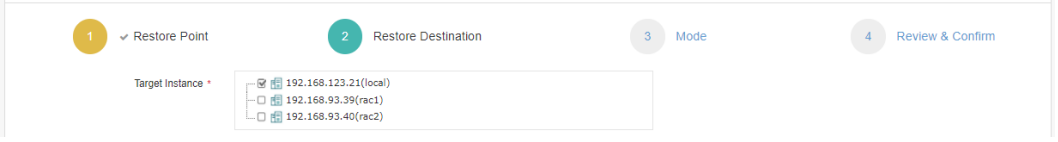
In the Restore Point dropdown list, select a backup node which stores the desired restore points.

Select a target database restore point under your database which you want to restore. You can quickly find the target restore point by searching the job name, database name or the date of the restore point. One restore job only can select one restore point.



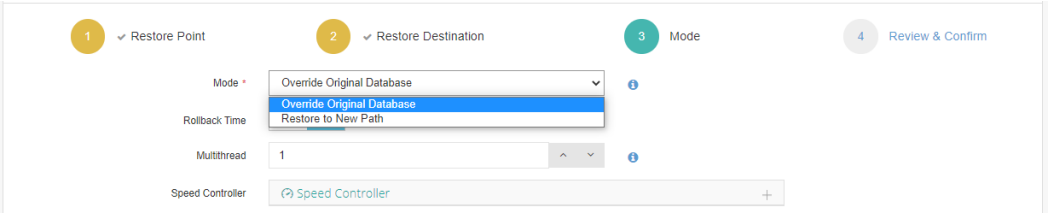
Step 2: Restore Destination

After selecting restore point, select **Target Instance** which you wish to restore.

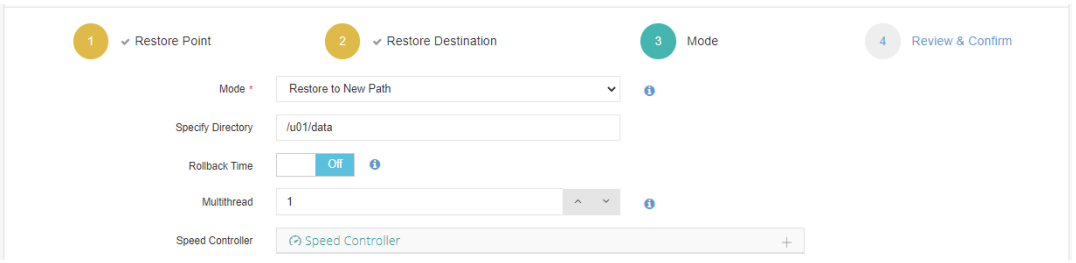


Step 3: Restore Strategy

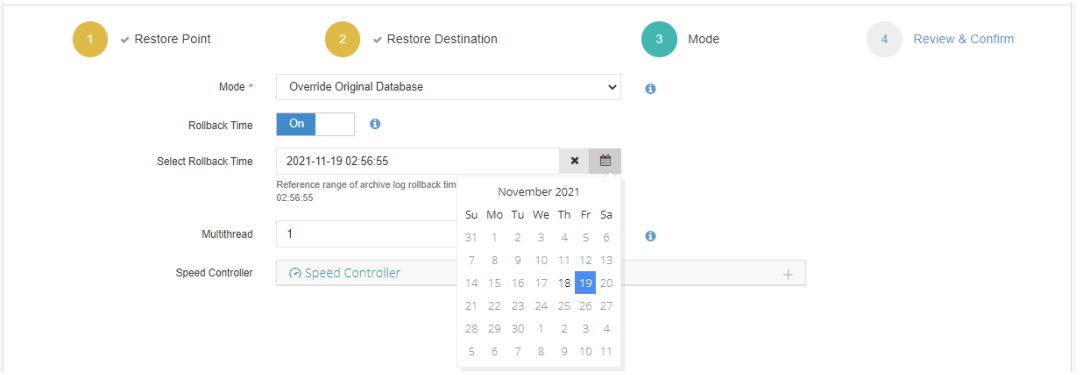
Mode: Override Original Database applies to restore the data to the production database server. Override the data of the original database instance.



Restore to New Path applies to restore data to a new directory. The directory needs to be created by the Oracle database installation user, do not use a directory which does not exist.



Rollback Time: if you had selected archive log backup restore point, you are able to rollback Oracle database state within the given time range.



If you disable rollback time it will by default restore to the latest time point of when the backup has been taken.

Multithread: backup data will be transferred over multiple channels to improve the restore speed. The default value is 1, and the maximum value is 6.

Speed Controller: Same as database backup, while restoring databases, you can also configure speed controller to limit the database restore speed accordingly.

Step 4: Review & Confirm

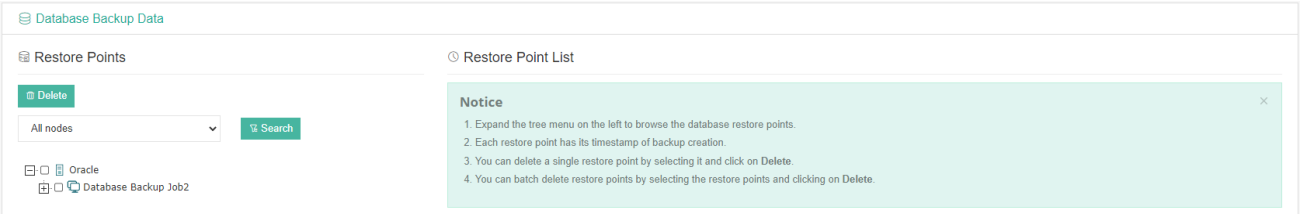
After completing the above-mentioned settings, you are able to review and confirm the settings in one screen. Once the job has been created, you'll be redirected to the **Monitor Center** > **Jobs** page.

As the database restore job is by default to be executed right after the creation of the job, so it will run automatically, when you see it in the current job list, it should be in running status already, and once completed, the job will be automatically deleted from the current job list.

After this you can browse the restored job from History Jobs. Your restored data will be found in the path you selected.

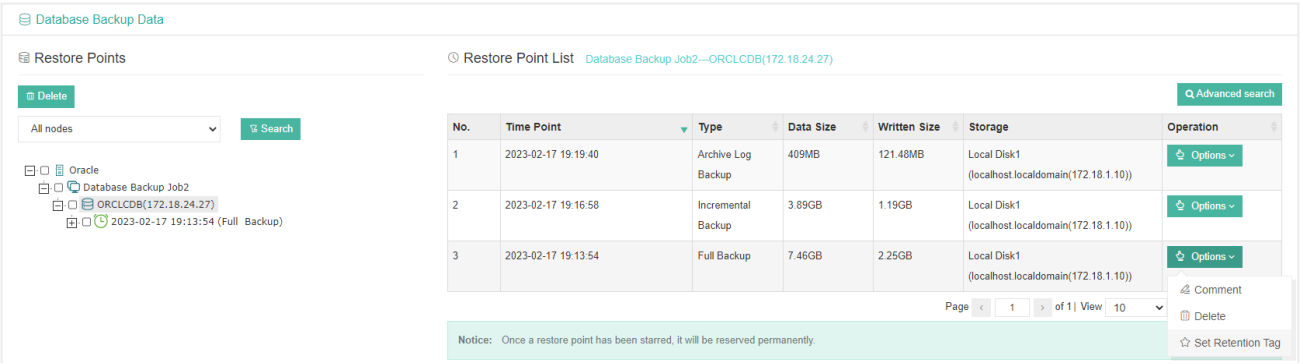
Oracle Backup Data

The database backup data can be managed from **Physical Backup** > **Database Backup** > **Backup Data** page.



If you want to delete a restore point or multiple restore points, you can first select target restore point(s) from the left tree view, and click on the **Delete** button. The incremental, differential and log backup cannot be deleted Independently, they will be deleted along with the dependent full backup.

When deleting backup data, you need to provide your login password to confirm the deletion, once deleted the data will be unrecoverable.



For the restore point list in the right column, you need to select a database in the left tree menu to view all restore points of the selected database. Information like backup type, data size, written backup size and storage will be given.

You can add comments to the full backups, incremental backups, differential backups and the log backups, and set retention tags for the full restore point to keep the full backup and its dependent incremental, differential and log backups to not be deleted by retention policy.

A full restore point can be also deleted from the Restore Point List by clicking on Options and then select Delete, the dependent incremental, differential and log backups will be deleted along with the full restore point.

PostgreSQL Database Backup

Preparation for PostgreSQL Backup

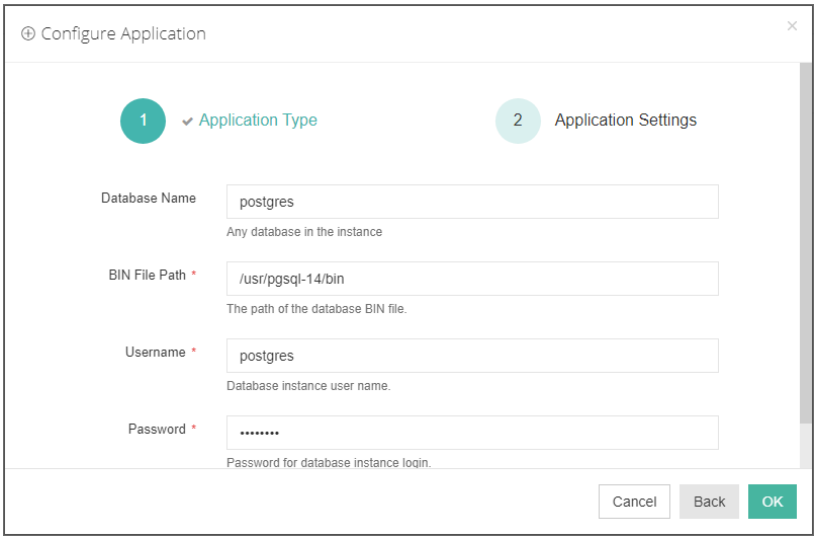
After the installation of Vinchin physical backup agent on PosrgreSQL database server, users have to license the agent with database backup module.

When done installation and licensing, please open Vinchin Backup Server web console and go to **Resources** > **Agents** page, find the target agent, click on **Options** and then select **Application** to configure application settings for database backup.

Click on **Configure Application** button to configure the application settings.

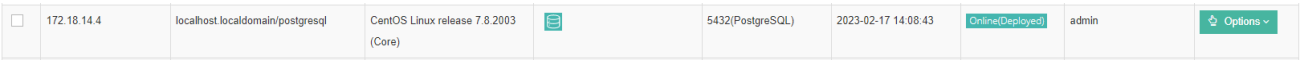
In the **Application Type** dropdown list, please select **PostgreSQL**.

The database instances of PostgreSQL will be listed in the **Select Instance** field. Select the database instance and click on **Next** button to get the instance authenticated for backup.



You need to specify the database bin file path and the database user credentials to get it authenticated.

When PostgreSQL application is successfully configured, in the agents list, you should see the agent look like below.



Now you should be able to create backup jobs for the PostgreSQL database server.

Notice

DBA must check the below prerequisites before taking PostgreSQL database backups.

1. The database backup agent needs to use 2 service ports: 23100 and 23101. On the database server firewall, these 2 ports need to be opened for Vinchin backup server.

2. Archivelog mode needs to be enabled with the database instance before taking backups.

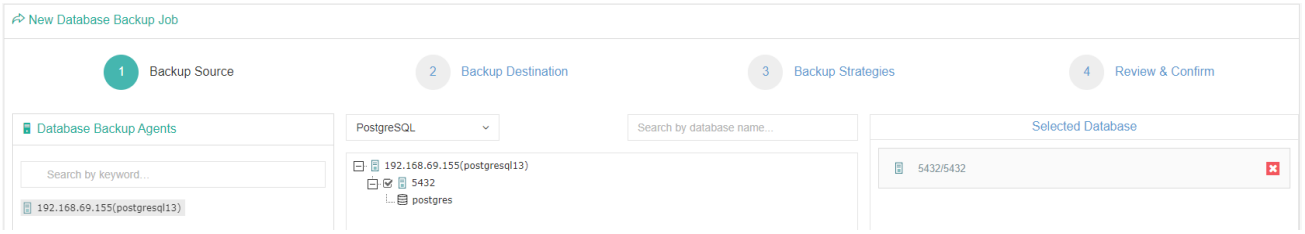
3. The password-based authentication should be “md5” or “scram-sha-256”.

Create PostgreSQL Backup Job

To create database backup jobs, please go to **Database Backup** > **Backup** page. There are 4 steps to create a database backup job.

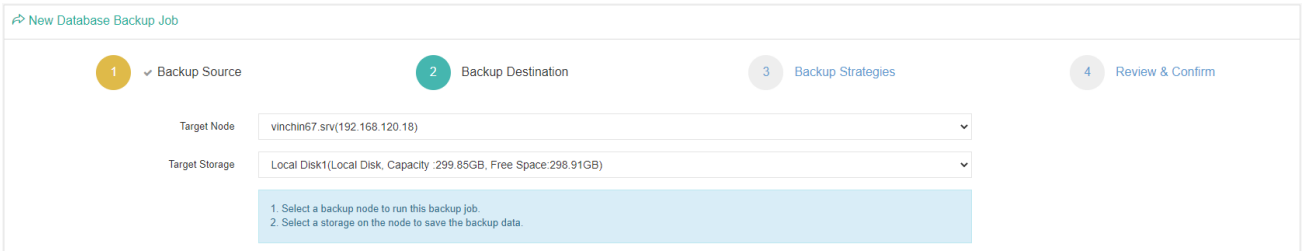
Step 1: Backup Source

First you need to select a target database server from the left column, then select PostgreSQL database instance you wish to backup, in the right column will show the instance you have selected.



Step 2: Backup Destination

A backup destination (backup storage) should be associated with this backup job.

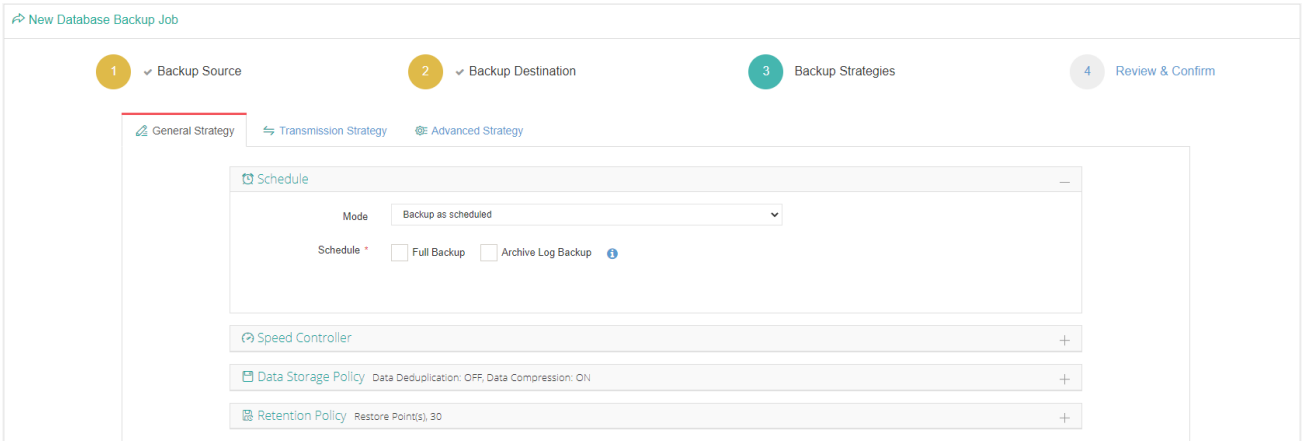


In the **Target Node** dropdown list, you can select a backup node on which you want the backup data to be processed and stored.

In the **Target Storage** dropdown list, the storages belong to the selected backup node can be selected.

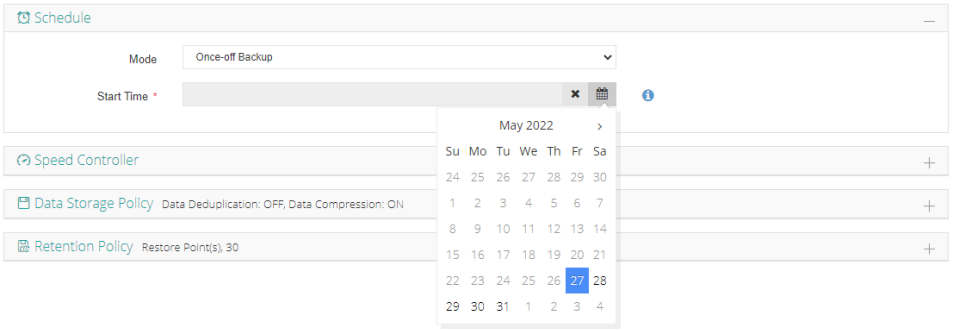
Step 3: Backup Strategies

In the General Strategy it including Schedule, Speed Controller, Data Storage Policy and Retention Policy.



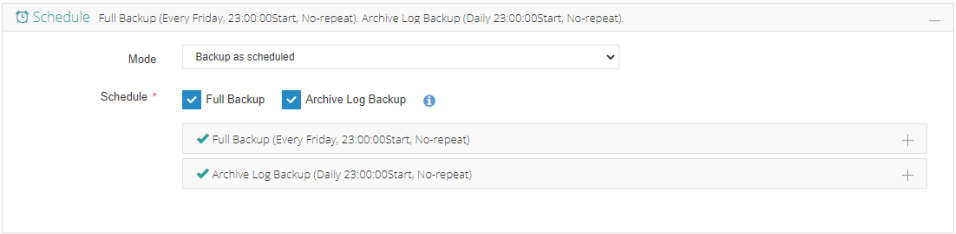
In the Schedule field, you can configure the time schedule of the backup job, you can configure the job as a **Backup as Scheduled** job or a **Once-off Backup** job.

For a once-off backup job, the job will only run for once, and only full backup will be performed. You only have to appoint a time of when to start the backup job, in the Start Time field.



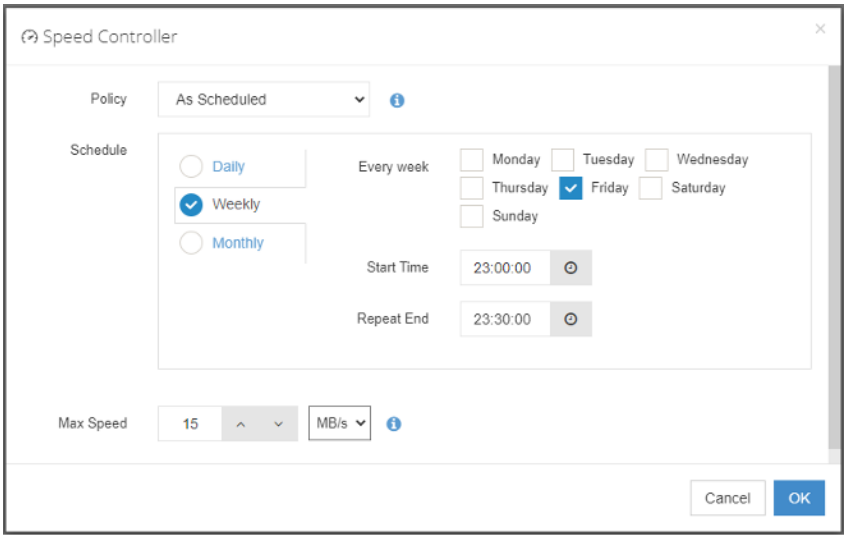
If you want to setup a Backup as Scheduled job, you can schedule Full Backup and Archive Log Backup.

For PostgreSQL database, it is recommended to schedule weekly full backup with daily archive log backup.



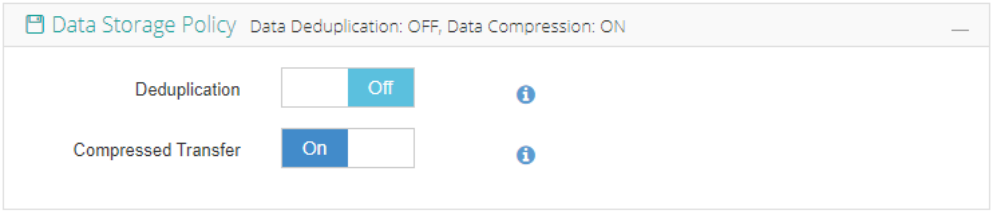
Speed Controller is optional. It can be used to limit the transmission speed during database backup if needed.

The speed controller policy can be configured as either As Scheduled or Permanent. An As Scheduled policy can be configured to limit the backup speed on Daily, Weekly and Monthly basis.



A Permanent policy will always limit the backup speed within the specified Max Speed.

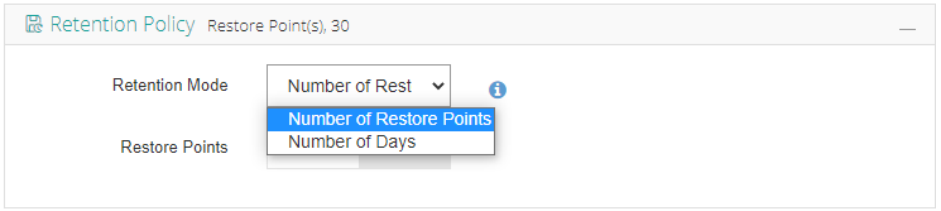
There are 2 options in Data Storage Policy section, Data Deduplication and Data Compression. By enabling these 2 options, the backup data will be deduplicated and compressed before saving into backup storage.



For the retention policy of the database backup, there are 2 retention modes, retain the database backups according to **Number of Restore Points** or **Number of Days**.

For the retention mode **Number of Restore Points**, the restore points will be counted by number of full restore points, including the archive log backups dependent on the corresponding full restore points.

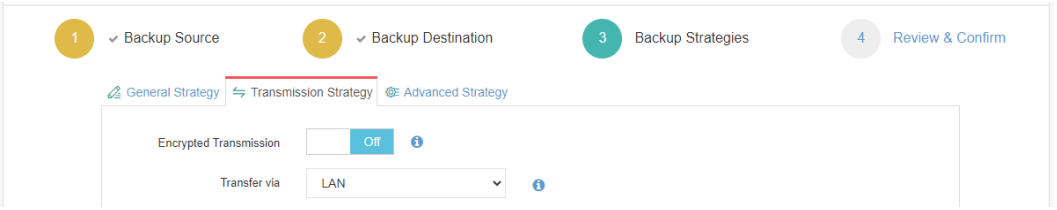
For retention mode **Number of Days**, Vinchin Backup Server will save the restore points within the specified number of days.



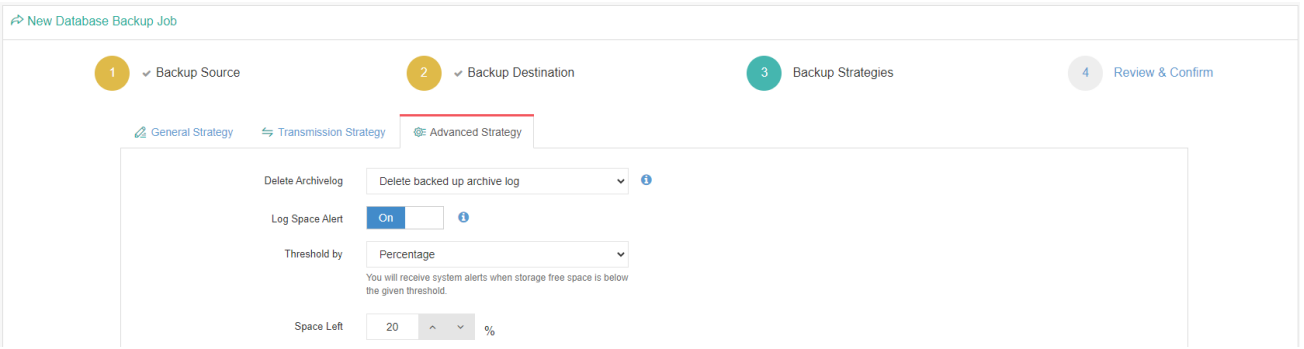
When the retention policy is triggered, the outdated restore points will be purged to comply with the retention policy.

In the transmission Strategy, you can choose to enable **Encrypted Transmission** for data safety.

The backup data will be transferred through LAN by default.



Advanced Strategy allows you to configure archive log deletion and log space monitoring options.



Delete Archivelog: there are 3 options **Delete backup up archive log**, **Do not delete** and **Delete all archive log**. It is recommended to use the Delete backed up archive log option to delete the archive log which had been backed up.

Log Space Alert: if enabled, Vinchin backup server will monitoring on the archive log space usage, when exceeded the specified threshold you will receive alerts on the Vinchin web console.

Notice

If Delete Archivelog has been set to Do not delete, DBA must manually delete archivelog files regularly, otherwise, production database crash may occur once space is fulfilled with archive log files. It is recommended to set Delete Archivelog option to Delete backed up archive log.

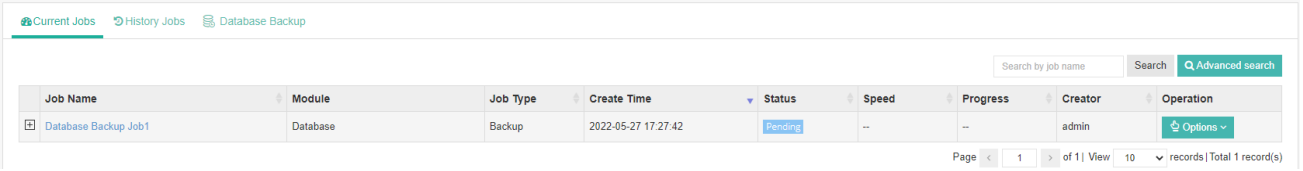
Step 4: Review & Confirm

After completing the above-mentioned settings, you are able to review and confirm the settings in one screen.

A job name can be specified for identification of the database backup jobs, and by clicking on the Submit button to confirm the creation of the backup job.

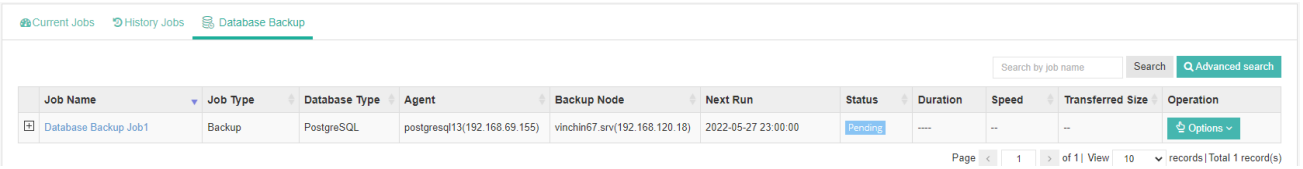
PostgreSQL Backup Job Management

Once a database backup job had been created, you will be redirected to the **Monitor Center** > **Jobs** page.



The status of the newly created job will usually be **Pending**, when the time condition matches the schedule, it will automatically run. And the status will change to Running, you can also see the transfer speed here within the job list.

Besides the Current Job list, there's a dedicated tab to show database backup jobs. More detailed information of database backup jobs, including database type, database agent info, backup node, next run time and some more detailed information dedicated for database backup will be given.



By clicking on the job name you can check more detailed information on the **Job Detail** page.

For a scheduled backup job, after running one of the schedules, the status will change to Pending again and then wait for the next run.

For a once-off backup job, after running the job for once, it will be removed from the **Current Job** list. And you can find it from the **History Job** list.

Create PostgreSQL Restore Job

Vinchin Backup & Recovery supports two recovery mode for PostgreSQL database: **Override Original Database** restore and **Restore to New Path**.

Before starting to restore PostgreSQL database, there are some database configurations need DBA to check. The target recovery database server must have database backup agent installed, and the service ports: 23100 and 23101 need to be opened for Vinchin backup server.

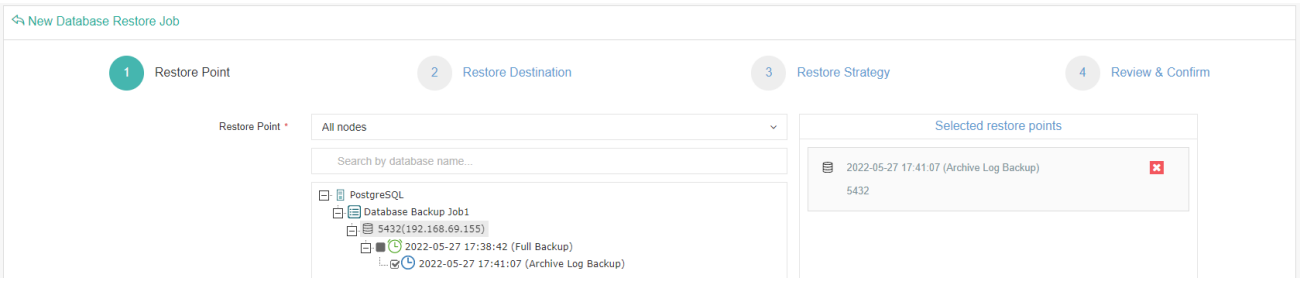
If override original database restore, the target PostgreSQL database instance needs to be shutdown, the path of data directory and archive log directory must be the same as original database server, and the free storage space of the database server must be enough to save the full restore point data size.

If restore to new path, you must specify a custom port number to run the database instance and the port number should not be used by any other services on the database server. And you need to specify new directories for data and the archive log, these 2 directories should be empty and should not be any directory which is being used by any other services on the database server. For the free storage space required, it must be 2 times more than the full restore point data size.

To create a PostgreSQL database restore job, please go to **Physical Backup** > **Database Backup** -> **Restore** page and follow the steps below.

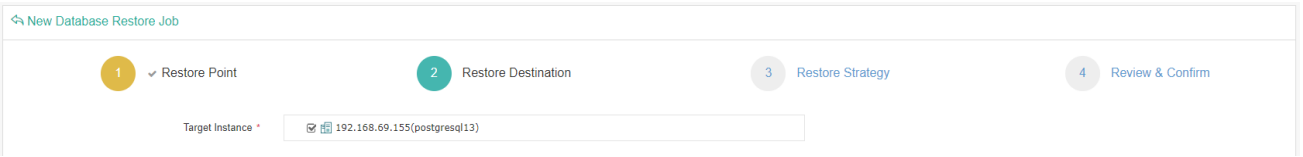
Step 1: Restore Point

If you select a full restore point, you'll be able to directly restore PostgreSQL database to the state of when the backup was taken. If you select an archive log restore point, you are able to roll back the database state to any time point between the first full backup timepoint and the selected archive log backup time point.



Step 2: Restore Destination

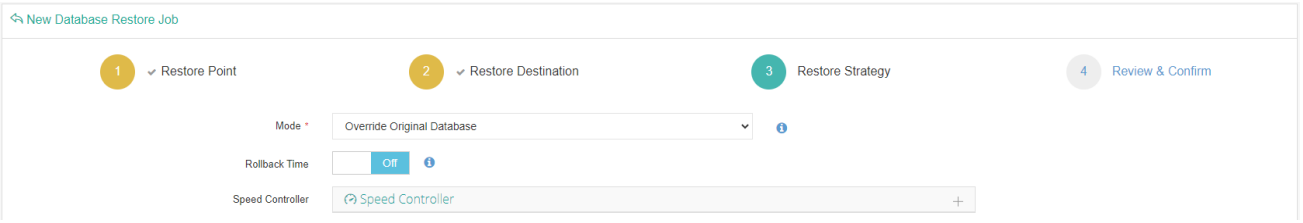
After selecting restore point, select **Target Instance** which you wish to restore.



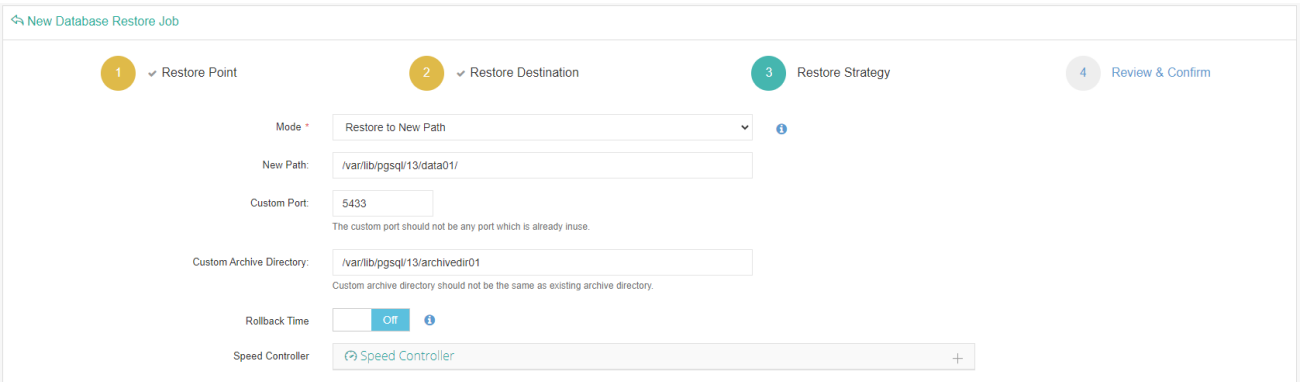
The target database instance can be the original database server or a new database server.

Step 3: Restore Strategy

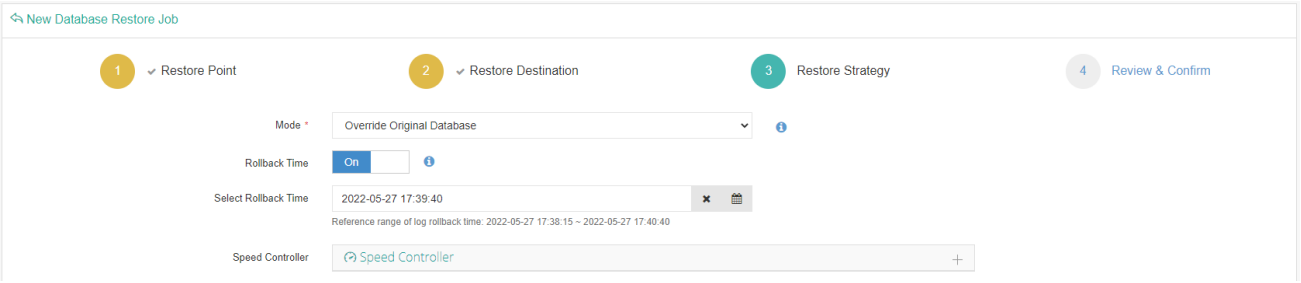
Mode: Override Original Database applies to restore the data to the production database server. Override the data of the original database instance.



Restore to New Path applies to restore data to a new directory. The directory needs to be created by the PostgreSQL database user and has PostgreSQL user permissions.



Rollback Time: if you had selected archive log backup restore point, you are able to rollback PostgreSQL database state within the given time range.



If you disable rollback time it will by default restore to the latest time point of when the backup has been taken.

Speed Controller: Same as database backup, while restoring databases, you can also configure speed controller to limit the database restore speed accordingly.

Step 4: Review & Confirm

After completing the above-mentioned settings, you are able to review and confirm the settings in one screen.

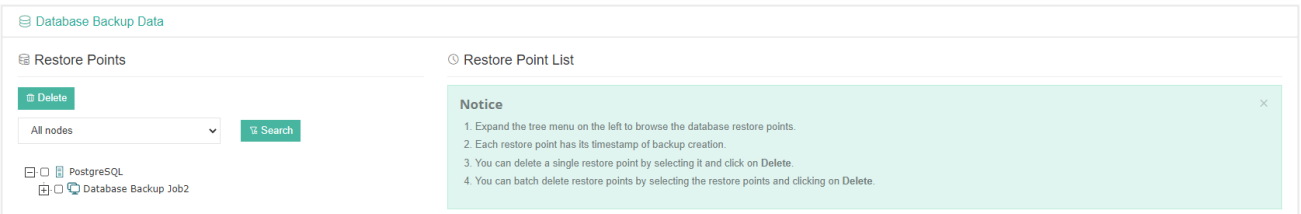
Once the job has been created, you'll be redirected to the **Monitor Center** > **Jobs** page.

As the database restore job is by default to be executed right after the creation of the job, so it will run automatically, when you see it in the current job list, it should be in running status already, and once completed, the job will be automatically deleted from the current job list.

During the database restore process, the full data size of the full backup will be transferred from Vinchin backup server to the database server, and the data will be written in to a temporary directory, after transmission is completed then it will perform restore/roll backup restore operations according to the job configurations.

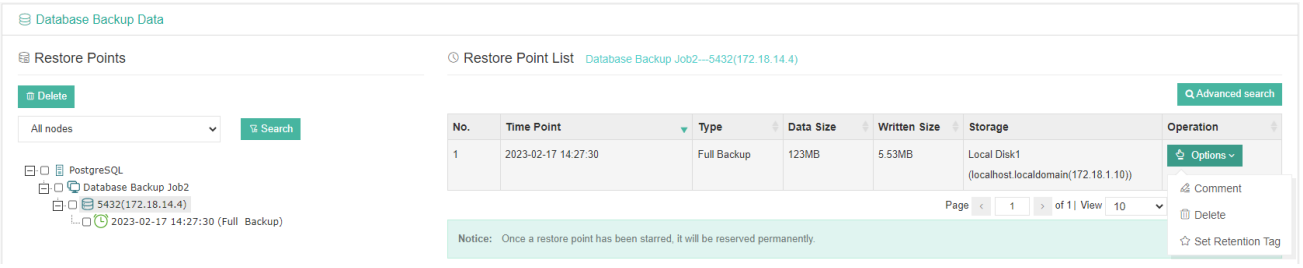
PostgreSQL Backup Data

The database backup data can be managed from **Physical Backup** > **Database Backup** > **Backup Data** page.



If you want to delete a restore point or multiple restore points, you can first select target restore point(s) from the left tree view, and click on the **Delete** button. The archive log backups cannot be deleted individually, they will be deleted along with the dependent full backup.

When deleting backup data, you need to provide your login password to confirm the deletion, once deleted the data will be unrecoverable.



For the restore point list in the right column, you need to select a database in the left tree menu to view all restore points of the selected database. Information like backup type, data size, written backup size and storage the backup resides in will be given.

You can add comments to the full backups and the archive log backups, and set retention tags for the full restore point to keep the full backup and its dependent archive log backups to not be deleted by retention policy.

A full restore point can be also deleted from the Restore Point List by clicking on Options and then select Delete, the dependent archive log will be deleted along with the full restore point.

Notice

1. In the restore point list, users are not allowed to delete an individual archive log restore point, when you click on Options button you are only able to add remarks to an archive log restore point.

2. If it's a full restore point, you are allowed to add remarks to it or to delete it, but deleting a full restore point will also delete the archive log restore point dependent on the full restore point.

MariaDB Database Backup

Preparation for MariaDB Backup

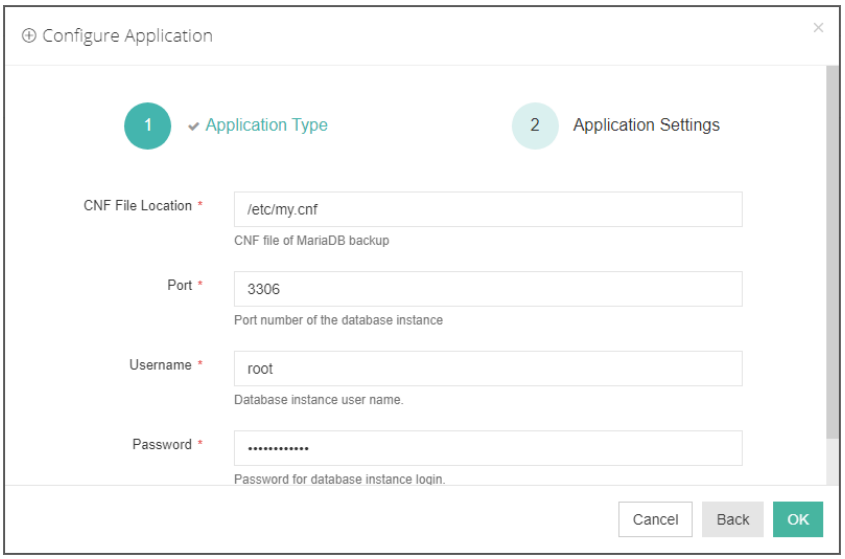
After the installation of Vinchin physical backup agent on MariaDB database server, users have to license the agent with database backup module.

When done installation and licensing, please open Vinchin Backup Server web console and go to **Resources** > **Agents** page, find the target agent, click on **Options** and then select **Application** to configure application settings for database backup.

Click on **Configure Application** button to configure the application settings.

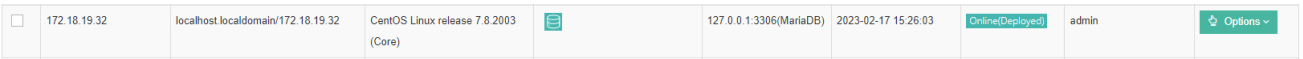
In the **Application Type** dropdown list, please select **MariaDB** and then click on **Next**.

In the Applications Settings screen, please configure the following settings.



In the **CNF File Location** field, please type in the file path of MariaDB cnf file. Leave the Port number with default value and provide database administrator username and password, click on OK to complete the application configuration.

When MariaDB application is successfully configured, in the agents list, you should see the agent look like below.



Now you should be able to create backup jobs for the MariaDB database server.

If you want to run MariaDB log backup, MariaDB database needs binary logging enabled. You can check with below command from MariaDB database command line interface.

```
show variables like '%log_bin%';
```

If you got log_bin value as on, which means binary logging is enabled.

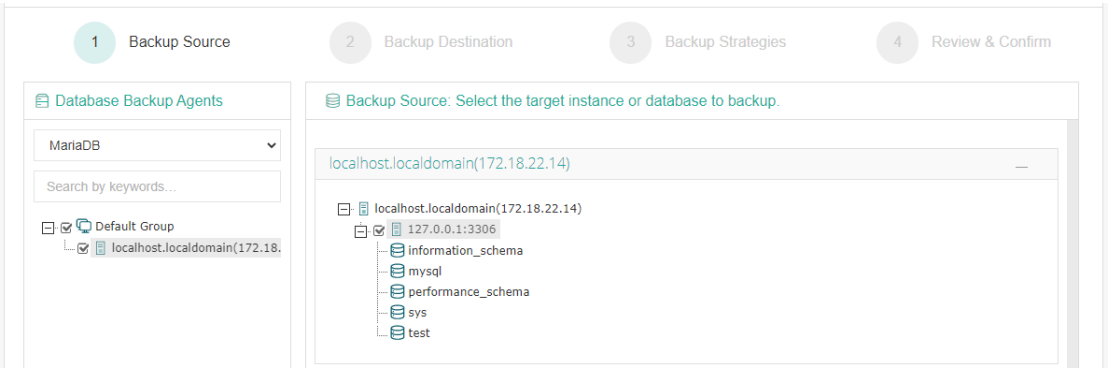
If binary logging is not enabled, it needs the database administrator to enable it.

Create MariaDB Backup Job

To create database backup jobs, please go to **Physical Backup** > **Database Backup** > **Backup** page. There are 4 steps to create a database backup job.

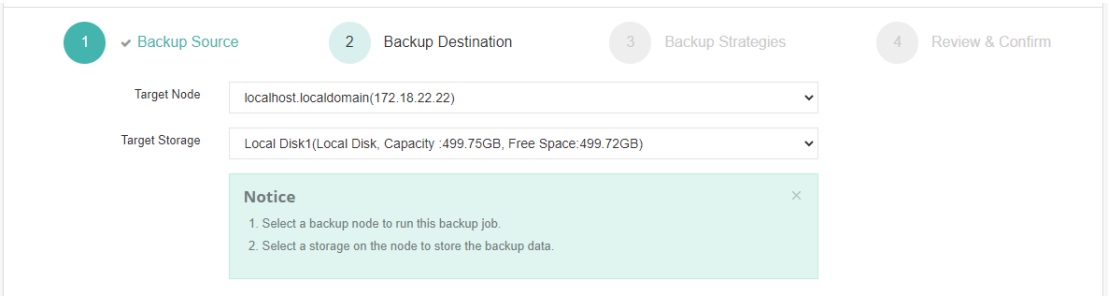
Step 1: Backup Source

First select backup source from left column, then select MariaDB database instance you wish to backup, in the right column will show which instance you selected.



Step 2: Backup Destination

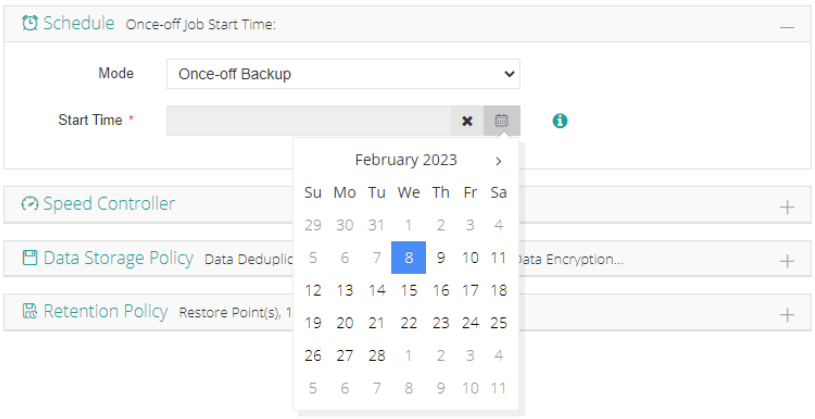
A backup destination (backup storage) should be associated with this backup job.



In the **Target Node** dropdown list, you can select a backup node on which you want the backup data to be processed and stored.
In the **Target Storage** dropdown list, the storages belong to the selected backup node can be selected.

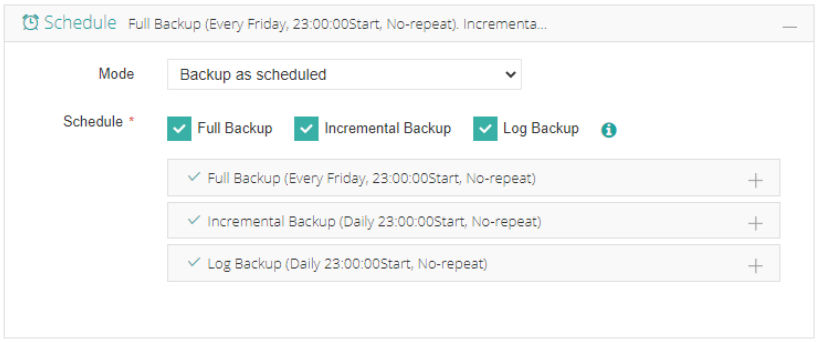
Step 3: Backup Strategies

In the General Strategy, you can configure the time schedule of the backup job, you can configure the job as a **Backup as Scheduled** job or a **Once-off Backup** job.
For a once-off backup job, the job will only run for once, and only full backup will be performed. You only have to appoint a time of when to start the backup job, in the **Start Time** field.



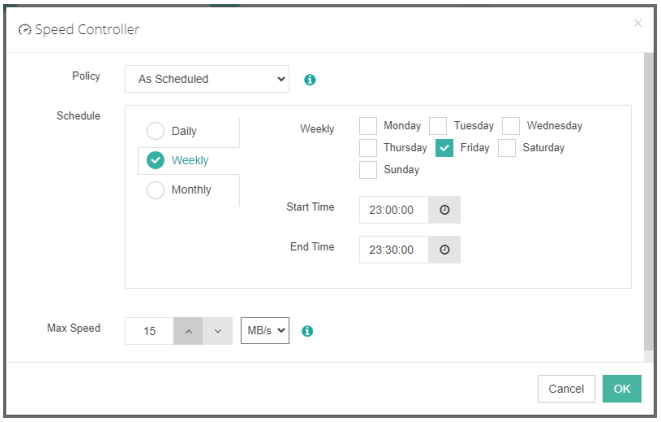
For backup job type, you can schedule Full Backup, Incremental Backup and Log Backup.

Here we take these three backups as an example. Please set the backup mode and backup schedule as per your actual demands.

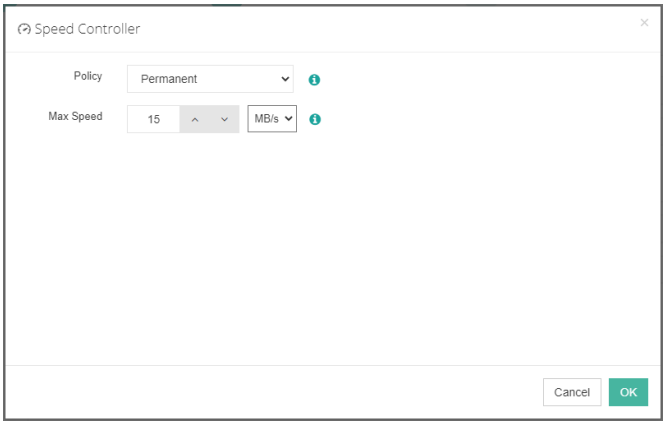


Speed Controller is optional. It can be used to limit the transmission speed during database backup if needed.

The speed controller policy can be configured as either As Scheduled or Permanent. An As Scheduled policy can be configured to limit the backup speed on Daily, Weekly and Monthly basis.



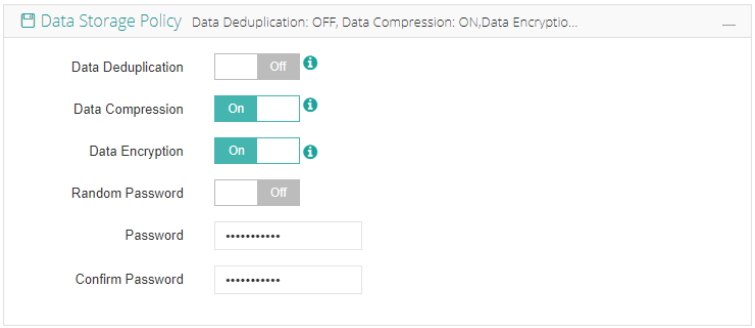
A Permanent policy will always limit the backup speed within the specified Max Speed.



