vinchin

VINCHIN BACKUP & RECOVERY v6.7

Admin User Guide

2022/07

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

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 jobs and at the same time save data repository space. When a disaster occurs causing 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 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.

Supported Environments

Virtual Platform (VM Backup)

- VMware vSphere: 5.5, 6.0, 6.5, 6.7, 7.0(U1, U2, U3)
- Microsoft Hyper-V Server: 2012, 2012R2, 2016, 2019, Windows 10 (Desktop)
- Microsoft Hyper-V on Windows Server: 2012, 2012 R2, 2016, 2019
- Citrix XenServer: 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: 4.0, 4.1, 4.2, 4.3, 4.4
- oVirt: 4.0, 4.1, 4.2, 4.3, 4.4, 4.5
- OpenStack: M to W with Centralized or Distributed storage
- Sangfor HCI: 5.x, 6.0.1, 6.0.1R1, 6.2.0, 6.3.0, 6.7.0, 6.7.0R2
- Oracle Linux Virtualization Manager (OLVM): 4.3, 4.4
- Huawei FusionCompute (KVM): 6.5.1, 8.0.0, 8.0.1
- H3C UIS: E0606, E0611, E0716, E0720, E0721, E0750
- H3C CAS: E0506, E0526, E0530, E0535, E0706, E0709, E0710, E0718, E0730
- ZStack: 3.5, 3.7, 3.8, 3.9, 3.10, 4.0.1, 4.3.0, 4.3.28, 4.4.16

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

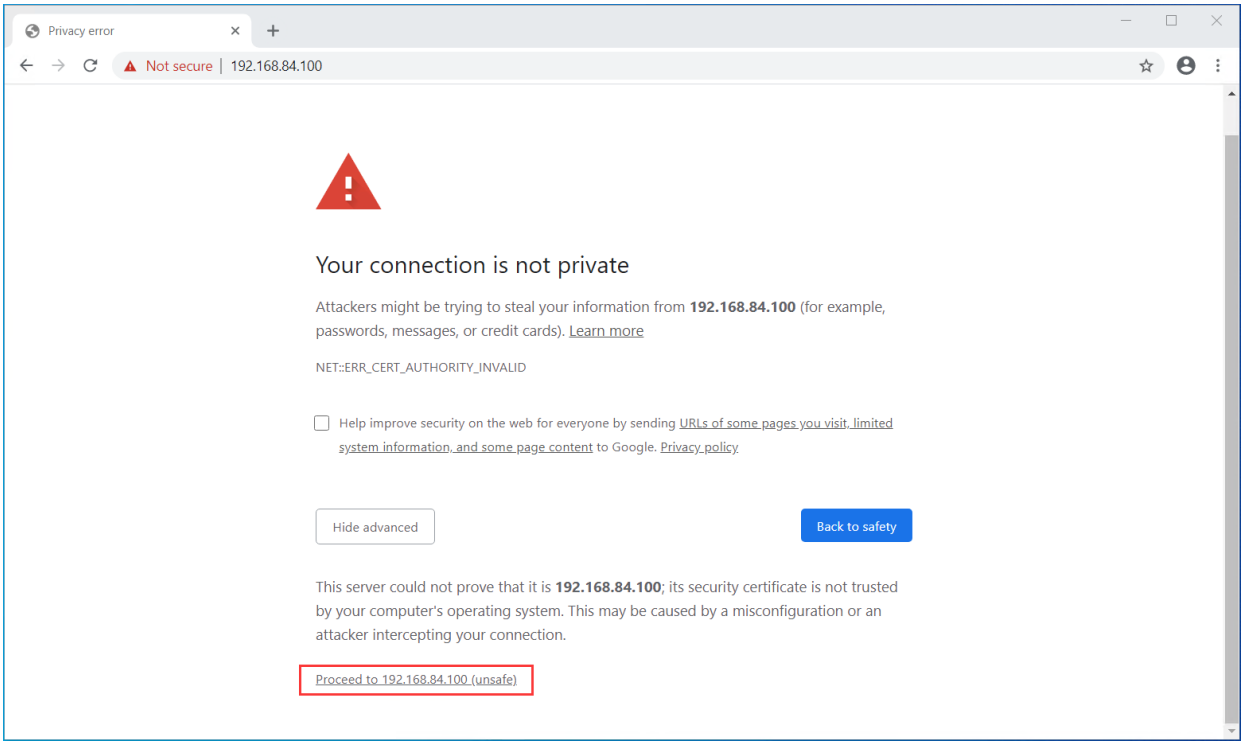
Database (Database Backup)

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

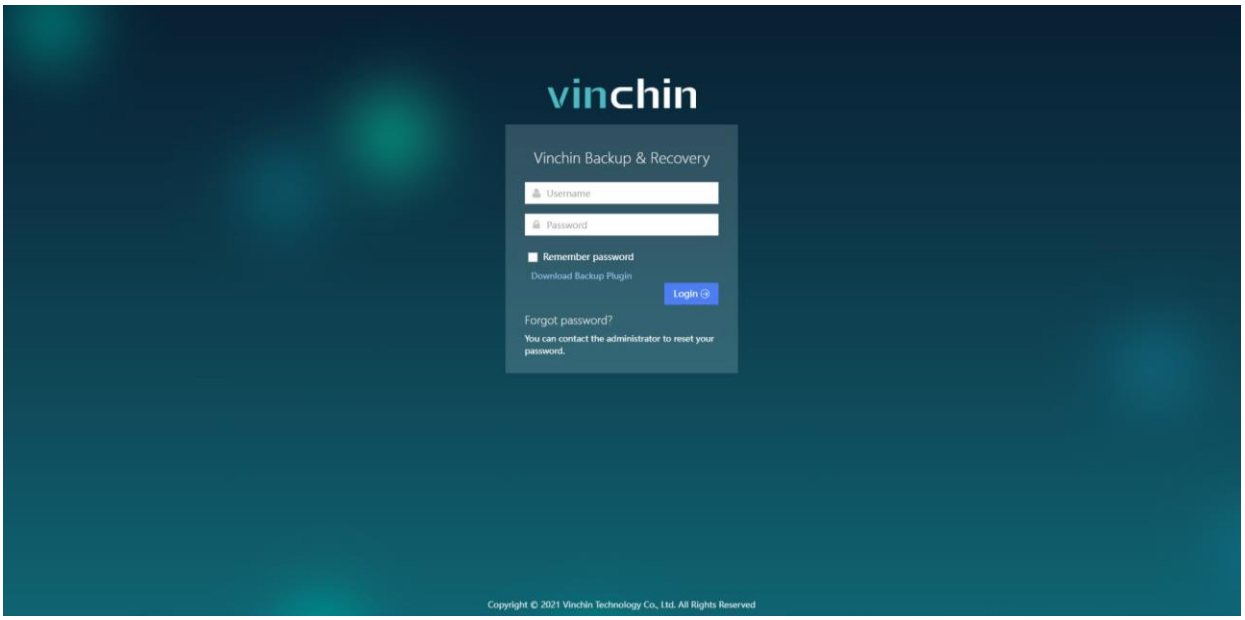
Getting Started

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.



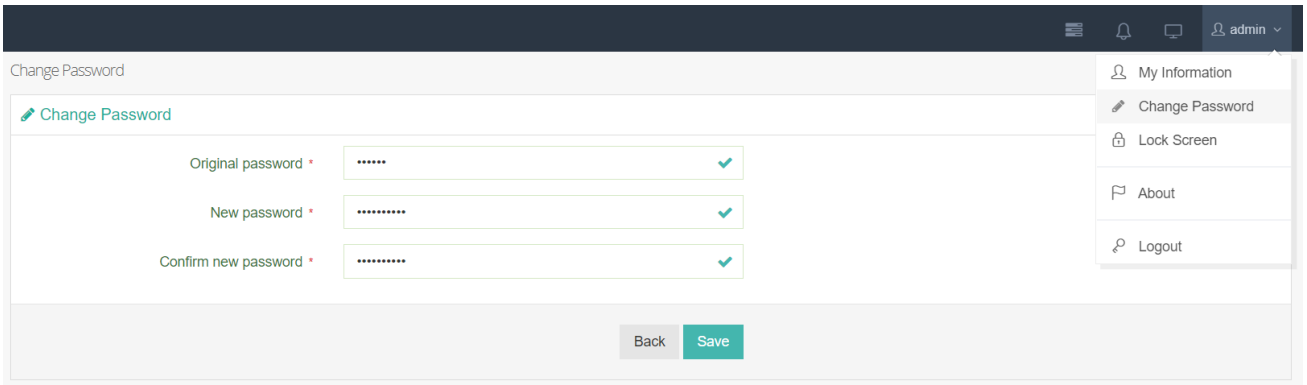
System Login

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:

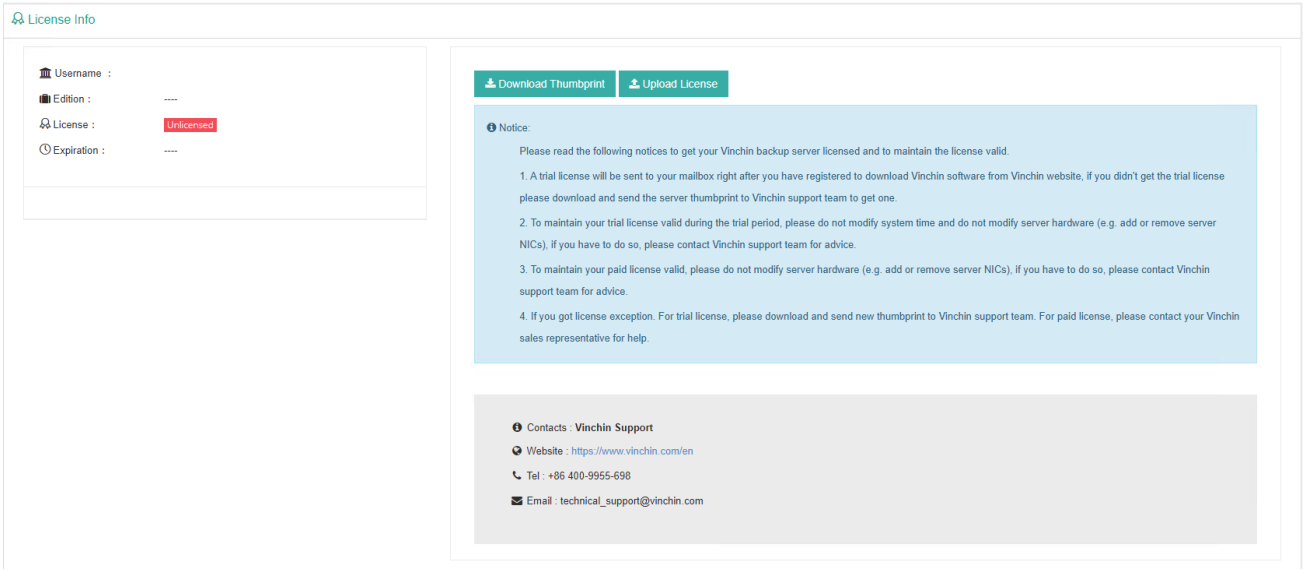
For operator/auditor user, please contact your administrator to reset your password.

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.

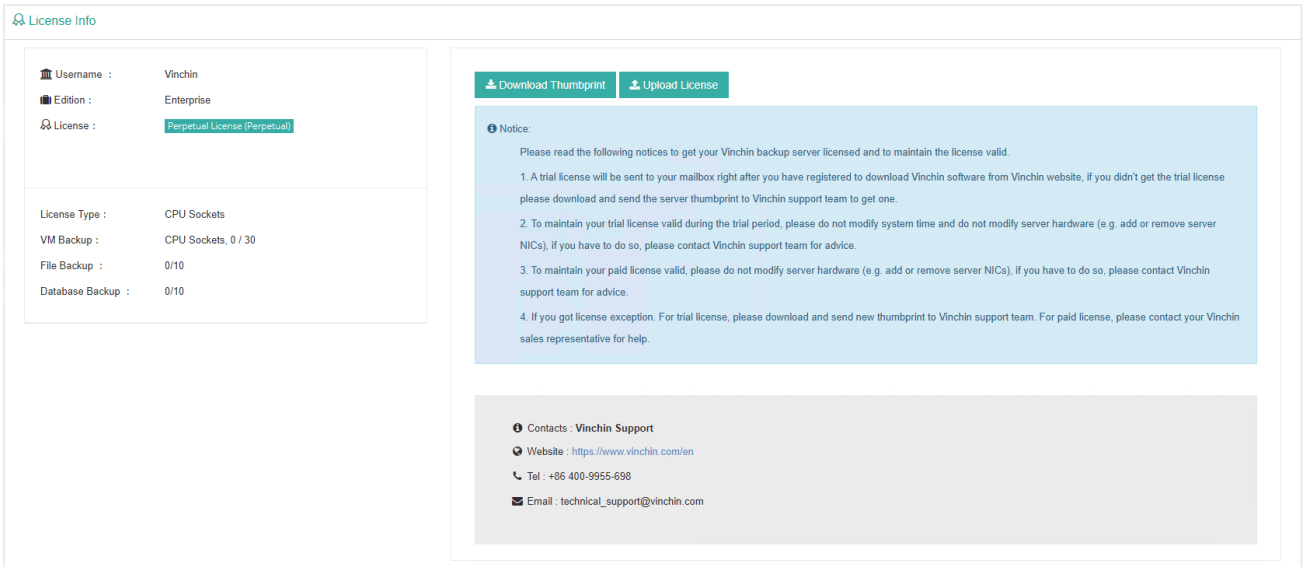
System License

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 trial 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**.

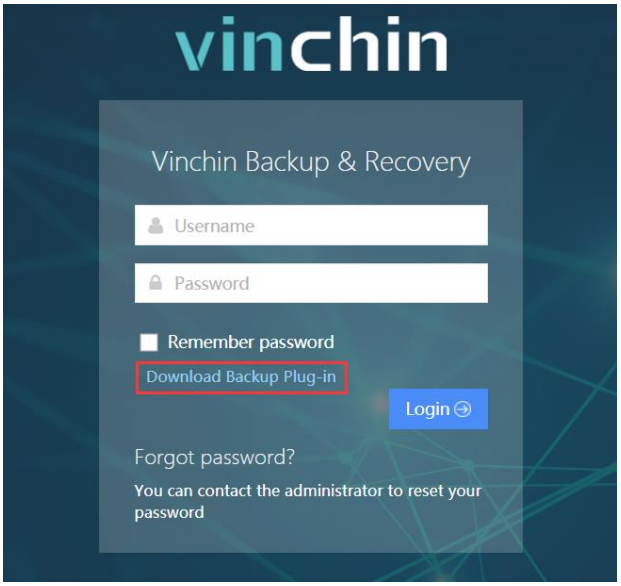
The number of licensed virtual infrastructure CPU sockets for VM backup, the number of licensed hosts for file backup and the licensed hosts for database backup will be given in “used/licensed” format. The actual license info depends on the order you have placed.

Install Backup Plugin

For VMware vSphere, Huawei FusionCompute(KVM) OLVM 4.4.8 and RHV/oVirt (4.4.7 or higher versions), backup plugin installation on the hypervisor level is not required, so you can simply skip this chapter now.

For Microsoft Hyper-V, Citrix Hypervisor/XenServer, XCP-ng, Sangfor HCI, OpenStack, RHV/oVirt (4.4.6 or older versions), H3C CAS/UIS and OLVM 4.3 virtual platforms, backup plugin needs to be installed on corresponding virtual platforms' hosts (hypervisor level) for VM backup by Vinchin Backup Server v6.5.

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

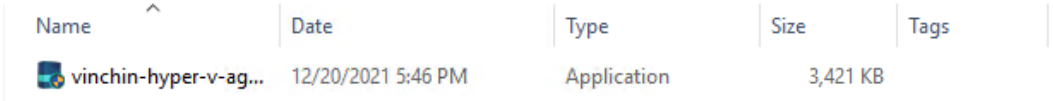


Click on **Download Backup Plug-in** to download the plugins for corresponding virtual platform. For detailed instructions of how to download and install backup plugins for your virtual platforms, please refer to the below corresponding explanations.

Hyper-V Backup Plug-in Installation

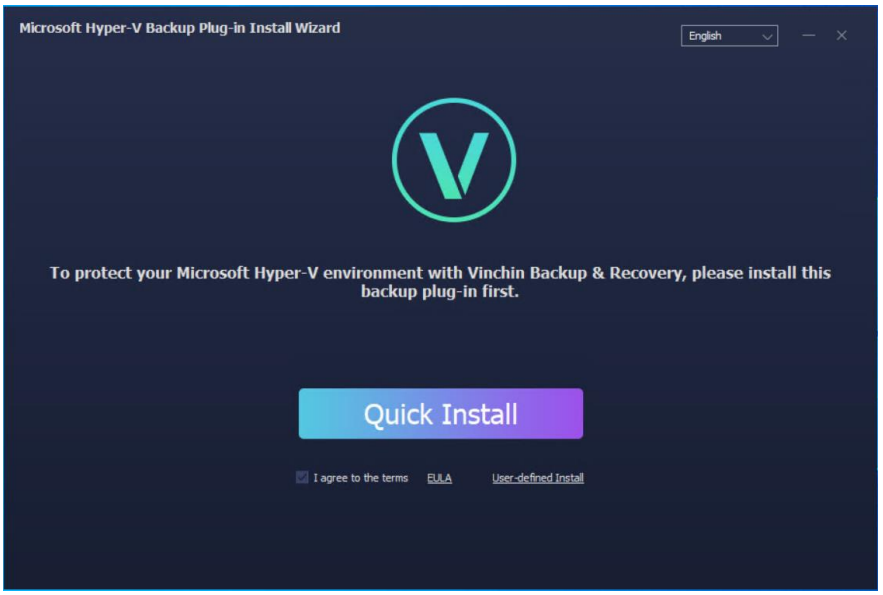
To download backup plugin for Microsoft Hyper-V, in the **Platform** dropdown list, please select **Microsoft Hyper-V**, then click on the **Download** button to download.

The downloaded backup plugin should be an executable exe file.



- Installation on Windows Server with Desktop Experience

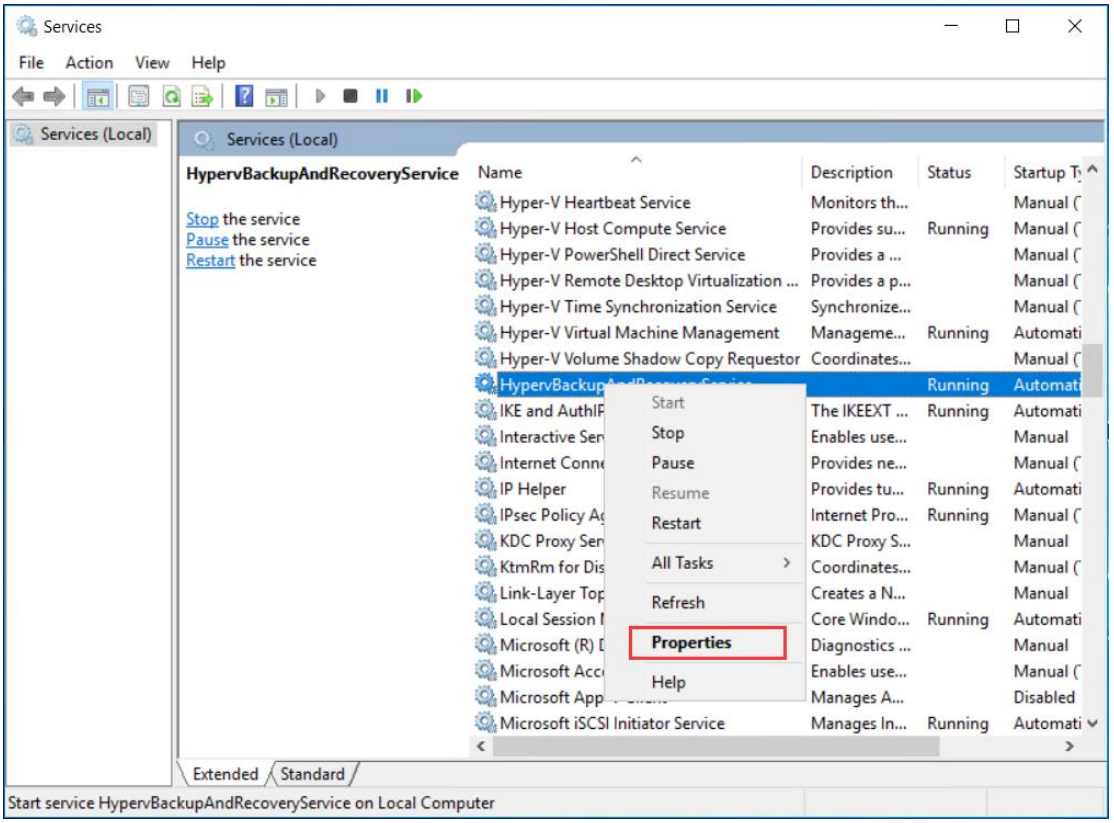
The downloading could be done directly on Hyper-V host and SCVMM server, right click to run the installer with administrator privileges (In SCVMM environment, please use SCVMM domain user to install the backup plugin on both Hyper-V host and SCVMM server).



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

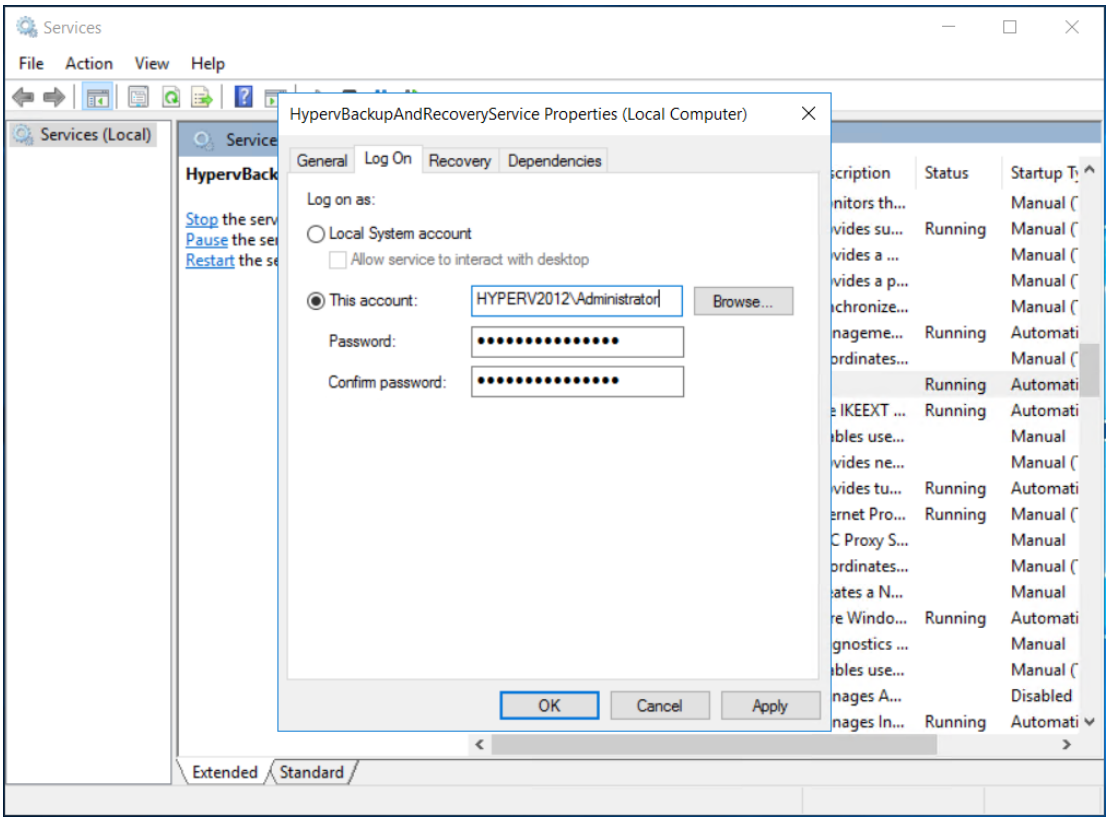
In case of a Failover Clustering environment, you also need to modify the Backup Plugin service's login permission as a domain user with local administrator privileges, and then restart the Backup Plugin services.

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

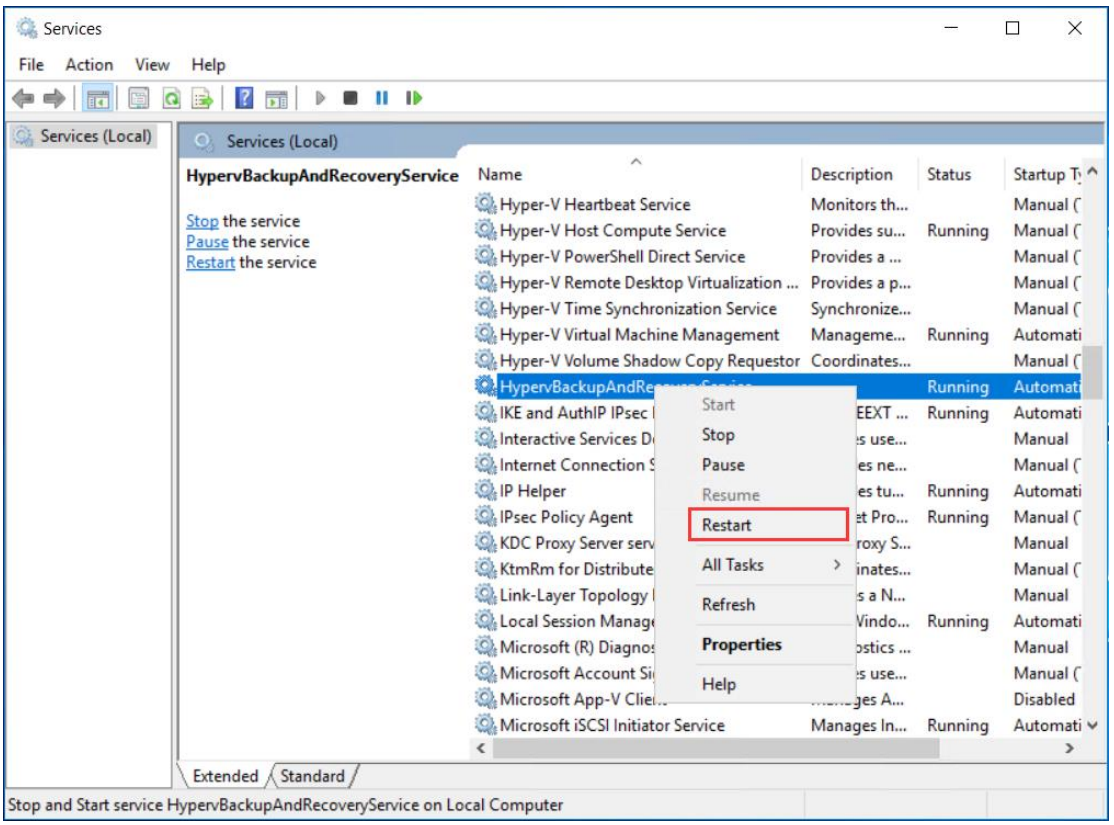


Find the **HypervBackupAndRecoveryService** in the Services Manager, right click on this service and select **Properties**.

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.

“file_name1” should be the exact backup plugin installer file name, in this case it should be “vinchin-hyper-v-agent.windows.6.5.0.15363.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.6.5.0.15363.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
```

Citrix Hypervisor/XenServer Backup Plugin Installation

To download backup plugin for Citrix Hypervisor/XenServer, in the **Platform** dropdown list, please select **Citrix XenServer/Citrix Hypervisor**, 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-6.7.0-19890.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 Plugin 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 an 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-6.7.0-19890.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 Plugin 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-6.7.0.19890-Debian.7-x86_64.tar.gz
```

Enter the backup plugin package folder.

```
cd vinchin-kvm-backup-patch-6.7.0.19890-Debian.7-x86_64
```

To install the backup plugin, run below command.

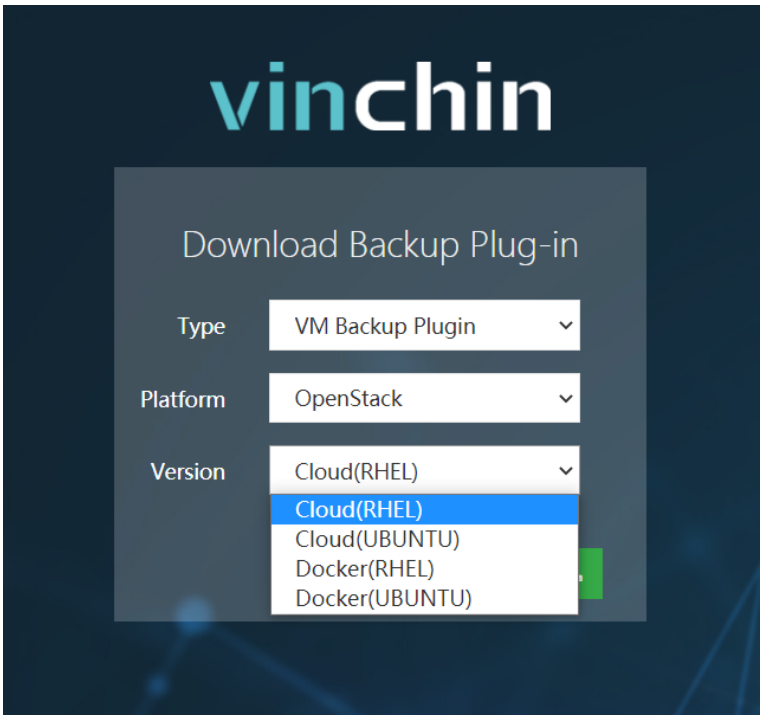
```
./kvm_backup_patch_install
```

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

```
./kvm_backup_patch_uninstall
```

OpenStack Backup Plugin 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 an 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 an 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-stack-patch-cloud-6.7.0.19890-1.el7.x86_64.rpm
```

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

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

Docker (RHEL) install.

```
rpm -i vinchin-stack-patch-docker-6.7.0.19890-1.el7.x86_64.rpm
```

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

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

Cloud (UBUNTU) install.

```
sudo dpkg -i vinchin-stack-patch-cloud-6.7.0.19890.Ubuntu.x86_64.deb
```

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

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

Docker (UBUNTU) install.

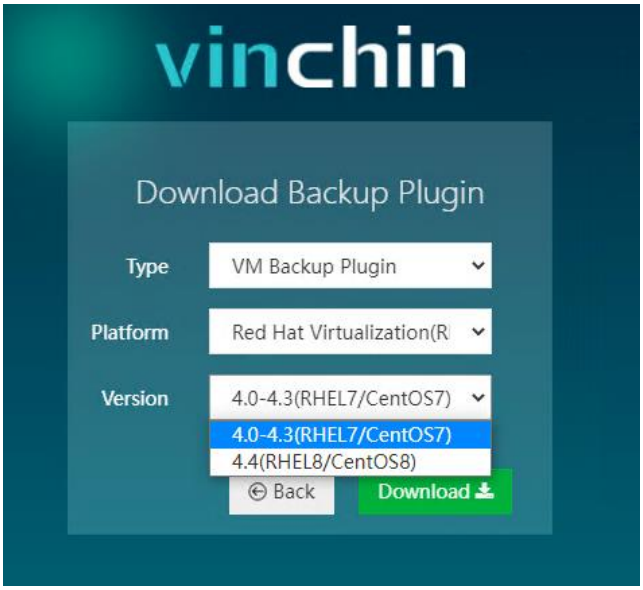
```
sudo dpkg -i vinchin-stack-patch-docker-6.7.0.19890.Ubuntu.x86_64.deb
```

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

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

Red Hat RHV/oVirt Backup Plugin Installation

To download backup plugin for Red Hat RHV or oVirt, in the **Platform** dropdown list, please select **Red Hat Virtualization (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 a RPM package.

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

```
yum install vinchin-stack-patch-cloud-6.7.0.19890-1.el7.x86_64.rpm
```

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

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

Warning

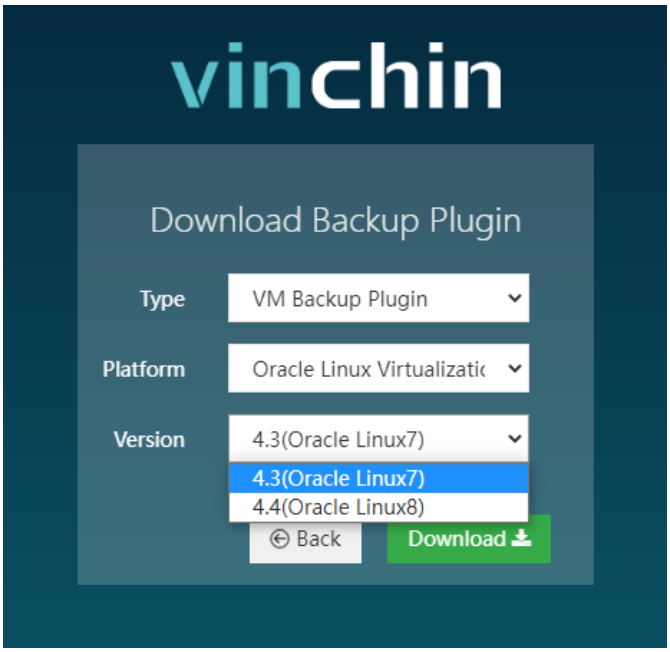
1. Backup plugin should not be installed on the RHV/oVirt Engine.

2. If you are running RHV/oVirt 4.4.7 or higher versions, you can use ImageIO API for VM backup and restore, backup plugin installation is not required, otherwise please install backup plugin on RHVH or oVirt Hosts.

3. Please use 'yum' command to install the backup plugin instead of 'rpm' command.

Oracle Linux Virtualization Manager (OLVM) Backup Plugin 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 an RPM 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 install the backup plugin.

```
yum install vinchin-stack-patch-cloud-6.7.0.19890-1.el7.x86_64.rpm
```

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

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

Warning

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

2. Please use 'yum' command to install the backup plugin instead of 'rpm' command.

H3C UIS/CAS Backup Plugin Installation

To download backup plugin for H3C UIS/CAS, in the **Platform** dropdown list, please select **H3C UIS/CAS**, 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 backup plugin should be a .tar.gz package.

Please upload the downloaded backup plugin to the H3C UIS/CAS 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 node hosts from Windows desktop, you can use WinSCP or PSCP, or any other methods that you are familiar with.

After uploading, enter the H3C 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-6.7.0.19890-RHEL.7-x86_64.tar.gz
```

Enter the backup plugin package folder.

```
cd vinchin-kvm-backup-patch-6.7.0.19890-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
```

ZStack Backup Plugin Installation

If your ZStack backend storage is Ceph, you could choose to run LAN-free backup without installing backup plugin on the ZStack hosts, otherwise please follow the below steps to install backup plugin.
To download backup plugin for ZStack, in the **Platform** dropdown list, please select **ZStack Cloud**, 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 backup plugin should be an RPM package.
Please upload the downloaded backup plugin to the node hosts (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 ZStack 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 ZStack node command line interface and enter the directory where you uploaded the backup plugin, and then use below command to install the backup plugin.

```
yum install vinchin-stack-patch-cloud-6.7.0.19890-1.el7.x86_64.rpm
```

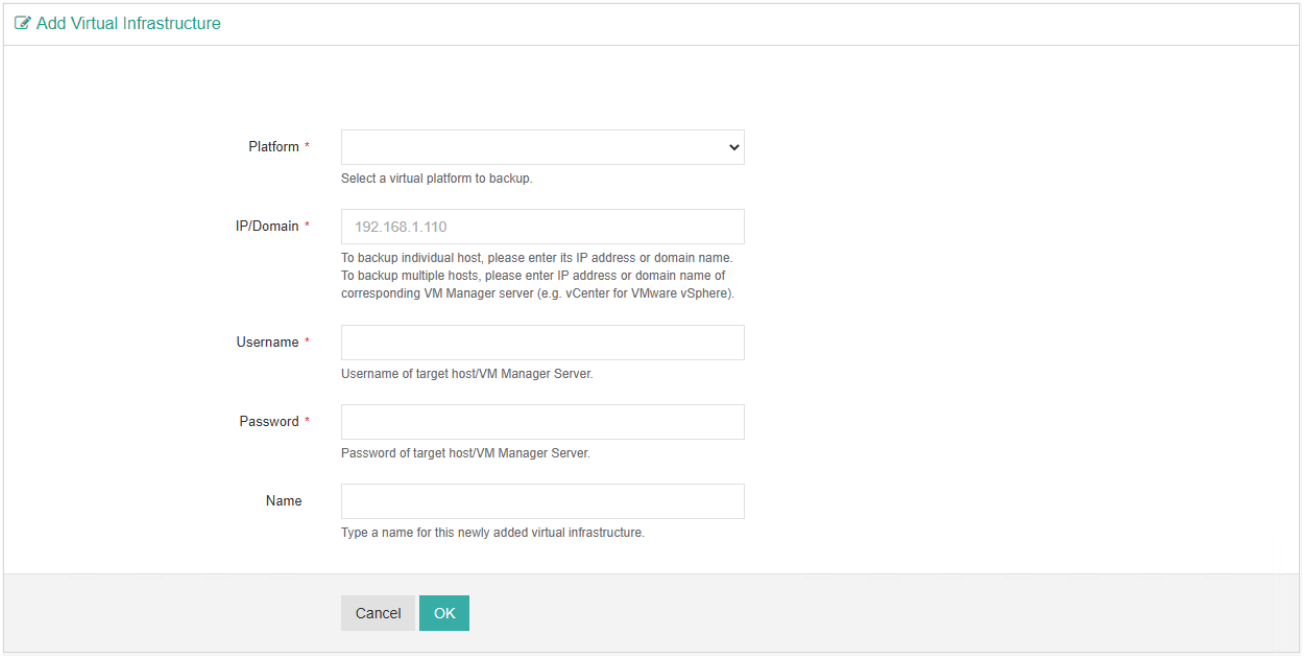
Use below command to uninstall (once uninstalled, backup/restore jobs will fail).

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

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.

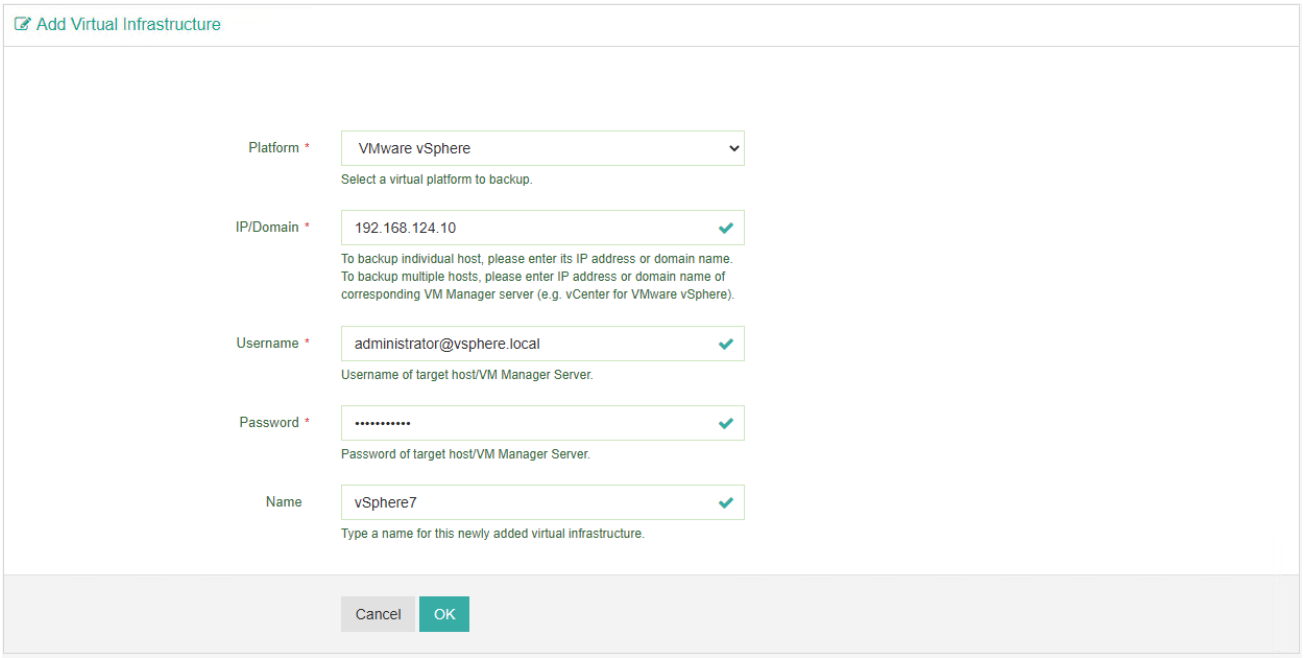
Go to **VM Backup** > **Virtual Infrastructure** page. And click on Add button to add a virtual platform to the Backup Server.



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**.



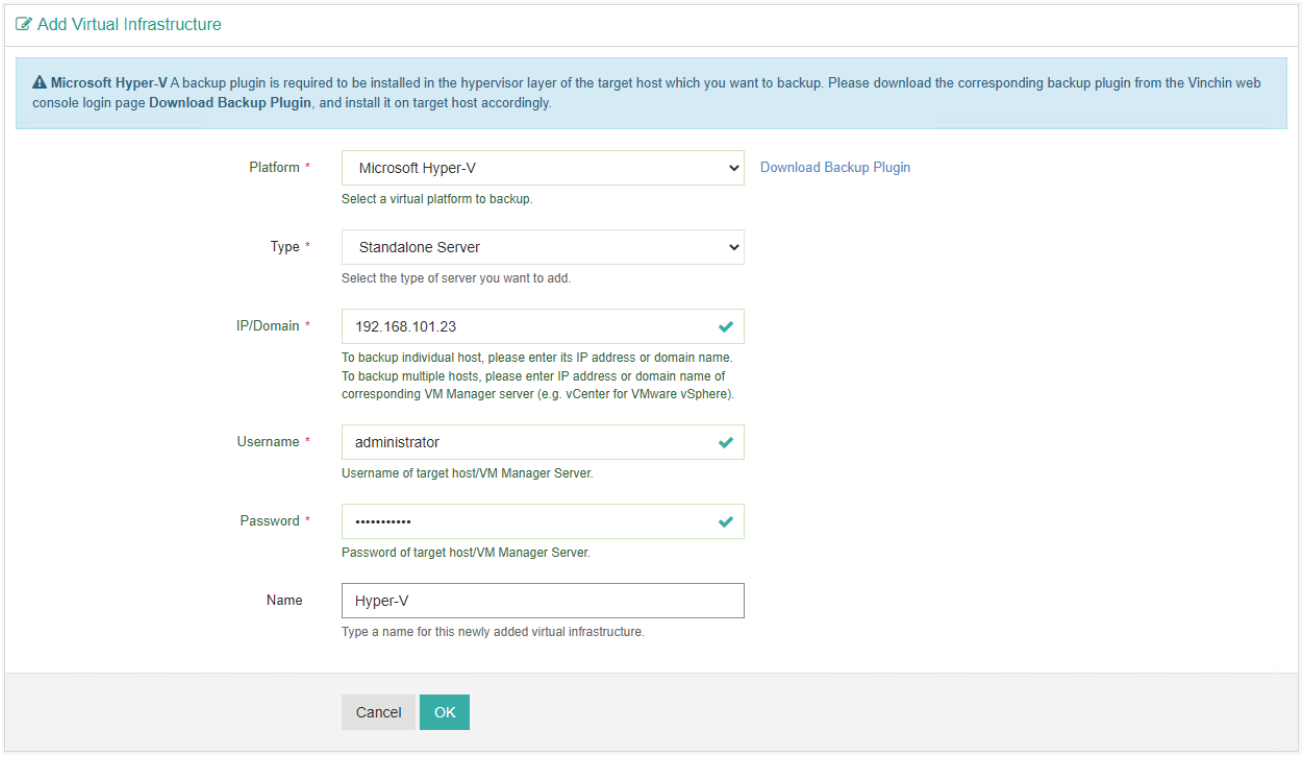
In the **IP/Domain** field, please type in the IP address of the vCenter server. Or if you are using standalone ESXi server, please type in the IP address of the ESXi server.

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.

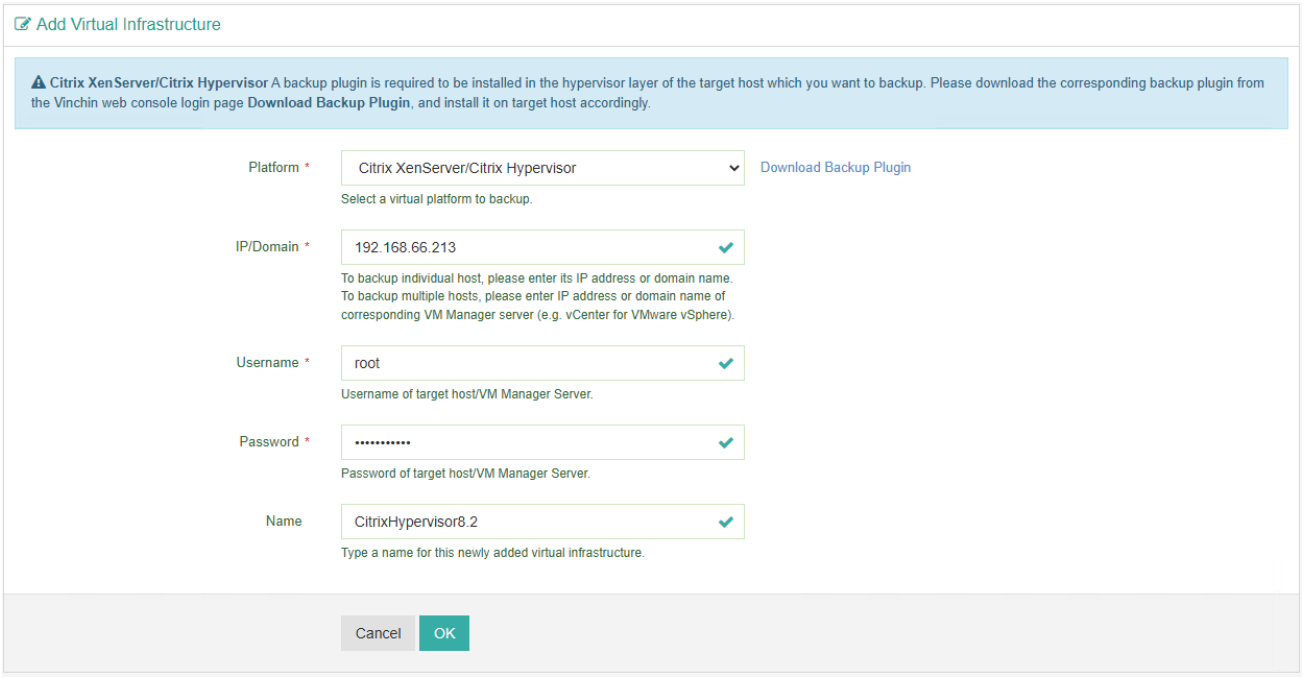
In the **Username** field, enter the domain user with administrator permissions of the SCVMM server and all other hosts if your Hyper-V virtual infrastructure is managed by a SCVMM management server; enter the domain user with local administrator permissions of all clustered hosts if it's a failover 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 Hypervisor/Citrix XenServer/XCP-ng Virtual Platform

If you are using Citrix Hypervisor/XenServer or XCP-ng virtual platform, in the **Platform** dropdown list, please select **Citrix XenServer/Citrix Hypervisor** or **XCP-ng** accordingly.

The principle of registering Citrix XenServer/Citrix Hypervisor and XCP-ng to Vinchin Backup Server is the same, below is an example of registering Citrix Hypervisor 8.2 to Vinchin backup server, XCP-ng should be registered the same way.



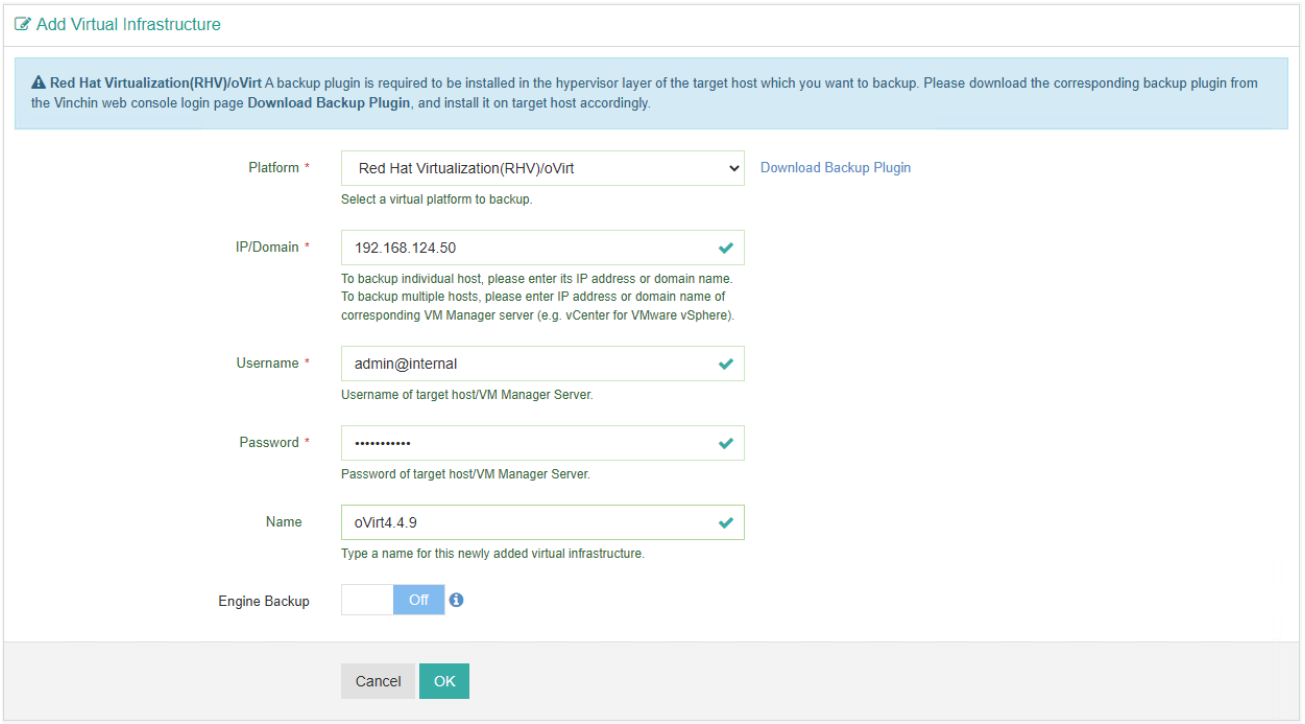
In the **IP/Domain** field, the IP address of the pool master should be used.

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 RHV or oVirt, please select **Red Hat Virtualization(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 oVirt as an example.



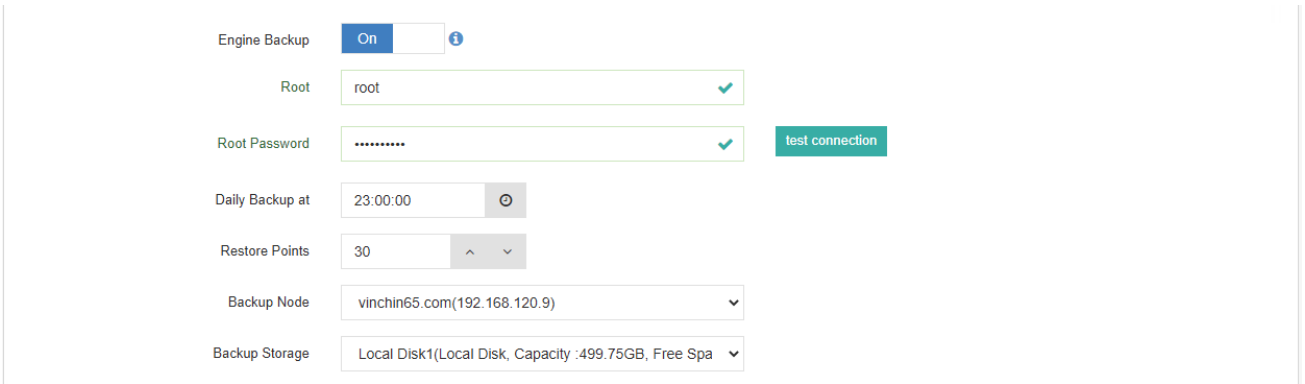
In the **IP/Domain** field, the IP address or domain name of the oVirt engine should be used.

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.

If it’s a fresh new installation of oVirt 4.5.1 virtual environment, Keycloak is configured as a default SSO provider for oVirt Engine, you should use “admin@ovirt@internalsso” as the username. Upgrading from older versions to oVirt 4.5.1 does not change the username.

In the **Password** field, please type in the password for admin that you specified during the installation.

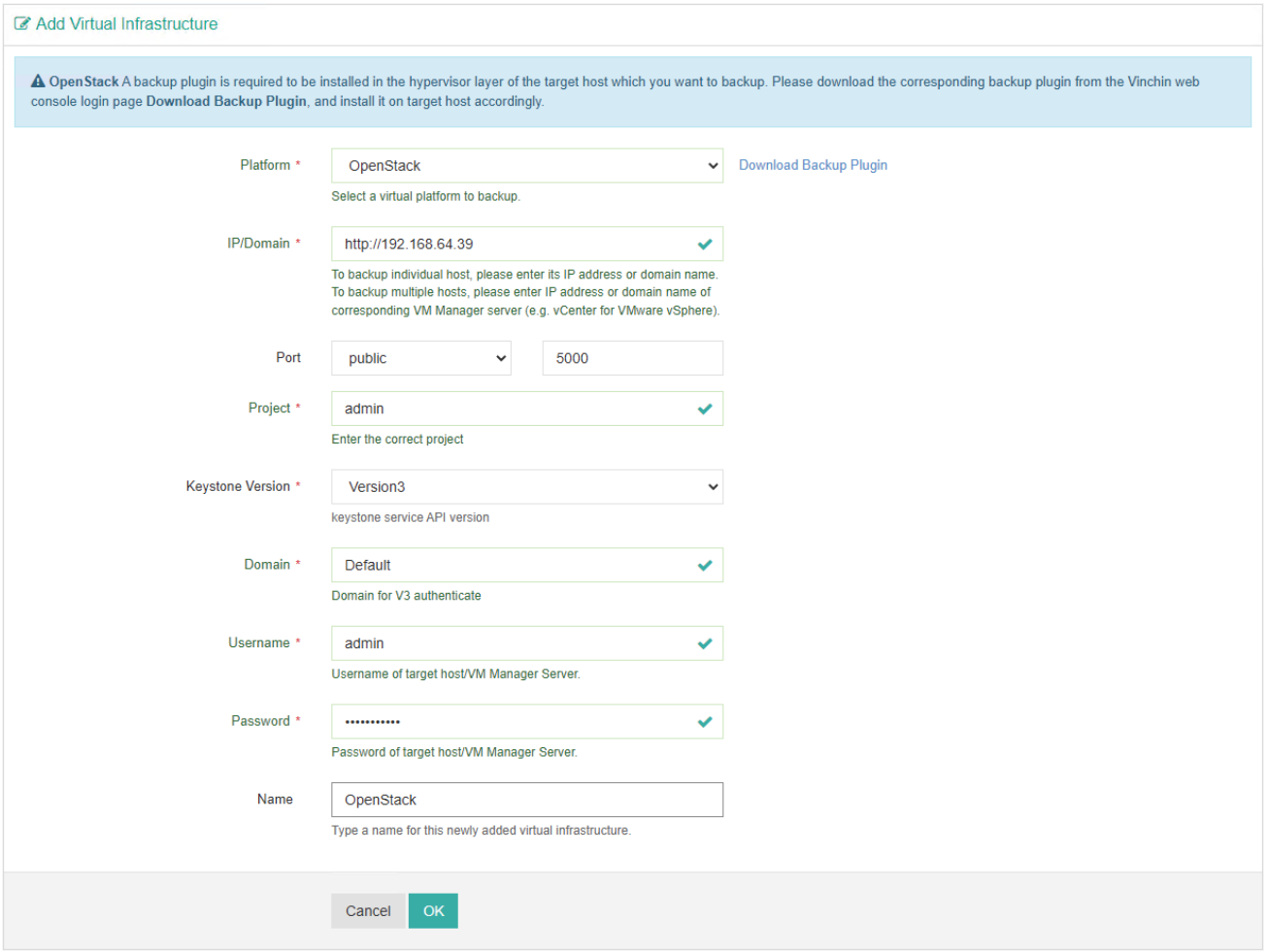
As for **Engine Backup**, it is used to backup the oVirt engine metadata. To enable engine backup, you need to use root permission of the oVirt engine.



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”.

In the **Port** field, you may need to use the Public API endpoint, and please use the default port number, otherwise you need to check the keystone identity services to determine the port number.

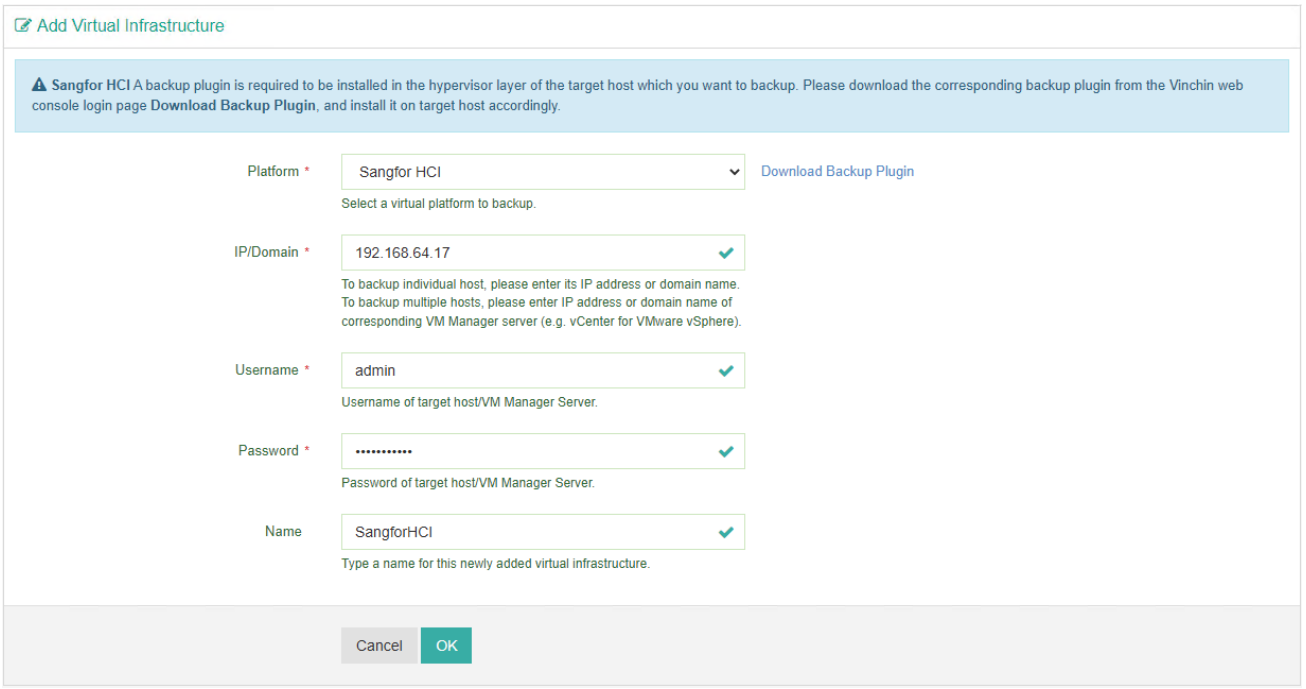
In the **Project** field, enter a project name which its VMs need to be backed up.

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.

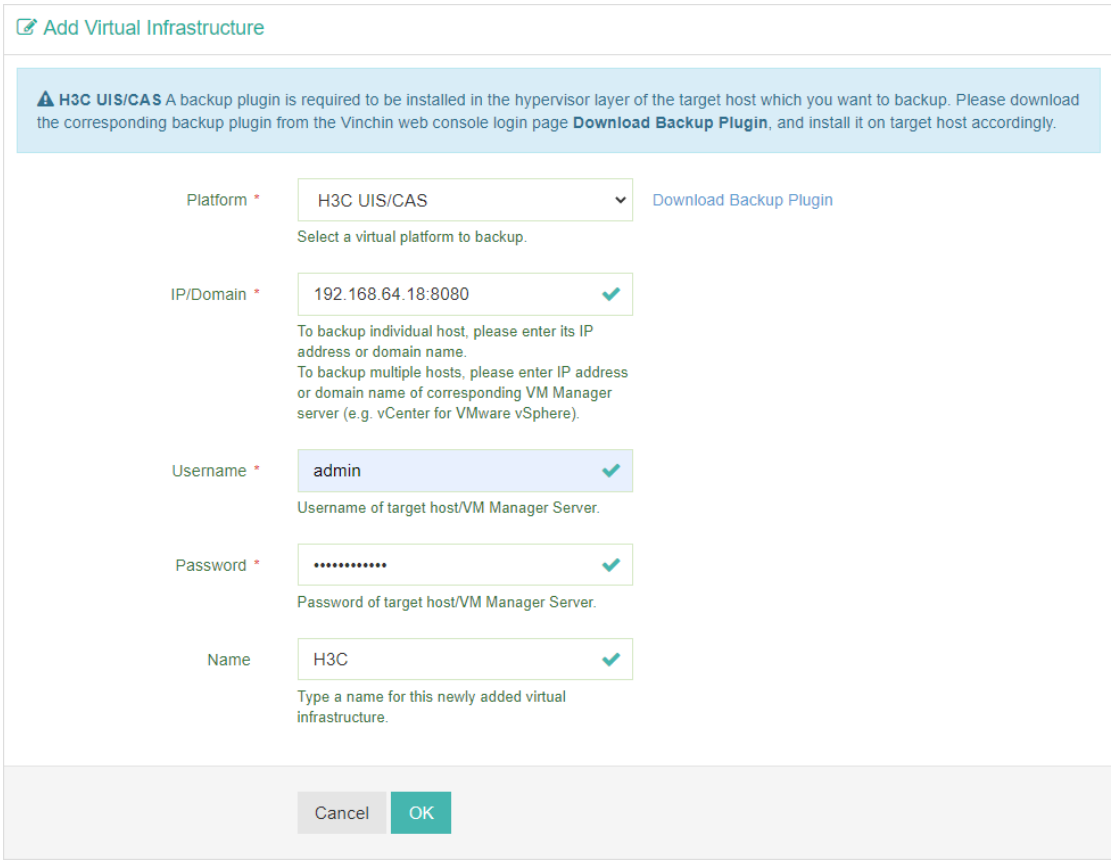
In the **Username** and **Password** fields, type in the super admin user name and password.

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

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

Add H3C UIS/CAS Virtual Platform

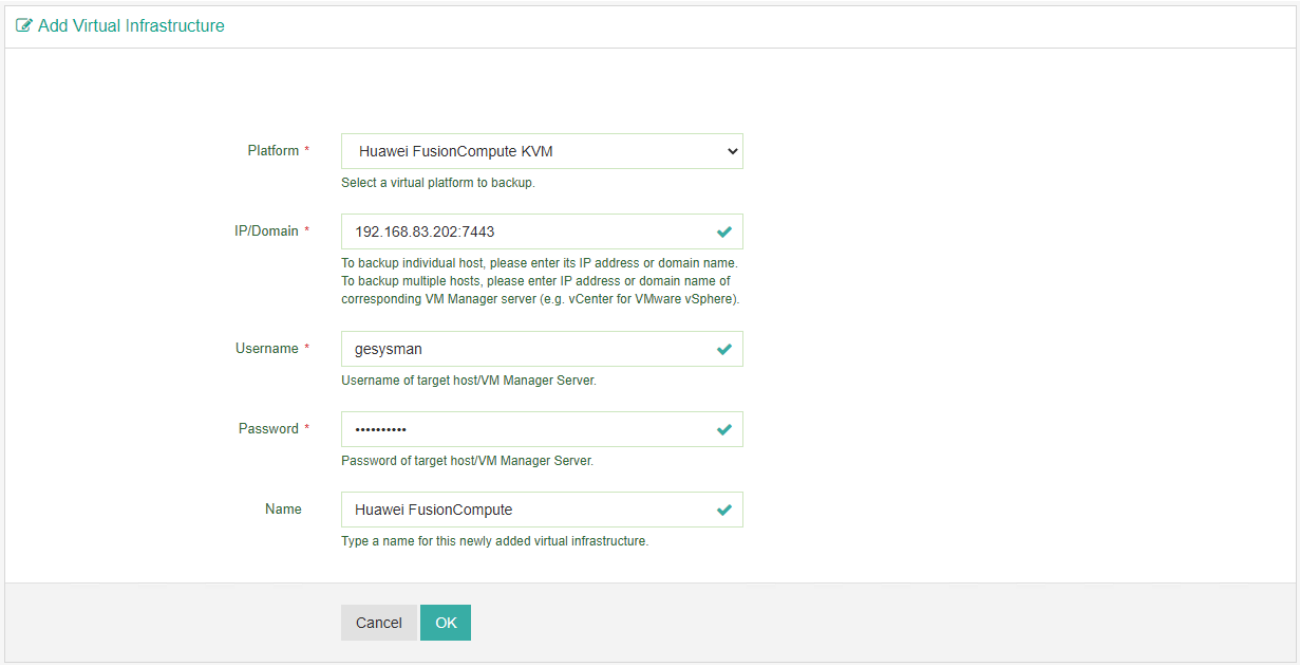
To add H3C UIS/CAS, in the **Platform** dropdown list, please select **H3C UIS/CAS**, then complete the below settings.



In the **IP/Domain** field, please type in the IP address of the H3C UIS/CAS server (e.g., *server-ip*:**8080**).
In the **Username** and **Password** fields, type in the administrative user's name and password.

Add Huawei FusionCompute Virtual Platform

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



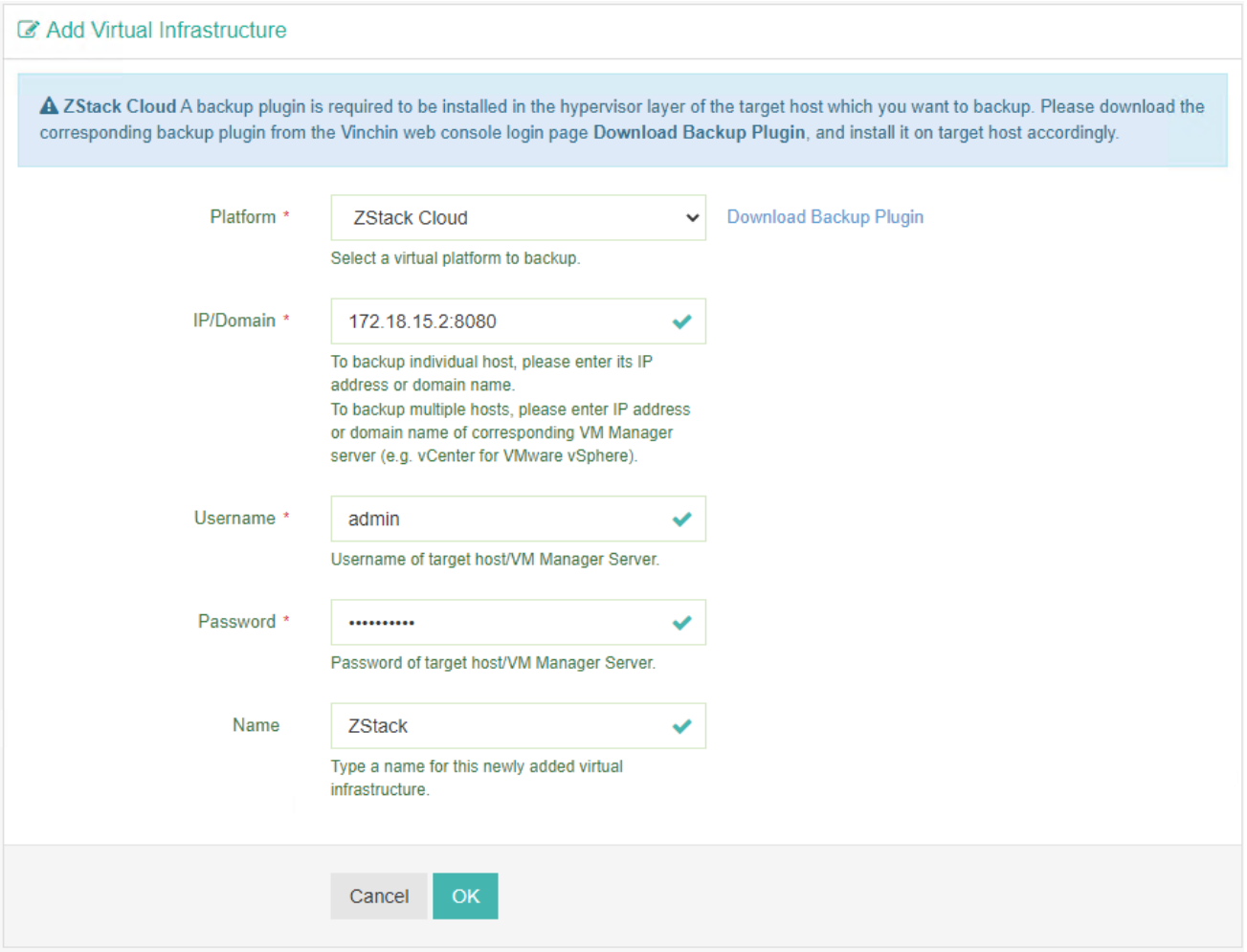
In the **IP/Domain** field, type in the IP address and port number of the FusionCompute Virtual Resource Manager (VRM) server, e.g., server_ip:7443.

In the **Username** field, the northbound interface authentication account should be used, the default username used by FusionCompute is “gesysman”.

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

Add ZStack Cloud Virtual Platform

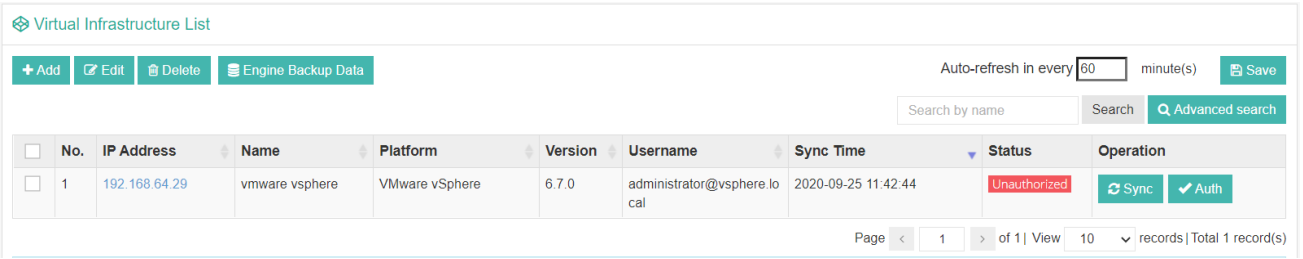
To add ZStack Cloud virtual platform, in the **Platform** dropdown list, please select **ZStack Cloud**, then complete the below settings.



In the **IP/Domain** field, please type in the IP address of the ZStack management node (e.g., *server-ip*:**8080**).
In the **Username** and **Password** fields, type in the administrative user's name and password.

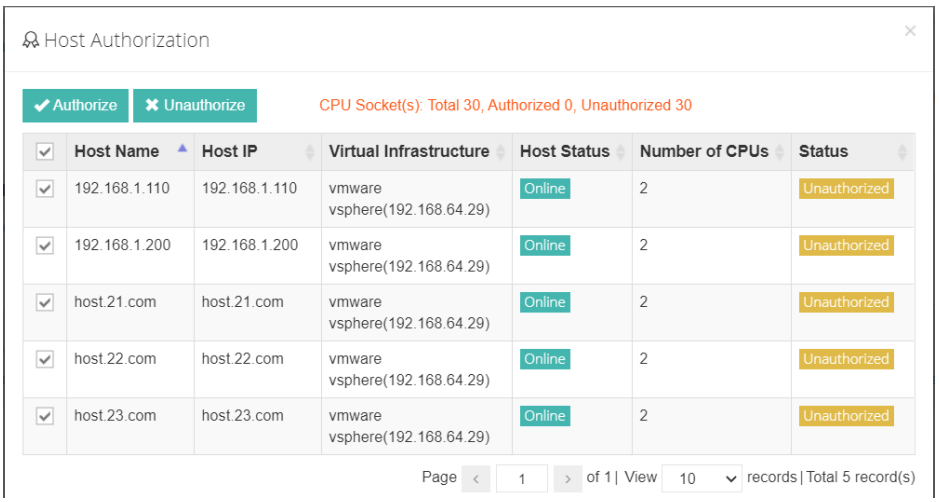
Authorize Virtual Infrastructure

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

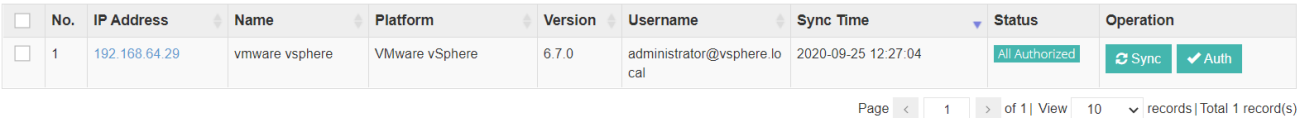


If your license type is per CPU socket, then the virtual infrastructure status will be **Unauthorized**, you are unable to perform backups with unauthorized virtual infrastructure. If your license type is per virtual machine or per GB storage capacity, then the virtual infrastructure status will be **Authorized** and you don't have to manually authorize the virtual infrastructure.

To authorize the virtual infrastructure for Vinchin Backup Server to backup 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**. Now you should be able to backup the VMs on the authorized hosts.

Note

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

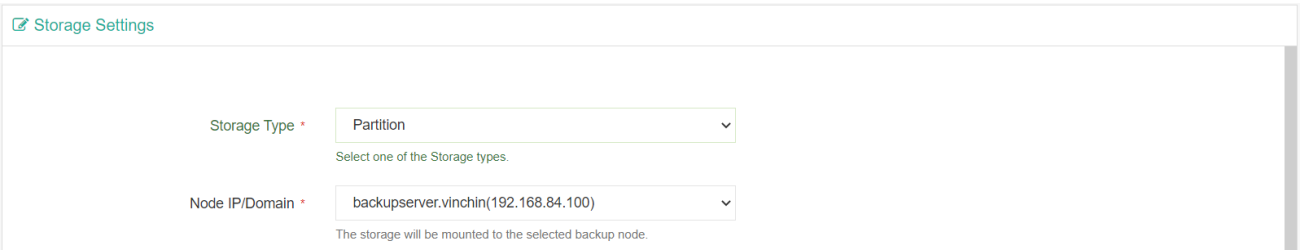
2. It is recommended to get all hosts authorized within the virtual infrastructure, in case the VMs with HA enabled might automatically migrate from host to host, if the VM migrated to unauthorized host, the backup job might fail.

3. VM backup requires the virtual infrastructure to be authorized (licensed), VM restore does not require virtual infrastructure to be authorized.

Add Storages

A backup storage 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, logical volume, Fibre 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

- **Disk Partition**

An unmounted local partition on the Backup Server or Backup Node can be used as Backup storage, Backup Copy storage and also Backup Archive storage.

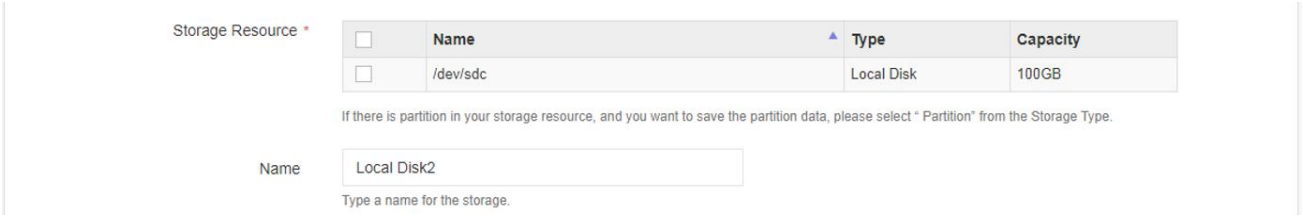
To add a partition as backup/copy/archive storage, please select on which node the partition exists.

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**

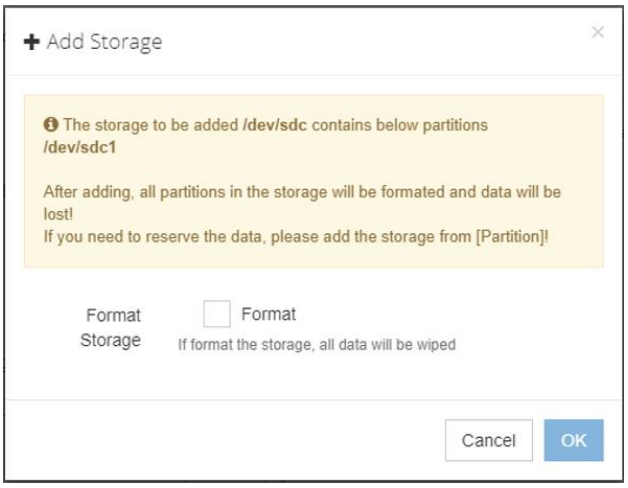
An unpartitioned local disks on the Backup Server or Backup Node can be used as Backup storage, Backup Copy storage and also Backup Archive storage.

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**.



- **Logical Volume**

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.

