vinchin

# VINCHIN BACKUP & RECOVERY v7.0

## User Guide for SQL Server Database

2023/07

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

# Table of Contents

# Supported SQL Server Environments

Supported Deployments:

- Standalone
- Failover Cluster
- Always On availability groups

Supported MS SQL Server Versions:

- MS SQL SERVER 2008 R2
- MS SQL SERVER 2012
- MS SQL SERVER 2016
- MS SQL SERVER 2017
- MS SQL SERVER 2019

Supported Operating Systems:

- Windows server 2008 R2
- Windows Server 2012 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2017
- Windows Server 2019

# Preparation for SQL Server Backup

## Download Agent

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

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

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

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

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

## Install Agent

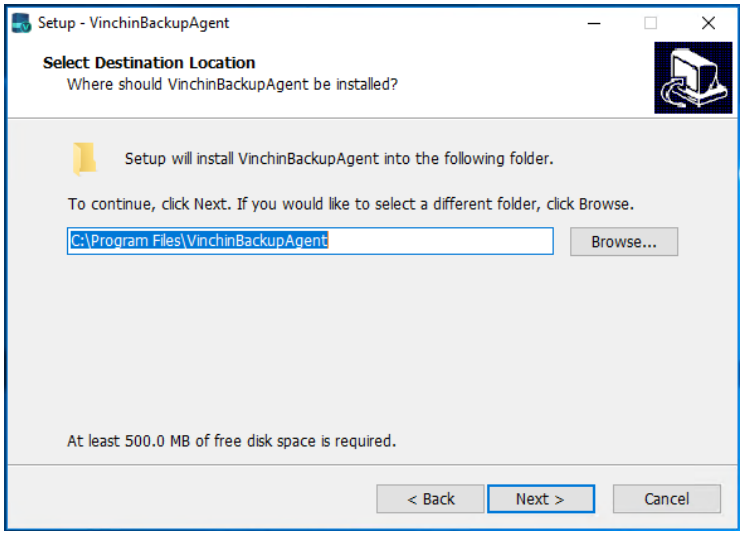
Please follow the installation wizard to complete the database backup agent installation.

Install the backup agent follow the steps below.

1. Run the backup agent installer with administrator permission by right clicking on the installer

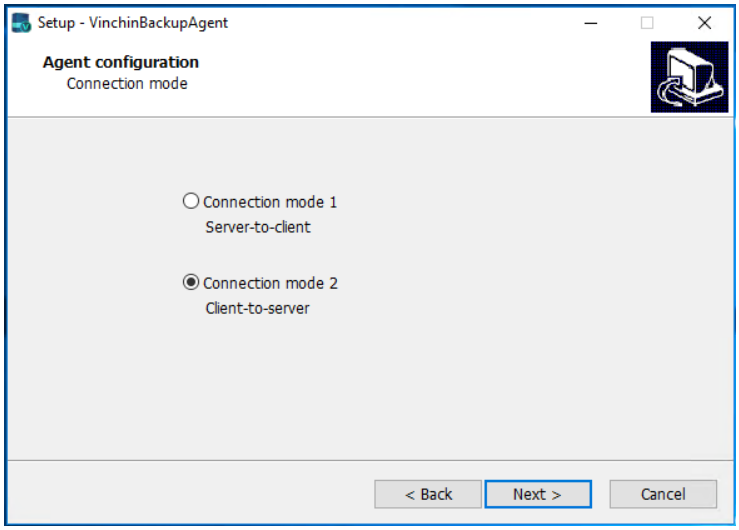
and select **Run as administrator**.

2. Specify installation location.




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

3. Specify connection mode.

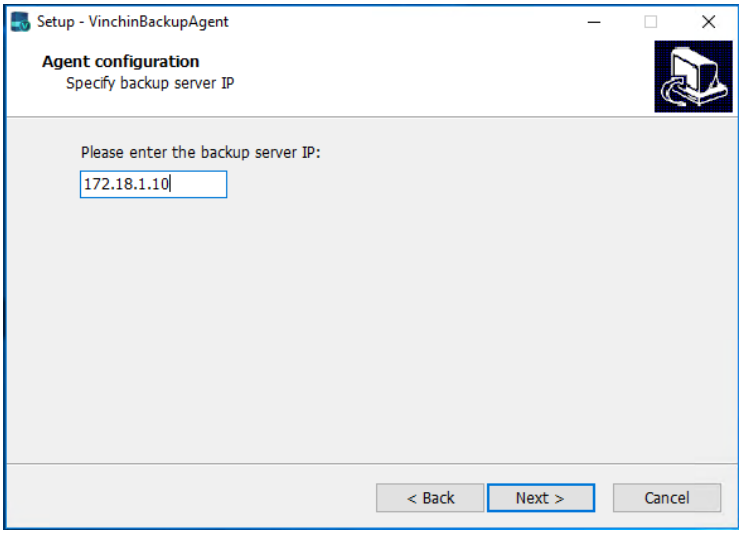



Choose between Connection mode 1 and 2 to determine "Server-to-client" or "Client-to-server" connection mode.

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

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

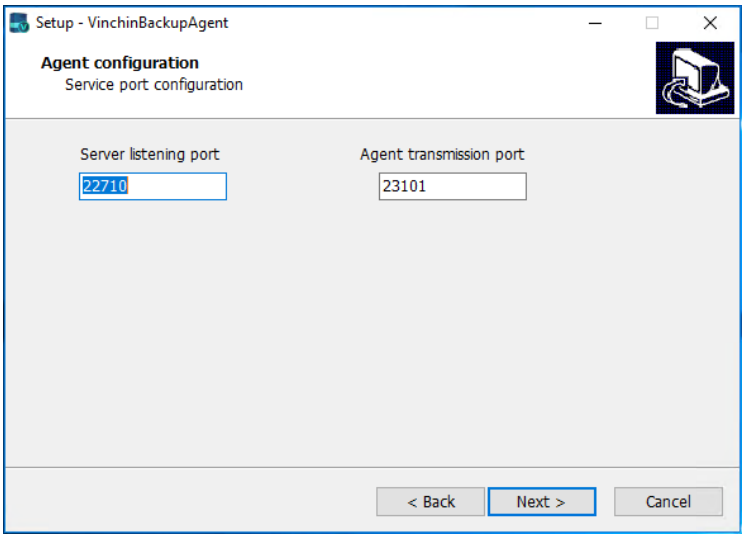
4. Specify backup server IP.



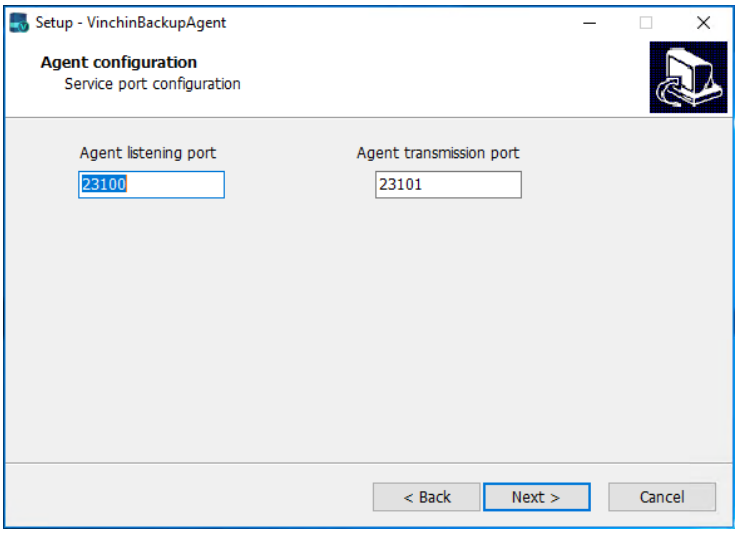

If you had chosen Connection mode 2, please enter the backup server IP address and click on next to continue.

