vinchin

VINCHIN BACKUP & RECOVERY V7.2

User Guide for MariaDB Database

2023/10

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

Table of Contents

Supported MariaDB Environments

Supported Deployment: Stand-alone
Supported MariaDB Versions: 10.5~10.10.2
Supported Operating System: RHEL 7, 8 & CentOS Linux 7,8

Preparation for MariaDB Backup

Download Agent

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

Install Agent

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

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

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

2. Enter the backup plugin package folder.

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

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

3. Install with the below command.

```
./agent_install
```

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

4. Choose the connection mode.

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

Choose between 1 and 2 to determine “server to client” or “client to server” connection mode.
If 1 (input 1 and press enter), the agent will only be installed and will not connect to server, users will have to add the agent from Vinchin Backup & Recovery web console after the agent installation.
If 2 (directly press enter or input 2 and press enter), users will be asked to provide the Vinchin backup server IP for the agent being able to automatically connect to after the installation.

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

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

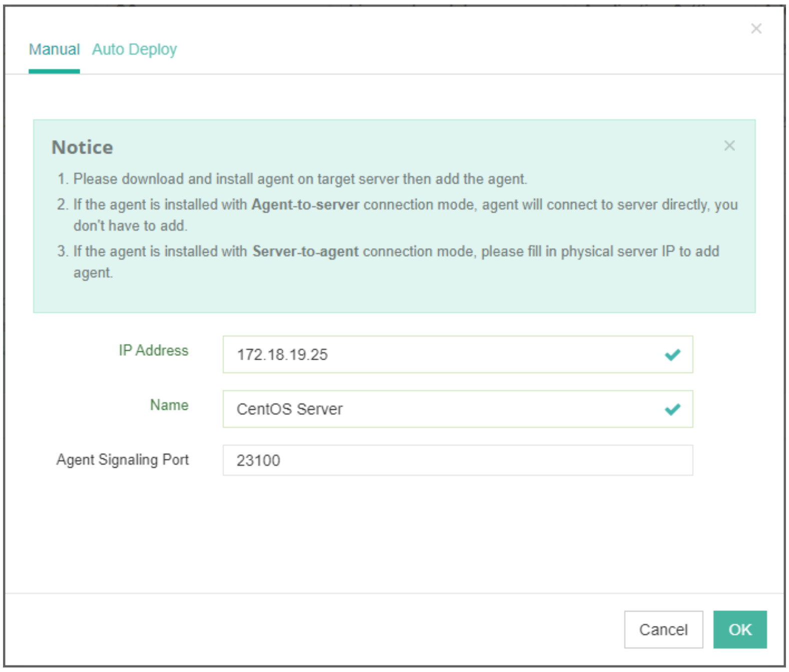
Please enter Vinchin backup server IP then press enter.

6. Specify client/server listening port.
If the connection mode is 1, users will be asked to specify the client listening port. It’s not recommended to change the port number, please press enter to continue.
If the connection mode is 2, users will be asked to specify the server listening port. It’s not recommended to change the port number, please press enter to continue.

7. Specify client transport port.
It’s not recommended to change the client transport port, please press enter to confirm the installation.
Once the users completed the above settings, the installation will be done in a few seconds, if you had chosen connection mode 1 (server to client), after the agent installation, please open Vinchin Backup & Recovery web console to add the agent to Vinchin backup server, please refer to Add Agent.

Add Agent

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



Notice

1. Please download and install agent on target server then add the agent.
2. If the agent is installed with **Agent-to-server** connection mode, agent will connect to server directly, you don't have to add.
3. If the agent is installed with **Server-to-agent** connection mode, please fill in physical server IP to add agent.

IP Address: 172.18.19.25

Name: CentOS Server

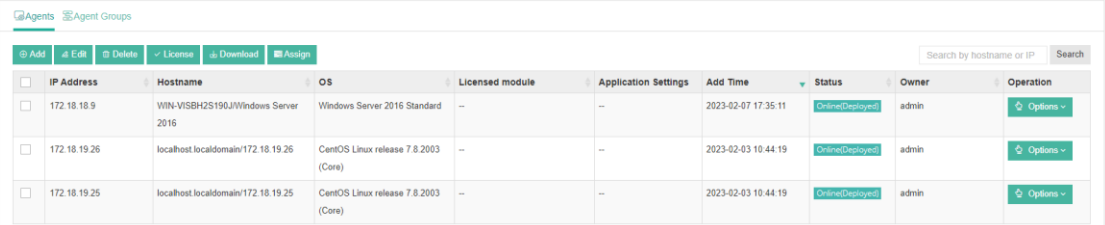
Agent Signaling Port: 23100

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.



