

Distributed Transactional Database

HotDB Server -

[Intelligent Inspection]

Function Manual

Version No.: V2.5.6

Shanghai Hotpu Networks Technology Co., Ltd.

Nov. 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. Intelligent inspection.....	4
1.1. Premise of use	4
1.2. Function description	4
1.2.1. Patrol report	4
1.2.1.1. Layout	4
1.2.1.2. Start a patrol.....	5
1.2.1.3. Periodical plan.....	8
1.2.1.4. Export the report	9
1.2.2. Patrol indicator setting	9
1.2.2.1. Layout	9
1.2.2.2. Server hardware and software configuration.....	10
1.2.2.3. Server resource usage	11
1.2.2.4. Server hardware reliability.....	12
1.2.2.5. Compute node running status and statistics.....	13
1.2.2.6. Data source running status and statistics	15
1.2.2.7. Data verification and detection	16
1.2.2.8. Others.....	18
1.2.2.9. Batch edit.....	20
1.2.2.10. Batch reset	20
1.2.3. Historical records	21
1.2.3.1. Layout	21
1.2.3.2. View the details	21
1.2.3.3. Delete the task	22
1.2.3.4. Download the report	23
1.2.3.5. Batch deletion	23
1.2.4. Patrol details	24
1.2.4.1. Description of patrol matching logic.....	24
1.2.4.2. Description of patrol result logic	25

1. 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.

Function Entry: log in to the common role of the management platform, and click “Tool” -> “Intelligent inspection” to enter the intelligent inspection page.

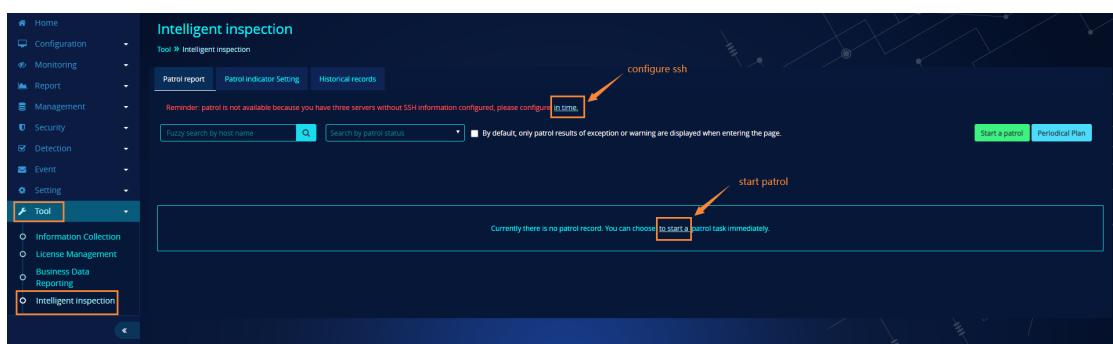
1.1. Premise of use

To initiate an intelligent inspection, the following preconditions shall be satisfied.

- The current user has the privilege of “intelligent inspection”.
- SSH information of the server needs to be configured.

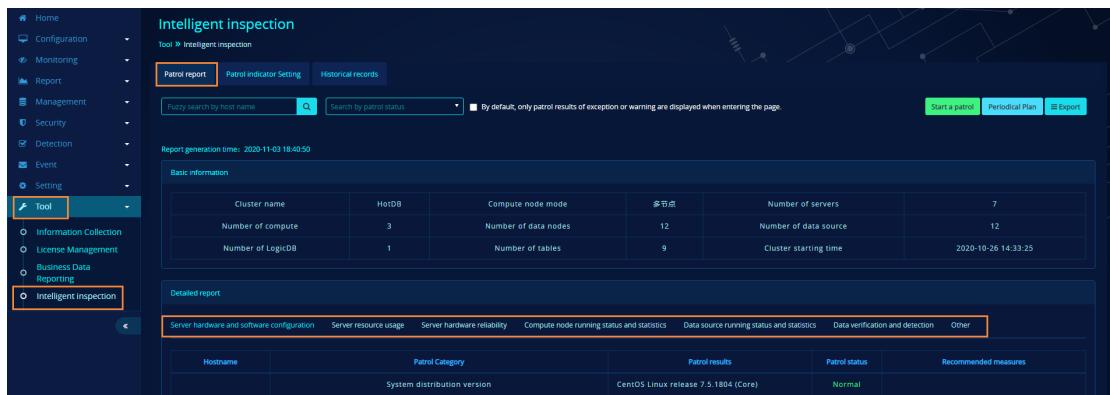
1.2. Function description

Intelligent inspection mainly includes three TABs: patrol report, patrol indicator setting and historical records, among which the patrol report is displayed by default, with the latest patrol result. When there is no historical record, it will prompt: “Currently there is no patrol record. You can choose to start a patrol task immediately.”



1.2.1. Patrol report

1.2.1.1. Layout



The screenshot shows the 'Intelligent inspection' section of the HotDB Server interface. On the left, a sidebar menu includes 'Tool' and 'Intelligent inspection' under the 'Tool' category. The main content area has tabs for 'Patrol report', 'Patrol indicator Setting', and 'Historical records'. It features a search bar for host name and patrol status, and a note about default display settings. Below is a table of basic cluster information:

Cluster name	HotDB	Compute node mode	节点数	Number of servers	7
Number of Compute	3	Number of data nodes	12	Number of data source	12
Number of LogiDB	1	Number of tables	9	Cluster starting time	2020-10-26 14:33:25

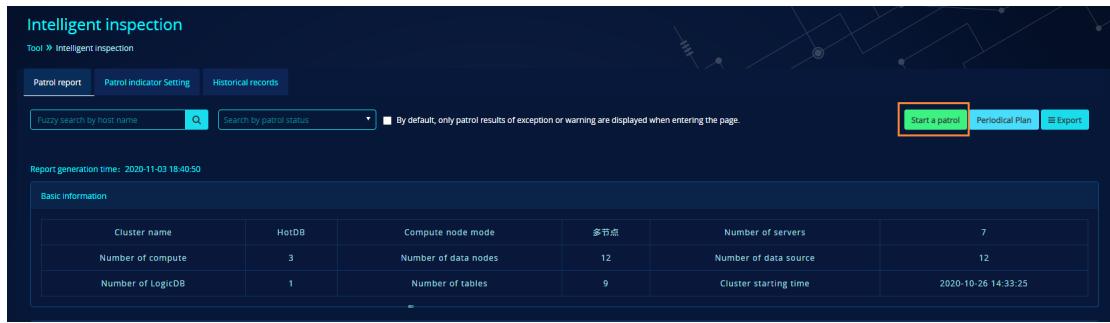
The 'Detailed report' section contains tabs for various monitoring metrics. A table below shows system details:

Hostname	Patrol Category	Patrol results	Patrol status	Recommended measures
	System distribution version	CentOS Linux release 7.5.1804 (Core)	Normal	

- Searching options includes fuzzy search by host name and search by patrol status.
- If you check “by default, only patrol results of exception or warning are displayed when entering the page”, only warnings or exceptions will be shown in the report, and this status will maintain even if you exit the page. If you cancel the checking, all items will be displayed.
- The report is divided into basic information and detailed report. The basic information shows information about the current cluster group, and the detailed report is divided into 7 modules, namely:
 - Server hardware and software configuration
 - Server resource usage
 - Server resource reliability
 - Compute node running status and statistics
 - Data source running status and statistics
 - Data verification and detection
 - Others

1.2.1.2. Start a patrol

(1) Start a patrol

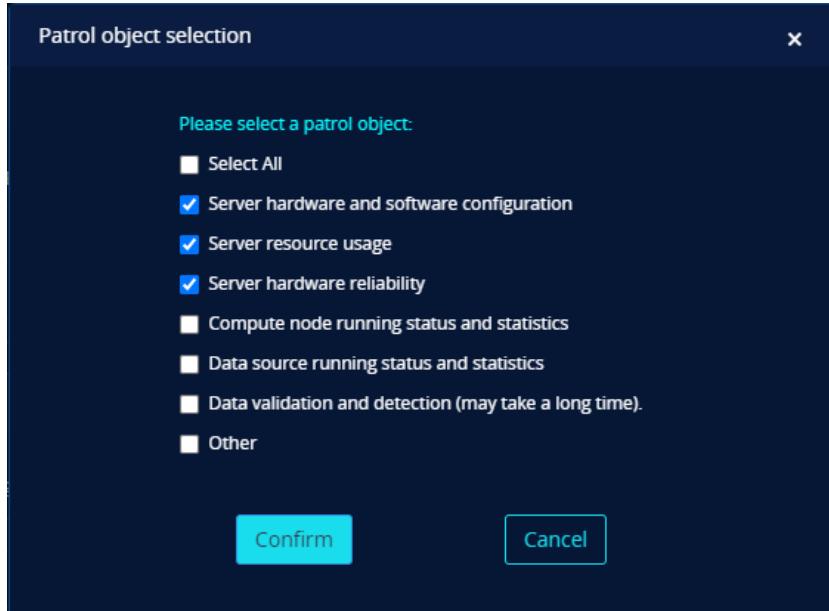


The screenshot shows the 'Intelligent inspection' page. At the top, there are tabs for 'Patrol report', 'Patrol indicator Setting', and 'Historical records'. Below the tabs is a search bar with 'Fuzzy search by host name' and 'Search by patrol status'. A checkbox indicates that by default, only patrol results of exception or warning are displayed. On the right side, there are buttons for 'Start a patrol', 'Periodical Plan', and 'Export'. Below the search area, it says 'Report generation time: 2020-11-03 18:40:50'. Under 'Basic information', there is a table with the following data:

Cluster name	HotDB	Compute node mode	多节点	Number of servers	7
Number of compute	3	Number of data nodes	12	Number of data source	12
Number of LogicDB	1	Number of tables	9	Cluster starting time	2020-10-26 14:33:25

- Click Start a patrol, the patrol object selection box will pop up.

(2) Patrol object selection



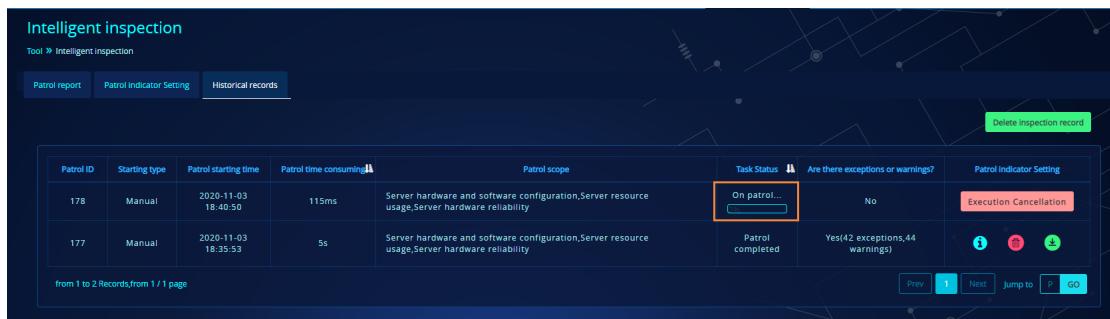
The dialog box is titled 'Patrol object selection'. It contains the message 'Please select a patrol object:' followed by a list of checkboxes:

- Select All
- Server hardware and software configuration
- Server resource usage
- Server hardware reliability
- Compute node running status and statistics
- Data source running status and statistics
- Data validation and detection (may take a long time).
- Other

At the bottom are 'Confirm' and 'Cancel' buttons.

- Check objects and start patrol.

(3) On patrol



The screenshot shows the 'Historical records' page for patrols. It displays two rows of patrol tasks:

Patrol ID	Starting type	Patrol starting time	Patrol time consuming	Patrol scope	Task Status	Are there exceptions or warnings?	Patrol Indicator Setting
178	Manual	2020-11-03 18:40:50	115ms	Server hardware and software configuration,Server resource usage,Server hardware reliability	On patrol...	No	Execution Cancellation
177	Manual	2020-11-03 18:35:53	5s	Server hardware and software configuration,Server resource usage,Server hardware reliability	Patrol completed	Yes(42 exceptions,44 warnings)	! ! !