5. Port configurations.

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

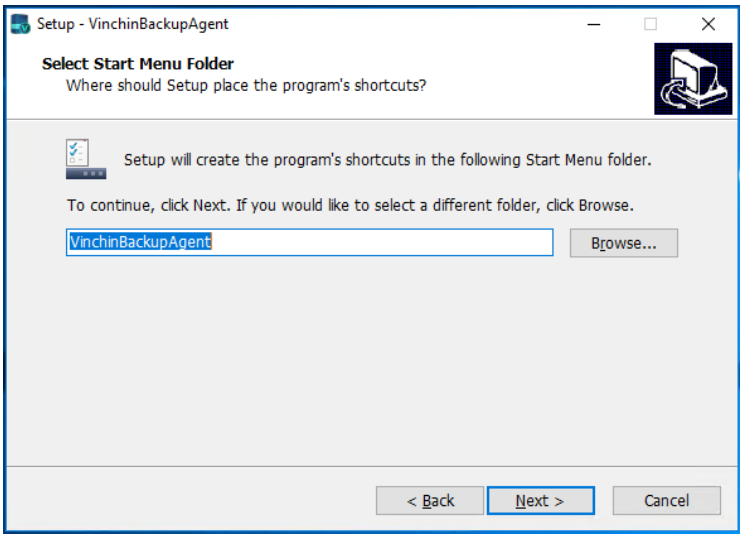



If Connection mode 2, users have to specify the server listening port and agent transmission port.



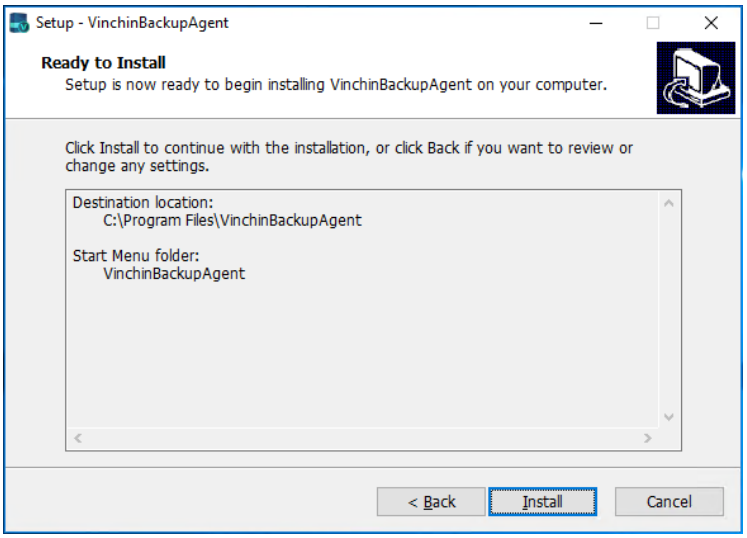

For both scenarios, it's always recommended to use the default port numbers.

6. Specify the start menu folder.




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

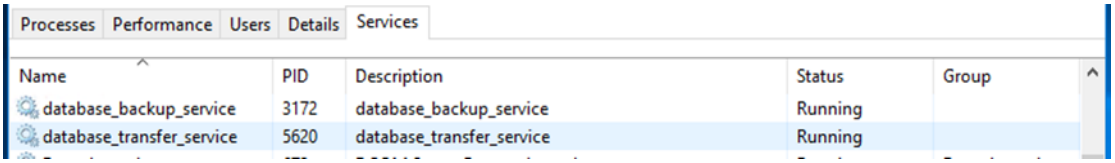
7. Confirm installation.



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

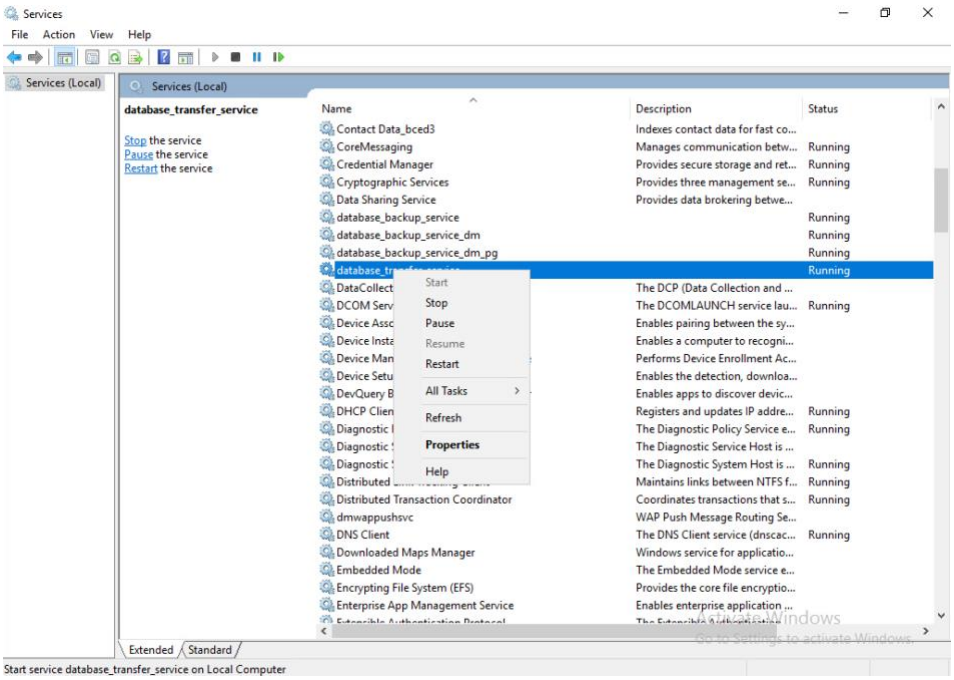
Once the installation is completed, please click on Finish to exist the agent installation wizard. If you had chosen Connection mode 1 (Server-to-client), after the agent installation, please open Vinchin Backup & Recovery web console to add the agent to Vinchin backup server, please refer to Add Agent.

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 back up plugin on the Windows system.

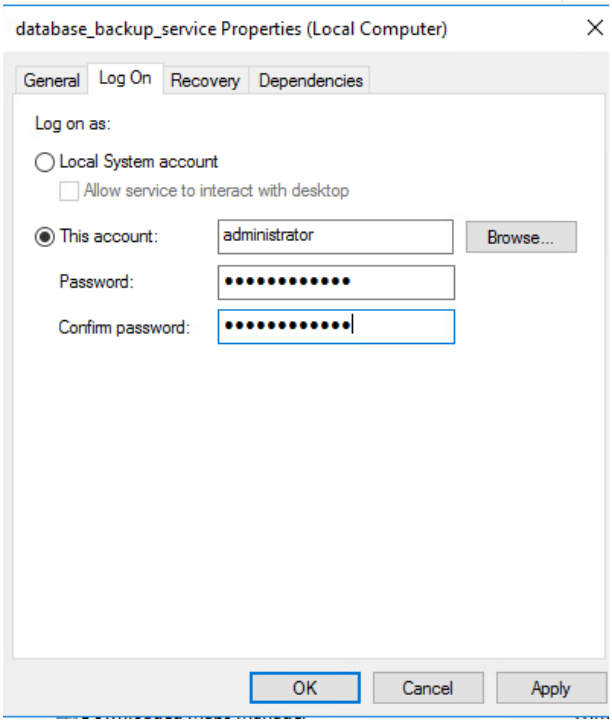



If you want to use Windows authentication to backup the database, please edit the database backup services to log on as **administrator** from Windows **Services**.

