

Tibero Monitoring

release date. 2026. 09. 11.

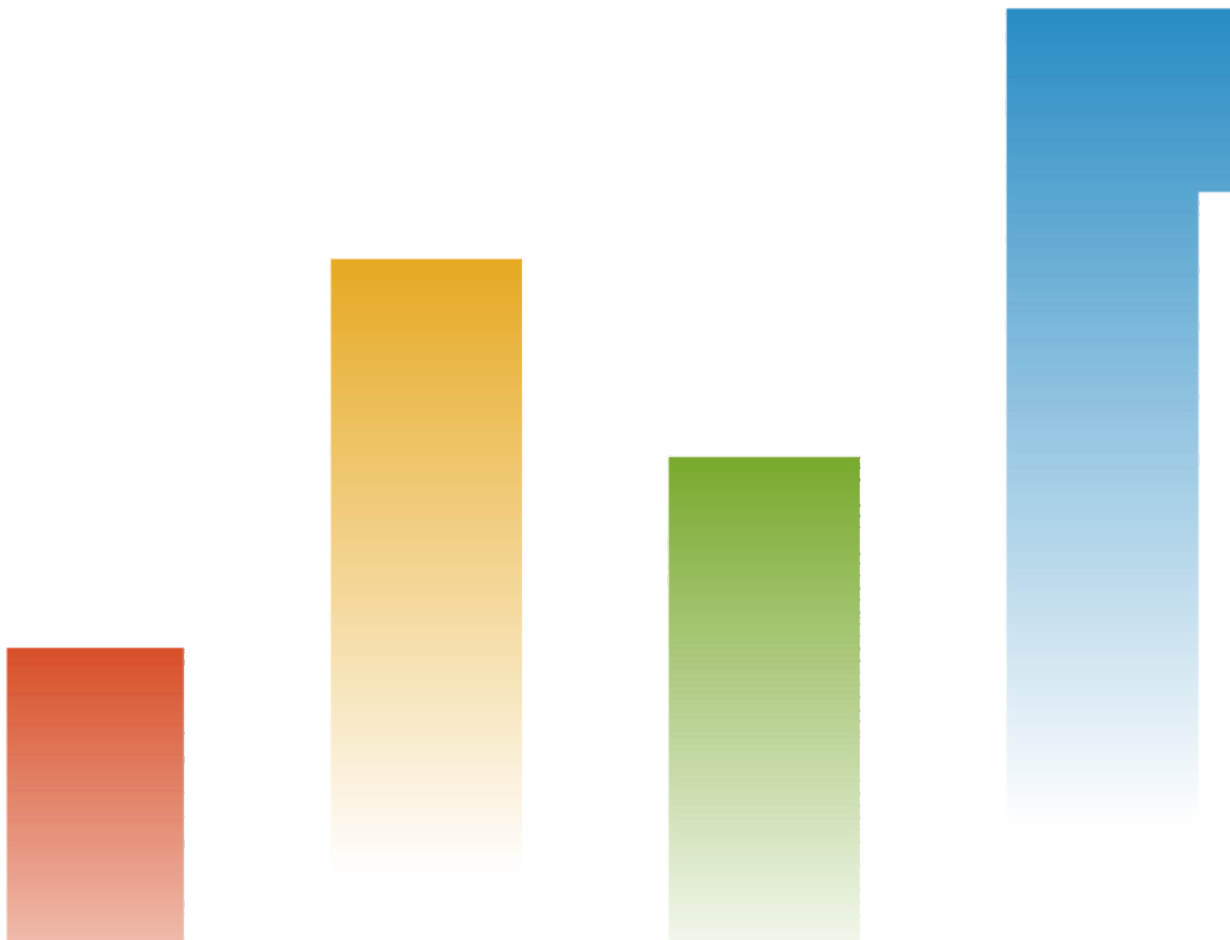


Table Of Contents

• Tiberio Monitoring	4
◦ Getting started.....	6
◦ Supported Environment.....	8
◦ Installation	
■ Agent Installation.....	15
■ Installation checking items	25
■ Troubleshooting	27
◦ Configuration	29
■ DBX Agent Setting.....	31
■ XOS agent configuration	37
◦ Management.....	42
◦ Dashboard	46
■ Instance List.....	48
■ Monitoring a Database Instance.....	50
■ Monitoring Multiple Instances	64
■ Flex Board	77
■ Using Flex board	80
■ Managing the widgets	90
◦ Analysis	
■ Count trend and comparison	95
■ Lock tree.....	106
■ Parallel query tree.....	112
■ Database Parameter	115
◦ Metrics.....	117

■ Tiberio metrics.....	119
■ Metrics Chart	127
■ Metrics Search	130
■ Metric Anomaly Detection	132
■ Metrics Trend Analysis.....	135
◦ Stat/Report	
■ SQL Statistics.....	138
■ Tablespace Size.....	143
■ SGA size	150
■ Report.....	154
◦ Alert	157
■ Event Configuration	0
■ Metrics	164
■ Composite Metrics.....	186
■ Anomaly Detection	193
■ Real-time logs	197
■ Composite log	210
■ Event Configuration	224
■ Event Notification Settings.....	228
■ Event Notification Format.....	250
■ Event History and Monitoring	258
■ Real-time Notifications.....	266
■ System Events	269
◦ Laboratory	272
■ OpenMetrics Explorer.....	273

Tibero Monitoring

The DB performance management monitors the database performance in real time, diagnoses and analyzes problems, tunes problematic SQLs, and monitors whether problems have been resolved.

The WhaTap database monitoring service is designed to manage a series of operations in cycles. It is configured to help maintain consistent levels of availability and performance by monitoring, diagnosing, and analyzing the database behaviors. When a problem occurs in the database, this service sends an alarm to the staff to recognize the situation and helps you identify the root cause by analyzing the database situation more precisely through the collected data.

! For more information about the supported features for each database platform, see [the following](#).

Features

- **Realtime DB Monitoring**

It collects real-time DB performance metrics and the data of running clients (active sessions). You can check the operation status at a glance to immediately recognize the load occurrence status, and you can immediately recognize any problems through alarm settings.

- **Specific point analysis**

By using the metrics' short-term trends, long-term trends, and metric comparison functions, you can analyze problems at the past. The database parameter change history is traced.

- **Efficient structure even on a large scale**

Even when managing multiple DB servers, it provides an optimal analysis environment through unified performance data collection and efficient data storage structure.

- **Cloud DB monitoring available**

Structure for query-based monitoring data collection does not depend on the DB server type. DBs in AWS, GCP, Azure, and OCI environments can also be monitored, and monitoring for cloud resource metrics and integrated items is also possible.

- **Integrated Monitoring**

If you have installed all applications, servers, and database monitoring products, you can quickly analyze the causes of failures through linked views when detecting service problems.

- **WhaTap SaaS**

You can select from various database products, and freely set the period of use by monthly subscription.
(available also with an installation type)

Getting Started

WhaTap monitoring starts with the following steps:

[Step 1. Sign up](#)

[Step 2. Select a product](#)

[Step 3. Create a project](#)

[Step 4. Check the access key](#)

After confirming the supported environment, proceed to the agent installation step.

Sign up

To use the WhaTap monitoring service, you must first [sign up](#). For more information about signing up, see the [Account Management > Sign Up](#) documentation.

Select a product

1. Log in to the [WhaTap Monitoring Service](#).
2. Select  **All Projects** > **+ Project**.
3. On the **Select product** screen, select the Go product to monitor and then click the Create button.

Create a project

After selecting the product to monitor, create a project before installing the agent.

1. On the **Create project** screen, enter or select the following items to create a project:
 - **Project name** (required): Enter the project name.
 - **Data server region** (required): Select the region where the data server is located. A region is a collection of data centers that provide cloud services. Your data is stored in the selected region.

- **Time zone** (required): Set the time zone that serves as the reference for generating alerts and reports.
- **Notification language setting** (required): Set the language for alert notification messages generated in the project (supports Korean and English).
- **Project groups**: You can group and manage multiple projects. Select a group if there is one to join.
- **Project description**: Enter an additional description for the project.

2. After completing all settings, click the **Creating a project** button.

ⓘ When adding a project with an organization selected, you must set the **Groups of organization** as required. For more information about groups, see [the following documentation](#).

Check the access key

The **access key** is a unique ID for activating the WhaTap service.

In the installation guide section, select the **Getting the access key** button. After automatically issuing the **access key**, proceed to the next step.

ⓘ After creating a project, you are automatically redirected to the **Agent installation** page. If you are not redirected to the **Agent installation** page, select **Management > Agent installation** from the left menu.

Support Environment

Before starting the Tiberio monitoring, check the following support environment.

Supported versions for the database

It supports Tiberio 5.x or later.

- ! The server to install the agent on must have Java 8 or later installed.
- The database server must allow inbound connections so that the DBX agent can access the DB port.
- It is required to open the outbound on the port 6600 so that the DBX agent can send data to the WhaTap server.

Agent minimum installation specifications

- CPU:** Approximately 20 agents can be installed per core (may differ depending on the DB server load).
- Memory:** 200 MB
- Disk:** 100 MB (Agent space of 50 MB + Log file generation space of 50 MB)

! Minimum installation requirements based on the number of agents

Number of installed agents	CPU	Memory	Disk
10	1-core	2 GB	1 GB
20	1-core	4 GB	2 GB
40	2-core	8 GB	4 GB

Agent operation method

The DB agent basically operates in the following way:

- **Execution cycle:** 5 secs (default)
- **Number of queries performed:** 5 to 6
- **Speed:** It terminates within 1 second when the server load is normal.
- Up to 2 sessions (5-second collection session, other information collection session)

When a timeout occurs during collection query, the DB agent operates in the following way to minimize the load.

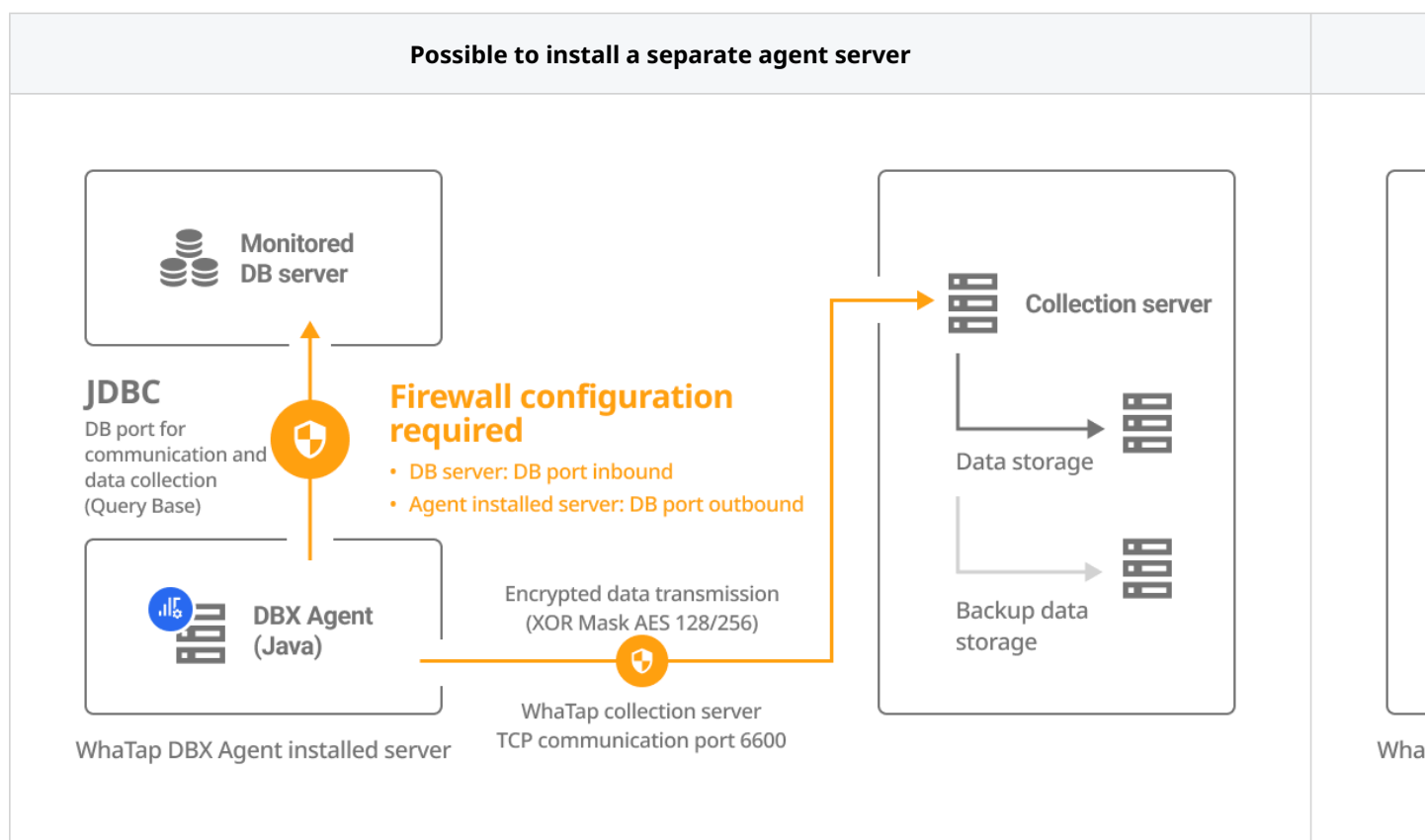
- Do not run a new collection query until the previous collection query has finished.
- If the timeout exceeds 12 seconds (exceeds 2 refresh cycles), the session is reconnected after termination.
- If timeout occurs 3 times or more, wait 10 seconds and try again.

ⓘ Depending on the load status of the DB server, it may take a long time or a timeout may occur until the result of a collection query appears on the WhaTap monitoring service screen.

Agent structure

The WhaTap database monitoring service consists of an agent and a collection server, and the data is encrypted for security between the agent and the collection server. It is made without an external library so there is no need to restart the system for installation and update.

- WhaTap database monitoring service can perform monitoring on a separate agent server without installing an agent on the database server. Monitoring can be applied flexibly according to the user environment.



- The XOS agent is an optional add-on agent that can monitor the process usage of the database server. To monitor the process usage of the database server, run a separate agent on the database server to collect data.
- The agent and server use the binary communication protocol. In addition, data is selectively encrypted to ensure data security while reducing the burden of encryption.

- ⓘ • The WhaTap agent must be installed on a server that can communicate over the network with the database server to be monitored.
- **JDK of Java 8** or later must be installed on the WhaTap DBX agent server.

Service deployment models

You can use WhaTap Monitoring as a SaaS or on-premises (self-hosted) service. Whichever you choose, you use the same agents and the same monitoring features.

Deployment	Support	Description
SaaS		Connects to collection servers operated by WhaTap. See the firewall section for regional addresses
On-premises (self-hosted)		Collection servers you build and operate yourself (air-gapped environments supported). Contact your sales representative for the scope

ⓘ You can also deploy WhaTap on-premises in air-gapped environments without internet connectivity.

Feature differences by deployment model

Whichever you choose, the monitoring features are the same. The mobile app is the only exception and is available on the service.whatap.io SaaS service only.

ⓘ To use certain features on-premises, a separate agreement is required.

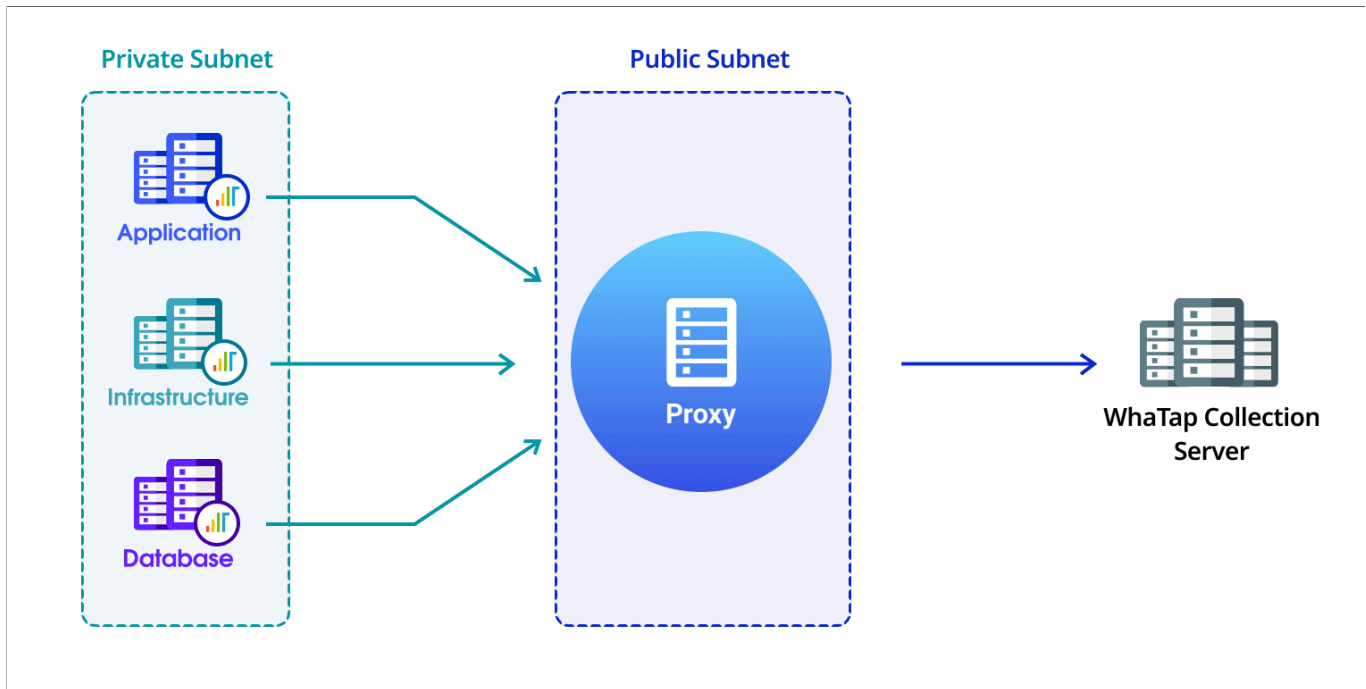
Firewall

The WhaTap agent must be able to access the collection server through **TCP port 6600**. Allow access to the collection server address that is closest to the monitored target.

Source: WhaTap agent

Cloud	Destination	Destination IP	Port
AWS	WhaTap collection server (Seoul)	13.124.11.223 / 13.209.172.35	TCP 6600
	WhaTap collection server (Tokyo)	52.68.36.166 / 52.193.60.176	TCP 6600
	WhaTap collection server (Singapore)	18.138.0.93 / 18.139.67.236	TCP 6600
	WhaTap collection server (Jakarta)	108.136.91.69 / 108.137.158.44	TCP 6600
	WhaTap collection server (Thailand)	43.209.109.219 / 43.209.48.86	TCP 6600
	WhaTap collection server (Mumbai)	13.127.125.69 / 13.235.15.118	TCP 6600
	WhaTap collection server (California)	52.8.223.130 / 52.8.239.99	TCP 6600
	WhaTap collection server (Virginia)	107.23.220.101 / 54.236.221.105	TCP 6600
	WhaTap collection server (Frankfurt)	3.125.142.162 / 3.127.76.140	TCP 6600
Azure	WhaTap collection server (Seoul)	52.231.66.38 / 20.194.5.115	TCP 6600
	WhaTap collection server (Tokyo)	52.246.169.54 / 20.210.27.232	TCP 6600
Kakao	WhaTap collection server (Seoul)	61.109.237.237 / 61.109.238.166	TCP 6600

If the agent cannot directly access the collection server, use the provided proxy module to access it.



Supporting the browser

WhaTap Monitoring is available in web browsers and mobile Apps.

Browser	Recommended	Supported version
Google Chrome	O	111 or later
Mozilla FireFox	X	Latest version
Edge	X	Latest version
Safari	X	Latest version

! Support guidance

- For browser compatibility and performance reasons, the latest version of Chrome is recommended.
- The user interface (UI) is implemented using HTML5 standard technologies, so Internet Explorer is



not supported.

Limitations

WhaTap's web interface does not support mobile browsers. To access WhaTap on a mobile device, install the WhaTap app for Android or iOS. The WhaTap mobile app is optimized for mobile environments. For more information about the WhaTap mobile app, see [this document](#).

Mobile app

The WhaTap mobile app supports both Android and iOS environments. You can install the WhaTap app by following the link or scanning the QR code. For detailed information about the mobile app, see [the following](#).

iOS	Android
 iOS 12 or later	 Android 5.0 or later

Agent Installation

The following guides you to the basic installation method for using the WhaTap database monitoring service.

Checking the project access key

Project access key is the unique ID for activating the WhaTap services.

In the installation guide section, select **Getting the access key**. After automatic reception of **project access key**, proceed to the next step.

- ✓ After a project has been created, the **Agent installation** page appears automatically. If the **Agent installation** does not appear, select **All projects** on the left and then select a newly created project.

Downloading the WhaTap database agent

1. Download the agent file. Use the following two methods.
 - On the WhaTap monitoring service screen, select [Download](#) for downloading.
 - You can download with the Linux wget method. Use the following command.

```
wget -O whatap.agent.database.tar.gz "https://service.whatap.io/download/dbx_agent?type=tibero&format=tar.gz"
```

- ⓘ For those who cannot download tar files due to security settings, ZIP files are also provided. On the installation screen, select the **.zip Download** button.

2. Copy the downloaded file to the server to be analyzed, and then unzip it. (Same for Windows and Linux)

Agent configuration file





File name	Description
<code>whatap.conf</code>	This is the file where you can enter the address of the collection server that collects data from the database server and the server's project access key. For more information about the agent configuration, see the following .
<code>alert/alert.conf</code>	This is the file that sets thresholds for monitoring items to be collected. An alert occurs when the threshold is exceeded.
<code>scripts/</code>	This directory contains the scripts that can remotely run SQL scripts.
<code>ps.sh</code>	This script fetches the process ID. When ending the agent process, the ID is referenced.
<code>stop.sh</code>	This script is used when ending the agent process.
<code>uid.sh (uid.bat)</code>	This shell script file generates an encrypted UID by combining the database connection data. It creates the <code>db.user</code> file. Once you have set it for the first time, it collects data from the database server to be monitored through the encrypted UID. For more details about creation of an account for monitoring, see the following .
<code>start.sh (start.bat)</code>	This shell script file runs the agent. When the agent starts, it starts collecting monitoring data from the database server.
<code>startd.sh (startd.bat)</code>	This shell script file runs the agent, which can be run in the background.
<code>whatap.agent.dbx-X.Y.Z.jar</code>	The Tracer program is a program that collects data from the database server and transmits the collected data to the

File name	Description
	server.
jdbc	This directory collects the libraries referenced for database server connection. Download the library for connecting the agent and database server and use it by setting the path in the class path option of Java.
xos/	The directory contains the optional agent that can monitor the process usage of the database server.
└ xos.conf	This file is used to enter the address and communication port of the agent server for collecting the process usage of the database server and transmitting the data.
* xcub/	This directory contains additional agent files that collect SQL texts from the CUBRID database and calculate metrics.
└ * xcub.conf	This file is used to enter the CUBRID database and additional agent connection settings.

ⓘ *: The files in the xcub path are dedicated files for CUBRID Monitoring.

- Enter the unzipped folder and then check the `whatap.conf` file. In `whatap.conf`, enter the project access key, WhaTap server data, and DB connection data.

whatap.conf

```
license=Project access key
whatap.server.host=13.124.11.223/13.209.172.35 // WhaTap server information

dbms=tibero
```

```
db=Database name (sid)
db_ip=Database IP
db_port=Database port
```

- Download the JDBC driver to the following directory. `/unzipped folder/jdbc`

Download the JDBC driver for the OS and version of your database server.

Tibero JDBC Drivers: `{ $TB_HOME } /client/lib/jar/tibero {Version} -jdbc.jar`

! In `/unzipped folder/jdbc/README.md`, you can also see the JDBC driver installation paths for each database.

Account creation

Create an account with roles required for database monitoring. Log in with the root account and then create accounts.

- !
- To use the previous accounts, go to [Create DB User File](#). If you do not have any permission, you may not be able to proceed with normal monitoring.
 - In the example code, `whatap` is the DB user account name. Change it to your account name.
 - Enter your password in `DB_Password` in the example code.

```
1 create user whatap identified by 'DB_PASSWORD'; ## Enter the desired password.
2 grant create session to whatap;
3 grant select any dictionary to whatap;
4
5 ## When using the kill session
6 grant alter system to whatap;
```

DB user file creation

Generate an encrypted UID for database connection. Enter the username and password and then run the shell script (or batch file).

The `uid.sh` shell script file (or `uid.bat` batch file) can be found in the path where the WhaTap database agent has been installed. Set `DB_USER` to `default` if there is only a password without user.

• Linux Windows

```
./uid.sh DB_USER DB_PASSWORD
```

- After setting it once, it collects data from the database server to be monitored through the encrypted UID.
- To create a DB user file, enter the project access key in the `whatap.conf` file. [Checking the project access key](#)
- In the Azure database environment, enter `DB_USER` in the form of `DB_USER@DB_name`.
- If special characters are included in `DB_USER` or `DB_PASSWORD`, enter the escape character (`\`) together before any special characters.

Example

```
./uid.sh whatap whatap\!pwd
```

If there are multiple special characters, add the escape character(\) for each.

```
./uid.sh whatap whatap\!\@pwd
```

```
uid.bat "DB_USER" "DB_PASSWORD"
```

- After setting it once, it collects data from the database server to be monitored through the encrypted UID.
- To create a DB user file, enter the project access key in the `whatap.conf` file. [Checking the project](#)

! access key

- In the Azure database environment, enter `DB_USER` in the form of `DB_USER@DB_name`.
- In the Windows environment, escape characters are not needed for special characters in passwords. However, if quotation marks (`"`) are used in the password, escape characters are required.

Viewing the default plan

When creating the **default plan user file**, you can configure the agent to automatically view the plan by using the predefined DB information.

• Linux Windows

1. Add the `plan_db` option to the agent configuration ([whatap.conf](#)) file and then enter the DB name.

whatap.conf

```
plan_db=(dbname)
```

2. After configuring the DB, use the `planuid.sh` script to set the user and password.

```
./planuid.sh user pwd
```

! If the user (`user`) and password (`pwd`) include special characters, add backslashes (`\`) before each special character.

e.g. `user$example` → `user\$example`

1. Add the `plan_db` option to the agent configuration ([whatap.conf](#)) file and then enter the DB name.

whatap.conf

```
plan_db=(dbname)
```

2. After configuring the DB, use the `planuid.bat` script to set the user and password.

```
planuid.bat user pwd
```

Starting the monitoring

Execute a shell script (or batch file) from the path where you have installed the agent.

- [Linux](#) [Windows](#)

```
./start.sh
```

To use it like a daemon, execute the following command. However, it works only in the environment where **nohup** has been installed.

```
./startd.sh
```

```
start.bat
```

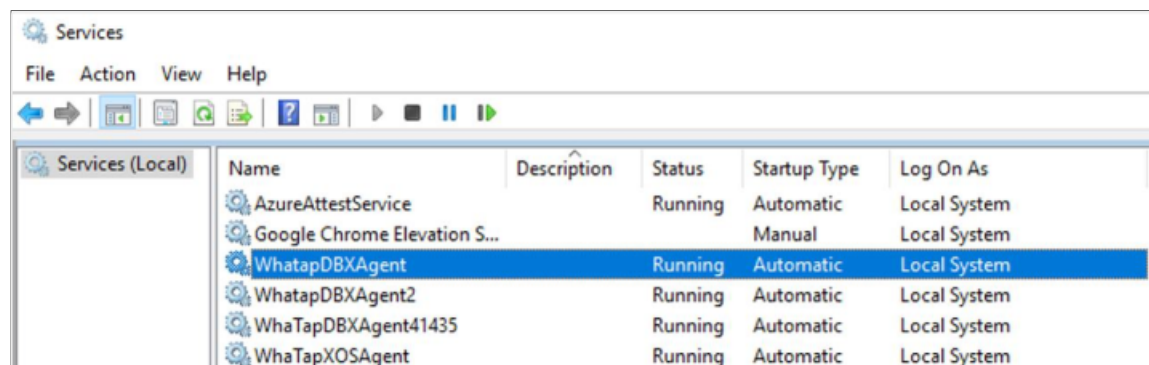
Check whether there are any errors in the execution log displayed on the screen, and check whether a chart appears normally on the dashboard screen (**Instance List**). If there is no problem, press Ctrl+C to terminate the execution, and then register it as a Windows service in the following order.

Registering a service

Execute the following command to register a service.

```
install_WindowsService.bat create WhatapDBXAgent
```

When a service is registered, you can check it in the service management tools as shown below. Find the service, right-click it, and then select the Start option to start the service.



❗ In **Control Panel > Windows Tools > Services** (services.msc), you can start or stop the **WhatapDBXAgent** service. Depending on the Windows version, the **service** path may differ.

Deleting a service

Execute the following command to delete a service.

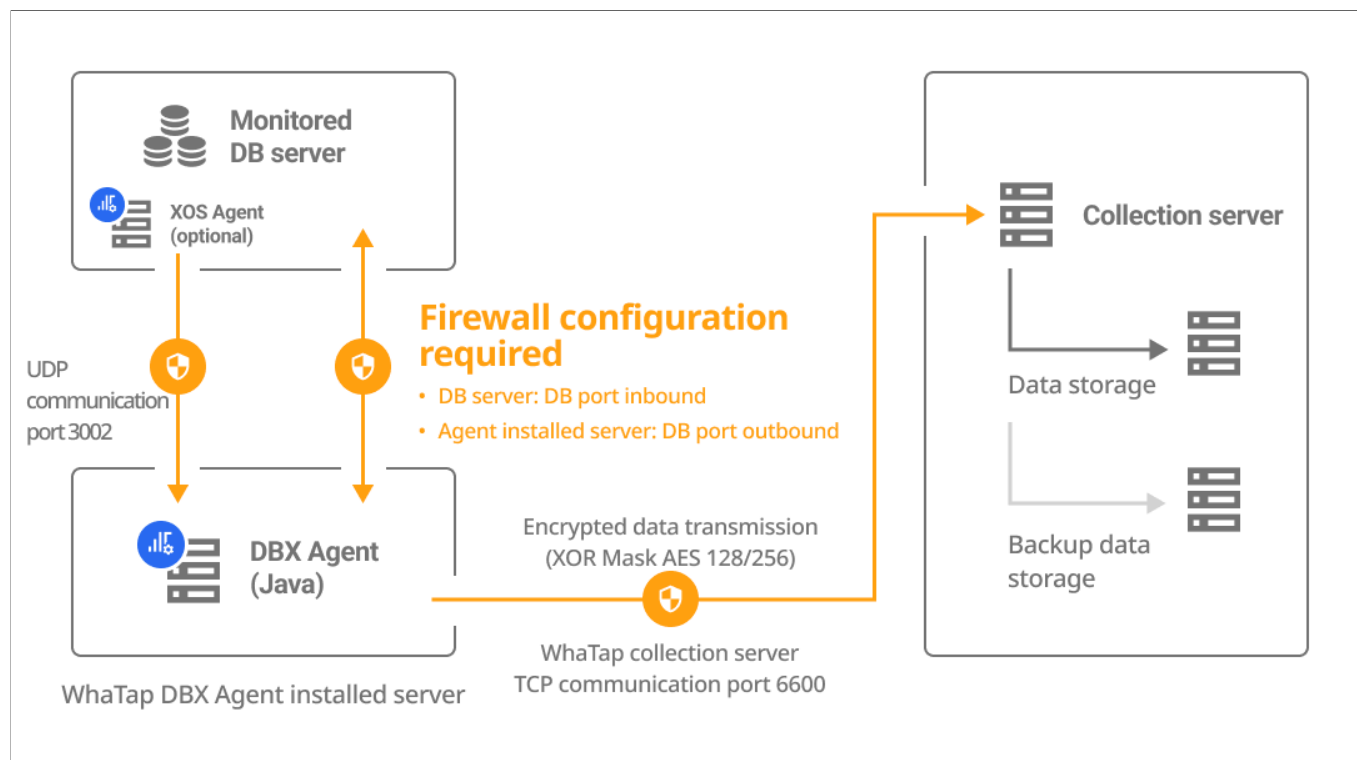
```
install_WindowsService.bat delete WhatapDBXAgent
```

You completed installing the agent for database monitoring. In [the following](#), check the post-installation checklist.

Installing the additional agent (XOS) and applying other options

To additionally monitor the resources of the database server, run a separate XOS agent process on the database server to collect data.

- ❗ • It can be applied to only the OS environment running on the x86 architecture.
- The additional agent installation process is **optional**.
- For more information about the XOS agent configuration options, see [the following](#).



Configuring the whatap.conf file

Set the following options in the [whatap.conf](#) file in the path where the DBX agent has been installed.

whatap.conf

```
xos=1
xos_port=3002
```

Move the [xos](#) folder (`/unzip folder/xos/`) to the database server.

Configuring the xos.conf file

Set the following options in the [xos.conf](#) file in the [xos](#) path moved to the database server.

xos.conf

```
dbx_ip={DB_Agent_IP}
```

```
dbx_port=3002 # default 3002
cpu_limit=0
mem_limit=10240
```

- ✓ In **Agent Installation**, when you enter the DB data to **DB Agent IP** and **DB Agent Port**, the agent options are automatically generated.

Running the XOS agent

Run the XOS agent.

```
./start.sh
```

- ⓘ
- To transmit monitored data to the DBX agent, the port set to `dbx_port` (default 3002) must have been open. (**UDP Outbound**)
 - To run the XOS agent in the background, run the `./startd.sh` file.

Installation Checking Items

The database monitoring has been installed completely. After installation, check if the installation was successful by doing the following:

Checking the agent installation

Run the `start.sh` shell script file or the `start.bat` batch file from the installation path of the database agent. When you run the agent, it starts collecting monitoring data from the database. If the WhaTap logo is displayed in the terminal after executing the shell script, it is normally executed.

start.sh

```
$ ./start.sh
```

| | | / / / _ _ / _ / _ _ _
 | | | / / _ \ _ \ / / / / _ \ _ \
 | _ / | _ / / \ \ / / / \ \ _ /
 / /

Just Tap, Always Monitoring

WhaTap DBX version X.Y.Z YYYYMMDD

❗ To use it like a daemon, execute the `startd.sh` command. However, it works only in the environment where **nohup** has been installed.

Checking the logs

- whatap.log

All logs related to the agent startup and collection can be found in the `$WHATAP_HOME /logs/whatap.log` file.

Every day at 00:00 UTC, the existing `whatap.log` file is automatically renamed to `whatap_yymmdd.log_` and

stored by date, and a new [whatap.log](#) file is created to record subsequent logs.

Log files stored by date are automatically deleted after 7 days.

- [xos.log](#)

The logs related to the startup of XOS are recorded in the `$XOS installation path /xos yymmdd .log` file and are automatically created by date.

Checking the agent processes

You can check the status of the active WhaTap DBX agent process with the following command.

```
$ ps -ef | grep dbx
```

Checking the monitoring

To check that the log has been normally uploaded from the server and the console has been registered normally, go to the initial screen of [Whatap Monitoring Service](#). Select the project to check and then select **Management > Agent List** on the left. From **Agent List**, you can check the name of the database server. To set the names of database servers separately, see [the following](#).

Status	Name (Initial)	ID	Start time	Active / Inactive	Agent version	Agent IP	DB IP	DB Port	DB Version	CPU Core	
Active	DBX-2-60-6379	2122651642	2024-03-13 18:36:35	2024-03-13 18:36:35	1.6.32 20240306	172.17.0.1	192.168.2.60	6379	7.0.11	1	
Active	DBX-2-60-6380	-2134789231	2024-03-13 18:36:10	2024-03-13 18:36:10	1.6.32 20240306	172.17.0.1	192.168.2.60	6380	7.0.11	0	
Active	DBX-2-60-6381	-137985273	2024-03-13 18:36:15	2024-03-13 18:36:15	1.6.32 20240306	172.17.0.1	192.168.2.60	6381	7.0.11	0	
Active	DBX-2-60-6382	1859113661	2024-03-13 18:36:20	2024-03-13 18:36:20	1.6.32 20240306	172.17.0.1	192.168.2.60	6382	7.0.11	0	

Troubleshooting

Check for possible problems upon database agent installation.

Firewall configuration checking

Unblock your firewall. Monitoring data cannot be sent to the server if the TCP outbound firewall is set for the WhaTap server.

How to check the firewall

It is normal only when the following connection-related information appears after executing the `telnet` command. (`telnet [Server IP] [Server Port]`)

Example

```
$ telnet 52.193.60.176 6600
Trying 52.193.60.176...
Connected to 52.193.60.176.
Escape character is '^['.
```

! The WhaTap collection server data can be found in **Management > Agent installation**.

Constraints

Multiple regions impossible to be selected as a single project

- In the [WhaTap monitoring service](#) website, when creating a project, you cannot select multiple regions. When using multiple regions, create separate projects.
- If servers exist in multiple regions as in the cloud environment, the collection servers must be located in each region to avoid constraints on the performance data collection such as network latency.

- WhaTap builds collection servers for each region to meet customer requirements.

Duplicate agent names (ONAME) impossible to be used

WhaTap DBX monitoring uses the agent's IP address and port to identify the agent. If the database server to be monitored in the user environment uses the same IP and port, the WhaTap server cannot identify the server instance.

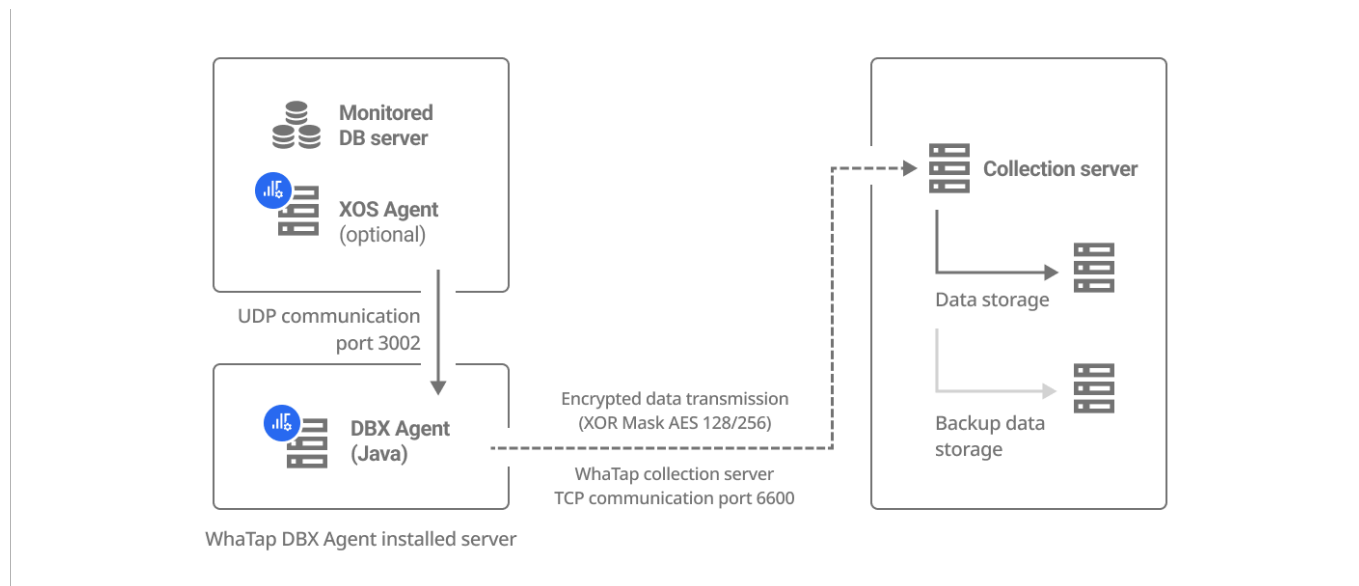
- If the server instance is not dynamically expanded, you can bypass it by manually setting a name for database identification by seeing [the following](#).
- If the databases to be monitored use internal addresses or duplicate IPs due to network virtualization, use separate database naming patterns by seeing [the following](#).

Configuration

You can take a look at the structure of the WhaTap agent, set additional functions through various options, and monitor the resources of the DB server to be monitored.

Agent structure

The following displays the WhaTap agent's structure map.



- **Collection server**

It collects and stores the database performance data collected by agents, extracts statistical data, and efficiently provides them to users. The collection server can be set by region. Different collection server addresses are allocated to each region. The collection server address may differ depending on the selected region. When creating a project, the region is also set.

- **DBX agent (default agent)**

Query-based performance data is collected and transmitted to the server. Monitoring is possible through a separate agent server without installing agents directly on the database server to be monitored.

- **XOS Agent (additional agent)**

The additional agent is an optional add-on agent that can monitor the process usage of the database server. To monitor the process usage of the database server, run a separate agent on the database server to collect data.

❗ The XOS agent can be applied to only the OS environment running on the x86 architecture.

- **Network**

- Default agent: The WhaTap monitoring agent uses the external communication (TCP) port 6600 to transfer the collected monitoring data to the WhaTap collection server.
- Additional agent: The external communication (UDP) port 3002 is used between the server where the agent has been installed and the database server. If the internal port conflicts, the port can be changed using the `dbx_port` option.

Agent CONFIG.

For more information about agent installation, see the following.

DBX Agent Setting

It guides you to the options you can set in the `whatap.conf` file.

XOS agent configuration

The following explains how to configure the database process monitoring.

DBX Agent Setting

Write the settings for the DBX agent in the [whatap.conf](#) file. For the options that can be set, see the following.

Default options

- **license** *String*

To install the agent, set the project access key granted from the server. The project access key includes the agent's project and the encryption key for secured communication.

- **whatap.server.host** *String*

Default `127.0.0.1,127.0.0.1`

Specify the IP address of the collection server to transfer the data collected by the agent. If there are multiple IP addresses for collection server redundancy, use comma (,) as the delimiter. The collection server proxy daemon must be serviced in the listening state for the set IP address.

- **whatap.server.port** *String*

Default `6600`

Set the port of the collection server. Because only one port can be set, use the same port set in the "whatap_server_host" option.

- **dbms** *String*

`tibero`

 If other option values are entered, data collection for monitoring may not work.

- **db** *String*

Database name.

- **db_ip** *String*

Set the IP address of the database server to be monitored.

- **db_port** *String*

Set the port used for DB communication.

Collecting data

- **db_param_enabled** Boolean

Default true

It sets whether or not to collect the DB parameters.

- **conn_fail_count** Int

Default 15

It sends a notification when the connection error occurs consecutively 15 times. You can adjust the notification trigger criteria by entering the desired number.

- **long_run_session_sec** Second

Default 10 (unit: second)

A session that has been running longer than the set time is treated as a long run session.

- **tables** Boolean

Default true

It collects the table size information. In **Stat/Report>Tablespace Size**, you can see the table size by selecting the database.

- **tables_hour** Int

Default 5

Set the time to collect data for storing the table size information. The default value is 5 and collection starts at 5 am.

- **tables_min_size** Int

Default 10

When collecting the table data, the table data smaller than the set value is not collected. The minimum collection value for the table is 10 MB by default.

