

SingleStore Monitoring

release date. 2026. 09. 11.

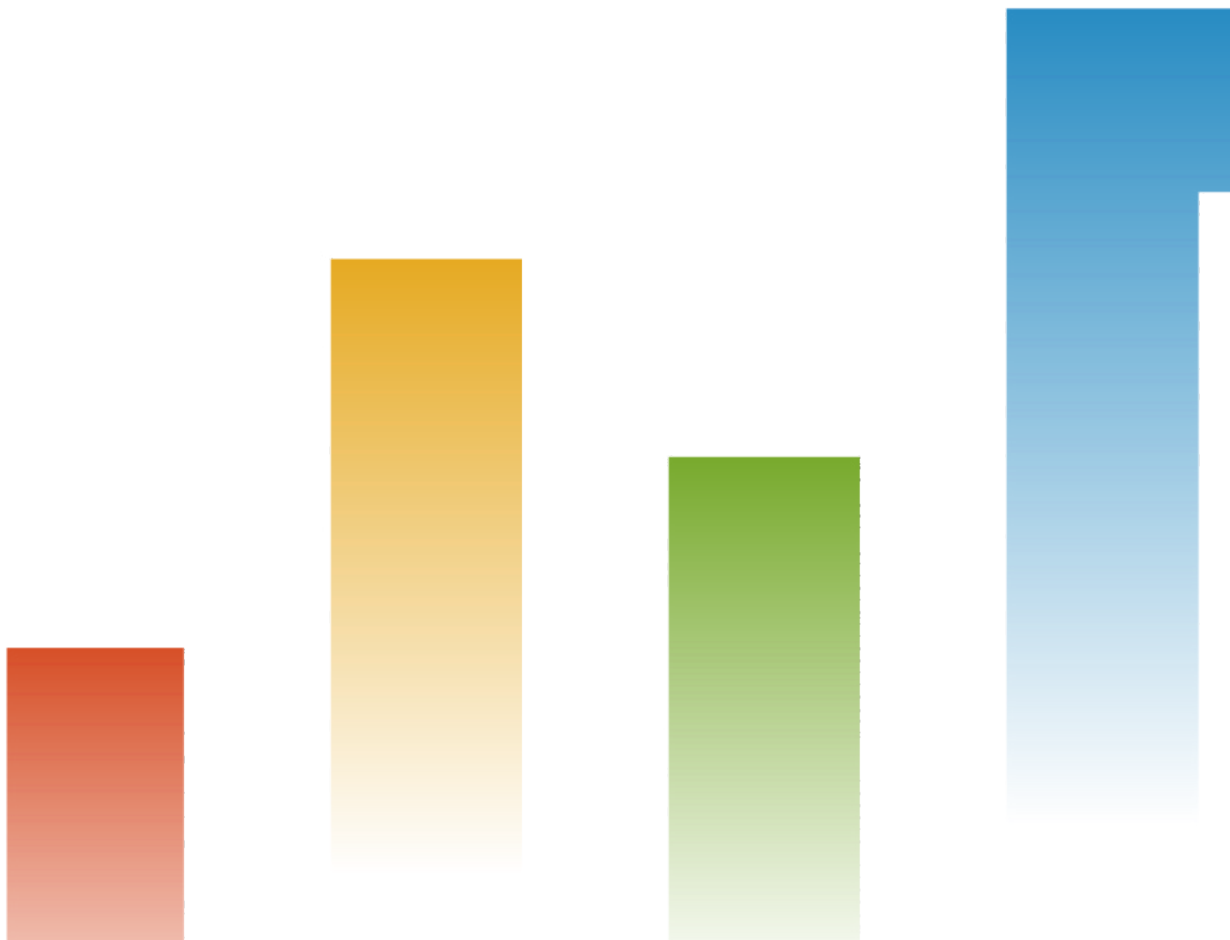


Table Of Contents

• SingleStore Monitoring.....	4
◦ Getting Started.....	6
◦ Installation	
■ Manual Installation	8
◦ Configuration	
■ DBX Agent Setting.....	11
◦ Dashboard	12
■ Instance List.....	13
■ Instance Monitoring	16
■ Multi-Instance Monitoring	20
■ Storage Engine	21
■ Flex Board	25
■ Using the Flex Board	28
■ Managing Widgets	38
◦ Analysis	43
■ Trend Comparison.....	44
■ Lock Tree	48
■ Session History	51
■ Partition	54
■ Pipeline.....	58
■ Database Parameter	62
■ Metrics Chart	65
■ Metrics Trend Analysis.....	87
◦ Stat/Report	90

■ Top SQL.....	91
■ Database Size.....	95
■ Report.....	96
◦ Log.....	99
■ Live Tail.....	101
■ Log Explorer.....	114
■ Log Trend	121
■ Log setting	128
◦ OpenMetrics.....	160
■ Template List.....	161
■ Explorer	164
■ Agent Installation.....	167
◦ Alert.....	169
■ Event Configuration.....	0
■ Metrics Event.....	176
■ Composite Metric Event.....	198
■ Anomaly Detection Event	205
■ Real-time logs	209
■ Composite log.....	222
■ Event Notification Settings.....	236
■ Notification format.....	258
■ Event history	266
■ Event pause.....	274
◦ Laboratory	275
■ MXQL Data Lookup	276
■ Alert messages	277

SingleStore Monitoring

SingleStore is a distributed SQL database that stores data across multiple nodes. As the number of nodes grows, it becomes harder to tell at a glance which node is under load or whether data is skewed to one side. WhaTap database monitoring gathers the overall cluster state, per-node metrics, and SQL performance into one view. It helps DBAs and data platform engineers who operate SingleStore quickly locate load points and data skew.

WhaTap works by having the **DBX agent** connect to the SingleStore cluster and collect metrics. When you install the agent on only one aggregator node, it automatically detects leaf nodes through `MV_NODES` and collects the entire cluster, so you do not need to install the agent on every node. For details on how to get started, see the [Getting Started](#) document.

SingleStore cluster architecture

A SingleStore cluster is made up of nodes with different roles. Node roles appear throughout the screens, including the `ROLE` column in the instance list, so it helps to understand them first.

ROLE	Name	Description
MA	Master Aggregator	The primary aggregator responsible for managing cluster metadata and routing queries
CA	Child Aggregator	A secondary aggregator that helps distribute query processing
Leaf	Leaf	A leaf node that stores actual data and performs computation

In simple terms, the aggregators (MA, CA) are the front desk that receives requests and distributes them, while the leaf nodes are closer to the workers that hold the data and do the work.

Monitoring screen layout

SingleStore monitoring provides screens focused on the items most often checked in a distributed environment.

Screen	Description
Instance Monitoring	Check per-node CPU, memory, disk, and network metrics and active sessions in real time
Multi-Instance Monitoring	Gather metrics from multiple nodes into one dashboard for comparison
Storage Engine	Check Rowstore and Columnstore memory and disk usage and data skew
Partition	Check whether table partitions are evenly distributed across nodes by their deviation
Pipeline	Check the throughput, latency, and errors of data ingestion pipelines
Database Size	Check capacity trends by database
Top SQL	Analyze high-load SQL with metrics and trend charts
Session History	Look up past active sessions in chronological order
Lock Tree	Check lock waits and deadlocks in a tree view

Supported environments

Based on the official installation guide, the following environments are supported.

- SingleStore 9.0 or later
- DBX agent installed on an aggregator node (leaf nodes are auto-detected through `MV_NODES`)
- Monitoring account privileges `grant select, process, cluster on *.*;`

Getting Started With SingleStore Monitoring

This document guides the entire flow for those setting up SingleStore monitoring for the first time. Once you create a monitoring account on the cluster and connect the DBX agent, metric collection begins within a few minutes. The intended readers are DBAs and infrastructure engineers who operate SingleStore.

Installation proceeds in the following order. The SingleStore installation screens are built on top of the MySQL installation screens, so the flow is similar.

1. Check the Access Key
2. Review the architecture diagram
3. Create a DB account
4. Download the DBX agent
5. Configure the DBX agent
6. Start monitoring

Check the Access Key

When you create a WhaTap project, an **Access Key** is issued. This key identifies which project the agent sends data to. Enter it in the `license` field of the `whatap.conf` file.

Review the architecture diagram

The installation screen shows the SingleStore cluster architecture diagram. You can see how the aggregator (MA, CA) and leaf (Leaf) nodes are connected and where the DBX agent connects. The DBX agent connects to an aggregator node, and leaf nodes are auto-detected through `MV_NODES` and collected together. For a description of node roles, see the [SingleStore Monitoring](#) document.

Create a DB account

For the DBX agent to query cluster metrics, a dedicated monitoring account is required. Grant the following privileges.

```
grant select, process, cluster on *.* to '{monitoring_account}'@'%';
```

The part that can be confusing here is the privilege setup. Some of the dedicated privileges mentioned in the MySQL or MariaDB installation guides are not used in SingleStore; the installation guide states that the three privileges above are sufficient.

Download and configure the DBX agent

Download and install the DBX agent on an aggregator node, then configure the [whatap.conf](#) file. In `db_ip`, enter the address of the aggregator node to connect to. Leaf nodes are auto-detected through `MV_NODES` without being specified separately. SingleStore uses the following default settings.

whatap.conf

```
license={AccessKey}  
whatap.server.host={WhaTap_Server_Address}  
dbms=singlstore  
db_ip={Aggregator_Node_IP}  
db_port={DB_Server_Port}
```

For detailed descriptions of the configuration items, see the [Manual Installation](#) and [DBX Agent Configuration](#) documents.

For the firewall, allow Outbound traffic on port `6600` from the DBX agent to the WhaTap Server.

Start monitoring

Once you finish the configuration and run the agent, metric collection begins. When collection works properly, you can check the data on each screen in [SingleStore Monitoring](#).

Manual Installation

WhaTap database monitoring collects metrics by having the DBX agent connect to the SingleStore cluster. You only need to install the agent on one aggregator node; leaf nodes are auto-detected through `MV_NODES` and collected together with the rest of the cluster. There is no need to install the agent on every node. This document guides the basic method of installing the agent manually and configuring the `whatap.conf` file. It targets SingleStore 9.0 or later environments.

Create a monitoring account

Create a dedicated monitoring account for the DBX agent and grant the following privileges.

```
grant select, process, cluster on *.* to '{monitoring_account}'@'%';
```

Privilege	Description
<code>select</code>	Query the system views and tables required for monitoring
<code>process</code>	Query information about running sessions and queries
<code>cluster</code>	Query cluster node configuration and distribution state

Some of the dedicated privileges included in the MySQL or MariaDB guides are not required in SingleStore.

Download the DBX agent

On the installation screen, download the DBX agent that matches your operating system. SingleStore installation uses the Manual method.

Basic whatap.conf configuration

Set the following items in the [whatap.conf](#) file in the directory where the agent is installed.

whatap.conf

```
license={AccessKey}
whatap.server.host={WhaTap_Server_Address}
dbms=singlestore
db_ip={DB_Server_IP}
db_port={DB_Server_Port}
```

Option	Description
license	Project Access Key
whatap.server.host	WhaTap Server address to send data to
dbms	Fixed to singlestore
db_ip	IP of the SingleStore aggregator node to connect to
db_port	Connection port

The part that can be confusing here is the `dbms` value. For MySQL it is `dbms=mysql`, but for SingleStore it must be set to `singlestore`; the installation guide states that this is required for the SingleStore-specific screens to be enabled.

For detailed descriptions of the configuration options, see the [DBX Agent Configuration](#) document.

Firewall configuration

You must allow Outbound traffic on port `6600` from the DBX agent to the WhaTap Server.

Type	Direction	Port
DBX agent → WhaTap Server	Outbound	6600

Start monitoring

Once you finish the configuration and run the agent, metric collection begins.

DBX Agent Setting

Write the settings required by the DBX agent in the [whatap.conf](#) file. This document guides you through the options used for SingleStore monitoring.

Default options

Option	Type	Description
<code>license</code>	<code>string</code>	Project Access Key
<code>whatap.server.host</code>	<code>string</code>	Address of the WhaTap Server to send data to
<code>dbms</code>	<code>string</code>	Fixed to <code>singlestore</code>
<code>db_ip</code>	<code>string</code>	IP of the SingleStore node to connect to
<code>db_port</code>	<code>integer</code>	Connection port

`whatap.conf`

```
license={AccessKey}  
whatap.server.host={WhaTap_Server_Address}  
dbms=singlestore  
db_ip={DB_Server_IP}  
db_port={DB_Server_Port}
```

Additional options

Dashboard

The dashboard is the starting point for grasping the status of a SingleStore cluster at a glance. You can review the aggregator and leaf nodes together to scan the overall cluster state, then drill straight into a problematic node to check its detailed metrics and sessions.

Screen layout

Screen	Description
Instance List	Check the state, role (MA , CA , Leaf), and key metrics of the nodes in the cluster at a glance in a table
Instance Monitoring	Check the CPU, memory, disk, and network metrics and active sessions of a single node in real time
Multi-Instance Monitoring	Place the key metrics of multiple nodes side by side on one screen for comparison
Storage Engine	Analyze Rowstore and Columnstore usage and at-risk or excessive tables
Flex Board	Compose a custom dashboard by combining the widgets you want

You can drill into each screen to analyze per-node detailed metrics and sessions.

Instance List

The instance list screen gathers the nodes in a SingleStore cluster into a table, one per row. Because you can check the aggregator and leaf nodes together on one screen, it serves as the starting point for quickly scanning the overall cluster state and drilling straight into a problematic node.

Summary area

The area above the table shows the total node count and a breakdown by state.

Item	Description
Total	Total number of nodes being collected
Critical	Number of nodes classified as critical
Warning	Number of nodes classified as warning
Normal	Number of nodes in a normal state

Node list table

Each row corresponds to one node. The default columns are as follows.

Item	Description
Status	The collection and state of the node
Server Name	Node name (for example, 1-MA-150, LF-152). Click it to go to the corresponding Instance Monitoring
IP	Node IP address

Item	Description
Port	Connection port (default 3306)
Database	List of databases the node is responsible for
ROLE	Node role. MA (Master Aggregator), CA (Child Aggregator), Leaf
Cluster Name	Name of the cluster the node belongs to
Threads_running	Number of running threads
Questions	Number of processed queries
innodb_buffer_pool_read_requests	Number of buffer pool read requests
lock_wait_sessions	Number of sessions waiting on a lock

ⓘ For SingleStore, when you install the DBX agent only on an aggregator node, it auto-detects leaf nodes through MV_NODES and the entire cluster appears in the list. You can quickly distinguish roles by the MA , CA , and LF prefixes in node names.

Working with the table

- **Column selection:** You can add or hide the columns shown in the table.
- **Multi-view:** Select multiple nodes to switch to a screen that compares them together.
- After selecting a node, you can drill into the detail screen to examine its metrics and sessions in detail.

Data interpretation guide

Checkpoint	Description
Sudden spike in <code>Threads_running</code> on a specific node	Suspect load or contention concentrated on that node
Accumulating <code>lock_wait_sessions</code>	Lock waits are occurring; trace the cause with Lock Tree
Metric deviation among Leaf nodes	Possible data skew; check the layout in Partition

Instance Monitoring

On the instance monitoring screen, you can check the key metrics of a single SingleStore node in real time. When CPU and memory usage suddenly rise or sessions pile up on a specific node, it helps you quickly grasp what is happening on which node. The intended readers are DBAs who operate SingleStore.

Basic screen guide

Select the node to view from the instance selector at the top of the screen. A node's role is reflected in its name. You can distinguish node roles by the `MA` (Master Aggregator), `CA` (Child Aggregator), and `Leaf` values in the `ROLE` column of the instance list. The time range is queried in a default 10-minute window based on LIVE, and metrics refresh every 5 seconds.

At the top of the screen are KPI tiles for a quick view of node state.

Item	Description
Threads Running	Number of running threads
Connections	Number of connections
Queries	Query throughput
Successful Read Queries	Number of successful read queries
Failed Read Queries	Number of failed read queries
Failed Write Queries	Number of failed write queries

Below the KPI tiles are resource usage chart widgets.

Widget	Metric
CPU	<code>cpu_user_pct</code> · <code>cpu_system_pct</code> · <code>cpu_iowait_pct</code> · <code>cpu_idle_pct</code>

Widget	Metric
Memory	host_total_mb · host_used_mb
Disk Usage	os_mount_total_mb · os_mount_used_mb
Network Bandwidth	Node network IN and OUT

At the bottom of the screen is an area that switches between active sessions and the lock tree by tabs, along with a Lock Wait sessions widget.

Active session area

In the active session table at the bottom of the screen, you can check the sessions currently running on the cluster. Because SingleStore splits a single query across multiple nodes, it groups active sessions by aggregator activity. This lets you grasp what work the cluster is currently performing at the level of each task.

The table columns are as follows.

Column	Description
instance	Node where the session is running
node_id	Node identifier
database	Target database
session_id	Session identifier
user	Session user
state	Session state (for example, <code>executing</code>)
command	Type of command being run (for example, <code>Query</code>)
activity	Activity name

Column	Description
<code>raw_task</code>	Raw text of the running SQL
<code>sql_param</code>	SQL parameter
<code>aggregator_activity</code>	Aggregator activity name used as the grouping key
<code>elapsed(ms)</code> · <code>avg elapsed(ms)</code>	Execution time (max and average)
<code>cpu(ms)</code> · <code>cpu wait(ms)</code>	CPU usage and wait time
<code>lock wait(ms)</code>	Lock wait time
<code>network(ms)</code>	Network time
<code>disk i/o(ms)</code>	Disk I/O time
<code>disk spilling</code> · <code>avg spilling</code>	Disk spilling amount (max and average)
<code>part rows</code>	Number of partition rows processed
<code>conn</code>	Number of connections
<code>memory</code> · <code>avg memory</code>	Memory usage (max and average)

`node_id` , `aggregator_activity` , `part rows` , and `disk spilling` are SingleStore-specific columns that are meaningful only in a distributed execution environment.

When you click the SQL of a specific session in the active sessions, a detail window opens. For the SQL detail window, see the SQL detail view description in the [Top SQL](#) document.

Stopping a session

In SingleStore, you can select an active session and stop (Kill) it. The stop target is identified by its session ID (`session_id`).

⚠ Stopping a session forcibly terminates the running query. Check the scope of impact before using it with care.

Multi-Instance Monitoring

On the multi-instance monitoring screen, you can gather the metrics of multiple nodes in a cluster into one dashboard for comparison. In a distributed environment, load is sometimes concentrated on a specific node, and placing per-node metrics side by side lets you quickly find the skew.

Basic screen guide

The default dashboard (Default preset) consists of charts that gather the key metrics of each node and an active session table. As in instance monitoring, an `MA`, `CA`, or `LF` role tag is shown in front of each node name.

Adding widgets

You can compose the multi-instance dashboard by adding SingleStore-specific widgets from the widget palette. The method for adding, editing, and deleting widgets is the same as the common database dashboard editing method.

Active session area

In the active session table at the bottom of the dashboard, you can check sessions across the cluster. For column descriptions and the SQL detail view, see the [Instance Monitoring](#) and [Top SQL](#) documents.

Storage Engine

On the Storage Engine screen, you can check the memory and disk usage of Rowstore and Columnstore, the two ways SingleStore stores data. In a distributed environment, skew—where data piles up on a particular node—leads to performance degradation, and this screen shows the distribution across nodes at a glance to help you quickly find skew. The intended readers are DBAs who operate SingleStore.

Rowstore and Columnstore

SingleStore stores data in two ways. Knowing these two concepts first makes the screen easier to read.

- **Rowstore** stores data in memory by row. It is good for fast reads and writes but uses a lot of memory. Simply put, it is closer to keeping the items you use often on top of your desk.
- **Columnstore** stores data on disk by column in compressed form. It is good for large-scale analysis and has high disk efficiency. It is closer to compressing items you rarely use and putting them in a warehouse.

The screen shows these two separately.

Summary information

When you select the cluster to query (for example, `memsql_cluster`) at the top of the screen, it shows the state of Rowstore and Columnstore in two summary cards. Each card shows a `WARN` badge when the state needs attention.

Card	Description
Rowstore summary information	Total in Memory, Max Node Mem, Avg Memory Deviation, Worst skew table
Columnstore summary information	Total on Disk, Compression, Avg Disk Deviation, Worst skew table

`Avg Memory Deviation` and `Avg Disk Deviation` express the usage deviation across nodes as a multiple. The larger the value, the more data is concentrated on a particular node. `Worst skew table` also points out the table with the most severe skew.

Rowstore area

Since Rowstore uses memory, memory usage and per-node distribution are the key metrics.

Widget	Description
Memory usage by node	Displays per-node host memory usage as a gauge
Memory Trend	The time trend of Table Memory (Rowstore) and Server Memory (Process)
Memory-Risk Tables (TOP 5)	The top 5 tables with high memory risk

The per-node memory gauge shows host memory usage together with the usage and total capacity (for example, 2.4 / 3.7 GB) and the percentage. It distinguishes the <80% , 80-90% , and >90% ranges by color, and aggregator (MA/CA) nodes are collapsed by default and can be expanded to view.

Memory-Risk Tables (TOP 5) is made up of the following columns.

Column	Description
Table	The table name and database
Worst Node	The node with the highest usage
Size (Total)	The total memory usage and row count
Parts	The number of partitions
Skew	The skew multiple across nodes

Columnstore area

Since Columnstore uses disk, disk usage and segment state are key.

Widget	Description
Disk usage by node	Displays per-node disk usage as bars
Segment Group trend	A daily comparison of the number of segment groups (<code>group_cnt</code>) and the top tables
Size Top 5	The top 5 tables that take up the most disk

The per-node disk bar shows the disk SingleStore uses, divided by area. Clicking a bar lets you check the detailed composition per node.

Area	Description
Data	Columnstore data
Snapshot	Snapshot
Log	Transaction log
Temp	Temporary data
Etc	Areas outside partitions
Others	Other OS usage
Free	Remaining space

Size Top 5 shows, per table, the compressed size (`Size (Total)`), the compression ratio (`Compression`), the row count (`Rows`), and the node with the highest usage (`Worst Node`).

A part that can be confusing here is the Segment Group trend. SingleStore manages Columnstore data as segments, and a background merger combines small segments to tidy them up. The Segment Group trend compares the cluster's `group_cnt` sum against the day before and shows it, and provides the top 5 tables with the largest current `group_cnt` in a table together with their 24-hour change (`Δ24h`) and partition count. If `group_cnt` keeps trending upward, it can be seen as a sign that the automatic merger is not keeping up with the INSERT rate, in which case you would consider an `OPTIMIZE` operation.

Checking data skew

In a distributed database, when data is skewed toward a particular node, only that node ends up bearing the load. The Storage Engine screen shows skew with the following metrics.

Metric	Description
Max Node Mem	The highest memory usage among the nodes
Avg Memory Deviation	The average deviation (multiple) of Rowstore memory usage across nodes
Avg Disk Deviation	The average deviation (multiple) of Columnstore disk usage across nodes
Skew	The skew multiple across nodes at the table level
Worst skew table	The table with the most severe skew

Clicking a row of a table with severe skew opens the detail drawer, where you can check the per-node distribution along with the **OPTIMIZE** recommendation.

OPTIMIZE recommendation

In the table detail drawer, it guides you step by step on whether data cleanup (**OPTIMIZE**) is needed. The guidance is divided according to the recommendation level.

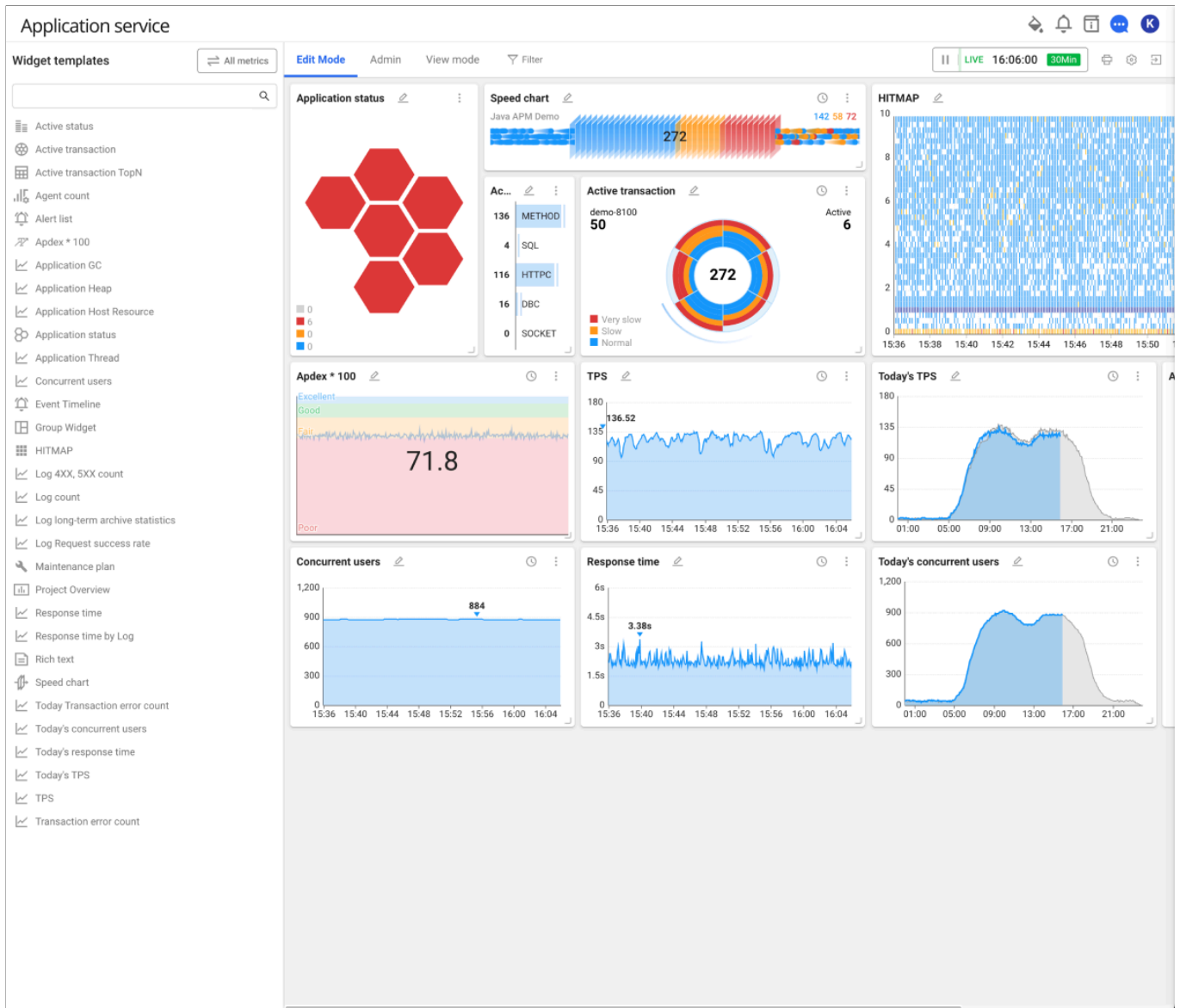
Query point

The screen uses the real-time time selector. It shows the latest collected values according to the collection cycle, and by default Memory Trend queries the last 1 hour and the cluster summary queries the last 7 days.

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 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.

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.