At the bottom, it says 'from 1 to 2 Records from 1 / 1 page' and has buttons for 'Prev', 'Next', 'Jump to', and 'Go'.

- After starting a patrol, you will enter the historical record page and view the patrol tasks that are currently in progress.

- The task status column shows progress of the current patrol task, and the page is refreshed every 5s.
- When there is a patrol task in progress, a new patrol cannot be started (based on the current group).

(4) Patrol completed

Intelligent inspection						
Tool > Intelligent inspection						
Patrol report		Patrol indicator Setting		Historical records		
Patrol ID	Starting type	Patrol starting time	Patrol time consuming	Patrol scope	Task Status	Are there exceptions or warnings?
178	Manual	2020-11-03 18:40:50	5s	Server hardware and software configuration,Server resource usage,Server hardware reliability	Patrol completed	Yes(42 exceptions,44 warnings)
177	Manual	2020-11-03 18:35:53	5s	Server hardware and software configuration,Server resource usage,Server hardware reliability	Patrol completed	Yes(42 exceptions,44 warnings)

from 1 to 2 Records,from 1 / 1 page

Prev 1 Next Jump to P GO

- Once the patrol is completed, “Task Status” will be updated to patrol completed.
- If there are patrol items of warnings or exceptions, “Are there exceptions or warning” will count the number of warnings or exceptions in all patrol items.
- If there is no warnings or exceptions, “No” will be displayed in “Are there exceptions or warning”.
- When the patrol is completed, a result file and patrol report generated during the patrol process will be shown in “hotdb-management/data/Inspection”.

(5) Execution cancelled

Intelligent inspection						
Tool > Intelligent inspection						
Patrol report		Patrol indicator Setting		Historical records		
Patrol ID	Starting type	Patrol starting time	Patrol time consuming	Patrol scope	Task Status	Are there exceptions or warnings?
179	Manual	2020-11-03 18:41:38	83ms	Server hardware and software configuration,Server resource usage,Server hardware reliability	On patrol	No
178	Manual	2020-11-03 18:40:50	5s	Server hardware and software configuration,Server resource usage,Server hardware reliability	Patrol completed	Yes(42 exceptions,44 warnings)
177	Manual	2020-11-03 18:35:53	5s	Server hardware and software configuration,Server resource usage,Server hardware reliability	Patrol completed	Yes(42 exceptions,44 warnings)

from 1 to 3 Records,from 1 / 1 page

Prev 1 Next Jump to P GO

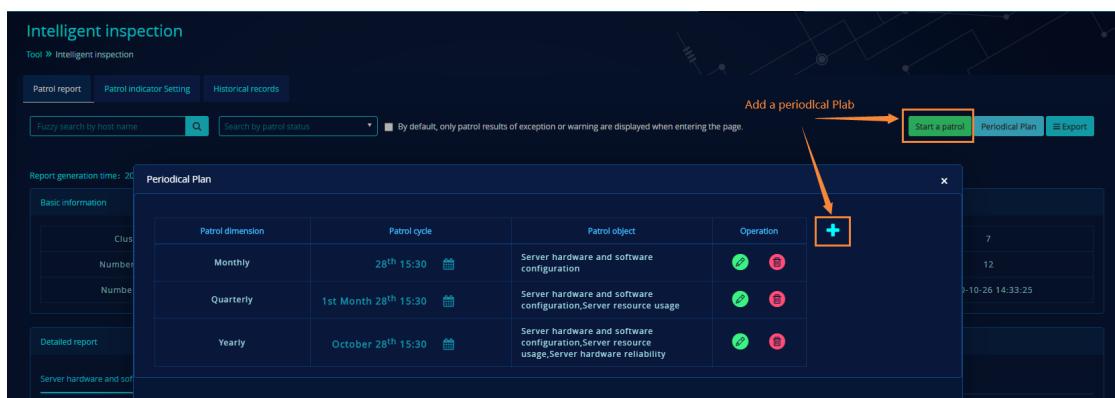
- Click “Execution Cancellation” to cancel the current patrol task.
- When the task is cancelled successfully, “Task Status” will be updated to “Patrol failed”.
- “No” will be shown in “Are there exceptions or warning”.
- When the patrol task is cancelled, no files will be generated in “hotdb-management/data/Inspection”.



Patrol ID	Starting type	Patrol starting time	Patrol time consuming	Patrol scope	Task Status	Are there exceptions or warnings?	Patrol Indicator Setting
180	Manual	2020-11-03 18:42:17	2s	Server hardware and software configuration, Server resource usage, Server hardware reliability	Patrol Failure	No	

1.2.1.3. Periodical plan

In addition to manually starting patrol task, you can also add a periodical plan. Click “Periodical Plan” to manage the current periodical plans.



Patrol dimension	Patrol cycle	Patrol object	Operation
Monthly	28 th 15:30	Server hardware and software configuration	 
Quarterly	1 st Month 28 th 15:30	Server hardware and software configuration, Server resource usage	 
Yearly	October 28 th 15:30	Server hardware and software configuration, Server resource usage, Server hardware reliability	 

- You can only add six items at most in Periodical Plan, "Monthly", "Quarterly" and "Yearly" can be selected in Patrol dimension.
- For others, please refer to the manual task starting description.
- When there is overlap in the Periodical Plan, the program will only execute one periodical plan.

- If there are other patrol tasks are in progress during the execution of Periodical Plan, it will be retried after 1 min and wait for 10 min at most. If there are still unfinished patrol tasks, the patrol result will be set as "patrol failed", with the failure reason: "there are other patrol tasks in progress at the same time".

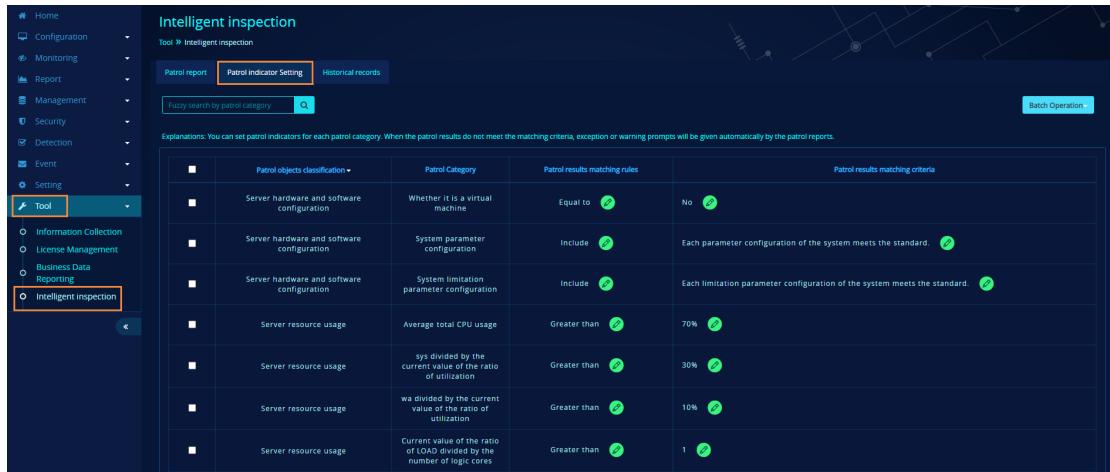
1.2.1.4. Export the report



- Click “Export – Export exceptions and warning data”, and the downloaded report will only contain patrol items with warnings and exceptions.
- Click “Export – Export the whole data”, and the downloaded report will contain all items.
- After the patrol, the report will be stored in the directory hotdb-management/data/Inspection.
- In the exported data, the "you can download the file to view details" will be replaced with "details can be viewed in the downloaded files under the directory /data/Inspection/".
- In the exported data, if there is "manually click the Install button to install relevant software" in the list of historical patrol inspection results, it will be replaced with: "please manually install relevant software".
- In the exported data, the " manuallly click the Install button to install relevant software " will be replaced with "please manually install relevant software".

1.2.2. Patrol indicator setting

1.2.2.1. Layout

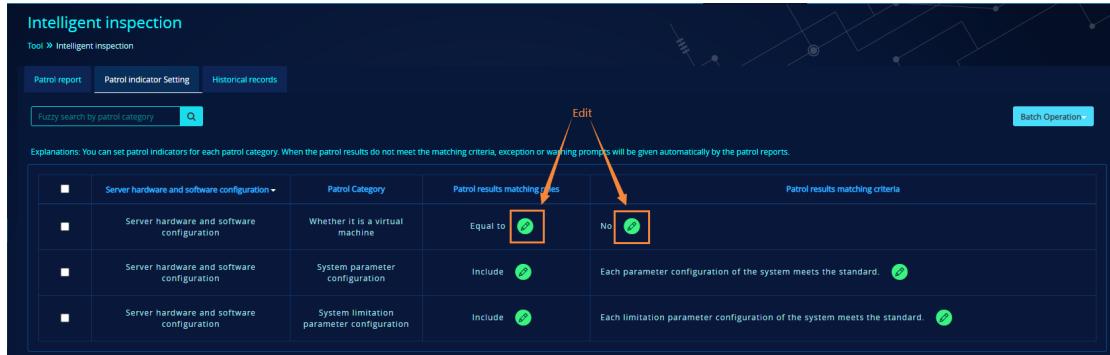


The screenshot shows the 'Intelligent inspection' section of the HotDB interface. On the left, there's a navigation sidebar with 'Tool' selected. The main area displays a table of patrol objects classification, categorized by Patrol Category. Each row includes a 'Patrol results matching rules' column with edit buttons and a 'Patrol results matching criteria' column.

Patrol objects classification	Patrol Category	Patrol results matching rules	Patrol results matching criteria
Server hardware and software configuration	Whether it is a virtual machine	Equal to 	No 
Server hardware and software configuration	System parameter configuration	Include 	Each parameter configuration of the system meets the standard. 
Server hardware and software configuration	System limitation parameter configuration	Include 	Each limitation parameter configuration of the system meets the standard. 
Server resource usage	Average total CPU usage	Greater than 	70% 
Server resource usage	sys divided by the current value of the ratio of utilization	Greater than 	30% 
Server resource usage	wa divided by the current value of the ratio of utilization	Greater than 	10% 
Server resource usage	Current value of the ratio of LOAD divided by the number of logic cores	Greater than 	1 

- Displays indicators of all patrol categories, and supports fuzzy search by patrol category.
- Patrol objects can be classified by the header “patrol objects classification”.
- You can change corresponding matching rules by clicking the Edit button of matching rules and matching criteria.

1.2.2.2. Server hardware and software configuration



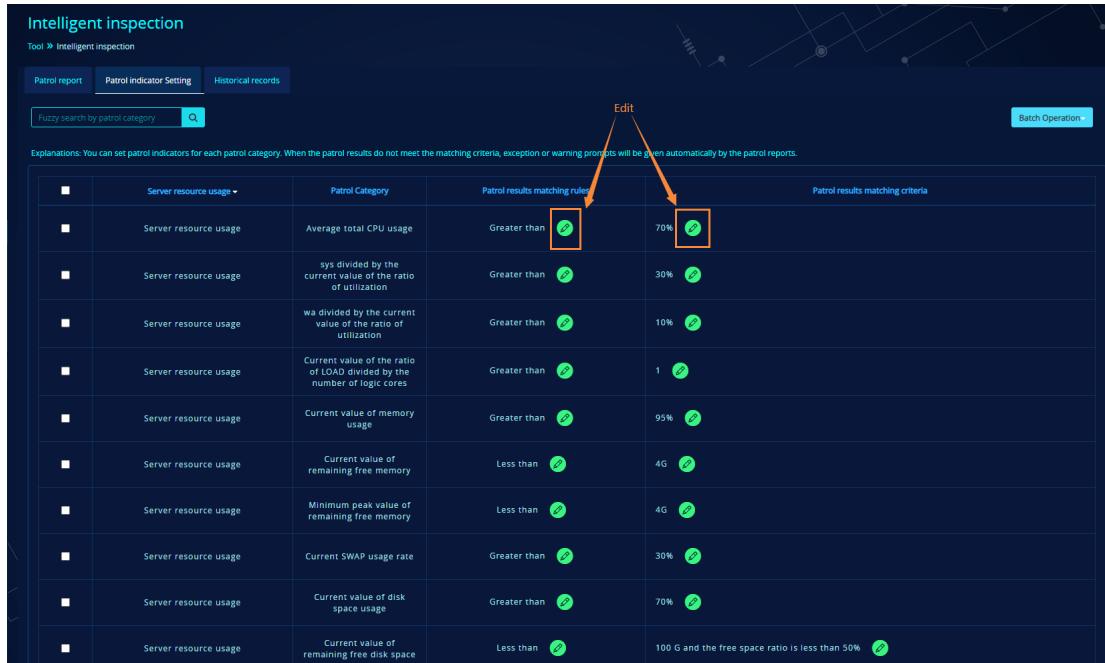
This screenshot shows the same 'Intelligent inspection' interface as above, but with a specific focus on the 'Server hardware and software configuration' category. An orange arrow points from the word 'Edit' to the edit icon in the 'Patrol results matching rules' column of the first row.