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



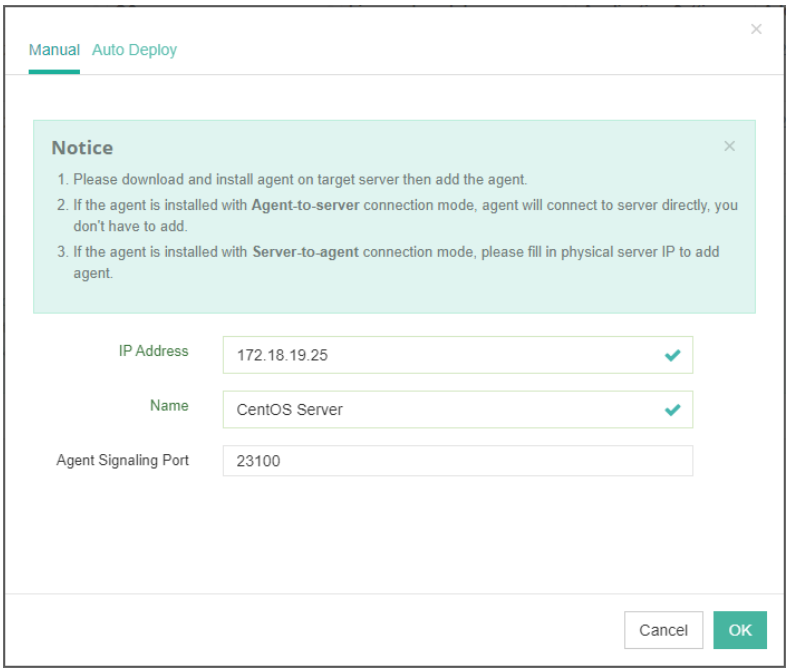

When these 2 services had been stopped, right click on them and select **Properties > Log On**, select log on as **This account**, then fill in the administrator account name and password, click on **Apply** and restart the services.




# Add Agent

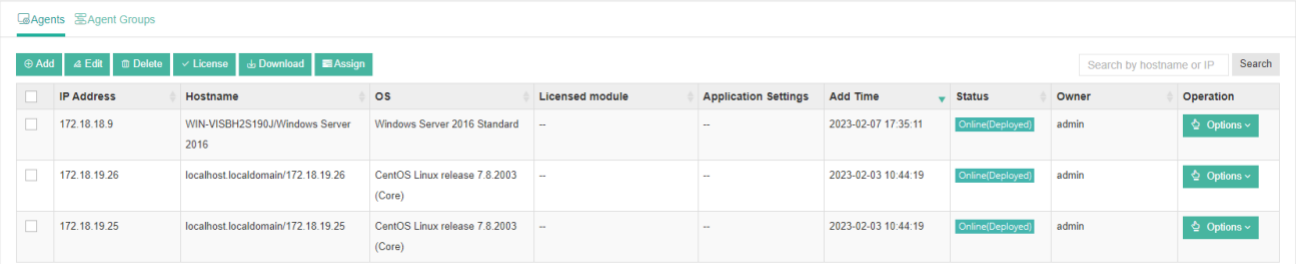
If the connection mode is 1 (Server-to-client), after the agent installation, users have to added the agents from Vinchin Backup & Recovery web console from **Resources** > **Agents** page.

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




In the **IP Address** field, please input the IP of the Linux/Windows server which you had installed the agent with

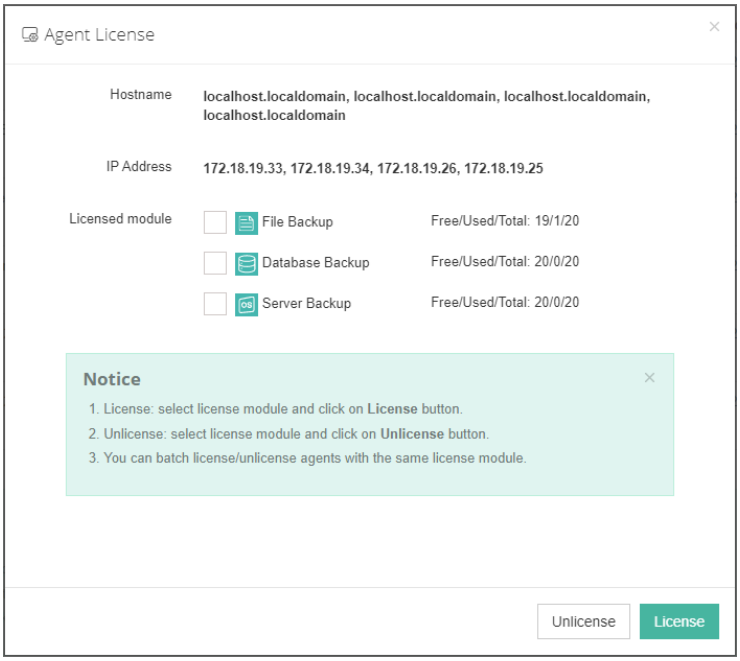
Server-to-client connection mode.
In the **Name** field, you can give it a name for identification.
As for the **Agent Signaling Port**, it's not recommended to change it, please leave it as default.
Once done, click **OK** to add the agent.




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

# License Agent

All physical backup agents connected to Vinchin backup server will be listed on the **Resources** > **Agents** page.
Before users can perform file, database or server backup, the agents need to be licensed with corresponding license modules.
Select one or a group of physical backup agents and click on License button, you'll be able to enable backup of those agents.




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

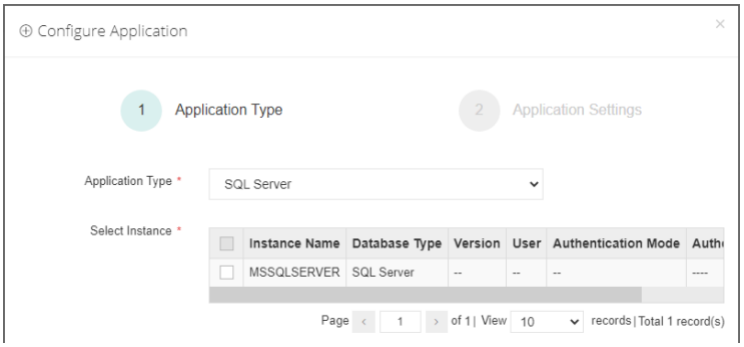
# Configure Application

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

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

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

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

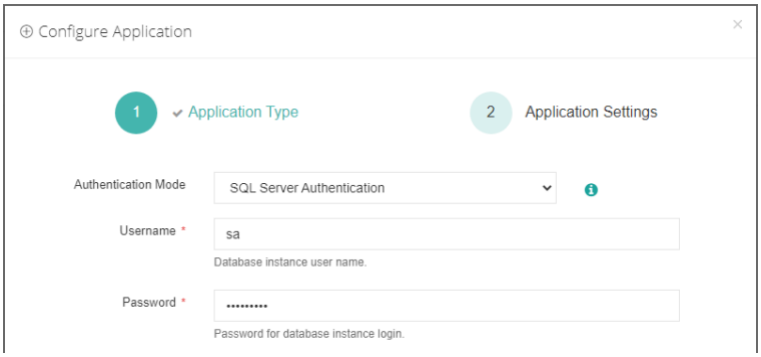



Select the SQL Server instance and click on **Next**.

