

Network Management System

release date. 2026. 09. 11.



Table Of Contents

• Network Management System	5
◦ Getting Started.....	9
◦ Installation	
■ Support Environment	11
■ Manager Installation	17
◦ Network Insights	
■ Topology.....	21
■ Device Overview	28
■ Group Navigator.....	31
■ Flex Board	37
■ Using Flex board	40
■ Managing the widgets	50
◦ Device Status	
■ Interface status	55
■ Device Trend	57
■ Health Check Status	65
◦ Device Management	
■ Device Inventory	69
■ Group Management	75
◦ Network Automation	
■ Task Configuration	79
■ Task Status	84
■ Config Changes	86
■ Preventive Profiles	90

■ Preventive Rules	93
■ Preventive Reports	96
◦ SNMP OID Management	99
◦ Alert	100
■ Event Configuration	0
■ Metrics	106
■ Composite Metrics	128
■ Real-time logs	135
■ Composite log	148
■ Event Notification Settings	162
■ Event Notification Format	184
■ Event History and Monitoring	192
■ Real-time Notifications	200
■ System Events	203
◦  	
■ Usage Analysis	206
◦ Log Monitoring	211
◦ Device Asset Management	0
◦ Configuration	
■ SNMP Trap Setting	0
■ Syslog configuration	0
■ General Config	0
◦ Analysis	
■      	0
◦ Management	

■ Manager Info	0
----------------------	---

Network Management System

A **Network Management System (NMS)** is a platform that centrally monitors network devices such as routers, switches, servers, firewalls, and wireless access points to maintain performance and stability. It provides real-time visibility into traffic, device status, and bandwidth usage, enabling quick identification of root causes when failures occur.

NMS focuses on failure prevention and problem detection to minimize performance degradation and ensure consistent service quality (QoS). By using WhaTap NMS, organizations can operate IT infrastructure efficiently and maintain business continuity.

Key advantages

- **Extensive multi-vendor support**

Based on the standard SNMP protocol, it provides strong compatibility that is not limited to specific manufacturers. From global vendors such as Cisco and Juniper to domestic equipment, it supports a flexible operating environment where all network devices supporting SNMP can be integrated and managed with a single WhaTap NMS.

- **Efficient MIB management and data retrieval**

It has a built-in intuitive MIB (Management Information Base) browser that makes it easy to check and verify vast amounts of data provided by each network device. In particular, if a specific manufacturer's private MIB or new device MIB file that is not provided by the system by default is required, it supports the ability for users to upload and manage files directly.

- **OID list provision**

It systematically selects and provides key OID (Object Identifier) items that are frequently used in operational sites in list form. It minimizes the hassle of administrators having to directly search and verify individual OIDs within complex MIB structures, and supports rapid identification and application of performance indicators essential for setting thresholds for each device and interface, maximizing management optimization and operational efficiency.

- **Flexible installation environment and hybrid infrastructure support**

It supports various operating systems (OS) to minimize installation environment constraints and provides

deployment methods optimized for customers' infrastructure environments such as on-premise and cloud. Through this, an uninterrupted monitoring system can be built not only in closed internal networks but also in complex hybrid cloud environments, and it supports flexible deployment models optimized for corporate security policies and network structures.

Key features

- **Device and performance real-time monitoring (SNMP Polling)**

It periodically collects key operational indicators and performance data of network devices to maintain optimal operating conditions. It precisely monitors the status of hardware resources such as CPU load, memory usage, and session occupancy, and identifies the data inflow/outflow (Throughput) for each interface and the physical connection status (Link Up/Down) of ports in real time to prevent network performance bottlenecks in advance.

- **Hierarchy structure and topology map (Hierarchy & Topology)**

It provides management intuitiveness by visualizing the affiliation and connection status of network assets. While organizing devices into tree structures by region, building, and business service units, the overall network configuration and the scope of impact in case of failure can be immediately identified by implementing the physical and logical connection relationships between devices as a topology map.

- **Availability and quality check (Health Check)**

It constantly checks whether network devices and operating services are operating normally based on responsiveness. It confirms the real-time survival (Alive) of devices through ICMP (Ping) and TCP protocols, and manages to ensure that user service quality (SLA) does not deteriorate by analyzing response time (RTT) and network delay variation (JITTER) values.

- **Real-time event and log management**

It analyzes SNMP Trap and Syslog messages generated from devices in real time to immediately deliver failure situations to administrators, and supports an analysis environment where the cause of failure at a specific point in time can be precisely searched and tracked based on the stored event history.

- **Auto Discovery**

The system identifies itself without the hassle of manually registering complex and vast network environments one by one. It utilizes the SNMP protocol to scan devices within the network and automatically

database device types, interface configurations, and detailed specifications to shorten the initial construction time.

Data collection scope

WhaTap NMS (Network Management System) supports the following network data collection methods.

- **SNMP Polling**

It periodically requests and collects network device status and performance data and supports all `SNMP v1/v2c/v3` protocols.

- **SNMP Trap**

It collects and processes event and notification information generated from network devices and supports `SNMP Trap v1/v2c/v3` protocols.

- **Syslog**

It collects log data generated from network devices and analyzes it in real time.

- **ICMP**

It measures **Alive**, **RTT**, **Jitter**, etc. of devices using the ICMP protocol.

- **TCP**

It measures **Alive** and **RTT** of devices or services based on TCP ports.

Manager main services

NMS collects and refines agent data from the manager and performs pre-configuration and testing before integration with WhaTap.

Web-based Management Console & APIs

`uicorn.service` is a management UI and API service that provides overall operational management functions such as NMS configuration management, system status check, and configuration backup and recovery in a local

environment.

ⓘ Generally, manager access is not required for NMS operation. If access is required, please contact the WhaTap technical team.

- **Ports used:** HTTP 5000, HTTPS 8443 (when configured)
- **Service start and stop:** You can start, stop, or restart `uvicorn.service` with the following command.

```
systemctl {start|restart|stop} uvicorn.service
```

NMS engine

`nmscore.service` is a service that acts as the engine of the Network Management System (NMS). It provides network device and traffic monitoring, management, and event processing functions.

- **Ports used:**
 - **SNMP Polling:** UDP 161 (default)
 - **SNMP Trap:** UDP 162 (default)
 - **Syslog:** UDP 514 (default)
- **Service start and stop:** You can start, stop, or restart `nmscore.service` with the following command.

```
systemctl {start|restart|stop} nmscore.service
```

Health Check

`icmptcphealthd.service` performs ICMP and TCP-based Health Check on network devices and continuously monitors device availability and connection status through periodic status checks.

- **Service start and stop:** You can start, stop, or restart `icmptcphealthd.service` with the following command.

```
systemctl {start|restart|stop} icmptcphealthd.service
```


Getting Started

This guide walks you through the steps required to start WhaTap monitoring.

[Step 1. Sign up](#)

[Step 2. Select a product](#)

[Step 3. Create a project](#)

After checking the supported environment, proceed to the [Manager Installation](#) step.

Step 1. Sign up

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

Step 2. Select a product

1. Log in to [WhaTap Monitoring Service](#).
2. Click  **All Projects** > **+ Project**.
3. In the **Select product** screen, click the **Create** button for the product you want to monitor.

Step 3. Create a project

Once you have selected the product to monitor, create a project before installing the agent.

1. In the **Create project** screen, enter or select the following items to create a project.
 - **Project name** (required): Enter the name of the project.
 - **Data server region** (required): Select the region where the data server is located. A region is a collection of data centers that provide cloud services. Your data is stored in the selected region.
 - **Time zone** (required): Set the standard time for notifications and report generation.

- **Notification language setting** (required): Set the language for alert notification messages generated in the project. (Korean and English supported)
 - **Project groups**: You can group multiple projects together for management. If there is a group to belong to, select it. If not, you can add a group by clicking the Add Group button.
 - **Project description**: Enter an additional description for the project.
2. After completing all settings, click the **Creating a project** button.

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

Support Environment

WhaTap Network Control Management System is installed on a standalone virtual machine (VM) in a standalone manner. This allows the network management system to operate independently and reliably provide all the features required for network monitoring and management.

System requirements

The following are the recommended minimum specifications to ensure stable performance of the WhaTap Network Management System.

Item	Specification
CPU	4 core (minimum 2 core)
Memory	Minimum 16GB or more (minimum 8G)
Disk	50G or more SSD recommended (minimum 30G)
Network Interface	1Gbps or more

OS support

OS	Python version	Support status
Ubuntu 22.04	3.10	Supported, Recommended
Ubuntu 23.04	3.11	Supported
Ubuntu 24.04	3.12	Supported
Rocky 9.4	3.9	Supported, Recommended

OS	Python version	Support status
Rocky 8.10	3.11	Supported
Redhat 8.10	3.11	Supported, Recommended

Python version support

Support is available depending on the Python version regardless of the OS type. However, it is recommended to use the recommended OS whenever possible.

Family	Supported Python versions
Debian family	Python 3.10, 3.11, 3.12
Redhat family	Python 3.9, 3.10, 3.11, 3.12

TCP/UDP ports used

The specified TCP and IP port numbers are the default ports used by the service and can be changed to suit the customer's environment.

Category	TCP	UDP	Description	Direction	Notes
SNMP	-	161	polling	Outbound	Default port
SNMP Trap	-	162	trap message	Inbound	Default port
syslog	-	514	syslog message	Inbound	Default port
manager U/I	5000(http) 8443(https)	-	NMS Control Manager GUI	Inbound	Default http, requires port 8443 permission when using https

Category	TCP	UDP	Description	Direction	Notes
whatap collection server	6600	-	Data transmission	Outbound	-
ICMP	-	-	ICMP health Check	-	ICMP protocol permission required
TCP	-	-	TCP-based health Check	In/Out	Monitoring target TCP port number connection permission required (Options)

Service deployment models

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

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

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

Feature differences by deployment model

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

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

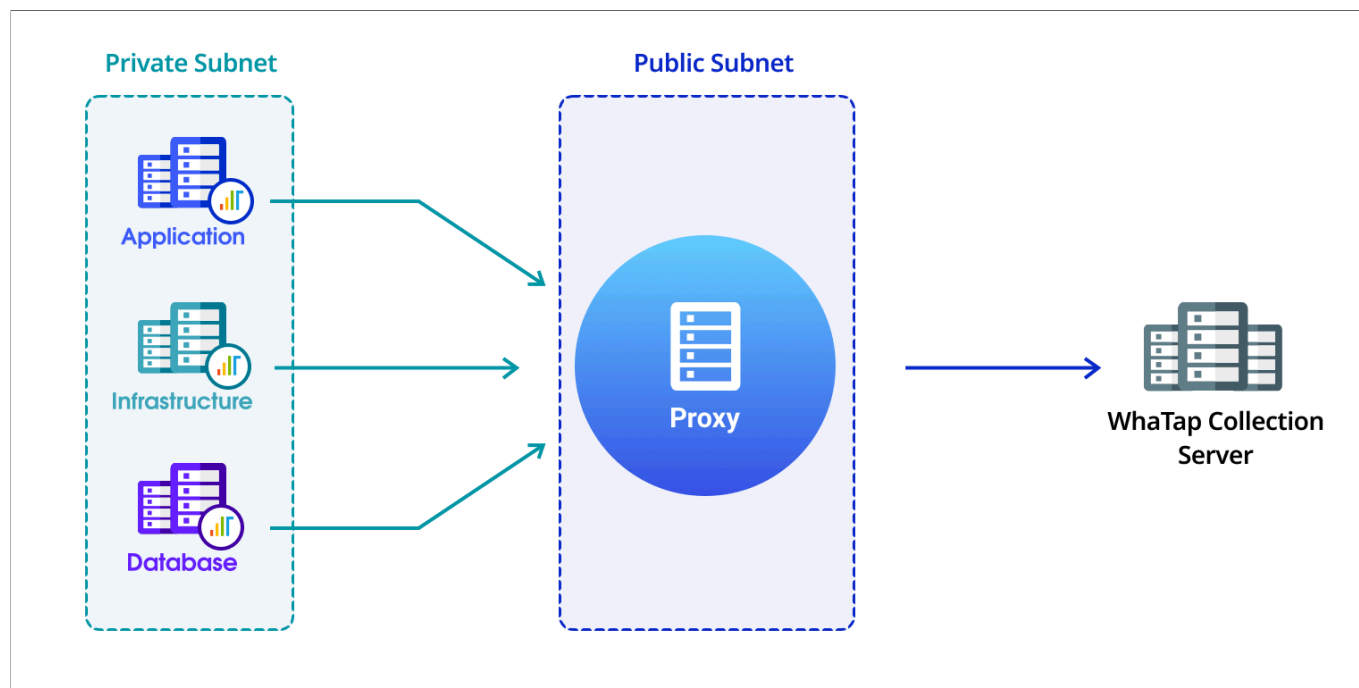
Firewall

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

Source: WhaTap agent

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

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



Main service components and ports

NMS Control Manager Web-Based U/I

`uvicorn.service` is a management UI and API service that runs in a local environment, providing overall operational management functions such as NMS configuration management, system status check, and configuration backup and recovery.

- **Ports used:** HTTP 5000, HTTPS 8443 (when configured)
- **Service start and stop:** You can start, stop, or restart `uvicorn.service` with the following command.

```
systemctl {start|restart|stop} uvicorn.service
```

ⓘ Please contact the **WhaTap technical team** for manager access information.

NMS engine

`nmscore.service` is a service that acts as the engine of the Network Management System (NMS). It provides network device and traffic monitoring, management, and event processing functions.

- **Ports used:**
 - **SNMP Trap:** UDP 162 (default)
 - **Syslog:** UDP 514 (default)
- **Service start and stop:** You can start, stop, or restart `nmscore.service` with the following command.

```
systemctl {start|restart|stop} nmscore.service
```

Health Check

`icmptcphealthd.service` performs ICMP and TCP-based Health Check on network devices and continuously monitors device availability and connection status through periodic status checks.

- **Service start and stop:** You can start, stop, or restart `icmptcphealthd.service` with the following command.

```
systemctl {start|restart|stop} icmptcphealthd.service
```


Manager Installation

This guide explains how to install the **NMS Manager**, the agent for **WhaTap NMS (Network Management System)**. Before proceeding with the installation, be sure to check the following.

 Before installing the manager, **WhaTap sign up** and **project creation** must be completed. For more information, see the [Getting Started](#) document.

- System requirements can be found in the [Supported Spec](#) document.

Manager installation

Check the project access key

The **access key** is a unique ID for activating the WhaTap service. After automatically receiving the **access key**, proceed to the next step.

1. In the installation guide section, click the **Getting the access key** button.
2. Copy the issued access key by clicking the **Copy** button. The access key can be reconfirmed.

 After creating a project, it automatically moves to the **Agent installation** page. If you do not move to the **Agent installation** page, select **Management > Manager Installation** from the left menu on the screen.

Run the installation command

After checking the project access key in the **Management > Manager Installation** guide section, proceed with the installation suitable for the operating system in order.

Red Hat-based Linux

ⓘ WhaTap Network Management System supports Rocky and Redhat Linux environments.

1. Run the following command to register the WhaTap **repository**.

```
sudo rpm --import https://repo.whatap.io/centos/release.gpg
sudo rpm -ivh https://repo.whatap.io/centos/5/noarch/whatap-repo-1.0-1.noarch.rpm
```

2. Run the following command to install the **package**.

```
sudo dnf install -y whatap-nms
```

3. Run the following command. Enter the **access key** and set the WhaTap server **host**.

```
$ sudo wtinitset -a xxxxxxxx-xxxxxxx-xxxxxxx -s 192.168.10.100

$ sudo wtinitset --help
usage: wtinitset [-h] -a LICENSE -s HOST [-v]

Whatap-nms access key manager tool

optional arguments:
-h, --help            show this help message and exit
-a LICENSE, --accesskey LICENSE
                        Access key for project
-s HOST, --server HOST
                        Whatap host ip address for data transfer
-v, --view            View current configuration

example:
# wtinitset -a znun32arkonto-76rbkt4ftlrwh9-s0dywogeww1lhs -s 192.168.10.100
# wtinitset -a znun32arkonto-76rbkt4ftlrwh9-s0dywogeww1lhs -s 10.10.10.10/10.10.10.20
```

4. After installation is complete, run the following command to check if the NMS manager is running normally.

```
sudo service uvicorn status
sudo service nmscore status
sudo service icmptcphealthd status
```

Debian-based Linux

ⓘ WhaTap Network Management System supports Ubuntu environment.

1. Run the following command to register the WhaTap **repository**.

```
curl -s https://repo.whatap.io/debian/release.gpg | gpg --dearmor | sudo tee /etc/apt/trusted.gpg.d/whatap-
release.gpg > /dev/null
echo "deb [signed-by=/etc/apt/trusted.gpg.d/whatap-release.gpg] https://repo.whatap.io/debian unstable/" |
sudo tee /etc/apt/sources.list.d/whatap.list
```

2. Run the following command to install the **package**.

```
sudo apt-get update
sudo apt-get install -y whatap-nms
```

3. Run the following command. Enter the **access key** and set the WhaTap server **host**.

```
$ sudo wtinitset -a xxxxxxxx-xxxxxxxx-xxxxxxx -s 192.168.10.100
```

```
$ sudo wtinitset --help
usage: wtinitset [-h] -a LICENSE -s HOST [-v]
```

Whatap-nms access key manager tool

optional arguments:

-h, --help show this **help** message and **exit**

-a LICENSE, --accesskey LICENSE

Access key *for* project

-s HOST, --server HOST

Whatap **host ip** address *for* data transfer

```
-v, --view      View current configuration
```

example:

```
# wtinitset -a znun32arkonto-76rbkt4ftlrwh9-1234ogeww1lhs -s 192.168.10.100
```

```
# wtinitset -a znun32arkonto-76rbkt4ftlrwh9-1234wogeww1lhs -s 10.10.10.10/10.10.10.20
```

4. After installation is complete, run the following command to check if the NMS manager is running normally.

```
sudo service uvicorn status
```

```
sudo service nmscore status
```

```
sudo service icmptcphealthd status
```

NMS service access

Once the installation is complete, access <https://service.whatap.io> to start NMS monitoring.

Topology

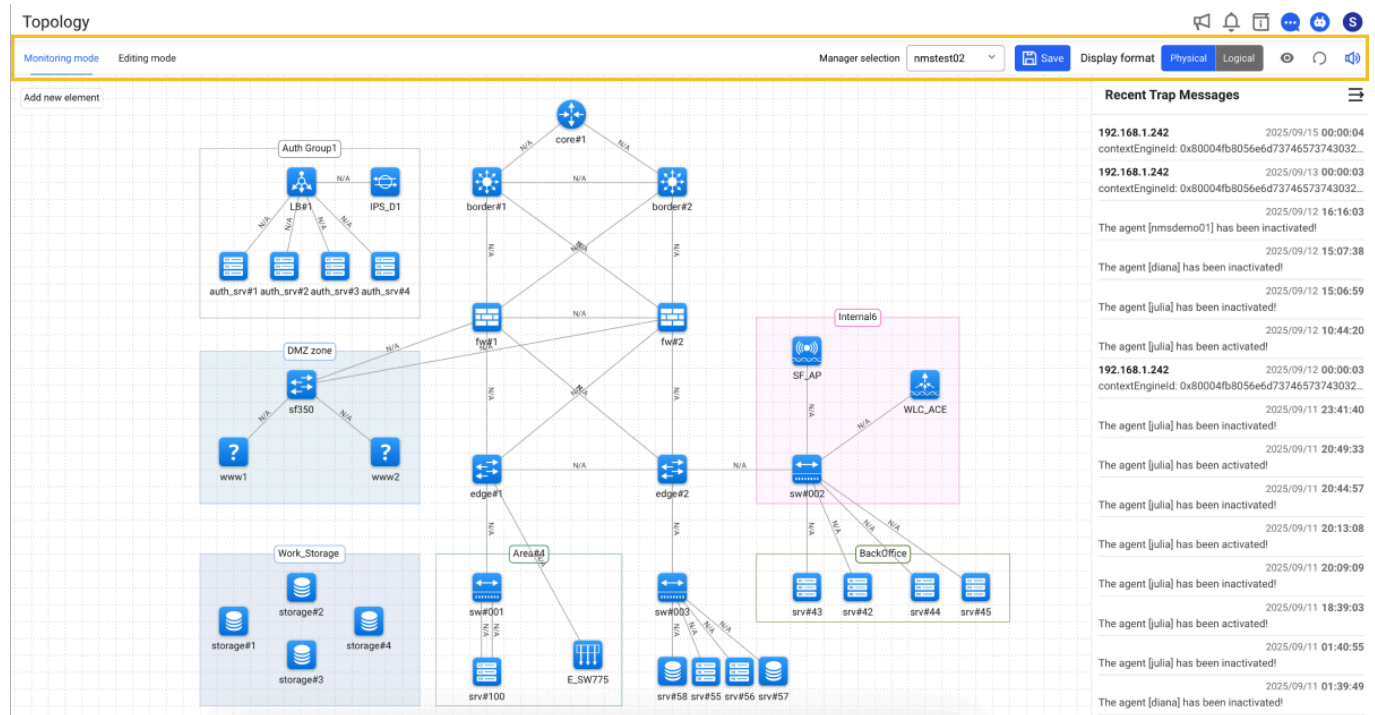
The **Network Insights Topology** view provides a visual representation of network devices and link structures.

It not only shows the structure but also immediately reflects real time events such as link down, allowing administrators to quickly understand the network status. Topology provides two modes.

- **Monitoring mode:** view mode to check the entire network structure and monitor real time events
- **Edit mode:** create areas, or add, delete, edit nodes, and connect links to manage screen layout

Basic screen and settings

At the top of the topology screen, you can switch modes, select managers, change display formats, and access other main control functions.



Menu	Description
Mode selection	Choose the Monitoring mode or Edit mode tab - Monitoring mode: view mode to check the entire network structure and monitor real time events - Edit mode: create areas or add, delete, edit nodes, and connect links
Manager selection	Select the connected NMS manager
 Save	Save the positions of devices and areas adjusted by the user
Display type	Switch between Physical and Logical topology - Physical: view all ports actually connected between devices - Logical: focus on logical connection structures between devices
	Choose whether to show node IPs
	Restore all screen settings to default
	Toggle ON / OFF to play a sound when an anomaly occurs in the topology

Topology Map icons

Icon	Node type	Description
	Router	Device that routes network traffic to other networks
	L3 Switch	Layer 3 switch with routing capabilities
	L2 Switch	Layer 2 switch, data link layer device supporting VLAN etc.
	Firewall	Security device that filters network traffic

Icon	Node type	Description
	Load Balancer	Load balancing device that distributes traffic across multiple servers
	Hub	Simple network distribution device (non-intelligent)
	IPS	Intrusion Prevention System
	WAF	Web Application Firewall
	WLC	Wireless LAN Controller
	Access Point	Wireless access point
	Server	Server that provides services or data
	Storage	Data storage device (NAS, SAN, etc.)
	IP Phone	VoIP-based voice communication device
	Appliance	Purpose-built network device (e.g., Proxy, UTM, etc.)
	Unknown	Unclassified or unidentified device

Common functions

- **Pan:** drag an empty area of the screen to move the view
- **Zoom in/out:** use the mouse wheel to zoom in or out

Monitoring mode

In monitoring mode, you can view the network structure in real time and immediately detect event changes.

1. Go to **Network Insights > Topology**.
2. Click the **Monitoring mode** tab to view the main topology view and Recent Trap Messages.

Main topology view

- Network devices are displayed as icons, with icon shapes differing depending on the device type such as router, switch, and firewall.
- Connections between devices are displayed as lines, with styles depending on status.
 - Normal (gray solid line)
 - When throughput is present, data flow is displayed as an animation via SNMP settings. SNMP configuration is required.
 - Link down (red solid line)
- If a device is powered off or disconnected from the network, a warning icon (⚠) is displayed so you can immediately check the status.
- A custom feature to group devices by area is provided.

Recent Trap Messages

The right panel displays trap messages collected in real time in sequence. You can check device and link events in **text log format**.

- Example: specific link down, device activation or deactivation

Edit mode

In the **Edit mode** tab, you can add/edit nodes, areas, and links.

1. Go to **Network Insights > Topology**.
2. Click the **Edit mode** tab, then select the desired mode from the right side of the screen to edit.
 -  Topology Edit: Modify mode
 -  Add Device: Add device mode
 -  Add Area: Add area mode
 -  Add Link: Add link mode

Modify mode

In Modify mode, you can edit placed elements.

- You can drag nodes and areas to change their positions.
- Click an element to edit its properties.

Edit area

You can edit the properties of created areas.

- You can change the **background color** and **border color** of the area for easier visual distinction.
- Click the  icon to enter or change the area name.
- To remove an unnecessary area, click the  **Delete** button.

Edit node

When you select a network device (node), you can edit its name and device type.

- Click the  icon to enter or change the network node information.
- To delete a node, click the  **Delete** button.
- Available device types: router, switch, hub, host, ap, phone, firewall, unknown

Add device mode

In Add device mode, you can add nodes to the topology. Select the device type and click on an empty space in

the topology to add a node.

Add area mode

In Add area mode, you can add new areas to the topology. Drag the empty space in the topology to add a new area.

Add link mode

In Add link mode, you can connect nodes to each other. Click one node, then click another node to create a link.

Edit history

In **Edit History** on the right of the top option bar, you can undo or redo the tasks performed with the edit tools.

Item	Description
Undo	Cancels the previous edit. Shortcut <code>Ctrl+Z</code>
Redo	Reapplies the canceled edit. Shortcut <code>Ctrl+Shift+Z</code> or <code>Ctrl+Y</code>

If there is nothing to undo, each button is displayed as disabled.

- Reversible tasks: adding, editing, and deleting areas; dragging and resizing nodes and areas; adding, moving, and deleting page guides
- Irreversible tasks: adding, modifying, and deleting nodes and links (applied to the server immediately on save); panning and zooming

ⓘ The edit history keeps up to 50 steps and does not work while dragging. Changes to the same target that occur consecutively within a short time are grouped into one step.

Auto-rotation playback bar

When the topology is divided into multiple sections, the auto-rotation playback bar is displayed. On the playback bar, you can control both moving between sections and auto-rotation.

Item	Description
Page display	Shows the number of sections and the current position. Selecting an item moves to that section immediately
Play/Stop	Starts or stops auto-rotation. The current interval (seconds) is displayed at the top right of the icon
Interval selection	Selects the auto-rotation interval. The presets are 3, 5, 10, and 30 seconds, and direct input ranges from 1 to 120 seconds
Progress bar	Shows the time remaining until moving to the next section

The playback bar is displayed only when there are two or more sections.

Device Overview

Device Overview is a dashboard composed of [Common options](#) and [Widgets](#). It provides an at-a-glance view of the status and performance metrics of network devices in a project. Administrators can check key operational data such as interface status, traffic handling, HealthCheck, Syslog, Trap events, and real time logs in widget form.

ⓘ **Device Dashboard** is a real-time dedicated monitoring screen and does not provide the feature to select and view a past specific time point.

Common options

These features apply across the entire Overview screen and allow you to set the data query range, select managers, and save widget layouts.

- **Select preset:** load a saved widget layout and use it in the same arrangement
- **Save preset:** save the current screen configuration for later reuse
- **Widget management:** add, delete, rearrange, and resize widgets
 - **Delete widget:** right click on the widget you want to delete and click the **Delete** button
 - **Add widget:** right click on empty space and select the widget you want to add

Widgets

You can intuitively check network status through the various widgets displayed on the dashboard.

Device status

The number of active interfaces is displayed as **Connected / Total Interfaces**, allowing you to check how many interfaces are active. When you hover over a device, status information appears. When you click a device, the view opens **Interface status** if interface information is available; if not, it moves to **Usage Status**.

- Example: 8 / 22 → 8 active out of 22 total

! Interface information requires collecting SNMP ifTable (1.3.6.1.2.1.2.2) or ifXTable (1.3.6.1.2.1.31.1.1) data. Support may vary by device.

HealthCheck

The HealthCheck widget displays network jitter and maximum round trip time (Max RTT) in a graph. If the status is abnormal, the corresponding IP address is shown in red. Monitoring results are updated in 10 minute intervals.

1. Go to **Device inventory** and click the  icon of the device you want to configure.
2. In the device settings screen, configure it under the **Health Check** tab.

Today's Syslog

Syslog events generated today are displayed in a pie chart by severity level, categorized from Emergency to Debug. This lets you intuitively check log frequency and severity distribution.

Top 10 devices by Trap events

Displays the devices with the most Trap messages in the last 24 hours, sorted in descending order by event frequency. This helps quickly identify devices with concentrated events.

Maximum throughput interface

Displays the interface with the maximum throughput recorded in the last 24 hours, sorted in descending order by traffic volume.

- Example: 41.09 Mbps (FastEthernet8, 2025-08-27 16:50:36)

Maximum PPS interface

Displays the interface with the maximum Packets Per Second (PPS) recorded in the last 24 hours.