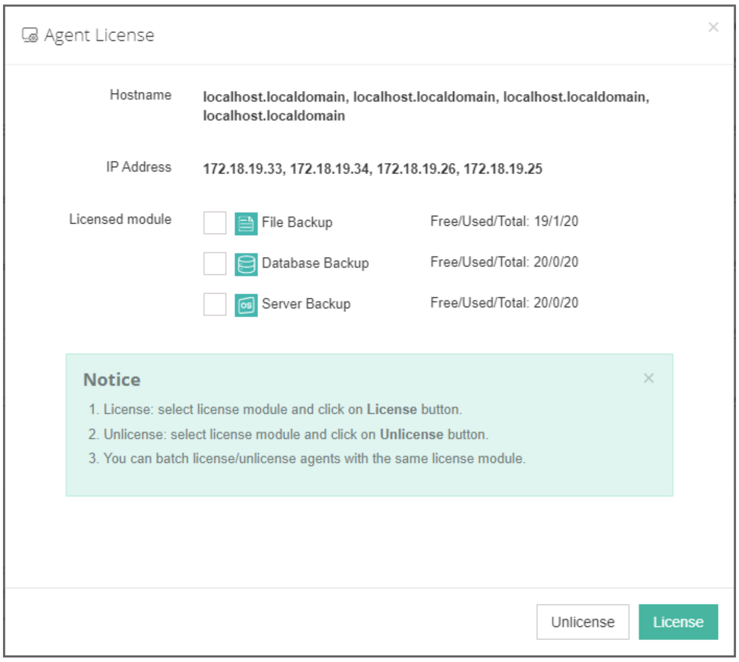
□	IP Address	Hostname	OS	Licensed module	Application Settings	Add Time	Status	Owner	Operation
□	172.18.18.9	WIN-VISBH2S190J/Windows Server 2016	Windows Server 2016 Standard	--	--	2023-02-07 17:35:11	Online(Deployed)	admin	Options
□	172.18.19.26	localhost.localdomain/172.18.19.26	CentOS Linux release 7.8.2003 (Core)	--	--	2023-02-03 10:44:19	Online(Deployed)	admin	Options
□	172.18.19.25	localhost.localdomain/172.18.19.25	CentOS Linux release 7.8.2003 (Core)	--	--	2023-02-03 10:44:19	Online(Deployed)	admin	Options

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 Agents

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

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



Hostname localhost.localdomain, localhost.localdomain, localhost.localdomain, localhost.localdomain

IP Address 172.18.19.33, 172.18.19.34, 172.18.19.26, 172.18.19.25

Licensed module

□ File Backup	Free/Used/Total: 19/1/20
□ Database Backup	Free/Used/Total: 20/0/20
□ Server Backup	Free/Used/Total: 20/0/20