Patrol objects classification	Patrol Category	Patrol results matching rules	Patrol results matching criteria
Server hardware and software configuration	Whether it is a virtual machine	Equal to 	No 
Server hardware and software configuration	System parameter configuration	Include 	Each parameter configuration of the system meets the standard. 
Server hardware and software configuration	System limitation parameter configuration	Include 	Each limitation parameter configuration of the system meets the standard. 

- Patrol categories of the server hardware and software configuration are as follows:
 - Whether it is a virtual machine
 - System parameter configuration
 - System limitation parameter configuration
- The default value of matching rule of “Whether it is a virtual machine” is “equal to”, which can be edited as: equal to, not equal to, and no attention is required; the default matching criteria is “no”, which can be edited as no and yes.

- For other patrol categories, the default matching rules is “include”, which can be edited as include, not include, and no attention is required. The default matching criteria is the indicator of each patrol category, and can be edited as any value.

1.2.2.3. Server resource usage



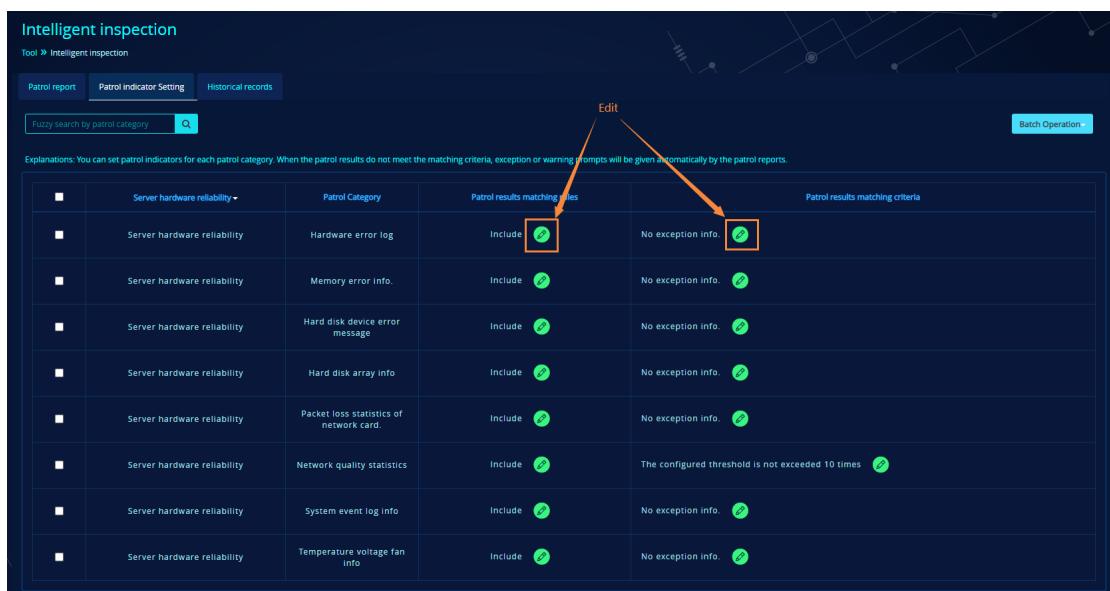
The screenshot shows the 'Intelligent inspection' interface with the 'Tool > Intelligent inspection' menu selected. The 'Patrol report' tab is active. A callout arrow points to the 'Edit' button located next to the 'Patrol results matching rules' column in the table below. The table lists various server resource usage metrics and their corresponding patrol categories and matching rules.

	Server resource usage	Patrol Category	Patrol results matching rules	Patrol results matching criteria
■	Average total CPU usage		Greater than 	70% 
■	sys divided by the current value of the ratio of utilization		Greater than 	30% 
■	wa divided by the current value of the ratio of utilization		Greater than 	10% 
■	Current value of the ratio of LOAD divided by the number of logic cores		Greater than 	1 
■	Current value of memory usage		Greater than 	95% 
■	Current value of remaining free memory		Less than 	4G 
■	Minimum peak value of remaining free memory		Less than 	4G 
■	Current SWAP usage rate		Greater than 	30% 
■	Current value of disk space usage		Greater than 	70% 
■	Current value of remaining free disk space		Less than 	100 G and the free space ratio is less than 50% 

- Patrol categories of the server resource usage are as follows:
- Average total CPU usage
 - Sys divided by the current value of the ratio of utilization
 - Wa divided by the current value of the ratio of utilization
 - Current value of the ratio of LOAD divided by the number of logic cores
 - Current value of memory usage
 - Current value of remaining free memory
 - Minimum peak value of remaining free memory
 - Current SWAP usage rate
 - Current value of disk space usage
 - Current value of remaining free disk space

- Current value of disk IO utilization
- Current value of network bandwidth utilization (NetIn)
- Current value of network bandwidth utilization (NetOut)
- The default value of matching rule of "current value of remaining free memory" and "minimum peak value of remaining free memory" is "greater than"; the default value of matching rule for other patrol categories is "less than".
- The matching rules can be edited as follows: greater than, less than, greater than or equal to, less than or equal to, no attention is required.
- When the matching criteria is displayed in percentage, the minimum value is 0 and the maximum value is 100.

1.2.2.4. Server hardware reliability



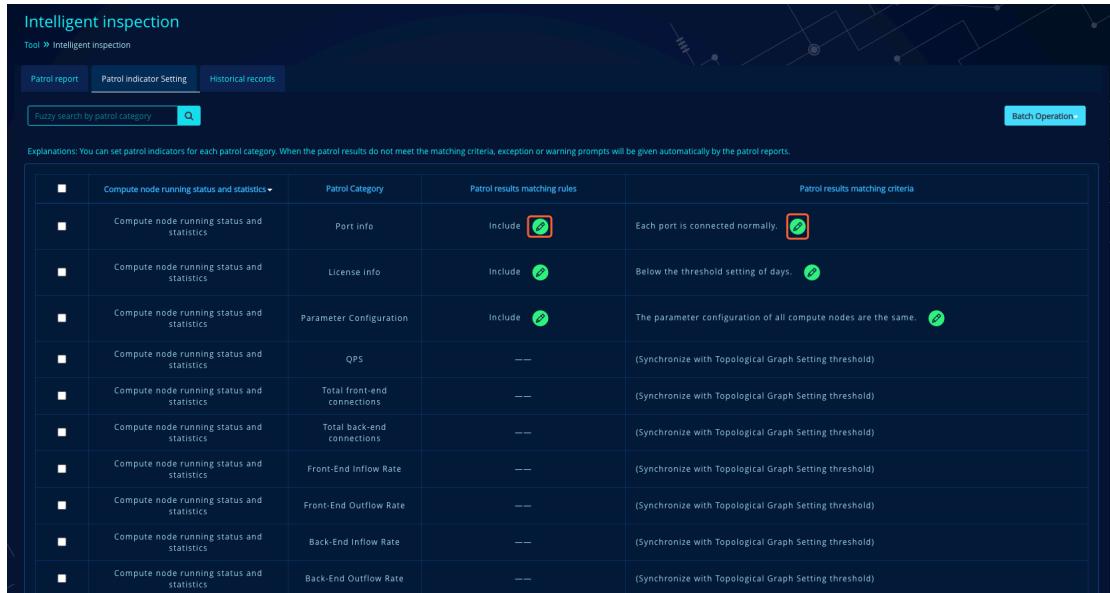
The screenshot shows the 'Intelligent inspection' interface with the 'Patrol indicator Setting' tab selected. A table lists patrol categories and their matching rules. Two specific rows are highlighted with red boxes: 'Include' and 'No exception info.' with a green checkmark icon. An 'Edit' button is shown above the table.

	Patrol Category	Patrol results matching rules	Patrol results matching criteria
■	Server hardware reliability	Include 	No exception info. 
■	Server hardware reliability	Memory error info.	
■	Server hardware reliability	Hard disk device error message	
■	Server hardware reliability	Hard disk array info	
■	Server hardware reliability	Packet loss statistics of network card.	
■	Server hardware reliability	Network quality statistics	
■	Server hardware reliability	System event log info	
■	Server hardware reliability	Temperature voltage fan info	

- Patrol categories of the server hardware reliability are as follows:
 - Hardware error log
 - Memory error info.
 - Hard disk device error message
 - Hard disk array info
 - Packet loss statistics of network card

- Network quality statistics
 - System event log info
 - Temperature voltage fan info.
- The default value of matching rule is “include”, which can be edited as: include, not include and no attention is required.
- The default value of matching rule is 10 and the minimum value is 0; for other patrol categories, the default value is no exceptions info and can be edited as any value.

1.2.2.5. Compute node running status and statistics



The screenshot shows the 'Intelligent inspection' interface under the 'Tool > Intelligent inspection' menu. The 'Patrol report' tab is selected. A table lists various patrol categories and their matching rules and criteria:

	Compute node running status and statistics ▾	Patrol Category	Patrol results matching rules	Patrol results matching criteria
■	Compute node running status and statistics	Port info	Include <input checked="" type="checkbox"/>	Each port is connected normally. <input checked="" type="checkbox"/>
■	Compute node running status and statistics	License info	Include <input checked="" type="checkbox"/>	Below the threshold setting of days. <input checked="" type="checkbox"/>
■	Compute node running status and statistics	Parameter Configuration	Include <input checked="" type="checkbox"/>	The parameter configuration of all compute nodes are the same. <input checked="" type="checkbox"/>
■	Compute node running status and statistics	QPS	--	(Synchronize with Topological Graph Setting threshold)
■	Compute node running status and statistics	Total front-end connections	--	(Synchronize with Topological Graph Setting threshold)
■	Compute node running status and statistics	Total back-end connections	--	(Synchronize with Topological Graph Setting threshold)
■	Compute node running status and statistics	Front-End Inflow Rate	--	(Synchronize with Topological Graph Setting threshold)
■	Compute node running status and statistics	Front-End Outflow Rate	--	(Synchronize with Topological Graph Setting threshold)
■	Compute node running status and statistics	Back-End Inflow Rate	--	(Synchronize with Topological Graph Setting threshold)
■	Compute node running status and statistics	Back-End Outflow Rate	--	(Synchronize with Topological Graph Setting threshold)

- Patrol categories of the compute node running status and statistics are as follows:
- Port info
 - License info
 - Parameter Configuration
 - QPS
 - Total front-end connections
 - Total back-end connections

- Front-End inflow rate
 - Front-End outflow rate
 - Back-End inflow rate
 - Back-End outflow rate
 - heap memory usage
 - direct memory usage
 - The cluster integrity
 - High availability status
 - DR status
 - Password security management
 - The SQL firewall
 - The IP whitelist
 - Slow query SQL records
 - ERROR level
 - WARN level
- Description of patrol categories of port info, license info, parameter configuration, cluster integrity, high availability status, DR status, password security management and slow query SQL record.
- The default matching rule is “include”, which can be edited as: include, not include and no attention is required.
 - The default value of matching criteria of high availability status, DR status and password security management is “no exceptions” and can be edited to any value.
 - The default value of matching criteria of port info, license info, parameter configuration, cluster integrity and slow query SQL records is the indicator of each patrol category and can be edited to any value.