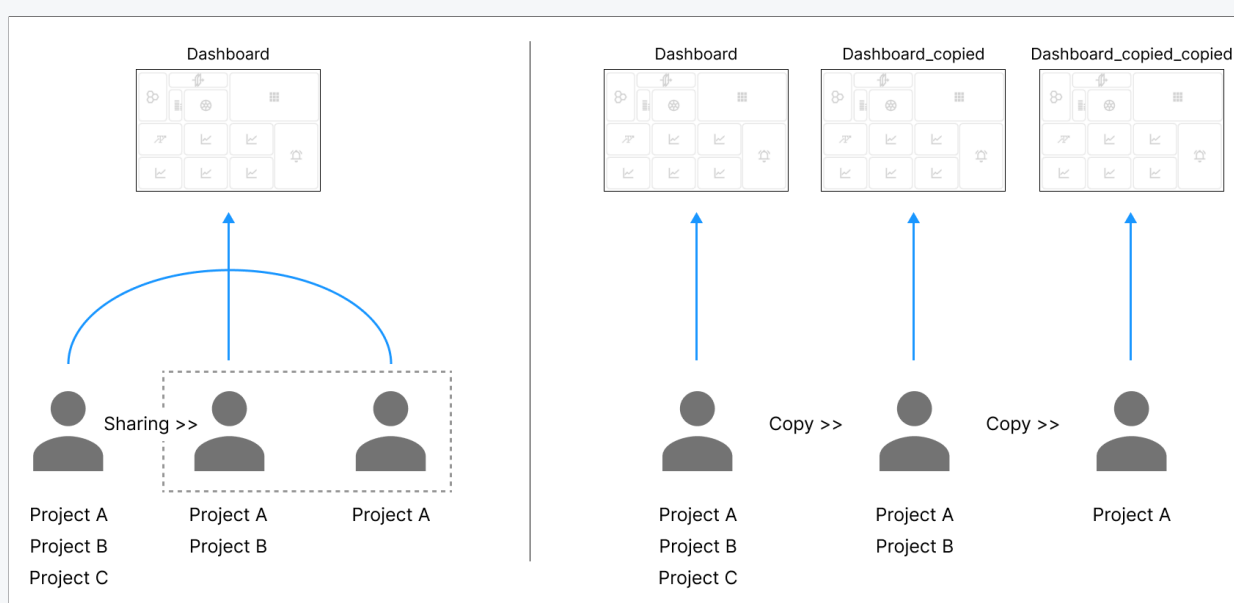
- If a user who received a shared dashboard deletes it, it is deleted only from that user's **Dashboard list**. The original dashboard remains.

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 to 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 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**

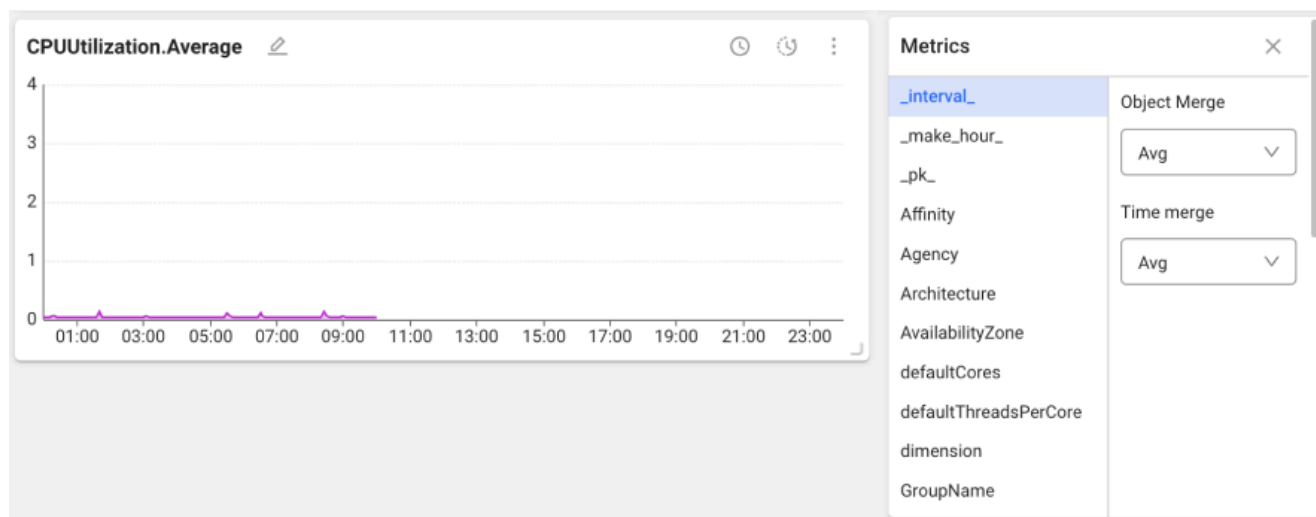
It is used to group the chart data based on the tag (e.g. agent name) selected on the left. At this time, if the tags match among the data with different fields (e.g. CPU), the corresponding data is merged.

- **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**.

Analysis

In the Analysis menu, you dig deep into the root causes of anomalies discovered in the dashboard. You can examine sessions and locks, the distributed structure (partitions and pipelines), and metric trends from various angles to find the root cause.

Screen Composition

Screen	Description
Trend Comparison	Compare key metrics and session flows of two points in time side by side
Lock Tree	Trace lock wait relationships in a tree to identify blocking causes
Session History	Query and analyze past active sessions in chronological order
Partition	Check data skew and Shard Key suitability
Pipeline	Track pipeline ingestion status (processing rate, failures, backlog)
Database Parameter	Query parameter values and compare them by date
Metrics Chart	Query metric data as charts
Metrics Trend Analysis	Analyze long-term metric trends

Trend Comparison

On the Trend Comparison screen, you can place two different points in time side by side and compare key metrics and session flows. This helps when comparing the load on an unusual day against a normal one, or comparing before and after a change to see what differed.

Setting Comparison Conditions

At the top of the screen, specify the two points in time and the targets to compare.

Item	Description
Base Date	The date that serves as the basis for comparison
Comparison Date	The date to compare against the base
Instance	Select the target node (<code>oname</code>) for the base and the comparison respectively
Database	Displays the databases handled by the selected instance
Preset	Save and load frequently viewed chart configurations (<code>Default</code> provided)

If you specify different instances for the base and the comparison, you can also compare different nodes on the same date.

KPI Comparison Charts

Overlays the key metrics of the base time and the comparison time on the same axis, displayed in 5-minute intervals.

Metric	Description
Threads Running	Number of running threads

Metric	Description
Connections	Number of connections
Queries	Number of queries processed
Successful Queries	Number of successful queries
Failed Queries	Number of failed queries
CPU	CPU usage
Engine Memory	Memory used by the engine
Disk Usage	Disk usage
Network Bandwidth	Network bandwidth

Since each chart overlays the curves of the base and comparison times, you can see at a glance how much the load differed during the same time period.

ⓘ Engine Memory is the same memory metric as the Memory widget on the instance monitoring screen, labeled for the Trend Comparison screen.

Base and Comparison Session Tables

Below the charts, the session lists of the base time and the comparison time are displayed side by side. When you select a specific time on the time bar above, you can view the sessions collected at that point in time on both sides together.

Both tables use the same columns.

Column	Description
instance	The node where the session was executed. Click to move to the corresponding Instance Monit

Column	Description
	oring screen
id	Session identifier
user	The user who executed the session
host	Connecting host
db	Target database
command	The type of command the session is executing (Query , etc.)
runtime	Execution time
state	Session status (executing , etc.)
query	SQL being executed
query_param	Bound parameter values
type	Session type
connection_type	Connection type

Data Interpretation Guide

Checkpoint	Description
Metric spike in the same time period	A period with increased load compared to the comparison time; suspect the impact of a change or event
Failed Queries concentrated on one side	Errors concentrated on a specific date; check correlation with deployments or data changes

Checkpoint	Description
Increase in session count and execution time	Suspect a change in query patterns or increased contention; trace the causal query through the session table

Lock Tree

On the Lock Tree screen, you can view sessions that are waiting on each other due to locks in a tree form. It shows which session is holding a resource (holder) and which session is waiting for it (waiter) as a parent-child relationship, helping you quickly find the session that caused a deadlock.

Locks and the Lock Tree

Simply put, a lock is a locking mechanism that prevents the same data from being changed simultaneously. While one session is modifying data, other sessions must wait. As the number of waiting sessions grows and they become entangled with each other, a deadlock occurs. The Lock Tree lays out these wait relationships in a tree shape so you can find the session holding the resource (the cause) at the very top.

Basic Screen Guide

At the top of the screen, select an instance and a database. First, select the point in time when a lock wait occurred in the Lock Wait Sessions chart, and you can then view the Lock Tree and Total Locks at that point. It highlights locks that have persisted for several minutes or more, so you can quickly find long-held locks.

Area	Description
Lock Wait Sessions	A chart of lock wait session counts by time period. Select a point in time to query
Lock Tree	Displays the lock wait relationships at the selected point in time as a tree
Total Locks	The total number of locks at the selected point in time

Column Guide

The session holding a resource (holder) and the session waiting (waiter) are displayed with the following columns.

Column	Description
instance	The node where the session is running
node_id	Node identifier
session_id	Session ID
db	The database in use
user	Connected user
tx_state	Transaction state
lock_type	Lock type
row_locks	Number of row locks
partition_locks	Number of partition locks
activity	Activity name
raw_task	The raw text of the SQL being executed
sql_param	SQL parameters
command	The type of command being executed
elapsed_time_ms	Execution time (milliseconds)

One point that can be confusing here is how sessions are identified. MySQL identifies a session by a single session ID, but because SingleStore is a distributed environment, it uses the node identifier and the session ID together (`node_id` + `session_id`) as the matching key. This is because even the same session ID refers to a different session if the node differs. `row_locks` and `partition_locks` distinguish whether a lock is at the row level or the partition level in a distributed environment.

Resolving Locks

After identifying the causal session (holder), you can stop that session if necessary. For how to stop a session, refer to the [Session History](#) and [Instance Monitoring](#) documents.

Analyzing with AI

Click the **WhaTap AI** button on the screen to open the WhaTap AI chat window, where the queried screen data is summarized and the analysis result is shown as a conversation. After reading the result, you can continue with follow-up questions in the same conversation.

- The data used for the analysis is three sets: the trend for the whole query range, the 30-minute interval aggregation, and the lock tree snapshot at the selected point in time.
- The analysis target is the data queried on the screen. If you change the query conditions and analyze again, the analysis is based on the changed data.
- The conversation history is recorded in the `AI Analysis - {screen name}` format.

Session History

On the Session History screen, you can query past collected session information in chronological order. You can go back in time to analyze which session executed which SQL at a specific time period and how much resources it used. This helps when retracing the cause after an incident has passed.

Data is provided based on active session snapshots (`db_singlestore_active_session`).

Basic Options

Set query conditions in the top filter area.

Item	Description
Time	Select the query time range
Instance	Select the target node (<code>oname</code>) to query
Filter	Add conditions per field; AND logic is applied for multiple conditions
Download	Export in CSV format

Session Trend Chart

Displays the number of active sessions during the query period as a bar chart. The X-axis is time and the Y-axis is the number of sessions.

- Drag the chart area with the mouse to narrow down to that interval for detailed analysis.
- Click a bar in the chart to move to the [Instance Monitoring](#) screen for that point in time (±5 minutes). You can check the node status at the time when sessions were numerous.

Long-Running Sessions

Along with the session trend, a Long-Running Sessions area is provided. It collects and displays sessions that ran for a long time during the query period, so you can quickly pick out inefficient queries or stalled transactions.

Session List Table

Displays the collected session information in chronological order. You can apply conditions using the fields and filters at the top, and adjust the number of rows shown at once using the page size setting at the bottom.

The columns share the same distributed execution metrics as the active session table in [Instance Monitoring](#) (`instance` , `node_id` , `session_id` , `state` , `elapsed(ms)` , `cpu(ms)` , `memory` , `aggregator_activity` , etc.), and add the following columns for historical queries.

Column	Description
<code>time</code>	The time when the session was collected
<code>sql_hash</code>	A hash value that groups identical SQL

With `sql_hash` , you can group repeated executions of the same query, which helps determine whether a specific SQL repeatedly consumes a lot of resources.

Stopping Sessions

You can select a session and stop (Kill) it. The stop target is identified by the session ID (`session_id`), and the node identifier (`node_id`) is normalized to a number for processing.

⚠ Stopping a session forcibly terminates the running query. Use it carefully after checking the scope of impact.

Data Interpretation Guide

Checkpoint	Description
Sessions with long execution time	Long-running sessions; suspect lock contention, inefficient queries, or incomplete transactions
Many sessions in waiting state	Contention for a specific resource has occurred; lock cause analysis needed
Sessions concentrated on a specific node	Suspect data skew or routing bias

Partition

On the Partition screen, you can check how evenly a table's data is divided across the cluster nodes. SingleStore splits a table into multiple partitions and distributes them across nodes; if this distribution is skewed to one side, only certain nodes end up doing more work. This screen shows the skew as a deviation from the average, helping you find tables whose balance is broken.

What is a partition

Simply put, a partition is the unit by which a large table is split into pieces scattered across nodes. When data is spread evenly, the nodes can share the work and run faster. Conversely, when the pieces pile up on one node, that node becomes a bottleneck. That is why, in a distributed database, it matters whether partitions are spread evenly.

Partition layout map (by host)

When you select a cluster at the top of the screen, it shows, in a grid, which host (leaf node) each partition is placed on, per database. The total number of partitions (for example, `PARTITIONS=16`) is shown for each database, and the color of each partition cell distinguishes its skew state. You can narrow the scope with the all-hosts and all-DB filters.

State	Meaning
Hot	2x or more of the average
Warning	1.5x or more of the average
Normal	Within the normal range
Empty	A partition with no rows (<code>rows=0</code>)
Offline	An offline partition

Table-level Partition Distribution

At the center of the screen is the table-level partition distribution table. It shows how evenly each table is distributed across nodes with `Avg Deviation` . `Avg Deviation` is `Max / Avg` , the multiple indicating how many times the largest partition is over the average. The closer the value is to 1x, the more evenly distributed it is; the larger it is, the more it is skewed toward a particular partition. By default the table is sorted in descending order of `Avg Deviation` , so the most skewed tables rise to the top.

The columns of the table are as follows.

Column	Description
Table	The <code>database.table</code> name
Storage	Storage engine (<code>ROWSTORE</code> / <code>COLUMNSTORE</code>)
Shard Key	The column used to divide data across nodes
Cardinality	The number of distinct values of the Shard Key
Partitions	The total number of partitions
Used Parts	The number of partitions that contain data
Total Rows	The total number of rows
Total Size	The total size
Max Part Size	The size of the largest partition
Avg Deviation	The skew multiple across nodes (<code>Max / Avg</code>)

Looking at `Shard Key` and `Cardinality` together helps you pinpoint the cause of skew. When the Shard Key has few distinct values (low cardinality), the same values tend to pile up in one partition, making skew more likely.

The state is classified by the `Avg Deviation` value as follows.

State	Criteria
Healthy	< 1.5x
Warning	1.5x ~ 2x
Critical	≥ 2x, or empty partitions exist

Tables that do not meet the per-node statistics collection threshold are hard to evaluate for distribution, so they are treated as N/A and excluded from the table. This behavior keeps the comparison to reliable data only. You can adjust the display scope with the all-states and Top 5 filters.

Row Count Growth (Top 5 Hot Partitions)

Shows the trend of the top 5 partitions whose row count is growing the fastest. Each item is shown in the form `P#partition_number table (node)` (for example, `P#9 merge_active_demo (LF-153)`). Partitions whose data is growing rapidly may soon break the distribution balance, so it helps to look at them in advance.

Partition detail drawer

Clicking a table row in the table opens the partition detail drawer. The drawer shows disk and memory usage as gauges in two areas, along with key metrics (KPIs) such as row count, size, and skew.

Query point

The screen uses the RangeTimeSelector, with a default range of today (from 00:00 to 00:00 the next day). With the Quick buttons, you can quickly select 6 hours, 12 hours, today, yesterday, 2 days ago, 7 days ago, or 30 days ago.

⚠ Partition data is collected at 1-hour intervals. If you set the query range to shorter than 1 hour, data may not appear, so setting it to 1 hour or longer is recommended.

If the query range is shorter than 1 hour or exceeds 24 hours, an information box appears on the screen. The values shown are the last collected values within the range (LAST-ONLY).

Pipeline

The Pipeline screen lets you check how well SingleStore's data ingestion pipelines are running. When a pipeline falls behind or fails, data does not arrive on time. This screen brings together throughput, latency, and errors so that you can quickly pinpoint where the problem is.

What is a pipeline

A SingleStore pipeline automatically pulls data from external sources (files, message queues, and so on) and loads it into tables. In simple terms, it is like a conveyor belt that continuously moves data. If the belt slows down or stops, data piles up, so it is important to watch the processing speed and errors.

Basic screen guide

Select the cluster to query at the top of the screen. The screen consists of a status summary, KPI cards, trend charts, a pipeline details table, and recent errors.

KPI cards

The cards show the key metrics of the overall pipeline.

Card	Description
PIPELINES	Total number of pipelines
FAILING PIPELINES	Number of pipelines that are currently failing
BATCH SUCCESS RATE	Batch success rate
FAILED BATCHES	Number of failed batches
BATCHES	Number of processed batches (batches per interval)

Each card also shows a secondary unit such as `rows/s (avg)` , `batches per interval` , or `milliseconds (avg)` .

Trend charts

Two time-series charts show the processing status of the pipelines.

Chart	Description
<code>RPS by Pipeline</code>	Rows processed per second for each pipeline (rows per second)
<code>Batch Success / Failure</code>	Trend of batch successes and failures

Clicking a specific pipeline in a chart filters both the chart and the table below by that pipeline.

Pipeline Details table

The table shows the processing status of each pipeline. You can search by pipeline, source, or table name in the search box at the top.

Column	Description
<code>Pipeline</code>	Pipeline name
<code>Source</code>	Data source
<code>Target Table</code>	Target table for ingestion
<code>Type</code>	Source type
<code>Kind</code>	Pipeline kind
<code>RPS (avg)</code>	Rows processed per second (average)
<code>Rows Total</code>	Total number of rows ingested

Column	Description
Batches OK	Number of successful batches
Failed	Number of failed batches
Queued	Number of queued batches (backlog)

Clicking a pipeline row in the table opens the batch-level details drawer. In the drawer, you can review the batch metric charts and recent errors for the selected pipeline.

Recent Pipeline Errors

At the bottom of the screen, you can check the pipeline errors that occurred recently.

Column	Description
Error Time	Time the error occurred
Pipeline	Pipeline where the error occurred
Batch	Batch identifier
Code	Error code
Message	Error message
Host	Host where it occurred
Instance	Instance where it occurred

- Opening the batch drawer automatically queries recent errors.
- The error list is shown across multiple pages.
- You can search by pipeline, type, code, or message in the search box.

Query time

You can check the last collection time at the top right of the screen.

Database Parameter

Home > Select Project > **Analysis** > **Database Parameter**

Using the database configuration inquiry, you can view the database settings of the past. You can compare parameter values in the database by date through the comparison function. By default, you can see the data of the current time.

If a problem occurs due to a parameter in the database, the cause can be quickly recognized through the database parameter comparison function.

Database parameter		
Reference date	Comparison date	Instance
2023/10/04	2023/10/10	demo-01
View Changes		
Key	2023/10/04	2023/10/10
wsrep_ready(stat)	ON	OFF
wsrep_provider_version(stat)	4.9(rcece3ba2)	4.9(rcece3ba2)
wsrep_provider_vendor(stat)	Codership Oy <info@codership.com>	Codership Oy <info@codership.com>
wsrep_provider_name(stat)	Galera	Galera
wsrep_provider_capabilities(stat)	:MULTI_MASTER:CERTIFICATION:PARALLEL_APPLYING:TRX_REPLAY:ISOLATION:P AUSE:CAUSAL_READS:INCREMENTAL_WRITESET:UNORDERED:PREORDERED:STRE AMING:NBO:	:MULTI_MASTER:CERTIFICATION:PARALLEL_APPLYING:TRX_REPLAY:ISOLATION:P AUSE:CAUSAL_READS:INCREMENTAL_WRITESET:UNORDERED:PREORDERED:STRE AMING:NBO:
wsrep_connected(stat)	ON	ON
wsrep_cluster_status(stat)	Primary	non-Primary
wsrep_cluster_state_uuid(stat)	37ea72c5-ee15-11ed-8f3e-67510a6d46e9	37ea72c5-ee15-11ed-8f3e-67510a6d46e9
wsrep_cluster_capabilities(stat)		
wsrep_gcomm_uuid(stat)	c094ae4d-56c3-11ee-8772-57dd9d06a011	c094ae4d-56c3-11ee-8772-57dd9d06a011
wsrep_evs_state(stat)	OPERATIONAL	OPERATIONAL
wsrep_evs_rep_latency(stat)	0.000372136/0.000778795/0.0157565/0.00107258/1859	0/0/0/0/0
wsrep_evs_evict_list(stat)		
wsrep_evs_delayed(stat)		
wsrep_incoming_addresses(stat)	10.21.1.236:0,10.21.1.86:0,10.21.1.136:0	10.21.1.86:0
wsrep_local_state_comment(stat)	Synced	Initialized
wsrep_flow_control_requested(stat)	false	false
wsrep_flow_control_active(stat)	false	false
wsrep_local_state_uuid(stat)	37ea72c5-ee15-11ed-8f3e-67510a6d46e9	37ea72c5-ee15-11ed-8f3e-67510a6d46e9
Ssl_version(stat)		
Ssl_session_cache_mode(stat)	NONE	NONE
Ssl_server_not_before(stat)		
Ssl_server_not_after(stat)		
Ssl_cipher_list(stat)		
Ssl_cipher(stat)		
Slave_running(stat)	OFF	OFF
Rpl_status(stat)	AUTH_MASTER	AUTH_MASTER
Rpl_semi_sync_slave_status(stat)	OFF	OFF
Rpl_semi_sync_master_status(stat)	OFF	OFF
Innodb_have_punch_hole(stat)	ON	ON
Innodb_have_snappy(stat)	ON	ON
Innodb_have_bzip2(stat)	OFF	OFF
Innodb_have_lzma(stat)	OFF	OFF
Innodb_have_lzo(stat)	OFF	OFF
Innodb_have_lz4(stat)	ON	ON
Innodb_buffer_pool_load_incomplete(stat)	OFF	OFF

1. Set values for **Reference date** and **Comparison date**.
2. Select a desired instance in **Instance**.
3. Click .

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

Database parameter		
Reference date	Comparison date	Instance
2023/10/04	2023/10/10	demo-01
View Changes		
Key	2023/10/04 Value	2023/10/10 Value
wsrep_ready(stat)	ON	OFF
wsrep_cluster_status(stat)	Primary	non-Primary
wsrep_evsv_rep_latency(stat)	0.000372136/0.000778795/0.0157565/0.00107258/1859	0/0/0/0/0
wsrep_incoming_addresses(stat)	10.21.1.236:0,10.21.1.86:0,10.21.1.136:0	10.21.1.86:0
wsrep_local_state_comment(stat)	Synced	Initialized
auto_increment_offset	2	1
auto_increment_increment	3	1

✔ Comparing database parameters for today

Database parameter

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 Chart

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

The **Metrics Chart** *New* menu is a core feature of the WhaTap monitoring solution, which provides the data collected from various monitoring targets in a visualized time-series chart. This allows users to effectively monitor the system performance, quickly identify anomalies, and gain insights for resolving issues.

- You can visually check various metrics via time series charts, and analyze multiple metrics upon failure at a time.
- You can select a specific time range to view past data and analyze the performance at that period.
- You can filter data based on specific time zones or conditions for more accurate analysis.
- Users can place their desired charts on the screen and freely adjust the layout.
- Users can arrange desired metrics and save them as presets for loading at any time.

ⓘ Difference from the Metrics Chart menu

The following are the changes since the [Service 2.8.0](#) update. To check the changes on the screen after the update, select **Tutorials** on the upper right.

- User experience (UX) has been improved so that users can set the time, target, and interval options, and then specify the metrics to monitor and add charts.
- You can change the time range of a chart view without deleting the widgets placed on the dashboard.
- It provides a batch **Batch Change** feature that allows you to apply options to all widgets placed on the dashboard at once.
- The preset feature allows you to save and load the widgets placed on the dashboard.
- You can adjust the layout of the dashboard and the functionality of the widgets through various options provided.

Adding a chart widget

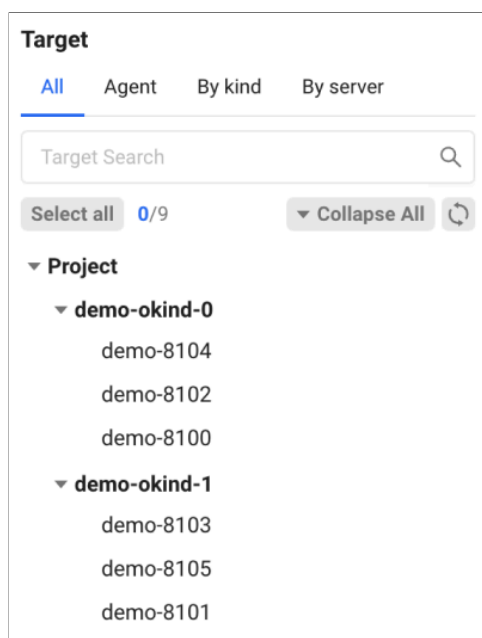
To add a metric as a widget to the dashboard, select **Add chart** on the upper left.

Setting the lookup time

In **Time**, set the date and time to view the metric.

Selecting a target

Select a desired target from the agents in the project. You can select an individual agent or a group classified by the agent configuration.



- **Agent:** You can select an individual agent or all agents.
- **By kind:** Agents can be monitored in each group classified by `whatap.okind` in the agent configuration.
- **By server:** Agents can be monitored in each group classified by `whatap.onode` in the agent configuration.

- Depending on the set time and date, available targets may change.
- You can select or deselect targets by clicking in the agent list. You can also select multiple agents at once by using the **Shift** key.
- By clicking **Select all** or **Deselect all**, you can select or deselect related sub-targets at once.
- If a desired agent does not appear in the list, select **Refresh**.
- By selecting **Collapse All** or **Expand All**, you can hide or expand the list by group.

Selecting a metric

Select a target agent to monitor. Then the list that can be selected on the **Metric** panel appears. Select a desired metric in the list.

A chart widget for the selected metric is placed on the dashboard on the right. You can add chart widgets by selecting additional metrics. To enlarge the chart area, select **×** on the right of the **Time** option. The **Target** and **Metric** panels disappear, leaving only the chart area visible on the screen.

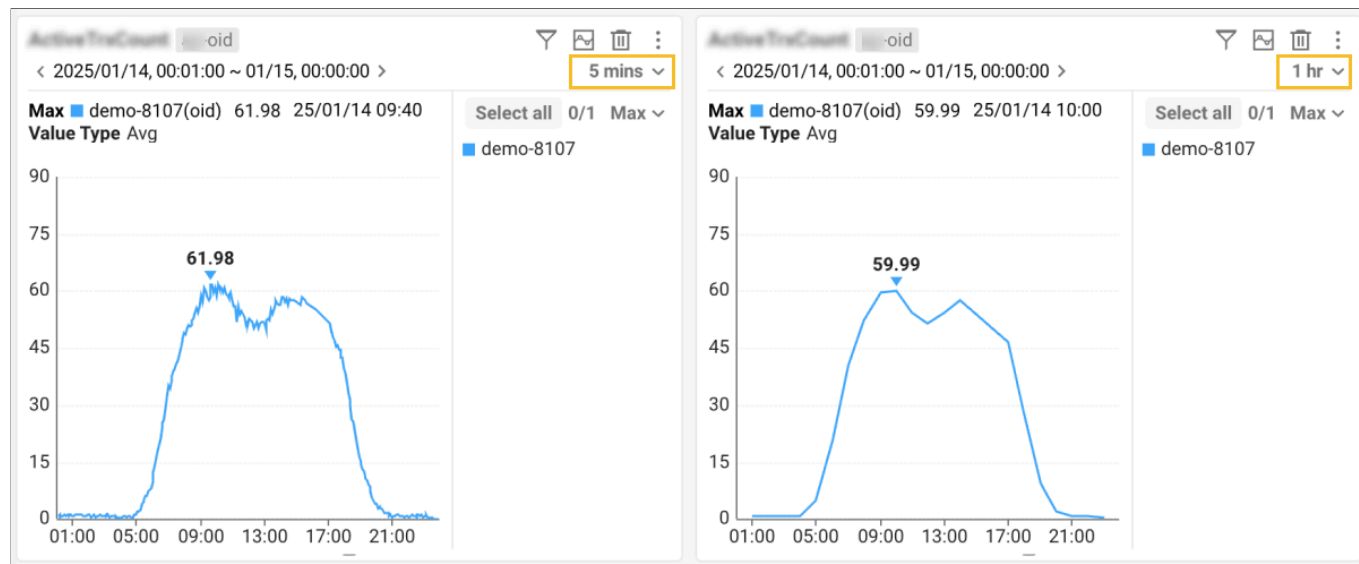
- If you enter a string in the **Search indicator** field, you can quickly search for a desired metric.
- By selecting **Collapse All** or **Expand All**, you can hide or expand the metrics list by category.
- If a desired metric does not appear in the list, select **Refresh**.