There are 3 options in Data Storage Policy section, Data Deduplication, Data Compression and Data Encryption.

By enabling **Data Deduplication** and **Data Compression**, you can save the bandwidth and storage resources for transmitting and storing the backup data.

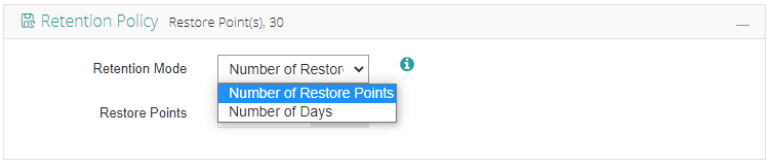
By enabling **Data Encryption**, the backup data will be encrypted and then stored into the backup storage. A password needs to be specified to secure the data encryption, when creating a database restore job, password verification is required to perform database restore.



For the retention policy of the database backup, there are 2 retention mode, retain the database backups according to **Number of Restore Points** or **Number of Days**.

For the retention mode **Number of Restore Points**, the restore points will be counted by full restore points, including the incremental backups and log backups dependent on this full backup.

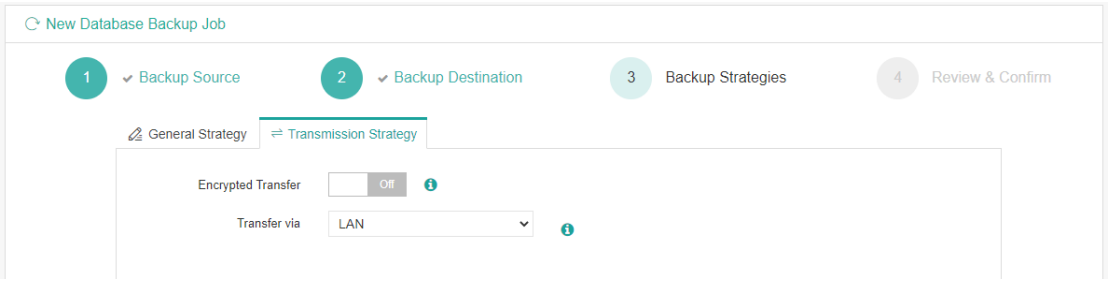
For retention mode **Number of Days**, Vinchin Backup Server will save the restore points within the specified number of days.



When the retention policy is triggered, the outdated restore points will be purged to comply with the retention policy.

In the Transmission Strategy, you can choose to enable **Encrypted Transmission** for data safety.

The backup data will be transferred through LAN by default.

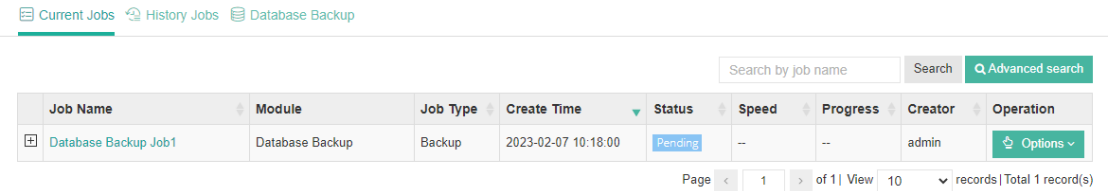


Step 4: Review & Confirm

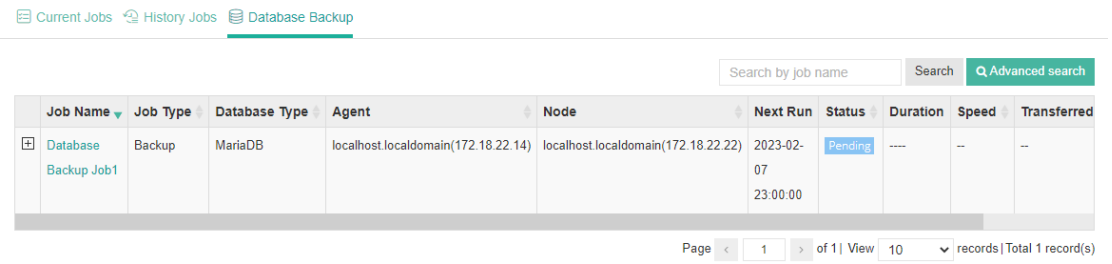
After completing the above-mentioned settings, you are able to review and confirm the settings in one screen.
A job name can be specified for identification of the database backup job, and by clicking on the Submit button to create the backup job.

MariaDB Backup Job Management

Once a database backup job had been created, you will be redirected to the **Monitor Center** > **Jobs** page.



The status of the newly created job will usually be **Pending**, when the time condition matches the schedule, it will automatically run. And the status will change to Running, you can also see the transfer speed here within the job list.
Besides the Current Job list, there's a dedicated tab to show database backup jobs. More detailed information of database backup jobs, including database type, database agent info, backup node, next run time and some more detailed information dedicated for database backup will be given.



By clicking on the job name you can check more detailed information on the **Job Detail** page.
For a scheduled backup job, after running one of the schedules, the status will change to Pending again and then wait for the next run.
For a once-off backup job, after running the job for once, it will be removed from the Current Job list. And you can find it from the History Job list.

Create MariaDB Restore Job

There are two methods to recover MariaDB database, **Override Original Database** and **Redirect Restore to New Path**.

For **Override Original Database** restore, Maria database needs to be shutdown. For example:

```
systemctl stop mariadb
```

And an empty temporary directory needs to be created and should be granted with mysql user permission for storing cache data during restoration process. For example:

```
mkdir /data
chown -R mysql:mysql /data
```

All data in the original data directory (datadir) needs to be cleared before restoration, it's recommended to rename the original data directory and create a new directory with the original data directory name, and it needs to be granted with mysql user permission, for example:

```
cd /var/lib/
mv mysql mysql.bk
mkdir mysql
chown -R mysql:mysql mysql
```

Note

1. The above operations should be done by the Maria database admin.

2. The temporary directory is recommended to be created on the same partition as original data directory.

2. For the datadir, it's configured in the my.cnf file, database admin should perform the above operations according to the actual environment.

For **Redirect Restore to New Path**, a temporary directory and a new data directory need to be created and need to be granted with mysql user permissions, for example:

```
mkdir /data
chown -R mysql:mysql /data
mkdir /data1
chown -R mysql:mysql /data1
```

Notice

1. Redirect Restore to New Path does not require shutdown Maria database services.

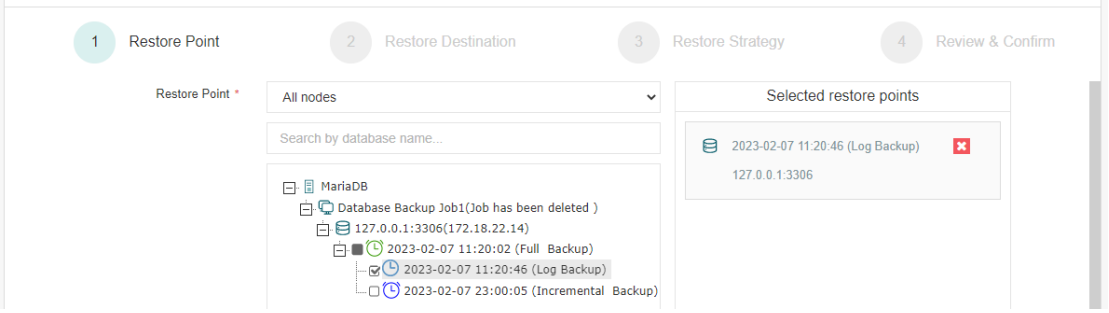
2. The restored data will be saved in the new data directory, database admin can use the restored data to create new database or modify the my.cnf file to start Maria database from the new data directory.

To restore MariaDB database from its backup restore points, please go to **Physical Backup** > **Database Backup** > **Restore** page. There are 4 steps to restore databases from the database backup restore points.

Step 1: Restore Point

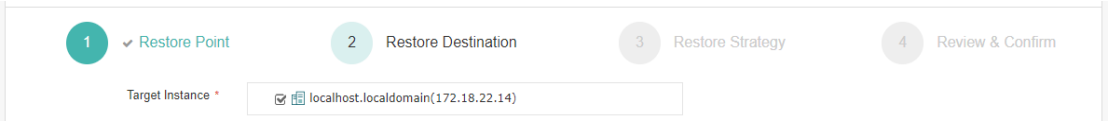
In the Restore Point dropdown list, select a backup node which stores the desired restore points.

Select a target database restore point under your database which you want to restore. You can quickly find the target restore point by searching the job name, database name or the date of the restore point. One restore job only can select one restore point.



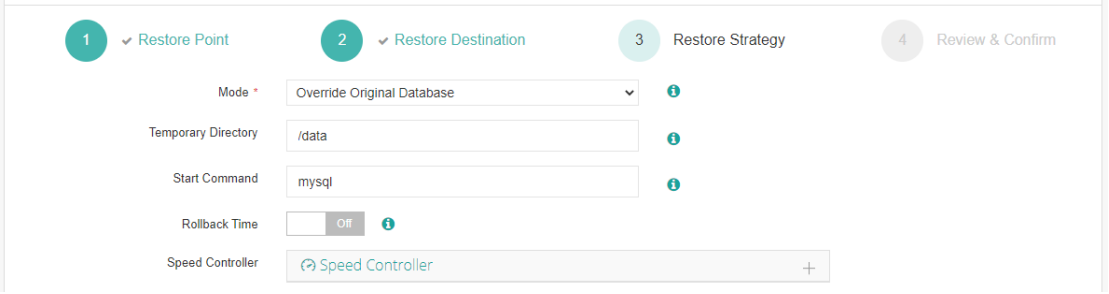
Step 2: Restore Destination

After selecting restore point, select **Target Instance** to restore to.



Step 3: Restore Strategy

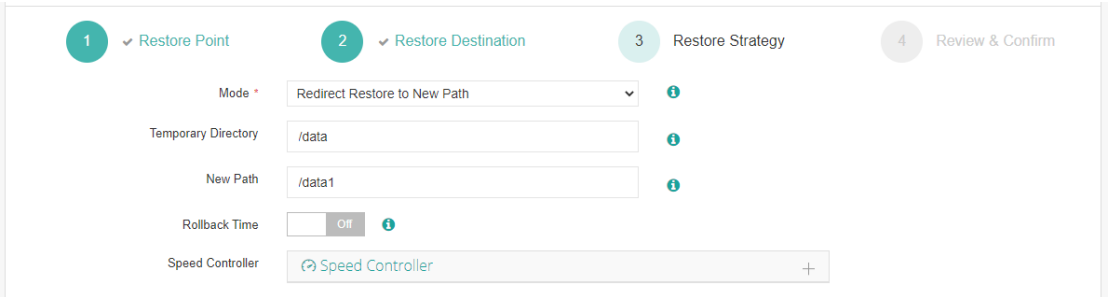
For **Override Original Database** restore, fill in the temporary directory path.



Notice

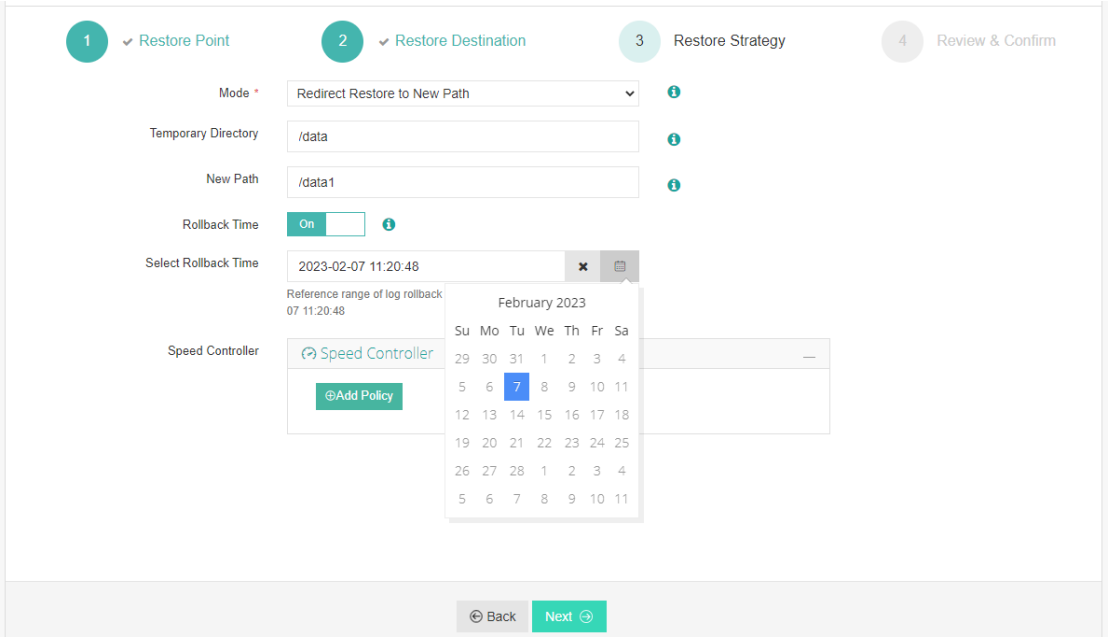
If you use log backup point to override original database, MariaDB service will auto restart, no need to manually start MariaDB service. The [Start Command] is 'mysql' by default. It will be used to restart database service. You need to change it to the service name of your environment instance. For example: this is a MariaDB, fill in the service name as 'mariadb'. Then the command 'service mariadb restart' will execute.

For **Redirect Restore the New Path** restore, fill in the temporary directory path and the new data directory path.



Rollback time: if you had selected log backup restore point, you are able to rollback MariaDB database state within

the given time range.



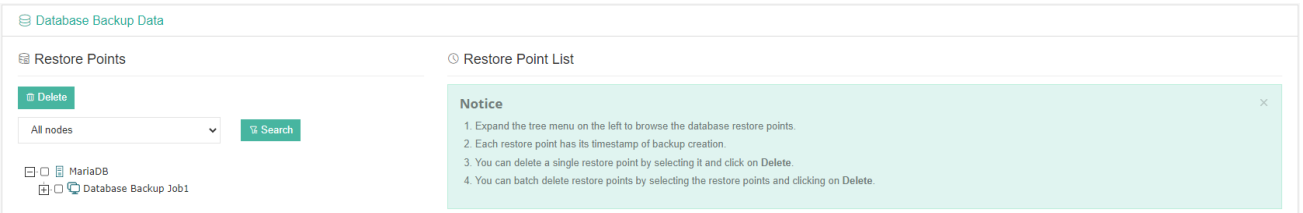
Same as database backup, while restoring databases, you can also configure **Speed Controller** to limit the database restore speed accordingly.

Step 4: Review & Confirm

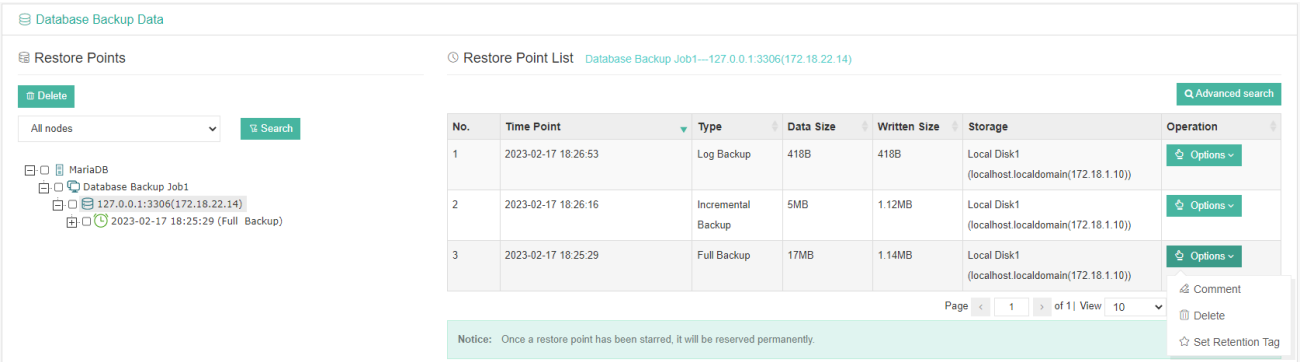
After completing the above-mentioned settings, you are able to review and confirm the settings in one screen.
Once the job has been created, you'll be redirected to the **Monitor Center** > **Jobs** page.
As the database restore job is by default to be executed right after the creation of the job, so it will run automatically, when you see it in the current job list, it should be in running status already, and once completed, the job will be automatically deleted from the current job list.
After this you can browse the restored job from History Jobs. Your restored data will be found in the path you configured during creating the restore job.

MariaDB Backup Data

The database backup data can be managed from **Physical Backup** > **Database Backup** > **Backup Data** page.



If you want to delete a restore point or multiple restore points, you can first select target restore point(s) from the left tree view, and click on the **Delete** button. The incremental backup and log backup cannot be deleted independently, they will be deleted along with the dependent full backup.



When deleting backup data, you need to provide your login password to confirm the deletion, once deleted the data will be unrecoverable.

For the restore point list in the right column, you need to select a database in the left tree menu to view all restore points of the selected database. Information like backup type, data size, written backup size and storage will be given.

You can add comments to the full backups, incremental backups and the log backups, and set retention tags for the full restore point to keep the full backup and its dependent incremental and log backups to not be deleted by retention policy.

A full restore point can be also deleted from the Restore Point List by clicking on Options and then select Delete, the dependent incremental and log backups will be deleted along with the full restore point.

Server Backup

Server backup of Vinchin Backup & Recovery allows customers to take backups of entire Linux and Windows server's operating system or specific volume(s) of the physical server.

Preparation for Server Backup

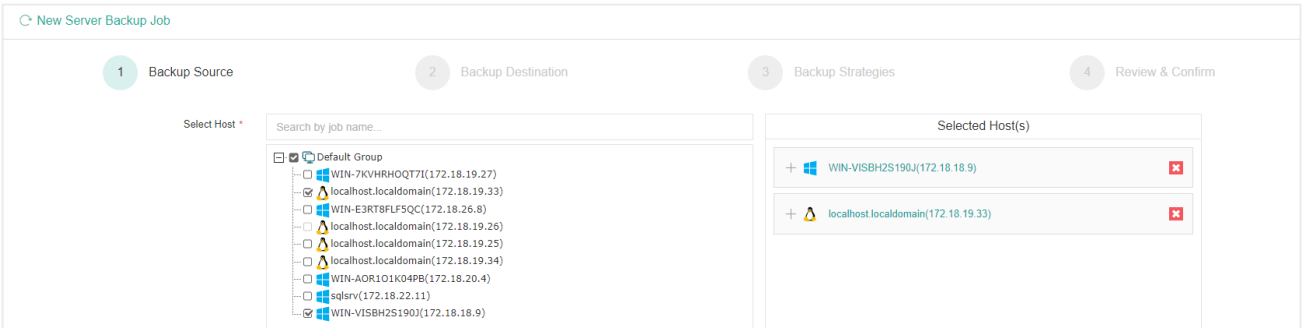
Physical server backup is agent-based backup which requires a physical backup agent to be deployed on the target server, if you haven't done this yet, please first refer to Preparation for Physical Backup to get the agent deploy and licensed for server backup.

Create Server Backup Job

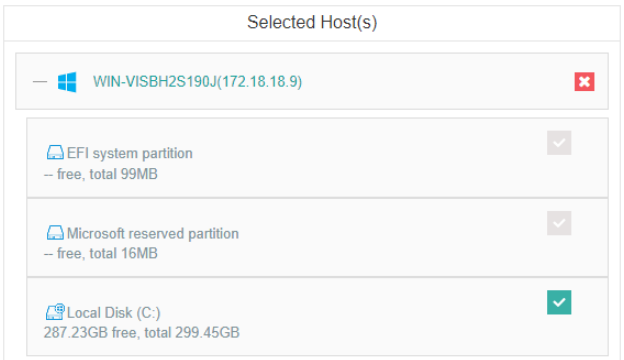
To create server backup jobs, please go to **Physical Backup** > **Server Backup** > **Backup** page. There are 4 steps to create a server backup job.

Step 1: Backup Source

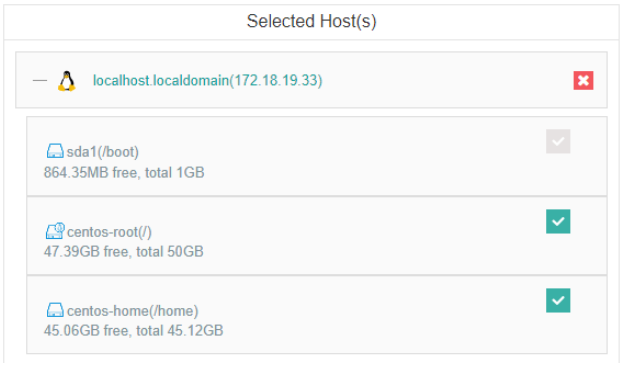
Select the hosts you want to backup from the Group tree, expand the group until you see the hosts. Select the host(s) you need to back up, the selected host(s) will be added to the **Select Host(s)** column.



Click on the selected host(s), you can select or exclude the partition(s) or disk(s) from this backup job by unticking the front check box of the partition(s) or disk(s). For Windows Operating System, **EFI system partition** and **Microsoft reserved partition** will be selected and backed up by default.



For Linux servers, **boot** partition is selected and will be backed up by default.



Notice

1. Windows servers only which file system type is NTFS support partition backup.

2. Windows servers which disk type is Dynamic does not support backup.

3. Windows disk state is offline or uninitialized cannot be backed up.

4. Windows servers must have at least 300MB free space in each partition.

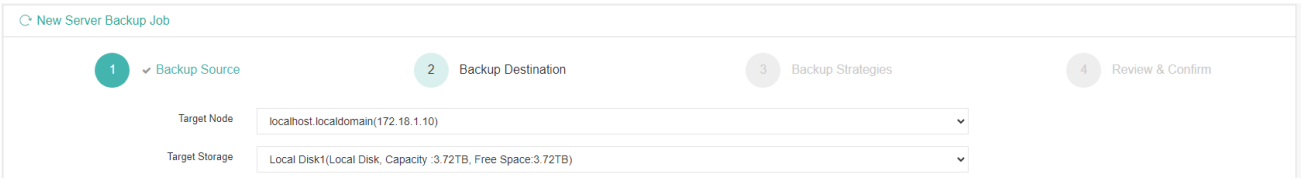
5. Windows servers protected by security software may fail to back up.

6. RHEL/CentOS booted with GPT+BIOS cannot be backed up.

7. RHEL/CentOS 8.4, 8.5 are not supported with server backup.

Step 2: Backup Destination

On the Backup Destination page, you need to specify a backup storage to save your backup data.



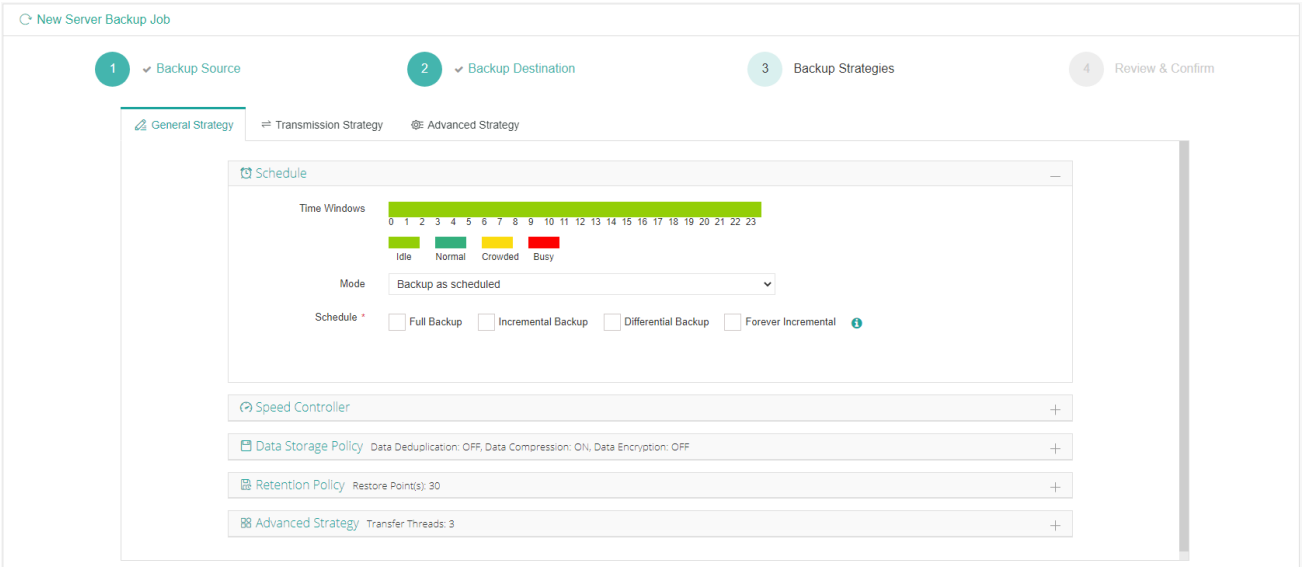
In the **Target Node** dropdown list, you can select a backup node on which you want the backup data to be processed and stored.

In the **Target Storage** dropdown list, the storages which belong to the selected backup node can be selected.

When done selecting the backup storage, please click on **Next** button to continue.

Step 3: Backup Strategies

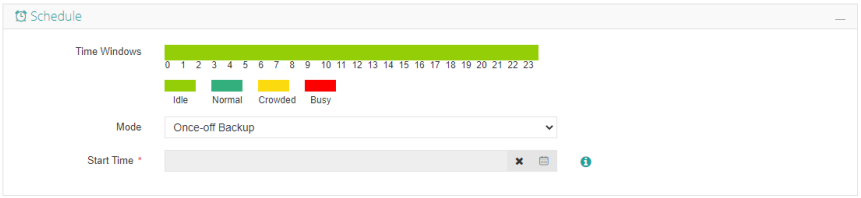
Under the **General Strategy** tab, you can setup the backup Time Schedule, Speed Controller, Data Storage Policy, Retention Policy and Advanced Strategy.



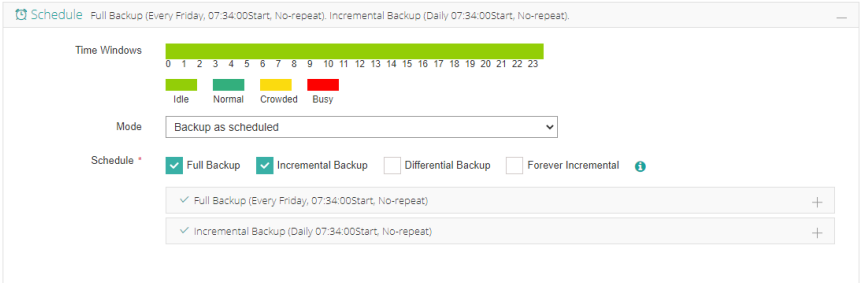
To determine the backup window of this job, the **Time Windows** indicator can be a reference for you to determine in which time window the job should be scheduled.

In the **Mode** dropdown list, you can choose the backup mode of this backup job, you can configure the job as a **Backup as Scheduled** job or a **Once-off Backup** job.

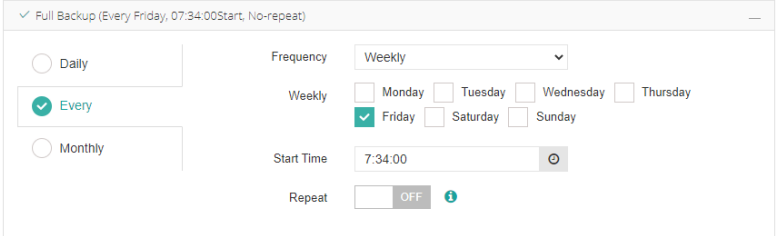
For a once-off backup job, the job will only run for once, and only full backup will be performed. You only have to appoint a time of when to start the backup job in the **Start Time** field.



For a **Backup as Scheduled** job, you can schedule full, incremental, differential and even forever incremental backups for the server backup job as per your needs.



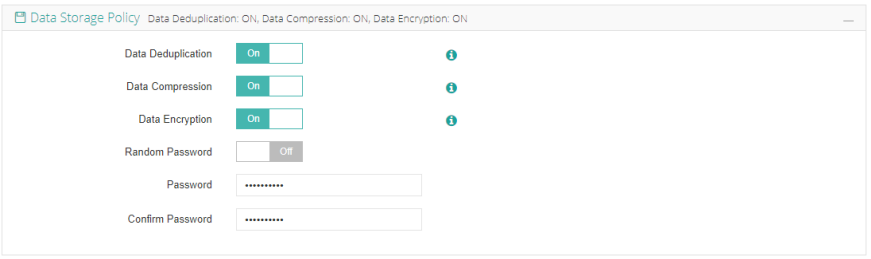
By clicking on the + icon, you can configure when exactly to run the backup job on daily, weekly or monthly basis.



Usually, it's recommended to run the full backups on weekly basis and run the incremental backups on daily basis.

For the Speed Controller settings, it's optional, only the highly efficient backup process will impact on the server performance, you can choose to configure the speed controller policy to limit the backup speed.

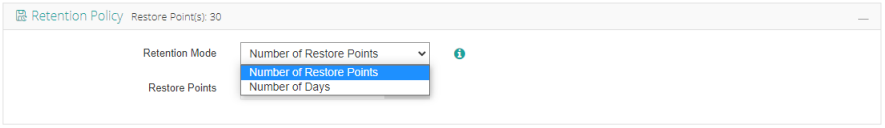
Data Storage Policy including **Deduplication**, **Compression** and **Encryption** of the backup data.



By enabling **Data Deduplication** and **Data Compression**, you can save the bandwidth and storage resources for transmitting and storing the backup data.

By enabling **Data Encryption**, the backup data will be encrypted and then stored into the backup storage. A password needs to be specified to secure the data encryption, when creating a server restore job, password verification is required to perform server restore.

For the **Retention Policy**, it can be used to define how much/long the backup data to be reserved in the backup storage, you can either define the retention policy with **Number of Restore Points** or **Number of Days** mode.

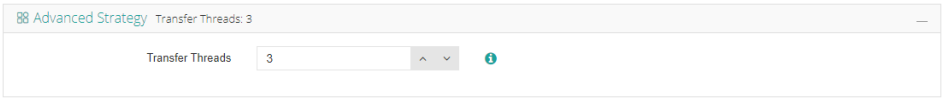


If you only enable full backup for the server backup job, only full restore points will be generated, and to comply with the retention policy, the restore point exceeded the given number of restore points or number of days will be directly deleted.

For the incremental backup jobs, to comply with the retention policy, Vinchin backup server will merge the first full backup with the following incremental backup restore points to comply with the retention policy. If it's a forever incremental backup job, Vinchin backup server will always merge backup restore points. If there are full backups to be taken regularly, then the first full backup will be merged with the incremental backup restore points between the first and the second full backup restore points one by one, when there's no incremental backup between the first and the second full backup, the first full backup restore point will be deleted at the next run of the job.

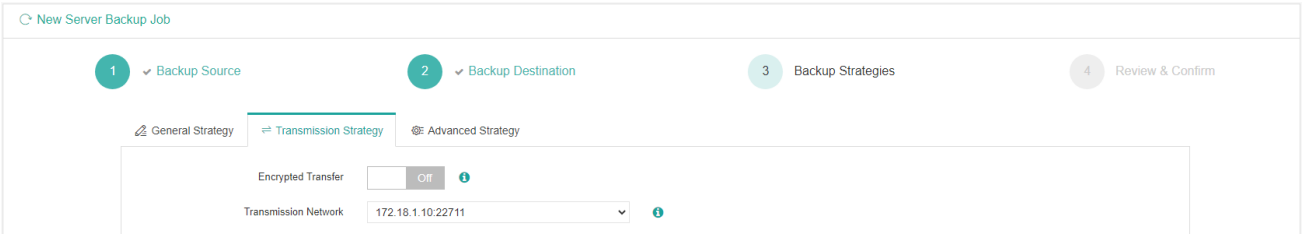
For differential backup jobs, Vinchin backup server will delete the first differential backup restore point to comply with the retention policy, if all differential backup restore points between the first and the second full backup restore points had been deleted, the first full backup restore point will be deleted at the next run of the job.

For the **Transfer Threads**, you can define 1 to 8 transfer threads for a single server backup job to implement multithreaded transmission.



If the high efficient backup process will impact on the server performance, please decrease the transfer threads number or consider enabling Speed Controller policy.

Under the **Transmission Strategy** tab, users can enable Encrypted Transfer and select transmission network for this backup job.



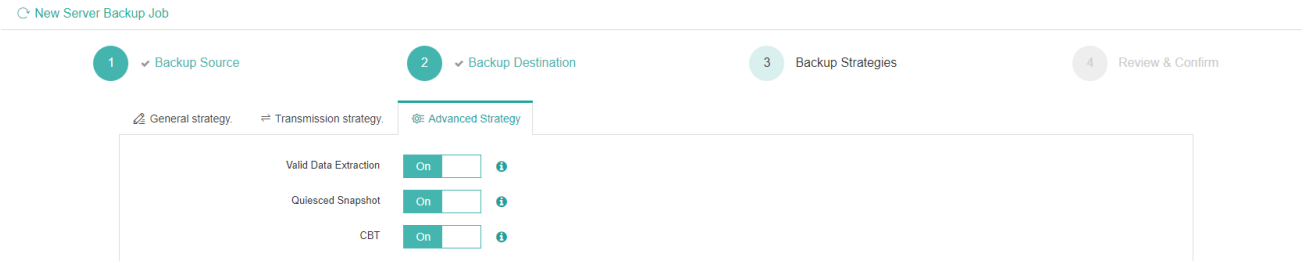
By enabling **Encrypted Transfer**, the transmission path between the physical server and Vinchin backup server will be encrypted to guarantee you data safety during backup process.

If your backup server has multiple networks connected, in the **Transmission Network** dropdown list, you can select a network to carry out the data transmission.

Under the **Advanced Strategy** tab, you can configure the **Valid Data Extraction** option.

You can enable **Quiesced Snapshot** to keep file systems or applications of the sever in a consistent state via application-awareness processing. Before taking the snapshot, Applications on Windows OS are required to support Microsoft VSS.

You can enable **CBT** to run server incremental backups for faster backup speed. (Please ensure that you have clicked on install driver when installing the server agent.)



This option can be used to extract the valid data of the server partitions, in order to reduce the backup storage usage.

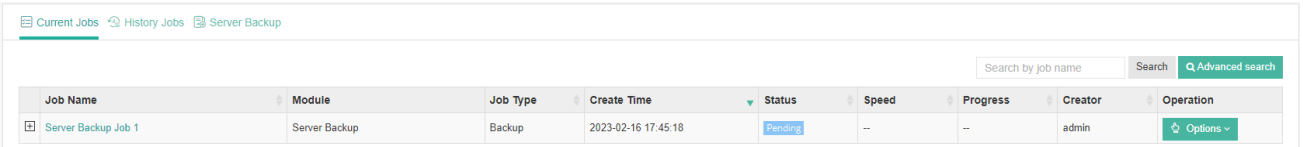
Step 4: Review & Confirm

After completing the above-mentioned settings, you are able to review and confirm the settings in one screen.

A job name can be specified for identification of the VM backup jobs, and by clicking on the Submit button to confirm the settings and create the backup job.

Server Backup Job Management

Once a server backup job had been created, you will be redirected to the **Monitor Center** > **Jobs** page.



The status of the newly created job will usually be **Pending**, when the time condition matches the schedule, it will automatically run. And the status will change to Running, you can also see the transfer speed here within the job list.

Besides the Current Job list, there's a dedicated tab to show server backup jobs. More detailed information of server

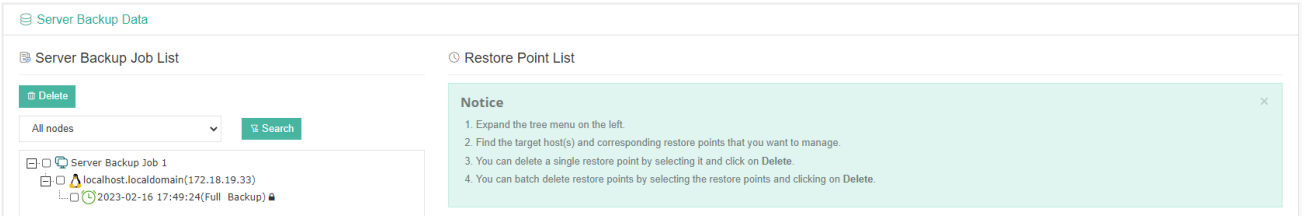
backup jobs will be given.
By clicking on the job name, you can check more detailed information on the **Job Detail** screen.
For a scheduled backup job, after running one of the schedules, the status will change to Pending again and then wait for the next run.
For a once-off backup job, after running the job for once, it will be removed from the Current Job list. And you can find it from the History Job list.

Server Backup Data

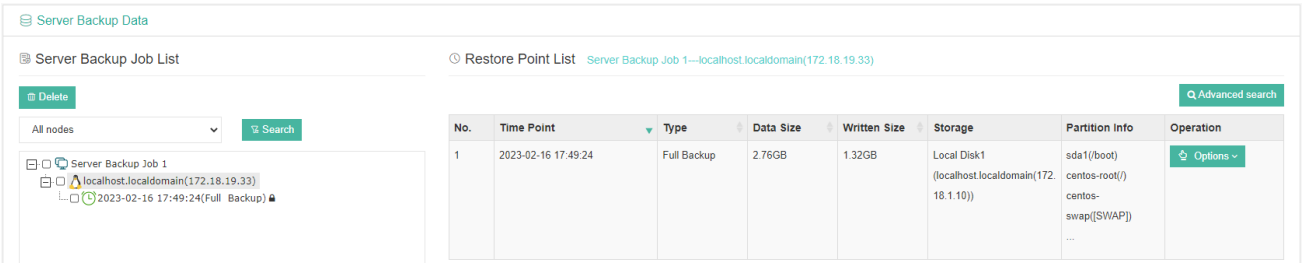
The server backup data can be managed from **Physical Backup > Server Backup** > **Backup Data** page.

View Backup Data

By default, all server backups of all backup nodes from Vinchin backup agents will be displayed, if you wish to view backups of a specific backup node, please select a node from the dropdown list.
The server backup data is organized with a Backup Job > Physical Server > Restore Point structure as shown below.



Each restore point is named with the timestamp of its creation and will be marked with its backup type. If there's a icon behind the restore point, which means the backup data is encrypted. To view more information of the restore points, simply click on the server name, all the restore points of the selected server will be listed in the right with more detailed information.

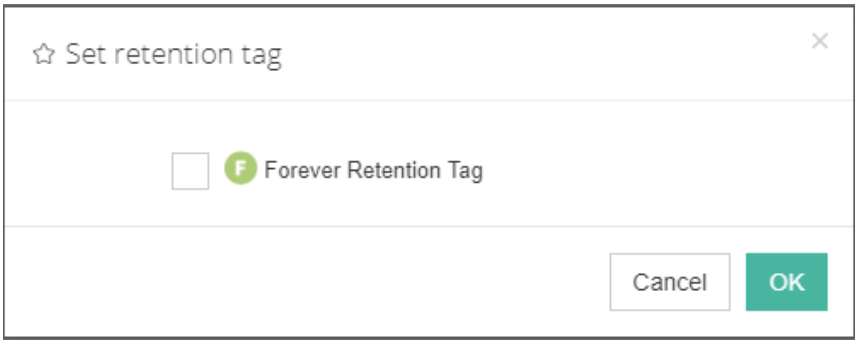


You can get more information like the actual data size, written size and the storage which is used to store the restore point data.
To search specific restore point(s), you can use the **Search** button on the left or use the **Advanced search** button at the right side of the **Restore Point List**.

Retention Tags

The purpose of using the retention tags is to avoid the general retention policy from purging some specific backups and keep them for a longer time period.
For server backup data, you can set **F**: forever retention tag. The **F** tag can only be manually set. To manually set

retention tags, please go to **Physical Backup > Server Backup** > **Backup Data** page. By selecting a server from a backup job, all the restore points will be listed on the right, find the restore point which you wish to set/unset retention tags and click **Options** button, and then select **Set Retention Tag**.



In the set retention tag dialog, check the forever retention tag option and click on OK, then the restore point will be tagged with a F tag and it will be kept in the backup storage permanently until the tag has been removed.

Delete Backup Data

We recommend configuring comprehensive retention policies for the server backup jobs to automatically purge the out-of-date backups instead of manual deletion of the backup data. It is a highly risk operation by deleting the backup data manually. If you have to do this, please follow the below instructions.
To delete server backup data, please go to **Physical Backup > Server Backup** > **Backup Data** page. There are two approaches to perform the deletion.
Please unfold the server backup job, and unfold the server which you wish to delete backup data from. Then select the restore point(s) you wish to be deleted and click on the **Delete** button on the top left of the tree view. You'll have to provide you password to confirm the deletion of selected restore point(s).
If it's a standalone full restore point, no incremental or differential restore points dependent on it, you can select and delete the standalone full restore point directly.
If it's a backup chain, formed by a full restore point and a series of incremental (or differential) restore points dependent on the full restore point, you can only delete the backup chain from the tree view.

Preparation for Server Restore

For the physical server restore, the target server could be the original one or a new one. If restoring to a new server, the hardware configurations should be the same as the original server, including mainboard, CPU, RAM disks, etc.
If the original operating system is running on the server which you are going to restore, only the data disks can be restored. If that's what you are going to do, please skip this part and continue from Create Server Restore Job.
If you want to restore the whole operating system, you need to boot the server with LiveCD or WinPE ISO image provided by Vinchin.

LiveCD Operation Procedures

The LiveCD ISO image is provided by the version of CentOS 8 Linux system, please download the LiveCD ISO image

from here.

Before you can boot the target server with LiveCD image, please create a bootable USB drive or CD/DVD disc using the downloaded ISO image, after that please boot your server from the USB drive or CD/DVD drive.

When you see the booting options screen, please select **Start LiveCD OS Restore** and press enter.

After the LiveCD system is completely started up, please login with the following credentials.

Username: **root**

Password: **Backup@3R**

When logged in, please use below command to get started connecting the server to Vinchin backup server.

```
sh os_restore
```

If the server has multiple NICs on board, you need to select the NIC which can be used to connect to Vinchin backup server by typing the NIC number and press enter.

Input a valid IP address under the following prompt:

```
Input IP address, e.g., 192.168.31.1:
172.18.19.106
```

Input a valid netmask under the following prompt:

```
Input netmask, e.g., 255.255.255.0:
255.255.192.0
```

Input a valid gateway under the following prompt:

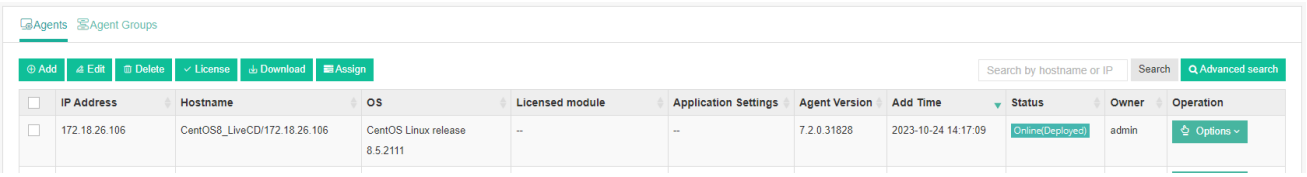
```
Input gateway, e.g., 192.168.31.1, press enter directly without setting gateway:
172.18.0.1
```

Once you had configured the network settings, the server network services will restart, when you see the following prompt, please input Vinchin backup server IP address.

```
Input backup server IP address:
172.18.1.10
```

Now the server running LiveCD will try to Ping Vinchin backup server to test the network connection, after that will try to download and install the physical server backup agent.

The whole process is automated, no further operations required. Once the agent installation is successful, please log in Vinchin Backup Server web console, in **Resources** > **Agents** page, it will display the server running LiveCD.



To restore the backups to this server running LiveCD, it does not need to be licensed, as it is only for temporary use of server restoration.

Notice

1. The server memory should be at least 2GB when booting with LiveCD.

2. When configuring LiveCD network settings, make sure to avoid IP address conflict in your LAN.

3. LiveCD can be used to restore both Linux and Windows server. (Except for Windows XP and Windows Server 2003. If you want to boot Windows XP or Windows Server 2003, please contact Vinchin technical support.)

WinPE Operation Procedures

Before you can boot the target server with WinPE ISO image, please download the WinPE ISO image from here. After downloading, please create a bootable USB drive or CD/DVD disc using the downloaded ISO image, after that please boot your server from the USB drive or CD/DVD drive.

When you see the message “Press any key to boot from CD or DVD” please press a random key to start the server from WinPE.

If the server has multiple NICs on board, you need to select the NIC which can be used to connect to Vinchin backup server by typing the NIC number and press enter.

Input a valid IP address under the following prompt:

```
Input IP address for WinPE, e.g., 192.168.31.1:
172.18.19.106
```

Input a valid netmask under the following prompt:

```
Input netmask, e.g., 255.255.255.0:
255.255.192.0
```

Input a valid gateway under the following prompt:

```
Input gateway, e.g., 192.168.31.1, press enter directly without setting gateway:
172.18.0.1
```

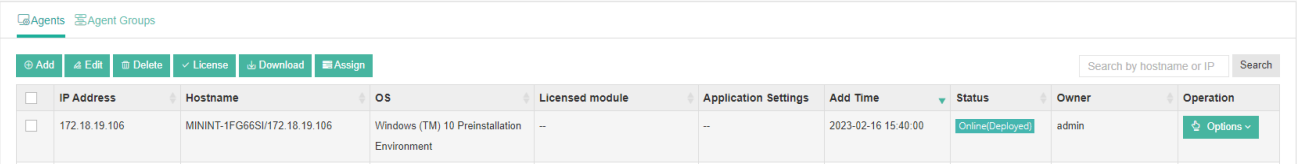
Input Vinchin backup server IP address under the following prompt.

```
Input backup server IP address:
172.18.1.10
```

Now the server running WinPE will try to Ping Vinchin backup server to test the network connection, after that will try to download and install the physical server backup agent.

The whole process is automated, no further operations required. Once the agent installation is successful, you’ll see prompt “Press any key to continue”, please press a key to complete the process.

Log in Vinchin Backup Server web console, in **Resources** > **Agents** page, it will display the server running WinPE.



To restore the backups to this server running WinPE, it does not need to be licensed, as it is only for temporary use of server restoration.

Notice

1. A WinPE booted server should not be powered on for more than 24 hours.

2. The server memory should be at least 2GB when booting with WinPE.

3. When configuring WinPE network settings, make sure to avoid IP address conflict in your LAN.

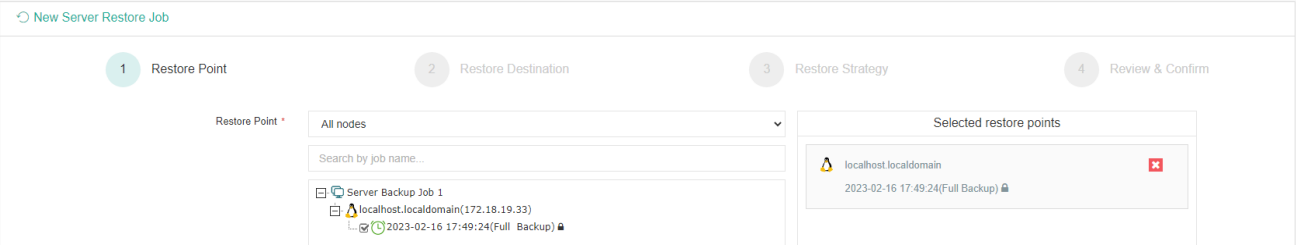
4. WinPE can be only used to restore Windows server. (Except for Windows XP and Windows Server 2003. If you want to boot Windows XP or Windows Server 2003, please contact Vinchin technical support.)

Create Server Restore Job

To create a server restore job, go to the **Physical Backup** > **Server Backup** > **Restore** page. Please follow the below steps to create a physical server restore job.

Step 1: Restore Point

Form the Restore Point dropdown list, select a backup node on which the server backup data is stored.

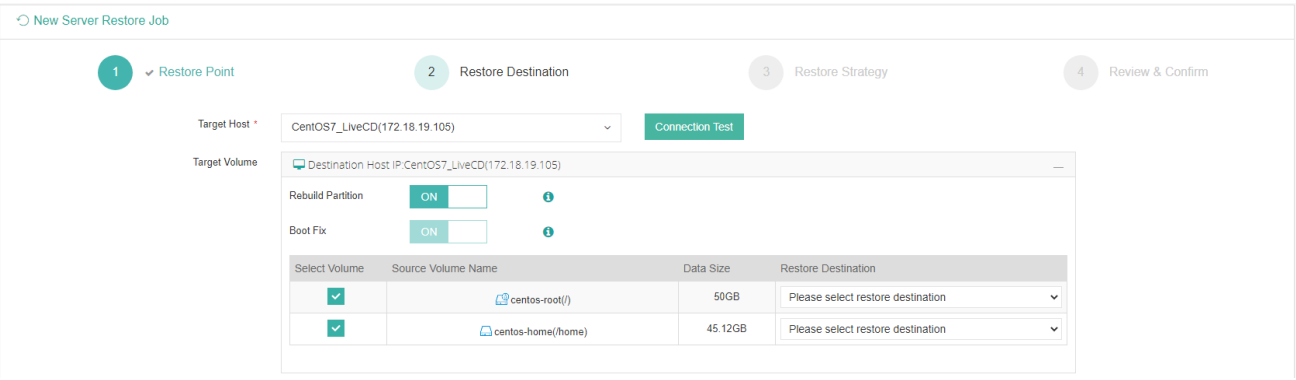


Then select desired restore point and click on **Next**. The restore point can be full, incremental or differential depending on which backup method you applied for server backup.

Step 2: Restore Destination

In the Target Host dropdown list, select the target physical server which you wish to restore to. If you only need to restore the data disk/partition, please select the original host. If you wish to restore the whole system, you'll need to boot the host from LiveCD or WinPE, for how to do this, please refer to Preparation for Server Restore.

