

Distributed Transactional Database

HotDB Server -

[Management Platform]

Function Manual

Version No. V2.5.6.1

Shanghai Hotpu Networks Technology Co., Ltd.

Dec. 2020

All rights reserved! Without the written consent of the company, no unit or individual is allowed to extract and copy the contents hereof in part or in whole, and disseminate them in any form.

Trademark statement

HotDB trademark of Hotpu is the registered trademark or trademark of our company or its affiliated company which is legally protected. Any infringement shall be investigated. Without the written permission of the company or the trademark owner, no unit and individual is allowed to use, copy, modify, disseminate, transcribe or bundling sell any part of this trademark in any form or for any reason. Any infringement of the trademark right of the company shall be investigated for legal liability.

Cautions

The products, services or features you purchase shall be subject to the commercial contracts and terms of Shanghai Hotpu Networks Technology Co., Ltd. The final interpretation right of the products, services or features in this document shall belong to Shanghai Hotpu Networks Technology Co., Ltd.

Shanghai Hotpu Networks Technology Co., Ltd.

Address: 603-605, Block A, SIM Technology building, No. 633, Jinzhong Road, Changning District, Shanghai

Postcode: 200050

Website: www.hotdb.com

Service email: service_hotdb@hotdb.cm

Service Tel: 021-5218 0789

Contents

1. New functions and features of Version 2.5.6.....	1
2. Preface	3
3. Instructions for use.....	4
3.1. Glossary.....	4
3.2. HotDB Management architecture	4
3.3. Access mode.....	5
4. Admin index.....	7
4.1. Cluster switching	7
4.2. Basic data.....	7
4.3. Statistics.....	9
4.4. Peak data	10
4.5. Running data	11
4.6. Configuration data	12
5. User management	14
5.1. User management table	14
5.2. Add user information.....	15
5.3. User password	17
5.4. Login history	17
6. Cluster management.....	19
6.1. Compute node cluster	19
6.1.1. Cluster management record	19
6.1.2. Add cluster	22
6.1.3. High availability switch	24
6.1.4. High availability reconstruction	28
6.1.5. Switching, removal and repair of IDC	33
6.1.6. IDC switching drill	33
6.2. Single Component Deployment	33
6.3. Deployment environment examination	34
7. Instance management.....	39

7.1. Instance management information.....	39
8. Audit logs	42
8.1. Manager operation.....	42
8.2. General user operation.....	43
8.2.1. Platform operation	44
8.2.2. Security protection	45
8.2.3 Management port operation	46
9. Tool.....	48
9.1. License management	48
9.1.1 Update license	48
9.1.2 Update record.....	63
9.2. Platform configuration data management	63
9.2.1 ConfigDB file management	64
9.2.2 Platform ConfigDB Status and Operation.....	65
9.2.3 Platform configuration backup data.....	67
9.2.4 Backup record & restore	69
9.2.5 Other instructions.....	71
10. Upgrade center	75
11. OEM management	83
11.1. Modify the system name	83
11.2. Modify the product logo	84
11.3. Retain the original product information.....	85
12. General user login.....	88
12.1. Login	88
12.2. Cluster selection.....	88
13. Home	91
13.1. Cluster security	91
13.2. Summary of important information.....	92
13.3. Data node throughput.....	93
13.4. Event notice	93
13.5. Cluster throughput.....	94

13.6. Overview of data amount and throughput	94
13.6.1. Client throughput today	94
13.6.2. Back-end throughput today	95
13.6.3. New data amount today	95
13.6.4. Total data amount	96
13.7. Sharding grade	96
13.8. TOP 10 table today	97
13.9. Throughput rate	98
13.10. Cluster overview	98
14. Configuration	102
14.1. Node management	102
14.1.1. Add data source group	104
14.1.2. Add node	106
14.1.3. Master/slave setup	109
14.1.4. Switching rule	113
14.1.5. Heartbeat paused	115
14.1.6. Master/Slave switch	117
14.1.7. Data node management	119
14.1.8. Enable/Disable data source	120
14.2. LogicDB	123
14.2.1. Add LogicDB	123
14.2.2. Edit LogicDB	124
14.2.3. Delete LogicDB	125
14.3. Table configuration	125
14.3.1. Add new table configuration	126
14.3.2. Add new child table	129
14.3.3. Edit table configuration	130
14.3.4. Table record export	132
14.3.5. Delete table	133
14.3.6. Historical compatibility description	133
14.4. Sharding function	134
14.4.1. MATCH	135
14.4.2. RANGE	138
14.4.3. ROUTE	140
14.4.4. SIMPLE_MOD	143

14.4.5. CRC32_MOD	145
14.4.6. Edit sharding function	147
14.4.7. Delete sharding function	148
14.4.8. Replicate sharding function	148
14.4.9. Special description	149
14.5. Config checking	149
14.6. Cluster metadata backup and restore	157
14.6.1. Cluster metadata backup	157
14.6.2. Cluster metadata restore	159
14.7. Parameter configuration	160
14.7.1. Basic functions and notes	160
14.7.2. Enable master configDB	163
14.8. Database user management	165
14.8.1. Query by username	165
14.8.2. Add users	165
14.9. Server	171
14.9.1. Obtain server IP automatically	171
14.9.2. Add server	173
14.9.3. Configure SSH	174
14.9.4. Other description	175
15. Monitoring	176
15.1. Logic Topological Graph	176
15.1.1. Topological graph component description	176
15.1.2. Interface adjustment function	182
15.1.3. 2.5D topological graph	183
15.2. Physical topological graph	184
15.3. Monitoring panel	188
15.3.1. Add and set monitoring item	188
15.3.2. Monitoring panel description	189
15.3.3. Data increment prediction	193
15.3.4. Cluster resource monitoring	198
15.4. Monitoring management	208
15.4.1. Instructions before use	209
15.4.2. Monitoring command description	210
15.5. JOIN correlation analysis	221

15.5.1. Prerequisites for use	222
15.5.2. JOIN correlation diagram	222
15.5.3. JOIN correlation details	225
16. Report	228
16.1. Cluster data volume	228
16.1.1. Graph mode	228
16.1.2. Table mode	233
16.1.3. Statistical mode descriptions	234
16.2. Compute node throughput	234
16.2.1. Graph mode	234
16.2.2. LogicDB Dimension Throughput Report	239
16.2.3. Table Dimension Throughput Report	239
16.2.4. Table mode	240
16.3. Data node throughput	240
16.3.1. Graph mode	241
16.3.2. Table mode	245
16.4. Compute node connection	246
16.4.1. Graph mode	246
16.4.2. Table mode	251
17. Management	252
17.1. Data backup	252
17.1.1. Introduction to HotDB Backup	252
17.1.2. Installation description	252
17.1.3. Manual backup	253
17.1.4. Backup plan	257
17.1.5. Special instructions for backup	259
17.1.6. Backup log description	261
17.2. Data restore	262
17.2.1. Start restore	263
17.2.2. Instructions for executing data restore	265
17.2.3. Recovery task details	266
17.2.4. Special instructions for data restore	267
17.2.5. Recovery log description	268
17.3. Data source migration	269

17.3.1. Data source migration preparation	269
17.3.2. Source data node and target data source.....	271
17.3.3. Data source migration preparation	272
17.3.4. Pre-check.....	273
17.3.5. Data source migration.....	275
17.4. Table structure change	275
17.4.1. Ordinary DDL.....	276
17.4.2. Online DDL	277
17.5. View SQL routing plan	278
17.6. Online change of sharding plan	279
17.6.1. Online change of sharding plan	279
17.6.2. Start modification task	281
17.6.3. Fill in modification plan	282
17.6.4. Modification plan pre-detection	282
17.6.5. Modification plan confirmation	284
17.6.6. Start modification in batches	285
17.6.7. Sharding plan modification exception handling.....	287
17.7. Table Recycle Bin	292
17.7.1. Premise for use	292
17.7.2. Table Recycle Bin.....	293
17.7.3. Table restore	293
17.7.4. Table deletion	294
17.7.5. Table batch restore	295
17.7.6. Table batch deletion	297
17.7.7. Special instructions for Table Recycle Bin.....	298
17.7.8. History record.....	300
17.7.9. Delete history record.....	301
18. Security	302
18.1. White List.....	302
18.2. SQL Firewall	303
18.3. Password security management.....	305
18.3.1. Database user password	305
18.3.2. Data source password	306
19. Detection	309

19.1. Master/Slave data consistency detection	309
19.1.1. Start a detection.....	309
19.1.2. Periodical plan	311
19.1.3. Notes.....	312
19.2. Global table data detection.....	312
19.2.1. Start a detection task.....	313
19.2.2. View detection details.....	313
19.2.3. Data restore.....	315
19.2.4. Periodical plan	316
19.3. Table structure & index detection	316
19.3.1. Start a detection.....	317
19.3.2. Page description	317
19.3.3. Table structure details	321
19.4. Sharding grade.....	322
19.4.1. Description of grade dimensions	322
19.4.2. Record export	323
19.5. Sharding plan recommendation	324
19.5.1. Start a recommendation	324
19.5.2. Sharding plan recommendation	327
19.5.3. Influencing factors of sharding plan recommendation	328
19.6. Sharding route detection	328
19.6.1. Start a detection.....	329
19.6.2. Detection record details	329
19.6.3. Route abnormal details	330
19.7. Data unique constraint detection	331
19.7.1. Start a detection.....	331
19.7.2. Detection record details	332
20. Events.....	334
20.1. History events	334
20.1.1. Alert type description	334
20.2. Compute node log	336
20.2.1. View log	337
20.2.2. Log acquisition description.....	337
20.2.3. Log type description	338
20.3. Slow Query Log Analysis	342

20.3.1. Slow query log record description	343
20.3.2. SQL Performance Tracking	348
20.4. Notification strategy.....	349
20.4.1. Add notification strategy.....	350
20.4.2. Description of monitoring items.....	352
20.5. Audit logs.....	364
20.5.1. Platform operation	365
20.5.2. Security protection	366
20.5.3. Management port operation	367
20.5.4. Audit log setting	368
21. Setting.....	369
21.1. Periodical detection setting	369
21.1.1. Periodical detection setting.....	369
21.1.2. Periodical plan	369
21.2. Topological graph alert setting.....	370
21.3. Monitoring panel setting	371
21.4. Notification setting.....	374
21.4.1. Email sender setting	374
21.4.2. Notification frequency setting.....	377
21.5. Audit logs setting	378
22. Tool.....	379
22.1. Data collection	379
22.2. License management	382
22.3. Business data reporting	382
22.4. Intelligent inspection	391
23. Navigation	392
23.1. Version	392
23.2. Compute node cluster switching	393
23.3. Help	394
23.3.1. Tutorial	394
23.4. Reload	394
23.4.1. Reload instructions	394
23.4.2. Function exercise	396
23.4.3. Reload triggering scenario	398

23.5. Notice	399
23.6. Theme	399
23.7. User information	400
23.7.1. Switch user view	400
23.7.2. Modify user information	400
23.8. Sign out	402
23.9. Language	403
23.10. HTTPS secure access	403
23.10.1. Start with default configuration	403
23.10.2. Customized HTTPS configuration	404

1. New functions and features of Version

2.5.6.1

This chapter will briefly introduce the newly added or optimized functions in HotDB Management V2.5.6. Please go to the specific function menu for details.

- Add new functions including [visualized switching, repair, removal of IDC and IDC switching drill](#) to improve the reliability and ease of use of IDC operation and reduce the operation and maintenance cost of cross-IDC operation;
- Add the function of [Intelligent Inspection](#), which helps with the cluster inspection in database;
- Add the function of [Platform Configuration Data Management](#). The management platform ConfigDB is able to support high availability switching and backup and restore of ConfigDB;
- Add functions such as "Disable", "Comment", "Online time" in [User Management](#);
- Optimize the configuration function of some sharding functions, so that the [MATCH](#) and [ROUTE](#) type are able to support prefix/infix/suffix matching, and the [RANGE](#) type to support the maximum and minimum boundary value matching;
- Optimize the function of [Upgrade Center](#) to match the new JDK version in v.2.5.6 and the self-developed license;
- Optimize the function of [Add New Table Configuration](#): when adding new table configuration, all data nodes under the LogicDB will be associated by default;
- Optimize the function of [Alert Type](#) in History Events, and add cluster election or switching reminders;
- Optimize the function of [Update License](#) to adapt to the new self-developed encrypted authorization plan;
- Optimize the [master/slave consistency detection](#), and give a prompt to the tables that are not configured with switching functions or whose data sources are unavailable;

- Optimize the function of [Config Checking](#), add checking item of whether to configure switching functions, and give warnings for the data nodes with replication relations that are not configured with switching functions;
- Add the identification of whether the data of data sources are consistent on the data nodes in the [Logic Topological Graph](#);
- Optimize the [high availability switching](#) function of data source, and do compatibility processing for master_delay replication latency. Add "switching" button, you can cancel the switching task halfway via the button;
- The [Topological Graph Alert Setting](#) is compatible with master_ delay configuration to make it within the aletrt range. Besides, add "Reset" button to the Topological Graph Alert Setting and Monitoring Panel Setting to restore the default configuration;
- Optimize the page of [Compute Node Cluster Management](#) to unfold/hide more deployment info and improve the page access rate;
- Optimize the function of [data unique constraint detection](#) to make it compatible with prefix unique index;
- Set the entrance for data sharding route periodical detection plan, data unique constraint periodical detection plan in the [Periodical Plan](#) of the management platform;
- Optimize the [user privilege](#) table page, so that the privilege info of LogicDB can be directly seen on the page;
- Optimize the function of [OEM Management](#), remove the original menu, and access it by hyperlink (also applicable to v.2.5.5);
- Enhance the password strength of [database users](#) (the password of database users shall be no less than 8 digits and must be composed of numbers and letters).
- 增加管理平台服务授权管理功能，可限制可用计算节点集群组数和每组计算节点可用计算节点个数。

批注 [11]:

2. Preface

This document describes the operation of the distributed transactional database platform (hereinafter referred to as HotDB Management). HotDB Management is a configuration, monitoring and O&M tool used with the distributed transactional database (HotDB Server). It is simple and easy to use, and can easily configure the database, table and sharding function of distributed transactional database and provide multi-dimensional monitoring information and abundant O&M functions to help users reduce the usage threshold and improve work efficiency.

This document mainly describes the configuration operation process and related functions of HotDB Management, aiming at reducing the difficulties in the use process and reducing the communication costs. This document is prepared based on the current identification version of HotDB Management and provides descriptions based on the normal deployment environment of HotDB Server and HotDB Management. Some screenshots contain the HotDB Management versions and the detailed differences which need no special attention, and the version number described in this document shall prevail. This document can be read in conjunction with the supporting *Distributed Transactional Database HotDB Server [Standard] Function Manual* to quickly understand key function points.

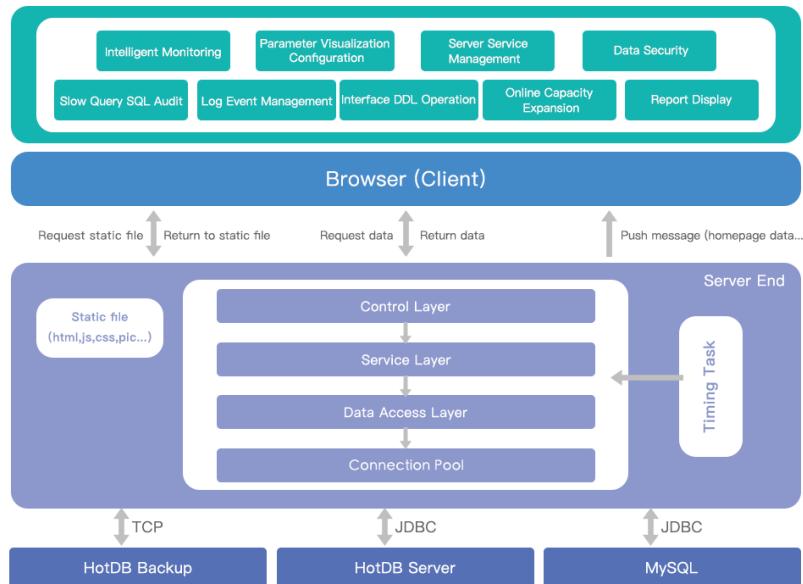
3. Instructions for use

3.1. Glossary

HotDB Management contains many special terms. Please read the *Distributed Transactional Database HotDB Server [Glossary] Function Manual* before use to be familiar with various technical terms which helps to understand and use HotDB Management.

3.2. HotDB Management architecture

HotDB Management is a B/S structure management and control product. The bottom layer connects compute nodes of the distributed transactional database by JDBC mode to provide configuration, monitoring and O&M services for compute nodes. It connects HotDB Management ConfigDB by JDBC mode, and connects distributed transactional database backup program by TCP/IP mode. The function data interaction of browser is transmitted by JSON mode, and the business logic support is provided by HotDB Management service layer.



3.3. Access mode

Manual deployment of HotDB Management is required before use. For detailed deployment instructions, please read the [Distributed Transactional Database HotDB Server \[Installation and Deployment\] Function Manual](#).

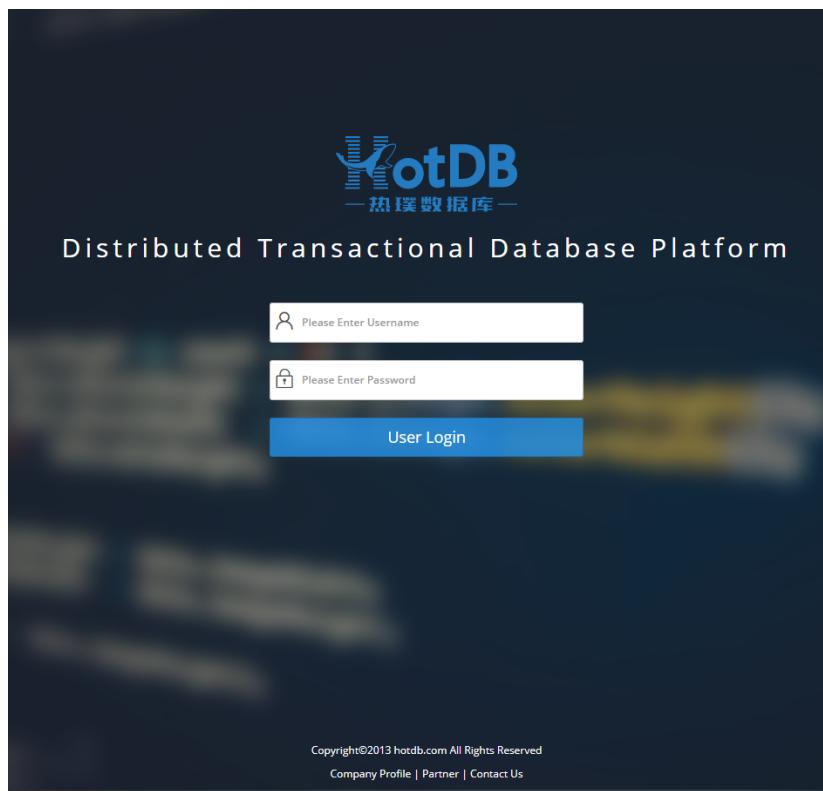
For deployed and launched HotDB Management, the access address can be entered in the browser for login access.

Browser requirements: Chrome 49 or Firefox 61 and above is recommended.

Access address format: `http://` HotDB Management Server IP: Access port /login.html

Example: <http://192.168.200.201:3324/login.html>

HotDB Management login page appears after successful connection.



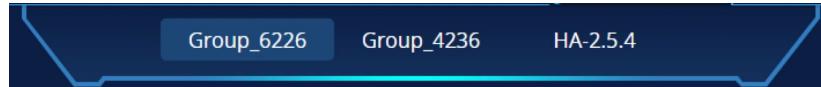
Login user: The initial login can use the default built-in management user (**account: admin** **password: admin**) of HotDB Management to enter the management interface.

4. Admin index

The admin index page mainly provides the manager user with a global perspective to view the managed cluster basic data, running data, peak data, statistics and configuration data, etc.

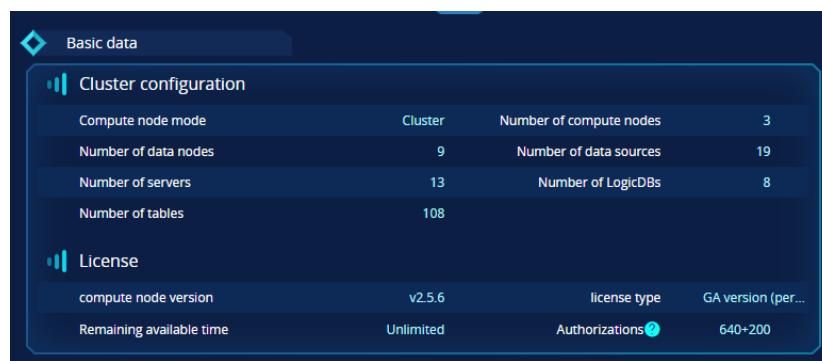


4.1. Cluster switching



- The manager user can view the basic data of all compute node clusters with "monitoring enabled" on the index page
- You can switch to the corresponding page of cluster by clicking the tabs of different cluster names. When there are more than 3 clusters displayed, you can click the left and right buttons to turn pages of the remaining clusters.

4.2. Basic data



The screenshot shows the 'Basic data' section of the HotDB Management Platform. It includes two main sections: 'Cluster configuration' and 'License'.

Cluster configuration:

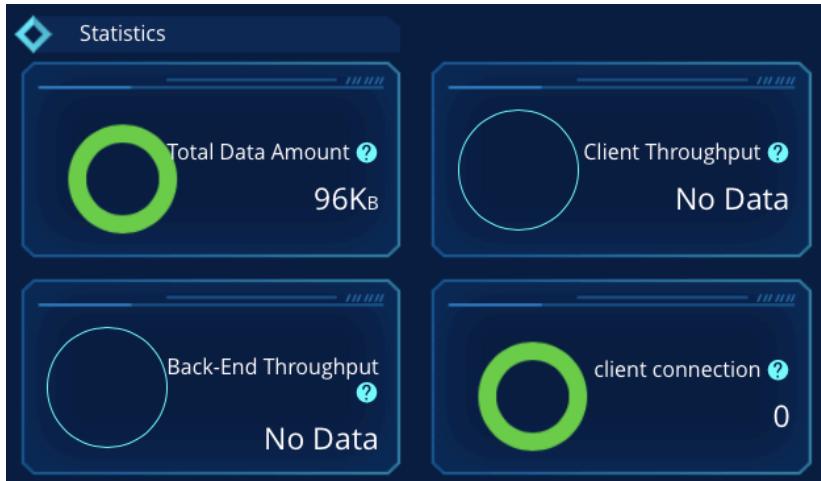
Compute node mode	Cluster	Number of compute nodes	3
Number of data nodes	9	Number of data sources	19
Number of servers	13	Number of LogicDBs	8
Number of tables	108		

License:

compute node version	v2.5.6	license type	GA version (per...
Remaining available time	Unlimited	Authorizations 	640+200

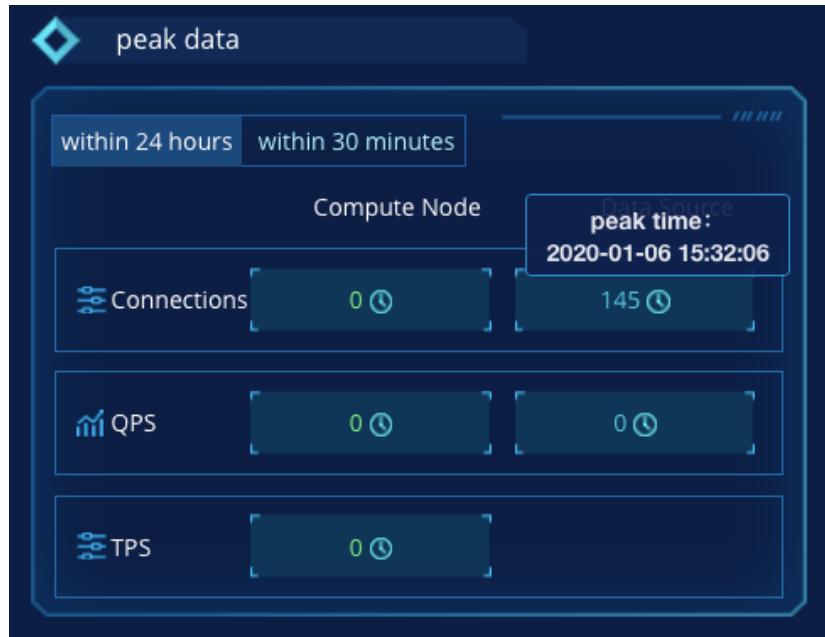
- The basic data includes the cluster configuration and license information, etc.
- Note:
 - The table quantity is the total quantity of all created and not created tables in the current cluster.
 - If the license information type is permanent, the remaining available time is not displayed. If it is a beta version and the remaining time is less than 7 days, an alert will be given in red.
 - Authorizations include the number of available data nodes and the number of available LogicDBs, among which the limit of number of ConfigDBs is added in v.2.5.6 and above.

4.3. Statistics



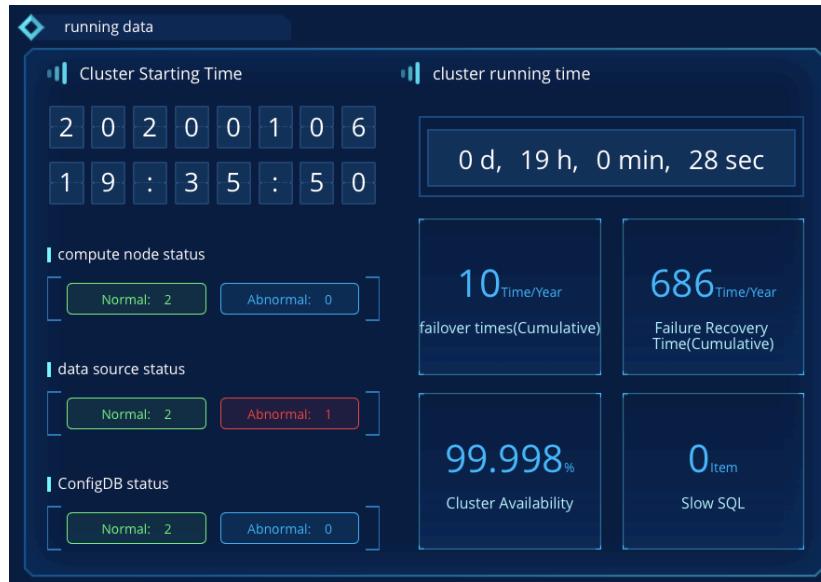
- Statistics includes total data amount, client throughput, back-end throughput and client connection. For the data acquisition of the total data amount, client throughput and back-end throughput, please refer to the corresponding content on [the home page of general users](#).
- Total data volume: the value is the total data volume of the current cluster, and the pie chart on the left is the proportion of data volume of TOP10 LogicDB.
- Client throughput: the data displayed is the throughput of compute nodes since midnight of the day. The pie chart on the left calculates the proportions according to the operation type (SELECT/UPDATE/DELETE/INSERT/OHTHER) .
- Back-end throughput: the data displayed is the throughput of data nodes since midnight of the day. The pie chart on the left calculates the proportions according to the operation type (SELECT/UPDATE/DELETE/INSERT/OHTHER) .
- Client connection: it displays the number of front-end connections of the current compute node. The pie chart on the left shows the connection proportion of TOP10 applications (differentiated by client IP address) with the longest connection durations in a week.

4.4. Peak data



- On the index page, you can view the cluster peak data within 24 hours and within 30 minutes, mainly with two objects: compute node and data source, and three dimensions: connections, QPS and TPS.
- Peak data includes the highest peak data and the time point within the selected time range. If there are multiple peak data, the latest peak data will be taken.
- The management platform collects the peak data on the compute node and data source once a minute for a scheduled task. The data is saved for 24 hours by default, and is automatically cleaned when it expires.
- When the compute node cluster is a single node or a master/slave node, the peak data of the compute node only takes data of the current active node; if it is a multi-node cluster, the peak data is the sum of all the compute nodes.
- By default, the peak data of the data source is the sum of the data of all data sources (excluding the slave) in the cluster. The data source has no TPS data, and the dimension is empty.

4.5. Running data



- Under the running data, cluster starting time, cluster running time, failover times (cumulative), failure recovery time (cumulative), cluster availability, slow SQL are consistent with [the home page of general users](#).
- The compute node status shows the number of compute nodes running normally (the connection of the management port is normal) and abnormally in the current cluster. Green is for the normal compute nodes; red and blue are for the abnormal compute nodes, among which red will be displayed when the number of exceptions is greater than 0, and blue when there is no exception.
- The data source status shows the number of data sources running normally (data sources which can be connected normally and whose status is not set as unavailable) and abnormally in the current cluster. The color depends on the status. For details, please refer to the relevant descriptions in the compute node status part.
- ConfigDB status shows the number of ConfigDBs running normally or abnormally in the current cluster compute nodes.

4.6. Configuration data

◆ configuration data				
category	parameter name	value	parameter name	value
Management platform	Periodical system detection	Enable Part	White List	OFF
	Mail notification	Enable All	SQL Firewall	OFF
	Whether to adopt XA transaction	No	sql execution timeout time	3600(s)
	Whether to enable heartbeat	Yes	Timeout time of blocked write operation in front-end connection	10(s)
	Global auto-incremental serial number	Enable the global auto increment	Deadlock detection period	3000(ms)
	Whether to enable master-slave delay detection	Yes	Maximum connections at the front end	5000
Compute Node	Whether to account SQL execution	No	Maximum connections at the user front end	4900
	Whether to enable Data Source Current Limiting	Yes	The number of limited concurrency of high memory consumption statement	32

- Configuration data mainly shows the configuration of some key parameters including management platform, compute node and data source.
- For the parameter configuration display of the management platform, please refer to the corresponding parameter explanation on [the home page of general users](#). When the management platform parameters are not enabled, the page will alert with red font, and if not all of them are enabled, the page will alert with orange font.
- The parameters of the compute node mainly come from the settings of the function page "[Parameter Configuration](#)". Different clusters may display different parameters due to different versions of compute nodes
- The parameters of the data source display the settings of all data source instance parameters in the cluster. If some data source instance settings are inconsistent, the page will alert with red font and display the inconsistent settings (at this time, it is recommended that the user timely modify the data source instance parameters with inconsistent settings)
- If some data source instances cannot be connected normally in the cluster, the parameter settings displayed do not include the data source instances that cannot be connected.

- The parameters of the management platform and the compute node are obtained in real time from the ConfigDB and the server.xml file when refreshing the page; the parameters of the data source are detected every hour by the regular task of the management platform, and the detected data is stored in the management flat memory. When the admin index page is refreshed, the configuration of data source parameters is obtained from the latest detection results of memory.

5. User management

The users managed by this function are the users using the HotDB Management platform. The “User Management” function can be used to add, modify, delete and record platform users.

5.1. User management table

The user management table is the platform user record that has been added by the current HotDB Management. The fuzzy search of user name and user info and the search of user status can be performed by the search box in the upper left corner.

List field description

- Username: Username for login to the HotDB Management account
- Role: User-assigned roles include manager users and general users
- Compute Node Cluster Privilege: The user-assigned compute node cluster privilege. Possession of privilege means that the compute node cluster can be accessed or controlled.
- Status: including Online, Offline and Disabled (Note: when logging in two different users using the same browser successively, the info of the second user will cover the first one, that is, the first user status will become offline).
- Last login time: records the last login time of the user. If there is no login record, it will be blank. Click "last login time", it will switch to the user login page.
- Comment: displays the comments entered by users when adding or editing.
- Operation: “ Disable”, “Enable”, “Reset password”, “Edit” and “Delete” operations of users can be performed. The admin user cannot perform “Disable” and “Delete”.

User Management								
User Management		Compute Node Cluster Privilege			Operation			
Username	Role	0005-10C-Bank (Control)	0005-LoadBalancing_Bank (Control)	0005-10C-Bank (Control)	Status	Last login time	Remark	
zhufei	Manager Users	0005-LoadBalancing_Bank (Control)	0005-10C-Bank (Control)	0005-10C-Bank (Control)	Offline	2020-12-27 22:35:17		
HSC	Manager Users	0005-LoadBalancing_Bank (Control)	0005-10C-Bank (Control)	0005-10C-Bank (Control)	Offline	2020-12-28 17:38:04		
zjrcb	Manager Users	0005-LoadBalancing_Bank (Control)	0005-10C-Bank (Control)	0005-10C-Bank (Control)	Offline	2020-12-09 09:44:20	渤海银行	
wl625	Manager Users	0005-LoadBalancing_Bank (Control)	0005-10C-Bank (Control)	0005-10C-Bank (Control)	Offline		深圳沃伦恒文万能	
sunlei	Manager Users	0005-LoadBalancing_Bank (Control)	0005-10C-Bank (Control)	0005-10C-Bank (Control)	Offline	2020-12-17 13:28:08	华夏	
trbank	Manager Users	0005-LoadBalancing_Bank (Control)	0005-10C-Bank (Control)	0005-10C-Bank (Control)	Offline	2020-12-04 12:35:21	天津农商行	
ehuatu	Manager Users	0005-LoadBalancing_Bank (Control)	0005-10C-Bank (Control)	0005-10C-Bank (Control)	Offline	2020-12-24 14:44:18	华夏	
synergisten	Manager Users	0005-LoadBalancing_Bank (Control)	0005-10C-Bank (Control)	0005-10C-Bank (Control)	Offline		渤海银行-北京分行	
yzsoftware	General Users	0005-LoadBalancing_Bank (Control)	0005-10C-Bank (Control)	0005-10C-Bank (Control)	Offline	2020-12-22 09:42:54	上海盈智信息科技有限公司	
KSaas	Manager Users	0005-LoadBalancing_Bank (Control)	0005-10C-Bank (Control)	0005-10C-Bank (Control)	Offline		KSaas(苏州)电子商务有限公司 北京分公司-盈智科技有限公司	

5.2. Add user information

Adding a platform user needs to fill in two parts of content information: User Basic Information and User Menu Privilege.

User Basic Information: including user account name, user role, compute node cluster privilege, etc.

- At present, there are no specific restrictions on user names, except that they cannot be duplicated with existing names.
- The default password of newly added user is service_hotdb@hotdb.com. When first logging into the management platform through the new account, the user will be required to change the password.
- Added users need to be assigned with specific roles, which are general users by default. The difference between the two types of roles is as follows:

General user: can only manage compute node clusters with existing privileges in the general user interface.

Manage user: can enter the management interface and manage compute node clusters with existing privileges in the general user interface. The interface views can be switched back and forth in the personal information dropdown box in the upper right corner.

- Assigning compute node cluster privileges to users means that the users can see the cluster and enter the cluster for management after logging into the general user

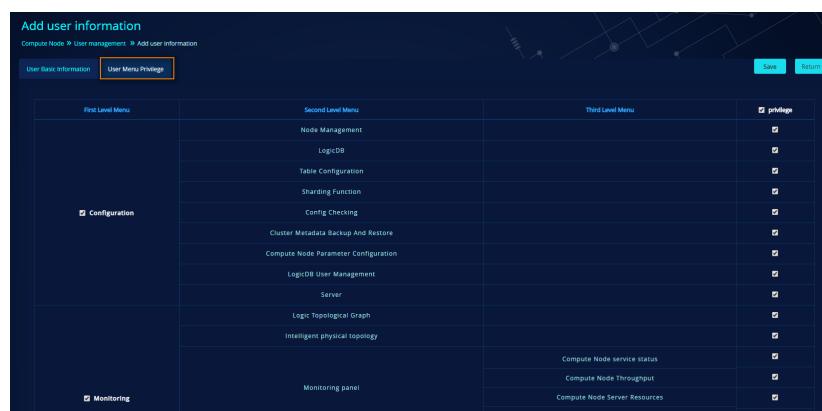
interface.

- There are two kinds of compute node cluster privileges: **access** and **control**. Users assigned with “access privileges” can only query after entering the cluster. All operations that affect the data will trigger a prompt of “insufficient privileges”. Users assigned with “control privileges” automatically have “access privileges” and can perform all operations on the cluster.
- you can enter "comments" on the adding and editing page. It is not required.

Compute Node Cluster Name	Access	Control
HotDB2.5.3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HotDB2.4.5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HotDB2.4.7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HotDB2.4.9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HA-231	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HA-251	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

User Menu Privilege: The menu privileges for users when they enter the cluster management through accessing the general user interface can be configured.

- When there is no special requirement, all menu privileges are granted by default. If it needs to mask the menu of a user, directly remove the checked item from the menu.
- If HotDB Management has been upgraded, the menu privileges of historical platform users need to be checked to see whether the menu privileges in the new version need to be assigned. **Currently, due to the menu function security problem, the new function menu privileges in the new version will not be assigned to historical users by default, and need to be added by the users.**



5.3. User password

Reset Password: The users can reset the password when forgetting the login password. The password can be reset with the “Reset Password” button in the operation column via the “User Management” interface, or by clicking “Reset Password” on the “Edit User Information” page.

Change Password: User password change will be required when the users first log into HotDB Management. Later change can be operated in “Personal Information - > Modify User Information” in the upper right corner of the page.

5.4. Login history

The login history displays the history of login and logout of the management platform by all users.

Function entry: User Management > Login history

User Management

User Management

Filter by Username	IP	Role	Compute Node Cluster Privilege	Status	IP	Last login time	Remark	Operation
zhufei		Manager Users	DB05_mh_Bank (Control) DB05_LoadBalancing_Bank (Control) DB05_SOC_Bank (Control)	Offline		2020-12-27 22:30:17		
HSC		Manager Users	DB05_LoadBalancing_Bank (Control) DB05_SOC_Bank (Control)	Offline		2020-12-28 17:38:04		
gpcba		Manager Users	DB05_LoadBalancing_Bank (Control) DB05_SOC_Bank (Control)	Offline		2020-12-29 09:44:23	申请银行	
wikidS		Manager Users	DB05_LoadBalancing_Bank (Control) DB05_SOC_Bank (Control)	Offline			后台迁移监控王立峰	
sunfei		Manager Users	DB05_LoadBalancing_Bank (Control) DB05_SOC_Bank (Control)	Offline		2020-12-17 13:29:08	外部	
crfbank		Manager Users	DB05_LoadBalancing_Bank (Control) DB05_SOC_Bank (Control)	Offline		2020-12-04 12:35:21	天津农商行	
zhuhui		Manager Users	DB05_LoadBalancing_Bank (Control) DB05_SOC_Bank (Control)	Offline		2020-12-26 14:44:18	新额度	

Login history

User Management > Login history

Filter by Username	IP	Role	Login time	Logout time	Login IP	Online time
yds		Manager Users	2020-12-28 09:34:48	online now	192.168.200.6	
augene		Manager Users	2020-12-28 23:54:50	2020-12-29 09:59:29	58.213.76.90	11:46min39s
guest_dbs_dba_limit		General Users	2020-12-28 22:24:22	2020-12-28 22:24:30	113.128.74.33	2s
yds		Manager Users	2020-12-28 19:30:34	2020-12-28 20:37:14	192.168.200.6	1h3min0s
ct		Manager Users	2020-12-28 19:35:51	2020-12-28 19:36:34	180.169.139.90	59min4s
ct		Manager Users	2020-12-28 19:36:20	2020-12-28 19:36:51	180.169.139.90	31s
guest_dbs_dba_limit		General Users	2020-12-23 17:24:32	2020-12-28 19:31:32	222.95.200.120	5d9h26min42s
jwy		Manager Users	2020-12-28 18:01:56	2020-12-28 19:31:32	192.168.200.6	1h27min36s
ct		Manager Users	2020-12-28 19:10:53	2020-12-28 19:31:32	180.169.139.90	20min39s
lwg		Manager Users	2020-12-28 17:07:35	2020-12-28 18:42:53	192.168.200.6	1h17s
HSC		Manager Users	2020-12-28 17:08:54	2020-12-28 18:38:12	223.220.64.90	1h58s
hth		Manager Users	2020-12-28 15:45:25	2020-12-28 18:26:47	171.82.20.218	2h41min22s
augene		Manager Users	2020-12-28 14:09:45	2020-12-28 17:55:02	106.21.182.125	3h45min17s
jwy		Manager Users	2020-12-28 16:47:49	2020-12-28 17:52:37	192.168.200.6	1h46min58s
ct		Manager Users	2020-12-28 16:49:30	2020-12-28 17:16:37	100.169.139.90	1h17s
yds		Manager Users	2020-12-28 15:25:17	2020-12-28 16:31:52	192.168.200.6	56min40s
lwg		Manager Users	2020-12-28 14:02:06	2020-12-28 16:17:57	192.168.200.6	1h22min51s
ct		Manager Users	2020-12-28 14:02:36	2020-12-28 16:14:37	180.169.139.90	1h51min11s
yds		Manager Users	2020-12-28 14:02:35	2020-12-28 16:25:12	192.168.200.6	1h38min47s
hth		Manager Users	2020-12-28 10:58:14	2020-12-28 12:45:07	171.82.20.218	1h48min33s

Note: Keep login history within six months at most.

From 1 to 20 Records, from 1 / 40 page. Note: Keep login history within six months at most.

Prev [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15] [16] [17] [18] [19] [20] Next Jump to [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15] [16] [17] [18] [19] [20]

- "Logout time" of the current online user is empty.
- The login history of all users will not be accumulated. A single login and logout is a record, in which a single "online time" is recorded. The user login history can record the user login within 6 months at most.
- Fuzzy search by username and login IP is supported.
- Operations such as "Log out", "Automatic exit after timeout" and "Automatic exit after resetting password" during the login will be sensed and recorded by the management platform.

6. Cluster management

6.1. Compute node cluster

Cluster management mainly provides users with management operations such as deployment, addition, start-stop monitoring and deletion of compute node clusters.

6.1.1. Cluster management record

The cluster management page displays the compute node clusters deployed or added. The compute node cluster name can be searched quickly through the fuzzy search in the upper left corner search box. You can also control the content to be displayed in the cluster table via the Unfold/Hide more on the right side.

List field description:

- Cluster Name: The cluster name of a group of compute nodes, which can be used to distinguish with other compute node clusters. The name is unique throughout HotDB Management. Click the cluster name to enter the “Edit Compute Node Cluster” page.

Cluster name color description: Red indicates that the HotDB Management has stopped monitoring the cluster; yellow indicates that the cluster high availability environment in master/slave mode needs to be rebuilt; and blue indicates that HotDB Management normally opens the cluster under monitoring.

- Cluster Mode: At present, the compute node cluster modes which are supported include the single node, master/slave node and multi-node modes. For details, please refer to the [Distributed Transactional Database HotDB Server \[Glossary\] Function Manual](#). The version number of compute node is shown at the bottom of the mode.
- Component Name: The compute node name is used to represent the difference between different compute nodes in the cluster. If the server SSH information is configured for compute nodes in the cluster in the master/slave node mode, the current Keepalived Virtual IP (VIP) mark will be displayed next to the name to facilitate users to quickly understand the location of master compute node in the current cluster.

- IP Address: It refers to the server IP deployed by the compute node.
- Service Port: It refers to the port for compute nodes to provide data service to the outside world, which can be modified in the server.xml configuration file.
- Management Port: It refers to the port for compute nodes to provide monitoring management queries to the outside world, which can be modified in the server.xml configuration file.
- Type: The compute node cluster in the master/slave mode can identify the master/slave role of compute nodes. This field has little meaning in single-node and multi-node clusters.
- Compute Node: This field belongs to the cluster deployment information and mainly displays the current running status of compute node service program. If the compute node cluster is not deployed by the current management platform, this field is displayed as NULL.
- High Available Components: This field mainly displays the running status of Keepalived components in the cluster in the master/slave node mode. The LVS virtual IP address (VIP) is displayed when the running status of LVS component is displayed in the multi-node mode cluster. If the compute node cluster is not deployed by the current management platform, this field is displayed as NULL.
- ConfigDB: It displays the running status of configDB used by the compute node cluster. If the compute node cluster is not deployed by the current management platform, this field is displayed as NULL.
- NTPD Time Service: It displays the running status of NTPD Time Service installed on the compute node cluster.
- Data Source: It displays the running status of all data sources in the compute node cluster.
- Deployment Environment Grade: The compute node cluster that successfully performed the “[Deployment Environment Examination](#)” function will display the latest examination grade.
- Cluster Operation: If the cluster is added by the “Cluster Deployment” function on the current management platform, the [Deployment Topology] button will be

displayed in the cluster operation bar. Click to view the component topology framework of the deployed cluster; if the cluster mode is “Master/Slave Node”, the operation column will display the [Rebuilding] or [Switch] button according to whether the current high availability rebuilding environment of the cluster meets the switching conditions.

- Buttons of [Switch the active center], [Remove the IDC], [Repair the IDC] can be seen in the cluster with DR mode enabled and conditions satisfied. You can refer to the [Distributed Transactional Database HotDB Server - V2.5.5 \[Visualization of Cross-IDC DR Switching\] Function Manual](#).



Function button description:

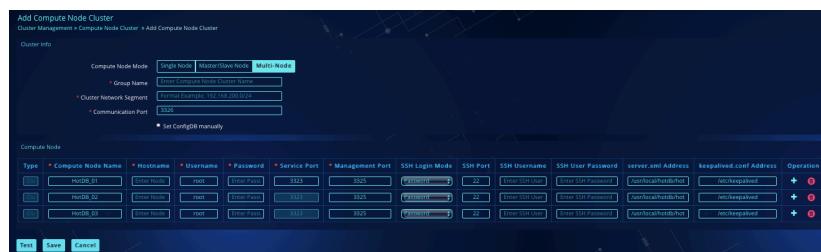
- Deploy Cluster: Deploy a complete set of compute node clusters from 0. For details, please refer to the [Distributed Transactional Database HotDB Server \[Installation and Deployment\] Function Manual](#).
- Add Cluster: Manually add compute node cluster (the compute node has been deployed offline) information of HotDB Management
- More->Start Monitoring: Restart the monitoring of compute node clusters whose monitoring has been stopped (the cluster name is displayed on a red background)
- More->Stop Monitoring: If the monitoring of compute node clusters under monitoring is stopped, HotDB Management will stop monitoring the cluster status. The cluster not under monitoring cannot be viewed by the user when logging into the general user role page.
- More->Delete Cluster: Delete the managed compute node cluster on the page.
- More->IDC Switching Drill: you can refer to the [Distributed Transactional](#)

[Database HotDB Server - V2.5.5 \[Visualization of Cross-IDC DR Switching\]](#)
[Function Manual](#)

6.1.2. Add cluster

Because the compute node clusters manually deployed by some users offline need to be added to HotDB Management for management, the cluster management function provides cluster addition. Users only need to fill in the information in HotDB Management according to the filling requirements to complete the management and monitoring of compute node clusters.

Click [Add Cluster] on the cluster management page to enter the “Add Compute Node Cluster” page.



Type	Compute Node Name	Hostname	Username	Password	Service Port	Management Port	SSH Login Mode	SSH Port	SSH Username	SSH User Password	server.xml Address	keepalived.conf Address	Operation
Host	HotDB_01	Enter Hostname	root	Enter Password	3323	3325	password	22	Enter SSH User	Enter SSH Password	/var/local/hafile/soft	/etc/keepalived/soft	+ (red)
Host	HotDB_02	Enter Hostname	root	Enter Password	3323	3325	password	22	Enter SSH User	Enter SSH Password	/var/local/hafile/soft	/etc/keepalived/soft	+ (red)
Host	HotDB_03	Enter Hostname	root	Enter Password	3323	3325	password	22	Enter SSH User	Enter SSH Password	/var/local/hafile/soft	/etc/keepalived/soft	+ (red)

Filling instructions:

(I) Cluster information

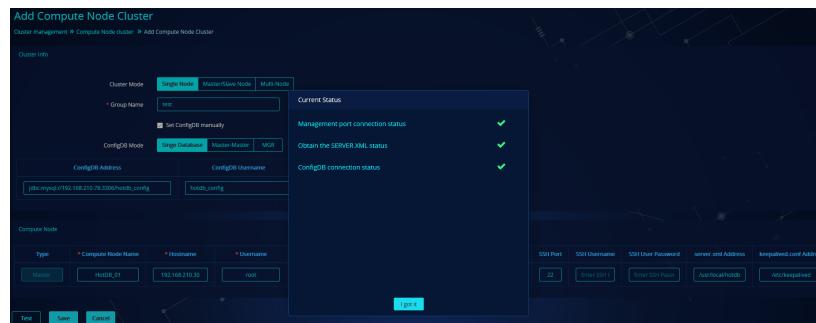
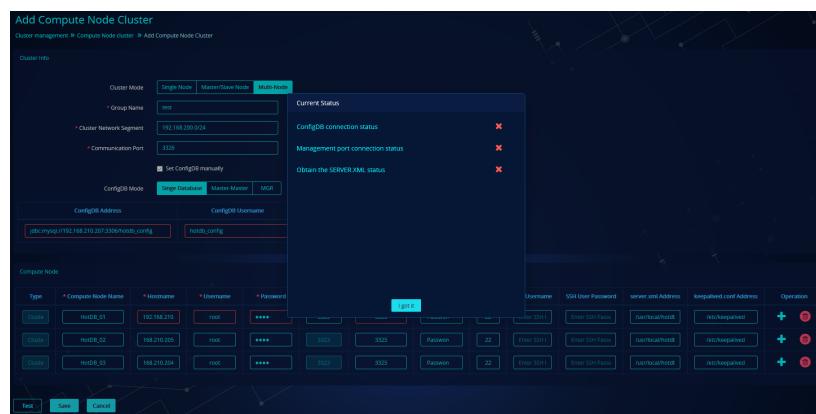
- Select the cluster mode of the deployed cluster, and the input parameters of different modes are different.
- The cluster name cannot be duplicated with the current existing compute node cluster name.
- The cluster network segment appears as the network segment to which the compute node belongs when the “Cluster Mode” is “Multi-Node”. The format is: IP/subnet mask length, for example, 192.168.200.0/24. This parameter can be viewed or modified in server.xml.
- The communication port appears as the port used for communication between multiple compute nodes in the deployed cluster only when the “Cluster Mode” is “Multi-Node”. This parameter can be viewed or modified in server.xml.

- “Set ConfigDB Manually” is not checked by default and is not required to be filled in. Only when the added compute node cannot connect to the management port (usually 3325), the user needs to manually specify the configDB address.
- Set ConfigDB Manually specifies that configDB needs to select the configDB replication mode and the configDB address needs to be filled in according to the given example. The configDB username and configDB password refer to the account and password connecting configDB instance.

Note: Any configDB in the replication mode strongly requires that the configDB connection address in server.xml shall be consistent with the IP address of the server where the actual configDB is located. It cannot be configured as 127.0.0.1 or localhost, so as mainly to prevent the risk of misjudging the actual address when the management platform obtains multiple configDB addresses in case that the management platform and the compute node service are not on the same service..

(II) Compute node

1. Different “Cluster Mode” displays different compute node records need to be configured. The “Single Node” mode only needs to configure one record. The “Master/Slave Node” mode needs to configure one master record and one slave record. The “Multi-Node” mode needs to configure at least three records, up to nine records.
2. The fields with red * must be filled in, including: compute node name, hostname, username, password, service port and management port.
3. The fields without red * may not be filled in, but when **the compute node cluster is in the master/slave mode**, users are recommended to fill in these parameter values because they may be used for high availability rebuilding and high availability switch later.
4. After filling in the compute node name, test whether the compute node can be connected via the [Test] button. The connection exception and successful connection are shown in the following figure:



Note: for more notes on DR mode and multi-node mode, you can refer to the supporting documents including [Installation and Deployment], [Cross-IDC DR Switching].

6.1.3. High availability switch

In the master/slave mode cluster, if the cluster meets the high availability switch conditions, click the [Switch] button in the “Cluster Operation” column of cluster record to manually perform the Master/Slave switching operation of compute node.

Compute Node cluster									
Cluster Management > Compute Node cluster									
List by Compute Node Cluster Name									
Cluster Deployment Info									
Group Name		Cluster Mode		Cluster Configuration		Cluster Deployment Info		Cluster Operation	
HA-01	Master-Slave	Master-Slave		Node01_01		IP Address: 192.168.210.86		Deployment Environment: Standard	
		Node02_01		IP Address: 192.168.210.87		Service Port: 5323		Deployment Status: Enabled	
HA-02	Master-Slave	Master-Slave		Node01_01		IP Address: 192.168.210.49		Deployment Environment: Standard	
		Node02_01		IP Address: 192.168.210.70		Service Port: 5323		Deployment Status: Enabled	
Single Node	Master	Single Node		Node01_01		IP Address: 192.168.228.161		Deployment Environment: Standard	
		Node02_01		IP Address: 192.168.228.140		Service Port: 7773		Deployment Status: Enabled	
Single Node	Master	Single Node		Node01_01		IP Address: 192.168.228.160		Deployment Environment: Standard	
		Node02_01		IP Address: 192.168.210.70		Service Port: 5323		Deployment Status: Enabled	

High availability switch operation instructions

High availability switch mainly includes four steps: Confirmation of SSH and Configuration File Location, Pre-inspection of Switching, High-availability Switching, and Switching Complete. It is not allowed to proceed to the next step when the previous step is not completed, and the completion of all steps represents the success of high availability switch.

(I) Confirmation of SSH and configuration file location

High availability switch

Cluster Management > Compute Node Cluster > High availability switch

Step One: confirmation of SSH and configuration file location

Step Two: Pre-inspection of Switching

Step Three: High-availability Switching

Step Four: Switching Complete

Master/Slave Server SSH privilege configuration

SSH Login Mode:

ComputeNode-01	ComputeNode-02
Hostname: <input type="text" value="192.168.240.159"/>	Hostname: <input type="text" value="192.168.240.160"/>
Username: <input type="text" value="root"/>	Username: <input type="text" value="root"/>
Password: <input type="password" value="*****"/>	Password: <input type="password" value="*****"/>

Confirmation of master/slave configuration file location

Master server xml Address	Slave server xml Address
<input type="text" value="/usr/local/hosts/db/hosts-server/conf"/>	<input type="text" value="/usr/local/hosts/db/hosts-server/conf"/>

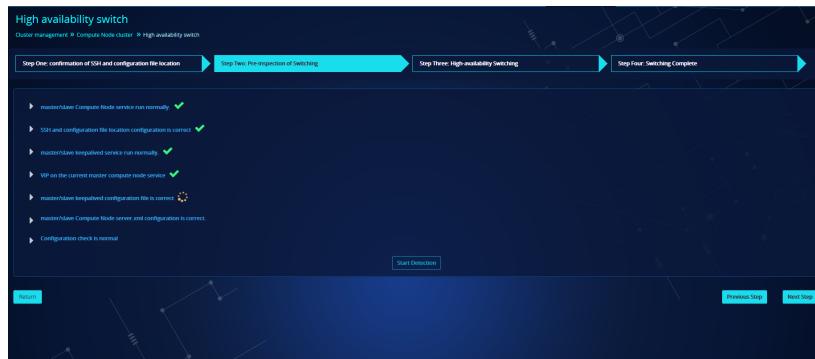
Master keepalived Configuration files	Slave keepalived Configuration files
<input type="text" value="/etc/keepalived"/>	<input type="text" value="/etc/keepalived"/>

- This step mainly confirms whether the SSH connection information and configuration file (server.xml and keepalived.conf) storage address of master/slave compute node configuration is filled in correctly.
 - SSH login mode may choose Login with User Password or Sign in without Password, the information will be saved after successful connection, and the

information will not be saved if one-time login is chosen.

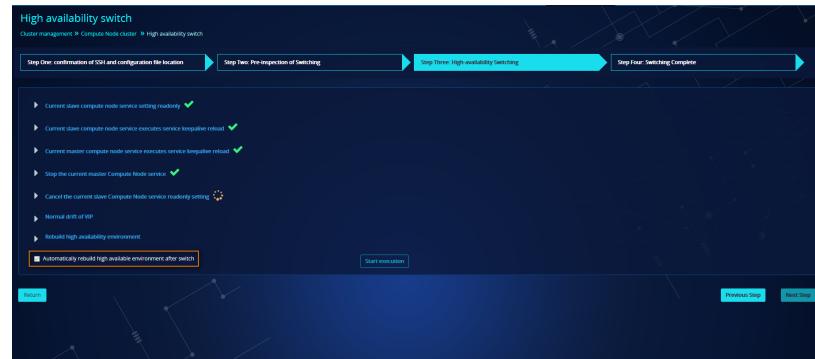
- The current logged-in user must have the read-write access privilege of master/slave configuration files.
- If the SSH Sign in without Password mode is chosen, the server where HotDB Management is located must set the public key of the account started and copy it to the server to be accessed. (Note: The user who can sign in without password must be consistent with the server user who starts the management platform currently).
- If the current connection account has the Sign in without Password privilege, even if Login with User Password is selected and wrong password is entered, the login will be successful and priority will be given to the judgement of whether there is Sign in without Password privilege. The check of password will be filtered directly if there is Sign in without Password privilege.
- The configuration file directory shall be consistent with the real service directory, otherwise the connection test will fail.
- If the SSH information and the configuration file address of compute node are configured in “[Add Cluster](#)”, the page information will be displayed automatically. It only needs to click [Connection Test] to verify the information correctness.
- Only when SSH information and configuration file address pass the test, the [Next Step] button can be clicked normally to proceed to the next step.

(II) Pre-inspection of switching



- Click [Start Detection] to check whether the current cluster high availability environment meets the requirements before high availability switch.
- This step requires all detection items to pass the test before proceeding to the next step. Otherwise, it is necessary to manually intervene to solve the abnormal problem of the failed item.

(III) High-availability switch

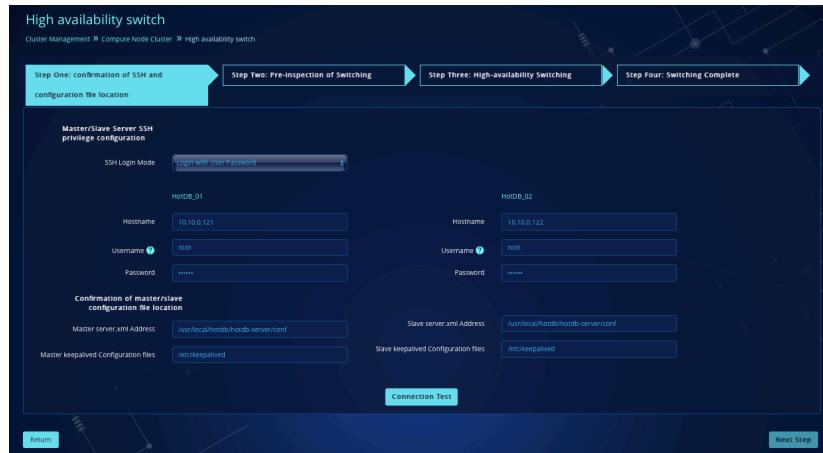


- This step is a high availability switch execution step. The high availability switch is successful only when all execution items are completed normally.
- The slave compute node randomly will be set before switch (no setting for below V2.4.8). After the switch is successful, the setting will be canceled automatically.
- The “Automatically rebuild high available environment after switch” on the page will be automatically ticked, that is, the program automatically rebuilds the

environment after the switch is completed to satisfy the next high availability switch operation without manual rebuilding.

- If the execution fails, manual intervention is needed to check and solve the problem.

(IV) Switch complete



- Reaching this step means that the high availability switch has been completed. The current VIP drift position and the opening and closing of master/slave compute node service port can be viewed.

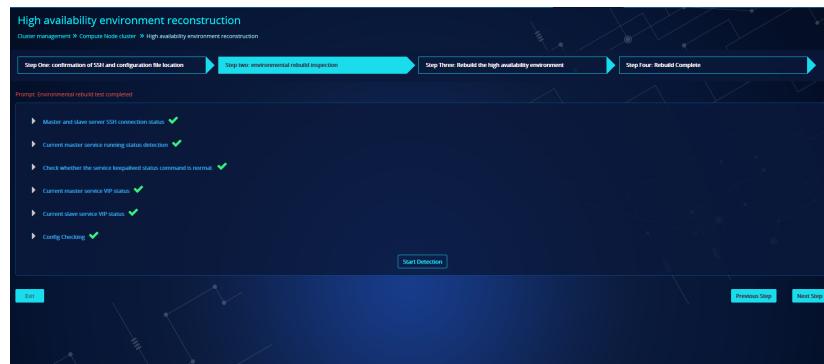
6.1.4. High availability reconstruction

The master/slave mode clusters identify the master/slave role mainly through the server.xml and keepalived.conf configuration files. The high availability switch only allows the switch from the Master role to the Slave role. After the failover or manual switch of compute node, in order to ensure the compute node can be smoothly switched back in the next failure, high availability reconstruction must be performed to ensure correct master/slave compute node configuration.

Compute Node cluster									
Cluster Management > Compute Node Cluster									
How to Create Node Cluster									
Cluster Configuration									
Cluster Deployment Info									
Cluster Operation									
Cluster Name:									
Cluster Mode:									
Master/Slave Node									
Master/Slave Node IP Address:									
Master/Slave Node Port:									
Master/Slave Node Management Port:									
Master/Slave Node Monitor Port:									
Cluster Configuration Info									
Cluster Deployment Info									
Cluster Operation									
Cluster Name:									
Cluster Mode:									
Master/Slave Node									
Master/Slave Node IP Address:									
Master/Slave Node Port:									
Master/Slave Node Management Port:									
Master/Slave Node Monitor Port:									
Cluster Configuration Info									
Cluster Deployment Info									
Cluster Operation									
Cluster Name:									
Cluster Mode:									
Master/Slave Node									
Master/Slave Node IP Address:									
Master/Slave Node Port:									
Master/Slave Node Management Port:									
Master/Slave Node Monitor Port:									
Cluster Configuration Info									
Cluster Deployment Info									
Cluster Operation									
Cluster Name:									
Cluster Mode:									
Master/Slave Node									
Master/Slave Node IP Address:									
Master/Slave Node Port:									
Master/Slave Node Management Port:									
Master/Slave Node Monitor Port:									
Cluster Configuration Info									
Cluster Deployment Info									
Cluster Operation									
Cluster Name:									
Cluster Mode:									
Master/Slave Node									
Master/Slave Node IP Address:									
Master/Slave Node Port:									
Master/Slave Node Management Port:									
Master/Slave Node Monitor Port:									
Cluster Configuration Info									
Cluster Deployment Info									
Cluster Operation									
Cluster Name:									
Cluster Mode:									
Master/Slave Node									
Master/Slave Node IP Address:									
Master/Slave Node Port:									
Master/Slave Node Management Port:									
Master/Slave Node Monitor Port:									
Cluster Configuration Info									
Cluster Deployment Info									
Cluster Operation									
Cluster Name:									
Cluster Mode:									
Master/Slave Node									
Master/Slave Node IP Address:									
Master/Slave Node Port:									
Master/Slave Node Management Port:									
Master/Slave Node Monitor Port:									
Cluster Configuration Info									
Cluster Deployment Info									
Cluster Operation									
Cluster Name:									
Cluster Mode:									
Master/Slave Node									
Master/Slave Node IP Address:									
Master/Slave Node Port:									
Master/Slave Node Management Port:									
Master/Slave Node Monitor Port:									
Cluster Configuration Info									
Cluster Deployment Info									
Cluster Operation									
Cluster Name:									
Cluster Mode:									
Master/Slave Node									
Master/Slave Node IP Address:									
Master/Slave Node Port:									
Master/Slave Node Management Port:									
Master/Slave Node Monitor Port:									
Cluster Configuration Info									
Cluster Deployment Info									
Cluster Operation									
Cluster Name:									
Cluster Mode:									
Master/Slave Node									
Master/Slave Node IP Address:									
Master/Slave Node Port:									
Master/Slave Node Management Port:									
Master/Slave Node Monitor Port:									
Cluster Configuration Info									
Cluster Deployment Info									
Cluster Operation									
Cluster Name:									
Cluster Mode:									
Master/Slave Node									
Master/Slave Node IP Address:									
Master/Slave Node Port:									
Master/Slave Node Management Port:									
Master/Slave Node Monitor Port:									

- SSH login mode may choose Login with User Password or Sign in without Password; the information will be saved after successful connection, and the information will not be saved if one-time login is chosen.
- The current logged-in user must have the read-write access privilege of master/slave configuration files.
- If the SSH Sign in without Password mode is chosen, the server where the distributed transactional database platform is located must set the public key of the account started and copy it to the server to be accessed. (Note: The user who can sign in without password must be consistent with the server user who starts the management platform currently).
- If the current connection account has the Sign in without Password privilege, even if Login with User Password is selected and wrong password is entered, the login will be successful and priority will be given to the judgement of whether there is Sign in without Password privilege. The check of password will be filtered directly if there is Sign in without Password privilege.
- The configuration file directory shall be consistent with the real service directory, otherwise the connection test will fail.
- Enter the correct configuration information, the connection test will be successful and the corresponding configuration will be saved to the compute node cluster synchronously. Click [Next Step] to enter the environment reconstruction detection page. If the current page information does not pass the test, the operation button for the next step cannot be triggered.

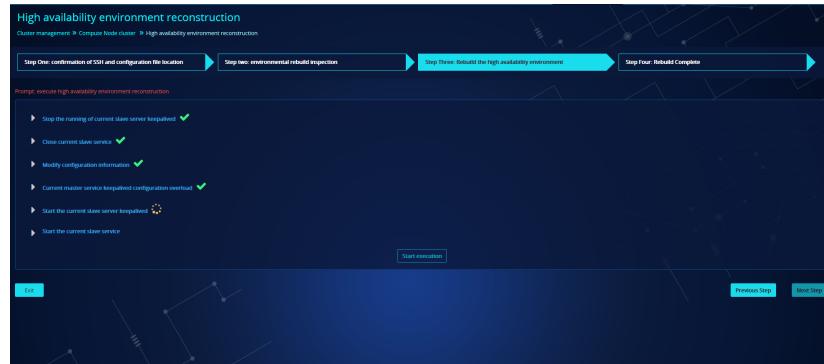
(II) Environment rebuild inspection



Attentions shall be paid when clicking [Start Detection]:

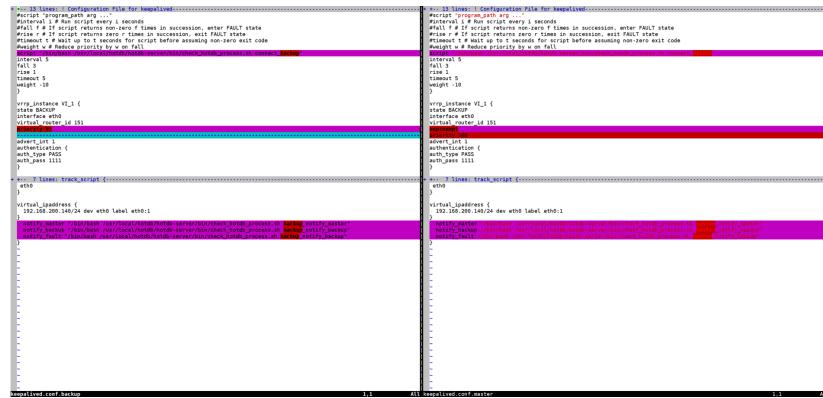
- The detection will be stopped if any item fails, and the cause of detection failure can be located and processed according to the failure error information.
- Config Checking mainly checks whether the configuration is reasonable and whether the configuration used in the memory is consistent with that in the configDB. If an inconsistency is detected, it can be processed by reloading, which is a feasible but not unique method.
- When the detection is completed, click [Next Step] to enter the high availability environment reconstruction page. If the current page information fails the detection, the [Next Step] button cannot be triggered.

(III) Rebuild the high availability environment



The reconstruction is mainly to modify the relevant configuration information as follows:

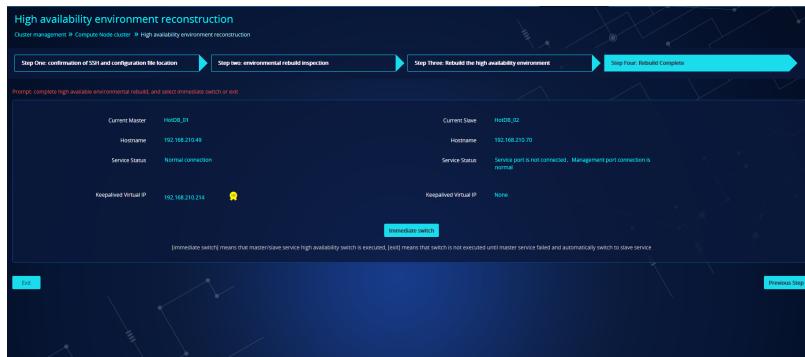
- Modify the (haState, haNodeHost) role information in the master/slave compute node server.xml
- Modify the master/slave keepalived configuration files. The keepalived configuration file modification points are as follows:



Notes for high availability reconstruction:

- Click [Start Execution]. The execution will be stopped if any item fails, and the cause of execution failure can be located and processed according to the failure error information.
- For the modification of server.xml configuration by the reconstruction process, if the actual deployed environment management network and the running network are separate, the haNodeHost configuration may have incorrectness risks, in which case manual intervention is needed because the server connection IP is currently used.
- When the reconstruction is completed, click [Next Step] to enter the high availability environment reconstruction page. If the current page information is not completed or the execution fails, the [Next Step] button cannot be triggered.

(IV) Rebuild complete



- When the high availability reconstruction is completed, the master/slave compute node services are running normally. Click [Immediate Switch] and manually perform the [High Availability Switch](#) operation to complete the reconstruction page.

6.1.5. Switching, removal and repair of IDC

With DR mode enabled, the visualized switching, removal and repair of IDC can be performed in the qualified clusters by the management platform. For details, you can refer to the [Distributed Transactional Database HotDB Server - V2.5.5 \[Visualization of Cross-IDC DR Switching\] Function Manual](#).

6.1.6. IDC switching drill

With DR mode enabled, the visualized IDC switching drill can be performed in the qualified clusters by the management platform. For details, you can refer to the [Distributed Transactional Database HotDB Server - V2.5.5 \[Visualization of Cross-IDC DR Switching\] Function Manual](#).

6.2. Single Component Deployment

Single Component Deployment provides HotDB Management users with the function of installing and deploying a single component, which makes up for the defect that a

component cannot be installed separately in cluster deployment function. For specific function description and operation steps, please refer to [Distributed Transactional Database HotDB Server \[Installation and Deployment\] Function Manual](#).

6.3. Deployment environment examination

Deployment grade Examination is a set of operation environment examination grade functions tailored specifically for HotDB Server clusters. Users can use this function to evaluate the environment of clusters installed manually or deployed through the management platform. After the evaluation, it displays the results of nearly 140 examination sub-items of the whole cluster in five dimensions, and supports the export of examination result records.

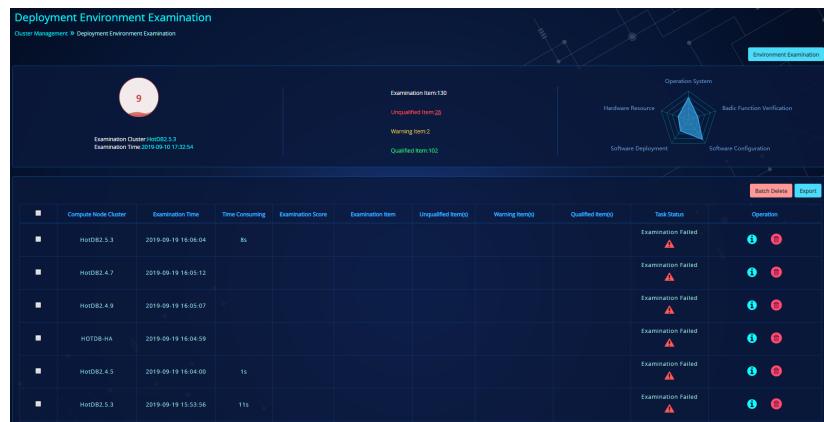
Function Entry: Login Management User Interface->Compute Node Cluster->Deployment Environment Examination

Examination dimension:

Examination dimension	Examination item
Hardware resource	Server attribute
	Disk space
	Disk IO response time
	Memory
	CPU
	Network quality
Operation system	periodical scheduling
	sysctl.conf
	Time synchronization
	Can be connected to the external network
	Firewall and selinux
	yum
	Time zone
	tune
	limits.cnf
	Character set

	SSH connection
Software deployment	Backup program
	MySQL client
	MySQL server
	Java environment
	MySQL connection
Software configuration	MySQL high availability
	Compute node startup script
	ConfigDB
	MySQL disk space
	MySQL parameter configuration
	MySQL user privilege
	server.xml
	Compute node high availability
	Monitoring port
	Data source high availability switch
Basic function verification	Compute node high availability switch
	LogicDB privilege
	Backup program
	10 s performance test

Examination panel:



The screenshot shows the 'Deployment Environment Examination' interface. At the top, there's a navigation bar with 'Cluster Management' and 'Deployment Environment Examination'. Below the navigation is a header with a circular icon containing the number '9', the text 'Examination Cluster: HotDB2.5.3', and 'Examination Time: 2019-09-19 17:32:54'. To the right of the header is a map-like visualization with nodes labeled 'Operation System', 'Hardware Resource', 'Software Deployment', and 'Software Configuration'. Below the visualization, there are three status indicators: 'Examination Item(130)', 'Warning Item(2)', and 'Qualified Item(102)'. A large table below the status indicators displays examination results for various clusters. The table has columns for 'Compute Node Cluster', 'Examination Time', 'Time Consuming', 'Examination Score', 'Examination Item', 'Unqualified Item(s)', 'Warning Item(s)', 'Qualified Item(s)', 'Task Status', and 'Operation'. Most clusters listed show 'Examination Failed' in the Task Status column, indicated by a red triangle icon.

Compute Node Cluster	Examination Time	Time Consuming	Examination Score	Examination Item	Unqualified Item(s)	Warning Item(s)	Qualified Item(s)	Task Status	Operation
HotDB2.5.3	2019-09-19 16:06:04	8s						Examination Failed	● ● ●
HotDB2.4.7	2019-09-19 16:05:12							Examination Failed	● ● ●
HotDB2.4.9	2019-09-19 16:05:07							Examination Failed	● ● ●
HotDB-HA	2019-09-19 16:04:59							Examination Failed	● ● ●
HotDB2.4.5	2019-09-19 16:04:00	1s						Examination Failed	● ● ●
HotDB2.5.3	2019-09-19 15:53:56	11s						Examination Failed	● ● ●

Examination panel content description

The examination panel displays an overview of cluster reports that have been

successfully examined recently.

- **Score:** The left score ball is the total examination score. Scores are obtained from the examination results of cluster examination items. The total score is 100. If the corresponding examination item in examination does not meet the evaluation criteria, the score of this item will be deducted. If the examination item meets the evaluation criteria, no score will be deducted or added. When the total score is deducted or the score deducted is greater than 100, the examination score is 0.
- **Examination item:** The examination item is the number of items needing examination in the compute node cluster examination. Different modes of compute node clusters or different replication modes of MySQL data sources will affect the number of examination items. Unqualified items in the figure above are items not meeting the evaluation criteria. Warning items are items that do not involve deduction but need attention in physical examination, and qualified items are items meeting the evaluation criteria.
- **Radar chart:** Radar chart displays the deduction in five dimensions in examination. The less points deducted in the dimension, the closer the highlighted part is to the edge of radar chart, which indicates a good examination result in the dimension. Move the mouse cursor cursor into the radar chart to view the detailed deductions in each dimension and the percentage of total examination item score in the dimension.

Start environment examination:

Click [Environment Examination] button on the deployment environment examination page to Start the cluster running environment examination task. After the initiation, the compute node cluster needing examination can be selected (the clusters not under monitoring do not support initiating examination, and such clusters will be automatically filtered in the cluster selection drop-down box). After submitting the task, the current cluster environment will be pre-detected, and the task initiation will fail if

the pre-detection fails.

Pre-detection item

1. All servers in the cluster are configured with available SSH information and the user is root or is configured with sudo operation privilege.
2. All related component programs in the cluster run normally
3. The cluster is configured with at least one data node and one logicDB

Note: The status detection of all related component programs in the cluster depends on a 2-minute periodic detection task, so there may be a 2-minute detection error between the current detection status and the actual component status.

Examination report detail:

A successful examination task will generate a examination report. Click  detail button in the task record operation column to access the “Examination report detail page”.

Examination report description

The examination report defaults to display unqualified and warning examination items. Click different dimensions to expand the detailed examination item information of the dimension. The red and orange dots that appear in each dimension heading represent unqualified and warning examination items in the dimension. Each tab in the dimension is a specific examination item in the dimension. The red and orange markings in the upper right corner of the Tab represent the same meaning with that of the above dots.

Examination item: specific examination item in the dimension

Examination result: the examination results of examination items include Unqualified, Warning and Qualified

Deduction: the actual deduction of the examination item

Exception object: instances of servers or applications not meeting the evaluation criteria of examination items

Prompt: unqualified and warning examination items inform users of the risks that exist or suggestions

Evaluation criteria: the program evaluation criteria for judging whether an item passes the detection

Examination Report Detail

Cluster management > Deployment environment examination > Examination Report Detail

Examination Cluster: HotDB-Cluster30
Examination Time: 2019-09-19 16:02:16

Examination Item: 133

■ Unqualified item: 22
■ Warning item: 2
■ Qualified item: 109

Hardware Resource Operation System Basic Function Verification
Software Deployment Software Configuration

Hardware Resource

Memory Disk space CPU Server Attribute

Examination Item	Examination Result	Deduction	ID	Exception Object	Message	Evaluation Criteria
Server memory	Unqualified	-5	192.168.210.30	Server192.168.210.30: Uninstalled: 1 Compute Node, 1 Compute Node, 1 Compute Node, 1 Compute Node, Required memory 35G, Actual Existing Memory 23.59G.	One Compute Node(s)3 One Management Port max22G max22G max22G Data Source MySQL, Ins LVS Instance 2 LVS Instance 2 LVS Instance 2 One Compute Node(s) One Management Port max22G max22G max22G Data Source MySQL, Ins LVS Instance 2 LVS Instance 2 LVS Instance 2 One Compute Node(s) One Management Port max22G max22G max22G Data Source MySQL, Ins LVS Instance 2 LVS Instance 2 LVS Instance 2 One Compute Node(s)	
			192.168.210.31	Server192.168.210.31: Uninstalled: 1 Compute Node, 1 Compute Node, 1 Compute Node, 1 Compute Node, Required memory 35G, Actual Existing Memory 23.59G.		
			192.168.210.40	Server192.168.210.40: Uninstalled: 1 Compute Node, 1 Compute Node, 1 Compute Node, 1 Compute Node, Required memory 35G, Actual Existing Memory 23.59G.		
			192.168.210.41	Server192.168.210.41: Uninstalled: 1 Compute Node, 1 Compute Node, 1 Compute Node, 1 Compute Node, Required memory 35G, Actual Existing Memory 23.59G.		
			192.168.210.44	Server192.168.210.44: Uninstalled: 1 Compute Node, 1 Compute Node, 1 Compute Node, 1 Compute Node, Required memory 35G, Actual Existing Memory 23.59G.		

Operation Systems
Software Deployment
Software Configuration
Basic Function Verification

Results **Export**

Note:

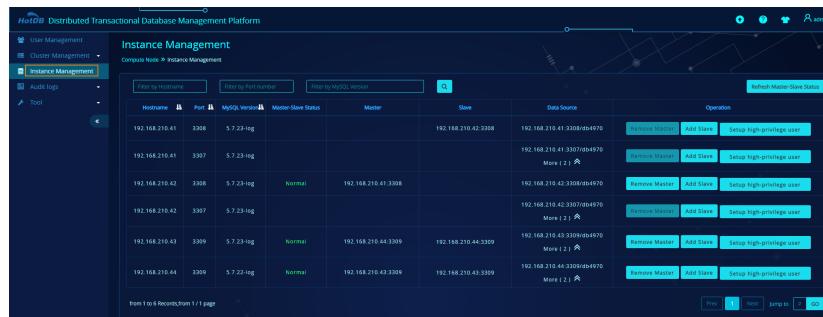
The deployment environment examination function has no requirement for HotDB Server version. However, when the Server version used for examination is below 2.5.3, the “10 s performance test” and “master/slave or MGR configDB data consistency” examination items are not supported.

7. Instance management

This function is used to view and manage the master-slave relation of the instances of data sources in all compute node clusters. The instance information can be filtered by hostname, port and MySQL version.

7.1. Instance management information

Function Entry: Login Management User Interface -> Instance Management



Hostname	Port	MySQL Version	Master-Slave Status	Master	Slave	Data Source	Operation
192.168.210.41	3308	5.7.23-log		192.168.210.42:3308	192.168.210.41:3308	192.168.210.41:3308/0b4970	[Remove Master] [Add Slave] [Setup High-privilege user]
192.168.210.41	3307	5.7.23-log		192.168.210.41:3307	192.168.210.41:3307	192.168.210.41:3307/0b4970	[Remove Master] [Add Slave] [Setup High-privilege user]
192.168.210.42	3308	5.7.23-log	Normal	192.168.210.41:3308	192.168.210.42:3308	192.168.210.42:3308/0b4970	[Remove Master] [Add Slave] [Setup High-privilege user]
192.168.210.42	3307	5.7.23-log		192.168.210.42:3307	192.168.210.42:3307	192.168.210.42:3307/0b4970	[Remove Master] [Add Slave] [Setup High-privilege user]
192.168.210.43	3309	5.7.23-log	Normal	192.168.210.44:3309	192.168.210.44:3309	192.168.210.43:3309/0b4970	[Remove Master] [Add Slave] [Setup High-privilege user]
192.168.210.44	3309	5.7.23-log	Normal	192.168.210.43:3309	192.168.210.43:3309	192.168.210.44:3309/0b4970	[Remove Master] [Add Slave] [Setup High-privilege user]

The instance management information displays a record in the form of a MySQL instance, and performs operations such as “Remove Master”, “Add Slave”, and “Setup High-privilege User” of specific MySQL instances.

- **Remove Master:** Click [Remove Master] to stop the replication of this instance and perform the operation of clearing replication information (stop slave; reset slave all;).
- **Add Master:** Click [Add Master] to add a slave to this instance and set this instance as a host when performing a “change master” operation on the slave. When selecting a slave, only instances without master can be selected and instances have been configured with master shall first remove the Master.

Select Slave Instance					
	Hostname	Port	MySQL Version	Connection status	
■	192.168.210.41	3307	5.7.23-log	Normal	
■	192.168.210.42	3307	5.7.23-log	Normal	
■	192.168.210.44	3308	5.7.22-log	Normal	
■	192.168.210.76	3307	8.0.16	Normal	
■	192.168.220.149	3309	5.7.25-log	Normal	

from 1 to 5 Records, from 1 / 2 page

⚠ Requirement: It is recommended that master/slave Data Source is the instance newly installed and not generating data.

Prev 2 Next Jump to

➤ Setup High-privileges User: Mainly used for users configured with “change master/slave” privileges to perform “Remove Master” and “Add Slave” operations. High-privilege users need to have “super, replication slave, replication client, create user, reload” privileges. If the data source does not have these privileges, they need to be added to the instance.

Setup high-privileges user

Hostname	192.168.210.44
Port	3308
High privilege Username	hotdb_datasource
High privilege Password	*****
User-Defined Master/Slave replication User	<input type="checkbox"/>
Master/Slave replication Username	hotdb_repl
Master/Slave replication Password	*****

Click the [Replication] button to replicate and add the SQL statement of high-privilege user to the instance for execution.

“Master/Slave Replication Username” and “Master/Slave Replication Password” are users created automatically when a master/slave relation is created for an instance by a

high-privilege user. By default, the “hotdb_repl” replication user with password of “hotdb_repl” and only the “replication slave” privilege is created. Users can also customize the username and password for the created replication user.

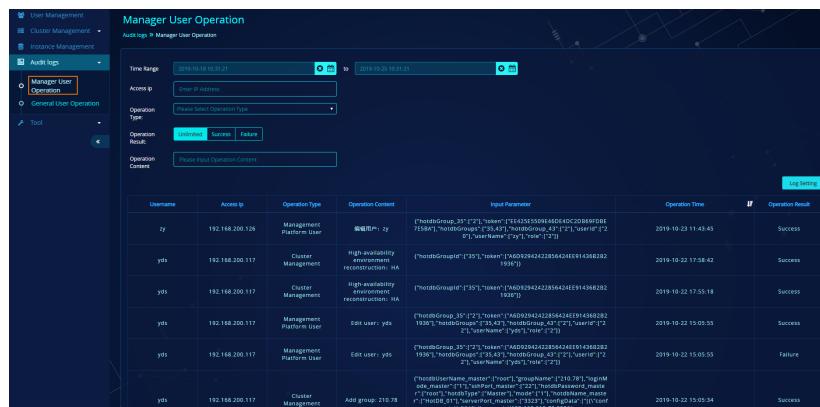
8. Audit logs

The audit logs of the management user interface is mainly used to view the HotDB Management operation records of the management user, and to view the basic operations of general users in all managed compute node clusters.

8.1. Manager operation

The operation of all manager users on the management platform can be viewed. The type of operation can be viewed in the operation type drop-down box on the page. Access IP and operation content supports fuzzy query.

Function Entry: Login Management User Interface->Audit Logs->Manager Operation



List Setting						
Username	Access IP	Operation Type	Operation Content	Input Parameter	Operation Time	Operation Result
zy	192.168.200.128	Management Platform user	高可用性环境恢复: HA	{"hostGroup": "35", "token": "164235550946040DC20869D8E7156A7", "hostGroupId": "35", "hostId": "164235550946040DC20869D8E7156A7", "hostName": "HostGroup_35", "hostIp": "192.168.200.128", "hostPort": "22", "userIp": "127.0.0.1", "userPort": "22", "user": "zy", "password": "zy", "isSuccess": true}	2019-10-23 11:49:49	Success
yds	192.168.200.117	Cluster Management	高可用性环境恢复: HA	{"hostGroup": "35", "token": "1609294242856436161434802121936"}, {"hostGroup": "35", "token": "1609294242856436161434802121936"}	2019-10-22 17:58:42	Success
yds	192.168.200.117	Cluster Management	高可用性环境恢复: HA	{"hostGroup": "35", "token": "1609294242856436161434802121936"}, {"hostGroup": "35", "token": "1609294242856436161434802121936"}	2019-10-22 17:55:18	Success
yds	192.168.200.117	Management Platform user	Edit user: yds	{"hostGroup": "35", "token": "1609294242856436161434802121936", "hostName": "HostGroup_35", "hostIp": "192.168.200.117", "hostPort": "22", "userIp": "127.0.0.1", "userPort": "22", "user": "yds", "password": "yds", "isSuccess": true}	2019-10-22 15:05:35	Success
yds	192.168.200.117	Management Platform user	Edit user: yds	{"hostGroup": "35", "token": "1609294242856436161434802121936"}, {"hostGroup": "35", "token": "1609294242856436161434802121936"}	2019-10-22 15:05:35	Failure
yds	192.168.200.117	Cluster Management	Add group: 210.78	{"hostUserName": "yds", "programName": "1710.181.1", "loginMode": "master", "hostPort": "22", "hostPassword": "yds", "hostIp": "192.168.200.117", "hostName": "HostGroup_35", "hostGroup": "35", "hostId": "210.78", "hostGroupId": "35", "userIp": "127.0.0.1", "userPort": "22", "user": "yds", "password": "yds", "isSuccess": true}	2019-10-22 15:05:34	Success

List information description:

- Username: The user used to login to the management platform.
- Access IP: The local IP used to login to the management platform. It supports fuzzy query.
- Operation Type: All supported types are displayed in the drop-down box. After checking the checkbox, only logs of the selected operation type are displayed.
- Operation Content: Record the user's real operation and important parameters, and

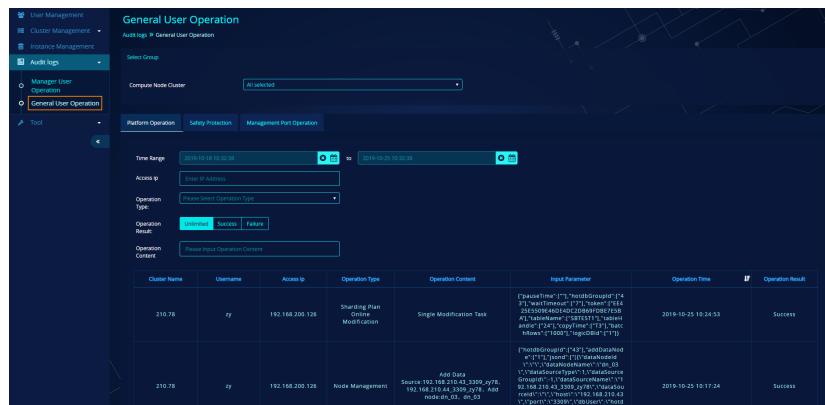
support fuzzy query.

- Input Parameter: More detailed user operation logs for easy analysis of user operations.
 - Operation Time: Record the actual operation time, and support the selection of time range to display log records. The time range of record here is determined by the default retention days in the settings.
 - Operation Result: Record the actual operation results. Log records can be filtered by the operation results.

8.2. General user operation

The operations of all general users on the management platform can be viewed. The log records of all compute node groups are displayed by default. Check the drop-down box to filter the log information of compute node groups can be viewed, including Platform Operation, Safety Protection and Management Port Operation, which are consistent with the view mode of general user login.

Function Entry: Login Management User Interface->Audit Logs->General User Operation



8.2.1. Platform operation

The operations of all general users on the management platform can be viewed. The operation type specifically recorded can be viewed in the operation type drop-down box on the page. Access IP and operation content input boxes support fuzzy query. If the compute node group is selected, only the operation records of the selected compute node group are displayed, and all compute node groups are displayed by default.

User Management	Cluster Management	Instance Management	Audit Logs	Manager User Operation	General User Operation	Tool
General User Operation						
Audit Log > General User Operation						
<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> Select Group: <input type="text" value="Corpuose Node Cluster"/> <input type="button" value="All selected"/> </div> <div style="display: flex; justify-content: space-between;"> Platform Operation Safety Protection Management Port Operation </div>						
Time Range	2019-10-25 00:00:00	<input type="button" value=""/>	to	2019-10-25 10:00:00	<input type="button" value=""/>	
Access IP	<input type="text" value="Enter IP Address"/>					
Operation Type	<input type="button" value="Please Select Operation Type"/>					
Operation Result	<input type="button" value="Unsuccess"/>	<input type="button" value="Success"/>	<input type="button" value="Failure"/>			
Operation Content	<input type="text" value="Please Input Operation Content"/>					
Cluster Name	Username	Access IP	Operation Type	Operation Context	Input Parameter	Operation Time
210.78	zy	192.168.200.126	Changing Plan Of User Modification	Single Modification Task	{"planTime": "1", "hostGroup": "1", "planType": "1", "planContent": "1", "planStatus": "1", "planId": "2343506462442038691087538", "planName": "1", "planContentList": "1", "planContent": "1", "planStatus": "1", "planTime": "1", "planHost": "1", "logTime": "1", "logHost": "1"}	2019-10-25 10:24:53
210.78	zy	192.168.200.126	Add Data	Source:192.168.210.43_2306_xy78.192.168.200.126_2306_xy78.192.168.200.126_2306_xy78	node_01_01_en_03	2019-10-25 10:17:24
						Success

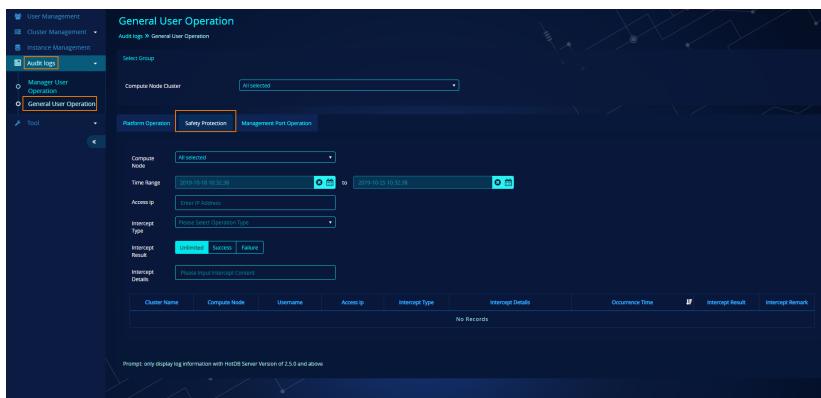
List information description:

- Group Name: The name of the compute node group queried.
 - Username: The user used to login to the management platform.
 - Access IP: The local IP used to login to the management platform. It supports fuzzy query.
 - Operation Type: All supported types are displayed in the drop-down box. After checking the checkbox, only logs of the selected operation type are displayed.
 - Operation Content: Record the user's real operation and important parameters, and support fuzzy query.
 - Input Parameter: More detailed user operation logs for easy analysis of user operations.

- Operation Time: Record the actual operation time, and support the selection of time range to display log records. The time range of record here is determined by the default retention days in the settings.
- Operation Result: Record the actual operation results. Log records can be filtered by the operation results.

8.2.2. Security protection

The operation logs related to security protection performed by all general users can be viewed. The operation type specifically recorded can be viewed in the operation type drop-down box on the page. Access IP and Intercept Details input boxes support fuzzy query. If the compute node group is selected, only the operation records of the selected compute node group are displayed, and all compute node groups are displayed by default. A specific compute node can be selected, and all compute nodes are selected by default.



List information description:

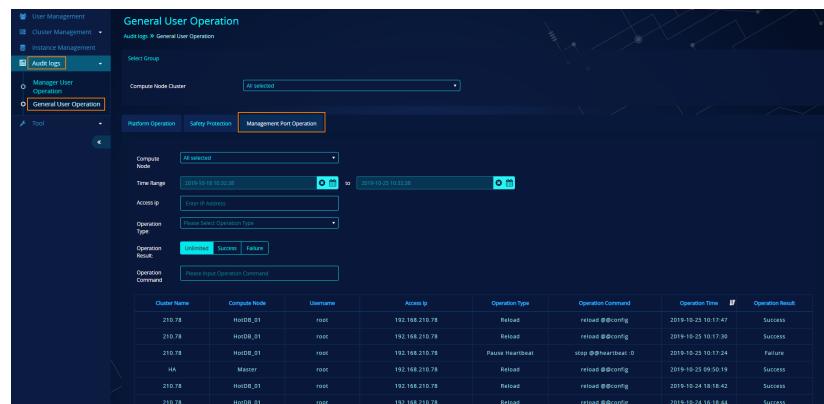
- Group Name: The name of the compute node group queried.
- Username: The user used to execute the operation.
- Access IP: The local IP used to perform the operation. It supports fuzzy query.

- Intercept Type: All supported types are displayed in the drop-down box. After checking the checkbox, only logs of the selected operation type are displayed.
- Intercept Details: Record the commands executed. It supports fuzzy query.
- Operation Time: Record the actual operation time, and support the selection of time range to display log records. The time range of record here is determined by the default retention days in the settings.
- Operation Result: Record the actual operation results. Log records can be filtered by the operation results.

Note: If the compute node version is below V2.5.0, the page does not display the security audit log record.

8.2.3 Management port operation

The operation records of all general users on the management port can be viewed. The operation type specifically recorded can be viewed in the operation type drop-down box on the page. Access IP and Intercept Details input boxes support fuzzy query. If the compute node group is selected, only the operation records of the selected compute node group are displayed, and a specific compute node can also be selected. All compute nodes are selected by default.



List information description:

- Group Name: The name of the compute node group queried.
- Username: The user used to login to the management port.
- Access IP: The IP used to login to the management port.
- Operation Type: All supported types are displayed in the drop-down box. After checking the checkbox, only logs of the selected operation type are displayed.
- Operation Command: The command actually executed on the management port.
- Operation Time: Record the actual operation time, and support the selection of time range to display log records. The time range of record here is determined by the default retention days in the settings.
- Operation Result: Record the actual operation results. Log records can be filtered by the operation results.

Note: If the compute node version is below V2.5.0, the page does not display the management port operation audit log record.

9. Tool

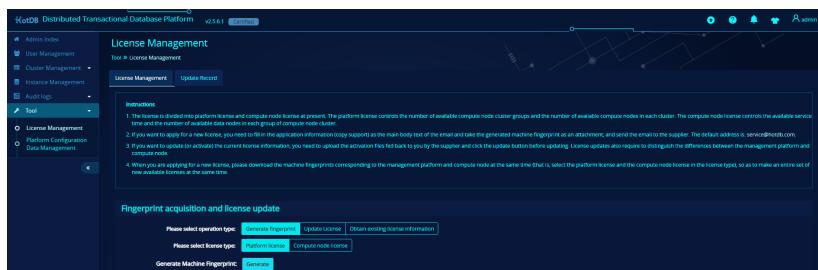
9.1. License management

Provide users with operations such as platform license, compute node license, update license and obtain the existing license information.

9.1.1 Platform license

9.1.1.1 Update entry

- “License Management” in the “Tool” menu under admin role.

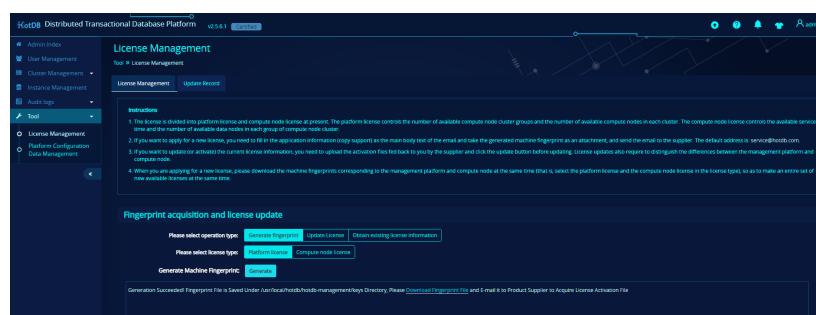


- The "license management" hyperlink in the “certified” menu of management platform.



9.1.1.2 Generate fingerprint

- Enter the license management page, select [Generate license] for operation type, select [Platform license] for license type, and click [Generate].



- Click the [Download Fingerprint File] hyperlink to download the fingerprint file (the fingerprint file is saved under the directory hotdb-management/keys by default, and the format is: management-fingerprint-year-month-day-hour-minute-second).
- Fill in the information of the applicant and license properties (not required), and copy the application information.