- Example: 5.56K PPS (FastEthernet8, 2025-08-27 16:50:36)

Real time log events

Logs generated in the project are displayed in a real time table showing time, host, and log details. New logs appear instantly in live tail format. By analyzing logs in real time, you can quickly detect system failures and abnormal signs.

Group Navigator

In **Group Navigator**, you can browse network devices and interfaces in a hierarchical structure and check performance metrics in real time. Drill down in the order of  **Site** →  **Building** →  **Floor** →  **Device** →  **Interface**, and visualize traffic, status, and error information for each level.

In **Group Navigator**, you can monitor network status in real time through the following tasks.

- Navigate quickly to a desired location
- Check device and interface status summaries for each hierarchy level
- Analyze traffic and error metrics in detail for devices or interfaces

Basic screen and settings

Set query conditions in the top option bar of the **Group Navigator** screen, and select monitoring targets in the left panel.

Time selection

In the top option bar **Time selection**, you can set the query time range.

 **LIVE** mode refreshes data every 5 seconds and allows queries for up to 31 days. The default live range is 1 hour.

Select Manager

In the top option bar **Select Manager**, select the NMS manager that collects data to check performance metrics.

Group Selection

The **Group Selection** panel allows you to navigate the hierarchy in a tree structure:  Site →  Building →  Floor →  Device →  Interface.

Item	Description
— Collapse all	Collapse the entire tree
+ Expand all	Expand the entire tree
☰ / ☱	Close/open panel

Breadcrumb navigation

Breadcrumb navigation is displayed. The path of the selected node is shown at the top. Click each path to navigate to a higher level.

- Example: Site A > Building 1 > Floor 2 > Device-001

! The current selection position is saved as a URL parameter (`nodeKey`) and can be bookmarked or shared.

Group level summary

Item	Description
Devices	Total number of devices within the selected scope
Interfaces	Total number of interfaces within the selected scope
Group card	Shows the number of devices/interfaces per subgroup; click to drill down into that group

Checking device status and traffic information

When you select a specific device, you can check the status and traffic information of the interfaces belonging to that device.

Filter options

You can toggle the **Hide Logical Interfaces** and **Hide Unused Interfaces** options in the upper right of the screen.

Item	Description
Hide Logical Interfaces	Hides logical interfaces such as VLAN and Loopback from the list; shows only physical ports (ethernetCsmacd, fastEther, etc.)
Hide Unused Interfaces	Hides interfaces with no traffic during the query period from the list

! Filter settings are saved in the browser and retained for the next session.

Interface summary panel

Item	Description
Total	Total number of interfaces
Link Up	Number of interfaces with active links
Link Down	Number of interfaces with disconnected links
Admin Down	Number of interfaces disabled by administrator

! Click each status count to display a **detail list modal**. The modal shows a list of interfaces with that status.

Charts

Chart name	Description
Peak Throughput Interface (Time Range)	Interface with the highest traffic during the query period and its trend; click to navigate to that interface
Peak Throughput Interface (Current)	Interface with the highest traffic at the current time and its trend
Total Throughput	Overall device traffic trend (Line Chart)
Throughput (Inbound / Outbound)	Inbound/outbound traffic trend per interface; color-coded per interface (Stacked Line Chart)
Inbound by Interface	Comparison of inbound traffic per interface (Horizontal Bar Chart)
Outbound by Interface	Comparison of outbound traffic per interface (Horizontal Bar Chart)

Interface Status

Column	Description
Status	Interface status icon ( Connected,  Link Down,  Admin Down,  Unavailable)
Interface	Interface name and ifIndex
Link Status	Link connection status (up/down)
Admin Status	Admin status (up/down)
Inbound	Inbound traffic (Kbps)
Outbound	Outbound traffic (Kbps)

Column	Description
Inbound PPS	Inbound packets per second
Outbound PPS	Outbound packets per second
Utilization	Bandwidth utilization (%)
Error Ratio	Error ratio (%)
Max Link Speed	Maximum interface speed
Interface Type	Interface type (e.g., ethernetCsmacd)
Last Seen Time	Time of last data received

Analyzing interface performance metrics

When you select a specific interface, you can check detailed performance metrics for that interface.

NMS group-navigator

Interface information

Item	Description
ifIndex	Interface identification number
Link Status	Link status badge (Link Up / Link Down / Admin Down)
Admin	Admin status (UP/DOWN)
Oper	Operational status (UP/DOWN)
Speed	Interface speed (e.g., 1Gbps)

Item	Description
Type	Interface type (e.g., ethernetCsmacd)

Charts

Chart name	Description
Throughput (Inbound / Outbound)	Inbound/outbound traffic time-series graph (Stacked)
Packets Per Second (In/Out)	Packets per second time-series graph
Errors (In/Out)	Inbound/outbound error occurrence trend

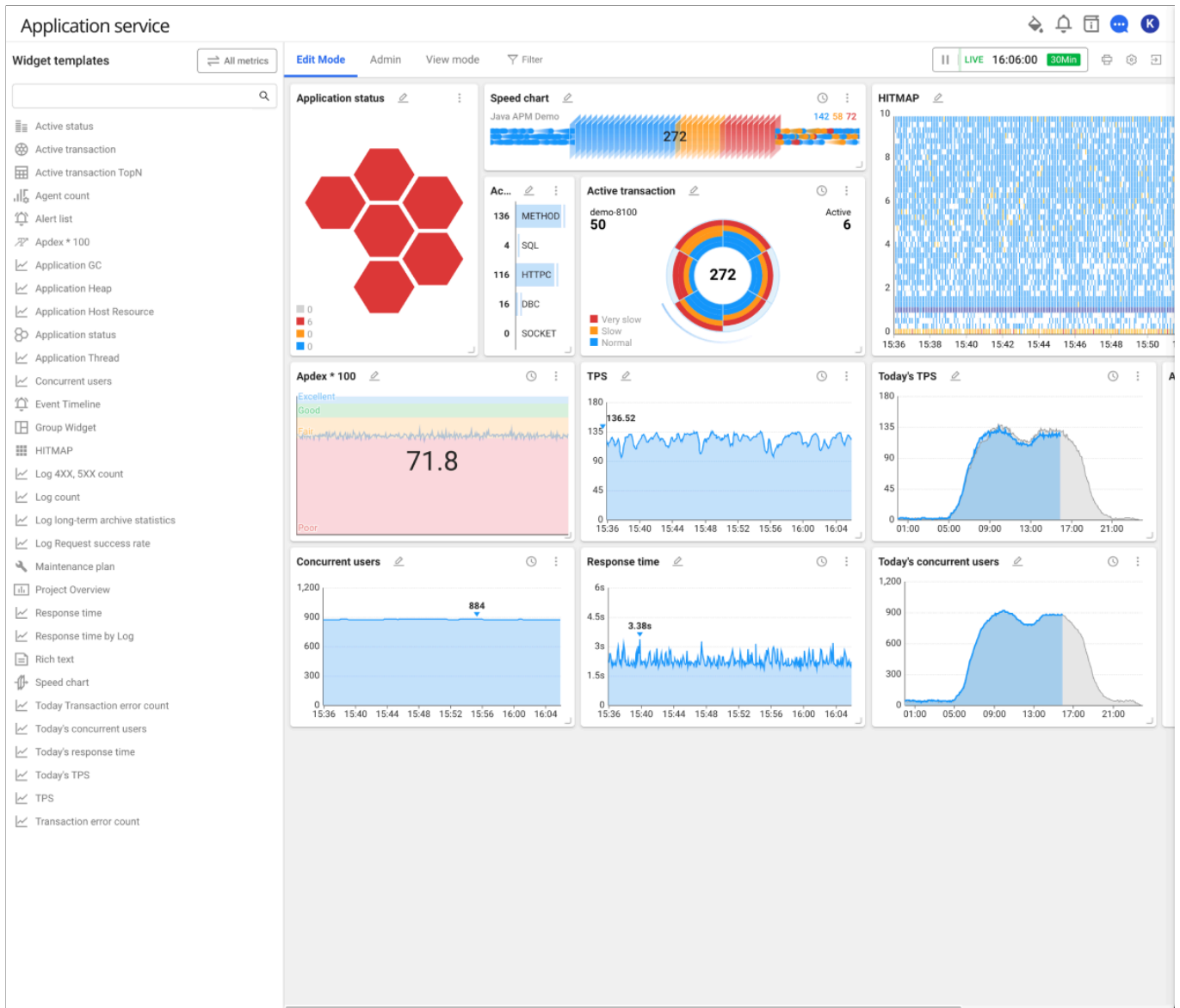
Statistics cards

Category	Item	Description
Total Throughput	Current / Max / Avg	Current, maximum, and average values of total traffic (Kbps)
Inbound Throughput	Current / Max / Avg	Inbound traffic statistics
Outbound Throughput	Current / Max / Avg	Outbound traffic statistics
PPS In	Current / Max / Avg	Inbound packets per second statistics
PPS Out	Current / Max / Avg	Outbound packets per second statistics
Error In	Current / Max / Avg	Inbound error statistics
Error Out	Current / Max / Avg	Outbound error statistics

Flex Board

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

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



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

Home > Integrated Flex Board

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

Home > Select Project > Dashboard > Flex Board

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

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

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

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

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

Using Flex Board

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

Apply a preset template

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

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

Create a Flex board

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

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

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

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

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

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

Edit a Flex board

! Flex board edit permissions

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

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

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

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

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

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

Delete a Flex board

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

 Dashboard deletion behavior differs for owners and shared users.

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



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

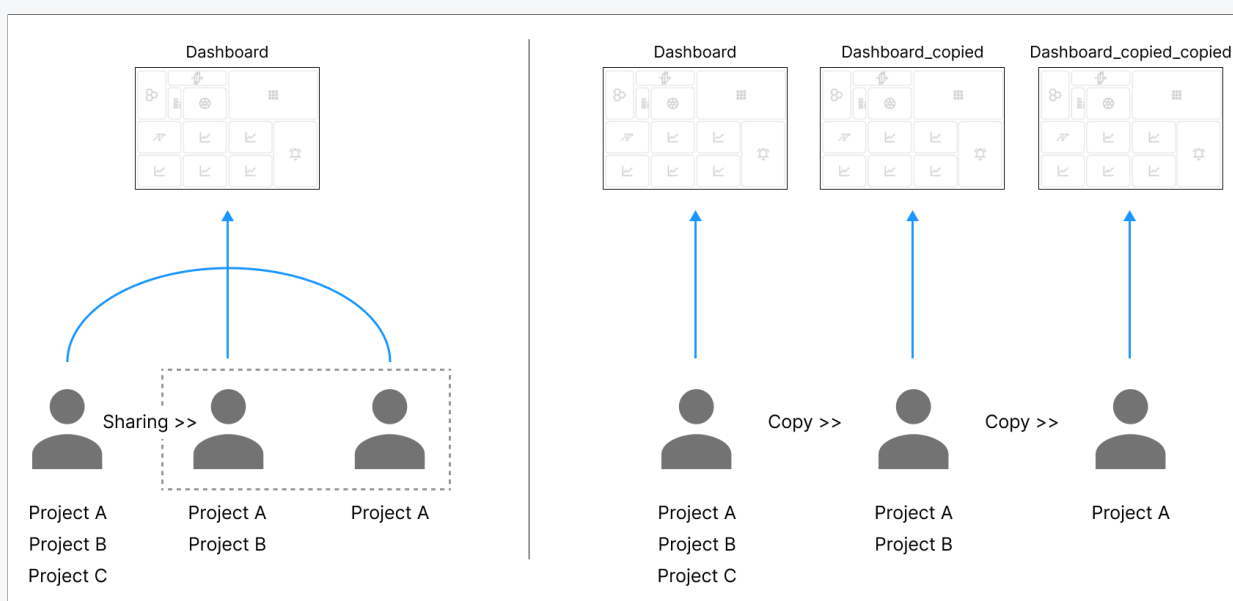
Share a Flex board



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



Difference between share and copy



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

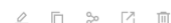


- You can share a dashboard only with members who belong to at least **one** of the projects included in the dashboard. Check whether the member to share or copy to belongs to the relevant project.

☆ 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 The Widgets

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

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

Adding a widget

You can add any widget to the created Flex board.

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

Changing the widget attributes

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

Changing the widget name

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

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

Time Setting

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

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

Setting the output data options

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

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

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

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

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

Changing the metrics widget data

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

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

Data merge options

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

- **Object Merge**

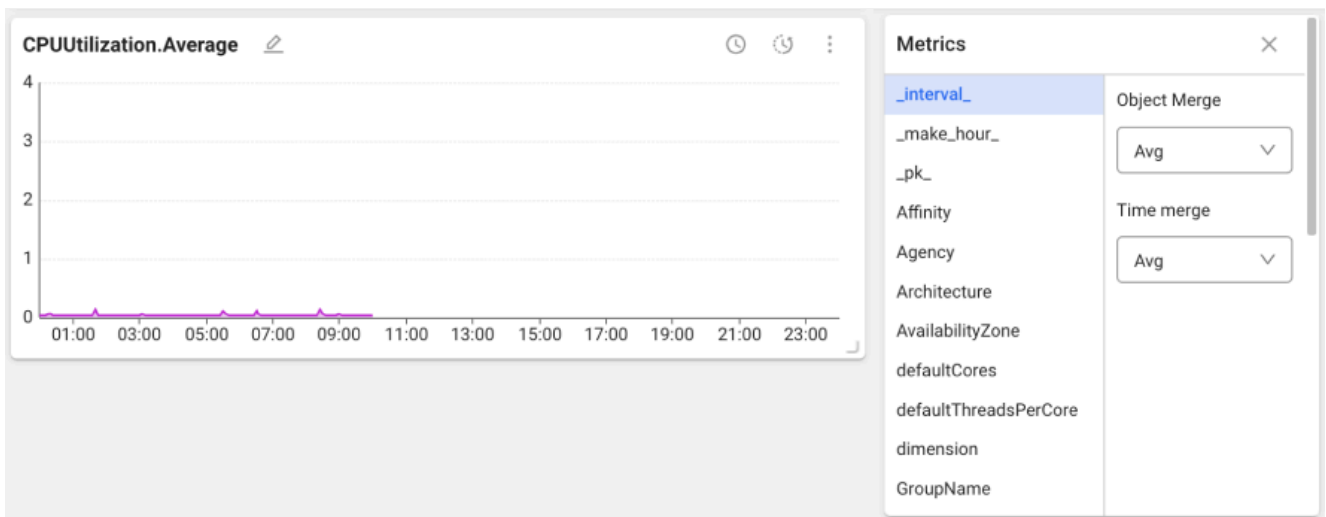
It is used to group the chart data based on the tag (e.g. agent name) selected on the left. At this time, if the tags match among the data with different fields (e.g. CPU), the corresponding data is merged.

- **Time merge**

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

- **AWS ColudWatch Metrics**

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



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

Copying a widget

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

Delete Widget

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

Interface Status

Home > Select Project > **Device** > **Interface Status**

In **Interface Status**, you can monitor the network interface status of the device in real time. It visually displays the connection to interfaces and provides detailed information about each interface, allowing you to easily analyze the network performance.

Basic screen and settings

The **Interface Status** screen consists of an interface list area on the left, an interface status area on the upper right, and an interface detail area on the lower right. When you select an interface to view from the interface list, you can see the interface status and details in the area on the right.

Interface Status

1. In the **Time selection** option bar at the top of **Interface Status**, set the query time range.
 - **LIVE** mode automatically refreshes the last 30 minutes of data and does not support querying past times.
2. In the top option bar **Select Manager**, select the NMS manager that collects data to check the interface status.

Interface status

You can see the connection status of the interface.

- **Connected** : The interface is normally connected. It appears when both the link status and Admin status are "up."
- **Link Down** : The network link is down. The link status appears upon "down" and the Admin status appears upon "up."
- **Admin Down** : The interface is disabled by the administrator. It appears when both the link status and Admin status are "down."
- **Unavailable** : It indicates the number of unusable interfaces, such as virtual interfaces that are not

physically active, loopback interfaces, or fiber interfaces that do not have an SFP module inserted.

Interface details

It displays information details about each interface in a list format. If an interface is clicked, the device trend page appears to display the status in more detail.

Device Trend

Home > Select Project > **Device Status** > **Usage Status**

In **Usage Status**, you can check the data related to the device status change in real time. It provides visual metrics for devices and interfaces, allowing you to immediately identify changes in the network performance.

Basic screen and settings

1. In the top option bar **Time selection**, select the query time point. It displays the most recent 10 minutes of data based on the selected time.
2. In the top option bar **Select Manager**, select the NMS manager that collects data to check the usage status.
3. In the **Device selection** area, select the device or specific interface to analyze.

Selection	View displayed
Device only	Device level view (all interface trends)
Device > Interface	Interface level view (single interface details)

4. Check the usage status of the selected device or interface.

Interface display format

When you select a device, you can choose the interface display format.

Interface display format

Item	Description
Device	Arranges and displays the ports in the same layout as the front panel of the actual equipment

Item	Description
Status	Displays the interface status as a list

For equipment without physical port information, the message `There is no collected interface port information.` is displayed instead of the frame, and the entry point for the port layout settings is not exposed either.

Port layout settings

In the **Device** format, you can adjust the port layout displayed on the screen to match the actual equipment.

1. Click the  icon. The **Port Layout Settings** window opens.
2. Select the equipment specification in the **Frame** area.

Item	Description
Width	Number of ports one row holds. <code>24 ports</code> or <code>48 ports</code>
Height	Number of frame rows. <code>1</code> to <code>3</code>
SFP port	Adds 4 extra port slots on the right of each row

3. Drag a port, or click a port and then click the position to move it to, to change its location.
4. Click the **Apply** button to save. To revert, click the **Cancel** button.
 - To return to the default layout, click the **Restore default layout** button.

❗ If the frame capacity is insufficient, the message `{count} ports are left outside the frame. Increase the width or height.` is displayed. When all ports are placed, the number of placed ports and remaining slots is displayed.

❗ In the **Status** format, or when there are no physical ports to edit, the port layout settings button is displayed as disabled and the reason is shown in a tooltip.

Usage Status - Device

When a device is selected, the overall interface traffic trends for that device are displayed in a line chart.

Usage status device

Chart panels

Panel	Description
Total Throughput	Total throughput of all interfaces combined, displayed across the full width of the screen
Inbound Throughput	Inbound traffic per interface, with each interface displayed as a separate line
Outbound Throughput	Outbound traffic per interface
Top N (Daily)	Interface ranking table based on maximum daily throughput
Top N (10 min)	Interface ranking table based on maximum throughput in the last 10 minutes

Top N table columns

Column	Description
Interface	Interface name
Today / Recent 10 Min	Maximum throughput (in bps) for the period
Current	Current throughput (in bps)

ⓘ The Top N table is sorted in descending order by throughput, allowing you to quickly identify interfaces with the highest traffic.

Private MIB widget

If a custom OID (Private MIB) is configured for the device, an additional widget is displayed.

Item	Description
Display condition	When OIDs other than <code>AllInterfaces</code> are configured
Widget content	Custom metric charts by OID

Private MIB chart customization

Click the  icon at the top right of the Private MIB widget to open the **Chart Setting** window. The **Chart Setting** window consists of three areas.

Area	Description
Chart Preview	Preview of how the chart appears with the current settings
OID Information	Detailed information about the OID
	OID: Target OID to collect (for example, <code>1.3.6.1.4.1.9.6.1.101.1.8.0</code>) MIB Info: MIB module and symbol information (for example, <code>CISCOB-MIB::rlCpuUtilDuringLastMinute</code>) Node Type: MIB node type (for example, <code>Integer32</code>, <code>Counter64</code>) Description: OID description defined in the MIB file
Chart Setting	Setting options such as chart type and unit

Chart Setting options

Set the Chart Setting options: **Time Range**, **Chart Type**, and **Unit**.

Time Range

Option	Description	Available charts
Recent 30 Min	Displays the last 30 minutes of data as a time series	Line, Bar
Latest	Displays only the most recent value	Text, Table

! When you change the Time Range, the available Chart Types change automatically.

Chart Type

Type	Chart	Description
When Time Range is Recent 30 Min	Line	Time series line chart. Suitable for trend analysis
	Bar	Time series bar chart. Suitable for comparison by interval
When Time Range is Latest	Text	Displays the latest value as large text. Suitable for monitoring a single metric
	Table	Displays the values in a table. Suitable for comparing multiple index values

Unit

Unit	Description	Usage example
Count	Plain number (default)	Number of packets, number of sessions
Byte	Automatic conversion in byte units (KB, MB, GB)	Memory usage, file size
Bit	Automatic conversion in bit units (Kb, Mb, Gb)	Storage capacity

Unit	Description	Usage example
bps	Automatic conversion in bits per second (Kbps, Mbps, Gbps)	Bandwidth, throughput
Percent (0-100)	Percentage (0 to 100 range)	CPU usage, memory usage
Percent (0-1)	Percentage (0 to 1 range, displayed multiplied by 100)	Usage on some equipment
Severity	Custom status value mapping	Equipment status, alarm level

Severity customization

When you select Severity as the Unit, you can map numeric values to meaningful status labels.

Default Severity settings

Value	Label
0	Normal
1	Warning
2	Critical

How to set Severity

1. Select **Severity** from the Unit dropdown.
2. The three default statuses (Normal, Warning, Critical) are displayed.
3. Modify the settings of each status.
 - **Label:** Status name displayed on the screen (for example, **Normal** , **Warning** , **Critical**)
 - **Value:** OID value recognized as that status (integer)
4. Add a new status with the **Add Severity** button.
5. Click the X button to delete an unnecessary status.

- ✓ Severity is useful when converting status codes of SNMP equipment into labels that are easy for people to read.

Severity usage examples

Equipment operation status monitoring

Value	Label	Meaning
1	Running	Operating normally
2	Standby	Standby status
3	Down	Failure status

Port status monitoring

Value	Label	Meaning
1	Up	Active
2	Down	Inactive
3	Testing	Under test

Usage Status - Interface

When a specific interface is selected, detailed metrics for that port are displayed in 4 chart panels.

Usage status interface

Chart panels

Panel	Metric	Unit	Description
Throughput In/Out	bpsIn, bpsOut	bps	Inbound/outbound throughput
Discard In/Out	discardIn, discardOut	count	Number of discarded packets
Error In/Out	errorIn, errorOut	count	Number of error packets
PPS In/Out	ppsIn, ppsOut	count	Packets per second

Statistics

Input/Output statistics are displayed at the bottom of each chart.

Item	Description
Current	Current value (most recent data point)
Max	Maximum value within the query period
Avg	Average value within the query period

Health Check Status

In **Health Check Status**, you can monitor health check results in real time. View detailed metrics such as response status, RTT, Jitter, and packet loss for each target.

Basic screen and settings

Health check status

Time selection

The top option bar **Time selection** displays the real-time data refresh interval.

Select Manager

In the top option bar **Select Manager**, select the NMS manager that collects data to view health check results.

Select health check target

In the left panel, select the device or health check target to query.

Selection level	Description
ALL [n]	All health check results; the number in parentheses shows Alive/Dead count
Device name	Shows only health checks registered to a specific device
Target (IP/FQDN)	Shows only detailed results for a specific target

Status display

The health check status result is displayed next to each item in the format `total count [alive count/dead count]` .

- **Green:** Alive (responding)
- **Red:** Dead (not responding)

Health check results

Charts

Displays metrics for the selected target as a time-series chart.

Chart	Description
Jitter	Jitter trend (ms); provided for ICMP type
Max RTT	Maximum RTT (Round Trip Time) trend (ms); provided for all types

Time range

- Displays data for a fixed 10-minute range.
- Auto-refreshes every 10 seconds.

Health check list

Column	Description
Alive	Response status - ● : Alive (responding normally) - ● : Dead (not responding)
Type	Health check type (ICMP, TCP, etc.)
IP	Target IP address for health check
FQDN	Fully Qualified Domain Name

Column	Description
Port	TCP port number (for TCP type)
Avg RTT	Average Round Trip Time (ms)
Max RTT	Maximum Round Trip Time (ms)
Packet Loss	Packet loss rate (%)
Jitter	Jitter value (ms)
Error	Error message
Last Seen Time	Time of last response received

Appendix

Metrics

Metrics by type	ICMP	TCP
Alive	O	O
Avg RTT	O	-
Max RTT	O	O
Jitter	O	-
Packet Loss	O	-
Port	-	O
Error	O	O

- **RTT (Round Trip Time)**

Metric	Description
Avg RTT	Average round-trip time - average response latency
Max RTT	Maximum round-trip time - slowest response time

- **Packet Loss**

The percentage (%) of packets lost out of total packets sent.

- **Jitter**

The variation in network latency. High jitter indicates unstable network quality.

Data refresh interval

The page auto-refreshes every 10 seconds.

Item	Value
Refresh interval	10 seconds
Time range	Last 10 minutes

Supported health check types

Type	Description
ICMP	Check connection status based on ICMP Ping
TCP	Check TCP port connection status

Device Inventory

Device Inventory manages the registration of network devices and monitoring settings. Devices can be automatically discovered using the Auto Discovery feature provided by the manager or manually added as needed. Each registered device can be configured with SNMP based monitoring and Health Check to monitor real time status. This allows integrated management of devices to be monitored in the network management system.

Basic screen and settings

In **Device Inventory**, you can view all registered network devices in a table. The top menu provides key functions related to device registration and management.

Device inventory

Manager selection

Select the connected NMS Manager instance.

Add device

Click the + **Add Device** button to manually add a new network device. For more information, see [Add device](#).

SNMP Polling bulk settings

Click the + **SNMP Polling Bulk Settings** button to apply SNMP Polling settings to multiple devices at once.

Status summary

Item	Description
Total	Total number of registered devices

Item	Description
SNMP Enabled	Number of devices with SNMP Polling enabled
SNMP Disabled	Number of devices with SNMP Polling disabled

! Click a status summary item to filter the list and view only the devices in that status.

Device list

Device list column	Description
	Edit device settings. Clicking it opens the device settings drawer
Alias	Device alias
Host	Device IP address
Hostname	Device hostname
Description	Device description (model name, etc.)
Manufacturer	Manufacturer (for example, Cisco Systems)
Location	Installation location
Contact	Contact person information
Host Type	Host type (for example, Switch, Router)
Role	Device role (for example, Border Router, Edge Switch)
Serial No.	Device serial number
Firmware	Firmware version

Device list column	Description
SNMP Polling	SNMP Polling status and the number of collected OIDs
Health Check	Health Check status and the number of settings

+ Add device

You can manually register a new network device.

1. On the **Device Inventory** screen, click the **+ Add device** button.
2. In **Add device**, enter information in the **Device Info** tab.
 - **Host** (**Required**): device IP address
 - **Host Name**: device hostname
 - **Manufacturer**: manufacturer information
 - **Contact**: contact person information
 - **Role**: role in the network
 - **Alias**: management alias
 - **Description**: detailed description
 - **Location**: physical installation location
 - **Host Type**: device type
 - **Serial No.:** serial number
3. Click the **Add** button.

Device details management

1. Click the [✎](#) for a registered device.
2. In the details window, check or edit information in the **Device Info**, **SNMP Polling**, **Health Check** tabs, then click the **Save** button.

Device Info tab

Configure basic information for the device.

SNMP Polling tab

Manage settings to periodically collect performance and status data from the device using the SNMP protocol. After editing, click **Save** to apply.

- **Port** (Required): SNMP port (default: 161)
- **Community** (Required): SNMP v1/v2c community string (default: public)
- **Version** (Required): SNMP version (v1, v2c, v3)
- **User Name**: SNMPv3 username
- **Security Level**: security level (noAuthNoPriv, authNoPriv, authPriv)
- **Authentication Protocol**: authentication protocol
 - **Authentication Key**: authentication key
- **Privacy Protocol**: encryption protocol
 - **Privacy Key**: encryption key

OID selection and management

1. Click the **Edit OID** button and select the MIB information to collect from the OID list.

OID list column	Description
OID	SNMP OID value
MIB Information	MIB name and details
Manufacturer	Manufacturer
Category	Metric type

OID list column	Description
Description	Detailed description

- Click the **OK** button.

Set collection interval

- **Custom Polling Interval:** configure data collection interval (unit: seconds, default: 60)
- **Activate:** enable or disable SNMP Polling

Health Check tab

Monitor the availability of network devices in real time. You can also add health check targets.

Health Check column	Description
Activate	Health check activation status
Target Host	Target IP address or FQDN
Protocol	Health check protocol (ICMP, etc.)
Memo	Note or description
Actions	Edit (✎) or delete (🗑️) health check targets

Add health check target

- In the **Health Check** tab, click the **+ Add** button.
- In the **Add health check target** popup, enter the following information:
 - **Target Host:** enter IP address or FQDN
 - **Protocol:** select ICMP (dropdown)

- **Memo:** optional note
 - **Activate:** choose whether to activate immediately
3. Click the **OK** button to save.

Group Management

In the **Group Management** menu, you can manage devices in a  Site →  Building →  Floor hierarchy. Organizing devices by group makes management and monitoring more convenient in large-scale network environments.