When done selecting the target host, click on **Connection Test** to test the connection between the physical server and Vinchin backup server.



If the connection test is successful, you'll now be able to configure the restore options.

Rebuild Partition: if enabled, the partition table of the target server will be reconstructed to ensure that the new partition information is the same as that of the original host. If this option is enabled, all data on the partition will be erased, please be caution.

Boot Fix: if enabled, the /etc/fstab and grub.cfg files of the Linux systems will be re-configured on the new host after restore. If restore to the original host, and the backup partition corresponds to the source partition path, this option can be turned off.

If you are going to restore only the data disk/partition, please turn off both Rebuild Partition and Boot Fix options. And in the **Select Volume** column, please select only the data disk/partition to restore, and in the **Restore**

Destination column, please select the original partition. Only if the retore destination is a new disk, you can turn the **Rebuild Partition** option on.

If you are going to restore the whole system, make sure in the Target Host dropdown list you've selected a server which is booted from LiveCD or WinPE.

To make sure the restored server is bootable, please enable **Rebuild Partition** and **Boot Fix**, in the **Restore Destination** column, please select the disk for each partition to be restored to.

Notice

1. Hosts that are not booted with LiveCD and WinPE can only recovery data disks, please use LiveCD or WinPE to restore the whole system or system partitions if needed.

2. If restoring to different machine the Rebuild Partition option needs to be enabled.

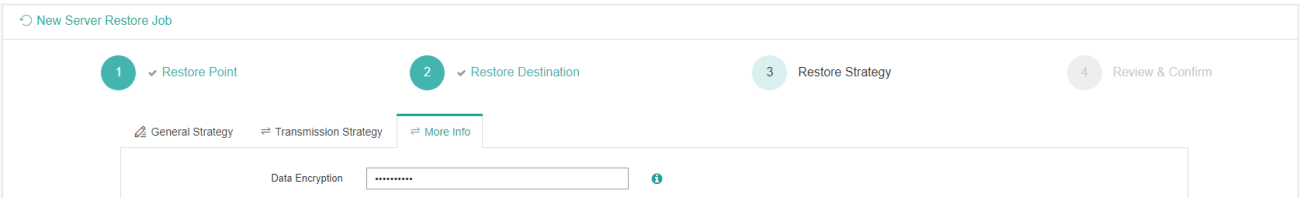
3. Server backups from Linux machine cannot be restored to a Windows machine and vice versa.

Step 3: Restore Strategy

Under the **General Strategy** tab, you could set **Speed Controller** and **Transfer Threads** for the server restore job same as when creating a server backup job. You could use the default settings.

Under the **Transmission Strategy** page, you could enable Encrypted Transfer to secure the data transmission and you can optionally select a transmission network.

If the server backup data had been encrypted (Data Encryption enabled in server backup job), then here on this page you'll have a **More Info** tab, under which you need to provide the encryption password before restoring the server backups.



Step 4: Review & Confirm

In this step, you could rename the job, review the job settings and submit to create a restore job.

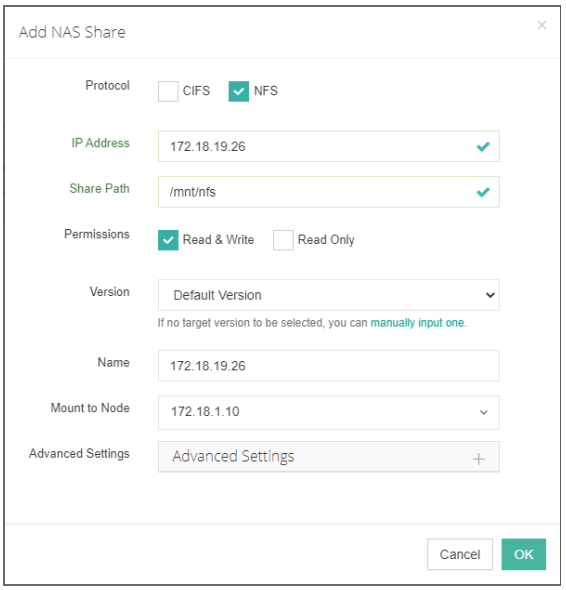
A server restore job will automatically run after its creation, when restoration done, you can power off the server to boot it from its local hard disk.

NAS Backup

Preparation for NAS Backup

Add NAS Shares

To add the NAS shares to Vinchin Backup & Recovery for backup, please go to **Resources** > **NAS Shares** page. Click on the **Add** button to add a NAS share.



The supported NAS protocols are CIFS and NFS, please select the target protocol of the NAS share which you are going to add.

In the **IP Address** field, input the IP of the NAS server, then in the **Share Path** field input the correct share path.

As for the **Permissions**, it's recommended to select Read & Write permissions in order to enable Vinchin backup server being able to perform NAS backup and restore, otherwise if **Read only**, Vinchin backup server will only be able to do NAS backup but not restore.

In the Version dropdown list, select the CIFS/NFS protocol version, if no option available, please click on **manually input one** to provide a protocol version manually.

In the **Name** field, users can define a customized name for the NAS share for identification.

If adding a CIFS share, user credentials should be provided in the **Username** and **Password** fields.

For the **Mount to Node** option, users can select one or several backup nodes (if any), the NAS share will be mounted to the selected nodes and users can then run NAS backups on multiple nodes.

In the **Advanced Settings** section, users can configure customized mount parameters for both CIFS and NFS shares, and additionally the customized port number for NFS share if needed.

License NAS Shares

Once a NAS share had been added, its status is **Unlicensed**, users have to license it with Vinchin NAS backup license module to enable backup of the NAS share.

Click on the **License** button to show the **License NAS Share** dialog.

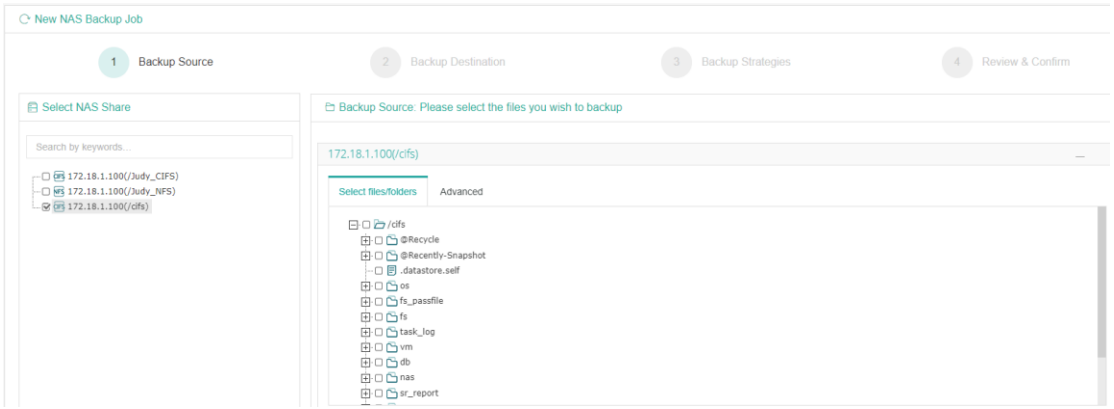
Select the NAS shares you've added and then click on **License** button to get the NAS shares licensed for backup.

Create NAS Backup Job

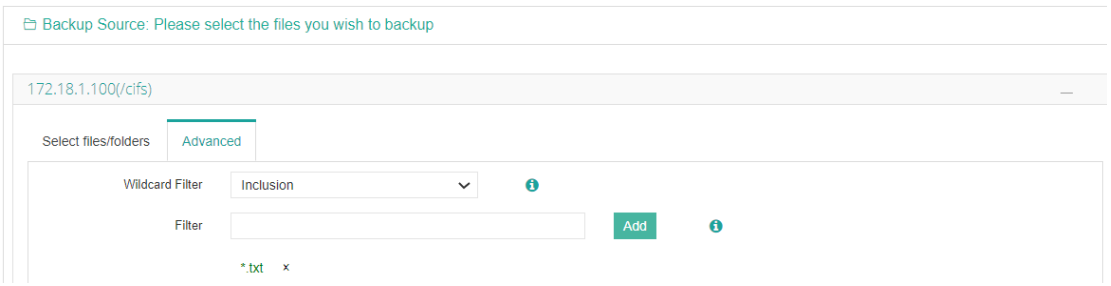
To create NAS backup jobs, please go to **NAS Backup** > **Backup** page. There are 4 steps to create a NAS backup job.

Step 1: Backup Source

First you need to select a target NAS share from the **Select NAS Share** column for this backup job. Each NAS backup job can only have one NAS share selected.



After selecting the target NAS share, please select the files or folders you want to back up from the **Backup Source** column. In the **Select files/folders** column, the files/folders could be selected by use the checkbox.



After selecting the files/folders, you can click **Advanced** to set wildcard filter rules for the NAS backup job, this is optional.

In the **Wildcard Filter** dropdown list, you can choose None, Exclusion and Inclusion.

None: backup all the selected files/folders which you've selected and do not use any filters.

Exclusion: backup all files except the ones to be excluded by exclusion filters.

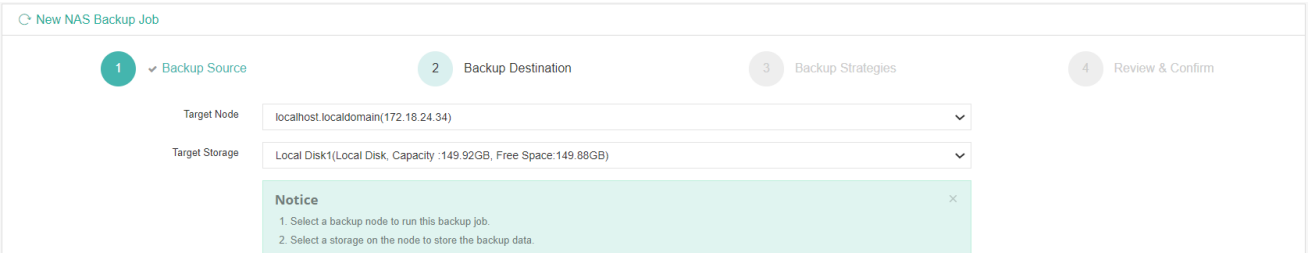
Inclusion: only backup the files which will be matched by the inclusion filters.

In the **Filter** field, type a filter rule e.g.: *.docx and click **Add** to add it; multiple filters can be applied to a single backup job; '*' can match 0, 1 or multiple characters, '?' can only match 1 character.

After setting the wildcard policy, please click on **Next** to continue.

Step 2: Backup Destination

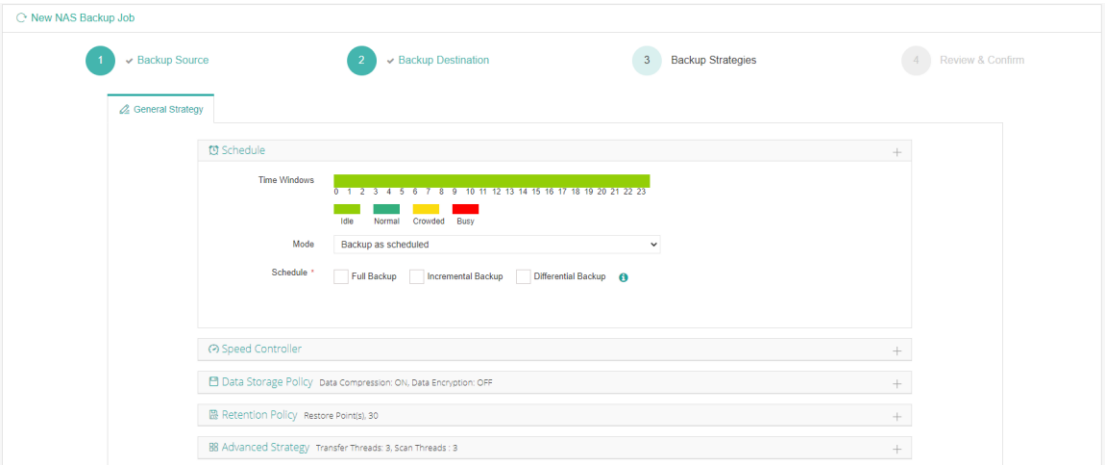
A backup destination (backup storage) should be associated with this backup job.



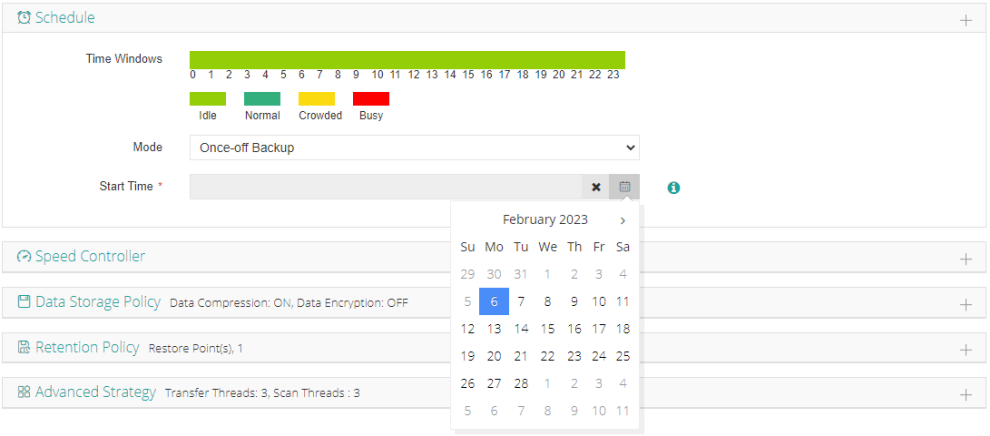
In the **Target Node** dropdown list, you can select a backup node on which you want the backup data to be processed and stored.
In the **Target Storage** dropdown list, the storages which belong to the selected backup node can be selected.
When done selecting the backup storage, please click on **Next** button to continue.

Step 3: Advanced Strategy

In the General Strategy it including Schedule, Speed Controller, Data Storage Policy, Retention Policy and Advanced Strategy.

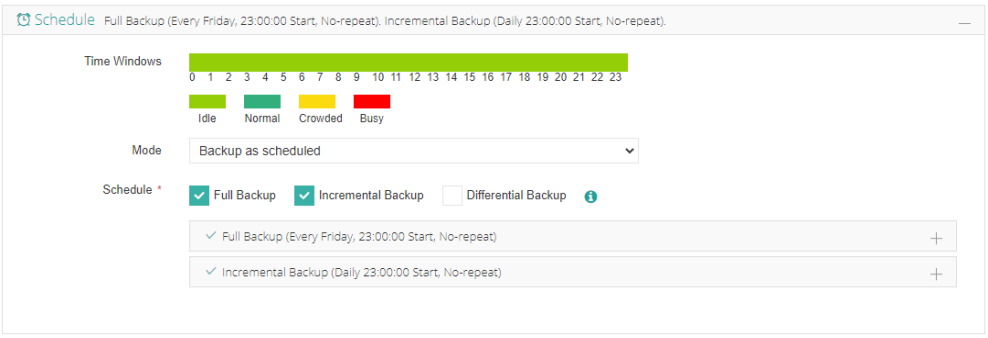


In the Schedule field, you can configure the time schedule of the backup job, you can configure the job as a **Backup as Scheduled** job or a **Once-off Backup** job.
For a once-off backup job, the job will only run for once, and only full backup will be performed. You only have to appoint a time of when to start the backup job in the Start Time field.



For a backup as scheduled job, you can schedule Full Backup, Incremental Backup and Differential Backup.

Here we take full with incremental backups as an example. Please set the backup mode and backup schedule as per your actual demands, then please click on **Next** to continue.

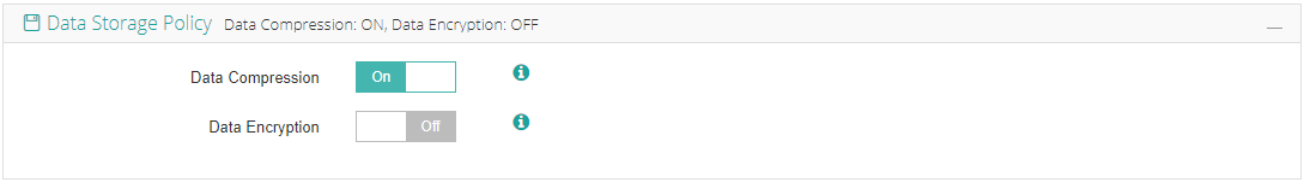


Speed Controller is optional. It can be used to limit the transmission speed during NAS backup if needed.

The speed controller policy can be configured as either **As Scheduled** or **Permanent**. An **As Scheduled** policy can be configured to limit the backup speed on Daily, Weekly and Monthly basis.

A **Permanent** policy will always limit the backup speed within the specified Max Speed.

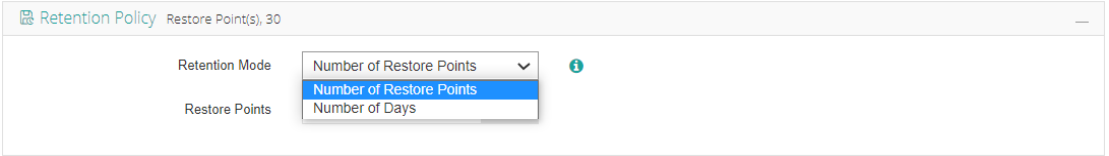
There are 2 options in **Data Storage Policy** section, **Data Compression** and **Data Encryption**. By enabling these 2 options, the backup data will be compressed and encrypted before saving into backup storage.



For the retention policy of the NAS backup, there are 2 retention mode, retain the NAS backups according to **Number of Restore Points** or **Number of Days**.

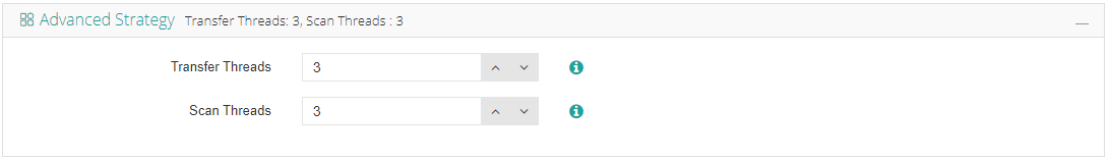
For the retention mode **Number of Restore Points**, Vinchin Backup Server will save the specified number of restore points. If you choose to retain the backups by number of restore points, the number will be counted by full restore points.

For retention mode **Number of Days**, Vinchin Backup Server will save the restore points within the specified number of days.

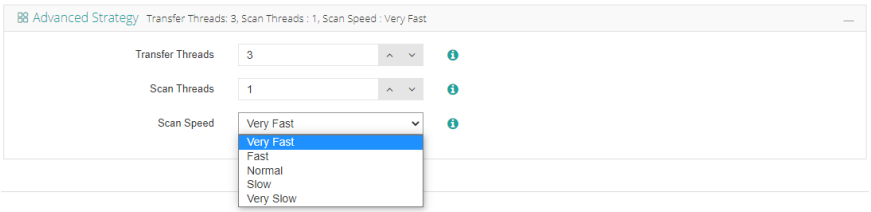


When the retention policy is triggered, the outdated restore points will be purged to comply with the retention policy.

Advanced Strategy contains transfer threads and scan threads. You can set 1 to 32 transfer/ scan threads for a single backup job. Increasing the number of threads can improve backup job efficiency, but multi-threading will occupy the resources of the NAS server, so the number of threads should be set reasonably according to the actual situation.



In order to eliminate the high efficiency backup impact on the performance of the NAS server, users can set the transfer and scan thread number to 1. And when the scan thread has been set to 1, users also able to configure the scan speed.



The scan speed can be configured with **Very Fast**, **Fast**, **Normal**, **Slow** and **Very Slow** options to balance the NAS server performance and backup speed.

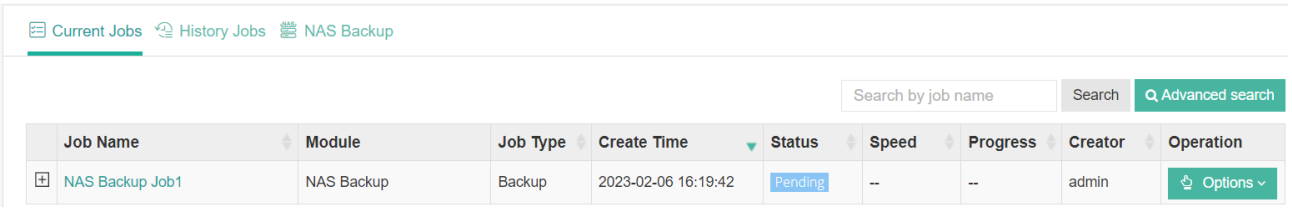
Step 4: Review & Confirm

After completing the above-mentioned settings, you are able to review and confirm the NAS backup job settings in one screen.

You can give this job a customized name then click on **Submit** to finish creating this NAS backup job.

NAS Backup Job Management

Once a NAS backup job had been created, you will be redirected to the **Monitor Center** > **Jobs** page.



The newly created NAS backup job will be in pending status, you can start, stop, edit or delete the job from the current job list.

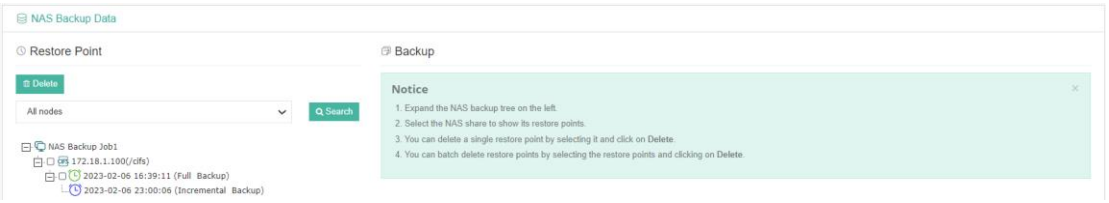
NAS Backup Data

After running each NAS backup job session, all the NAS backup data can be found and managed from **NAS Backup** > **Backup Data** page.

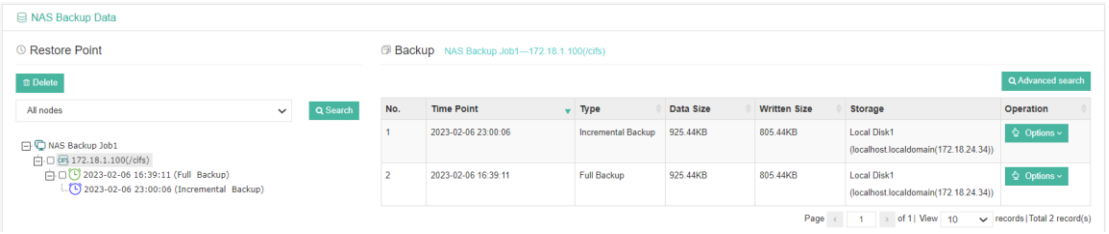
View Backup Data

By default, all NAS backups of all backup nodes from Vinchin backup infrastructure will be displayed, if you wish to view backups of a specific backup node, please select a node from the dropdown list.

The NAS backup data is organized with Backup Job > NAS Share > Restore Point structure as shown below.



Each restore point is named with the timestamp of its creation and will be marked with its backup type. To view more information of the restore points, simply click on the NAS share name, all the restore points of the selected NAS share will be listed on the right with more detailed information.



You can get more information like the actual data size, written size and the storage which is used to store the NAS backup data.

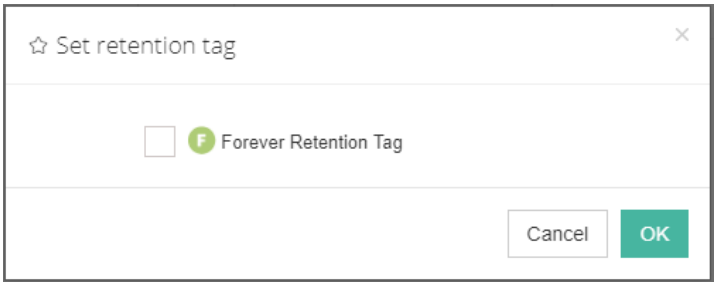
To search specific restore point(s), you can use the **Search** button on the left or use the **Advanced search** button at the right side of the **Restore Point List**.

You can also comment on the target recovery point by clicking **Options** and then select **Comment**.

Retention Tags

The purpose of using the retention tags is to avoid the general retention policy from purging some specific backups and keep them for a longer time period. For NAS Backup, the **F** (forever retention) tag can be set for the full restore points of NAS backup.

To manually set retention tags, please go to **NAS Backup > Backup Data** page. By selecting a NAS share from a backup job, all the restore points will be listed on the right, find the full restore point which you wish to set/unset retention tags and click **Options** button, and then select **Set Retention Tag**.



In the popup dialog you can set/unset retention tags for the selected full restore point.

Delete Backup Data

We recommend configuring comprehensive retention policies for the NAS backup jobs to automatically purge the out-of-date backups instead of manual deletion of the backup data. It is a highly risk operation by deleting the backup data manually. If you have to do this, please follow the below instructions.

To delete NAS backup data, please go to **NAS Backup** > **Backup Data** page. There are two approaches to perform the deletion, batch (or single) deletion of restore points from the left side tree view and single restore point deletion from the right side restore point list view.

Deleting restore point(s) from the tree view.

Please unfold the associated backup job, and unfold the NAS share which you wish to delete backup data from. Then select the restore point(s) you wish to be deleted and click on the **Delete** button on the top left of the tree view. You'll have to provide you password to confirm the deletion of selected restore point(s).

If it's a standalone full restore point, no incremental or differential restore points dependent on it, you can select and delete the standalone full restore point directly.

If it's a backup chain, formed by a full restore point and a series of incremental (or differential) restore points dependent on the full restore point, you can only delete the backup chain from the tree view.

Deleting restore point from the restore point list view.

Please select a NAS share from the left tree, the associated restore points will be listed on the right-side list view. By clicking on the **Options** button of a specific restore point and selecting **Delete** you are able to delete that single full restore point, and the incremental/differential restore point dependent on it will be delete together. Single incremental/differential restore point cannot be deleted.

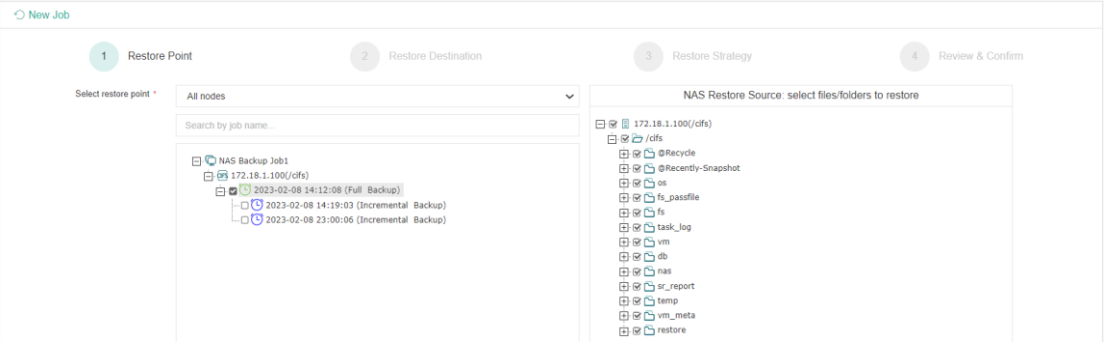
Create NAS Restore Job

To restore files from NAS backup restore points, please go to **NAS Backup** > **Restore** page. There are 4 steps to restore files from the NAS backup restore points.

Step 1: Restore Point

First you need to select a target NAS share and a desired restore point from the **Select Restore Point** column.

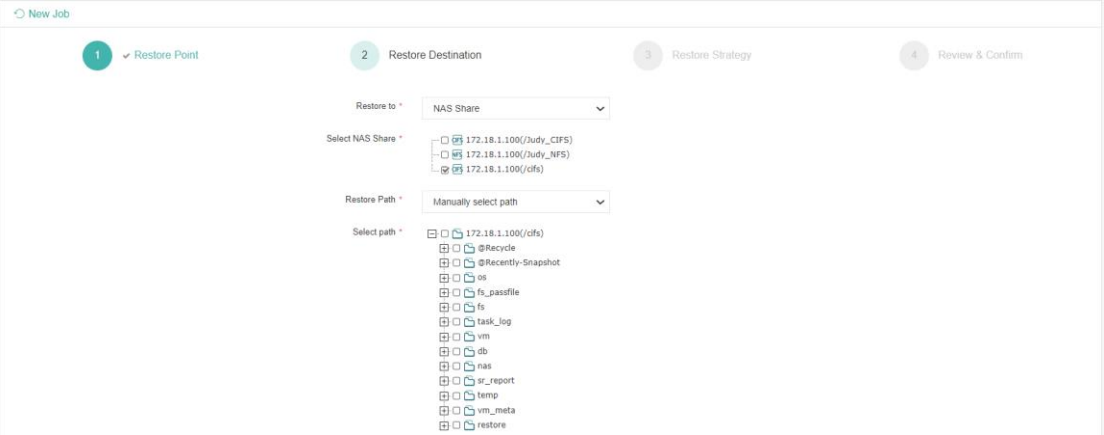
Then select the desired files/folders from the **NAS Restore Source** column.



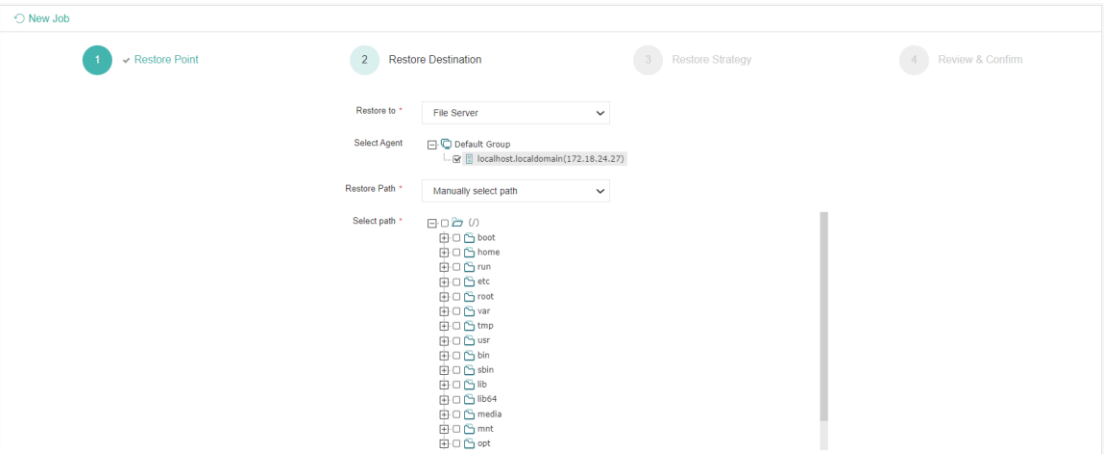
When done selecting files/folders, click on **Next** button to continue.

Step 2: Restore Destination

By default, the files/folders will be restored to the NAS share.
And when you selected the target NAS share, please select restore path, the default is manually select path, you can select the desired host or the desired path then continue.



If you want to restore to the original path, select recover to the original path and click on Next to continue.
If you want to restore to a file server, in **Restore to** dropdown list, select a file server, and then select the agent you desire, select the path you want to restore the files/folders then continue.



Notice

The files/folders can be only restored to the NAS shares/file servers that have been registered to Vinchin Backup Server.

Step 3: Restore Strategy

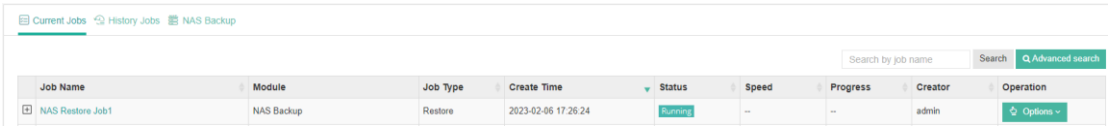
In the General Strategy it including Speed Controller and Advanced Strategy.
Similar to NAS backup, the speed controller is optional, it is used to limit the transmission speed of NAS restore. And in Advanced Strategy, you can set 1 to 32 transfer threads for a single NAS restore job.

Click on **Next** button to continue.

Step 4: Review & Confirm

After finishing the above settings, you are able to review and confirm all settings here. Click **Submit** to confirm creating this job.

Once the job has been created, you'll be redirected to the **Monitor Center** > **Jobs** page.



As the NAS restore job is by default to be executed right after the creation of the job, so it will run automatically, when you see it in the current job list, it should be in running status already, and once completed, the job will be automatically deleted from the current job list.

After this you can browse the restored files/folders from the selected NAS share/file server in the selected path.

Backup Copy

Backup copy is a feature which can be used to make duplicated version of your backup data to a secondary storage (onsite copy) or location (offsite copy). The copy data is usually of the same version, size and type of your original backup data, and can be used to restore the backup data from any accidental deletion and corruption.
Vinchin Backup & Recovery enabled backup copy for the following type of data assets.

- VM backups
- File backups
- Database backups
- Server backups
- NAS backups

Prerequisites of Backup Copy

Onsite Backup Copy

To make a copy of your backup data onsite, please check the following prerequisites:

- Vinchin backup server should be at least licensed with Standard Edition license.
- Vinchin backup server/node must have an onsite backup copy storage added.
- A backup job must be created before creating a backup copy job.

Offsite Backup Copy

To make a copy of your backup data offsite, please check the following prerequisites:

- Primary site Vinchin backup server should be at least licensed with Standard Edition license.
- A backup job must be created on primary Vinchin backup server before creating a copy job.
- Remote site must have a Vinchin backup server installed and an onsite backup copy storage must be added.
- Primary site and remote site should be interconnected via dedicated connection or VPN connection, if there's firewall, service ports 22804 and 23005 need to be accessible on the remote site Vinchin backup server. If the connection goes directly through Internet, the remote site must have a dedicated public IP address, and on the remote site firewall/router, the service ports 22804 and 23005 need to be opened for the remote site Vinchin backup server.
- Bandwidth between 2 sites must be fast enough to transfer new backup data generated during the previous copy job session to the next copy job session.

Notice
For offsite copy feature, the remote site Vinchin backup server does not necessarily to be licensed with a paid license. Use a free trial license for testing or if you had applied paid license for the onsite Vinchin server, you can contact Vinchin sales representative to get a free license for offsite copy.

VM Copy

Create VM Copy Job

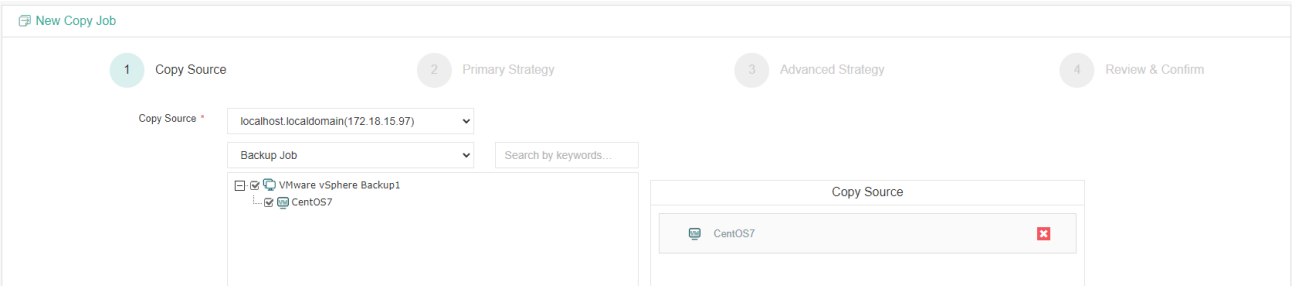
To create a VM copy job, please go to **VM Backup** > **Backup Copy** > **Copy** page, then follow the below steps to create the VM copy job.

Step 1: Select Coy Source

To select the backup copy source, first please select the Copy Source then choose the source node and filter the backup data by Backup Job, Virtual Platform or Restore Points.

- If you select Backup Job, all backup jobs will be listed, by expanding the backup job you can select the copy source as per the VMs included in the backup job.
- If you select Virtual Platform, the virtual platform will be listed and you could select corresponding VMs to copy the backup data of the selected VMs.
- If the backup job has been deleted or it's a once-off backup job, you can filter the backup data by selecting Restore Points.

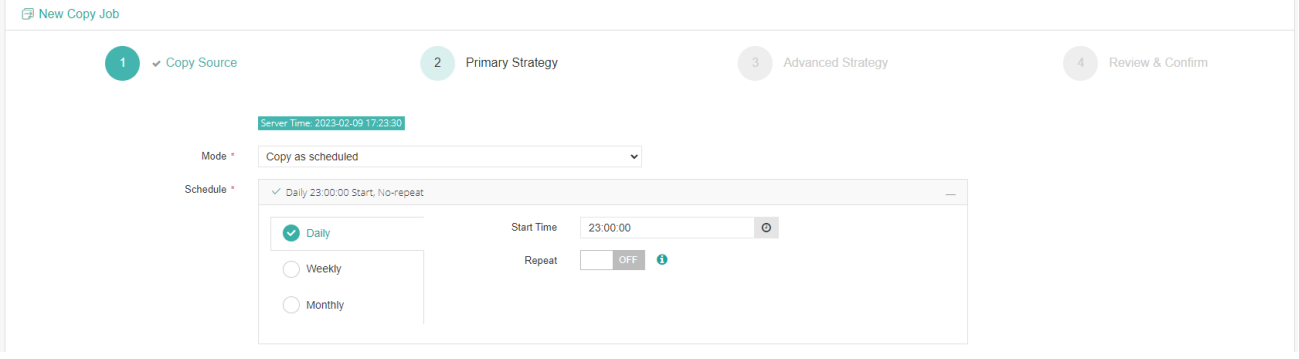
You can select the copy source either way as per your convenience.



Once the copy source is selected, please click on Next button to continue.

Step 2. Configure Primary Strategies

For Primary Strategy, you can set the backup copy mode, options are **Copy as scheduled** and **Once-off copy**. Copy as scheduled is suitable for the regularly scheduled backup jobs.

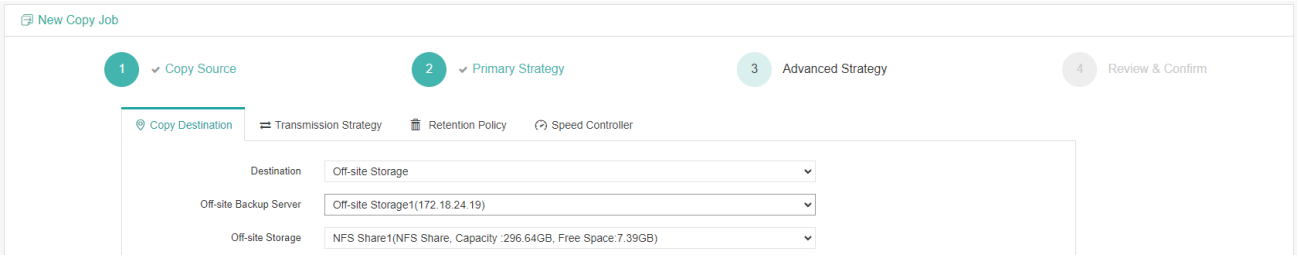


You can set the copy schedule as per the backup job schedule. But the schedules of backup copy job should not be more frequently than the schedules of backup job.
If you wish the backup copy to run regularly as per the backup job runs, please set **Copy as Scheduled**, otherwise set **Once-off Copy** to run the copy job for only once.
As for the schedule of the copy job, it is recommended to run the copy job right after the backup job finishes. For example, the backup job runs at 11 PM each day, and it takes approximately 2 hours to complete the backup job, so you can set the copy job to start 3 or 4 hours later than the backup job.
After done the mode settings, click on the **Next** button to continue.

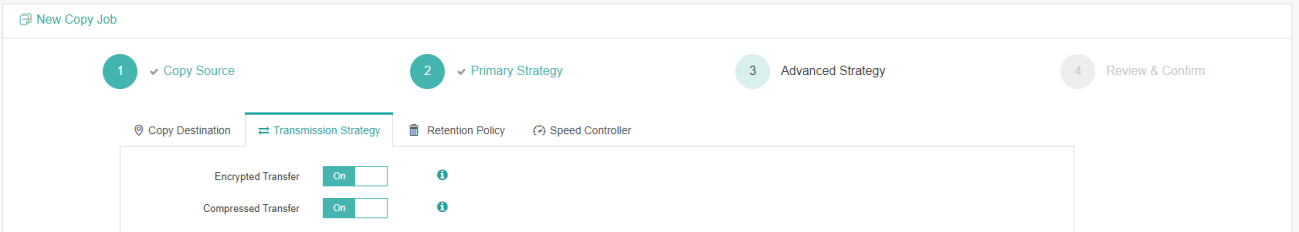
Notice
If the VM copy job mode is copy as scheduled, then the first time running this backup copy job, all the backup data (restore points) will be copied to the backup copy storage, the next time running this job, only the new backup data will be copied. This will keep the backup copy data identical with the backup data, but stored in different storages (or locations).

Step 3. Configure Advanced Strategies

For the **Copy Destination**, VM copy can be stored in the On-site Storage or Off-site Storage. An on-site backup copy storage is a storage which had been added to local Vinchin Backup Server or local Vinchin Backup Node. An off-site backup copy storage is a backup storage added to remote site Vinchin Backup Server deployed in another location. Please select the corresponding storage destination as per your actual deployment and requirements, here we take off-site storage as an example.



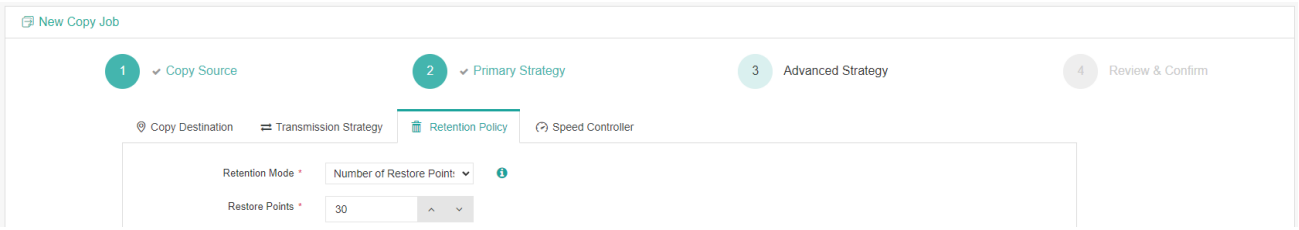
In the Destination dropdown list, Off-site Storage should be selected.
In the Off-site Backup Server dropdown list, select the target remote Vinchin backup server.
Once the remote Vinchin backup server had been selected, the backup copy storage added on the remote backup server will be loaded automatically, and if there're multiple backup copy storages you can select one from the dropdown list.
For the **Transmission Strategy** settings including Encrypted Transfer and Compressed Transfer.



Encrypted Transfer: The data transmitted from backup source to backup copy storage will be encrypted to ensure the safety of the data transmission.
Compressed Transfer: Enable it to compress the backup data during transmission. The backup data will be

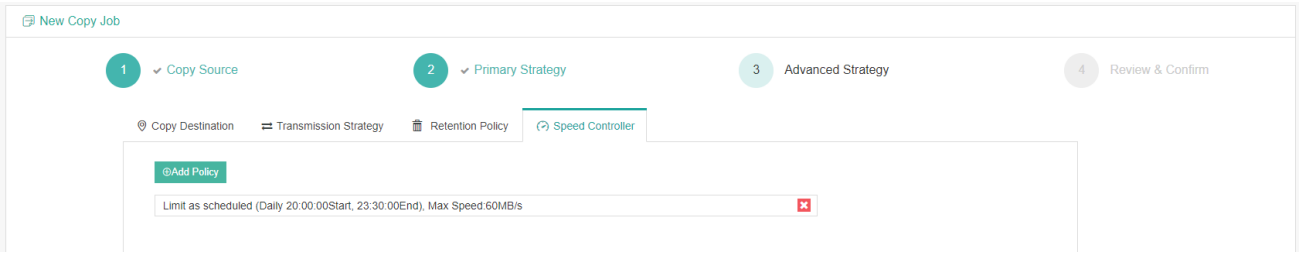
decompressed when it arrives the backup copy storage.

For **Retention Policy**, VM copy retention policy is similar with the backup retention policy, it is used to reserve backup copy data stored on the backup copy storage.



There's only **Number of Restore Points** retention mode for backup copy jobs, Vinchin Backup Server will save the specified number of restore points for each VM included in the copy job, the older restore points will be deleted or merged (restore point merge is only applicable for VM restore points) to comply with the retention policy.

For **Speed Controller**, it's optional, only if the VM copy jobs will bring network or I/O overload to your production environment, you can configure the speed controller accordingly.



The speed controller can be configured as a Permanent or As Scheduled policy.

Step 4. Review and Confirm Job Settings

After completing the above settings, you are able to review and confirm the settings.

You can optionally customize a job name and then click on Submit button to confirm the creation of this VM copy job.

VM Copy Job Management

Once a VM copy job had been created, you will be redirected to the **Monitor Center** > **Jobs** page.

The job status will be pending, and it should be automatically executed according to the scheduled time. You are also able to manually run the job by clicking on **Options** and select **Start Job**. Or if you want to stop the job, you can click on **Options** and select **Stop**.

After the backup copy job is completed, the backup copy data will be stored in the target backup copy storage. And if it's a once-off copy job, the job will be automatically deleted once completed, if it's a scheduled backup copy job, the job status will change to pending again and wait for the next run.

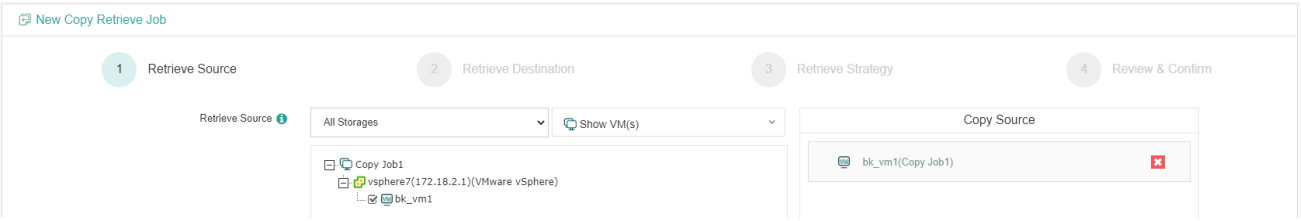
VM Copy Retrieve

The onsite VM copy data can be used to restore VMs directly without copy retrieve. But for the backup copy data stored on the off-site backup copy storage cannot be used to restore VMs directly to primary site, it should be retrieved to an on-site storage first, then from the **VM Backup** > **Restore** page you can create restore jobs to restore the VMs.

To create a VM copy retrieve job, please go to **VM Backup** > **Backup Copy** > **Copy Retrieve** page, then follow the steps below to create a copy retrieve job.

Step 1: Retrieve Source

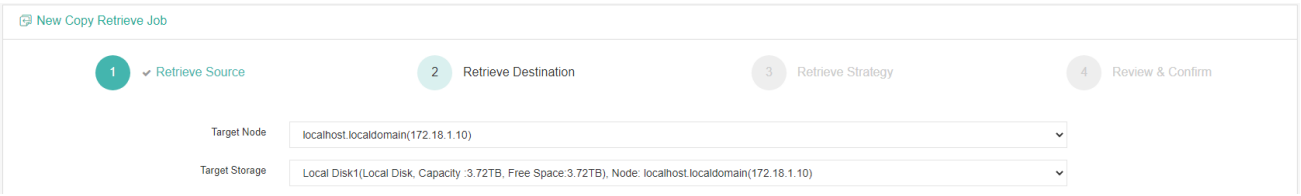
To retrieve VM copy from offsite storage, please select an off-site backup copy storage, and select the **Show VM(s)** or **Show Restore Points** as per your requirements.



Select the desired VM(s) or restore point(s) then click on **Next** to continue.

Step 2: Retrieve Destination

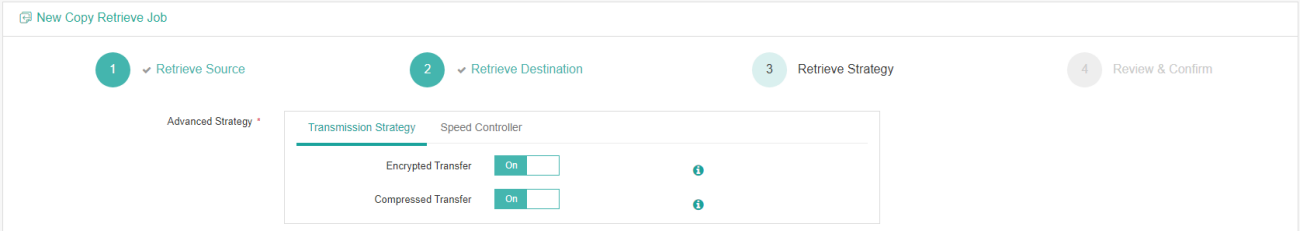
Select an on-site storage where you want to save the restored backup copy data.



Either local backup or local (onsite) copy storage can be used to store the retrieved VM copy data.

Step 3: Retrieve Strategy

Retrieve strategy including Encrypted Transfer and Compressed Transfer.



Encrypted Transfer: The data transmitted from off-site backup copy storage to on-site storage will be encrypted to ensure the safety of the data transmission.

Compressed Transfer: Enable it to compress the copy data during transmission. The copy data will be decompressed when it arrives the on-site storage.
Speed Controller: It is optional, only if the copy retrieve jobs will bring network or I/O overload to your production environment, you need to configure the speed controller accordingly.