- **tables_exclude_sys** Boolean

Default `true`

Set whether to collect table data owned by SYS, OUTLN, SYSGIS, and SYSCAT for collection. If set to `true`, the table data is not collected.

- **replication_name** `String`

If you set the replication name, it is considered that there is a Master/Slave relationship between DBs with the same `replication_name`.

As an option to define the replication set, if you set the `replication_name` option that has the same value for both master and slave nodes, the **Monitoring a Database Instance** displays a tree structure. It also provides a widget to monitor the replication status in **Flex Board** based on the option value.

- **skip_whatap_session** `Int`

Default `0`

If you set `1`, the session in which the query to collect from WhaTap operates, does not appear in the active session list. (Default value: 0)

User Metric Collection (SQLMON)

SQLMON periodically collects the results of user-defined SQL queries and stores them as metrics. It is suitable for lightweight queries that return numeric results.

- **sqlmon** `Int`

Default value: `1`

- `1` : Run both dbx and sqlmon simultaneously
- `2` : Run only sqlmon

Supported version: 2.3.5 or later

Configuration

1. Create a `sqlmon` directory under the dbx agent and create `<filename>.sql` files for the queries you want to collect.

```
dbx/
```

```
└─ sqlmon/
  └─ active_sessions.sql
  └─ lock_count.sql
```

2. Save the query to be collected as a `<filename>.sql` file.

Write the execution options on the **first line** and the SQL statement from the **second line** onward.

Option format

```
interval(min);run_time;tag_name
SQL statement
```

Item	Description	Example
Interval	Execution interval in minutes, minimum 1	1 → runs every 1 minute
Run time	HHMM-HHMM format, multiple ranges separated by comma (,). Set 0 to run at all times	0900-1100 → runs only 09:00-11:00
Tag name	Tag name stored in metrics. If omitted, the file name is used as the tag name	whatap

Example: 1 min interval, 09:00-11:00, tag name whatap

```
1;0900-1100;whatap
SELECT count(*) FROM active_sessions
```

Example: 1 min interval, always running, file name as tag

```
1;0
SELECT count(*) FROM active_sessions
```

- Run time can span across dates. (e.g., 2300-0100 → 23:00 to 01:00 the next day)
- When omitting the tag name, do not add a semicolon (;) after the run time.
- Do not add a semicolon (;) at the end of the SQL statement.

3. Enable SQLMON in `whatap.conf`.
4. Restart the agent.
5. In the  **Sitemap** > **Metrics Search** menu, check the `sqlmon` category.

```
# whatap.conf
sqlmon=1
```

Applying the AES 256 encryption

The WhaTap DBX agent transfers the collected data to the server after encryption. You can change this depending on the importance of the data or setting. Basically, the XOR operation and encryption through the AES algorithm are used, and encryption and decryption are performed by dividing the plain text into 128-bit units. It can be expanded up to 256 bits depending on the setting.

Add the following options to the `whatap.conf` file in the path where the WhaTap DBX agent has been installed.

`whatap.conf`

```
1 cypher_level=256
```

Add the settings and then restart the agent.

Agent name setting

Automatic configuration

If you do not set the agent name in the agent configuration (`whatap.conf`), the agent name is automatically determined by combining the IP address and the port number. For example, if the IP address is **10.11.12.13** and the port number is **3000**, the agent name is set to **DBX-12-13-3000**.

The key variables that determine the agent name are as follows:

Configuration	Description
{type}	The DBX value is used.
{ip0}	The first byte of the IPv4 address is used. (e.g. 10 in 10.11.12.13)
{ip1}	The second byte of the IPv4 address is used. (e.g. 11 in 10.11.12.13)
{ip2}	The third byte of the IPv4 address is used. (e.g. 12 in 10.11.12.13)
{ip3}	The fourth byte of the IPv4 address is used. (e.g. 13 in 10.11.12.13)
{port}	Database server port

❗ If the IP address is not numeric like RDS, the name is set in the following format: DBX- {ip0} - {hash} - {port} , where the {hash} value is the IP address that has been converted to 4-digit hexadecimal number.

Manual configuration

To set the agent name manually, enter a desired name for the `whatap.name` or `object_name` option in the `whatap.conf` file. The entered name is assigned to the agent name.

`whatap.conf`

```
whatap.name=agent-1234
# or
object_name=agent-1234
```

XOS Agent Configuration

To additionally monitor the resources of the database server, run a separate XOS agent process on the database server to collect data.

- ! • It can be applied to only the OS environment running on the x86 architecture.
- For more information about the XOS agent installation, see [the following](#).

Configuring the whatap.conf file

Set the following options in the [whatap.conf](#) file before running the XOS agent.

- **xos** Int

Default

Set whether or not to use the XOS agent. If the value is the XOS agent is not used for collection. Enter the value as or IP address of the XOS agent. If the IP address is specified, data is collected from only the XOS agent.

- **xos_port** String

Default

Set the port to communicate with the XOS agent. XOS agent can be communicated via UDP. If you have set a firewall on that port, disable it for UDP communication.

- **xos_cpu_iowait** Int

Default

Set whether the CPU utilization collected from the XOS agent is to include the iowait value. If the value is set to , the iowait value is included. If set to , the value is not included.

- **xos_mem_buffcache** Int

Default

Set whether the memory utilization collected from the XOS agent is to include the buffcache value. If the

value is set to `1`, the buffcache value is included. If set to `0`, the value is not included.

Configuring the xos.conf file

Copy the `xos` directory to the database server, and then enter the agent server information and set additional options in the `xos.conf` file.

- **dbx_ip** `String`

Enter the IP address of the server in which the DBX agent has been installed.

- **dbx_port** `String`

Default `3002`

Set the port to communicate with the DBX agent. DBX agent can be communicated via UDP. If you have set a firewall on that port, disable it for UDP communication.

- **cpu_limit** `Int`

Default `0`

It collects the process data with a value greater than the set limit. If it is 1.23% (1/100% step), set it to `123`.

- **mem_limit** `Int`

Default `10240`

It collects the process data with a value greater than the set limit. 10240 (Kbytes) indicates 10 MB.

- **disk_usage_interval** `Second`

Default `60`

It displays the disk utilization, free sizes, and total sizes for each instance. If the value is `0`, the disk utilization is not collected.

- **port_check** `String`

The XOS agent attempts to connect directly to the port specified as an option. If it fails, the port list is sent to the `db_port_check` category.

`xos.conf`

```
port_check=192.168.122.113:3333,192.168.122.113:3334
```

If access cannot be made via the specified port, you can check it after selecting the `db_port_check` category in **Analysis > Metrics Search**.

-	Time	Oid	Tags	Fields	
			oname	error_count 	port_list
1	2025-01-17 18:39:41	1064156037	DBX-5-112-1521	2	192.168.122.113:3333,192.168.122.113:3334
2	2025-01-17 18:39:41	1064156037	DBX-5-112-1521	2	192.168.122.113:3333,192.168.122.113:3334
3	2025-01-17 18:39:51	1064156037	DBX-5-112-1521	2	192.168.122.113:3333,192.168.122.113:3334
4	2025-01-17 18:39:51	1064156037	DBX-5-112-1521	2	192.168.122.113:3333,192.168.122.113:3334

- **process_check** String

You can monitor the running status of processes. Enter the process name as an option. You can register multiple items using comma (,) as the delimiter.

```
xos.conf
```

```
process_check=pmon,smon,tnslsnr,melong,haha
```

When the process containing the string is not monitored, the data is sent to the `db_process_check` category. For example, if there have no **melong** and **haha** processes, you can check it after selecting the `db_process_check` category from the **Analysis > Metrics Search** menu.

-	Time	Oid	Tags	Fields	
			oname	error_count 	process_name
1	2025-01-17 18:35:06	1064156037	DBX-5-112-1521	2	melong,haha
2	2025-01-17 18:35:06	1064156037	DBX-5-112-1521	2	melong,haha
3	2025-01-17 18:35:12	1064156037	DBX-5-112-1521	2	melong,haha
4	2025-01-17 18:35:12	1064156037	DBX-5-112-1521	2	melong,haha

① You can use the `process_check` option to send an alert when a process running in the database ends. For more information, see [the following](#).

- **process_check_interval** Second

Default `6`

The `process_check` option sets the time interval for collecting the process execution status.

- **iplist_interval** Second

Default `0` (Off)

Set the time interval for collecting the IP list for the database server. You can set the time interval in seconds (minimum of 3 seconds).

① If the `xos_dbip=true` option is set in the `whatap.conf` file, it is sent to the `db_ip_list` category. You can check it after selecting the `db_ip_list` category from the **Analysis > Metrics Search** menu.

User Metric Collection (SHMON)

SHMON periodically collects the results of user-defined shell scripts and stores them as metrics.

- **shmon** Int

Default value: `1`

Supported version: dbx 2.55.01 or later & xos 1.2.0f or later

Configuration

1. Create a `shmon` directory in the agent installation path.
2. Save the script to be collected as a `.sh` file.
3. Enable SHMON in `xos.conf`.
4. Restart the agent.
5. In the  **Sitemap > Metrics Search** menu, check the `shmon` category.

```
# xos.conf
shmon=1
```

Running the XOS agent

Run the following batch file on the database server.

```
$ ./start.sh
```

```
# or
```

```
$ ./startd.sh # When running in the background
```

Management

Agent Update

Updating to the latest version

Home > Select Project > **Management** > **Agent Update**

Agent Update

Agent update guide

When you click the 'Update' button, the latest agent file will be downloaded to the agent installation location and automatically restarted. The update process takes approximately 1 minute. Once complete, the agent version will change to the latest version.

ⓘ

The agent installed in the Windows environment does not support a self-update. [Show more](#)

ⓘ

If the update is not performed properly, please refer to [Whatap Docs](#).

Agent list

Latest agent version 2.3.3 [Update all agents to the latest version](#) [Previous version](#)

no.	id	ip	name	agent path	version	update
1	704779695	192.168.1.100	Agent-001	C:\Program Files\Whatap\agent\whatap-agent.exe	2.2.8 20241212	Update
2	1652207373	192.168.1.100	Agent-002	C:\Program Files\Whatap\agent\whatap-agent.exe	2.2.8 20241212	Update
3	755606486	192.168.1.101	Agent-003	C:\Program Files\Whatap\agent\whatap-agent.exe	2.1.4 20241101	Update

When you update the agent, the latest version of the agent file is automatically downloaded to the agent installation path ([agent path](#)) and it is restarted. The update takes about 1 minute. During an update, the download and update success messages appear on the screen step by step. After an update, the agent is automatically changed to the latest version.

- For the agents that can be updated, the **Update** button is enabled.
- To update agents individually, select **Update** to the right of each agent.
- To update all agents at a time, select **Update all agents to the latest version**.

✔ If you move to another menu while updating an agent, you cannot check its progress. While updating an agent, you cannot update another agent at the same time.

ⓘ The agents installed in the Windows environment do not support the automatic update. Manually reinstall the latest agent or place the latest [whatap.agent.dbx-*.jar](#) file in the previous agent folder and

❗ register the service again.

1. Delete Windows service

```
install_WindowsService.bat delete WhatapDBXAgent # existing service name
```

2. Create Windows service

```
install_WindowsService.bat create WhatapDBXAgent # existing service name
```

In case of update failure

In case of no agent restart

If the agent is not automatically changed to the latest version after display of a successful download message, manually restart the agent. Run the [stop.sh](#) and [startd.sh](#) batch files sequentially in the agent installation path ([agent path](#)).

Manual download of the agent

If downloading is not possible, proceed with agent installation in the following order:

1. Go to **Management > Agent Installation**.
2. Select **Download** in 2 of the **Install guide** section to download the latest version of the agent.
3. Unzip the downloaded file.
4. Upload only the [whatap.agent.dbx-X.Y.Z.jar](#) file to the agent installation path ([agent path](#)).
5. Run the [stop.sh](#) and [startd.sh](#) batch files to restart the agent.

Returning to the previous version

1. On the upper right of the screen, select **Previous version**.
2. The list of downloadable agents appears.
3. Select a desired version.
4. Select **Download** for the agent to return to the selected version.

5. Download the file to the installation path of the selected agent.
6. Delete the `whatap.agent.dbx-X.Y.Z.jar` file of the higher version from the agent installation path.
7. Run the `stop.sh` and `startd.sh` batch files to restart the agent.

ⓘ Because the batch file is set to run the highest version of the agent in the installation path, delete the higher version of JAR file to run the previous version of the agent.

Agent deletion

Deleting from the server where the agent have been installed

- [Linux](#) [Windows](#)

Among the Java processes running on the server, the process containing `whatap.agent.dbx` string is terminated. Run `stop.sh` in the path where the agent has been installed. Afterwards, delete the agent file and user roles registered in the agent.

Among the Java processes running on the server, find the process running with the jar file of the agent file name and then stop it. If the batch file is running in the foreground, end the batch execution script. Afterwards, delete the agent file and user permission registered in the agent.

Deleting on the service screen

To delete the agent from [Whatap Monitoring Service](#), go to **Agent List**. Before deleting the agent, terminate the agent process on the server where the agent has been installed.

1. Select a project to delete the agent from the **Project List**.
2. On the left of the screen, select **Management > Agent List**.
3. Select  on the utmost right of the agent to delete from **Agent List**.

ⓘ • Only inactive agents can be deleted.



Status	Name (Initial)	ID
 Active		
 Inactive		
 Active		

- Depending on the agent version, the delete function may not be supported. Update the agent to the latest version.

Dashboard

After installing the WhaTap agent, log in [WhaTap Monitoring Service](#). The initial screen is **Project List**. In **Project List**, you can see the installed project. If a project is selected from the **Project List**, you can enter [Instance List](#).

In the WhaTap database monitoring service, the dashboard allows you to see the overall status of the project at a glance. You can check the total resource size for monitoring and filter the resources to be monitored on the real-time dashboard.

- It is configured to show key performance metrics and status. The performance metrics are updated every 5 seconds.
- You can check the active sessions (including queries), lock information, and process information. To apply both the public cloud and private cloud, the products are configured for query-based monitoring.
- In a single instance, multiple databases are filtered.
- Based on the collected data, it provides the function to analyze the overall trend for a specific day. You can analyze slow queries after identifying active sessions at a specific time point.

Instance List

You can see the list of database servers in which the agent has been installed. It is configured to display key performance metrics and status. The performance metrics are updated every 5 seconds, and the columns in the list can be arranged through settings. For more information, see [the following](#).

Monitoring a Database Instance

- You can monitor key metrics and the details on active sessions of the database server in real time and check the warnings that may be problematic. You can select desired key metrics and monitor the overall system status.
- The real-time monitoring checks the performance metrics at an interval of 5 seconds. You can check the **Active sessions**, **Lock tree**, and **Process Info**.

For more information, see [the following](#).

Monitoring Multiple Instances

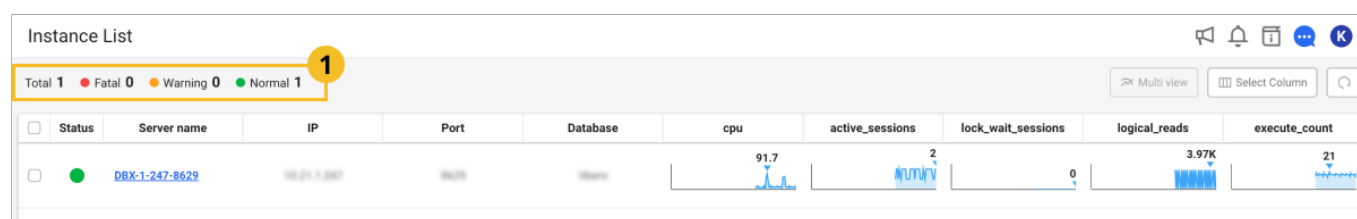
All instances registered in the project are monitored in real time at an interval of 5 seconds. You can also filter and monitor by specific instances. For more information, see [the following](#).

Instance List

Home > Select Project > **Dashboard** > **Instance List**

You can see the list of database servers in which the agent has been installed. You can check key performance metrics and status for each instance. The performance metrics are updated every 5 seconds, and the order of the columns and the metrics in the list can be changed through settings.

Basic screen guide

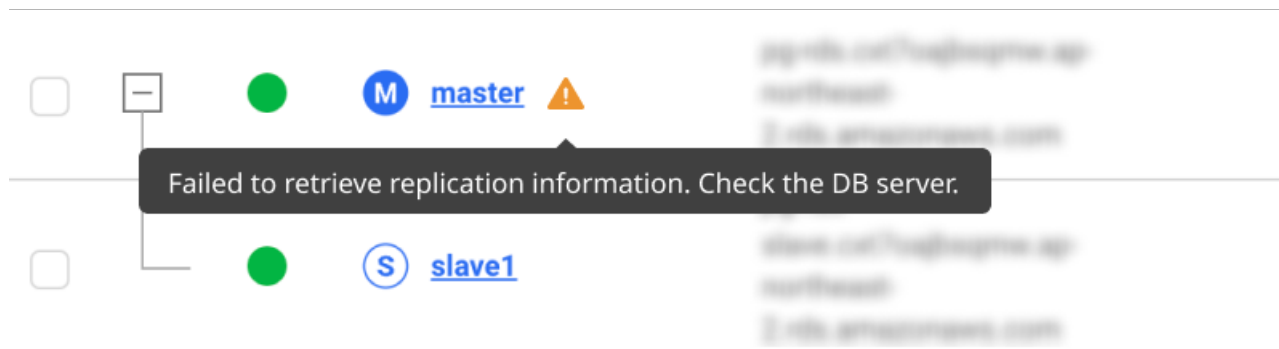


- The **1** area displays the status of instances set in the project. The displayed status data matches the total number of instances and matches the **Status** column data in the table.
- If you click an abnormal icon in the **Status** column, the **Event** window appears. You can see the history of events in the instance.
- If you select each instance, **Monitoring a Database Instance** appears. You can monitor the detailed information about the selected instances in real time.

! For more information about **Monitoring a Database Instance**, see [the following](#).

- It provides the key performance metrics in graph charts. The highest number appears on the chart. Hover your mouse over the chart to see the number at that location. For more information about the performance metrics, see [the following](#).
- In the **Instance list**, **(M)**, **(S)**, and **(C)** displayed in the **Server name** column mean Master, Slave, and Cluster respectively. It is displayed in case of the DB composed as replication.

If the replication instance is abnormal, the **!** icon appears.



- You can see real-time alerts by selecting  at the upper right of the screen. For more information about the alert settings, see [the following](#).

 For more information about the fixed area on the top of the screen, see [the following](#).

-  In **Instance list**, to change **Server name**, use the `object_name` option in the agent configuration file (`whatap.conf`). For more information, see [the following](#).

Comparing the instance metrics

You can select multiple instances to compare the performance metrics. If you select an instance to compare the performance metrics from the list, the **Multi view** button becomes active on the upper right of the screen. If you select **Multi view**, the **Monitoring Multiple Instances** menu appears. You can see the graph charts for comparing data for key performance metrics and the detailed information about active sessions and lock trees.

-  For more information about **Monitoring Multiple Instances**, see [the following](#).

Displaying or hiding columns

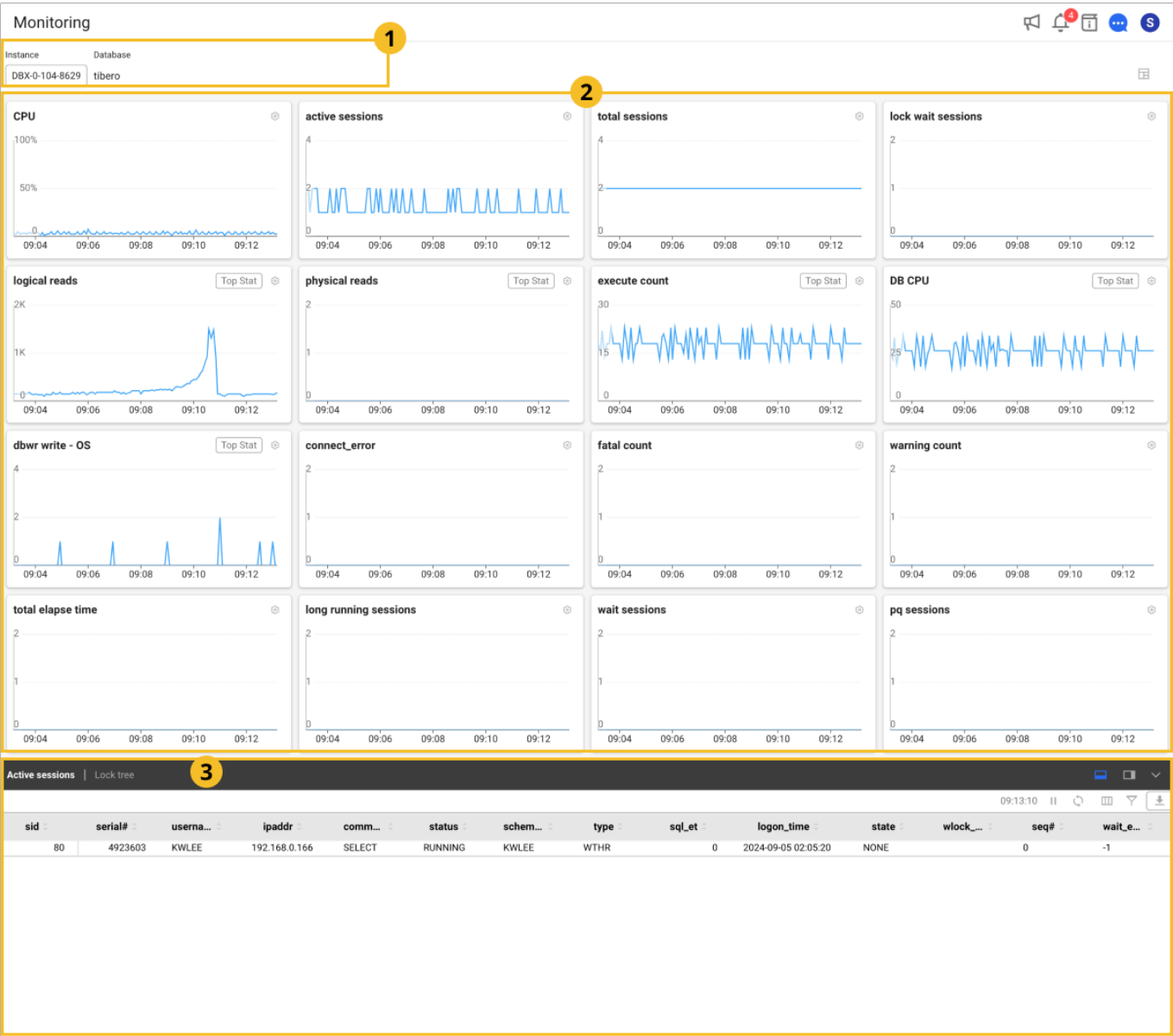
You can display or hide the performance metrics columns in the instance list. Select **Select Column** on the upper right of the screen. Check or uncheck the desired items. You can display or hide the columns.

Monitoring A Database Instance

Home > Select Project > **Dashboard** > **Monitoring a Database Instance**

In **Monitoring a Database Instance**, you can monitor the key metrics of the database server, information details on active sessions, lock tree, PQ tree, and process information in real time. You can also see the alerts that could be problematic warnings. By default, the collected data for the last 10 minutes is retrieved in real time. Collected data is updated every 5 seconds.

Basic screen guide



- **1** Selecting a lookup target
- You can select an instance and a database included in the instance for data inquiry. The collected data of the selected instance and its database are automatically applied to the **2** graph chart and the **3** [Active Sessions](#) table.

- **2** Graph chart section

The horizontal axis of each widget is time, and the vertical axis is the metric number. If you select a specific time period in each widget, **Analysis > Counts Trend** appears.

- **3 Active sessions | Lock tree | Process Info**

You can view the active session, lock tree, and process information.

- **Active sessions**

You can view active sessions and queries. If you select an item in the rightmost **sql_text** or **query** column in the table, the **SQL details** window appears. You can see the full text and plan information for the selected query. For more information, see [the following](#).

- **Lock tree**

You can see the lock session information, and holder and waiter information in real time. For more information about the table columns, see [the following](#).

- **Process Info**

You can query the resource usage of the database server in real time.

- Colors in the database correspond to the ones in the graph chart.
- For more information about **Counts Trend**, see [the following](#).
- For more information about each metric, see [the following](#).
- For more information about the columns, see [the following](#).
- The **Process Info** can be viewed by additionally configuring the XOS agent. For more information, see [the following](#).

Selecting a metric

You can change the metric of the graph chart widget placed on the screen to another one.

1. Select  on the upper right of the widget to change the metrics.
2. If the **Count selector** window appears, select a desired metric.



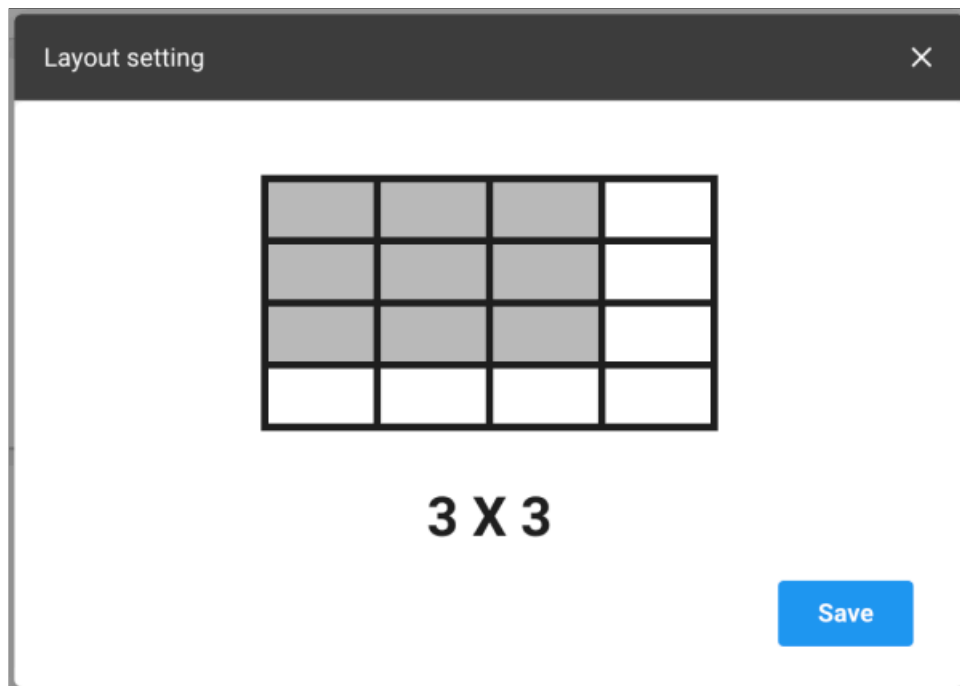
3. Select **Save**.

The metric of the selected widget is changed.

! For more information about each metric, see [the following](#).

Layout setting

To set the layout on the metrics chart, on the upper right of the screen, select . Nine (3x3) metrics charts are set on the default layout, and you can change the number of charts on a page.



Using the active session section

Through **Active sessions** at the bottom of the screen, you can see the real-time active sessions. The following provides the guide for the button on the upper right of the table.

- : You can stop changing the data collected in real time. To restart it again, select .
- : The list of tables is refreshed.
- : The column header entries in the table can be displayed or hidden.
- : You can filter the list based on the column header entries in the table. After selecting the button, you can set the conditions in each header column such as **Includes**, **Excludes**, **Equal**, and **Unequal**.

Adjust the column width if the text field for filter condition options is invisible.

- : You can download the content of the table as a CSV file.

Stopping an active session

You can stop a session(s) that has been running for a long time.

1. In the **Active sessions** list, move your mouse cursor to the session to terminate.
2. Select the  that appears on the utmost right.
3. If the **Session kill** window appears, enter the password.
4. Select **Apply**.

The session is stopped.

- Through the [paramkey.txt](#) file in the DBX agent installation path, you can find the password.
- This feature is only available to the members with **Edit** role. For more information about member roles, see [the following](#).

Zooming in the graph chart section

If the current screen is small and difficult to see the widget, you can check the graph chart widget in a wider screen. Select ▼ in the **Active sessions** section at the bottom of the screen. The **Active sessions** section is collapsed and the graph chart widget section is enlarged.

To zoom out the graph chart widget, select ▲ at the bottom of the **Active sessions** section.

View SQL Details

To check the SQL query information of the executing session, select the **query** (or **sql_text**) column in the **Active sessions** section. The **SQL details** window appears. You can check the SQL query statements and plan information.

Click the **View SQL Statistics** → button to move to **SQL statistics**, where you can view statistical information related to the selected SQL query.

The screenshot shows a database monitoring interface. At the top, there's a table with columns like 'id', 'type', 'state', 'command', 'text', 'time', 'wait_time', 'wait_type', 'wait_reason'. A row is highlighted with a yellow box containing the text: `execute sleep(1)` and `select /* WhaTap8D#1 */ s.*,t.seqnum,t.event...`. Below this, a 'SQL details' panel is open, showing a query (hash: -485691958) and its execution plan. The query is a complex SELECT statement with multiple columns and a subquery. The execution plan shows two steps: a 'SIMPLE' step with a 'p' operator and an 'ALL' access path, and another 'SIMPLE' step with an 'i' operator and an 'ALL' access path.

Viewing the default plan

When creating the **default plan user file**, you can configure the agent to automatically view the plan by using the predefined DB information. After checking the box for **Default plan inquiry**, search for the plan through the specified DB connection information as follows.

- **Linux** **Windows**

1. Add the `plan_db` option to the agent configuration (`whatap.conf`) file and then enter the DB name.

whatap.conf

```
plan_db=(dbname)
```

2. After configuring the DB, use the `planuid.sh` script to set the user and password.

```
./planuid.sh user pwd
```

❗ If the user (`user`) and password (`pwd`) include special characters, add backslashes (`\`) before each special character.

! e.g. `user$example` → `user\example`

1. Add the `plan_db` option to the agent configuration ([whatap.conf](#)) file and then enter the DB name.

whatap.conf

```
plan_db=(dbname)
```

2. After configuring the DB, use the `planuid.bat` script to set the user and password.

```
planuid.bat user pwd
```

Changing the table columns

You can display or hide the column entries in the table, and change their order.

1. Select  on the upper right of the table.
2. When the [Column Setting](#) window appears, hide, add, or change the order of items to be displayed in the table columns.
 - Select a column, and then `<`, `>`, `+` or `-`. Go to [Visible](#) or [Invisible](#).
 - You can move the position by dragging the column while it is selected.
3. After all settings are finished, select [Save](#).

! The setting is saved as a browser cookie value to maintain the state even after refreshing the page. If an error occurs between settings due to cookie deletion or other reasons, it is initialized.

Column information guide

For more information about columns, see [the link](#).

- [Active session](#) Lock tree Process information

Item	Description
<code>action</code>	Name of the running job.
<code>block_updates</code>	Number of block updates.
<code>block_updates_sigma</code>	Total number of block updates.
<code>client_identifier</code>	Client ID.
<code>client_info</code>	Additional information of the client.
<code>client_pid</code>	PID of the client process.
<code>command</code>	Command running in the current session.
<code>consumed_cpu_time</code>	CPU time consumed by the session.
<code>consumer_group</code>	Consumer group to which the session belongs.
<code>cpu(xos)</code>	CPU utilization
<code>cpuusage</code>	CPU usage consumed by the session.
<code>event_name</code>	Name of the waiting event.
<code>execute_count</code>	Number of SQL executions.
<code>execute_count_sigma</code>	Total number of executions.
<code>id1</code>	First identifier value.

Item	Description
id2	Second identifier value.
ioread(xos)	Actual time spent reading the block (milliseconds).
iowrite(xos)	Actual time spent writing the block (milliseconds)
ipaddr	Client IP address.
logon_time	Time when the session logged in the database.
logical_reads	Number of logical read operations.
logical_reads_sigma	Total number of logical read operations.
machine	Name of the machine on which the session is running.
module	Name of the running module.
os_thr_id	Thread ID of the operating system.
osuser	User of the operating system running the session.
parse_count_hard	Number of hard parses.
parse_count_hard_sigma	Total number of hard parses.
parse_count_total	Total number of parses.
parse_count_total_sigma	Total number of parses.
pdml_enabled	Whether parallel DML is enabled or not.
pdml_status	Status of the parallel DML.
pddl_status	Status of the parallel DDL.

Item	Description
<code>pga_used_mem</code>	Amount of memory being used in the process global area (PGA).
<code>physical_reads</code>	Number of physical read operations.
<code>physical_reads_sigma</code>	Total number of physical read operations.
<code>pid</code>	PID of the database process.
<code>pq_status</code>	Status of the parallel query.
<code>prev_sql</code>	Text of the previously executed SQL statement.
<code>prev_sql_id</code>	Unique ID of the previously executed SQL statement.
<code>prev_sql_param</code>	Parameter of the previously executed SQL.
<code>prog_name</code>	Name of the program running the session.
<code>pss(xos)</code>	Process specific memory usage + Percentage of shared memory occupied by one process.
<code>row_wait_block_no</code>	Block number of the waiting row.
<code>row_wait_file_no</code>	File number of the waiting row.
<code>row_wait_obj_id</code>	Object ID of the waiting row.
<code>row_wait_row_no</code>	Row number of the waiting row.
<code>rss(xos)</code>	Resident Set Size (RSS) that is the number of physical pages associated with the process.
<code>schemaname</code>	Name of the schema the session is using.
<code>seq#</code>	Value indicating the sequence number of the session.

Item	Description
<code>sid</code>	Session ID that uniquely identifies the session.
<code>sql_et</code>	SQL execution time.
<code>sql_hash</code>	Hash value of the SQL statement.
<code>sql_id</code>	Unique ID of the SQL statement being executed.
<code>sql_param</code>	Parameters used to execute SQL.
<code>sql_text</code>	Text of the SQL statement being executed.
<code>sql_trace</code>	Whether to trace SQL.
<code>state</code>	Current state of the session.
<code>status</code>	Status of the session.
<code>terminal</code>	Name of the terminal to which the session is connected.
<code>type</code>	Type of the session.
<code>usn</code>	Undo segment number.
<code>used_blk</code>	Number of used blocks.
<code>used_rec</code>	Number of used records.
<code>wait_event</code>	Event that the session is waiting for.
<code>wait_time</code>	Waiting time.
<code>wlock_wait</code>	Whether the session is waiting for a lock or not.
<code>wthr_id</code>	Thread ID of the session's work.

Item	Description
event	Name of the waiting event.
holder type	Type of the session that owns a lock.
id1	First identifier value.
id2	Second identifier value.
lock mode	Lock mode requested or owned by the current session.
lock request	Status of the lock requested by the session.
module	Name of the running module.
pid	PID of the database process.
prev_sql_id	Unique ID of the previously executed SQL statement.
prev_sql_param	Parameter of the previously executed SQL.
prev_sql_text	Text of the previously executed SQL statement.
prog_name	Name of the program running the session.
serial#	Serial number that distinguishes repeated attempts for the same session.
sid	Session ID that uniquely identifies the session.
sql_et	SQL execution time.
sql_id	Unique ID of the SQL statement being executed.
sql_param	Parameters used to execute SQL.
sql_text	Text of the SQL statement being executed.

Item	Description
status	Status of the session.
username	Name of the user running the session.
waiter type	Type of the session waiting for a lock.

The following items are the metrics collected if the XOS agent has been installed.

Item	Description
cputime	CPU usage time
cpuusage	CPU Utilization
elapse	Elapsed time of CPU usage
vsize	Virtual memory size (Kb)
rss	Resident Set Size (RSS) that is the number of physical pages associated with the process.
state	Process status
ioread	Actual time spent reading the block (milliseconds)
iowrite	Actual time spent writing the block (milliseconds)
pss	Process specific memory usage + Percentage of shared memory occupied by one process
uid	user id
cmd	Executing command
longcmd	Full path of cmd

ⓘ WhaTap basically stores the client-related information.

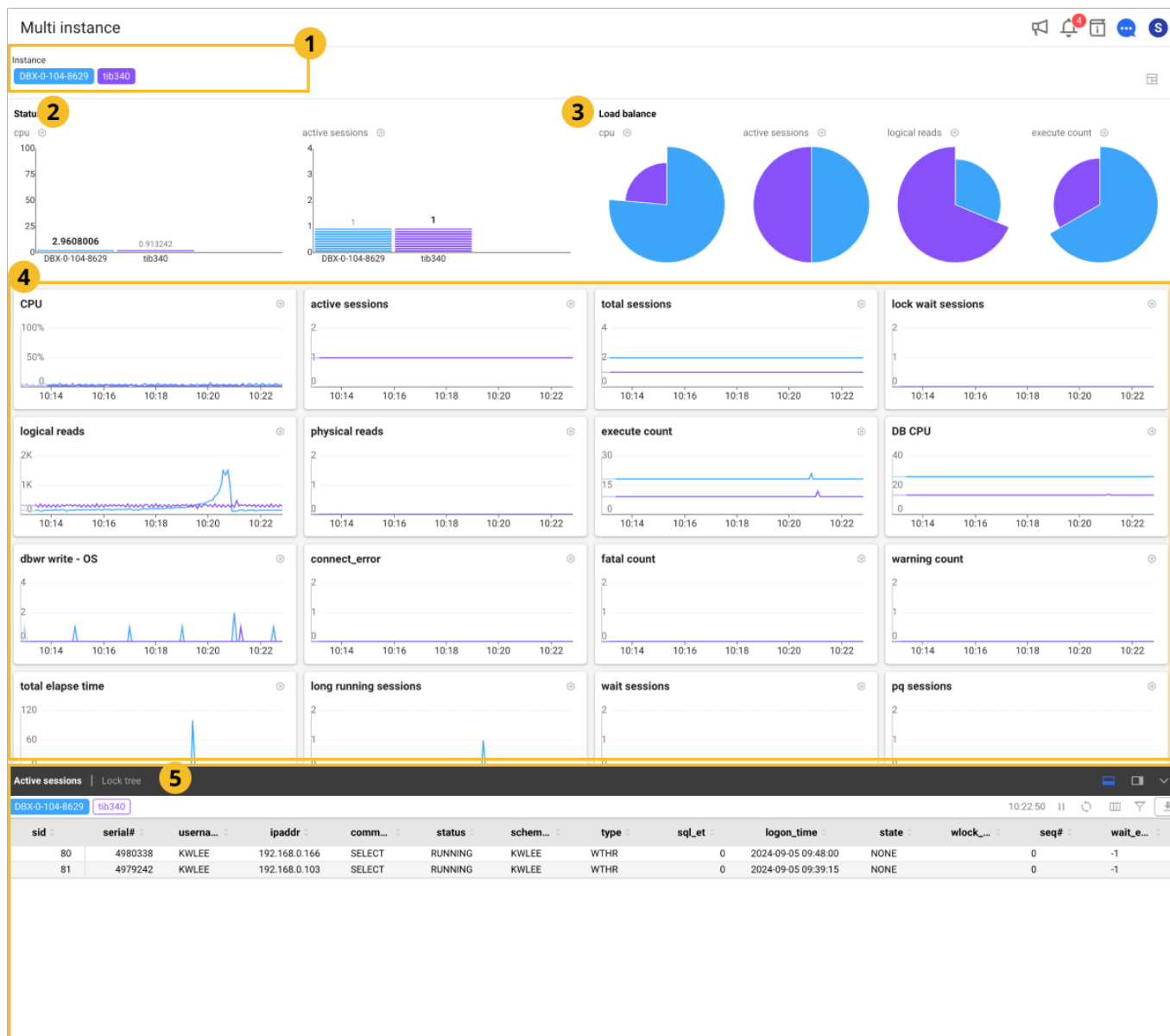
Monitoring Multiple Instances

Home > Select Project > [Dashboard](#) > [Multiple Instance Monitoring](#)

In [Instance Monitoring](#), to monitor only one instance, [Multiple Instance Monitoring](#) allows you to check and compare metrics and active sessions of multiple instances on one screen. Graph charts make it easy to see how instances' metric values are trending and which instances have higher metric values.

- ✓ If you select an agent to compare in **Dashboard > Instance List**, and then select **Multi view**, the **Monitoring Multiple Instances** menu appears.

Basic screen guide



• **1** Instance

It is a list of instances (databases) where the agent has been installed. The color of the instance matches the color of the graph chart placed on the screen. To exclude some instances of data from the graph chart, select the corresponding instances. If you select the instance again, the graph chart reflects the instance data.

- **2 Status**

You can monitor the metrics related to the resources of your database server.

- **3 Load balance**

You can monitor whether the load is concentrated on one server by checking which instance has a high metric value.

- **4 Graph chart section**

The horizontal axis of each widget is time, and the vertical axis is the metric number.

- **5 Active sessions | Lock tree | Process Info**

You can view the active session, lock tree, and process information for a specific instance. Select Instance Name.

- For more information about each metric, see [the following](#).
- For more information about the columns, see [the following](#).
- The **Process Info** can be viewed by additionally configuring the XOS agent. For more information, see [the following](#).

Selecting a metric

You can change the metric of the graph chart widget placed on the screen to another one.

1. Select  on the upper right of the widget to change the metrics.
2. If the **Count selector** window appears, select a desired metric.



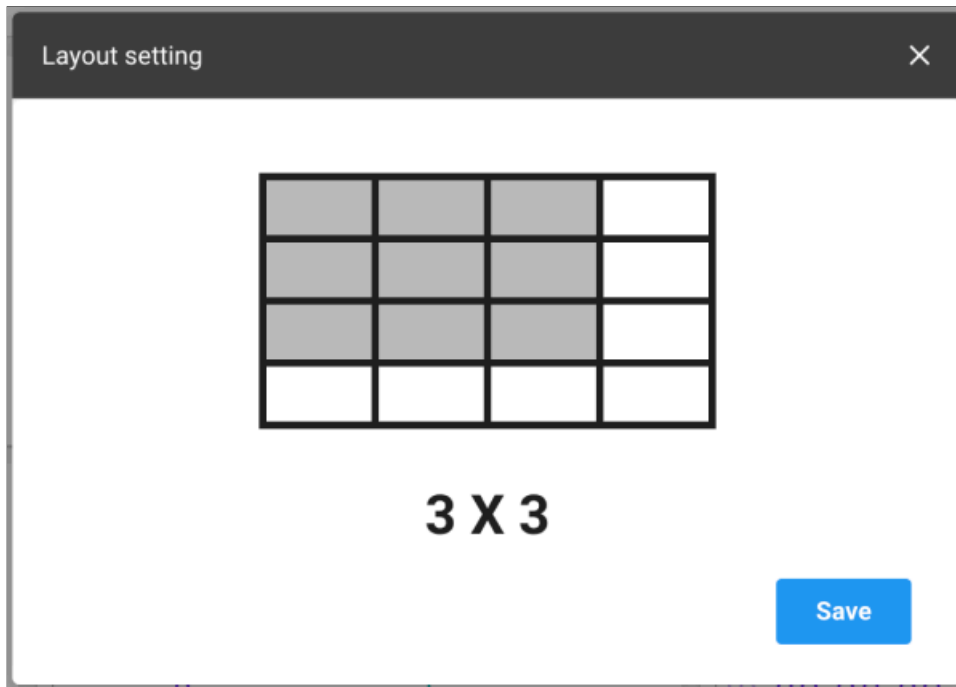
3. Select **Save**.

