vinchin

VINCHIN BACKUP & RECOVERY v6.0

User Guide

2020/9

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 4

Product Overview 4

Key Features 5

Supported Environments 6

Virtual Platform (VM Backup) 6

Operating System (File Backup) 6

Getting Started 7

Web Console 7

System License 8

Install Backup Plugin 9

Hyper-V Backup Plug-in Installation 9

XenServer Backup Plug-in Installation 13

XCP-ng Backup Plug-in Installation 14

SANGFOR HCI Backup Plug-in Installation 15

OpenStack Backup Plug-in Installation 16

Red Hat RHV/oVirt Backup Plug-in Installation 17

Oracle Linux Virtualization Manager (OLVM) Backup Plug-in Installation 19

System Login 20

Register Virtual Infrastructure 21

Add Storages 27

Storage Types 27

Storage Objectives 32

Usage Alert 33

Data Importing and Storage Formatting 33

Informational 35

Dashboard 35

Monitor Center 38

Jobs 38

Alerts 40

Logs 41

Reports 43

Backup 45

Backup 45

Virtual Machines 45

Create Backup Job 46

Backup Job Operations 53
Restore 54
Create Restore Job 54
Restore Job Operations 57
Instant Restore 59
Create Instant Restore Job 59
Instant Restore Job Operations 60
VM Migration 61
Granular Restore 63
Create Granular Restore Job 63
Granular Restore Job Operations 63
Backup Data 65
File Backup 66
Install File Backup Agent 66
Windows 66
Linux 68
Register File Backup Agent 70
File Backup 71
Create File Backup Job 71
File Backup Job Operations 73
File Restore 73
File Backup Data 75
Backup Copy 76
Backup Copy 76
Create Backup Copy Job 76
Copy Job Operations 79
Copy Restore 80
Copy Data 82
Backup Archive 83
Archive 83
Create Archive Job 83
Archive Job Operations 86
Archive Restore 87
Archive Data 89
Resources 90
Virtual Infrastructure 90
Add Virtual Infrastructure 90

Virtual Infrastructure Management 90
Proxy 92
Backup Node 93
Storage 94
Add Storage 94
Manage Storages 94
LAN-Free 95
Strategy 98
System 99
System Settings 99
Network Settings 99
Time Settings 99
Notifications 100
DNS Settings 102
Restart & Poweroff 103
Upgrade 103
Data Visualization 104
System Tools 105
User Management 107
Add User 107
Other User Management Options 108
User Settings 109
User Information 109
Change Password 109
Lock Screen 110
About 110
Logout 110

Introduction

Product Overview

Vinchin Backup & Recovery is an easy-to-use, secured and reliable virtual machine data protection software designed to support multiple hypervisors including VMware vSphere, Microsoft Hyper-v, Citrix XenServer, RedHat Virtualization and open-source KVM under different virtual environments. It is an image-based agentless backup product which can be seamlessly integrated with your existing virtualization environments.

Vinchin Backup & Recovery supports Web UI management which allows users to manage & monitor any of their backup/restore tasks on either PC, mobile or tablet device. Flexible backup schedules set by daily, weekly, monthly let the backup jobs run as scheduled without system manager. All you need to do is to pre-set the job schedule when first running the software. Meanwhile, the Retention Policy helps users “save the valid” and “delete the expired” backed up data, so as to ensure the continuous operation of the backup tasks and same time save data repository space. When a disaster occurs cause the damage of the virtual machines, you only need to choose the latest restore point and specify a target host to restore to, the virtual machines will be recovered to the pre-disaster status. To help the administrators monitor and review their backup & restore jobs, Vinchin Backup & Recovery supports current jobs view, history jobs review, and system logs review & management etc.

There are 3 infrastructure components (Vinchin Backup & Recovery products) that can be used to construct your data center backup infrastructure.

- Vinchin Backup & Recovery Server
- Vinchin Backup & Recovery Node
- Vinchin Backup & Recovery Proxy

Among these 3 infrastructure components, Vinchin Backup & Recovery Server (hereinafter called Vinchin Backup Server) is the primary infrastructure component which needs to be installed to protect your virtual and hybrid environments. Vinchin Backup & Recovery Node (hereinafter called Vinchin Backup Node), Vinchin Backup & Recovery Proxy (hereinafter called Vinchin Backup Proxy) are optional components.

Vinchin Backup Node is needed only for backup and recovery of large scale virtual infrastructures. It is used to decentralize the work load of the Backup Server.

Vinchin Backup Proxy is supported by Vinchin Backup & Recovery v6.0, and it is dedicated for VMware vSphere virtual infrastructure without a Storage Area Network (SAN). It needs to be installed on the vSphere ESX/ESXi server as a virtual machine, to improve the backup and restore efficiency.

Key Features

- **High Compatibility**: Supports VMware, Hyper-v, XenServer, XCP-ng, RHV/oVirt, OLVM, OpenStack, Sangfor HCI and Huawei FusionCompute virtual platforms.
- **Agentless Backup**: No need to install any backup agent on guest OS, Vinchin Backup & Recovery system directly protects VMs on hypervisor-level, leads non-consumption of OS resources. Thus to reduce VM deployment and maintenance workload.
- **Forever Incremental Backup**: Create a full backup at the very first time, following backups are all incremental backups. The number of restore points to be kept depends on retention policy.
- **Smart Backup Strategy**: Flexible & smart backup strategies help to do backup & restore jobs as scheduled according to your actual demands in different scenarios.
- Time granularity of full backup, incremental backup and differential backup can be set to minute-level. Which means your backup job can be automatically repeated every xxx hours/minutes/seconds.
- Multiple VMs can be backed up and restored concurrently under virtual environments.
- CBT technology tracks the changed data of a virtual machine from a CBT log file since the last backup which can minimize the backup time.
- Use bank grade AES encryption to secure the transmission of VM backups.
- **Deduplication & Compression**: Built-in data deduplication and compression at backup destination can reduce backup size and save storage space.
- **LAN-Free Data Transfer**: Using LAN-Free to backup and restore VMs under SAN environment helps reduce backup and recovery time, lower the production system load.
- **BitDetector**: Detect and skip unnecessary data including swap files and un-partitioned disk space when doing backup. So that to reduce the total backup size, speed up data transfer as well as save backup storage space.
- **Specify VM disk to backup and restore**: If a VM has multiple disks, you can select certain disk to back up and restore, no need to backup/restore them all.
- **Copy VM backups to offsite**: The local backup data can be copied to offsite storage regularly. The backup data can be saved with multiple copies to increase the security of backup data.
- **Granular file-level restore**: Restore any single file from any restore point, no need to restore the entire VM, saves IT manager time and works.
- **Instant VM Recovery**: Instant VM Recovery helps to recover TB sized VMs in 15 secs, all business recovery in 1 min, minimized the break-off time of critical businesses.
- **Quick-verify Recovery Availability**: Recovering the VM backups to Data Verification Area (which is isolated with Business Area) by Instant VM Recovery helps to quick-verify the availability of backed up data.
- **Live Migration**: After instantly recovering, the VM can be synchronously migrated to the production area via virtualization platform live-migration or Vinchin Backup & Recovery's live migration function without effecting the normal operation of your business.
- **Full VM Recovery**: When any damage or mistaken-delete happens to the backed up VM, you can fully restore it from any backup point in time rather than just "the latest backup point".
- **Backup Archive to Cloud Storage**: Archive backup data to AWS S3 or Alibaba Cloud storages.

Supported Environments

Virtual Platform (VM Backup)

- VMware vSphere: 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0
- Microsoft Hyper-V Server: 2012, 2012R2, 2016, 2019, Windows 10 (Desktop)
- Microsoft Hyper-V on Windows Server: 2012, 2012 R2, 2016, 2019
- Citrix XenServer: 5.6, 6.x, 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/oVirt: 4.0, 4.1, 4.2, 4.3, 4.4
- OpenStack: M to W with Centralized or Distributed storage
- Sangfor HCI: 5.x, 6.x
- Oracle Linux Virtualization Manager (OLVM): 4.3
- Huawei FusionCompute: 5.0, 5.1, 6.0, 6.1

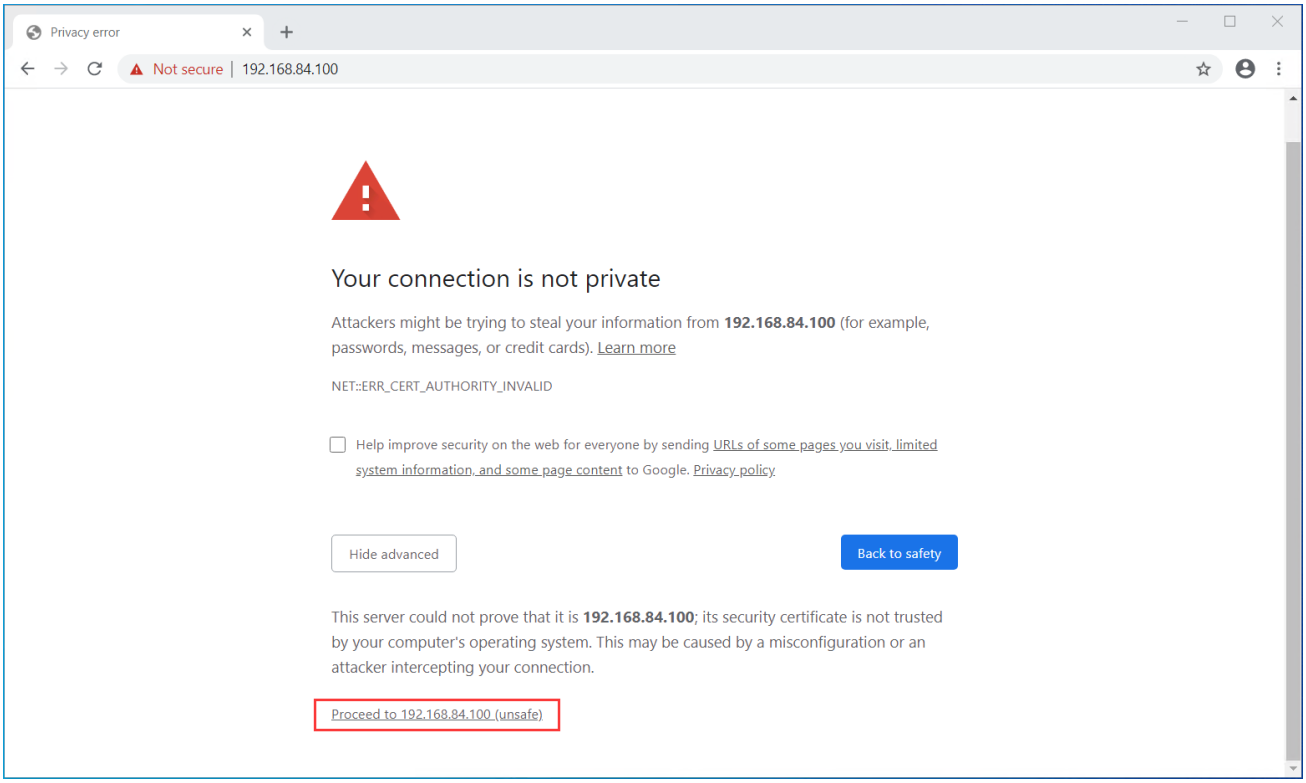
Operating System (File Backup)

- Windows Desktop: Windows XP, Windows 7, Windows 8, Windows 10
- Windows Server: Server 2003, Server 2008, Server 2012, Server 2016, Server 2019
- RHEL (Red Hat Enterprise Linux): 6, 7, 8
- CentOS Linux: 6, 7, 8
- Debian Linux: 7 to 10
- Ubuntu Linux: 12 to 20

Getting Started

Web Console

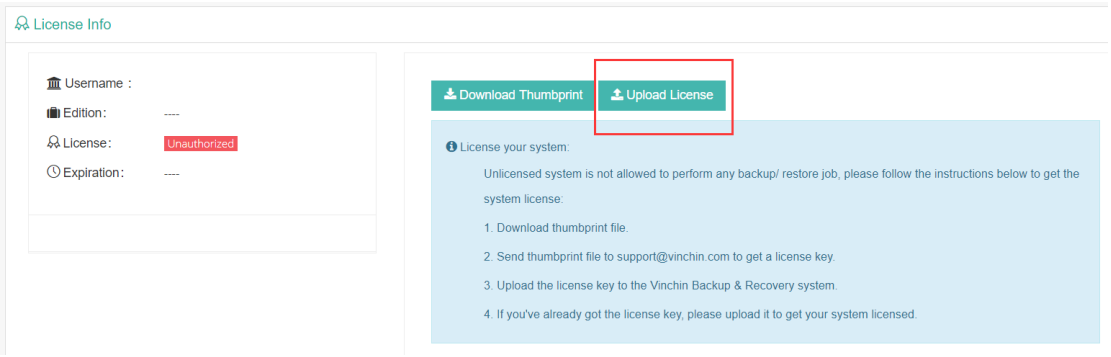
To open Vinchin Backup Server web console, it is recommended to use Google Chrome web browser. In the browser address bar, enter the IP address that you have assigned to the Backup Server during installation. You'll probably see the below "**You connection is not private**" warning message.



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. Now you should see the login screen as below.

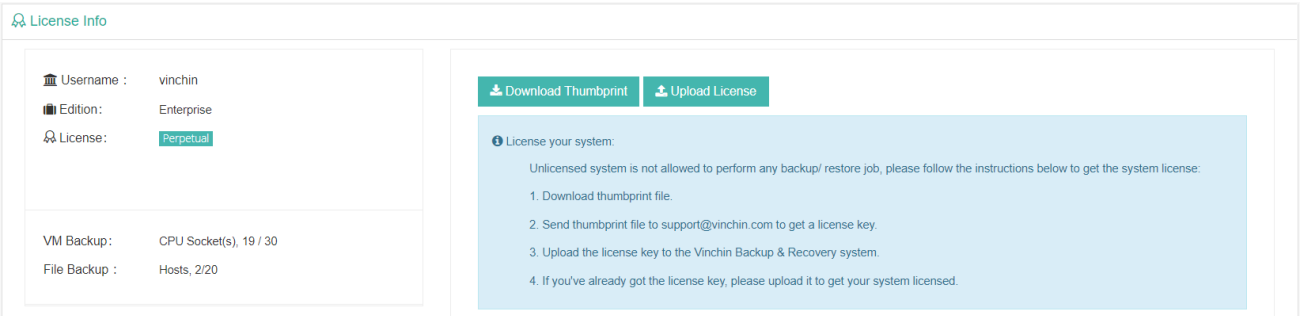
System License

When you have registered to download Vinchin Backup Server installation ISO image, a 60-day full featured trial license key will be sent, please go to **System** > **System License** page to upload the trail license.



If you wish to buy perpetual license for Vinchin Backup & Recovery, please contact our sales team and send them the thumbprint. Please find our contact information on the last page on this document.

Once you had uploaded a perpetual license, your system license page should look like below.



The license type should be **Perpetual**.

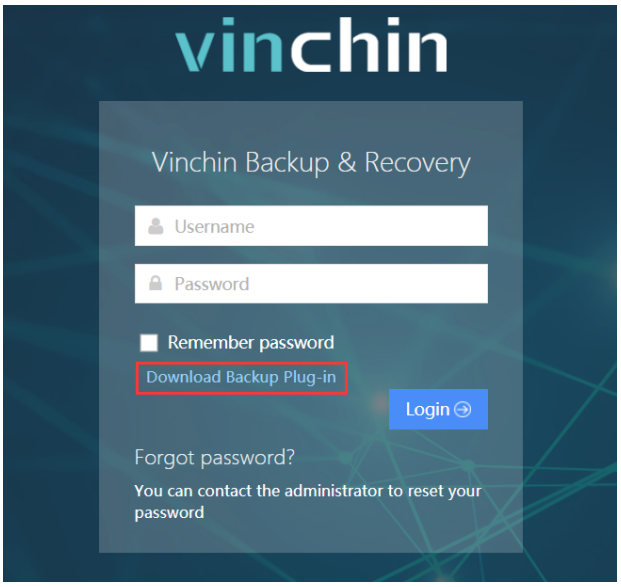
The number of licensed virtual infrastructure CPU sockets for VM backup, and the number of licensed hosts for file backup will be given in “used/licensed” format. The actual license info depends on the order you have placed.

Install Backup Plugin

With Vinchin Backup Server v6.0, backup plugin is not required for backing up and restoring virtual machines on VMware vSphere and Huawei FusionCompute virtual platforms. So, if your virtual platform is VMware vSphere or Huawei FusionCompute, then you can simply skip this chapter now.

For Microsoft Hyper-V, Citrix XenServer, XCP-ng, Sangfor HCI, OpenStack, Red Hat RHV/oVirt and Oracle Linux Virtualization Manager (OLVM) virtual platforms, backup plugin needs to be installed on corresponding virtual platforms' host(s) for VM protection by Vinchin Backup Server v6.0.

Backup plugins can be downloaded from the login page of Vinchin Backup Server web console.

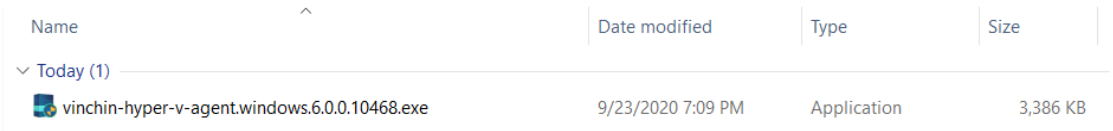


Click on **Download Backup Plug-in** to download the plugins for corresponding virtual platform. For detailed instructions of how to download and install backup plugins for your virtual platforms, please refer to the below corresponding explanations.

Hyper-V Backup Plug-in Installation

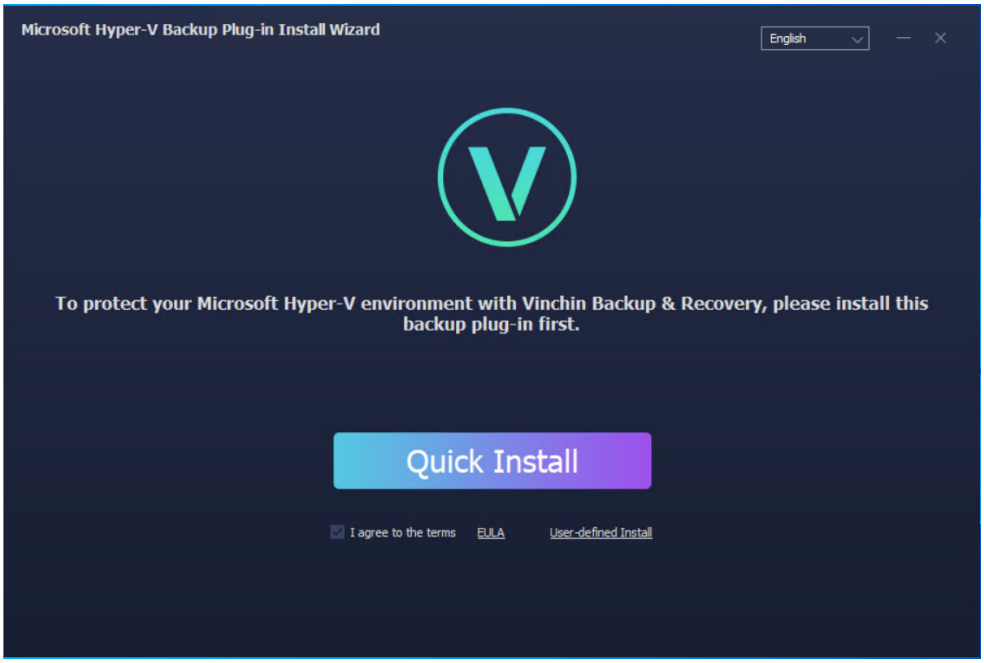
To download backup plugin for Microsoft Hyper-V, in the **Platform** dropdown list, please select **Microsoft Hyper-V**, then click on the **Download** button to download.

The downloaded backup plugin should be an executable exe file.



- Installation on Windows Server with Desktop Experience

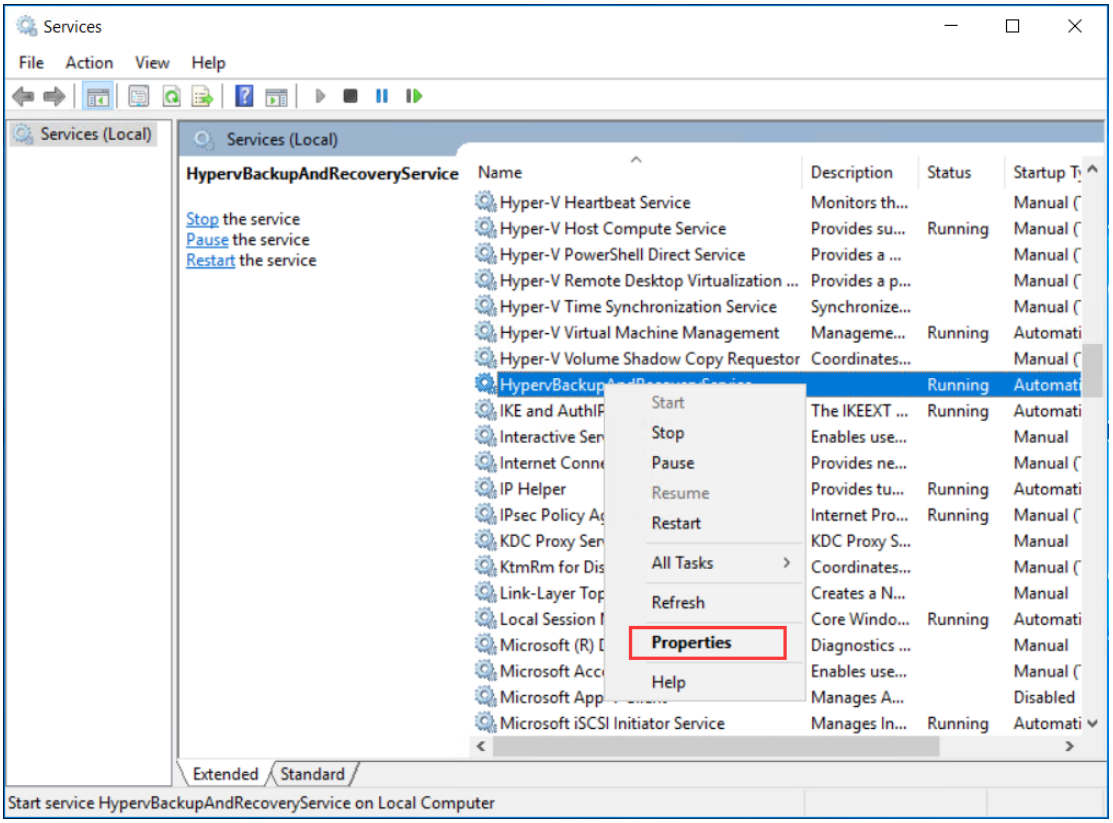
The downloading could be done directly on Hyper-V host and SCVMM server, right click to run the installer with administrator privileges (In SCVMM environment, please use SCVMM domain user to install the backup plugin on both Hyper-V host and SCVMM server).



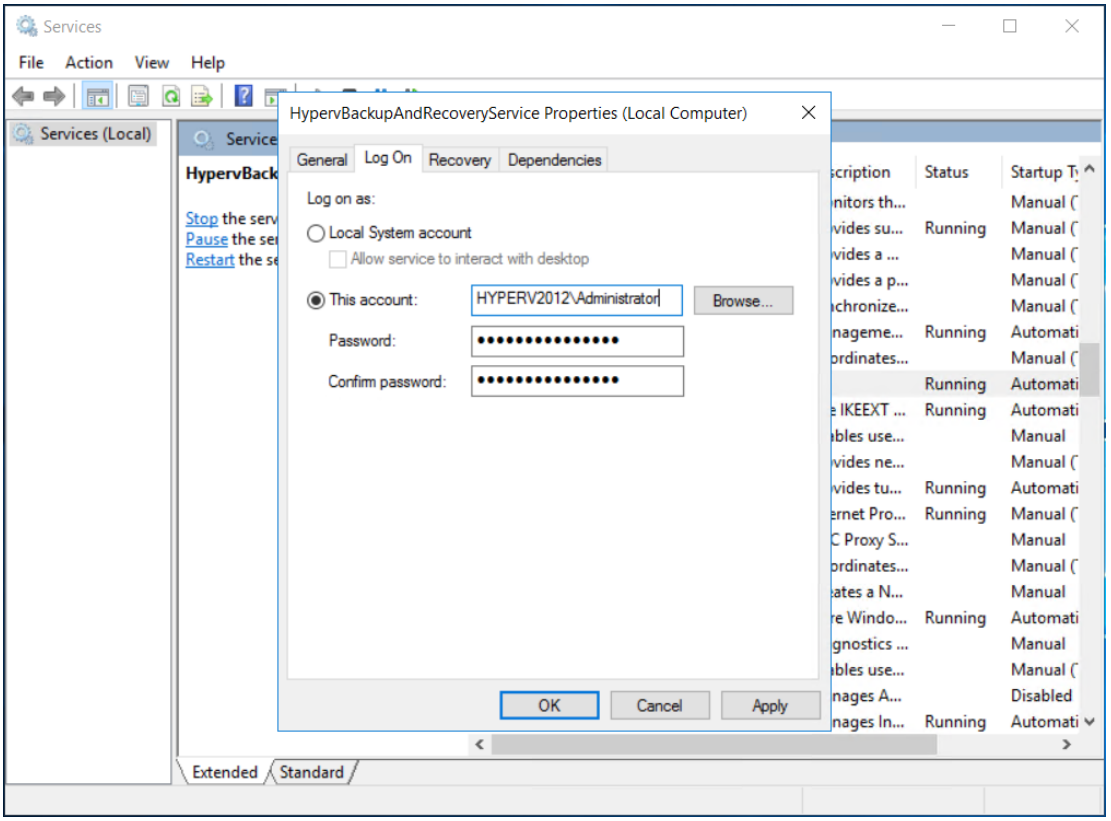
Click on **Quick Install** to install it to the Windows Server.

In case of a Failover Clustering 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.

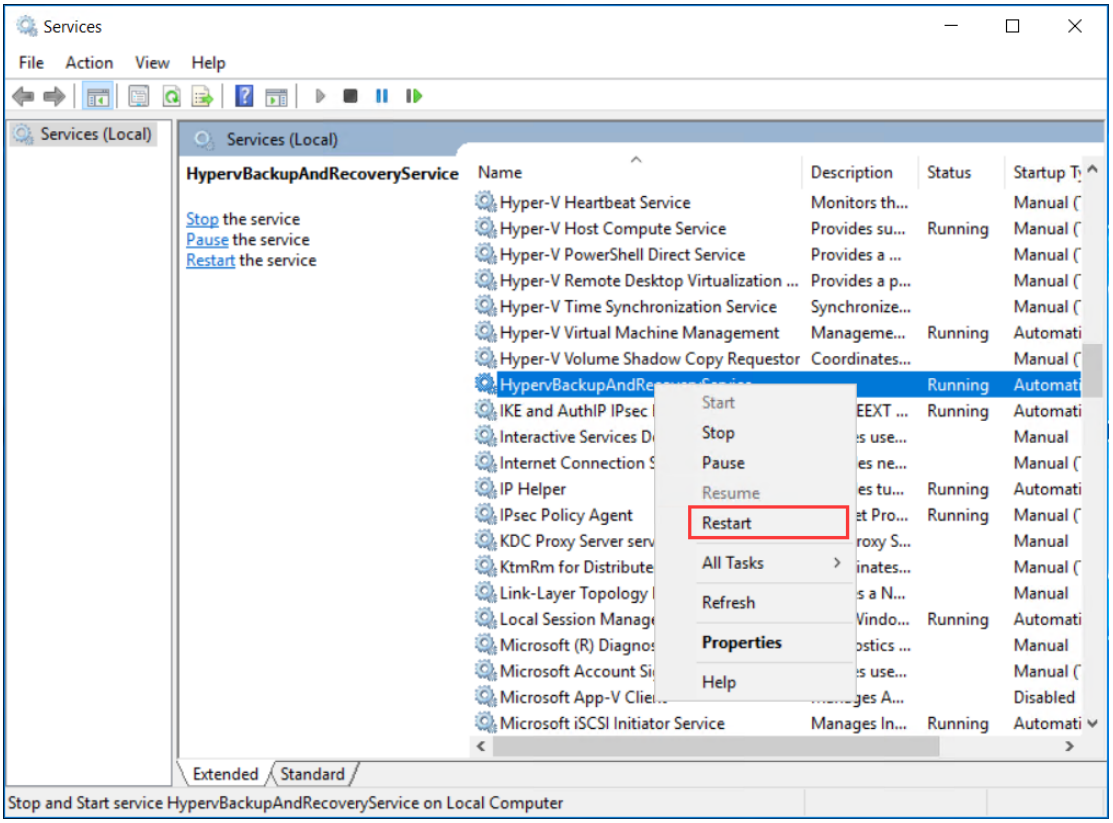
Right click the **Start** icon, select **Run**, type services.msc in the Run box and press **Enter** to open the Windows Services Manager.



Find the **HypervBackupAndRecoveryService** in the Services Manager, right click on this service and select **Properties**. In the property settings dialog, select **Log On**, and set a domain user with local administrator privileges as below.



When done apply the changes and then restart the service.



- Silent Mode Installation

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” should be the exact shared folder name on the Windows PC.

“filen_name1” should be the exact backup plugin installer file name, in this case it should be“vinchin-hyper-v-agent.windows.6.0.0.10468.exe”.

“path” should be the full path on Hyper-V host or Windows Server Core where you want to save the installer, e.g. “C:\Users\Administrator\Downloads”.

“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 command below.

```
vinchin-hyper-v-agent.windows.6.0.0.10468.exe /verysilent
```

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

```
netstat -a
```

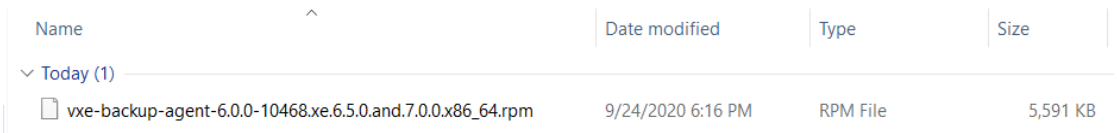
If you got active TCP connection on port 20090 and 20100 as shown below, then the backup plugin is up running normally.

```
  TCP    0.0.0.0:20090          WIN-L2MSB093K5D:0      LISTENING
  TCP    0.0.0.0:20100          WIN-L2MSB093K5D:0      LISTENING
```

XenServer Backup Plug-in Installation

To download backup plugin for XenServer, in the **Platform** dropdown list, please select **Citrix XenServer**, then in the **Version** dropdown list, please select the exact virtual platform version, and then click on the **Download** button to download the backup plugin.

The downloaded file (version 6.5/7.x/8.x for example) should be an RPM package.



Please download the corresponding version of backup plugin and upload to the XenServer pool Master and each Slave of the pool.

To upload the backup plugin package to the XenServer Master/Slave node from Windows desktop, you can use WinSCP or PSCP, or any other methods that you are familiar with.

After uploading, enter the Master/Slave node command line interface and enter the directory where you uploaded the backup plugin, and then run the below command to install.

```
rpm -i vxe-backup-agent-6.0.0-10468.xe.6.5.0.and.7.0.0.x86_64.rpm
```

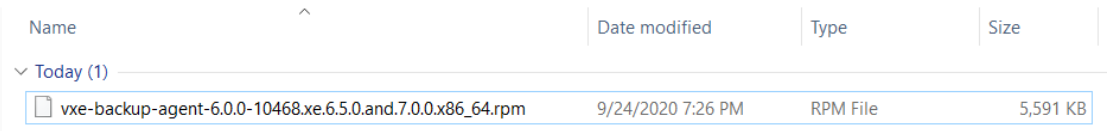
Use command below to uninstall (once uninstalled, backup/restore jobs will fail).

```
rpm –e vxe-backup-agent
```

XCP-ng Backup Plug-in Installation

To download backup plugin for XCP-ng, in the **Platform** dropdown list, please select **XCP-ng**, then in the **Version** dropdown list, please select the exact virtual platform version, and then click on the **Download** button to download the backup plugin.

The downloaded file should be a RPM package.



Please download the corresponding version of backup plugin and upload to the XCP-ng pool Master and each Slave in the pool.

To upload the backup plugin package to the XCP-ng Master/Slave node from Windows desktop, you can use WinSCP or PSCP, or any other methods that you are familiar with.

After uploading, enter the Master/Slave node command line interface and enter the directory where you uploaded the backup plugin, and then run the below command to install.

```
rpm -i vxe-backup-agent-6.0.0-10468.xe.6.5.0.and.7.0.0.x86_64.rpm
```

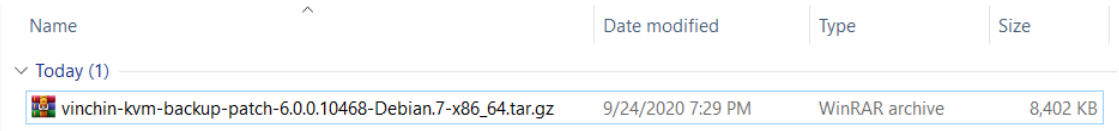
Use command below to uninstall (once uninstalled, backup/restore jobs will fail).

```
rpm –e vxe-backup-agent
```

SANGFOR HCI Backup Plug-in Installation

To download backup plugin for Sangfor HCI, in the **Platform** dropdown list, please select **SANGFOR HCI**, then click on the **Download** button to download the backup plugin.

The downloaded file should be a .tar.gz package.



Please upload the downloaded backup plugin to the Master node and each other clustered node in the pool of Sangfor HCI.

To upload the backup plugin package to the Sangfor HCI Master/Slave node from Windows desktop, you can use WinSCP or PSCP, or any other methods that you are familiar with.

After uploading, enter the Master/Slave node command line interface and enter the directory where you uploaded the backup plugin, and then use below command to decompress the .tar.gz package.

```
tar -zxvf vinchin-kvm-backup-patch-6.0.0.10468-Debian.7-x86_64.tar.gz
```

Enter the backup plugin package folder.

```
cd vinchin-kvm-backup-patch-6.0.0.10468-Debian.7-x86_64
```

To install the backup plugin, run below command.

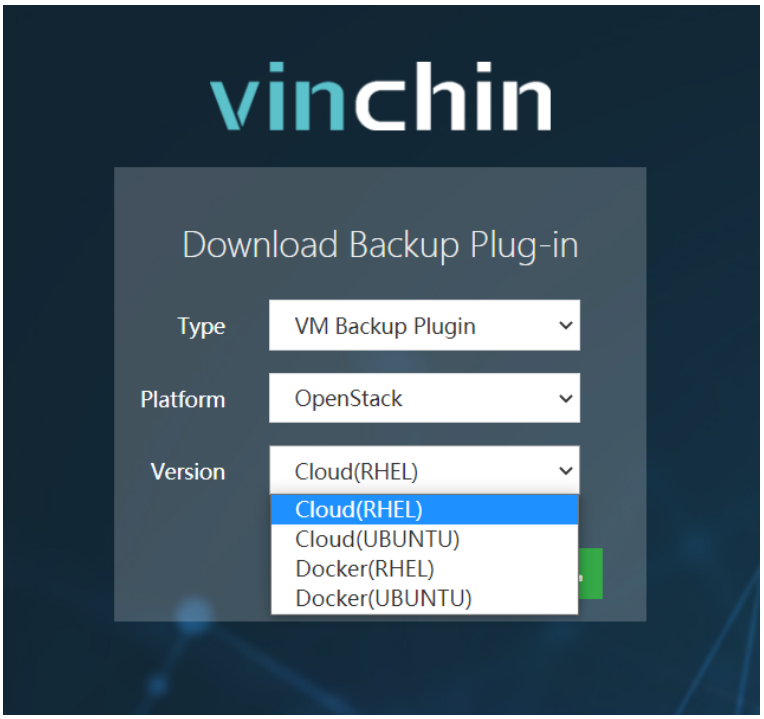
```
./kvm_backup_patch_install
```

Use below command to uninstall (once uninstalled, backup/restore jobs will fail).

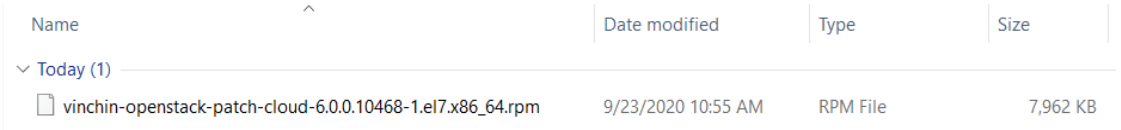
```
./kvm_backup_patch_uninstall
```

OpenStack Backup Plug-in Installation

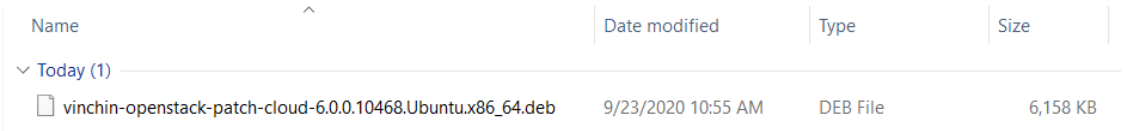
To download backup plugin for OpenStack, in the **Platform** dropdown list, please select **OpenStack**, then in the **Version** dropdown list, please select the exact virtual platform version, and then click on the **Download** button to download the backup plugin.



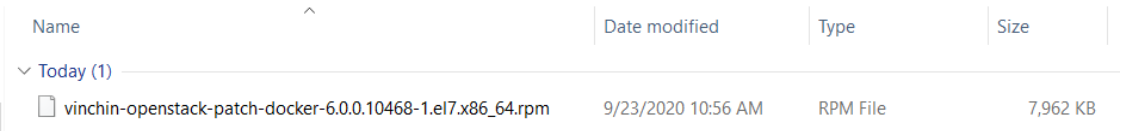
Cloud (RHEL) is for OpenStack on Red Hat Enterprise Linux. The downloaded backup plugin should be a RPM package.



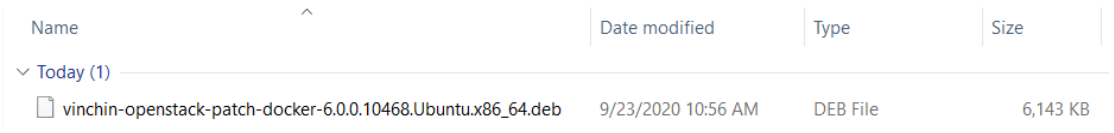
Cloud (UBUNTU) is for OpenStack on Ubuntu Linux. The downloaded backup plugin should be a Deb package.



Docker (RHEL) is for OpenStack containerized with Docker on Red Hat Enterprise Linux. The downloaded plugin should be a RPM package.



Docker (UBUNTU) is for OpenStack containerized with Docker on Ubuntu Linux. The downloaded plugin should be a Deb package.



Please download the corresponding backup plugin and upload to the controller node (if there are multiple controller nodes, please upload and install the plugin on each of the controller nodes).

To upload the backup plugin package to the controller node from Windows desktop, you can use WinSCP or PSCP, or any other methods that you are familiar with.

After uploading, enter the command line interface of the controller node and enter the directory where you uploaded the backup plugin, and then run the below command to install.

Cloud (RHEL) install.

```
rpm -i vinchin-openstack-patch-cloud-6.0.0.10468-1.el7.x86_64.rpm
```

Cloud (RHEL) uninstall (once uninstalled, backup/restore jobs will fail).

```
rpm -e vinchin-openstack-patch-cloud
```

Docker (RHEL) install.

```
rpm -i vinchin-openstack-patch-docker-6.0.0.10468-1.el7.x86_64.rpm
```

Docker (RHEL) uninstall (once uninstalled, backup/restore jobs will fail).

```
rpm -e vinchin-openstack-patch-docker
```

Cloud (UBUNTU) install.

```
sudo dpkg -i vinchin-openstack-patch-cloud-6.0.0.10468.Ubuntu.x86
```

Cloud (UBUNTU) uninstall (once uninstalled, backup/restore jobs will fail).

```
sudo dpkg –r vinchin-openstack-patch-cloud
```

Docker (UBUNTU) install.

```
sudo dpkg -i vinchin-openstack-patch-docker-6.0.0.10468.Ubuntu.x86_64.deb
```

Docker (UBUNTU) uninstall (once uninstalled, backup/restore jobs will fail).

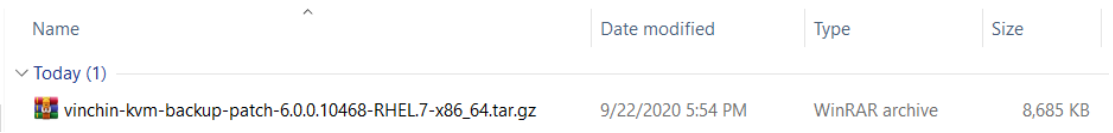
```
sudo dpkg -r vinchin-openstack-patch-docker
```

Red Hat RHV/oVirt Backup Plug-in Installation

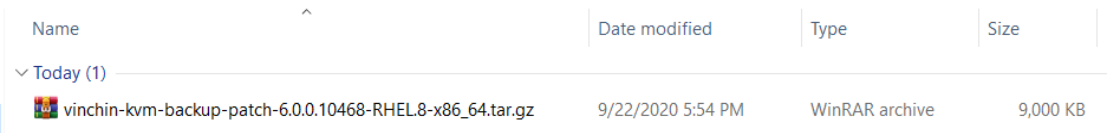
To download backup plugin for Red Hat RHV or oVirt, in the **Platform** dropdown list, please select **Redhat RHV/oVirt**, then in the **Version** dropdown list, please select the exact virtual platform version, and then click on the **Download** button to download the backup plugin.

The downloaded file should be the following format.

4.0-4.3(CentOS 7):



4.4(CentOS 8):



Please download the corresponding backup plugin and upload to each of the RHV/oVirt hosts (the backup plugin needs to be installed on all RHV or oVirt hosts).

To upload the backup plugin package to the RHV/oVirt node from Windows desktop, you can use WinSCP or PSCP, or any other methods that you are familiar with.

After uploading, enter RHV/oVirt node command line interface and enter the directory where you uploaded the backup plugin, and then run the below command to decompress the backup plugin package.

```
tar -zxvf vinchin-kvm-backup-patch-6.0.0.10468-RHEL.7-x86_64.tar.gz
```

Enter the backup plugin package folder.

```
cd vinchin-kvm-backup-patch-6.0.0.10468-RHEL.7-x86_64
```

Run the below command to install backup plugin.

```
./kvm_backup_patch_install
```

Use below command to uninstall (once uninstalled, backup/restore jobs will fail).

```
./kvm_backup_patch_uninstall
```

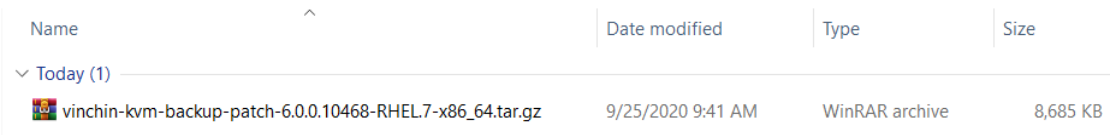
Warning

Backup plugin should not be installed on the RHV/oVirt Engine.

Oracle Linux Virtualization Manager (OLVM) Backup Plug-in Installation

To download backup plugin for Oracle Linux Virtualization Manager, in the **Platform** dropdown list, please select **Oracle Linux Virtualization Manager (OLVM)**, then click on the **Download** button to download the backup plugin.

The downloaded backup plugin should be a .tar.gz package.



Please upload the downloaded backup plugin to the OLVM node (if there are multiple node hosts, please upload and install the plugin on each of the nodes).

To upload the backup plugin package to the OLVM node host(s) from Windows desktop, you can use WinSCP or PSCP, or any other methods that you are familiar with.

After uploading, enter the OLVM node command line interface and enter the directory where you uploaded the backup plugin, and then use below command to decompress the .tar.gz package.

```
tar -zxvf vinchin-kvm-backup-patch-6.0.0.10468-RHEL.7-x86_64.tar.gz
```

Enter the backup plugin package folder.

```
cd vinchin-kvm-backup-patch-6.0.0.10468-RHEL.7-x86_64
```

To install the backup plugin, run below command.

```
./kvm_backup_patch_install
```

Use below command to uninstall (once uninstalled, backup/restore jobs will fail).

```
./kvm_backup_patch_uninstall
```

Warning

Backup plugin should not be installed on the OLVM Engine node.

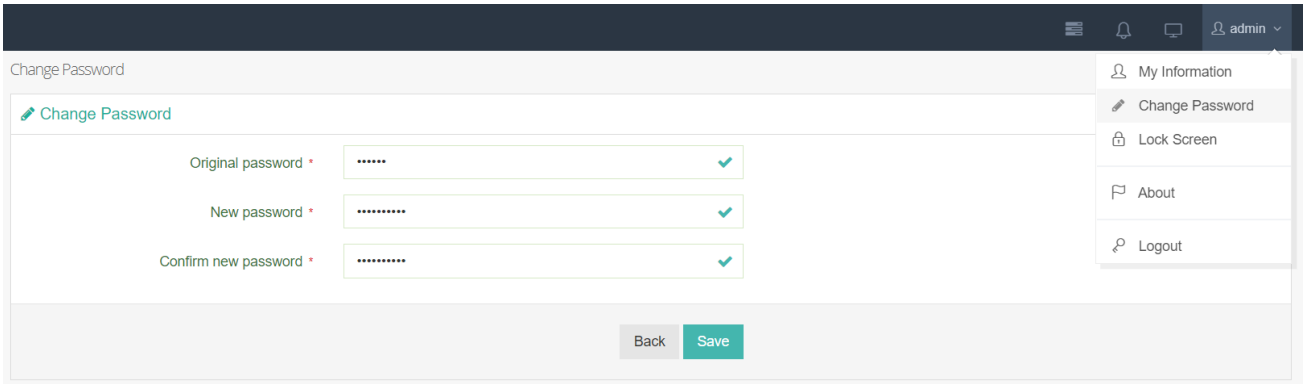
System Login

Please open your web browser (Google Chrome is recommended), in the address bar, enter the IP address of the Vinchin Backup Server which you had assigned to Vinchin Backup Server during the installation. On the login screen, please use the below default credentials to log in.

Username: **admin**

Password: **123456**

For the safety of Vinchin Backup Server, please change the default administrator password right after your first login, the password can be changed from **admin** > **Change Password** screen.



Note

1. If you forgot your password:

For operator/auditor user, please contact your administrator to reset your password.