➤ SQL firewall and IP whitelist

- The default value of matching rule is “not equal to”, which can be edited as: equal to, not equal to, and no attention is required.
- The default value of matching criteria is “not enabled” and can be edited to any value.

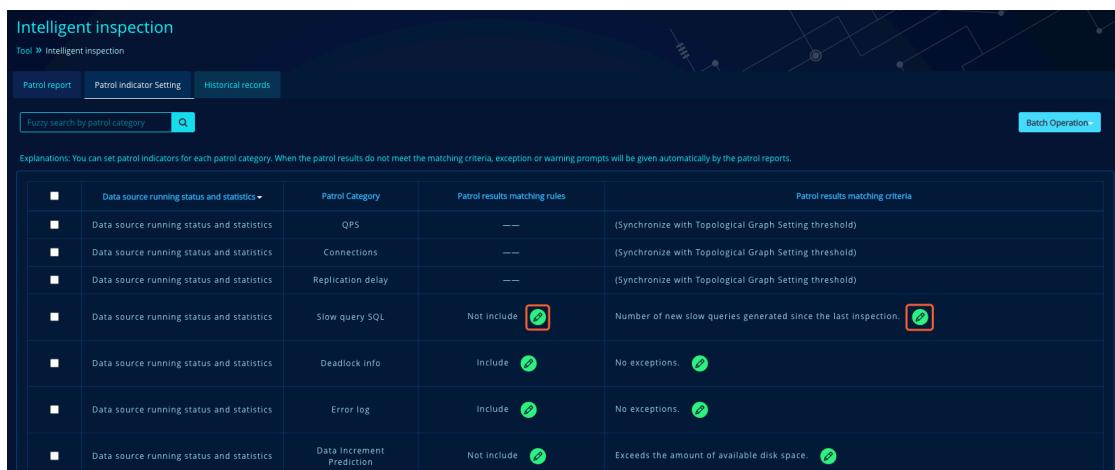
➤ ERROR level, WARN level

- The default value of matching rule is “less than or equal to”, which can be edited as greater than, less than, greater than or equal to, less than or equal to, no attention is required.
- The default value of matching criteria is 0, and can be edited to any value.

➤ QPS, total front-end connections, total back-end connections, front-end inflow rate, front-end outflow rate, back-end inflow rate, back-end outflow rate, heap memory usage, direct memory usage.

- The matching rules are as follows:--
- The matching criteria is synchronized with the threshold value of Setting -> Topological graph Alert Setting.

1.2.2.6. Data source running status and statistics



The screenshot shows the 'Intelligent inspection' section of the HotDB interface. At the top, there are tabs for 'Patrol report', 'Patrol indicator Setting', and 'Historical records'. Below these are search and batch operation buttons. A table lists patrol categories and their settings:

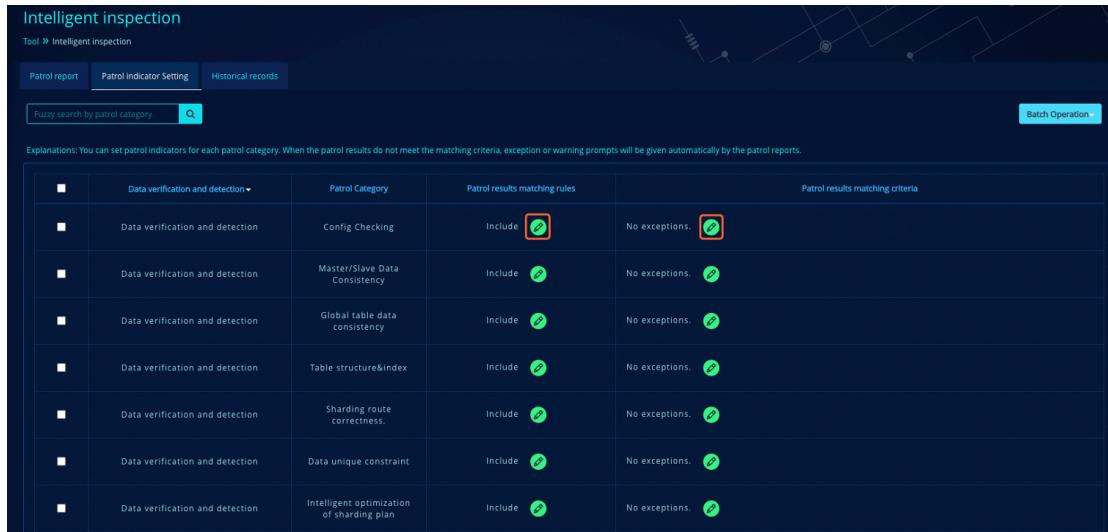
	Patrol Category	Patrol results matching rules	Patrol results matching criteria
Data source running status and statistics	QPS	— —	(Synchronize with Topological Graph Setting threshold)
Data source running status and statistics	Connections	— —	(Synchronize with Topological Graph Setting threshold)
Data source running status and statistics	Replication delay	— —	(Synchronize with Topological Graph Setting threshold)
Data source running status and statistics	Slow query SQL	Not include	Number of new slow queries generated since the last inspection.
Data source running status and statistics	Deadlock info	Include	No exceptions.
Data source running status and statistics	Error log	Include	No exceptions.
Data source running status and statistics	Data increment Prediction	Not include	Exceeds the amount of available disk space.

Explanations: You can set patrol indicators for each patrol category. When the patrol results do not meet the matching criteria, exception or warning prompts will be given automatically by the patrol reports.

- Patrol categories of the data source running status and statistics are as follows:

- QPS
 - Connections
 - Replication latency
 - Slow query SQL
 - Deadlock info
 - Error log
 - Data incremental Prediction
- Slow query SQL, data incremental prediction
- The default value of matching rule is “not include”, which can be edited as: include, not include and no attention is required.
 - The default value of matching criteria is the indicator of each patrol category, which can be edited to any values.
- Deadlock info. and error log
- The default value of matching rule is “include”, which can be edited as: include, not include and no attention is required.
 - The default value of matching criteria is “no exceptions”, which can be edited to any values.
- QPS, connections, replication delay
- The matching rules are as follows: --
 - The matching criteria is synchronized with the threshold value of Setting -> Topological graph Alert Setting.

1.2.2.7. Data verification and detection



The screenshot shows the 'Intelligent inspection' section of the HotDB interface. At the top, there are tabs for 'Patrol report', 'Patrol Indicator Setting', and 'Historical records'. Below these are search and batch operation buttons. A table lists patrol categories and their matching rules:

	Patrol Category	Patrol results matching rules	Patrol results matching criteria
■ Data verification and detection	Config Checking	Include	No exceptions.
■ Data verification and detection	Master/Slave Data Consistency	Include	No exceptions.
■ Data verification and detection	Global table data consistency	Include	No exceptions.
■ Data verification and detection	Table structure&index	Include	No exceptions.
■ Data verification and detection	Sharding route correctness.	Include	No exceptions.
■ Data verification and detection	Data unique constraint	Include	No exceptions.
■ Data verification and detection	Intelligent optimization of sharding plan	Include	No exceptions.

➤ Patrol categories of the data verification and detection are as follows:

- Config checking
- Master/Slave data consistency
- Global table data consistency
- Table structure & index
- Sharding route correctness
- Data unique constraint
- Intelligent optimization of sharding plan
- Examination score of deployment environment
- Sharding grade
- Validity detection of business data backup
- Validity detection of configuration data backup
- Consistency detection of configuration in memory

➤ Examination score of deployment environment and sharding grade

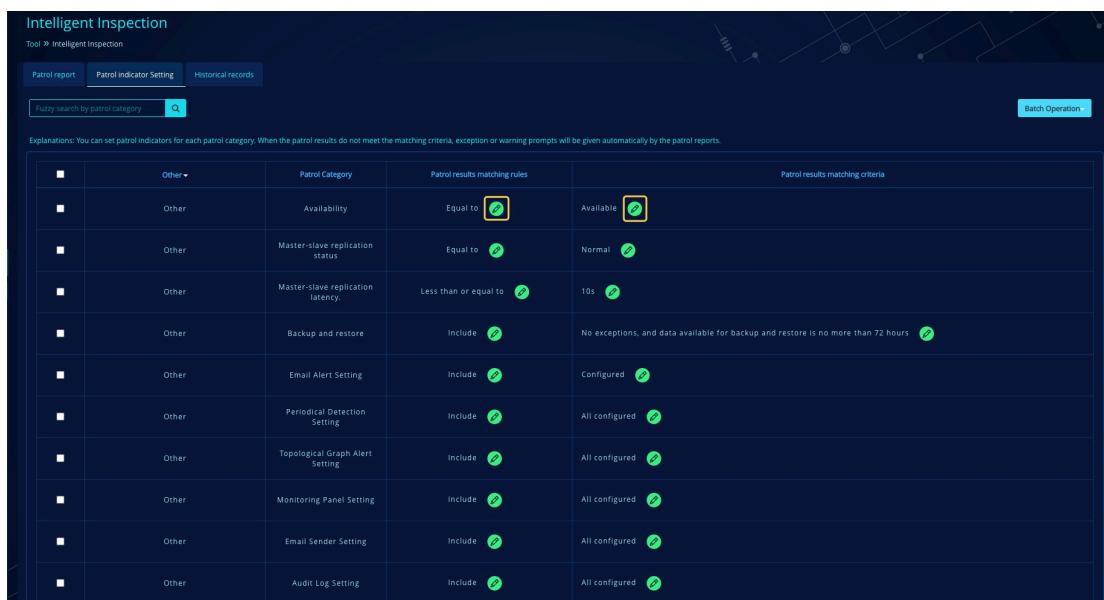
- The default value of matching rule is “greater than or equal to”, which can be edited as greater than, less than, greater than or equal to, less than or equal to, and no attention is required.

- For the matching criteria, the default value of examination score of the deployment environment is 100; the default value of sharding grade is 80. They can be edited to any integer value between [0, 100], unit: score.

➤ Others

- The default value of matching rule is “include”, which can be edited as: include, not include and no attention is required.
- The matching criteria: the default value of validity detection of business data backup is "no exceptions, and data available for backup and restore is no more than 24 hours."; the default value of validity detection of configuration data backup is "no exceptions, and the data available for backup and restore is no more than 72 hours". The matching criteria of these two results should be positive integers, unit: hours.
- The default matching criteria is “no exceptions” for patrol categories except for the above two items and can be edited to any value.