The metric of the selected widget is changed.

! For more information about each metric, see [the following](#).

Layout setting

To set the layout on the metrics chart, on the upper right of the screen, select . Nine (3x3) metrics charts are set on the default layout, and you can change the number of charts on a page.



Using the active session section

Through **Active sessions** at the bottom of the screen, you can see the real-time active sessions. The following provides the guide for the button on the upper right of the table.

- **II** : You can stop changing the data collected in real time. To restart it again, select **▶**.
- **🔄** : The list of tables is refreshed.
- **☰** : The column header entries in the table can be displayed or hidden.
- **🔍** : You can filter the list based on the column header entries in the table. After selecting the button, you can set the conditions in each header column such as **Includes**, **Excludes**, **Equal**, and **Unequal**.

ⓘ Adjust the column width if the text field for filter condition options is invisible.

- **⬇️** : You can download the content of the table as a CSV file.

Stopping an active session

You can stop a session(s) that has been running for a long time.

1. In the **Active sessions** list, move your mouse cursor to the session to terminate.
2. Select the  that appears on the utmost right.
3. If the **Session kill** window appears, enter the password.
4. Select **Apply**.

The session is stopped.

- ! • Through the [paramkey.txt](#) file in the DBX agent installation path, you can find the password.
- This feature is only available to the members with **Edit** role. For more information about member roles, see [the following](#).

Zooming in the graph chart section

If the current screen is small and difficult to see the widget, you can check the graph chart widget in a wider screen. Select ▼ in the **Active sessions** section at the bottom of the screen. The **Active sessions** section is collapsed and the graph chart widget section is enlarged.

To zoom out the graph chart widget, select ▲ at the bottom of the **Active sessions** section.

View SQL Details

To check the SQL query information of the executing session, select the **query** (or **sql_text**) column in the **Active sessions** section. The **SQL details** window appears. You can check the SQL query statements and plan information.

Click the **View SQL Statistics** → button to move to **SQL statistics**, where you can view statistical information related to the selected SQL query.

The screenshot shows a SQL monitoring tool interface. At the top, there's a query editor with a highlighted line: `select /* WhaTap8D#1 */ s.*, t.seqnum, t.event...`. Below the editor, there's a "SQL details" section with a "View SQL Statistics" button. The main area displays a table with columns: "Plan", "test", "whatap", and a search icon. The table has two rows of data:

Plan	test	whatap	Search
1	SIMPLE	p	ALL
1	SIMPLE	i	ALL

Below the table, there's a "Query (hash: -485691958)" section with buttons for "Default Bind", "Reset Bind", and "Formatting". The query text is:

```
select
/* WhaTap6D#4 */
processlist_id,
processlist_user,
processlist_host,
processlist_db,
processlist_command,
processlist_state,
thread_id,
processlist_time,
type,
name,
connection_type,
thread_os_id,
i.info
from
performance_schema.threads p
left outer join information_schema.processlist i on p.processlist_id = i.id
where
type <> 'BACKGROUND'
and processlist_command <> 'Sleep'
```

Changing the table columns

You can display or hide the column entries in the table, and change their order.

1. Select  on the upper right of the table.
2. When the [Column Setting](#) window appears, hide, add, or change the order of items to be displayed in the table columns.
 - Select a column, and then `<`, `>`, `+` or `-`. Go to [Visible](#) or [Invisible](#).
 - You can move the position by dragging the column while it is selected.
3. After all settings are finished, select [Save](#).

 The setting is saved as a browser cookie value to maintain the state even after refreshing the page. If an error occurs between settings due to cookie deletion or other reasons, it is initialized.

Column information guide

For more information about columns, see [the link](#).

- [Active session](#) **Lock tree** **Process information**

Item	Description
<code>action</code>	Name of the running job.
<code>block_updates</code>	Number of block updates.
<code>block_updates_sigma</code>	Total number of block updates.
<code>client_identifier</code>	Client ID.
<code>client_info</code>	Additional information of the client.
<code>client_pid</code>	PID of the client process.
<code>command</code>	Command running in the current session.
<code>consumed_cpu_time</code>	CPU time consumed by the session.
<code>consumer_group</code>	Consumer group to which the session belongs.
<code>cpu(xos)</code>	CPU utilization
<code>cpuusage</code>	CPU usage consumed by the session.
<code>event_name</code>	Name of the waiting event.
<code>execute_count</code>	Number of SQL executions.
<code>execute_count_sigma</code>	Total number of executions.
<code>id1</code>	First identifier value.

Item	Description
id2	Second identifier value.
ioread(xos)	Actual time spent reading the block (milliseconds).
iowrite(xos)	Actual time spent writing the block (milliseconds)
ipaddr	Client IP address.
logon_time	Time when the session logged in the database.
logical_reads	Number of logical read operations.
logical_reads_sigma	Total number of logical read operations.
machine	Name of the machine on which the session is running.
module	Name of the running module.
os_thr_id	Thread ID of the operating system.
osuser	User of the operating system running the session.
parse_count_hard	Number of hard parses.
parse_count_hard_sigma	Total number of hard parses.
parse_count_total	Total number of parses.
parse_count_total_sigma	Total number of parses.
pdml_enabled	Whether parallel DML is enabled or not.
pdml_status	Status of the parallel DML.
pddl_status	Status of the parallel DDL.

Item	Description
pga_used_mem	Amount of memory being used in the process global area (PGA).
physical_reads	Number of physical read operations.
physical_reads_sigma	Total number of physical read operations.
pid	PID of the database process.
pq_status	Status of the parallel query.
prev_sql	Text of the previously executed SQL statement.
prev_sql_id	Unique ID of the previously executed SQL statement.
prev_sql_param	Parameter of the previously executed SQL.
prog_name	Name of the program running the session.
pss(xos)	Process specific memory usage + Percentage of shared memory occupied by one process.
row_wait_block_no	Block number of the waiting row.
row_wait_file_no	File number of the waiting row.
row_wait_obj_id	Object ID of the waiting row.
row_wait_row_no	Row number of the waiting row.
rss(xos)	Resident Set Size (RSS) that is the number of physical pages associated with the process.
schemaname	Name of the schema the session is using.
seq#	Value indicating the sequence number of the session.

Item	Description
<code>sid</code>	Session ID that uniquely identifies the session.
<code>sql_et</code>	SQL execution time.
<code>sql_hash</code>	Hash value of the SQL statement.
<code>sql_id</code>	Unique ID of the SQL statement being executed.
<code>sql_param</code>	Parameters used to execute SQL.
<code>sql_text</code>	Text of the SQL statement being executed.
<code>sql_trace</code>	Whether to trace SQL.
<code>state</code>	Current state of the session.
<code>status</code>	Status of the session.
<code>terminal</code>	Name of the terminal to which the session is connected.
<code>type</code>	Type of the session.
<code>usn</code>	Undo segment number.
<code>used_blk</code>	Number of used blocks.
<code>used_rec</code>	Number of used records.
<code>wait_event</code>	Event that the session is waiting for.
<code>wait_time</code>	Waiting time.
<code>wlock_wait</code>	Whether the session is waiting for a lock or not.
<code>wthr_id</code>	Thread ID of the session's work.

Item	Description
event	Name of the waiting event.
holder type	Type of the session that owns a lock.
id1	First identifier value.
id2	Second identifier value.
lock mode	Lock mode requested or owned by the current session.
lock request	Status of the lock requested by the session.
module	Name of the running module.
pid	PID of the database process.
prev_sql_id	Unique ID of the previously executed SQL statement.
prev_sql_param	Parameter of the previously executed SQL.
prev_sql_text	Text of the previously executed SQL statement.
prog_name	Name of the program running the session.
serial#	Serial number that distinguishes repeated attempts for the same session.
sid	Session ID that uniquely identifies the session.
sql_et	SQL execution time.
sql_id	Unique ID of the SQL statement being executed.
sql_param	Parameters used to execute SQL.
sql_text	Text of the SQL statement being executed.

Item	Description
status	Status of the session.
username	Name of the user running the session.
waiter type	Type of the session waiting for a lock.

The following items are the metrics collected if the XOS agent has been installed.

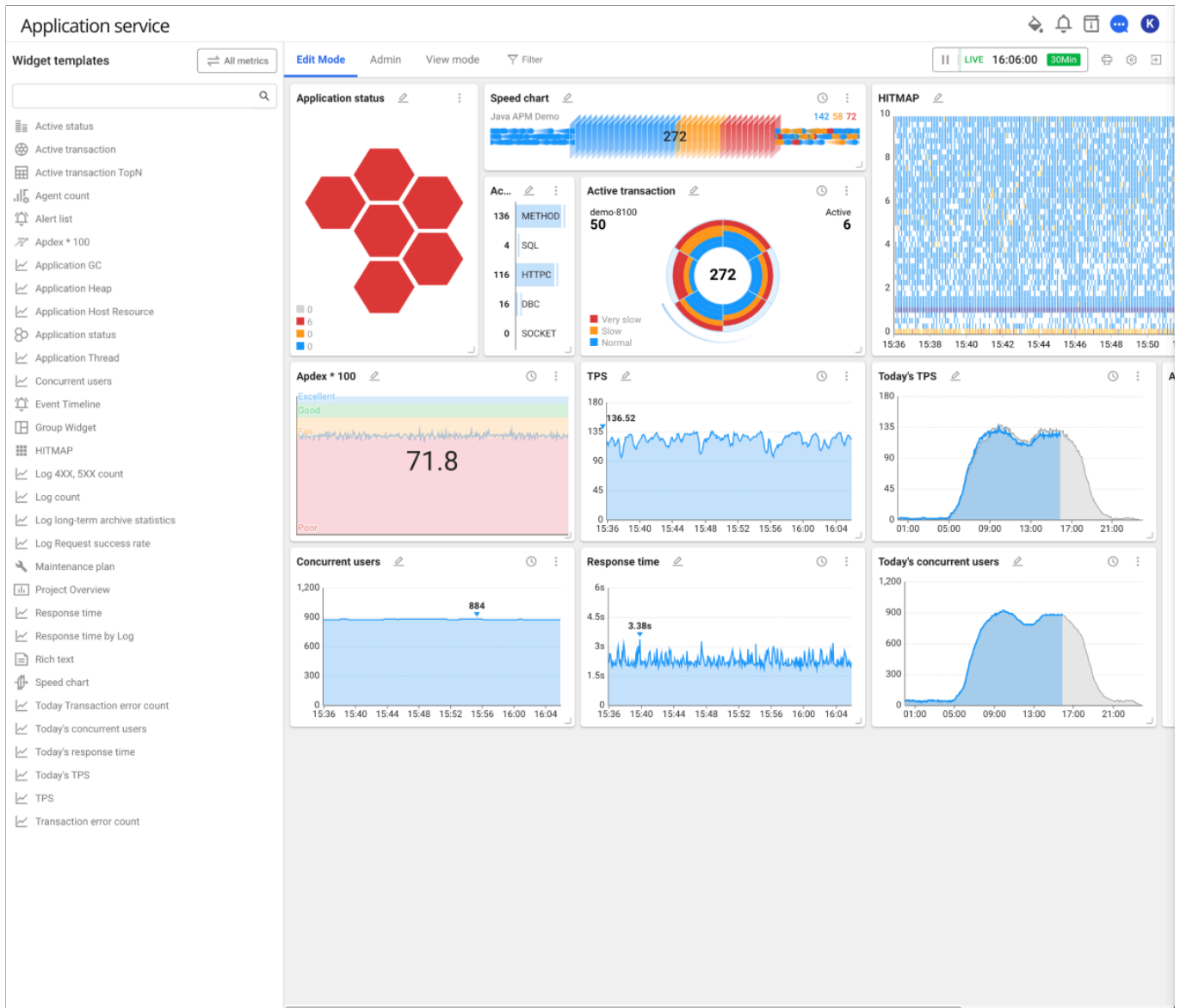
Item	Description
cputime	CPU usage time
cpuusage	CPU Utilization
elapse	Elapsed time of CPU usage
vsize	Virtual memory size (Kb)
rss	Resident Set Size (RSS) that is the number of physical pages associated with the process.
state	Process status
ioread	Actual time spent reading the block (milliseconds)
iowrite	Actual time spent writing the block (milliseconds)
pss	Process specific memory usage + Percentage of shared memory occupied by one process
uid	user id
cmd	Executing command
longcmd	Full path of cmd

ⓘ WhaTap basically stores the client-related information.

Flex Board

Flex Board is a custom integrated dashboard. You can create a real-time dashboard with the project data such as applications, servers, databases, and containers.

You can quickly complete the initial setup with preconfigured templates and build dashboards in your preferred format. By adding data widgets or modifying properties, you can display information in the form you need, and with filtering functions, you can narrow down monitoring targets. When you set a time range, you can check data from a specific point in time, and by using auxiliary charts, you can analyze data in various ways. Dashboards can be added to favorites for easy access, and personalized dashboards can be copied to other accounts for reuse.



The usage scope of the Flex board differs depending on the following entry:

Home > Integrated Flex Board

- When creating a widget, all projects that can be viewed are provided as options.
- The dashboard is saved in your account and can be shared with other users with the "To copy" feature.
- Individual account dashboards are not affected by the role, but the shared dashboards are read-only and cannot be edited.

Home > Select Project > Dashboard > Flex Board

- When creating a widget, the related project data is automatically entered.
- The created Flex board is automatically shared with other project members.
- The users with the project **Edit** role or **Project flexboard update** role, and **site admin** role can modify the board.

✓ Users with edit permissions for the Flex Board can use the following features:

- Export and import dashboards as JSON files
- Check data requests and responses within the dashboard
- View and edit widget configuration options in JSON format

ⓘ In the **Flex Board** menu within the project, only the users with the dashboard editing role can access **Edit Mode**, **Admin Mode**, and **Filter**.

- Accessible member permissions
 - Project **Edit** role
 - **Project flexboard update** role
 - **Site Admin** role
- For more information about the **View mode** and **Filter**, see [the following](#).
- For more information about the member roles, see [the following](#).

Using Flex Board

- ✓ You can build dashboards using various widget templates, including metrics widgets.
For details on the features and usage of each template, see the [Widget template](#) document.

Apply a preset template

Use a preset template to speed up the initial setup, then modify it as needed.

1. Select the **Flex Board** menu.
2. From the **Template** list on the left, select the template you want.
3. When the **Flex board management** window appears, enter a name in **Rename**.
 - In **Layout**, select a widget and drag it to the position you want.
4. Click the **Save** button. A Flex board is created based on the selected template.
 - You can check the created board in the board list of **Flex Board**.

Create a Flex board

You can create a Flex board and place widgets to build your own dashboard.

1. In **Flex Board**, click the **Create Dashboard** button at the top right.
2. When the **Create Dashboard** window appears, enter the dashboard **Name** in the input box.
3. Select a widget placement method, then click the **Create Dashboard** button.
 - **Fixed layout flexboard**: free widget placement with pixel basis
 - **Responsive flexboard**: responsive grid layout based on browser size
(configure the grid, then click the **Create Dashboard** button)
4. In the **Widget templates** selection screen, choose the widgets to place on the dashboard.

- To add metrics widgets, click the **All Metrics** button on the right of **Widget templates**.

- ! • **Widget templates:** choose from a predefined widget list that summarizes key indicators commonly used in monitoring.
- **All metrics:** create widgets based on all metrics data collected in your project. For details about metrics widgets, see [the following document](#).

5. Move the placed widgets or adjust their size.
 - When a crosshair cursor appears at the top of a widget, click and drag the widget to move it.
 - When an arrow cursor appears at the bottom right of a widget, click and drag to resize it.
6. After you finish placing widgets, select **View mode** to review the layout. To edit the layout again, select **Edit Mode** and adjust widget placement.
7. When all steps are complete, click the  (**Go to list**) icon at the top right.
 - You can check the created board in **Flex Board** under **Dashboard list**. Select the created board to view the new Flex board.

- ! We plan to add dashboard templates or widgets based on customer feedback. If you need a specific dashboard template or widget, contact us at support@whatap.io.

Edit a Flex board

! Flex board edit permissions

- **Home > Integrated Flex Board:** this is a personal account dashboard, so permissions do not apply; however, dashboards shared as read only cannot be edited.
- **Home > Select project > Dashboard > Flex Board:** users with project edit permission, project Flex board edit permission, or Site Admin permission can edit.

For details on member permissions, see [the following document](#).

1. In **Flex Board** under **Dashboard list**, click the edit icon . The **Flex board management** window appears on the right.
2. In the **Flex board management** window, configure Name, Project, Layout, widget.json, and option.json.
 - **Rename:** edit the dashboard name.
 - **Project:** select the project from which widgets will fetch data.

 You can configure the **Project** option only in **Home > Integrated Flex Board**. If you entered from **Integrated Flex Board**, you can select the data source project for each widget.

1. Click the **+** button at the top right of a widget, then search and select one or multiple projects.
2. After selecting projects, click the **Apply** button.

- **Layout**
 - Drag widgets to move them.
 - Click and drag the bottom right of a widget to resize it.
 - To delete a widget, click the  icon at the top right of the widget.
- **Widget.json:** import dashboard widget settings in JSON format. Click the  icon to copy the JSON.
- **Option.json:** import dashboard option settings in JSON format. Click the  icon to copy the JSON.

Delete a Flex board

1. In **Flex Board > Dashboard list**, click the  icon for the item to delete.
2. In the confirmation message, click the **Delete** button.

 Dashboard deletion behavior differs for owners and shared users.

- If the dashboard owner deletes a dashboard, it is deleted for all user accounts with whom it was shared.



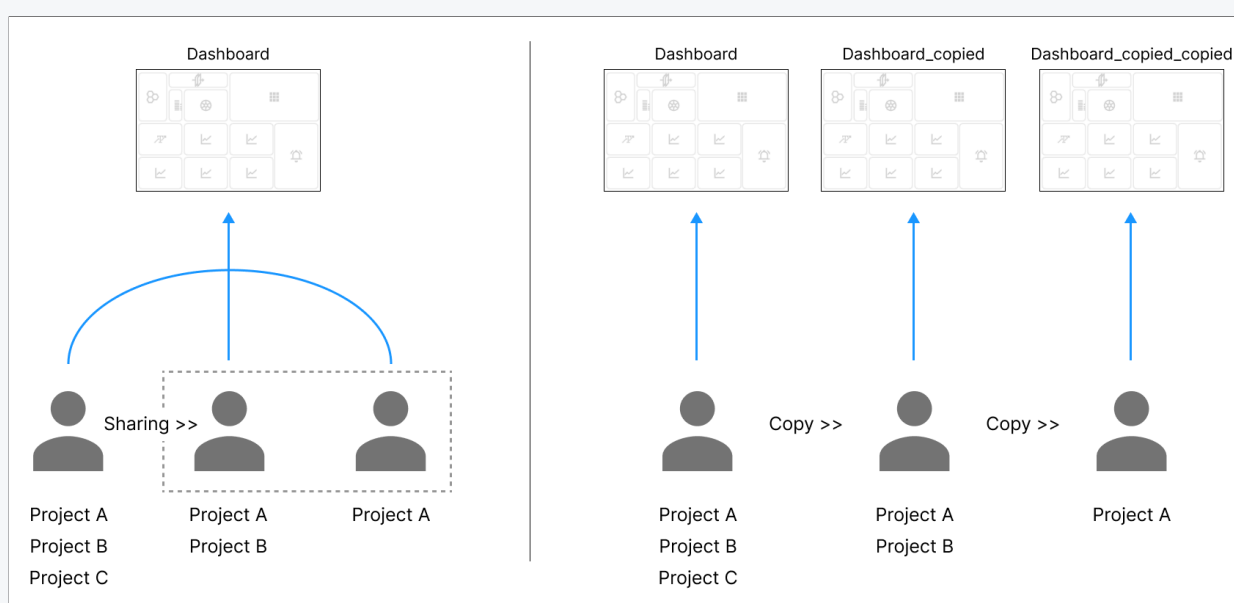
- If a user who received a shared dashboard deletes it, it is deleted only from that user's **Dashboard list**. The original dashboard remains.

Share a Flex board



- The Flex board sharing feature is available only in **Home > Integrated Flex Board**. It is not provided in a project's **Flex board** menu.

! Difference between share and copy



- Share: all members you share with view the same dashboard.
- Copy: if you copy a dashboard to another member or to yourself, you view a separate copied dashboard.
- Dashboards shared or copied as **Read only** cannot be edited. They can be edited only if shared as **Edit mode**.
- Members who receive a dashboard as **Read only** can also **re-share as read only** or **copy** that dashboard.



- You can share a dashboard only with members who belong to at least **one** of the projects included in the dashboard. Check whether the member to share or copy belongs to the relevant project.

☆ test

K8S-JINS-OKD-TEST, K8S-JINS-TEST-MICROK8S, DB-M...

Updated: 2023/12/22 11:10:24 AM



You can share a Flex board created in **Integrated Flex Board** with other members. When the owner edits a shared dashboard, the changes apply to all members it was shared with.

- In **Integrated Flex Board** under **Dashboard list**, click the icon for the dashboard to share.
- When the **Sharing a dashboard** window appears, select one or multiple members to share with, or enter accounts directly.
 - If you select **Read only**, members cannot edit the shared dashboard.
 - Share targets must belong to at least one of the projects included in the dashboard.
- Click the **Share** button.
 - Shared items display the **Shared** tag. Hover over the **Shared** tag to view information about the members you shared with.
 - Items shared as read only display the **Read only** tag.

When you receive a shared dashboard	When you share a dashboard (dashboard owner)



Dashboard sharing conditions

- The dashboard sharing feature is available only in **Home > Integrated Flex Board**.



- Anyone can share their own dashboard, and you can re-share or copy a dashboard you received.
- Dashboards received as **Read only** cannot be edited; dashboards received as **Edit mode** can be edited.
- If the **owner** deletes a dashboard, it is deleted for all accounts that received it.
- If a **recipient** deletes a dashboard, it is removed only from that user's **Dashboard list** and the original remains.
- For projects in a received dashboard where you do not have **View** permission, you cannot view data.

Copy a Flex board

Users can copy a Flex board and send it to other members.

1. In **Integrated Flex Board** under **Dashboard list**, click the  icon.
2. Choose a copy option.
 - **Copy to me:** copy to your own account.
 - a. An item with the `_copied` suffix is added to **Dashboard list**.
 - **Copy to others:** copy to another member's account.
 - a. Click **+ Account**.
 - b. Select the email of the member to copy to and click the **Copy dashboard** button.
 - c. An item with the `_copied` suffix is added to that member's **Dashboard list**.

Share as a JSON file

You can export Flex board settings to a JSON file to share with other members, or import settings from other members.

Export

1. Go to **Integrated Flex Board** or a project's **Flex board** menu.
2. In **Dashboard list**, click the  button.
3. Choose an export option.
 - **Include Project Information:** include dashboard project information in the JSON file when sharing.
 - **Except Project Information:** share without including dashboard project information in the JSON file.
4. Download the JSON file and send it to the member you want to share with.

Import

1. Go to **Integrated Flex Board** or a project's **Flex board** menu.
2. Click the  **Import** button at the top right.
3. Select the downloaded JSON file.

 Only members with **Edit** permission for the project can use this feature.

Flex board screen modes

Features vary by Flex board screen mode.

Accessible member permissions

Only users with **Edit** permission in a project's **Flex Board** menu can access **Edit Mode**, **Admin**, and **Filter**. For details on member permissions, see [the following document](#).

- **Project Edit** permission
- **Project flexboard update** permission
- **Site Admin** permission

Modes

Available features differ by **Flex Board** screen mode.

- **Edit Mode:** place widgets from the widget template list on the Flex board layout; edit, delete, or reposition widgets.
- **Admin:** manage widget properties in JSON format. Click the  button at the top right of a widget on the layout.
- **View mode:** after finishing layout, sizing, and detailed options, monitor each widget's data in real time like a dashboard.

Common features

- Data filtering
- Real time data time range settings
- Print mode
- Flex board management
- Data merge options

Data filtering

Use data filtering to narrow monitoring targets and build an efficient Flex board.

1. At the top of the screen, click the  **Filter** tab.
2. In the **Filter** window on the right, select filter targets. To select all filter targets, choose **Select all**.
 - **Agent** option: select agent types or an application list, with **Search** available
 - **Metrics** option: select a project or agent type; add **+ And** conditions, or auto select by string with **Contain** or **Exclude**
3. After selecting filter targets, click the **Apply** button.
4. Save frequently used conditions with the **Save filter** button.
 - a. Enter a filter name and select **Save**. **Saved filters** appears at the bottom of the **Filter** window.

Filtering conditions

Filtering conditions are divided into agent type and metrics type.

Agents provide only basic monitoring targets as selectable options, while metrics provide selectable tags for all metrics data collected in the project. The metrics type is useful when you collect data in a non agent form and want to apply filtering. For details on metrics, see [the following document](#).

Type	Agent	Metrics
Selection options	WhaTap project monitoring targets (applications, servers, databases, containers, Kubernetes PODs and NODEs)	All metrics tags including agents
Scope	All widgets	All widgets that use metrics data
Filtering method	Checkboxes	Equal, Contain, Exclude

Set the lookup time

Use the time selector at the top right of **Flex Board** to set data lookup time for widgets.

- : stop real time mode and set a specific lookup time
- : switch back to real time mode

Print

You can save the Flex board screen as a PDF and print it.

1. On the Flex board screen, click the  icon at the top right to switch to print mode.
2. Configure options.
 - **Viewing filter options:** toggle filter options on the screen
 - **Convert to {mode} orientation / Convert to {mode} orientation:** change orientation to horizontal or vertical
3. After finishing, select **PDFDownload**.

4. To exit print mode, click the  **Exit print mode** at the top right.

Flex board management

You can change the Flex board layout; move, resize, or rename widgets; and use other management features. You can also open **Flex board management** by clicking the  icon in **Dashboard > Flex Board** under **Dashboard list**.

1. On the Flex board screen, click the  icon at the top right to open the **Flex board management** window.
 - **Rename:** change the Flex board name
 - **Layout:** move, resize, and delete widgets
 - **Don't Allow Other Users to Modify.:** restrict modifications
 - Members with edit permission can edit, delete, and modify; if you enable the option, it changes to **Don't Allow Other Users to Modify.: On**
 - **Widget.json:** edit and manage widgets on the Flex board in JSON
 - **Option.json:** edit and manage Flex board settings in JSON (project info, Flex board filters, time selection, and other settings)

 The **Widget.json** and **Option.json** features are available only to dashboard administrators.

2. After completing all settings, click the **Save** button.

Add a dashboard to favorites

You can add a Flex board you created to favorites for quick access. In **Dashboard > Flex Board** under **Dashboard list**, click the  button for the dashboard to add. It changes to .

Managing The Widgets

You can customize your dashboard by handling the widgets placed on the Flex board.

- ✓ You can build dashboards using various widget templates, including metrics widgets.
For details on the features and usage of each template, see the [Widget template](#) document.

Adding a widget

You can add any widget to the created Flex board.

1. In **Dashboard list** of **Flex Board**, select a dashboard to add the widget.
 2. On the upper left of the screen, select **Edit Mode**.
 3. Select a desired widget from the **Widget templates** list on the left. To add a metrics widget, select **All metrics** and then click a desired widget.
- If you have entered **Integrated Flex Board** on the Home screen and added a widget, click **Project selection** and then select target projects to collect.
 - If you have more widgets to add, repeat the same procedure.
4. After all steps are finished, select **View mode** to check the layout and then select  (**Go to list**).

Changing the widget attributes

In **Dashboard list** of **Flex Board**, select a board to change the widget properties. It goes to **Edit Mode**.

Changing the widget name

1. On the right of the widget name to change, select .
2. Set the widget values for **Title**, **Font size**, and **Color**, and then select **Save**.

- If the **Apply to the entire widget** toggle button is enabled, the font size and color are applied to other widgets.
- To lock the widget title, select [Configuration icon](#) and then click **Save**.

Time Setting

1. On the upper right of the widget to set the time, select ⌚.
2. Set the time in the **Select a time** window.
 - To apply the set time to the dashboard, check **Use dashboard settings**. The time setting on the dashboard is located on the upper right.
 - To apply a desired time setting, uncheck **Use dashboard settings**. Use < or > to set the desired time.
3. After setting the time, select ✕.

ⓘ Depending on the data type of the widget, the time setting may not be available.

Setting the output data options

By setting the output data options of the chart widget, you can select the desired data.

1. At the top right of the widget, click the ⋮ icon to configure the output data options.
 - You can filter data by selecting types for project, agent, application, etc.
 - You can change the type of the graph displayed on the chart by selecting individual or merged data.
 - Select ⋮ > ⚙️. You can change the option details through the **Chart settings** window. The options that can be set are as follows.
 - **Chart type:** This option allows you to display the current aggregated figures on the chart.
 - **y axis Chart max value:** The chart maximum value on the Y axis can be selected with one of **Auto** and **Fix**.
 - **Set horizontal line:** Select **Add** to display the threshold or range as a horizontal line. You can

apply multiple items added. After adding the horizontal line, select **Apply** to apply it to the chart.

- **Show chart max value:** The maximum value of the graph is displayed on the chart.
 - **Sub-chart:** You can add a sub-chart to the main charts of the widget. Select a type of sub-chart and then select its layout, size, and whether or not to merge data. To apply to other widgets, select **Apply to the entire widget**. Sub-charts are useful to view data in various ways.
2. After setting all options, on the left of the **Chart settings** window, click **×** or click the outside of the **Chart settings** window.

ⓘ Depending on the widget's data type, available options may differ.

Changing the metrics widget data

You can change the data query conditions of the metrics widget.

1. In **Flex Board > Dashboard list**, select the dashboard where you want to change the widget data.
2. In **Edit Mode**, click the **⋮** icon at the top right of the widget you want to modify.
3. Click the **<>** icon to open the data settings edit window.
4. Change the settings referencing the following, and then select **< Apply to the widget**.
 - Metrics options that are created by default when creating a widget appear on the tab.
 - Metrics options are **Category**, **Field**, and **Tag**.
 - The **Category** currently restricts the editing function.
 - In **Field** and **Tag**, multiple items can be selected. The chart data is grouped using the selected tag options.
 - Select **🔍** to query the original data.
 - For more information about **Object Merge** and **Time merge**, see the [Data merge options](#).

Data merge options

The metrics widget placed on the **All metrics** list of the Flex board provides the data merge options. Data merge provides the following methods: **Object Merge** and **Time merge**.

- **Object Merge**

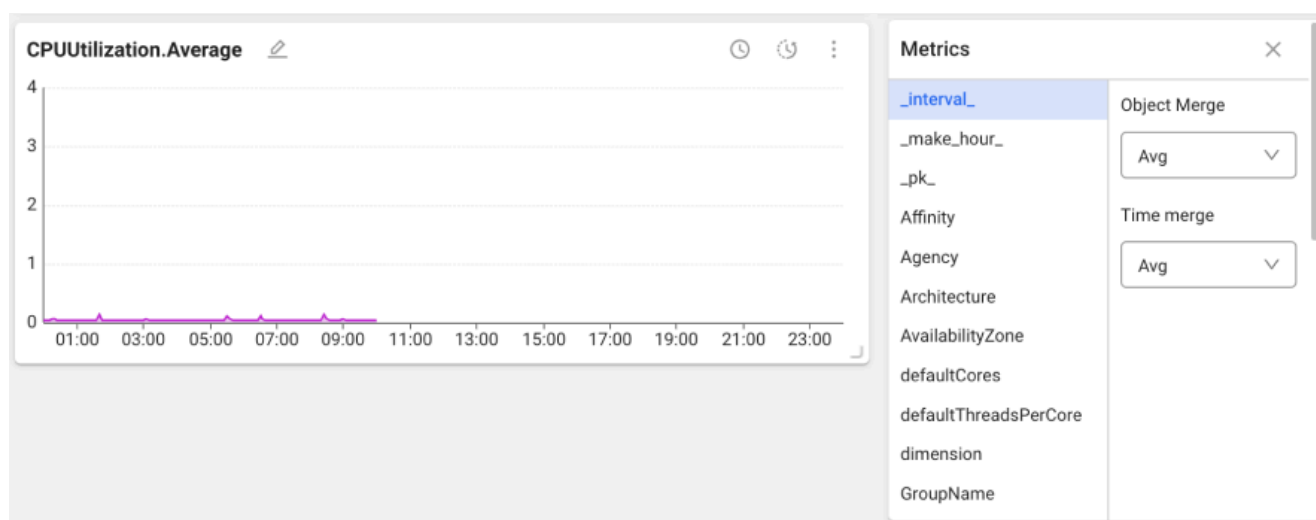
It is used to group the chart data based on the tag (e.g. agent name) selected on the left. At this time, if the tags match among the data with different fields (e.g. CPU), the corresponding data is merged.

- **Time merge**

It is mainly used if the lookup time is too long. Data with the same fields in the original data are merged at regular time intervals (5 minutes or 1 hour) depending on the time range. This method is called "Time Merge."

- **AWS ColudWatch Metrics**

In case of AWS monitoring metrics, the statistical method is added after the field name in the form of suffix. Data merging defaults reference this suffix.



1. In **Edit Mode**, select **All metrics** and then change the **Widget templates** list to the **All metrics** list.
2. Place the metrics widget on the layout.
3. On the upper right of the metrics widget, select **:**.
4. If a tag (e.g. agent name) option is selected, the data merge options appear. Depending on the widget size, the metrics option's location may differ.

Copying a widget

1. Click  on the upper right of the widget.
2. Click .
3. If the **Copy** window appears, click **+ Add widget**.
4. Change the widget name in the list.
5. Click **Apply**.
6. In **Edit Mode**, you can see the copied widget.

Delete Widget

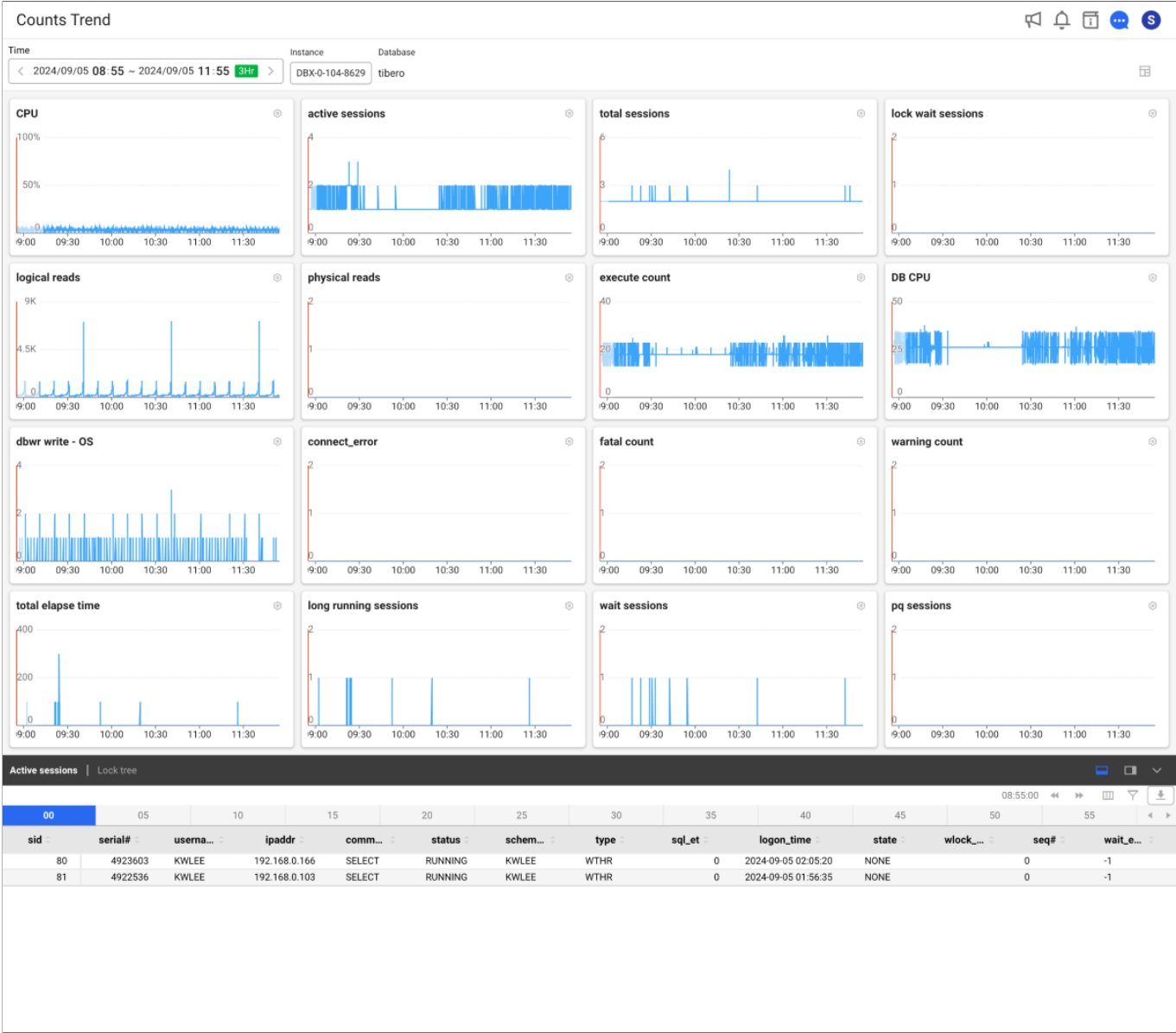
1. Click  on the upper right of the widget.
2. Click .
3. If the confirmation message appears, click **Delete**. To cancel the deletion, select **Cancel**.

Count Trend And Comparison

Counts Trend

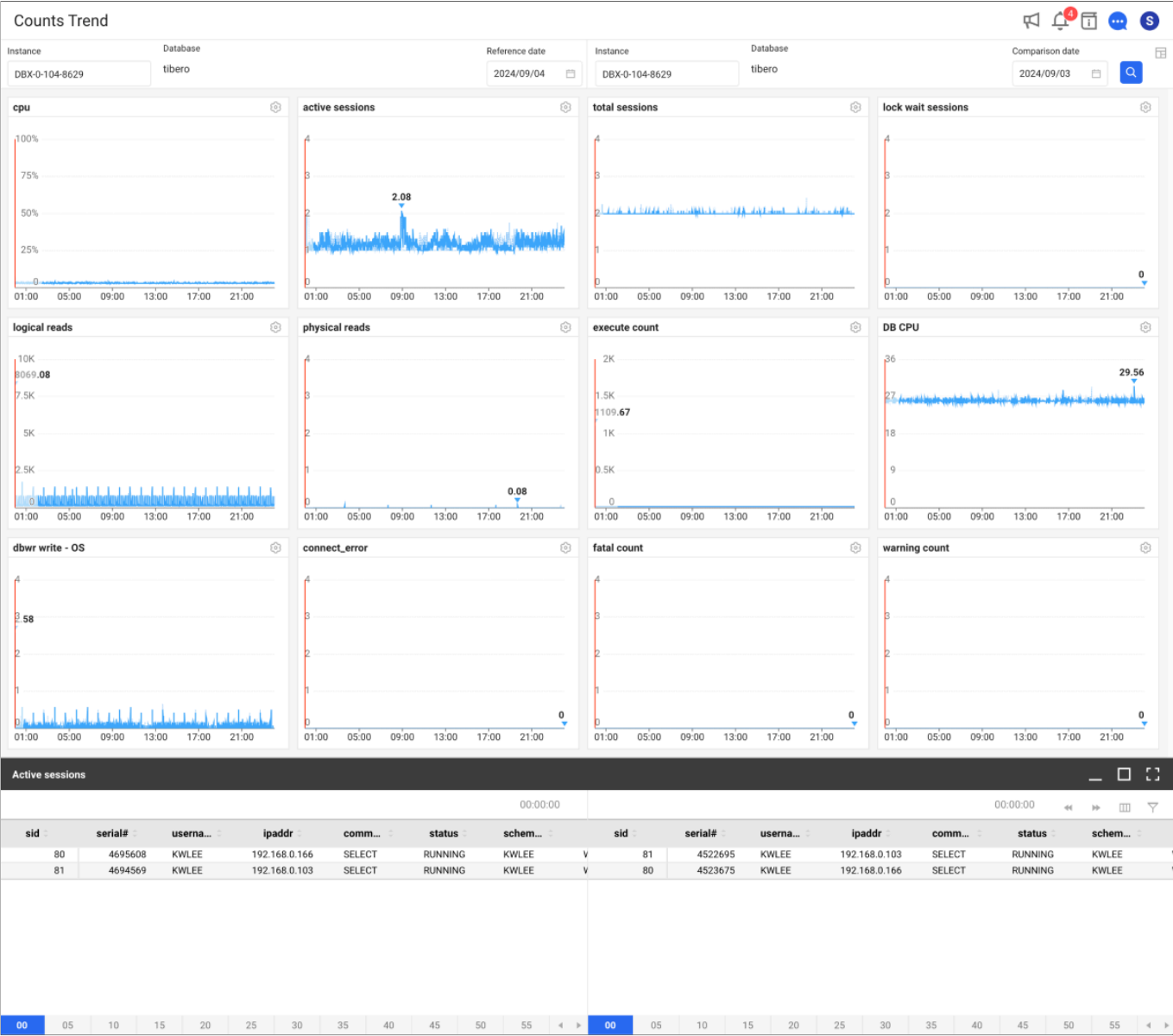
Home > Select Project > **Analysis** > **Counts Trend**

You can check the operation trend of the key metrics of the database over time and trace the performance. You can check the current active session data and distinguish the long-running sessions.



Comparison between count trends

Home > Select Project > Analysis > Counts Trend Comparison



You can compare the count trends for different dates.

1. Select the desired instances from the Instance area. You can also select different instances.
2. Set values for Reference Date and Comparison Date.
3. Select .

Using the chart and active session area

Select  on the screen. In the **Layout setting** window, set it to **1 x 3** and then select **Save**. **Time** must be set to **Last 24 hours**. You can see the database key metrics in detail for the day, as follows:



- In **1 Time**, set a desired time interval.

- Click the green icon to select a search time.
- With the lookup period selected, select < or > . Then you can change the lookup time at the set time intervals.
- If you select the date and time, you can set the desired time in detail. After configuration, select **Confirm**.
- **2 Instance:** You can select an instance that is connected with the project.
- If you click a specific time point of the metrics chart, the (number3) area appears with red lines and the collected active sessions can be also displayed.
- To change the metrics in the chart, select ⚙ on the upper right.
- The active session data is collected every 5 seconds. You can search the data by selecting the 4 5-second cells at the bottom of the screen.
- To move the time by 1 minute, select 5 ⏪ or ⏩ .
- 5 ☐: The column header entries in the table can be displayed or hidden.
- 5 ⚙: You can filter the list based on the column header entries in the table. After selecting the button, you can set the conditions in each header column such as **Includes**, **Excludes**, **Equal**, and **Unequal**.
- 5 ⬇: You can download the content of the table as a CSV file.

Column information guide

For more information about columns, see [the link](#).

- **Active session** Lock tree Process information

Item	Description
action	Name of the running job.
block_updates	Number of block updates.
block_updates_sigma	Total number of block updates.
client_identifier	Client ID.
client_info	Additional information of the client.