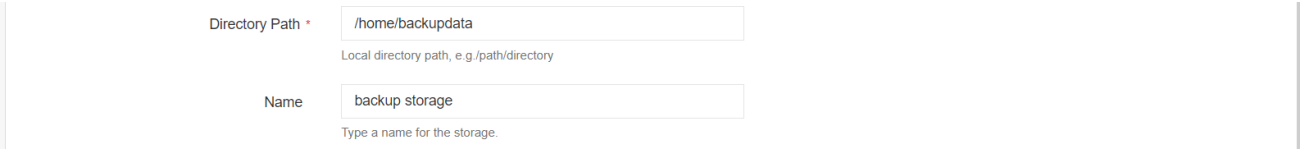
- **Local Directory**

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
```

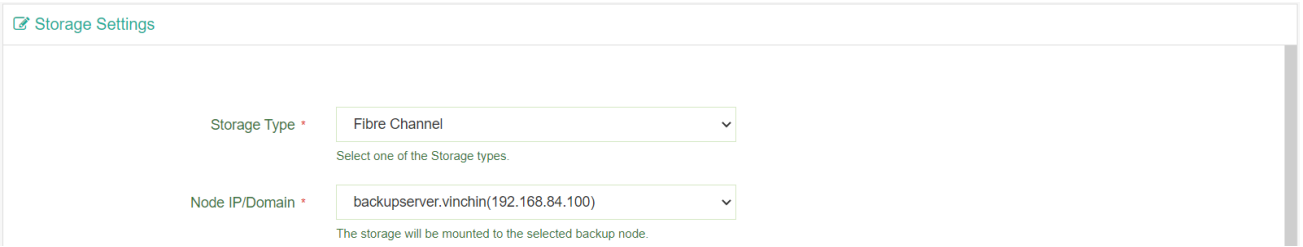
Then to add it as below.



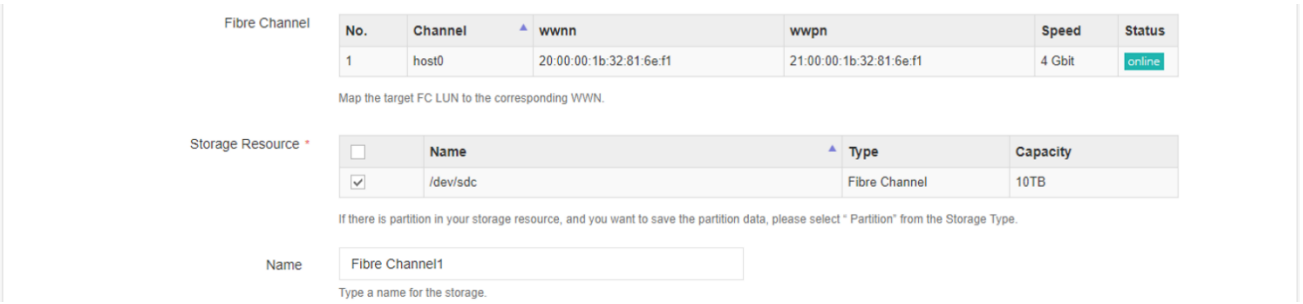
In the **Directory Path** field, please type in the full path of the directory you have created.

- **Fibre Channel**

To add Fibre Channel 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 fibre channel and the wwpn of the HBA interface card, use this information to map the LUN of the FC storage to Vinchin Backup Server. After this, add the FC storage again, and Vinchin Backup Server will detect the mapped LUN storage.

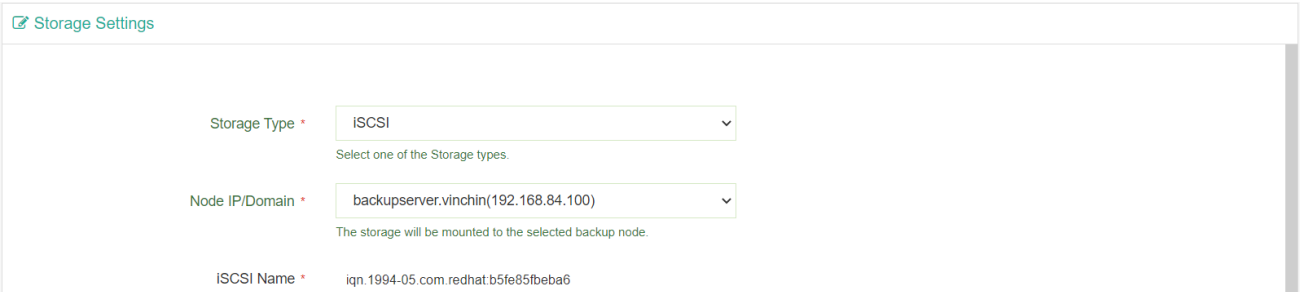


Note

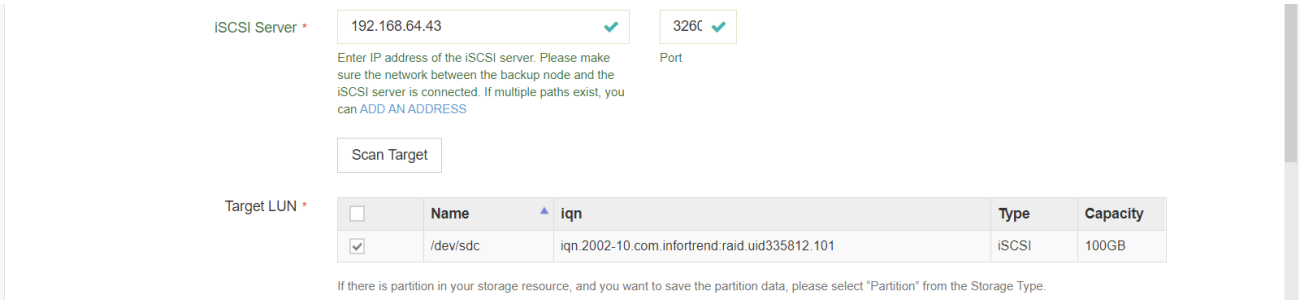
To add FC storage, the added LUN will be formatted, all data in the LUN will be erased. If there's previous backup data in the LUN and you don't want to format it, please add this storage as Partition and then import the existing backup data.

- **iSCSI**

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



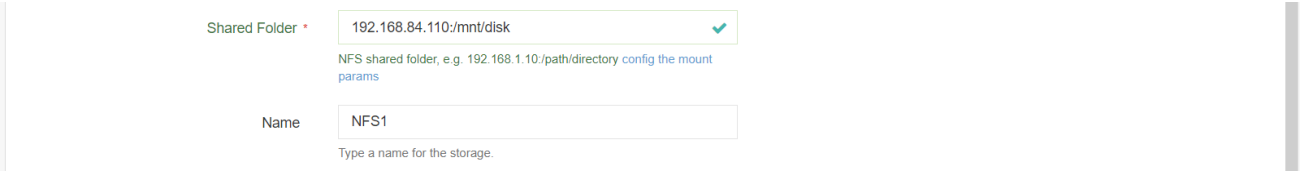
Please use the IQN to map the LUN of the iSCSI storage to the backup server from the iSCSI storage server. After this, input the iSCSI storage server IP address here and click on **Scan Target** button to scan the target storage.



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 **Shared Folder** field.



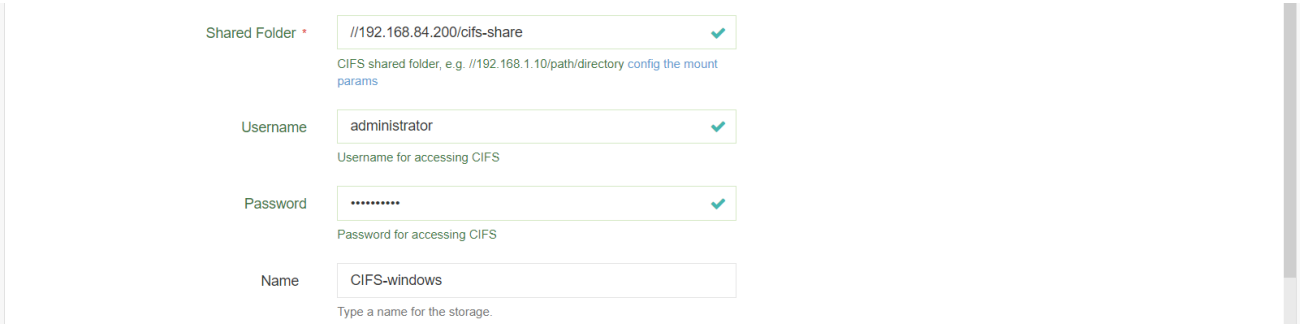
If you had difficulty to add an NFS share to Vinchin backup server, please make sure Vinchin backup server has write permission to the NFS share.

And by default, Vinchin backup server will mount the NFS share using NFS protocol version 3.0, if your NFS server runs other protocol version, please click on “config the mount params” and in the Mount Params field fill in another version like “vers=2.0”.

While adding an NFS share, 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 username and password of the user on the CIFS storage server, who shared this storage.

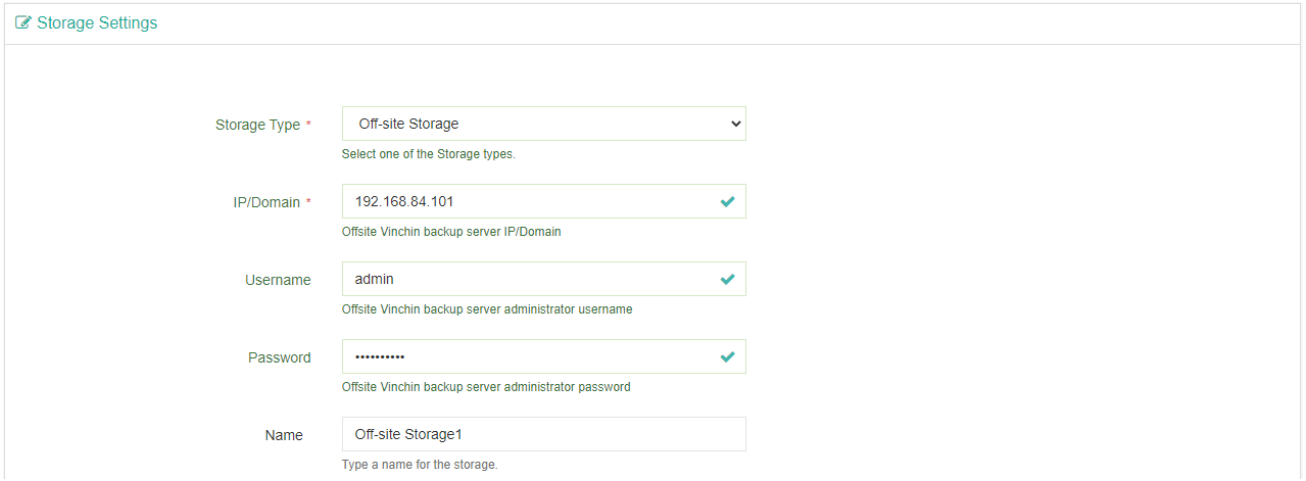
By default, Vinchin backup server will mount the CIFS share using CIFS protocol version 3.0, if your CIFS server runs other protocol version, please click on “config the mount params” and in the Mount Params field fill in another version like “vers=2.0”.

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

- **Off-site Storage**

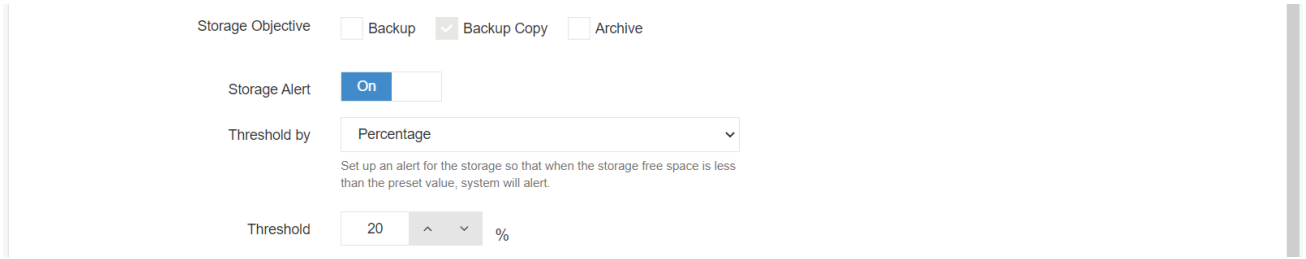
An off-site storage is another Vinchin Backup Server in another location, it is used as Backup Copy storage only. By using off-site storage, you can save remote backup copy to secure the backup data from any possible site disasters. Before adding an off-site storage, please make sure another Vinchin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

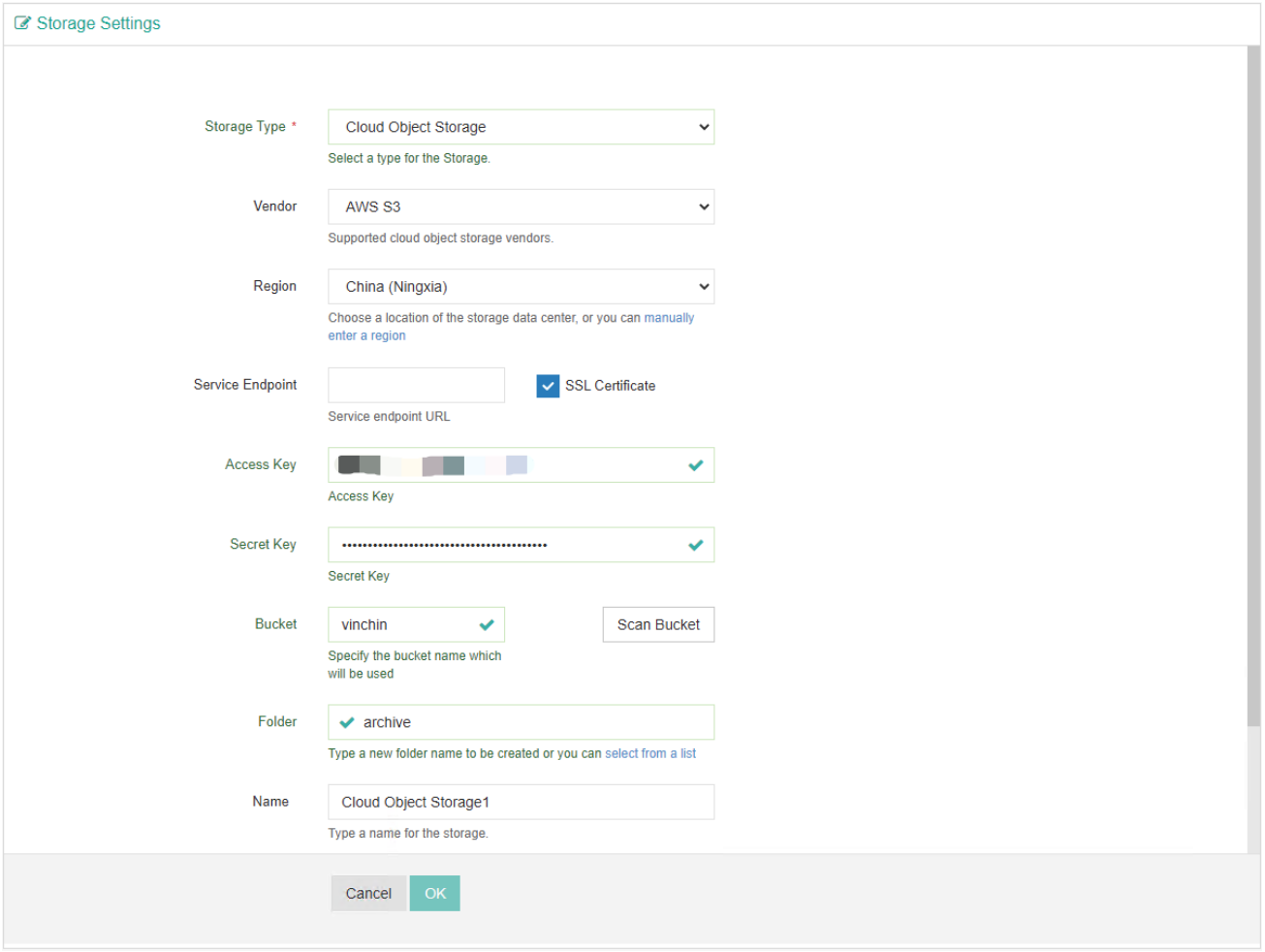
If you are connecting the remote off-site storage over Internet, please open TCP port 30050 and 30051 on the remote site router or firewall.

- **Cloud Object Storage**

Cloud storage is used for archiving the backup data only. Vinchin Backup Server v6.5 now supports the following Cloud Object storages:

- Amazon AWS S3 cloud storage
- MS Azure Blob storage
- Alibaba cloud storage
- Huawei cloud storage
- Tencent cloud storage
- Wasabi cloud storage
- MinIO object storage
- Ceph S3 object storage

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



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

In the **Region** dropdown list, please select the region which you want to connect to.

The **Service Endpoint** field is optional, if you need to specify the service endpoint URL, and if it's SSL enabled, please enable **SSL Certificate** option, and input the URL without "https://".

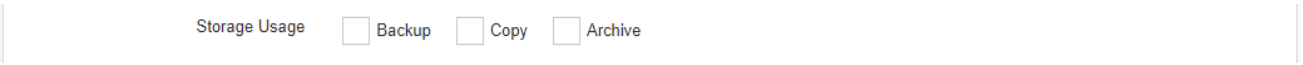
In the **Access Key ID**, **Secret Access Key** and **Bucket Name** fields, please enter the credentials provided by Amazon AWS S3.

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.

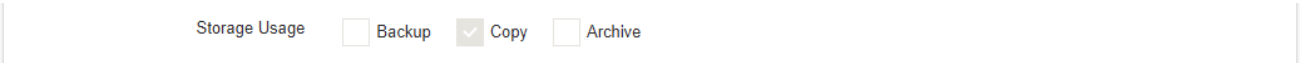
After scanning, if there are existing folders in the bucket, you are able to select from the **Folder** dropdown list. The selected folder will be used to save the backup archive data. If you want to create a new folder for backup archive data, you can manually type a new folder name here, once you confirm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

Storage Usage

For the storage types: disk partition, local disk, local directory, logical volume, Fibre Channel(FC), iSCSI, NFS share and CIFS share. The usage 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.

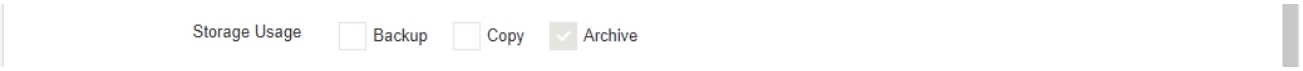


For the Off-site Storage, it is another remote/off-site Vinchin Backup Server, and it can be only used as Backup Copy (off-site) storage.



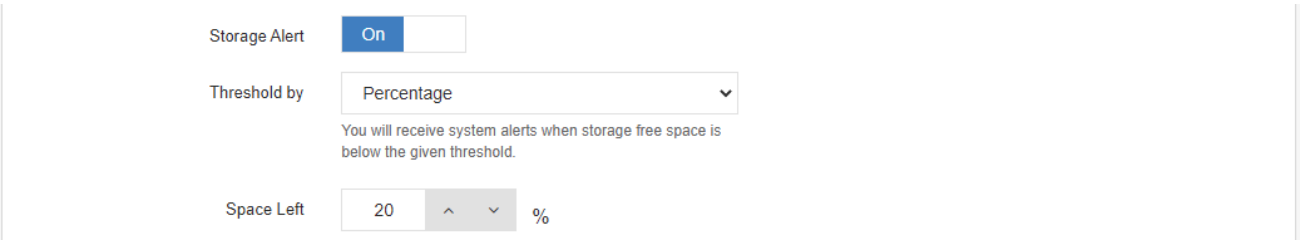
When you add the off-site storage, Backup Copy will be selected by default, and you cannot change the storage usage.

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.



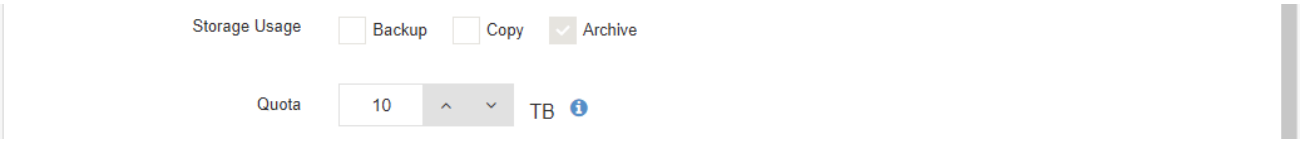
Usage Alert

For the storage types: disk partition, local disk, local directory, logical volume, Fibre Channel (FC), iSCSI, NFS share, CIFS share 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, you can configure the storage quota to limit the storage capacity usage, see the figure below.

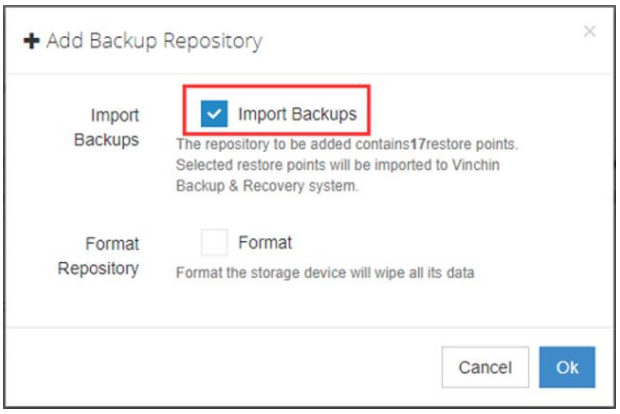


You only have to specify the quota of data size allowed to be uploaded to the cloud storage, then Vinchin Backup Server will alert you when you are running out of the quota.

Data Importing and Storage Formatting

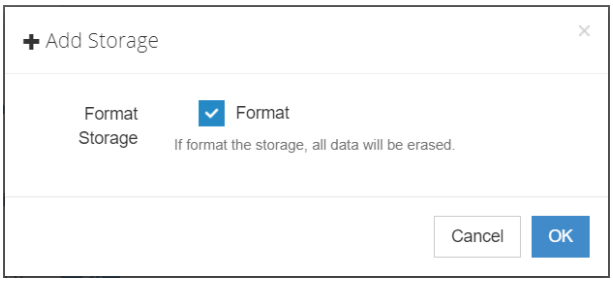
For the storages to be added, if once they had been used by Vinchin Backup Server, the backup/copy/archive data should still remain on them. When you try to add them again, the data will be automatically recognized by Vinchin Backup Server.

For the block storages disk partition, local disk, logical volume, Fibre Channel(FC), iSCSI, you have options to import the backup data or to format the storage. See the figure below.

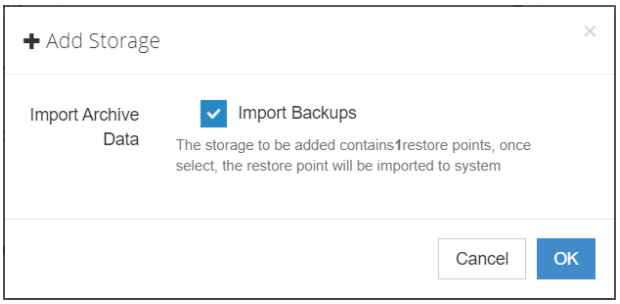


It is recommended to import the backup data and then add it to Vinchin Backup Server. Otherwise, if you choose to format, Vinchin Backup Server will erase all data on the block storage then add it as a fresh new storage device.

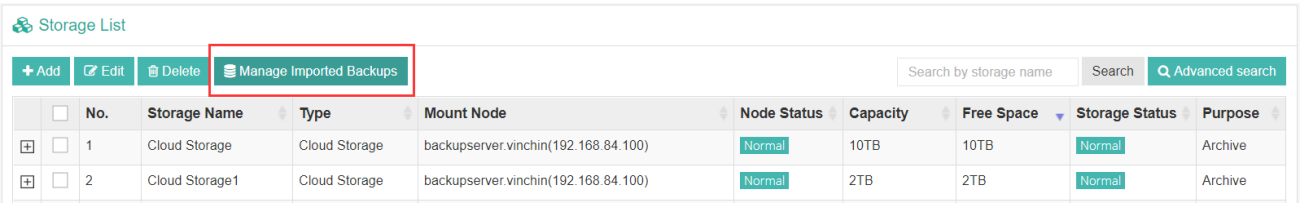
If the block storage had not been used by Vinchin Backup Server before, but it may contain other data, please make sure you had backed up all the data before formatting.



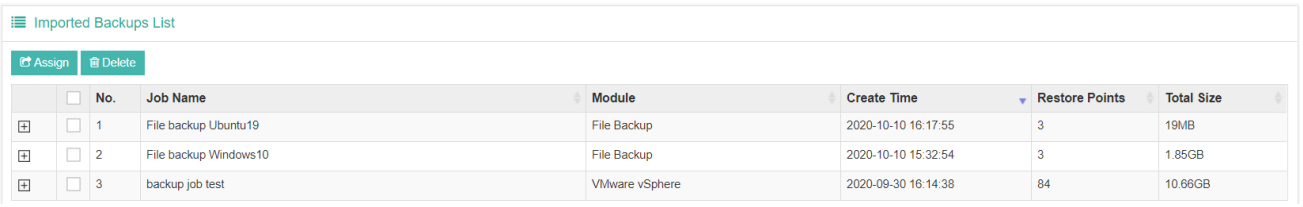
For the file storages and object storages, if there's existing backup data, you'll have to import the data to add it to Vinchin Backup Server.



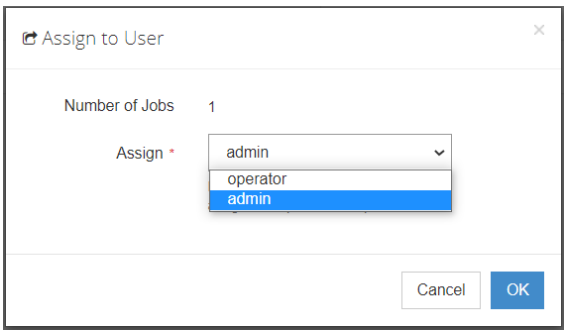
The imported backup data can be found on the **Resources** > **Storage** page by clicking on the **Manage Imported Backups** button.



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.

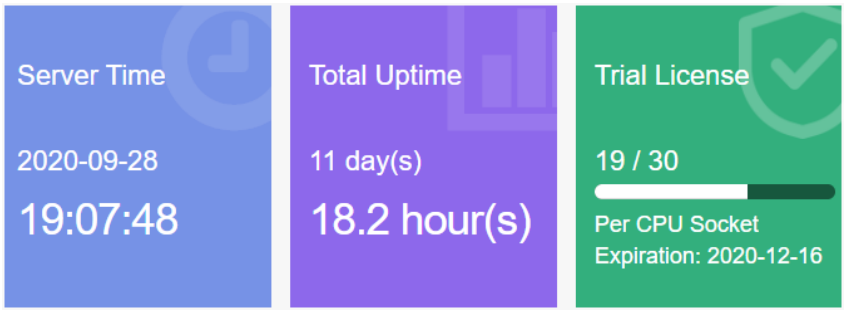


Once the backup data had been assigned to a user, the user will be able to see the backup data and create restore jobs with those data.

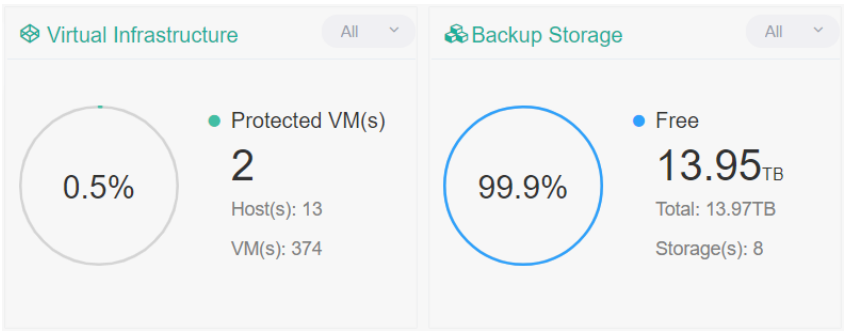
Informational

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.

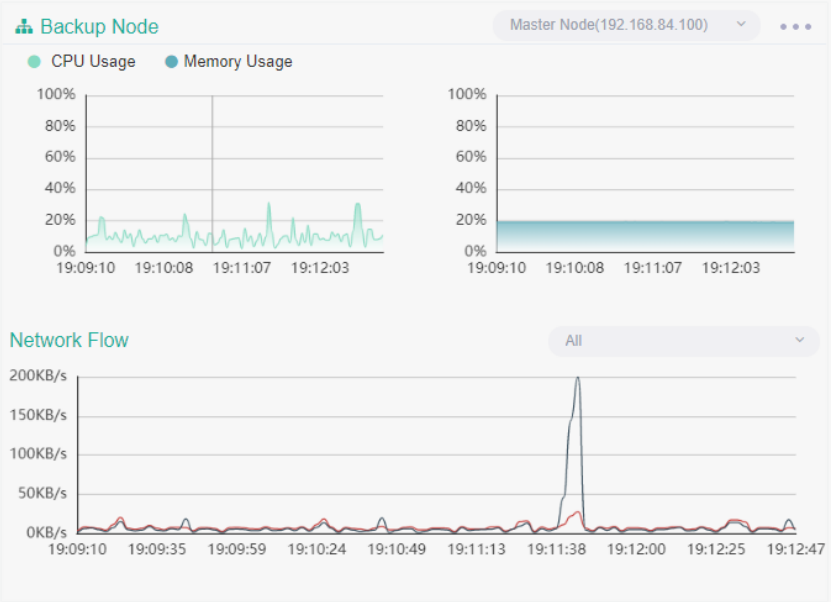


Here are the information of your virtual infrastructure(s) and backup storages.



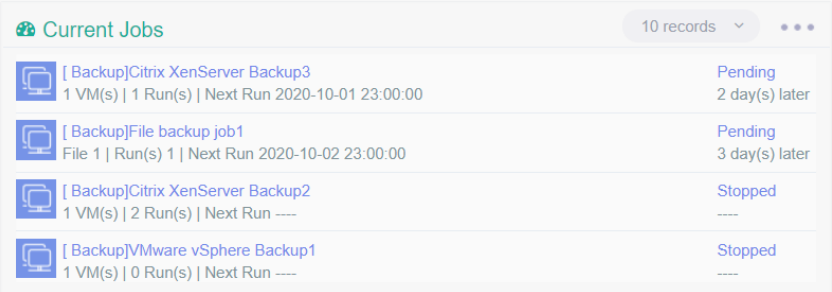
In the **Virtual Infrastructure** column, the total number of hosts, VMs and protected VMs will be displayed. If you had added multiple virtual infrastructures, click on the dropdown list on the top right, you can check an individual infrastructure information.
In the **Backup Storage** column, the total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



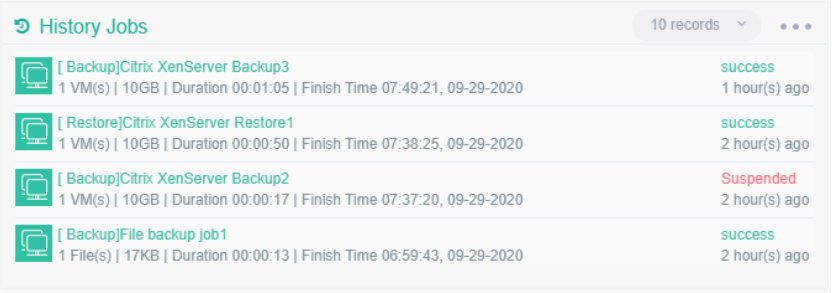
Select a node from the top right dropdown list you are able to monitor the CPU and memory usage, and also the network flow. In the **Network Flow** chart, it shown the network flow of all NICs of the selected node, to view the network flow of an individual NIC, please select that NIC from the Network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

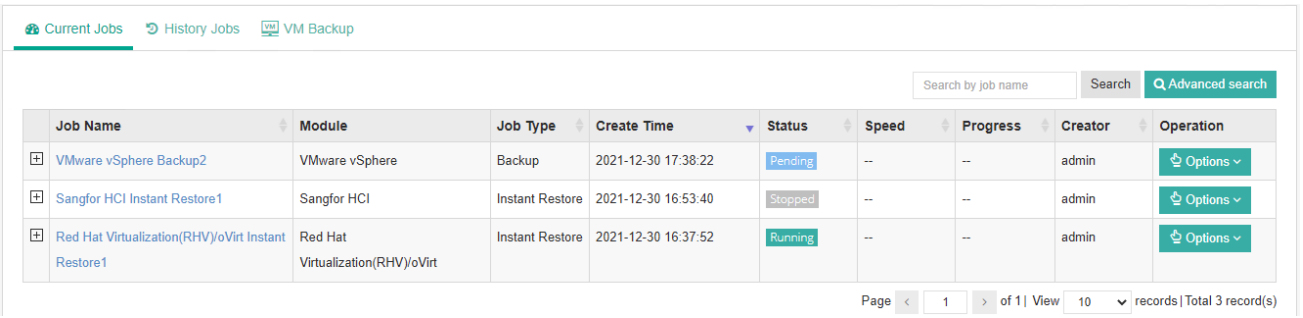
Monitor Center

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.



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.

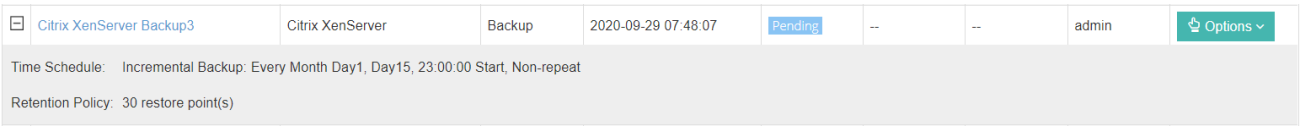
Edit: to modify the configurations of a job in Stopped state.

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

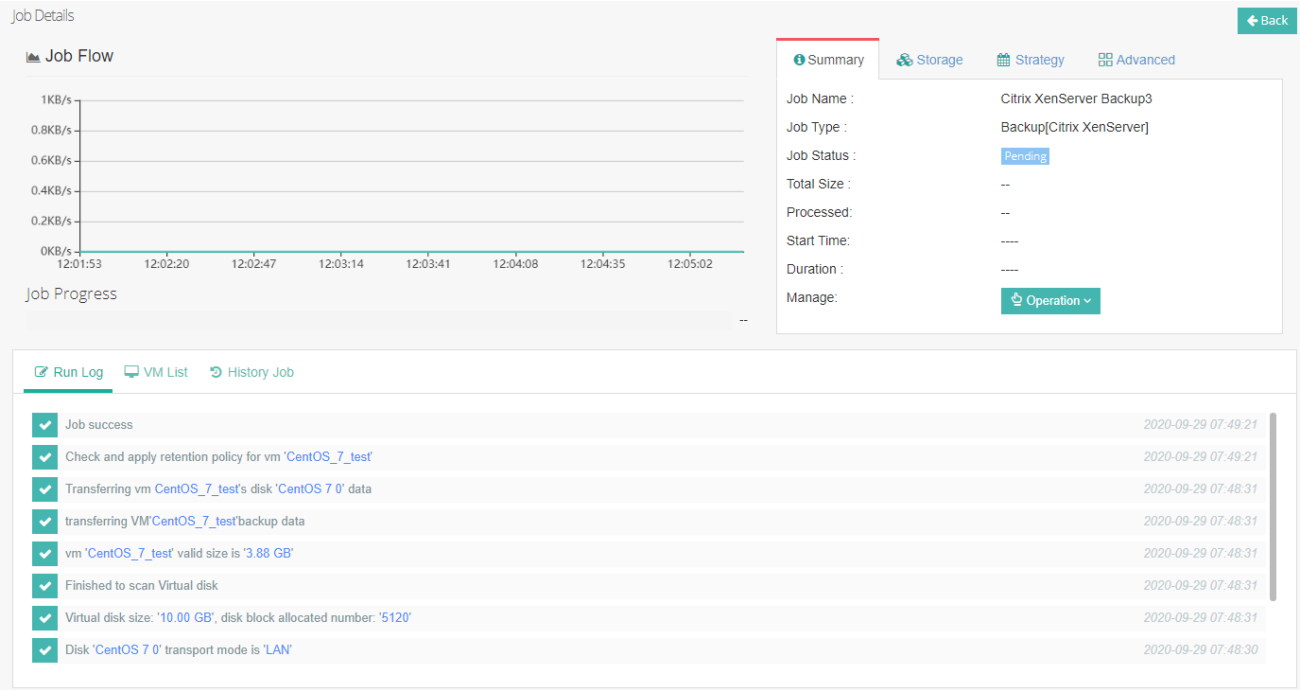
Note

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.

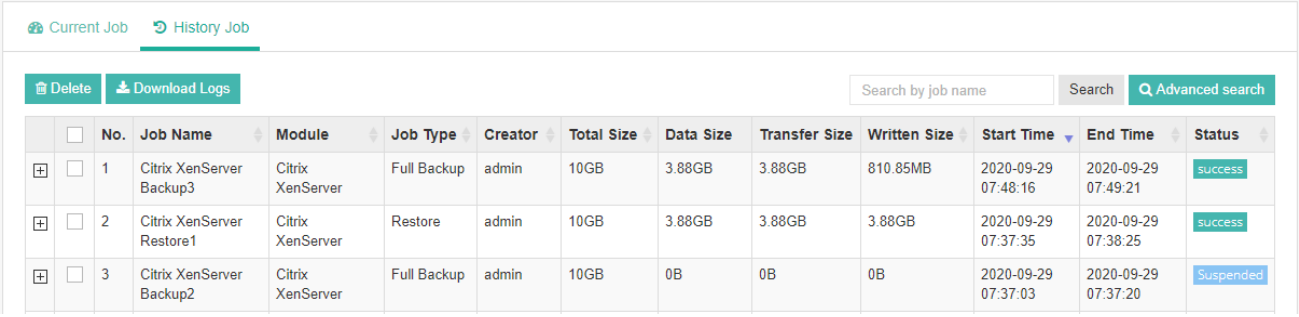
Run Log: if the job is currently running, it will be the real-time log output; if the job is pending or stopped, it will provide the logs of the last time of running.

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

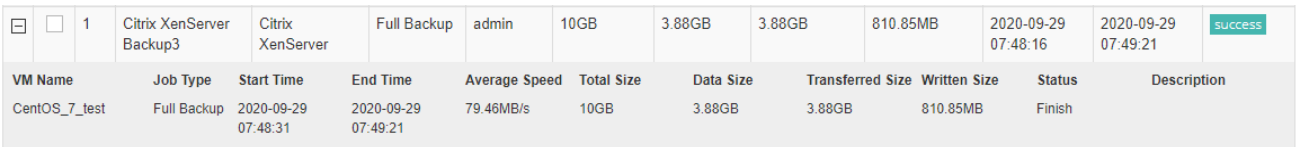
History Job: the running history of the job.

- **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.

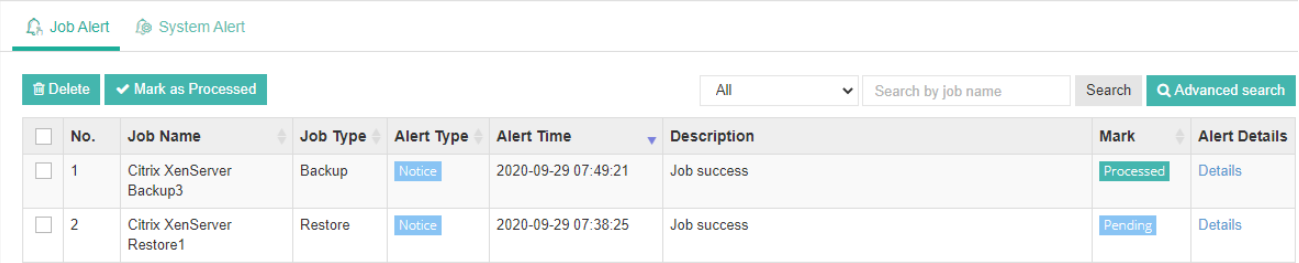


To delete the history jobs, please select the job logs and click on the **Delete** button.
And for the failed jobs, you can select that job and click on **Download Logs** button to download the detailed logs of that job for troubleshooting.

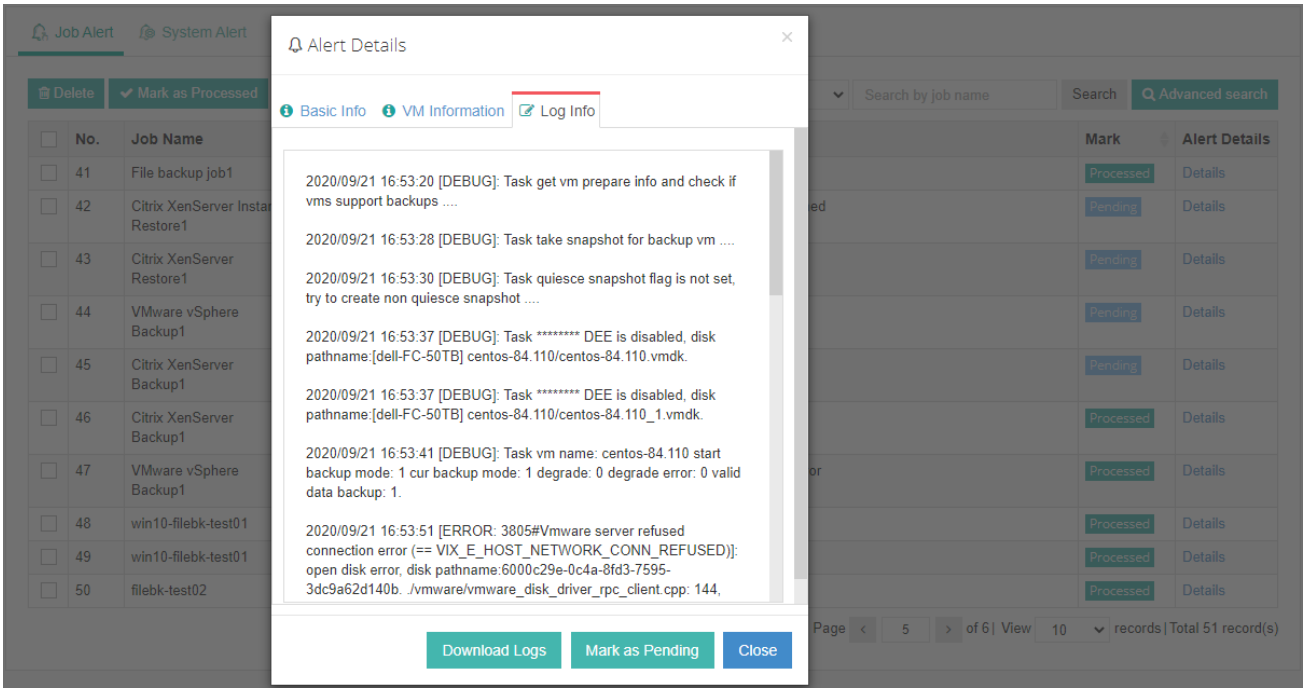
Alerts

- **Job Alert**

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



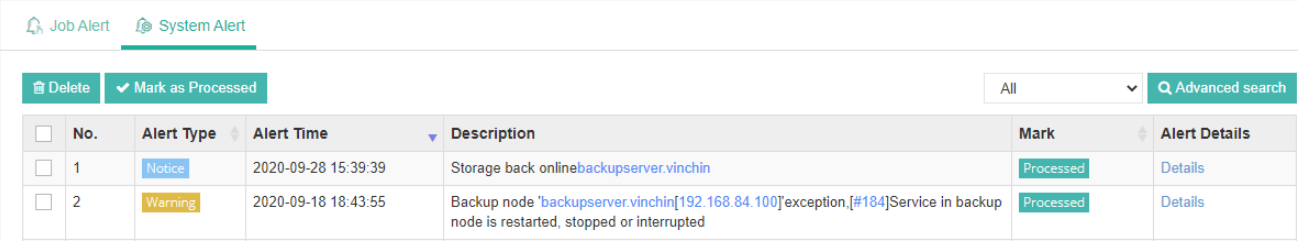
By using the dropdown list above the alert list, you can filter the alert messages by alert types, including notices, warnings and errors.
Click on **Details** button of an alert, you can view the detailed description of the alert message, and at the same time the alert message will be marked as **Processed**.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



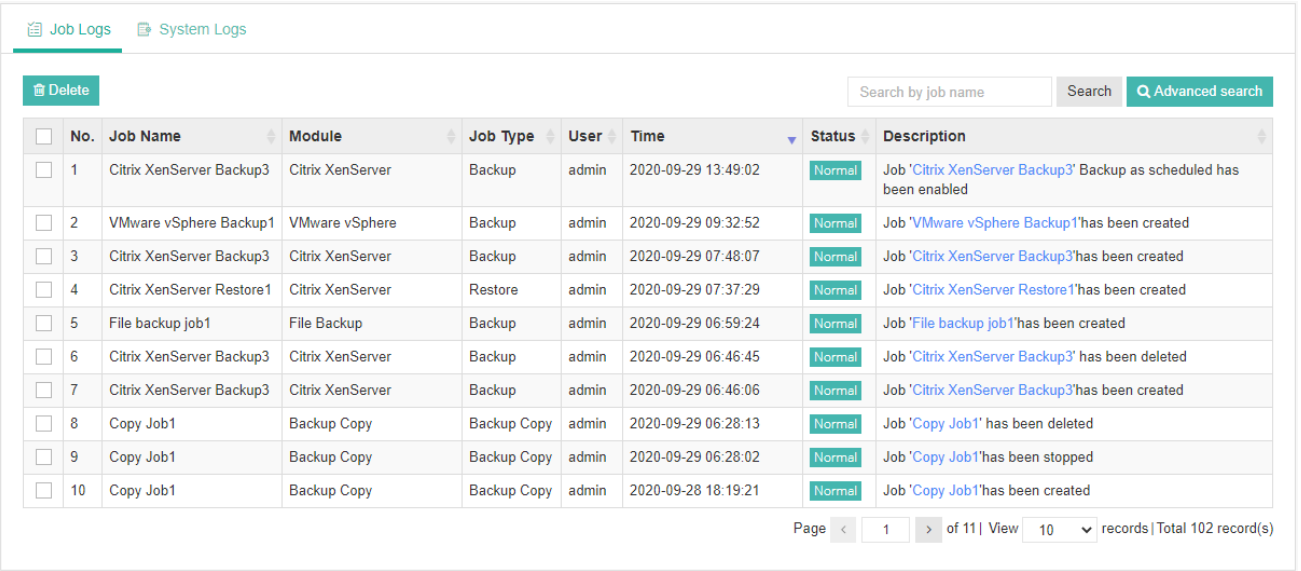
Similar as the job alerts, you can have the same options to filter these alert messages and you can mark the messages as processed or pending state.

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

Logs

- **Job Logs**

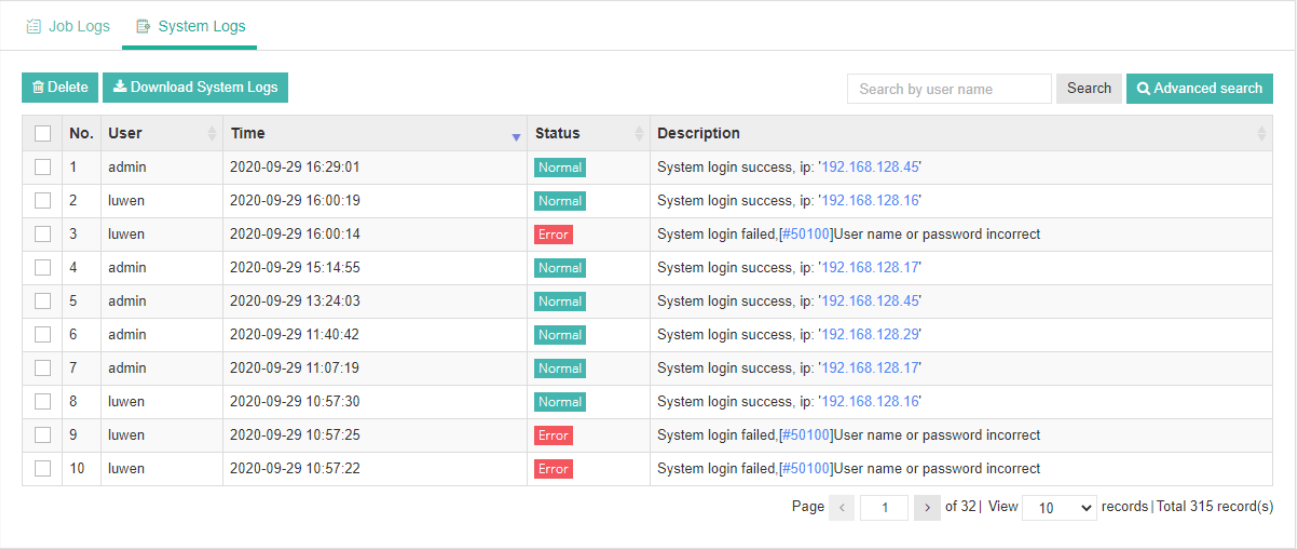
On the **Monitor Center** > **Logs** page, under the **Job Logs** tab, the operations related with job stop, job schedule on, job creation, job deletion and job modification can be all found here.



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.

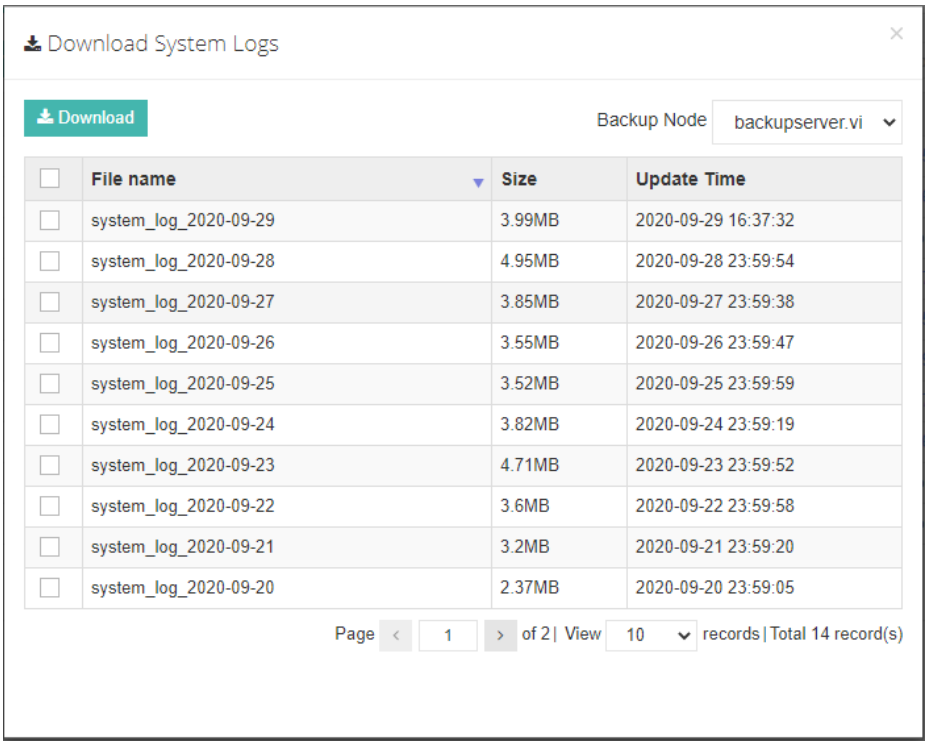
- **System Logs**

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.



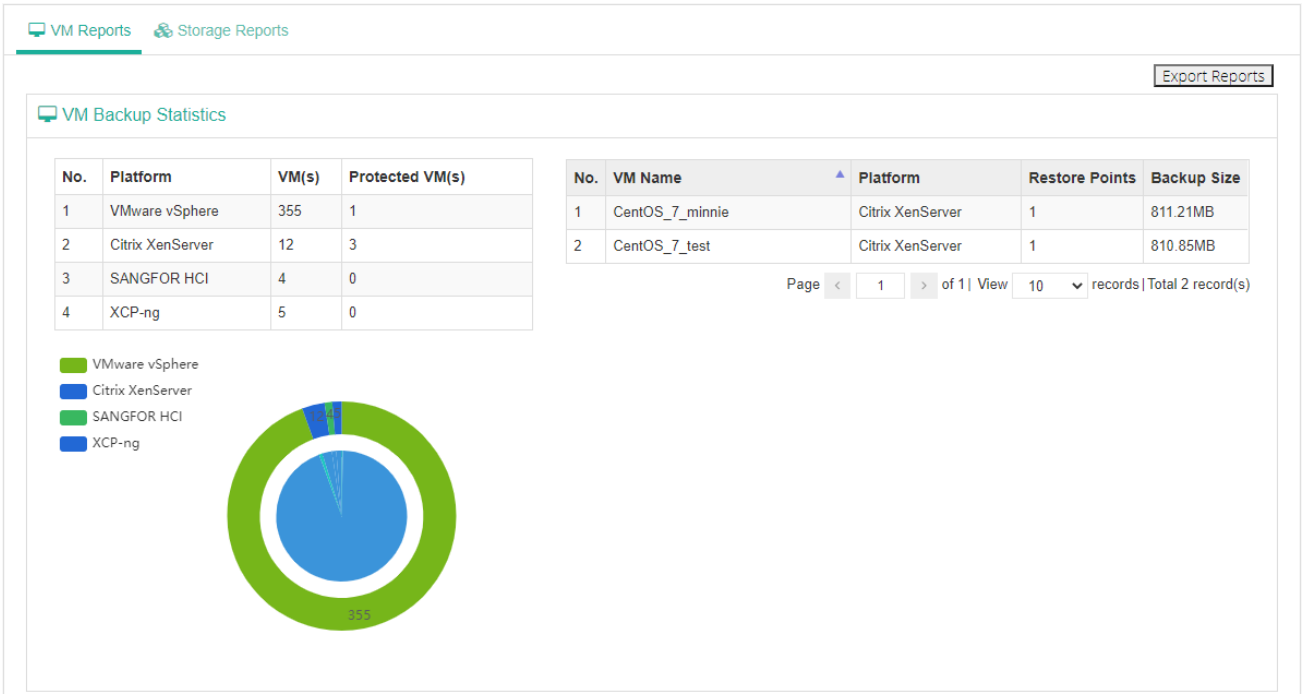
In the **Download System Logs** dialog, the logs are arranged by date. You can select the desired logs and click on the **Download** button to download the logs.

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.

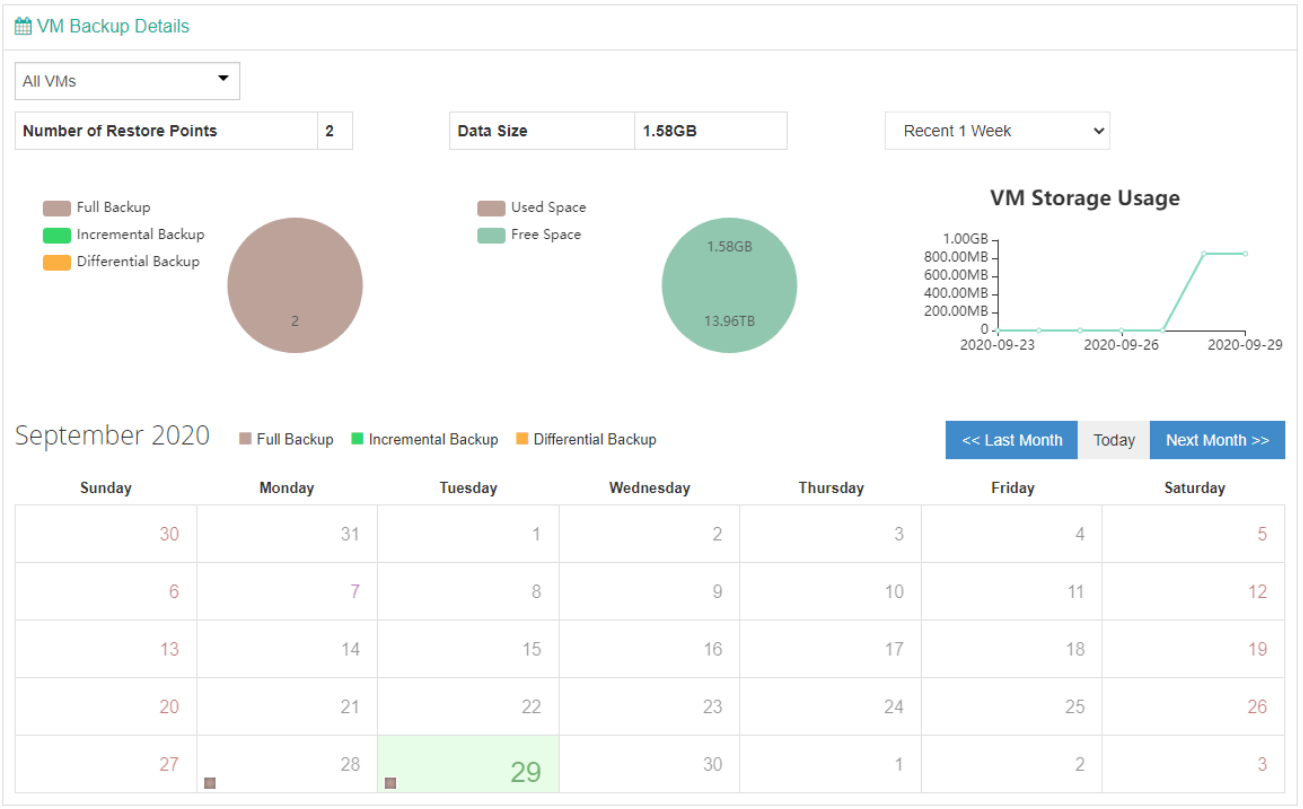
Reports

- **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.

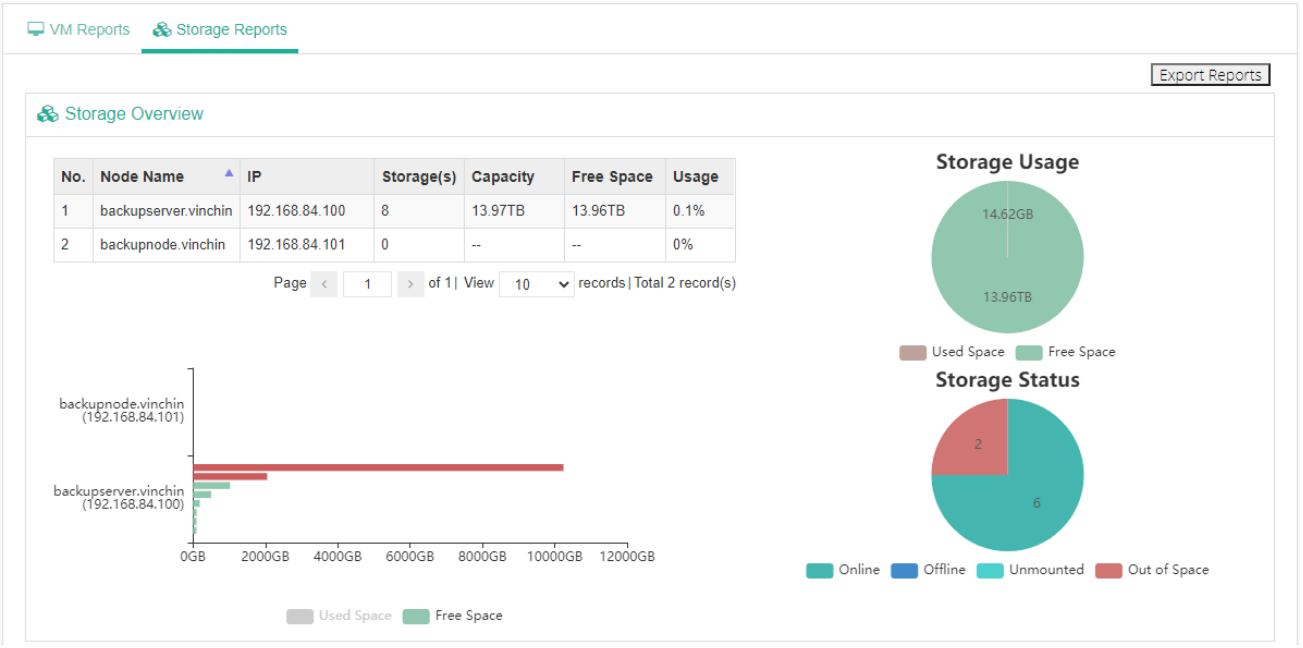


In the VM Backup Details section, you can have the following statistics reports:

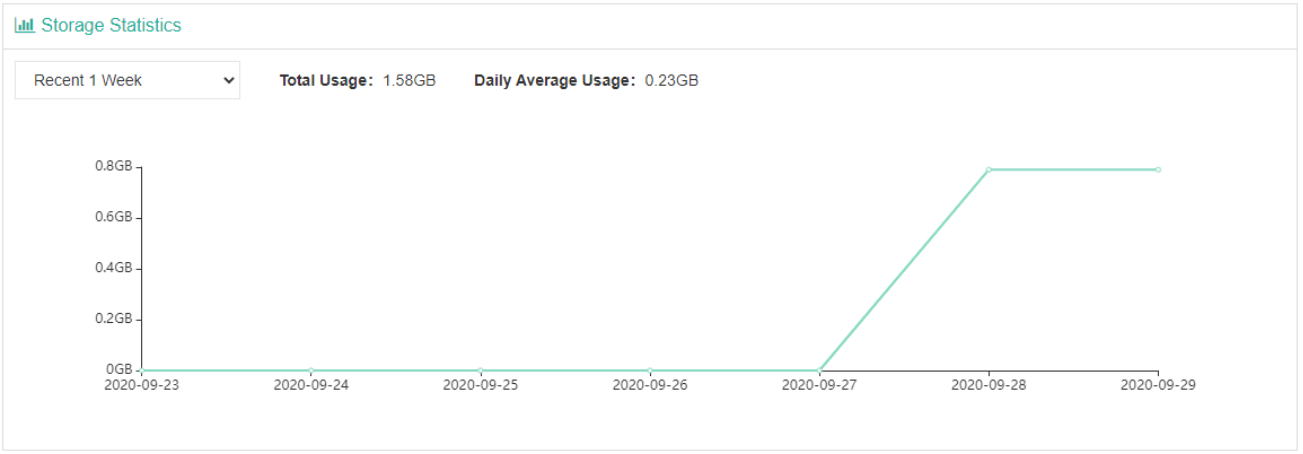
- Number of restore points and a pie chart of restore points by different backup technologies.
- The total size of all backup data.
- The line chart of storage usage per 1 week, 2 week or a month.
- The backup schedules in calendar view.

- **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.



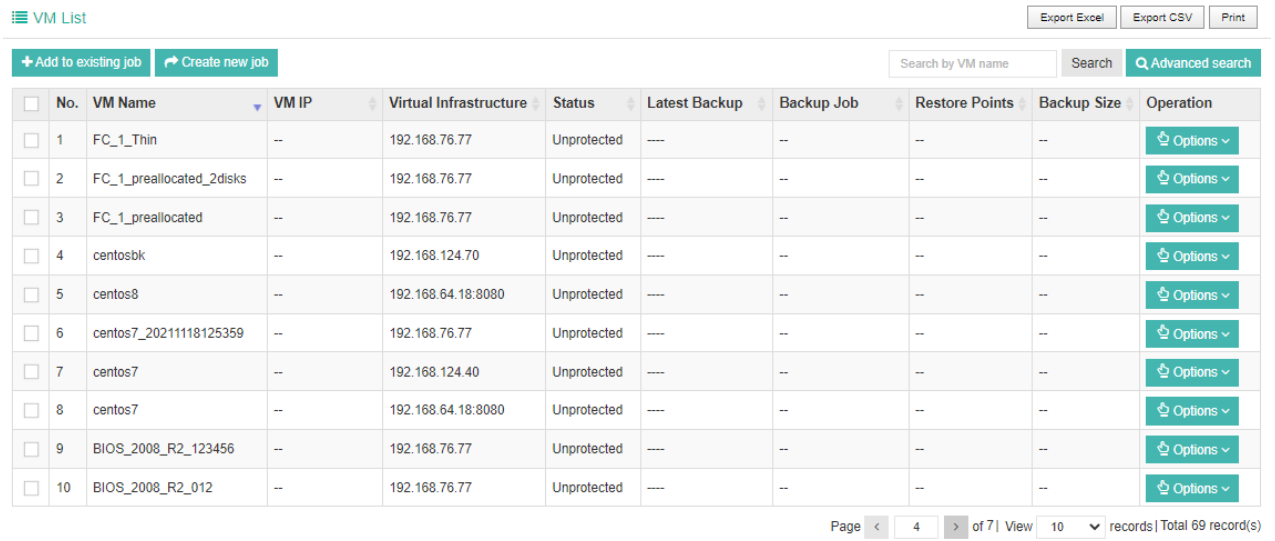
In the **Storage Statistics** section, you can have the reports of total storage usage and daily average usage. And a line chart of storage usages per 1 week, 2 weeks, 1 month, 2 months or 3 months.

VM Backup

Backup

Virtual Machines

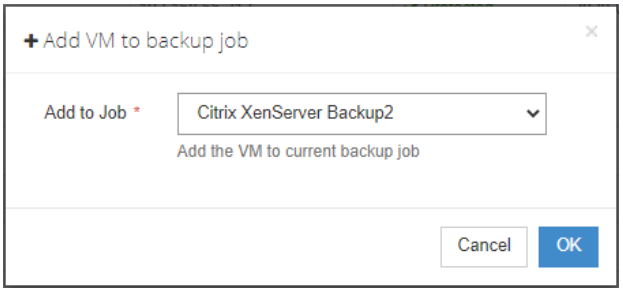
On the **VM Backup** > **Virtual Machines** page, you can view all the VMs from all virtual platforms which you've added into Vinchin backup server.



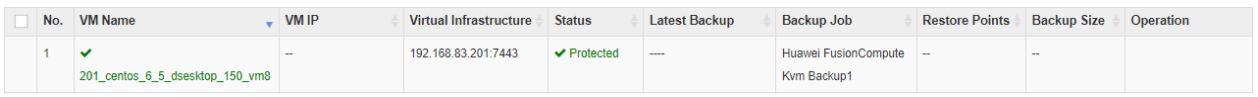
You can select multiple unprotected VMs to add to an existing backup job or create a new backup job. By clicking **Options**, you can choose to add a specific VM to an existing backup job, or choose to create a new backup job for this specific VM.

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

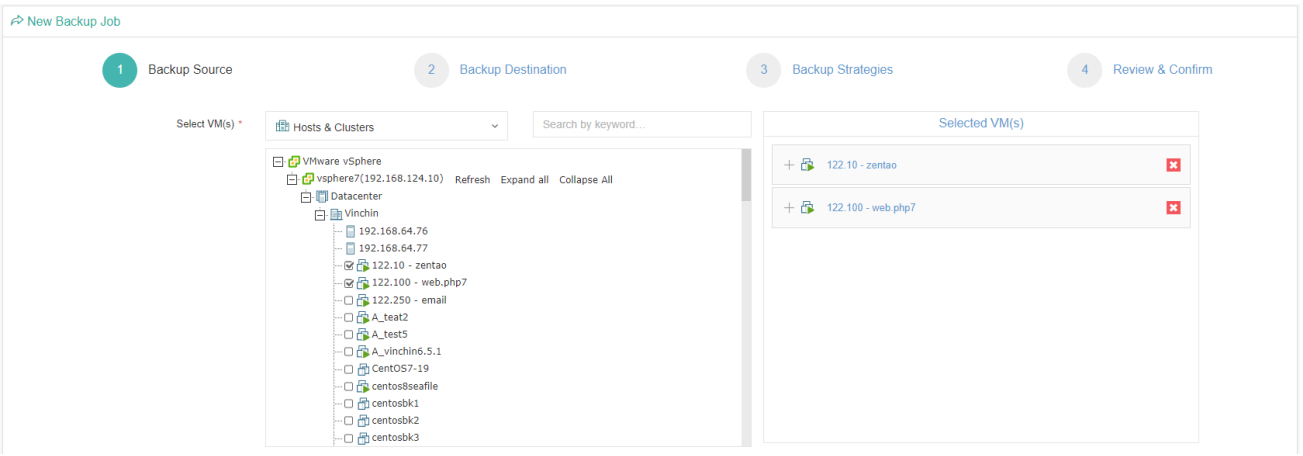


Create Backup Job

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. Select the virtual machines you need to back up, the selected virtual machine(s) will be added to the **Selected VM(s)** column.

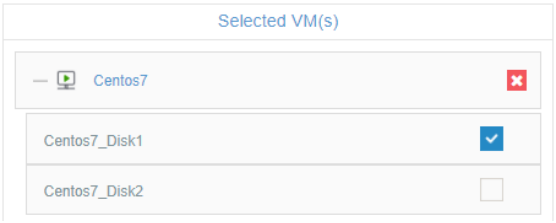


Note

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

2. You can only add VMs to a backup job from the same virtualization platform, if you have multiple virtualization platforms, please create new jobs for the VMs in the other virtualization platforms.

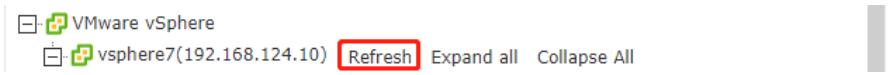
Click on the selected VM, all the virtual disks attached to this VM will show up, you can choose to exclude specific disk(s) from this backup job by unticking the disk(s).



Note

Exclude VM disk from backup job does not support with OpenStack platform.

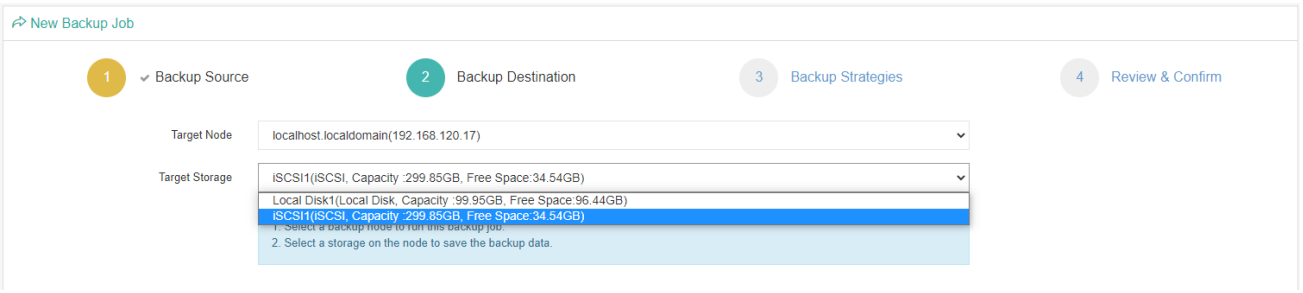
If your virtual infrastructure has been updated recently, click on **Refresh** button to update and sync the VM list to Vinchin backup server.



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.

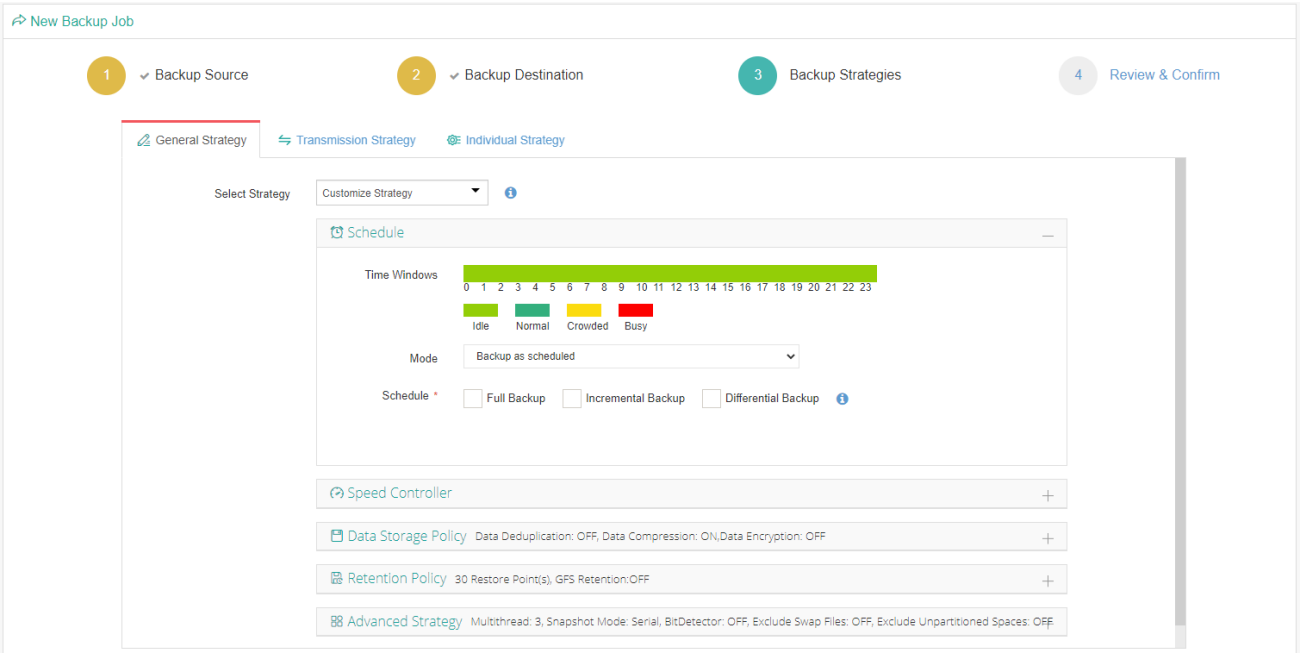
In the **Target Storage** dropdown list, the storages which belong to the selected backup node can be selected.

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, Data Storage Policy, Retention Policy and Advanced Strategy.

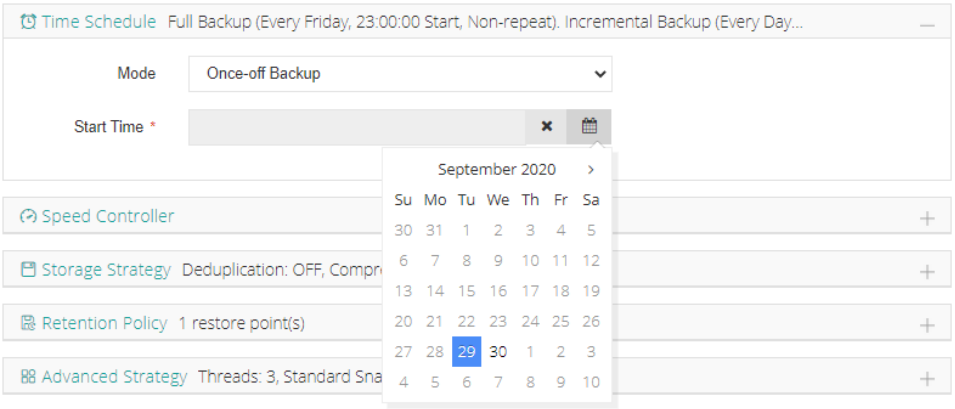


In the **Select Strategy** dropdown list, you can select a preconfigured strategy template, if you had created strategy templates, otherwise choose **Customize Strategy**. For how to create strategy templates, please refer to Strategy Templates.

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

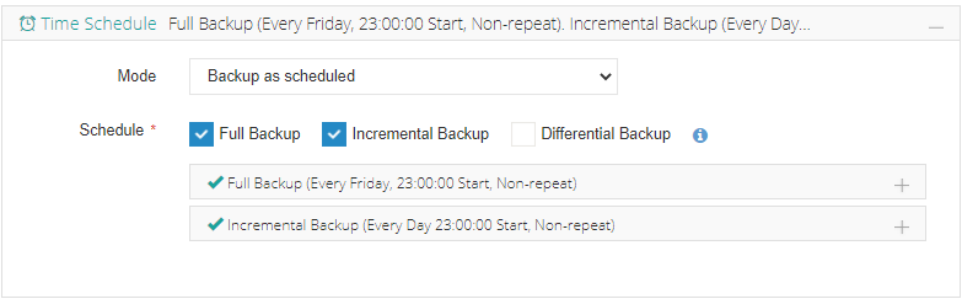
In the Time Schedule field, you can configure the time schedule of the backup job, you can configure the job as a **Backup as Scheduled** job or a **Once-off Backup** job.

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



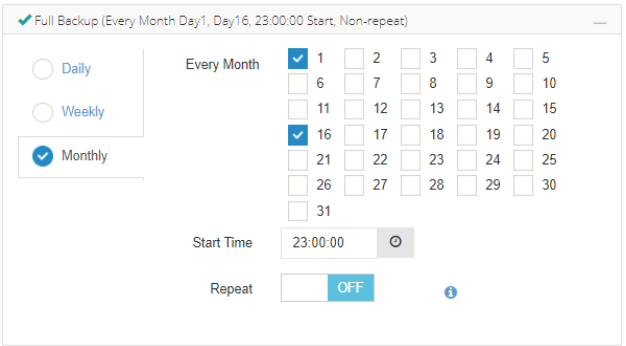
For Scheduled backup job, you can schedule Full Backup with Incremental Backup combination, Full Backup with Differential backup combination or Forever Incremental Backup (enable incremental backup only).

Here we take Full Backup with Incremental Backup as an example.

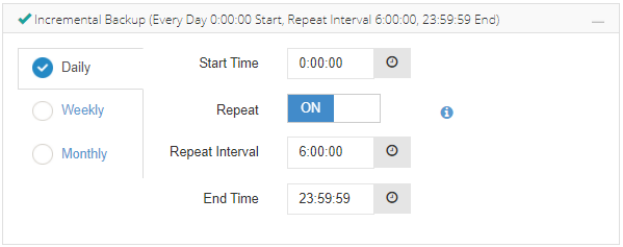


By default, full backups will be scheduled on each Friday night at 11PM. And incremental backups will be scheduled each day at 11PM (when the time point of a full backup is overlapped with an incremental backup, full backup will be taken, and the incremental backup with be taken on the next scheduled 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.

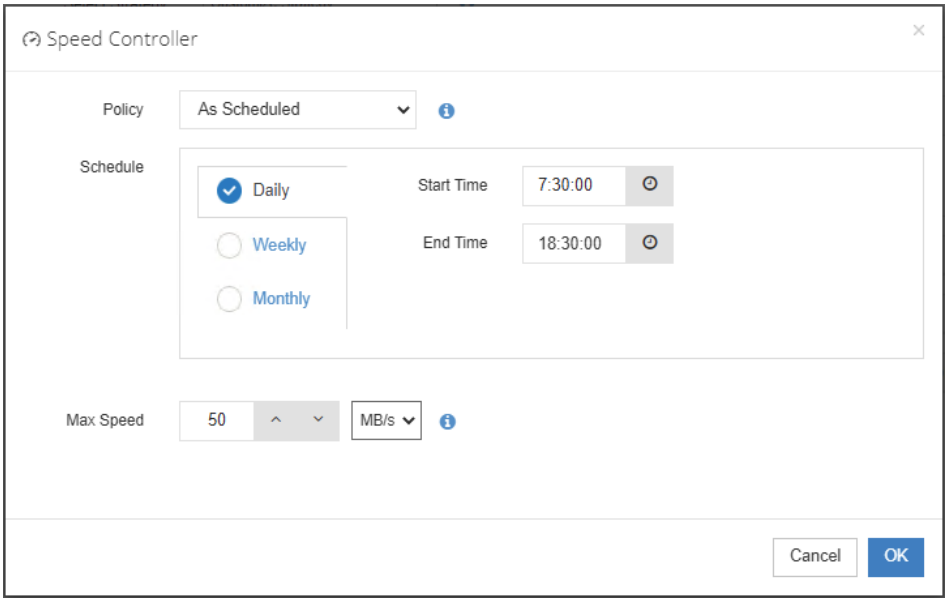


Then configure several incremental backups each day, by default incremental backup will run only for once each day, to run incremental backups several times a day, you can enable the **Repeat** option.



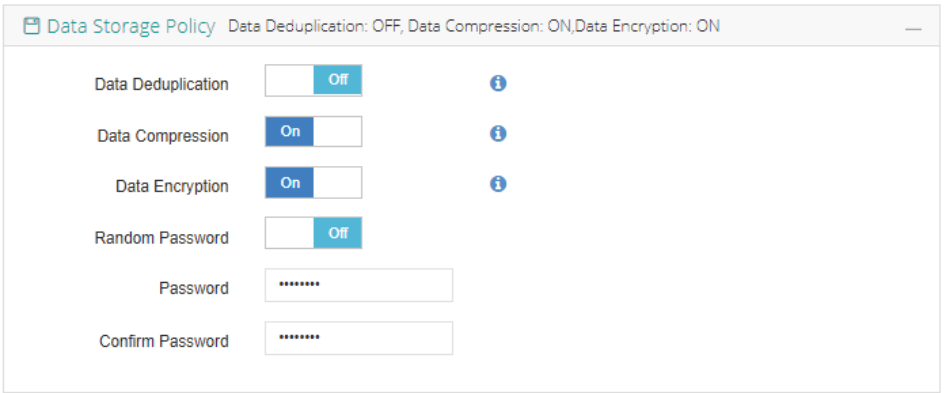
In the above example, full backups will run on day 1 and day 16 of each month, incremental backups will run every 6 hours each day. This is just an example, you should configure the schedules per your requirements based on your actual virtual environments.

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 policy can be configured as **Permanent** or **As Scheduled**.

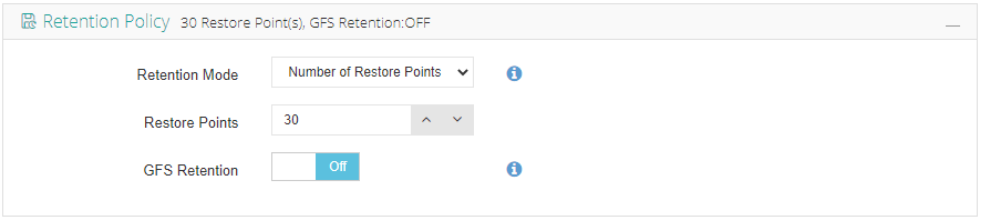
Data Storage Policy including **Deduplication**, **Compression** and **Encryption** of the backup data.



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

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

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



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

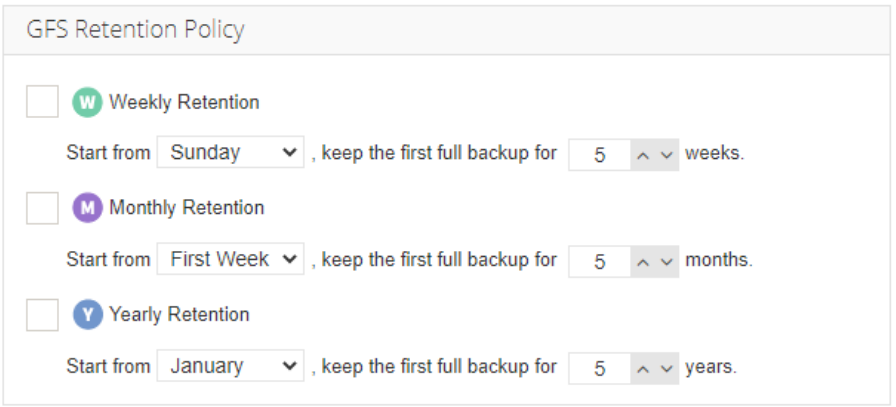
For the backup jobs with full backup schedules only, Vinchin Backup server will delete the older backup restore points directly to comply with the retention policy.

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

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

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.

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



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

For example, if **Sunday** is selected, Vinchin backup server will tag the full restore point of each Sunday with a "**W**"

tag. If there's no full restore point generated on Sunday, it will start waiting and tagging the first coming full restore point of the week. The tagged full restore point will be kept for the specified number of weeks.

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

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

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

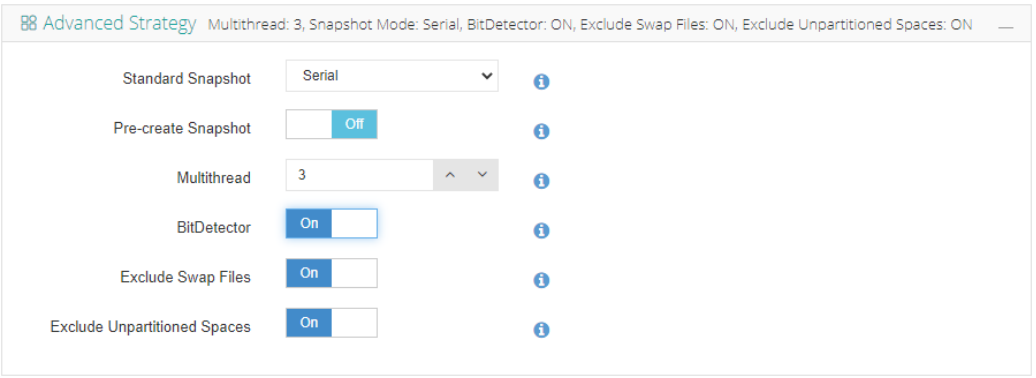
To be able to turn on monthly GFS retention, you should at least configure the full backup schedules to run on weekly basis.

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

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

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

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



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

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

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

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

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.

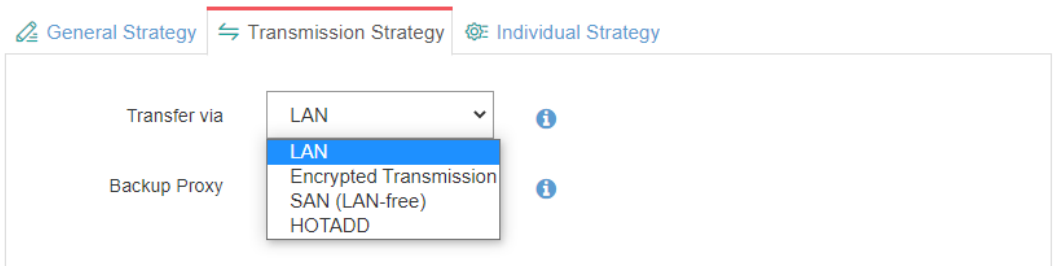
4. It is recommended to set the backup schedule to run at night or in the other nonproduction hours.

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:



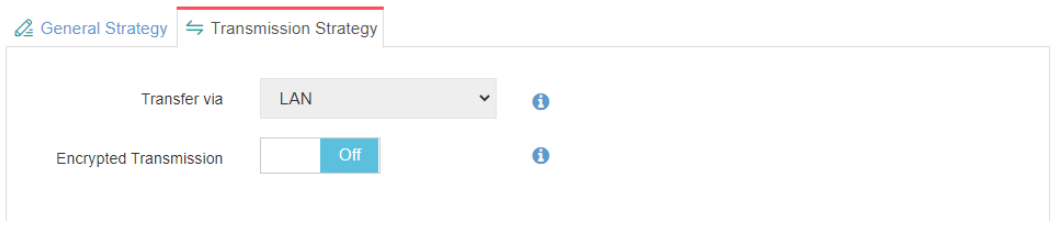
For VMware vSphere, the backup data can be transferred through LAN, LAN (Encrypted Transmission), SAN (LAN-Free) or HOTADD (LAN-Free).

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. LAN-Free path needs to be configured, please refer to LAN-Free.

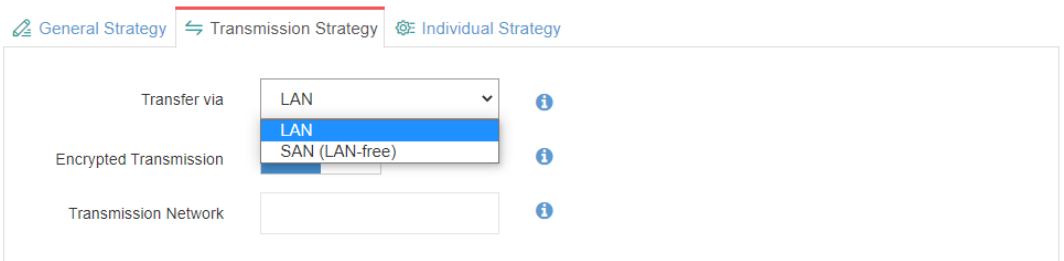
HOTADD (LAN-Free) can be used only if Vinchin Backup Server is installed on the ESXi server as a virtual machine.

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 and OLVM (4.3):



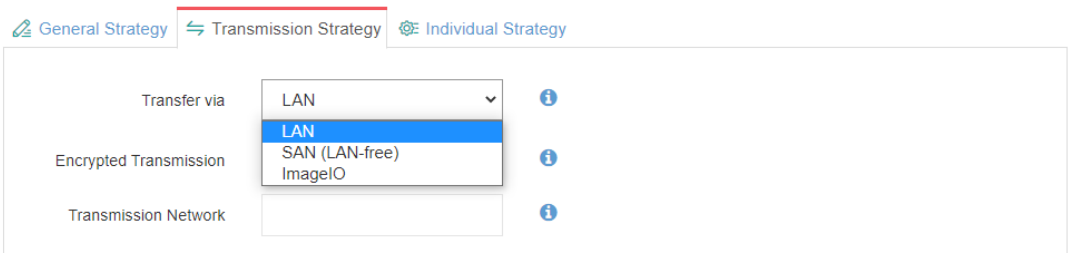
For Citrix XenServer, XCP-ng and OLVM, the backup data can be transferred through LAN or through the storage area network.

If you choose to do the backups over LAN, by default, the backup data will be transferred via the production network. But if you have a separated network for VM backup, please specify the network address in the

Transmission Network field in "network/prefix_length" format, e.g., 172.16.0.0/16. And you can choose to either encrypt the transmission or not by turning **Encrypted Transmission** on or off.

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

Red Hat Virtualization(RHV)/oVirt and OLVM (4.4.8):



For RHV/oVirt, the backup data can be transferred through LAN or through the storage area network, or through ImageIO API.

For **LAN** and **ImageIO**, the data will be transferred through production network by default, but if you have a separated network for VM backup, please specify the network address in the **Transmission Network** field in "network/prefix_length" format, e.g., 172.16.0.0/16. And you can choose to either encrypt the transmission or not by turning **Encrypted Transmission** on or off.

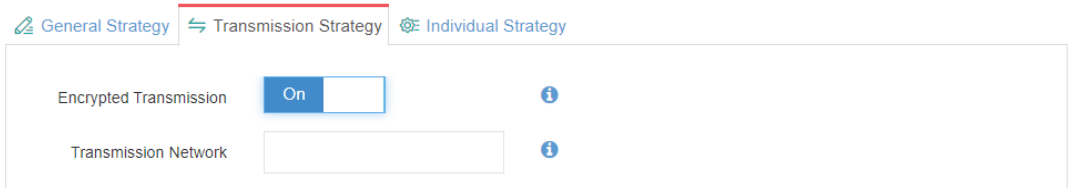
SAN (LAN-Free) can be used to transfer the backup data from the storage area network. LAN-Free path needs to be configured, please refer to LAN-Free.

Note

1. If you set transmission strategy as LAN, backup plugin needs to be installed on RHVH/oVirt hosts.

2. If you set transmission strategy as ImageIO, RHV/oVirt version must be 4.4.7 or higher.

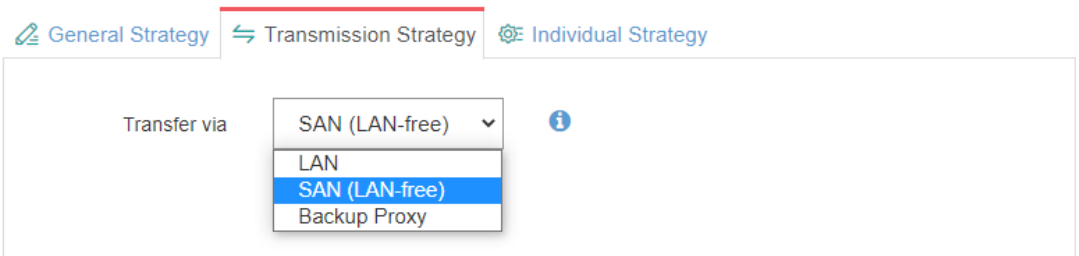
H3C UIS/CAS and Sangfor HCI:



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

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

OpenStack:



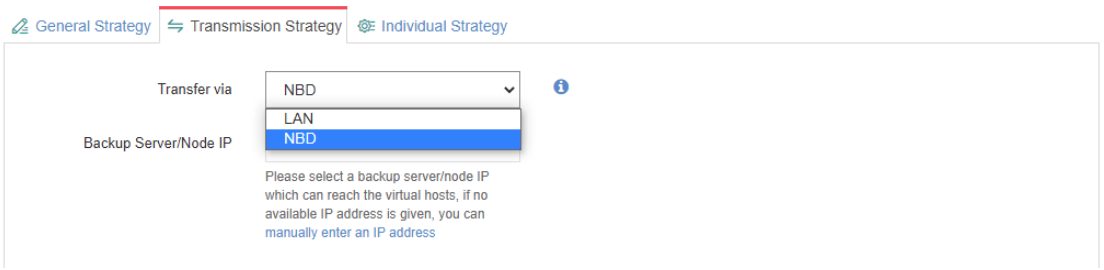
For OpenStack, the backup data can be transferred through LAN or through the storage area network, or through Backup Proxy.

If **LAN**, Vinchin backup plugin for OpenStack needs to be installed on both OpenStack Compute nodes and Controller nodes.

If **SAN (LAN-Free)**, OpenStack backend storage must be Ceph and Vinchin backup server/node must have access to the Ceph Public network.

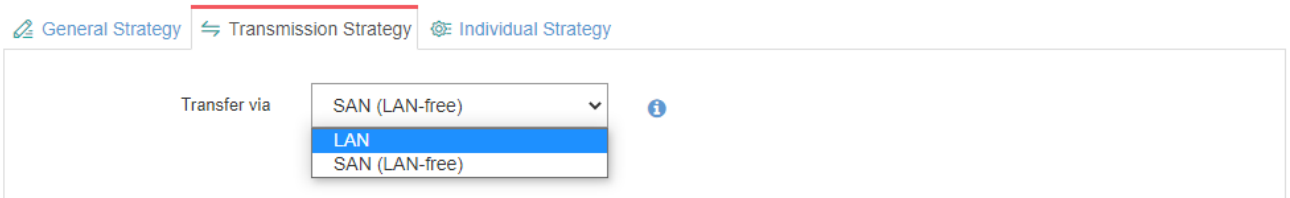
If **Backup Proxy**, Vinchin backup proxy must be installed in the OpenStack virtual platform.

Huawei FusionCompute (KVM):



For Huawei FusionCompute, backup data can be transferred through LAN or via NBD.

ZStack Cloud:

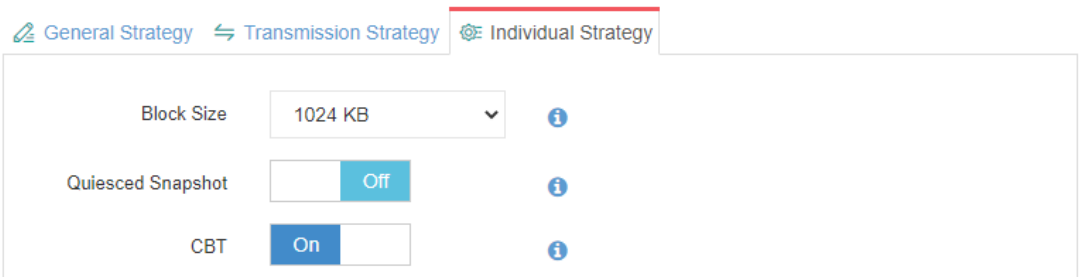


For ZStack Cloud, backup data can be transferred through LAN or SAN. SAN (LAN-free) backup is only applicable when the backend storage of ZStack is Ceph, otherwise please select LAN.

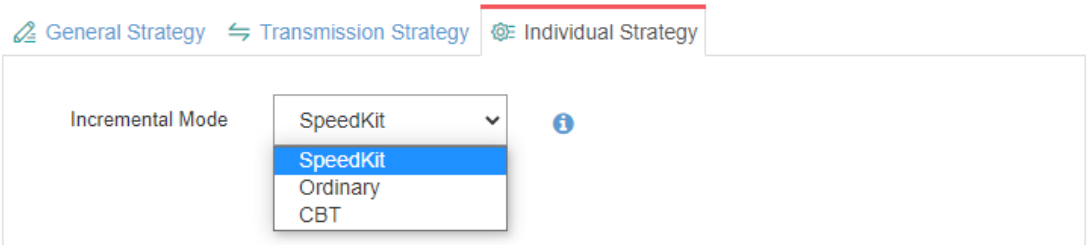
➢ Individual Strategy

The individual strategies for different virtual platforms are different.

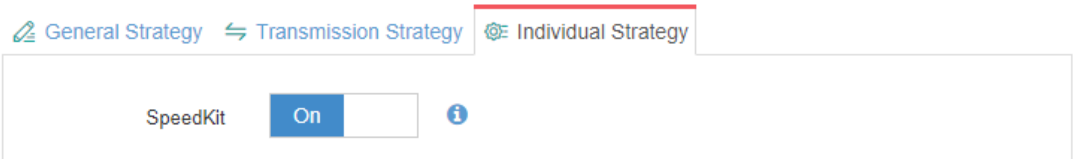
VMware vSphere:



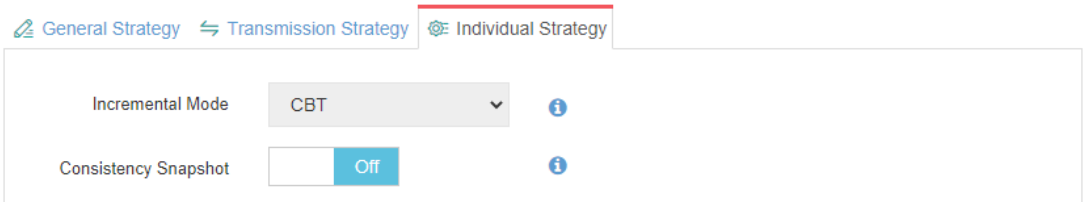
RHV/oVirt, OLVM (4.4.8), Citrix XenServer and XCP-ng:



H3C UIS/CAS, Sangfor HCI, OpenStack and ZStack:



Huawei FusionCompute KVM:



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 enabled 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.

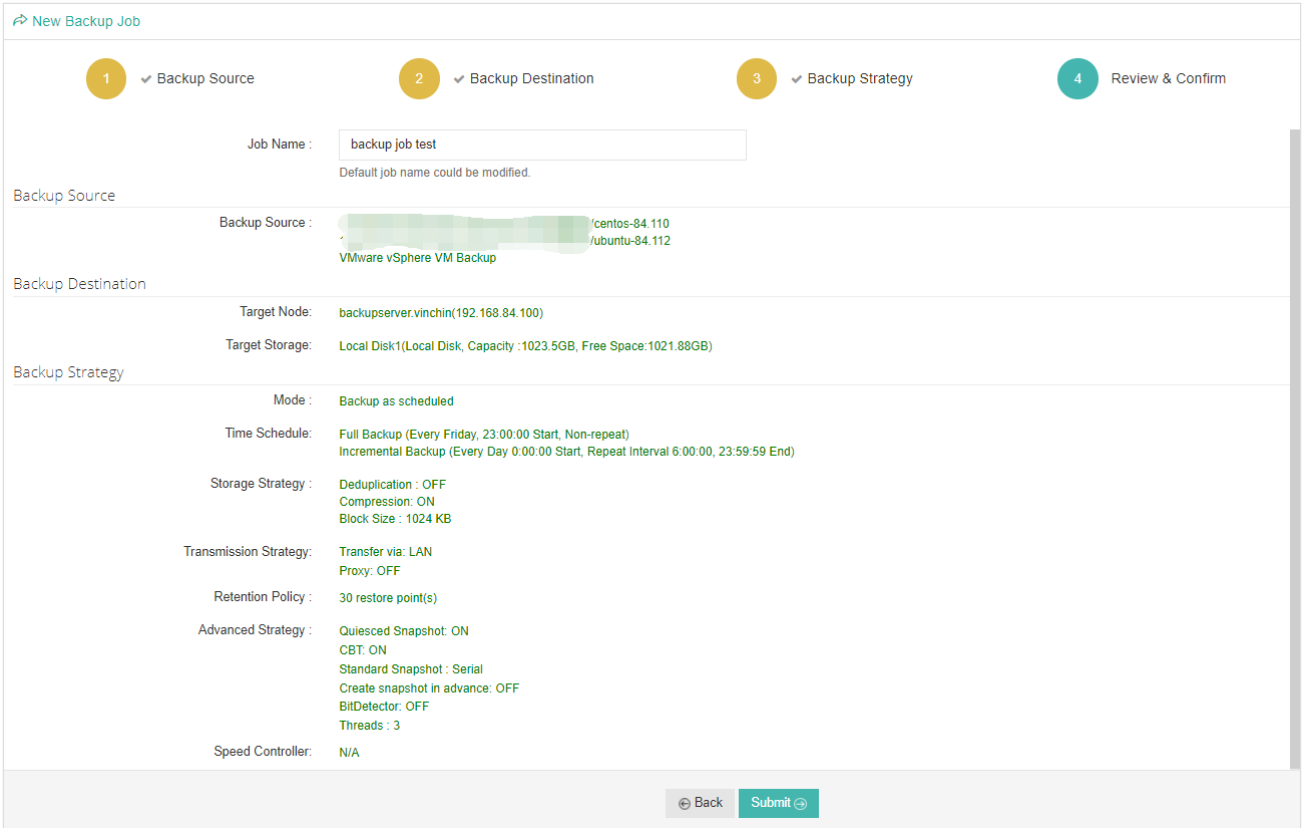
CBT (Changed Block Tracking) is now supported with VMware vSphere, Citrix XenServer (7.3 and higher), XCP-ng and Huawei FusionCompute, it is a more advanced way to perform incremental backups than using SpeedKit or Ordinary mode.

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

Consistency Snapshot is configurable with Huawei FusionCompute(KVM), it is used to ensure the VM data consistency when creating VM snapshot.

Step 4: Review & Confirm

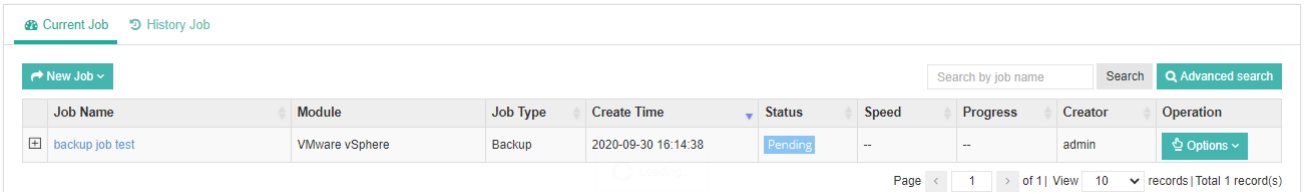
After completing the above-mentioned settings, you are able to review and confirm the settings in one screen.



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.

VM Restore

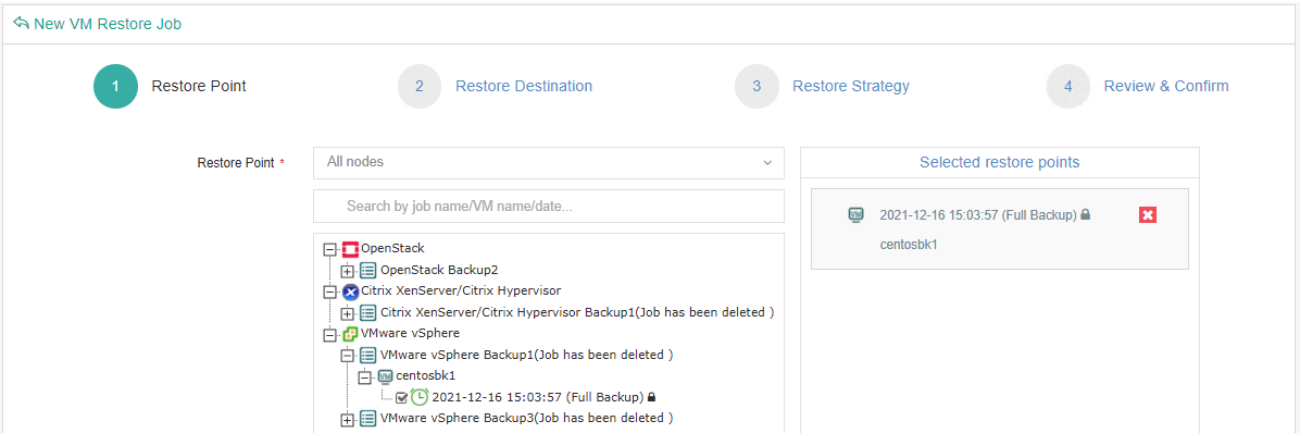
Create Restore Job

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.

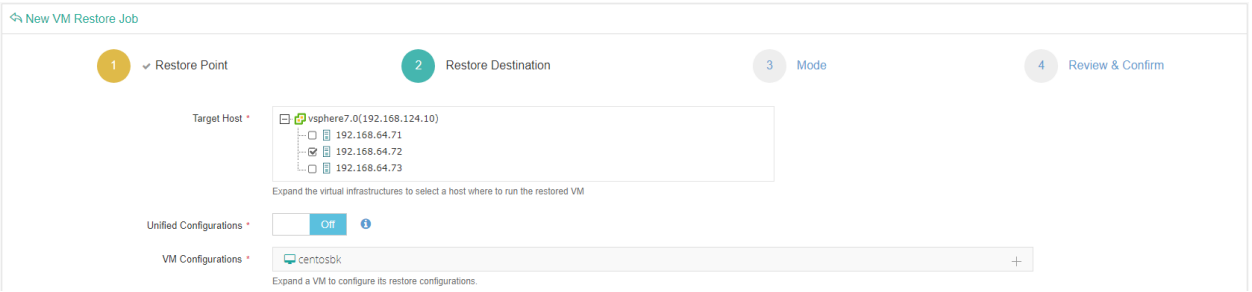
Select a target VM restore point under your virtual infrastructure which you want to restore. You can quickly find the target restore point by searching the job name, VM name or the date of the restore point.



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

Step 2: Restore Destination

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



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

Note

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

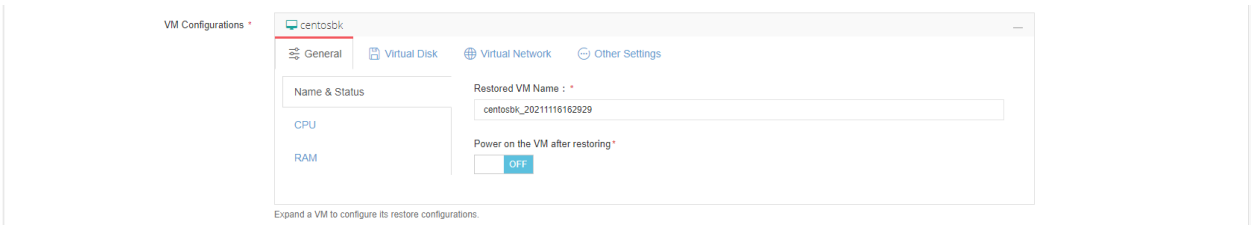
2. If the host is offline, you cannot select it as restore destination.

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

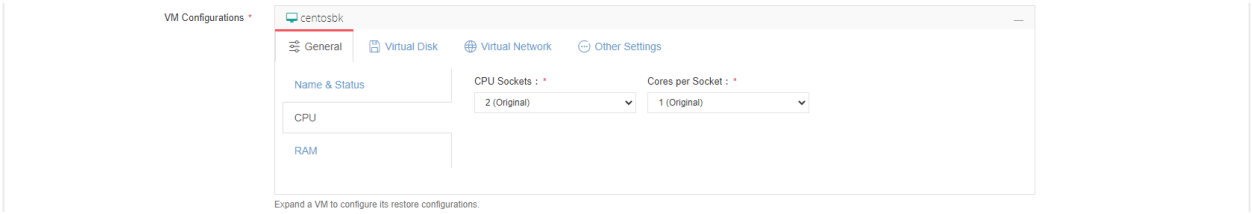
Unified Configurations: If you are restoring a group of VMs, enable this function you can set the storage, network, and choose whether to power on the target VMs after restoring.

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

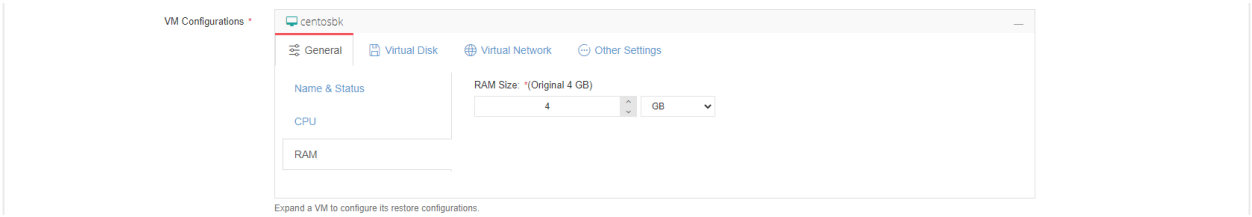
Name & Status: You can set a customized name for the VM to be restored and set its power status after restoring.



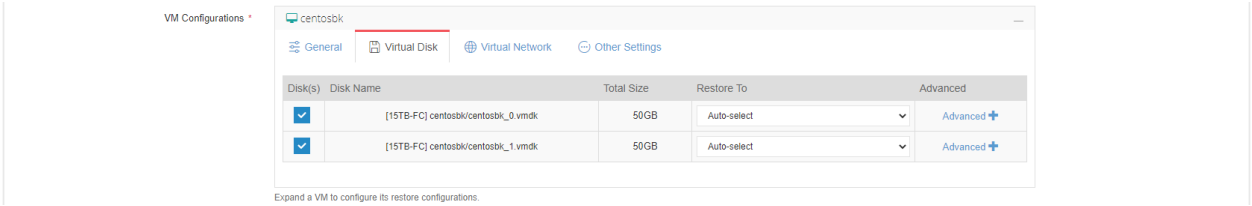
CPU: Here you are allowed to change the number of CPUs or CPU cores for the VM to be restored if necessary.



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



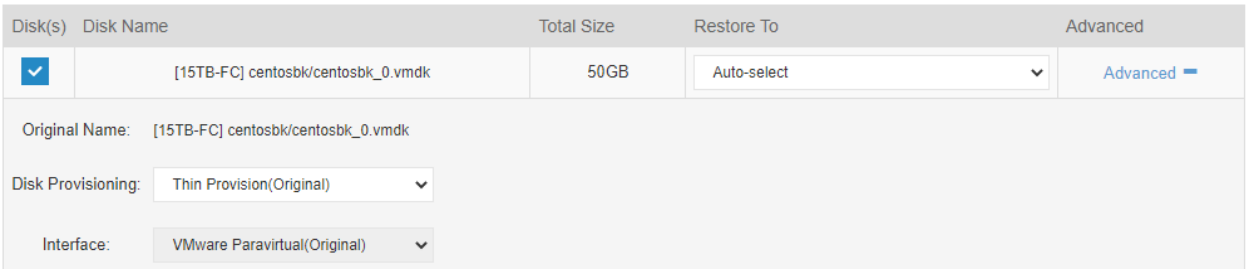
Virtual Disk: Virtual Disk settings are optional, you can proceed with the given default settings.



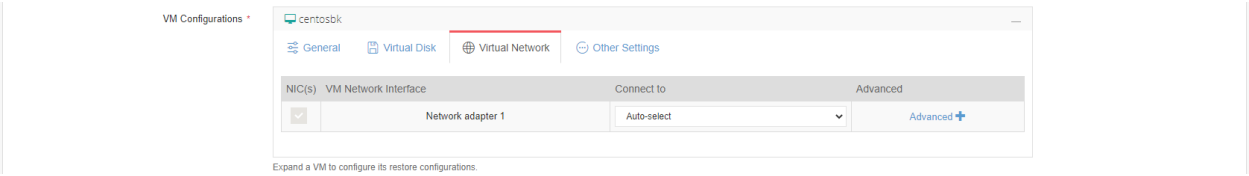
In the **Disk(s)** column, there are checkboxes for the VM virtual disks, when a VM has multiple disks, you can choose to restore specific disk(s) without having to restore all the disks of the VM. But if you don't restore the disk on which the operating system is installed, the restored VM will not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

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

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

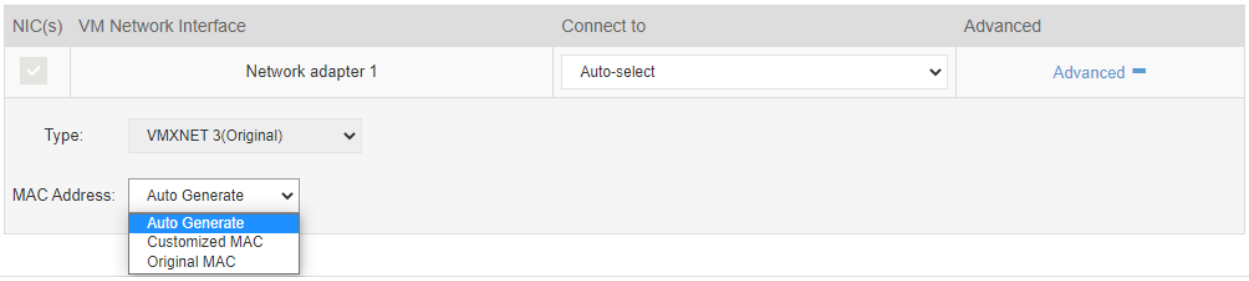


Virtual Network: Virtual Network settings are also optional. It allows you to select the virtual network to be connected to and the MAC address assignment of the restored VM.



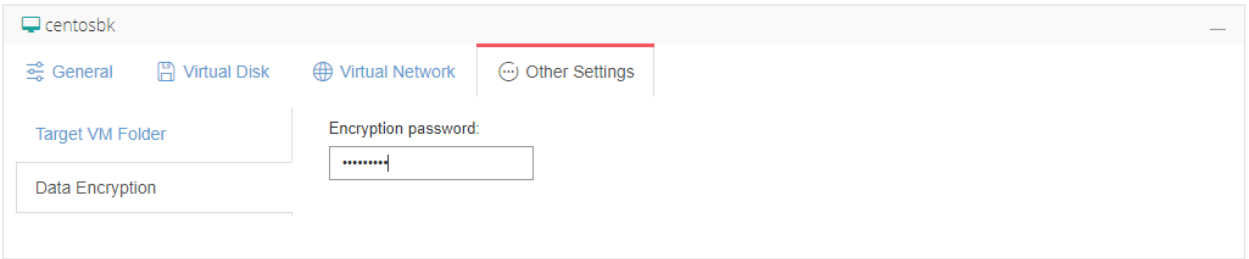
In the **Connect to** column, you can select a desired virtual network for specific virtual network interface of the VM, by default it will automatically select one from the available virtual networks.

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



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

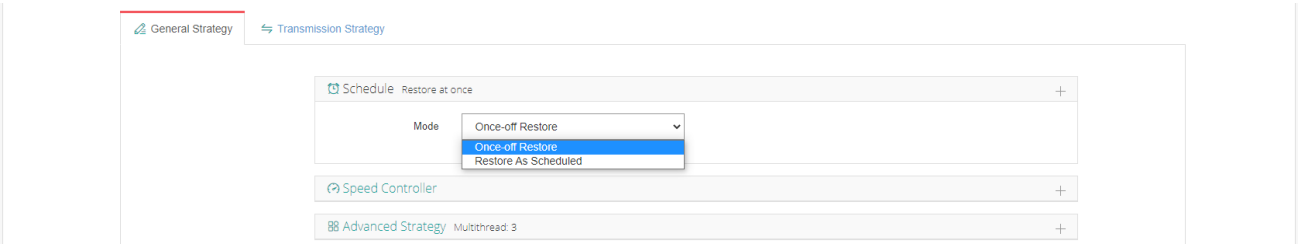
Other Settings: Currently, Other Settings option will not present to all VM restore job settings. This option will present for certain virtualizations for some additional configurations of the VM restore job.