Basic screen and settings

Group Management

Manager selection

nmsdevu2204

+

Add Location

NAME	DESCRIPTION	DEVICES	
Seoul HQ	-	-	+ Add Edit Delete
SparkPlus	-	-	+ Add Edit Delete
13F	-	View Devices	Edit Delete
Tokyo Office	-	-	+ Add Edit Delete
Nakayama B/D	-	-	+ Add Edit Delete
11F	-	View Devices	Edit Delete

1. At the top of the **Group management** screen, select the manager you want to manage groups for in **Select Manager**. The group list is displayed based on the selected manager.
2. You can view, add, and delete the group list displayed based on the selected manager. Groups are displayed in a tree structure of  Site →  Building →  Floor.

Table | Group list

Column	Description
Name	Group name (location/building/floor)
Description	Group description

Column	Description
Devices	View devices included in the group
Actions	Add/edit/delete group

Adding a group

Adding a Location

1. Click the **+ Add Location** button at the top of the screen.
2. In the **Add Location** dialog, enter a name and type.
3. Click the **Save** button to create a new Location.

Adding a Building

1. Click the **+ Add** button for the Location where you want to add a Building.
 - You can also click the **+ Add Location** button at the top of the screen to add one.
2. In the **Add building** dialog, enter a name.
3. Click the **Save** button to create a new Building.

Adding a Floor

1. Click the **+ Add** button for the Building where you want to add a Floor.
 - You can also click the **+ Add Location** button at the top of the screen to add one.
2. In the **Add floor** dialog, enter a name.
3. Click the **Save** button to create a new Floor.
4. Click the **View Devices** button to check assigned devices.

Editing a group

1. Click the  **Edit** button for the group you want to modify.
2. Change the group name or description.
3. Click the **Save** button to apply the changes.

Deleting a group

1. Click the  **Delete** button to the right of the group you want to delete.
2. In the delete confirmation popup, click **Delete** to remove the group.

Device assignment

When you click the **View Devices** button for a Floor in the group management list, the device assignment window opens.

Adding/deleting devices

- Click the + **Add** button to select an unassigned device and it will be immediately assigned.
- Click the  icon to unassign individual devices.

Bulk edit

You can manage multiple devices at once.

1. Click the **View Devices** button for a Floor to open the device assignment window.
2. Click the  **Edit** button to go to the bulk edit window.

Panel	Description
Unassigned (left)	List of unassigned devices; click + to assign
Assigned (right)	List of assigned devices; click - to unassign

3. In the bulk edit screen, click the **Save** button to save changes.

Task Configuration

Network Automation lets you connect to network devices via SSH and automatically execute commands. For example, you can schedule daily backups of router configuration files or register tasks that automatically run diagnostic commands when specific events occur.

To add a task, you need account credentials (username/password or SSH key file) that allow SSH access to the target device.

Viewing the task list

Go to **Network Automation > Task Configuration** to view the list of registered tasks. Select an NMS Manager from the **Select Manager** dropdown at the top of the screen, then search by device alias, host, username, or memo to quickly locate tasks.

The number of tasks per status is displayed at the top of the screen. Click a chip to filter tasks by that status.

Chip	Description
All	Total number of registered tasks
Active	Number of tasks currently active and running
Inactive	Number of suspended tasks
Scheduled	Number of tasks set to run automatically on a recurring basis

Key list columns

Key information available in the task list.

Column	Description
No.	Task sequence number

Column	Description
Active	Green dot (blinking) = active; gray dot = inactive
Alias	Device alias. Click to navigate to the task's execution history
Host	Device IP address or hostname
Username	SSH login account name
Port	SSH connection port
Auth method	Password or Key file
Schedule	manual, every N min (periodic), or detector (event-triggered)
Commands	Number of commands registered in the task
Retries	Number of retry attempts on failure
Key file	Key file name when key file authentication is used
Timeout	Command execution time limit
Last status	Last execution result: success, failure, or pending
Last run time	Time of the last execution
Next run time	Next scheduled execution time (blank for manual)
Memo	Task description memo

Adding a task

1. Click the **Add Task** button in the upper right.
2. Configure each field in the popup and click **Save**.

Step 1: Enter basic information

Specify which device to connect to and with which account.

Field	Required	Description
Device	Required	Select the target device to run commands on
Username	Required	SSH login account name
SSH port	Required	SSH port — change only if different from the default (22)
Device type	Required	CLI driver type. If unsure, enable Auto Detect and the server will determine it automatically when the task is saved
Enabled		Enable or disable this task configuration
Retries	Required	For unstable network environments, 1–3 retries is recommended
Timeout (sec)	Required	For slow-responding devices, set higher than the default
Memo		Free-text note about the task

Step 2: Choose execution timing (schedule)

Decide when this task should run.

Schedule type	When to use
Manual	Run by clicking the execute button manually — for tasks that do not need automatic execution
Scheduler	Automatic execution every N minutes or at a specific time each day — suitable for periodic backups and data collection

Schedule type	When to use
Detector	Automatic execution when a specific event or condition is detected — suitable for automated incident response

Step 3: Choose SSH authentication method

Auth method	When to use
Password	Enter the SSH password directly — for quick setup
Key file	Authenticate with an SSH key file for secure, password-free access — the key file must be uploaded in SSH Key Management in advance

Step 4: Register commands to execute

Add commands to execute in order. At least one command is required.

1. Click the + **Add Command** button and enter a command.
2. Use the ↑ ↓ buttons to adjust the execution order.
3. Adding a description for each command makes them easier to identify later.

Test connection before saving

It is recommended to verify connectivity before saving.

1. Click the **Test Connection** button.
2. The result appears at the bottom of the popup.
 - Success: preview of the connection prompt
 - Failure: error type and cause message

Edit, run now, and delete tasks

Use the action buttons on the right side of the list to perform each operation.

Button	Description
Edit	Opens the configuration popup to modify existing values
Run Now	Confirms and immediately executes the task — results are viewable in Task Status
Delete	Deletes the task — execution history is also removed

SSH key file management

Key file authentication requires registering the key file first. Click the **SSH Key Management** button in the upper right.

Action	How to
Upload	Select an SSH private key file (e.g., <code>.pem</code>), enter a file name, and enter the passphrase if the key is passphrase-protected
Delete	Remove key files no longer in use from the list

Task Status

Task Status shows the execution history of automation tasks and the output of each command. Use it to verify that a task is running as expected or to investigate the cause of a failure. Clicking a device alias on the Task Configuration screen opens Task Status with the execution history for that task already filtered.

Finding results (filters)

When there is a large amount of execution history, use filters to narrow the scope. Click **Reset** to clear all filters.

Filter	How to use
Select Manager	Select an NMS Manager
Task	Select to view results for a specific task only
Command	Search by command name
Status	Filter to show only successes or failures
Start date / End date	Query execution history for a specific period
Display count	Maximum number of records to load at once (100 / 500 / 1000 / 5000)

Execution result summary

A summary of the current query results is displayed below the filters.

Item	Description
Total	Total number of executions retrieved
Success	Number of executions completed successfully

Item	Description
Failure	Number of executions that ended in failure

Execution history list

The list is displayed in reverse chronological order.

Column	Description
Run time	Time the task was executed
Host	Hostname of the target device
Alias	Device alias
Command	Command that was executed
Status	Success (green) / Failure (red)
Duration	Time taken to execute the command (e.g., 1.234s)
Error	Error message on failure (truncated with ellipsis if long — hover to see the full message)

Viewing execution result details

1. Click a row in the list to expand the full output of that command below.
2. Use the output as needed.
 - **Copy:** copy to clipboard
 - **Download:** save as a text file (filename format: automation_YYYY-MM-DD_alias_ID.txt)
3. Click a row with a Failure status to see the error message and how far the command executed before failing.

Config Changes

Config Changes lets you view snapshots of device configuration files collected by automation tasks and compare them against previous states to see exactly what changed. For example, if you run a router configuration backup task daily, this screen shows you line-by-line what differs between yesterday's and today's configuration.

Configuration change history is only collected for tasks that have the **Config Change Tracking** option enabled at task creation.

Filters

Set the query scope from the top of the screen.

Filter	How to use
Select Manager	Select an NMS Manager
Task	Select to view history for a specific task only
Start date / End date	Date range to query - Only dates within the data retention period are selectable; by default, data from the past 30 days can be queried
Display count	Maximum number of records to load at once (100 / 500 / 1000 / 5000)
Scope	Changes only : show only snapshots where the configuration actually changed All : show all snapshots regardless of whether changes occurred

Change overview

The **Change Overview** panel below the filters provides a quick summary of the overall situation. Use the arrow on the right side of the header to collapse or expand the panel, and drag the divider between the panel and the list to adjust the panel height.

Statistics

Item	Description
Total	Total number of snapshots collected during the query period
Changed	Number of snapshots where the configuration changed compared to the previous snapshot

Summary table

View the top 5 entries per tab to identify which devices, commands, or dates had the most concentrated changes.

Tab	Content
Most changed hosts	List of devices with the most configuration changes — useful for identifying frequently modified equipment
Commands by impact	List of commands that affected the most devices — useful for identifying changes with a wide scope
Top change dates	Dates with the most configuration changes — useful for identifying days when large-scale changes occurred

Daily change chart

Displays the number of configuration changes per day as a bar chart. **Click a specific date bar** to show only snapshots from that date in the list. Click **Back** to return to the full list.

Configuration snapshot list

A list of collected snapshots. Each row represents the state of a configuration file captured during a single task execution.

Column	Description
No.	Snapshot sequence number
Capture time	Time the snapshot was captured
Host	Hostname of the target device
Alias	Device alias
Command	CLI command used to collect the configuration
Added	Number of lines added compared to the previous snapshot (green)
Deleted	Number of lines removed from the previous snapshot (red)
Change	<code>modified</code> (changed, orange) / <code>unchanged</code> (no change, gray) / <code>initial</code> (first collection)
Detail	Click View to see the full change details

Viewing change details

1. Click the **View** button in the list to open a popup.
2. Check the host, alias, command, and change status at the top of the popup. Click the arrow to collapse the top summary.
3. Select a comparison mode that suits your needs.

Comparison modes

Mode	Description
Unified	Displays added (green <code>+</code>) and removed (red <code>-</code>) lines in sequence in a single view — similar to <code>git diff</code> format

Mode	Description
Split	Compares the previous and current configurations side by side — for viewing the full context together
Simple	Highlights only changed lines with color for a quick scan

Preventive Profiles

Preventive Check is a feature that lets you select some of the commands registered in a **Network Automation** task as check items, map judgment rules to each item, and automatically evaluate the execution results. Every time the task runs, a report is generated that automatically judges each item as normal, warning, or critical according to the mapped rules — so you can standardize repetitive checks and detect threshold-based anomalies without manual review. It's intended for network administrators and infrastructure engineers who repeatedly inspect network devices.

Profiles are check templates for Preventive Check. A profile defines which automation task's commands to use as check targets, and which item label and judgment rule to apply to each command's result.

Viewing the profile list

Go to **Network Automation > Preventive Profiles** to view the list of registered profiles. You must first select an NMS Manager from the **Select Manager** dropdown at the top of the screen for the list to appear.

Key list information

Column	Description
No.	List sequence number
Profile	Profile name. Click to open the edit popup
Automation task	Device alias or host of the automation task linked to the profile
Target	Device address the task actually connects to
Commands	Number of check commands registered in the profile
Latest report	Status badge (Normal · Warning · Critical · Unknown) and creation time of the most recently generated report

Column	Description
Profile enabled	Shows enabled status as an Enabled · Disabled badge. Cannot be toggled directly in the list — change it only in the edit popup
Actions	View details, edit, and delete icons. Both view details and edit open the same edit popup

! Type a profile name in the search box to narrow the list instantly.

Adding or editing a profile

1. Click the **Add Profile** button at the top right. To modify an existing profile, click the **Edit** icon in the list instead.
2. Configure each field in the popup, then click **Save Profile**.

Step 1: Enter basic information

Field	Required	Description
Profile name	Required	Name to identify the check template
Automation task	Required	Select the automation task to use as the check target. Tasks already used by another profile are excluded from the list
Profile enabled		Enable toggle, enabled by default
Memo		Write a description memo for the profile

Once you select an automation task, a summary card shows the selected task's **CLI driver**, **schedule**, **latest execution result**, and **command count**.

Step 2: Mapping check items

The commands registered in the selected automation task appear in a table in execution order. Configure the check method for each command in its row.

Column	Field	Description
Use	Checkbox	Unchecked commands are not saved to the profile
Automation command	Text (read-only)	The original command registered in the task
Item label	Input field	Enter the check item name to display in the report
Use parser	Dropdown	You must select Use to select a Match field below
Match field	Dropdown	Select the column, parsed from the command execution result, to use for judgment. If parsing failed for a command, enter the value manually
Applied rule	Dropdown	Select the judgment rule to apply to this item. If there is no rule, select No rule

Click the **Manage Rules** button at the top right to open the rule edit popup layered over the profile edit popup. You can register a new rule and immediately select it in the **Applied rule** dropdown.

- ✔ If the command execution result is parsed into a table, the **Match field** dropdown is automatically filled with the actual column names. If parsing failed, enter the value directly into **Match field**.

Deleting a profile

1. Click the **Delete** icon in the list to open a confirmation dialog.
2. Click confirm to delete the profile.

Preventive Rules

A **Rule** is the judgment criterion applied to each check item in a [Preventive Profile](#). When a command's execution result satisfies a rule's condition, it is automatically judged as **Warning** or **Critical**. A single rule can be reused across check items in multiple profiles, so changing a threshold or judgment condition in one rule applies to every linked item.

Viewing the rule list

Go to **Network Automation > Preventive Rules** to view the list of registered rules. You must first select an NMS Manager from the **Select Manager** dropdown at the top of the screen for the list to appear.

Key list information

Column	Description
No.	List sequence number
Rule name	Rule name
Judgment method	Displayed as a badge: <code>threshold</code> , <code>count</code> , <code>contains</code> , or <code>regex</code>
Warning condition	Condition judged as warning. Shown as N/A for <code>contains</code> · <code>regex</code> methods
Critical condition	Condition judged as critical. Shown as the value only for <code>contains</code> · <code>regex</code> methods (e.g. <code>down</code>)
Unit	Unit of the threshold value. Shown as N/A for <code>contains</code> · <code>regex</code> methods
Actions	Edit and delete icons

Adding or editing a rule

1. Click the **Add Rule** button at the top right (to modify an existing rule, click the **Edit** icon in the list instead).
2. Configure each field in the popup, then click the save button.

Field	Required	Description
Name	Required	Name to identify the rule
Judgment method	Required	Refer to the table below to select the method that fits the check result
Warning condition		Enter an operator and value only when the judgment method is threshold or count . For contains or regex , enter only a value
Critical condition		Same input rules as the warning condition
Unit		Enter only when the judgment method is threshold or count
Description		Optional description memo for the rule

Behavior by judgment method

Changing the judgment method automatically switches the input fields.

Judgment method	Operator	Value	Unit	Judgment criteria
threshold	Choose from >= · > · == · !=	String parsed as a number	Used	Judges whether the result value satisfies the specified numeric condition
count	Choose from	String parsed as	Used	Judges by the number of result rows matching the

Judgment method	Operator	Value	Unit	Judgment criteria
	>= · > · == · !=	a number		condition
contains	Not used	String to search for	Not used	Judges whether the execution result contains the specified string
regex	Not used	Regular expression pattern	Not used	Judges whether the execution result matches the regular expression pattern

Deleting a rule

Click the **Delete** icon in the list to see the following confirmation message.

Delete this rule?

Any profile mapping using this rule will change to **No rule**. Continue?

Click confirm to delete the rule. Check items in profiles that used this rule only have their rule link removed — the items themselves remain unchanged.

Preventive Reports

Every time an automation task linked to a [Preventive Profile](#) runs, a **Report** is automatically generated, judged according to the mapped [rules](#). Reports let you see at a glance which check items on which devices are in an abnormal state. Only the 2 most recent reports are kept per profile, and the latest report also shows the status changes compared to the previous report.

Viewing the report list

Go to **Network Automation > Preventive Reports** to view the latest report list by profile. You must first select an NMS Manager from the **Select Manager** dropdown at the top of the screen for the list to appear.

ⓘ The list does not refresh automatically. It is queried automatically only on first load and when you change the manager — afterward, click the refresh button at the top of the screen to update it.

Summary cards

Cards summarizing the number of profiles by status appear above the list. Selecting a card filters the list to that status, and the selected card is highlighted with a border.

Card	Description
Check targets	Total number of profiles subject to report generation
Reported	Number of profiles with a report generated during this query period
Not reported	Number of profiles with no report generated yet. Selecting this switches to a separate list with different columns
Normal	Number of profiles judged normal
Warning	Number of profiles judged warning

Card	Description
Critical	Number of profiles judged critical
Unknown	Number of profiles in a state that cannot be judged

Key list information

Column	Description
No.	List sequence number
Device	Target device of the report. Click to go to the manager information screen
Profile	Name of the profile that generated the report. Click to open the report detail popup
Created at	Time the report was generated
Check items	Number of check items included in the report
Result summary	Color-coded summary of the number of normal, warning, critical, and unknown items
Trigger	Badge for the execution method that generated the report (scheduler · manual · detector)
Actions	View details icon

ⓘ Selecting the **Not reported** card shows a list of profiles that don't have a report yet, displaying only the profile name, linked automation task, and number of check items.

Viewing report details

1. Click a profile in the list to open the report detail popup.
2. The top shows cards for **Total items/Normal/Warning/Critical/Unknown** counts, followed by detailed

results for each check item below.

3. Each item is displayed differently depending on whether its execution result was parsed successfully.
 - **Parsing succeeded:** Shows the check item's result in a table, along with the applied rule's judgment condition text (e.g. `Warning >=10 / Critical >=30`), the judgment reason, and the status change compared to the previous report. Select **View original** to see the command's raw execution result.
 - **Parsing failed:** Shows the raw execution result directly, with an "Unsupported or cannot be parsed" notice.

Comparison with the previous report

Each check item also shows information comparing it to the previous report.

Situation	Displayed content
No previous report to compare	Notice that there is no previous report
Status unchanged from previous report	Notice that there is no status change
Status different from previous report	Highlights the change from the previous status to the current status (e.g. <code>Warning → Critical</code>)

SNMP OID Management

Home > Select Project > **CONF.** > **SNMP OID Management**

In **SNMP OID Management**, you can register OIDs to be collected via SNMP polling. OID is an identifier for collecting various performance metrics of the network equipment.

Basic screen

By default, OIDs are pre-registered in the system and can be added to collect dedicated metrics for specific devices. The added OIDs are used to connect to the device from the device management screen and collect data via SNMP polling.

OID Management

Adding OID

You can manually add OIDs to collect custom metrics provided by a specific device.

1. Select an agent on the upper left.
2. Click the + **Add OID** button on the upper right, and then enter the following information in the **Add OID** window.

[OID](#), [Description](#), [Manufacture](#), [Category](#)

ⓘ [Category](#) is used to define the resources that each OID collects. This allows you to categorize and manage the metrics that the OID collects.

Modifying the OID

You can modify the related information by selecting the [✎](#) Edit icon in the [Edit](#) column on the left of the OID list.

Alert Notifications

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

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

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

Key Features

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

Permissions

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

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

Reference

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

Event Configuration

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

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

Metrics

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

Composite Metrics

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

Real-time logs

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

Composite log

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

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

Event setting provides features to configure and manage events based on anomaly signals that may occur in monitored systems or applications. When configured conditions are met, you can receive notifications through

your preferred channels such as email, SMS, messengers, or app push notifications. You can design event configurations according to your monitoring objectives.

Metrics

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

Composite Metrics

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

Real-time logs

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

Composite log

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

Reference

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

Common Features

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

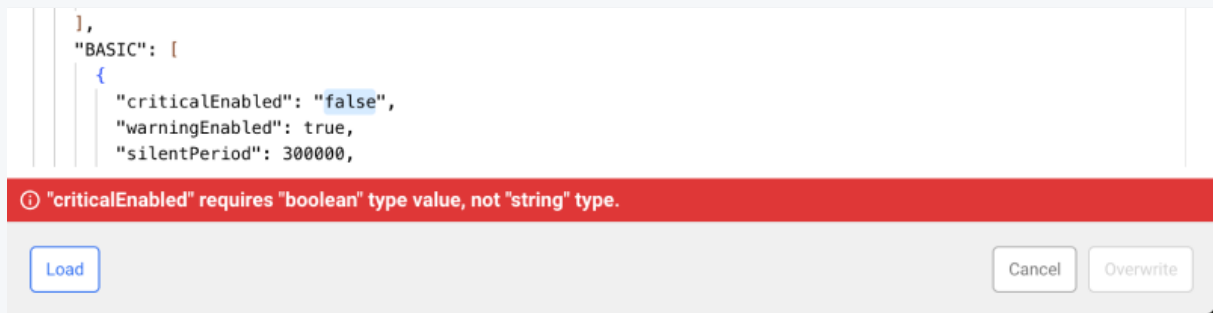
- **Batch JSON Edit:** Edit all event conditions in bulk using JSON format.
- **Batch JSON Download:** Save all currently registered event conditions as a JSON file.
- **Batch Excel Download:** Download the event list as an Excel file for external reporting or backup purposes.

Batch JSON Edit

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

 **After overwriting, you cannot restore the previous event configuration.**

- Arbitrarily modifying the values of the `productType` or `platform` properties may cause events to malfunction in other projects.
- The JSON editor includes built-in validation. If the format or values are invalid, an error message appears below the editor and the [Overwrite] button is disabled.



The screenshot shows a JSON editor with the following content:

```

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

```

A red error bar at the bottom of the editor displays the message: **"criticalEnabled" requires "boolean" type value, not "string" type.**

At the bottom of the editor, there are three buttons: **Load**, **Cancel**, and **Overwrite**. The **Overwrite** button is disabled.

 **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

JSON Field	Description
◇ LOG_REALTIME	Real-time log events
◇ METRICS	Metrics
◇ COMPOSITE_LOG	Composite log events
◇ BASIC	Basic events
◇ COMPOSITE_METRICS	Composite metrics
◇ ANOMALY	Anomaly detection

Batch JSON Download

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

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

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

Batch Excel Download

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

Metrics

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

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

Default Options

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

Table | Metrics Event List Structure

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

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

Event Configuration

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

Add Event

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

How to Add a Metrics Event
Step 1. Select Template: Choose the basic structure of the event.
Step 2. Define Event Conditions: Configure the conditions that determine when the event is triggered.
Step 3. Select Event Target: Select the monitoring targets where the event applies.
Step 4. Basic Information and Notification Settings: Configure the event name, message, and recipients.

Select Template

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

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

Define Event Conditions

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

Metric Settings

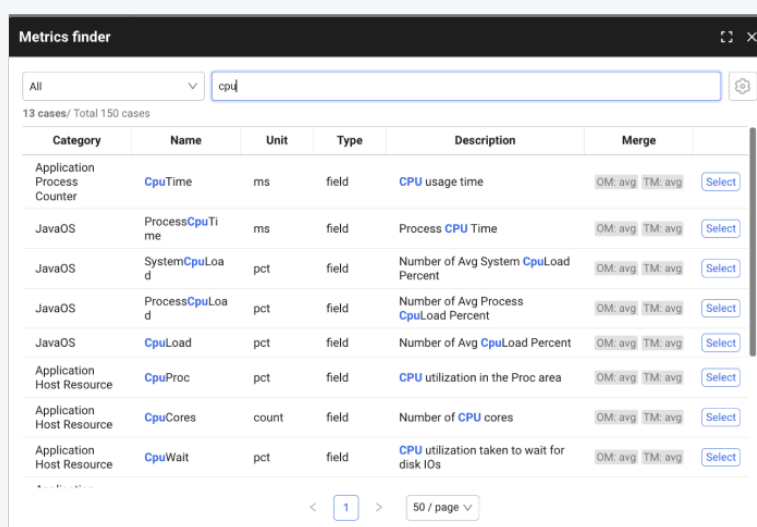
- Enter a category in the search field, or select a category (metric) from the category list. You must select a category to proceed with metric configuration.

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

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

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

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



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

❗ **Event Level Behavior**

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

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



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

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

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

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

b. Click — to remove the condition.



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

Trigger Count

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

1. Select the trigger frequency.

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

2. Enter the trigger count.

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

Pause

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

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

ⓘ When recovery notifications are enabled

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

Resolved Notification

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

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

Event Operation Time

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

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

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

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

Simulation

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

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

Start Simulation

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

Understanding Simulation Results

1. Time-Series Data

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

2. Event Counts by Level

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

3. Target-Level Details

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

4. Peak Interval Identification

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

✓ Simulation Tips

- **Simulate Different Time Ranges**

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

- **Include Actual Incident Periods**

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

- **Add Target Filtering**

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

- **Adjust Thresholds Gradually**

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

Select Event Target

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

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

Target Selection

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

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

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

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

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

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

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

Basic Information and Notification Settings

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

Event Activation

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

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

Event Name

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

Message

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

- **Variable Usage Rules**

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

- **Variable Usage Example**

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

Event Recipients

Specify the members who will receive event notifications.

- **Receive All Receive by Tag Selection**

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

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

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

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

ⓘ Reception Tags

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

Edit/Delete Event

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

Event Sharing

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

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

Export

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

Import

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

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

Edit in JSON Format

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

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

JSON error

JSON Data Structure

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

```

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

```

Table | JSON Data Structure

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

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

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

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

Appendix

Trigger Conditions and Target Selection Guide

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

Level Behavior Guide

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

1. Priority-based Event Triggering

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

Example

Configuration:

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

Current state: CPU 95%

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

2. Level Escalation

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

Example

Configuration:

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

Scenario:

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

3. Level De-escalation

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

Example

Configuration:

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

Scenario:

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

4. Execution Flow

- Warning: CPU > 70%

- Critical: CPU > 90%

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

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

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

Condition Configuration Guide

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

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

Examples using `${}` :

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

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



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

1. Comparison Operators

Numeric Comparison

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

String Comparison

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

2. Arithmetic Operators

- Basic arithmetic operations

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

- Controlling precedence with parentheses

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

- Negative values

```
cpu > -100
```

3. Logical Operators

- AND operator (&&)

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

- OR operator (| |)

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

- Combined logical operations

```
(cpu > 50 && memory > 50) | | disk < 20  
cpu > 80 && (memory > 1000 | | disk > 500)
```

4. Pattern Matching Operators

- LIKE operator

```
oname like 'prod-*'  
url like '*error*'  
message like 'WARN%'
```

- NOT LIKE operator

```
oname not like 'test-*'  
url not like '*debug*'
```

5. Built-in Functions

- Null check functions

```

isNull(value)      # Checks whether the value is null
isNotNull(value)   # Checks whether the value is not null
nvl(value, 0)      # Returns a default value if null
isEmpty(str)       # Checks whether the string is empty
isNotEmpty(str)    # Checks whether the string is not empty

```

- Aggregate functions

```

sum(cpu, memory, disk)    # Sum
avg(cpu, memory)          # Average
max(cpu, memory, disk)    # Maximum
min(cpu, memory, disk)    # Minimum
count(value1, value2, value3) # Count

```

- Math functions

```

round(cpu, 2)    # Rounds to 2 decimal places

```

- String functions

```

length(str)      # String length
startsWith(str, 'prefix') # Checks prefix
endsWith(str, 'suffix') # Checks suffix
indexOf(str, 'search') # String index
substring(str, 0, 10) # Substring
trim(str)        # Trims whitespace
replace(str, 'old', 'new') # String replacement
hasStr(str, 'search') # Checks string containment

```

- Conditional functions

- **if:** A conditional function that returns the `trueValue` if the condition evaluates to `true`, or the `falseValue` if it evaluates to `false`

Syntax

```

if(condition, trueValue, falseValue)

```

Example

```
if(value >= 90, 'High', 'Medium') == 'High'
```

- **decode:** Compares a value against conditions and returns the result of the matching condition, or a default value if no match is found

Syntax

```
decode(value, condition1, result1, condition2, result2, ..., conditionN, resultN, defaultValue)
```

Example

```
decode(value, 1, 'Low', 2, 'Medium', 3, 'High', 'Unknown') == 'Unknown'
```

- **in:** Returns `true` if the value matches any of the specified candidates; otherwise returns `false`

Syntax

```
in(value, candidate1, candidate2, ..., candidateN)
```

Example

```
in(status, 200, 201, 204) == false
```

! Writing Guidelines

- Recommended
 - Use simple variable names without `${}` (e.g. `cpu`, `memory`)
 - Always use `${}` when special characters are included
 - Use parentheses to clearly separate complex expressions
 - Enter function names exactly as defined (case-sensitive)
- Avoid



- Incomplete expressions (e.g. `cpu > , memory && )`)
- Mismatched parentheses (e.g. `(cpu > 80 && cpu > 70) )`)
- Consecutive or invalid operators (e.g. `cpu >> 80 , cpu >< 80 )`)

Composite Metrics

Home > Select Project >  **Alert** > **Event Configuration** > **Composite metrics** tab

You can create events and send alert notifications using complex rules.