1.2.2.8. Others



The screenshot shows the 'Intelligent Inspection' interface with the 'Patrol report' tab selected. A table lists various patrol categories and their matching rules:

	Other	Patrol Category	Patrol results matching rules	Patrol results matching criteria
■	Other	Availability	Equal to <input checked="" type="checkbox"/>	Available <input checked="" type="checkbox"/>
■	Other	Master-slave replication status	Equal to <input checked="" type="checkbox"/>	Normal <input checked="" type="checkbox"/>
■	Other	Master-slave replication latency	Less than or equal to <input checked="" type="checkbox"/>	10s <input checked="" type="checkbox"/>
■	Other	Backup and restore	Include <input checked="" type="checkbox"/>	No exceptions, and data available for backup and restore is no more than 72 hours <input checked="" type="checkbox"/>
■	Other	Email Alert Setting	Include <input checked="" type="checkbox"/>	Configured <input checked="" type="checkbox"/>
■	Other	Periodical Detection Setting	Include <input checked="" type="checkbox"/>	All configured <input checked="" type="checkbox"/>
■	Other	Topological Graph Alert Setting	Include <input checked="" type="checkbox"/>	All configured <input checked="" type="checkbox"/>
■	Other	Monitoring Panel Setting	Include <input checked="" type="checkbox"/>	All configured <input checked="" type="checkbox"/>
■	Other	Email Sender Setting	Include <input checked="" type="checkbox"/>	All configured <input checked="" type="checkbox"/>
■	Other	Audit Log Setting	Include <input checked="" type="checkbox"/>	All configured <input checked="" type="checkbox"/>

➤ Patrol categories of patrol objects are as follows:

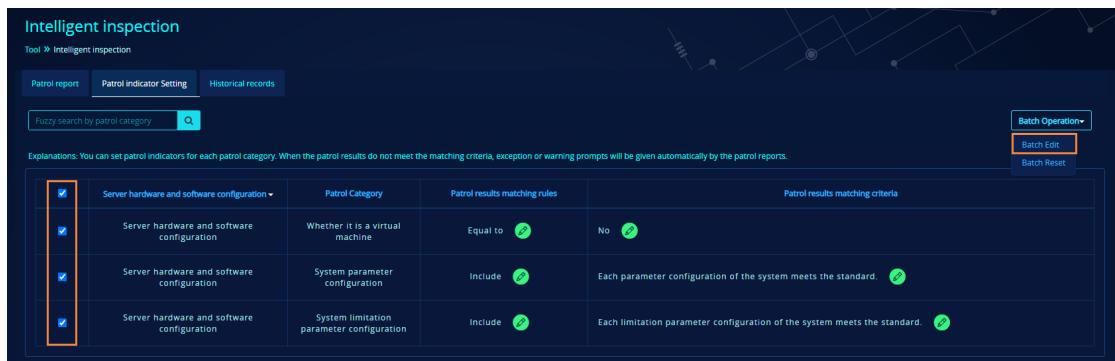
- Availability
- Master-slave replication status

- Master-slave replication latency
 - Backup and restore
 - Email alert setting
 - Periodical detection setting
 - Topological graph alert setting
 - Monitoring panel setting
 - Email sender setting
 - Audit log setting
 - Platform log
- Master/slave replication latency
- The default matching rule is “less than”, which can be edited as greater than, less than, greater than or equal to, less than or equal to, and no attention is required.
 - The default criteria is 10s, which can be edited as 0 or any positive integer value, unit: seconds.
- Availability and master-slave replication status
- The default matching rule is equal to, which can be edited are: equal to, not equal to, and no attention is required.
 - The default matching criteria of availability is available; the default matching criteria of the master-slave replication status is normal, and can be edited to any value.
- Others
- The default matching rule is “include”, which can be edited as: include, not include and no attention is required.
 - The matching criteria
 - 1) The default value of platform log is “no exceptions” and can be edited to any value.

- 2) The default value of notification strategy is “configured” and can be edited to any value.
- 3) The default value of backup and restore is "no exceptions, and the data available for backup and restore is no more than 72 hours". The matching criteria should be positive integers, unit: hours.
- 4) For all other patrol categories, the default value of the matching criteria is " all configured " and can be edited to any value.

1.2.2.9. Batch edit

(1) Start batch edit



	Server hardware and software configuration	Patrol Category	Patrol results matching rules	Patrol results matching criteria
<input checked="" type="checkbox"/>	Server hardware and software configuration	Whether it is a virtual machine	Equal to <input checked="" type="radio"/>	No <input checked="" type="radio"/>
<input checked="" type="checkbox"/>	Server hardware and software configuration	System parameter configuration	Include <input checked="" type="radio"/>	Each parameter configuration of the system meets the standard. <input checked="" type="radio"/>
<input checked="" type="checkbox"/>	Server hardware and software configuration	System limitation parameter configuration	Include <input checked="" type="radio"/>	Each limitation parameter configuration of the system meets the standard. <input checked="" type="radio"/>

- Check and click “Batch Operation” -> “Batch Edit”

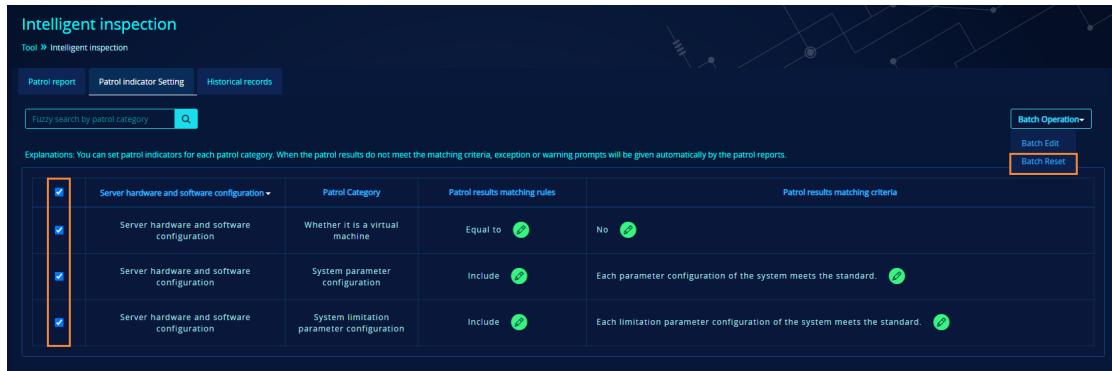
(2) Fill in batches and save



parameter name	Description of parameter	parameter value	The way to work
Server hardware and software configuration	Whether it is a virtual machine	Equal to	No
Server hardware and software configuration	System parameter configuration	Include	Each parameter configuration o
Server hardware and software configuration	System limitation parameter configuration	Include	Each limitation parameter config

- The corresponding matching rules and matching criteria of patrol categories display the default value, which can be edited.

1.2.2.10. Batch reset



The screenshot shows the 'Intelligent inspection' tool interface. At the top, there are tabs for 'Patrol report', 'Patrol indicator Setting' (which is selected), and 'Historical records'. Below the tabs is a search bar labeled 'Fuzzy search by patrol category' with a magnifying glass icon. To the right, there is a 'Batch Operation' dropdown menu with options 'Batch Edit' and 'Batch Reset'.

Below the search bar, a note says: 'Explanations: You can set patrol indicators for each patrol category. When the patrol results do not meet the matching criteria, exception or warning prompts will be given automatically by the patrol reports.'

The main area displays a table with four rows of patrol indicator settings:

Patrol Category	Patrol results matching rules	Patrol results matching criteria
Server hardware and software configuration	Equal to	No
System parameter configuration	Include	Each parameter configuration of the system meets the standard.
System limitation parameter configuration	Include	Each limitation parameter configuration of the system meets the standard.

- Check and click “Batch Operation” -> “Batch Reset”.
- After the reset, the matching rules and matching criteria will be reset to the system default value.

1.2.3. Historical records

1.2.3.1. Layout



The screenshot shows the 'Historical records' interface. On the left, there is a navigation sidebar with various tools and settings, and the 'Intelligent inspection' option is highlighted with an orange box. The main area has a title 'Intelligent inspection' and a subtitle 'Tool > Intelligent inspection'. It features three tabs: 'Patrol report', 'Patrol indicator Setting' (selected), and 'Historical records'.

Below the tabs, there is a table with columns: Patrol ID, Starting type, Patrol starting time, Patrol time consuming, Patrol scope, Task Status, Are there exceptions or warnings?, and Patrol indicator Setting. The table contains three rows of data:

Patrol ID	Starting type	Patrol starting time	Patrol time consuming	Patrol scope	Task Status	Are there exceptions or warnings?	Patrol indicator Setting
181	Automatic	2020-11-04 11:00:00	10s	Server hardware and software configuration,Server resource usage,Server hardware reliability	Patrol completed	Yes(42 exceptions,44 warnings)	
180	Manual	2020-11-03 18:42:17	2s	Server hardware and software configuration,Server resource usage,Server hardware reliability	Patrol Failure	No	
178	Manual	2020-11-03 18:40:50	5s	Server hardware and software configuration,Server resource usage,Server hardware reliability	Patrol completed	Yes(42 exceptions,44 warnings)	

At the bottom, there is a pagination bar with buttons for 'Prev', 'Next', 'Jump to', and 'Go'.

- Displays all historical patrol tasks.
- Click "patrol time consuming" to display in ascending or reverse order according to the patrol time consuming.
- The "starting type" includes manual and automatic. The automatic type refers to the periodical plan.

1.2.3.2. View the details

The screenshot shows the 'Intelligent inspection' interface. At the top, there are three tabs: 'Patrol report', 'Patrol indicator Setting', and 'Historical records'. The 'Historical records' tab is selected. Below the tabs is a table with columns: Patrol ID, Starting type, Patrol starting time, Patrol time consuming, Patrol scope, Task Status, Are there exceptions or warnings?, and Patrol Indicator Setting. Three rows of data are listed:

Patrol ID	Starting type	Patrol starting time	Patrol time consuming	Patrol scope	Task Status	Are there exceptions or warnings?	Patrol Indicator Setting
181	Automatic	2020-11-04 11:00:00	10s	Server hardware and software configuration,Server resource usage,Server hardware reliability	Patrol completed	Yes(42 exceptions,44 warnings)	
180	Manual	2020-11-03 18:42:17	2s	Server hardware and software configuration,Server resource usage,Server hardware reliability	Patrol Failure	No	
178	Manual	2020-11-03 18:40:50	5s	Server hardware and software configuration,Server resource usage,Server hardware reliability	Patrol completed	Yes(42 exceptions,44 warnings)	

At the bottom of the table, there are navigation buttons: 'Prev', '1', 'Next', 'Jump to', 'P', and 'GO'.

- Click “Operation - > [Details]” to enter the detail page.
- The page is basically consistent with the "patrol report" page.
- Click the "return" button to return to the "historical records" page.

The screenshot shows the 'Intelligent inspection' interface. At the top, there are three tabs: 'Patrol report', 'Patrol indicator Setting', and 'Historical records'. The 'Historical records' tab is selected. There are search and filter options at the top: 'Fuzzy search by host name' and 'Search by patrol status'. Below the tabs is a table with columns: Cluster name, Compute node mode, Multi-node Compute Node, Number of servers, Number of compute, Number of data nodes, Number of data source, Number of LogicDB, Number of tables, and Cluster starting time. One row of data is shown:

Cluster name	HotDB	Compute node mode	Multi-node Compute Node	Number of servers	7
Number of compute	3	Number of data nodes	12	Number of data source	12
Number of LogicDB	1	Number of tables	9	Cluster starting time	2020-10-26 14:33:25

Below this is a 'Detailed report' section with tabs: Server hardware and software configuration, Server resource usage, Server hardware reliability, Compute node running status and statistics, Data source running status and statistics, Data verification and detection, and Other. Under 'Server hardware and software configuration', there is a table with columns: Hostname, Patrol Category, Patrol results, Patrol status, and Recommended measures. Two rows of data are shown:

Hostname	Patrol Category	Patrol results	Patrol status	Recommended measures
	System distribution version	CentOS Linux release 7.5.1804 (Core)	Normal	
	System kernel version	Linux 203-MySQL 3.10.0-514.26.2.el7.x86_64 #1 SMP Tue Jul 4 15:04:05 UTC 2017 x86_64 GNU/Linux	Normal	

1.2.3.3. Delete the task

The screenshot shows the 'Intelligent inspection' interface. At the top, there are three tabs: 'Patrol report', 'Patrol indicator Setting', and 'Historical records'. The 'Historical records' tab is selected. Below the tabs is a table with columns: Patrol ID, Starting type, Patrol starting time, Patrol time consuming, Patrol scope, Task Status, Are there exceptions or warnings?, and Patrol Indicator Setting. Three rows of data are listed:

Patrol ID	Starting type	Patrol starting time	Patrol time consuming	Patrol scope	Task Status	Are there exceptions or warnings?	Patrol Indicator Setting
181	Automatic	2020-11-04 11:00:00	10s	Server hardware and software configuration,Server resource usage,Server hardware reliability	Patrol completed	Yes(42 exceptions,44 warnings)	
180	Manual	2020-11-03 18:42:17	2s	Server hardware and software configuration,Server resource usage,Server hardware reliability	Patrol Failure	No	
178	Manual	2020-11-03 18:40:50	5s	Server hardware and software configuration,Server resource usage,Server hardware reliability	Patrol completed	Yes(42 exceptions,44 warnings)	

At the bottom of the table, there are navigation buttons: 'Prev', '1', 'Next', 'Jump to', 'P', and 'GO'.