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

Step 3: Restore Strategy

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



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

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 Once-off Restore.

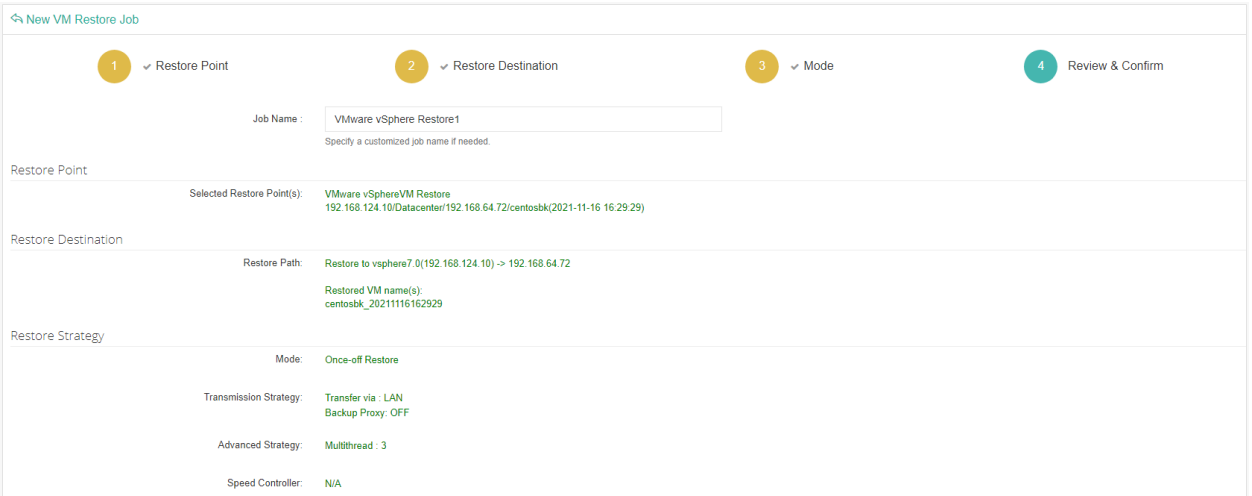
For **Speed Controller**, it works the same principle as the VM backup jobs.

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

For **Transmission Strategy**, please refer to Create 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.

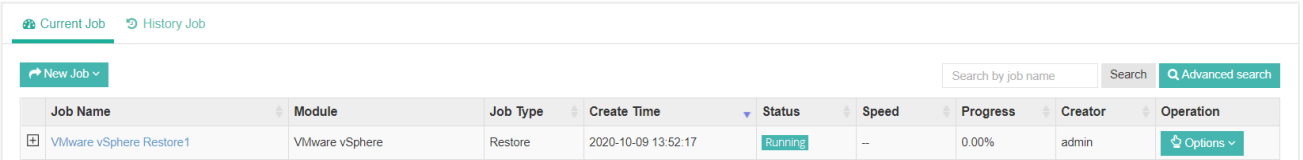


Note

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

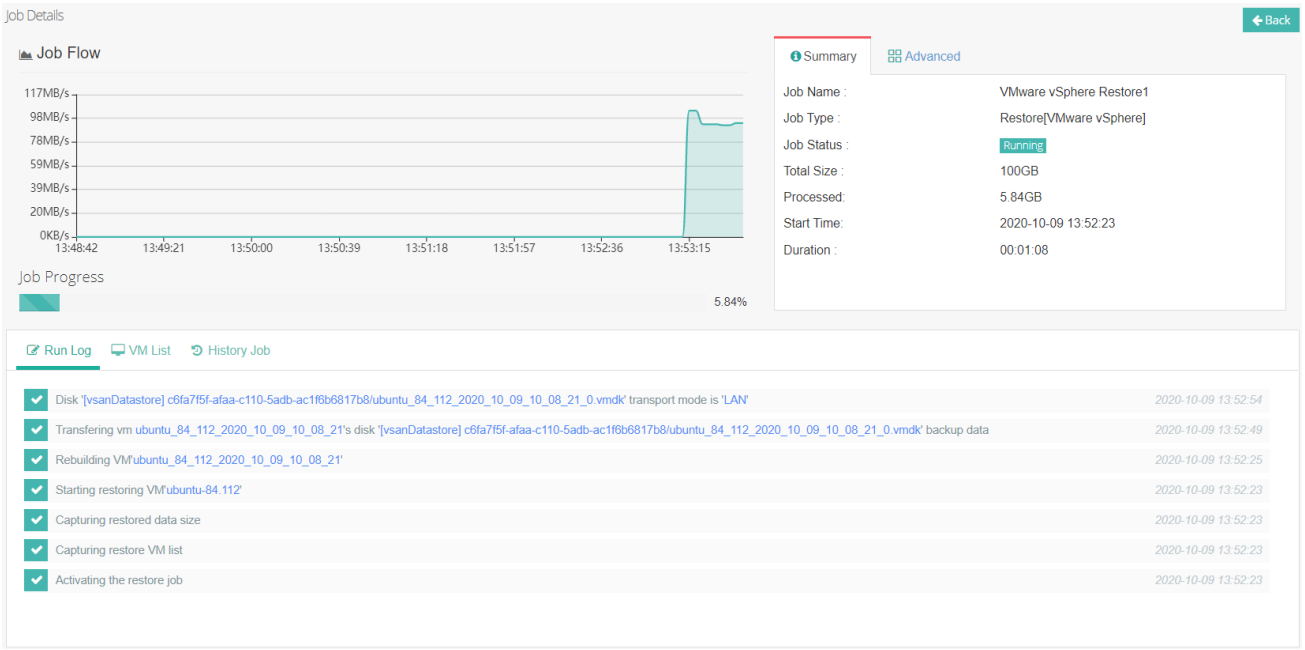
After creating a new restore job, you will be redirected to the **Monitor Center** > **Jobs** page, and you'll be able to see the VM restore job you created in the job list.



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

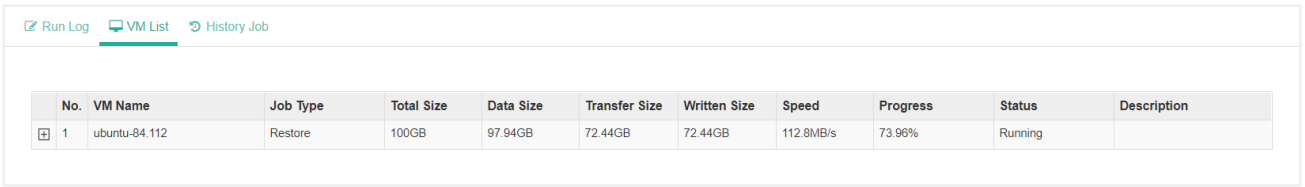
If you want to manually start the job, please click on **Options**, and then select **Start Job** to run it manually.

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



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

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



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

Warning

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

Instant Restore

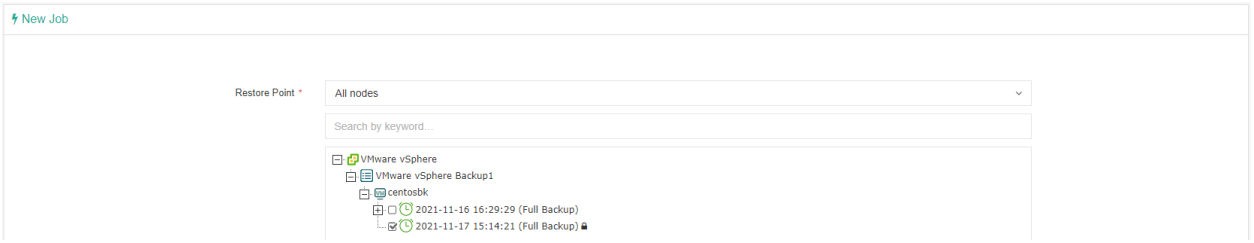
VM Instant Restore helps to recover a VM within 1 min, minimizes the downtime of critical businesses. It can be very helpful in emergency situations to directly start a VM from its backup data, without the need to transfer backup data back to production storage then resume the VM.

Note

Instant Restore is currently not supported with Microsoft Hyper-V and OpenStack in Vinchin Backup & Recovery v6.5.

Create Instant Restore Job

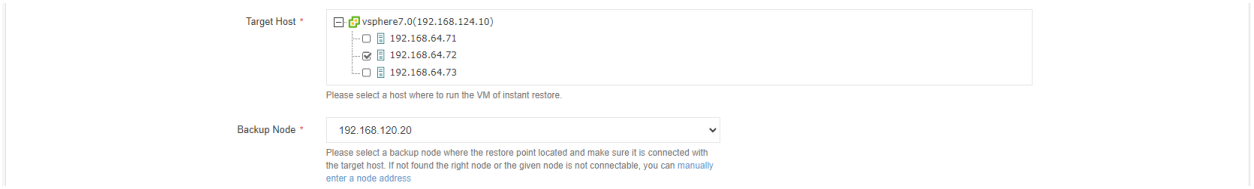
To create an Instant Restore job, please go to **VM Backup** > **Instant Restore** page, select a target VM restore point under your virtual infrastructure which you want to instantly recover. You can quickly find the target restore point by specifying backup node and selecting Group by VMs or Group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



Note

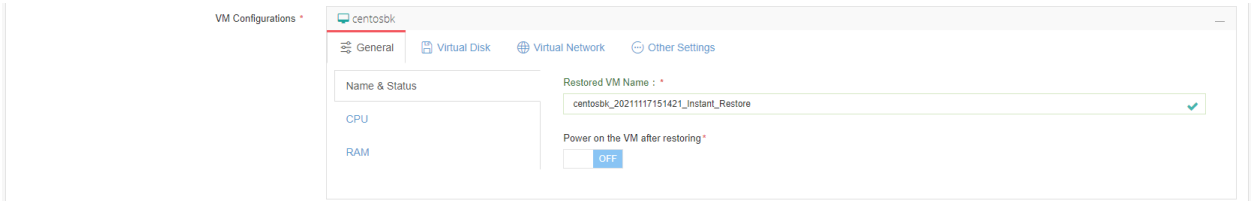
The restore point to be used for instant restore can be a full backup restore point, an incremental backup restore point or a differential backup restore point, but you can only select one restore point for each instant restore job.

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 is mounted.

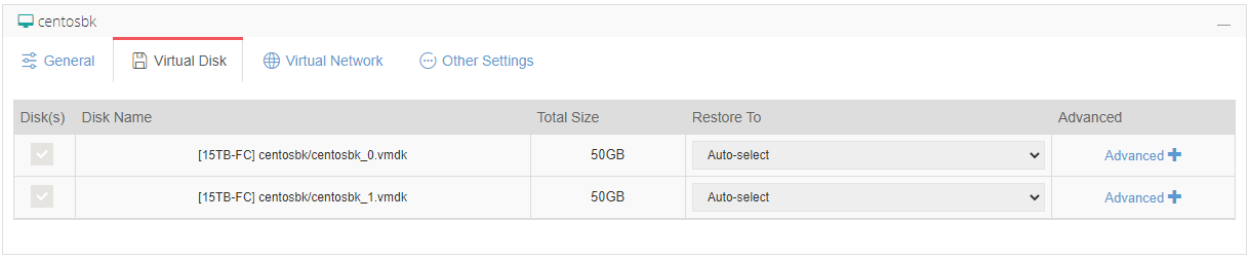


When a host is selected, in the VM configurations section it will show loading state, it will take a few seconds to request for the virtual platform resources information.

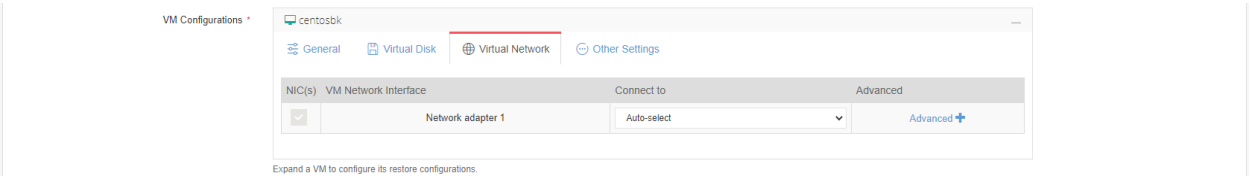
Under **General** tab, you are able to set VM name, power state, CPU and RAM size for the instant restore VM.



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

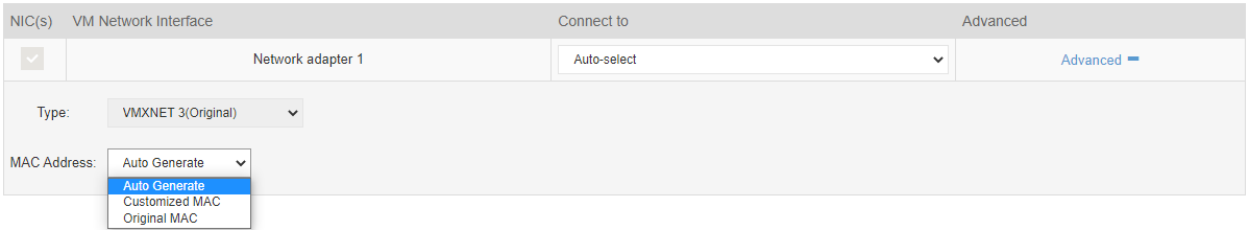


Virtual Network: It allows you to select the virtual network to be connected to and the MAC address assignment of the restored VM.



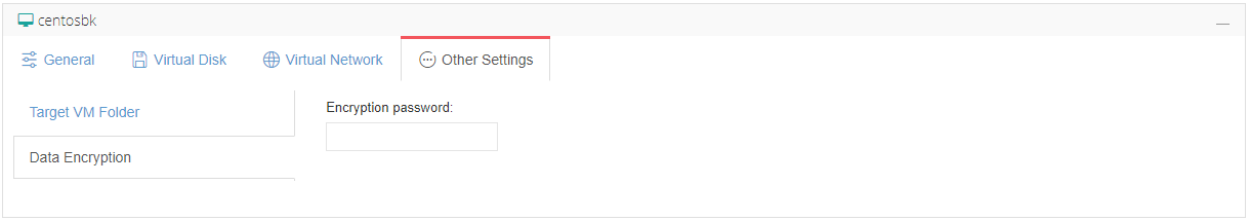
In the **Connect to** column, you can select a desired virtual network for specific virtual network interface of the VM, by default it will automatically select one from the available virtual networks.

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



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

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

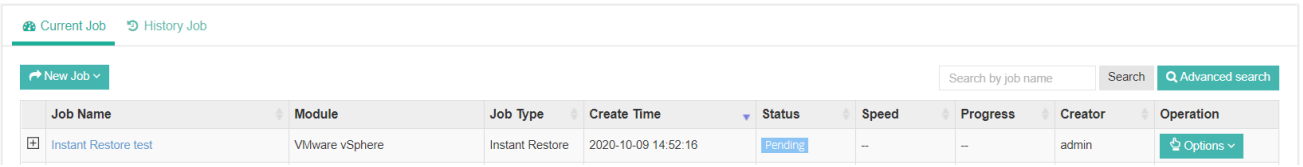


If the VM backup data is encrypted (Data Encryption enabled in backup job), when restoring the VM you need to provide the data encryption password for verification under Other Settings tab, otherwise without the data encryption password, the VM cannot be restored.

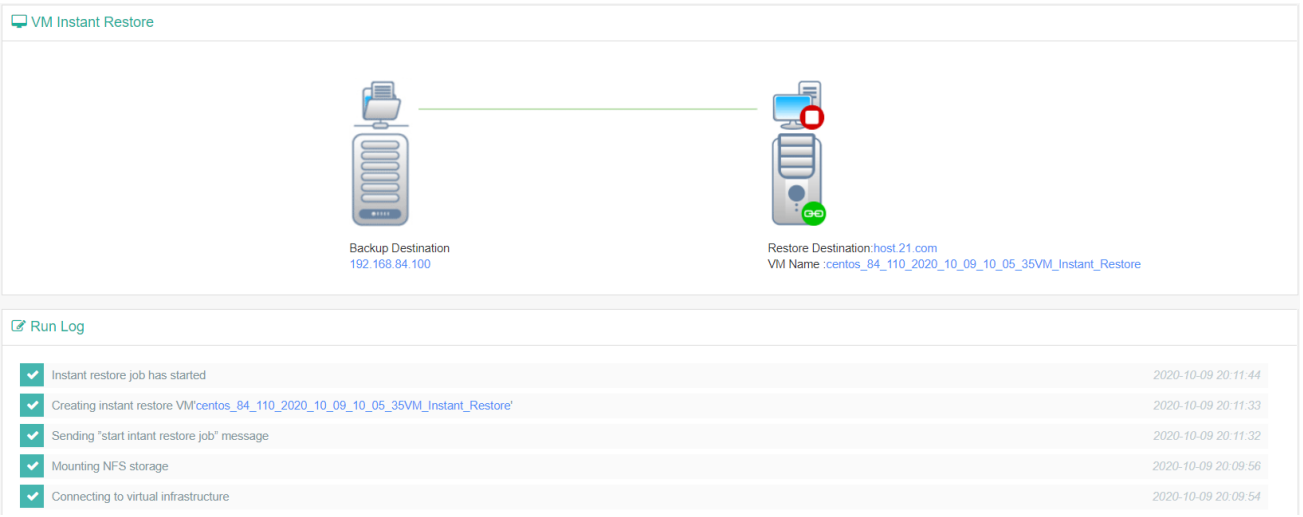
Once done, click on OK button to submit the creation of the instant restore job.

Instant Restore Job 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.

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

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

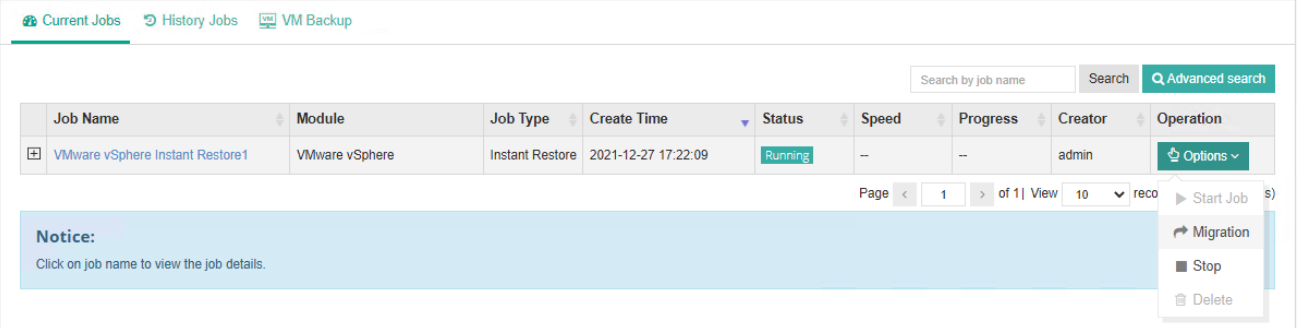
Warning

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

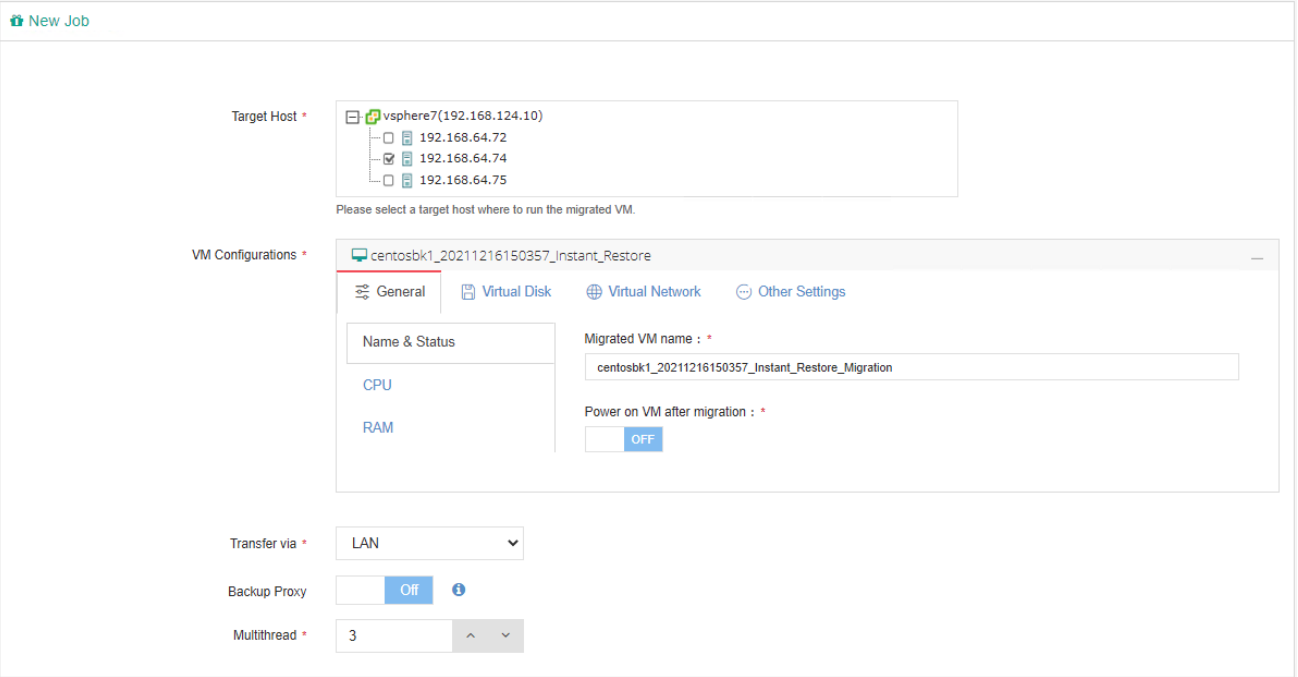
2. Do not create snapshot on the instant restore VM, or change any disk information. Otherwise, error will occur to the instant restore VM or it will crash.

VM Migration

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



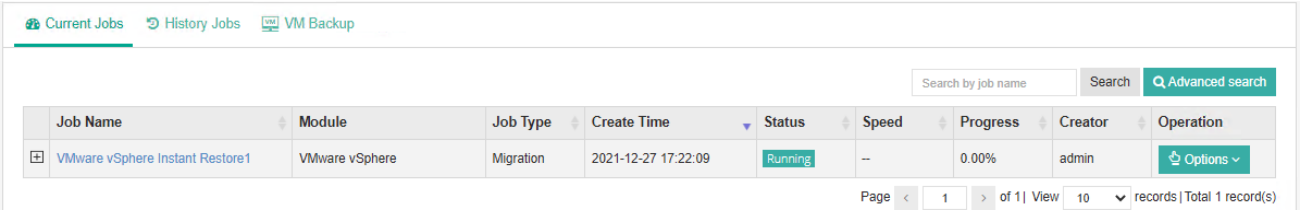
Select a host where to migrate the VM. Then you can rename the migrated VM and choose to whether power on it after migration, set virtual disk configurations, virtual network configurations for the VM. For more details of the VM Configurations please refer to Create VM Restore Job.



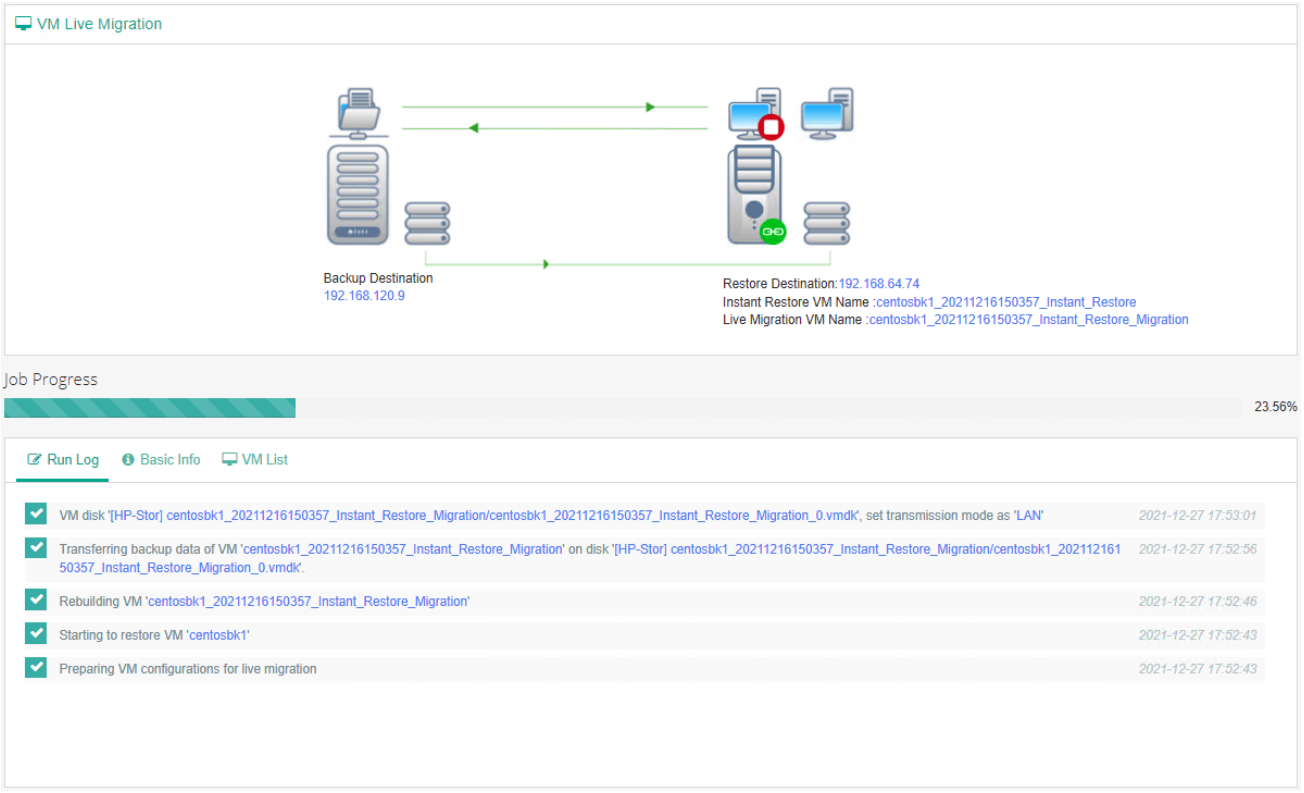
For the password verification, it's not required to perform VM migration, because password verification had already been done during VM instant restore job creation process.

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

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



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



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

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

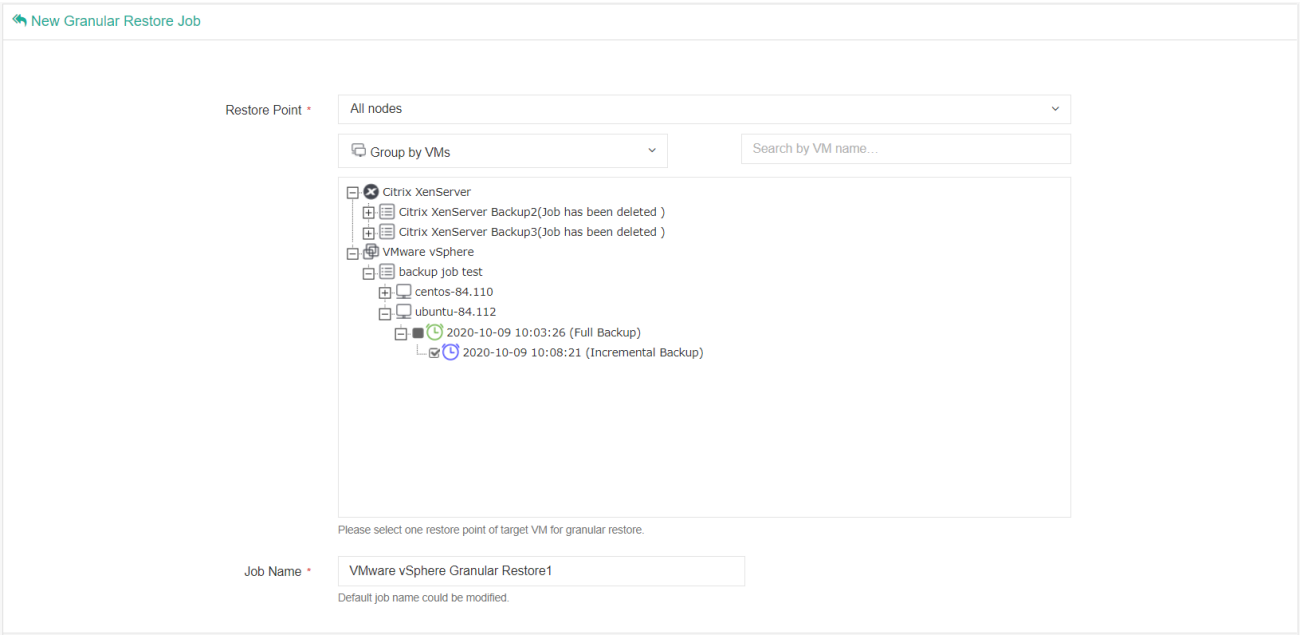
Warning

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

Granular Restore

Create Granular Restore Job

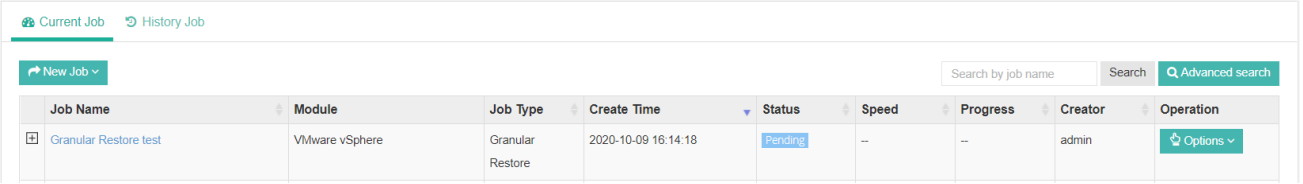
Granular Restore feature allows you to recover files or folders from the VM backup restore point, you don't have to restore the entire virtual machine for the purpose of recovering some files.
To create a granular restore job, please go to **VM Backup** > **Granular Restore** page, you will see all the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

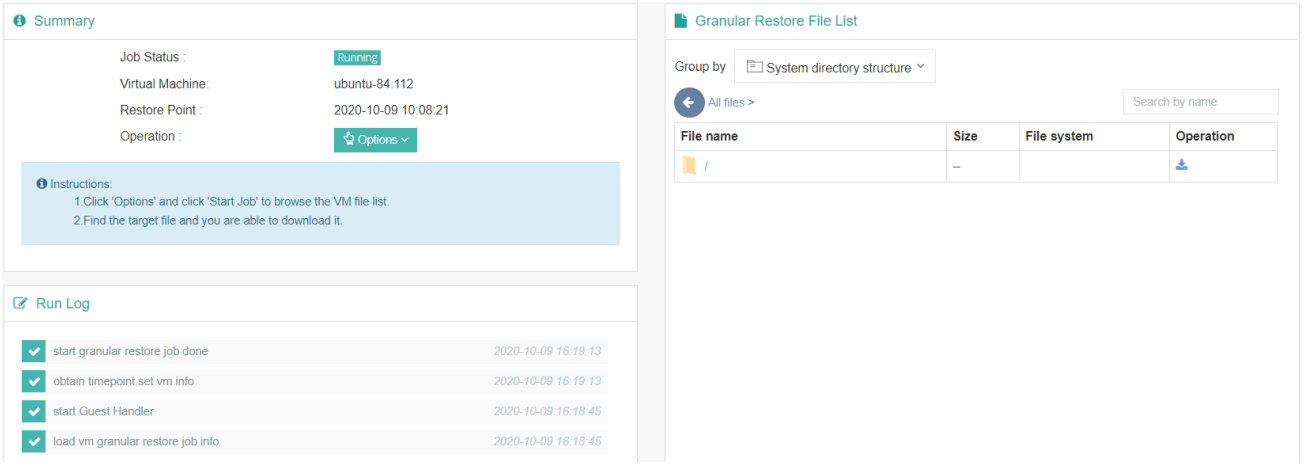
Granular Restore Job Operations

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



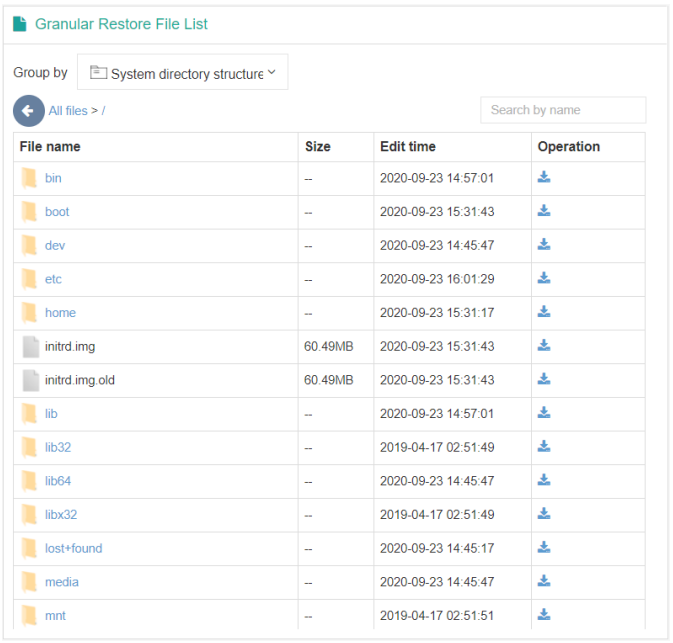
To run the granular restore job, please click on **Options**, then select **Start Job**. And the job status will change into preparing. The preparation process will take several seconds to several minutes depending on the VM size and the performance of Vinchin Backup Server hardware. After this, the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

When you get running status, please click on the job name to browse the file list of the VM.



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

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



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

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

Note

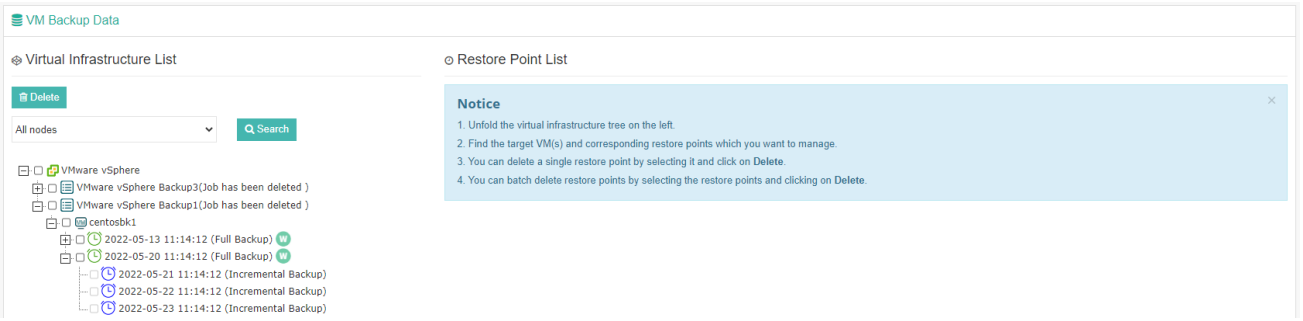
Once you have done retrieving the files, please return to current job list, and stop the granular restore job. As if the granular restore job keeps running, certain system resources will always be occupied. And if the job is no longer needed, you can also delete the job from the current job list.

Backup Data

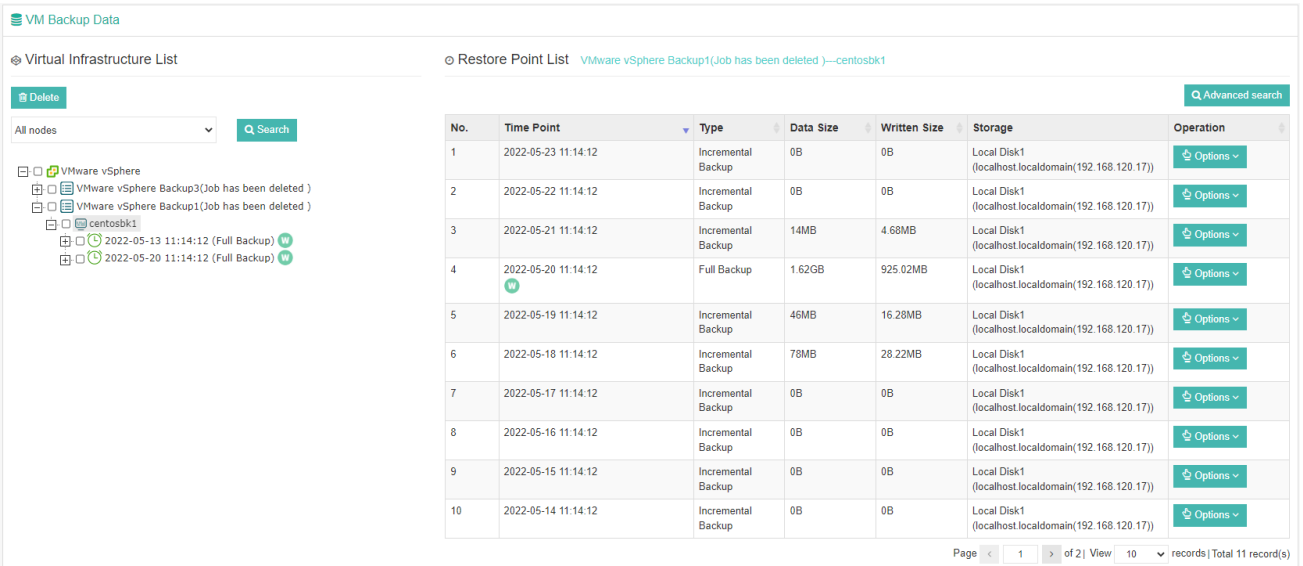
After running each VM backup job session, all the VM backup data can be found and managed from **VM Backup** > **Backup Data** page.

View Backup Data

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



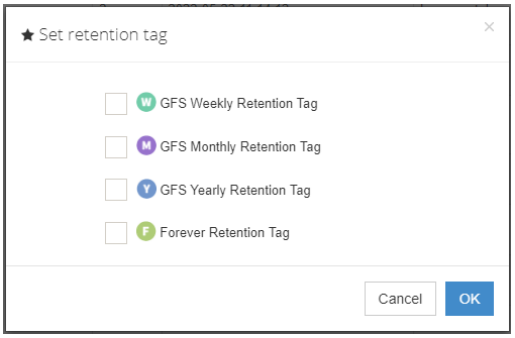
Each restore point is named with the timestamp of its creation and will be marked with its backup type. To view more information of the restore points, simply click on the VM name, all the restore points of the selected VM will be listed in the right with more detailed information.



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

Retention Tags

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



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

Delete Backup Data

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

To delete VM backup data, please go to **VM Backup** > **Backup Data** page. There are two approaches to perform the deletion, batch (or single) deletion of restore points from the left side tree view and single restore point deletion from the right side restore point list view.

Deleting restore point(s) from the tree view.

Please unfold the virtual infrastructure and the associated backup job, and unfold the VM which you wish to delete backup data from. Then select the restore point(s) you wish to be deleted and click on the **Delete** button on the top left of the tree view. You'll have to provide you password to confirm the deletion of selected restore point(s).

If it's a standalone full restore point, no incremental or differential restore points dependent on it, you can select and delete the standalone full restore point directly.

If it's a backup chain, formed by a full restore point and a series of incremental (or differential) restore points dependent on the full restore point, you can only delete the backup chain from the tree view.

Deleting restore point from the restore point list view.

Please select a VM from the left tree, the associated restore points will be listed on the right-side list view. By clicking on the **Options** button of a specific restore point and selecting **Delete** you are able to delete that single restore point, no matter it's full, incremental or differential.

If it's a standalone full restore point, no incremental restore points or differential restore points dependent on it, you can delete the standalone full restore point directly.

If it's a backup chain formed by a full restore point and a series or incremental restore points dependent on the full restore point, while deleting the incremental restore point in the end of the incremental chain, it will be directly deleted, if you delete any other restore point it will lead to data blocks merging with the next restore point. For example, you got an incremental backup chain, full on Monday, incremental on Tuesday and Wednesday, if you delete the incremental restore point of Tuesday, its data blocks will be merged with Wednesday incremental restore point. This mechanism can guarantee the backup data consistency.

If it's a backup chain formed by a full restore point and a series of differential restore points dependent on the full restore point, while deleting the full restore point is not allowed but you can delete the differential restore points, and there will not be data blocks merging required.

Virtual Infrastructure

Add Virtual Infrastructure

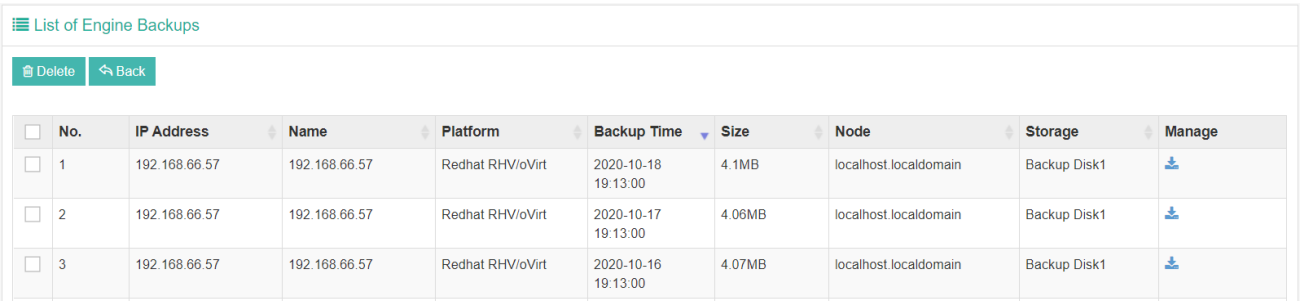
If your virtual infrastructure is VMware vSphere or Huawei FusionCompute, please refer to Register Virtual Infrastructure. For other virtual infrastructures, please first refer to Install Backup Plugin, then refer to Register Virtual Infrastructure.

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 RHV, oVirt or OLVM, and if you had enabled engine backup, the backup data can be managed by clicking on the **Engine Backup Data** button.



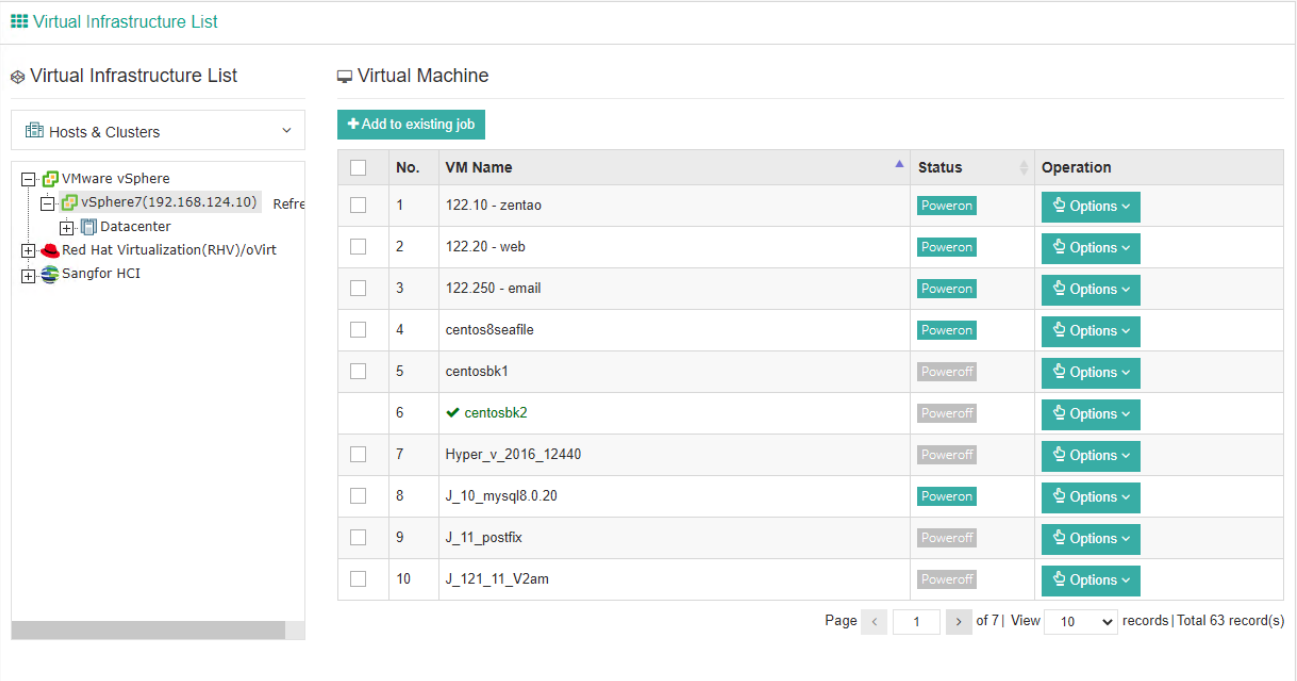
The engine backup data can be downloaded from Vinchin Backup Server, then to be uploaded to the engine host of the Red Hat RHV, oVirt or OLVM to restore the engine host configurations.

For the VM creation/deletion or any other updates of the VMs on your virtual infrastructure, you can rely on the **Auto Refresh** of the virtual infrastructures or you can manually perform the refresh. Click on the **Auto Refresh** button, you can set the auto-refresh time (default 60 minutes, minimum 5 minutes). And in the virtual infrastructure list, you can click on the **Sycn** button to manually refresh the corresponding virtual infrastructure.

From the virtual infrastructure list, you can also change the authorization status of the hosts in the virtual

infrastructure by clicking on the **Auth** button, for more details, please refer to Register Virtual Infrastructure.

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



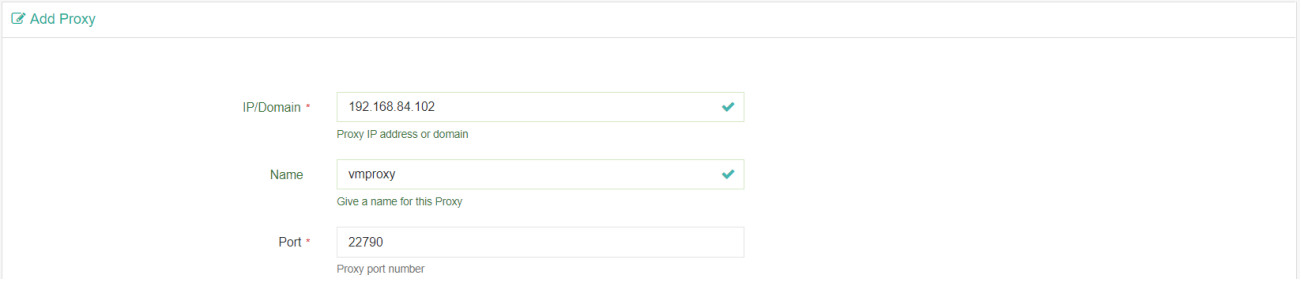
By selecting the VMs from the virtual machine list and click on the **Add to existing job** button, you can add the selected VMs to an existing backup job. Or you can add a single VM to an existing backup job by clicking on the **Options** button then select **Add to existing job**.

And by clicking on the **Options** button, you'll have options to suspend or power off a VM in **Poweron** status, or if the VM is in **Poweroff** status, you'll have option to power it on.

Backup Proxy

Vinchin Backup Proxy is an optional component for backup VMware vSphere virtual infrastructure, and it needs to be installed on the ESXi server as a VM. If you are using other virtual platforms, please just skip this part.

If Vinchin Backup Server is installed on the ESXi server as a VM, then a Backup Proxy is not needed. To add a Backup Proxy to Vinchin Backup Server, please go to **VM Backup** > **Backup Proxy** page and click on the **Add** button to add the Backup Proxy.

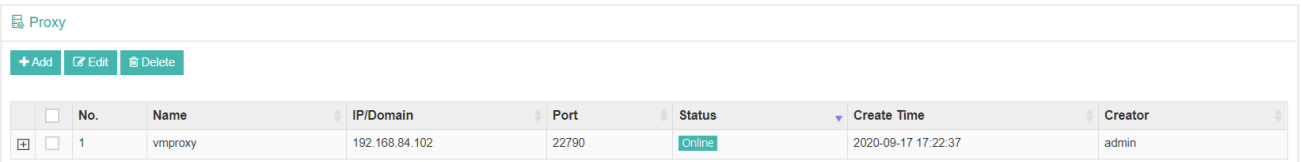


In the **IP/Domain** field, please enter the IP address of the Backup Proxy.

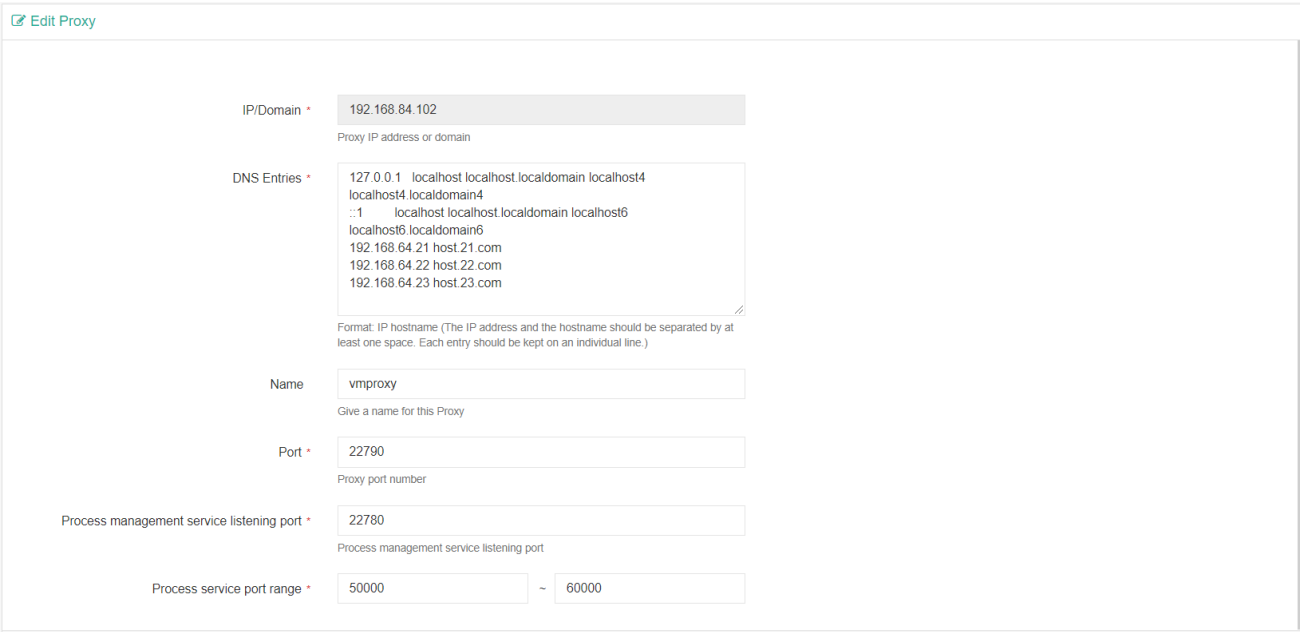
In the **Name** field, you can optionally define a customized name for the Backup Proxy.

In the **Port** field, the default port number should not be modified.

When done the above settings, click on **OK** button to add the Backup Proxy to the Backup Server.



By selecting the Proxy and clicking on the **Edit** button, you are able to edit the Proxy settings.



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

And usually the port number settings should not be changed.

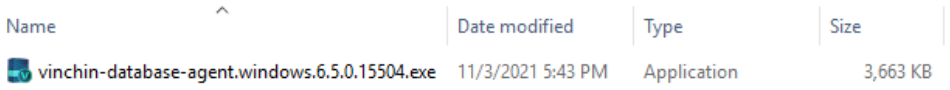
Database Backup

SQL Server Database Backup and Restore

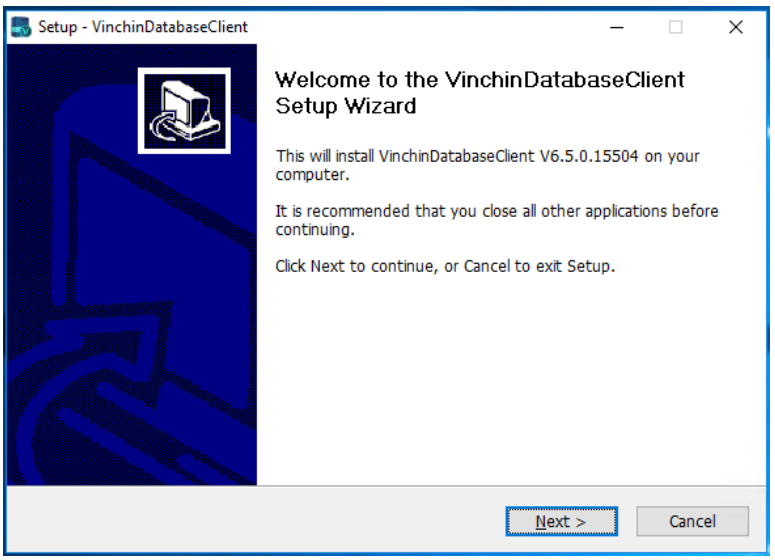
Install Database Backup Agent

The supported Windows systems including Windows Server 2008, 2012, 2016 and 2019.
To install SQL Server Database 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 **Database Backup Agent**. In the **Operating System (OS)** dropdown list, please select Windows. Then click on Download button to download.
The downloaded database backup plugin should be an executable exe file.

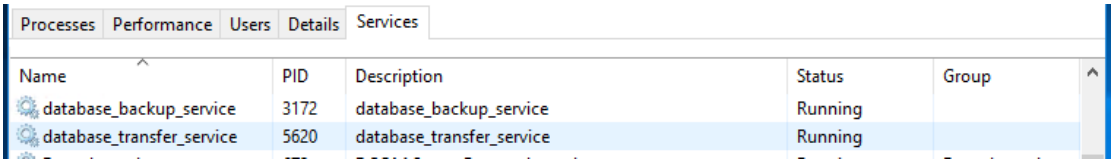


To install the backup plugin, please right click on it and select **Run as administrator** to install the backup plugin with administrator permissions.



Please follow the installation wizard to complete the database backup agent installation.

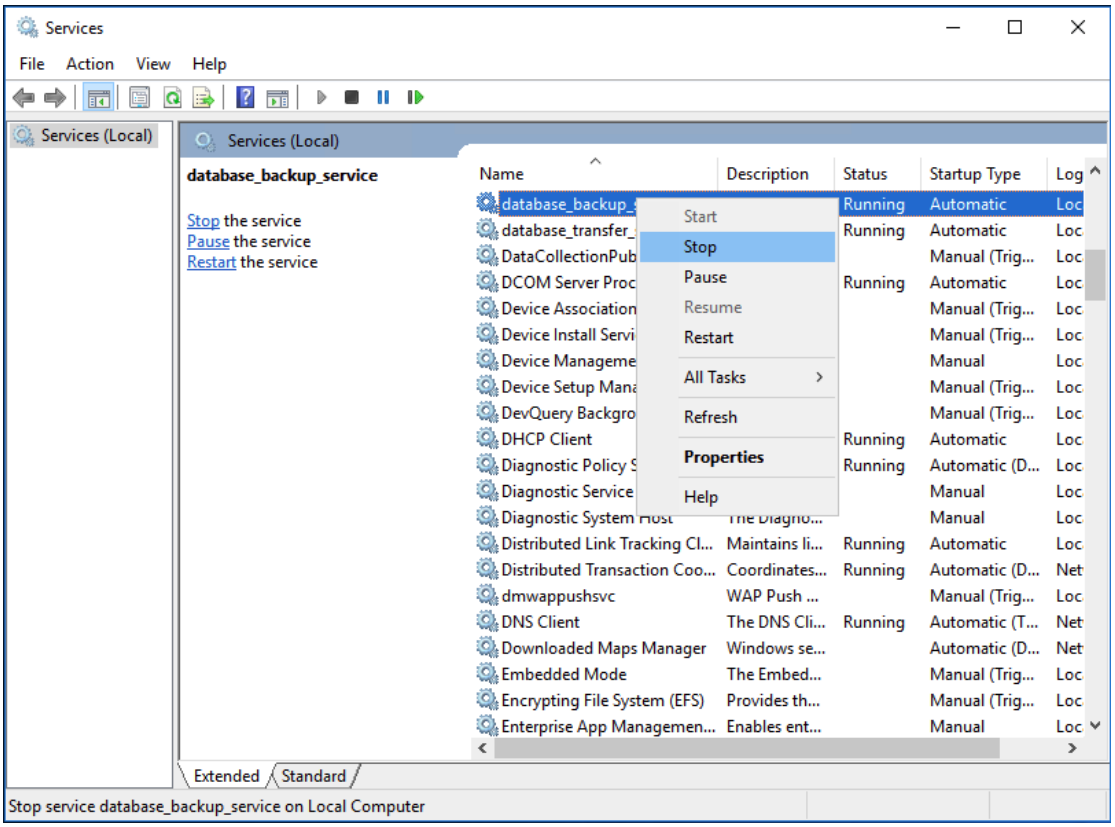
Once the installation completed, there will be two services 'database_backup_service' and 'database_transfer_service' running which could be found in Windows **Services**. Then you have successfully installed the SQL Server backup plugin on the Windows system.



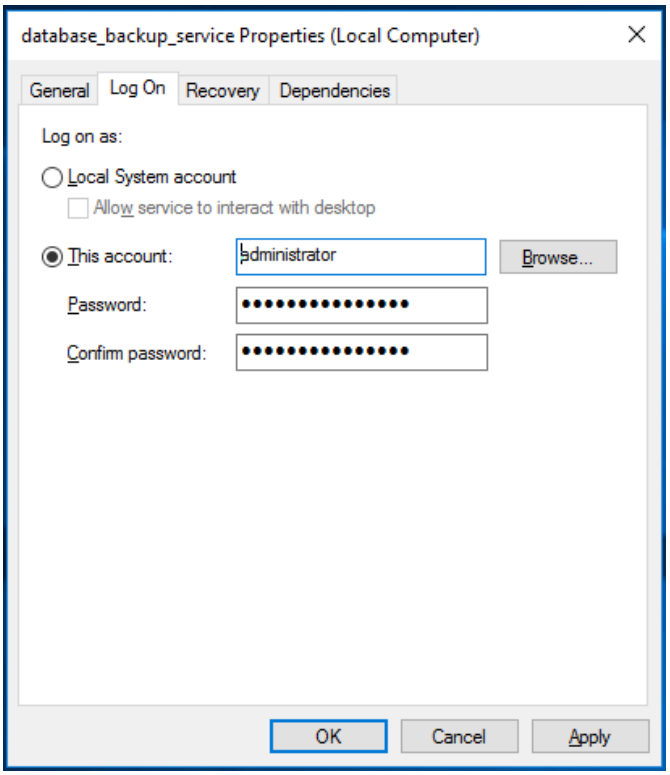
There are 3 ports: 20200, 20300, 20400 will be opened on your database server while installing the database backup agent.

If you want to use Windows administrator to backup the database, please edit the database backup services to log on as **administrator** from Windows **Services**.

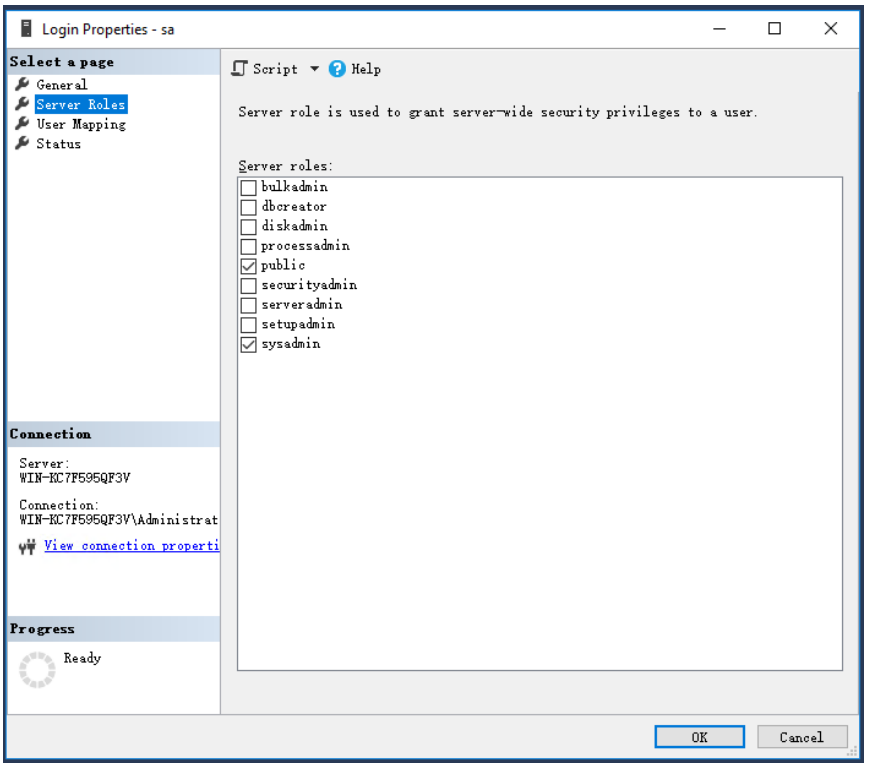
Please first stop 'database_backup_service' and 'database_transfer_service' services by right clicking on them and select **Stop**.



When these 2 services had been stopped, right click on them and select **Properties > Log On**, select log on as **This account**, then fill in the administrator account name and password, click on **Apply** and restart the services.



Check the database user permissions which you wish to perform SQL Server database backup, at least ensure the

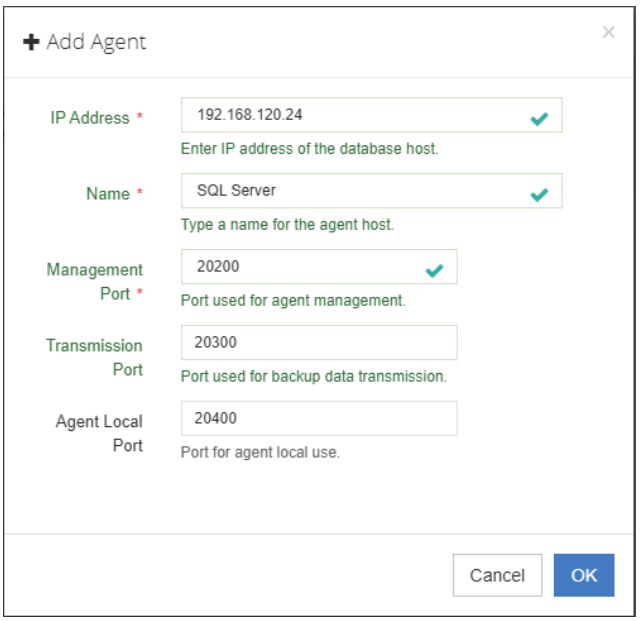


user have **sysadmin** permission, check the details as below.

Register Database Backup Agent

After the installation of Vinchin database backup agent, please open Vinchin Backup Server web console and go to **Database Backup** > **Backup Agent** page to register the database backup agent.

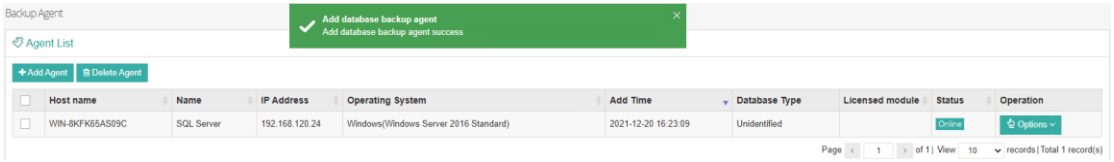
Click on Add Agent button to start registering a database backup agent.



In the IP Address field, enter the IP address of the database server which you wish to backup, database agent must be installed on the server.

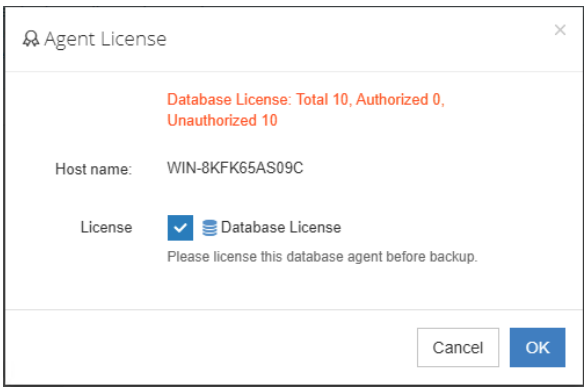
In the Name field, you can optionally enter a name for identification. For the Management Port, Transmission Port and Agent Local port, please use default settings and do not change them.

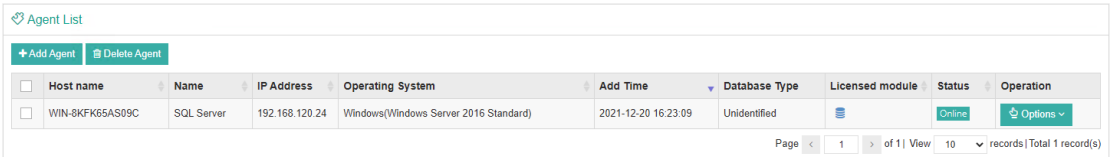
When done, click on **OK**, then in the **Agent List** it will show the database backup agent you just added.



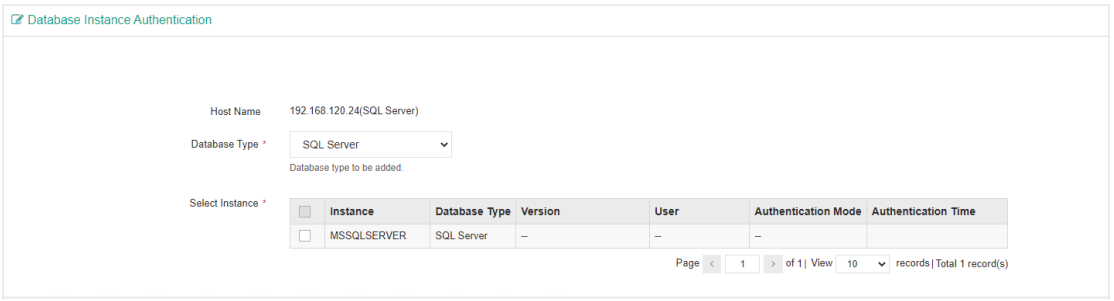
Once a database agent had been added, you need to license the database agent and authenticate the database instance before performing database backups.

Click on **Options** > **License** in the popup dialog, click on License checkbox to license the database backup agent.

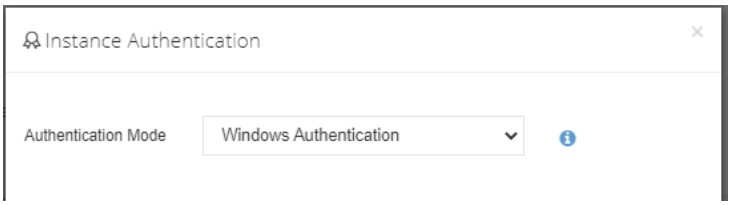




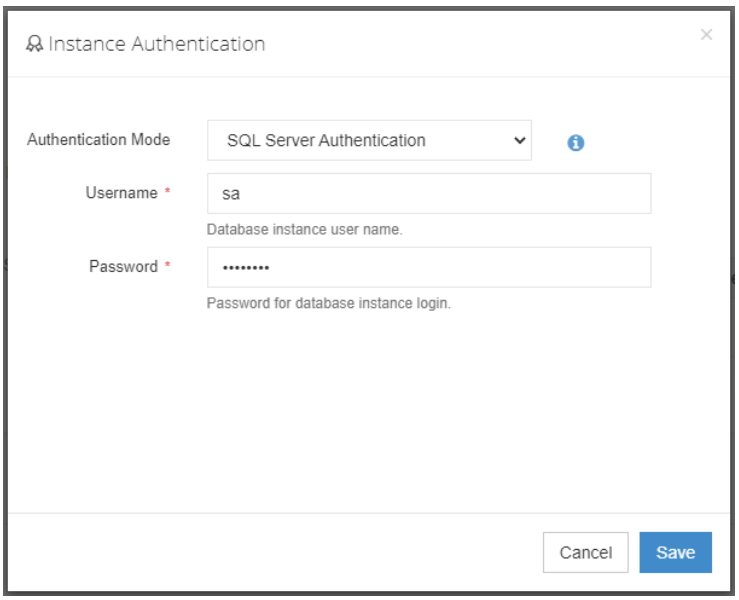
Click on **Options** > **Authentication** to authenticate the database instance for backup. In database type dropdown list, select SQL Server. It will automatically show database Instance of the database server. Select the Instance you wish to backup and click on **Authenticate** button.



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



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



Note

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

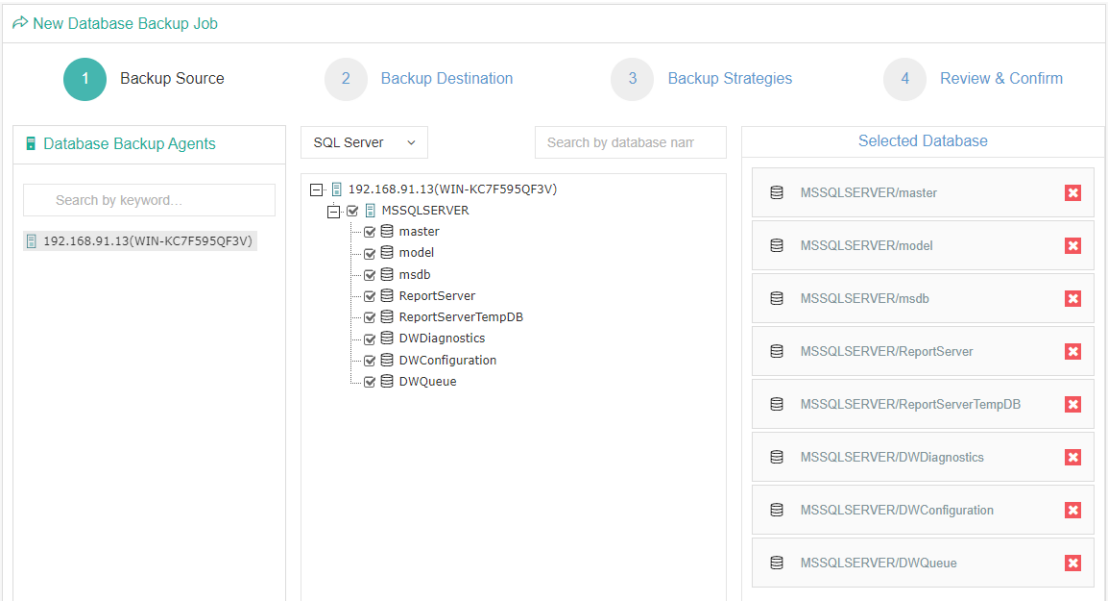
SQL Server Database Backup

Create Database Backup Job

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

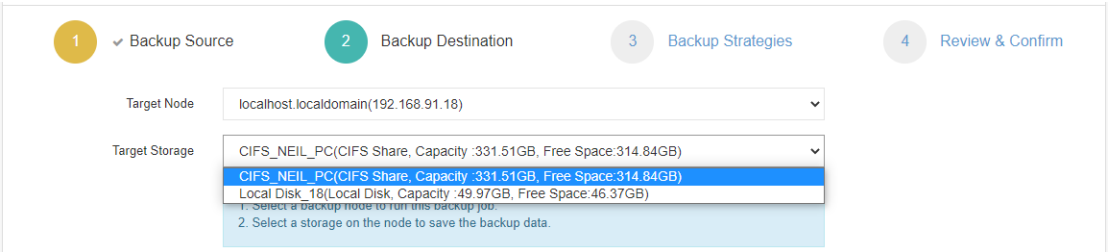
Step 1: Backup Source

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



Step 2: Backup Destination

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



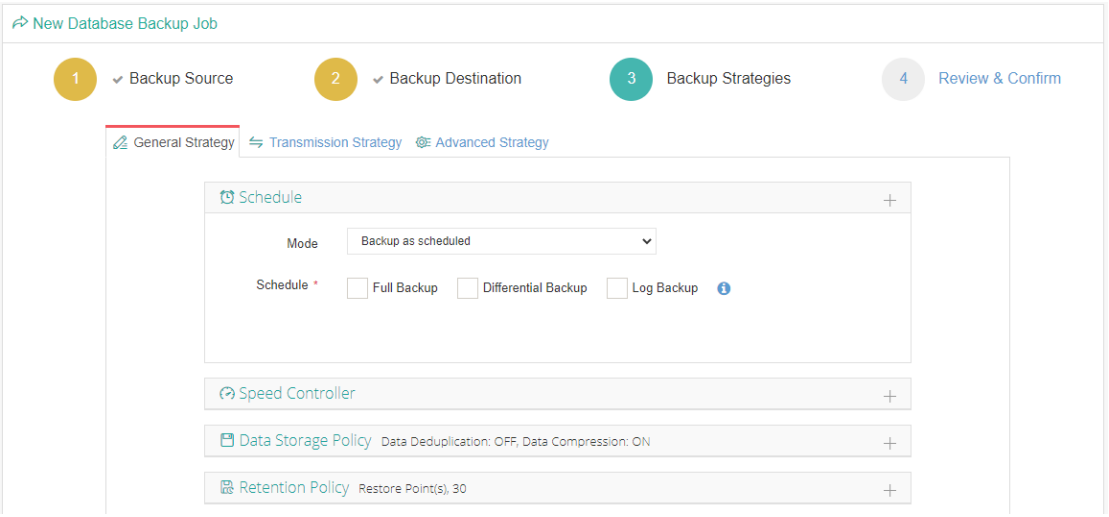
In the **Target Node** dropdown list, you can select a backup node on which you want the backup data to be processed and stored.

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

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

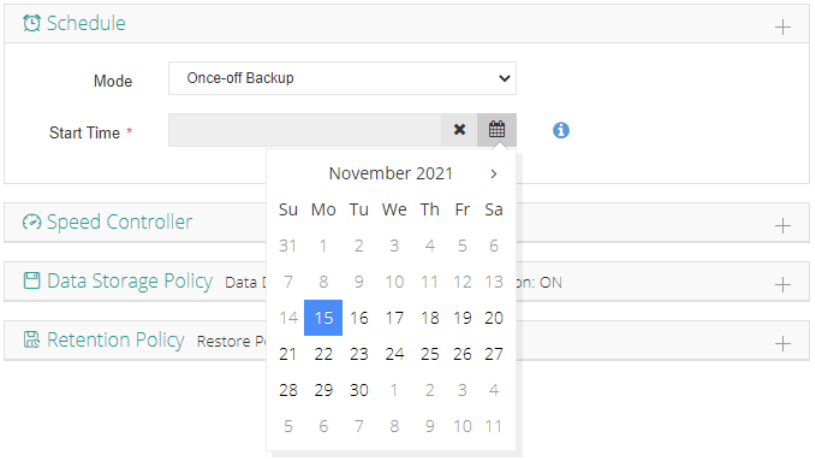
Step 3: Backup Strategies

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



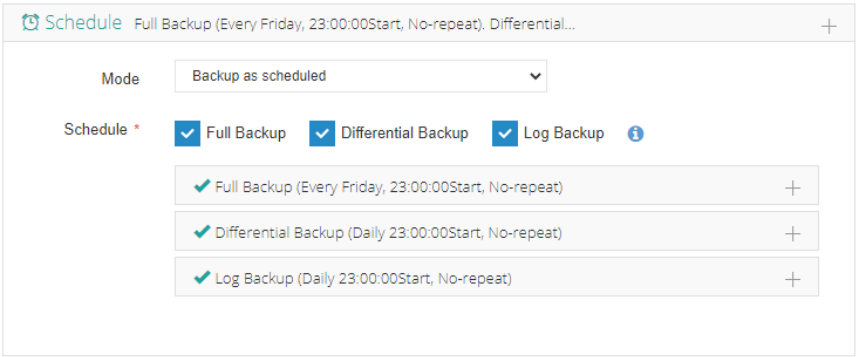
In the Schedule field, you can configure the time schedule of the backup job, you can configure the job as a **Backup as Scheduled** job or a **Once-off Backup** job.

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



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

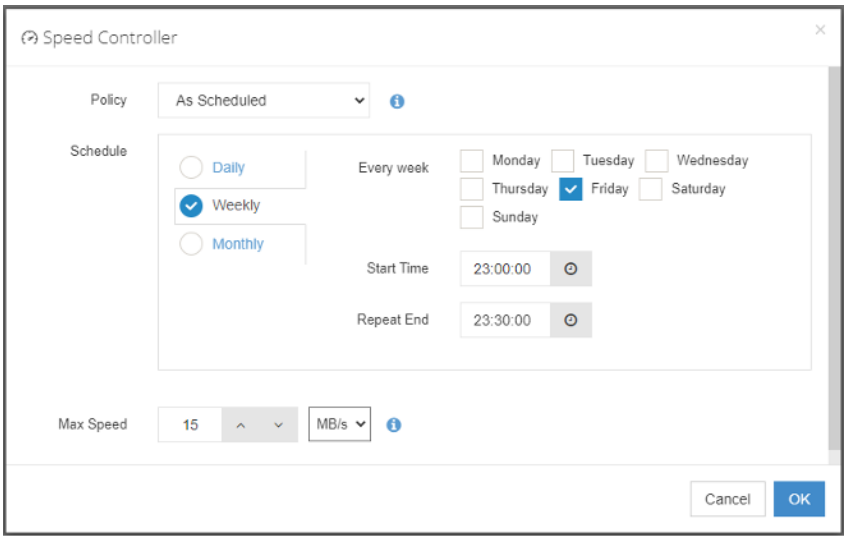
Here we take these three Backup as an example. Please set the backup mode and backup schedule as per your actual demands, then please click on **Next** to continue.



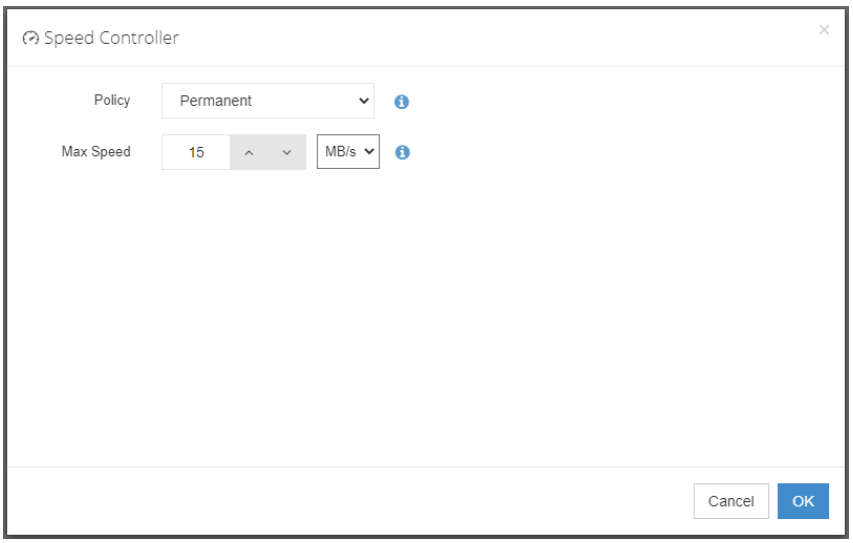
Speed Controller is optional. It can be used to limit the transmission speed during database backup if needed.

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

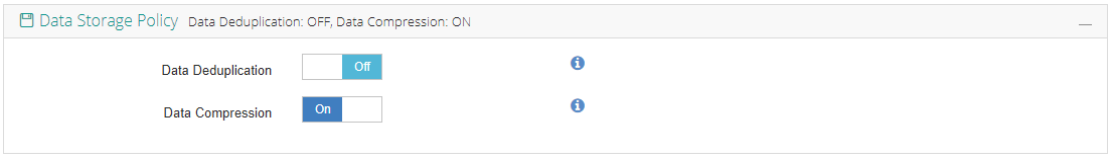
configured to limit the backup speed on Daily, Weekly and Monthly basis.



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



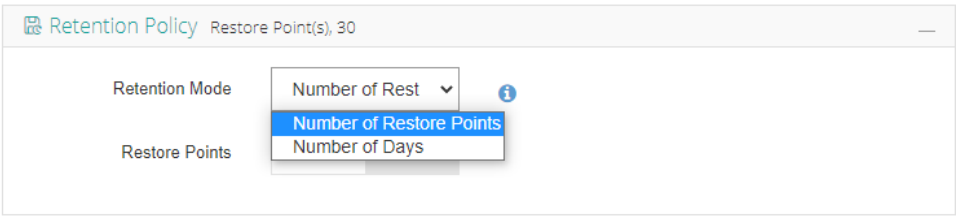
There are 2 options in Data Storage Policy section, Data Deduplication and Data Compression. By enabling these 2 options, the backup data will be deduplicated and compressed before saving into backup storage.



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

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

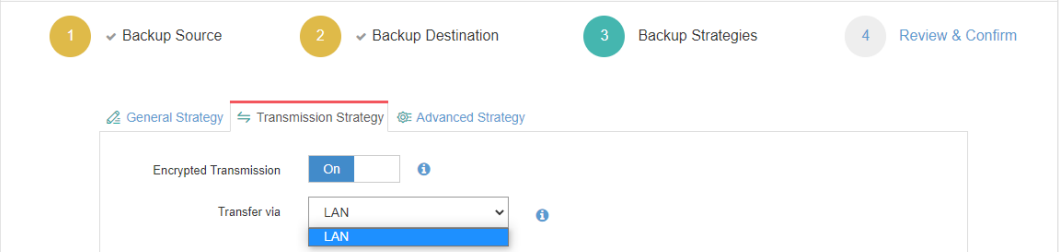
For retention mode **Number of Days**, Vinchin Backup Server will save the restore points within the specified number of days.



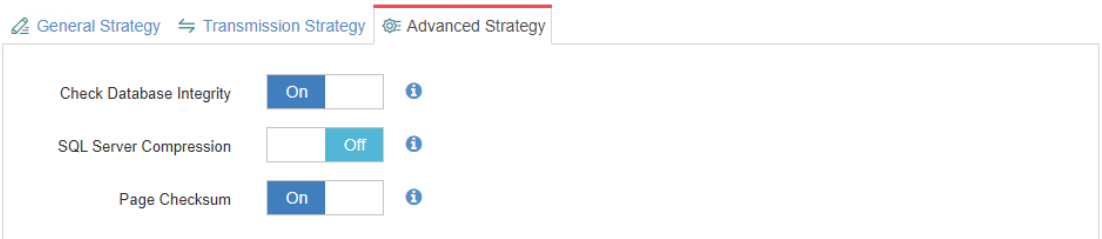
When the retention policy is triggered, the outdated restore points will be purged to comply with the retention policy.

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

The backup data will be transferred through LAN by default.



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



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

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

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

Note

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

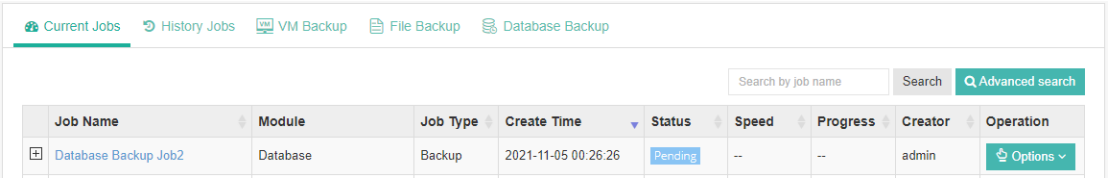
Step 4: Review & Confirm

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

A job name can be specified for identification of the database backup job, and by clicking on the Submit button to create the backup job.

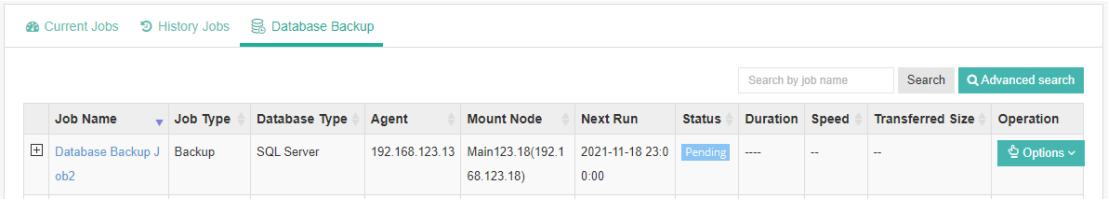
Database Backup Job Operations

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



The status of the newly created job will usually be **Pending**, when the time condition matches the schedule, it will automatically run. And the status will change to Running, you can also see the transfer speed here within the job list.

Besides the Current Job list, there's a dedicated tab to show database backup jobs. More detailed information of database backup jobs, including database type, database agent info, backup node, next run time and some more detailed information dedicated for database backup will be given.



By clicking on the job name you can check more detailed information on the **Job Detail** page.

For a scheduled backup job, after running one of the schedules, the status will change to Pending again and then wait for the next run.

For a once-off backup job, after running the job for once, it will be removed from the Current Job list. And you can find it from the History Job list.

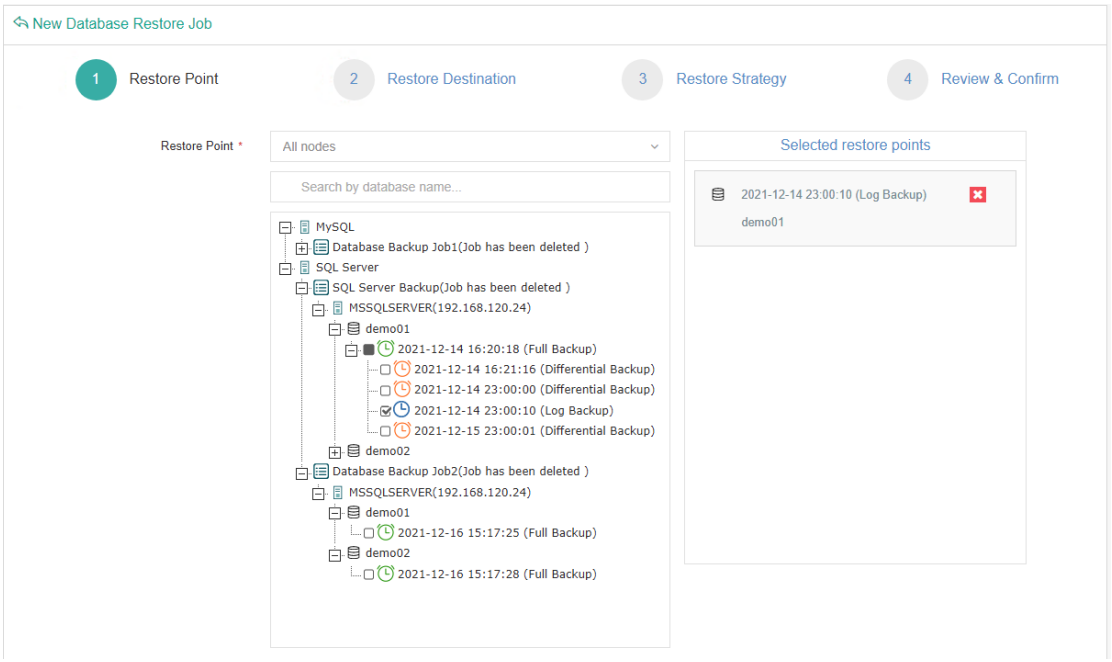
Database Restore

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

Step 1: Restore Point

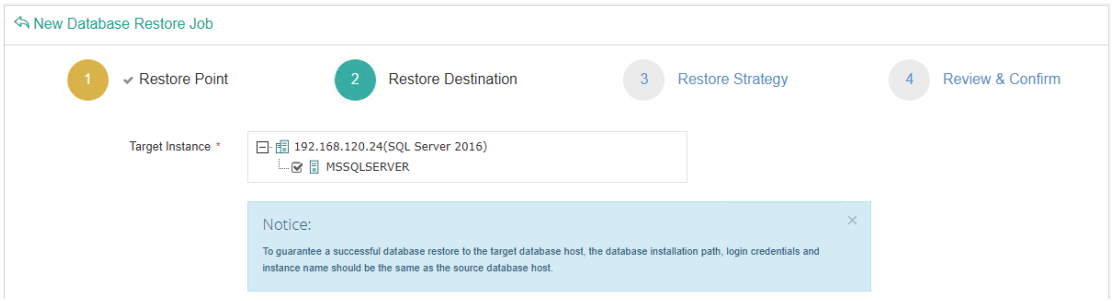
In the Restore Point dropdown list, select a backup node which stores the desired restore points.

Select a target database restore point under your database which you want to restore. You can quickly find the target restore point by searching the job name, database name or the date of the restore point. One restore job can only select one restore point.



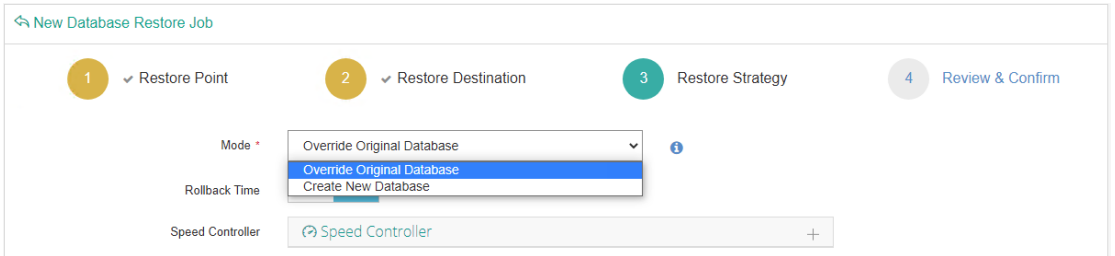
Step 2: Restore Destination

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

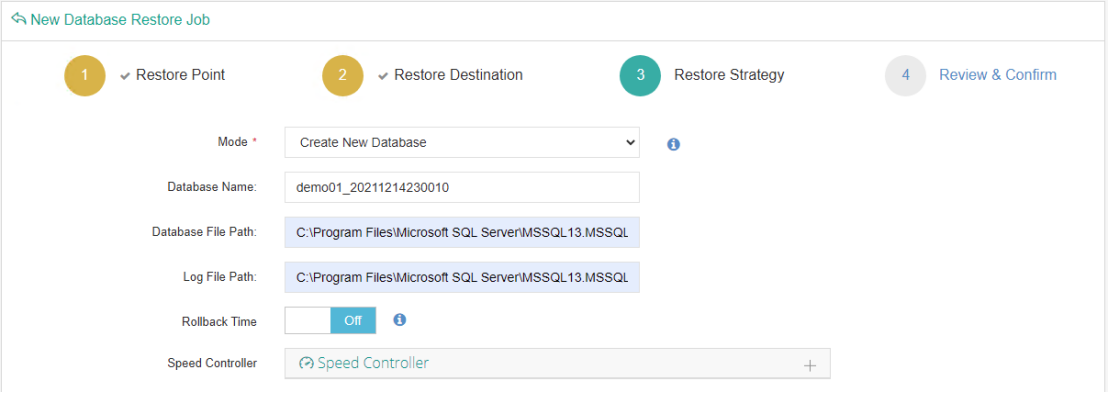


Step 3: Restore Strategy

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

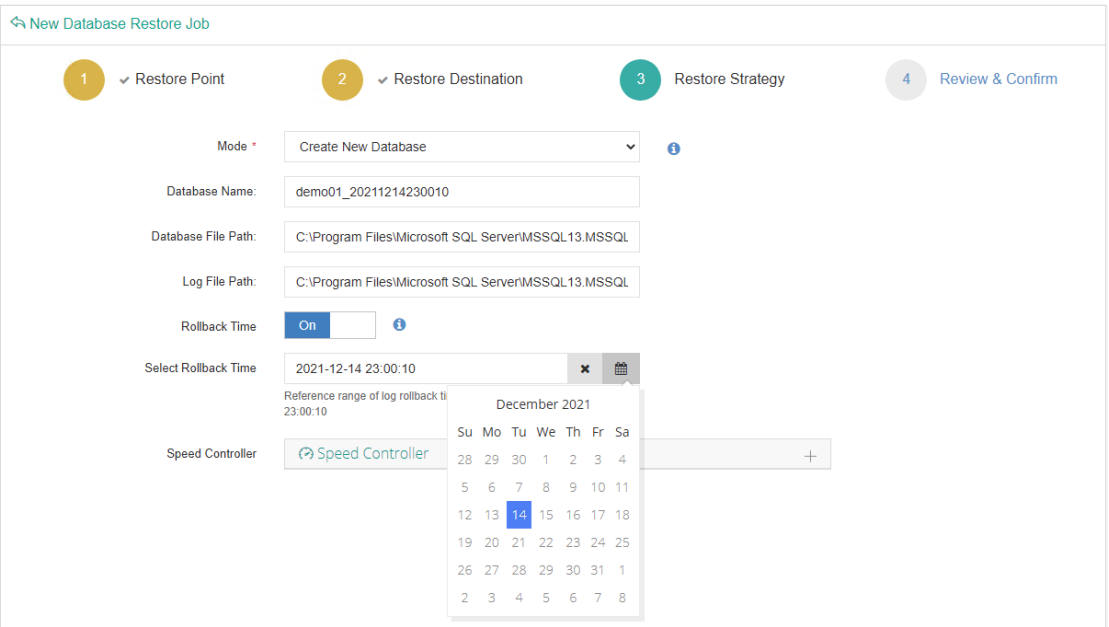


Select Create New Database need to edit database name, database file path, log file path. The path must be correct and have enough free disk space, the path will be automatically created during restore process.



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

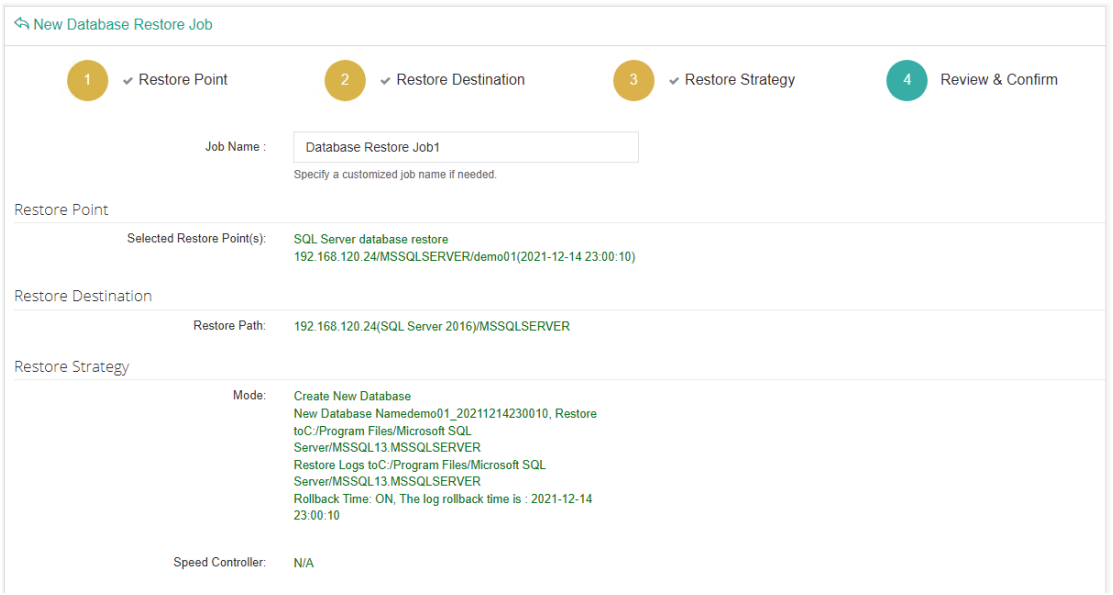
You can select the rollback time in second level within the reference range of log rollback time, so you can rollback the database to the state of any desired time point.



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

Step 4: Review & Confirm

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



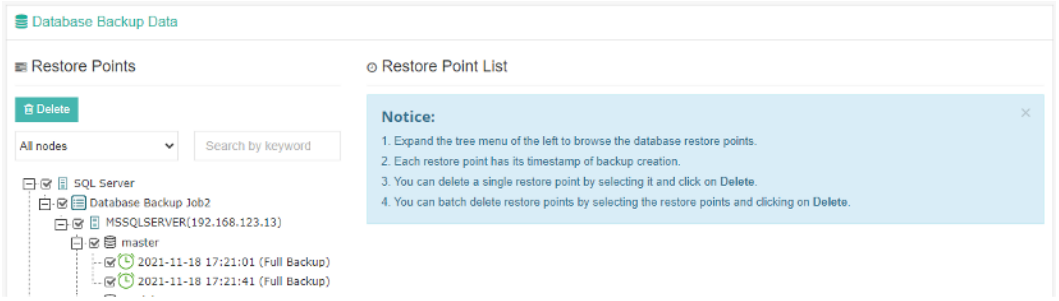
Once the job has been created, you'll be redirected to the **Monitor Center** > **Jobs** page.

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

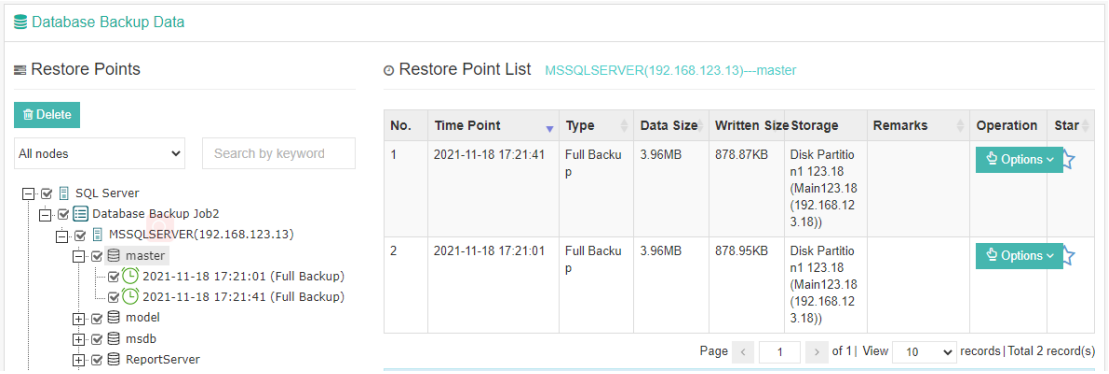
After this you can browse the restored job from History Jobs. Your restored data will be found in the path you configured during creating the restore job.

Database Backup Data

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



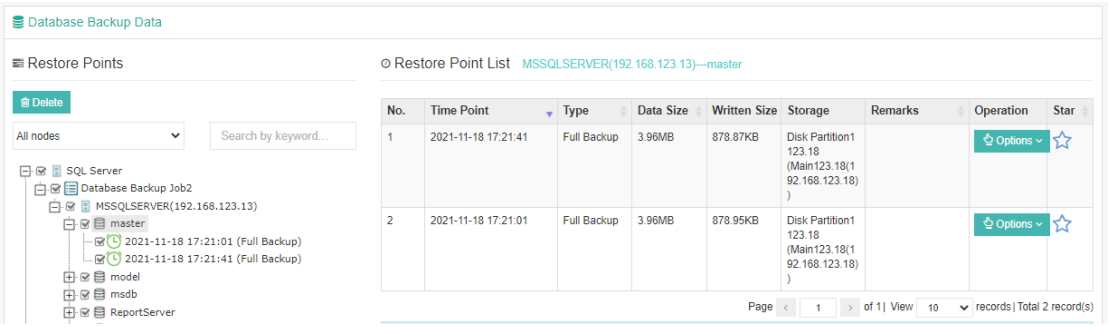
If you want to delete a restore point or multiple restore points, you can first select target restore point(s) from the left tree, and click on the **Delete** button. The differential backup and log backup cannot be deleted individually, they will be deleted along with the dependent full backup.



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

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

You can add remarks to the restore points, and click ☆ with full restore point to keep the full backup and its dependent differential and log backups to not be deleted by retention policy.



MySQL Database Backup and Restore

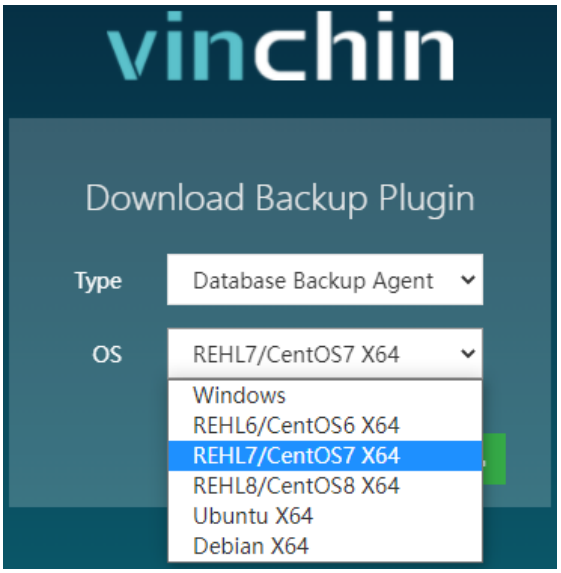
For MySQL database backup, supported MySQL database versions are as follows:

- MySQL 5.5.62
- MySQL 5.6.51
- MySQL 5.7.33
- MySQL 5.7.35
- MySQL 8.0.20

The supported Linux distributions and versions including RHEL 6 to 8, Centos 6 to 8, Ubuntu x64 and Debian x64, MySQL Windows version is not supported on current version.

Install Database Backup Agent

Please download MySQL database backup plugin from Vinchin Backup & Recovery login screen. Select the corresponding Linux distribution and version then click on the Download button to download the database backup plugin.



The downloaded backup plugin should be a .tar.gz package. Please upload the downloaded file to the database server for installation, 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-database-backup-agent-xxx.tar.gz
```