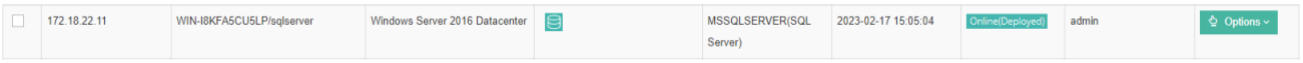
There are two authentication modes, **Windows Authentication** and **SQL Server Authentication.**

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

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




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




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

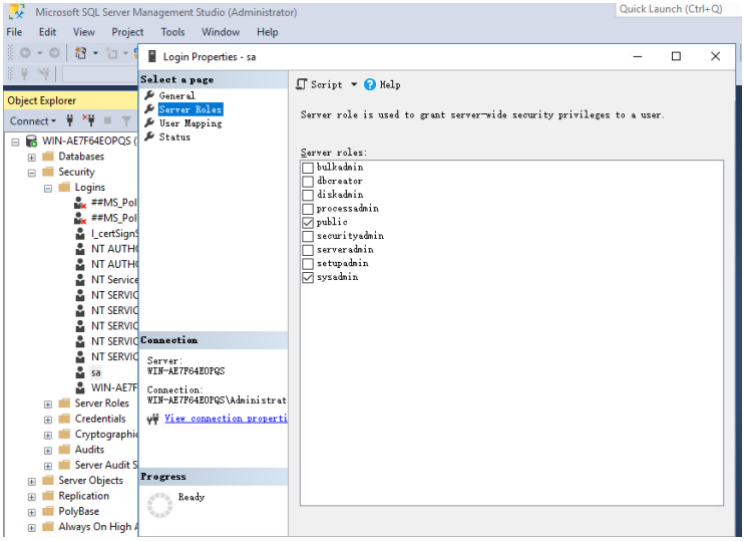
***Note***

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

# Before Backing Up MS SQL Server

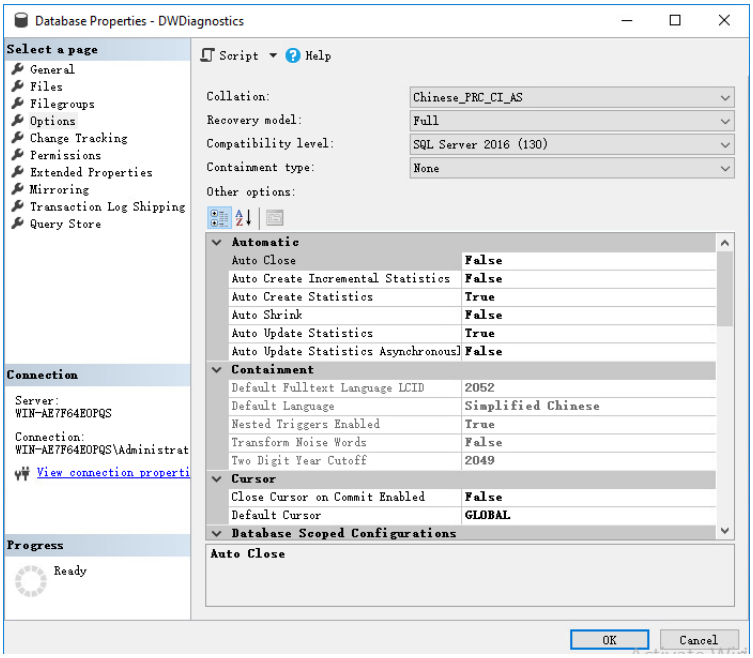
## Check Database User Permission

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.



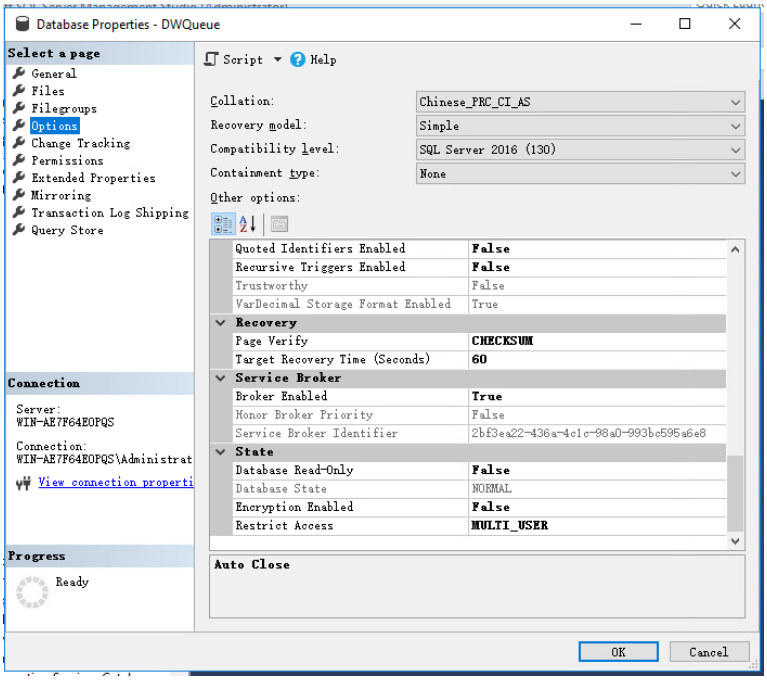

## Check Recovery Model

Check the recovery model of database, please ensure the recovery mode is “Full”, otherwise log backup job will fail.



## Check Restrict Access

Check the Restrict Access is 'MULTI_USER' in database properties so that the database can be multiple access when do backup or restore job.