- Click “Operation - > [Delete]” to delete the patrol task.
- When the patrol task is deleted, the corresponding file and local patrol report will

be deleted too.

1.2.3.4. Download the report

Patrol ID	Starting type	Patrol starting time	Patrol time consuming	Patrol scope	Task Status	Are there exceptions or warnings?	Patrol Indicator Setting
181	Automatic	2020-11-04 11:00:00	10s	Server hardware and software configuration,Server resource usage,Server hardware reliability	Patrol completed	Yes(42 exceptions,44 warnings)	
180	Manual	2020-11-03 18:42:17	2s	Server hardware and software configuration,Server resource usage,Server hardware reliability	Patrol Failure	No	
178	Manual	2020-11-03 18:40:50	5s	Server hardware and software configuration,Server resource usage,Server hardware reliability	Patrol completed	Yes(42 exceptions,44 warnings)	

- Click “Operation - > [Download]” to download the patrol report.
- For the operations, you can refer to "patrol report" - > "export the complete report".

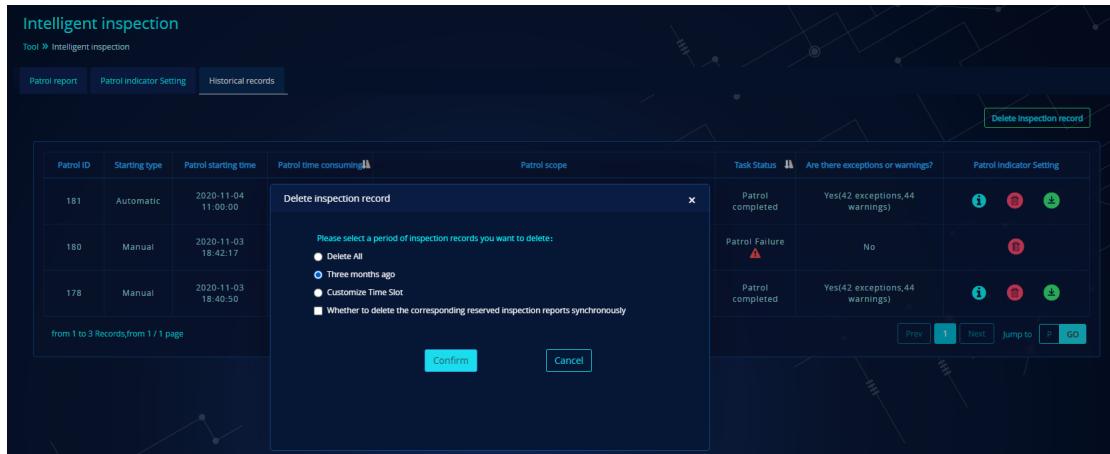
1.2.3.5. Batch deletion

(1) Start a batch deletion

Patrol ID	Starting type	Patrol starting time	Patrol time consuming	Patrol scope	Task Status	Are there exceptions or warnings?	Patrol Indicator Setting
181	Automatic	2020-11-04 11:00:00	10s	Server hardware and software configuration,Server resource usage,Server hardware reliability	Patrol completed	Yes(42 exceptions,44 warnings)	
180	Manual	2020-11-03 18:42:17	2s	Server hardware and software configuration,Server resource usage,Server hardware reliability	Patrol Failure	No	
178	Manual	2020-11-03 18:40:50	5s	Server hardware and software configuration,Server resource usage,Server hardware reliability	Patrol completed	Yes(42 exceptions,44 warnings)	

- Click “delete inspection record” on the page “Intelligent inspection → historical records”.

(2) Select a period of inspection records you want to delete



- "Three months ago" is selected by default. You can also select "delete all" or "customize time slot".
- If you check "whether to delete the corresponding reserved inspection reports synchronously", the files and patrol reports generated under the directory hotdb-management / data / Inspection will be deleted synchronously.
- Click Cancel, and the batch deletion operation will be cancelled.

1.2.4. Patrol details

1.2.4.1. Description of patrol matching logic

The matching is based on patrol results and patrol indicators:

1. When the matching rule is "include":
 - If the matching succeeds, the patrol status will be “normal”.
 - If the matching fails, the corresponding patrol status and recommended measures will be output for different patrol categories according to different patrol results.
2. When the matching rule is "not include":
 - If the patrol result matches the warning logic, the patrol status will be “warning”.
 - Otherwise, “normal” or “abnormal” will be output according to the matching results.
3. When matching rule is "equal to" or "not equal to":

- If the matching succeeds, the patrol status will be “normal”.
- If the matching fails, the corresponding patrol status and recommended measures will be the output.

4. When the matching rule is "greater than", "less than", "greater than or equal to", "less than or equal to":

- If the matching succeeds, the patrol status will be “normal”;
- If the matching fails, the corresponding patrol status and recommended measures will be the output.

5. When the matching rules is "no attention is required": the patrol status is normal and no recommended measures.

1.2.4.2. Description of patrol result logic

1.2.4.2.1. Server hardware and software configuration

Report generation time: 2020-11-04 11:00:00					
Basic information					
Cluster name	HotDB	Compute node mode	Multi-node Compute Node	Number of servers	7
Number of compute	3	Number of data nodes	12	Number of data source	12
Number of LogicDB	1	Number of tables	9	Cluster starting time	2020-10-26 14:33:25

Detailed report					
Server hardware and software configuration					
Hostname	Patrol Category	Patrol results	Patrol status	Recommended measures	
10.10.0.203	System distribution version	CentOS Linux release 7.5.1804 (Core)	Normal		
	System kernel version	Linux 203-MySQL 3.10.0-51.42.2.el7.x86_64 #1 SMP Tue Jul 4 15:04:05 UTC 2017 x86_64 x86_64 GNU/Linux	Normal		
	Whether it is a virtual machine	No	Normal		
	CPU model	Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.40GHz	Normal		
	CPU logical cores	56	Normal		
	Total memory capacity	251.803GB	Normal		
	Total disk capacity	sda: 278.875GB sdb: 3.636TB	Normal		
	Network card info	em1: Speed: 10000Mb/s Duplex: Full em4: Speed: 1000Mb/s Duplex: Full	Normal		
	System parameter configuration	There are 3 configured system parameter values inconsistent with the standard. Please manually confirm whether to modify the /etc/sysctl.conf configuration. You can download the file to view the details of inconsistent parameters.			Abnormal
	System limitation parameter configuration	Each limitation parameter configuration of the system meets the standard.			Abnormal

View the patrol report on “Historical records ->Detailed report ->Server hardware and software configuration”.

Whether it is a virtual machine

- Detect whether the server is a virtual machine. If it is a virtual machine, the patrol result will be "No".

System parameter configuration

- Compare the one-click deployment script parameters and the common parameter values from the sysctl-a command (the annotated parameters are not included).
- If parameters from the sysctl-a command do not exist, the parameters in the one-click deployment script will be compared with parameters in files under /etc/sysctl.conf; if parameters in files under /etc/sysctl.conf do not exist either, the comparison will not be carried out.
- You can view the inconsistent parameters by clicking the "Download" button in the patrol results.
- If the parameters are all consistent, you can view all parameters of sysctl-a by clicking the "Download" button in the patrol results.

System limitation parameter configuration

- Obtain configuration of the last three users, mysql, hotdb, and root, from /etc/security/limits.conf. Judgement: nofile < 10240(standard value), nproc< 262140 (standard value).
 - If it is less than the standard value, it will prompt in the patrol result that the parameters are inconsistent, and the inconsistent parameters will be listed.
 - If it is greater than or equal to the standard value, it will prompt in the patrol result that the parameters meet the standard.
 - If you have no privilege to view the file, it will prompt in the patrol result that the privilege is insufficient.

Note: items not mentioned above are only displayed and do not match the patrol indicators.

1.2.4.2.2. Server resource usage

Report generation time: 2020-11-09 11:02:29						
Basic information						
Cluster name	HotDB	Compute node mode	Multi-node Compute Node	Number of servers	7	
Number of compute	3	Number of data nodes	12	Number of data source	12	
Number of LogicDBs	1	Number of tables	11	Cluster starting time	2020-10-26 14:33:25	

Detailed report						
Server hardware and software configuration		Server resource usage	Server hardware reliability	Compute node running status and statistics	Data source running status and statistics	Data verification and detection
Hostname		Patrol Category		Patrol results		Recommended measures
CPU		Total CPU utilization		Average value 0.29%	Normal	
		sys divided by the current value of the ratio of utilization		Peak value 0.29%	Normal	
		wa divided by the current value of the ratio of utilization		Current value 43.75%(above the threshold)	Abnormal	The proportion of system in the used CPU resources is too high. Please check whether there are processes that consume excessive CPU resources of the system.
		LOAD		Current value 0.0%	Normal	
Memory		The ratio of LOAD divided by the logical core number		Current value load1mavg: 0.04 load5mavg: 0.15 load15mavg: 0.16	Normal	
		Memory error log		Current value load1mavg: 0.0 load5mavg: 0.0 load15mavg: 0.0	Normal	

View the patrol report on “Historical records ->Detailed report ->Server resource usage”.

- The current value of each patrol category: the real-time value of the corresponding monitoring script.
- The average value, maximum peak value and minimum peak value of each patrol category: the value within half an hour of the corresponding monitoring script.

1.2.4.2.3. Server hardware reliability

Report generation time: 2020-11-09 11:02:29						
Basic information						
Cluster name	HotDB	Compute node mode	Multi-node Compute Node	Number of servers	7	
Number of compute	3	Number of data nodes	12	Number of data source	12	
Number of LogicDBs	1	Number of tables	11	Cluster starting time	2020-10-26 14:33:25	

Detailed report						
Server hardware and software configuration		Server resource usage	Server hardware reliability	Compute node running status and statistics	Data source running status and statistics	Data verification and detection
Hostname		Patrol Category		Patrol results		Recommended measures
10.10.0.209		Hardware error log		No exception info	Normal	
		Memory error info.		No exception info	Normal	
		Hard disk device error message		Unable to detect because SMART is not enabled in /dev/nvme0-d nvme device.	Warning	Please manual intervention
		Hard disk array info		The result of executing the command /opt/MegaRAID/MegaCli/MegaCli64 -CfgDsply -aAll grep 'Er for Count' is empty	Warning	Please manual intervention
		Packet loss statistics of network card.		No exception info	Normal	
		Network quality statistics		No exception info	Normal	
		System event log info		The system event log info cannot be obtained because the ipmitool command cannot be executed. Please manually click the [Install] button to install the relevant software.	Warning	Please manual intervention
		Temperature voltage fan info		The system event log info cannot be obtained because the ipmitool command cannot be executed. Please manually click the [Install] button to install the relevant software.	Warning	Please manual intervention

View the patrol report on “Historical records ->Detailed report ->Server hardware reliability”.

reliability".

Hardware error log

- If mcelog is not installed, it will prompt in the patrol result that the software is not installed. You can directly install the software by clicking the "Install" button in the patrol result.
- If there is info output after executing "mcelog", it will prompt in the patrol result that "There is an error log. Please download the file to check the details".
- If there is no info output after executing "mcelog", it will prompt in the patrol result that "no abnormal info".
- If the server is a virtual machine, it will prompt in the patrol result that "No detection is required because the server is a virtual machine", with the patrol status being "no patrol is required".

Memory error info.

- If not all output is 0, the non-0 results will be displayed in the patrol result.
- If all output is 0, it will prompt in the patrol result that "no abnormal info".
- If you have no privilege to view the file, it will prompt in the patrol result that the privilege is insufficient.
- If the server is a virtual machine, it will prompt in the patrol result that "No detection is required because the server is a virtual machine", with the patrol status being "no patrol is required".

Hard disk device error info.

- If smartmontools is not installed, it will prompt in the patrol result that the software is not installed. You can directly install the software by clicking the "Install" button in the patrol result.
- If SMART is not enabled on the equipment, it will prompt in the patrol result that "Unable to detect because SMART is not enabled"
- If the output is empty after the command is executed, it will prompt in the patrol result that "The result is empty after executing command smartctl --scan".