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

Enter the database backup plugin package folder.

```
cd vinchin-database-backup-agent-xxx
```

To install the backup plugin, run below command.

```
./db_backup_agent_install
```

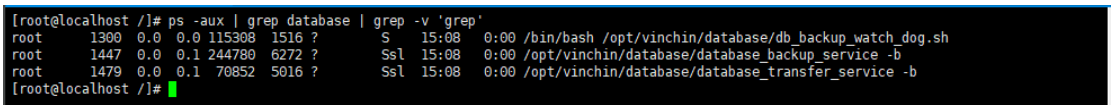
Use below command to uninstall (once uninstalled, database backup and restore will no longer work on this database server).

```
./db_backup_agent_uninstall
```

After installing the database backup plugin, please check its services use below command.

```
ps -aux | grep database | grep -v 'grep'
```

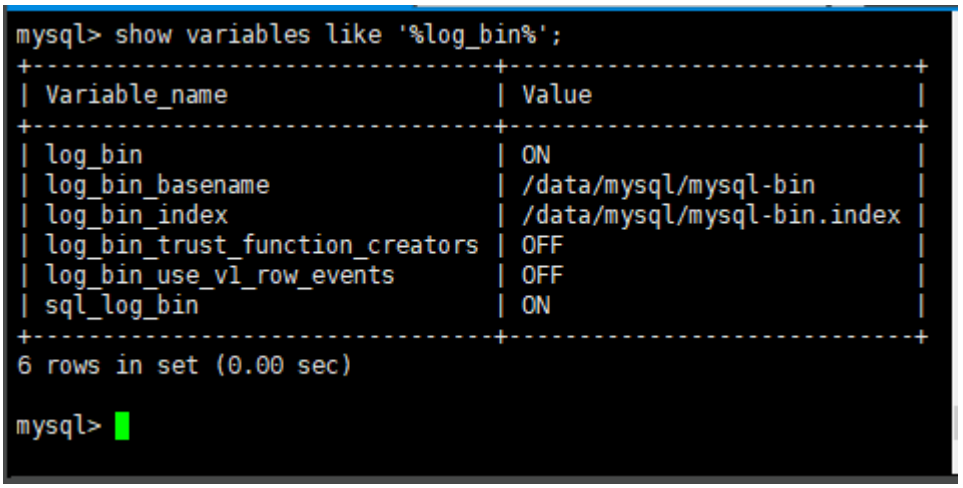
If you got the below output which has 3 services, bd_backup_watch_dog.sh, database_backup_service and database_transfer_service, this means database backup agent installed successfully, the services are up running and ready for backup and restore.



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

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

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

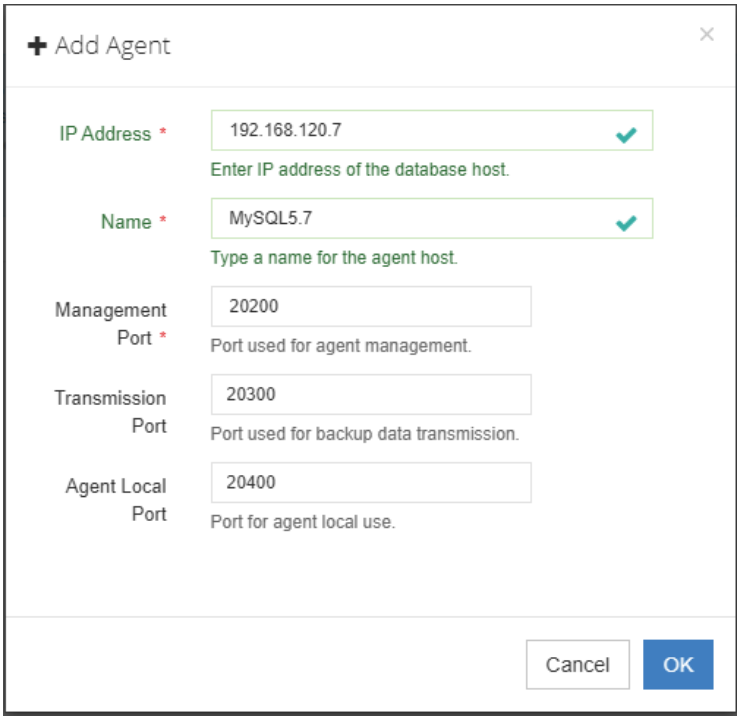


If binary logging is not enabled, it needs the database administrator to enable it.

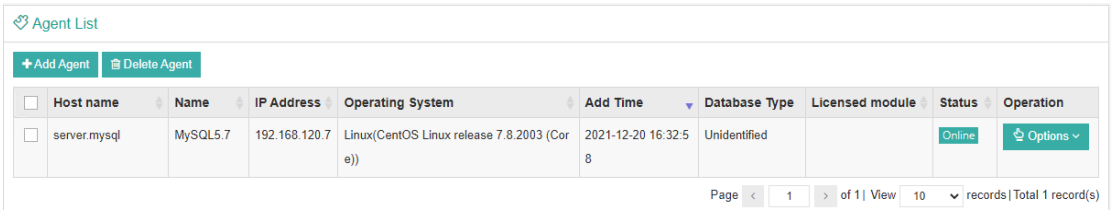
Register Database Backup Agent

After the installation, please open Vinchin Backup Server web console and go to **Database Backup** > **Backup Agent** page.

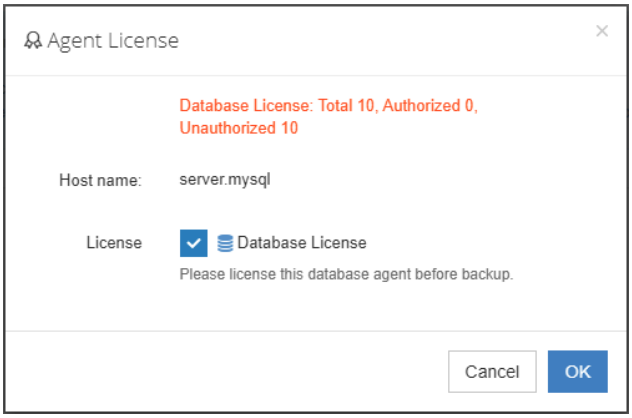
Click on Add Agent, enter the IP address and Name, Management Port set as default.



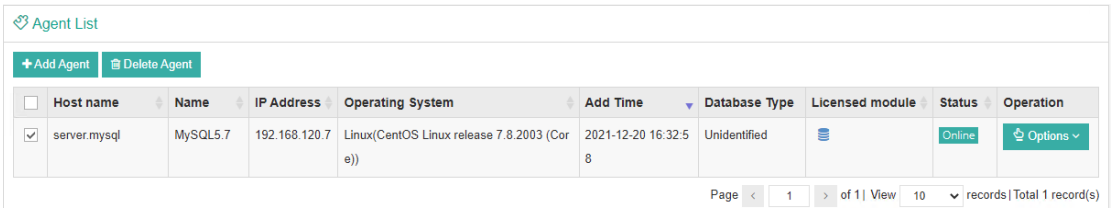
Click on **OK**, then will show the database you just added.



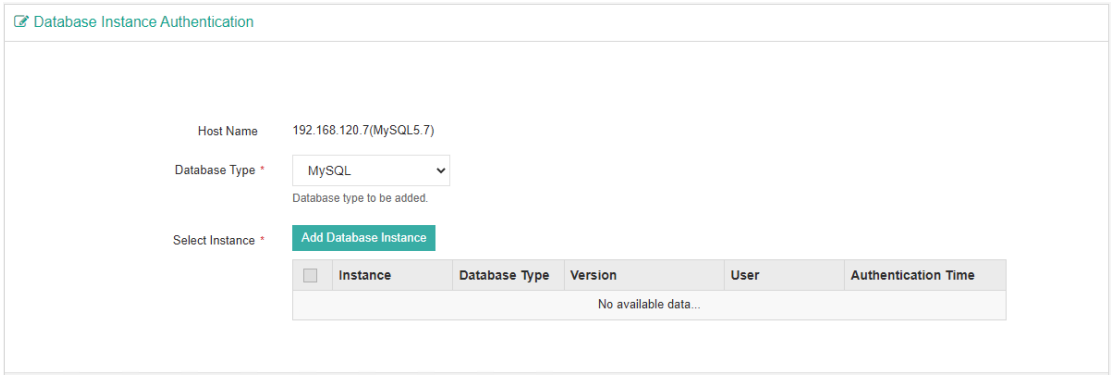
Once the database backup agent has been added, please click on **Options** > **License** to get it licensed for backing up.



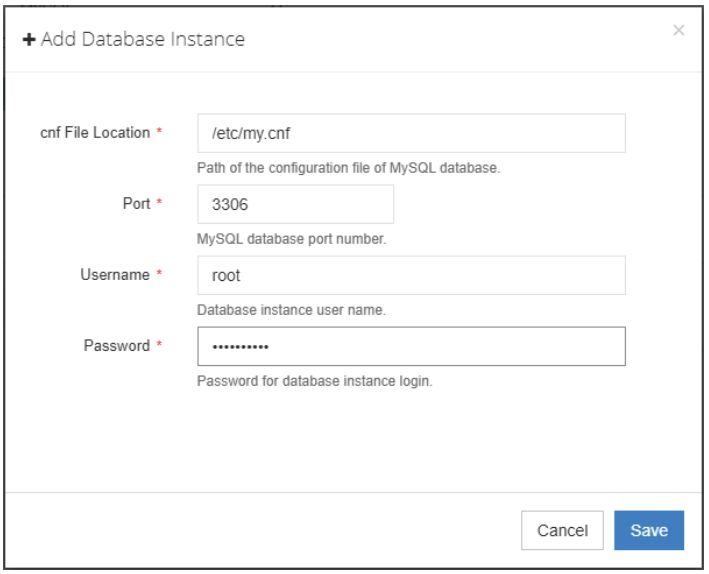
After licensing the database backup agent, please click **Options** > **Authentication** to get the database instance authenticated.



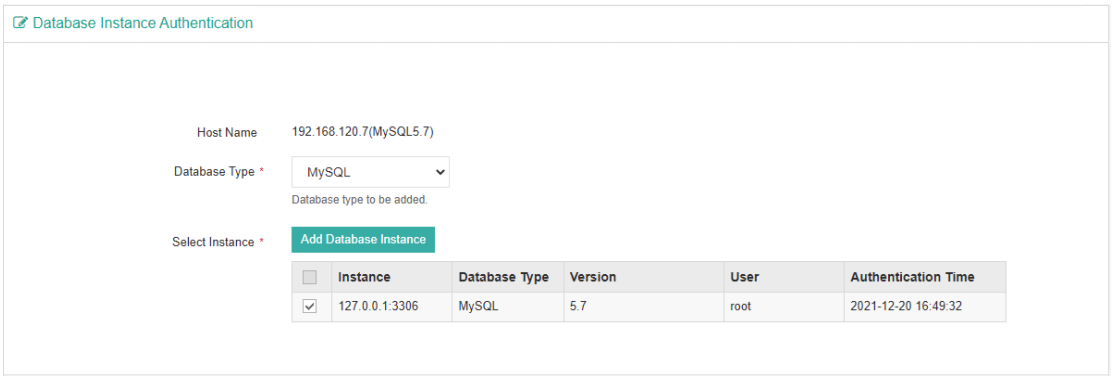
In Database Type dropdown list, select MySQL, and then click on Add Database Instance.



In the popup dialog, type in the full path of the MySQL cnf file, leave the **Port** number with default value and provide database administrator **Username**/**Password**.



Click on save, then you have successfully added database instance.



If the configurations of database have changed, select the database instance you wish to edit, click on **Authenticate** to edit.

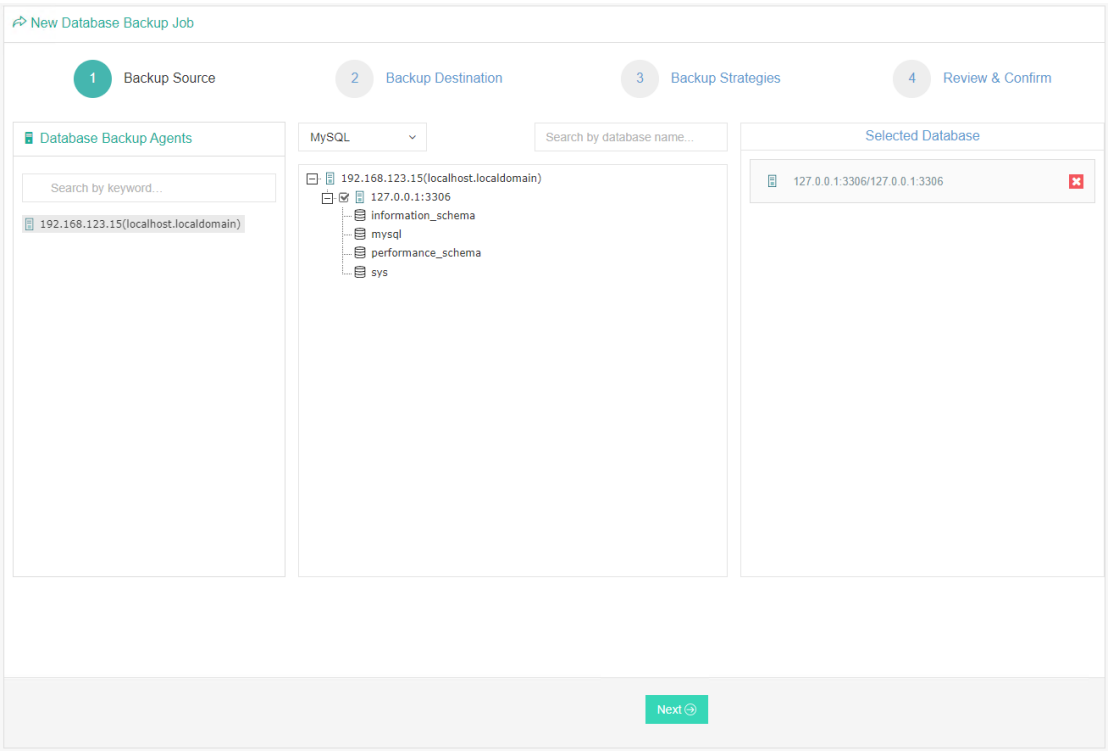
MySQL Database Backup

Create Database Backup Job

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

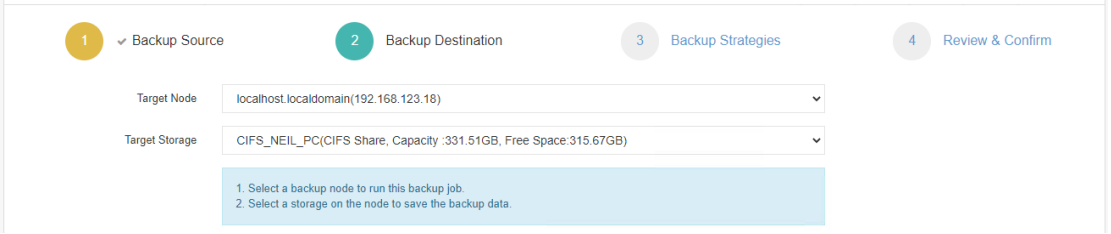
Step 1: Backup Source

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



Step 2: Backup Destination

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

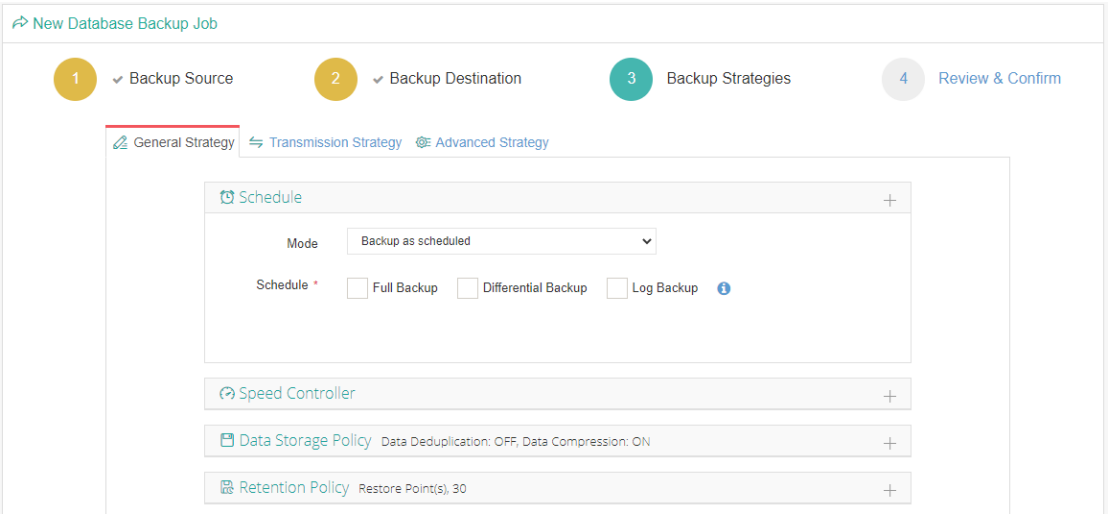


In the **Target Node** dropdown list, you can select a backup node on which you want the backup data to be processed and stored.

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

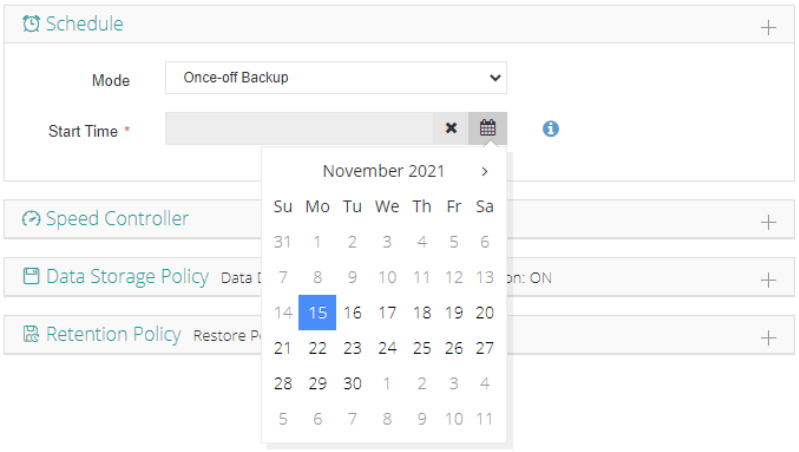
Step 3: Backup Strategies

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



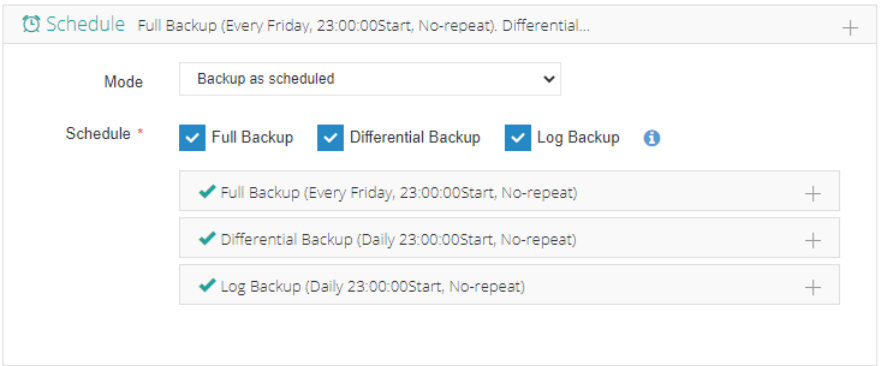
In the Schedule field, you can configure the time schedule of the backup job, you can configure the job as a **Backup as Scheduled** job or a **Once-off Backup** job.

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



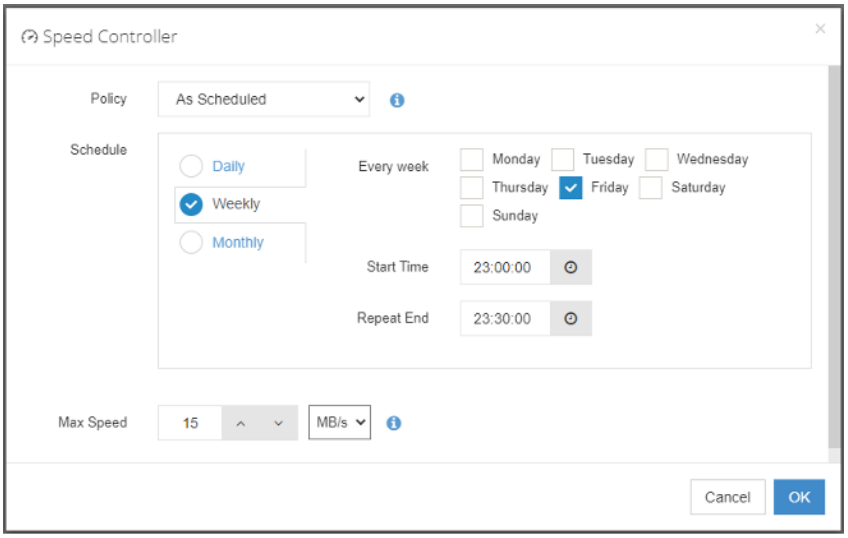
For backup job type, you can schedule Full Backup, Incremental Backup and Log Backup.