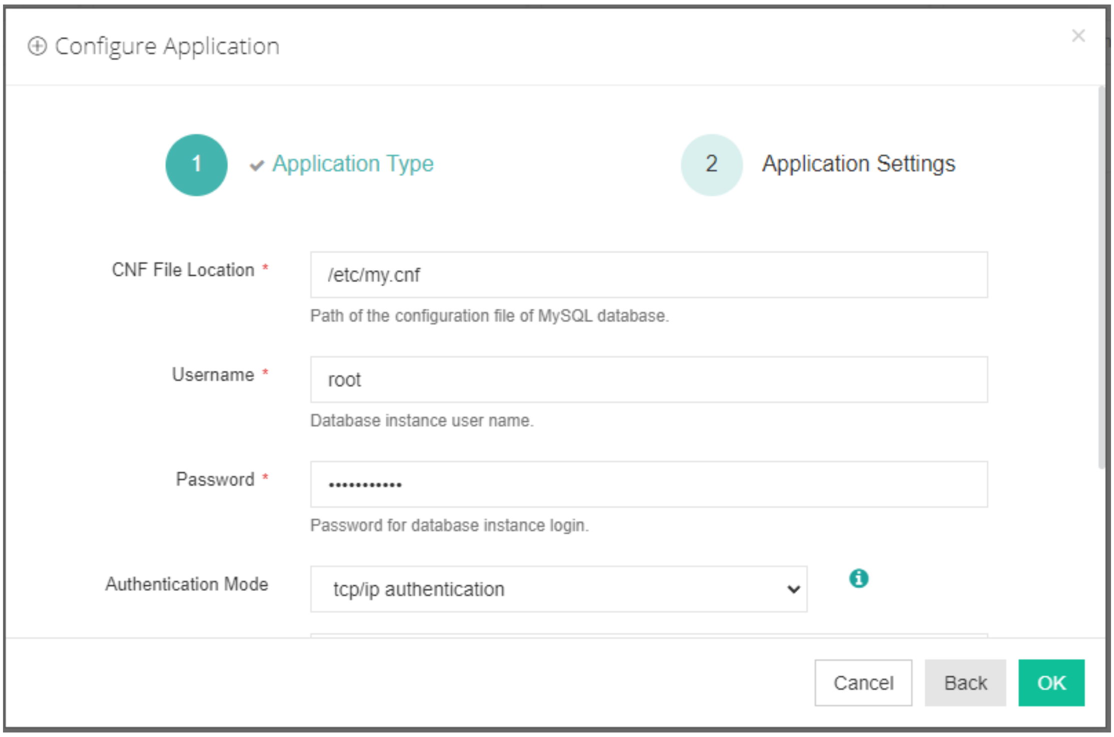
Notice

1. License: select license module and click on **License** button.
2. Unlicense: select license module and click on **Unlicense** button.
3. You can batch license/unlicense agents with the same license module.

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 MariaDB database server, users have to **license** the agent with database backup module.
When done installation and licensing, please open Vinchin Backup Server web console and go to **Resources** > **Agents** page, find the target agent, click on **Options** and then select **Application** to configure application settings for database backup.
Click on **Configure Application** button to configure the application settings.
In the **Application Type** dropdown list, please select **MariaDB** and then click on **Next**.
In the Applications Settings screen, please configure the following settings.



CNF File Location *: /etc/my.cnf
Path of the configuration file of MySQL database.

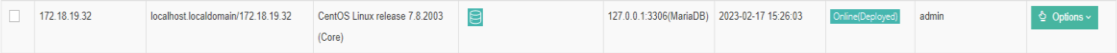
Username *: root
Database instance user name.

Password *: •••••••••••
Password for database instance login.

Authentication Mode: tcp/ip authentication

In the **CNF File Location** field, please type in the file path of MariaDB cnf file. Providing database administrator username and password. Vinchin provides two authentication modes: **tcp/ip authentication** and **sock file authentication**. If connecting to MySQL via tcp/ip authentication, default IP address is 127.0.0.1, default port is 3306 (please fill the IP address and port based on actual situation). If connecting to MySQL via sock file authentication, the default host name is localhost, and the sock file path is filled in according to the actual situation. Leave the IP Address and Port number with default value and click on OK to complete the application configuration.

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



□	172.18.19.32	localhost.localdomain/172.18.19.32	CentOS Linux release 7.8.2003 (Core)		127.0.0.1:3306(MariaDB)	2023-02-17 15:26:03	Online(Deployed)	admin	Options

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

Before Backing Up MariaDB Database

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

```
show variables like ‘%log_bin%’;
```

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

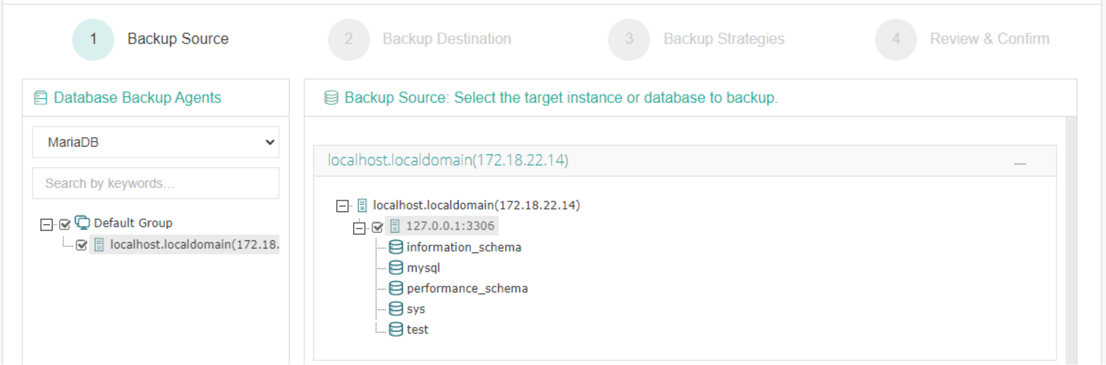
If binary logging is not enabled, it needs the database administrator to enable it.

Create Backup Job

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

Step 1: Backup Source

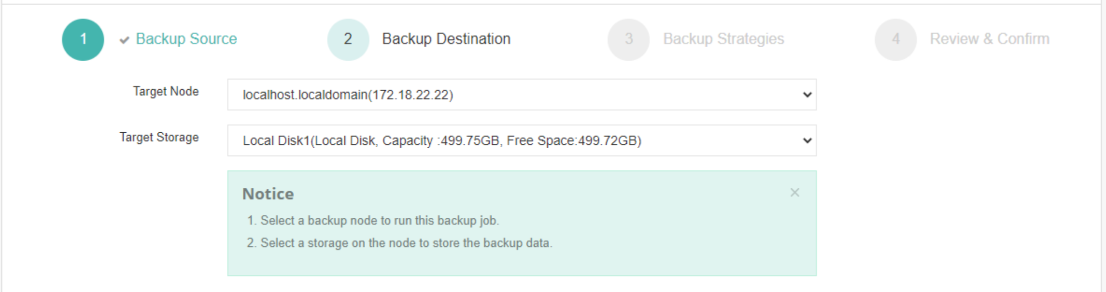
First select backup source from left column, then select MariaDB database instance you wish to backup, in the right column will show which instance you selected.