Item	Description
client_pid	PID of the client process.
command	Command running in the current session.
consumed_cpu_time	CPU time consumed by the session.
consumer_group	Consumer group to which the session belongs.
cpu(xos)	CPU utilization
cpuusage	CPU usage consumed by the session.
event_name	Name of the waiting event.
execute_count	Number of SQL executions.
execute_count_sigma	Total number of executions.
id1	First identifier value.
id2	Second identifier value.
ioread(xos)	Actual time spent reading the block (milliseconds).
iowrite(xos)	Actual time spent writing the block (milliseconds)
ipaddr	Client IP address.
logon_time	Time when the session logged in the database.
logical_reads	Number of logical read operations.
logical_reads_sigma	Total number of logical read operations.
machine	Name of the machine on which the session is running.

Item	Description
module	Name of the running module.
os_thr_id	Thread ID of the operating system.
osuser	User of the operating system running the session.
parse_count_hard	Number of hard parses.
parse_count_hard_sigma	Total number of hard parses.
parse_count_total	Total number of parses.
parse_count_total_sigma	Total number of parses.
pdml_enabled	Whether parallel DML is enabled or not.
pdml_status	Status of the parallel DML.
pddl_status	Status of the parallel DDL.
pga_used_mem	Amount of memory being used in the process global area (PGA).
physical_reads	Number of physical read operations.
physical_reads_sigma	Total number of physical read operations.
pid	PID of the database process.
pq_status	Status of the parallel query.
prev_sql	Text of the previously executed SQL statement.
prev_sql_id	Unique ID of the previously executed SQL statement.
prev_sql_param	Parameter of the previously executed SQL.

Item	Description
prog_name	Name of the program running the session.
pss(xos)	Process specific memory usage + Percentage of shared memory occupied by one process.
row_wait_block_no	Block number of the waiting row.
row_wait_file_no	File number of the waiting row.
row_wait_obj_id	Object ID of the waiting row.
row_wait_row_no	Row number of the waiting row.
rss(xos)	Resident Set Size (RSS) that is the number of physical pages associated with the process.
schemaname	Name of the schema the session is using.
seq#	Value indicating the sequence number of the session.
sid	Session ID that uniquely identifies the session.
sql_et	SQL execution time.
sql_hash	Hash value of the SQL statement.
sql_id	Unique ID of the SQL statement being executed.
sql_param	Parameters used to execute SQL.
sql_text	Text of the SQL statement being executed.
sql_trace	Whether to trace SQL.
state	Current state of the session.

Item	Description
status	Status of the session.
terminal	Name of the terminal to which the session is connected.
type	Type of the session.
usn	Undo segment number.
used_blk	Number of used blocks.
used_rec	Number of used records.
wait_event	Event that the session is waiting for.
wait_time	Waiting time.
wlock_wait	Whether the session is waiting for a lock or not.
wthr_id	Thread ID of the session's work.

Item	Description
event	Name of the waiting event.
holder type	Type of the session that owns a lock.
id1	First identifier value.
id2	Second identifier value.
lock mode	Lock mode requested or owned by the current session.
lock request	Status of the lock requested by the session.
module	Name of the running module.

Item	Description
pid	PID of the database process.
prev_sql_id	Unique ID of the previously executed SQL statement.
prev_sql_param	Parameter of the previously executed SQL.
prev_sql_text	Text of the previously executed SQL statement.
prog_name	Name of the program running the session.
serial#	Serial number that distinguishes repeated attempts for the same session.
sid	Session ID that uniquely identifies the session.
sql_et	SQL execution time.
sql_id	Unique ID of the SQL statement being executed.
sql_param	Parameters used to execute SQL.
sql_text	Text of the SQL statement being executed.
status	Status of the session.
username	Name of the user running the session.
waiter type	Type of the session waiting for a lock.

The following items are the metrics collected if the XOS agent has been installed.

Item	Description
cputime	CPU usage time
cpuusage	CPU Utilization

Item	Description
elapsed	Elapsed time of CPU usage
vsize	Virtual memory size (Kb)
rss	Resident Set Size (RSS) that is the number of physical pages associated with the process.
state	Process status
ioread	Actual time spent reading the block (milliseconds)
iowrite	Actual time spent writing the block (milliseconds)
pss	Process specific memory usage + Percentage of shared memory occupied by one process
uid	user id
cmd	Executing command
longcmd	Full path of cmd

ⓘ WhaTap basically stores the client-related information.

Lock Tree

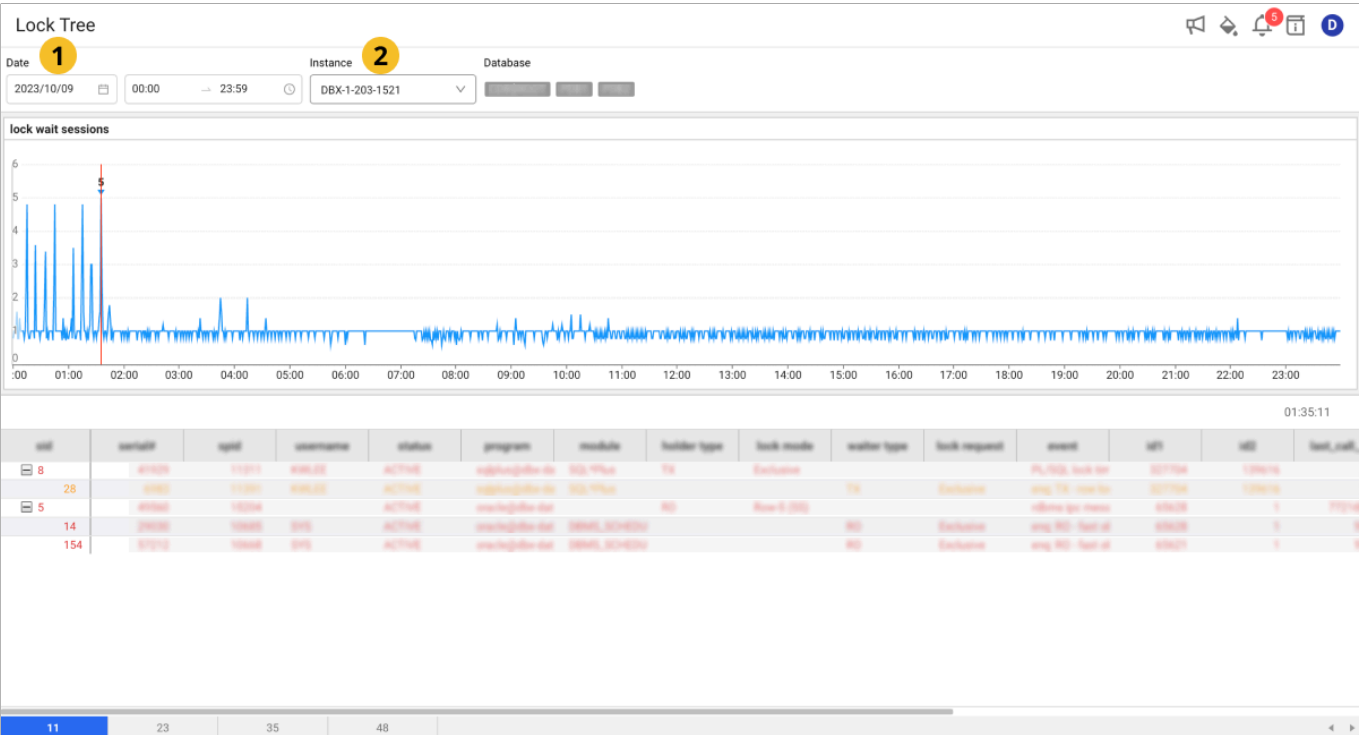
Home > Select Project > **Analysis** > **Lock Tree**

This tool analyzes the trend of locks that occurred during the day. This function allows you to visually check the tree structure of the session that generated the lock (lock holder) and the session waiting for the lock (lock waiter). You can analyze the relationship between the holder and waiter of the lock that occurred at a specific time point. Through the WhaTap's **Lock Tree** feature, the DB administrator can identify and resolve the DB lock issues and optimize the DB performance.

Key features are as follows:

- **Lock trend analysis:** The trends of locks that occurred during the set search period are traced over time and displayed in a graph. This allows you to visually check how the locks are created and resolved.
- **Check lock holder and waiter:** You can see the holder and waiter for each lock in a tree structure. Through this, when a specific lock occurs, you can check the relationship between the session that generated the lock and the waiting session.
- **Inter-session relationship analysis:** By analyzing the relationship between the session that generated the lock and the waiting session, you can identify the cause of the lock that occurred during the query execution and transaction handling.
- **Visual lock trend by time:** Through the **1-Min Lock Trends** and **Lock Wait Sessions** features, the lock occurrence data can be analyzed in time zones.

Basic usage guide



1. Select the date to view and set the time in **Time** at the top of the screen.
2. Select an instance to monitor.

You can check the lock that occurred during the set time on the selected instance.

If any lock occurs during the set period, you can analyze whether locks are concentrated in a specific time period or whether a specific session continuously causes locks in the **Lock Wait Sessions** graph and the table at the bottom.

- You can see the data in 5-second increments by dragging within 3 hours on the chart. However, the data in 5-second increments can only be viewed within the most recent month. The data earlier than one month can only be viewed as 5-minute summary data. For example, you can drag (drill down) lock tree data from 40 days ago for the 5-minute summary data, but you cannot see 5-second data.

Lock Wait Sessions

The [Lock Wait Sessions](#) feature allows you to analyze the lock wait sessions. Depending on the query period, the lock wait session data is provided at 5-minute intervals when the query is for 3 hours or more, and at 5-second intervals when the query is for less than 3 hours. You can also adjust the time range by dragging the chart flexibly.

1-Min Lock Trends

If you click a specific time zone in [Lock Wait Sessions](#), the lock occurrence status for 30 minutes, from 15 minutes before to 15 minutes after is visualized. This allows you to effectively analyze the lock occurrence trend at 30-minute intervals.

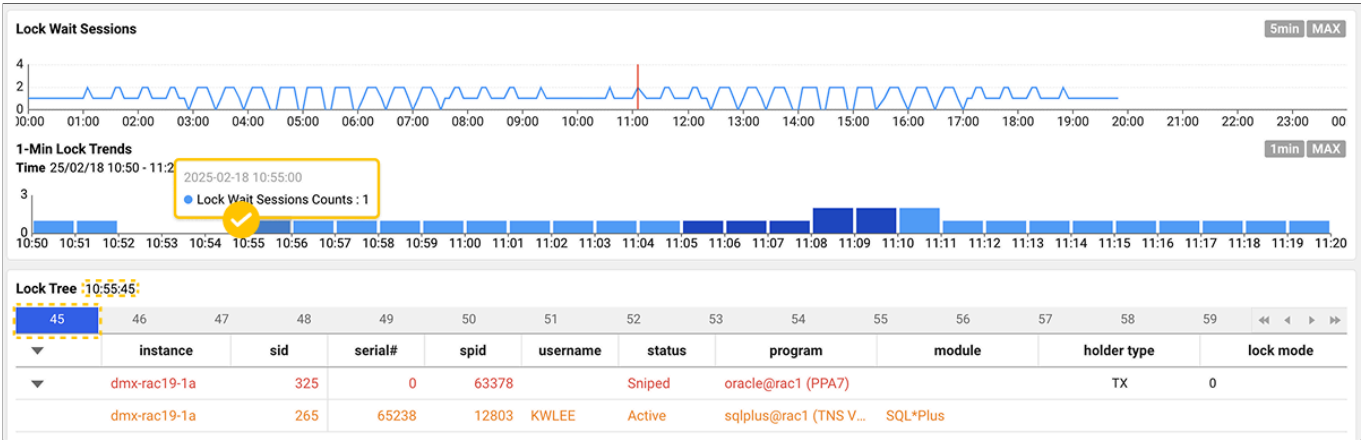
! **Total Locks** indicates the total number of locks generated in the time zone.

Viewing time

[1-Min Lock Trends](#) and [Lock Tree](#) tables are timed based on the maximum number of locks that occurred at the clicked time in [Lock Wait Sessions](#). This allows you to find the zone with the most locks.



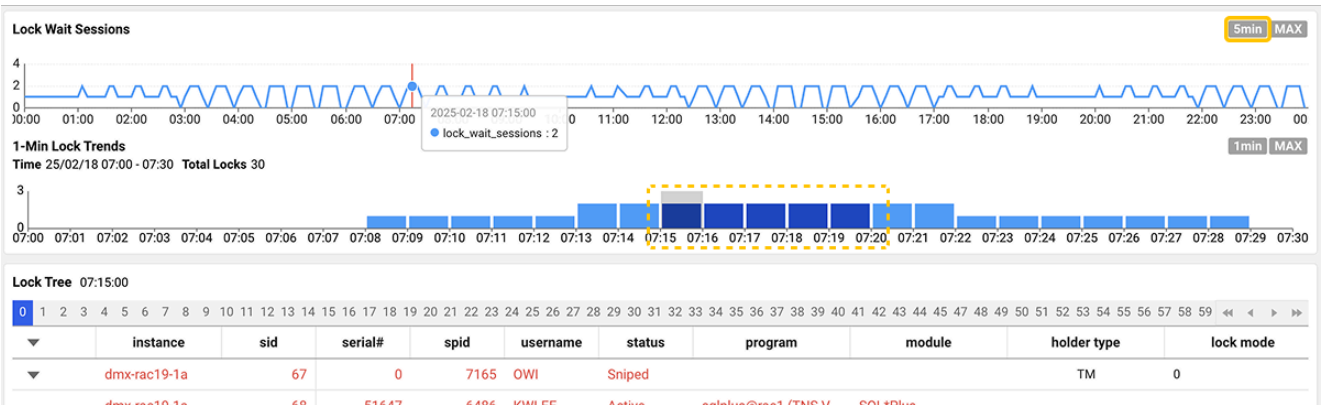
If you click the bar of a different time zone in the [1-Min Lock Trends](#) chart with the [Lock Wait Sessions](#) unchanged, the time range is synced to the [Lock Tree](#) table by using the seconds with the highest number of locks for the minute. This allows you to see the information reflected in the [Lock Tree](#) table when changing the time zone.



- **Viewing for 3 hours or more (using 5-minute data)**

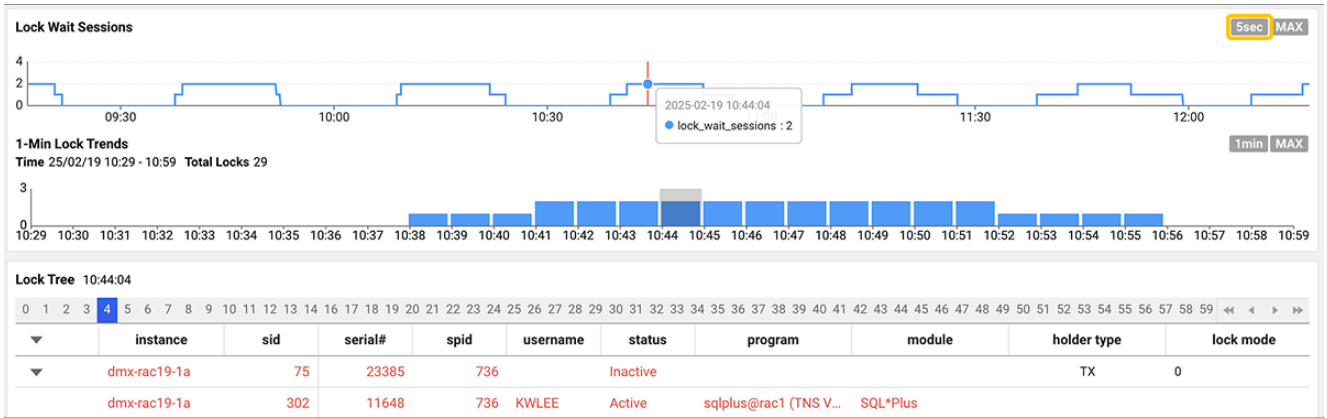
The bar color of the 5-minute zone from the time of inquiry appears more prominent.

When the 07:15:00 time point is clicked, the color of the 07:15:00-07:20:00 zone's bar chart appears more prominent.



- **Viewing for less than 3 hours (using 5-minute data)**

It is useful for analyzing the locks that occur within short time intervals.



Column information guide

Details for each session are provided in the following columns:

Item	Description
event	Name of the waiting event.
holder type	Type of the session that owns a lock.
id1	First identifier value.
id2	Second identifier value.
lock mode	Lock mode requested or owned by the current session.
lock request	Status of the lock requested by the session.
module	Name of the running module.
pid	PID of the database process.
prev_sql_id	Unique ID of the previously executed SQL statement.
prev_sql_param	Parameter of the previously executed SQL.

Item	Description
prev_sql_text	Text of the previously executed SQL statement.
prog_name	Name of the program running the session.
serial#	Serial number that distinguishes repeated attempts for the same session.
sid	Session ID that uniquely identifies the session.
sql_et	SQL execution time.
sql_id	Unique ID of the SQL statement being executed.
sql_param	Parameters used to execute SQL.
sql_text	Text of the SQL statement being executed.
status	Status of the session.
username	Name of the user running the session.
waiter type	Type of the session waiting for a lock.

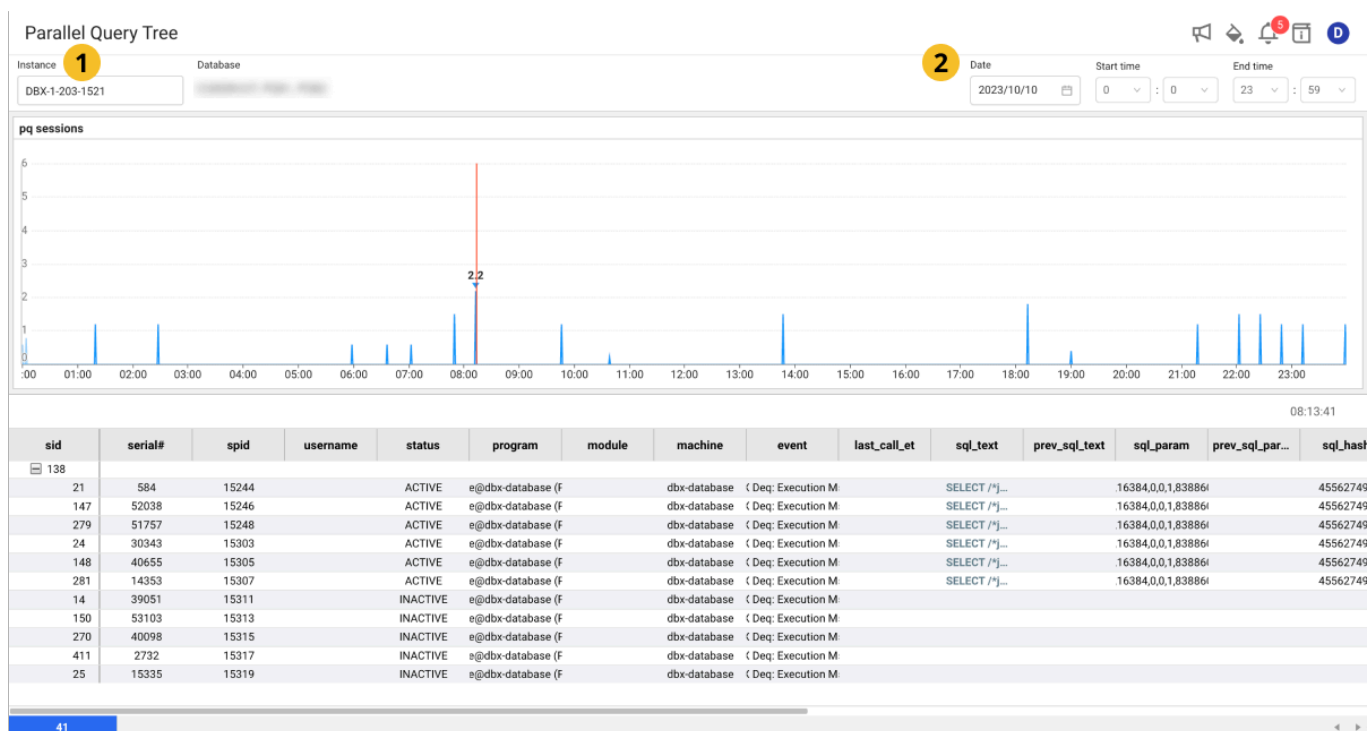
❗ WhaTap basically stores the client-related information.

Parallel Query Tree

Home > Select Project > **Analysis** > **Parallel Query Tree**

Parallel Query Tree provides the function to analyze the trend of parallel queries per day. The slave processes that perform actual tasks and the coordinator processes that assign tasks to them are distinguished, and overall executions are displayed in an easy-to-understand manner. It can help determine what purpose it was used for by providing information about parallel queries performed at a specific time point.

Basic screen guide



In **1 Instance**, select the instance to search parallel queries from, and then **2** set the **Date**, **Start time**, and **End time**.

You can check the trend of parallel queries that meet the set conditions through a graph chart, and the structure of coordinators and slaves is represented in the form of tree.

Column information guide

Item	Description
<code>block_updates</code>	Number of block updates.
<code>client_pid</code>	PID of the client process.
<code>event</code>	Name of the waiting event.
<code>logon_time</code>	Time when the session logged in the database.
<code>logical_reads</code>	Number of logical read operations.
<code>machine</code>	Name of the machine on which the session is running.
<code>module</code>	Name of the running module.
<code>physical_reads</code>	Number of physical read operations.
<code>pid</code>	PID of the database process.
<code>prev_sql_param</code>	Parameter of the previously executed SQL.
<code>prev_sql_text</code>	Text of the previously executed SQL statement.
<code>prog_name</code>	Name of the program running the session.
<code>seq#</code>	Value indicating the sequence number of the session.
<code>sid</code>	Session ID that uniquely identifies the session.
<code>sql_et</code>	SQL execution time.
<code>sql_param</code>	Parameters used to execute SQL.

Item	Description
sql_text	Text of the SQL statement being executed.
status	Status of the session.
usn	Undo segment number.
used_blk	Number of used blocks.
used_rec	Number of used records.
username	Name of the user running the session.
wait_time	Waiting time.

! WhaTap basically stores the client-related information.

To check the changes between the current time and the selected past date at a glance, select **View Changes**.

Database Parameter

Reference date

2024/06/14

Comparison date

2024/05/19

Instance

DBX-0-104-8629

View Changes

	2024/06/14 12:59:48 Today	2024/05/19 00:00:00
Key	Value	Value
FLASHBACK_LOG_ARCHIVE_FORMAT	fb-t%t-r%s-s.arc	
SEPARATION_OF_DUTIES	NO	
USE_SSVR	NO	
RMGR_TAR_PATH		
RMGR_BACKUP_DEST	/home/tibero/tibero6/database/tibero/backup/	
STAR_TRANSFORMATION_ENABLED	FALSE	
DB_CACHE_ADVICE	NO	
IP_VERSION	0	
BLOCK_CHANGE_TRACKING		
SQL_TRANSLATION_PROFILE		
ACT_LOG_FILE_SIZE	104857600	
ACT_LOG_DEST	/home/tibero/tibero6/instance/tibero/dump/act/	
CPU_COUNT	0	
RSRC_CONTROL_THRESHOLD	90	
RSRC_CHECK_INTERVAL	3	
USE_RESOURCE_MANAGER	NO	

✔ Comparing database parameters for today

Reference date

2024/06/14

Comparison date

2024/06/14

Instance

DBX-0-104-8629

View Changes

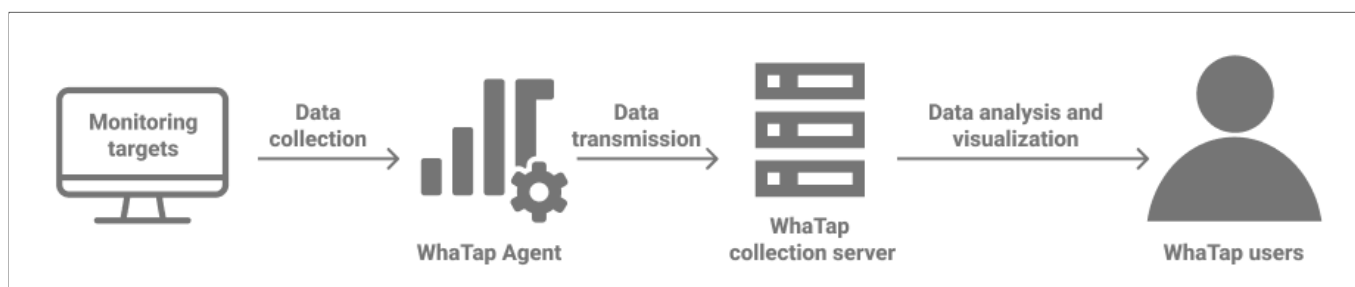
	2024/06/14 12:59:00 Today	2024/06/14 01:32:37 Today
Key	Value	Value
FLASHBACK_LOG_ARCHIVE_FORMAT	fb-t%t-r%s-s.arc	fb-t%t-r%s-s.arc
SEPARATION_OF_DUTIES	NO	NO
USE_SSVR	NO	NO
RMGR_TAR_PATH		
RMGR_BACKUP_DEST	/home/tibero/tibero6/database/tibero/backup/	/home/tibero/tibero6/database/tibero/backup/
STAR_TRANSFORMATION_ENABLED	FALSE	FALSE
DB_CACHE_ADVICE	NO	NO
IP_VERSION	0	0

If you set both **Reference date** and **Comparison date** to the date for today, you can view and compare the real-time data and the last saved data. The storage time of the last data may differ depending on the database server environment.

Metrics

What is the metrics?

WhaTap collects data from monitoring targets and provides them to users. The data collected from agents is called **metrics**.



Metrics consists of the following components:

- **Category**: A group of related metrics
- **Tags**: Data containing unique identifiers to find the targets to collect
- **Fields**: Metrics collected from the agent
- **Time**: Time when the metric has been collected
- **Oid**: Unique number of the agent that has collected metrics

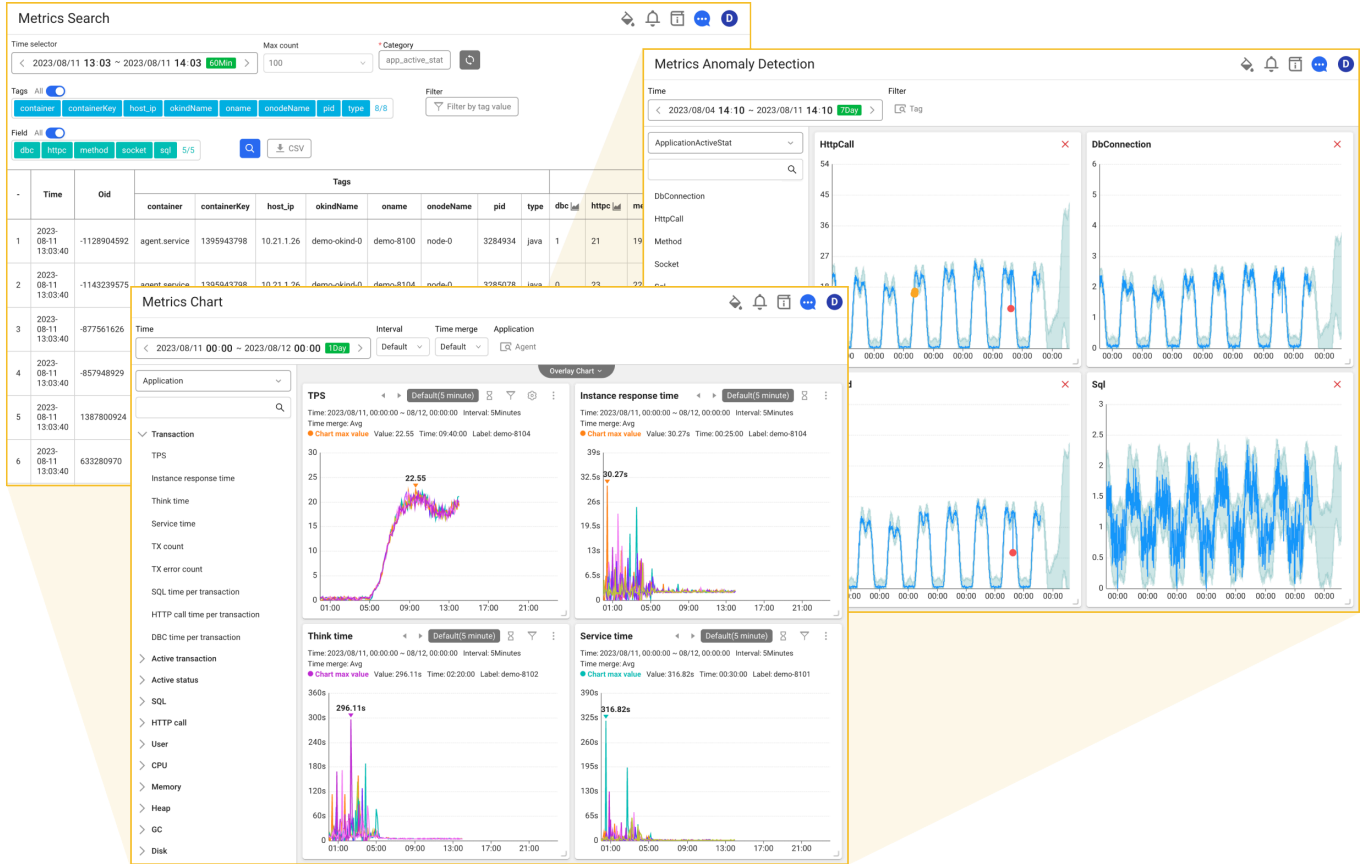
To view collected data, select a project on the Home screen, and then select [Sitemap](#) > [Metrics Search](#).

For example, select a category named `db_tibero_counter` and view the related metrics. You can see the **(tags)** and **(fields)** that correspond to the category as follows.

Viewing and visualizing the metrics data

WhaTap provides a list of original data collected according to the conditions specified by user and various charts

visualized for convenience as follows. See the menus such as **Metrics Search** that can look up the original data of metrics, **Metrics Chart** that can look up metrics data through visualized charts, and **Metrics Anomaly Detection** that can detect out-of-pattern anomalies by comparing with the patterns of metrics learned by AI.



Tibero Metrics

Database metrics are a comprehensive collection of database workloads and resource usages. The WhaTap monitoring service continuously collects metrics to identify bottlenecks in the database and provides data to help identify the root causes of performance issues.

For more information about columns, see [the link](#).

agent_status_summary

This category collects metrics related to agent status every 10 seconds.

Fields

Field	Type	Unit	Description
inActTime	-	Millisecond(ms)	Amount of time the agent remains inactive
isActive	Boolean	-	Whether the agent is active or not
isRestart	Boolean	-	Whether the agent was restarted recently (<code>true</code> / <code>false</code>)
lastActTime	-	Millisecond(ms)	Last time when the agent was activated (<code>0</code> : Disabled)
oid	-	-	Unique IDs for each agent in the project
startTime	-	Millisecond(ms)	Timestamp when the agent was started.

db_tibero_counter

Tags

The following lists the tags that are collected in the `db_tibero_counter` category.

Tag	Description	Remarks
<code>agentIp</code>	IP address per agent.	-
<code>dbIsMulti</code>	Whether to support the multitenant or not.	-
<code>dbName</code>	Database name.	-
<code>dbType</code>	Database type.	-
<code>dbVersion</code>	Version of the database in use.	-
<code>oname</code>	Agent name	Unique value

Field

The following lists the fields that are collected in the `db_tibero_counter` category.

Metrics	Description
<code>active_sessions</code>	Number of active sessions.
<code>block_updates</code>	Number of occurrences of block update.
<code>connect_error</code>	Number of connection errors occurred.
<code>DB_CPU</code>	Percentage of CPU used by the database.
<code>DB_CPU_time</code>	Total time (in milliseconds) the database spent on CPU processing.

Metrics	Description
dbwr_write_-_OS	Number of database creation tasks executed by the operating system.
execute_count	Number of executions of the SQL command.
fatal_count	Number of fatal errors.
lock_wait_sessions	Number of sessions waiting for locks.
logical_reads	Number of logical read operations that occurred.
logons_cumulative	Number of cumulative logins.
long_running_sessions	Number of long running sessions.
parse_count_(hard)	Number of hard parsing operations that occurred.
parse_count_(total)	Total number of parsing operations that occurred.
physical_reads	Number of physical read operations that occurred.
pq_sessions	Number of sessions in which parallel query operations were executed.
sorts_(memory)	Number of sorting operations occurred in memory.
the_number_of_user_commits_performed	Number of user commits executed.
total_elapse_time	Total elapsed time.
total_sessions	Total number of sessions.
wait_sessions	Number of waiting sessions.
warning_count	Number of warnings occurred.

Metrics	Description
WE_BUF_FREE_time_waited	Total time for the process to wait for the buffer to be cleared.
WE_BUF_FREE_total_timeouts	Number of timeouts that occurred while waiting to empty the buffer.
WE_BUF_FREE_total_waits	Total number of waits due to buffer emptying events.
WE_BUF_WAIT_time_waited	Total time spent in buffer waiting events.
WE_BUF_WAIT_total_timeouts	Number of timeouts that occurred while waiting for the buffer.
WE_BUF_WAIT_total_waits	Total number of waits due to buffer waiting events.
WE_BUF_WRITE_time_waited	Total time spent in buffer write events.
WE_BUF_WRITE_total_timeouts	Number of timeouts that occurred during buffer writing.
WE_BUF_WRITE_total_waits	Total number of waits due to buffer writing events.
WE_CKPT_WAIT_time_waited	Total time waiting in checkpoint waiting events.
WE_CKPT_WAIT_total_timeouts	Number of timeouts that occurred while waiting for the checkpoint.
WE_CKPT_WAIT_total_waits	Total number of waits due to checkpoint waiting events.
WE_LGWR_ARCHIVE_time_waited	Total time the logger waited for archive tasks.
WE_LGWR_ARCHIVE_total_timeouts	Number of timeouts that occurred during logger archive operations.
WE_LGWR_ARCHIVE_total_waits	Total number of waits due to logger archive operations.
WE_LGWR_LNW_time_waited	Total time the logger waited for logs to be written over the network.
WE_LGWR_LNW_total_timeouts	Number of timeouts that occurred while writing to the logger via the network.
WE_LGWR_LNW_total_waits	Total number of waits due to logger writing operations via the

Metrics	Description
	network.
WE_LOG_FLUSH_REQ_time_waited	Total time taken to wait for log flush requests.
WE_LOG_FLUSH_REQ_total_timeouts	Number of timeouts that occurred during log flush requests.
WE_LOG_FLUSH_REQ_total_waits	Total number of waits due to log flush requests.
WE_LOG_FLUSH_SPACE_time_waited	Total time taken to wait for log flush space.
WE_LOG_FLUSH_SPACE_total_timeouts	Number of timeouts that occurred while waiting for log flush space.
WE_LOG_FLUSH_SPACE_total_waits	Total number of waits due to waiting for the log flush space.
WE_MBR_WAIT_time_waited	Total time taken to wait for MBR (Multi Block Read).
WE_MBR_WAIT_total_timeouts	Number of timeouts that occurred while waiting for the MBR.
WE_MBR_WAIT_total_waits	Total number of waits due to MBR waiting.
WE_PROC_DOWN_time_waited	Total time taken to wait for process termination.
WE_PROC_DOWN_total_timeouts	Number of timeouts that occurred while waiting for the process termination.
WE_PROC_DOWN_total_waits	Total number of waits for process termination.
WE_SEQ_FLUSH_time_waited	Total time while waiting for sequence flush.
WE_SEQ_FLUSH_total_timeouts	Number of timeouts that occurred while waiting for sequence flush.
WE_SEQ_FLUSH_total_waits	Total number of waits due to waiting for sequence flush.
WE_SEQ_FREESLOT_time_waited	Total time while waiting for sequence free slots.
WE_SEQ_FREESLOT_total_timeouts	Number of timeouts that occurred while waiting for sequence free

Metrics	Description
	slots.
WE_SEQ_FREESLOT_total_waits	Total number of waits for sequence free slots.
WE_SEQ_NEXTVAL_time_waited	Total time while waiting for sequence NEXTVAL.
WE_SEQ_NEXTVAL_total_timeouts	Number of timeouts that occurred while waiting for sequence NEXTVAL.
WE_SEQ_NEXTVAL_total_waits	Total number of waits for sequence NEXTVAL.
WE_SEQ_WRITEBACK_time_waited	Total time while waiting for sequence writing.
WE_SEQ_WRITEBACK_total_timeouts	Number of timeouts that occurred while waiting for sequence writing.
WE_SEQ_WRITEBACK_total_waits	Total number of waits for sequence writing.
WE_WLOCK_DML_time_waited	Total time taken to wait for DML locking.
WE_WLOCK_DML_total_timeouts	Number of timeouts while waiting for DML locks.
WE_WLOCK_DML_total_waits	Total number of waits for DML locks.
WE_WLOCK_TX_time_waited	Total time taken to wait for transaction locks.
WE_WLOCK_TX_total_timeouts	Number of timeouts while waiting for transaction locks.
WE_WLOCK_TX_total_waits	Total number of waits for transaction locks.
WE_WTHR_MSG_time_waited	Total waiting time for thread messages.
WE_WTHR_MSG_total_timeouts	Number of timeouts while waiting for thread messages.
WE_WTHR_MSG_total_waits	Total number of waits for thread messages.

Metrics	Description
<code>WE_WTHR_READY_time_waited</code>	Total waiting time while waiting for threads to be ready.
<code>WE_WTHR_READY_total_timeouts</code>	Number of timeouts that occurred while waiting for threads to become ready.
<code>WE_WTHR_READY_total_waits</code>	Total number of waits for threads to be ready.
<code>WE_WTHR_START_time_waited</code>	Total waiting time for threads to start.
<code>WE_WTHR_START_total_timeouts</code>	Number of timeouts while waiting for threads to start.
<code>WE_WTHR_START_total_waits</code>	Total number of waits for threads to start.

XOS-related metrics

The following describes the metrics collected from the XOS agent.

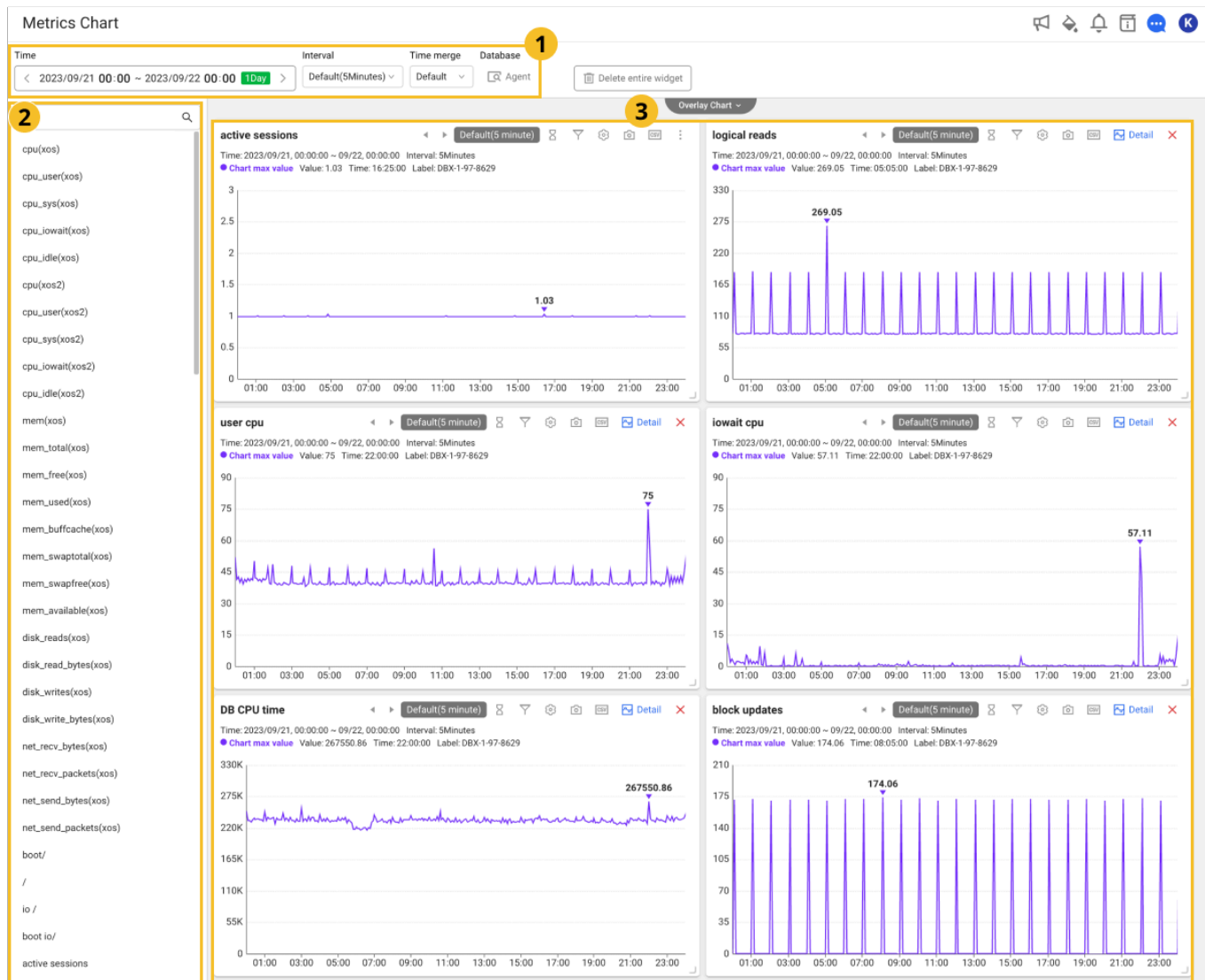
Metric	Unit	Description
<code>cpu(xos)</code>	pct	CPU utilization <code>cpu_user</code> + <code>cpu_sys</code> + <code>cpu_iowait</code>
<code>cpu_idle(xos)</code>	pct	CPU idle time
<code>cpu_iowait(xos)</code>	pct	CPU's I/O waiting time
<code>cpu_sys(xos)</code>	pct	CPU's kernel code execution time
<code>cpu_user(xos)</code>	pct	CPU's user code execution time
<code>disk_read_bytes(xos)</code>	byte	Number of data blocks read from disk
<code>disk_reads(xos)</code>	block	Number of buffers read from disk

Metric	Unit	Description
<code>disk_write_bytes(xos)</code>	byte	Number of pages written to disk
<code>disk_writes(xos)</code>	block	Number of buffers written to disk
<code>mem(xos)</code>	pct	Memory utilization
<code>mem_available(xos)</code>	MB	Shared memory size
<code>mem_buffcache(xos)</code>	MB	Amount of memory used by the buff/cache
<code>mem_free(xos)</code>	MB	Memory not in use
<code>mem_swapfree(xos)</code>	MB	Unused swap space size Because swap uses disk space, it may cause performance degradation.
<code>mem_swaptotal(xos)</code>	MB	Total swap size It is used when physical memory is insufficient.
<code>mem_total(xos)</code>	MB	Total memory size
<code>mem_used(xos)</code>	MB	Memory size in use
<code>net_recv_bytes(xos)</code>	byte	Amount of data transmitted over the network
<code>net_recv_packets(xos)</code>	count	Number of data packets transmitted over the network
<code>net_send_bytes(xos)</code>	byte	Amount of data transmitted over the network
<code>net_send_packets(xos)</code>	count	Number of data packets transmitted over the network

Metrics Chart

Home > Select Project > **Analysis** > **Metrics Chart**

In **Metrics Chart**, you can view the metrics data collected from the monitoring targets in a chart as follows. Specifying the time and metrics is required.