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

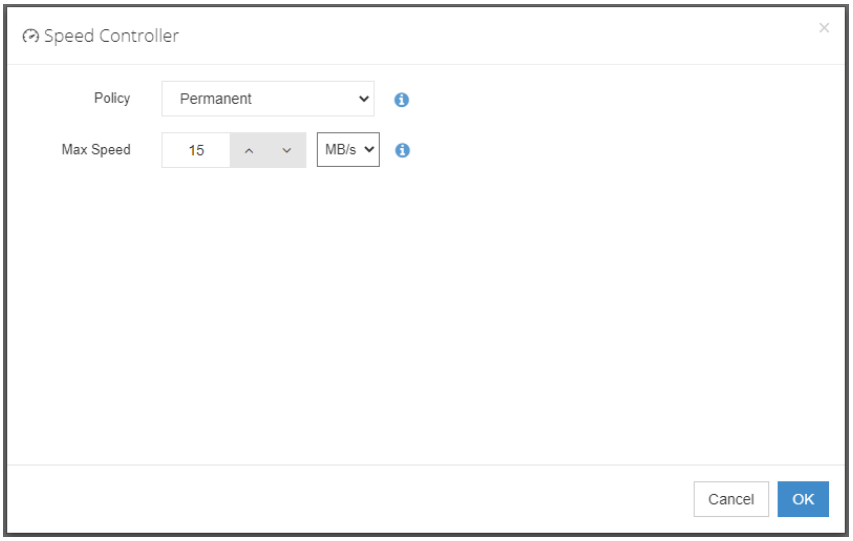


Speed Controller is optional. It can be used to limit the transmission speed during database backup if needed.

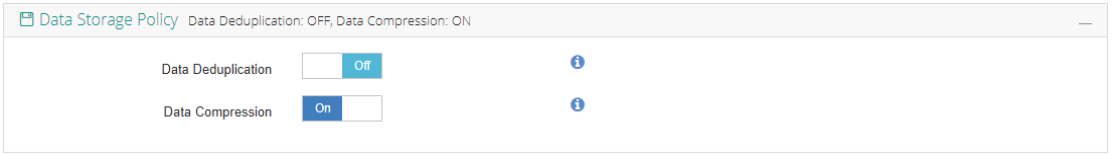
The speed controller policy can be configured as either As Scheduled or Permanent. An As Scheduled policy can be configured to limit the backup speed on Daily, Weekly and Monthly basis.



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



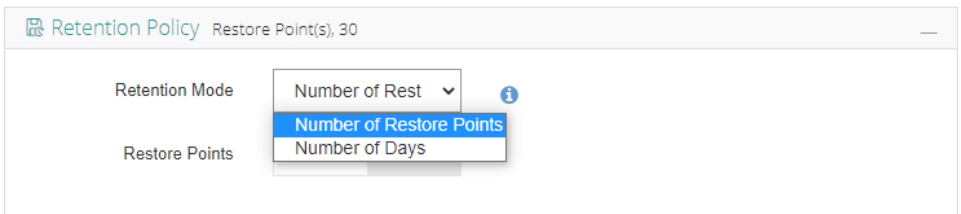
There are 2 options in Data Storage Policy section, Data Deduplication and Data Compression. By enabling these 2 options, the backup data will be deduplicated and compressed before saving into backup storage.



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

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

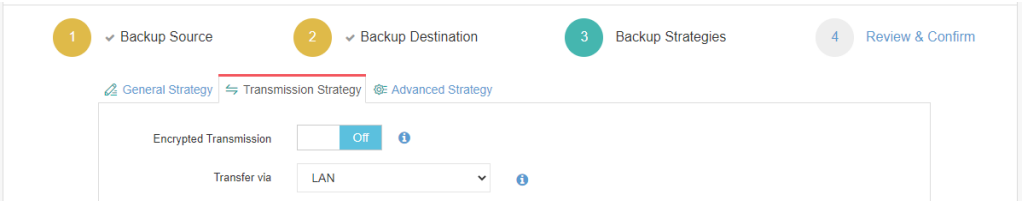
For retention mode **Number of Days**, Vinchin Backup Server will save the restore points within the specified number of days.



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

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

The backup data will be transferred through LAN by default.



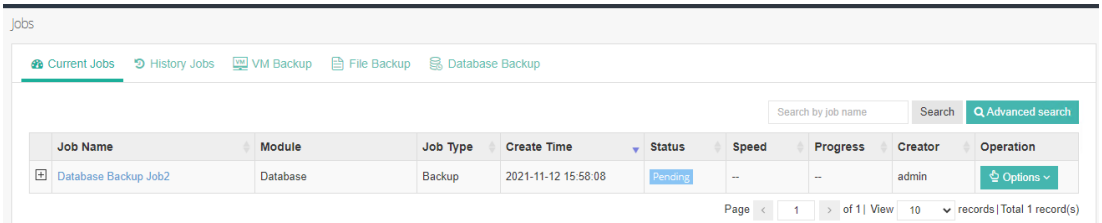
Step 4: Review & Confirm

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

A job name can be specified for identification of the database backup job, and by clicking on the Submit button to create the backup job.

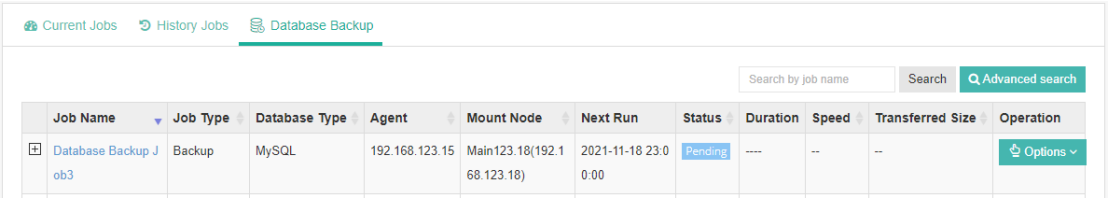
Database Backup Job Operations

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



The status of the newly created job will usually be **Pending**, when the time condition matches the schedule, it will automatically run. And the status will change to Running, you can also see the transfer speed here within the job list.

Besides the Current Job list, there's a dedicated tab to show database backup jobs. More detailed information of database backup jobs, including database type, database agent info, backup node, next run time and some more detailed information dedicated for database backup will be given.



By clicking on the job name you can check more detailed information on the **Job Detail** page.

For a scheduled backup job, after running one of the schedules, the status will change to Pending again and then wait for the next run.

For a once-off backup job, after running the job for once, it will be removed from the Current Job list. And you can find it from the History Job list.

Database Restore

There are two methods to recover MySQL database, **Override Original Database** and **Redirect Restore to New Path**.

For **Override Original Database** restore, MySQL database needs to be shutdown. For example:

```
systemctl stop mysqld
```

And an empty temporary directory needs to be created and should be granted with mysql user permission for storing cache data during restoration process. For example:

```
mkdir /data
chown -R mysql:mysql /data
```

All data in the original data directory (datadir) needs to be cleared before restoration, it's recommended to rename the original data directory and create a new directory with the original data directory name, and it needs to be granted with mysql user permission, for example:

```
cd /var/lib/
mv mysql mysql.bk
mkdir mysql
chown -R mysql:mysql mysql
```

Note

1. The above operations should be done by the MySQL database admin.

2. The temporary directory is recommended to be created on the same partition as original data directory.

2. For the datadir, it's configured in the my.cnf file, database admin should perform the above operations according to the actual environment.

For **Redirect Restore to New Path**, a temporary directory and a new data directory need to be created and need to be granted with mysql user permissions, for example:

```
mkdir /data
chown -R mysql:mysql /data
mkdir /data1
chown -R mysql:mysql /data1
```

Note

1. Redirect Restore to New Path does not require shutdown MySQL database services.

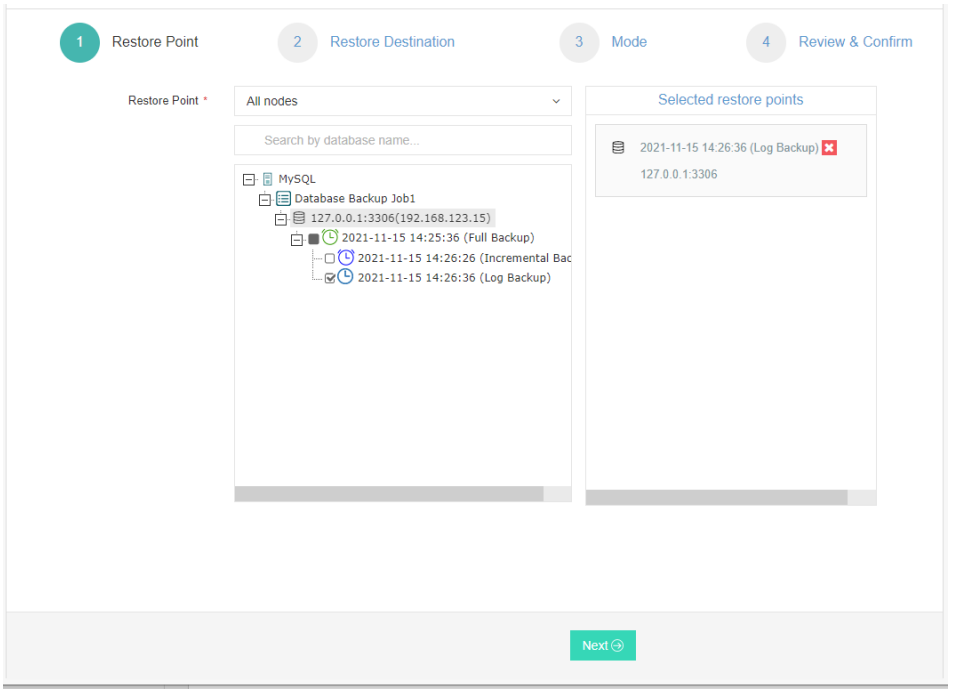
2. The restored data will be saved in the new data directory, database admin can use the restored data to create new database or modify the my.cnf file to start MySQL database from the new data directory.

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

Step 1: Restore Point

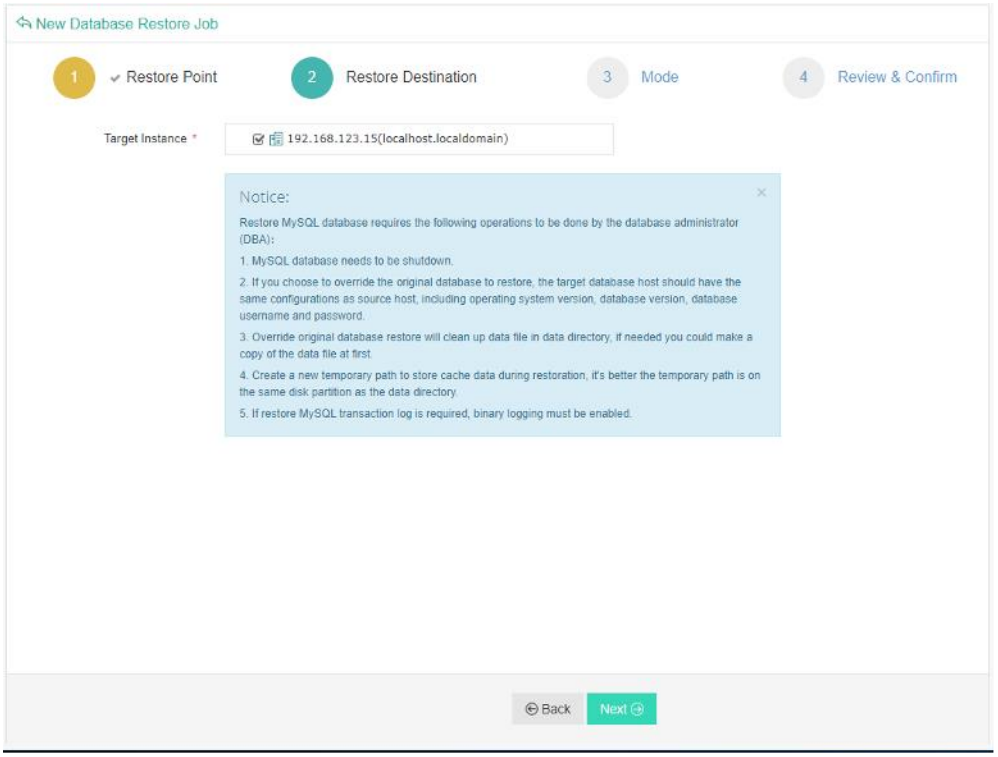
In the Restore Point dropdown list, select a backup node which stores the desired restore points.

Select a target database restore point under your database which you want to restore. You can quickly find the target restore point by searching the job name, database name or the date of the restore point. One restore job only can select one restore point.



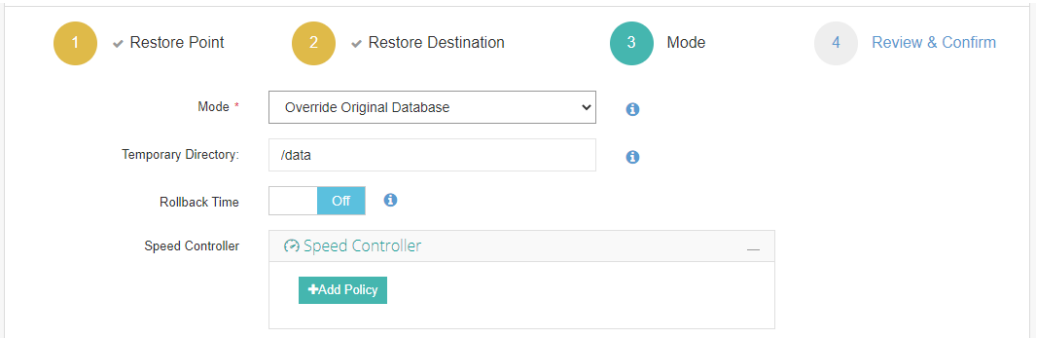
Step 2: Restore Destination

After selecting restore point, select **Target Instance** to restore.

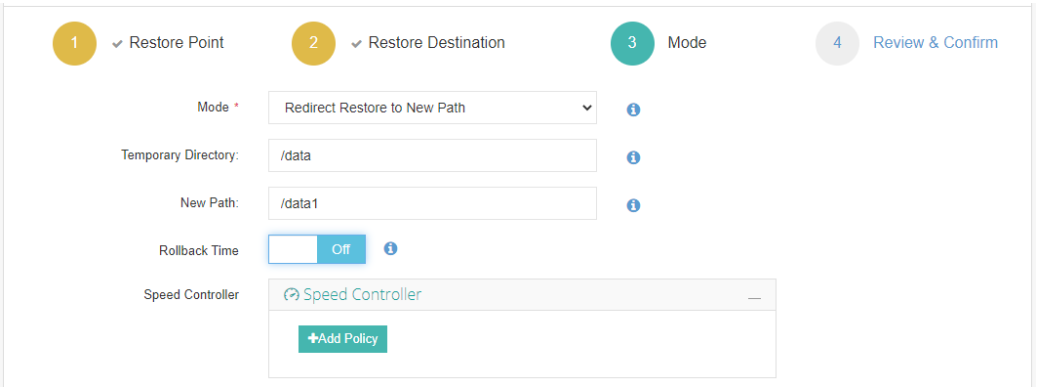


Step 3: Restore Strategy

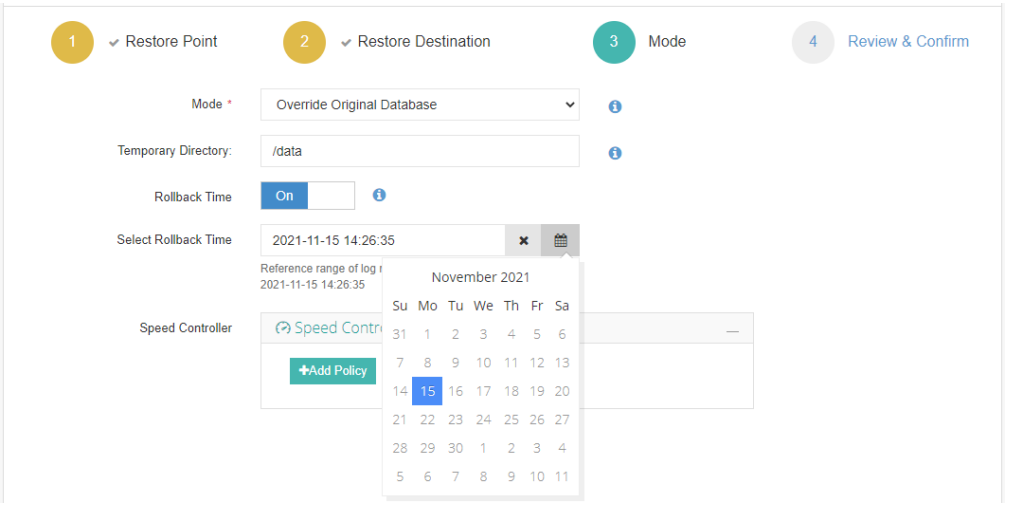
For **Override Original Database** restore, fill in the temporary directory path.



For **Redirect Restore the New Path** restore, fill in the temporary directory path and the new data directory path.



Rollback time: if you had selected log backup restore point, you are able to rollback MySQL database state within the given time range.

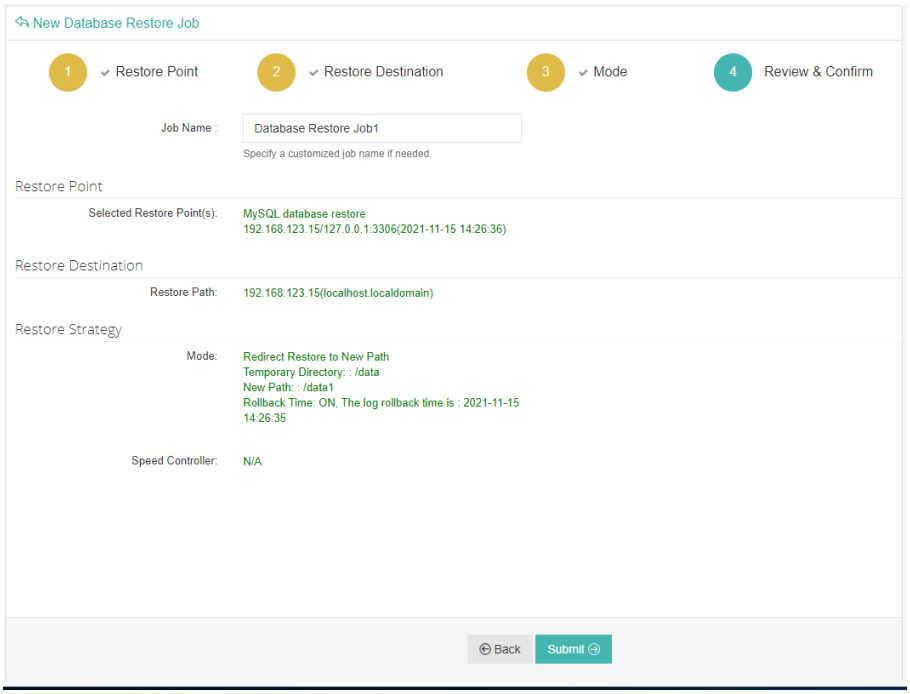


If you disable rollback time it will by default restore to the latest time point of the backup when it's been taken.

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

Step 4: Review&Confirm

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



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

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

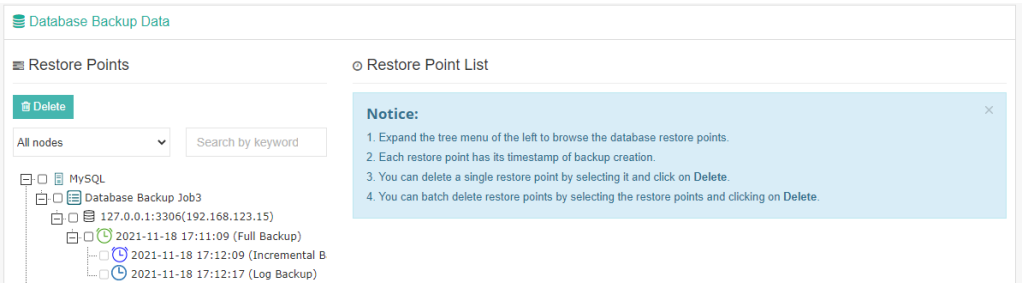
After this you can browse the restored job from History Jobs. Your restored data will be found in the path you configured during creating the restore job.

Note

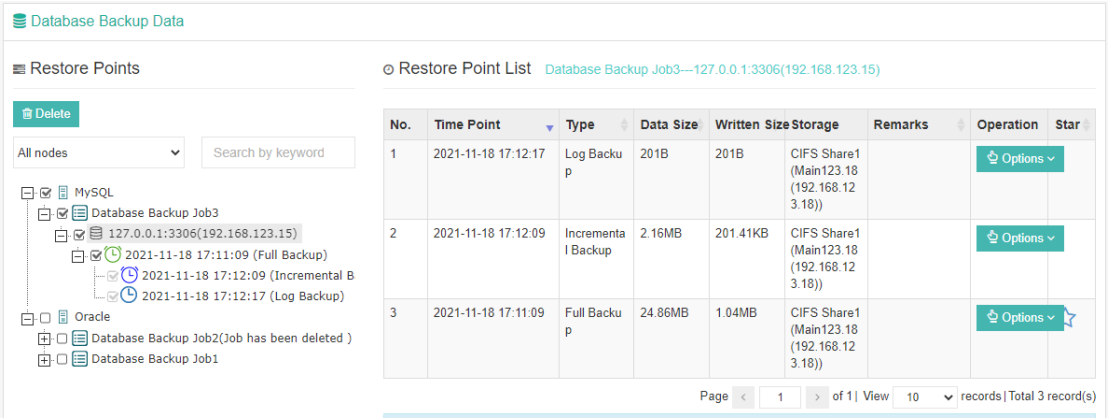
If you use log backup point to override original database, MySQL service will auto restart, no need to manually start MySQL service.

Database Backup Data

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



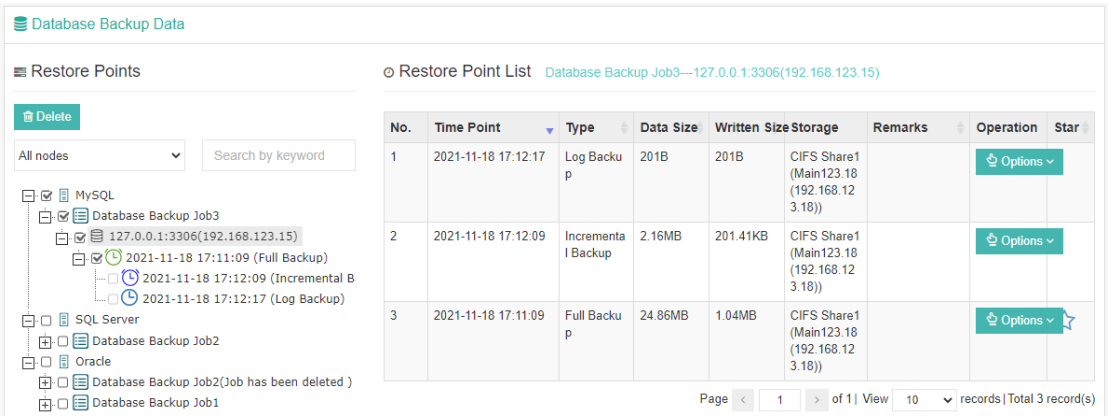
If you want to delete a restore point or multiple restore points, you can first select target restore point(s) from the left tree, and click on the **Delete** button. The incremental backup and log backup cannot be deleted individually, they will be deleted along with the dependent full backup.



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

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

You can add remarks to the restore points, and click ☆ with full restore point to keep the full backup and its dependent incremental and log backups to not be deleted by retention policy.



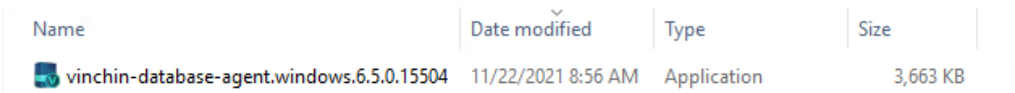
Oracle Database Backup and Restore

Install Database Backup Agent

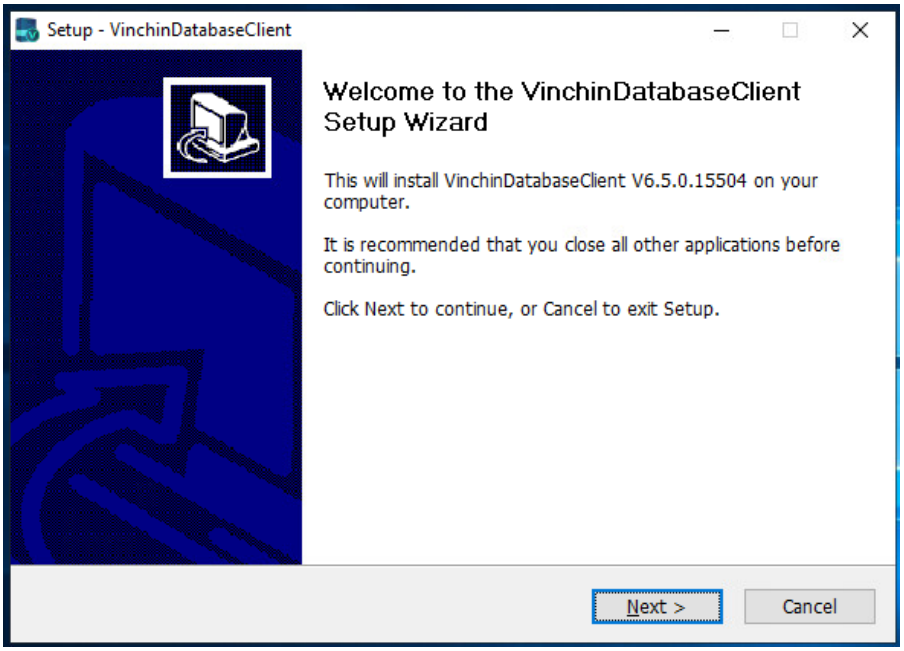
Windows

The Supported Windows system versions including Windows Server 2008/2012/2016/2019.
To download database backup plugin, please go to the login screen of Vinchin Backup Server web console, click on **Download Backup Plugin** to go to the backup plugin download page.

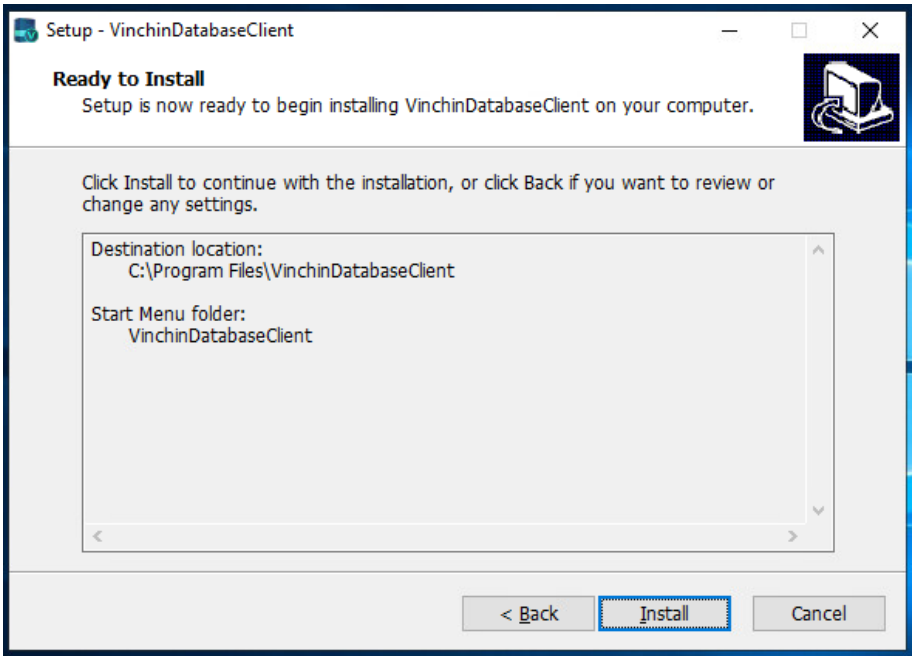
In **Type** dropdown list, select **Database Backup Agent**, in **OS** dropdown list, select **Windows**, and then click on **Download** button to download.
The downloaded database backup plugin should be an executable exe file.



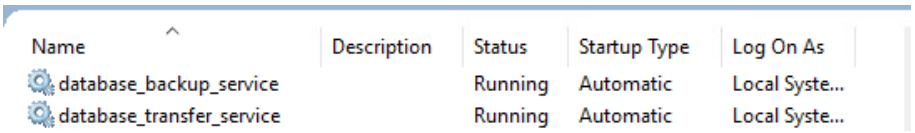
To install the backup plugin, please right click on it and select **Run as administrator** to install the backup plugin with administrator permissions.



Click on **Install** button to start the installation.

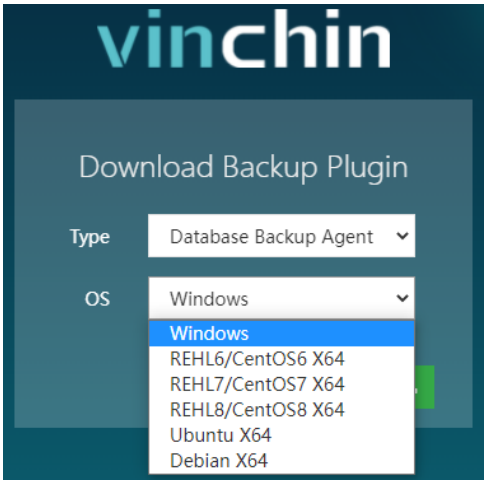


After the installation, check whether if 'database_backup_service' and 'database_transfer_service' are running, if yes, it means the agent is successfully installed.



Linux

The supported Linux distributions and versions including RHEL 6 to 8, CentOS 6 to 8 and Oracle Linux 6 to 8.
Please go to login screen and click on **Download backup plugin** to go to the database backup plugin download page.



Select the corresponding Linux distribution and version then click on the Download button to download the database 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-database-backup-agent-xxx.tar.gz
```

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

```
cd vinchin-database-backup-agent-xxx
```

To install the backup plugin, run below command.

```
./db_backup_agent_install
```

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

```
./db_backup_agent_uninstall
```

Use below command to check Vinchin database backup services status

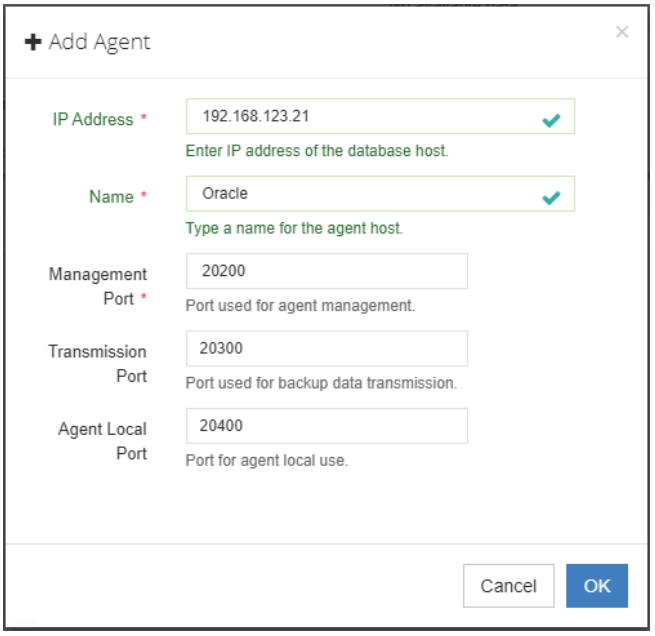
```
ps -aux | grep database | grep -v 'grep'
```

Three process services should be running as shown below.

```
[oracle@local home]$ ps -aux | grep database | grep -v 'grep'
Warning: bad syntax, perhaps a bogus '-'? See /usr/share/doc/procps-3.2.8/FAQ
root      8500  0.0  0.0 106240  1340 pts/1    S    Nov16   0:05 /bin/bash /opt/vinchin/database/db_backup_watch_dog.sh
root      8507  0.0  0.1 266216  6700 ?        Ssl  Nov16   0:01 /opt/vinchin/database/database_backup_service -b
root      8514  0.0  0.1 145096  5064 ?        Ssl  Nov16   0:00 /opt/vinchin/database/database_transfer_service -b
[oracle@local home]$
```

Register Database Backup Agent

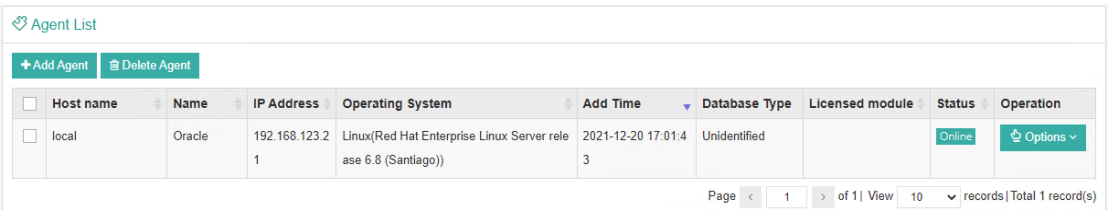
After the database backup agent installation, please open Vinchin Backup Server web console and go to **Database Backup** > **Backup Agent** page. Click on **Add Agent** button to start adding database backup agent.



In the IP Address field, enter the IP address of the database server which you wish to backup, database agent must be installed on the server.

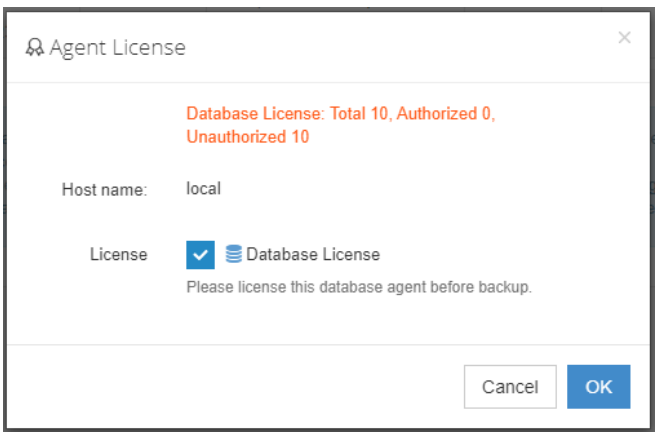
In the Name field, you can optionally enter a name for identification. For the Management Port, Transmission Port and Agent Local port, please use default settings and do not change them.

When done, click on **OK**, then in the **Agent List** it will show the database backup agent you just added.

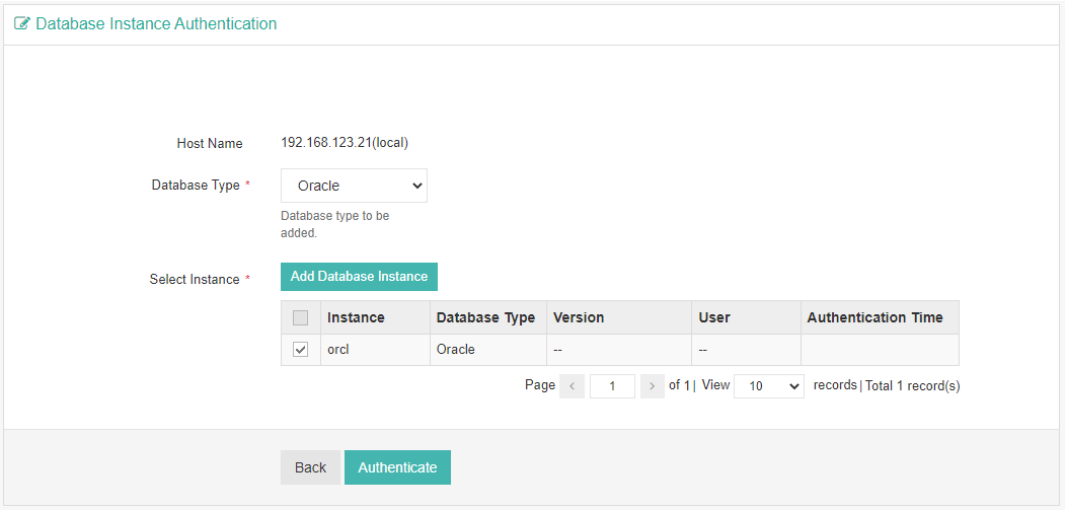


Once a database agent had been added, you need to license the database agent and authenticate the database instance before performing database backups.

Click on **Options** > **License** in the popup dialog, click on License checkbox to license the database backup agent.

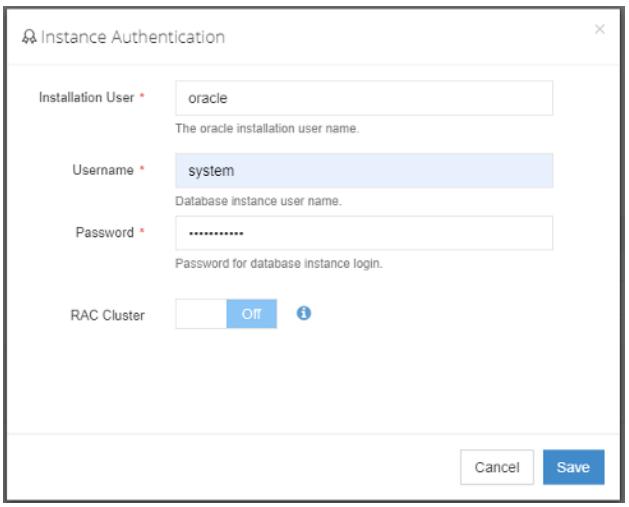


Click on **Options** > **Authentication** to authenticate the database instance for backup. In database type dropdown list, select Oracle. It will automatically show database Instance of the database server. Select the Instance you wish to backup and click on **Authenticate** button.



In the popup dialog, specify the **Installation User** of Oracle database, if the database server is Windows server, then use the default installation user, only fill in the database username and password.

If the database server is Linux, you need to change the **Installation User** only when the Linux user is not oracle.



The user to be used to backup Oracle database must have dba and sysdba permissions. You can login to oracle database use below commands to check user permissions.

Check if GRANTED_ROLE = DBA by using command:

```
select * from dba_role_privs where grantee='username';
```

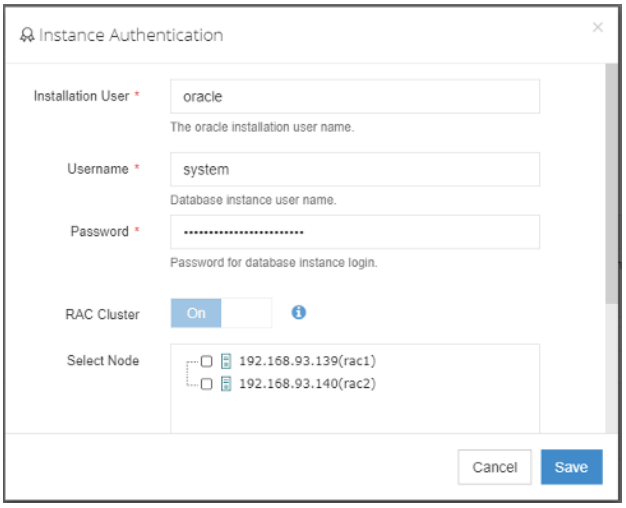
Check if SYSDBA = TRUE by using command:

```
select * from v$pwfile_users where username='username';
```

It's recommended to grant sysdba permission to the system user, then use system user to backup Oracle database.

For **RAC Cluster**, database backup agent needs to be installed on each of the cluster nodes, then add all nodes (backup agents) to Vinchin backup server.

To enable RAC Cluster, only need to do it on one of the nodes with Instance Authentication. By turning the RAC Cluster option on, and in the Select Node field, select all the other nodes of the RAC cluster.



Then click on save, and then the database instance will be successfully authenticated.

Note

1. If database server is Linux, the database backup agent needs to use 3 service ports: 20200, 20300 and 20400. On the database server firewall, these 3 ports need to be opened for Vinchin backup server.

2. To add RAC Cluster, database backup agent needs to be installed on all the cluster nodes, and all nodes (agents) need to be added to Vinchin.

3. Choose one Oracle database agent to do Instance Authentication for the RAC cluster.

4. To back up the Oracle RAC cluster environment, run the show all command on the RMAN command line to check whether the control file snapshot is set to the shared storage.

5. Only one backup job needs to be created for one of the RAC cluster node.

6. If one or some of the RAC cluster node fail, backup will be performed on other node, there's no need to modify the backup job under such situation.

7. Archivelog mode needs to be enabled with the database instance before taking backups.

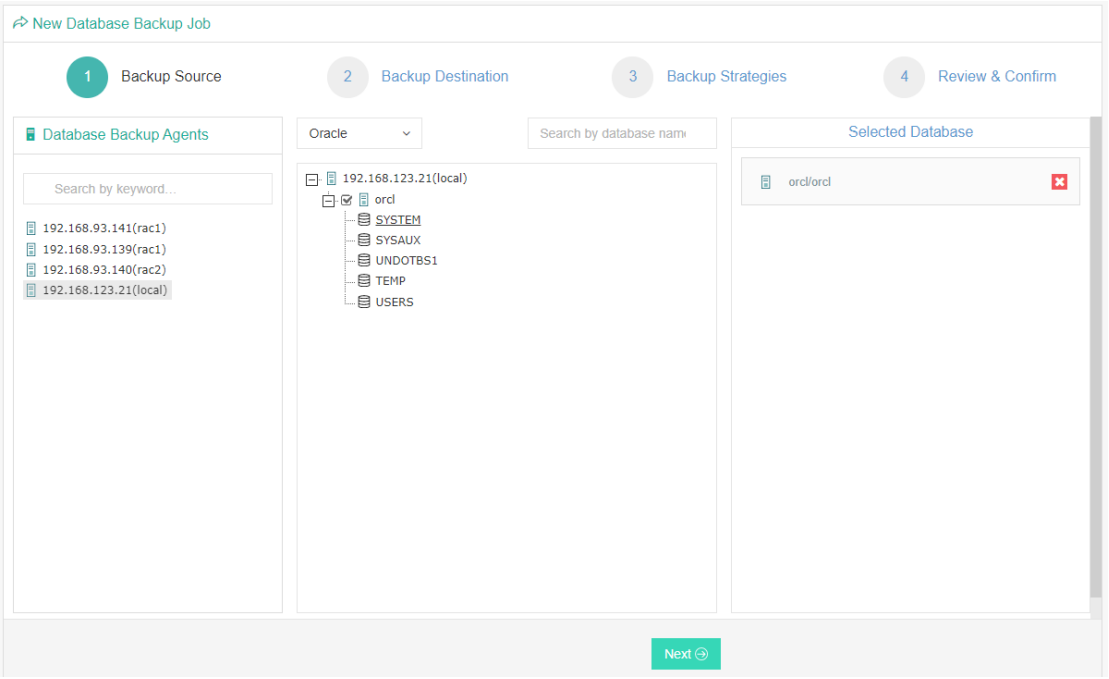
Oracle Database Backup

Create Database Backup Job

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

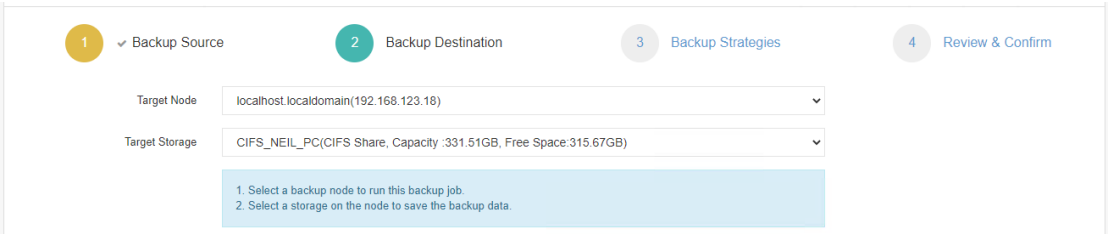
Step 1: Backup Source

First you need to select a target host from the left column, then select Oracle database instance you wish to backup, in the right column will show the instance you select. Click on next to step 2.



Step 2: Backup Destination

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

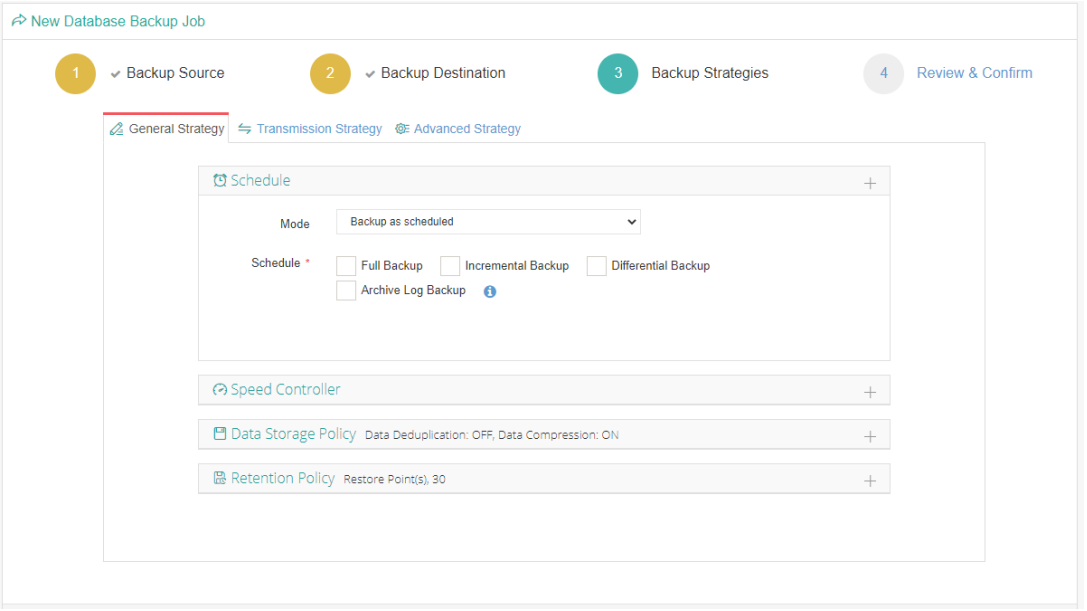


In the **Target Node** dropdown list, you can select a backup node on which you want the backup data to be processed and stored.

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

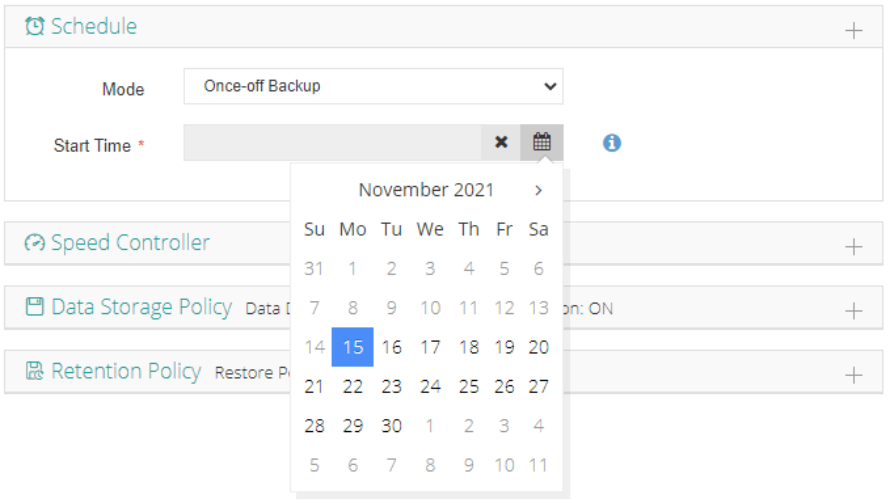
Step 3: Backup Strategies

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



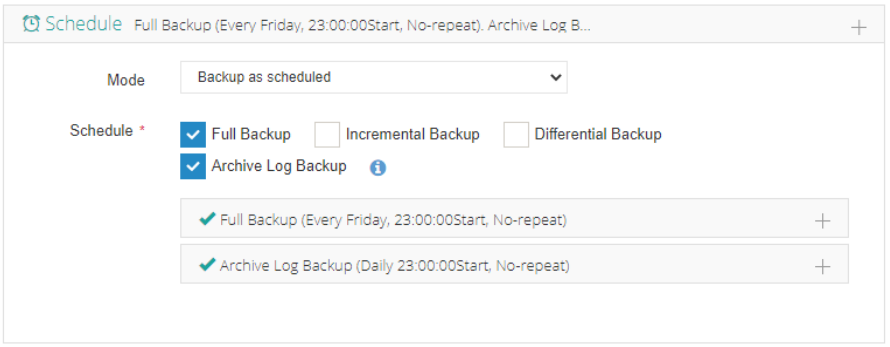
In the Schedule field, you can configure the time schedule of the backup job, you can configure the job as a **Backup as Scheduled** job or a **Once-off Backup** job.

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

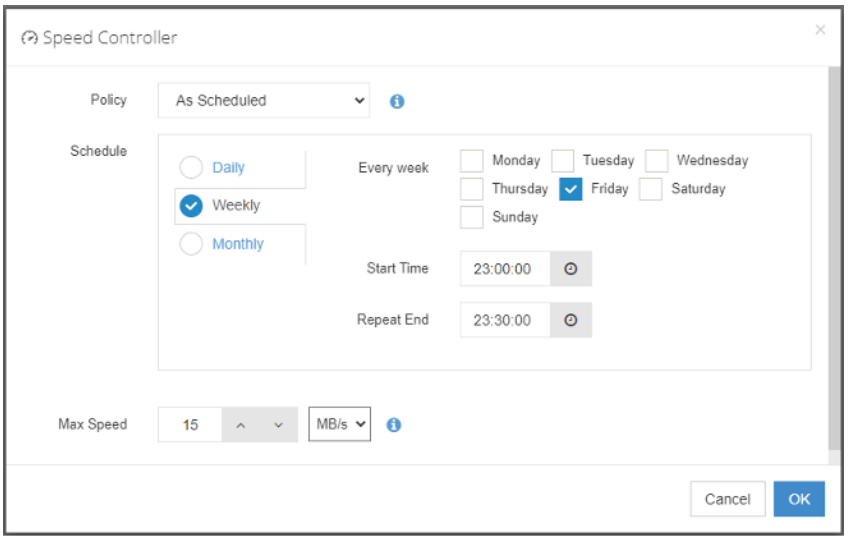


For backup job type, you can schedule Full Backup, Incremental Backup, Differential Backup and Archive Log Backup.

For Oracle database must have **Full Backup** and **Archive Log Backup**. Please set the backup mode and backup schedule as per your actual demands, then please click on **Next** to continue.

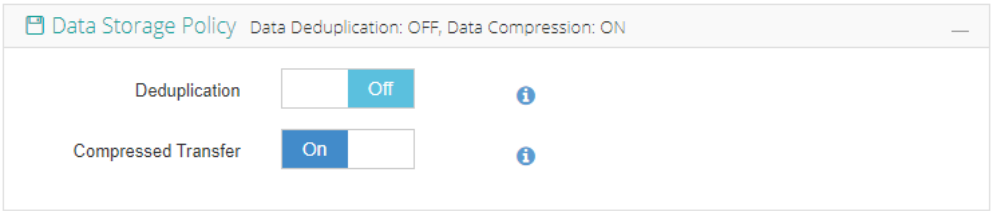


Speed Controller is optional. It can be used to limit the transmission speed during database backup if needed.
The speed controller policy can be configured as either As Scheduled or Permanent. An As Scheduled policy can be configured to limit the backup speed on Daily, Weekly and Monthly basis.

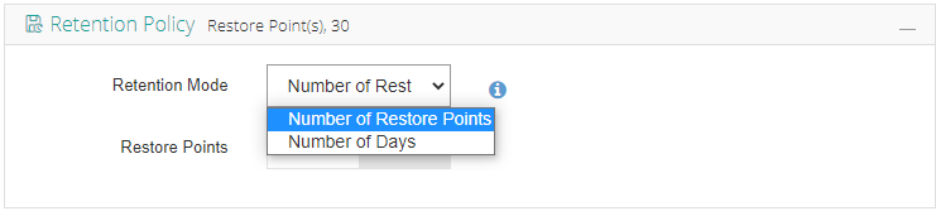


A Parmanent policy will always limit the backup speed within the specified Max Speed.

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



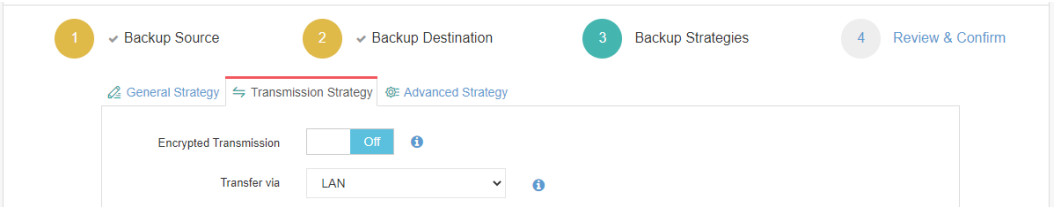
For the retention policy of the database backup, there are 2 retention mode, retain the database backups according to **Number of Restore Points** or **Number of Days**.
For the retention mode **Number of Restore Points**, the restore points will be counted by full restore points, including the differential backups and log backups dependent on this full backup.
For retention mode **Number of Days**, Vinchin Backup Server will save the restore points within the specified number of days.



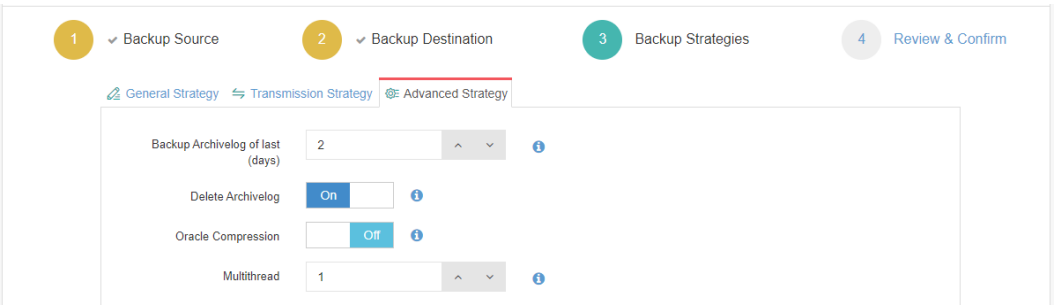
When the retention policy is triggered, the outdated restore points will be purged to comply with the retention policy.

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

The backup data will be transferred through LAN by default.



Advanced Strategy allows you to configure Backup Archivelog of last (days), Delete Archivelog, Oracle Compression and Multithreaded transmission.



Backup archivelog of last(days): The default value of the recent archivinglog days is associated with the frequency of archiving log backup set in the schedule policy. e.g. if Archive Log Backup set to Daily, default is 2 days. If Archive Log backup set to every week, default is 8 days. If Archive Log Backup set to Monthly, default is 31.

Delete Archivelog: enabled delete archivelog can delete backed up archivelog file from database server, reclaim archive space from the database server. If disabled this option, database admin needs manually delete archivelog files.

Oracle Compression: provide by Oracle to reduce data transfer, data backup time and save backup storage, disabled by default.

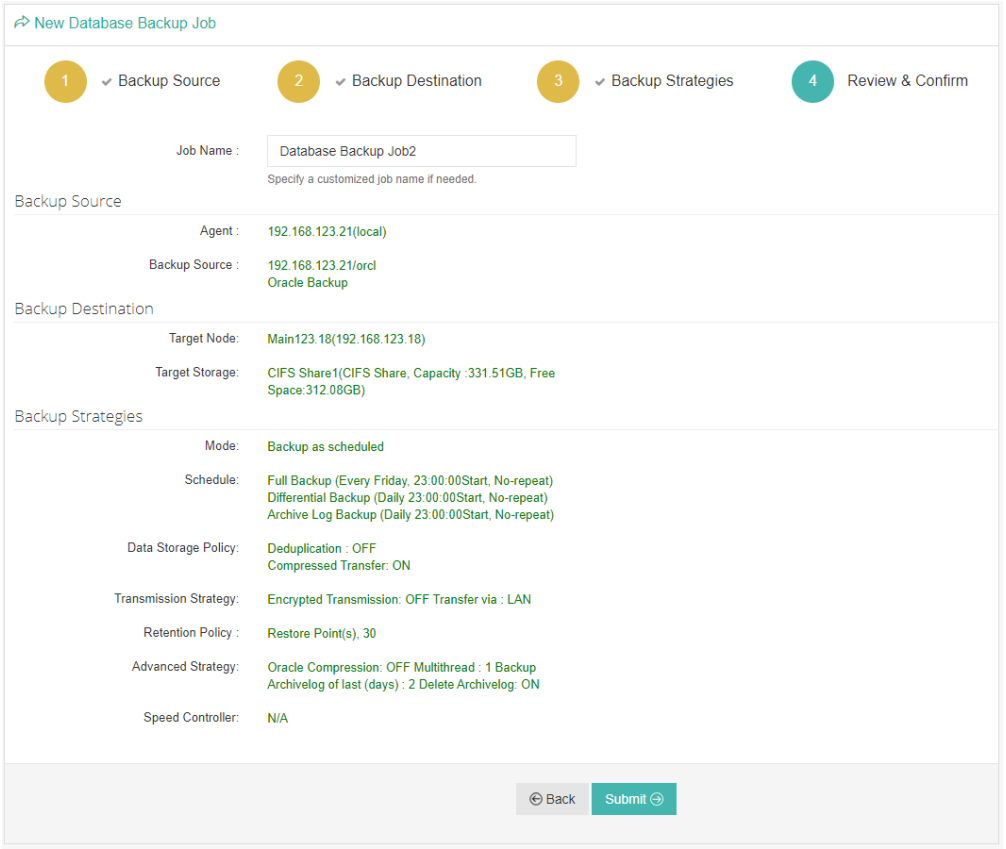
Multithread: backup data will be transferred over multiple channels to improve the backup speed. The default value is 1, and the maximum value is 6.

Note

If Delete Archivelog is disabled, DBA must manually delete archivelog files regularly, otherwise, production database crash may occur once space is fulfilling with archive log files. It is recommended to enable this function.

Step 4: Review & Confirm

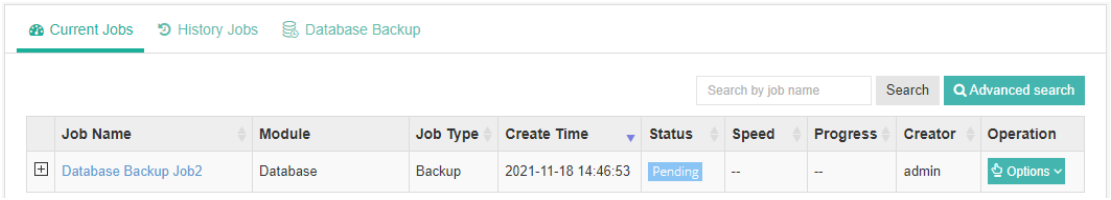
After completing the above mentioned settings, you are able to review and confirm the settings in one screen.



A job name can be specified for identification of the database backup jobs, and by clicking on the Submit button to confirm the creation of the backup job.

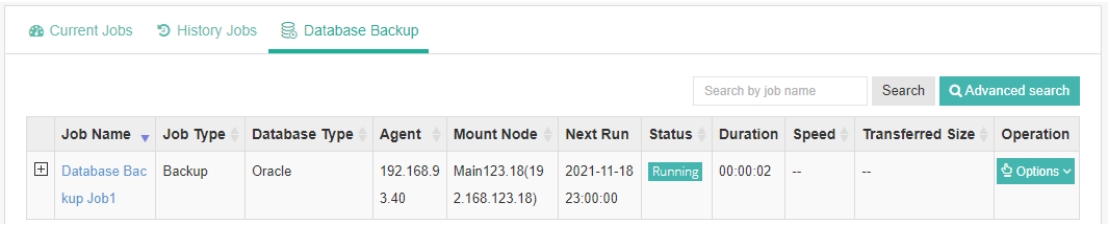
Database Backup Job Operations

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



The status of the newly created job will usually be **Pending**, when the time condition matches the schedule, it will automatically run. And the status will change to Running, you can also see the transfer speed here within the job list.

Besides the Current Job list, there's a dedicated tab to show database backup jobs. More detailed information of database backup jobs, including database type, database agent info, backup node, next run time and some more detailed information dedicated for database backup will be given.



By clicking on the job name you can check more detailed information on the **Job Detail** page.

For a scheduled backup job, after running one of the schedules, the status will change to Pending again and then wait for the next run.

For a once-off backup job, after running the job for once, it will be removed from the Current Job list. And you can find it from the History Job list.

Database Restore

Before starting to restore Oracle database, there are some configurations need DBA to check.

Target recovery database server needs database backup agent installed, and if it's Linux system, the service ports: 20200, 20300 and 20400 needs to be open to Vinchin backup server.

Target Oracle database instance needs to be shutdown, and static listener registration needs to be configured in listener.ora file.

Archivelog mode needs to be enabled with the target Oracle database server. You can check status by login to sqlplus and using below command.

```
archivelog list;
```

Check if **Automatic archival** status is **Enabled**, if not please configure this by DBA.

Check whether the database instance can be connected by using below command. In standalone environment.

```
rman target=username/password@instancename
```

In RAC cluster, use below command.

```
rman target=username/password@publicIP:1521/instancename
```

If connection fails, the restore job will failure, please contact DBA to fix it.

If **Override Original Database** restore to another database server, it requires the target database server configurations should be the same as the source database server, including operating system, database version, installation path and instance name. Please be careful to use override original database function.

If **Restore to New Path**, the database path will be automatically changed to the new path specified during the restore process. After restoration, DBA can just start the database services directly from the new path.

Warning:

Restore to New Path does not work with Oracle RAC, because the database path will only change on the RAC node which the restore job is associated to, other nodes will not be changed. If you use Restore to New Path with Oracle RAC, it will cause Oracle RAC exception!

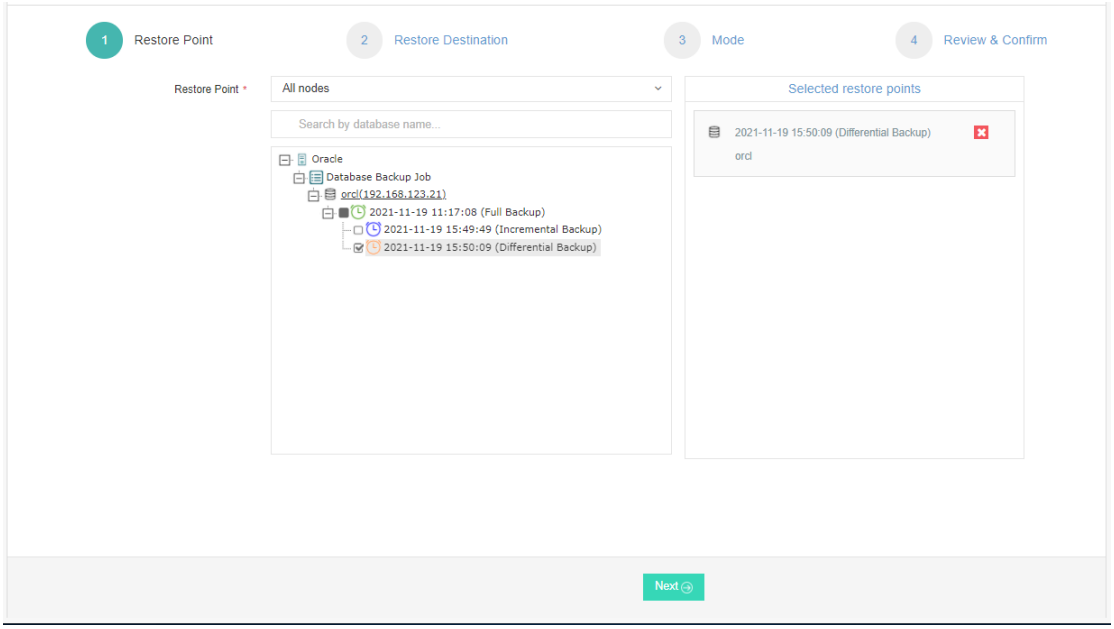
To restore databases from database backup restore points, please go to **Database Backup** > **Restore** page. There are 4 steps to restore databases from the database backup restore points.

Step 1: Restore Point

In the Restore Point dropdown list, select a backup node which stores the desired restore points.

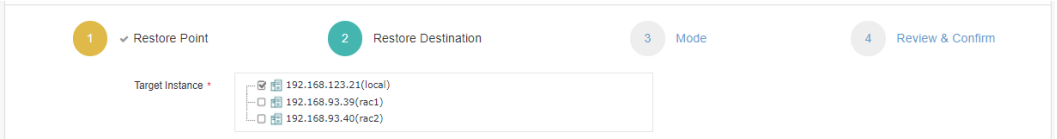
Select a target database restore point under your database which you want to restore. You can quickly find the

target restore point by searching the job name, database name or the date of the restore point. One restore job only can select one restore point.



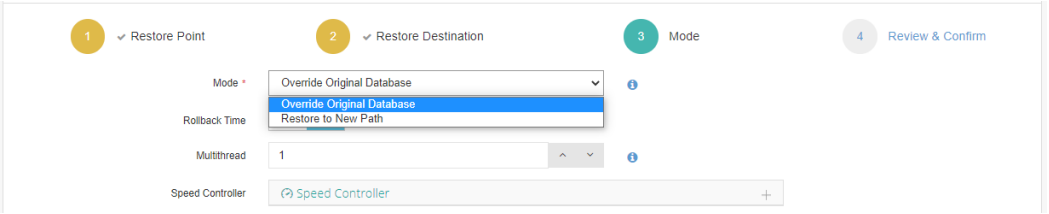
Step 2: Restore Destination

After selecting restore point, select **Target Instance** which you wish to restore.

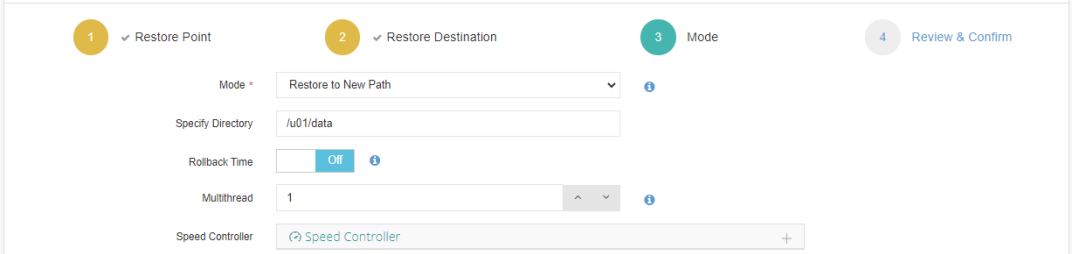


Step 3: Restore Strategy

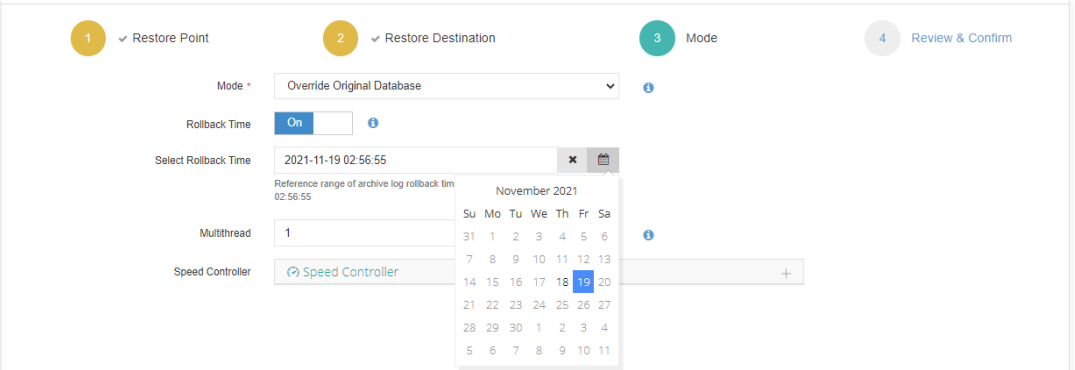
Mode: Override Original Database applies to restore the data to the production database server. Override the data of the original database instance.



Restore to New Path applies to restore data to a new directory. The directory needs to be created by the Oracle database installation user, do not use a directory which does not exist.



Rollback Time: if you had selected archive log backup restore point, you are able to rollback Oracle database state within the given time range.



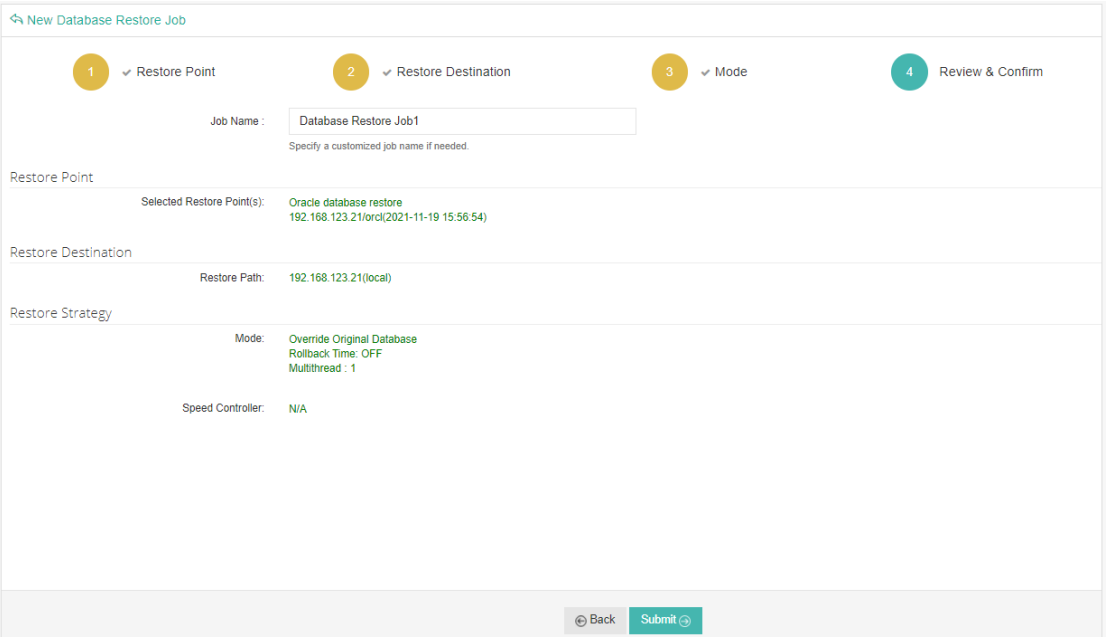
If you disable rollback time it will by default restore to the latest time point of when the backup has been taken.

Multithread: backup data will be transferred over multiple channels to improve the restore speed. The default value is 1, and the maximum value is 6.

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

Step 4: Review & Confirm

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



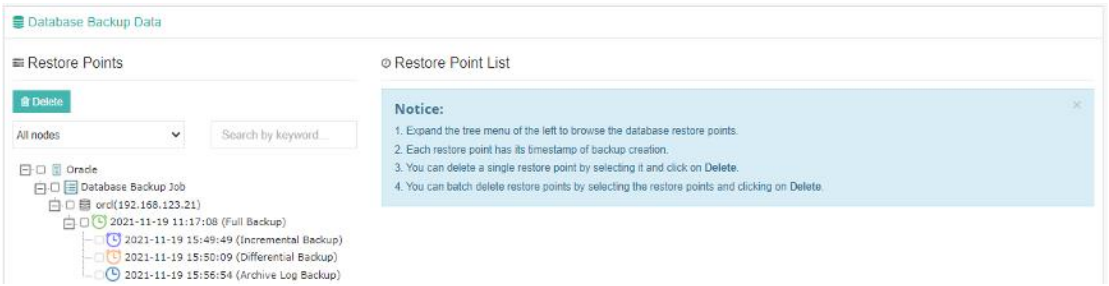
Once the job has been created, you'll be redirected to the **Monitor Center** > **Jobs** page.

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

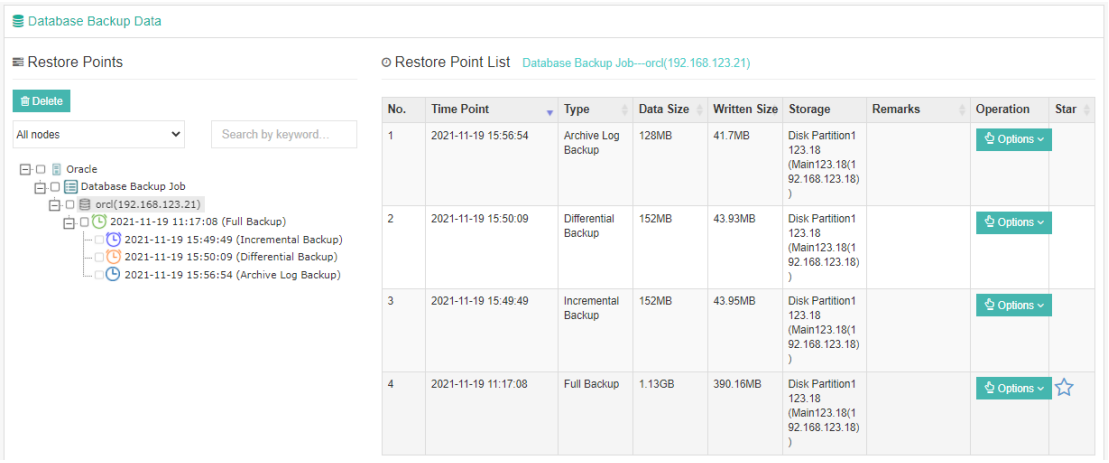
After this you can browse the restored job from History Jobs. Your restored data will be found in the path you select.

Database Backup Data

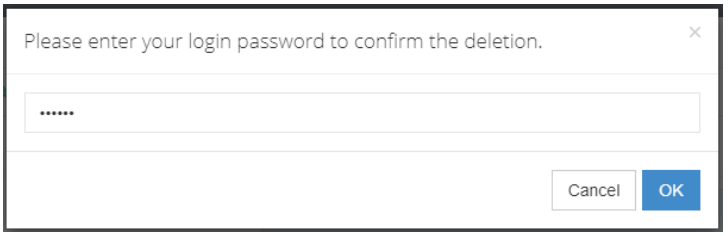
The database backup data can be managed from **Database Backup** > **Backup Data** page.



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

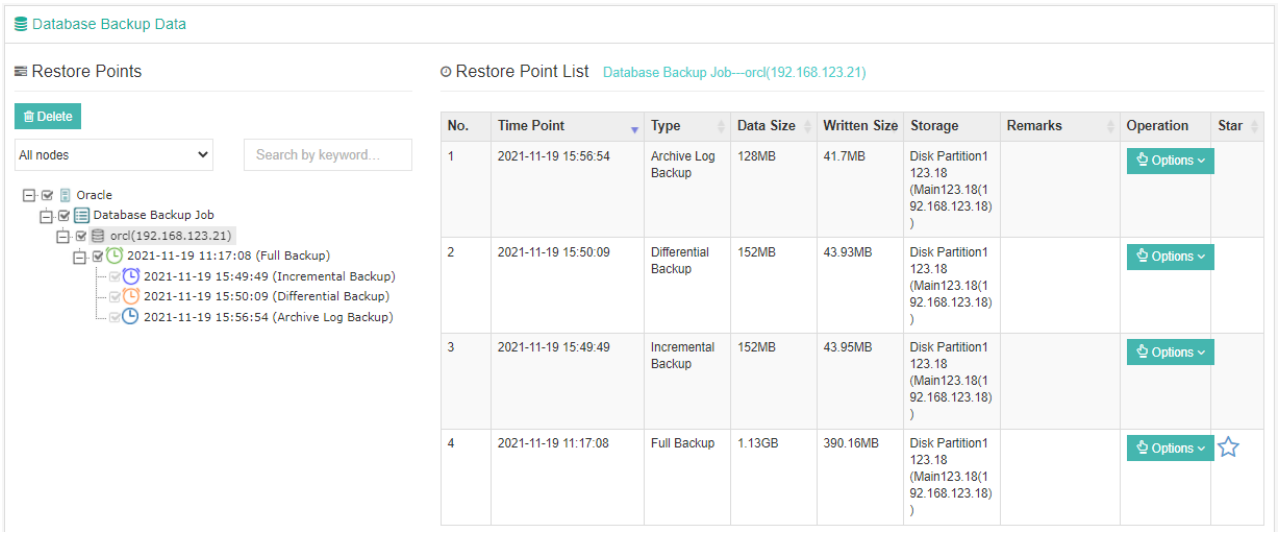


When deleting backup data, you need to provide your login password to confirm the deletion, once deleted the data will be unrecoverable.



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

You can add remarks to the restore points, and click ☆ with full restore point to keep the full backup and its dependent incremental and log backups to not be deleted by retention policy.


Database Backup Data
Restore Points
Delete
All nodes
Search by keyword...
Oracle
Database Backup Job
orcl(192.168.123.21)
2021-11-19 11:17:08 (Full Backup)
2021-11-19 15:49:49 (Incremental Backup)
2021-11-19 15:50:09 (Differential Backup)
2021-11-19 15:56:54 (Archive Log Backup)
Restore Point List
Database Backup Job---orcl(192.168.123.21)
No.
Time Point
Type
Data Size
Written Size
Storage
Remarks
Operation
Star
1
2021-11-19 15:56:54
Archive Log Backup
128MB
41.7MB
Disk Partition1 123.18 (Main123.18(192.168.123.18))
Options
2
2021-11-19 15:50:09
Differential Backup
152MB
43.93MB
Disk Partition1 123.18 (Main123.18(192.168.123.18))
Options
3
2021-11-19 15:49:49
Incremental Backup
152MB
43.95MB
Disk Partition1 123.18 (Main123.18(192.168.123.18))
Options
4
2021-11-19 11:17:08
Full Backup
1.13GB
390.16MB
Disk Partition1 123.18 (Main123.18(192.168.123.18))
Options

PostgreSQL Database Backup and Restore

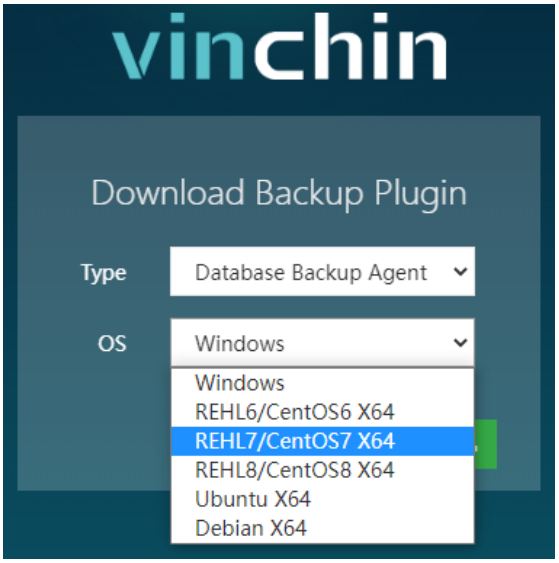
For PostgreSQL database backup, supported database versions are as follows:

- PostgreSQL 12
- PostgreSQL 13
- PostgreSQL 14

The supported PostgreSQL database server operating system including RHEL/CentOS 7 and 8 x64. PostgreSQL running on Windows server is currently not supported.

Install Database Backup Agent

Please download PostgreSQL database backup agent from Vinchin Backup & Recovery login screen. Select the corresponding Linux distribution and version then click on the Download button to download the database backup plugin.



After downloading, you should get a .tar.gz package. Please upload the downloaded file to the database server for installation, 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-database-backup-agent-xxx.tar.gz
```

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

```
cd vinchin-database-backup-agent-xxx
```

To install the backup plugin, run below command.

```
./db_backup_agent_install
```

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

```
./db_backup_agent_uninstall
```

After installing the database backup plugin, please check its services use below command.

```
ps -aux | grep database | grep -v 'grep'
```

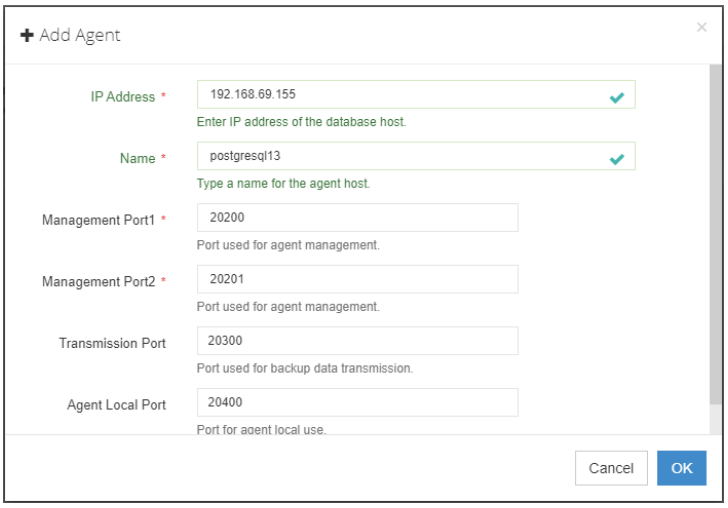
If you got the below output which has 4 services, bd_backup_watch_dog.sh, database_backup_service, database_backup_service_dm_pg and database_transfer_service, this means database backup agent installed successfully, the services are up running and ready for backup and restore.

```
[root@postgre ~]# ps -aux | grep database | grep -v 'grep'
root      2731  0.0  0.0 113280  1464 ttyl     S    05:39   0:00 /bin/bash /opt/vinchin/database/db_backup_watch_dog.sh
root      2738  0.0  0.2 304648  8108 ?        Ssl  05:39   0:00 /opt/vinchin/database/database_backup_service -b
root      2745  0.0  0.1 103992  5612 ?        Ssl  05:39   0:00 /opt/vinchin/database/database_backup_service_dm_pg -b
root      2753  0.0  0.1 106744  5532 ?        Ssl  05:39   0:00 /opt/vinchin/database/database_transfer_service -b
```

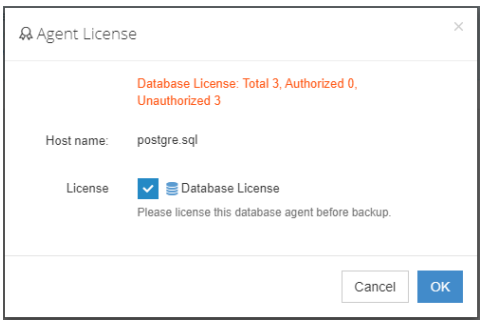
Register Database Backup Agent

After the installation of database backup agent, please open Vinchin Backup Server web console and go to **Database Backup** > **Backup Agent** page.