Setting the interval

You can set intervals for each chart, allowing you to adjust the aggregation unit of data to visualize at different time intervals. If you select **⌚** on the upper right of the **Metric** panel, you can select an interval option.

Each metric has a different default interval time, and the interval time changes depending on the query time range.

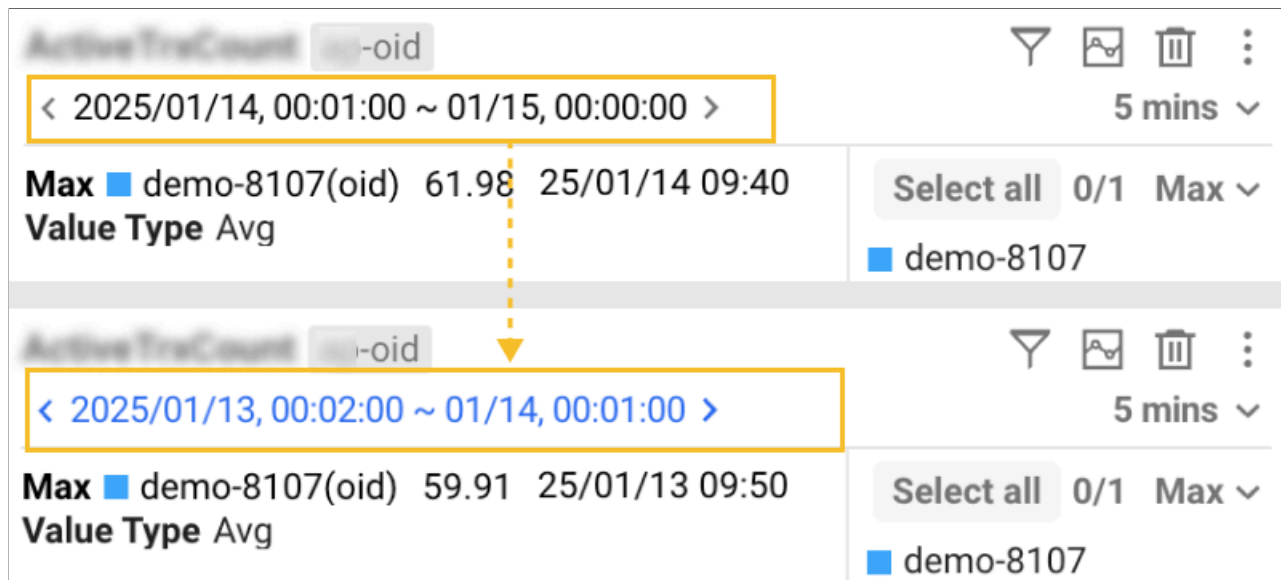
For example, the **5 min** interval displays average values for 5-minute intervals, and the **1 hour** interval displays average values for every one hour.



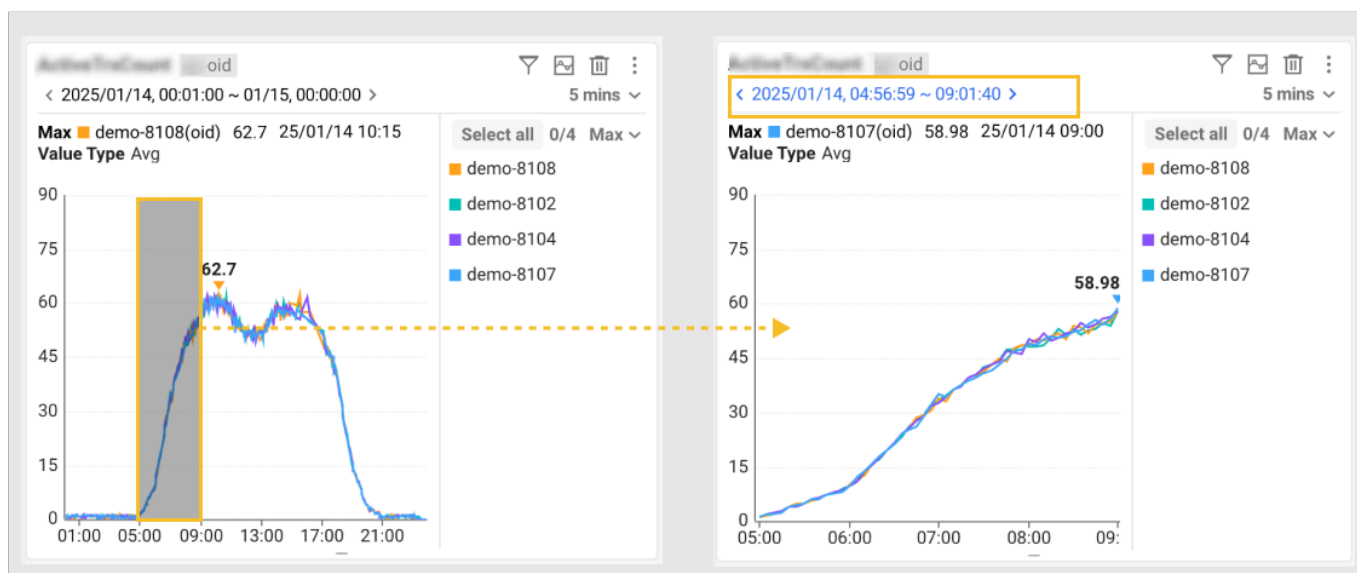
- ✓ By adjusting the interval option, you can analyze the data from different perspectives, from detailed data over a short time to overall trend over a long time.

Changing the query time

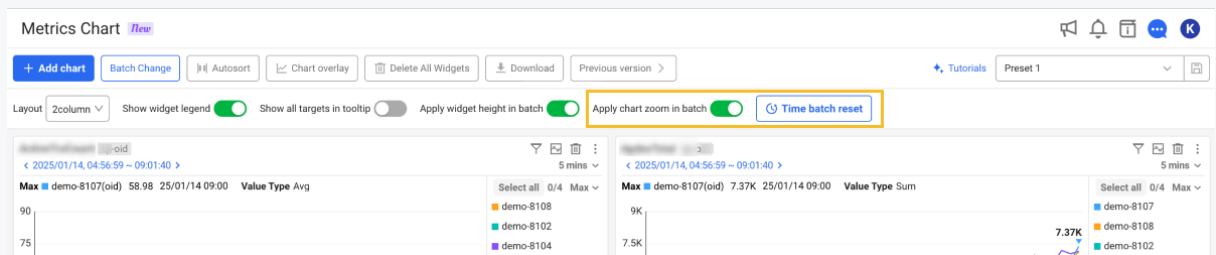
To change the chart query time range for an individual widget, select **<** or **>** at the top of the widget. The time change range is the same as the time reference set in the **Time** option. For example, if the **Time** option is set to **1 day** and you select **<** or **>**, you can change the time to a daily interval.



Alternatively, by dragging a specific area of the chart, you can change the time according to the dragged range for a view.



- You can change the time for all widgets by changing for each widget with the **Apply chart zoom in batch** option enabled at the top of the screen.



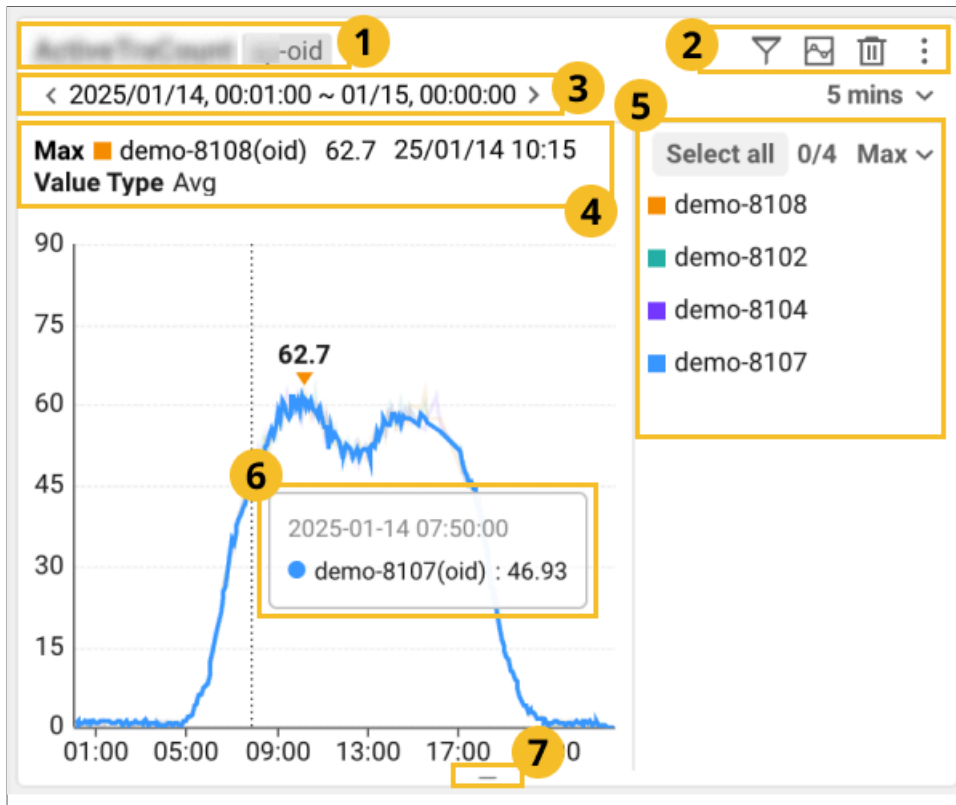
- To change the query time range and then change it back to a recent time, select

If the **Apply chart zoom in batch** option is enabled at the top of the screen, the **Time batch reset** button appears. By selecting this button, you can reset the time for all widgets.

- ! By using the **Batch Change** feature, you can change the time for all widgets and change the monitoring target and interval. For more information, see [the following](#).

Chart details

See details for each item displayed in the chart widget.



- **1 Metric name and category:** It displays the metric name of the chart widget. On the right of the metric, the categories of the query targets are displayed in tag format. The category name may differ depending on the product.
 - `*oid` : It is displayed when an individual agent is selected.
 - `project` : It is displayed when the target is selected on a project basis.
 - `okind` : It is displayed when a group classified as `whatap.okind` is selected in the agent configuration.
 - `onode` : It is displayed when a group classified as `whatap.onode` is selected in the agent configuration.
- **2 Widget option:** Option menu of the chart widget. For more information, see [the following](#). For more information about the interval options, see [the following](#).
- **3 Time:** It displays the time range for which data in the chart is viewed. By selecting `<` or `>`, you can adjust the time range for a query.
- **4 Data:** You can check the maximum value (**Max**) of the data viewed from the monitoring targets and the data merge method (**Value Type**).
- **5 Legend:** It displays the monitoring targets as a legend. For more information about the display of legend,

see [the following](#).

- **6 Chart:** It displays the viewed data in a time series graph. If you hover your mouse pointer over the graph, you can see detailed information through a tooltip. By dragging a specific area of the chart, you can change the time according to the dragged range for a view.
- **7 Resize:** You can adjust the size by dragging the center of the bottom of the chart widget.

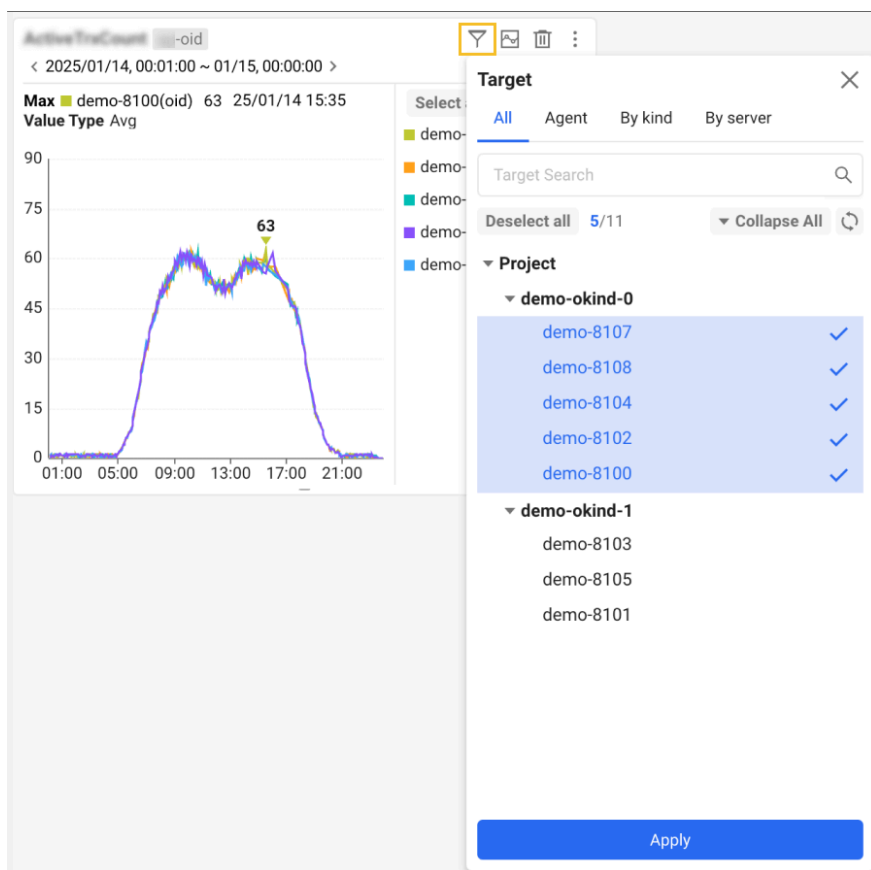
Using the chart widget options

Various features can be used through the option buttons on the upper right of the chart widget.

Filtering targets

You can add or remove monitoring targets to/from the chart widget added to the screen.

1. If you select , a pop-up menu appears for you to select monitoring targets.



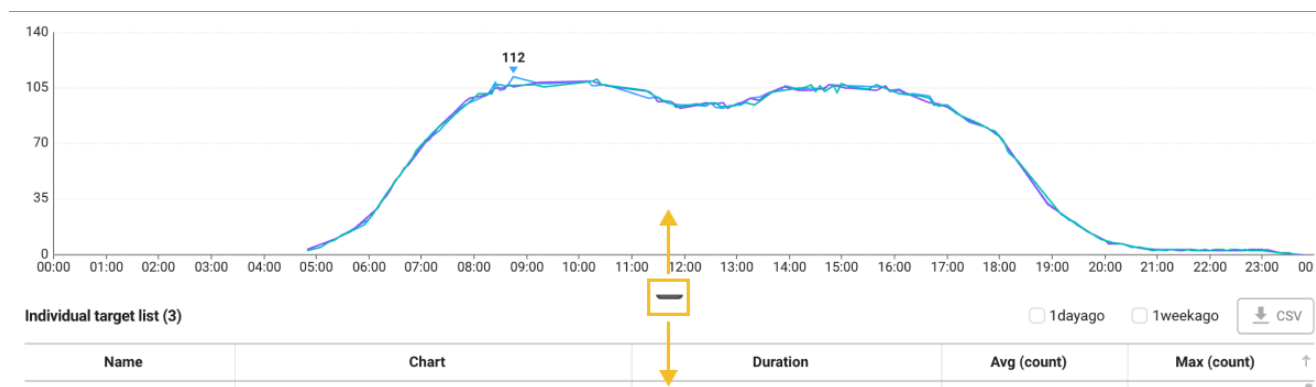
2. Select the desired targets according to the instructions on the screen.
3. Select **Apply**.

Viewing the details

To check the detailed information about the chart data in a wider screen, select . The **View details** window appears. You can view charts, averages, and maximum values for individual targets.



- **1dayago:** You can compare the data with that from the previous day.
- **1weekago:** You can compare the data with that of the previous week.
- **↓ CSV:** The viewed data can be downloaded as a CSV file.
- You can resize the chart by dragging the icon at the bottom of the graph.

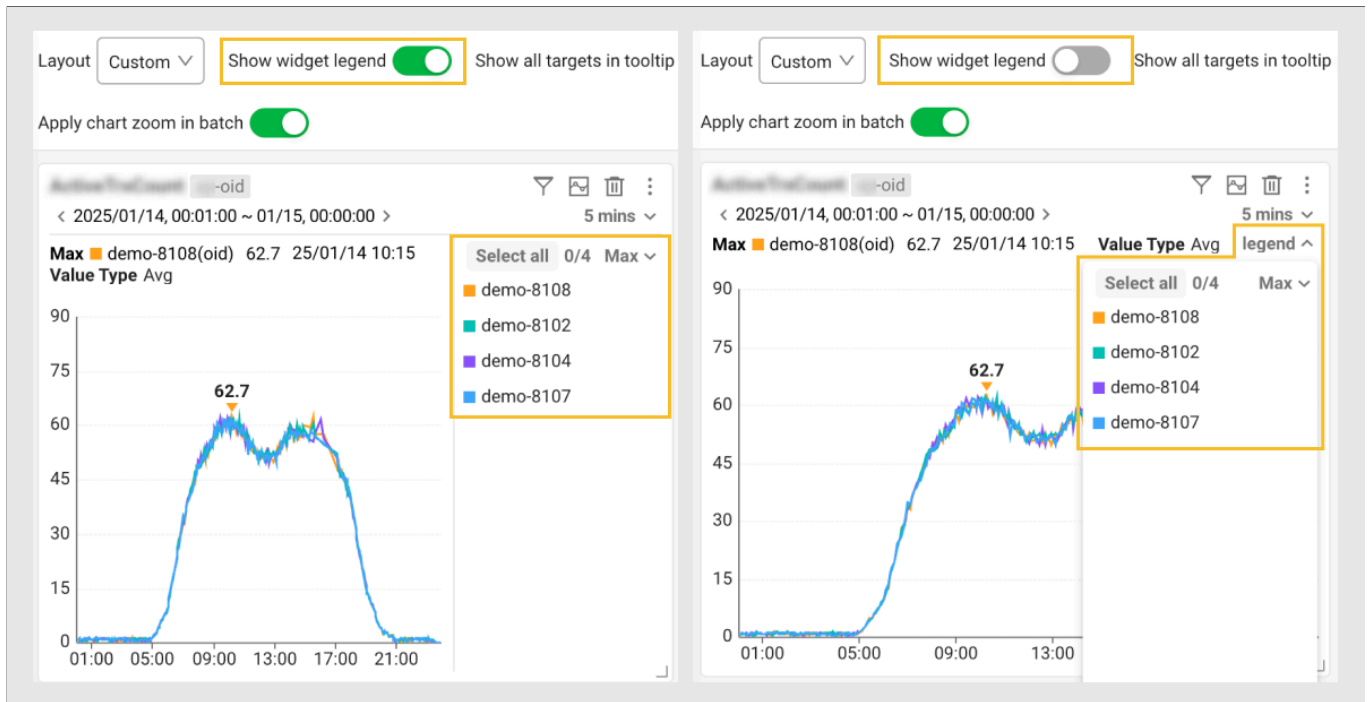


Removing the chart widget

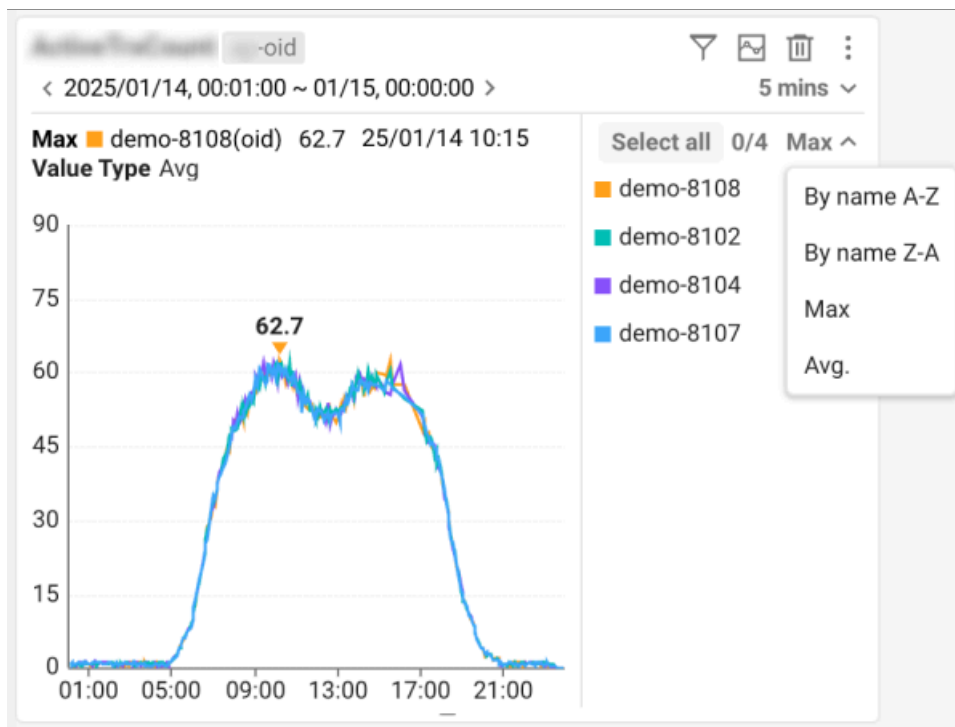
To remove any chart widgets placed on the screen, select .

Using the legend

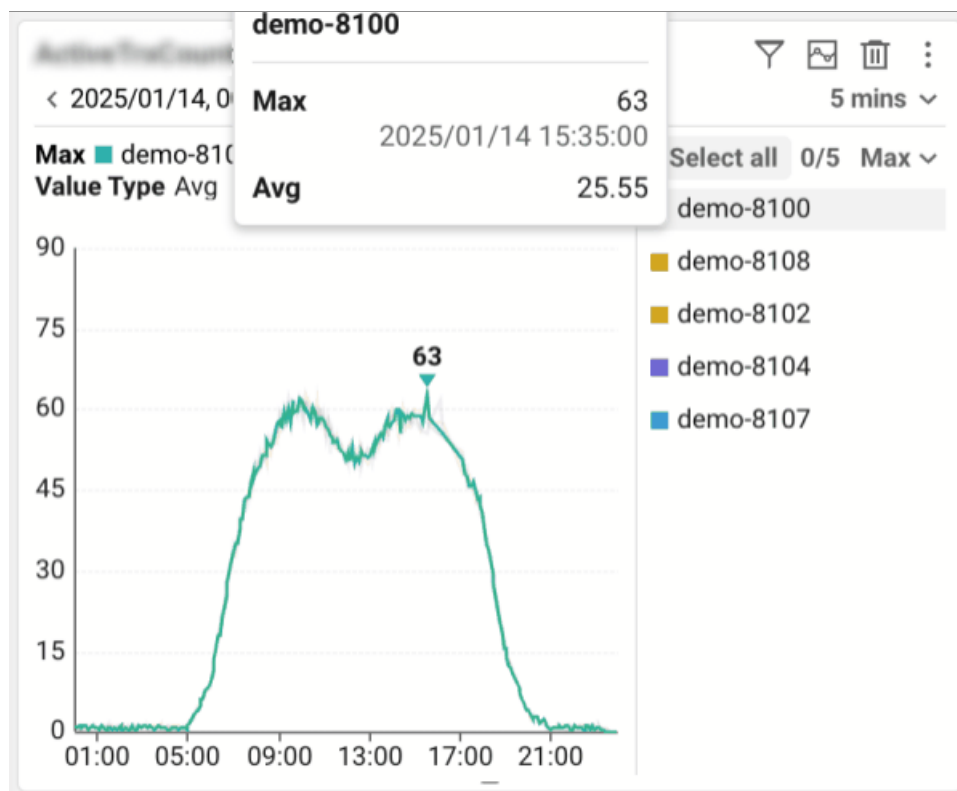
You can check the monitoring targets displayed on the chart through the legend and then sort or filter them by desired criteria. You can show or hide the legend on the right of the widget's chart by turning on or off the **Show widget legend** option at the top of the screen. With the option turned off, you can check and select the monitoring targets by clicking **legend**.



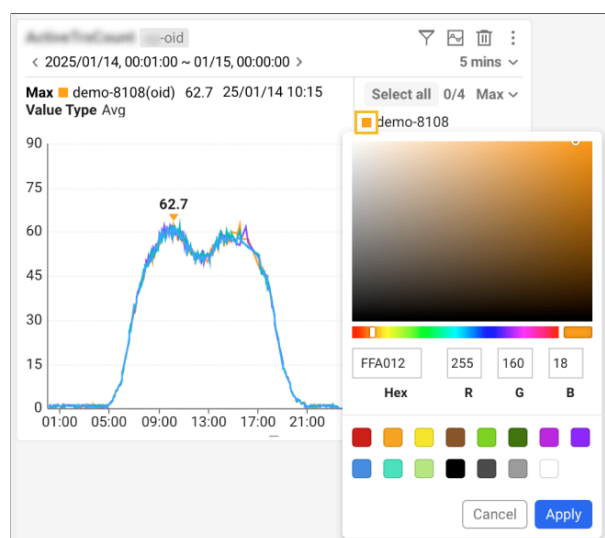
- You can select or unselect monitoring targets by selecting **Select all/Deselect all**.
- In the legend list, you can sort monitored objects by name, maximum value, or average value.



- If you hover the mouse over each item in the legend list, the highlighted graph for the monitoring targets appears and a tooltip indicating the specific time at which the maximum value is recorded. Alternatively, you can filter by selecting a target from the legend list.



Changing the legend color



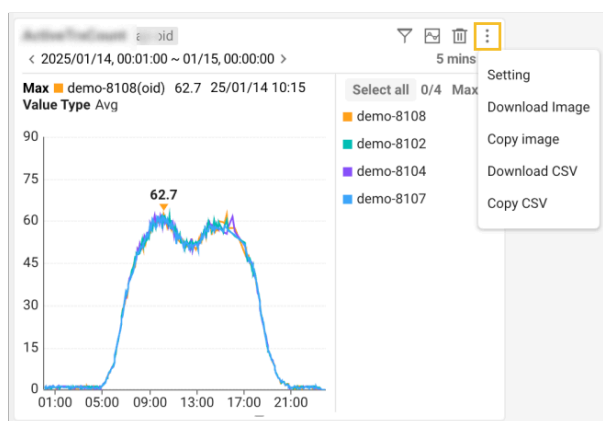
You can change the graph color corresponding to a monitoring target. In the legend list, select the square box

on the left of the target to change its color. Select a desired color and then click **Apply**.

! The set colors are not saved via the preset feature. This feature is to be provided in a future update.

Using additional options

If you select  on the upper right of the chart widget, you can select the following additional options.



- **Setting**
 - **Use Y axis automatically:** The size of the Y-axis can be automatically adjusted within the searched range.
 - **Show maximum value:** You can display the maximum value in the graph area of the chart.
- **Download Image:** You can download the chart as an image file.
- **Copy image:** You can copy the chart to the clipboard as an image format.
- **Download CSV:** You can download the data searched from the chart as a CSV file.
- **Copy CSV:** You can copy the data viewed in the chart to the clipboard in a CSV format.

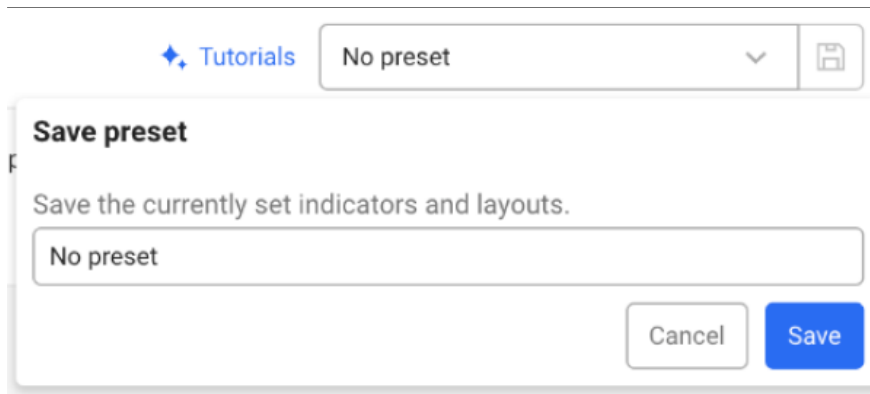
Setting presets

You can save and load the settings and layouts for widgets on the dashboard. You can create a new preset by adjusting its size and placing it on the desired position.