Fill in the information of the applicant and the license properties (not required)

Applicant Name:	<input type="text" value="zhangsan"/>	Number of available compute nodes cluster groups:	<input type="text" value="3"/> (0 means unlimited)
Corporate name to which it belongs:	<input type="text" value="xx Technology Co., Ltd."/>	Number of compute nodes available for each cluster:	<input type="text" value="6"/> (0 means unlimited)
Contact number:	<input type="text" value="18899999999"/>		
Email:	<input type="text" value="zhangsan@163.com"/>		
Personal or corporate WeChat ID:	<input type="text" value="zhangsan"/>		
Copy the above application information			

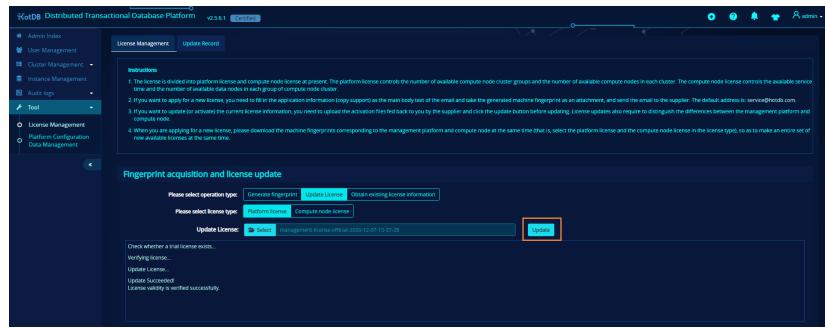
- Click the default address hyperlink of supplier (service@hotdb.com), and call the local mailbox.



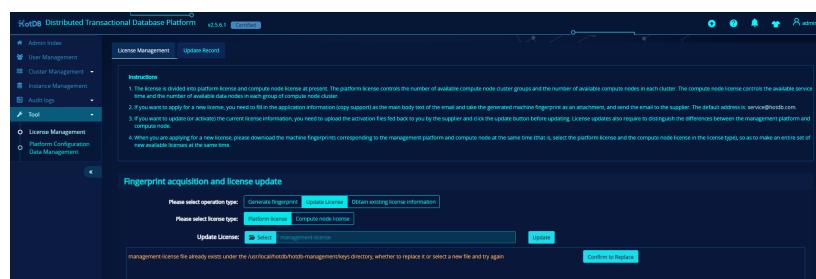
- Paste the application information to the email, upload the fingerprint file to the email attachment and send it to the supplier to obtain the new license file.

9.1.1.3 Update license

- Enter the license management page, select [Update license] for operation type, select [Platform license] for license type, and click [Select] to upload the license file.
 - Click [Update] to update the license, and then refresh the page to make the new license take effect.

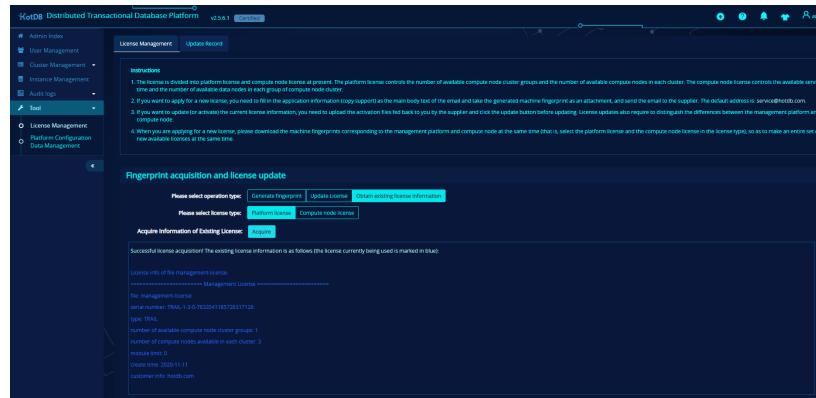


- When the name of the newly uploaded license file is consistent with that of the currently used license file, click [Update], it will prompt that license file already exists and whether to replace it. Click [Confirm to replace] to replace the existing license file and enter the Update process.



9.1.1.4 Obtain existing license information

- Enter the license management page, select [Obtain the existing license information] for operation type, select [Platform license] for license type, and click [Acquire] to obtain the existing license information.



The license information is as follows:

file: license file name

serial number: serial number of license file

type: license type, example: OFFICIAL, TRIAL

Num of available compute node cluster groups: number of available compute node cluster groups. 0 means that there are no restrictions

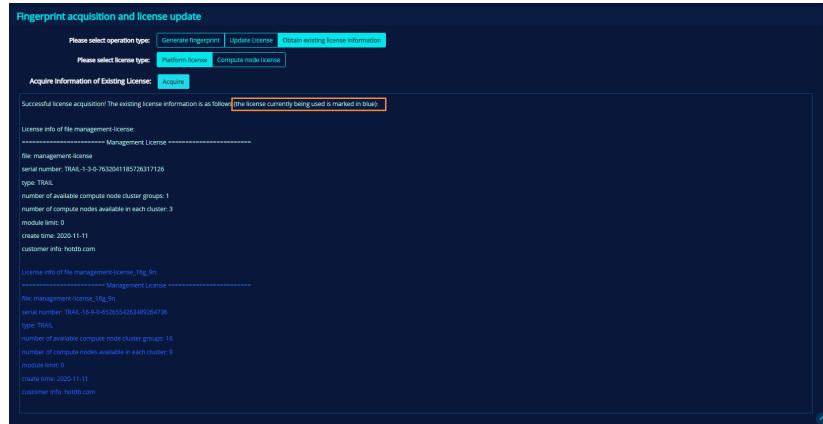
Num of compute nodes available in each cluster: number of compute nodes available in each cluster. 0 means that there are no restrictions

module limit: module limit (can be ignored temporarily)

create time: create time

customer info: customer info

- When there are multiple license files in the management platform, the license marked in blue is the license currently being used.



9.1.1.5 Other instructions

(1) The default address of the supplier can be configured.



Connect to the ConfigDB of management platform, and configure SQL for the first time as follows:

```
insert into hotdb_setting values('emailAddress',1,'your_email@xx.cn',1,1);
```

The SQL configuration is changed as follows:

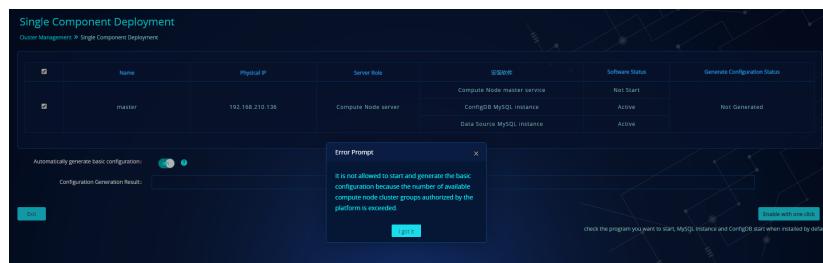
```
update `hotdb_setting` set `value` ='new_email@xx.cn' where `key`='emailAddress';
```

(2) Notes on updating platform license

- Manual tampering with the license file will invalidate the license.
- Manual tampering with the license dependency package will result in failure to update the license.
- If the user has no privilege for management/keys directory, the license update will fail.
- Uploading unauthorized file updates will result in failed license update.
- If the number of available cluster groups of the new license is less than the number of existing cluster groups, the update will fail.
- If the number of available compute nodes in each cluster of the new license is less than the number of existing compute nodes, the update will fail.
- After the new license is updated, the old license will not be deleted, but transferred to the management/databak/keys directory of the management platform.

(3) Restrictions of platform license on single-IDC deployment

- If the number of existing compute node clusters (including those with stopped monitoring and normal monitoring) has reached the number of available compute node cluster groups authorized by the platform license, the user has enabled the "Automatically generate basic configuration" and the started list includes clusters recorded in the high availability setup of compute nodes, then click [Enable with one click] on the single-IDC deployment page, and a pop-up window will be displayed: "It is not allowed to start and generate basic configuration because the number of available compute node cluster groups authorized by the platform is exceeded."

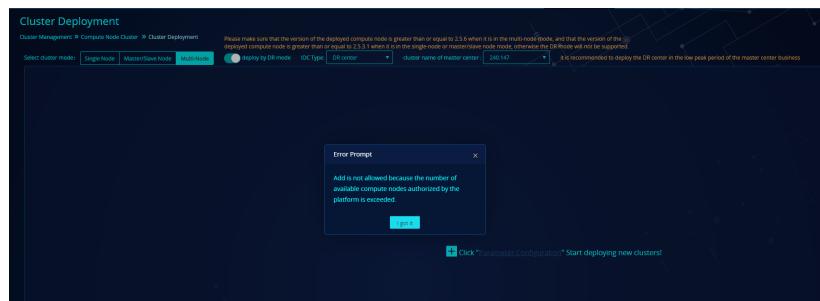


(4) Restrictions of platform license on cluster deployment

- In normal mode deployment, when the number of compute node cluster groups has reached the number of available compute node cluster groups authorized by the license, a prompt of 3s will be given when clicking [Parameter configuration]: Cluster addition through parameter configuration is not allowed because the number of available compute node cluster groups authorized by the platform is exceeded.

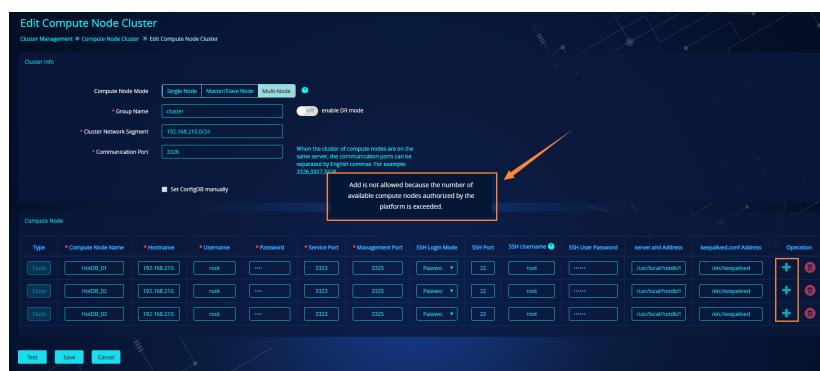


- The deployment of the master center in the DR mode is the same as that in the ordinary mode. That is, when the number of the current compute node cluster groups has reached the license limit, the deployment of the master center will not be allowed.
- Because the deployment of the DR center in the DR mode is in the same cluster group with the master center, the deployment of the DR center is not limited by the number of compute node cluster groups, but limited only by the number of available compute nodes in each group.
- The deployment of DR center is limited by the number of available compute nodes in each cluster. When the number of remaining available compute nodes is less than the number of compute nodes in the DR center to be deployed, deployment is not allowed.

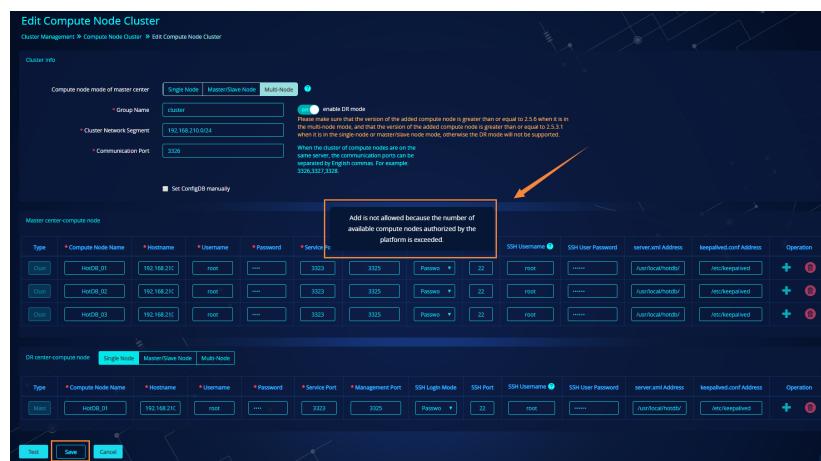


(5) Restrictions of platform license on cluster editing

- When the number of compute nodes in the group has reached the number of available compute nodes in each cluster of the license limit, click [Add compute nodes], it will prompt: Add is not allowed because the number of available compute nodes authorized by the platform is exceeded.



- When DR mode is enabled on the Edit Compute Node Cluster page, if the number of compute nodes in the group exceeds the number of available compute nodes in each group limited by the license, the current cluster will not be saved when you click [Save], and it will prompt: "Add is not allowed because the number of available compute nodes authorized by the platform is exceeded."

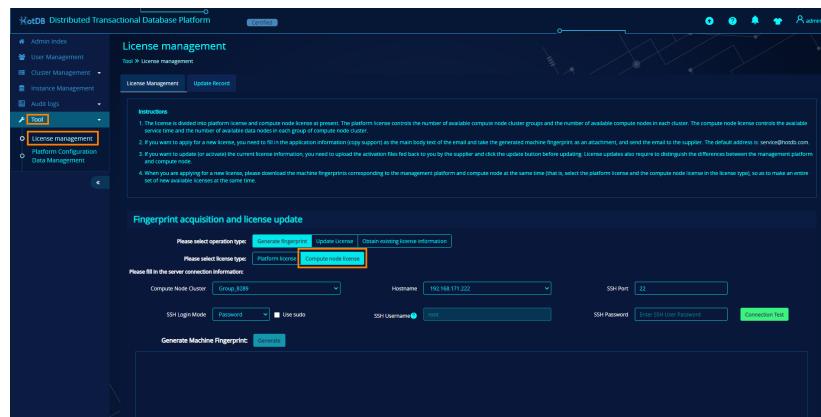


The screenshot shows the 'Edit Compute Node Cluster' interface. In the top left, there's a warning message: "Add is not allowed because the number of available compute nodes authorized by the platform is exceeded." An orange arrow points from this message to the 'Master center-compute node' table below. The table lists three entries: 'HostOr_01', 'HostOr_02', and 'HostOr_03'. Each entry has columns for Type, Compute Node Name, Hostname, Username, Password, Service Port, Management Port, SSH Login Mode, SSH Port, SSH Username, SSH User Password, server.xml Address, keepalive.conf Address, and Operation. At the bottom of the table, there are 'Save' and 'Cancel' buttons.

9.1.2 Compute node license

9.1.2.1 Update entry

- “License Management” in the “Tool” menu under admin role.

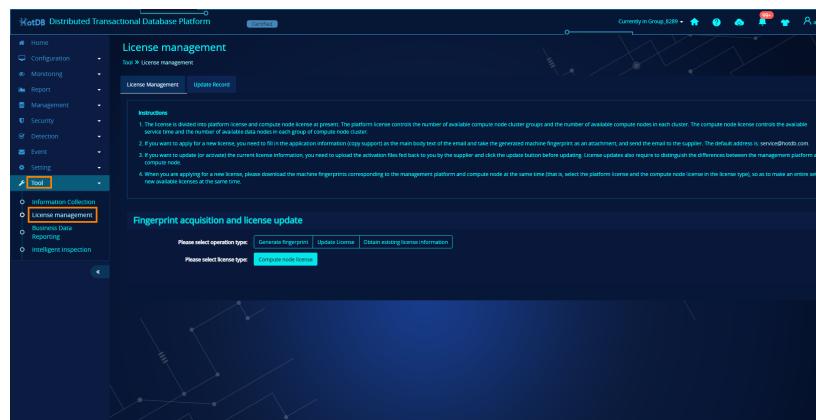


The screenshot shows the 'License management' page. On the left, there's a sidebar with 'Admin index', 'User Management', 'Cluster Management', 'Instance Management', 'Audit Log', 'Audit Log', 'License management' (which is highlighted), 'Platform Configuration', and 'Data Management'. The main area is titled 'License management' and 'Tool > License management'. It contains sections for 'Instructions' (with 4 numbered steps) and 'Fingerprint acquisition and license update'. Under 'Fingerprint acquisition and license update', there are tabs for 'Generate Fingerprint', 'Upload license', and 'Download existing license information'. A dropdown 'Please select operator type' is set to 'Generate Fingerprint'. A dropdown 'Please select license type' is set to 'Platform license' (which is highlighted). Below these are fields for 'Please fill in the server connection information': 'Compute Node Cluster' (set to 'Group_B3B9'), 'Hostname' (set to '192.168.171.222'), 'SSH Port' (set to '22'), 'SSH Login Mode' (dropdown), 'Password' (dropdown), 'Use Sudo' (checkbox), 'SSH Username' (set to 'root'), 'Enter SSH User Password' (text input), and 'Connection Test' (button). At the bottom is a 'Generate Machine Fingerprint' button.

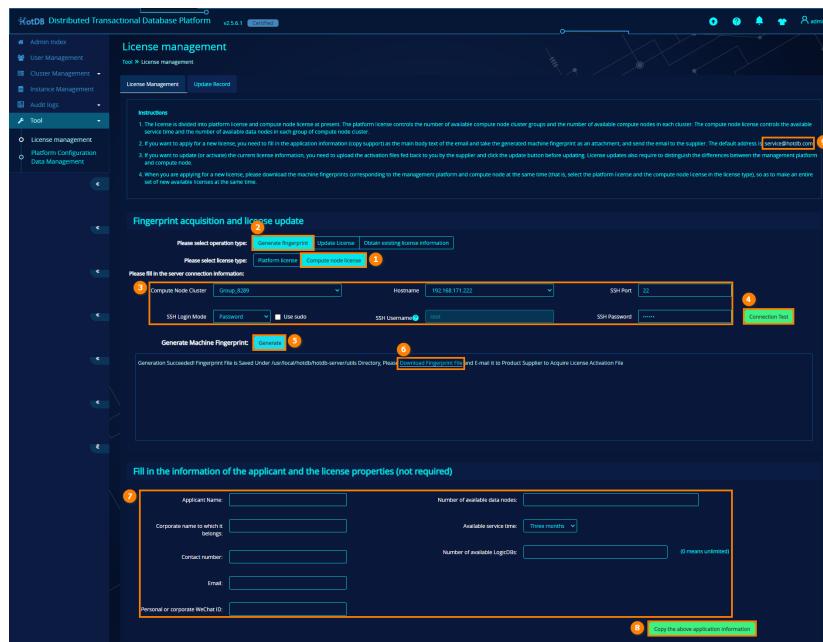
- “License Management” in the “Tool” menu under general role.



- The "license management" hyperlink in the “certified” menu of management platform under general role.



9.1.2.2 Generate fingerprint



Step 1: select the [Compute node license] for License Type;

Step 2: select the [Generate fingerprint] for Operation Type;

Step 3: select the [Compute Node Cluster] and [Hostname] to be operated and execute on all servers of all compute nodes in the cluster. Then fill in the SSH connection information of the corresponding server;

Step 4: click [Connection Test] to check the availability of SSH information. Only through SSH connection test can follow-up operation be carried out;

Step 5: click [Generate] to generate the fingerprint;

Step 6: after the fingerprint is generated successfully, the corresponding prompt will be output in the information column, and you can click [Download Fingerprint File];

Step 7: if you want to apply for custom license information, you can fill in the information of the applicant and license properties (not required);

Fill in the information of the applicant and the license properties (not required)

Applicant Name:	SanZhang	Number of available data nodes:	128
Corporate name to which it belongs:	XK Technology Co., Ltd	Available service time:	One year
Contact number:	13800000000	Number of available LogicDBs:	8 (0 means unlimited)
Email:	zhangsan@qq.com		
Personal or corporate WeChat ID:	zhangsan123	Copy the above application information	

Step 8: click [Copy the above application information] to copy the filled information to the cutting board;

Step 9: click the hyperlink of the email address, the existing local mailbox will be automatically opened. Paste the information copied in the previous step into the email body, and send the email with fingerprint file as an attachment to the supplier.

收件人: 热数据库技术咨询<service@hotdb.com>;
 抄送:
 主题: Authorization license application, Name_Corporate name

微软Word 10.5

Fill in the information of the applicant and the license properties:

Applicant Name:SanZhang
 Corporate name to which it belongs:XX Technology Co., Ltd
 Contact number:13800000000
 Email:zhangsan@qq.com
 Personal or corporate WeChat ID:zhangsan123
 License type:Compute node license
 Number of available data nodes:128
 Available service time:One year
 Number of available LogicDBs:8

9.1.2.3 Update license

HotDB Distributed Transactional Database Platform

Fingerprint acquisition and license update

Please select operation type: Generate Fingerprint, Update license, Obtain existing license information
 Please select license type: Platform license, Compute node license

Please fill in the server connection information:

③ Compute Node Cluster: Group_A3B Hostname: 192.168.1.111.222 SSH Port: 22
 SSH Login Mode: Password, SSH Username: root, SSH Password: Connection Test
 ④ Update License: File path: /tmp/registration/2020-12-10-15-09-2-222 License
 ⑤ Verifying license... Update Successful! License validity is verified successfully

Step 1: select the [Compute node license] for License Type

Step 2: select the [Update license] for Operation Type;

Step 3: select the [Compute Node Cluster] and [Hostname] to be operated and execute on all servers of all compute nodes in the cluster. Then fill in the SSH connection information of the corresponding server;

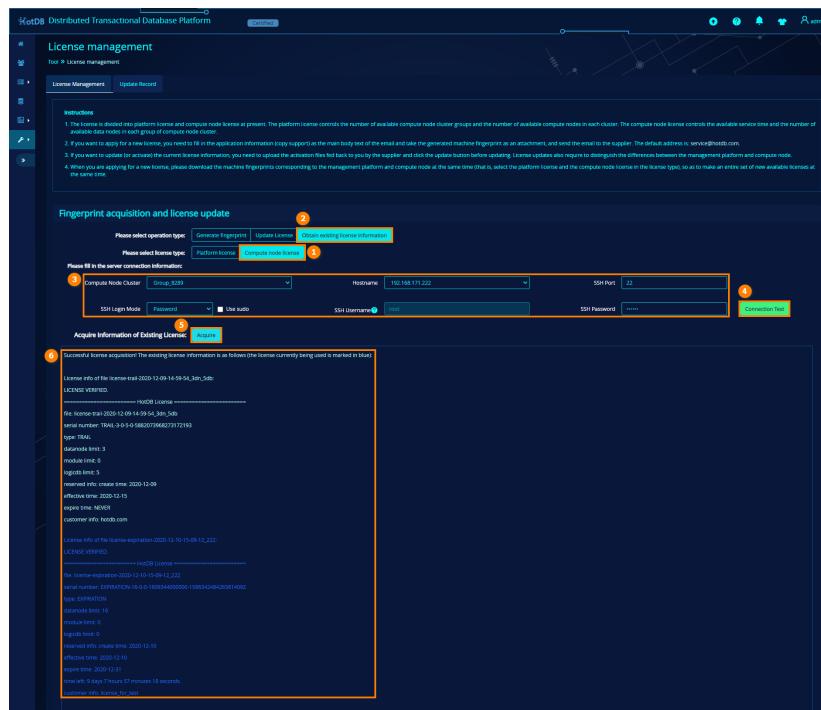
Step 4: click [Connection Test] to check the availability of SSH information. Only through SSH connection test can follow-up operation be carried out;

Step 5: click [Select] to select license file;

Step 6: click [Update] to check and update the license;

Step 7: the corresponding update information will be output in the information column;

9.1.2.4 Obtain existing license information



Step 1: select the [Compute node license] for License Type;

Step 2: select the [Obtain existing license information] for Operation Type;

Step 3: select the [Compute Node Cluster] and [Hostname] to be operated and execute on all servers of all compute nodes in the cluster. Then fill in the SSH connection information of the corresponding server;

Step 4: click [Connection Test] to check the availability of SSH information. Only through SSH connection test can follow-up operation be carried out;

Step 5: click [Acquire] to obtain existing license information;

Step 6: after successful acquisition, the information all available licenses of the corresponding compute node will be output in the information column, among which the one marked in blue is the license currently being used;

9.1.2.5 Other instructions

- When the compute node version is lower than V2.5.6, the license management activates and updates the license according to the historical logic;
- If the compute node is not running normally, you need to manually specify the installation directory of the compute node. The entered directory needs to end with /. Then click [Continue to Update];

- If an activation file with the same name is found under the key/ directory of the installation directory of the compute node, it will prompt whether to replace. Click

[Confirm to Replace], the old activation file will be replaced and the new file will be put in the /key directory;

- When the license is updated, the validity of the license will be checked. The check items include whether the license is available, whether the number of authorized nodes meets the current number of existing nodes, and whether the number of authorized LogicDBs meets the current number of existing LogicDBs. If the new license does not meet the validity check, it will prompt that the update is invalid;

- If sudo mode is used for license management, sudo users and privileges should be configured in advance. In particular, the java environment variables of sudo users also need to be configured.

9.1.2 Update record

License management						
License Management		Update Record				
License update type	Compute Node Cluster	IP Address	Update Time	Operation User	Update Status	License Information before Update
Platform license	--	192.168.171.221	2020-12-21 16:52:12	admin	Upgraded Successfully	Authentication type:Trial version Number of available compute node cluster groups:16 Number of compute nodes available for each cluster:9
Platform license	--	192.168.171.221	2020-12-21 16:38:32	admin	Upgraded Successfully	Authentication type:Trial version Number of available compute node cluster groups:16 Number of compute nodes available for each cluster:9
Platform license	--	192.168.171.221	2020-12-21 16:38:20	admin	Upgrade Failed	The license validity verification failed. Reason for failure: The number of available logic libraries for the newly authorized license is less than the number of currently existing logic libraries, and this update is invalid.
Compute node license	Group_8289	192.168.171.222	2020-12-21 16:35:56	admin	Upgraded Successfully	Fail to get uskKey information
Compute node license	Group_8289	192.168.171.222	2020-12-21 16:34:05	admin	Upgraded Successfully	Fail to get uskKey information
Compute node license	Group_8289	192.168.171.222	2020-12-21 15:57:51	admin	Upgraded Successfully	License type:Trial License status:Normal License remaining time:永不过期 Limit the number of logic nodes:5 Limit the number of logic nodes:16

- The update record is primarily the user's update and authorization operation records of the compute node license and the platform license.
- In update failure records, move the mouse cursor cursor into the failure mark to see the specific reason for failure.
- The record can view the status information of the compute node license and the platform license before and after the update.
- When the license update type is platform license, the column of compute node cluster displays "--";
- The admin user can view all the update records, while the general user can only view the update records of the compute node cluster that he has visited.

9.2. Platform configuration data management

The platform ConfigDB supports the high availability mode. When the platform ConfigDB fails, it can switch to the slave ConfigDB. Function entry: admin > Tool > Platform Configuration Data Management.

Platform Configuration Data Management								
Platform ConfigDB status and operation								
Hostname	Port	ConfigDB	Configuration users	Type	Available	Master-slave replication status	Master-slave replication latency	Master-slave switch
192.168.210.134	3308	hotdb_cloud_config134	hotdb_cloud	Active Master	Available	Normal		
192.168.210.135	3308	hotdb_cloud_config134	hotdb_cloud	Standby Master	Available	Normal		 

9.2.1 ConfigDB file management

Add three parameters in the configuration file application.properties: spring.datasource.bakurl/spring.datasource.bakusername/spring.datasource.bakpassword. When spring.datasource.bakurl and spring.datasource.url correspond to the same ConfigDB instance, it is regarded as single-node mode. In high availability mode, the two parameters need to be configured as master and standby master or master and slave respectively.

If the slave ConfigDB is not added through platform cluster deployment or stand-IDC deployment, the replication relation between the master and slave ConfigDBs needs to be built manually. The corresponding types will be displayed on the platform configuration data management page according to the master-master and master-slave replication relation.

Configure master-master or master-slave type:

```
spring.datasource.url=jdbc:mysql://192.168.210.134:3308/hotdb_cloud_config134?useUnicode=true&characterEncoding=UTF-8&autoReconnect=true&connectTimeout=3000&socketTimeout=3600000&useSSL=false

spring.datasource.username=hotdb_cloud

spring.datasource.password=hotdb_cloud

spring.datasource.bakurl=jdbc:mysql://192.168.210.135:3308/hotdb_cloud_config134?useUnicode=true&characterEncoding=UTF-8&autoReconnect=true&connectTimeout=3000&socketTimeout=3600000&useSSL=false

spring.datasource.bakusername=hotdb_cloud

spring.datasource.bakpassword=hotdb_cloud
```

When starting the management platform service program, if the master ConfigDB is not available, it will fail after reconnection for 30 minutes (reconnection every 10 seconds, timeout for 5 seconds will be judged as failure). If the master ConfigDB is available and the slave ConfigDB is not available, the slave ConfigDB can be

reconnected for 10 minutes at most. If it is unable to connect eventually, the slave ConfigDB will be set to "not available" and the master ConfigDB will be started in "available" status.

9.2.2 Platform ConfigDB Status and Operation

Users can perform switching, enabling, disabling, deletion and other operations to the platform ConfigDB on the platform configuration data management page.

Platform ConfigDB status and operation									
Hostname	Port	ConfigDB	Configuration users	Type	Available	Master-slave replication status	Master-slave replication latency	Master-slave switch	Operation
192.168.210.135	3308	hotdb_cloud_config134	hotdb_cloud	Active Master	Available	Normal			
192.168.210.134	3308	hotdb_cloud_config134	hotdb_cloud	Standby Master	Available	Normal			

● Active ● Slave ● Unavailable

(1) Switch

After the switching of master-master ConfigDB, the original standby master ConfigDB will be updated to the master ConfigDB, and the original master ConfigDB will be updated to the standby master ConfigDB. Parameters in the corresponding configuration file application.properties in spring.datasource.bakurl will be updated synchronously.

The standby master ConfigDB will be updated to:

```
spring.datasource.url=jdbc:mysql://192.168.210.135:3308/hotdb_cloud_config134?useUnicode=true&characterEncoding=UTF-8&autoReconnect=true&connectTimeout=3000&socketTimeout=3600000&useSSL=false

spring.datasource.username=hotdb_cloud

spring.datasource.password=hotdb_cloud

spring.datasource.bakurl=jdbc:mysql://192.168.210.134:3308/hotdb_cloud_config134?useUnicode=true&characterEncoding=UTF-8&autoReconnect=true&connectTimeout=3000&socketTimeout=3600000&useSSL=false
```

```
spring.datasource.bakusername=hotdb_cloud
```

```
spring.datasource.bakpassword=hotdb_cloud
```

After the switching of master-slave ConfigDB, the original slave ConfigDB will be updated to the master ConfigDB, and the original master ConfigDB will be updated to the slave ConfigDB, and the slave ConfigDB status will be updated to "unavailable".

Platform ConfigDB status and operation									
Hostname	Port	ConfigDB	Configuration users	Type	Available	Master-slave replication status	Master-slave replication latency	Master-slave switch	Operation
192.168.210.134	3308	hotdb_cloud_config134	hotdb_cloud	Active Master	Available	Normal	Normal		
192.168.210.135	3308	hotdb_cloud_config134	hotdb_cloud	Standby Slave	Unavailable	Abnormal	Normal		

(2) Disable

Click “Disable”, the availability status of the ConfigDB will be updated to “unavailable” and marked in red, the master-slave replication status will be “abnormal”, and “Disable” will be updated to “Enable”.

Platform ConfigDB status and operation									
Hostname	Port	ConfigDB	Configuration users	Type	Available	Master-slave replication status	Master-slave replication latency	Master-slave switch	Operation
192.168.210.135	3308	hotdb_cloud_config134	hotdb_cloud	Active Master	Available	Normal	Normal		
192.168.210.134	3308	hotdb_cloud_config134	hotdb_cloud	Standby Master	Unavailable	Abnormal	Normal		

(3) Enable

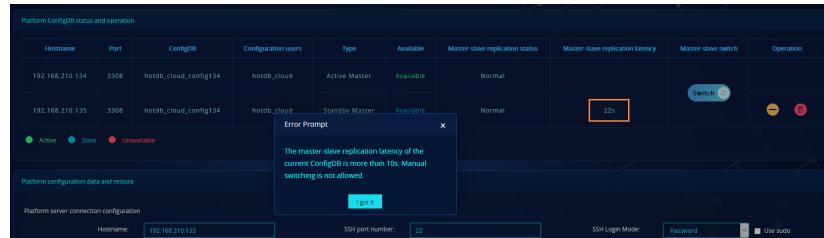
Click “Enable”, the availability status, master-slave replication status and operation button will be restored to the previous status.

Platform ConfigDB status and operation									
Hostname	Port	ConfigDB	Configuration users	Type	Available	Master-slave replication status	Master-slave replication latency	Master-slave switch	Operation
192.168.210.135	3308	hotdb_cloud_config134	hotdb_cloud	Active Master	Available	Normal	Normal		
192.168.210.134	3308	hotdb_cloud_config134	hotdb_cloud	Standby Master	Available	Normal	Normal		

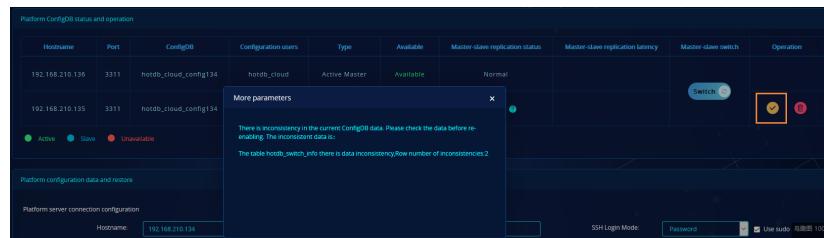
Notes:

- In the single-node mode, there are no switching, disabling, deletion and other operations.

- When the slave ConfigDB is unavailable, the switching operation will prompt that there is no available slave ConfigDB.
- If the replication latency exceeds 10 seconds, it will prompt "the master-slave replication latency of the current ConfigDB exceeds 10s, manual switch is not allowed.".



- When enabling the slave ConfigDB, if the data of the master and slave ConfigDBs are inconsistent, switch is not allowed.



9.2.3 Platform configuration backup data

The function supports manual and scheduled backup for the platform ConfigDB and ConfigDB files. For scheduled backup, the backup task is performed by the scheduled plan instead of manual operation.

Platform configuration data and restore

Platform server connection configuration

Hostname:	192.168.210.133	SSH port number:	22	SSH Login Mode:	Password	<input type="checkbox"/> Use sudo
SSH user name:	root	SSH password:	*****	<input type="button" value="Test connection and save"/>		

Manual Backup

Backup platform metadata:	ConfigDB	Backup range:	Backup basic data only	Configuration File Name:	ManagementConfigData	<input type="checkbox"/> Backup to Remote Simultaneously	<input type="button" value="Launch Backup"/>
---------------------------	----------	---------------	------------------------	--------------------------	----------------------	--	--

When only the basic data is backed up, the backed up tables can be used when the platform recovers the basic data. Special large tables will not be backed up. For example, tables related to functions such as reports, monitoring, intelligent query of operation logs, and compute node logs will not be backed up.

Periodical Backup

Backup Metadata	Backup Period	Backup Time	Backup to Remote	Backup Range	Operation	<input type="button" value="+"/>
ConfigDB	Daily	21:30	Yes	Backup basic data only		
ConfigDB	Daily	10:30	No	Full backup		
ConfigDB	Daily	03:00	No	Full backup		

Remote Replication Mode: SCP RSYNC

Remote Hostname:	192.168.210.134	Remote Host User:	root	<input type="checkbox"/> Sign in without password
File save directory:	/var/local/HotDB	Remote Host Password:	*****	

(1) Platform server connection configuration

Platform server connection configuration

Hostname:	192.168.210.133	SSH port number:	22	SSH Login Mode:	Password	<input type="checkbox"/> Use sudo
SSH user name:	root	SSH password:	*****	<input type="button" value="Test connection and save"/>		

- Connection configuration is required before backup. The configured server host name must be consistent with the server host name where the service program runs.
- SSH supports password free and sudo mode. After the test connection is passed, the configuration is saved directly, and no filling will be required in the next time.

(2) Manual backup

For manual backup, ConfigDB and backup basic data only are selected by default. The format of backup file name is ManagementConfigDatabase+year+month+day+hour+minute+second+backup type. After selecting to backup ConfigDB or ConfigFile, the backup will generate the corresponding backup record.

- When “backup basic data only” is selected, it will prompt that “when only the basic data is backed up, the backed-up tables can be used when the platform recovers the basic data. Special large tables will not be backed up. For example, tables related to functions such as reports, monitoring, intelligent query of operation logs, and compute node logs will not be backed up.”.

Manual Backup

Backup platform metadata:	ConfigDB	Backup range:	Backup basic data only	Configuration File Name:	ManagementConfigData	<input type="checkbox"/> Backup to Remote Simultaneously	<input type="button" value="Launch Backup"/>
---------------------------	----------	---------------	------------------------	--------------------------	----------------------	--	--

When only the basic data is backed up, the backed up tables can be used when the platform recovers the basic data. Special large tables will not be backed up. For example, tables related to functions such as reports, monitoring, intelligent query of operation logs, and compute node logs will not be backed up.

- When “full backup” is selected, it will prompt that “full backup may take a long time, please be patient.”



When “ConfigFile” is selected, the file application.properties is mainly backed up. The default format of the backup file name is ManagementConfigDatabase+year+month+day+hour+minute+second+backup type. “Backup to remote simultaneously” is checked compulsorily, and a corresponding prompt will be given when the cursor moves in.



(3) Scheduled backup

Add a scheduled backup task, and backup the platform ConfigDB and ConfigFile regularly.

Periodical Backup					
Backup Metadata	Backup Period	Backup Time	Backup to Remote	Backup range	Operation
ConfigDB	Daily	14:00	No	Full backup	
ConfigDB	Daily	13:30	No	Backup basic data only	
ConfigFile	Daily	03:00	Yes		

Remote Replication Mode: SCP RSYNC

Remote Hostname: 192.168.210.133 Remote Host User: root Sign in without password

File save directory: /usr/local/hotdb/ Remote Host Password: *****

For backup data, you can select ConfigDB and ConfigFile. When “ConfigDB” is selected, you shall select the “Backup range” and “Backup to remote simultaneously”; when “ConfigFile” is selected, you shall fill in the remote backup server information.

9.2.4 Backup record & restore

When a manual or scheduled task is performed, the corresponding backup record will be generated. After the backup succeeds, the backup can be restored.

Backup Record						
	Backup Metadata	Configuration File Name	Backup Range	Starting Time	Time Consuming	Backup to Remote Simultaneously
■	Backup ConfigDB	ManagementConfigDatabase_202001030140000_Auto_allData.dump	Full backup	2020-10-30 14:00:00	4s	No
■	Backup ConfigDB	ManagementConfigDatabase_202001030153000_Auto_allData.dump	Full backup	2020-10-30 13:30:00	4s	No
■	Backup ConfigDB	ManagementConfigDatabase_20201030030000_Auto_basicData.dump	Backup basic data only	2020-10-30 03:00:00	0ms	No
■	Backup ConfigDB	ManagementConfigDatabase_20201030030000_Auto_allData.dump	Full backup	2020-10-30 03:00:00	4s	No
■	Backup ConfigDB	ManagementConfigDatabase_2020010209173636_Manual_basicData.dump	Backup basic data only	2020-10-29 17:36:30	1s	No
■	Backup configuration file	ManagementConfigFile_202001027180736_Manual		2020-10-27 18:07:38	1s	Yes
■	Backup configuration file	ManagementConfigFile_202001027180526_Manual		2020-10-27 18:05:27	1s	Yes
■	Backup configuration file	ManagementConfigFile_202001027104808_Manual		2020-10-27 10:48:10	0ms	Yes
■	Backup ConfigDB	ManagementConfigDatabase_20201023103000_Auto_allData.dump	Full backup	2020-10-23 10:30:00	25s	No
■	Backup ConfigDB	ManagementConfigDatabase_20201023103000_Auto_basicData.dump	Backup basic data only	2020-10-23 10:30:00	0ms	No

From 1 to 10 Records, from 1 / 20 page Prev [1] 2 3 4 5 ... 20 Next Jump to P Go

(1) Backup record

Backup record includes: Data type, ConfigFile name, Backup range, Starting time, time consuming, Backup to remote simultaneously, backup status. After the backup succeeds, the ConfigDB backup file will be saved in the corresponding data/HotDB_Management_Backup of the management platform, and the ConfigFile will be saved in the /conf directory, as shown in the following figure:

ManagementConfigDatabase_202001030190958_Manual_basicData.dump	ManagementConfigFile_20201031180000_Auto
ManagementConfigDatabase_202001030191023_Manual_allData.dump	ManagementConfigFile_20201011180000_Auto
ManagementConfigDatabase_202001030191106_Manual_allData.dump	ManagementConfigFile_20201102103000_Auto
ManagementConfigDatabase_202001030191136_Manual_allData.dump	ManagementConfigFile_20201102103737_Manual
ManagementConfigDatabase_20201030030000_Auto_allData.dump	ManagementConfigFile_20201102103755_Manual

During the backup, the backup status displays "backup in progress"; after the backup, the backup status displays "success" or "failure". When the backup fails, it will prompt the specific reason of the failure. If the local backup is successful but the remote backup fails, a warning prompt will also be given, as shown in the following figure:

■	Backup ConfigDB	ManagementConfigDatabase_20200821173000_Auto_allData.dump	Full backup	2020-08-21 17:30:00	3s	No	Local backup succeeded but data backup to remote server failed
■	Backup ConfigDB	ManagementConfigDatabase_20200820173504_Manual_allData.dump	Full backup	2020-08-20 17:36:34	15s	Yes	Success

(2) Backup restore

After the backup, find the corresponding record and click Restore to restore the backup.

Notes:

- During the restore, if you perform other operations on the management platform, it will prompt "Operations are not allowed temporarily because the management

platform ConfigDB is being restored".

- When restoring, if the configuration library of the management platform is changed, you will be prompted that "the currently restored ConfigDB is inconsistent with the original ConfigDB. Are you sure to continue the restore?".



- During the restore, if the backup file is deleted, the restore will fail and a prompt will be given "restore file does not exist".

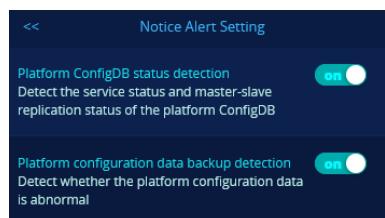
(3) Backup deletion

Click Delete to delete the backup record. After deletion, the corresponding backup files in the platform service program directory will also be deleted.

9.2.5 Other instructions

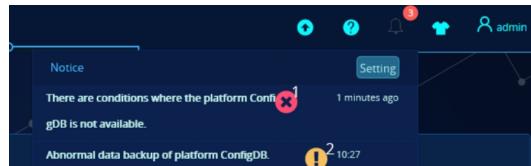
(1) Notice alert

Click Notice on the top navigation bar and click the "Setting" button to enable or disable the notice alert of "platform ConfigDB status detection and platform configuration data backup detection".



- When the ConfigDB is in single-node mode, the "platform ConfigDB status detection" will be hidden:
- After the notice alert setting is enabled, the notice alert will give a reminder when the ConfigDB status is abnormal, the replication relations between the master-slave

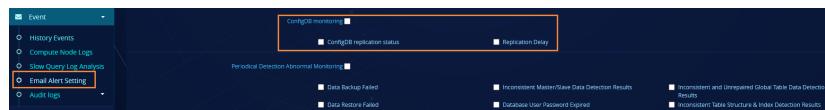
ConfigDBs is abnormal, or the latest backup record shows that the configuration backup is abnormal.



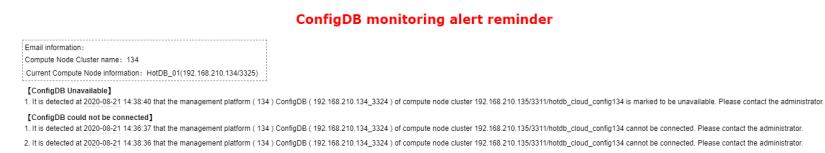
- After the exception is recovered, reminders will disappear automatically.
- With notice alert disabled, no reminders will be given if exception occurs.

(2) Email alert

Check ConfigDB replication status and Replication delay, you will receive an email reminder when the ConfigDB status or replication status is abnormal.



- The email reminder for abnormal status of ConfigDB replication is as follows:



- The email reminder for abnormal replication relations of ConfigDB is as follows:



(3) Cluster deployment

When the platform ConfigDB is in single-node mode, the switch "Do you want to add a slave for the existing platform ConfigDB" will be displayed on the cluster deployment parameter configuration page; if the current ConfigDB is already in standby master mode or master-slave mode, this switch will not be displayed.



- The deployment version is consistent with the existing platform ConfigDB and cannot be modified.
- The platform ConfigDB being deployed cannot conflict with the existing platform ConfigDB, the deployed compute node ConfigDB or the data source instance.
- If the management platform ConfigDB is deployed, the replication relations of the platform ConfigDB and whether it is built successfully will also be verified during the deployment process.

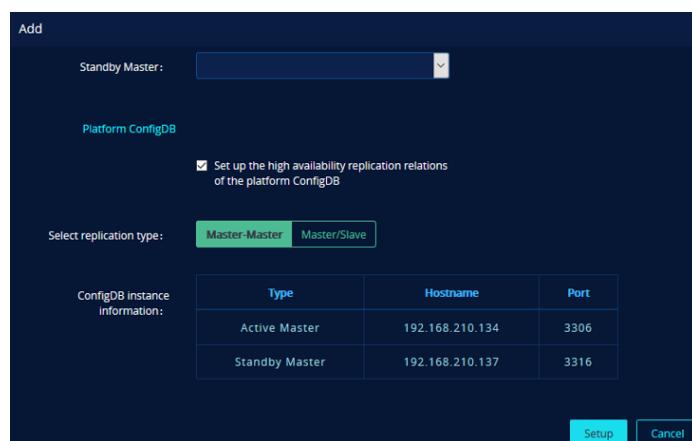
(4) Single-IDC deployment

For the single-IDC deployment, when selecting to deploy compute node or data source servers, the switch "Do you want to add a slave for the existing platform ConfigDB" will be displayed among the ConfigDB MySQL instance options. This option is only displayed when the platform ConfigDB is in single-node mode, and it is checked by default.



After the single-IDC deployment, you can set up platform ConfigDB high availability in the ConfigDB high availability setup.

- By default, replication type and platform ConfigDB instance are not displayed. When “Set up the high available replication relations of the platform ConfigDB” is checked, the select replication type (master-master or master/slave) and ConfigDB instance information are displayed.

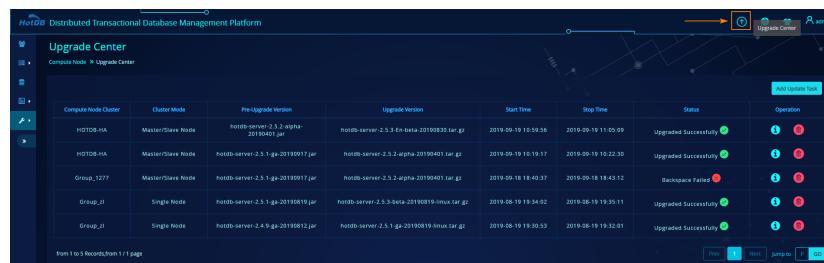


- Before setting up replication, data of the original master ConfigDB needs to be imported to the new slave ConfigDB.
- After the setup, you can view the availability status and replicaiton status of the ConfigDB on the "Platform Configuration Data Management" page, and the corresponding configuration files application.properties will also be updated synchronously.

10. Upgrade center

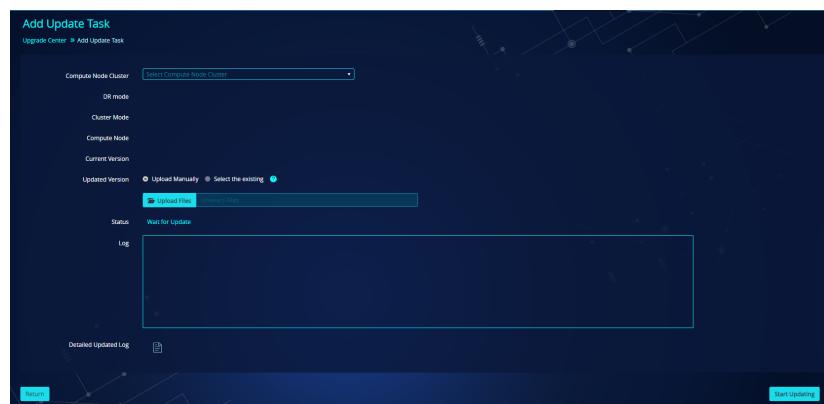
The upgrade center provides HotDB Management with the online upgrade function for compute node version. It satisfies the iteration of cross-version or minor version upgrade for single-node, master/slave, multi-node and DR mode cluster. At the same time, it can provide users with automatic rollback protection mechanism when exceptions occur during upgrade process. The program tries to ensure that the cluster is rolled back to the pre-upgrade status to reduce the impact on online services.

Function Entry: Login Management User Interface -> “Upgrade Center” in the upper right corner of the page



Compute Node Cluster	Cluster Mode	Pre-Upgrade Version	Upgrade Version	Start Time	Stop Time	Status	Operation
HOTDB-HA	Master/Slave Node	hotdb-server-2.5.2-alpha-20190403.jar	hotdb-server-2.5.3-bin-beta-20190830.tar.gz	2019-09-19 10:59:56	2019-09-19 11:05:09	Upgraded Successfully	OK
HOTDB-HA	Master/Slave Node	hotdb-server-2.5.1-ga-20190917.jar	hotdb-server-2.5.2-alpha-20190401.tar.gz	2019-09-19 10:10:17	2019-09-19 10:22:30	Upgraded Successfully	OK
Group_1277	Master/Slave Node	hotdb-server-2.5.1-ga-20190917.jar	hotdb-server-2.5.2-alpha-20190401.tar.gz	2019-09-18 18:40:37	2019-09-18 19:43:12	BackupSpace Failed	Error
Group_21	Single Node	hotdb-server-2.5.1-ga-20190919.jar	hotdb-server-2.5.3-alpha-20190819-linux.tar.gz	2019-09-19 18:42:02	2019-09-19 19:35:11	Upgraded Successfully	OK
Group_21	Single Node	hotdb-server-2.4.9-ga-20190812.jar	hotdb-server-2.5.1-ga-20190819-linux.tar.gz	2019-09-19 19:30:53	2019-09-19 19:32:01	Upgraded Successfully	OK

Click the [Add Upgrade Task] button to enter the upgrade center to Start an upgrade task. Details are as follows:



Add Update Task

Upgrade Center > Add Update Task

Compute Node Cluster: Select Compute Node Cluster

DR mode: DR mode

Cluster Mode: Cluster Mode

Compute Node: Compute Node

Current Version: Current Version

Updated Version: Upload Manually Select the existing

Upload File:

Status: Wait for Update

Log: Detailed Updated Log

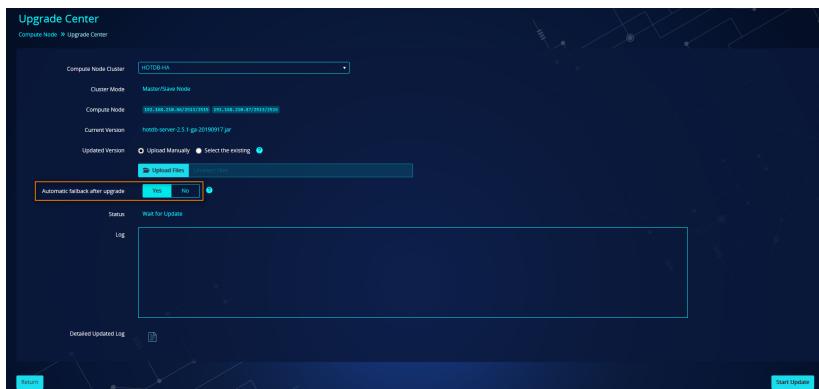
Start Upgrading

- Select the compute node cluster that needs to be upgraded.

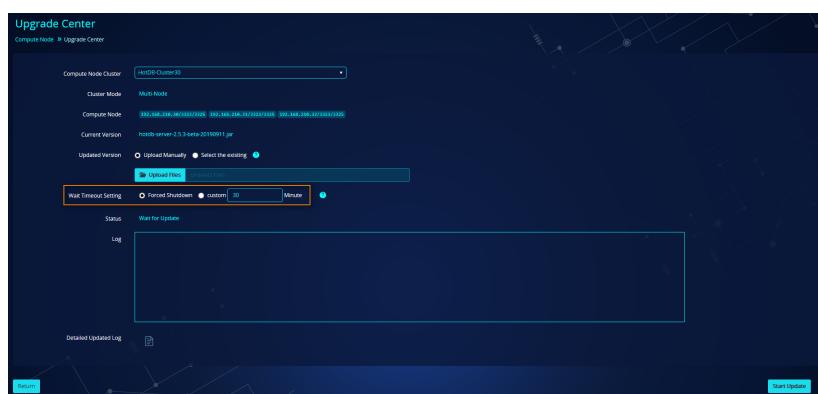
After selecting the cluster, the cluster will be automatically checked to see whether it meets the upgrade criteria:

- The cluster is not currently performing upgrade tasks
- The compute nodes of the cluster are configured with available SSH information
- The master/slave mode cluster also needs to verify whether the available configuration file storage address is configured

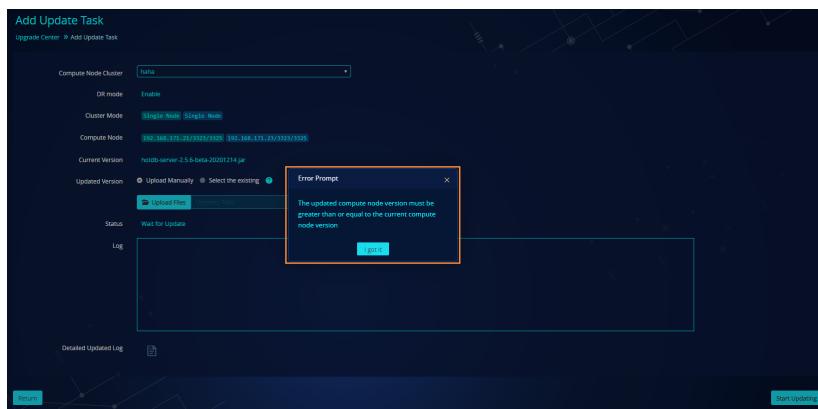
- Clusters that meet the above upgrade conditions will automatically display information such as "DR mode", "cluster mode", "compute node", "current version", "upgrade version", "status", "log". Different cluster modes will be slightly different besides the basic information.
 - When it is in the single-node mode: no other information will be displayed.
 - When it is in the master/slave mode, the message "whether to switch back after upgrading" will be displayed. If "Yes", it will switch back to the original master compute node after the upgrading; if "No", the status of the master and slave nodes after the exchange will be maintained (the master/slave high availability switch will be performed during the upgrading)



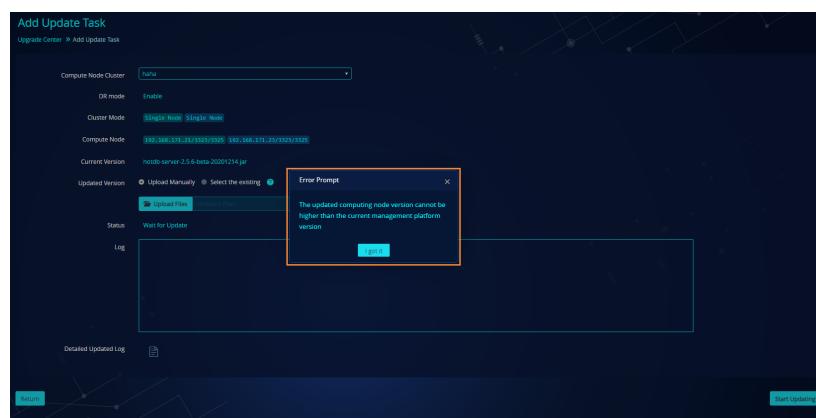
- When the selected compute node cluster is in multi-node mode, the page will display the "Wait Timeout Setting" (QPS needs to be detected when the multi-node cluster shuts down the compute node service. If it is less than 100, the compute node service will be directly closed. If it is greater than or equal to 100, shutdown will be executed after QPS drops to less than 100). If a custom timeout waiting time or a forced shutdown is set, the program can execute a forced shutdown after the custom time or a direct shutdown without waiting.



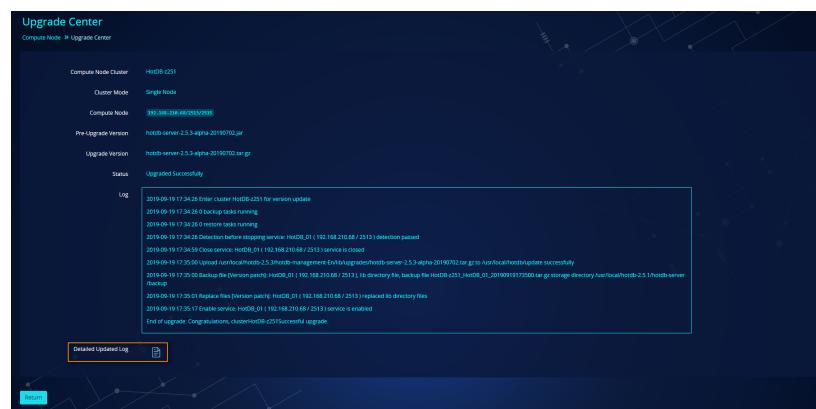
- If the selected cluster is a DR mode cluster, the DR mode will be ON, otherwise it is not.
- Users can manually upload the upgrade version or select the existing upgrade package. The upgrade package uploaded manually is stored under the installation directory /bin/upgrades of the hotdb management server by default. If there is no such directory, the program will create one automatically. (the upgrade version package must be no less than the version of the current compute node and no higher than the version of the current HotDB Management)
- If the uploaded version is less than the current existing version, it will prompt "the updated version must be greater than or equal to the current version".



- If the uploaded version is higher than the current version, it will prompt "the updated version can not be higher than the current version".



- Before clicking [Start Update], the "status" is “wait for update”; after clicking [Start Update], "status" is “updating”; after the update completed, "status" is “successful update or update failed”.
- After clicking the [Start Update] button, if the current compute node is performing tasks such as High availability switch (Master/Slave Mode only), Reload, Data Backup, Data Recovery, Data Source Migration, Online DDL, Sharding Plan Online Modification, Unfinished Transaction, the pre-service detection will not be passed and the upgrade task will fail directly.
- After satisfying the legitimate upgrade logic, click [Start Update] to perform the upgrade task. During the execution of upgrade task, the log box will display the upgrade task log in real time. You can download the detailed update log to view more detailed log info.



- Clusters that fail to upgrade will perform a rollback process, and the program will try to restore the cluster to the status before initial upgrade. If the rollback fails, manual intervention is required to restore the cluster. In case of manual intervention, **Detailed Update Log** can be used to view the commands executed by the program and the stage of upgrade or rollback to help restore the cluster.

```

2019-09-19 17:34:26 Enter cluster HotDB-z251 for version update
2019-09-19 17:34:26 Execute check @upgrade_condition
2019-09-19 17:34:26 0 backup tasks running
2019-09-19 17:34:26 0 restore tasks running
2019-09-19 17:34:26 Detection before stopping service: HotDB_01 ( 192.168.210.68 / 2513 ) detection passed
2019-09-19 17:34:50 Close service: HotDB_01 ( 192.168.210.68 / 2513 ) service is closed
2019-09-19 17:35:00 Upload /usr/local/hotdb-2.5.3/hotdb-management-En/lib/upgrades/hotdb-server-2.5.3-alpha-20190702.tar.gz to
/usr/local/hotdb/update successfully
2019-09-19 17:35:00 Execute mkdir-p /usr/local/hotdb-2.5.1/hotdb-server /backup on host: 192.168.210.68
2019-09-19 17:35:00 Execute cd /usr/local/hotdb-2.5.1/hotdb-server ; tar -zcvf ./backup/HotDB_01_20190919173500.tar.gz lib on host:
192.168.210.68
2019-09-19 17:35:00 Backup file [Version patch]: HotDB_01 ( 192.168.210.68 / 2513 ), lib directory file, backup file HotDB-
z251_HotDB_01_20190919173500.tar.gz storage directory /usr/local/hotdb-2.5.1/hotdb-server /backup
2019-09-19 17:35:00 Execute cd /usr/local/hotdb-2.5.1/hotdb-server ; rm -rf lib on host: 192.168.210.68
2019-09-19 17:35:00 Execute mkdir -p /usr/local/hotdb/update/ PZG4x on host: 192.168.210.68
2019-09-19 17:35:01 Execute tar -zvxf /usr/local/hotdb/update/ hotdb-server-2.5.3-alpha-20190702.tar.gz -C /usr/local/hotdb/update/ PZG4x on
host: 192.168.210.68
2019-09-19 17:35:01 Execute cp -R /usr/local/hotdb/update/ PZG4x /hotdb-server/lib /usr/local/hotdb-2.5.1/hotdb-server /lib on host: 192.168.210.68
2019-09-19 17:35:01 Execute rm -rf /usr/local/hotdb/update/ PZG4x on host: 192.168.210.68
2019-09-19 17:35:01 update_upgrade_info set bak_name='HotDB-z251_HotDB_01_20190919173500.tar.gz' where id=21
2019-09-19 17:35:01 Replace files [Version patch]: HotDB_01 ( 192.168.210.68 / 2513 ) replaced lib directory files
2019-09-19 17:35:17 Enable service: HotDB_01 ( 192.168.210.68 / 2513 ) service is enabled
End of upgrade: Congratulations, clusterHotDB-z251Successful upgrade.

```

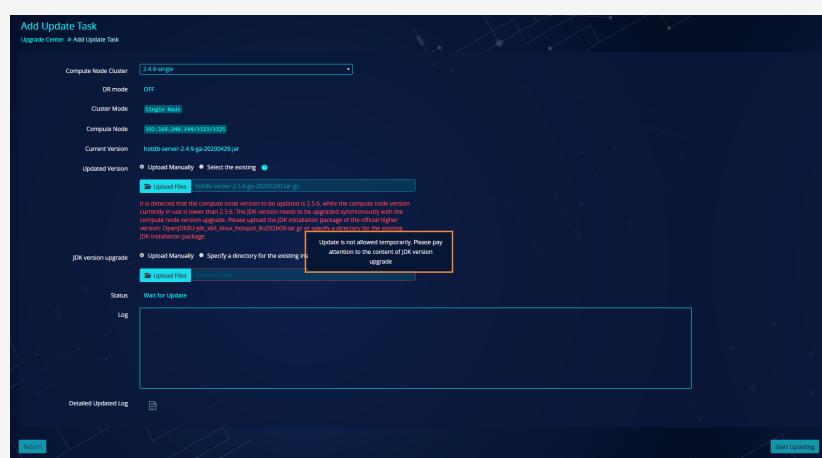
Note:

It supports the version upgrade of the compute nodes with NDB services installed. During the upgrade process, the management platform automatically copies the NDB installation directory of the former compute node to the directory of new compute node version. After the upgrade, the NDB service remains the same as before. Note that in this process the NDB version will not be upgraded.

During the upgrading, check whether the current version to be upgraded is greater than or equal to v2.5.6, and whether the version currently in use is less than v2.5.6. If so, there will be an upgrade entry for JDK version and authorization file.

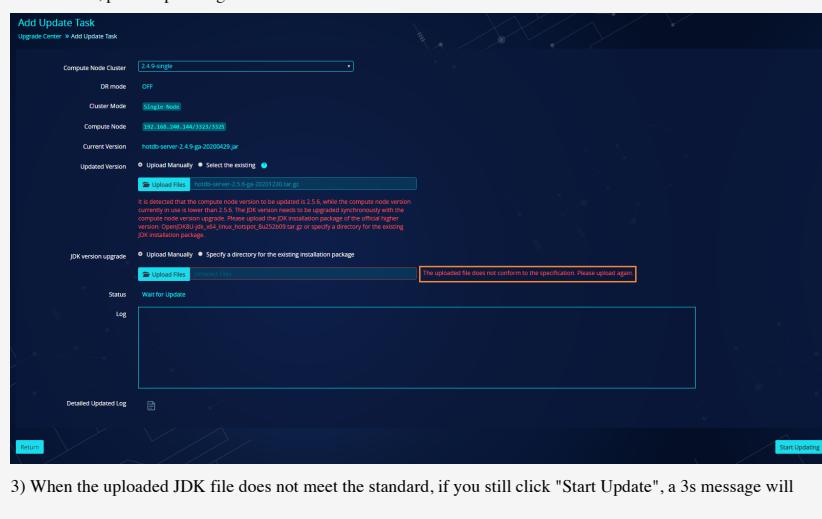
JDK version upgrade: manual upload by default. When "specify the storage directory of existing installation package" is checked, the default directory is /usr/local/hotdb/. Users can also specify the storage directory as needed. When the upgrade fails and rolls back, the upgraded JDK will not be cleaned up, because the JDK version can be compatible with the lower version of the compute node.

1) When the version of the uploaded update package is greater than or equal to 2.5.6 and the current version of is less than 2.5.6, if you click "start update" after the upload succeeds, a 3s message will appear that "Update is not allowed temporarily, please pay attention to the content of JDK version upgrade", and "JDK version upgrade option" will be given at the same time.



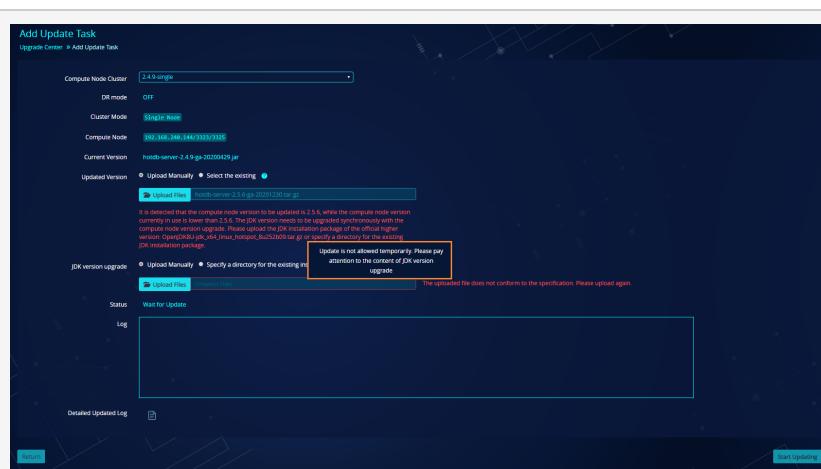
2) If "manual upload" is selected for JDK version upgrade, when the uploaded file does not match

"OpenJDK8U-jdk_x64_linux_hotspot_8u252b09.tar.gz", it will prompt that "the uploaded file does not meet the standard, please upload again".

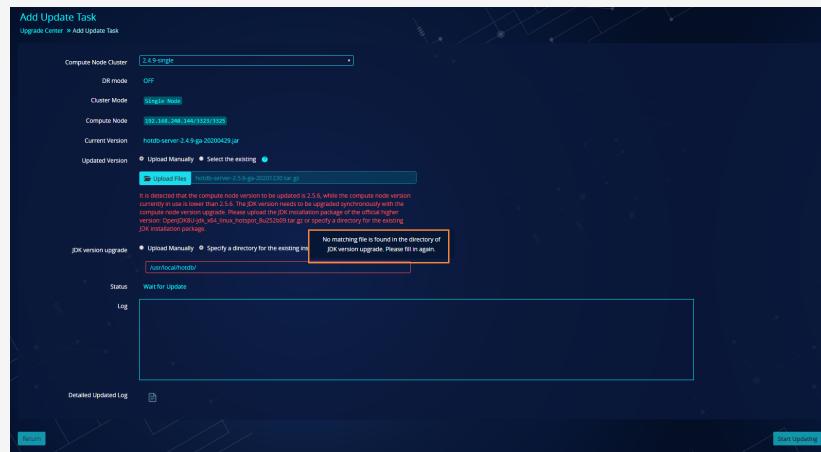


3) When the uploaded JDK file does not meet the standard, if you still click "Start Update", a 3s message will

appear that "Update is not allowed temporarily, please pay attention to the content of JDK version upgrade".



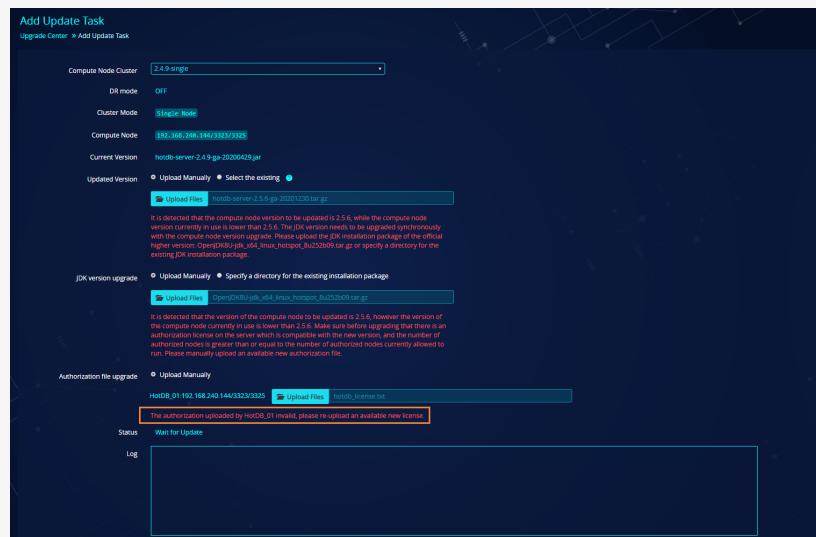
- 4) When "specify the storage directory of existing installation package" is selected for "JDK version upgrade", if no JDK upgrade matching file is found in the corresponding directory, click "Start Update", a 3s message will appear that "No matching file is found in the directory corresponding to JDK version upgrade, please fill in again".



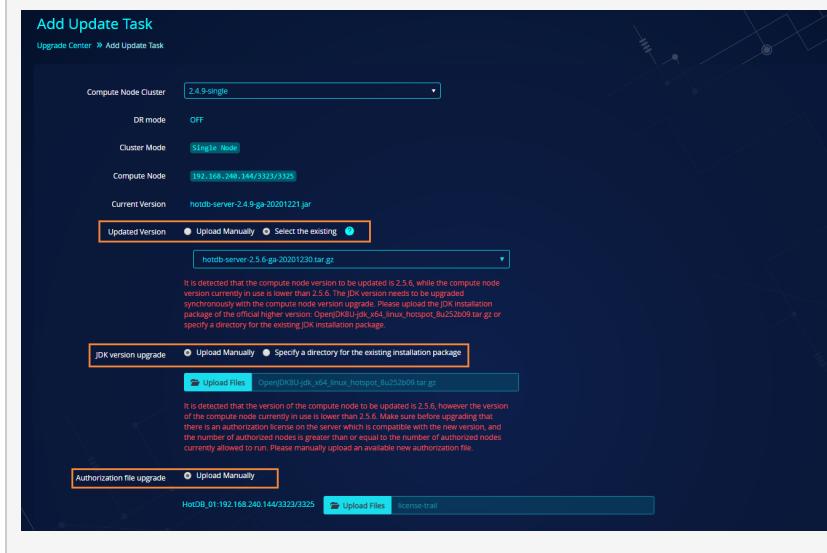
license file upgrade: the self-developed license starts to be used in v2.5.6, and the license file is in the keys directory by default. In upgrading, it is necessary to ensure that the authorization is available and the number of authorized nodes is not less than the number of existing nodes and the number of authorized ConfigDBs is not less than the number of existing ConfigDBs.

- 1) When the user uploads the authorization file, if it is invalid (that is, the new authorization is not available or the number of authorized nodes is less than the number of existing nodes, the number of authorized

ConfigDBs is not less than the number of existing ConfigDBs), a warning will be given on the page "the authorization uploaded by the compute node is invalid, please re-upload available new authorization license file".



when the uploaded update package, JDK version and license of the compute node are valid and available, the upgrade page is as follows



11. OEM management

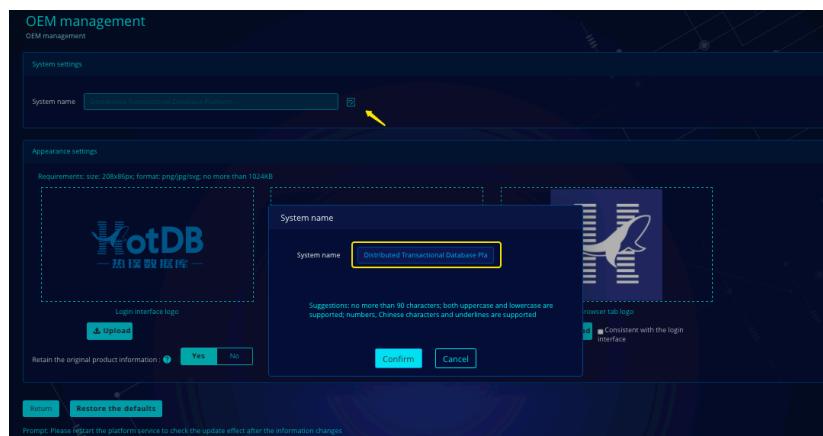
To facilitate the replacement of the product logo and product name of the management platform, OEM management is introduced to provide an entry for visualized updating of logo and product name.

Function entry: manager users can enter the function page through the hyperlink of OEM management after logging in to the platform. The hyperlink path is <http://192.168.240.147:3324/page/index.html?page=oem>, i.e. url of the original page plus ?page=oem.



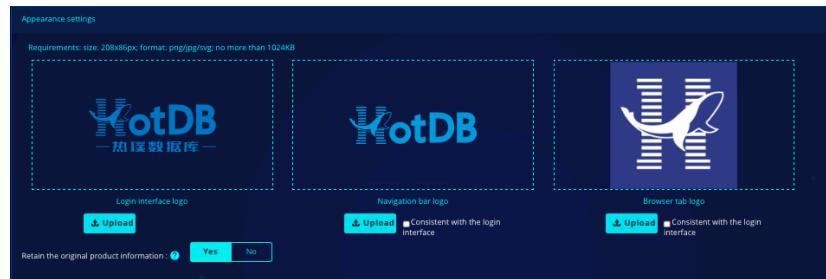
11.1. Modify the system name

Click the edit button of System Name and edit, then click Confirm to save the name. With the system name saved successfully, the name displayed on the management platform login page and the upper left corner of the menu page are modified synchronously.



11.2. Modify the product logo

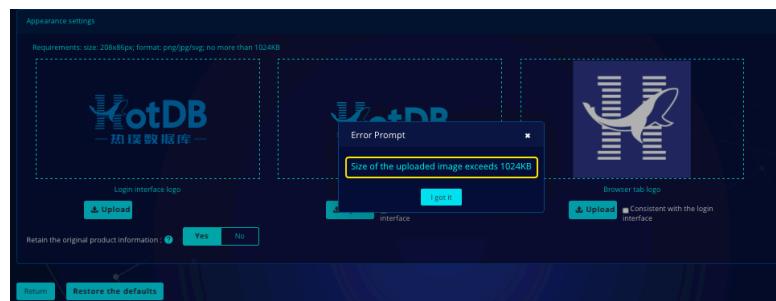
The preview area displays the default logo image of the management platform, as shown below:

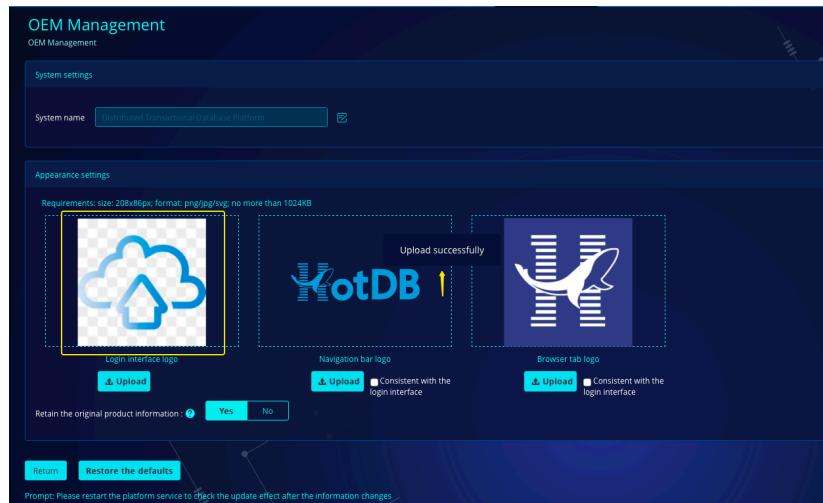


Click [Upload] to open the file selection window, and select the logo image.

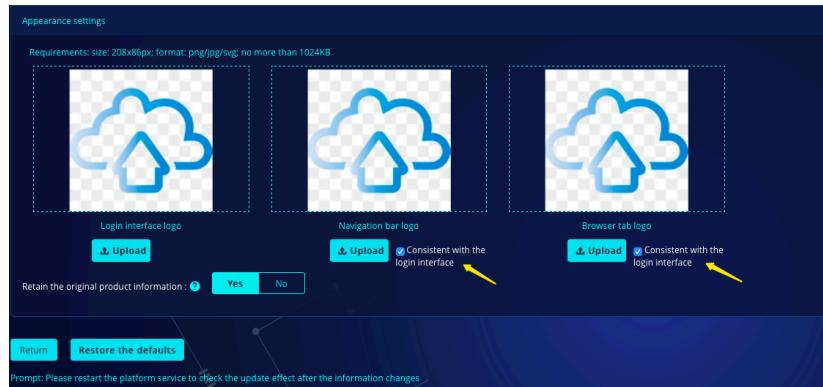


Note: the image is required to be no more than 1024KB and the suffix should be “.png/.jpg/.svg”. With the image requirements met, the preview area will display the effect picture of the uploaded image, as shown in the following figure:





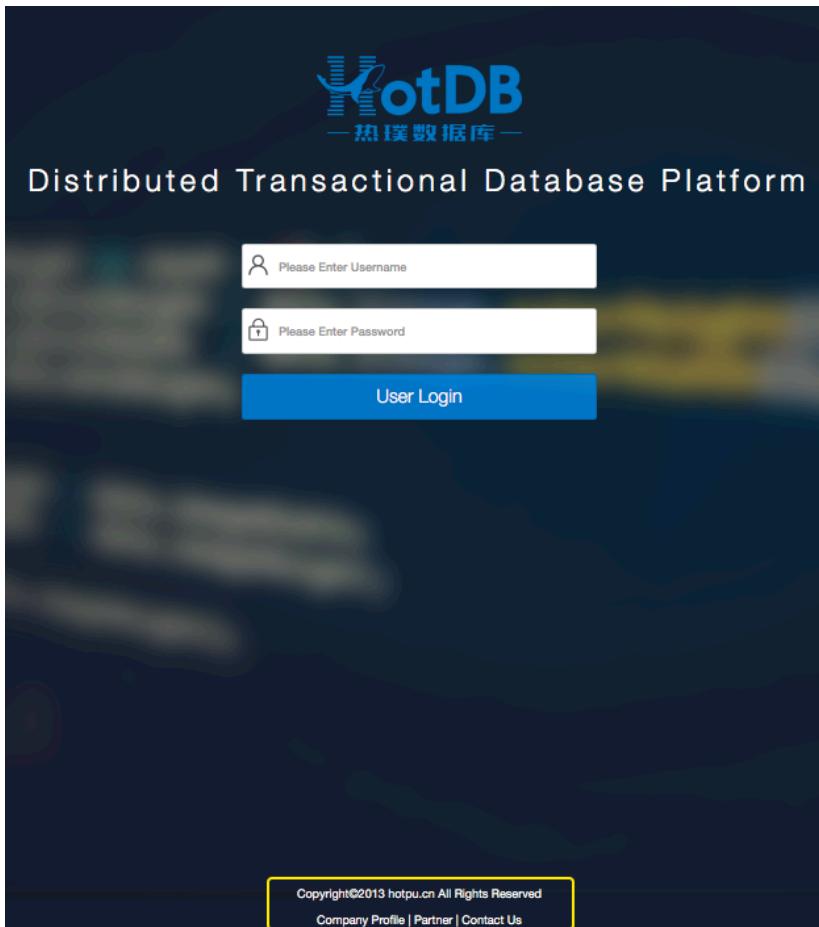
The check box “Consistent with the login page” for the navigation bar logo and the browser tab logo is not checked by default. When it is checked, the Upload button will be grayed and cannot be operated, and the corresponding logo preview will display the same as the login page logo.



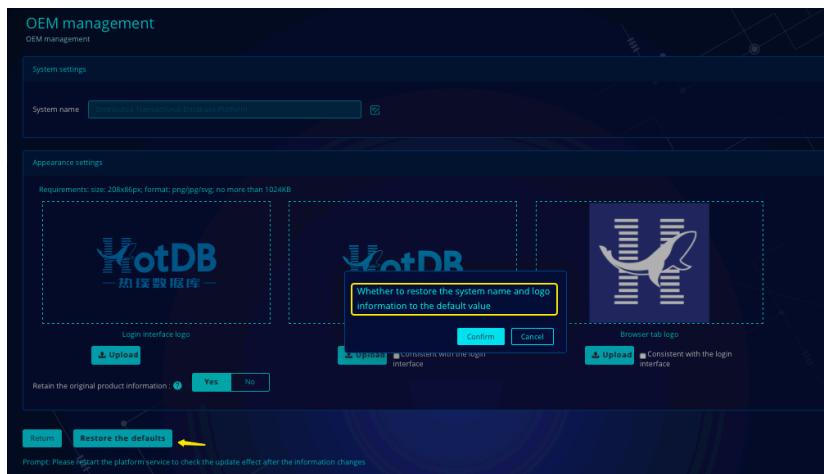
11.3. Retain the original product information

When it is Yes by default, the logo and copyright declaration of HotDB will be displayed at the bottom of the management platform login page and cluster selection page; when No is selected, the logo and copyright declaration of HotDB will be hidden at the bottom of the management platform page and cluster selection page. As

shown below:



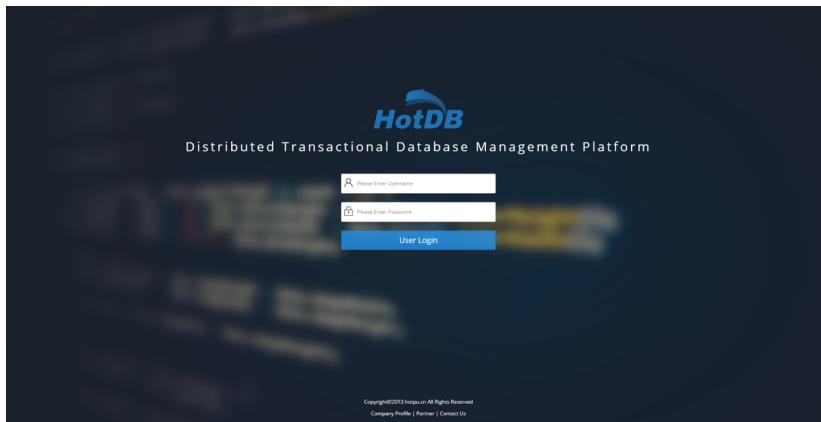
Click Restore the defaults. After the setting takes effect, image files under the logo directory of the management platform will be cleared. Meanwhile, the system name on pages will be reset to the “Distributed Transactional Database Platform”; the logo preview will restore the default logo of the management platform, and the switch Retain the original product information will be changed to yes.



12. General user login

12.1. Login

General users are created by the manager user in the “[User Management](#)” of the management interface, and the access mode is the same as that of the manager user.

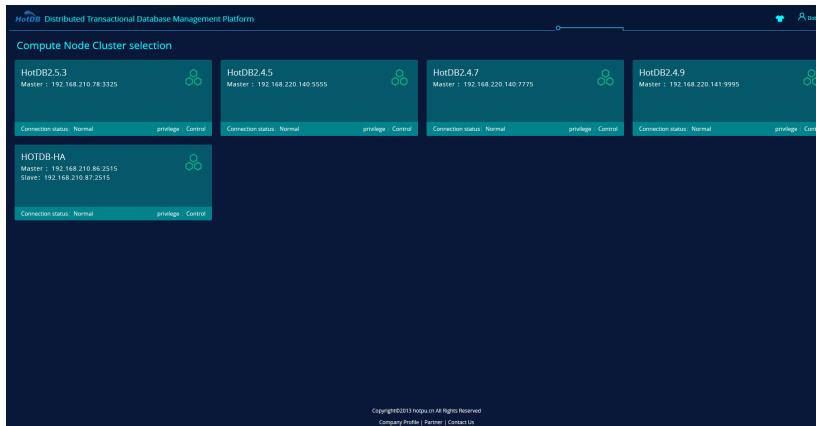


For general users logging in for the first time, HotDB Management forces the password change and the initial password is “hotdb@hotpu.cn” by default.

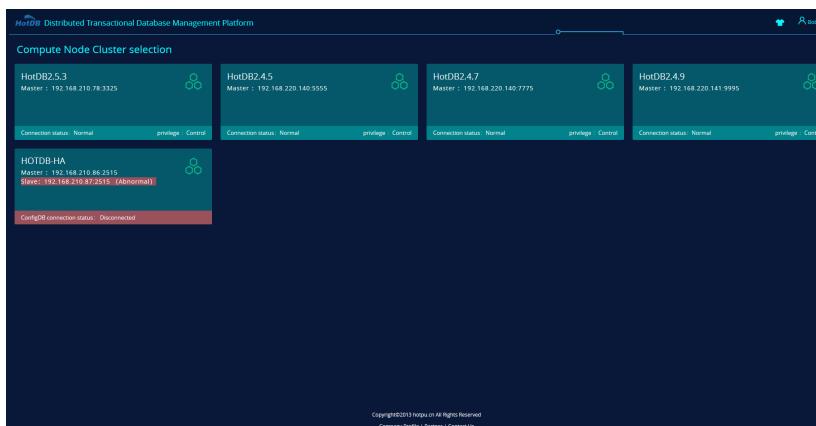
12.2. Cluster selection

General users enter the Cluster Selection page after logging into HotDB Management successfully. If the DR mode is enabled, please refer to the chapter "Compute node cluster selection" in the [Distributed Transactional Database HotDB Server - Cross-IDC Disaster Recovery Function Specification](#) for the display and explanation of the cluster selection page.

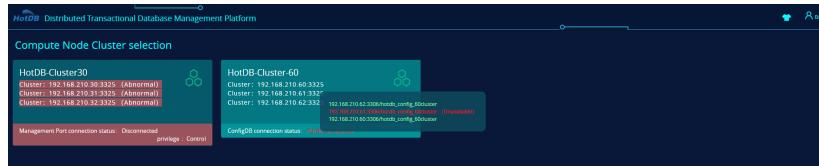
- The compute node cluster displayed is the compute node cluster with access or control privilege owned by the login user. Click on a specific cluster to enter the cluster for viewing and management operations. When the cluster compute node and configDB are running normally, the page icon is green (as shown below) and the cluster can be accessed normally.



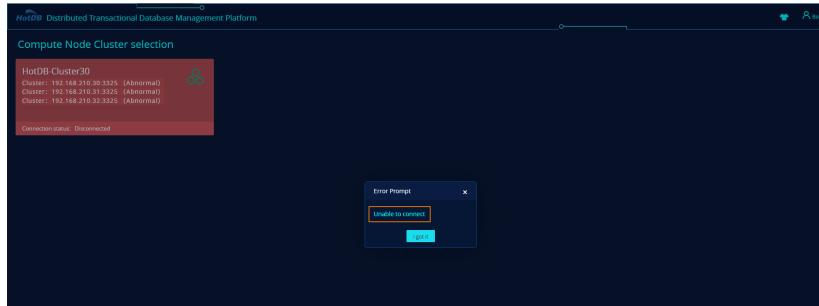
- When the cluster slave compute node cannot be connected but the configDB is connected properly, the cluster slave compute node is red and abnormal.



- When the configDB cannot be connected and the compute node is running normally, the bottom configDB connection will display an exception. When the configDB cannot be connected partially, move the mouse cursor to the “Partial Exception” to display the specific configDB connection exception information.



- When all compute nodes in the cluster and the configDB cannot be connected, the cluster panel is displayed in red. When clicking on the cluster panel with the mouse, “Unable to connect” will be displayed and it is unable to enter the cluster.

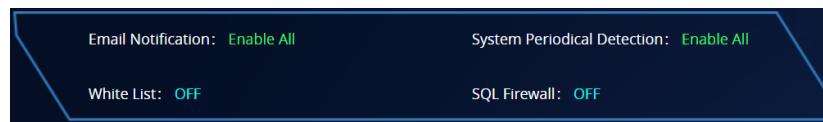


13. Home

HotDB Management displays real-time user-concerned information such as data volume, access flow, cluster component status, warning event, and security prevention and control of compute node cluster in the home page function through data visualization.



13.1. Cluster security



- Email Notification: Judge according to whether the monitoring switch in the notification setting is turned on, which can be divided into: Enable All, Not Enable and Partially Enable. Click to jump to the notification setting page.
- System Periodical Detection: Judge according to whether all switches on the periodical detection setting page are turned on, which can be divided into: Enable All, Not Enable and Partially Enable. Click to jump to the periodical detection setting page.
- White List: Judge according to the actual switch state of the white list function,

which can be divided into: ON and OFF. Click to jump to the white list page.

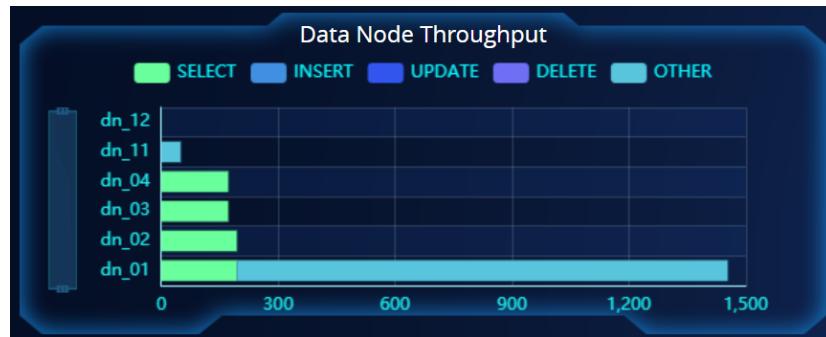
- SQL Firewall: Judge according to whether the SQL interception status of SQL firewall is enabled or not, which can be divided into: All ON, Partial ON and OFF. Click to jump to the SQL firewall page.

13.2. Summary of important information

Table Configuration: 23 Table	SQL Log: 0 Optimize	Totals of Backup: 0 Backup	Cluster Log: 999+ Log
Definition Warning: 6	Slow SQL: 0	Failure Backup : 0	Unread: 999+

- **Table:** The first row “Table Configuration” is the number of all tables on the “[Table Configuration](#)” page, and the second row “Definition Warning” is the number of tables detected to be abnormal in the “[Table Structure & Index Detection](#)”.
- **Optimization:** The first row “SQL Log” is the number of SQL records recorded in the “[Slow Query Log Analysis](#)” function of HotLog Management. The second row “Slow SQL” is the SQL marked with ⓘ in the “[Slow Query Log Analysis](#)” function of HotLog Management. (“SQL Log” and “Slow SQL” are displayed are not enabled when the Slow Query Log Analysis does not enable SQL statistics)
- **Backup:** The first row “Totals of Backup” is the number of all backup records in the “[Backup Task](#)” function of HotDB Management, and the second row “Failure Backup” is the number of task records with backup status as “Backup Failed”.
- **Log:** The first row “Cluster Log” is the total number of logs in the “[Compute Node Log](#)” function of HotDB Management. The second row “Unread” is the number of logs with status as “Unread” in the compute node log. When the number of logs is greater than 999, the page displays 999+.

13.3. Data node throughput



Note: Display the real-time throughput of all data nodes in the cluster. Throughput types include: SELECT/INSERT/UPDATE/DELETE/OTHER. Click on the title to jump to the “[Data Node Throughput](#)” report function page.

13.4. Event notice

Event Notice		More >
Notice	Time	
1139066Unread HOTDB log(s)	47 minutes ago	
2 Sharding plan online change completed	September19	
20 Master/Slave consistency detection completed	September12	

Note: The events are the history events with event warning mark in the upper right corner of HotDB Management. Click [More] to link to “[Historical Event](#)” for more notice details.

13.5. Cluster throughput

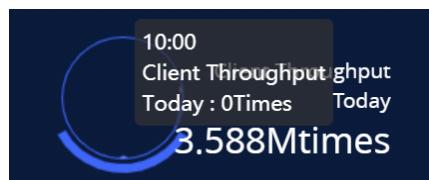


Note: Display the number of transactions per second (TPS: Transactions Per Second) and the query per second (QPS: Query Per Second) in the cluster.

- The “Cluster Throughput” displayed by clusters in multi-node mode is the sum of all compute nodes.
- Extra-transaction TPS does not count SELECT operations, and intra-transaction SELECT/UPDATE/DELETE/INSERT will be counted.
- QPS does not count transaction statements such as “begin, commit”.
- Click on the title to link to the “Compute Node Flow” function page.
- Page data refreshing rate is 3 seconds

13.6. Overview of data amount and throughput

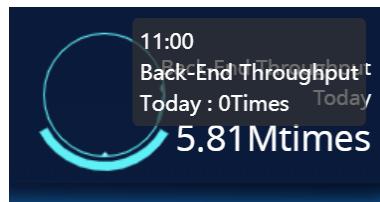
13.6.1. Client throughput today



Note: The client throughput is the operations (SELECT, INSERT, UPDATE, DELETE, OTHER) sent by front-end application to compute node

- Display the client throughput data of all compute nodes in the cluster today, which is counted according to the natural day.
- The page refreshing rate is 1 minute.
- The client throughput today is cleared at 0 a.m. every day, and displayed as 0 if no operations are performed on that day.
- Click on the graph to link to the “[Compute Node Throughput](#)” report details page.

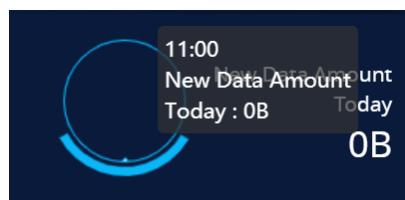
13.6.2. Back-end throughput today



Note: The back-end throughput is the operations (SELECT, INSERT, UPDATE, DELETE, OTHER) sent by compute node to the underlying data node.

- Display the back-end throughput data of all compute nodes in the cluster today, which is counted according to the natural day.
- The page refreshing rate is 1 minute.
- The client throughput today is cleared at 0 a.m. every day, and displayed as 0 if no operations are performed on that day.
- Click on the graph to link to the “[Compute Node Throughput](#)” report details page.

13.6.3. New data amount today



Note: The new data amount today is a description of the change of business data volume in the cluster from 0 a.m. today to the current time. If it is negative, it means that the data amount is less than that at 0 a.m.

- Page data is updated once every hour.
- The data is cleared at 0 a.m. every day.
- Calculation formula: The sum of data amount of all tables in the data source of the cluster minus the data amount recorded before 0 a.m. today.
- Click on the graph to link to the “[Cluster Data Amount](#)” report details page.

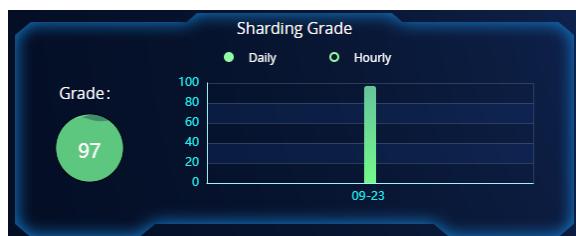
13.6.4. Total data amount



Note: Display the current total data amount of all data nodes in the cluster, that is, the sum of data amounts of all tables in the normal data source.

- Page data is updated once every hour.
- Only the data amount of master data source in the current data node is obtained.
- Click on the graph to link to the “[Cluster Data Amount](#)” report details page.

13.7. Sharding grade



Note: It uses grading to reflect the sharing advantages and disadvantages of the sharding table in the cluster. When the compute node starts for less than 24 hours, the grade cannot be calculated and the page is not displayed. Click on the title to jump to the “[Sharding Grade](#)” details screen. The grade trend graph displays the changes of the recent sharding rationality grade, which can be viewed by day and by hour.

13.8. TOP 10 table today

Top 10 table (2019-09-23)			
Throughput (Ktimes)	Ranking		Data Amount (KB)
34.272	test_yds.sbtest19	▼	bk_db.testz
33.952	test_yds.sbtest14	▼	bk_db.test_spz
33.68	test_yds.sbtest4	▼	
33.609	test_yds.sbtest10	▼	
33.594	test_yds.sbtest15	▼	
33.402	test_yds.sbtest11	▼	
33.275	test_yds.sbtest2	▼	
33.234	test_yds.sbtest8	▼	
33.219	test_yds.sbtest17	▼	
33.122	test_yds.sbtest6	▼	

Note: Display the top 10 business tables with the largest change in daily data amount and the highest throughput in the cluster.

- TOP 10 data amount change is ranked by the absolute value of table data added or reduced.
- The data amount of the global table is the average of data amounts of the master data source under each data node.
- The data amount of the sharding table is the sum of data amounts of the master data source under all data nodes.
- Click on the “TOP 10 Table Throughput Today” area to link to the “Compute Node Throughput” report details page; and click on the “TOP 10 Data Amount Table Today” area to link to the “Cluster Data Amount” report details page.

13.9. Throughput rate



Note: Display the operation frequency of the real-time front-end (sent by front-end application to compute node) and back-end (sent by compute node to data node) SELECT, INSERT, UPDATE and DELETE in times/s.

- Page data refreshing frequency is 3 seconds.
- Calculation method: The operation frequency per second is obtained by dividing the operation increment in the fixed time by the interval time.
- Multi-node mode cluster operation increment is the sum of all compute nodes in the cluster.
- Click on the “Front-End Throughput Rate” area to link to the “Compute Node Throughput” report details page; and click on the “Back-End Throughput Rate” area to link to the “Data Node Throughput” report details page.

13.10. Cluster overview

Overview of master/slave node mode clusters:



Overview of multi-node mode clusters:



- Cluster Starting Time: Display the actual starting time of the current master compute node.
- Cluster Running Time: Display the current running time of the master compute node since starting.
- Compute Node Switch Times: The high availability switch times of compute nodes of master/slave mode clusters or the master switch times of compute nodes of multi-node mode clusters calculated based on the natural year.
- Cluster Availability: It is obtained by dividing the “Failure Recovery Time” by a natural year.

- Failure Recovery Time: The time consumed by high availability switch or master switch of the cluster, that is, the period from failure to availability recovery. The cumulative statistics are made according to the natural year.
- Front-End Application: Display the total number of front-end applications, the front-end applications with the highest connections, and the front-end applications with the highest QPS. The data is obtained from the "[Logic Topological Graph](#)".
- LogicDB: Display the total number of logicDB, the number of logicDB with normal or warning status, and the logicDB with the maximum data amount and the highest throughout. The data is obtained from the "[Logic Topological Graph](#)".
- Data Node: Display the total number of data nodes, the number of data nodes with normal or warning status, and the data node with the maximum data amount and the highest throughout. The data is obtained from the "[Logic Topological Graph](#)".
- Data Source: Display the total number of data sources, the number of data sources with normal or warning or failure status, and the data source with replication latency. The data is obtained from the "[Logic Topological Graph](#)".