Click on **Add Agent**, enter the IP address of the PostgreSQL database server, and give it a name, leave the port numbers with the default values.

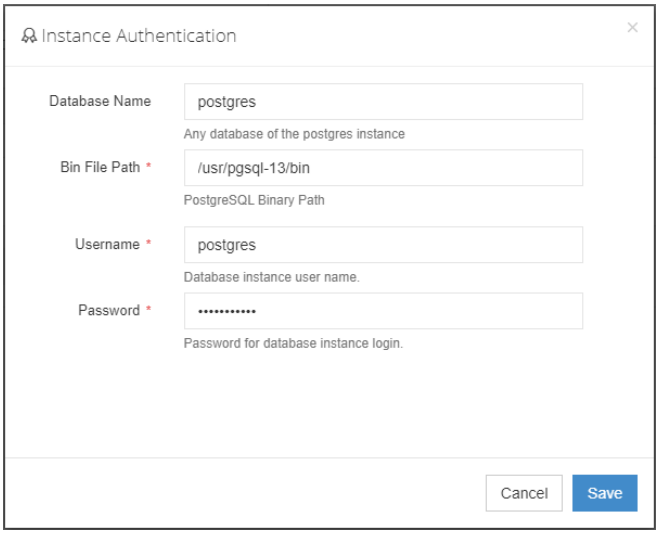


After adding the backup agent, please click on **Options** button and select **License** to license it with Vinchin Backup & Recovery database backup license.

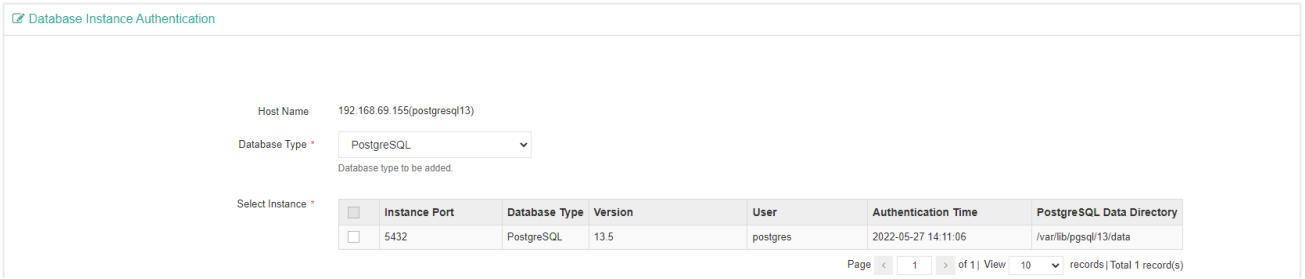


After that, click on **Options** again and select **Authentication**. In the Database **Type dropdown** list, please select **PostgreSQL**.

The database instances of PostgreSQL will be listed in the **Select Instance** field. Select the database instance and click on **Authenticate** button to get the instance authenticated for backup.



You need to specify the database bin file path and the database user credentials to get it authenticated. After this you are ready to take backups of the PostgreSQL database.



Note

DBA must check the below prerequisites before taking PostgreSQL database backups.

1. The database backup agent needs to use 4 service ports: 20200, 20201, 20300 and 20400. On the database server firewall, these 4 ports need to be opened for Vinchin backup server.

2. Archivelog mode needs to be enabled with the database instance before taking backups.

3. The password-based authentication should be “md5” or “scram-sha-256”.

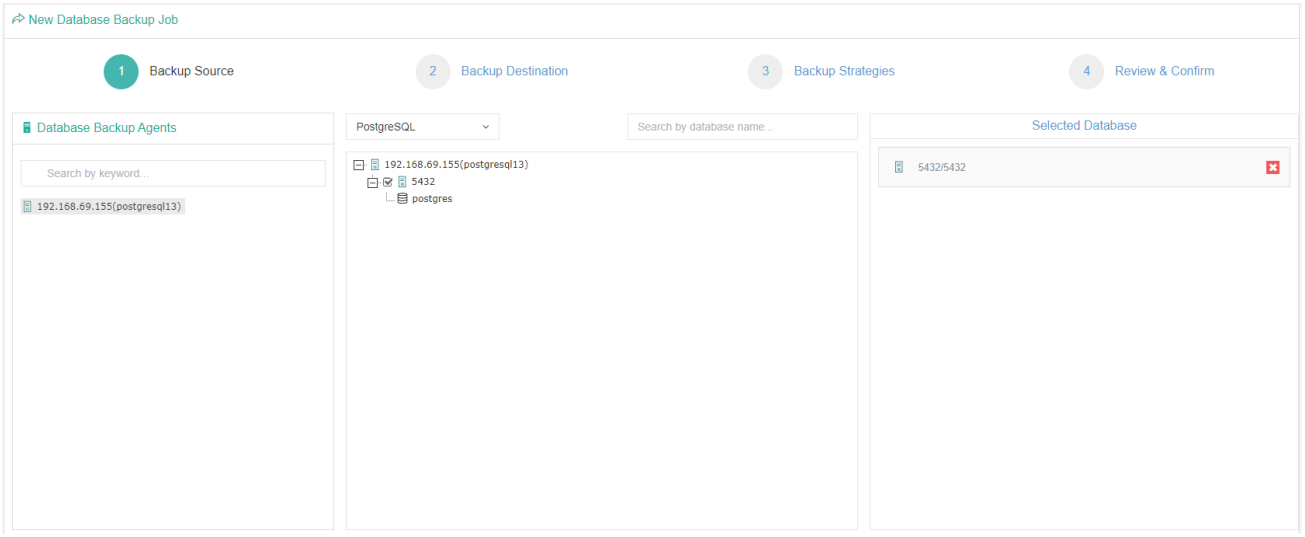
PostgreSQL Database Backup

Create Database Backup Job

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

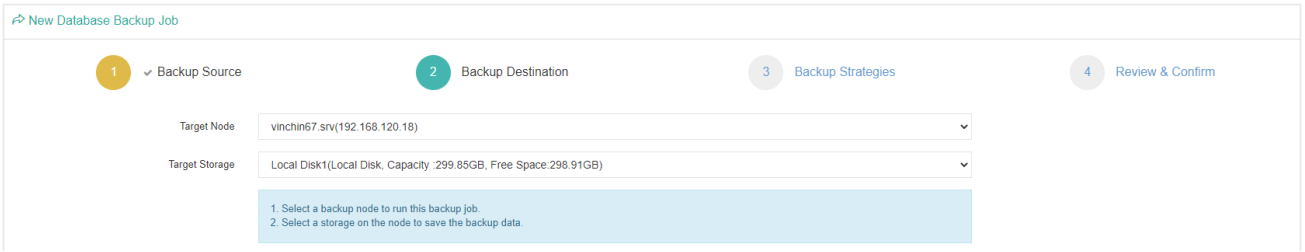
Step 1: Backup Source

First you need to select a target database server from the left column, then select PostgreSQL database instance you wish to backup, in the right column will show the instance you have selected.



Step 2: Backup Destination

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

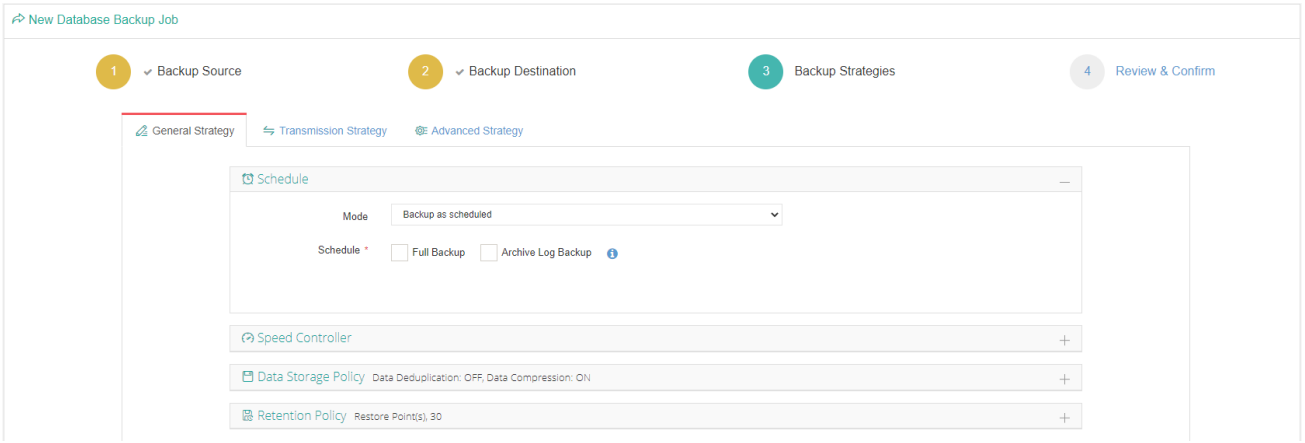


In the **Target Node** dropdown list, you can select a backup node on which you want the backup data to be processed and stored.

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

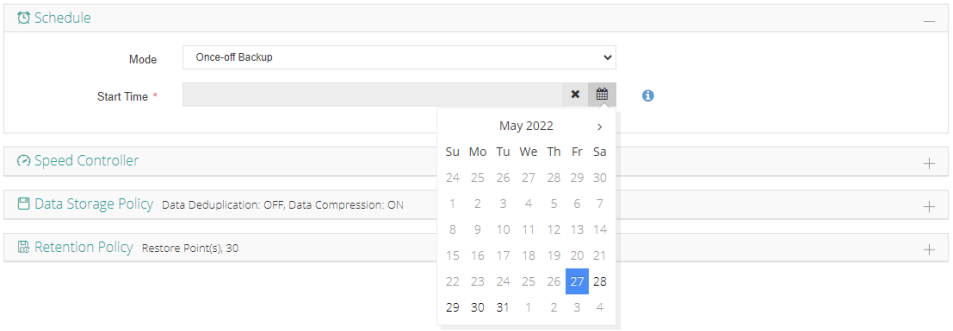
Step 3: Backup Strategies

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



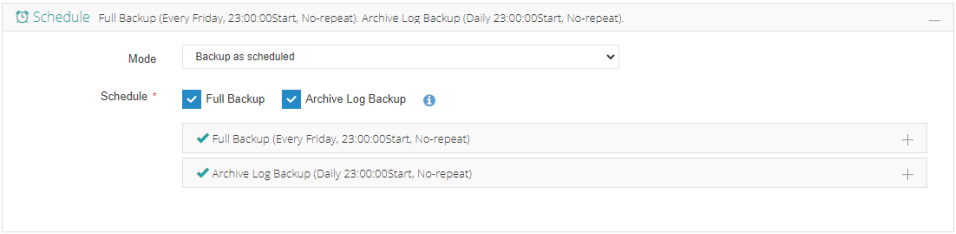
In the Schedule field, you can configure the time schedule of the backup job, you can configure the job as a **Backup as Scheduled** job or a **Once-off Backup** job.

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



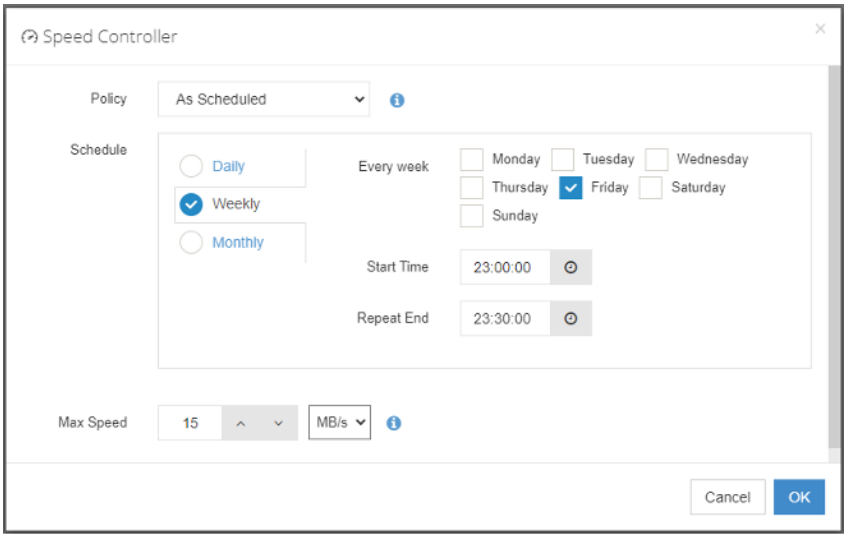
If you want to setup a Backup as Scheduled job, you can schedule Full Backup and Archive Log Backup.

For PostgreSQL database, it is recommended to schedule weekly full backup with daily archive log backup.

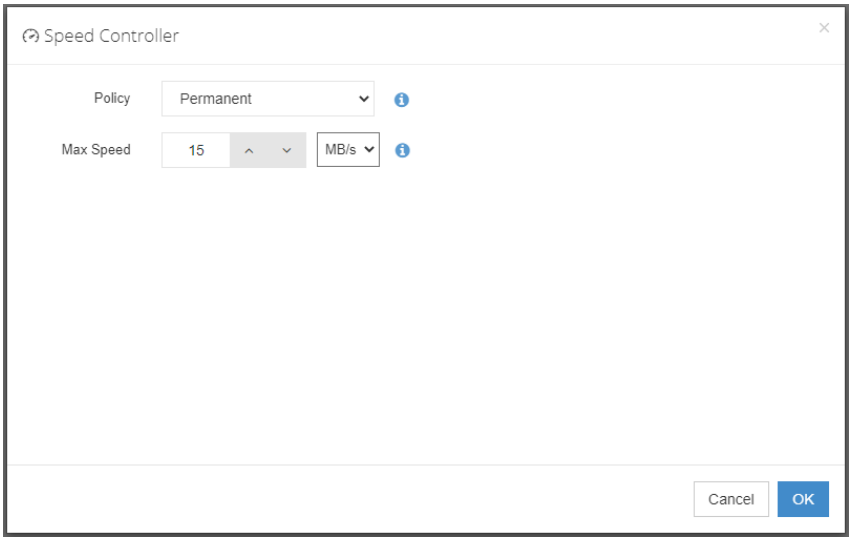


Speed Controller is optional. It can be used to limit the transmission speed during database backup if needed.

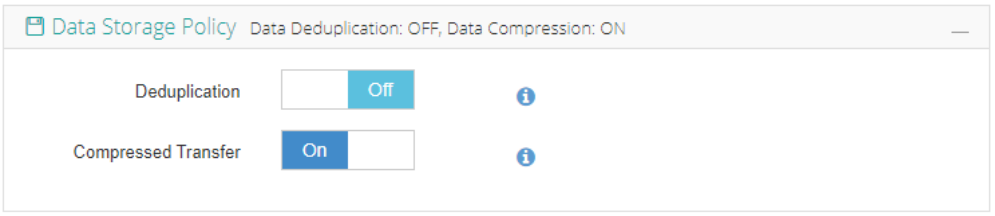
The speed controller policy can be configured as either As Scheduled or Permanent. An As Scheduled policy can be configured to limit the backup speed on Daily, Weekly and Monthly basis.



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



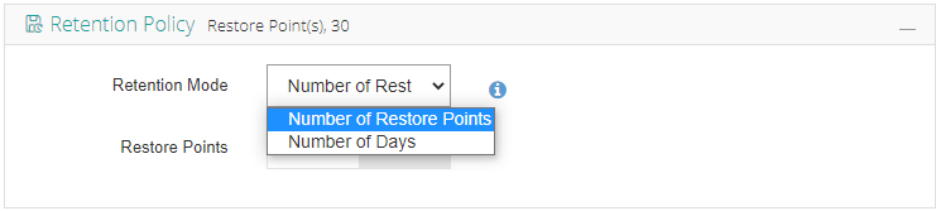
There are 2 options in Data Storage Policy section, Data Deduplication and Data Compression. By enabling these 2 options, the backup data will be deduplicated and compressed before saving into backup storage.



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

For the retention mode **Number of Restore Points**, the restore points will be counted by number of full restore points, including the archive log backups dependent on the corresponding full restore points.

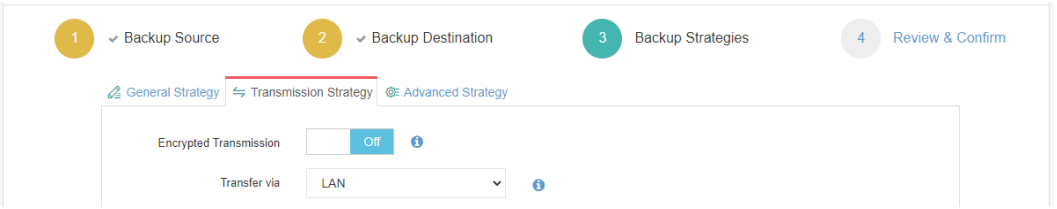
For retention mode **Number of Days**, Vinchin Backup Server will save the restore points within the specified number of days.



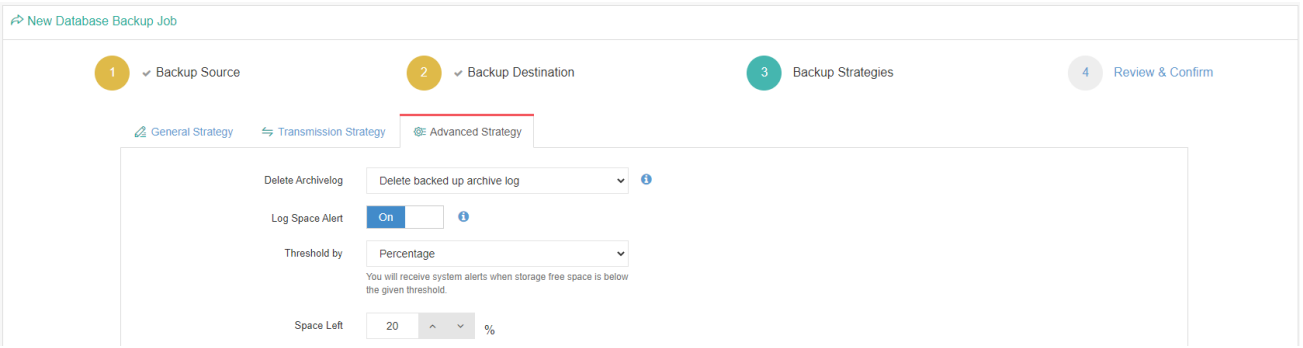
When the retention policy is triggered, the outdated restore points will be purged to comply with the retention policy.

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

The backup data will be transferred through LAN by default.



Advanced Strategy allows you to configure archive log deletion and log space monitoring options.



Delete Archivelog: there are 3 options **Delete backup up archive log**, **Do not delete** and **Delete all archive log**. It is recommended to use the Delete backed up archive log option to delete the archive log which had been backed up.

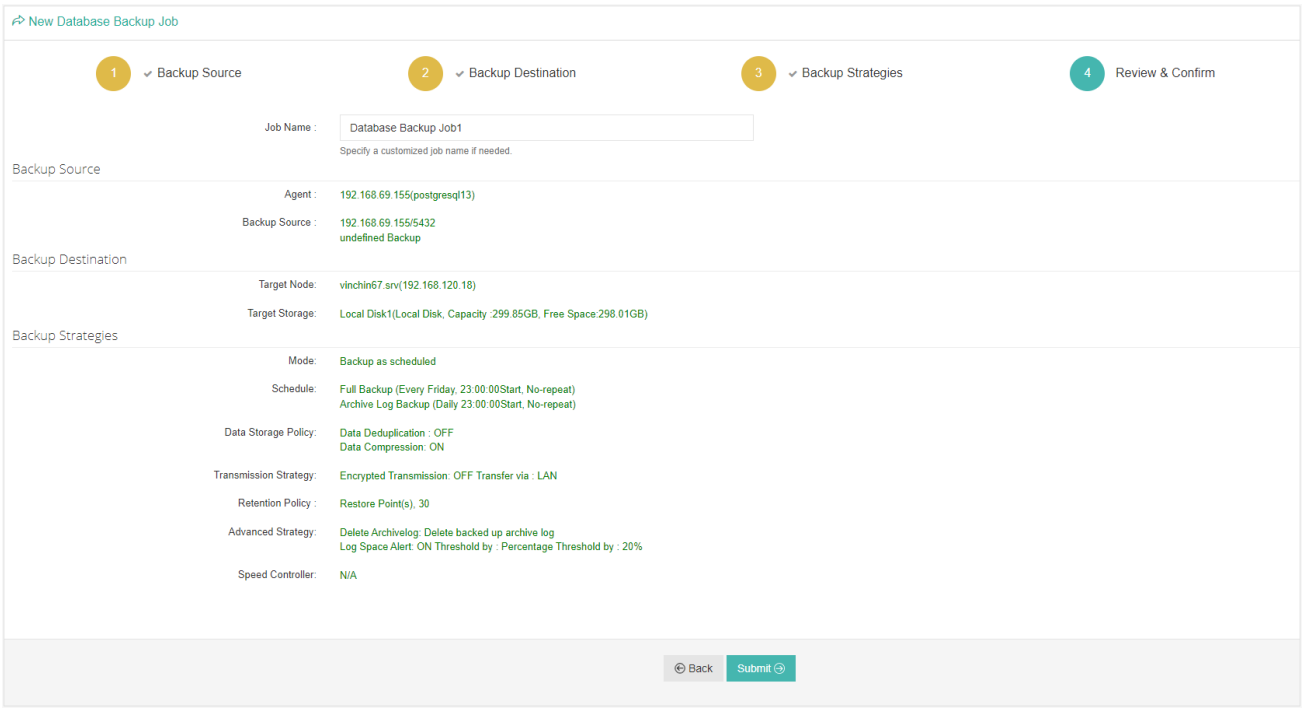
Log Space Alert: if enabled, Vinchin backup server will monitoring on the archive log space usage, when exceeded the specified threshold you will receive alerts on the Vinchin web console.

Note

If Delete Archivelog has been set to Do not delete, DBA must manually delete archivelog files regularly, otherwise, production database crash may occur once space is fulfilling with archive log files. It is recommended to set Delete Archivelog option to Delete backed up archive log.

Step 4: Review & Confirm

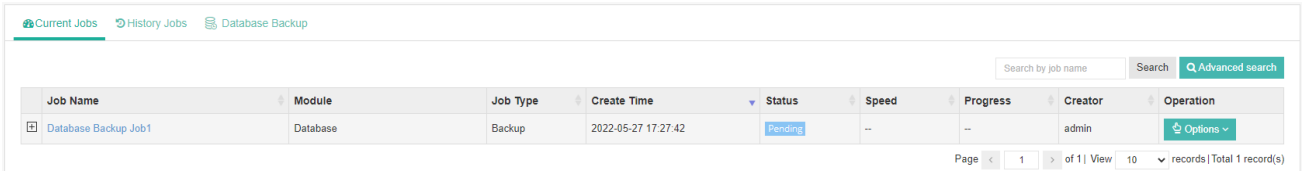
After completing the above-mentioned settings, you are able to review and confirm the settings in one screen.



A job name can be specified for identification of the database backup jobs, and by clicking on the Submit button to confirm the creation of the backup job.

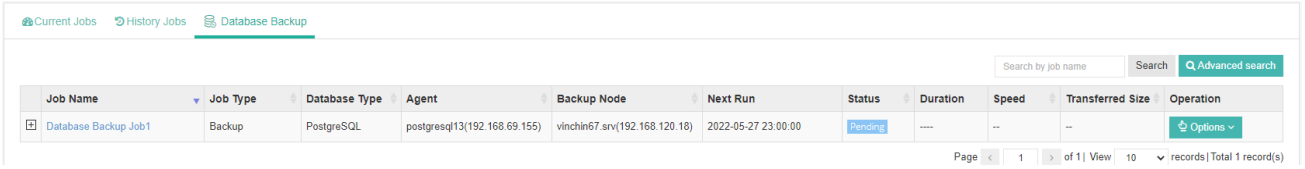
Database Job Operations

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



The status of the newly created job will usually be **Pending**, when the time condition matches the schedule, it will automatically run. And the status will change to Running, you can also see the transfer speed here within the job list.

Besides the Current Job list, there's a dedicated tab to show database backup jobs. More detailed information of database backup jobs, including database type, database agent info, backup node, next run time and some more detailed information dedicated for database backup will be given.



By clicking on the job name you can check more detailed information on the **Job Detail** page.

For a scheduled backup job, after running one of the schedules, the status will change to Pending again and then wait for the next run.

For a once-off backup job, after running the job for once, it will be removed from the **Current Job** list. And you can find it from the **History Job** list.

Database Restore

Vinchin Backup & Recovery supports two recovery mode for PostgreSQL database: **Override Original Database** restore and **Restore to New Path**.

Before starting to restore PostgreSQL database, there are some database configurations need DBA to check. The target recovery database server must have database backup agent installed, and the service ports: 20200, 20201, 20300 and 20400 needs to be opened for Vinchin backup server.

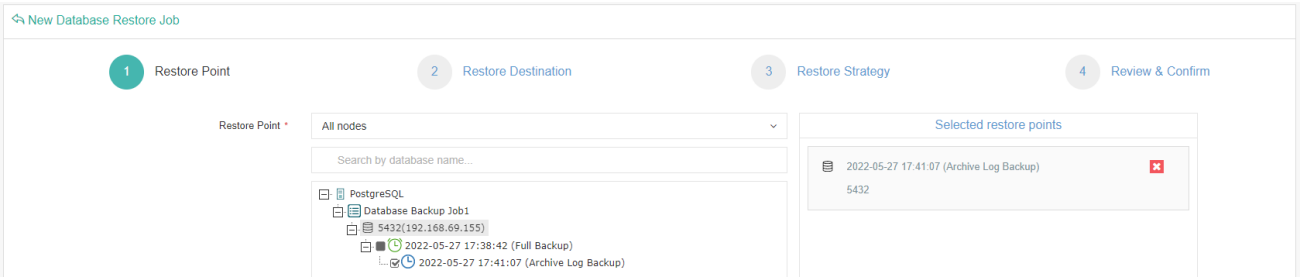
If override original database restore, the target PostgreSQL database instance needs to be shutdown, the path of data directory and archive log directory must be the same as original database server, and the free storage space of the database server must be enough to save the full restore point data size.

If restore to new path, you must specify a custom port number to run the database instance and the port number should not be used by any other services on the database server. And you need to specify new directories for data and the archive log, these 2 directories should be empty and should not be any directory which is being used by any other services on the database server. For the free storage space required, it must be 2 times more than the full restore point data size.

To create a PostgreSQL database restore job, please go to **Database Backup** -> **Restore** page and follow the steps below.

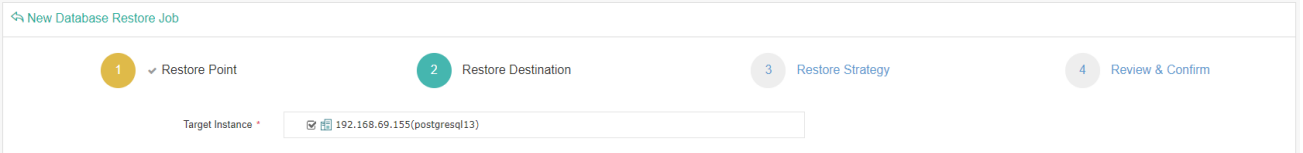
Step 1: Restore Point

If you select a full restore point, you'll be able to directly restore PostgreSQL database to the state of when the backup was taken. If you select an archive log restore point, you are able to roll back the database state to any time point between the first full backup timepoint and the selected archive log backup time point.



Step 2: Restore Destination

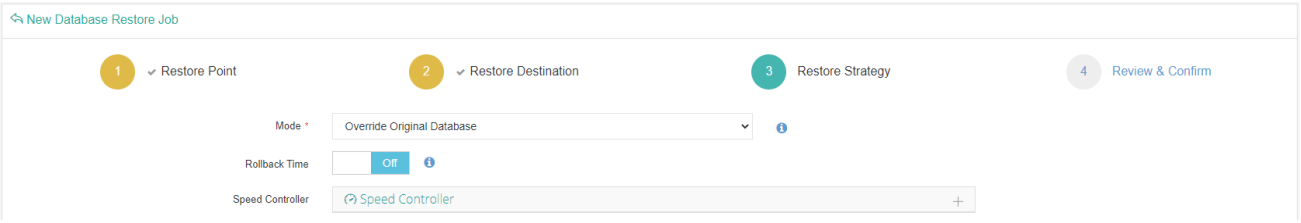
After selecting restore point, select **Target Instance** which you wish to restore.



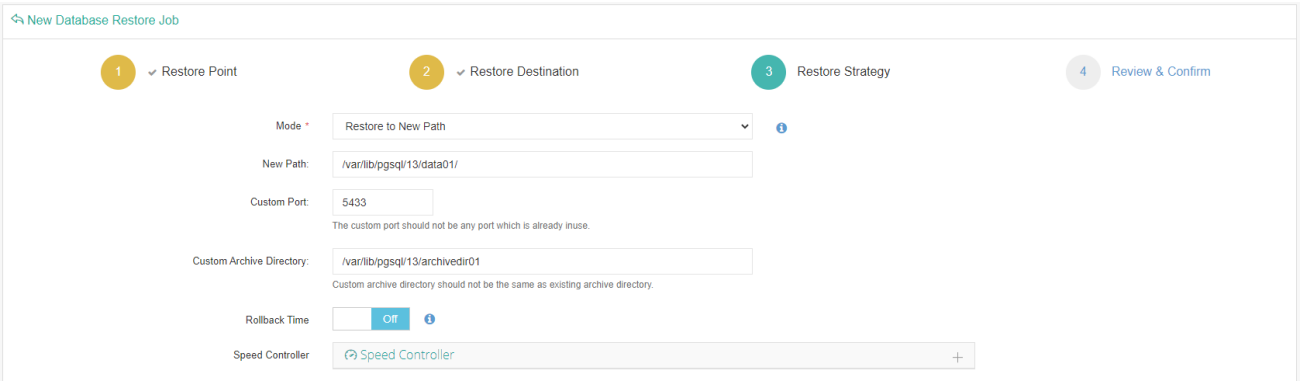
The target database instance can be the original database server or a new database server.

Step 3: Restore Strategy

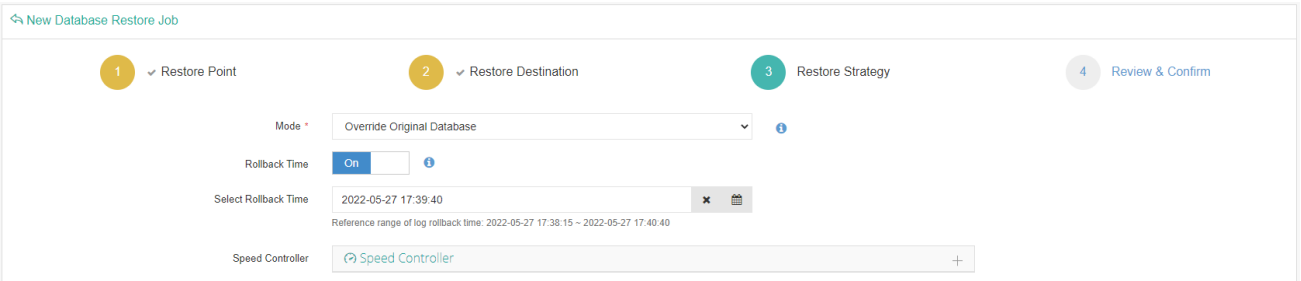
Mode: Override Original Database applies to restore the data to the production database server. Override the data of the original database instance.



Restore to New Path applies to restore data to a new directory. The directory needs to be created by the PostgreSQL database user and has PostgreSQL user permissions.



Rollback Time: if you had selected archive log backup restore point, you are able to rollback PostgreSQL database state within the given time range.

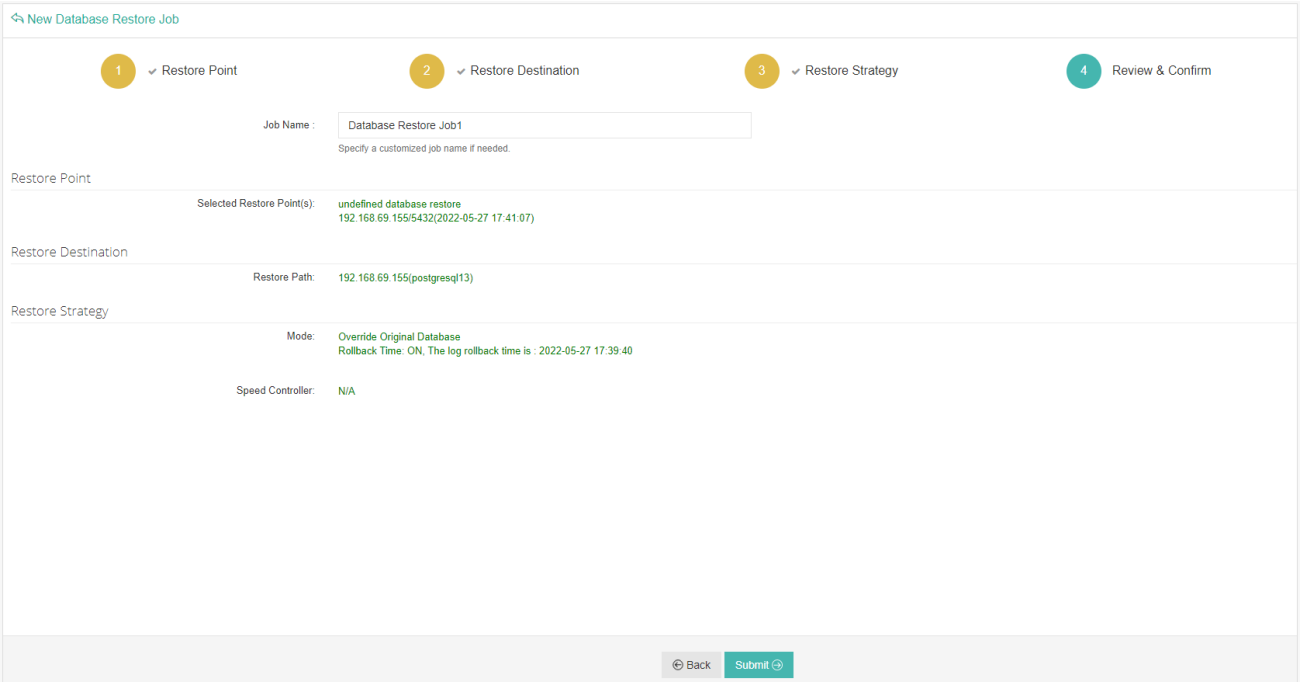


If you disable rollback time it will by default restore to the latest time point of when the backup has been taken.

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

Step 4: Review & Confirm

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



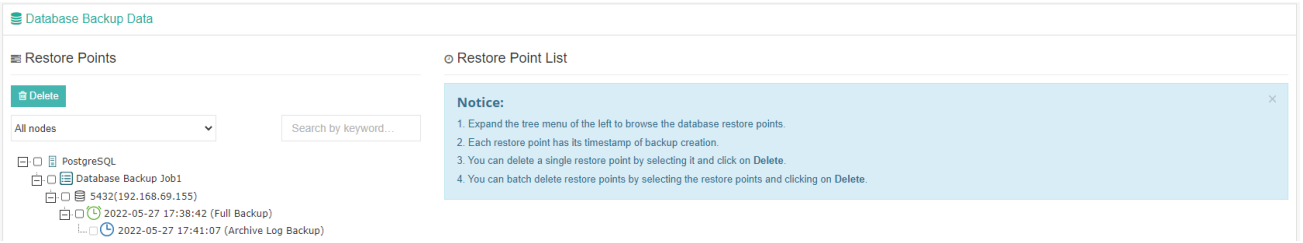
Once the job has been created, you'll be redirected to the **Monitor Center** > **Jobs** page.

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

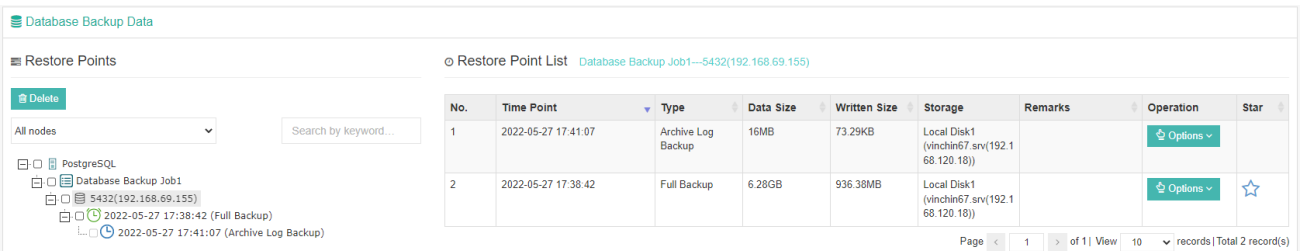
During the database restore process, the full data size of the full backup will be transferred from Vinchin backup server to the database server, and the data will be written in to a temporary directory, after transmission is completed then it will perform restore/roll backup restore operations according to the job configurations.

Database Backup Data

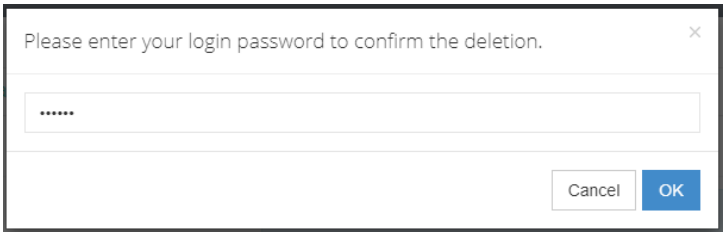
The database backup data can be managed from **Database Backup** > **Backup Data** page.



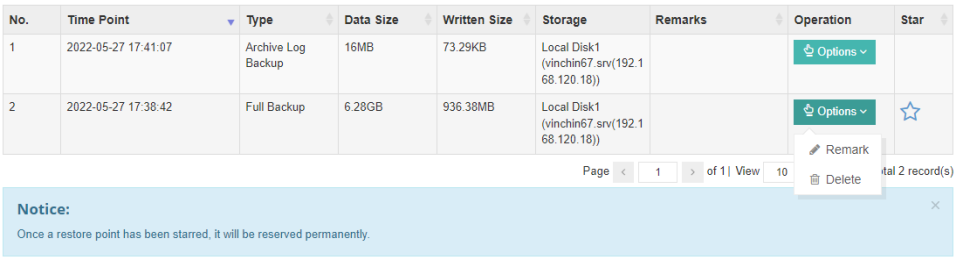
If you want to delete a restore point or multiple restore points, you can first select target restore point(s) from the left tree, and click on the **Delete** button. The archive log backups cannot be deleted individually, they will be deleted along with the dependent full backup.



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



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



You can add remarks to the full backups and the archive log backups, and click ☆ with full restore point to keep the full backup and its dependent archive log backups to not be deleted by retention policy.

Note:

1. In the restore point list, users are not allowed to delete an individual archive log restore point, when you click on Options button you are only able to add remarks to an archive log restore point.

2. If it's a full restore point, you are allowed to add remarks to it or to delete it, but deleting a full restore point will also delete the archive log restore point dependent on the full restore point.

File Backup

Install File Backup Agent

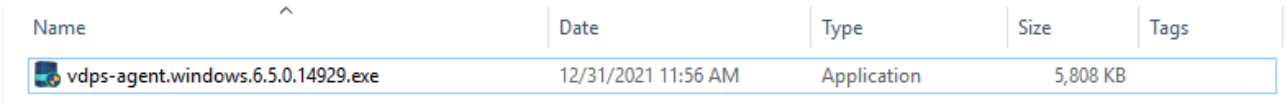
Windows

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

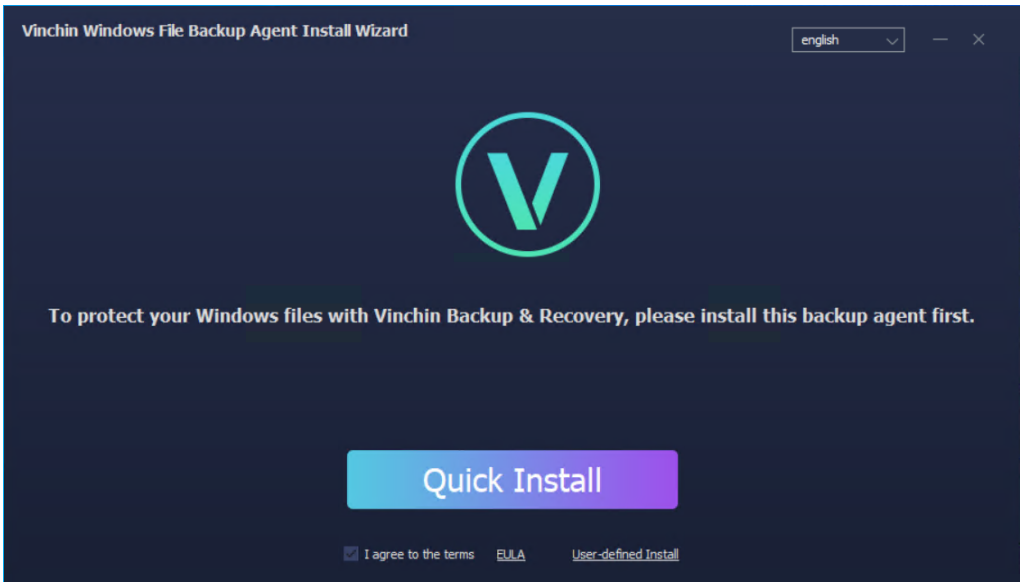
To install file backup plugin, you can open Vinchin Backup Server web console from the target Windows system directly, on the login screen, click on **Download Backup Plugin** to go to the backup plugin download page.

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.

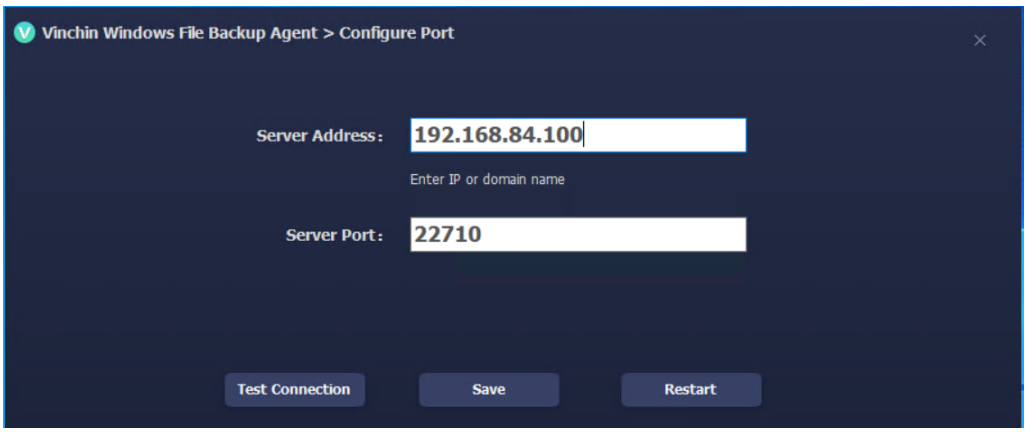
The downloaded file backup plugin should be an executable exe file.



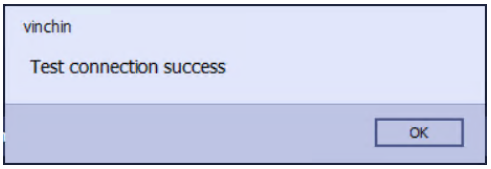
To install the backup plugin, please right click on it and select **Run as administrator** to install the backup plugin with administrator permissions.



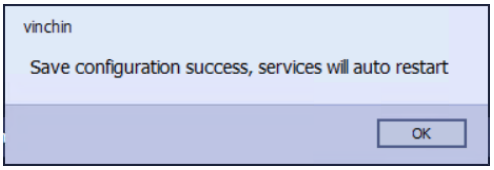
Click on **Quick Install** button to start the installation, the installation will take a few seconds. Once installation completed, please find the backup plugin icon from the taskbar and right click on the icon, and then select **Agent Configure**.



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.

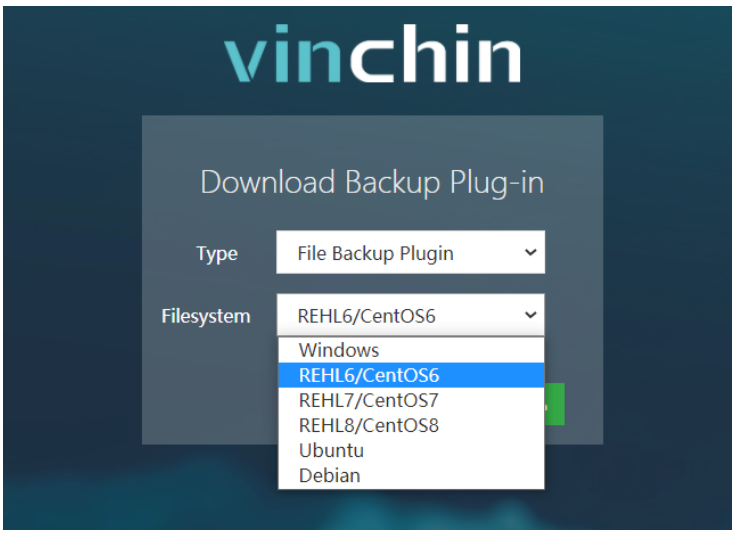
Note

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>
```

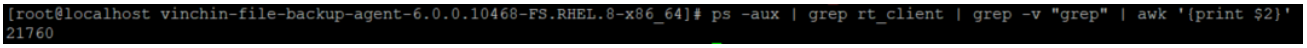
```
        <client_key_name>client.key</client_key_name>
        <log_dir>/var/log/vinchin/</log_dir>
        <log_num>60</log_num>
        <log_level>debug</log_level>
</router-client-conf>
```

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.



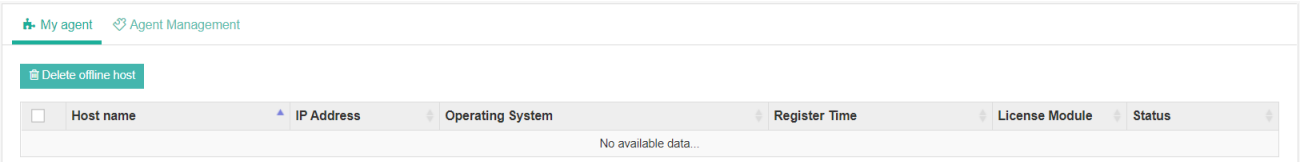
In this example, the PID is 21760, please terminate the process using the command below.