Default Options

- **Search:** Search for specific events by selecting an event name or an event recipient tag
- **JSON Download/Upload:** Edit event rules directly in the JSON editor, or download them as a file, modify them, and upload them again
- **Alert Message Settings:** Select detailed fields for alert messages and edit the content for each field
- **+ Add Event:** Add a new composite metrics event

Permissions

To configure **Composite metrics** events, you must have **Alert Settings** permission. You can grant this permission by clicking the  icon for the member in **Home > Select Project > Management > Integrated Member Management**.

Table | Composite Metrics Event List Layout

Item	Description
Event Title	User-defined event name - Up to 255 bytes
Condition	Event trigger conditions
Notify on Event Recovery	Whether to receive RECOVERED (normal) notifications when Critical or Warning events are resolved – Enabled: Sends a RECOVERED notification when the state changes from in-progress to normal, and allows you to distinguish in-progress and resolved states in event history – Disabled: Triggers a one-time event each time the threshold is exceeded

Item	Description
Event Recipient Tag	Users or groups that receive notifications for the event
	Edit or delete the event
	Event enablement status – Enabled: Event is triggered when conditions are met – Disabled: Event does not run and conditions are not evaluated

Event Configuration

Composite metrics events define event conditions based on **MXQL**, the metric data query language. The **Create from Chart** feature provides a combo box to support MXQL auto-completion.

Add Event

1. Click the **Composite metrics** tab from  **Alert > Event Configuration**.
2. Click the [+ Add Event] button on the right side of the screen.
3. In the **Composite metrics** window, click **Create from Chart**.
 - a. You can use the provided templates.
4. In the **Event Configuration** screen, first query the event data, then configure the event conditions.

Query Event Data

Query event data to build charts. In the **Event Configuration** screen, select either the **Widget** or **Text** option under **Query event data** on the right to configure events.

- **Widget** Text

Using the options for configuring a time series chart, you can automatically complete the **MXQL** used for event configuration.

1. Select the date range for querying data.
2. Select the **Category** (target) for querying data.
3. Click + **Add Filter** under **Filter** to create event conditions.
 - a. In the filter window, select an expression, tag, and filter value.
 - b. Click + **Add** to add additional conditions.
 - c. To delete a condition, click the – icon next to it.
4. Under **Grouping**, select the grouped metric data. Multiple selections are supported.
5. Under **Time Unit**, set the time interval for grouped data by selecting `seconds` , `minutes` , or `hours` .
6. Under **Field**, select the fields to be used for event trigger conditions. Multiple selections are supported.

 MXQL entered in text mode is not compatible with widget mode.

An editor appears where you can directly modify **MXQL**.

1. Edit **MXQL** directly and click the **Query** button.
2. After selecting a date, you can view the results as a chart or graph.

Notification

Enter the basic information for alert notification settings.

- **Enable Event:** When the toggle is enabled, the event becomes active.
- **Level:** Select the event level (Critical, Warning, Info).
 - **Notify on Event Recovery:** When the toggle is enabled, a notification is sent when the event is resolved and enters the normal (RECOVERED) state.
- **Title:** Enter a title for the event rule.
- **Message:** Enter the content of the alert message delivered when the event is triggered. You can use variables in the message to include actual values at the time the event occurs.

Message example

✔ Variable Usage Rules

- Variable format: `${metricName}`
- Only metrics within the **same category as the configured category** can be used as variables.
- You can combine multiple variables to compose a detailed message.
- The list of available variables can be checked in **Metric Query**.

Event Trigger Conditions

- **Data Query Range:** Select the real-time data query window.
 - Available ranges: 30 seconds , 1 minute , 2 minutes , 5 minutes , 10 minutes , 30 minutes , 1 hour , 2 hours , 3 hours
- **Condition:** Enter the event trigger condition. Only fields included in the event data query can be used.

Additional Information

- **Interval:** The alert condition is evaluated at the selected interval (1 minute , 5 minutes , 10 minutes , 30 minutes , 1 hour , 12 hours).
- **Silence:** After an event is triggered, the same event is suppressed for the selected duration (unset , 1 minute , 5 minutes , 10 minutes , 30 minutes , 1 hour , 12 hours).
- **Event Active Time:** Configure tags to control when the event runs, such as working hours, non-working hours, or maintenance windows. If no tag is set, the event runs continuously for 24 hours while it is enabled.
 1. Click + **Add**.
 2. Under **Event Active Time**, click + **Create New Tag**.
 3. In **Create Event Active Time Tag**, select a **Tag Name**, **Days**, **Time**, and **Color**, then click the [Apply] button.
 4. Created tags appear in the tag list and can be applied by selecting the checkbox.
 5. To edit or delete a tag, click the  icon and modify or remove it in **Edit Event Active Time Tag**.

 When a tag is deleted, it is removed from all users to whom it is applied. However, tags that are

 currently in use by event rules cannot be deleted.

- **Event Recipient Tags:** When recipient tags are configured, notifications are sent to project members who have those tags. If no recipient tag is set, notifications are sent to all users in the project.

1. Click + **Add Tag** or the + icon.
2. Click + **Create New Tag** at the bottom of the **Event Recipient Tags** window.
3. In the **Create Tag** window, enter a tag name, select a color, and click the [Create Tag] button.
4. To edit or delete a created tag, click the  icon in the tag list.
5. Select the desired tag from the **Tag List** in the **Event Recipient Tags** window to apply it.

 When configuring events, selecting event recipient tags allows notifications to be sent to project members and third-party plugins associated with those tags. You can assign tags to project members and third-party plugins separately via **Alert > Notifications**.

Test Event Rules

You can test the configured conditions against historical data to estimate how many events would have been triggered.

1. Select the date for testing the event rules and click the [Confirm] button.
2. Click the [Run] button to check the number of triggered events.

Edit/Delete Event

1. Go to the **Alert > Notifications > Composite metrics** tab.
2. In the composite metrics list, click the  icon of the event you want to edit or delete.
3. In the **Notifications** screen, update the options and click the [Save] button.
 - a. To delete the selected event, click the [Delete] button in the upper right corner of the **Notifications** screen.

Event Sharing

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

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

Export

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

Import

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

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

Edit in JSON Format

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

 If the modified content does not conform to the JSON format, an error message will be displayed at the

! bottom of the screen and the content cannot be saved. The error message may vary depending on the type of formatting issue.

JSON error

Alert Message Settings

You can select detailed fields for the messages to be received and edit the content for each field.

Appendix

MXQL Syntax Guide

Composite metrics operates based on MXQL queries. For detailed syntax, refer to the [MXQL Syntax Guide](#).

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

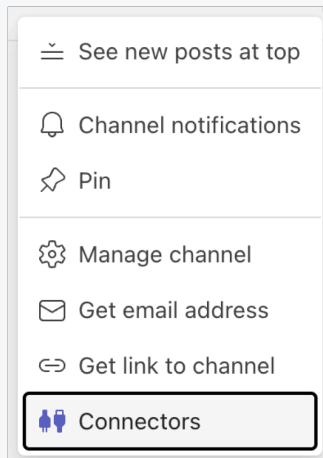


- `/remove` : Enter the project code for which you want to stop receiving alerts
- `/list` : View the list of project codes currently receiving alerts

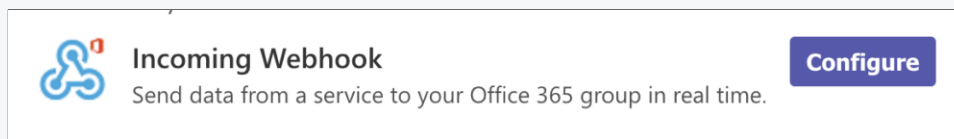
Teams



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

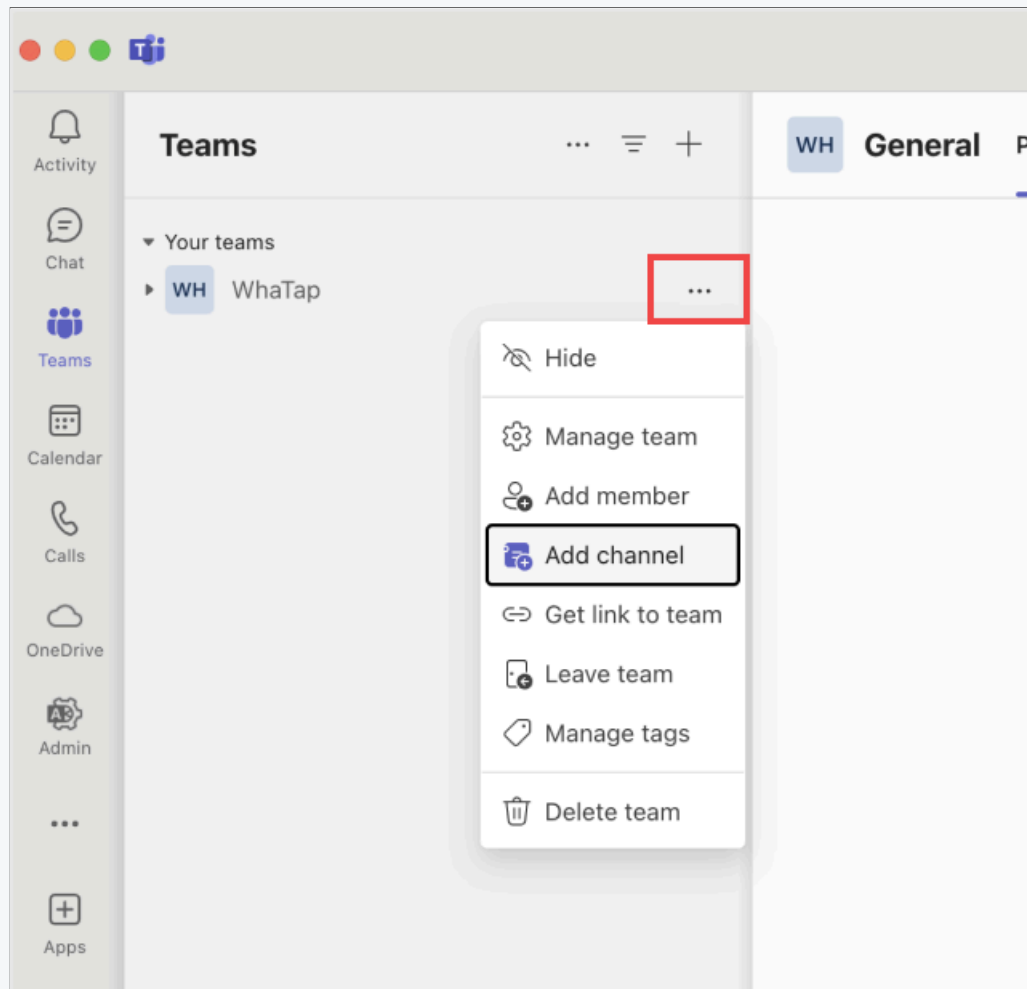
5. Return to the **Add a third-party plug-in** window in the WhaTap Monitoring service, and enter values for **Channel Name** and **Webhook URL** at the bottom of the **Teams** tab.
6. Click the [**Registration**] button.

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**.

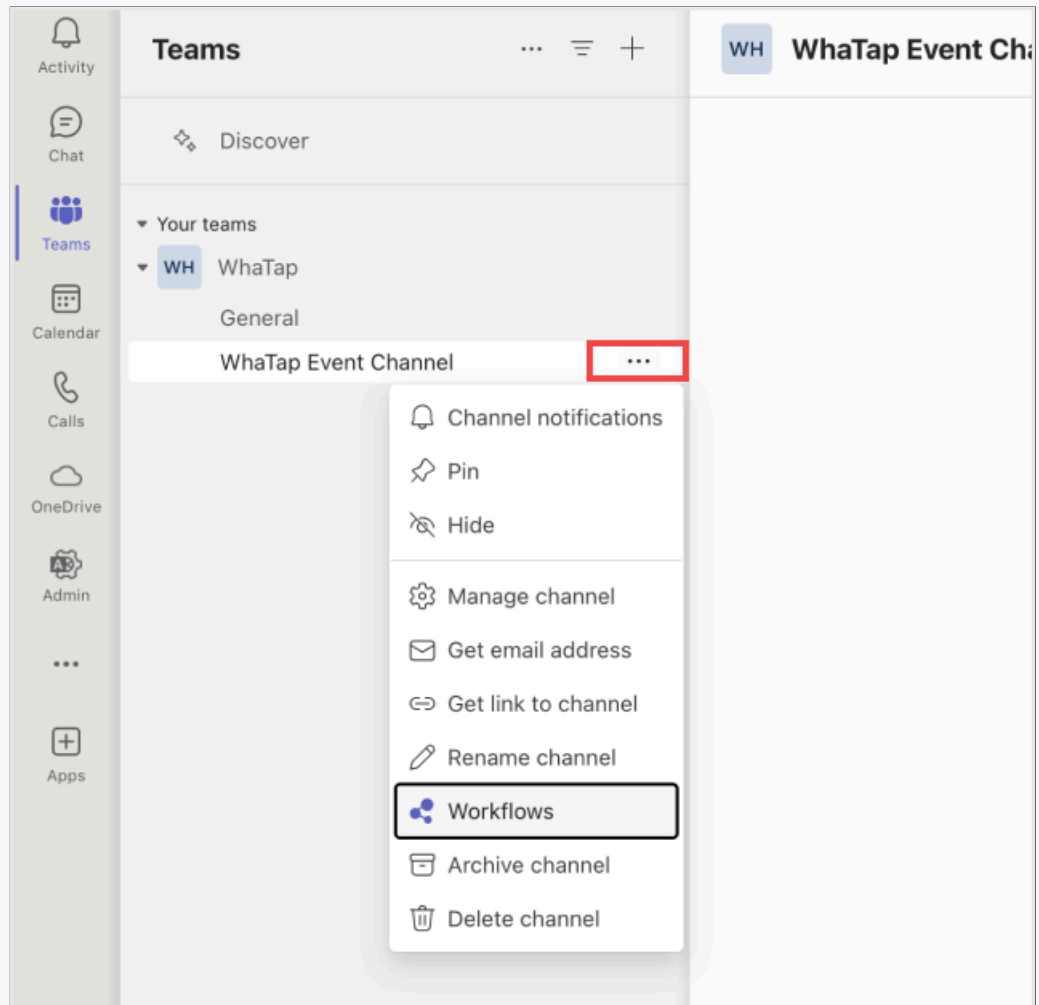


2. In the **Create a channel** window, enter the **Channel name** and **Description**. For **Channel type**, select **Standard**, then click the [Create] button.

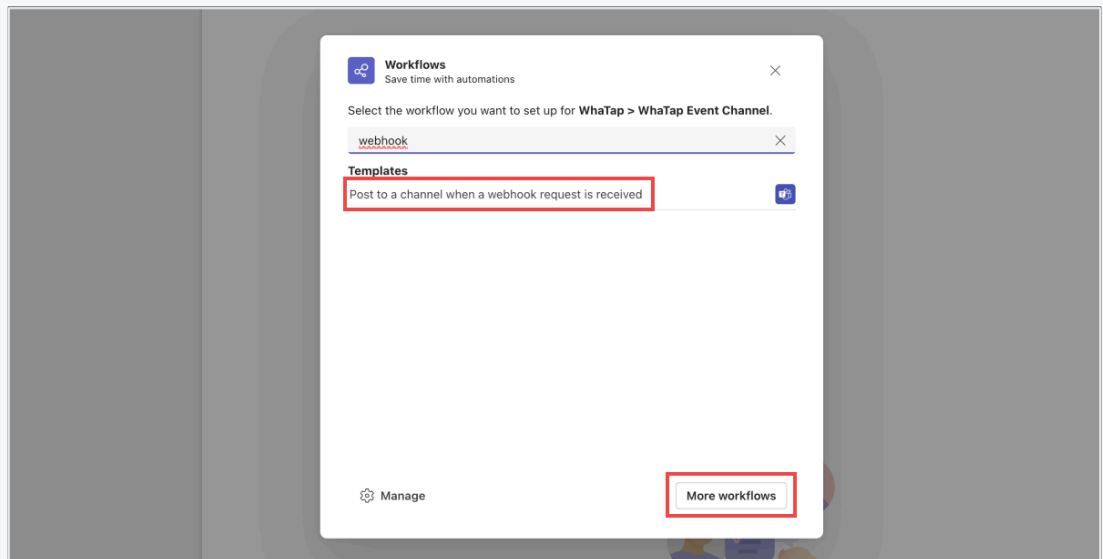


 If you select **Shared** as the channel type, workflows cannot be used. If you select **Private**, workflows can be added but notifications cannot be received.

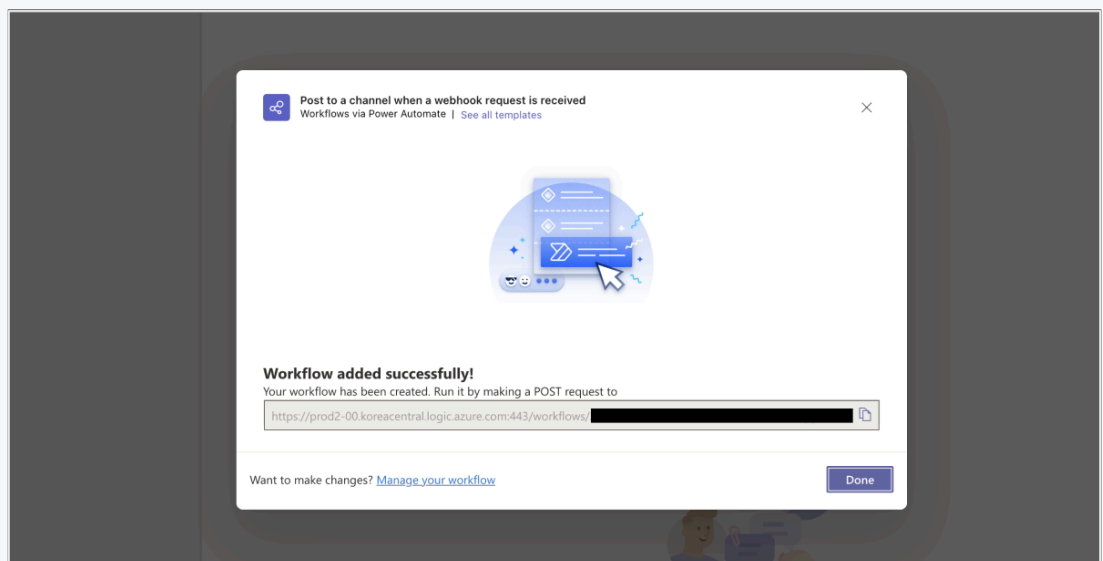
3. Click **More actions (...)** of the created channel, then select **Workflows**.



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.



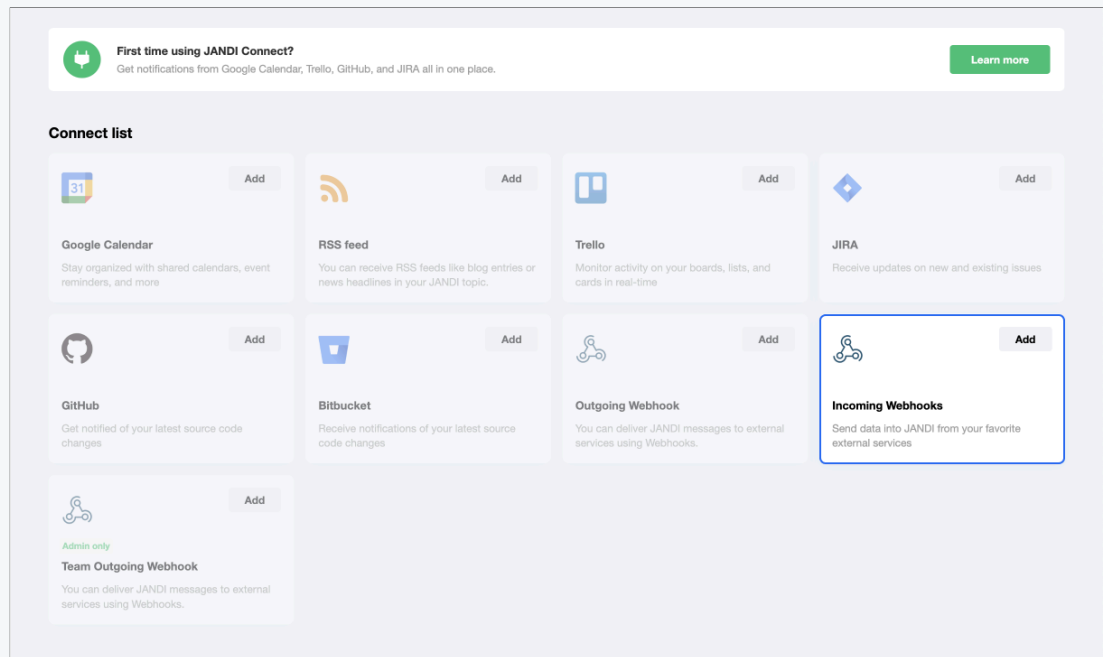
9. Click the [**Registration**] button.



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...>

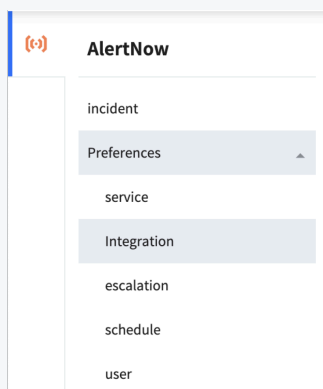
Copy

- 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**.

5. Click the [Confirm] button to create the integration.
6. Check the list of created integrations and select the newly created integration.

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.

Basic Information	
Integration type	WhaTap
Integration key	fda527a5140
URL	https://alertnowitgr.opsnow.com/integration/whatap/v1/
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}",
}
```



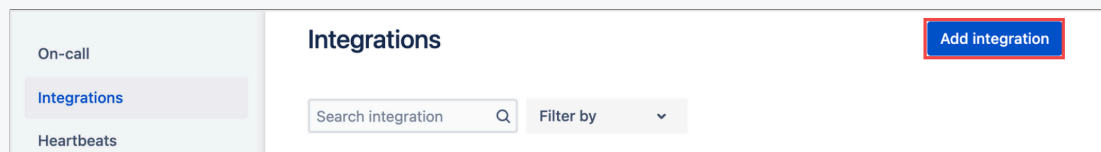
```
"metricName": "${metricName}",
"metricValue": "${metricValue}",
"metricThreshold": "${metricThreshold}",
"uuid": "${uuid}",
"okind": "${okind}",
"onode": "${onode}"
}
```

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.

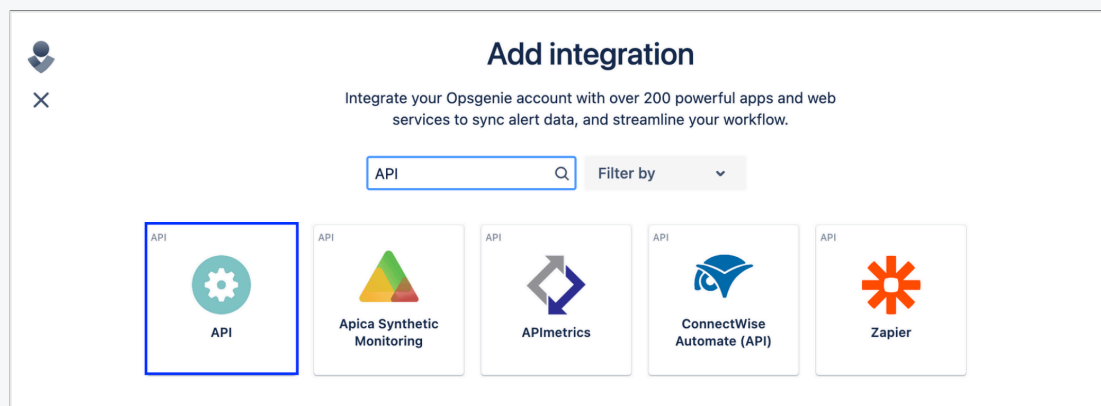
Opsgenie



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

3. 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.

1. Go to **Alert > Event History** and click the [CSV] button.
2. 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.

1. Go to **Alert > Event History** and click the [View Only Events in Progress] button.
2. 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
```

Real-time Notifications

The **Alert status** feature displays pop-up notifications when events configured in **Event Configuration** occur. You can receive alerts immediately when an event is triggered, allowing you to quickly recognize issues and respond. You can also review notifications that have already occurred or were missed, helping you understand and resolve situations where real-time response was difficult.

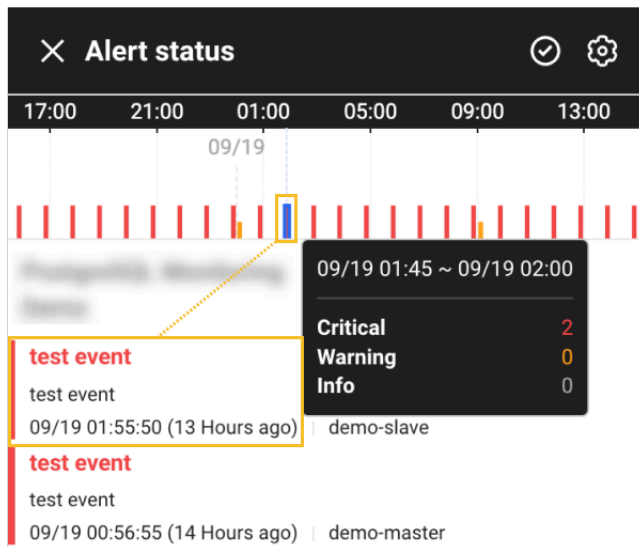
Viewing Real-time Notifications

Real-time notifications appear as pop-ups in the upper-right corner of the screen. You can check the time, title, and message of each notification.

- To close an individual notification, click the  button in the upper-right corner of the message.
- To close all pop-up notifications displayed on the screen, click **Close All Notifications**.

Viewing Notification History

1. Click the  icon at the top of the screen after selecting a project.
2. The **Alert status** window appears.
 - You can view up to 100 notifications from the past 24 hours for the current project.
 - Selecting an individual event item navigates you to the related menu.
 - In the time-based chart within the **Alert status** window, selecting a specific time range takes you to the corresponding event items.



- To view the full notification history, click **View All Notification History**. This navigates to **Alert > Event History**.

ⓘ If the **Alert status** list is empty, the **View All Notification History** button is displayed. Disable the **Receive notifications without reception tags** option.

Resolving Events in Bulk

You can resolve all ongoing events at once from the **Alert status** list. The bulk resolution process may take approximately 30 seconds to 1 minute to complete.

- When using the **Add Acknowledge** feature, a large number of recovery (resolved) notifications may be generated for currently ongoing events.
- Even after using the **Add Acknowledge** feature, events may occur again if the event rules remain enabled and the data still exceeds the threshold.
- Recovery notifications can be disabled by editing the event in **Alert > Event Configuration**. Disable **Send additional notification when the event is resolved** or **Recovered notification**.

How to use:

1. Click the  icon at the top of the screen after selecting a project.
2. When the **Real-time Notifications** window appears, click the  icon in the upper-right corner.
3. When the message `Resolve all ongoing events in the real-time notification list.` appears, click the **Resolve** button.

Configuring Real-time Notifications

1. Click the  icon at the top of the screen after selecting a project.
2. When the **Alert status** window appears, click the  icon in the upper-right corner.
3. Configure each option in the real-time notification settings window.
 - **Popup notifications:** Displays notifications as pop-ups even when the **Alert status** window is closed.
 - **Show resolved events:** Allows resolved events to be displayed in the **Alert status** list.
 - **Preview notification sound:** Lets you preview browser notification sounds. Click the  button next to **Critical** or **Warning**. If you cannot hear the sound, check your browser settings.

System Events

WhaTap Monitoring provides common system events that are automatically detected and generated across the platform. This document explains the types of events generated by the system, their trigger conditions, and recommended response actions.

EVENT_BLOCKED_BY_SYSTEM

If an excessive number of events occurs within a short period of time in a project, the WhaTap system detects this situation and blocks further events. When events are blocked, the system delivers the following message to the user. If you encounter this event, review and adjust your event configuration settings.

 **Critical**



Event Message

Excessive events detected, event blocked for stability. name: server agent

Project No	8
Project Name	new server
Target	server agent
Event Title	EVENT_BLOCKED_BY_SYSTEM
Event Time	(GMT+0900) 2024-11-18 17:58:58

Log In to WhaTap

Events are blocked as a result of excessive events in the server agent of new server project. If no events occur in server agent for a period of time, it is automatically unblocked.

Blocking Criteria

Events are blocked based on the following criteria:

1. Agent-level blocking

If **10 events** occur within **1 minute** from a single agent, all subsequent events from that agent are blocked.

2. Project-wide blocking triggered by multiple agents

If **3 or more agents** are blocked within **1 minute** according to condition 1, events from the entire project are blocked.

3. Project-level blocking

If **100 events** occur within **1 minute** in a single project, all events from that project are blocked.

How to Release the Block

When events are blocked by the system, no events must occur from the affected agent or project for **1 minute**.