Options at the top

In the **1** area, you can specify the time range of the chart and the agent to be monitored through the options at the top of **Metrics Chart**.

- **Time:** You can specify the start and end of the X-axis as the total range in time.
- **Interval:** You can specify the X-axis data interval as the time interval.
- **Time merge:** As one of the data merging methods, you can merge data within the time specified by intervals.

For example, **Avg** indicates the average value of data within 1 hour.

-  **Agent:** You can specify the agents to query. If not specified, all items are queried.

 For more information on how to use the time selector.

Metrics list

The **2** area is a list of metrics to query for options. First select a **Category**. After querying the metrics under the selected **Category**, select a desired metric. If you select the **Category** and metric, Based on the data within the time range specified in the top menu of the area **1**, you can see the data via the chart widgets in the **3** area.

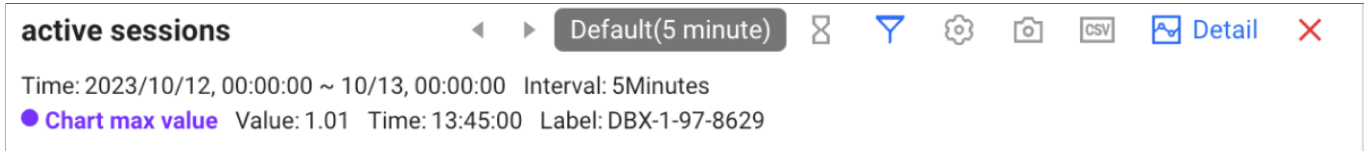
Data Merge

Data merge provides the following methods: **Object Merge** and **Time merge**.

- **Time merge** merges data with the same field values at regular intervals in the original data.
- **Object Merge** merges data with matching tags among data with different field values.

Chart widget

On the top left of **3**, you can see the metric name. On the top right of the chart widget, you can see the following options:



- Time movement: ◀ ▶ Using the left arrow button or right arrow button, it can be moved by -1 or +1 as much as the selected time range.

For example, if the time range is between 00:00 on February 13 and 00:00 on February 14, when you select the ◀ left arrow button, you can see the data within the time range between 00:00 on February 12 and 00:00 on February 13.

- Interval/Time Merge: In the menu at the top of ❶, you can modify the specified interval and time merge.
- By selecting the monitoring target: ⚙, you can specify the monitoring targets. If not selected, it searches for all.
- Time comparison: If you select ⌛, you can compare the current trend of the same metric with that of the previous time zone.
- By selecting the snapshot: 📷 icon, you can snapshot charts except for widget options.
- By selecting the CSV: 📄 icon, you can download the plot data on the chart as a CSV file.
- **Detail:** By selecting the 📊 icon, the detailed view can be seen. When there are many monitoring targets, you can see the metrics trends for each monitoring target individually.

❗ If you do not see any options at the top of the metrics chart widget, select the ⋮ icon.

Deleting a widget

To delete all widgets placed on the screen, select 🗑 **Delete All Widgets** on the screen.

Metrics Search

Home > Select Project > **Analysis** > **Metrics Search**

You can query specific metrics based on tags in **Metrics Search**.

1 Metrics Search

Time selector: < 2023/08/17 07:57 ~ 2023/08/17 08:57 60Min > Max count: 100 Category: app_counter

2 Tags: All container containerKey host_ip okindName oname onodeName pid type 8/8 Filter: Filter by tag value

Field: All active_tx_3 active_tx_8 active_tx_count apdex_satisfied apdex_tolerated apdex_total arrival_rate httpc_count httpc_error httpc_time meterlog resp90 resp95 resp_time sql_count sql_error sql_fetch_count sql_fetch_time sql_time tps tx_count tx_doc_time tx_error tx_http_time tx_sql_time tx_time tx_time_sql_sum 5/29

3

	Time	Oid	Tags								Fields				
			container	containerKey	host_ip	okindName	oname	onodeName	pid	type	active_tx_3	arrival_rate	sql_time	tps	tx_error
1	2023-08-17 07:57:40	633280970	agent.service	1395943798	10.21.1.26	demo-okind-1	demo-8103	node-1	3285013	java	10	20.57942	7.822286	20.94554	0
2	2023-08-17 07:57:40	-857948929	agent.service	1395943798	10.21.1.26	demo-okind-1	demo-8105	node-1	3284721	java	10	17.974834	10.626543	20.609276	0

1 Time and category selection

In the **1** area, you can specify the **Time selector**, **Max count**, and **Category** for the collected metrics. **Time selector** and **Category** must have been specified.

- **Time selector:** You can query by specifying the time when metrics were collected. The default value is **1 hour**. In addition to the lookup time provided as the default option, you can specify the date and time after selecting the **Time selector** tab.

! For more information on how to use the **Time selector** option.

- **Max count:** You can specify the maximum number of metrics to search in the **3** list. You can set the count up to **10**, **50**, **100**, **200**, **300**, **1000**, **2000**, and **3000**.
- **Category:** It is a classification unit for the related metrics. You can set the desired **Category** after selecting the **Category** tab.
- **Refresh categories, tags, and field options:** **Category**, **Tags**, and **Field** options can be fetched.

2 Tag and field selection

In the 2 area, select **Tags** and **Field**. The default setting is "Select All," unless specified separately by user.

- **Tags:** Unique data that can identify the collected targets.
- **Field:** Metrics collected from the monitored targets.
- **Filter:** Select  **Filter by tag value** and then set the tag value for filtering.

For example, you can search filtered data by setting the value of `oname` to `demo-8101`.

-  **Search:** If you set the conditions and then select **Search**, you can search the source data of the metric in the 3 area.
-  : You can download the source data of the metric as a CSV file.

3 Metrics table

Because the metrics to be collected cannot be specified in advance, it is important to check the source data for all metrics being collected. After setting the desired conditions in the condition area above, you can search the original data of the metric in a table format in the 3 area. Columns in the table are changed when you specify the conditions for **Tags** and **Field**.

- To search metrics, **Time selector** and **Category** must have been specified.
- To search metrics, **Tags** and **Field** are optional.

Metric Anomaly Detection

Home > Select Project > **Analysis** > **Metrics Anomaly Detection**

You can compare the patterns of various metrics with the expected patterns learned by the AI. Anomaly detections that deviate from the expected patterns can be viewed through the graph chart. You can check recurring patterns based on the past data and use them to predict future metrics values.

- ❗ The widgets placed on the screen are not saved and reset when you go to another menu.
- It is similar to **Analysis** > **Metrics Chart** except for the pattern and anomaly display.
- The alert, **Anomaly detection** is based on the **Metric anomaly detection**. For more information about the **Anomaly detection** alert setting, see [the following](#).

Checking the widgets



- ❶ The bright color areas of the graph are the estimated patterns analyzed by the AI.
- ❷ The blue graph is the metrics trend of the project.
- If it deviates from the expected pattern analyzed by the AI, it displays dots on the graph in Orange and Red steps. The values that are far from the expected pattern range appear in red.

Placing the widgets



1. In **1 Time**, set a desired time interval. You can set the interval up to 1 month.
2. In **2 Filter**, select a range of the metrics.
3. In the following list, select a metric for monitoring.

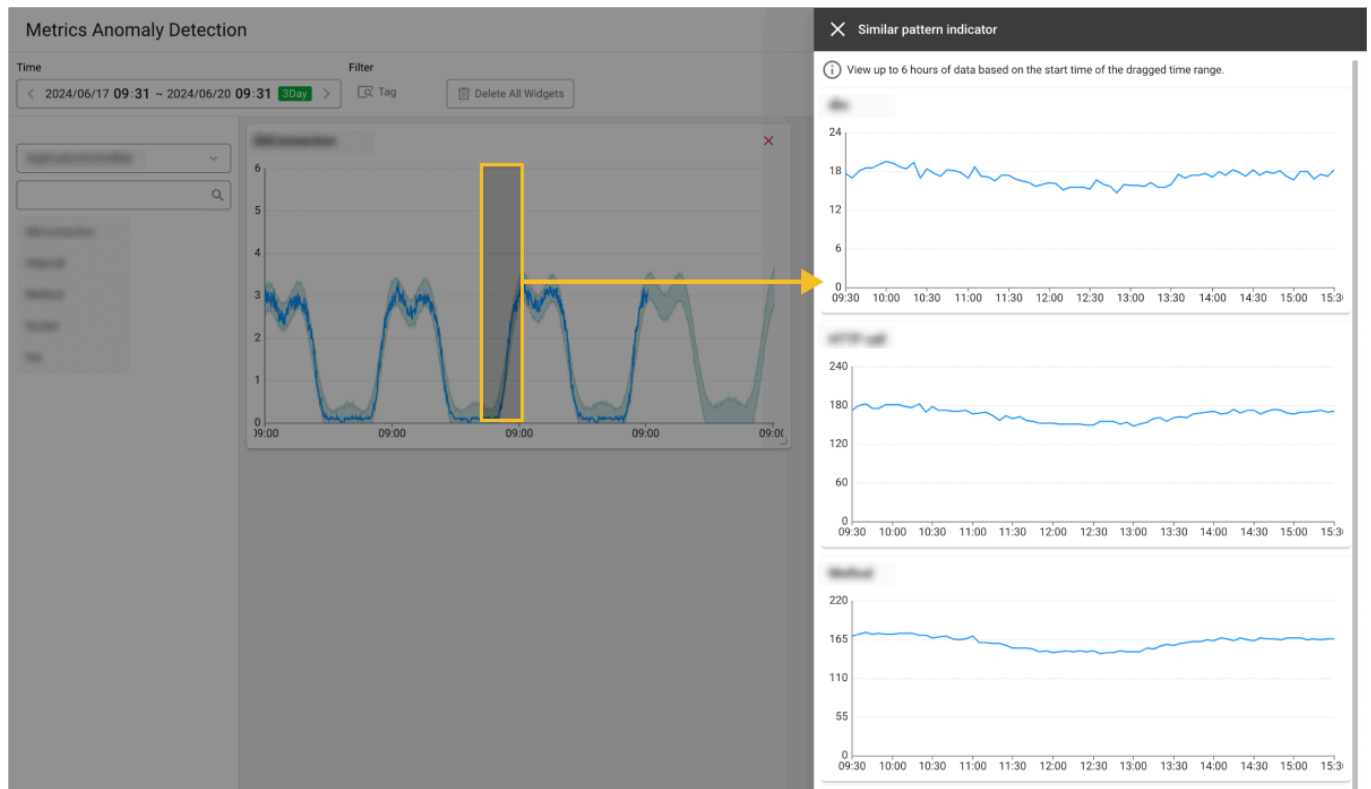
Place the selected metric to the right of the screen.

- Select **2 Tag** to check the metrics separately by selecting a monitoring target. A tag selection list appears on the right of the screen. Select desired items, and then add widgets.
- The widgets placed on the screen are not reflected in the chart even if the **Time** or **Tag** values have been changed.
- Select **X** on the upper right of the widget on the screen to delete.
- You can reposition a widget by dragging it while selecting the upper left part of the widget.
- You can resize a widget by selecting the upper right part of the widget and then dragging it.

Deleting a widget

To delete all widgets placed on the screen, select **Delete All Widgets** on the screen.

Checking the related metrics



Drag part of the chart in the widget. The **Similar pattern indicator** window appears on the right of the screen. You can search the related metrics for up to 6 hours based on the start time of the time range you dragged.

Metrics Trend Analysis

Metrics trend analysis provides a feature that visualizes metric changes within the past 30 days, allowing you to compare and analyze trends.

You can view key database performance metrics by period or time, helping you quickly identify patterns at specific moments or time intervals.

Default Screen

Metrics trend analysis consists of a **top option bar** and a **bottom chart area**.

When you select the viewing range and metrics in the option bar, trend graphs that match those conditions are automatically displayed.

Option Bar

The option bar provides functions such as time range selection, metric selection, and preset management.

Time Window

Use this option when you want to view data only for a specific time period.

When the toggle is enabled, the time range input fields become active. The default state is disabled.

For example, to analyze data during business hours (09:00–18:00), enable the Time Window and set that range.

Instance

Select the database instance to view.

A list of instances connected to the project is displayed, and you can quickly search for an instance using the search box.

Metrics

Select the metrics you want to view.

Metrics are categorized by field, allowing you to choose specific items for display.

Preset

Save and load frequently used chart configurations.

- The click states of the top date charts are saved in the preset.
- The click states of the lower date trend charts are **not** saved.

Save a Preset

Save the configured metrics and layout as a preset.

1. Set **Time Window**, **Metrics**, and other options as desired.
2. Click the  icon at the top right of the screen.
3. In the **Save as Preset** window, enter a name and click **Save**.

Load a Preset

1. Select a saved preset from the preset dropdown list.
2. The saved **Time Window**, **Metrics**, and **Chart** settings are applied automatically.

✔ Saving presets allows you to view charts immediately without repeating the same setup.

Chart

The chart area in **Metrics trend analysis** visualizes changes in the selected metrics.

You can compare trends, averages, and maximum values over specific periods.

You can add new charts as needed or remove unnecessary ones.

Add a Chart

1. (Optional) Set the **Time Window** in the top option bar.
2. Select the desired field under **Metrics**.
3. Click the + **Add Chart** button at the top right to add a chart.

Delete a Chart

Click the  icon at the top right of the chart you want to delete.

Widget

The bottom chart area in **Metrics trend analysis** includes **Interval** and **Open Link** functions.

These allow for detailed data analysis of specific periods or direct navigation to the detailed monitoring view for that time range.

Interval

Change the aggregation unit of the displayed data.

You can view data in hourly or 5-minute intervals.

By default, the data is displayed hourly; to see more detailed data, switch to the 5-minute interval view.

Open Link

Click a bar in the chart representing a specific time range to move directly to that time's detailed monitoring page.

- ⓘ The **Open Link >** button becomes active only when a specific time bar is selected.
You can then view detailed metrics for that selected time range.

SQL Statistics

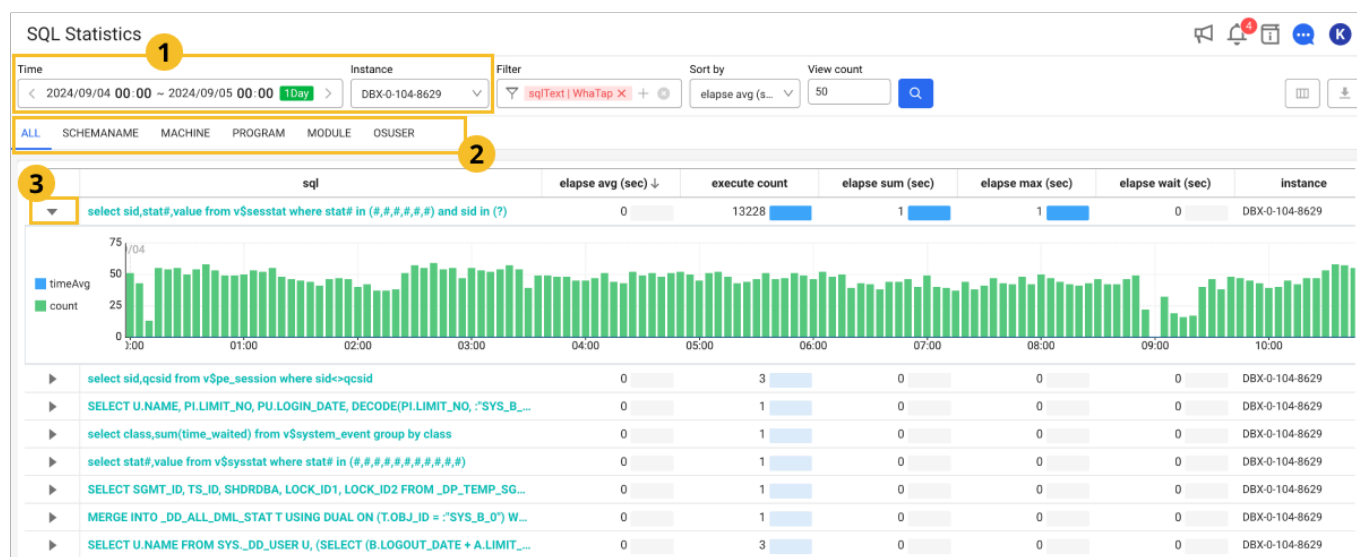
Home > Select Project > **Stat/Report** > **SQL Statistics**

Statistics are created based on the SQL execution count, execution time, and waiting time within the active sessions collected by the agent, and a list of top SQLs for the search period is provided. It provides a basis for analyzing frequently performed SQL performance through the average and maximum execution time.

- **execute count**: Execution count of the SQL
- **elapse sum (sec)**: Total execution time (secs) of the SQL
- **elapse avg (sec)**: Average SQL execution time (sec), which is the result of **elapse sum** / **execute count**
- **elapse max (sec)**: Maximum execution time (sec) of the SQL

! **SQL Statistics** function creates statistics based on the SQL that excludes literal values.

Basic screen guide



1. In **1 Time**, select the time and date to view the data. You can select a lookup time after selecting the

green button.

2. In **1 Instance**, select a target to view the data.
3. Select .

The top 50 entries appear in the table.

- ! • Select the clock display area to query a random date and time. If you click the date and time text area, the selectable options for the date and time appear.
- If you select each column in the table header, you can sort the list by the selected item.
- You can sort the searched results by the item selected in **Sort by**. Select a desired item and then select .
- In **View count**, you can set the number of entries to display in the table. Finish the settings and then select .
- To download the viewed data as a CSV file, select .

Checking the query-based execution trend

On the utmost left for each item of the table, select **1** . A chart appears that displays the number of executions every 5 minutes and the average execution time of the query statement. If you hover your mouse over each bar graph, you can see the number of that time.

To classify and view data by usage category, select the desired tab from **2**.

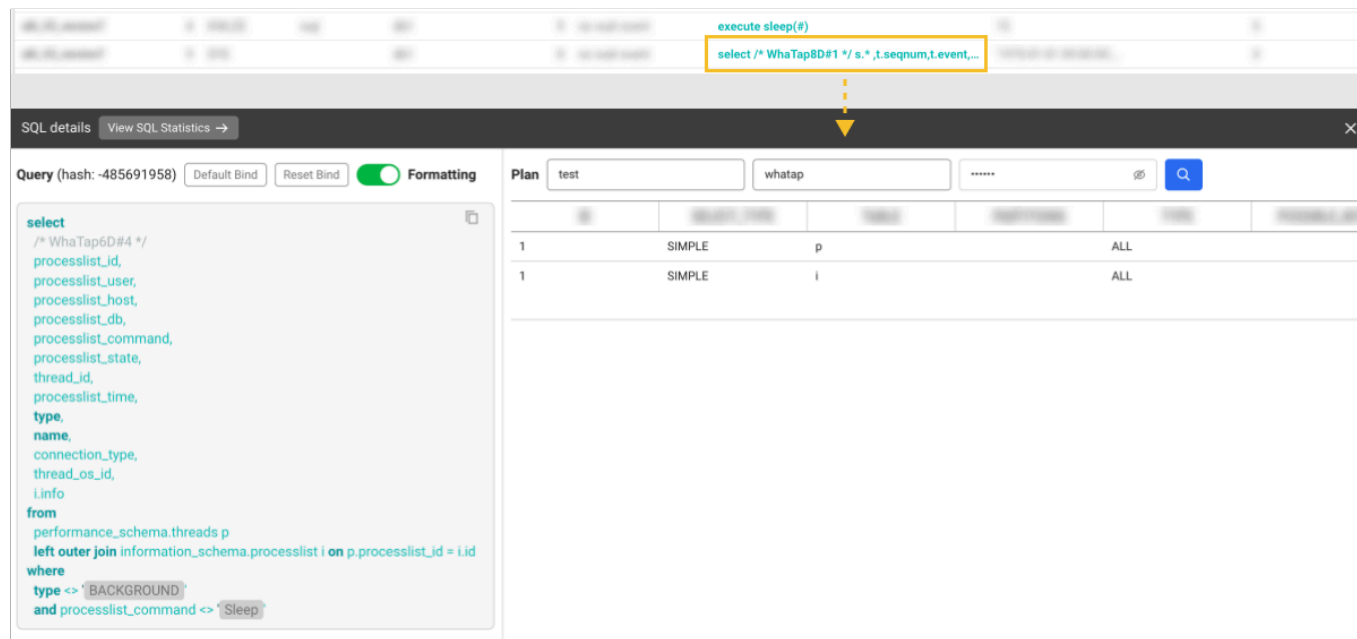
Previewing the query

sql	elapse avg (sec)	execute count ↓	elapse sum (sec)
select /* WhaTap6D\$4 */ processlist_id,processlist_user,processlist_host,proces...	<pre>select /* WhaTap6D\$4 */ processlist_id,processlist_user,processlist_host,processlist_db,processlist_command,processlist_state,thread_id,processlist_time,type,name,connection_type,thread_os_id,i.info from performance_schema.threads p left outer join information_schema.processlist i on p.processlist_id=i.id where type<>'S' and processlist_command<>'S'</pre>		

You can preview the query statement by moving the mouse pointer to the [sql](#) column in the search results list.

See query details

3 Select a query statement. The **SQL details** window appears to display the query statement and SQL plan.



The screenshot shows the SQL details window for a query with hash -485691958. The query is a SELECT statement that retrieves information from the performance_schema.threads table, joined with the information_schema.processlist table. The query is executed on a database named 'test' with a user named 'whatap'. The execution plan shows two steps: a simple query plan for the join operation and a simple query plan for the select operation.

Query (hash: -485691958) ☒ **Formatting**

```

select
/* WhaTap6D#4 */
processlist_id,
processlist_user,
processlist_host,
processlist_db,
processlist_command,
processlist_state,
thread_id,
processlist_time,
type,
name,
connection_type,
thread_os_id,
i.info
from
performance_schema.threads p
left outer join information_schema.processlist i on p.processlist_id = i.id
where
type <> 'BACKGROUND'
and processlist_command <> 'Sleep'

```

Plan test whatap ***** 🔍

Step	Operation	Table	Access	Filter	Estimated Rows
1	SIMPLE	p	ALL		
1	SIMPLE	i	ALL		

Click the **View SQL Statistics** → button to navigate to the **SQL statistics** menu, where you can view the statistical information related to the SQL query.

Filtering the searched results

Adding the filter conditions

You can filter the results by SQL text, agent name, or DB user name.

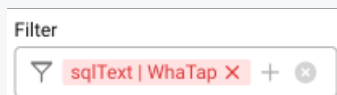
1. In the **Filter** option, click +.
2. In **Filter key**, select a desired filtering criteria.
 - If the value of the selected item is text, you can select any of **Includes** (blue) and **Excludes** (red).

example

- If the value of the selected item is number, you can select any condition of `==` (equal to), `>=` (greater than or equal to), and `<=` (less than or equal to).
3. In **Condition**, select a condition.
 4. Enter a string or number to match the condition.
 5. Select **Apply**.

! Adding and Deleting Filter Conditions

- To add a filtering condition, click the **Add** button and repeat steps 1~5. Added conditions are applied using the AND (`&&`) operator.
- To delete specific conditions while adding, click the  button on the right side of the filter condition. To delete all conditions, click the  **Delete All** button.
- To quickly remove all applied conditions from the **Filter** option, click the `×` button.
- The default setting is to exclude if `sqlText` contains 'WhaTap'.



Modifying the filter conditions

1. Click the applied item in the **Filter** option at the top of the screen.
2. In the **Edit filter** window, edit the desired item and click the **Apply** button.

Setting the table columns

You can hide the table header columns or add any of them. You can also change the column order. Select .

- After configuration, select **Confirm** to apply the settings in the table.
- In the **3** search bar, enter text to search the desired columns. Only the columns that meet the entered text are displayed.
- Images may differ depending on the product, project, or menu.

Adding columns

From the **1** list, select the items to add as table header columns. To select all items, select **Select All**.

Deleting columns

From the **1** list, unselect the columns to delete. Alternatively, select **×** on the right of the item to delete from the **2** list.

Changing the column order

Drag an item to reposition from the **2** list, and then move it to the desired position.

Initializing the configuration

To cancel all changes and reset them, select **↺ Initialized**.

Tablespace Size

Tablespace Size is a screen for monitoring and managing the usage of database tablespaces. You can quickly check the size change trend of each tablespace using a line chart, and detect space shortages in advance through daily changes and **Remaining Day**.

- **Tablespace Size Trend:** Use the line chart to track the capacity change trend of major tablespaces.
- **Disk Usage:** View disk usage and remaining days per mount point. Available when the XOS agent is installed.
- **Tablespace Size Detail:** Analyze the latest usage, daily changes, and remaining days for individual tablespaces.

Prerequisites

To display data on the Tablespace Size screen, [DB Configuration](#) and [Agent Configuration](#) are required.

DB Configuration

Grant permissions to the monitoring account so the agent can query tablespace and segment information.

```
GRANT SELECT ANY DICTIONARY TO whatap;
```

Or grant permissions to individual views.

```
GRANT SELECT ON dba_segments TO whatap;
```

Agent Configuration

This configuration is for collecting segment size (TOP 50) data. Based on the conditions below, the agent collects segment size data once a day at the configured time. Data may not be collected due to conditions such as `segments_min_size`. Without this configuration, segment size information will not be available.

Option	Type	Default	Description
segments	boolean	true	Enable/disable segment information collection
segments_hour	int	5	Time to collect segment information. Default is 5, which starts collection at 5 AM.
segments_min_size	int	10	Minimum segment size (MB) for collection
segments_exclude_sys	int	1	Exclude sys account segments (1: exclude, 0: include)
segments_max_count	int	50	Number of segments to collect per tablespace

Tablespace Size

Basic Options

In the top filter area of the **Tablespace Size** screen, you can select the time range and target database to query.

- **Time:** Select the query time range. Up to 3 weeks can be queried; queries over 3 days are displayed as daily averages.
- **Instance:** Select the target DB instance to query.
- **Data Unit:** Select from MiB/GiB/TiB. All table size values are displayed in the selected unit.
- **Database:** Select the target database to query.

Tablespace Size Trend

Displays the size change of each tablespace as a **line chart**. Tablespaces are color-coded and can be identified in the legend at the bottom. Hover over the chart to see detailed values by time period.

Item	Description
Top 5/10/15/20	Select the number of top tablespaces to display on the chart

Item	Description
Size/Used	Switch between Size (total size) and Used (usage)

Disk Usage

! Disk usage can be collected after installing the XOS agent.

Displays disk usage per mount point. The **Latest Data** section shows the most recently collected data within the query range selected in the time selector. You can check the size, Usage (%), Increase AVG, and Remaining Day at that point in time.

Latest Data

Column	Description
Mount Point	Disk mount path
Size	Total disk size
Used	Used size
Free Size	Remaining free space
Usage(%)	Usage rate (visualized as a progress bar)
Increase AVG	Average daily increase over the query period
Remaining Day	Remaining available days based on the current growth rate

Daily Columns

Displays **Size** and daily change (**Inc**) for each date in the query period.

- **Search:** Filter by Label or Path

- **CSV:** Export in CSV format

Tablespace Size Detail

Displays detailed usage for individual tablespaces. The **TOTAL** row at the top shows the overall total. The **Latest Data** section shows the most recently collected data within the query range selected in the time selector. You can check the size, Usage (%), Increase AVG, and Remaining Day at that point in time.

Latest Data

Column	Description
Tablespace	Tablespace name
Auto Ext	Auto extension status (YES/NO). Column visibility can be toggled in settings.
Inc By	Increment unit for auto extension. Column visibility can be toggled in settings.
Max Size	Maximum size limit. Column visibility can be toggled in settings.
Total Size	Total tablespace size
Used Size	Used size
Free Size	Remaining free space
Usage(%)	Usage rate (visualized as a progress bar)
Increase AVG	Average daily increase over the query period
Remaining Day	Remaining days based on current growth rate, calculated as $\text{Free Size} \div \text{Increase AVG}$

Daily Columns

Displays **Size** and daily change (**Inc**) for each date in the query period. Increases are shown as positive values and decreases as negative values, color-coded for distinction.

Additional Features

-  **Magnifier icon:** Displays a popup of the top 50 segments by space usage in the tablespace.
-  **Expand:** Expand the list of data files belonging to the tablespace.
- **Search:** Filter by container or tablespace.
- **CSV Download:** Export or download in CSV format, with the option to select **Tablespace** or **Datafile** unit.

Table Settings

Click the  **Settings** button in the top right to configure table display options.

Item	Description
Column: Auto Ext / Inc By / Max Size	Toggle the display of <code>Auto Ext</code> , <code>Inc By</code> , and <code>Max Size</code> columns.
Warning(%)	Usage rate (%) for warning level; displayed in orange when exceeded. - Default: 80
Critical(%)	Usage rate (%) for critical level; displayed in red when exceeded. - Default: 100
Reset Settings	Reset all settings to default values.

Segment Size (TOP 50)

Click the  **magnifier icon** in the tablespace row to display a popup showing the top 50 segments occupying the most space in that tablespace.

Click the  **Download** button at the top right of the popup to export the list shown in the popup to a CSV file. The column configuration and display format visible on the screen are reflected in the file as they are, and the saved file name is `table_size_top50.csv`.

 The `segments` option must be enabled in the Agent configuration. The agent collects segment size data once a day, and without this configuration, data will not be available.

Column	Description
Tablespace Name	Tablespace the segment belongs to
Owner	Schema that owns the segment
Segment Name	Segment name. Click to view object details in the Object Detail popup.
Segment Type	Segment type (TABLE, INDEX, LOBSEGMENT, etc.)
Partition Name	Partition name (if a partitioned table)
Size	Segment size. Size changes can be tracked via date columns.

Object Detail

Click a segment name in the Segment Size (TOP 50) popup to send a real-time query request to the agent and display detailed information about that object.

- **Object Basic Info:** owner, table_name, num_rows, blocks, avg_row_len, tablespace_name, partitioned, last_analyzed, compression, status, etc.
- **Column/Index:** Column list (column_id, column_name, nullable, data_type, data_default, num_distinct, num_buckets) and index information.

Data Interpretation Guide

Key Checkpoints

- **Tablespace with high Usage(%)**
Risk of space shortage → Consider cleaning up unnecessary data or expanding the tablespace.
- **Tablespace with high Increase AVG**
Rapidly growing → Check Remaining Day and take proactive action.
- **Short Remaining Day**

Available space will be exhausted soon based on current growth rate → Immediate action required.

- **Tablespace with `Auto Ext` set to NO**

Auto extension is disabled; errors may occur when space is exhausted → If usage is high, consider manual expansion or enabling Auto Ext.

- **Sudden change in daily `Inc` value**

Large-scale data load or deletion occurred on a specific date → Investigate the cause.

Practical Use Scenarios

Scenario 1. Proactive Space Shortage Detection

1. Sort by `Usage(%)` in descending order in **Tablespace Size Detail**
2. Check `Remaining Day` for tablespaces with high usage
3. If remaining days are few, expand the tablespace or clean up unnecessary data

Scenario 2. Capacity Surge Root Cause Analysis

1. Check for rapidly increasing tablespaces in the **Tablespace Size Trend** chart
2. Identify the date when the increase occurred in the daily `Inc` column of that tablespace
3. Click the  **magnifier icon** for that tablespace to analyze segments occupying the most space
4. Review segment details for unnecessary indexes or ways to reduce data size; if none found, consider disk expansion

Scenario 3. Auto Extension Configuration Check

1. Enable **Auto Ext/Inc By/Max Size** columns in settings
2. Among tablespaces with `Auto Ext` set to NO, check those with high `Usage(%)`
3. If necessary, enable auto extension or manually expand the tablespace

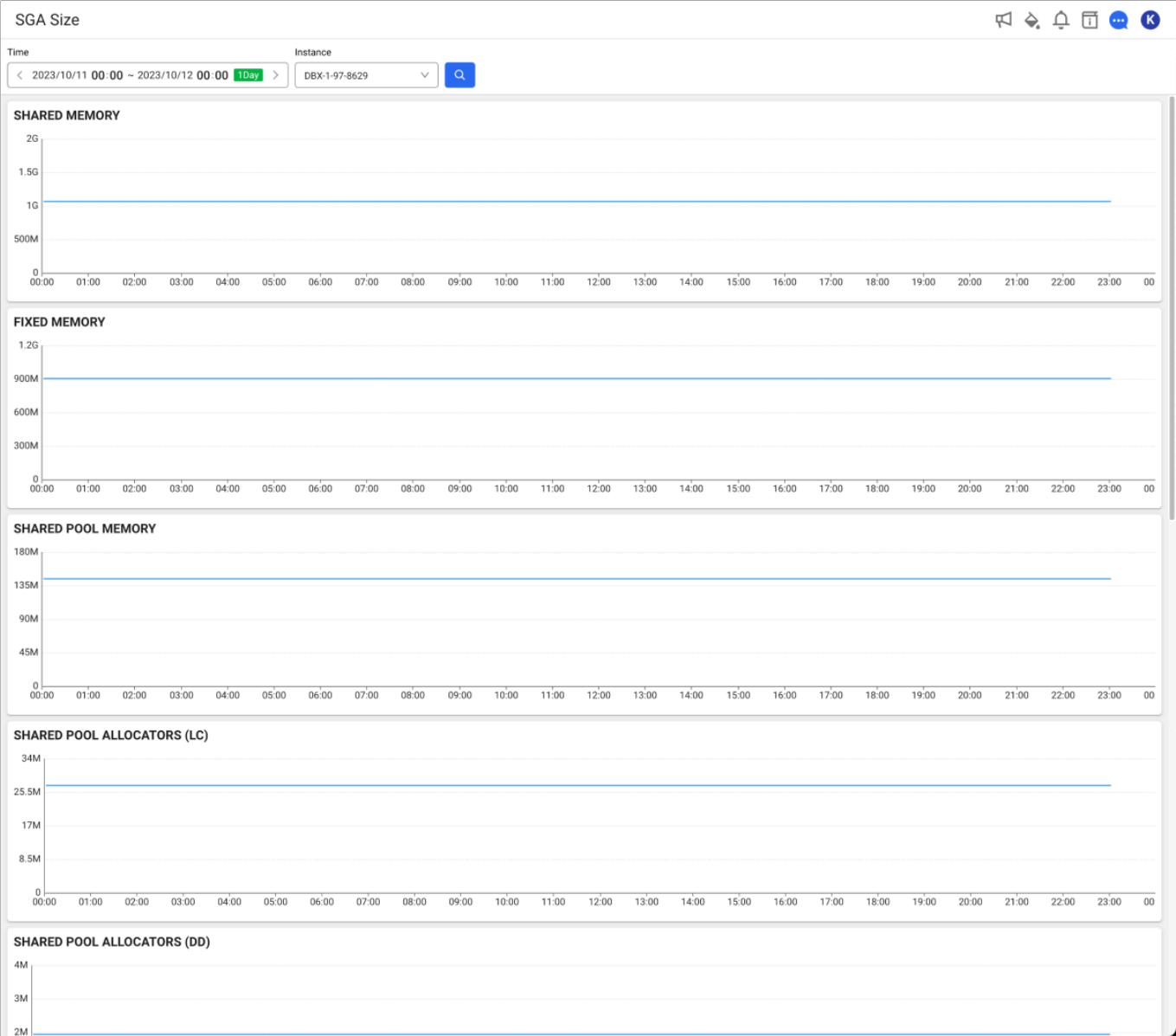
SGA Size

Home > Select Project > **Stat/Report** > **SGA Size**

You can monitor timely changes by saving summaries of System Global Area (SGA) that is an server memory area.

- **Performance optimization:** By monitoring the sizes and usage of various memory areas within the SGA to proactively prevent performance issues and optimally manage memory resources.
- **Bottleneck detection:** By early detecting the bottlenecks occurring in each memory area, the availability and stability of the system can be improved.
- **Resource management:** You can check whether memory resources are allocated appropriately to reduce unnecessary memory usage and efficiently distribute memory resources.
- **Troubleshooting:** By identifying which part of the SGA area are overused so you can quickly troubleshoot the cause of poor performance.

Basic usage guide



1. Set the time to search in **Time**.
2. Select an instance name to view the trend data of the instance.
3. Select .

- ! • The query time can be set up to 3 weeks.

Monitoring items

By continuously monitoring the following items, improve the efficiency of the database and prevent occurrence of incidents.

- **SHARED MEMORY**

It is the memory area shared between multiple processes in the database. It stores key data and program codes and allows multiple processes to access it simultaneously. You can determine the capacity and efficiency of the memory being used by the database and prevent memory shortages or bottlenecks in advance.

- **FIXED MEMORY**

It is a fixed memory area that is initialized when the database boots, and various fixed structures required for database operation are located there. It is set to a fixed size, so it does not change but you can check how much of the total memory usage it occupies. If a memory shortage occurs, check the fixed memory area.

- **SHARED POOL MEMORY**

It is a memory area that includes SQL and PL/SQL cursors, library cache, data dictionary cache, and such. This memory plays an important role in SQL reusability. You can monitor this memory to check SQL reusability and see if SQL hard parsing increases due to memory shortage. This helps prevent performance degradation.

- **SHARED POOL ALLOCATORS (LC)**

Amount of memory allocated to the library cache, which caches execution plans and SQL statements to improve the performance. Determine whether execution plan caching works effectively or unnecessary memory usage degrades the performance.

- **SHARED POOL ALLOCATORS (DD)**

Amount of memory allocated to the data dictionary cache, which stores information about database objects. Keeping the data dictionary cache at an appropriate size can improve performance by allowing quick query about database objects.

- **SHARED POOL ALLOCATORS (SLAB)**

Memory slab is a space used to manage memory allocation more efficiently. You can monitor this memory to improve the memory management efficiency. Try reducing unnecessary memory usage or resource waste.

- [SHARED POOL ALLOCATORS \(MISC\)](#)

It is the memory area of SHARED POOL that is used for various purposes. Trace other memory usage to see if any abnormal memory usage occurs.

- [SHARED POOL ALLOCATORS \(Total\)](#)

Total memory size allocated from SHARED POOL. This is the total sum including LC, DD, SLAB, MISC, and such. It can help you understand the overall memory usage and prevent performance degradation caused by memory shortage.

- [Database Buffers](#)

The database buffer cache stores data blocks in memory to reduce physical disk I/O. You can monitor the usage of database buffers to increase cache hit rate and optimize performance. Make sure data blocks are cached appropriately.

- [Redo Buffers](#)

A buffer that records changes when transactions occur in the database. This information is later saved as a log. Monitoring the Redo buffer usage can help you manage it so that log writing does not become a bottleneck. This can help improve the transaction performance.

Report

Home > Select Project > **Stat/Report** > **Report**

If you click  in **Report** on the screen, you can see various analysis reports classified by daily, weekly, and monthly. Select a desired report format, and then set the date and time to view and filtering options. You can check the selected report by selecting .

Report is a document that reports the service usage status and failure records for individual projects. The persons in charge of service monitoring share the status report with the people of related departments.

The monitoring data analysis is important because it serves as a metric for determining the direction of improvement. However, it is cumbersome to aggregate and document data from multiple dashboards.

WhaTap's **Report** menu supports **automated report creation**. Through the **Report** menu, you can create weekly reports, share reports at the set times, and manage various templates.

Download Report

If you want to download the report or schedule the printing or mailing, click the  Download button. You can download it in HTML format.

Report types

The basic report is a form that is actually used by large enterprises, government agencies, and IT service companies. If you have any desired form, please send a request to support@whatap.io. The requested report template is to be added in the **Stat/Report** > **Report** list.

Email delivery schedule

To receive regular reports by email, select **Reservation of Report Email**. You can replace various service checking tasks performed right after work with email confirmation.

Reservation of Report Email

Report will be sent on 04~06 o'clock from tomorrow.

Maximum 5 report mail settings can be registered.

Report type

Report time
00:00 ~ 23:59

Weekdays
☒ Mon
☒ Tue
☒ Wed
☒ Thu
☒ Fri
☐ Sat
☐ Sun

Emails

Daily DB Report

The daily database report allows you to check the database performance for the day in figures and charts. When creating a report, you can set the start date, start time, and end time if necessary, and you can select and view only specific instances. When all is selected, all instances are viewed at once.

Trend Chart

You can see metrics charts for each database instance. The maximum value of each metric is displayed in circle, and the time when the maximum value occurred is also displayed.

- Metrics drawn as charts may differ depending on the configuration.
- On the upper right of each chart, use [CSV](#) to download the data in an Excel file format.

SQL Top 10

You can check the statistics of SQL queries during the query period for all or selected instances. It retrieves only the top 10 sorted items in descending order based on the maximum value of query execution time.

Weekly DB Report

The weekly database report displays the database performances for the week with figures and charts. You can

enter the start date and see from 7 days prior to the day of inquiry.

Trend Chart

You can compare weekly metrics for each database instance with figures and charts. The maximum value during the query period is displayed in circle and the occurrence time is also displayed.

- ! • Metrics drawn as charts may differ depending on the configuration.
- On the upper right of each chart, use [CSV](#) to download the data in an Excel file format.

SQL Top 10

You can check the statistics of SQL queries during the query period for all or selected instances. It retrieves only the top 10 sorted items in descending order based on the maximum value of query execution time.

Monthly DB Report

This report allows you to check the database performance for a month with numbers and charts. You can set the start date and search up to 30 days from the start date. You can check the change amount in each metric over a month by instance, and you can also check the SQL query statistics of the top 10 items performed during the query period.

Alert Notifications

This feature delivers notifications to users based on predefined conditions when issues occur in monitored systems or applications. Notifications can be sent through various channels such as email, SMS, messengers, and mobile push notifications.

For example, you can configure alert thresholds for key performance indicators such as CPU usage, memory usage, disk I/O, network traffic, transaction count, error occurrences, and response time latency. When these thresholds are exceeded or abnormal behavior is detected, notifications are automatically sent.

With WhaTap's AI-based alerting, you do not need to define complex conditions manually. The AI learns normal application behavior patterns and automatically detects and notifies anomalies. Additionally, by using tag-count alerts, you can define conditions on values aggregated by specific tags, enabling precise detection even in complex scenarios.

Key Features

- **Event Configuration:** Configure threshold-based alert conditions and notification channels
- **Event Notification Settings:** Configure notification channels and time schedules per user
- **Event History:** View the history of alert occurrences

Permissions

To add or configure events, the **Alert Configuration** permission is required.

- **View:** To view metrics event configurations, the **View & Analyze** permission is required.
- **Add/Edit/Delete:** To modify configurations, the **Alert Configuration** permission is required.
- **Receive Notifications:** To receive notifications, the **Alert Receive** permission is required.

Reference

For more details, see [Member Permissions](#).