14. Configuration

Configuration is the function developed by the management platform for visual configuration of HotDB Server, including configuring parameters such as data nodes, data sources, data source groups, logicDB, sharding function, table configuration, database users and compute nodes for HotDB Server. At the same time, the auxiliary functions of configuration parameter verification and backup recovery are set.

14.1. Node management

The node management menu mainly provides users with the management of data source groups, data nodes and data sources, including basic addition, deletion and modification. It can also set up the replication relation or high-availability switching rules of the underlying data sources for the configured data nodes.

If the DR mode is enabled, please refer to the chapter "Node management" in the [Distributed Transactional Database HotDB Server - Cross-IDC Disaster Recovery Function Specification](#) for the node management function display and operation explanations

Function Entry: Click “Configuration” - > “Node Management” on the management platform page

Data Source								Master/Slave Status	Master/Slave Switch
DNID	Data Node Name	Hostname	Port	Data Source	Type	Status	Operation		
6	dn_2	192.168.210.42	3307	phy4118	Active Master	Available			
5	not delete_1	192.168.210.05	3306	dionoideate	Active Master	Available			
4	dn_4	192.168.210.42	3308	db4970	Active Master	Unavailable			
3	dn_2	192.168.210.41	3309	db4970	Standby Slave	Available			
3	dn_2	192.168.210.43	3309	db4970	Active Master	Available			
2	dn_2	192.168.210.44	3309	db4970	Standby Master	Available			
1	dn_3	192.168.210.41	3307	db4970	Active Master	Available			

From 1 to 6 Records from 1 / 1 page

Available Slave Unavailable

Prev | **1** Next | Jump to: of

List information description:

DNID: Data node ID

Data Node Name: Click on the button in the Data Node Name to link to the “Data Node Management” page

Data Source_Hostname: Address of the server where the data source is located

Data Source_Port: Data source MySQL instance port

Data Source_Database: Database in the data source MySQL instance

Data Source_Type: The roles of data source in data node include Active Master, Standby Slave, Standby Master and MGR.

Data Source_Status: The data source statuses include availability and unavailability. The unavailability status is displayed in red font. The data source which is an Active Master and available is displayed in green font. The data source which is a Standby Slave or Standby Master and available is displayed in blue font. The data source available and whose listener fails to connect is displayed in orange font.

Operation: Including “Details”, “Enable/Disable” and “Delete” from left to right

Master/Slave Status: The replication status between data sources in data node. Only data sources with master-master or master/slave replication relation will display the master/slave statuses as follows: Building Failed, Building, Abnormal, Unknown and

Normal. For a detailed description of the status, please refer to the “[Master/Slave Setup](#)” chapter.

Master/Slave Switch: The entry for manually performing the high availability switch operation of data source, which only appears in data sources with master-master or master/slave replication relation as with the master/slave status. The master/slave switch depends on the switching rule configured for the data node. For the specific switching rule configuration, please refer to the “[Switching Rule](#)” chapter.

14.1.1. Add data source group

Add Data Source Group allows to easily add or modify a set of data sources with the same parameter values.

Function Entry: Click on “Configuration” -> “Node Management” -> “Data Source Group” -> “Add Group” on the management platform page to enter the “Add Data Source Group” function page.

Function Description: Check the parameter items that need to be used by the data source and have the same parameter values, and then set the parameter values of the checked parameter items. Click the “Save and Return” button to complete the addition of data source group.

Parameter Description:

- Group Name: Enter the data source group name
- Connection User: Username with the database access privilege
- Connection User Password: User password with the database access privilege
- Database Name: Database name can be referenced in the data source, such as “db01”
- Backup User: (optional) Username used to back up the database;
- Backup User Password: (optional) User password used to back up the database;

- Character Set: The character set of database connected, which is utf8mb4 by default;
- Max Connections: Maximum connections of the MySQL database, which is 4200 by default;
- Initial Connections: Initial connections of the MySQL database, which is 32 by default;
- Max Idle Connections: Maximum idle connections of the MySQL database, which is 512 by default;
- Min Idle Connections: Minimum idle connections of the MySQL database, which is 32 by default;
- Idle Examination Period (second): Idle examination period of the MySQL database, which is 600 by default.

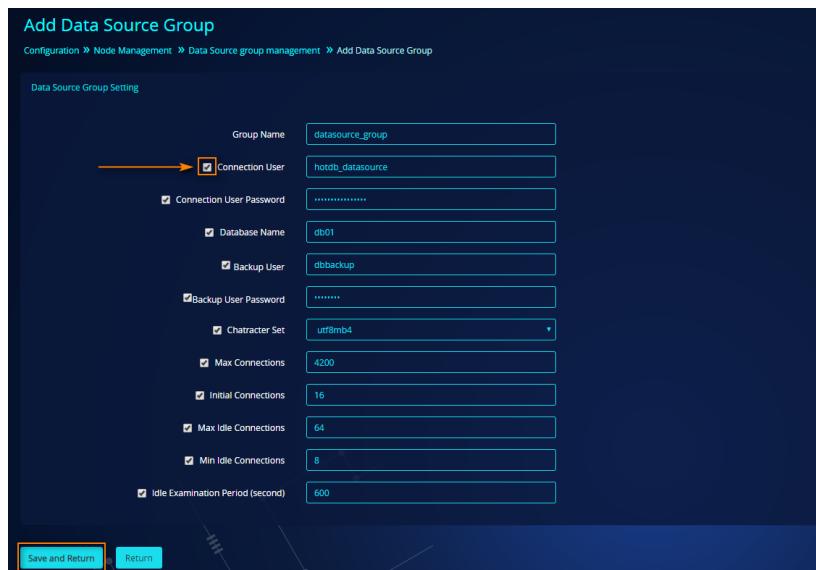
Add Data Source Group

Configuration > Node Management > Data Source group management > Add Data Source Group

Data Source Group Setting

Group Name	datasource_group
Connection User	hotdb_datasource
Connection User Password
Database Name	db01
Backup User	dbbackup
Backup User Password
Character Set	utf8mb4
Max Connections	4200
Initial Connections	16
Max Idle Connections	64
Min Idle Connections	8
Idle Examination Period (second)	600

Save and Return **Return**



14.1.2. Add node

Add Node function allows to quickly configure data nodes, data sources and listeners for HotDB Server in the early stage and to configure data sources separately.

Function Entry: Click on “Configuration” -> “Node Management” -> “Add Node” on the management platform page to enter the “Add Node” function page.

Example Description: The Add Node function is displayed taking adding 4 data nodes (dn_01, dn_02, dn_03, dn_04) and 8 data sources (master-master: ds_01, ds_02, single database: ds_03, master/slave: ds_04, ds_05, MGR: ds_06, ds_07, ds_08) for example as follows.

The screenshot shows the "Node Management" section of the HotDB Management Platform. On the left, there's a sidebar with various configuration options like Node Management, LogDB, Data Configuration, and so on. The main area has tabs for "Data Source Management" and "Data Node Management". Under "Data Node Management", there's a table with columns: DND, Data Node Name, Hostname, Port, Database, Type, Status, Operation, Master/Slave Status, and Master/Slave Switch. There are four data nodes listed: dn_01, dn_02, dn_03, and dn_04. Each node has two entries under "Data Node Name". The "Operation" column contains icons for edit, delete, and add. The "Master/Slave Status" column shows "Normal" and the "Master/Slave Switch" column shows "Switch". At the bottom, there are buttons for "First", "Last", "Next", "Previous", and "Jump to". A legend at the bottom defines the colors: green for Active, blue for Standby, and red for Inavailable.

Generation of example data:

Step 1: Set the parameter value of data node number as 4, and other generated parameters adopt the page default values.

Step 2: Click the “Generate” button to generate the data into the list

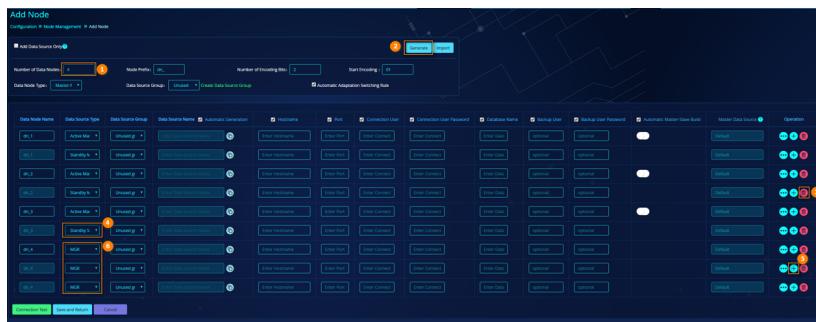
Step 3: Click the button in the “Operation” column to delete the excessive records generated in the dn_02 data node.

Step 4: Modify “Date Source Type” under dn_03 data node to “Standby Slave”

Step 5: Click the button in the “Operation” column of dn_04 data node record to

add a record under dn_04.

Step 6: Modify “Date Source Type” under three records of dn_04 to MGR



Configure data source data:

Step 1: Use the previously added data source group and link it to each data source record

Step 2: Remove the checked “Automatic Generation” and customize the data sources in turn, which shall not be the same. It is generally recommended to check “Automatic Generation”

Step 3: Fill in the hostname, port, connection user, connection password, database name, backup user and backup user password of data source (connection user and password are used for connecting the compute node with the data source which must be filled in; backup user and password are specially used for data source data backup which are recommended to be filled in though as optional items)

Step 4: Enable “Automatic Master/Slave Setup”. After adding the data source, the program automatically performs setup operation for data node process that needs to build the master/slave or master-master replication relation. If it is not enabled, the “Master/Slave Setup” function can be used for operation later.

Step 5: “Master Data Source” adopts the default value “Default”. In case of the master-master with slave(s) or master-master with multi-slave relation of data node, the master

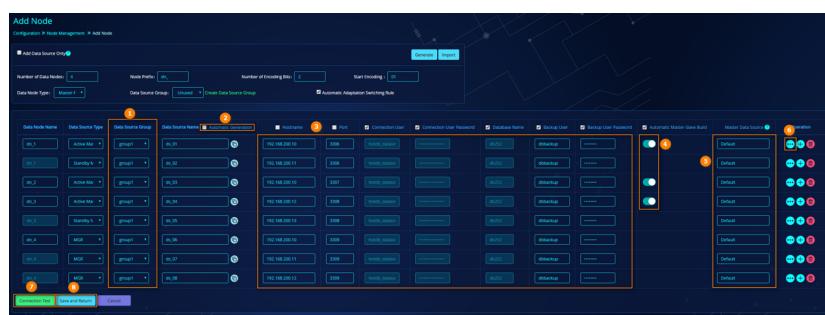
data source to which the data source belongs can be specified here. The program automatically determines the master/slave relation by default.

Step 6: The parameters expanded by the “...” button in the “Operation” column are not modified by default. The parameters in the data source group or the system default values can be directly used. If there are special requirements, click to edit the internal parameters. (if the “Synchronize to other data sources which do not use groups” in more parameters is checked, more parameters of the data source modified can be applied to records of other data source which do not use groups)

Step 7: Click the “Connection Test” button to verify the availability of connection of the configured data source information. If the configured information is unavailable, the “Hostname”, “Port”, “Connection User”, “Connection User Password” and “Database Name” input boxes of the corresponding data source will be identified. If it is detected that the data source is connectable but the database does not exist, it prompts whether to create database for the user, but the configured connection user shall have create privilege.

Backup user test: The availability testing of backup users depends on the backup program (HotDB) on the server where the data source is located. If the server where the data source is located is not installed with the backup program or the backup program is not started, the availability of backup user cannot be detected and the “Connection Test” cannot be passed.

Step 8: Click the “Save and Return” button to save the configured node data



14.1.3. Master/slave setup

Master/Slave Setup function can set up a replication relation for a data source that has been configured but has not yet built a replication relation.

Function Entry: Click “Configuration” -> “Node Management” -> “High Availability Setting” -> “Master/Slave Setup” on the management platform page to enter the “Master/Slave Setup” function page.



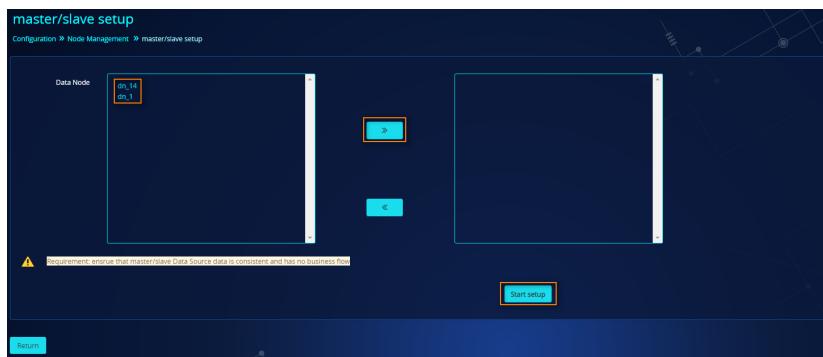
DNID	Data Node Name	Hostname	Port	Data Source	Type	Status	Operation	Master/Slave	
								Setting Rule	Inter Slave Switch
6	dn_6	192.168.210.42	3307	phy1418	Active Master	Available			
5	master_1	192.168.210.66	3306	donotdelete	Active Master	Available			
4	dn_4	192.168.210.42	3308	db4970	Active Master	Unavailable			
		192.168.210.41	3308	db4970	Standby Slave	Available			
3	dn_3	192.168.210.43	3309	db4970	Active Master	Available			
		192.168.210.44	3309	db4970	Standby Master	Available			
2	dn_2	192.168.210.42	3307	db4970	Active Master	Available			
1	dn_1	192.168.210.41	3307	db4970	Active Master	Available			

After entering the Master/Slave Setup page, it will automatically display the data nodes that need to be set up. If it is NULL,it means there is no data node to be set up.

Setup instructions:

1. The data source selected must be running normally and the page “Status” field is displayed as available
2. The data source selected shall not be configured or have multiple target replication relations
3. The my.cnf configuration parameters of the data source selected shall be correct (for those based on binlog and GTID replication, the corresponding parameters shall be opened respectively)

4. If the connection user of the data source selected has no create user and super privileges, the program will try to set up with the account “repl” and password “repl”. If the repl account does not exist in the data source or the password is incorrect, the user needs to manually specify the replication account of master/slave setup.
5. The replication account must have two basic privileges: “replication slave, replication client”.
6. The data source selected shall ensure that the master/slave data is consistent (except for mysql, information_schema, performance_schema, sys database)
7. If the data source selected adopts the GTID mode for replication setup, GTID shall have no breakpoints
8. The data source selected shall have no traffic flow currently



Master/slave setup process:

Step 1: Select the data node that needs to set up the replication relation and click “Start setup”

Step 2: Detect whether there are multiple target replication relations for the set data source (if any exist, the setup fails)

Step 3: Check whether the data source parameters are configured correctly and

determine whether the replication mode is binlog or GTID (if the parameter checking fails, the setup fails).

Step 4: Set up a replication account or try to use “repl” as a replication account (if the setup fails or the use of “repl” account fails, the pop-up window requires to manually specify the available replication account, and if the manually specified account is still invalid, the setup fails).

Step 5: Detect the data consistency of master/slave data source. If the GTID replication mode is adopted, it needs to determine whether there are GTID breakpoints (if the GTID breakpoints exist, the setup fails)

Step 6: Detect whether there is traffic flow on the data source (if the traffic flow exists, the setup fails)

Step 7: replication relation setup

Step 8: Detect if there is a delay (if there is a delay, the specific delay information will be prompted, but the setup result will not be affected)

Other description:

1. For the master/slave setup of master-master with slave(s) data node, the master of the standby slave is the active master by default. If it needs to set up standby master, it needs to edit the “Master Data Source Name” to be standby master in the “Data Source Management” before setup, as shown below:

Data Source Management

Configuration > Node Management > Data Source Management

Node Selection: dn_1

Select Data Source: 192.168.210.41_3307_db253

Data Source Information

Data Source Group	No Group
Hostname	192.168.210.41
Port	3307
Connection User	hotdb_datasource
Backup User	
Database Name	db253
Data Source Type	MGR
Data Source Status	Available
Character Set	utf8mb4
Max Connections	4200
Initial Connections	32
Max Idle Connections	512
>Min Idle Connections	32
Idle Examination Period (second)	600
Master Data Source Name	None

Edit

Return

2. If the user enters other menu pages or exits the login in the setup process, the master/slave setup task will still run in the background. The setup can be viewed in the “Master/Slave Status” on the “Node Management” function page. The detailed master/slave status is as follows:

- **Blank:** When the current data node has only one data source or is of MGR type, no status is displayed
- **Normal:** The master/slave replication status is normal viewed through display slave status (Slave_IO_Running: YES, Slave_SQL_Running: YES) and is consistent with the master/slave relation configured for the data source under the current node.
- **Abnormal:** The master/slave replication status is abnormal (Slave_IO_Running: NO, Slave_SQL_Running: NO)

- **Unknown:** Data source cannot be connected, data source privileges are insufficient, detection is periodical out (timeout time: 1 minute), and current node has no master/slave replication relation (no master/slave relation setup or wrong master/slave relation setup)
- **Setup Failed:** There is a detection failure or setup failure during the master/slave setup process. Move the mouse cursor into the "Setup Failure" to prompt the specific failure information.
- **Setup:** The master/slave setup task is currently under way. If the setup is completed in the background, refresh the page to display normal or failed setup.

14.1.4. Switching rule

Configuring switching rule provides users with a guarantee of high availability of data source. The compute node periodically checks the availability of data source. Once a data source failure is detected, the compute node automatically switches to the standby data source according to the configured switching rule to ensure the service stability and reliability. Users can also switch manually.

Function Entry: Click “Configuration” -> “Node Management” -> “High Availability Setting” -> “Switching Rule” on the management platform page to enter the “Data Node Switch Configuration” function page.



Function description: Generally, when “Auto Adaptation of Switching Rule” is selected in “Add Node”, the data source switching rule will be automatically configured by default. If the switching rule is not configured, click the “Add switching rule” button on the “switching rule” page to customize the rule or click the “Auto Adaptation” button to automatically adapt the switching rule.

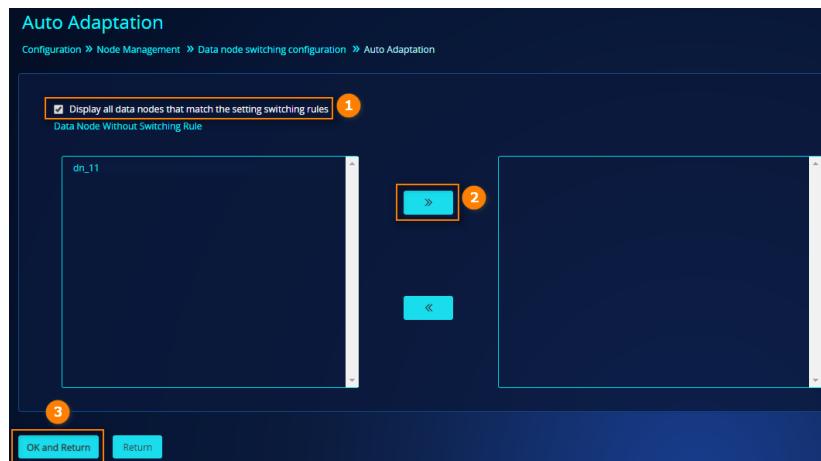
Add switching rule

1. Click the “Add switching rule” button, the page will automatically add a switching rule record
2. Select the data node that needs to configure the switching rule.
3. Select the source data source
4. Select the standby node to be switched when the source data source fails, that is, standby data source.
5. Set the switching priority. The smaller the moving number displayed, the higher the switching priority.
6. Click on the “√”button to save the switching rule record. Click on the “×” button to cancel the record.



Auto Adaptation operation instructions

1. Check “Display data nodes without switching rule only”, otherwise the switching rule configured may be overrode.
2. Click the “>>”full right-shift button or double-click the data nodes displayed on the left to choose options needing to be automatically adapted.
3. Click the “OK and Return” button. The program will automatically adapt the switching rule for the selected data node.



Auto Adaptation rule description

- When the data node type is “Single Database”, clicking “Auto Adaptation” will not generate a switching rule.
- When the node type is “Master/Slave”, click “Auto Adaptation” to generate the switching rule from active master to standby slave (in case of one master and multiple slaves, the switching rule from active master to any standby slave will be automatically adapted, and manual operation is required for other standby slaves)
- When the node type is “Master-Master”, click “Auto Adaptation” to generate the switching rule from active master to standby master and the rule for switching from standby master to active master (in case of master-master with slave(s), the switching rule for standby slave will not be automatically adapted and manual operation is required)
- When the node type is “Others”, the node is judged to be abnormal (for example, there are two active masters), and no operation will be performed after clicking “Auto Adaptation”
- MGR does not need to be configured with high-availability switching rules. The program automatically switches according to the MySQL master node election rules.

14.1.5. Heartbeat paused

Heartbeat: Heartbeat is a strategy of HotDB Server to maintain high availability of data nodes. The compute node periodically sends heartbeat detection to the underlying

data node at a certain frequency. If the data source normally feeds back the detection of compute node, the current state of data source is normal. If the data source does not send detection feedback to the compute node within the specified time and at the specified frequency, the data source status is considered by the compute node to be abnormal, and the data node high availability switch operation will be performed.

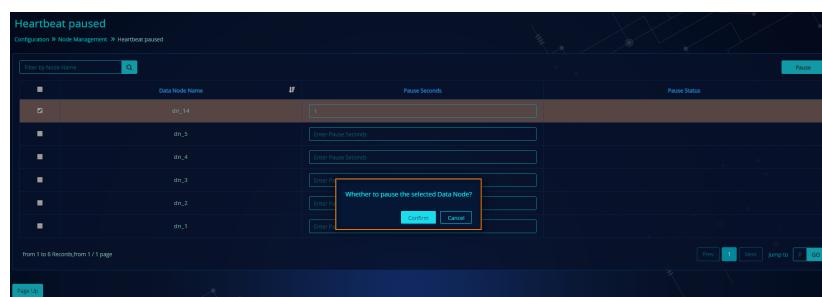
Heartbeat paused: When a data node needs special maintenance, it needs to pause the heartbeat detection from the compute node. The heartbeat paused function can be used to pause the data source heartbeat by the compute node in the set time period.

Function Entry: Click “Configuration” -> “Node Management” -> “High Availability Setting” -> “Heartbeat paused” on the management platform page to enter the “Heartbeat paused” function page.



Function operation instructions:

1. Check the data node to be paused and enter the number of seconds to be paused.
2. Click the “Pause” button and the pop-up box prompts “whether to pause the selected Data Node?” After clicking the “Confirm” button, the program will perform the heartbeat paused operation and the “Pause Status” recorded on the page is “Pause Succeeded”. After clicking the “Cancel” button, the program will not perform the heartbeat paused operation and return to the previous level.
3. After the pause period, the data node will automatically respond to the heartbeat detection.



Hotbeat paused

Data Node Name

Pause Seconds

Pause Status

Whether to pause the selected Data Node?

Confirm Cancel

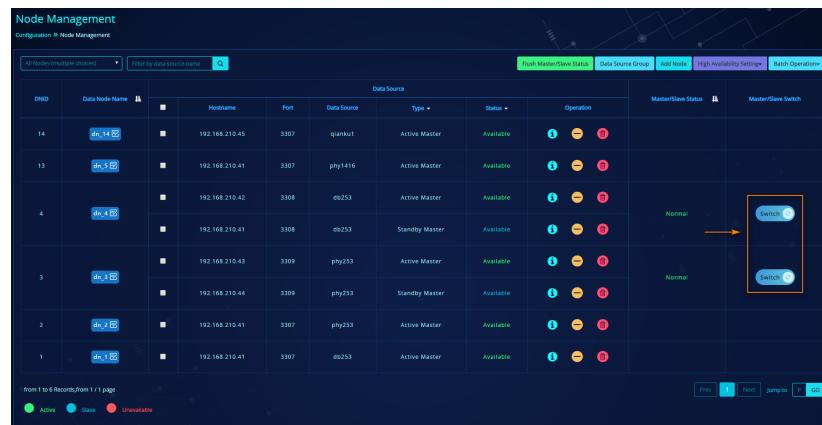
14.1.6. Master/Slave switch

For data nodes with multiple data sources and configured with switching rules, the master/slave switching of data node can be performed manually.

Function Entry: Click “Configuration” -> “Node Management” -> “Switch” -> on the management platform page.

Instructions for use:

- The data node high availability switch rule has been configured and reloaded to the compute node.
- The master/slave and master-master replication relations under the node have been set up, and the replication latency time shall not exceed 10s.
- MGR node does not support manual switching, and the active master is selected by MySQL



Node Management

All Nodes (multiple choice) Filter by data source name

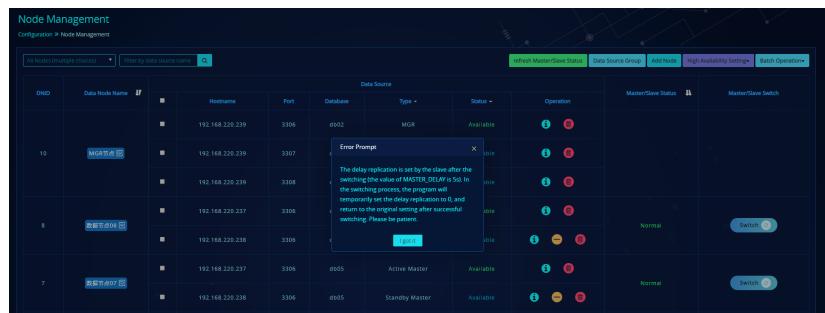
DNID	Data Node Name	Hostname	Port	Data Source	Type	Status	Operator	Master/Slave Status		Master/Slave Switch	
								Rout Master/Slave Status	Data Source Group	Add Node	High Availability Settings
14	dn_14	192.168.210.45	3307	qiankun	Active Master	Available					
13	dn_5	192.168.210.41	3307	phy1416	Active Master	Available					
4	dn_4	192.168.210.42	3308	db253	Active Master	Available					
3	dn_3	192.168.210.41	3308	phy253	Standby Master	Available					
2	dn_2	192.168.210.48	3309	phy253	Standby Master	Available					
1	dn_1	192.168.210.41	3307	db253	Active Master	Available					

from 1 to 6 Records, from 1 / 1 page

Active Slave Unavailable

Function description:

1. If the data node is the master/slave architecture, the highest priority is selected when switching manually. After switching, the master data source and other slaves will set by HotDB Server to be unavailable and cannot be switched again.
2. In case of master-master, the active master will not be unavailable after switch and can be further switched manually.
3. If the delay setting of master_delay is detected during switching, the value of master_delay will be automatically cancelled. After the switching, the delay setting will be restored. If the replication latency is still greater than 10s after cancelling master_delay, switching will not be allowed, and the previously set value of master_delay will be restored.



4. If the highest priority standby slave is unavailable or delayed for more than 10s, the program will select the remaining standby slaves with higher priority to switch manually. If none is available or delayed for more than 10s, no switch will be performed and an error will be prompted (the switch failure log prompts: switch datasource datasource id failed due to: no available backup found).
5. After the switch is completed, other data sources need to be manually made available, and the active master will be reused after reloading. However, it is recommended to perform the “Master/Slave Consistency Detection” to ensure data consistency before manually setting them available.

6. During the switch process, the program will wait for standby slave catching up with copy.

7. Add "switching" button. You can cancel the switch operation midway by clicking the button.

Node Management									
Configuration > Node Management									
Data Source									
DNode	Data Node Name	Hostname	Port	Database	Type	Status	Operation	Master/Slave Status	Master/Slave Switch
10	MGR1@10	192.168.220.239	3306	db02	MGR	Available			
	MGR2@10	192.168.220.239	3307	db02	MGR	Available			
8	dn_1@8	192.168.220.239	3308	db02	MGR	Available			
	dn_2@8	192.168.220.237	3306	db05	Active Master	Available			
7	dn_3@7	192.168.220.238	3306	db05	Standby Master	Available			
	dn_4@7	192.168.220.237	3306	db05	Active Master	Available			

8. After the switch is successful, HotDB Server will record the switch process log.

14.1.7. Data node management

Each data node has its own details page, where the user can manage the basic information of the data node, data source, and data node switching rules.

Function Entry: Click “Configuration” -> “Node Management” -> “” -> on the management platform page.

Function description:

1. Click “Select Node” to switch to view the details of different data nodes.
2. Click “Delete” to delete the selected data node, but if the data node is associated with a data source, it needs to clear the data source first.
3. Click the “Edit” button to change the data node name.
4. Click the “Refresh” button to refresh the status of master/slave data sources under the data node.

5. The logicDB name associated with the data node is displayed in the logicDB box.
6. The table name created under the data node is displayed in the table configuration.
7. The data source configuration is a data source configured under the data node.
8. The data node switch includes the switching rule that has been configured under the data node, and the switching rule can be added or automatically adapted for a newly configured data source. The “Auto Adaptation of Node Switching” can be checked to perform the auto adaptation of switching rules for newly added data sources under the data node in the future.

The screenshot shows the Data Node Management interface with several sections:

- Node Selection:** Shows "dn_4" selected in a dropdown menu.
- Basic Information:** Displays "Data NodeID: 4", "Data Node Name: dn_4", "Node Type: Master-Master", and "LogicDB: db_253".
- Table Configuration:** Shows tables "sm_q1_b1", "sm_q2_b1", "sm_q3_b1", "sm_b1_b1", "sm_c1_b1", and "sm_d1_b1".
- Data Source Information:** A table listing data sources:

Name	Hostname	Port	Username	Data Source	Type	Status	Operation
192.168.210.42_3308_db253	192.168.210.42	3308	hotdb_datasource	db253	Active Master	Available	
192.168.210.41_3308_db253	192.168.210.41	3308	hotdb_datasource	db253	Standby Master	Available	
- Data Node Switching:** Includes a checkbox for "Automatic Adaptation Node Switching" and two buttons: "Add Rule" and "View High Availability Setting". It lists data nodes with their hostnames, HA priority, and operation status.

14.1.8. Enable/Disable data source

Disable data source

Special maintenance for a data source can be operated by disabling the data source when required.

Function Entry: Click “Configuration” -> “Node Management” -> “” -> on the management platform page.

Function operation: On the data source management page, click the “Disable” button to confirm, then the data source is disabled successfully, and the “Status” field on the node management page displays the corresponding data source unavailable. If the disabled master data source is reloaded, the data node switches to the standby data source.

Note: Data sources of the MGR type shall not be arbitrarily disabled, otherwise the data source switch will be abnormal.

The screenshot shows the "Node Management" page with a table of data sources. A modal dialog titled "Disable ID" is open over the row for data source ID 4. The dialog contains the text "Disable ID" and two buttons: "Cancel" and "OK". The "OK" button is highlighted in blue. The data source row for ID 4 is marked as "Standby Master" and "Available". To the right of the table, there is a "Master/Slave Status" section with a "Normal" status and a "Switch" button. The top navigation bar includes links for "Master/Slave Status", "Data Source Group", "Add Node", "High Availability Settings", and "Batch Operations".

Enable data source

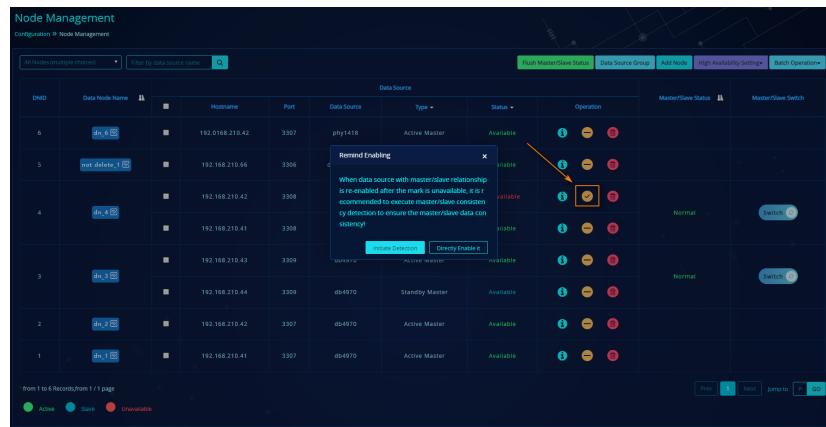
If the abnormal status of the data source is restored after the failure or manual marking of the data source as unavailable, the data source can be re-enabled on the management platform.

Function Entry: Click “Configuration” -> “Node Management” -> “” -> on the management platform page.

Function description:

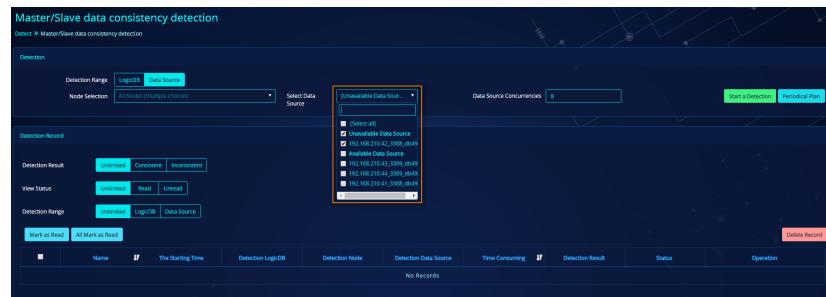
1. Single database and MGR data source can be directly enabled.

2. When a single or a batch of data sources with master/slave or master-master architecture is enabled, the enabled data source shall have at least one record of passing master/slave data consistency detection according to the data source dimension after it is marked as unavailable for the last time, or a prompt window is popped up to remind the user.



The screenshot shows the 'Node Management' section of the HotDB Management Platform. It lists seven data nodes (dn_1 to dn_7) with their hostnames, ports, and status. A modal dialog titled 'Remind enabling' is open over node dn_5, stating: 'When data source with master/slave relationship is re-enabled after the mark is unavailable, it is recommended to execute master/slave consistency detection to ensure the master/slave data consistency!'. It has two buttons: 'Cancel' and 'Directly Enable it'. The 'Directly Enable it' button is highlighted with a yellow arrow. The status of dn_5 is 'Available'.

3. Click “Start Detection” to jump to the master/slave consistency detection page. The enabled data source is selected by default. Manually click to Start a detection. If “Directly Enable it” is selected, it is necessary to manually ensure that the enabled data source is consistent with the data of other data sources under the data node.



The screenshot shows the 'Master/Slave data consistency detection' section. It includes a 'Detection Range' dropdown set to 'Logistic', a 'Select Data Source' dropdown showing 'Unavailable Data Source' (with several options like 'dn_1', 'dn_2', etc., listed), and a 'Data Source Concurrences' input field set to 8. Below these are sections for 'Detection Record' and 'View Status'. The 'Detection Record' table is currently empty, showing 'No Records'. The 'View Status' table also shows 'No Records'.

14.2. LogicDB

Function description: LogicDB is a database accessible by client program after connecting to compute node server, describing the collection of database tables, similar to a database seen after directly connecting to MySQL server.

Function Entry: Click “Configuration” -> “LogicDB” on the Distributed Transactional Database Platform page.

On the logicDB page, enter the logicDB name and click “Search” to search the corresponding information.



The screenshot shows the LogicDB configuration interface. On the left, there's a sidebar with navigation links like Home, Configuration, Node Management, LogicDB, Table Configuration, Sharding Function, Config Checking, Cluster Data Backup & Restore, LogDB User Management, and Server. The main area is titled "LogicDB Configuration > LogicDB". It has a search bar labeled "Filter by LogicDB Name" with a magnifying glass icon. Below it is a table with columns: LogicDB Name, Default Sharding Node, Physical Table Name, Data Node, and Operation. The table contains four rows with names: test, DSCY, zj_d91, and pnt. Each row has a "Delete" button in the Operation column. At the bottom right of the table, there are "Prev", "Next", and "Jump to" buttons, along with a page number indicator "From 1 to 4 Records from 1 / 1 page".

14.2.1. Add LogicDB

Function Entry: “Configuration -> LogicDB -> Add LogicDB”

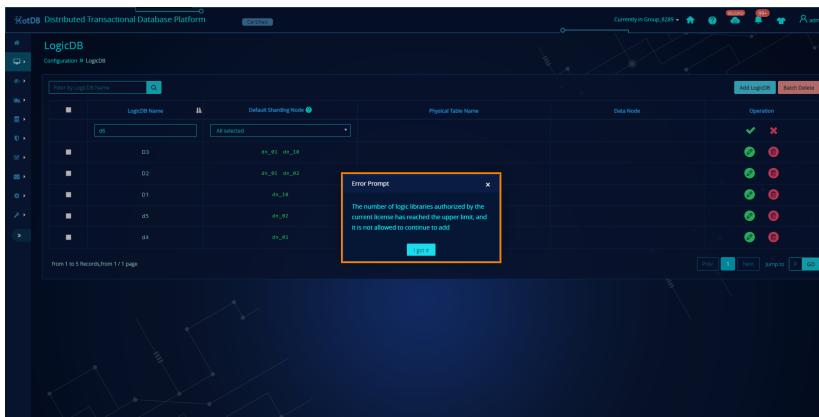


This screenshot shows the "Add LogicDB" form within the LogicDB configuration interface. The search bar at the top is empty. The table below has an additional row for "Enter LogicDB Name" with a text input field and a "Create Data Node" button. The other columns (Default Sharding Node, Physical Table Name, Data Node, Operation) remain the same as the previous screenshot. The table now contains five rows: DB_0919, ba_db, test_backup, and the newly added entry.

- LogicDB name is unique and not empty
- **Default Sharding Node** users can choose whether to configure or not. If it is not configured, table definition information needs to be added on the “[Table Configuration](#)” page of HotDB Management when creating tables under the

logicDB. If it has been configured, table creation statement is directly executed under the logicDB bypassing HotDB Management (when a node is configured by default, execute table creation statement to create vertical sharding tables under the logicDB by default, and when multiple nodes are selected, sharding tables of AUTO_CRC32 type are created by default).

- Click “√”, then the logicDB is added successfully (at this time, the logicDB is empty).
- When the number of existing LogicDBs exceeds the number of authorized LogicDBs, it is not allowed to add new LogicDBs.



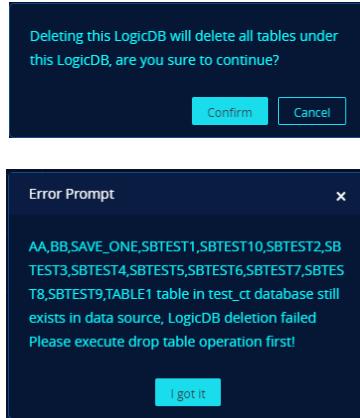
14.2.2. Edit LogicDB

Select “Configuration” -> “LogicDB” -> “Edit LogicDB” in HotDB Management. When changing the logicDB name, it will prompt: “Changing the name may change user privileges associated with the logicDB”, so the logicDB name shall be changed with caution.



Click “√”, then the logicDB is edited successfully.

14.2.3. Delete LogicDB



Description: Deleting the logicDB will delete all tables under the logicDB that have not created the table structure, but if there is any table without “drop table” in the background, a pop-up window will prompt that the logicDB cannot be deleted.

14.3. Table configuration

Function description: The management platform provides visual configuration of business tables for HotDB Server cluster. Generally, in order to create business tables under the service of connecting compute node 3323 ports, it is necessary to define the corresponding tables in the “Table Configuration” function of management platform first, and then reload them successfully to normally create and use the table structure.

Function Entry: Click “Configuration” -> “Table Configuration” on the Distributed Transactional Database Platform page.

Table Type: Global Table, Child Table, Sharding Table and Vertical Sharding Table

Table Type

Compute Node provides four table types: Sharding Table, Vertical Sharding Table, Global Table, Child Table.

Added table information only includes the configuration information of the table, and you need to add table structure with CREATE TABLE syntax on Compute Node server.

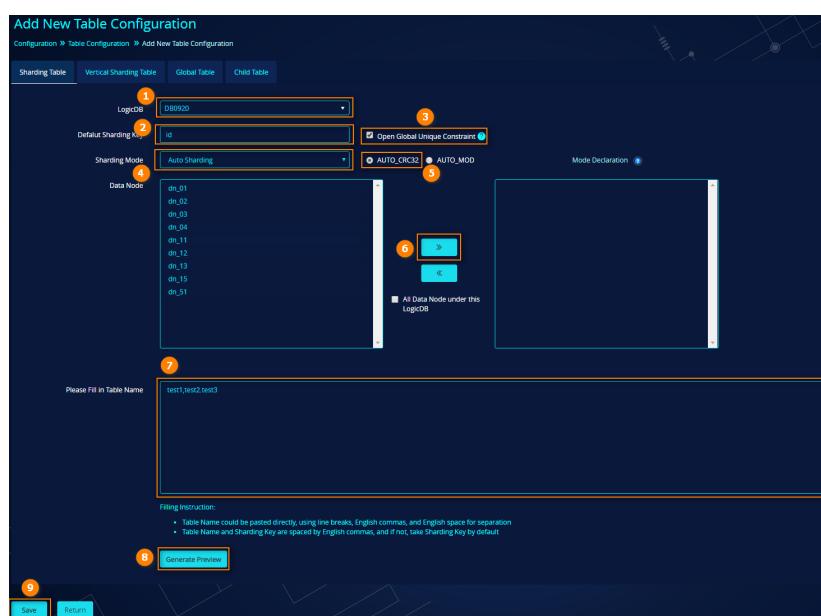
Table Type	Definition
Sharding Table	Data lines are split according to Sharding Keys and Sharding Function, and stored on multiple nodes specified. This is suitable for table with large data amount.
Vertical Sharding Table	Tables only associated with unique nodes and with no sharding function; tables not split or replicated
Global Table	A table is stored on all Data Nodes of this LogicDB. It is suitable for small tables with small data amount or frequent JOIN operation; it is not suitable for tables modified frequently.
Child Table	Parent table is associated with child table through the associated keys of parent table (sharding table), the keys associated with child table are stored in position of Parent Table Associated Key. This can reduce some cross-database.

14.3.1. Add new table configuration

Add New Table Configuration currently supports adding: Sharding Table, Vertical Sharding Table, Global Table and Child Table. The adding of Sharding Table is demonstrated in two modes as follows: Auto Sharding and Advanced Sharding.

Add sharding table in Auto Sharding mode:

Auto Sharding can add sharding tables of AUTO_CRC32 and AUTO_MOD types and AUTO_CRC32 is the default sharding type used by the page. For the difference between them, please refer to the “Mode Description” on the page. For a more detailed introduction, please refer to the “[Sharding Function](#)” chapter.



Step 1: Select the logicDB to which the created sharding table belongs

Step 2: Fill in the sharding key used by the sharding table

Step 3: Check “Open Global Unique Constraint” by default. For a specific description of global unique constraint, please refer to the relevant chapter of *Distributed Transactional Database HotDB Server [Standard] Function Manual*.

Step 4: Select the sharding mode, which is Auto Sharding by default.

Step 5: Select the sharding type as “AUTO_CRC32”.

Step 6: Select the data node of the sharding route of added sharding table (“All Data Node under this LogicDB” is checked by default and matches the data in “Default Sharding Key”. If the “Default Sharding Key” column is not configured, the “Data Node” column data will be matched. If the “Data Node” column is NULL, it will prompt that “there is no relevant data node in the current LogicDB” when the LogicDB is selected).

Step 7: Please Fill in Table Name supports batching addition of table name, and the table can be spaced by line breaks, English commas and English space. If the tables added in batches use the same sharding key, only the table name can be added. If not, enter “table name: sharding key” in the input box to specify the table name, such as: test: id, test1:name.

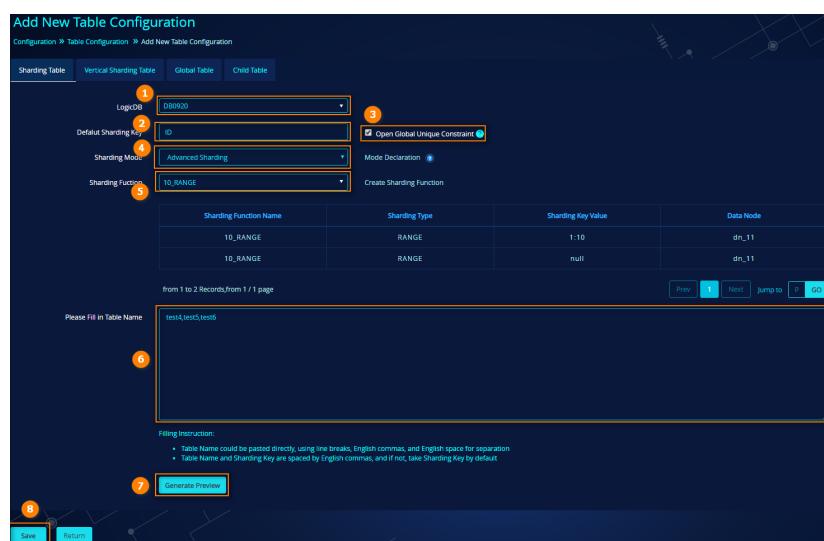
Step 8: Click the “Generate Preview” button to view the table configuration to be added. It is not allowed to directly “Save” unpreviewed tables.

Step 9: Click the “Save” button to add new table configuration to the configDB. [Reload](#) is also required if it needs to take effect immediately into the compute node.

Add sharding table in Advanced Sharding mode:

Brief description of operation steps:

Select LogicDB, fill in Default Sharding Key, select “Advanced Sharding” in Sharding Mode, select Sharding Function (in case of no sharding function, refer to [Add New Sharding Function](#)), fill in the Table Name, click “Generate Preview”, click “Save” and [Reload](#).



The screenshot shows the 'Add New Table Configuration' page with the following steps highlighted:

1. LogicDB dropdown: DB0920
2. Default Sharding Key: ID
3. Open Global Unique Constraint checkbox
4. Sharding Mode: Advanced Sharding
5. Sharding Function: 10_RANGE
6. Table Name input field: test4,test5,test6
7. Generate Preview button

The interface includes a table for sharding function details:

Sharding Function Name	Sharding Type	Sharding Key Value	Data Node
10_RANGE	RANGE	1..10	dn_11
10_RANGE	RANGE	null	dn_11

Below the table, there is a note: "Filling Instruction:
• Table Name could be pasted directly, using line breaks, English commas, and English space for separation
• Table Name and Sharding Key are spaced by English commas, and if not, take Sharding Key by default".

Multiple tables with the same function can be added at one time.

14.3.2. Add new child table

Child table: The child table is an association table and a special set of sharding tables, including a parent table and at least one child table. The data node to which the child table data belongs is determined by the data node to which the parent table data belongs.

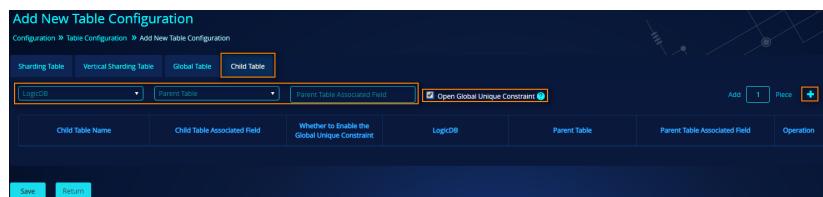
Use of child table: When compute nodes do not support cross-node JOIN operations, compute nodes are designed with the pattern of parent-child tables to support cross-node JOIN operations. The storage location of child table records is based on the storage location of parent table records, which can effectively solve the efficiency and performance problems of JOIN operations across data nodes when the sharding fields are associated keys.

Suggestion for child table: Currently, since compute node support cross-node JOIN operations, the pattern of parent-child tables will not be updated later, so child tables are not recommended

Mode to add child table: Child tables can be added directly in the management platform or added under the parent table record on the table configuration page.

Add new child table directly:

1. Select “Configuration” -> “Table Configuration” -> “Add Table” on the Distributed Transactional Database Management Platform page. select child table on the Add Table Configuration page.
2. Under the child table, select LogicDB and Parent Table, enter the Parent Table Associated Field and the number of child tables to be added, and click on “+” to generate the input field with LogicDB, Parent Table, and Parent Table Associated Field.



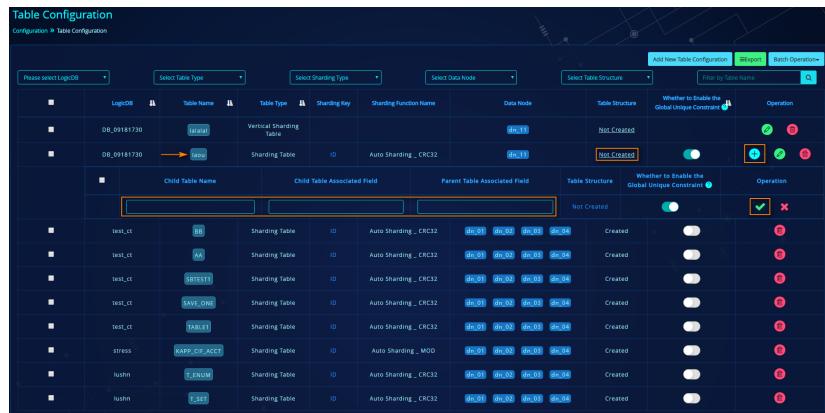
3. Then enter the Child Table Name and Child Table Associated Field, and click “Save”

to add the child table successfully.

Add a child table under the parent table record on the table configuration page:

1. On the table configuration page, select the record with Table Type of “Sharding Table” and Table Structure of “Not Created”.
2. Click on “+”, and then enter the Child Table Name, Child Table Association field, and Parent Table Association Field.
3. Click on “√” to add the child table successfully.

Note: If multiple child tables need to be added under the parent table, the Parent Table Association Field filled in must be consistent. No child table shall be added under the parent table with created table structure.



The screenshot shows the 'Table Configuration' page. At the top, there are dropdown menus for 'Select LogicDB', 'Select Table Type', 'Select Sharding Type', 'Select Data Node', and 'Select Table Structure'. Below these are buttons for 'Add New Table Configuration', 'Delete', and 'Batch Operations'. A search bar with placeholder 'Filter by Table Name' is also present. The main area displays a table with columns: Table Name, Table Type, Sharding Key, Sharding Function Name, Data Node, Table Structure, Whether to Enable the Global Unique Constraint, and Operation. One row is highlighted with an orange border, and its details are shown in a modal dialog at the bottom. The modal has fields for 'Child Table Name' (set to 'test_ct'), 'Child Table Associated Field' (set to 'id'), 'Parent Table Associated Field' (set to 'Auto Sharding_CRC32'), and 'Table Structure' (set to 'Not Created'). It also has checkboxes for 'Whether to Enable the Global Unique Constraint' (unchecked) and 'Operation' (checked). The 'Operation' checkbox is highlighted with an orange border.

14.3.3. Edit table configuration

Function Entry: Select “Configuration” -> “Table Configuration” on the Distributed Transactional Database Platform page, and click the “Edit” button or click the table name to enter “Edit table configuration” page.

Tables can be divided into two statuses: Created and Not Created. When table structure type is Not Created, the table name, logicDB, sharding key, sharding mode and data node can be changed by editing.

Edit table information

Configuration > Table Configuration > Edit table information

Table Name	iacu
Table Structure	Not Created
LogicDB:	DB_09181730
Table Type	Sharding Table
Sharding Key	ID
Sharding Mode	Auto Sharding
Data Node	dn_01 dn_02 dn_03 dn_04 dn_12 dn_13 dn_19 dn_51
	<input type="checkbox"/> Open Global Unique Constraint <input checked="" type="radio"/> AUTO_MOD Mode Declaration
	dn_11 dn_11
	<input type="button" value=">>"/> <input type="button" value="<<"/>

Save **Return**

Click “Save” to edit the table configuration successfully. When the table structure type is Created, it is not allowed to modify the table definition but the table can be modified using “Modify Table Structure” or “Modify Table Configuration”.

Edit table information

Configuration > Table Configuration > Edit table information

Table Name	SITEST1	Modify Table Configuration	Modify Table Structure
Table Structure	Created		
LogicDB:	test_ct		
Table Type	Sharding Table		
Sharding Key	ID		
Sharding Mode	Auto Sharding		
Data Node	dn_11 dn_12 dn_13 dn_15 dn_51		
	<input type="checkbox"/> Open Global Unique Constraint <input checked="" type="radio"/> AUTO_CRC32 <input checked="" type="radio"/> AUTO_MOD Mode Declaration		
	dn_01 dn_02 dn_03 dn_04		
	<input type="button" value=">>"/> <input type="button" value="<<"/>		

Return

Click “Modify Table Structure” to jump to “[Online DDL](#)” function page, and click “Modify Table Configuration” to jump to “[Sharding Plan Online Modification](#)” function page.

14.3.4. Table record export

From 1 to 10 Records/From 1 / 2 page

Table Configuration - DDL										
	A	B	C	D	E	F	G	H	I	J
	Table DB	Table Name	Table Type	Vertical Sharding Table	Sharding key	Sharding Function Name	Node	Table Structure	Are you sure to enable globally unique constraint	Table structure details
1	LogDB	DB_09181730	Table	Vertical Sharding Table	Setting		Not created		No	CREATE TABLE `DB_09181730` (`id` int(11) NOT NULL , `name` varchar(20) DEFAULT NULL , `ENGINE=InnoDB DEFAULT CHARSET=utf8mb4`) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
2	DB_09181730	DB_09181730	Table	Sharing Table		Auto Sharding _ CRC32	dn_11	Not created	Yes	CREATE TABLE `DB_09181730` (`id` int(11) NOT NULL , `name` varchar(20) DEFAULT NULL , `ENGINE=InnoDB DEFAULT CHARSET=utf8mb4`) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
3	test_ct	BB	Sharing Table			Auto Sharding _ CRC32	dn_11	Not created	No	CREATE TABLE `test_ct_BB` (`id` int(11) NOT NULL , `name` varchar(20) DEFAULT NULL , `ENGINE=InnoDB DEFAULT CHARSET=utf8mb4`) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
4	test_ct	AA	Sharing Table			Auto Sharding _ CRC32	dn_01,dn_02,dn_03,dn_04	Created	No	CREATE TABLE `test_ct_AA` (`id` int(11) NOT NULL , `name` varchar(20) DEFAULT NULL , `ENGINE=InnoDB DEFAULT CHARSET=utf8mb4`) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
5	test_ct	SBTEST1	Sharing Table			Auto Sharding _ CRC32	dn_01,dn_02,dn_03,dn_04	Created	No	CREATE TABLE `test_ct_SBTEST1` (`id` int(11) NOT NULL , `name` varchar(20) DEFAULT NULL , `ENGINE=InnoDB DEFAULT CHARSET=utf8mb4`) ENGINE=InnoDB AUTO_INCREMENT=999999 DEFAULT CHARSET=utf8mb4;
6	test_ct	SAVE_ONE	Sharing Table			Auto Sharding _ CRC32	dn_01,dn_02,dn_03,dn_04	Created	No	CREATE TABLE `test_ct_SAVE_ONE` (`id` int(11) NOT NULL , `name` varchar(20) DEFAULT NULL , `PRIMARY KEY (id)` , `ENGINE=InnoDB DEFAULT CHARSET=utf8mb4`) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
7	test_ct	TABLE1	Sharing Table			Auto Sharding _ CRC32	dn_01,dn_02,dn_03,dn_04	Created	No	CREATE TABLE `test_ct_TABLE1` (`id` int(11) NOT NULL , `name` varchar(20) DEFAULT NULL , `ENGINE=InnoDB DEFAULT CHARSET=utf8mb4`) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;

Click the “Export” button on the table configuration page to export the checked records. If not checked, all table configuration records are exported by default.

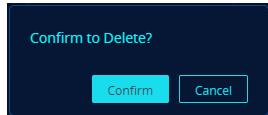
If the “Export Table Structure of Created Tables” is checked, the “Table structure details” column is automatically added to the exported content to display the “Create Table Statement” of the created table.

“Table structure details” in the export record is obtained by the display @@ddl command in the compute node management port (3325), and the sharding table and the global table adopt the minimum DDL of DNID in the data node. If the current master 3325 port cannot be connected, the “Table Structure” and “Table structure details” are NULL.

14.3.5. Delete table

Function Entry: Select “Configuration” -> “Table Configuration” -> “Delete” on the Distributed Transactional Database Platform page.

Function description: Click the “Delete” button, then the pop-up box will prompt: “Confirm to Delete?”. Click “Confirm” to delete the uncreated table successfully.



Note:

- Tables with no table structure created can be deleted directly
- After deleting the created table, a prompt will pop up: “The xxx table still exists on the server, and the deletion of table fails. Please delete it after dropping the table on the server”.

14.3.6. Historical compatibility description

HotDB Server after V2.4.6 dropped HASH (including HASH23) and AUTO sharding function. Subsequent new tables will no longer support the use of dropped sharding function, except for tables that have historically used HASH (including HASH23) and AUTO, but attention shall be paid to: “If String-type Sharding Key Operation is Applied in SQL, the Case Sensitivity shall be Paid Attention to (That is to Ensure that the case in SQL, Sharding Key is Consistent with Data Input). At the same time, if the management platform detects tables which cite HASH (including HASH23) and AUTO in the system, Table Configuration, Add Table and Edit Table pages will have corresponding prompt information, as shown in the following figure:

Table Configuration
Configuration > Table Configuration

Please select Log DB Select Table Type Select Sharding Type Select Data Node Select Table Structure Filter by Table Name

Log DB	Table Name	Select Sharding Type	Sharding Key	Sharding Function Name	Data Node	Table Structure	Operation
pm	userxx	Automatic sharding	id	Automatic sharding	dn245.01 dn245.02 dn245.03 dn245.04	Created	
hotdb	tb2	Sharding Table	id	Automatic sharding	dn245.01 dn245.02 dn245.03 dn245.04	Created	
hotdb	tb3	Sharding Table	id	Automatic sharding	dn245.01 dn245.02 dn245.03 dn245.04	Created	

From 1 to 3 Records, from 1 / 1 page

Note: When Sharding Rule Using AUTO or HASH Sharding Function, It Needs to Notice That, If String-type Sharding Key Operator is Applied in SQL, the Case Sensitivity Shall be Paid Attention to (That Is to Ensure the Case Sensitivity in SQL Sharding Key is Consistent with Data Input). It's Recommended Using Online Modification of Sharding Function to Migrate the Table Which Historically Uses AUTO or HASH Sharding Function, and for the Mode of Migration, Contact the Manager User or View Relevant Documentation.

Data migration description: It is recommended migrating the table data to a new sharding function table if there are tables which historically cite HASH (including HASH23) and AUTO sharding functions in the system. Table data migration can be performed manually or using the sharding plan online modification command provided by the management port. For details, please refer to [Manual for \[Manager Command\] Function of Distributed Transactional Database HotDB Server](#).

14.4. Sharding function

Sharding Function provides the route method and algorithm for horizontal splitting of tables. Currently, compute nodes support the following sharding function types: five advanced sharding types (ROUTE, RANGE, MATCH, SIMPLE_MOD, CRC32_MOD), and two auto sharding types (AUTO_MOD, AUTO_CRC32). Refer to the new chapters of sharding table for AUTO_MOD and AUTO_CRC32.

Function Entry: Select “Configuration” -> “Sharding Function” on the Distributed Transactional Database Platform page.

Seven sharding types are described in detail as follows:

Advanced Sharding Type				
Sharding Type	Sharding Type Declaration	Applicable Sharding Key type	Input value	Recommended scenario
MATCH	Full Character Match, case insensitive	Character string, enum type	Input value of string type	The organization name, type and other string field
RANGE	Sharding based on successive ranges, the range value includes the critical value on both sides	Value type	The min value and the max value in a range, or automatically calculate step length by the platform and then divide the range	Numeric fields such as postal type. Note: timestamp is not suitable for Sharding Key, but it is necessarily to be considered as field in MYSQL partition
ROUTE	Equivalent matched integer input value	Integer Type	Integers or the min value, max value and step length in a range to divide several integers	Organization ID, postal code, type code and other integer fields
SIMPLE_MOD	(After implicit conversion) Remainder is taken based on module value and value and raise in corresponding Data Node	Numeric, character type types	Module value, module value must be greater than the number of the selected Data Node	It is recommended to use fields that are regularly generated on the application client

Auto Sharding Type				
Sharding Type	Sharding Type Declaration	Applicable Sharding Key Type	Input value	Recommended scenario
AUTO_MOD	Module value is given based on the number of Data Node by the platform, which is similar to the calculation of SIMPLE_MOD	Numeric, character string, time type	No need to fill in	suitable for general scenarios
CRC32_MOD	Module value is given based on the number of Data Node by the platform, which is similar to the calculation of SIMPLE_MOD	Nearly all the types	No need to fill in	suitable for general scenarios

Description of historical changes of the sharding function:

HASH (dropped after V2.4.6), CRC32_MOD (new in V2.4.7), AUTO (replaced by AUTO_MOD after V2.4.6) and AUTO_CRC32 (new in V2.4.7).

14.4.1. MATCH

Adding sharding function with sharding type of MATCH is displayed taking the auto setting and manual setting modes as an example as follows.

Add sharding function of MATCH type in auto setting mode

Function demonstration:

Step 1: “Automatic Generation of Sharding Function Name” (automatic generation of function: existing sharding function maximum ID+1_sharding type name) is checked by default. It shall be unchecked in case of any custom name requirement.

Step 2: Select “MATCH” for “Sharding Type”

Step 3: Select the default “Auto Setting” mode

Step 4: Select the data node to be used for sharding function

Step 5: Check “For NULL Value, Distribute Route Node Automatically” and “For Blank String, Distribute Route Node Automatically” by default. That is, when the sharding key value of the inserted data is NULL or blank string, the program will automatically select the route data node.

In v.2.5.6 and above, "Match by Digit Number" is added (not checked by default) for some numerical scenario that requires prefix/infix/suffix for sharding. After checking and fill in the matching rule. According to the filling, the corresponding route rules will be generated automatically. The routing of data is based on the rules corresponding to "from left" or "from right", instead of full matching routing according to the original string.

For example:



For example, if the express delivery order number "YTQSXXXX4587XXX" needs to be matched according to the first four letters YTQS, you can set the matching rule as: Start from the first on the left to match 4 digits, and enter the value "YTQS". If you need to match from the last four numbers"4587", you can set the matching rule as: start from the seventh on the right to match 4 digits backward, and enter the value "4587".

When “Match by Digit Number” is checked, the digit number of the input value must be the same as the number of matching digit number. Otherwise, it will prompt that the preview cannot be saved when previewing. For example, as shown in the figure below, if the matching digit number is 2 and the input value has more than 2 digits, it is will not be allowed to save.

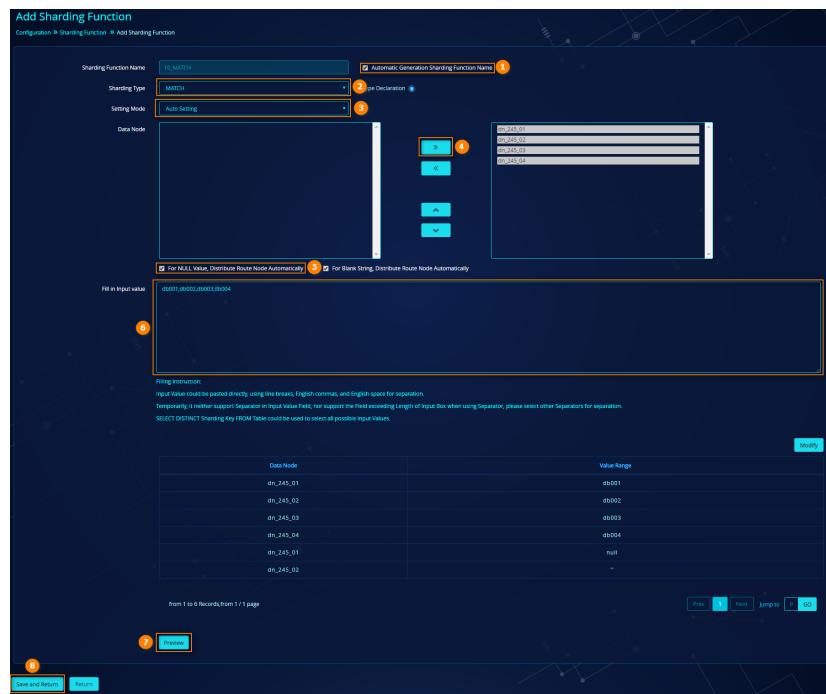


Step 6: Enter the value matching each data node, which can be spaced by line breaks, English commas or English space.

Step 7: Click “Preview” to view the effect of sharding function.

Step 8: Click the “Save and Return” button to save the new sharding function to the

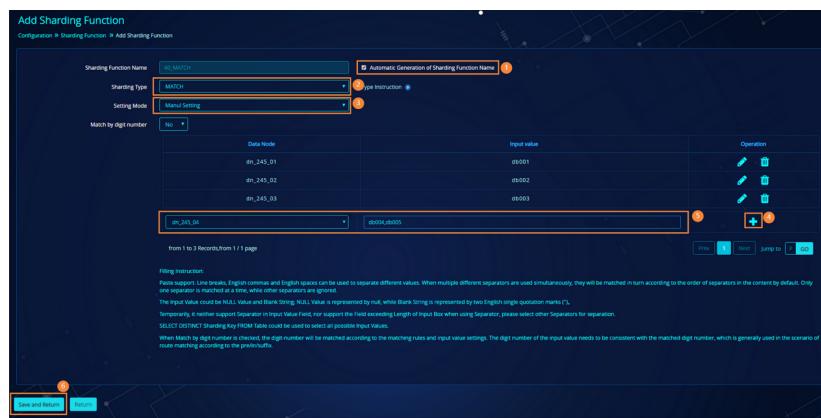
configDB. [Reload](#) is also required if it needs to take effect immediately into the compute node.



Add sharding function of MATCH type in manual setting mode

Brief description of operation steps:

Select “Automatic Generation of Sharding Function Name” by default, select MATCH sharding type, set “Manul Setting” mode, check “Match by Digit Number” and fill the matching rule or not, click “+” to add records, select data nodes and matching values, click “Save and Return” and [Reload](#).



Note: Manual setting of input values supports the input of multiple values which shall be spaced by English commas or English space

14.4.2. RANGE

Adding sharding function with sharding type of RANGE is displayed taking the auto setting and manual setting modes as an example as follows.

Add sharding function of RANGE type in auto setting mode

Function demonstration:

Step 1: “Automatic Generation of Sharding Function Name” (automatic generation of function: existing sharding function maximum ID+1_sharding type name) is checked by default. It shall be unchecked in case of any custom name requirement.

Step 2: Select “RANGE” for “Sharding Type”

Step 3: Select the default “Auto Setting” mode

Step 4: Select the data node to be used for sharding function

Step 5: Check “For NULL Value, Distribute Route Node Automatically” by default. That is, when the sharding key value of the inserted data is NULL, the program will automatically select the route data node.

When it is in 2.5.6 and above, "Automatically distribute route nodes to the maximum /

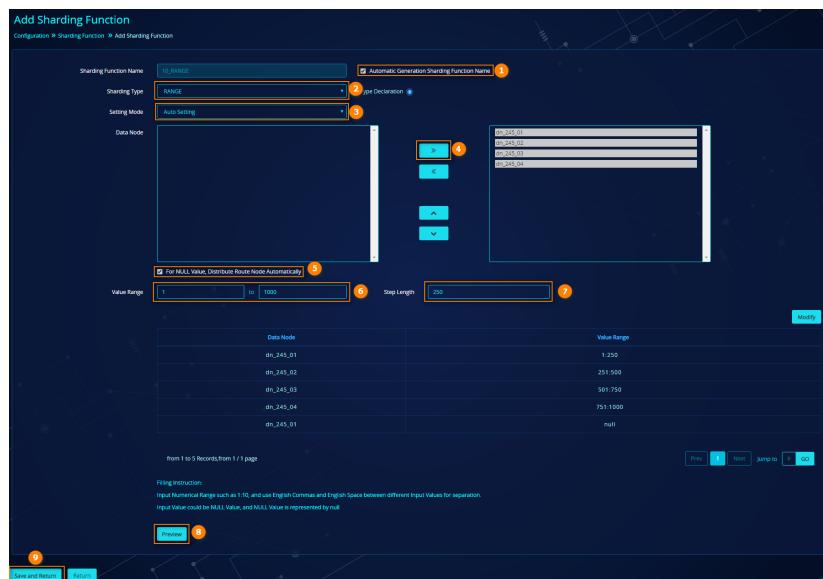
"minimum boundary value" is added (not checked by default). If checked, the maximum and minimum value boundary will be automatically generated according to the value range filled in by the user. For example, fill in 1-100 and check "Automatically distribute route nodes to the maximum / minimum boundary value", then the boundary data less than 1 and greater than 100 will be automatically sharded, so there is no need to worry that the boundary value cannot be routed.

Step 6: The value range is the range of sharding key values (only integers are allowed)

Step 7: Select the generated step length by default (step length calculation formula: larger value minus smaller value and divide the number of selected data nodes) and modify the default generated value if it needs to customize the step length.

Step 8: Click the “Preview” button to view the sharding effect.

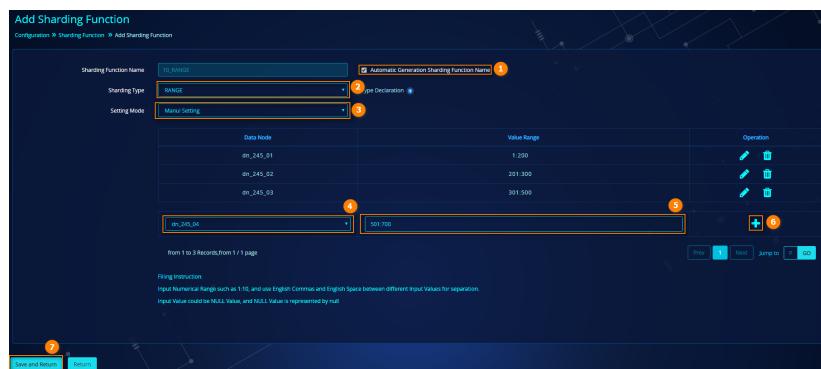
Step 9: Click the “Save and Return” button to save the new sharding function to the configDB. [Reload](#) is also required if it needs to take effect immediately into the compute node.



Add sharding function of RANGE type in manual setting mode

Brief description of operation steps:

Select “Automatic Generation of Sharding Function Name” by default, select RANGE sharding type, set “Manul Setting” mode, select data nodes and range of matching values (value range is represented by an English colon, such as 10:20), click “+” to add records, and click “Save and Return”



Note: Manual setting of input values supports the input of multiple values which shall be spaced by English commas or English space. When it is in v.2.5.6 and above, “greater than” or “less than” is supported for the value range to distinguish the maximum and minimum value boundary.

14.4.3. ROUTE

Adding sharding function with sharding type of RANGE is displayed taking the auto setting and manual setting modes as an example as follows.

Add sharding function of ROUTE type in auto setting mode

Function demonstration:

Step 1: “Automatic Generation of Sharding Function Name” (automatic generation of function: existing sharding function maximum ID+1_sharding type name) is checked by default. It shall be unchecked in case of any custom name requirement.

Step 2: Select “ROUTE” for “Sharding Type”

Step 3: Select the default “Auto Setting” mode

Step 4: Select the data node to be used for sharding function

Step 5: Check “For NULL Value, Distribute Route Node Automatically” by default. That is, when the sharding key value of the inserted data is NULL, the program will automatically select the route data node.

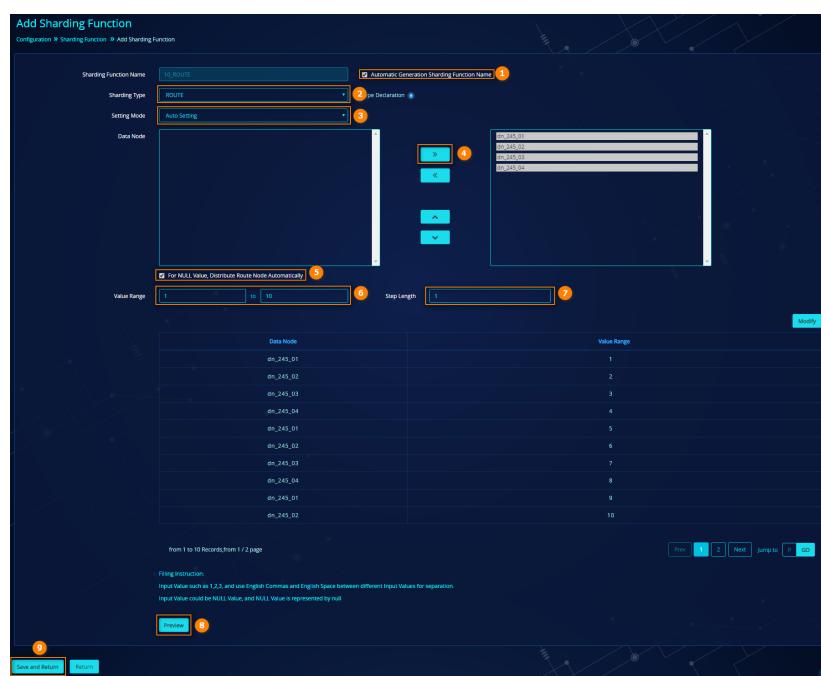
The same as MATCH type. When it is v.2.5.6 and above, you can also select "Match by Digit Number" (not checked by default) and fill in the matching rule. According to the filling, the corresponding route rules will be generated automatically. Here the ROUTE type is suitable for some numerical scenario that requires prefix/infix/suffix for sharding. The routing of data is based on the rules corresponding to "from left" or "from right", instead of full matching routing according to the original string.

Step 6: The value range is the range of sharding key values (only integers are allowed)

Step 7: Select the generated step length by default and modify the default generated value if it needs to customize the step length.

Step 8: Click the “Preview” button to view the sharding effect.

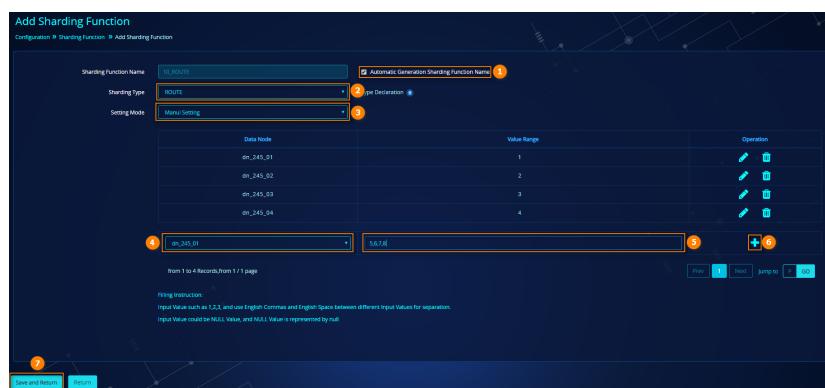
Step 9: Click the “Save and Return” button to save the new sharding function to the configDB. [Reload](#) is also required if it needs to take effect immediately into the compute node.



Add sharding function of ROUTE type in manual setting mode

Brief description of operation steps:

Select “Automatic Generation of Sharding Function Name” by default, select ROUTE sharding type, set “Manul Setting” mode, check “Match by Digit Number” and fill the matching rule or not, select data nodes and matching values, click “+” to add records, and click “Save and Return”.



Note: Manual setting of input values supports the input of multiple values which shall be spaced by English commas or English space

14.4.4. SIMPLE_MOD

Adding sharding function with sharding type of SIMPLE_MOD is displayed taking the auto setting and manual setting modes as an example as follows.

Add sharding function of SIMPLE_MOD type in auto setting mode

mode

Function demonstration:

Step 1: “Automatic Generation of Sharding Function Name” (automatic generation of function: existing sharding function maximum ID+1_sharding type name) is checked by default. It shall be unchecked in case of any custom name requirement.

Step 2: Select “SIMPLE_MOD” for “Sharding Type”

Step 3: Select the default “Auto Setting” mode

Step 4: Select the data node to be used for sharding function

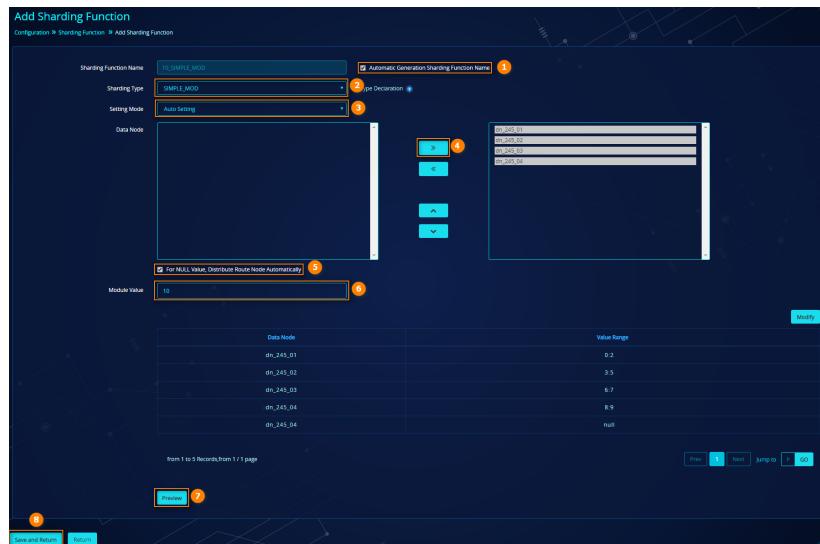
Step 5: Check “For NULL Value, Distribute Route Node Automatically” by default. That is, when the sharding key value of the inserted data is NULL, the program will automatically select the route data node.

Step 6: Input the module value (positive integers only), which is a parameter of the

reminder calculation between sharding key value and input module value. It is finally routed to the corresponding data node according to the obtained remainder.

Step 7: Click the “Preview” button to view the sharding effect.

Step 8: Click the “Save and Return” button to save the new sharding function to the configDB. [Reload](#) is also required if it needs to take effect immediately into the compute node.

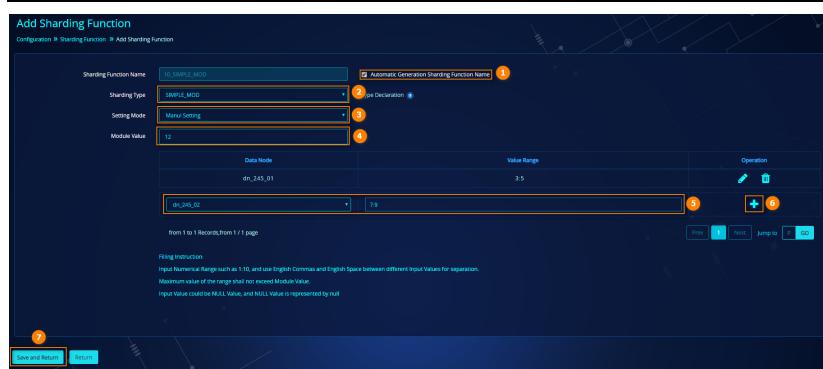


Add sharding function of SIMPLE_MOD type in manual setting mode

mode

Brief description of operation steps:

Select “Automatic Generation of Sharding Function Name” by default, select SIMPLE_MOD sharding type, set “Manul Setting” mode, set the module value, select data nodes and matching values, click “+” to add records, and click “Save and Return”



Note: Manual setting of input values supports the input of multiple values which shall be spaced by English commas or English space

14.4.5. CRC32_MOD

Adding sharding function with sharding type of CRC32_MOD is displayed taking the auto setting and manual setting modes as an example as follows.

Add sharding function of CRC32_MOD type in auto setting mode

Function demonstration:

Step 1: “Automatic Generation of Sharding Function Name” (automatic generation of function: existing sharding function maximum ID+1_sharding type name) is checked by default. It shall be unchecked in case of any custom name requirement.

Step 2: Select “CRC32_MOD” for “Sharding Type”

Step 3: Select the default “Auto Setting” mode

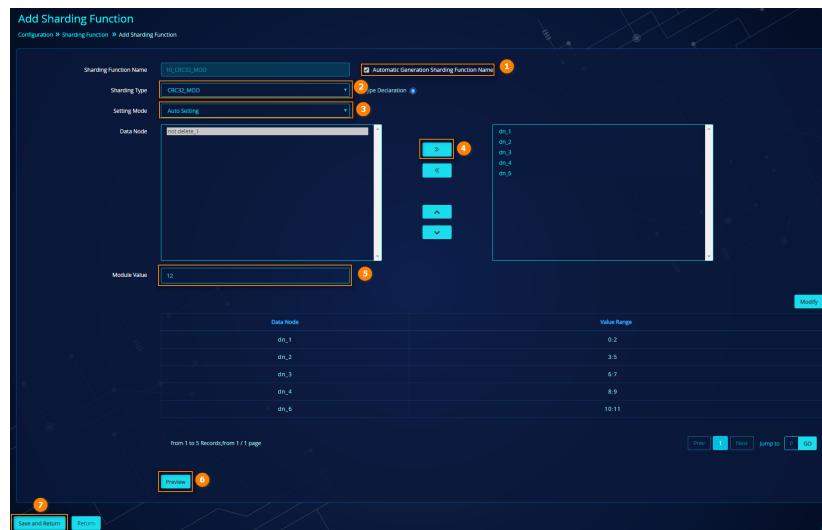
Step 4: Select the data node to be used for sharding function

Step 5: Input the module value (positive integers only), which is a parameter of the remainder between sharding key value and input module value. It is finally routed to the corresponding data node according to the obtained remainder.

Step 6: Click the “Preview” button to view the sharding effect.

Step 7: Click the “Save and Return” button to save the new sharding function to the configDB. [Reload](#) is also required if it needs to take effect immediately into the compute

node.



Add sharding function of CRC32_MOD type in manual setting mode

mode

Brief description of operation steps:

Select “Automatic Generation of Sharding Function Name” by default, select CRC32_MOD sharding type, set “Manul Setting” mode, set the module value, select data nodes and matching values, click “+” to add records, and click “Save and Return”

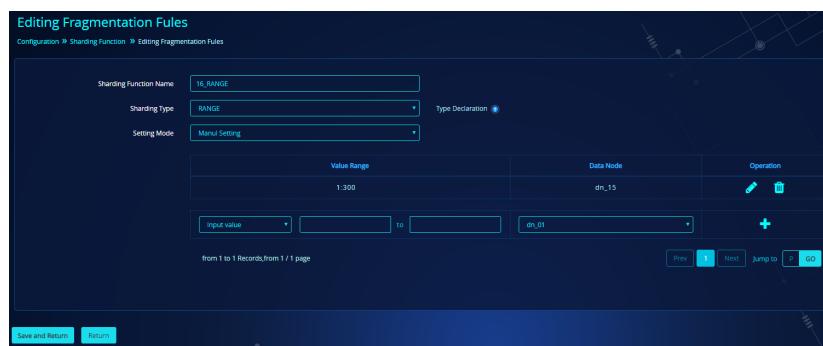


Note: Manual setting of input values supports the input of multiple values which shall be spaced by English commas or English space

14.4.6. Edit sharding function

Function Entry: Select “Configuration” -> “Sharding Function” -> “Edit sharding function” on the Distributed Transactional Database Platform page.

Function operation: On the Edit sharding function page, change the Sharding Function Name, Sharding Type, Setting Mode, etc., and click “Save and Return” to edit the sharding function successfully.



Value Range	Data Node	Operation
1:300	dn_15	
<input type="text"/> Input value	<input type="text"/> dn_01	

Modification notes:

- Sharding Function Name shall not be repeated.
- Sharding Function Name shall not be NULL.
- Modification of sharding function for tables with associated table structure created: No modification shall not be allowed for AUTO (history version), HASH (history version), and SIMPLE_MOD type

The RANGE, ROUTE and MATCH types allow the addition of sharding function parameters (adding a new node requires creating tables manually on the node), but allow no modification of the original sharding function parameters.

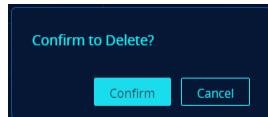
Parent and child table: Once defined, the sharding function for patent table shall

not be modified.

14.4.7. Delete sharding function

Function Entry: Select “Configuration” -> “Sharding Function” -> on the Distributed Transactional Database Platform page, and click “Delete” on the Sharding Function page.

Function description: Click the “Delete” button and then a pop-up box will prompt: “Confirm to Delete?” Click “Confirm” to delete the sharding function successfully.

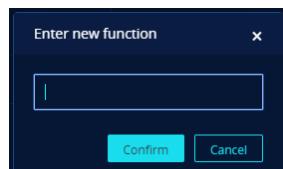


Note: The sharding function that has been cited by the table cannot be deleted.

14.4.8. Replicate sharding function

Function Entry: Select “Configuration” -> “Sharding Function” -> “Replication” 

Function description: Click the “Replicate” button on the sharding function page to pop up the new sharding function name input box, enter the new function name and click “Confirm” to replicate the sharding function successfully.

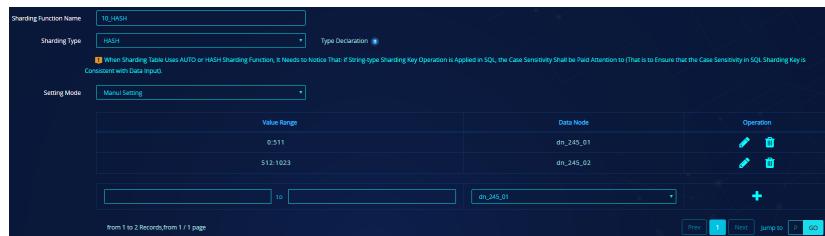


Replication notes:

- New sharding function name shall not be NULL.
- New sharding function name shall not be repeated.

14.4.9. Special description

When the sharding key is of string type and the sharding type is AUTO or HASH, Hot DB Server has different route results for string case, that is, when the sharding key is of string type, it is sensitive to case. When using sharding key in SQL, its case shall be consistent with that when storing data to query the corresponding data. Therefore, the AUTO and HASH sharding types have been dropped in V2.4.7. For the new version, it is recommended to replace HASH\AUTO with partition types such as CRC32_MO_D\AUTO_CRC32, while sharding tables of HASH\AUTO type are still allowed for the thought of smooth transition. If historical data contains partition types like AUTO or HASH, the page will give the following prompt, which requires extra attention when using.

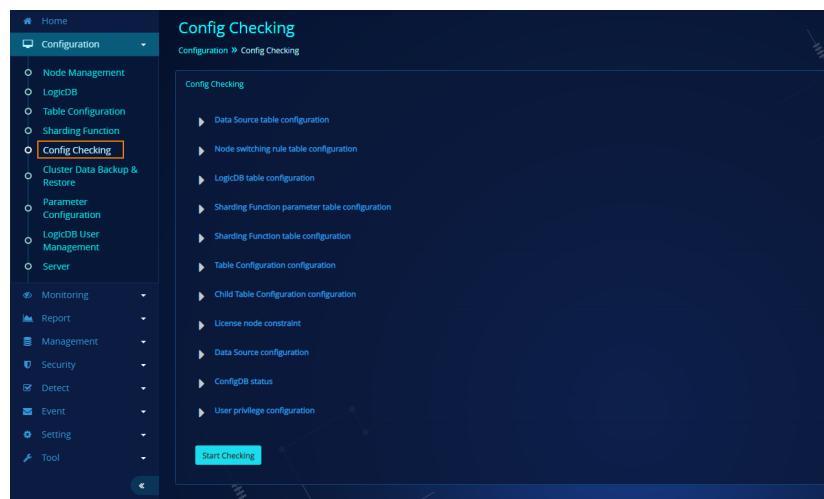


14.5. Config checking

Config checking mainly provides checking for the related configuration of compute nodes to prevent abnormal operation caused by manual setting error or offline modification of the related configuration of compute nodes.

DR mode explanation: when the DR mode is enabled, please refer to the chapter "Config checking" in the [Distributed Transactional Database HotDB Server - Cross-IDC Disaster Recovery Function Specification](#) for the relevant logical explanations of configuration checking.

Function Entry: Select “Configuration” -> “Config Checking” on the Distributed Transactional Database Platform page.



Operation description: Click the [Start Checking] button to directly Start Config checking. When all checking items are passed, the checking is successful and there is no problem with the current configuration. When an error is reported in the checking information, the user who fails the checking shall modify according to the checking failure prompt, and then perform Config checking.

Checking tips: Config checking failures are divided into ERROR (red font display) and WARNING (orange font display) generally. When ERROR level information appears, users need to modify and solve the related problems immediately, otherwise [Reload](#) cannot be performed. WARNING information indicates a failure to which attention shall be paid and which does not affect the operation of compute nodes.

Config Checking

Compute Node Configuration > Config Checking

Config Checking

- ▼ Data Source table configuration error ✖
 - a. Data Node reference is normal ✓
 - b. Data Source database does not repeat ✓
 - ▼ Data Source cannot be connected ✖
 - Data Source name (Data Source ID)
 - 192.168.210.43_3308_phy09181615(16)
 - 192.168.210.41_3307_phy1437(18)
 - 192.168.210.76_3307_phy1447(19)
 - d. One data node has only one Active Master ✓
 - e. Data Node must contain Data Source ✓
 - f. A Data node must contain available data source ✓
 - g. One Data Node must contain a Data Source of Active Master type ✓
 - h. The character set of data source must be consistent ✓
 - i. Non-MGR Data Node cannot cite MGR type Data Source ✓
 - j. Data node cannot cite common master-slave data source ✓
 - k. ConfigDB cannot be added as data source ✓
 - l. Data Source user and ConfigDB user cannot share ✓
- ▶ Node switching table Config Checking passed ✓
- ▶ LogicDB table Config Checking passed ✓
- ▶ Sharding function parameter table Config Checking passed ✓
- ▶ Sharding Function table Config Checking passed ✓
- ▶ Table Configuration configuration error ✖
- ▶ Child Table Configuration Config Checking passed ✓
- ▶ License node constraint checking passed ✓
- ▼ Data Source Config Checking error ✖
 - a. Whether Data Source configuration is correct
 - Data Node: dn_249_01 Data Source under 192.168.220.149_3307_db249_01 (192.168.220.149.3307/db249_01) The time difference with Compute Node is within 0.5~3 seconds, with a difference of 1s
 - Data Node: dn_249_02 Data Source under 192.168.220.149_3307_db249_02 (192.168.220.149.3307/db249_02) The time difference with Compute Node is within 0.5~3 seconds, with a difference of 1s
 - Data Node: dn_249_03 Data Source under 192.168.220.149_3307_db249_03 (192.168.220.149.3307/db249_03) The time difference with Compute Node is within 0.5~3 seconds, with a difference of 1s
 - Data Node: dn_10 Data Source under 192.168.210.41_3307_db249_xy (192.168.210.41.3307/db249_xy) The time difference with Compute Node is within 0.5~3 seconds, with a difference of 1s
 - Data Node: dn_11 Data Source under 192.168.210.42_3307_db249_xy (192.168.210.42.3307/db249_xy) The time difference with Compute Node is within 0.5~3 seconds, with a difference of 1s
 - b. Reload requirement: the replication delay between available master Data Source and original master Data Source cannot exceed 10s ✓
 - c. Reload requires that the replication status between available master data source and original master data source shall be normal ✓
- ▶ ConfigDB connection is normal ✓
- ▶ User permission configuration is normal ✓

[Return](#)

Config Checking Items:

Type	Checking Content
	Data Node reference is normal
	Data Source database does not repeat

Data source table configuration	Data Source cannot be connected
	A Data Node must contain available data source
	Data Node must contain Data Source
	One data node has only one Active Master
	One Data Node must contain a Data Source of Active Master type
	The character set of data source must be consistent
	Non-MGR Data Node cannot cite MGR type Data Source
	Data node cannot cite common master-slave data source
	ConfigDB cannot be added as data source
	Data source user and configDB user cannot share
The logical architecture of compute nodes in the master center and the DR center is the same.	
Node switching rule table configuration	Data Source reference is normal
	Data Source and Data Node high availability source cannot be the same
	Data Source and Data Node high availability source must belong to the same data node
LogicDB table configuration	Data Node reference is normal
	Sharding function reference is normal
	Data Node reference is normal

Sharding function parameter table configuration	The column_value of RANGE or HASH route method must be in the form of an interval, such as: a:b, and a and b shall be numbers, a<=b
	The sharding parameter value range of HASH route method cannot contain negative numbers
	The sharding parameter value of automatic Sharding Route method shall be a positive integer
	The sharding parameter value of ROUTE route method shall be an integer
	Sharding function parameter is normal
	Sharding interval of RANGE or HASH shall have no overlap
	The column_value of SIMPLE_MOD or CRC32_MOD route method can be a number greater than or equal to 0 or an interval, such as: a:b, and a and b shall be numbers, a>=0, b>=0, a<=b
	The module value of SIMPLE_MOD or CRC32_MOD must be within 2-2147483647
	SIMPLE_MOD or CRC32_MOD must be configured with module values
Sharding function table configuration	The sharding parameter value interval of SIMPLE_MOD or CRC32_MOD shall have no overlap
	Sharding function reference is normal

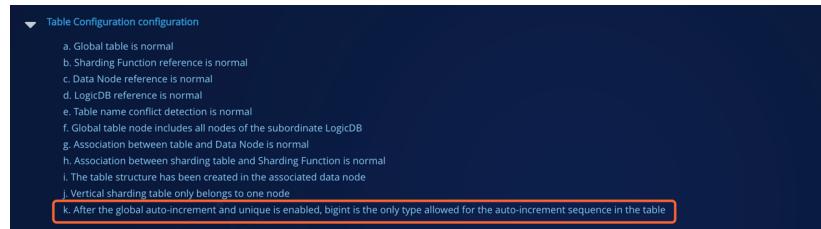
Table Configuration	Global table is normal
	Sharding function reference is normal
	Data Node reference is normal
	LogicDB reference is normal
	Table name conflict detection is normal
	Global table node must contain all nodes of the logicDB it belongs to
	Association between table and data node is normal
	Sharding table sharding function association is normal
	Vertical sharding table belongs to only one node
Child table configuration	After the global auto-increment and unique is enabled, bigint is the only type allowed for the auto-increment sequence in the table.
	Parent table reference is normal
	Parent table sharding type is normal
	Association between one parent table and multiple child tables is normal
	Relation between child table and parent table is normal
License management	Child table has no conflict with parent table name
	Node number limitation checking passed
	LogicDB number limitation checking passed

Data source configuration	Data source configuration is correct
	Reload requirement: the replication latency between available master Data Source and original master Data Source cannot exceed 10s
	Reload requires that the replication status between available master data source and original master data source shall be normal
ConfigDB status	ConfigDB connection is normal
	ConfigDB replication status is normal
user privilege configuration	The data source connection user privilege configuration is normal (privilege shall not be lower than: select,insert,update,delete,create,drop,index,alter,process,references,super,reload (only when the node version is greater than or equal to V2.5.3), lock tables,replication slave,replication client,trigger,display view,create view,create routine,xa_recover_admin (only for data source instances of version 8.0 and above), alter routine,execute,event)
	The configDB connection user privilege configuration is normal (privilege shall not be lower than: select,insert,update,delete,create,drop,index,alter,create temporary tables,references,super,reload (only when the compute node version is greater than or equal to V2.5.3), lock tables,replication slave,replication client)
Compute node configuration	Whether the currently configured compute node mode matches the real compute node mode.

Notes:

“k. After the global auto-increment and unique is enabled, bigint is the only type allowed for the auto-increment sequence in the table.” is a newly added verification rule

for management platforms of v.2.5.5 and above, as shown in the following figure:



When in cluster mode and autoIncrement is set to 2 (auto-increment and unique), if there is historical auto-increment sequence of type smallint, tinyint, mediumint, int, the dynamic loading will be affected and “After the global auto-increment and unique is enabled, bigint is the only type allowed for the auto-increment sequence in the table.” will be prompted, as shown below:

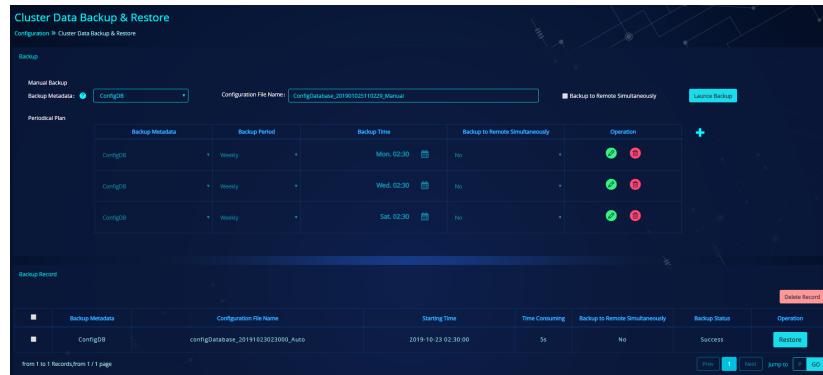


This verification rule verifies tables with auto-increment columns enabled under all LogicDBs only when autoIncrement is set to 2, that is, "global auto-increment and unique" and the compute node mode is multi-node cluster. The displayed information includes: LogicDB, table name, field name of auto-increment column and current type of auto-increment column that does not conform to the verified table.

14.6. Cluster metadata backup and restore

Config metadata refers to compute node configDB data and configuration files. HotDB Management backs up metadata for compute nodes manually or periodically in case important configuration data is lost or damaged and cannot be recovered.

14.6.1. Cluster metadata backup



The screenshot shows the 'Cluster Data Backup & Restore' section of the management platform. It includes a 'Periodical Plan' table and a 'Backup Record' table.

Periodical Plan:

Backup Metadata	Backup Period	Backup Time	Backup to Remote Simultaneously	Operation
ConfigDB	Weekly	Mon. 02:30	No	(green)
ConfigDB	Weekly	Wed. 02:30	No	(green)
ConfigDB	Weekly	Sat. 02:30	No	(green)

Backup Record:

Backup Metadata	Configuration File Name	Starting Time	Time Consuming	Backup to Remote Simultaneously	Backup Status	Operation
ConfigDB	configDatabase_201910230200_Manual	2019-10-23 02:30:00	5s	No	Success	Restore

Manual Backup



The screenshot shows the 'Manual Backup' configuration screen for 'ConfigDB'.

Configuration File Name: configDatabase_20190924113442_Manual

Backup to Remote Simultaneously

[Launch Backup]

- Metadata Backup can be divided into the “ConfigDB” or “ConfigFile”. ConfigDB is the data in the master configDB currently used by the compute node; ConfigFile is all files under the bin, conf, and lib directories of the current master compute node, and the master/slave mode clusters also include backup keepalived.conf file.
- Click the [Launch Backup] button to issue a backup command by HotDB Management. ConfigDB MySQL instance performs a backup operation through mysqldump and stores the backup file under the HotDB Management installation directory data/. The configFile is directly backed up from the master compute node server to the HotDB Management installation directory data/.