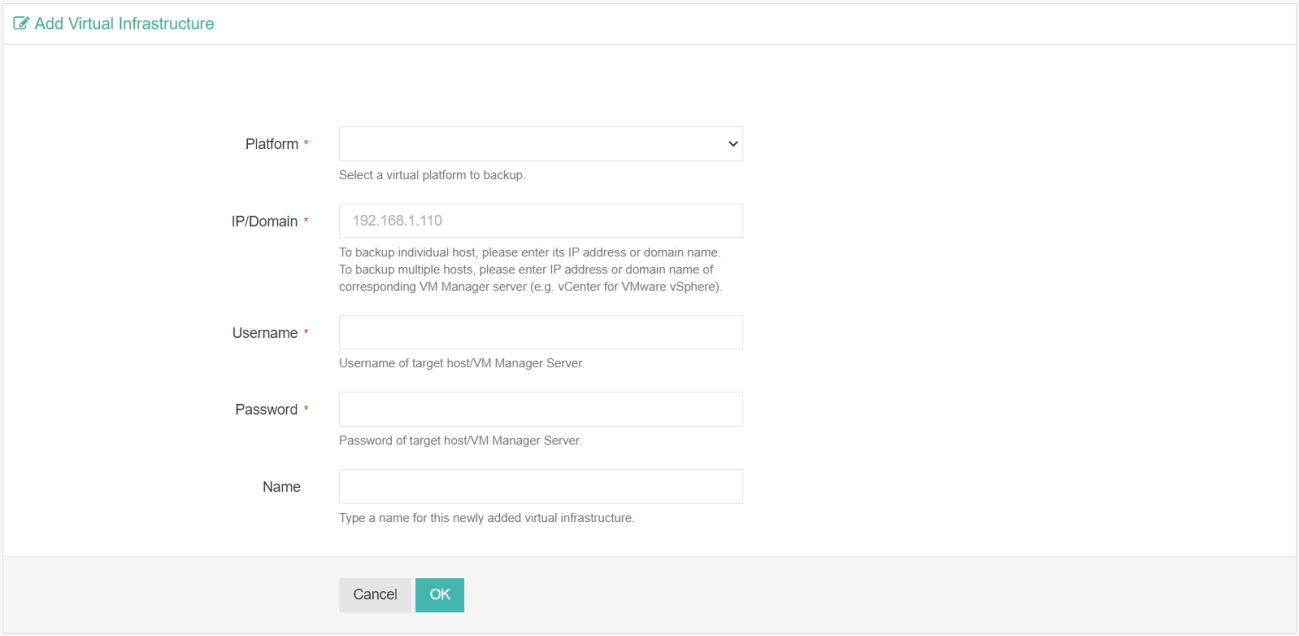
For administrator user, please contact Vinchin Support Team to reset your password.

2. Only VMware vSphere and Huawei FusionCompute do not require installation of backup plug-in. If you are using any other virtual platform, please download the corresponding backup plug-in from the login screen and install it on each virtual platform host that you need to protect.

Add Virtual Infrastructure

Before you start to backup and recover the VMs on your virtual platforms, you need to add your virtual platform(s) to Vinchin Backup Server first.

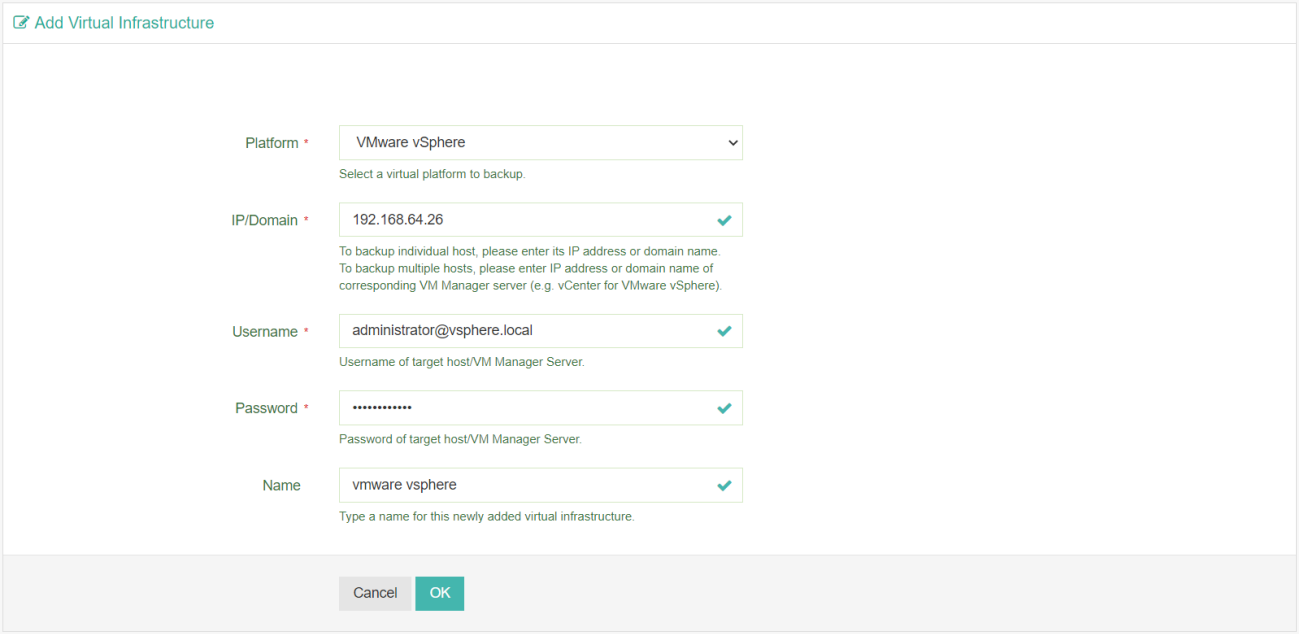
Go to **Resources** > **Virtual Infrastructure** page. And click on Add button to add a virtual platform to the Backup Server.



In the Platform dropdown list, select the virtual platform you are using. Then on the same page, the corresponding settings of registering your virtual platform to Vinchin Backup Server will be listed here.

- **Add VMware vSphere Virtual Platform**

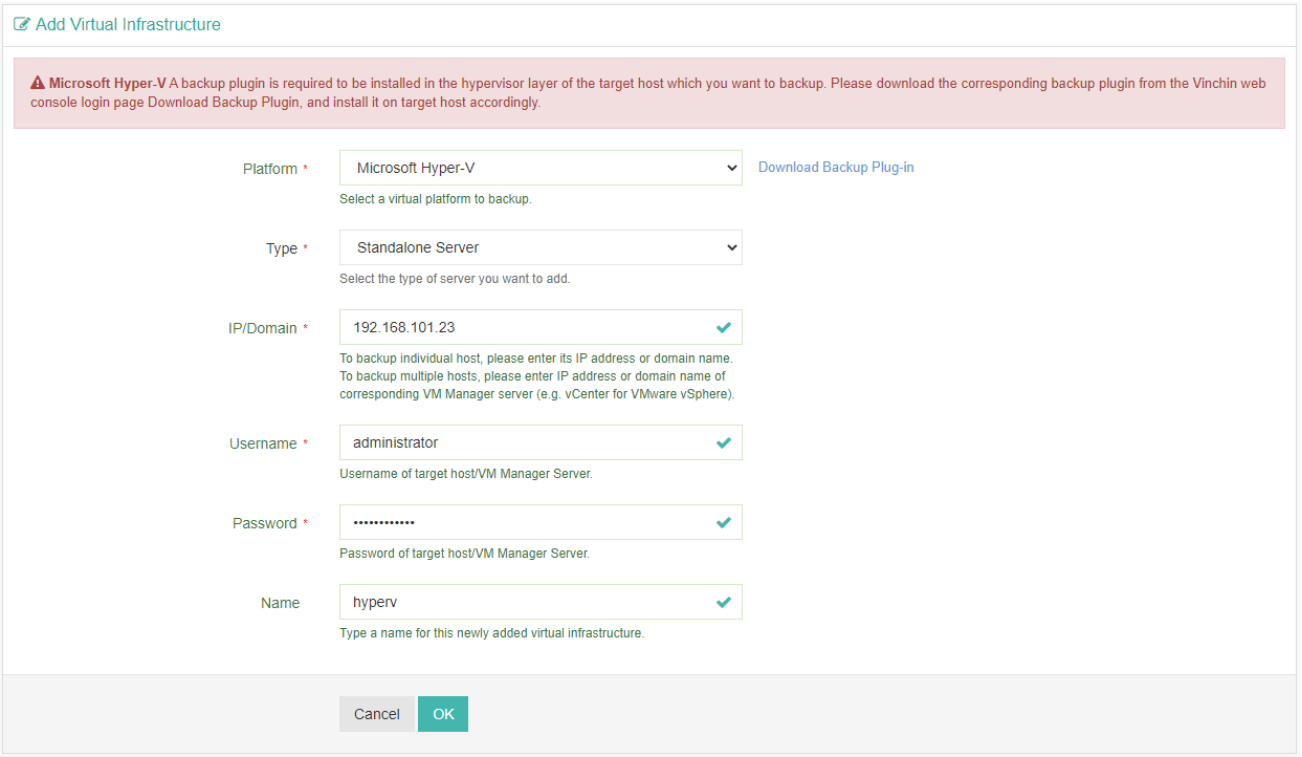
If you are using VMware vSphere, In the **Platform** dropdown list, please select **VMware vSphere**.



In the **IP/Domain** field, please type in the IP address of the vCenter server. Or if you are using standalone ESXi server, please type in the IP address of the ESXi server.
In the **Username** field, type in the user name in vsphere.local domain, e.g. administrator@vsphere.local. To add a standalone ESXi server, please type in root user name here.
In the **Password** field, type in the password for administrator@vsphere.local or the password for ESXi root user.

- **Add Microsoft Hyper-V Virtual Platform**

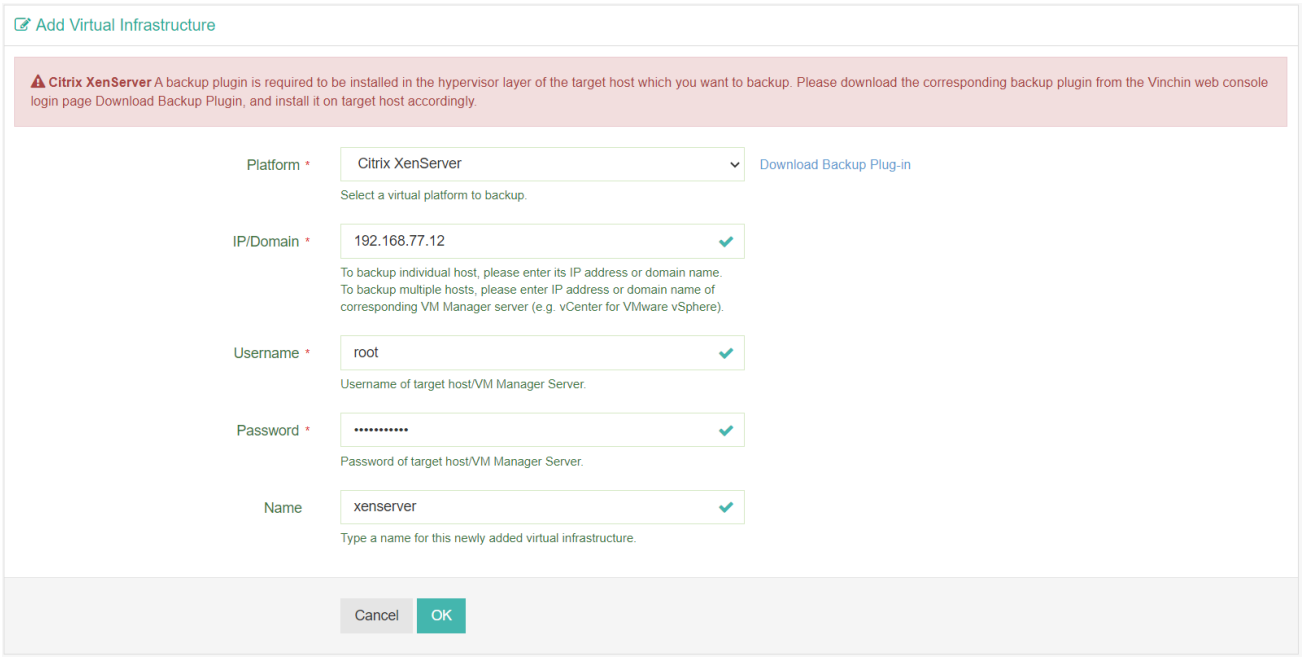
If you are using Microsoft Hyper-V, in the Platform dropdown list, please select **Microsoft Hyper-V**.



In the **Type** field, please select your Hyper-V deployment type.
In the **IP/Domain** field, enter the SCVMM server IP if your Hyper-V virtual infrastructure is managed by a SCVMM management server; enter the cluster IP if your Hyper-V virtual infrastructure 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.
In the **Username** field, enter the domain user with administrator permissions of the SCVMM server and all other hosts if your Hyper-V virtual infrastructure 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.
In the **Password** field enter the corresponding password of the username you specified above.

- **Add Citrix XenServer/XCP-ng Virtual Platform**

If you are using Citrix XenServer or XCP-ng virtual platform, in the Platform dropdown list, please select **Citrix XenServer** or **XCP-ng** correspondingly.
The principle of registering XenServer and XCP-ng to Vinchin Backup Server is the same, below is an example of registering XenServer, XCP-ng should be registered the same way.



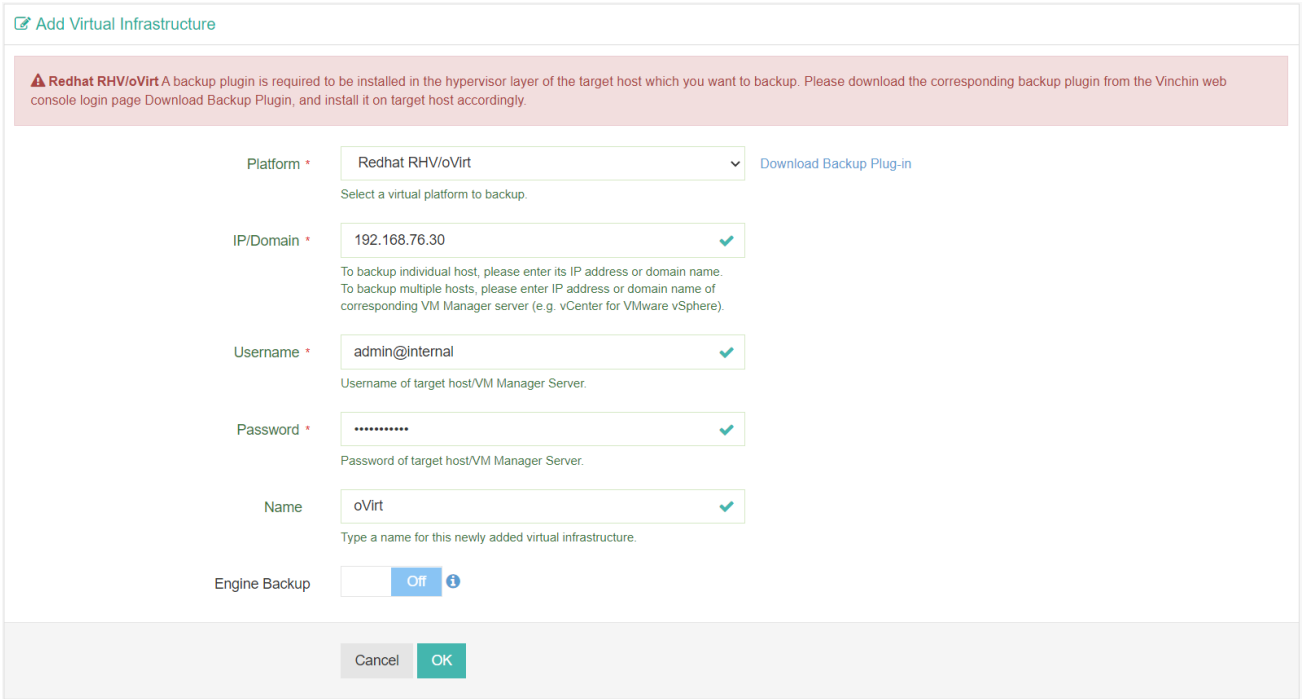
In the **IP/Domain** field, the IP address of the pool master should be used.

In the **Username** field, the root user should be used.

In the **Password** field, should use the password for root user.

- **Add RHV/oVirt/OLVM Virtual Platform**

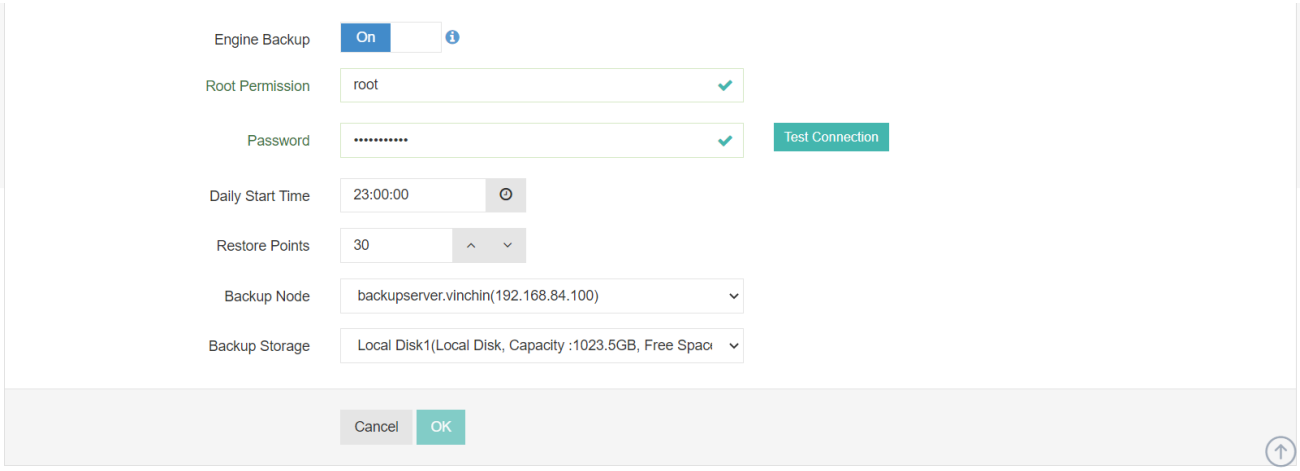
If you are using Red Hat RHV or oVirt, please select **Redhat RHV/oVirt** in the **Platform** dropdown list; if you are using OLVM, please select **Oracle Linux Virtualization Manager (OLVM)**. As the settings of adding RHV, oVirt and OLVM are the same, here we will take RHV and oVirt as an example.



In the **IP/Domain** field, the IP address of the RHV or oVirt engine should be used.

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.

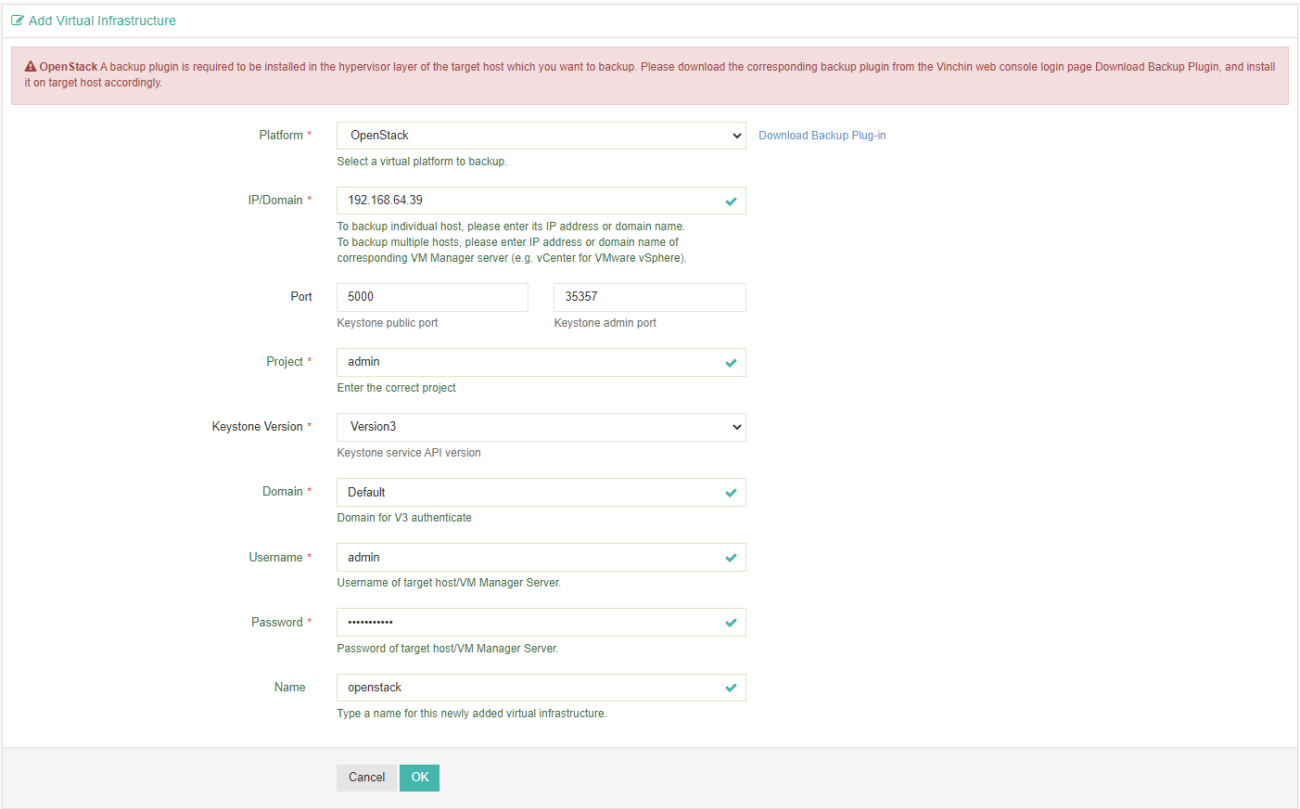
In the **Password** field, please type in the password for admin that you specified during the installation.
As for **Engine Backup**, it is used to backup the RHV or oVirt engine metadata. To enable engine backup, you need to use root permission of the RHV or oVirt engine server.



And the backup strategy and backup storage options can be configured as per your requirements.

- **Add OpenStack Virtual Platform**

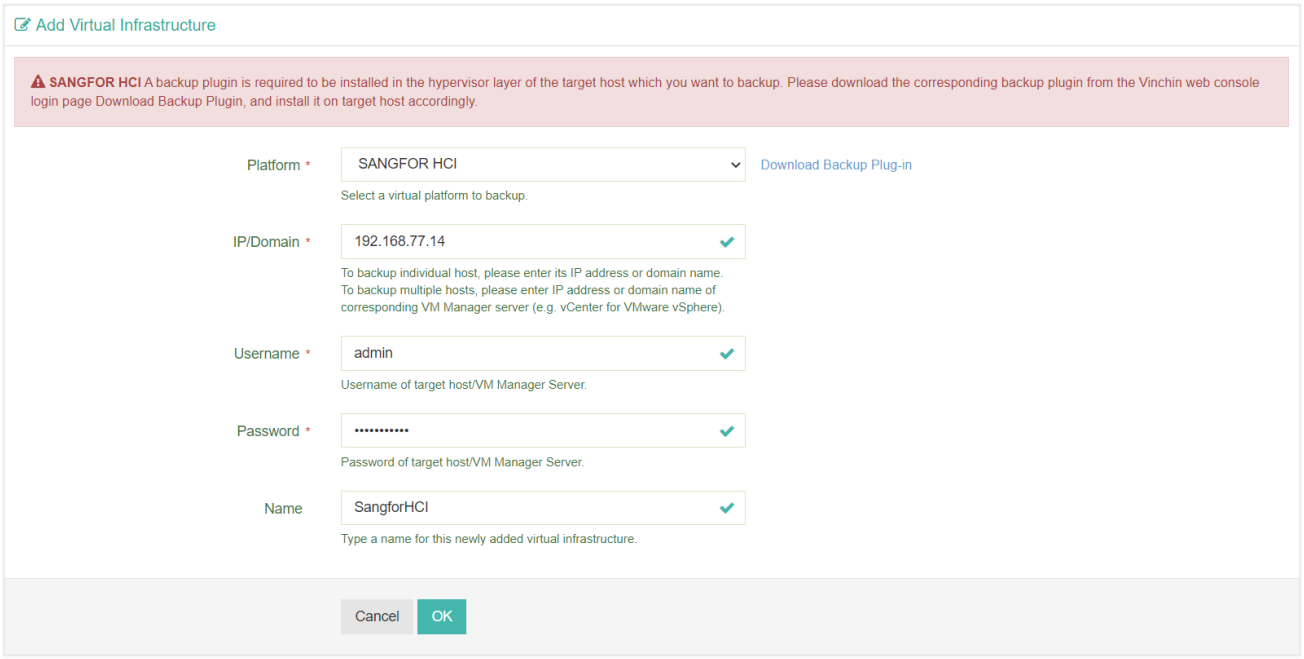
To add OpenStack virtual platform, please select **OpenStack** in the **Platform** dropdown list.



In the **IP/Domain** field, please enter the “kolla_internale_vip_address”.
Normally the **Port** number of Keystone should not be changed, please use the default port number.
In the **Project** field, enter a project name which needs to be protected.
The **Keystone Version** should be the version that matches your real deployment.
In the **Domain** field, enter the Keystone domain and corresponding user credentials.

- **Add Sangfor HCI Virtual Platform**

To add Sangfor HCI, in the **Platform** dropdown list, please select **SANGFOR HCI**, then complete the below settings.

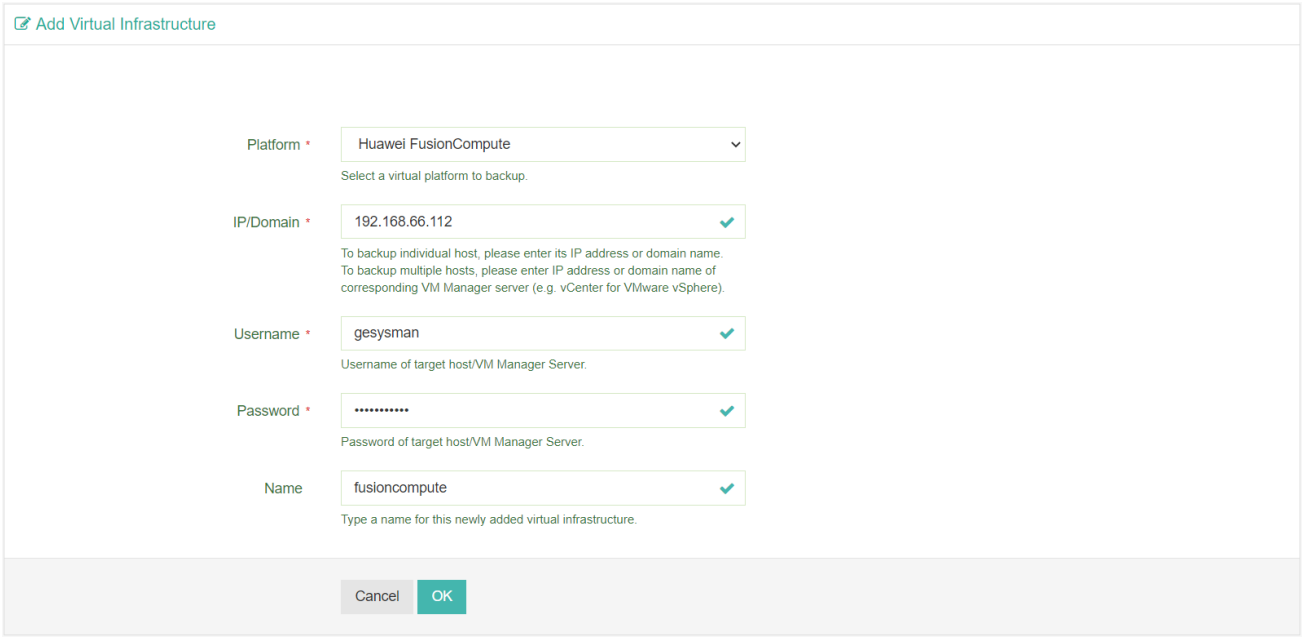


In the **IP/Domain** field, please type in the IP address of the Sangfor HCI master node, or if it's cluster deployment, the virtual IP of the cluster must be used.

In the **Username** and **Password** fields, type in the super admin user name and password.

- **Add Huawei FusionCompute Virtual Platform**

To add Huawei FusionCompute, in the **Platform** dropdown list, please select **Huawei FusionCompute**, then complete the following settings.

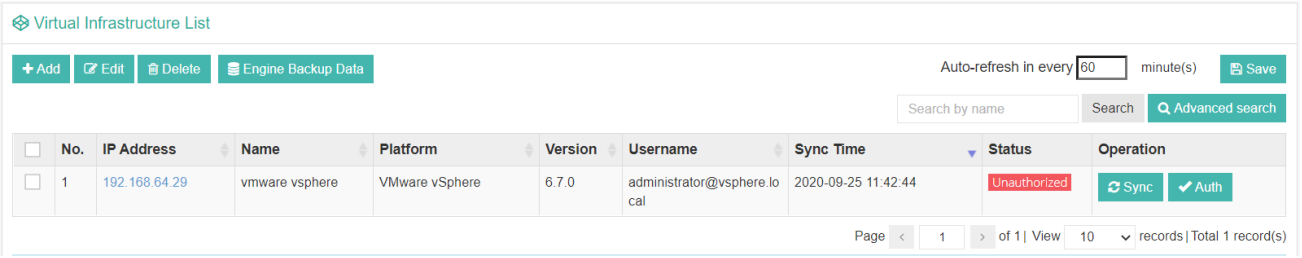


In the **IP/Domain** field, type in the IP address of the FusionCompute Virtual Resource Manager (VRM) server.

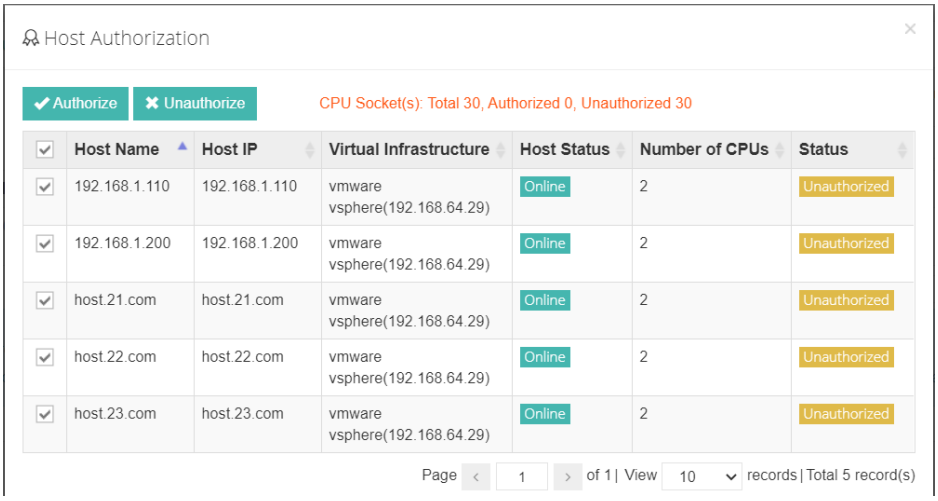
In the **Username** field, the northbound interface authentication account should be used, the default username used by FusionCompute is "gmsysman".

In the **Password** field, please type in the northbound interface authentication account password.

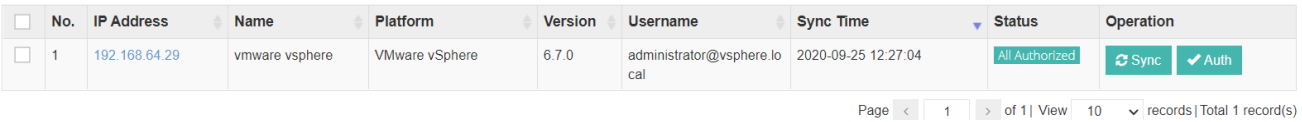
Once completed the settings of corresponding virtual platform, click on **OK** to add the infrastructure to Vinchin Backup Server.



The newly added virtual infrastructure status will be **Unauthorized**, to authorize Vinchin Backup Server backup and restore the VMs on the virtual infrastructure, please click on **Auth** button.



Select the hosts that you want to protect, then click on **Authorize** button.



After authorization, the virtual infrastructure status will be All Authorized. If you have only authorized part of the hosts, the status will be Partial Authorized.

Now you should be able to backup and recover the VMs on the authorized hosts.

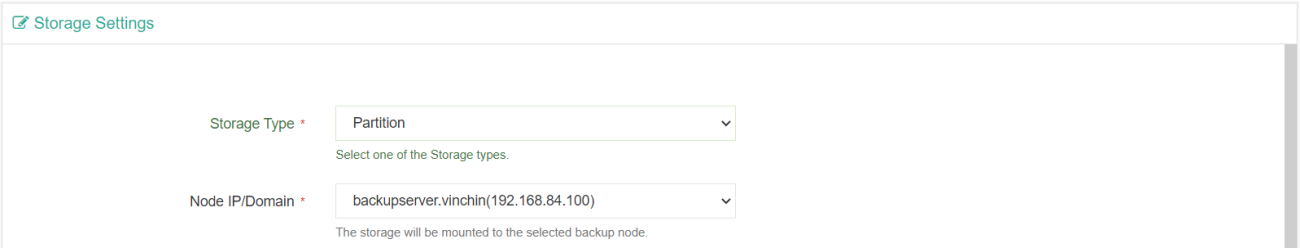
Note

You can only backup the virtual machines running on the authorized hosts.

Add Storages

A backup storages is an essential component that need to be added to Vinchin Backup Server before you can get started to backup the VMs in your virtual infrastructure.

To add storages, please go to **Resources** > **Storage** page, and click on **Add** button to add a desired storage.



In the **Storage Type** dropdown list, select the target storage type that you had prepared for backup/copy/archive backup data. The supported storage types including: Partition, Local Disk, Local Directory, LVM, Fiber Channel, iSCSI, NFS, CIFS, Off-site Storage, Cloud Storage. Among those storages, Off-site Storage is dedicated to store offsite backup copy data, while the Cloud Object Storage is dedicated to store backup archive data.

In the **Node IP/Domain** field, you can choose to add the storage from a specific node, by default, the storage will be added from the Vinchin Backup Server, if you had deployed Vinchin Backup Node and want to add the storage from the Backup Node then select that node in the dropdown list.

Warning

The following operations of adding storages to Vinchin Backup Server will involve formatting storages! Please make sure that you had made copies of the data on the storages before adding to Vinchin Backup Server!

Storage Types

- **Partition**

Local partitions on the Backup Server or Backup Node can be used as Backup storage, Backup Copy storage and also Backup Archive storage.

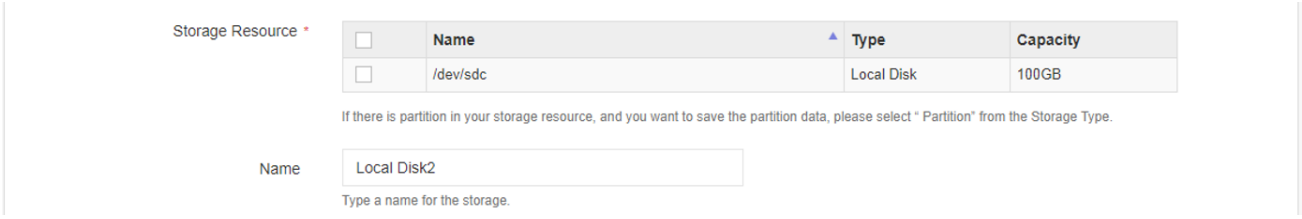
To add a partition as backup/copy/archive storage, please select on which node the partition exists.

Vinchin Backup Server will recognize the partitions which are not yet mounted to the file system, choose the target partition from the **Storage Resource** list, and then give it a name to add it to Vinchin Backup Server as backup/copy/archive storage.

- **Local Disk**

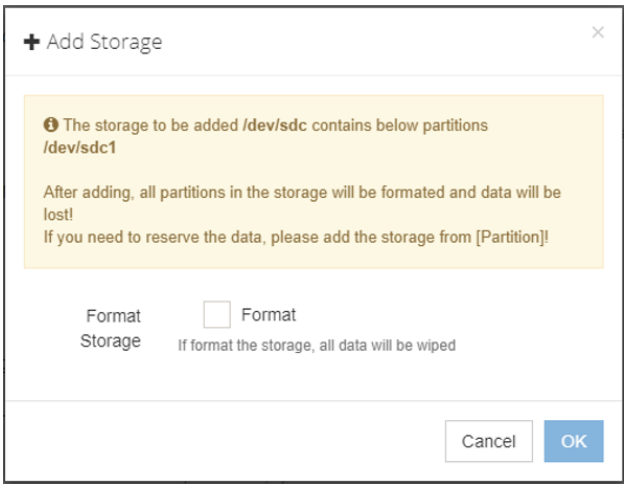
Local disks on the Backup Server or Backup Node can be used as Backup storage, Backup Copy storage and also Backup Archive storage.

To add a disk as backup/copy/archive storage, please select on which node the disk exists.



Vinchin Backup Server will recognize the disks which are not yet partitioned or which contains partitions but not yet mounted to the file system, choose the target disk from the Storage Resource list, and then give it a name to add it to Vinchin Backup Server as backup/copy/archive storage.

When you are adding a disk which contains partitions on that disk, you can choose **Format** to delete the partitions and all data, if you want to keep the partitions please add the storage use **Partition** type instead of **Disk**.



- **LVM**

To add an unmounted logical volume to Vinchin Backup Server, please select on which node the logical volume exists, and Vinchin Backup Server will try to detect the storage.

The unmounted logical volume will be detected and displayed in the **Storage Resource** list. Please select the target logical volume to add to Vinchin Backup Server.

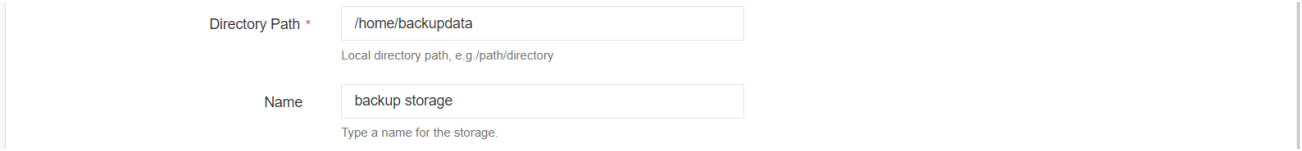
- **Local Directory**

The local directories in the Backup Server or Backup Node file system can be used as backup/copy/archive storages. If you have allocated sufficient storage space to the Backup Server or Backup Node file system, and you want to store backup/copy/archive data in the native file system, you can use local directory.

The directories need to be created in the Backup Server or Backup Node file system before adding. Please add the directories through the command line interface of the backup server or backup node. For example, to create a directory named “backupdata” for backup storage in the “/home/” directory.

```
mkdir /home/backupdata
```

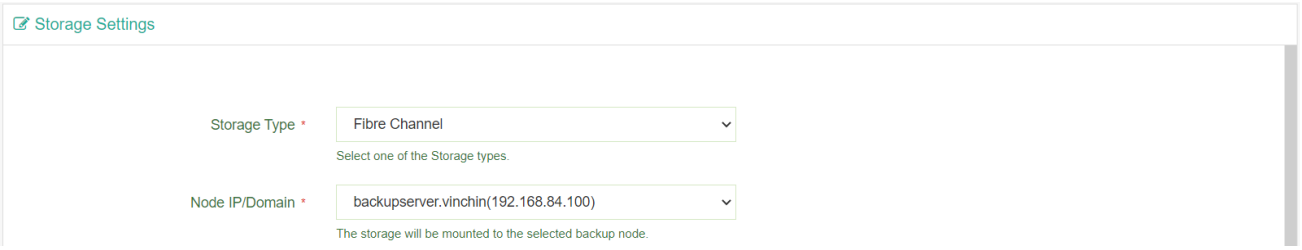
Then to add it as below.



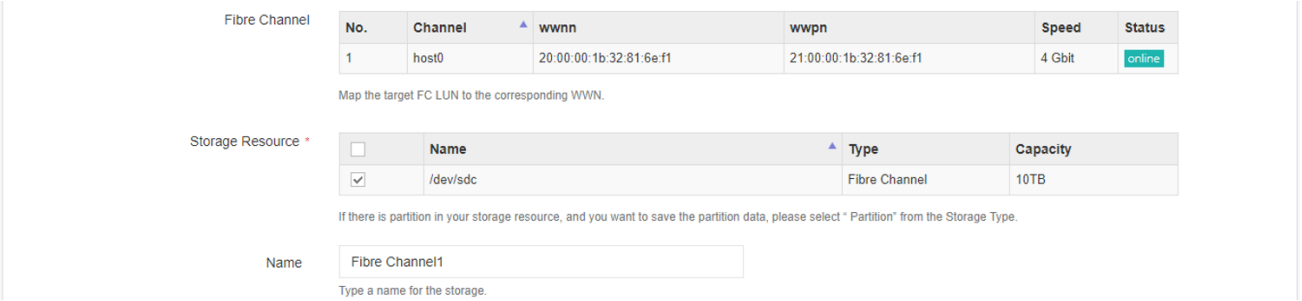
In the **Directory Path** field, please type in the full path of the directory you have created.

- **Fiber Channel**

To add Fiber Channel Storage Area Network (FC SAN) storage to Vinchin Backup Server as backup/copy/archive storages, please select Fibre Channel in the Storage Type dropdown list, and then select the node on which the HBA interface card connects to the FC switch.



Now Vinchin Backup Server will detect the fiber channel and the wwpn of the HBA interface card, use this information to map the LUN of the FC SAN storage to Vinchin Backup Server. After this, add the FC SAN storage again, and Vinchin Backup Server will detect the mapped LUN storage.

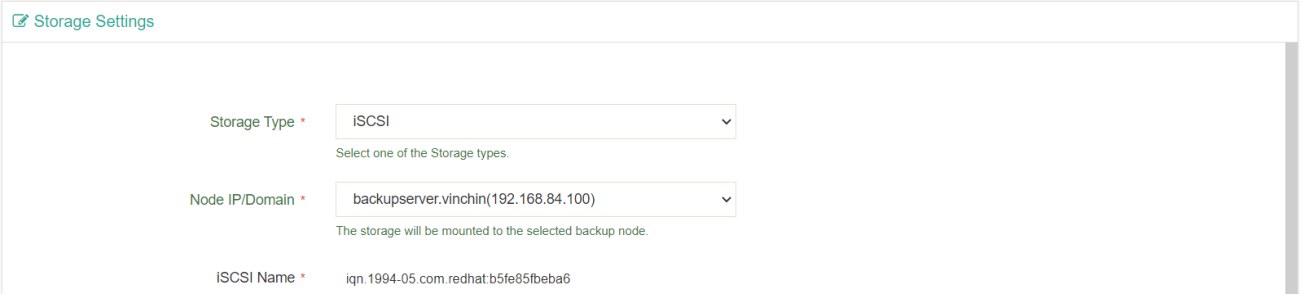


Note

To add FC SAN storage, the added LUN will be formatted, all data in the LUN storage will be erased. If there's previous backup data in the LUN and you don't want to format it, please add this storage as Partition.

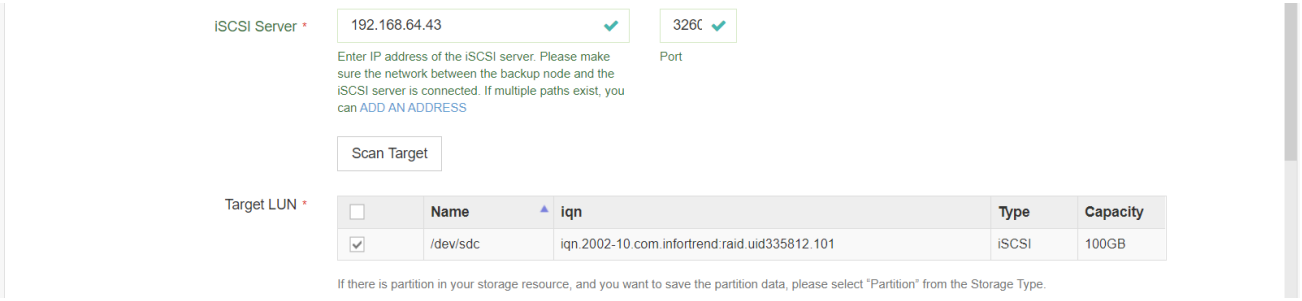
- **iSCSI**

To add iSCSI storage, please select the target node, and the iSCSI qualified name (IQN) of the selected node will be given.



Please use the IQN to map the LUN of the iSCSI storage to the backup server from the iSCSI storage server. After this,

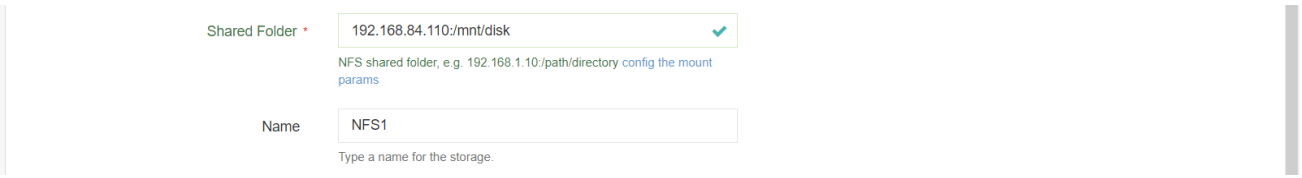
input the iSCSI storage server IP address here and click on **Scan Target** button to scan the target storage.



Select the scanned storage to add it to Vinchin Backup Server.

- **NFS**

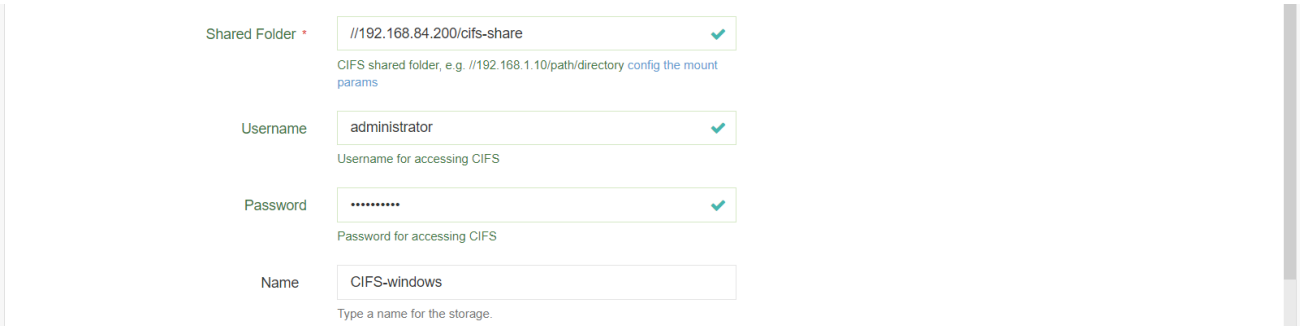
To add an NFS storage, simply type in the path of the shared folder in the **Share Folder** field.



Vinchin Backup Server will not delete the existing data on the NFS storage.

- **CIFS**

To add a CIFS storage, simply type in the path of the shared folder in the **Share Folder** field.