```
kill -9 21760
```

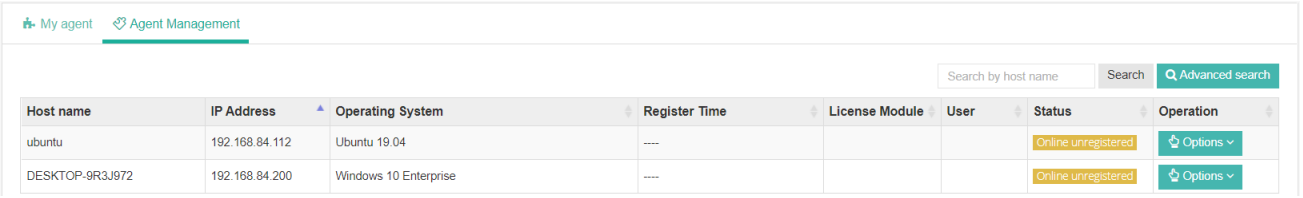
After terminating the rt_client process, it will be automatically restarted by the file backup plugin daemon process, and the modification of the server IP should be effective now.

Register File Backup Agent

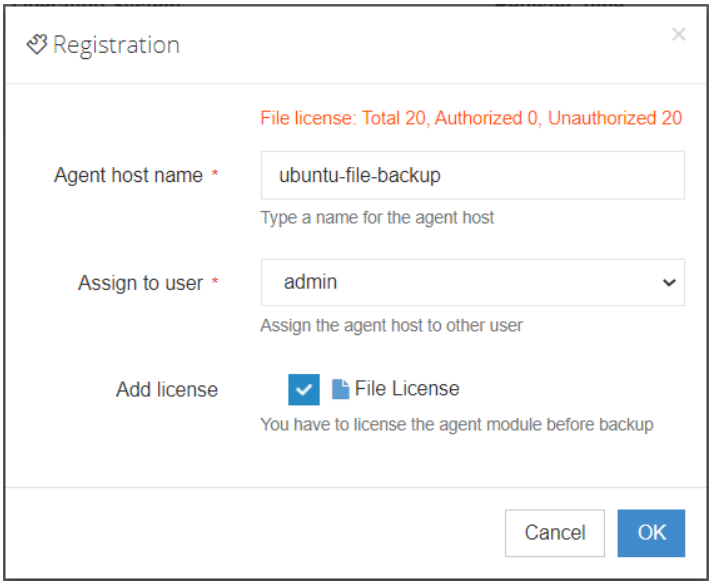
After the installation and configuration of the backup plugin on the target host(s), please open Vinchin Backup Server web console and go to **File Backup** > **Backup Agent** page.



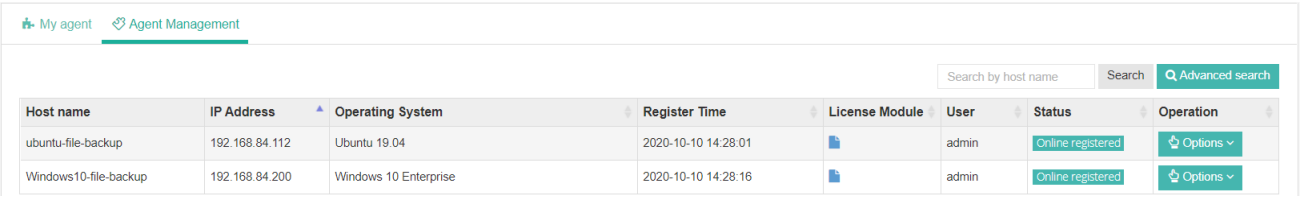
Click on the **Agent Management** tab to register those hosts to Vinchin Backup Server.



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 customize 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.



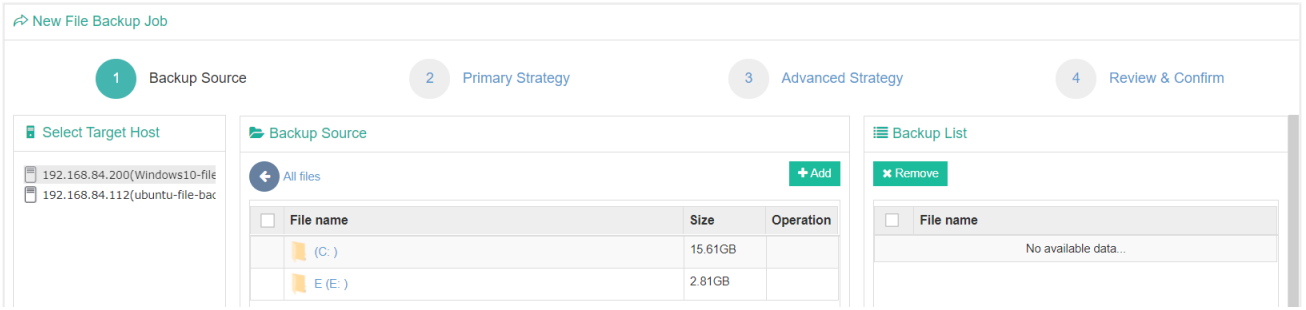
File Backup

Create File Backup Job

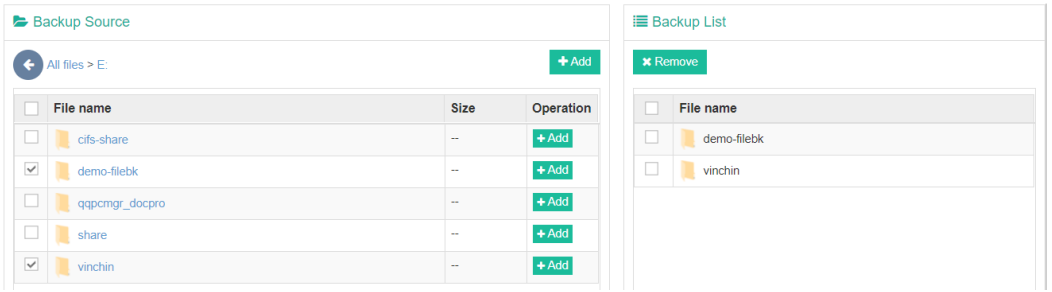
To create file backup jobs, please go to **File Backup** > **Backup** page. There are 4 steps to create a file backup job.

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.



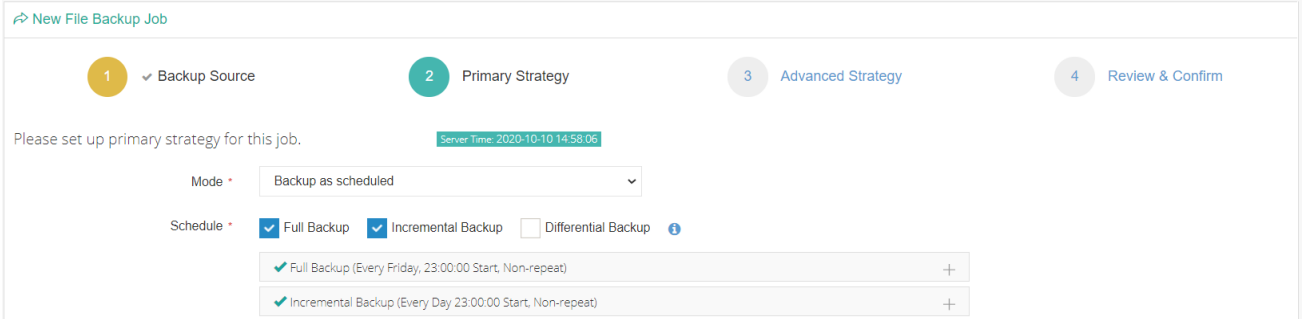
After selecting the files/folders, please click on **Next** to continue.

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

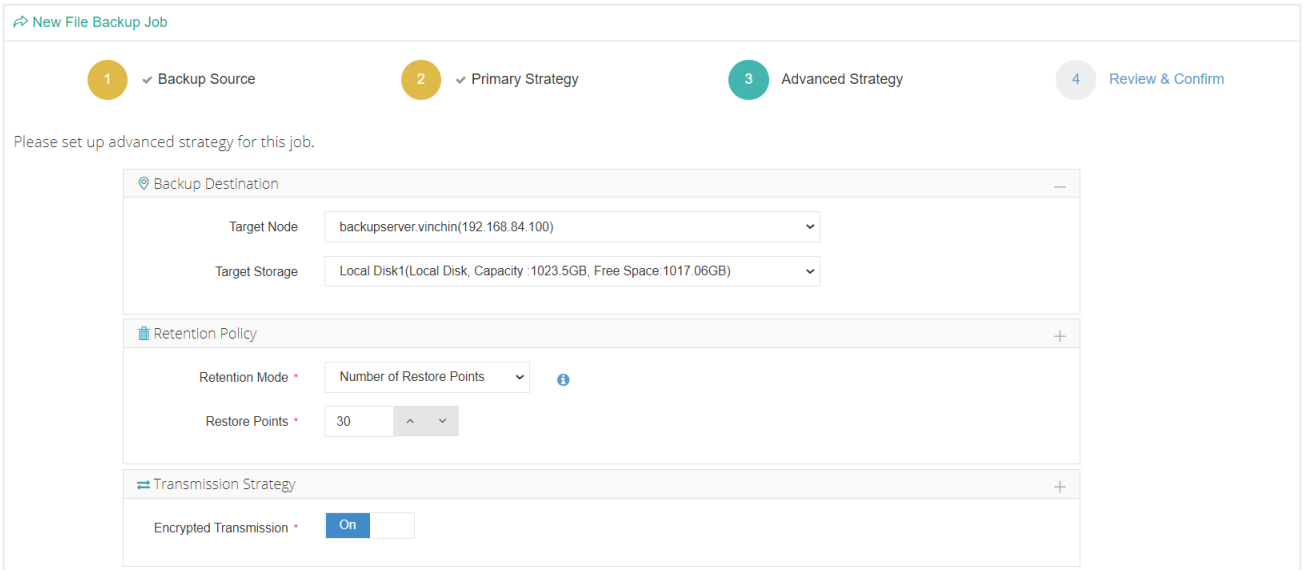
For the backup mode, you could choose between **Backup as scheduled** and **Once-off Backup**, the principle of these backup modes are similar with VM backup.



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.

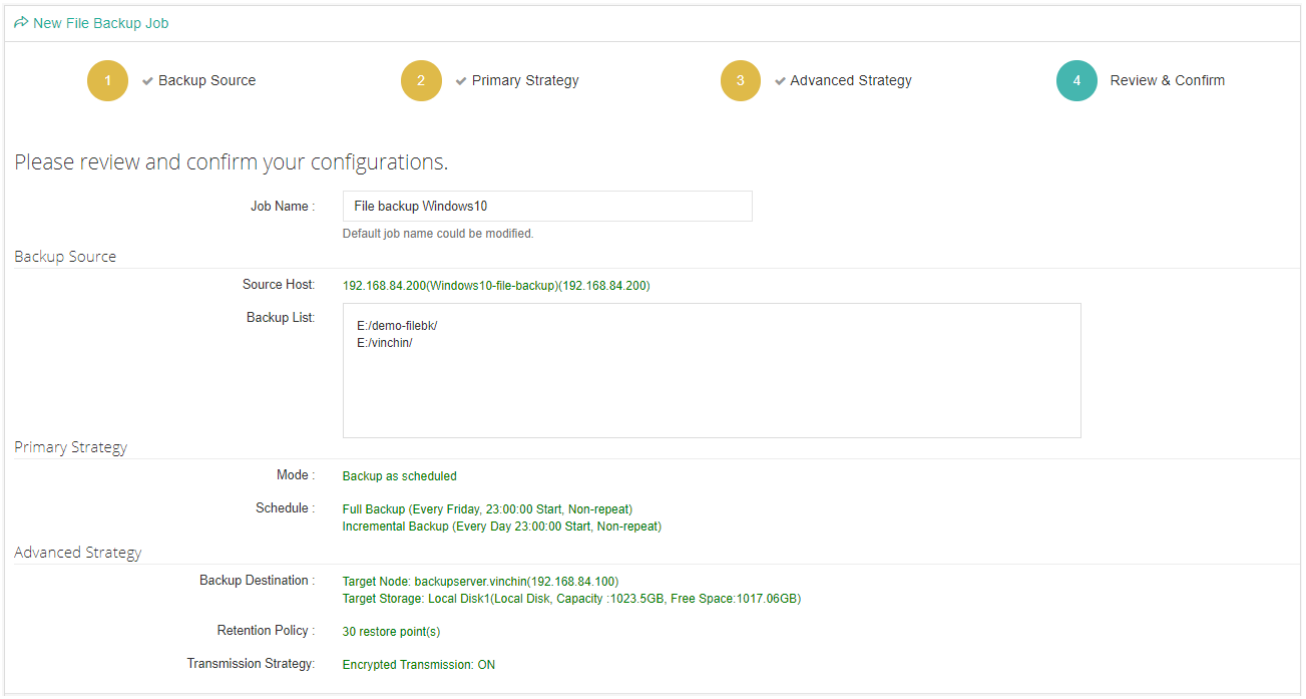


If you have chosen once-off backup, then there's no need to configure the retention policy, as there will only be one restore point for this file backup job.

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

Step 4: Review & Confirm

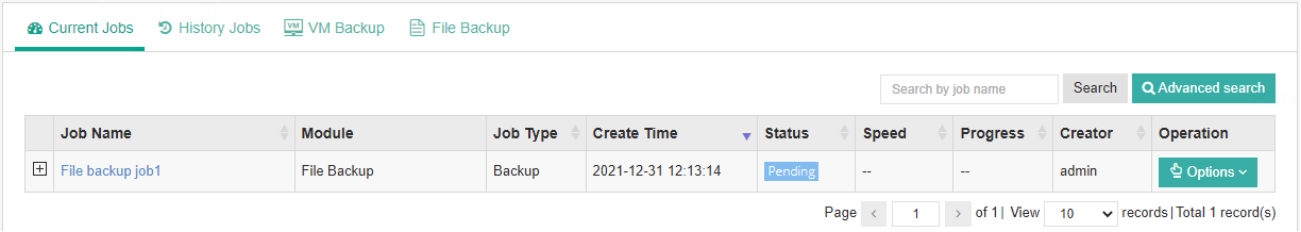
After completing the above mentioned settings, you are able to review and confirm the file backup job settings in one screen.



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.



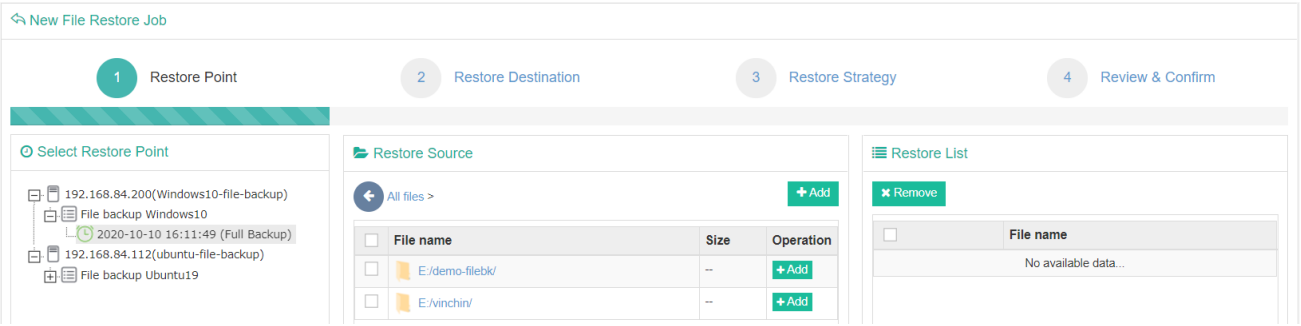
The newly created file backup job will be in pending status, the operations which can be done to the file backup job is similar with the VM backup jobs, you can start, stop, edit or delete the job from the current job list.

File Restore

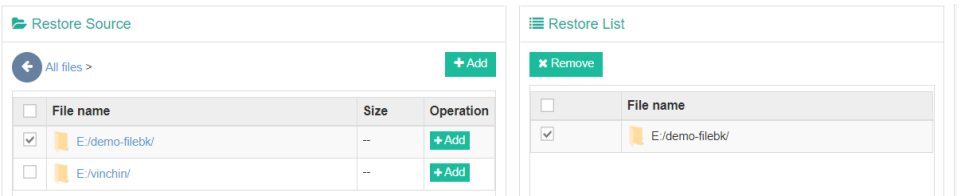
To restore files from file backup restore points, please go to **File Backup** > **Restore** page. There are 4 steps to restore files from the file backup restore points.

Step 1: Restore Point

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



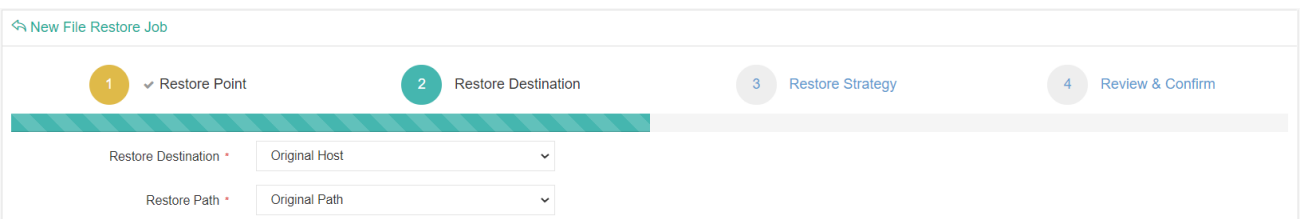
Then select the desired files/folders from the **Restore Source** column and add them to the **Restore List** column.



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

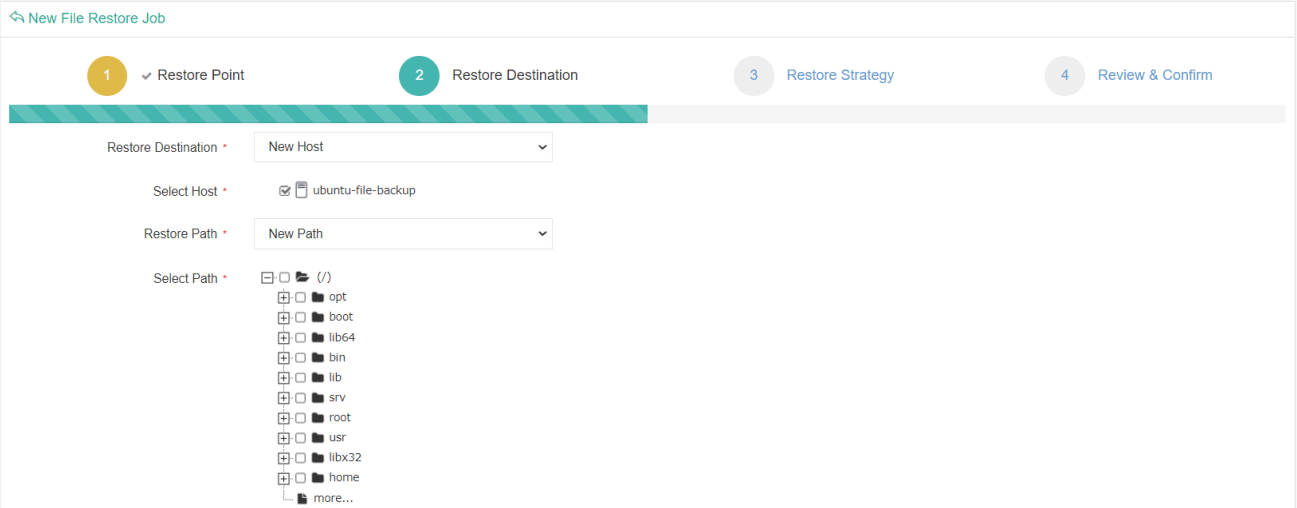
Step 2: Restore Destination

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.

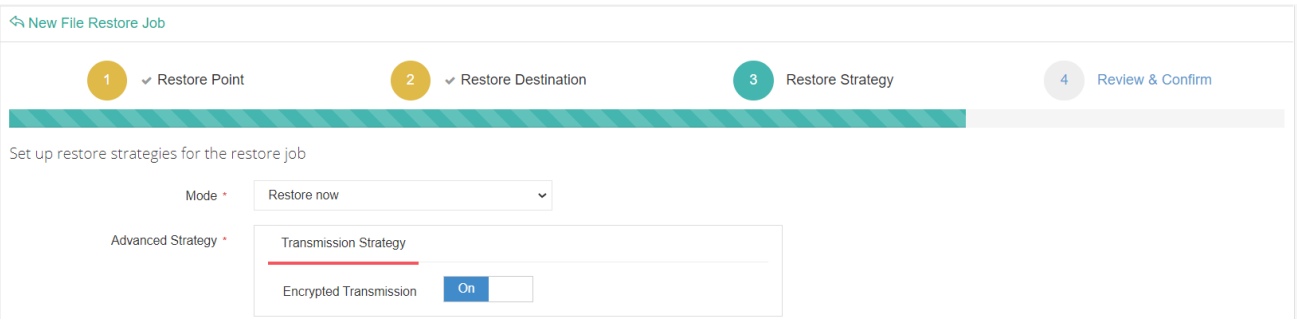


Note

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

Step 3: Restore Strategy

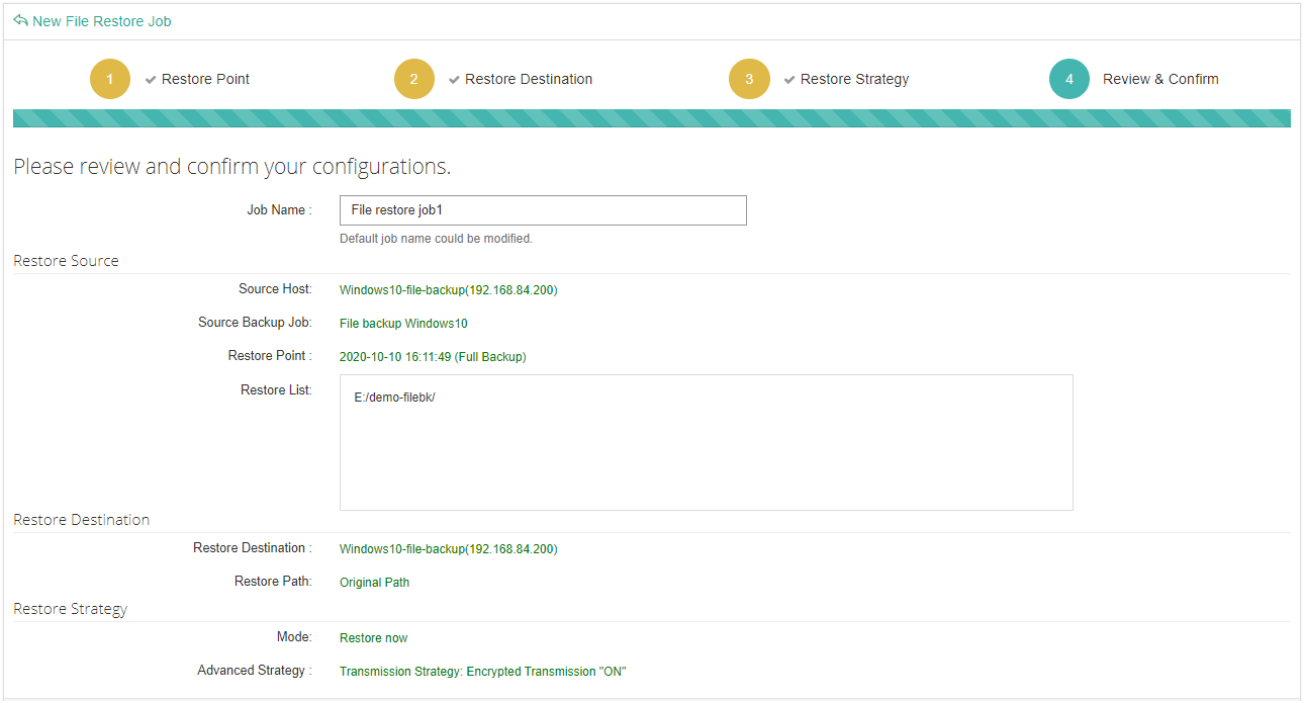
The restore mode of files/folders can only be **Restore now**, you can choose to enable **Encrypted Transmission** for data safety.



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.



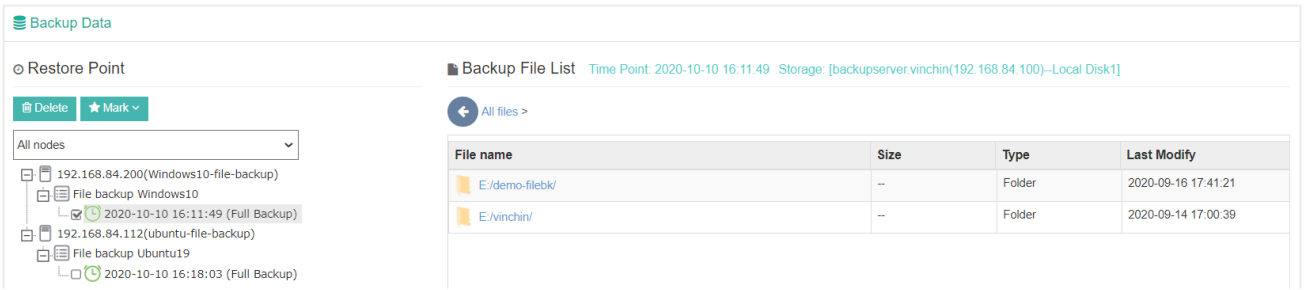
Once the job has been created, you'll be redirected to the **Monitor Center** > **Jobs** page.

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 is a feature which can be used to make duplicate versions of your backup data to a secondary storage or location. The copied data is usually of the same version, size and type of your original backup data, and can be used to restore the backup data from any accidental deletion and corruption.

With Vinchin Backup & Recovery, you can copy your backup data to an onsite copy storage or to an offsite copy storage (offsite copy storage is a Vinchin Backup Server installed on remote site).

The onsite backup copy data can be used to restore VMs directly if you have lost both the production data and backup data.

If you had configured offsite backup copy, even if you have lost all data on primary site, the VMs can be restored on remote site to bring back the production VMs of virtual platform on the remote site.

Or after the primary site had been rebuilt, the offsite copy data can be restored back to the primary site Vinchin Backup Server for restoring production VMs and data on primary site.

In conclusion, you can achieve offsite DR (Disaster Recovery) by using offsite copy feature of Vinchin Backup & Recovery which is consistent with 3-2-1 Rule: three copies of your data, on two different storage media, one being off-site.

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 backup job should be completed at first place, no matter it's a VM backup, file backup or database backup job.*

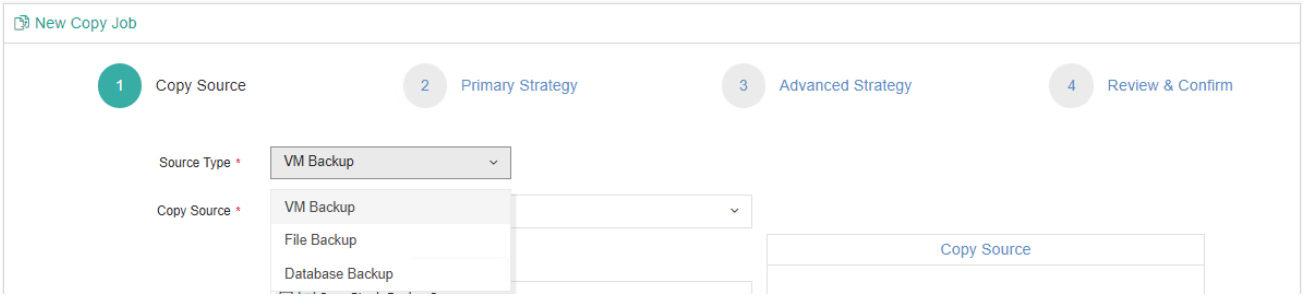
Backup Copy

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 corresponding **Source Type** from the dropdown list, by VM Backup, by File Backup, or by Database Backup**.**



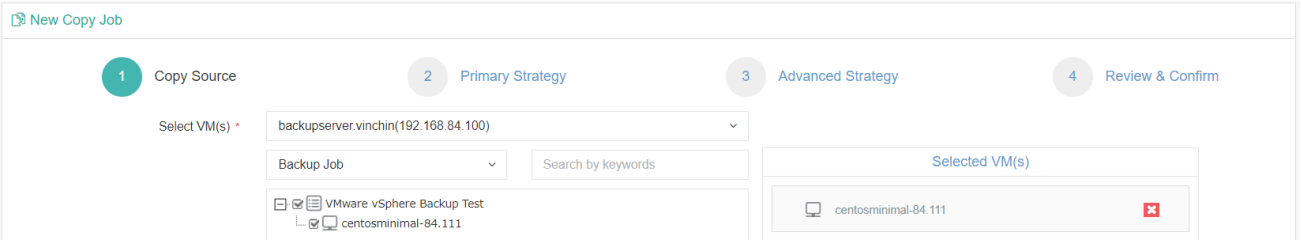
Next, select the backup node on which the backup data is stored, then you can select the backup data per Backup Job, Virtual Infrastructure (VM Backup only) or Restore Points (VM Backup only).

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.



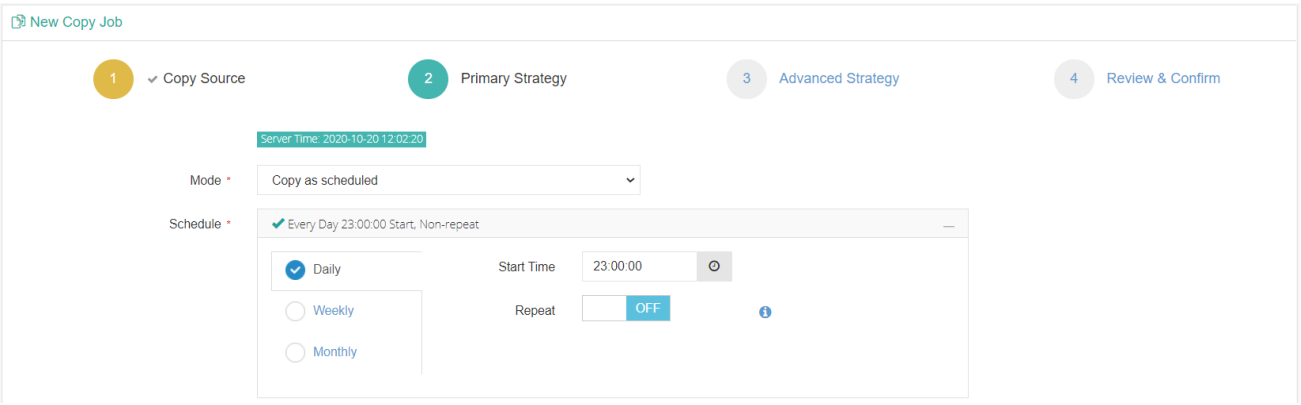
Once the copy source is selected, please click on **Next** button to continue.

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.

If you wish the backup copy to run regularly as per the backup job runs, please set **Copy as Scheduled**, otherwise set **Once-off Copy** to run the copy job for only once.

As for the schedule of the copy job, it is recommended to run the copy job right after the backup job finishes. For example, the backup job runs at 11 PM each day, and it takes approximately 2 hours to complete the backup job, so you can set the copy job to start 3 or 4 hours later than the backup job.

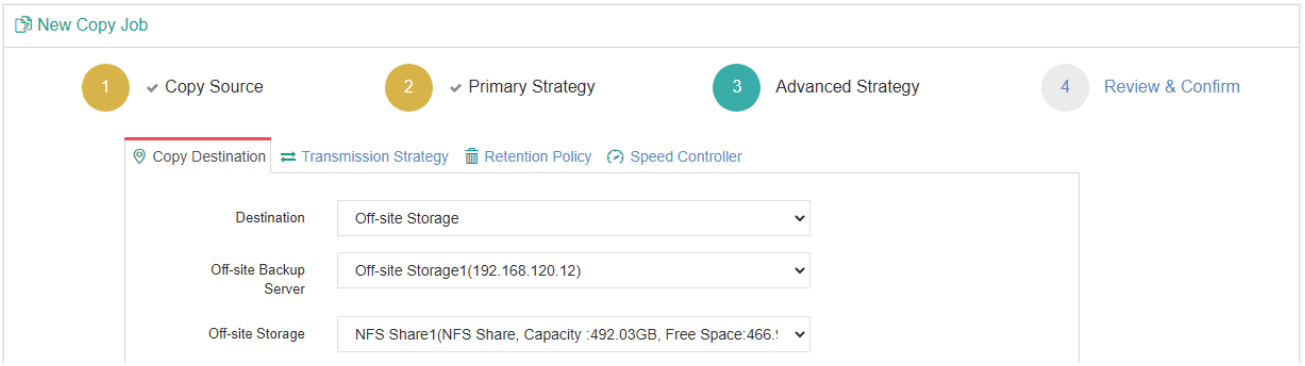
After done the mode settings, click on the **Next** button to continue.

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.



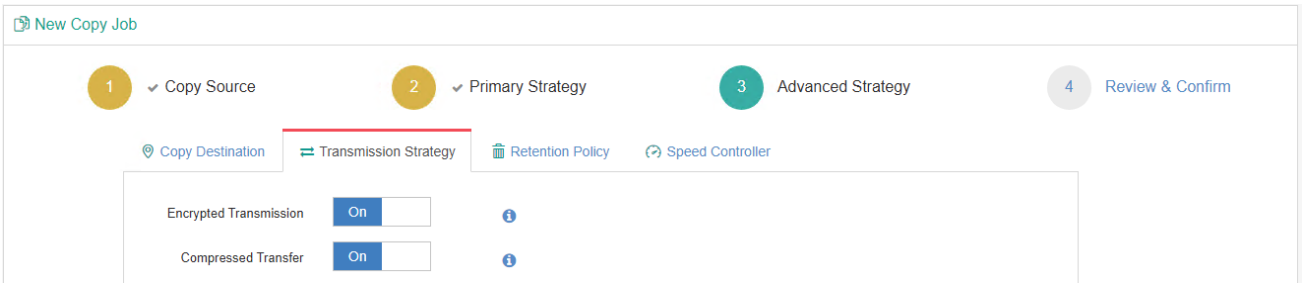
In the Destination field, Off-site Storage should be selected.

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.

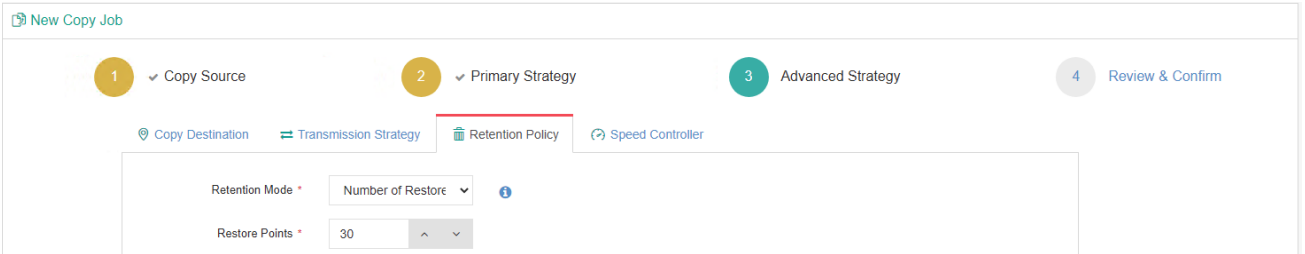


Encrypted Transmission: The data transmitted from backup source to backup copy storage will be encrypted to ensure the safety of the data transmission.

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.

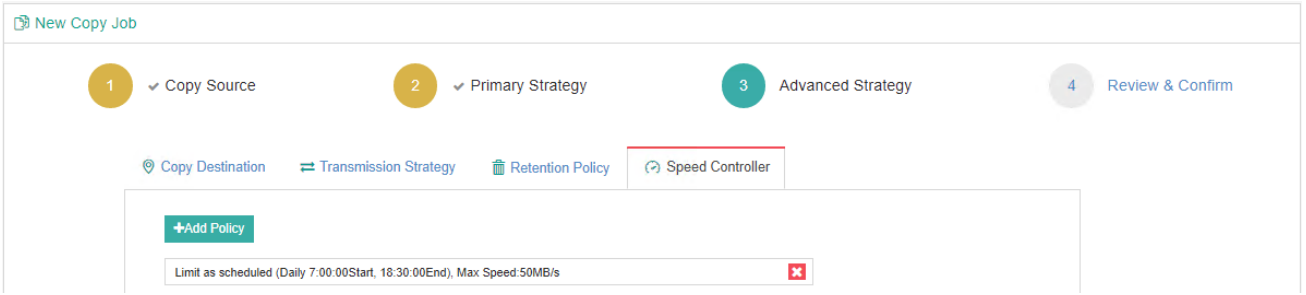


There's only **Number of Restore Points** retention mode for backup copy jobs, Vinchin Backup Server will save the specified number of restore points (for each VM, database and file backups included in the copy job), the older

restore points will be deleted or merged (restore point merge is only applicable for VM restore points) to comply with the retention policy.

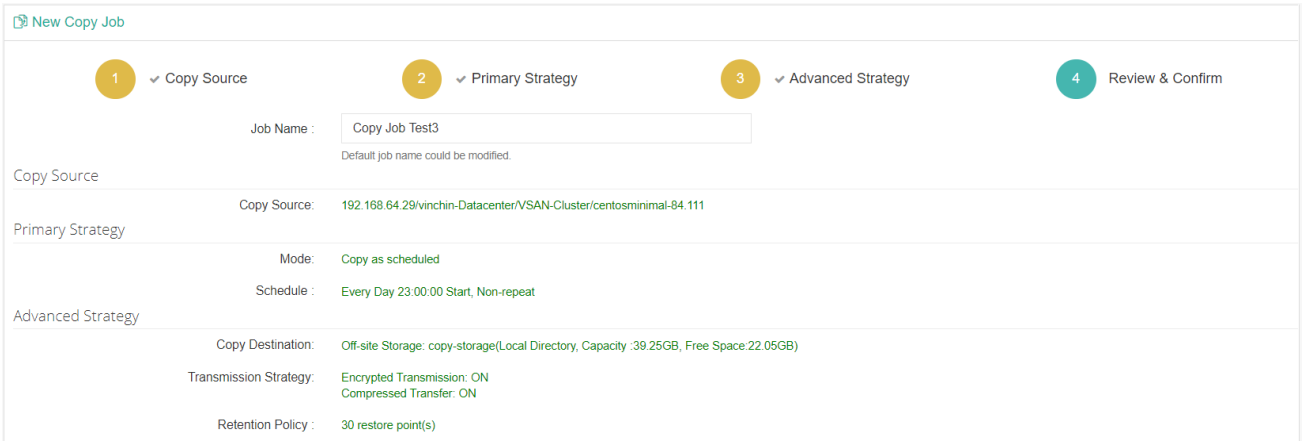
➢ Speed Controller

The speed controller settings are optional, only if the backup copy jobs will bring network or I/O overload to your production environment, you need to configure the speed controller accordingly.



Step4: Review & Confirm

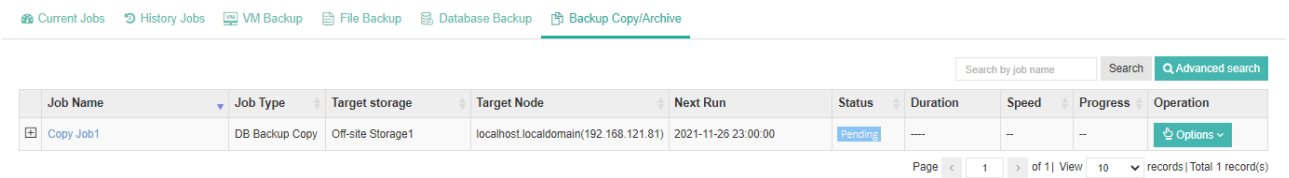
After completing the above settings, you are able to review and confirm the settings.



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.

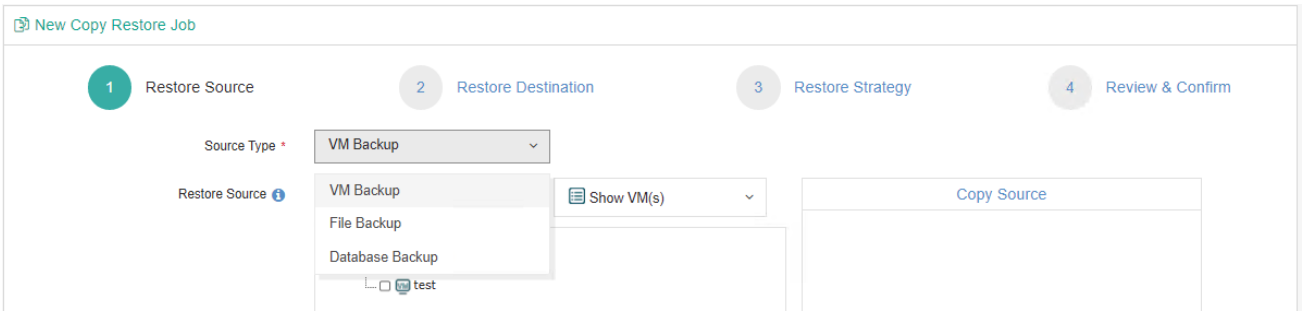
Copy Restore

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/Database/Files on primary site. But the backup copy data stored on the off-site backup copy storage cannot be used to restore VMs/Database/Files directly to primary site, it should be restored to an on-site storage first, then from the **VM Backup** > **Restore**, **Database Backup > Restore** and **File Backup > Restore** page you can create restore jobs to restore the VMs/Database/Files.

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 select the **Source Type** which you wish to restore, and then select the restore point(s).



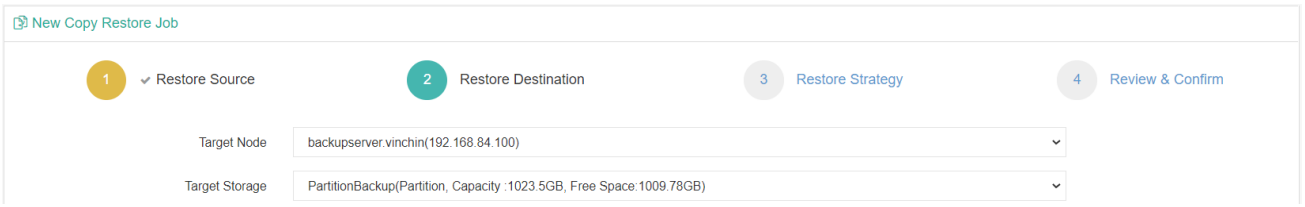
Click on **Next** to continue.

Note

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

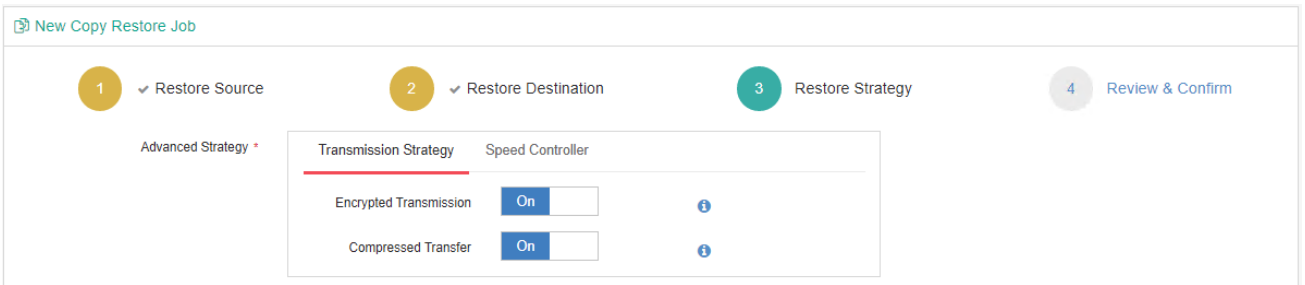
Step 2: Restore Destination

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.



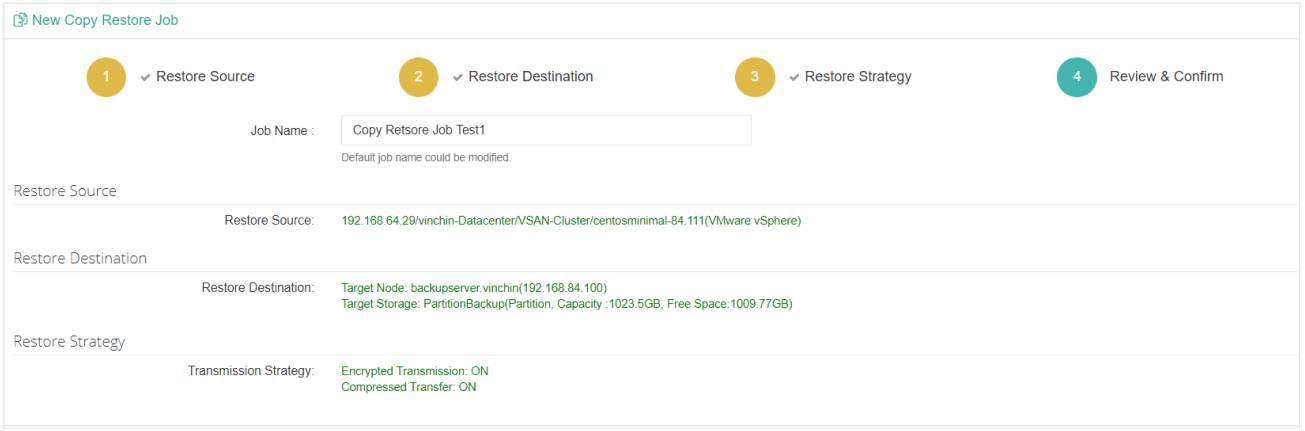
Encrypted Transmission: The data transmitted from off-site backup copy storage to on-site storage will be encrypted to ensure the safety of the data transmission.

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

Speed Controller: It is optional, only if the restore jobs will bring network or I/O overload to your production environment, you need to configure the speed controller accordingly

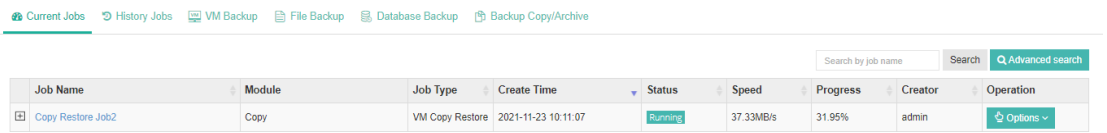
Step 4: Review & Confirm

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



You can optionally customize a job name and then click on Submit button to confirm the creation of this copy 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. Or if you restored offsite database backup copy or file backup copy, please go to **Database Backup > Restore** or **File Backup > Restore** page to create restore jobs accordingly.

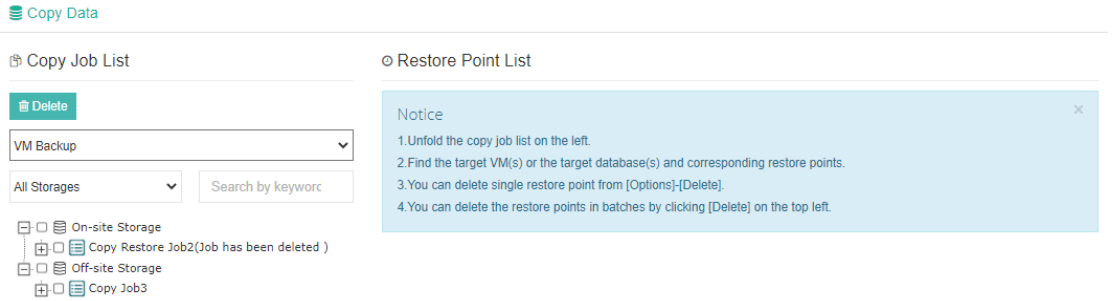
Note

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

Copy Data for VM Backup

All backup copy data can be managed from the **Backup Copy** > **Copy Data** page. No matter the data storage is in the on-site storage or off-site storage.



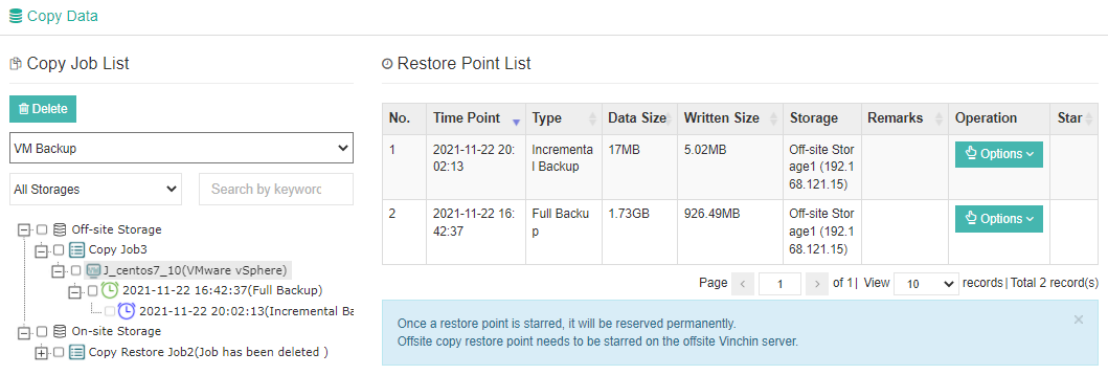
The Default source type from Copy Data page is VM Backup.

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.

Note

Please be careful to delete the copy data because the deletion CAN NOT be rolled back any more.

By clicking on a virtual machine, you'll be able to see all the copy restore points of the virtual machine.



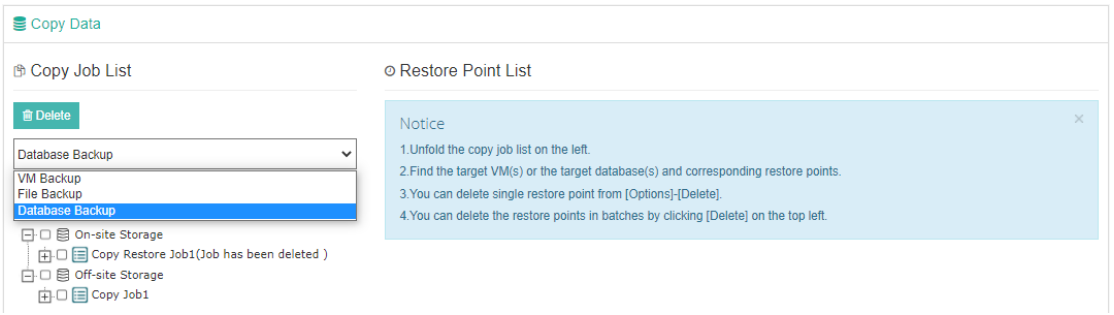
By clicking on **Options**, you will be able to remark or delete the restore point.

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.

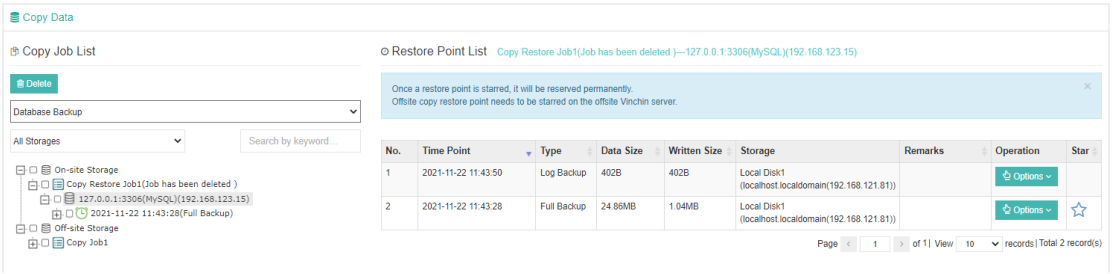
Copy Data for Database Backup

The copy data for database backup 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.

The Default source type from Copy Data page is **VM Backup**, please select the **Database Backup** from the dropdown list.



By unfolding the copy storages and the copy jobs, you are able to view all the copy data. And by selecting corresponding restore points, you are able to delete the selected copy data with the **Delete** button on the top left.

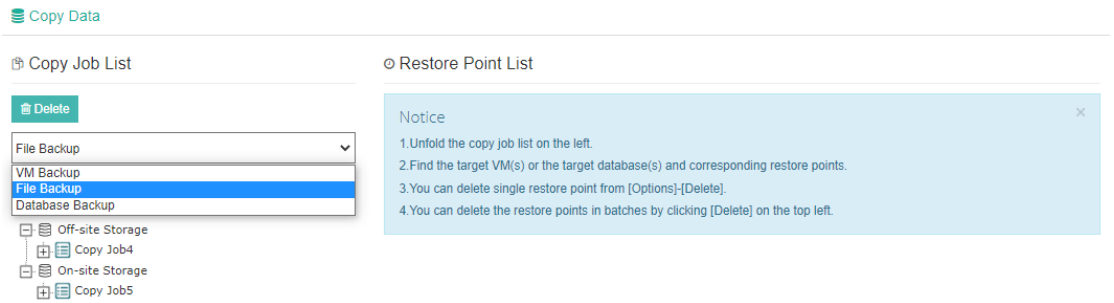


By selecting the copy data from on-site storage, you are able to view the detailed database information of the restore points, remark and star it. And the database information of copy data from off-site storage can be deleted and remarked only.

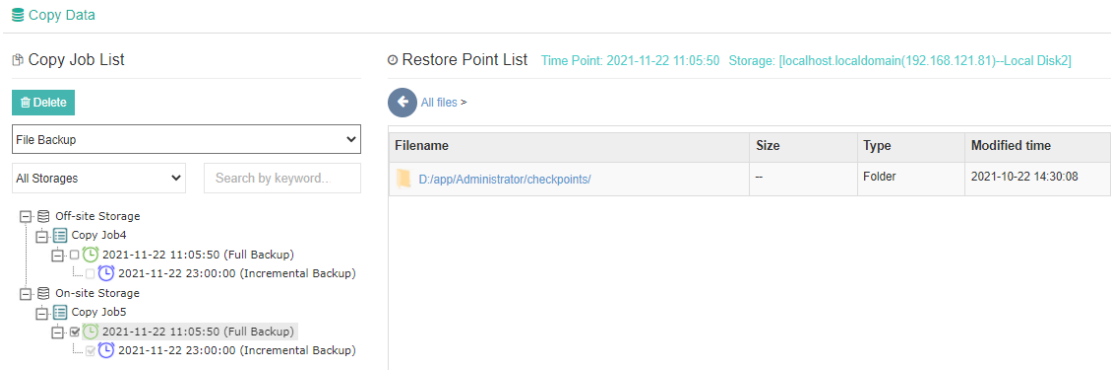
Copy Data for File Backup

The copy data for file backup 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.

The Default source type from Copy Data page is **VM Backup**, please select the **File Backup** from the dropdown list.



By unfolding the copy storages and the copy jobs, you are able to view all the copy data. And by selecting corresponding restore points, you are able to delete the selected copy data with the **Delete** button on the top left.



By selecting the copy data from on-site storage, you are able to view the detailed file information of the restore points. And the file information of copy data from off-site storage is not visible.

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 currently not supported with Microsoft Hyper-V.

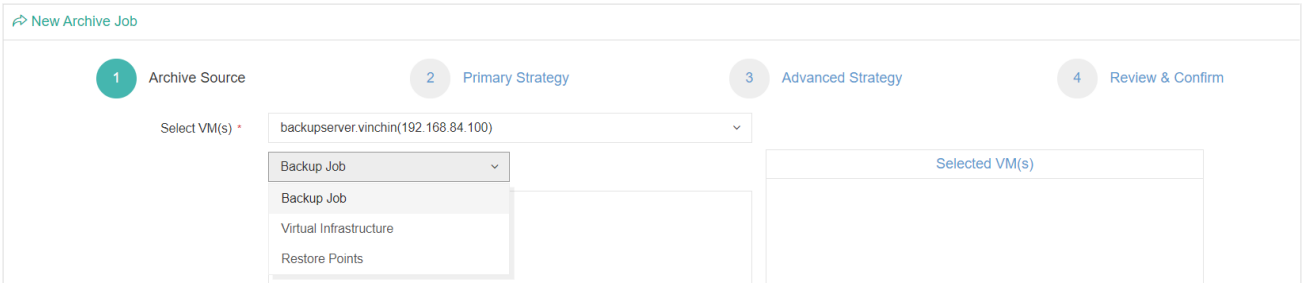
Archive

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.

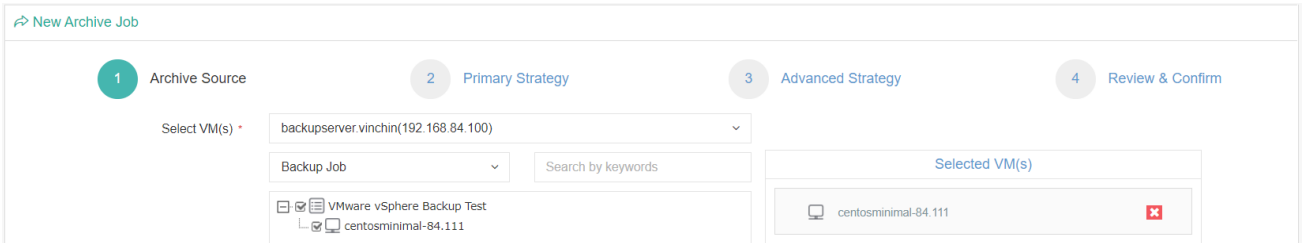


If you select Backup Job, existing backup jobs will be listed, by expanding the backup job you can select the archive source as per the VMs included in the backup job.

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.

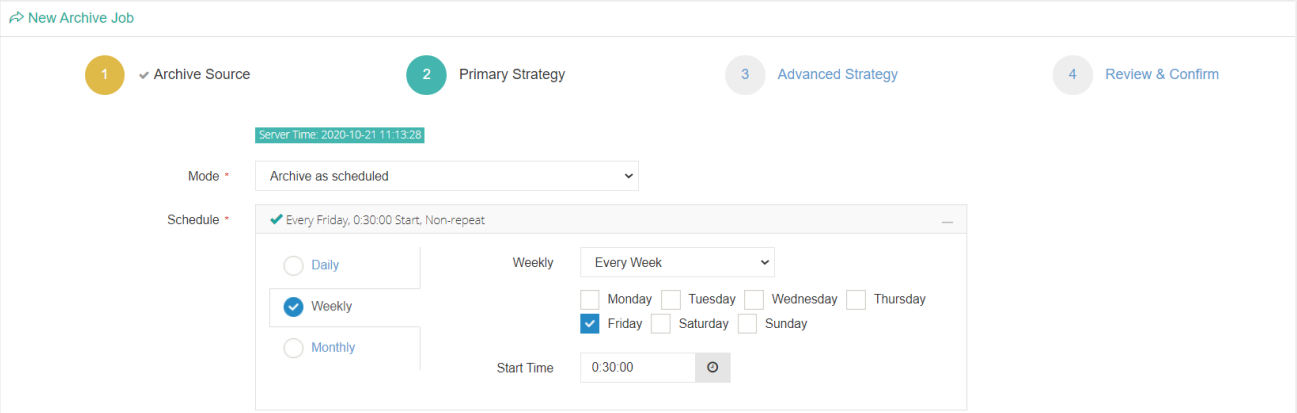
You can select the archive source either way as per your convenience.



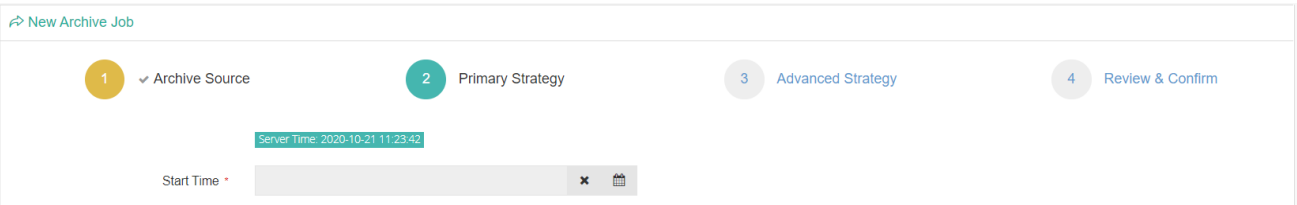
Once the archive source is selected, please click on **Next** button to continue.

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.

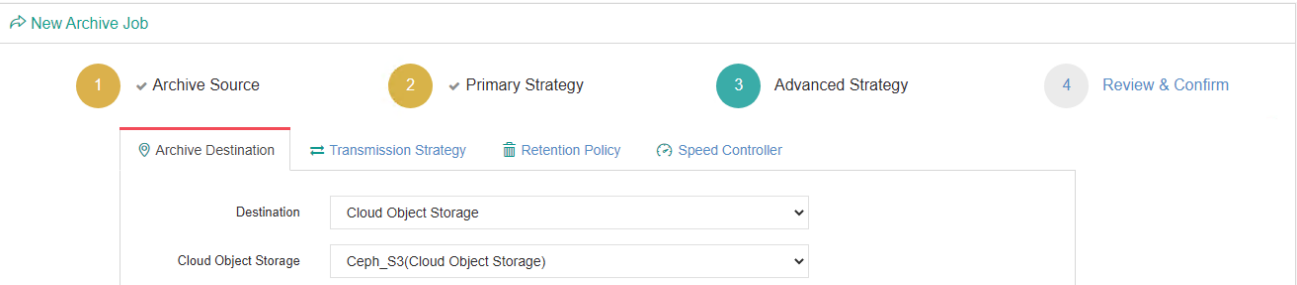
Each of the further archive jobs will always archive a latest full backup restore point to the backup archive storage.

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 AWS S3, Ceph S3, MS Azure Blob, Alibaba, Wasabi cloud storage, etc.

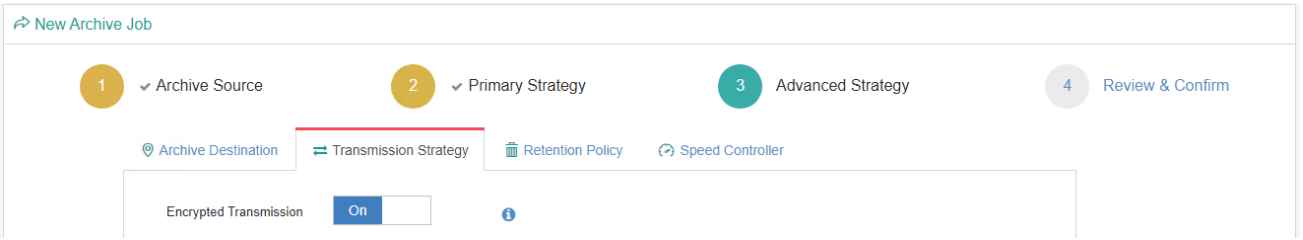
Please select the corresponding storage destination as per your actual deployment and requirements, here we take Ceph S3 object storage as an example.



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

➢ Transmission Strategy

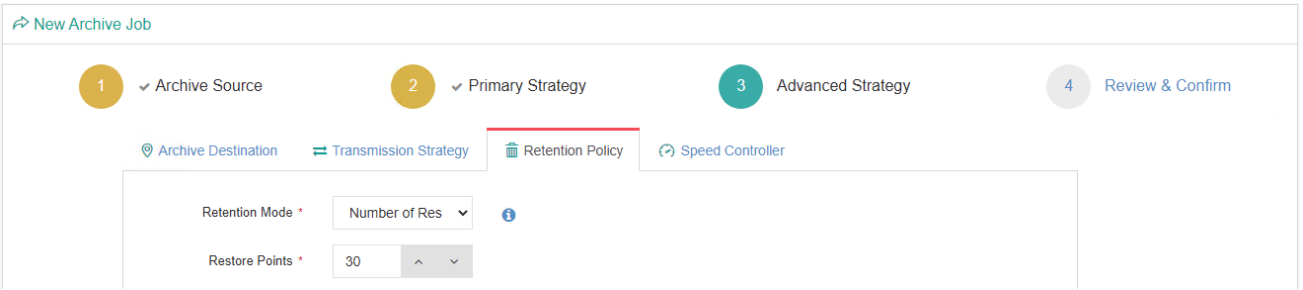
Transmission strategy including Encrypted Transmission and Compressed Transfer.



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

➢ Retention Policy

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



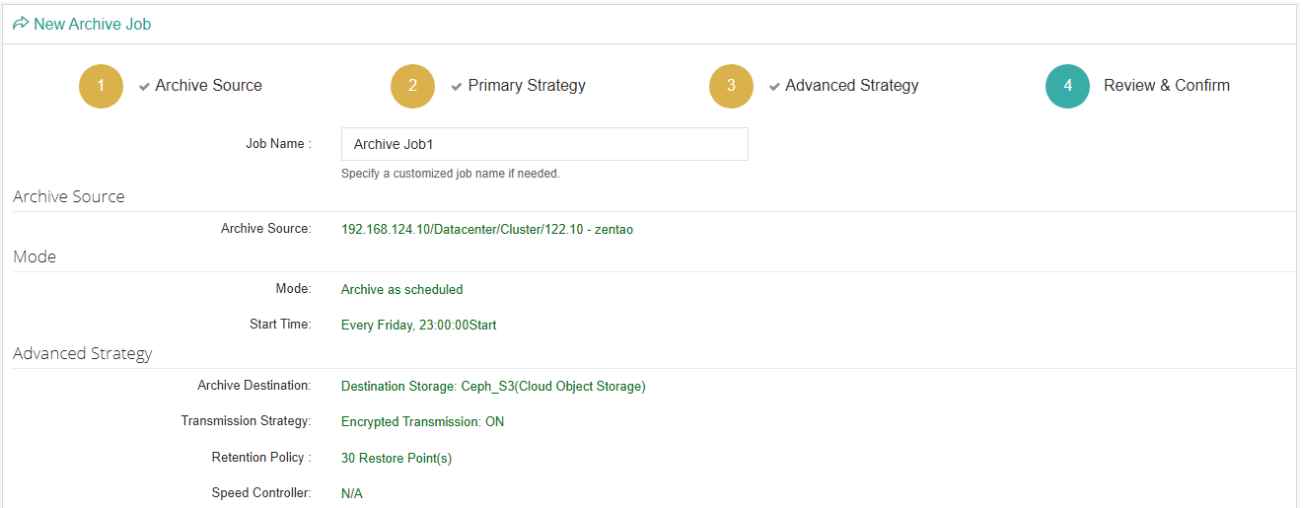
For example, if the number of restore points is configured as 30, there will always be 30 full backup restore points stored in the backup archive storage.

➢ Speed Controller

The speed controller settings are optional, only if the backup archive jobs will bring network or I/O overload to your production environment, you need to configure the speed controller accordingly.

Step 4: Review & Confirm

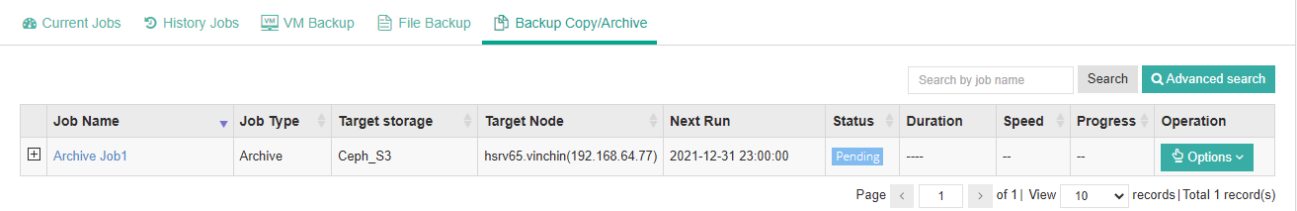
After completing the above settings, you are able to review and confirm the settings.



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

Archive Job 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.

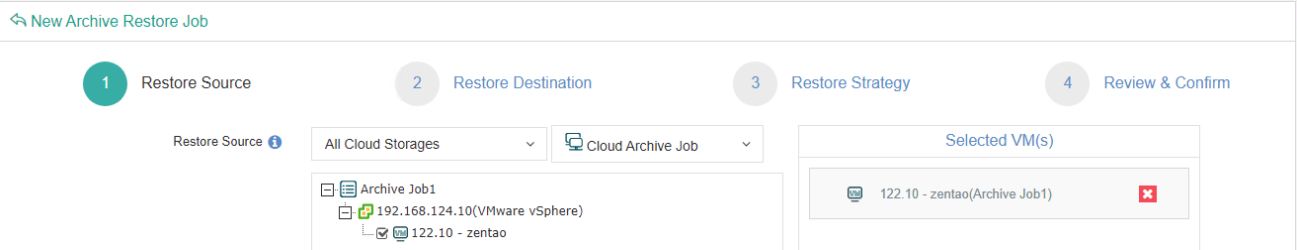
Archive Restore

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 an 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).



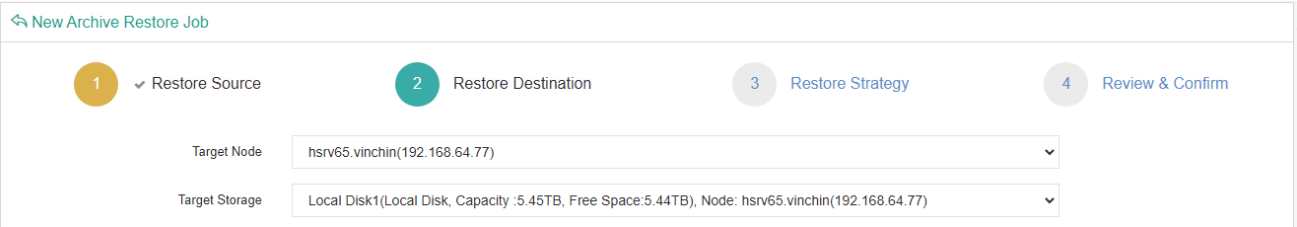
Click on **Next** to continue.

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.

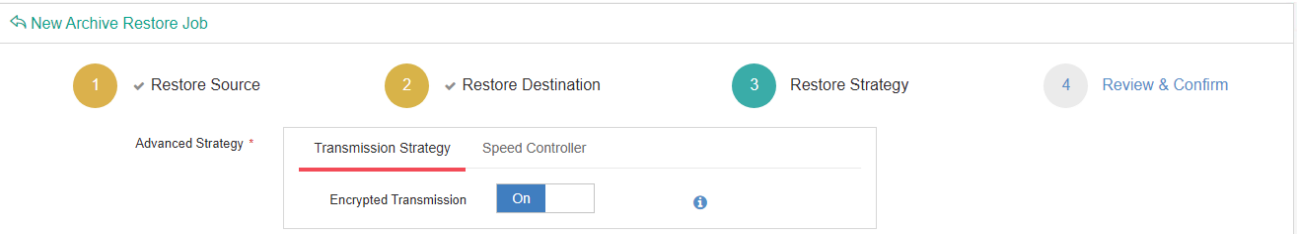
Step 2: Restore Destination

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.

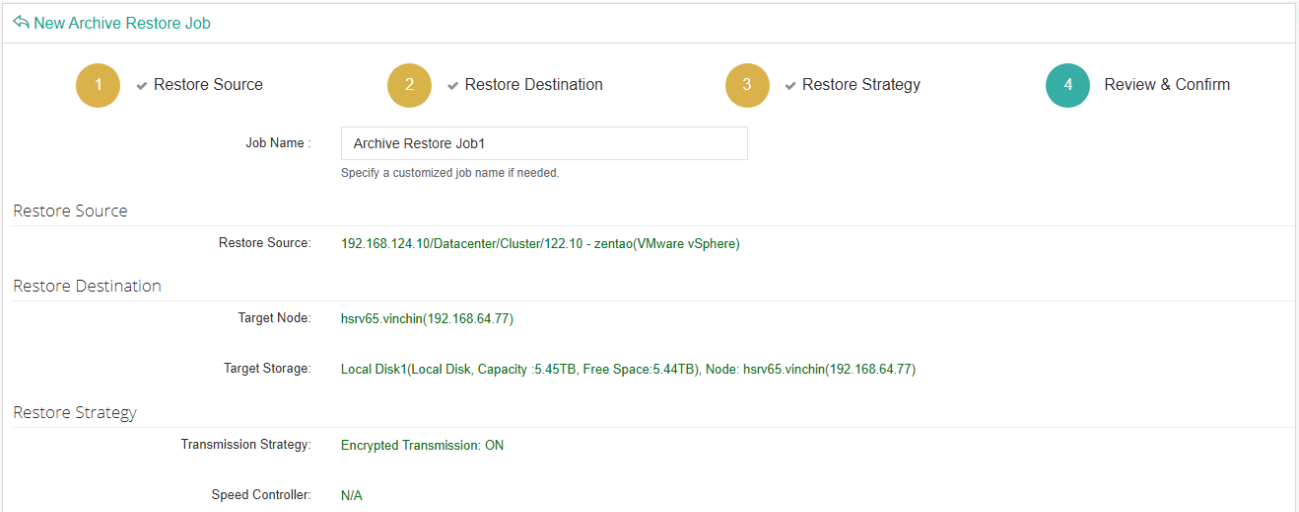


Encrypted Transmission: The archive data transmitted from cloud storage to on-site storage will be encrypted to ensure the safety of the data transmission.

Speed Controller: The speed controller settings are optional, only if the archive restore job will bring network or I/O overload to your production environment, you need to configure the speed controller accordingly.

Step 4: Review & Confirm

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



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

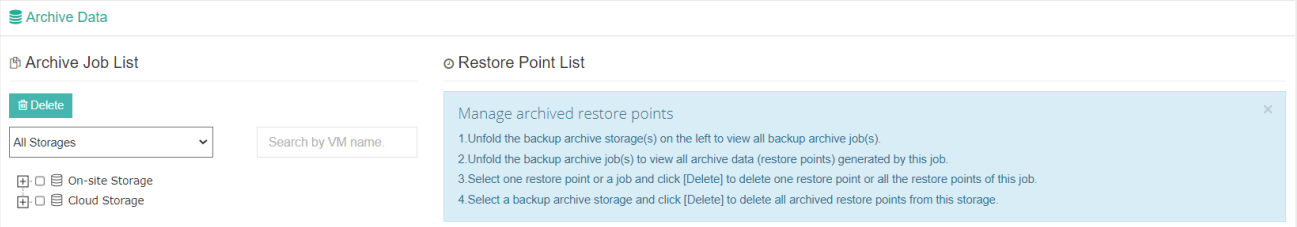
After a new archive restore job has been created, you will be redirected to the **Monitor Center** > **Jobs** page, and you will immediately see the archive restore job run automatically.

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.

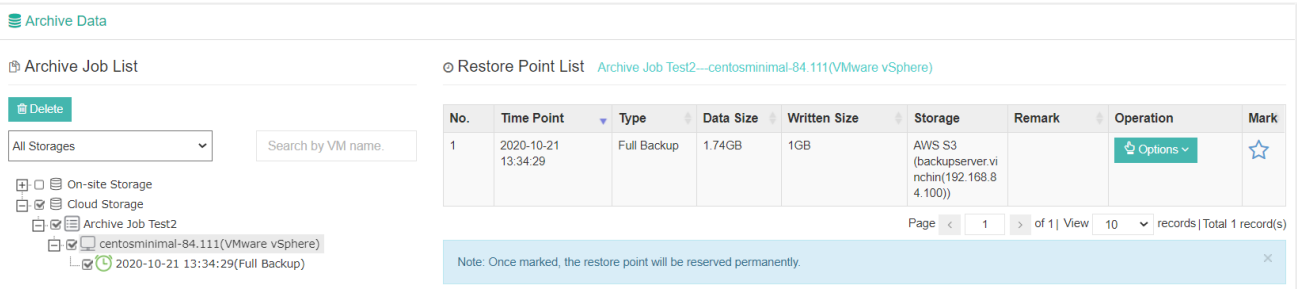
Archive Data

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.



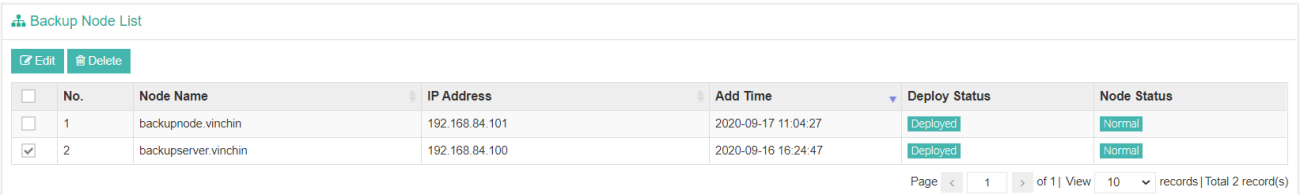
By clicking on Options, you will be able to remark or delete the restore point.

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

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

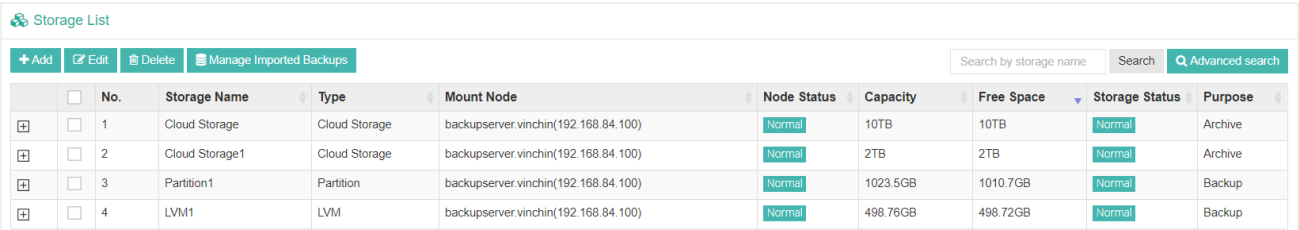
The storages for Backup, Backup Copy and Backup Archive can be added and managed from the **Resources** > **Storage** page.

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 Fibre Channel, iSCSI and NFS for LAN-Free backup and restore through the SAN (Storage Area Network).

If you want to implement LAN-Free backup and restore, Vinchin Backup Server needs to meet the following requirements:

- Vinchin Backup Server is installed on a dedicated physical server.
- For fibre channel SAN, the physical server needs a fibre channel HBA (Host Bus Adaptor) interface card to be able to connect to the fibre channel SAN via the FC switch.
- For iSCSI and NFS (IP SAN), the physical server needs an extra NIC to be able to connect to the storage area network via the storage network switch.
- LAN-Free path needs to be configured.

To add LAN-Free path, please follow the instructions below.

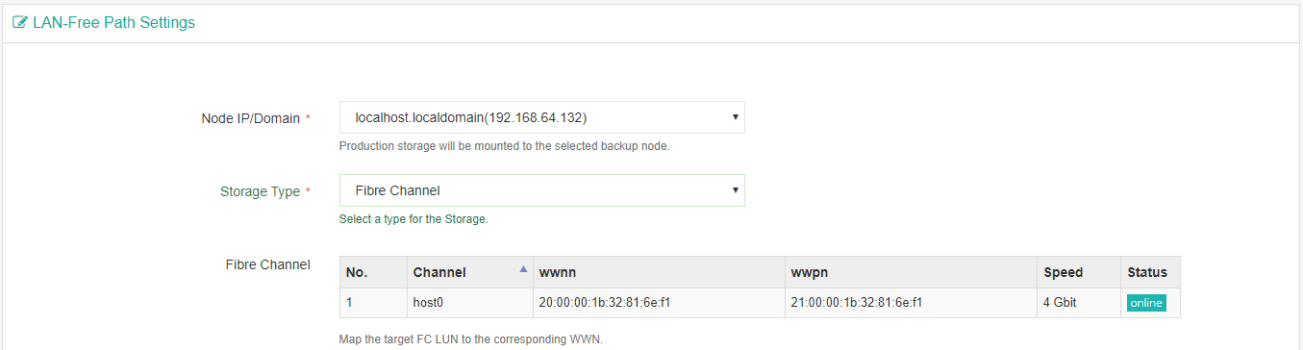
Note

1. LAN-Free backup and restore is not supported with Microsoft Hyper-V and Sangfor HCI in Vinchin Backup & Recovery version v6.5.

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

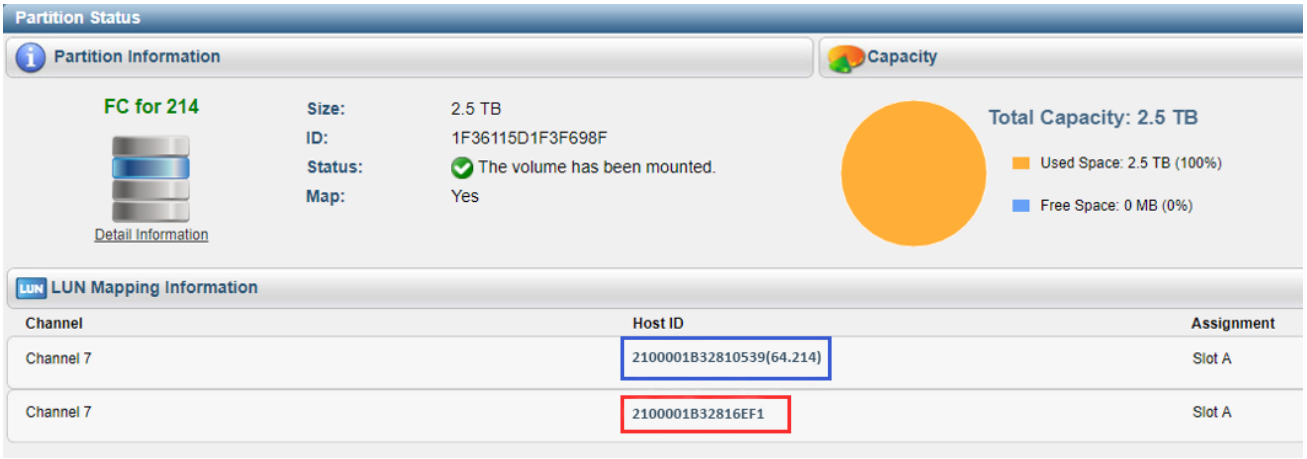
➢ Fibre Channel

From Vinchin Backup Server web interface, on the **Resources** > **LAN-Free** page, click on **Add** button to add a fibre



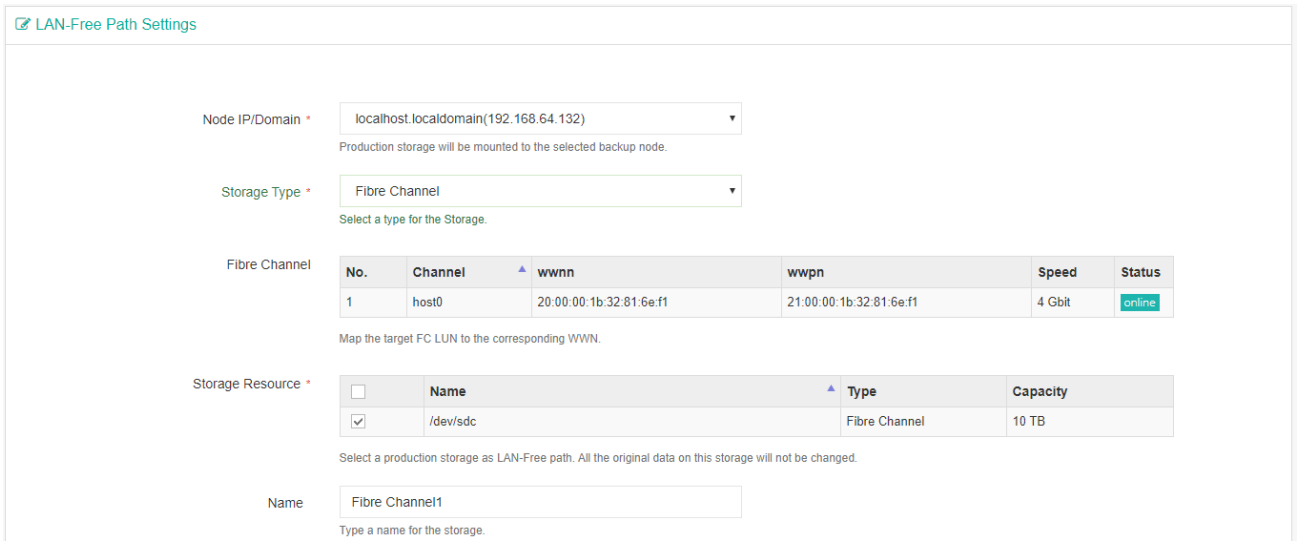
channel storage, in the **Storage Type** field, please select **Fibre Channel**.

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



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

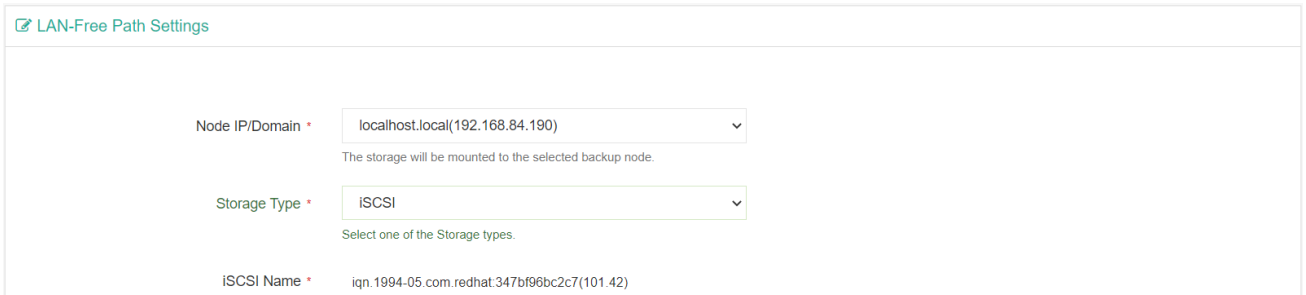
Add the fibre channel again, Vinchin Backup Server will recognize the LUN which is mapped to it, and the storage will be able to be added to Vinchin Backup Server as LAN-Free path.



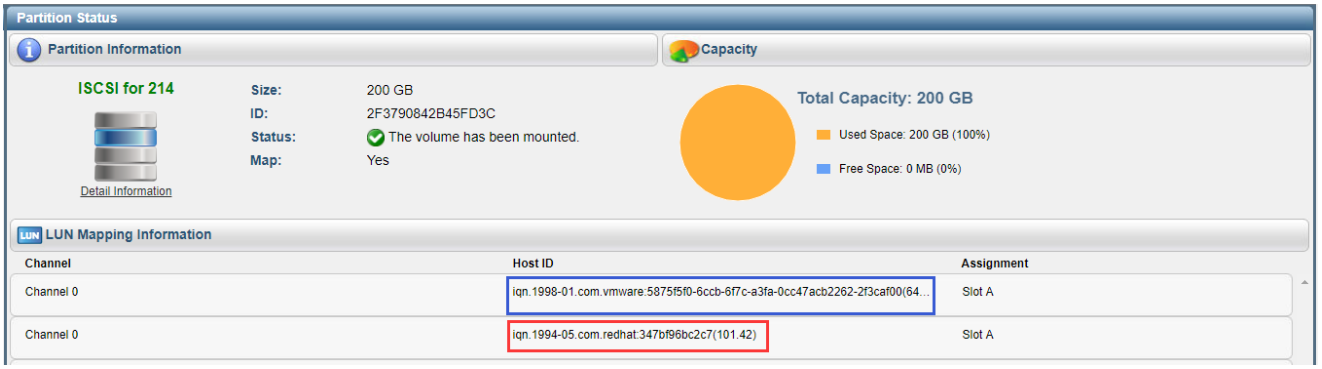
Select the production storage and click OK to add it to the LAN-Free Path List.

➢ iSCSI

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



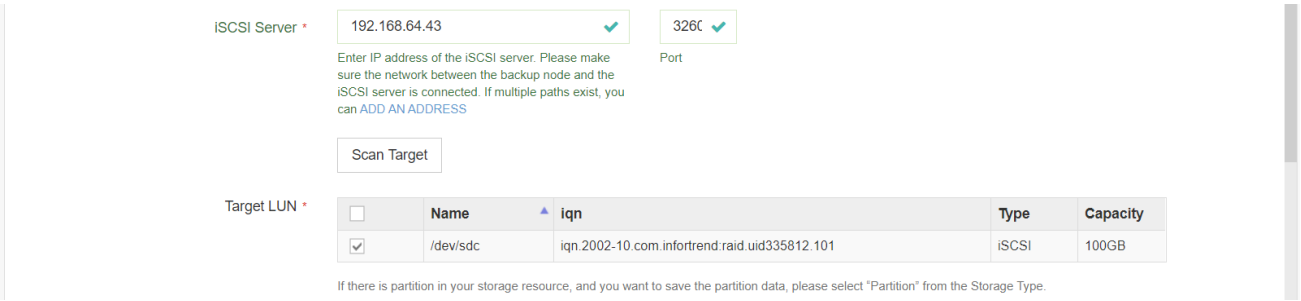
Please use the IQN to map the LUN of the production storage to the backup server from the storage server management interface.



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

After this, add the iSCSI storage again, and input the storage server IP address in the iSCSI Server field and click on **Scan Target** button to scan the target storage.

The system will discover the production LUN storage which is mapped to Vinchin backup server, and the storage will be able to be added to Vinchin Backup Server as LAN-Free path.

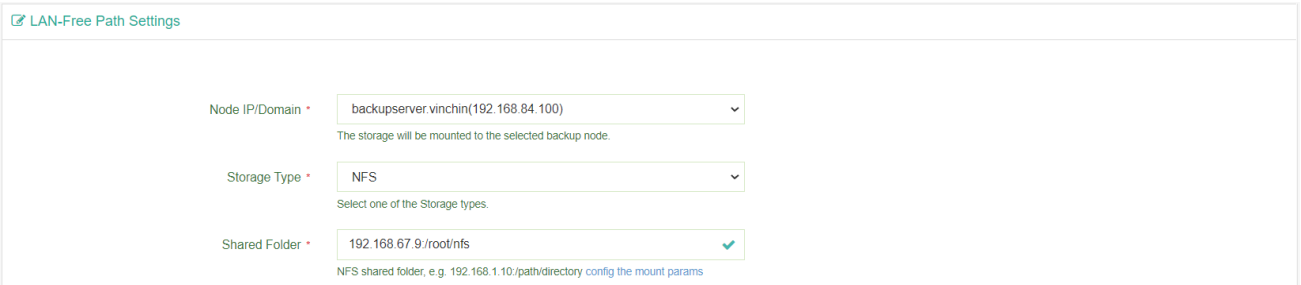


Select the production storage and click OK to add it to the LAN-Free Path List.

➢ NFS Storage

If the production system uses NFS shared storage as the production storage, the NFS storage can be added to Vinchin Backup Server as LAN-Free path.

From Vinchin Backup Server web interface, on the **Resources** > **LAN-Free** page, click on **Add** button to add an iSCSI storage, in the **Storage Type** field, please select **NFS**.



In the **Shared Folder** field, simply type in the path of the NFS production storage to add it to Vinchin Backup Server as LAN-Free path.

After adding the LAN-Free path, while creating a backup/restore job, the transmission strategy should select SAN (LAN-Free).

Warning

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

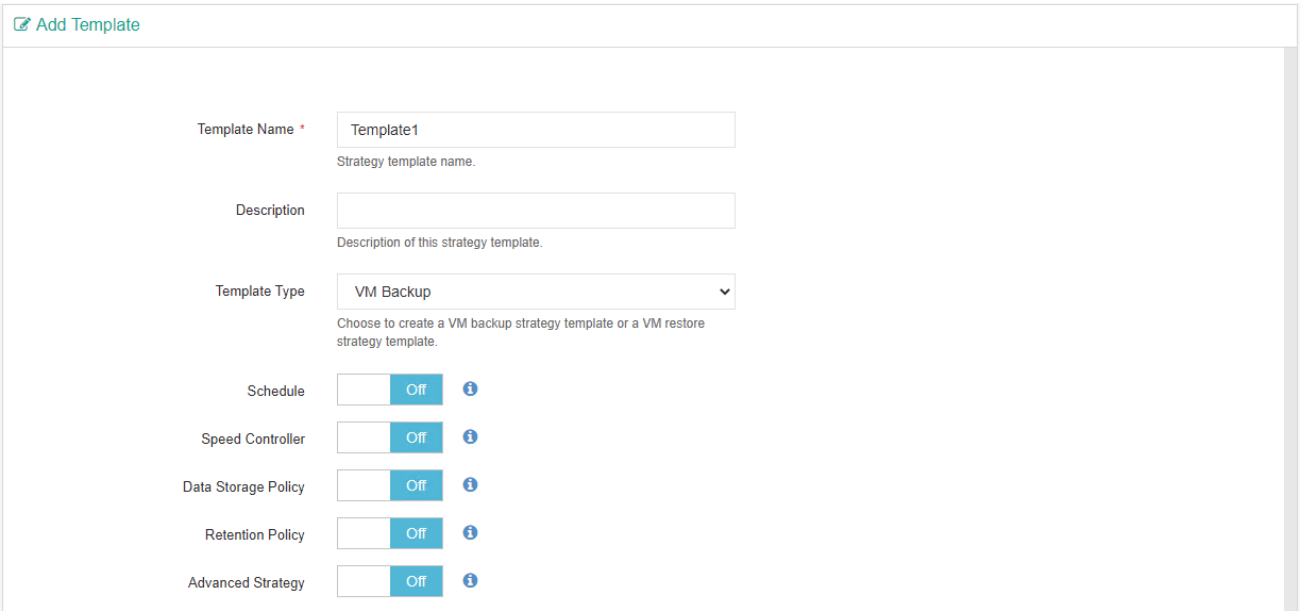
formatted, all the production data will be erased.

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 Templates

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.

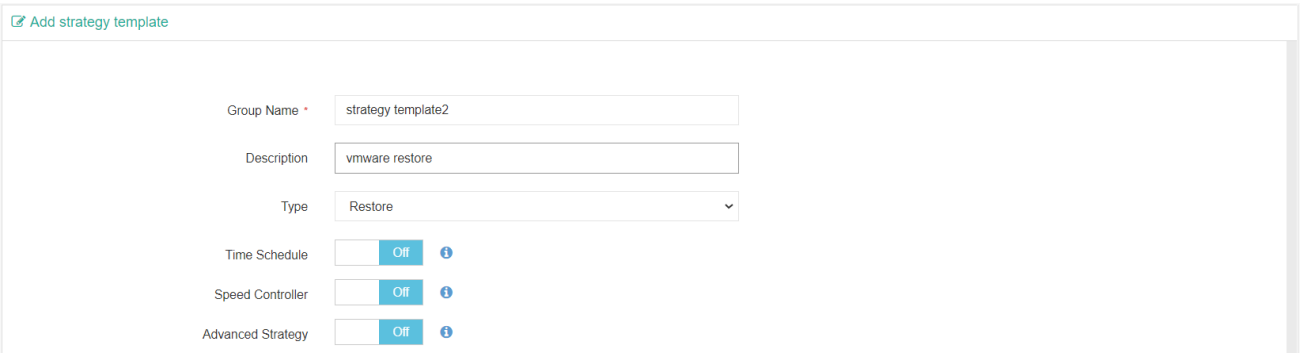


In the **Group Name** field, you can define a name for this template, and in the **Description** field you can optionally add some descriptions of this template.

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

For the **Schedule**, **Speed Controller**, **Data Storage Policy**, **Retention Policy** and **Advanced Strategy**, you can optionally enable and configure some of those settings in this template, the settings which are not enabled and configured in this template, when you creating a backup job and select this template, those un-configured settings will be given with system default settings.

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.

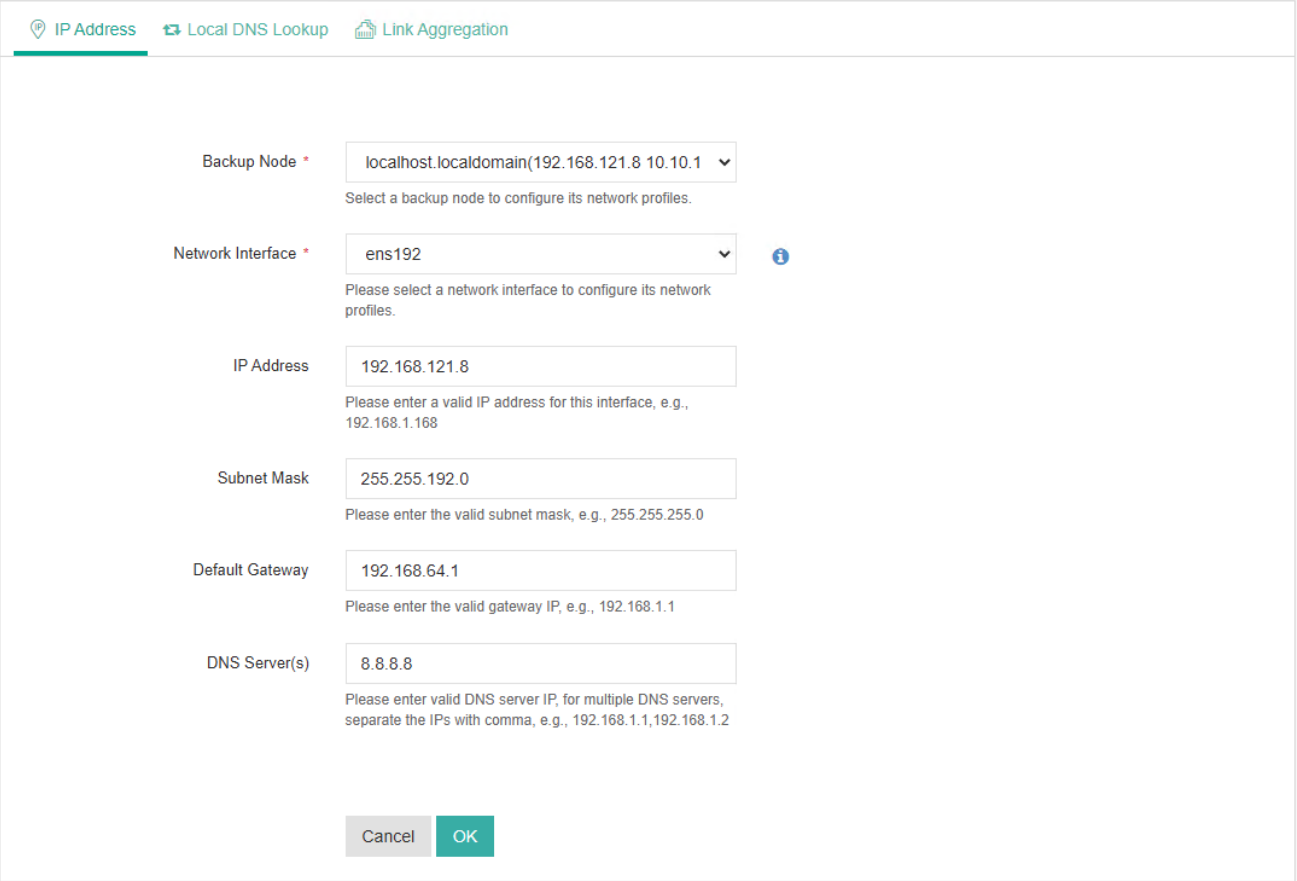
System

System Settings

Network Settings

IP Address

The network profile of Vinchin Backup Server should be well configured during the installation process. If modifications are required, you can do it from **System** > **System Settings** > **Network Settings** page.



From the **Backup Node** dropdown list, you can select a backup node to modify its network profiles.
From the **Network Interface** dropdown list, you can select a network interface to set its network profiles.
And the below settings including IP address, subnet mask, default gateway and DNS server.

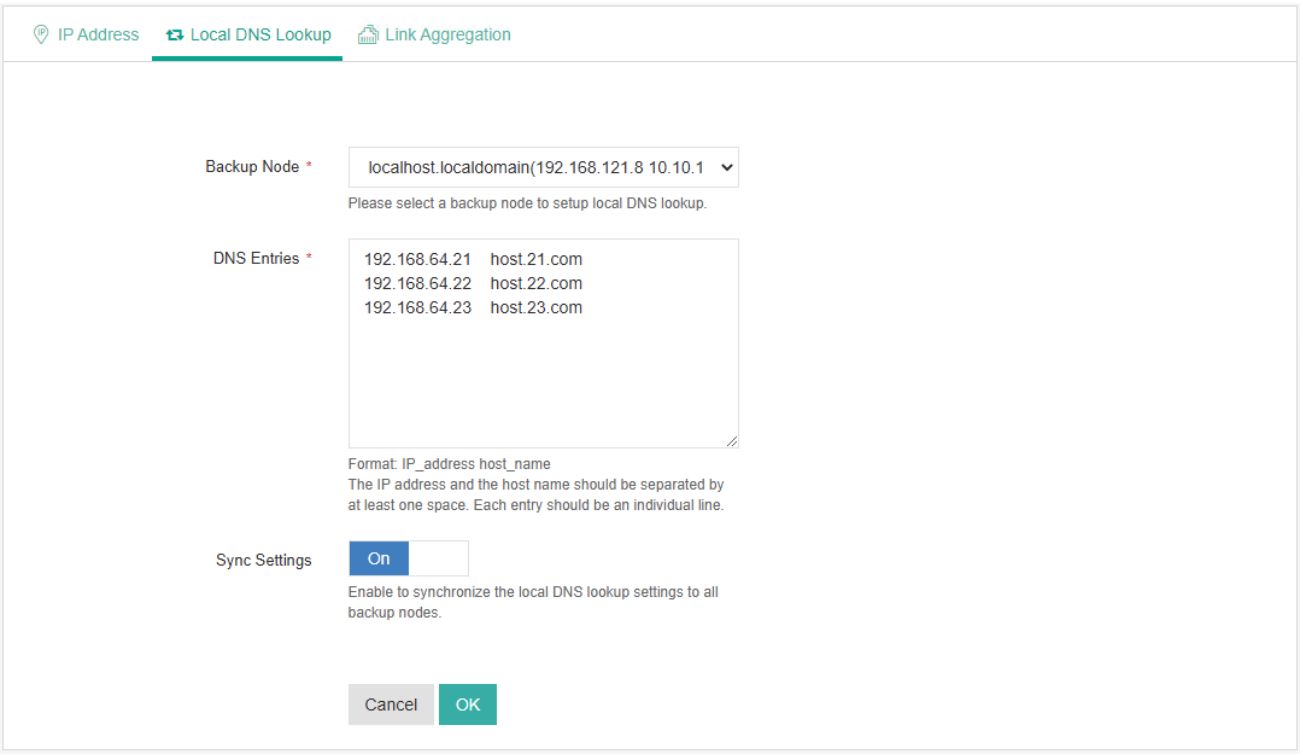
Warning

1. If the IP address of the backup server had been changed, please type in the new IP address in the browser address bar to reopen the backup server web console.

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

Local DNS Lookup

If an ESXi host was added to the vCenter via its domain name, then this ESXi host's corresponding domain name needs to be configured in the Vinchin backup server, so that Vinchin backup server will be able to communicate with the ESXi hosts. Otherwise, the VM backup jobs will fail.



First fill in the IP address of the ESXi host and its domain name separated with a space. If there are multiple ESXi hosts, please fill in the DNS records in different lines. After this please click OK to save.

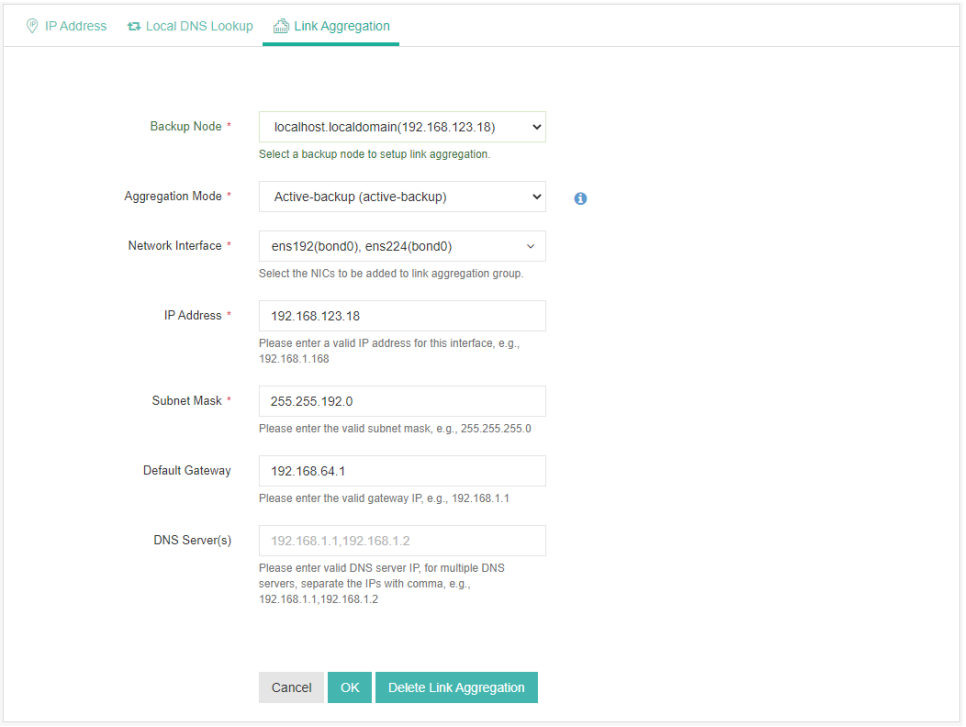
If you have deployed backup node(s) to Vinchin Backup Server, please enable DNS Sync option, so you don't have to configure DNS settings for each node separately.

Link Aggregation

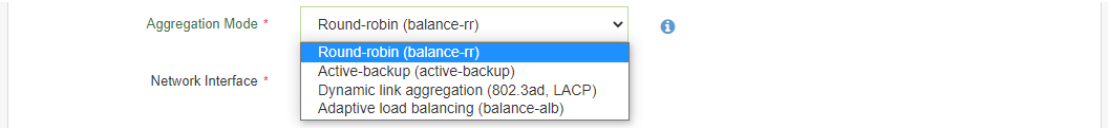