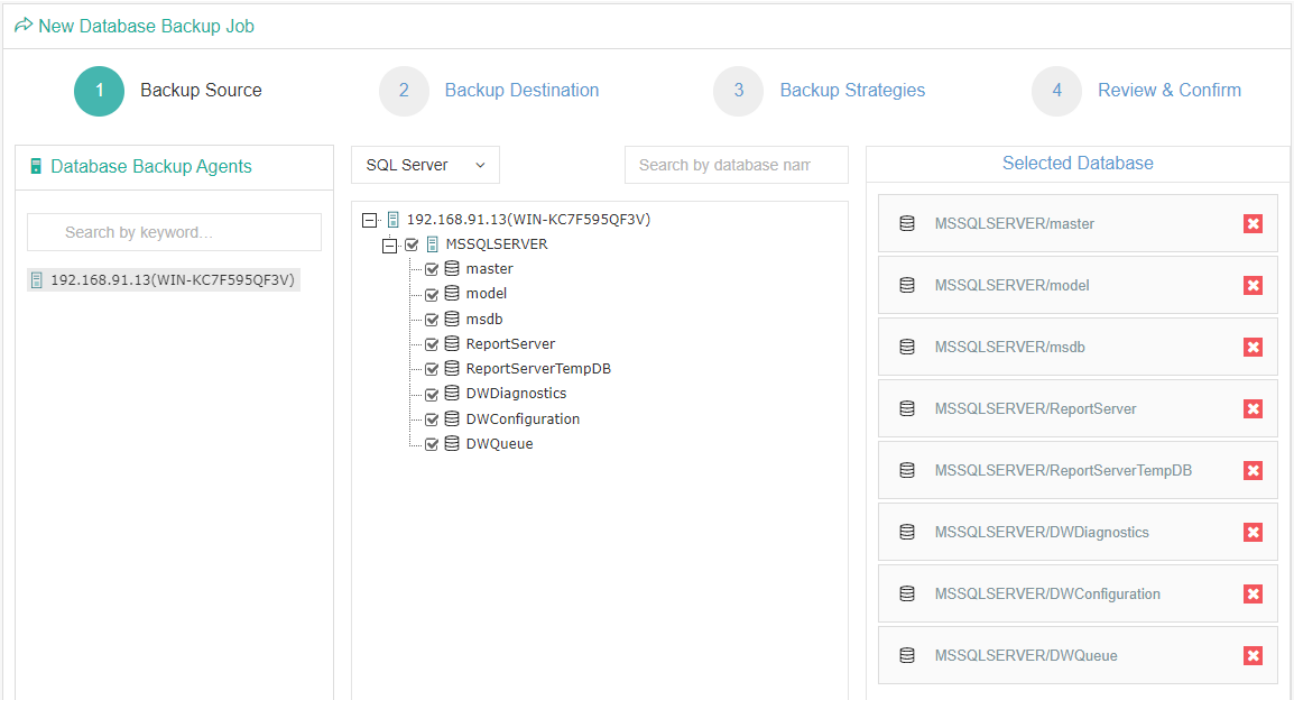



# Create Backup Job

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

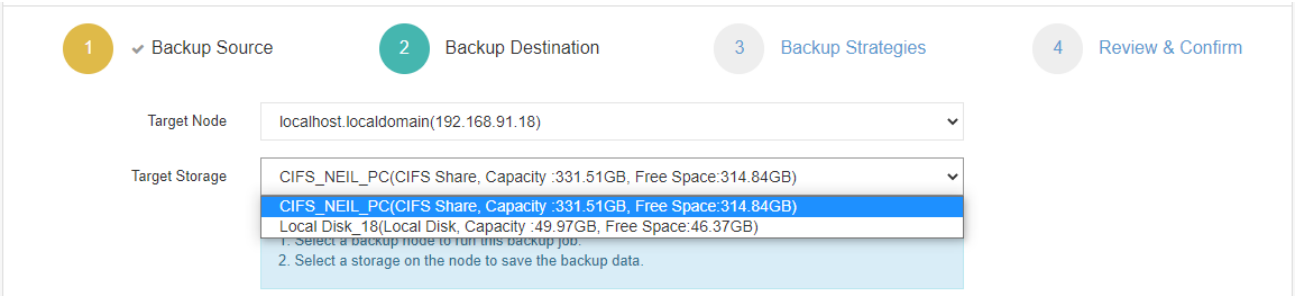
## Step 1: Backup Source

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




## Step 2: Backup Destination

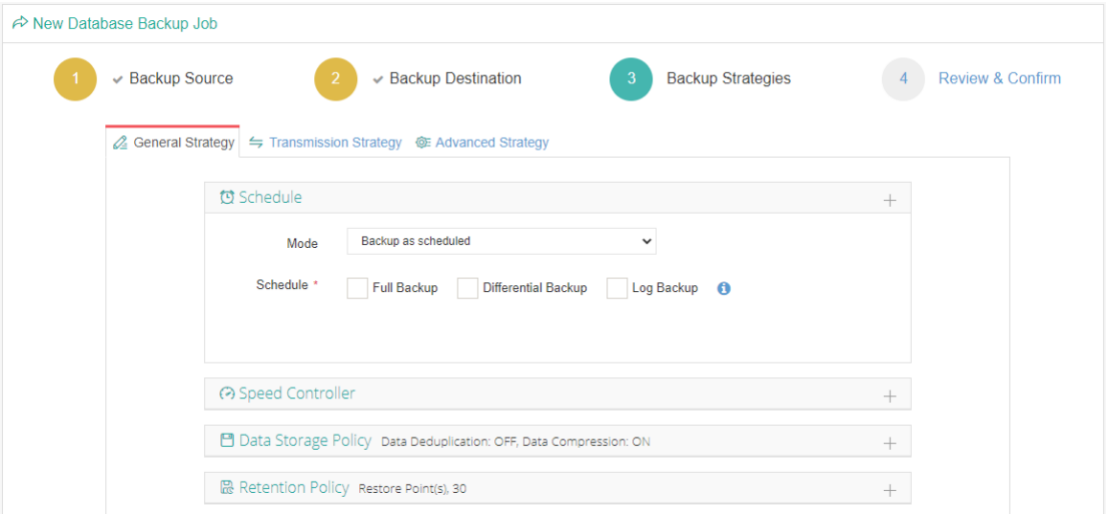
A backup destination (backup storage) should be associated with this backup job.




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

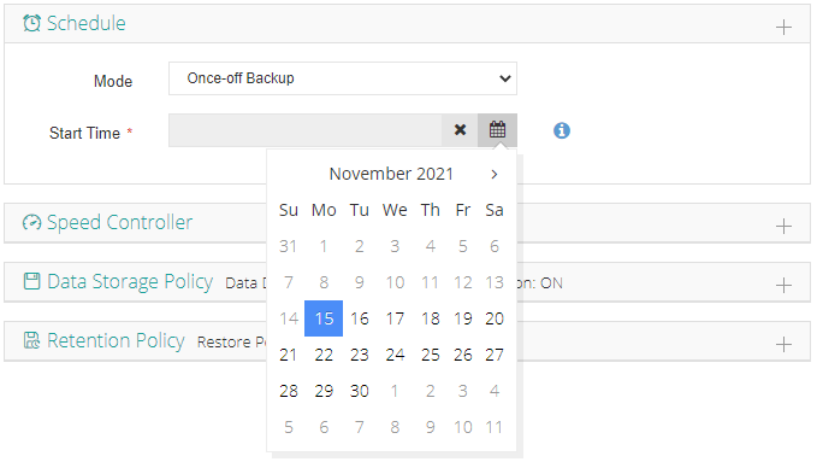
## Step 3: Backup Strategies

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



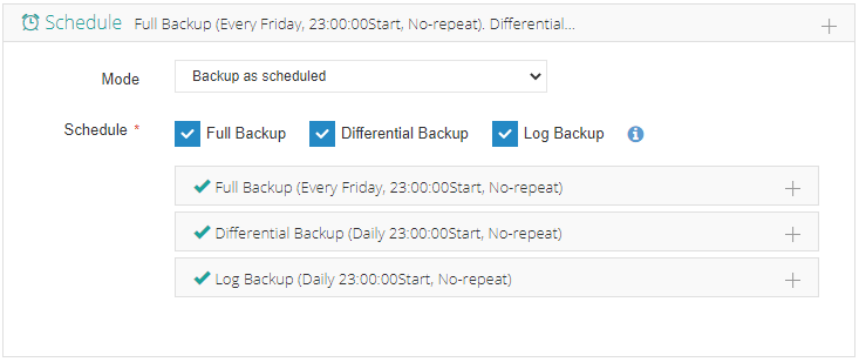

In the Schedule field, you can configure the time schedule of the backup job, you can configure the job as a **Backup as Scheduled** job or a **Once-off Backup** job.