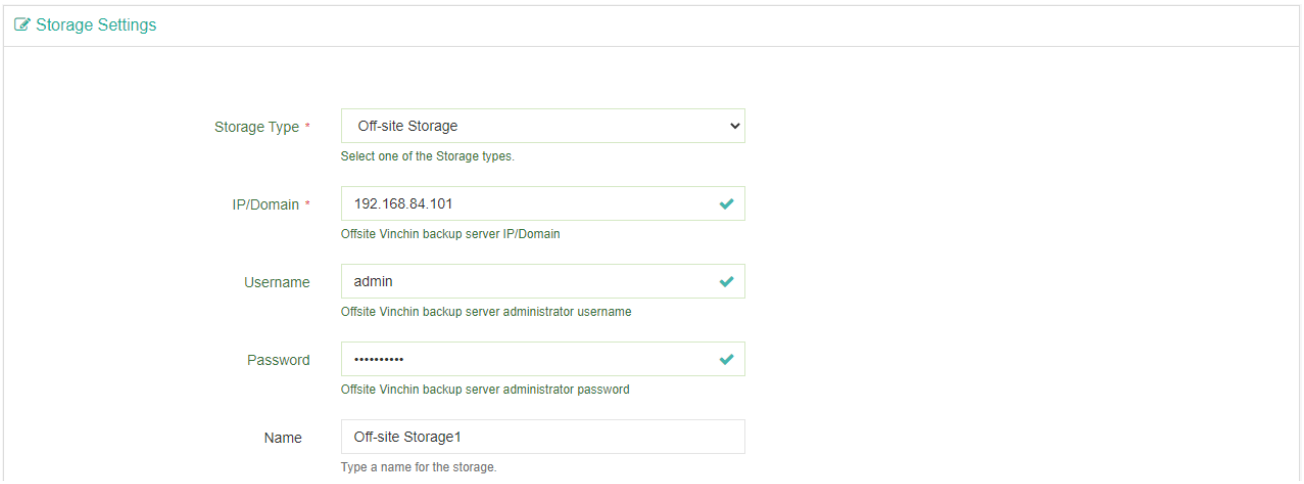
In the **Username** and **Password** fields, please enter the user name and password of the user on the CIFS storage server, who shared this storage.

Vinchin Backup Server will not delete the existing data on the CIFS storage.

- **Off-site Storage**

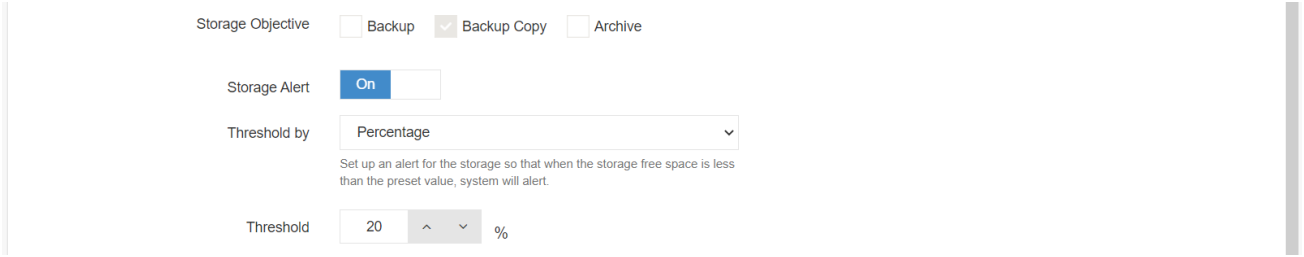
An off-site storage is another Vinchin Backup Server in another location, it is used as Backup Copy storage only. By using off-site storage, you can save remote backup copy to secure the backup data from any possible site disasters. Before adding an off-site storage, please make sure another Vinchin Backup Server had been deployed in your remote location, and Backup Copy Storage had been added to it.

To add the off-site storage, please select **Off-site Storage** in the **Storage Type** field.



In the IP/Domain field, please enter the IP address of the remote site Vinchin Backup Server.

In the Username and Password fields, please enter the administrator username and password.



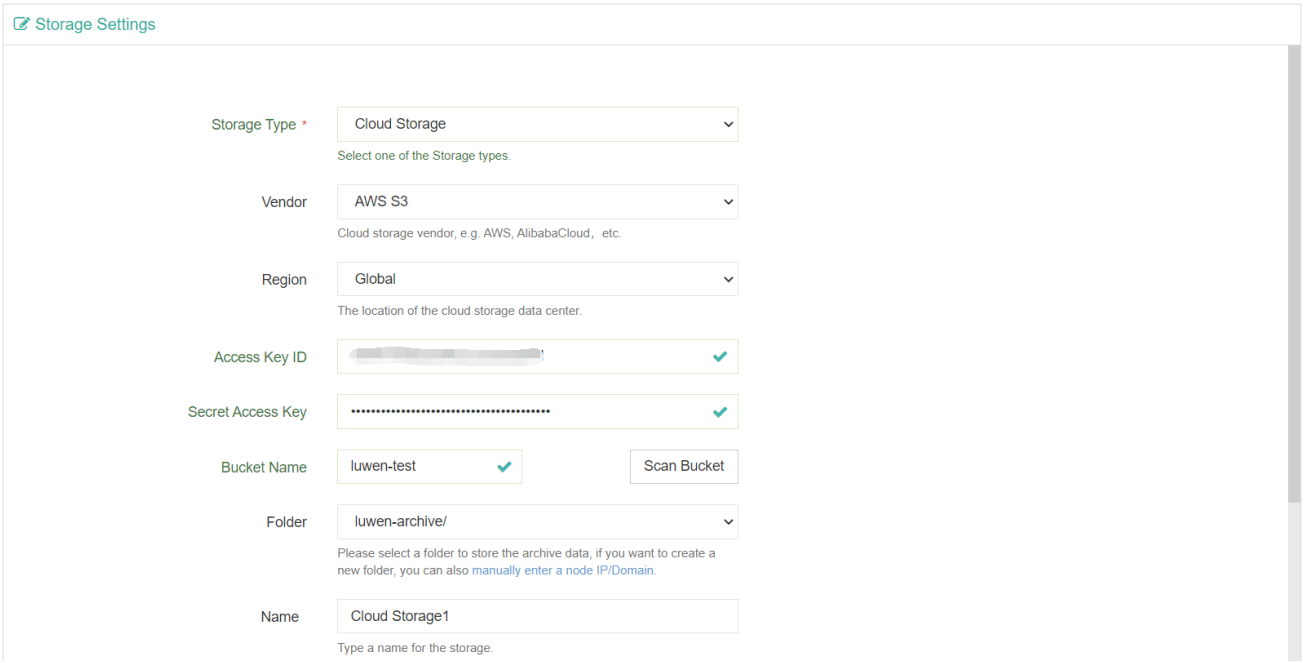
Note

If you are connecting the remote off-site storage over Internet, please open TCP port 30050 and 30051 on the remote site router or firewall.

- **Cloud Storage**

Cloud storage is used for archiving the backup data only. Amazon AWS S3, S3 compatible and Alibaba Cloud storage are supported by Vinchin Backup Server v6.0.

To add a cloud storage (AWS S3 for example), please select **Cloud Storage** in the **Storage Type** field.



In the **Vendor** field, please select **AWS S3**.

In the **Region** dropdown list, please select **Global**.

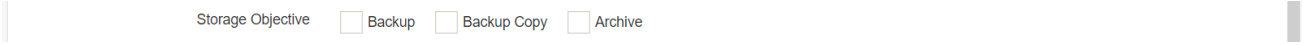
In the **Access Key ID**, **Secret Access Key** and **Bucket Name** fields, please enter the credentials provided by Amazon AWS S3.

After you had entered the correct credentials, please click on **Scan Bucket** button. Vinchin Backup Server will try to scan the specified bucket of your account.

After scanning, if there are existing folders in the bucket, you are able to select from the **Folder** dropdown list. The selected folder will be used to save the backup archive data. If you want to create a new folder for backup archive data, you can manually type a new folder name here, once you confirm to add the cloud storage, the new folder will be created in the specified bucket.

Storage Objectives

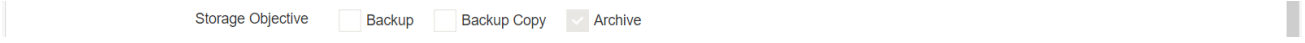
For the storage types: Partition, Local Disk, Local Directory, LVM (logical volume), Fibre Channel, iSCSI, NFS and CIFS. The objective of these storage types can be configured as Backup storage, Backup Copy storage or Archive storage, but one storage device can be only configured with one objective.



For the Off-site Storage, it is another remote/off-site Vinchin Backup Server, and it can be only used as Backup Copy (off-site) storage.

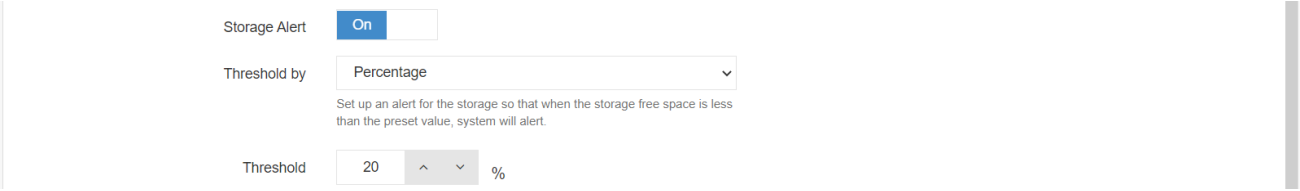
When you add the off-site storage, Backup Copy will be selected by default, and you cannot change the storage objective.

For the Cloud Storage (Amazon S3 or Alibaba Cloud), when you add it you'll see the Storage Objective is defaulted to Archive as below.



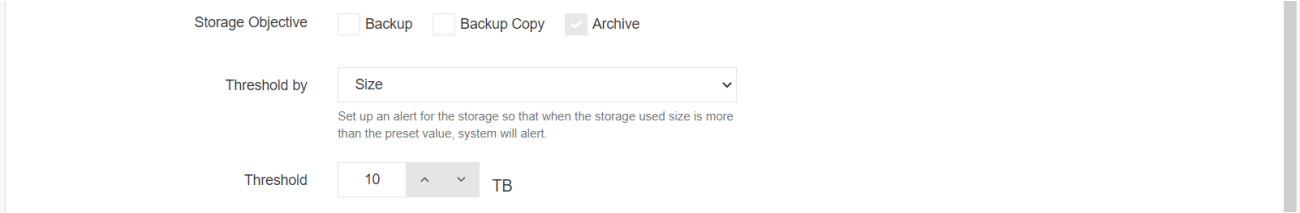
Usage Alert

For the storage types: Partition, Local Disk, Local Directory, LVM (logical volume), Fibre Channel, iSCSI, NFS, CIFS and Off-site Storage. You can choose either to enable the storage usage alert or not.



The storage usage alert threshold can be configured per the percentage of free space or the actual value of free space. When the storage usage reaches the specified threshold, Vinchin Backup Server will alert in the notification center.

As for the cloud storages, the alert of storage usage is enabled by default, see the figure below.

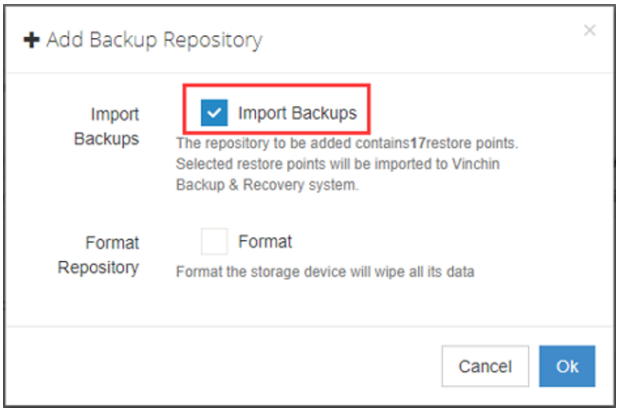


The threshold of alerting is per the total size of data that have been uploaded to the cloud storage. You only have to specify the quota of data size, then Vinchin Backup Server will alert you when you are running out of the quota.

Data Importing and Storage Formatting

For the storages to be added, if once they had been used by Vinchin Backup Server, the backup/copy/archive data should still remain on them. When you try to add them again, the data will be automatically recognized by Vinchin Backup Server.

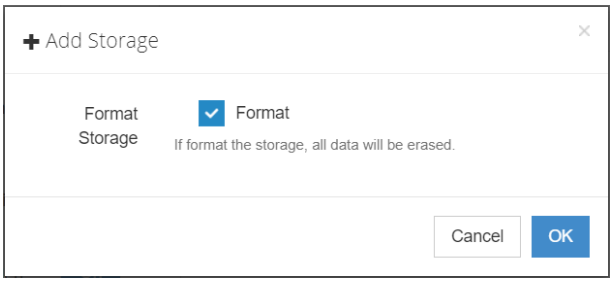
For the block storages Partition, Disk, LVM, Fiber Channel, iSCSI, you have options to import the backup data or to format the storage. See the figure below.



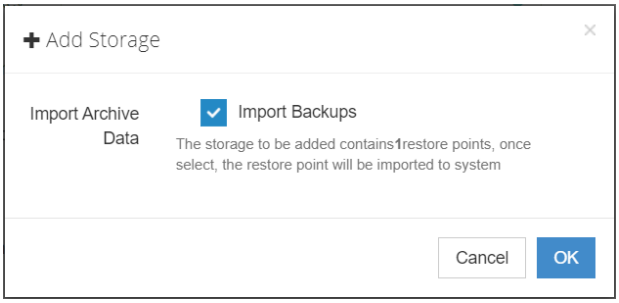
It is recommended to import the backup data and then add it to Vinchin Backup Server. Otherwise, if you choose to format, Vinchin Backup Server will erase all data on the block storage then add it as a fresh new storage device.

If the block storage had not been used by Vinchin Backup Server before, but it may contain other data, please make

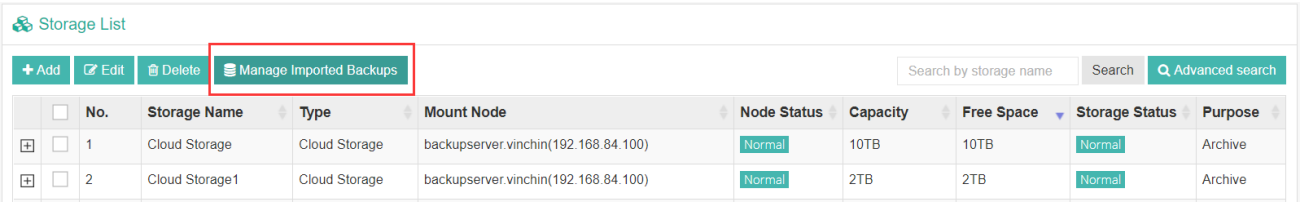
sure you had backed up all the data before formatting.



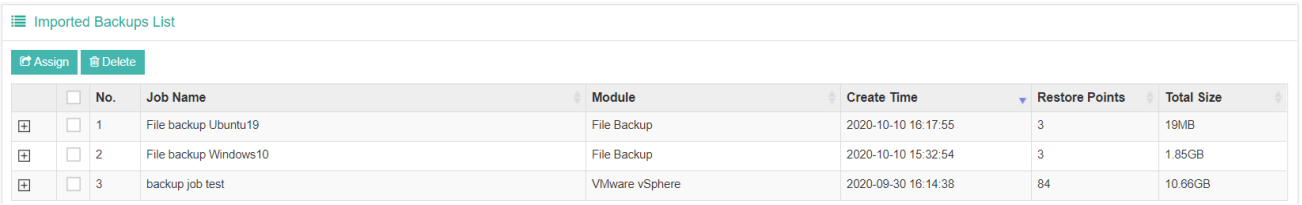
For the file storages and object storages, if there's existing backup data, you'll have to import the data to add it to Vinchin Backup Server.



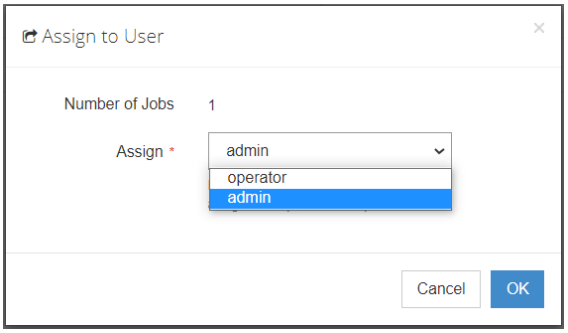
The imported backup data can be found on the **Resources** > **Storage** page by clicking on the **Manage Imported Backups** button.



The imported backups will be organized by the backup job name.



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.

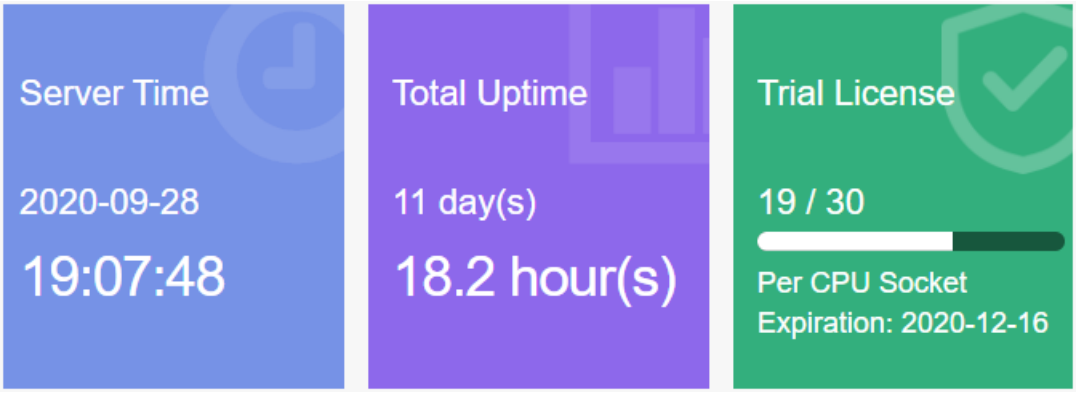


Once the backup data had been assigned to a user, the user will be able to see the backup data and create restore jobs with those data.

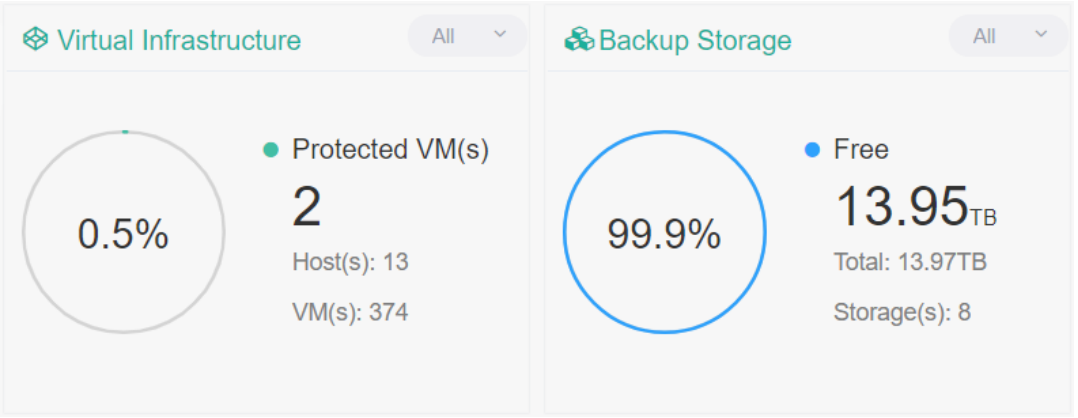
Informational

Dashboard

Each time when you log in to Vinchin Backup Server you'll first see the Dashboard screen, here you can have an overview of the backup server status.
Here are the server time, total uptime and license information.

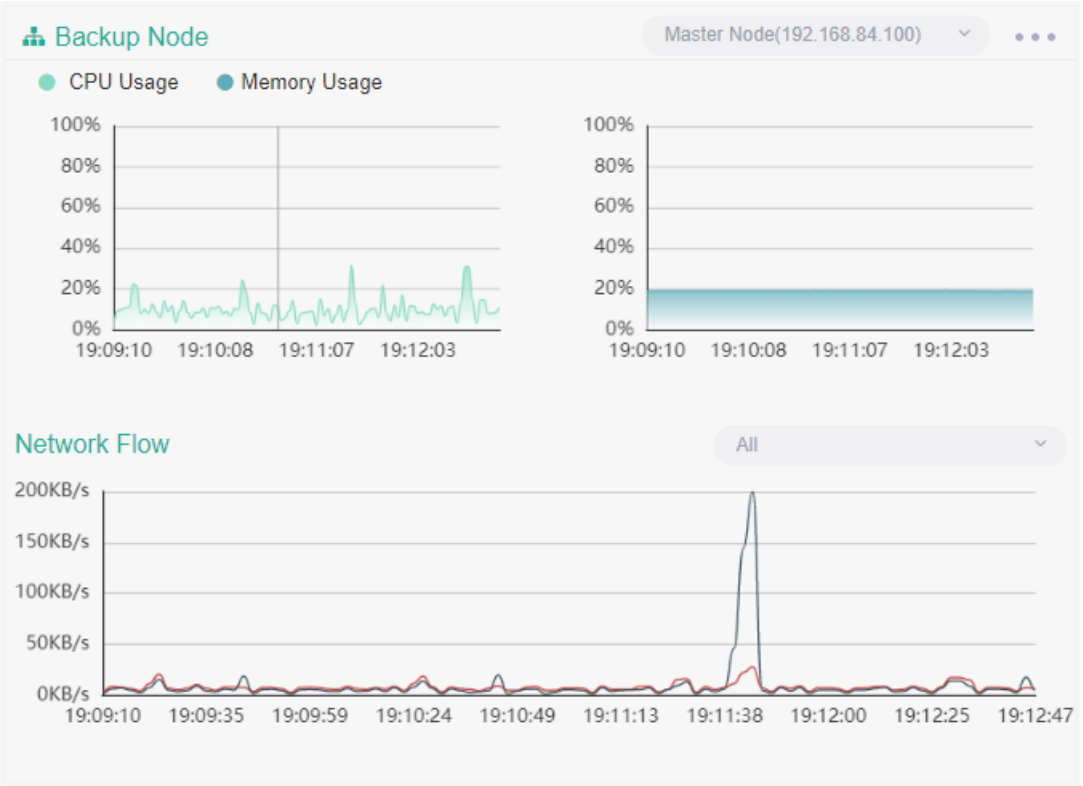


Here are the information of your virtual infrastructure(s) and backup storages.



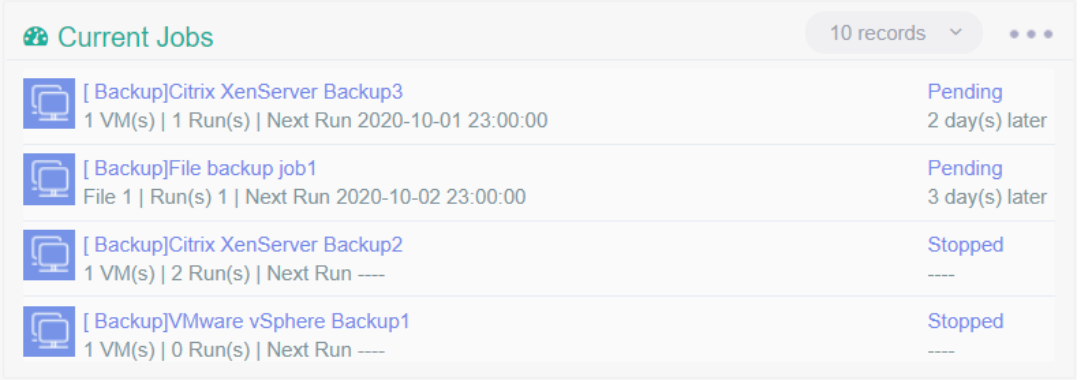
In the **Virtual Infrastructure** column, the total number of hosts, VMs and protected VMs will be displayed. If you had added multiple virtual infrastructures, click on the dropdown list on the top right, you can check an individual infrastructure information.
In the **Backup Storage** column, the total storage capacity added to Vinchin Backup Server will be displayed. Click on the dropdown list on the top right, you can check an individual storage device information.

The system resources of the master node and slave node(s) can be monitored as shown in the figure below.



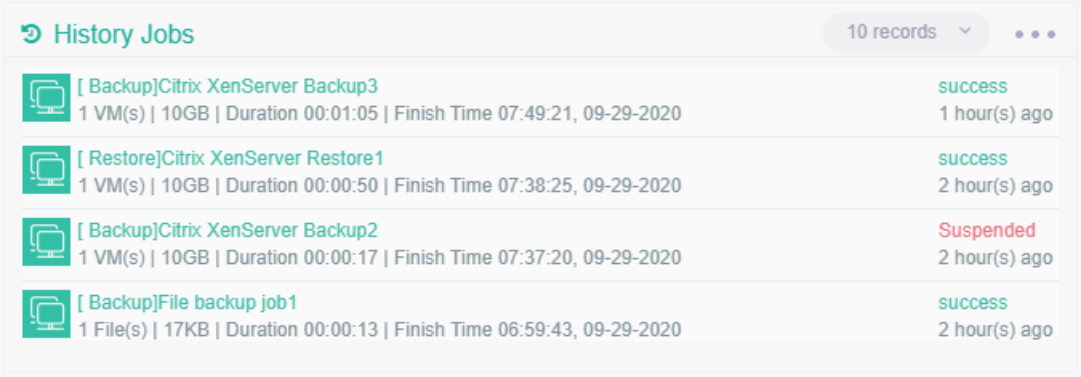
Select a node from the top right dropdown list you are able to monitor the CPU and memory usage, and also the network flow. In the **Network Flow** chart, it shown the network flow of all NICs of the selected node, to view the network flow of an individual NIC, please select that NIC from the Network Flow dropdown list.

In the **Current Jobs** section, the currently running jobs and the jobs which will be executed most recently will be listed here.



From the job list, by clicking on one of the jobs you are able to view the job details. Or if you want to check more jobs' information please go to the **Monitor Center** > **Jobs** page, and you can find those jobs in the **Current Jobs** list.

In the **History Jobs** section, a list of recently executed jobs will be displayed here.



To check more logs of the history jobs, please go to **Monitor Center** > **Jobs** page, and you can find more history jobs in the **History Jobs** list.

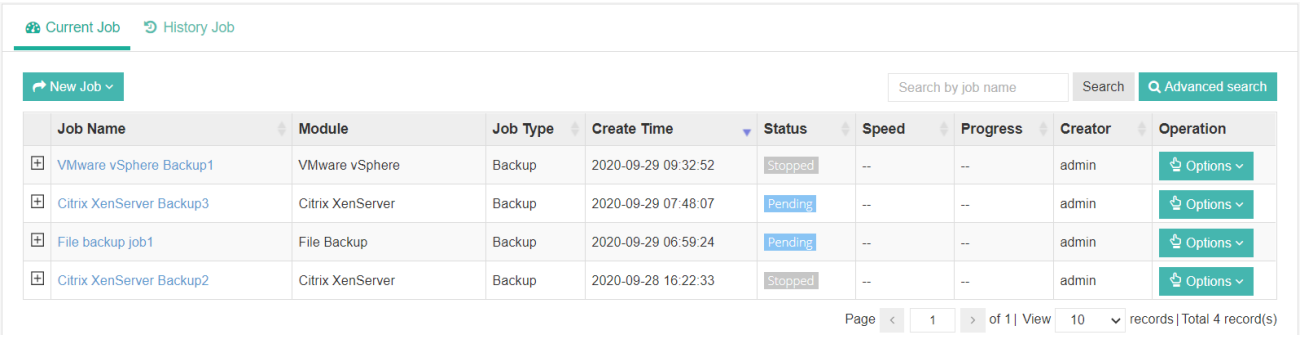
Monitor Center

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.



To create a new job, please click on the **New Job** button, and then you'll be given the options to create a VM Backup, File Backup, Backup Copy or Backup Archive job.

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.

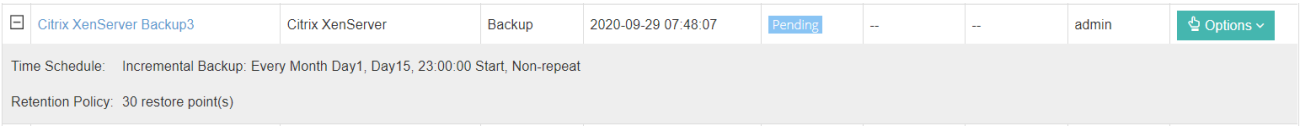
Edit: to modify the configurations of a job in Stopped state.

Delete: to delete a job and all the schedules, but the backup data will remain.

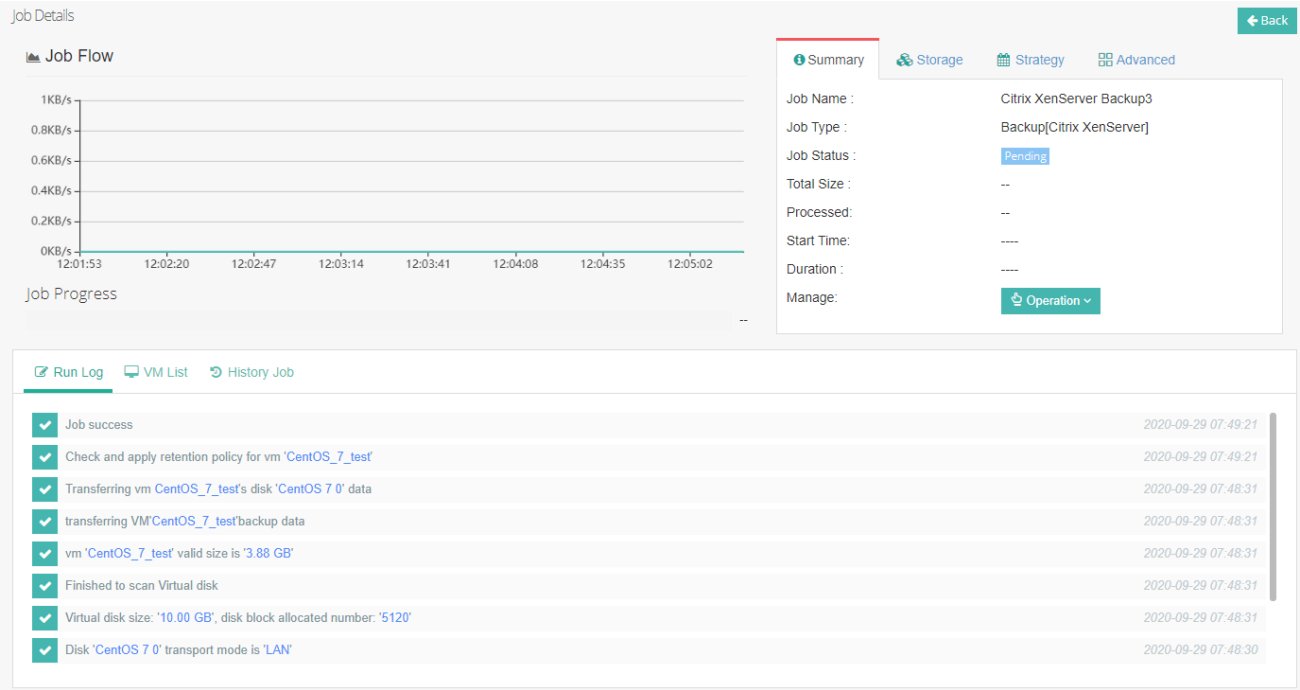
Note

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.

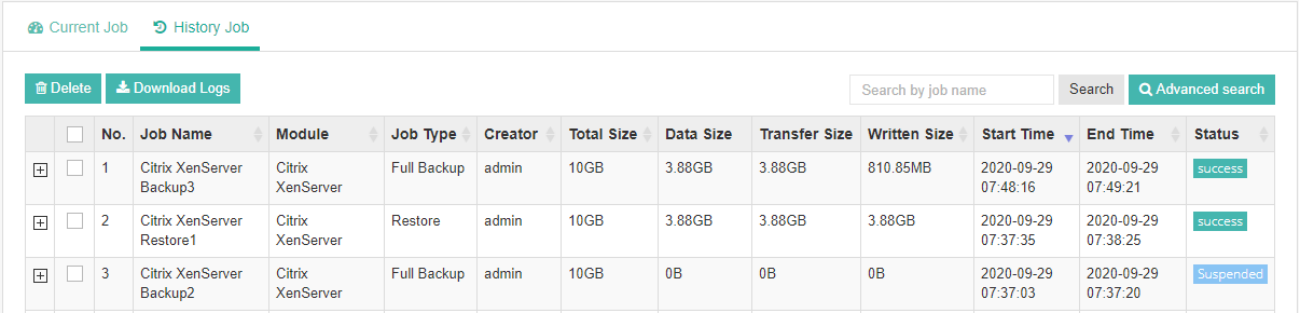
Run Log: if the job is currently running, it will be the real-time log output; if the job is pending or stopped, it will provide the logs of the last time of running.

VM List: if the job is running, all VMs included in this job will be listed here.

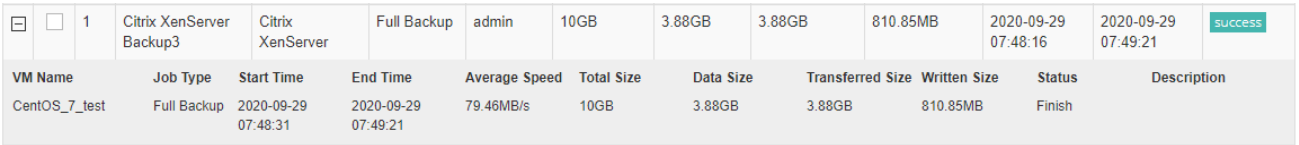
History Job: the running history of the job.

- **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.

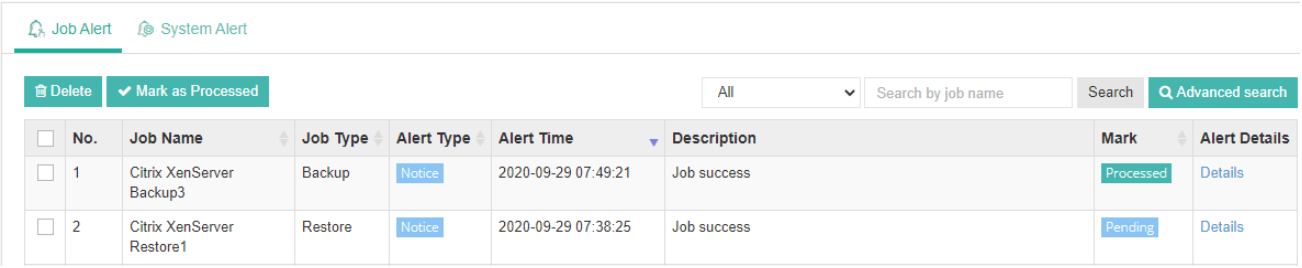


To delete the history jobs, please select the job logs and click on the **Delete** button.
And for the failed jobs, you can select that job and click on **Download Logs** button to download the detailed logs of that job for troubleshooting.

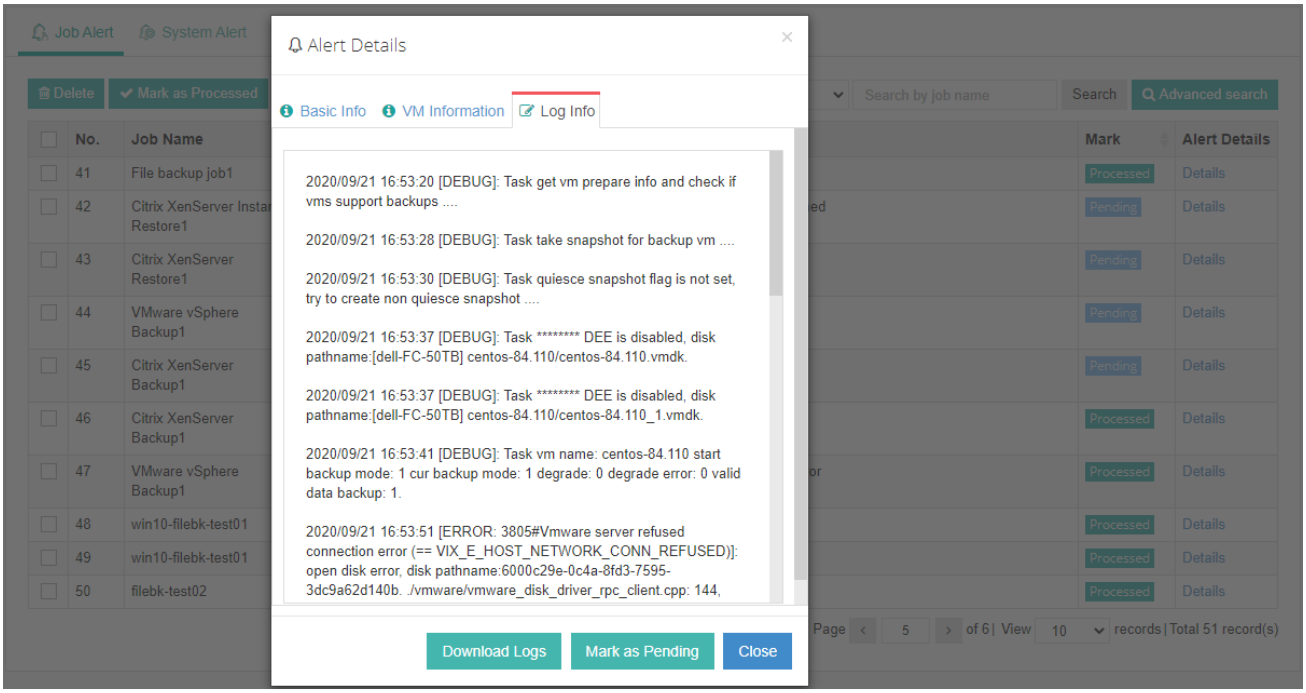
Alerts

- **Job Alert**

Job alerts can be found on the **Monitor Center** > **Alerts** page, under the **Job Alert** tab.



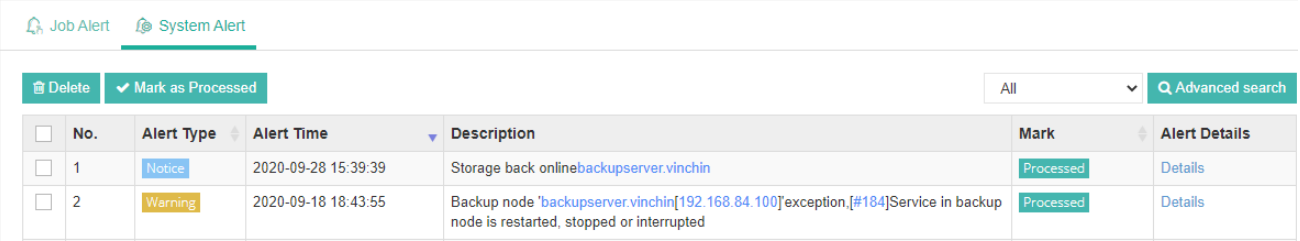
By using the dropdown list above the alert list, you can filter the alert messages by alert types, including notices, warnings and errors.
Click on **Details** button of an alert, you can view the detailed description of the alert message, and at the same time the alert message will be marked as **Processed**. 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.



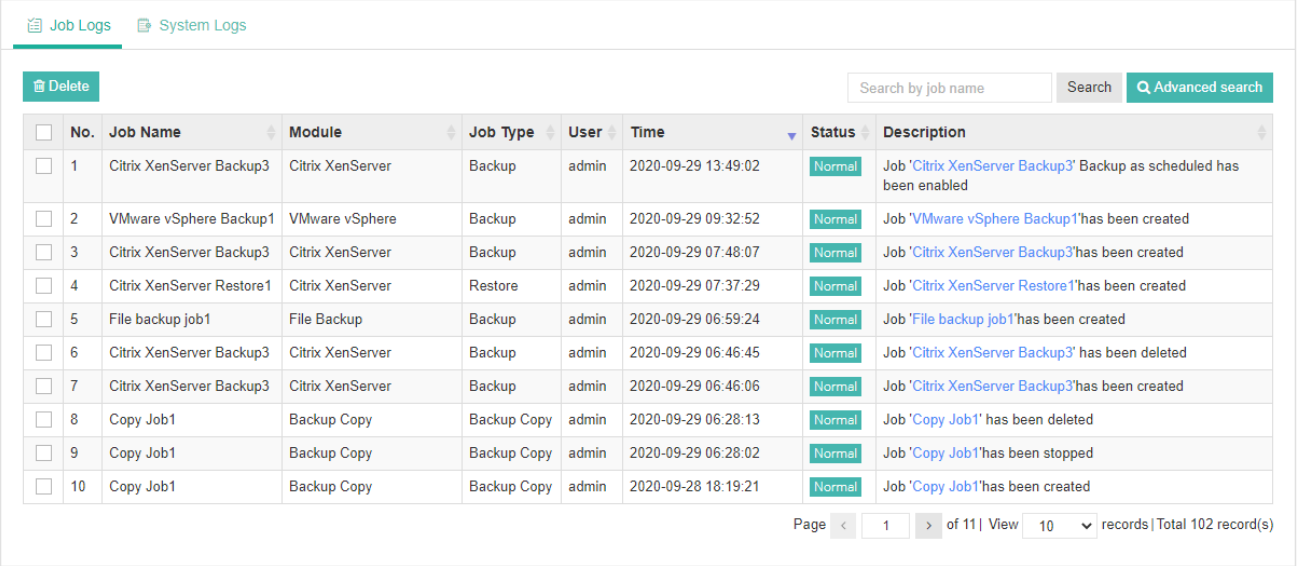
Similar as the job alerts, you can have the same options to filter these alert messages and you can mark the messages as processed or pending state.

System alert messages are mainly used to notify users about the backup server, backup node(s) and storages status.

Logs

- **Job Logs**

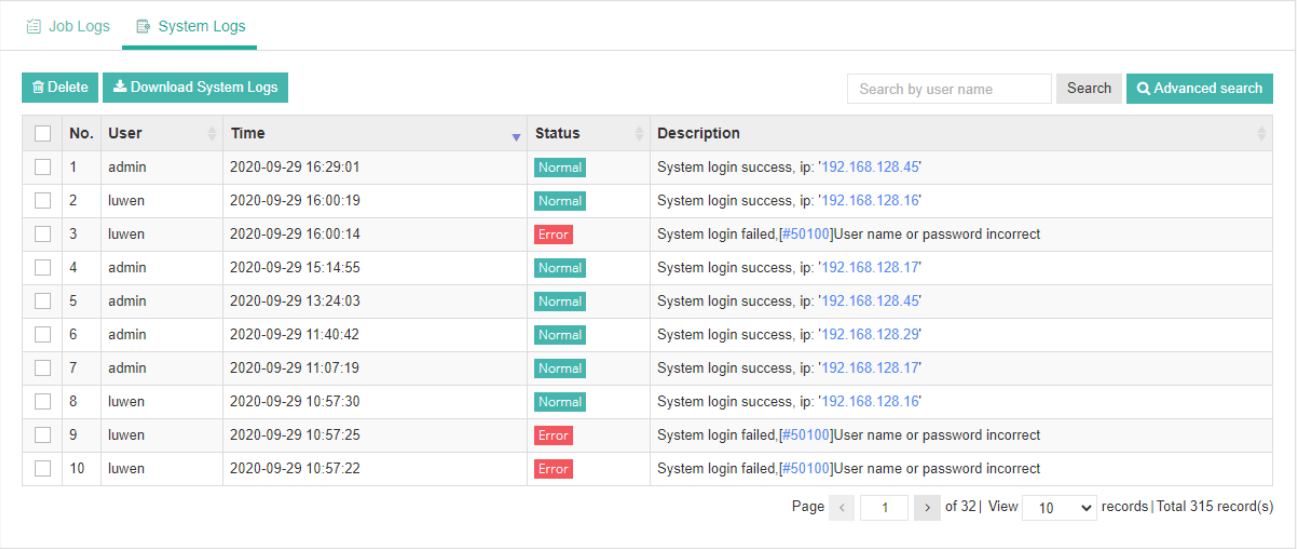
On the **Monitor Center** > **Logs** page, under the **Job Logs** tab, the operations related with job stop, job schedule on, job creation, job deletion and job modification can be all found here.



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.

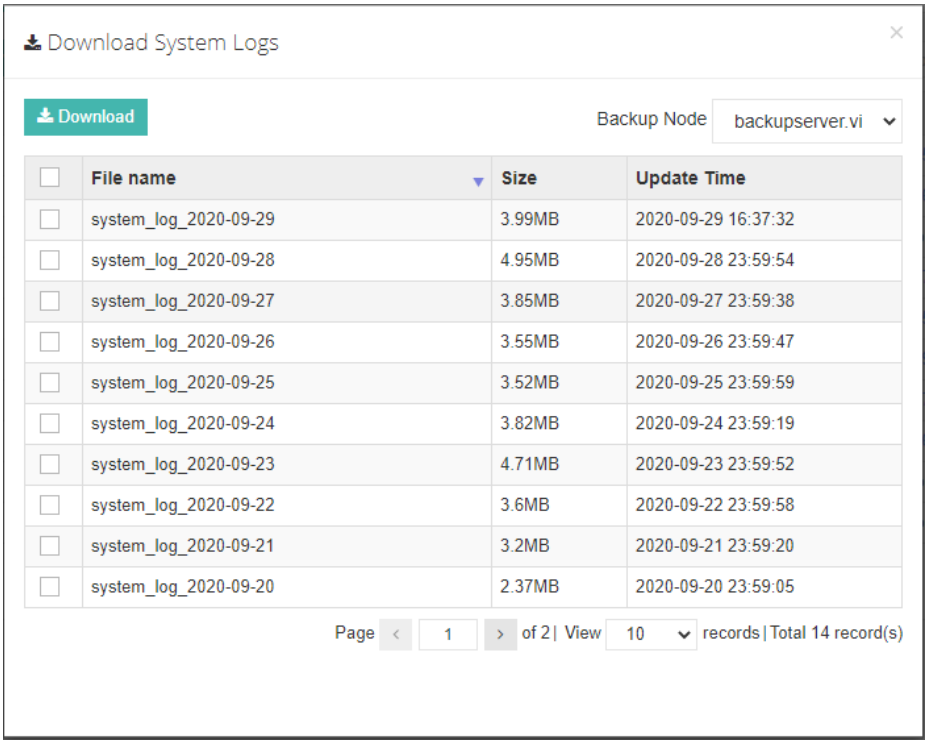
- **System Logs**

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.