Event Configuration

Home screen > Select project  **Alert** > **Event Configuration**

In **Event setting**, you can configure and manage events based on anomaly conditions that may occur in monitored systems or applications. When the configured conditions are met, notifications can be delivered through your preferred channels such as email, SMS, messengers, or app push notifications. You can tailor event configurations according to your monitoring objectives.

Metrics

Metrics events allow you to monitor system and application performance indicators based on real-time data.

Composite Metrics

The composite metrics feature allows you to create events using complex rules and send alert notifications.

Anomaly Detection

The anomaly detection feature allows you to configure alert notifications by detecting unexpected patterns.

Real-time logs

Sends alert notifications when event conditions configured in real-time collected logs are detected.

 Composite log

Configure composite log events that trigger alert notifications based on log content.

Home Screen > Select Project >  **Alert** > **Event Configuration**

Event setting provides features to configure and manage events based on anomaly signals that may occur in monitored systems or applications. When configured conditions are met, you can receive notifications through your preferred channels such as email, SMS, messengers, or app push notifications. You can design event configurations according to your monitoring objectives.

 Metrics

Metrics events allow you to monitor system and application performance indicators based on real-time data.

 Composite Metrics

The composite metrics feature allows you to create events using complex rules and send alert notifications.

 Anomaly Detection

The anomaly detection feature allows you to configure alert notifications by detecting unexpected patterns.

 Real-time logs

Sends alert notifications when event conditions configured in real-time collected logs are detected.

 Composite log

Configure composite log events that trigger alert notifications based on log content.

 Reference

- When configuring events, use appropriate threshold values to prevent unnecessary event generation.
- When setting up notifications, consider enabling recovery notifications (alerts sent when issues are resolved) to support effective operational response.

Common Features

All event configurations can be downloaded in **JSON or Excel format**. By sharing the same type of product configuration, you can reduce repetitive event setup work.

- **Batch JSON Edit:** Edit all event conditions in bulk using JSON format.
- **Batch JSON Download:** Save all currently registered event conditions as a JSON file.
- **Batch Excel Download:** Download the event list as an Excel file for external reporting or backup purposes.

Batch JSON Edit

1. Click the [Batch JSON Edit] button at the top of the screen.
2. Import a JSON file downloaded via the **Batch JSON Download** feature, or edit the content directly.
3. Click the [Overwrite] button to save.
4. When a confirmation message appears, click the [Overwrite] button.

 After overwriting, you cannot restore the previous event configuration.

- Arbitrarily modifying the values of the `productType` or `platform` properties may cause events to



malfunction in other projects.

- The JSON editor includes built-in validation. If the format or values are invalid, an error message appears below the editor and the [Overwrite] button is disabled.

```

    ],
    "BASIC": [
      {
        "criticalEnabled": "false",
        "warningEnabled": true,
        "silentPeriod": 300000,

```

❗ "criticalEnabled" requires "boolean" type value, not "string" type.

Load Cancel Overwrite

JSON Data Structure



```

{
  "productType": "{productType}",
  "platform": "{platform}",
  "events": {
    "HITMAP": {
      ...
    },
    "LOG_REALTIME": [
      {...}
    ],
    "METRICS": [
      {...}
    ],
    "COMPOSITE_LOG": [
      {...}
    ],
    "BASIC": [
      {...}
    ],
    "COMPOSITE_METRICS": [
      {...}
    ],

```



```
"ANOMALY": [
  {...}
]
}
```

JSON Field	Description
productType	Product type (e.g. APM, Infra)
platform	Platform information (e.g. java, node)
events	Event data
◊ HITMAP	Hitmap pattern
◊ LOG_REALTIME	Real-time log events
◊ METRICS	Metrics
◊ COMPOSITE_LOG	Composite log events
◊ BASIC	Basic events
◊ COMPOSITE_METRICS	Composite metrics
◊ ANOMALY	Anomaly detection

Batch JSON Download

Click the [Batch JSON Download] button at the top of the screen.

- The JSON file name follows the format **integrated-event- YYYYMMDD .json**.
- The structure of the JSON data and the sub-properties under the **events** attribute may vary depending on the product (**platform**) or product type (**productType**).

⚠ If you arbitrarily modify the values of the `productType` or `platform` properties in the JSON data, events may not function correctly in other projects.

Batch Excel Download

Click the [Batch Excel Download] button at the top of the screen.

Metrics

Home > Select Project >  **Alert** > **Event Configuration** > **Metrics** tab

You can view the complete list of all metrics-based events configured for the project. You can review, edit, or delete existing metrics events, or add new events as needed.

Default Options

- **Event Level:** Indicates the severity of an event and is classified into three levels: Normal (**Info**), Warning (**Warning**), and Critical (**Critical**).
- **Duplicate Agent Alert Suppression:** If two or more agents with the same name run simultaneously, events are not triggered for the selected duration (30 seconds, 1 minute, 3 minutes, 5 minutes, 10 minutes).
- **Search:** Search events by event name.
- **JSON Download/Upload:** Edit event rules directly in the JSON editor, or download them as a file, modify them, and upload them again.
- **+ Add Event:** Add a new metrics event.
- **Resize Columns:** Adjust column widths by dragging column borders.

Table | Metrics Event List Structure

Item	Description
No.	Event sequence number
	Event activation status – Enabled: An event is triggered when conditions are met – Disabled: The event does not run and conditions are not evaluated
	Edit or delete event settings
Event Name	User-defined event name – Up to 255 characters

Item	Description
Rule	Event trigger conditions
Target	Monitoring targets to which the event applies
Trigger Count	The time window and number of occurrences required to trigger an event – An event is triggered when conditions are met the configured number of times within the selected duration
Pause	Temporarily suppresses the same event after an alert is triggered – Available durations: Disabled, 5 min, 10 min, 15 min, 20 min, 30 min, 1 hr, 2 hrs, 3 hrs, 6 hrs, 12 hrs, 1 day – If recovery notifications are enabled, alerts are not triggered for the selected duration after a RECOVERED notification is sent
Recovery Notification	Whether to receive a RECOVERED (normal) notification when Critical or Warning events are resolved – Enabled: Sends a RECOVERED notification when the status changes from in progress to normal and allows viewing active and resolved states in event history – Disabled: Triggers a one-time event each time the threshold is exceeded
Event Recipients	Users or groups that receive notifications for the event (recipient tags)

Event Configuration

Metrics events allow you to define events based on conditions that occur in monitored targets and configure notifications so you can respond efficiently.

Add Event

To add a metrics event, go to **Event Configuration > Metrics** tab, then click the [+ Add Event] button in the upper-right corner.

How to Add a Metrics Event

Step 1. Select Template: Choose the basic structure of the event.

Step 2. Define Event Conditions: Configure the conditions that determine when the event is triggered.

Step 3. Select Event Target: Select the monitoring targets where the event applies.

Step 4. Basic Information and Notification Settings: Configure the event name, message, and recipients.

Select Template

- Depending on how you want to configure the event, select one of the three templates on the left side of the screen.
 - Create New:** Freely configure categories and metrics from scratch. This option is suitable for advanced users who need complex conditions or fine-grained monitoring rules.
 - Quick Setup:** Provides predefined categories, metrics, and default thresholds. You can apply it quickly by adjusting only the threshold values, which makes it suitable for beginners.
 - Advanced Setup:** Add conditions or freely modify settings based on predefined categories and metrics.

ⓘ Metrics events support multiple configuration approaches. The available templates may vary depending on the monitoring platform.

Define Event Conditions

In the **Define Event Conditions** step, configure the metrics that determine when the event is triggered, along with the trigger count, pause settings, recovery notifications, and event active time.

Metric Settings

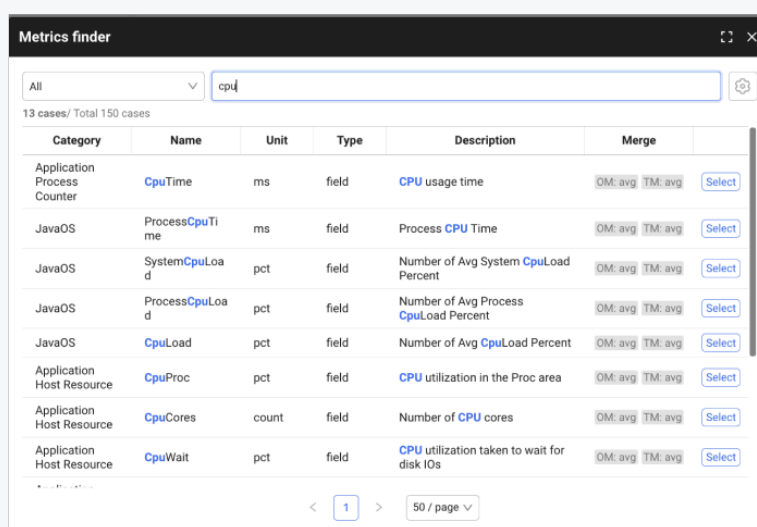
- Enter a category in the search field, or select a category (metric) from the category list. You must select a category to proceed with metric configuration.

- The category list shows the category name, data collection interval, and key. It displays metrics data collected in the project within the last 3 hours.
2. If the metric you need is not listed, select **Direct Input** and enter the category manually.

❗ **If you are not sure about categories or metrics, use the Metrics Finder.**

When configuring metrics for the first time, the Metrics Finder helps you locate metrics more quickly.

- Search for a metric in the Metrics Finder to view related categories and detailed information.
- Click the [Select] button for a metric in the search results to automatically apply the selected value to the event configuration screen.



3. Select the event level (**Critical**, **Warning**, Info). You can configure multiple levels for a single metric.

❗ **Event Level Behavior**

Even when multiple conditions are satisfied, only the highest-priority level (**Critical** → **Warning** → **Info**) triggers an event. For details, see the [Level Action Guide](#).

- Event levels are classified as Critical (**Critical**), Warning (**Warning**), and Info (Info).



- It is recommended to configure multiple levels for the same metric with stepwise thresholds.

4. Enter the field, operator, and value for the selected event level.

a. Click + **Add** to add more conditions.

- **&&** : An event is triggered only when **all conditions are satisfied simultaneously**
- **||** : An event is triggered when **at least one condition is satisfied**

b. Click — to remove the condition.



For condition syntax and supported operators, refer to the [Condition Settings Guide](#).

Trigger Count

Configure how many times a condition must be met before an event is triggered. This is useful for detecting persistent issues only.

1. Select the trigger frequency.

- **Consecutive:** An event is triggered when the condition occurs consecutively for the configured number of times.
- **Recent:** An event is triggered when the condition occurs the configured number of times within the selected time window.
 - Available durations: 5 seconds , 10 seconds , 15 seconds , 30 seconds , 1 minute , 2 minutes , 3 minutes , 4 minutes , 5 minutes , 10 minutes , 30 minutes , 1 hour

2. Enter the trigger count.

- The **Interval** value corresponds to the data collection interval of the selected category. (Interval: 10s)

Pause

To prevent excessive event generation, select a pause duration for event execution. After an event occurs, the same event will not be triggered again during the configured time period.

- Available durations: Disabled , 5 minutes , 10 minutes , 15 minutes , 20 minutes , 30 minutes , 1 hour , 2 hours , 3 hours , 6 hours , 12 hours , 1 day

ⓘ When recovery notifications are enabled

Even if the same event condition is met again, no notification is sent until the configured time has passed since the **RECOVERED** notification was received.

Resolved Notification

When the resolved notification feature is enabled, you can track state changes after an event occurs (in progress → resolved). The event is shown as an ongoing event in the **Event History** menu.

- Resolved notifications apply only to **Critical** and **Warning** levels. Info-level events always operate as one-time events.
- When a **Critical** or **Warning** event is resolved, a notification with the RECOVERED (normal) state is sent.
- Click the toggle button to **enable** or **disable** this feature.
 -  **Enabled:** Events operate based on state. They enter an in-progress state when the threshold is exceeded and transition to a resolved state when the value recovers below the threshold.
 -  **Disabled:** A one-time event is generated each time the threshold is exceeded.

Event Operation Time

Configure tags so that events operate only during specific time periods (such as business hours, non-business hours, or maintenance windows). If no tag is configured, events operate continuously for 24 hours while enabled.

1. Click **+ Add**.
2. In Event Operation Time, click **+ Create New Tag**.

3. In **Create Event Operation Time Tag**, select the **tag name, days, time, and color**, then click the [Apply] button.
4. You can view created tags in the tag list, and apply them by selecting the checkbox.
5. To modify or delete a tag, click the  icon and update or delete it in **Edit Event Operation Time Tag**.

 When a tag is deleted, it is removed from all users to whom it was applied. However, tags that are currently in use by event rules cannot be deleted.

Simulation

The simulation feature lets you pretest configured event conditions using historical data. If the expected number of events is too high or too low, you can adjust the conditions to find optimal threshold values.

- **Rule Validation:** Verify how newly created event rules would behave when applied to historical data.
- **Threshold Tuning:** Adjust thresholds to an appropriate level when events occur too frequently or not at all.

Start Simulation

1. After completing event condition settings, click the [Simulation] button.
2. Review the expected number of events and the visualized results.

Understanding Simulation Results

1. Time-Series Data

A graph displays metric changes over time along with threshold lines for each level, allowing you to intuitively identify when events are triggered.

2. Event Counts by Level

The number of events for the Critical, Warning, and Info levels is shown on the right side of the screen. This helps you understand overall event distribution and frequency.

3. Target-Level Details

Hover over a specific point on the chart to see the exact metric value and monitoring target at that moment. When multiple targets exist, they are distinguished by color. If patterns differ by target, you can use filtering to analyze them individually.

4. Peak Interval Identification

Identify periods where metrics spike sharply to understand when issues occur most frequently or to recognize recurring patterns.

✓ Simulation Tips

- **Simulate Different Time Ranges**

Run simulations for weekdays vs. weekends and peak vs. off-peak hours to set optimal thresholds for each time period.

- **Include Actual Incident Periods**

Include past outage periods in simulations to verify whether current rules accurately detect real incidents.

- **Add Target Filtering**

When many targets are monitored, simulation results can become complex. Use filters to focus on specific targets for clearer insights.

- **Adjust Thresholds Gradually**

Instead of making large changes at once, adjust thresholds incrementally, such as in 10 percent steps, to find optimal values.

Select Event Target

If no event target is specified, events are triggered for all targets in the project, which can result in excessive events. It is therefore recommended to clearly define the targets to which the event applies.

ⓘ If you change the event targets, the number of events may change. Click the **Simulation** button and run it again to check the updated expected event count.

Target Selection

You can specify the targets to which the event applies using either **Select Input** or **Direct Input**.

- **Select Input** **Direct Input**

1. Select or enter a tag, operator, and value.
 - a. If it is difficult to find a tag, you can search for it using the **Metrics Finder**.
2. Click + **Add** to add event targets using conditions (`&&` , `||`).

Enter the tag, operator, and value of the target to monitor directly.

- When you choose direct input, a list of available tags (**Tag Select Input**) is provided below the input field.

```
ex. endsWith(okindName, 'example_name') && container == 'prod.billing'
ex. ${4xxErrorType} == '401'
```

 If you change the input method, any content you have entered will be reset.

Basic Information and Notification Settings

Configure the **event name**, **message**, and **recipients**. Because this information is displayed as is in event history and actual notification messages, it should be clear and easy to identify.

Event Activation

Configure whether the event is triggered when the defined conditions are met.

-  **Enabled:** The event is triggered when the configured conditions are satisfied.
-  **Disabled:** Conditions are not evaluated.

Event Name

Enter the event name to be used as the event title. The configured event name is displayed in the **Event List** and **Event History** menus and can be used as a search keyword.

Message

Enter the event message. The message you enter is used in event history and notifications. Click the  icon to view previously written message history. You can include variables in the message to insert actual values at the time the event occurs.

- **Variable Usage Rules**

- Variable format: `${metric_name}`
- Only metrics within the **same category as the configured category** can be used as variables.
- You can combine multiple variables to create a more detailed message.
- The list of available variables can be found in the **Metrics Query** menu.

- **Variable Usage Example**

	Event Configuration	When Event Occurs
Title	Disk Usage Increase	Disk Usage Increase
Message	Disk = <code>\${disk}%</code>	Disk = 89.9%

Event Recipients

Specify the members who will receive event notifications.

- **Receive All Receive by Tag Selection**

Notifications are sent to all targets (members and channels) in the project that have event reception enabled.

Notifications are sent to project members who have the selected tag.

1. Select **Receive by Tag Selection**.
2. In the **Reception Tag** section, click the [+ Add Tag] or [+] button.
3. Under the **Event Reception Tag** window, click + **Create New Tag**.
4. In the **Create Tag** window, enter a tag name, select a color, and click the [Create Tag] button.
5. You can edit or delete created tags by clicking the  icon in the tag list.

6. In the **Event Reception Tag** window, select the desired tag from the **Tag List** to apply it.

ⓘ Reception Tags

Reception tags are a feature for managing users or channels that receive notifications **at a group level**. When a reception tag is assigned to an event, notifications are delivered only to users associated with that tag. If no reception tag is set, notifications are sent to all users in the project.

Edit/Delete Event

1. Go to **Alert Notifications > Event Settings** and open the **Metrics** tab.
2. In the event list, click the  icon for the event you want to edit or delete.
3. In the **Edit Event Rule** window, update the options and click the [Save] button.
 - a. To delete the selected event, click the [Delete] button in the upper-right corner of the **Edit Event Rule** window.

Event Sharing

You can save metric event settings as a JSON file to share configurations with other users or import settings created by others.

- JSON file name: `event-rules-YYYYMMDD.json`

Export

1. Click the [**JSON** ] button at the top right of the screen.
2. When the JSON editor opens, click the [ Export] button.
 - If you use the export function after searching for events, only the searched list will be downloaded as a JSON file.
3. After the JSON file is downloaded, share it with other users.

Import

1. Click the [] button at the top right of the screen.
2. Select the JSON file downloaded using the **Export** function.
3. When the JSON editor opens, choose either [Add to List] or [Overwrite].

 It is recommended to use this feature between projects of the same product type. You can import event settings from projects of different products, but they may not function correctly.

Edit in JSON Format

1. Click the [**JSON** ] button at the top right of the screen.
2. When the editor opens, modify the content according to the JSON format.
3. After completing the edits, click the [Save] button at the bottom of the screen.

 If the modified content does not conform to the JSON format, an error message will be displayed at the bottom of the screen and the content cannot be saved. The error message may vary depending on the type of formatting issue.

JSON error

JSON Data Structure

```
{
  "version": 2,
  "eventId": "zcef7s7f27rum1",
  "enabled": true,
  "stateful": false,
  "title": "Active Transaction",
  "message": "Active Transaction = ${active_tx_count}",
  "category": "app_counter",
  "alertLabel": [
    "oid"
  ],
  "repeatCount": 1,
  "repeatDuration": 0,
```

```

"silent": 300000,
"receiver": [],
"timeTag": [],
"selectString": "",
"conditions": [
  {
    "level": 20,
    "enabled": true,
    "rule": "active_tx_count > 100"
  }
],
"createTime": 1763632674345,
"lastModifiedTime": 1763632674347,
"lastModifiedUser": "support@whatap.io",
"basic": true,
"metaId": "java004",
"selectCondition": {
  "oid": [
    "-1010758404",
    "-250906941"
  ]
}
}

```

Table | JSON Data Structure

JSON Field	Type	Description	Notes
version	Integer	Version of the event rule	Restricted
eventId	String	Unique identifier of the event rule	
enabled	boolean	Whether the event is enabled	
stateful	boolean	Whether the event is state-based	
title	String	Event rule name defined by the user	
message	String	Event rule message defined by the	

JSON Field	Type	Description	Notes
		user	
category	String	Data category	
alertLabel	List<String>	Default identifier (primary key) value assigned per category for event state management	Restricted
repeatCount	Integer	Number of repetitions	
repeatDuration	Long	Duration for repetition	
silent	Integer	Pause duration	
receiver	List<String>	List of recipient tag keys	
timeTag	List<String>	List of operation-time tag keys	
selectString	String	Target selection	
conditions	List<Object>	List of trigger conditions by level	
◇ level	byte	Level value	Critical : 30, Warning : 20, Info : 10
◇ enabled	boolean	Whether the level is enabled	
◇ rule	String	Trigger condition for the level	
createTime	Long	Initial creation time of the event rule	
lastModifiedTime	Long	Last modification time of the event rule	
lastModifiedUser	String	Account that last modified the event rule	

JSON Field	Type	Description	Notes
basic	boolean	Whether the event was created using Quick Setup	Restricted
metaId	String	Unique identifier of the Quick Setup template	Restricted: This value exists only for events created via Quick Setup (basic=true).
selectCondition	Object	Target selection value for Quick Setup	This value exists only for events created via Quick Setup (basic=true).

 Fields marked as “Restricted” may affect event behavior, so it is recommended not to modify their values.

Appendix

Trigger Conditions and Target Selection Guide

Metric alert trigger conditions and event target selection use the same syntax. However, trigger conditions use the field key as the variable, while target selection uses the tag key as the variable.

Level Behavior Guide

Event levels are categorized into Critical, Warning, and Info.

1. Priority-based Event Triggering

When multiple level conditions are met at the same time, only the event with the highest priority is triggered.

Example

Configuration:

- Warning: CPU > 70%
- Critical: CPU > 90%

Current state: CPU 95%

→ Result: Only the Critical event is triggered (Warning is suppressed)

2. Level Escalation

For events that maintain an in-progress state, when a higher-level condition is met while a lower-level event is already in progress, both levels enter the in-progress state.

Example

Configuration:

- Warning: CPU > 70%
- Critical: CPU > 90%

Scenario:

- 1) CPU 80% → Warning triggered (in progress)
- 2) CPU 95% → Warning (in progress), Critical (in progress)

3. Level De-escalation

For events with an in-progress state, when the level transitions from a higher level to a lower level, the higher-level event is resolved while the lower-level event remains active.

Example

Configuration:

- Warning: CPU > 70%
- Critical: CPU > 90%

Scenario:

- 1) CPU 97% → Critical triggered
- 2) CPU 85% → Critical resolved, Warning remains
- 3) CPU 65% → Warning resolved

4. Execution Flow

- Warning: CPU > 70%

- Critical: CPU > 90%

Metric value: 60% → 75% → 92% → 85% → 60%

State: Info Warning Critical Warning Info
 (triggered) (triggered) (maintained) (resolved)
 Warning
 (maintained)

- ⓘ Events that have an in-progress state remain active as long as their conditions are met and continue until those conditions are cleared.

Condition Configuration Guide

- ⓘ If a metric name starts with a number or contains special characters, you must wrap it in the `${metric_name}` format.

- Brackets `()`, `[]`
- Operators `+`, `-`, `*`, `/`, `%`
- Delimiters `:`, `@`, `#`, `,`, `,`, (space)
- Other special characters `!`, `^`, `&`, `|`, `~`, ```, `"`, `=`

Examples using `${}` :

```
${cpu(xos)} > 50
${mem[0]} >= 100
${cpu-usage} > 80
${namespace:cpu} > 70
${metric name} > 60
${4xx_error} > 10
```

Usable without `${}` : Metric names that contain only alphabetic characters, underscores (`_`), or dots (`.`)



```
cpu > 80
cpu_usage > 50
CPUUtilization.Average > 0.8
```

1. Comparison Operators

Numeric Comparison

```
Greater than:      cpu > 80
Greater than or equal:  cpu >= 80
Less than:         memory < 1000
Less than or equal:  memory <= 1000
Equal to:          status == 200
Not equal to:       error != 0
```

String Comparison

```
status == 'OK'
region == "us-east-1"
```

2. Arithmetic Operators

- Basic arithmetic operations

```
Addition:    cpu + 10 >= 90
Subtraction:  memory - 100 >= 500
Multiplication:  cpu * 2 >= 100
Division:       disk / 1024 >= 100
Modulo:         value % 10 == 0
```

- Controlling precedence with parentheses

```
(cpu + memory) * 2 >= 200
(disk - used) / total >= 0.2
((cpu + memory) / 2) >= 50
```

- Negative values

```
cpu > -100
```

3. Logical Operators

- AND operator (&&)

```
cpu > 80 && memory > 1000  
${cpu(xos)} > 50 && ${mem(xos)} > 60
```

- OR operator (| |)

```
cpu > 90 | | memory > 90  
disk < 10 | | network > 1000
```

- Combined logical operations

```
(cpu > 50 && memory > 50) | | disk < 20  
cpu > 80 && (memory > 1000 | | disk > 500)
```

4. Pattern Matching Operators

- LIKE operator

```
oname like 'prod-*'  
url like '*error*'  
message like 'WARN%'
```

- NOT LIKE operator

```
oname not like 'test-*'  
url not like '*debug*'
```

5. Built-in Functions

- Null check functions

```

isNull(value)      # Checks whether the value is null
isNotNull(value)   # Checks whether the value is not null
nvl(value, 0)      # Returns a default value if null
isEmpty(str)       # Checks whether the string is empty
isNotEmpty(str)    # Checks whether the string is not empty

```

- Aggregate functions

```

sum(cpu, memory, disk)    # Sum
avg(cpu, memory)          # Average
max(cpu, memory, disk)    # Maximum
min(cpu, memory, disk)    # Minimum
count(value1, value2, value3) # Count

```

- Math functions

```

round(cpu, 2)    # Rounds to 2 decimal places

```

- String functions

```

length(str)      # String length
startsWith(str, 'prefix') # Checks prefix
endsWith(str, 'suffix') # Checks suffix
indexOf(str, 'search') # String index
substring(str, 0, 10) # Substring
trim(str)        # Trims whitespace
replace(str, 'old', 'new') # String replacement
hasStr(str, 'search') # Checks string containment

```

- Conditional functions

- **if:** A conditional function that returns the `trueValue` if the condition evaluates to `true`, or the `falseValue` if it evaluates to `false`

Syntax

```

if(condition, trueValue, falseValue)

```

Example

```
if(value >= 90, 'High', 'Medium') == 'High'
```

- **decode:** Compares a value against conditions and returns the result of the matching condition, or a default value if no match is found

Syntax

```
decode(value, condition1, result1, condition2, result2, ..., conditionN, resultN, defaultValue)
```

Example

```
decode(value, 1, 'Low', 2, 'Medium', 3, 'High', 'Unknown') == 'Unknown'
```

- **in:** Returns `true` if the value matches any of the specified candidates; otherwise returns `false`

Syntax

```
in(value, candidate1, candidate2, ..., candidateN)
```

Example

```
in(status, 200, 201, 204) == false
```

! Writing Guidelines

- Recommended
 - Use simple variable names without `${}` (e.g. `cpu`, `memory`)
 - Always use `${}` when special characters are included
 - Use parentheses to clearly separate complex expressions
 - Enter function names exactly as defined (case-sensitive)
- Avoid



- Incomplete expressions (e.g. `cpu > , memory && )`)
- Mismatched parentheses (e.g. `(cpu > 80 && cpu > 70) )`)
- Consecutive or invalid operators (e.g. `cpu >> 80 , cpu >< 80 )`)

Composite Metrics

Home > Select Project >  **Alert** > **Event Configuration** > **Composite metrics** tab

You can create events and send alert notifications using complex rules.

Default Options

- **Search:** Search for specific events by selecting an event name or an event recipient tag
- **JSON Download/Upload:** Edit event rules directly in the JSON editor, or download them as a file, modify them, and upload them again
- **Alert Message Settings:** Select detailed fields for alert messages and edit the content for each field
- **+ Add Event:** Add a new composite metrics event

Permissions

To configure **Composite metrics** events, you must have **Alert Settings** permission. You can grant this permission by clicking the  icon for the member in **Home > Select Project > Management > Integrated Member Management**.

Table | Composite Metrics Event List Layout

Item	Description
Event Title	User-defined event name - Up to 255 bytes
Condition	Event trigger conditions
Notify on Event Recovery	Whether to receive RECOVERED (normal) notifications when Critical or Warning events are resolved – Enabled: Sends a RECOVERED notification when the state changes from in-progress to normal, and allows you to distinguish in-progress and resolved states in event history – Disabled: Triggers a one-time event each time the threshold is exceeded

Item	Description
Event Recipient Tag	Users or groups that receive notifications for the event
	Edit or delete the event
	Event enablement status – Enabled: Event is triggered when conditions are met – Disabled: Event does not run and conditions are not evaluated

Event Configuration

Composite metrics events define event conditions based on **MXQL**, the metric data query language. The **Create from Chart** feature provides a combo box to support MXQL auto-completion.

Add Event

1. Click the **Composite metrics** tab from  **Alert > Event Configuration**.
2. Click the [+ Add Event] button on the right side of the screen.
3. In the **Composite metrics** window, click **Create from Chart**.
 - a. You can use the provided templates.
4. In the **Event Configuration** screen, first query the event data, then configure the event conditions.

Query Event Data

Query event data to build charts. In the **Event Configuration** screen, select either the **Widget** or **Text** option under **Query event data** on the right to configure events.

- Widget Text

Using the options for configuring a time series chart, you can automatically complete the **MXQL** used for event configuration.

1. Select the date range for querying data.
2. Select the **Category** (target) for querying data.
3. Click + **Add Filter** under **Filter** to create event conditions.
 - a. In the filter window, select an expression, tag, and filter value.
 - b. Click + **Add** to add additional conditions.
 - c. To delete a condition, click the – icon next to it.
4. Under **Grouping**, select the grouped metric data. Multiple selections are supported.
5. Under **Time Unit**, set the time interval for grouped data by selecting `seconds` , `minutes` , or `hours` .
6. Under **Field**, select the fields to be used for event trigger conditions. Multiple selections are supported.

 MXQL entered in text mode is not compatible with widget mode.

An editor appears where you can directly modify **MXQL**.

1. Edit **MXQL** directly and click the **Query** button.
2. After selecting a date, you can view the results as a chart or graph.

Notification

Enter the basic information for alert notification settings.

- **Enable Event:** When the toggle is enabled, the event becomes active.
- **Level:** Select the event level (Critical, Warning, Info).
 - **Notify on Event Recovery:** When the toggle is enabled, a notification is sent when the event is resolved and enters the normal (RECOVERED) state.
- **Title:** Enter a title for the event rule.
- **Message:** Enter the content of the alert message delivered when the event is triggered. You can use variables in the message to include actual values at the time the event occurs.

Message example

✔ Variable Usage Rules

- Variable format: `${metricName}`
- Only metrics within the **same category as the configured category** can be used as variables.
- You can combine multiple variables to compose a detailed message.
- The list of available variables can be checked in **Metric Query**.

Event Trigger Conditions

- **Data Query Range:** Select the real-time data query window.
 - Available ranges: 30 seconds , 1 minute , 2 minutes , 5 minutes , 10 minutes , 30 minutes , 1 hour , 2 hours , 3 hours
- **Condition:** Enter the event trigger condition. Only fields included in the event data query can be used.

Additional Information

- **Interval:** The alert condition is evaluated at the selected interval (1 minute , 5 minutes , 10 minutes , 30 minutes , 1 hour , 12 hours).
- **Silence:** After an event is triggered, the same event is suppressed for the selected duration (unset , 1 minute , 5 minutes , 10 minutes , 30 minutes , 1 hour , 12 hours).
- **Event Active Time:** Configure tags to control when the event runs, such as working hours, non-working hours, or maintenance windows. If no tag is set, the event runs continuously for 24 hours while it is enabled.
 1. Click + **Add**.
 2. Under **Event Active Time**, click + **Create New Tag**.
 3. In **Create Event Active Time Tag**, select a **Tag Name**, **Days**, **Time**, and **Color**, then click the [Apply] button.
 4. Created tags appear in the tag list and can be applied by selecting the checkbox.
 5. To edit or delete a tag, click the  icon and modify or remove it in **Edit Event Active Time Tag**.

 When a tag is deleted, it is removed from all users to whom it is applied. However, tags that are

 currently in use by event rules cannot be deleted.

- **Event Recipient Tags:** When recipient tags are configured, notifications are sent to project members who have those tags. If no recipient tag is set, notifications are sent to all users in the project.

1. Click + **Add Tag** or the + icon.
2. Click + **Create New Tag** at the bottom of the **Event Recipient Tags** window.
3. In the **Create Tag** window, enter a tag name, select a color, and click the [Create Tag] button.
4. To edit or delete a created tag, click the  icon in the tag list.
5. Select the desired tag from the **Tag List** in the **Event Recipient Tags** window to apply it.

 When configuring events, selecting event recipient tags allows notifications to be sent to project members and third-party plugins associated with those tags. You can assign tags to project members and third-party plugins separately via **Alert > Notifications**.

Test Event Rules

You can test the configured conditions against historical data to estimate how many events would have been triggered.

1. Select the date for testing the event rules and click the [Confirm] button.
2. Click the [Run] button to check the number of triggered events.

Edit/Delete Event

1. Go to the **Alert > Notifications > Composite metrics** tab.
2. In the composite metrics list, click the  icon of the event you want to edit or delete.
3. In the **Notifications** screen, update the options and click the [Save] button.
 - a. To delete the selected event, click the [Delete] button in the upper right corner of the **Notifications** screen.

Event Sharing

You can save metric event settings as a JSON file to share configurations with other users or import settings created by others.

- JSON file name: `event-rules- YYYYMMDD .json`

Export

1. Click the [**JSON** ] button at the top right of the screen.
2. When the JSON editor opens, click the [ Export] button.
 - If you use the export function after searching for events, only the searched list will be downloaded as a JSON file.
3. After the JSON file is downloaded, share it with other users.

Import

1. Click the [] button at the top right of the screen.
2. Select the JSON file downloaded using the **Export** function.
3. When the JSON editor opens, choose either [Add to List] or [Overwrite].

 It is recommended to use this feature between projects of the same product type. You can import event settings from projects of different products, but they may not function correctly.

Edit in JSON Format

1. Click the [**JSON** ] button at the top right of the screen.
2. When the editor opens, modify the content according to the JSON format.
3. After completing the edits, click the [Save] button at the bottom of the screen.

 If the modified content does not conform to the JSON format, an error message will be displayed at the

! bottom of the screen and the content cannot be saved. The error message may vary depending on the type of formatting issue.

JSON error

Alert Message Settings

You can select detailed fields for the messages to be received and edit the content for each field.

Appendix

MXQL Syntax Guide

Composite metrics operates based on MXQL queries. For detailed syntax, refer to the [MXQL Syntax Guide](#).

Anomaly Detection

Home > Select Project >  **Alert** > **Event Configuration** > **Anomaly detection** tab

Anomaly detection identifies abnormal rising or falling patterns in metric data and triggers events when movements that differ from the usual behavior are detected.

Default Options

- **Search:** Search for specific events by selecting an event name or an event recipient tag.
- **+ Add Event Rule:** Add a new anomaly detection event.

Table | Anomaly Detection Event List Layout

Item	Description
Event Message	Message sent when an event is triggered
Category	Unit used to classify metric data and serve as the basis for metric event configuration
Field	Metric field used to detect anomalies
Filter	Conditions that limit the data range subject to anomaly detection
Rising/Falling Pattern	Sensitivity of rising or falling patterns
Event Recipient Tag	Users or groups that receive notifications for the event
	Edit event settings
	Delete event
	Event enablement status - Enabled: Event is triggered when conditions are met - Disabled: Event does not run and conditions are not evaluated

Event Configuration

You can configure alert notifications to be sent when metric values rise or fall in a way that differs from their usual behavior.

Add Event Rules

1. Click the [+ Add Event Rule] button on the right side of the screen.
2. Configure **Event Basic Information**, **Metrics**, **Anomaly Detection**, and **Additional Information** in order.

Event Basic Information

1. Select the event level (**Critical**, **Warning**, Info).
 - This determines the event priority and alert level.
2. Enter the alert message to be delivered when the event is triggered.
 - You can use variables in the message to include actual values at the time the event occurs.

! Available Variables

- `$pcode` : Project code
- `$category` : Category
- `$field` : Field
- `$value` : Triggered value
- `$oname` : Event target

Metrics

1. Select a **Category**.
 - This category serves as the baseline for the metric data used to detect anomalies.

2. Select the **Field** to be used for the event trigger conditions. Multiple selections are supported.
3. Select filters that define the event condition targets used to narrow the event scope. Multiple selections are supported.

Anomaly Detection

1. Select the sensitivity levels for **Rising Pattern** and **Falling Pattern**.
2. Use the toggle buttons to enable or disable each pattern.
 - To detect only rising patterns: Rising Pattern **ON**, Falling Pattern **OFF**
 - To detect only falling patterns: Falling Pattern **ON**, Rising Pattern **OFF**

Additional Information

Event Active Time

Configure tags to control when an event runs, such as working hours, non-working hours, or maintenance windows. If no tag is set, the event runs continuously for 24 hours while it is enabled.

1. Click **+ Add**.
2. Under **Event Active Time**, click **+ Create New Tag**.
3. In **Create Event Active Time Tag**, select a **Tag Name**, **Days**, **Time**, and **Color**, then click the [Apply] button.
4. Created tags appear in the tag list and can be applied by selecting the checkbox.
5. To edit or delete a tag, click the  icon and modify or remove it in **Edit Event Active Time Tag**.

 When a tag is deleted, it is removed from all users to whom it is applied. However, tags that are currently in use by event rules cannot be deleted.

Event Recipient Tags

When event recipient tags are configured, notifications are sent to project members who have those tags. If no recipient tag is set, notifications are sent to all users in the project.

1. Click + **Add Tag** or the + icon.
2. Click + **Create New Tag** at the bottom of the **Event Recipient Tags** window.
3. In the **Create Tag** window, enter a tag name, select a color, and click the [Create Tag] button.
4. To edit or delete a created tag, click the  icon in the tag list.
5. Select the desired tag from the **Tag List** in the **Event Recipient Tags** window to apply it.

✓ When configuring events, selecting event recipient tags allows notifications to be sent to project members and third-party plugins associated with those tags. You can assign tags to project members and third-party plugins separately via **Alert > Notifications**.

Edit Event

1. Go to the **Alert > Event Configuration > Anomaly detection** tab.
2. In the **Anomaly Detection** list, click the  icon on the right of the event you want to edit.
3. In the **Anomaly Detection** window, update the options and click the [Save] button.

Delete Event

1. Go to the **Alert > Event Configuration > Anomaly detection** tab.
2. In the **Anomaly Detection** list, click the  icon on the right of the event you want to delete.
3. In the delete confirmation window, click the [Delete] button.

Real-time Log Events

Home > Select Project >  **Alert** > **Event Configuration** > **Real-time Log** tab

You can set alert notifications by filtering collected log data against conditions. Log monitoring must be activated to use log events. For more information on **activating log monitoring**, refer to the log documentation for each product.

- **Real-time log event:** An event is triggered when the configured event conditions are met in real-time collected logs.

Default options

- **Search:** Search for events by selecting an event name or event notification tag
- **JSON download/upload:** Event rules can be directly edited through the JSON editor, or downloaded as a file, modified, and re-uploaded
- **Notification message settings:** Select detailed items for the message to receive and edit the content for each item
- **+ Add event:** Add a new log event

Table | Real-time log event list configuration

Item	Description
Event name	Event name used as the notification title - Up to 255 bytes
Category	Log classification name (log folder name)
Search key	The field to search for in log data - Example: To access an HTTP response status code, use the search key <code>status</code>
Search value	The actual value corresponding to the search key. An alert is sent when logs contain the specified value

Item	Description
	- Example: If the search key is <code>status</code> and the search value is <code>200</code>, an alert is triggered when logs containing HTTP status code 200 are collected
Pause event notifications	Pauses the same event notification for a specified time after an event notification is triggered - Available times: Disabled, 5 min, 10 min, 15 min, 20 min, 30 min, 1 hour, 2 hours, 3 hours, 6 hours, 12 hours, 1 day - If resolved notifications are enabled, no notification is sent for the same event during the selected time after receiving a normal (RECOVERED) status notification
Event target filtering	Conditions that define the targets to which the event applies - If no condition is set, alerts are evaluated for all collected data - Select input: Build conditions by selecting tags, operators, and values - Direct input: Manually enter conditions to specify targets
Event notification tags	User or group (notification tag) to receive the event notification
	Edit and delete events
	Whether the event is active - Enabled: Event occurs when conditions are met - Disabled: Event does not operate and conditions are not checked

Event settings

Log events allow you to configure alert notifications when logs are collected in real time or when logs that meet specific conditions accumulate.

Add real-time log event

1. Click the **Real-time Log** tab in **Alert > Event Configuration**.

2. Click the [+ Add event] button on the right side of the screen.
3. Set the log event conditions in the **Add event rule** window.
 - **Event name:** Enter a name to use as the event title.
 - **Event activation:** When the toggle button is activated, an event occurs when conditions are met.
 - **Level:** Select the event level (**Critical**, **Warning**, **Info**).
 - **Message:** Enter the notification message to receive when the event is triggered. You can use variables in the message to include actual values at the time of event occurrence.

✓ **Variable usage rules**

- Variable format: `${metricName}`
 - Only metrics within the **same category as the configured category** can be used as variables.
 - You can combine multiple variables to compose a detailed message.
 - A list of available variables can be checked in **Metrics Query**.
- **Category:** Select the log classification name (log folder name) from the list or enter it directly. You must select a category before entering a search key and search value.
 - **Search key:** Enter the field you want to search for in log data.
 - Example: To access an HTTP response status code, use the search key `status`.
 - **Search value:** Enter the actual value corresponding to the **search key**. An alert is sent when logs contain the specified value.
 - Example: If the **search key** is `status` and the **search value** is `200`, an alert is triggered when logs containing HTTP status code 200 are collected.
 - **Event target filtering:** Enter conditions to define the targets to which the event applies. If no value is entered, alerts are evaluated for all collected data.
 - **Select input:** Select a tag, operator, and value to set the target conditions.

ⓘ For condition expression syntax and supported operators, refer to the [Condition](#)

! settings guide.

- **Direct input:** Enter conditions directly.
- **Pause event notifications:** Select a duration to temporarily suppress alerts. After the event is triggered, the same event will not occur during the selected time.
 - Available times: Disabled , 1 min , 2 min , 3 min , 5 min , 10 min , 20 min , 30 min , 1 hour , 3 hours , 6 hours , 12 hours
- **Event operation time:** Set tags to activate the event during specific time periods (work/non-work/maintenance hours, etc.). If no tag is set, the event operates 24 hours a day when activated.
 1. Click + **Add**.
 2. Click + **Create new tag** in **Event operation time**.
 3. In **Create event operation time tag**, select the **tag name, day of week, time, and color**, then click the [Apply] button.
 4. Created tags can be viewed in the tag list and are applied by selecting the checkbox.
 5. Click the  icon for the tag to modify or delete, and edit or delete the tag in **Edit event operation time tag**.

! Deleting a tag removes the tag for all users to whom it has been applied. However, tags in use by event rules cannot be deleted.

- **Event notification tags:** If notification tags are set for an event, notifications are sent to project members with those tags. If no recipient tags are set, notifications are sent to all users in the project.
 1. Click + **Add tag** or +.
 2. Click + **Create new tag** at the bottom of the **Event notification tags** window.
 3. In the **Create tag** window, enter the tag name, select a color, and click the [Create tag] button to create the tag.

4. Edit or delete created tags by clicking the  icon in the tag list.
5. Select the desired tag from the **tag list** in the **Event notification tags** window to apply it.