- Disable all configured events from **Alert > Event Configuration**. **Review your event settings and adjust thresholds to prevent excessive event generation.**
- Before configuring events, use the **Simulation** feature to estimate how many events may occur.

Usage Analysis

In the Network Bandwidth Usage menu, you can view historical traffic trends for devices and interfaces. Analyze long-term trends by examining historical data for up to 31 days.

Basic screen and settings



1. In the top option bar **Time selection** of **Usage Analysis**, select the time range to query. You can set up to 31 days.

- Click **1 Minute** to change the data query interval.

Quick select option	Description
Last 5 min	Query last 5 minutes of data
Last 10 min	Query last 10 minutes of data
Last 1 hour	Query last 1 hour of data
Last 1 day	Query last 24 hours of data (default)
Last 7 days	Query last 7 days of data
Last 21 days	Query last 21 days of data
Today (0~24h)	Query from 00:00 to 23:59 today
1 day ago (0~24h)	Query from 00:00 to 23:59 one day ago
7 days ago (0~24h)	Query from 00:00 to 23:59 seven days ago

- In the top option bar **Select Manager**, select the NMS manager that collects data.
- In the **Select Device** area, select the device or interface to query and analyze usage.
 - Device list:** Registered devices are displayed sorted by name. Expand each device to view the list of interfaces for that device.

Selection level	Description
Device	Displays total traffic trend for the device
Interface	Displays detailed trend for a specific interface

Chart options

- **Unit display**

Traffic data is automatically converted to an appropriate unit.

Value range	Unit
0 ~ 1,000	bps
1,000 ~ 1,000,000	Kbps
1,000,000 ~ 1,000,000,000	Mbps
1,000,000,000 or more	Gbps

- **Tooltip**

Hover over the chart to see detailed values at that point in time. Values for multiple series are displayed simultaneously.

Usage analysis - Device

When you select a device in the **Select Device** area, the total traffic trend for that device is displayed as a chart.

Basic charts

Chart	Description
Total Throughput	Total throughput (full width)
Inbound Throughput	Inbound traffic
Outbound Throughput	Outbound traffic

Private MIB widget

If custom OIDs are configured for the device, additional charts for those metrics are displayed. Widget settings are saved in local storage.

Usage analysis - Interface

When you select a specific interface in the **Select Device** area, the detailed trend for that interface is displayed. The layout is the same as the interface view in [Usage Status](#).

Charts

- Traffic trend (bps)
- PPS trend (packets per second)
- Error trend

Download query results

You can save the queried screen as a file.

1. Click the **Download** button on the right of the top option bar.
2. Select a file format from the dropdown.

Item	Description
PDF	Saves the screen as an A4-sized document. Long content is split across multiple pages
PNG	Saves the screen as a single image

The capture covers the chart area on the right; the **Select Device** panel on the left is not included. Areas hidden by scrolling are also saved.

The following information is recorded at the top of the saved file.

- Date (query period)
- Project name
- Manager
- Target (device or interface)

ⓘ If there is no data to query, the **Download** button is displayed as disabled. If saving fails, a file or image download failure notice is displayed.

URL parameters

You can access the page directly with specific conditions by including parameters in the page URL.

Parameter	Description
oid	NMS manager OID
host	Device Host IP
idx	Interface Index
stime	Start time (timestamp)
etime	End time (timestamp)

Log Monitoring

Logs are the files that have recorded the events and messages that occurred in applications and systems. It is important to check the logs to find anomalies for preventing system deterioration or detecting the failure causes.

Modern IT service building environments are changing to MSA or Kubernetes. As a result, the targets to be managed are increasing. In typical log monitorings, the `tail` command or editor is used for checking after connecting the servers. However, in this case, it is difficult to use simple methods such as accessing individual servers one by one. How can you view the logs from hundreds or thousands of servers in severe cases?

Through the WhaTap log monitoring service, you can easily manage numerous logs.

! The Linux `tail` command is mainly used to check the logs whose content is added over time.

Key features

- **Central integrated management**

WhaTap can manage a large number of logs from the center. It is very convenient because you can check the log details without accessing individual servers.

- **Collection of all logs**

While collecting the logs selectively, important data may be missing. In general, WhaTap collects all logs. The collected logs can be checked in real time through the [Live Tail](#) menu.

- **Visibility**

You can check the logs through various charts provided by WhaTap. Through this visibility, you can increase access to errors and issues and detect failures as soon as possible.

- **Flexible capacity management**

While loading logs on individual servers, the logs may cause an excessive file system capacity being occupied. However, if the logs are collected through WhaTap, there is no need to maintain log files that occur on individual servers, and only the log maintenance period can be managed centrally.

- **Various analysis perspectives**

To find and predict failures, you have to analyze logs from various perspectives. WhaTap can check the log count trends with specific tags or the logs filtered by specific tags. For frequently used patterns, you can save them as charts so that you can search them at any time.

- **Pattern notification**

Once you have found a pattern of failures, you can set this as an alert to recognize or prevent problems as soon as possible. WhaTap provides [Real-time Log Alert](#) to receive notifications when specific keywords are included on an individual log basis and [Composite Log Alert](#) to receive notifications based on the count trend of logs containing specific tags.

Analyzing logs

Live Tail

Through [Live Tail](#), the logs collected in real time can be viewed as they flow through the screen, just like using the `tail` command. For more information about [Live Tail](#), see [the following](#).

Log Trend

Through [Log Trend](#), you can see all the collected logs or the log count trend with specific tags. If the log counts are closely related to the times of failure occurrence and resolution, the failure cause analysis and response can be accelerated through the log occurrence trend. For more information about the [log trend](#), see [the following](#).

Log Search

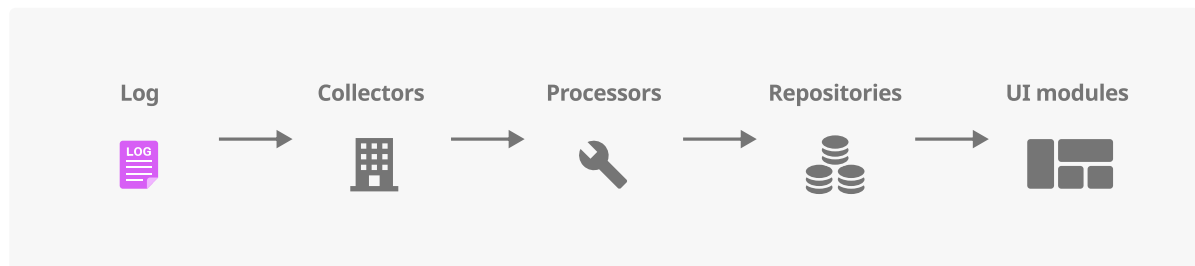
Through [Log Search](#), you can view all the collected logs or the logs with specific tags. The logs generated in a specific time period or specific server can be viewed based on tags. The Adjacent Log function that checks the logs that occurred before and after a selected log, can be used to see the situation in which a specific error or exception occurred. For more information about [Log Search](#), see [the following](#).

Applying The Log Monitoring

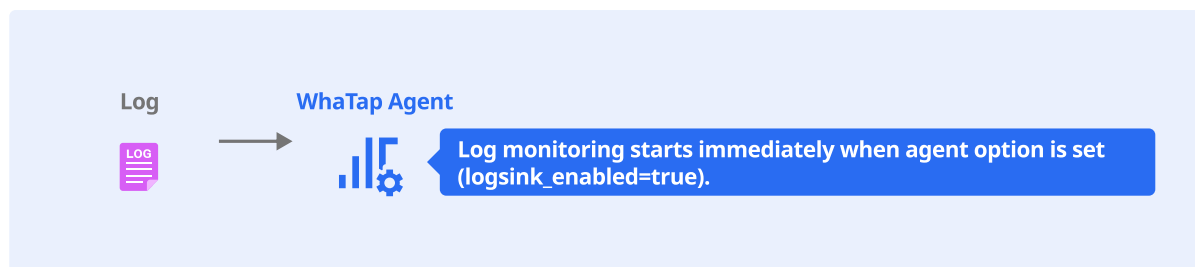
The following guides you to the basic application method for using the WhaTap log monitoring service. WhaTap log monitoring does not require configuring additional agents or applying a parser according to the logs. A simple configuration gets you started quickly.

Operating principle of log monitoring

Common log integration services



WhaTap log monitoring service



A typical log integration service consists of the collector, processor, repository, and UI module. The process of building each module is cumbersome and additional costs are incurred because it requires step-by-step configuration and structuring.

WhaTap log monitoring is easy to apply. Because the previous monitoring agent acts as a collector, the log monitoring can be started simply by turning on the agent option.

- [Java](#) [PHP](#) [Python](#) [Go](#) [Server](#) [Kubernetes](#)

- It directly collects the logs that are forwarded to the log library of your Java application rather than reading the output file.
- Because the logs are collected directly, it does not cause file I/O so the performance impact on the system is very low.
- You can check logs from the transaction traces by obtaining the connection traceability for transaction traces and logs.

! Java log library

Representative Java log libraries are Apache Log4j and Logback.

! They are available in Java Agent 2.1.1 or later.

- The log collection function has been added to the existing agent. The monitoring agent collects by using the output logs in addition to log files.

! They are available in PHP Agent 2.3.2 or later.

- The log collection function has been added to the existing agent. The monitoring agent collects by using the output logs in addition to log files.
- If the transaction ID is output to the log, you can check logs from the transaction traces by obtaining the connection traceability for transaction traces and logs.

! They are available in Python Agent 1.2.2 or later.

- The log collection function has been added to the existing agent. The monitoring agent collects by using the output logs in addition to log files.
- The log collection function has been added to the existing agent. The monitoring agent collects by using the output logs in addition to log files.

 They are available in Server Agent 2.1.2 or later.

- Logs can be collected in the Kubernetes container.
- You can collect logs from the applications in Kubernetes containers.

 They are available in Kubernetes Agent 1.1.35 or later.

Applying the log monitoring

The application method according to the used application is as follows. Before application of Log Monitoring, check the [supported version](#).

1. Check the version of the supported agent and perform [update](#).
2. Set the [options](#) for Log Monitoring.
3. **Enable** the log monitoring.

Java

Learn how to collect logs from your Java application.

PHP

Learn how to collect logs from your PHP application.

 Node.js

Learn how to collect logs from your Node.js application.

 Python

Learn how to collect logs from your Python application.

 Go

Learn how to collect logs from your Go application.

 Server

Learn how to collect logs from your server application.

 Kubernetes

The following guides you through collecting logs from Kubernetes containers and the applications in Kubernetes containers.

Java

To collect logs from your Java application, complete the following 3 steps:

Agent Update

It is available from Java agent 2.1.1. For more information about update, see [the following](#).

Checking the agent settings

Home > Select Project > **Log** > **Log Setting**

Select a project in the initial screen of the WhaTap monitoring service, and then select **Log** > **Log Setting** under Project Menu. Proceed with the process according to the instructions in the **Check agent settings** tab of the **Getting started with log monitoring** section.

1. Under Project Menu, select **Management** > **Agent CONFIG..**
2. In **Write options**, select **Direct Input**. Add the `logsink_enabled=true` option to the input field as follows:
3. Restart the application to apply the log monitoring.

Key options

- **hooklog_enabled** Boolean

Default `false`

It enables the log monitoring by hooking the log library.

 Before running the application, this option must have been enabled in `whatap.conf` to dynamically turn on or off the monitoring through the `logsink_enabled` setting. If the `logsink_enabled` option is set to `true` before running the application, log monitoring is possible without a separate setting.

ⓘ If there is a possibility to use the log monitoring, it is recommended to set this option in advance.

- **hooklog_custom_methods**

Register a custom log. An arbitrary log framework content is delivered. Use this to trace logs of the log module created on the website.

Java

```
package io.home.test;

public class MyLog {
    public void customLog(String log) { ... }
}
```

whatap.conf

```
hooklog_custom_methods=io.home.test.MyLog.customLog
```

- **logsink_enabled** Boolean

Default false

It turns on or off Log Monitoring.

ⓘ Before running the application, if in [whatap.conf](#), the `hooklog_enabled` option is set, this option can dynamically turn on or off the log monitoring.

- **logsink_trace_enabled** Boolean

Default false

Set whether or not to expose the log tab of the transaction trace by inserting the transaction ID into the logs.

Enabling the log monitoring

Home > Select Project > [Log](#) > [Log Setting](#)

You can enable or disable the WhaTap log monitoring with the toggle button in the [Activate log monitoring](#) tab of the [Starting the log monitoring](#) section.

- If you turn on , the log monitoring is enabled. You can try for free for 15 days from the activation date.
- If you turn off , the log monitoring is disabled. Logs are no longer saved.

Role

After agent installation, you can enable the log monitoring settings only when you have the [edit permission](#) on the project. For more information about the roles, see [the following](#).

PHP

To collect logs by your PHP application, check the following:

Agent Update

It is available from PHP agent 2.3.2. For more information about update, see [the following](#).

Checking the agent settings

Home > Select Project > [Log](#) > [Log Setting](#)

Select a project in the initial screen of the WhaTap monitoring service, and then select [Log](#) > [Log Setting](#) under Project Menu. Proceed with the process according to the instructions in the [Check Agent Settings](#) tab of the [Start Log Monitoring](#) section.

Checking the configuration file path

Check the **configuration file path** of the file for log monitoring. You can check it in the CLI environment or on the web.

Checking in the CLI environment

```
$ php -i | grep 'Scan'
Scan this dir for additional .ini files => /etc/php8.0.d
```

ⓘ If the path is "(None)," the configuration file path is [/usr/whatap/php](#).

Checking on the web

If the PHP settings of the CLI and Apache environments are different, check the results of the `phpinfo()`

function on the web. .

Entering the command

Log monitoring starts when you enter the command including the configuration file path.

```
export LOGFILES=/some/path/file1,/some/other/file2
echo "whatap.logsink_enabled=true" | sudo tee -a [configuration file path]/whatap.ini
echo "whatap.logsink.files=$LOGFILES" | sudo tee -a [configuration file path]/whatap.ini
```

Enabling the log monitoring

Home > Select Project > [Log](#) > [Log Setting](#)

You can enable or disable the WhaTap log monitoring with the toggle button in the [Activate log monitoring](#) tab of the [Starting the log monitoring](#) section.

- If you turn on , the log monitoring is enabled. You can try for free for 15 days from the activation date.
- If you turn off , the log monitoring is disabled. Logs are no longer saved.

! Role

After agent installation, you can enable the log monitoring settings only when you have the [edit permission](#) on the project. For more information about the roles, see [the following](#).

Node.js

To collect logs by your Node.js application, check the following.

Agent Update

It is available from Node.js agent 0.5.1. For more information about the update, see [the following](#).

Checking the agent settings

Home > Select Project > Log > Log Setting

Select a project in the initial screen of the WhaTap monitoring service, and then select **Log > Log Setting** under Project Menu. Proceed with the process according to the instructions in the **Check agent settings** tab of the **Getting started with log monitoring** section.

1. Under Project Menu, select **Management > Agent CONFIG..**
2. In **Write options**, select **Direct Input**. Add the `logsink_enabled=true` option to the input field as follows:
3. Restart the application to apply the log monitoring.

Key options

- **logsink_enabled** Boolean

Default `false`

Set whether or not to enable the log monitoring.

- **logsink_trace_txid_enabled** Boolean

Default `true`

Set whether or not to expose the log tab of the transaction trace by inserting the transaction ID into the logs.

- **logsink_limit_content_enabled** Boolean

Default `true`

Set whether or not to limit the maximum size for log messages.

- **logsink_limit_content_length** Number

Default `10,000`

Set the maximum length of the log message. This value is applied only when the `logsink_limit_content_enabled` option is set to `true`.

Enabling the log monitoring

Home > Select Project > [Log](#) > [Log Setting](#)

You can enable or disable the WhaTap log monitoring with the toggle button in the [Activate log monitoring](#) tab of the [Starting the log monitoring](#) section.

- If you turn on , the log monitoring is enabled. You can try for free for 15 days from the activation date.
- If you turn off , the log monitoring is disabled. Logs are no longer saved.

Role

After agent installation, you can enable the log monitoring settings only when you have the [edit permission](#) on the project. For more information about the roles, see [the following](#).

Python

To collect logs by your Python application, check the following.

Agent Update

It is available from Python agent 1.2.2. For more information about update, see [the following](#).

Checking the agent settings

Home > Select Project > [Log](#) > [Log Setting](#)

Select a project in the initial screen of the WhaTap monitoring service, and then select [Log](#) > [Log Setting](#) under Project Menu. Proceed with the process according to the instructions in the [Check Agent Settings](#) tab of the [Start Log Monitoring](#) section.

Enabling the collection of logs

If you enter the command including the configuration file path ([WHATAP_HOME](#)), log collection starts.

```
export LOGFILES={Log file's full path},...  
echo "logsink_enabled=true" | sudo tee -a {Configuration file path}/whatap.conf  
echo "logsink.files=$LOGFILES" | sudo tee -a {Configuration file path}/whatap.conf
```

Linking the log and web transaction

Version 1.3.6 or later

Starting from the version 1.3.6, transactions and logs can be integrated using the following methods. Currently, WhaTap supports the Python's logging and loguru libraries. Configure [whatap.conf](#) according to your Python log libraries.

- logging module

logging

```
echo "trace_logging_enabled=true" | sudo tee -a {configuration file path}/whatap.conf
```

- loguru module

loguru

```
echo "trace_loguru_enabled=true" | sudo tee -a {configuration file path}/whatap.conf
```

Version 1.3.6 or earlier

The transaction ID `{txid}` is output to the log so that the logs generated by each transaction can be viewed separately. WhaTap Monitoring automatically injects `{txid}` into Python LogRecord so that `{txid}` can be output to the log file when setting the formatter.

```
settings.py
...
LOGGING = {
...
    'formatters': {
        ...
    },
    'handlers': {
        ...
    },
    'loggers': {
        ...
        '{logger_name}': {
            'handlers': [...],
            ...
        },
    },
}
```

```

try:
    import whatap.trace.mod.logging as whatap_logging
    if whatap_logging.logging_injection_processed:
        LOGGING["formatters"]["whatap.formatter"]={
            '()': 'django.utils.log.ServerFormatter',
            'format': '[{server_time}] -- {{ "@txid" : "{txid}" }} -- {message}',
            'style': '{',
        }
        LOGGING["handlers"]["whatap"]={
            'level': 'DEBUG',
            'class': 'logging.handlers.RotatingFileHandler',
            'filename': os.path.join(BASE_DIR, 'logs','whatap_log.log'),
            'formatter': 'whatap.formatter',
        }
        LOGGING["loggers"][Logger name]["handlers"].append('whatap')
except:
    pass
...

```

Enabling the log monitoring

Home > Select Project > [Log](#) > [Log Setting](#)

You can enable or disable the WhaTap log monitoring with the toggle button in the [Activate log monitoring](#) tab of the [Starting the log monitoring](#) section.

- If you turn on , the log monitoring is enabled. You can try for free for 15 days from the activation date.
- If you turn off , the log monitoring is disabled. Logs are no longer saved.

! Role

After agent installation, you can enable the log monitoring settings only when you have the [edit permission](#) on the project. For more information about the roles, see [the following](#).

Go

To collect logs by your Go application, check the following.

Checking the agent settings

Home > Select Project > [Log](#) > [Log Setting](#)

Select a project in the initial screen of the WhaTap monitoring service, and then select [Log](#) > [Log Setting](#) under Project Menu. Proceed with the process according to the instructions in the [Check Agent Settings](#) tab of the [Start Log Monitoring](#) section.

Enabling the collection of logs

If you enter the following command, log collection is started immediately.

```
export LOGFILES=/some/path/file1,/some/other/file2
echo "logsink_enabled=true" | sudo tee -a /usr/whatap/agent/whatap.conf
echo "logsink.files=$LOGFILES" | sudo tee -a /usr/whatap/agent/whatap.conf
```

Enabling the log monitoring

Home > Select Project > [Log](#) > [Log Setting](#)

You can enable or disable the WhaTap log monitoring with the toggle button in the [Activate log monitoring](#) tab of the [Starting the log monitoring](#) section.

- If you turn on , the log monitoring is enabled. You can try for free for 15 days from the activation date.
- If you turn off , the log monitoring is disabled. Logs are no longer saved.

! Role

After agent installation, you can enable the log monitoring settings only when you have the [edit](#)

! permission on the project. For more information about the roles, see [the following](#).

Server

To collect logs by your server application, check the following:

Agent Update

It is available from Server agent 2.1.2. For more information about update, see [the following](#).

Checking the agent settings

Home > Select Project > Log > Log Settin_

Select a project in the initial screen of the WhaTap monitoring service, and then select **Log > Log Setting** under Project Menu. In the OS selection tab at the top of **Check Agent CONF.**, select a server OS (**Linux (shell)**, **Windows (Powershell)**). See **Basic Installation** or **Install with Category** for the process.

! The following configuration requires restart of the agent.

Linux Shell

- [Basic installation](#)

Linux Shell

```
export LOGFILES=/some/path/file1,/some/other/file2
echo "logsink.files=$LOGFILES" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

- [Install with Category](#)

Linux Shell

```
1 cd /usr/whatap/infra
```

```

2  sudo mkdir extension
3
4  cat <<EOL | sudo tee extension/logsink.conf > /dev/null
5  [[inputs.logsink]]
6    category = "serverlog"
7    ## Whether to transfer the log generation statistics as separate data
8    stats_enabled = true
9    ## Log generation statistics category
10   stats_category = "logsink_stats"
11   ## Set the log file name to be excluded if the log file path contains asterisk (*).
12   excludeNames = [ ".gz", ".zip" ]
13   [[inputs.logsink.file]]
14     ## When setting a log file, you can set the date pattern (strftime.org).
15     path = "/some/path/%Y-%m-%d/.log"
16     disabled = false
17     encoding = "utf-8"
18
19   [[inputs.logsink.file]]
20     path = "/some/other/log"
21     disabled = false
22     encoding = "utf-8"
23
24   [[inputs.logsink.file]]
25     ## When searching for the keyword in the line-by-line log, merge it with the previous log.
26     nowrap_keywords = ["Caused by:", "Test"]
27
28   [[inputs.logsink.file]]
29     ## When entering the project code and project license, the logs can be transferred to a desiged project in the
30     same region.
31     # pcode = Project code
32     # license = "Project license"
33
34   [[inputs.logsink.file]]
35     # whatap_host_ip = "Collection server IP1/Collection server IP2"
36     # whatap_host_port = 6600
37
38   [[inputs.logsink.file]]
39     path = "/tmp/mixed.log"
40     disabled = false

```

```

40 encoding = "utf-8"
41 ## The [{ "A":1,"B":2},{ "C":3,"D":4},...] format can be divided into individual logs.{ "A":1,"B":2} { "C":3,"D":4}
42 multiline_pattern = "simple_json_array"
43 EOL
44
45 sudo service whatap-infra restart

```

Windows Powershell

- [Basic installation](#)

Windows Powershell

```

$LOGFILES="c:\\whatap\\logs\\%Y-%m-%d\\*.log,c:\\whatap\\logs\\*.log"
Add-Content "c:\\Program Files\\WhatapInfra\\whatap.conf" -Value "logsink.files=$LOGFILES"

```

- [Install with Category](#)

Windows Powershell

```

1  # The administrator role required
2  New-Item -type "Directory" -Path "C:\\Program Files\\WhatapInfra\\extension"
3
4  $contentToAdd = @"
5  [[inputs.logsink]]
6  category = "serverlog"
7  ## Whether to transfer the log generation statistics as separate data
8  stats_enabled = true
9  ## Log generation statistics category
10 stats_category = "logsink_stats"
11 ## Set the log file name to be excluded when the log file path contains asterisk (*).
12 excludeNames = [ ".gz",".zip" ]
13 [[inputs.logsink.file]]
14 ## The date pattern (strftime.org) can be entered when setting the log file.
15 path = "c:\\whatap\\logs%Y-%m-%d_.log"
16 disabled = false
17 encoding = "euc-kr"
18

```

```

19 [[inputs.logsink.file]]
20 ## When searching for the keyword in the line-by-line logs, it merges with the previous log.
21 nowrap_keywords = ["Caused by:", "Test"]
22
23 [[inputs.logsink.file]]
24 ## When entering the project code and project license, logs can be transferred to a desired project in the same
   region.
25 # pcode = Project code
26 # license = "Project license"
27
28 [[inputs.logsink.file]]
29 # whatap_host_ip = "Collection server IP1/Collection server IP2"
30 # whatap_host_port = 6600
31
32 [[inputs.logsink.file]]
33 path = "/tmp/mixed.log"
34 disabled = false
35 encoding = "utf-8"
36 ## The [{"A":1,"B":2},{ "C":3,"D":4},...] format can be divided into individual logs.{"A":1,"B":2} {"C":3,"D":4}
37 multiline_pattern = "simple_json_array"
38
39 "@
40
41 New-Item -path "C:\Program Files\WhatapInfra\extension" -name "logsink.conf" -type "file" -value $contentToAdd
   -Force
42
43 Restart-Service "Whatap Infra"

```

Configuring options

- `stats_enabled` : Set whether or not to collect the collection status data. The default value is `false` . The value must be set to `true` . If set to `true` , statistical data is generated in the category (`logsink_stats`) set in the following `stats_category` .
- `stats_category` : Set the metrics category to store the collection status data in. The value must be set to `logsink_stats` . Statistical data fields are as follows:
 - `file`

- `checkInterval`
- `encoding`
- `filepos`
- `checkedLocalTime`
- `lastupdatedLocalTime`
- `fileSize`
- `error`
- `firstCheck`
- `transferBytes`
- `excludeNames` : By including asterisks (*) in the log file path, you can set the file name to exclude non log files. You can set multiple values using comma (,) as a separator.

Example

```
excludeNames = [ ".gz", ".zip" ]
```

- `nowrap_keywords` : While searching logs by line, if any keyword is detected by a specified option value, it is merged with the previous log.
- `pcode` : Enter the project code of the same region to which you want to send the logs.
- `license` : Enter the license code of the project in the same region to which you want to send the logs.

ⓘ In case of the `pcode` and `license` options, it is supported from Server Agent 2.7.4 or later.

Configuring the log options for Windows events

When collecting Windows event logs, you can set the options as follows:

```
1 # The administrator role required
2 New-Item -type "Directory" -Path "C:\Program Files\WhatapInfra\extension"
3
4 $contentToAdd = @"
5 [[inputs.win_eventlog]]
```

```

6  category = "win_event_log"
7  stats_category = "win_event_log_stats"
8  stats_enabled = true
9  enabled = true
10 [[Inputs.win_eventlog.file]]
11     #true | false
12     enabled = true
13     # Application, Security, Setup, System, ForwardedEvents
14     file = "Application"
15     #1: Information, 2: Warning 3: Error 4: Audit Success 5 Audit Fail
16     #event_type =
17     #event_id =
18     #event_id =
19     #event source name
20     #source_name = ""
21     #When entering the project code and project license, logs can be transferred to the desired project in the same region.
22     #pcode = Project code
23     #license = "Project license"
24     #whatap_host_ip = "Collection server IP1/Collection server IP2"
25     #whatap_host_port = 6600
26
27 "@
28
29 New-Item -path "C:\Program Files\WhatapInfra\extension" -name "win_eventlog.conf" -type "file" -value $contentToAdd
30 -Force
31 Restart-Service "Whatap Infra"

```

- It is required to specify the `category` .
e.g. `win_event_log`
- It is required to specify the statistics category (`stats_category`).
e.g. `win_event_log_stats`
- The statistics category On/Off (`stats_enabled`) is required.
e.g. `true` or `false`
- The collection On/Off (`enabled`) is required.

e.g. `true` or `false`

- The file-based collection On/Off (`enabled`) is required.

e.g. `true` or `false`

- The file (`file`) is required.

e.g. `Application` , `Security` , `Setup` , `System` , `Forwarded`

- The event type (`event_type`) is optional.

e.g. `1` , `2` , `3` , `4` , `5`

! Event type

1. Information
2. Warning
3. Error
4. Audit Success
5. Audit Fail

- The event ID (`event_id`) is optional.
- The event source name (`source_name`) is optional.
- Project code (`pcode`) optional
- Project license (`license`) optional

- ! • For Windows event log collection, the Server Agent 2.5.2 or later is supported.
- Among the Windows event log options, `pcode` and `license` are supported in the Server Agent 2.7.4 or later.

Specifying and separating multiple files

Specifying multiple files

To categorize multiple log files under the same category, add each log file path into the `[[inputs.logsink.file]]` entry and specify the file path by using the `path` setting. Additionally, you can configure additional settings, such as log generation statistics and options such as `category` , `stats_enabled` , and `stats_category` . The example is where the `/root/test1` and `/root/test2` files are assigned the same category (`serverlog`).