Backup Source: Select the target instance or database to backup.

Step 2: Backup Destination

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



Target Node: localhost.localdomain(172.18.22.22)

Target Storage: Local Disk1(Local Disk, Capacity :499.75GB, Free Space:499.72GB)

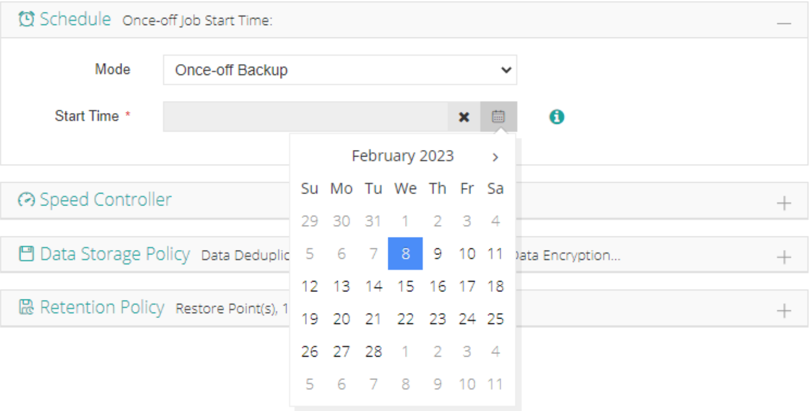
Notice

1. Select a backup node to run this backup job.
2. Select a storage on the node to store the backup data.

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

Step 3: Backup Strategies

In the General Strategy, you can configure the time schedule of the backup job, you can configure the job as a **Backup as Scheduled** job or a **Once-off Backup** job.
For a once-off backup job, the job will only run for once, and only full backup will be performed. You only have to appoint a time of when to start the backup job, in the **Start Time** field.



Schedule Once-off Job Start Time:

Mode: Once-off Backup

Start Time *

February 2023

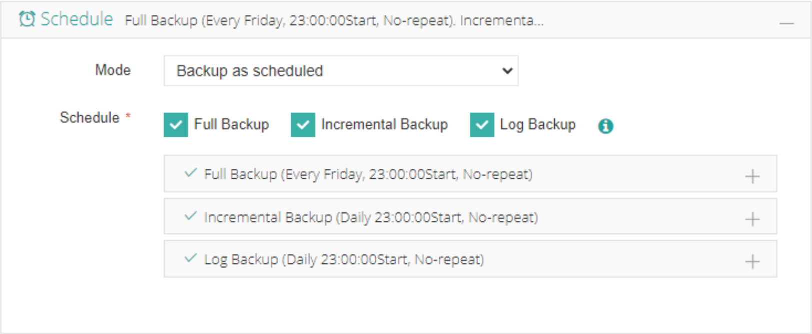
Su	Mo	Tu	We	Th	Fr	Sa
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	1	2	3	4
5	6	7	8	9	10	11

Speed Controller

Data Storage Policy Data Deduplic… ɔata Encryption…

Retention Policy Restore Point(s), 1

For backup job type, you can schedule Full Backup, Incremental Backup and Log Backup. Here we take these three backups as an example. Please set the backup mode and backup schedule as per your actual demands.



Schedule Full Backup (Every Friday, 23:00:00Start, No-repeat). Incrementa…

Mode: Backup as scheduled

Schedule *: ☑ Full Backup ☑ Incremental Backup ☑ Log Backup

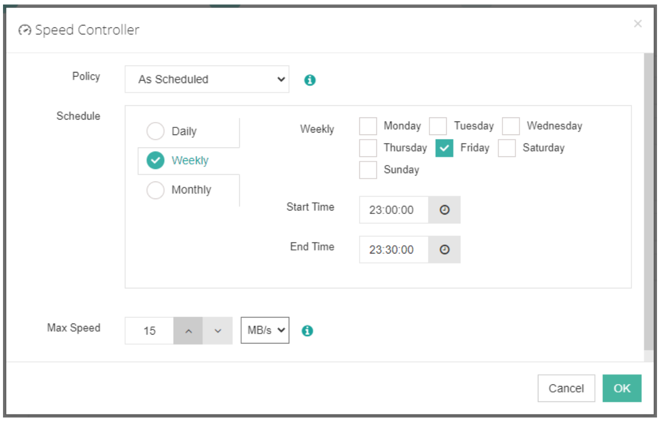
✓ Full Backup (Every Friday, 23:00:00Start, No-repeat)

✓ Incremental Backup (Daily 23:00:00Start, No-repeat)

✓ Log Backup (Daily 23:00:00Start, No-repeat)

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.