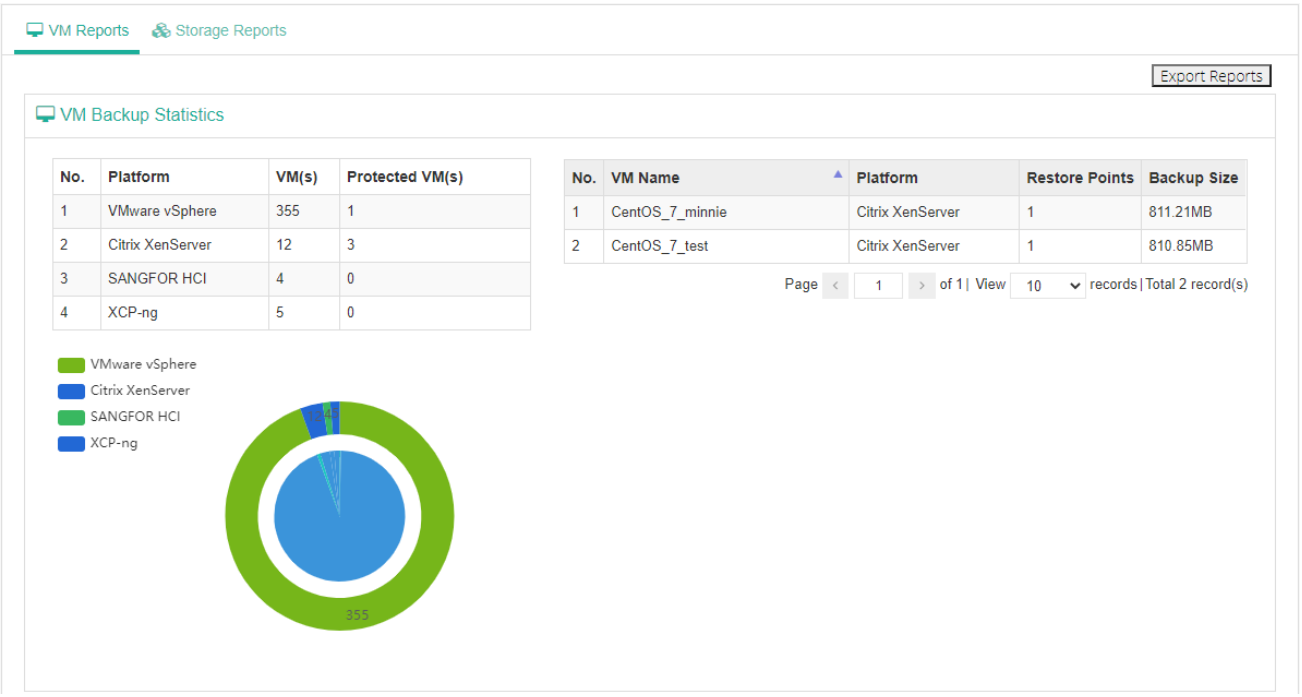
In the **Download System Logs** dialog, the logs are arranged by date. You can select the desired logs and click on the **Download** button to download the logs.

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.

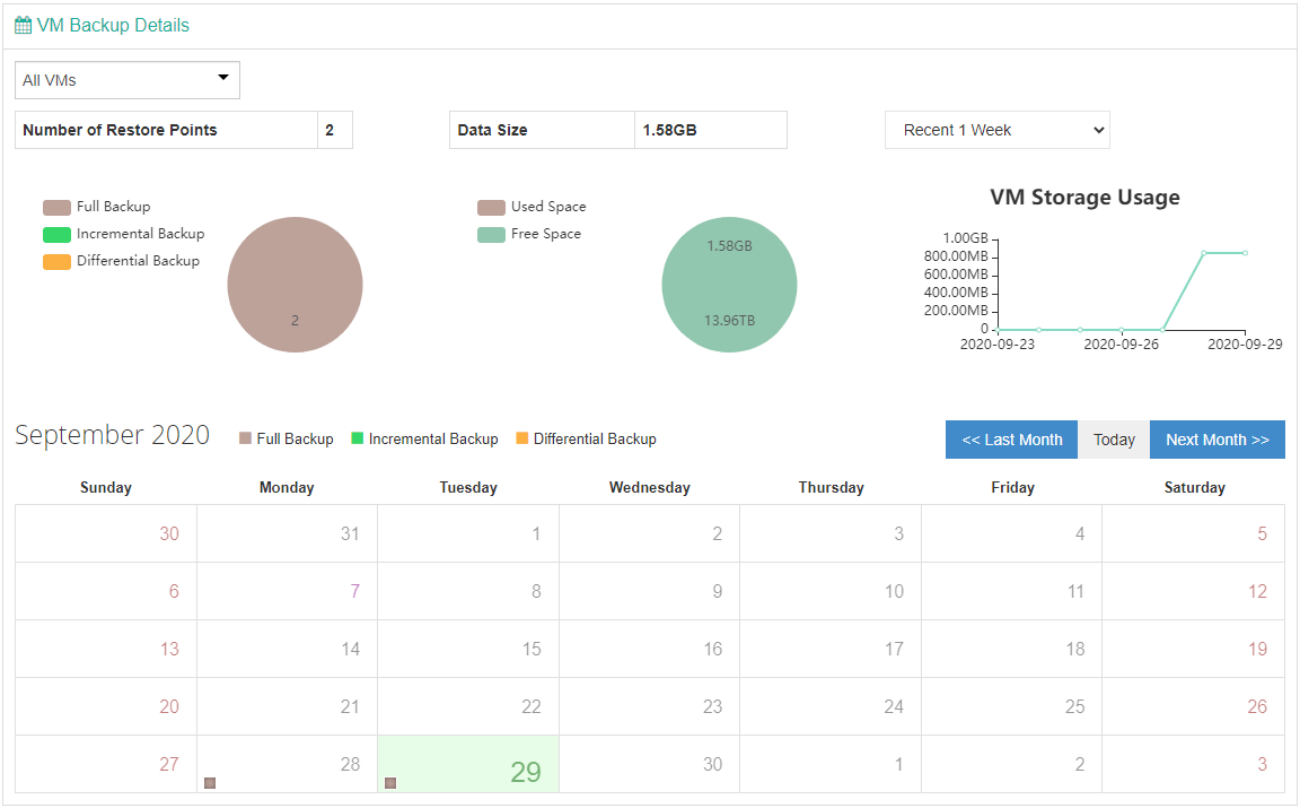
Reports

- **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.

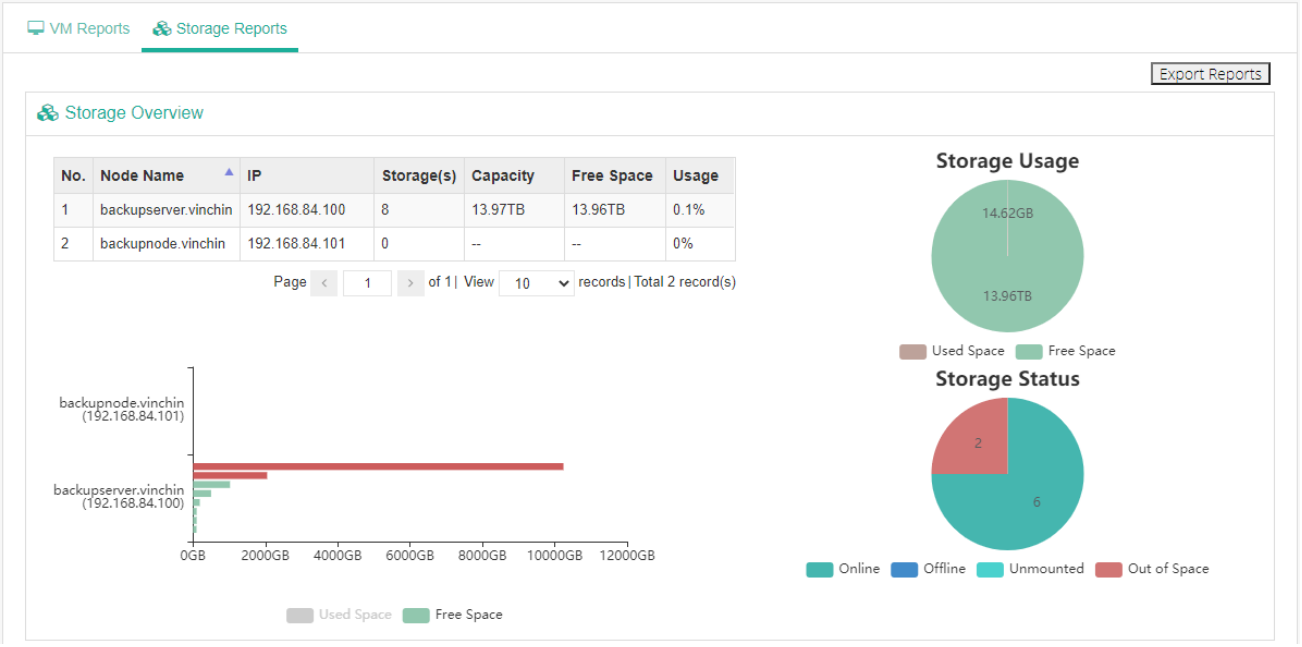


In the VM Backup Details section, you can have the following statistics reports:

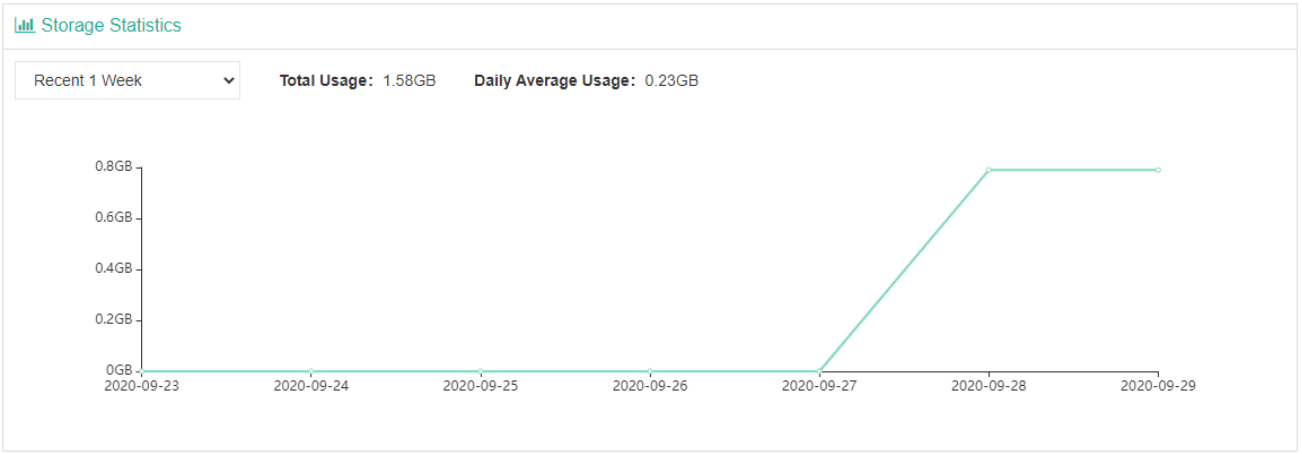
- Number of restore points and a pie chart of restore points by different backup technologies.
- The total size of all backup data.
- The line chart of storage usage per 1 week, 2 week or a month.
- The backup schedules in calendar view.

- **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.



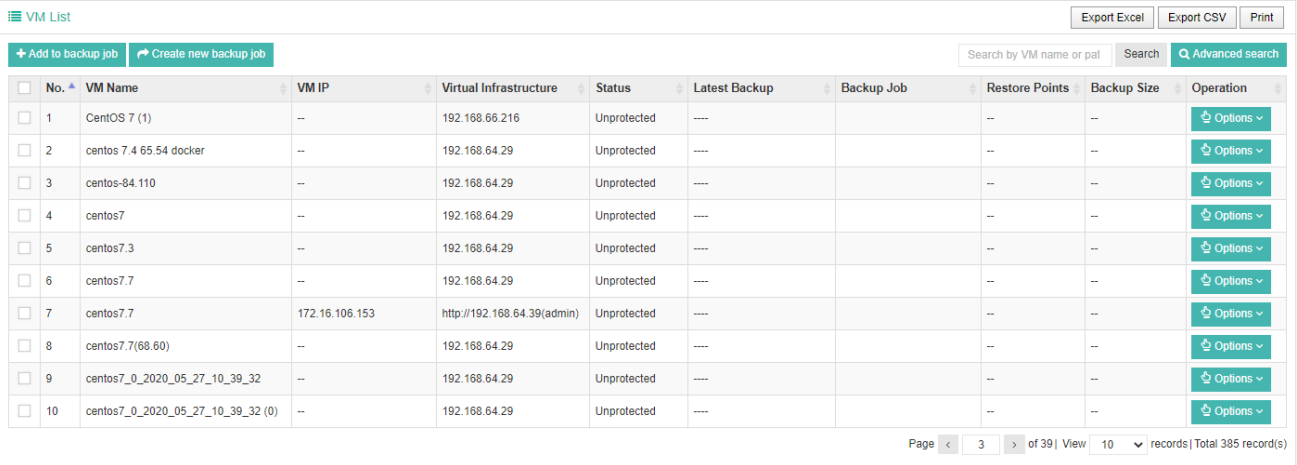
In the **Storage Statistics** section, you can have the reports of total storage usage and daily average usage. And a line chart of storage usages per 1 week, 2 weeks, 1 month, 2 months or 3 months.

Backup

Backup

Virtual Machines

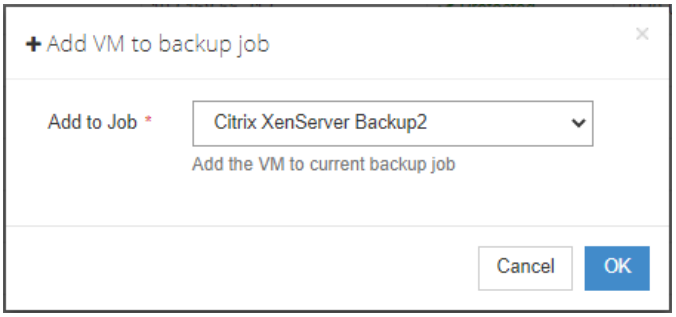
On the **VM Backup** > **Virtual Machines** page, you can view all the VMs from all virtual platforms which you've added into Vinchin backup server.



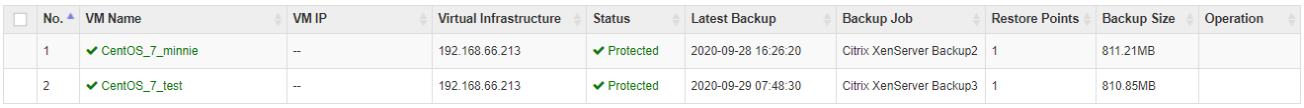
You can select multiple unprotected VMs to add to an existing backup job or create a new backup job. By clicking **Options** under **Operation**, you can choose to add a specific VM to an existing backup job, or choose to create a new backup job for this specific VM.

Or you can select the target VM(s) and click on the **Add to backup job** button to add the VM(s) to existing backup jobs, or you can click on **Create new backup job** to create a new backup job to protect the selected VM(s).

To add the selected VM(s) to existing backup job, please select the existing backup job as below.



When a VM has been added to a backup job, the status will be change to Protected, and the number of restore points and the backup data size will be organized on the Virtual Machines page.

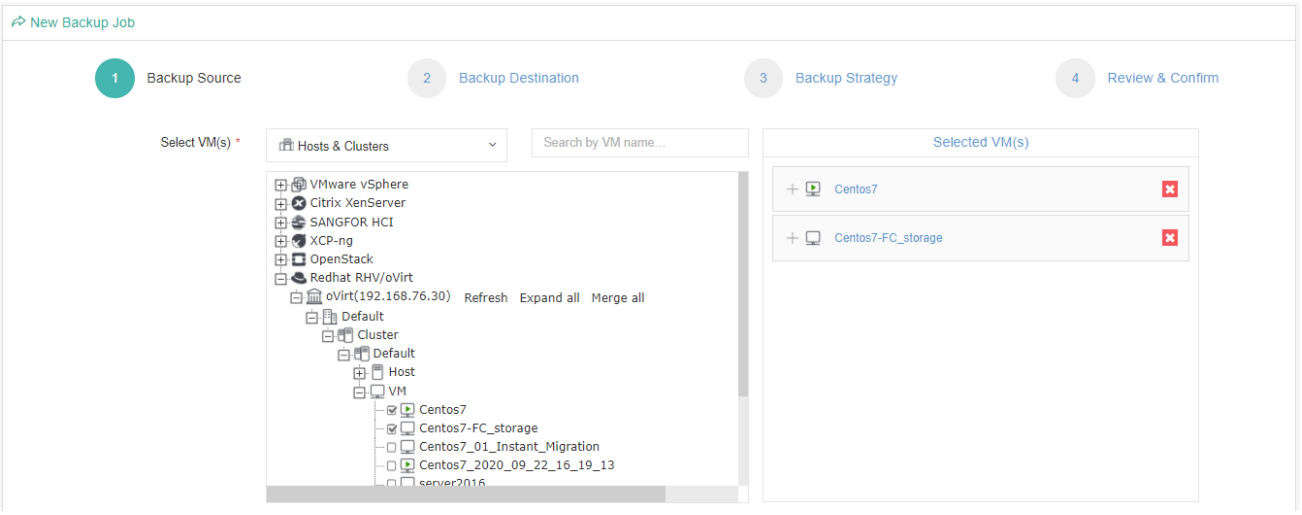


Create Backup Job

To create a backup job, you can do it from the Virtual Machines page by selecting target VM(s) and then click on Create new backup job, or you can do it on **VM Backup** > **Backup** page. Please follow the below steps to create VM backup jobs.

Step 1: Backup Source

Select the virtual machines you want to back up from the virtualization infrastructure tree, expand the infrastructure until you see the virtual machines. Tick any virtual machines you need to back up, the selected virtual machine(s) will be added to the **Selected VM(s)** column.

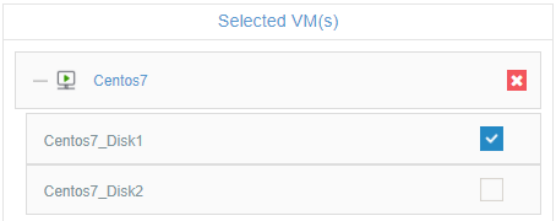


Note

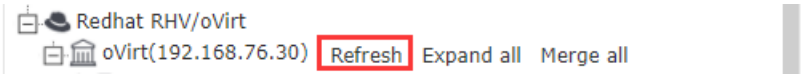
1. If the VM is already in an existing backup job, it will be highlighted in Green and un-selectable.

2. If you want to add multiple VMs in one backup job, you can only select multiple VMs from the same virtual platform.

Click on the selected VM, all the virtual disks mounted to this VM will show up, you can choose to exclude specific disk(s) from this backup job by unticking the disk(s).



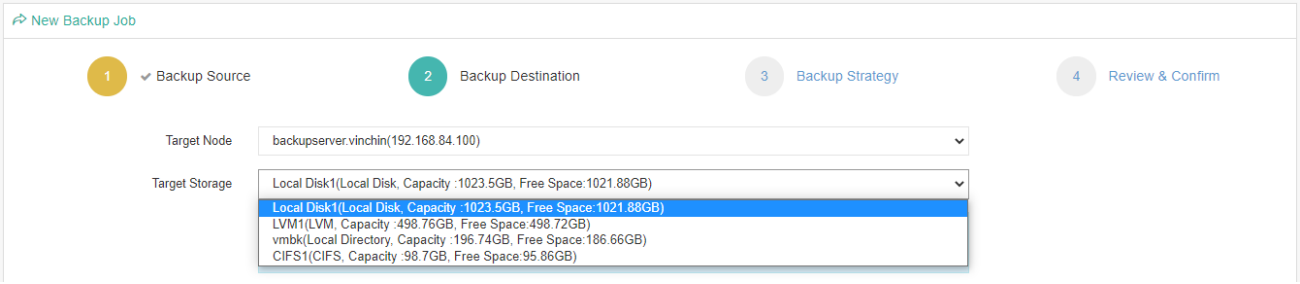
If your virtual infrastructure has been updated recently, click “Refresh” to update and sync the VM list to Vinchin backup server.



When done adding the target VM(s), please click on **Next** button 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.

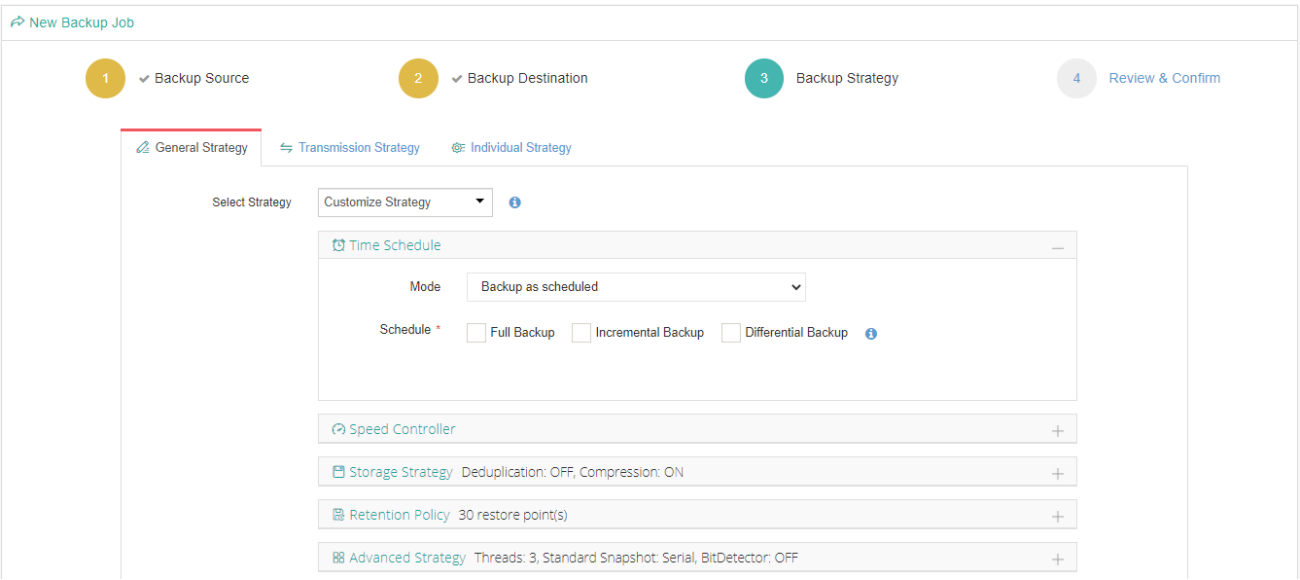
In the **Target Storage** dropdown list, the storages which belong to the selected backup node can be selected.

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

Step 3: Backup Strategy

➢ General Strategy

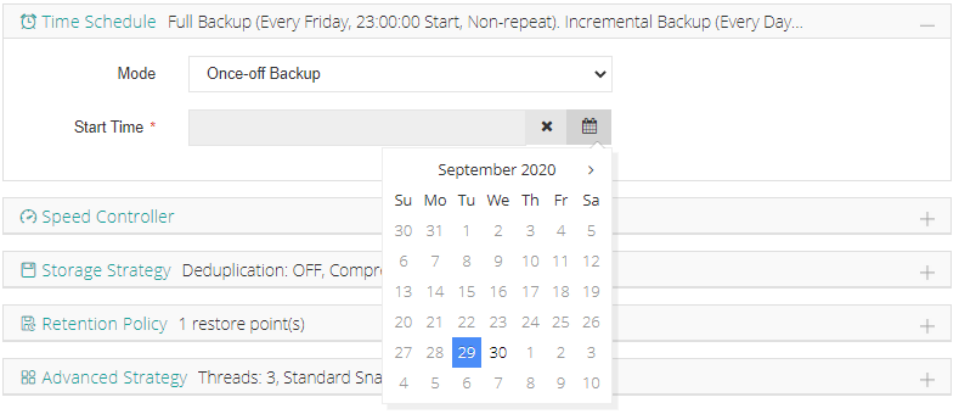
Under the General Strategy tab, you can setup the backup Time Schedule, Speed Controller, Storage Strategy, Retention Policy and Advanced Strategy.



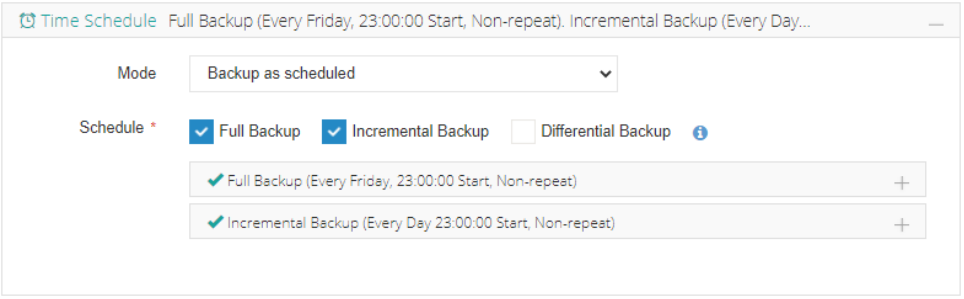
In the **Select Strategy** dropdown list, you can select a preconfigured strategy template, if you had created strategy templates, otherwise choose **Customize Strategy**. For how to create strategy templates, please refer to Strategy.

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.

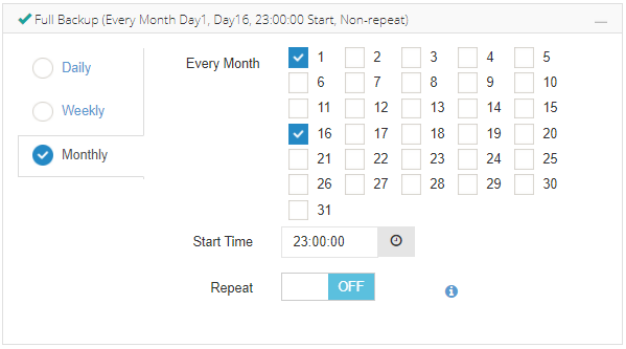
For a once-off backup job, the job will only run for once, and only full backup will be performed. You only have to appoint a time of when to start the backup job in the Time Schedule field.



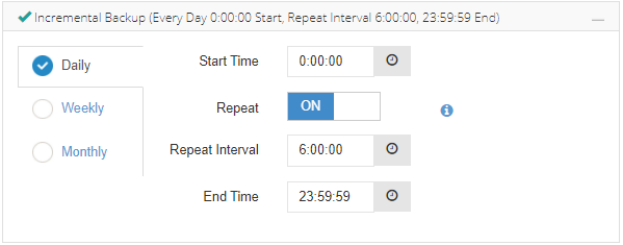
For Scheduled backup job, you can schedule Full Backup with Incremental Backup combination, Full Backup with Differential backup combination or Forever Incremental Backup (enable incremental backup only).
Here we take Full Backup with Incremental Backup as an example.



By default, full backups will be scheduled on each Friday night at 11PM. And incremental backups will be scheduled each day at 11PM (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 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.

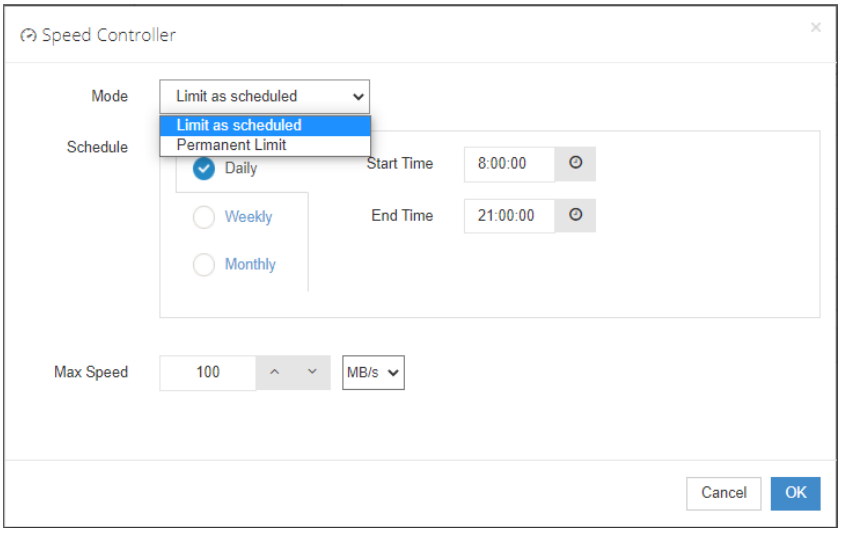


Then configure several incremental backups each day, by default incremental backup will run only for once each day, to run incremental backups several times a day, you can enable the **Repeat** option.



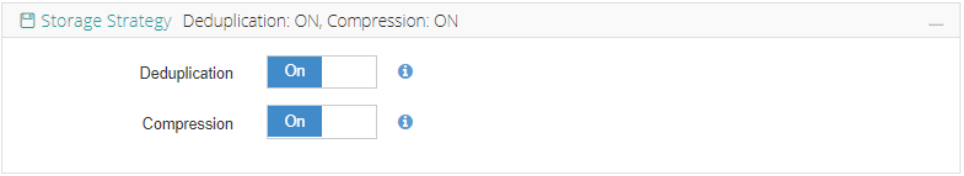
In the above example, full backups will run on day 1 and day 16 of each month, incremental backups will run every 6 hours each day. This is just an example, you should configure the schedules per your requirements based on your actual virtual environments.

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.



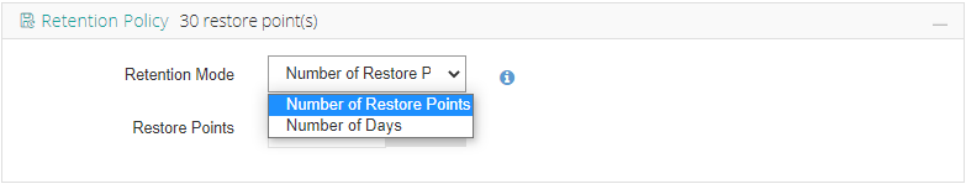
The speed controller can be configured as **Permanent Limit** or **Limit as scheduled**.

Storage Strategy including **Deduplication** and **Compression** of the backup data.



By enabling these 2 options, you can save the bandwidth and storage resources for transmitting and storing the backup data.

Retention Policy can be configured as per the **Number of Restore Points** or the **Number of Days**. It is applicable for the scheduled backups, as the once-off backup will only generate one restore point, so the retention policy is not applicable.



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.

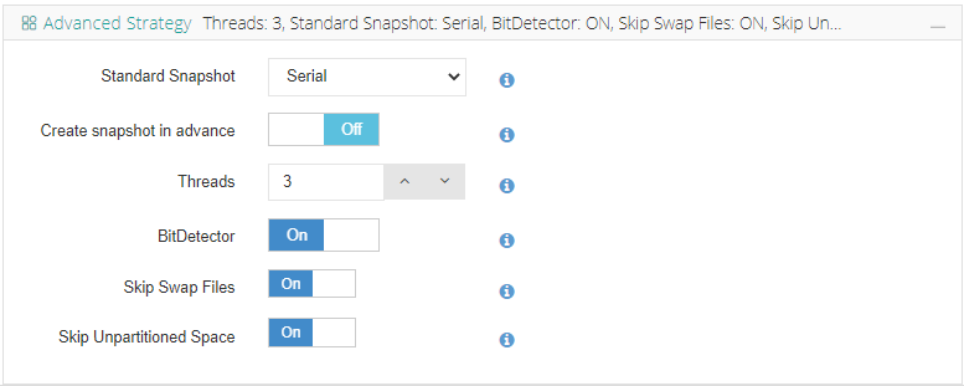
For the incremental backup jobs, to comply with the retention policy, Vinchin backup server will merge the first full backup with the following incremental backup restore points to comply with the retention policy. If it's a forever

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 time running the backup 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 time running the backup job.

For Microsoft Hyper-V, the retention policy is different with other virtual platforms, it is based on full backup restore points. It will lead a deletion of the furthest full backup point together with its corresponding incremental or differential backup points when a new full backup point is generated.

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 send to the virtual platform. It's not recommended to set parallel snapshot, as it may cause the production environment overload. Only if the VMs are service correlated which requires all the snapshots to be time consistent.

Create snapshot in advance can be enabled to create the next VM's disk snapshot while the previous VM is being transferred to the backup storage. The feature is not applicable with Microsoft Hyper-V.

By specifying the number of **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 16, but usually 3 threads will be enough.

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

Note

1. If you only select incremental backup or differential backup without selecting full backup, when first time starting this job, system will automatically execute a full backup.

*2. Incremental backup can be configured without full backup, after first time running this job in full backup mode, it will turn into a forever incremental backup mode (*Forever Incremental Backup is not supported with Microsoft Hyper-V).

3. It is recommended to do a full backup each week/month and do an incremental backup every day.

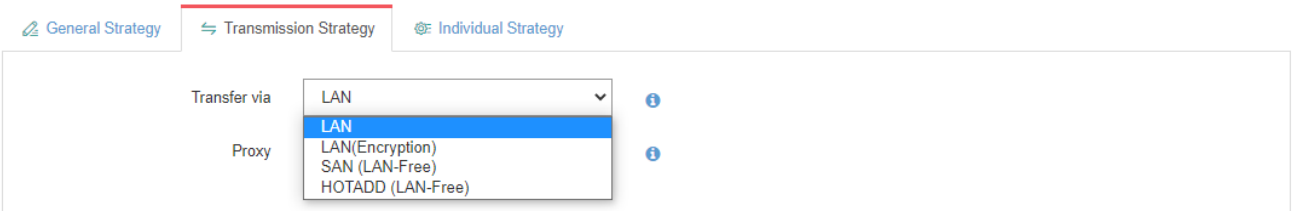
4. It is recommended to set the backup schedule to run at night or in the other nonbusiness hours.

5. Multithreaded transmission does not mean backup several VM disks simultaneously, it only adds additional threads to process one VM disk to improve the transmission speed.

➢ Transmission Strategy

The transmission strategies for different virtual platforms are different.

VMware vSphere:



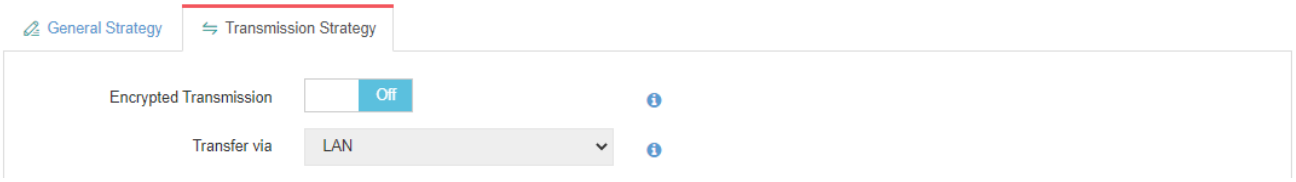
For VMware vSphere, the backup data can be transferred through LAN, LAN (Encryption), SAN (LAN-Free) or HOTADD (LAN-Free).

When you choose to transfer via **LAN** or **LAN (Encryption)**, **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.

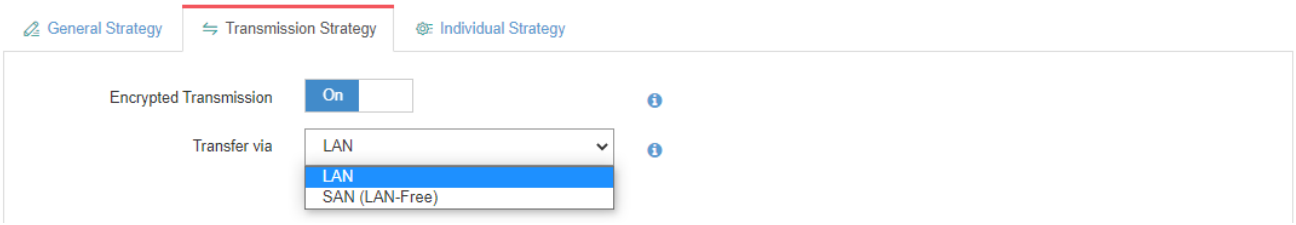
HOTADD (LAN-Free) can be used only if Vinchin Backup Server is installed on the ESXi server as a virtual machine.

Microsoft Hyper-V:



For Microsoft Hyper-V, the backup data transmission is LAN based, you can choose to either encrypt the backup data or not.

Citrix XenServer, XCP-ng, Red Hat RHV/oVirt and OpenStack:

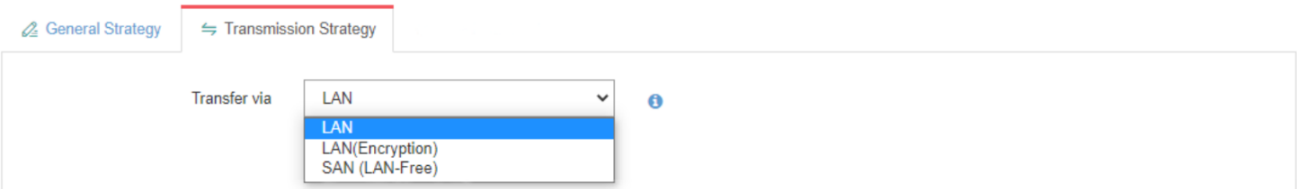


For Citrix XenServer, XCP-ng, Red Hat RHV/oVirt and OpenStack, the backup data can be transferred through LAN or through the storage area network, and you can choose to either encrypt the transmission or not.

SANGFOR HCI:

For Sangfor HCI, the backup data transmission is LAN based, you can choose to either encrypt the backup data or not.

Huawei FusionCompute:

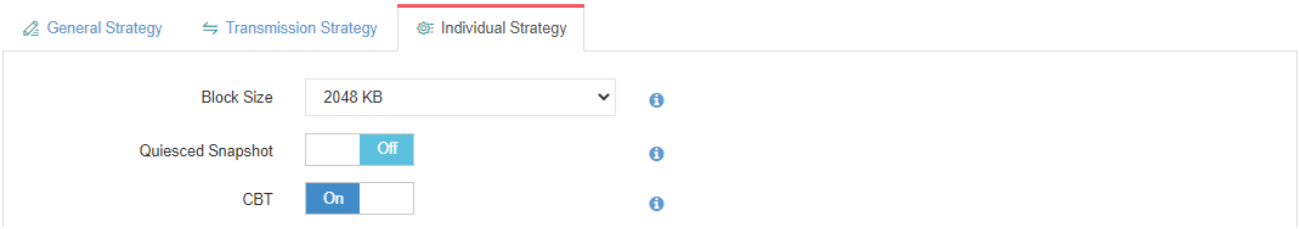


For Huawei FusionCompute, backup data can be transferred through LAN with or without encryption, or can be transferred through the storage area network without encryption.

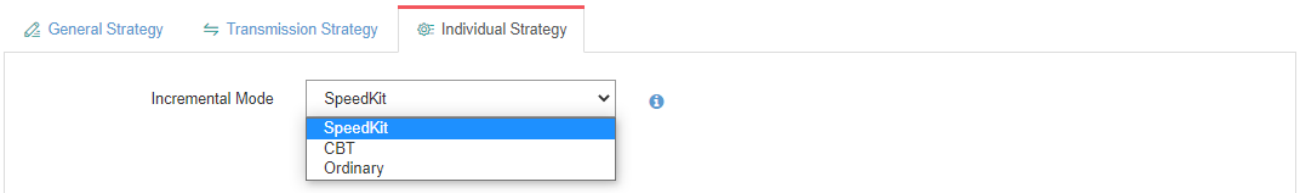
➢ Individual Strategy

The individual strategies for different virtual platforms are different.

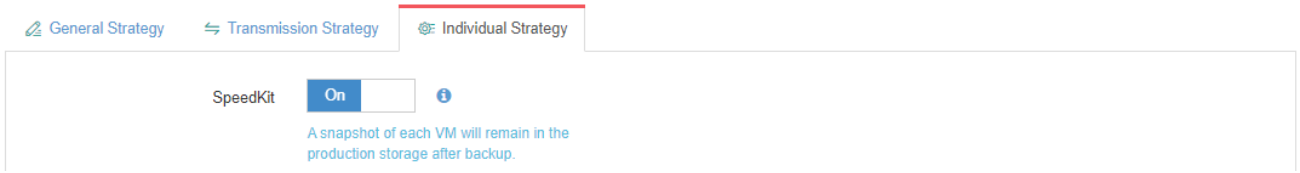
VMware vSphere:



Citrix XenServer and XCP-ng:



RHV/oVirt, SANGFOR HCI, OpenStack:



Huawei FusionCompute:

Strategy descriptions:

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.

SpeedKit is a Vinchin technology to improve the efficiency of incremental backups. It is recommended to be selected if you have sufficient production storage, as there will always be a snapshot kept in your production storage. If you don't want to keep the snapshots or you have limited production storage, disable SpeedKit will release the production storage. Please be noted that after disabling Speedkit, the next incremental backup will automatically run as a full backup, the following incremental backup will be slower.

When performing incremental backups using **Ordinary** mode, a snapshot is not required to be always kept in your production environment, but it will take relatively longer time for incremental backup job.

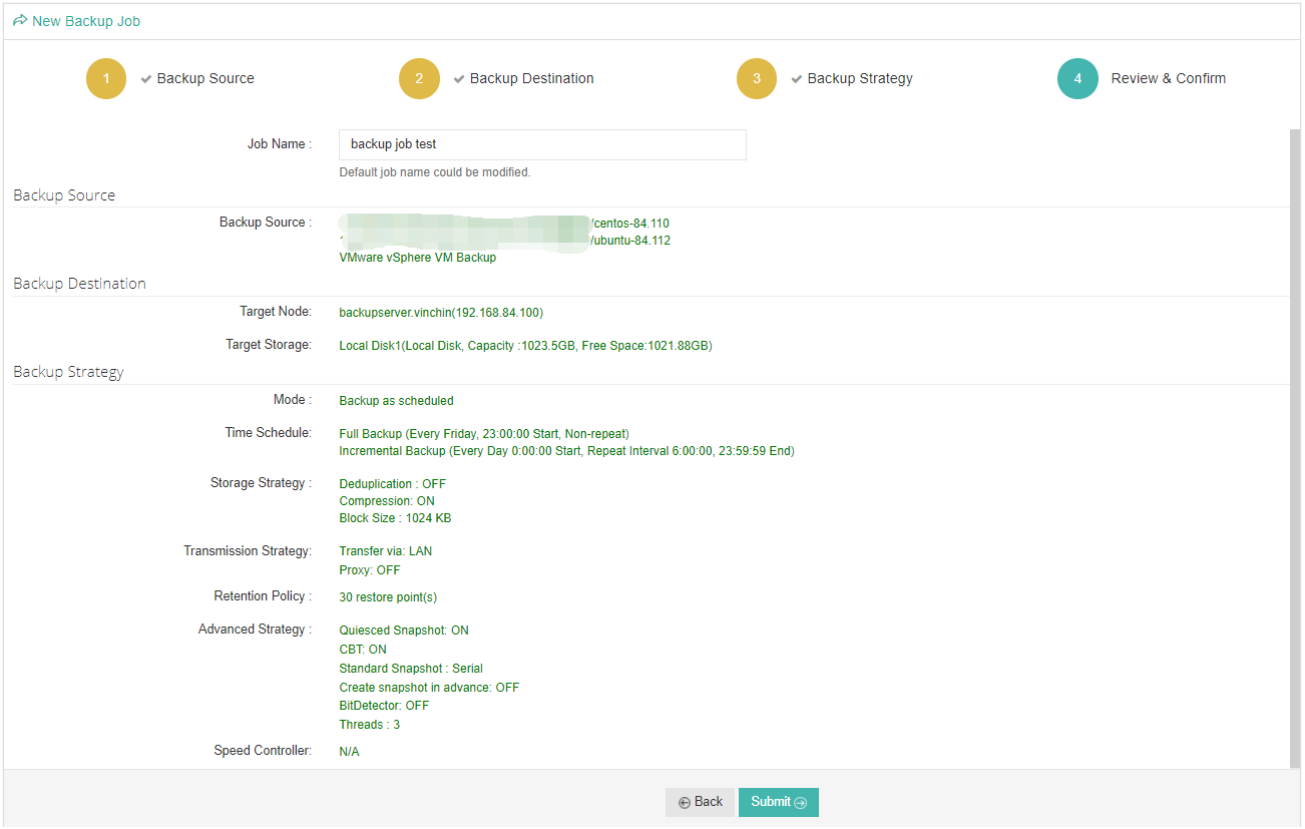
CBT (Changed Block Tracking) is now supported with VMware vSphere, Citrix XenServer (7.3 and newer) and XCP-

ng, it is a more advanced way to perform incremental backups than using SpeedKit or Ordinary mode.

Quiesced Snapshot is a technology to keep file systems or applications on the VM in a consistent state via application-awareness processing (e.g. VMware tools) before the VM snapshot is created. Applications on Windows OS are required to support Microsoft VSS. If failed to take quiesced snapshot, system will take standard snapshot.

Step 4: Review & Confirm

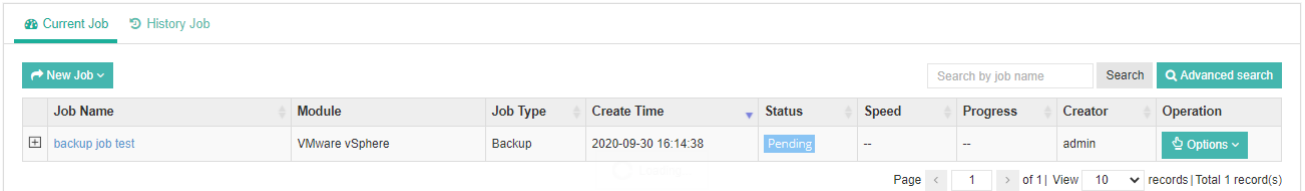
After completing the above-mentioned settings, you are able to review and confirm the settings in one screen.



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.

Backup Job Operations

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.

Restore

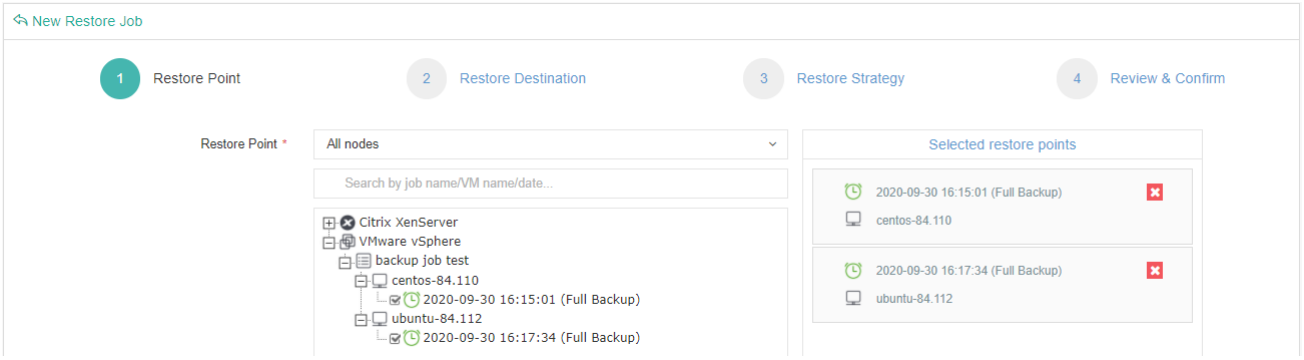
Create Restore Job

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.