✓ When configuring events, you can send notifications to project members and 3rd-party plugins with the selected event notification tags. You can assign tags to project members and 3rd-party plugins respectively in **Alert notifications > Event notification settings**.

4. When configuration is complete in the **Add event rule** window, click the [Save] button.

Edit/delete events

1. Go to the **Real-time log** tab in **Alert > Event Configuration**.
2. Click the  icon for the event to edit or delete in the log event list.
3. Modify options in the **Event settings** screen and click the [Save] button.
 - a. To delete the selected event, click the [Delete] button in the upper right of the **Event settings** screen.

Event sharing

You can save metric event settings as a JSON file to share configurations with other users or import settings created by others.

- JSON file name: **event-rules-** `YYYYMMDD` **.json**

Export

1. Click the [**JSON** ] button at the top right of the screen.
2. When the JSON editor opens, click the [ **Export**] button.
 - If you use the export function after searching for events, only the searched list will be downloaded

as a JSON file.

3. After the JSON file is downloaded, share it with other users.

Import

1. Click the [] button at the top right of the screen.
2. Select the JSON file downloaded using the **Export** function.
3. When the JSON editor opens, choose either [Add to List] or [Overwrite].

 It is recommended to use this feature between projects of the same product type. You can import event settings from projects of different products, but they may not function correctly.

Edit in JSON Format

1. Click the [JSON ] button at the top right of the screen.
2. When the editor opens, modify the content according to the JSON format.
3. After completing the edits, click the [Save] button at the bottom of the screen.

 If the modified content does not conform to the JSON format, an error message will be displayed at the bottom of the screen and the content cannot be saved. The error message may vary depending on the type of formatting issue.

JSON error

Appendix

Trigger Conditions and Target Selection Guide

Metric alert trigger conditions and event target selection use the same syntax. However, trigger conditions use the field key as the variable, while target selection uses the tag key as the variable.

Level Behavior Guide

Event levels are categorized into Critical, Warning, and Info.

1. Priority-based Event Triggering

When multiple level conditions are met at the same time, only the event with the highest priority is triggered.

Example

```
Configuration:  
- Warning: CPU > 70%  
- Critical: CPU > 90%  
  
Current state: CPU 95%  
→ Result: Only the Critical event is triggered (Warning is suppressed)
```

2. Level Escalation

For events that maintain an in-progress state, when a higher-level condition is met while a lower-level event is already in progress, both levels enter the in-progress state.

Example

```
Configuration:  
- Warning: CPU > 70%  
- Critical: CPU > 90%  
  
Scenario:  
1) CPU 80% → Warning triggered (in progress)  
2) CPU 95% → Warning (in progress), Critical (in progress)
```

3. Level De-escalation

For events with an in-progress state, when the level transitions from a higher level to a lower level, the higher-level event is resolved while the lower-level event remains active.

Example

Configuration:

- Warning: CPU > 70%
- Critical: CPU > 90%

Scenario:

- 1) CPU 97% → Critical triggered
- 2) CPU 85% → Critical resolved, Warning remains
- 3) CPU 65% → Warning resolved

4. Execution Flow

- Warning: CPU > 70%
- Critical: CPU > 90%

Metric value: 60% → 75% → 92% → 85% → 60%

State:	Info	Warning	Critical	Warning	Info
		(triggered)	(triggered)	(maintained)	(resolved)
		Warning			
		(maintained)			

- ⓘ Events that have an in-progress state remain active as long as their conditions are met and continue until those conditions are cleared.

Condition Configuration Guide

- ⓘ If a metric name starts with a number or contains special characters, you must wrap it in the `${metric_name}` format.

- Brackets `()`, `[]`
- Operators `+`, `-`, `*`, `/`, `%`
- Delimiters `:`, `@`, `#`, `,`, `.`, (space)
- Other special characters `!`, `^`, `&`, `|`, `~`, `"`, `=`

Examples using `${}` :



```

${cpu(xos)} > 50
${mem[0]} >= 100
${cpu-usage} > 80
${namespace:cpu} > 70
${metric name} > 60
${4xx_error} > 10

```

Usable without `${}` : Metric names that contain only alphabetic characters, underscores (`_`), or dots (`.`)

```

cpu > 80
cpu_usage > 50
CPUUtilization.Average > 0.8

```

1. Comparison Operators

Numeric Comparison

```

Greater than:      cpu > 80
Greater than or equal:  cpu >= 80
Less than:         memory < 1000
Less than or equal:  memory <= 1000
Equal to:          status == 200
Not equal to:       error != 0

```

String Comparison

```

status == 'OK'
region == "us-east-1"

```

2. Arithmetic Operators

- Basic arithmetic operations

```

Addition:    cpu + 10 >= 90
Subtraction: memory - 100 >= 500
Multiplication: cpu * 2 >= 100

```

```
Division:  disk / 1024 >= 100
Modulo:    value % 10 == 0
```

- Controlling precedence with parentheses

```
(cpu + memory) * 2 >= 200
(disk - used) / total >= 0.2
((cpu + memory) / 2) >= 50
```

- Negative values

```
cpu > -100
```

3. Logical Operators

- AND operator (&&)

```
cpu > 80 && memory > 1000
${cpu(xos)} > 50 && ${mem(xos)} > 60
```

- OR operator (||)

```
cpu > 90 || memory > 90
disk < 10 || network > 1000
```

- Combined logical operations

```
(cpu > 50 && memory > 50) || disk < 20
cpu > 80 && (memory > 1000 || disk > 500)
```

4. Pattern Matching Operators

- LIKE operator

```
oname like 'prod-*'
url like '*error*'
```

```
message like 'WARN%'
```

- NOT LIKE operator

```
oname not like 'test-*'
url not like '*debug*'
```

5. Built-in Functions

- Null check functions

```
isNull(value)      # Checks whether the value is null
isNotNull(value)   # Checks whether the value is not null
nvl(value, 0)      # Returns a default value if null
isEmpty(str)       # Checks whether the string is empty
isNotEmpty(str)    # Checks whether the string is not empty
```

- Aggregate functions

```
sum(cpu, memory, disk)    # Sum
avg(cpu, memory)          # Average
max(cpu, memory, disk)    # Maximum
min(cpu, memory, disk)    # Minimum
count(value1, value2, value3) # Count
```

- Math functions

```
round(cpu, 2)    # Rounds to 2 decimal places
```

- String functions

```
length(str)      # String length
startsWith(str, 'prefix') # Checks prefix
endsWith(str, 'suffix') # Checks suffix
indexOf(str, 'search') # String index
substring(str, 0, 10) # Substring
```

```
trim(str)          # Trims whitespace
replace(str, 'old', 'new') # String replacement
hasStr(str, 'search') # Checks string containment
```

- Conditional functions

- **if:** A conditional function that returns the `trueValue` if the condition evaluates to `true`, or the `falseValue` if it evaluates to `false`

Syntax

```
if(condition, trueValue, falseValue)
```

Example

```
if(value >= 90, 'High', 'Medium') == 'High'
```

- **decode:** Compares a value against conditions and returns the result of the matching condition, or a default value if no match is found

Syntax

```
decode(value, condition1, result1, condition2, result2, ..., conditionN, resultN, defaultValue)
```

Example

```
decode(value, 1, 'Low', 2, 'Medium', 3, 'High', 'Unknown') == 'Unknown'
```

- **in:** Returns `true` if the value matches any of the specified candidates; otherwise returns `false`

Syntax

```
in(value, candidate1, candidate2, ..., candidateN)
```

Example

```
in(status, 200, 201, 204) == false
```

Writing Guidelines

- Recommended
 - Use simple variable names without `${}` (e.g. `cpu`, `memory`)
 - Always use `${}` when special characters are included
 - Use parentheses to clearly separate complex expressions
 - Enter function names exactly as defined (case-sensitive)
- Avoid
 - Incomplete expressions (e.g. `cpu >` , `memory &&`)
 - Mismatched parentheses (e.g. `(cpu > 80 && cpu > 70)`)
 - Consecutive or invalid operators (e.g. `cpu >> 80` , `cpu >< 80`)

Composite Log Event Settings

Home > Select Project >  **Alert** > **Event Configuration** > **Composite Log** tab

You can set alert notifications by filtering collected log data against conditions. Log monitoring must be activated to use log events. For more information on **activating log monitoring**, refer to the log documentation for each product.

- **Composite log event:** An event is triggered when the number of logs that meet the log search conditions within the configured **data query range** reaches or exceeds the threshold count.

Permission

Alert configuration permission is required to configure composite metrics events. Alert configuration permission can be set by clicking the  icon for the member to grant permission in **Home Screen** > **Select Project** > **Management** > **Integrated Member Management**.

Default options

- **Search:** Search for events by selecting an event name or event notification tag
- **JSON download/upload:** Event rules can be directly edited through the JSON editor, or downloaded as a file, modified, and re-uploaded
- **Notification message settings:** Select detailed items for the message to receive and edit the content for each item
- **+ Add event:** Add a new log event

Table | Composite log event list configuration

Item	Description
Event name	Event name used as the notification title
Template	Composite log template

Item	Description
Category	Log classification name (log folder name)
Rule	Conditions that trigger the event
Additional notification when event is resolved	Whether to receive notifications in normal (RECOVERED) status when Critical and Warning level events are resolved - Enabled: Sends a RECOVERED notification when transitioning from in-progress → normal status, and the in-progress/resolved status can be distinguished in event history - Disabled: A one-time event occurs each time the threshold is exceeded
Pause event notifications	Pauses the same event notification for a specified time after an event notification is triggered - Available times: Disabled, 5 min, 10 min, 15 min, 20 min, 30 min, 1 hour, 2 hours, 3 hours, 6 hours, 12 hours, 1 day - If resolved notifications are enabled, no notification is sent for the same event during the selected time after receiving a normal (RECOVERED) status notification
Interval	Time range for querying log data
Event notification tags	User or group (notification tag) to receive the event notification
	Edit and delete events
	Whether the event is active - Enabled: Event occurs when conditions are met - Disabled: Event does not operate and conditions are not checked

Event settings

The composite log event feature triggers alert notifications when the number of logs matching the log search conditions within the configured **data query range** reaches or exceeds the threshold count.

Add composite log event

1. Click the **Composite Log** tab in **Alert > Event Configuration**.
2. Click the [+ Add event] button on the right side of the screen.
3. Set the log event conditions in the **Add event rule** window. For details, refer to [Basic settings](#), [Detail settings](#), and [Additional settings](#).

Add composite log event

4. When configuration is complete in the **Add event rule** window, click the [Save] button.

Basic settings

- **Event name:** Enter a name to use as the event title.
- **Event activation:** When the toggle button is activated, an event occurs when conditions are met.
- **Level:** Select the event level (**Critical**, **Warning**, Info).

Detail settings

Configure [Template \(preset\)](#), [Message](#), [Category](#), [Filter](#), and [Event trigger conditions](#).

Template (preset)

Selecting a predefined preset automatically configures the **filter**, **query type**, and **event trigger conditions**. You can modify the settings after selecting a preset.

Composite log template types		
Preset	Query type	Default rule
None	none	rows > 10
2xx status code count	count	count > 10



Preset	Query type	Default rule
3xx status code count	count	count > 10
4xx status code count	count	count > 10
5xx status code count	count	count > 10
Normal status code (2xx, 3xx) count	count_v2	include_minus_exclude_count > 10
Error status code (4xx, 5xx) count	count_v2	include_minus_exclude_count > 10
Error received count	count	count > 10
Exception received count	count	count > 10
Log count per second	rps	rps > 100
Field aggregation (Aggregation)	aggr	avg > 1000
Rate	rate	rate > 10
Unique value count (Cardinality)	cardinality	cardinality > 100
Percentile	percentile	p99 > 3000

Message

Enter the notification message to receive when an event occurs. You can use variables in the message to compose dynamic notifications.

- **Example:** Message `${host} error ${count} occurred` → Notification message web-01 error 15 occurred

Table | Message variables

Variable	Description	Usage condition
<code>\${count}</code>	Number of logs matching the condition	Always available
<code>\${groupField}</code>	Grouping field name	Grouped notifications only
<code>\${groupValue}</code>	Grouping field value	Grouped notifications only
<code>\${fieldName}</code>	Grouping field value (referenced directly by field name)	Grouped notifications only

ⓘ The `${count}` variable can be used in all notifications regardless of grouping. The `${groupField}`, `${groupValue}`, and `${fieldName}` variables are only substituted when a grouping field is configured.

Category

Select the log classification name (log folder name) from the list or enter it directly. You can enter the search key and search value only after selecting a category.

Filter

Enter log search conditions using Lucene query syntax. Two input modes are supported.

- **Filter mode** : Build a query by selecting fields and values.
- **Code mode** : Enter Lucene queries directly.

Table | Lucene query examples

Query	Description
<code>level:ERROR</code>	Logs where the level field is ERROR
<code>status_nxx:status_4xx OR status_nxx:status_5xx</code>	4xx or 5xx status codes
<code>appender:accessLog</code>	Logs from the accessLog appender
<code>response_time.n:*</code>	Logs where the response_time.n field exists

Query	Description
host:web-01 AND level:ERROR	Error logs from host web-01

Event trigger conditions

Configure by query type. Additional settings are displayed depending on the selected template (preset) or query type.

Table | Event trigger condition key meanings

Key	Meaning
rows / count	Number of logs matching the filter condition
rps	Log count per second (count / interval in seconds)
avg	Average value of the target field
sum	Sum of the target field values
min	Minimum value of the target field
max	Maximum value of the target field
rate	Numerator count / denominator count × 100 (%)
cardinality	Number of unique values in the target field
p99 / p95 / p90 / p75 / p50	Percentile values of the target field
include_minus_exclude_count	Include filter count – exclude filter count

- **Count (count / none):** Counts the number of logs matching the configured filter conditions.

Table | Count settings

Setting	Description
Filter	Log search condition (Lucene query)
Event trigger condition	<code>count</code> or <code>matching logs</code> <code>{operator}</code> <code>{threshold}</code> (e.g., <code>count > 10</code>)

- **Log count per second (rps):** Calculates the number of logs per second (Requests Per Second) matching the configured filter conditions. The total count during the interval is divided by the interval in seconds.

Table | Log count per second settings

Setting	Description
Filter	Log search condition (Lucene query)
Event trigger condition	<code>RPS</code> <code>{operator}</code> <code>{threshold}</code> (e.g., <code>rps > 0.5</code>)

- **Field aggregation (aggr):** Calculates the aggregated value (average, sum, min, max) of the specified numeric field. The aggregation method can be selected from a dropdown in the event trigger condition.

Table | Field aggregation settings

Setting	Description
Filter	Log search condition (Lucene query)
Target field	Numeric field to aggregate (e.g., <code>response_time.n</code>)
Event trigger condition	<code>avg / sum / min / max</code> <code>{operator}</code> <code>{threshold}</code> (e.g., <code>avg > 1000</code>)

- **Rate:** Calculates the percentage (%) ratio of the numerator filter count to the denominator filter count. Useful for monitoring the ratio of specific conditions against all logs.

Table | Rate settings

Setting	Description
Filter (numerator)	Log condition for the numerator (e.g., <code>level:ERROR</code>)
Denominator filter	Log condition for the denominator (e.g., <code>level:*</code>)
Event trigger condition	<code>Rate (%) {operator} {threshold}</code> (e.g., <code>rate > 10</code>)

- **Example:** Filter `level:ERROR`, denominator filter `level:*`, rule `rate > 10` → Alert triggered when the error rate among all logs exceeds 10%
- **Unique value count (cardinality):** Counts the number of unique values in the specified field. Useful for detecting an abnormally large variety of values.

Table | Unique value count settings

Setting	Description
Filter	Log search condition (Lucene query)
Target field	Field to calculate unique values for (e.g., <code>host</code>)
Event trigger condition	<code>Unique value count {operator} {threshold}</code> (e.g., <code>cardinality > 100</code>)

- **Percentile:** Calculates the percentile value of the specified numeric field. Useful for monitoring tail latency in response times. Changing the percentile selection automatically updates the key in the event trigger condition.

Table | Percentile settings

Setting	Description
Filter	Log search condition (Lucene query)
Target field	Numeric field to calculate percentile for (e.g., <code>response_time.n</code>)
Percentile	Select from P99, P95, P90, P75, P50

Setting	Description
Event trigger condition	P99 / P95 / ... {operator} {threshold} (e.g., p99 > 3000)

Table | Percentile meanings

Percentile	Meaning
P50	Median. 50% of all data is at or below this value
P75	75% of all data is at or below this value
P90	90% of all data is at or below this value
P95	95% of all data is at or below this value
P99	99% of all data is at or below this value

- **Include/exclude count (count_v2):** Calculates the net count by subtracting the exclude filter count from the include filter count.

Table | Include/exclude count settings

Setting	Description
Filter (include)	Log conditions to include (e.g., status_nxx:status_4xx OR status_nxx:status_5xx)
Filter exclude	Log conditions to exclude (e.g., status_nxx:status_4xx)
Denominator filter	Denominator for ratio calculation (optional)
Event trigger condition	Include-exclude count {operator} {threshold} (e.g., include_minus_exclude_count > 10)

- **Example:** Filter status_nxx:status_4xx OR status_nxx:status_5xx , filter exclude status_nxx:status_4xx → Alert triggered when the net 5xx count (4xx+5xx minus 4xx) exceeds 10

Group by field (Group By)

When a group by field is configured, alert conditions are evaluated independently for each value of that field. Select the field to group by from the dropdown. Clicking the dropdown shows a list of available fields for the current category with autocomplete.

- **Example:** Filter `level:ERROR` , group by field `host` , rule `rows > 3`

Table | Grouping comparison

Item	Without grouping	With grouping
Evaluation unit	All logs aggregated as one	Independent aggregation per group value
Alert occurrence	1 alert	One per group meeting the condition
Alert title	Event title	[Group value] Event title
Stateful	State transition based on all logs	Independent state transition per group

- `[web-01] Error alert` — 8 errors from web-01 → alert triggered
- `[web-02] Error alert` — 5 errors from web-02 → alert triggered
- `[api-01] Error alert` — 2 errors from api-01 → condition not met, no alert

❗ When **Additional notification when event is resolved** is enabled, the ABNORMAL → RECOVERED state transition occurs independently per group. For example, when errors from `web-01` are resolved, a `[web-01] RECOVERED` notification is triggered, with no effect on other hosts.

Additional settings

- **Interval:** Check alert conditions at the selected time interval (`unset` , `1 min` , `5 min` , `10 min` , `30 min` , `1 hour` , `12 hours`).
- **Mute:** After an event occurs, the same event is not triggered during the selected time (`unset` , `1 min` , `5 min` , `10 min` , `30 min` , `1 hour` , `12 hours`).

- **Event operation time:** Set tags to activate the event during specific time periods (work/non-work/maintenance hours, etc.). If no tag is set, the event operates 24 hours a day when activated.
 1. Click **+ Add**.
 2. Click **+ Create new tag** in **Event operation time**.
 3. In **Create event operation time tag**, select the **tag name**, **day of week**, **time**, and **color**, then click the **[Apply]** button.
 4. Created tags can be viewed in the tag list and are applied by selecting the checkbox.
 5. Click the  icon for the tag to modify or delete, and edit or delete the tag in **Edit event operation time tag**.

 Deleting a tag removes the tag for all users to whom it has been applied. However, tags in use by event rules cannot be deleted.

- **Event notification tags:** If notification tags are set for an event, notifications are sent to project members with those tags. If no recipient tags are set, notifications are sent to all users in the project.
 1. Click **+ Add tag** or **+**.
 2. Click **+ Create new tag** at the bottom of the **Event notification tags** window.
 3. In the **Create tag** window, enter the tag name, select a color, and click the **[Create tag]** button to create the tag.
 4. Edit or delete created tags by clicking the  icon in the tag list.
 5. Select the desired tag from the **tag list** in the **Event notification tags** window to apply it.

 When configuring events, you can send notifications to project members and 3rd-party plugins with the selected event notification tags. You can assign tags to project members and 3rd-party plugins respectively in **Alert notifications > Event notification settings**.

Simulation

You can simulate using historical data before saving the alert to check the expected number of alert occurrences.

1. After completing the alert configuration, select a time range at the bottom.
2. Click the [Simulation] button.
3. The chart displays data by time period and the number of alert occurrences.

 You can adjust the simulation time range to check alert occurrence patterns across different time periods. Data from the last 1–2 minutes may not be available due to index build delays.

4. When configuration is complete in the **Add event rule** window, click the [Save] button.

Create alert from Log Explorer

You can create alerts directly from Log Explorer.

1. Navigate to **Log > Log Search** menu.
2. Configure the category and search query.
3. Click the [Add event] button in the upper right of the screen.
4. The alert configuration form opens in a drawer, with the current category and search query automatically filled in.
5. Complete additional settings and click the [Save] button.
6. After saving, click the [Go] button to navigate to the alert list.

Edit/delete events

1. Go to the **Composite log** tab in **Alert > Event Configuration**.
2. Click the  icon for the event to edit or delete in the log event list.
3. Modify options in the **Event settings** screen and click the [Save] button.
 - a. To delete the selected event, click the [Delete] button in the upper right of the **Event settings** screen.

Event sharing

You can save metric event settings as a JSON file to share configurations with other users or import settings created by others.

- JSON file name: `event-rules-YYYYMMDD.json`

Export

1. Click the [**JSON** ] button at the top right of the screen.
2. When the JSON editor opens, click the [ Export] button.
 - If you use the export function after searching for events, only the searched list will be downloaded as a JSON file.
3. After the JSON file is downloaded, share it with other users.

Import

1. Click the [] button at the top right of the screen.
2. Select the JSON file downloaded using the **Export** function.
3. When the JSON editor opens, choose either [Add to List] or [Overwrite].

 It is recommended to use this feature between projects of the same product type. You can import event settings from projects of different products, but they may not function correctly.

Edit in JSON Format

1. Click the [**JSON** ] button at the top right of the screen.
2. When the editor opens, modify the content according to the JSON format.
3. After completing the edits, click the [Save] button at the bottom of the screen.

- ❗ If the modified content does not conform to the JSON format, an error message will be displayed at the bottom of the screen and the content cannot be saved. The error message may vary depending on the type of formatting issue.

JSON error

Database

Home > Select project >  **Alert** > **Event Configuration** classic

Alert notifications are sent by configuring event conditions for each database metric. By entering threshold values per metric, notifications can be sent at **Critical** and **Warning** levels.

Default options

You can configure event conditions based on key metrics of the database instance.

- **Instance:** The database agent for which event conditions are configured
- **Database:** The target database to monitor
- **Inactive agent alert:** Sends an alert when no response is received from the agent after the configured time

Table | Database event configuration screen

Item	Description
Metrics	Database metrics used to define event conditions
Critical	Threshold for the Critical level
Warning	Threshold for the Warning level
Detection count	The number of consecutive times the metric exceeds the threshold while being collected every 5 seconds – Example: If set to 3, an alert is triggered when the condition is met for 5 seconds × 3 consecutive times
Send notification when event is resolved	Sends an additional notification when the event state is recovered after occurring – Supported in DBX agent version 1.6.30 or later
	Delete event

Item	Description
	Enable or disable the event - Enabled: An event occurs when conditions are met - Disabled: The event does not operate and conditions are not evaluated

Add event

Based on the selected **Metrics** item, you can configure alerts to be sent when the entered **Critical** and **Warning** conditions are met for the specified **Detection count**.

1. Navigate to **Alert > Event Configuration** *classic*.
2. Select the agent for which you want to configure alerts under **Instance**.
3. Click the [+ Add event] button.
4. Select the desired metric from **Metrics**.
5. Choose a comparison operator (**<** , **≤** , **>** , **≥**) for **Critical** and **Warning**, then enter values.
 - An alert is triggered when the configured value is exceeded.
6. Enter the desired value for **Detection count**.
 - An alert is triggered when the condition occurs consecutively at 5 second intervals for the specified count.
 - Example: If the detection count is 3
 5 seconds (1st) - 5 seconds (2nd) - 5 seconds (3rd) → Total 15 seconds → Alert sent
7. If **Send notification when event is resolved** is enabled, an additional notification is sent when the event state is recovered (RECOVERED).

 The **Send notification when event is resolved** feature is supported in **DBX agent version 1.6.30 or later**.
8. Enable the toggle button on the far right () to send alert notifications.
 - a. To delete an event, click the  icon for that event.

Copy alerts

You can copy alert events created for the currently selected instance to other instances.

1. Navigate to **Alert > Event Configuration** *classic*.
2. Click the [Copy alerts] button.
3. In the **Copy alerts** window, select the target instances. To copy to all instances, select **Select all**.
4. Click the [Copy] button to duplicate the alerts.

 If you use the **Copy alerts** feature when the target instance already has alert events configured, the existing alert events will be deleted.

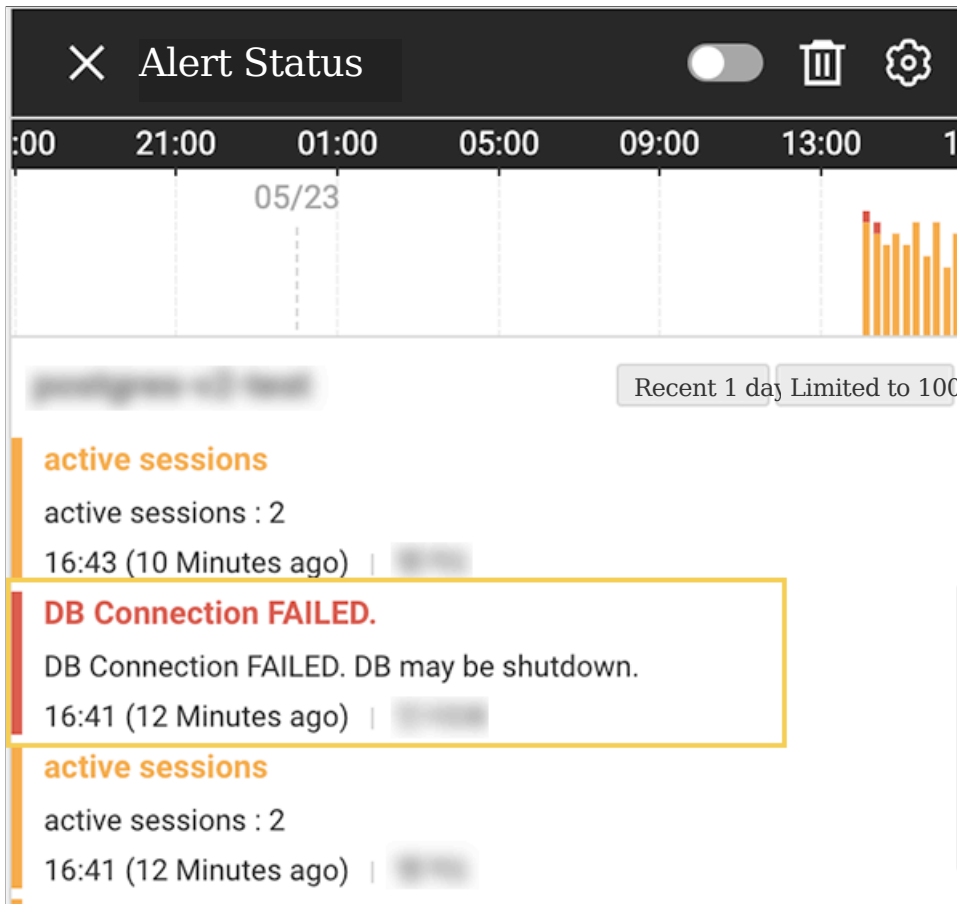
Inactive agent alert

An alert is sent when no response is received from the agent after the configured time.

1. Navigate to **Alert > Event Configuration** *classic*.
2. Under **Inactive agent alert**, select the desired time (30 seconds , 1 minute , 2 minutes , 3 minutes , 5 minutes , 10 minutes , 30 minutes).
3. Click the toggle button on the right to enable it.
 -  **Enabled:** If no data is received from the agent for the configured time, an **INACTIVE MONITORING AGENT** event occurs.

Default alert: Connection FAILED

Even without configuring event rules, an alert is sent when the agent fails to connect to the database 15 times or more. This may occur due to database shutdowns, network issues, or account or permission problems.



Event Notification Settings

Home > Select Project >  **Alert** > **Notifications**

Event Notification Settings per User

 Information about other members in **Event notification settings per-user** can only be viewed by members with the **Member Management** permission. For all other members, required information is masked.

- Mobile device management for bulk event notification receipt settings and access control can be managed in **Account Information**.
- For detailed information about member permissions, refer to the [following document](#).

Notification Methods

Alerts are available via [Email](#), [SMS](#), [WhatsApp](#), and [Mobile](#).

In the **Event notification settings per-user** section, select the checkbox for the desired notification method to receive alerts. If you clear the checkbox for a notification method, alerts will not be sent through that channel.

 All users except the project super administrator can change only their own notification settings.

Email Alerts

Email alerts are sent to the email address provided during sign-up.

SMS Alerts

You can receive alerts via SMS.

ⓘ The SMS alert feature is available only for paid projects.

1. Click your **profile icon** at the top right of the screen, then go to **Manage Accounts**.
2. In **Account Information**, click the [General Mobile Phone] button in the **User Phone Number** section.
3. Enter the **phone number** that will receive the verification code.
 - Only **Korean mobile phone numbers** can be registered to receive SMS alerts.
4. Click the [Save] button.

✔ Change or delete the registered phone number

- To change the phone number, click the [Change] button. SMS verification is required.
- To delete the phone number, click the [Delete] button. After deletion, you will no longer receive alerts via SMS.

WhatsApp Alerts

You can receive alerts via WhatsApp.

ⓘ The WhatsApp alert feature is available only for paid projects.

1. Click your **profile icon** at the top right of the screen and go to **Manage Accounts**.
2. In **Account Information**, click the [WhatsApp] button in the **User Phone Number** section.
3. Enter the **phone number** that will receive the verification code.
4. Click the [Send Verification Code] button.
5. Enter the 6-digit verification code sent to your WhatsApp application.
 - If you do not receive the verification code within 10 minutes, click the [Resend Verification Code] button.
6. Click the [Verify] button.

Mobile Alerts

Users who need to receive mobile alerts must install the WhaTap application on their mobile device and log in.

- Download the WhaTap application – [Android](#)
- Download the WhaTap application – [iOS](#)

Repeated Alerts (Escalation) Settings

If the alert condition is not resolved after an alert is triggered, you can configure repeated alert intervals based on the time of the initial alert. This setting applies only to **Critical** level alerts.

For example, to repeat alerts immediately (0 minutes), 1 hour later, and 1 day later after the initial alert, enter `0,1H,1D` in the **Repeated Alerts (Escalation)** column.

1. Go to **Alert > Notifications** and navigate to the **Event notification settings per-user** section.
2. Configure the settings in the **Repeated Alerts (Escalation)** field.
 - **M**: minutes, **H**: hours, **D**: days. If the unit is omitted, the value is interpreted as minutes.
 - Enter a number or a number with a unit (**M**, **H**, **D**). If the input format is invalid, an error message is displayed.
3. Click the [Save] button. The settings will not be applied unless they are saved.

Event Reception Tags

When configuring events, you can select **event reception tags** to send alerts to project members and 3rd-party plugins associated with those tags. If no event reception tag is set, alert notifications are sent to **all project members**.

Add / Edit / Delete Event Reception Tags

 Event reception tags that are **currently applied to an event** cannot be deleted.

1. Go to **Alert > Notifications**.

2. In the user list under the **Event notification settings per-user** section, click + **Add Tag** or +.
3. In the **Event reception tag** window, click + **Create New Tag**.
4. In the **Create Tag** dialog, enter a tag name, select a color, and click the [Create Tag] button.
5. To edit or delete a created tag, click the  icon in the tag list.
6. Select the desired tag from the **Tag List** in the **Event reception tag** window to apply it.

Remove Event Reception Tags

1. Go to **Alert > Notifications** and open the **Event notification settings per-user** section.
2. Click + in the **Event reception tag** field for the user whose event reception tag you want to remove.
3. In the **Event reception tag** window, click the **X** on the tag you want to remove. The tag will be removed.

Receive Alerts Without Reception Tags

When configuring events, you can select event reception tags to send alerts to project members and 3rd-party plugins associated with those tags.

- To receive alerts **without event reception tags**, enable the **Receive alerts without reception tags** option.
- If you want to receive **only alerts that have event reception tags**, disable this option.

 To stop receiving all alerts, disable this option and make sure that no **Event reception tag** is selected.

Selecting the event reception mode

In the **Event notification settings per-user** section, you can select the event alert reception scope per member or third-party channel from the following three modes. The reception mode is selected in the **Event reception tags** column of each member or channel row.

Mode	Description
Receive all alerts	Receive all alerts regardless of the event reception tags
Receive alerts for selected tags	Receive only alerts that have the selected event reception tags. Select at least

Mode	Description
only	one tag
Receive no alerts	Receive no event alerts. The selected tags are preserved without being deleted

- In the **Receive alerts for selected tags only** mode, select at least one tag to receive alerts in the tag selection area.
- To also receive alerts that have no event reception tag specified, select the **Unclassified** virtual tag in the tag selection area. The **Unclassified** tag can be selected or deselected like a normal tag, but the tag itself cannot be edited or deleted.

ⓘ In the **Receive no alerts** mode, the corresponding member or channel receives no event alerts at all. The selected tags are preserved without being deleted, so if you switch back to the **Receive alerts for selected tags only** mode, you can use the previously selected tag settings as is.

Select Notification Language

You can choose the language in which you receive alert notifications.

1. Go to **Alert > Notifications**.
2. In the user list under the **Event notification settings per-user** section, click the ► button at the far left of the user whose language you want to configure.
3. Select the **Notification Language**.

Day and Time-based Notification Settings

You can configure whether a user receives notifications by day of the week and time of day.

1. Go to **Alert > Notifications**.
2. In the user list under the **Event notification settings per-user** section, click the ► button at the far left of the user whose day and time settings you want to configure.

3. Select the days and/or enter the time ranges during which you want to receive alerts.

- Settings can be configured separately for each notification method.

3rd-party Plugins

You can receive alert notifications through external applications.

- **Supported applications:** Slack, Telegram, Teams, Teams Workflows, Jandi, AlertNow, Webhook, Webhook JSON, Opsgenie, PagerDuty, LINE, ilert

ⓘ Internal messengers that are not included in WhaTap Labs' supported scope can be integrated via standard **Webhook** or **Webhook JSON**.

Table | 3rd-party Plugin List

Item	Description
Plugin Name	Name of the plugin
Auth Key	Authentication key
Auth Value	Authentication value
Receive Level	Notification level: Warning, All, or Critical
Repeated Alerts (Escalation)	Re-notification interval from the initial alert time if the issue is not resolved - Applies only to Critical alerts
Smart Message (AI)	AI-powered notifications available when adding the Telegram plugin - Supported languages: Korean, English, Japanese
Event Reception Tag	Whether to receive alerts for specific members or teams in the project
Delete	Delete the 3rd-party plugin

Add a 3rd-party Plugin

1. Go to **Alert > Notifications**.
2. In the **3rd-party Plugins** section, click **Add**.
3. In the **Add 3rd-party Plugin** window, select the desired service tab.
4. Follow the instructions for the selected service (see [How to add 3rd-party plugin notifications](#)).
5. Click **Test Receive** to verify the configuration.
6. When finished, click **Add** or **Register**.

How to Add 3rd-party Plugin Notifications

Slack

- ⓘ In the **Add 3rd-party Plugin** window, click the [**Add To Slack**] button on the **Slack** tab to register **WhaTapNotiBot** to your Slack team and channel.

Telegram

- ⓘ
1. In **Telegram**, search for **@WhaTapApmNotiBot**.
 2. Select the bot and click the [**Start**] button.
 3. In the chat window, enter the `/license` command followed by the access key of the project for which you want to receive alerts.

Telegram

ⓘ Available commands

- `/help` : View the list of commands
- `/license` : Enter the access key of the project to receive alerts

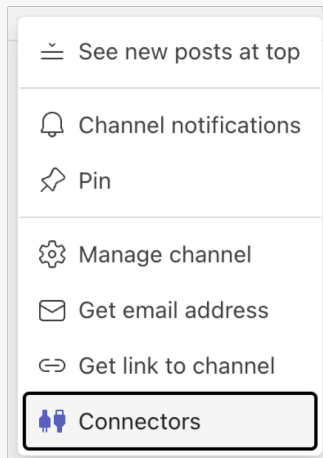


- `/remove` : Enter the project code for which you want to stop receiving alerts
- `/list` : View the list of project codes currently receiving alerts

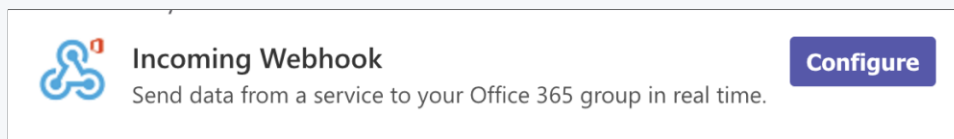
Teams



1. Go to the **connector** of the channel where you want to receive alerts.



2. Add a **Webhook** and click the [Configure] button.



3. Enter a webhook name and click the [Create] button.



Incoming Webhook

[Send feedback](#)

The Incoming Webhook connector enables external services to notify you about activities that you want to track. To use this connector, you'll need to create certain settings on the other service, which needs to support a webhook that's compatible with the [Office 365 connector format](#).

Fields marked with * are mandatory

To set up an Incoming Webhook, provide a name and select Create. *

Customize the image to associate with the data from this Incoming Webhook.

Upload Image



Default Image

Create

Cancel

4. Copy the generated **Webhook URL**.

Copy the URL below to save it to the clipboard, then select Save. You'll need this URL when you go to the service that you want to send data to your group.

<https://whatap.webhook.office.com/webhook>



Url is up-to-date.

Done

Remove

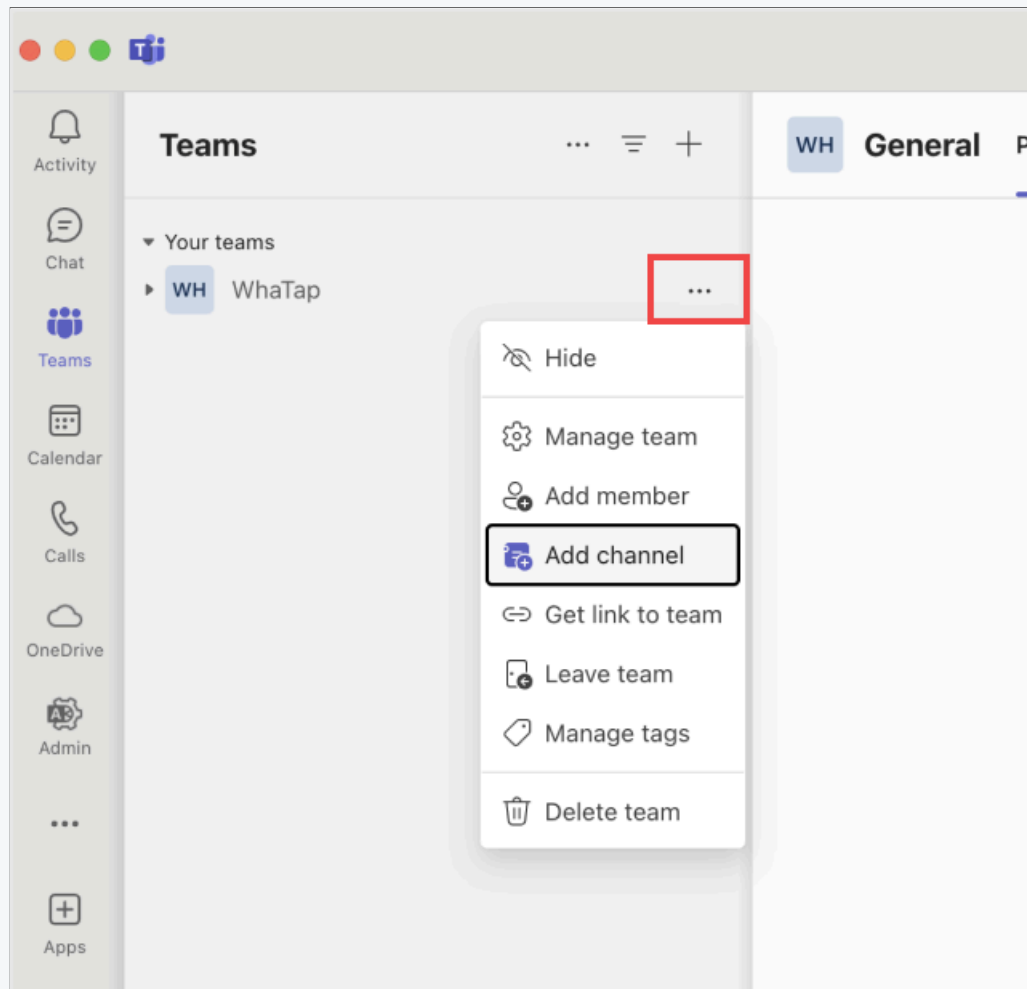
5. Return to the **Add a third-party plug-in** window in the WhaTap Monitoring service, and enter values for **Channel Name** and **Webhook URL** at the bottom of the **Teams** tab.
6. Click the [**Registration**] button.

Teams Workflows



- ⓘ To use workflows, you need an account that can access **Microsoft Teams** and a **Business plan subscription**.

1. In the **Teams** menu, click **More actions (...)** > **Add channel**.

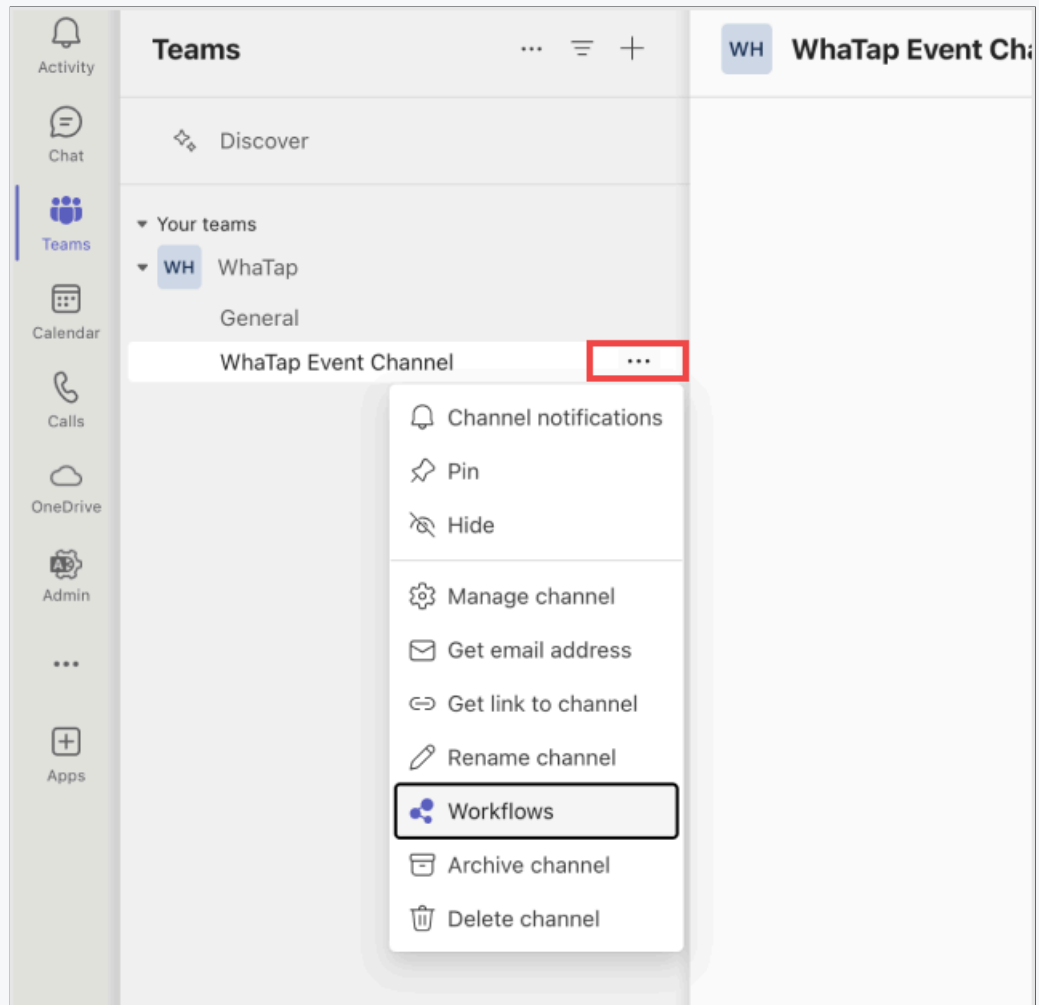


2. In the **Create a channel** window, enter the **Channel name** and **Description**. For **Channel type**, select **Standard**, then click the [Create] button.