Speed Controller

Policy: As Scheduled

Schedule: ○ Daily ● Weekly ○ Monthly

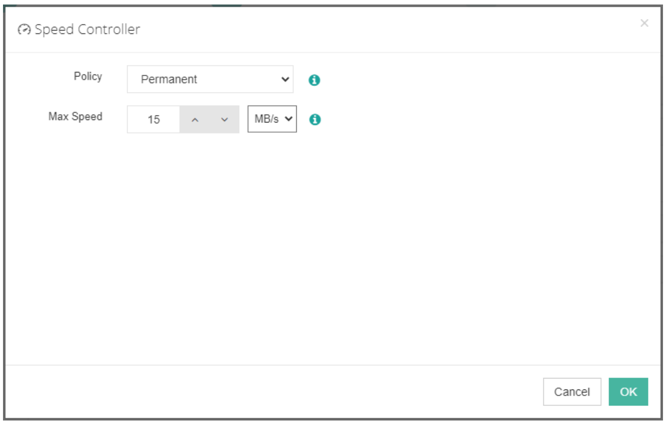
Weekly: □ Monday □ Tuesday □ Wednesday □ Thursday ☑ Friday □ Saturday □ Sunday

Start Time: 23:00:00

End Time: 23:30:00

Max Speed: 15 MB/s

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



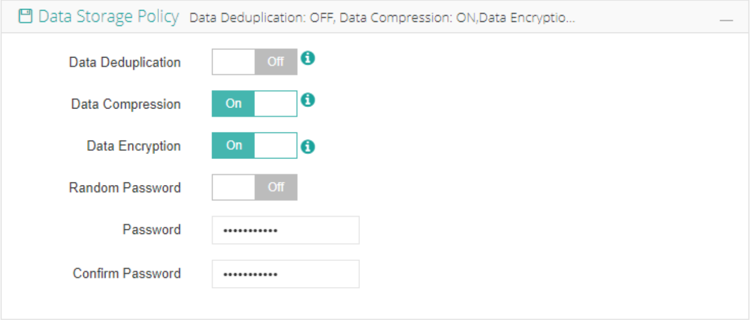
Policy: Permanent

Max Speed: 15 MB/s

There are 3 options in Data Storage Policy section, Data Deduplication, Data Compression and Data Encryption.

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

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



Data Deduplication: OFF, Data Compression: ON,Data Encryptio...

Data Deduplication: Off

Data Compression: On

Data Encryption: On

Random Password: Off

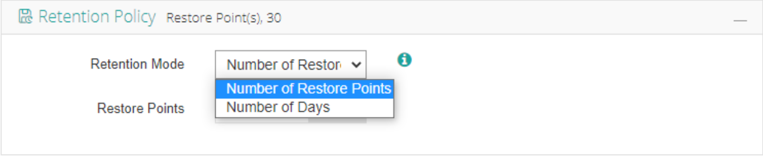
Password: •••••••••••

Confirm Password: •••••••••••

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.



Restore Point(s), 30

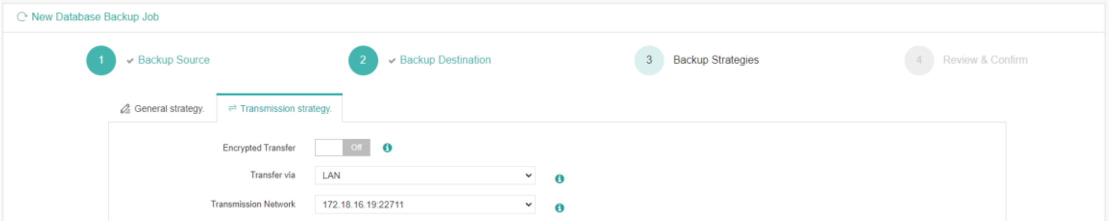
Retention Mode: Number of Restor

Restore Points

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, and you can set the transmission network for data transfer.