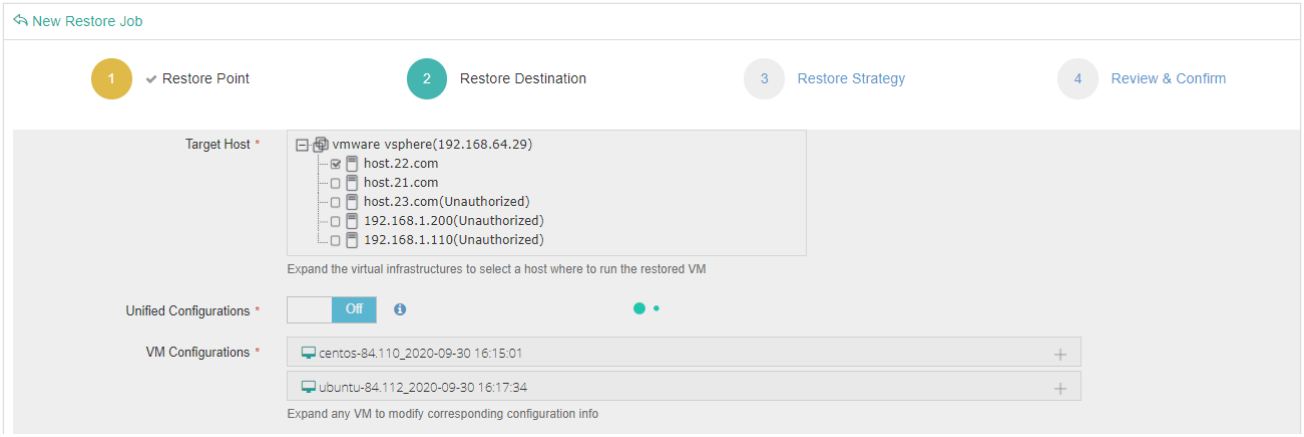
Select a target VM restore point under your virtual infrastructure which you want to restore. You can quickly find the target restore point by searching the job name, VM name or the data of the restore point.



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.

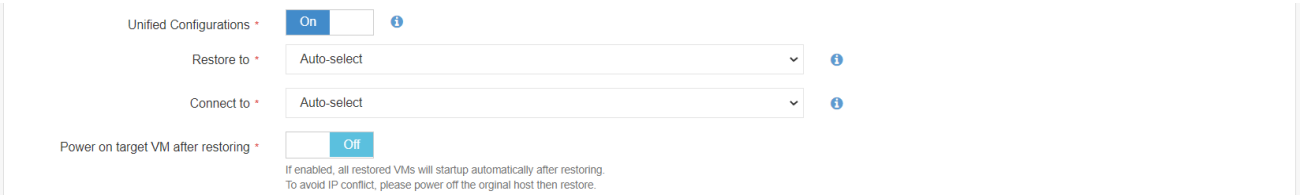
Note

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

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

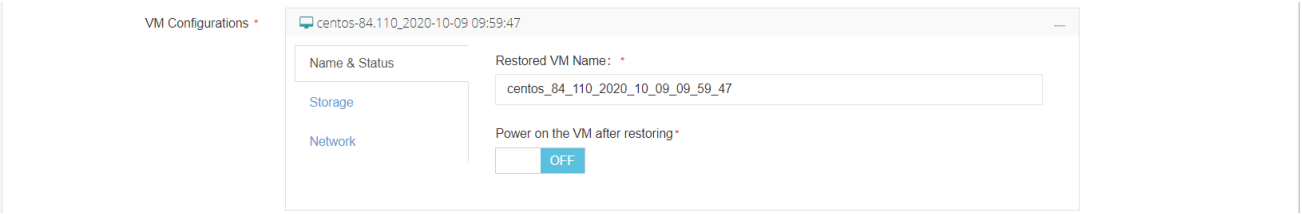
3. You can restore a VM to an unauthorized host.

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.



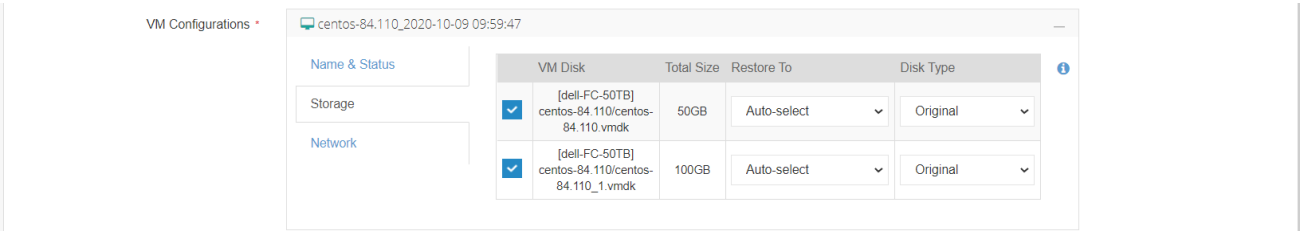
VM Configurations: Here you can modify the configurations of each VM, modifying the configurations of one VM will not affect the unified configurations of the other VMs.

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



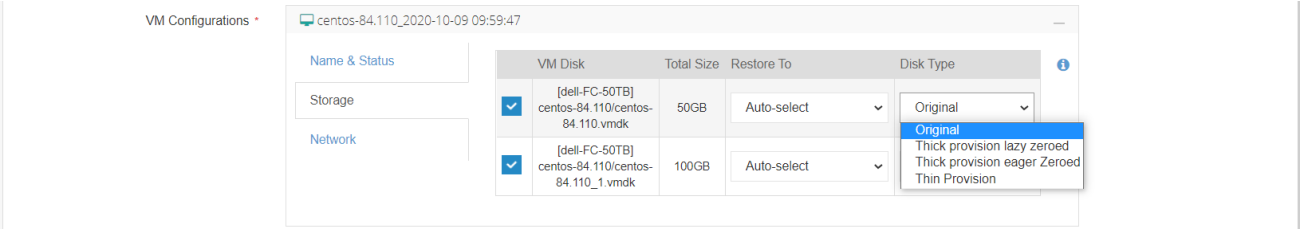
When renaming the VM, please do not use special characters. Any combination of letters, numbers and underscore characters are recommended.

Storage: When a virtual machine has multiple disks, you can choose target disk to restore without having to restore all the disks on the virtual machine.



If the target storage is set as **Auto-select**, Vinchin Backup Server will automatically choose the storage with most free space to restore this VM. If all the storages are out of free space, the restore job will fail, and system will remind insufficient space.

For VMware and Hyper-V, you can choose disk type: same as original, thick provision lazy zeroed, thick provision eager zeroed or thin provision.

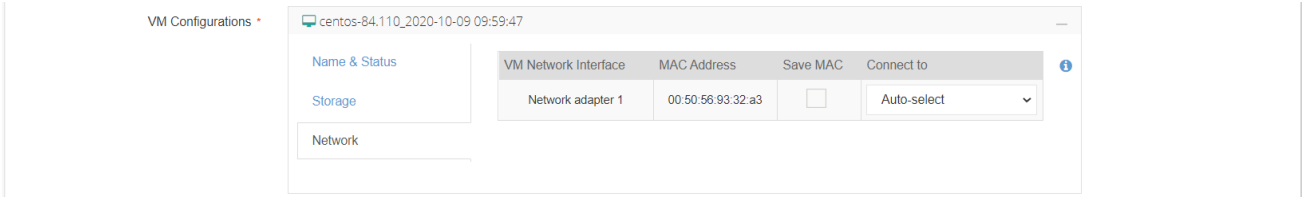


Note

If you don't restore the OS disk, there will be no operating system in the restored VM, you need to re-install a new

operating system or mount the data disk to another VM to be able to access this virtual disk.

Network: You can pre-set the MAC address of the VM to be restored and the network to be connected to.

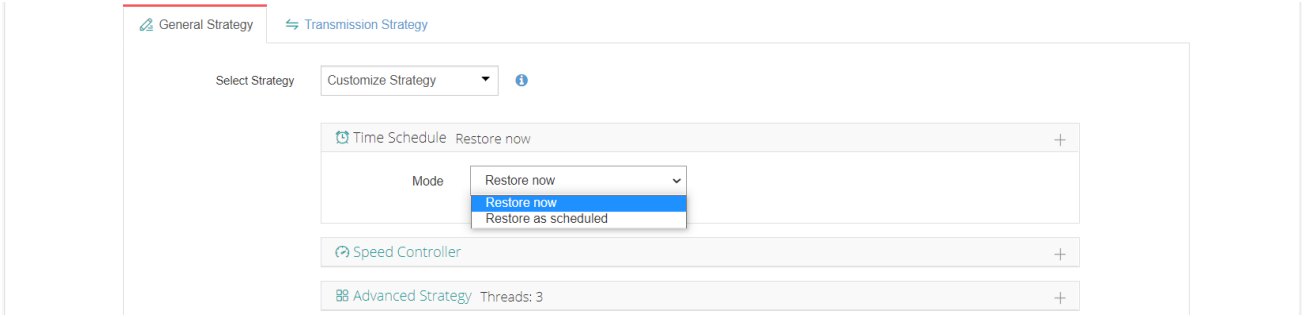


If there's already a VM with the same MAC address in the restored host or virtual infrastructure, the MAC address should not be reserved. If you want to save the MAC, you need to delete or power off the VM which has the same MAC in the same network.

Step 3: Restore Strategy

VM restore jobs can be configured with pre-set strategies, you can select a strategy template from the Select Strategy dropdown list if you had pre-configured any VM restore strategy templates. For more information of strategy templates please refer to Strategy.

For customized strategy, you can configure the VM restore job as restore now or restore as scheduled.



If you choose **Restore now**, 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.

Note

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 Restore now, as restoring too many VMs will occupy production resources.

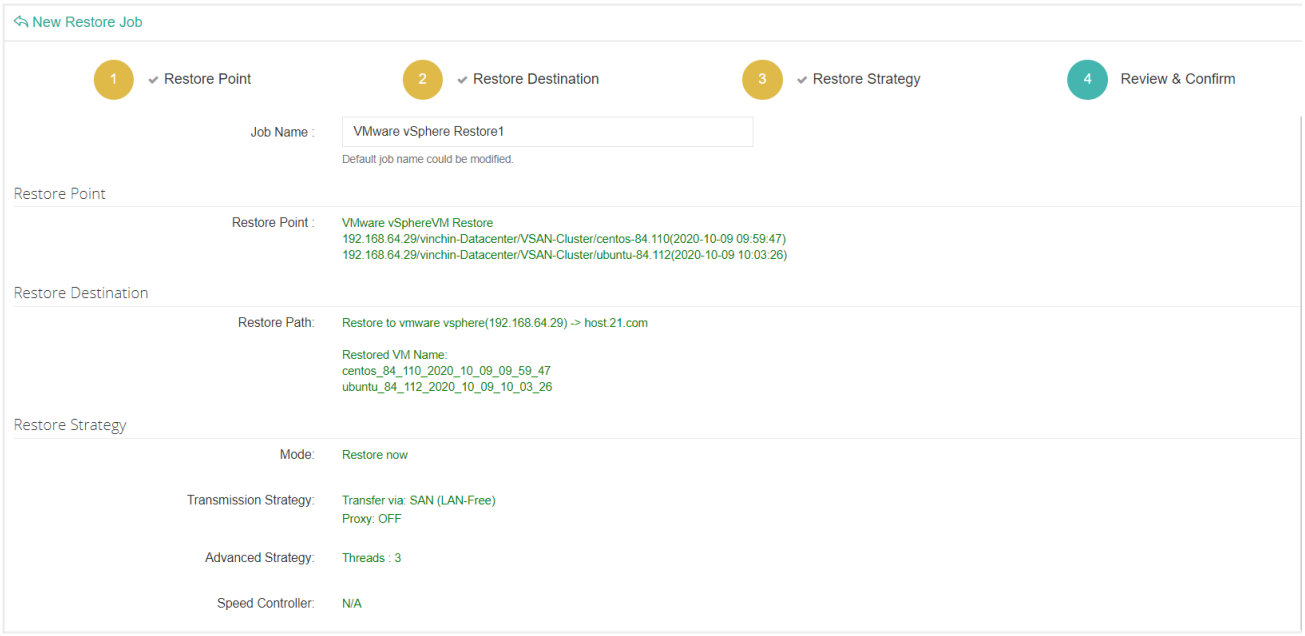
For **Speed Controller**, it works the same principle as the VM backup jobs.

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 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.

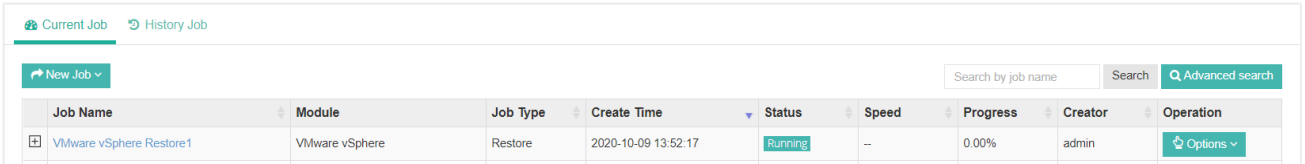


Note

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

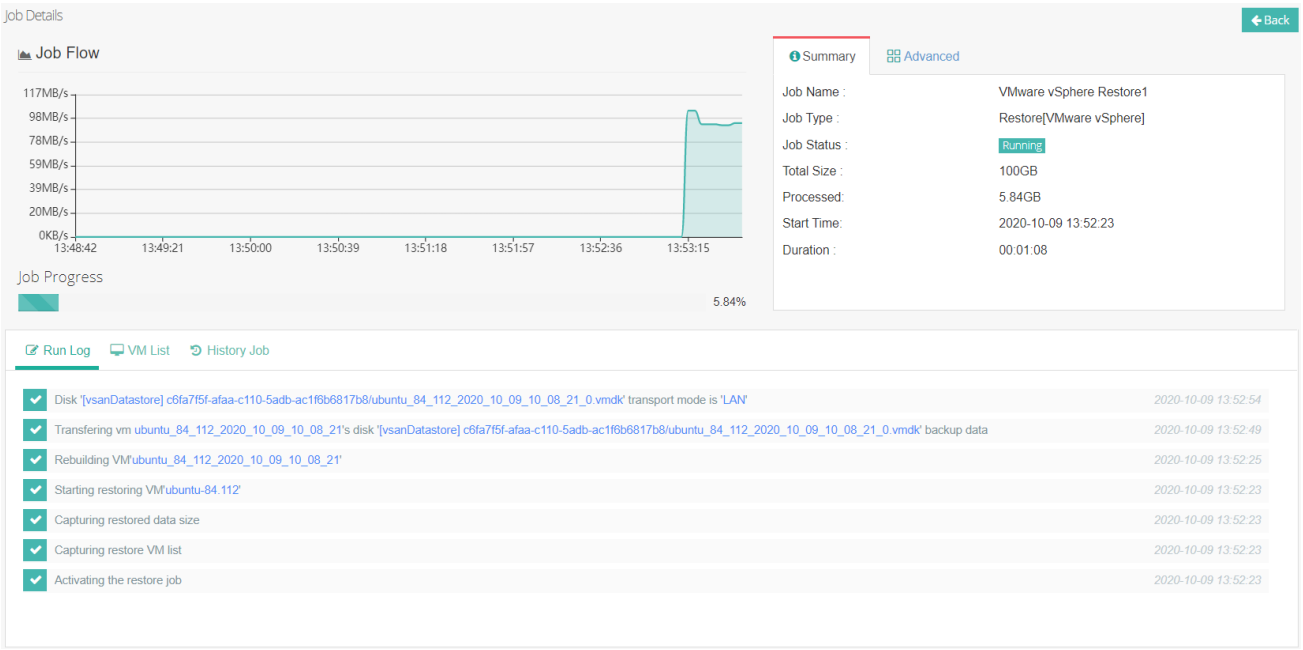
After creating a new restore job, you will be redirected to the **Monitor Center** > **Jobs** page, and you'll be able to see the VM restore job you created in the job list.



If the job is supposed to "restore now", 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.

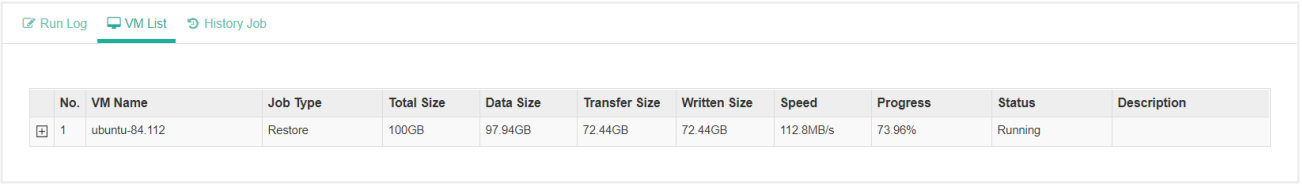
If you want to manually start the job, please click on **Options**, and then select **Start Job** to run it manually.

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: If you've set "Restore now" for this 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 Restore

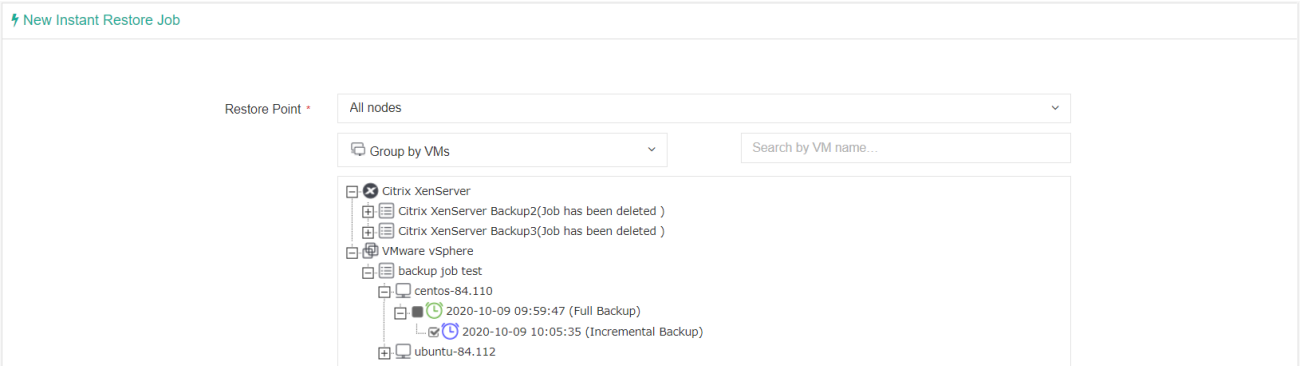
VM Instant Restore helps to recover a VM within 1 min, minimizes the downtime of critical businesses. It can be very helpful in emergency situations to directly start a VM from its backup data, without the need to transfer backup data back to production storage then resume the VM.

Note

Instant Restore is currently not supported with Microsoft Hyper-V and OpenStack in Vinchin Backup & Recovery v6.0.

Create Instant Restore Job

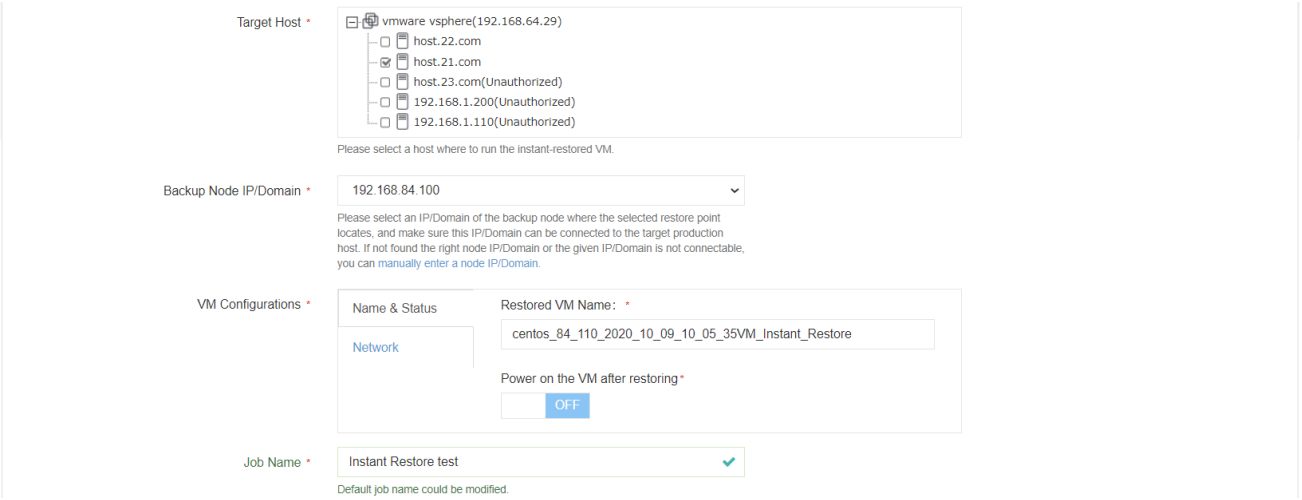
To create an Instant Restore job, please go to **VM Backup** > **Instant Restore** page, select a target VM restore point under your virtual infrastructure which you want to instantly recover. You can quickly find the target restore point by specifying backup node and selecting Group by VMs or Group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



Note

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

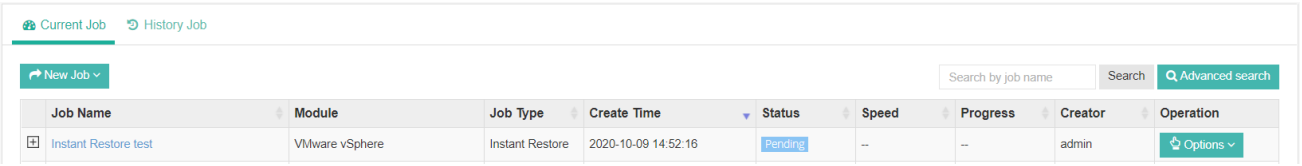
Select a host as the restore destination where you want to run the instant restored VM, and select the backup node IP/domain where the backup storage was mounted. You can also set the VM name, network info and whether to power on the VM after restoring.



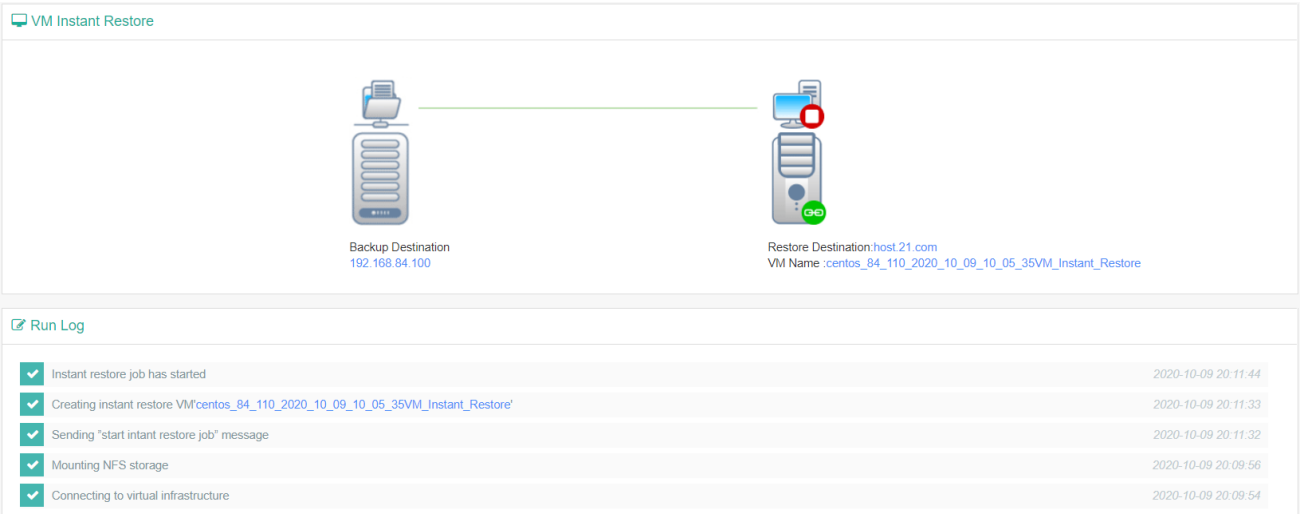
Once done, click on OK button to submit.

Instant Restore Job Operations

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.

Warning

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

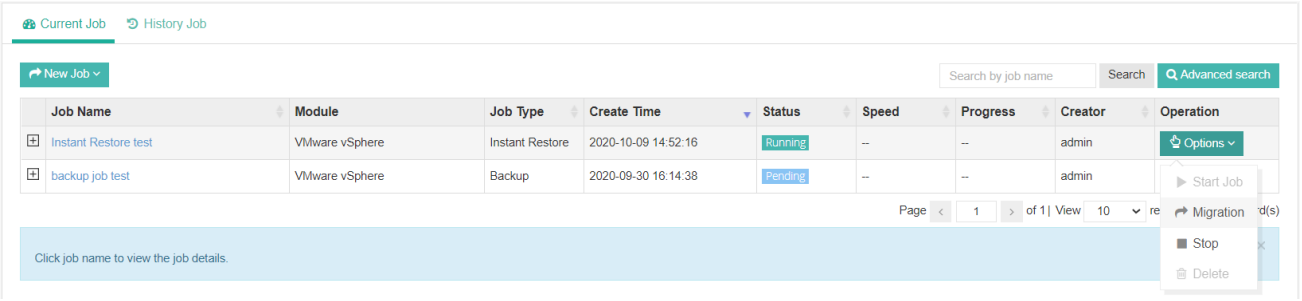
If you want to delete the instant restore job, you can go back to the current job list and click **Options** of the running instant restore job and then select **Stop**, after the job has been stopped, then click **Options** again and select **Delete**.

Warning

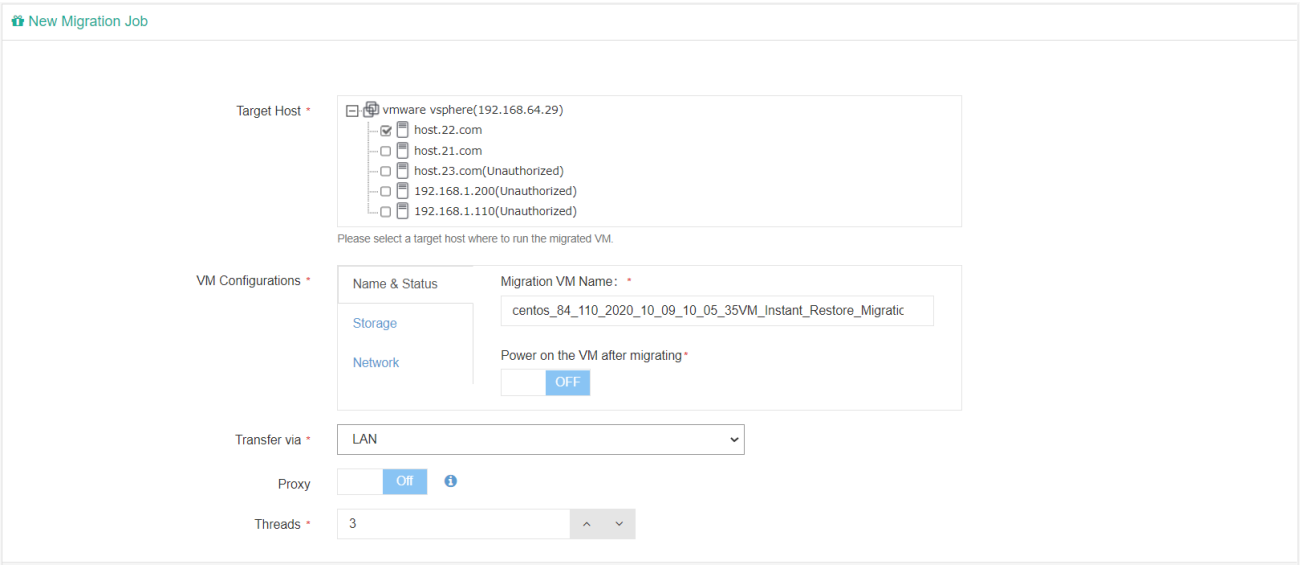
All the data of the instant restored VM is actually on Vinchin Backup Server/Node which is mounted to the selected host as NFS storage, if you delete the instant restore job, all the data of the restored VM will be deleted from the virtual platform host (including newly written data during the instant 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.

VM Migration

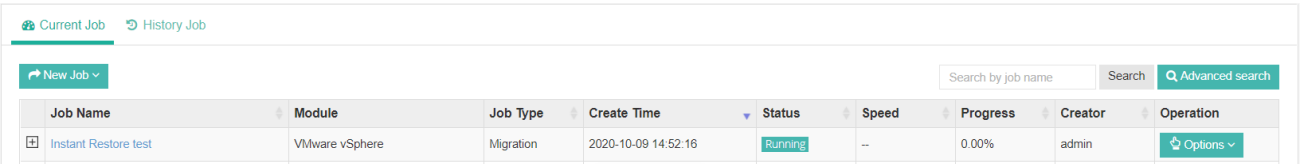
When performing instant restore job, the VM and newly written data can be migrated to the production storage via VMware vMotion or Vinchin live migration function without effecting the normal operation of your business. Select an instant restore job in running status, click on **Options** and then select **Migration**.



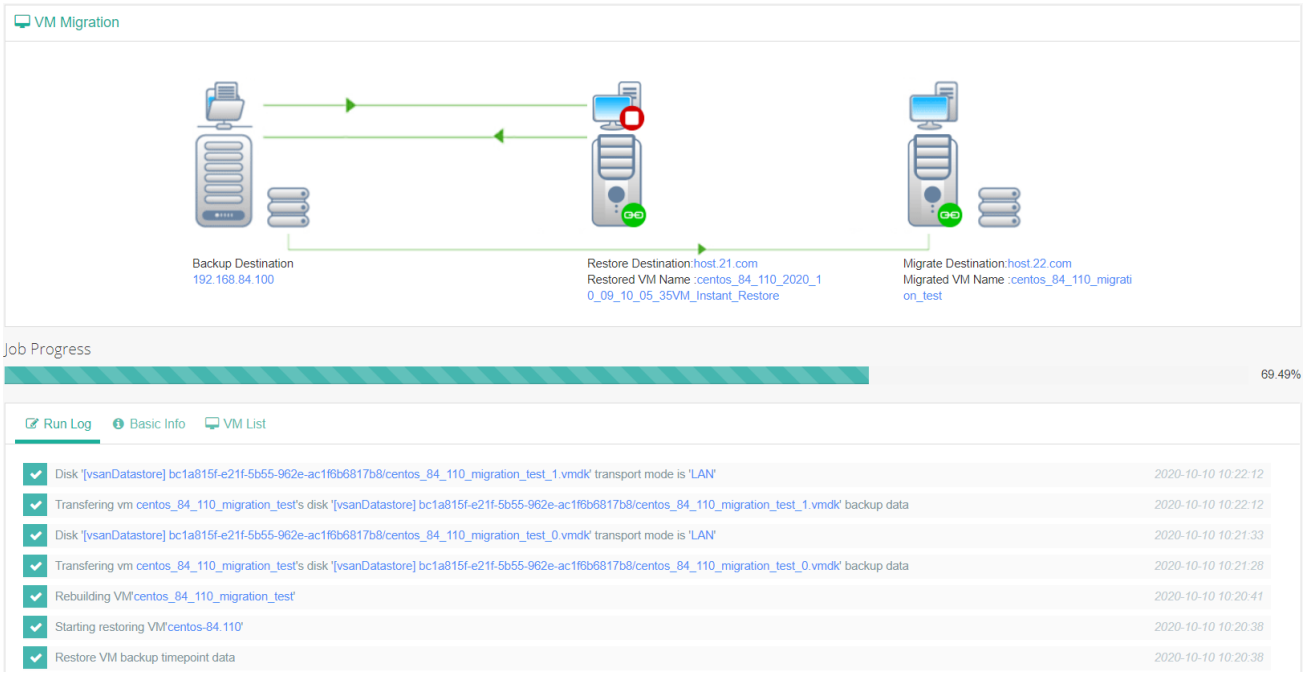
Select a host where to migrate the VM. Then you can rename the migrated VM and choose to whether power on it after migration, set storage, network configurations for the VM. You can also select transmission mode. For a detailed description of each transmission mode, please refer to Create Backup Job.



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.

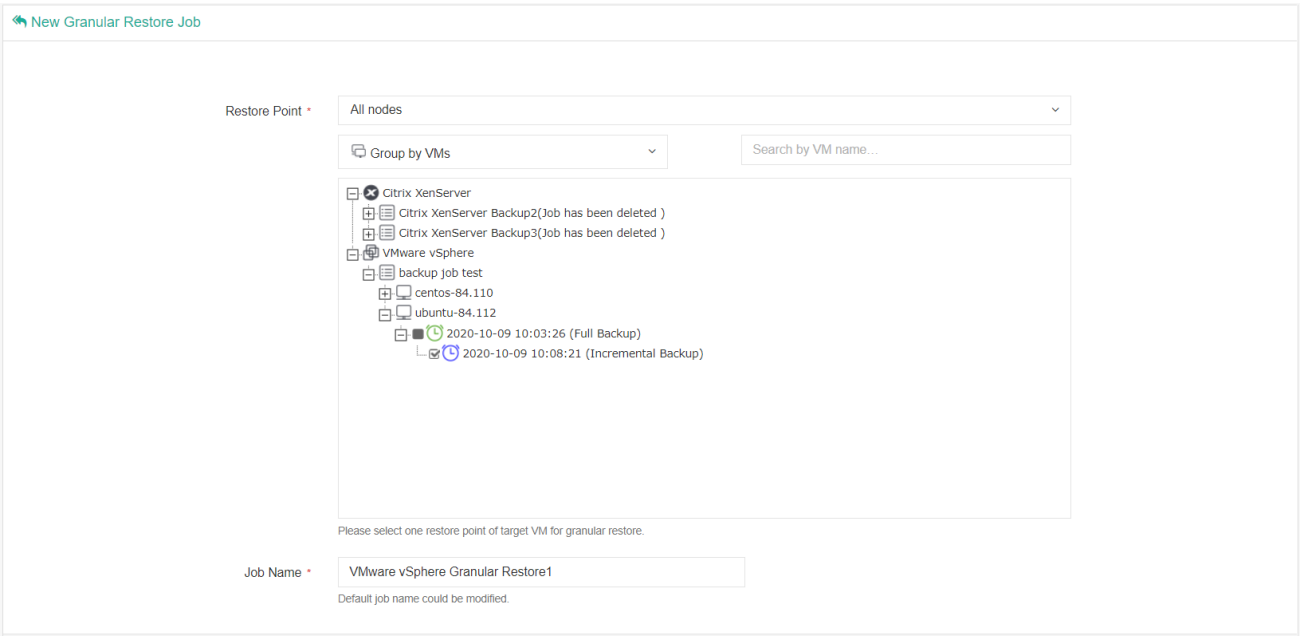
Warning

Do not power on the VM when it is being migrated, otherwise the VM migration will fail.

Granular Restore

Create Granular Restore Job

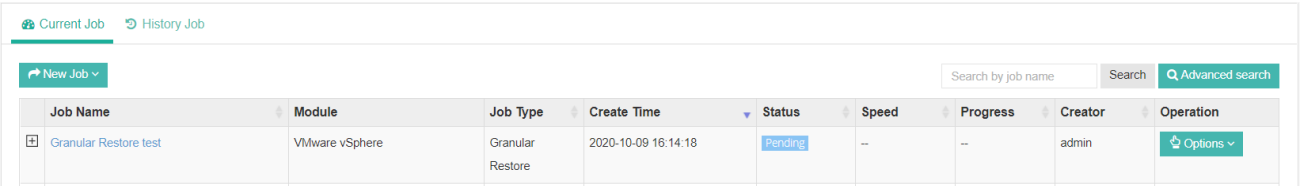
Granular Restore feature allows you to recover files or folders from the VM backup restore point, you don't have to restore the entire virtual machine for the purpose of recovering some files.
To create a granular restore job, please go to **VM Backup** > **Granular Restore** page, you will see all the 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 backup, an incremental backup or a differential restore point.
When done selecting the restore point, you may rename the granular recovery job if necessary, then click on OK button to submit.

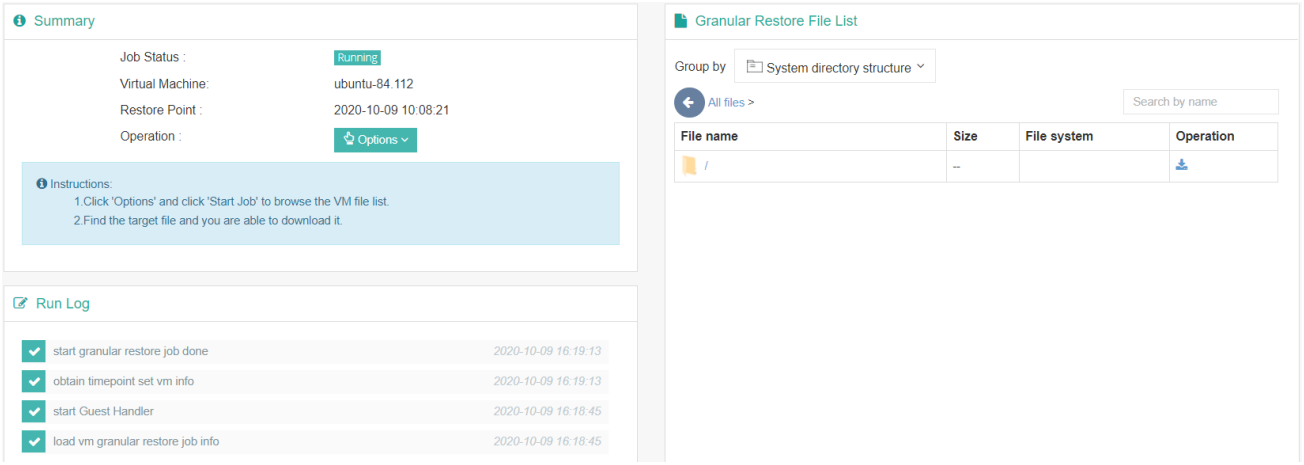
Granular Restore Job Operations

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.



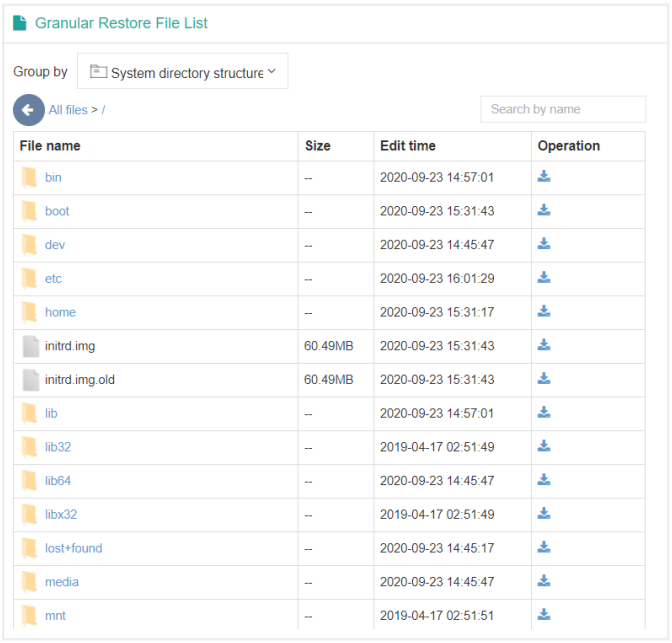
To run the granular restore job, please click on **Options**, then select **Start Job**. And the job status will change in to preparing. The preparation process will take several minutes depending on the VM size and the performance of Vinchin Backup Server hardware. After this, the status will change 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.

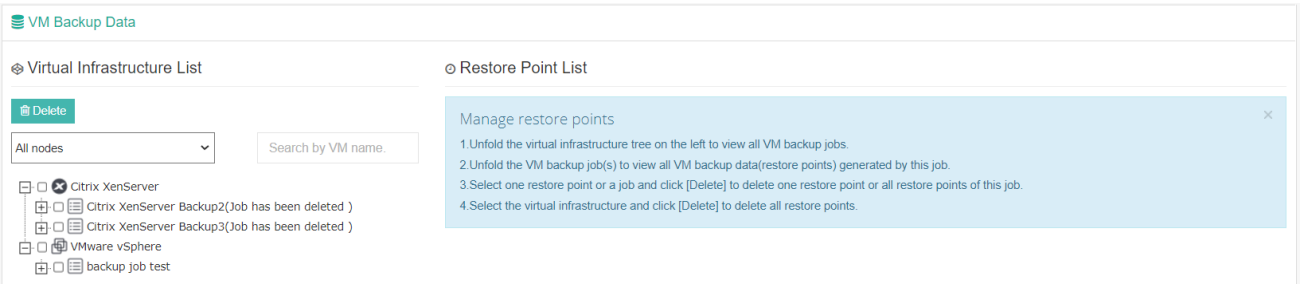
```
tar -zxvf foldername.tar.gz
```

Note

Once you have 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.

Backup Data

To manage all the backup data, please go to **VM 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, and click on the **Delete** button.

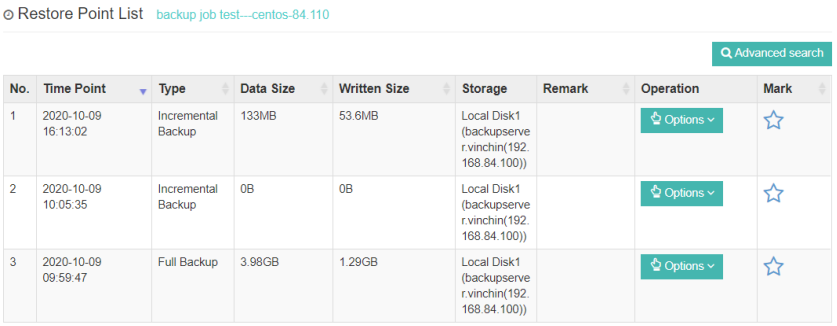
If the restore point(s) is in use by a VM (instant) restore job, the restore point(s) cannot be deleted, you'll have to delete the restore job then to delete the restore point(s).

When deleting full backup restore point, corresponding incremental backup or differential backup restore point will be automatically deleted with the full backup restore point.

Warning

Once a restore point had been deleted, it is not recoverable. Please think twice before deletion.

For more options of the restore points, please click on a VM, all restore points of this VM will be listed on the right side table.



Click on **Options**, you will be able to add remarks or delete the restore point.

By clicking on the ☆ icon, you are able to mark a restore point, the marked restore point(s) will be kept permanently, and even the retention policy will not delete the marked restore point(s). If the marked restore point is an incremental backup restore point, the retention policy will only cause Vinchin Backup Server merge the last full backup of this incremental backup and the other incremental backups between them to a new full backup restore point, and this merged restore point will be kept permanently.

For VMware, you can mark full backup, incremental backup and differential backup restore point. For other virtual platforms, only full backup restore point can be marked.

File Backup

Install File Backup Agent

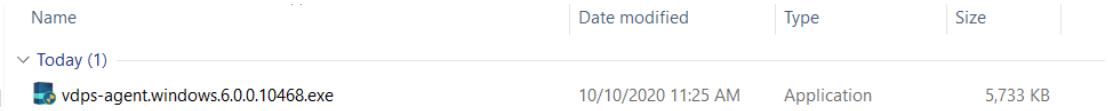
Windows

The supported Windows systems including Windows XP, 7, 8 and 10, Windows Server 2003, 2008, 2012, 2016 and 2019.

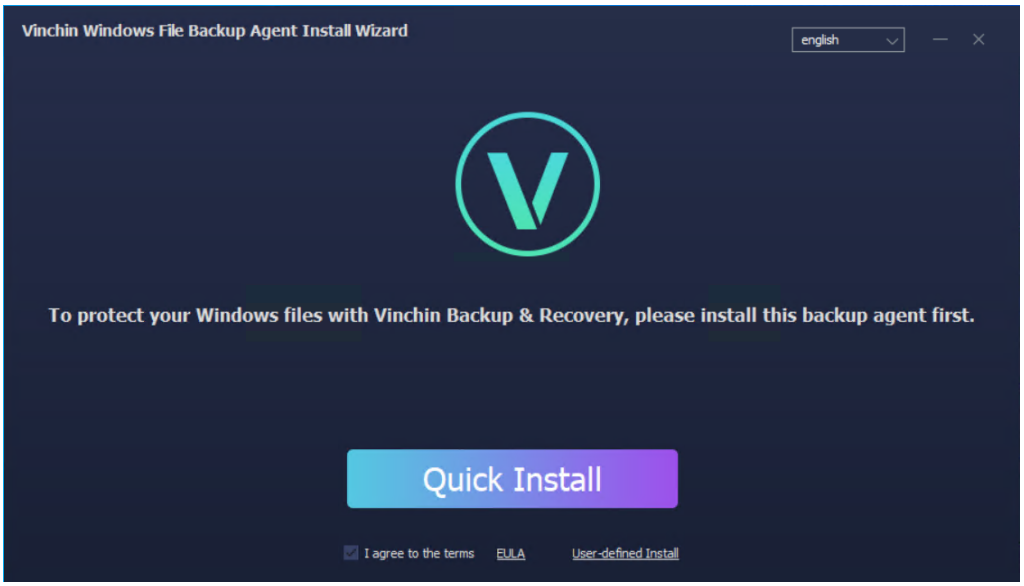
To install file backup plugin, you can open Vinchin Backup Server web console from the target Windows system directly, on the login screen, click on **Download Backup Plugin** to go to the backup plugin download page.

In the Type dropdown list, please select **File Backup Plugin**. In the **Filesystem** dropdown list, please select Windows. Then click on **Download** button to download.

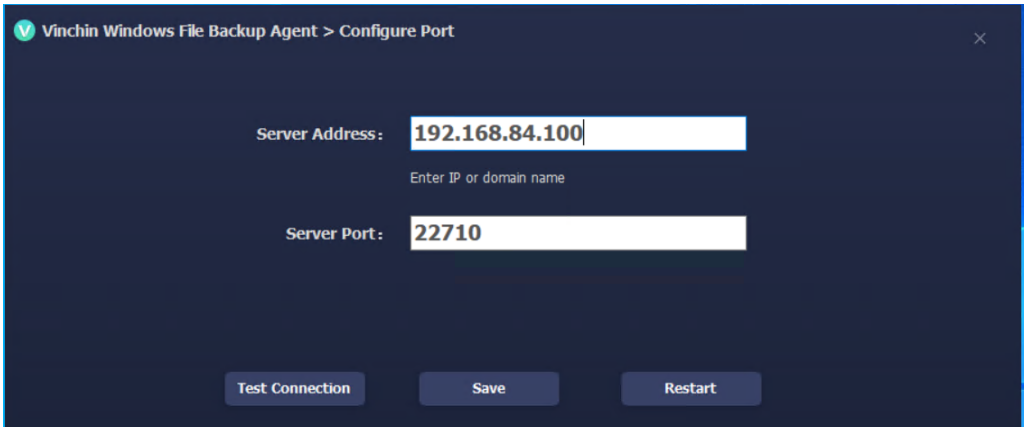
The downloaded file backup plugin should be an executable exe file.



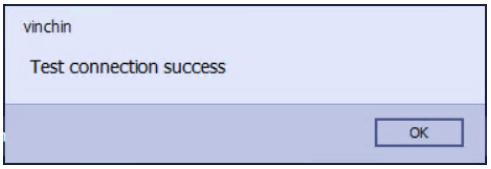
To install the backup plugin, please right click on it and select **Run as administrator** to install the backup plugin with administrator permissions.



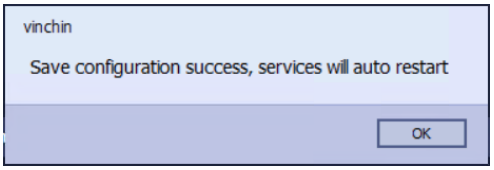
Click on **Quick Install** button to start the installation, the installation will take a few seconds. Once installation completed, please find the backup plugin icon from the taskbar and right click on the icon, and then select **Agent Configure**.