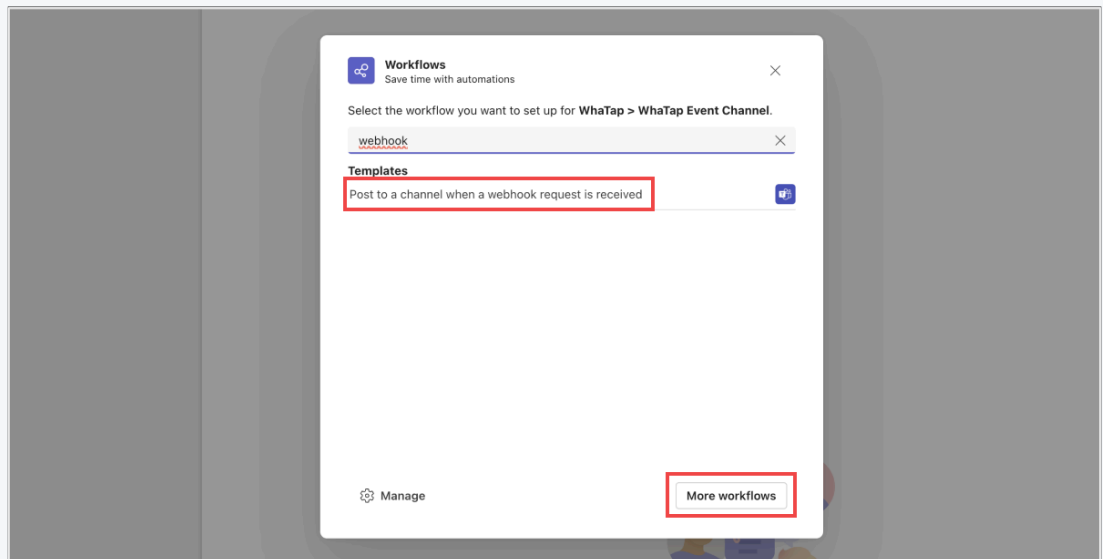


⚠ If you select **Shared** as the channel type, workflows cannot be used. If you select **Private**, workflows can be added but notifications cannot be received.

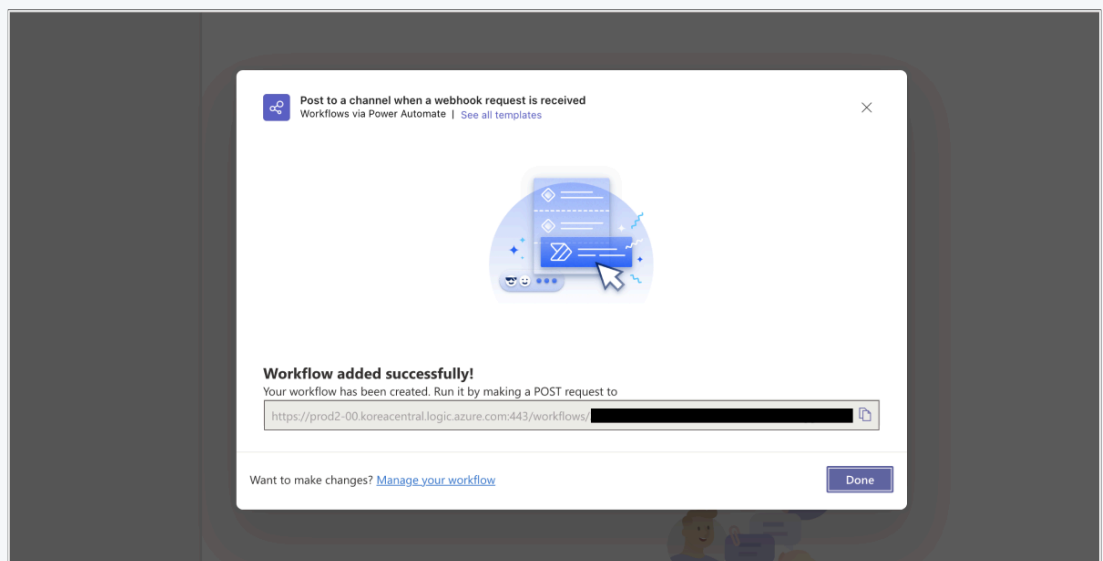
3. Click **More actions (...)** of the created channel, then select **Workflows**.



4. In the **Workflows** dialog, select **Post to a channel when a webhook request is received** from the workflow list, then click the [Add workflow] button.



5. Check the **Name** and **Connection** status, then click the [Next] button.
6. Review the **Details**, then click the [Add workflow] button.
7. The workflow has been added. Copy the generated URL.



8. Return to the **Add a third-party plug-in** window in the WhaTap Monitoring service, and enter values for **Channel Name** and **Webhook URL** at the bottom of the **Teams Workflows** tab.



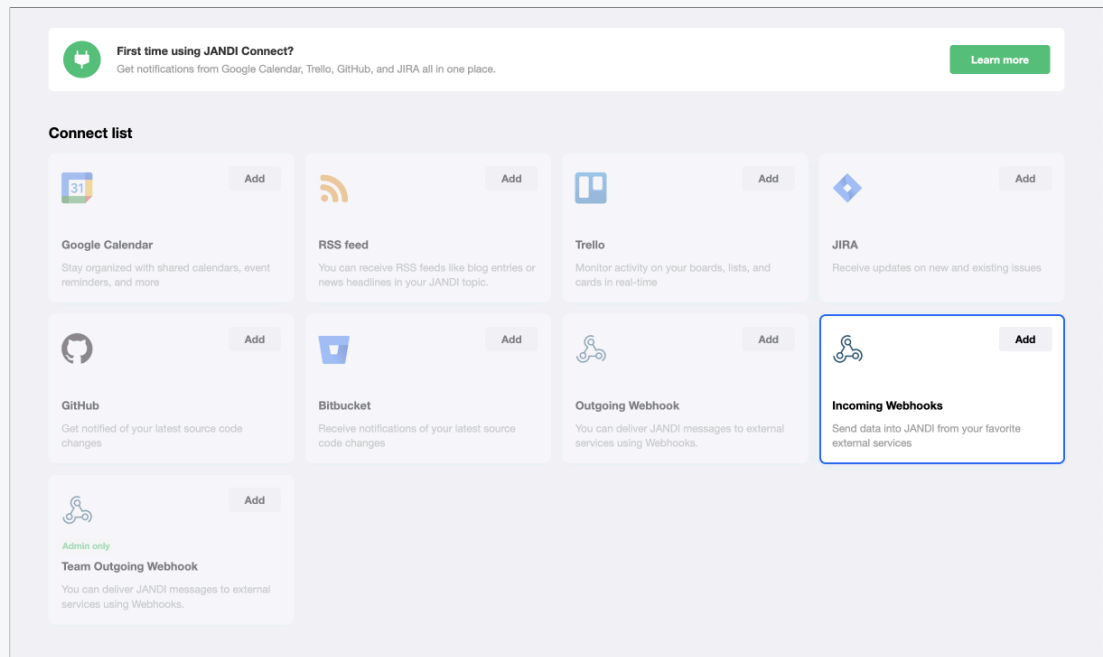
9. Click the [**Registration**] button.



Jandi



1. Go to **Jandi Connect settings** in the topic or chat where you want to receive notifications.
2. In the **Connect list**, find **Webhook Receiver (Incoming Webhook)** and click the [**Connect**] button.



3. Click the [**Add Webhook Receiver**] button.
4. Copy the Webhook URL from the **Register Webhook URL** section.



Connect settings

Profile settings

Change the name or profile image that appears for messages from this integration

 Incoming Webhooks

Topic / JANDI selection

Please select a topic or DM to receive integration messages. You change it after saving it.

JANDI

Webhook URL Registration

Webhook URL

Copy the generated Webhook URL and register with the service.

 <https://wh.jandi.com/connect-api/webhook/31257583/d3...>

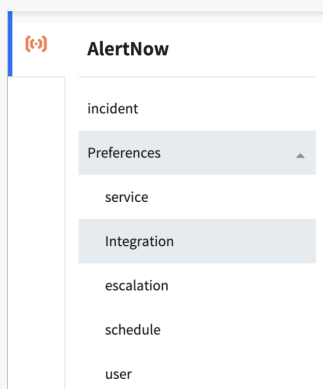
Copy

- Return to the **Add a third-party plug-in** window in the WhaTap Monitoring service, and enter values for **Channel Name** and **Webhook URL** at the bottom of the **Jandi** tab.
- Click the [**Registration**] button.

AlertNow



- Access the **AlertNow** service, then go to **Settings > Integration**.



- On the **Integration** screen, click the [Create Integration] button.
- From the list of integration types, select **WhaTap**.
- On the **Create Integration** screen, configure the **Name** and **Naming Rules**.

Integration

Entire

Integration name *

Enter integration name

Integration type *

WhaTap

Set naming convention *

Define and manage incident naming rules.

naming convention

[[level]][title] {projectName} {oname} {oid}

Preview rule settings

Incident names are limited to 3500 bytes in length.

[Warning]CPU Used > 10 % OTE-SERVER ote-front-330494549

sample data

```
{
  "metricName": "cpu",
  "pcode": 188,
  "level": "Warning",
  "metricValue": "26.888296",
  "oid": "-330494549",
  "title": "CPU Used > 10 %",
  "message": "MEMORY is too high 98%",
  "uid": "4dfe0b7686-c4335f0ef4c1cfa45754",
  "metricThreshold": "18.0",
  "oname": "ote-front",
  "time": 1592887274971,
  "projectName": "OTE-SERVER",
  "status": "on"
}
```

56/1600 byte

5. Click the [Confirm] button to create the integration.
6. Check the list of created integrations and select the newly created integration.

Integration

Create integration

Enter search term

Last update: 2024-02-21 11:31:17

Integration name	Integration type	Integration key	service name
whatap-test	WhaTap		whatap-test

7. On the details screen, click the copy icon on the right side of the URL to copy it.

Integration

whatap-test

Basic Information

Integration type

WhaTap

Integration key

fda527a5140

URL

https://alertnowitgr.opsnow.com/integration/whatap/v1/

Copy to clipboard

constructor

Lisa

8. Return to the **Add a third-party plug-in** window in the WhaTap Monitoring service, and enter values for **Channel Name** and **Webhook URL** at the bottom of the **AlertNow** tab.
9. Click the [**Registration**] button.

Webhook



1. Register the Webhook that will receive notifications. The alert `title` and `text` are sent to the registered URL via the **POST** method.

```
{
  "title": "Alert Title",
  "text": "Sample warning message"
}
```

2. Enter values for **Webhook Name** and **Webhook URL**.
3. Click the [**Registration**] button.

Webhook JSON



1. Register the Webhook that will receive notifications. Alert data is sent to the registered URL in **JSON format** via the **POST** method. For substitution variables that can be included in the JSON payload, see **Available Variables**.
 - `${something}` represents a substitution value provided by WhaTap. Refer to **Available Variables** for the full list and descriptions.
 - The event status (`status`) is categorized as **event triggered** (`on`) or **event recovered** (`off`).
 - The `level` is categorized as `None` , `Info` , `Warning` , or `Critical` .

```
{
  "pcode": "${pcode}",
  "projectName": "${projectName}",
  "time": "${time}",
  "oid": "${oid}",
  "oname": "${oname}",
  "title": "${title}",
  "message": "${message}",
  "level": "${level}",
  "status": "${status}",
}
```



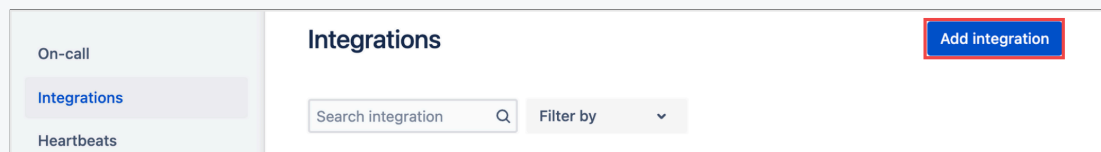
```
"metricName": "${metricName}",
"metricValue": "${metricValue}",
"metricThreshold": "${metricThreshold}",
"uuid": "${uuid}",
"okind": "${okind}",
"onode": "${onode}"
}
```

2. Enter values for the **Webhook Name** and **Webhook URL** fields.
3. To add a header value, click + **Add** in **Add user header value**, then enter the key and value.
4. Click the [**Registration**] button.

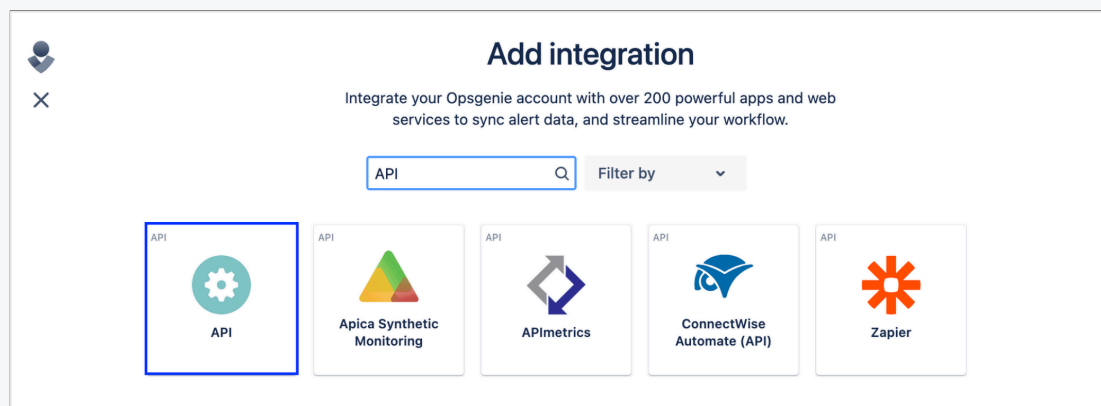
Opsgenie



1. In the **Teams** menu, select the team that will receive notifications.
2. Go to the **Integration** menu and click the [Add Integration] button.



3. In the integration list, search for and select **API**.





4. Set the API name, assign a team, configure the required permissions, and then click the [Save Integration] button.

5. Return to the **Add a third-party plug-in** window in the WhaTap monitoring service, and enter values for **Name** and **API Key** at the bottom of the **Opsgenie** tab.
6. Click the [**Registration**] button.

PagerDuty



1. Sign up for a [PagerDuty](#) account and log in.
2. In PagerDuty, go to **Services > Service Directory**, then click the [+ New Service] button.

PagerDuty

3. Enter the service information (**Name**) and click the [Next] button.

PagerDuty

4. Configure the **Escalation Policy**, then click the [Next] button.



PagerDuty

5. Configure **Alert Grouping** and **Transient Alerts**, then click the [Next] button.

PagerDuty

6. In **Integrations**, select **Event API V2**, then click the [Create Service] button.

PagerDuty

7. On the created service page, copy the **Integration Name** and **Integration Key** values.

PagerDuty

8. Return to the **Add a third-party plug-in** screen in the WhaTap monitoring service and enter the **Integration Name** and **Integration Key** values.
9. Click the [Register] button.

ⓘ If you do not receive messages or the plugin is not registered, check whether the **Integration Name** or **Integration Key** values are correct.

LINE



1. Install the LINE app.
2. Scan the QR code below to add the official **WhaTapLabs** channel as a friend.

Add LINE 3rd-party plugin

3. Use the following commands to link your project with LINE and configure notifications.

Commands

```
/help # Show available commands
/list # View the list of linked projects
/license [ACCESS_KEY] # Add a new project linkage
/remove [PROJECT_CODE] # Remove a linked project
/language [ko|ja|en] # Set notification language (Korean/Japanese/English)
```



- You can find the project access key under **Management > Project Management**.
- Using the `/language` command in LINE applies **only to the current LINE chat room**. It does not change the notification language for other 3rd-party plugins or projects.

Examples

```
/license XXXXXXXXXX # Link a project
/language ko # Set language to Korean
/list # Check linked projects
```



- **Project access key:** Available under **Management > Project Management** in the WhaTap project.
- **Language settings:** The `/language` command applies only within the LINE chat room and does not affect other notification channels.

ilert



1. In the ilert console, click [+ Create alert source] at the top right of the **Alert sources** page.
2. In the **Integration type** step, enter `WhaTap` in the **Filter integrations** search field at the bottom to search.
3. From the search results, select the **WhaTap** tile and click the [Next] button.
4. Enter the alert source name and assign a team, then click the [Next] button.
 - You can create a new escalation policy or select an existing one.
5. Select the alert grouping method and click the [Continue setup] button.
 - The initially selected **Do not group alerts** option can be changed later.
6. On the next screen, you can configure additional settings such as **alert templates and priorities**. For now, click the [Finish setup] button to complete the setup.
7. When the setup is complete, an **API key** or **Webhook URL** will be generated on the completion screen.



8. Copy the generated **Webhook URL** from the **Webhook JSON** tab and paste it into the **Webhook URL** input field below.
9. Click the [Register] button.

Preventing Alert Storms

If a large number of alerts occur within a short period, alert notifications are temporarily paused for a specified duration. For example, if 20 events occur within 5 minutes, alert notifications will be suspended for the next 5 minutes. Once the configured **Pause Duration** has elapsed, the alert-storm prevention feature is automatically released.

1. Go to **Alert > Notifications > the Avoids a large number of alerts** section.
2. Click the toggle button to **Enable** or **Disable** the feature.
 -  **Enabled:** Temporarily pause alerts when an alert storm is detected
 -  **Disabled:** Resume alert notifications
3. Configure the **Detection Time**, **Detection Count**, and **Pause Duration**.
 - If the number of events exceeds the **Detection Count** within the **Detection Time**, alert notifications are paused for the configured **Pause Duration**.



When alerts are blocked due to an alert storm, a notification banner is displayed. To immediately release the alert-storm block, click the **Stop Alert Storm Prevention** button in the banner.

Event Notification Format

Common Alert Template

The common template can be applied in most cases. It allows you to receive alerts in a consistent format across various environments.

- Product Type: Application, Database, Kubernetes
- Event Type: Application Alerts, Database Alerts, Metrics Alerts
- Event Channel: SMS, Mobile, 3rd-party plugins, Plugins

Event Title

Event title format

```
[Level][Platform][ProjectName][ApplicationName][EventTitle]
```

Event title example

```
[Info][JAVA][Application Project][TC-0-1-8081][CRITICAL_HIGH_MEMORY]
```

❗ If ApplicationName is not set, it is omitted from the event title.

- Platform is displayed as one of the following.
 - JAVA
 - NODEJS
 - PYTHON
 - PHP
 - DOTNET
 - GO
 - POSTGRESQL



- ORACLE
- MYSQL
- MSSQL
- BSM_JAVA
- CLOUDWATCH
- TIBERO
- KUBERNETES
- KUBE_NS
- URLCHECK
- URLCHECK_ADMIN
- CUBRID
- ALTIBASE
- CLUSTER
- REDIS
- MONGODB
- VR
- RUM

Event Message

This section describes the information that can be included in the event message. If `optional` is set to `false`, the item is always included in the message. If `optional` is set to `true`, the item is displayed only when the data is available.

Event message example

```
Project Name : Application Project
Project Code : 3
Agent Name : TC-0-1-8081
Message : RECOVERED: Memory is too high. less than 10%
```

Event Time : 2022-04-12 18:53:24 +0900
 Event OFF Time : 2022-04-12 18:53:24 +0900
 Alert Type : APPLICATION_MEMORY
 Metric Name : memory
 Metric Value : 20
 Metric Threshold : 10
 Stateful : true

Table | Event Message Components

En	Ko	Supported Alert Types	Description
Project Name	Project name	All	-
Project Code	Project code	All	-
Agent Name	Agent name	All (optional)	oname
Message	Event message	All	-
Alert Type	Alert type	All	See the AlertType table below
Event Time	Event occurrence time	All	In 2022-04-13 10:40:49 +0900, +0900 indicates the GMT offset
Event Off Time	Event recovery time	All (optional)	In 2022-04-13 10:40:49 +0900, +0900 indicates the GMT offset
Metric Name	Metric name	All (optional)	Name of the metric used to evaluate the event condition
Metric Value	Metric value	All (optional)	Included when the metric value exceeds the threshold
Metric Threshold	Metric threshold	All	Threshold value used to determine the event

En	Ko	Supported Alert Types	Description
		(optional)	condition
Stateful	Recovered-event notification	All (optional)	<code>true</code> if recovered-event notification is enabled; otherwise <code>false</code>
Event Rule	Event trigger condition	Metrics alerts	-
Target Filter	Event target filter	Metrics alerts	Evaluates event conditions only for metrics collected from specific targets
Repeat Count	Event repeat count	Metrics alerts	The event is triggered when the condition is met the specified number of times within the repeat duration
Repeat Duration	Event repeat duration	Metrics alerts	Time window used to evaluate the repeat count
Receiver	Receiver	Metrics alerts	-
Query	MXQL query	Composite metrics alerts	-
Rule	Event trigger condition	Composite metrics alerts	-
Query Period	Query period	Composite metrics alerts	-
Query Interval	Query interval	Composite	-

En	Ko	Supported Alert Types	Description
		metrics alerts	
Silent Time	Silent time	Composite metrics alerts	-
Query	URL	Exception alerts	URL of the request that caused the exception
TXID	Transaction ID	Exception alerts	-
Class	Error class name	Exception alerts	-
Log Message	Log message	Server – file log alerts	-
Log File	Log file path	Server – file log alerts	-
IP	IP address	All server alerts	-
CPU	CPU usage	All server alerts	Snapshot at the time the event occurred
CPU_load1	CPU load (1 min)	All server alerts	Snapshot at the time the event occurred
CPU_loadPerCore	CPU load per core	All server	Snapshot at the time the event occurred

En	Ko	Supported Alert Types	Description
		alerts	
Memory	Memory usage	All server alerts	Snapshot at the time the event occurred
Swap	Swap usage	All server alerts	Snapshot at the time the event occurred
Disk Name Used Percent Free Size IO Percent	Disk performance	All server alerts	Snapshot at the time the event occurred
Name Bps Pps	Network traffic performance	All server alerts	Snapshot at the time the event occurred
Message Time Name	Acknowledgement information	All server alerts	-

ⓘ This section displays as much information as possible that can be provided for the event.

- **AlertType** is displayed as one of the following values.

AlertType	Description
APPLICATION_CPU	Application CPU alert
APPLICATION_MEMORY	Application memory alert
APPLICATION_DISK	Application disk alert
APPLICATION_ACTIVE_TRANSACTION	Application active transaction alert
APPLICATION_ERROR_TRANSACTION	Application error transaction alert



AlertType	Description
APPLICATION_SLOW_TRANSACTION	Application slow transaction (response time) alert
METRICS	Metrics alert
COMPOSITE_METRICS	Composite metrics alert
ANOMALY	Anomaly detection alert
LOG_REALTIME	Real-time log alert
COMPOSITE_LOG	Composite log alert
SERVER_REBOOT	Server reboot alert
SERVER_NO_DATA	Server no-data alert
SERVER_PORT	Server port alert
SERVER_NETWORK_IOPS	Server network IOPS alert
SERVER_NETWORK_BPS	Server network BPS alert
SERVER_DISK_IO	Server disk I/O alert
SERVER_DISK_QUOTA	Server disk usage alert
SERVER_DISK_INODE	Server inode alert
SERVER_CPU	Server CPU alert
SERVER_MEMORY	Server memory alert
SERVER_CPU_STEAL	Server CPU steal alert



AlertType	Description
SERVER_MEMORY_SWAP	Server swap memory alert
SERVER_LOG_FILE	Server log file alert
SERVER_WINDOW_EVENT	Server Windows event alert
SERVER_OFF	Server alert OFF notification
SERVER_ACKNOWLEDGE	Server acknowledge notification
SERVER_PROCESS_COUNT	Server process count alert
SERVER_PROCESS_CPU	Server process CPU alert
SERVER_PROCESS_MEMORY	Server process memory alert
SERVER_PROCESS_OFF	Server process alert OFF notification
AGENT_ACTIVE	Agent activated alert
AGENT_INACTIVE	Agent deactivated alert
AGENT_REACTIVATED	Agent reactivated alert
URL	URL alert
TOO_MANY_EVENT	Too many events alert
CLOUD_WATCH	CloudWatch alert
EXCEPTION	Exception alert

Event History And Monitoring

Home > Select Project >  **Alert** > **Event History**

Event History allows you to view events that have occurred in the project and analyze their detailed information. It supports Elasticsearch DSL queries, enabling you to find events that match specific conditions quickly and accurately.

Viewing Event History

Click the **event title** in the search results to move to a screen where you can analyze detailed data for the time period when the event occurred. This allows you to comprehensively understand the situation before and after the event.

1. Go to **Alert > Event History**.
2. In the **Event History** screen, use **Time Selection** to set the period for viewing event records.
3. Enter a query in the filter input field and click the [Magnifying Glass] button.
 - If no query is entered, all events are displayed.

Column Settings

You can choose which columns to display or hide.

1. In the **Event History** screen, click the [ Column Settings] button at the top left.
2. In the **Column Settings** window, select the columns you want to show or hide.
 - You can change the column order in **Displayed Items**.
 - You can search for specific columns using the **Column Name Search** field.

Column Item	Description
Event Name	The title of the event

Column Item	Description
Message	The event message or snapshot information
Event Status	The current status of the event
Agent Name	The name (Oname) of the agent where the event occurred - Displayed as blank if the event is not associated with a specific agent
Agent Group	The agent type (OkindName) where the event occurred - Displayed as blank if the event is not associated with a specific agent
Agent Node	The server (OnodeName) of the agent where the event occurred - Displayed as blank if the event is not associated with a specific agent
Event Occurred Time	The time when the event occurred
Event Resolved Time	The time when the event was resolved - Displayed as - for events without a resolved state

- After completing the settings, click the [Confirm] button to apply the column configuration.

↓ CSV Download

You can download the query results as a CSV file.

- Go to **Alert > Event History** and click the [CSV] button.
- The list of events that match the current filter conditions is saved as a CSV file.

View Only Events in Progress

You can view only events that are currently in progress.

- Go to **Alert > Event History** and click the [View Only Events in Progress] button.
- The following condition is automatically added to the filter query and applied to the search.

Stateful: **true** and Status : **"ON"**

Event Search

- **Precise Search:** Specify exact conditions to retrieve only the events you need
- **Composite Conditions:** Search across multiple fields at once to handle complex conditions in a single query
- **Flexible Patterns:** Supports various search methods such as wildcards and partial matches
- **High Performance:** Fast searches powered by indexed data

Searchable Fields

Field names and values are not case sensitive.

- **Field Name Tag:** Event types that support the field
- **Field Type:** The data type of the field
 - : Number
 - : String
 - : Boolean
 - : Date

Event Information Fields

Field Name	Type	Description	Example Value
Title	String	Event title	"Database Connection Error"
OffTitle	String	Event recovery title	"RECOVERED: Database Connection Error"
Message	String	Event message	"Connection timeout occurred"
OffMessage	String	Event recovery message	"RECOVERED: Connection timeout occurred"

Field Name	Type	Description	Example Value
Level	String	Current event level	Critical, Warning, Info
OriginLevel	String	Original event level	Critical, Warning, Info
Status	String	Event status	ON, OFF, CANCEL, ACKNOWLEDGE, MAINTENANCE, DISABLED
ActCount	Number	Number of occurrences	2
MetricName	String	Metric name	"memory"
MetricValue	String	Metric value	"85.5"
OffValue	String	Recovery value	"72.8"
MetricThreshold	String	Threshold value	"80"
alertType	String	Event type	"BASIC", "METRICS", "TRANSACTION", etc.
alertId	String	Unique identifier of the event rule	"zf3uojer0fv4v7"

Type-specific Supported Fields

ⓘ These fields are supported only for specific event types. If the event type does not match, the value may be empty.

Field Name	Type	Event Type	Description	Example Value
eventRule	String	Basic, Metrics	Event trigger rule	"memory ≥ 80"
field	String	Real-	Log search	"content"

Field Name	Type	Event Type	Description	Example Value
		time Log	key	
keyword	String	Real-time Log	Log search value	"Error"
logCategory	String	Real-time Log	Log category	"AppLog"
logContent	String	Real-time Log	Log content	"00:00000:00009:2025/04/06 23:03:52.55 server Error: 1601, Severity: 17, State: 3\n00:00000:00009:2025/04/06 23:03:52.55 server There are not enough 'user connections' available to start a new process."

Target Fields

Field Name	Type	Description	Example Value
Oid	Number	Agent unique identifier	-98765432
Oname	String	Agent name	"web-server-01"
Okind	Number	Agent type unique identifier	867318026
OkindName	String	Agent type name	"web-server"
Onode	Number	Agent node unique identifier	334634079
OnodeName	String	Agent node name	"production-node-1"

Unique Event Fields

Field Name	Type	Description	Example Value
Id	Number	Unique identifier of the event	5768121
UUID	String	Unique event identifier	"550e8400-e29b-41d4-a716"

State / Flag Fields

Field Name	Type	Description	Example Value
Stateful	Boolean	Whether the event is state based	true, false
Disabled	Boolean	Whether the event is disabled	true, false
Escalation	Boolean	Whether escalation is applied	true, false
SystemEvent	Boolean	Whether it is a system event	true, false

Query Syntax by Search Type

ⓘ For the basic search syntax, refer to the [WhaTap log search query syntax](#) documentation.

1. Keyword Search

Events that contain the string "Database Connection"

```
title: "Database Connection"
```

2. Multiple Value Search

Retrieves events that include any one of the specified values.

```
title: Database Connection
```

Events whose current event level is Info or Warning

```
level: info warning
```

3. Pattern Search

You can search using patterns with wildcards.

Find events that occurred on specific agents using a name pattern

```
oname: web-*-prod
```

タイトルが Connection で終わるイベントを検索

```
title: *Connection
```

4. Complex Condition Search

You can combine multiple conditions to perform precise searches.

Events with a Critical level and a title containing Database

```
level: critical and title: Database
```

Warning or Critical events from a specific agent

```
oname: web-server-01 and level: Warning Critical
```

5. OR Condition Search

Retrieves events that satisfy **at least one** of the specified conditions.

Events where the title or message contains a specific keyword

```
title: Connection or message: Connection
```

6. Exclusion Conditions

You can exclude specific conditions from the search.

All events except those with an Info level

```
not level: info
```

Real-time Notifications

The **Alert status** feature displays pop-up notifications when events configured in **Event Configuration** occur. You can receive alerts immediately when an event is triggered, allowing you to quickly recognize issues and respond. You can also review notifications that have already occurred or were missed, helping you understand and resolve situations where real-time response was difficult.

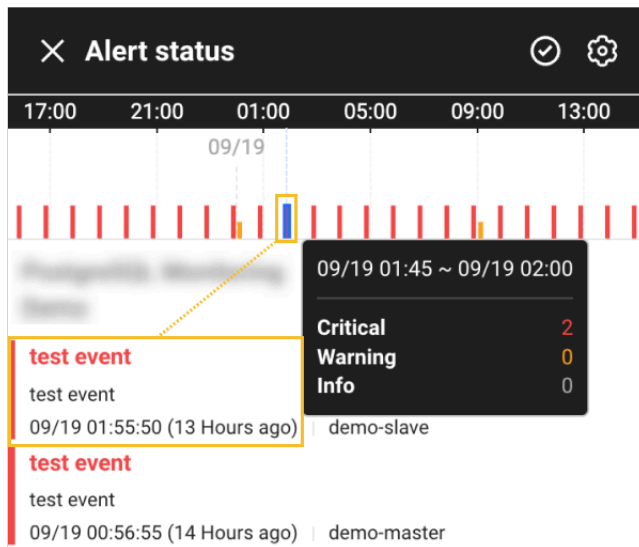
Viewing Real-time Notifications

Real-time notifications appear as pop-ups in the upper-right corner of the screen. You can check the time, title, and message of each notification.

- To close an individual notification, click the  button in the upper-right corner of the message.
- To close all pop-up notifications displayed on the screen, click **Close All Notifications**.

Viewing Notification History

1. Click the  icon at the top of the screen after selecting a project.
2. The **Alert status** window appears.
 - You can view up to 100 notifications from the past 24 hours for the current project.
 - Selecting an individual event item navigates you to the related menu.
 - In the time-based chart within the **Alert status** window, selecting a specific time range takes you to the corresponding event items.



- To view the full notification history, click **View All Notification History**. This navigates to **Alert > Event History**.

ⓘ If the **Alert status** list is empty, the **View All Notification History** button is displayed. Disable the **Receive notifications without reception tags** option.

Resolving Events in Bulk

You can resolve all ongoing events at once from the **Alert status** list. The bulk resolution process may take approximately 30 seconds to 1 minute to complete.

- When using the **Add Acknowledge** feature, a large number of recovery (resolved) notifications may be generated for currently ongoing events.
- Even after using the **Add Acknowledge** feature, events may occur again if the event rules remain enabled and the data still exceeds the threshold.
- Recovery notifications can be disabled by editing the event in **Alert > Event Configuration**. Disable **Send additional notification when the event is resolved** or **Recovered notification**.

How to use:

1. Click the  icon at the top of the screen after selecting a project.
2. When the **Real-time Notifications** window appears, click the  icon in the upper-right corner.
3. When the message `Resolve all ongoing events in the real-time notification list.` appears, click the **Resolve** button.

Configuring Real-time Notifications

1. Click the  icon at the top of the screen after selecting a project.
2. When the **Alert status** window appears, click the  icon in the upper-right corner.
3. Configure each option in the real-time notification settings window.
 - **Popup notifications:** Displays notifications as pop-ups even when the **Alert status** window is closed.
 - **Show resolved events:** Allows resolved events to be displayed in the **Alert status** list.
 - **Preview notification sound:** Lets you preview browser notification sounds. Click the  button next to **Critical** or **Warning**. If you cannot hear the sound, check your browser settings.

System Events

WhaTap Monitoring provides common system events that are automatically detected and generated across the platform. This document explains the types of events generated by the system, their trigger conditions, and recommended response actions.

EVENT_BLOCKED_BY_SYSTEM

If an excessive number of events occurs within a short period of time in a project, the WhaTap system detects this situation and blocks further events. When events are blocked, the system delivers the following message to the user. If you encounter this event, review and adjust your event configuration settings.

 **Critical**



Event Message

Excessive events detected, event blocked for stability. name: server agent

Project No	8
Project Name	new server
Target	server agent
Event Title	EVENT_BLOCKED_BY_SYSTEM
Event Time	(GMT+0900) 2024-11-18 17:58:58

Log In to WhaTap

Events are blocked as a result of excessive events in the server agent of new server project. If no events occur in server agent for a period of time, it is automatically unblocked.

Blocking Criteria

Events are blocked based on the following criteria:

- 1. Agent-level blocking**

If **10 events** occur within **1 minute** from a single agent, all subsequent events from that agent are blocked.

- 2. Project-wide blocking triggered by multiple agents**

If **3 or more agents** are blocked within **1 minute** according to condition 1, events from the entire project are blocked.

3. Project-level blocking

If **100 events** occur within **1 minute** in a single project, all events from that project are blocked.

How to Release the Block

When events are blocked by the system, no events must occur from the affected agent or project for **1 minute**.

- Disable all configured events from **Alert > Event Configuration**. **Review your event settings and adjust thresholds to prevent excessive event generation.**
- Before configuring events, use the **Simulation** feature to estimate how many events may occur.

Laboratory

This menu provides new or experimental features to users. Through  **Laboratory** or **Sitemap** in the side menu, you can access it. The provided features may differ depending on the product.

 The functionality of the **Laboratory** menu is currently in Beta version and may cause unexpected errors. Be careful when using the **Laboratory** menu. It is not recommended to use the menu in handling important data or in the operating environment. If you have any feedback or issues, feel free to contact the support team at support@whatap.io.

- **MXQL Data**

MXQL is a query language to flexibly query WhaTap's performance data (metrics). It is used to comprehensively search and use the metrics collected from multiple agents in a project. For more information about **MXQL**, see [the following](#).

 In the side menu, if the  **Laboratory** menu does not appear, you can access it through **Sitemap**.
Under the side menu, select . If the **Sitemap** window appears, select a desired menu in the **Laboratory** section on the lower right of the window.

OpenMetrics Explorer

OpenMetrics Explorer is a feature that allows you to directly explore custom metrics based on Prometheus using PromQL, visualize them in various formats, and check metric states or gain insights.

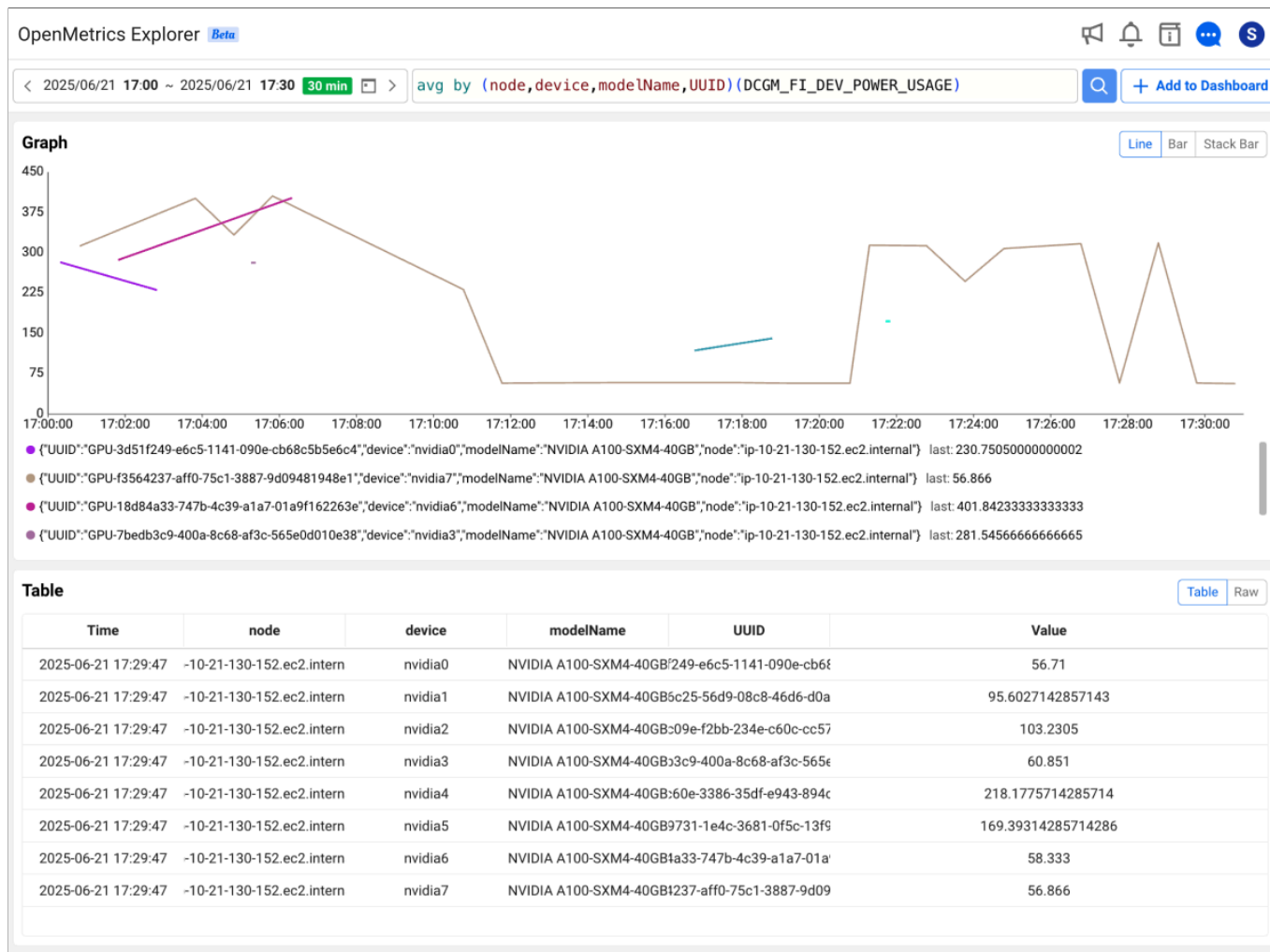
With this feature, you can freely query the metrics you need, extract meaningful data, or connect them to dashboards for continuous monitoring.

ⓘ To use OpenMetrics Explorer, you must install the Open Agent.

- See [Install WhaTap Operator](#).

Exploring with PromQL

In **OpenMetrics Explorer**, you can run PromQL queries and view the results with different visualization options.



Graph

- **Line:** Default time-series line chart
- **Bar:** Visualizes values as a bar chart
- **StackBar:** Stacked bar chart that shows accumulated values

Table / Raw

- **Table:** Displays time-series values in chronological order as a table
- **Raw:** View the Prometheus API response directly in JSON format

PromQL Syntax Support and Autocomplete

When you enter metrics such as `node_cpu_seconds_total` or `container_memory_usage_bytes`, the autocomplete feature suggests available metrics and operators.

It also supports label filtering in the form `{pod="example"}`.

Adding to Dashboard

You can save a queried PromQL as a dashboard widget and continuously monitor the desired metrics.

How to Add

1. In the **OpenMetrics Explorer** screen, click the **+ Add to Dashboard** button in the upper right corner.
2. In the **Add to Dashboard** window, select an existing dashboard or create a new one.
3. Click **Apply** to add the widget to the chosen dashboard.
 - You can enter a widget name and description in the added dashboard.
 - Added widgets can be freely repositioned in the Flexboard grid layout and edited with PromQL.