Link aggregation is the combining (aggregating) of multiple network connections in parallel by any of several methods, in order to increase network throughput or provide redundancy of the network links.

Link aggregation is optional, if you want to setup link aggregation group, your Vinchin backup server or node must have multiple network interfaces available.

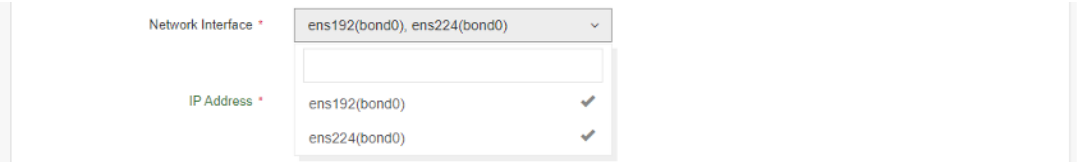
In **Backup Node** dropdown list, you should select a node on which you wish to setup link aggregation.



There are 4 aggregation mode: **Round-robin(balance-rr)**, **Active-backup (active-backup)**, **Dynamic link aggregation (802.3ad, LACP)** and **Adaptive load balancing (balance-alb)**. Please select the desired mode which suits your requirement.



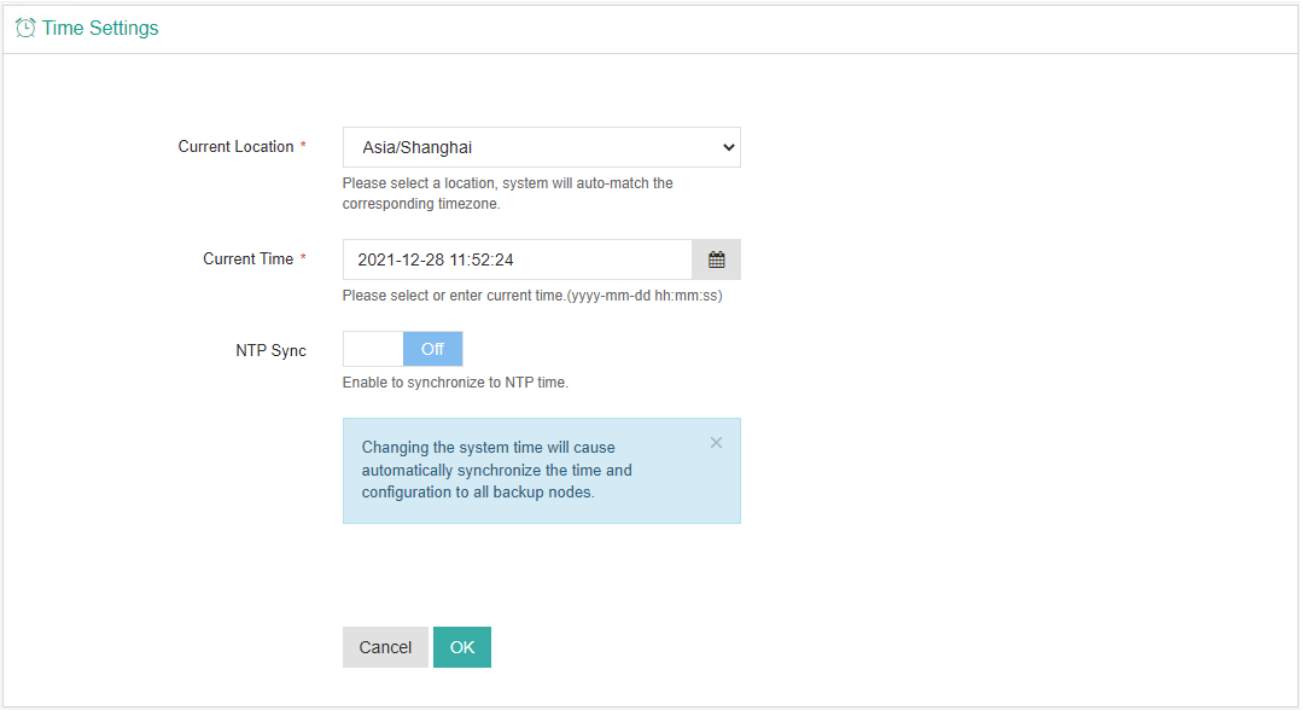
In Network Interface dropdown list, select the network interfaces which you wish to add to the link aggregation group.



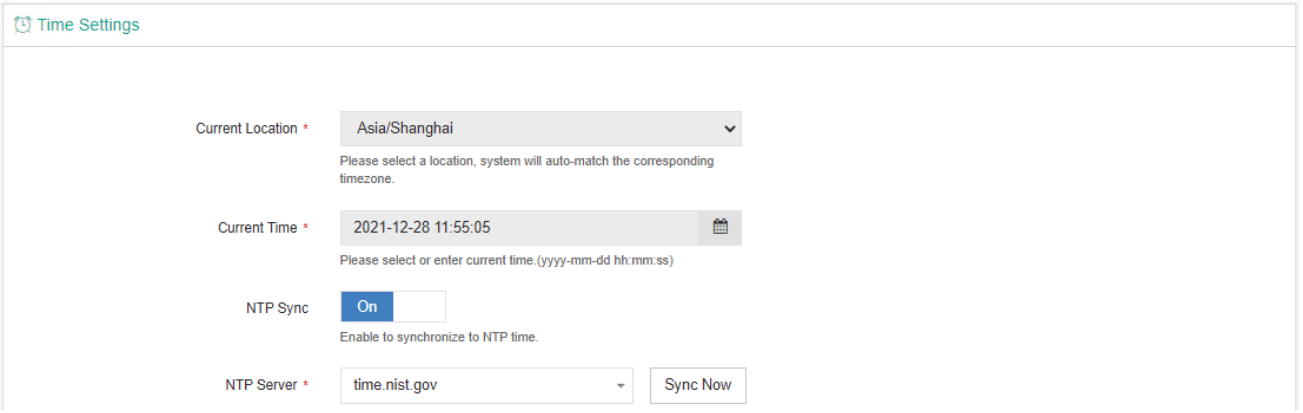
Fill the rest fields, click on OK, the network services will restart, please be patient to wait the link aggregation complete.

Time Settings

The time settings should have been done during the installation of Vinchin Backup Server, but if you want to modify the time settings, for example, set the system to use manual time or NTP time can be done from **System > System Settings > Time Settings**.



In the **Time Zone** field, you should select the correct time zone that you are located in. And if you want to set a manual time, you can select from the calendar or manually input the current time in the **Manual Time** field.
If you want to synchronize the current time from an NTP server, please enable **NTP Time**, and then specify a desired NTP server address in the **NTP Server** field, after this click on the **Sync Now** button to obtain time from the specified NTP server, or you can click on OK button to save the settings and do the time synchronization.

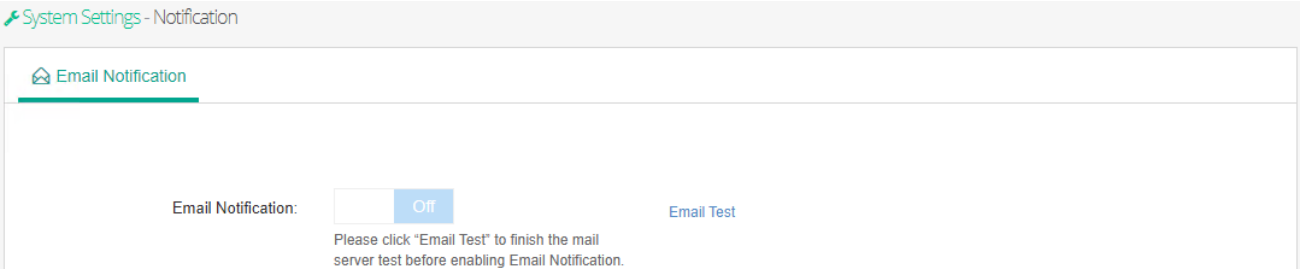


Warning

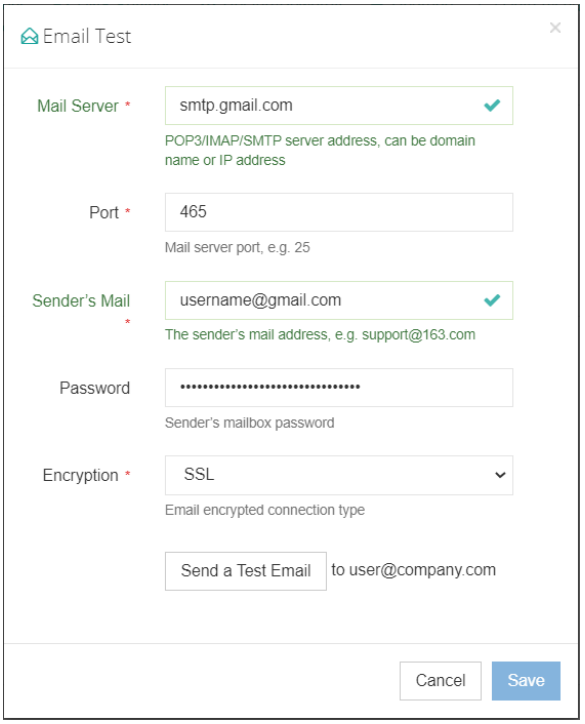
Please make sure the time settings are correct and accurate, as if you had deployed backup node(s), the time settings will be automatically synchronized to all backup nodes connected to this backup server, and as a result, all the scheduled job will run based on the current backup server time.

Notifications

Email Notifications can be enabled to send various kinds of notifications and reports of Vinchin backup server to the administrator and other recipients for users to be informed of the running status of Vinchin backup services.



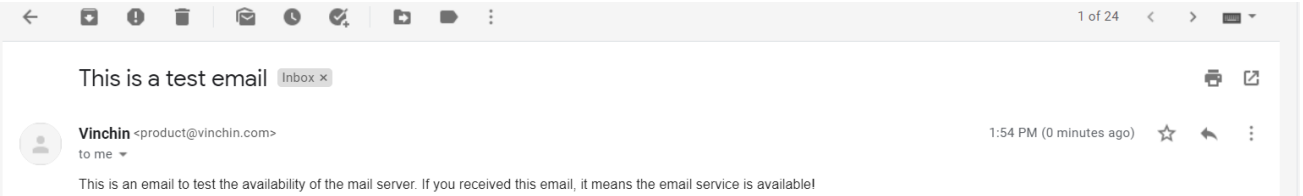
To enable email notification, first make sure you had specified an Email address from **admin** > **My Information**, then click on Email Test to complete the mail server settings.



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.

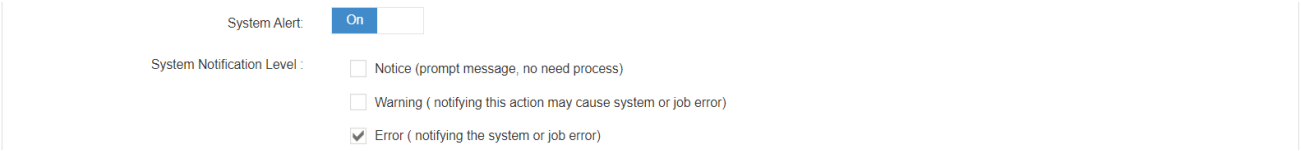
In the above example, Gmail SMTP is used as the outgoing mail server. The **Mail server** should be smtp.gmail.com, **Encryption** should be SSL or TLS, the **Port** number should be 465 or 587, and you must configure a mail account here as the sender. After this, you can click on **Send a Test Email** 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.



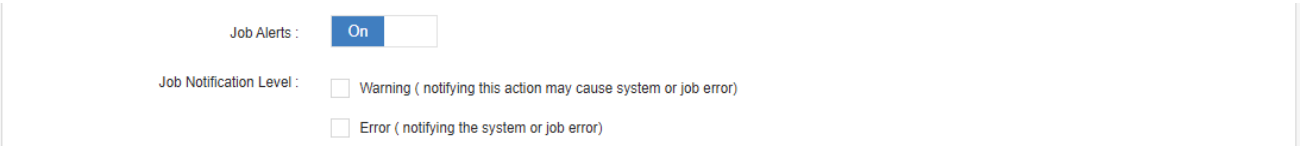
After you had received the test email please save the mail service settings, then you are able to enable Email notification. Once enabled, you are able to configure how the notifications to be sent.

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.

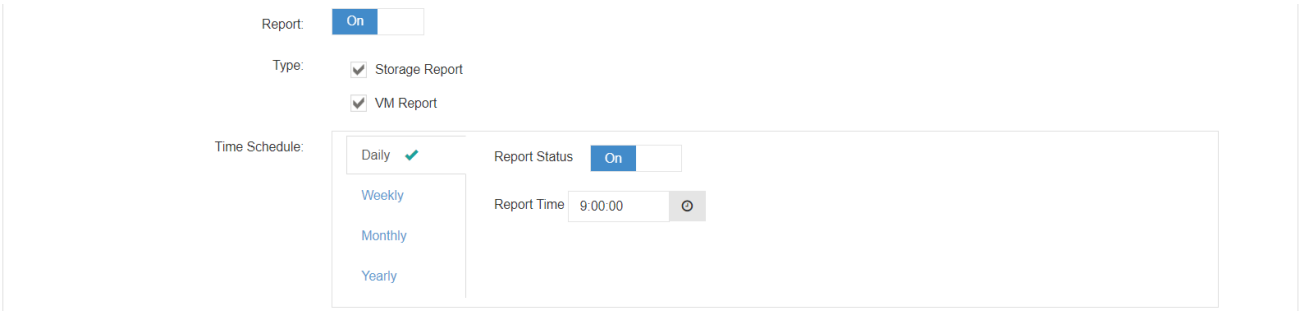


It is recommended to enable sending critical system level notifications, as users don't have to pay much attention on the system level notices.

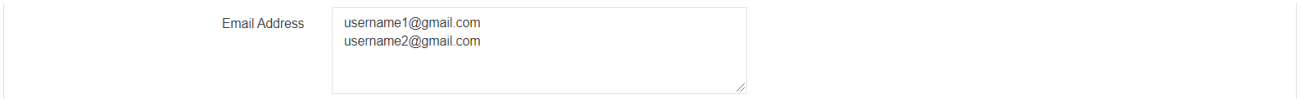
The Job Alert can be enabled to send backup/restore job level notifications, including job success notices, warnings or errors of the jobs.



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.



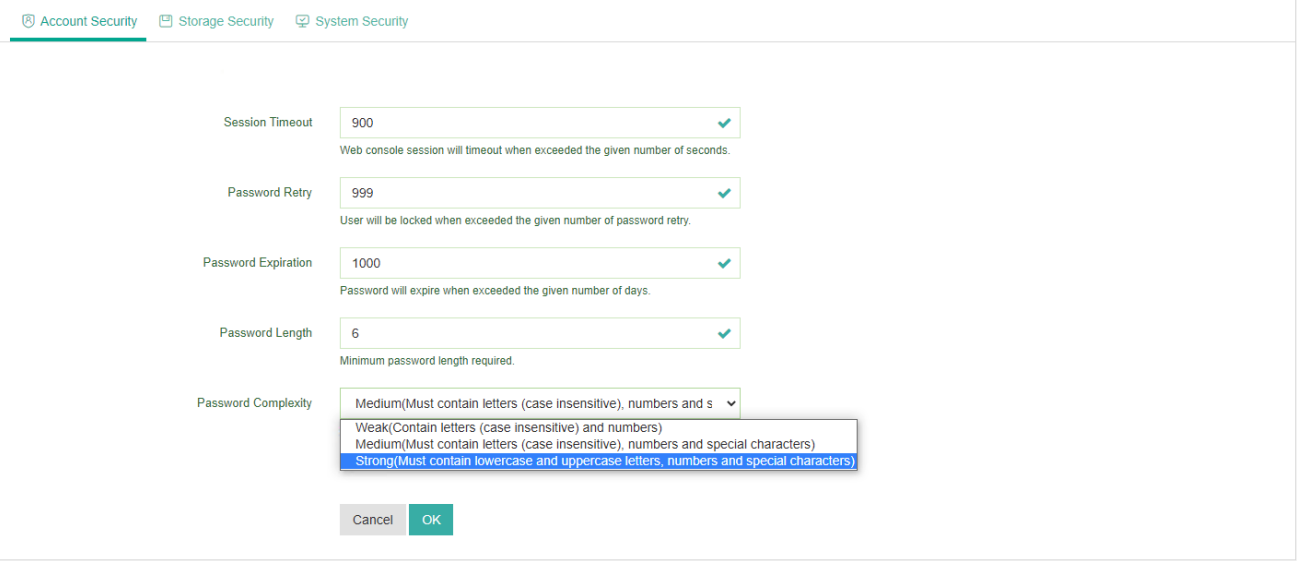
The system alerts and reports will be sent to the system administrator by default. The job alerts will be sent to the creator by default. The newly added recipient will receive all the enabled notifications.

Security Settings

From **System > System Settings > Security Settings** page, admin user can configure **Account Security**, **Storage Security** and **System Security** settings.

Account Security

Account security settings define some global user account configurations, including Vinchin backup server web console session timeout, max password retry, password expiration time, minimum password length and password complexity settings.



The **Session Timeout** option determines when the web console session will expire due to inactive user activity.

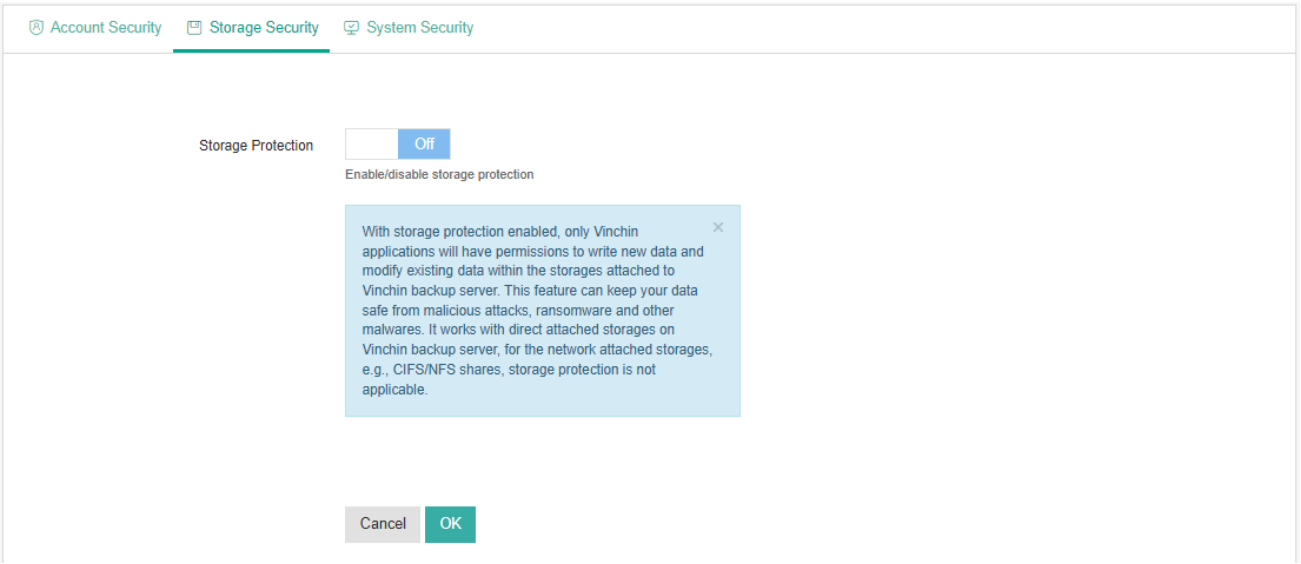
Password Retry options determines the max password retry allowed before a user account is locked. Once a user account is locked, admin user needs to unlock this user account from **System > User Management > Users** page (admin user will not be locked).

Password Expiration option determines how long the user account password expires, when the password is about to expire, user will receive popup notification on the web console, when password is expired, user will be redirected to the change password screen to change password and re-login.

For the **Password Length** and **Password Complexity**, these 2 options determine the minimum password length and the password complexity rule.

Storage Security

Under **Storage Security** tab, you are able to enable **Storage Protection** which can effectively protect your backup data stored in the backup storage.



By default, storage protection is disabled, when enabled, only Vinchin applications are allowed to modify the backup data saved in the backup storages attached to Vinchin backup server/node. And as a result, it can protect your backup data against ransomware and other malwares from modifying your backup data.

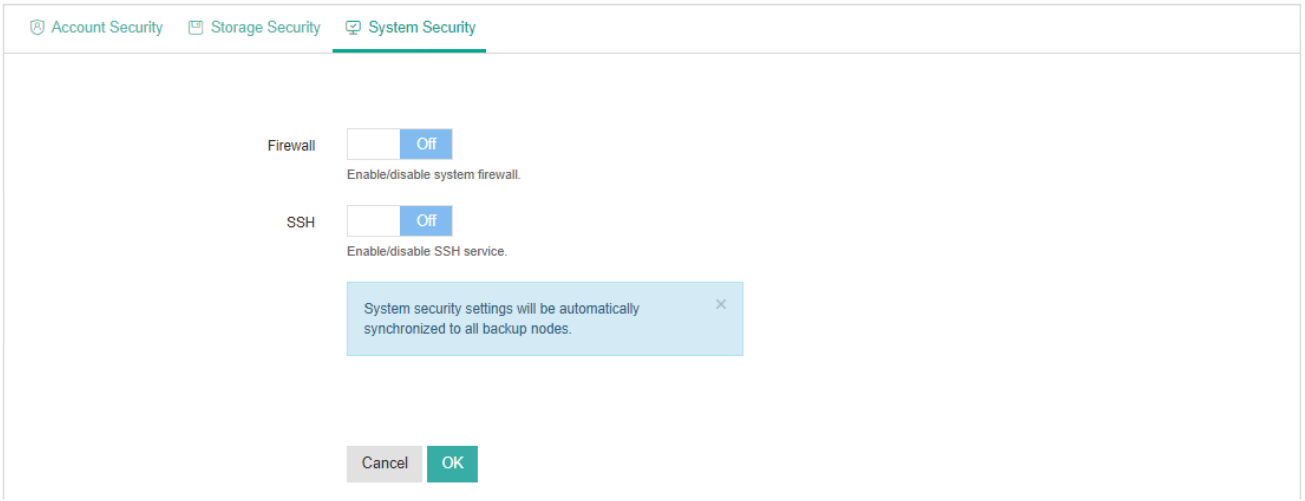
Note

1. Before upgrading Vinchin software, please temporarily disable Storage Protection, otherwise, software upgrade will fail. After upgrading, please turn it back on.

2. To guarantee Storage Protection always works, the backup storage of Vinchin backup server must be exclusive block devices, like local disks, disk partitions, logical volumes, fibre channel LUNs and iSCSI LUNs, for other file storages, Storage Protection might not work, because ransomware and other malwares might access your backup data by-passing Vinchin backup server.

System Security

Under System Security tab, you are able to turn Vinchin backup server firewall and SSH services on or off.

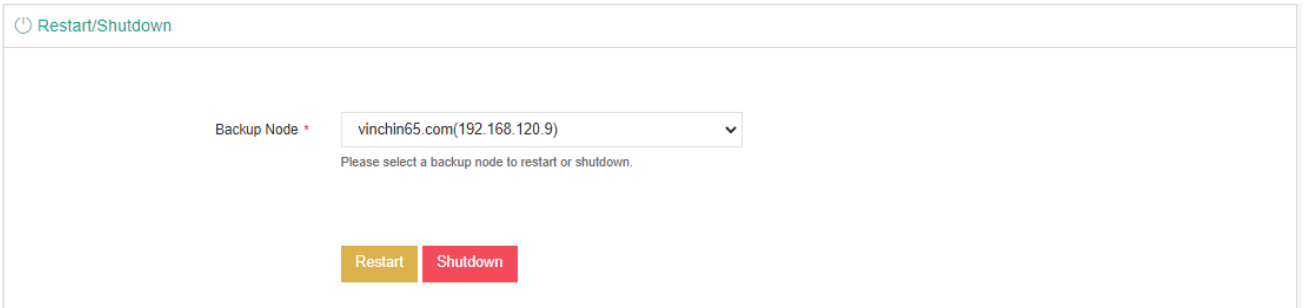


Vinchin backup server has some built-in security rules configured with the system firewall, it can be enabled for system security. While it also has the necessary services enabled to ensure the functionalities of backup and restore activities.

For SSH option, it determines whether users can connect to Vinchin backup server CLI via SSH connection. It is recommended to disable this option when SSH access to Vinchin backup server CLI is not needed.

Restart & Shutdown

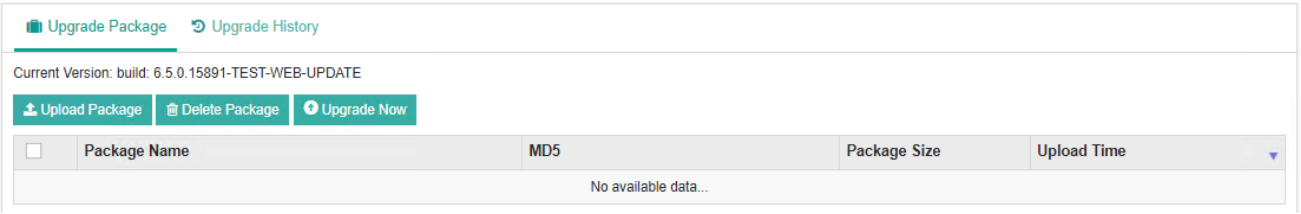
Restart and Shutdown functionalities can be used for the backup server or backup node(s) maintenance or some other circumstances which require system restart or power off.



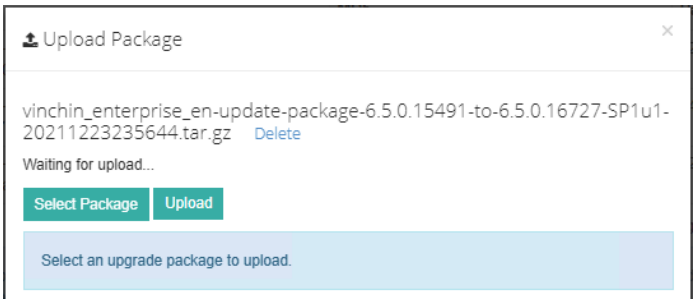
You can select the target node then click on Restart or Shutdown button to perform the corresponding operation to the select node. Both restart and shutdown operation will terminate backup/restore jobs on the selected system, so before doing this, please make sure there's no job running on the selected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

Upgrade

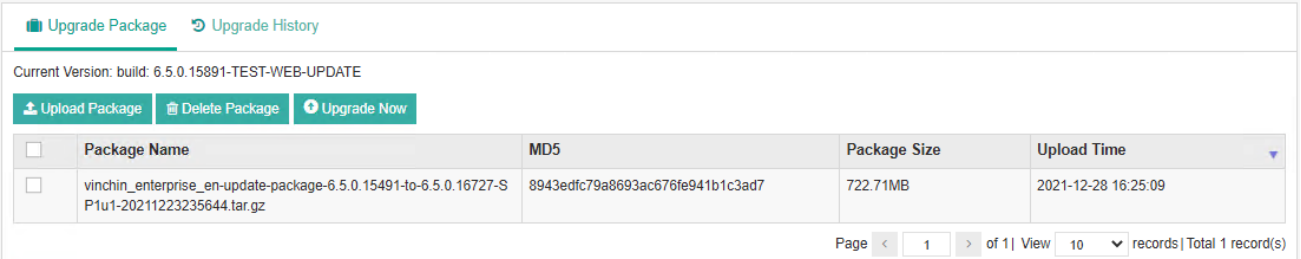
When new software or patch upgrade for Vinchin Backup Server or Backup Node is required, you can upload and upgrade Vinchin backup server or backup node from here.



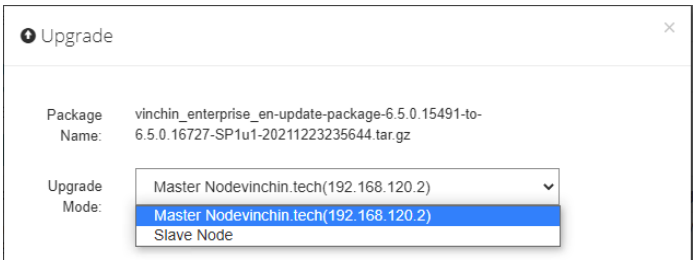
To upload a software package, please click on **Upload Package** button. In the popup dialog, click on Select Package to locate the software package.



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



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



In the popup dialog, select the backup node and click on OK to upgrade. Please make sure you first upgrade the backup server (master node) then upgrade the backup node (slave node).

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

Note

Software upgrade will require service restart, please make sure there're not jobs running on the backup server or backup node before upgrading.

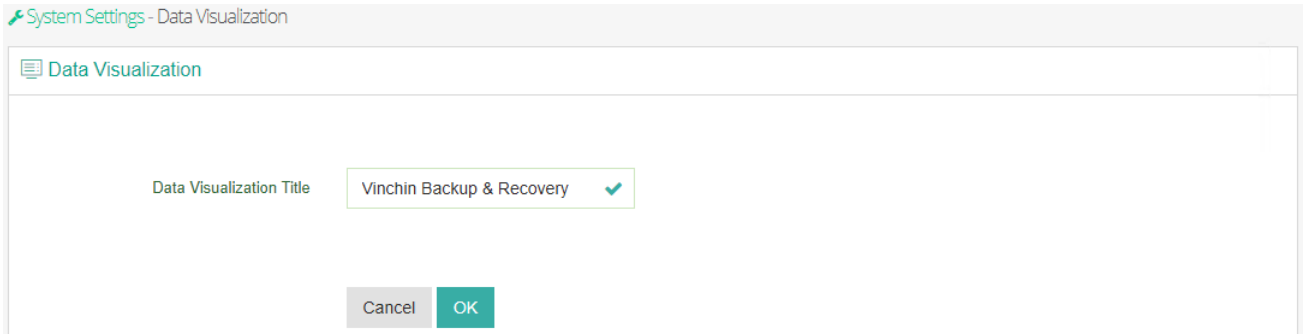
Data Visualization

Data visualization is a value-added feature which is available in Vinchin Backup & Recovery Enterprise edition, it briefly presents the real-time status and 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.

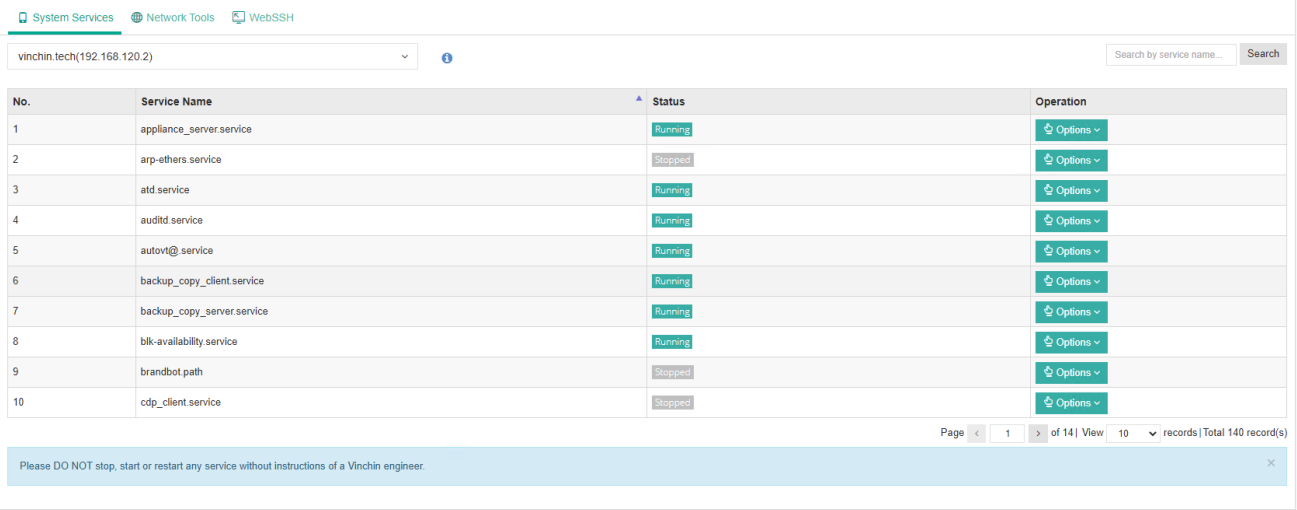
Users can customize the data visualization project name from the **System** > **System Settings** > **Data Visualization** page.



System Tools

System Services

Service management can be used to check the backup server or backup node system service status and you can start, stop or restart the services.



In the dropdown list, you can select from Vinchin Backup Server and the backup nodes registered to the backup server to check the service status and perform operations to the services. And you can search specific services by service name.

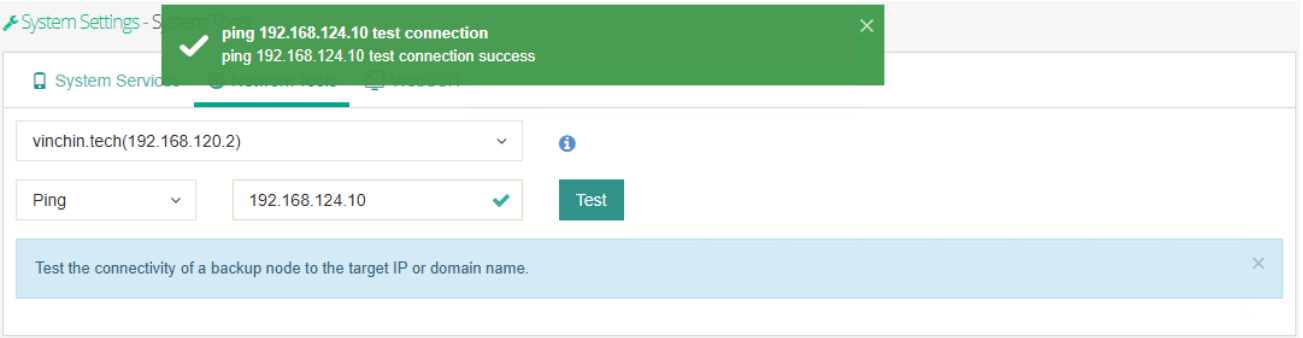
Warning

Service management is used for maintenance only, please DO NOT start/stop/restart any of the system services without the advice of a Vinchin engineer, otherwise your backup infrastructure may malfunction.

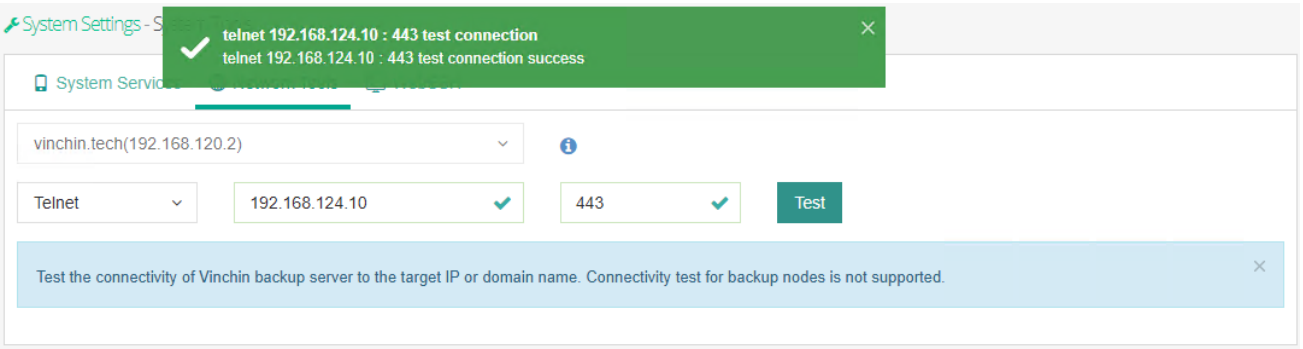
Network Tools

Network tools can be used to exam and troubleshoot the connectivity of each backup server/node with the target IP network.

Ping test can be used to test the reachability from the selected backup node to a specific IP address.

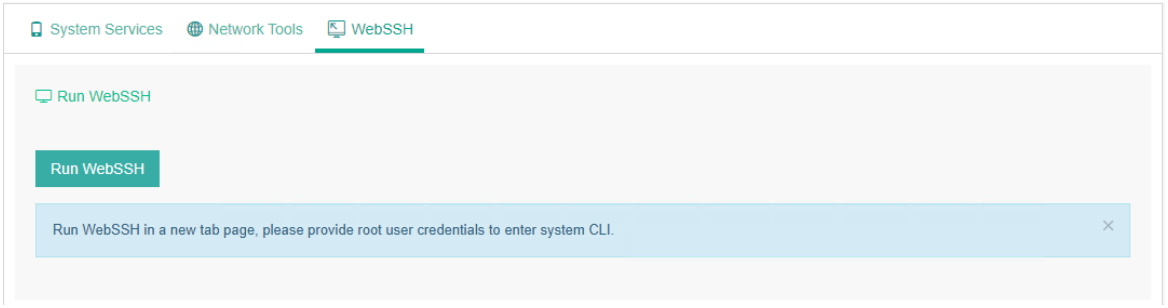


Telnet can only test the connectivity from the backup server to a specific host IP with a service port number.

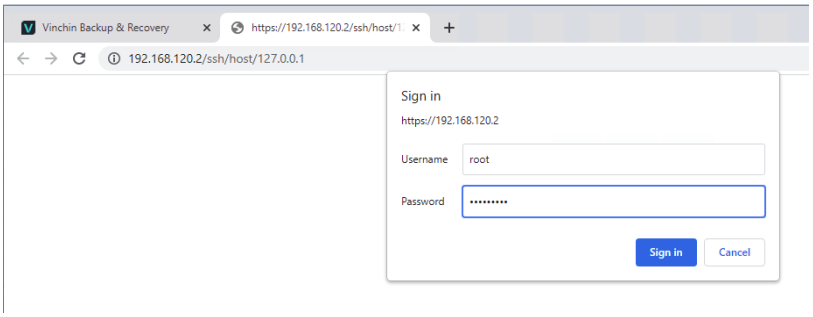


WebSSH & File Upload

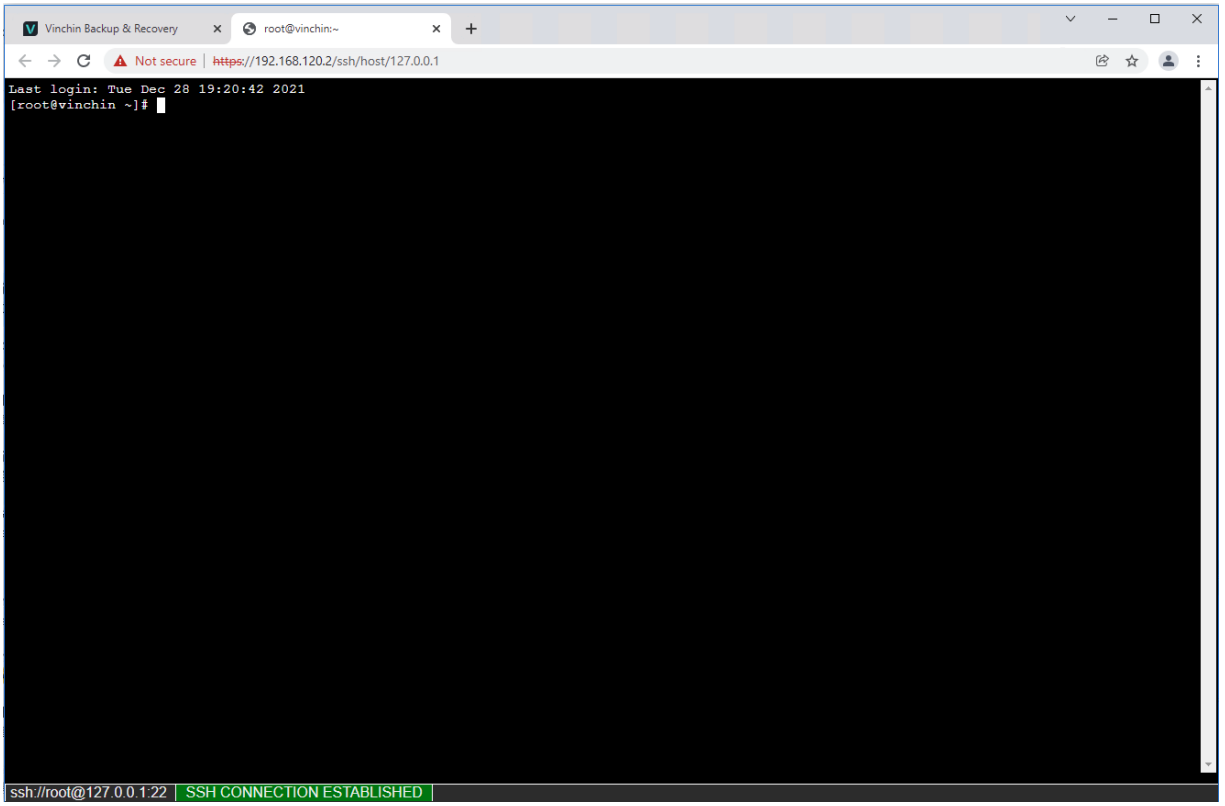
WebSSH can be used to connect to Vinchin backup server CLI directly through web browser, it is useful for server maintenance from CLI with using an additional SSH client application.



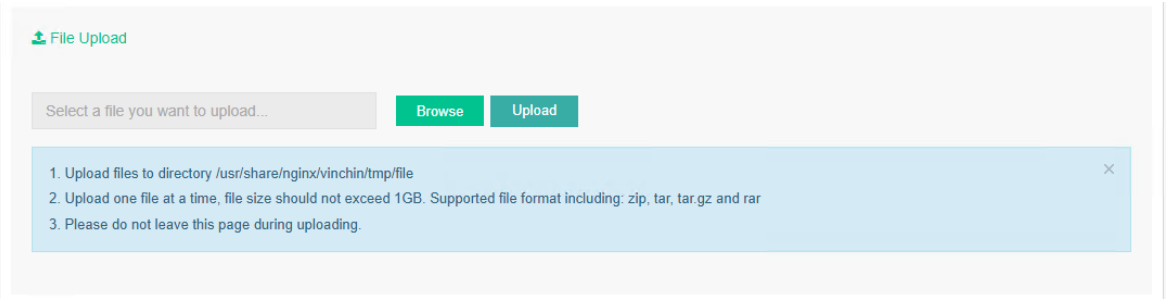
Click on the **Run WebSSH** button, a new tab page will be opened and prompting for CLI user credentials.



Simply enter the CLI user credentials and click on **Sign in** to connect to Vinchin backup server CLI. From within the WebSSH console, users are able to run commands the same way as using SSH client applications.



File upload can be used to upload certain types of files to Vinchin backup server file system without using a third-party tool.



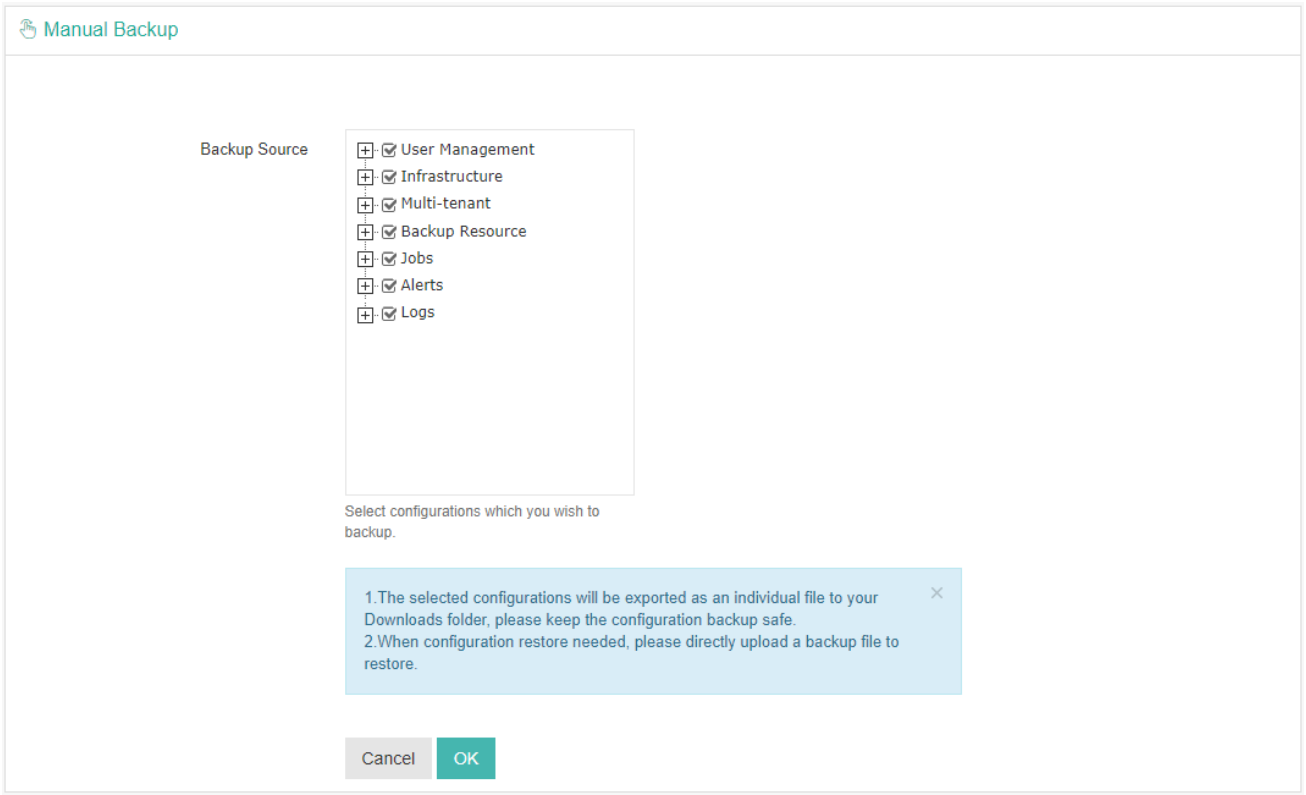
The supported file format including zip, tar, tar.gz, and rar, and the maximum file size allowed is 1GB. After uploading a file, users can find it from path /usr/share/nginx/vinchin/tmp/file/.

Configuration Backup

Configuration backup feature allows you to export the configurations of Vinchin backup server as backup files, and the backup files can be used for configuration restoration purpose upon a Vinchin server reinstallation or upon a Vinchin server configuration accidental deletion.

Manual Backup

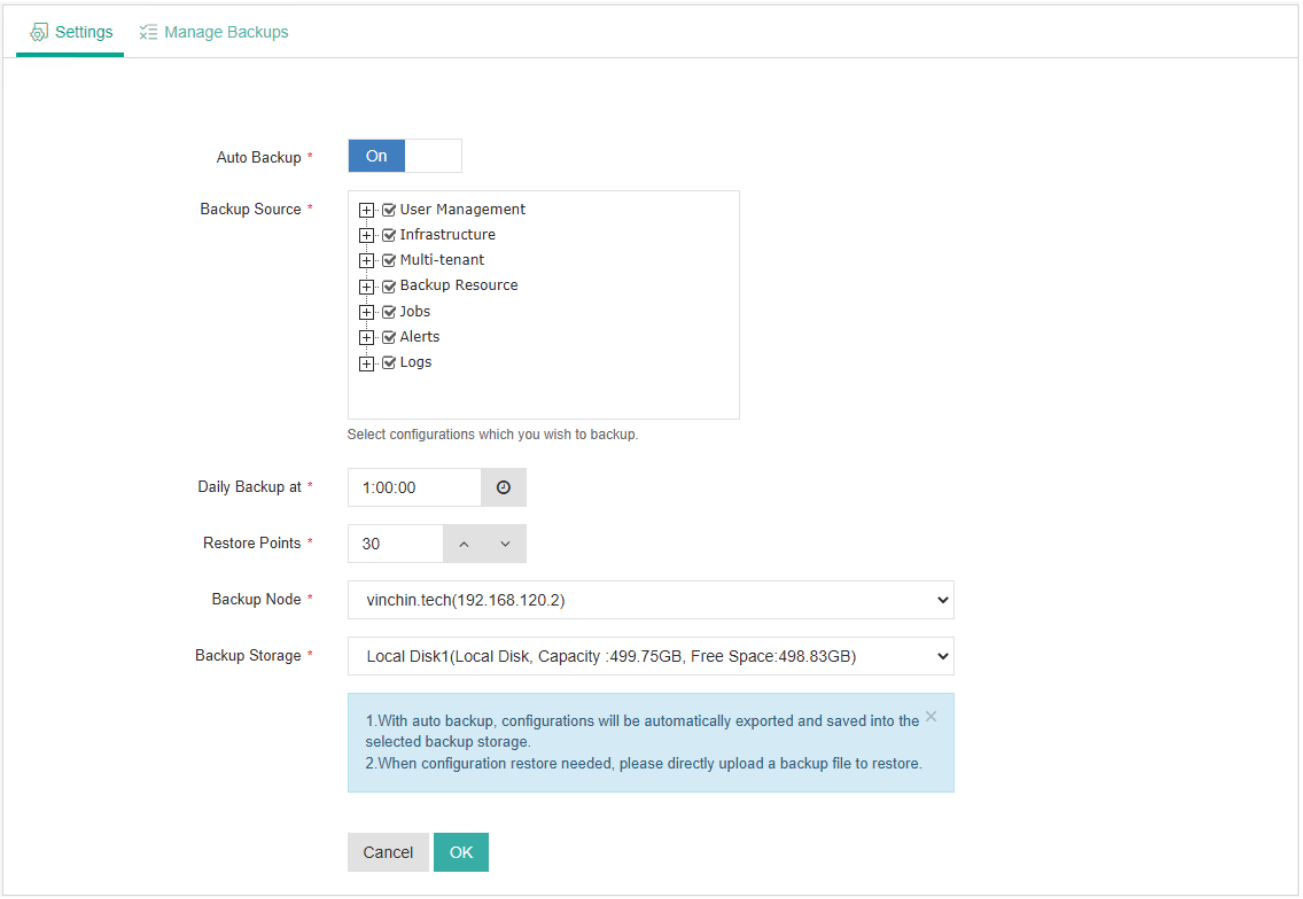
Select configurations which you wish to backup.



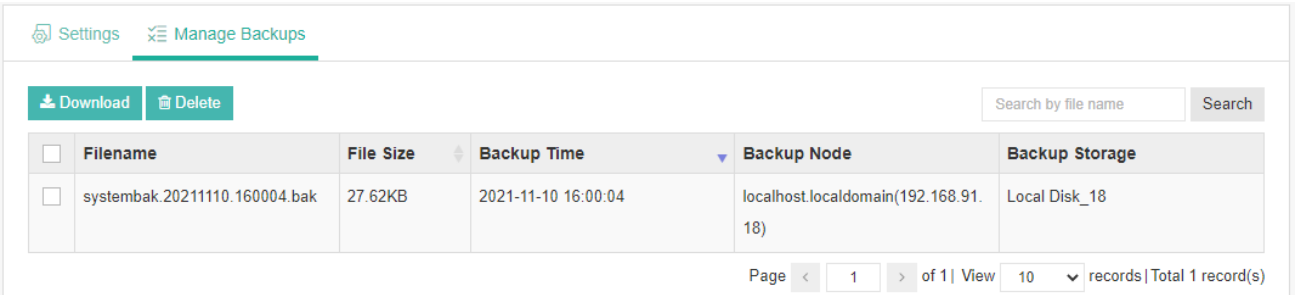
The selected configurations will be exported as an individual file and downloaded to your Downloads folder, please keep the configuration backup safe.
When configuration restore needed, please directly upload a backup file to restore.

Auto Backup

Auto Backup enables automatically backup of Vinchin backup server configurations on daily basis.



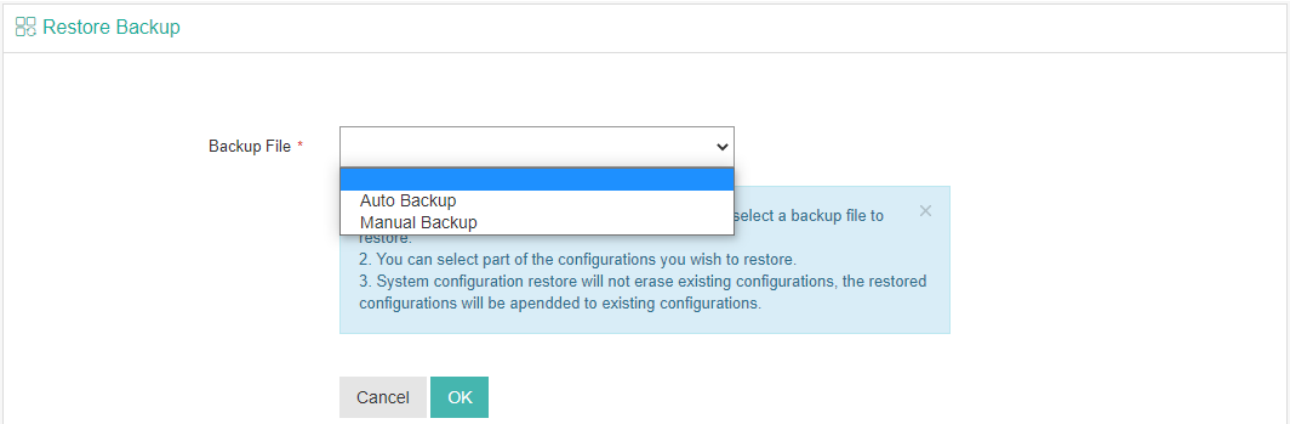
When enabled auto backup, users can select which configurations need to be backed up, and can pick a time of the day to run the backup. Restore points of the configuration backup determines how many (days of) backup files to be kept. A backup node and a corresponding backup storage can be selected to save the backup files.
The configuration backups can be accessed under **Manage Backups** tab.



Select the desired backup file and click on Download to download the backup file to your Downloads folder, or if the backup file is not needed or contain invalid configurations, select the backup file and click on Delete to delete it from the backup storage.

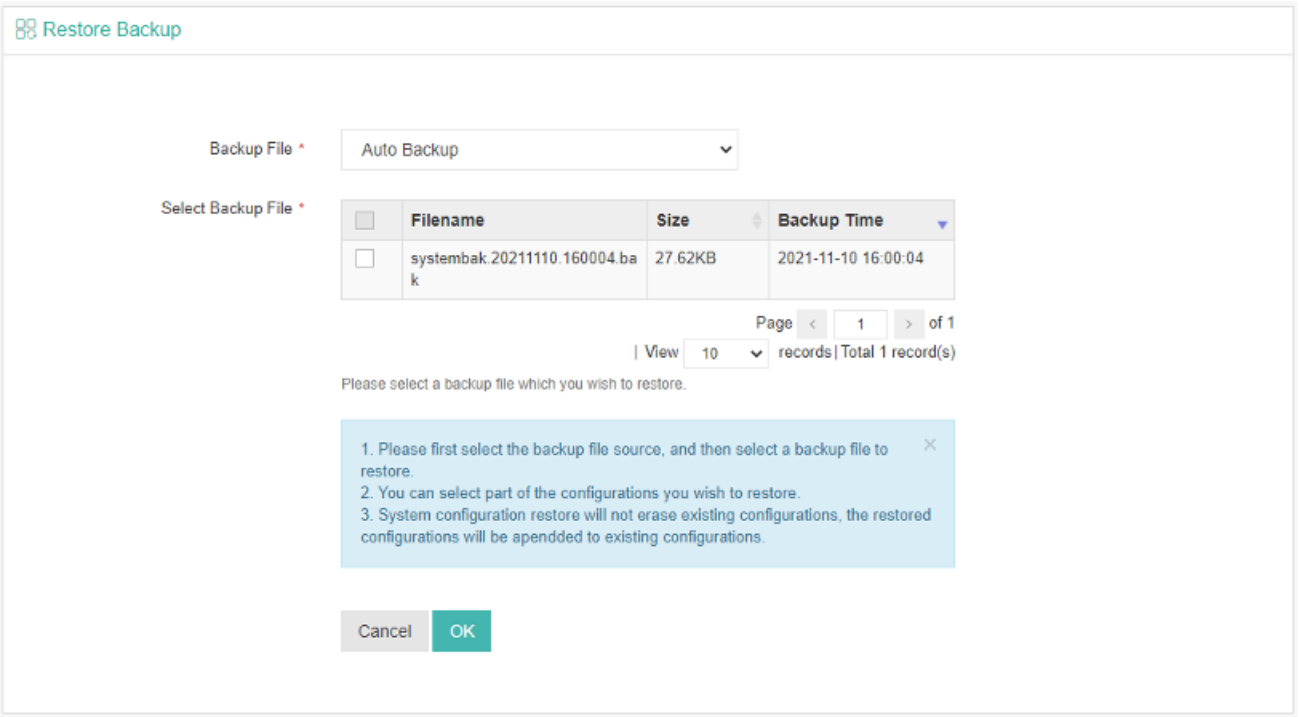
Restore Backup

When configuration restore is required, please go to **System > System Settings > Configuration Backup > Restore Backup** page.

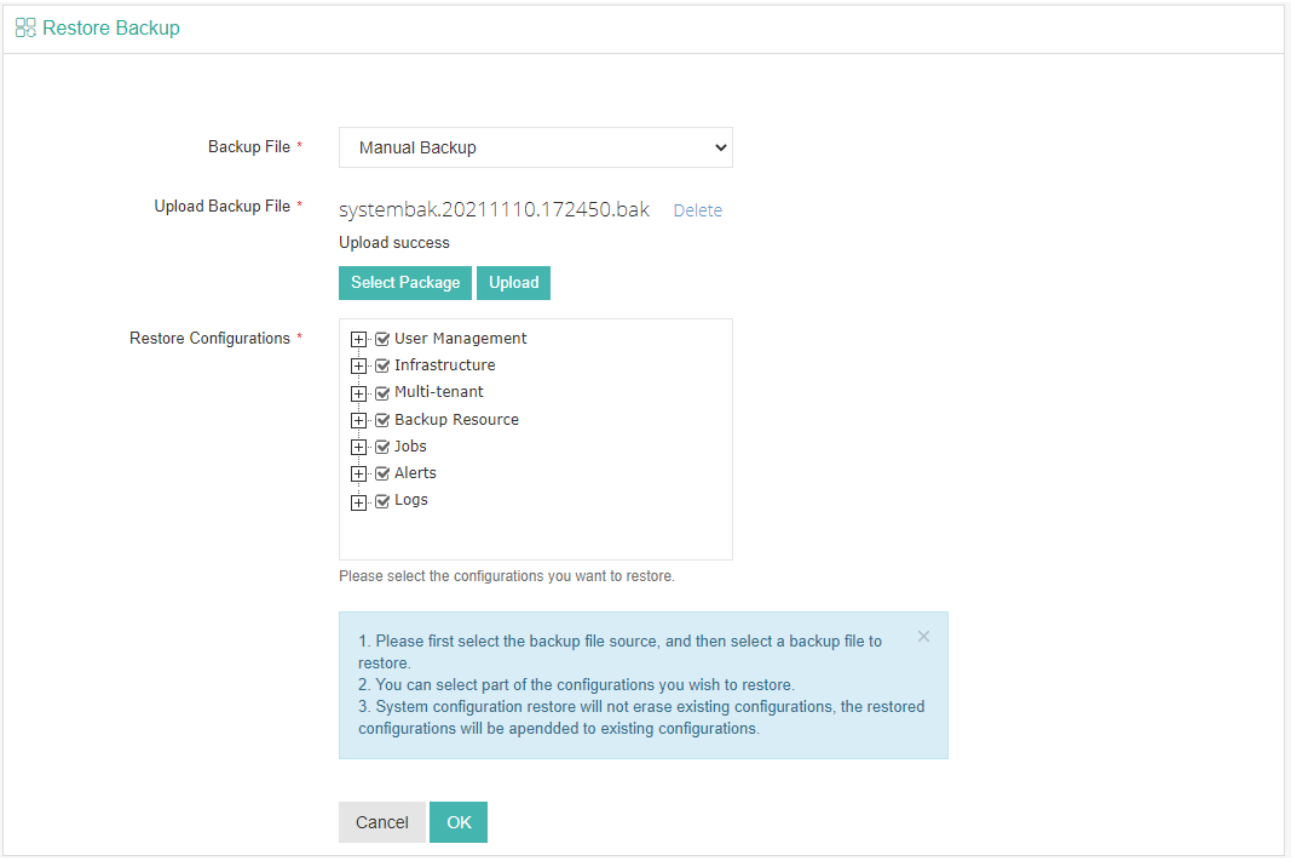


Select the backup file source, either auto backup or manual backup.

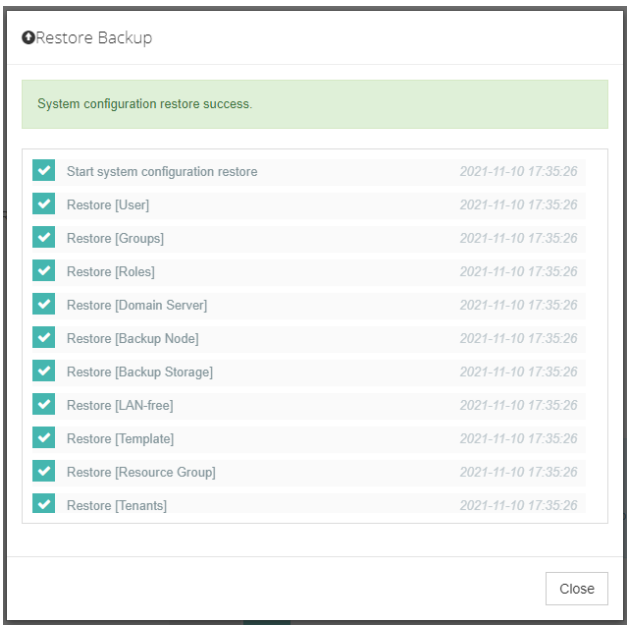
If Auto Backup, there will be a list of the backup files, you can simply select a desired backup file to restore the configurations.



If Manual Backup, you need to upload the configuration backup file to restore the configurations.



When the backup file is selected from the auto backup list or uploaded from user desktop to Vinchin backup server, please select the desired configurations you wish to be restored. Then click on **OK** to restore the configurations.



Note

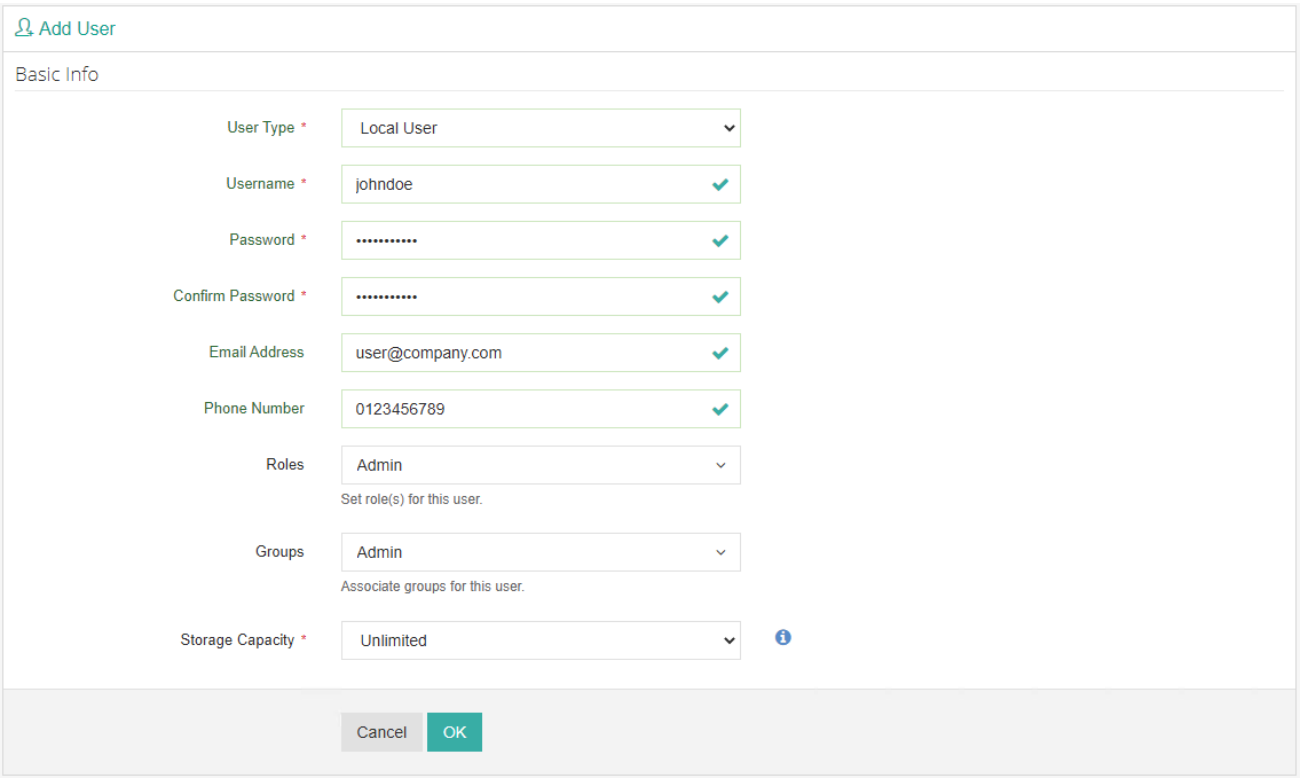
System configuration restore will not erase existing configurations; the restored configurations will be appended to existing configurations.

User Management

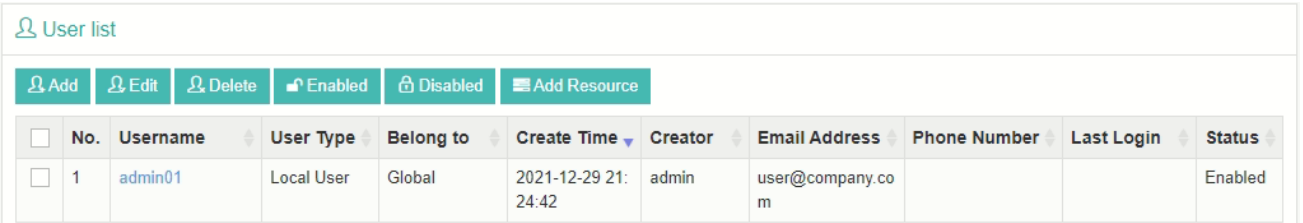
For an enterprise, administrators of Vinchin backup server can add users from internal departments of the enterprise who owns Vinchin Backup & Recovery infrastructure. They can share the resources of the backup infrastructure, like backup node and storage resources. But they need to add their own workloads to Vinchin backup server for backup and restore, like virtual infrastructure, file servers and database servers. So, each department runs their own backup services separately on the same backup infrastructure.

Users

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



The **User Type** can be **Local User** or **External User**. For local user, administrator needs to create a new user locally within Vinchin backup server. If external user, domain server integration must be done first. The newly added users can be assigned with different user roles and can be associated with desired user groups for permission management. And for storage capacity allowed to be used by this user can be set as Unlimited or Customized. Once a user had been added, it will be listed on the user management page.



You have the options to enable or disable a user from accessing Vinchin Backup & Recovery. To delete a user, if the

user has created subusers, it cannot be deleted, the subusers need to be deleted first.
And before this user can start any backup and restore services, administrator has to assign resources to the user at first place. The resources can be assigned to users including backup proxy, backup node and backup storage.
For the workloads which need to be backed up, users need to add from their own web portal, including virtual infrastructure (for VM backup), file backup agent and database backup agent.
If a user attempted to login with wrong password exceeded the Password Retry defined in Account Security settings, the account will be disabled. Only the administrator user who created that user has the permission to enable the account. Please select the disabled user and click on the **Enable** button to enable the user.

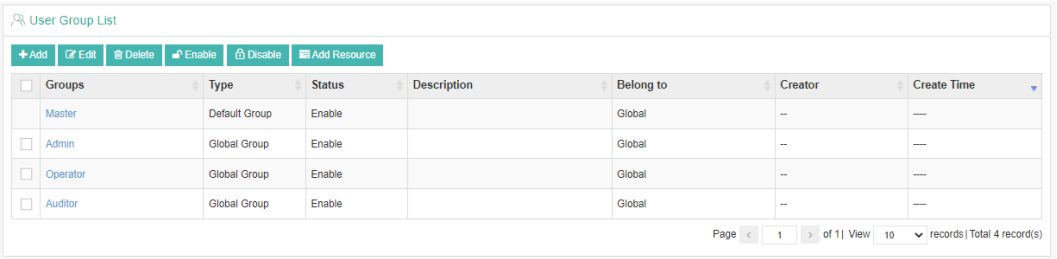
Note

Before deleting a user, you need to unregister all the virtual infrastructures registered by this user, otherwise the user cannot be deleted.

If the user role is admin and this admin user had added other users, then you need to delete the other users added by this admin user before deleting this admin user.

Groups

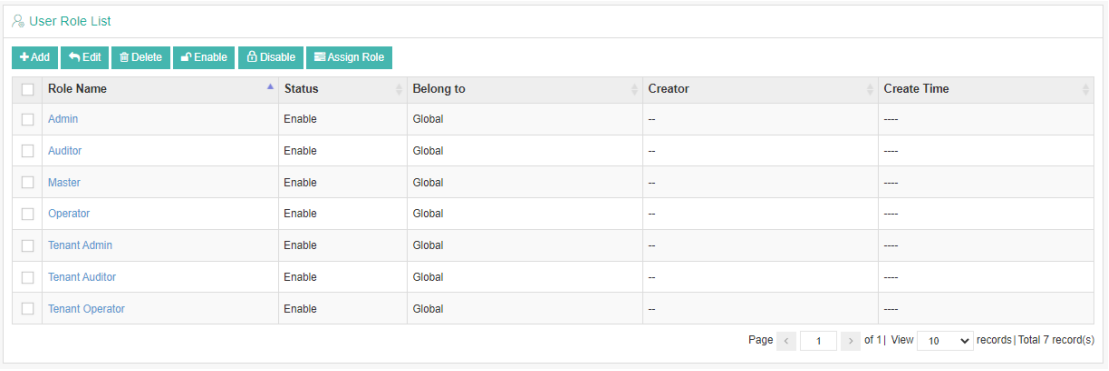
A user group is a collection of users who share the same resources and permissions.
There are default user groups which can be used for user permission management, but if needed, administrator can create new user groups with customized permissions.



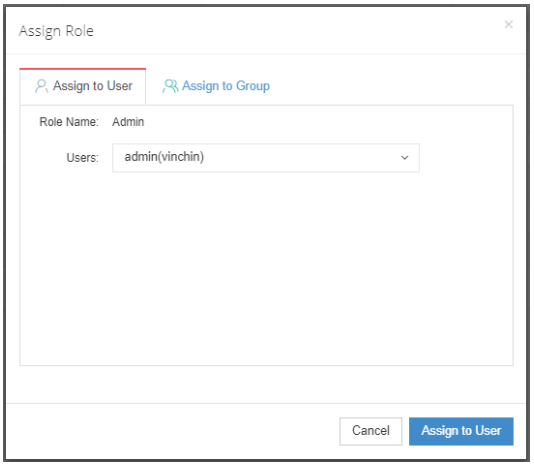
Click on **Groups** to view details about User, Roles, Resource Group and Permissions.
Click on Add Resource to add Backup Proxy, Backup Node, Storage Resources and Resource Group for groups. For the workloads which need to be backed up by the global users within the group, global users need to add from their own web portal, including virtual infrastructure (for VM backup), file backup agent and database backup agent.

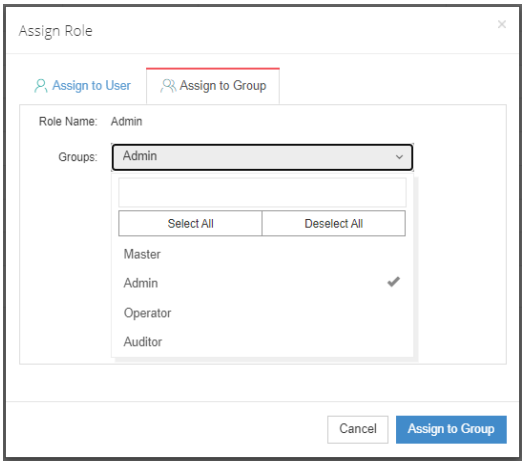
Roles

By default, there are 7 user roles available to be assigned to users or user groups.
Below are the permissions for different roles.

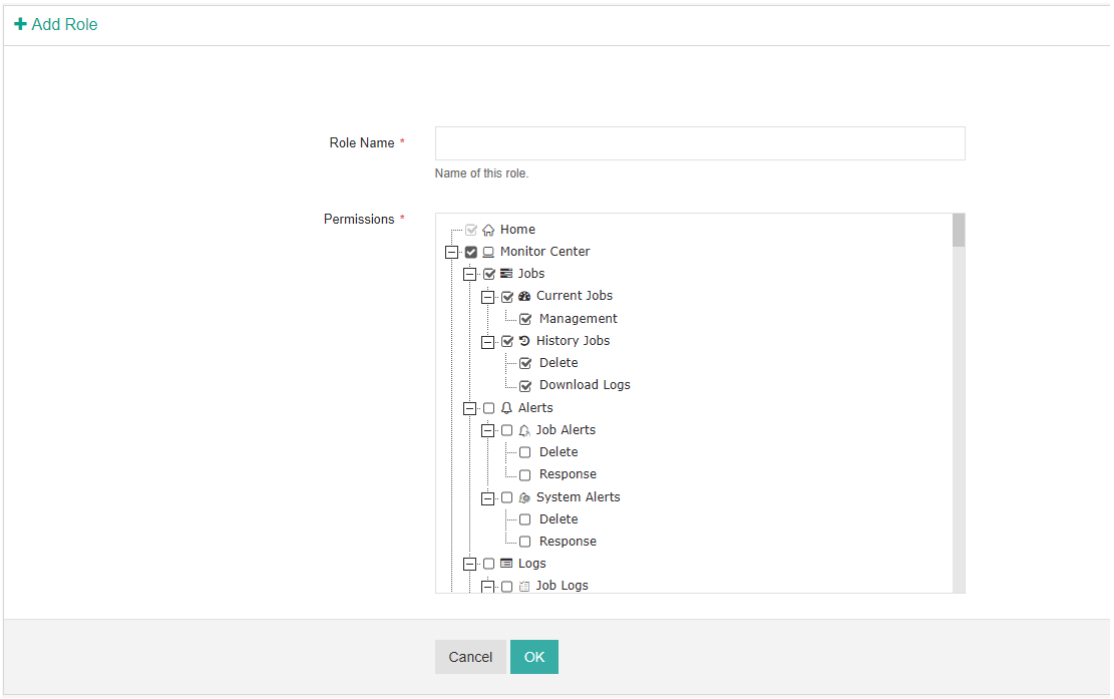


Master: the highest permission, has all management rights of Vinchin Backup Server.
Admin: System Alerts, System Logs, Storage Report, VM Report, Backup Node, Storage, LAN-free, Resource Group, all the System dropdown list and all User Management.
Operator: Current Jobs, History Jobs, Job Alerts, Job Logs, VM report, VM Backup, Database Backup, File Backup, Backup Copy, Backup Archive and Strategy Templates.
Auditor: Current Jobs, History Jobs, Job Alerts, System Alerts, Job Logs, System Logs, Storage Report and VM Report.
Tenant Admin: Current Jobs, History Jobs, Job Alerts, Job Logs, System Logs, VM Report, VM Backup, Database Backup, File Backup, Strategy Templates, Resource Group, Tenant Info and all User Management.
Tenant Operator: Current Jobs, History Jobs, Job Alerts, Job Logs, VM report, VM Backup, Database Backup, File Backup and Strategy Templates.
Tenant Auditor: Current Jobs, History Jobs, Job Alerts, Job Logs and System Logs.
You can assign role to users or user groups by selecting a role and clicking on **Assign Role** button, select user or user group you wish to assign.





Once a role had been assigned to a user or user group, the corresponding permissions of the role will be assigned to the user or user group as well.
If the default user roles cannot meet your actual requirements, you can also add customized new user roles by clicking on the Add button.

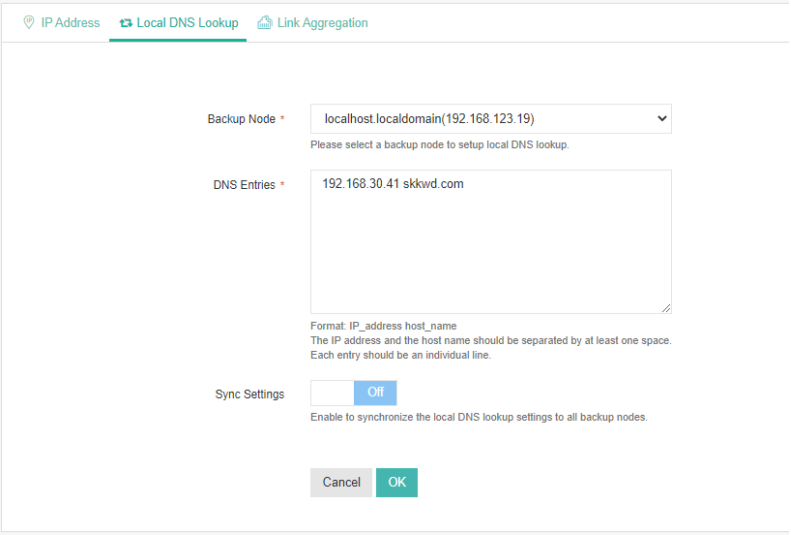


A role name is required to identify this new user role. And in the Permissions field, there's a tree menu showing all available web pages and operations of Vinchin web console, you can customize the permissions as per your needs.

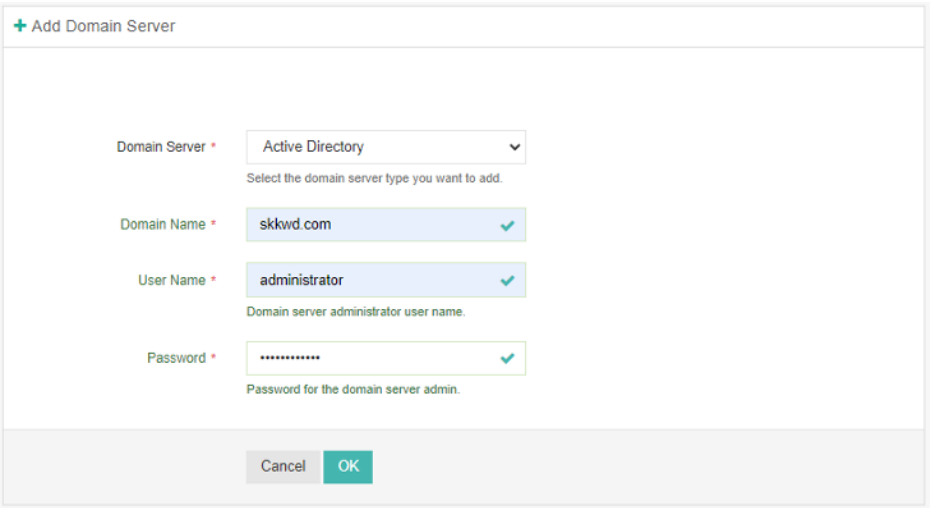
Domain Server

Domain server integration allows administrator to do user authentication by using the domain server. When a domain server is integrated, while adding new users, administrator can select to add External User which is from domain server. We currently support Active Directory server integration.

Before adding the domain server, first you may need to setup local DNS lookup. Click on **System** > **System Settings** > **Network Settings > Local DNS Lookup**, to set up Local DNS lookup, by using "IP_address host_name" format DNS entry is the DNS entries field.



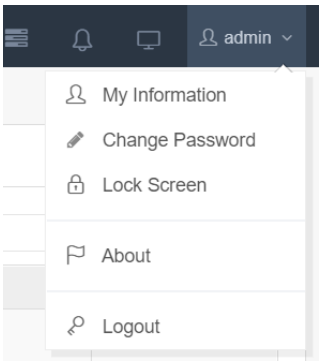
After setting up local DNS lookup, please go to **System > User Management > Domain Server** screen, click on Add button to add an Active Directory domain server.



Once a domain server is added, you are able to add external users from Active Directory domain server.

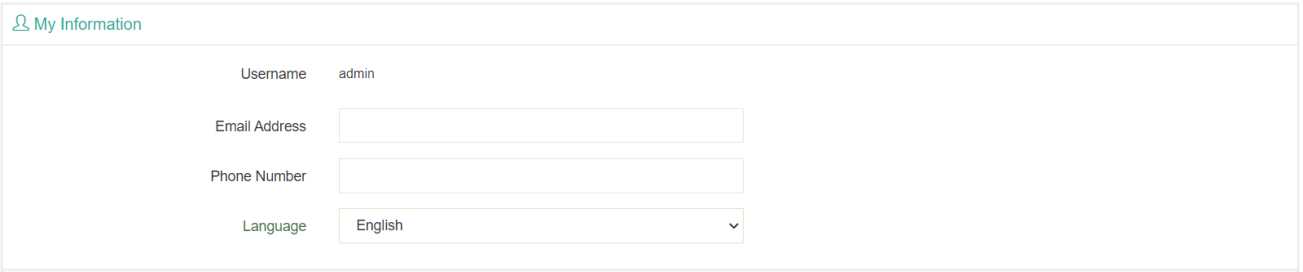
Account Settings

On the top right of Vinchin Backup Server web console, the current user login is displayed. Click on the username you'll be able to view the user information and manage some user settings.



User Information

On the user information screen, users are able to modify some basic user settings.



In the **Email Address** field, you need to fill in your Email address here, when you are trying to enable system notifications, an Email address is required here, and the system notifications will send to this Email address by default.

In the **Phone Number** field, you can optionally enter your phone number.

In the **Language** dropdown list, you can select a language which you are familiar with as the web console display language.

Change Password

Users can change their own passwords here and it is recommended to use strong password for system security. A strong password should be at least 6 characters, and should be a combination of digits, lower case and upper case letters and symbols.

Lock Screen

Users can lock Vinchin Backup Server web console from here, authentication will be required to unlock.

About

On the About page, users can get the system information and Vinchin contact information, and can follow us on social media, and also can participate in our user experience survey to help us to improve our products and services.

Logout

Users can sign out the current user login from here.

vinchin

Contact Information

Head Office

F5, Block 8, National Information Security

Industry Park, No.333 YunHua Road,

High-Tech Zone, Chengdu, China.

P.C.610041

Sales

Tel: +86-135-5029-3426

Email: sales@vinchin.com

Support

Tel: +86-159-2884-8843

Email: technical_support@vinchin.com

Website

www.vinchin.com