- If SMART is supported in the server, check whether the SMART Health Status is OK or whether the self-assessment test result is PASSED. If it is not OK / PASSED, it will prompt in the patrol result that "Smartctl detected that the SMART of XXX device reported abnormal status. You can download the file to view the details".
- If all the detections above are passed, you need to judge whether the data in the last column of "Reallocated_Sector_Ct", "Reported_Uncorrect", and "Total new blocks reassigned" is 0; if not, it will prompt in the patrol result that "XXX is greater than 0. You can download the file to view the details, and manually intervene to determine whether there is an exception."
- If all the detections are passed, it will prompt in the patrol result that "no abnormal info."
- If the server is a virtual machine, it will prompt in the patrol result that "No detection is required because the server is a virtual machine", with the patrol status being "no patrol is required".

Hard disk array info.

- If MegaCli is not installed on the server when starting the patrol for the first time, it will be installed automatically during the patrol.
- If the return is empty after executing the command, it will prompt in the patrol result that "The result is empty after executing command /opt/MegaRAID/MegaCli/MegaCli64 -CfgDsply -aAll|grep 'Error Count' ".
- If not all output is 0, it will prompt in the patrol result that "MegaCli64 found an item with Error Count not 0. You can download the file to view the details".
- If all output is 0, it will prompt in the patrol result that "no abnormal info".
- If the server is a virtual machine, it will prompt in the patrol result that "No detection is required because the server is a virtual machine", with the patrol status being "no patrol is required".

Packet loss statistics of network card

- If there is no last patrol result, the patrol result will be "no abnormal info".

- If the difference between the data of this patrol result and the previous patrol result, such as errors, dropped and overrun are greater than or equal to 1000, then the patrol result will be "there is a record of more than 1000 times exceptional packet loss of network card from the last patrol to this patrol, you can download the file to view the details".
- If the difference is less than 1000, the patrol result will be "no abnormal info".
- If there are exceptions in the patrol process, the patrol result will be "unable to view the packet loss info of network card".

Statistics of network quality

- If there is no last patrol result, the patrol result will be "no abnormal info".
- If no ping packets are recorded from the last patrol to the present, the patrol result will be "no abnormal info".
- If ping packets are recorded from the last patrol to the present, the patrol result will be "during the process from the last patrol to this patrol, the total number of ping small packet timeout: 0, the number of ping large packet timeout: 0, the total number of packet loss: 0, the number of times of not exceeding the configuration threshold :10".
- The configuration threshold of indicators is editable.
- If the server is non-compute node server, the patrol category will not be displayed.
- When the compute node version is lower than 2.5.5, the patrol category will not be displayed.

System event log info

- If ipmitool is not installed, it will prompt in the patrol result that the software is not installed. You can directly install the software by clicking the "Install" button in the patrol result.
- Execute the command to view the Last Add Time in the record. If it is later than the last patrol, the patrol result will be "there is a new log generated from the last patrol, please download the file to view the details by clicking 'download'".

- If no new log is generated from the last patrol to the present, the patrol result will be "no abnormal info".
- If the server is a virtual machine, it will prompt in the patrol result that "No detection is required because the server is a virtual machine", with the patrol status being "no patrol is required".

Temperature and voltage fan info

- If ipmitool is not installed, it will prompt in the patrol result that the software is not installed. You can directly install the software by clicking the "Install" button in the patrol result.
- Execute the command. If there is an item in the last column that is not ok or ns, the patrol result will be "the following indicators do not meet the patrol requirements, please intervene manually and list the unqualified items".
- If items are all ok or ns, the patrol result will be "no abnormal info".
- If the server is a virtual machine, it will prompt in the patrol result that "No detection is required because the server is a virtual machine", with the patrol status being "no patrol is required".

1.2.4.2.4. Compute node running status and statistics

Report generation time : 2020-11-05 15:22:40					
Basic information					
Cluster name	256_three_report	Compute node mode	Multi-node Compute Node	Number of servers	11
Number of compute	3	Number of data nodes	6	Number of data source	10
Number of LogicDBs	3	Number of tables	1	Cluster starting time	2020-11-05 14:44:45

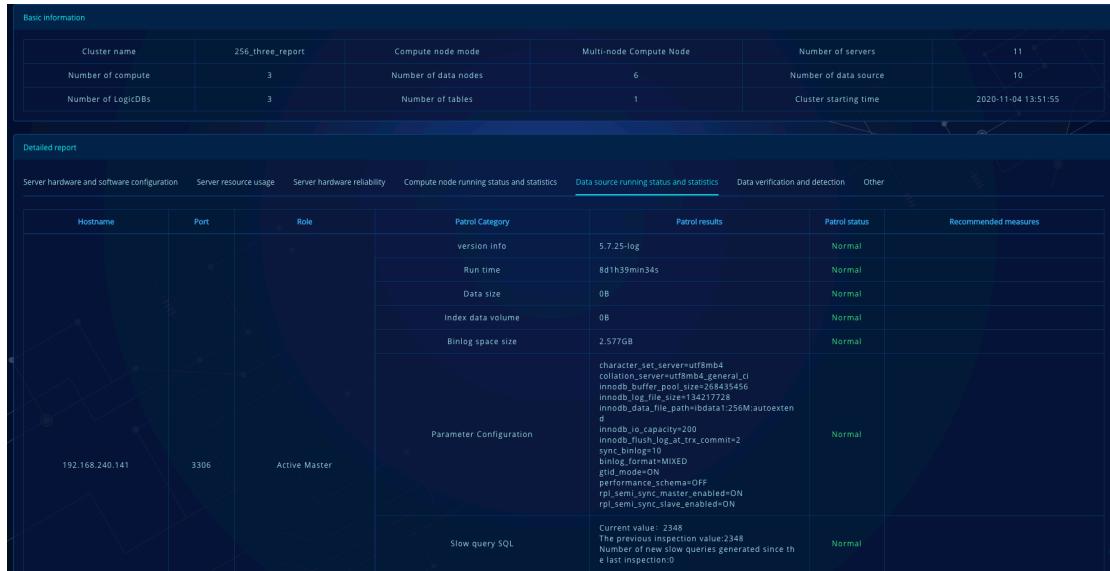
Detailed report						
Server hardware and software configuration	Server resource usage	Server hardware reliability	Compute node running status and statistics	Data source running status and statistics	Data verification and detection	Other
Note: some inspection categories in this project will count the statistical info after the last inspection, the last inspection time.: 2020-11-05 14:50:10						
Hostname	Patrol Category		Patrol results	Patrol status	Recommended measures	
	Heap memory	Configuration value	1024M	Normal		
		Current value	74M	Normal		
	Direct Memory	Configuration value	1024M	Normal		
		Current value	157M	Normal		
	Safety control	SQL Firewall	Off	Normal		
		IP whitelist	Off	Normal		
		Password Safety	No exceptions.	Abnormal	Please retry later	
	License info	The number of Beta version (55 days left, below the threshold) authorized nodes: 64.		Abnormal	Please retry later	
	version info	v2.5.6		Normal		
	Slow query SQL record	The inspection is not available temporarily because relevant parameters are not enabled.		Warning	Check whether the "statistics of SQL execution" is enabled in the parameter setting of the compute node.	

View the patrol report on “Historical records ->Detailed report ->Compute node running status and statistics”.

- **License info:** displays the remaining license authorization time and the number of authorized nodes according to the license authorization information.
- **Heap memory:**
 - Configuration value: obtain max_memory from show @@server
 - Current value: obtain used_memory from show @@server
- **Direct memory:**
 - Configuration value: obtain max_direct_memory from show @@server
 - Current value: obtain used_direct_memory from show @@server
- **QPS and TPS of throughput:**
 - Current value: consistent with the current value recorded in "Monitoring → Monitoring panel".
 - Peak value: consistent with the original data displayed on the admin index page.
 - Average value (within half an hour): the monitoring data within half an hour before the patrol start time is taken as the collection standard.
- **Total number of front-end connections and back-end connections:**
 - Current value: consistent with the data collected at "Monitoring → Logic topological graph".
 - Peak value: consistent with the original peak data of the compute node displayed on the admin index page.
 - Average value: the monitoring data within half an hour before the patrol start time is taken as the collection standard.
- **front-end inflow rate, front-end outflow rate, back-end inflow rate, back-end outflow rate, heap memory usage, and direct memory usage:**
 - Consistent with the data collected at "Monitoring → Logic topological graph".
- **Total data volume and cluster availability:** consistent with the original data displayed on the admin index page.

- **DR status:** whether the DR mode is configured in the current compute node; if it is, check whether the current "switching the active center" can be verified normally.
- **Cumulative failure time and switching times after the last patrol:** calculate the cumulative failure time, abnormal interruption time and abnormal switching times between the two patrols.
- **Password security management:** remind whether there is password expiration according to the password setting at "Setting → Periodical detection setting".
- **SQL firewall and IP whitelist:** consistent with the data of SQL firewall and IP whitelist displayed on the admin index page.
- **Slow query SQL record:** records the total number of slow query logs on "Events → Slow query log analysis" page.
- **Cumulative operation volume after the last patrol:** consistent with data on the compute node throughput page.
- **Statistics of compute node logs of ERROR level and WARN level after the last patrol:** the statistics of compute node logs of ERROR level and WARN level between the last patrol and the current Patrol (logs of multiple compute nodes shall be counted in the cluster mode).
- **Compute node GC statistics:** execute the command jstat -gc [pid] 1s 10 to obtain the result.

1.2.4.2.5. Data source running status and statistics



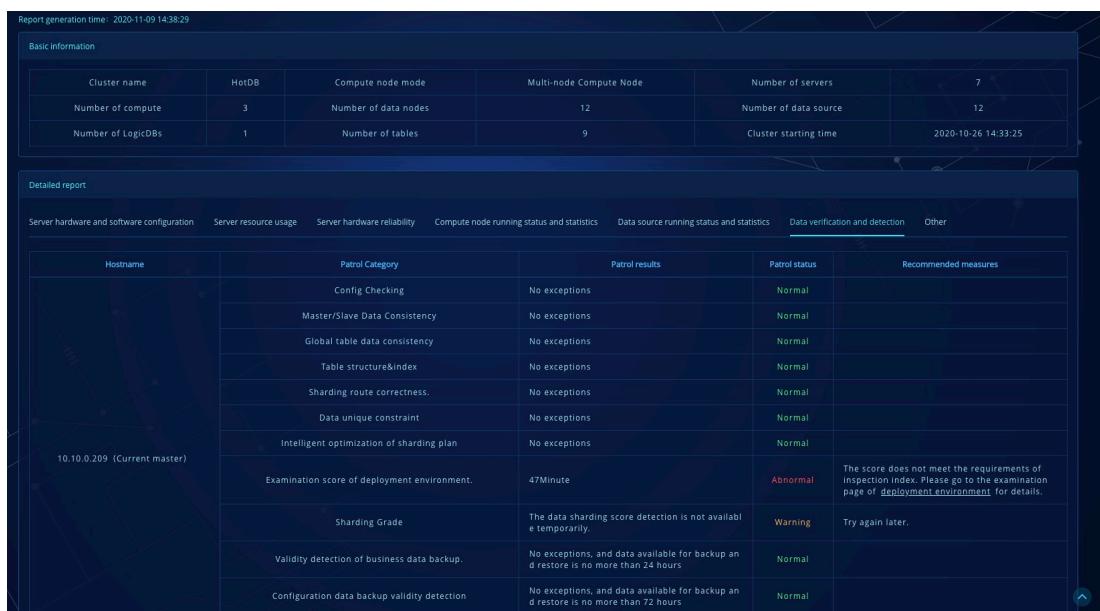
Basic information						
Cluster name	256_three_report	Compute node mode	Multi-node Compute Node	Number of servers	11	
Number of compute	3	Number of data nodes	6	Number of data-source	10	
Number of LogicDBs	3	Number of tables	1	Cluster starting time	2020-11-04 13:51:55	