In the **Server Address** field, please enter the IP address of Vinchin Backup Server. After this you can click on Test Connection button to test if the file backup plugin can communicate with Vinchin Backup Server.



If you get **Test connection success**, then please click on **Save** button to save the settings.



Click on OK to restart the file backup plugin services then you have successfully installed and configured the file backup plugin on the Windows system.

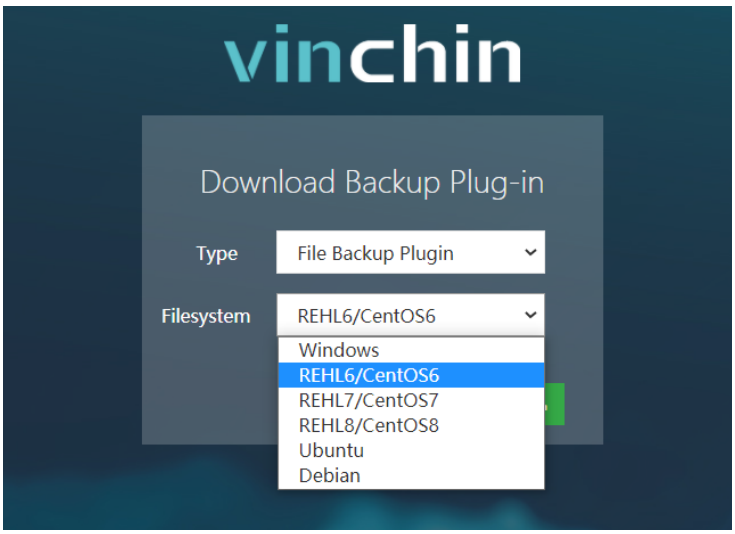
Note

Please keep the file backup plugin running on the Windows system, otherwise file backup or restore will fail.

Linux

The supported Linux distributions and versions including RHEL 6 to 8, CentOS 6 to 8, Ubuntu 12 to 20, Debian 7 to 10.

Please go to login screen and click on **Download backup plugin** to go to the file backup plugin download page.



Select the corresponding Linux distribution and version then click on the Download button to download the file backup plugin.

The downloaded backup plugin should be a .tar.gz package. Please upload the downloaded file to the Linux system, to upload from Windows desktop, you can use WinSCP or PSCP, or any other methods that you are familiar with.

After uploading, please enter the Linux system command line interface and use the below command to decompress the package.

```
tar -zxvf vinchin-file-backup-agent-xxx.tar.gz
```

Where 'xxx' should be the actual file name of the file backup plugin package.

Enter the file backup plugin package folder.

```
cd vinchin-file-backup-agent-xxx
```

To install the backup plugin, run below command.

```
./file_backup_agent_install
```

Use below command to uninstall (once uninstalled, file backup and restore will no longer work on this Linux host).

```
./file_backup_agent_uninstall
```

After installing the file backup plugin, please modify the conf file use below command.

```
vim /etc/backup_system/rt_client.conf.xml
```

Specify Vinchin Backup Server IP address in the row '<server_ip>0.0.0.0</server_ip>' and replace the address 0.0.0.0 with the actual IP address of your Vinchin Backup Server. In this example, the server IP is 192.168.84.100.

```
<?xml version="1.0" encoding="UTF-8" ?>
<router-client-conf>
        <install_path>/opt/vinchin/</install_path>
        <server_ip>192.168.84.100</server_ip>
        <server_port>22710</server_port>
```

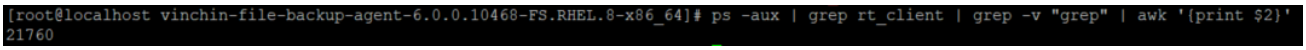
```
        <listen_ip>0.0.0.0</listen_ip>
        <listen_port>22810</listen_port>
        <client_key_name>client.key</client_key_name>
        <log_dir>/var/log/vinchin/</log_dir>
        <log_num>60</log_num>
        <log_level>debug</log_level>
</router-client-conf>
```

When done, save the modifications.

Next, the rt_client process needs to be terminated, first please find its PID use below command.

```
ps -aux | grep rt_client | grep -v "grep" | awk '{print $2}'
```

The output should be a number and it's the PID of the rt_client process.



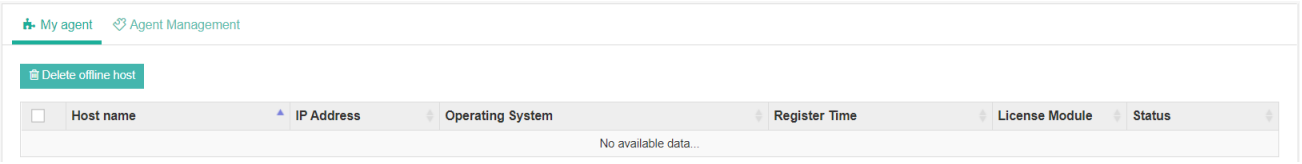
In this example, the PID is 21760, please terminate the process using the command below.

```
kill -9 21760
```

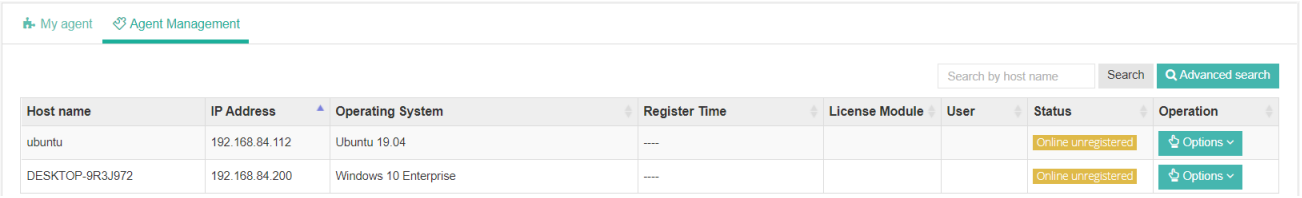
After terminating the rt_client process, it will be automatically restarted by the file backup plugin daemon process, and the modification of the server IP should be effective now.

Register File Backup Agent

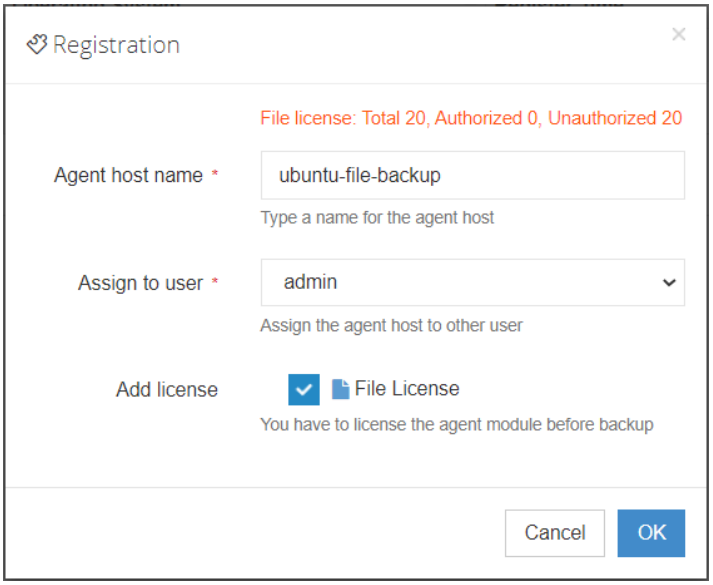
After the installation and configuration of the backup plugin on the target host(s), please open Vinchin Backup Server web console and go to **File Backup** > **Backup Agent** page.



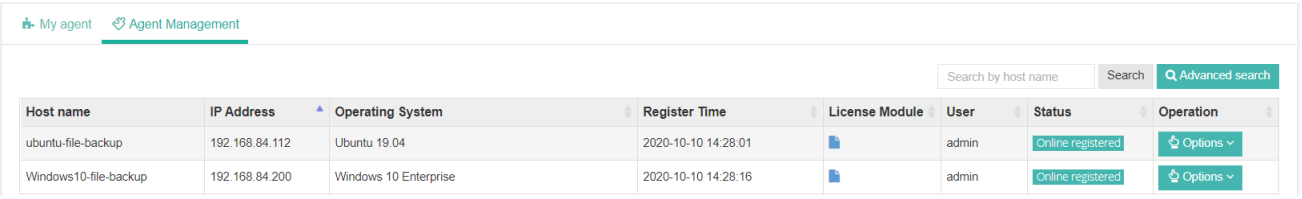
Click on the **Agent Management** tab to register those hosts to Vinchin Backup Server.



For both Windows and Linux hosts, click on **Options** and then select **Register** to register them to Vinchin Backup Server.



In the popup dialog, you can customized the agent host name, assign the host to specific Vinchin Backup Server user, and ensure the File License checkbox is selected and then click on OK to register this host. Once registered, the host status will change to Online registered status, now you can backup files of the register host.



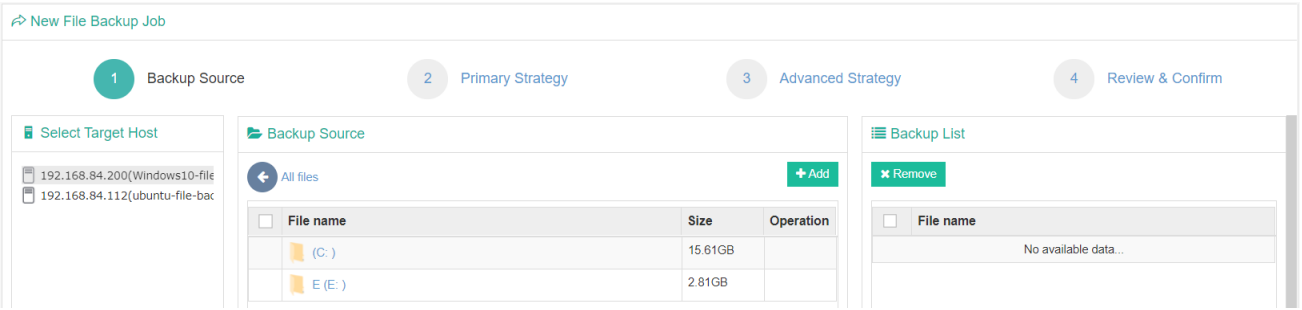
File Backup

Create File Backup Job

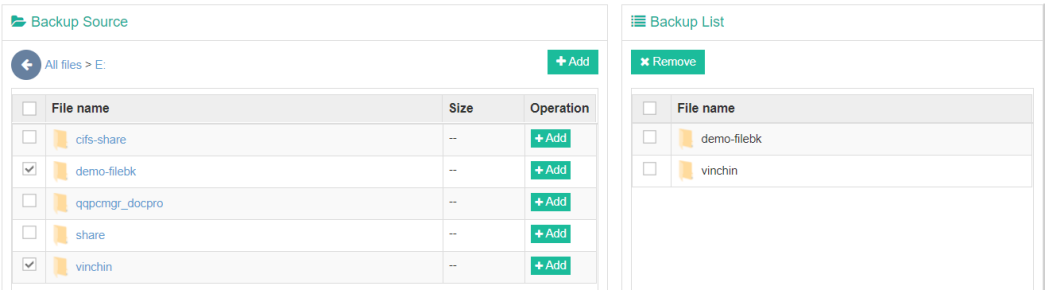
To create file backup jobs, please go to **File Backup** > **Backup** page. There are 4 steps to create a file backup job.

Step 1: Backup Source

First you need to select a target host from the **Select Target Host** column for this backup job. Each file backup job can only have one host selected.



After selecting the target host, please add the files or folders you want to back up from the Backup Source column. The files/folders could be added by clicking on the Add button corresponding to each file/folder, or you can use the checkbox to select the desired files/folders then use the Add button on the top right of the Backup Source column. The selected files/folders will be listed in the Backup List column.



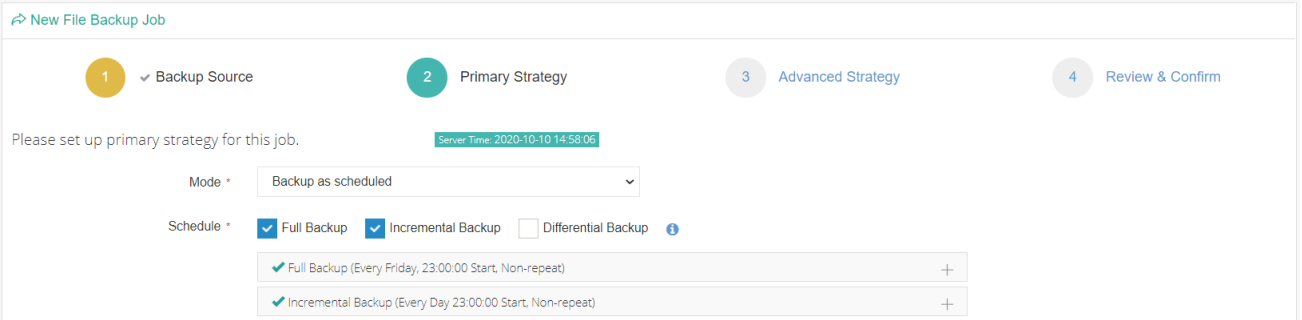
After selecting the files/folders, please click on **Next** to continue.

Note

If you have already selected a parent folder, then the files or subfolders will not be able to be selected, and it's also unnecessary to select files/folders inside the parent folder.

Step 2: Primary Strategy

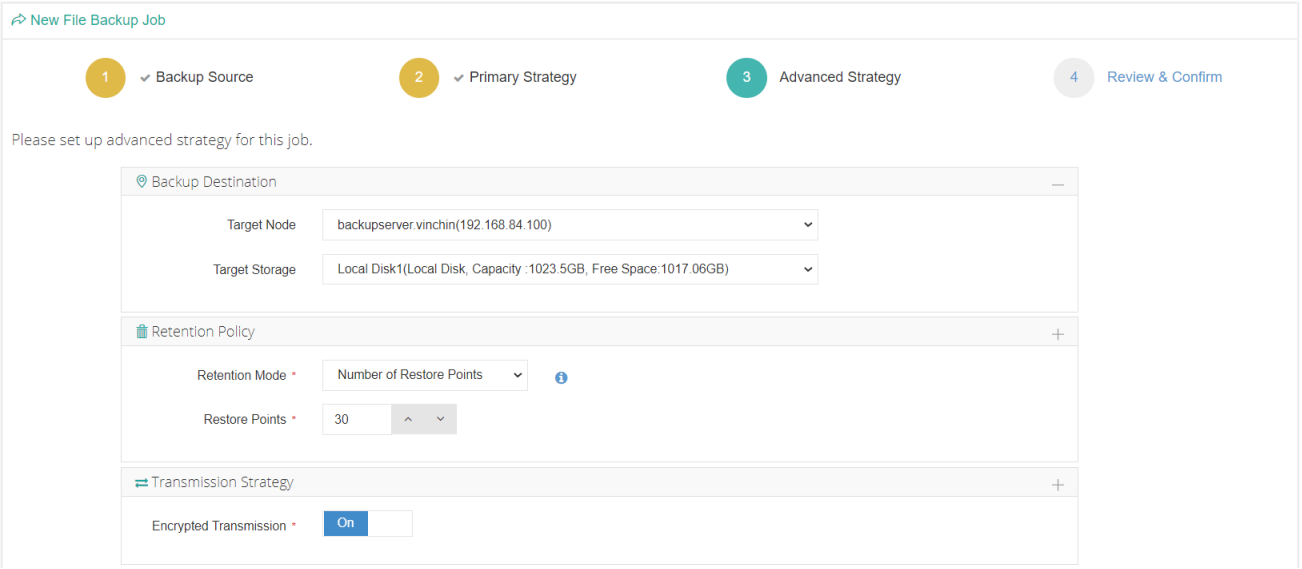
For the backup mode, you could choose between **Backup as scheduled** and **Once-off Backup**, the principle of these backup modes are similar with VM backup.



Please set the backup mode and backup schedule as per your actual demands, when done please click on **Next** to continue.

Step 3: Advanced Strategy

Advanced strategy allows you to select the backup storage for file backup, setup the retention policy and the transmission strategy. These settings are also similar with VM backup.

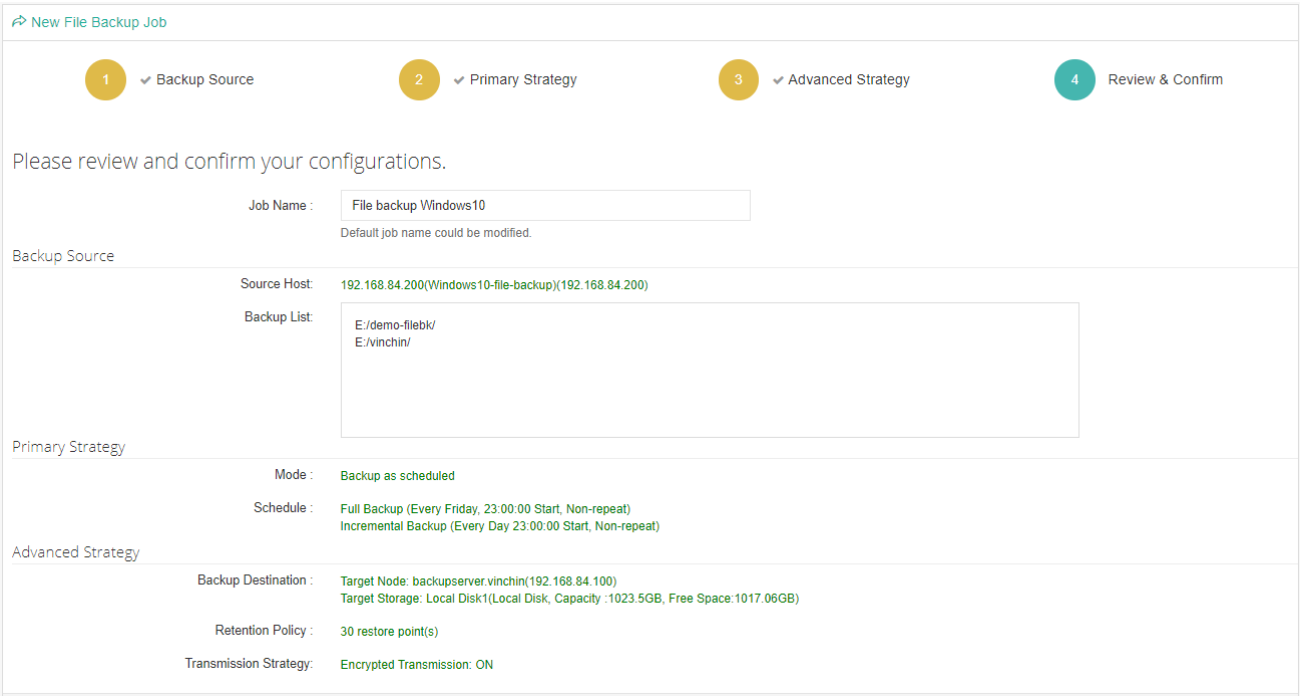


If you have chosen once-off backup, then there's no need to configure the retention policy, as there will only be one restore point for this file backup job.

When done the advanced strategy settings, please click on **Next** to continue.

Step 4: Review & Confirm

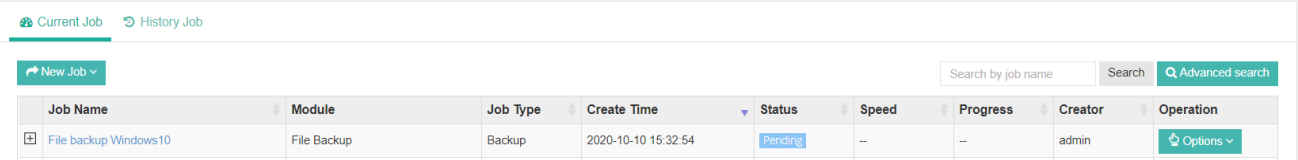
After completing the above mentioned settings, you are able to review and confirm the file backup job settings in one screen.



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

File Backup Job Operations

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



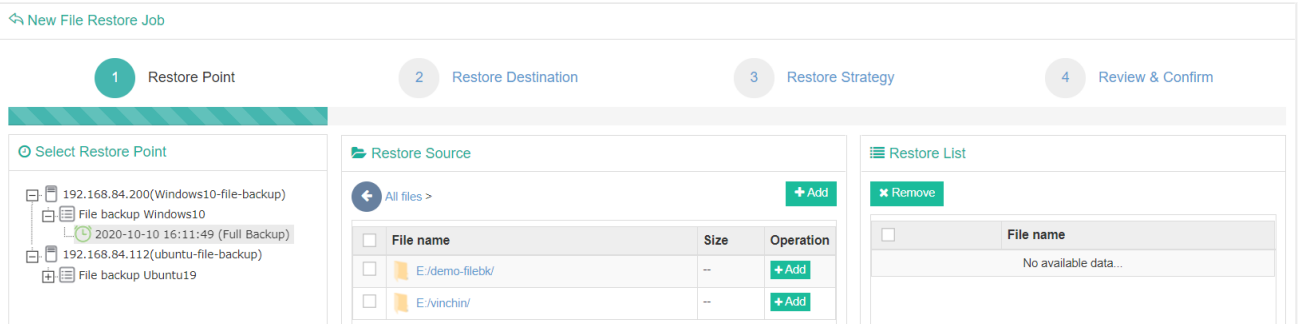
The newly created file backup job will be in pending status, the operations which can be done to the file backup job is similar with the VM backup jobs, you can start, stop, edit or delete the job from the current job list.

File Restore

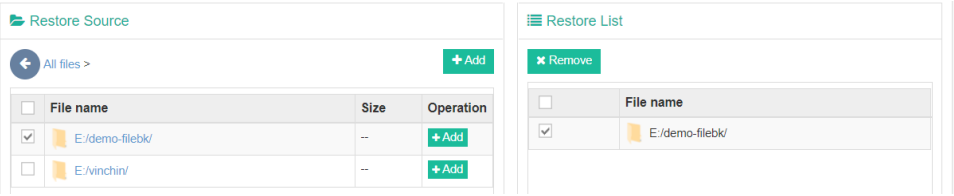
To restore files from file backup restore points, please go to **File Backup** > **Restore** page. There are 4 steps to restore files from the file backup restore points.

Step 1: Restore Point

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



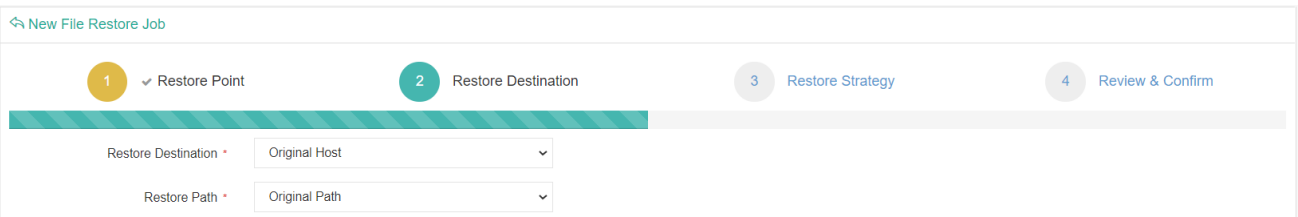
Then select the desired files/folders from the **Restore Source** column and add them to the **Restore List** column.



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

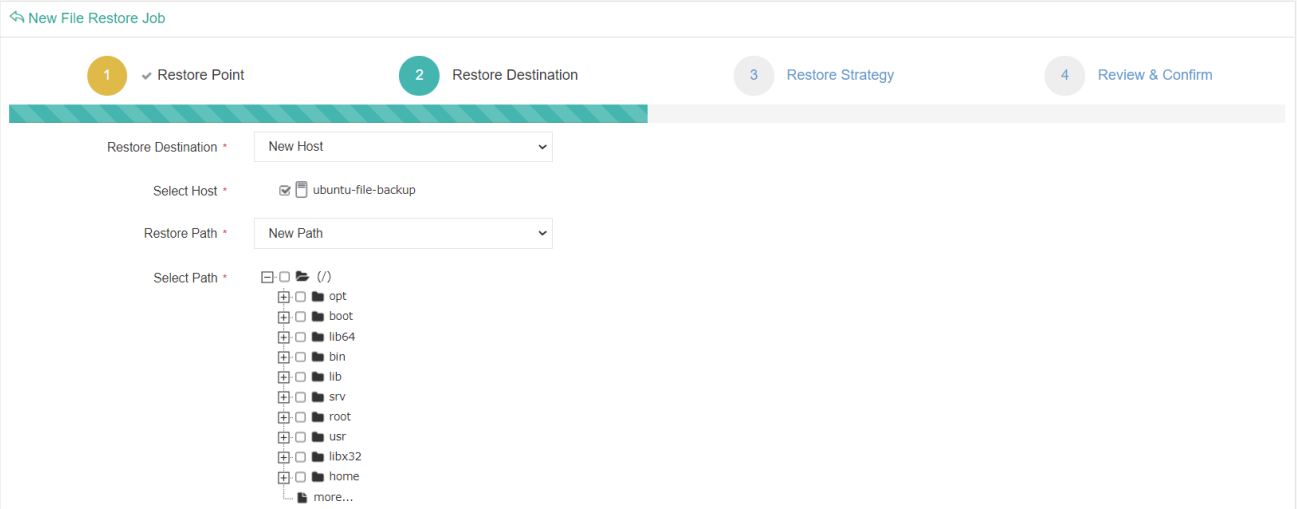
Step 2: Restore Destination

This step, you need to specify the destination for the selected files/folders to be restored to.



The default settings are to restore the files/folders to the original host and the original path. If so, please click on **Next** to continue.

If you want to restore the files/folders to another host or a new path, please select the desired host or the desired path then continue.

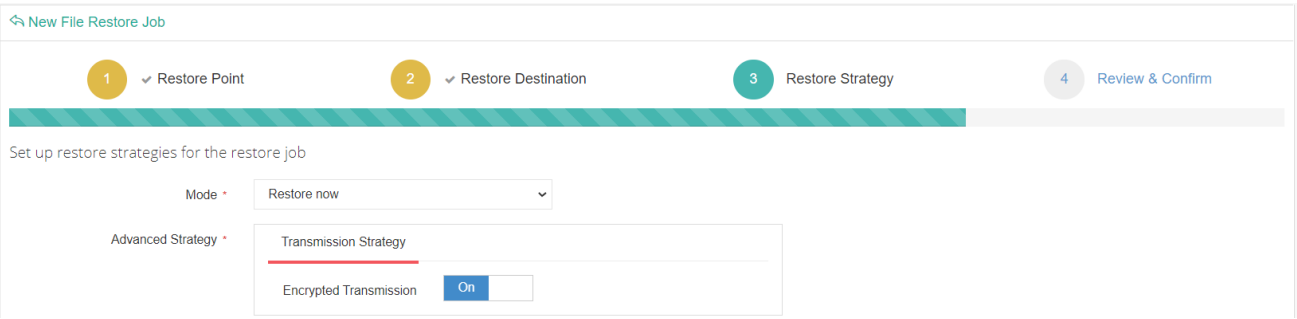


Note

The files/folders can be only restored to the hosts that have been registered to Vinchin Backup Server.

Step 3: Restore Strategy

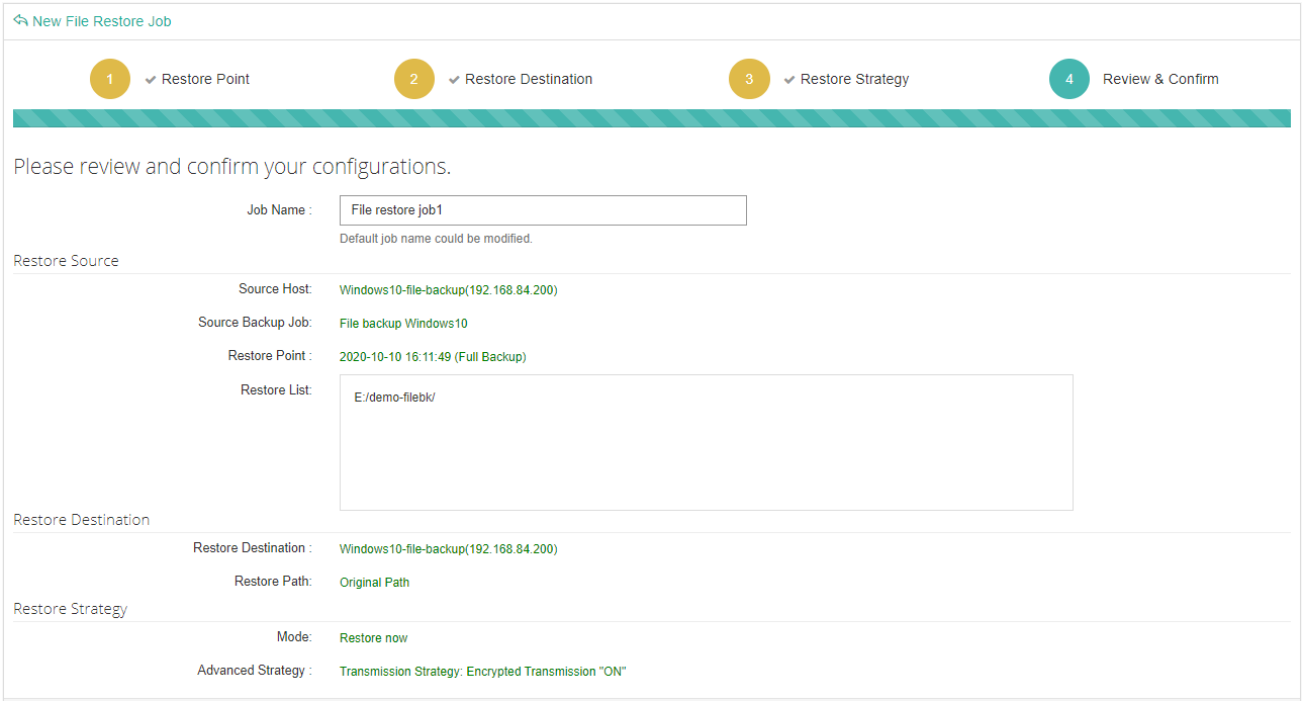
The restore mode of files/folders can only be **Restore now**, you can choose to enable **Encrypted Transmission** for data safety.



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.



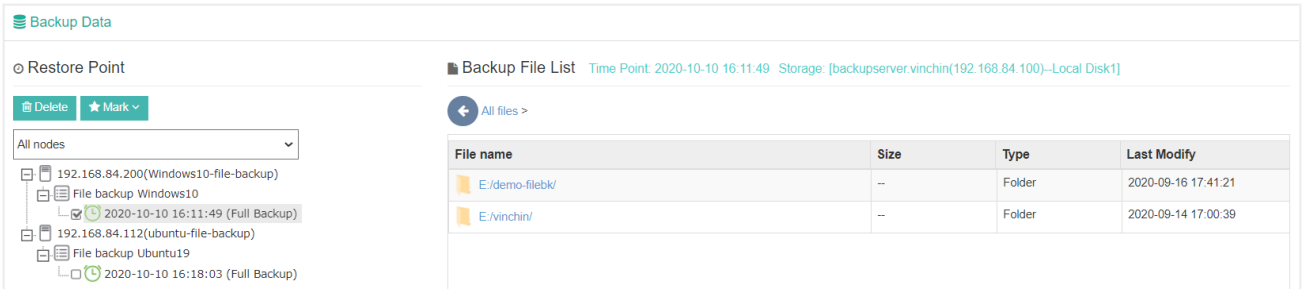
Once the job has been created, you'll be redirected to the **Monitor Center** > **Jobs** page.

As the 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 host and the selected path.

File Backup Data

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



By selecting a host and a file backup job, and then a backup restore point, you are able to browse the backup data of the restore point.

The file backup restore points are similar as the VM backup restore points, you can delete the restore points here and can also mark the restore points to reserve the marked restore points permanently.

Backup Copy

Backup Copy can be used to make one more copy of the VM backup data to an on-site backup copy storage or an off-site backup copy storage to keep the VM backup data safe from any site disasters.

Note

1. *To create backup copy jobs, a backup copy storage needs to be added, for more details of adding backup copy storages please refer to Add Storages.*
2. *To run a backup copy job, a VM backup job should be completed at first place.*
3. *Backup Copy only works with VM backup data but not the file backup data.*

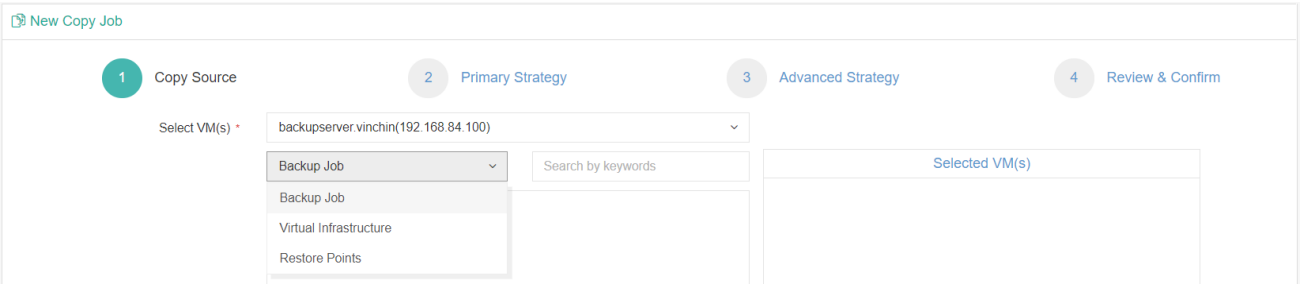
Backup Copy

Create Backup Copy Job

To create a backup copy job, please go to **Backup Copy** > **Copy** page, then follow the below steps to create the backup copy job.

Step 1: Copy Source

To select the backup copy 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.

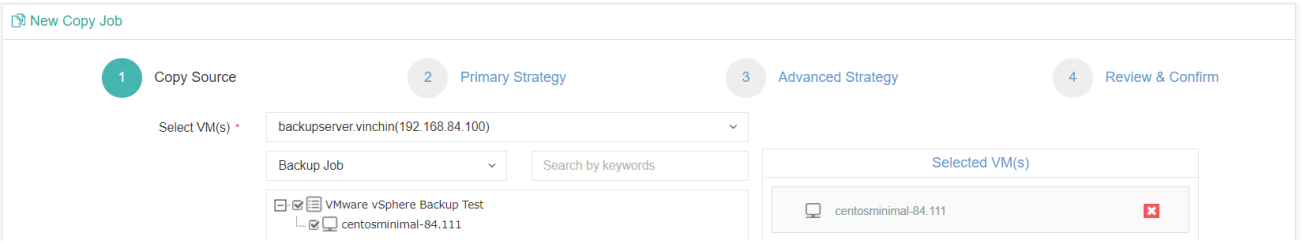


If you select Backup Job, backup jobs will be listed, by expanding the backup job you can select the copy source as per the VMs included in the backup job.

If you select Virtual Infrastructure, the virtual infrastructures will be listed and you should 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.



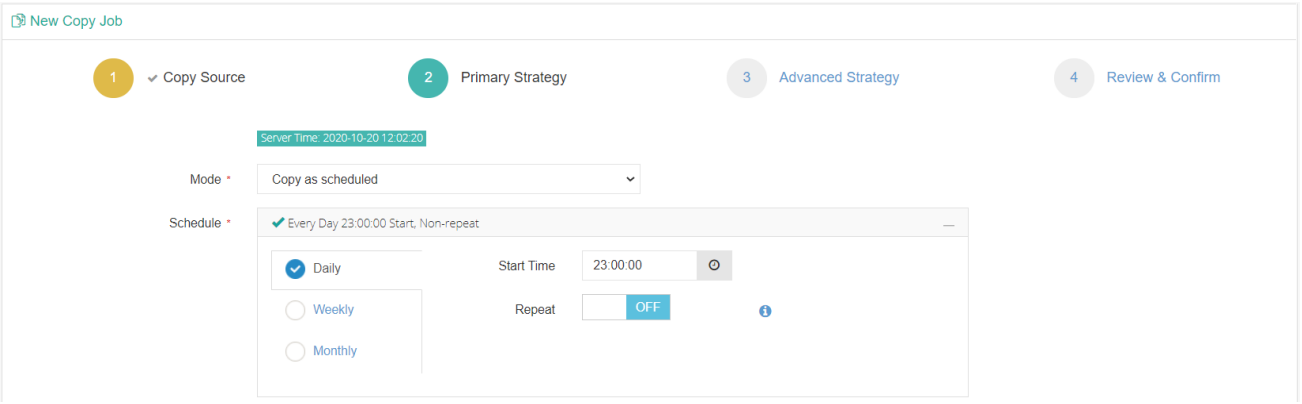
Once the copy source is selected, please click on **Next** button to continue.

Note

If the backup 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).

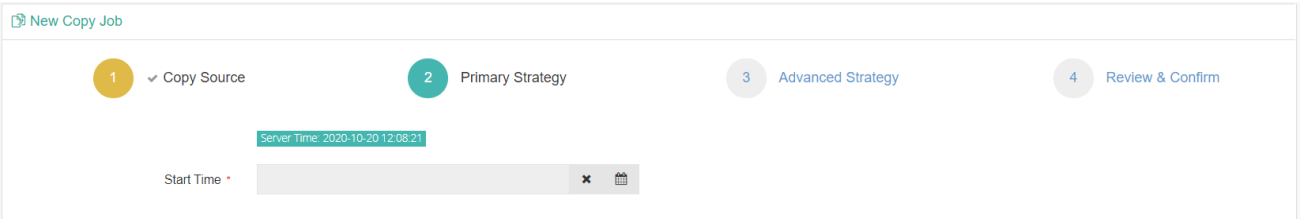
Step 2: Primary Strategy

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.

Once-off copy can be used to copy the backup data for only once, when the copy source is selected with restore points, the backup copy mode will be once-off copy by default. And you can only set an individual running time point for the backup copy job.



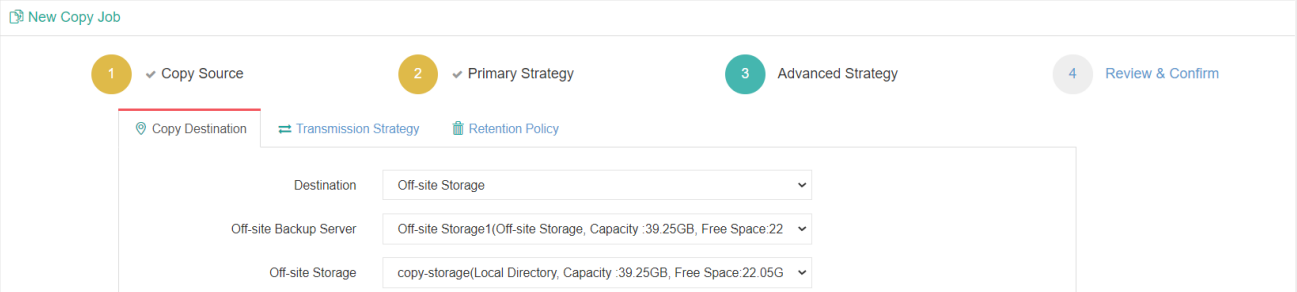
After done the primary strategy settings, click on the **Next** button to continue.

Step3: Advanced Strategy

➢ Copy Destination

Backup 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 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.



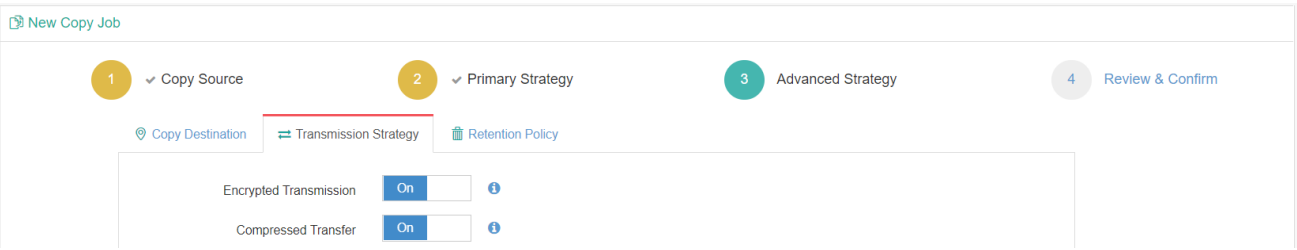
In the Destination field, Off-site Storage should be selected.

In the Off-site Backup Server field, select the target remote backup server.

Once the remote 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.

➢ Transmission Strategy

Transmission strategy including Encrypted Transmission and Compressed Transfer.

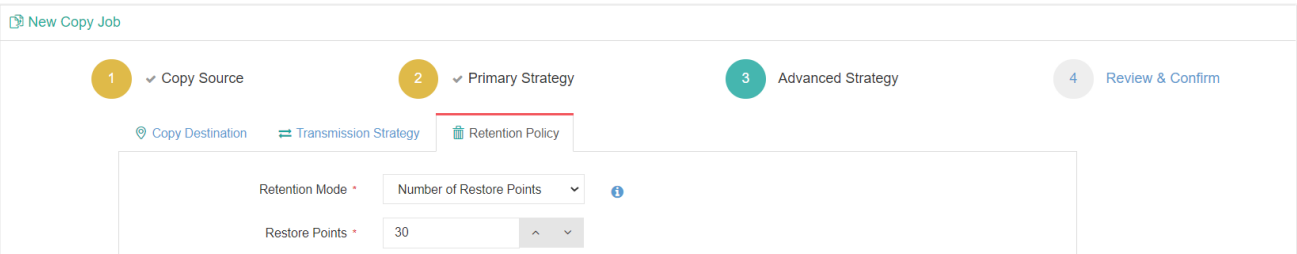


Encrypted Transmission: The data transmitted from backup source to backup copy storage will be encrypted to ensure the safety of the data transmission.

Compressed Transfer: Enable it to compress the backup data during transmission. The backup data will be decompressed when it arrives the backup copy storage.

➢ Retention Policy

Backup copy retention policy is similar with the backup retention policy, it is used to reserve backup copy data stored on the backup copy storage.

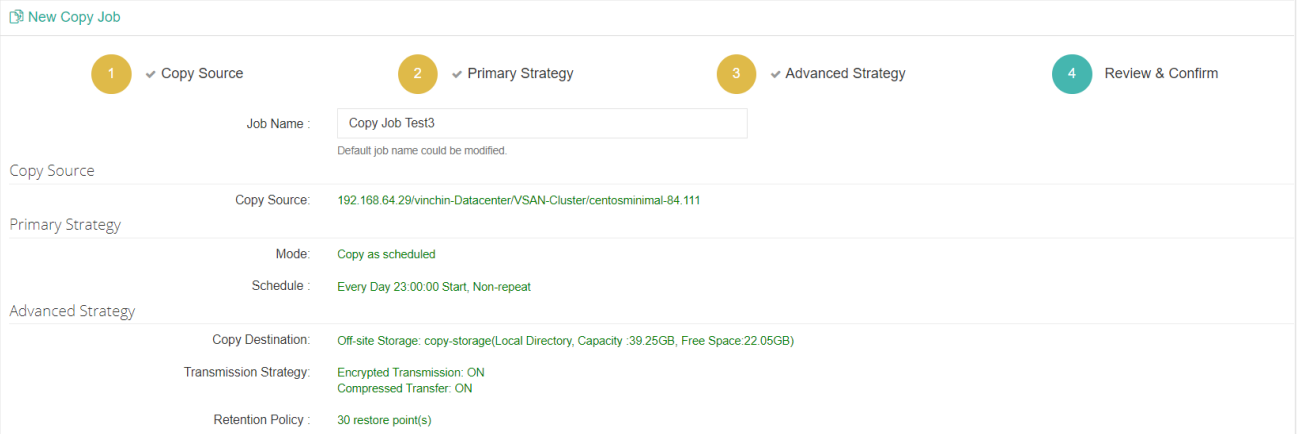


If you choose the retention policy as number of restore points, Vinchin Backup Server will save the specified number of restore points (for each VM included in the copy job), if you choose number of days, Vinchin Backup Server will save the restore points within the specified number of days (for each VM included in the copy job), the older restore points will be deleted or merged to comply with the retention policy.

For more details of how retention policy works, please refer to the instructions of retention policy from Create Backup Job. The retention policy for backup job and copy job works independently but with the same principles.

Step4: Review & Confirm

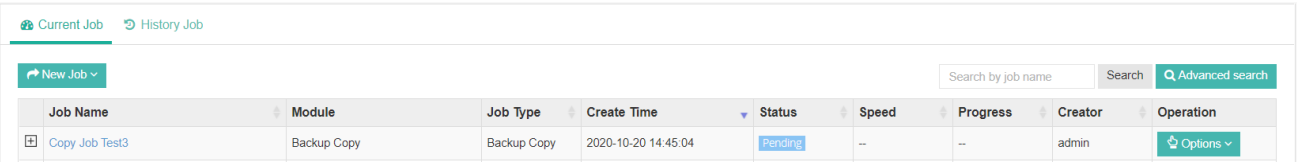
After completing the above settings, you are able to review and confirm the settings.



You can optionally customize a job name and then click on Submit button to confirm the creation of this backup copy job.

Copy Job Operations

Once a backup 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.

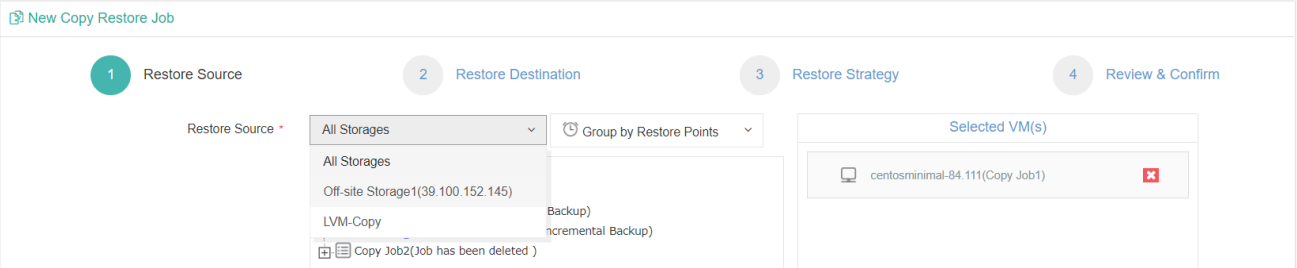
Copy Restore

If the production data and backup data are all lost on your primary site, you can use the backup copy data on off-site backup copy storage (off-site Vinchin Backup Server) to restore the VMs on primary site. But 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 restored to an on-site storage first, then from the **VM Backup** > **Restore** page you can create a VM restore job to restore the VMs.

To create a backup copy restore job, please go to **Backup Copy** > **Copy Restore** page, then follow the steps below to create a copy restore job.

Step 1: Restore Source

Select an off-site backup copy storage, and then select the restore point(s).



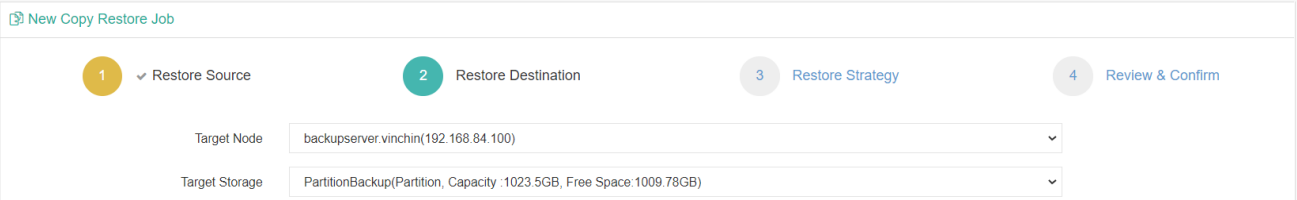
Click on **Next** to continue.