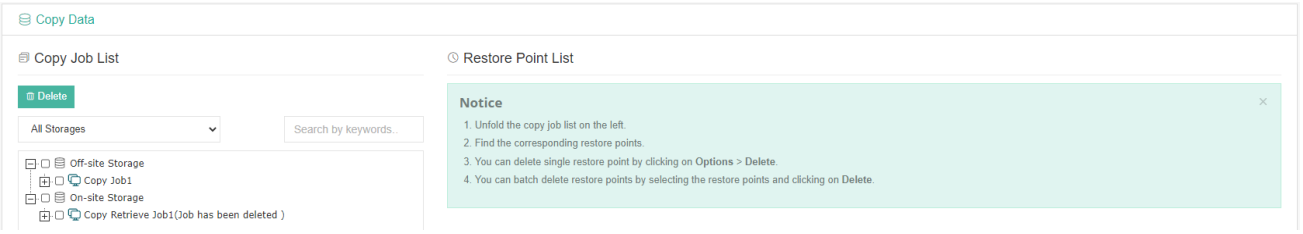
Step 4: Review & Confirm

After completing the above settings, you are able to review and confirm the settings.
You can optionally customize a job name and then click on Submit button to confirm the creation of this copy retrieve job.
After a new copy retrieve job has been created, you will be redirected to the **Monitor Center** > **Jobs** page, and you will immediately see the copy retrieve job run automatically.
Once the copy retrieve job is completed, the job will be automatically deleted from the current job list.
Now you can go to **VM Backup** > **Restore** page and create a VM restore job with the retrieved VM copy data.

Notice
If you have virtual platform on the remote DR site, you can restore the backed up VMs on remote site virtual platform using the backup copy data transferred from the primary site to the remote site backup copy storage on the off-site Vinchin Backup Server.

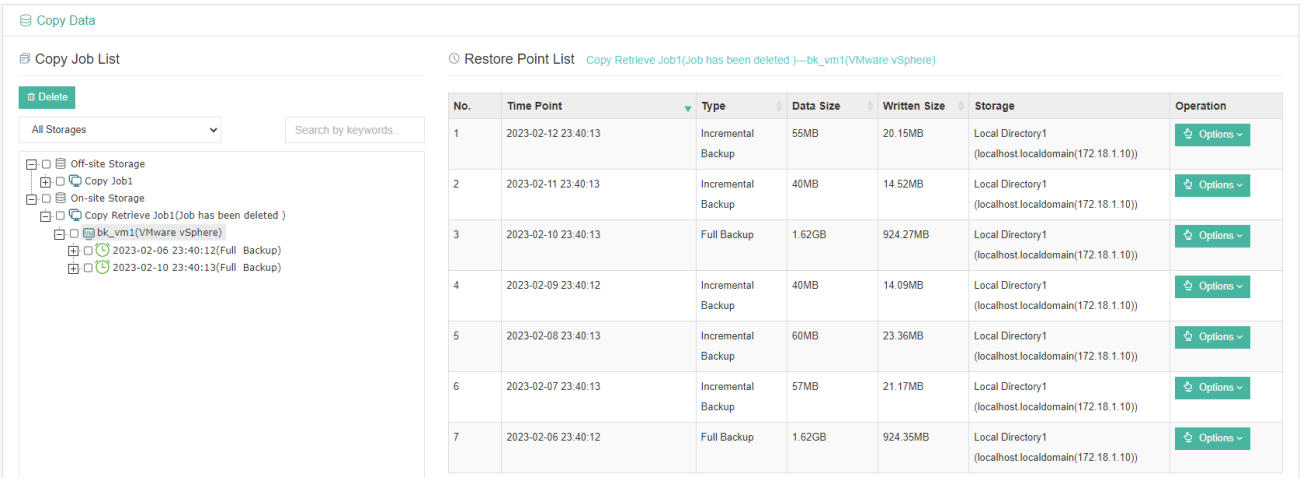
VM Copy Data

All VM copy data can be managed from the **VM Backup** > **Backup Copy** > **Copy Data** page. No matter the data is stored in the on-site storage or off-site storage.



By unfolding the copy storages and the copy jobs, you are able to view all the copy data. And by selecting corresponding restore points, copy job or the copy storage, you are able to delete the selected copy data.

By clicking on a virtual machine, you'll be able to see all the copy restore points of the virtual machine.



By clicking on **Options**, you will be able to comment, delete or set retention tag for the restore point.

The tagged restore point(s) will be marked with an **F** (forever retention tag) and be kept permanently, even the retention policy will not delete the restore point(s) with an **F** tag.

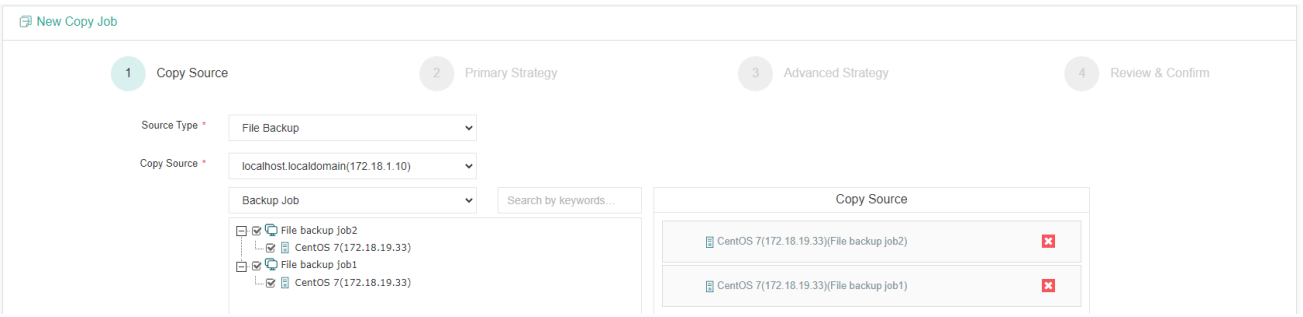
File Copy

Create File Copy Job

To create a file copy job, please go to **Physical Backup** > **Backup Copy** > **Copy** page, then follow the below steps to create the file copy job.

Step 1: Copy Source

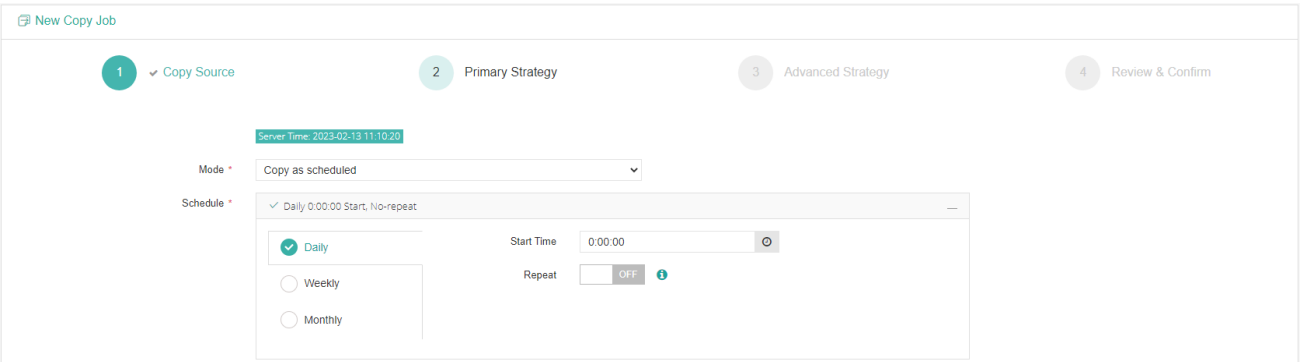
In the **Source Type** dropdown list, please select **File Backup**. Then in the Copy Source dropdown list, please select a backup node on which the file backups are stored.



All the file backup jobs will be listed, please select the jobs/file servers for which you wish to copy the backups.

Step 2: Primary Strategy

For a file copy job, it can be configured as a **Copy as Scheduled** or **Once-off Copy** mode. Copy as scheduled is suitable for the regularly scheduled file backup jobs.



You can set the copy schedule as per the backup job schedule. But the schedules of backup copy job should not be more frequently than the schedules of backup job.

If you wish the file copy to run regularly as per the backup job runs, please set **Copy as Scheduled**, otherwise set **Once-off Copy** to run the copy job for only once.

As for the schedule of the copy job, it is recommended to run the copy job right after the backup job finishes. For example, the backup job runs at 11 PM each day, and it takes approximately 2 hours to complete the backup job, so you can set the copy job to start 3 or 4 hours later than the backup job.

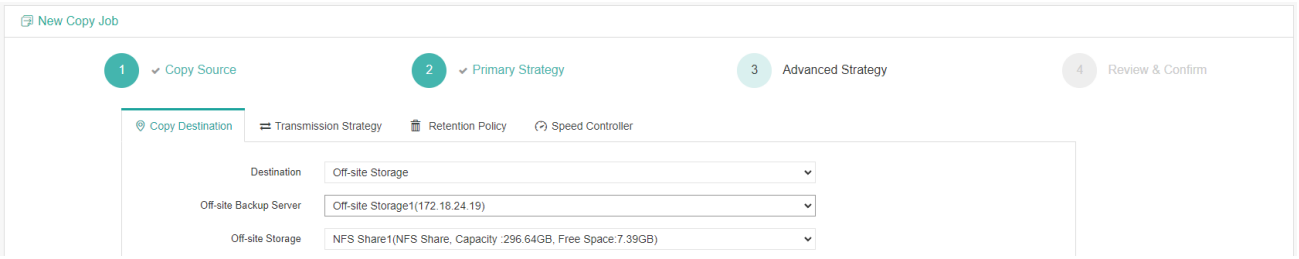
After done the mode settings, click on the **Next** button to continue.

Notice

If the file copy job mode is copy as scheduled, then the first time running this backup copy job, all the backup data (restore points) will be copied to the backup copy storage, the next time running this job, only the new backup data will be copied. This will keep the backup copy data identical with the backup data, but stored in different storages (or locations).

Step 3: Advanced Strategy

For the **Copy Destination**, file copy can be stored in the On-site Storage or Off-site Storage. An on-site backup copy storage is a storage which had been added to local Vinchin Backup Server or local Vinchin Backup Node. An off-site backup copy storage is a backup storage added to remote site Vinchin Backup Server deployed in another location. Please select the corresponding storage destination as per your actual deployment and requirements, here we take off-site storage as an example.

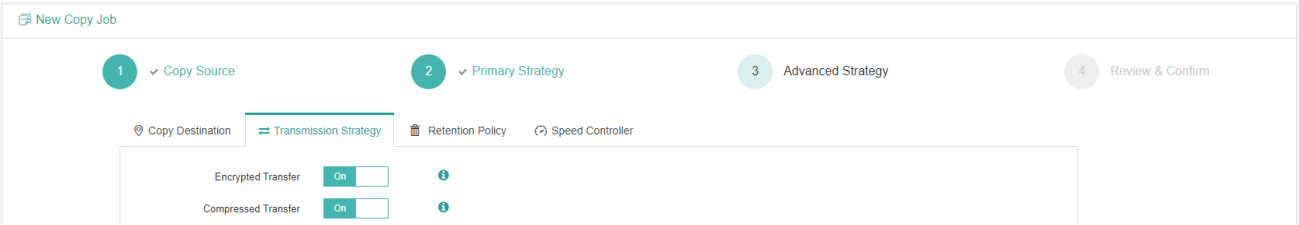


In the **Destination** dropdown list, **Off-site Storage** should be selected.

In the **Off-site Backup Server** dropdown list, select the target remote Vinchin backup server.

Once the remote Vinchin backup server had been selected, the backup copy storage added on the remote backup server will be loaded automatically, and if there're multiple backup copy storages you can select one from the dropdown list.

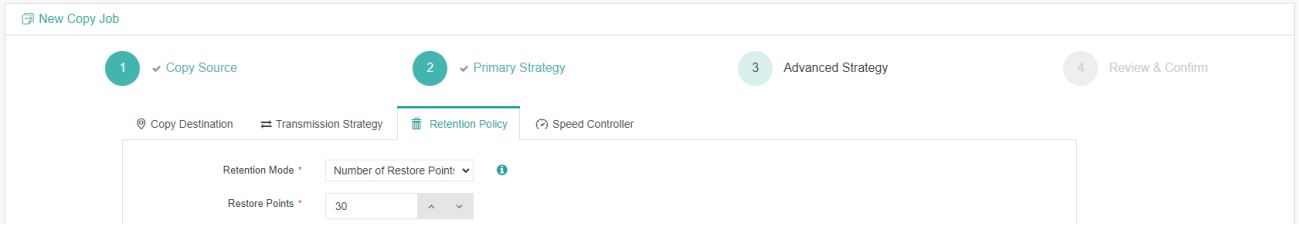
For the **Transmission Strategy** settings users can enable **Encrypted Transfer** and **Compressed Transfer**.



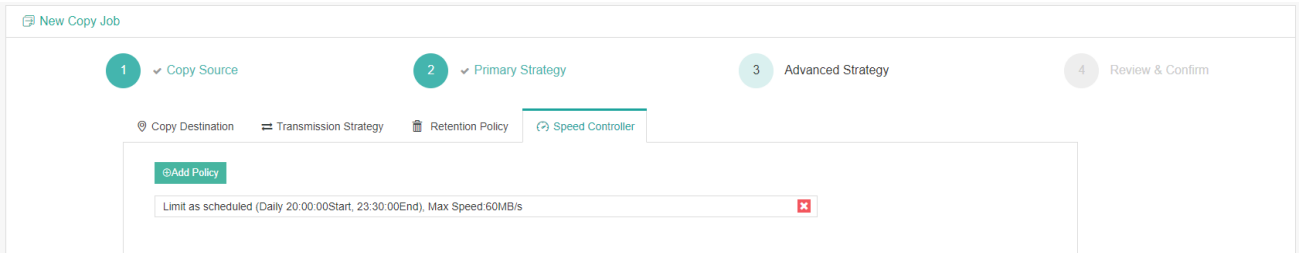
Encrypted Transfer: the transmission path between Vinchin backup server and the target storage will be encrypted to secure the data transmission process.

Compressed Transfer: the backup data will be compressed then be transferred to the copy storage, it can reduce the bandwidth consumption during backup copy process.

For **Retention Policy**, file copy retention policy is similar with the file backup retention policy, it is used to reserve backup copy data stored on the backup copy storage.



There's only **Number of Restore Points** retention mode for file copy jobs, Vinchin Backup Server will save the specified number of restore points for each file server included in the copy job, the older restore points will be deleted.
For **Speed Controller**, it's optional, only if the file copy jobs will bring network or I/O overload to your production environment, you can configure the speed controller accordingly.



The speed controller can be configured as a Permanent or As Scheduled policy.

Step 4: Review & Confirm

After completing the above settings, you are able to review and confirm the job settings.
You can optionally customize a job name and then click on **Submit** button to confirm the creation of this file copy job.

File Copy Job Management

Once a file copy job had been created, you will be redirected to the **Monitor Center** > **Jobs** page.
The job status will be pending, and it should be automatically executed according to the scheduled time. You are also able to manually run the job by clicking on **Options** and select **Start Job**. Or if you want to stop the job, you can click on **Options** and select **Stop**.
After the backup copy job is completed, the backup copy data will be stored in the target backup copy storage. And if it's a once-off copy job, the job will be automatically deleted once completed, if it's a scheduled backup copy job, the job status will change to pending again and wait for the next run.

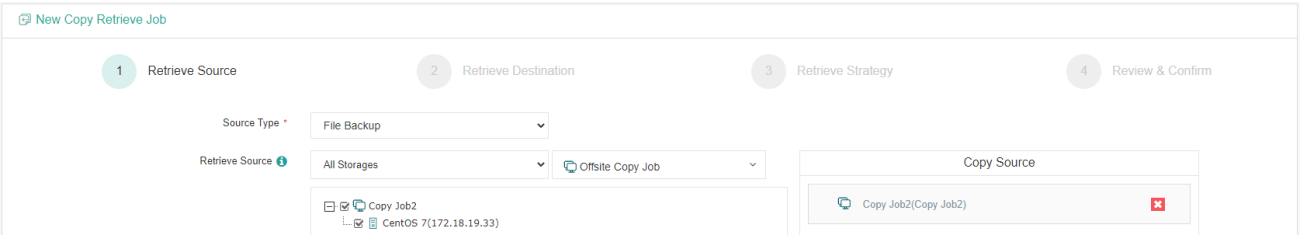
File Copy Retrieve

The onsite file copy data can be used to restore files directly without copy retrieve. But for the backup copy data stored on the off-site backup copy storage cannot be used to restore files directly to primary site, it should be retrieved to an on-site storage first, then from the **Physical Backup** > **File Backup > Restore** page you can create restore jobs to restore the files.
To create a file copy retrieve job, please go to **Physical Backup** > **Backup Copy** > **Copy Retrieve** page, then follow the steps below to create a copy retrieve job.

Step 1: Retrieve Source

To retrieve file copy from offsite storage, please first select **File Backup** in the **Source Type** dropdown list, then select

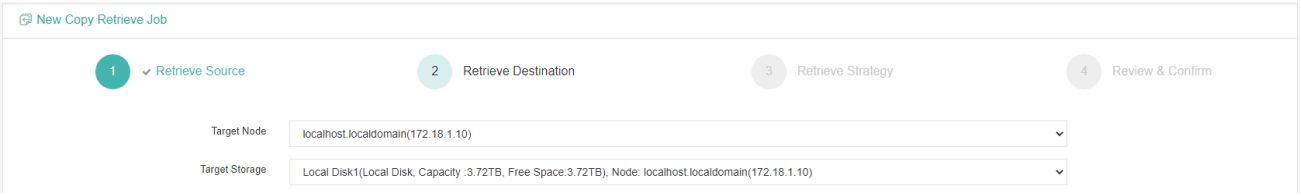
an off-site backup copy storage.



Select the desired file server(s) or restore point(s) of the file server(s) then click on **Next** to continue.

Step 2: Retrieve Destination

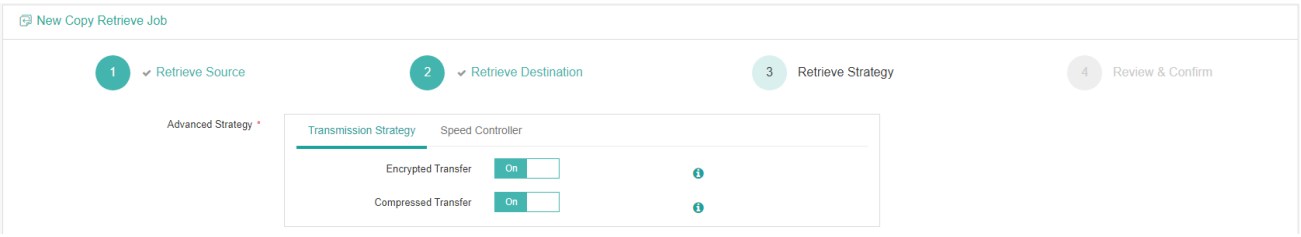
Select an on-site storage where you want to save the restored backup copy data.



Either local backup or local (onsite) copy storage can be used to store the retrieved file copy data.

Step 3: Retrieve Strategy

Retrieve strategy including Encrypted Transfer, Compressed Transfer and Speed Controller.



Encrypted Transfer: The data transmitted from off-site backup copy storage to on-site storage will be encrypted to ensure the safety of the data transmission.
Compressed Transfer: Enable it to compress the copy data during transmission. The copy data will be decompressed when it arrives the on-site storage.
Speed Controller: It is optional, only if the copy retrieve jobs will bring network or I/O overload to your production environment, you need to configure the speed controller accordingly.

Step 4: Review & Confirm

After completing the above settings, you are able to review and confirm the settings.
You can optionally customize a job name and then click on Submit button to confirm the creation of this copy retrieve job.
After a new copy retrieve job has been created, you will be redirected to the **Monitor Center** > **Jobs** page, and you will immediately see the copy retrieve job run automatically.
Once the copy retrieve job is completed, the job will be automatically deleted from the current job list.

Now you can go to **Physical Backup > File Backup** > **Restore** page and create a file restore job with the retrieved file copy data.

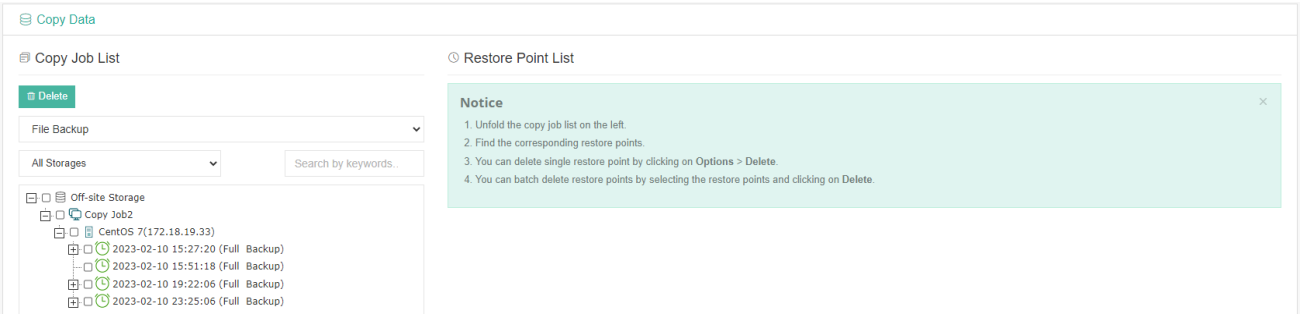
Notice

If needed, you can restore the files on remote site file servers using the backup copy data transferred from the primary site to the remote site backup copy storage on the off-site Vinchin Backup Server.

File Copy Data

The copy data for file backup can be managed from the **Physical Backup** > **Backup Copy** > **Copy Data** page. No matter the data is stored in the on-site storage or off-site storage.

The default source type from **Copy Data** page is **File Backup**, the file copy data will be listed on this page directly.



By unfolding the copy storages and the copy jobs, you are able to view all the copy data. And by selecting corresponding restore points, you are able to delete the selected copy data with the **Delete** button on the top left.

In the Restore Point List on the right, by clicking on the **Options** button, users can comment, delete or set retention tags for the restore points.

Users can comment on all restore points, no matter full, incremental or differential.

Deletion of restore points can be only performed with the full restore point, but the dependent incremental or differential restore points will be deleted along with the full restore points.

As for setting retention tags, only full restore points can be set with a forever retention tag, and the full restore point with a forever retention tag, its dependent incremental or differential restore points will be reserved permanently along with the full restore point.

Setting retention tags for the onsite copy data can be done directly from the web console of local Vinchin server, but for the offsite copy data, it needs to be done on the web console of the remote Vinchin server.

Database Copy

To create a database copy job, please go to **Physical Backup** > **Backup Copy** > **Copy** page.

Create Database Copy Job

The principle of creating a database copy job is similar with creating a file copy job, in the **Source Type** dropdown list, please select **Database Backup**, then please follow the instructions of Create File Copy Job to create a database copy job.

Database Copy Retrieve

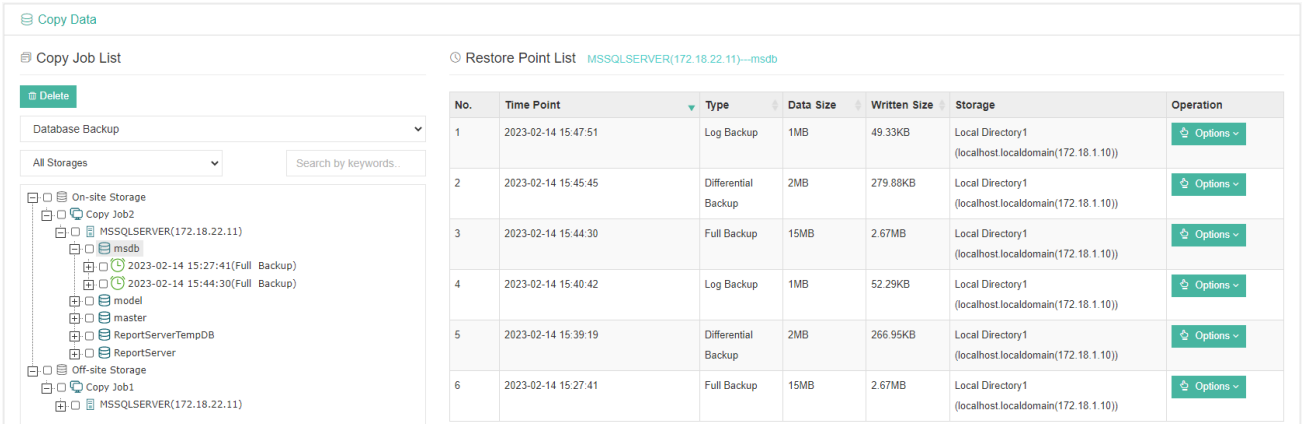
The onsite database copy data can be used to restore databases directly without copy retrieve. But for the backup copy data stored on the off-site backup copy storage cannot be used to restore directly to primary site, it should be retrieved to an on-site storage first, then from the **Physical Backup > Database Backup > Restore** page you can create restore jobs to restore the databases.

To create a database copy retrieve job, please go to **Physical Backup** > **Backup Copy** > **Copy Retrieve** page, then refer to File Copy Retrieve to create a copy retrieve job.

Database Copy Data

The copy data for database backup can be managed from the **Physical Backup** > **Backup Copy** > **Copy Data** page. No matter the data is stored in the on-site storage or off-site storage.

Please select **Database Backup** as the copy data type from the dropdown list to show database copy data.



By unfolding the copy storages and the copy jobs, you are able to view all the copy data. And by selecting corresponding restore points, you are able to delete the selected copy data with the **Delete** button on the top left.

In the Restore Point List on the right, by clicking on the **Options** button, users can comment, delete or set retention tags for the restore points.

Users can comment on all restore points, no matter full, incremental, differential or log backups.

Deletion of restore points can be only performed with the full restore point, but the dependent incremental or differential restore points will be deleted along with the full restore points.

As for setting retention tags, only full restore points can be set with a forever retention tag, and the full restore point with a forever retention tag, its dependent incremental, differential or log backup restore points will be reserved permanently along with the full restore point.

Setting retention tags for the onsite copy data can be done directly from the web console of local Vinchin server, but for the offsite copy data, it needs to be done on the web console of the remote Vinchin server.

Server Copy

To create a server copy job, please go to **Physical Backup** > **Backup Copy** > **Copy** page.

Create Server Copy Job

The principle of creating a server copy job is similar with creating a file copy job, in the **Source Type** dropdown list, please select **Server Backup**, then please follow the instructions of Create File Copy Job to create a server copy job.

Server Copy Retrieve

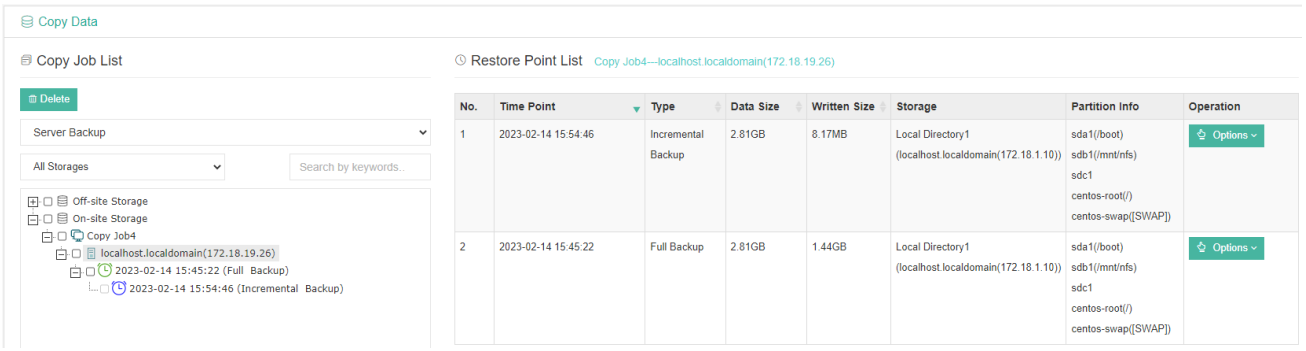
The onsite server copy data can be used to restore servers directly without copy retrieve. But for the backup copy data stored on the off-site backup copy storage cannot be used to restore directly to primary site, it should be retrieved to an on-site storage first, then from the **Physical Backup > Server Backup > Restore** page you can create restore jobs to restore the servers.

To create a server copy retrieve job, please go to **Physical Backup** > **Backup Copy** > **Copy Retrieve** page, then refer to File Copy Retrieve to create a copy retrieve job.

Server Copy Data

The copy data for server backup can be managed from the **Physical Backup** > **Backup Copy** > **Copy Data** page. No matter the data is stored in the on-site storage or off-site storage.

Please select **Server Backup** as the copy data type from the dropdown list to show server copy data.



By unfolding the copy storages and the copy jobs, you are able to view all the copy data. And by selecting corresponding restore points, you are able to delete the selected copy data with the **Delete** button on the top left.

In the Restore Point List on the right, by clicking on the **Options** button, users can comment and set retention tags for the restore points.

As for setting retention tags, an F tag will be added to the restore point and one the restore point has been tagged, it will not be deleted by the retention policy.

Setting retention tags for the onsite copy data can be done directly from the web console of local Vinchin server, but for the offsite copy data, it needs to be done on the web console of the remote Vinchin server.

NAS Copy

To create a NAS copy job, please go to **NAS Backup** > **Backup Copy** page.

Create NAS Copy Job

The principle of creating a NAS copy job is similar with creating a file copy job, in the **Source Type** dropdown list, please select **NAS Backup**, then please follow the instructions of Create File Copy Job to create a NAS copy job.

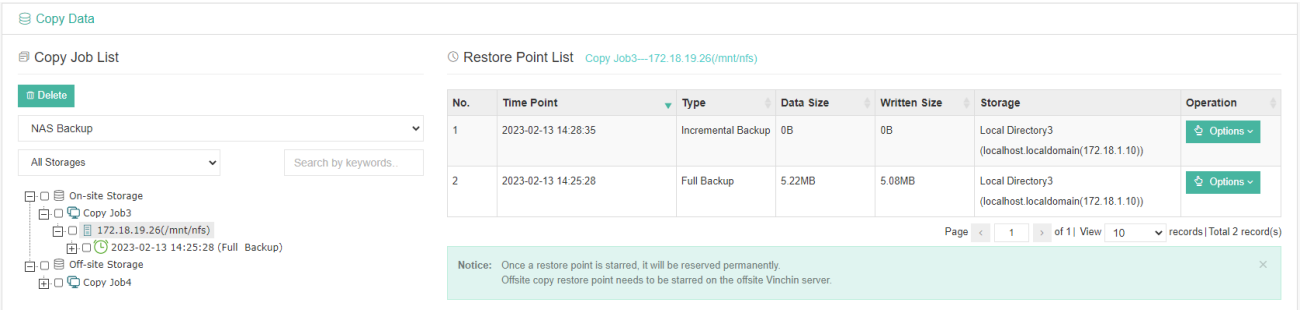
NAS Copy Retrieve

The onsite NAS copy data can be used to restore files directly without copy retrieve. But for the backup copy data stored on the off-site backup copy storage cannot be used to restore files directly to primary site, it should be retrieved to an on-site storage first, then from the **NAS Backup > Restore** page you can create restore jobs to restore the files.

To create a NAS copy retrieve job, please go to **NAS Backup** > **Backup Copy** > **Copy Retrieve** page, then refer to File Copy Retrieve to create a copy retrieve job.

NAS Copy Data

The copy data for NAS backup can be managed from the **NAS Backup** > **Backup Copy** > **Copy Data** page. No matter the data is storage in the on-site storage or off-site storage.



By unfolding the copy storages and the copy jobs, you are able to view all the copy data. And by selecting corresponding restore points, you are able to delete the selected copy data with the **Delete** button on the top left.

In the Restore Point List on the right, by clicking on the Options button, users can comment, delete or set retention tags for the restore points.

Users can comment on all restore points, no matter full, incremental or differential.

Deletion of restore points can be only performed with the full restore point, but the dependent incremental or differential restore points will be deleted along with the full restore points.

As for setting retention tags, only full restore points can be set with a forever retention tag, and the full restore point with a forever retention tag, its dependent incremental or differential restore points will be reserved permanently along with the full restore point.

Setting retention tags for the onsite copy data can be done directly from the web console of local Vinchin server, but for the offsite copy data, it needs to be done on the web console of the remote Vinchin server.

Backup Archive

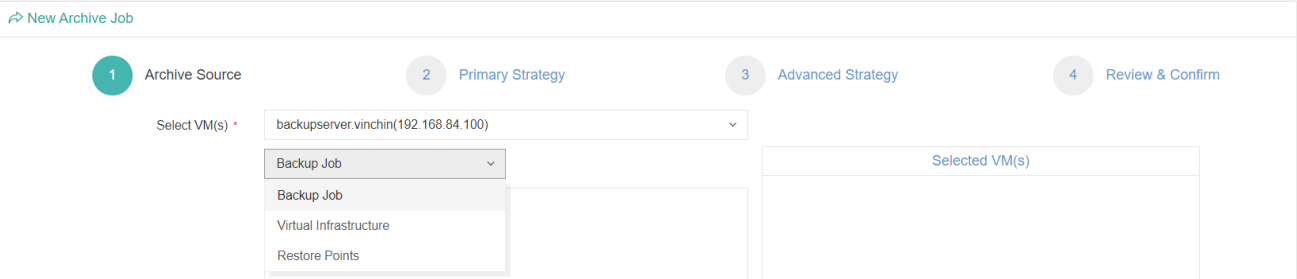
Here are the preconditions for a Backup Archive job to be completed successfully:
1. A backup archive storage had been added, for more details please refer to Storage Repository.
2. To run a backup archive job, a VM backup job should be completed at first place.

Create Archive Job

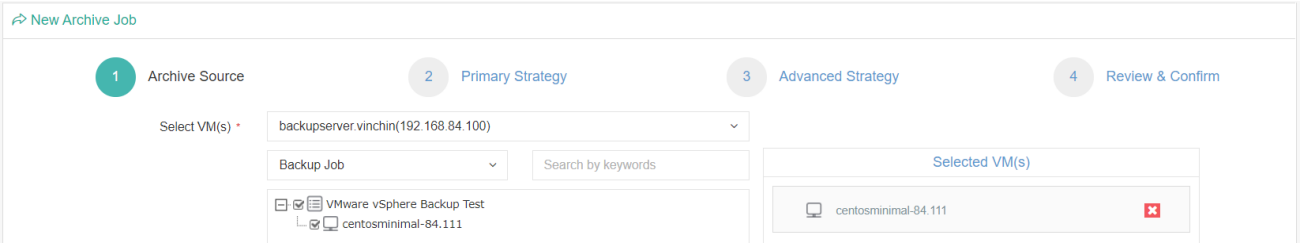
To create a backup archive job, please go to **VM Backup** > **Backup Archive** > **Archive** page, then follow the below steps to create the backup archive job.

Step 1: Archive Source

To select the backup archive source, first please select the backup node on which the backup data is stored, then you can select the backup data per Backup Job, Virtual Infrastructure or Restore Points.



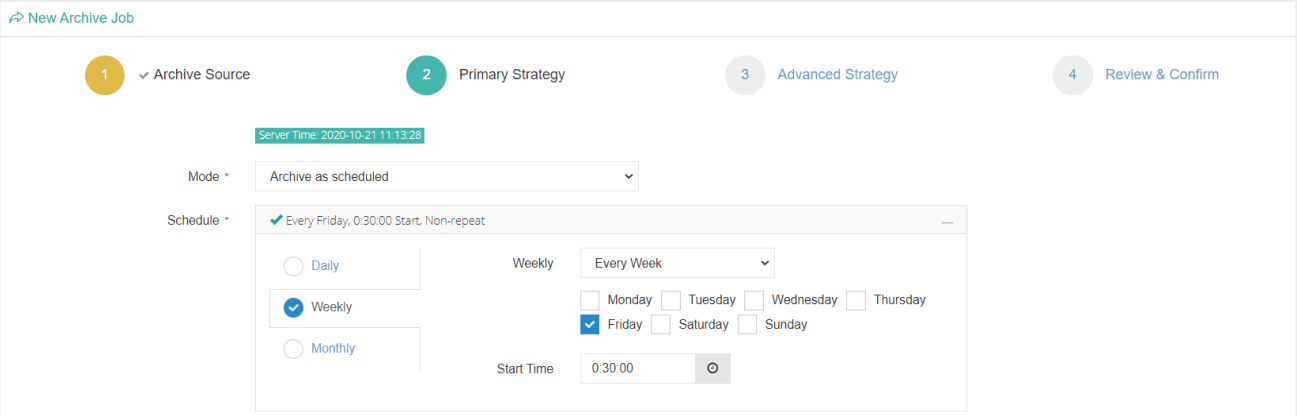
If you select **Backup Job**, existing backup jobs will be listed, by expanding the backup job you can select the archive source as per the VMs included in the backup job.
If you select **Virtual Platform**, the virtual platforms will be listed and you should select corresponding VMs to archive the backup data of the selected VMs.
If the backup job has been deleted or it's a once-off backup job, you can filter the backup data by selecting **Restore Points**.
You can select the archive source either way as per your convenience.



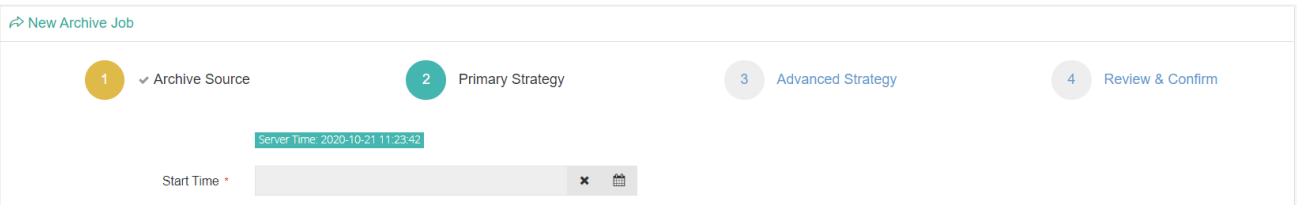
Once the archive source is selected, please click on **Next** button to continue.

Step 2: Primary Strategy

For **Primary Strategy**, you can set the backup archive mode, options are **Archive as Scheduled** and **Once-off Archive**. Archive as scheduled is suitable for the regularly scheduled backup jobs.



You can set the archive schedule on daily, weekly or monthly basis. Each time of the backup archive job will archive the latest backup restore point to the backup archive storage (native/cloud object storage).
Once-off archive can be used to archive the backup data for only once, when the archive source is selected with restore points, the backup archive mode will be once-off archive by default. And you can only set an individual running time point for the backup archive job.



After done the primary strategy settings, click on the **Next** button to continue.

Notice

The backup archive job will archive the latest restore point, even if the backup job you selected which has multiple restore points, when the archive job run for the first time the latest restore point will be archived.

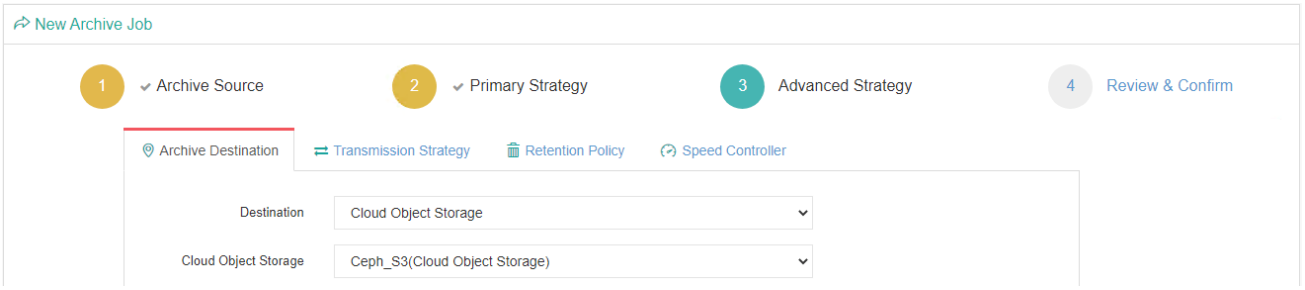
If the latest restore point is an incremental backup or differential backup, Vinchin Backup Server will merge this restore point with other dependent restore point(s) to a new full backup restore point and archive to the backup archive storage.

Each of the further archive jobs will always archive a latest full backup restore point to the backup archive storage.

Step 3: Advanced Strategy

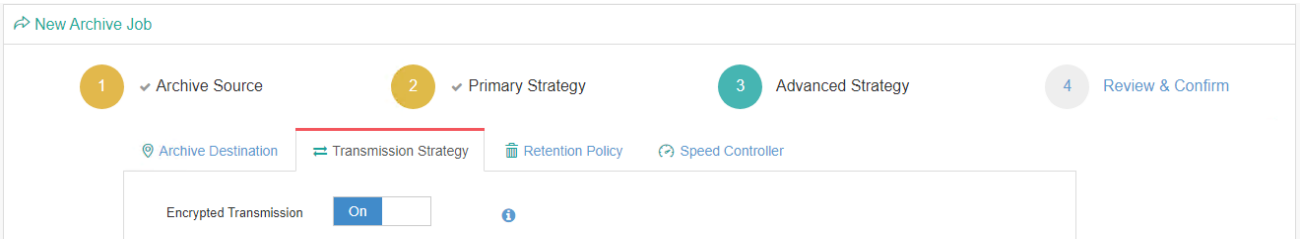
For the **Archive Destination**, VM backup archive can be stored in the On-site archive storage or cloud archive storage. An On-site backup archive storage is a storage which had been added to Vinchin Backup Server or Vinchin Backup Node locally. A cloud backup archive storage can be AWS S3, Ceph S3, MS Azure Blob, Alibaba, Wasabi cloud storage, etc.

Please select the corresponding storage destination as per your actual deployment and requirements, here we take Ceph S3 object storage as an example.



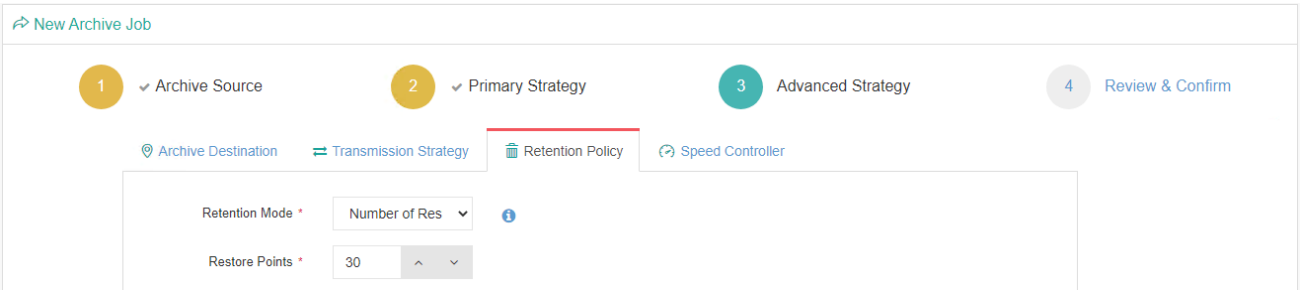
In the Destination field, Cloud Object Storage should be selected.
In the Cloud Object Storage field, the cloud storages added to Vinchin Backup Server will be available for selecting.

Under the **Transmission Strategy** tab, you can enable **Encrypted Transfer** option.



Encrypted Transfer: the transmission path between Vinchin backup server and the archive storage will be encrypted to secure the data transmission process.

The **Retention Policy** of the backup archive job can be configured per the number of restore points.



For example, if the number of restore points is configured as 30, there will always be 30 full backup restore points stored in the backup archive storage.

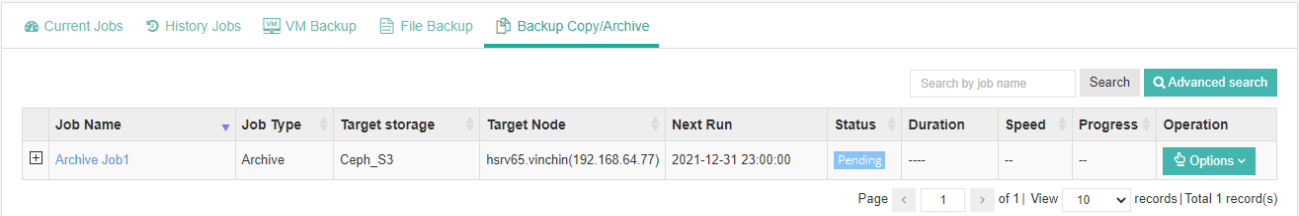
The speed controller settings are optional, only if the backup archive jobs will bring network or I/O overload to your production environment, you need to configure the speed controller accordingly.

Step 4: Review & Confirm

After completing the above settings, you are able to review and confirm the settings.
You can optionally customize a job name and then click on **Submit** button to confirm the creation of this backup archive job.

Archive Job Management

Once a backup archive job had been created, you will be redirected to the **Monitor Center** > **Jobs** page.



The job status will be pending, and it should be automatically executed according to the scheduled time. You are also able to manually run the job by clicking on **Options** and select **Start Job**. Or if you want to stop the job, you can click on **Options** and select **Stop**.

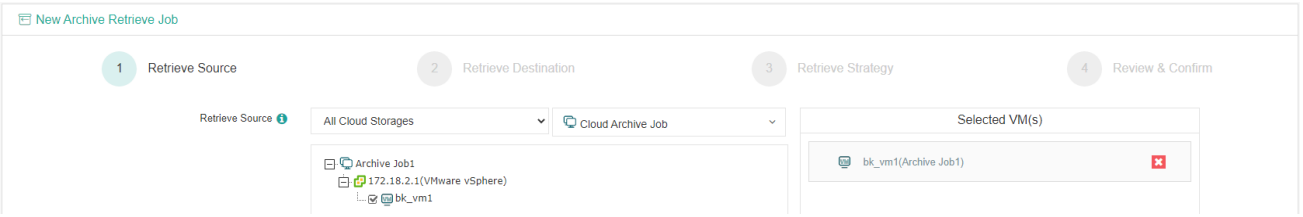
After the backup archive job is completed, the backup archive data will be stored in the target backup archive storage. And if it's a once-off backup archive job, the job will be automatically deleted once completed, if it's a scheduled backup archive job, the job status will change to pending again and wait for the next run.

Archive Retrieve

Backup archive data stored on the cloud storage cannot be used to restore virtual machine directly, it should be retrieved to an on-site storage first, then from the **VM Backup** > **Restore** page you can create a VM restore job to restore the virtual machine.
To create an archive retrieve job, please go to **VM Backup** > **Backup Archive** > **Archive Retrieve** page, then follow the steps below to create an archive retrieve job.

Step 1: Retrieve Source

Select a cloud storage which stores your archive data, and then select the restore point(s).



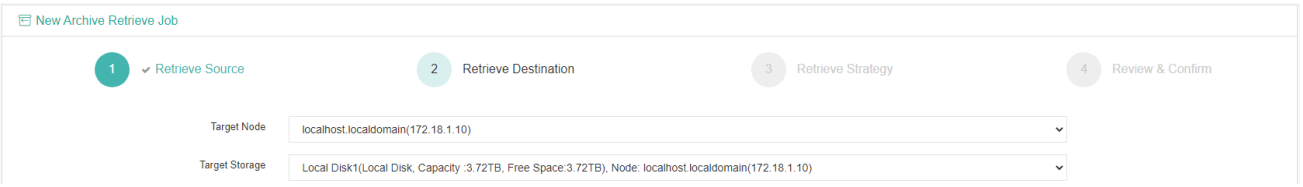
Click on **Next** to continue.

Notice

As the archive data stored on the on-site archive storage can be used to restore virtual machines directly, so you don't have to restore the on-site archive data.

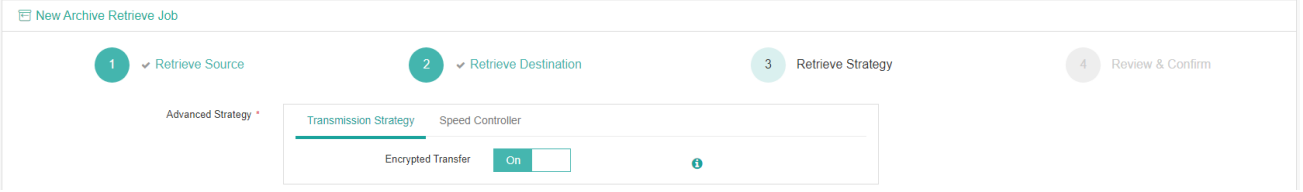
Step 2: Retrieve Destination

Select an on-site storage where you want to save the retrieved archive data.



Step 3: Retrieve Strategy

Retrieve strategy settings including Encrypted Transfer and Speed Controller.

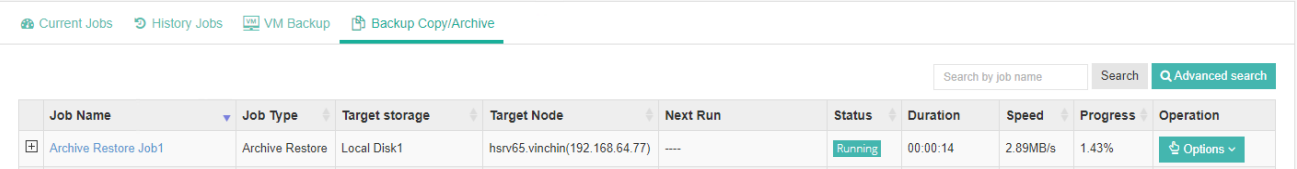


Encrypted Transfer: the transmission path between Vinchin backup server and the cloud object storage will be encrypted to secure the data transmission during archive retrieve process.

Speed Controller: The speed controller settings are optional, only if the archive retrieve job will bring network or I/O overload to your production environment, you need to configure the speed controller accordingly.