! You can save or modify the presets with the **Edit project** role. For more information about the member roles, see [the following](#).

Creating a new preset

1. Place the widgets in the desired format on the dashboard. You can also resize and place only the widgets to be frequently checked.
2. On the upper right of the screen, select .
3. Enter a new preset name.



4. Select **Save**.

You can see the newly saved preset from the preset list.

- ! • If any changes are made to the newly created preset, save the preset again. Select  and then save the preset with the same name. Any changes are overwritten in the existing preset.
- If you go to another menu without saving changes on the dashboard, the changes are not saved.
- Presets are saved on a project basis and can be shared with other users.
- The targets saved in the preset are the layout of the dashboard, the widgets placed on the dashboard, and the options (**Target**, **Interval**) modified in the widgets. The **Time** option at the top of the screen is not saved.
- To change the widget query time after loading a preset, use the **Batch Change** feature. For more information, see [the following](#).

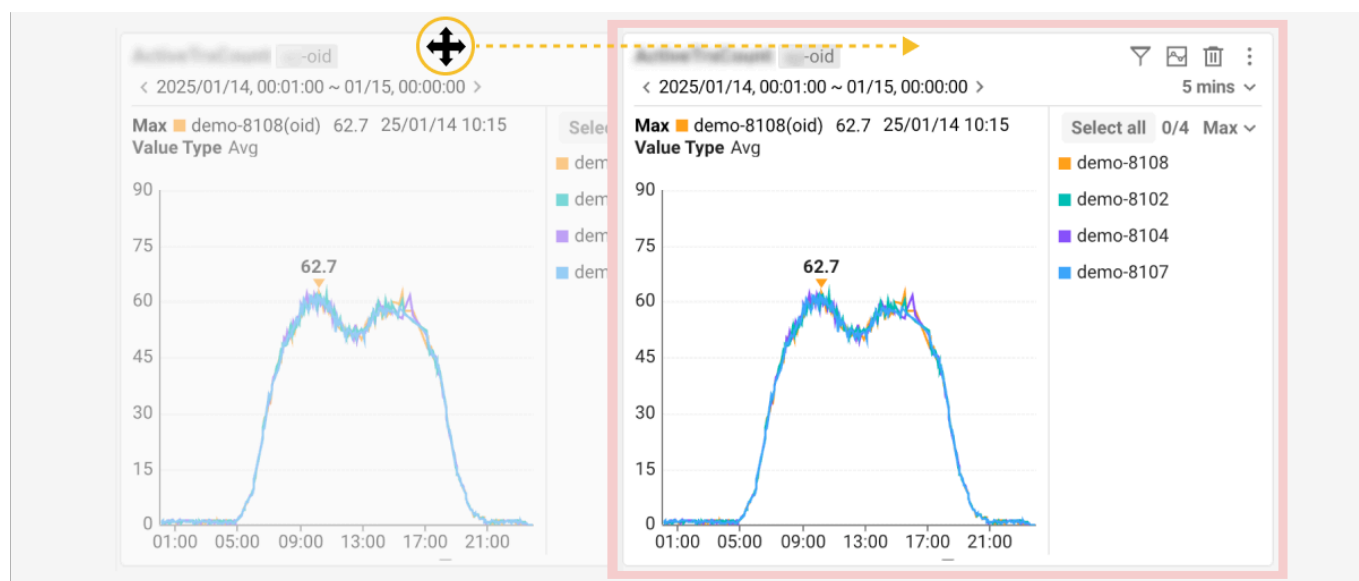
Deleting presets

If you have unused presets, you can delete them from the preset list. Select **×** on the right of the item to delete from the preset list.

Editing a dashboard widget

The widgets placed on the dashboard can be placed and resized to the user's desired location.

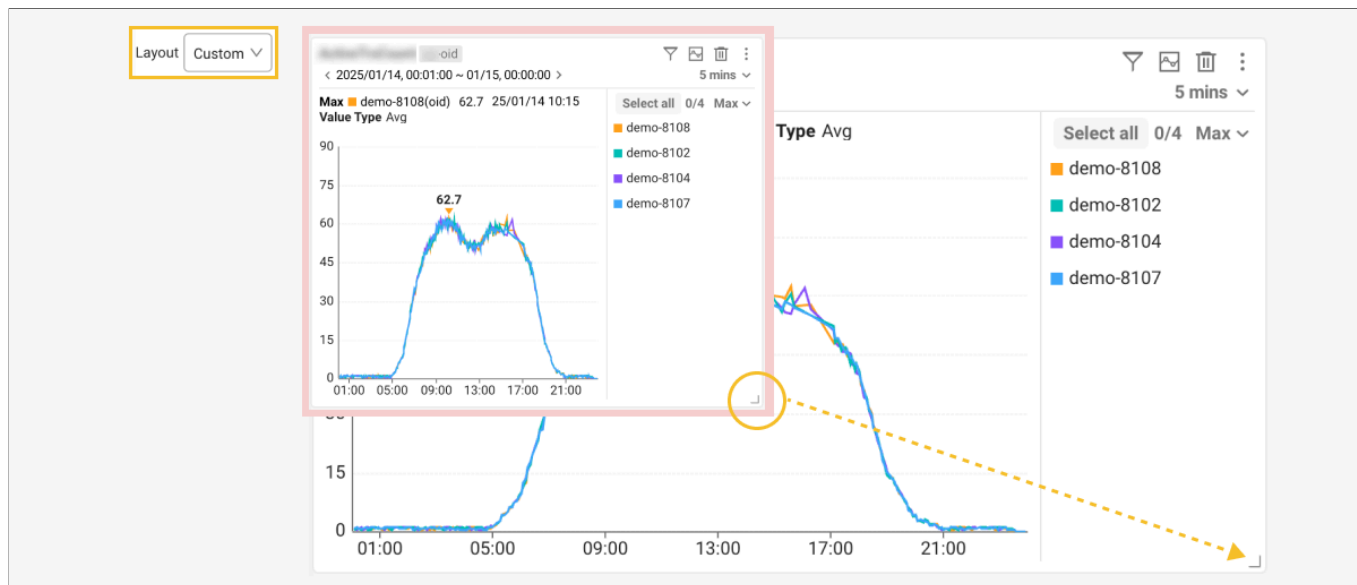
Moving a widget



When you move the top part of the widget by using the mouse pointer, it changes to the **+** shape. At this time, you can move the widget by dragging with your mouse to the desired position.

Resizing a widget

If **Layout** among the dashboard options is set to **Custom**, you can resize the widget.

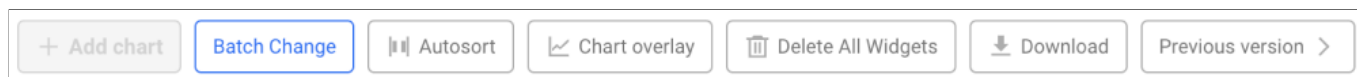


Click and hold the mouse on the  element at the lower right of the widget, and then drag it to the desired size.

ⓘ If **Layout** is not set to **Custom**, you can adjust only the height of the widget. Resize the widget with the bottom center of the widget clicked with your mouse.

Using the dashboard options

You can apply various settings to the chart widget at once using the Option menu located at the top of the screen. You can also customize the dashboard layout to your desired format.



Batch update of the chart widget options

It provides the feature to apply detailed options to the chart widgets on the screen at once. On the upper left of the screen, select **Batch Change**. If the **Batch Change** window appears, set the desired options and then select **Apply**.

- **Time:** You can set the data query range for the chart.

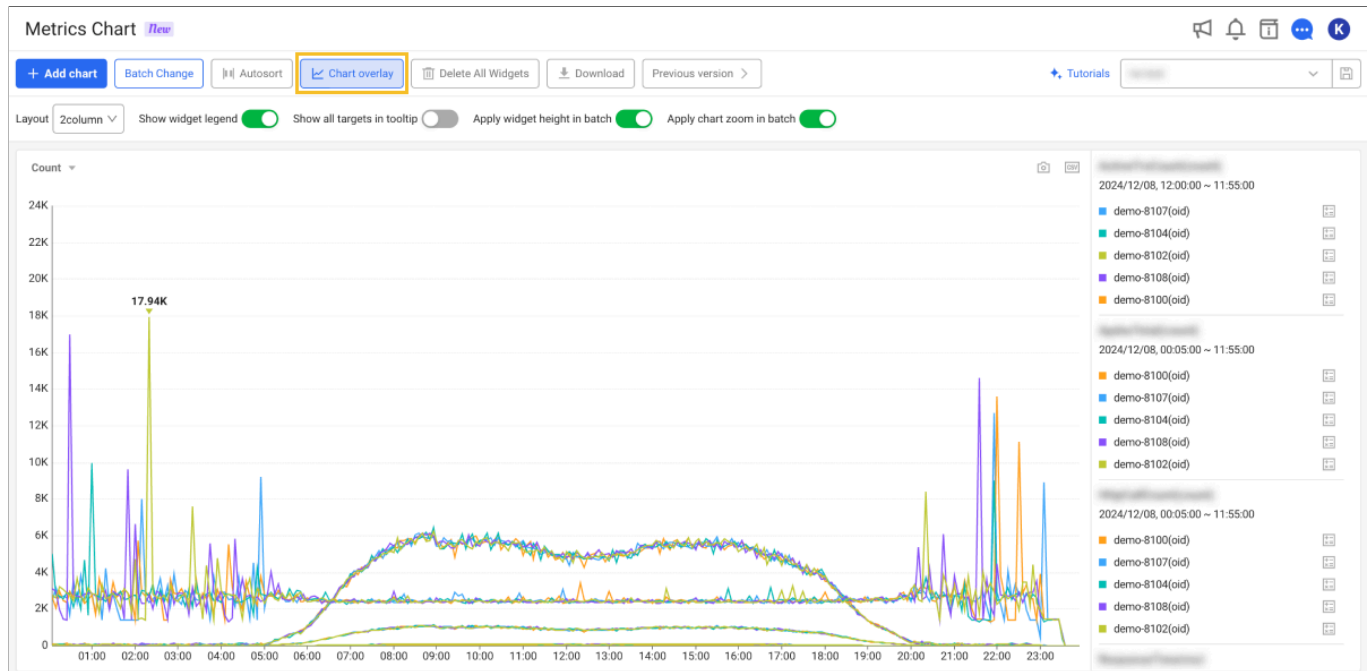
- **Target:** Select a monitoring target. You can select an individual agent or a group classified by the agent configuration.
 - **Agent:** You can select an individual agent or all agents.
 - **By kind:** Agents can be monitored in each group classified by `whatap.okind` in the agent configuration.
 - **By server:** Agents can be monitored in each group classified by `whatap.onode` in the agent configuration.
- **Interval:** You can adjust the data aggregation unit to various time intervals.
- **Apply widget:** Select a chart widget to apply the options to change. You can apply changed options to the selected widget at once.

Auto-aligning the dashboard

To auto-align the widgets placed on the dashboard, select **Autosort**. It auto-aligns widgets in order of their width and height, from smallest to largest. If the widths are the same, it aligns them in order of height, from smallest to largest.

Comparing multiple charts

This feature allows you to view data from multiple charts placed on the dashboard in a single chart. This feature allows you to compare multiple metrics from the same time period with others. Select **Chart overlay**. You can place overlay charts on the screen.



- If you select **Count** on the upper left of the overlay chart, a list appears where you can change the data criteria for the x-axis chart. You can compare the data of the chart by selecting a desired item.
- : You can download the chart as an image file based on the current view.
- : You can download the chart as a CSV file based on the current view.
- In the right section, you can see a list of agents for each metric. The colors of individual agents match the graph colors on the chart.

Batch deletion of placed widgets

You can delete multiple widgets placed on the dashboard all at once. Select **Delete All Widgets**. When the confirmation message appears, select **Delete**.

Downloading as a CSV file

You can download data from the widgets placed on the dashboard as a CSV file. Select **Download > Download CSV**. You can check the data of metrics for each time zone.

Downloading as an image file

You can download all the widgets placed on the dashboard as a single image file. Select **Download** > **Download Image**. You can save a captured image of the dashboard screen as is.

Using the previous version

To use the **Metrics Chart** menu of the previous version, select **Previous version**. Alternatively, you can see in the  **Sitemap** > **Analysis** > **Metrics Chart** **Old** path.

! For more information about **Metrics Chart Old**, see [the following](#).

Using other options

Other options below allow you to adjust the layout of the dashboard or easily and conveniently batch set the applied options to the widgets.

Layout 2column ▾
Show widget legend ☒
Show all targets in tooltip ☐
Apply widget height in batch ☒
Apply chart zoom in batch ☒

- **Layout:** You can set the number of columns in the dashboard (or the number of widgets that can be placed in a row). You can set up to 4 columns. If **Custom** is selected, widgets can be placed regardless of the number of columns.

! In **Custom**, you can freely adjust the width and height of the widget. If you select another option, you can only adjust the height of the widget.

- **Show widget legend:** Turning the option on or off shows or hides the legend on the right of the widget's chart. With the option turned off, you can check and select the monitoring targets by clicking **legend**. For more information about the use of legend, see [the following](#).
- **Show all targets in tooltip:** When you hover your mouse pointer over the chart, you can see the value for the point on the graph through a tooltip. Turn on the option to view data for all targets in the time zone where the mouse pointer is located through the tooltip.

- **Apply widget height in batch:** Enabling this option forces all widgets to have the same height.
- **Apply chart zoom in batch:** When changing the data query time of an individual chart widget, turn on this option to also change the chart times for other widgets.

Using the tutorial

When you select **Tutorials** on the upper right of the screen, you can check the changes after the [Service 2.8.0](#) update.

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.

Statistics/Reports

In the Statistics/Reports menu, you can gather data accumulated over a period of time to grasp trends in SQL execution and database size, and receive the operational status as periodic reports.

Screen Composition

Screen	Description
Top SQL	Analyze SQL that used a lot of resources based on execution count and time
Database Size	Check the growth trend of database capacity
Reports	Report service usage status and incident records on a daily, weekly, and monthly basis

Top SQL

Provides a list of Top SQL during the query period. These are SQL statistics for which WhaTap independently calculates metrics such as execution count and execution time, based on the SQL within active sessions collected by the agent. It helps you find high-load SQL and set tuning priorities.

The trend chart lets you visually grasp the SQL occurrence pattern for a specific time period, and statistics are calculated based on SQL with literal values excluded.

Basic Options

Set query conditions in the top filter area.

Item	Description
Time	Select the query time range
Cluster	Select the target cluster to query
Sort Order	Select the metric used as the basis for selecting Top SQL
Number of Results	Set the number of items to display in the table
Field / Filter	Narrow down the list by applying conditions on fields such as SQL Text

One point that can be confusing here is the top selector. MySQL Top SQL selects a target **instance**, but SingleStore Top SQL selects a target **cluster**. Since SingleStore processes SQL in a distributed manner at the cluster level, statistics are aggregated on a cluster basis.

Analysis Criteria Tabs

In the analysis criteria tabs, select the basis on which to group Top SQL.

Tab	Description
ALL	Check directly at the SQL level
DB	Analyze SQL load at the database level
USER	Analyze SQL load by user account
NODE	Analyze SQL load by node (<code>node_id</code>)

Top SQL Trends Chart

Displays the trend of the top SQL based on the selected metric as a time-series chart. You can see at a glance which SQL has a high load at which time period. Clicking the legend or the chart highlights the corresponding SQL line.

SQL List Table

Displays the list of Top SQL during the query period as a table.

Column	Description
SQL Text	The full SQL text (with literal values excluded)
SQL Hash Value	A hash value that groups identical SQL
User	Executing user
Execute Count	Execution count
Elapsed Time	Cumulative execution time
Avg Elapsed Time	Average execution time

Column	Description
Max Elapsed Time	Maximum execution time

Per-Query Charts

Click the expand button on a table item to view the execution count and average execution time charts for an individual query. Clicking a bar in the chart moves to the [Instance Monitoring](#) screen for that time period, where you can check the node status and active sessions at that point together.

SQL Details View

Clicking a SQL opens a detail popout. The popout consists of the following areas.

Area	Description
Query	The full SQL text
SQL Statistics	Statistics such as execution count and execution time
Elapsed Time Trends	Execution time trend
Plan	Execution plan

Plan (Execution Plan)

The Plan area shows the SQL's execution plan as a tree table. You can check the number of rows processed (Rows), node cost (Node Cost), and execution plans (Plans) at each stage step by step.

Simply put, an execution plan is the work plan the database lays out for the order in which it will process the SQL. By finding the high-cost stages, you can gauge where it takes a long time.

Data Interpretation Guide

Metric	Meaning	Interpretation
Execute Count	SQL call count	The higher it is, the more frequently it is called, so optimization has a greater effect
Elapsed Time	Cumulative execution time	The higher it is, the greater the overall load of the SQL
Avg Elapsed Time	Average execution time per call	The higher it is, the slower each execution, making it a priority tuning target
Max Elapsed Time	Maximum execution time	A large gap from the average suggests intermittent performance degradation

Database Size

On the Database Size screen, you can see how the capacity of each SingleStore database changes over time. Knowing in advance which database is growing quickly helps with capacity planning.

Default screen layout

At the top of the screen, select the cluster and the period to query. The default range is the last 7 days, and you can query up to 3 weeks.

Item	Description
Cluster selector	Select the target cluster to query
Period selector	Select the query period (default last 7 days, up to 3 weeks)
Data unit selector	Select the display unit (byte-based)
Download	Export in CSV or Excel format

Size trend chart

Displays the total capacity (TOTAL) and the capacity of each database as a line chart. The unit is automatically shown on a byte basis according to the data size.

Detail table

Displays the capacity metrics of each database in a table. For each metric, the start value, end value, and change over the query period are shown together so you can compare growth at a glance. The total (TOTAL) row is highlighted.

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.

Log

WhaTap's log monitoring has improved user convenience and accessibility based on the establishment of an integrated system. WhaTap supports the efficiency of the parser as well as Live Tail, explorer, searcher, and event notification that users mainly use through reliable data collection based on its own technology.

The **Log** menu provides functions such as lookup, analysis, and options setting. Through the **Event Configuration** menu, you can set the log-related event notifications.

- Home > Select Project > **Log**

Select a project on the initial screen of the WhaTap monitoring service, and then select **Log** under the project menu. By using the following functions, you can access complex logs more easily and then check and analyze them in real time under various conditions.

- **Live Tail**
- **Log Trend**
- **Log Search**

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

Select a project on the initial screen of the WhaTap monitoring service, and then select **Alert** under the Project menu to enter the **Event Configuration** menu. You can set event conditions and receive alerts through various routes such as email, SMS, messenger, and App Push.

The guide to the main menus of WhaTap log monitoring service is provided as follows.

Live Tail

It guides you to Live Tail of the log monitoring.

 Log Explorer

Guides you through the Log Explorer menu in Log Monitoring.

 Log Trend

It guides you to the Log Trend menu of Log Monitoring.

 Log setting

It explains how to set the log monitoring.

Live Tail

! Without the **Log Read** role, you cannot enter the menu.

Home > Select Project > **Log** > **Live Tail**

In the **Live Tail** menu, you can directly check the log data stream on the monitoring screen without connecting to the server console. Even with large volumes of complex logs, you can filter and quickly identify them using the **Filter** and **Highlight** features. The log data retrieval cycle is 2 seconds.

The major terms are as follows:

- **Category:** Unit for log collection and inquiry
- **Content:** Log messages
- **Search Key:** It is generated through the log parser settings.
- **Tag:** Key to search the collected logs

! You can change the column width by dragging an edge of the log table column.

Agent option

If the agent option is set, the log levels are collected and the colors for each log level appear as follows:

2023-12-18	14:31:02.563	level	INFO	pcode	2277	agenttime	1702877462042	oid	778873916	category	AppLog	loggerName	io.home.test.logback02starter.base.web.LogbackControllerGreeting
													INFO log in our greeting method.
2023-12-18	14:31:02.563	level	WARN	pcode	2277	agenttime	1702877462043	oid	778873916	category	AppLog	loggerName	io.home.test.logback02starter.base.web.LogbackControllerError
												threadName	http-nio-19090-exec-2
													io.home.test.logback02starter.base.errors.exception.ApiException: [2204] Process failure. Please try again.
2023-12-18	14:31:02.586	level	error	pcode	2277	agenttime	1702877462043	oid	778873916	category	AppServer	_event_status_	error
												_event_status_literal_name_	level
													Servlet.service() for servlet [dispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.error
2023-12-18	14:31:02.586	level	error	pcode	2277	agenttime	1702877462057	oid	778873916	category	AppServer	_event_status_	error
												_event_status_literal_name_	level
													Servlet.service() for servlet [dispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.error
2023-12-18	14:31:02.586	level	error	pcode	2277	agenttime	1702877462081	oid	778873916	category	AppServer	_event_status_	error
												_event_status_literal_name_	level
													Servlet.service() for servlet [dispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.error
2023-12-18	14:31:02.586	level	error	pcode	2277	agenttime	1702877462087	oid	778873916	category	AppServer	_event_status_	error
												_event_status_literal_name_	level
													Servlet.service() for servlet [dispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.error

! Setting the agent options



- The agent options are as follows:

```
# whatap.conf
weaving=log4j-2.17
weaving=logback-1.2.8
```

- In Java agent 2.2.22 or later, it can be used when setting log4j-2.17 or logback-1.2.8 in the weaving setting. It is required to restart the agent.
- The log level is determined based on the `level` and `type` among the parsed keywords. When there are keys parsed as `level` and `type`, and the parsed values have **FATAL**, **CRITICAL**, **ERROR**, **WARN**, **WARNING**, and **INFO**, the log level color appears.

1 Filter area

Apply Filter

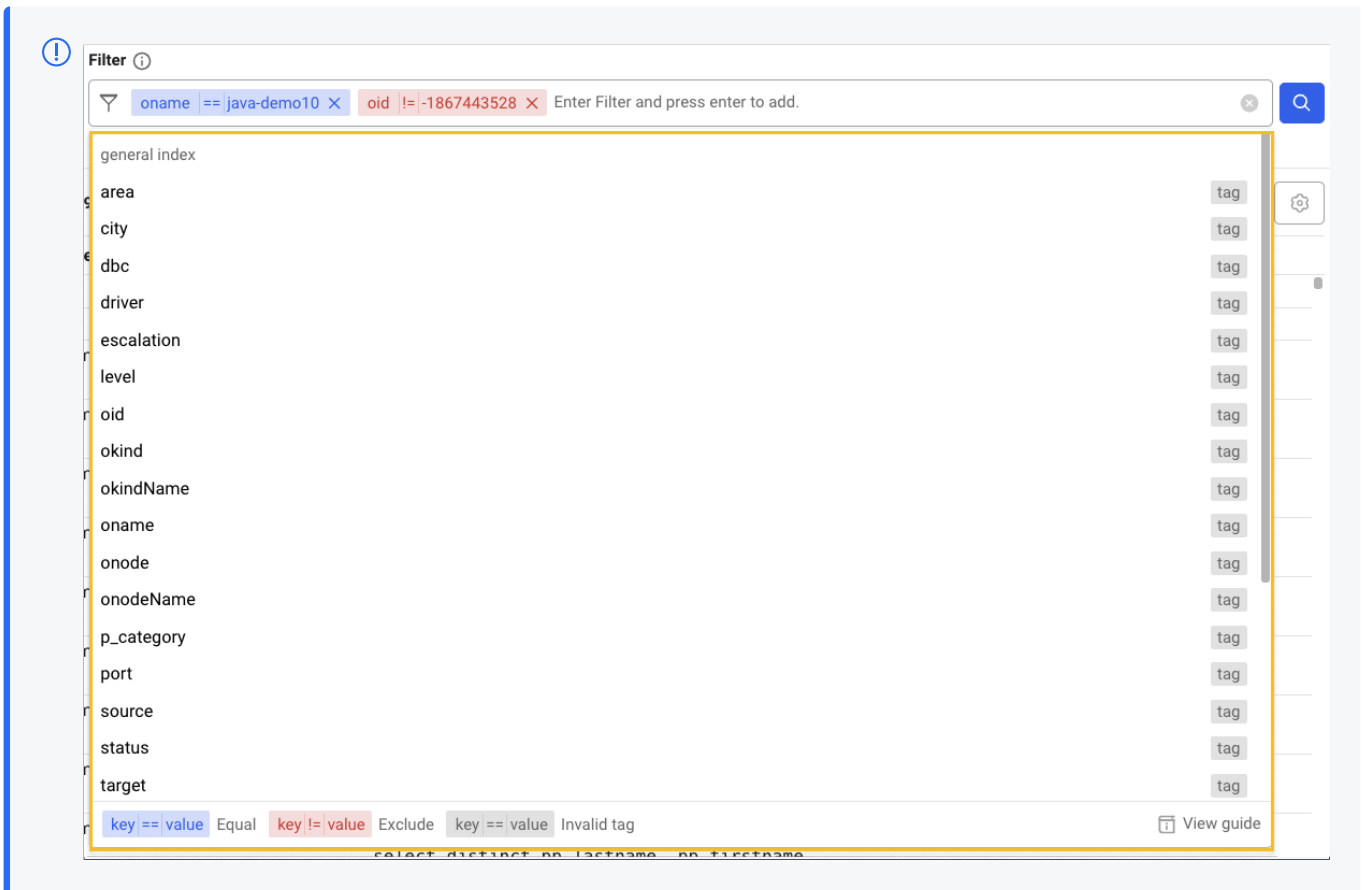
When a filter is applied, the logs that match the specified conditions are filtered. You can enter multiple filters. OR (`||`) if the filters have the same tags, otherwise AND (`&&`).

You can specify a filter by directly entering a value in the input field or clicking the **Filter** field. Filter tags are entered in the following order: `Search key`, `Operator`, and `Search value`. If you select  **Search**, the data with the filter applied can be viewed log list area.



Guide UI

The **Guide UI** is provided under the input field as follows: You can close the **Guide UI** via the ESC key when your mouse cursor is over the input field or filter tag.



Entry of the search key, operator, and search value

- Upon entry of the **search key**, recommended values are provided by distinguishing for general index, reserved word index, and numeric index.
- When entering an **operator**, for a general index search key, **==** and **!=** options are provided at the bottom. In case of the numeric index, the **>**, **<**, **<=**, **>=**, **==**, and **!=** options are provided.
- Upon entry of the **search value** for matched search (**>**, **<**, **<=**, **>=**, **==**), it is highlighted in **blue**. In case of excluded search (**!=**), it is highlighted in **red**. Upon entry of the **search value**, you can search using the case-sensitive option.

- If the filter tags exceed 2 lines, you can fold it by selecting the **^ Fold** icon.
- After entering a filter tag, you can use the Shift and Tab keys simultaneously in the input field to go to the previous filter tag.



- After entering a filter tag, you can use the Tab key in the input field to go to the next filter tag.

Adding filter tags

To add a filter tag, type the desired text in the input field and press **Enter** or **Tab**.