- When backing up the “ConfigFile”, it needs to configure the SSH connection information of the server where the compute node is located on the “Configuration->Server” menu page and ensure the normal connection. Also, it needs to ensure that the master compute node in the cluster runs normally. In addition, the configured SSH connection user also needs to have privileges to view the compute node running thread information. If the above requirements are not met, the configuration file cannot be backed up normally.

Remote Backup

Remote Replication Mode: SCP RSYNC

Remote Hostname: _____ Remote Host User: _____ Sign in without password

Remote Storage Directory: _____ Remote Host Password: _____

- To improve the backup metadata security, this function also backs up the backup metadata to a remote server. Check “Backup to Remote Simultaneously” to manually Start a backup. Select “Yes” for “Backup to Remote Simultaneously” in the plan of periodical backup.
- Using the remote backup function requires configuring remote server related parameters.

Remote Replication Mode: Supporting both SCP and RSYNC. If RSYNC replication mode is selected, it needs to install RSYNC tools on all compute node servers and remote servers in advance.

Sign in without password: If a remote server is connected through Sign in without password, all compute node servers are required to establish a password-free channel with the remote server. For the establishment of password-free channel, refer to the “Password-free Channel Description” chapter of the [Distributed Transactional Database HotDB Server \[Installation and Deployment\] Function Manual](#).

Remote Hostname: IP address of the remote server

Remote Host User/Password: SSH information for remote server connection

Remote Storage Directory: The directory where the backup metadata is stored in the remote server, which must be a directory that exists and in which remote connection accounts have write privileges

Periodical Backup

Periodical Plan					
Backup Metadata	Backup Period	Backup Time	Backup to Remote Simultaneously	Operation	
ConfigDB	Weekly	Mon. 02:30	No		
ConfigDB	Weekly	Wed. 02:30	No		
ConfigDB	Weekly	Sat. 02:30	No		

- Periodical Backup time can be set to 3 types: daily, weekly and monthly, but the “Cluster metadata backup and restore” function in HotDB Management can only add up to 6 periodical backup plans.
- Periodical tasks can periodically back up configDB or configFile. When configuring backup plans with the same metadata type and conflicting backup time, only one of the periodical tasks will be executed.

14.6.2. Cluster metadata restore

Cluster metadata restore

Backup Record							
	Backup Metadata	Configuration File Name	Starting Time	Time Consuming	Backup to Remote Simultaneously	Backup Status	Operation
■	ConfigDB	ConfigDatabase_20190924114303_Auto	2019-09-24 11:43:33	0s	No	Success	
■	ConfigDB	ConfigDatabase_20190924114303_Auto	2019-09-24 11:43:10	0s	No	Success	
■	ConfigDB	configDatabase_20190808230900_Auto	2019-08-08 02:30:00	0s	No	Backup in Progress	

- Currently, only the configDB data restore is supported. The configuration file restore needs to be manually replaced.
- In the backed up record, the backup record corresponding to the restore time point can be selected. Click the [Restore] button to restore the configDB data.
- HotDB Management automatically backs up the current configDB before restore to ensure available latest backup can be restored after data misoperation. The

automatically backed up file restored is automatically named “backup time + restoreBackup”.

14.7. Parameter configuration

“Parameter Configuration” is a function of Management Platform to provide users with visual configuration compute node server.xml parameter.

DR mode explanation: when the DR mode is enabled, please refer to the chapter "Parameter configuration" in the [Distributed Transactional Database HotDB Server - Cross-IDC Disaster Recovery Function Specification](#) for the relevant logical explanations of the parameter configuration.

Function entry: log in to the management platform, enter the “Configuration -> Parameter configuration” page.

14.7.1. Basic functions and notes



Type	parameter name	Description of parameter	parameter value	The way to work	Status	Operation
Basic configuration	clusterName	cluster group name	Cluster	Restart the service	Worked	
Basic configuration	serverPort	Service Port	3323	Restart the service	Worked	
Basic configuration	managerPort	Management Port	3325	Restart the service	Worked	

Through the compute node drop-down box, you can view all the compute nodes in the current cluster. The current active compute node is displayed at the top of the drop-down box, format: (IP the current active). And other compute nodes are displayed in the drop-down box in turn, format: compute node name (IP). The synchronization box "Slave compute node automatically synchronized" is checked by default. Adding or modifying parameters will be automatically synchronized to other slave compute nodes (no synchronization in single-node mode), including seven parameters [haMode: DR mode], [idcId: ID of IDC], [idcNodeHost: master compute node information of the corresponding IDC], [ServerId: cluster node number], [clusterHost: IP where the

compute node is located], [hsaState: configuration of master/slave roles in high availability mode of compute node], [HaNodeHost: connection information of the current active compute node in the high availability mode of compute node], which are controlled by respective compute nodes and will not be modified synchronously.

For the list, you can search by parameter name and parameter description, or filter by "Basic configuration, High availability setting, Database features, SQL grammar and function, Database performance, Database operation and maintenance", as shown in the following figure:

The screenshot shows the 'Parameter Configuration' interface. The 'Compute Node' dropdown is set to 'HotDB_01 (192.168.240.150 Current Master)'. The 'Type' dropdown is set to 'Select All'. The table lists the following parameters:

Type	parameter name	Description of parameter	parameter value	The way to work	Status	Operation
Basic configuration	clusterName	cluster group name	Cluster	Restart the service	Worked	
High Availability Setting	serverPort	Service Port	3323	Restart the service	Worked	
Database Features	managerPort	Management Port	3325	Restart the service	Worked	
SQL grammar and function	url	Master ConfigDB Address	jdbc:mysql://192.168.240.159:3306/hotdb_config	Reload	Worked	
Database performance	username	Master ConfigDB Username	hotdb_config	Reload	Worked	
Database operation and maintenance						

At the same time, parameters can be modified, reset, batch modified, and batch reset. After these operations, Status of parameter will not be "Worked" immediately. You can make it "Work" through reload or restarting the service (refer to the description of "The way to work")

The screenshot shows the 'Parameter Configuration' interface. The 'Compute Node' dropdown is set to 'HotDB_01 (192.168.240.150 Current Master)'. The 'Type' dropdown is set to 'auto'. The table lists the following parameters:

Type	parameter name	Description of parameter	parameter value	The way to work	Status	Operation
Basic configuration	heartbeatPeriod	Heartbeat period	2 (s)	Restart the service	not worked	
Database features	autoincrement	v2.5.4 below: whether to adopt the global auto-increment sequence; v2.5.4 and above: the global auto-increment sequence	Enable global auto-increment	Reload	not worked	
Basic configuration	clusterName	cluster group name	HotDB-Cluster222	Restart the service	Worked	
Basic configuration	serverPort	Service Port	3323	Restart the service	Worked	
Basic configuration	managerPort	Management Port	3325	Restart the service	Worked	

Click the hyperlink of parameter name, the page will jump to the "Parameter Details Explanation" page and navigate to the parameter, which gives a detailed description of the parameter.

Parameter Details Explanation							
Parameter name		Description of parameter	Default value	Min value	Max value	The way to work	Common or not
Basic configuration	clusterName	cluster group name	HotDB-Cluster	/	/	Restart the service	Yes
Basic configuration	serverPort	Service Port	5323	1	65535	Restart the service	Yes
Basic configuration	managerPort	Management Port	5325	1	65535	Restart the service	Yes
Basic configuration	url	Master ConfigDB Address	jdbc:mysql://192.168.200.1:3306/hotdb_config	/	/	Reload	Yes
Basic configuration	username	Master ConfigDB Username	hotdb_config	/	/	Reload	Yes
Basic configuration	password	Master ConfigDB Password	hotdb_config	/	/	Reload	Yes
Basic configuration	bakUrl	Slave ConfigDB Address	jdbc:mysql://192.168.200.1:3306/hotdb_config	/	/	Reload	Yes
Basic configuration	bakUsername	Slave ConfigDB Username	hotdb_config	/	/	Reload	Yes
Basic configuration	bakPassword	Slave ConfigDB Password	hotdb_config	/	/	Reload	Yes

Click the "Add parameters" button at the upper right corner to jump to the Add parameters page. It displays all the uncommon parameters of the compute node, which need to be modified and added according to the actual need.

Add parameters					
<small>① The following parameters are not commonly used, and modifications by users are generally not recommended. If necessary, users can check and set the parameters before clicking [OK] and adding them to the common parameters.</small>					
Type	Parameter name	Description of parameter	parameter value	The way to work	
High Availability Setting	clusterStartedPacketTimeoutMs	Cluster started broadcast packet expiration time	5000 (ms)	Reload	
High Availability Setting	clusterHeartbeatTimeoutMs	Cluster heartbeat timeout	5000 (ms)	Reload	
High Availability Setting	clusterPacketTimeoutMs	Cluster communication packet timeout	5000 (ms)	Reload	
High Availability Setting	clusterElectionTimeoutMs	Cluster election timeout	2000 (ms)	Reload	

Special notes:

- The virtual IP parameter Keepalived is recommended to be configured when the cluster mode is the master/slave compute nodes (ignored in a single compute node), and it needs to be current actual.
- When some parameters are modified, there will be a suspended prompt message, as follows:

axIdleTransactionTimeout -> 0 means never timeout.

statisticsUpdatePeriod -> 0 means no data persistence.

dropTableRetentionTime -> 0 means no retention.

deadlockCheckPeriod -> 0 means not enable.

maxUserConnections -> 0 means unlimited.

VIP -> No filling or the format is not IPv4 means that this item is empty.

- For frontConnectionTrxIsoLevel, if enableXA is set to true, the parameter drop-down box will be grayed and the option READ UNCOMMITTED will not be available.
- If there is a compute node failure, the failed compute node will not be displayed in the compute node selection box.
- In the DR mode, idcId and idcNodeHost need to be configured. idcId configures the ID of IDC. 1 is for the master center and 2 is for the DR center. 1 is set by default.
- If the DR mode is not enabled in haMode, “master/slave” will be displayed when the compute node is a single compute node or a master/slave compute node, and “cluster” will be displayed when it is a multi-node.

14.7.2. Enable master configDB

When the configDB mode used by compute node cluster is master/slave or master-master mode, if the master configDB fails, the compute node cluster will automatically switch the configDB connection to the master/slave configDB. At this time, if the master configDB is restored manually and started normally, the compute node cluster will not automatically use the master configDB, but the master configDB shall be re-enabled according to the following operations.

1. After the failure of the master ConfigDB, the Parameter Configuration page is shown as follows:

Type	parameter name	Description of parameter	parameter value	The way to work	Status	Operation
Basic configuration	clusterName	cluster group name	HotDB-Cluster222	Restart the service	Worked	
Basic configuration	serverPort	Service Port	3323	Restart the service	Worked	
Basic configuration	managerPort	Management Port	3325	Restart the service	Worked	
Basic configuration	url	Master ConfigDB Address	jdbc:mysql://192.168.210.45:3310/hotdb_config_255ha	Reload	Worked	<input checked="" type="checkbox"/>
Basic configuration	username	Master ConfigDB Username	hotdb_config	Reload	Worked	
Basic configuration	password	Master ConfigDB Password	hotdb_config	Reload	Worked	
Basic configuration	bkurl	Slave ConfigDB Address	jdbc:mysql://192.168.210.46:3310/hotdb_config_255ha	Reload	Worked	

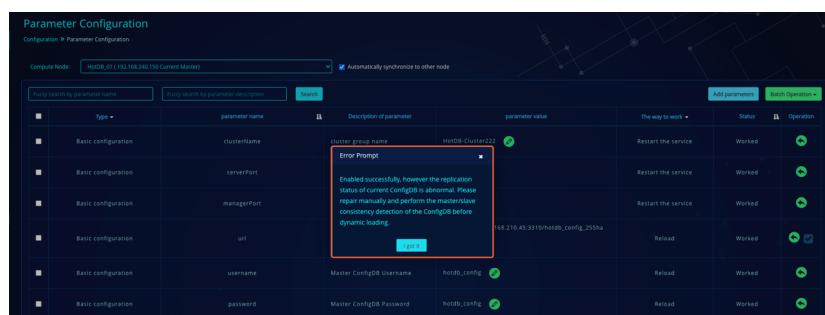
2. If the master configDB is restored and consistent with the slave configDB data, the master configDB can be enabled by clicking the enable button on the compute node Configuration page.

3. After clicking the button, click the [Reload] button to re-enable the master configDB.

Parameter Configuration						
Computer Node		Parameter Name		Parameter Value		
Type	parameter name	Description of parameter	parameter value	The way to work	Status	Operation
Basic configuration	clusterName	cluster group name	HotDB-Cluster222	Restart the service	Worked	
Basic configuration	serverPort	Service Port	3323	Restart the service	Worked	
Basic configuration	managerPort	Management Port	3325	Restart the service	Worked	
Basic configuration	url	Master ConfigDB Address	jdbc:mysql://192.168.210.45:3310/hotdb_config_255ha	Reload	Worked	
Basic configuration	username	Master ConfigDB Username	hotdb_config	Reload	Worked	
Basic configuration	password	Master ConfigDB Password	hotdb_config	Reload	Worked	

For the DR mode, attention should be paid to:

- When the DR center is the current standby IDC and the master configDB fails, the compute node will set both the master-slave ConfigDB of the DR center to the unavailable status.
- When the DR center is the current standby IDC, it is necessary to confirm that the current master ConfigDB is available when enabling the slave ConfigDB of the DR center. Otherwise, the slave ConfigDB of the DR center cannot be enabled, that is, the master ConfigDB of the DR center must be enabled before enabling the slave ConfigDB of the DR center.
- If you want to enable any ConfigDB in two IDCs, you need to ensure that the replication status of the current IDC and between the IDC is normal. If any replication status is abnormal, dynamic loading will succeed with alert prompt, as follows:

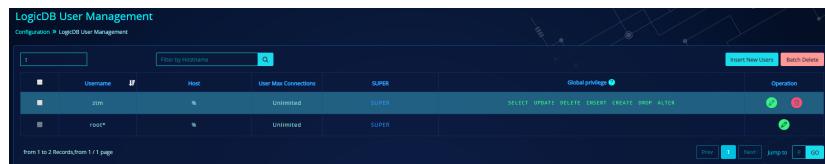


Type	parameter name	Description of parameter	parameter value	The way to work	Status	Operation
Basic configuration	cluster_ip	cluster_ip: name	HotDB-Cluster22	Restart the service	Worked	
Basic configuration	serverPort			Restart the service	Worked	
Basic configuration	managerPort			Restart the service	Worked	
Basic configuration	url		192.168.45.33:10/hotdb_config_255ha	Reload	Worked	
Basic configuration	username	Master ConfigDB Username	hotdb_config	Reload	Worked	
Basic configuration	password	Master ConfigDB Password	hotdb_config	Reload	Worked	

14.8. Database user management

HotDB Server controls compute node user privileges to the table level, and has SELECT, UPDATE, DELETE, INSERT, CREATE, DROP, ALTER privileges for logicDB or table. The specific privileges are given by HotDB Management users.

14.8.1. Query by username

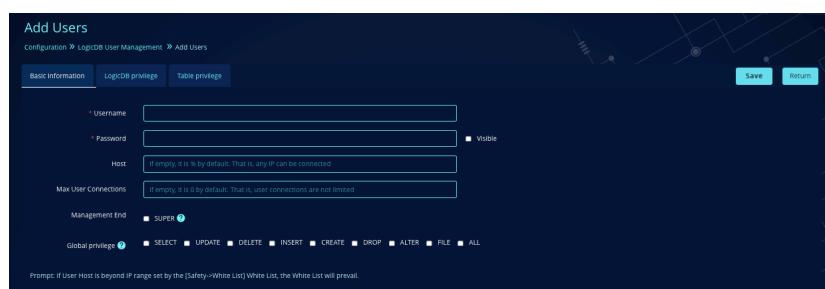


Username	Host	User Max Connections	SUPER	Global privilege	Operation
zlim	%	Unlimited	SUPER	SUPER	
root*	%	Unlimited	SUPER	SUPER	

- The page displays the compute node database user records added, which support fuzzy search by username or hostname.
- The “root” on the page is the built-in user when the HotDB Management installation is initialized, which cannot be deleted (HotDB Management uses root to connect and access the compute node).

14.8.2. Add users

Click the [Add Users] button to enter the Add User information page. There are three modules on the Add User information page: Basic Information, logicDB privilege and Table level privilege.



Prompt: If User Host is beyond IP range set by the [Safety->White List] White List, the White List will prevail.

(1) Basic Information: including required items “Username”, “Password”, optional items “Host”, “Max User Connections”, “super privilege” and “Global privilege”

- “Username” and “Password” are the database account information used when logging into the compute node. “Username” shall not be repeated and in Chinese. “Password” shall meet the requirements.
- “Host” is an optional item. When it is null, it is “%” by default. That is, any IP can be connected. When the white list constraint is currently enabled, and Host User is beyond IP range set by “Security -> [White List](#)”, the White List will prevail.
- “Max User Connections” is an optional item. When it is null, it is “0” by default. That is, user connections are not limited. For the maximum connections for all users, the “Front-end Max Connections” will prevail.
- super privilege is the user’s privilege for management port login (3325 by default).
- Global privilege is an optional item. If user set global privilege, the user will have the selected operation privileges of all objects under all logicDBs. For example, if global privileges SELECT, UPDATE, INSERT, CREATE are checked, current users can perform S/U/I/C operations on all logicDBs and tables after saving.
- Username and host can determine the uniqueness of user, that is, username + host represents an independent user. This rule is consistent with MySQL privilege system.



(II) LogicDB privilege: Select the corresponding logicDB to set the corresponding privileges, or create a new logicDB and set the privilege.

- If global privilege is set in the basic information, the relevant privileges at the logicDB level can not be changed with the global privilege, and the cursor focus will prompt “Inherited from global privilege”.
- When selecting or adding a logicDB to assign privilege, the page automatically checks the basic privilege item “S/U/D/I”.
- Check the “ALL” privilege to perform “S/U/D/I/C/D/A” operation on the logicDB. If it needs to adjust the privilege of the logicDB that has been given the “ALL” privilege later, the ALL option shall be first unchecked.
- If a new logicDB is added and the corresponding privileges are set, the new logicDB information is not synchronized to the actual logicDB table, and is only saved as a pre-configured privilege information in the configDB.
- LogicDB deletion only deletes the privilege record corresponding to the current logicDB, and does not affect the actual logicDB.

Note: Changing the logicDB name may affect the logicDB privileges that some users have added and invalidate table privilege configuration. Therefore, the logicDB name change by logicDB list shall be used with caution.

(III) Table privilege: User table-level privileges are divided into two parts: table-level privilege allowed and table-level privilege denied. The privilege allowed is the privilege of users to perform table operations. The privilege denied is the privilege not given to

users to perform table operations.

➤ **Table privilege Allowed**

Select existing tables to configure privileges or add new table configuration and assign privileges. Select the logicDB and then select the table to be configured from the drop-down box or enter the name of new table. When clicking [Confirm], the page generates a configuration record.

- If the current logicDB has set privileges or global privileges, the table-related privileges cannot be changed with the global privilege, and the cursor focus will prompt “Inherited from global privilege”.
- After configuring a table privilege record, the page automatically checks the basic privilege item “S/U/D/I”.
- Check the “ALL” privilege to perform “S/U/D/I/C/D/A” operation on the table. If it needs to adjust the privilege of the table that has been given the “ALL” privilege, the “ALL” option shall be first unchecked.
- If a new table is added and the corresponding privileges are set, the new table is not synchronized to the actual table configuration and is only saved as a pre-configured information. The corresponding privileges are directly matched after the table is created.
- Table deletion only deletes the privilege record corresponding to the current table, and does not affect the actual table configuration.

➤ **Table privilege Denied**

Configuration of table privilege denied is consistent with configuration of table privilege allowed. Table privilege denied is greater than global privilege, logicDB privilege and table-level privilege allowed.

- Table privilege denied is independent of global privilege and logicDB

privileges, and no privileges are checked by default.

- If a new table is used to set corresponding privileges, the new table does not synchronize to the real table configuration, but only serves as a configuration information of pre-rejection privileges. After the table is created, the corresponding privileges are matched directly.
- Table deletion only deletes the denial of privilege records corresponding to the current table, and has no effect on the real table configuration.

Privilege matching note:

- When logging in to the server to read the user tables, they are first sorted by the most specific Host value (hostname and IP are the most specific), and the entries with the same Host value are matched by the most specific username first, for example, adding two users with the same username and different Host values, as shown in the following figure:

LogicDB User Management						
Configuration > LogicDB User Management						
	Username	Host	User Max Connections	SUPER	Global privilege	Operation
■	test	%	Unlimited	SUPER	SELECT UPDATE DELETE INSERT CREATE DROP ALTER	
■	test	192.168.200.%	Unlimited	SUPER	SELECT UPDATE DELETE INSERT	

- User test logs in through host 192.168.200.51 and performs INSERT/ALTER operation. Because the most specific Host is matched, the ALTER unprivileged operation is denied, shown in the following figure:

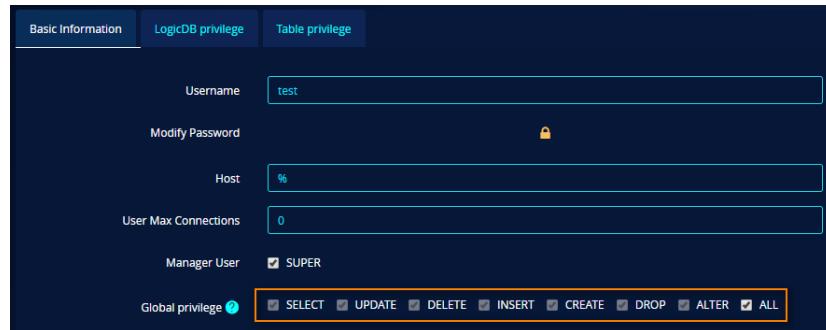
```
test@192.168.220.104 : TEST_ZY 08:54:51> insert into join_cross_a_jwy(adnid) value
(101);

Query OK, 1 row affected (0.05 sec)

test@192.168.220.104 : TEST_ZY 08:56:11> alter table join_cross_a_jwy add column apassword int after
aname;

ERROR 1045 (HY000): [ALTER] command denied to user 'test' to logic database 'TEST_ZY'
```

- The configured table-level privilege allowed do not conflict with the global, logicDB, and table-level privilege allowed, and the priority is higher than all. For example, the test user sets the global privilege ALL, as shown in the following figure:



Basic Information LogicDB privilege Table privilege

Username: test

Modify Password:

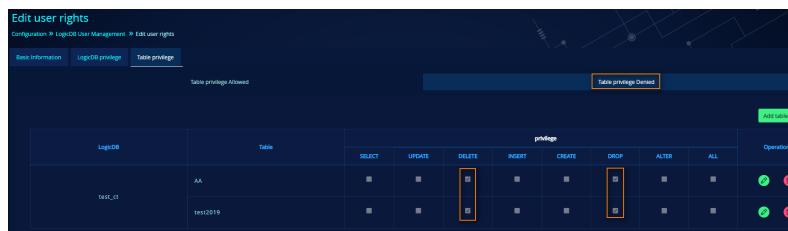
Host: %

User Max Connections: 0

Manager User: SUPER

Global privilege: SELECT UPDATE DELETE INSERT CREATE DROP ALTER ALL

- Test user sets test_ct.test_temp table privileges denied DELETE, DROP



Edit user rights

Configuration > LogicDB User Management > Edit user rights

Basic Information LogicDB privilege Table privilege

Table privilege Allowed

LogDB	Table	privilege	Operation
		SELECT UPDATE DELETE INSERT CREATE DROP ALTER ALL	
test_ct	AA	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
	test2019	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	

Add value

- The user test logs into the service port to perform DELETE and DROP operations on the test_temp table, which are denied. The privilege matching is as follows:

```
test@192.168.200.51 : (none) 08:53:25> use test_ct
Database changed

test@192.168.200.51 : test_ct 08:53:32> insert into test2019(a) values(30);
Query OK, 1 row affected (0.09 sec)

test@192.168.200.51 : test_ct 08:53:51> delete from test2019 where a=30;
```

ERROR 1045 (HY000): [DELETE] command refused to user 'test' to table 'TEST2019' of logic database 'TEST_CT'

14.9. Server

Server menu mainly provides server SSH information for users to configure all components in the cluster on HotDB Management to facilitate HotDB Management to monitor the server status. In addition, it also supports adding servers outside the cluster to HotDB Management for monitoring.

Server					
Configuration > Server					
Hostname (multiple choices)		SSH Connection Status (m.)		Operation	
Hostname	Service Program Association	SSH Connection Status	Username	Operation	
192.168.210.37	Data Source	Normal	root	Configuration SSH Stop Monitoring Remove	
192.168.210.41	192.168.210.41/33027/gny2531 192.168.210.41/33027/gny2532	Normal	root	Configuration SSH Stop Monitoring Remove	
192.168.210.42	192.168.210.42/33027/gny2531 192.168.210.42/33027/gny2532	Normal	root	Configuration SSH Stop Monitoring Remove	
192.168.210.43	192.168.210.43/3308/gny22	Normal	root	Configuration SSH Stop Monitoring Remove	
192.168.210.44	192.168.210.44/3308/gny991431	Normal	root	Configuration SSH Stop Monitoring Remove	
192.168.210.49		Normal	root	Configuration SSH Stop Monitoring Remove	
192.168.210.70		Normal	root	Configuration SSH Stop Monitoring Remove	

14.9.1. Obtain server IP automatically

The server page automatically displays the server IP of all components in the cluster group and the associated service programs in the server.

(I) Single node cluster mode

Server					
Configuration > Server					
Hostname (multiple choices)		SSH Connection Status (m.)		Operation	
Hostname	Service Program Association	SSH Connection Status	Username	Operation	
192.168.210.68		Not Configured	root	Configuration SSH Start Monitoring Remove	
192.168.210.69		Not Configured	root	Configuration SSH Start Monitoring Remove	
192.168.220.140	Compute Node HotDB_01/192.168.220.140/5555 ConfigDB	Not Configured	root	Configuration SSH Start Monitoring Remove	
192.168.220.149	192.168.220.149/3306/node0_config_245 Data Source 192.168.220.149/3309/db245_01 192.168.220.149/3309/db245_02 Data Source 192.168.220.150/3309/db245_03 192.168.220.150/3309/db245_04	Not Configured	root	Configuration SSH Start Monitoring Remove	

HotDB Management automatically obtains the server IP information of the compute node, data source, and configDB components.

(II) Master/slave node mode cluster

Server					
Configuration > Server					
Hostname multiple choices		SSH Connection Status Inc.		Operation	
Hostname	Service Program Association	SSH Connection Status	Username	Operation	
192.168.210.42	Data Source 192.168.210.42/21307/phy1418	Not Configured	root	[Configuration Stop] [Start Monitoring] [Remove]	
192.168.210.66	Data Source 192.168.210.66/3307/monitor	Not Configured	root	[Configuration Stop] [Start Monitoring] [Remove]	
192.168.210.41	Data Source 192.168.210.41/3307/phy4970 192.168.210.41/3308/phy4970	Normal	root	[Configuration Stop] [Stop Monitoring] [Remove]	
192.168.210.42	Data Source 192.168.210.42/3308/phy4970 192.168.210.42/3309/phy4970	Normal	root	[Configuration Stop] [Stop Monitoring] [Remove]	
192.168.210.43	Data Source 192.168.210.43/3309/phy4970	Normal	root	[Configuration Stop] [Stop Monitoring] [Remove]	
192.168.210.44	Data Source 192.168.210.44/3309/phy4970	Normal	root	[Configuration Stop] [Stop Monitoring] [Remove]	
192.168.210.49	Compute Node Master@192.168.210.49/33253 keepalived vip@192.168.210.214	Normal	root	[Configuration Stop] [Stop Monitoring] [Remove]	
192.168.210.70	Compute Node Backup@192.168.210.70/33253 ConfigDB 192.168.210.70/3307/mvdb_config_253_en keepalived vip@192.168.210.214	Normal	root	[Configuration Stop] [Stop Monitoring] [Remove]	

HotDB Management automatically obtains the server IP information of the compute node, data source, configDB and keepalived components.

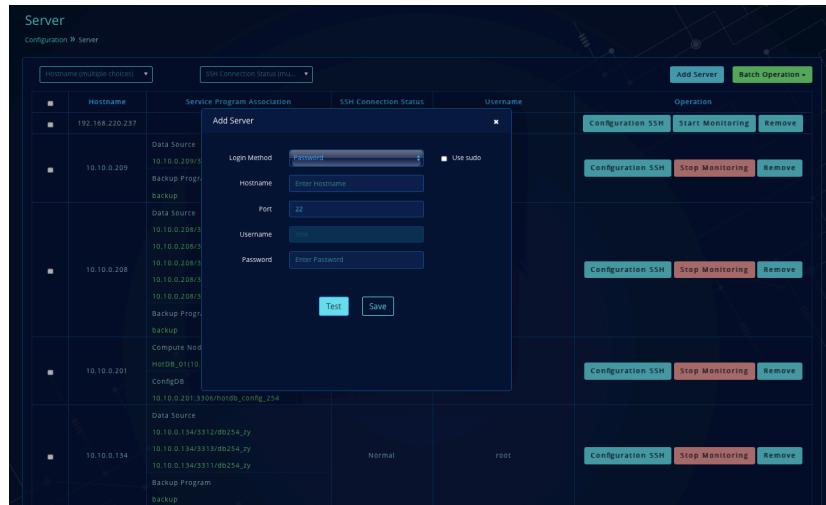
(III) Multi-node mode cluster

Server					
Configuration > Server					
Hostname multiple choices		SSH Connection Status Inc.		Operation	
Hostname	Service Program Association	SSH Connection Status	Username	Operation	
192.168.210.39	Compute Node HotDB_39@192.168.210.39/33253	Not Configured	root	[Configuration Stop] [Start Monitoring] [Remove]	
192.168.210.31	ConfigDB 192.168.210.31/3307/mvdb_config_en_test353	Not Configured	root	[Configuration Stop] [Start Monitoring] [Remove]	
192.168.210.32	Compute Node HotDB_31@192.168.210.31/33253	Not Configured	root	[Configuration Stop] [Start Monitoring] [Remove]	
192.168.210.41	Data Source 192.168.210.41/3307/phy253 192.168.210.41/3308/phy253 192.168.210.41/3309/phy253	Not Configured	root	[Configuration Stop] [Start Monitoring] [Remove]	
192.168.210.43	Data Source 192.168.210.43/3308/phy379	Not Configured	root	[Configuration Stop] [Start Monitoring] [Remove]	
192.168.210.44	Data Source 192.168.210.44/3309/phy379	Not Configured	root	[Configuration Stop] [Start Monitoring] [Remove]	
192.168.210.45	Data Source 192.168.210.45/3309/phy379	Not Configured	root	[Configuration Stop] [Start Monitoring] [Remove]	
192.168.210.34	LVS	Normal	root	[Configuration Stop] [Stop Monitoring] [Remove]	
192.168.210.42	Data Source 192.168.210.42/3308/phy253	Normal	root	[Configuration Stop] [Start Monitoring] [Remove]	

HotDB Management automatically obtains the server IP information of the compute node, data source, and configDB components. If the cluster is manually added, a prompt appears at the bottom of the page: The program cannot obtain the server IP of LVS components which shall be configured by the user in [Add Server].

14.9.2. Add server

Click the [Add Server] button to add a server outside the cluster.

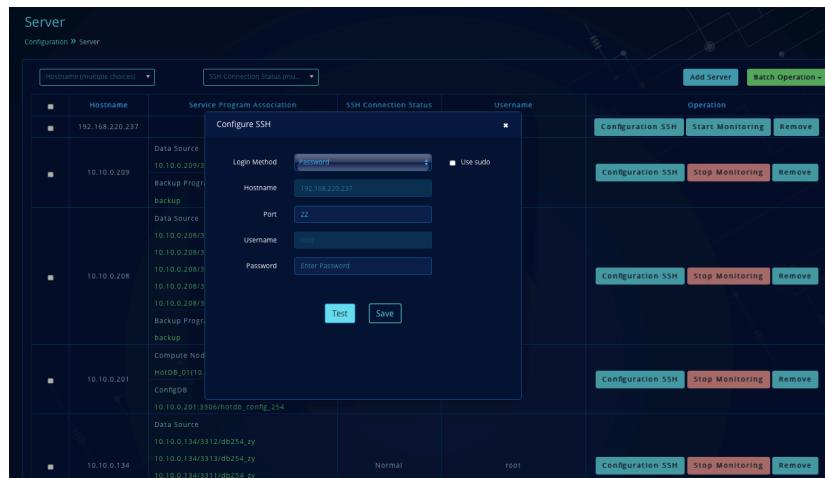


- Login Method: Password and Sign in without password. If “Sign in without password” is selected, it needs to be set in advance. For details, refer to the “Instructions for Sign in without Password” module of the *Distributed Transactional Database HotDB Server [Installation and Deployment] Function Manual*.
- Hostname: Server ip.
- Port: 22 by default.
- Username: The server login username.

- Password: The server login password; it is gray when “Sign in without password” is selected.
- LVS Server: In case of “Yes”, click the [Test] button to check whether the LVS service in the server is normal. After the test is passed, the saving can be successful. This option is only for multi-compute node cluster environments, and is not displayed for single compute node and master/slave compute node.
- Multiple servers can also be added quickly by selecting “Batch Operation -> Batch Add”.

14.9.3. Configure SSH

By default, the SSH connection status of cluster component server is “Not Connected”. Users need to manually configure SSH information to HotDB Management. Monitoring will be automatically turned on when the configuration is complete.



- Configure SSH information by simply filling in: Port (22 by default), Username and Password (not applicable for Sign in without password).

- When selecting “Yes” for LVS Server, the cluster component LVS exists in the server.
- The configured server automatically starts monitoring (the monitoring script is sent by HotDB Management to the server that starts monitoring).

14.9.4. Other description

- Click [Remove] to delete the added server record. If the removed record is the server IP of the cluster component, the configuration SSH information shall be removed.
- Click [Stop Monitoring] to stop regularly executing the monitoring script in the server, but this operation will make HotDB Management unable to grasp the health status of cluster server, which causes certain hidden dangers.
- The servers that “Stop Monitoring” do not display the server resource status in “Monitoring -> Monitoring Panel -> [Other Servers](#)”. The servers that are not monitored in the “Monitoring -> [Physical Topological Graph](#)” function cannot view the server details.

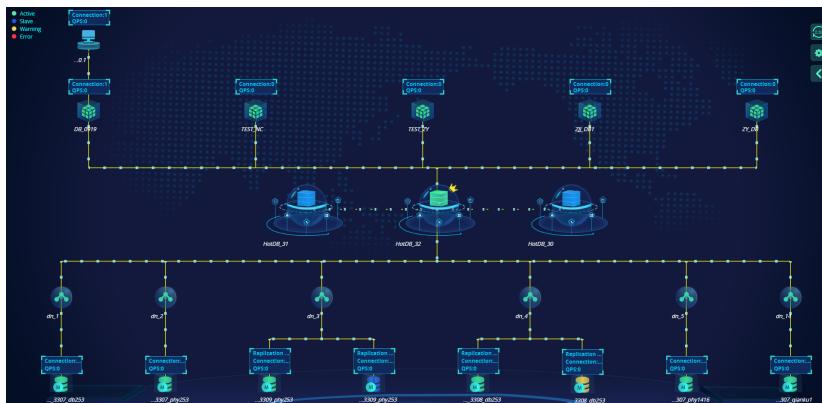
15. Monitoring

15.1. Logic Topological Graph

HotDB Management fully displays the physical and logic components such as front-end application, logicDB, compute node, data node, data source in the cluster in a visual mode. The QPS and connections on the component is dynamically generated through the front-end application connection pool and the back-end database connection pool information. “Logic Topological Graph” enables users to quickly understand the running status of the whole cluster and help users achieve efficient operation and maintenance.

DR mode explanation: when the DR mode is enabled, please refer to the chapter "Logic topological graph" in the [Distributed Transactional Database HotDB Server - Cross-IDC Disaster Recovery Function Specification](#) for the relevant logical explanations of the logic topological graph.

15.1.1. Topological graph component description



The topological graph consists of five layers of components from top to bottom: front-end application, logicDB, compute node, data node, and data source.

(I) Front-end application

The front-end application layer is the front-end application client that connects to the compute node. The application connects to the specified logicDB through IP, port, and

user password (the connection method is consistent with the MySQL connection), that is, the related connection information can be seen in the topological graph. If the real-time connections and QPS of the front-end application exceed the set threshold, the topological graph will display a warning with an orange up arrow.

(II) LogicDB

- LogicDB layer is physically a virtual layer and a virtual concept of the HotDB Server product. The topological graph allows to view all logicDBs that exist in the whole cluster.
- The logicDB icon displays the related “Connection” and “QPS”.
- “Connection” is the sum of all front-end application connections of the current logicDB.
- “QPS” is the sum of all front-end application QPSs of the connected logicDB (the logicDB QPS occasionally has a single digit deviation from the total number).
- When “QPS” and “Connection” exceed the set threshold, the page will display a warning with an orange arrow.

(III) Compute node

- The compute node is the core component of the whole cluster, providing the underlying computing route query service for data.
- The topological graph displays the corresponding number of compute node icons according to the cluster mode. One is displayed in single node mode, two are displayed in master/slave mode, and the multi-node mode is based on the number of compute nodes.
- Green represents the current master compute node and blue represents the current slave compute node by default. Red indicates that the compute node is abnormal and cannot be connected, and orange indicates that the compute node parameter exceeds the set threshold.
- A cluster in master/slave or multi-node mode has a “crown” icon on the current master compute node to represent the master of current cluster.
- When the mouse cursor is hovering over the compute node icon, the back-end

connections, direct memory usage, front-end connections, heap memory usage, back-end inflow rate, back-end outflow rate, front-end inflow rate, front-end outflow rate and QPS are displayed. When the data exceeds the warning limit, it will be marked with an orange up arrow.

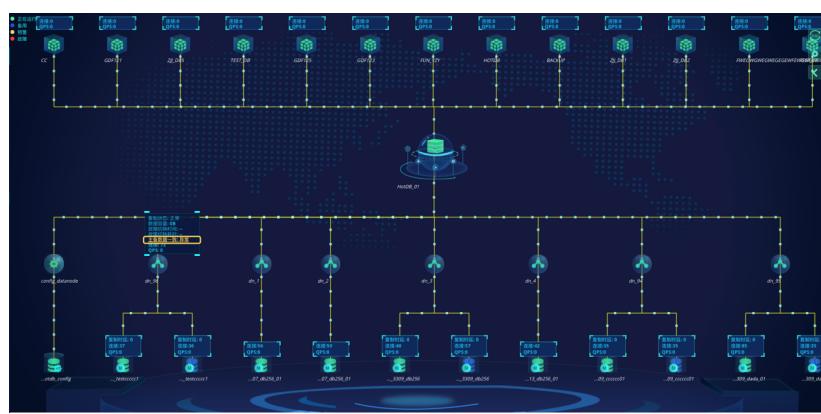
(IV) Data node

- The data node is a virtual concept of the HotDB Server, which does not actually exist at the physical level.
- The data node can manage a group of data sources with replication relations for easy viewing and later operation and maintenance.
- Data node information: “Replication Status” is the replication status parameter displayed on the master-master and master/slave data source. The replication status includes: Normal, Abnormal and Unknown. The replication status is consistent with the “Master/Slave Status” on the Node Management page.
- When the replication status is Unknown, the slave data source is displayed in yellow and blinks. Move the mouse cursor to display the Unknown cause which shall be consistent with the cause prompted in the [Master/Slave Status](#) of node management. There are four cases of Unknown: Data source cannot be connected, data source privileges are insufficient, detection is periodical out (timeout time: 1 minute), and current node has no master/slave replication relation. In addition to, in case of master-master and slave, if the master_id is configured and the master/slave relation is not matched, the “Unknown” status is also displayed and it prompts that “The current node master/slave relation is inconsistent with the configuration”.
- Data node information: “Data Capacity” The data capacity is based on the current active master data capacity under the data node. That is, the current active master data volume = data capacity displayed by the data node. (The unit of data volume is represented by K, M, G). When the data volume reaches M, it is displayed by M.

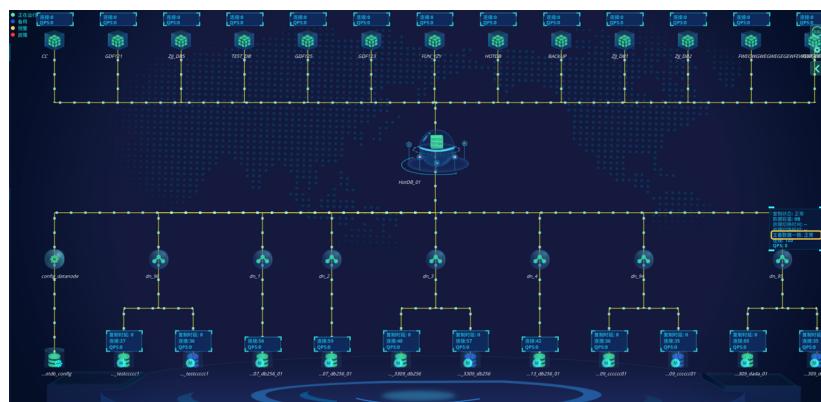
- Data node information: "Failover Time" is the time when the standby slave officially takes over the service.
- Data node information: "Failover Time" is the time consumed from the active master fails and the standby slave starts to wait for catching up with and then the connection is switched to the standby slave when the standby slave starts to provide the normal service. This parameter is displayed only when the switch is successful. If the replication is normal or the switch fails or the active master is restored during the switch, the parameter displays “- -” instead of the time. The switch time is displayed in ms, s, min and h. The time is displayed in min when it exceeds s.
- Data node information: "Master/slave Data Consistency" when the node type is master-master, master/slave, or one master with multiple slaves, whether the data and objects on multiple data sources are consistent will be identified. There are three values: "--", "normal" and "abnormal", which are displayed according to the latest detection results of "Detection - > Master/slave Data Consistency Detection".
 - 1) When the master/slave data consistency detection is not performed in the selected node, the master/slave data consistency will be shown as "--"



- 2) When the detection result of the selected node is "unable to detect" or "inconsistent": the master/slave data consistency will be shown as "abnormal", with a hyperlink in orange. Click the hyperlink to jump to the details page of the master/ slave consistency detection result.



3) When the detection result of the selected node is "consistent": the master/slave data consistency will be shown as "normal".



4) When the detection result of the selected node is "consistent", with a prompt "There are conditions which cannot be detected." (i.e. multiple detection nodes): the master/slave data consistency will be shown according to the actual detection results. For the "consistent" nodes, it will be shown as "normal", and for the nodes that cannot be detected, it will be shown as "abnormal" with a hyperlink in orange.

- Data node information "connections": obtained by adding the connections on all data sources under the data node.
- Data node information "QPS": obtained by adding QPS on all data sources under

the data node.

(V) Data source

- It is a real storage layer of business data consisting of MySQL instances.
- Green “M” represents the current master data source, blue “S” represents the slave data source, blue “M” represents the standby master, and “MGR” represents the MGR type data source.
- Red icon indicates that there is an error. Move the mouse cursor into the faulty data source icon to display the error cause. Orange indicates that there is a replication latency or the last data source under the data node is unavailable.
- The data source displays the “Replication latency” (the data source with master-slave or master-master relation is displayed, and the delayed data is obtained from the display slave status), “Connection” (generated dynamically according to the back-end MySQL connection pool) and “QPS”

(VI) ConfigDB

- The ConfigDB components of the compute nodes in the cluster are always displayed on the left of the storage layer.
-  is a non-status icon, which connects one or two ConfigDBs , respectively representing a single node ConfigDB and a master-master ConfigDB. In single-IDC mode, if three or more ConfigDBs are connected, it represents the ConfigDB in MGR mode.  will be in orange when all ConfigDBs are not available.
- Similar to the data source, icon of ConfigDB in red means a failure exists; moving the cursor over the red icon, the failure cause can be displayed. Orange means an abnormal replication status exists, moving the cursor over the orange icon, the abnormality cause can be displayed.
- The monitoring information of "Replication latency" is displayed in the ConfigDB. Similar to the data source, the alert threshold of replication latency can be set under ConfigDB module in “Setting → [Topological Graph Alert Setting](#)”.

Other description

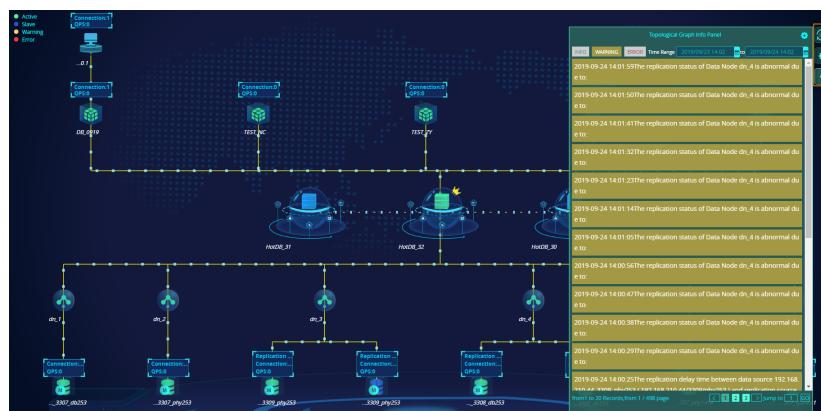
For more details about the components, please refer to the Distributed Transactional Database HotDB Server [Glossary] Function Manual.

The threshold value of the component display parameter alert information in the topological graph can be configured in “Setting —> Topological Graph Alert Setting”.

The data node icon can directly execute the master/slave switch by right clicking. The switching logic is the same as "Node management —> master/slave switch". (there is no such operation entry on the single-node page or data node page of MGR type)

The data source icon can quickly replicate connection information of the data source by right clicking, such as mysql -uhotdb_datasource -p -P3306 -h192.168.220.232 -Ddb05. (the connection password is empty due to security issues).

15.1.2. Interface adjustment function



(I) Visual switching

The topological graph can be switched to “2.5D” visual effect through the [2.5D] button on the interface, and can be switched back to normal visual effect by clicking the [2D] button.

(II) Topological graph setting

“QPS” and “Connection” information of components can be hidden or displayed.

If there are too many logicDBs on the topological graph page, the logicDB Filter in the setting can be used for targeted viewing.

Because each component can be dragged in the “General View” of topological graph, in order to reposition the scrambled component, click [Reset Component Arrangement] to restore the position of each component.

(III) Topological Graph Info Panel

Move the mouse cursor into the [<] button to activate the Topological Graph Info Panel which mainly records the INFO (addition or deletion of page component), WARNING (information of component warning parameter exceeding the threshold) and ERROR (information appears when the component is abnormal) in the topological graph.

The information recorded in the Topological Graph Info Panel cannot be deleted manually. However, the window period (local retention time) of the recorded information can be set using the [Setting] button in the upper right corner of the Info Panel. In order to reduce the excessive information at the WARNING level, the information can be set to be recorded only when the warning occurs for three consecutive times.

15.1.3. 2.5D topological graph

2.5D topological graph is a visual upgrade based on the original basic topological graph content. The component and component information displayed by this function are consistent with that of the above-mentioned “General View” topological graph, and the functions are similar.



Special description of 2.5D topological graph:

2.5D topology does not support arbitrary component dragging, and all component are fixed.

When the compute node fails, the failed compute node is displayed on the right of master compute node.

The display status of all application servers, logicDB, compute nodes, data nodes, and data sources on the page is consistent with that in normal mode.

The upper right corner switch, setting and information pop-up panel functions are consistent that in normal mode.

It supports zooming on the view by mouse cursor scrolling or page page zooming button, and supports page dragging.

15.2. Physical topological graph

Physical topological graph mainly displays the relation between cluster components and servers from the perspective of server. At the same time, the usage of server resources and the running health of cluster component services can be viewed. Before using, it is necessary to configure the available SSH connection information for the cluster server. Otherwise, only the relation between the current server and the cluster component can be viewed, and the status of the server and the component program cannot be viewed.

DR mode explanation: when the DR mode is enabled, please refer to the chapter "Physical topological graph" in the [Distributed Transactional Database HotDB Server - Cross-IDC Disaster Recovery Function Specification](#) for the relevant logical explanations of the physical topological graph.

(1) Overview of physical topological graph



Total servers: The total number of cluster servers (servers of associated cluster service programs) shown in the “Configuration - > [Server](#)” page list.

Server health status: The statuses include Normal, Warning and Error which are displayed in green, orange and red respectively in the statistics. The server error causes include: the server SSH connection information is incorrect, the server network connection is abnormal, and the server cannot connect normally; the server warning cause is: the server resource usage parameter value reaches the threshold in “Setting - Monitoring Panel Setting - [Compute Node/Other Server Resource Setting](#)”.

Total service programs: The total number of “Associated Service Program” displayed on the “Configuration -> [Server](#)” page.

Service program type: compute node, data source, configDB, keepalived (master/slave mode cluster), and LVS (multi-node mode cluster).

Service program health status: The running status of corresponding service program. Compute nodes statuses include Error (cannot be connected), Warning (exceed the threshold), and Normal (normal service operation). Other service programs have only two statuses: Normal (normal operation) and Error (abnormal operation). Move the mouse cursor into the error or abnormal status area to view the details.

(II) Physical Topological Graph page



Page description:

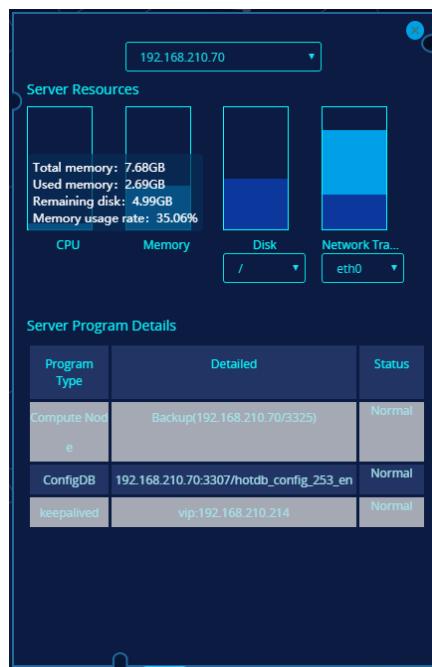
It displays the relation between servers and service programs. The server is represented by a square, each layer represents a server type, and the server IP is displayed in the lower right corner of the bottom layer. Normal, Warning and Error are represented by blue, orange and red squares respectively. Unconfigured servers are displayed as transparent.

The corresponding service programs on the server are all displayed in layers. The type and number of service programs are consistent with those shown in the overview.

The servers not configured or not enabled for monitoring on the “Configuration -> [Server](#)” page is transparent in the figure. Click on the server to pop up the prompt “SSH is not configured or the server is not enabled for monitoring”.

The servers that have been configured on the “Configuration -> [Server](#)” page and have unavailable SSH information due to SSH modification and change later are displayed as transparent in the figure. Click on the server to pop up the prompt “SSH information is unavailable”.

(III) Server details panel



Server Resource Details:

CPU usage rate: It displays the current CPU usage. Move the mouse cursor to display specific details. If the threshold is exceeded, a warning will appear in the prompt.

Memory usage rate: It displays the current memory. Move the mouse cursor to display specific details: (total memory, used memory, remaining memory, and memory usage rate); memory is uniformly displayed in GB. If the memory is a decimal, it shall be accurate to two decimal places.

Disk space usage rate: It displays the total disk space usage rate of the corresponding drive. Move the mouse cursor to display specific details: (drive name, total disk volume, used disk, remaining memory, and disk usage rate) are uniformly displayed in GB. The bottom drive can be switched to display the monitoring data of the corresponding drive;

Flow: It displays the current network traffic in/out. Move the mouse cursor to display specific details and the unit is KBps or MBps according to the actual situation.

Service Program Details:

It displays the components specifically installed in the server, including the current status of component.

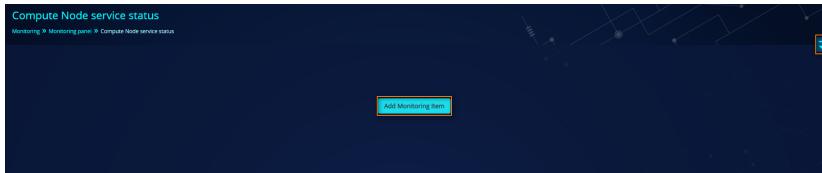
15.3. Monitoring panel

The monitoring panel provides users with the function of monitoring the parameters of compute nodes and servers, including: compute node service status, compute node throughout, compute node server resources, and other server resources.

Data collection description:

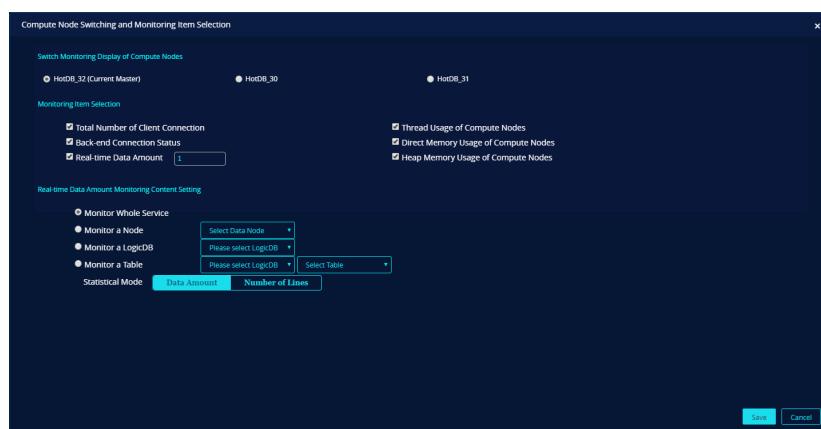
The monitoring panel displays the data collected within 24 hours (it shall be enlarged for viewing; the normal view only displays the data within half an hour). The system collects the data every 5 minutes and records it in the server memory deployed by HotDB management. If the distributed management platform restarts, the data stored in the memory will be cleared, that is, the data collected within 24 hours will be cleared.

15.3.1. Add and set monitoring item



Click [Add Monitoring Item] first when entering this function for the first time.

Click the [Switch] button to adjust the monitored items or select other compute nodes (multi-node mode cluster) to be displayed.



In multi-node mode cluster, “Switch Monitoring Display of Compute Nodes” can be selected to display the monitoring data of master compute node of the cluster by default. Single-node and master/slave node mode clusters can only view the monitoring data of the current master compute node.

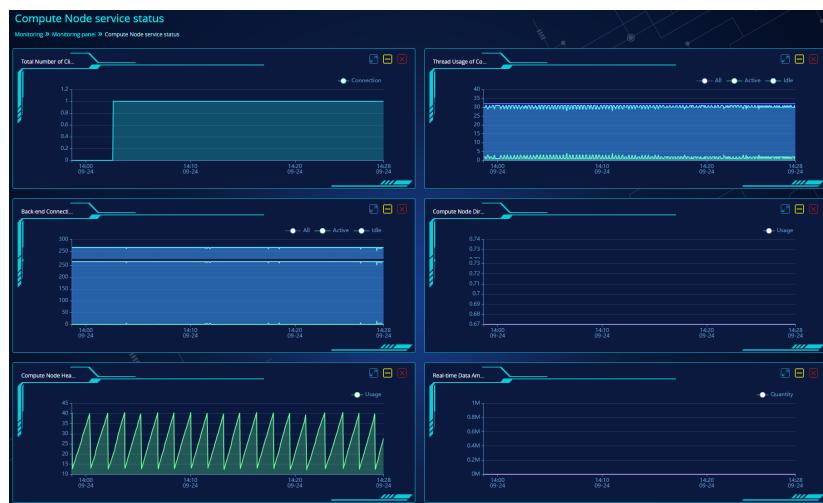
Users can check the monitoring items to be displayed according to the actual situation. All are checked by default. (unchecked will not affect the monitoring data)

Multiple real-time data amounts can be displayed according to the monitoring dimension setting. By default, the data amount of Monitor Whole Service, that is, the change of data amount of the whole cluster is displayed.

The settings of other monitoring items are similar to the above description, and the specific adjustment can refer to the above description.

15.3.2. Monitoring panel description

(I) Compute node service status



➤ Total Number of Client Connection

It displays the number of connections actually established between the current “Front-end Application” and the compute node, in unit of pcs.

➤ Thread Usage of Compute Nodes

It displays the total number of threads, the occupied thread and the idle thread used by the current connection to the compute node, in unit of pcs.

➤ Back-end Connection Status

It displays the total number of threads, the occupied thread and the idle thread used by connection between the compute node and the back-end data source, in unit of pcs.

➤ Direct Memory Usage of Compute Nodes

It displays the current usage of direct memory configured by the compute node, shown as a percentage.

➤ Real-time Data Amount

It displays the monitoring of data amount in the cluster. It supports two statistical modes: line capacity and data capacity. The units of the line are 1, K and M adopting automatic carry, and the units of data capacity are 1byte, KB, MB and GB adopting automatic carry. The data of the whole cluster is monitored by default, and the monitoring

dimension can also be added or adjusted in “[Setting](#)”.

➤ Heap Memory Usage of Compute Nodes

It displays the current usage of heap memory configured by the compute node, shown as a percentage.

(II) Compute node throughout



➤ Network traffic monitoring

It displays the inflow and outflow of the whole cluster, including front-end traffic in/out and back-end traffic in/out in Bps.

➤ TPS

It displays the number of transactions executed per second for the whole cluster, in unit of pcs.

➤ QPS

It displays the number of queries per second for the whole cluster, in unit of pcs.

➤ Client operation rate

It displays the compute node operation throughput of the client in times/s, and monitors the whole cluster by default. The monitoring dimension can also be added or adjusted in “[Setting](#)”.

➤ Back-end operation rate

It displays the operation throughput of compute node and back-end data source in times/s, and monitors the whole cluster by default. The monitoring dimension can also be added or adjusted in “[Setting](#)”.

(III) Compute node server resources



➤ **Server memory usage**

It displays the current memory usage of the server where the compute node is located. The total memory, used memory and remaining memory can be viewed. The server memory usage of master compute node is monitored by default, and the multi-node mode cluster can be switched to view other compute nodes in “[Setting](#)”.

➤ **Server disk space usage**

It displays the current disk space usage of the server where the compute node is located. The total disk space, used disk space and remaining disk space can be viewed. The server disk space usage of master compute node is monitored by default, and the multi-node mode cluster can be switched to view other compute nodes in “[Setting](#)”.

➤ **Server CPU load condition**

It displays the CPU load of the server where the compute node is located. The CPU load of master compute node is monitored by default, and the multi-node mode cluster

can be switched to view other compute nodes in “[Setting](#)”.

➤ **Server CPU usage**

It displays the CPU usage of the server where the compute node is located. By default, the CPU usage of master compute node is monitored by default, and the multi-node mode cluster can be switched to view other compute nodes in “[Setting](#)”.

➤ **Server disk read/write status**

It displays the disk IO read/write status of the server where the compute node is located. The disk read/write status of master compute node is monitored by default, and the multi-node mode cluster can be switched to view other compute nodes in “[Setting](#)”.

➤ **Server network traffic**

It displays the network traffic in/out of the server where the compute node is located, expressed in Bps. The network traffic in/out of master compute node is monitored by default, and the multi-node mode cluster can be switched to view other compute nodes in “[Setting](#)”.

➤ **Server disk IO bandwidth usage**

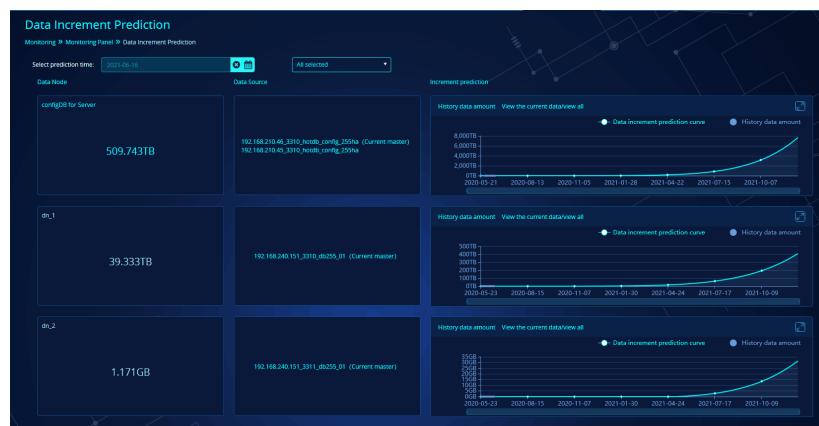
It displays the disk IO bandwidth usage of the server where the compute node is located, expressed by a percent sign. The disk IO bandwidth usage of master compute node is monitored by default, and the multi-node mode cluster can be switched to view other compute nodes in “[Setting](#)”.

15.3.3. Data increment prediction

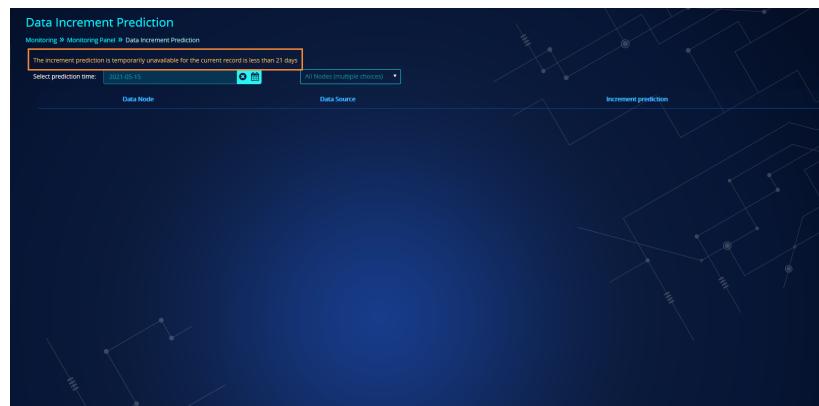
The management platform can evaluate the data capacity growth trend of data sources, ConfigDBs and other components through the intelligent scientific prediction and provide reference for capacity expansion and reduction.

(1) Page information description

The total data of ConfigDB and data nodes (current active ConfigDB and master data source) is collected at two o'clock each morning and recorded in the ConfigDB of the management platform. After 21 days of record, a prediction curve of data increment will be drew using polynomial fitting method, based on the history data amount.

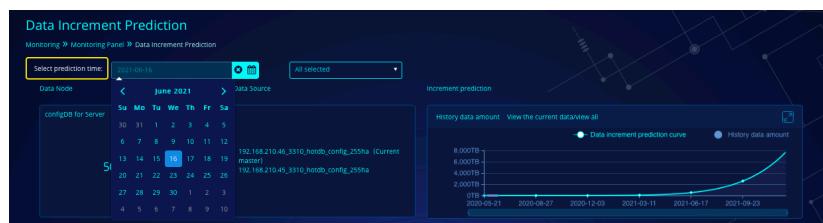


If the history data of compute node ConfigDB, management platform ConfigDB and all data nodes is less than 21 days, the prediction curve will not be generated, and the page will give an orange reminder.



(2) Select prediction time

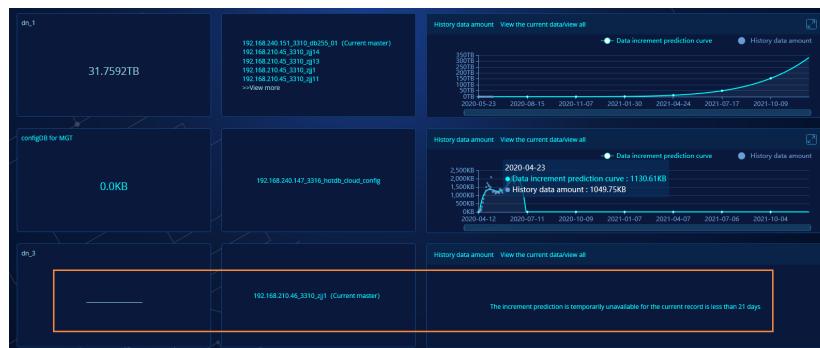
You can select the prediction time, and the minimum unit is day. The timeline of the curve is based on the selected prediction time.



- The prediction time is today one year later by default.
- Time range: Dates within three years from today. If today is May.15, 2020, only dates between May.16, 2020 and May.15, 2023 (May.15, 2020 is not included) can be selected. Other dates will be displayed gray.

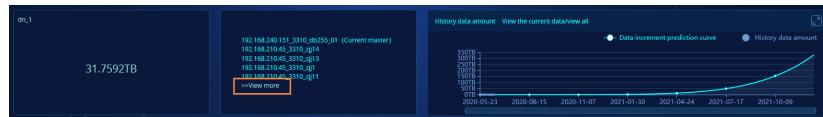
(III) Prediction data display

The page is divided into three parts: data node, data source and the data increment prediction. Five pieces of information are displayed on a single page in descending order of data capacity. The data node or ConfigDB whose history data record is less than 21 days will be displayed at the bottom, as shown in the following figure:



- Display of data node: Data node/ConfigDB name + prediction result. For the data node plate, move the cursor over the plate, you can view the hyperlink effect; click the plate, you can jump to the data node details page. For the ConfigDB plate, there is no special effect. The prediction result displayed is the data capacity of the selected prediction time.
- Display of data source: IP_Port_Data source name. It displays all data sources under the data node and identifies the current active data source. If the number of data sources exceeds five, only five data sources will be displayed. Click ">> View

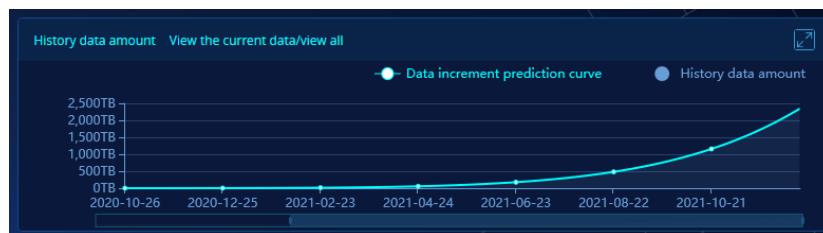
more" to jump to the data node details page.



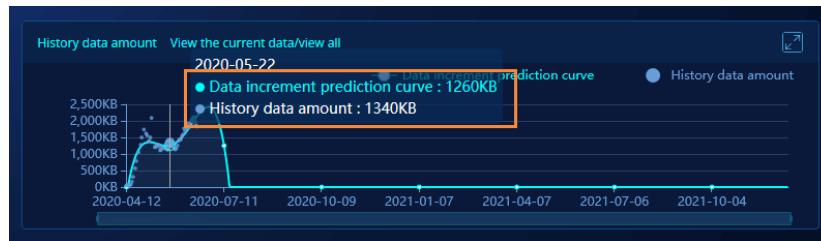
- Increment prediction: the prediction curve calculated by the management platform according to the history data amount and time of the current active data source or ConfigDB.

(IV) Prediction curve

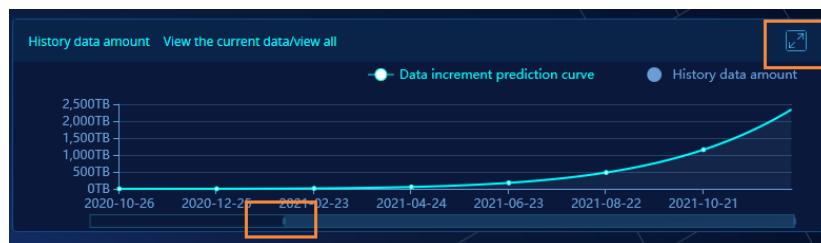
The prediction curve has two parts: one is the history data amount collected every day, which is displayed in the form of blue scatter; the other is the curve generated by fitting the collected history data, which is displayed in green solid line.



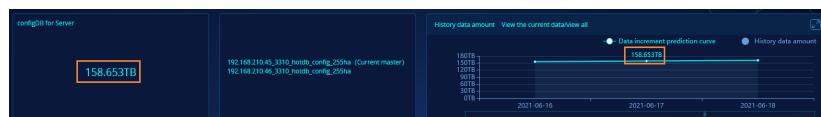
- X-axis: The prediction time. The starting time is the recording time of history data capacity within two years, and the ending time is the selected prediction time plus six months. If the recording time is Feb.6, 2019, today is Jan.23, 2020, the selected prediction time is Dec.23, 2020, which after plus six months is Jun.23, 2021, and the final length of this X-axis is Feb.6, 2019 to Jun.23, 2021.
- Y-axis: The data capacity. The unit size is from B to TB, and the unit changes automatically according to the value size.
- History data amount: Displayed in blue scatter. When the cursor is moved above the scatter position, the time and the corresponding data amount will be displayed.



- Increment prediction curve: Displayed in green solid line. Move the cursor above the curve, the specific time and corresponding prediction value will be displayed. A scroll bar is under the curve to facilitate the viewing of specific time periods. Click the zoom in button at the upper right to display the chart in full screen.



- Click View the current data, the curve will only display the prediction value of current prediction time, which is consistent with the prediction result displayed in the data node.



Notes:

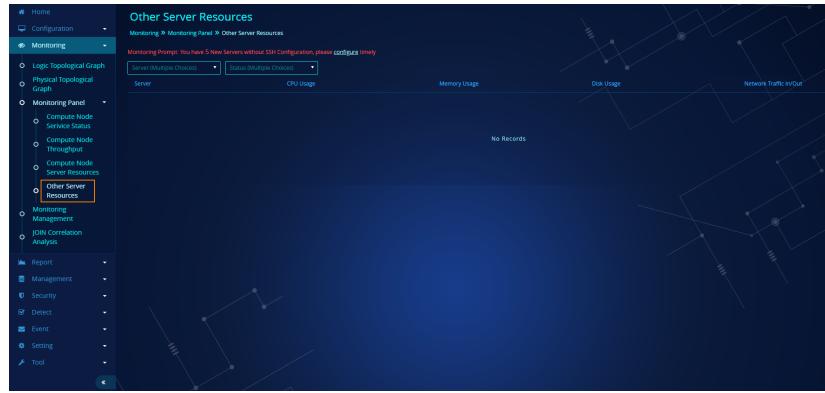
The data capacity predicted by the current prediction method is only for reference, which needs further manual judgment based on the actual situation. The longer data prediction time, the more accurate the prediction results.

15.3.4. Cluster resource monitoring

15.3.4.1. Server performance

When the server SSH information is configured on the “Configuration -> [Server](#)” page and the monitoring is enabled, the server resource details can be monitored in this monitoring panel. When the “Server” page is “Stopped” or the SSH configuration is “Removed”, the monitoring page removes the server monitoring, the monitoring information is displayed in pages, and 5 records are displayed per page.

(I) Page information description

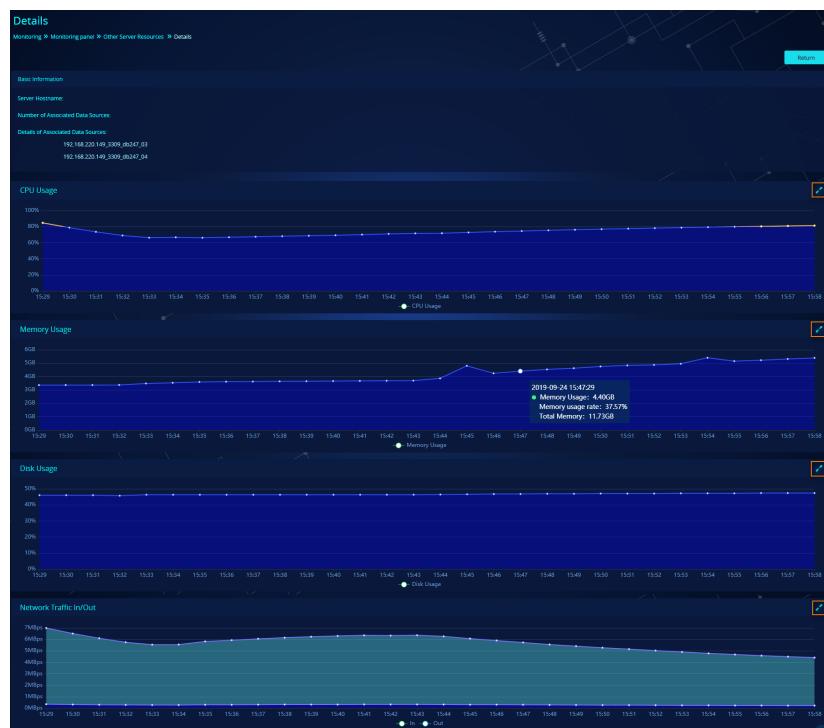


When there is a record of server not configured with SSH information on the “Configuration -> [Server](#)” page, the monitoring page will provide a monitoring reminder, and server monitoring can be enabled by clicking the hyperlink to the “Server” configuration page.

The monitoring status panel displays the detailed monitoring information for all servers included in the monitoring, including: CPU, memory, disk usage (switchable drive), and network traffic in/out (switchable monitoring network card).

The page displays the failure and warning records first by default with a priority of Failure > Abnormal.

The server can select multiple servers by the fuzzy search box in the filtering drop-down box; and the servers can also filter by status. The filtering items include: “Normal, Warning and Failure”.



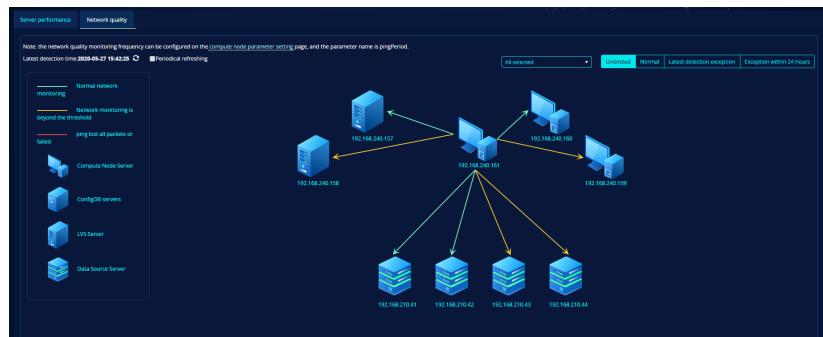
Click the “Status Box” to enter the details page, as shown above.

Click the [Enlarge] button in the upper right corner of the monitoring module to enlarge and view the monitoring data.

15.3.4.2. Network quality

The management platform can monitor the network quality in the cluster operation link, and display the operation network quality, replication network, cross-IDC network, etc. according to the detection data.

15.3.4.2.1. Network quality topology



(1) Page information description

Triggering network quality detection manually will obtain the detection data of network quality executed this time. When [Periodical refreshing] is checked, the management platform will periodically detect the network quality (10s/time) and display data, and the Latest detection time will be synchronously updated.

The filter server is a multi-selection drop-down box with a search box. All servers in the current cluster (servers associated with the cluster service program) are displayed in the drop-down box, among which the check box of the current active compute node server should be checked by default and grayed. As shown below:



Network status descriptions:

Unlimited: data result of the latest detection.

Normal: data of the latest detection is below the threshold.

Latest detection exception: data of the latest detection is above the threshold, the latest detection failed to ping or the packet loss rate is 100%.

Exception within 24 hours: within 24 hours, there is data above the threshold, detection failing to ping or the packet loss rate of 100%.

Topology descriptions:

Network quality monitoring pings all cluster servers outward for the current active compute node server.

If the cluster service programs are shared, the server attributes are divided according to the following priorities: master > compute node > slave > compute node > LVS > ConfigDB > data source.

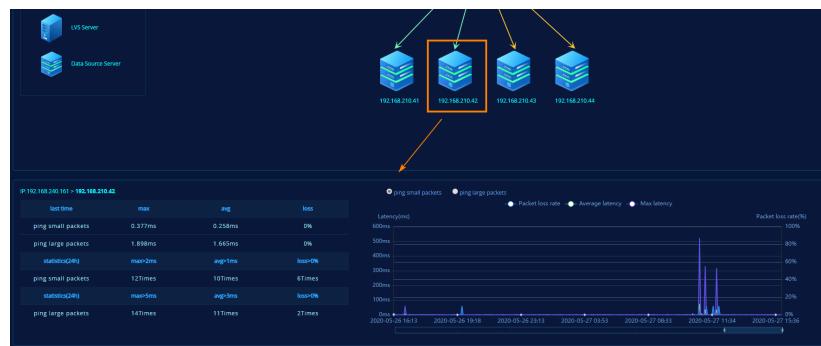
Data is above the threshold (edges in orange), detection failed to ping or the packet loss rate is 100% (edges in red).

Right click to jump to "Monitoring -> Physical Topological Graph" to view the resources of the corresponding server.



15.3.4.2.2. Network quality overview

When entering the network quality page for the first time, the priority of the overview display of server network quality status is, by default, failure>alert>normality, and the data on the panel will not be automatically refreshed no matter you manually refresh the detection, switch the status filter label on the topology, filter the server or other operations. Click the corresponding server, and the network quality from the active compute node to the server will be displayed.

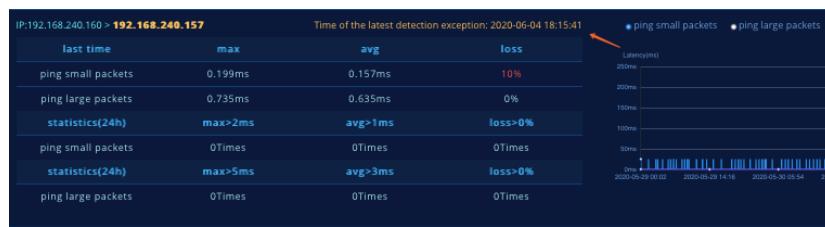


Descriptions of network quality overview:

- IP: the former IP is of the active compute node, and the latter IP is of the pinged cluster server. The IP has two statuses: normality (green) and exception (orange/red). Exception determination: the latest detection data is above the threshold (orange), detection failed to ping and the packet loss rate is 100% (red).
- The network quality data includes the latest detection data and data within 24 hours,

which is divided into ping small packets and ping large packets. For the latest detection data, the max latency, average latency and packet loss rate will be displayed. When the packet loss rate is 100%, i.e. ping packets are all lost, max and avg will be displayed with "-" (no value); if any of the max latency, average latency and packet loss rate is above the threshold set by the management platform, it will be displayed in red. For data within 24 hours, the times of max latency>2ms, average latency>1ms or packet loss rate > 0% above the threshold within 24 hours will be counted and displayed.

- If there is an exception in the latest network quality detection, click the abnormal server, the time of the latest detection exception will automatically appear in “orange” on the monitoring quality overview page; if the latest network quality detection is in the normal status, the time of the latest detection exception will also appear in “blue”.



15.3.4.2.3. Network quality panel

The network quality panel displays the corresponding network quality detection data. The data within 24 hours will be displayed by default. If it is less than 24 hours, the drag block will be hidden. By dragging the block towards left and right you can control the display of data within 7 days. Move the cursor into the line chart to view the data of specific time points. Click button in the upper left corner to switch the ping packet type, for which “ping small packets” is selected by default. Click “packet loss rate”, “average latency”, “max latency” to see the corresponding data. Data acquisition frequency of the monitoring panel is the same as data acquisition frequency controlled by the parameter pingPeriod in server.xml. In the case of network quality failure, the acquisition frequency will be automatically increased to once per minute (for the standard of network quality failure, please refer to the function description of relevant parameters of pingPeriod).



Note: the threshold displayed in the network quality monitoring should be set through Monitoring Panel Setting>Cluster resource monitoring>Network quality. The switch is OFF by default. When it is OFF, the data threshold warning will not be displayed. If the switch is ON, the page will display and judge according to the specific value in the threshold setting, as shown in the following figure:



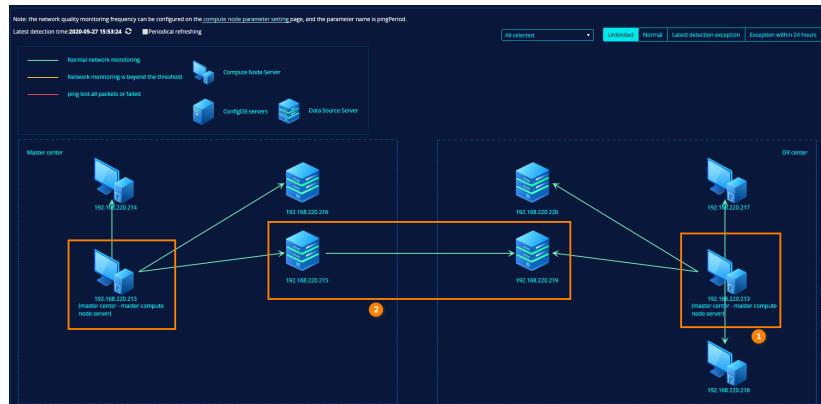
The screenshot shows the 'Network quality' configuration panel. It includes a sidebar with 'Setting' and 'Periodical Detection Setting'. The main area has two sections: 'Small packets continuously ping' and 'Large packets continuously ping'. Each section has input fields for 'Times' (e.g., 3, 5), 'And/or' logic, 'Max latency exceeds' (e.g., 2, 5 ms), 'Packet loss rate exceeds' (e.g., 0, 10 %), and 'Average latency exceeds' (e.g., 1, 3 ms).

IP:192.168.240.161 > 192.168.210.42			
last time	max	avg	loss
ping small packets	5.756ms	5.442ms	0%
ping large packets	6.874ms	6.712ms	0%
statistics(24h)	max>2ms	avg>1ms	loss>0%
ping small packets	4Times	4Times	0Times
statistics(24h)	max>10ms	avg>5ms	loss>10%
ping large packets	1Times	4Times	0Times

15.3.4.2.4. Cross-IDC network quality

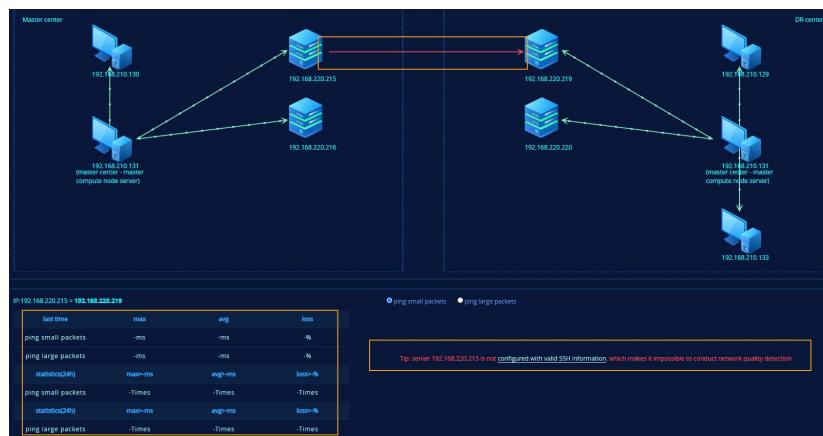
The cross-IDC network quality overview and network quality panel are the same as those of the single IDC, which will not be described here in detail.

However, there are differences between the cross-IDC network quality topology and that of the single IDC.

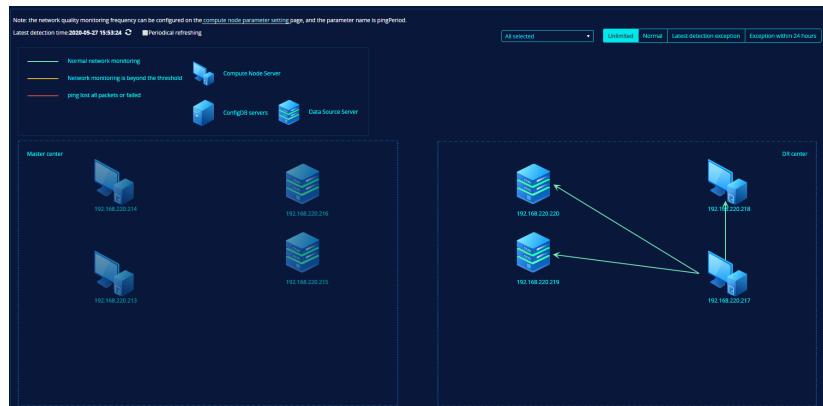


Page Description:

- The master compute node server in the master center needs to ping all servers in the master center except for itself and all servers in the DR center, so the master compute node server in the master center is placed in the master center and the DR center in the topology area above (as shown in mark 1 above);
- The cross-IDC network quality topology only displays: the master center compute node server (including the master/slave compute nodes), the DR center compute node server (including the master/slave compute nodes), the master center ConfigDB server, the master center data source server, the DR center ConfigDB server, the DR center data source server;
- If the server is shared by the service programs, the server role is divided according to the priority described in the single IDC network;
- The cross-IDC network replication relation requires the network quality link connection according to the replication relation between the master/slave data sources of the master IDC and the DR center (as shown in Note 2 above);
- The network quality from the current active data source/ConfigDB in the master center to the target standby data source/ConfigDB in the DR center can obtain the monitoring data only after SSH privilege is configured.



IDC switching instructions:

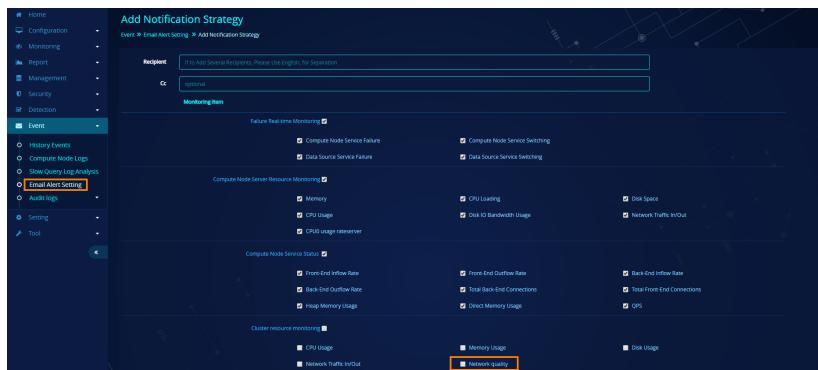
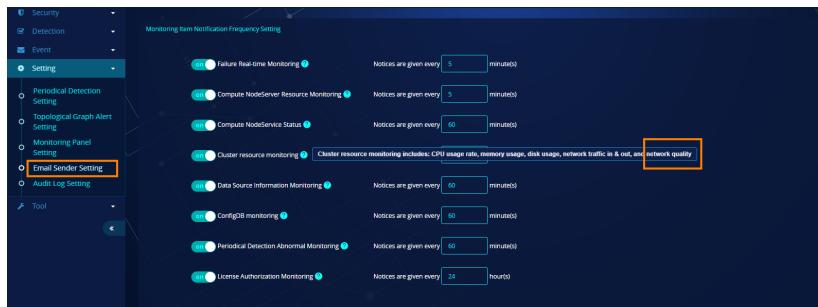


If the IDC switching happens, that is, the compute node of the current DR center provides service, only the network quality monitoring status of the DR center will be displayed; all components in the master center will be displayed gray with no monitoring. There will be no network connection from the DR center to the master center, and the network connection relation of the DR center degenerates to be consistent with that of the single IDC.

14.3.4.2.5. Email alert of network quality

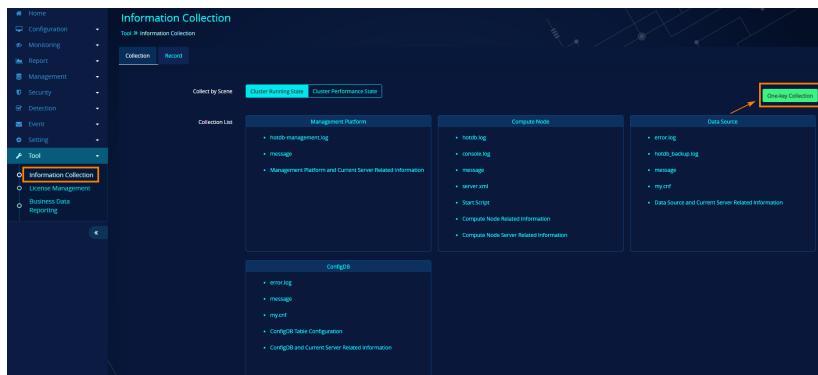
Add a new monitoring item Network Quality through Event -> Email Alert Setting -> Add Notification Strategy, enable Cluster Resource Monitoring in Email Sender Setting

and set the notification frequency of the monitoring item. If the network quality is above the set threshold, an alert email will be sent.



14.3.4.2.6. Network quality information collection

Add network quality detection data through Tool -> Information Collection.



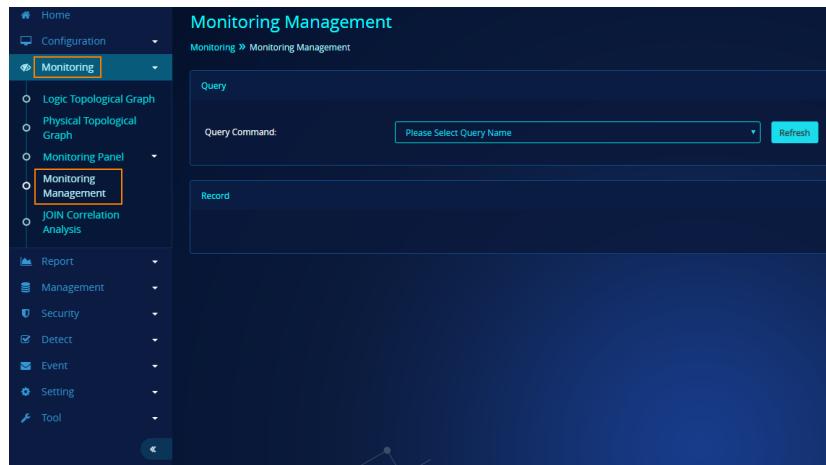
The detection data is added to the "server related information.txt" file in the corresponding server, as shown below:

```
lvs_server_related_information.txt
38 cpul0iowaitusused:0.0227
39 cpul0us:0.2440
40 cpul0y:0.0307
41 cpul0ni:0.0000
42 cpul0id:0.7091
43 cpul0wa:0.0066
44 cpul0hi:0.0000
45 cpul0si:0.0000
46 cpul0ri:0.0000
47 loadlmsavrp:2.53
48 loadlmsavrl:71
49 loadlmsavgi:1.38
50 proc_running:3
51 procs_blocked:0
52 cpucores:4
53 cputhreads:4
54
55 Memory:
56 memoryusage:0.7693
57 memoryavailable:1848024KB
58 memorytotal:8010284KB
59 swapusage:0.0152
60 swapfree:8131920KB
61
62 Disk Space:
63 diskspaceusage:0.9913:mountpoint:/
64 diskspacefree:714MB:mountpoint:/
65 diskspacetotal:81895MB:mountpoint:/
66 diskreadps:2391.4682:diskname:vda
67 diskwriteps:289.1769:diskname:vda
68 diskqueueuelength:0:diskname:vda
69 diskutil:0.1178:diskname:vda
70 diskreadkbytesps:37316.6611:diskname:vda
71 diskwritekbytesps:261.6892:diskname:vda
72 diskutiltop:0.1175:diskname:vda
73
74 Network incoming and outgoing traffic:
75 networkincomesage:-1.0000:interfaceName:eth0
76 networkoutputusage:-1.0000:interfaceName:eth0
77 networklinkspeed:-1:interfaceName:eth0
78 networkincomebytespeed:199626:interfaceName:eth0
79 networkoutputbytespeed:101897:interfaceName:eth0
80 networkincomepacketspeed:453:interfaceName:eth0
81 networkoutputpacketspeed:483:interfaceName:eth0
82 networkincomeusage:-1.0000:interfaceName:lo
83 networkoutputusage:-1.0000:interfaceName:lo
84 networklinkspeed:-1:interfaceName:lo
85 networkincomebytespeed:286104:interfaceName:lo
86 networkoutputbytespeed:286104:interfaceName:lo
87 networkincomepacketspeed:1417:interfaceName:lo
88 networkoutputpacketspeed:1417:interfaceName:lo
89
90 NetworkQuality
91 192.168.240.160->192.168.240.157
92 ping small packet:max latency,average latency,packet loss rate[0.795ms,0.208ms,0.0%]
93 ping big packet:max latency,average latency,packet loss rate[1.475ms,0.89ms,0.0%]
94
```

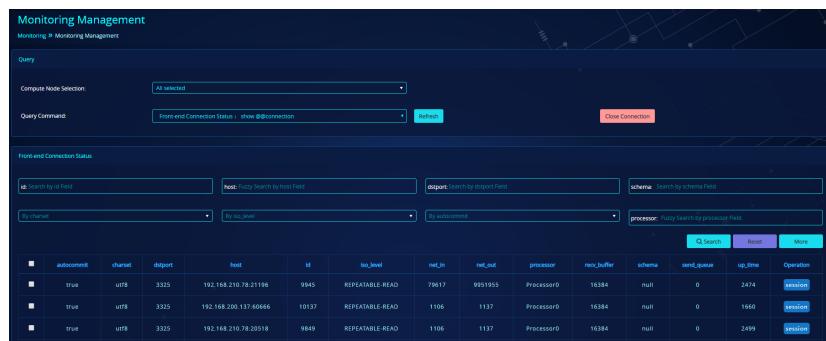
15.4. Monitoring management

The “Monitoring Management” function is to execute the compute node management port (default 3325) related commands through the management platform, and to view the relation between front-end and back-end connection of compute nodes and other effective management information.

15.4.1. Instructions before use



- Multi-node mode cluster can choose the scope of executing query commands, and all compute nodes are selected by default. Single-node and master/slave node mode clusters do not need to select compute nodes, and query commands are executed on the current master compute node by default.
- Commands need to be selected in the “Query Command” for execution. After first entering the function page and selecting the “Query Command”, it is necessary to use the “[Compute Node Database User](#)” with SUPER privilege to login to the management port for cluster security. Only after successful login can the command be executed (except the display processlist command).
- The “host” configured for the login user must contain the IP address of the server where the management platform is located, otherwise the login will fail.
- The commands that can be queried online currently only include a part of the actual management port. The specific executable commands are shown in the following drop-down box.



	autocommit	charset	dbport	host	id	Inode_level	net_in	net_out	processor	read_buffer	schema	send_queue	up_time	Operation
■	true	utf8	3325	192.168.210.78:21196	9945	REPEATABLE-READ	79617	995155	Processor0	16384	null	0	2474	SESSION
■	true	utf8	3325	192.168.200.137:60646	10137	REPEATABLE-READ	1106	1137	Processor0	16384	null	0	1660	SESSION
■	true	utf8	3325	192.168.210.78:20518	9849	REPEATABLE-READ	1106	1137	Processor0	16384	null	0	2499	SESSION

- The command can be sent to port 3323 or port 3325 for execution after login, the query result is displayed in the query panel, and the latest data can be obtained in real time through the [Refresh] button.

15.4.2. Monitoring command description

➤ Server Connection Information display processlist

This function is similar to the display processlist function of MySQL, which is used to view the current compute node server connection processing.



	id	user	host	db	command	time	state	info	Operation
19738	root	192.168.210.78:53986	null	Query	0	executing	show processlist	connection	

- Click [Refresh] to re-execute the selected query command. If a filter condition is added, refresh to display the records that meet the filter criteria.
- You can use with the help of filter items, among which user, db, command and state are exact matches; host and info are fuzzy matches. Exact match search requires complete match keywords.

If jing01 is the user, you need to enter the complete search keyword jing01 in the user input box before filter.

Server Connection Information							
User: jing01		host: Fuzzy Search by host Field		db: Search by db Field		command: Search by command	
state: Search by state Field		info: Fuzzy Search by info Field					
ID	User	Host	DB	Command	Time	State	Info
1146	jing01	127.0.0.1:43266	null	Sleep	2204		null
1147	jing01	127.0.0.1:43392	null	Sleep	1902		null
1169	jing01	192.168.240.117:42840	null	Query	0	executing	show processlist where user='jing01'

If jing is entered, you cannot get the record information of user jing01.

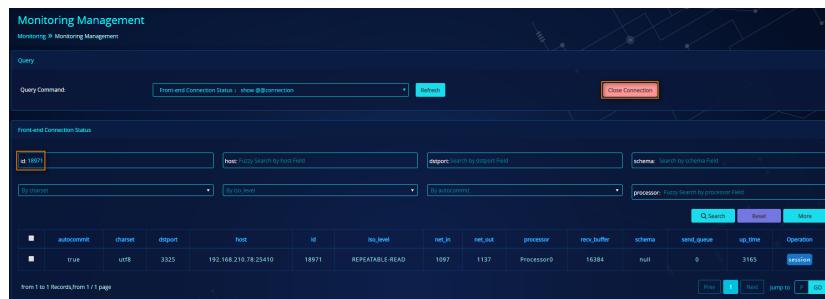
Server Connection Information									
User: jing		host: Fuzzy Search by host Field		db: Search by db Field		command: Search by command			
state: Search by state Field		info: Fuzzy Search by info Field							
No Records									

- After entering the search keywords in the box, click Search to trigger a filter query. Click [Reset] to clear the search box.
- After the display processlis query, move the mouse cursor into the header to display the comment information of the specific field.
- When moving the mouse cursor into the connection link in the operation bar, the prompt is displayed as below. Click the link to obtain the ID of this record and perform filtering query in command “display @@connection” (that is, [Front-end Link Status](#)). Note: If the login information of the node user expires, it needs to log in again.

Monitoring Management							
Monitoring > Monitoring Management							
Query							
Query Command: Server Connection Information: show processlist							
Default							
Server Connection Information							
M	User	Host	DB	Command	Time	State	Info
19738	root	192.168.210.78:53668	null	Query	0	executing	show processlist

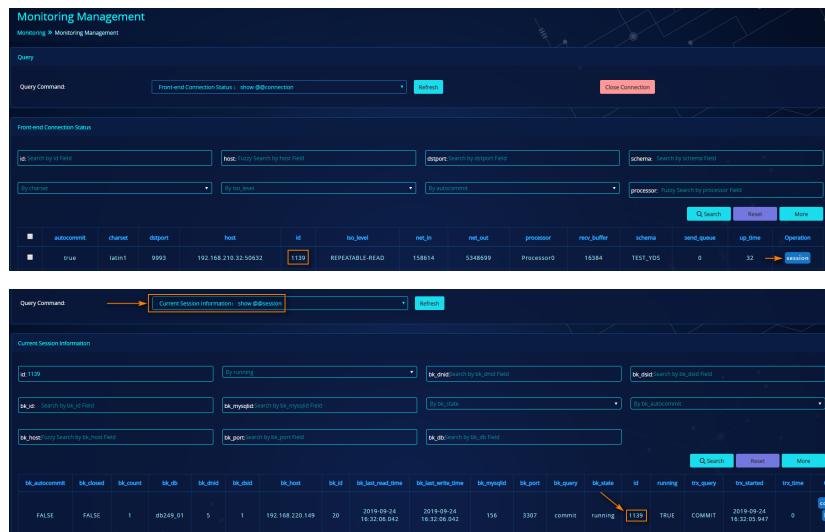
➤ Front-end Connection Status display @@connection

It displays the connection status of the compute node front-end connection (including the server and the management).