New Database Backup Job

1 ✓ Backup Source — 2 ✓ Backup Destination — 3 Backup Strategies — 4 Review & Confirm

General strategy | Transmission strategy

Encrypted Transfer: Off

Transfer via: LAN

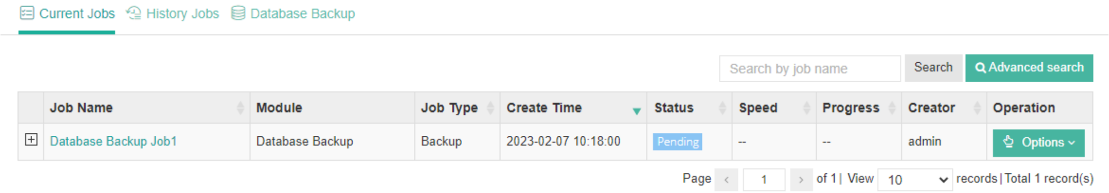
Transmission Network: 172.18.16.19:22711

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

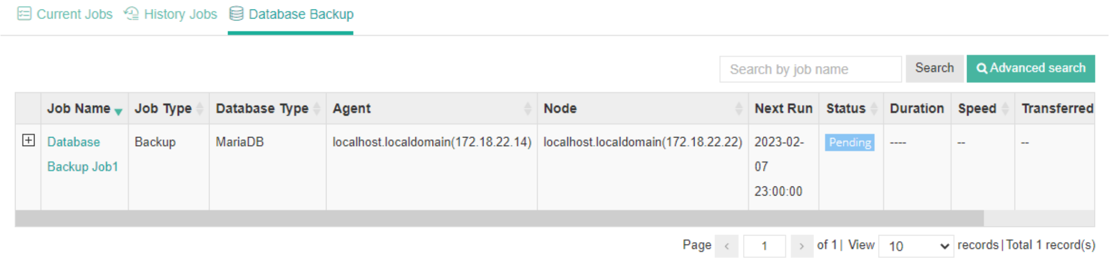
Once a database backup job had been created, you will be redirected to the **Monitor Center** > **Jobs** page.



	Job Name	Module	Job Type	Create Time	Status	Speed	Progress	Creator	Operation
⊞	Database Backup Job1	Database Backup	Backup	2023-02-07 10:18:00	Pending	--	--	admin	Options

Page 1 of 1 | View 10 records | Total 1 record(s)

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.



	Job Name	Job Type	Database Type	Agent	Node	Next Run	Status	Duration	Speed	Transferred
⊞	Database Backup Job1	Backup	MariaDB	localhost.localdomain(172.18.22.14)	localhost.localdomain(172.18.22.22)	2023-02-07 23:00:00	Pending	----	--	--

Page 1 of 1 | View 10 records | Total 1 record(s)

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.

Before Restoring MariaDB Database

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

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

```
systemctl stop mariadb
```

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

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

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

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

Note

1. The above operations should be done by the MariaDB 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 MariaDB database services.

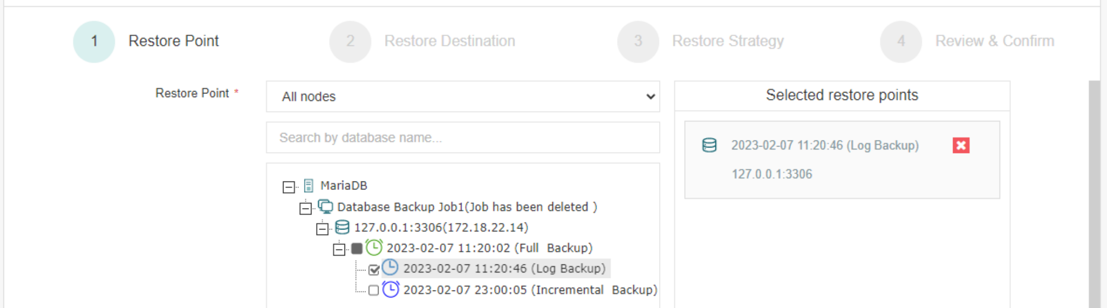
2. The restored data will be saved in the new data directory, database admin can use the restored data to create new database or modify the my.cnf file to start MariaDB database from the new data directory.

Create Restore Job

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

Step 1: Restore Point

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



Restore Point * All nodes

Search by database name...

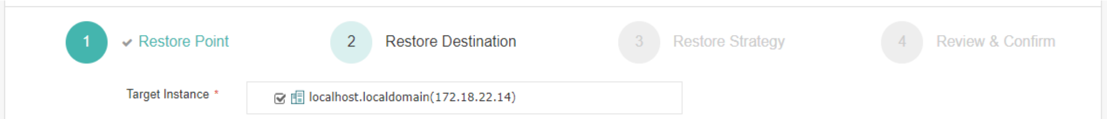
- MariaDB
  - Database Backup Job1(Job has been deleted)
    - 127.0.0.1:3306(172.18.22.14)
      - 2023-02-07 11:20:02 (Full Backup)
        - ☑ 2023-02-07 11:20:46 (Log Backup)
        - □ 2023-02-07 23:00:05 (Incremental Backup)