Step 4: Review & Confirm

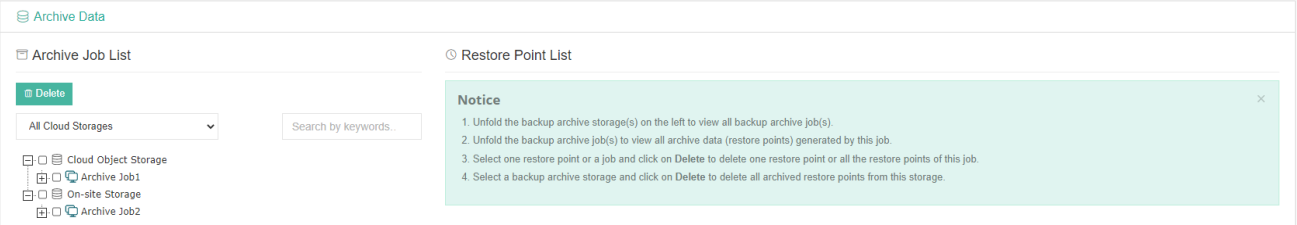
After completing the above settings, you are able to review and confirm the settings.
You can optionally customize a job name and then click on Submit button to confirm the creation of this archive restore job.
After a new archive retrieve job has been created, you will be redirected to the **Monitor Center** > **Jobs** page, and you will immediately see the archive retrieve job run automatically.



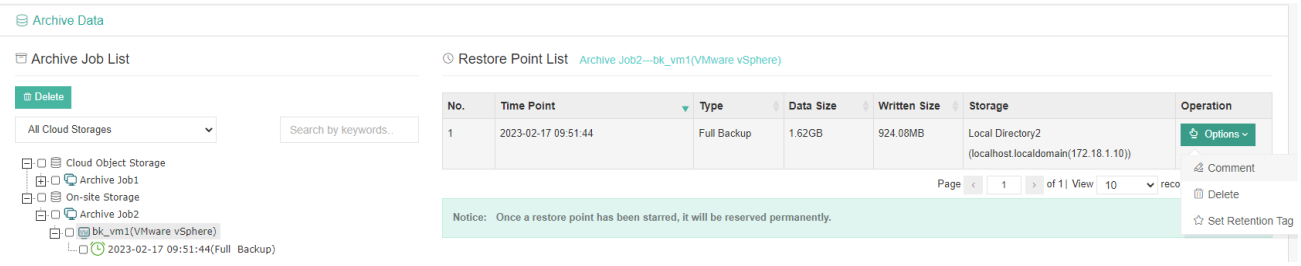
Once the archive retrieve job is completed, the job will be automatically deleted from the current job list.
Now you can go to **VM Backup** > **Restore** page and create a VM restore job with the retrieved VM archive data.

Archive Data

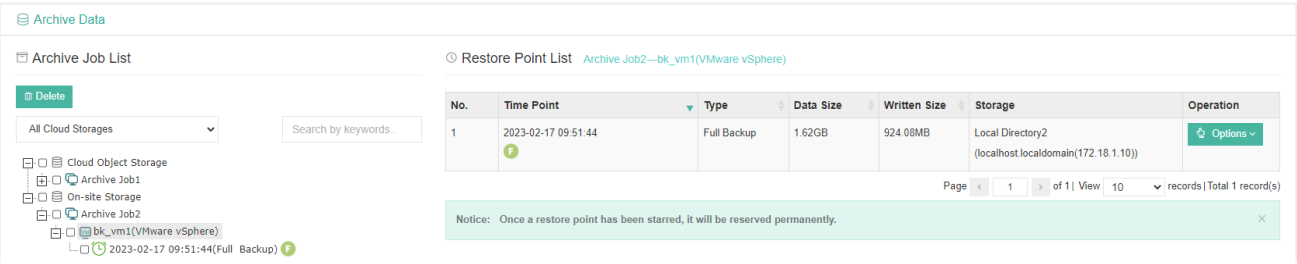
All archive data can be managed from the **VM Backup** > **Backup Archive** > **Archive Data** page. No matter the data is storage in the on-site storage or cloud object storage.



By unfolding the archive storages or the archive jobs, you are able to view all the archive data. And by selecting corresponding restore points, archive job or the archive storage, you are able to delete the selected archive data.
By clicking on a virtual machine, you'll be able to see all the archive restore points of the virtual machine.



By clicking on Options, you will be able to comment, delete and set retention tag for the archive restore point.
Comment and delete archive restore point options are supported with both onsite and cloud archives.
Set retention tag is only supported with the onsite archives. Once an archive restore point had been tagged, it will be marked with an F tag.



This archive restore point will be kept in the archive storage permanently until the F tag has been removed by user.

Backup Verification

Backup Verification in Vinchin Backup & Recovery allows users to easily set up a verification lab on VMware virtual platform for the verification of VMware backup data validity.
With the verification lab an isolated environment will be prepared on the VMware virtual platform to automatically (or manually) run verification jobs with the VMware VM backups, verification reports will also be generated and sent to users via email to show the verification results (no reports generated for manual verification jobs).

Create Verification Lab

Before creating a verification job, a verification lab needs to be created on the VMware virtual platform. Creating a verification lab involves creating the following items on the VMware virtual platform.

- A VM folder: used to place the gateway proxy and verification VMs
- An isolated virtual network: used to test the verification VM network connectivity without interfering with the production network.
- A gateway proxy: used to test the verification VM network connectivity. The gateway proxy is a lightweight Linux VM which will only be powered on when running verification jobs.

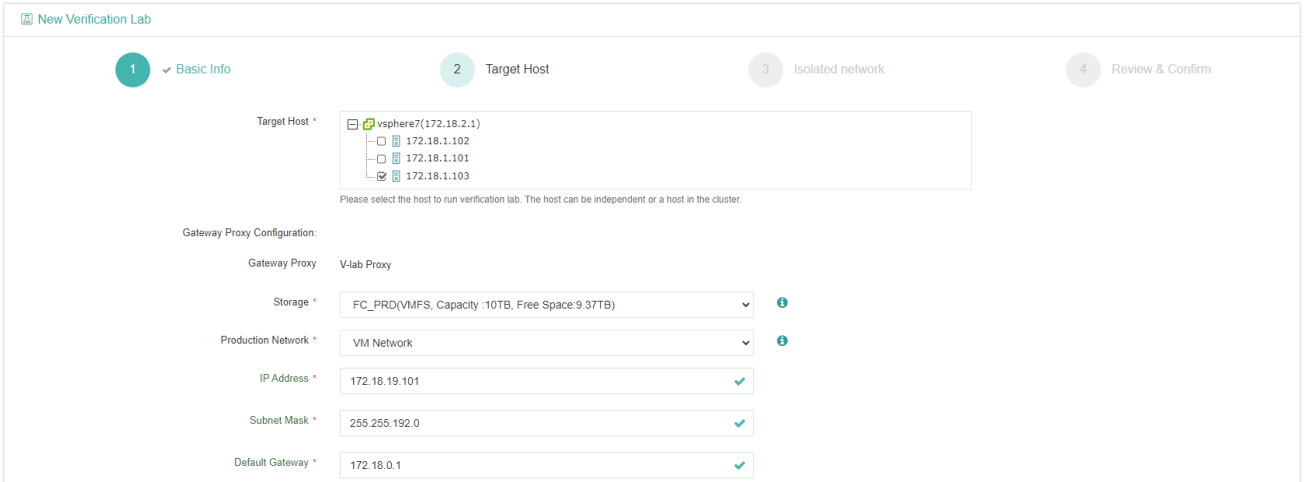
To create a verification lab, please go to **Backup Verification** > **Verification Lab** page.

Step 1: Basic Info

In the **Verification Lab Name** field, enter a name for identification. This name will also be applied to the gateway proxy, resource pool, VM folder and virtual switch.

Step 2: Target Host

In the **Target Host** list, please select an ESXi host to deploy the gateway proxy.

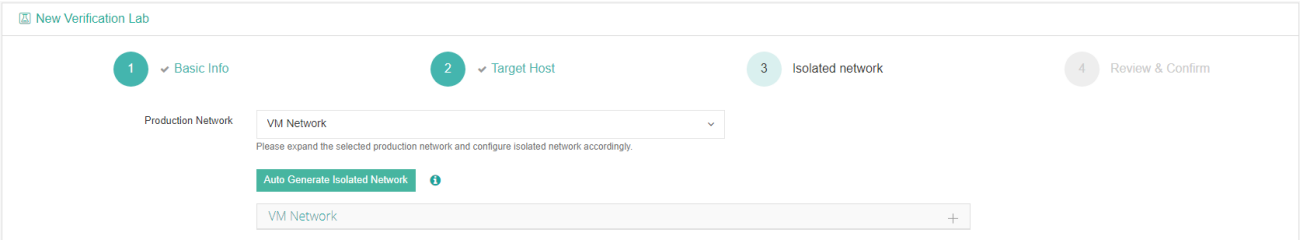


In the **Storage** dropdown list, select a datastore on which the proxy VM virtual disks will be stored.
In the **Production Network** dropdown list, select a virtual network through which the gateway proxy can

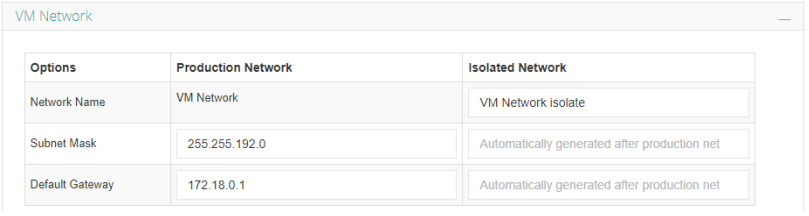
communicate with Vinchin backup server.
In the **IP Address**, **Subnet Mask** and **Default Gateway** fields, please configure the IP address of the gateway proxy for being able to communicate with Vinchin backup server.

Step 3: Isolated Network

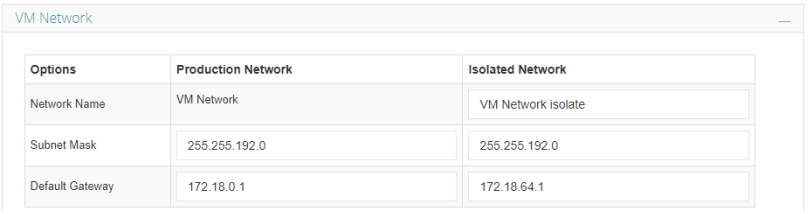
In the **Production Network** dropdown list, please select the virtual network(s) on which you run the production VMs.



Click on the virtual network to specify its subnet mask and default gateway for Vinchin backup server to automatically generate an isolated network.



Once completed specifying the production network info, click on the **Auto Generate Isolated Network** button to automatically generate an isolated network for verification of the VM backups.



If modification is required with the isolated network, users can modify the network name, subnet mask and default gateway before proceed.

Step 4: Review & Confirm

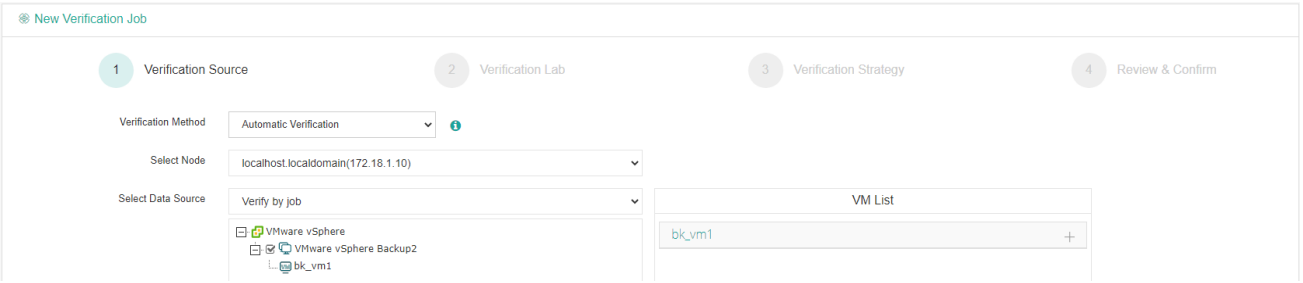
After completing the above-mentioned settings, you are able to review and confirm all the settings of the verification lab to be deployed. By clicking on **Submit** to confirm deploying the verification lab.
When a verification lab is being deployed, it will be in “Deploying(xx%)” state. Once deployment is completed, the status will change to “Deployed”, and users now can run verification jobs with this verification lab.

Create Verification Job

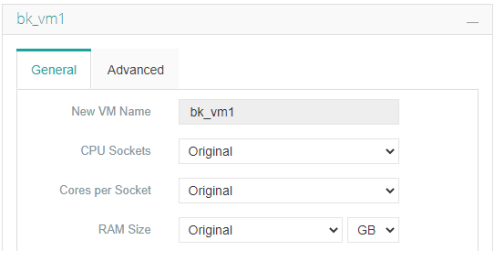
Before creating a verification job, please make sure you had created a verification lab already, if you haven't done this yet, please refer to Create Verification Lab to first create a verification lab.
To create a backup verification job please go to **Backup Verification** > **Verification** page.

Step 1: Verification Source

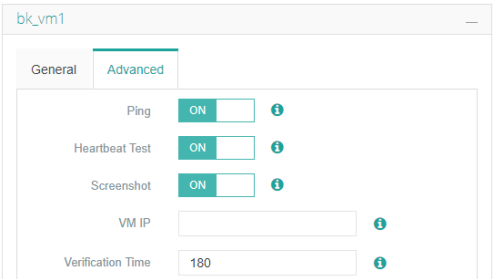
In this screen, the verification method and data source for verification need to be specified.



In the **Verification Method** dropdown list, please select between **Automatic Verification** and **Manual Verification**. If automatic, the VM backups will be verified automatically right after the job is created or on a time schedule basis. If manual, the VM backups will be used to run the VM in the verification lab, and users will be required to verify the VM manually from VMware virtual platform.
In the **Select Node** dropdown list, select a backup node on which the backups are stored.
In the **Select Data Source** dropdown list, select between **Verify by job** or **Verify by VM**. If by job, a VMware backup job needs to be selected and all VMs in this job will be verified. If by VM, users could select specific VM(s) in the backup job to be verified.
In the VM List, by expanding a VM, users can configure the VM configurations and verification options.



Under the **General** tab, users can optionally customize the number of CPUs, cores per CPU socket and the RAM size of the VM to be verified.
Under the Advanced tab, users can configure the verification options. These options are necessary when running automatic verification jobs, if manual verification job, the advanced tab will not show up.



To verify the validity of the VM backups, the verification options including **Ping** test, **Heartbeat** test and **Screenshot**

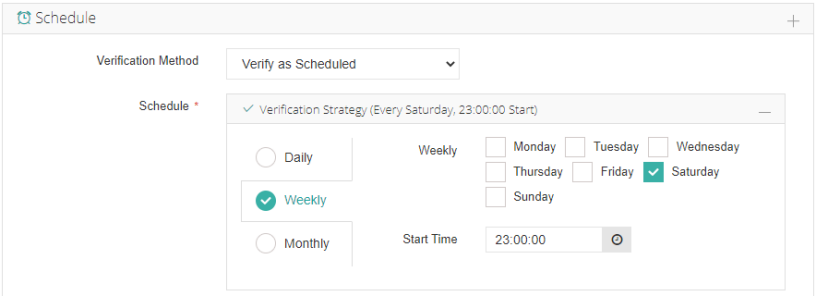
capturing.
In the **VM IP** field, please specify the IP of the VM if VMware Tools is not installed. If it has VMware Tools installed, then Vinchin backup server can obtain the VM IP and this field can be left blank.
In the **Verification Time** field, it defines the verification time of this VM after it's powered on. The verification operations will be done within the given time (in seconds). After that the verification will timeout.

Step 2: Verification Lab

In this screen, please select a verification lab from the **Select Verification Lab** dropdown list.

Step 3: Verification Strategy

For a **Manual Verification** job, the default schedule is Verify Now, which means the verification will start after the job is created.
For an **Automatic Verification** job, the Verification Method can be configured between **Verify Now** and **Verify as Scheduled**.
If verify now, the verification will start right after the job is created, once done, the verification job status will be changed to pending, it will not run again until users manually start it when needed.
If verify as scheduled, users have to configure the time schedule of running the verification regularly on daily, weekly or monthly basis.



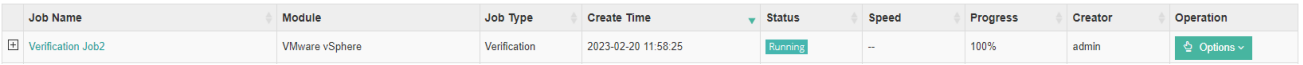
If running the verification job regularly on daily, weekly or monthly basis, the latest restore point of the VM(s) will be verified.

Step 4: Review & Confirm

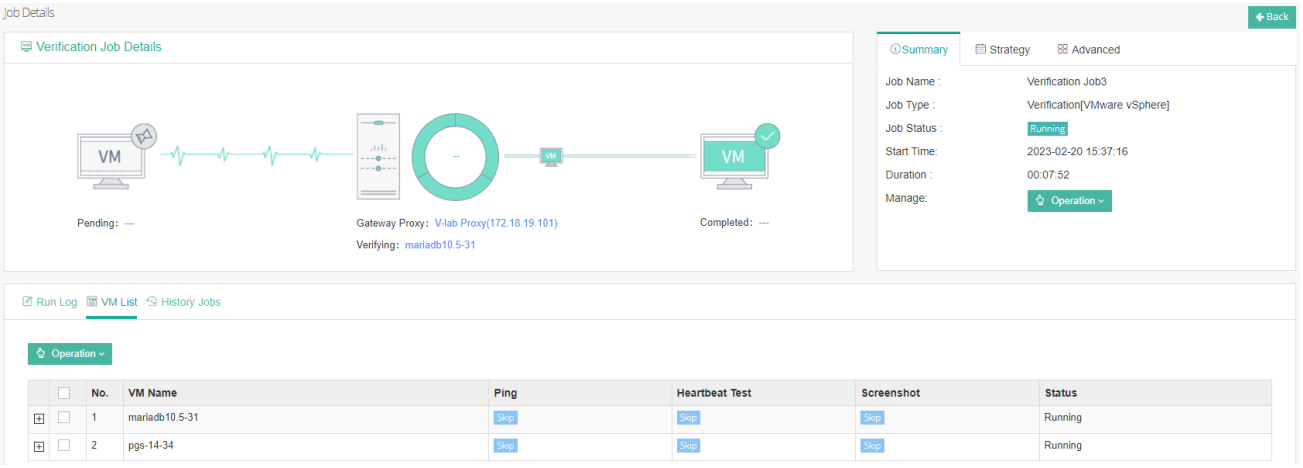
After completing the above-mentioned settings, you are able to review and confirm all the settings of the verification job to be created. By clicking on **Submit** to confirm creating the verification job.

Verification Job Management

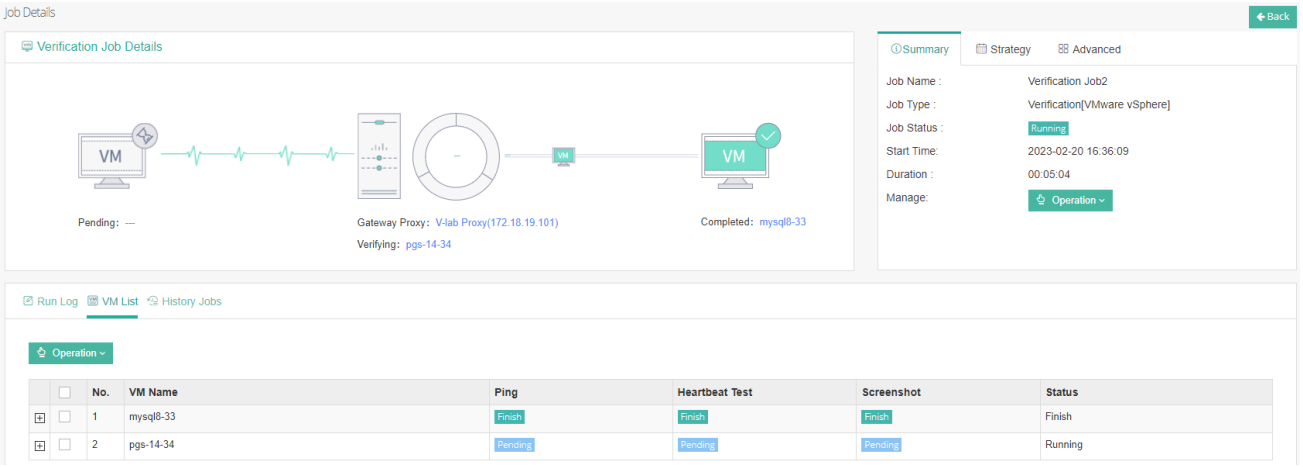
Once a verification job is created, you'll be redirected to the **Monitor Center** > **Jobs** page.
For a manual verification job, once the job is created it will run automatically.



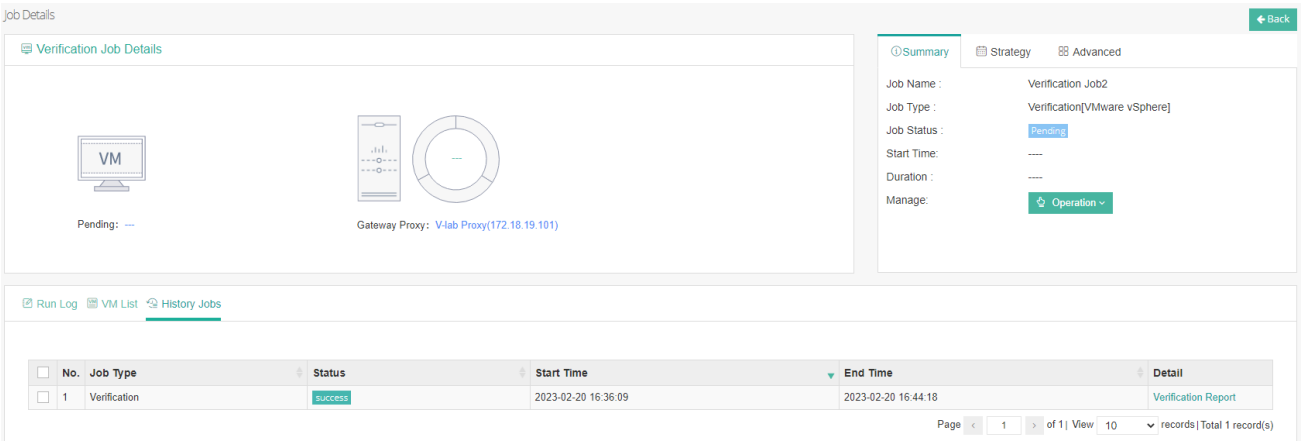
When you see the job progress reaches 100%, which means the VM backups included in this job had been all powered on from the verification lab and ready to be verified manually. By clicking on the verification job name you can view more details of this job.



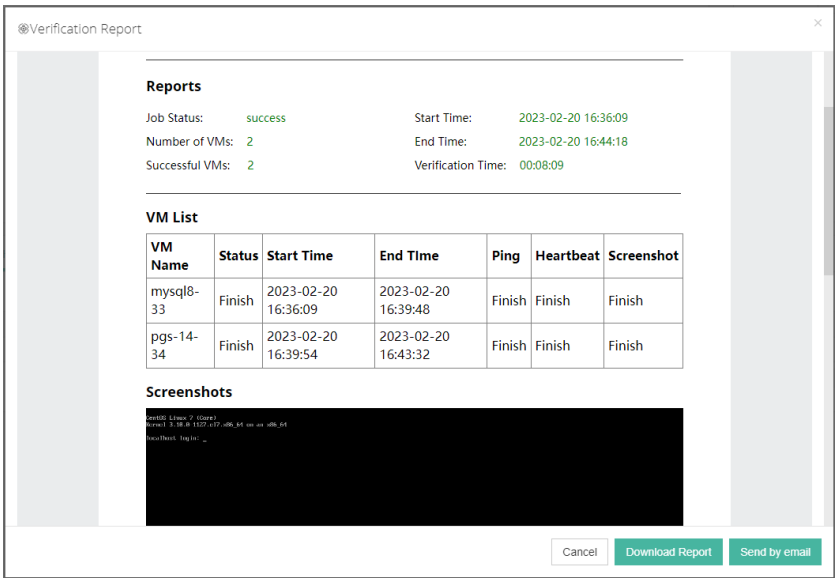
Then you can open VMware vCenter web console to check the VM running state and manually perform the VM verification operations. Once done, you can manually stop this job to complete the verification process.
For an automatic verification job, if it's configured as verify now, then after the job is created it will start verification automatically. If it's configured as verify as scheduled, then after the job is created it will be pending. Users can manually start or stop the job from running.
When running an automatic verification job, by default, each VM included in this job will be powered on for verification for 180 seconds.



When verification is completed for all the VMs, verification reports will be generated for each of the VMs and can be found by clicking on the **History Jobs** tab.



By clicking on Verification Report of the history job, users can view the detailed reports of the verification job.



The verification reports can be downloaded to user's local desktop by clicking on the **Download Report** button. And can be sent to the user's mailbox by clicking on the **Send by email** button.

If the verification job is configured to run regularly on daily, weekly or monthly basis, users can also configure Vinchin Backup & Recovery to send the verification reports automatically by email, for more information of how to send the verification reports, please refer to Notifications.

Resources

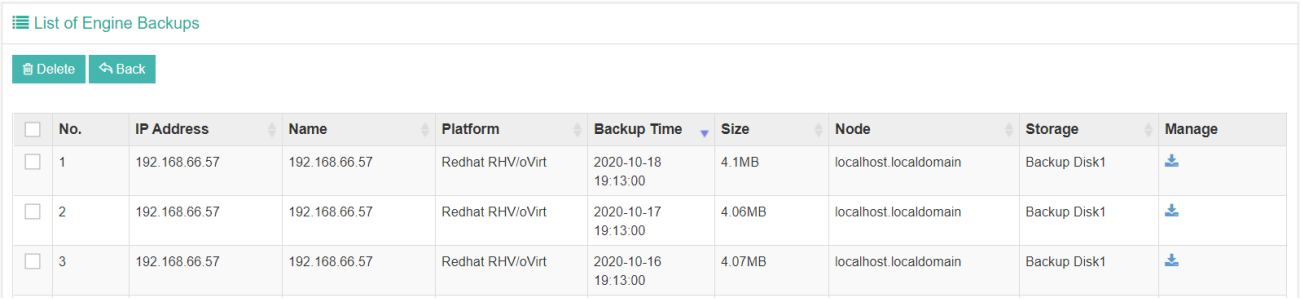
Virtual Infrastructure

Virtual Platform

After adding the virtual infrastructures, you can find and manage them on the **Resources** > **Virtual Infrastructure** page.

Select a virtual infrastructure and click on the **Edit** button to edit the connection settings of the virtual infrastructure, or click on the **Delete** button to delete the virtual infrastructure from Vinchin Backup Server. The virtual infrastructure cannot be deleted when it is included in a running job. You must delete the running job before deleting the virtual infrastructure.

If your virtual infrastructure is RHV, oVirt or OLVM, and if you had enabled engine backup, the backup data can be managed by clicking on the **Engine Backup Data** button.

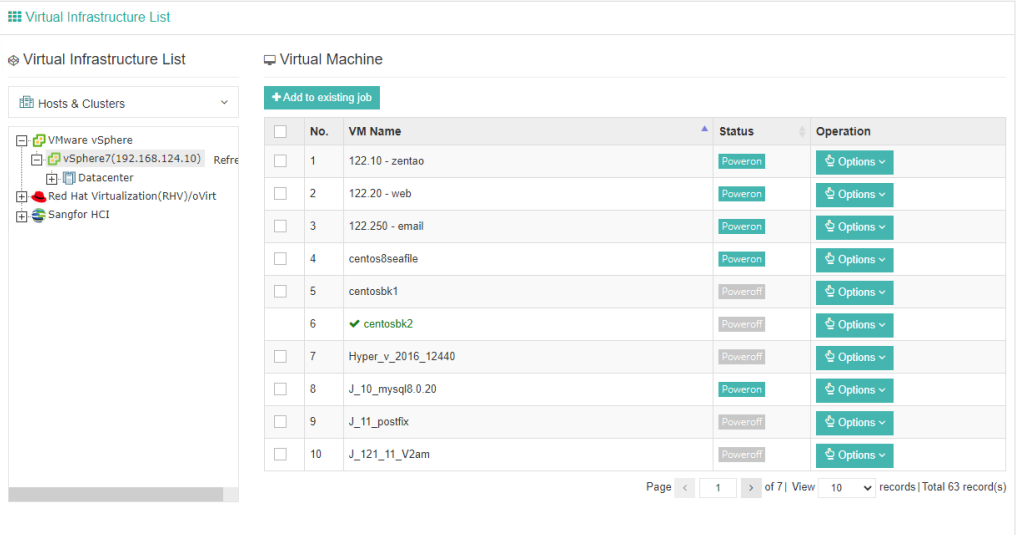


The engine backup data can be downloaded from Vinchin Backup Server, then to be uploaded to the engine host of the Red Hat RHV, oVirt or OLVM to restore the engine host configurations.

For the VM creation/deletion or any other updates of the VMs on your virtual infrastructure, you can rely on the **Auto Refresh** of the virtual infrastructures or you can manually perform the refresh. Click on the **Auto Refresh** button, you can set the auto-refresh time (default 60 minutes, minimum 5 minutes). And in the virtual infrastructure list, you can click on the **Sycn** button to manually refresh the corresponding virtual infrastructure.

From the virtual infrastructure list, you can also change the authorization status of the hosts in the virtual infrastructure by clicking on the **Auth** button, for more details, please refer to Add Virtual Infrastructure.

By clicking on the IP address of a virtual infrastructure, you can check the virtual machines on this virtual platform.



By selecting the VMs from the virtual machine list and click on the **Add to existing job** button, you can add the selected VMs to an existing backup job. Or you can add a single VM to an existing backup job by clicking on the **Options** button then select **Add to existing job**.

And by clicking on the **Options** button, you'll have options to suspend or power off a VM in **Poweron** status, or if the VM is in **Poweroff** status, you'll have option to power it on.

Cloud Platform

On the Resources > Virtual Infrastructure > Cloud Platform page, users can add and manage the OpenStack cloud platform. For more information about how to add OpenStack cloud platform, please refer to OpenStack.

LAN-Free

Vinchin Backup & Recovery supports Fibre Channel, iSCSI and NFS for LAN-free backup and restore through the SAN (Storage Area Network).

If you want to implement LAN-free backup and restore, Vinchin Backup Server needs to meet the following requirements:

- Vinchin Backup Server is installed on a dedicated physical server.
- For fibre channel SAN, the physical server needs a fibre channel HBA (Host Bus Adaptor) interface card to be able to connect to the fibre channel SAN via the FC switch.
- For iSCSI and NFS (IP SAN), the physical server needs an extra NIC to be able to connect to the storage area network via the storage network switch.
- LAN-Free path needs to be configured.

To add LAN-Free path, please follow the instructions below.

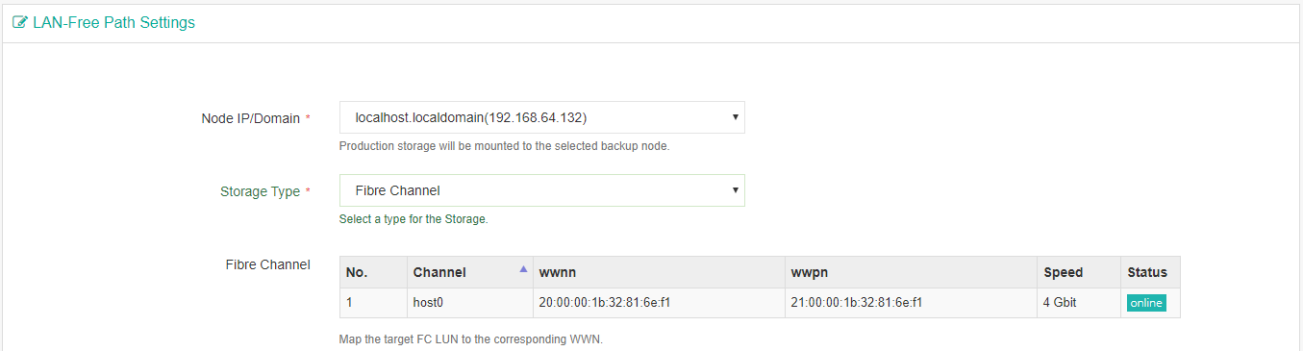
Notice

1. LAN-Free backup and restore is not supported with Microsoft Hyper-V and Sangfor HCI in Vinchin Backup & Recovery version v6.5.

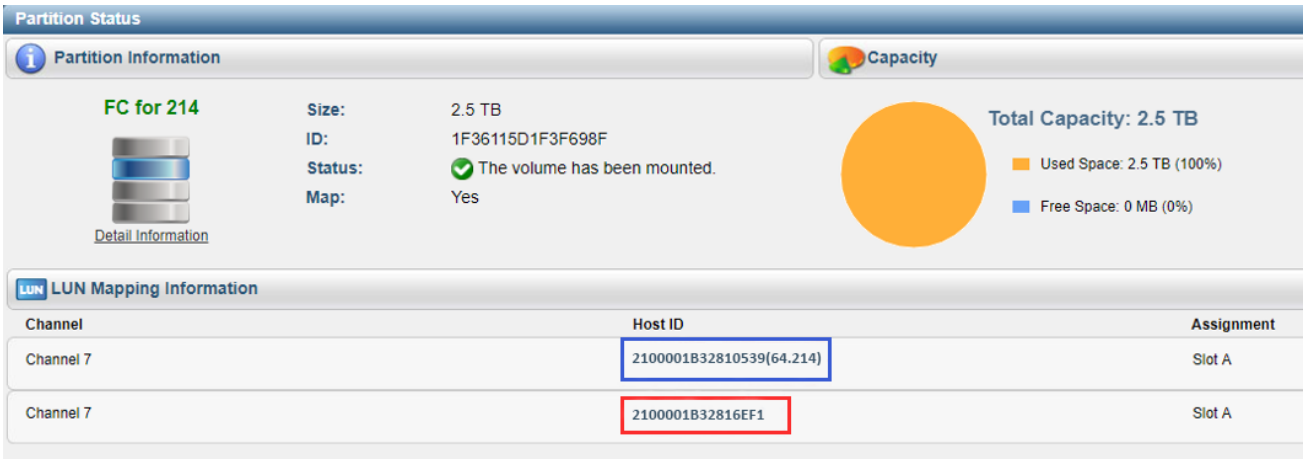
2. The following instructions are for reference only, as the LUN mapping varies from different storage servers.

Fibre Channel

From Vinchin Backup Server web interface, on the **Resources** > **LAN-Free** page, click on **Add** button to add a fibre channel storage, in the **Storage Type** field, please select **Fibre Channel**.

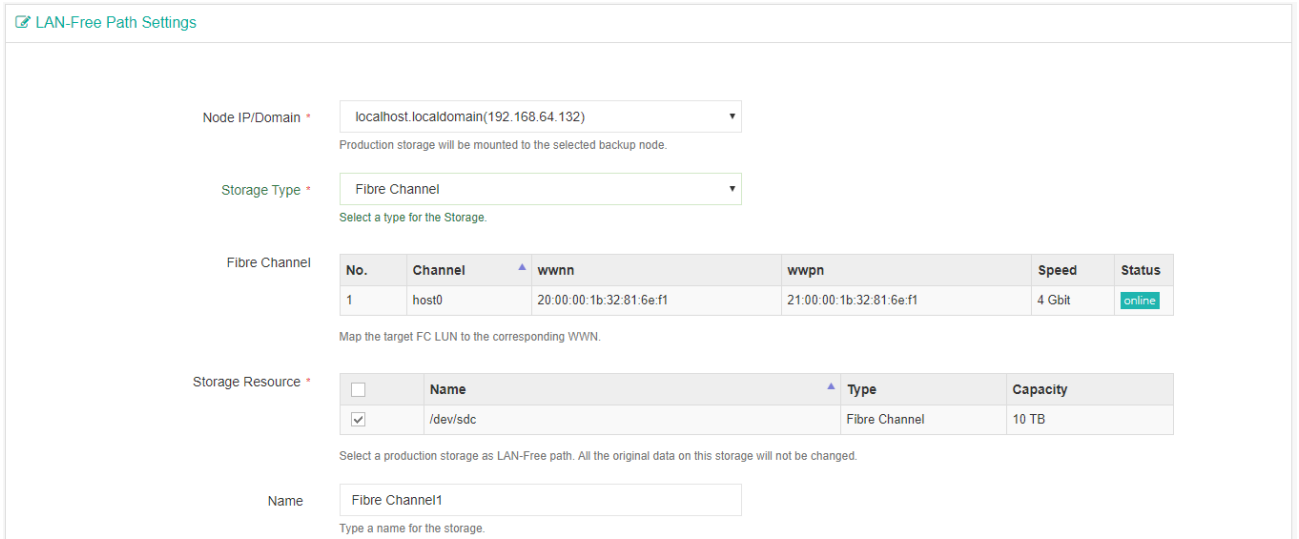


Now Vinchin Backup Server will detect the fibre channel and the wwpn of the HBA interface card, use these information to map the LUN of the production storage to Vinchin Backup Server from the storage server management interface.



The Host ID marked with blue belongs to the production host, the Host ID marked with red belongs to Vinchin Backup Server, which means the same LUN had been mapped to both of them.

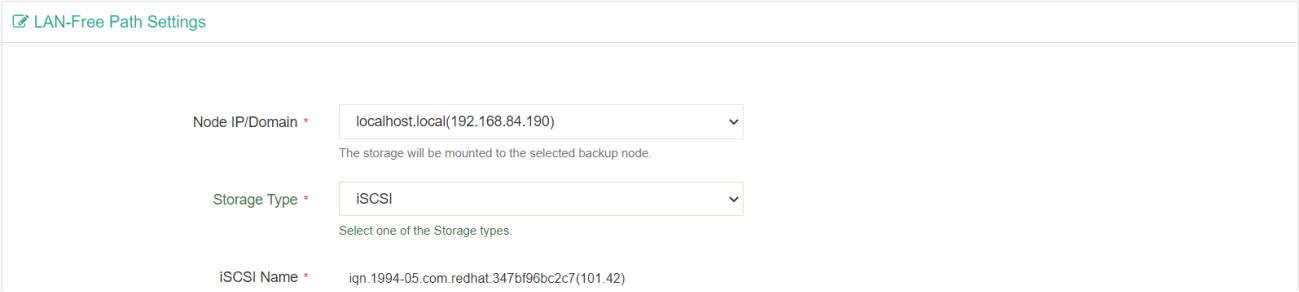
Add the fibre channel again, Vinchin Backup Server will recognize the LUN which is mapped to it, and the storage will be able to be added to Vinchin Backup Server as LAN-Free path.



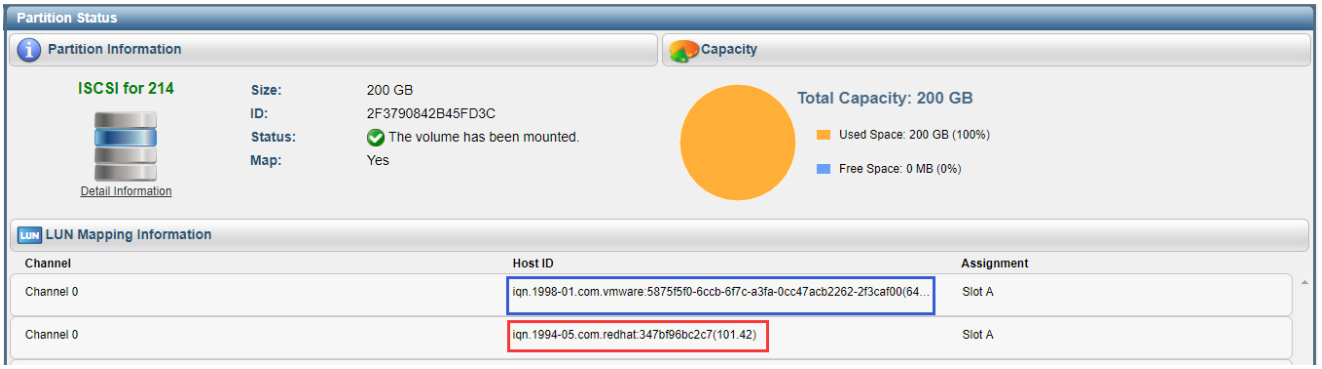
Select the production storage and click OK to add it to the LAN-Free Path List.

iSCSI

From Vinchin Backup Server web interface, on the **Resources** > **LAN-Free** page, click on **Add** button to add an iSCSI storage, in the **Storage Type** field, please select **iSCSI**.



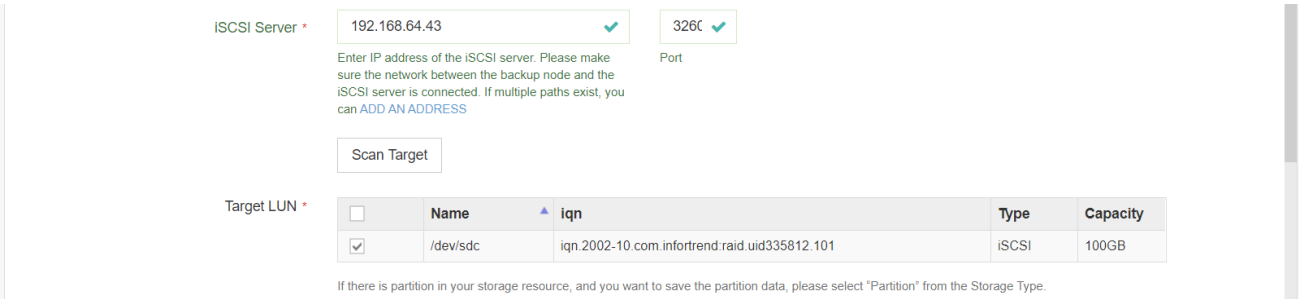
Please use the IQN to map the LUN of the production storage to the backup server from the storage server management interface.



The Host ID marked with blue belongs to the production host, the Host ID marked with red belongs to Vinchin Backup Server, which means the same LUN had been mapped to both of them.

After this, add the iSCSI storage again, and input the storage server IP address in the iSCSI Server field and click on **Scan Target** button to scan the target storage.

The system will discover the production LUN storage which is mapped to Vinchin backup server, and the storage will be able to be added to Vinchin Backup Server as LAN-Free path.

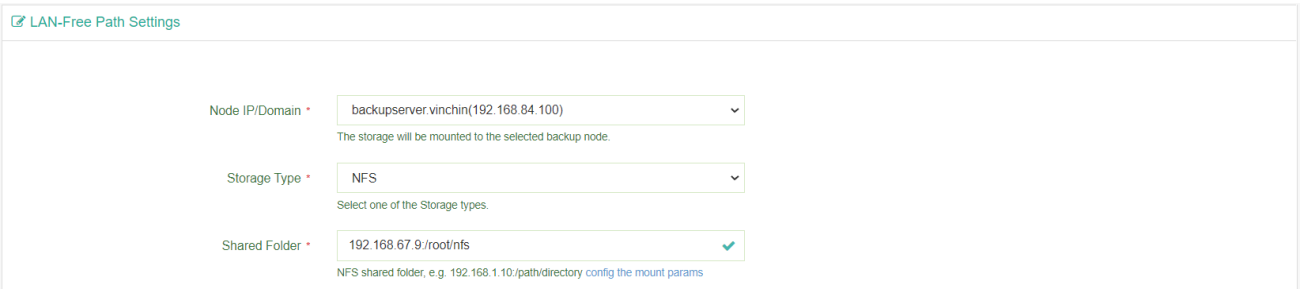


Select the production storage and click OK to add it to the LAN-Free Path List.

NFS Storage

If the production system uses NFS shared storage as the production storage, the NFS storage can be added to Vinchin Backup Server as LAN-Free path.

From Vinchin Backup Server web interface, on the **Resources** > **LAN-Free** page, click on **Add** button to add an iSCSI storage, in the **Storage Type** field, please select **NFS**.



In the **Shared Folder** field, simply type in the path of the NFS production storage to add it to Vinchin Backup Server as LAN-Free path.

After adding the LAN-Free path, while creating a backup/restore job, the transmission strategy should select SAN (LAN-Free).

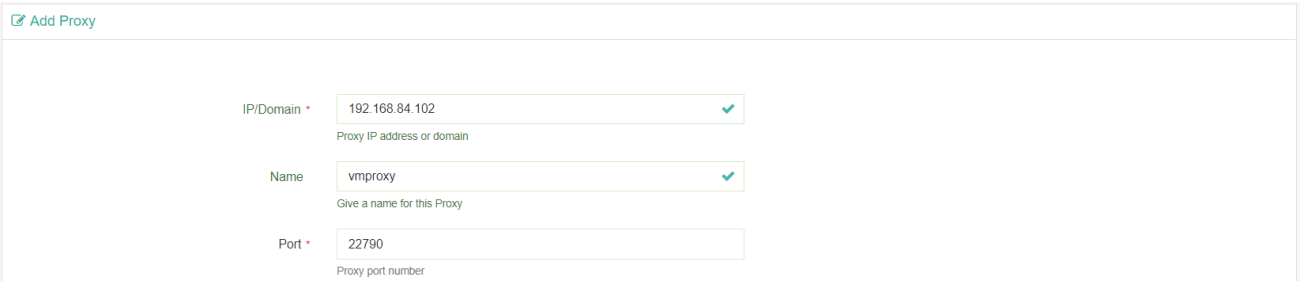
Warning

The production storage which has been mapped to the Vinchin backup server as LAN-free path should NOT be added as a backup storage! Adding a LAN-free path as a backup storage will cause the production storage been formatted, all the production data will be erased.

Backup Proxy

Vinchin Backup Proxy is an optional component for backup VMware vSphere virtual infrastructure, and it needs to be installed on the ESXi server as a VM. If you are using other virtual platforms, please just skip this part.

If Vinchin Backup Server is installed on the ESXi server as a VM, then a Backup Proxy is not needed. To add a Backup Proxy to Vinchin Backup Server, please go to **Resources** > **Virtual Infrastructure** > **Backup Proxy** page and click on the **Add** button to add the Backup Proxy.

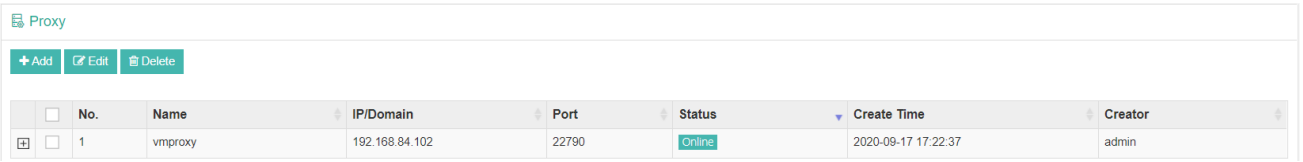


In the **IP/Domain** field, please enter the IP address of the Backup Proxy.

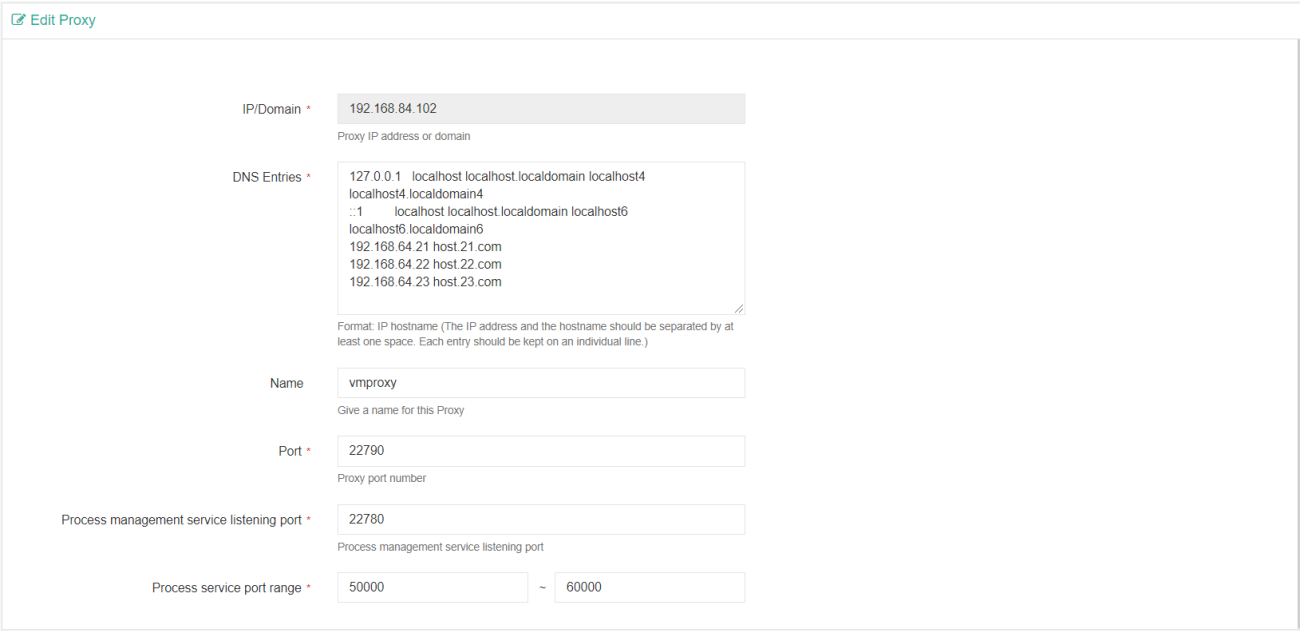
In the **Name** field, you can optionally define a customized name for the Backup Proxy.

In the **Port** field, the default port number should not be modified.

When done the above settings, click on **OK** button to add the Backup Proxy to the Backup Server.



By selecting the Proxy and clicking on the **Edit** button, you are able to edit the Proxy settings.



The DNS Entries should be synchronized from the Backup Server if DNS settings had been configured on the DNS Sync option is enabled on the Backup Server. Otherwise, you can configure the DNS settings manually here.

And usually the port number settings should not be changed.

Agents

For agent management, please refer to Preparation for Physical Backup.