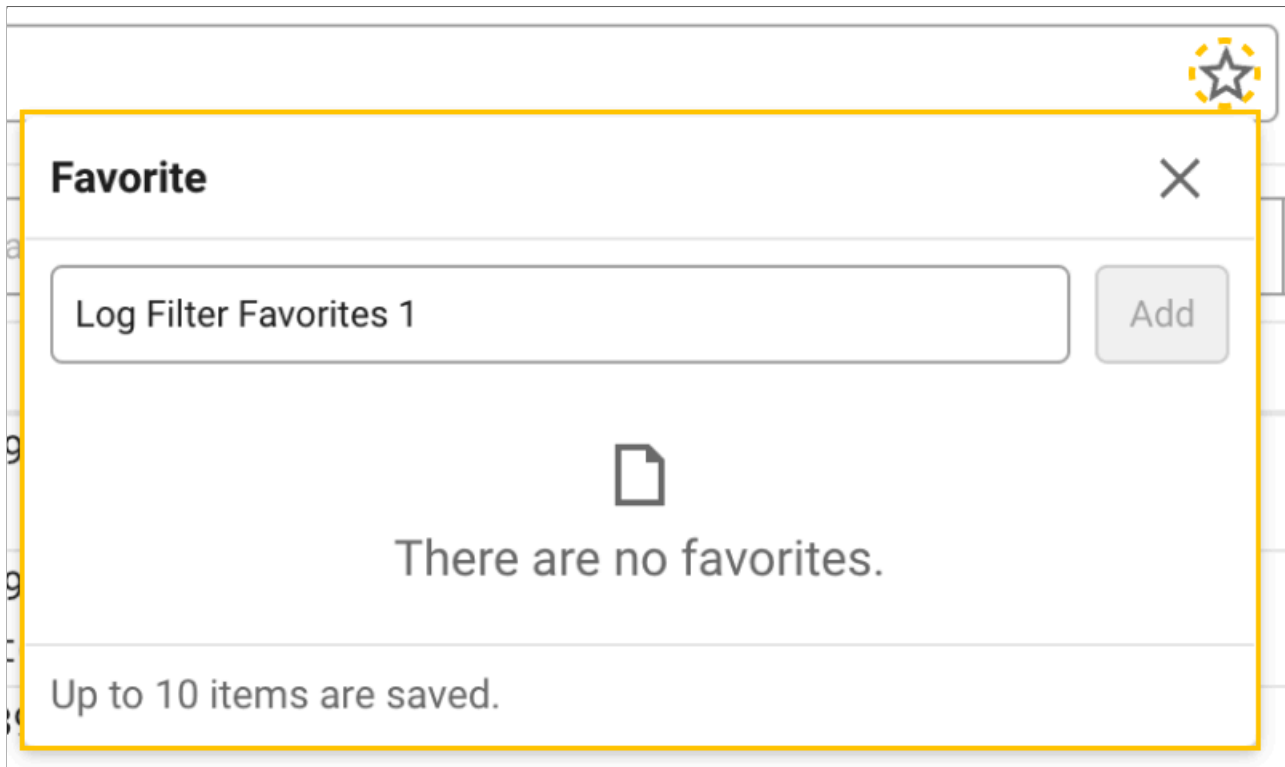
You can also select a recommended value from the **Guide UI** below the input field by clicking it or navigating with the arrow keys.

Deleting filter tags

To remove a single tag, press **Backspace** or click the **X** icon on the tag. To clear all tags at once, click the **X** icon located on the right side of the input field.

Filter favorites

The filter **favorites** feature is provided. You can select the ☆ **Favorites** icon on the right of the input window to **add**, **delete**, and select desired filter search conditions in the favorites. **Favorites** can store up to 50 cases.



Exceptional cases for application of filters

- In the tag with a numeric index (`search key` that ends with `.n`), only numbers can be input for the `search value` .
- Duplicate 'search key' and 'search value' cannot be entered.
- Searching is not possible if there is a tag whose `search key` or `search value` is missing. Invalid tags appear in gray.

ⓘ You cannot enter a `category` with the **Live Tail** `search key` .
The expression under the entered filter value is a preview of the filter expression for querying the log data.

Applying non-parsing keyword filters

You can search the logs containing keywords that have not been parsed, or for which no index has been created.

In this case, all logs in the specified range are fully scanned. Therefore, the search speed may be slower compared to the indexed key. For standardized log data, it is recommended to search using the index key through **Log parser setting**.

Filter ⓘ

🔍
oid != -1009464250 ✕
okind == -398596773 ✕
content == *select* ✕
Enter Filter and press enter to add.
✕

oid != -1009464250 && okind == -398596773 && content == *select*

1. Select **Category**.
2. In the **Filter** field, enter a desired keyword for a search after leaving spaces on the **content** basis.
e.g. `content *select*`
3. Click 🔍 **Search** to view the logs.

- ⓘ • In case of **Live Tail**, all logs can be viewed. Thus, the category is not required to be specified.
- For more information about the parser configuration, see [the following](#).

Modifying the filter

Enter a value in the filter and then click the specified value to modify it.

Filter ⓘ

oname == ote-account X key == aws.base.index X appender != fileAppender X Enter Filter and press enter to add. X

☐ Case Sensitive

fileAppender

searchValue*	Search logs starting with the search value. ex key!=searchValue*
*searchValue	Search logs ending with the search value. ex key!=*searchValue
searchValue	Search logs containing the search values. ex key!=*searchValue*
*search*Value*	Search logs containing the search values. ex key!=*search*Value*
re:searchValue	Search logs that match official expressions. ex key!=re:searchValue
**	Search all logs matching the search key. ex key!=**

key == value Equal key != value Exclude key == value Invalid tag View guide

- You can modify the filter by entering text again in the input field.
- You can modify the recommended values by selecting them in the **Guide UI** below the input field.

Search Key

In the following image, the blue boxed part is the search key for parsing. In **Log Configuration**, you can register and set the parsing logic in **Log parser setting** tab with the search key.

Search key

Filter input syntax

A tag consists of a search key and a search value. In the following example, the search key is `exception` and the search value is `UnknownHostException`. The example searches for the log data that includes an exception (`UnknownHostException`) that is generated when the server cannot connect the host because the IP address and domain address do not match among the collected log data.

exception == UnknownHostException X

Search key types

Search key types	Search key format	Meaning	Example for Search key and search value	Search example
String keyword	keyword	File Name	- Key: fileName - Value: /data/whatap/logs/yard.log	fileName:/data/whatap/logs/yard.log
Numeric keyword	keyword.n	Response Time	- Key: response_time.n - Value: 2945	response_time.n>=2945
Reserved keyword (predefined keyword)	@keyword	Transaction ID	- Key: @txid - Value: 85459614215434144	-
Log body's keyword	content	Log body	- Key: content - Value: user input	content: *ERROR*

ⓘ Content search key

- The content search key searches the bodies of unindexed logs. For example, if you enter `content *ERROR*`, the logs containing `ERROR` are searched among the log bodies.
- If you do not know which keywords need to be used for indexing, use the content search keys to identify the logs containing problematic keywords. Afterwards, you can improve the search performance by setting a parser with the keyword through the log parser settings in **Log Configuration** and creating indexes.

Common syntaxes

Syntax type	Description	Example
<code>==searchValue</code>	Searches for the logs that match the search value.	<code>exception==RuntimeExceptionexception</code>

Syntax type	Description	Example
<code>!=searchValue</code>	Searches for the logs that exclude the search value.	<code>exception!=RuntimeException</code>
<code>*searchValue</code>	Searches for the logs ending with the search value.	<code>word==*hello</code>
<code>searchValue*</code>	Searches for the logs starting with the search value.	<code>word==hello*</code>
<code>*searchValue*</code>	Searches for the logs that contain the search value in the middle.	<code>word==*hello*</code>
<code>*search*Value*</code>	Searches for the logs that contain the search value.	<code>word==*he*llo*</code>
<code>re:{regex}</code>	Searches for the logs that match a regular expression.	<code>caller==re:^(i\.w\.a\.w\.s\.v\.r\.</code>
<code>**</code>	Searches all logs that match the search key.	

Syntax in case the search key has a numeric value (keyword.n)

The following syntax is supported only when the search key is in `keyword.n` format.

- Search values must only be numbers.
- No prefix is attached to the value of the `.n` keyword. All keywords other than `.n` must be attached with a prefix.

For example, `+>searchValue` is invalid.

Syntax type	Description	Example
<code>>searchValue</code>	Searches for the logs containing values greater than the search value.	<code>response_time.n>3000</code>

Syntax type	Description	Example
<code>>=searchValue</code>	Searches for the logs containing values greater than or equal to the search value.	<code>response_time.n>=3000</code>
<code>==searchValue</code>	Searches for the logs containing the same search value.	<code>response_time.n==3000</code>
<code>!=searchValue</code>	Searches for the logs that contain values different from the search value.	<code>response_time.n!=3000</code>
<code><searchValue</code>	Searches for the logs containing values less than the search value.	<code>response_time.n<3000</code>
<code><=searchValue</code>	Searches for the logs containing values less than or equal to the search value.	<code>response_time.n<=3000</code>

Viewing personal information

If you have the **log personal information query** role, you can display de-identified personal information by enabling the **Display personal information**  toggle button.

- For more information about the **log personal information query** role, see [the following](#).
- For more information about **De-identification of personal information**, see [the following](#).

2 Content highlight area

The highlight function allows you to easily identify desired keywords in log content. You can filter with single or multiple keywords.

Live Tail

Category: ApplLog Filter: content == *select* Enter Filter and press enter to add.

select

▶	oname	Timestamp	Log
▶	demo-8105	2023-11-24 14:08:35.620	@txid 5935183317842444630 pcode 5490 oname demo-8105 onodeName node-1 oid -857948929 okindName demo-okind-1 okind -628198688 select
▶	demo-8105	2023-11-24 14:08:35.624	@txid 4922255873619405363 pcode 5490 oname demo-8105 onodeName node-1 oid -857948929 okindName demo-okind-1 okind -628198688 select productmodelid, avg(listprice) as [average list price]
▶	demo-8105	2023-11-24 14:08:35.630	@txid 4922255873619405363 pcode 5490 oname demo-8105 onodeName node-1 oid -857948929 okindName demo-okind-1 okind -628198688 select productid, avg(unitprice) as [average price]
▶	demo-8105	2023-11-24 14:08:35.635	@txid 4922255873619405363 pcode 5490 oname demo-8105 onodeName node-1 oid -857948929 okindName demo-okind-1 okind -628198688 select

- Enter the keyword you want to highlight in the keyword input field.
 - Example: `select`
- The searched keyword will be highlighted in the Content of the log list.
 - If you click the  **Log full screen** icon, you can view **Log** and **Timestamp** in fullscreen.
 - You can navigate between highlighted keywords using shortcuts.
 - `Enter` : Move to the next row
 - `Shift+Enter` : Move to the previous row
 - `^` / `↓` icons: Move between rows
 - `Cmd + F` (Mac) / `Ctrl + F` (Windows): Search keywords

Multi-keyword condition

When highlighting with multiple keywords, write as follows:

String to input	Description	Result
a b c	Separate each keyword with a space.	a, b, c
"Whatap is good."	To include spaces in keywords, wrap them in <code>'</code> or <code>"</code> .	Whatap is good.
"Whatap\\ is good."	If <code>\</code> is included in the keyword surrounded by <code>"</code> , enter it as <code>\\</code> .	Whatap\ is good.

Setting the highlight color

By selecting  **Highlight**, you can set the keyword and its color for highlighting.

- In addition, enter the keyword to set the color for.
- If you click **Color** on the left of the input field, available colors appear.
- Basically, different highlighting by the level (**WARN**, **ERROR**, **FATAL**) is applied.
- The settings are saved in **Project Rules**.

Table settings

Column settings

Right of the  area, select  **Column settings**. You can add columns or set order.

- **Adding columns**

You can add columns to the table by selecting tags. If you unselect the **log** column, you cannot see **Log view detail setting**. Be sure to select at least one column.

- **Setting the column order**

When you add a column, the column is added to **Display columns**. Drag a desired column to change the order of the columns.

Log view detail setting

On the right of , select  **Log view detail setting**. **content** and **Tag** are all checked and two items are also displayed. Be sure to select any of **content** and **Tag**.

Unchecked items are not displayed in the table. If you deselect the **Tag** as follows, the log's **Tag** does not appear in the table.

Log table tag invisible

When you add tags in the **Tag management** list, the tags in the log are listed in the order you added. You can change the order of the tags by dragging them. If you disable an added tag, the disabled tag does not appear.

- **Column settings** and **Log view detail setting** can be used in **Live Tail**, **Log Search**, and **Log Trend**.
- In the same project, the **Live Tail**, **Log Search**, and **Log Trend** menus share **Column settings** and **Log view detail setting**.

Log Explorer

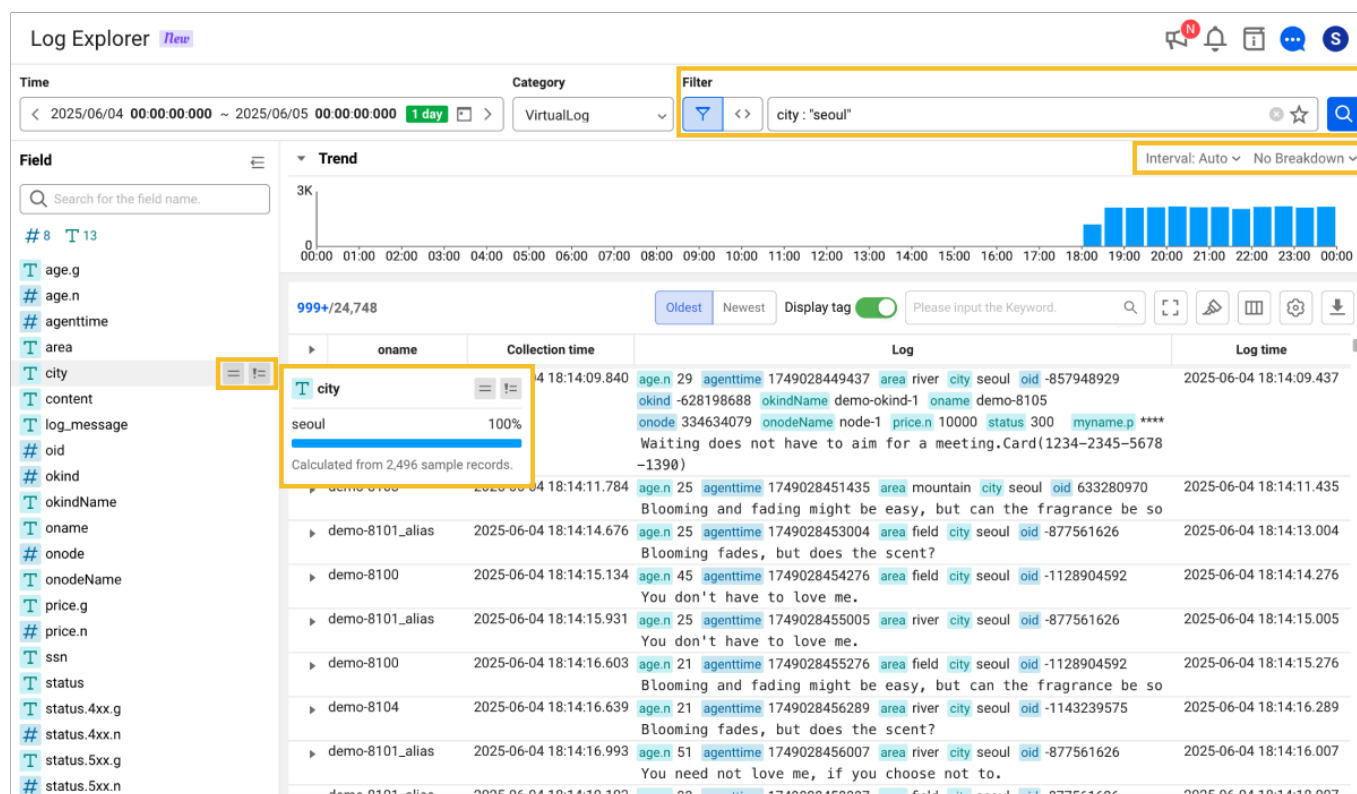
ⓘ Without the **Log Read** role, you cannot enter the menu.

Home screen > Select Project > **Log** > **Log Explorer** *New*

The **Log Explorer** feature allows you to quickly search, filter, and analyze log data. You can understand the field structure, perform query-based filtering to efficiently search for logs, and visualize the results. This feature is based on the Lucene index and offers the following key functions:

1. **Log trend analysis and search:** Enables both log trend visualization and search, helping you understand log patterns over time.
2. **Fast search and filtering:** Search for problematic logs quickly using simple keywords. Supports both WhaTap log search query and Lucene query syntax for defining various search conditions.
3. **Autocomplete functionality:** Helps users write and learn queries easily through auto-suggestions.
4. **Data visualization:** Uses stacked graphs to visualize the volume of logs over time. Drill-down capability allows deep analysis of specific logs.
5. **Favorites and sharing:** Save frequently used filters as favorites and share them easily via URL.

Basic Screen Overview



Time Range Selection

Set the time range for the log search using the **Time Selector** in the top option bar.

Category

Select the type of log you want to explore in **Select Category** on the top option bar (e.g., AppLog).

Filter

In the **Filter** on the top option bar, select the query language and enter the search conditions to apply the filter. The search query syntax supports both WhaTap Log Search Query and Lucene Query.

-  : WhaTap Log Search Query
-  : Lucene Query

Search Query Syntax

WhaTap log search query

WhaTap log search queries support autocomplete and allow quick log searches with simple keyword input. You can define various search conditions using operators like `and` , `or` , etc.

- Example: Entering `error` in the search filter will search within the log content.
 1. In the top option bar, click the filter icon and select a field from the query search box (fields are shown based on selected time and category).
 2. Choose an operator:
 - a. Default: `:` , `.*` , `and` , `or`
 - b. If the field is of type `Number` : Default + `<=` , `>=` , `<` , `>`
 - c. If the field is of type `String` : Default only
 3. Select a value (values shown based on selected time, category, and field).

Search Index Field Types

Only three field types are supported: `Number` , `String` , and `Boolean` .

- `Number` : Numeric values like long, double, float
- `String` : Full text such as email body
- `Boolean` : A value of either True or False

 For more details about WhaTap log search query syntax, refer to the [documentation](#).

Lucene

Use the standard syntax of Apache Lucene version 8.11.1. Autocomplete is not supported.

 For more information on the Lucene QueryParser Classic package, see the [official documentation](#).

Field List

Can be used for drill-down analysis.

Apply Field Info to Filter

Check field names in the **Field List** and click the **=** or **!=** buttons to apply them as filter conditions.

- Hovering over a field shows the **=** and **!=** buttons, which can be clicked to apply filters.
- Use the field search function to quickly find the desired field.

Trend Chart

Use **Trend Chart** to view logs in graph form with **interval** and **breakdown** applied.

- **Graph Interaction:** Zoom in using mouse drag or the  button, and click bars to view logs in that area
- **Interval:** Choose from Auto, 1s, 5s, 30s, 1m, 5m, 10m, 30m, 1h
- **Breakdown:** Visualize distribution of Top 3 values + Others for a specific field, and apply drill-down filters

Breakdown

Breakdown is a visualization feature that analyzes log count trends by a specific field.

- Displays a stacked graph separating the Top 3 values and Others for a given field
- Useful for drill-down analysis. You can click parts of the legend or stacked graph to highlight specific values or add filter conditions.

View Logs

You can view logs that match your search conditions. In the **Field List**, field data and log tags are displayed in matching highlight colors.

Content Highlight

The highlight function allows you to easily identify desired keywords in log content. You can filter with single or multiple keywords.

1. Enter the keyword you want to highlight in the keyword input field.
 - Example: `select`
2. The searched keyword will be highlighted in the Content of the log list.
 - If you click the  **Log full screen** icon, you can view **Log** and **Timestamp** in fullscreen.
 - You can navigate between highlighted keywords using shortcuts.
 - `Enter` : Move to the next row
 - `Shift+Enter` : Move to the previous row
 - `^` / `↓` icons: Move between rows
 - `Cmd + F` (Mac) / `Ctrl + F` (Windows): Search keywords

Multi-keyword condition

When highlighting with multiple keywords, write as follows:

String to input	Description	Result
<code>a b c</code>	Separate each keyword with a space.	a, b, c
<code>"Whatap is good."</code>	To include spaces in keywords, wrap them in <code>'</code> or <code>""</code> .	Whatap is good.
<code>"Whatap\\ is good."</code>	If <code>\</code> is included in the keyword surrounded by <code>""</code> , enter it as <code>\\</code> .	Whatap\ is good.

Setting the highlight color

By selecting  **Highlight**, you can set the keyword and its color for highlighting.

- In addition, enter the keyword to set the color for.
- If you click **Color** on the left of the input field, available colors appear.
- Basically, different highlighting by the level (**WARN**, **ERROR**, **FATAL**) is applied.
- The settings are saved in **Project Rules**.

Column settings

Click the  button to add columns or change their order.

- **Add Columns**

In **Column Settings**, select tags to add them as columns in the table.

 If no log columns are selected, **Log view detail setting** will not be visible. At least one column must be selected.

- **Reorder Columns**

Added columns will appear in **Display columns**. Drag them to change the display order.

Log view detail setting

Click the  button to configure log display options. By default, both **content** and **Tag** are selected and shown.

- Either **content** or **Tag** must be selected.
- Tags added in **Tag management** appear in order in the log display. You can reorder tags by dragging. Disabled tags are not shown.
- If an item is unchecked, it is not shown in the table. For example, if **Tag** is unchecked, log tags are not displayed.

log table contents remove tag sc

! Scope of Column and Log Display Settings

- **Column settings** and **Log view detail setting** can be used in **Live Tail**, **Log Search**, and **Log Trend**.
- In the same project, **Live Tail**, **Log Search**, and **Log Trend** share **Column settings** and **Log view detail setting**.

Download Log File

You can download the collected logs that match your search results in [CSV](#) or [TXT](#) file formats.

1. Click the  **Download** button at the right center of the screen.
2. Click **Download CSV** or **Download Log** to download the file in your preferred format.

Log Trend

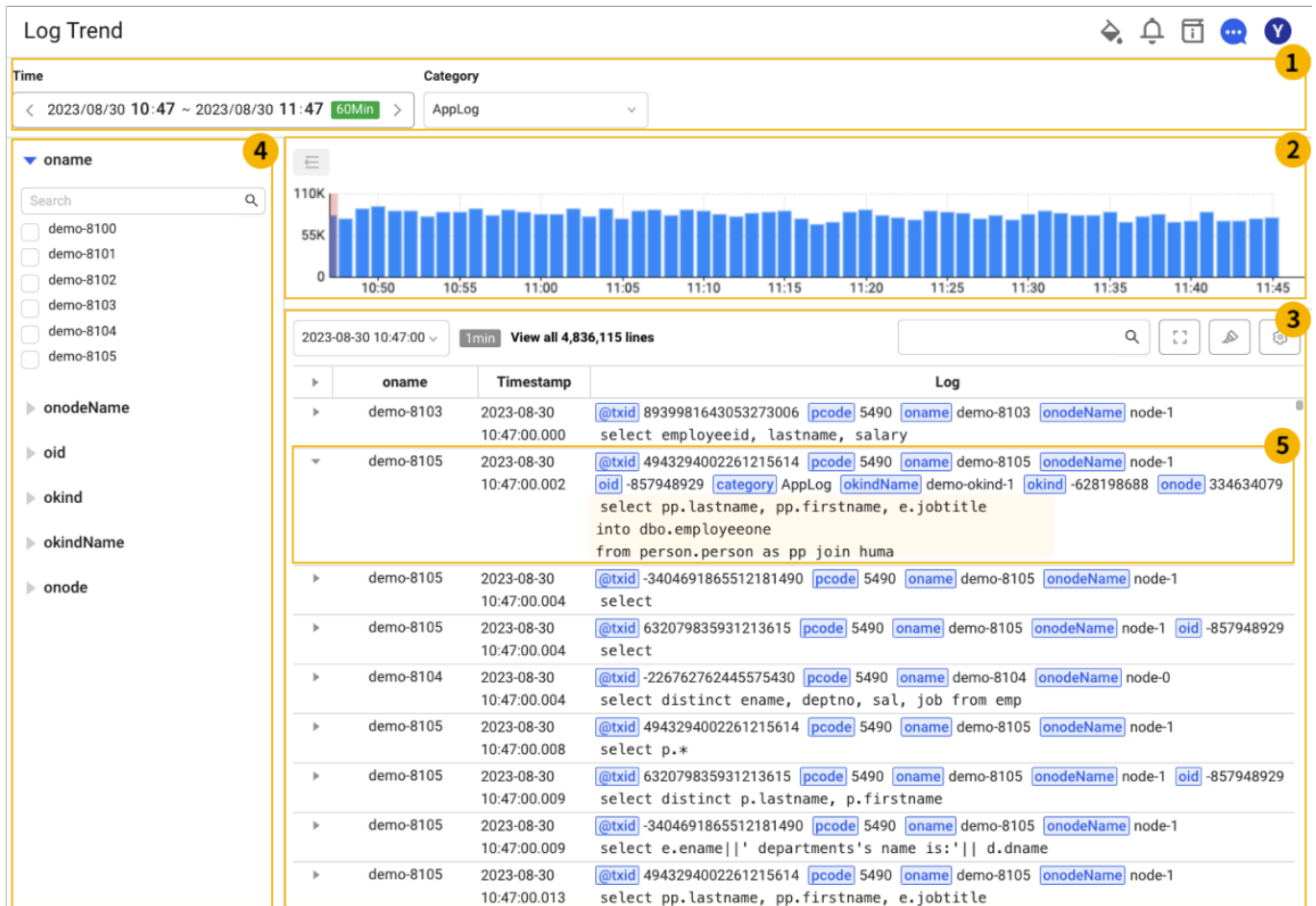
ⓘ Without the **Log Read** role, you cannot enter the menu.

Home > Select Project > **Log** > **Log Trend**

In **Log Trend**, you can check the occurrence pattern of a specific error type through the occurrence count trend of the logs classified by type and see the log data details by time. You can quickly see the desired log through the highlighting feature. You can also check the trends of the collected logs by category.

The major terms are as follows:

- **Category:** Unit for log collection and inquiry
- **Content:** Log messages
- **Search Key:** It is generated through the log parser settings.
- **Tag:** Key to search the collected logs



Request Data

- If the scroll reaches the bottom, the next data is retrieved.
- In 1, specify the **time** and collection unit, **category**, of the log data to be searched.
- If the **category** is changed, the logs that correspond to the selected category are searched. You can see the logs in 2 bar chart and 3 log table.
- If you click a bar in 2 bar chart, the logs are viewed that correspond to the time range of the bar.
- 3 You can see the total number of logs viewed from the upper left of the log table.
- On the upper right of the 3 log table, select the  **full screen** icon, you can see the **log** and **collection time** in the full screen.

- **4** In Side menu, you can see the logs filtered by tags. Up to two search keys can be selected, and multiple search values can be selected.
- If the agent option is set, the log levels are collected and the colors for each log level appear as follows:

2023-12-18 14:31:02.563	level	INFO	pcode	2277	agenttime	1702877462042	oid	778873916	category	AppLog	loggerName	io.home.test.logback02starter.base.web.LogbackControllerGreeting
												INFO log in our greeting method.
2023-12-18 14:31:02.563	level	WARN	pcode	2277	agenttime	1702877462043	oid	778873916	category	AppLog	loggerName	io.home.test.logback02starter.base.web.LogbackControllerError
											threadName	http-nio-19090-exec-2
												io.home.test.logback02starter.base.errors.exception.ApiException: [2204] Process failure. Please try again.
2023-12-18 14:31:02.586	level	error	pcode	2277	agenttime	1702877462043	oid	778873916	category	AppServer	event_status	error
											event_status_literal_name	level
												Servlet.service() for servlet [DispatcherServlet] in context with path [/] threw exception [Request processing failed: io.home.test.logback02starter.base.err
2023-12-18 14:31:02.586	level	error	pcode	2277	agenttime	1702877462057	oid	778873916	category	AppServer	event_status	error
											event_status_literal_name	level
												Servlet.service() for servlet [DispatcherServlet] in context with path [/] threw exception [Request processing failed: io.home.test.logback02starter.base.err
2023-12-18 14:31:02.586	level	error	pcode	2277	agenttime	1702877462081	oid	778873916	category	AppServer	event_status	error
											event_status_literal_name	level
												Servlet.service() for servlet [DispatcherServlet] in context with path [/] threw exception [Request processing failed: io.home.test.logback02starter.base.err
2023-12-18 14:31:02.586	level	error	pcode	2277	agenttime	1702877462087	oid	778873916	category	AppServer	event_status	error
											event_status_literal_name	level
												Servlet.service() for servlet [DispatcherServlet] in context with path [/] threw exception [Request processing failed: io.home.test.logback02starter.base.err

① Setting the agent options

- The agent options are as follows:

```
# whatap.conf
weaving=log4j-2.17
weaving=logback-1.2.8
```

- In Java agent 2.2.22 or later, it can be used when setting log4j-2.17 or logback-1.2.8 in the weaving setting. It is required to restart the agent.
- The log level is determined based on the `level` and `type` among the parsed keywords. When there are keys parsed as `level` and `type`, and the parsed values have **FATAL**, **CRITICAL**, **ERROR**, **WARN**, **WARNING**, and **INFO**, the log level color appears.