The screenshot shows the 'Monitoring Management' section under 'Monitoring'. The 'Front-end Connection Status' table is displayed. A connection with ID 1139 is highlighted. The table includes columns such as host, id, io_level, net_in, net_out, processor, recv_buffer, schema, send_queue, up_time, and Operation. The 'Operation' column for this row shows a link labeled 'session'.

- After the command completes the query, select the connection ID and manually close the corresponding connection through the [Close Connection] button.
- When moving the mouse cursor into the session link in the operation bar, the prompt is displayed as below. The [Current Session Information display @@session](#) of the connection ID can be viewed. Click the link to obtain the connection ID of this record and jump to the session information viewing window.

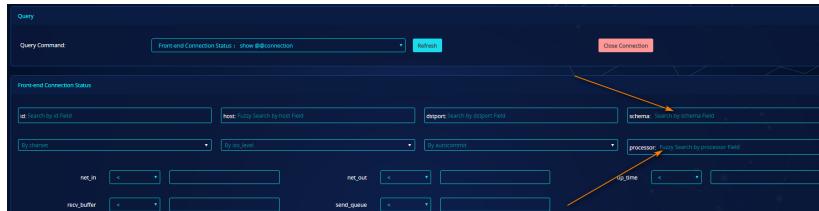


The screenshot shows the 'Monitoring Management' section under 'Monitoring'. The 'Current Session Information' table is displayed. A connection with ID 1139 is highlighted. The table includes columns such as id, host, io_level, net_in, net_out, processor, recv_buffer, schema, send_queue, up_time, and Operation. The 'Operation' column for this row shows a link labeled 'session'.

Below the table, there is a 'Query Command' input field containing 'Current Session Information - show @@session'. An arrow points from this input field to the 'session' link in the table's 'Operation' column.

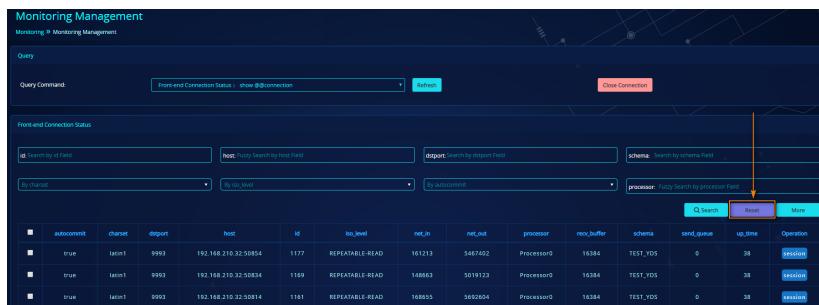
- After entering the condition value in the filter input box and the drop-down box, click the [Search] button to trigger the filtering action. Multiple filters are connected with “and”.
- If the input box prompts “Fuzzy Search”, the back-end uses fuzzy match. If the

input box prompts “Search”, the back-end uses exact match.



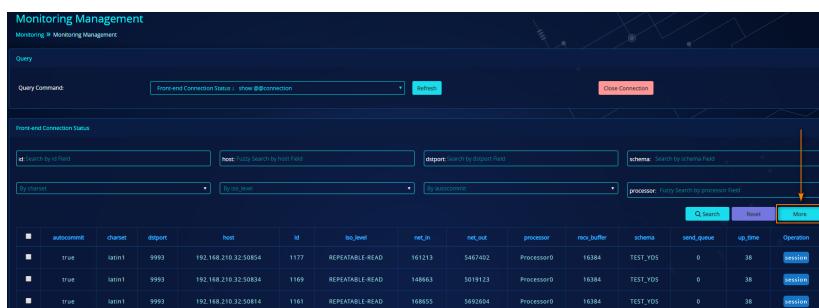
The screenshot shows the 'Query' section of the management interface. It includes several search input fields: 'host' (exact), 'port' (exact), 'schema' (exact), 'processor' (exact), and 'session' (exact). Below these are dropdowns for 'By channel', 'By ip_level', 'By autoconnect', and 'By processor'. There are also numerical input fields for 'net_in', 'net_out', 'processor', 'recv_buffer', and 'send_queue'.

- Click the [Reset] button to clear all values in the filter boxes.



The screenshot shows the 'Monitoring Management' section. It features a table with columns: autocommit, charset, dport, host, id, iso_level, net_in, net_out, processor, recv_buffer, schema, send_queue, up_time, and Operation. A row of data is shown with values corresponding to the columns. Above the table is a search bar with four input fields: 'host', 'port', 'schema', and 'processor', each with its own 'Reset' button. The 'processor' field's 'Reset' button is highlighted with a red arrow.

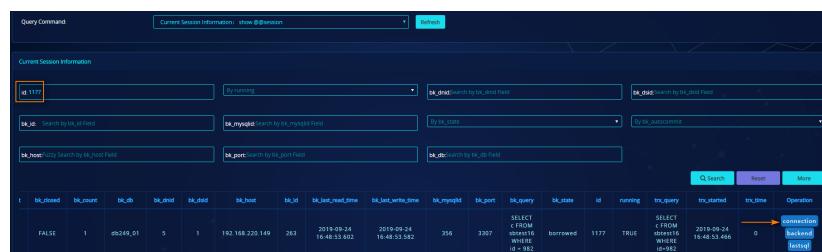
- Click [More] to expand search fields:



The screenshot shows the same 'Monitoring Management' section as above, but with the 'More' button from the previous screenshot clicked. This has expanded the search bar to include additional fields: 'host', 'port', 'schema', and 'processor', each with its own 'Search' button. The 'processor' field's 'Search' button is highlighted with a red arrow.

➤ Current Session Information display @@session

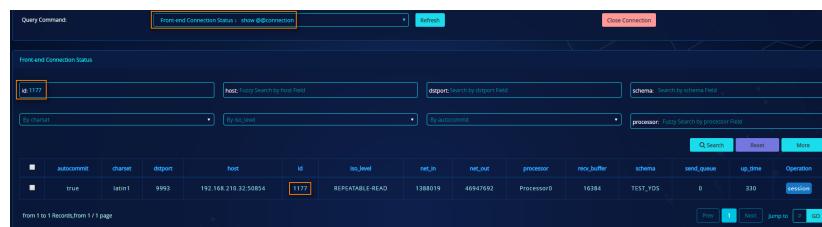
It displays the current session processing information of the compute node.



Current Session Information

id	bk_closed	bk_count	bk_db	bk_did	bk_did	bk_host	bk_id	bk_last_read_time	bk_last_write_time	bk_myqid	bk_port	bk_query	bk_state	id	running	trs_query	trs_started	trs_time	Operation
1177	FALSE	1	db249_01	5	1	192.168.220.149	263	2018-09-24 16:48:53.602	2018-09-24 16:48:53.582	356	3307	SELECT * FROM t1 WHERE id = 982;	borrowed	1177	TRUE	SELECT * FROM t1 WHERE id = 982;	2018-09-24 16:48:53.466	0	Connection

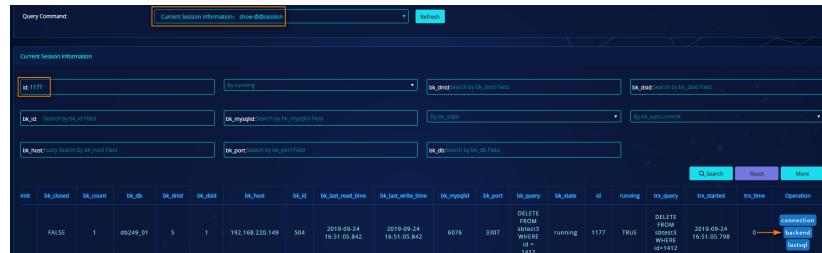
- When moving the mouse cursor into the connection, backend, and lastsql links in the operation bar, the following prompt is displayed: “View the [Front-end Connection Status, Back-end Connection Status, and Finally Executed SQL](#) corresponding to the session ID. Click the link to obtain the id value of this record and jump to display @@connection;
- Click connection to obtain the id value of this record and jump to display @@connection:



Front-end Connection Status

id	autocommit	charset	dialect	host	id	isolation	net_in	net_out	processor	recv_buffer	schema	send_queue	up_time	Operation
1177	true	latin1	9993	192.168.210.32:50854	1177	REPEATABLE-READ	1388019	46947693	Processor0	16384	TST_YDS	0	330	connection

- Click backend to obtain the bk_id field value and jump to display @@backend



Current Session Information

id	bk_closed	bk_count	bk_db	bk_did	bk_did	bk_host	bk_id	bk_last_read_time	bk_last_write_time	bk_myqid	bk_port	bk_query	bk_state	id	running	trs_query	trs_started	trs_time	Operation
1177	FALSE	1	db249_01	5	1	192.168.220.149	504	2019-09-24 16:51:05.842	2019-09-24 16:51:05.842	6076	3307	DELETE FROM t1 WHERE id = 1412;	running	1177	TRUE	DELETE FROM t1 WHERE id = 1412;	2019-09-24 16:51:05.798	0	connection

Query Command	Backend Connection Status: show @@backend	Switch	Default Connection Pool
Backend Connection Status			
ID	User	Host	Schema
10	ok_myself	learnt by ok_myself free	ok_myself learnt by ok_myself free
schemaclear	learnt by schema Field	(S) sleep	by ok_myself
By comment			
			CL search Reset More

autocommit	charset	closed	comment	dead	host	id	max_allowed_packet	port	mysqlbinlog	net_id	net_old	processor	schema	send_query	status	up_time	version	Operation
false	latin1	false	querying	5	192.168.220.149:3307	504	REPEATABLE-READ	46634	5076	131578009	3964531	ProcessorA	db249_01	0	running	1550	0	SESSION

- Click `lastsql` to obtain the `bk_id` field value and jump to display `@@lastsql`:

Query Command: Borrowed Connection Finally Executed SQL Information - show diffkern

Search: Advanced Search

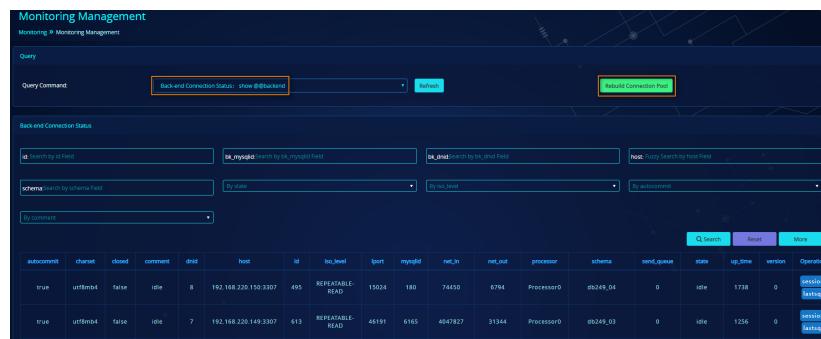
Borrowed Connection Finally Executed SQL Information

Value	mpgsql_conn_by_repeated_host	host	last_executed_sql	mpgsql_id	Operation
S-1	192.168.220.149:3307/ob289,0!	20	UPDATE interest2 SET k = k + 1 WHERE id = 1010	156	session backend

From 1 to 1 Records(0.1 page)

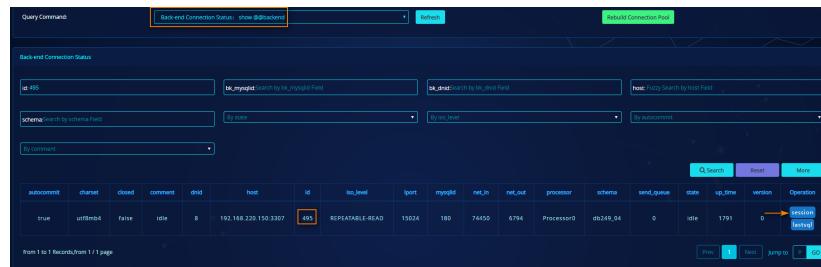
- #### ➤ Back-end Connection Status display @@backend

It displays the back-end connection of the compute node (that is, between compute node and data source).



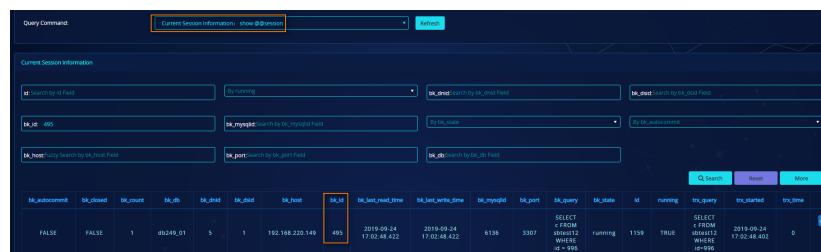
autocommit	charset	closed	comment	dialed	host	id	is_low	iport	mysqlid	net_in	net_out	processor	schema	send_queue	state	up_time	version	Operation
true	utf8mb4	false	idle	8	192.168.220.150:3307	495	REPEATABLE READ	15024	180	76450	6794	Processor0	db249_04	0	idle	1738	0	session lastsql
true	utf8mb4	false	idle	7	192.168.220.149:3307	613	REPEATABLE READ	46191	6165	4047827	31344	Processor0	db249_03	0	idle	1256	0	session lastsql

- After the command is executed, click the [Rebuild Connection Pool] button in the panel to rebuild the back-end connection. As with the management rebuild @@pool command, it prompt “Rebuild Succeeded/Failed” after the execution.
- When moving the mouse cursor into the session and lastsql links in the operation bar, the following prompt is displayed: “View the corresponding session information, view the finally executed SQL”. click the link to obtain the id field value of this record and filter in the command “display @@session, display @@lastsql”. (the bk_id in display@@session record and the id in display@@lastsql record correspond to it). Click the session button in the operation bar:



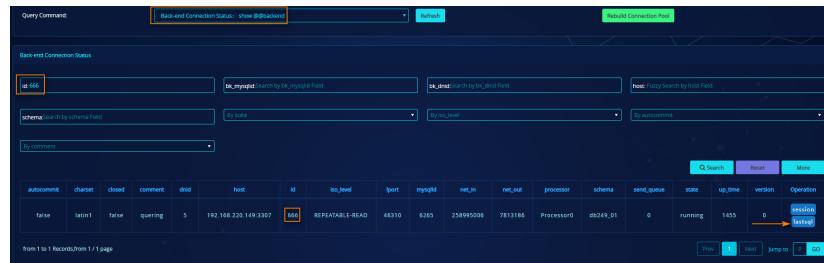
autocommit	charset	closed	comment	dialed	host	id	is_low	iport	mysqlid	net_in	net_out	processor	schema	send_queue	state	up_time	version	Operation
true	utf8mb4	false	idle	8	192.168.220.150:3307	495	REPEATABLE READ	15024	180	76450	6794	Processor0	db249_04	0	idle	1793	0	session lastsql

from 1 to 1 Records, from 1 / 1 page



bk_id	bk_closed	bk_count	bk_db	bk_dialed	bk_disted	bk_host	bk_id	bk_iport	bk_is_low	bk_iprotocol	bk_iprot	bk_query	bk_state	bk_id	running	bk_query	bk_started	bk_time
495	2019-09-24 17:02:48.422	2019-09-24 17:02:48.422	5	1	192.168.220.149	495	6136	3307	running	1159	TRUE	SELECT c FROM t WHERE id = 999	2019-09-24 17:02:48.402	0				

- Click the lastsql button in the operation bar:



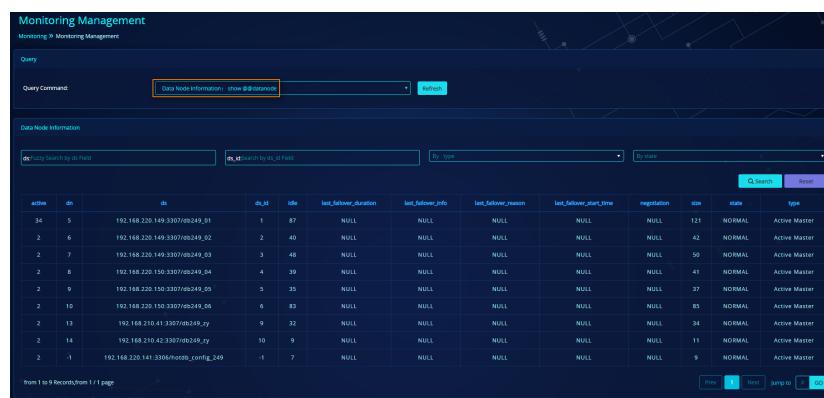
The screenshot shows the 'Backend Connection Status' section of the management platform. It displays a table of connection details with various filters and search fields at the top. A prominent 'lastsql' button is located in the top right corner of the table's header area.



The screenshot shows the 'Borrowed Connection Finally Executed SQL Information' section. It lists recently executed SQL queries with their execution details. Similar to the first screenshot, a 'lastsql' button is visible in the top right of the table's header.

➤ Data Node Information display @@datanode

It displays information about all data nodes in the current compute node. The query results include: "Current Data Source of Node", "Active Connection", and "Node Status".



The screenshot shows the 'Monitoring Management' section, specifically the 'Data Node Information' part. It lists data nodes with their details like active status, ID, and configuration. A 'lastsql' button is located in the top right of the table's header.

➤ Data Source Information display @@datasource

It displays information about all data sources in the current cluster. The query results

include: “Host IP Address”, “Port”, “Database Name”, and “Unavailable Reason of Data Source”.

Monitoring Management												
Data Source Information												
active	ds	ds_id	flow_control	host	Mw	port	schema	size	status	type	unavailable_reason	
3	5	1	11/64	192.168.220.149	88	3307	ds249_01	121	Available	Active Master	NULL	
2	6	2	0/16	192.168.220.149	40	3307	ds249_02	42	Available	Active Master	NULL	
2	7	3	0/64	192.168.220.149	68	3307	ds249_03	50	Available	Active Master	NULL	
2	8	4	0/16	192.168.220.150	39	3307	ds249_04	41	Available	Active Master	NULL	
2	9	5	0/16	192.168.220.150	35	3307	ds249_05	37	Available	Active Master	NULL	
2	10	6	0/16	192.168.220.150	83	3307	ds249_06	85	Available	Active Master	NULL	
2	13	9	0/64	192.168.210.41	32	3307	ds249_zy	34	Available	Active Master	NULL	
2	14	10	0/16	192.168.210.42	9	3307	ds249_zy	31	Available	Active Master	NULL	
2	-1	-1	N/A	192.168.220.141	7	3306	hotdb_config_249	9	Available	Active Master	NULL	

➤ Back-end Heartbeat Status display @@heartbeat

It displays the back-end heartbeat status of the current cluster. The query results include: Data Source Type, Host Address, Database Name, Heartbeat Status, and Heartbeat Period.

Monitoring Management												
Back and Heartbeat Status												
db	ds	ds_id	ds_type	execute_time	host	last_active_time	period	port	retry	status	stop	
ds249_01	5	1	master	0,0,3	192.168.220.149	2019-09-24 17:11:31	2000	3307	0	idle	false	
ds249_02	6	2	master	0,0,3	192.168.220.149	2019-09-24 17:11:31	2000	3307	0	idle	false	
ds249_03	7	3	master	0,0,3	192.168.220.149	2019-09-24 17:11:31	2000	3307	0	idle	false	
ds249_04	8	4	master	0,1,1	192.168.220.150	2019-09-24 17:11:30	2000	3307	0	idle	false	
ds249_05	9	5	master	0,2,1	192.168.220.150	2019-09-24 17:11:30	2000	3307	0	idle	false	
ds249_06	10	6	master	0,0,1	192.168.220.150	2019-09-24 17:11:30	2000	3307	0	idle	false	
ds249_zy	13	9	master	0,0,2	192.168.210.41	2019-09-24 17:11:30	2000	3307	0	idle	false	
ds249_zy	14	10	master	0,2,2	192.168.210.42	2019-09-24 17:11:29	2000	3307	0	idle	false	
hotdb_config_249	-1	-1	master	0,0,0	192.168.220.141	2019-09-24 17:11:31	2000	3306	0	idle	false	

➤ Synchronization Delay display @@latency

It displays the synchronization delay. The query results include “Current Data Source Path”, “Slave Data Source Path”, and “Synchronization Delay Time (in ms)”.



Query Command: Synchronization Delay : show @@bufferpool

Synchronization Delay

dn	info	latency
192.168.210.63:3308/proxy/9114121	11	0 ms

from 1 to 1 Records from 1 / 1 page

➤ Buffer Pool Status display @@bufferpool

It queries the buffer pool status. The query results include “Thread Name”, “Buffer Pool Size”, and “Local Cache Thread Application Buffer”.



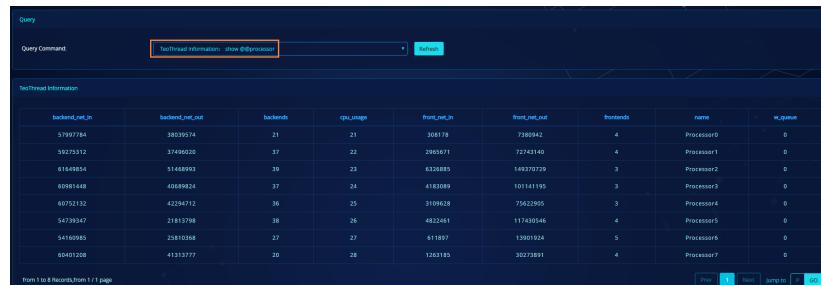
Query Command: Buffer Pool Status : show @@bufferpool

Buffer Pool Status

local_allocate_ops	local_get_size	other_allocate_ops	other_recycle_ops	pool_size	queue_recycle_ops	thread
4213	4212	0	null	1	0	\$NIOExecutor-0-0
34975	34959	0	null	16	0	\$NIOExecutor-1-1
8735	8730	0	null	5	0	\$NIOExecutor-0-2
34123	34114	0	null	9	0	\$NIOExecutor-1-0
74721	74706	0	null	15	0	\$NIOExecutor-2-3
58791	58789	0	null	2	0	\$NIOExecutor-5-3
35705	35699	0	null	6	0	\$NIOExecutor-1-3
75802	75773	0	null	27	0	\$NIOExecutor-2-0
50902	50877	0	null	25	0	\$NIOExecutor-3-2

➤ TeoThread Information display @@processor

It displays the current TeoThread Information. The query results include “Thread Name”, “Byte Received by Front/Back End”, and “Byte Sent by Front/Back End”.



Query Command: TeoThread information: show @@processor

TeoThread Information

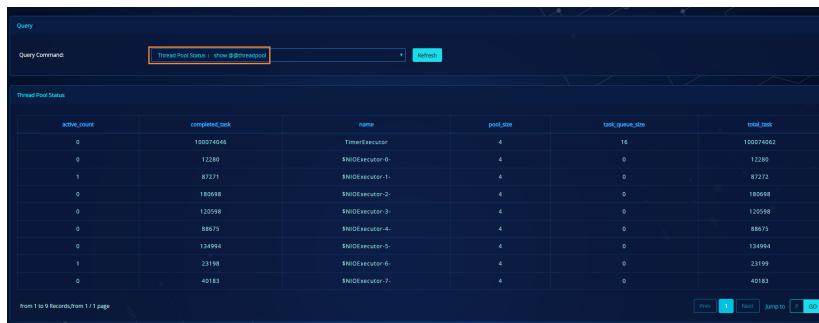
backend_net_in	backend_net_out	backends	cpu_usage	front_net_in	front_net_out	frontends	name	w_query
57907784	38039574	21	21	308178	7380942	4	Processor0	0
59275312	37490020	37	23	2903671	72743140	4	Processor1	0
61649854	5146893	19	23	6326885	149370729	3	Processor2	0
65981448	40889624	37	24	4180389	101141195	3	Processor3	0
60753132	42294712	36	25	3109628	75622905	3	Processor4	0
54739347	21813798	38	26	4822461	117430546	4	Processor5	0
54160985	25810618	27	27	611897	13901924	5	Processor6	0
65401208	41313777	20	28	1263185	30273891	4	Processor7	0

from 1 to 8 Records from 1 / 1 page

➤ Thread Pool Status display @@threadpool

It displays the current thread pool status. The query results include “Thread Pool Name”,

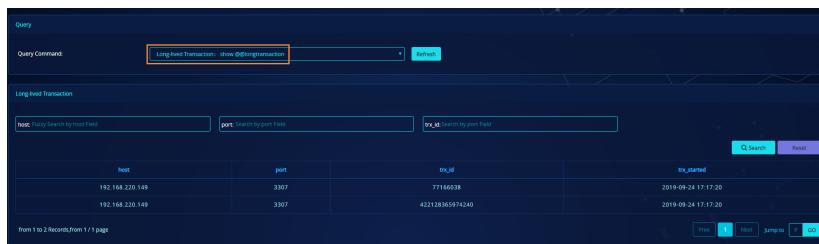
“Thread Pool Size”, and “Active Thread”. Chinese prompt will be displayed when moving the mouse cursor to the column name.



active_count	completed_task	name	pool_size	task_queue_size	total_task
0	100074046	TimeExecutor	4	16	100074062
0	12280	\$!\$!Executor-0-	4	0	12280
1	87271	\$!\$!Executor-1-	4	0	87272
0	180598	\$!\$!Executor-2-	4	0	180598
0	120598	\$!\$!Executor-3-	4	0	120598
0	88675	\$!\$!Executor-4-	4	0	88675
0	134694	\$!\$!Executor-5-	4	0	134694
1	23198	\$!\$!Executor-6-	4	0	23199
0	40183	\$!\$!Executor-7-	4	0	40183

➤ Long-lived Transaction display @@longtransaction

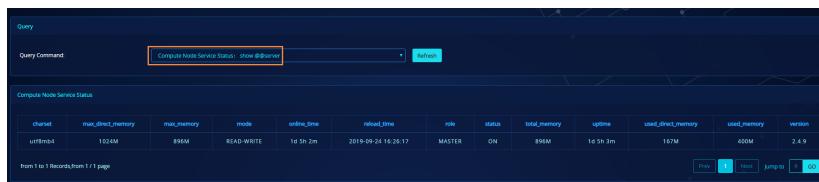
It displays the long-lived transaction and the query results include “Host IP Address”, “Port”, and “Long-Lived Transaction id”. Chinese prompt will be displayed when moving the mouse cursor to the column name.



host	port	trx_id	trx_started
192.168.220.149	3307	77166038	2019-09-24 17:17:20
192.168.220.149	3307	422128365974240	2019-09-24 17:17:20

➤ Compute node server status display @@server

It displays the compute node server status. The query results include the running startup information of the compute node server, such as “Memory Usage”, “Read/ Write Mode”, “Starting Time”, and “High Availability Role”. Chinese prompt will be displayed when moving the mouse cursor to the column name.



charset	max_direct_memory	max_memory	mode	online_time	released_time	role	status	total_memory	uptime	used_direct_memory	used_memory	version
utf8mb4	1524M	896M	READ-WRITE	1d 5h 2m	2019-09-24 16:26:17	MASTER	ON	896M	1d 5h 3m	167M	650M	2.4.9

➤ Borrowed Connection Finally Executed SQL Information

Queries of the borrowed connection finally executed SQL information is usually used to view the connection exception information. The results include: “Finally Executed SQL Statement”, “Back-end mysql Connection id”, “Host”, and “Node”.

Borrowed Connection Finally Executed SQL Information						
id	host	id	last_executed_sql	mysqlid	Operation	
14-10	192.168.210.42.3107/d9249_2y	247	REPLACE INTO hotdb_heartbeat SET master_record=28163190838212474,id=2	184	session	backend
5-1	192.168.220.149.3307/d9249_01	622	UPDATE hotdb_heartbeat SET id=89,last_heartbeat_time=now(),master_record=1921682201419993 where id=89 and master_record=1921682201419993	6210	session	backend
5-1	192.168.220.149.3307/d9249_01	572	DESC test_1	6106	session	backend
5-1	192.168.220.149.3307/d9249_01	38	REPLACE INTO hotdb_heartbeat SET master_record=283044293436920,id=2	179	session	backend

➤ Acquire the File under conf Directory and the Last Modification Time

It displays the modification record of configuration file.

Acquire the File under conf Directory and the Last Modification Time	
	data
	1 : hotdb_config.sql time:2019-07-08 21:29
	2 : keepalive.conf backup time:2019-07-08 10:33
	3 : keepalive.conf master time:2019-07-08 10:33
	4 : log4j2.xml time:2019-07-08 21:29
	5 : server.xml time:2019-07-08 14:05
	6 : server.xml time:2019-09-04 13:56

15.5. JOIN correlation analysis

The “JOIN Correlation Analysis” function is to map the JOIN correlation diagram of the table in current business scenario by parsing the SQL statement in slow query log (i.e. [Slow Query Log Analysis](#) list data), thereby allowing users to have a global monitoring of the current business join table query JOIN. It also provides the cross-node cross JOIN correlation diagram, and users can pay attention to the current cross-node cross JOIN situation to optimize the table structure or the SQL query statement.

15.5.1. Prerequisites for use

To view the JOIN correlation diagram, the following prerequisites shall be met:

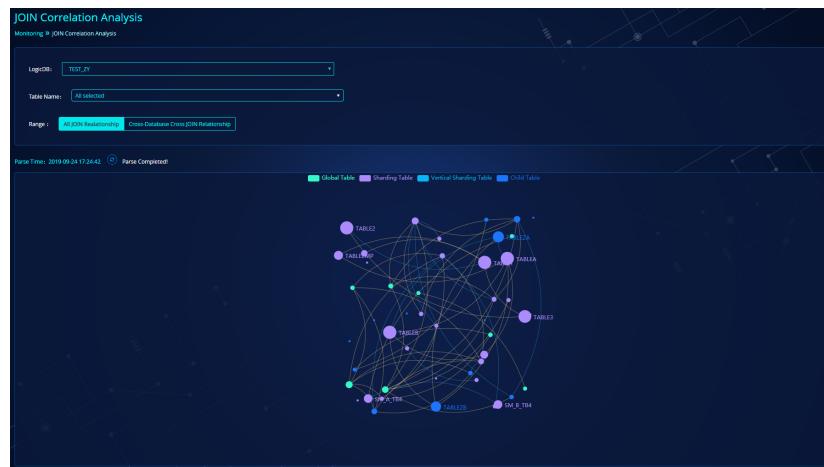
- The current user has the “Slow Query Log Analysis” menu privilege;
- The current compute node parameter “Allow JOIN query” is on;
- The current compute node parameter “Statistics on SQL implementation conducted or not” is on;

15.5.2. JOIN correlation diagram

After selecting a logicDB and table name, all JOIN correlation diagrams (as shown below) or cross-node cross JOIN correlation diagrams can be viewed. The management platform refreshes the parse results at 0 a.m every day, or you can click  to manually refresh the parse results.

Description of vertices and edges in the JOIN correlation diagram:

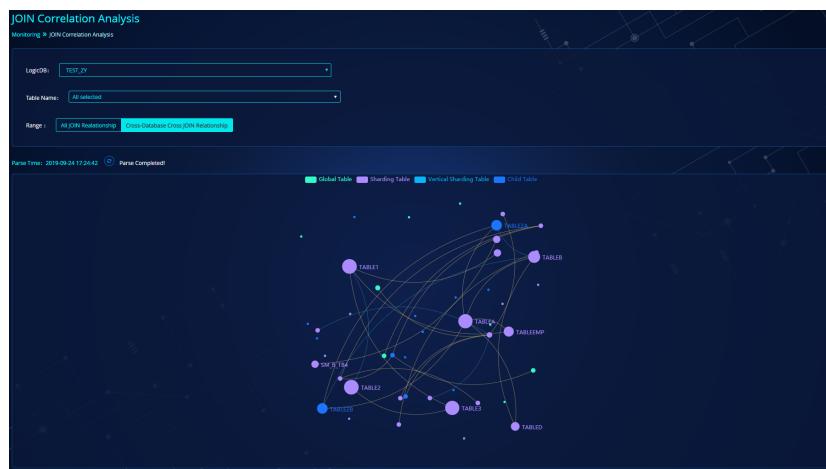
- The vertexes represent tables and are divided into four colors according to the table type ( Global Table  Sharding Table  Vertical Sharding Table  Child Table).
- The edge between vertex A and vertex B represents the JOIN/cross-node no-cross JOIN correlation between table A and table B, and the yellow edge indicates that there is an associated key rather than sharding key in the JOIN correlation.
- The more the total JOIN/total cross-node JOIN queries, the larger the circle of the vertex; when moves the mouse cursor into the vertex, the table name and the total JOIN/total cross-node JOIN queries are displayed;
- Scroll mouse to zoom the JOIN correlation diagram which displays the names of ten tables with the most total JOIN/total cross-node JOIN queries;
- The table without JOIN correlation is displayed as scatter on the diagram, that is, if the table under the currently selected logicDB has no JOIN query or no-cross JOIN query record over cross-nodes, the selected table is displayed as scatter
- Click on the vertex to display the [JOIN Correlation Details](#);



Cross-node cross JOIN query judgment logic:

JOIN query that does not satisfy the following conditions is judged to be a cross-node cross JOIN query (as shown below):

- If the JOIN query is between two sharding tables, the two tables must have the same sharding type and node distribution, and the association conditions use respective sharding key to query, such as `a.shardkey_a=b.shardkey_b`;
- JOIN query between parent table and child table needs an equivalent association condition associated by `join_key`;
- If a global table exists in JOIN query, the node where the global table resides must contain all nodes where other sharding tables reside.
- If there is only a vertical sharding table in JOIN query, the nodes of these tables must be on the same node.



Note: the judgmental logic of the management platform currently is simplified logic. Compared with a specific version of HotDB server, the judgmental results may be different under complex and special circumstances. For example, for the following two types of JOIN queries, the management platform may uniformly determine them to be cross JOIN correlation over cross-nodes, which may be a single-node query based on the value range:

1. The associated key contains the sharding keys of all tables and are equivalent judgements, for example:

```
select * from table01 join table02 on table01.shardcol=1 and table02.shardcol=2
```

Shardcol is the sharding key of two tables. If data values table01.shardcol=1 and thetable02.shardcol=2 share the same node, the JOIN query is a single-database query.

2. In case of associated query of two tables, one is a vertical sharding table and is stored exactly on the associated query condition node of the other table, for example:

```
select * from table01 join table02 on table02.i=10;
```

If all the data of table02.i=10 is stored on the data node dn_01, and table01 is a vertical sharding table also stored on dn_01, the JOIN query is a single-database query.

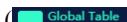
Difference between cross-node cross and cross-node no cross:

- Cross-node cross: JOIN queries require matching computation across data nodes;

- Cross-node no cross: JOIN queries need to be delivered to multiple data nodes, but only need to be computed in the data node. No cross-computation between data nodes is needed.

15.5.3. JOIN correlation details

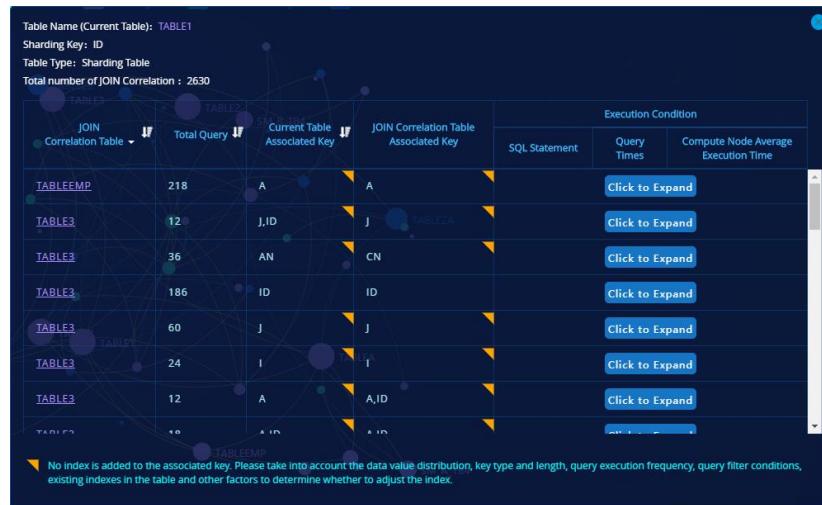
Click on the vertex to display all/cross-node cross JOIN correlation details. This document takes All JOIN correlation details as an example. The table parameters are as follows:

- **JOIN Correlation Table:** A table with a JOIN correlation with the current table. The table name color is consistent with the vertex color according to the table type ( Global Table  Sharding Table  Vertical Sharding Table  Child Table). Click on the table name to jump to the JOIN Correlation Details page for the table.
- **Current Table Association Key:** The associated key of the current table in JOIN query statement. Multiple associated keys are indicated by parentheses, such as (a, b, c).

Associated field description: The table uses the field associated with the JOIN query, for example: SELECT * FROM Persons INNER JOIN Orders ON Persons.id = Orders.oid, then the id is the associated key of Persons, and oid is the associated key of Orders

- **JOIN Correlation Table Association Key:** The associated key of the JOIN correlation table in JOIN query statement. Multiple associated keys are indicated by parentheses, such as (a, b, c).
- **Execution Condition:** The JOIN query statements with identical JOIN correlation table, current table associated key and JOIN correlation table associated key are displayed. Click [Click to Expand] to view the execution details of all collapsed JOIN query statements.
- **Total Query:** The total accumulated queries of the collapsed JOIN query statements.
- **Orange corner mark:** This associated key or this group of associated keys has no index. Please combine the key value distribution, key type and length, query execution frequency, query filter condition, existing index in the table, etc. to

determine whether to adjust the index.



Click [Click to Expand] to view the execution details of all collapsed JOIN query statements. Click on the details under Compute Node Average Execution Time to jump up to the [Slow Query Log Analysis](#) page.



Slow Query Log Analysis

Event: > Slow Query Log Analysis

Please select LogDB: Please select LogDB | Compute Node Average Execution Time: All selected | MySQL Average Execution Time: All selected

SQL Statement Abstract: `SELECT COUNT(*) AS z FROM table1 AS a RIGHT JOIN table2 AS b` | Compute Node Total Execution Times: < | MySQL Total Execution Times: <

Search | More Operations

LogicID	IP	SQL Statement Abstract		Compute Node Execution Condition		MySQL Execution Condition									
		SQL Standard Setting to be Optimized	Optimized SQL	Compute Node Total Execution Time	IF	Compute Node Total Execution Time	IF	Compute Node Average Execution Time	IF	Compute Node Execution Consuming Time	IF	MySQL Total Execution Time	IF	MySQL Average Execution Time	IF
test_zz		SELECT COUNT(*) AS z FROM table1 AS a RIGHT JOIN table2 AS b.		10.30ms	2	5.15ms		7.56ms		3.78ms		Viewing Consuming Time distribution		Viewing Consuming Time distribution	

from 1 to 1 Records from 1 / 1 page

Note: If there is no data at present, please make sure "whether to record SQL execution" is enabled at [Compute Node Parameter Configuration](#) page.
means To-Be-Optimized SQL, and criteria could be adjusted in [\[To Be Optimized SQL Criteria Setting\]](#)

Prev | 1 | Next | Jump to | Go

16. Report

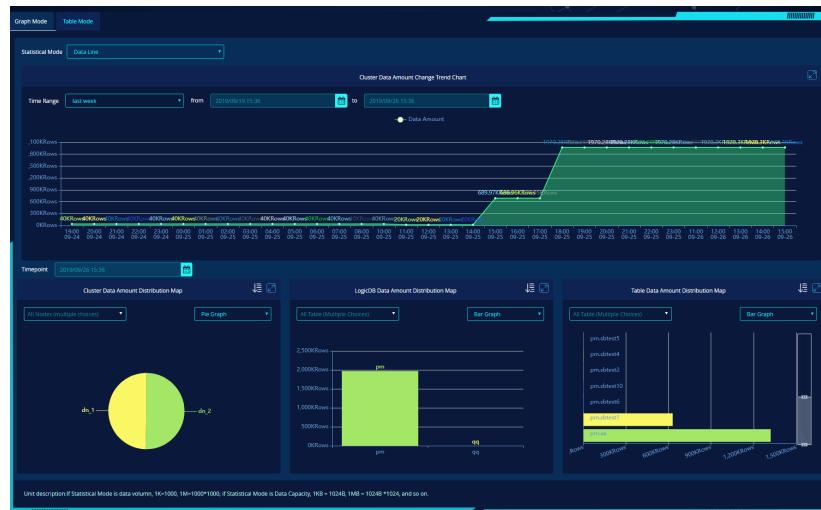
The cluster data volume report, throughput report and connection status report are visualized to provide the graph mode and the table mode, and the data report can be viewed through different dimensions.

16.1. Cluster data volume

The data volume distributions of data nodes, logicDB and tables for all members in the cluster are displayed in graph mode and report mode.

16.1.1. Graph mode

The graph mode has four dimensions. The data volume reports of all members in the cluster are displayed by default. The data volume reports of data nodes, logicDB and tables to be displayed can be selected.



- The default displayed compute node cluster level is divided into 4 graph areas. The data statistics of 4 graph areas are unified, and the statistical mode can be [data row or data capacity](#).

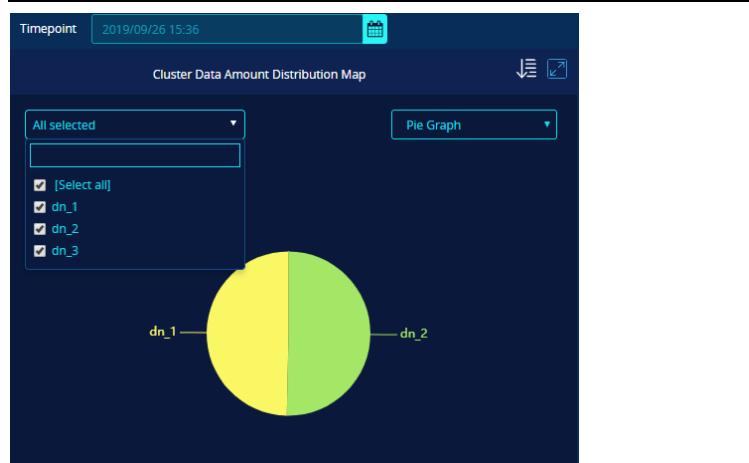
(I) Cluster Data Amount Change Trend Chart



- This chart describes the change trend of data amount in the whole compute node cluster in a certain period of time.
- This chart is a line chart with two coordinate axes for time and data volume respectively.
- The time range options include Last Year, Last Three Months, Last Month, Last Week, Last Day, and Custom. When the time range is less than 7 days, the trend chart is displayed with data collected every hour. When the time range is over 7 days, the trend chart is displayed with data collected at 23:00 per day.
- Cluster Data Amount Change Trend Chart can be enlarged.

(II) Cluster Data Amount Distribution Map





- It depicts the distribution of data volume in the whole compute node cluster in the data node dimension at a certain time point.
- It may be a bar graph or a pie graph which can be switched. The coordinate axes are data node and data volume.
- It supports enlarging the graph to full screen.
- It allows to filter nodes.
- Click on a bar or fan on the map to enter the data volume report at the corresponding data node level.
- Bar graph supports the sorting function, including ascending and descending orders.

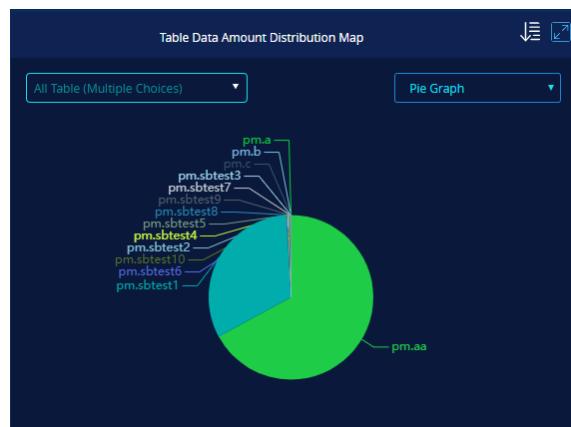
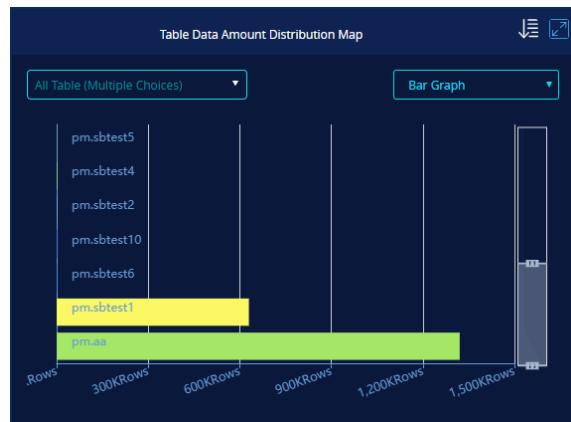
(III) LogicDB Data Amount Distribution Map



- It depicts the distribution of data volume in the whole compute node cluster in the logicDB dimension at a certain time point.
- It may be a bar graph or a pie graph which can be switched. The coordinate axes are logicDB and data volume.
- It supports enlarging the graph to full screen.
- It allows to filter logicDB.
- Click on a bar or fan on the map to enter the data volume report at the corresponding logicDB level.
- Bar graph supports the sorting function, including ascending and descending

orders.

(IV) Table Data Amount Distribution Map



- It depicts the distribution of data volume in the whole compute node cluster in the table dimension at a certain time point.
- It may be a bar graph or a pie graph which can be switched.
- The table name is displayed in the form of [LogicDB name].[table name], which is usually long. The bar graph is horizontal here.
- It supports enlarging the graph to full screen.

- It allows to filter tables.
 - Click on a bar or fan on the map to enter the data volume report at the corresponding table level.
 - Bar graph supports the sorting function, including ascending and descending orders.

16.1.2. Table mode

In addition to the “Graph Mode”, Cluster Data Volume can also view the data distribution of each table under each data node in the whole cluster through the “Table Mode”.

- The interface record can export the table data volume information to the local through the [Export] button. Currently, the file in the “CSV” or “XLS” format can be exported.
 - Statistical modes include: [“Data Row”](#) or [“Data Capacity”](#). When the statistical mode is Data Row, 1K=1000, 1M=1000*1000; when the statistical mode is Data Capacity, 1KB = 1024B, 1MB = 1024B*1024 and so on.
 - If data volume statistics involve the global table, the sum of data volume of all data nodes is counted when calculating at the logicDB dimension, the data volume of each data node is separately counted when calculating at the data node dimension, and the average data volume of the data node where the table reside is counted when calculating at the table dimension.

16.1.3. Statistical mode descriptions

At present, the compute node cluster data volume supports two statistical modes: data row and data capacity. Data row comes from the total number of table rows in information_schema.tables, which is not that precise because the parameter itself is the estimated value; data capacity comes from the total number of data_length in information_schema.tables, which cannot accurately reflect the real data capacity because the parameter is based on the allocated data blocks and is affected by the change of data fill rates in the data block.

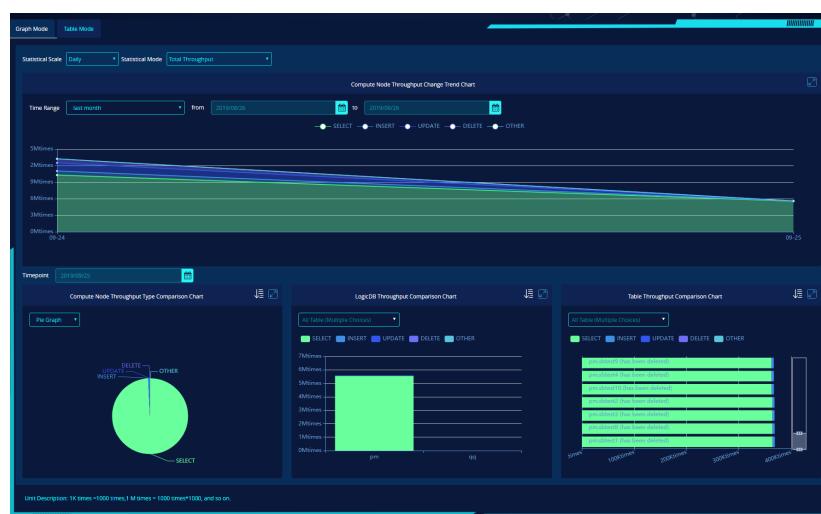
If you need to know the size of real data rows, you can calculate the size of each row according to different data types by yourself and then add them. Such calculation method, however, needs to scan all the data of the whole table, which has high cost and the possibility of affecting the operation of the database.

16.2. Compute node throughput

Compute node throughput is the operations sent by the front-end application to the compute node. Five types of user operations are generally described: SELECT, UPDATE, DELETE, INSERT, and OTHER.

16.2.1. Graph mode

The graph mode has four dimensions, including the whole cluster throughput. The operation type, logicDB, and table throughput can also be displayed.



- The statistical scale and statistical mode of all throughput charts are consistent.
- Statistical scales include: month, day, hour and minute.
- Statistical modes include: total throughput and average throughput rate.

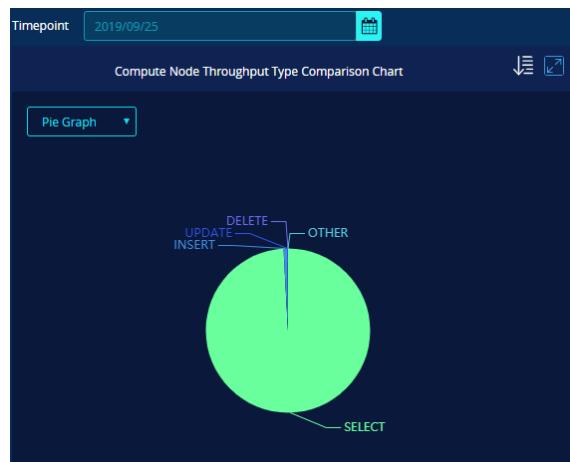
(I) Compute Node Throughput Change Trend Chart



- It describes the change trend of throughput in the whole compute node cluster in a certain period of time and the proportion of each operation in the total throughput.
- This chart is area chart with two coordinate axes for time and throughput respectively. Different color bars in the area indicate the throughput of different operations.
- The time range includes: Last Month, Last Three Months, and Custom.
- When the mouse hovers over a certain point, the throughput data of each operation is displayed. When clicking a point on the chart, the time points of the last three

charts are set to be consistent with the time point.

(III) Compute Node Throughput Type Comparison Chart



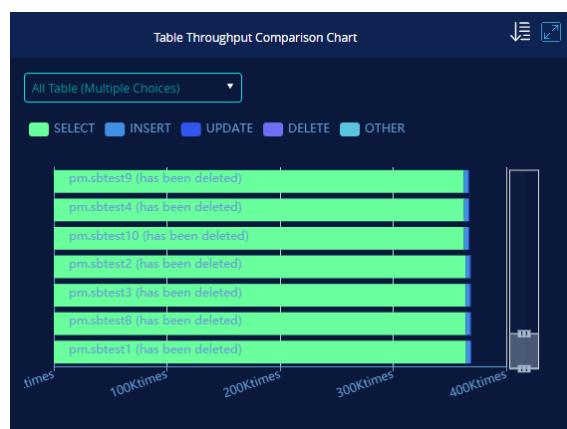
- It describes the proportion of each operation in the throughput of the whole compute node cluster over a period of time.
- It may be a bar graph or a pie graph which can be switched, and is a pie graph by default. The coordinate axes are operation type and throughput.
- The pie chart displays percentage and specific number at the same time.
- It supports enlarging the graph to full screen.
- Bar graph supports the sorting function, including ascending and descending orders.

(III) LogicDB throughput Comparison Chart



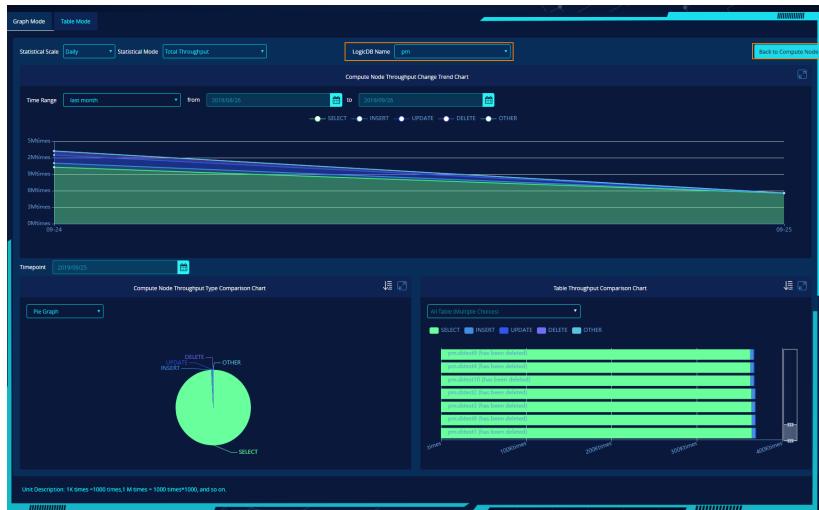
- It describes the comparison of throughput in the whole compute node cluster in the logicDB dimension at a certain time point.
- It is a stacked bar graph with values displayed at each layer. The coordinate axes are logicDB and throughput.
- It supports enlarging the graph to full screen.
- It allows to filter logicDB.
- Click on a bar on the chart to enter the corresponding [LogicDB Dimension Throughput Report](#).
- Bar graph supports the sorting function, including ascending and descending orders. Sorting can be based on the throughput type.

(IV) Table Throughput Comparison Chart



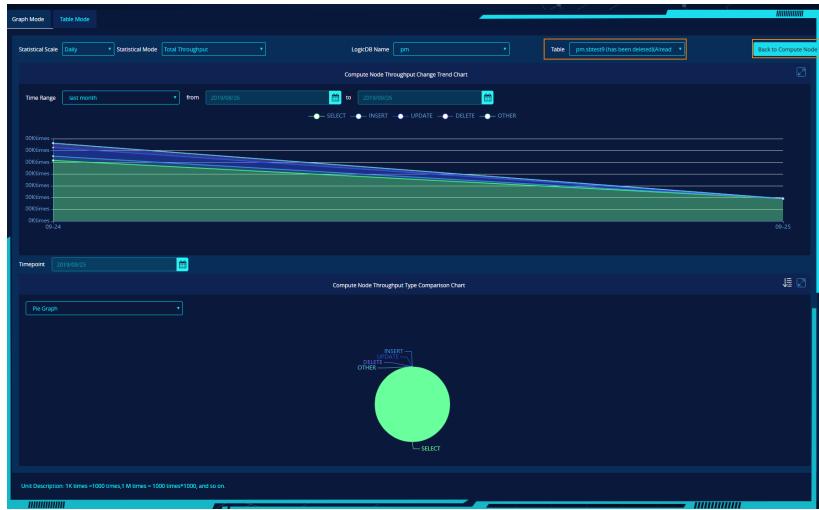
- It describes the comparison of throughput in the whole compute node cluster in the table dimension at a certain time point.
- It is a stacked bar graph with values displayed at each layer. The coordinate axes are table and throughput.
- The table name is displayed in the form of [LogicDB name].[table name].
- It supports enlarging the graph to full screen and allows to filter tables.
- Bar graph supports the sorting function, including ascending and descending orders. Sorting can be based on the throughput type.
- Click on a table bar on the chart to enter the corresponding [Table Dimension Throughput Report](#).

16.2.2. LogicDB Dimension Throughput Report



- LogicDB level is divided into three graph areas. The statistical time scale and statistical mode of the three graph areas are consistent. It supports filtering the logicDB. The [Back to Compute Node View] throughput report button is in the upper right corner.

16.2.3. Table Dimension Throughput Report



- The table level is divided into three graph areas. The statistical time scale and statistical mode of the three graph areas are consistent. It supports switching tables and logicDB through the checkbox. When switching logicDB, it switches to the table with the smallest id under the logicDB by default. The [Back to Compute Node View] throughput report button is in the upper right corner.

16.2.4. Table mode

In addition to the “Graph Mode”, Compute Node Throughput can also view the SELECT, UPDATE, DELETE, INSERT and OTHER operations of each table in the whole cluster through the “Table Mode”.

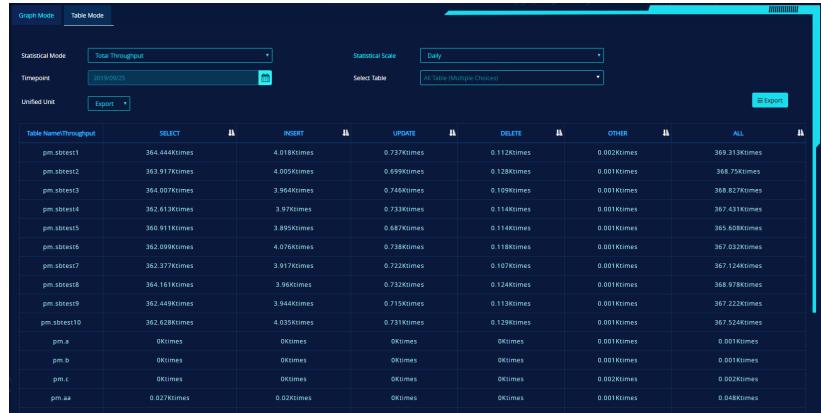


Table Name/Throughput	SELECT	INSERT	UPDATE	DELETE	OTHER	ALL
pm_stress1	364.444Ktimes	4.018Ktimes	0.637Ktimes	0.112Ktimes	0.002Ktimes	369.73Ktimes
pm_stress2	363.917Ktimes	4.005Ktimes	0.639Ktimes	0.128Ktimes	0.001Ktimes	368.75Ktimes
pm_stress3	364.007Ktimes	3.964Ktimes	0.746Ktimes	0.109Ktimes	0.001Ktimes	368.82Ktimes
pm_stress4	362.613Ktimes	3.971Ktimes	0.733Ktimes	0.114Ktimes	0.001Ktimes	367.431Ktimes
pm_stress5	360.911Ktimes	3.895Ktimes	0.687Ktimes	0.115Ktimes	0.001Ktimes	365.608Ktimes
pm_stress6	362.099Ktimes	4.076Ktimes	0.738Ktimes	0.118Ktimes	0.001Ktimes	367.032Ktimes
pm_stress7	362.377Ktimes	3.917Ktimes	0.722Ktimes	0.107Ktimes	0.001Ktimes	367.124Ktimes
pm_stress8	364.161Ktimes	3.965Ktimes	0.732Ktimes	0.124Ktimes	0.001Ktimes	368.978Ktimes
pm_stress9	362.449Ktimes	3.944Ktimes	0.7159Ktimes	0.113Ktimes	0.001Ktimes	367.222Ktimes
pm_stress10	362.628Ktimes	4.035Ktimes	0.731Ktimes	0.125Ktimes	0.001Ktimes	367.524Ktimes
pm_a	0Ktimes	0Ktimes	0Ktimes	0Ktimes	0.001Ktimes	0.001Ktimes
pm_b	0Ktimes	0Ktimes	0Ktimes	0Ktimes	0.001Ktimes	0.001Ktimes
pm_c	0Ktimes	0Ktimes	0Ktimes	0Ktimes	0.002Ktimes	0.002Ktimes
pm_aa	0.027Ktimes	0.020Ktimes	0Ktimes	0Ktimes	0.001Ktimes	0.048Ktimes

- Statistical modes include: total throughput and average throughput rate.
- Statistical scale: month, day, hour and minute.
- Unified units include: adaptive, times, K, M, G.
- CSV and XLS files can be exported.
- The table name is displayed in the form of [LogicDB name].[table name].

16.3. Data node throughput

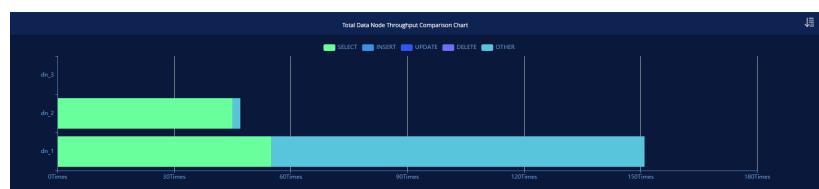
The data node throughput is the operation quantity statistics of the compute node to the data source. Generally, the user operations are described by five types: SELECT, UPDATE, DELETE, INSERT, and OTHER.

16.3.1. Graph mode

The data node throughput graph mode includes five dimensions: data node throughput total comparison graph, data node throughput change trend comparison graph, cluster throughput type comparison graph, logicDB throughput comparison graph, and table throughput comparison graph.



Total Data Node Throughput Comparison Chart



- It describes the total throughput of each node, and only calculates the throughput of master data source under the current data node.
- The operation amount is accumulated from the start of the compute node. The data

is stored in the ConfigDB of the management platform and is retained for 365 days by default. You can adjust the parameter "hotdb.management.dataExpired.day" in the management platform configuration file application.properties.

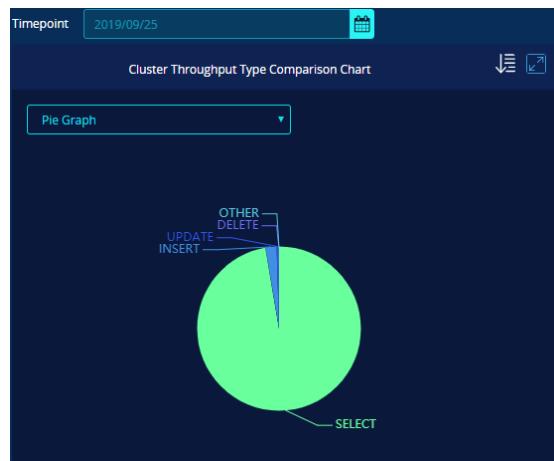
- The throughput of different operation types of each node can be viewed by selecting the operation type.
- It supports enlarging the graph to full screen.

(II) Data Node Throughput Change Trend



- It describes the change trend of throughput of all data nodes in a certain period of time and the proportion of each operation in the total throughput.
- This chart is area chart with two coordinate axes for time and throughput respectively. Different color bars in the area indicate the throughput of different operations.
- The time range includes: Last Month, Last Three Months, and Custom.
- It supports enlarging the graph to full screen.
- When the mouse hovers over a certain point, the throughput data of each operation is displayed.

(III) Cluster Throughput Type Comparison Chart



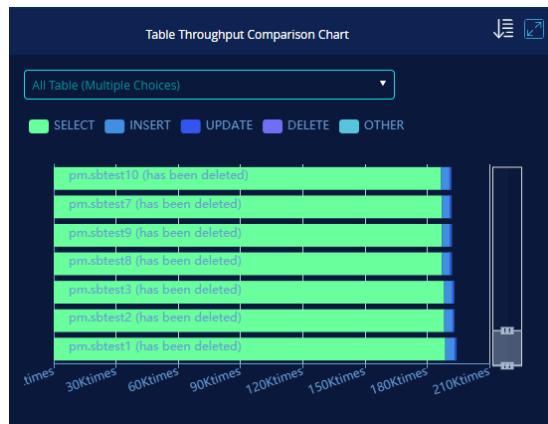
- It describes the proportion of each operation in the throughput of all data nodes at a certain time period.
- It may be a bar graph or a pie graph which can be switched, and is a pie graph by default. The coordinate axes are operation type and throughput.
- The pie graph displays percentage and specific number at the same time.
- It supports enlarging the graph to full screen.
- Bar graph supports the sorting function, including ascending and descending orders.

(IV) LogicDB throughput Comparison Chart



- It describes the comparison of throughput of all data nodes in the logicDB dimension at a certain time point.
- It is a stacked bar graph with values displayed at each layer. The coordinate axes are logicDB and throughput.
- The drag box will be displayed when there are over 8 logicDB.
- It supports enlarging the graph to full screen.
- It allows to filter logicDB.
- Bar graph supports the sorting function, including ascending and descending orders. Sorting can be based on the operation type.

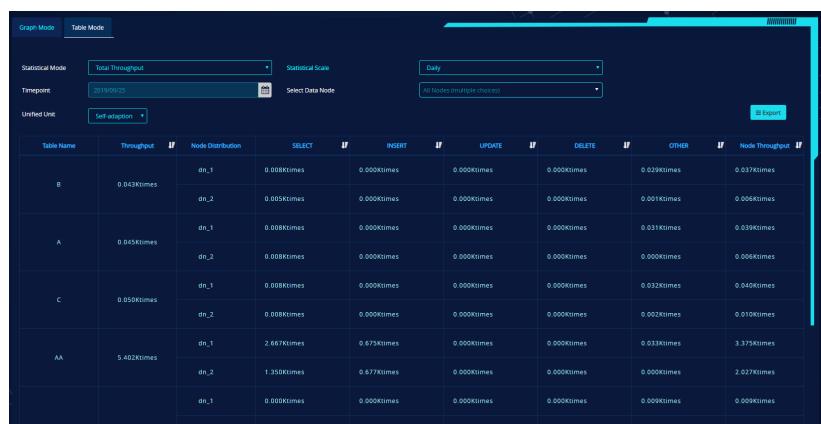
(V) Table Throughput Comparison Chart



- It describes the comparison of throughput of all data nodes in the table dimension at a certain time point.
- It is a stacked bar graph with values displayed at each layer. The coordinate axes are table and throughput.
- The table name is displayed in the form of [LogicDB name].[table name].
- It supports enlarging the graph to full screen.
- It allows to filter tables.
- The global table select throughput only counts one node, and the INSERT, UPDATE, and DELETE operations count all nodes.
- Bar graph supports the sorting function, including ascending and descending orders. Sorting can be based on the operation type.

16.3.2. Table mode

In addition to the “Graph Mode”, Data Node Throughput can also view the SELECT, UPDATE, DELETE, INSERT and OTHER operations of each table in the whole cluster on each node through the “Table Mode”.



The screenshot shows a table mode interface for monitoring database throughput. The top navigation bar includes 'Graph Mode' and 'Table Mode'. Below it, there are sections for 'Statistical Mode' (set to 'Total Throughput') and 'Statistical Scale' (set to 'Daily'). A 'Timepoint' dropdown shows '2019/09/25'. A 'Select Data Node' dropdown is set to 'All Nodes (multiple choices)'. Under 'Unified Unit', 'Self-selection' is chosen. An 'Export' button is visible in the top right.

Table Name	Throughput	Node Distribution	SELECT	INSERT	UPDATE	DELETE	OTHER	Node Throughput
B	0.043Ktimes	dn_1	0.008Ktimes	0.000Ktimes	0.000Ktimes	0.000Ktimes	0.029Ktimes	0.037Ktimes
		dn_2	0.005Ktimes	0.000Ktimes	0.000Ktimes	0.000Ktimes	0.001Ktimes	0.006Ktimes
A	0.045Ktimes	dn_1	0.008Ktimes	0.000Ktimes	0.000Ktimes	0.000Ktimes	0.031Ktimes	0.039Ktimes
		dn_2	0.008Ktimes	0.000Ktimes	0.000Ktimes	0.000Ktimes	0.000Ktimes	0.006Ktimes
C	0.050Ktimes	dn_1	0.008Ktimes	0.000Ktimes	0.000Ktimes	0.000Ktimes	0.032Ktimes	0.040Ktimes
		dn_2	0.008Ktimes	0.000Ktimes	0.000Ktimes	0.000Ktimes	0.002Ktimes	0.010Ktimes
AA	5.402Ktimes	dn_1	2.667Ktimes	0.673Ktimes	0.000Ktimes	0.000Ktimes	0.033Ktimes	3.375Ktimes
		dn_2	1.350Ktimes	0.677Ktimes	0.000Ktimes	0.000Ktimes	0.000Ktimes	2.027Ktimes
			dn_1	0.000Ktimes	0.000Ktimes	0.000Ktimes	0.000Ktimes	0.000Ktimes

- Statistical modes include: total throughput and average throughput rate.
- Statistical scale: month, day, hour and minute.
- Unified units include: adaptive, times, K, M, G.
- CSV and XLS files can be exported.
- The throughput related to global table is counted according to the throughput type. The SELECT counts only one node, and the INSERT, UPDATE and DELETE throughput count all nodes. If a statement involves cross-node throughput, the number of throughput of each node is counted.

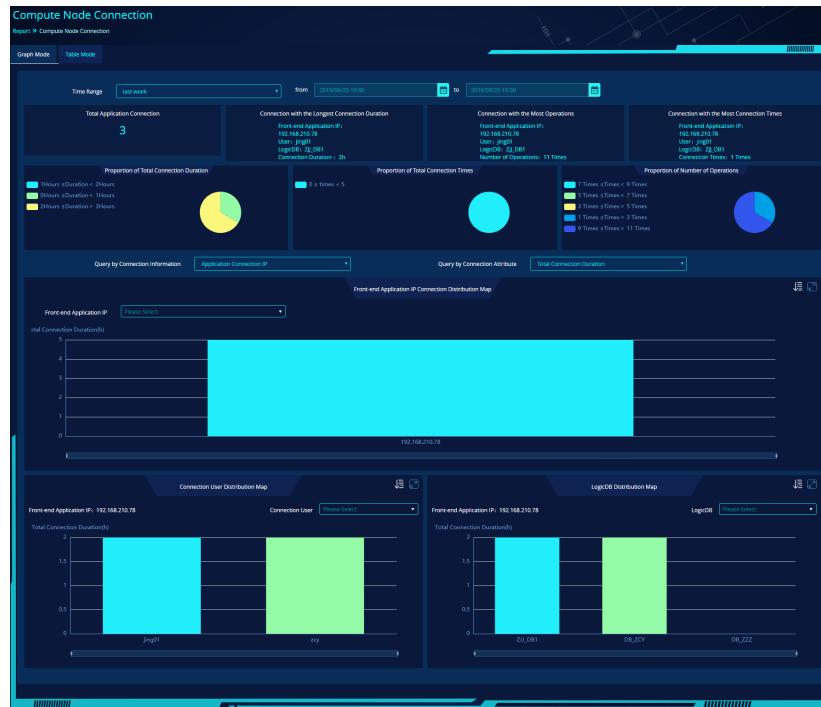
16.4. Compute node connection

The Compute Node Connection Report function displays the status of all connection information associated with the compute node, and records information about the front-end application and user access, such as the number of connections, connection duration, and number of operations.

16.4.1. Graph mode

The graph mode mainly displays the total application connections of the current compute node, three TOP1 connections (connection with the longest connection duration, connection with the most operations, and connection with the most connection times), proportion of total connection duration, proportion of total connection times, proportion of number of operations, front-end application IP connection distribution

map, connection user distribution map, and logicDB distribution map.



- Connections in the selected range can be filtered according to the time range, and all connections in the last three months are displayed by default. This time range is valid for all data in graph mode, and is the primary condition for all query result reports.

Total application connections

- It displays the number of application connections to the compute node currently, and a connection is determined by the front-end application IP + connection user + logicDB (actually use the logicDB).

Connection with the longest connection duration

- It displays the connection with the longest duration of connection to the compute node in all current connections.
- Duration calculation method: In the selected time range, the connection duration

of same connections (consistent IP+connection user+logicDB) is accumulated. If a connection is not ended within the query period, the time at which the query range ends is used as the temporary end time of the connection for statistics.

Note: If the statistical units, that is, IP + LogicDB + connection users are consistent, it will be counted as a connection. Thus, the connection duration of A (this connection has 1000 concurrencies at the same time and each concurrency duration is 1 minute) may be longer than the connection duration of B (this connection has only one concurrency and the concurrency duration is one hour)

Connection with the most operations

- It displays the connection with the most operations (SQL operations sent to compute nodes) in all current connections.
- Operation calculation method: In the selected time range, the operations of same connections (consistent IP+connection user+logicDB) are accumulated. If a connection is not ended within the query period, the time at which the query range ends is used as the temporary end time of the connection for statistics.

Connection with the most connection times

- It displays the connection with the most times of connection to compute nodes (1 connection is the period from establishment to end) in all current connections.
- Connection times calculation method: In the selected time range, the same connections (consistent IP+connection user+logicDB) are accumulated to obtain the connection with the most connection times. If a connection is not ended within the query period, it will be counted as one connection.

Proportion of total connection duration

- It analyzes the proportion of connection duration of all connections within the query time range.
- Calculation method for proportion of total connection duration: In the connection data within the query time range, take the maximum and minimum connection duration (accumulated value of same connections), and then divide the difference between the maximum duration and the minimum duration into 5 equal parts to calculate the proportion of connections in each interval in the total connection.

For example:

Time interval selection: 2018-10-10:00 to 2018-10-11:10:00,

After the same connection information is merged, the total application connection is: 50

Maximum connection duration, 40s, minimum connection duration: 5s, the difference is divided into 5 equal parts (5-11s, 12-18s, 19-25s, 26-32s, 33-40s), i.e. 5 equal-scale dimensions (maximum connection times and maximum operations are the same, and the difference is divided into 5 equal parts)

5-11s connection: 5, proportion: $5 \div 50 = 10\%$

12-18s, 20, proportion: $20 \div 50 = 40\%$

19-25s: 8, proportion: $8 \div 50 = 16\%$

26-32s: 7, proportion: $7 \div 50 = 14\%$

33-40s: 10, proportion: $20 \div 50 = 20\%$

The proportions are obtained according to the properties of each connection information in the same manner

Proportion of total connection times

- It analyzes the proportion of connection times of all connections within the query time range.
- Calculation method for proportion of connection times: In the connection data within the query time range, take the maximum and minimum connection times (accumulated value of same connections), and then divide the difference between the maximum times and the minimum times into 5 equal parts to calculate the proportion of connection times in each interval.

Proportion of number of operations

- It analyzes the proportion of number of operations of all connections within the query time range.
- Calculation method for proportion of number of operations: In the connection data within the query time range, take the maximum and minimum number of operations (accumulated value of same connections), and then divide the difference between the maximum number of operations and the minimum number

of operations into 5 equal parts to calculate the proportion of number of operations in each interval.

Front-end application IP connection distribution map

- It displays the IPs of application connections to the compute nodes within the query time range. When there are too many IP addresses, drag the bottom drag bar to display more. IP distribution information can also be viewed by the Enlarge button or sorting.
- The X-axis displays “Application Connection IP” by default. The horizontal coordinate can be switched to the “Connection User” or “LogicDB” dimension through the “Query by Connection Information” filter box. When modifying the X-axis to view dimensions, the chart title will also be switched accordingly.
- The Y-axis displays “Total Connection Duration” by default. The vertical coordinate can be switched to the “Total Connection Times” or “Operation Times” dimension through the “Query by Connection Properties” filter box. Switching the filter box will change the Y-axis display dimension of bottom secondary charts.
- Click the specific bar in the icon to link with the display effect of bottom secondary charts “Connection User Distribution Map” and “LogicDB Distribution Map”. For example, when clicking on the application connection IP “192.168.200.30”, the bottom “Connection User Distribution Map” displays the connection users used for clicking the IP, and the “LogicDB Distribution Map” displays the logicDB used for clicking the IP.

Connection user distribution map

- The user distribution of the first application connection IP (when the X axis of the chart above is the “Application Connection IP” dimension) is displayed by default. Click on the specific IP bar above to view the user distribution of other application connection IP.
- The displayed connection users can be filtered and viewed, or the information to be viewed can be displayed by sorting and enlarging.
- The chart title of this module will change with the switch of filter box “Query by Connection Information”.

LogicDB distribution map

- The logicDB distribution of the first application connection IP (when the X axis of the primary chart is the “Application Connection IP” dimension) is displayed by default, that is, the logicDB connected in the IP.
- The displayed connection users can be filtered and viewed, or the information to be viewed can be displayed by sorting and enlarging.
- The chart title of this module will change with the switch of filter box “Query by Connection Information”.

16.4.2. Table mode

In addition to displaying connection information in graph mode, the details of each connection can be viewed in table mode and can be exported for local storage.

Compute Node Connection									
Report > Compute Node Connection									
Graph Mode		Table Mode							
Compute Node	IP	Front-end Application IP	Connection User	LogicDB	Total Connection Duration	Total Connection Times	Number of Operations	Final Connection Close Time	Active or not?
Active or not?	All selected	Time Range	recent three months	from 2019/09/20 10:00 to 2019/09/25 10:00	Export	Print	Copy	Reset	Print
HotDB_78	192.168.210.78	zxy	DB_ZCY	0Hours	1 Times	9 Times	2019-09-11 19:02:18	2019-09-11 19:02:18	No
HotDB_78	192.168.210.78	zcy	DB_JZZ	0Hours	1 Times	1 Times	2019-09-11 16:09:35	2019-09-11 16:09:35	No
HotDB_78	192.168.210.78	jmg01	ZJ_DB1	2Hours	1 Times	11 Times	2019-09-11 19:02:18	2019-09-11 19:02:18	No

- The record displayed is the front-end application information (IP+Connection User+LogicDB Identification) of each connection to compute nodes, and the same connection information is aggregated into one.
- The multi-node mode cluster supports querying the compute node service through which each connection connects to the logicDB.
- All data in the report is saved for up to one year by default, and the connection data information of more than one year is automatically cleared.
- In the table mode, the current survival status of each connection can be viewed.

17. Management

The management menu mainly provides the functions for managing business data, such as backup and recovery of data or execution of DDL statements of business tables.

17.1. Data backup

Data backup is a disaster recovery backup function for business data to ensure that the data backup can be restored in case of data loss or damage. At present, the data backup function needs to rely on the backup function HotDB Backup self-developed by Hotpu, and only supports logical backup currently.

17.1.1. Introduction to HotDB Backup

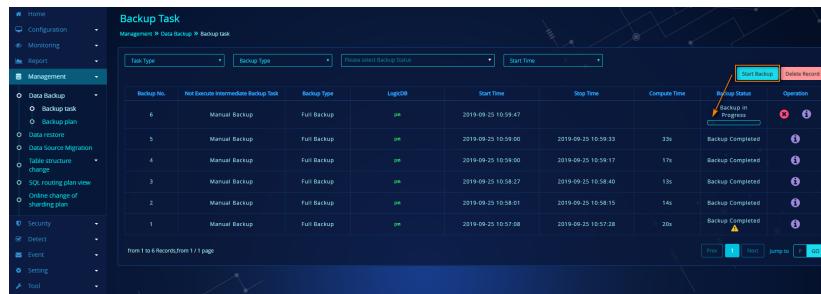
MySQL's own mysqldump tool exports multiple tables in turn through a single-thread work, but it lacks a parallel mechanism, which makes it impossible to back up data quickly. As a utility tool, mydumper can support multi-threaded work well, and can read data in parallel multi-threaded tables and write data to different files at the same time, which makes it faster than traditional mysqldump in processing speed. One of the functions of mydumper is that the list needs to be locked during processing, so if we need to perform backup work during the working hours, the DML blocking will occur. But generally MySQL now has master and slave, and most of the backups are performed on standby slave, so the lock problem can be ignored and mydumper can better complete the backup task. There is also a local program similar to mydumper in HotDB Server. Each data node uses this program to listen for requests from HotDB-Management and complete data backup. The program is called "HotDB Backup".

17.1.2. Installation description

To use the data backup function of HotDB Management, it needs to install the HotDB Backup program on the server where the backed-up data source reside. For the installation and deployment of HotDB Backup, please refer to the backup program deployment chapter of Distributed Transactional Database HotDB Server [Installation and Deployment] Function Manual.

17.1.3. Manual backup

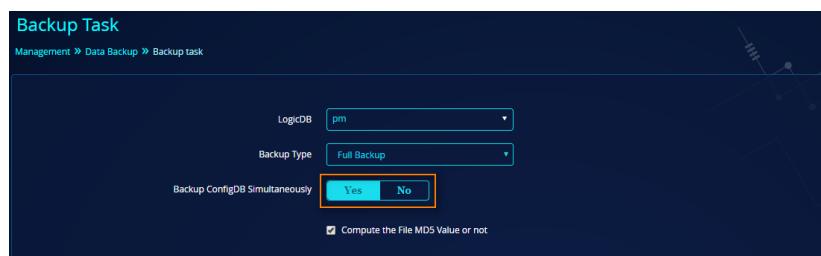
(I) Start backup



Backup No.	Not Execute Intermediate Backup Task	Backup Type	LogicDB	Start Time	Stop Time	Compute Time	Backup Status	Operation
6	Manual Backup	Full Backup	pm	2019-09-25 10:59:47			Backup in Progress	Stop
5	Manual Backup	Full Backup	pm	2019-09-25 10:59:00	2019-09-25 10:59:33	33s	Backup Completed	View
4	Manual Backup	Full Backup	pm	2019-09-25 10:58:00	2019-09-25 10:59:17	17s	Backup Completed	View
3	Manual Backup	Full Backup	pm	2019-09-25 10:58:27	2019-09-25 10:58:40	13s	Backup Completed	View
2	Manual Backup	Full Backup	pm	2019-09-25 10:58:01	2019-09-25 10:58:15	14s	Backup Completed	View
1	Manual Backup	Full Backup	pm	2019-09-25 10:57:08	2019-09-25 10:57:28	20s	Backup Completed	View

- Click “Manage -> Data Backup -> Backup Task -> [Start Backup]” to manually start a backup task.

(II) Select backup method



Backup Task

Management > Data Backup > Backup task

LogicDB: pm

Backup Type: Full Backup

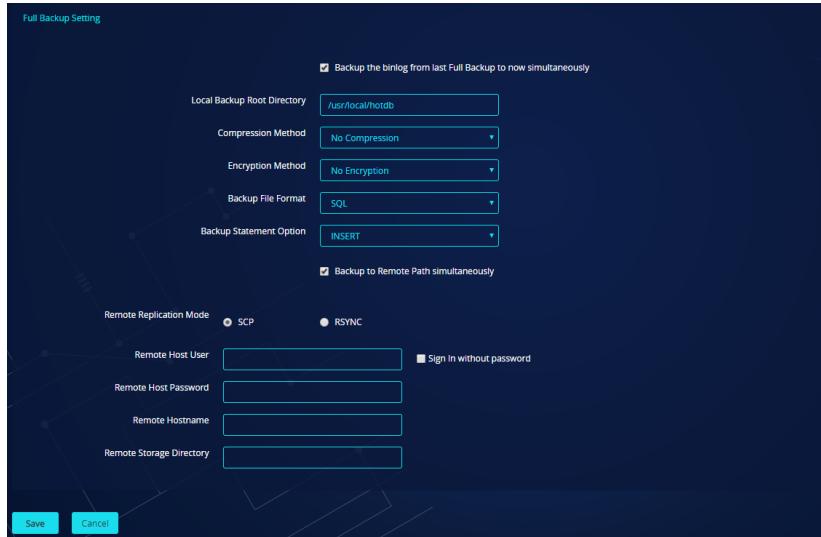
Backup ConfigDB Simultaneously: Yes

Compute the File MD5 Value or not

- LogicDB: Backup is performed in unit of logicDB, and one or more logicDB can be selected for backup at a time.
- Backup Type: Full Backup and Incremental Backup. “Full Backup” is to backup all data in the current logicDB, and “Incremental Backup” is to continue backing up the new binlog based on the last full or incremental backup. Note: In the first incremental backup, it needs to ensure that the logicDB to be backed up has had a full backup, otherwise the incremental backup cannot be started.
- Backup logicDB simultaneously: When the backup is started, the configDB data backup is performed once, with the same effect as manual backup in the “Config Data Backup & Restore”.
- Compute the File MD5 Value or not: It is checked by default, and mainly records

the MD5 value of backup file to facilitate the comparison of file MD5 values during data recovery to ensure the integrity and consistency of data.

(III) Backup setting



- **Backup the binlog from last Full Backup to now simultaneously:** It is checked by default, and is used to backup the binlog from last full backup to the current full backup. Note: This is an insurance measure, but the last full backup will not be found during the first full backup, so this option is meaningless for the first full backup.
- **Local Backup Root Directory:** It is the local directory of the server where each data source resides and backup file is stored. This directory needs to be created in advance on the server where each node resides, and the directory of each server shall be consistent. Otherwise, the backup fails and the backup failure message prompts: Failed to create backup directory.

Tip: when the data is backed up under different directories due to different hardware specifications and configuration methods of servers, you can use the soft link to unify the directories used for backup.

- **Compression Method:** It is used to control whether the backup file is compressed, with options of No Compression, ZLIB Flow Compression, and LZ4

Compression. LZ4 compression is to first output the file and then call the system compression operation command.

- Encryption Method: It is used to control whether the backup file is encrypted, with options of No Encryption, 3DES, and AES. When selecting other encryption methods, it needs to enter the encryption password which is used for decryption in data recovery.
- Backup File Format: It is used to control the data format of backup file, and is divided into SQL, MySQL CSV and standard CSV. The default format is SQL.
Note: The standard CSV format is mainly used for data exchange with other systems, such as exporting data to Hadoop, but it does not support recovery currently.
- Backup Statement Option: When the backup file format is SQL, the SQL to be backed up can be in the insert, insert ignore or replace form.
- Backup to Remote Path Simultaneously: The backup file can be transferred to a remote server. It is not checked by default. When backing up to a remote server, all backup files are merged and transferred to the specified directory on the remote server.
- Remote Replication Mode: it is divided into: SCP and RSYNC. It is recommended to use the SCP mode. If RSYNC is used, it shall be deployed on a remote server.
- Remote Replication IP, User and Password: Fill in the information of the actual remote server.
- Remote Backup File Root Directory: The directory for storing backup files shall be filled out according to the actual situation, but it needs to be created in advance.

(IV) Backup task record

Backup Task								
Management > Data Backup > Backup task								
Task Type	Backup Type	LogicDB	Start Time	Stop Time	Compute Time	Backup Status	Operation	
7	Manual Backup	Incremental Backup	pm	2019-09-25 11:04:32	2019-09-25 11:04:48	16s	Backup Completed	
6	Manual Backup	Full Backup	pm	2019-09-25 10:59:47	2019-09-25 11:00:09	22s	Backup Completed	
5	Manual Backup	Full Backup	pm	2019-09-25 10:59:00	2019-09-25 10:59:33	33s	Backup Completed	
4	Manual Backup	Full Backup	pm	2019-09-25 10:59:00	2019-09-25 10:59:17	17s	Backup Completed	
3	Manual Backup	Full Backup	pm	2019-09-25 10:58:27	2019-09-25 10:58:40	13s	Backup Completed	
2	Manual Backup	Full Backup	pm	2019-09-25 10:58:01	2019-09-25 10:58:15	14s	Backup Completed	
1	Manual Backup	Full Backup	pm	2019-09-25 10:57:08	2019-09-25 10:57:28	20s	Backup Completed	

- The backup task completed or being executed are displayed on the Backup Task page.
- Backup sequence number: unique identification of each backup task
- Task type: displays whether the backup task is a manual backup or a scheduled backup
- Backup type: displays whether the backup task is an incremental backup or a complete backup
- LogicDB: displays which LogicDB are to be backed up
- Start time: displays the start time of backup task
- End time: displays the end time of the backup task. If the backup task is not completed, the expected end time will be displayed
- Total time consumption: displays the time consumption of backup task
- Backup status: displays the status of the current backup task, including backup failed, backup invalid, backup completed, backup in progress, cancelling, manually cancelled, automatically cancelled, and delayed. The backup task being executed will display the backup progress in the form of progress bar.
- Operation: click "details" to display the backup details of the current backup task, failure reason, etc.
- Failed and invalid backup will be displayed in the backup list with the and marks. When moving the mouse cursor to them, the specific reason will be displayed.

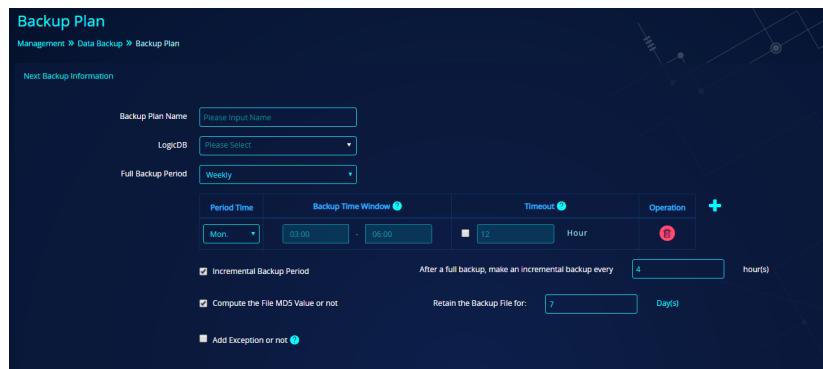
- Click [Delete Record] to delete the backup record on the page. Whether the backup file in the server is deleted simultaneously can also be checked, but the backup file on the remote server will not be deleted. (for example, setting up a backup to a remote server).

17.1.4. Backup plan

The backup plan can set periodical backup task for HotDB Management. After setting the periodical backup plan, all backup tasks are performed by the periodical plan on time without manually starting the backup task.



(I) Add backup plan



- Click “Manage -> Data Backup -> Backup Plan -> [Add New Plan] in HotDB Management to enter the Add Backup Plan page.
- Backup Plan Name: Users can set the backup plan name which shall not be same as the existing backup plan name.
- LogicDB: The logicDB needs to be backed up in periodical backup. One or more logicDB can be selected for backup.
- Full Backup Period: Users can select the full backup period based on actual

business needs.

- After the “Full Backup Period” is selected, detailed settings such as “Period Time: Date of Specific Full Backup”, “Backup Window Period: Time Range of Backup Start”, and “Timeout: If the backup task is not completed within the set time, the backup will be canceled automatically and it needs to be checked to take effect” can be performed on full backup.
- Incremental Backup Period: It is checked by default. If not, the backup plan only performs full backup and no incremental backup will be performed.
- Incremental backup execution time can be set, and an incremental backup is executed after 4 hours of full backup by default.
- Backup File Retention: The retention time of backup file in the server directory can be set, which is 7 days by default.

Notes on “Backup File Retention”

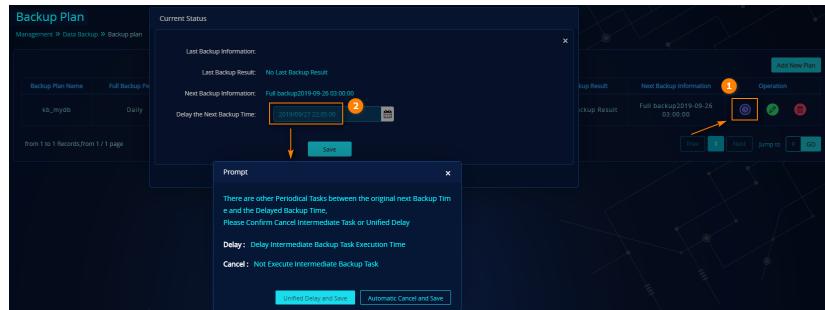
- (1) The file retention period is only for scheduled backups (i.e. for manual backups, the backup file will not be deleted).
- (2) The file retention period is the retention time of the backup file. The backup record will not be deleted accordingly.
- (3) The scheduled task is executed at 0:00 every day. When the backup is deleted, a full backup will be reserved, that is, it does not fully match the time (for example, if the retention period is 24 hours, a full backup A which is greater than or equal to 24 hours will be found, and all automatic backup files before A will be deleted).

- Add Exception or not: Exceptions for backup can be set in the periodical backup plan. For example, if a periodical plan executes a full back at 0:00 a.m. every morning and executes an incremental backup every 4 hours, but xxx is set as an exception, the backup plan will not be executed on that day.
- Backup Setting: For details, please refer to the “Backup Setting” description in “Manual Backup”.

(II) Specific setting instructions for backup plan

- Backup plan can set timeout cancellation or add exceptions (no backup plan is executed).

- The added backup plan can postpone the “next backup task”. Click “Management -> Data Backup -> Backup Plan -> Page Record [Delay the Next Backup Time]” to set the execution delay time.
- After setting [Delay the Next Backup Time], the program will automatically check “whether there are periodical backup tasks between the last backup task completion time and the next task delay time”. If there is no interval, successful modification will be prompted directly. If there are periodical backup tasks, a prompt will pop up to inform the user as shown below:



- Click [Unified Delay and Save] to set the periodical task to the delay state in the background. When the next backup task is completed, the periodical task will be executed according to the set backup period. After clicking [Automatic Cancel and Save], the periodical task will be canceled by default and the backup task will not be executed in the background.
- After the delayed backup task is completed, the backup type recorded on the page is “Delayed Completion”.

17.1.5. Special instructions for backup

When the backup task is enabled, if there is a long-lived transaction (that is, a long uncommitted transaction and an operation statement that has been executed for a long time) in the backed up data source, the backup will not be started immediately, and will be executed after the long-lived transaction retry mechanism is completed.

- If the current data source page is not configured with a backup user account, the backup will use the data source connection account for backup. When the backup

is completed, it will prompt: “The current backup uses the connection account, please add a dedicated backup account on the data source configuration page”.

- Example of statement created by backup user:

```
GRANT
SELECT,INSERT,UPDATE,DELETE,CREATE,DROP,INDEX,ALTER,RELOAD,PROCESS,REFERENCES,
SUPER,LOCK TABLES,REPLICATION SLAVE,REPLICATION CLIENT,TRIGGER,display VIEW,CREATE
VIEW,CREATE ROUTINE,ALTER ROUTINE,EVENT ON *.* TO 'DBBACKUP'@'127.0.0.1' IDENTIFIED
BY 'DBBACKUP';
```

Note: Data source instances deployed by HotDB Management generate DBBACKUP users by default, needing no special creation.

- All backup files are stored in the backup directory by the backup task ID. The file directories are: Backup Task ID -> Data Source Name -> Database Name -> Table Data/Table Definition Statement. In each backup, in addition to the data, my.cnf, account and privilege data are backed up simultaneously and stored in the same directory of data source. The data and table definition statements are stored in the lower directory of data source.
- The backup task is performed on the master data source being used by the current node. When the data source is switched, the backup object will also be switched. But since only the active master is backed up and the standby slave is not backed up, the incremental backup on standby slave cannot be executed until a full backup is available.
- If the My.cnf file is backed up, it shall exist in any of the following paths: /etc/my.cnf, /etc/mysql/my.cnf and /usr/etc/my.cnf, otherwise the configuration file cannot be backed up.
- HotDB-Backup does not need to be restarted when closing or restarting HotDB-Management.
- The reasons for backup failure include but are not limited to:

```
Backup file directory does not exist
```

HotDB-Backup program is not deployed or started

Data source user privilege for backup node is insufficient

There are other backup tasks in progress

User, password and server IP information of the remote backup are incorrect

The server where the node backed up is not installed with RSYNC

The server backed up has no free disk space or no sufficient disk space

Data source cannot be connected

➤ The reasons for backup failure include but are not limited to:

Modify the data source name, hostname, port and database

Modify the table name, logicDB, table type, sharding key, sharding mode and data node of undefined tables

Modify the sharding function that has been applied to the table and add route information (that is, modify the sharding function of defined/undefined tables)

Modify the default node of the logicDB (that is, the default node that affects automatic table creation)

Add a new table, and the table introduces nodes not included in the previous backup

Modify defined tables by online modification of the sharding plan

DDL executed by the table automatically created through automatic table creation statement or setting default data node in logicDB to bypass the management platform

(CREATE \ ALTER \ DROP \ TRUNCATE \ RENAME) operation

17.1.6. Backup log description

Start backup means to start the backup task.

Backup is stopped means that the backup task is stopped.

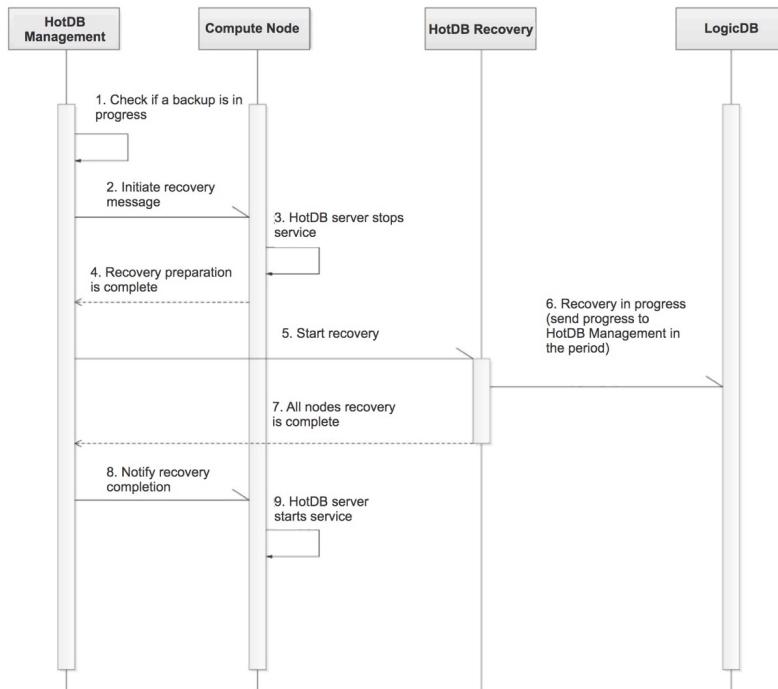
Connected to server successfully! means that connection is established normally between backup program and Management.

Get a quit signal from user, will quit after backup is finished means that the backup program quits normally.

17.2. Data restore

When business data is damaged or lost, Data Restore function can be used to restore the backed up data to a damaged or lost logicDB.

Data restore sequence diagram:



17.2.1. Start restore

The screenshot shows the 'Start Restore' interface. At the top, there's a breadcrumb navigation: Management > Data Restore > Start Restore. Below it, there are several dropdown menus and input fields:

- LogicDB requiring Restore:** A dropdown menu showing "LogicDB (Multiple Choices)".
- Restorable Timepoint:** A dropdown menu showing "Please Select Timepoint". To its right is a checkbox labeled "Restore to the customized time point" with a question mark icon.
- Full Backup to be used:** A dropdown menu showing "Please Select Full Backup to be used".
- Incremental Backup to be used in Restore:** A large empty rectangular box.
- Whether to conduct DROF Operation to the Restored Table before Restore?**: A checkbox with a question mark icon.
- Full Backup File Encryption Method:** A dropdown menu showing "No Encryption".

At the bottom left are two buttons: "Start Restore" and "Return".

(I) Start instructions

- Click “Data Management -> Data Restore -> [Start Restore]” to jump to the data restore page.
- For data security reasons, if there is no data backup for more than 3 h before the restore is started, the user will be informed whether to execute a backup immediately. If a backup is needed, it will jump to the backup window for Manual Backup first.