Note

As the backup copy data stored on the on-site backup copy storage can be used to restore virtual machines directly, so you don't have to restore the on-site backup copy data.

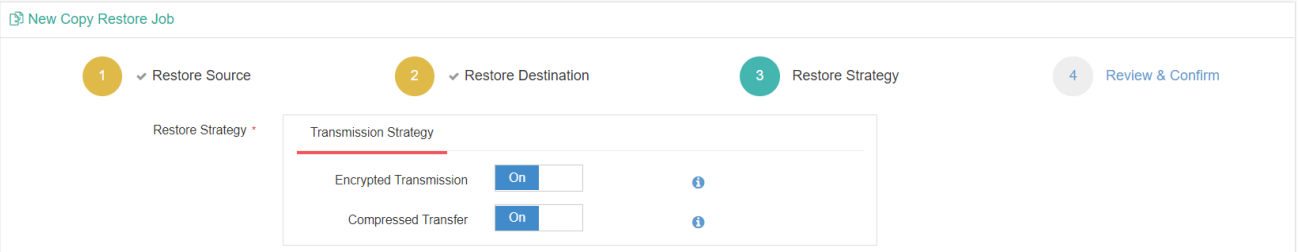
Step 2: Restore Destination

Select an on-site storage where you want to save the restored backup copy data.



Step 3: Restore Strategy

Restore strategy including Encrypted Transmission and Compressed Transfer.



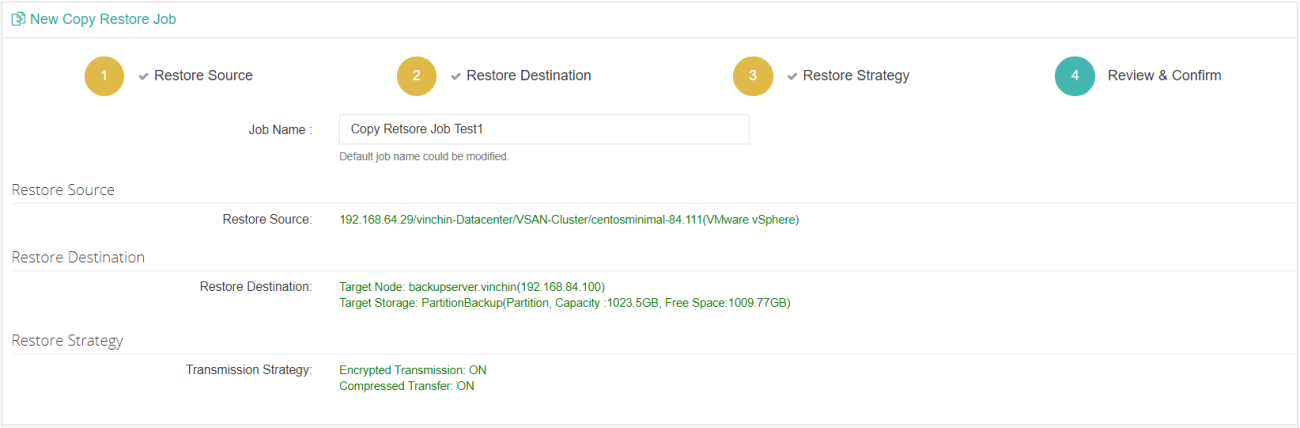
Encrypted Transmission: The data transmitted from off-site backup copy storage to on-site storage will be encrypted to ensure the safety of the data transmission.

Compressed Transfer: Enable it to compress the copy data during transmission. The copy data will be

decompressed when it arrives the on-site storage.

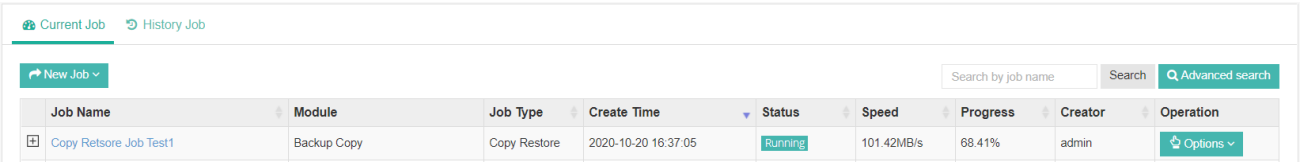
Step 4: Review & Confirm

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 restore job.

After a new copy restore job has been created, you will be redirected to the **Monitor Center** > **Jobs** page, and you will immediately see the copy restore job run automatically.



Once the copy restore job is completed, the job will be automatically deleted from the current job list.

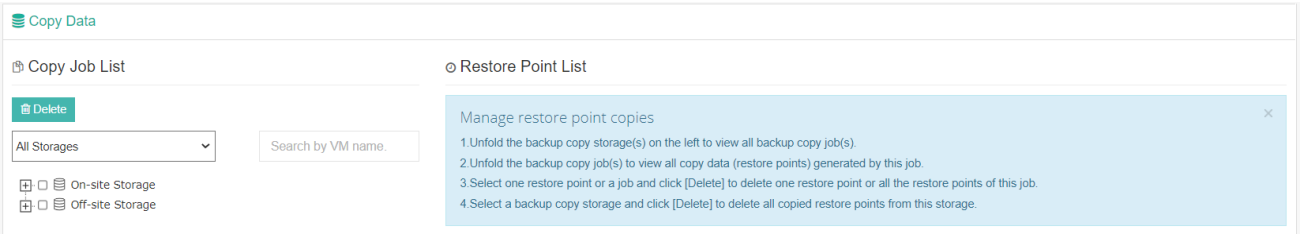
Now you can go to **VM Backup** > **Restore** page and create a VM restore job with the restored backup copy data.

Note

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 (off-site Vinchin Backup Server).

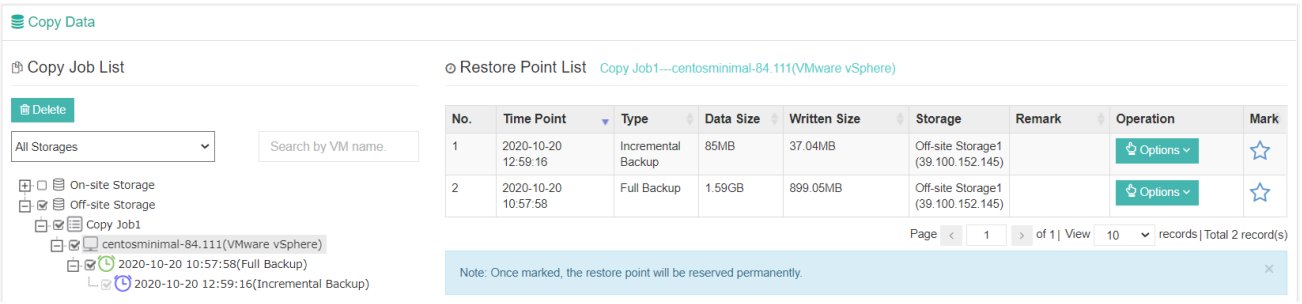
Copy Data

All backup copy data can be managed from the **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, 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 remark or delete the restore point.

And by clicking on the ☆ icon, you are able to mark a restore point, the marked restore point(s) will be kept permanently, and even the retention policy will not delete the marked restore point(s). If the marked restore point is an incremental backup restore point, the retention policy will only cause Vinchin Backup Server merge the last full backup of this incremental backup and the other incremental backups between them to a new full backup restore point, and this merged restore point will be kept permanently. For Hyper-V virtual platforms, only full backup restore point can be marked. For other virtual platforms, you can mark full backup, incremental backup and differential backup restore point.

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 Add Storages.
2. To run a backup archive job, a VM backup job should be completed at first place.
3. Backup Archive is not supported with Microsoft Hyper-V.

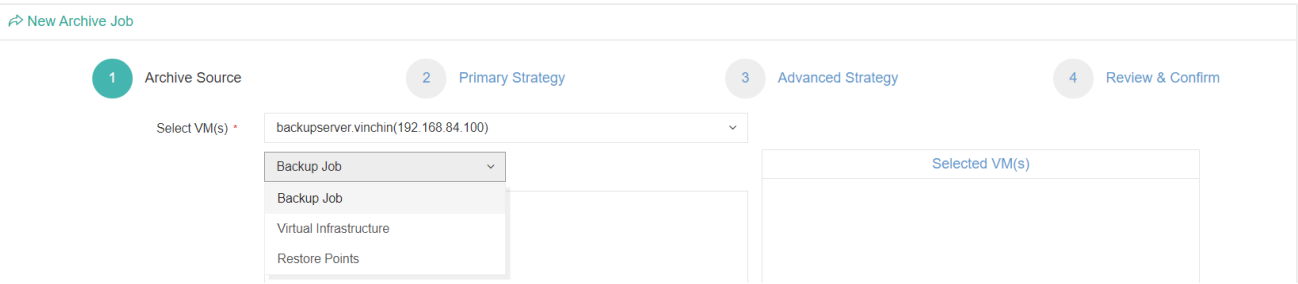
Archive

Create Archive Job

To create a backup archive job, please go to **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.

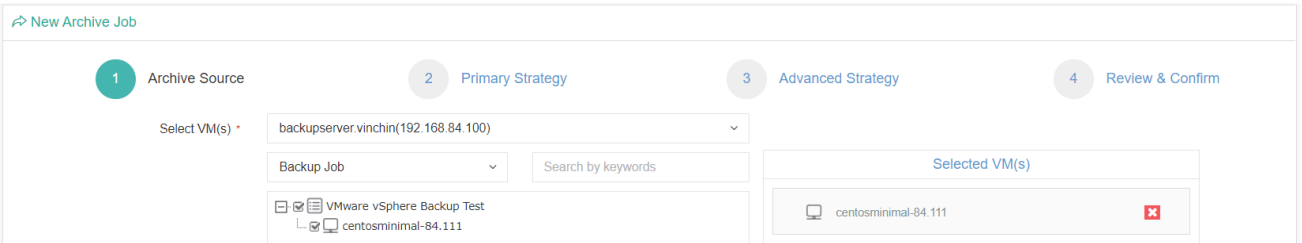


If you select Backup Job, existing backup jobs will be listed, by expanding the backup job you can select the archive source as per the VMs included in the backup job.

If you select Virtual Infrastructure, the virtual infrastructures 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.

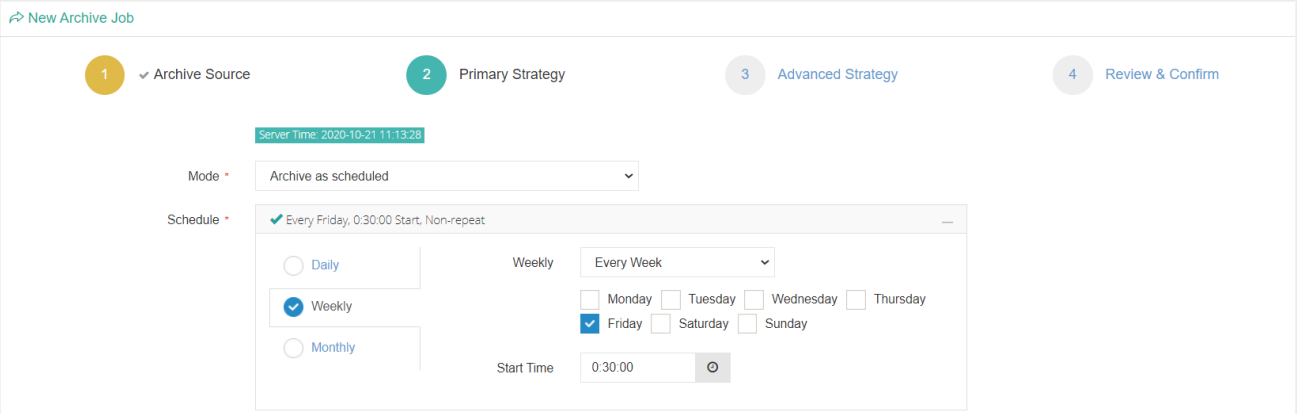
You can select the archive source either way as per your convenience.



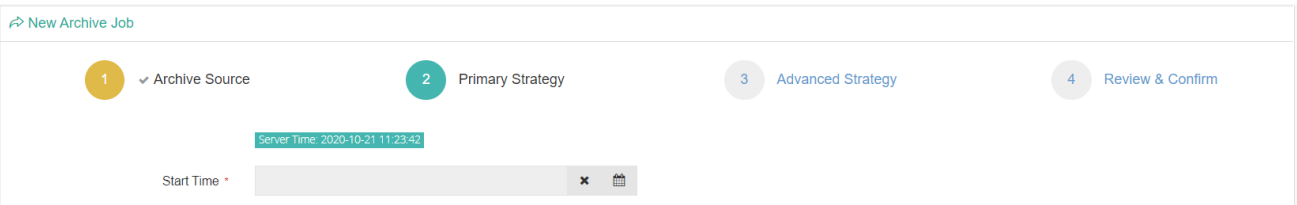
Once the archive source is selected, please click on **Next** button to continue.

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 backup archive 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.

Note

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.

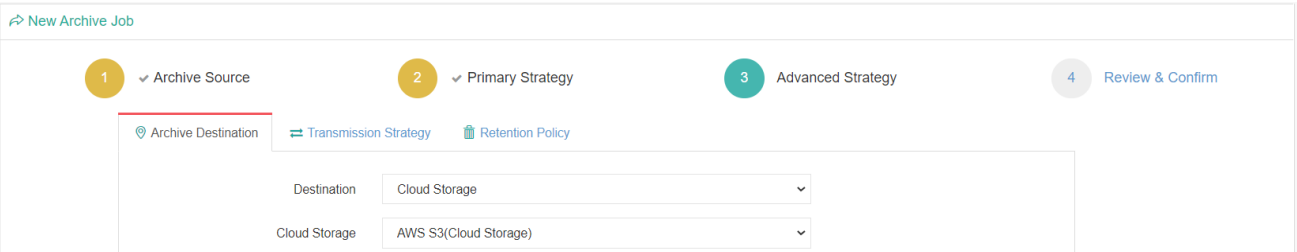
Each of the further archive jobs will always archive a latest full backup restore point to the backup archive storage.

Step 3: Advanced Strategy

➢ Archive Destination

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 Alibaba Cloud storage or AWS S3 cloud storage.

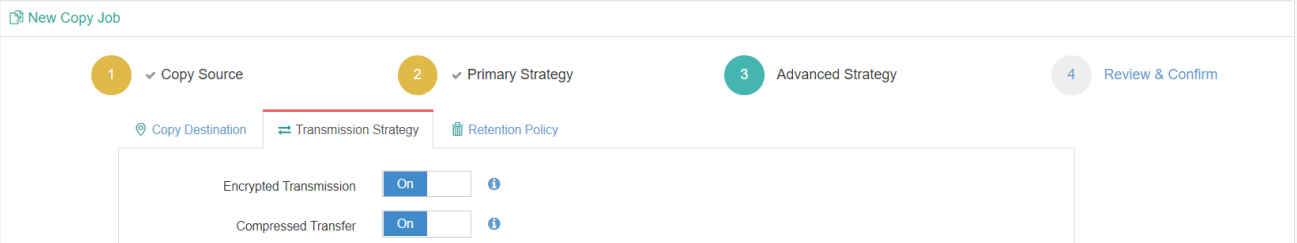
Please select the corresponding storage destination as per your actual deployment and requirements, here we take AWS S3 cloud storage as an example.



In the Destination field, Cloud Storage should be selected.
In the Cloud Storage field, the cloud storages added to Vinchin Backup Server will be available for selecting.

➢ Transmission Strategy

Transmission strategy including Encrypted Transmission and Compressed Transfer.

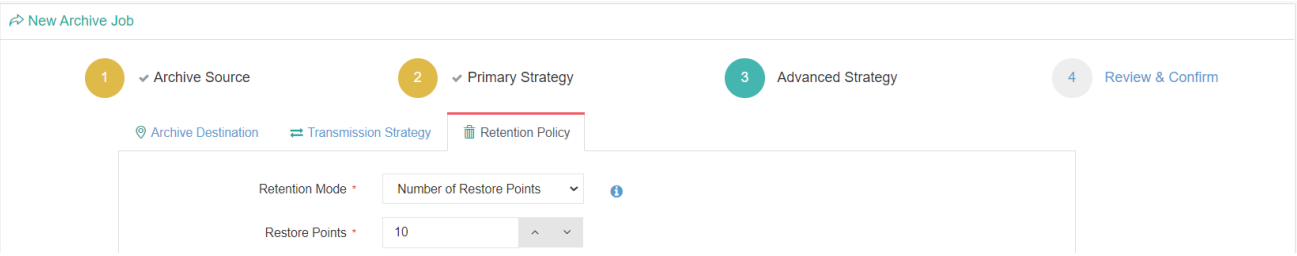


Encrypted Transmission: The data transmitted from backup storage to archive storage will be encrypted to ensure the safety of the data transmission.

Compressed Transfer: Enable it to compress the archive data during transmission. The archive data will not be decompressed when it arrives the archive storage.

➢ Retention Policy

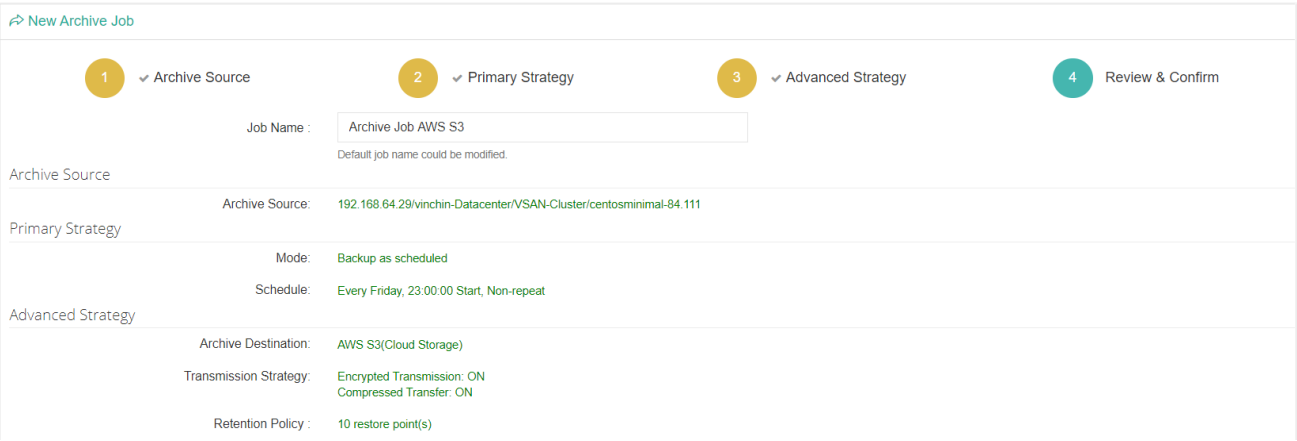
The retention policy of the backup archive job can be configured per the number of restore points.



For example, if the number of restore points is configured as 10, there will always be 10 full backup restore points stored in the backup archive storage.

Step 4: Review & Confirm

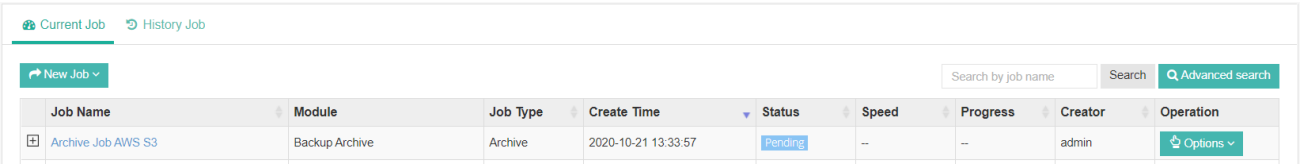
After completing the above settings, you are able to review and confirm the settings.



You can optionally customize a job name and then click on Submit button to confirm the creation of this backup archive job.

Archive Job Operations

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.

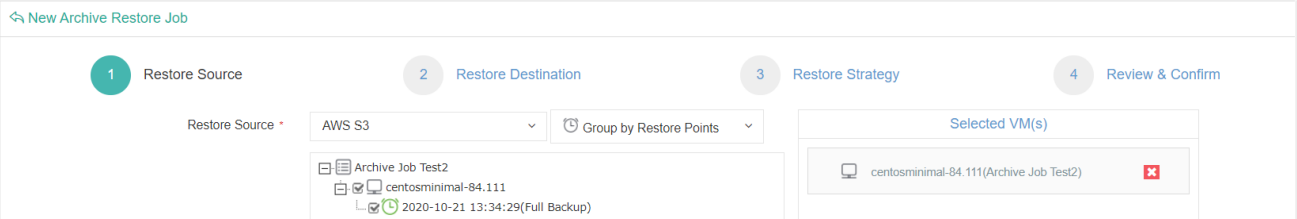
Archive Restore

Backup archive data stored on the cloud storage cannot be used to restore virtual machine directly, it should be restored 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 a archive restore job, please go to **Backup Archive** > **Archive Restore** page, then follow the steps below to create an archive restore job.

Step 1: Restore Source

Select a cloud storage which stores your archive data, and then select the restore point(s).



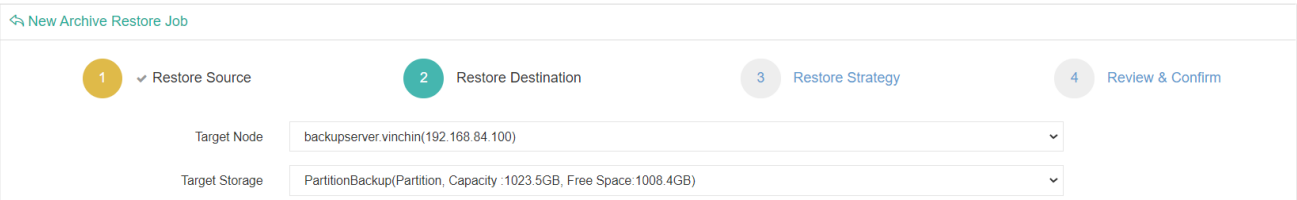
Click on **Next** to continue.

Note

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.

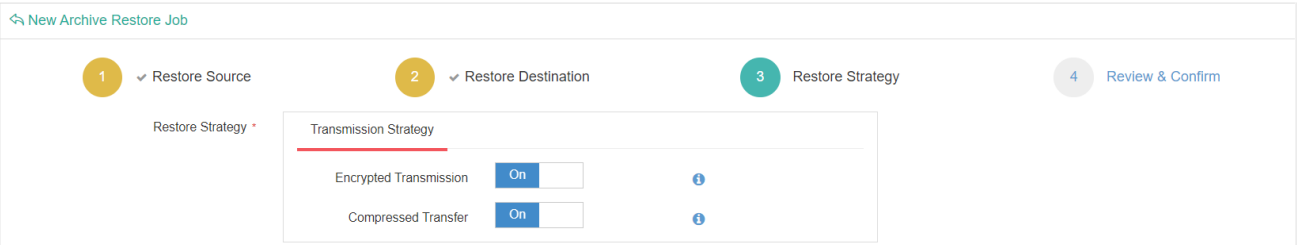
Step 2: Restore Destination

Select an on-site storage where you want to save the restored archive data.



Step 3: Restore Strategy

Restore strategy including Encrypted Transmission and Compressed Transfer.

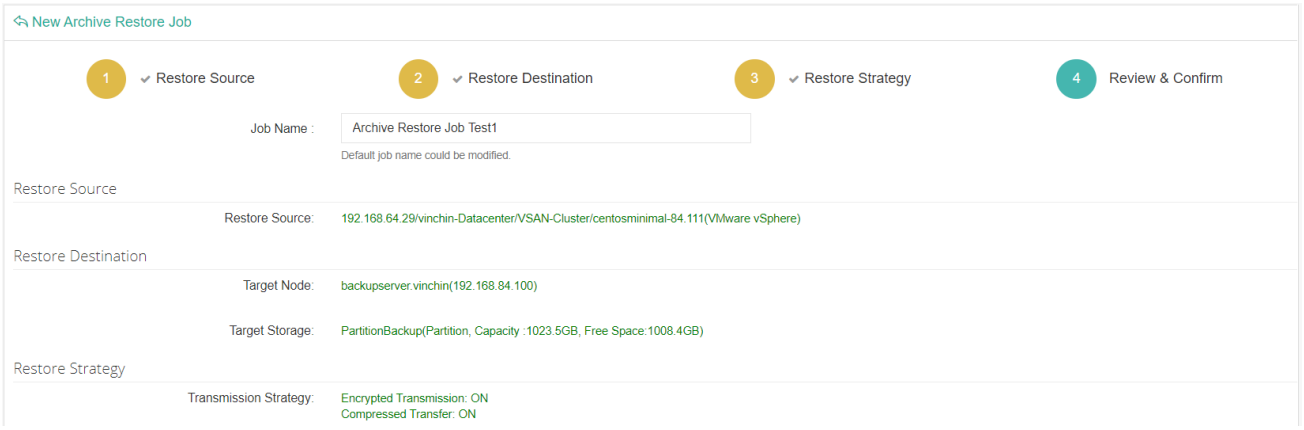


Encrypted Transmission: The archive data transmitted from cloud storage to on-site storage will be encrypted to ensure the safety of the data transmission.

Compressed Transfer: Enable it to compress the archive data during transmission. The archive data will be decompressed when it arrives the on-site storage.

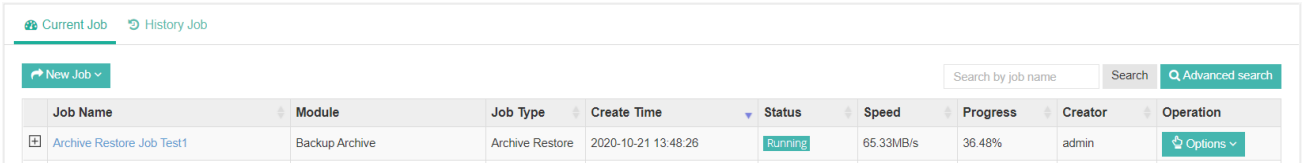
Step 4: Review & Confirm

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 restore job has been created, you will be redirected to the **Monitor Center** > **Jobs** page, and you will immediately see the archive restore job run automatically.

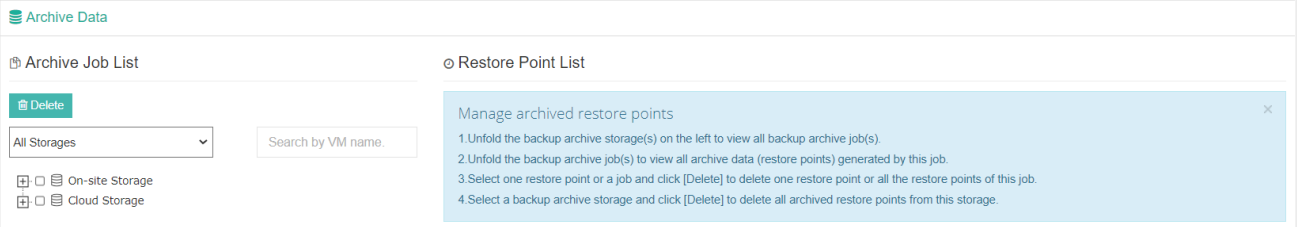


Once the archive restore job is completed, the job will be automatically deleted from the current job list.

Now you can go to **VM Backup** > **Restore** page and create a VM restore job with the restored archive data.

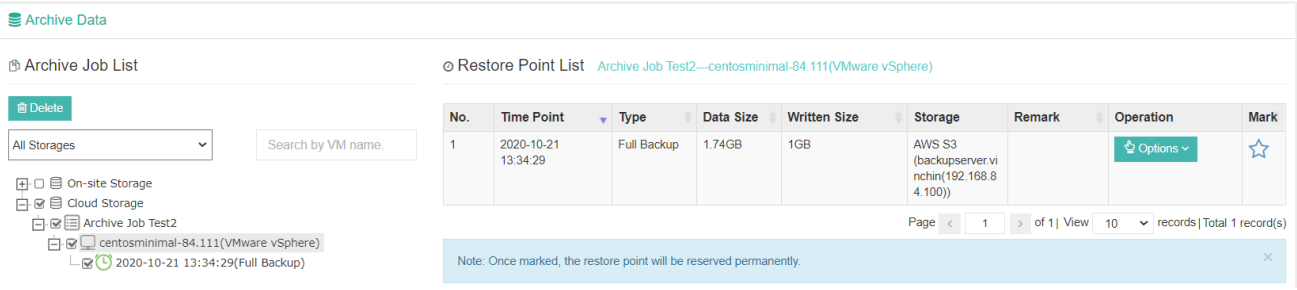
Archive Data

All archive data can be managed from the **Backup Archive** > **Archive Data** page. No matter the data is storage in the on-site storage or cloud 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 remark or delete the restore point.

And by clicking on the ☆ icon, you are able to mark a restore point, the marked restore point(s) will be kept permanently, and even the retention policy will not delete the marked restore point(s).

Resources

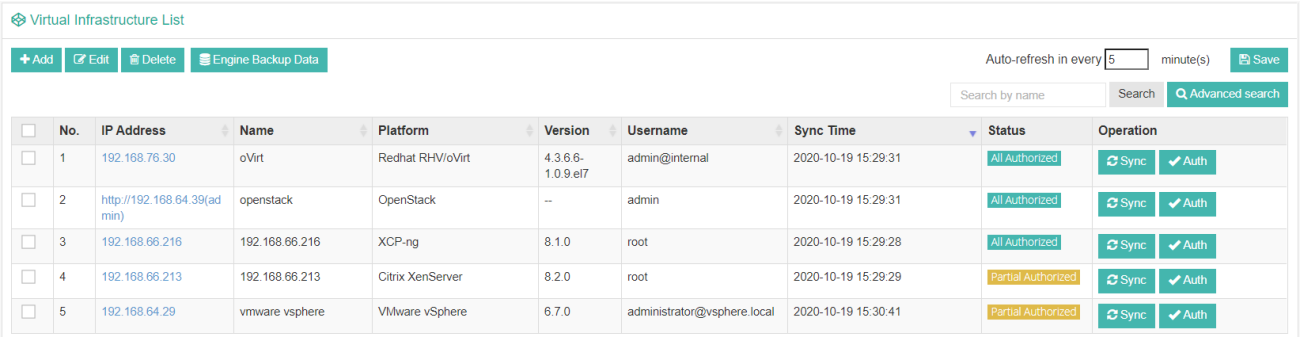
Virtual Infrastructure

Add Virtual Infrastructure

If your virtual infrastructure is VMware vSphere or Huawei Fusion Compute, please refer to Register Virtual Infrastructure. For other virtual infrastructures, please first refer to Install Backup Plugin, then refer to Register Virtual Infrastructure.

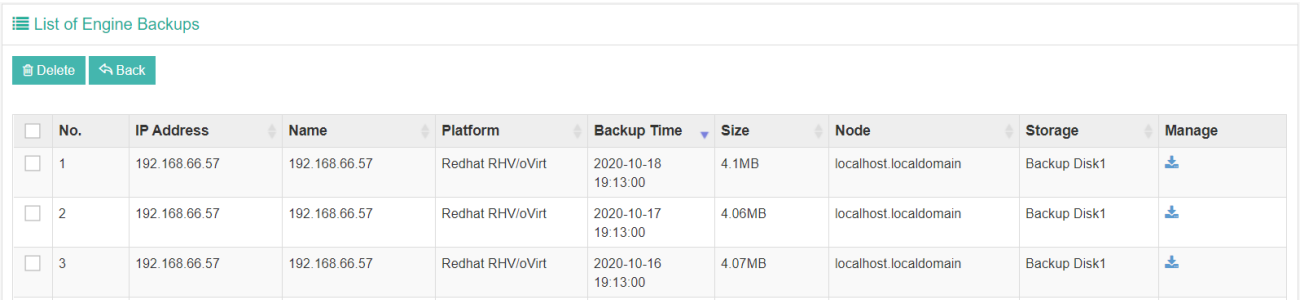
Virtual Infrastructure Management

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 Red Hat 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.



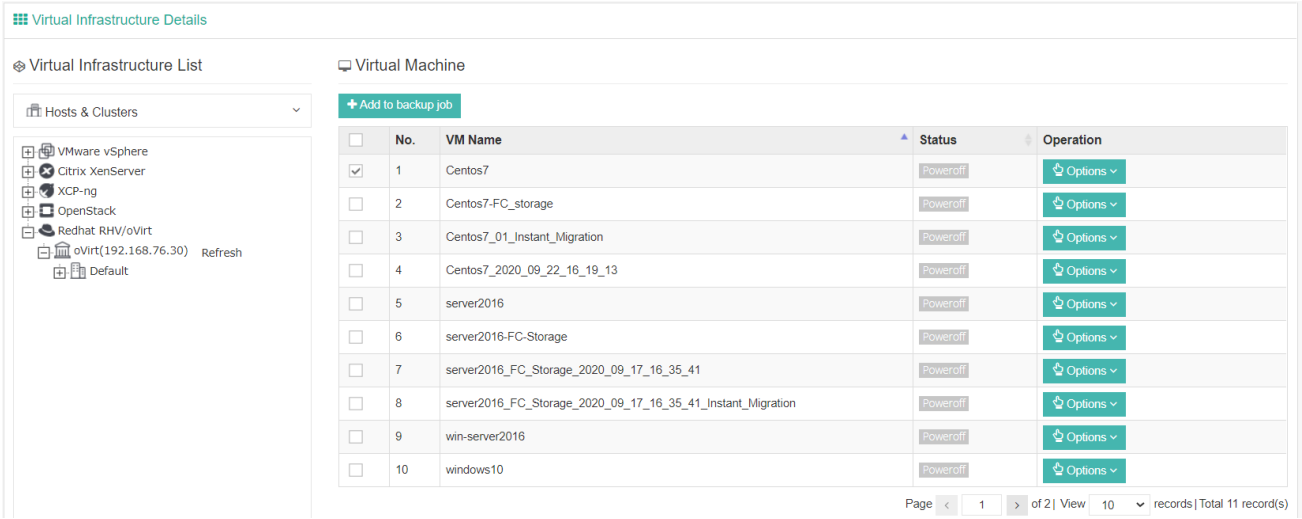
The engine backup data can be downloaded from Vinchin Backup Server, then to be uploaded to the engine host of the Red Hat RHV, oVirt or OLVM to restore the engine host configurations.

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. In the **Auto-refresh in every [ ] minutes** field, 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 Register Virtual Infrastructure.

By clicking on the IP address of a virtual infrastructure, you can check the virtual machines on this virtual infrastructure.



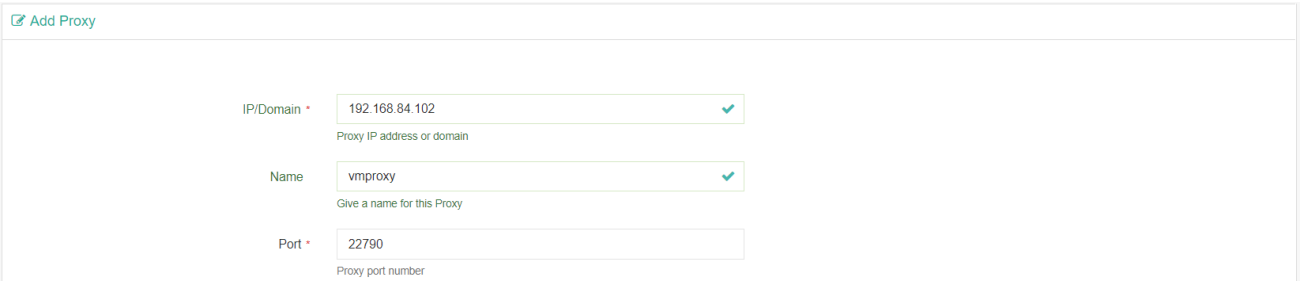
By selecting the VMs from the virtual machine list and click on the **Add to backup job** button, you can add the selected VMs to an existing backup job. Or you can add a single VM to an existing backup job by clicking on the **Options** button then select **Add to current job**.

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.

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** > **Proxy** page and click on the **Add** button to add the Backup Proxy.

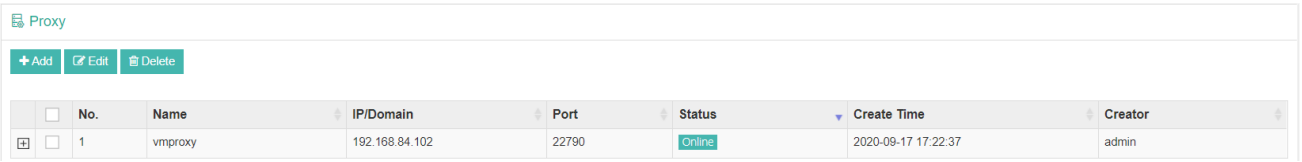


In the **IP/Domain** field, please enter the IP address of the Backup Proxy.

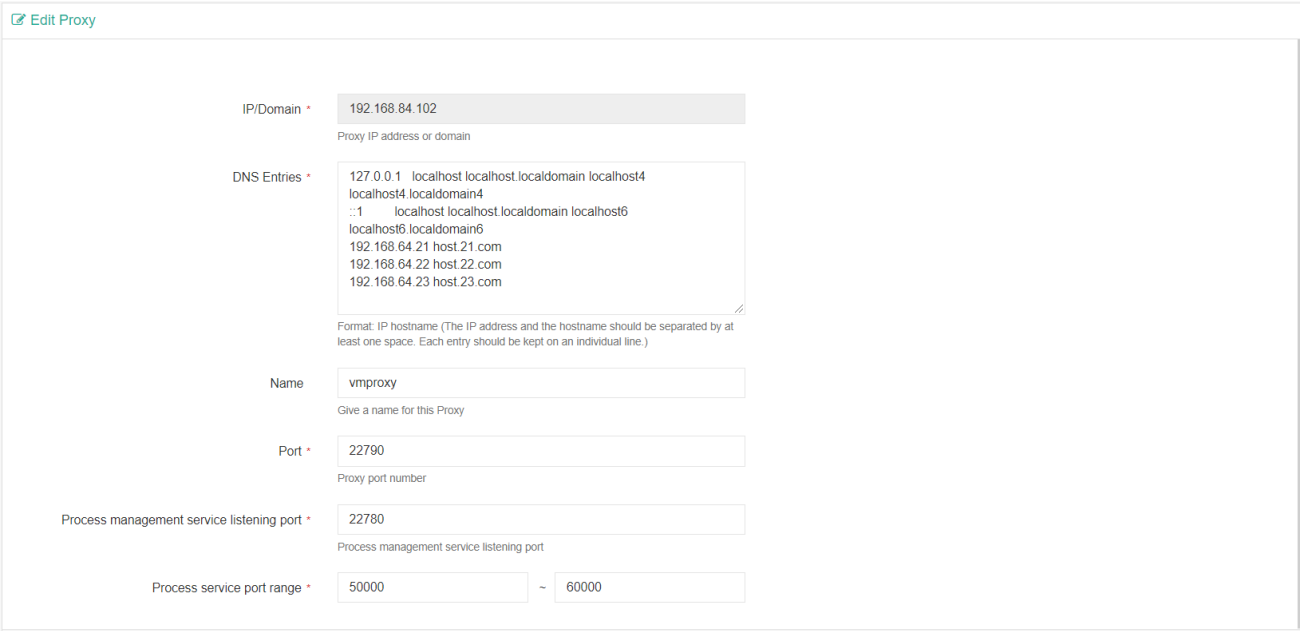
In the **Name** field, you can optionally define a customized name for the Backup Proxy.

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.

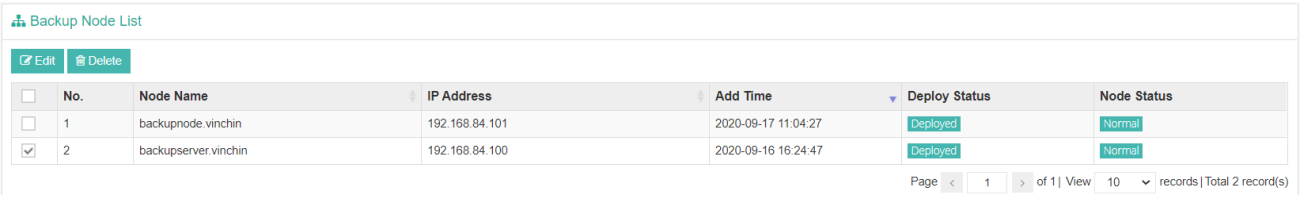


The DNS Entries should be synchronized from the Backup Server if DNS settings had been configured on the DNS Sync option is enabled on the Backup Server. Otherwise, you can configure the DNS settings manually here.

And usually the port number settings should not be changed.

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 to 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.

Storage

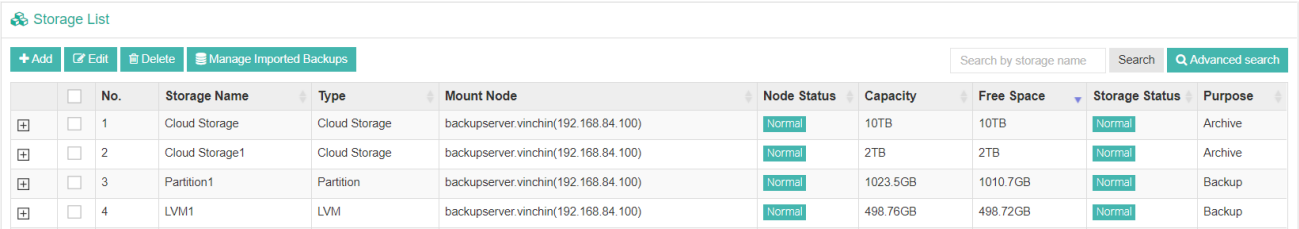
The storages for Backup, Backup Copy and Backup Archive can be added and managed from the **Resources** > **Storage** page.

Add Storage

For how to add storages to Vinchin Backup Server/Node, please refer to Add Storages.

Manage Storages

All storages add to Vinchin Backup Server/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 Backup Node. If there's backup/copy/archive data on the target storage, the data will not be deleted from the storage.

For managing imported backup data, please refer to Data Importing and Storage Formatting.

LAN-Free

Vinchin Backup Server currently supports Fiber 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 fiber channel SAN, the physical server needs a fiber channel HBA (Host Bus Adaptor) interface card to be able to connect to the fiber 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.

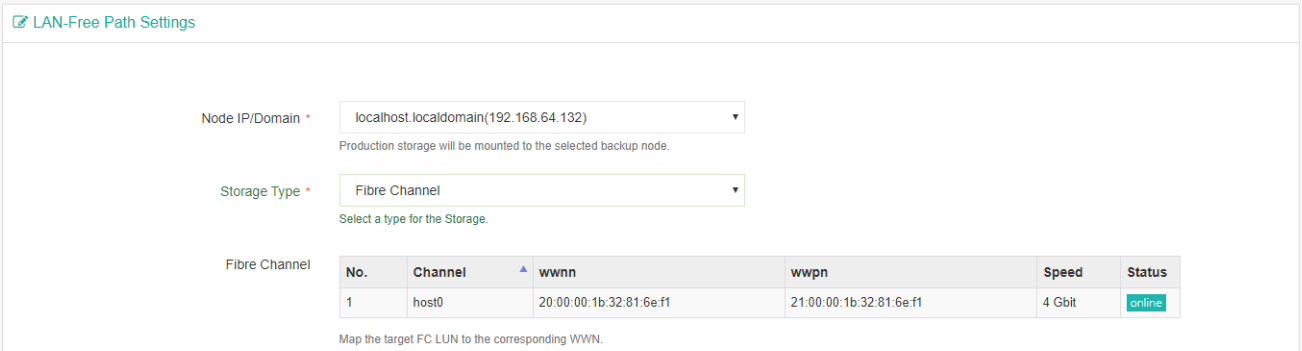
Note

1. LAN-Free backup and restore is not supported with Microsoft Hyper-V and Sangfor HCI in Vinchin Backup & Recovery version 6.0.

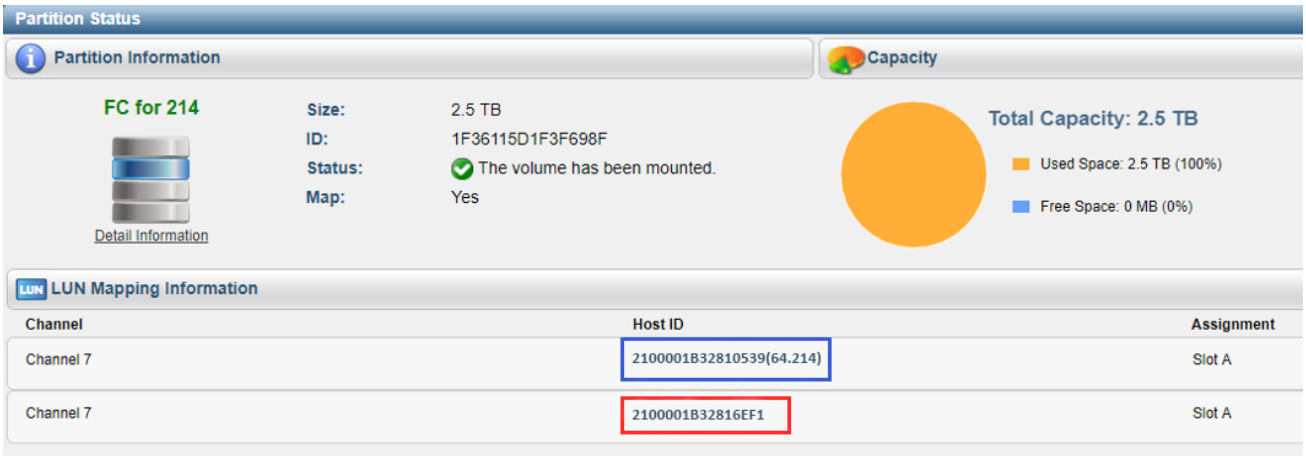
2. The following instructions are for reference only, as the LUN mapping varies from different storage servers.

➢ Fiber Channel

From Vinchin Backup Server web interface, on the **Resources** > **LAN-Free** page, click on **Add** button to add a fiber channel storage, in the **Storage Type** field, please select **Fibre Channel**.