```
[[inputs.logsink]]
  category = "serverlog"
  stats_enabled = true
  stats_category = "logsink_stats"
  excludeNames = [ ".gz", ".zip" ]
```

```
[[inputs.logsink.file]]
  path = "/root/test1"
  disabled = false
  encoding = "utf-8"
```

```
[[inputs.logsink.file]]
  path = "/root/test2"
  disabled = false
  encoding = "utf-8"
```

❗ For information about options such as `category` , `stats_enabled` , `stats_category` , and `nowrap_keywords` , see the guidance [above](#).

In this example, you can see the following in **Live Tail**.

serverlog													
▼	oname												
▼	APPSVR	2024-10-11	18:14:30.325	file	/root/test1	pcode	34	oname	APPSVR	agenttime	1728638069515	oid	1988910709
				kdjfhakdhgldfkjggha;dfghad;fkjggha;dfkjggha;dfgjha;fkjgh;fgjh									
▼	APPSVR	2024-10-11	18:14:30.325	file	/root/test1	pcode	34	oname	APPSVR	agenttime	1728638069515	oid	1988910709
				kdjfhakdhgldfkjggha;dfghad;fkjggha;dfkjggha;dfgjha;fkjgh;fgjh									
▼	APPSVR	2024-10-11	18:14:30.325	file	/root/test1	pcode	34	oname	APPSVR	agenttime	1728638069515	oid	1988910709
				kdjfhakdhgldfkjggha;dfghad;fkjggha;dfkjggha;dfgjha;fkjgh;fgjh									
▼	APPSVR	2024-10-11	18:14:30.325	file	/root/test1	pcode	34	oname	APPSVR	agenttime	1728638069515	oid	1988910709
				kdjfhakdhgldfkjggha;dfghad;fkjggha;dfkjggha;dfgjha;fkjgh;fgjh									
▼	APPSVR	2024-10-11	18:14:30.325	file	/root/test1	pcode	34	oname	APPSVR	agenttime	1728638069515	oid	1988910709
				kdjfhakdhgldfkjggha;dfghad;fkjggha;dfkjggha;dfgjha;fkjgh;fgjh									
▼	APPSVR	2024-10-11	18:14:40.326	file	/root/test2	pcode	34	oname	APPSVR	agenttime	1728638079521	oid	1988910709
				sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbcvmbn.bcmn									

File separation

To specify different categories for log files, create separate `logsink{number}.conf` files and then set different `category` values in each file. The following example shows how to set different log categories through `logsink.conf` and `logsink1.conf`.

logsink.conf

```
# cat logsink.conf
[[inputs.logsink]]
  category = "serverlog1"
  stats_enabled = true
  stats_category = "logsink_stats"
  excludeNames = [ ".gz", ".zip" ]

[[inputs.logsink.file]]
  path = "/root/test1"
  disabled = false
  encoding = "utf-8"
```

logsink1.conf

```
#cat logsink1.conf
[[inputs.logsink]]
  category = "serverlog2"
  stats_enabled = true
  stats_category = "logsink_stats"
  excludeNames = [ ".gz", ".zip" ]

[[inputs.logsink.file]]
  path = "/root/test2"
  disabled = false
  encoding = "utf-8"
```

❗ For information about options such as `category` , `stats_enabled` , `stats_category` , and `nowrap_keywords` , see the guidance [above](#).

In this example, you can see the following in **Live Tail**.

Filter		View	
All logs			
▼	oname		
▼	APPSVR	2024-10-11 18:20:55.084	file /root/test1 pcode 34 oname APPSVR agenttime 1728638454313 oid 1988910709 category serverlog1 kdjfhakdhgldkjg ha,dfghad;fkjggha;dfkjgha;dfgjha;fkgjha;fgjh
▼	APPSVR	2024-10-11 18:20:55.087	file /root/test1 pcode 34 oname APPSVR agenttime 1728638454313 oid 1988910709 category serverlog1 kdjfhakdhgldkjg ha,dfghad;fkjggha;dfkjgha;dfgjha;fkgjha;fgjh
▼	APPSVR	2024-10-11 18:21:05.103	file /root/test2 pcode 34 oname APPSVR agenttime 1728638464315 oid 1988910709 category serverlog2 sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbcvmbn.bcmn
▼	APPSVR	2024-10-11 18:21:05.104	file /root/test2 pcode 34 oname APPSVR agenttime 1728638464315 oid 1988910709 category serverlog2 sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbcvmbn.bcmn
▼	APPSVR	2024-10-11 18:21:05.104	file /root/test2 pcode 34 oname APPSVR agenttime 1728638464315 oid 1988910709 category serverlog2 sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbcvmbn.bcmn
▼	APPSVR	2024-10-11 18:21:05.104	file /root/test2 pcode 34 oname APPSVR agenttime 1728638464315 oid 1988910709 category serverlog2 sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbcvmbn.bcmn
▼	APPSVR	2024-10-11 18:21:05.104	file /root/test2 pcode 34 oname APPSVR agenttime 1728638464315 oid 1988910709 category serverlog2 sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbcvmbn.bcmn

Enabling the log monitoring

Home > Select Project > Log > Log Setting

You can enable or disable the WhaTap log monitoring with the toggle button in the **Activate log monitoring** tab of the **Starting the log monitoring** section.

- If you turn on , the log monitoring is enabled. You can try for free for 15 days from the activation date.
- If you turn off , the log monitoring is disabled. Logs are no longer saved.

Role

After agent installation, you can enable the log monitoring settings only when you have the [edit permission](#) on the project. For more information about the roles, see [the following](#).

Kubernetes

To collect logs from Kubernetes containers and the applications in Kubernetes containers, check the following.

Agent Update

It is available from Kubernetes agent 1.1.35. For more information about update, see [the following](#).

Checking the agent settings

Home > Select Project > [Log](#) > [Log Setting](#)

Select a project in the initial screen of the WhaTap monitoring service, and then select [Log](#) > [Log Setting](#) under Project Menu. Proceed with the process according to the instructions in the [Check Agent CONF.](#) tab of the [Set up the agent and enable log monitoring](#) section.

Enabling the container log collection

To collect logs in Kubernetes containers, select [Apply log settings](#) in the [Check agent configuration](#) tab.

Enabling application log collection in the container

It is available from Java 2.1.1 and Python 1.2.2. To collect logs of the applications running on Kubernetes containers, see the following.

1. On the lower part of [Check agent settings](#), select **1**  [Agent CONFIG..](#)
2. Go to [Application Agent CONFIG.](#), and then select [Direct Input](#) in the **2** [Write Options](#) window.
3. Enter the [key](#), `logsink_enabled` and the [value](#), `true` of the following agent configuration command in the **3** field.

```
logsink_enabled=true
```


4. Select  **Apply**. You can collect application logs in the Kubernetes containers.

- For more information about the collection of Java application logs, see [the following](#).
- For more information about the collection of Python application logs, see [the following](#).
- For more information about the collection of Go application logs, see [the following](#).

Enabling the log monitoring

Home > Select Project > [Log](#) > [Log Setting](#)

You can enable or disable the WhaTap log monitoring with the toggle button in the [Activate log monitoring](#) tab of the [Starting the log monitoring](#) section.

- If you turn on , the log monitoring is enabled. You can try for free for 15 days from the activation date.
- If you turn off , the log monitoring is disabled. Logs are no longer saved.

Role

After agent installation, you can enable the log monitoring settings only when you have the [edit permission](#) on the project. For more information about the roles, see [the following](#).

Kubernetes log monitoring category guide

You can check various logs related to Kubernetes. The monitoring categories provided by WhaTap Kubernetes are as follows. Depending on the settings, duplicate log contents may be stored. Be sure to check for duplicates.

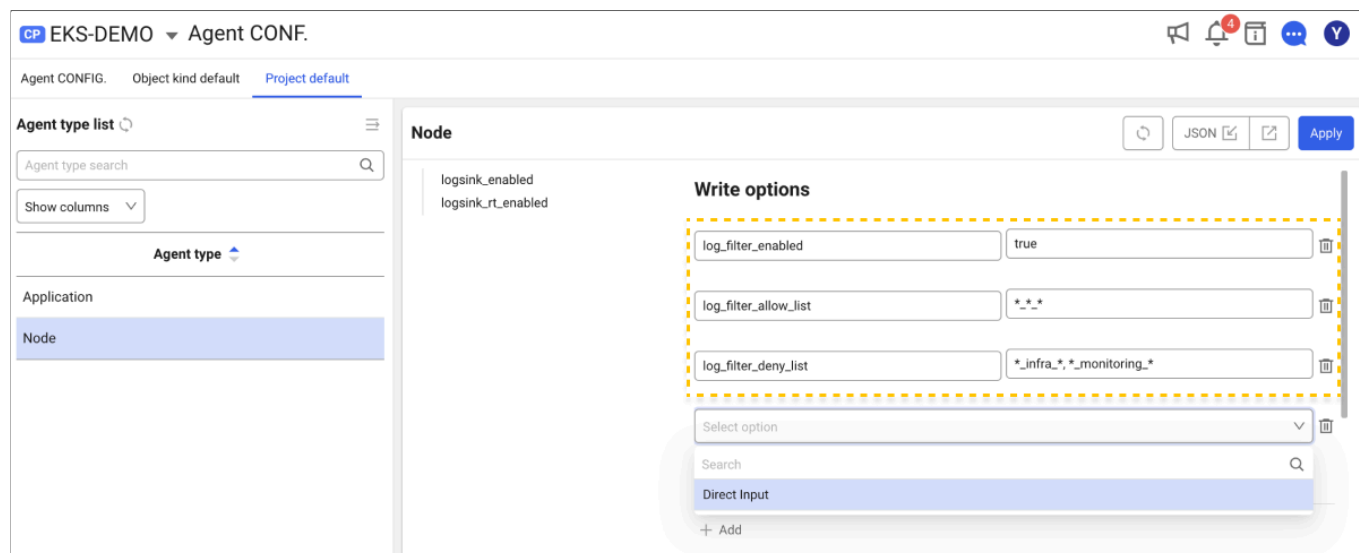
Category	Description
#K8sEvent	• Logs that store the events that occur in Kubernetes • Generation by default regardless of user settings

Category	Description
#WhatapEvent	• Logs that store the events that occur by WhaTap event settings • Generation by default regardless of user settings
containerStdout	• Container Standard Out logs • Generation by user settings • When <code>logsink_enabled=true</code> setting is added to the node agent
AppLog	• Application logs in the container • Generation by user settings • When <code>logsink_enabled=true</code> setting is added to the application agent

Setting the containerStdOut log filter

Home > Select Project > **Management** > **Agent CONF.**

The following guides you to filtering options to select information needed in the Kubernetes logs. You can set which logs to allow or exclude through filtering. In **Agent CONF.**, select **Direct Input** in the **Write options** manner.



Log naming conventions

The Kubernetes containerStdOut logs are generated under the `/var/log/containers/` path on the node. They keep the following naming conventions.