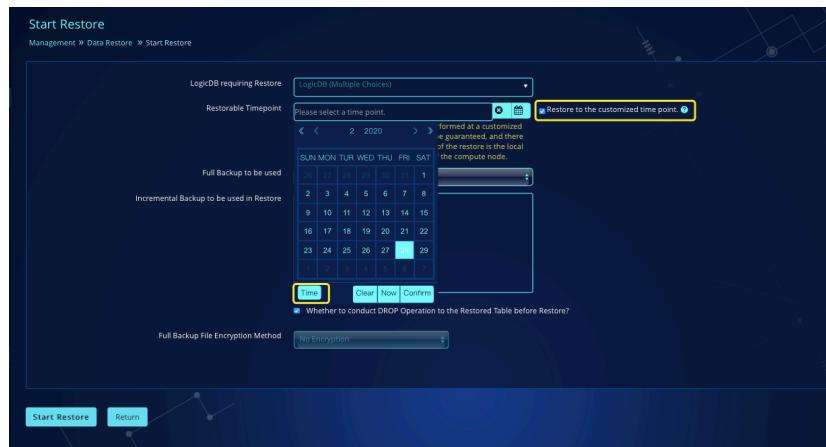
(II) Page description

- LogicDB: One or more logicDB can be selected to restore.
- Restorable Timepoint: the backup time point that can be restored. Hotdb Management calculates the target time interval that can be restored currently according to the backup file information of the corresponding logicDB recorded, that is, the time point when the backup of logicDB is successful and not cleaned up (excluding the backup that is invalid due to lonfigDB modification).
- You can also select to restore to any restorable time point after selecting "restore to the user-defined time point". For details, please refer to (III) restore to the user-defined time point.
- Full Backup to be Used: the file information that can be restored, which is the

latest full backup file by default. Deleted or invalid files are not displayed (backup files shall be fully consistent with the logicDB).

- Incremental Backup to be used in Restore: Calculate the incremental backup to be used based on the selected restore time point and the full backup to be used selected by users. If there are multiple incremental backups, the latest incremental backup is displayed by default.
- Whether to Conduct Drop Operation for the Restored Table before Restore: It is checked by default, otherwise the restored table shall be deleted manually. If restore is executed directly without checking this option and deleting the restored table manually, users will be prompted that the table already exists.
- Full Backup File Encryption Method: Unencrypted, 3DES and AES. By default, it will be the encryption method used in full backup.
- Full Backup File Encryption Key: It is not displayed when the encryption method is Unencrypted.

(III) Restore to the user-defined time point



- After selecting "restore to the user-defined time point", select any time point within the restorable time range through the second-level time selector. The restorable time range is from the earliest time point when the current LogicDB backup succeeds and has not been cleared till the latest time point.

- If the selected time point can only correspond to one full backup, while it is within the restorable time range, it can only be restored to the time of full backup instead of the specified time.
- If the cluster is non-XA cluster, when it is restored to the user-defined time point, data consistency is not guaranteed, and there may be half a transaction, and the restore end point is the local time of each node rather than the time of the compute node. It is recommended to use this function only in clusters with XA transaction enabled.
- When a user-defined time point is selected, the full backup and incremental backup used for restore will be automatically filled. Click [start restore] to restore to the user-defined time point.

17.2.2. Instructions for executing data restore



Restore Start Time	Stop Time	Restore Point	Operator	LogIDB	Task Status	Consuming Time	Operation
2019-09-25 11:26:05	Estimated end time: 2019-09-25 11:26:46	2019-09-25 11:04:32.0	Bob	#	Restore in Progress	0min	Start
2019-09-25 11:25:09	2019-09-25 11:25:36	2019-09-25 11:04:32.0	Bob	#	Restore Successful	0min	Start

From 1 to 2 Records / 1 / 1 page

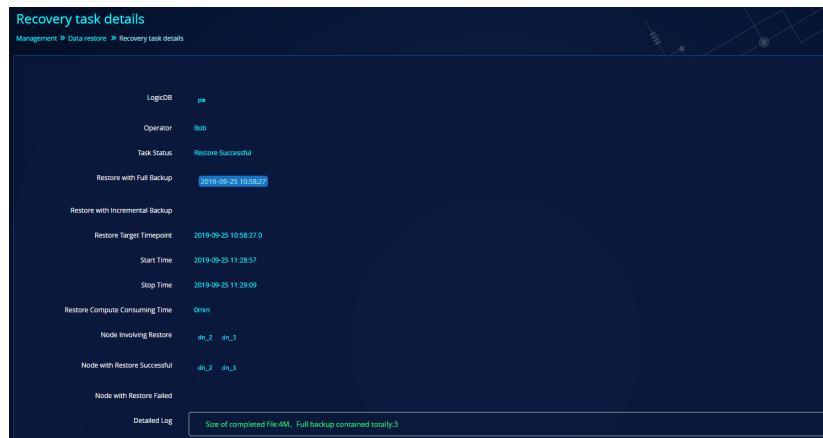
```
[root@datasource_ms logs]# ll
total 0
-rw-r--r-- 1 root root 0 Sep 25 11:28 hotdb_backup.log
[root@datasource_ms logs]# tailf hotdb_backup.log
Wed Sep 25 11:28:59 2019 [INFO] Initialize recovery [id: 3]
Wed Sep 25 11:28:59 2019 [INFO] Start recovery
Wed Sep 25 11:28:59 2019 [INFO] 192.168.210.41_3307_db253_en: Recovery start
Wed Sep 25 11:28:59 2019 [INFO] 192.168.210.41_3307_db253_en: Start full recovery
Wed Sep 25 11:28:59 2019 [INFO] 192.168.210.41_3307_db253_en: Recovery table data from SQL files
Wed Sep 25 11:29:01 2019 [INFO] 192.168.210.41_3307_db253_en: Recovery finished
Wed Sep 25 11:29:03 2019 [INFO] Recovery is stopped
```

- Input the correct restore information into the restore page, and jump to the restore page after submitting the restore task. The task status displays Restore in Progress and the restore process update. If the deletion operation is triggered at this time, it prompts “Restore in Progress, Cannot be Deleted”.
- The compute node will suspend the service during the restore period and restart the service automatically after the restore. (If the restore fails halfway, the compute node service needs to be started manually.)
- All ongoing transactions are rolled back before the compute node service is

stopped on restore.

- The corresponding tables under the database is parsed when starting restore, except for tables have been restored (the backup logicDB has data source crossing), and the heartbeat table will be restored.
- If a data node with SQL execution errors occurs in restore, all data sources under the data node are unavailable and require manual intervention by DBA.
- Backups all follow the data source being used currently. If the data source is switched during the restore process, the current restore task will be marked as failed. Data restore can only be performed after the original failed data source is restored, in the absence of a new full backup.
- If the configDB is backed up when backing up, the configDB is not restored in restore operation.

17.2.3. Recovery task details



Recovery task details	
Management	> Data restore > Recovery task details
LogicDB	pb
Operator	Bob
Task Status	Restore Successful
Restore with Full Backup	2019-09-25 10:58:27
Restore with Incremental Backup	
Restore Target Timepoint	2019-09-25 10:58:27.0
Start Time	2019-09-25 11:28:57
Stop Time	2019-09-25 11:29:09
Restore Complete Consuming Time	0min
Node Involving Restore	dn_2 dn_3
Node with Restore Successful	dn_2 dn_3
Node with Restore Failed	
Detailed Log	Size of completed file-4M, Full backup contained totally-3

Completed data recovery tasks can be viewed for recovery task details.

- LogicDB: The logicDB included in the recovery.
- Operator: HotDB Management user who Starts the recovery task.
- Task Status: including Restore in Progress, Restore Succeeded, and Restore Failed.
- Restore with Full Backup: Full backup information restored for use. Click the time

link to jump to the corresponding Backup Task Details page.

- Restore with Incremental Backup: Incremental backup information restored for use. Click the time link to jump to the corresponding Incremental Backup Task Details page.
- Restore Target Timepoint: It displays the restore target timepoint.
- Start Time: The start time of recovery task.
- Stop Time: The stop/failure time of the task. The ongoing task does not display the time.
- Restore Compute Consuming Time: Time consumed for restore.
- Node Involving Restore: The data nodes affected by the recovery are displayed with a list of data node names.
- Node with Successful Restore: The successfully restored data nodes are displayed with a list of data node names.
- Node with Failed Restore: The data nodes that failed to restore are displayed with a list of data node names. Data sources under failed data nodes will be set unavailable.
- Detailed Log: The restore log page displays the restore details. If there is an error in restore, the error details will be displayed.
- If the task is in progress, the data will be refreshed regularly at a frequency of 30s/time.

17.2.4. Special instructions for data restore

- Attention shall be paid to data source user privileges in recovery operation, and insufficient privileges will lead to recovery failure.
- If a backup is running or a recovery is being executed in recovery operation, the system will refuse to submit the recovery operation until the backup or recovery in progress is completed.
- When multiple cluster compute nodes share one data source, the recovery will prompt that the heartbeat table is repeated. The reason is that the heartbeat table

will be deleted before recovery, but if another cluster compute node has been executing heartbeat detection, the heartbeat table will be recreated, leading to the primary key conflict and the prompt of existence of the heartbeat table in recovery.

- Once a data node fails to restore in the recovery process, the service port of compute node will not be restarted automatically.
- If the recovery fails, the backup or recovery operation is executed again after restarting the compute node service. If a prompt similar to “... Recovery (id: xxx) is running” appears, HotDB Backup shall be restarted correspondingly, for the reason that although recovery fails, the recovery process may not be closed.

17.2.5. Recovery log description

```

Wed Feb 7 11:23:57 2018 [INFO] Initialize_recovery, id: 6
Wed Feb 7 11:23:57 2018 [INFO] Start recovery
] Start recovery
Wed Feb 7 11:23:57 2018 [INFO] ] 192.168.200.51_3308.phy248: Recovery start
Wed Feb 7 11:23:57 2018 [INFO] 192.168.200.51_3310.phy248: Recovery start192.168.200.51_3310.phy248: Recovery start
Wed Feb 7 11:23:57 2018 [INFO] 192.168.200.51_3310.phy248: Start full recovery192.168.200.51_3310.phy248: Start full recovery
Wed Feb 7 11:23:57 2018 [INFO] 192.168.200.51_3308.phy248: Start full recovery192.168.200.51_3308.phy248: Start full recovery
Wed Feb 7 11:23:57 2018 [INFO] INFO] 192.168.200.51_3311.phy248: Recovery start
Wed Feb 7 11:23:57 2018 [INFO] 192.168.200.51_3311.phy248: Start full recovery
Wed Feb 7 11:23:57 2018 [INFO] ] 192.168.200.51_3309.phy248: Recovery start
Wed Feb 7 11:23:57 2018 [INFOINFO] 192.168.200.51_3309.phy248: Start full recovery192.168.200.51_3309.phy248: Start full recovery
Wed Feb 7 11:23:57 2018 [INFOINFO] 192.168.200.51_3311.phy248: Recovery table data from SQL files
192.168.200.51_3311.phy248: Recovery table data from SQL files
Wed Feb 7 11:23:57 2018 [INFO] 192.168.200.51_3310.phy248: Recovery table data from SQL files
192.168.200.51_3310.phy248: Recovery table data from SQL files
Wed Feb 7 11:23:57 2018 [INFO] 192.168.200.51_3309.phy248: Recovery table data from SQL files
] 192.168.200.51_3309.phy248: Recovery table data from SQL files
Wed Feb 7 11:23:57 2018 [INFO] 192.168.200.51_3311.phy248: Recovery table data from SQL files
] 192.168.200.51_3311.phy248: Recovery table data from SQL files
Wed Feb 7 11:23:57 2018 [INFO] 192.168.200.51_3310.phy248: Recovery finished
Wed Feb 7 11:23:59 2018 [INFO] 192.168.200.51_3311.phy248: Recovery finished
Wed Feb 7 11:23:59 2018 [INFO] 192.168.200.51_3310.phy248: Recovery finished
] 192.168.200.51_3310.phy248: Recovery finished
Wed Feb 7 11:23:59 2018 [INFO] 192.168.200.51_3309.phy248: Recovery finished
Wed Feb 7 11:23:59 2018 [INFO] 192.168.200.51_3308.phy248: Recovery finished
Wed Feb 7 11:24:01 2018 [INFO] Recovery is stopped

```

Connected to server successfully! means that connection is established normally between program and Management.

Got a quit signal from user, will quit after recovery is finished means that the program will quit after the recovery.

Start recovery means to start the recovery task.

Start full recovery on datasource: 192.168.200.51\3306\ct05, backup id: 101135 means that a recovery task is started on the data node.

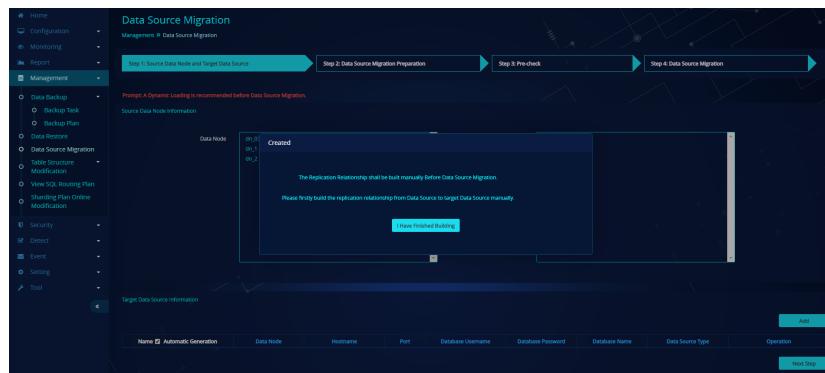
Recovery is stopped means that the recovery task is stopped.

17.3. Data source migration

When a data source in the cluster needs version upgrade or server configuration upgrade and it needs to migrate the data source data to a new data source, copy the data of the old data source to the new data source manually, establish the replication, and then migrate the data source using data source migration.

DR mode explanation: when the DR mode is enabled, please refer to the chapter "Data source migration" in the Distributed Transactional Database HotDB Server - Cross-IDC Disaster Recovery Function Specification for the relevant logical explanations of the data source migration.

17.3.1. Data source migration preparation



Click HotDB Management “Management -> Data Source Migration” to enter the “Data Source Migration” function page. Attention shall be paid to the following before using the Data Source Migration function:

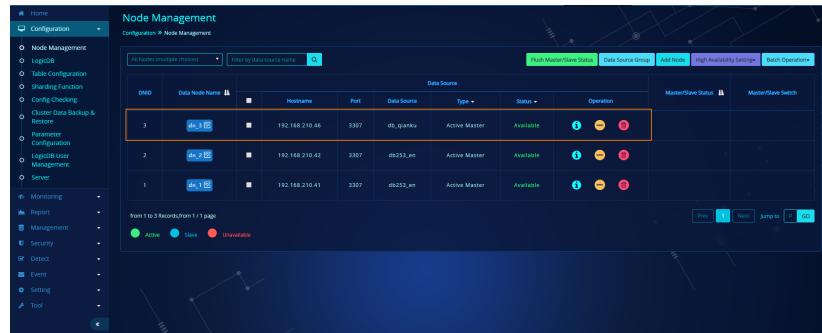
- First import the data from the old data source into the new data source manually.
- Build the replication relation from the old data source to the new data source.

If the data sources under multiple data nodes are different databases in the same instance, it needs to add the filter condition: Replicate_Wild_Do_Table, Replicate_Wild_Ignore_Table when building the replication relation between old and new data sources.

Example Scenario: Data sources built by data node dn_3 are different databases in the instance

192.168.210.46:3307. If only the data in database db_qianku is replicated to the target data source before

migration, an exception will occur when building the replication relation from old data source to new data sources.



The screenshot shows the Node Management interface. On the left, there's a navigation sidebar with sections like Home, Configuration, Node Management, Monitoring, Report, Management, Security, Detect, Event, Setting, and Tool. The main area is titled "Node Management" and "Configurations > Node Management". It displays a table with three rows, each representing a data node:

DNO	Data Node Name	Hostname	Port	Data Source	Type	Status	Operation	Master/Slave Status	Master/Slave Switch
3	dn_3	192.168.210.46	3307	db_qianku	Active Master	Available	OK	Master	Slave
2	dn_2	192.168.210.42	3307	db03_en	Active Master	Available	OK	Master	Slave
1	dn_1	192.168.210.41	3307	db03_en	Active Master	Available	OK	Master	Slave

At the bottom, there are buttons for "All", "Data", and "Unknown".

```

Master_Port: 3308
Connect_Retry: 600
Read_Master_Log_Pos: 108153252
Relay_Log_File: mysql-relay-bin.000002
Relay_Master_Log_File: mysql-bin.000001
Slave_SQL_Running: No
Replicate_Ignore_DB:
Replicate_Ignore_Server_Ids:
Replicate_Wild_Ignore_Table:
Replicate_Wild_Do_Table:
Last_Error: Error 'Table 'zjj1.hotdb_heartbeat' doesn't exist' on query. Default database: 'zjj1'. Query: 'REPLACE INTO hotdb_heartbeat SET master_record=11260
549895287740,`id`2
Skip_Counter: 0
Executed_Gtid_Set: 10815325
Relay_Log_Pos: 3678
Until_Condition: None
Until_Log_Pos: 0
Until_Log_File: 
Master_SSL_CACert:
Master_SSLCert:
Master_SSLKey:
Second_SSL_Cert: NULL
Master_SQLVerifyServerCert: No
Last_IO_Error: 
Last_SQL_Error: 
549895287740,`id`2
Last_SQL_Error: Error 'Table 'zjj1.hotdb_heartbeat' doesn't exist' on query. Default database: 'zjj1'. Query: 'REPLACE INTO hotdb_heartbeat SET master_record=11260
Replicate_Ignore_Server_Ids:
Master_Server_Id: 21051308
Master_Xid: 525400abec61
Master_Info_File: mysql.slave_master_info
SQL_Remaining_Delay: NULL
Slave_SQL_Running: No
Master_Retry_Count: 86400
Master_Retry_Kind:

```

At this point, it needs to add Replicate_Wild_Do_Table and Replicate_Wild_Ignore_Table parameters when building the instance replication relation to filter out the replication of other databases and ensure that only the database currently in use is replicated.

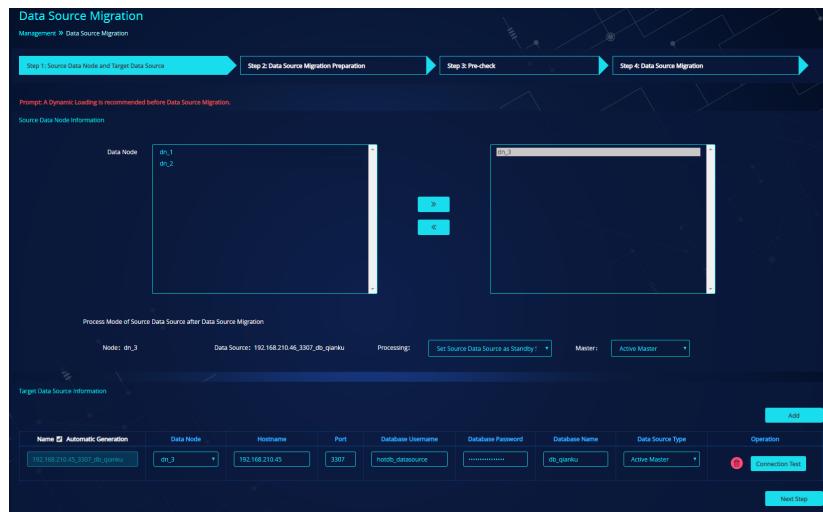
```

Master_Port: 3309
Connect_Retry: 60
Master_Log_File: mysql-bin.000002
Read_Master_Log_Pos: 1058741
Relay_Log_File: mysql-relay-bin.000002
Relay_Log_Pos: 2420
Relay_Master_Log_File: mysql-bin.000002
Slave_IO_Running: Yes
Slave_SQL_Running: Yes
Replicate_Do_DB:
Replicate_Ignore_DB:
Replicate_Do_Table:
Replicate_Ignore_Table:
Replicate_Wild_Ignore_Table: ziji_qianku.%
Replicate_Wild_Ignore_Table: ziji.%
Last_Error: 0
Last_Error_Retries: 0
Skip_Counter: 0
Exec_Master_Log_Pos: 1058741
Relay_Log_Space: 2707
Until_Condition: None
Until_Log_File:
Until_Log_Pos: 0
Master_SSL_Allowed: No
Master_SSL_CA_File:
Master_SSL_CA_Path:
Master_SSL_Cert:
Master_SSL_Cipher:
Master_SSL_Key:
Seconds_Behind_Master: 0
Master_SSL_Verify_Server_Cert: No
Last_IO_Errorno: 0
Last_SQL_Errorno: 0
Last_SQL_Error:
Replicate_Ignore_Server_Ids:

```

- The parameters of the new data source need to be consistent with those of the old data source. A Reload is recommended before data source migration. Data source migration will fail if the Reload of the modified data in configDB is not performed.
- Configured target new database instances cannot coincide with existing database instances.

17.3.2. Source data node and target data source



The screenshot shows the "Data Source Migration" interface. At the top, there is a navigation bar with "Management" and "Data Source Migration". Below it is a progress bar with four steps: "Step 1: Source Data Node and Target Data Source", "Step 2: Data Source Migration Preparation", "Step 3: Pre-check", and "Step 4: Data Source Migration". A note below the progress bar says "Prompt: A Dynamic Loading is recommended before Data Source Migration.".

The main area is divided into two sections: "Source Data Node Information" and "Target Data Source Information".

Source Data Node Information:

- Section title: "Source Data Node Information".
- Content: Shows a list of data nodes: "dn_1" and "dn_2".
- Buttons: "Next Step" and "Cancel".

Target Data Source Information:

- Section title: "Target Data Source Information".
- Content: Shows a table with columns: Name, Data Node, Hostname, Port, Database Username, Database Password, Database Name, Data Source Type, and Operation.
- Table data:

Name	Data Node	Hostname	Port	Database Username	Database Password	Database Name	Data Source Type	Operation
192.168.210.05_3307_dn_qianku	dn_3	192.168.210.05	3307	hotdb_datasource	dr_qianku	Active Master	Connection Test
- Buttons: "Add" and "Next Step".

- After selecting the data node to be migrated and the source data node, the interface will automatically display all data sources under the node.
- Set up the processing mode of original data source after the selected data node has been migrated. Currently, three modes are supported: Delete Source Data Source, Set Source Data Source as Standby Master, and Set Source Data Source as Standby Slave. (if it is set to Standby Slave, please select whether it is Active Master replication or Standby Master replication)
- Fill in the target data source information: data node, hostname, port, database user name, database password, database name, and data source type. Then click on [Connection Test] to ensure that the data source information is correct.
- Click [Next Step] to verify the above information, and all shall pass the verification before going to the next step.

Each new target data node must have one and only one active master, and one standby master at most

Target data node cannot be of single database type. They must have a standby master or standby slave.

The new target data source cannot coincide with any existing data source.

Each new data source can be connected normally.

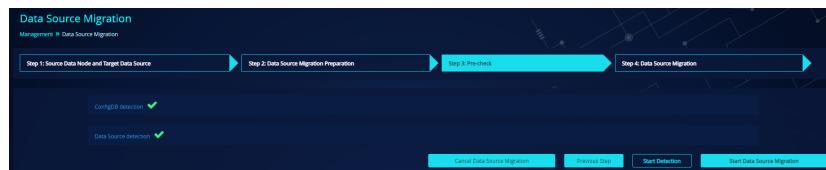
The master of new active master must be the active master or standby master of old node.

17.3.3. Data source migration preparation

The screenshot shows the 'Data Source Migration' interface in the HotDB Management Platform. The current step is 'Step 2: Data Source Migration Preparation'. The interface includes a progress bar with four steps: Step 1: Source Data Node and Target Data Source, Step 2: Data Source Migration Preparation (highlighted in blue), Step 3: Pre-check, and Step 4: Data Source Migration. Below the progress bar, there is a checkbox for 'Execute Change Master by the system' and a note: 'The following change master will be executed during the building process'. There is also a 'Automatic Configuration' button. A table lists data sources with columns: Source, Change master, and Operation. The table shows one entry: '192.168.210.45_3307_db_qianku' with '192.168.210.46_3307_db_qianku' as the change master and 'Modification' in the operation column. An 'Add' button is available for adding more entries. Below the table, there are two radio buttons for creating replication relationships: 'Use Target Data Source Username and Password to create Replication Relationship' (selected) and 'Designate New Data Source Username and Password to create Replication Relationship'. Input fields for 'Data Source Username' and 'Password' are provided. At the bottom, there are checkboxes for 'After Data Source Migration Completed, the system will make Automatic Adoption to Switching Rule' and 'After Data Source Migration Completed, Delete Liveness Database'. Navigation buttons at the bottom include 'Cancel Data Source Migration', 'Previous Step', and 'Next Step'.

- “Execute change master by the system” can choose whether the change master is executed by the compute node. Checking this option will allow the compute node to perform the replication building operation. The compute node will calculate the data source that needs to perform the change master according to the master-slave relation. It can also be configured manually. (Users who perform replication need Reload operation privileges and can be the same users as data sources or other users can be filled in, in which case the usernames and passwords of all data sources shall be the same.)
- If this item is not checked, the compute node will not execute the change master operation and the users need to manually build replication in the data source instance.
- Select whether the switching rule is automatically configured by the compute node after the completion of data source migration. If this item is checked, the compute node will automatically create the switching rule according to the master-slave relation. If this item is not checked, the users will need to configure the Switching Rule manually.
- Select whether to delete the database on old data source after the completion of data source migration. If this item is checked, the compute node will delete the database on old data source. However, it needs to ensure that the replication from old data source to new data source has been disconnected. Therefore, the compute node needs to execute the change master. If this item is not checked, no operation will be executed on old data source.

17.3.4. Pre-check



Pre-check will check the following information. If the check fails, it needs to modify the configuration information according to prompts before data source migration.

a. ConfigDB detection

Check whether the current configDB is correct, which is same as the Config Checking operation. If there is a configuration error, an error is reported and the data source migration cannot be executed.

b. Target data source connection status

Whether each target data source can be connected normally with the filled data source account. If any of the target data sources cannot be connected with the filled data source account, an error is reported.

c. Target data source replication relation

Each target data source shall have a correlation with new target data source established by DBA in advance. It shall be ensured that a non-loop directed connected graph of the target data source of each node and the active master/standby master of source data source is built. The master-master status of target data source can only be the master/slave.

d. Source data source and target data source replication latency detection

Detect the replication latency to ensure that the delay of all new data source and compute node mechanisms is less than 10 seconds. If this condition is not met, an error is prompted (delay from xx data source to xx data source is too large), and the automatic data source migration function can be used only after the replication latency catches up. Make sure that there are multiple new pure standby slaves. Automatic data source migration is not allowed if all replication data of slave new active master/new master-master standby slave does not meet this condition.

e. Target data source user privilege detection

If “execute change master by the compute node” is checked, it needs to determine the data source that needs change master, and check the corresponding account privileges. If the target data source username and password are used, check whether the account has the replication slave privilege. If the specified new data source username and password are selected and the username already exists, check whether the password is correct and whether the replication privilege is available. If the username does not exist, an error is reported.

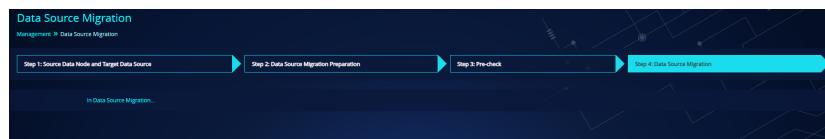
f. Existing data source replication relation

Detect the replication direction of each node that needs data source migration (the detection range is valid new and old data sources). If this condition is not met, automatic data source migration is not allowed.

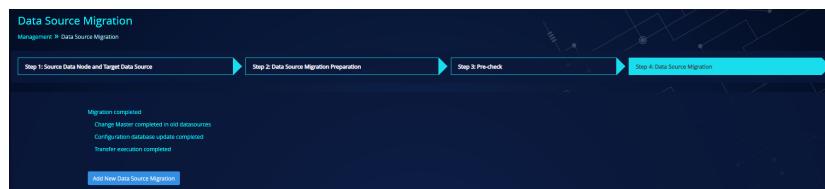
g. Heartbeat table cannot have records with an id value of 3 or 4.

h. The switching of data node shall not be in progress

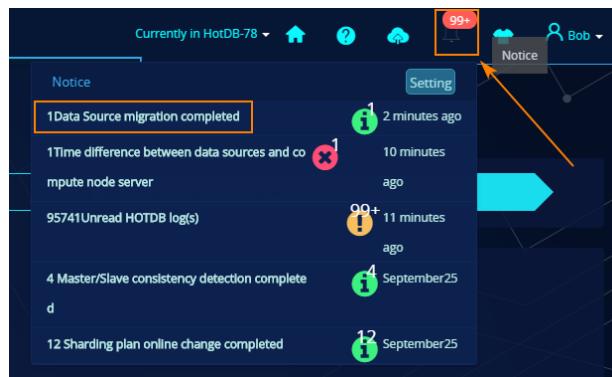
17.3.5. Data source migration



- After clicking [Start Data Source Migration] when the check is completed, the compute node starts to perform the data source migration task. In Data Source Migration is displayed during the execution process, and Migration completed is prompted after the execution is completed. If an exception occurs, a corresponding prompt is given and manual processing is required.



- Data Source Migration completed is also displayed in the “Notice”.

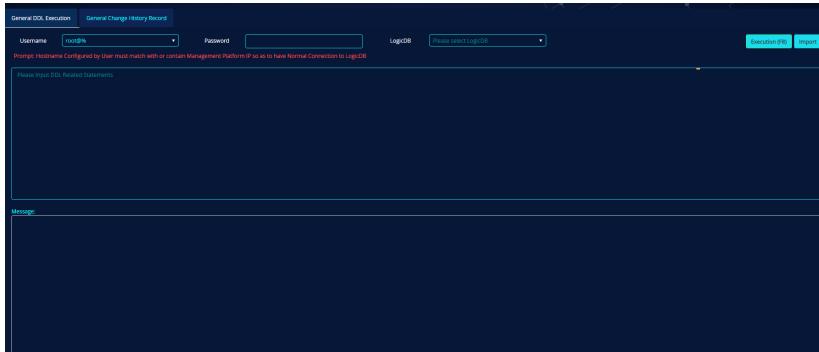


17.4. Table structure change

HotDB Management provides users with an entry point to execute DDL statements online through the “Table Structure Change” function. At the same time, the online DDL mode can also be selected when performing DDL operations on business tables with large amount of data.

17.4.1. Ordinary DDL

Ordinary DDL is a data definition type statement, such as CREATE\DROP\TRUNCATE\RENAME.



- Enter “Management -> Table Structure Change -> Ordinary DDL” to enter the Ordinary DDL operation interface.
- In the Ordinary DDL operation interface, enter the username and password (the username and password are the compute node database user).

Note: When selecting the compute node database user for login, the set “host” range must include the IP address of the server to which the current HotDB Management belongs. Otherwise, the compute node cannot be connected.

- After selecting the logicDB corresponding to the operation, the relevant DDL statement can be executed.
- Currently, the number of columns in single table created by table creation statement of the interface shall not exceed 4096, and the maximum byte in the input box shall not exceed 65535.
- Click the [Import] button on Ordinary DDL page to import external txt or sql type files. After the file is imported into the input box, manually click to execute with the same execution effect as manual input of DDL statement.

General DDL Execution		General Change History Record		
Please select LogDB		Unfinished	Search	Delete History Record
LogDB		General Change Statement	Execution User	Execution Time
pm		create table c (link a)	Bob	2019-09-25 14:18:13
pm		create table c (id int)	Bob	2019-09-25 14:17:35
pm		create table b (id int)	Bob	2019-09-25 14:17:18
pm		create table a (id int)	Bob	2019-09-25 14:17:06

From 1 to 4 Records, from 1 / 1 page

Execution Successful (4) Execution Failed (0)

- All general change records executed can be viewed in the General Change History Record.

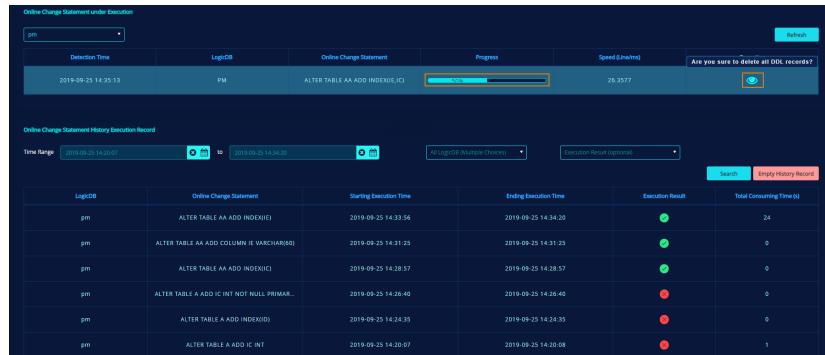
17.4.2. Online DDL

Online DDL is the change statement executed by the Online DDL algorithm on the management end of HotDB Management (3325 by default). The change does not affect the execution of IUD (INSERT, UPDATE, DELETE) statements, has little impact on the system, does not affect the business, and reduce the probability of slave delay. However, online DDL execution is much slower than Ordinary DDL, and the execution may take tens to hundreds of hours for large tables.

Online DDL	
Management > Table structure change > Online DDL	
Online DDL Execution	
Username	cmdbk
Password	[...]
LogDB	pm
Prompt	Hostname Configured by User must match with or contain Management Platform IP so as to have Normal Connection to LogDB
Statement	alter table a add id int;
Message	Success: 0 Failure: 1
Details	execute VO_L_DDL execute "alter table a add id int"; ERROK 1048 (41000): table must have a UNIQUE KEY on a single column

- Enter the online DDL operation interface through “Data Management -> Table Structure Change -> Online DDL”.
- The online DDL function can only execute DDL statements that start with Alter table.

- As with Ordinary DDL, it needs to enter username and password to connect to the logicDB of a specific compute node.
- Currently, the number of columns in single table created by table creation statement of the interface shall not exceed 4096, and the maximum byte in the input box shall not exceed 65535.



The screenshot shows two main sections of the management interface:

- Online Change Statement under Execution:** This section displays a progress bar for an ongoing task: "ALTER TABLE AA ADD INDEX(I,C)". The progress is at 26.3577%. A button labeled "Delete" is visible.
- Online Change Statement History Execution Record:** This section lists completed DDL tasks with their details:

LogicDB	Online Change Statement	Starting Execution Time	Ending Execution Time	Execution Result	Total Consuming Time (s)
pm	ALTER TABLE AA ADD INDEX(I)	2019-09-25 14:33:56	2019-09-25 14:34:20	Success	24
pm	ALTER TABLE AA ADD COLUMN IE VARCHAR(60)	2019-09-25 14:31:23	2019-09-25 14:31:25	Success	0
pm	ALTER TABLE AA ADD INDEX(I,C)	2019-09-25 14:28:57	2019-09-25 14:28:57	Success	0
pm	ALTER TABLE A ADD IC INT NOT NULL PRIMAR...	2019-09-25 14:26:40	2019-09-25 14:26:40	Failure	0
pm	ALTER TABLE A ADD INDEX(I)	2019-09-25 14:24:35	2019-09-25 14:24:35	Failure	0
pm	ALTER TABLE A ADD IC INT	2019-09-25 14:20:07	2019-09-25 14:20:08	Failure	1

- All executed online change records can be viewed in the online change history record. “Online Change Statement under Execution” is used to view the online DDL task under execution and the progress of the task under execution. “Online Change Statement History Execution Record” is used to view the online DDL that has been executed.
- When there is an online DDL statement under execution, click the Filter button to view the changes related to the table under execution in the history record.

17.5. View SQL routing plan

In the HotDB Management, the route of SQL statement executed by the compute node can be parsed through the “View SQL Routing Plan” function.

- Enter the correct username and password and select the logicDB where the table executing SQL is located.
- Enter the SQL statement that needs to be parsed, and click [Execution] to view it.
- This function is the same as the execution of EXPLAIN command on the server (3323 by default).

17.6. Online change of sharding plan

It provides online change support for the table type, sharding function, sharding key, and data node to which the sharding belongs of business tables in four dimensions. Business tables will not be locked during the change, and normal IUD operations can be performed on the table.

17.6.1. Online change of sharding plan

LogiDB	Table Name	Source Table Configuration	Modification Information	Status	The Starting Time	Consuming Time	View Status	Operation
PM	SBTEST6	Sharing Table AUTO_CRC32 ID Global Table	Sharing Function AUTO_MDD Sharing Key ID	Pending	2019-09-25 14:46:27	0s	View Results	Execution Cancellation
PM	AA	Sharing Table AUTO_CRC32 ID Vertical Partitioning Table	Sharing Function AUTO_MDD Sharing Key ID	Pending	2019-09-25 14:45:55	30s	View Results	Execution Cancellation
PM	SBTEST7	Sharing Table AUTO_CRC32 ID Vertical Partitioning Table	Sharing Function AUTO_MDD Sharing Key ID	Success	2019-09-25 14:45:20	0s	View Results	Unread
PM	SBTEST5	Sharing Table AUTO_CRC32 ID Global Table	Sharing Function AUTO_MDD Sharing Key ID	Success	2019-09-25 14:44:55	0s	View Results	Unread
PM	SBTEST6	Sharing Table AUTO_CRC32 ID Sharding Table	Sharing Function AUTO_CRC32 Sharing Key ID	Success	2019-09-25 14:44:21	0s	View Results	Unread
PM	AA	Sharing Table AUTO_CRC32 ID Sharding Table	Sharing Function AUTO_CRC32 Sharing Key ID	Success	2019-09-25 14:43:50	2min10s	View Results	Unread

- The page displays the record of modification task that has been executed or is being executed. The rollback operation of modification task under execution is

allowed through [Cancel Execution].

- The task being executed can view the execution progress in real time, which is refreshed every 3 seconds.
- The task record can be filtered by “LogicDB”, “Table Name”, and “Status”.
- The task record “Status” usually includes 9 types, which are:
 - A. Successful: The task is completed normally without data inconsistency.
 - B. Successful⚠: The task is completed normally with some inconsistent data automatically restored by the program. The warning sign displays: “The data consistency detection after the change found that a small amount of data is inconsistent and has been automatically restored by the program”.
 - C. Successful⚠: The task is completed normally and the inconsistent data is fixed by the program, but there are still some inconsistencies, and the user chooses to ignore the inconsistent data and complete the modification task. The warning tag prompts: “After the program automatically has restored the inconsistent data, the data still has inconsistencies, and the user chooses to allow partial data inconsistency”.
 - D. Failed✖: The task fails because the user manually cancels the task. Error mark prompts: “Manually cancel modification task execution”.
 - E. Failed✖: The task fails because the data inconsistency still exists after automatic restore by the program, and the user chooses to abandon this modification task. Error tag prompts: “data inconsistency still exists after automatic restore by the program, and the user chooses to abandon this modification task”.
 - F. Failed✖: The task fails because the data is found inconsistent after the change is completed and data inconsistency still exists after automatic restore by the program which shall be confirmed by the user. The user fails to process within the set waiting time which causes the task to fail. Error tag prompts: “The data inconsistency has not been processed within the set time range, and the modification task automatically fails”.
 - G. Failed✖: The task fails because the modification plan fails the “modification plan Pre-check” after the task is started in batches. Error tag prompts: “After the

task is started in batches, the modification plan fails the pre-check, causing the task to fail."

H. Waiting: The task is not completed, and data inconsistency needs to be confirmed by the user. Warning tag prompts: "Inconsistent data still exists after the program automatically has restored the inconsistent data, waiting for the user to confirm and process".

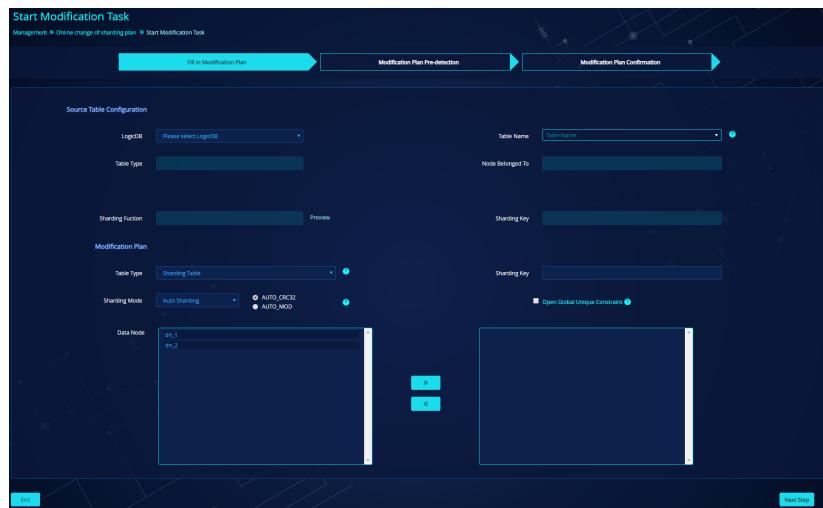
I. Pause  : After the task is started, because the user sets the pause replication period, after the task enters the period, the page displays the task status as Pause, and "The modification task is in the pause data replication period" is prompted when moving the mouse cursor into it.

17.6.2. Start modification task



- Click the [Start Modification Task] button on the “Management->Online Change of Sharding Plan” page to enter the “Start Modification Task” configuration page.

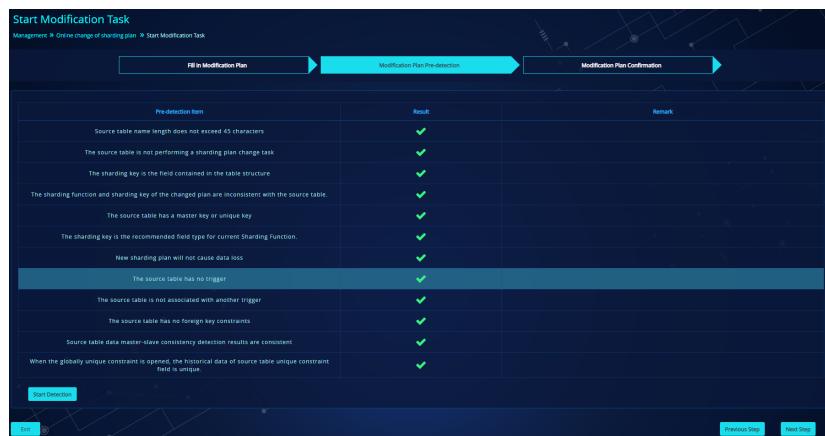
17.6.3. Fill in modification plan



- Select the logicDB where the modification table is located and the table name to be changed. (Selecting a parent table or a table without table structure is not supported)
- “Source Table Configuration” displays the original information of the table that has been selected from the logicDB, including (table type, node information, sharding function and sharding key).
- Modification plan can choose the target “Table Type” (child table is not supported currently), “Sharding Key” (when the table type is sharding table), “Sharding Mode” (when the table type is sharding table), and “Data Node”.
- If “Open Global Unique Constraint” is checked, it needs to ensure that the unique constraint key values in the source table must be unique.

17.6.4. Modification plan pre-detection

Modification plan pre-detection is mainly to check whether the pre-selected modification plan for the source table meets the modification requirements and whether the data consistency can be guaranteed. Click [Start Detection] to perform the modification plan pre-detection.



Special pre-detection item description

- **The master/slave consistency detection results of the source table data shall be consistent.**

If the logicDB where the source table is located has been verified within 24 hours and the detection results of the source table are consistent, a prompt box will pop up to prompt whether to continue the detection or skip the detection. (Otherwise, master/slave consistency detection of the table needs to be performed once)

- **New sharding plan will not lead to data loss**

The modification of sharding function and sharding key may lead to data inconsistency. The system will judge whether the data may be inconsistent according to sharding function and sharding key.

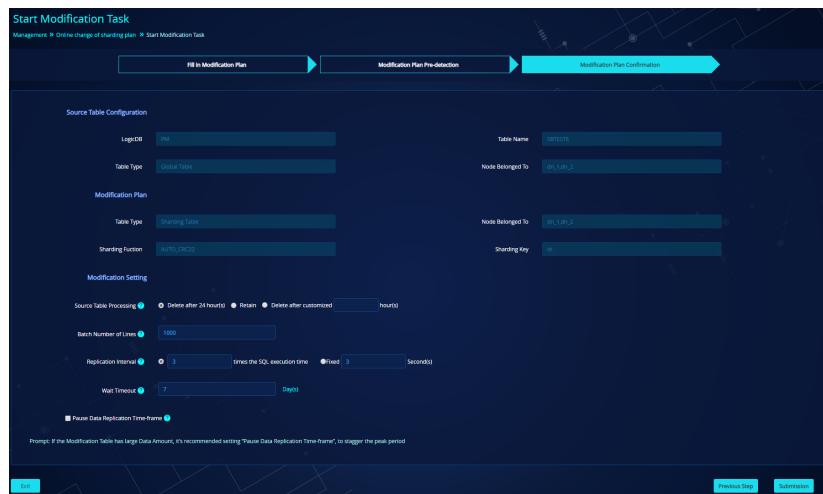
- **When the global unique constraint is opened, the historical data of the source table unique constraint key is unique**

If “Open Global Unique Constraint” in “Fill in Modification Plan” is checked, the modification plan pre-detection will detect whether the historical data of the source table unique constraint key is unique. If it is not checked or the changed table is not a sharding table, the item passes directly without detection.

Pre-detection item “3, 4, 6” is skipped when changing to global table or vertical sharding table type.

17.6.5. Modification plan confirmation

Check the modification table configuration and modification plan information, and set the special settings of the modification task at execution.



- The source table configuration and modification plan information cannot be modified. If modification is needed, click [Previous Step] to return to the “Fill in Modification Plan”, and perform a detection after the modification.
- Modification setting:
 - Source table processing: After selecting Delete after 24 hours or Delete after customized time, the source table is automatically deleted according to the set time. After selecting to reserve the source table, it will exist in the form of source table name +roYYMMDDHHMMSS. The source table will not be processed when the modification task fails. The source table can be viewed in the logicDB, but will not be displayed on the table configuration page.
 - Batch Number of Lines: The number of data lines replicated per batch during data replication, which shall not be more than 10,000 and not be less than 1.
 - Replication Interval: The interval between batches during data replication. “x times the SQL execution time” means the interval is x times the execution time of inserting a new table for each batch of replicated data. “Fixed x

Second(s)" means that the interval of replication for each batch is fixed x seconds. The input range of multiples is [0.1-100000], and the input range of seconds is [0.001-100].

- Wait Timeout: It is the time to wait for the user to make processing when the modification causes data inconsistency. If data inconsistency is not confirmed within the set time range, the modification task will automatically fail. It can be edited and modified within 7 days by default. The input box only allows input of positive integers within [1- 30].
 - Pause Data Replication Time-frame: During the selected time range, data replication between new and old tables is not performed and paused. The sharding modification task will be performed after the set time frame. (If the Modification Table has large Data Amount, it's recommended setting "Pause Data Replication Time-frame" to avoid the peak period)
- After clicking the [Submission] button, the system submits the sharding modification task to the compute node for background execution. The current execution status can be viewed on the Online Change of Sharding Plan page. After the task is completed, click the "View Results" button to view the task execution details.

17.6.6. Start modification in batches

(I) Start mode

LogIDB	Please Select	Table Name	Please Select	Source Table Configuration				Modification Information			Status	The Starting Time	Consuming Time	View	Batch Details
				Table Type	Sharding Function	Sharding Key	Table Type	Sharding Function	Sharding Key						
PM	SBTEST16	AA	Unread	Global Table	Sharding Table	ID	AUTO_CRC32	ID	SUCCESS	2019-09-25 14:50:18	0s	Unread	View Results	Start Modification Task in Batches	
PM	AA	AA	Unread	Sharding Table	AUTO_MOD	ID	Sharding Table	AUTO_CRC32	ID	Success	2019-09-25 14:48:02	1mseconds	Unread	View Results	
PM	SBTEST16	AA	Unread	Sharding Table	AUTO_MOD	ID	Global Table			Success	2019-09-23 14:46:23	0s	Unread	View Results	
PM	AA	AA	Unread	Sharding Table	AUTO_CRC32	IC	Sharding Table	AUTO_MOD	ID	Success	2019-09-25 14:45:55	1min4s	Unread	View Results	
PM	SBTEST17	AA	Unread	Sharding Table	AUTO_CRC32	ID	Vertical Sharding Table			Success	2019-09-25 14:45:55	0s	Unread	View Results	
PM	SBTEST15	AA	Unread	Sharding Table	AUTO_CRC32	ID	Global Table			Success	2019-09-25 14:44:55	0s	Unread	View Results	
PM	SBTEST16	AA	Unread	Sharding Table	AUTO_CRC32	ID	Sharding Table	AUTO_MOD	ID	Success	2019-09-25 14:44:21	0s	Unread	View Results	
PM	AA	AA	Unread	Sharding Table	AUTO_CRC32	ID	Sharding Table	AUTO_CRC32	IC	Success	2019-09-25 14:41:06	2min10s	Unread	View Results	

- Click "[Batch Operation]->[Start Modification Task in Batches]" on the "Online

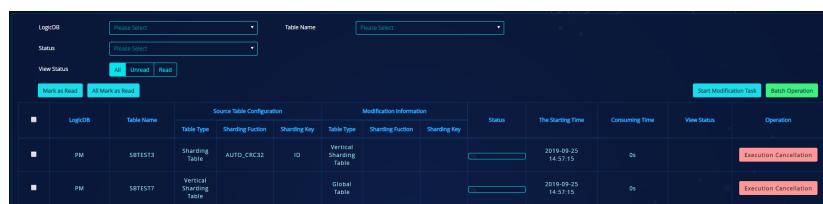
Change of Sharding Plan” page, or select multiple sharding recommendation plan records in the “Sharding Plan Recommendation” function to start modification task in batches through [Online Modification].

(II) Filling instructions for starting modification task in batches



- If the pre-detection of batch started modification task fails, the entire task fails. During the pre-detection process, if the LogicDB to which the source table belong has executed the master/slave consistency detection within 24 hours and the results are consistent, the “Master/Slave Data Consistency Detection” item will not be executed in the table pre-detection.
- The “Source Table Processing” and “Replication Interval” settings in batch started modification do not support customized input values, and only the drop-down box option is supported.

(III) Execute batch task

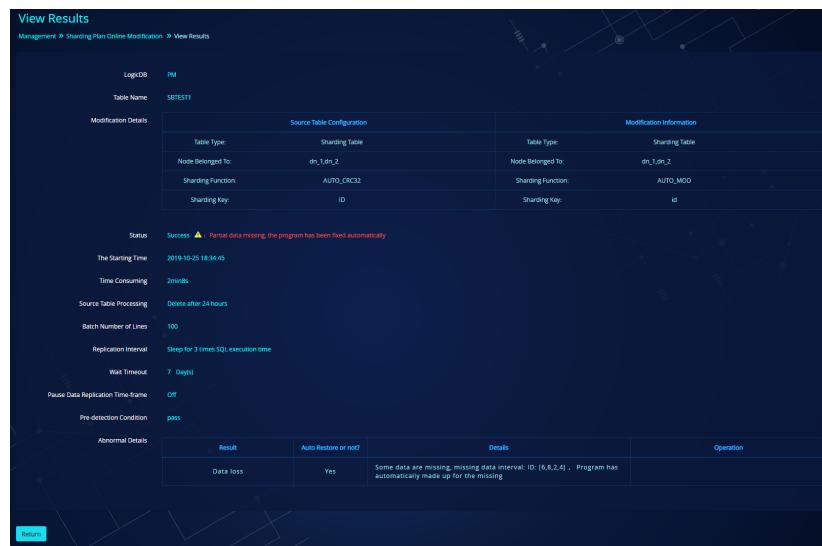


- If any of the multiple tasks started in the same batch is manually canceled, other tasks will fail even if no exception occurs, and “Because one of the tasks started in the same batch is manually canceled, the current task is automatically canceled” is prompted.
- If any of the multiple tasks started in the same batch fails the pre-detection (or failure due to loss/excess/inconsistency of a large number of data), other tasks will fail even if no exception occurs, and “An exception exists in one of the tasks started in the same batch, causing the task to automatically fail” is prompted.

17.6.7. Sharding plan modification exception handling

It refers to the case that the data of new table and source table after modification is found to be inconsistent when the sharding plan modification task is completed, and the processing instructions need to be made according to the exception.

- When a small amount of data is lost during modification, HotDB Management will prompt the range of lost data and automatically compensate for the lost data, as shown below:



Result	Auto Restore or not?	Details	Operation
Data loss	Yes	Some data are missing, missing data interval: ID: (6,8,2,4) . Program has automatically made up for the missing	

- When there is a small amount of excessive data during modification, HotDB Management will prompt the range of excessive data and automatically delete the excessive data, as shown below:

- When there is a small amount of inconsistent data during modification, HotDB Management will prompt the range of inconsistent data and automatically restore the inconsistent data, as shown below:

- When there is a large amount of inconsistent data during modification, HotDB Management will prompt the range of inconsistent data, but will not restore such a large number of inconsistent data, as shown below:

View Results

Management > Sharding Plan Online Modification > View Results

LogicDB	PM																				
Table Name	SBITSITI																				
Modification Details	<table border="1"> <thead> <tr> <th colspan="2">Source Table Configuration</th> <th colspan="2">Modification Information</th> </tr> <tr> <th>Table Type:</th> <th>Sharding Table</th> <th>Table Type:</th> <th>Sharding Table</th> </tr> </thead> <tbody> <tr> <td>Node Belonged To:</td> <td>dn_1,dn_2</td> <td>Node Belonged To:</td> <td>dn_1,dn_2</td> </tr> <tr> <td>Sharding Function:</td> <td>AUTO_CRC32</td> <td>Sharding Function:</td> <td>AUTO_MDD</td> </tr> <tr> <td>Sharding Key:</td> <td>ID</td> <td>Sharding Key:</td> <td>ID</td> </tr> </tbody> </table>	Source Table Configuration		Modification Information		Table Type:	Sharding Table	Table Type:	Sharding Table	Node Belonged To:	dn_1,dn_2	Node Belonged To:	dn_1,dn_2	Sharding Function:	AUTO_CRC32	Sharding Function:	AUTO_MDD	Sharding Key:	ID	Sharding Key:	ID
Source Table Configuration		Modification Information																			
Table Type:	Sharding Table	Table Type:	Sharding Table																		
Node Belonged To:	dn_1,dn_2	Node Belonged To:	dn_1,dn_2																		
Sharding Function:	AUTO_CRC32	Sharding Function:	AUTO_MDD																		
Sharding Key:	ID	Sharding Key:	ID																		
Status	Failure (●) Data consistency detection after change finds the inconsistency of a large amount of data, automatic recovery of the program failed																				
The Starting Time	2019-10-23 18:27:56																				
Time Consuming	1m36s																				
Source Table Processing	Delete after 24 hours																				
Batch Number of Lines	100																				
Replication Interval	Sleep for 3 times SQL execution time																				
Wait Timeout	7 Days(0)																				
Pause Data Replication Time-frame	Off																				
Pre-detection Condition	pass																				
Abnormal Details	<table border="1"> <thead> <tr> <th>Result</th> <th>Auto Restore or not?</th> <th>Details</th> <th>Operation</th> </tr> </thead> <tbody> <tr> <td>Data inconsistency</td> <td>No</td> <td>Data consistency detection after change finds a large amount of data inconsistency, inconsistency interval is ID:(1500001-1600000), and the program cannot automatically repair</td> <td></td> </tr> </tbody> </table>	Result	Auto Restore or not?	Details	Operation	Data inconsistency	No	Data consistency detection after change finds a large amount of data inconsistency, inconsistency interval is ID:(1500001-1600000), and the program cannot automatically repair													
Result	Auto Restore or not?	Details	Operation																		
Data inconsistency	No	Data consistency detection after change finds a large amount of data inconsistency, inconsistency interval is ID:(1500001-1600000), and the program cannot automatically repair																			

Buttons

- When a small amount of inconsistent (lost or excessive) data occurs during modification for the first time, HotDB Management will actively restore the inconsistent data. If inconsistent data occurs again after the restore is completed, HotDB Management will prompt that the data is still inconsistent after automatic restore, give the range of inconsistent (lost or excessive) data, and wait for the user to choose: [Ignore Inconsistency] or [Discard Modification] rather than automatically restoring them.

View Results

Management > Sharding Plan Online Modification > View Results

LogiDB	PM																																
Table Name	QUAN_A																																
Modification Details	<table border="1"> <thead> <tr> <th colspan="2">Source Table Configuration</th> <th colspan="2">Modification Information</th> </tr> </thead> <tbody> <tr> <td>Table Type:</td> <td>Global Table</td> <td>Table Type:</td> <td>Sharding Table</td> </tr> <tr> <td>Node Belonged To:</td> <td>dn_1,dn_2</td> <td>Node Belonged To:</td> <td>dn_1,dn_2</td> </tr> <tr> <td>Sharding Function:</td> <td></td> <td>Sharding Function:</td> <td>AUTO_CRC32</td> </tr> <tr> <td>Sharding Key:</td> <td></td> <td>Sharding Key:</td> <td>ID</td> </tr> </tbody> </table> <p>Status: Waiting ⚠: Additional partial data, automatic recovery of the program failed.</p> <p>The Starting Time: 2019-10-25 17:08:35</p> <p>Time Consuming: 10s</p> <p>Source Table Processing: Delete after 24 hours</p> <p>Batch Number of Lines: 1000</p> <p>Replication Interval: Sleep for 3 times SQL execution time</p> <p>Wait Timeout: 7 Day(s)</p> <p>Pause Data Replication Time-frame: Off</p> <p>Pre-detection Condition: pass</p> <p>Abnormal Details</p> <table border="1"> <thead> <tr> <th>Result</th> <th>Auto Restore or not?</th> <th>Details</th> <th>Operation</th> </tr> </thead> <tbody> <tr> <td>Inconsistency still exists after automatic repair</td> <td>No</td> <td>Some data are missing, missing data interval: ID [6415], Program cannot be repaired automatically</td> <td>Ignore the Inconsistency Give Up Modification</td> </tr> <tr> <td>Inconsistency still exists after automatic repair</td> <td>No</td> <td>Extra data, extra data interval: ID [6416], Program cannot be repaired automatically</td> <td>Ignore the Inconsistency Give Up Modification</td> </tr> </tbody> </table>	Source Table Configuration		Modification Information		Table Type:	Global Table	Table Type:	Sharding Table	Node Belonged To:	dn_1,dn_2	Node Belonged To:	dn_1,dn_2	Sharding Function:		Sharding Function:	AUTO_CRC32	Sharding Key:		Sharding Key:	ID	Result	Auto Restore or not?	Details	Operation	Inconsistency still exists after automatic repair	No	Some data are missing, missing data interval: ID [6415], Program cannot be repaired automatically	Ignore the Inconsistency Give Up Modification	Inconsistency still exists after automatic repair	No	Extra data, extra data interval: ID [6416], Program cannot be repaired automatically	Ignore the Inconsistency Give Up Modification
Source Table Configuration		Modification Information																															
Table Type:	Global Table	Table Type:	Sharding Table																														
Node Belonged To:	dn_1,dn_2	Node Belonged To:	dn_1,dn_2																														
Sharding Function:		Sharding Function:	AUTO_CRC32																														
Sharding Key:		Sharding Key:	ID																														
Result	Auto Restore or not?	Details	Operation																														
Inconsistency still exists after automatic repair	No	Some data are missing, missing data interval: ID [6415], Program cannot be repaired automatically	Ignore the Inconsistency Give Up Modification																														
Inconsistency still exists after automatic repair	No	Extra data, extra data interval: ID [6416], Program cannot be repaired automatically	Ignore the Inconsistency Give Up Modification																														

When selecting [Discard Modification], the modification task fails and “The data is still inconsistent after the program has automatically restored the inconsistent data and the user chooses to discard the modification task” is prompted, as shown below:

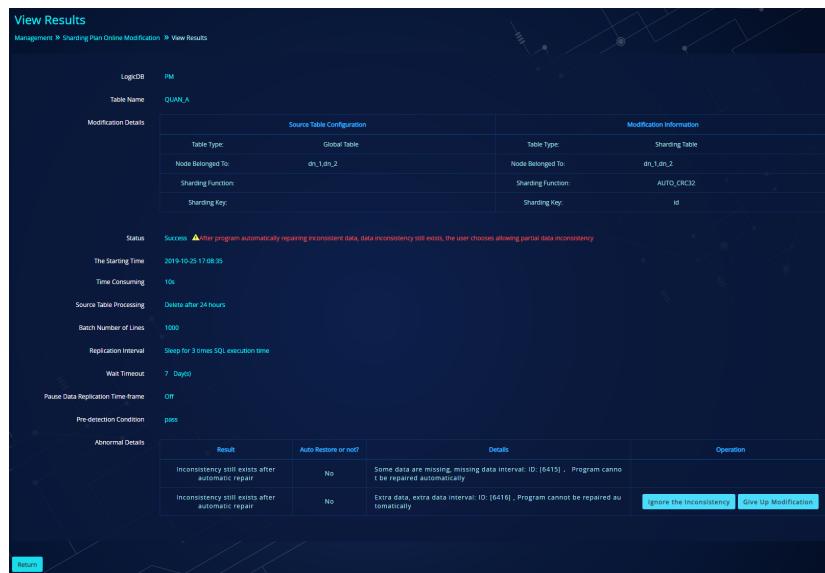
View Results

Management > Sharding Plan Online Modification > View Results

LogiDB	PM																																
Table Name	QUAN_A																																
Modification Details	<table border="1"> <thead> <tr> <th colspan="2">Source Table Configuration</th> <th colspan="2">Modification Information</th> </tr> </thead> <tbody> <tr> <td>Table Type:</td> <td>Global Table</td> <td>Table Type:</td> <td>Sharding Table</td> </tr> <tr> <td>Node Belonged To:</td> <td>dn_1,dn_2</td> <td>Node Belonged To:</td> <td>dn_1,dn_2</td> </tr> <tr> <td>Sharding Function:</td> <td></td> <td>Sharding Function:</td> <td>AUTO_CRC32</td> </tr> <tr> <td>Sharding Key:</td> <td></td> <td>Sharding Key:</td> <td>ID</td> </tr> </tbody> </table> <p>Status: Failure 🔴: After the program automatically repairs the inconsistent data, the data inconsistency still exists, and the user chooses to abandon the change task.</p> <p>The Starting Time: 2019-10-25 17:08:35</p> <p>Time Consuming: 10s</p> <p>Source Table Processing: Delete after 24 hours</p> <p>Batch Number of Lines: 1000</p> <p>Replication Interval: Sleep for 3 times SQL execution time</p> <p>Wait Timeout: 7 Day(s)</p> <p>Pause Data Replication Time-frame: Off</p> <p>Pre-detection Condition: pass</p> <p>Abnormal Details</p> <table border="1"> <thead> <tr> <th>Result</th> <th>Auto Restore or not?</th> <th>Details</th> <th>Operation</th> </tr> </thead> <tbody> <tr> <td>Inconsistency still exists after automatic repair</td> <td>No</td> <td>Some data are missing, missing data interval: ID [6415], Program cannot be repaired automatically</td> <td>Give Up Modification</td> </tr> <tr> <td>Inconsistency still exists after automatic repair</td> <td>No</td> <td>Extra data, extra data interval: ID [6416], Program cannot be repaired automatically</td> <td>Ignore the Inconsistency Give Up Modification</td> </tr> </tbody> </table>	Source Table Configuration		Modification Information		Table Type:	Global Table	Table Type:	Sharding Table	Node Belonged To:	dn_1,dn_2	Node Belonged To:	dn_1,dn_2	Sharding Function:		Sharding Function:	AUTO_CRC32	Sharding Key:		Sharding Key:	ID	Result	Auto Restore or not?	Details	Operation	Inconsistency still exists after automatic repair	No	Some data are missing, missing data interval: ID [6415], Program cannot be repaired automatically	Give Up Modification	Inconsistency still exists after automatic repair	No	Extra data, extra data interval: ID [6416], Program cannot be repaired automatically	Ignore the Inconsistency Give Up Modification
Source Table Configuration		Modification Information																															
Table Type:	Global Table	Table Type:	Sharding Table																														
Node Belonged To:	dn_1,dn_2	Node Belonged To:	dn_1,dn_2																														
Sharding Function:		Sharding Function:	AUTO_CRC32																														
Sharding Key:		Sharding Key:	ID																														
Result	Auto Restore or not?	Details	Operation																														
Inconsistency still exists after automatic repair	No	Some data are missing, missing data interval: ID [6415], Program cannot be repaired automatically	Give Up Modification																														
Inconsistency still exists after automatic repair	No	Extra data, extra data interval: ID [6416], Program cannot be repaired automatically	Ignore the Inconsistency Give Up Modification																														

When selecting [Ignore Inconsistency], the task is successful but there is some

inconsistent data, and “Online modification is completed, and the user allows the existence of some inconsistency after modification” is prompted, as shown below:



View Results

Management > Sharding Plan Online Modification > View Results

LogicDB	PM																				
Table Name	QUAN_A																				
Modification Details	<table border="1"> <thead> <tr> <th colspan="2">Source Table Configuration</th> <th colspan="2">Modification Information</th> </tr> <tr> <th>Table Type:</th> <th>Global Table</th> <th>Table Type:</th> <th>Sharding Table</th> </tr> </thead> <tbody> <tr> <td>Nodes Belonged To:</td> <td>dn_1,dn_2</td> <td>Nodes Belonged To:</td> <td>dn_1,dn_2</td> </tr> <tr> <td>Sharding Function:</td> <td></td> <td>Sharding Function:</td> <td>AUTO_CRC32</td> </tr> <tr> <td>Sharding Key:</td> <td></td> <td>Sharding Key:</td> <td>Id</td> </tr> </tbody> </table>	Source Table Configuration		Modification Information		Table Type:	Global Table	Table Type:	Sharding Table	Nodes Belonged To:	dn_1,dn_2	Nodes Belonged To:	dn_1,dn_2	Sharding Function:		Sharding Function:	AUTO_CRC32	Sharding Key:		Sharding Key:	Id
Source Table Configuration		Modification Information																			
Table Type:	Global Table	Table Type:	Sharding Table																		
Nodes Belonged To:	dn_1,dn_2	Nodes Belonged To:	dn_1,dn_2																		
Sharding Function:		Sharding Function:	AUTO_CRC32																		
Sharding Key:		Sharding Key:	Id																		
Status	Success ⚠ After program automatically repairing inconsistent data, data inconsistency still exists, the user chooses allowing partial data inconsistency																				
The Starting Time	2019-10-25 17:08:35																				
Time Consuming	10s																				
Source Table Processing	<table border="1"> <tr> <td>Delete after 24 hours</td> </tr> </table>	Delete after 24 hours																			
Delete after 24 hours																					
Batch Number of Lines	1000																				
Replication Interval	Sleep for 3 times SQL execution time																				
Wait Timeout	7 Days																				
Pause Data Replication Time-frame	OFF																				
Pre-detection Condition	pass																				
Abnormal Details	<table border="1"> <thead> <tr> <th>Result</th> <th>Auto Restore or not?</th> <th>Details</th> <th>Operation</th> </tr> </thead> <tbody> <tr> <td>Inconsistency still exists after automatic repair</td> <td>No</td> <td>Some data are missing, missing data interval: ID: [6415], Program cannot be repaired automatically</td> <td>Ignore the inconsistency Give up Modification</td> </tr> <tr> <td>Inconsistency still exists after automatic repair</td> <td>No</td> <td>Extra data, extra data interval: ID: [6416], Program cannot be repaired automatically</td> <td>Ignore the inconsistency Give up Modification</td> </tr> </tbody> </table>	Result	Auto Restore or not?	Details	Operation	Inconsistency still exists after automatic repair	No	Some data are missing, missing data interval: ID: [6415], Program cannot be repaired automatically	Ignore the inconsistency Give up Modification	Inconsistency still exists after automatic repair	No	Extra data, extra data interval: ID: [6416], Program cannot be repaired automatically	Ignore the inconsistency Give up Modification								
Result	Auto Restore or not?	Details	Operation																		
Inconsistency still exists after automatic repair	No	Some data are missing, missing data interval: ID: [6415], Program cannot be repaired automatically	Ignore the inconsistency Give up Modification																		
Inconsistency still exists after automatic repair	No	Extra data, extra data interval: ID: [6416], Program cannot be repaired automatically	Ignore the inconsistency Give up Modification																		

17.7. Table Recycle Bin

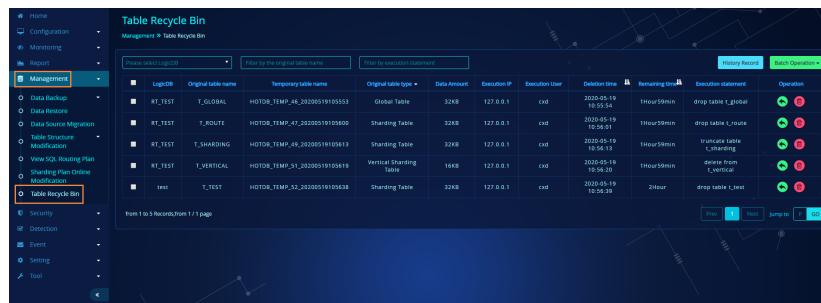
Table Recycle Bin is a function that when the parameter dropTableRetentionTime is enabled, the tables operated by the server (3323 by default) with DROP, TRUNCATE, DELETE without WHERE condition (auto commit) will enter the recycle bin. The management platform supports the visualized data flashback operation within the retention time. In addition, it also includes the functions of viewing the list of restorable data, restoring (flashback) data, deleting data, and viewing historical record.

17.7.1. Premise for use

The following requirements shall be met for using Table Recycle Bin:

- The current user has the menu privilege of Table Recycle Bin.
- The current compute node parameter dropTableRetentionTime shall not be 0.
- Tables are operated by the server (3323 by default) with DROP, TRUNCATE, DELETE without WHERE condition (auto commit).

17.7.2. Table Recycle Bin



The screenshot shows the "Table Recycle Bin" page with a list of temporary tables. The columns include: LogicDB, Original table name, Temporary table name, Original table type, Data Amount, Execution IP, Execution User, Deletion time, Remaining time, Execution statement, and Operation. The table contains the following data:

LogicDB	Original table name	Temporary table name	Original table type	Data Amount	Execution IP	Execution User	Deletion time	Remaining time	Execution statement	Operation
RT_TEST	T_GLOBAL	HOTDB_TEMP_46_20200519105553	Global Table	32KB	127.0.0.1	cxd	2020-05-19 12:22:53	1hour59min	drop table t_global	
RT_TEST	T_ROUTE	HOTDB_TEMP_47_20200519104600	Sharding Table	32KB	127.0.0.1	cxd	2020-05-19 12:22:51	1hour59min	drop table t_route	
RT_TEST	T_SHARDING	HOTDB_TEMP_49_20200519105613	Sharding Table	32KB	127.0.0.1	cxd	2020-05-19 12:22:53	1hour59min	truncate table t_sharding	
RT_TEST	T_VERTICAL	HOTDB_TEMP_51_20200519105619	Vertical Sharding Table	16KB	127.0.0.1	cxd	2020-05-19 12:22:50	1hour59min	drop table t_vertical	
test	T_TEST	HOTDB_TEMP_52_20200519105638	Sharding Table	32KB	127.0.0.1	cxd	2020-05-19 12:22:59	2hour	drop table t_test	

- The page displays the temporary table which entered the recycle bin after the server (3323 by default) performed three operations.
- You can filter and view table recycle bin records through LogicDB, original table name, and execution statement.
- After the table retention time, table in the recycle bin will be automatically deleted and not recorded in history record.

17.7.3. Table restore

(1) Click Restore



The screenshot shows the "Table Recycle Bin" page with a list of temporary tables. The columns include: LogicDB, Original table name, Temporary table name, Original table type, Data Amount, Execution IP, Execution User, Deletion time, Remaining time, Execution statement, and Operation. The "RESTORE" button is highlighted for the first row. The table data is identical to the one in the previous screenshot.

- Click the Restore button of the temporary table on the "Management -> Table Recycle Bin" page, and the input box for connection information will pop up.

(2) Fill in the connection information

Table Recycle Bin

Fill in the connection information

Please provide the connection information of the following LogiDB and confirm the restored table name

LogiDB	Database user	User password	Original table	Temporary table	Restored name
RT_TEST	cxd	[User password]	T_GLOBAL	HOTDB_TEMP_1_20200514172118	T_GLOBAL

Execution Result

Execution completed. Successful: 1, Failed: 0.
view details in the history records

Confirm Cancel

- Select a database user.
- Enter user password.
- The input box for the restored name displays the original table name by default, which can be modified.

(3) Confirm the restore

Table Recycle Bin

Fill in the connection information

Please provide the connection information of the following LogiDB and confirm the restored table name

LogiDB	Database user	User password	Original table	Temporary table	Restored name
RT_TEST	cxd	[.....]	T_GLOBAL	HOTDB_TEMP_41_20200519105055	T_GLOBAL

Execution Result

Execution completed. Successful: 1, Failed: 0.
view details in the history records

Confirm Cancel

- After the restore, the execution result will be displayed, including the number of successes, the number of failures, and the history record.
- Click History Record to jump to history record page.

17.7.4. Table deletion

(4) Click Delete

Table Recycle Bin

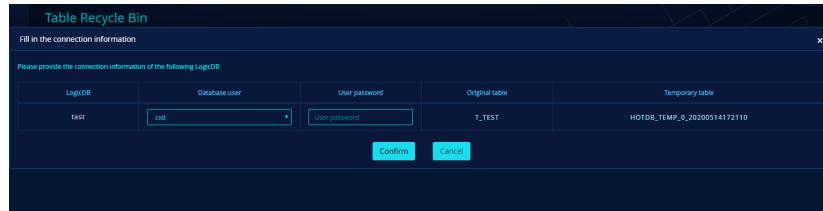
Management > Table Recycle Bin

Drop reason	LogiDB	Original table name	Temporary table name	Original table type	Data Amount	Execution IP	Execution User	Deleted time	Remaining time	Execution statement	Operation
	test	T_TEST	HOTDB_TEMP_E_20200518182218	Sharding Table	32KB	127.0.0.1	cxd	2020-05-18 18:22:19	1Hour45min	drop table t_test	
	RT_TEST	T_VERTICAL	HOTDB_TEMP_13_20200518182358	Vertical Sharding Table	16KB	127.0.0.1	cxd	2020-05-18 18:22:58	1Hour46min	delete from t_vertical	
	RT_TEST	T_ROUTE	HOTDB_TEMP_15_20200518182331	Sharding Table	32KB	127.0.0.1	cxd	2020-05-18 18:23:32	1Hour46min	truncate table t_route	

- Click the Delete button of the temporary table on the "Management -> Table

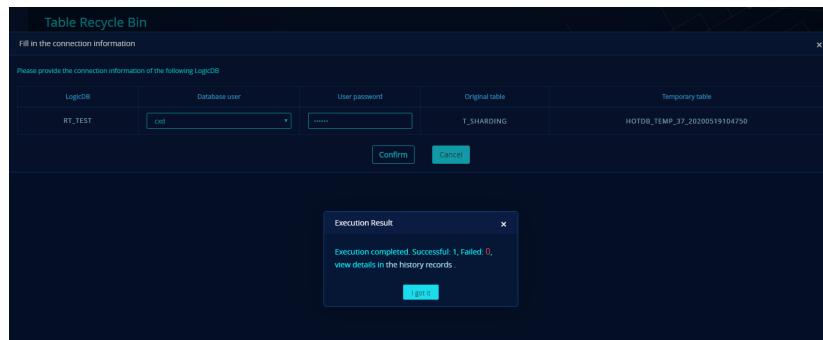
"Recycle Bin" page, the deletion confirmation box will pop up. Click Confirm, the input box for connection information will pop up.

(5) Fill in connection information



- Select a database user.
- Enter user password.

(6) Confirm the deletion



- After the deletion, the execution result will be displayed, including the number of successes, the number of failures and the history record.
- Click History Record to jump to history record page.

17.7.5. Table batch restore

(1) Click Batch restore

Table Recycle Bin										
Management > Table Recycle Bin										
Please select LogicDB		Filter by original table name		Filter by execution statement		History Record			Batch Operation	
LogicDB	Original table name	Temporary table name	Original table type	Data Amount	Execution IP	Execution user	Deletion time	Remaining time	Execution statement	
RT_TEST	T_TEST	HOTDB_TEMP_8_20200518182218	Sharding Table	32KB	127.0.0.1	cx0	2020-05-18 18:22:19	1Hour45min	drop table T_TEST	
RT_TEST	T_VERTICAL	HOTDB_TEMP_12_20200518182258	Vertical Sharding Table	16KB	127.0.0.1	cx0	2020-05-18 18:22:58	1Hour46min	delete from T_VERTICAL	
RT_TEST	T_ROUTE	HOTDB_TEMP_15_20200518182311	Sharding Table	32KB	127.0.0.1	cx0	2020-05-18 18:23:11	1Hour46min	truncate table T_ROUTE	
RT_TEST	T_SHARDING	HOTDB_TEMP_16_20200518182443	Sharding Table	32KB	192.168.220.102	cx0	2020-05-18 18:28:43	1Hour32min	rename table HOTDB_TEMP_11_20200518182250 to T_SHARDING	

- Check tables to be restored, and click “Batch Operation -> Batch restore” on the “Management -> Table Recycle Bin” page.

(2) Batch restore connection information

Table Recycle Bin

Fill in the connection information

Please provide the connection information of the following LogicDB and confirm the restored table name

LogicDB	Database user	User password	Original table	Temporary table	Restored name
RT_TEST	cx0	<input type="password"/> User password	T_SHARDING	HOTDB_TEMP_3_20200514172126	<input type="text"/> T_SHARDING
			T_VERTICAL	HOTDB_TEMP_5_20200514172134	<input type="text"/> T_VERTICAL

Confirm Cancel

- If the checked tables all belong to the same LogicDB, only one piece of connection information needs to be filled in.
- If the checked tables belong to multiple LogicDBs, connection information need to be filled in separately.
- If there is an error in one piece of connection information, none of the tables can be restored.
- The input box for the restored name displays the original table name by default, which can be modified.

(3) Confirm the batch restore

Table Recycle Bin

Fill in the connection information

Please provide the connection information of the following LogicDB and confirm the restored table name

LogicDB	Database user	User password	Original table	Temporary table	Restored name
RT_TEST	cxld	T_VERTICAL	HOTDB_TEMP_39_20200519104822	T_VERTICAL
			T_GLOBAL	HOTDB_TEMP_42_20200519105355	T_GLOBAL

Execution Result

Execution completed. Successful: 2, Failed: 0.
view details in the history records.

Confirm **Cancel**

- After the batch restore, the execution result will be displayed, including the number of successes, the number of failures, and the history record.
- Click History Record to jump to history record page.

17.7.6. Table batch deletion

(1) Click Batch deletion

Table Recycle Bin

Management > Table Recycle Bin

LogicDB	Original table name	Temporary table name	Original table type	Data Amount	Execution IP	Execution User	Deletion time	Remaining time	Execution statement
<input checked="" type="checkbox"/> test	T_TEST	HOTDB_TEMP_B_20200518182218	Sharding Table	32KB	127.0.0.1	cxld	2020-05-18 13:23:18	1 hour 45 min	drop table t_test
<input checked="" type="checkbox"/> RT_TEST	T_VERTICAL	HOTDB_TEMP_19_20200518182258	Vertical Sharding Table	16KB	127.0.0.1	cxld	2020-05-18 18:22:58	1 hour 46 min	delete from t_vertical
<input checked="" type="checkbox"/> RT_TEST	T_ROUTE	HOTDB_TEMP_19_20200518182331	Sharding Table	32KB	127.0.0.1	cxld	2020-05-18 18:23:12	1 hour 46 min	truncate table t_route
<input checked="" type="checkbox"/> RT_TEST	T_SHARDING	HOTDB_TEMP_16_20200518182843	Sharding Table	32KB	192.168.220.102	cxld	2020-05-18 18:28:43	1 hour 52 min	TRUNCATE TABLE HOTDB_TEMP_16_20200518182843 to T_SHARDING

History Record **Batch Operation**

Batch remove **Batch delete**

- Check tables to be deleted, and click “Batch Operation -> Batch deletion” on the “Management -> Table Recycle Bin” page.

(2) Batch deletion connection information

Table Recycle Bin

Fill in the connection information

Please provide the connection information of the following LogicDB

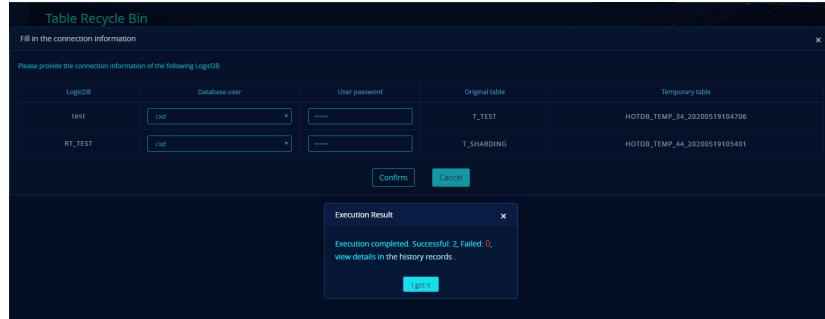
LogicDB	Database user	User password	Original table	Temporary table
RT_TEST	cxld	T_GLOBAL	HOTDB_TEMP_7_20200514172837
test	cxld	T_TEST	HOTDB_TEMP_B_20200514173102

Confirm **Cancel**

- If the checked tables all belong to the same LogicDB, only one piece of connection information needs to be filled in.

- If the checked tables belong to multiple LogicDBs, connection information need to be filled in separately.
- If there is an error in one piece of connection information, none of the tables can be deleted.

(3) Confirm the batch deletion

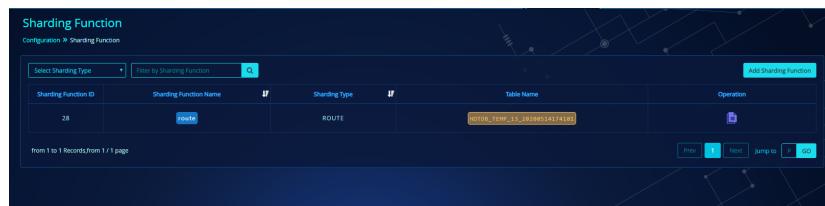


- After the batch deletion, the execution result is displayed, including the number of successes, the number of failures and the history record.
- Click History Record to jump to history record page.

17.7.7. Special instructions for Table Recycle Bin

Some special situations that may occur in the recycle bin are described here.

- After a table with advanced sharding function enters the recycle bin, the table configuration will be deleted while the sharding function cannot be edited or deleted until the table in the recycle bin is deleted. On the sharding function page, a temporary table will be displayed. Click the temporary table to jump to the table recycle bin page. As shown below:



- Restore failures include, but may not be limited to:

- ◆ The configuration of the original table is inconsistent with that of the restored table (including table type, sharding key, sharding function and data node). As shown below:

History Record							
Management > Table Recycle Bin > History Record							
Please select LogDB		Filter by the original table name					
■ LogDB	Original table name	Temporary table name	Original table type	restored table name	Execution User	Operation Time	
■ RT_TEST	T_GLOBAL	HOTDB_TEMP_16_20200515172413	Global Table	T_global	cxd	2020-05-15 17:24:13	table T_GLOBAL is using a different configuration

- ◆ The LogicDB of the original table is inconsistent with that of the restored table. As shown below:

History Record							
Management > Table Recycle Bin > History Record							
Please select LogDB		Filter by the original table name					
■ LogDB	Original table name	Temporary table name	Original table type	restored table name	Execution User	Operation Time	
■ RT_TEST	T_SHARDING	HOTDB_TEMP_22_20200520170217	Sharding Table	T_SHARDING	cxd	2020-05-20 17:04:08	Table T_SHARDING is already configured in database 12

- ◆ When the original table is restored with another table name, the table name is already created. As shown below:

History Record							
Management > Table Recycle Bin > History Record							
Please select LogDB		Filter by the original table name					
■ LogDB	Original table name	Temporary table name	Original table type	restored table name	Execution User	Operation Time	
■ RT_TEST	T_SHARDING	HOTDB_TEMP_14_20200520183322	Sharing Table	T_SHARDING_02	cxd	2020-05-20 18:58:04	Table T_SHARDING_02 is already created

- ◆ Among two tables of parent-child relation, the parent table has been deleted when the child table is restored. As shown below:

History Record							
Management > Table Recycle Bin > History Record							
Please select LogDB		Filter by the original table name					
■ LogDB	Original table name	Temporary table name	Original table type	restored table name	Execution User	Operation Time	
■ RT_TEST	C	HOTDB_TEMP_4_20200519165952	Sharing Table	C	cxd	2020-05-19 16:59:52	parent table P is not created

- ◆ Among two tables of parent-child relation, the parent table has deleted part of the data associated with the child table when the child table is restored. As shown below:

History Record							
Management > Table Recycle Bin > History Record							
Please select LogDB		Filter by the original table name					
■ LogDB	Original table name	Temporary table name	Original table type	restored table name	Execution User	Operation Time	
■ RT_TEST	T_C	HOTDB_TEMP_22_20200519162039	Sharing Table	T_C	cxd	2020-05-19 16:20:39	can't find the position of parent table's record by the information you offered

- ◆ Among two tables of foreign key relation, the parent table has been deleted when the child table is restored. As shown below:

History Record									
Management > Table Recycle Bin > History Record									
Please select LogID		Original table name		Temporary table name	Original table type	restored table name	Execution User	Operation Time	C: Cannot add foreign key constraint
■	LogID	Original table name	Temporary table name	Original table type	restored table name	Execution User	Operation Time	C: Cannot add foreign key constraint	Success
■	RT_TEST	C_FK	HOTDB_TEMP_15_20200520163832	Sharding Table	C_FK	cxd	2020-05-20 16:38:45	C: Cannot add foreign key constraint	Failure

- ◆ Among two tables of foreign key relation, the parent table has deleted part of the data associated with the child table when the child table is restored. As shown below:

History Record									
Management > Table Recycle Bin > History Record									
Please select LogID		Original table name		Temporary table name	Original table type	restored table name	Execution User	Operation Time	C: Cannot add update a child row a foreign key constraint fails
■	LogID	Original table name	Temporary table name	Original table type	restored table name	Execution User	Operation Time	C: Cannot add update a child row a foreign key constraint fails	Success
■	RT_TEST	C_FK	HOTDB_TEMP_17_2020052016400	Sharding Table	C_FK	cxd	2020-05-20 16:54:16	C: Cannot add update a child row a foreign key constraint fails	Failure

- If the restored table has existed, a prompt box “The restored table is already defined. Whether to delete the existing table before restore?” will pop up during the restore. Click Confirm to delete the existing table to the recycle bin, as shown below:

Table Recycle Bin									
Management > Table Recycle Bin									
Please select LogID		Original table name		Temporary table name	Original table type	Data Amount	Execution IP	Execution User	Deletion time
■	LogID	Original table name	Temporary table name	Original table type	Data Amount	Execution IP	Execution User	Deletion time	Remaining time
■	RT_TEST	T_SHARDING	HOTDB_TEMP_16_20200518182843	Sharding Table	32KB	192.168.230.102	cxd	2020-05-18 18:28:43	1hour46min
■	RT_TEST	T_VERTICAL	HOTDB_TEMP_13_20200518182258	Vertical Sharding Table	16KB	127.0.0.1	cxd	2020-05-18 18:22:58	1hour38min
■	RT_TEST	T_ROUTE	HOTDB_TEMP_15_20200518182311	Sharding Table	32KB	127.0.0.1	cxd	2020-05-18 18:23:11	1hour38min
■	test	T_TEST	HOTDB_TEMP_8_20200518182218	Sharding Table	32KB	127.0.0.1	cxd	2020-05-18 18:22:18	1hour37min

- Table with foreign key relation, if data status is normal, will reestablish the foreign key relation after restore.

17.7.8. History record

Table Recycle Bin									
Management > Table Recycle Bin									
Please select LogID		Original table name		Temporary table name	Original table type	Data Amount	Execution IP	Execution User	Deletion time
■	LogID	Original table name	Temporary table name	Original table type	Data Amount	Execution IP	Execution User	Deletion time	Remaining time
■	RT_TEST	T_SHARDING	HOTDB_TEMP_16_20200518182843	Sharding Table	32KB	192.168.230.102	cxd	2020-05-18 18:28:43	1hour46min
■	RT_TEST	T_VERTICAL	HOTDB_TEMP_13_20200518182258	Vertical Sharding Table	16KB	127.0.0.1	cxd	2020-05-18 18:22:58	1hour38min
■	RT_TEST	T_ROUTE	HOTDB_TEMP_15_20200518182311	Sharding Table	32KB	127.0.0.1	cxd	2020-05-18 18:23:11	1hour38min
■	test	T_TEST	HOTDB_TEMP_8_20200518182218	Sharding Table	32KB	127.0.0.1	cxd	2020-05-18 18:22:18	1hour37min

History Record							
Management > Table Recycle Bin > History Record							
Please select LogicDB		Filter by the original table name		Search deletion			
LogicDB	Original table name	Temporary table name	Original table type	restored table name	Execution User	Operation Time	OperationType Status
RT_TEST	T_C	HOTDB_TEMP_1_20200518174625	Sharding Table	T_C	cxd	2020-05-18 17:46:18	Success Failure ▲
RT_TEST	T_C	HOTDB_TEMP_0_20200518174004	Sharding Table	T_C	cxd	2020-05-18 17:40:14	Success Success
RT_TEST	T_C	HOTDB_TEMP_1_20200518160239	Sharding Table	T_C	cxd	2020-05-18 17:15:12	Success Success
RT_TEST	T_C	HOTDB_TEMP_1_20200518160239	Sharding Table	T_C	cxd	2020-05-18 16:02:53	Success Failure ▲
RT_TEST	T_C	HOTDB_TEMP_3_20200518133238	Sharding Table	T_C	cxd	2020-05-18 11:23:44	Success Success
RT_TEST	T_C	HOTDB_TEMP_1_20200518112156	Sharding Table	T_C	cxd	2020-05-18 11:21:56	Success Success
RT_TEST	T_P	HOTDB_TEMP_2_20200518112237	Sharding Table	T_P	cxd	2020-05-18 11:23:01	Success Success
RT_TEST	T_C	HOTDB_TEMP_1_20200518112216	Sharding Table	T_C	cxd	2020-05-18 11:22:45	Success Failure ▲
RT_TEST	T_C	HOTDB_TEMP_1_20200518111449	Sharding Table	T_C	cxd	2020-05-18 11:22:02	Success Success
RT_TEST	T_SHARINGD	HOTDB_TEMP_0_20200518104722	Sharding Table	T_SHARINGD	cxd	2020-05-18 10:47:46	Success Failure ▲

- Click History Record on the “Management -> Table Recycle Bin” page to enter the table recycle bin operation history page.
- You can view the history record by filtering through LogicDB and original table name.

17.7.9. Delete history record

History Record							
Management > Table Recycle Bin > History Record							
Please select LogicDB		Filter by the original table name		Batch deletion			
LogicDB	Original table name	Temporary table name	Original table type	restored table name	Execution User	Operation Time	OperationType Status
RT_TEST	T_C	HOTDB_TEMP_1_20200518174625	Sharding Table	T_C	cxd	2020-05-18 17:46:18	Success Failure ▲
RT_TEST	T_C	HOTDB_TEMP_0_20200518174004	Sharding Table	T_C	cxd	2020-05-18 17:40:14	Success Success
RT_TEST	T_C	HOTDB_TEMP_1_20200518160239	Sharding Table	T_C	cxd	2020-05-18 17:15:12	Success Success
RT_TEST	T_C	HOTDB_TEMP_1_20200518160239	Sharding Table	T_C	cxd	2020-05-18 16:02:53	Success Failure ▲
RT_TEST	T_C	HOTDB_TEMP_3_20200518133238	Sharding Table	T_C	cxd	2020-05-18 11:23:44	Success Success
RT_TEST	T_C	HOTDB_TEMP_1_20200518112156	Sharding Table	T_C	cxd	2020-05-18 11:21:56	Success Success
RT_TEST	T_P	HOTDB_TEMP_2_20200518112237	Sharding Table	T_P	cxd	2020-05-18 11:23:01	Success Success
RT_TEST	T_C	HOTDB_TEMP_1_20200518112216	Sharding Table	T_C	cxd	2020-05-18 11:22:45	Success Failure ▲
RT_TEST	T_C	HOTDB_TEMP_1_20200518111449	Sharding Table	T_C	cxd	2020-05-18 11:22:02	Success Success
RT_TEST	T_SHARINGD	HOTDB_TEMP_0_20200518104722	Sharding Table	T_SHARINGD	cxd	2020-05-18 10:47:46	Success Failure ▲

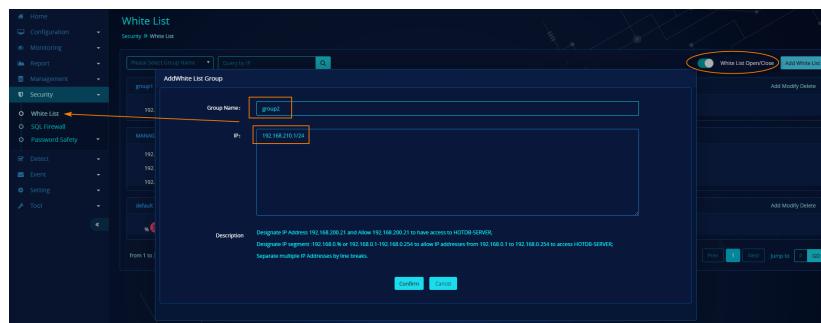
- Check the history records you want to delete and click Batch deletion.

18. Security

The security menu is mainly used for the security protection of the connection and execution of compute nodes, as well as the security management of relevant component passwords to improve the security of business systems.

18.1. White List

HOTDB Management supports the white list function which restricts hosts outside the white list from connecting to compute node services.



- To use the white list function, it needs to enable the white list switch in “Security->White list” first.
- It needs to use “[Reload](#)” to enable or disable the white list or to add, modify or delete white list information.
- After adding a host that can access the compute node, the host outside the white list will be intercepted when connecting to the compute node. Interception records can be viewed in “Event - > Audit Log - > [Safety Protection](#)”.

Special description:

Currently, only hosts in IP format can be configured, and the domain name format is not supported.

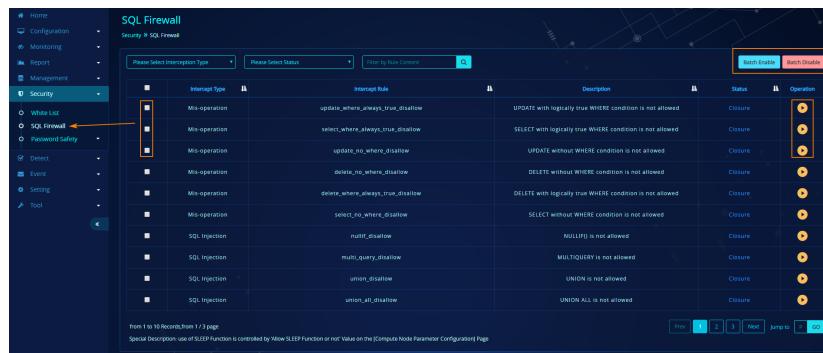
HotDB Management defaults to include a white list group with “MANAGEMENT” as the “group name” in the white list function, which contains the IP address of the server where the current HotDB Management is located. The white list group can not be

deleted or modified in the page.

When it needs to change the HotDB Management of compute node cluster, you have to first disable the white list function. It can be enabled after the new HotDB Management is started and the server IP of new HotDB Management is added to the white list, otherwise the IP address of new HotDB Management is not in the white list, which causes failure of HotDB Management to connect to compute nodes.

18.2. SQL Firewall

The “SQL Firewall” function provided by HotDB Management can intercept high-risk SQL, mis-operation SQL, etc. for users to improve system security.



Intercept Type	Intercept Rule	Description	Status	Operation
Mis-operation	update_where_always_true_dissallow	UPDATE with logically true WHERE condition is not allowed	Closure	
Mis-operation	select_where_always_true_dissallow	SELECT with logically true WHERE condition is not allowed	Closure	
Mis-operation	update_no_where_dissallow	UPDATE without WHERE condition is not allowed	Closure	
Mis-operation	delete_no_where_dissallow	DELETE without WHERE condition is not allowed	Closure	
Mis-operation	delete_where_always_true_dissallow	DELETE with logically true WHERE condition is not allowed	Closure	
Mis-operation	select_no_where_dissallow	SELECT without WHERE condition is not allowed	Closure	
SQL Injection	nullif_dissallow	NULLIF() is not allowed	Closure	
SQL Injection	multi_query_dissallow	MULTIQUERY is not allowed	Closure	
SQL Injection	union_dissallow	UNION is not allowed	Closure	
SQL Injection	union_all_dissallow	UNION ALL is not allowed	Closure	

SQL Firewall currently only supports the interceptable SQL templates provided by HotDB Management, and does not support custom SQL.

A single or batch can be enabled or disabled through “[Reload](#)”. If the intercepted SQL is executed in the compute node after it takes effect, it will prompt “ERROR 10029 (HY000): You are using SQL Firewall, this sql isn't allowed”.

Currently, HotDB Management provides 31 interceptable SQL templates, and records of intercepted SQL can be viewed in “Event - > Audit Logs - > [Safety Protection](#)”.

- In v.2.5.5 and above, an interception rule is added to the SQL firewall to support the interception of WHERE without sharding key, so as to improve the query efficiency of the system.

The management platform displays the rule "Not allowed to use WHERE without sharding key" on Security -> SQL Firewall, as shown below:

Intercept Type	Intercept Rule	Description	Status	Operation
Malfunction	sql_where_no_shardcolumn	不允许where条件不带分片键(Not allowed to use WHERE without sharding key)	Closure	
Malfunction	constants_compare_disallow	不允许使用常数比较(Comparison between constants is not allowed)	Closure	
Malfunction	update_limit_disallow	不允许UPDATE LIMIT(UPDATE LIMIT is not allowed)	Closure	
Malfunction	selectWildcard_non_noCache_disallow	不允许执行 * , SELECT /*+H40001 SQL_NO_CACHE */ * (SELECT /*+H40001 SQL_NO_CACHE */ * FROM ...)	Closure	
Malfunction	constants_operation_disallow	不允许使用常数操作(Operation of constants is not allowed)	Closure	
Mis-operation	set_password_disallow	不允许设置PASSWORD, 特殊绑定操作(Not allowed to use SET PASSWORD, except for special bindings)	Closure	
Mis-operation	modify_transaction_isolation_disallow	不允许修改事务隔离级别(Modify transaction isolation level is not allowed)	Closure	

This rule is closed by default. After it is opened, it requires the dynamic loading to take effect and the status will change to "Intercept in progress":

Intercept Type	Intercept Rule	Description	Status	Operation
Malfunction	sql_where_no_shardcolumn	不允许where条件不带分片键(Not allowed to use WHERE without sharding key)	Intercept in Progress	
Malfunction	constants_compare_disallow	不允许使用常数比较(Comparison between constants is not allowed)	Closure	
Malfunction	update_limit_disallow	不允许UPDATE LIMIT(UPDATE LIMIT is not allowed)	Closure	

When the status is "Intercept in progress", all WHERE without sharding key (associated field for the child table) executed on the service end of the compute node with the operation table of sharding table or child table will be intercepted.