NAS Shares

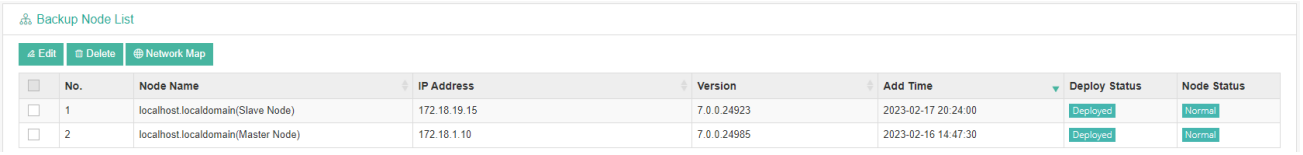
For NAS share management, please refer to Preparation for NAS Backup.

Storage

For Storage management, please refer to Storage Repository.

Backup Node

If you had deployed Vinchin Backup Node, the Backup Node can be managed on the **Resources** > **Backup Node** page.

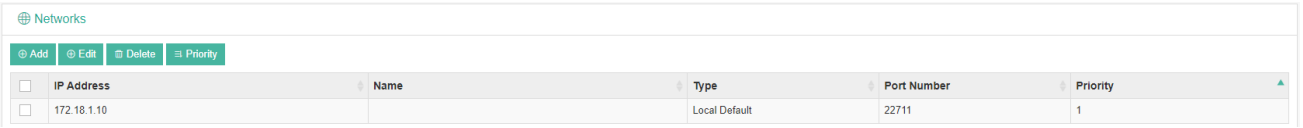


The connection of a Backup Node to the Backup Server is configured during the installation process of the Backup Node, for more details please refer to the Installation Guide of Vinchin Products.

The Node Name is as per the hostname you configured during the installation, if you want to modify the Node name, please select the node and click on the **Edit** button.

To delete a Backup Node from Vinchin Backup Server (the server node cannot be deleted), please make sure there's no storage added on the backup node which is in use by any backup job. Otherwise please delete the jobs and then delete the storage added to this backup node. After this you can power off the backup node and its status will change to offline, you can delete it when it's offline.

For the **Network Map** configurations, it's used when deploying Vinchin on the Internet.

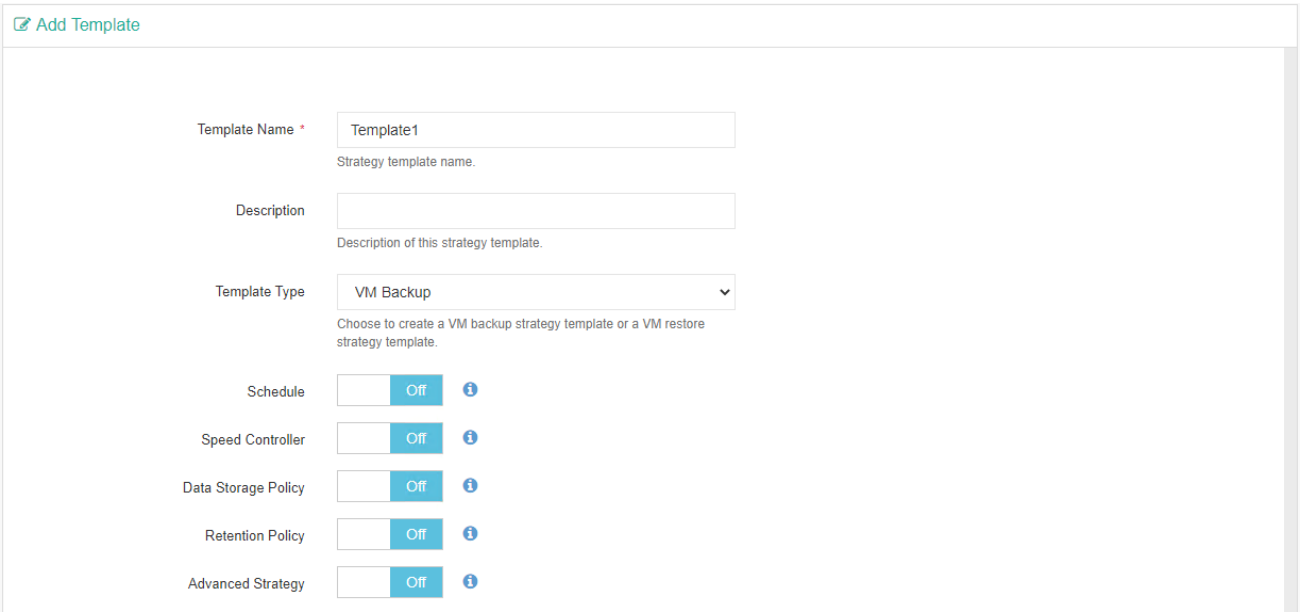


There's a default record please do not delete it.

If Vinchin backup server is deployed behind NAT but requires backing up workloads over Internet, a network map needs to be added here. Please contact Vinchin support team for help on configuring network map.

Strategy Templates

Strategy templates for VM backup jobs can be pre-configured from **Resources** > **Strategy** page. When users creating new VM backup jobs, the strategy templates can be used to reduce the work of setting up various common settings. Click on the **Add** button to add a new strategy template.



In the **Group Name** field, you can define a name for this template, and in the **Description** field you can optionally add some descriptions of this template.

For the **Schedule**, **Speed Controller**, **Data Storage Policy**, **Retention Policy** and **Advanced Strategy**, you can optionally enable and configure some of those settings in this template, the settings which are not enabled and configured in this template, when you creating a backup job and select this template, those un-configured settings will be given with system default settings.

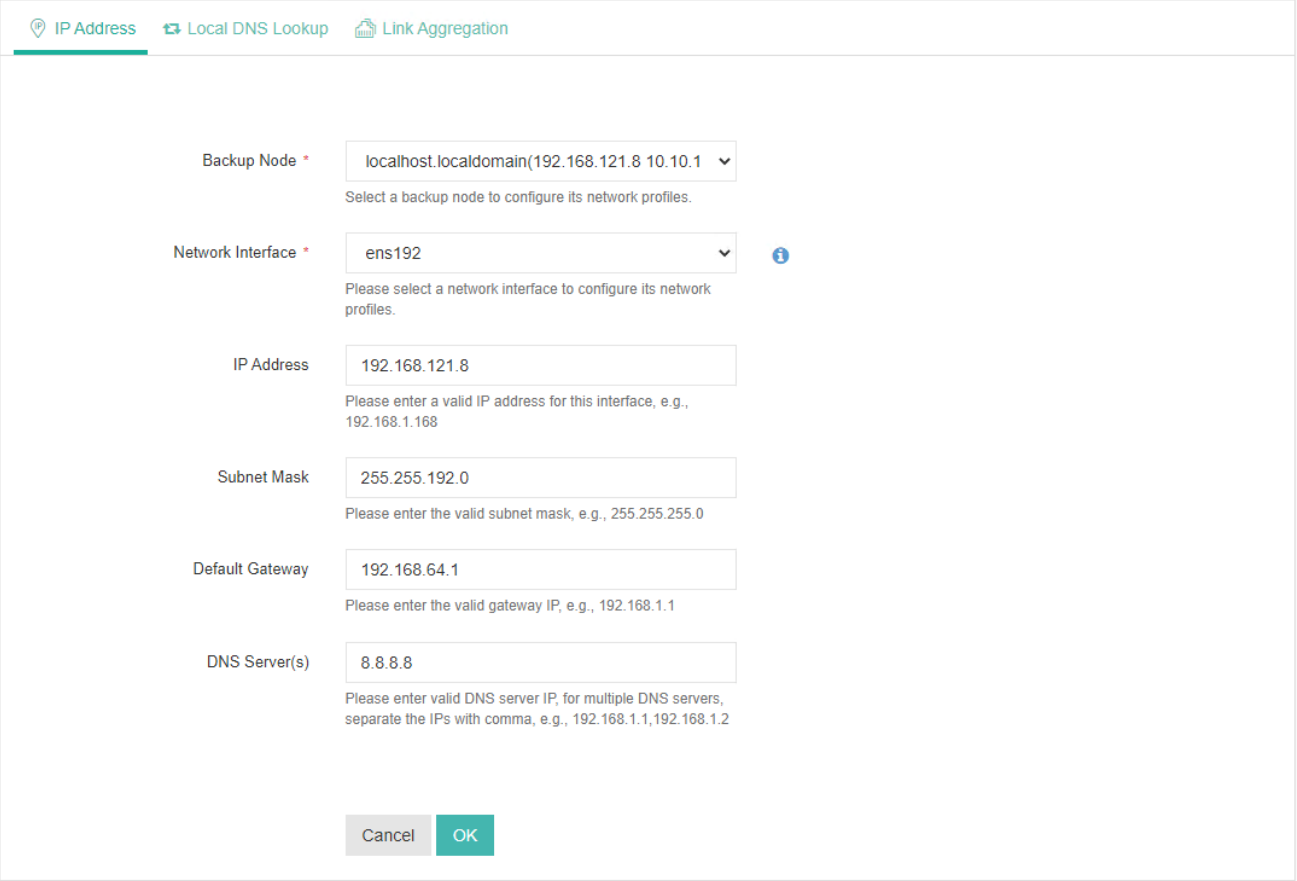
System

System Settings

Network Settings

IP Address

The network profile of Vinchin Backup Server should be well configured during the installation process. If modifications are required, you can do it from **System** > **System Settings** > **Network Settings** page.



From the **Backup Node** dropdown list, you can select a backup node to modify its network profiles.
From the **Network Interface** dropdown list, you can select a network interface to set its network profiles.
And the below settings including IP address, subnet mask, default gateway and DNS server.

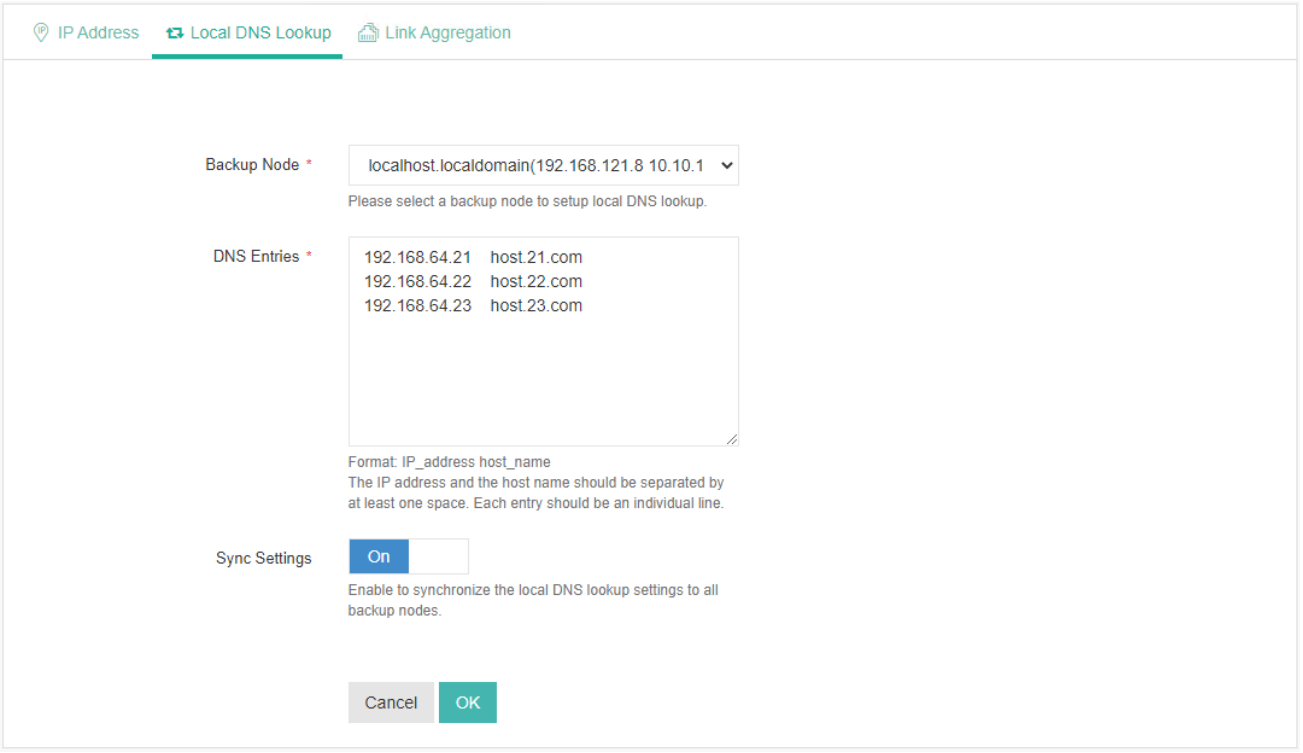
Warning

1. If the IP address of the backup server had been changed, please type in the new IP address in the browser address bar to reopen the backup server web console.

2. Please DO NOT change the IP address of Vinchin Backup Server unless it's really necessary! After changing the IP address of backup server will result in disconnection of the backup node and the backup plugins, please change the listening IP of the backup node and the backup plugins accordingly.

Local DNS Lookup

If an ESXi host was added to the vCenter via its domain name, then this ESXi host's corresponding domain name needs to be configured in the Vinchin backup server, so that Vinchin backup server will be able to communicate with the ESXi hosts. Otherwise, the VM backup jobs will fail.

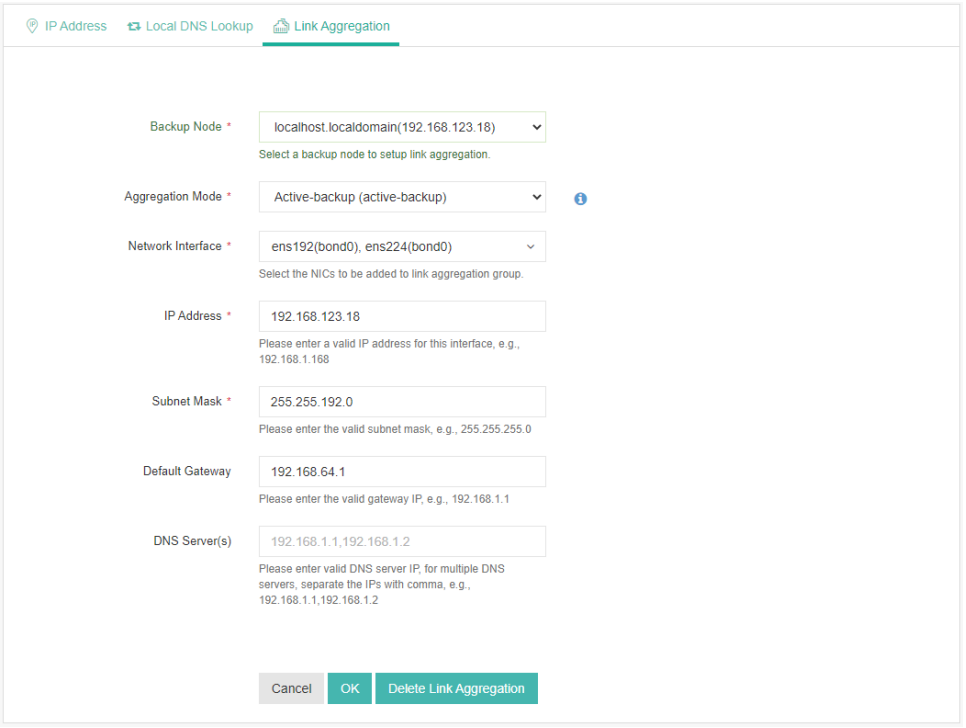


First fill in the IP address of the ESXi host and its domain name separated with a space. If there are multiple ESXi hosts, please fill in the DNS records in different lines. After this please click OK to save.

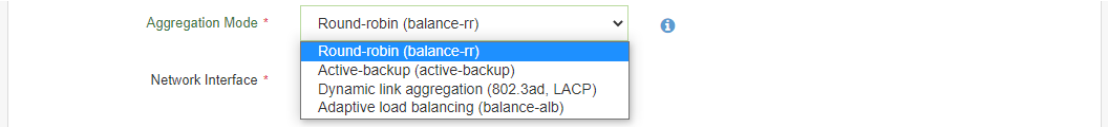
If you have deployed backup node(s) to Vinchin Backup Server, please enable DNS Sync option, so you don't have to configure DNS settings for each node separately.

Link Aggregation

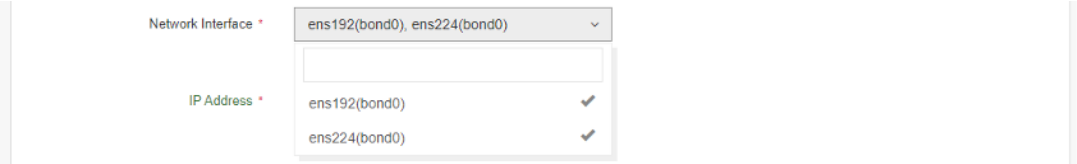
Link aggregation is the combining (aggregating) of multiple network connections in parallel by any of several methods, in order to increase network throughput or provide redundancy of the network links.
Link aggregation is optional, if you want to setup link aggregation group, your Vinchin backup server or node must have multiple network interfaces available.
In **Backup Node** dropdown list, you should select a node on which you wish to setup link aggregation.



There are 4 aggregation mode: **Round-robin(balance-rr)**, **Active-backup (active-backup)**, **Dynamic link aggregation (802.3ad, LACP)** and **Adaptive load balancing (balance-alb)**. Please select the desired mode which suits your requirement.



In Network Interface dropdown list, select the network interfaces which you wish to add to the link aggregation group.



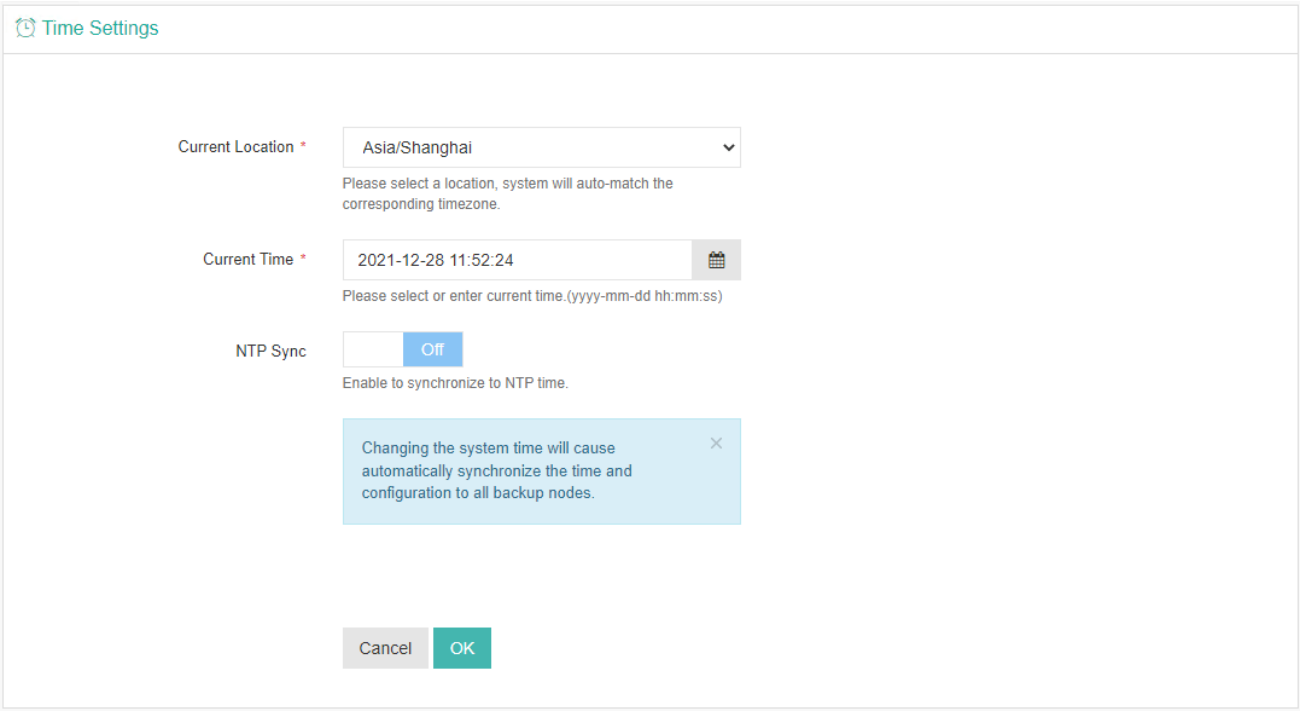
Fill the rest fields, click on OK, the network services will restart, please be patient to wait the link aggregation complete.

Warning

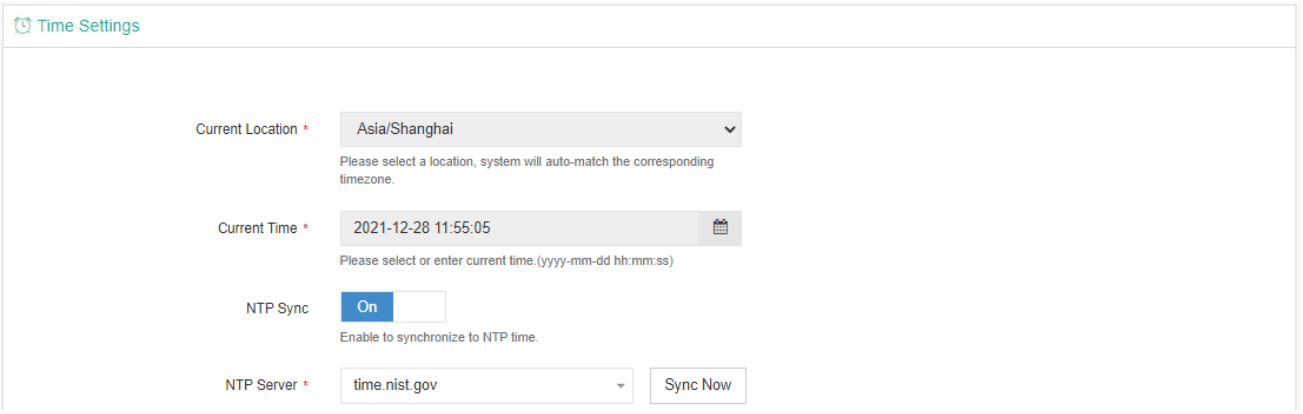
The license will be invalid after link aggregation, please contact with your technical support to renew the license.

Time Settings

The time settings should have been done during the installation of Vinchin Backup Server, but if you want to modify the time settings, for example, set the system to use manual time or NTP time can be done from **System > System Settings > Time Settings**.



In the **Time Zone** field, you should select the correct time zone that you are located in. And if you want to set a manual time, you can select from the calendar or manually input the current time in the **Manual Time** field.
If you want to synchronize the current time from an NTP server, please enable **NTP Time**, and then specify a desired NTP server address in the **NTP Server** field, after this click on the **Sync Now** button to obtain time from the specified NTP server, or you can click on OK button to save the settings and do the time synchronization.

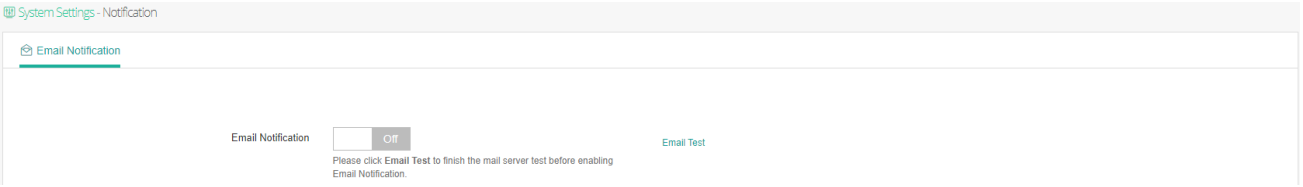


Warning

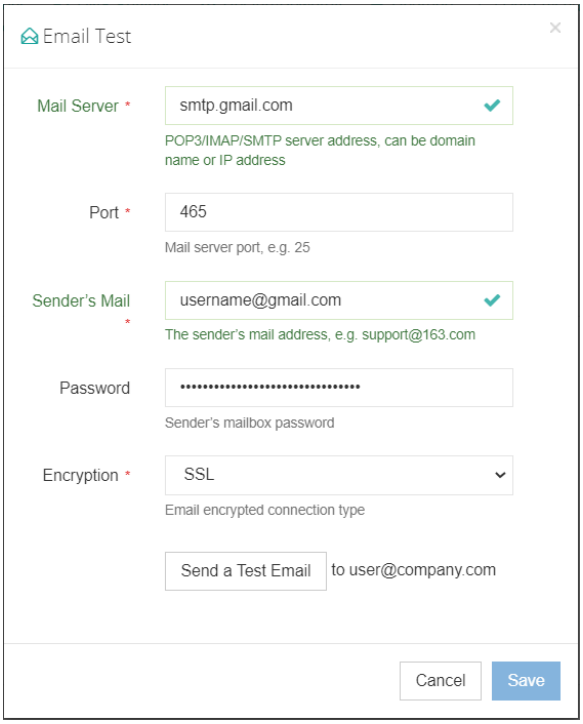
Please make sure the time settings are correct and accurate, as if you had deployed backup node(s), the time settings will be automatically synchronized to all backup nodes connected to this backup server, and as a result, all the scheduled job will run based on the current backup server time.

Notifications

Email Notifications can be enabled to send various kinds of notifications and reports of Vinchin backup server to the administrator and other recipients for users to be informed of the running status of Vinchin backup services.



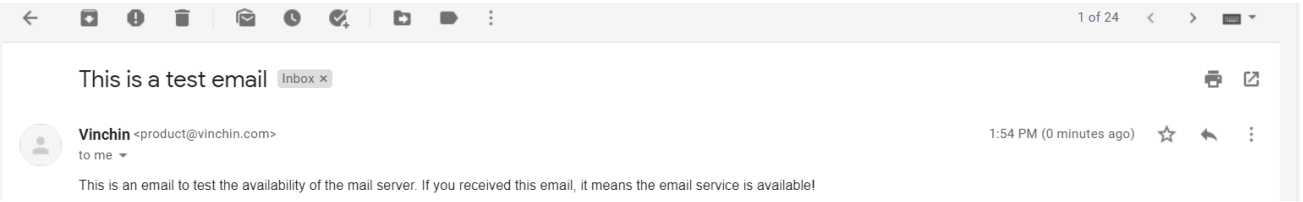
To enable email notification, first make sure you had specified an Email address from **admin** > **Account Settings**, then click on Email Test to complete the mail server settings.



To configure your outgoing mail services, the mail server can be POP3, IMAP or SMTP, you can choose one of the mail server type and configure the mail service as per the instructions of your mail service provider.

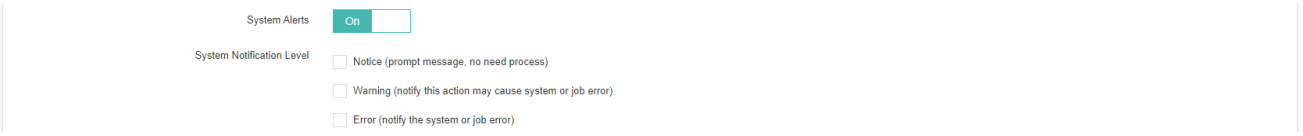
In the above example, Gmail SMTP is used as the outgoing mail server. The **Mail server** should be smtp.gmail.com, **Encryption** should be SSL or TLS, the **Port** number should be 465 or 587, and you must configure a mail account here as the sender. After this, you can click on **Send a Test Email** to test the mail services. The recipient of the test email is the current user, whose Email address is configured in the account settings.

You should now receive a test email stated as below.



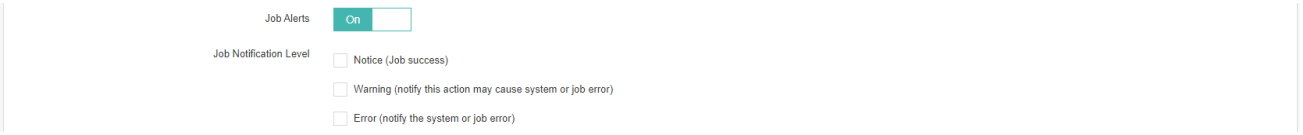
After you had received the test email please save the mail service settings, then you are able to enable Email notification. Once enabled, you are able to configure how the notifications to be sent.

System Alert is not enabled by default, you may enable it if required. The system level notice, warning and error messages are configurable to be sent to specific user(s) via emails.

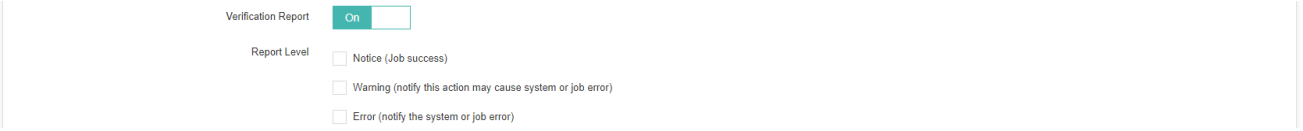


It is recommended to enable sending critical system level notifications, as users don't have to pay much attention on the system level notices.

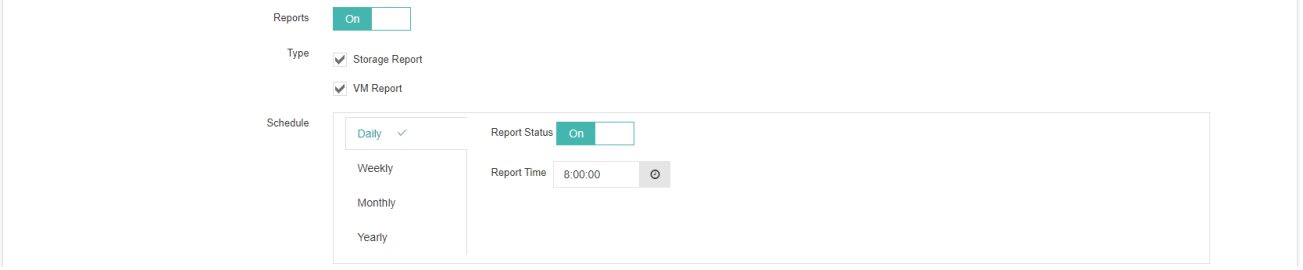
The **Job Alerts** can be enabled to send backup/restore job level notifications, including job success notices, warnings or errors of the jobs.



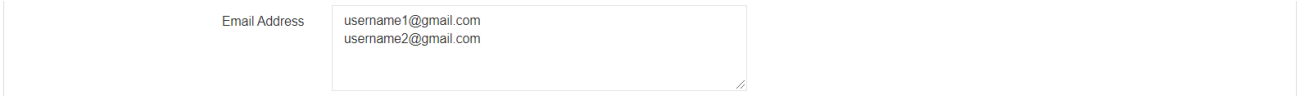
Verification Report can be enabled to send reports of the backup verification results.



Reports can be enabled to send reports of the storage usage and VM protection status on a specific time point or multiple time points on daily, weekly, monthly and yearly basis.



After setting up the notification types and timing, in the Email address field you can optionally enter more user email addresses to add them to the email notification mailing list. The email address of your own is not needed to be added from here.



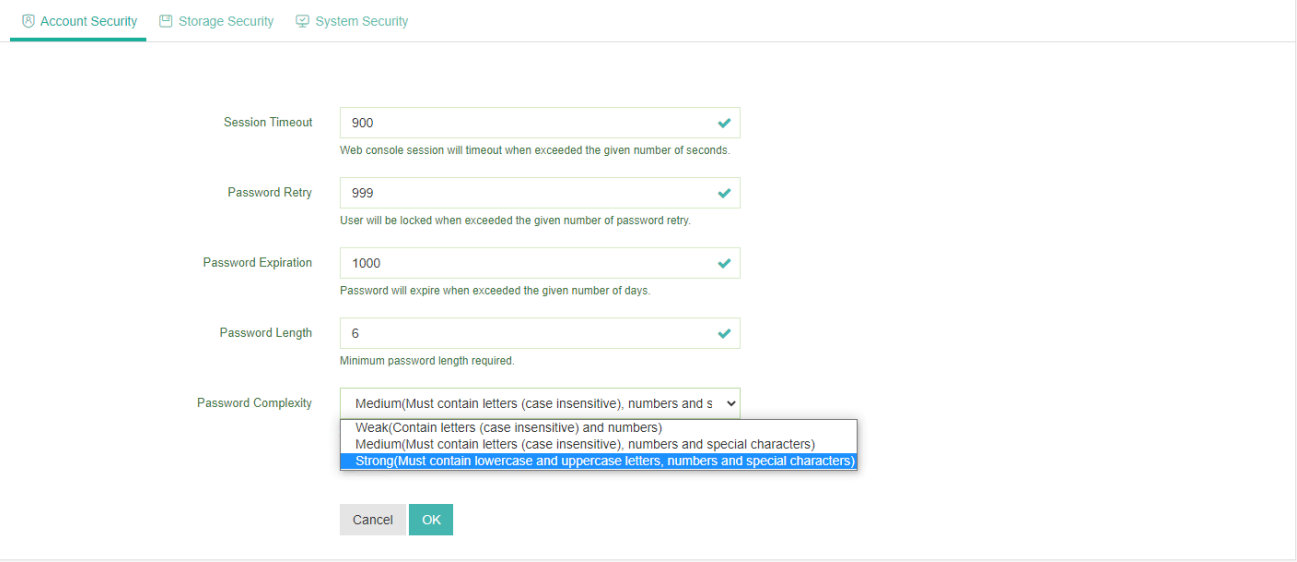
The system alerts and reports will be sent to the system administrator by default. The job alerts will be sent to the job creator by default. The newly added recipient will receive all the enabled notifications.

Security Settings

From **System > System Settings > Security Settings** page, admin user can configure **Account Security**, **Storage Security** and **System Security** settings.

Account Security

Account security settings define some global user account configurations, including Vinchin backup server web console session timeout, max password retry, password expiration time, minimum password length and password complexity settings.



The **Session Timeout** option determines when the web console session will expire due to inactive user activity.

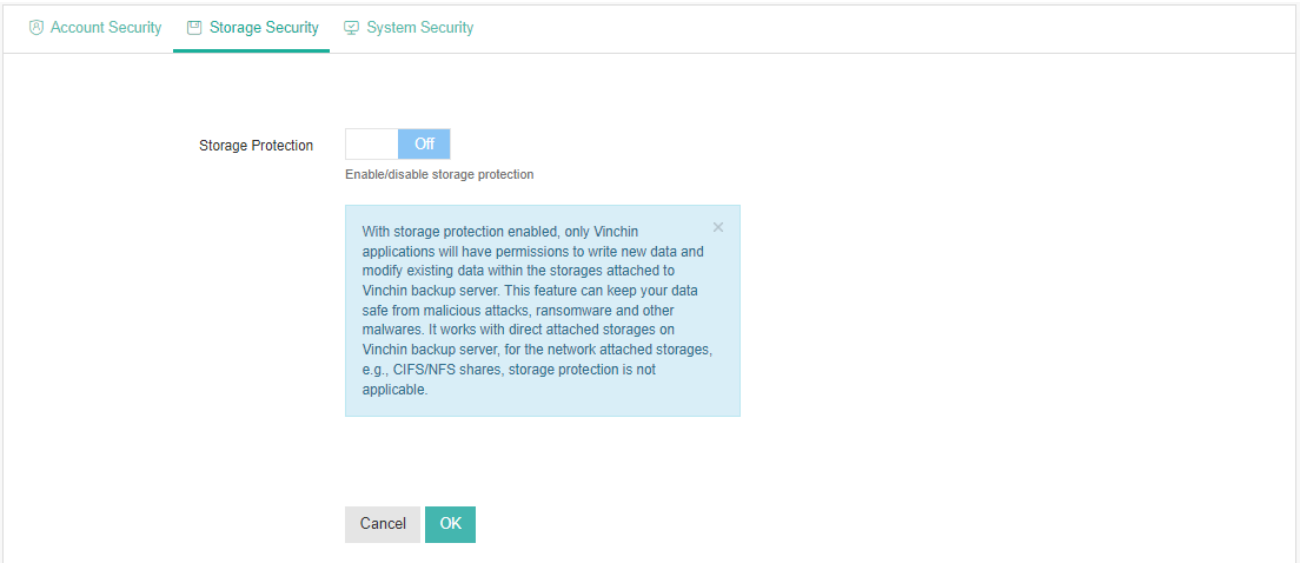
Password Retry options determines the max password retry allowed before a user account is locked. Once a user account is locked, admin user needs to unlock this user account from **System > User Management > Users** page (admin user will not be locked).

Password Expiration option determines how long the user account password expires, when the password is about to expire, user will receive popup notification on the web console, when password is expired, user will be redirected to the change password screen to change password and re-login.

For the **Password Length** and **Password Complexity**, these 2 options determine the minimum password length and the password complexity rule.

Storage Security

Under **Storage Security** tab, you are able to enable **Storage Protection** which can effectively protect your backup data stored in the backup storage.



By default, storage protection is disabled, when enabled, only Vinchin applications are allowed to modify the backup data saved in the backup storages attached to Vinchin backup server/node. And as a result, it can protect your backup data against ransomware and other malwares from modifying your backup data.

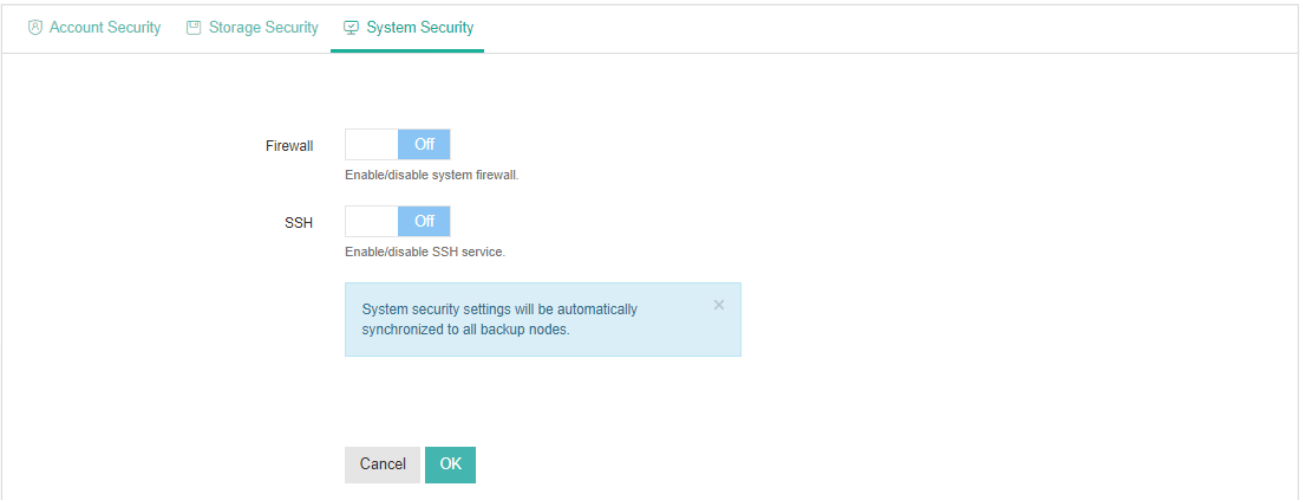
Notice

1. Before upgrading Vinchin software, please temporarily disable Storage Protection, otherwise, software upgrade will fail. After upgrading, please turn it back on.

2. To guarantee Storage Protection always works, the backup storage of Vinchin backup server must be exclusive block devices, like local disks, disk partitions, logical volumes, fibre channel LUNs and iSCSI LUNs, for other file storages, Storage Protection might not work, because ransomware and other malwares might access your backup data by-passing Vinchin backup server.

System Security

Under System Security tab, you are able to turn Vinchin backup server firewall and SSH services on or off.

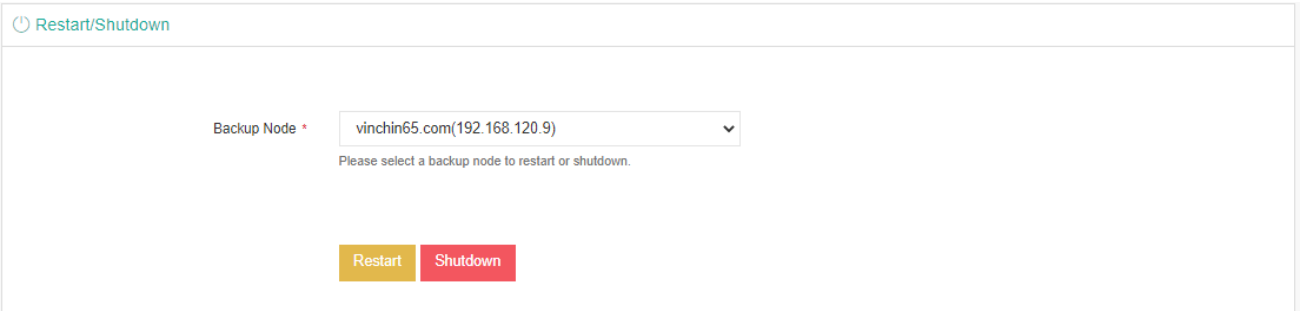


Vinchin backup server has some built-in security rules configured with the system firewall, it can be enabled for system security. While it also has the necessary services enabled to ensure the functionalities of backup and restore activities.

For SSH option, it determines whether users can connect to Vinchin backup server CLI via SSH connection. It is recommended to disable this option when SSH access to Vinchin backup server CLI is not needed.

Restart & Shutdown

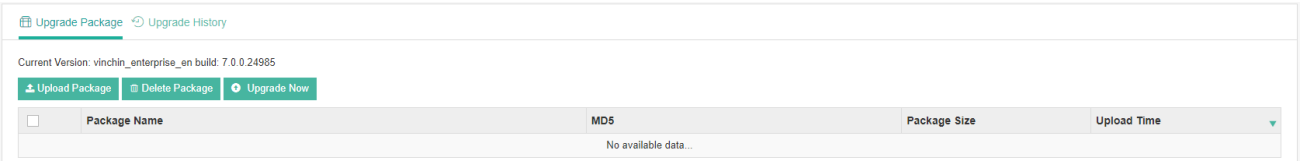
Restart and Shutdown functionalities can be used for the backup server or backup node(s) maintenance or some other circumstances which require system restart or power off.



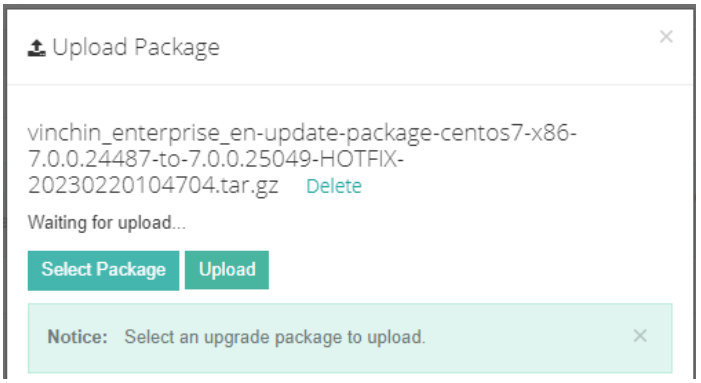
You can select the target node then click on Restart or Shutdown button to perform the corresponding operation to the select node. Both restart and shutdown operation will terminate backup/restore jobs on the selected system, so before doing this, please make sure there's no job running on the selected node.

Upgrade

When new software or patch upgrade for Vinchin Backup Server or Backup Node is required, you can upload and upgrade Vinchin backup server or backup node from here.

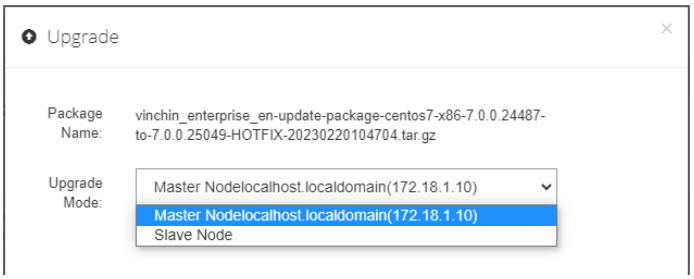


To upload a software package, please click on **Upload Package** button. In the popup dialog, click on Select Package to locate the software package.



You can upload multiple packages at a time, once selected all packages, please click **Upload** button to start uploading the selected software package(s).

Once uploaded, please select the target package and then click on the **Upgrade Now** button.



In the popup dialog, select the backup node and click on OK to upgrade. Please make sure you first upgrade the backup server (master node) then upgrade the backup node (slave node).

If you have multiple backup node deployed, you can select them all and upgrade them at the same time.

Notice

Software upgrade will require service restart, please make sure there're not jobs running on the backup server or backup node before upgrading.

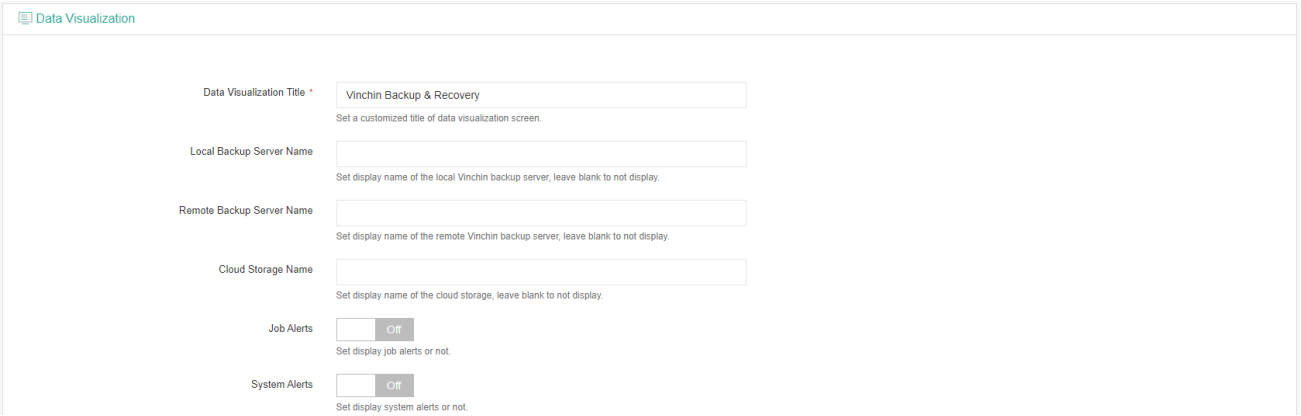
Data Visualization

Data visualization is a value-added feature which is available in Vinchin Backup & Recovery Enterprise edition, it briefly presents the real-time status and statistics of each data protection module. It can help users monitoring the backup infrastructure status on a command center screen or large screen monitors.

To open the data visualization screen, please click on the icon from the top right of Vinchin Backup Server web console.

A new tab page of data visualization will be opened.

Users can customize the data visualization settings from the **System** > **System Settings** > **Data Visualization** page.



In the **Data Visualization Title** field, users can define a customized name.

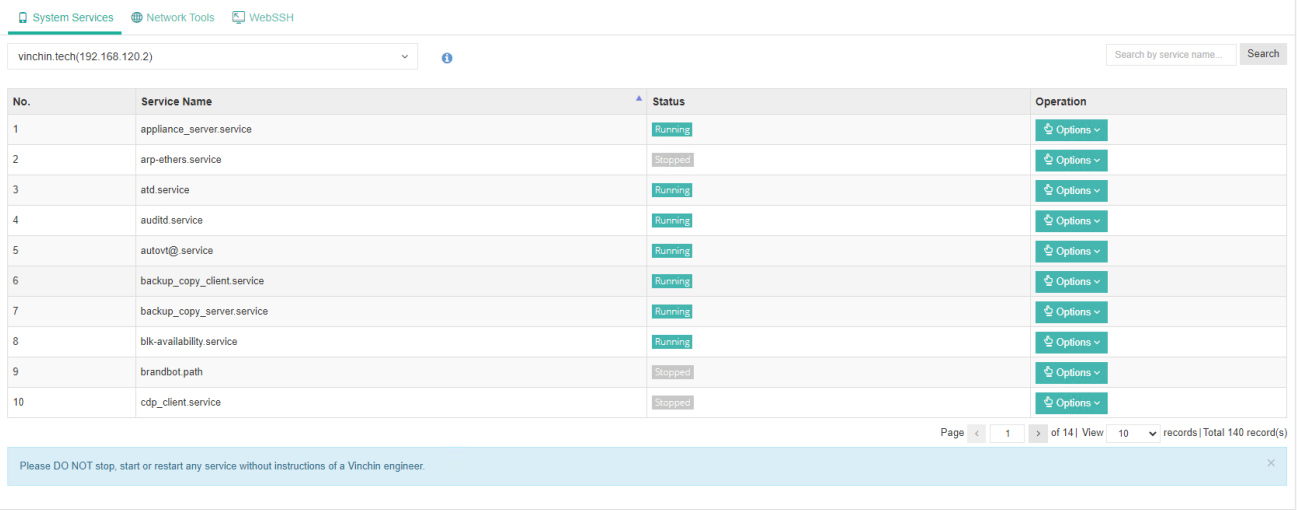
As for **Local Backup Server Name**, **Remote Backup Server Name** and **Cloud Storage Name**, users can also customize these items as per the actual deployment and demands.

For **Job Alerts** and **System Alerts**, if enabled, alerts of the jobs and system will be displayed on the data visualization screen.

System Tools

System Services

Service management can be used to check the backup server or backup node system service status and you can start, stop or restart the services.



In the dropdown list, you can select from Vinchin Backup Server and the backup nodes registered to the backup server to check the service status and perform operations to the services. And you can search specific services by service name.