Selected restore points

2023-02-07 11:20:46 (Log Backup)
127.0.0.1:3306

Step 2: Restore Destination

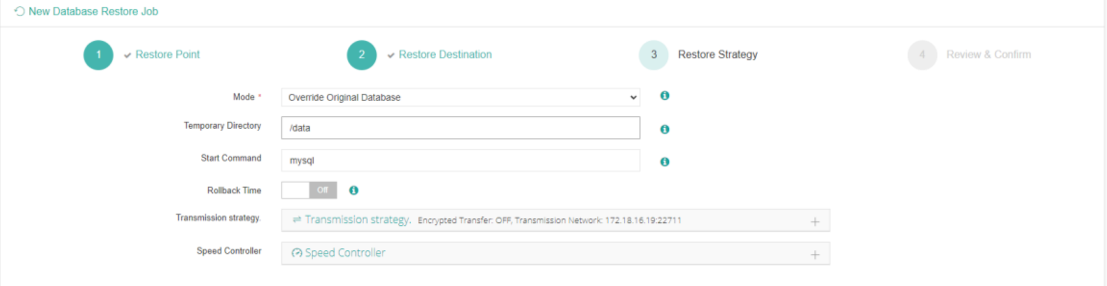
After selecting restore point, select **Target Instance** to restore to.



Target Instance * ☑ localhost.localdomain(172.18.22.14)

Step 3: Restore Strategy

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



Mode * Override Original Database

Temporary Directory /data

Start Command mysql

Rollback Time Off

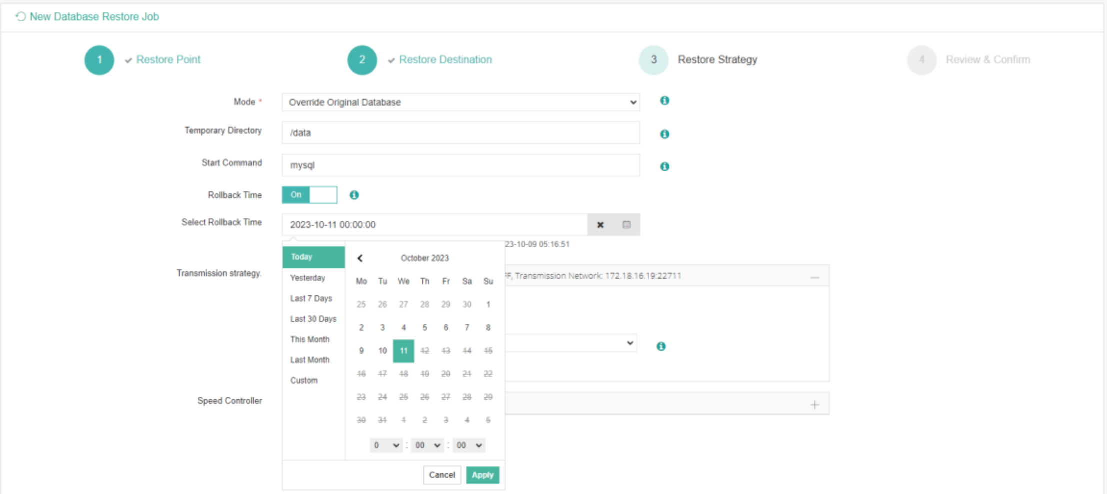
Transmission strategy. Transmission strategy. Encrypted Transfer: OFF, Transmission Network: 172.18.16.19:22711

Speed Controller Speed Controller

Note

If you use log backup point to override original database, MariaDB service will auto restart, no need to manually start MariaDB service. The [Start Command] is 'mysql' by default. It will be used to restart database service. You need to change it to the service name of your environment instance. For example: this is a MariaDB, fill in the service name as 'mariadb'. Then the command 'service mariadb restart' will execute.

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



Mode *: Override Original Database

Temporary Directory: /data

Start Command: mysql

Rollback Time: On

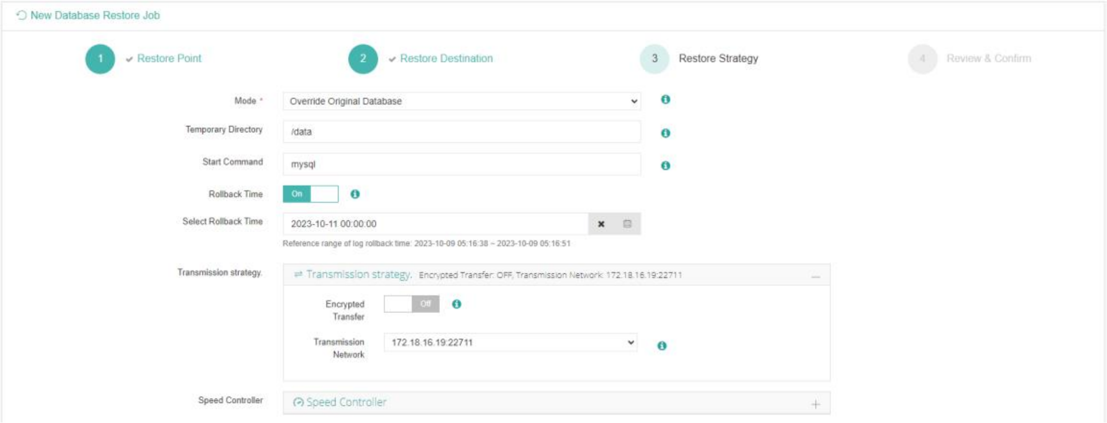
Select Rollback Time: 2023-10-11 00:00:00