- ① You can change the column width by dragging an edge of the log table column.

Viewing personal information

If you have the **log personal information query** role, you can display de-identified personal information by enabling the **Display personal information**  toggle button.

- For more information about the **log personal information query** role, see [the following](#).
- For more information about **De-identification of personal information**, see [the following](#).

Checking the log content

! What is content?

Content means the log messages.

- The first line of the log column is the log's parsed key and value, and the second line is the log's content.
- 3 For each row (log) of the log table, the ▶ **More** button exists. If you select the ▶ **More** button, you can check the entire content of the log like 5.

Configure Highlight

- The highlight function is provided to easily identify the desired keywords.
- 3 In the [input field](#) on the right, enter the keyword to highlight. You can check the highlighted keywords like this.

Content Highlight

The highlight function allows you to easily identify desired keywords in log content. You can filter with single or multiple keywords.

1. Enter the keyword you want to highlight in the keyword input field.
 - Example: `select`
2. The searched keyword will be highlighted in the Content of the log list.
 - If you click the [] **Log full screen** icon, you can view **Log** and **Timestamp** in fullscreen.
 - You can navigate between highlighted keywords using shortcuts.
 - `Enter` : Move to the next row
 - `Shift+Enter` : Move to the previous row
 - `^ / v` icons: Move between rows
 - `Cmd + F` (Mac) / `Ctrl + F` (Windows): Search keywords

Multi-keyword condition

When highlighting with multiple keywords, write as follows:

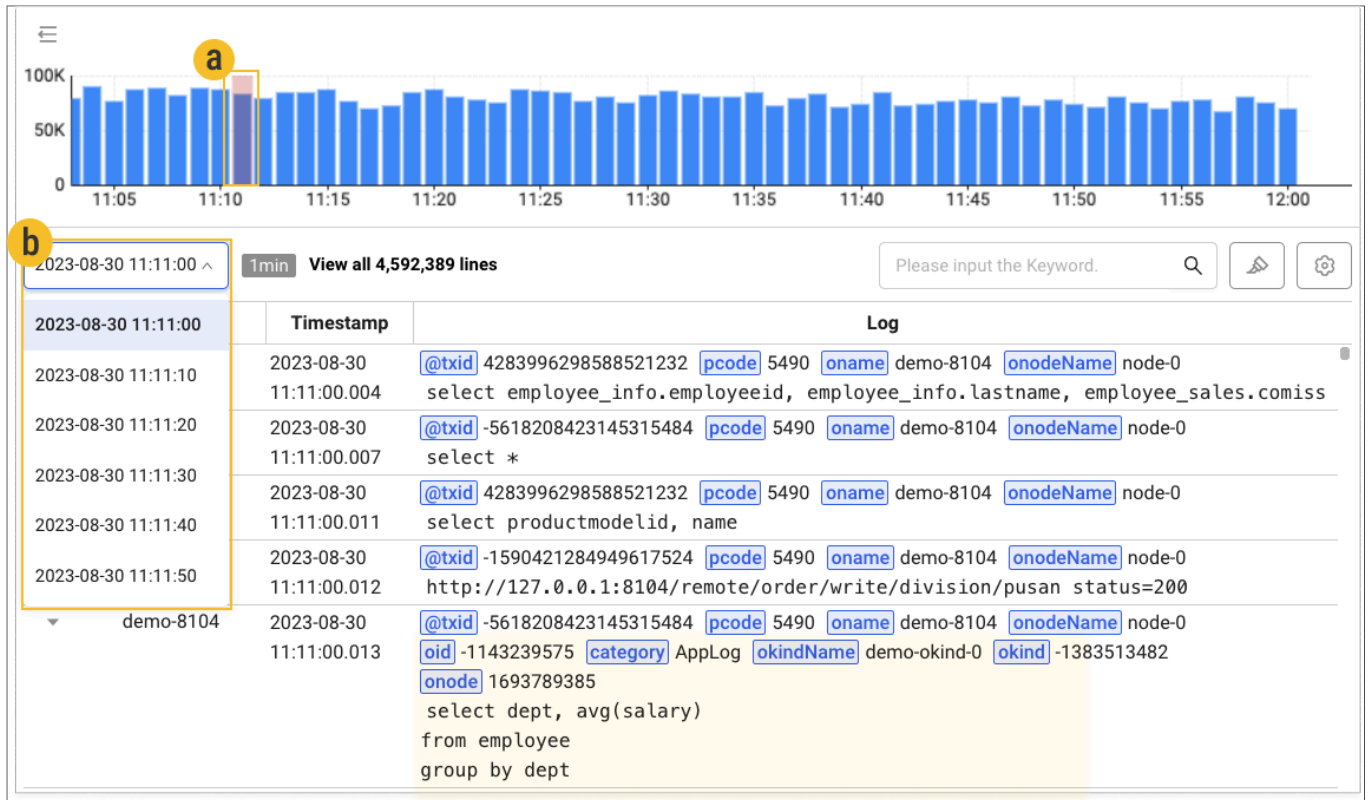
String to input	Description	Result
a b c	Separate each keyword with a space.	a, b, c
"Whatap is good."	To include spaces in keywords, wrap them in "'" or "\"".	Whatap is good.
"Whatap\\ is good."	If \ is included in the keyword surrounded by "", enter it as \\.	Whatap\ is good.

Setting the highlight color

By selecting  **Highlight**, you can set the keyword and its color for highlighting.

- In addition, enter the keyword to set the color for.
- If you click **Color** on the left of the input field, available colors appear.
- Basically, different highlighting by the level (**WARN**, **ERROR**, **FATAL**) is applied.
- The settings are saved in **Project Rules**.

Viewing the logs with a chart



- You can click or drag the desired time range bar on the bar chart (a) to view the logs for the time range.
- You can use the (b) time selection option on the upper left of the log table under the bar chart to further refine your log search in the selected time zone:
 - 1min: interval (spacing between bars on the chart)
 - Select a time option: Time zone whose time range is divided into 6 segments.

Setting the table

Column settings

Right of the (3) area, select **Column settings**. You can add columns or set order.

- **Adding columns**

You can add columns to the table by selecting tags. If you unselect the **log** column, you cannot see **Log view detail setting**. Be sure to select at least one column.

- **Setting the column order**

When you add a column, the column is added to **Display columns**. Drag a desired column to change the order of the columns.

Log view detail setting

On the right of 3, select  **Log view detail setting**. **content** and **Tag** are all checked and two items are also displayed. Be sure to select any of **content** and **Tag**.

Unchecked items are not displayed in the table. If you deselect the **Tag** as follows, the log's **Tag** does not appear in the table.

Log table tag invisible

When you add tags in the **Tag management** list, the tags in the log are listed in the order you added. You can change the order of the tags by dragging them. If you disable an added tag, the disabled tag does not appear.

- **Column settings** and **Log view detail setting** can be used in **Live Tail**, **Log Search**, and **Log Trend**.
- In the same project, the **Live Tail**, **Log Search**, and **Log Trend** menus share **Column settings** and **Log view detail setting**.

Log Setting

You can configure the log monitoring related settings in **Log Configuration**. Using the tab at the top, you can use menus for checking the agent settings, determining whether to enable log monitoring, setting the log data retention period and lookup password, registering the log parser, and setting the quick indexes.

- To use the **Activate log monitoring** function, the **Edit project** role is required.
- The **Log edit** role allows you to modify the **Log Configuration** menu other than **Activate log monitoring**.

Starting the log monitoring

At the top, select the **Getting started with log monitoring** tab. If you select the  **View guide** icon and the **View plans** button, the corresponding guide screen appears.

Set up the agent and enable log monitoring

Log monitoring data setting

In the  area, you can see the **Log usage**. You can also change the **Log retention period** and **Log lookup password** settings.

Log retention period

This is the default data retention period to be applied commonly. If not specified, the default value is 1 day. In addition to the option to select a log retention period, you can enter a desired period of time. If not set separately in the **Log usage** list, this log data retention period is applied by default. If you set the data retention periods for each category in the **Log usage** list and select **Initialized**, the default data retention period is reset.

Log usage amount

You can specify the log data retention periods for each category in the **Log usage** list. **Log Count** means the number of logs stacked for the period. For example, **Daily log count** is the number of logs accumulated during the day, and **Expected log count** is the number of logs of the today's log count multiplied by the days of data retention.

You can specify the log data retention period as follows. You can free the space by deleting old data according to the specified period.

- **Trial Project**

You can select 1, 2, or 3 days for the data retention period.

- **Paid Project**

For the data retention period, you can select one of 1 day, 2 days, 3 days, 4 days, 5 days, 6 days, 7 days, 10 days, 30 days, and 40 days.

- **Data size-based billing**

The price differs depending on the data retention period.

For example, if an average of 2 million logs per day accumulates and the data retention period is set to 3 days, an average of 6 million logs is kept on the collection server and subject to billing.

Log lookup password

To enhance security, set the **Log lookup password**. The log lookup password is optional. If you are using a log lookup password, enter the password to go to the log screen.

 In case you forgot the password

If you have the **Edit Log** role, you can modify it with a new password in **Log Configuration**.

Log primary parser setting

Select the **Log primary parser setting** tab at the top of **Log Configuration** to register parsers for collected logs.

The log primary parser provides **GROK** and **JSON** parsers, essential for aggregating log counts by type and searching for specific logs. It extracts search keys and values that match pattern conditions, and the parsed keys are used for log type classification and search indexing.

- **GROK**: This parsing is based on the regular expression by default. It provides parsing based on the reserved keywords.
- **JSON**: Batch parsing is provided for the JSON output parts of the logs.

✓ In case of no parsing logic registered, keys for search

category , oid , oname , okind , okindName , @txid , @login , httpost

Reserved words that cannot be registered for the parser

timestamp , message , pcode , category , content , logContent

- For the following reserved words, indexes are not created even if a parser has been registered.

! For more information about the log parser, see [the following](#).

Setting item

Set value	Description	ETC
Category	Category to apply the pattern to	required
Log detection condition	Enter the search key and search value to be applied as the filter. The pattern is applied only to the log data that meets the log detection conditions. If you do not enter any log detection condition, the pattern is applied to all logs.	optional
Pattern	It is the pattern to parse the log for. Parsing is performed according to the created pattern, and indexes are created. It supports GROK, regular expression syntax.	required

Parser list

You can search for registered parsers, add, or edit them. Parsers are evaluated in registered order, and only the first matching parser is applied.

- If you select + **Add** on the upper right, the **Parser Add** window appears.
- You can change the order of parser settings by dragging the  icon in the **Priority** column of the parser list.
- Through the parser list's  **Enable** toggle button, you can set whether or not to enable the parser.
- Through the parser list's  **Edit** and  **Delete** icons, you can modify or delete the registered parser.

Parser registration order

The following shows the common parser registration procedure.

1. In **Log primary parser setting**, select + **Add**.
2. In the **Parser Add** window, select a **Parser**.

Parser and pattern registration method

- [GROK Parser and Pattern Registration](#)
- [JSON Parser and Pattern Registration](#)

3. When you select a parser, the **Register pattern** button is enabled. After clicking **Register pattern**, enter the pattern and log in the **Parser Simulation** window.

a. Enter the **Pattern**.

b. Enter the **Log Category** and **simulation parsing log**. Click the **Log Search** button, then click the **Select** button to the right of the desired log in the search results to auto-fill the log.

 Through **Log Search**, you can select a sample log from collected logs. The selected log is automatically reflected in the simulation input field, allowing you to test immediately without copying and pasting.

c. To check whether the pattern is normal, click **Simulation** and then measure the performance of

simulation and pattern.

! For more information on simulation and performance measurement, see [the following](#).

4. After confirming the simulation result parses successfully, click **Apply Pattern**.
5. Click **Add** to add the parser.

! Personal information de-identification

If the search key name is specified as `search-key.p` during parser registration, de-identification is applied by default (e.g. `myname.p **`). WhaTap recommends managing de-identification in the **De-identification of personal information** tab. For more information, see [Personal information de-identification](#).

GROK parser pattern registration

The default syntax is `%{SYNTAX:SEMANTIC}`. For more information about the GROK parser, see [the following](#). Pattern registration and simulation are required.

- **SYNTAX**

GROK definition pattern.

- **SEMANTIC**

It is the key allocated to the parsed data.

! It is recommended to use combination words in SEMANTIC so that reserved words are not used.

Registering the JSON format parser pattern

If all or part of a log is output in JSON format, you can parse the JSON output through the JSON format parser. To detect the JSON output of the log, the **prefix** and **postfix** options are combined to specify which part of the log to be recognized by JSON for parsing. For more information about the JSON parser, see [the following](#). Simulation is required.

Option	Description
Prefix	Specify the string before the beginning of JSON string. If not specified, it is identified as a JSON string from the beginning of the log output.
Postfix	Specify the string after the end of JSON string. If not specified, it is identified as a JSON string up to the end of the log output.
Ignore	Specify fields in the JSON output to exclude from key extraction.

• Registration example

Log

```
[2022-10-25 10:15:34:145]...(line feed)
Request : {"key1":"value1","key2":"value2",...}(line feed)
Response : {"key3":"value3","key4":"value4",...}
```

As in the example, to parse both Request JSON and Response JSON for incoming logs, register the following two patterns.

- Pattern for request parsing

Strings between "Request : " and "Response" `{"key1":"value1","key2":"value2",...}`

- Pattern for response parsing

Strings from "Response : " to the end of a log `{"key3":"value3","key4":"value4",...}`

• JSON custom pattern registration

If part of a log is output in JSON format, the JSON output can be parsed by a dedicated custom parser. Enter the pattern as follows:

```
io.whatap.logsink.parser.JsonFormatParser{}
```

To detect the JSON output of the log, the **prefix** and **postfix** options are combined to specify which part of the log to be recognized by JSON for parsing.

Specify an option in `{}` of `JsonFormatParser{}` .

- **Registration example**

Log

```
[2022-10-25 10:15:34:145]...(line feed)
Request : {"key1":"value1","key2":"value2",...}(line feed)
Response : {"key3":"value3","key4":"value4",...}
```

As in the example, to parse both Request JSON and Response JSON for incoming logs, register the following two patterns.

- **Pattern for request parsing**

Strings between "Request : " and "Response" `{"key1":"value1","key2":"value2",...}`

```
io.whatap.logsink.parser.JsonFormatParser {prefix:"Request : ",postfix:"Response"}
```

- **Pattern for response parsing**

Strings from "Response : " to the end of a log `{"key3":"value3","key4":"value4",...}`

```
io.whatap.logsink.parser.JsonFormatParser {prefix: "Response : "}
```

Parser simulation and performance measurement

After the **parser simulation**, you can register a pattern. **Performance measurement** measures the time taken by the parser to perform repeated parsing on the target string for simulation.

1. Enter values for **Pattern** and **Log**. Click the **Log Search** button, then click the **Select** button to the right of the desired log in the search results to auto-fill the log.
2. Click **Simulation** to check whether the parsing has been successful with the pattern to register.
3. If the simulation is successful, you can view **Simulation result** and **Performance measurement results**.
4. When you click **Apply pattern** after simulation, the pattern that has been entered for the selected parser is applied.

Parsing success

If a key is generated by registering a parsing logic, the value parsed with the key is added upon log inquiry. As in the following **Live Tail** menu's example, the parsed key and value are added.

Timestamp	Log
2022-08-17 14:28:00.612	oname dev949400-8093 onodeName node-1 oid 413390913 category AppStdOut okindName dev-okind-1 load 52

The parsed key can be checked in **Live Tail**, **Log Search**, and **Log Trend**.

Log secondary parser setting

Select the **Log secondary parser setting** tab at the top of **Log Configuration** to register log parsers.

The log secondary parser processes the values extracted by the primary parser (GROK or JSON) to generate statistics data or new fields. In addition to the HTTP status code-based statistics parsers, it provides various processors such as keyword filters, field processing, response time classification, and GeoIP conversion.

! The log secondary parser provides the special purpose secondary parsing function for the primary parsed results. To use the secondary parser, the **primary parser** must have been **registered**.

Parser list

Log Configuration						
Getting started with log monitoring Log primary parser setting Log secondary parser setting Fast index setting Log long-term archive statistics Log 1-hour statistics widget data settings						
Log secondary parser setting This parser can be used if a Grok or JSON parser has already been parsed. + Add Save						
Priority	Parser	Category	Log detection condition	Pattern	Enable	
0	4xx, 5xx status code parser	AppStdErr	All logs		☒	
1	Status code success rate parser	AppLog	All logs		☒	

You can search for registered parsers, add, or edit them.

Adding parsers, changing order, enabling/disabling toggles, editing, and deleting work the same as in the

[primary parser list.](#)

Parser registration order

The following shows the common parser registration procedure.

× Parser Add

Parser*

WhaTap reserves the right to disable parsers that may affect the stability of the WhaTap service.

Please select the Parser. ▼

Status codes to exclude

Please select the Parser.

Category*

If multiple parsers are registered in the same category, only the first matching parser is applied.

Please select the Category.

Log detection condition

If you don't enter any filter, or if you enter only one of the search keys/values, the pattern is applied to all logs.

Search key

Search value

Add

1. If you select **+ Add**, the **Parser Add** window appears.
2. In the **Parser** selection window, select a parser. For more information about each parser's setting items, see the following.
 - **4xx, 5xx status code parser** [Setting item](#)
 - **Status code success rate parser** [Setting item](#)
3. Enter the **Status codes to exclude**.

4. In the **Category** selection window, select a category or enter it.
5. Select **Log detection condition** or enter it.
6. Select **Add** to register a parser.

4xx, 5xx status code parser setting item

The **4xx, 5xx status code parser** generates 4xx and 5xx count data based on the status values parsed by the primary parser. To exclude specific status codes, enter the status codes to exclude.

Setting item

Set value	Description	ETC
Category	It is the category to generate the 4xx, 5xx count data.	required
Log detection condition	Enter the search key and search value to be applied as the filter. The 4xx, 5xx count data is generated only for the log data that meets the log detection condition. If you do not enter any log detection condition, the data is generated for all logs.	optional
Status codes to exclude	The status codes to exclude upon generation of statistics data. If no entry, the 4xx, 5xx count data is generated for all error status codes that correspond between 4xx and 5xx.	optional

Registration example for the status parser

Log primary parser setting You can register parsers for the collected logs. Parsers are applied in the order they are applied, with only the first match being applied. + Add Save						
Priority	Parser	Category	Log detection condition	Pattern	Enable	
0	JSON	AppLog	status:404	status:404	☐	✎ ✖
1	JSON	AppLog	status:500	status:500	☒	✎ ✖
2	GROK	AppLog	All logs	%{NUMBER:status}	☒	✎ ✖

If the incoming log is `{"msg":"message","status":404}` and its status is parsed by the GROK parser as shown in

the example, it is parsed as `status: 404` . If you confirm that the status has been normally parsed, register the status codes to exclude by the 4xx, 5xx status code parser.

Data Search

If all parsers have been registered, go to **Integrated Flex Board** and then create the **Log 4XX, 5XX count** widget.

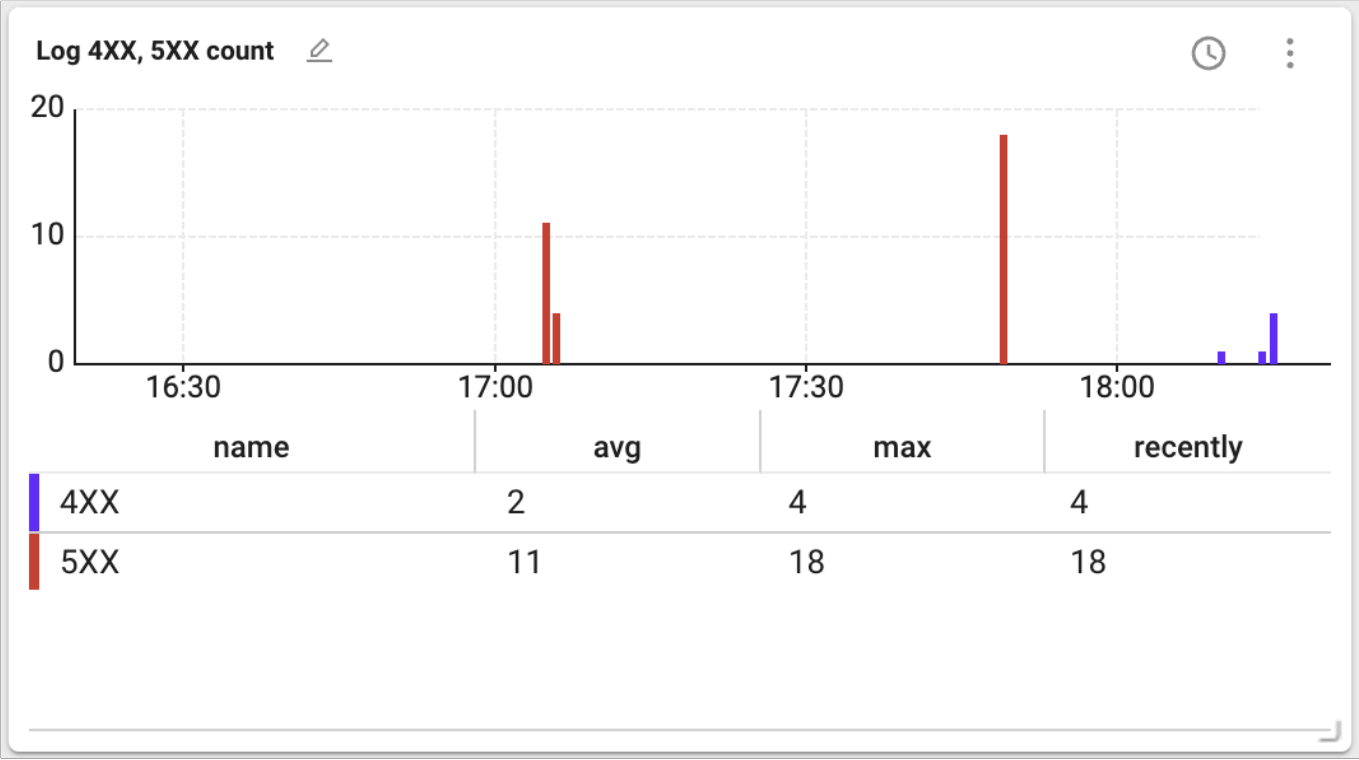
Widget templates

4xx

Q

Log 4XX, 5XX count

If the widget is created, you can see the following data.



- **avg**: Average value of the data during the query period

- **max**: Maximum value of the data during the query period
- **recently**: Final value of the data during the query period

Status code success rate parser setting item

The **Status code success rate parser** generates HTTP request success rate data based on the status values parsed by the primary parser. To exclude specific status codes, enter the status codes to exclude. For status parsing, see [4xx, 5xx status code parser setting item](#).

Setting item

Set value	Description	ETC
Category	It is the category to generate the request success rate data.	required
Log detection condition	Enter the search key and search value to be applied as the filter. The request success rate data is generated only for the log data that meets the log detection condition. If you do not enter any log detection condition, the data is generated for all logs.	optional
Status codes to exclude	The status codes to exclude upon generation of request success rate data. If no entry, the request success rate data is generated for all success rate status codes that correspond between 2xx and 3xx.	optional

Data Search

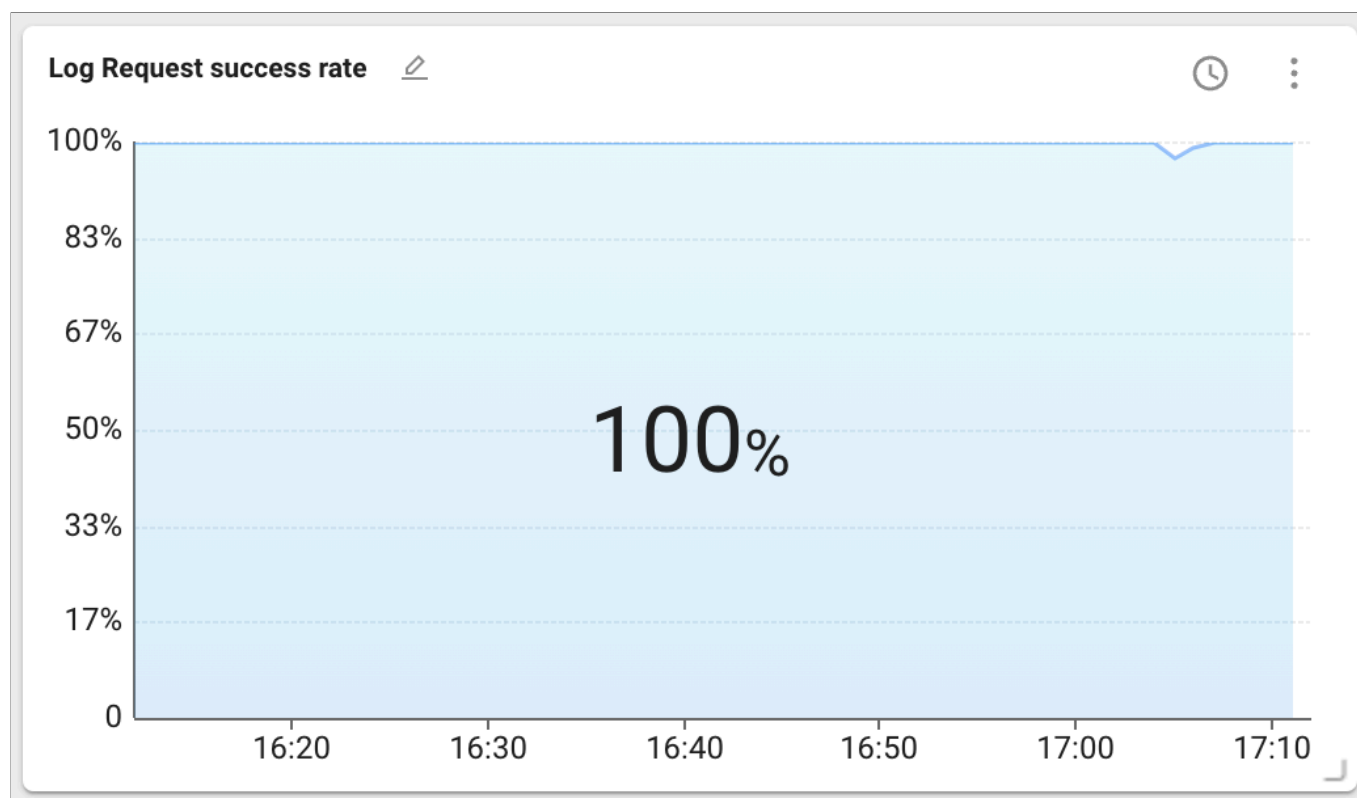
If all parsers have been registered, go to **Integrated Flex Board** and then create the log request success rate widget.

Widget templates

⇌ All metrics

 Log Request success rate

If the widget is created, you can see the following data.



The data above the chart represents statistics for the lookup period. You can select the statistical method with the latest value, maximum value, or average value. The latest value is selected by default.

Secondary parser processors

In addition to **4xx**, **5xx status code parser** and **Status code success rate parser**, the log secondary parser provides the following field processing processors.

Log secondary parser processor list

Processor	Description
Contains all keywords filter	Adds a flag field to logs that contain all of the specified keywords.
Contains any keyword filter	Adds a flag field to logs that contain at least one of the specified keywords.

Processor	Description
Rename field	Renames an existing field name to a different name.
Status code group classification	Automatically classifies HTTP status codes into 2xx/3xx/4xx/5xx groups.
URL static/dynamic classification	Classifies a URL as static content if it has an extension (.), and as a dynamic servlet if it does not.
URL parameter removal	Stores the value with the query parameters after ? removed from the URL.
Response time classification	Automatically classifies the response time (ms) into fast/normal/slow/critical ranges.
JSON field extraction	Extracts specific keys from a JSON string field and stores them as new fields.
GeoIP conversion	Converts an IP address into country/city information.
Custom input	Registers a processor directly with an FQN class name.

Contains all keywords filter

Adds a flag field to logs that contain **all** of the specified keywords.