For example:

Create a sharding table “teacher” with id as the sharding key. When the rule is opened, WHERE without sharding key is as shown in the following figure:

```
zcy@192.168.210.67:~mm 5.7.25-HotDB-2.5.5 11:00:38> select * from teacher where age = 49;
ERROR 1064 (HY000): Interception by sql firewall, because: not allowed to execute sql contained where condition without shard column
zcy@192.168.210.67:~mm 5.7.25-HotDB-2.5.5 11:01:19>
```

At the same time, you can see the relevant interception log through Event -> Audit logs -> safety protection:

Compute Node	Username	Access IP	Intercept Type	Intercept Details	Occurrence Time	Intercept Result	Intercept Remark
192.168.0.1	zcy	192.168.210.67	SQL Firewall	update teacher where age = 49	2020-05-26 11:07:39	Success	
192.168.0.1	zcy	192.168.210.67	SQL Firewall	select * from teacher where age = 49	2020-05-26 11:01:19	Success	

18.3. Password security management

Password security management can provide users with password validity monitoring reminders for compute node database users, data source connection users and backup users. When the password is about to expire, the users are automatically prompted to change the password to improve the system security.

18.3.1. Database user password

Description of empty page: If the record is displayed empty after entering the “Security -> Password Security Management -> Database User Password” page, it needs to check whether “Database User Password Expiration Alert” in “Setting -> Periodical Setting” is enabled. If the page is still empty after the switch is on, it needs to check whether the current database user password validity has reached the advance reminder time.

Expiration alert mode: When the “Database User Password Expiration Alert” is enabled, if the password validity has reached the advance reminder time, the pop-up window reminder prompts by default (if there is an expired user after logging in to HotDB Management, the pop-up window prompts); it can also notify database users of password expiration by email alert (it needs to be configured in “Event -> Email Alert Setting”).

(I) In-station alert description



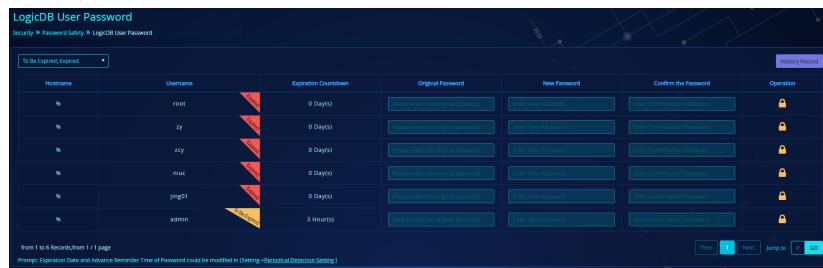
When a database user password expires, the login page will pop up a reminder window

to prompt how many users need to change the password in time, and the corresponding reminder will be given in the “[Event Notice](#)” in the upper right corner.

Users can click [Immediately modify] to jump to the “Security -> Password Security Management -> Database User Password” page to modify the password expired or to be expired.

Users can also click the [No Alert] button to close the pop-up window. The window will not pop up on the next login (if there is a new database user password expiration record, the pop-up window will prompt again).

(II) Password modification



The screenshot shows a table of database user records. The columns are: Username, Domain, Expiration Countdown, Original Password, New Password, Confirm the Password, and Operation. The rows contain the following data:

Username	Domain	Expiration Countdown	Original Password	New Password	Confirm the Password	Operation
root		0 Days(s)	Reset after the log-in password	Reset New Password	Reset Confirmation Password	
zy		0 Days(s)	Reset after the log-in password	Reset New Password	Reset Confirmation Password	
zcy		0 Days(s)	Reset after the log-in password	Reset New Password	Reset Confirmation Password	
muu		0 Days(s)	Reset after the log-in password	Reset New Password	Reset Confirmation Password	
jing01		0 Days(s)	Reset after the log-in password	Reset New Password	Reset Confirmation Password	
admin		3 Hours(s)	Reset after the log-in password	Reset New Password	Reset Confirmation Password	

From 1 to 6 Records, from 1 / 1 page
Warning: Expiration Date and Advance Reminder Time of Password could be modified in [Setting-objectual Detection Setting]

By default, the page only displays “To be Expired” and “Expired” database user records. In the Expired records, a red mark is displayed in the upper right corner of the “User Name” field, and “To be Expired” records have a yellow mark.

Click the password modification button in the “Operation” column to modify the database user password.

Click [History Record] to view the record of successful or failed modification.

Modifying the password of the exclusive user **root** account of HotDB Management connecting compute nodes requires the automatic execution of “[Reload](#)”. If Reload fails, the password modification operation also fails synchronously.

18.3.2. Data source password

Description of empty page: Refer to the description of empty page of the “[Database User Password](#)” chapter.

Expiration alert mode: Refer to the description of empty page of the “[Database User](#)

[Password](#)" chapter.

(I) In-station alert description



When there is a data source user to be expired or has expired, a prompt window will pop up when the user logs in to HotDB Management to select the compute node cluster and enters the home page, and a corresponding reminder will be given in the "[Event Notice](#)" in the upper right corner.

Users can click [Immediately modify] to jump to the "Security -> Password Security Management -> Data Source Password" page to modify the password expired or to be expired.

Users can also click the [No Alert] button to close the pop-up window. The window will not pop up on the next login (if there is a new data source user password expiration record, the pop-up window will prompt again)

(II) Password modification

Data Source User Password					
Security > Password Safety > Data Source User Password					
To be Expired, Expired	Filter by data source name			Search (F5)	Check/Setting
■	Data Source Example	Username	Expiration Countdown	Data Source Name	Operation
■	192.168.210.41:3308	hotdb_datasource	0 Day(s)	192.168.210.41_3108_db253	
■	192.168.210.42:3308	hotdb_datasource	0 Day(s)	192.168.210.42_3108_db253	
■	192.168.210.41:3307	hotdb_datasource	0 Day(s)	192.168.210.41_3107_db253	
■	192.168.210.44:3309	hotdb_datasource	0 Day(s)	192.168.210.44_3109_db253	
■	192.168.210.40:3307	hotdb_datasource	0 Day(s)	192.168.210.40_3107_db253	
■	192.168.210.43:3309	hotdb_datasource	0 Day(s)	192.168.210.43_3109_db253	
From 1 to 6 Records from 1 / 1 page Prompt: Expiration Date and Advance Reminder Time of Password could be modified in [Timing-Periodical Detection Setting]					
First Previous Next Last Jump to <input type="text" value="1"/>					

Display description

The records are displayed in the page in unit of data source instance. If the instances of multiple data sources are the same, they will be aggregated for display.

Username displays the “Connection User” and “Backup User” configured by the data source in HotDB Management (the actual configuration of backup user shall prevail).

Single modification

Click the [Modify] button in the “Operation” column of each record to modify the related user password of data source. The modified page automatically does not display the information of the record.

Batch modification

Batch modification can be executed through modifying multiple data source user passwords at one time in page record, or modifying all checked or default “Expired” and “To be Expired” records to the same password.

After executing the batch password modification tasks, the modification results will be prompted, including records of successful and failed modifications. The failed record can be viewed in the [History Record] page for the specific reason for failure.

(III) Special instruction

When the data source cannot be connected properly, the password modification operation will fail directly.

If multiple compute node clusters share one data source, users will be prompted not to modify.

When the configDB instance shares an instance with the data source and the accounts used are also the same, modification of the user will fail directly.

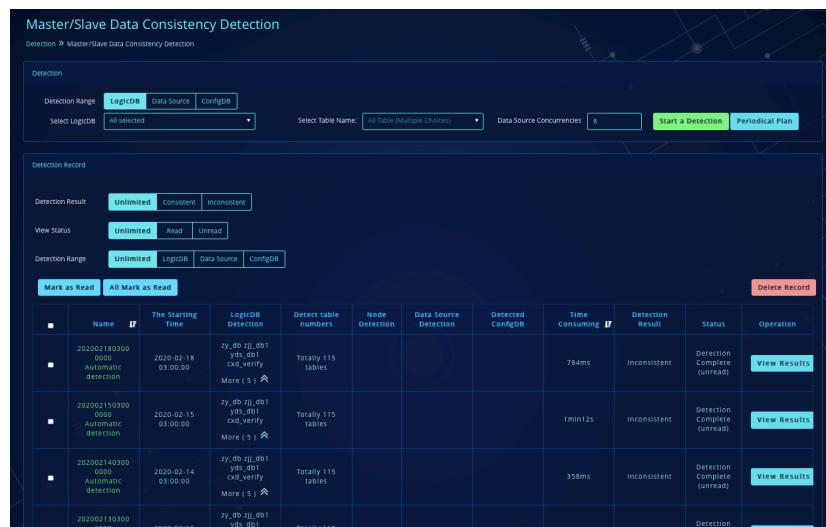
19. Detection

19.1. Master/Slave data consistency detection

When a data source or a compute node ConfigDB is running in a “master-master” or “master-slave” architecture, there may be problems of inconsistent data between the master and slave data sources due to replication latencies or other exceptions. HotDB Management supports finding hidden problem of data inconsistency through the “Master/Slave Data Consistency Detection” tool.

DR mode explanation: when the DR mode is enabled, please refer to the chapter "Master/Slave data consistency detection " in the [Distributed Transactional Database HotDB Server - Cross-IDC Disaster Recovery Function Specification](#) for the relevant logical explanations of the master/slave data consistency detection.

19.1.1. Start a detection



The screenshot shows the 'Master/Slave Data Consistency Detection' interface. At the top, there are tabs for 'LogicDB', 'Data Source', and 'ConfigDB'. The 'LogicDB' tab is selected. Below the tabs, there are dropdown menus for 'Select LogicDB' (set to 'All selected') and 'Select Table Name' (set to 'All Table (Multiple Choices)'). A 'Data Source Concurrency' input field is set to '8'. There are two buttons: 'Start a Detection' and 'Periodical Plan'.

The main area is titled 'Detection Record'. It contains a table with the following columns: Name, IF, Time Starting, LogicDB Detection, Detect table numbers, Node Detection, Data Source Detection, Detected ConfigDB, Time Consuming, IF, Detection Result, Status, and Operation. The table lists four detection records:

	Name	IF	Time Starting	LogicDB Detection	Detect table numbers	Node Detection	Data Source Detection	Detected ConfigDB	Time Consuming	IF	Detection Result	Status	Operation
■	202002100300 0000 Automatic detection		2020-02-18 03:00:00	zy_db_zj_db1 yds_db1 cxd_verify More (+) ↗	Totally 115 tables				784ms		Inconsistent	Detection Complete (unread)	View Results
■	202002100300 0000 Automatic detection		2020-02-15 03:00:00	zy_db_zj_db1 yds_db1 cxd_verify More (+) ↗	Totally 115 tables				1min12s		Inconsistent	Detection Complete (unread)	View Results
■	202002100300 0000 Automatic detection		2020-02-14 03:00:00	zy_db_zj_db1 yds_db1 cxd_verify More (+) ↗	Totally 115 tables				356ms		Inconsistent	Detection Complete (unread)	View Results
	202002100300 0000		2020-02-13	zy_db_zj_db1 yds_db1	Totally 115				1min12s		Inconsistent	Detection Complete (unread)	View Results

Step 1: Select the detection range, which is LogicDB by default.

LogicDB: detect data consistency between the master/slave data sources under the data node associated with the logicDB

Data source: specify the data consistency detection of data source under the data node

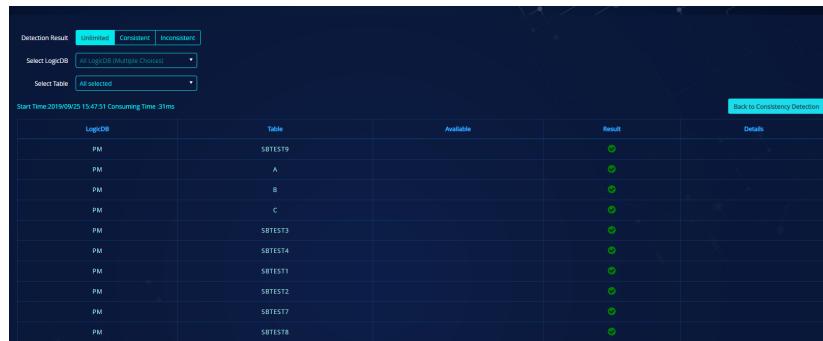
ConfigDB: detects the data consistency of the master/slave ConfigDBs in the compute node ConfigDB (master-slave or master-master replication structure)

Step 2: Select the logicDB or data node and data source to be detected.

Step 3: Configure data source concurrencies, i.e. the number of data sources can be detected at the same time, which is 8 by default and cannot exceed 32.

Step 4: Click the [Start a Detection] button to submit the detection task to the back end of compute node for execution. The progress of task execution can be viewed on the page.

View Results



LogiDB	Table	Available	Result	Details
PM	SHTEST9		●	
PM	A		●	
PM	B		●	
PM	C		●	
PM	SHTEST3		●	
PM	SHTEST4		●	
PM	SHTEST1		●	
PM	SHTEST2		●	
PM	SHTEST7		●	
PM	SHTEST8		●	

- After the task is executed, click [View Results] to view the specific detection details. If the detection results are inconsistent, the inconsistent data result records will be displayed. If there are a large number of inconsistent records, the inconsistencies will be displayed in the form of data intervals. If the number of inconsistencies exceeds 100,000 lines, manual positioning is required.
- Users can manually restore inconsistent data according to the detection execution details.
- Master/slave data consistency detection cannot be executed on table whose structure is not created or has no defined index.
- When data source is selected in the detection range, if the data source selected for

detection is the master data source under the current data node, the detection result will always be consistent (the master/slave consistency detection will always be based on the current master data source as the standard)

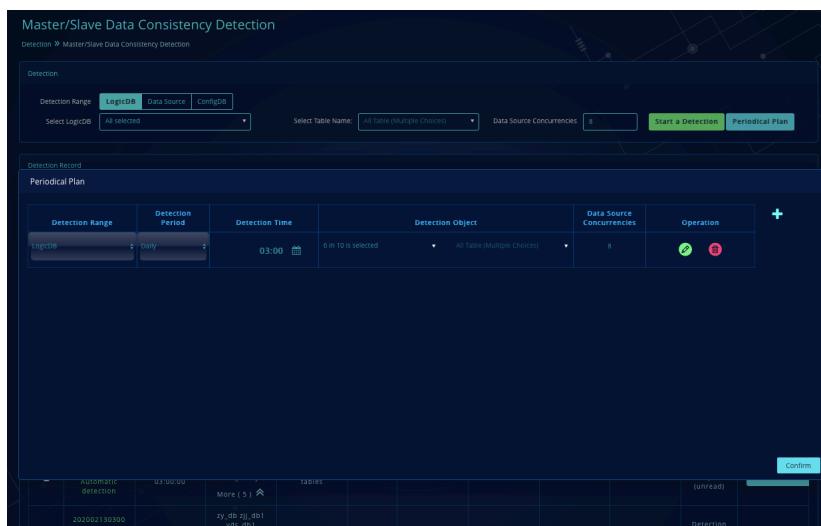
- If data node of the detected table is not configured with the corresponding "switching rule" or data source of the detected table is unavailable, the master/slave consistency detection cannot be performed for the table.



The screenshot shows the 'Detection Result Details' page. It has tabs for 'Unmarked', 'Consistent', 'Inconsistent', and 'Beyond Detection'. The 'Unmarked' tab is selected. It displays a table with columns: LogiDB, Table, Data Node, and Result. There are two rows for 'TEST_01S' and 'TEST01'. Both rows show a red circle icon in the 'Result' column, indicating failure. The 'Details' section below the table states: 'Table TEST01 cannot be detected because the data node dn_201681 where the table is located is not configured with `allow_cdc`' and 'Table TEST01 cannot be detected because the data node dn_201681 where the table is located is not configured with `allow_cdc`'. At the bottom, it says 'Item 2 / 2 Records/From 1 / 1 page' and 'Prompt: ① Detection Result Consistent ② Table cannot be detected ③ Detection Result Inconsistent'.

19.1.2. Periodical plan

In addition to manually starting the master/slave data consistency detection task, detection can also be executed automatically by adding a periodical task. Click [Periodical Plan] to manage the current periodical plan record.



The screenshot shows the 'Master/Slave Data Consistency Detection' page. It has tabs for 'Detection', 'Master/Slave Data Consistency Detection', and 'Detection Details'. The 'Master/Slave Data Consistency Detection' tab is selected. It includes fields for 'Detection Range' (set to 'LogiDB'), 'Data Source' (set to 'ConfigDB'), 'Select LogicDB' (set to 'All selected'), 'Select Table Name' (set to 'All Table (Multiple Choices)'), 'Data Source Concurrency' (set to '8'), and buttons for 'Start a Detection' and 'Periodical Plan'. Below this, the 'Periodical Plan' section shows a table with columns: Detection Range, Detection Period, Detection Time, Detection Object, Data Source Concurrency, and Operation. One row is listed: 'LogiDB' under 'Detection Range', 'Daily' under 'Detection Period', '03:00' under 'Detection Time', 'All Table (Multiple Choices)' under 'Detection Object', '8' under 'Data Source Concurrency', and a green circle and red circle under 'Operation'. At the bottom, there is a table for 'Automatic Detection' showing tasks for 'zy_db_zj_db1' and 'y95_db1'.

- At most six periodical plans can be added. The detection period includes “Daily”,

“Weekly” and “Monthly”.

- Other options can refer to description of starting a task manually.
- When the logicDB selected in periodical plan is consistent and the detection period and detection time overlap, the program will only execute one periodical task.
- Periodical plan is recommended to combine with the “Event -> [Email Alert Setting](#)” function. By adding an email alert setting, execution result exception will be alerted when the periodical plan execution is completed.

19.1.3. Notes

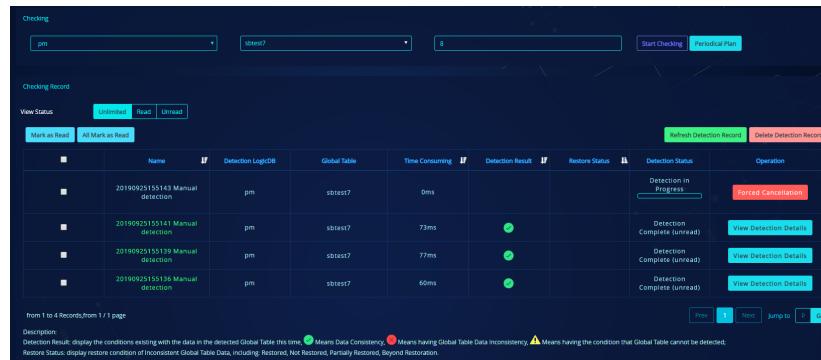
If there is actual data inconsistency between the master and slave, but the detection results are consistent, please check:

- Whether the detected table contains primary key or unique key.
- Whether the master/slave data sources under the detected data nodes are configured with "[switching rule](#)".
- Whether there is delay in the master/slave data sources under the detected data nodes. (view at the 3325 management end via the show @@latency command).
- Whether the configuration is loaded dynamically.

19.2. Global table data detection

It detects whether all global tables in the cluster have the same table structure and table data on each data node, and provides the function to restore inconsistent data online.

19.2.1. Start a detection task



The screenshot shows the 'Checking' interface with the following details:

- Checking Record:** LogicDB: pm, Global Table: sbtest7, Concurrency: 8.
- Start Checking** button is visible.
- Checking Record Table:**

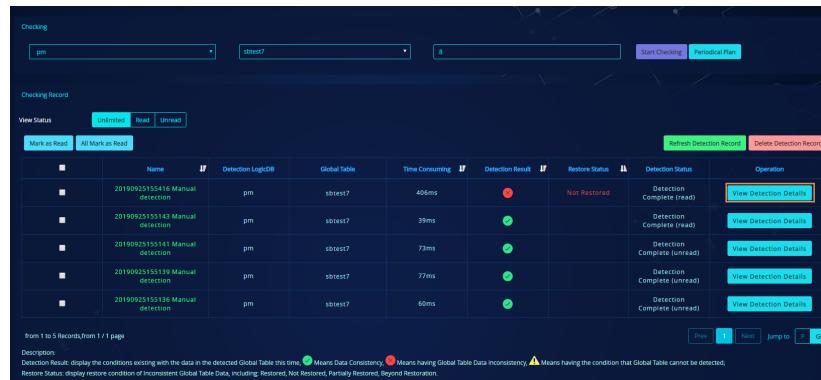
Name	Detection LogicDB	Global Table	Time Consuming	Detection Result	Restore Status	Detection Status	Operation
20190923151414 Manual detection	pm	sbtest7	0ms	● (green)	Not Restored	Detection in Progress	Forced Cancellation
20190923151414 Manual detection	pm	sbtest7	73ms	● (green)	Not Restored	Detection Complete (unread)	View Detection Details
20190923151414 Manual detection	pm	sbtest7	77ms	● (green)	Not Restored	Detection Complete (unread)	View Detection Details
20190923151414 Manual detection	pm	sbtest7	60ms	● (green)	Not Restored	Detection Complete (unread)	View Detection Details
- Description:** Detection Result: display the conditions existing with the data in the detected Global Table this time. ● Means Data Consistency. ○ Means having Global Table Data inconsistency. ▲ Means having the condition that Global Table cannot be detected.
- Restore Status:** display restore condition of inconsistent Global Table Data, including: Restored, Not Restored, Partially Restored, Beyond Restoration.

Step 1: Select the logicDB and the global table under the logicDB to be detected.

Step 2: Set the number of detection concurrency, which is 8 by default when it is empty and cannot exceed 32.

Step 3: Click the [Start Checking] button to submit the detection task to the back end of compute node for execution. The progress of the task being executed can be viewed on the page or the task execution can be canceled by clicking the [Forced Cancellation].

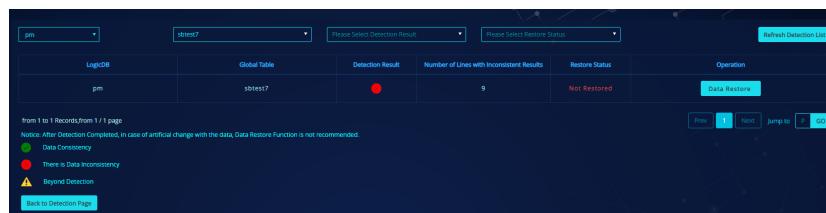
19.2.2. View detection details



The screenshot shows the 'Checking' interface with the following details:

- Checking Record:** LogicDB: pm, Global Table: sbtest7, Concurrency: 8.
- Start Checking** button is visible.
- Checking Record Table:**

Name	Detection LogicDB	Global Table	Time Consuming	Detection Result	Restore Status	Detection Status	Operation
20190923151414 Manual detection	pm	sbtest7	406ms	● (red)	Not Restored	Detection Complete (read)	View Detection Details
20190923151414 Manual detection	pm	sbtest7	39ms	● (green)	Not Restored	Detection Complete (read)	View Detection Details
20190923151414 Manual detection	pm	sbtest7	73ms	● (green)	Not Restored	Detection Complete (unread)	View Detection Details
20190923151414 Manual detection	pm	sbtest7	77ms	● (green)	Not Restored	Detection Complete (unread)	View Detection Details
20190923151414 Manual detection	pm	sbtest7	60ms	● (green)	Not Restored	Detection Complete (unread)	View Detection Details
- Description:** Detection Result: display the conditions existing with the data in the detected Global Table this time. ● Means Data Consistency. ○ Means having Global Table Data inconsistency. ▲ Means having the condition that Global Table cannot be detected.
- Restore Status:** display restore condition of inconsistent Global Table Data, including: Restored, Not Restored, Partially Restored, Beyond Restoration.



- Click the [View Detection Details] button of the detection task to view the detailed results of detection task.
- The detection results are divided into three: Data Consistency, There is Data Inconsistency, and Beyond Detection.

Data Consistency: The global table has the same data on all data nodes.

There is Data Inconsistency: The global table has inconsistent data on the data nodes. Inconsistent data can be restored online is judged through whether there is a [Data Restore] button in the operation column

Beyond Detection: The table cannot be detected due to some abnormal reason, including but not limited to the following reasons:

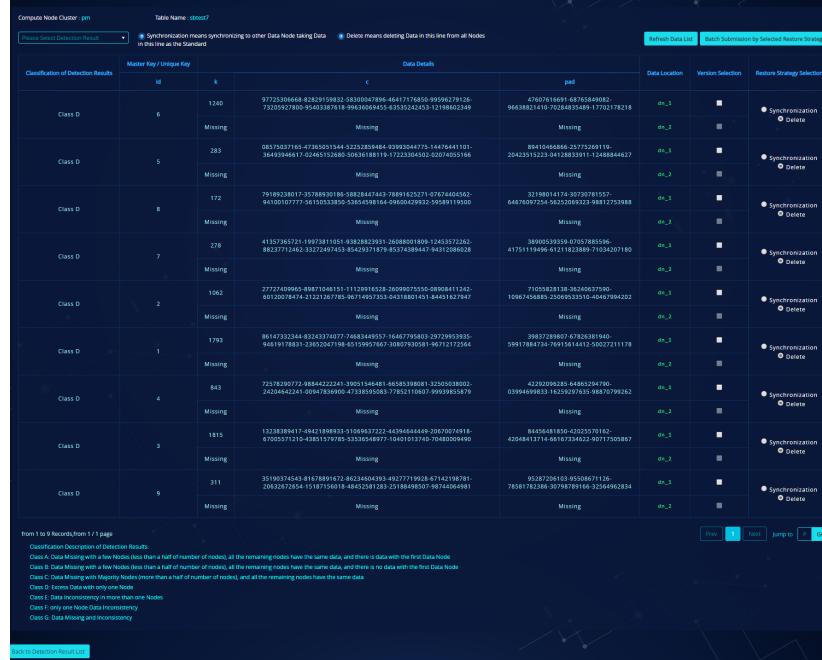
- Table has no index and cannot be detected
- The data node does not create the table structure of detection table and cannot be detected
- Table structure is not created and cannot be detected
- The compute node service status is abnormal and cannot be detected
- Beyond detection due to other reasons

- If the “Restore Status” is “Not Restored” in the record, the inconsistent data can be restored online by the [Data Restore] function. If the status is “Expired”, the restore cannot be executed.

Expired description: If the global table that has been detected is re-detected, the previous detection result will be invalid. When clicking [Data Restore], it will prompt “Data has expired, please re-detect”. When clicking [Refresh Detection List], the “Detection Status” is recorded as “Expired”.

Special case: If the global table that has been detected is re-detected but the detection task is manually canceled or fails due to the exception, the previous detection result will not be invalidated, data restore entry is still available, and the status will not change after refreshing the detection list.

19.2.3. Data restore



Data Restore currently supports the restore of the following seven types of data inconsistencies:

Class A: Data Missing with a few Nodes (less than a half of number of nodes); all the remaining nodes have the same data; there is data with the first Data Node, and the data inconsistency can be restored automatically.

Class B: Data Missing with a few Nodes (less than a half of number of nodes); all the remaining nodes have the same data; and there is no data with the first Data Node.

Class C: Data Missing with Majority Nodes (more than or equal to a half of number of nodes), and all the remaining nodes have the same data.

Class D: Excess Data with only one Node

Class E: Data Inconsistency in more than one Nodes

Class F: Only one Node Data Inconsistency

Class G: Data Missing and Inconsistency

- Data restore will display inconsistent data content in the table, and the version to be used can be selected according to the actual business situation. Check the checkbox in “Version Selection”, select [Synchronization] or [Delete], and then Click [Batch Submission by Selected Restore Strategy] to restore inconsistent data.
- When restoring, it is recommended to first select the restore strategy and version for all inconsistent data displayed on this page for unified submission, and then restore the inconsistent data record on the next page.
- After the restore is completed, the page automatically refreshes and hide the restored record. Click the [Back to Detection Result List] button to view the “Restore Status” on the page. The status is “Restored” under normal conditions.

19.2.4. Periodical plan

For the global table data detection periodical plan, please refer to the [Periodical Plan](#) description in “Master/Slave Data Consistency Detection”.

19.3. Table structure&index detection

Table Structure&Index Detection can be used to compare whether the table structures and index definitions in the compute node are consistent under each data node. Meanwhile, by detecting the table structure and the execution plan and execution time of the SQL statements related to the table, the optimization suggestions of the table structure or table index are provided.

Table Structure & Index Detection

Peterson > Table Structure & Index Detection

Periodical Detection

Periodical Plan	Detection Period	Detection Time	Operation
Weekly	Mon.	03:00	OK P
Weekly	Wed.	03:00	OK P
Weekly	Sat.	03:00	OK P

Detection Result

Table status: Please Select Table status | Select LogicDB: test_pc_jwy | Filter by Table Name: Refresh Detection Result

Detection Time: 2020-02-15 03:01:15

逻辑库	IF	表名称	IF	表状态	IF	表结构优化建议	索引优化建议	查看表结构
test_pc_jwy	pc_zd_jwy_auto	Normal				1.i.d. a. 此字段不存在NULL数据，建议修改为NOT NULL。 2.a. 此字段带下划线可能为状态标志位字段，建议修改为enumset类型。 3.当前表中超过一半字段没有默认值，建议添加默认值。 4.当前表中超过一半字段没有注释，建议添加注释。	1.当前表结构没有主键唯一键，建议添加自增字段的主键。 2.fk (A) 此索引检测时未被使用，建议检查后优化此索引。 3.i.d. 此分片字段参数较高，占总行数百分比大于10%，建议为此字段添加索引。	i
test_pc_jwy	pc_d_zwy_auto	Normal				1.i.d. a. 此字段不存在NULL数据，建议修改为NOT NULL。 2.a. 此字段带下划线可能为状态标志位字段，建议修改为enumset类型。 3.当前表中超过一半字段没有默认值，建议添加默认值。 4.当前表中超过一半字段没有注释，建议添加注释。	1.当前表结构没有主键唯一键，建议添加自增字段的主键。 2.a (A) 此索引检测时未被使用，建议检查后优化此索引。 3.i.d. 此分片字段参数较高，占总行数百分比大于10%，建议为此字段添加索引。	i

From 1 to 2 Records, from 1 / 1 page

Print View Edit Jump to Go

19.3.1. Start a detection

- Each refresh or entering into the “Table Structure & Index Detection” function page is a detection. [Refresh Detection Result] on the page can also be used for re-detection.
- Detection tasks can be executed automatically by adding a periodical plan. For introduction of periodical plan, please refer to the [Periodical Plan](#) description in “Master/Slave Data Consistency Detection”.

19.3.2. Page description

- Table records can be filtered by logicDB and table name.
- Tables with normal table structure, tables with abnormal table structure, tables with undefined table structure, and tables with abnormal index can be filtered and viewed.
- Table structure&index optimization suggestions are only provided for tables with "normal" table status or "undefined table index". Tables with table status of "table structure definition exception", "table index definition exception" and "table structure undefined" will be given specific location of data node over definition

exception in the optimization suggestions.

- Table structure optimization suggestions are listed as follows:
 - %s, there is no NULL data in this field, it is recommended to modify it to NOT NULL.
 - %s, the difference between the definition length of this field and the actual maximum length is greater than 256 characters. It is recommended to modify the definition length after viewing the table structure.
 - %s, this string field is of text type but the actual length is less than 3000 characters. It is recommended to change it to varchar\varbinary type or mediumtext\mediumblob type.
 - %s, this string field may be a status flag bit field. It is recommended to change it to enum\set type.
 - %s, this field is of timestamp type and the maximum time is greater than 2030. It is recommended to change it to datetime type.
 - In the current table, the field character set is not uniform. It is recommended to unify the character set and Latin1 and utf8mb4 are recommended.
 - More than half of the fields in the current table do not have default values. It is recommended to add default values.
 - More than half of the fields in the current table are not commented. It is

recommended to add comments.

- Table index optimization suggestions are as follows:
- %s(%s), this index was not used when it was detected. It is recommended to optimize this index after checking.
 - %s(%s), %s(%s), this index group is duplicated, it is recommended to keep only one index.
 - %s(%s), the cardinality of this index field is less than 100 or the cardinality divided by the total number of rows is less than 0.001, and the total number of table rows is less than 200. It is recommended to create other efficient indexes or combined indexes instead.
 - %s(%s), the index byte length is greater than 256 bytes and field prefix can achieve ideal selectivity. It is recommended to modify the index and take a reasonable length prefix, such as (the reasonable length prefix of this field).
 - %s(%s,%s), there is a difference of more than 10 times between the cardinality of two fields in this combined index. It is recommended to exchange the order and put the fields with low cardinality behind. For example, change to the index name (field name, field name).
 - %s(%s), %s(%s), this index group appears as combined indexes in 70% cases. It is recommended that one or more combined indexes should be set up reasonably, and delete the single index not used alone.
 - The current table structure does not have a unique primary key. It is recommended to add a primary key for the auto-incremental field.
 - The primary key of the current table structure is a long string, and the maximum byte length is greater than 32 bytes. It is recommended to add an auto-incremental field primary key, and change the existing primary key to a unique index.
 - The total execution consumption of non-complex SQL is more than 7200 seconds, and there is no efficient index. It is recommended to add a reasonable index.
 - %s, this field was used for the associated field of cross-node JOIN query. It is recommended to add an index for this field.

- %s, this sharding key has a high cardinality, and the cardinality divided by the total number of rows is more than 0.1. It is recommended to add an index for this field.
- %s, this field is used in more than 95% where conditions, and the specific values can be located to data less than 0.01% and less than 1000 rows or data less than 10 rows on average. It is recommended to add indexes for it.
- %s(%s), %s(%s), this is the combination of multiple AND in where condition. A single field has no efficient index, but the combination of multiple fields is of highly selectivity. It is recommended to add a combined index for it.
- %s(%s,%s), %s(%s,%s), this can be used as an efficient index in where condition. It is recommended to add a combined index for it.
- %s(%s), this index field is a long string field with a length greater than 64 characters. It is recommended to define the field length as "X"(X is calculated automatically by the management platform by default.)
- %s(%s), this index field is a time field and this index is an inefficient index, which is not located to data less than 0.01% and less than 1000 rows or is not frequently used. It is recommended to delete this index.

➤ Note:

➤ When in multi-node cluster mode and autoIncrement is set to 2 (auto-incremental and unique), if there is an auto-increment sequence in the table with the type of smallint, tinyint, mediumint, int, the table status column will be defined as "table structure definition exception". At the same time, the table structure optimization suggestion column will prompt that "After the global auto-increment and unique is enabled, bigint is the only type allowed for the auto-increment sequence in the table, so it is recommended that the type of id of auto-increment column be changed from tinyint to bigint", Click "Global auto-increment and unique" to jump to the parameter configuration page of compute node, as shown below:

Detection Result			
Table Status	Table Name	Table Status	Table Index optimization suggestions
LogicDB	T1	Table Structure is defined abnormal	Table structure optimization suggestions 1. When both auto-increment and unique configurations are enabled, the auto-increment sequence in the table only allows bigint type. It is recommended that the type of the self-increment field be changed to bigint. 2. This field is an auto-incremented field and of type XX. It is recommended to modify it to bigint. 3. More than half of the fields in the current table do not have default values. It is recommended to add default values. 4. Less than half of the fields in the current table are not commented. It is recommended to add comments.
cc	wwwwww	Table Structure is not defined	
cc_db	t_sharding	Table Structure is not defined	

- this verification rule verifies all tables with auto-increment columns enabled under all LogicDBs only when autoIncrement is set to 2, that is, "global auto-increment and unique" and the compute node mode is multi-node cluster.

19.3.3. Table structure details

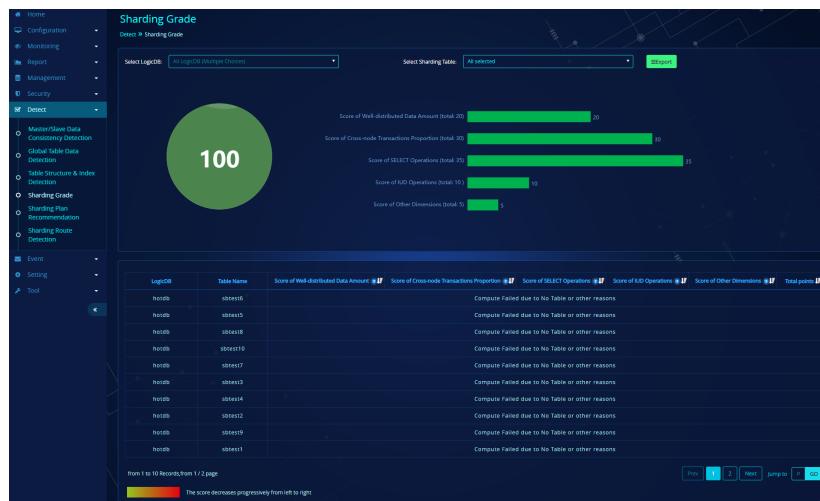
Table Structure Details																															
Demos > Table Structure & Index Detection > Table Structure Details																															
Table Name	pm_stress9																														
Table Definition Status	OK																														
Target Node	dn_1, dn_2																														
Node with Missing Table Definition																															
Node with Table Additionally Defined																															
Nodes Cannot be Connected																															
Definition Details	<table border="1"> <thead> <tr> <th>Current Node</th> <th>dn_1, dn_2</th> </tr> </thead> <tbody> <tr> <td></td><td></td></tr> </tbody> </table>	Current Node	dn_1, dn_2																												
Current Node	dn_1, dn_2																														
Build Table Statement	<pre>CREATE TABLE `stress9` (`id` int(11) NOT NULL AUTO_INCREMENT, `x` char(20) NOT NULL DEFAULT '', `c` char(60) NOT NULL DEFAULT '', `pad` char(60) NOT NULL DEFAULT '', PRIMARY KEY (`id`), KEY `X` (`x`)) ENGINE=innodb AUTO_INCREMENT=2001 DEFAULT CHARSET=utf8;</pre>																														
Structure	<table border="1"> <thead> <tr> <th>Field</th> <th>Type</th> <th>Null</th> <th>Key</th> <th>Default</th> <th>Extra</th> </tr> </thead> <tbody> <tr> <td>id</td> <td>int(11)</td> <td>NO</td> <td>PRI</td> <td>null</td> <td>auto_increment</td> </tr> <tr> <td>x</td> <td>char(20)</td> <td>NO</td> <td>MUL</td> <td>0</td> <td></td> </tr> <tr> <td>c</td> <td>char(60)</td> <td>NO</td> <td></td> <td></td> <td></td> </tr> <tr> <td>pad</td> <td>char(60)</td> <td>NO</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Field	Type	Null	Key	Default	Extra	id	int(11)	NO	PRI	null	auto_increment	x	char(20)	NO	MUL	0		c	char(60)	NO				pad	char(60)	NO			
Field	Type	Null	Key	Default	Extra																										
id	int(11)	NO	PRI	null	auto_increment																										
x	char(20)	NO	MUL	0																											
c	char(60)	NO																													
pad	char(60)	NO																													

- On the “Table Structure&Index Detection” page, click “Table Name” to view the table structure details.
- Details include: the data node of table, the current status of table, the build table statement, and the description of table field.
- Build Table Statement can be replicated through the [Replicate] button in the upper right corner of the page.
- For tables with inconsistent table structure under each data node, the page will display the Build Table Statement under each data node, and identify the inconsistent SQL statement with the red font.

19.4. Sharding grade

Sharding grade provides a reasonable score for a table after splitting. It can also obtain the average score according to the statistics of logicDB and multiple tables to help operators to find unreasonably split tables in time.

19.4.1. Description of grade dimensions



Sharding grade is divided into five dimensions:

- **Score of Well-distributed Data Amount**

Calculate the score according to whether the data distribution of each node is uniform and whether the growth is uniform

- **Score of Cross-node Transaction Proportion**

Calculate the score based on the proportion of cross-node transaction queries

- **Score of SELECT Operations**

Calculate the score according to whether the total queries of each node is uniform, the proportion of cross-node join queries, the proportion of single-database queries, and the proportion of queries that are routed to all nodes because they cannot be routed to the specified node.

➤ Score of IUD Operations

Calculate the score according to whether the IUD operation of each node is uniform and the single-database IUD operation proportion

➤ Score of Other Dimensions

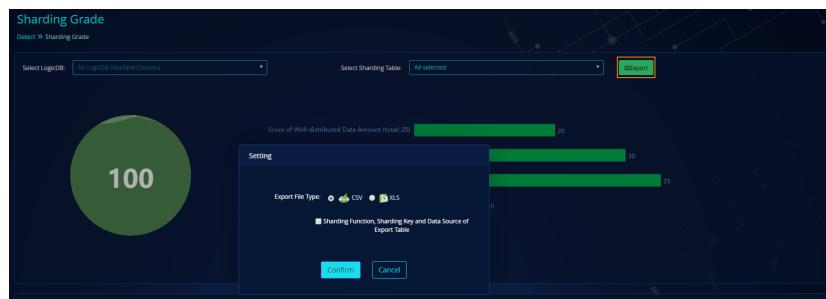
Calculate the score according to the number of times the query cannot find the node and whether the sharding key definition is reasonable.

Statistics description

- The compute node is responsible for the statistics and calculation of score. Each calculation is started at the start of compute node. If the compute node service is restarted, the previous statistics are cleared.
- The statistics and display of score can be performed only after 24 hours of the startup of compute node. Otherwise, it will prompt “calculation cannot be performed because the compute node starts for less than 24 hours”.
- If the compute node of master/slave mode cluster has a high-availability switch, calculation cannot be performed within 24 hours after the switch.

Note: Non-sharding table or table without table structure are not scored;

19.4.2. Record export



- Click the “Export” button on the “Sharding Grade” page to export the page record.
- Check the “Export Sharding Function, Sharding Key and Data Node of Table” to add “Sharding Function”, “Sharding Key” and “Data Node” columns after the

score record of each table.

- All records displayed on the page are exported by default after filtering the page records by the condition filter box.

19.5. Sharding plan recommendation

In order to help users find the appropriate table sharding solution through the actual business scenario, HotDB Management supports the sharding plan recommendation calculation through submitting the SQL log generated by the simulated pressure measurement environment to the compute node, to finally generate the business table sharding plan reference consistent with the actual production environment for users.

19.5.1. Start a recommendation

(1) Pre-start instructions

- The sharding plan recommendation function can only be used after the full simulated pressure measurement is started.

Full simulated pressure measurement: Connect the compute nodes to perform business operations according to the actual business situation. The business operations performed need to simulate the production environment business as much as possible.

- Before the full simulated pressure measurement, it needs to turn on the “Statistics of SQL Execution” parameter switch in “Configuration -> [Compute Node Parameters](#)”, and set the “Maximum Length of SQL Statement Record in SQL Execution Statistics” as large as possible to prevent statements from being truncated when executing SQL records.
- Before the full simulated pressure measurement, it is recommended to clear the history record log in the “Event -> [Slow Query Log Analysis](#)” function to prevent old data from interfering with the full simulated pressure measurement SQL record. After the history record log is cleared, you should execute the formal business SQL in the compute node and refresh the operation log page to make it the simulation initialization data.
- The SQL record switch in the “Event -> [Slow Query Log Analysis](#)” is temporarily

turned off in the calculation process started by the sharding plan intelligent recommendation function.

(II) Steps for starting a recommendation

The screenshot shows the "Sharding Plan Recommendation" page. It includes a sidebar with navigation items like Home, Configuration, Monitoring, Management, Security, and several sections under "Dedicated". The main area has tabs for "Sharding Plan Recommendation" and "Sharding Plan Audit". There are dropdowns for "LogicDB" (PM), "Table" (All selected), and "Table Status" (All unsharded). A note says "Warning: Table Without Simulated Pressure Measurement" and "Re-recommend Only Original Sharding Plan and Generated Plan". Below is a table with columns: LogicDB, Name, Table Type, Sharding Key, Table Size, Number of Lines with Simulated Pressure Measurement, Times Multiplier, Estimated Number of Lines for Production, Recommended Table Type, Recommended Sharding Plan, Alternative Sharding Plan 1, Alternative Sharding Plan 2, and Alternative Sharding Plan 3. The table lists multiple entries for PM tables.

- Click the [Start Task] button to start a sharding plan recommendation task, but if no SQL logs are recorded in the “Event -> [Slow Query Log Analysis](#)”, the task cannot be started.
- It is not allowed to start a task if there are recommendation tasks uncompleted currently.

The screenshot shows the "Start Task" page under "Sharding Plan Recommendation". It has a sidebar with "Start Task" and "Sharding Plan Recommendation". It includes dropdowns for "LogicDB" (PM) and "Table" (All selected). There are buttons for "Parameter Mode", "Times Multiplier", "Number of Lines", and "Batch Setting". A "Start Compute" button is at the bottom right. Below is a table with columns: LogicDB, Table Name, Number of Lines with Simulated Pressure Measurement, Times Multiplier, and Estimated Number of Lines for Production. The table lists several PM tables with their respective values.

- By default, all the tables in all logicDB of the cluster will be calculated and recommended when the task is started. Tables that do not need to be calculated and recommended can be filtered according to actual needs.
- The “Number of Lines with Simulated Pressure Measurement” of the table is the actual data line number of the table when performing full simulated pressure measurement. The number of lines with simulated pressure measurement of global table is the actual data line number plus node number.

- Configure “Times Multiplier” or “Estimated Number of Lines for Production” for each table before starting the task. This parameter is set to get closer to the actual execution scenario of business when calculating.

Times Multiplier:

Number of Lines with Simulated Pressure Measurement * Times Multiplier = Estimated Number of Lines for Production

Example 1: 10 days of operation of 1 million users in the simulated pressure measurement environment is simulated, but there are operations of 10 million users in the actual production environment and that data shall be stored for 90 days, the table times multiplier related to the service shall be set to 90.

Example 2: For the meta-information table such as configuration table, users can individually adjust the times multiplier of these tables to 1

Number of Lines:

Estimated Number of Lines for Production is the number of lines of the simulated table in the generated environment

Example 1: If a table has 1000 lines in the simulated pressure measurement environment, but the number of lines is estimated to reach 9900 in the actual production environment, the number of lines corresponding to the table may be set to 9900

- After selecting “Parameter Mode”, input the corresponding value directly in the right input box and click the [Setting Selected] (check the table to be set) or [Set All] (set all tables directly without checking) of [Batch Setting].
- Tables that have been set but need to be individually adjusted can be individually modified by the [Edit] button next to the parameter. Individually modified records are highlighted.
- Click [Start Compute] to start the sharding plan recommendation task for the selected and set tables. The page automatically displays the real-time execution of the current task.
- [Terminate Compute] can be executed during the execution process, but the recommended results displayed may be less accurate, so it shall be adopted with caution.

19.5.2. Sharding plan recommendation

Sharding Plan Recommendation										
Insert > Sharding Plan Recommendation										
LogID	File	Table	All selected	Table Status	All selected	Highlight Table Without Simulated Pressure Measurement	De-repetition Display of Original Sharding Plan and Generated Plan	More		
Please, This need the Generated Sharding Plan. All Tables are recommendation using rule of the File, and the Recommended Plan and the Alternative Plan can be adopted after saving.										
Generate Plan Time:2019-09-23 16:46:05 Task:Finding Middle-Point End Execution Consuming Time:54s										
Logical	Name	Table Type	Sharding Key	Table Status	Number of Lines with Simulated Pressure Measurement	Three Multiplier	Estimated Number of Lines for Production	Recommended Sharding Plan (0)Unrecommended SQL	Alternative Sharding Plan 1 (0)Unrecommended SQL	Alternative Sharding Plan 2 (0)Unrecommended SQL
File	air	Sharding Table	ID	Pressure Unmeasured	668136		668136	Sharing Table	ID	Sharing Table
File	stress01	Sharding Table	ID	Pressure Measured	3919		3919	Sharing Table	ID	Sharing Table
File	stress02	Vertical Sharding Table	ID	Pressure Unmeasured	2312		2312	Sharing Table	ID	Sharing Table
File	stress03	Sharding Table	ID	Pressure Measured	2000		2000	Sharing Table	ID	Sharing Table
File	stress08	Sharding Table	ID	Pressure Measured	2000		2000	Sharing Table	ID	Sharing Table
File	stress10	Sharding Table	ID	Pressure Measured	2000		2000	Sharing Table	ID	Sharing Table
File	stress09	Sharding Table	ID	Pressure Unmeasured	2000		2000	Sharing Table	ID	Sharing Table
File	stress02	Sharding Table	ID	Pressure Measured	2000		2000	Sharing Table	ID	Sharing Table
File	stress11	Sharding Table	ID	Pressure Measured	2000		2000	Sharing Table	ID	Sharing Table

- The page displays the results of the most recent successful recommendation, and the newly started record will overwrite the previous record.
- Click the “More” button to filter the page record by “Number of Lines with Simulated Pressure Measurement” and “Estimated Number of Lines for Production”.
- Tables to be viewed can be filtered out using page filtering condition. Records of repeated original sharding plan and generated plan can also be filtered by checking the “De-repetition Display of Original Sharding Plan and Generated Plan”.
- By default, three sets of recommend plans are generated. In general, the first one is optimal, and the latter two are alternatives.
- The generated plan includes the recommended table types: sharding table (representing the sharding table) + sharding key, and global table. When a sharding table is recommended, the plan does not include the sharding rule which needs to be selected by the user.
- Records with “Table Status” of “Pressure Unmeasured (not subjected to full simulated pressure measurement)” will be highlighted by the page. The recommended plan for this type of table **is not recommended** because it is not subjected to full simulated pressure measurement.
- The records in the page can be directly exported to the local. Click the [Export] button to export the records to be exported or all records.
- For tables that need to modify the table sharding plan, the sharding plan

modification can be directly completed by clicking [Online Modification].

Online modification notes:

- Click [Online Modification] to check the table record that needs to be modified, and click to directly link to the “Management -> Online Change of Sharding Plan” function page.
 - If the record checked is a parent table, the table structure is not created, and the table has been deleted, online modification cannot be performed.
 - If to adopt the generated sharding plan, all tables are recommended using one of the plans, and the recommended plan and the alternative plan cannot be adopted alternatively.
 - It is recommended to modify the sharding plan of tables with a JOIN correlation online in batches.
-
- When choosing a recommended plan, attention shall be paid to that some SQLs may not be executed. Click the [Unsupported SQL] button to view the SQL that may be unexecutable in the plan.

19.5.3. Influencing factors of sharding plan recommendation

Different number of lines and different sharding keys of a table will result in inconsistent results for the last recommended sharding.

The following factors will affect the sharding plan recommendation:

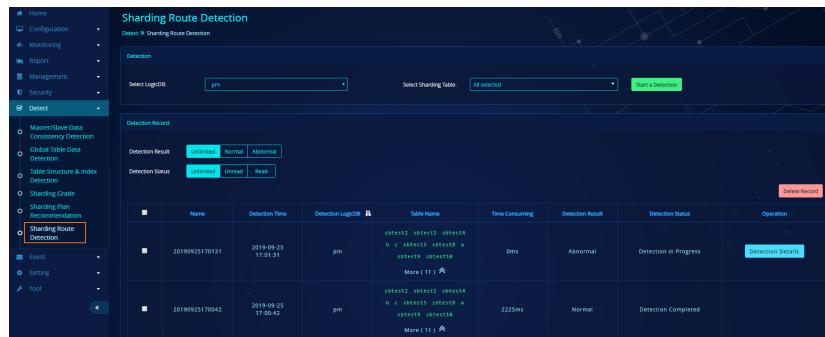
- The amount of data generated for table during the pressure measurement, and the generated test environment multiple or the number of lines set.
- In the query statement, the aggregate function, single/multi-node join statement, cross-node join, unsupported join statement, and cross-node/union statement will affect the sharding recommendation results.
- In the query or insert statement, the length of character, sharding table referred by foreign key, sharding key contained in primary key, and type of sharding key all affect the sharding recommendation result.

19.6. Sharding route detection

The sharding route correctness verification function can quickly solve problems of

verifying the correctness of sharding rule, whether the inserted data is routed according to the correct sharding rule, and whether the sharding data imported into the cluster by other distributed environments is inconsistent.

19.6.1. Start a detection

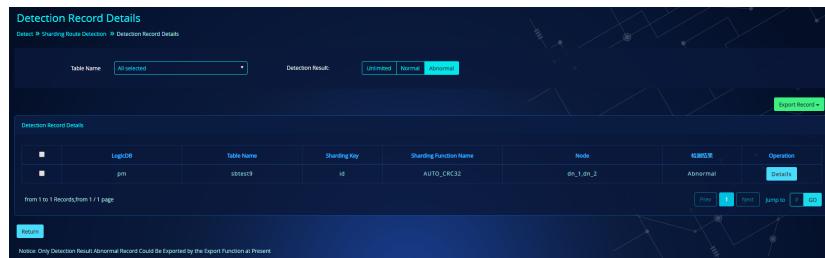


The screenshot shows the "Sharding Route Detection" page. On the left, there's a sidebar with navigation items like Home, Configuration, Monitoring, Report, Management, Security, and Detect. Under Detect, "Sharding Route Detection" is selected. The main area has tabs for "Detect" and "Sharding Route Detection". A search bar "Select LogicDB" with "pm" selected and a dropdown "Select Sharding Table" with "All sharding" are present. A green button "Starts Detection" is visible. Below this is a "Detection Record" section with two rows of data:

	Name	Detection Time	Detection LogicDB	Table Name	Time Consuming	Detection Result	Detection Status	Operation
<input checked="" type="checkbox"/>	20190925170131	2019-09-25 17:01:31	pm	shard1 shard2 shard3 N_1 shard1 shard2 shard3 More (11) ↗	0ms	Abnormal	Detection In-Progress	Detection Details
<input checked="" type="checkbox"/>	20190925170042	2019-09-25 17:00:42	pm	shard1 shard2 shard3 N_1 shard1 shard2 shard3 More (11) ↗	2225ms	Normal	Detection Completed	

- Select the logicDB and sharding table to be detected (excluding the table whose table type is child table), and click the [Start Detection] button for immediate detection.
- If the “Detection Result” of the completed detection task is “Normal”, there is no [Detect Details] button in the operation column. When it is “Abnormal”, click [Detect Details] to enter the “Detection Record Details” page.

19.6.2. Detection record details



The screenshot shows the "Detection Record Details" page. It has a top navigation bar with "Detect > Sharding Route Detection > Detection Record Details". A search bar "Dete Name" with "All selected" and a "Detection Result" filter with "Abnormal" selected are present. Below this is a "Detection Record Details" table with one row of data:

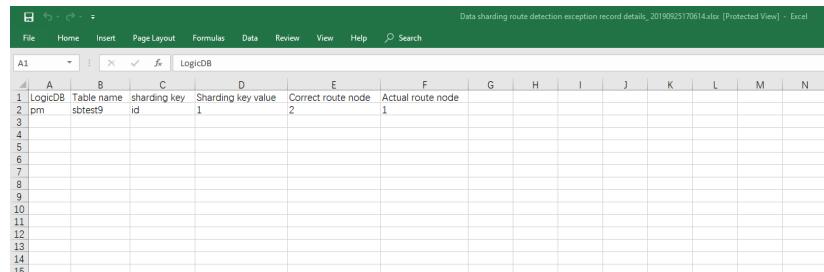
	LogicDB	Table Name	Sharding Key	Sharding Function Name	Node	ABNORMAL	Operation
<input checked="" type="checkbox"/>	pm	stress09	id	AUTO_CRC32	dn_1 dn_2	Abnormal	Details

Below the table, a note says "From 1 to 1 Records, from 1 / 1 page". There are "Return" and "Notice" buttons at the bottom.

- “Detection Record Details” mainly displays the detection records of all detection tables in the detection task. By default, table records with abnormal “Detection Result” are displayed.

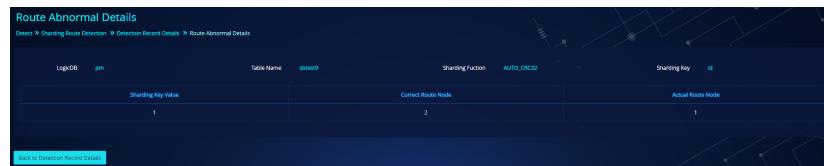
- For specific table route exception information, click [Details] to enter the “Route Abnormal Details” page.
- Click the [Export Record] button to save tables with abnormal route to the local.
Note: The export function currently only supports exporting route records with abnormal detection results.

 Data sharding route detection exception record details_20190925170614.xlsx



A1	B	C	D	E	F	G	H	I	J	K	L	M	N
1	LogicDB	Table name	sharding key	Sharding key value	Correct route node	Actual route node							
2	pm	sbtest9	id	1	2	1							
3													
4													
5													
6													
7													
8													
9													
10													
11													
12													
13													
14													
15													

19.6.3. Route abnormal details

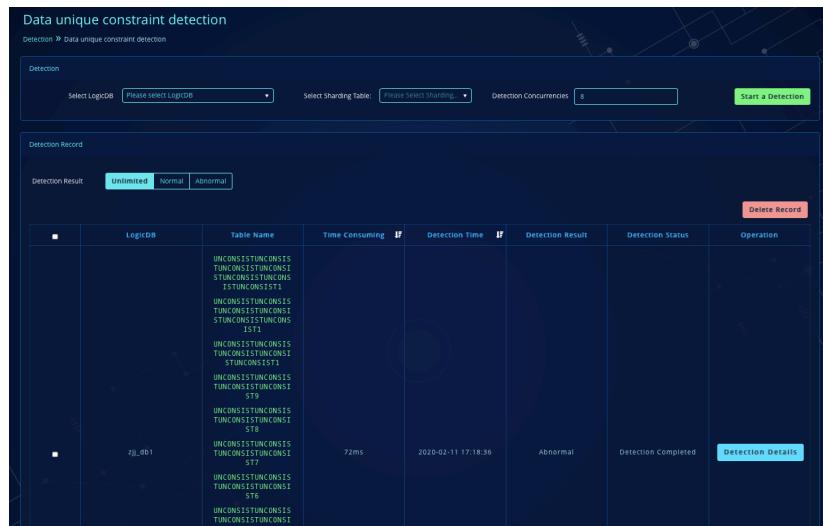


- The correct route node and the actual route node in the table are displayed in the form of “Node ID value”.
- Click the [Load More] button to obtain more undisplayed records. 50 records are added each time the page is loaded. If all records are loaded, the button will be hidden.
- Click the [Back to Detection Record Details] page to jump to “Detection Record Details”.

19.7. Data unique constraint detection

Data unique constraint detection can check the uniqueness of the historical data of the created horizontal partition table or sub table. It can help users to detect whether the columns with unique constraints have data conflicts in the distributed environment.

19.7.1. Start a detection



LogicDB	Table Name	Time Consuming	Detection Time	Detection Result	Detection Status	Operation
zjj_db1	UNCONSISTINGONSIS TUNCONSISTONCONSI STCONSISTONCONSI TSTCONSISTONCONSI ST7	72ms	2020-02-11 17:18:36	Abnormal	Detection Completed	Detection Details
	UNCONSISTINGONSIS TUNCONSISTONCONSI ST7			Normal		

Steps for starting a detection

- Select the LogicDB and sharding table for detection. among The sharding table can only be an already created sharding table or a subtable.
- The default detection concurrency is 8, which can be adjusted according to the actual needs, but the maximum value is no more than 32.
- Click [Start a Detection] to perform the unique constraint detection for the selected table.

Reason for detection starting failure

Generally, the reasons for detection starting failure include but are not limited to the following situations:

- Compute node service failure.
 - The unfinished detection task due to the management platform service stopping.
 - Manual cancellation of detection task.
 - Other exceptions (for details, see the prompt description in the exception identification).

3. Click [Delete Record] to delete the history detection record on the page. If the record has a result file generated during detection (when the details of detection results exceed 2048 bytes, the results are saved in the form of a file), the corresponding file will be deleted.

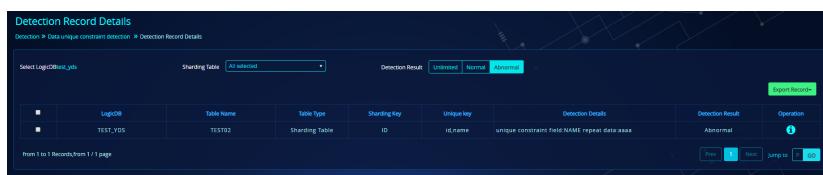
19.7.2. Detection record details

Detection Record Details									
Detection > Data unique constraint detection > Detection Record Details									
Select LogicDB[...].db1		Sharding Table		All selected	Detection Result		Unlimited	Normal	Abnormal
Export Records									
■	LogicDB	Table Name	Table Type	Sharding Key	Unique key	Detection Details		Detection Result	Operation
■	zjj_db1	unconsistunconsistunconsistunconsistunconsist	Sharding Table	ID	id,jd1			Normal	i
■	zjj_db1	unconsistunconsistunconsistunconsistunconsist	Sharding Table	ID	id,jd1			Normal	i
■	zjj_db1	unconsistunconsistunconsistunconsistunconsist	Sharding Table	ID	id,jd1			Normal	i
■	zjj_db1	unconsistunconsistunconsistunconsist1	Sharding Table	ID	id,jd1			Normal	i
■	zjj_db1	unconsistunconsistunconsistunconsist9	Sharding Table	ID	id,jd1			Normal	i
■	zjj_db1	unconsistunconsistunconsistunconsist8	Sharding Table	ID	id,jd1			Normal	i
■	zjj_db1	unconsistunconsistunconsistunconsist7	Sharding Table	ID	id,jd1			Normal	i
■	zjj_db1	unconsistunconsistunconsistunconsist6	Sharding Table	ID	id,jd1			Normal	i
■	zjj_db1	unconsistunconsistunconsistunconsist5	Sharding Table	ID	id,jd1			Normal	i
■	zjj_db1	unconsistunconsistunconsistunconsist49	Sharding Table	ID	id,jd1			Normal	i

1. The detection record details page shows the detection results of the corresponding table in the detection task. By default, only the table records with abnormal "detection results" are displayed.
 2. The unique key column in the displayed record displays the fields with unique constraints in the table. When there are multiple unique keys, they are separated by commas; if there are unique constraints composed of multiple field associations, they

are shown in brackets.

3. "Detection details" is the specific result description of the detected table. If "detection results" is abnormal, the column will display unique constraint fields and repeated data; if the result is normal, the column is empty.
4. When the detection details of the table exceed 2048 bytes, the "detection details" column will no longer display the specific repeated data, but will prompt that the specific details need to be downloaded for viewing.
5. Click the [View table information] button on the right to enter the detailed description page of the specific table. If the content of "detection details" in the table exceeds 2048 bytes, the [Download] button will appear in the operation column. Click the button to obtain the corresponding file (the file is generated according to the needs after the compute node detection and saved in the HotDB-TEMP / directory in the installation directory of the compute node by default).
6. Click [Export Record] to export all or part of the selected records on the page. Please note that the exported record does not include the record of normal "detection result".
7. If the unique constraint set in the table is prefix index, it can still be detected when the compute node version 2.5.6 and above.



The screenshot shows a table titled 'Detection Record Details' with the following data:

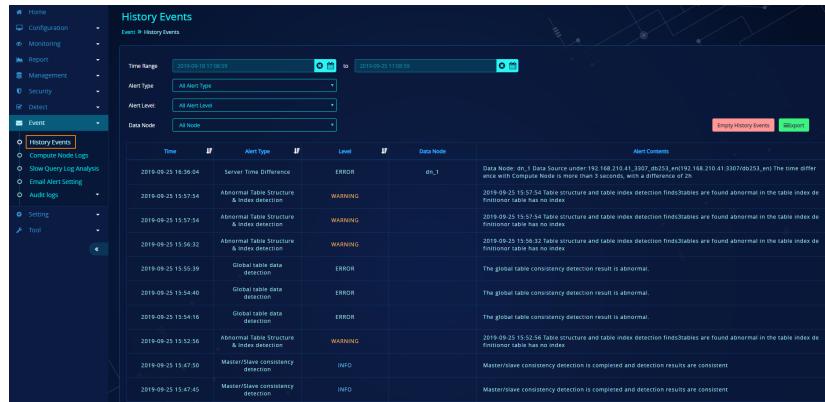
LogID	Table Name	Table Type	Sharding Key	Unique key	Detection Details	Detection Result	Operation
TEST_001	TEST02	Sharding Table	ID	ID_name	unique constraint field NAME repeat data area	Abnormal	

Below the table, there is a message: "from 1 to 1 Records from 1 to 1 page".

20. Events

20.1. History events

History events record and display history information at the HotDB Management platform level, including: task execution completion notification, periodical detection exception notification, and platform triggering alert prompt.



The screenshot shows the 'History Events' section of the HotDB Management Platform. The left sidebar has a tree view with nodes like Home, Configuration, Monitoring, Report, Management, Security, Audit logs, Event, History Events (which is selected and highlighted in orange), Compute Node Logs, Slow Query Log Analysis, Email Alert Setting, Audit logs, Setting, and Tool. The main area has a title 'History Events' and a sub-section 'Events > History Events'. It includes filters for Time Range (from 2019-09-18 11:00:00 to 2019-09-20 11:00:00), Alert Type (All Alert Type), Alert Level (All Alert Level), and Data Node (All Node). There are buttons for 'Empty History Events' and 'Delete'. Below these are two tabs: 'Alert Contents' (selected) and 'Logs'. A large table lists detected anomalies:

Time	Alert Type	Level	Data Node	Alert Contents
2019-09-20 16:56:04	Server Time Difference	ERROR	dn_1	Data Node: dn_1, Data Source: master (192.168.210.41, 3307, db513, en) and 192.168.210.41:3307/db253, en) The time difference between the data source server and the compute node server is more than 3 seconds, with a difference of 0s.
2019-09-20 15:57:34	Abnormal Table Structure & index detection	WARNING		2019-09-20 15:57:34 Table structure and table index detection findsTables are found abnormal in the table index detection table has no index
2019-09-20 15:57:34	Abnormal Table Structure & index detection	WARNING		2019-09-20 15:57:34 Table structure and table index detection findsTables are found abnormal in the table index detection table has no index
2019-09-20 15:58:32	Abnormal Table Structure & index detection	WARNING		2019-09-20 15:58:32 Table structure and table index detection findsTables are found abnormal in the table index detection table has no index
2019-09-20 15:55:39	Global table data detection	ERROR		The global table consistency detection result is abnormal.
2019-09-20 15:54:40	Global table data detection	ERROR		The global table consistency detection result is abnormal.
2019-09-20 15:54:40	Global table data detection	ERROR		The global table consistency detection result is abnormal.
2019-09-20 15:52:36	Abnormal Table Structure & index detection	WARNING		2019-09-20 15:52:36 Table structure and table index detection findsTables are found abnormal in the table index detection table has no index
2019-09-20 15:47:30	Master/Slave consistency detection	INFO		Master/slave consistency detection is completed and detection results are consistent
2019-09-20 15:47:45	Master/Slave consistency detection	INFO		Master/slave consistency detection is completed and detection results are consistent

20.1.1. Alert type description

➤ Server time difference

Description: HotDB Management periodically detects the time difference between the data source server and the compute node server. If there is a time difference, HotDB Management saves the detection result in the history event and prompts the user through the [Notice](#) in the upper right corner of the page.

Alert Level: The level is WARNING when the difference time is 0.5s-3s, and the level is ERROR when the difference time is more than 3s.

➤ Parameter perception

Description: The parameters of data source MySQL affect the processing of some commands by the compute node. Therefore, HotDB Management periodically checks

whether the parameters of each data source are consistent, and an alert is given if the parameters are inconsistent.

➤ **Data source is shared**

Description: HotDB Management will give an alert when the heartbeat detects that a data source is used by multiple compute nodes. The specific heartbeat detection mechanism is completed in the compute node, and the HotDB Management notifies the user of the detection result and displays the data source shared within 10 minutes.

➤ **Master/slave data consistency detection**

Description: It displays the detection result of whether the table structure, index and records on the master/slave data sources are consistent. The detection results are shown here.

➤ **Data source migration**

Description: When HotDB Management has performed a data source migration, a history event will be recorded to view whether the data source migration result is Successful, Failed, or Warning.

➤ **Periodic modification detection of database user password**

Description: When the database user password expiration reminder is enabled and it is detected that the database user password is about to expire or has expired, HotDB Management gives an alert and detailed information can be viewed in History Events.

➤ **Periodic modification detection of data source user password**

Description: When the data source password expiration reminder is enabled and it is detected that the data source user password is about to expire or has expired, HotDB Management gives an alert and detailed information can be viewed in History Events.

➤ Table structure&index detection exception

Description: When HotDB Management starts a “Table Structure & Index Detection” task, if the detection result is abnormal, HotDB Management records the abnormal detection result as a history event.

➤ Configuration modification backup failure

Description: When a user modifies certain configDB information under the HotDB Management configuration menu, the backup file of related logicDB may be affected. History events will record the failure of related logicDB backup file due to configuration modification. The level of this alert type is WARNING.

➤ Online change of sharding plan

Description: The history event records the task execution when the execution of “Online Change of Sharding Plan” task is completed. The level of this alert type is WARNING, ERROR and INFO.

➤ Global unique constraint exception

Description: When the global unique constraint of a created table fails to take effect or the global unique constraint is closed but the deletion of secondary index fails, an alert is given. The level of this alert type is WARNING.

➤ Compute node service status

Description: History events recorded when a compute node management port (3325 by default) or service port (3323 by default) is connected abnormally. The level of this alert type is ERROR; history events recorded when there is a switching or re-election in compute nodes in cluster mode. The level of this alert type is WARNING.

20.2. Compute node log

It records the log information generated by the compute node during the running process to help the user know the running status of the current compute node in real

time.

Compute Node Logs

Event: Compute Node Logs

Compute Node: HostDE_78

Time Range: 2019-09-25 17:09:56 to 2019-09-25 17:09:56

Log Type: All Types (Multiple Choices)

Log Level: All Levels (Multiple Choices)

View Status: All Unread Read

Log Contents

Mark as Read All Mark as Read highlight Advanced Log Refresh Log Log Setting Delete Log Download Log File

	Compute Node	View Status	Time	Level	Type	Log Contents	Operation
■	HostDE_78	Unread	2019-09-25 17:53:47	WARN	MANAGER	no same repl ds-record in new configuration datasource-id=1-modelid=1-192.168.210.78:3306/Compute Node ..	View Details
■	HostDE_78	Unread	2019-09-25 16:58:31	WARN	HEARTBEAT	Datasource-2 192.168.210.42:3307/repo25, an error came! Last packet sent at 2019-09-25 16:58:26.196, now (s..	View Details
■	HostDE_78	Unread	2019-09-25 16:53:49	ERROR	INIT	Startup error: java.net.BindException: Address already in use at sun.nio.ch.Net.bind(Native Method) ->[l.7,..	View Details
■	HostDE_78	Unread	2019-09-25 16:53:47	WARN	INIT	The datasource_time_zones are not consistent.	View Details
■	HostDE_78	Unread	2019-09-25 17:53:51	WARN	TRANSFER	connect(jd-id,modelid:1 192.168.210.43:3305/Compute Node_config on status 0/chardev util failed: msg Co..	View Details
■	HostDE_78	Unread	2019-09-25 16:51:48	WARN	FAILOVER	datanode -I switch datasource-1 to -1 in failover due to: MySQL Service Stopped	View Details
■	HostDE_78	Unread	2019-09-25 16:51:47	WARN	HEARTBEAT	datasource-1 192.168.210.43:3309/Compute Node_config on heartbeat failed due to connection already ..	View Details

20.2.1. View log

- Select “Compute Node” to switch to view the logs generated by other compute nodes in the cluster. The current master compute node running log is displayed by default.
 - The page displays logs of the recent one week by default, and logs can be viewed by adjusting the “Time Range”.
 - Logs can be filtered by log type.
 - Logs can be filtered by log level. Currently, the log types are divided into three levels: ERROR, WARNING and INFO.
 - Keyword can be input into the “Log Content” input box for fuzzy query of log information.
 - The page highlights the high-level log, that is, the ERROR level log information by default.
 - For detailed records of logs, click [View Details] for more detailed log information.

20.2.2. Log acquisition description

- HotDB Management takes a log file from the compute node every 10 minutes and writes it to the HotDB Management ConfigDB.

- The compute node log is stored in the compute node installation and deployment logs directory by default, which is usually hotdb.log. If there are too many log files, history log files will be saved in the form of date.
- HotDB Management defaults to obtain ERROR level log information and save it to the configDB. If it needs to obtain the WARNING or INFO level log, click [Log Setting] on the page to adjust.
- Click [Refresh Log] to obtain the latest log information in the configDB.
- Click [Download Log File] to save the compute node log to the local.

20.2.3. Log type description

The following is a description of all compute node log types:

Log type	Type description
AUDIT	Record all audit log related log information
AUTHORITY	Record license-related log information, such as checking whether the current data node exceeds the node limit contained in the license, etc.
BUFFER	Record cache-related log information, such as the failure to create direct caches, the size of the requested cache exceeds the set chunksize and other error messages
CCCONFIG	Record log information related to NDB connection configuration information, such as unsupported NDB service mode and other error messages
CCMETADATA	Record log information related to NDB metadata
CCONNECTION	Record log information related to NDB connection, such as error message of the maximum connections detected
CCPARSER	Record NDB log information related to SQL statement parsing, such as error message of unsupported SQL statements
CCRECORDRW	Record the read and write of NDB acquisition record, which refers to the log information when parsing from the SQL format to the NDB format, such as

	error message of unsupported column type or character set
CCSIGNAL	Record log information related to NDB signal parsing, such as error message of semaphore cannot be compressed
CCSQLBUILD	Record log information when the NDB protocol is parsed into a SQL statement
CLUSTER	Record log information related to the cluster, such as heartbeat detection information between clusters, cluster broadcast packet timeout information, etc.
CONNECTION	Record log information related to connection, such as INFO information that the front-end connection is closed due to a new connection requested in the bound session
CONNECTIONCLOSED	Record log information when the front-end connection is closed
CROSSDNJOIN	Record across-node JOIN query SQL statement
DDL	Record log information related to DDL, such as recording all DDL operations
DEADLOCK	Record log information related to deadlocks, such as exception information in deadlock detection
DISKSPACE	Record disk space-related log information, such as error message of detecting insufficient disk space caused by writing temporary files
EXIT	Record log information before the compute node is closed, for example, the data consistency detection result and the created temporary table are cleared before closing
FAILOVER	Record log information related to data source switching, such as data source manual switching failure due to unavailable data source
HEARTBEAT	Record log information related to the heartbeat detection, such as heartbeat detection failure due to the failure to obtain data source back-end connection, the heartbeat detection initialization abnormality, etc.

HOLD	Record log information related to HOLD operation, such as displaying the client information for sending the HOLD command, HOLD success or failure, etc.
HOTDBERROR	Record the custom ERROR of compute node. For details, please refer to Distributed Transactional Database HotDB Server [Compute Node Error Code]
HOTDBWARNING	Record the custom WARNING of compute node. For details, please refer to Distributed Transactional Database HotDB Server [Compute Node Error Code]
INIT	Record log information related to the initialization of compute node, for example, the compute node starts to monitor the management port at initialization, etc.
INNER	Record log information related to internal operations of compute node, such as failure to clear data nodes and create table configuration
JOIN	Record log information related to JOIN query, such as error message during JOIN query
LIMITOFFSETWITHOUTOR DERBY	Record SQL statements that use LIMIT but are not sorted
MANAGER	Log information related to management end, such as connection information when receiving the RELOAD command
MYSQLERROR	Record MySQL Error messages that appear in a connection, excluding deadlocks, lock timeouts, primary key or unique key conflicts, and foreign key violations
MYSQLWARNING	Record MySQL WARNING information that appears in a connection
NDB	Record log information related to NDB
ONLINEDDL	Record log information related to OnlineDDL, such as error message caused by OnlineDDL operation
RELATIVE	Record log information related to the auxiliary table of parent and child tables, such as error message of

	updating the parent and child tables related configuration (auxs column)
RESPONSE	Record log information related to back-end response when the back-end request is started, for example, the table structure does not exist after the back-end request is started
ROUTE	Record log information related to route, such as sharding type not meeting route conditions
SQL	Record log information related to executing SQL statements, such as error messages after executing a SQL statement
SQLFORWARD	Record the log information of forwarding the SQL log information from standby compute node to master compute node
SQLINTERCEPTED	Record statements intercepted by the SQL firewall
SQLKEYCONFLICT	Record MySQL ERROR information of primary key or unique key conflicts
SQLSYNTAXERROR	Record log information related to errors of executed SQL statements
SQLUNSUPPORTED	Record SQL statements that are not supported by the compute node, such as unsupported global function indexes
SUBQUERY	Record SQL statement of the subquery
SWITCHSOURCE	Record log information related to the data correctness guarantee after failover. For details, please refer to the “Data Correctness Guarantee after Failover” chapter of <i>Distributed Transactional Database HotDB Server [Standard] Function Manual</i>
TIMER	Record log information related to the timer, such as error information for delayed detection, completion of ONLINE operation executed by checkVIP timer, etc.
TRANSFER	Record log information related to data source migration, such as detecting whether the UUID of data source migration is empty or has been used
UNION	Record SQL statement of the UNION query

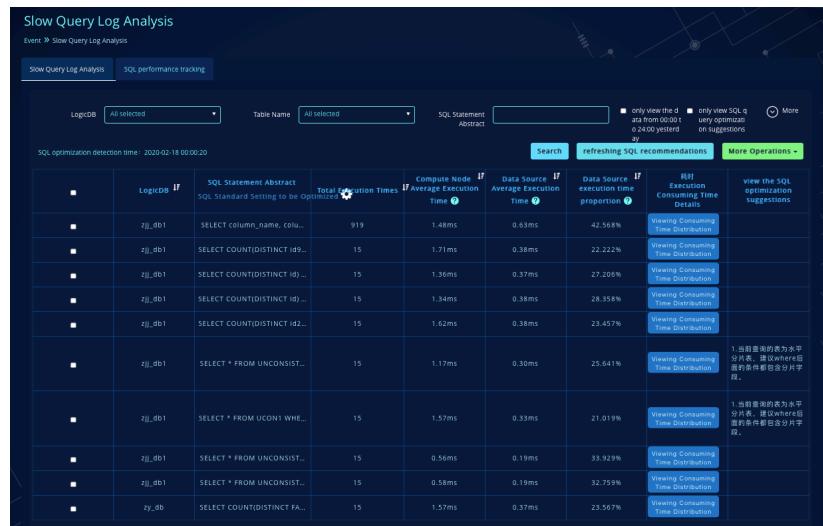
UNKNOWN	Record all log information except for other log types
WATCHDOG	Record log information of internal status monitoring of WATCHDOG related compute node service, such as detecting whether the compute node content has deadlocks

20.3. Slow Query Log Analysis

HotDB Management provides the Slow Query Log Analysis of the execution time and times details of SQL statements for select, insert, update, delete, transaction open, submission and rollback. The internal algorithm is used to automatically analyze the SQL statement that needs to be optimized and remind the user with the To-Be-Optimized mark. O&M personnel can also query the page statistics to obtain the actual SQL execution efficiency and SQL statements to be optimized to help improve system performance.

Enable Log Record: If the page is displayed as empty, it needs to check whether the SQL log statistics switch is enabled. Turn on the “Statistics on SQL implementation conducted or not” switch on the “Configuration -> [Compute Node Parameter Configuration](#)” page.

20.3.1. Slow query log record description



The screenshot shows the 'Slow Query Log Analysis' page. At the top, there are filters for 'LogicDB' (set to 'All selected'), 'Table Name' (set to 'All selected'), and 'SQL Statement Abstract'. Below these are checkboxes for 'only view the d from 00:00 to 23:00 yesterday' and 'only optimize on sessions'. A 'Search' button and a 'refreshing SQL recommendations' button are also present. The main area displays a table of slow queries:

LogicDB	SQL Statement Abstract	Total Execution Times	Average Execution Time	Data Source Average Execution Time	Data Source execution time proportion	RSS Execution Consuming Time Details	view the SQL optimization suggestions
zjj_db1	SELECT column_name, colu...	919	1.48ms	0.53ms	42.568%	Viewing Consuming Time Distribution	Viewing Consuming Time Distribution
zjj_db1	SELECT COUNT(DISTINCT id9...)	15	1.71ms	0.58ms	22.222%	Viewing Consuming Time Distribution	Viewing Consuming Time Distribution
zjj_db1	SELECT COUNT(DISTINCT id9...)	15	1.36ms	0.37ms	27.206%	Viewing Consuming Time Distribution	Viewing Consuming Time Distribution
zjj_db1	SELECT COUNT(DISTINCT id9...)	15	1.34ms	0.38ms	28.358%	Viewing Consuming Time Distribution	Viewing Consuming Time Distribution
zjj_db1	SELECT COUNT(DISTINCT id9...)	15	1.62ms	0.38ms	23.457%	Viewing Consuming Time Distribution	Viewing Consuming Time Distribution
zjj_db1	SELECT * FROM UNCONSIST...	15	1.17ms	0.30ms	25.541%	Viewing Consuming Time Distribution	Viewing Consuming Time Distribution
zjj_db1	SELECT * FROM UCONSIST WHE...	15	1.57ms	0.53ms	21.019%	Viewing Consuming Time Distribution	Viewing Consuming Time Distribution
zjj_db1	SELECT * FROM UNCONSIST...	15	0.56ms	0.19ms	33.929%	Viewing Consuming Time Distribution	Viewing Consuming Time Distribution
zjj_db1	SELECT * FROM UNCONSIST...	15	0.58ms	0.19ms	32.755%	Viewing Consuming Time Distribution	Viewing Consuming Time Distribution
zy_db	SELECT COUNT(DISTINCT FA...	15	1.57ms	0.37ms	23.567%	Viewing Consuming Time Distribution	Viewing Consuming Time Distribution

(I) Slow query log list field description

LogicDB: The name of the logicDB used for executing SQL.

SQL Statement Abstract: HotDB adopts the summary method similar to mysqldumpslow to group similar SQL statements. Here is the SQL after the summary.

Description of SQL Statement Abstract:

- The same SQL statements are accumulated in statistics
- In the SQL where condition, the constant string is replaced by "S" by default, and the constant value is replaced by "N". In some SQL where conditions, if the constant value is less than 10 or there is a constant with special meaning such as "Y" or "N", no replacement is performed and the original value is displayed.
- If the executed SQL statement has failed at the compute node level (for example, intercepting or not supporting SQL), the slow query log will not be recorded. If the SQL has been sent to the data source but the execution fails, the slow query log will still record the SQL execution information.
- The insert/replace values statement list, set statement list and update set statement list of inset set/insert onduplicate set do not determine whether the constant value is less than 10 or is a constant with special

meaning such as “Y” or “N”. It only needs to determine whether it is a value or string and display it with “S” and “N” (**valid in V2.5.3 and above**)

Compute Node Total Execution Times: Total execution times of all SQL statements of the SQL template in the compute node.

Compute Node Average Execution Time: It is calculated through dividing the compute node total execution time by the compute node total execution times. Compute node execution time refers to the time from the compute node receiving the first SQL statement packet to the compute node sending the last result packet of SQL; compute node total execution time refers to the total execution time of all SQL statements of the SQL template.

Data source Average Execution Time: It is calculated through dividing the data source total execution time by the data source total execution times. Data source execution time refers to the time from the compute node sending the first SQL statement packet to the back-end to the compute node receiving the last result packet of SQL from the slowest data node. If a SQL is split into n SQL for execution, the execution time is calculated in accumulation, while the processing time of the compute node in the progress is not included. Data node total execution time refers to the total execution time of all SQL statements of the SQL template.

Data Source Average Execution Time Proportion: the proportion of the data source average execution time in the compute node average execution time, with three decimal places reserved.

Time Consumption Distribution Details: the execution time distribution of all SQL statements of the SQL template in the compute node or data source can be viewed.

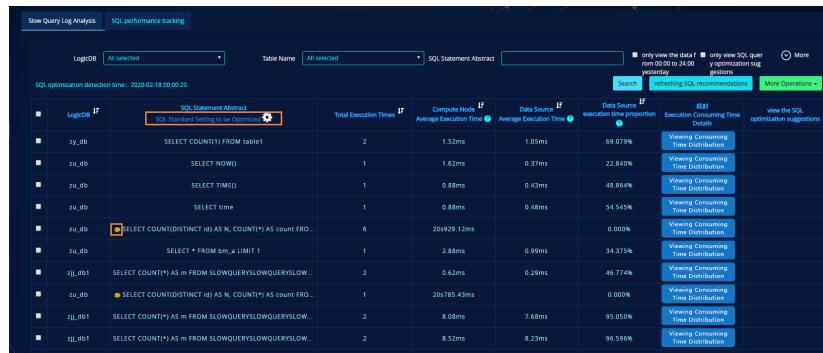
SQL Query Optimization Suggestions: the optimization suggestions for SQL query are given based on the internal algorithm.

(I) Compute time distribution



- Click [View Compute Time Distribution] to view the execution time distribution of SQL statements of the template in compute node or back-end data source.
- Execution compute time distribution is represented by a bar chart, which can be used to view the compute time interval with the maximum execution time.

(II) SQL to be optimized



The table displays slow query log analysis. The columns include LogID, SQL Statement Abstract, Total Execution Times, Compute Node IP, Data Source IP, Data Source execution time proportion, and Execution Consuming Time Details. A yellow snail icon indicates SQL statements that need optimization.

LogID	SQL Statement Abstract	Total Execution Times	Compute Node IP	Data Source IP	Data Source execution time proportion	Execution Consuming Time Details
zy_db	SELECT COUNT(*) FROM table1	2	1.52ms	0.37ms	69.07%	view the SQL optimization suggestions
zy_db	SELECT NOW()	1	1.62ms	0.45ms	22.84%	Viewing Consuming Time Distribution
zy_db	SELECT TIME()	1	0.88ms	0.48ms	48.86%	Viewing Consuming Time Distribution
zy_db	SELECT time	1	0.88ms	0.48ms	54.54%	Viewing Consuming Time Distribution
zy_db	SELECT COUNT(DISTINCT id) AS count FROM table1	6	20929.12ms		0.00%	Viewing Consuming Time Distribution
zy_db	SELECT * FROM dm_a LIMIT 1	1	2.88ms	0.99ms	34.07%	Viewing Consuming Time Distribution
zj_db1	SELECT COUNT(*) AS m FROM SLOWQUERYSLOWQUERYSLOW...	2	0.62ms	0.29ms	46.77%	Viewing Consuming Time Distribution
zj_db1	SELECT COUNT(DISTINCT id) AS N, COUNT(*) AS count FROM...	1	20978.43ms		0.00%	Viewing Consuming Time Distribution
zj_db1	SELECT COUNT(*) AS m FROM SLOWQUERYSLOWQUERYSLOW...	2	8.68ms	7.68ms	95.05%	Viewing Consuming Time Distribution
zj_db1	SELECT COUNT(*) AS m FROM SLOWQUERYSLOWQUERYSLOW...	2	8.52ms	8.23ms	96.59%	Viewing Consuming Time Distribution

- The SQL statement to be optimized is the SQL abstract with yellow snail mark on the page. In general, attention shall be paid to the SQL statement with this mark and low SQL execution efficiency shall be checked.
- For the standard for judging whether the SQL statement needs to be optimized, click the [SQL To-be-Optimized Setting] button to view or edit the standard setting to be optimized.

SQL To-be-Optimized Setting (Display To-Be-Optimized Mark if Meeting Any of a, b, c, d)

a: SELECT Query's Average Number of Lines Backed /100 Round Up to An Integer < SQL Total Execution ms, And the Average Execution Time in Compute Node Exceeds 5 s;

b: SELECT Query's Execution Exceeding 1440 Times in Recent One Day, and Compute Node's Average Execution Time Exceeds 10 s;

c: SELECT Query's Average Execution Time in HOTDB Exceeds 100 s;

d: Average Execution Time of UPDATE, DELETE and INSERT Statement in Compute Node Exceeds 100 s;

SQL Without Any Update for Above 3 Months Will be Removed Automatically

Notice that Average Execution Time Setting Rule of Compute Node in a, b, c is $c > b > a$

Save Cancel

(III) SQL query optimization suggestions

Slow Query Log Analysis

Event ▶ Slow Query Log Analysis

Slow Query Log Analysis SQL performance tracking

LogicDB All selected Table Name All selected SQL Statement Abstract

only view the data from 00:00 to 24:00 yesterday
only view SQL q uery optimized on suggestions

More

SQL optimization detection time : 2020-02-18 00:00:20

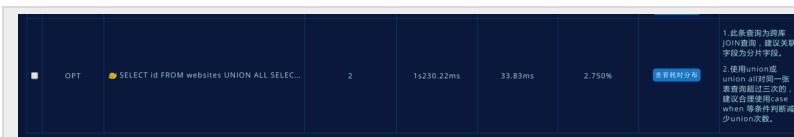
Search Refreshing SQL recommendations More Operations ▾

LogicDB	IF	SQL Statement Abstract	Total Execution Times	IF Compute Node Average Execution Time	IF Data Source Average Execution Time	IF Data source execution time proportion	IF Execution Consuming Time & Details	View the SQL optimization suggestions
■	zjj_gb1	SELECT * FROM UNCONST...	15	1.17ms	0.30ms	25.641%	Viewing Consuming Time Distribution	1.当前查询的表为水平分片表，建议where后面的条件都包含分片字段。
■	zjj_gb1	SELECT * FROM UCON1 WHERE...	15	1.57ms	0.39ms	21.019%	Viewing Consuming Time Distribution	1.当前查询的表为水平分片表，建议where后面的条件都包含分片字段。
■	zjj_gb1	SELECT * FROM UNCONST...	15	1.15ms	0.29ms	25.217%	Viewing Consuming Time Distribution	1.当前查询的表为水平分片表，建议where后面的条件都包含分片字段。
■	zy_db	SELECT * FROM SM_ZA_TB3 ...	15	1.67ms	0.27ms	16.168%	Viewing Consuming Time Distribution	1.当前查询的表为水平分片表，建议where后面的条件都包含分片字段。
■	zy_db	SELECT * FROM SM_Q3_TB4 ...	15	1.68ms	0.41ms	24.405%	Viewing Consuming Time Distribution	1.当前查询的表为水平分片表，建议where后面的条件都包含分片字段。
■	zy_db	SELECT * FROM SM_ZA_TB3 ...	15	1.65ms	0.28ms	16.970%	Viewing Consuming Time Distribution	1.当前查询的表为水平分片表，建议where后面的条件都包含分片字段。

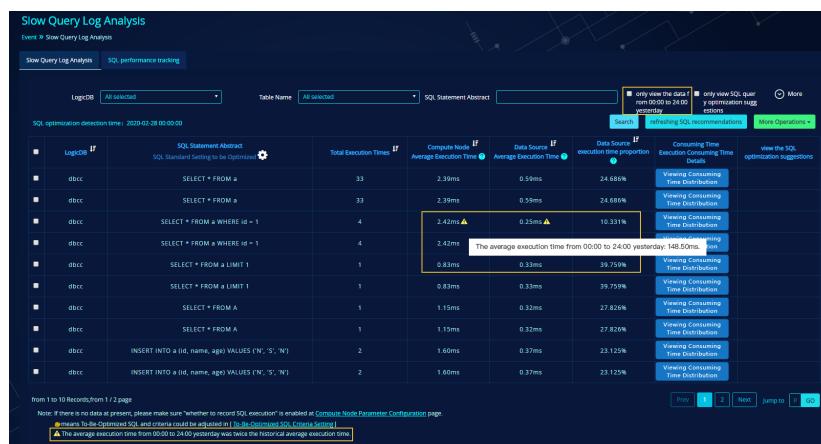
- Based on the internal algorithm of the management platform, this function checks the SQL statement structure, execution time, execution plan, etc., filters out unreasonable SQL statements, and gives optimization suggestions.
- Check the item "only view SQL query optimization suggestions" to filter out all the SQL statements proposed to be optimized.
- SQL suggestions are as follows:
 - The subqueries are nested in more than three layers. It is recommended to rewrite SQL according to business needs.

- If you use union or union all to query the same table more than three times, it is recommended to use case, when and other conditions to reduce the union usage.
- It is recommended to use union all instead of union according to business needs.
- The table being queried is a sharding table. It is recommended that the filter condition where contain sharding tables.
- This query is a cross-node JOIN query, and it is recommended that the associated field be a sharding key.

For example: this cross-node SQL JOIN query does not use the sharding key as the associated field. In this case, the compute node needs to cross-compare the data across the data nodes, which takes a lot of time. Therefore, suggestions are given for such SQL statements.



(IV) Average execution time is too long



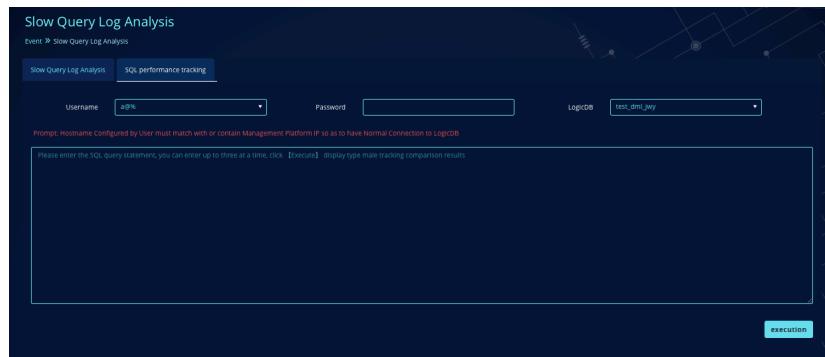
- For the compute node average execution time or the data source average execution time, if it is found that the average execution time from 0:00 to 24:00 yesterday is twice the average execution time of the history, a message with a triangle

identification will appear.

- Check the item "only view the data from 00:00 to 24:00 yesterday " to refresh the SQL execution condition from 00:00 to 24:00 yesterday.

20.3.2. SQL Performance Tracking

HotDB Management provides SQL performance tracking function, which visually shows the execution plan of SQL statements (HotDB Profiles). It can be used to compare and view the execution plan of a SQL statement before and after optimization, or to view the execution plan of a SQL statement separately.



- Input the username and password (the username and password are of the [database users](#) of the compute node), and select the LogicDB for query.

Note: host range set by User must contain IP address of the current HotDB Management service. Otherwise, the compute node cannot be connected normally.

- Enter SQL query statements, which can be entered up to three at a time. Click [Execute] to view the performance tracking comparison results. If the input SQL statement is not a SELECT statement or fails execution, an error message will be displayed.
- The execution plan will display the relative time point and time consumption (μ s) of each step. For details, please refer to the HotDB Profiles related sections in the [Distributed Transactional Database HotDB Server –\[Standard\] Function Manual](#).

SQL Statement		
compute node execution time	—	—
select * from ytb_test;	—	—
data source execution time	—	—
	relative time point	Time Consuming (μs)
Start receiving the first packet of SQL	0	NULL
Complete receiving the last packet of SQL	10	10
Complete Multquery parsing	77	66
Start SQL parsing	293	216
Complete SQL parsing	625	331
Start generating back-end SQL	625	NULL
Complete generating back-end SQL	9338150493048	-9338150493074
Start sending the first back-end SQL	2007	NULL
Complete sending the last back-end SQL	2302	294
Start receiving the first SQL result set packet	2114	NULL
Complete receiving the last SQL result set packet	2460	345
Start rewriting the result set received	2114	NULL
Complete rewriting of the received result set	2469	355
Start writing the first result set packet to the front end	2469	NULL
Complete writing the last result set to the front end	2567	97

view execution time diagram

- Click [View execution time graph] to view the visualized results of execution plan.
Only one execution time graph can be viewed at a time.



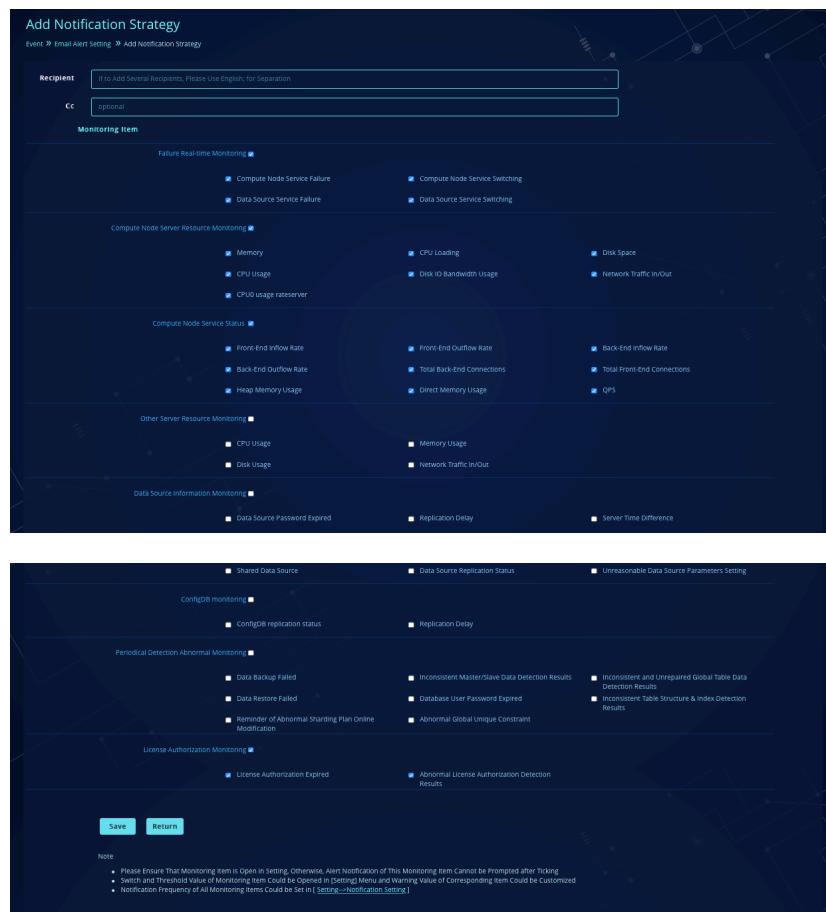
20.4. Notification strategy

HotDB Management supports the alert of faults or abnormalities that occur during cluster operations by emails. The current monitoring scope of email alerts includes: compute node and data source failure or switching, compute node service resource

status, compute node server status, data source related monitoring, system periodical task detection, and license authorization monitoring.