23-10-09 05:16:51

Transmission strategy: F, Transmission Network: 172.18.16.19:22711

Speed Controller

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



Mode *: Override Original Database

Temporary Directory: /data

Start Command: mysql

Rollback Time: On

Select Rollback Time: 2023-10-11 00:00:00

Reference range of log rollback time: 2023-10-09 05:16:38 ~ 2023-10-09 05:16:51

Transmission strategy: Transmission strategy. Encrypted Transfer: OFF, Transmission Network: 172.18.16.19:22711

Encrypted Transfer: Off

Transmission Network: 172.18.16.19:22711

Speed Controller: Speed Controller

Same as database backup, while restoring databases, you can configure **Transmission Strategy** to encrypt the data transmission channel and set the transmission network. 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.

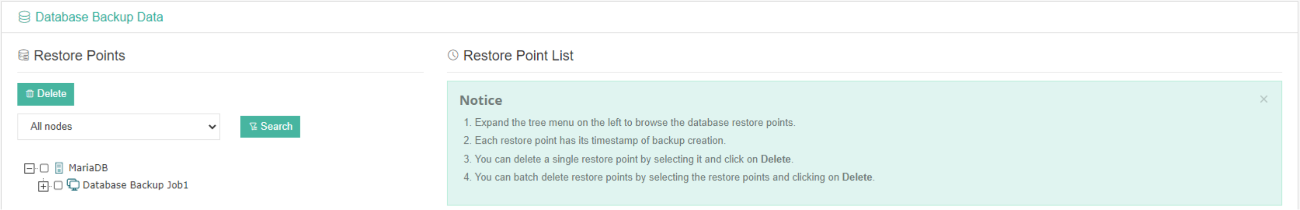
Once the job has been created, you'll be redirected to the **Monitor Center** > **Jobs** page.

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.

Managing Backup Data

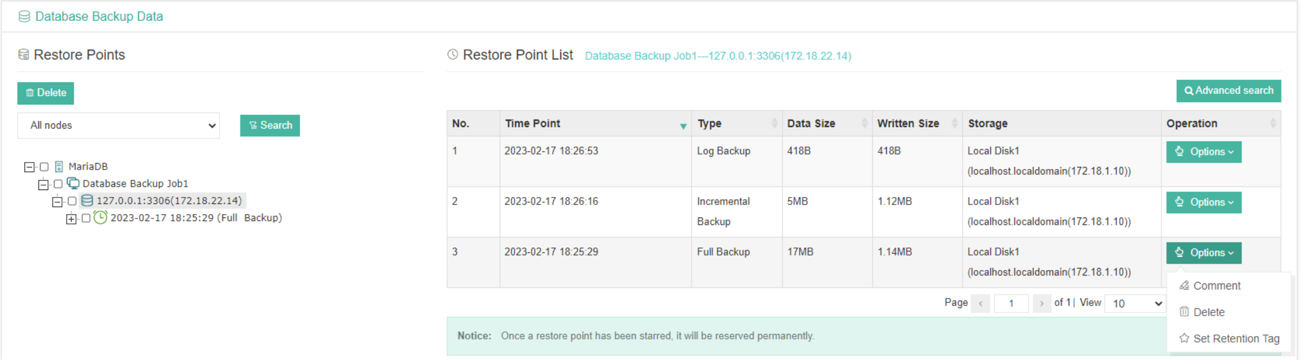
The database backup data can be managed from **Physical Backup** > **Database Backup** > **Backup Data** page.



Notice

1. Expand the tree menu on the left to browse the database restore points.
2. Each restore point has its timestamp of backup creation.
3. You can delete a single restore point by selecting it and click on **Delete**.
4. You can batch delete restore points by selecting the restore points and clicking on **Delete**.

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



No.	Time Point	Type	Data Size	Written Size	Storage	Operation
1	2023-02-17 18:26:53	Log Backup	418B	418B	Local Disk1 (localhost.localdomain(172.18.1.10))	Options
2	2023-02-17 18:26:16	Incremental Backup	5MB	1.12MB	Local Disk1 (localhost.localdomain(172.18.1.10))	Options
3	2023-02-17 18:25:29	Full Backup	17MB	1.14MB	Local Disk1 (localhost.localdomain(172.18.1.10))	Options

Notice: Once a restore point has been starred, it will be reserved permanently.

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

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

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

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