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




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

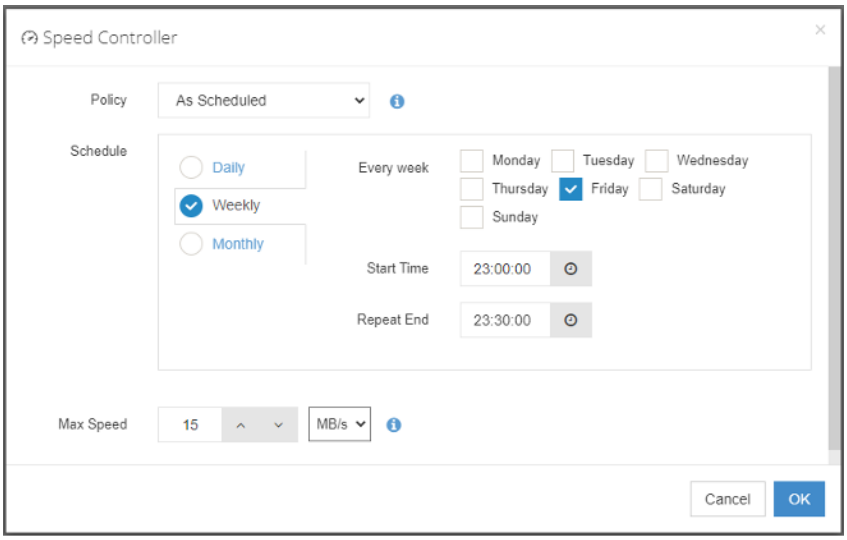
Here we take these three Backup as an example. Please set the backup mode and backup schedule as per your actual demands, then please click on **Next** to continue.



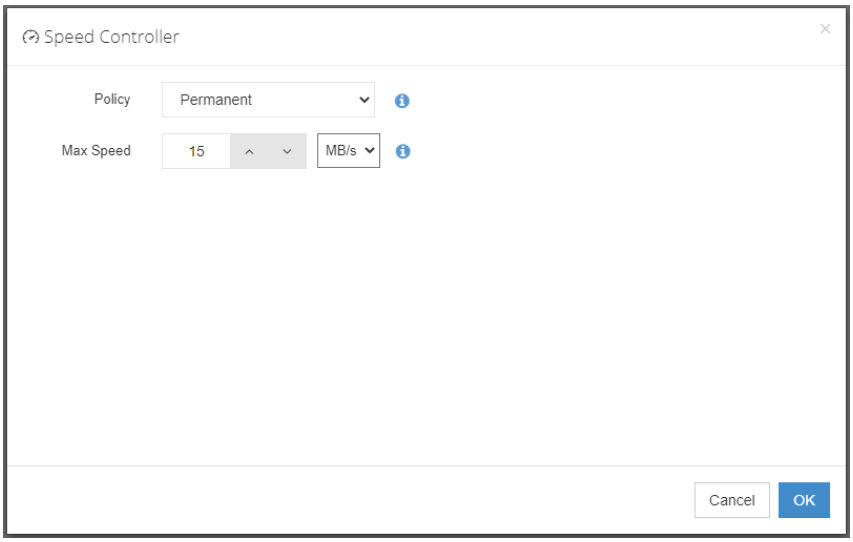

Speed Controller is optional. It can be used to limit the transmission speed during database backup if needed.

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

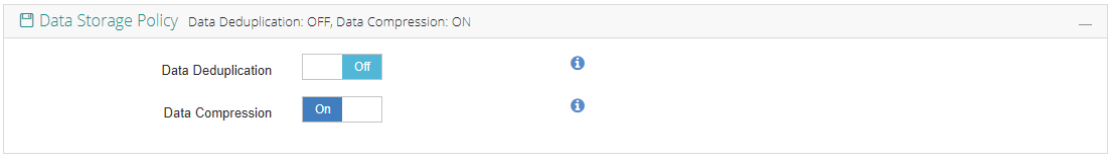
configured to limit the backup speed on Daily, Weekly and Monthly basis.




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



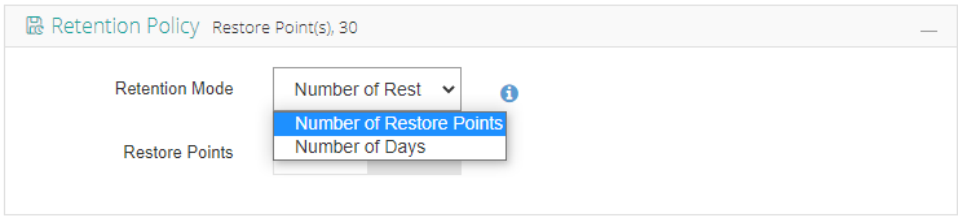

There are 2 options in Data Storage Policy section, Data Deduplication and Data Compression. By enabling these 2 options, the backup data will be deduplicated and compressed before saving into backup storage.




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

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

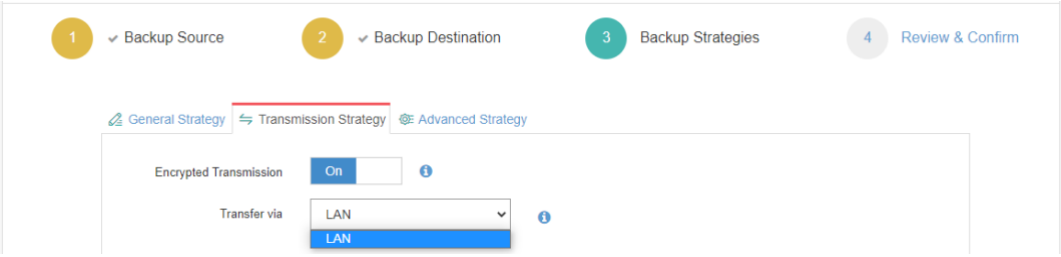
For retention mode **Number of Days**, Vinchin Backup Server will save the restore points within the specified number of days.



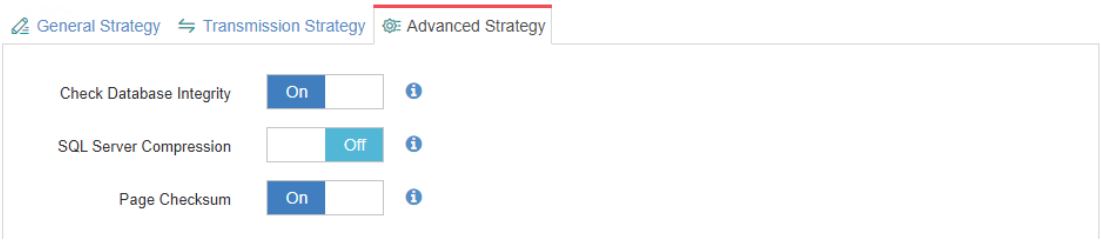

When the retention policy is triggered, the outdated restore points will be purged to comply with the retention policy.

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

The backup data will be transferred through LAN by default.




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




Check database integrity function is checking 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.*

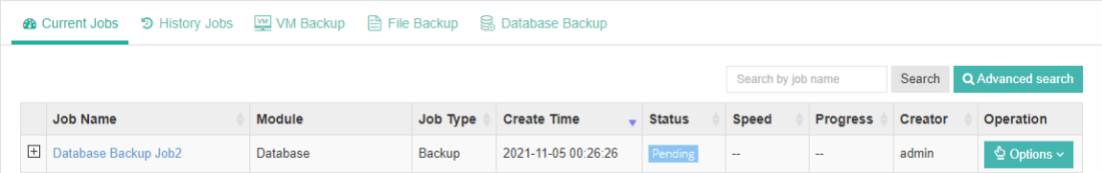
## Step 4: Review & Confirm

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.