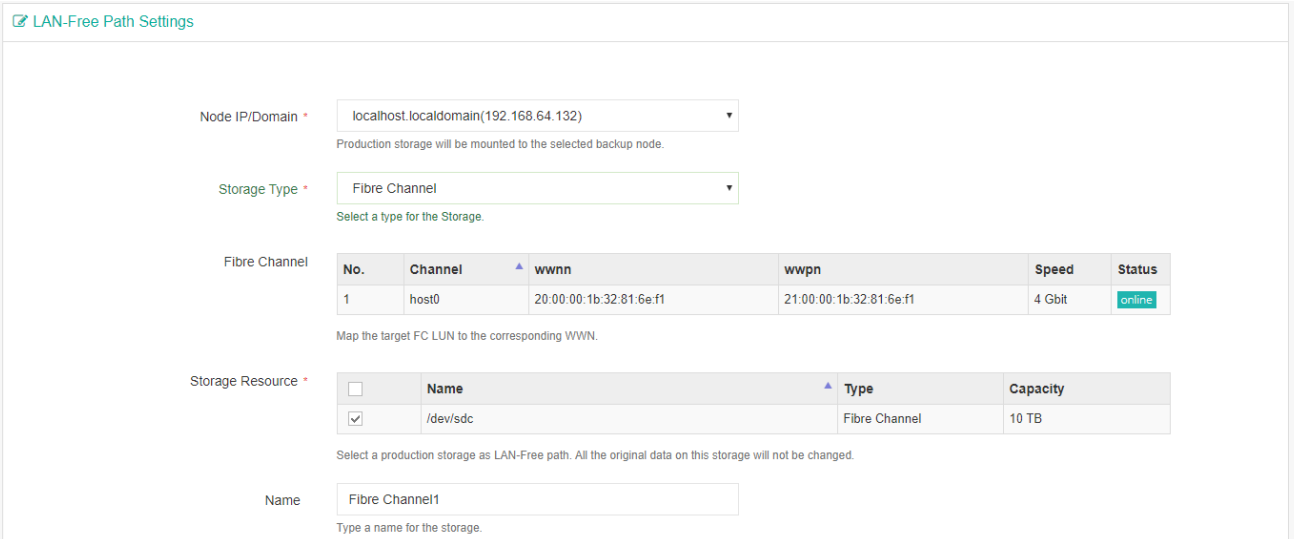


Now Vinchin Backup Server will detect the fiber channel and the wwpn of the HBA interface card, use these information to map the LUN of the production storage to Vinchin Backup Server from the storage server management interface.



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.

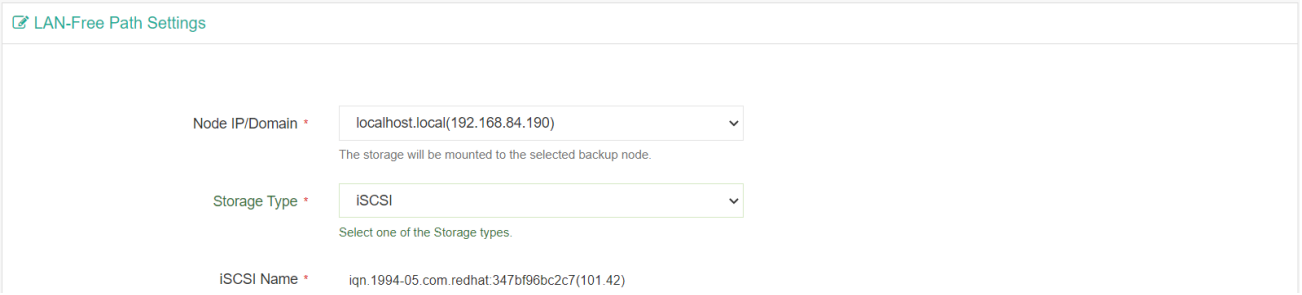
Add the fiber channel again, Vinchin Backup Server will recognize the LUN which is mapped to it, and the storage will be able to be added to Vinchin Backup Server as LAN-Free path.



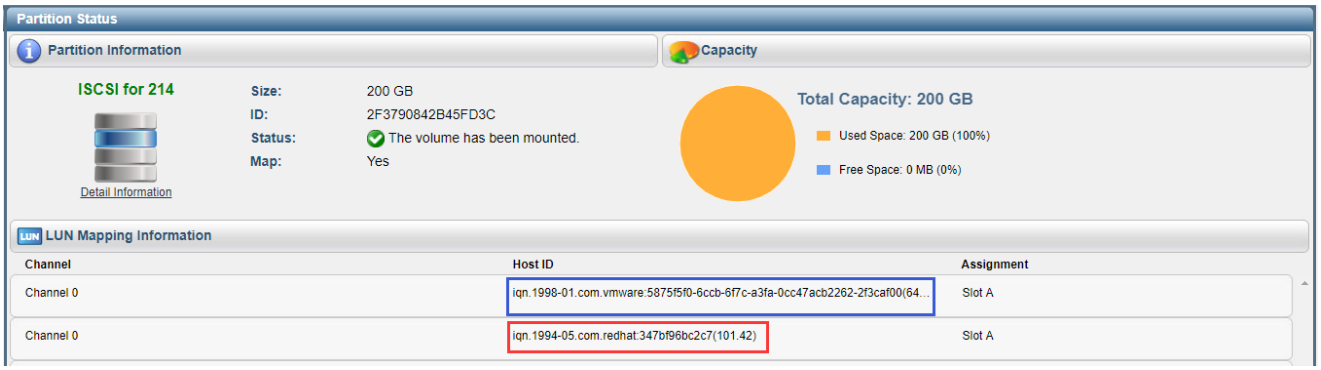
Select the production storage and click OK to add it to the LAN-Free Path List.

➢ 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.

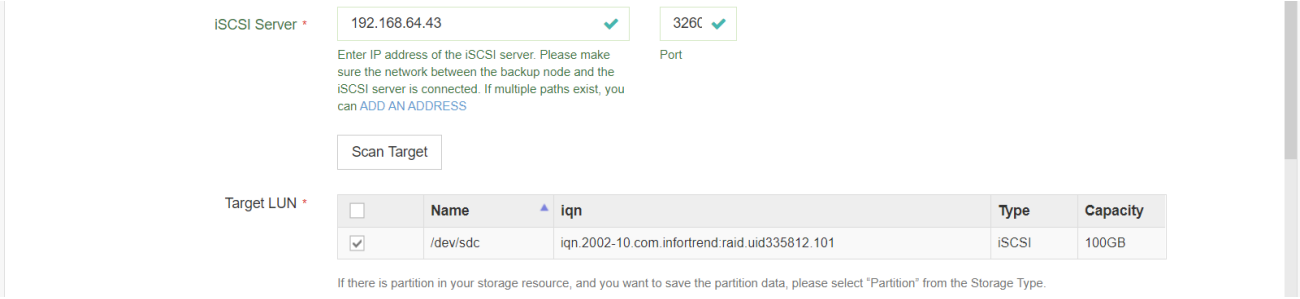


The Host ID marked with blue belongs to the production host, the Host ID marked with red belongs to Vinchin Backup Server, which means the same LUN had been mapped to both of them.

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.

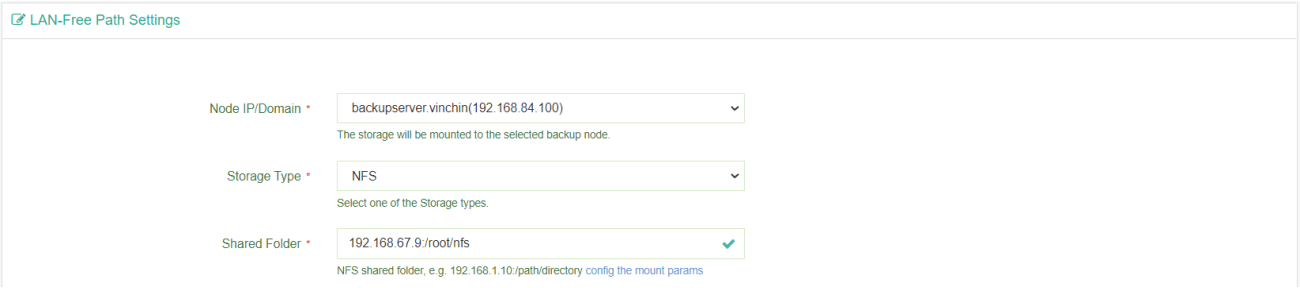


Select the production storage and click OK to add it to the LAN-Free Path List.

➢ 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

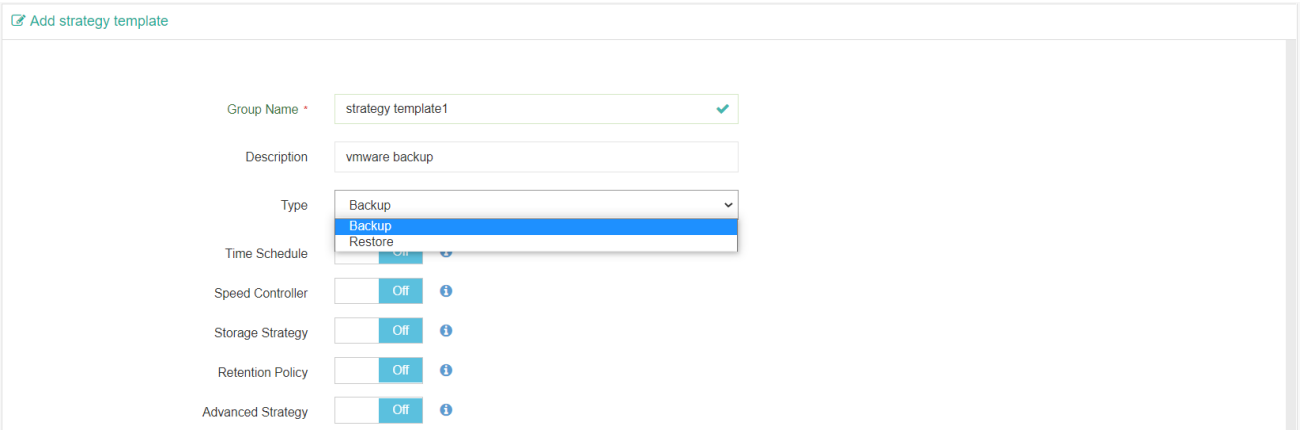
The production storage which has been mapped to the Vinchin backup server as LAN-Free path should NOT be added as a backup storage! Adding a LAN-Free path as a backup storage will cause the production storage been formatted, all the production data will be erased.

If LAN-Free is only used in backup job, not in restore job, the production LUN can be mapped to the backup server with read-only permission.

Strategy

Strategy templates for backup jobs and restore jobs can be pre-configured from **Resources** > **Strategy** page. When users creating new backup or restore 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.

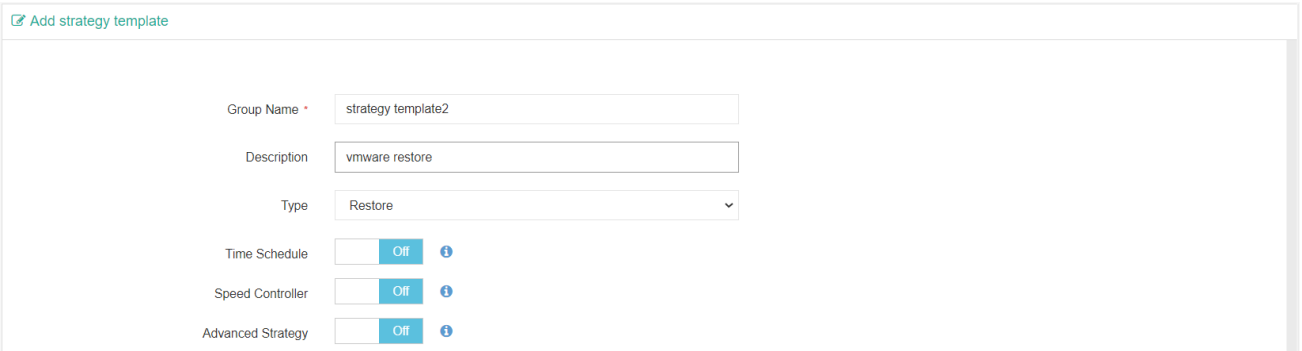


In the **Group Name** field you can define a name for this template, and in the **Description** field you can optionally add some descriptions of this template.

In the **Type** dropdown list, you can select to create a backup job strategy template or a restore job strategy template.

For the **Time Schedule**, **Speed Controller**, **Storage Strategy**, **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.

For backup restore job strategy templates, the principles are the same as creating a backup job strategy template.



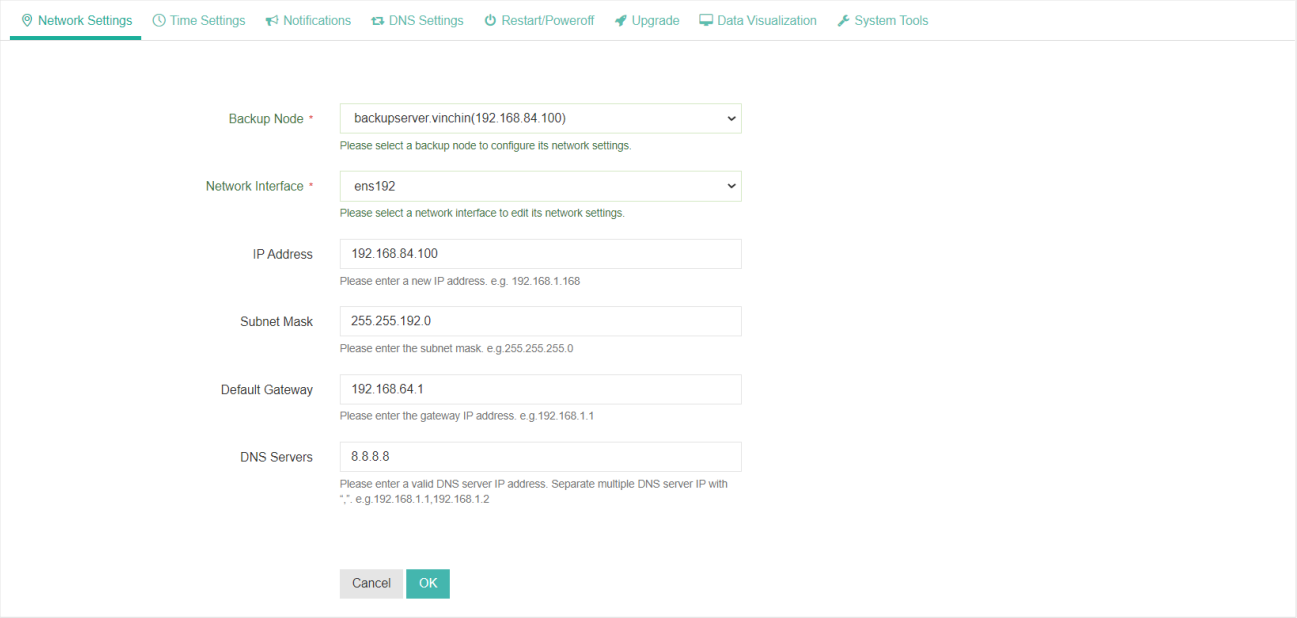
For more detailed explanations of configuring backup job strategy templates, please refer to Create Backup Job, and for the backup restore job strategy templates, please refer to Create Restore Job.

System

System Settings

Network Settings

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.

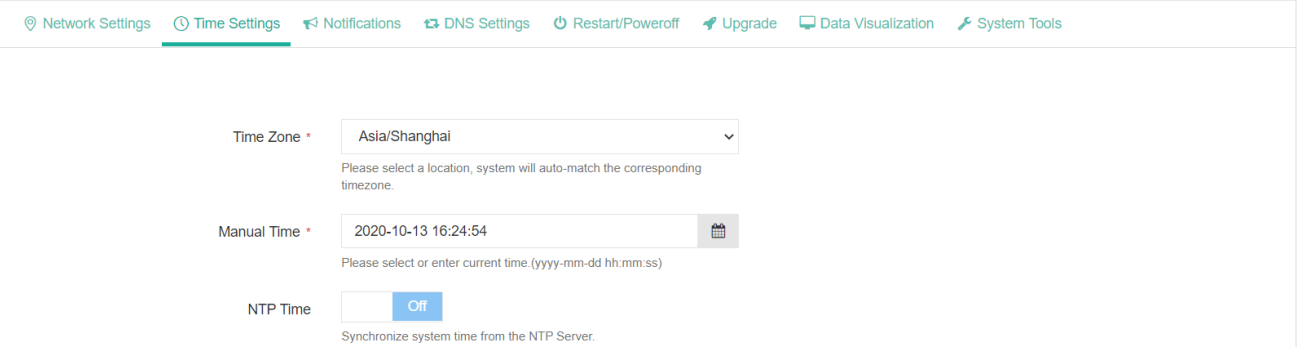
Warning

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.

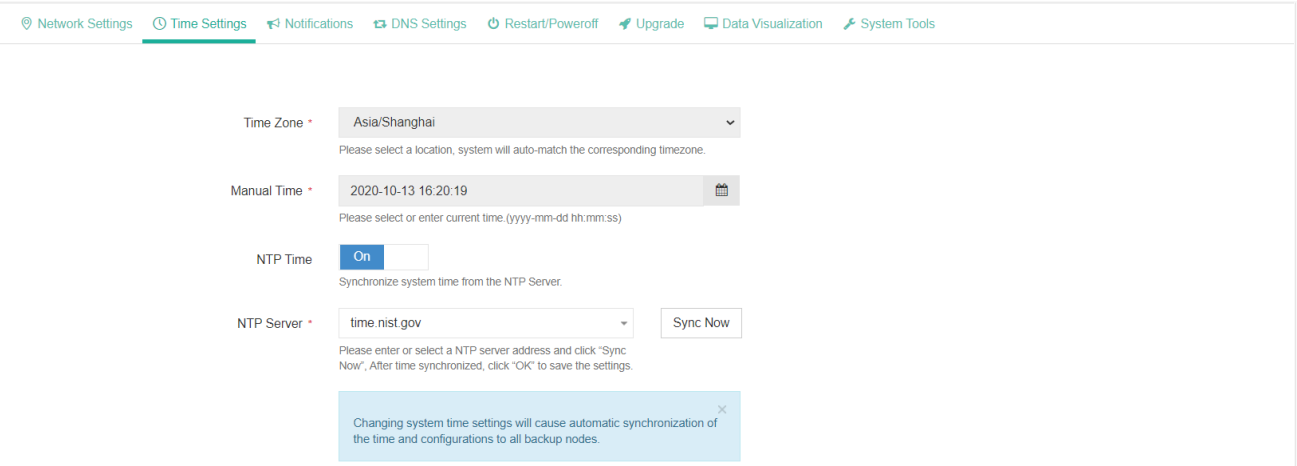
2. Please DO NOT change the IP address of Vinchin Backup Server unless it's really necessary! After changing the IP address of backup server will result in disconnection of the backup node and the backup plugins, please change the listening IP of the backup node and the backup plugins accordingly.

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 here.



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.

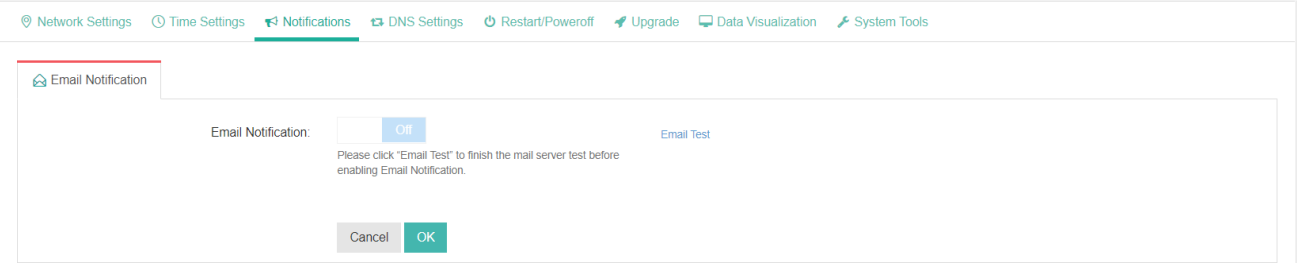


Warning

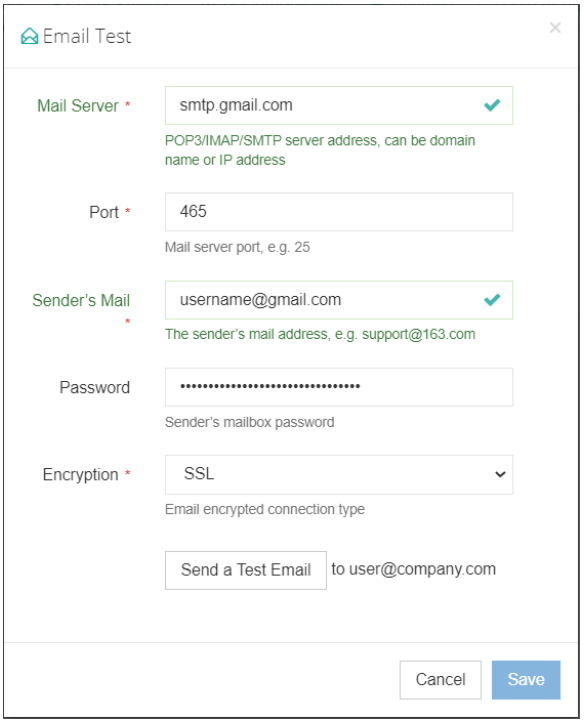
Please make sure the time settings are correct and accurate, as if you had deployed backup node(s), the time settings will be automatically synchronized to all backup nodes connected to this backup server, and as a results, all the scheduled job will run based on the current backup server time.

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.



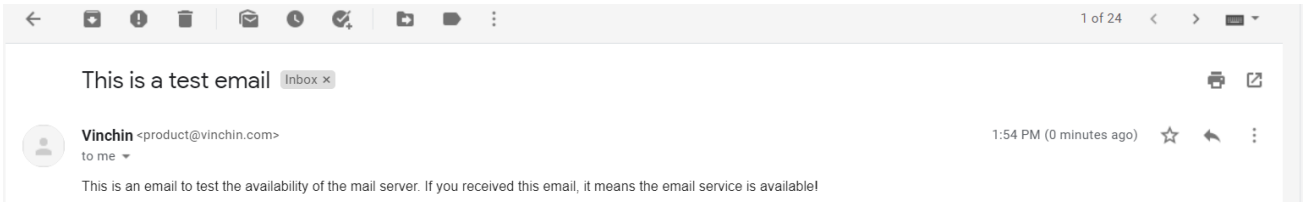
To enable email notification, please first make sure you had specified an Email address from **admin** > **My Information**, then click on Email Test to complete the mail server settings.



You can either use the built-in Vinchin mail service or you can configure your own mail services. To configure your own 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.

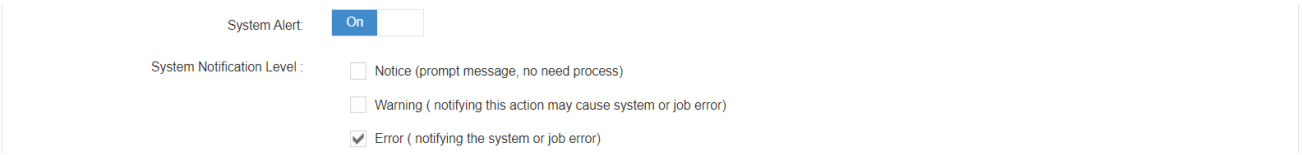
In the above example, Gmail SMTP is used as the outgoing mail server. The **Mail server** should be smtp.gmail.com, **Encryption** should be SSL or TLS, the **Port** number should be 465 or 587, and you must configure a mail account here as the sender. After this, you can click on **Send a Test Email** to test the mail services. The recipient of the test email is the current user, whose Email address is configured in the user information 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.

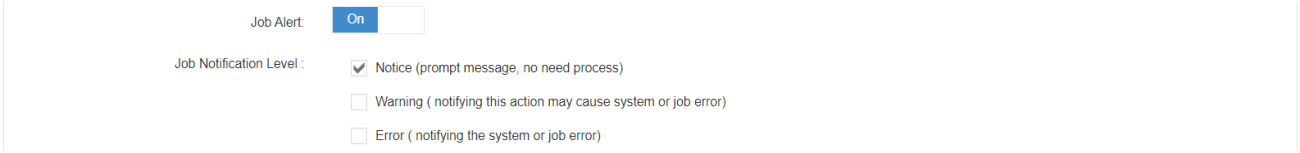
System Alert is not enabled by default, you may enable it if required. The system level notice, warning and error messages are configurable to be sent to specific user(s) via Emails.



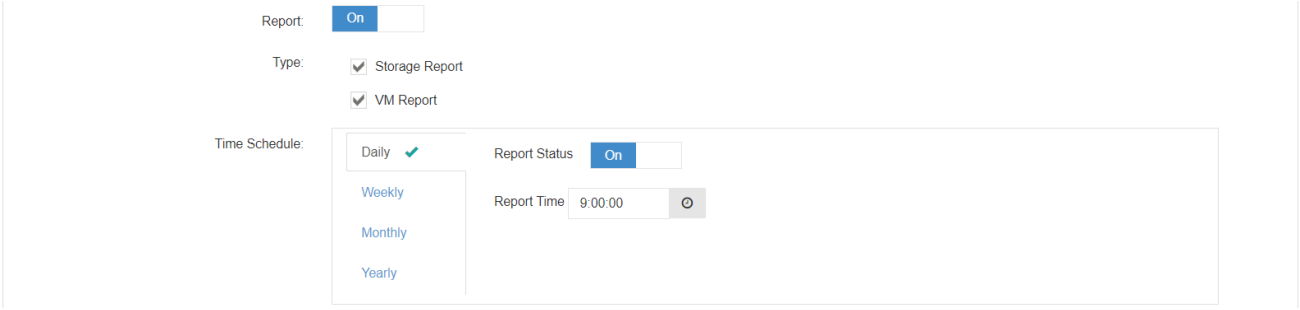
It is recommended to enable sending critical system level notifications, as users don't have to pay much attention on the system level notices.

The Job Alert can be enabled to send backup/restore job level notifications, including job success notices, warnings

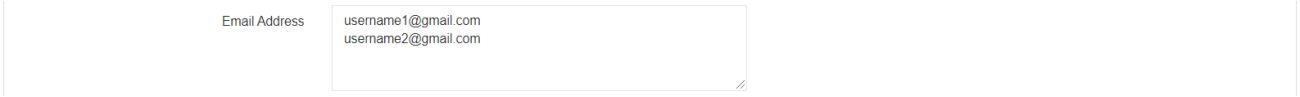
or errors of the jobs.



Report 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.



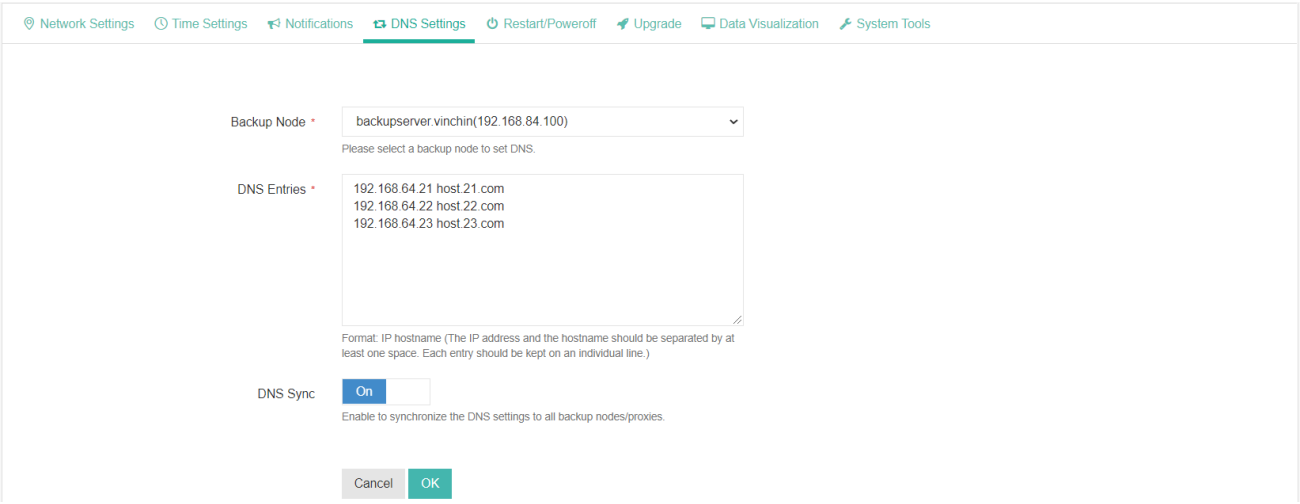
After setting up the notification types and timing, in the Email address field you can optionally enter more user Emails to add them to the Email notification mailing list. The Email address of your own is not needed to be added from here.



The system alerts and reports will be sent to the system administrator by default. The job alerts will be sent to the creator by default. The newly added recipient will receive all the enabled notifications.

DNS Settings

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.

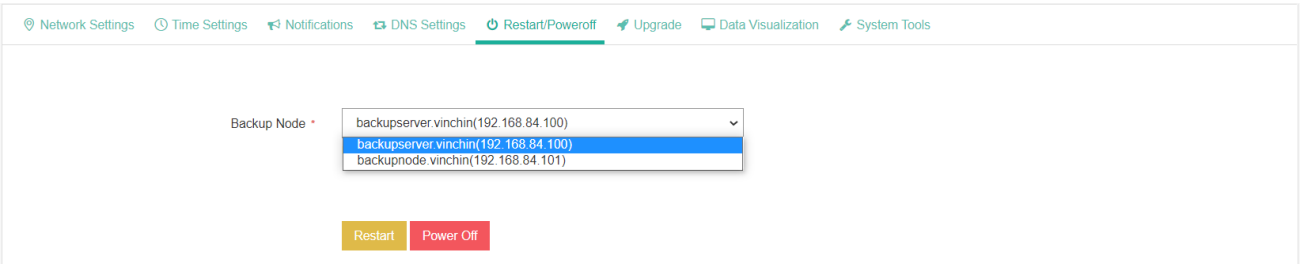


First fill in the IP address of the ESXi host and its domain name separated with a space. If there are multiple ESXi

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.

Restart & Poweroff

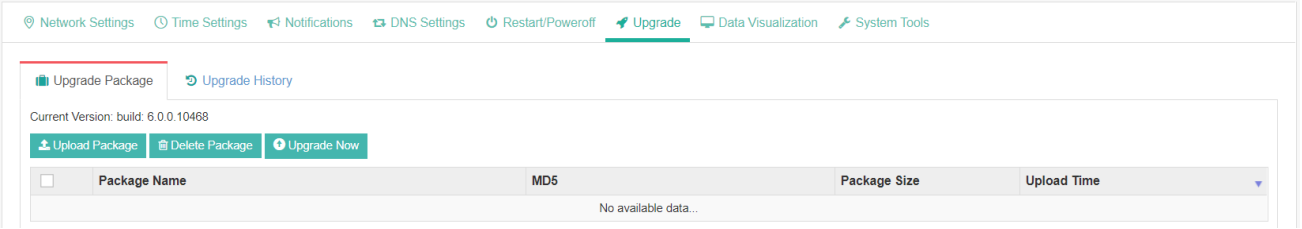
Restart and power off functionalities can be used for the backup server or backup node(s) maintenance or some other circumstances which require system restart or power off.



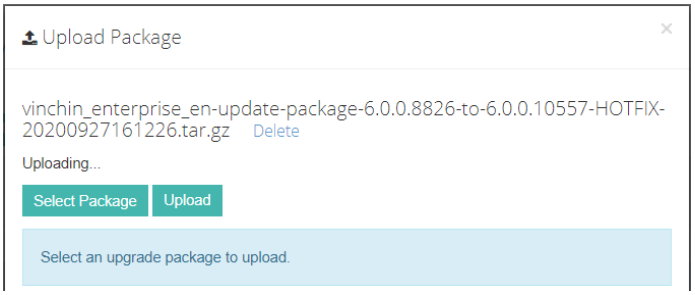
You can select the target node then click on Restart or Poweroff button to perform the corresponding operation to the select node. Both restart and power off operation will terminate backup/restore jobs on the selected system, so before doing this, please make sure there's no job running on the selected node.

Upgrade

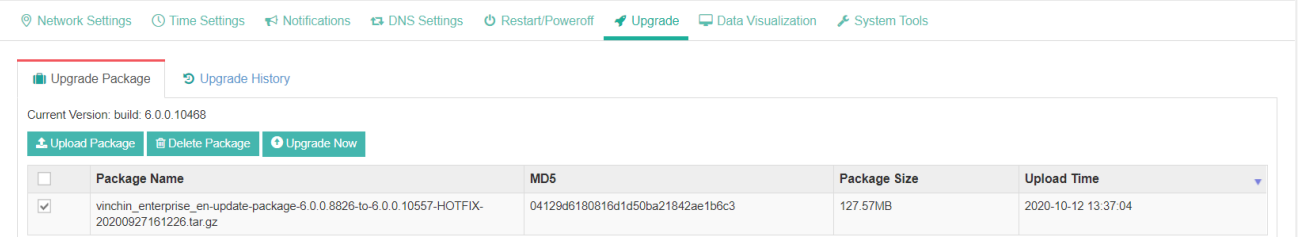
When new software or patch upgrade for Vinchin Backup Server or Backup Node is required, you can upload and upgrade Vinchin backup server or backup node from here.



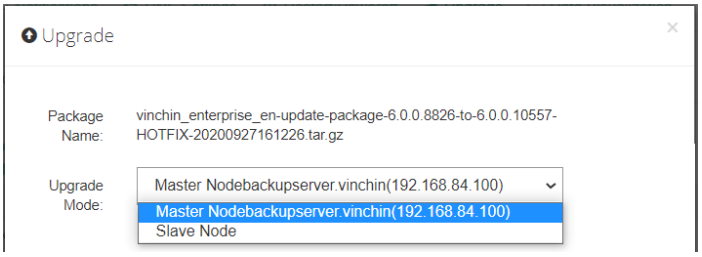
To upload a firmware package, please click on **Upload Package** button. In the popup dialog, click on Select Package to locate the firmware package.



You can upload multiple packages at a time, once selected all packages, please click **Upload** button to start uploading the selected firmware package(s).



Once uploaded, please select the target package and then click on the **Upgrade Now** button.



Select the backup node from the popup dialog and click on OK to upgrade.

If you have multiple backup node deployed, you can select them all and upgrade them at the same time.

Note

If you are going to upgrade backup server and the backup node, please first upgrade the server, then upgrade the node. And the upgrade will require system reboot, please make sure there're not jobs running on the backup server or backup node before upgrading.

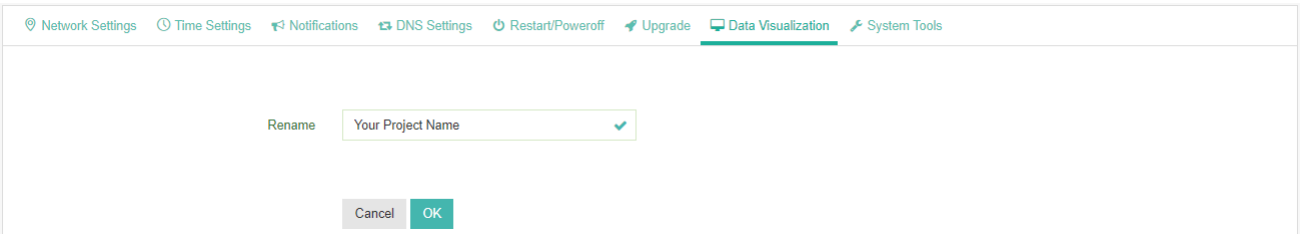
Data Visualization

Data visualization is a value-added service, it briefly presents the real-time status and useful information of the virtual infrastructure, protected virtual machines, backup storage, history jobs, current running jobs and more other information in a single intuitive graphical screen. 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 project name from the **System** > **System Settings** > **Data Visualization** page.

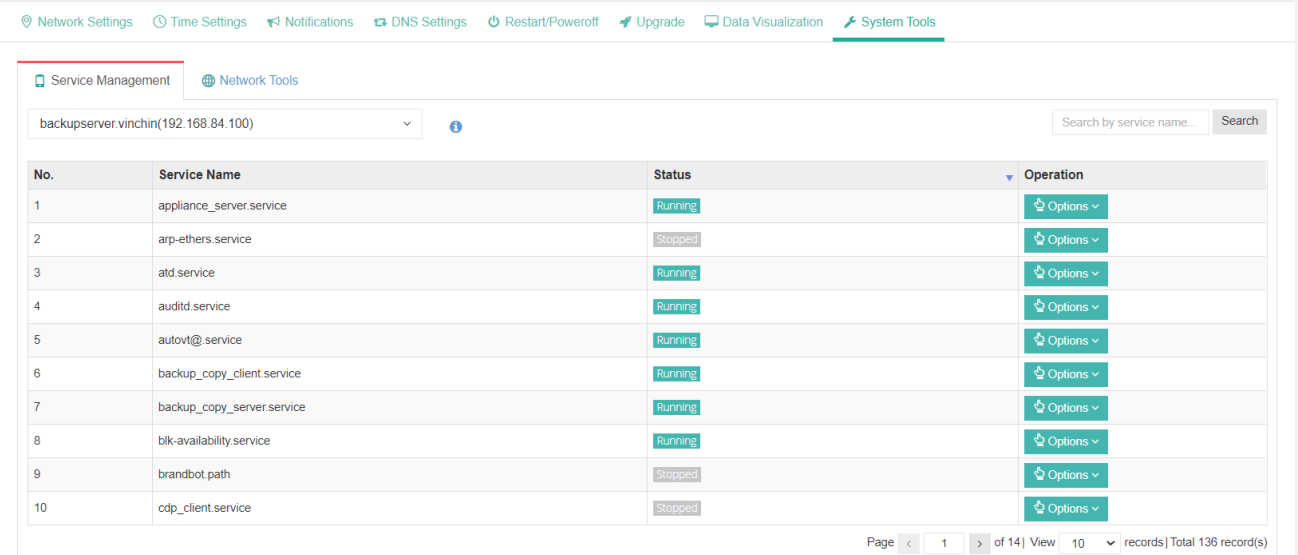


System Tools

System tools including the Service Management and Network Tools. They can be used for maintenance and troubleshooting purpose.

- **Service management**

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 services' status and perform operations to the services. And you can search specific services by service name.

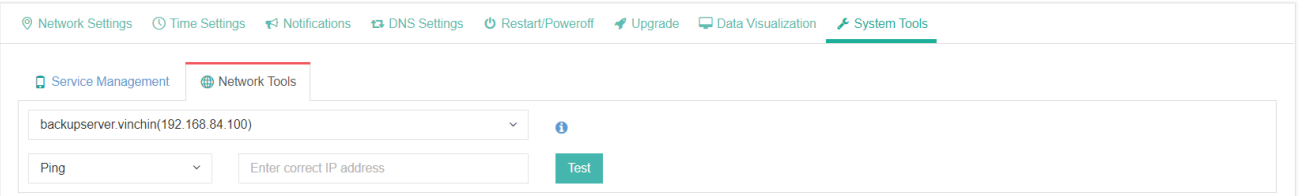
Warning

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 you backup infrastructure will malfunction.

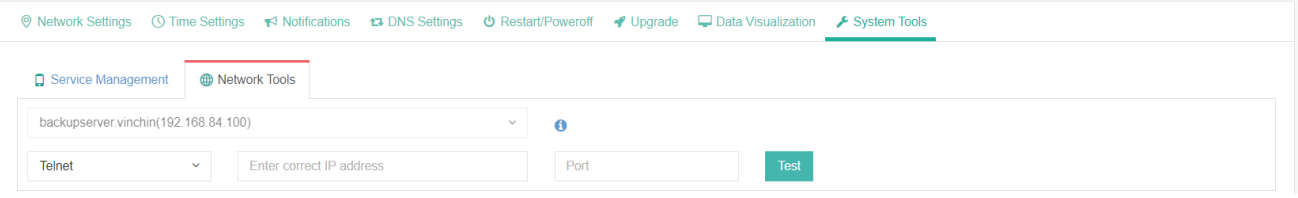
- **Network Tools**

Network tools can be used to exam and troubleshoot the connectivity of each backup 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.



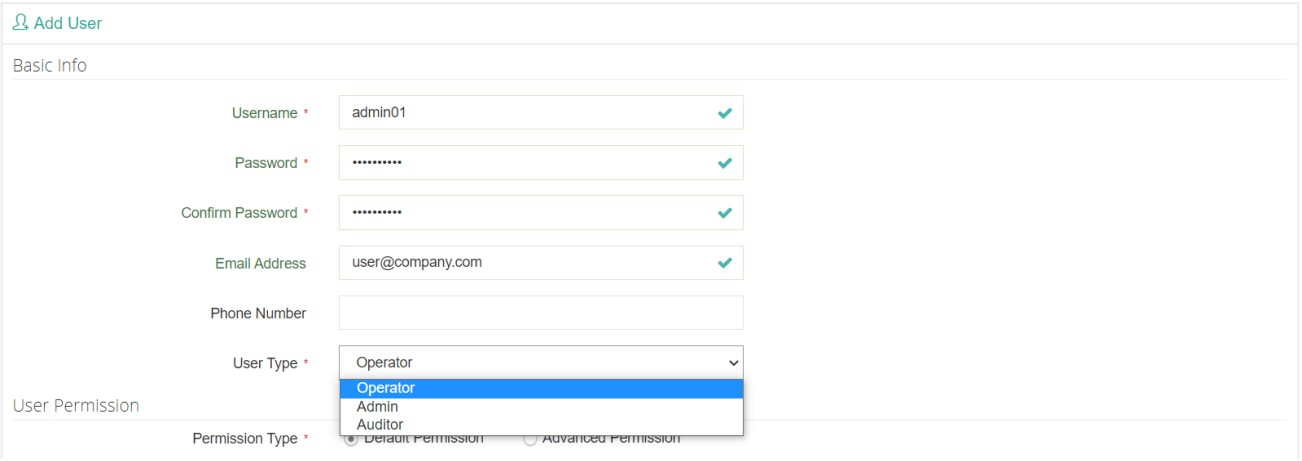
Telnet can only test the connectivity from the backup server to a specific host IP with a service port number.



User Management

Add User

Administrators are able to add multiple users from **System** > **User Management** page. By clicking on the Add button administrator can add a new user.



A new user name and password for this new user need to be specified.

And in the **Email Address** field, the Email address can be specified, so when this user tries to setup system notifications, test Email will be sent to the specified Email address.

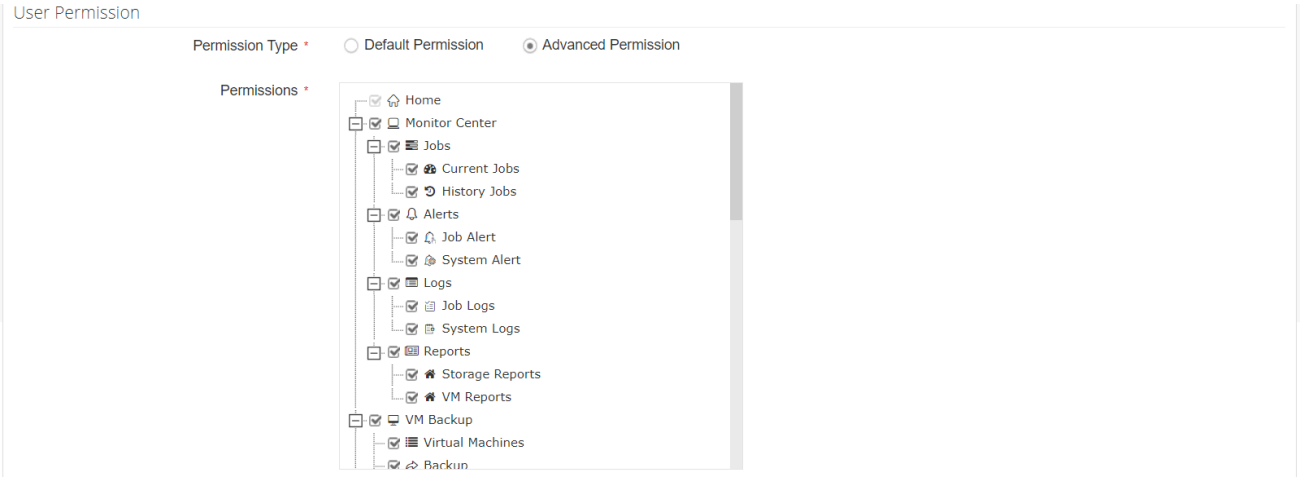
In the **User Type** dropdown list, the role of the user can be set, and corresponding default permissions will be given, the user role and default permissions as below:

Operator: Create and manage Backup/Restore jobs, job monitor, logs/warnings etc.

Auditor: Check logs, alerts, warnings and other reports.

Admin: All permissions.

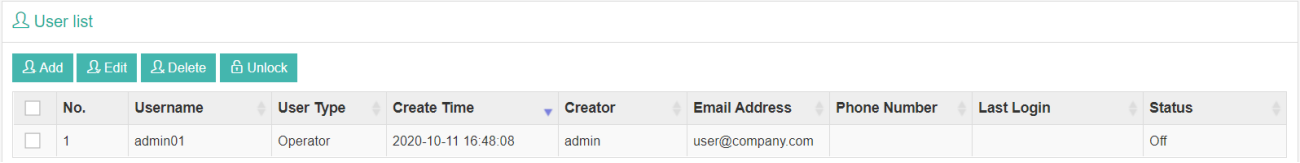
You can also customize the permissions for the added user in the **User Permission** section by selecting **Advanced Permission**.



In the **Permission** menu tree, you can configure customized permissions for the user to be added by enabling or disabling certain system menus.

Other User Management Options

The added user will be listed on the user management page. If there are multiple administrator users had been added to Vinchin Backup Server, each administrator can add new users, but the administrator can only manage the users created by themselves respectively.



To edit a user, please select that user from the user list, and click on **Edit** button. Then you'll be able to modify its password and permissions, but user type cannot be changed.

To delete a user, please select that user from the user list, and click on the Delete button.

If a user attempted to login with wrong password for 5 times, the account will be locked. Only the administrator user who added that user has the permission to unlock the account. Please select the locked user and click on the **Unlock** button to unlock the user.

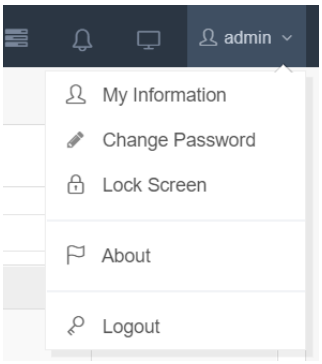
Note

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.

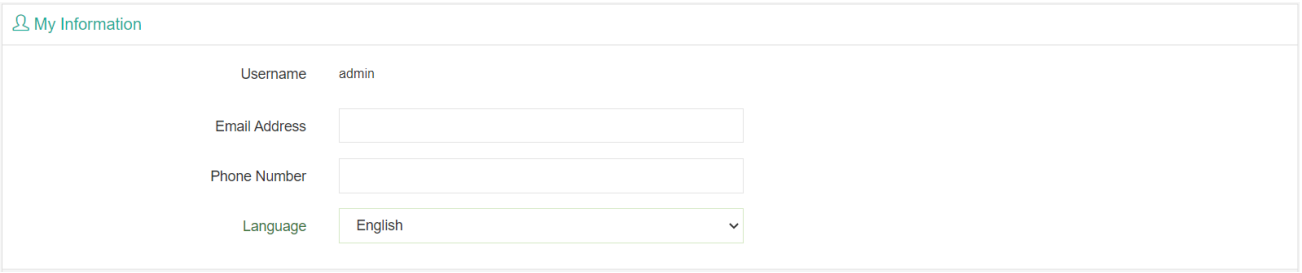
User Settings

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.

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: +86-28-85530156
Email: sales@vinchin.com

Support

Tel: +86-400-9955-698
Email: technical_support@vinchin.com

Website

www.vinchin.com