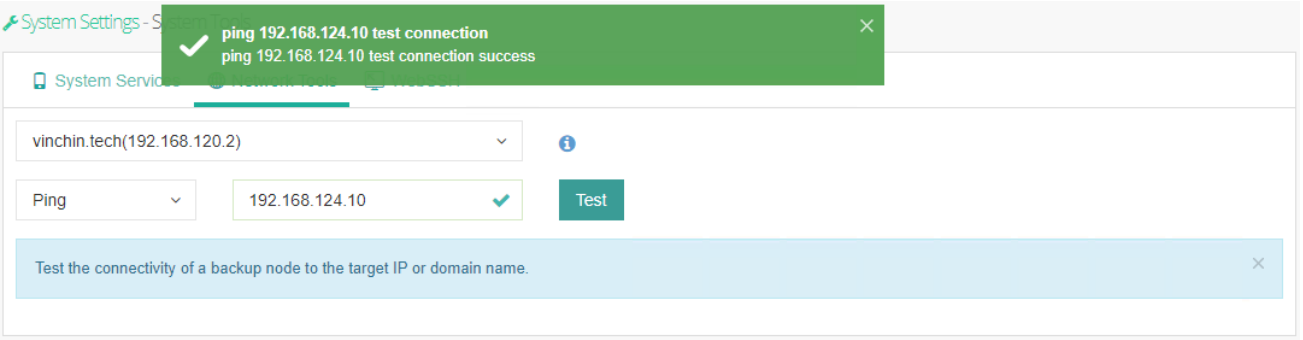
Warning

Service management is used for maintenance only, please DO NOT start/stop/restart any of the system services without the advice of a Vinchin engineer, otherwise your backup infrastructure may malfunction.

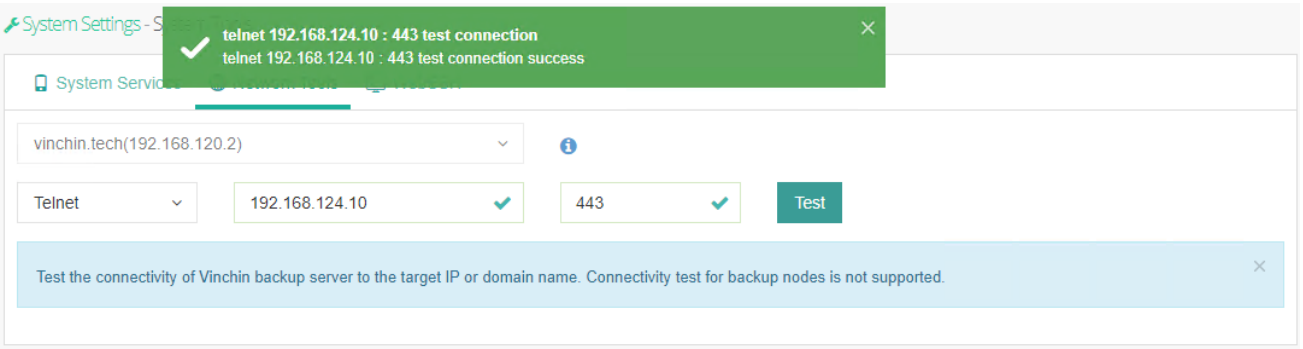
Network Tools

Network tools can be used to exam and troubleshoot the connectivity of each backup server/node with the target IP network.

Ping test can be used to test the reachability from the selected backup node to a specific IP address.

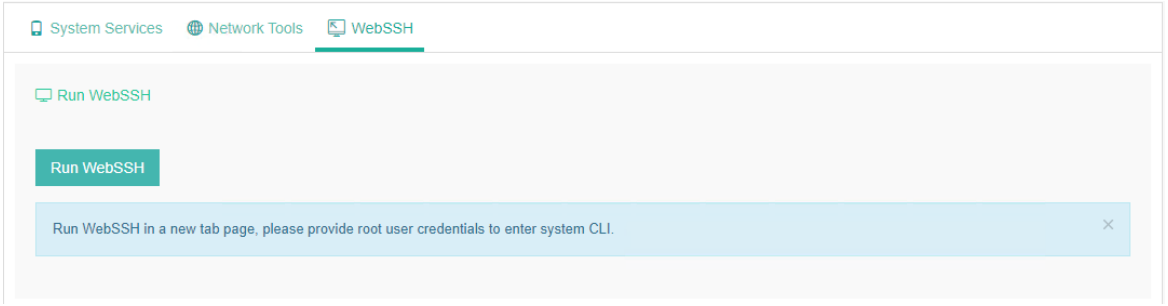


Telnet can only test the connectivity from the backup server to a specific host IP with a service port number.

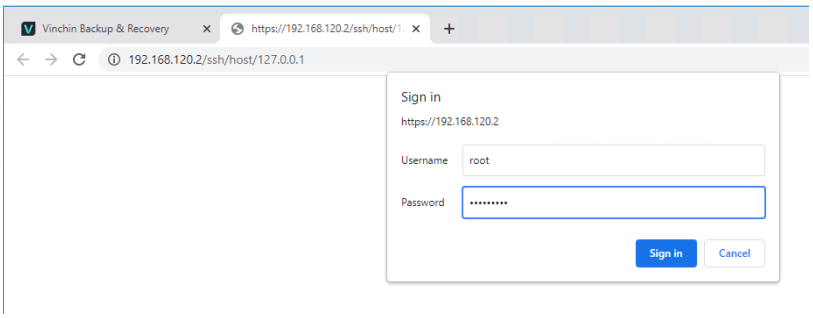


WebSSH & File Upload

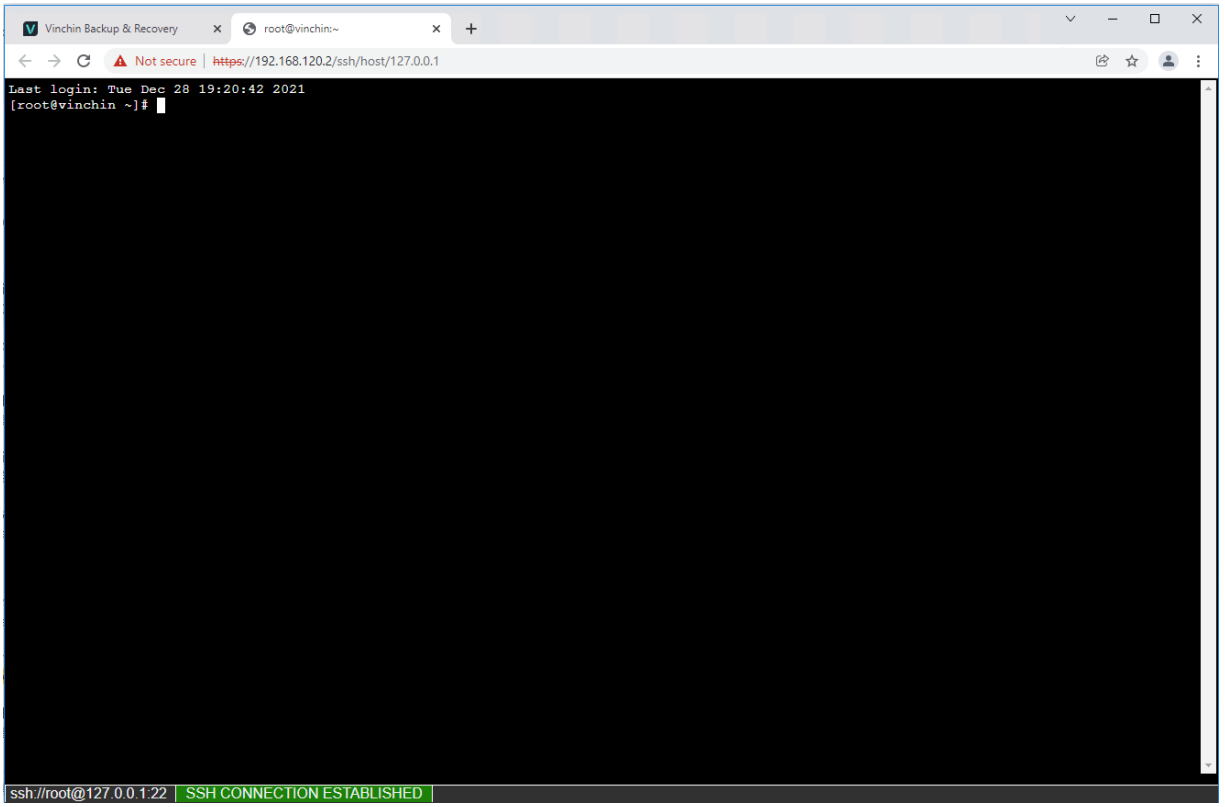
WebSSH can be used to connect to Vinchin backup server CLI directly through web browser, it is useful for server maintenance from CLI with using an additional SSH client application.



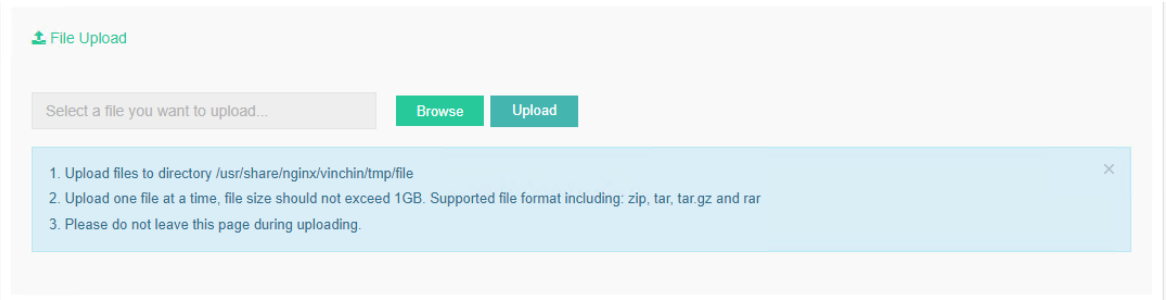
Click on the **Run WebSSH** button, a new tab page will be opened and prompting for CLI user credentials.



Simply enter the CLI user credentials and click on **Sign in** to connect to Vinchin backup server CLI. From within the WebSSH console, users are able to run commands the same way as using SSH client applications.



File upload can be used to upload certain types of files to Vinchin backup server file system without using a third-party tool.



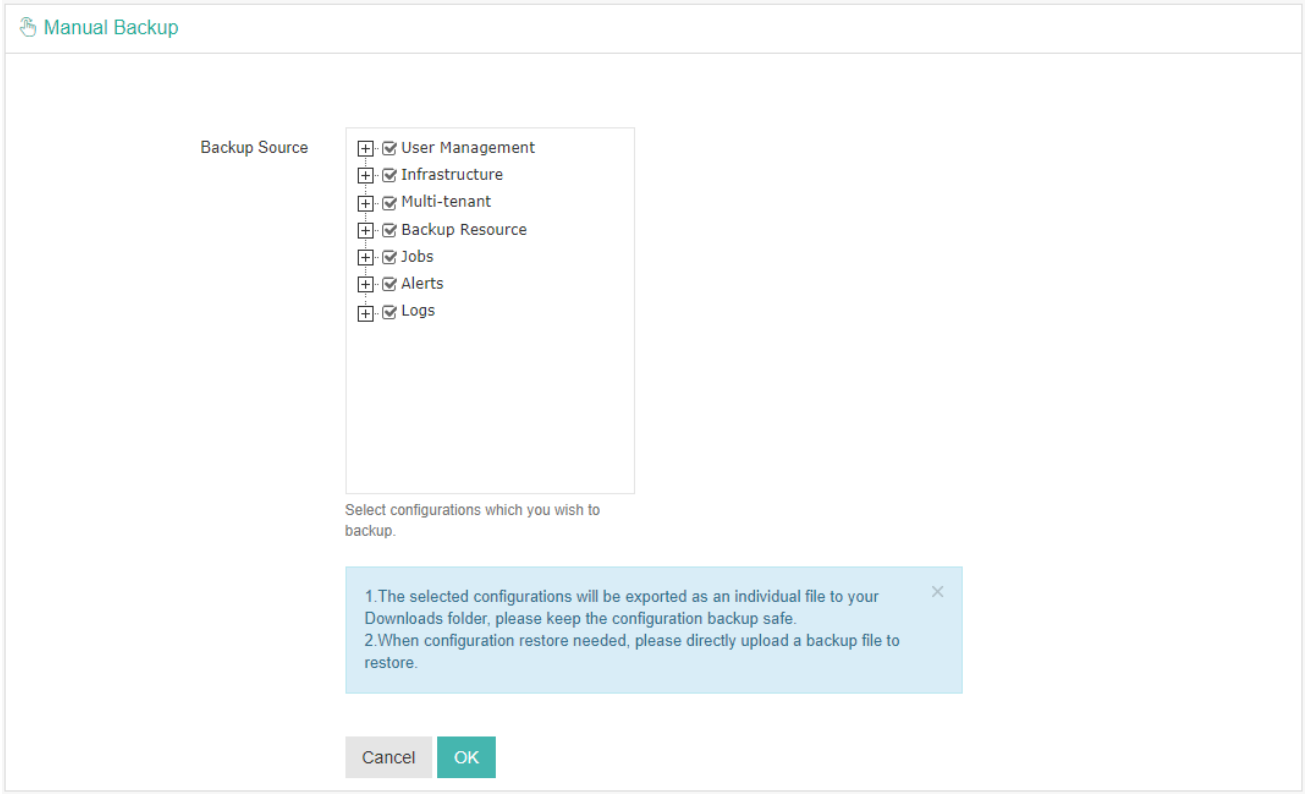
The supported file format including zip, tar, tar.gz, and rar, and the maximum file size allowed is 1GB. After uploading a file, users can find it from path /usr/share/nginx/vinchin/tmp/file/.

Configuration Backup

Configuration backup feature allows you to export the configurations of Vinchin backup server as backup files, and the backup files can be used for configuration restoration purpose upon a Vinchin server reinstallation or upon a Vinchin server configuration accidental deletion.

Manual Backup

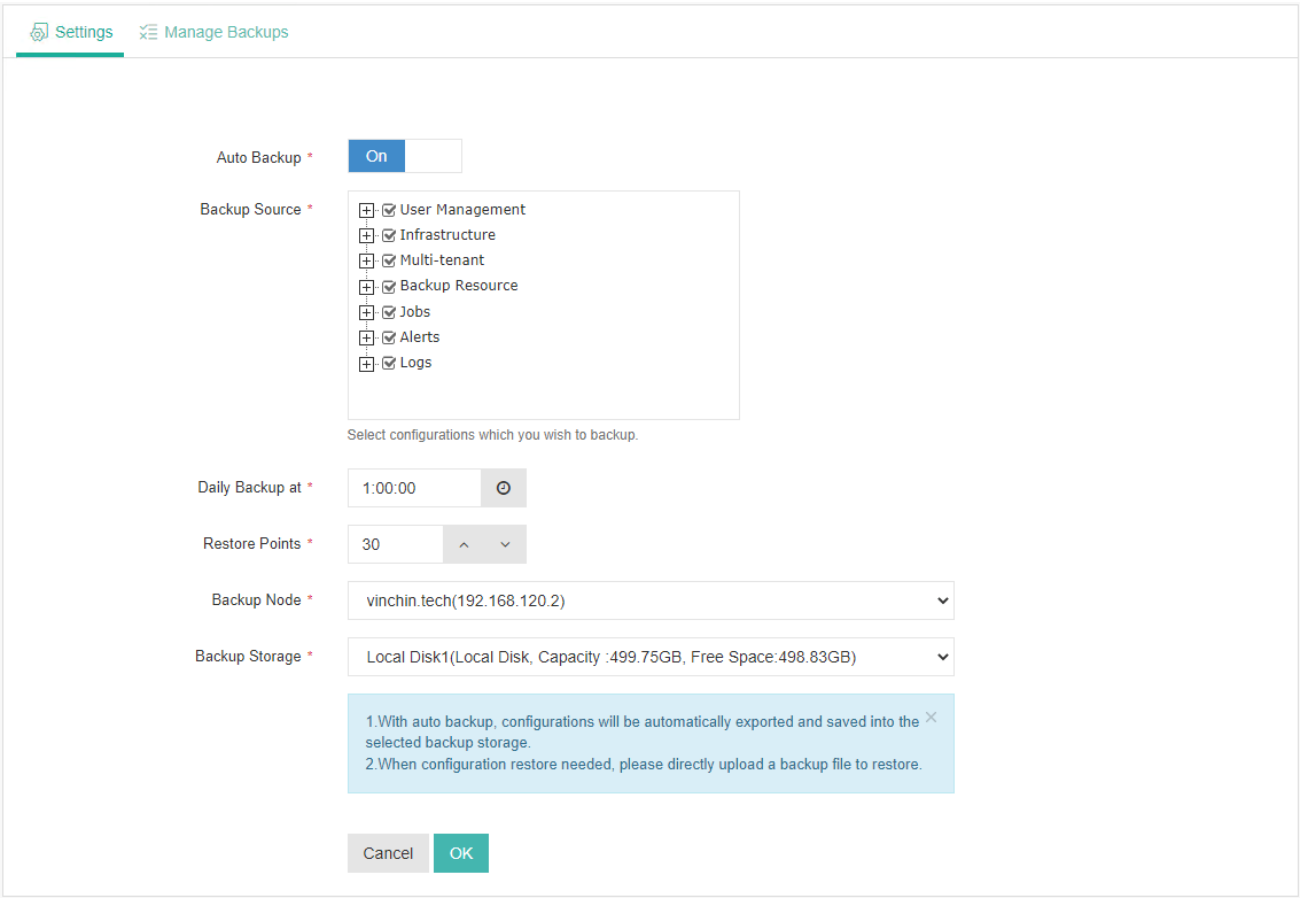
Select configurations which you wish to backup.



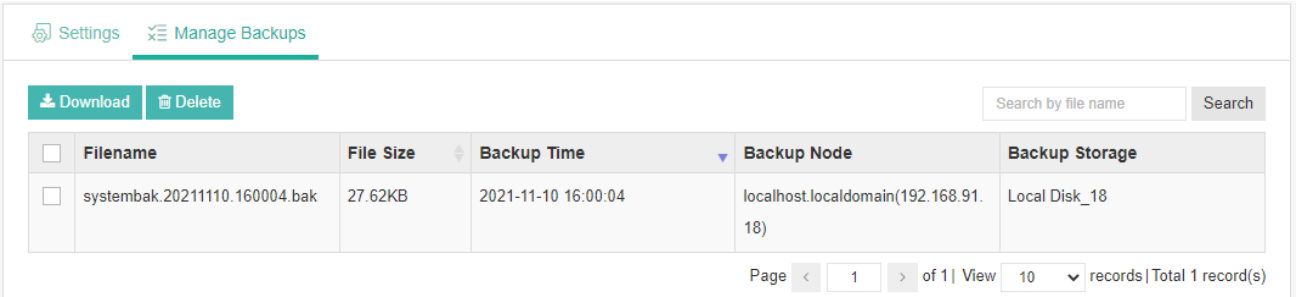
The selected configurations will be exported as an individual file and downloaded to your Downloads folder, please keep the configuration backup safe.
When configuration restore needed, please directly upload a backup file to restore.

Auto Backup

Auto Backup enables automatically backup of Vinchin backup server configurations on daily basis.



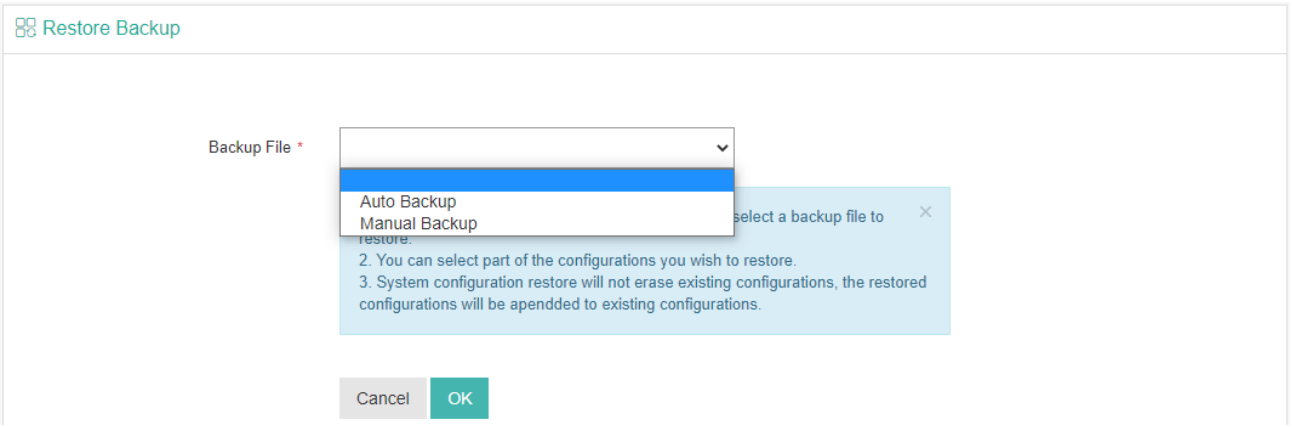
When enabled auto backup, users can select which configurations need to be backed up, and can pick a time of the day to run the backup. Restore points of the configuration backup determines how many (days of) backup files to be kept. A backup node and a corresponding backup storage can be selected to save the backup files.
The configuration backups can be accessed under **Manage Backups** tab.



Select the desired backup file and click on Download to download the backup file to your Downloads folder, or if the backup file is not needed or contain invalid configurations, select the backup file and click on Delete to delete it from the backup storage.

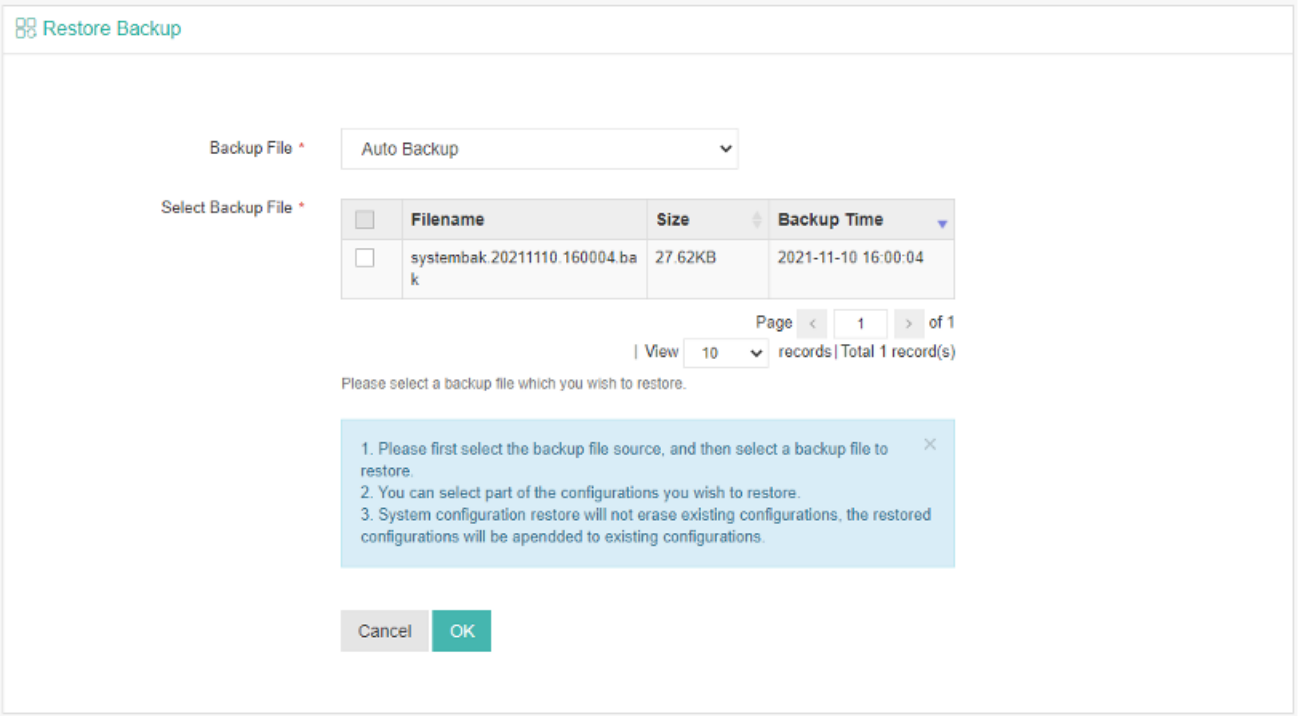
Restore Backup

When configuration restore is required, please go to **System > System Settings > Configuration Backup > Restore Backup** page.

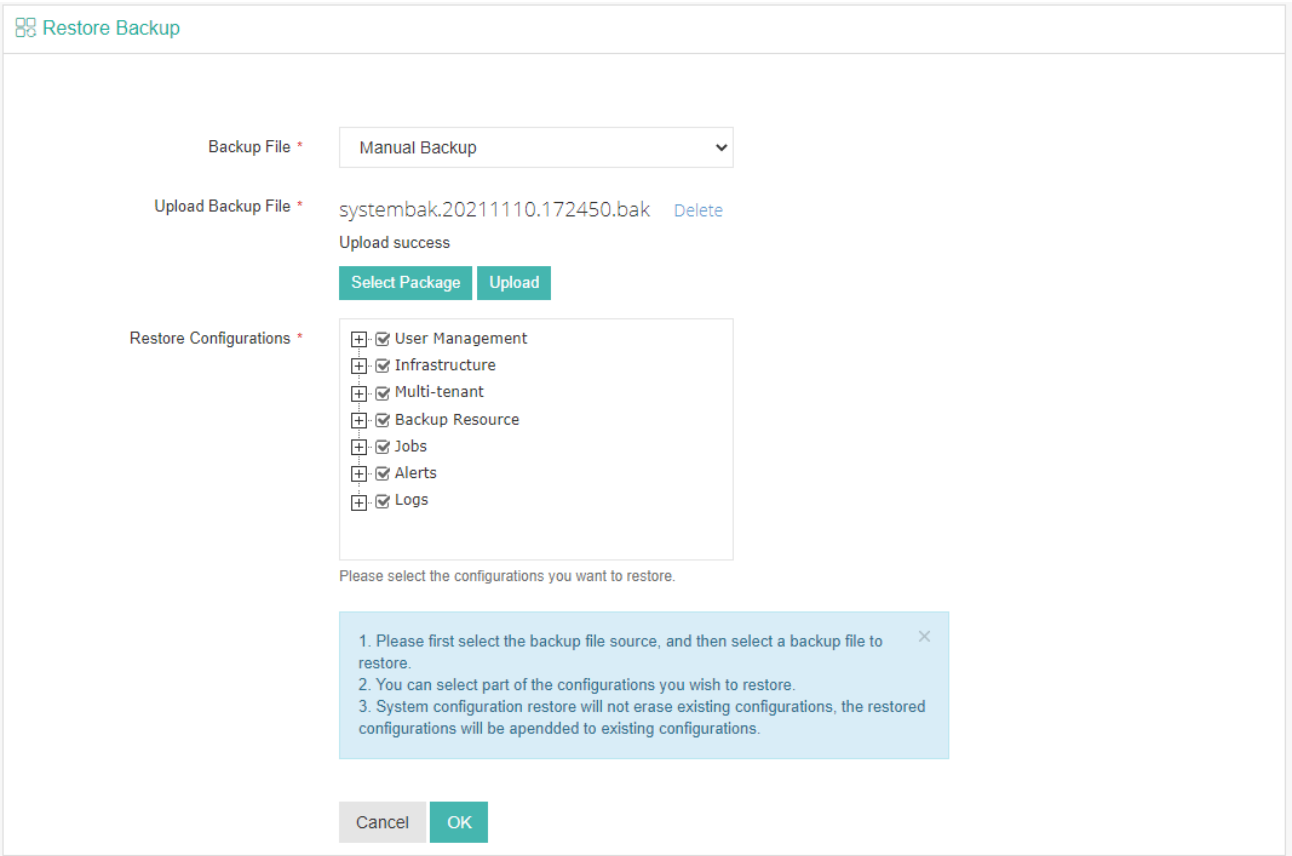


Select the backup file source, either auto backup or manual backup.

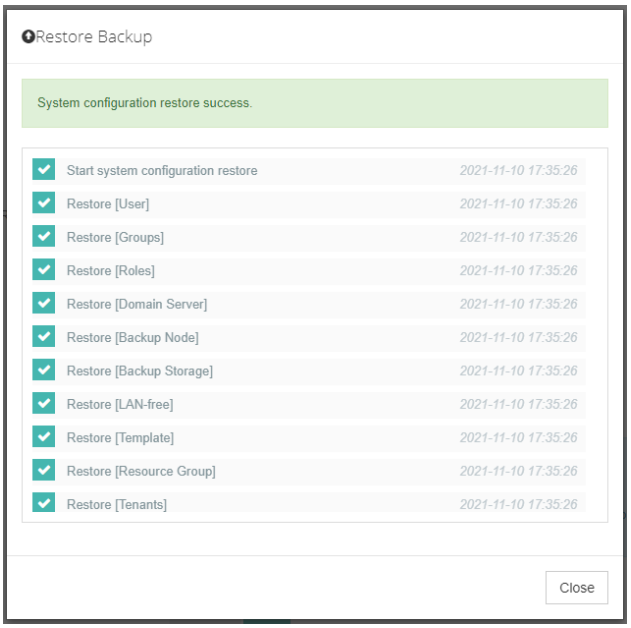
If Auto Backup, there will be a list of the backup files, you can simply select a desired backup file to restore the configurations.



If Manual Backup, you need to upload the configuration backup file to restore the configurations.



When the backup file is selected from the auto backup list or uploaded from user desktop to Vinchin backup server, please select the desired configurations you wish to be restored. Then click on **OK** to restore the configurations.



Note

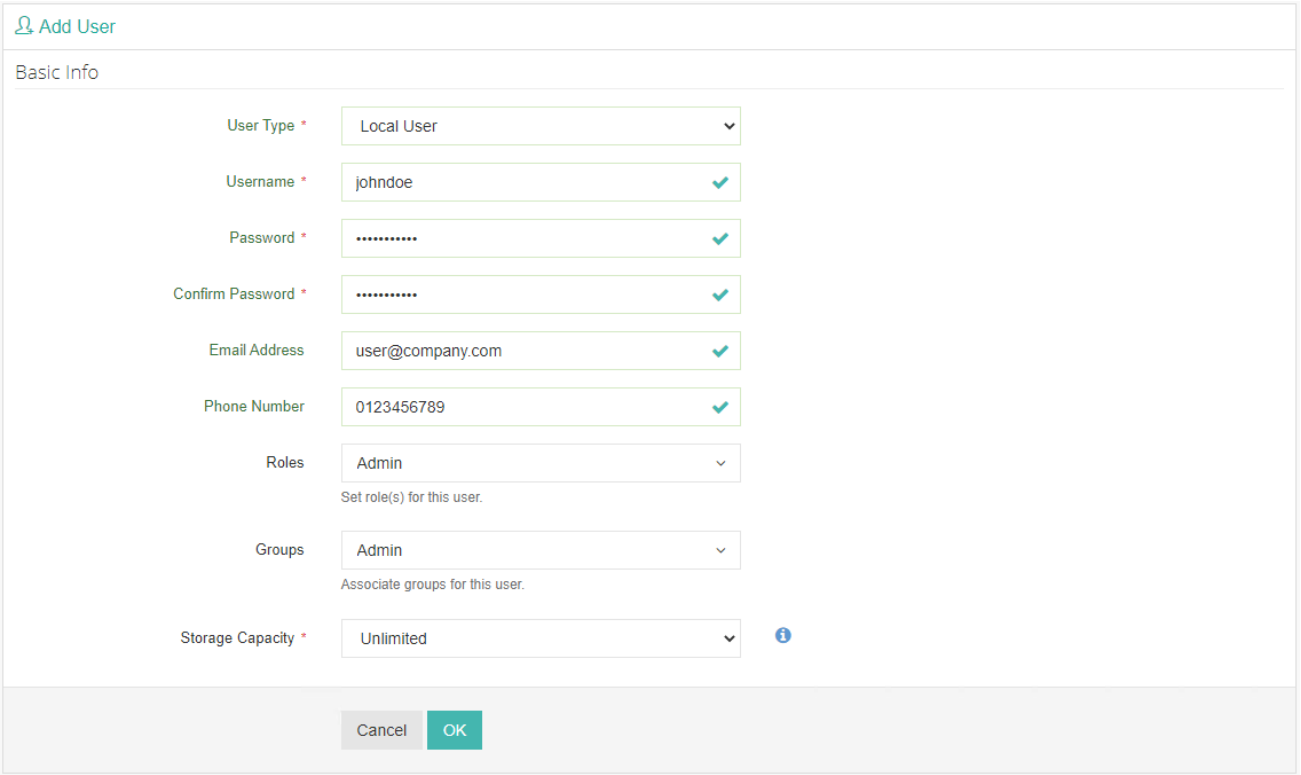
System configuration restore will not erase existing configurations; the restored configurations will be appended to existing configurations.

User Management

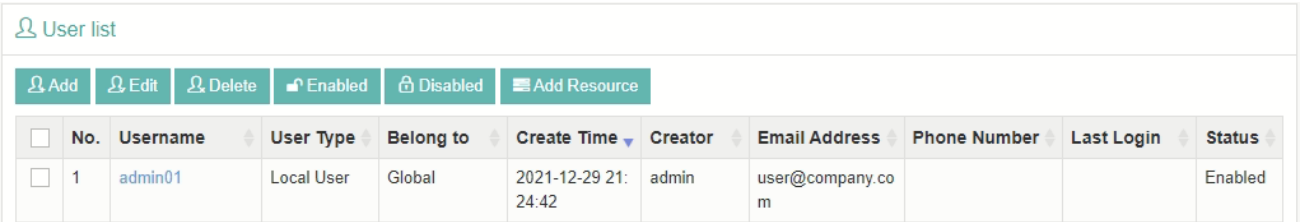
For an enterprise, administrators of Vinchin backup server can add users from internal departments of the enterprise who owns Vinchin Backup & Recovery infrastructure. They can share the resources of the backup infrastructure, like backup node and storage resources. But they need to add their own workloads to Vinchin backup server for backup and restore, like virtual infrastructure, file servers and database servers. So, each department runs their own backup services separately on the same backup infrastructure.

Users

Administrators are able to add multiple users from **System** > **User Management > Users** page. By clicking on the **Add** button administrator can add a new user.



The **User Type** can be **Local User** or **External User**. For local user, administrator needs to create a new user locally within Vinchin backup server. If external user, domain server integration must be done first. The newly added users can be assigned with different user roles and can be associated with desired user groups for permission management. And for storage capacity allowed to be used by this user can be set as Unlimited or Customized. Once a user had been added, it will be listed on the user management page.



You have the options to enable or disable a user from accessing Vinchin Backup & Recovery. To delete a user, if the

user has created subusers, it cannot be deleted, the subusers need to be deleted first.
And before this user can start any backup and restore services, administrator has to assign resources to the user at first place. The resources can be assigned to users including backup proxy, backup node and backup storage.
For the workloads which need to be backed up, users need to add from their own web portal, including virtual infrastructure (for VM backup), file backup agent and database backup agent.
If a user attempted to login with wrong password exceeded the Password Retry defined in Account Security settings, the account will be disabled. Only the administrator user who created that user has the permission to enable the account. Please select the disabled user and click on the **Enable** button to enable the user.

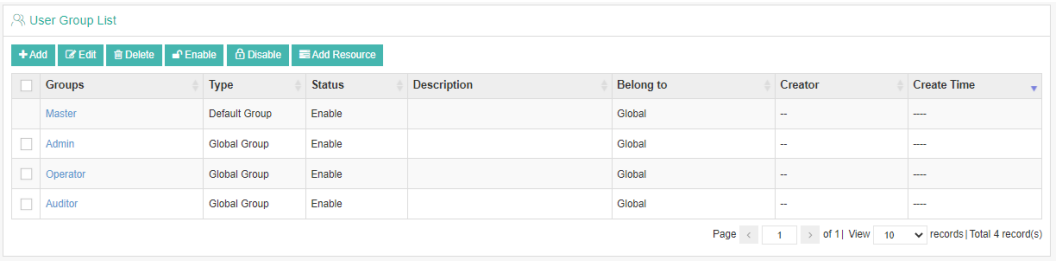
Note

Before deleting a user, you need to unregister all the virtual infrastructures registered by this user, otherwise the user cannot be deleted.

If the user role is admin and this admin user had added other users, then you need to delete the other users added by this admin user before deleting this admin user.

Groups

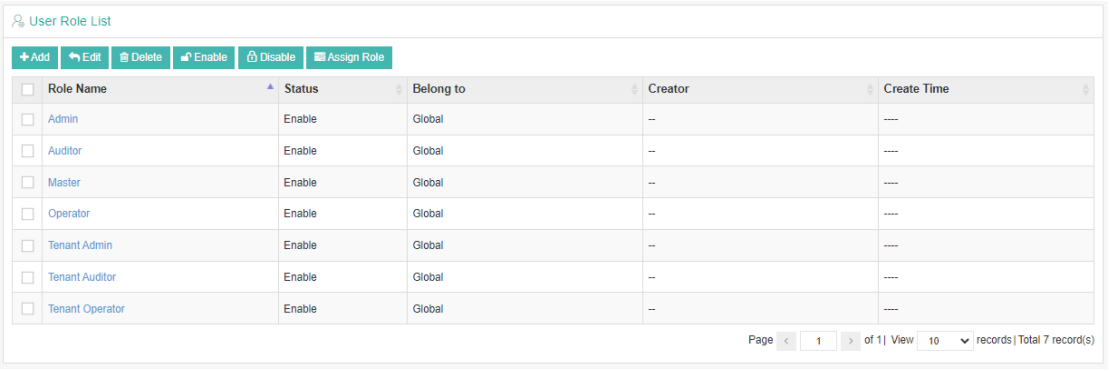
A user group is a collection of users who share the same resources and permissions.
There are default user groups which can be used for user permission management, but if needed, administrator can create new user groups with customized permissions.



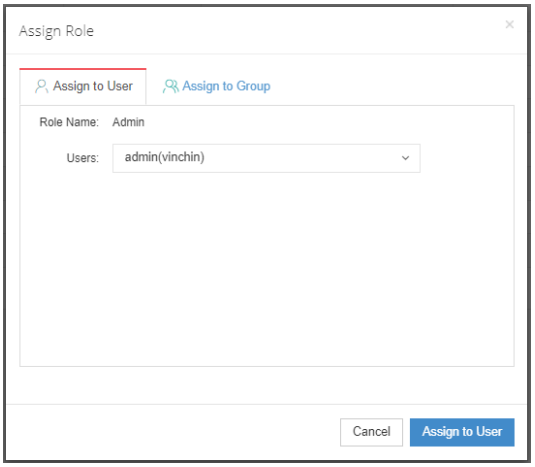
Click on **Groups** to view details about User, Roles, Resource Group and Permissions.
Click on Add Resource to add Backup Proxy, Backup Node, Storage Resources and Resource Group for groups. For the workloads which need to be backed up by the global users within the group, global users need to add from their own web portal, including virtual infrastructure (for VM backup), file backup agent and database backup agent.

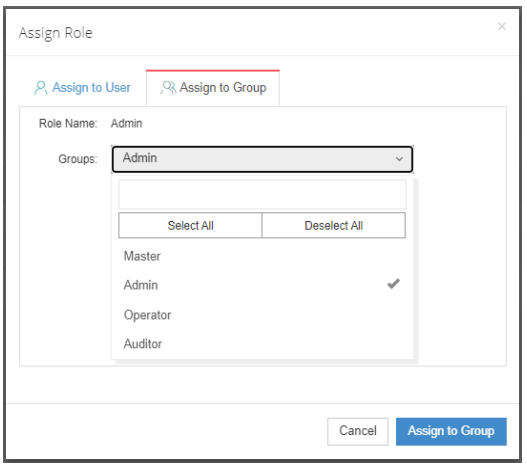
Roles

By default, there are 7 user roles available to be assigned to users or user groups.
Below are the permissions for different roles.

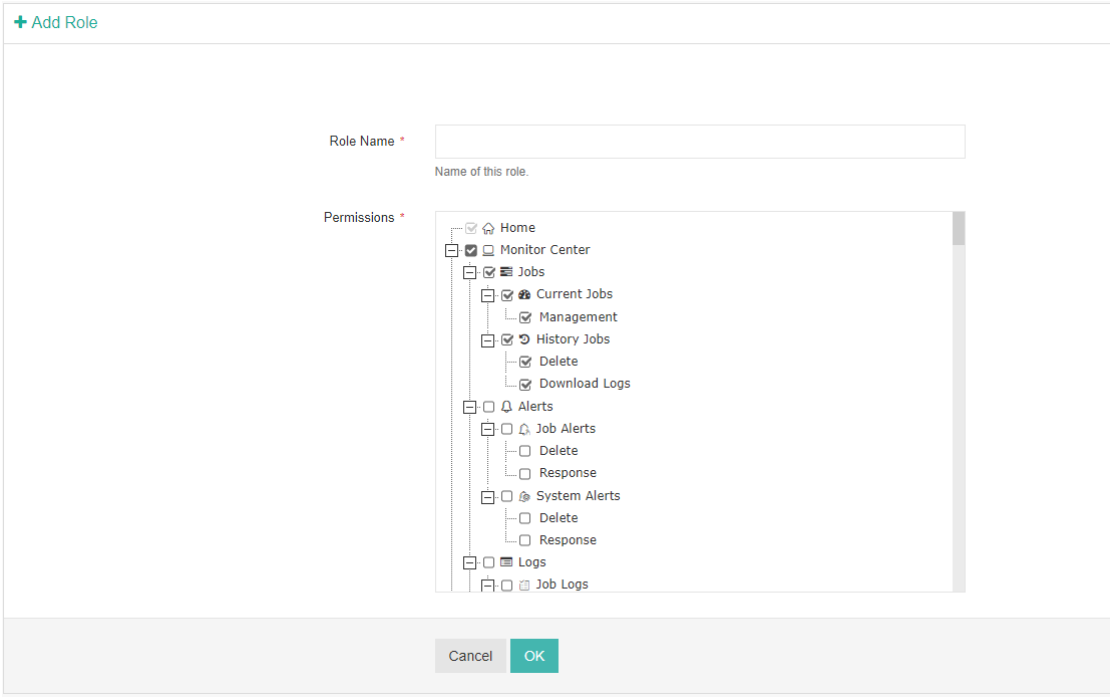


Master: the highest permission, has all management rights of Vinchin Backup Server.
Admin: System Alerts, System Logs, Storage Report, VM Report, Backup Node, Storage, LAN-free, Resource Group, all the System dropdown list and all User Management.
Operator: Current Jobs, History Jobs, Job Alerts, Job Logs, VM report, VM Backup, Database Backup, File Backup, Backup Copy, Backup Archive and Strategy Templates.
Auditor: Current Jobs, History Jobs, Job Alerts, System Alerts, Job Logs, System Logs, Storage Report and VM Report.
Tenant Admin: Current Jobs, History Jobs, Job Alerts, Job Logs, System Logs, VM Report, VM Backup, Database Backup, File Backup, Strategy Templates, Resource Group, Tenant Info and all User Management.
Tenant Operator: Current Jobs, History Jobs, Job Alerts, Job Logs, VM report, VM Backup, Database Backup, File Backup and Strategy Templates.
Tenant Auditor: Current Jobs, History Jobs, Job Alerts, Job Logs and System Logs.
You can assign role to users or user groups by selecting a role and clicking on **Assign Role** button, select user or user group you wish to assign.





Once a role had been assigned to a user or user group, the corresponding permissions of the role will be assigned to the user or user group as well.
If the default user roles cannot meet your actual requirements, you can also add customized new user roles by clicking on the Add button.

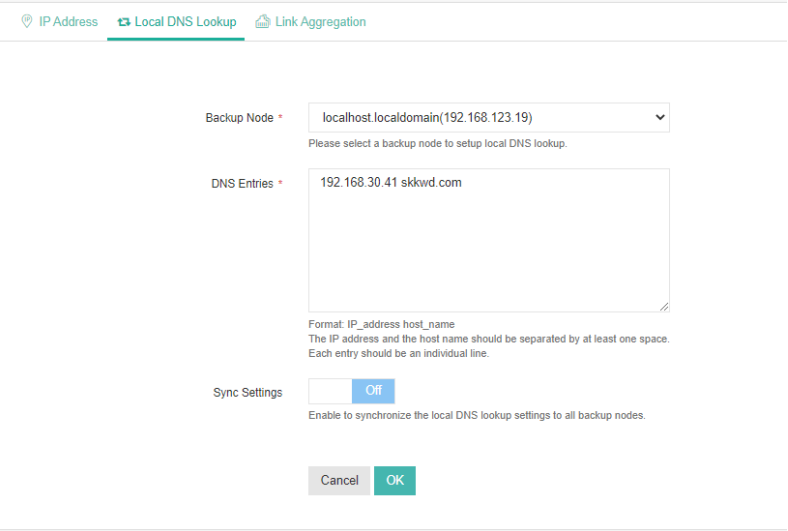


A role name is required to identify this new user role. And in the Permissions field, there's a tree menu showing all available web pages and operations of Vinchin web console, you can customize the permissions as per your needs.

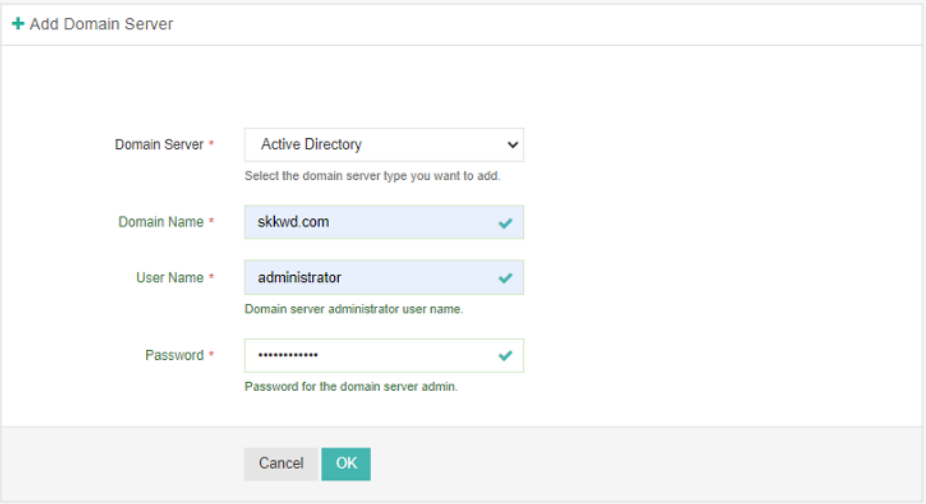
Domain Server

Domain server integration allows administrator to do user authentication by using the domain server. When a domain server is integrated, while adding new users, administrator can select to add External User which is from domain server. We currently support Active Directory server integration.

Before adding the domain server, first you may need to setup local DNS lookup. Click on **System** > **System Settings** > **Network Settings > Local DNS Lookup**, to set up Local DNS lookup, by using "IP_address host_name" format DNS entry is the DNS entries field.



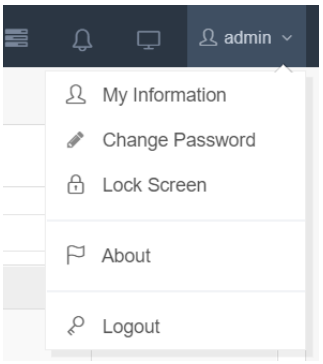
After setting up local DNS lookup, please go to **System > User Management > Domain Server** screen, click on Add button to add an Active Directory domain server.



Once a domain server is added, you are able to add external users from Active Directory domain server.

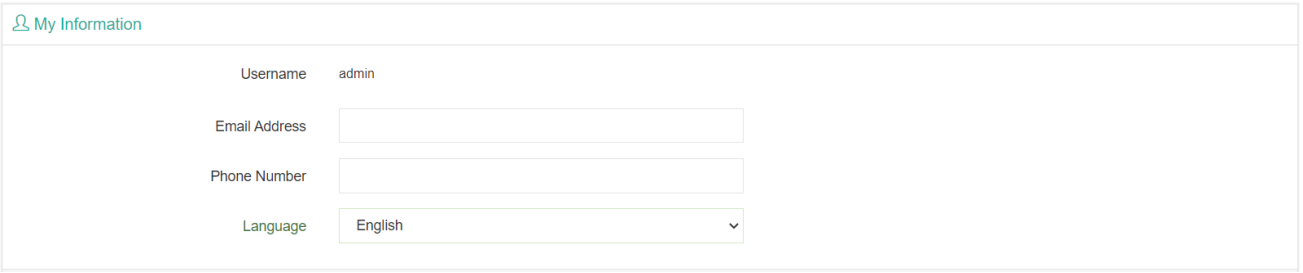
Account Settings

On the top right of Vinchin Backup Server web console, the current user login is displayed. Click on the username you'll be able to view the user information and manage some user settings.



User Information

On the user information screen, users are able to modify some basic user settings.



In the **Email Address** field, you need to fill in your Email address here, when you are trying to enable system notifications, an Email address is required here, and the system notifications will send to this Email address by default.

In the **Phone Number** field, you can optionally enter your phone number.

In the **Language** dropdown list, you can select a language which you are familiar with as the web console display language.

Change Password

Users can change their own passwords here and it is recommended to use strong password for system security. A strong password should be at least 6 characters, and should be a combination of digits, lower case and upper case letters and symbols.

Lock Screen

Users can lock Vinchin Backup Server web console from here, authentication will be required to unlock.

About

On the About page, users can get the system information and Vinchin contact information, and can follow us on social media, and also can participate in our user experience survey to help us to improve our products and services.

Logout

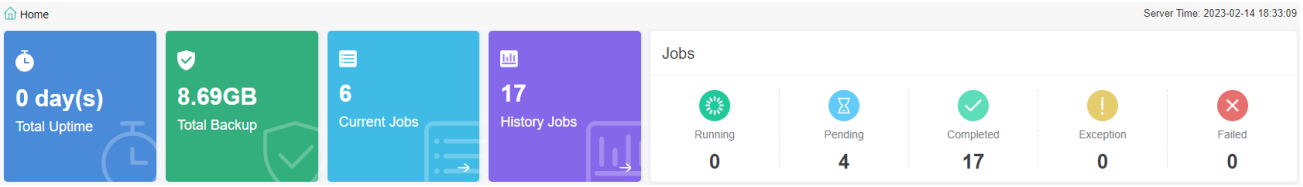
Users can sign out the current user login from here.

Informational

Home

Each time when you log in to Vinchin Backup Server you'll first see the **Home** screen, here you can have an overview of the backup server status.