```
<podName>_<namespace>_<containerName>-<containerId>.log
```

Log filtering options

- **log_filter_enabled** `bool`

Default `false`

It sets whether to use log filters.

- **log_filter_allow_list** `list`

It sets the list of logs to allow. It indicates the items to be included for filtering.

- **log_filter_deny_list** `list`

It sets the list of logs to exclude. It indicates the items to be excluded for filtering.

Log filtering operation

Log filters work only when the `log_filter_enabled` option is active. You can selectively collect logs via `log_filter_allow_list` and `log_filter_deny_list` when the value of the option is set to `true`.

Log filters work on a blacklist basis. For example, if you enable `log_filter_enabled` and do not set the items to be added to the `log_filter_allow_list` option, the log collection for all containers is blocked by default.

Additionally, in the log filters, deny rules take precedence over allow rules. If the same items are set in both allow and deny rules, the deny rule takes precedence and logs are not collected.

Log filter example

Collecting logs for a single namespace

- Allow `log_filter_allow_list` `*_infra_*`

All containers that exist in the `infra` namespace are targeted for collection.

Collecting multiple namespace logs

- Allow `log_filter_allow_list` `*_infra_*, *_monitoring_*`

All containers that exist in the `infra` and `monitoring` namespaces are specified as collection targets.

Pods containing specific terms are excluded.

- Allow `log_filter_allow_list` `*_*_*`
- Deny `log_filter_deny_list` `*prod*_**`

All containers are targeted for collection, but the logs that contain `prod` in `podName` are excluded.

Pods containing specific terms are collected.

- Allow `log_filter_allow_list` `*prod*_**`

Only the logs that contain `prod` in `podName` are collected.

Multi-namespace logs are collected and Pods containing specific terms are excluded.

- Allow `log_filter_allow_list` `*_infra_*, *_monitoring_*`
- Deny `log_filter_deny_list` `*prod*_**`

The logs for the `infra` and `monitoring` namespaces are collected, and the logs that contain `prod` in `podName` are excluded.

The container logs that start with a specific term in the container name are excluded.

- Allow `log_filter_allow_list` `*_*_db-*`

The container logs whose `containerName` starts with `db` in all namespaces are excluded.

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

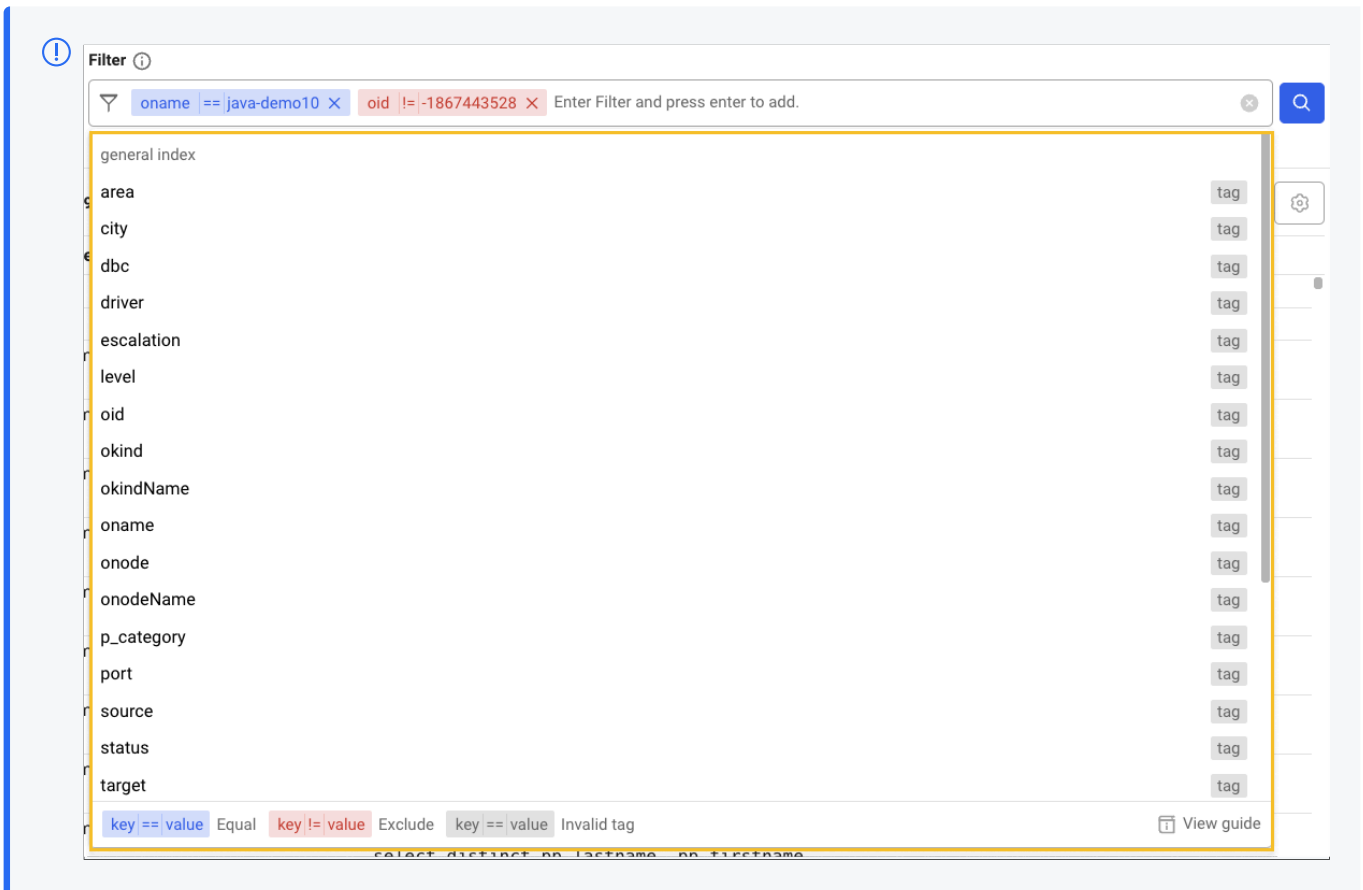
When a filter is applied, the logs that match the specified conditions are filtered. You can enter multiple filters. OR (`||`) if the filters have the same tags, otherwise AND (`&&`).

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**.

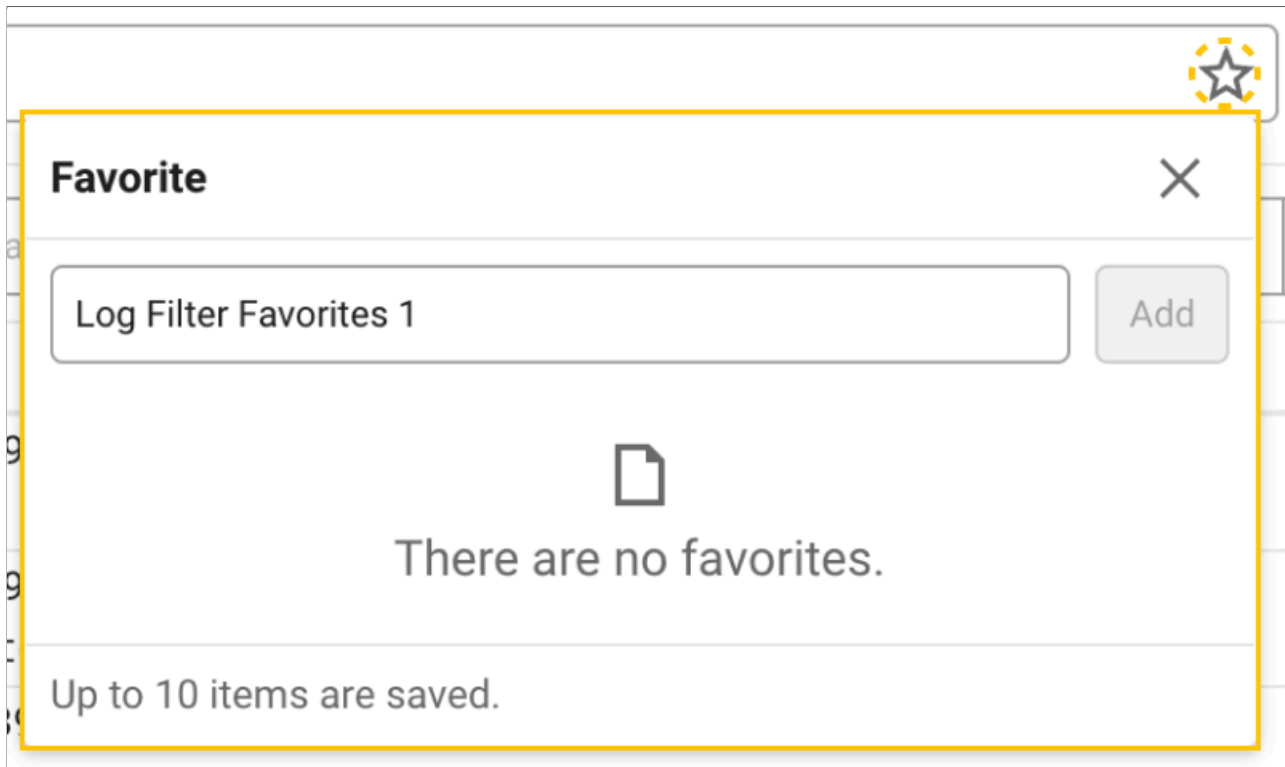
You can also select a recommended value from the **Guide UI** below the input field by clicking it or navigating with the arrow keys.

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.



- 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.

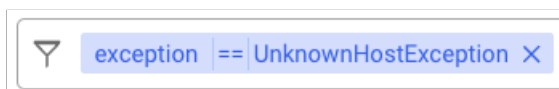
Search Key

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.



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*Ilo*</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

Enter Filter and press enter to add.

content == *select*

a

select

🔍

⏏

⏮

⏭

⏏

⚙

	oname	Timestamp	Log
b	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

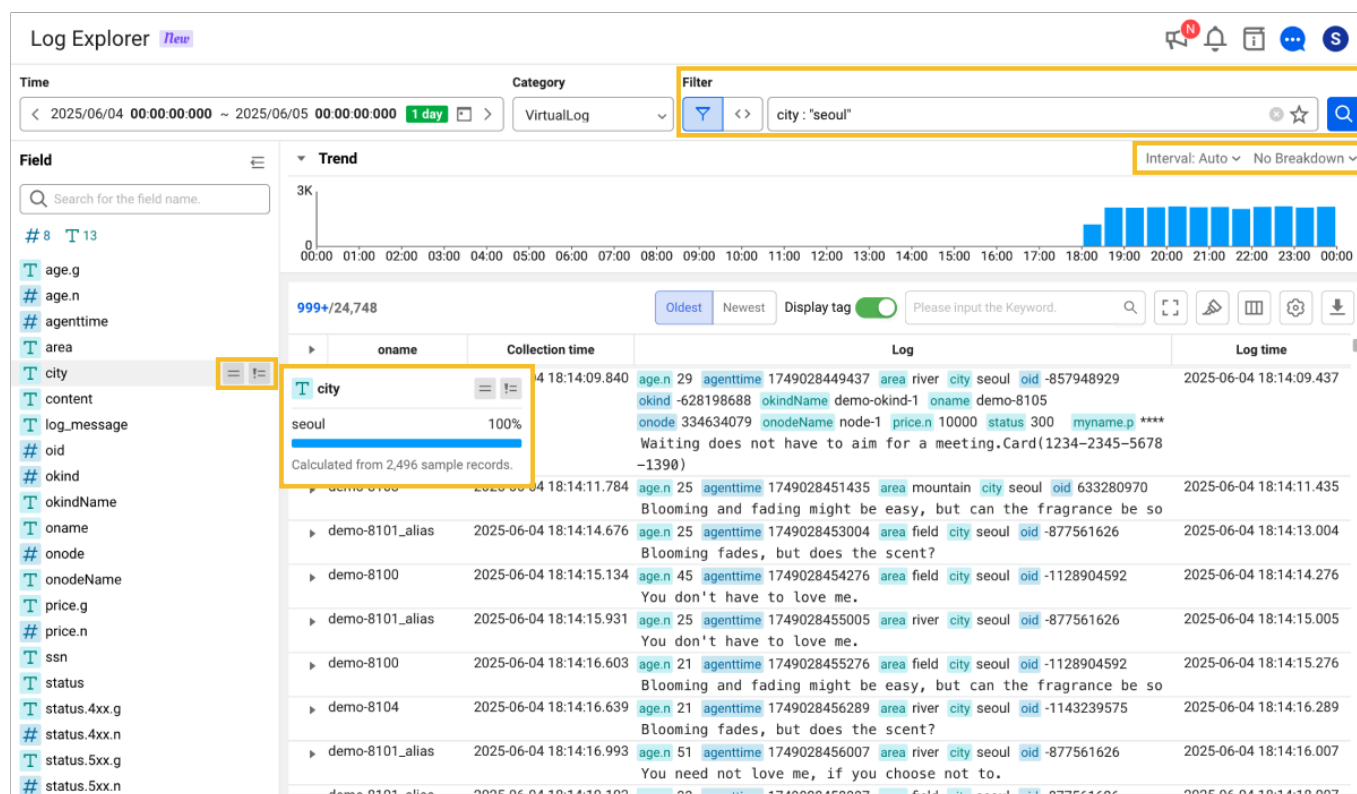
ⓘ Without the **Log Read** role, you cannot enter the menu.

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.

WhaTap Log Search Query Syntax

✓ This document describes the WhaTap log search query syntax used in the Log Explorer.

1. Equal

- `field : value`

2. Not

- `not field : value`

3. Wildcard (Only applicable to `String`-type fields; do not use `"` around the value)

- `field : val*`

4. Exist

- `field : *`

5. Range (Only applicable to `Number`-type fields)

- Operators supported: `<`, `>`, `<=`, `>=`
- Example: `field < 30 and field >= 10`

6. Combining Multiple Queries

- AND example: `field < 30 and field >= 10`
- OR example: `field < 30 or field >= 10`

7. Grouping

- Example: `(field < 30 or field >= 10) and other : 70`

8. Escaping Special Characters

- Special characters supported by Lucene escape: `&&` `|` `!` `()` `{}` `^` `"` `~` `*` `?` `:` `\` `/`
- Use `\` before the character to escape
- Example: To search `(1+1):2`, use `\\(1\\+1\\)\\:2`

Search Index Field Types

Supported field types: `Number` and `String`

- `Number` : Numeric values such as long, double, float
 - Use syntax like `field : "value"`
- `String` : Full text such as email body
 - Use syntax like `field : value`
- `Boolean` : True or False
 - Use as `field : true` or `field : false`

Log Trend

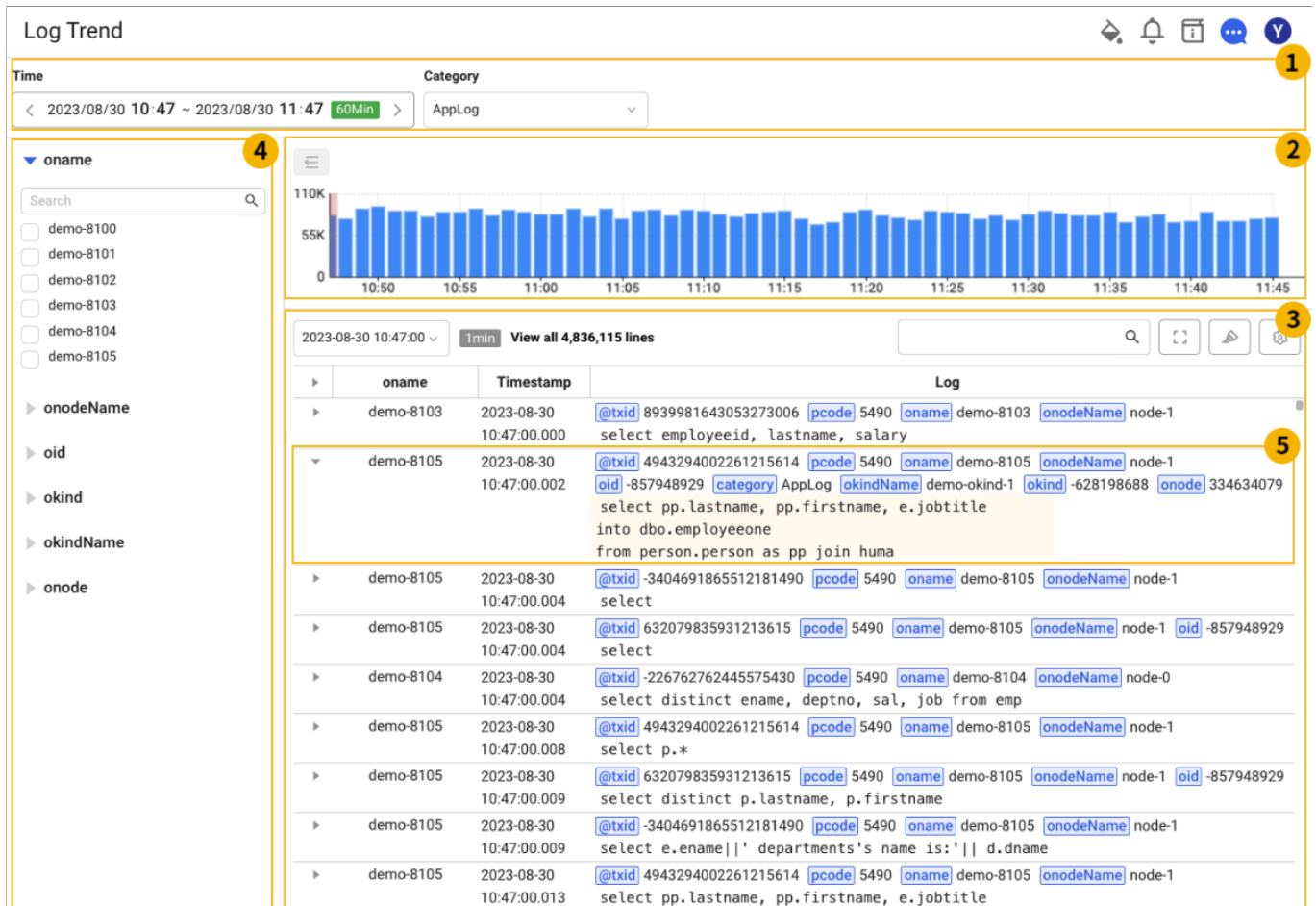
ⓘ Without the **Log Read** role, you cannot enter the menu.

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
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
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
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
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
Servlet.service() for servlet [DispatcherServlet] in context with path [/] threw exception [Request processing failed: io.home.test.logback02starter.base.error]												

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:

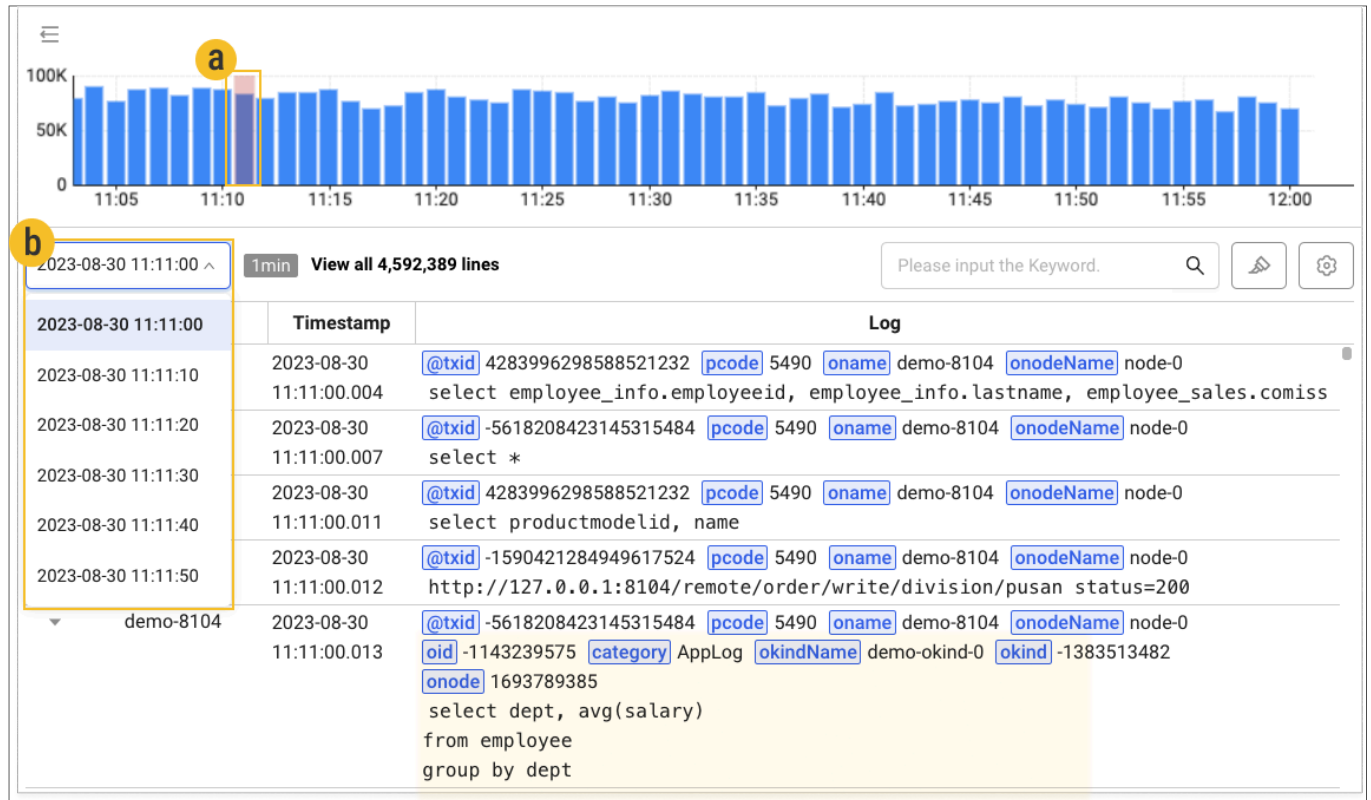
String to input	Description	Result
a b c	Separate each keyword with a space.	a, b, c
"Whatap is good."	To include spaces in keywords, wrap them in "'" or "\"".	Whatap is good.
"Whatap\\ is good."	If \ is included in the keyword surrounded by "", enter it as \\.	Whatap\ is good.

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 Search

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

Home > Select Project > **Log** > **Log Search**

In **Log Search**, you can search a large number of integrated logs under various conditions and specify the desired logs. Multiple search conditions can be specified with parsed keys and values, so only the log data that matches the desired conditions are extracted.

The searched log data is imported to the dynamic page line by line. If the scroll reaches the bottom, the next data is automatically retrieved and displayed.

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

1 Log Search

Time: < 2023/08/30 11:22 ~ 2023/08/30 12:22 60Min > Filter: category AppLog Enter Filter and press enter to add. category == AppLog

2 AppLog (4,517,902)

AppLog @txid oid okind okindName oname onode onodeName

AppStdErr (461)

AppStdErr @txid oid okind okindName oname onode onodeName

AppStdOut (19,839)

AppStdOut oid okind okindName oname onode onodeName

3 Of the total 4,538,718 results, 9999+ match your search. Oldest Newest Display tag Please input the Keyword.

▶	oname	Timestamp	Log
▶	demo-8101	2023-08-30 11:22:00.019	@txid -2940368816900096605 pcode 5490 oname demo-8101 onodeName node-1 http://127.0.0.1:8101/remote/account/pickup/dept/daegu status=200
▶	demo-8101	2023-08-30 11:22:00.025	@txid -6539276394531757588 pcode 5490 oname demo-8101 onodeName node-1 select ename, job, sal + 100 from emp
▼	demo-8101	2023-08-30 11:22:00.020	@txid -877561626 pcode 5490 oname demo-8101 onodeName node-1 oid -877561626 category AppLog okindName demo-okind-1 okind -628198688 onode 336434079 select distinct pp.lastname, pp.firstname from person.person pp join humanresources.employee e on e
▶	demo-8101	2023-08-30 11:22:00.032	@txid -6539276394531757588 pcode 5490 oname demo-8101 onodeName node-1 select productid, avg(orderqty) as averagequantity, sum(linetotal) as total
▶	demo-8101	2023-08-30 11:22:00.038	@txid -3664464458700254001 pcode 5490 oname demo-8101 onodeName node-1 select distinct ename, deptno, sal, job from emp
▶	demo-8101	2023-08-30 11:22:00.032	@txid -3664464458700254001 pcode 5490 oname demo-8101 onodeName node-1 select e.ename, d.dname
▶	demo-8101	2023-08-30 11:22:00.043	@txid -3664464458700254001 pcode 5490 oname demo-8101 onodeName node-1 select productmodelid, name
▶	demo-8101	2023-08-30 11:22:00.049	@txid -3664464458700254001 pcode 5490 oname demo-8101 onodeName node-1 select ename, sal from emp
▶	demo-8101	2023-08-30 11:22:00.054	@txid -3664464458700254001 pcode 5490 oname demo-8101 onodeName node-1 select ename, sal+1000 from emp
▶	demo-8101	2023-08-30 11:22:00.062	@txid -129020984714615108 pcode 5490 oname demo-8101 onodeName node-1 select employee_id, dept, name, age, salary
▶	demo-8101	2023-08-30 11:22:00.060	@txid -3664464458700254001 pcode 5490 oname demo-8101 onodeName node-1 select ename, job, sal + 100 from emp
▶	demo-8101	2023-08-30 11:22:00.067	@txid -3664464458700254001 pcode 5490 oname demo-8101 onodeName node-1 select p.name as productname,
▶	demo-8101	2023-08-30 11:22:00.067	@txid -129020984714615108 pcode 5490 oname demo-8101 onodeName node-1 select e.ename ' departments's name is:' d.dname
▶	demo-8101	2023-08-30 11:22:00.072	@txid -3664464458700254001 pcode 5490 oname demo-8101 onodeName node-1 select salesorderid, sum(linetotal) as subtotal

4

Request Data

- If the scroll reaches the bottom, the next data is retrieved. You can view 10,000 logs at a time.
- **3** You can see the total number of logs viewed from the upper left of the log table.
- Log data can be queried in chronological order. On the upper right of the **3** log table, select a desired search method among **Oldest** and **Newest**.
- After specifying the time range, select **Apply** to finish the search time setting, and then select **Search** to search for data.
- On the upper right of the **3** log table, select the **Log full screen** icon, you can see the **Log** and

Timestamp in the full screen.

- 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
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
2023-12-18 14:31:02.586	[level]	error	[pcode]	2277	[agenttime]	1702877462043	[oid]	778873916	[category]	AppServer	[event_status]	error
2023-12-18 14:31:02.586	[level]	error	[pcode]	2277	[agenttime]	1702877462057	[oid]	778873916	[category]	AppServer	[event_status]	error
2023-12-18 14:31:02.586	[level]	error	[pcode]	2277	[agenttime]	1702877462087	[oid]	778873916	[category]	AppServer	[event_status]	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.

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

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 **4**.
- If you select a tag in the log, a drop-down menu appears that allows you to perform **Copy**, **Search**, **Exclusion search**, and **Adjacent Log**.

Filter

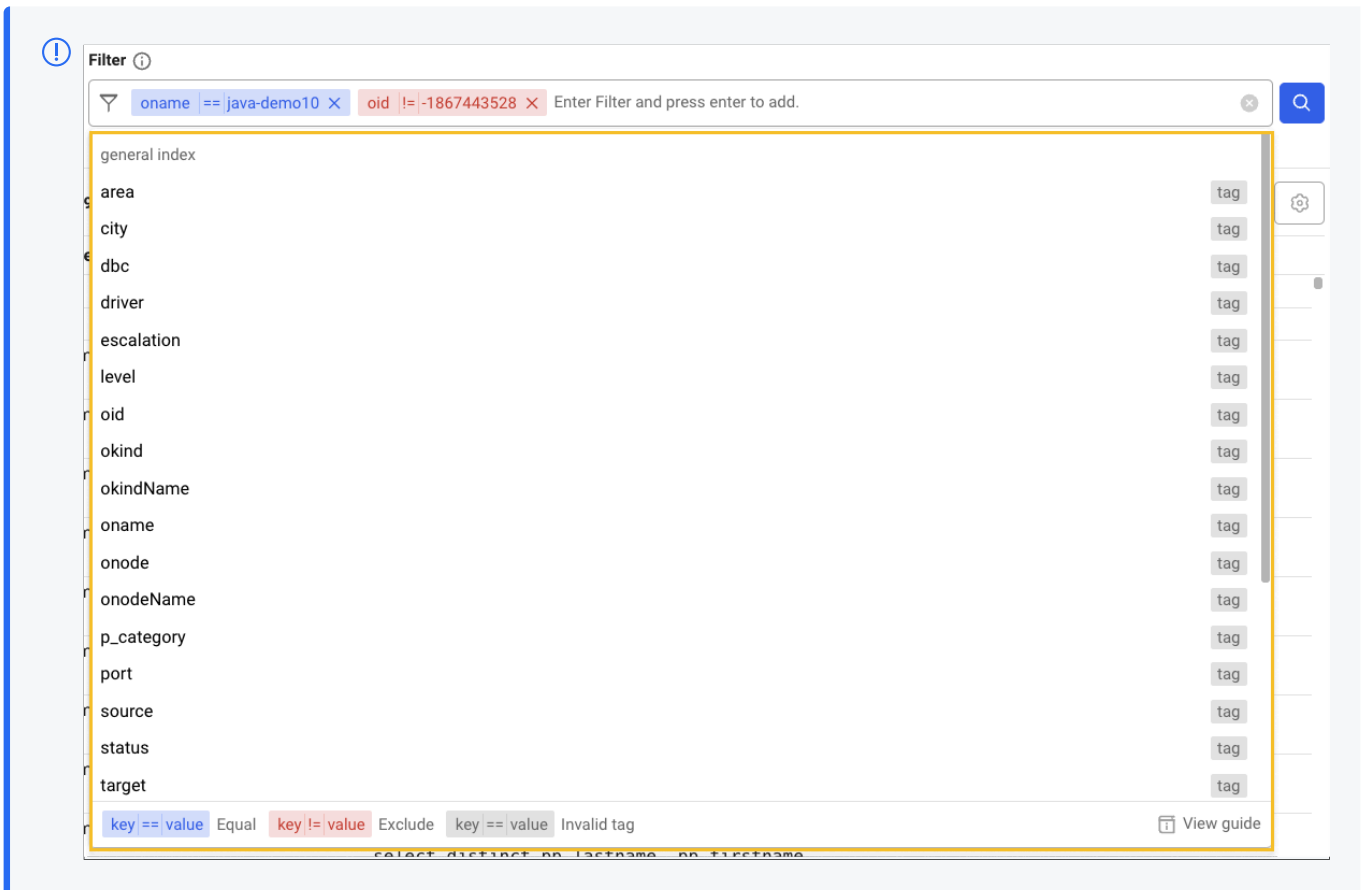
Apply Filter

In **Time selector** on the left of **1**, you can specify the time range. On the right, 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**.

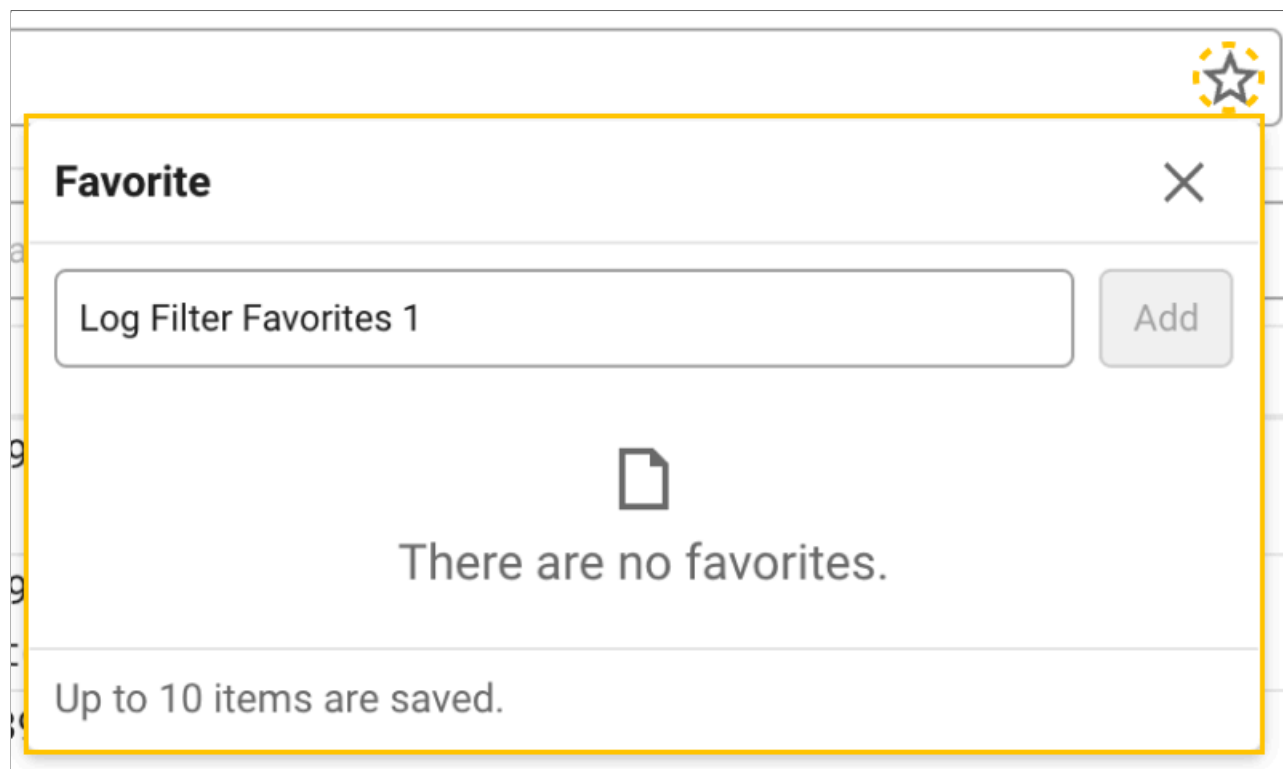
You can also select a recommended value from the **Guide UI** below the input field by clicking it or navigating with the arrow keys.

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.

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*

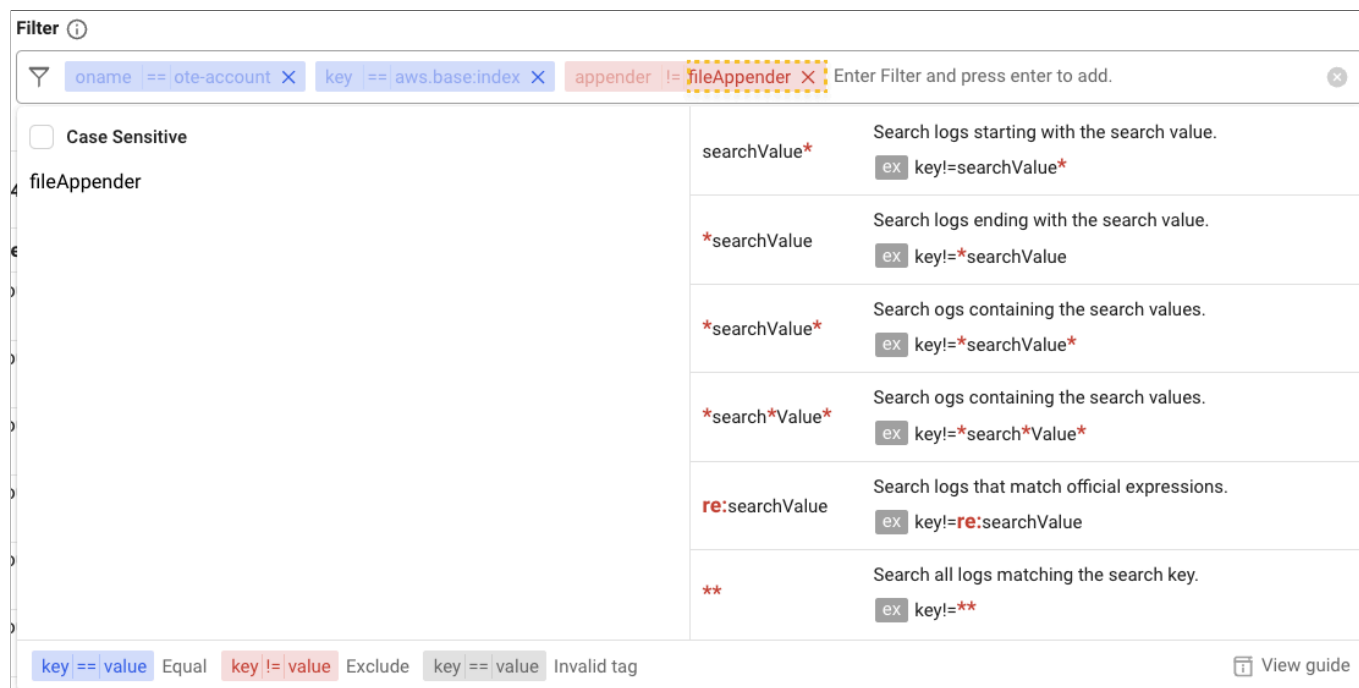
1. Select **Category**. It is required to set the category.
2. In the **Filter** field, enter a desired keyword for a search after leaving spaces on the **content** basis.
e.g. `content *select*`
3. Click **Search** to view the logs. Several logs are viewed first. You can view a maximum of 10,000 logs per each search.
4. You can make additional inquiries by scrolling down and selecting **View more** at the bottom.

The screenshot shows the Log Search interface. At the top, there's a filter bar with the same filters as above. Below it, a message states: "You have viewed 10,500 of the total 36,841 results, and the results retrieved are 9999+." The main area displays a list of logs with columns for Time, Category, and Content. A modal dialog is open, asking "Want to view more logs?" and providing instructions: "Adding a log parser enables search without additional lookups." It includes buttons for "Setting up a log parser" and "View more".

- Among all logs, 10,000 logs are viewed for a server search range. The default range for a server search is 200,000, but the ratio may differ depending on the total log volume.
- 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.



- 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

The search key Indicates an identifier for accessing a desired value within the log data. The actual data for the search key is the search value. The tags on the left ② area are the search keys parsed for each category. You can enter filters by selecting tags. The orange tag is the category, and the blue tag is the search key.

For example, **AppLog** and **AppStdOut** in ② are categories. The tags below such as **oid** are search keys parsed. In **Log > Log Configuration**, you can register and set the parsing logic in **Log parser setting** tab with the 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

×

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	-

Common syntaxes

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

Syntax type	Description	Example
	in the middle.	
*search*Value*	Searches for the logs that contain the search value.	word==*he*llo*
re:{regex}	Searches for the logs that match a regular expression.	caller==re:^(i\.w\.a\.w\.s\.v\.r\.
**	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
>searchValue	Searches for the logs containing values greater than the search value.	response_time.n>3000
>=searchValue	Searches for the logs containing values greater than or equal to the search value.	response_time.n>=3000
==searchValue	Searches for the logs containing the same search value.	response_time.n==3000
!=searchValue	Searches for the logs that contain values different from the search value.	response_time.n!=3000
<searchValue	Searches for the logs containing values less than the search value.	response_time.n<3000

Syntax type	Description	Example
<code><=searchValue</code>	Searches for the logs containing values less than or equal to the search value.	<code>response_time.n<=3000</code>

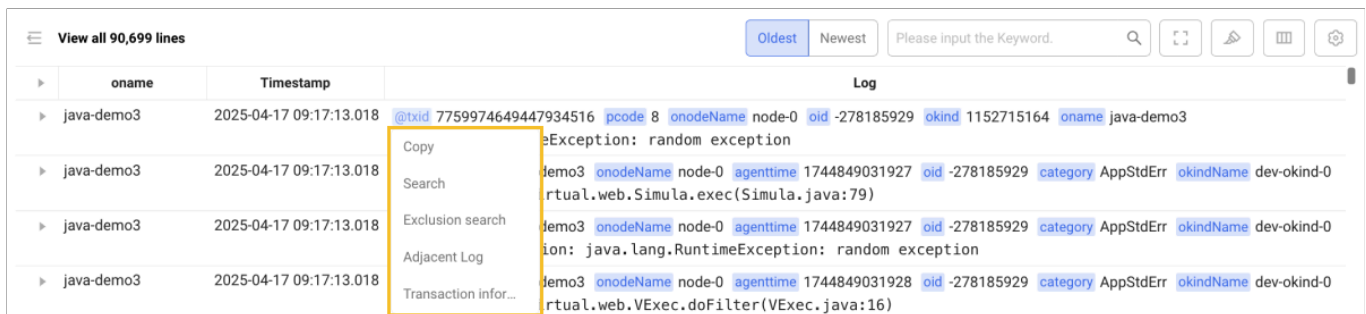
Viewing personal information

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](#).

Log tagging options

When you select a log tag, the following drop-down menu appears. You can find the **Search**, **Exclusion search**, **Adjacent Log** and **Transaction information** options.



- Copy
- Search

If you select the **Search** option, the tags that correspond to **Filter** are entered with the inclusion (`==`) condition.

- Exclusion search

If you select the **Exclusion search** option, the tags that correspond to **Filter** are entered with the exclusion (`!=`) condition.

- **Adjacent Log**

If you select the **Adjacent Log** option, the **Adjacent Log** detail window appears. Search for the logs of the target server and the logs in time zones adjacent to the selected log. You can click **Time selector** to see the logs in adjacent time zones. Reference logs appear with a blue background.

- **Transaction**

If the log contains the `@txid` and `@mtid` tags, you can see the information in the transaction Information details window by clicking the transaction information option.

Content highlighting

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
<code>a b c</code>	Separate each keyword with a space.	a, b, c

String to input	Description	Result
"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**.

Setting the table

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 Setting

Home > Select Project > **Log** > **Log Configuration**

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

Getting started with log monitoring | Log filter settings | Log primary parser setting | Log secondary parser setting | Fast index setting | Log long-term archive statistics | De-identification of personal information

Set up the agent and enable log monitoring ⓘ

View plans

You can easily check the log of the application with the Live Tail and Log Trend.

▼ 1. Check agent settings

To collect logs from Java applications, please check the following:

- Checking and Upgrading Agent Versions (available from v2.1.1 or later)
- Agent Settings > Direct Input > Enter the agent setting command below.
- Restart

Agent settings

logsink_enabled=true 

▶ 2. Activate log monitoring

Log monitoring data setting ⓘ

Initialized Save

Log lookup password ☐ Turn on to use the log lookup password.

Log retention period (initial value) ⓘ

15days ▼

 You can enter a value between 1 days and 40 days.

Log usage

Category	Data retention	Cumulative number of logs (based on the retention period) ⓘ	Average daily log count ⓘ	Yesterday's log count ⓘ	Expected log count per week ⓘ	Expected log count per month ⓘ
Total		3,523,236,480	234,882,433	124,084,216	1,644,177,010	7,046,472,900
AppLog	15days ▼	3,494,072,628	232,938,175	123,070,829	1,630,567,225	6,988,145,250
AppStdErr	15days ▼	338,233	22,548	12,222	157,836	676,440
AppStdOut	15days ▼	13,911,268	927,417	483,168	6,491,919	27,822,510
VirtualLog	15days ▼	14,914,351	994,290	517,997	6,960,030	29,828,700

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

In the **1** area, check the agent settings, and then click the **Activate log monitoring** toggle button to set whether or not to enable the log monitoring.

Check agent configuration

Check the agent version and settings to start the log monitoring. Select **Check Agent Configuration** to follow the onscreen instructions.

- **Server Monitoring**

Under **Apply**, check the application guides for each application. See the following guides: [Java](#), [PHP](#), [Node.js](#), [Python](#), [Go](#).

- **DB Monitoring**

Under **Apply**, check each individual application guide. See [the following](#). According to the instructions, add the settings for the log monitoring target file in [whatap.conf](#).

- **Kubernetes Monitoring**

Under **Apply**, check each individual application guide. See [the following](#).

Activate log monitoring

Select **Activate log monitoring** to set whether or not to enable the log monitoring.

- If you turn on the  toggle button, the log monitoring is enabled. You can try it for free for 15 days from the activation date.
- If you turn off the  toggle button, the log monitoring is disabled. Logs are no longer saved.

Log monitoring data setting

In the **2** 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 Filter Settings

Log Filter Settings allow you to store only the logs that match the filter conditions specified by the user. By storing only the necessary logs, you can reduce costs.

! Permission

Only users with log edit permissions can configure these settings.

Add a Log Filter Setting

This section explains how to add a new filter setting. When configuring log filter settings, **Filter Name**, **Show in Live Tail**, **Category**, and **Filter Condition** are required fields.

Even logs that are not stored by the filter can still be viewed in **Live Tail** if the **Show in Live Tail** toggle is enabled.

! Only one filter can be set per category.

1. Go to **Logs > Log Settings > Log Filter Settings** tab.
2. Click the + **Add** button to create a new filter setting.
3. In **Add Log Filter Setting**, enter **Filter Name**, **Show in Live Tail**, **Category**, and **Filter Condition**.
 - **Filter Name:** A name to identify the filter.
 - **Show in Live Tail:** Select whether to display in Live Tail regardless of storage.
 - **Category:** The log category to which the filter is applied (**multiple selection allowed**).
 - **Filter Condition:** Conditions for logs to be stored by the filter.

! For more details on filter conditions, see [WhaTap log search query syntax](#).

- **Example**

- **Include:** `oid : 123`
 - Collect only logs whose oid is 123.
 - **Exclude:** `not oid : 123`
 - Collect only logs whose oid is **not** 123.
 - **Include all:** leave the filter condition empty
 - **Exclude all:** `not content : *`
4. Click **Add** to review and edit the filter settings in the **Preview Results** screen.
 5. Once confirmed, click **Apply** to save the log filter settings.

Simulation

You can preview the log results based on the entered category and filter conditions before applying the log filter settings.

Click the **Simulation** button to display the **Log Search** screen with the applied filter settings.

Edit a Log Filter Setting

Registered log filters can be modified by clicking the edit icon. The **Edit Log Filter Setting** screen shows the existing values, which you can change and apply as needed.

 When editing log filter settings, only one category can be selected.

Delete a Log Filter Setting

Registered filters can be deleted by clicking the delete icon. After deletion, make sure to click the **Save** button.

 If changes are not saved, the filter will not be deleted.

Import/Export Log Filter Settings as JSON

Log filter settings can be imported or exported in JSON format.

This is useful if you want to apply the same log filter settings to another project.

Export JSON

1. Click the  button at the top right of the screen.
2. In the **Export JSON** window, click the **Export** button.
3. The log filter settings will be downloaded as a JSON file.

Import JSON

1. Click the  button at the top right of the screen.
2. Select the JSON file to import.
3. In the **Import JSON** window, click either **Add to List** or **Overwrite** to import the log filter settings.
4. Click the **Save** button to apply the changes.

Validation Rules

The following validation rules are applied when saving settings:

- **type:** Only `GENERAL` is supported.
- **category:** Required, supports `string` type.
- **condition**
 - **language:** Only `jsonDsl` and `lucene` are supported.
 - **description:** Invalid filter conditions cannot be saved.
- **showLiveTail:** Only `boolean` type is supported.
- **name:** Required, supports `string` type.

Parsing The Logs

The log parser helps you transform the irregular logs into a structured form. WhaTap Log Monitoring provides two types of parsers.

- **GROK parser:** The logs collected in arbitrary forms are parsed using regular expressions and GROK syntax.
- **JSON parser:** The logs collected in the JSON form are parsed.

! Common precautions

- If multiple parsers are registered in the same category, only the first matching parser is applied.
- WhaTap has the role to disable the parsers that may affect the stability of the WhaTap service.

GROK parser

If the logs are collected in an irregular form, you can use the GROK parser to parse them. GROK syntax provides named regular expressions, allowing you to use regular expressions more easily.

Starting GROK

GROK provides two types of syntaxes.

1. `%{SYNTAX:SEMANTIC}` : Syntax provided in the GROK library. Using the **named regular expressions**, you can extract tags. For usage examples, see [the following](#).
 - **SYNTAX:** Specify the named regular expressions provided by GROK.
 - **SEMANTIC:** Specify the name for the matched value.

! named regular expressions

The syntax is provided by GROK. This function provided by GROK allows you to assign names to complex regular expressions.



name	regular expression
WORD	<code>\b\w+\b</code>
SPACE	<code>\s*</code>
NOTSPACE	<code>\S+</code>
UUID	<code>[A-Fa-f0-9]{8}-(?:[A-Fa-f0-9]{4}-){3}[A-Fa-f0-9]{12}</code>

To see all named regular expressions provided by WhaTap, see the following [link](#).

2. `(?<SEMANTIC>REGX)` : The **named capturing group** syntax for regular expressions. You can use regular expressions to extract tags according to the user's intent. For usage examples, see [the following](#).

- **SEMANTIC**: Specify the name for matched values.
- **REGX**: Enter regular expressions for matching.



named capturing group

It is the syntax provided by regular expressions.

- capturing group: This indicates the function to bundle multiple tokens into one as a single matching unit.
- named capturing group: Name assigned to the capturing group.
- Let's look at the string matching example. [dev@whatap.io](#)
 - Example 1 `(\w+)@(\w+\.\w+)`
 - Example 2: When the entire email is matched and the username and domain are matched additionally, `(?<username>\w+)@(?<domain>\w+\.\w+)`

%{SYNTAX:SEMANTIC} Usage example

The following is an example that uses the `%{SYNTAX:SEMANTIC}` syntax.

Sample log