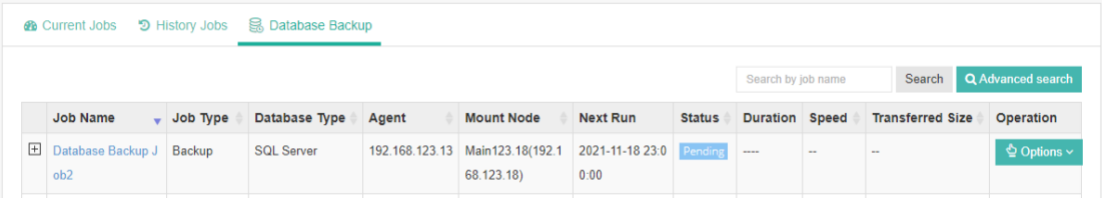
# Managing Backup Job

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




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

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




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

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

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

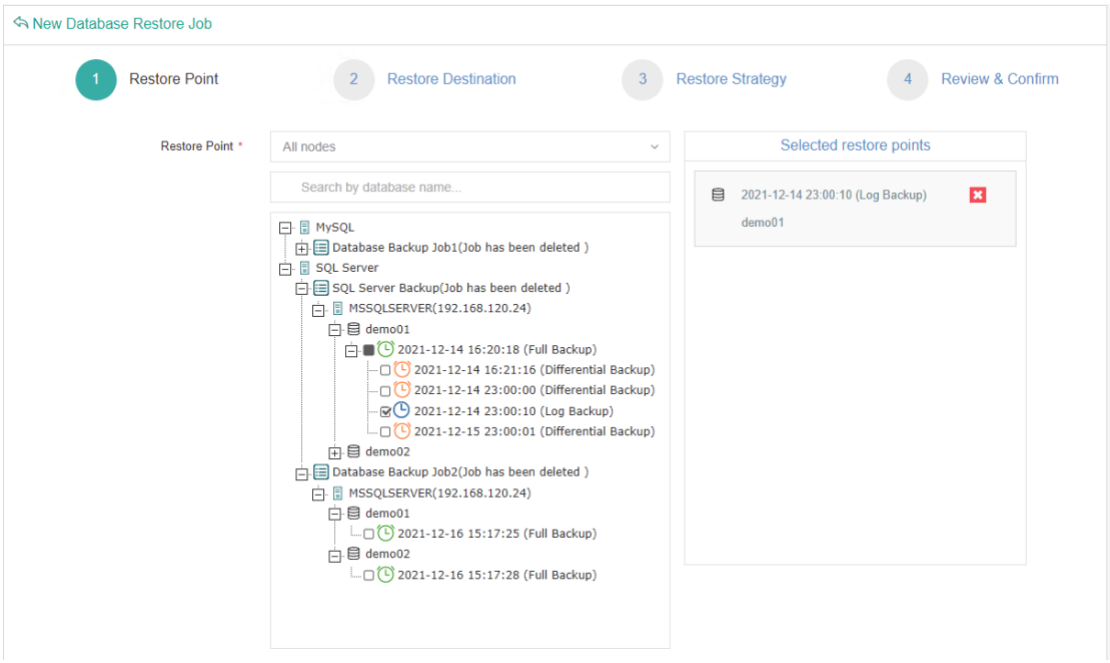
# Create Restore Job

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

## Step 1: Restore Point

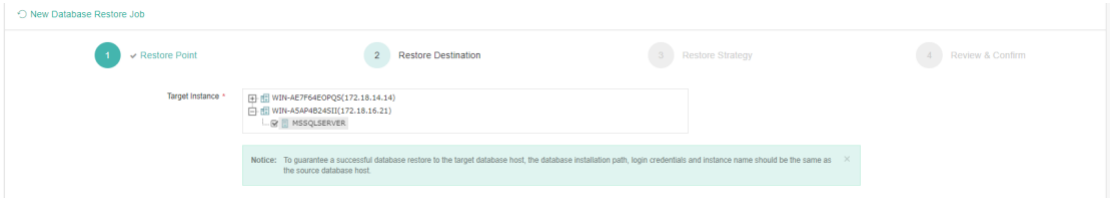
In the Restore Point dropdown list, select a backup node which stores the desired restore points.

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



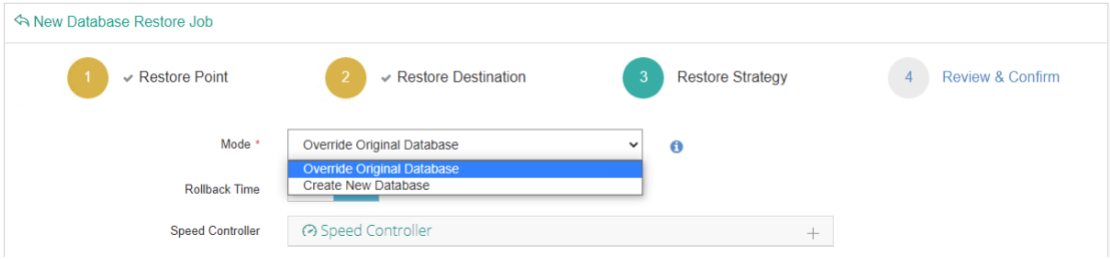

## Step 2: Restore Destination

After selecting the desired restore point, please select the target database instance on which you wish to restore. The target instance can be different but the version of your destination should keep consistent with backups.

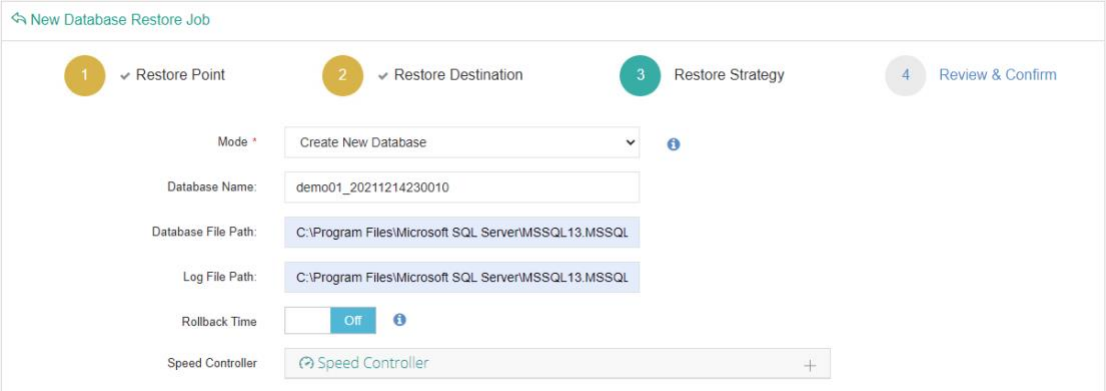



## Step 3: Restore Strategy

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.