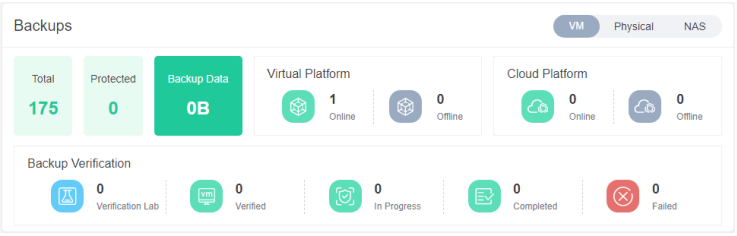
On the top of the home screen, the current server time is displayed.



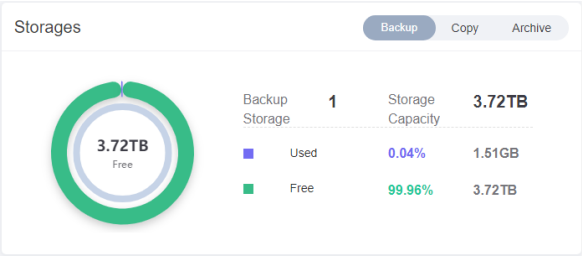
On the left the total server uptime, total backup size, current job counts and history job counts are displayed.

On the right, the Jobs section, the number of jobs (sessions) are categorized by running, pending, completed, exception and failed. Users can have a straightforward overview of the system running state.

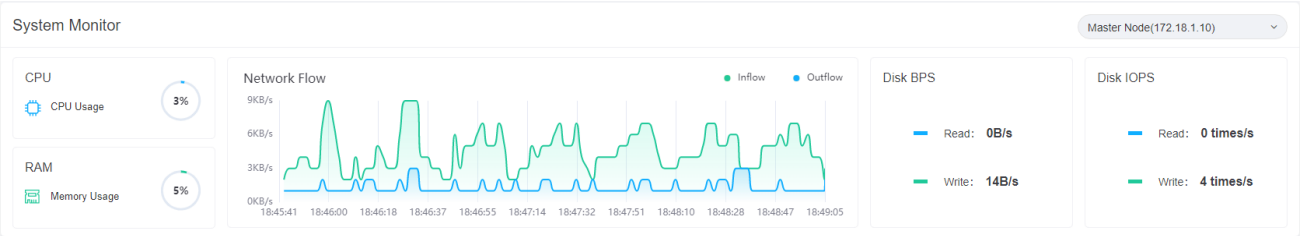
In the **Backups** section, the statistics of **VM**, **Physical** and **NAS** backup modules are displayed.



In the **Storages** section, the statistics of **Backup**, **Copy** and **Archive** storages are displayed.



In the System Monitor section, a basic monitoring view will be displayed.



If you wish to get more information of system monitoring, please go to **Monitor Center** > **System** page.

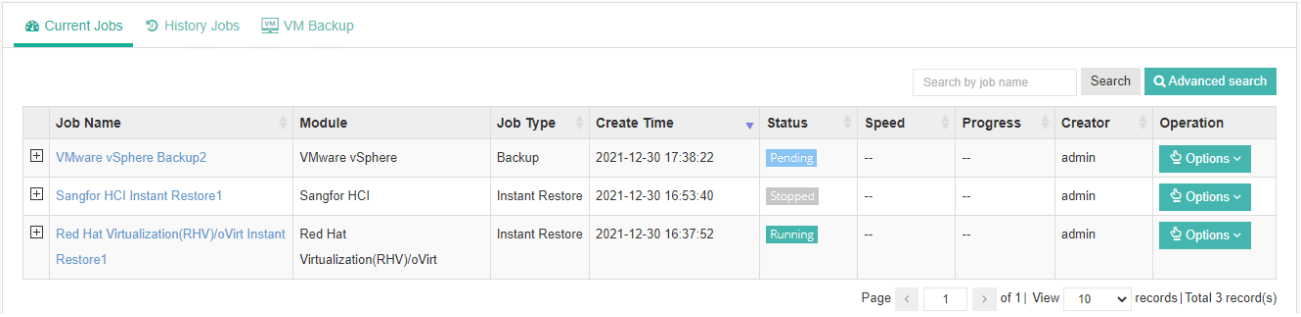
Monitor Center

Jobs

On the **Monitor Center** > **Jobs** page, all jobs created on Vinchin Backup Server are able to be viewed and managed here. The jobs which are in running state, pending state, stopped state and failed stated will all be listed in the **Current Job** list. And the jobs which had been executed will all go to the **History Job** list.

- **Current Job**

After creating a new job (backup/restore/archive), you can view and manage the newly created job in the **Current Job** list. All the basic information and status of the job will be shown in the current job list. You can start, stop, edit or delete the job accordingly.



Click on the **Options** button of a job, you'll have the following options.

Schedule On: to turn the schedule on of a **Stopped** job, after turning on, the job status should become Pending.

Start Full: manually perform a full backup of the VMs included in this backup job.

Start Incr.: manually perform an incremental backup of the VMs included in this backup job.

Start Diff.: manually perform a differential backup of the VMs included in the backup job.

Stop: to turn the schedule off of a pending job or to stop a running job.

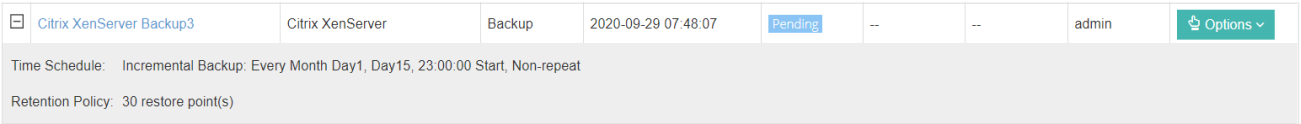
Edit: to modify the configurations of a job in Stopped state.

Delete: to delete a job and all the schedules, but the backup data will remain.

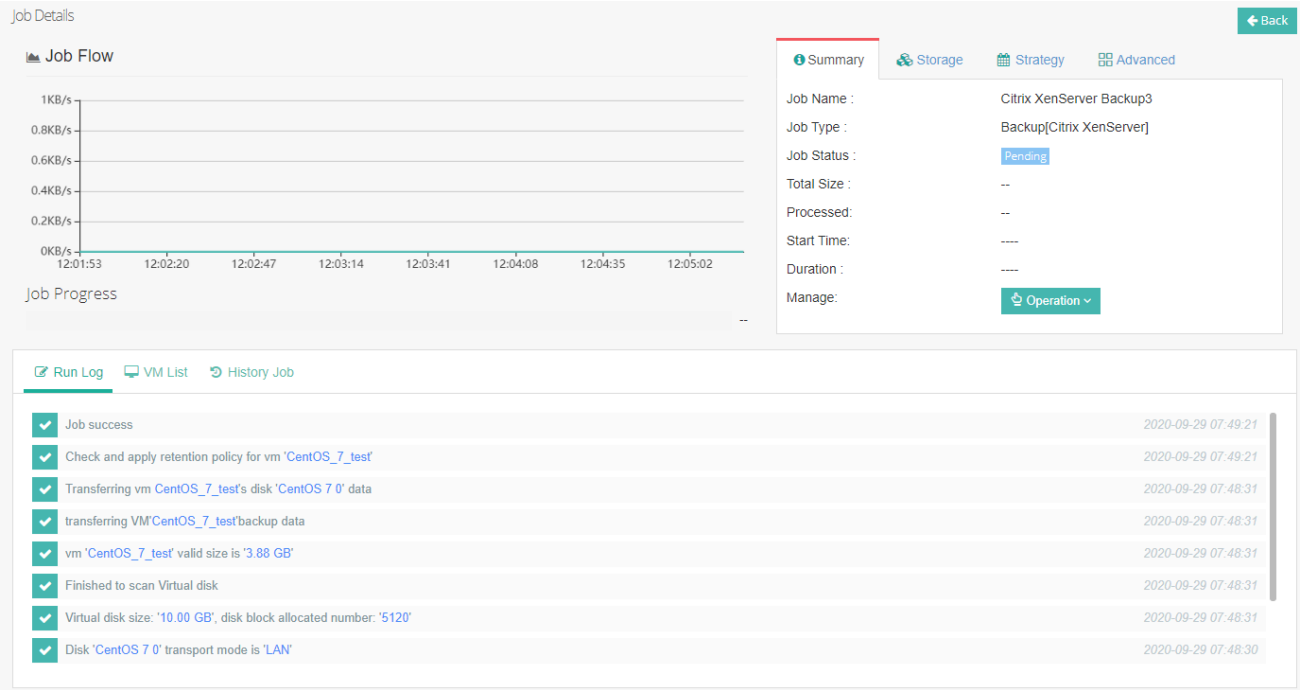
Note

To edit a job, the job needs to be stopped first.

From the job list, by clicking on the ⊞ button, you can check more information of a job.



Basic info such as the backup time schedule and retention policy will be given. If you want to check even more information, please click on the job name, then you'll be directed to the **Job Details** page.



Job details explanations:

Job Flow: the real-time data transmission flow will be displayed to indicate the transmission speed of a currently running job.

Job Progress: a real-time progress bar to show the progress of a running job.

Summary: basic description of the job.

Storage: the storage destination of the data flow.

Strategy: the type and schedule of the job.

Advanced: the advanced options for the job.

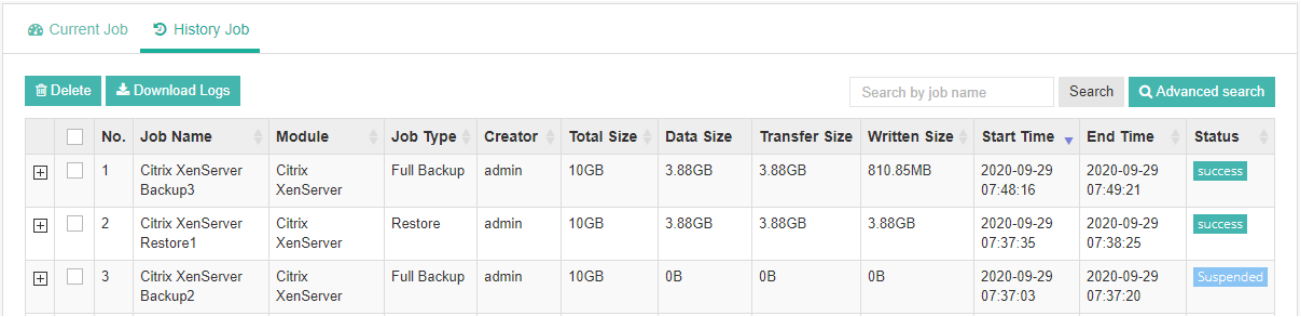
Run Log: if the job is currently running, it will be the real-time log output; if the job is pending or stopped, it will provide the logs of the last time of running.

VM List: if the job is running, all VMs included in this job will be listed here.

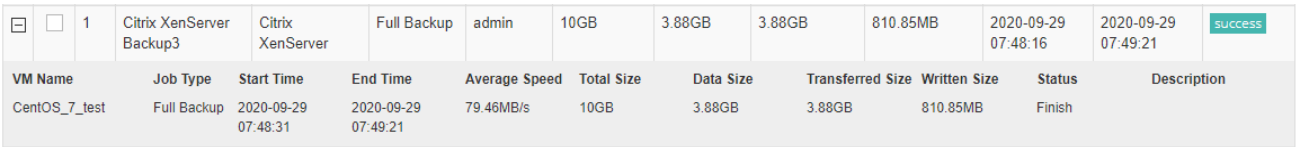
History Job: the running history of the job.

- **History Job**

All history jobs can be found on the **Monitor Center** > **Jobs** page, under the **History Job** tab.



Click on the ⊞ button you can expand a history job to view the detailed information.

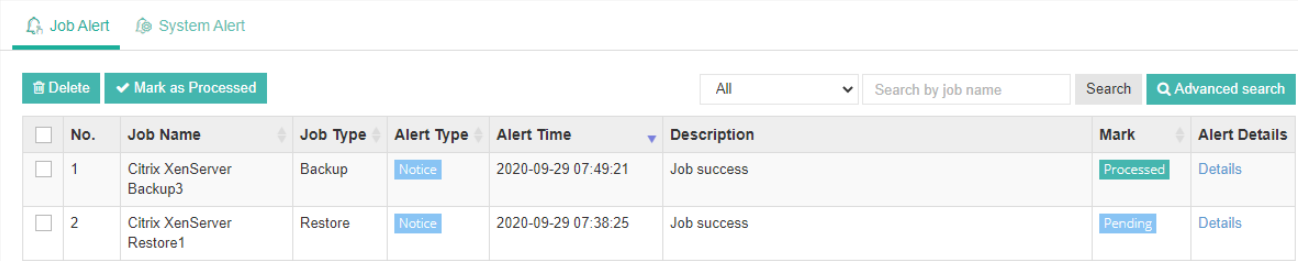


To delete the history jobs, please select the job logs and click on the **Delete** button.
And for the failed jobs, you can select that job and click on **Download Logs** button to download the detailed logs of that job for troubleshooting.

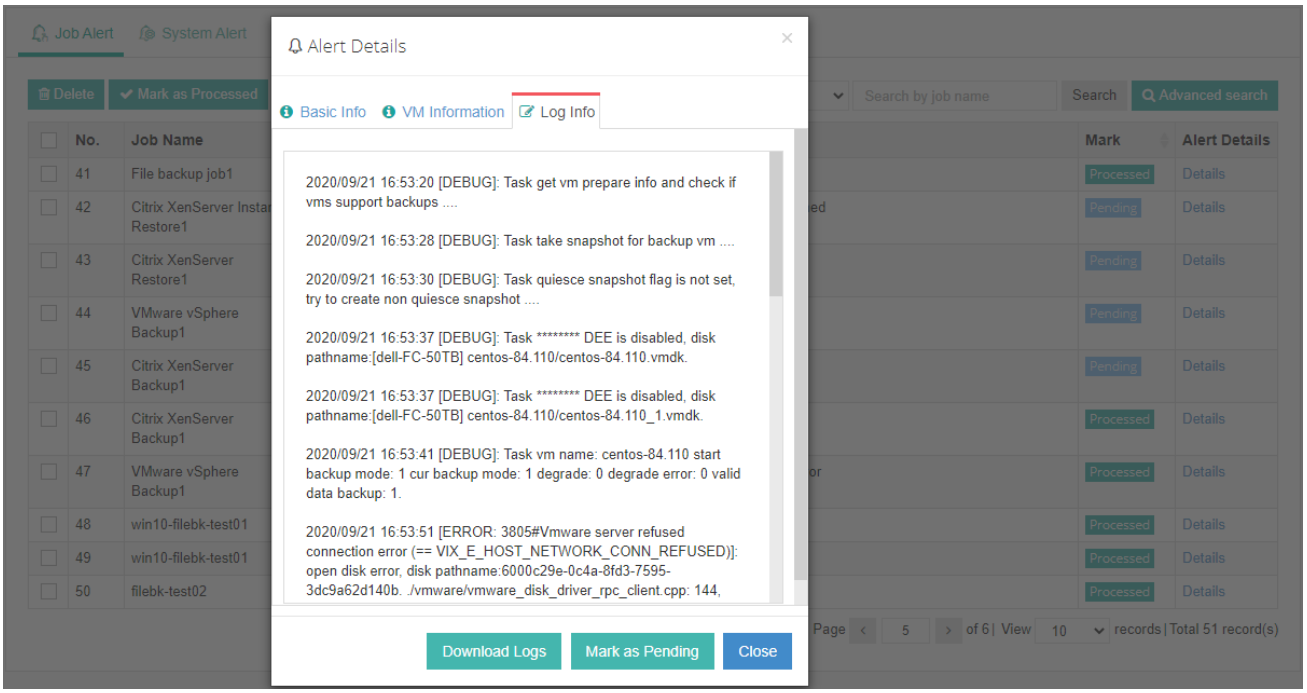
Alerts

- **Job Alert**

Job alerts can be found on the **Monitor Center** > **Alerts** page, under the **Job Alert** tab.



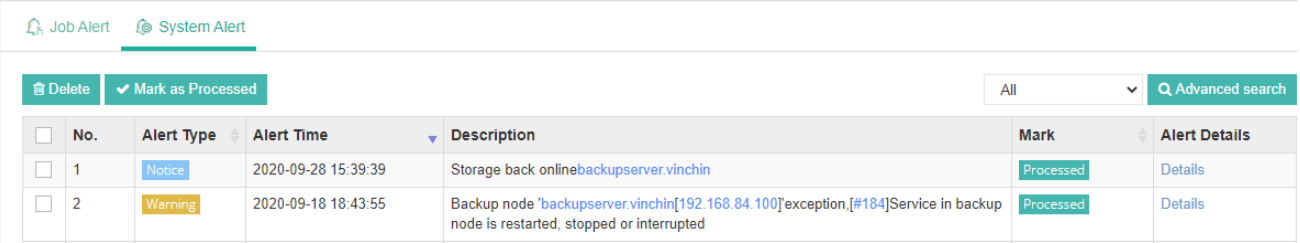
By using the dropdown list above the alert list, you can filter the alert messages by alert types, including notices, warnings and errors.
Click on **Details** button of an alert, you can view the detailed description of the alert message, and at the same time the alert message will be marked as **Processed**. The alert message mark will be viewed and processed by all users who have permissions to do this.
If it is an error alert, you can check the errors from **Log Info** tab as below.



The errors you got here can be used for troubleshooting the failure of the job, by clicking on the **Download Logs** button you can download the error logs as a plain text file. And if you don't want to mark the error alert message as processed, you can click on **Mark as Pending** button to mark this alert to pending state.

- **System Alert**

System alerts can be found on the **Monitor Center** > **Alerts** page, under the **System Alert** tab.



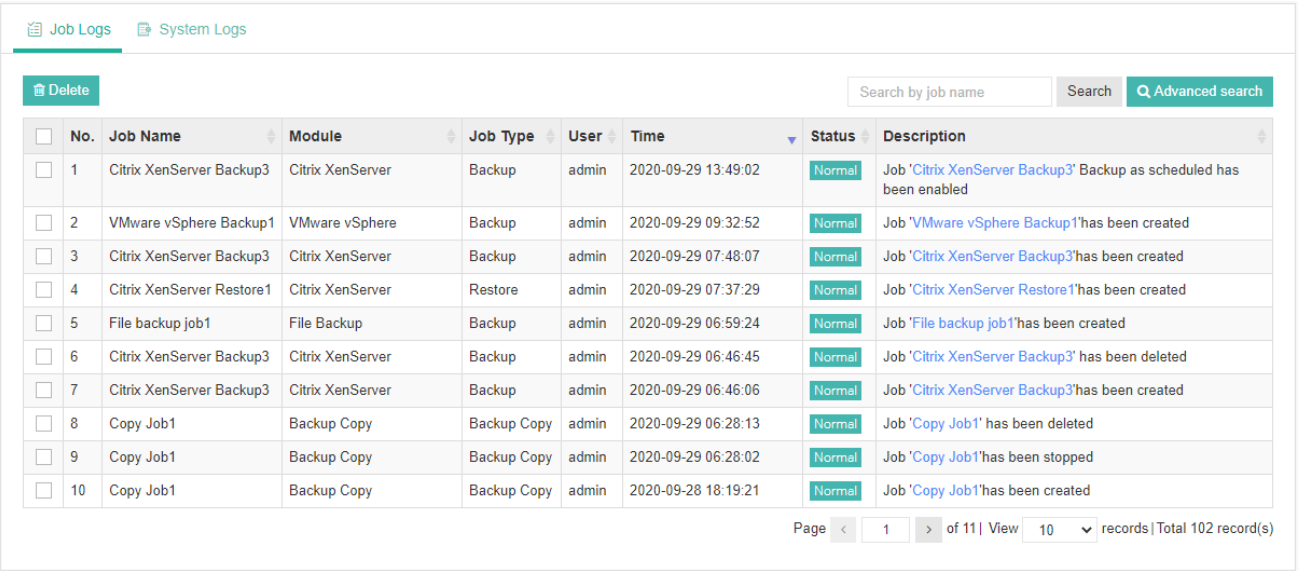
Similar as the job alerts, you can have the same options to filter these alert messages and you can mark the messages as processed or pending state.

System alert messages are mainly used to notify users about the backup server, backup node(s) and storages status.

Logs

- **Job Logs**

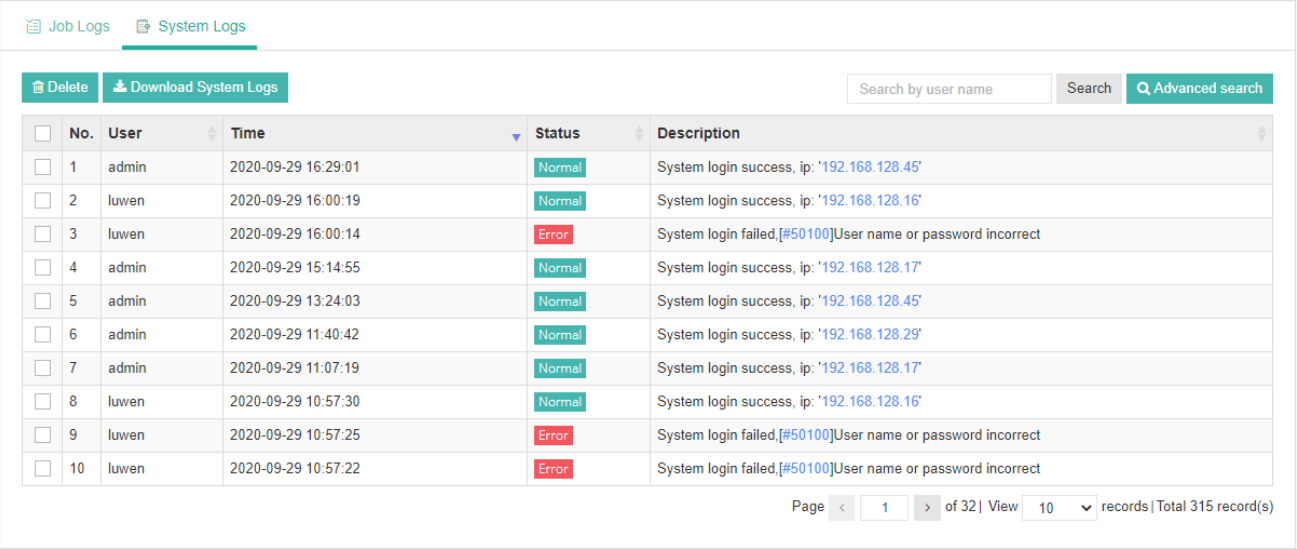
On the **Monitor Center** > **Logs** page, under the **Job Logs** tab, the operations related with job stop, job schedule on, job creation, job deletion and job modification can be all found here.



Each row in the job log list corresponds to an operation to a specific job. The name of the user who performed the operation and the time of when the operation had been performed will be given.

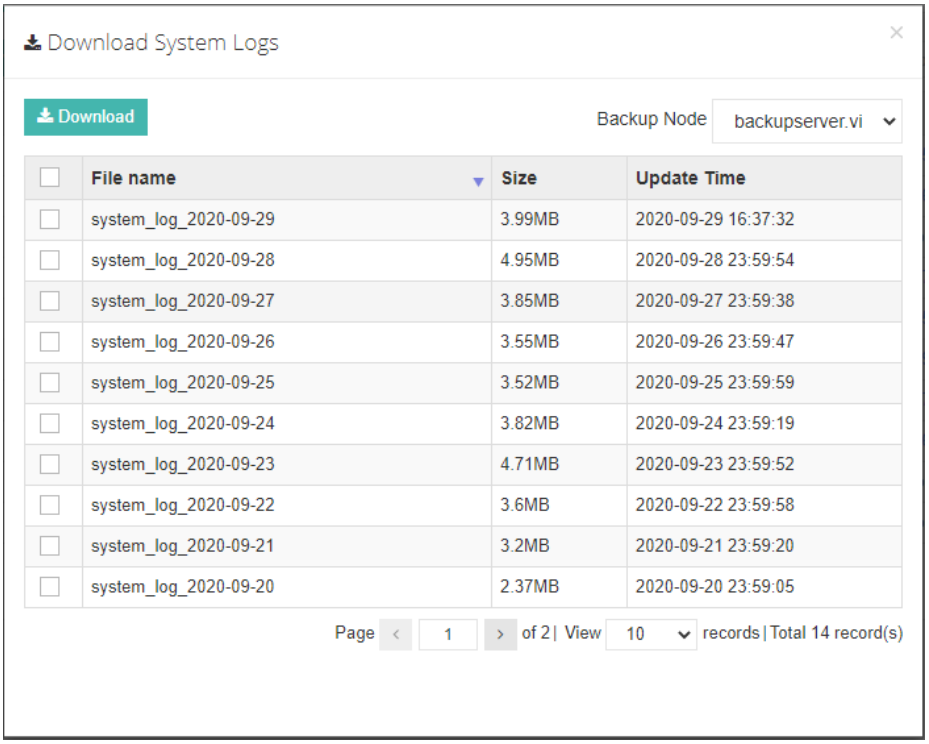
- **System Logs**

On the **Monitor Center** > **Logs** page, under the **System Logs** tab, all user activities can be found here.



The logs can be filtered by typing specific user name in the search box.

And you may download the system logs by clicking on the **Download System Logs** button.



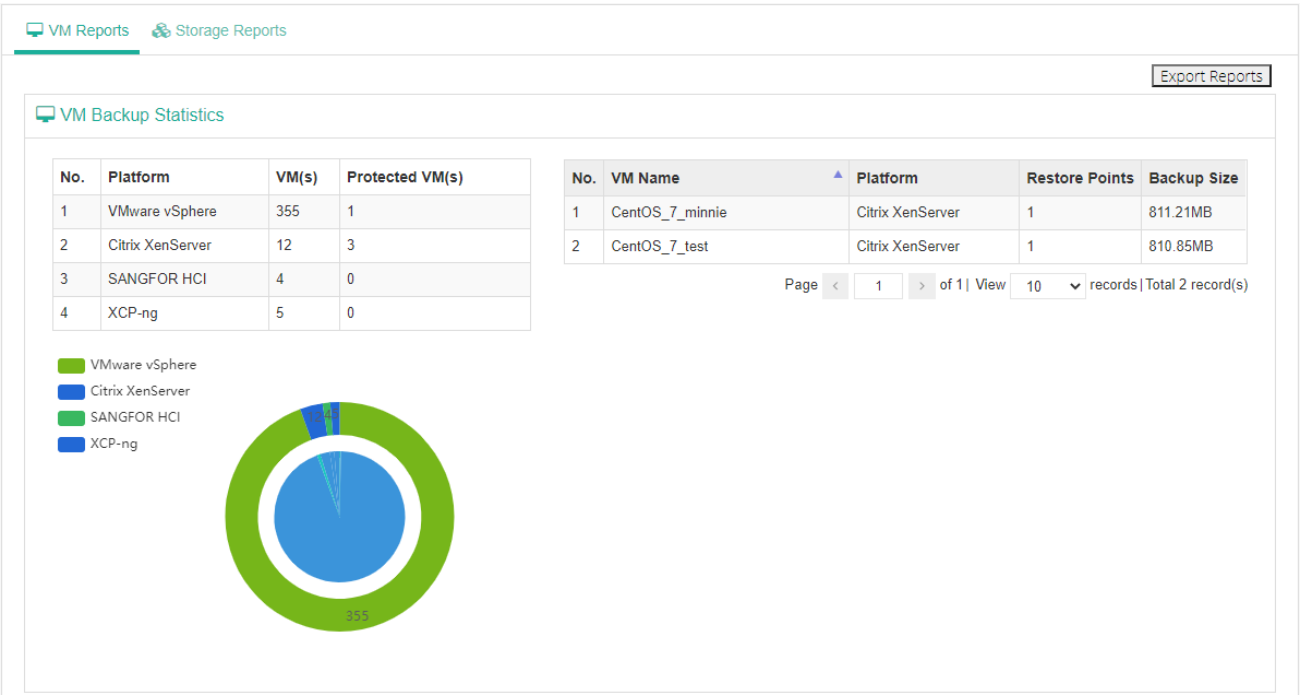
In the **Download System Logs** dialog, the logs are arranged by date. You can select the desired logs and click on the **Download** button to download the logs.

And on the top right of the dialog, you can choose a specific backup node to download the logs related to the selected backup node.

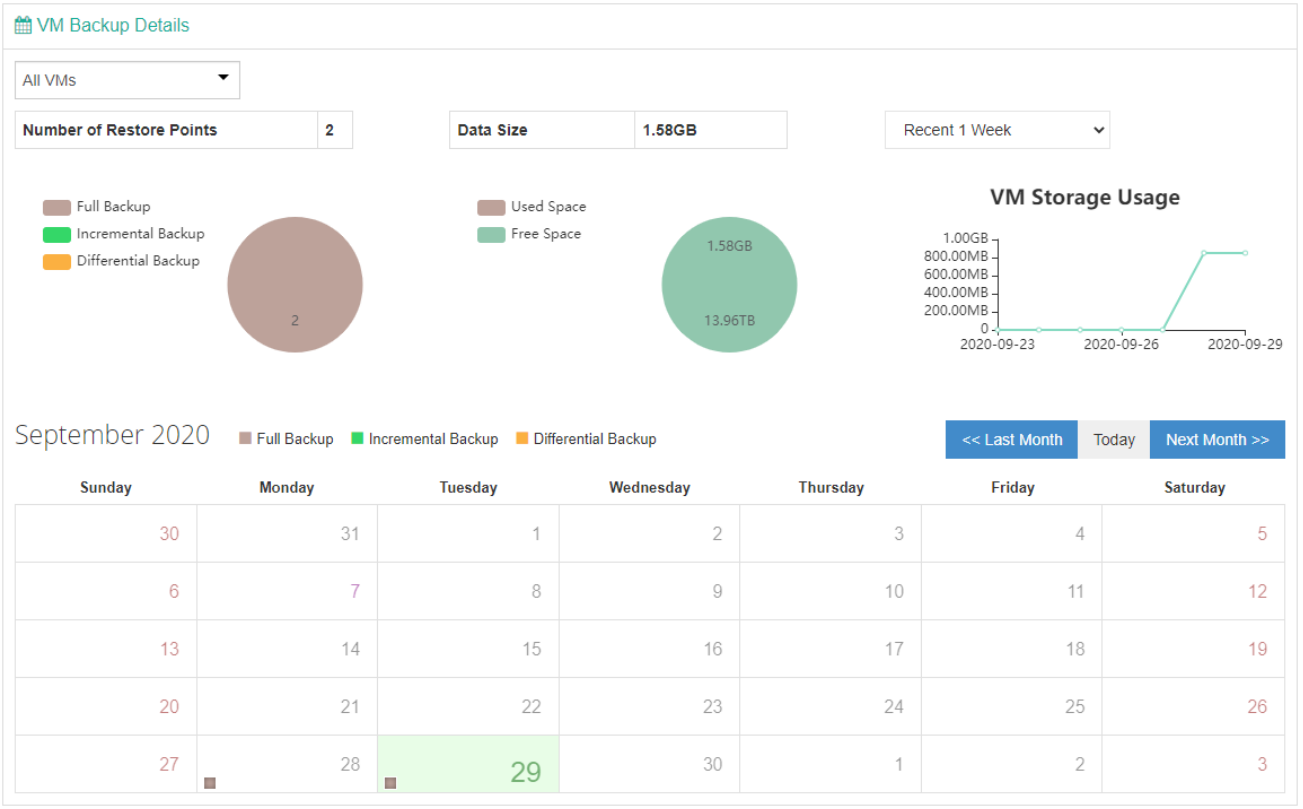
Reports

- **VM Reports**

You can check the VM Backup Statistics from the **Monitor Center** > **Reports** page, under the **VM Reports** tab.



In the VM Backup Statistics section, you can have the statistics reports of the virtual platforms, protected VMs and the restore points of the protected VMs. And you can export the reports to a PDF file by clicking on the **Export Reports** button.

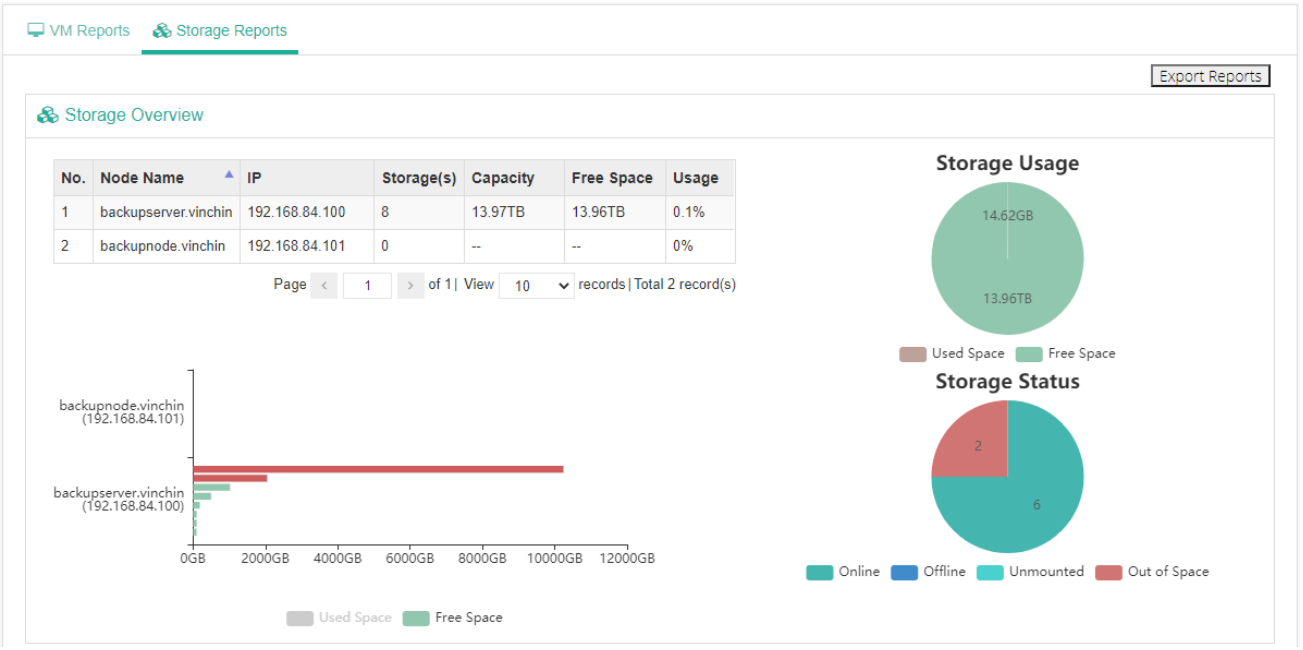


In the VM Backup Details section, you can have the following statistics reports:

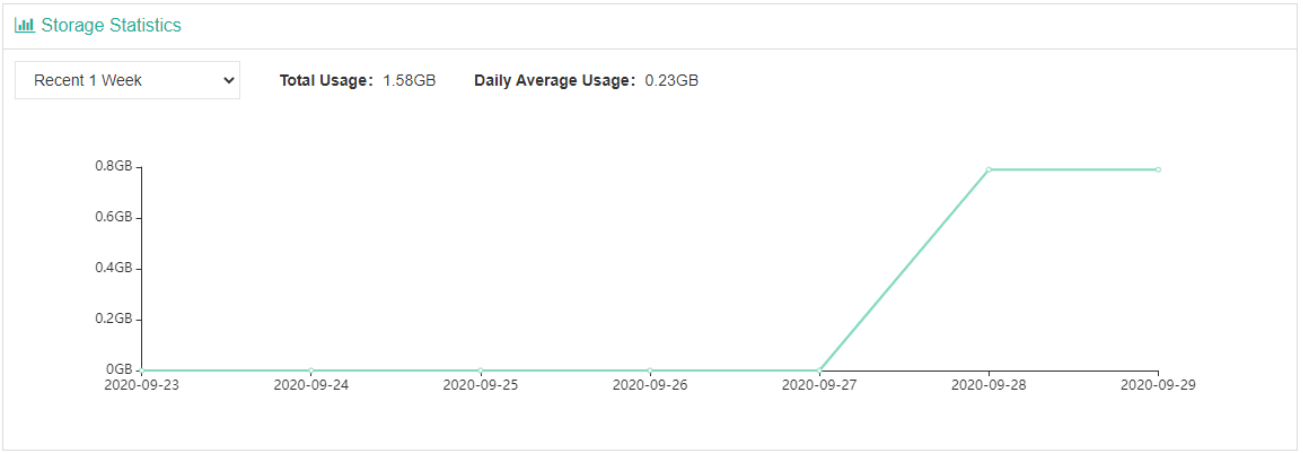
- Number of restore points and a pie chart of restore points by different backup technologies.
- The total size of all backup data.
- The line chart of storage usage per 1 week, 2 week or a month.
- The backup schedules in calendar view.

- **Storage Reports**

You can check the storage statistics reports from the **Monitor Center** > **Reports** page, under the **Storage Reports** tab.



In the Storage Overview section, storages on all backup nodes will be displayed here.



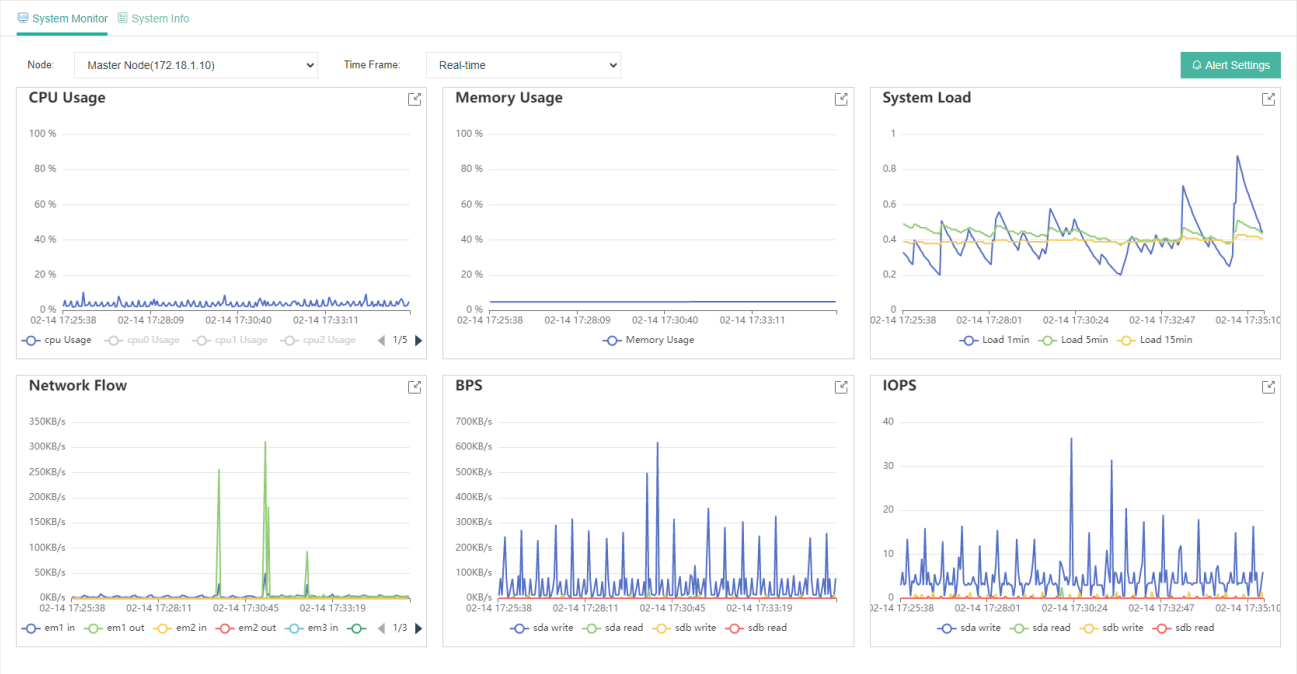
In the **Storage Statistics** section, you can have the reports of total storage usage and daily average usage. And a line chart of storage usages per 1 week, 2 weeks, 1 month, 2 months or 3 months.

System

On the **Monitor Center** > **System** page, users can monitor system status and check detailed system info.

System Monitor

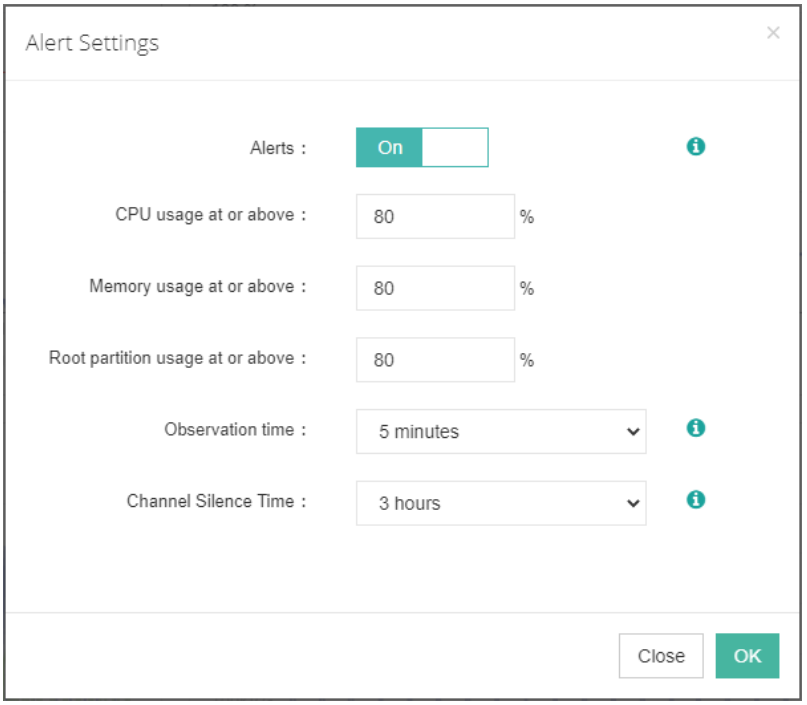
System Monitor screen displays the detailed information of system resources overhead. Including CPU usage, memory usage, system load, network flow, disk BPS and IOPS.



In the **Node** dropdown list, you can select a backup node to monitor its system resources.

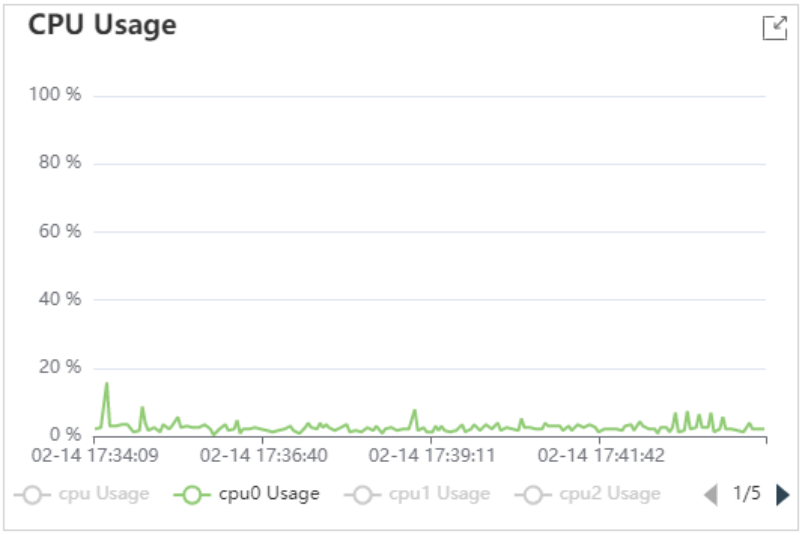
In the **Time Frame** dropdown list, you can select a time range or customize a time range to monitor the system resource information, otherwise use the default option **Real-time** which will monitor the system resource information of the last 10 minutes.

By clicking on the **Alert Settings** button, you are allowed to configure Vinchin Backup & Recovery to alert on the system resource usage.

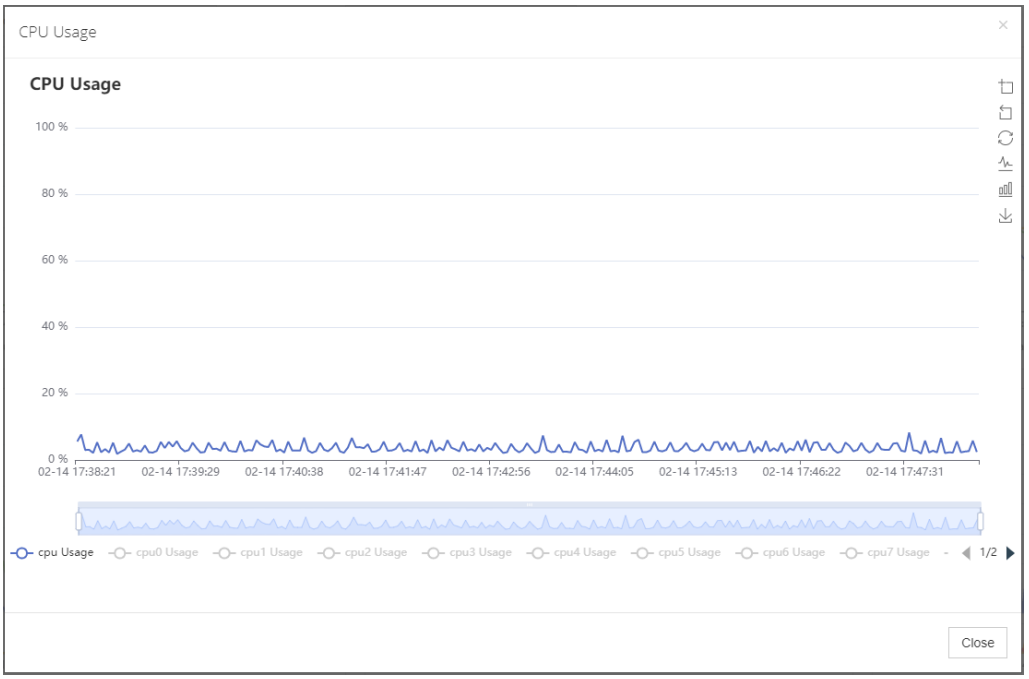


By turning the **Alerts** option on, you can configure the thresholds for CPU, memory and root partition usage. Once enabled, when the resource usage exceeded the given threshold, system alerts will be generated.

For each module, e.g., CPU usage, you can choose to display the usage of a single CPU core or multiple cores by highlighting the CPU core icon.



Or if you wish to see a clearer graph, please click on the icon on the top right of each module.



You can even try to zoom in a specific area by clicking on the icon then select that area in the line graph, to zoom out, you can click on the icon.

The icon can reset all operations you have done on this screen of view.

The icon and icon can switch the graph view between line view and histogram view.

And by clicking on the icon, you can capture and download the current graph as a .png image to your desktop.

System Info

On the **System Info** screen, users can view the operating system and hardware related information of Vinchin backup server and node.

In the Basic Info section, users can view the operating system related information.

Basic Info

Hostname:	localhost.localdomain	Processor Architecture:	x86_64
Kernel Release:	3.10.0-1160.el7.x86_64	Operating System:	CentOS Linux release 7.9.2009 (Core)
		iSCSI Initiator (IQN):	iqn.1994-05.com.redhat:f02dc8293bf2

In the **CPU & RAM Info** section, the CPU model, CPU counts, CPU core counts and RAM size will be displayed.

CPU & RAM Info

CPU Info:	12 Intel(R) Xeon(R) Bronze 3104 CPU @ 1.70GHz
Total CPU Cores:	2
Cores per CPU:	6
Total Logic Cores:	12
Total RAM:	62.24GB

In the **Disk & Root Partition** section, all block devices connected to the Vinchin backup server/node will be displayed

here.

Disk & Root Partition

Type	Vendor	Model	Version	Device Name	Capacity
disk	DELL	PERC H330 Mini	4.27	sda	223GB
disk	DELL	PERC H330 Mini	4.27	sdb	3.7TB
disk	HP	MSA2312fc	M110	sdc	14.6TB
disk	NETAPP	LUN C-Mode	9910	sdd	800GB
disk	NETAPP	LUN C-Mode	9910	sde	800GB

Root Partition Size:	50GB
Root Partition Used:	12GB
Percentage:	23%

And also, the root partition size and root partition usage info will be displayed.

In the **NIC & HBA Info** section, all the hardware related information of NICs and HBA interface cards will be displayed.

NIC & HBA Info

NIC Info	Device Name	MAC Address	Speed	Status
Broadcom Inc. and subsidiaries NetXtreme BCM5720 2-port Gigabit Ethernet PCIe	em1	18:66:da:f2:a8:dc	1000Mbps	up
Broadcom Inc. and subsidiaries NetXtreme BCM5720 2-port Gigabit Ethernet PCIe	em2	18:66:da:f2:a8:dd	-1Mbps	down
Broadcom Inc. and subsidiaries NetXtreme BCM5720 2-port Gigabit Ethernet PCIe	em3	18:66:da:f2:a8:de	-1Mbps	down
Broadcom Inc. and subsidiaries NetXtreme BCM5720 2-port Gigabit Ethernet PCIe	em4	18:66:da:f2:a8:df	-1Mbps	down
Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)	p2p1	90:e2:ba:b3:7d:62	-1Mbps	down
Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)	p2p2	90:e2:ba:b3:7d:63	-1Mbps	down

HBA Info	Name	Model	WWN	Speed	Status
QLogic Corp. ISP2532-based 8Gb Fibre Channel to PCI Express HBA (rev 02)	host15	QLE2562	0x21000024ff41f9aa	8 Gbit	Online
QLogic Corp. ISP2532-based 8Gb Fibre Channel to PCI Express HBA (rev 02)	host16	QLE2562	0x21000024ff41f9ab	unknown	Linkdown

As for the interface speed, only the interfaces which has connection will display the actual speed.

vinchin

Contact Information

Head Office

F5, Block 8, National Information Security
Industry Park, No.333 YunHua Road,
High-Tech Zone, Chengdu, China.
P.C.610041

Sales

Tel: +86-135-5029-3426
Email: sales@vinchin.com

Support

Tel: +86-159-2884-8843
Email: technical.support@vinchin.com

Website

www.vinchin.com