Detailed report							
Server hardware and software configuration		Server resource usage		Server hardware reliability		Compute node running status and statistics	
Hostname	Port	Role	Patrol Category		Patrol results	Patrol status	
192.168.240.141	3306	Active Master	version info	5.7.25-log	Normal		
			Run time	8d1h39min34s	Normal		
			Data size	0B	Normal		
			Index data volume	0B	Normal		
			Binlog space size	2.577GB	Normal		
			Parameter Configuration		character_set_server=utf8mb4 collation_server=utf8mb4_general_ci innodb_file_per_table=ON innodb_log_file_size=134217728 innodb_data_file_path=ibdata1:256M:autoextende d innodb_lg_capacity=200 innodb_flush_log_at_trx_commit=2 sync_binlog=1 binlog_format=MIXED gtid_mode=ON partitioning_type=OFF rpl_semi_sync_master_enabled=ON rpl_semi_sync_slave_enabled=ON	Normal	
			Slow query SQL		Current value: 2348 The previous inspection value:2348 Number of new slow queries generated since th e last inspection:0	Normal	

- View the patrol report on “Historical records ->Detailed report ->Data source running status and statistics”.
- **Version info:** execute select version () under the corresponding instance port of the data source.
- **Run time:** execute show global status like 'uptime' under the corresponding instance port of the data source, format: year, month, day, hour, minute, second.
- **QPS, connections and replication latency:** consistent with the current value recorded in "Monitoring → Logic topological graph".
- **Data size:** the total amount of data corresponding to each data source instance.
- **Index data volume:** the total index amount corresponding to each data source instance.
- **Binlog space size:** statistics of the "show binary logs;" of all data source MySQL instances in the current cluster. It is the total size of the current file that is counted.
- **Parameter configuration:** use show variables to view the parameter configuration.
- **Slow query SQL:** use show global status like 'Slow_ queries' to view the current value of slow query SQL, and use "show global status like 'uptime';" to view the start time of MySQL data source.

- **Deadlock info:** execute "show engine Innodb status \G;" under the corresponding data source instance to check whether there is deadlock info.
- **Error log:** you can view the storage location of error.log via show variables like 'log_error'; and check whether the latest log time is between the last patrol and this patrol.
- **Data increment prediction:** displays the data volume of data sources within one year before the patrol time, and the compare the predicted data volume with the remaining free disk space (if the data recorded currently is less than 21 days, it will be given that "the data recorded currently is less than 21 days, so the increment prediction is temporarily unavailable.")

1.2.4.2.6. Data verification and detection



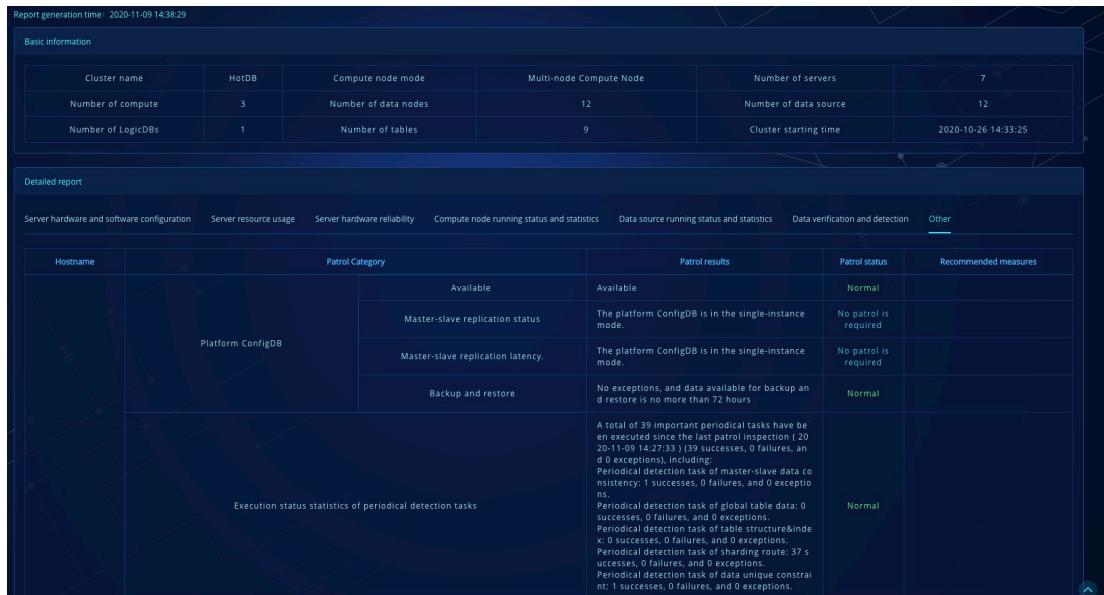
The screenshot shows the HotDB Intelligent Inspection interface. At the top, it displays basic cluster information: Cluster name (HotDB), Compute node mode (Multi-node Compute Node), Number of servers (7), Number of data nodes (12), Number of data source (12), Number of LogicDBs (1), Number of tables (9), and Cluster starting time (2020-10-26 14:33:25). Below this is a detailed report section titled 'Detailed report' which includes tabs for Server hardware and software configuration, Server resource usage, Server hardware reliability, Compute node running status and statistics, Data source running status and statistics, Data verification and detection, and Other. The 'Data verification and detection' tab is active, showing a table of patrol results for the current master node (10.10.0.209). The table columns include Hostname, Patrol Category, Patrol results, Patrol status, and Recommended measures. Patrol categories listed include Config Checking, Master/Slave Data Consistency, Global table data consistency, Table structure&index, Sharding route correctness, Data unique constraint, Intelligent optimization of sharding plan, Examination score of deployment environment, Sharding Grade, Validity detection of business data backup, and Configuration data backup validity detection. The 'Examination score of deployment environment' row shows an abnormal status with a note: 'The score does not meet the requirements of inspection index. Please go to the examination page of deployment environment for details.'

- View the patrol report on “Historical records ->Detailed report ->Data verification and detection”.
- **Config checking:** obtain the current result of "Configuration → Config checking→ Start checking"
- **Master/slave data consistency:**
 - A full data verification based on all LogicDBs (ConfigDBs are included).
- **Global table data consistency, table structure& index detection, sharding route correctness:**

- A full data verification based on all LogicDBs.
- **Data unique constraint and intelligent optimization of sharding plan:**
- A full data verification based on all the current LogicDBs. Each logicDB is marked with one verification record.
- **Examination score of deployment environment:**
- When the patrol starts, the examination score of deployment environment starts synchronously. You can view the examination progress details of the current deployment environment on the "Cluster management → Deployment environment examination" page.
 - Among all patrol objects, the longest time spent in the whole patrol process is "data verification and detection", while the longest time spent in the "data verification and detection" is the "deployment environment examination".
 - Whether the current cluster environment uses the physical machine or the virtual machine also directly affects the length of the physical examination (according to the current test situation, it takes about 18 minutes for a set of cluster environment with all virtual machines to conduct a patrol inspection of all patrol objects, while the time for a set of cluster environment with all physical machines for the same situation is less than 2 minutes Right).
 - Whether physical machine or virtual machine is used in the current cluster environment also directly affects the length of the examination (according to the current test, it takes about 18 minutes for a set of cluster environment with all virtual machines to conduct a patrol inspection of all patrol objects, while the time for a set of cluster environment with all physical machines for the same situation is about 2 minutes).
 - The patrol time is also affected by the number of components. The more components, the longer the time spent.
- **Sharding grade:** view the details on the "Detection → Sharding grade" page.
- **Validity detection of business data backup:** data backup with all LogicDBs as a unit. You can view the details on "Management > Data backup" page.

- **Validity detection of configuration data backup:** it is the ConfigDBs and configuration files of the current compute node that are backed up. You can view the backup details on the "Configuration > Cluster data backup & restore" page.
- **Configuration consistency check in memory:** check whether the current configuration in memory is consistent with the configuration marked in the running table of the configuration library
- **Consistency detection of the configuration in memory:** detect whether the configuration in current memory is consistent with the configuration marked in the running table of the ConfigDB.

1.2.4.2.7. Others



The screenshot shows a patrol report generated on 2020-11-09 14:38:29. It includes a 'Basic information' section with cluster details like name, number of compute nodes, and servers, and a 'Detailed report' section with tabs for various monitoring categories. The 'Other' tab is selected, showing patrol results for the Platform ConfigDB. The results table has columns for Hostname, Patrol Category, Patrol results, Patrol status, and Recommended measures. The 'Available' row indicates the platform ConfigDB is in single-instance mode. The 'Master-slave replication latency' row also shows it's in single-instance mode. The 'Backup and restore' row indicates no exceptions and data available for backup and restore within 72 hours. The 'Execution status statistics of periodical detection tasks' row provides detailed statistics for various detection tasks, all marked as 'Normal'.

Basic information					
Cluster name	HotDB	Compute node mode	Multi-node Compute Node	Number of servers	7
Number of compute	3	Number of data nodes	12	Number of data source	12
Number of LogicDBs	1	Number of tables	9	Cluster starting time	2020-10-26 14:33:25

Detailed report					
Server hardware and software configuration Server resource usage Server hardware reliability Compute node running status and statistics Data source running status and statistics Data verification and detection Other					
Hostname	Patrol Category	Patrol results	Patrol status	Recommended measures	
Platform ConfigDB	Available	Available	Normal		
	Master-slave replication status	The platform ConfigDB is in the single-instance mode.	No patrol is required		
	Master-slave replication latency	The platform ConfigDB is in the single-instance mode.	No patrol is required		
	Backup and restore	No exceptions, and data available for backup and restore is no more than 72 hours	Normal		
Execution status statistics of periodical detection tasks A total of 39 important periodical tasks have been executed in the current patrol inspection (20 success, 16 failure, 142733) (39 successes, 0 failures, and 0 exceptions), including: Periodical detection task of master-slave data consistency: 1 successes, 0 failures, and 0 exceptions. Periodical detection task of global table data: 0 successes, 0 failures, and 0 exceptions. Periodical detection task of table structure/index: 0 successes, 0 failures, and 0 exceptions. Periodical detection task of sharding route: 37 successes, 0 failures, and 0 exceptions. Periodical detection task of data unique constraint: 1 successes, 0 failures, and 0 exceptions.					

View the patrol report on “Historical records ->Detailed report ->Others”.

- **Platform ConfigDB:** log in to the manager role and enter the "Tool> Platform configuration data management" page.
 - **Availability status:** check whether the connection of ConfigDBs of the management platform is normal.
 - **Master-slave replication status and master-slave replication latency:** the master-slave replication status and replication latency between the ConfigDBs when the management platform ConfigDB is in master-slave or master-master mode.

- **Backup and restore:** it is the ConfigDBs and configuration files of the current management platform that are backed up.
- When the ConfigDB of management platform is in the single-instance mode, the availability in the patrol result will be displayed as available. It will prompt that "the platform configDB is in the single-instance mode" in the patrol results of master-slave replication status and master-slave replication latency.

➤ **Platform notification statistics**

- **Events:** statistics of the total number of event notification messages reported from the last patrol to this patrol by the management platform.
- **Email reminder:** statistics of the total number of email reminders from the last patrol to this patrol sent by the management platform.
- **Execution status statistics of periodical detection tasks:** summarize and display the periodical tasks of various detection types executed by the management platform, including the execution status of all periodical detection plans on the page of "Setting → Periodical detection setting" and the relevant submenu under the "detection" menu.
- **Audit log statistics:** statistics of the number of audit logs from the last inspection to the current inspection, including platform operation, security protection and management port operation.
- **Notification strategy, periodical detection setting, topological graph alert setting, monitoring panel setting, email sender setting and audit log setting:** set the notification strategy on the "Event → Email alert setting" page, and set other items in the "Setting" menu.
- **Platform log:** manually view hotdb-management.log and check whether there is a WARN or ERROR level platform log between the last patrol and the current patrol.
- **GC statistics:** execute the command jstat -gc [pid] 1s 10 to obtain the result. (pid is the process ID of the management platform).