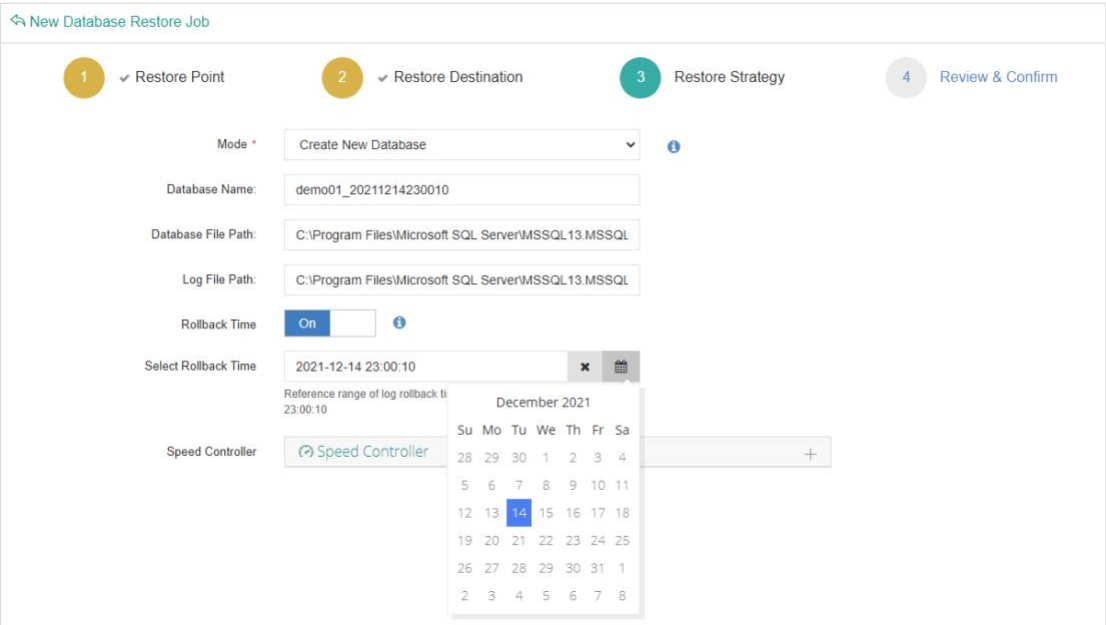



Select Create New Database need to edit database name, database file path, log file path. The path must be correct and have enough free disk space, the path will be automatically created during restore process.




**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.

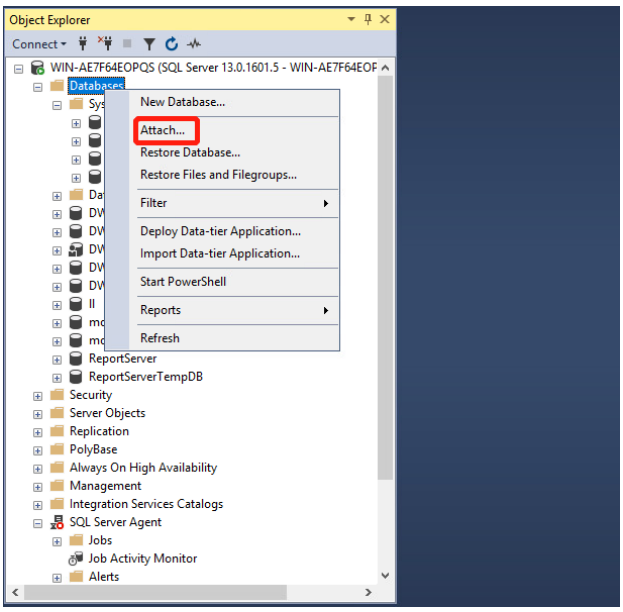
Once the job has been created, you'll be redirected to the **Monitor Center** > **Jobs** page.

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.

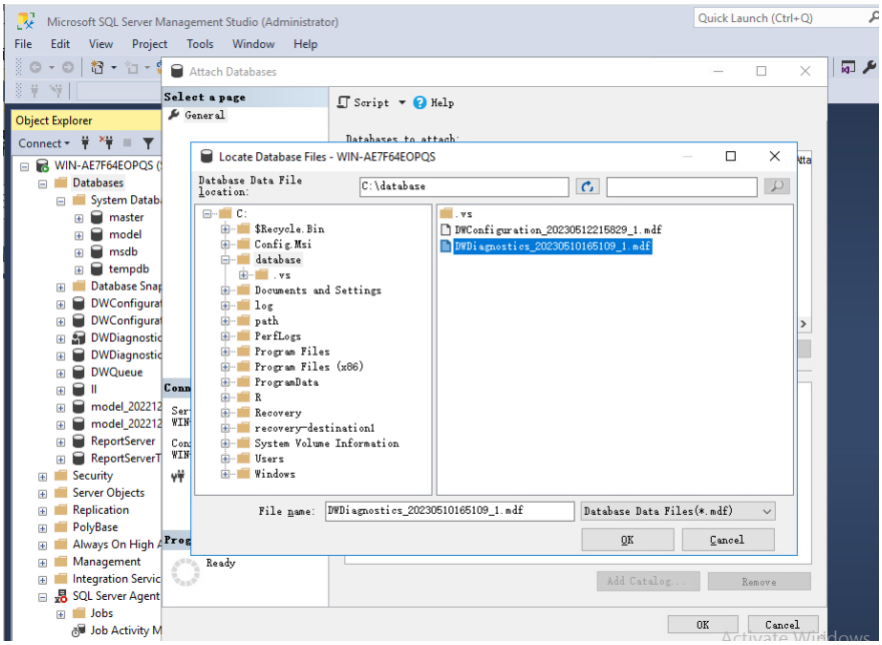
After this you can browse the restored job from History Jobs. Your restored data will be found in the path you configured during creating the restore job.

# Attach Restored Backup Data

If you create new database to restore, please login the SQL Server Management Studio (SSMS), right click database folder and select Attach option.

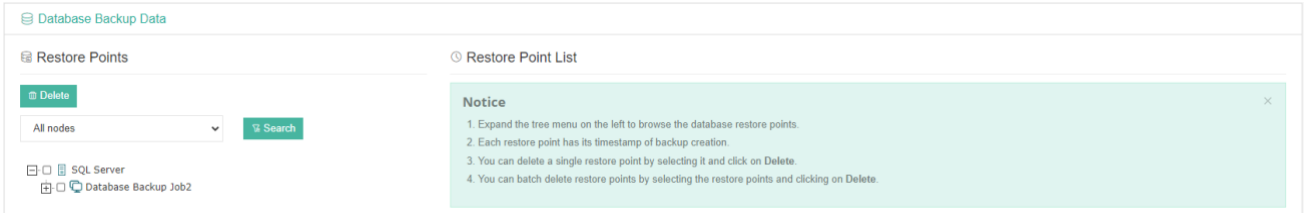



Then locate the database file to import while the log file of restored database will be automatically recognized and imported.



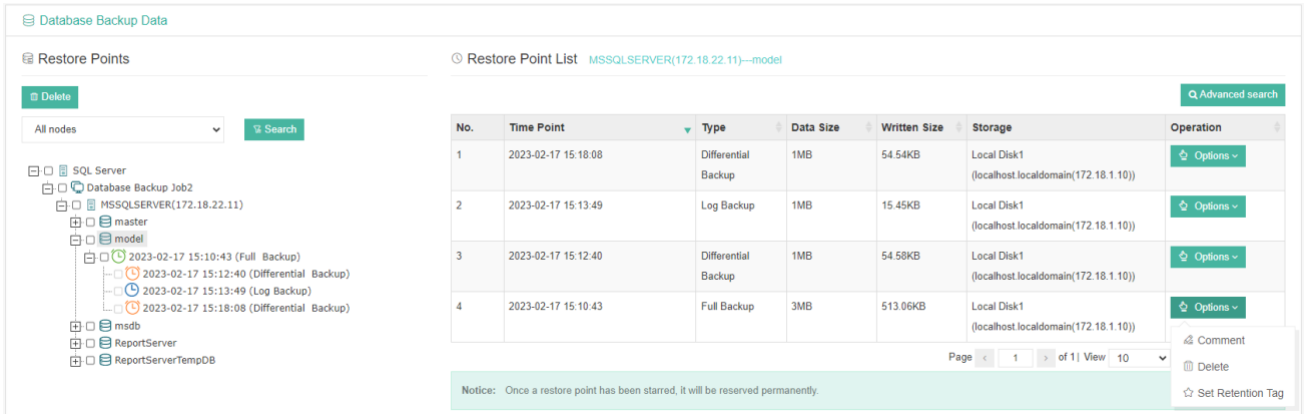
# Managing Backup Data

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




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

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




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

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

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