DR mode explanation: when the DR mode is enabled, please refer to the chapter "Notification strategy" in the [Distributed Transactional Database HotDB Server - Cross-IDC Disaster Recovery Function Specification](#) for the relevant logical explanations of the notification strategy.

20.4.1. Add notification strategy



Add Notification Strategy

Event > Email Alert Setting > Add Notification Strategy

Recipient

If to Add Several Recipients, Please Use English, for Separation
cc optional

Monitoring Item

Failure Real-time Monitoring

- Compute Node Service Failure
- Compute Node Service Switching
- Data Source Service Failure
- Data Source Service Switching

Compute Node Server Resource Monitoring

- Memory
- CPU Loading
- Disk Space
- CPU Usage
- Disk IO Bandwidth Usage
- Network Traffic In/Out
- CPU usage rateserver

Compute Node Service Status

- Front-End Inflow Rate
- Front-End Outflow Rate
- Back-End Inflow Rate
- Back-End Outflow Rate
- Total Back-End Connections
- Total Front-End Connections
- Heap Memory Usage
- Direct Memory Usage
- QPS

Other Server Resource Monitoring

- CPU Usage
- Memory Usage
- Disk Usage
- Network Traffic In/Out

Data Source Information Monitoring

- Data Source Password Expired
- Replication Delay
- Server Time Difference

ConfigIDB monitoring

- Shared Data Source
- Data Source Replication Status
- Unreasonable Data Source Parameters Setting
- ConfigIDB replication status
- Replication Delay

Periodical Detection Abnormal Monitoring

- Data Backup Failed
- Data Restore Failed
- Reminder of Abnormal Sharding Map Online Modification
- Inconsistent Master/Slave Data Detection Results
- Database User Password Expired
- Abnormal Global Unique Constraint
- Inconsistent and Unregular Global Table Data Detection Results
- Inconsistent Table Structure & Index Detection Results

License Authorization Monitoring

- License Authorization Expired
- Abnormal License Authorization Detection Results

Note

- Please Ensure That Monitoring item is Open in Setting. Otherwise, Alert Notification of This Monitoring Item Cannot be Prompted after Ticking Switch and Threshold Value of Monitoring Item Could be Opened in [Setting] Menu and Warning Value of Corresponding Item Could be Customized.
- Notification Frequency of All Monitoring Items Could be Set in [Setting]->Notification Setting

Save **Return**

(I) Add notification strategy parameter

- **Recipient:** Multiple recipients are separated by an English semicolon.
 - **Cc:** Optional.
 - **Monitoring Item:** The monitoring item in email reminder cannot be empty.
If the parent item in Monitoring Item is checked, the child item is automatically checked.
- **Monitoring item setting notes:**
- (1) To perform the email reminder of the corresponding item, it shall first ensure that the monitoring item has been opened in the [Setting](#). Otherwise, the email cannot prompt the alert notification of the monitoring item (the monitoring item can be opened in the “[Setting](#)” menu, and the alert value of the corresponding item can be customized).
 - (2) If the notification frequency switch of the item in the notification setting [Settings-->[Notification Setting](#)] is disabled, the email reminder will not be sent even if the current sub-item is checked. Enabling the notification setting switch is the premise of sending email.
 - (3) To add a notification strategy, you need to complete the configuration of [email sender setting](#) in advance. Otherwise, when you save the notification strategy, you will be prompted that you need to set the email sender first.
 - (4) When the above three points are met and the notification strategy is configured, if there is checked item in the parent item which is abnormal or exceeds the threshold, the email reminder will be sent according to the set notification frequency (the email reminder depends on the background related periodical task).
 - (5) The email reminder of monitoring item shall be the most recent alert condition within the monitoring frequency.

20.4.2. Description of monitoring items

(I) Failure real-time monitoring

Description: The failure status monitoring item sends an email reminder of the most recent exception detected within the notification frequency. If the failure is not repaired, the email will send repeated reminder until the failure has been repaired.



Email example: The prompt information for compute node service failure or switching is as follows:

Error real-time monitoring alert reminder

Email information:
 Compute NodeCluster name: Group_4378
 CurrentCompute Nodeinformation: ComputeNode-03(192.168.210.69/3325)
[Compute Node Failure]
 1. ComputeNode-02 (192.168.210.68 / 3325) is detected as failed at 2019-09-19 18:05:54 . Please log in to the management platform to view and repair it in time.

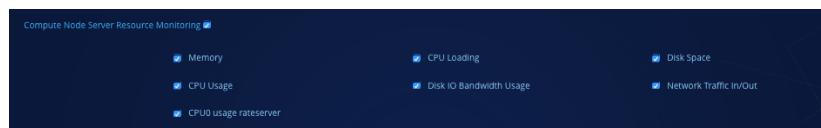
Email example: The prompt information for data source service failure or switching is as follows:

Error real-time monitoring alert reminder

Email information:
 Compute NodeCluster name: Group_4378
 CurrentCompute Nodeinformation: ComputeNode-03(192.168.210.69/3325)
[Data Source Failure]
 1. It is detected at 2019-09-19 18:05:54 that data source 192.168.210.68_3311_dn_02 (192.168.210.68 / 3311 / db01) service is marked as failed. Failure cause: (storage node service stop). Please log in to the management platform to view and repair it in time.

(II) Compute node service resource monitoring

Description: The compute node server resource monitoring item notice is about the most recent time when the threshold is exceeded during the notification time.



Threshold setting: To monitor the corresponding item of the compute node service resources, it shall be ensured that the monitoring item has been opened in “Setting -> [Monitoring Panel Setting](#)” and the corresponding thresholds have been set, as shown below:

The screenshot shows the 'Compute Node Server Resource' configuration page. On the left, a sidebar menu is open under the 'Setting' section, with 'Monitoring Panel Setting' highlighted. The main area displays various monitoring settings for server resources:

- Compute Node Traffic:** Includes Network Traffic Monitoring and Client Operating Speed.
- Compute Node Server Resource:** Includes:
 - Server Physical Memory Usage: Usage Rate >= 90 %
 - Server Disk Space Usage: Usage Rate >= 70 % and Disk Free Space < 80 G
 - Server CPU Load Condition: LOAD >= 2 (Default Threshold Value is Number of CPU Cores*0.7)
 - Server CPU Usage: Usage Rate >= 70 %
 - Server Disk IO Bandwidth Usage: Usage >= 70 %
 - Server Network Traffic In/Out: Feed Rate >= 100 MB/S Output Rate >= 100 MB/S (The Default Value Here is Gigabit Standard)
 - Server Disk Read/Write

Note: The above thresholds are the test environment settings and are for reference only.

Email example: The prompt information of real-time monitoring alert reminder of compute node server resources is as follows:

Compute Node server resource real-time monitoring alert reminder

Email information:
 Compute NodeCluster name: Group_4378
 CurrentCompute Nodeinformation: ComputeNode-03(192.168.210.69/3325)

[CPU Usage]
 1. Compute node service CPU usage reaches 11.50 % at 2019-09-19 19:57:46 , which is 10.50 % above the threshold

[Network Traffic In/Out]
 1. Compute Node Server network traffic incoming and outgoing rate reaches 25.08 KB/s at 2019-09-19 19:57:46 , which is 14.84 KB/s above the threshold
 2. Computer node server network traffic outgoing rate reaches 60.05 KB/s at 2019-09-19 19:57:46 , which is 49.81 KB/s above the threshold

[CPU Loading]
 1. Compute node service CPU load reaches 0.11 at 2019-09-19 19:55:48 , which is 0.01 above the threshold

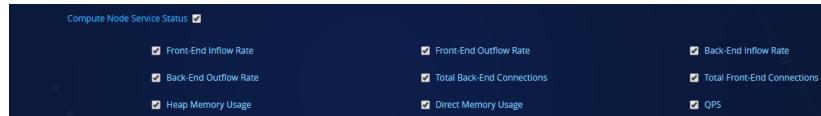
[Disk Space Usage]
 1. Compute Node service Disk: /dev/vda3 space usage rate reaches 34.40 % at 2019-09-19 19:57:46 , which is 33.40 % above the threshold, and the remaining space is less than 80.0 G
 2. Compute Node service Disk: /dev/vda1 space usage rate reaches 2.60 % at 2019-09-19 19:57:46 , which is 1.60 % above the threshold, and the remaining space is less than 80.0 G

[Disk IO Bandwidth Usage]
 1. Compute node service, disk (vda) IO bandwidth availability reaches 1.00 % at 2019-09-19 19:56:56 , which is 0.00 % above the threshold

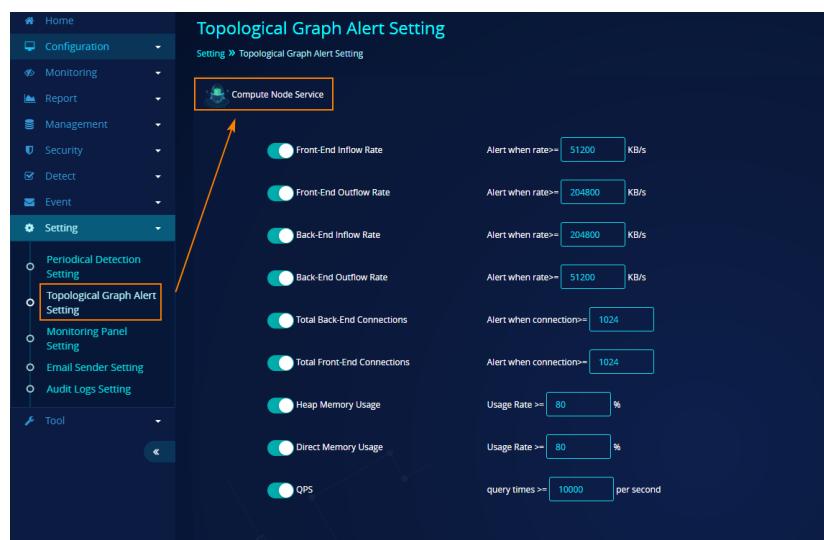
[Memory Usage]
 1. Compute node service, memory reaches 98.10 % at 2019-09-19 19:57:46 , which is 97.10 % above the threshold

(III) Compute node service status

Description: The compute node service status notice is about the most recent time when the threshold is exceeded during the notification time.



Threshold setting: To monitor the corresponding item of the compute node service status, it shall be ensured that the monitoring item has been opened in “Setting -> [Monitoring Panel Setting](#)” and the corresponding thresholds have been set, as shown below:



The screenshot shows the 'Topological Graph Alert Setting' page. On the left, a sidebar menu is open, with 'Setting' selected under 'Topological Graph Alert Setting'. The main content area displays a list of alerts for a 'Compute Node Service'. Each alert item includes a switch icon, the metric name, and a threshold value.

Metric	Alert when	Value
Front-End Inflow Rate	rate >=	51200 KB/s
Front-End Outflow Rate	rate >=	204800 KB/s
Back-End Inflow Rate	rate >=	204800 KB/s
Back-End Outflow Rate	rate >=	51200 KB/s
Total Back-End Connections	connections >=	1024
Total Front-End Connections	connections >=	1024
Heap Memory Usage	Usage Rate >=	80 %
Direct Memory Usage	Usage Rate >=	80 %
QPS	query times >=	10000 per second

Note: The above thresholds are the test environment settings and are for reference only.

Email example: The prompt information of compute node service status monitoring alert reminder is as follows:

Compute Node service status monitoring alert reminder

Email information:
 Compute NodeCluster name: Group_4378
 CurrentCompute Nodeinformation: ComputeNode-03(192.168.210.69/3325)

[Front-End Outflow Rate]

1. The ComputeNode-01 front end traffic rate in the Group_4378 group reaches 2019-09-17 17:38:28 KB/s at 45.65 , exceeding 44.65 KB/s
2. The ComputeNode-02 front end traffic rate in the Group_4378 group reaches 2019-09-17 17:38:27 KB/s at 9.04 , exceeding 8.04 KB/s
3. The ComputeNode-03 front end traffic rate in the Group_4378 group reaches 2019-09-17 17:38:18 KB/s at 19.85 , exceeding 18.85 KB/s

[Direct Memory Utilization]

1. The Group_4378 direct memory usage in the group 2019-09-17 17:38:28 reaches ComputeNode-01 % at 15.53 , exceeding 14.53 %
2. The Group_4378 direct memory usage in the group 2019-09-17 17:38:27 reaches ComputeNode-02 % at 15.43 , exceeding 14.43 %
3. The Group_4378 direct memory usage in the group 2019-09-17 17:38:18 reaches ComputeNode-03 % at 15.53 , exceeding 14.53 %

[QPS]

1. ComputeNode-01 QPS in the group Group_4378 reaches 253.00 at 2019-09-17 17:38:28 , exceeding 252.00
2. ComputeNode-03 QPS in the group Group_4378 reaches 675.00 at 2019-09-17 17:38:18 , exceeding 674.00

[Heap Memory Usage]

1. Group_4378 heap memory usage in group 2019-09-17 17:38:28 reaches ComputeNode-01 % at 15.29 , exceeding 14.29 %
2. Group_4378 heap memory usage in group 2019-09-17 17:38:27 reaches ComputeNode-02 % at 11.83 , exceeding 10.83 %
3. Group_4378 heap memory usage in group 2019-09-17 17:38:18 reaches ComputeNode-03 % at 10.60 , exceeding 9.60 %

[Total Back-End Connections]

1. The total back-end connections of ComputeNode-01 in the group Group_4378 reaches 173.00 at 2019-09-17 17:38:28 , exceeding 172.00
2. The total back-end connections of ComputeNode-02 in the group Group_4378 reaches 162.00 at 2019-09-17 17:38:27 , exceeding 161.00
3. The total back-end connections of ComputeNode-03 in the group Group_4378 reaches 174.00 at 2019-09-17 17:38:18 , exceeding 173.00

[Back-End Outflow Rate]

1. The ComputeNode-01 back end outgoing traffic rate in the Group_4378 group reaches 35.78 KB/s at 2019-09-17 17:38:28 , exceeding 34.78 KB/s
2. The ComputeNode-02 back end outgoing traffic rate in the Group_4378 group reaches 2.78 KB/s at 2019-09-17 17:38:27 , exceeding 1.78 KB/s
3. The ComputeNode-03 back end outgoing traffic rate in the Group_4378 group reaches 23.09 KB/s at 2019-09-17 17:38:18 , exceeding 22.09 KB/s

[Front-End Inflow Rate]

1. The ComputeNode-01 front-end incoming traffic rate in the Group_4378 group reaches 28.79 KB/s at 2019-09-17 17:38:28 , exceeding 27.79 KB/s
2. The ComputeNode-03 front-end incoming traffic rate in the Group_4378 group reaches 9.86 KB/s at 2019-09-17 17:38:18 , exceeding 8.86 KB/s

[Total Front-End Connections]

1. The ComputeNode-01 front-end connection in the group Group_4378 reaches 6.00 at 2019-09-17 17:38:28 , exceeding 5.00
2. The ComputeNode-03 front-end connection in the group Group_4378 reaches 10.00 at 2019-09-17 17:38:18 , exceeding 9.00

[Back-End Inflow Rate]

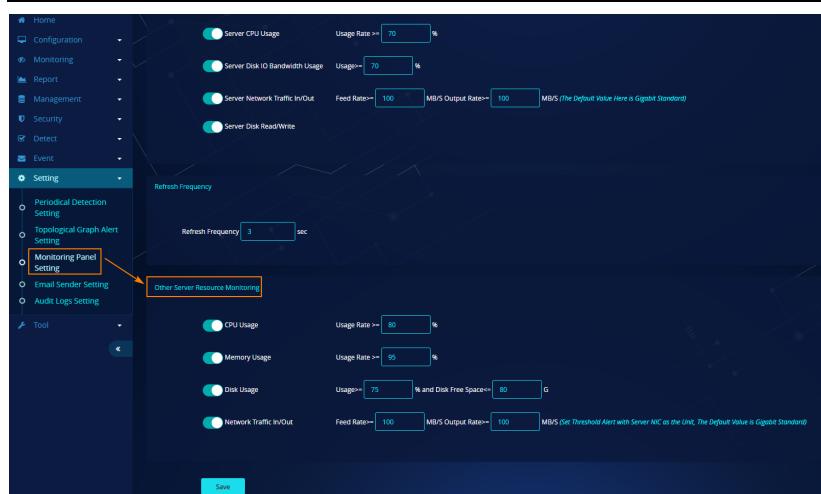
1. The ComputeNode-01 back-end inflow rate in the Group_4378 group reaches 2019-09-17 17:38:28 KB/s at 55.73 , exceeding 54.73 KB/s
2. The ComputeNode-02 back-end inflow rate in the Group_4378 group reaches 2019-09-17 17:38:27 KB/s at 6.31 , exceeding 5.31 KB/s
3. The ComputeNode-03 back-end inflow rate in the Group_4378 group reaches 2019-09-17 17:38:18 KB/s at 22.66 , exceeding 21.66 KB/s

(IV) Other server resource monitoring

Description: [Other Server Resource](#) status notification is about the most recent time when the threshold is exceeded during the notification time.



Threshold setting: To monitor the corresponding item of the compute node service resources, it shall be ensured that the monitoring item has been opened in “Setting -> [Monitoring Panel Setting](#)” and “Setting -> [Periodical Detection Setting](#)” and the corresponding thresholds have been set, as shown below:



Note: The above thresholds are the test environment settings and are for reference only..

Email example: The prompt information of other server resource monitoring exception reminder is as follows:

Other server resource monitoring anomaly reminder

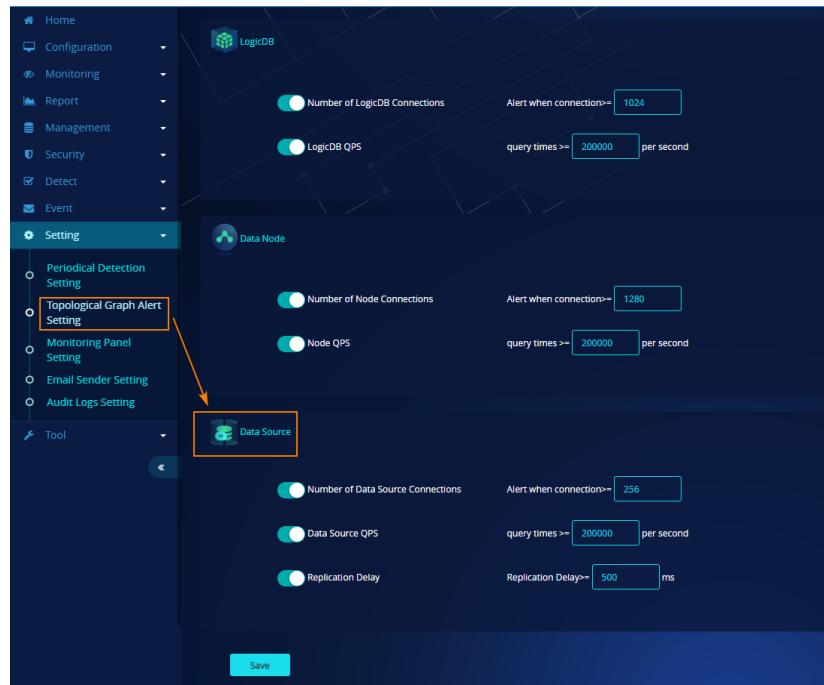
```
-----[Email information:-----  
Compute NodeCluster name: Group_4378  
CurrentCompute Nodeinformation: ComputeNode-03(192.168.210.69/3325)  
-----[Memory Usage]  
1. Server 192.168.210.69 Memory use rate at 2019-09-18 10:10:22 reaches 21.47 %, which is 20.47 % above the threshold  
-----[CPU Usage]  
1. Server 192.168.210.69 CPU use rate at 2019-09-18 10:10:22 reaches 7.12 %, which is 6.12 % above the threshold  
-----[Disk Usage]  
1. Disk / space use rate of server 192.168.210.69 reaches 30.85 % at 2019-09-18 10:10:22 which exceeds 29.85 % and the remaining disk space is less than 80.0 G  
-----[Network Traffic In/Out]  
1. Network inflow of Server 192.168.210.69 with adapter name of lo reaches 2019-09-18 10:10:22 M/S at 0.01 , exceeds 0.01 M/S  
2. Network outflow of server 192.168.210.69 with adapter name of lo reaches 0.01 M/S at 2019-09-18 10:10:22, which is 0.01 M/S above the threshold
```

(V) Data source information monitoring

Description: The data source information monitoring notification is bout the most recent exception during the notification time.



Threshold setting: To monitor the corresponding item of the data source, it shall be ensured that the monitoring item has been opened in “Setting -> Topological Graph Alert Setting” and the corresponding thresholds have been set, as shown below:



Note: The above thresholds are the test environment settings and are for reference only.

Email example: The prompt information of data source related monitoring alert reminder is as follows:

Data Source related monitoring alert reminder

```

Email information:
Compute NodeCluster name: Group_4378
CurrentCompute Nodeinformation: ComputeNode-03(192.168.210.69/3325)

[Shared Data Source]
1. Data source 192.168.210.69_3311_dn_02(192.168.210.69/3311/192.168.210.69_3311_dn_02) of data node dn_02 was used by another compute node
cluster, please log in to management platform to modify it in time

[Data Source Password Expired]
1. 5 Data source user passwords have expired or are about to expire, please log in to the management platform and timely change the password.

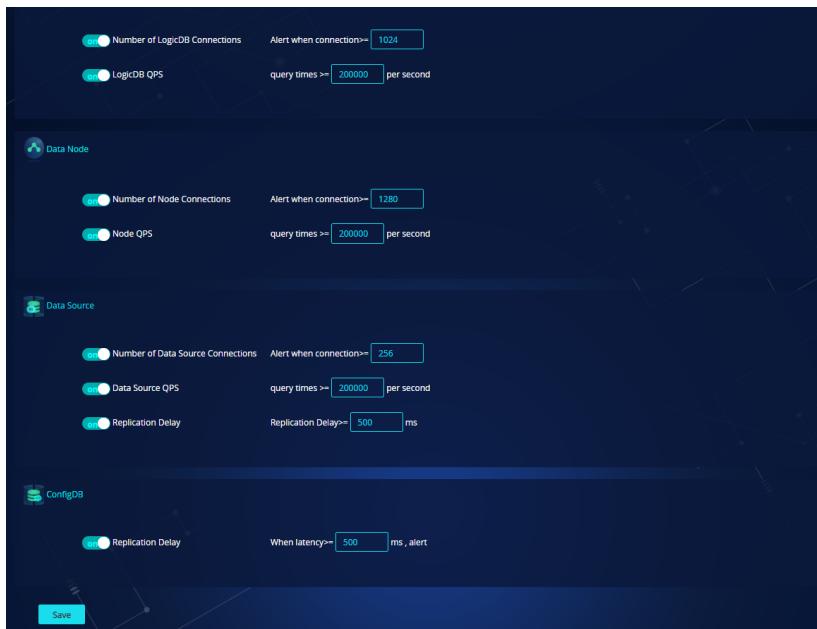
```

(VI) ConfigDB monitoring

Description: the ConfigDB monitoring notification takes the latest exception within the notification time.



Threshold setting: to monitor the corresponding items in the ConfigDB, you must first ensure that the monitoring items are opened in "Setting -> [Topological graph alert setting](#)" and the corresponding thresholds are set as follows:



Note: the above thresholds are set for the test environment and are for reference only.

Email example: ConfigDB monitoring alert reminders; the prompt information is as follows:

ConfigDB monitoring alarm

Email information:
 Compute Node Cluster name: Group_7843
 DR mode: Open
 Current master center: Master center
 Master centerCompute Node information: 计算节点-01(192.168.220.221/3325)
 DR centerCompute Node information: 计算节点-01(192.168.220.223/3325)

[Replication Delay]
 1. Replication latency between ConfigDB (192.168.220.223_3306) and ConfigDB (192.168.220.224/3306/hotdb_config) in dr center exceeds 373 seconds.
 2. Replication latency between master center ConfigDB (192.168.220.221_3306) and DR center ConfigDB (192.168.220.223/3306/hotdb_config) exceeds 373 seconds.

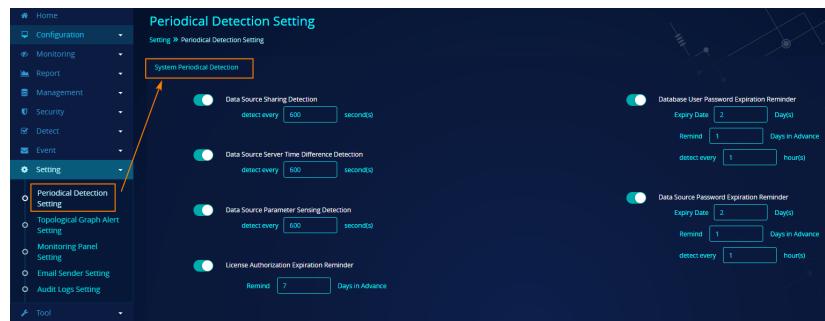
[Abnormal replication]
 1. Replication latency between ConfigDB(192.168.210.100/3306/hotdb_config) and ConfigDB(192.168.210.99/3306/hotdb_config) due to 'Error 'Table 'test2' already exists' on query. Default database: 'hotdb_config'. Query: 'create table test2 (id int primary key)' Error 'Table 'test2' already exists' on query. Default database: 'hotdb_config'. Query: 'create table test2 (id int primary key)' .

(VII) Periodical detection abnormal monitoring

Description: The periodical detection abnormal monitoring notification is bout the most recent exception (except for backup/restore failure) during the notification time.



Threshold setting: To monitor the corresponding item of the data source, it shall be ensured that the monitoring item has been opened in “Setting -> Periodical Detection Setting” and the corresponding thresholds have been set, as shown below:



Note. The above thresholds are the test environment settings and are for reference only.

periodical detection anomaly alert reminder

Email information:
 Compute NodeCluster name: Group_4378
 CurrentCompute Nodeinformation: ComputeNode-03(192.168.210.69/3325)

[Inconsistent Table Structure & Index Detection Results]

1. In the detection period (2019-09-19 15:35:22 to 2019-09-19 15:38:22), there are 2 notifications for inconsistent detection results of table structure & index detection. Please log in to the management platform for timely viewing and repair.

[Master/slave consistency]

1. In the detection period (2019-09-19 15:35:22 to 2019-09-19 15:38:22), there are 1 alerts for inconsistent detection of master/slave data. Please log in to the management platform to view and repair it in time.

Note: Backup/restore failure is alerted only if it occurs within the notification time range. This failures only includes those caused by abnormal conditions after normal backup/restore.

(VIII) License authorization monitoring

Description: When the compute node license authorization expires, if the detection switch is turned on and the reminder conditions are met, the notification email will be sent according to the set reminder frequency.



License authorization monitoring description:

- For “License Authorization Expired” and “Abnormal License Authorization Detection”, there are 3 methods of notification: page pop-up prompt; top information bar prompt (license status is displayed by default); and email reminder (receiving and sending information shall be set, otherwise no email prompt will be given).

Note: The pop-up prompt and top information bar prompt are not affected by the email settings.

- License Authorization Expired means that the current license has a certain period of validity. After checking this item, the system will send email reminder of license authorization expiration according to the license authorization monitoring setting status in [Notice Setting](#), the notification frequency in [Periodical Detection Setting](#), and the setting of advance notification days.

Email example: The license authorization expiration email reminder is as follows:

License authorization expiration reminder

Email information:
Compute NodeCluster name: Group_4378

[License authorization expiration]

CurrentCompute Nodeinformation: ComputeNode-03(192.168.210.69/3325)
The license authorization will expire after 80 Days. In order to avoid failure to use after expiration, please contact the administrator to update the authorization.,

CurrentCompute Nodeinformation: ComputeNode-01(192.168.210.67/3325)
The license authorization will expire after 80 Days. In order to avoid failure to use after expiration, please contact the administrator to update the authorization.,

CurrentCompute Nodeinformation: ComputeNode-02(192.168.210.68/3325)
The license authorization will expire after 87 Days. In order to avoid failure to use after expiration, please contact the administrator to update the authorization.,

- If the current license validity is permanent, the “License Authorization Expired” check box will be automatically hidden.



- If the current license is an expired license, the HotDB Server will stop serving.

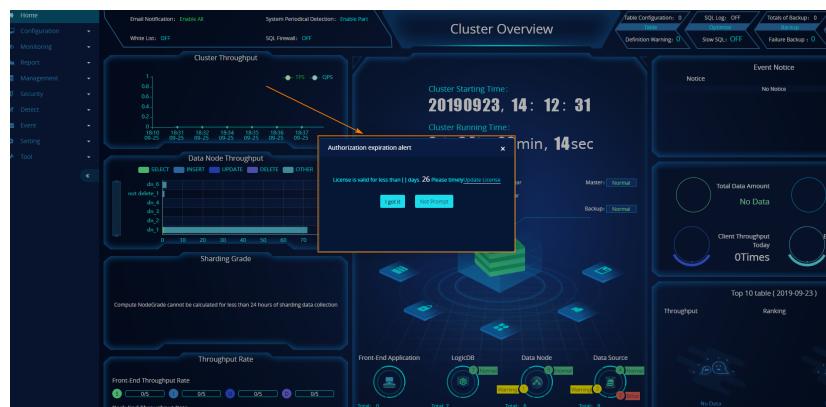


Click the [I got it] button to retract the pop-up window. Refresh the current page to

activate the pop-up window again.

- License authorization detection exception includes “exception occurred to obtain license authorization information” and “license authorization information cannot be updated” (when “exception occurs to obtain license authorization information” and “license authorization information cannot be updated” exist at the same time, “exception occurs to obtain license authorization information” pop-up window will be displayed first).

The license authorization expiration reminder pop-up prompt is as follows:



The pop-up prompt for exception occurred to obtain license authorization information is as follows:



Operation instructions:

Click the [×] button in the upper right corner to retract the pop-up window, and log in again or refresh the page to re-activate the pop-up window;

Click the [I got it] button to retract the pop-up window, and log in again or refresh the page to re-activate the pop-up window;

Click the [Not Prompt] button to retract the pop-up window, and the pop-up window will not be re-activated when logging in again or refreshing the page.

Email example: The email prompt for “License authorization information cannot be updated” is as follows:

Abnormal license authorization detection

Email information:
Compute NodeCluster name: HotDB-78
[Abnormal license authorization detection]
CurrentCompute Nodeinformation: HotDB_78(192.168.210.78/3325)
The license authorization information of current Compute Node cannot be updated normally, which however will not affect currently running services, and it is recommended that the Compute Node service should be restarted in due time at non-rush hour of business to obtain latest authorization information

20.5. Audit logs

The Audit Logs function is mainly used to view the operation records of HotDB Management users on the platform, as well as the security protection interception records of compute nodes in the cluster and the operations at the management port (3325 by default). This function is only supported on compute node V2.5.0 or above.

20.5.1. Platform operation

It can be used to view the operations of all general users in the cluster on the management platform. The specific types of operations recorded can be viewed in the operation type drop-down box on the page. Access IP and operation content input boxes support fuzzy search.

Platform Operation						
Event: Audit Log - Platform Operation						
Time Range		2019-10-18 00:00:00	to	2019-10-20 14:27:52		
Access IP				Please Select Operation Type		
Operation type				<input checked="" type="radio"/> Logout	<input type="radio"/> Success	<input type="radio"/> Failure
Operation Name				<input type="text"/>		
Operation Content				<input type="text"/>		
Username	Access IP	Operation Type	Operation Content	Input Parameter	Operation Time	Operation Result
ry	192.168.200.136	Basic Management	Master Slave Monitoring Experiments Monitoring switching of node_03	{"hostGroup": "4", "node": "174.252.50.99:4400:4C2D8B6F0B EXECACT"}	2019-10-20 15:20:26	Success
ry	192.168.210.43	Sharding Route Modification	Single Modification Task	{"passTime": "1", "hostGroup": "4", "task": "test", "interval": "1", "base": "174.252.50.99:4400:4C2D8B6F0B:7164:1", "table": "T1M", "x": "1", "y": "1", "z": "1", "start": "1", "end": "1", "step": "1", "batchSize": "1000", "l": "1", "op": "P", "t": "1"}	2019-10-20 15:25:17	Success
admin	192.168.200.134	Sharding Rule Detection	Start detection: pm	{"hostGroup": "4", "table": "T1M", "rule": "1", "start": "1", "end": "1", "step": "1", "batchSize": "1000", "l": "1", "op": "P", "t": "1"}	2019-10-20 16:13:38	Success
admin	192.168.200.134	Sharding Route Detection	Start detection: pm	{"hostGroup": "4", "table": "T1M", "rule": "1", "start": "1", "end": "1", "step": "1", "batchSize": "1000", "l": "1", "op": "P", "t": "1"}	2019-10-20 16:09:01	Success
admin	192.168.200.134	Sharding Rule Detection	Start detection: test	{"hostGroup": "4", "table": "T1M", "rule": "1", "start": "1", "end": "1", "step": "1", "batchSize": "1000", "l": "1", "op": "P", "t": "1"}	2019-10-20 14:48:54	Success
admin	192.168.200.134	Sharding Rule Detection	Start detection: test	{"hostGroup": "4", "table": "T1M", "rule": "1", "start": "1", "end": "1", "step": "1", "batchSize": "1000", "l": "1", "op": "P", "t": "1"}	2019-10-20 14:08:47	Success

List information description:

- Username: The account used to log in to the management platform.
 - Access IP: IP address for logging on to the management platform. It supports fuzzy query.
 - Operation Type: All supported types are displayed in the drop-down box. When checking the checkbox, only logs of the selected operation type are displayed.
 - Operation Content: It records the user's actual operation and important parameters. It supports fuzzy query.
 - Input Parameter: A more detailed user operation log for easy analysis of user operations.
 - Operation Time: It records the actual operation time and supports selecting the time range to display the log record. The time range of record is determined by the

default number of days of retention in the settings.

- Operation Result: It records the actual operation result. Log records can be filtered based on the operation results.

20.5.2. Security protection

It can be used to view the operation logs related to security protection performed by all ordinary users. The specific types of operations are recorded. You can view them in the operation type drop-down box on the page. Access IP and interception details input box support fuzzy search.

Safety Protection							
Event > Audit Log > Safety Protection							
Compute Node	Username	Access IP	Intercept Type	Intercept Details	Occurrence Time	Intercept Result	Intercept Remark
HotDB_78	zy	192.168.200.126	Error message login service port	mysql-zy-P3323->192.168.200.126	2019-09-25 16:19:10	Success	
HotDB_78	zy	192.168.200.126	Error message login service port	mysql-zy-P3323->192.168.200.126	2019-09-25 16:19:03	Success	
HotDB_78	zy	192.168.200.126	Error message login service port	mysql-zy-P3323->192.168.200.126	2019-09-25 16:19:53	Success	
HotDB_78	test	192.168.210.32	Error message login service port	mysql-utest-P3323->192.168.210.32	2019-09-24 16:07:09	Success	
HotDB_78	test	192.168.210.32	Error message login service port	mysql-utest-P3323->192.168.210.32	2019-09-24 16:07:04	Success	
HotDB_78	huichuang	192.168.210.32	Error message login service port	mysql-unichuang-P3323->192.168.210.32	2019-09-24 16:06:42	Success	
HotDB_78	huichuang	192.168.210.32	Error message login service port	mysql-unichuang-P3323->192.168.210.32	2019-09-24 16:06:34	Success	
HotDB_78	xx	192.168.210.32	Error message login service port	mysql-xx-P3323->192.168.210.32	2019-09-24 16:06:42	Success	

List information description:

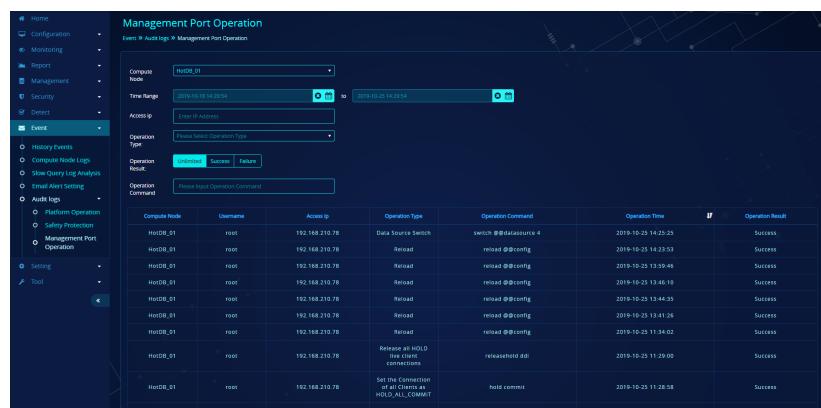
- Compute Node: It records the compute node to which it belongs.
- Username: The account used to perform the operation.
- Access IP: IP used for executing the operation. It supports fuzzy query.
- Intercept Type: All supported types are displayed in the drop-down box. When checking the checkbox, only logs of the selected operation type are displayed.
- Interception Details: It records the command executed and supports fuzzy query.
- Occurrence Time: It records the actual operation time and supports selecting the

time range to display the log record. The time range of record is determined by the default number of days of retention in the settings.

- Operation Result: It records the actual operation result. Log records can be filtered based on the operation results.

20.5.3. Management port operation

It can be used to view the operations of all general users on the management port. The specific types of operations recorded can be viewed in the operation type drop-down box on the page. Access IP and interception details input box support fuzzy search. If a compute node group is selected, only the operation records for the selected compute node group are displayed. A specific compute node can be selected, and all compute nodes are selected by default.



Compute Node	Username	Access IP	Operation Type	Operation Command	Operation Time	Operation Result
HotDB_01	root	192.168.210.78	Data Source Switch	switch @@datasource 4	2019-10-25 14:25:29	Success
HotDB_01	root	192.168.210.78	Reload	reload @@config	2019-10-25 14:23:53	Success
HotDB_01	root	192.168.210.78	Reload	reload @@config	2019-10-25 13:59:46	Success
HotDB_01	root	192.168.210.78	Reload	reload @@config	2019-10-25 13:46:19	Success
HotDB_01	root	192.168.210.78	Reload	reload @@config	2019-10-25 13:44:39	Success
HotDB_01	root	192.168.210.78	Reload	reload @@config	2019-10-25 13:41:28	Success
HotDB_01	root	192.168.210.78	Reload	reload @@config	2019-10-25 11:34:02	Success
HotDB_01	root	192.168.210.78	Release all HOLD connections	releasehold.dll	2019-10-25 11:29:09	Success
HotDB_01	root	192.168.210.78	Set the Connection Isolation Level & HOLD_ALL_COMMIT	hold commit	2019-10-25 11:28:58	Success

List information description:

- Compute node: The compute node to which the record belongs.
- User: The account used for logging onto the management port.
- Access IP: The IP used for logging onto the management port.
- Operation Type: All supported types are displayed in the drop-down box. When checking the checkbox, only logs of the selected operation type are displayed.

- Operation Command: The command actually executed on the management port.
- Operation Time: It records the actual operation time and supports selecting the time range to display the log record. The time range of record is determined by the default number of days of retention in the settings.
- Operation Result: It records the actual operation result. Log records can be filtered based on the operation results.

20.5.4. Audit log setting

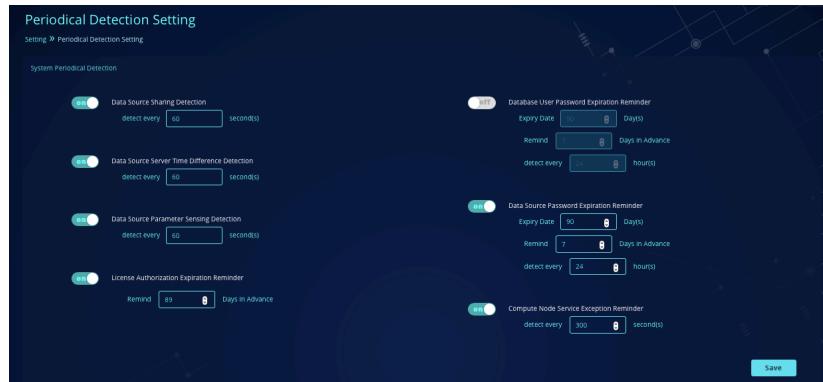
The audit object of audit log can be configured in “Setting -> [Audit Log Setting](#)”, and all existing monitoring objects are audited by default.

21. Setting

21.1. Periodical detection setting

21.1.1. Periodical detection setting

Description: The periodical detection setting is the function provided by HotDB Management for switch and related parameter setting of background execution periodical detection thread.



- Turn on the button (the button dot is turned to the right) to enable the background periodical detection thread, and turn off the button to stop operation.
- After turning on the switch, the specific detection frequency or abnormal detection reminder time can be set.
- If the periodical detection task is closed, the email alert in “Event -> [Notification Strategy](#)” may be affected.

21.1.2. Periodical plan

Description: It provides the entry for setting the periodical plan window. The effect after setting is the same as the periodical plan entry in the original function. The following are available currently: Config data periodical backup plan, global table data periodical detection plan, master/slave data consistency periodical detection plan, table

structure and table index periodical detection plan, data sharding route periodical detection plan, data unique constraint periodical detection plan. For the specific setting method, refer to the [Periodical Plan](#) description in “Detection -> Master/Slave Data Consistency Detection”.

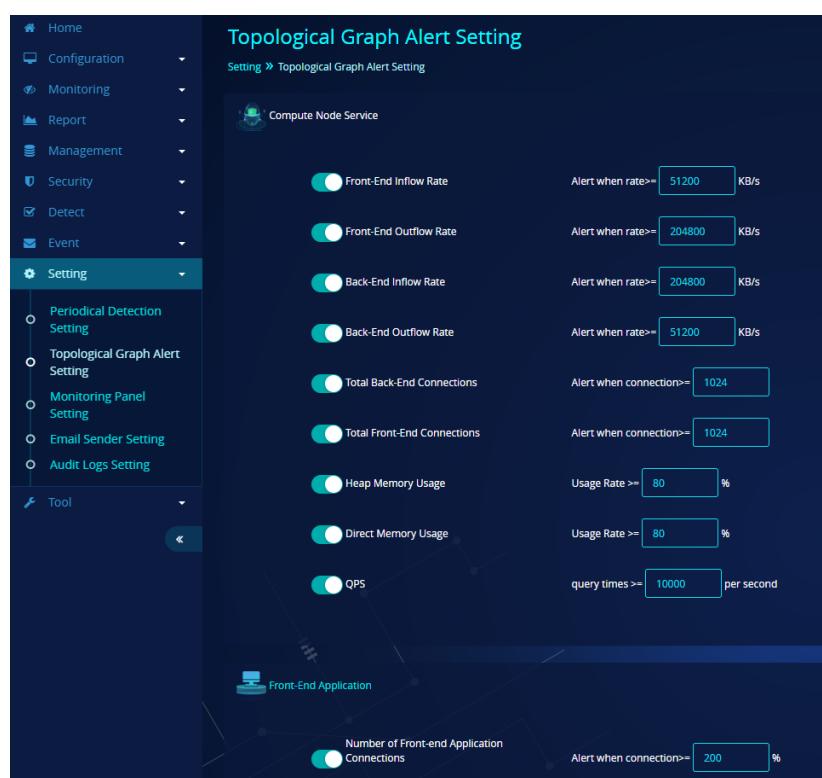


The screenshot displays the HotDB Management Platform interface under the 'Setting' section. It shows four configuration panels:

- Config Data Periodical Backup Plan:** A table with columns: Backup Metadata, Backup Period, Backup Time, Backup to Remote, and Operation. It lists three configurations: Config01 (Weekly, Mon. 02:30, No), Config02 (Weekly, Wed. 02:30, No), and Config03 (Weekly, Sat. 02:30, No).
- Global Table Periodical Detection Plan:** A table with columns: Detection Period, Detection Time, LogicDB Selection, Global Table, Detection Concurrency, and Operation.
- Master Slave Data Consistency Periodical Detection Plan:** A table with columns: Detection Range, Detection Period, Detection Time, Detection Object, Data Source, Concurrency, and Operation.
- Table Structure and Table Index Periodical Detection Plan:** A table with columns: Detection Period, Detection Time, and Operation. It lists two entries: Daily (03:00) and Daily (13:00).

21.2. Topological graph alert setting

Description: It can set the threshold for alerts for monitoring items at each layer in “Monitoring -> [Logic Topological Graph](#)”. When the threshold is exceeded, the topological graph displays the corresponding warning information. You can restore the default setting by clicking the Reset button.



The screenshot displays the "Topological Graph Alert Setting" page under the "Setting" section of the management platform. It lists several monitoring items with their respective alert thresholds:

- Compute Node Service:**
 - Front-End Inflow Rate: Alert when rate >= 51200 KB/s
 - Front-End Outflow Rate: Alert when rate >= 204800 KB/s
 - Back-End Inflow Rate: Alert when rate >= 204800 KB/s
 - Back-End Outflow Rate: Alert when rate >= 51200 KB/s
 - Total Back-End Connections: Alert when connection >= 1024
 - Total Front-End Connections: Alert when connection >= 1024
 - Heap Memory Usage: Usage Rate >= 80 %
 - Direct Memory Usage: Usage Rate >= 80 %
 - QPS: query times >= 10000 per second
- Front-End Application:**
 - Number of Front-end Application Connections: Alert when connection >= 200 %

21.3. Monitoring panel setting

It is used to enable or disable the monitoring items of “Compute Node Service Status”, “Compute Node Traffic”, “Compute Node Server Resource” and “Other Server Resources” panels in “Monitoring->[Monitoring Panel](#)”. the data refresh frequency and the server parameter status threshold can also be set.

Monitoring Panel Setting

Setting > Monitoring Panel Setting

Compute Node Service Status

- Total Number of Client Connections
- Real-time Data Amount
- Back-end Connection Status
- Direct Memory Usage
- Thread Usage
- Heap Memory Usage

Compute Node Traffic

- Network Traffic Monitoring
- Back-end Operating Speed
- Client Operating Speed

Compute Node Server Resource

- Server Physical Memory Usage Usage Rate >= 90 %
- Server Disk Space Usage Usage Rate >= 70 % and Disk Free Space <= 80 G
- Server CPU Load Condition LOAD >= 2 (Default Threshold Value is Number of CPU Cores*0.7)
- Server CPU Usage Usage Rate >= 70 %
- Server Disk IO Bandwidth Usage Usage >= 70 %
- Server Network Traffic In/Out Feed Rate >= 100 MB/S Output Rate >= 100 MB/S (The Default Value Here is Gigabit Standard)
- Server Disk Read/Write

Refresh Frequency

Refresh Frequency 3 sec

Other Server Resource Monitoring

- CPU Usage Usage Rate >= 80 %
- Memory Usage Usage Rate >= 95 %
- Disk Usage Usage >= 75 % and Disk Free Space <= 80 G
- Network Traffic In/Out Feed Rate >= 100 MB/S Output Rate >= 100 MB/S (Set Threshold Alert with Server NIC as the Unit, The Default Value is Gigabit Standard)

Monitoring Panel Setting

Setting > Monitoring Panel Setting

Compute Node Service Status

- Total Number of Client Connections
- Direct Memory Usage
- Real-time Data Amount
- Thread Usage
- Back-end Connection Status
- Heap Memory Usage

Compute Node Traffic

- Network Traffic Monitoring
- Client Operating Speed
- Back-end Operating Speed

Compute Node Server Resource

<input checked="" type="checkbox"/> Server Physical Memory Usage	Usage Rate >= <input type="text" value="1"/> %
<input checked="" type="checkbox"/> Server Disk Space Usage	Usage Rate >= <input type="text" value="1"/> % and Disk Free Space<= <input type="text" value="80"/> G
<input checked="" type="checkbox"/> Server CPU Load Condition	LOAD<= <input type="text" value="0.1"/> (Default Threshold Value is Number of CPU Cores*0.7)
<input checked="" type="checkbox"/> Server CPU Usage	Usage Rate >= <input type="text" value="1"/> %
<input checked="" type="checkbox"/> Server CPU0 Usage	Usage Rate >= <input type="text" value="1"/> %

Server Disk I/O Bandwidth Usage

- Usage >= %

Server Network Traffic In/Out

- Feed Rate >= MB/S Output Rate >= MB/S (The Default Value here is Gigabit Standard)

Server Disk Read/Write

Refresh Frequency

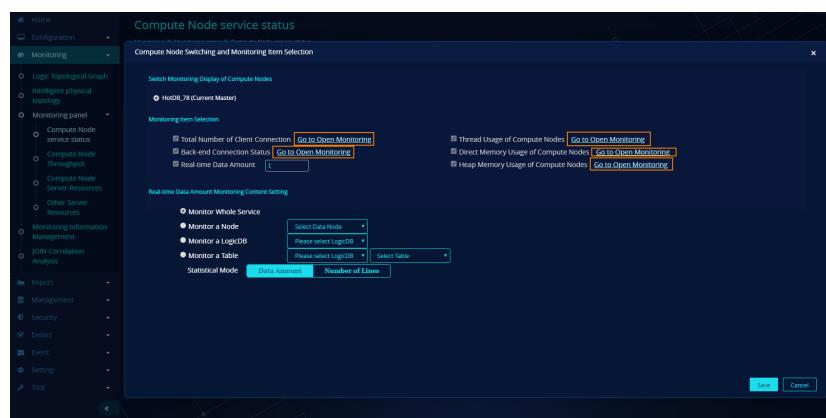
Refresh Frequency sec

Other Server Resource Monitoring

<input checked="" type="checkbox"/> CPU Usage	Usage Rate >= <input type="text" value="1"/> %
<input checked="" type="checkbox"/> Memory Usage	Usage Rate >= <input type="text" value="1"/> %
<input checked="" type="checkbox"/> Disk Usage	Usage <= <input type="text" value="1"/> % and Disk Free Space <= <input type="text" value="80"/> G
<input checked="" type="checkbox"/> Network Traffic In/Out	Feed Rate >= <input type="text" value="100"/> MB/S Output Rate >= <input type="text" value="100"/> MB/S (Set Threshold Alert with Server NIC as the Unit; The Default Value is Gigabit Standard)

Save

- Choose whether to enable each monitoring item.
- It allows to set the refresh frequency.
- When the button is turned off, the monitor panel needs to be opened for monitoring.

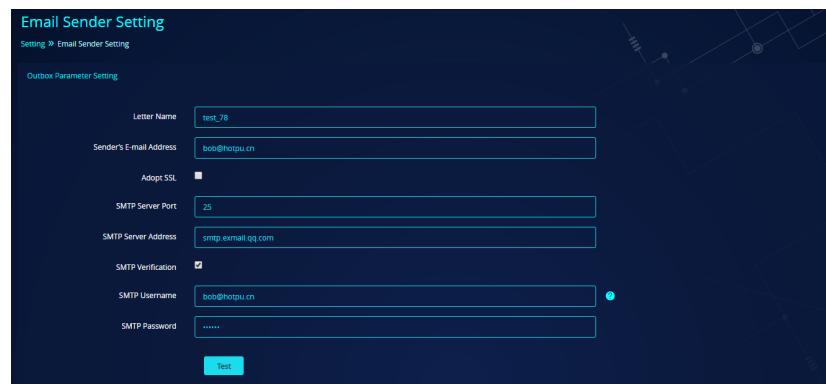


21.4. Notification setting

It sets the email sender parameter of email alert function in “Event->[Notification Strategy](#)” and the monitoring switch and frequency of monitoring item.

21.4.1. Email sender setting

In the email sender setting, enter the correct email sender parameter information for connection test, as shown below:



Email sender parameter description

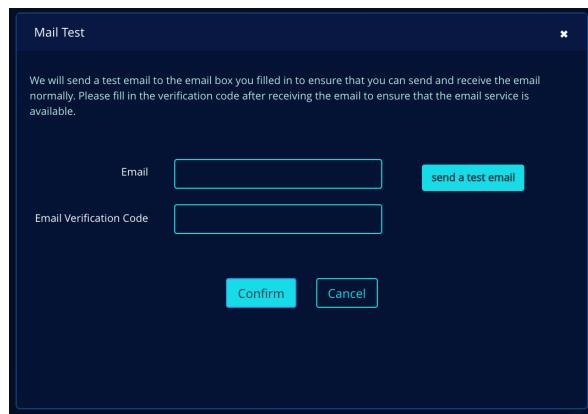
- **Letter Name:** The sender's remark information
- **Sender's E-mail Address:** Full e-mail address of the letter

- **SMTP Server Port:** SSL check box is used. If checked, the SMTP server port is 465 by default. If unchecked, the SMTP server port is 25 by default. The SMTP server port can also be edited.
- **SMTP Server Address:** The address of the email server, generally in the form of SMTP ([465/25 port](#)). Example of server address: smtp.exmail.qq.com
- **SMTP Verification:** It is checked by default. If checked, -> SMTP username and SMTP password must be checked; if not checked, -> SMTP username and SMTP password input box shall be empty and gray and cannot be edited (when using the intranet mailbox server to set the email password-free form, SMTP verification can be unchecked)
- **SMTP Username:** It is generally the left part of the sender's email address@, and some mailbox manufacturers require to complete email address
- **Password:** SMTP username password used to verify SMTP server user availability

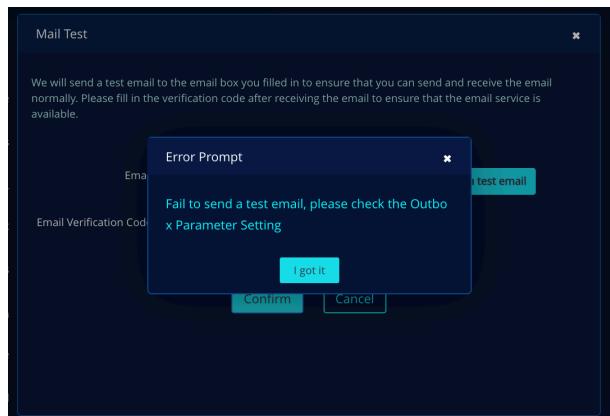
After inputting the correct parameters, click Test to verify whether the current email sender channel is successfully connected. If the verification fails, the page will return to the error cause and the error will be positioned.

Mail test

- Enter the correct parameters and click Test to pop up the mail test window, as shown below:



- **Email:** Enter the inbox address (in case of intranet, the corresponding inbox address needs to be filled in), click the “Send a test email” button to check the email sender parameter settings and inbox parameters, the inbox parameters are filled in. When the error occurs, the window prompts. “Test mail sending failed” is prompted when the email sender parameter is set incorrectly. “Email is sent successfully, please check it” when the email sender parameter is set correctly (the “Send a test email” button is gray and email cannot be sent again within 1 minute after successful sending). If the email sender parameter is set incorrectly, the pop-up window displays an error message, as shown below.



- Mail Test content is as shown below:

Hi:

HotDB is sending a test email now.

Verification code:**2762e7**,Please enter verification code in time. Ignore this email unless it is operated by you (this verification code is valid within 30 minutes, you need to re-generate it if time is out)

- **Mailbox Verification Code:** Correctly fill in the received email verification code and click the Confirm button, “Verification successful” is prompted. If the email verification code is filled in incorrectly, “Verification code error” is prompted (the verification code is not case sensitive, but please pay attention to whether there is any space)

21.4.2. Notification frequency setting

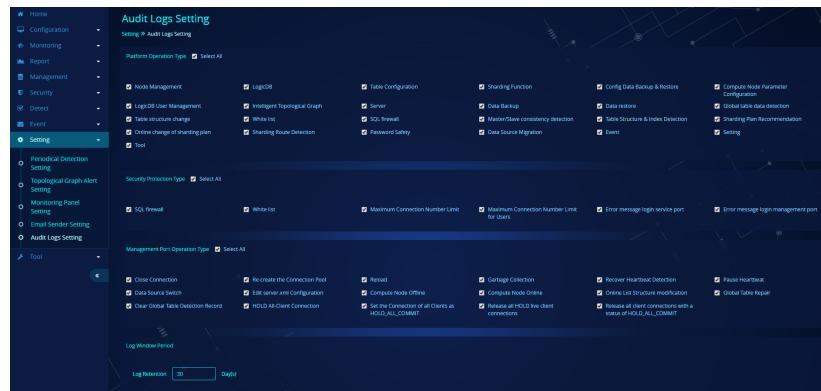
The monitoring notification frequency controls the email sending interval (also can be understood as the monitoring detection frequency) of monitoring items in the email alert, as shown below:

Monitoring Item	Notification Interval
Failure Real-time Monitoring	Notices are given every 5 minute(s)
Compute Node Server Resource Monitoring	Notices are given every 5 minute(s)
Compute Node Service Status	Notices are given every 60 minute(s)
Other Server Resource Monitoring	Notices are given every 60 minute(s)
Data Source Information Monitoring	Notices are given every 60 minute(s)
Periodical Detection Abnormal Monitoring	Notices are given every 60 minute(s)
License Authorization Monitoring	Notices are given every 24 hours

Closing the corresponding monitoring item may affect the email alert in “Event->[Notification Strategy](#)” . When closing, check whether there is a notification strategy added and whether a sub-item of the monitoring item is checked.

21.5. Audit logs setting

The operation function menu of audit log records and the audit log record retention time can be set in “Event -> [Audit Logs](#)”.

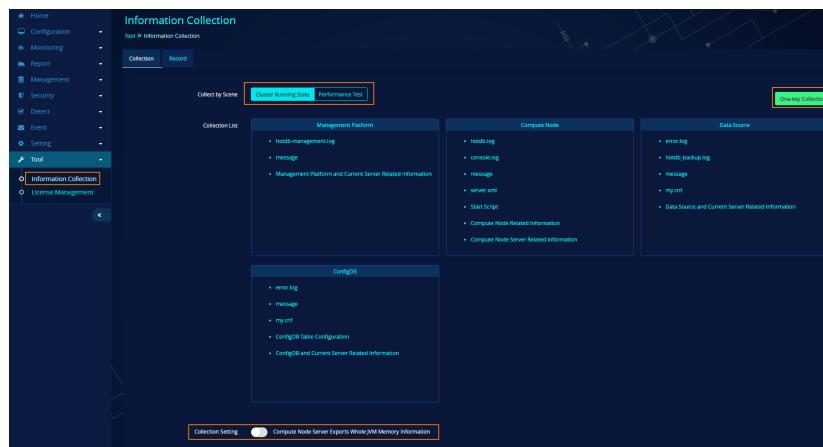


22. Tool

22.1. Data collection

There are many HotDB Server cluster components, and the operation mechanism is complicated. Troubleshooting is difficult when an exception or malfunction occurs. The data collection tool can be used to quickly collect the logs and configuration files required for exception analysis when the user has a cluster problem, thereby improving the impact of the problem-solving speed reduction on the business.

Function Entry: Click “Tools -> Data Collection” in the management platform to enter the “Data Collection” page.



Collection scenario:

According to the collection scenario, data collection is divided into two types: cluster running status and performance test.

- **Cluster Running Status:** Generally, it is used for data collection when faults, exceptions and running problems occur in the cluster running process. The data collected in this scenario includes the running logs, configuration files and server status of running components of the entire cluster.

- **Performance Test:** Generally, it is used when performance test results need to be analyzed or performance test bottlenecks need to be identified after the performance test of HotDB Server. The data collected in this scenario is mainly about compute nodes, data sources, configDB, and server related information.

Collection list:

The collection list contain files that need to be packed in one-key collection of data. The collection lists of different cluster modes are also different. For example, when the compute node is in the master/slave mode, the collection list will add keepalived component related data; when the compute node is in the multi-node load balancing mode, the collection list will add LVS component related data, and the page display list shall prevail.

Note: When collecting data in the “Cluster Running Status” scenario, if the configDB or data source instance version is MySQL8.0 or above, the mysqld_auto.cnf file will be collected according to the actual situation. This file is not displayed in the page list, and is only collected according to the actual situation after judging the version.

Function description:

Data collection shall focus on the following steps and issues.

1. Select the scenario according to the actual collection needs.
2. Select whether to turn on the collection setting according to the actual situation.

The compute node server exports the entire JVM memory data: This switch needs to be noted when collecting data in the “Cluster Running Status” scenario and is OFF on the page by default. If it is ON, it needs to consider the possible full GC problem. It is not recommended to turn on the switch in the production environment. If it is ON, the task will execute jmap -dump:live,format=b,file=dump.bin [pid] 2>&1 when collecting compute node related data. Note: pid is the compute node process ID

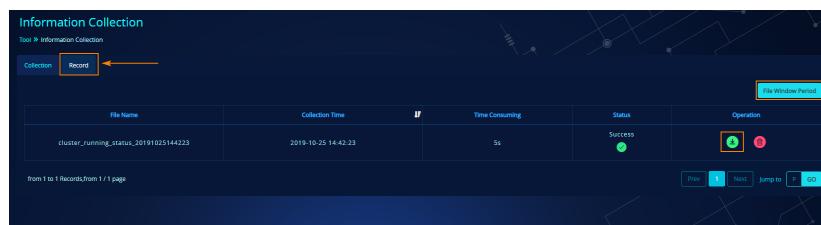
Allow to use smartctl and MegaCli commands to collect server-related data: This switch needs to be noted when collecting data in the “Performance Test” scenario and is ON on the page by default. If the corresponding components are not installed on the server when executing smartctl and MegaCli commands, the program will automatically install the corresponding commands through the yum mode.

3. Click the “One-key collection” button

Precautions for starting a collection task:

1. There shall be no other compute node groups performing data collection tasks on the current management platform, otherwise the collection task fails. “One-key Collection” can be performed normally only after the completion of other tasks.
2. The compute node cluster that starts a task needs to configure the available SSH data for all servers on the “Configuration -> Server” menu page. Otherwise, some server data may not be collected due to SSH connection failure during the collection process.
3. Ensure the normal running of compute node service as far as possible. If the task started detects that the compute node cannot run normally, the user needs to manually specify the location of the compute node log.

4. Pay attention to the task execution on the “Tool” -> “Data Collection” -> “Record” page.
5. The collected tasks will automatically download the collected data to the management platform in the form of a compressed package. The user can also re-download the previously started task collection file later on the management platform record page.
6. The files collected by the task are stored in the /opt directory of the management platform server by default. If the files in the directory are deleted manually, the corresponding “Download” button on the page is gray and the files cannot be downloaded.
7. For the collected files stored on the management platform server, the management platform provides a 30-day retention period by default. For files that are not in the file window period, the program performs the deletion task every morning and in the retention period.



8. When deleting the page record, the program will also delete the file content in the /opt directory of the management platform server.

9. Open the compressed packet of collected files, and summarize and divide data mainly according to the cluster component type. Open folders of each component type and summarize data by the server IP or the server IP+ identification port.

10. For the data cannot be collected or abnormal data collected, the “Task Collection Abnormal Report.txt” record is uniformly used in the compressed packet.



22.2. License management

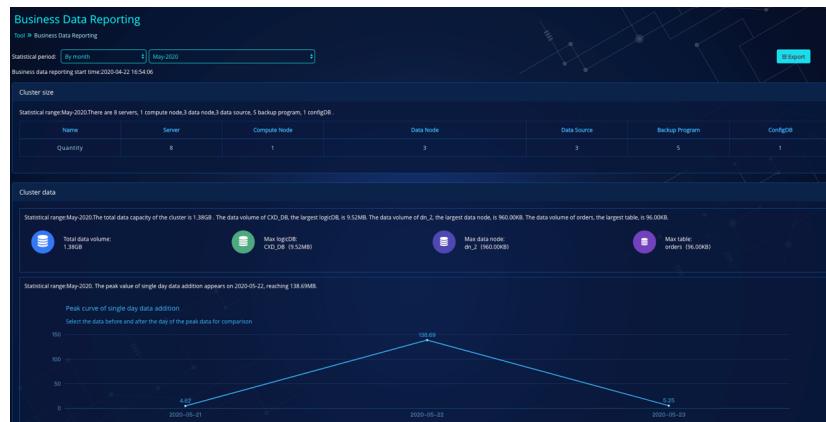
This function is the same as the “[License Management](#)” function in admin. For details, please refer to the relevant chapter.

22.3. Business data reporting

Business data reporting provides annual reports of the cluster for users, which support the statistics of the business data of the cluster and support users to have a knowledge of the actual benefits from the cluster to the enterprise and the defects of the cluster

operation.

Function entry: enter the Business data reporting page through "Tool" -> "Business data reporting" on the management platform, as shown in the following figure:

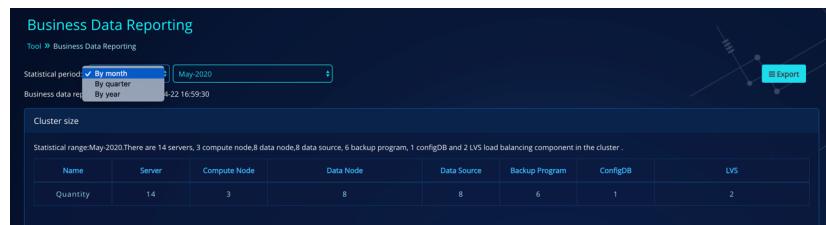


Each time entering the page, the business data will be automatically obtained. "By month" is selected by default and the business data of the "current month" will be displayed. The statistical cycle can be selected as "By month", "By quarter", and "By year".

By month: the selection range is from the month of the start time to the current month, format: "year + month".

By quarter: the selection range is from the quarter of the starting time to the current quarter, format: "year + quarter".

By year: the selection range is from the year of the start time to the current year, format: "year + year".



When you reselect the time range for business data statistics, the page will automatically refresh the matching data. Click Export to export the data report, format: PDF/WORD.

The exported file name is: cluster name + business data report + time range (i.e. the selected time range)

Business Data Reporting

Tool: Business Data Reporting

Statistical period: By year | The first half of -2020

Business data reporting start time:2020-04-22 16:54:06

Cluster scale

Statistical range:The first half of -2020.There are 8 servers, 1 compute node,3 data node,3 data source, 5 backup program,1 configDB.

Name	Server	Compute Node	Data Node	Data Source	Backup Program	ConfigDB
Quantity	8	1	3	3	5	1

Export Options: CSV, PDF, WORD

(1) Cluster scale

The Cluster scale shows the number of servers and components in the cluster, which is displayed in combination of graphics and text. The text shows the specific statistics of the name and number of current components in the selected time range (displayed according to the selection drop-down box).

Server: the number of servers in the current compute node cluster. The data is obtained through “configuration -> server”.

Compute node: the total number of compute nodes in the current compute node cluster.

Data node: the total number of data nodes in the current compute node cluster.

Data source: the total number of data sources in the current compute node cluster.

Backup program: number of backup programs on the data source server which are in the startup state.

ConfigDB: number of ConfigDBs of the current compute node.

LVS: number of LVS servers in cluster mode

The data of cluster scale is updated regularly in the early hours of each day, as shown in the following figure:

Cluster scale

Statistical range:Jun-2020 There are: 4 servers, 2 compute node, 2 data node, 2 data source, 1 backup program, 2 configDB

Name	Server	Compute Node	Data Node	Data Source	Backup Program	ConfigDB
Quantity	4	2	2	2	1	2

Note: when the system is in initial status and has not carried out data statistics, the number of all components will be displayed with "-".

(2) Cluster data

Cluster data consists of four parts: cluster data volume, peak curve of single day data addition, data capacity planning prediction and data operation. Each part is displayed in combination of graphics and text.

➤ Cluster data volume

Total data volume: the total data volume of tables of all data nodes in the current compute node cluster.

Max LogicDB: the LogicDB with the largest amount of data in the current compute node cluster.

Max data node: the data node with the largest amount of data in the current compute node cluster.

Max table: the table with the largest amount of data in the current compute node cluster.

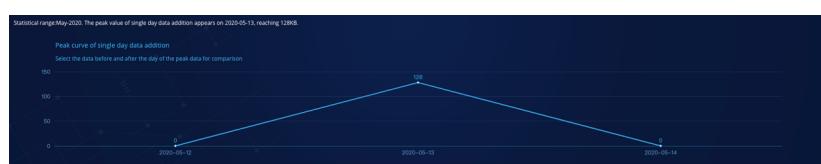
The data is updated regularly at zero every day for statistics and display, including the total data volume of the cluster, max LogicDB and its data volume, max data node and its data volume, max table and its data volume, as shown in the following figure:



Note: when the system is in initial status and has not carried out data statistics, the number of all components will be displayed with "-".

➤ Peak curve of single day data addition

The data is regularly updated at 0:00 every day, and the date with the largest peak amount of single day data addition within the statistical range, the corresponding data amount and the data of the day before and after will be displayed. If there is no corresponding data in the day before and after, the closest date and data will be selected for display, as shown in the following figure:



If there are multiple time points with the same peak value in the selected time range, the data closest to the selecting time will be displayed.

Note: when the system is in initial status and has not carried out data statistics, the page displays no data temporarily.

➤ Data capacity planning prediction

The data capacity planning prediction includes growth prediction of the cluster data volume in the next year, growth prediction of the compute node ConfigDB in the next year and growth prediction of management platform ConfigDB in the next year. The default time range displayed is one year from the current time, regardless of the specific time range selected by the user.

The data is regularly updated at 0:00 every day. The cluster data volume, compute node ConfigDB data volume and management platform ConfigDB data volume are counted respectively. If the statistical data in the current increment prediction is less than 21 days, "The data recorded currently is less than 21 days, so the increment prediction is temporarily unavailable." will be prompted, as shown in the following figure:



Click the zoom in icon at the upper right of the graph to view the curve on a full screen. When the cursor hovers over the graph, the current corresponding date and its historical data capacity statistics and capacity trend prediction will be displayed. Click the zoom in/out button again to go back to the business data reporting page, as shown below:



Note: when the system is in initial status and has not carried out data statistics, the page displays no data temporarily.

➤ Data operation

Data operations include the number of effective data backups, the number of successful data restore, the number of general DDL statements successfully executed, and the number of online DDL statements successfully executed. The data will be acquired and displayed in real time.

Data backup:

Management -> Data backup. The completed backup tasks will be counted in real time.

Data restore:

Management -> Data restore, the data restored successfully will be counted in real time.

General DDL:

Management -> Table structure modification -> General DDL. Execute general DDL, every DDL successfully executed will be counted in real time.

Online DDL:

Management -> Table structure modification -> Online DDL, execute online DDL, every DDL successfully executed will be counted in real time.

At present, the execution times of different operations will be counted by month. When the new month comes, the operation times will be accumulated again from zero, as

shown in the following figure:



Note: when the system is in initial status and has not carried out data statistics, the page displays no data temporarily.

(3) Cluster performance

The data displayed in the cluster performance is the peak value and corresponding time of the compute node within the selected time range, including two parts of data: the QPS, TPS and the number of connections of the compute node, and the QPS and the number of connections of the data source. The data will be updated regularly at 0:00 every day, as shown in the following figure:



Note: when the system is in initial status and has not carried out data statistics, the number of all components will be displayed with "-".

(4) Cluster support

Cluster support calculates the high available data of the current cluster's compute nodes, data nodes and ConfigDB respectively, including cumulative failure time, cumulative failure times and reliability. The data is updated regularly at 0:00 every day and displayed on the management platform in combination of graphics and text.

➤ Cumulative failure time

Cumulative failure time of compute node: the cumulative time of all high availability switch of the cluster's compute nodes within the selected time range, unit: seconds.

Cumulative failure time of data node: the cumulative time of all high availability switch of the cluster's all data nodes within the selected time range, unit: seconds.

Cumulative failure time of ConfigDB: the cumulative time of all high availability switch of the cluster's all ConfigDBs within the selected time range, unit: seconds.

➤ Total switching times

Cumulative switching times of compute node: the total number of high availability switch of the cluster's all compute nodes in the selected time range.

Cumulative switching times of data node: the total number of high availability switch of the cluster's all data nodes in the filtered time range.

Cumulative switching times of ConfigDB: the total number of high availability switch of the cluster's all ConfigDBs within the filtering time range.

➤ Reliability

Reliability = $(1 - (\text{cumulative failure time in the selected range} / \text{total time of the selected range})) * 100\%$. If the cumulative failure time is 0, the reliability will be 100% without calculation.



Note: when the system is in initial status and has not carried out data statistics, the number of all components will be displayed with "-". When the compute node, data node or ConfigDB is a single node, "a single node with no statistics for now" will be displayed.



(5) Cluster operation and maintenance

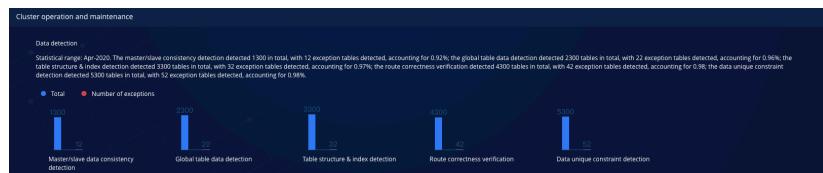
Cluster operation and maintenance includes data detection, deployment upgrade, alert optimization and safety protection.

➤ Data detection

It includes five types of detection, including master/slave data consistency detection, global table data detection, table structure&index detection, route correctness verification, and data unique constraint detection, which are displayed in combination

of graphics and text.

- 1) Proportion of exception tables = (number of exception tables / total number of detected tables) * 100%
- 2) In the detection submenu, master/slave data consistency detection, global table data detection, table structure&index detection, route correctness verification, and data unique constraint detection can be performed. Real-time statistics of detection data will be displayed, as shown in the following figure:



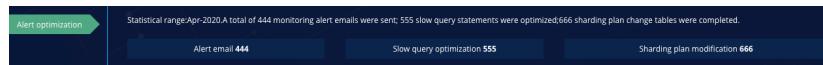
➤ Deployment upgrade

Display the number of cluster upgrades and license updates that have been successfully completed within the selected time range. When there are upgrade and update operations, the data will be counted and displayed in real time, as shown in the following figure:



➤ Alert optimization

It shows the number of alert emails successfully sent, the number of optimized slow queries and the number of tables with sharding plan modification in the selected time range. Real time statistics will be displayed as follows:



➤ safety protection

It shows the number of intercepted IP, the number of intercepted SQL and the number of intercepted wrong password login (wrong password of login server / management end) within the selected time range, as shown in the following figure:



Note: when the system is in initial status and has not carried out data statistics, the number of all components will be displayed with "-" or no data display temporarily.

22.4. Intelligent inspection

In order to facilitate the operation and maintenance personnel to detect whether there are hidden dangers or exceptions in the database cluster, we add the intelligent inspection function in v.2.5.6 and above. Through this function, you can carry out the day-to-day database inspection of the compute node cluster, and avoid the hidden trouble existing in the running process of the current database service in time.

For details, you can refer to the [Distributed Transactional Database HotDB Server - V2.5.6 \[Intelligent Inspection\] Function Manual](#).

23. Navigation

The navigation is at the top of HotDB Management and is displayed globally. For the above operations, menu privilege control is currently not supported.



23.1. Version



- It displays the current compute node cluster: cluster name, compute node version number, license authorization information (license type: beta or permanent version, remaining time), limit of number of nodes, limit of number of ConfigDBs.
- Click on “License Management” to hyperlink to the “[License Management](#)” function.

License information description:

- When the compute node cannot be connected, there will be a red dot mark. When clicking “Version No.”, it will prompt “Unable to connect to the compute node”, as shown below:



- For license status detection, when the license information is abnormal, the information bar displays the corresponding exception reminder information (orange dot reminder), as shown below:



Other forms of license exception notification: In case of license information detection exception, in addition to the corresponding prompt in the top information bar, an exception prompt will pop up when the user logging in to the management platform or refreshing the home page. In addition, the user can also configure the [Email Notification Strategy](#) to obtain an email reminder when the license information is abnormal. Relevant exception information is also recorded in the compute node log.

Special note: Currently, the abnormal license information will not cause the stop of compute node service, but it still needs to be noted. The problem can be solved by restarting the compute node service during the low peak period of service.

23.2. Compute node cluster switching

On the Compute Node Cluster Selection page, click the [Back to Compute Node Cluster Selection] button to enter the Compute Node Cluster Selection page.



23.3. Help

23.3.1. Tutorial

Description: In the navigation bar, click on the Help and select [Tutorial] to enter the tutorial guide page.



23.4. Reload

23.4.1. Reload instructions

Description: When the compute node related configDB parameters are modified in

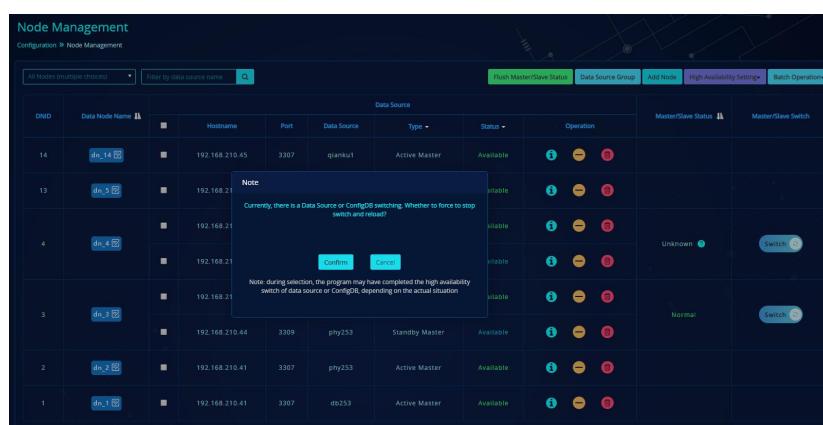
HotDB Management, the modified parameters shall be synchronized to the memory of compute node through the “Reload” function to take effect immediately. Currently, only some parameters support Reload.

Reload prompt description: When there is a scenario triggering reload in the management platform, a To Be Loaded mark appears on the [Reload] button. After the user clicks [Reload] and “Synchronization Complete” is prompted, the To Be Loaded mark will disappear automatically. If the user does not click [Reload], the mark still appears after logging out and logging in again. The mark is specifically in the cluster of compute nodes, and when different users enter the same compute node cluster, all To Be Loaded marks can be displayed, as shown below:



Reload special scenario description

If master/slave configDB and master/slave data source switch occur during Reload, the page will prompt the user and provide two options: [Forced Switch Stop] and [Cancel Reload]. The details are as follows:



The screenshot shows the Node Management page. A modal dialog box is overlaid on the list of nodes. The dialog contains a note: "Currently, there is a Data Source or ConfigDB switching. Whether to force to stop switch and reload?" It includes two buttons: "Confirm" and "Cancel". Below the note, a smaller text says: "Note: during selection, the program may have completed the high availability switch of data source or ConfigDB, depending on the actual situation".

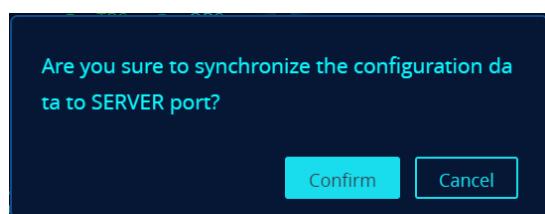
Click the [Confirm] button to forcibly cancel the current switch and perform synchronous loading, and then successful synchronous loading is prompted. Click the [Cancel] button to cancel the synchronous loading operation.

23.4.2. Function exercise



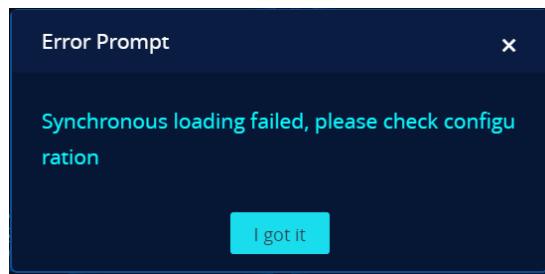
The screenshot shows the Cluster Overview page. In the top right corner of the navigation bar, there is a red 'RELOAD' button. The main content area displays the cluster's starting time as '2019-09-25, 18:32:03' and its running time as '04h, 57min, 09sec'. Below this, a chart titled 'Cluster Throughput' plots TPS (Transactions Per Second) and QPS (Queries Per Second) against time intervals from 09:25 to 09:29.

Step 1: Click the [Reload] button in the navigation bar. The pop-up box prompts: “Are you sure to synchronize the configuration data to SERVER port?”

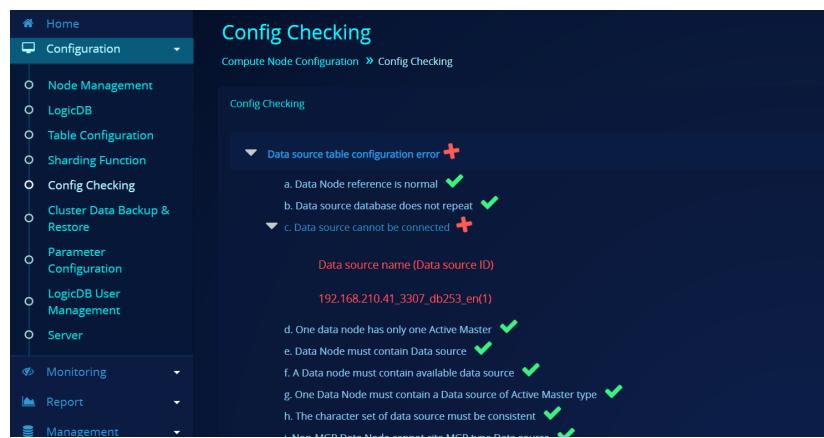


Step 2: Click [Confirm] to check whether there is an error in the contents of the “Configuration->[Config Checking](#)” module. “Synchronization succeeded” is prompted

when all detection items are normal. “Configuration verification failed” is prompted when there is an error.



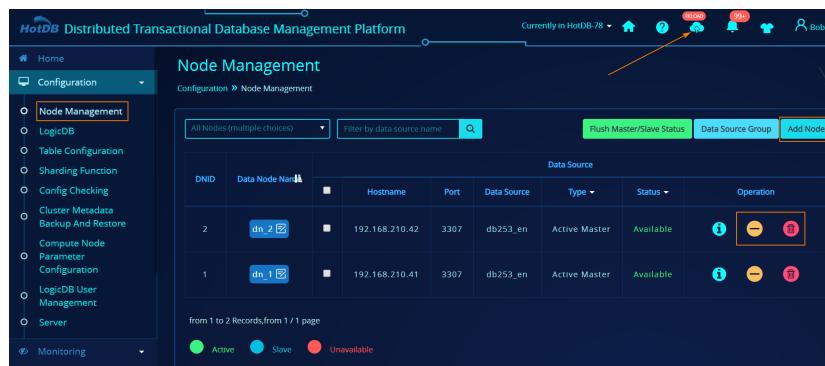
Step 3 (in case of an exception): After the config checking fails, click [Config Checking] to jump to the “Configuration->[Config Checking](#)” module to view the specific error information.



The screenshot shows the 'Config Checking' module. The left sidebar has a 'Configuration' section selected. The main area displays a tree structure of configuration errors. One error node is expanded, revealing several sub-error nodes, each marked with a green checkmark, indicating they have passed validation.

- ▼ Data source table configuration error +
 - a. Data Node reference is normal ✓
 - b. Data source database does not repeat ✓
 - ▼ c. Data source cannot be connected +
 - d. One data node has only one Active Master ✓
 - e. Data Node must contain Data source ✓
 - f. A Data Node must contain available data source ✓
 - g. One Data Node must contain a Data source of Active Master type ✓
 - h. The character set of data source must be consistent ✓

23.4.3. Reload triggering scenario



DNID	Data Node Name	Hostname	Port	Data Source	Type	Status	Operation		
2	dn_2	192.168.210.42	3307	db253_en	Active Master	Available			
1	dn_1	192.168.210.41	3307	db253_en	Active Master	Available			

from 1 to 2 Records, from 1 / 1 page

● Active ● Slave ● Unavailable

The function operations that trigger Reload are as follows:

- Node management: add, modify and delete
- Switch: add, modify and delete
- Data source group: add, modify and delete (the data source group of operation shall have associated data source, otherwise it will not be triggered)
- LogicDB: add, modify, delete and delete in batches
- Table configuration: quickly add table configuration, add new table, modify table, delete and delete in batches (including addition and deletion of child table)
- Sharding function: add, modify, delete and replicate
- Compute node parameter configuration: modify parameters
- Database user management: add, modify, delete and delete in batches
- White list: add, modify, switch, delete and add white list
- SQL Firewall: enable, enable in batches, disable and disable in batches
- Database user password: modify the password successfully
- Data source password: change, change in batches and setup with one click (set

selection and set all)

23.5. Notice

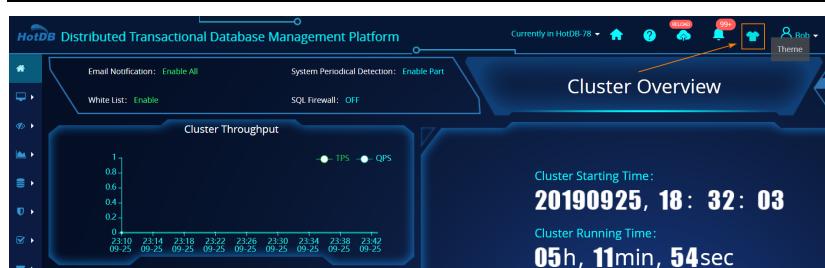
Description: This function is used to display various alert types of notification items and other notification items. When there is a notification item, the total number of notifications is displayed in the upper right corner. If there is no notification item, it is not displayed;



- The content of notice is consistent with the content of “[Event](#)” on the “Home”.
- Click on the specific event in the Notice to jump to “Event -> [History Event](#)” or specific function to view the details.
- The Notice content is divided into three levels: ERROR, WARNING and INFO, displayed with the icons of   and  respectively.
- Click the [Setting] button in the Notice to set whether to prompt the event.

23.6. Theme

Description: In the navigation bar, click [Theme] to change the theme style of the current HotDB Management.



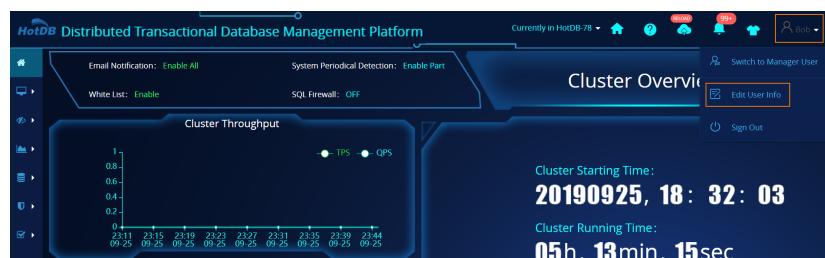
23.7. User information

23.7.1. Switch user view

- If the HotDB Management login user is “Manager User”, it can be switched to the manager user view page in the upper right corner in the general user view.
- If the HotDB Management login user is “Manager User”, it can be switched to the general user view page in the upper right corner in the manager user.

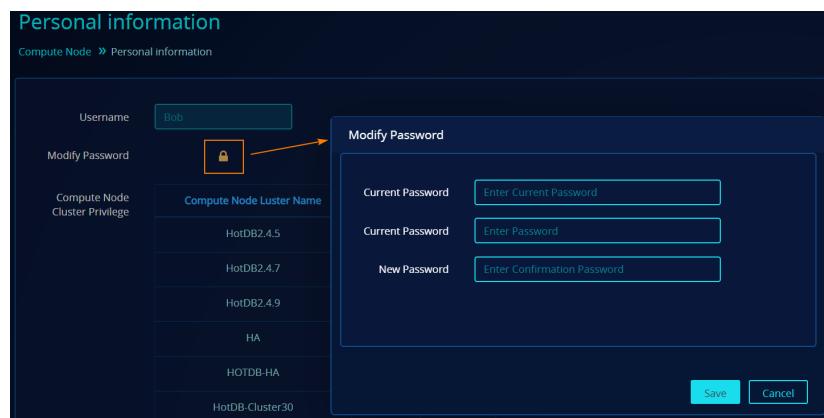
23.7.2. Modify user information

Description: In the Modify User Information page, only the personal password can be changed, and the username and compute node cluster privileges can be viewed. In the navigation bar, click [Modify User Information] to enter the personal information page.

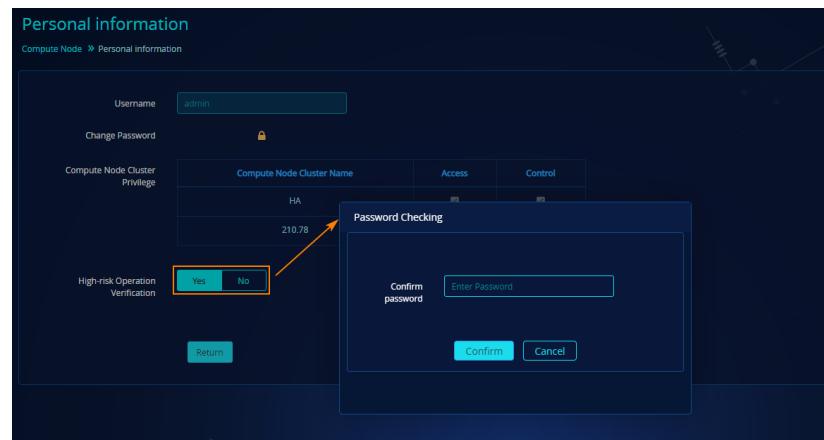


- On the Personal Information page, enter the current password, enter the new password and confirm the new password. Click [Save] to successfully change the user password.
- The new password shall not be the same as the current password.

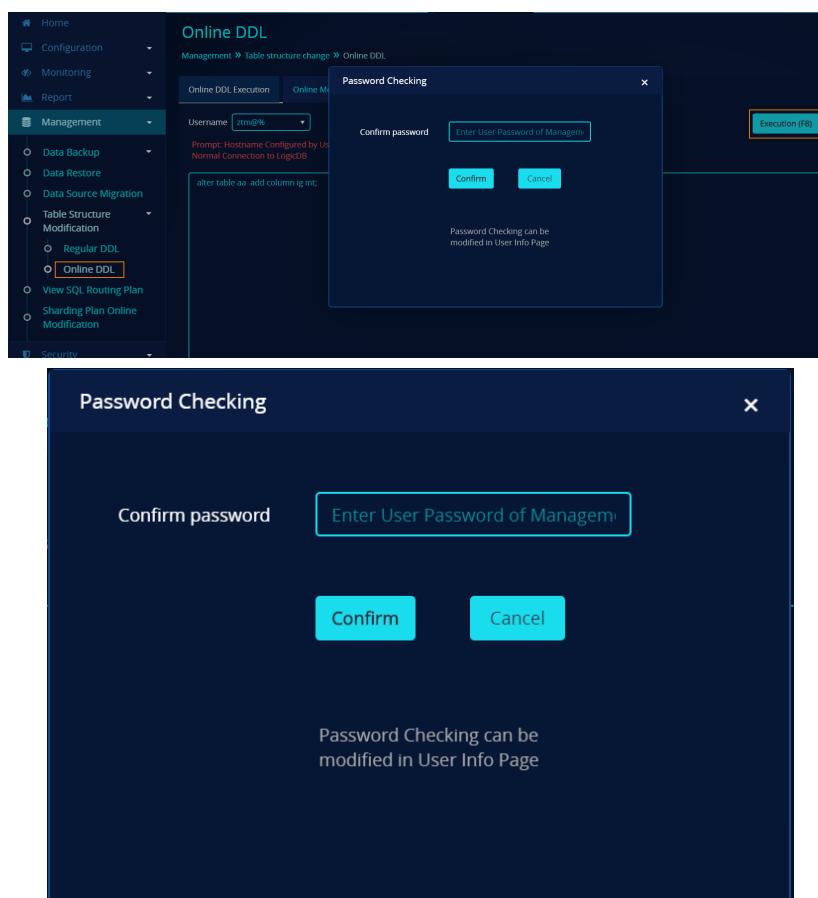
- If the password is forgotten, please contact super administrator to reset the password.



- High-risk operation qualification switch requires password checking by users when it is turned on or off.

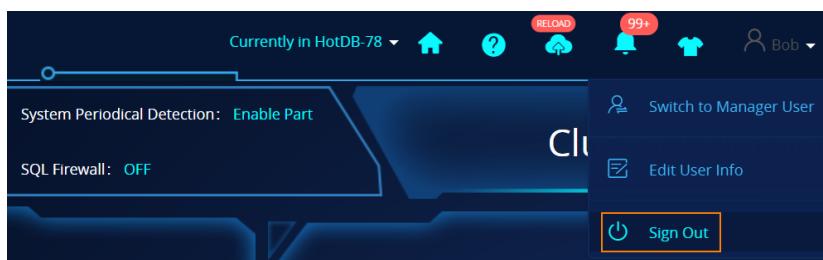


- When the high-risk operation switch is turned on, the page needs to confirm the advanced password if the user performs dangerous operations, such as data source password change, normal DDL and online DDL execution of SQL containing dangerous operation instructions such as “drop” and “truncate”.



23.8. Sign out

Description: In the navigation bar, click [Sign Out] to exit successfully. After signing out successfully, the program will jump to the login page.



23.9. Language

The management platform supports both Chinese and English; the default language is Chinese. If you want to switch to English, you can change the language parameters in application.properties under the installation conf/ directory on the management platform.

- Currently, the language parameter only supports Chinese and English.
 - You need to restart the management platform service to take effect after changing the parameters.

23.10. HTTPS secure access

The management platform supports encrypted access using HTTPS.

23.10.1. Start with default configuration

Under /conf/application.properties of the management platform installation directory, HTTPS configuration is annotated by default. If you want to enable it, delete the annotation and restart the management platform.

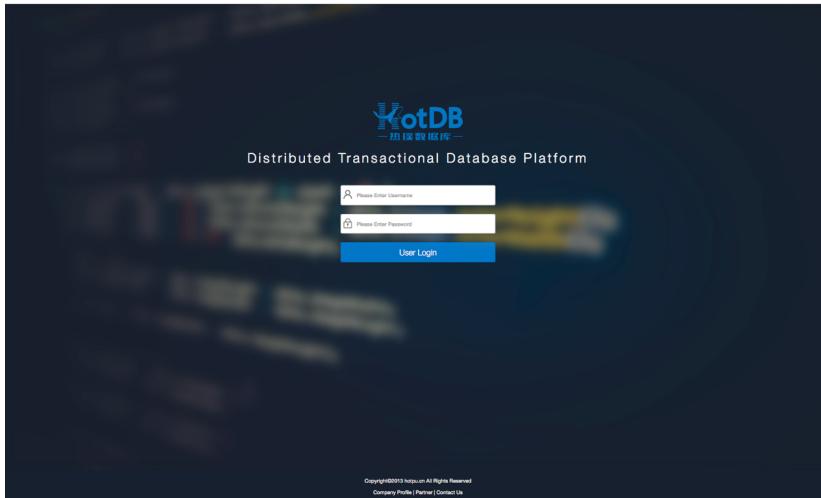
```
/usr/local/hotdb/hotdb-management-255/conf  
[root@drds-220-102 conf]# vim application.properties  
  
# http port  
server.port=3324  
  
# ssl socket port  
server.backup.port=3322  
  
# https  
# https.port=4322  
# https.keystore-password=zjsWg6977DwK6HBD  
# https.keystore-file=hotdb.jks
```

```
/usr/local/hotdb/hotdb-management-255/conf
[root@drds-220-102 conf]# vim application.properties

# http port
server.port=3324

# ssl socket port
server.backup.port=3322

# https
https.port=4322
https.keystore-password=zjsWg6977DwK6HBD
https.keystore-file=hotdb.jks
```



The meaning of HTTPS parameter is as follows:

https.port: HTTPS access port, 4322 by default.

https.keystore-password: Password of the generated .jks file, zjsWg6977DwK6HBD by default.

https.keystore-file: Name of the generated .jks file, hotdb.jks by default. The file is located under the directory /conf by default.

23.10.2. Customized HTTPS configuration

The management platform supports the customized name and password of jks file through JDK. The steps are as follows:

1. Execute the command through the /conf path of the management platform installation

directory.

You can generate it in two different ways.

Phased generation:

```
keytool -genkey -alias test -keypass 123456 -keyalg RSA -keysize 1024 -validity  
365 -keystore hotdbtest.jks -storepass 123456
```

Press Enter and input the relevant information.

One-time generation:

```
keytool -genkey -alias test -keypass 123456 -keyalg RSA -keysize 1024 -validity  
365 -keystore hotdbtest.jks -storepass 123456 -dname  
"CN=tester,OU=hotdb,O=hotdb,L=shanghai,ST=shanghai,C=CHINA"
```

Note:

Because jks files need to be placed in the /conf directory under the installation directory of the management platform, it is better to execute commands through the /conf path (or put it in the /conf directory after the file is generated).

The meaning of common commands of keytool in JDK are as follows:

-genkey: create a default file ".keystore" in the user's home directory, and an alias of mykey will also be generated. mykey contains the user's public key, private key and certificate (if no location is specified, .keystore will be located in the default directory of the user's system)

-alias: generate alias

-keystore: name of the specified keystore (the generated information will not be in the Keystore file)

-keyalg: algorithm for specifying the key (such as RSA, DSA)

-validity: specifies the validity period of the generated certificate, unit: day

-keysize: size of the specified key

-storepass: password for the specified keystore

```
-keypass: password for the specified alias

-dname: owner information of the specified certificate, for example: "CN = first
name and last name, OU = unit name, O = organization name, L = city or region
name, ST = state or province name, C = two letter country code of the unit"

-v: show certificate details in keystore

Note: more commands can be viewed using: keytool - help.
```

2. Modify https.keystore -password and https.keystore -file in application.xml to be the newly generated value and restart the management platform to access the management platform using HTTPS.

```
[root@drds-220-102 conf]#
[root@drds-220-102 conf]# keytool alias test -keypass test123456 -keyalg RSA -keysize 1024 -validity 365 -keystore hotdbtest.keystore -storepass 123456 -dname "CN=tester,OU=hotDB,O=hotDB,L=shanghai,ST=shanghai,C=CN"
total 200
drwxr-x 14 root root 122 May 29 12:03 .
drwxr-x 14 root root 122 May 29 16:59 ..
-rw-r--r-- 1 root root 28 May 29 16:59 application.properties
-rw-r--r-- 1 root root 28 May 29 16:59 application.properties_bak
-rw-r--r-- 1 root root 18 May 29 12:03 hotdbtest.keystore
[root@drds-220-102 conf]# vim application.xml
[root@drds-220-102 conf]#
[root@drds-220-102 conf]#
```

```
[root@drds-220-102 conf]# pwd
/usr/local/hotdb/hotdb-management-255/conf
[root@drds-220-102 conf]# vim application.properties

# http port
server.port=3324

# ssl socket port
server.backup.port=3322

# https
https.port=4322
https.keystore-password=123456
https.keystore-file=hotdbtest.jks
```