Set value	Description	Default
Input field	The field name to search for keywords	content
Storage field	The field name to store the result	has_str_all
keyword	The list of keywords to search (enter separated by commas)	required

Usage example: If you set the input field to `content` and the keywords to `error, timeout, database`, the `has_str_all` field is added only to logs that contain all three keywords.

Contains any keyword filter

Adds a flag field to logs that contain **at least one** of the specified keywords.

Set value	Description	Default
Input field	The field name to search for keywords	content
Storage field	The field name to store the result	has_str_any
keyword	The list of keywords to search (enter separated by commas)	required

Usage example: If you set the input field to `content` and the keywords to `reboot, shutdown, restart`, the `has_str_any` field is added to logs that contain at least one of the keywords.

Rename field

Renames an existing field name to a different name. If the target field name already exists, it is not overwritten.

Set value	Description	Default
Source field	The existing field name to rename	required
New field name	The field name after renaming	required

Status code group classification

Automatically classifies HTTP status codes into the `status_2xx`, `status_3xx`, `status_4xx`, and `status_5xx` groups.

Set value	Description	Default
Input field	The field name that contains the status code	status
Storage field	The field name to store the group classification result	status_nxx

Usage example: If the `status` value is `404`, `status_4xx` is stored in the `status_nxx` field.

URL static/dynamic classification

Classifies a URL as **static content** if it contains an extension (.), and as a **dynamic servlet** if it does not.

Set value	Description	Default
Input field	The field name that contains the URL	<code>url</code>
Storage field	The field name to store the classification result	<code>url_type</code>

URL parameter removal

Stores only the path with the query parameters after `?` removed from the URL.

Set value	Description	Default
Input field	The field name that contains the URL	<code>url</code>
Storage field	The field name to store the parameter removal result	<code>url_without_params</code>

Usage example: `/api/v1/users?page=1&size=20` → `/api/v1/users` is stored in the `url_without_params` field.

Response time classification

Automatically classifies the response time (ms) by range. You can set the range thresholds directly.

Set value	Description	Default
Input field	The field name that contains the response time (ms)	<code>elapsed</code>
Storage field	The field name to store the classification result	<code>response_class</code>
Fast upper limit (ms)	The upper limit of the fast range	<code>100</code>

Set value	Description	Default
Normal upper limit (ms)	The upper limit of the normal range	500
Slow upper limit (ms)	The upper limit of the slow range	2000

The classification results based on the default values are as follows.

Response time	Classification
0 ~ 100ms	fast
101 ~ 500ms	normal
501 ~ 2000ms	slow
2001ms or more	critical

Usage example: If you filter by `response_class: critical` in the log explorer, you can query only the logs whose response time exceeds 2 seconds.

JSON field extraction

If a field extracted by the primary parser contains a JSON string, this extracts specific keys from that JSON and stores them as new fields.

Set value	Description	Default
Input field	The field name that contains the JSON string	payload
Keys to extract	The list of JSON keys to extract (enter separated by commas)	required
Storage prefix	The prefix to prepend to the extracted key names (e.g., <code>json_</code>)	optional

- If the entire log is JSON, the primary JSON parser parses it automatically. This processor is useful for additionally parsing the JSON part contained within a text log when using the **GROK primary parser**.



- To protect performance, parsing is skipped if the JSON field size exceeds 10 KB.

Usage example

Primary GROK parsing result

```
payload = {"user":"alice","action":"purchase","product":"laptop","amount":45000}
```

If you set the input field to `payload`, the keys to extract to `user, action`, and the storage prefix to `pay_`, they are extracted as follows.

JSON field extraction result

```
pay_user = alice
pay_action = purchase
```

GeoIP conversion

Converts an IP address into country and city information. It uses the IP2Location database to enable region-based analysis of access logs.

Set value	Description	Default
Input field	The field name that contains the IP address	<code>client_ip</code>
Storage prefix	The prefix of the result field names	<code>geo</code>

As a result, two fields, `{prefix}_country` and `{prefix}_city`, are created.

Usage example: If the input field `client_ip` value is `223.130.195.200` and the storage prefix is `geo`:

GeoIP conversion result

```
geo_country = KR
geo_city = Seongnam
```

Custom input

You can register a processor that is not in the list directly with an FQN (Fully Qualified Name) class name.

Custom input format

```
io.whatap.logsink.processor.ClassName{"param1":"value1","param2":"value2"}
```

ⓘ The class name and parameter format must be accurate. If the input is incorrect, the processor may not work.

Secondary parser chaining

You can register multiple secondary parsers in the same category and chain them. Each processor runs in the order of registration.

Original log

```
2026-04-23T10:30:00.123+0900|INFO|api-01|192.168.1.10|/api/v1/orders?detail=true|200|1234|{"user":"alice","action":"purchase"}|Request processed
```

Order	Parser	Input → Output
Primary	GROK	timestamp, level, host, client_ip, url, status, elapsed, payload, content
Secondary-1	JSON field extraction	payload → user, action
Secondary-2	Response time classification	elapsed → response_class (slow)
Secondary-3	Status code group classification	status → status_nxx (status_2xx)
Secondary-4	URL parameter removal	url → url_without_params (/api/v1/orders)
Secondary-5	GeoIP conversion	client_ip → geo_country (KR), geo_city (Seoul)

! The **Category** of the secondary parser must be set identically to that of the primary parser. If you set a different category, the secondary parser is not applied to that log.

Fast Index Setting

Select the **Fast index setting** tab at the top of **Log Configuration**. Collecting a large number of logs can significantly decrease the log search performance. The frequently used search conditions are created as **index**, you can improve the log search performance for quick search. The setting items are as follows:

Set value	Required	Description
Category	Mandatory	Category to be set as fast index
Search Key	Mandatory	Search key for fast index setting
Case insensitive	Option	Whether to be case sensitive
Rule	Mandatory	* must be included at least one.
Enabled	Mandatory	Active or inactive (default value is <code>true</code>)

Importing/exporting log settings

You can save parser settings, Fast index setting, and filter settings in JSON file format, and apply them by importing a JSON file from other projects. You can reduce the hassle of creating the settings repeatedly for each project.

1. Add parser settings, Fast index setting, and filter settings to one project.
2. Select **JSON**  on the upper right of each configuration tab.
3. On the upper right of the **Export JSON** window, select **Export**.
4. The JSON configuration file is saved on your PC.
5. Move to another project and then go to the **Log > Log setting** menu.

6. Select the configuration tab where you have exported the JSON configuration file before, and then select .
7. If the file selection window appears, select the JSON configuration file saved on your PC.
8. If the **Import JSON** window appears, check the configuration file and then select **Add to list** or **Overwrite**.
9. Select **Save** on the upper right of the screen.

 After importing the JSON configuration file, you cannot save the imported settings unless you select **Save**.

Log long-term archive statistics

Select the **Log long-term archive statistics** tab at the top of **Log Configuration**. Log data is so large and difficult to retain for a long time. Using the Set log statistics data function, you can **save information on how many logs that meet specific conditions are collected every 5 minutes**. Even if actual log data has been deleted for a long time, you can check the trend of how many logs that meet the conditions are collected.

Adding the log long-term archive statistics

× Log long-term archive statistics Add

Statistic key*

Data retention period(disk usage)

Category*

Log detection condition* —

Exclude ☐ **Case Sensitive** ☒

[+ Add](#)

[Add](#)

If you select + **Add** under the **Log long-term archive statistics** tab, the **Log long-term archive statistics Add** window appears. You can add rules by using + **Add** or delete the created rules by using the - icon.

Setting item

Field	Description
Category	Category to apply the rule to.
Statistic Key	The same key cannot be set twice to save when a log that meets the rule is generated.
Log detection condition	Condition for generating log statistical data. Statistical data is generated based on how many logs that meet this condition are collected.
Exclude	If checked, statistical data is generated with values that do not correspond to the entered conditions.
Case Sensitive	Specify case sensitivity for the values of the entered log detection conditions.

Field	Description
Enabled	Active or inactive (default value is <code>true</code>)

Example

If a setting is added as follows, statistical data is generated with a key value of **TotalCount** for the logs whose status is `200` or `300`.

Log long-term archive statistics You can generate statistical data about how many logs have been collected that meet certain conditions.					
				+ Add	Save
Category	Statistic key	Log detection condition	Data retention period(disk usage)	Enable	
AppLog	TotalCount	status 200, 300	15 Days (About 3 MB)	☐	Edit Delete
AppLog	TotalCount	status 200	15 Days (About 3 MB)	☐	Edit Delete
AppLog	TotalCount	status 300	15 Days (About 3 MB)	☒	Edit Delete
AppLog	TotalCount	status 200, 300	15 Days (About 3 MB)	☒	Edit Delete

Data Search

1. Create a widget by searching **Log long-term archive statistics** in **Widget templates** of **Integrated Flex Board**.

Widget templates

[⇌ All metrics](#)

Log long-term archive statistics

2. Enter the **Category** and **Statistic key** to view and then select **Apply**.

Log long-term archive statistics

 Please select a category and a key.

Log long-term archive statistics Setting is required to collect the data that the widget represents.

If this setting is not set, refer to [Guide](#) and do **Log long-term archive statistics Setting**.
[Log setting](#)

Change a category

AppLog 

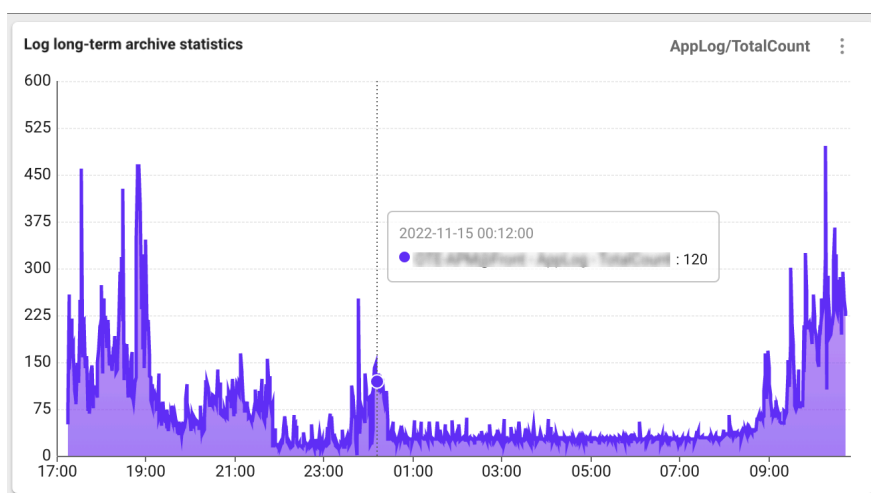
Statistic key

TotalCount 

Cancel

Apply

3. With the added settings, you can check the **Log long-term archive statistics** data as follows.



Personal information de-identification

In **De-identification of personal information**, you can mask personal information in log data or replace it with safe values.

- **Encryption:** Specified sensitive data is encrypted and stored in the database.

- Masking: When displayed on the log screen, sensitive data is masked (*******) by default.
- Substitution: Sensitive data is replaced with a user-specified value that is safe.

Personal information classification

The items classified as personal information are as follows: If there are any items that need to be treated as sensitive data in addition to personal information, mask or replace the desired items in the log data by using the **De-identification of personal information** feature.

- National ID number
- Passport number
- Driver's license number
- Foreigner registration number
- Credit card number
- Bank account number
- Biometric information

Required roles

De-identified personal information is displayed as masked. Only users with the **log personal information query** role can view original data through the **Display personal information** toggle. Adding or modifying de-identification target search keys requires the **log editing** role.

❗ For more information about the **log personal information query** and **log editing** roles, see [the following](#).

Setting the personal information de-identification

You can protect sensitive information by applying masking to new log data.

Log Configuration

Getting started with log monitoring | Log primary parser setting | Log secondary parser setting

De-identification of personal information When a search key containing personal information is detected, the data is encrypted, stored, and masked.

Enable	Category	Search key
☒	AppLog	@txid agenttime @mt

Log's personal information de-identification checking It de-identifies the log's personal information.

Time: < 2025/01/21 16:47 ~ 2025/01/21 17:47 1 hr >

Category: Please select the Category.

Personal information entity:

Personal information pattern:

Whether to apply substitution: ☒

Value to substitute:

De-identification of personal information Add

Category*: Please select the Category.

Search key*: Select search keys to be encrypted and masked.
Enter the search key to encrypt.

1. In the **De-identification of personal information** tab, select **Add**.
2. In the **De-identification of personal information Add** pane on the right, select **Category** and enter the **Search key** to mask.
3. Click **Add** to add the setting.
4. After checking the de-identified items in the **De-identification of personal information** list, click **Save** on the upper right to save the current settings.

De-identification of personal information If you add a search key containing personal information, the data is encrypted, stored, and masked.

Enable	Category	Search key	Edit
☐	VirtualLog	age n	edit delete
☒	VirtualLog	status	edit delete
☒	AppLog	agenttime	edit delete

- The de-identified search keys are output in the format of `search key.pii` in the log content.
- You can perform ☒ **Enable** for de-identified items in the **Enable** column of the **De-identification of personal information** list.
- You can **modify** and **remove** in the **edit** column of the **De-identification of personal**

information list.

- ✓ If the search key name is specified as `search-key.p` in the **Log primary parser setting** tab, it is automatically registered as a de-identification target. You can check or disable auto-registered items in **Specified search key** after selecting the **Category** in the **De-identification of personal information** tab.

We recommend configuring de-identification directly in the **De-identification of personal information** tab rather than using the `.p` suffix in parser settings.

Personal information display

De-identified data is displayed as masked in the **Live Tail**, **Log Trend**, and **Log Search** menus. Users with the **log personal information query** role can click the **Display personal information**  button in the log list to view the original data.

▼	java-demo2	2024-12-16 16:06:49.988	area	river	!privacy	true	status.pii	***	pcode	8	city	seoul	onodeName	node-0	myname.p	***
			oid	-1737750367	okind	1152715164	price.n	12000	oname	java-demo2	age.n	33				
			agenttime	1734332809555	category	VirtualLog	okindName	dev-okind-0	onode	1693789385						
			You need not love me, if you choose not to.													
▶	java-demo1	2024-12-16 16:06:49.993	area	mountain	!privacy	true	status.pii	***	pcode	8	city	junju	onodeName	node-1	myname.p	****
			Waiting does not have to aim for a meeting.													
▼	java-demo2	2024-12-16 16:06:49.988	area	river	!privacy	true	status.pii	500	pcode	8	city	seoul	onodeName	node-0	myname.p	lee
			oid	-1737750367	okind	1152715164	price.n	12000	oname	java-demo2	age.n	33				
			agenttime	1734332809555	category	VirtualLog	okindName	dev-okind-0	onode	1693789385						
			You need not love me, if you choose not to.													
▶	java-demo1	2024-12-16 16:06:49.993	area	mountain	!privacy	true	status.pii	200	pcode	8	city	junju	onodeName	node-1	myname.p	hong
			Waiting does not have to aim for a meeting.													
▶	java-demo6	2024-12-16 16:06:50.064	area	sea	!privacy	true	status.pii	200	pcode	8	city	daegu	onodeName	node-1	myname.p	song
			Waiting does not have to aim for a meeting.													

- ! The search key specified in the **De-identification of personal information** tab appears in the log content of the Log menu in the format of `Search key.pii`.

Example of status.pii ***

Checking the log's personal information de-identification

 If you replace the existing data using the **Log's personal information de-identification checking** feature, the data cannot be recovered.

Log's personal information de-identification checking identifies personal information in existing log data and replaces it with the **Value to substitute** specified by the user.

Replacement by target key

If you specify a target key, only the value stored in that key is replaced, and the rest of the log content is kept as is. The target key applies to both the **field** value and the **tag** value of a log. If you do not specify a target key, personal information is identified and replaced across the entire log content, the same as before.

 Replacement applies only to the stored log data. The original value may remain in the search index even after replacement.

You specify the target key in the **Target key** input field of the log personal information de-identification check form. On the screen, **field** and **tag** are not distinguished and are entered as a single target key.

Log's personal information de-identification checking
It de-identifies the accumulated logs.



Time < 2025/03/21 12:26 ~ 2025/03/21 13:26 1 hr >	Category VirtualLog	Search start time 2025/03/21 12:26
Category VirtualLog	Search end time 2025/03/21 13:26	Personal information entity Resident registration number
Personal information entity Resident registration number	Personal information pattern (?<!\w)\d{2}(0[1-9] 1[0-2])([0-2][0-9] 3[0-1])[1-4]\d{6}(?!w)	Value to substitute *****
Personal information pattern (?<!\w)\d{2}(0[1-9] 1[0-2])([0-2][0-9] 3[0-1])[1-4]\d{6}(?!w)	Pattern matching result 0	
Whether to apply substitution ☐	Inspection start time 2025/03/21 13:28	Inspection end time 2025/03/21 13:28
Value to substitute ⓘ *****	Whether to apply substitution No	Inspection result SUCCESS

Start inspection

Stop inspection

1. Specify the start time and end time.

2. Set values for **Category** .
3. Select **Personal information entity** from the examples or **Direct Input**.

ⓘ When selecting **Direct Input**, directly enter a regular expression pattern to identify personal information.

4. Select whether to replace personal information, if it is identified via the **Whether to apply substitution** toggle.
5. Enter **Value to substitute** to change the string identified by the regular expression pattern in the existing log.

ⓘ • **Value to substitute** must not be longer than the original value.

- When enabling the **Whether to apply substitution** toggle, be sure to enter **Value to substitute**.

6. Enter the conditions and then select **Start inspection**.

ⓘ You can stop this step at any time by clicking **Stop inspection** during the checkup.

7. When applying substitution, enter **Replace** in the **Start of inspection for personal information de-identification** confirmation window, and then click the **OK** button.

Start of inspection for personal information de-identification ×

The value that matches the selected personal information pattern is replaced.

ⓘ Data cannot be restored after replacement.

If replacement is required, see below. "Replace"Please enter directly.

Replace

Cancel
OK

8. After the inspection is finished, you can see **Inspection result** on the right as in the example image.

- **Category:** It displays the categories checked.
- **Search start time** and **Search end time:** It displays the time range for the checkup.
- **Personal information entity:** It displays the personal items that have been checked.
- **Personal information pattern:** It displays the regular expression pattern used.
- **Value to substitute:** It displays the applied replacement value.
- **Pattern matching result:** The number of personal data identified is displayed. You can check the sample logs by clicking **Check results**.
- **Inspection result:** It displays the result where personal information has been identified.

SUCCESS (check success), FAILED (check failure), STOP (check stop), TIMED_OUT (check ended due to timeout)

Check inspection history

To view the results of past checks after performing de-identification check for the log's personal information, click the **Check inspection history** button at the upper right. You can trace the substitution history, inspection time, and applied personal information items. You can also download the list information in CSV file format by clicking the  **CSV** button at the upper right of the **Check inspection history** window.

Check inspection history ⌵ ✕					
< 2025/03/25 08:17 ~ 2025/03/25 09:17 1 hr 📅 >		Personal infor... ▼		🔍 📄 CSV	
stitute	Pattern matching result	Inspection start time	Inspection end time	Whether to apply substi...	Inspection result
***	0	2025/03/25 09:16	2025/03/25 09:16	No	SUCCESS
***	0	2025/03/25 09:16	2025/03/25 09:16	No	SUCCESS
***	0	2025/03/25 09:16	2025/03/25 09:16	No	SUCCESS

Personal information pattern

Examples of regular expression patterns used to identify personal information in the existing log are as follows:

Personal information pattern	Personal information example	Regular expression pattern	Replacement value
National ID number	123456-1234567	(?<!w)d{2}(0[1-9] 1[0-2])([0-2][0-9] 3[0-1])-1-4d{6}(?!w)	*****_ *****
Passport number	M1234567	([MSRODTC][0-9]{7}\b)	*****
Driver's license number	01-23-456789-00	(?<!w)d{2}-d{2}-d{6}-d{2}(?!w)	**_*_*_ *****_**
Foreigner registration number	987654-1234567	(?<!w)d{6}-?[5-8]d{6}(?!w)	*****_ *****
Credit card number	1234-5678-9012-3456	(?<!w)d{4}-d{4}-d{4}-d{4}(?!w)	****_****_ ****_****
Mobile phone number	010-1234-5678	(?<!w)(+82-?1[016789]-?d{3,4}-?d{4} 01[016789]-?d{3,4}-?d{4})(?!w)	****_****_ ****
Email address	example@domain.com	([a-zA-Z0-9][a-zA-Z0-9._%+-]*@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,})	***@***.***
Bank account number	123456-01-654321	(?<!w)d{6}-d{2}-d{6}(?!w)	*****_*_*_ *****
Business	111-11-01111	(?<!w)d{3}-d{2}-d{5}(?!w)	***_*_*_*****

Personal information pattern	Personal information example	Regular expression pattern	Replacement value
registration number			
Corporate registration number	111111-11111111	(?<!w)d{6}-?d{7}(?!w)	*****_ *****

OpenMetrics

In the OpenMetrics menu, you can use OpenAgent to collect custom metrics from Prometheus endpoints, explore them directly with PromQL, or quickly visualize them with predefined templates.

Screen Layout

Screen	Description
Template List	Provides predefined visualization templates such as Nginx and Istio
OpenMetrics Explorer	Query and visualize custom metrics with PromQL
Agent Installation	Install OpenAgent for metric collection

OpenMetrics Template List

To help users new to **OpenMetrics** quickly collect and visualize metrics without a complex configuration process, basic and predefined templates are provided. This makes it easy to apply commonly used open-source metrics, lowering the barrier to initial adoption and helping operators build a scalable monitoring environment.

Template List

The **Template List** provides basic open-source template cards. Each card includes a brief description, template navigation, and collection guidance.

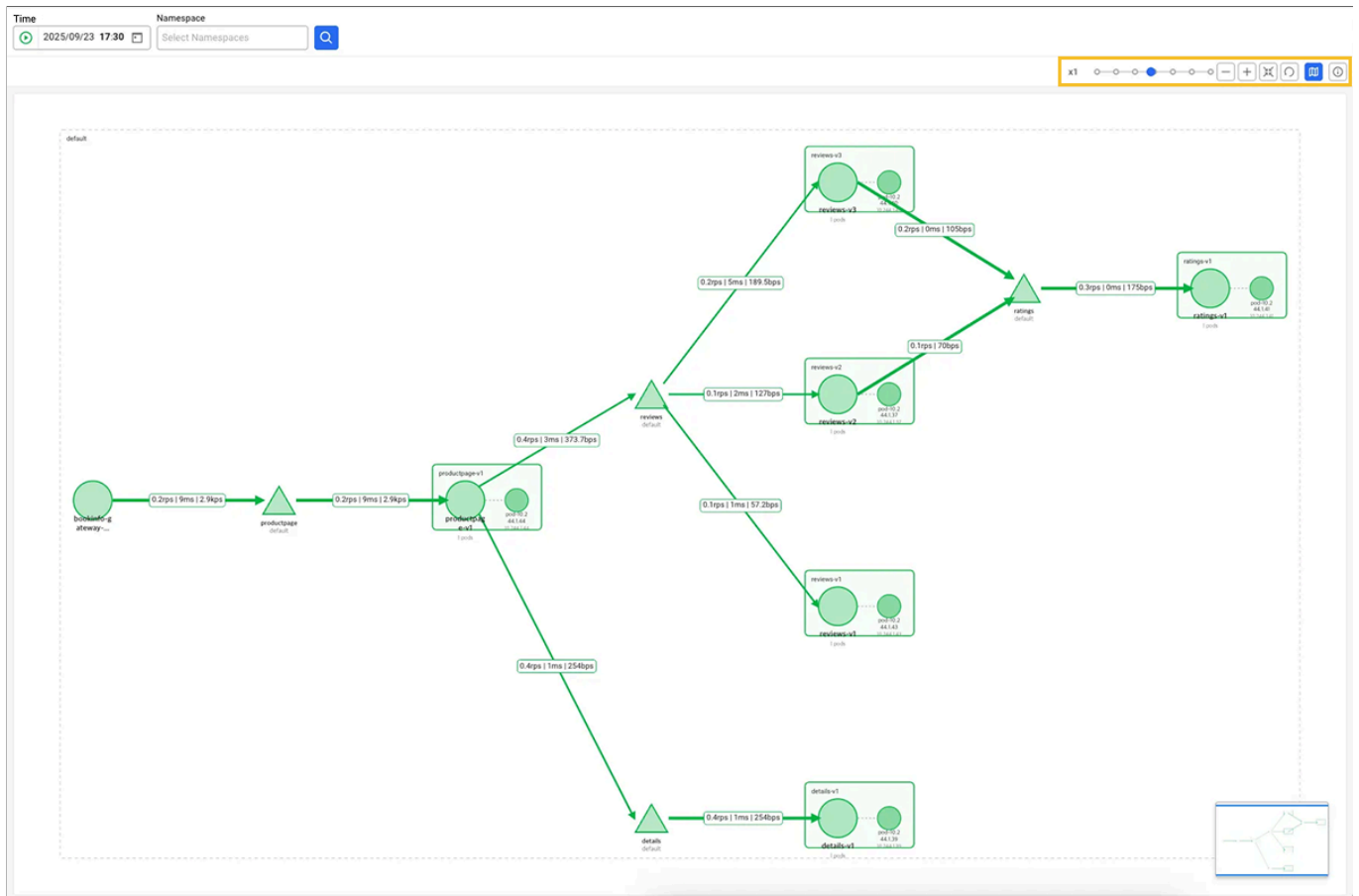
- Click the → **Template** icon to go directly to the corresponding template screen.
- Click the ⓘ **Collection guide** icon for guidance on how to configure data collection.

Nginx Template

With Nginx monitoring, you can track and analyze your web server's performance in real time.

Istio Template

This template visually represents the relationships between services and the traffic flow in an Istio service mesh environment, and links with WhatTap APM data to provide an integrated monitoring environment. Click the button at the top right of the screen to zoom the template in or out.



Legend

Click the ⓘ button at the top right of the screen to view the legend.

Node Shapes

- A triangle is a Kubernetes service
- A circle is a workload
- A square is an application
- A small circle is a Pod

Node Status

The ratio of errors (4xx, 5xx) among all HTTP requests/responses

- **Green** means an error rate below 5%
- **Orange** means an error rate of 5% or higher
- **Red** means an error rate of 10% or higher
- Gray means no requests

Pod Node Status

The Phase of a Kubernetes Pod

- **Green** means a Pod in the Running state
- **Orange** means a Pod in the Pending state
- **Red** means a Pod in the Failed state

Edge Colors

The ratio of errors (4xx, 5xx) in HTTP requests between two nodes

- **Green** means an error rate below 10%
- **Orange** means an error rate of 10% or higher
- **Red** means an error rate of 20% or higher
- **Blue** means TCP communication
- Gray means the status is unknown

OpenMetrics Explorer

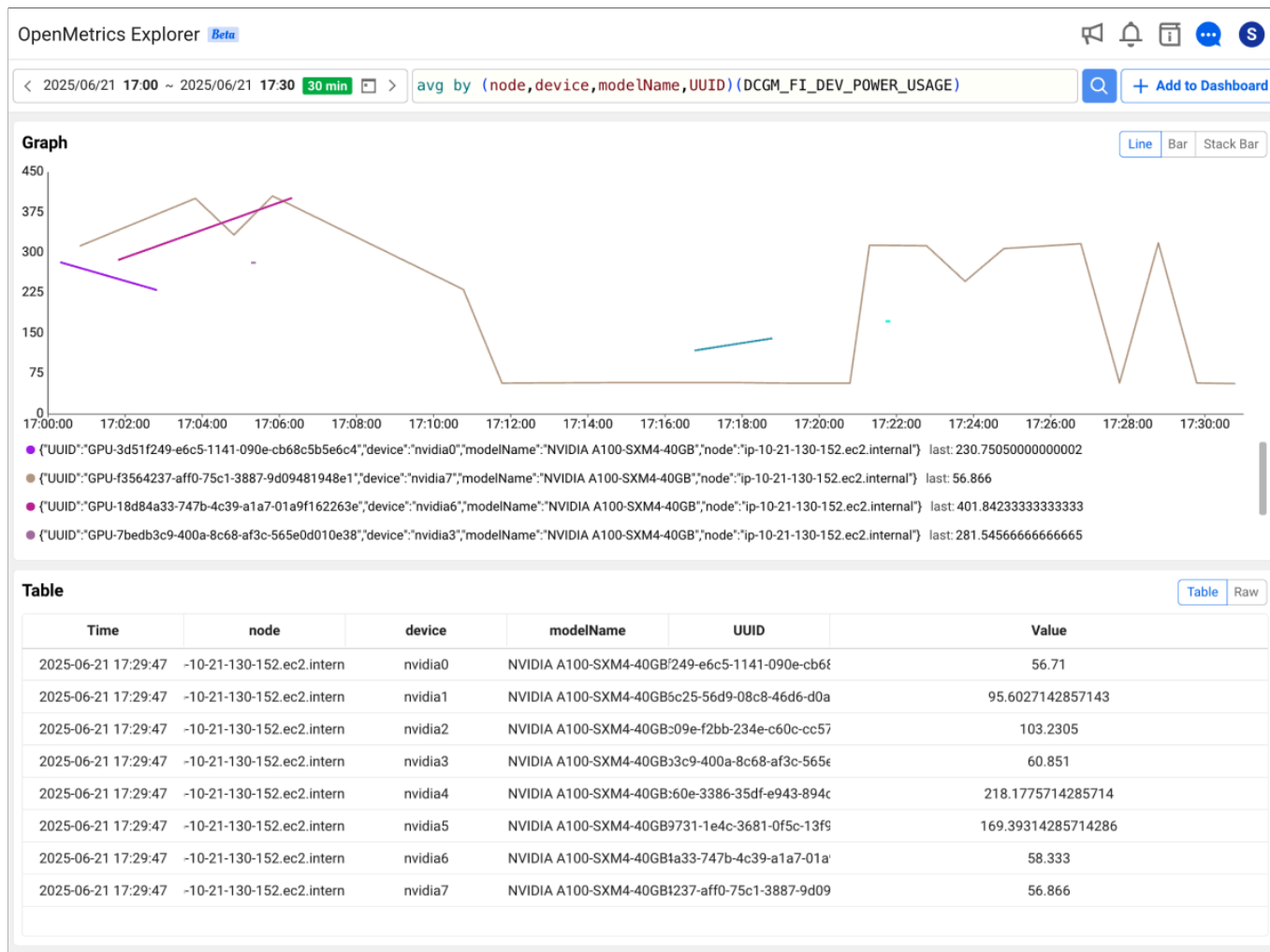
The **OpenMetrics Explorer** is a feature that lets you directly explore Prometheus-based custom metrics with PromQL and visualize them in various forms to check the state of your metrics or gain insights.

With this feature, you can freely query the metrics you want, extract meaningful data, or link it to a dashboard for continuous monitoring.

ⓘ OpenAgent installation is required to use the **OpenMetrics Explorer**.

Exploring with PromQL

In the **OpenMetrics Explorer**, you can run PromQL and view the results with various visualization options.



Graph

- **Line:** Default time-series line graph
- **Bar:** Visualized as a bar graph
- **StackBar:** Stacked bar chart showing accumulated values

Table / Raw

- **Table:** Displays the values of each time series in a table, sorted chronologically
- **Raw:** View the Prometheus API response (in JSON format) as is

PromQL Syntax Support and Autocomplete

When you enter a metric such as `node_cpu_seconds_total` or `container_memory_usage_bytes`, the autocomplete feature suggests a list of metrics and operators.

Label filtering in the form `{pod="example"}` is also supported.

Adding to a Dashboard

You can save a queried PromQL query as a dashboard widget to continuously monitor the metrics you want.

How to Add

1. Click the **+ Add to dashboard** button at the top right of the **OpenMetrics Explorer** screen. The **Add to dashboard** window opens.
2. In the **Add to dashboard** window, select an existing dashboard or create a new one.
3. Click the **Apply** button to add the widget to the specified dashboard.
 - You can enter a widget name and description on the dashboard you added it to.
 - On the Flex board's Grid layout, you can freely adjust the position of the added widget and edit its PromQL.

Installing The OpenMetrics Agent

OpenAgent is an agent that collects metrics from Prometheus endpoints and sends them to the WhaTap server. To use the OpenMetrics Explorer and templates in a SingleStore project, you must install OpenAgent first.

OpenAgent requires the following three files in the same directory to operate.

File	Description
<code>openagent</code>	Executable file for collecting and sending metrics
<code>whatap.conf</code>	Basic settings such as license and collection server address
<code>scrape_config.yaml</code>	Definition of scraping targets (endpoints)

Installation Steps Overview

1. Create the installation directory, then download the binary for your architecture (AMD64/ARM64).

```
mkdir -p /opt/whatap/openagent
cd /opt/whatap/openagent
wget https://repo.whatap.io/openagent/latest/amd/openagent
chmod +x openagent
```

2. Enter the license, server address, and port in `whatap.conf`.

```
echo "WHATAP_LICENSE=your-whatap-license" >> whatap.conf
echo "WHATAP_HOST=your-whatap-host" >> whatap.conf
echo "WHATAP_PORT=your-whatap-port" >> whatap.conf
```

3. Define the collection target endpoints in `scrape_config.yaml` (automatically reloaded when modified; no restart required).
4. Run in standalone mode.

```
./openagent standalone
```

ⓘ For the full installation steps, execution modes, detailed `scrape_config.yaml` options (StaticEndpoints, params, metricRelabelConfigs), and configuration items, refer to the [OpenAgent Installation](#) and [OpenAgent Configuration](#) documents. For Kubernetes environments, follow [OpenAgent Kubernetes Configuration](#).

ⓘ macOS Apple Silicon is not supported. It works only on Linux AMD64 or ARM64.

SingleStore Alert Notifications Overview

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 Event

Explains how to configure metric-based event conditions for SingleStore and trigger alert notifications.

Composite Metric Event

Introduces the composite metric event feature that sets event conditions by combining multiple metrics.

Anomaly Detection Event

Explains the event configuration that automatically detects anomalous patterns in SingleStore metrics to trigger alert notifications.

Real-time logs

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

 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 Event

Explains how to configure metric-based event conditions for SingleStore and trigger alert notifications.

 Composite Metric Event

Introduces the composite metric event feature that sets event conditions by combining multiple metrics.

 Anomaly Detection Event

Explains the event configuration that automatically detects anomalous patterns in SingleStore metrics to trigger alert notifications.

 Real-time logs

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

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 Event Configuration

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

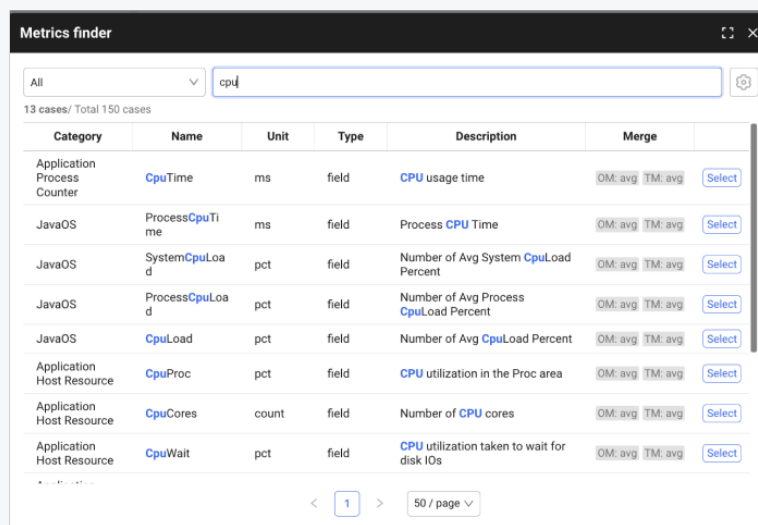
- Enter a category in the search field, or select a category (metric) from the category list. You must select a category to proceed with metric configuration.

- 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.

- Click **+ Add**.
- 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 Metric Event Configuration

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 Event Configuration

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

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

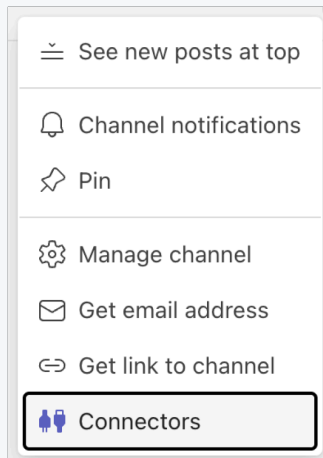


- `/remove` : Enter the project code for which you want to stop receiving alerts
- `/list` : View the list of project codes currently receiving alerts

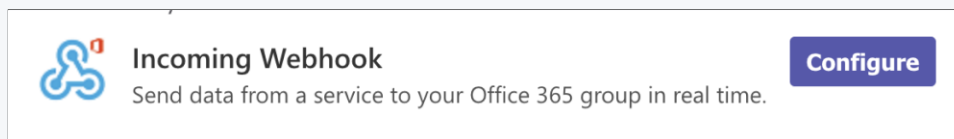
Teams



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

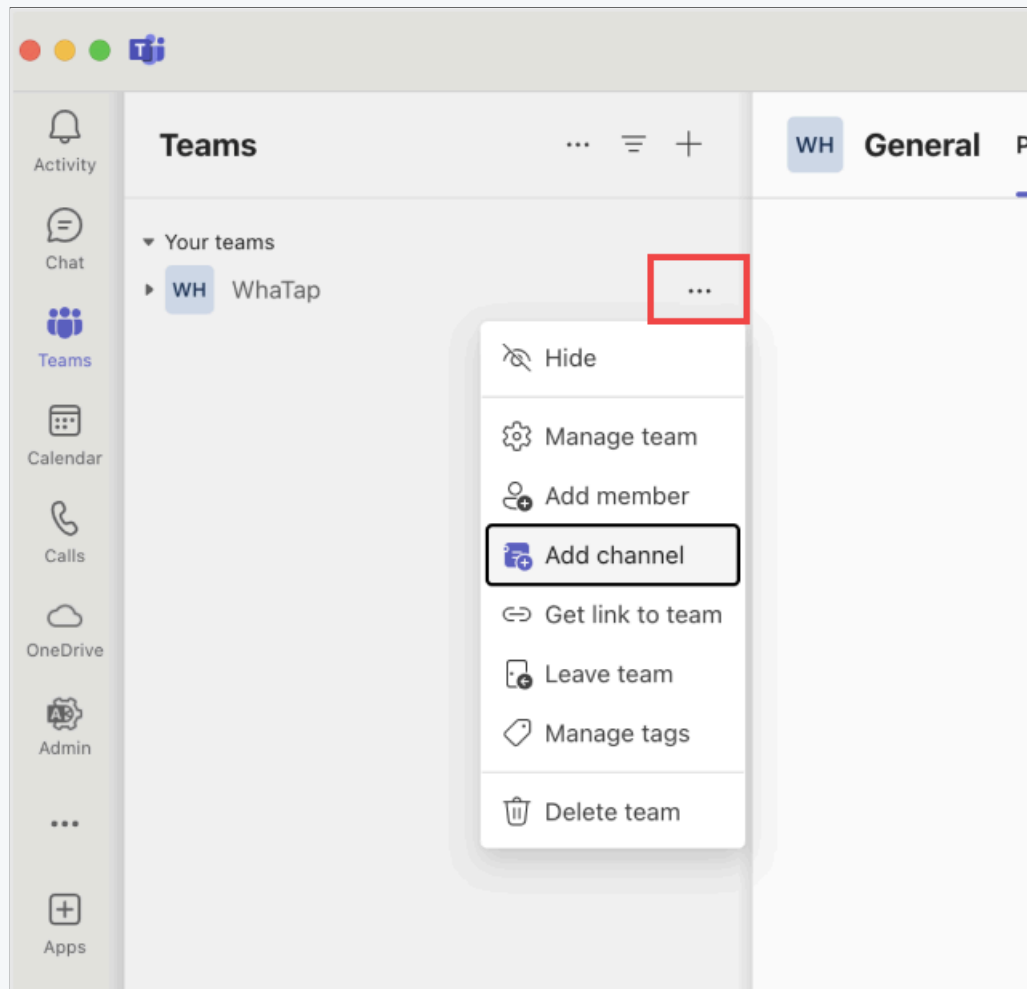
5. Return to the **Add a third-party plug-in** window in the WhaTap Monitoring service, and enter values for **Channel Name** and **Webhook URL** at the bottom of the **Teams** tab.
6. Click the [**Registration**] button.

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**.

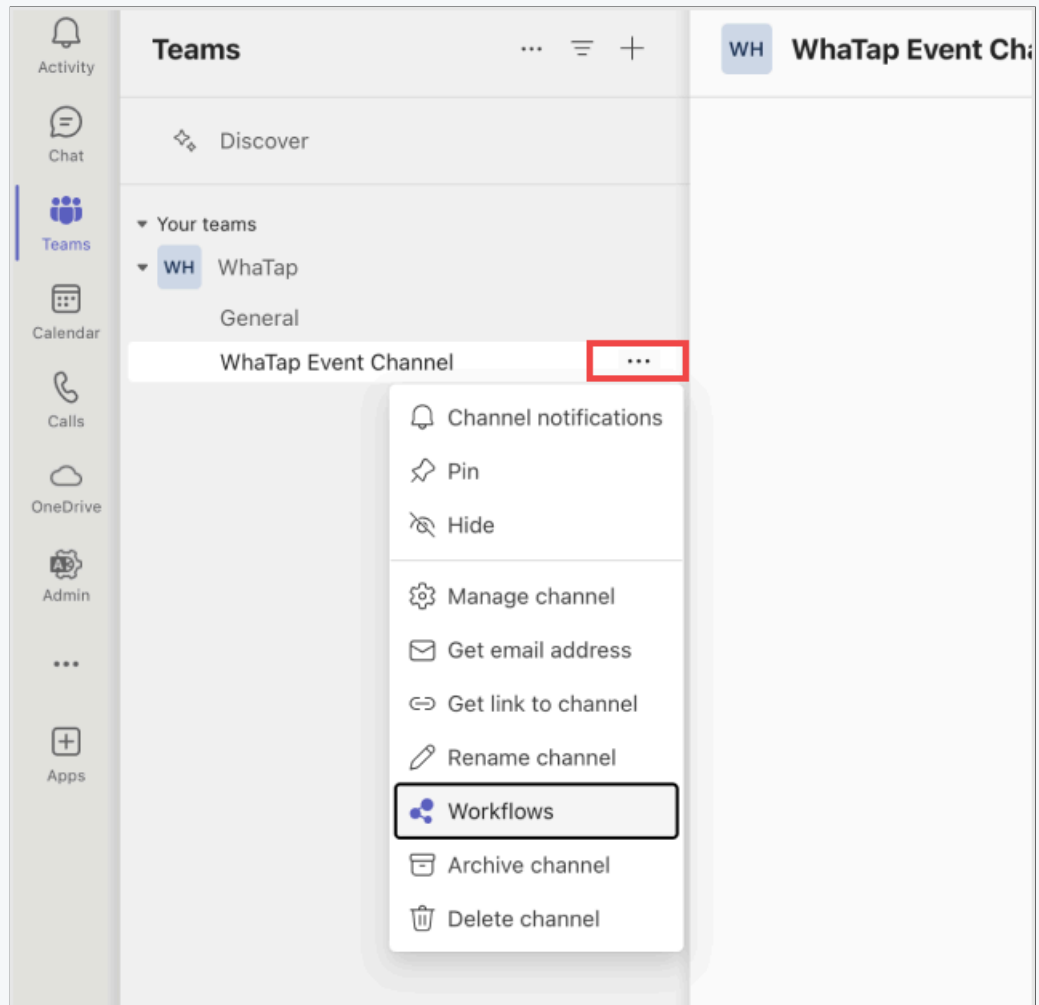


2. In the **Create a channel** window, enter the **Channel name** and **Description**. For **Channel type**, select **Standard**, then click the [Create] button.

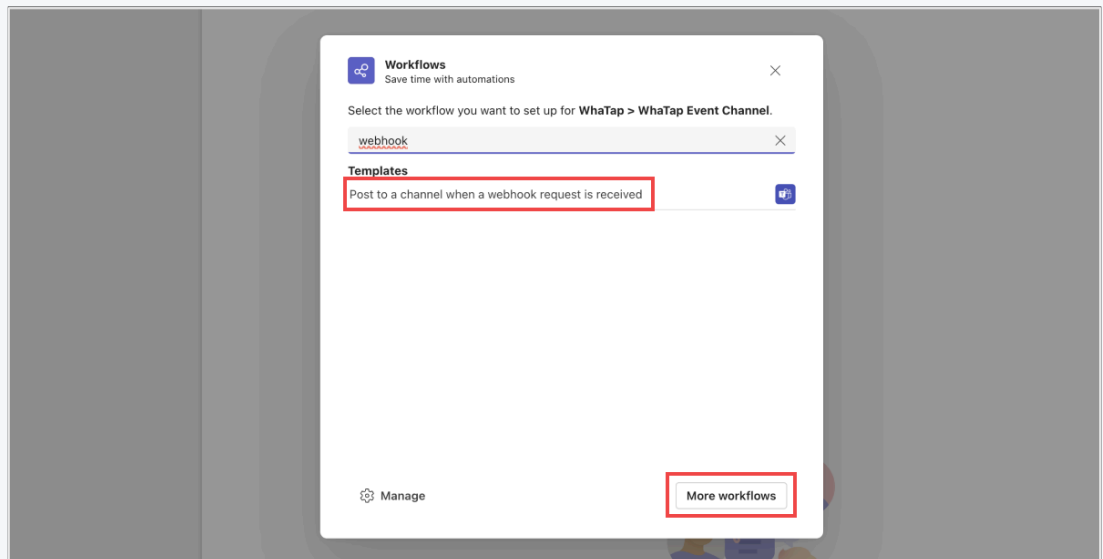


⚠ If you select **Shared** as the channel type, workflows cannot be used. If you select **Private**, workflows can be added but notifications cannot be received.

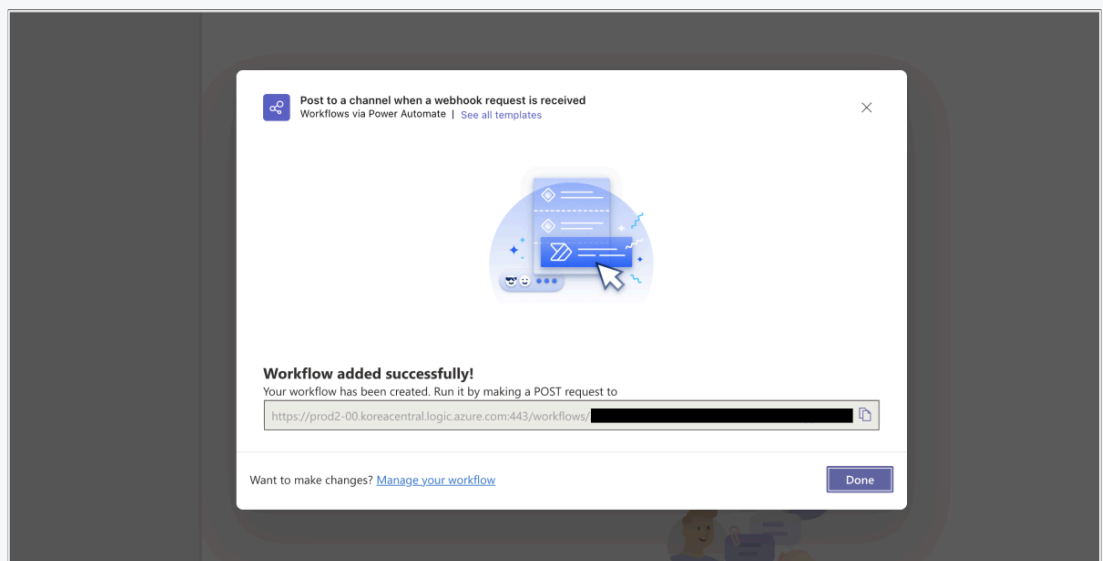
3. Click **More actions (...)** of the created channel, then select **Workflows**.



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.



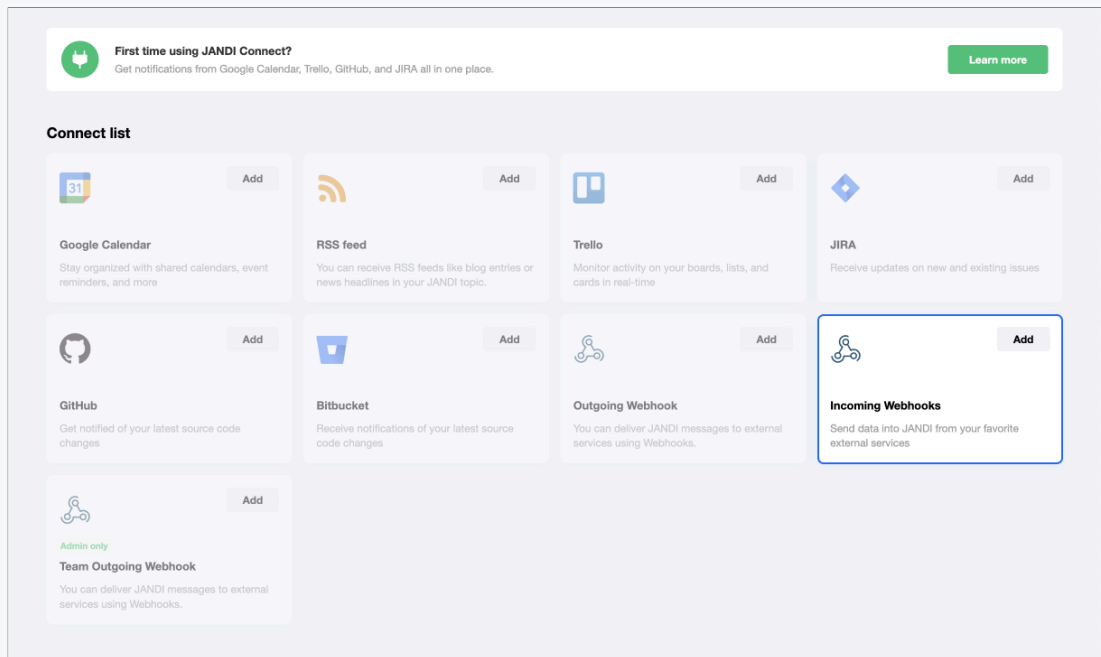
9. Click the [**Registration**] button.



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...>

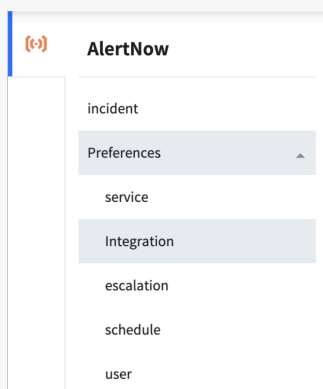
Copy

- 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}

5

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}",
}
```



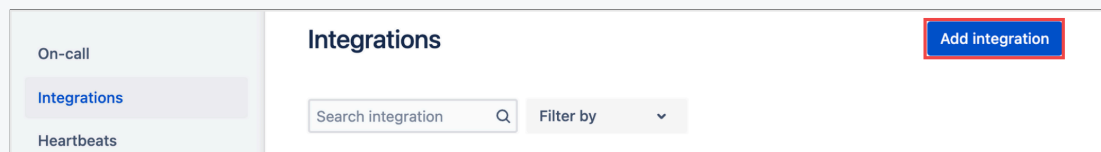
```
"metricName": "${metricName}",
"metricValue": "${metricValue}",
"metricThreshold": "${metricThreshold}",
"uuid": "${uuid}",
"okind": "${okind}",
"onode": "${onode}"
}
```

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.

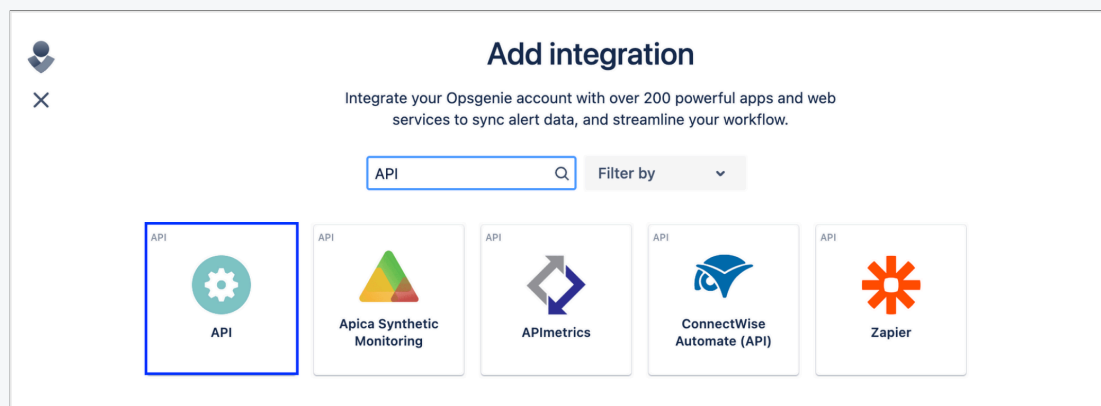
Opsgenie



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
 - **T:** 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
```

Event Pause

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

Event pause is a feature that temporarily stops event rules to limit event occurrences. Using it during periods when notifications are unnecessary, such as maintenance work or inspections, helps reduce unnecessary notifications.

 Once created, a pause rule cannot be modified, and it is automatically deleted when the configured period ends.

Screen layout

Item	Description
Active pause rules	The number of pause rules currently applied
Event pause list	The list of pause rules you created

Adding a pause rule

1. Click the **Add pause rule** button.
2. Set the target and period to pause.
3. When you save, notifications for the target event rules are stopped during that period, and the rule is automatically deleted when the period ends.

Labs

The Labs menu provides additional features for working directly with data or fine-tuning alerts beyond the default screens.

Screen layout

Screen	Description
MXQL Data Lookup	Query and visualize collected data directly with MXQL
Alert Message	Edit the items and content of event-triggered and event-resolved alert messages

MXQL Data Lookup

On the MXQL Data Lookup screen, you can query the data collected by WhaTap directly with MXQL (the WhaTap data query language). Use it to extract data in a form the default screens do not provide, or to check collected values directly.

! You can find the MXQL syntax and functions in the [MXQL Guide](#).

How to use

1. In the **Time** selector, choose the time range to query (for example, the last 1 day).
2. In the **MXQL Editor**, enter the query to run. For example, specify a category and tag in the form `CATEGORY db_real_counter TAGLOAD SELECT` to load data.
3. In the **Row Count** field, choose the number of rows to fetch at once (for example, Up to 100 lines).
4. After setting the options, run the search to display the results. Click the **Explore Metrics** button to explore the metric data as well.

Alert Messages

On the Alert Messages screen, you can select the detailed items of the message to receive when an event occurs or is resolved, and edit the content of each item. Use it to keep messages concise by including only the information essential to the alert.

Screen layout

Item	Description
Occurrence / Resolution	Edit the event occurrence message and the resolution message separately
Alert type	Compose messages separately for each alert type, such as Metrics and Composite metrics
All / Occurrence / Resolution, Search	Filter message items by state or search by name

At the top, you can manage settings in bulk with **Copy to another project**, **Reset all**, and **Save all**. Each alert type section provides **Reset**, **Preview**, **Save**, and **Enable all**.

Editing message items

For each item, you can turn its inclusion in the message on or off with the **Edit** switch, and edit the displayed content directly. The available items are as follows.

Item	Example
Status	OCCURED / SOLVED
Alert level	Warning

Item	Example
Project number / name	101 / Example Project
Agent name	Whatap-Front-01
Message	Message
Event occurrence time	2022-09-08 14:23:17 +0900
Event occurrence condition	tps > 20
Event target filtering	oid == 800488350
Resolved event notification feature	ON / OFF
Alert type / label	METRICS / oid(800488350)
Metric / current value / threshold	tps / 25 / 20
Current values (multiple)	tps=23.39, tx_error=7
Repeat count / repeat interval / silence period	5 / 5 minutes / 10 minutes
Processing history	- Disk Cleanup (20250101 08:30:00+0900, support@whatap.io)
Shortcut	https://service.whatap.io/link/event

After editing an item, use **Preview** to check the actual message format and then **Save**.