```
[2023-08-08 02:02:30,101 GMT][INFO ][i.w.y.l.c.LogSinkDexScheduleThread.realProcess(159)] 8 VirtualLog 20230808
02:01:00.000 {area=4, city=5} 56ms
```

You can look at the sample log to infer what each word means. When replacing each part with semantic words, it can be expressed as follows:

semantic replace

```
[date][logLevel][caller] projectCode logCategory dexBuildStartTime {area=areaEnum, city=cityEnum} dexBuildElapsed
```

Any semantic word can be replaced with a regular expression. The GROK parser allows you to use the predefined named regular expressions. `TIMESTAMP_ISO8601`, `LOGLEVEL`, and `DATA` used here are named regular expressions provided by GROK. These values are matched after replacing each of them with the following regular expression.

- name: `TIMESTAMP_ISO8601`
 - regular expression: `%{YEAR}-%{MONTHNUM}-%{MONTHDAY}[T]
%{HOUR}:%{MINUTE}(?:%{SECOND})?%{ISO8601_TIMEZONE}?`
- name: `LOGLEVEL`
 - regular expression: `LOGLEVEL
([Aa]lert | ALERT | [Tt]race | TRACE | [Dd]ebug | DEBUG | [Nn]otice | NOTICE | [Ii]nfo | INFO | [Ww]arn(?:ing)? | WARN(?:ING)?`
- name: `DATA`
 - regular expression: `.*`

GROK parsing pattern

```
\[%{TIMESTAMP_ISO8601:date}\sGMT\]\[%{LOGLEVEL:level}\s\]\[%{DATA:caller}\]
```

If you parse with the above syntax, you can extract tags as follows. In this way, GROK's `%{SYNTAX:SEMANTIC}` syntax helps you apply complex and long regular expressions easily and concisely.

Tag extraction

```
- date : 2023-08-08 02:02:30,101
- caller : i.w.y.l.c.LogSinkDexScheduleThread.realProcess(159)
- level : LEVEL
```

(?<SEMANTIC>REGX) Usage example

The parts that do not match with the named regular expressions can be parsed using the `(?<SEMANTIC>REGX)` pattern. In the [sample log](#) above, the parts that cannot be parsed with the `%{SYNTAX:SEMANTIC}` syntax are as follows.

Unparsed area

```
8 VirtualLog 20230808 02:01:00.000 {area=4, city=5} 56ms
```

When replacing each part of the log with semantic words, it can be expressed as follows.

semantic replace

```
projectCode logCategory dexBuildStartTime {area=areaEnum, city=cityEnum} dexBuildElapsed
```

These irregularly strings can be parsed using the `(?<SEMANTIC>REGX)` syntax.

Regular expressions that match for each sample log parsing keyword

Parsing keyword	(?<SEMANTIC>REGX)
8	(?<projectCode>\d)
VirtualLog	(?<logCategory>\w*)
20230808 02:01:00.000	(?<dexBuildStartTime>\d{8}\s\d{2}:\d{2}:\d{2}\.\d{3})
area=4	area=(?<areaEnum>\d)
city=5	city=(?<cityEnum>\d)

Parsing keyword	(?<SEMANTIC>REGX)
56ms	(?<dexBuildElapsed>\d{2})ms

Basic regular expression syntax

Syntax rule	Meaning	Alias
<code>?</code>	0 or 1	-
<code>+</code>	1 or more	-
<code>*</code>	0 or more	-
<code>a{5}</code>	exactly 5	-
<code>\w</code>	word character	<code>[a-zA-Z_0-9]</code>
<code>\s</code>	white space	-
<code>.</code>	any character except newline	-
<code>[abc]</code>	any of	-
<code>[^abc]</code>	not a,b, or c	-
<code>[a-z]</code>	character between a and z	-
<code>[1-3[7-9]]</code>	union (combining two or more character classes)	-
<code>[1-6&&[3-9]]</code>	intersection	-
<code>[0-9&&[^2468]]</code>	subtraction	-
<code>a{2,}</code>	2 or more	-
<code>a{1,3}</code>	between 1 and 3	-

Syntax rule	Meaning	Alias
<code>a+?</code>	match as few as possible	-
<code>{2,3}?</code>	match as few as possible	-
<code>(abc)</code>	capturing group (processes multiple strings as a single unit)	-
<code>\d</code>	digit	<code>[0-9]</code>
<code>\D</code>	non-digit	<code>[^0-9]</code>
<code>\W</code>	non-word character	-
<code>\S</code>	non-white space	-

By connecting the parsed keywords with space (`\s`) and special character escapes (`\{` , `\,` , `\}`), you can apply the pattern as follows.

GROK parsing pattern

```
(?<projectCode>\d)\s(?<logCategory>\w*)\s(?<dexBuildStartTime>\d{8})\s\d{2}:\d{2}:\d{2}\.\d{3})\s\{area=(?<areaEnum>\d),\scity=(?<cityEnum>\d)\}\s(?<dexBuildElapsed>\d{2})ms
```

If you parse with the above syntax, you can extract tags as follows.

Tag extraction

```
- projectCode : 8
- logCategory : VirtualLog
- dexBuildStartTime : 20230808 02:01:00.000
- areaEnum : 4
- cityEnum : 5
- dexBuildElapsed : 56
```

Applying GROK

Log Configuration > Log primary parser setting

1. To apply the GROK pattern parser, go to the **Log primary parser setting** tab in **Log Configuration**.
2. Select **+ Add** and then select the **GROK** parser in the **Parser** field.
3. When you select **Register pattern**, the pattern registration and simulation window appears on the right.
4. Enter **Pattern** and **Log**, and then click **Simulation** to check whether parsing is successful with the pattern to apply.

Pattern e.g.

```
[%{TIMESTAMP_ISO8601:date}\sGMT][%{LOGLEVEL:level}\s][%{DATA:caller}]\s(?:<projectCode>\d)\s(?:<logCategory>\d{2}:\d{2}:\d{2}\.\d{3})\s\{area=(?:<areaEnum>\d),\scity=(?:<cityEnum>\d)\}\s(?:<dexBuildElapsed>\d{2})ms
```

Log example:

```
[2023-08-08 02:02:30,101 GMT][INFO ][i.w.y.l.c.LogSinkDexScheduleThread.realProcess(159)] 8  
VirtualLog 20230808 02:01:00.000 {area=4, city=5} 56ms
```

5. If the simulation is successful, you can view **Simulation result** and **Performance measurement results**.
6. When you click **Apply pattern** after simulation, the pattern that has been entered for the selected parser is applied.
7. After applying the pattern, enter values for **Category**, **Log detection condition**, and **Pattern**.

Parser Add

Parser*

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

GROK

parser pattern*

The pattern is registered after the simulation is performed to ensure that the log is successfully parsed with the entered pattern.

Success

```

\[%{TIMESTAMP_ISO8601:date}\sGMT\}\[%{LOGLEVEL:level}\s\}\[%{DATA:caller}\}\s(?:<projectCode>\d)\s(?:
<logCategory>\w*)\s(?:<dexBuildStartTime>\d{8}\s\d{2}:\d{2}:\d{2}\.\d{3})\s\{area=(?:<areaEnum>\d),\scity=(?:
<cityEnum>\d)\}\s(?:<dexBuildElapsed>\d{2})ms

```

Modify parser pattern

Category*

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

AppLog

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.

oname

demo-8100

Add

- **Category**

Select a log category. **Category** is required.

- **Log detection condition**

- Only the logs that meet the conditions are applied to the parser.
- Select or enter values for **Search key** and **Search value**.
- **Log detection condition** are applied before all parsers are run. Accordingly, you cannot use the **Tag** that have been added for the parser.

8. Select **Add** to register a parser.

- In the log parser list, you can change the **Priority** or **Enable**, **Edit**, or **Delete** the parser.
- After **parser simulation**, you can register a pattern.

! GROK parser precautions

- GROK parser supports two patterns: `%{SYNTAX:SEMANTIC}` and `%{SYNTAX:SEMANTIC}` .
- When using the `%{SYNTAX:SEMANTIC}` pattern, `SEMANTIC` must be entered.
- When using the `%{SYNTAX:SEMANTIC}` pattern, `SEMANTIC` must be unique in a parser.
- When using the `(?<SEMANTIC>REGX)` pattern, `SEMANTIC` can only contain characters (a-z, A-Z), numbers (0-9), and specified special characters (`.` , `_` , `-`).
- `SEMANTIC` must start with a character (a-z, A-Z).
- `SEMANTIC` must end with a character (a-z, A-Z) or number (0-9).

Selecting additional GROK patterns

During GROK parser simulation, in addition to the basic patterns (`WORD` , `NUMBER` , `IP` , etc.), you can select **additional patterns** that match a specific log format. 32 pattern types, such as Java, Nginx, and MySQL, are provided grouped into 11 categories.

Additional pattern category dropdown

1. In the parser simulation window, click the dropdown in the **Additional patterns (optional)** area.
2. From the list of pattern types grouped by category, select the pattern type you need. You can also search by entering a pattern type name or description in the search box.
3. The selected pattern type is loaded together with the basic patterns during simulation.

! The basic patterns (Core) are always included automatically. Selecting additional patterns is optional.

Pattern type list by category

Category	Pattern type
Web Servers	haproxy, httpd, iis, nginx, squid
Application Servers & Frameworks	java, log4j, rails, ruby, springboot

Category	Pattern type
Databases	mongodb, mysql, oracle, postgresql, redis
Cloud	aws
System & Infrastructure	docker, kubernetes, linux-syslog
Messaging & Search	elasticsearch, kafka
Network & Security	bind, bro, firewalls, junos, zeek
Mail	exim, postfix
Monitoring & Backup	bacula, mcollective, nagios
Build Tools	maven

Usage example

To parse a Tomcat Catalina 8 log, select the **java** pattern type additionally and then use the `%{CATALINA8_LOG}` pattern.

Sample log

```
31-Jul-2020 16:40:38 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Server version name: Apache Tomcat/8.5.57
```

GROK parsing pattern

```
%{CATALINA8_LOG}
```

Tag extraction

```
- log_timestamp : 31-Jul-2020 16:40:38
- log.level : INFO
- java.log.origin.thread.name : main
- java.log.origin.class.name : org.apache.catalina.startup.VersionLoggerListener
```

```
- log.origin.function : log
- log_message : Server version name: Apache Tomcat/8.5.57
```

Viewing pattern details

You can check which patterns are included in the selected additional pattern type in the details window. You can look up the pattern definitions (regular expressions) and sample logs and apply them directly to the simulation.

Viewing pattern details

After selecting an additional pattern type, click the selected pattern type tag to open the details window on the right. The details window is displayed side by side without hiding the simulation form, so you can proceed with the simulation while checking the pattern definitions.

You can use the following functions in each pattern item.

Button	Function	Description
Sample	Enter a sample log	Automatically enters an example log that matches the pattern into the Simulation parsing log input box.
Select	Insert a pattern	Inserts it into the Pattern input box in the <code>%{pattern_name}</code> format. The corresponding pattern type is also selected automatically.
Copy	Copy to clipboard	Copies the <code>%{pattern_name}</code> format to the clipboard.

- When you click a pattern item, its pattern definition (regular expression) expands. You can expand multiple patterns at the same time to compare their definitions.
- In the `%{PATTERN:field}` references included in a pattern definition, the pattern name, field name, and literal characters are displayed distinguished by different colors.
- You can run the **simulation** directly with the log entered by the **Sample** button to check the parsing result.

Saving simulation sample logs

The log used in the simulation is saved automatically together with the parser settings. When you edit a parser, the sample log used previously is restored automatically to the simulation window, so you do not need to enter the log again each time.

JSON parser

If logs are collected in JSON format, they can be easily parsed using the JSON parser.

Applying the JSON

Log Configuration > Log primary parser setting

1. To apply the JSON pattern parser, go to the **Log primary parser setting** tab in **Log Configuration**.
2. Select **+** **Add** and then select the **JSON** parser in the **Parser** field.
3. When you select **Register pattern**, the pattern registration and simulation window appears on the right.
4. Enter **Pattern** and **Log**, and then click **Simulation** to check whether parsing is successful with the pattern to apply.

Example

```
2023-08-08 02:43:28,615 -- {"host":"10.21.3.24","method":"POST","status":"200","url":"http://dev.whatap.io/yard/
api/flush"} --
```

In the example log, if **Prefix** and **Postfix** are specified as `--` and `url` is specified in **Ignore**, only three **Tag** (`host` , `method` , `status`) are created.

- **Prefix** Specify the position where the JSON format begins in the log. If the entire log is in JSON format, set an empty value.
- **Postfix** Specify the position where the JSON format ends in the log. If the entire log is in JSON format, set an empty value.
- **Ignore** Specify the key for which tags are not created during JSON formatting.

5. If the simulation is successful, you can view **Simulation result** and **Performance measurement results**.

Parser Simulation

View Guide

Pattern

agenttime, category, content, logContent, message, pcode, time, timestamp is a reserved word.

Reserved words do not work even if registered as log detection conditions or patterns.

Prefix -

Postfix -

Ignore url

Log *

Log simulation is essential and additional pattern registration may be required depending on simulation results.

```
2023-08-08 02:43:28.615 --
{"host":"10.21.3.24","method":"POST","status":"200","url":"http://devote.whatap.io/yard/api/flush"} -

```

Simulation

Simulation result Success

Key	Value	Result
method	POST	Ok
host	10.21.3.24	Ok
status	200	Ok

Performance measurement results Success

Simulation count	Time min(ns)	Time max(ns)	Time a
1	7,047	7,047	7,047
10	2,663	4,255	2,872
100	2,655	4,574	2,818
1,000	2,651	94,191	2,961
10,000	2,651	146,472	2,987
100,000	2,648	194,424	2,917
1,000,000	2,647	80,465,427	3,136

Apply pattern

6. When you click **Apply pattern** after simulation, the pattern that has been entered for the selected parser is applied.
7. After applying the pattern, enter values for **Category**, **Log detection condition**, and **Pattern**.

× Parser Add

Parser*

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

JSON

parser pattern*

Simulate that the log is parsed successfully. Simulation must be performed, and additional pattern registration may be required depending on the simulation results.

✓ Success

Prefix --

Postfix --

Ignore url

Simulation verification and pattern modification

Category*

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

AppLog

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.

oname

demo-8100

Add

- **Category**

Select a log category. **Category** is required.

- **Log detection condition**

- Only the logs that meet the conditions are applied to the parser.
- Select or enter values for **Search key** and **Search value**.
- **Log detection condition** are applied before all parsers are run. Accordingly, you cannot use the **Tag** that have been added for the parser.

8. Select **Add** to register a parser.

- In the log parser list, you can change the **Priority** or **Enable**, **Edit**, or **Delete** the parser.
- Before registering a parser, you can check whether the pattern to register is normal through



Simulation. It is the same as the GROK parser registration simulation process. See [the following](#).

Example of using JSON format

Sample log

```
{"host":"10.21.3.24","method":"POST","status":"200","url":"http://dev.whatap.io/yard/api/flush"}
```

If the above sample log has been collected, select the **JSON** parser in the **Parser Add** window. Without having to write a complex parsing logic, you can extract the **Tag** for log analysis as follows:

Tag extraction

```
- host : 10.21.3.24
- method : POST
- status : 200
- url : http://dev.whatap.io/yard/api/flush
```

Usage example when configuring part of the JSON format

Some JSON format sample log

```
2023-08-08 02:43:28,615 -- {"host":"10.21.3.24","method":"POST","status":"200","url":"http://dev.whatap.io/yard/api/flush"} --
```

If part of the log is in JSON format as in the example, specify **Prefix** and **Postfix**. WhaTap log monitoring recognizes and parses the area between **Prefix** and **Postfix** in JSON format.

Tag extraction

```
- host : 10.21.3.24
- method : POST
- status : 200
- url : http://dev.whatap.io/yard/api/flush
```

Log Fast Index Setting

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 true)

Log Long-term Archive Statistics Setting

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*

Please input the Statistic key.

Data retention period(disk usage)

15 Days (About 3 MB) ▾

Category*

Please select the Category.

Log detection condition*

Please select a category first. ▾

Please select a category first.

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

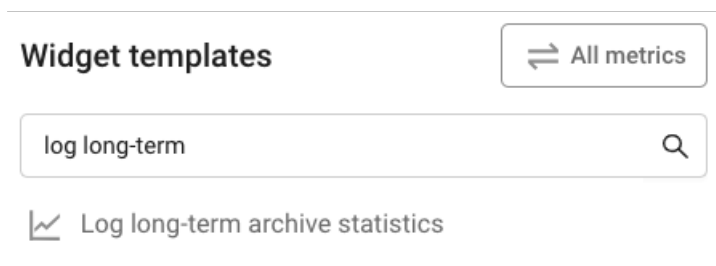
Example

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`.

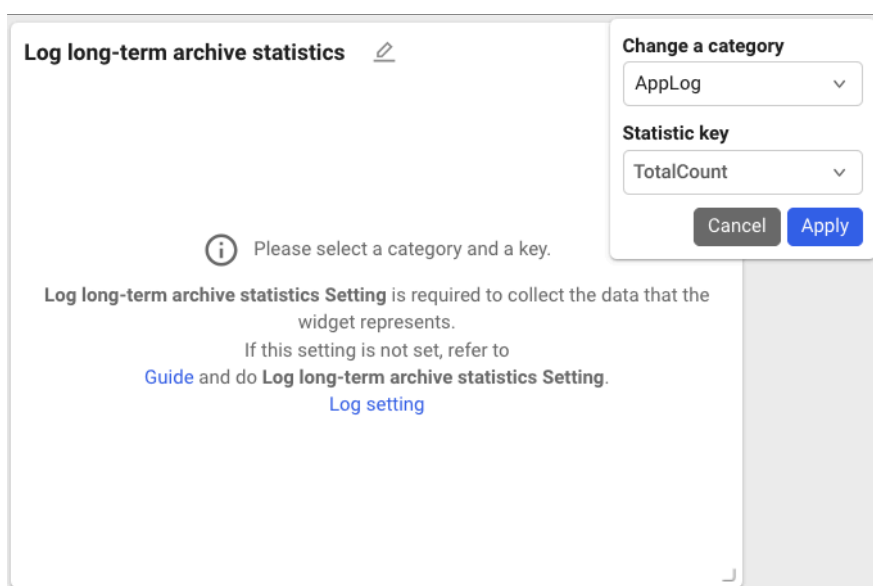
Log long-term archive statistics You can generate statistical data about how many logs have been collected that meet certain conditions.						+ Add	Save
Category	Statistic key	Log detection condition	Data retention period(disk usage)	Enable			
AppLog	TotalCount	status 200,300	15 Days (About 3 MB)	☐	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

Data Search

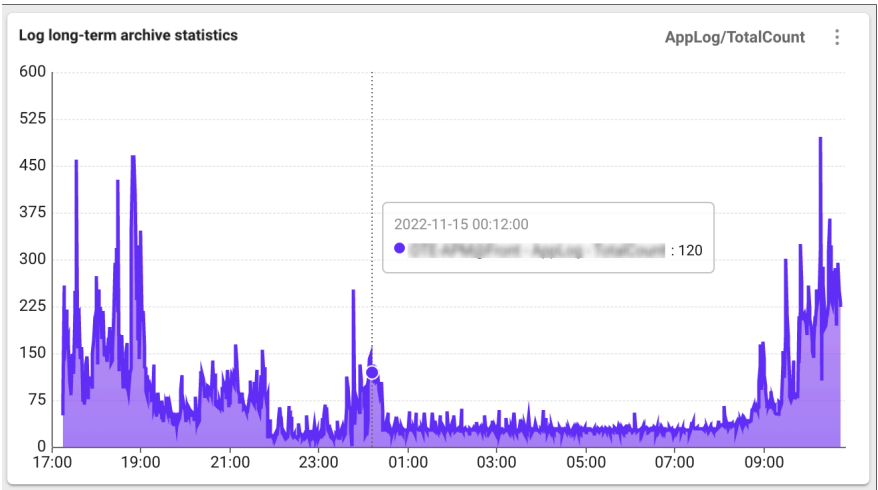
1. Create a widget by searching **Log long-term archive statistics** in **Widget templates** of **Integrated Flex Board**.



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



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



Log Personal Information De-identification

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.

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.				+ Add	Save
Enable	Category	Search key	Edit		
☐	VirtualLog	age.n	Edit	Delete	
☒	VirtualLog	status	Edit	Delete	
☒	ApplLog	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.
Check inspection history

Time

< 2025/03/21 12:26 ~ 2025/03/21 13:26 1 hr

Category

VirtualLog

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)

Whether to apply substitution

☐

Value to substitute

Start inspection

Stop inspection

Category

Search start time

Search end time

Personal information entity

Personal information pattern

Value to substitute

Pattern matching result

Inspection start time

Inspection end time

Whether to apply substitution

Inspection result

VirtualLog

2025/03/21 12:26

2025/03/21 13:26

Resident registration number

(?<!\w)\d{2}(0[1-9]|1[0-2])([0-2][0-9]|3[0-1])-[1-4]\d{6}(?!w)

0

Check results

2025/03/21 13:28

2025/03/21 13:28

No

SUCCESS

- Specify the start time and end time.
- Set values for **Category**.
- Select **Personal information entity** from the examples or **Direct Input**.

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

- Select whether to replace personal information, if it is identified via the **Whether to apply substitution** toggle.
- 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**.

- 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...

>

Q

Download 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])-[1-4]d{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)	*****_ *****

Personal information pattern	Personal information example	Regular expression pattern	Replacement value
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 registration number	111-11-01111	(?<!w)d{3}-d{2}-d{5}(?!w)	***_*_*_*****
Corporate registration number	111111-1111111	(?<!w)d{6}-?d{7}(?!w)	*****_ *****

Importing And Exporting Log Settings

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**.

Alert Notifications

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

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

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

Key Features

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

Permissions

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

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

Reference

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

Event Configuration

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

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

Metrics

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

Real-time logs

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

Composite log

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

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

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

Metrics

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

Real-time logs

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

Composite log

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

Reference

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

Common Features

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

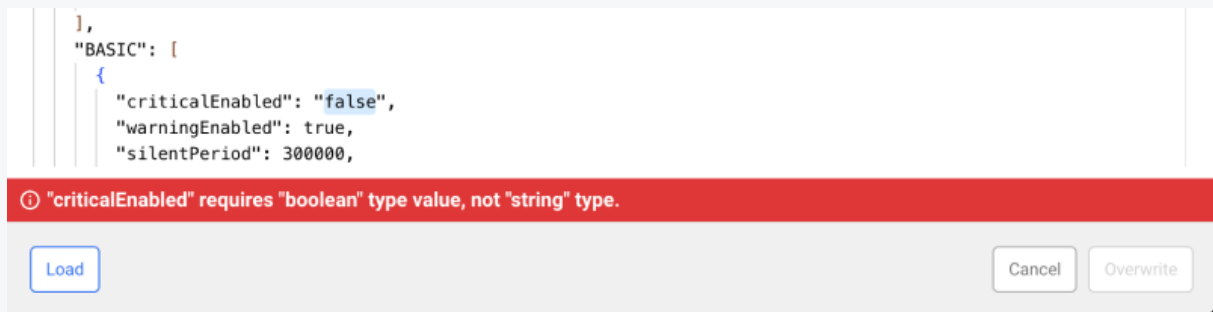
- **Batch JSON Edit:** Edit all event conditions in bulk using JSON format.
- **Batch JSON Download:** Save all currently registered event conditions as a JSON file.
- **Batch Excel Download:** Download the event list as an Excel file for external reporting or backup purposes.

Batch JSON Edit

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

⚠ After overwriting, you cannot restore the previous event configuration.

- Arbitrarily modifying the values of the `productType` or `platform` properties may cause events to malfunction in other projects.
- The JSON editor includes built-in validation. If the format or values are invalid, an error message appears below the editor and the [Overwrite] button is disabled.



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

JSON Field	Description
◇ ANOMALY	Anomaly detection

Batch JSON Download

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

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

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

Batch Excel Download

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

Metrics

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

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

Default Options

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

Table | Metrics Event List Structure

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

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

Event Configuration

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

Add Event

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

How to Add a Metrics Event

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

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

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

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

Select Template

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

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

Define Event Conditions

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

Metric Settings

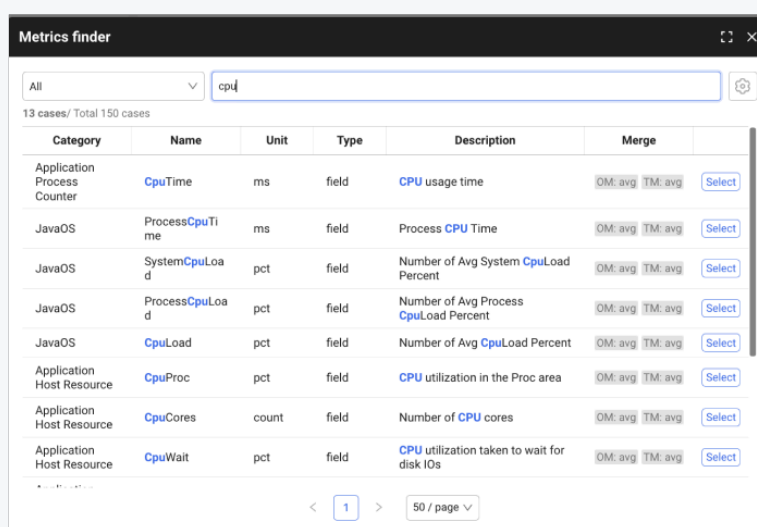
- Enter a category in the search field, or select a category (metric) from the category list. You must select a category to proceed with metric configuration.

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

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

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

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



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

❗ **Event Level Behavior**

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

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



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

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

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

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

b. Click — to remove the condition.



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

Trigger Count

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

1. Select the trigger frequency.

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

2. Enter the trigger count.

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

Pause

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

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

ⓘ When recovery notifications are enabled

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

Resolved Notification

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

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

Event Operation Time

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

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

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

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

Simulation

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

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

Start Simulation

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

Understanding Simulation Results

1. Time-Series Data

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

2. Event Counts by Level

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

3. Target-Level Details

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

4. Peak Interval Identification

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

✓ Simulation Tips

- **Simulate Different Time Ranges**

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

- **Include Actual Incident Periods**

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

- **Add Target Filtering**

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

- **Adjust Thresholds Gradually**

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

Select Event Target

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

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

Target Selection

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

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

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

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

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

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

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

Basic Information and Notification Settings

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

Event Activation

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

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

Event Name

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

Message

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

- **Variable Usage Rules**

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

- **Variable Usage Example**

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

Event Recipients

Specify the members who will receive event notifications.

- **Receive All Receive by Tag Selection**

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

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

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

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

ⓘ Reception Tags

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

Edit/Delete Event

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

Event Sharing

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

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

Export

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

Import

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

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

Edit in JSON Format

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

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

JSON error

JSON Data Structure

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

```

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

```

Table | JSON Data Structure

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

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

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

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

Appendix

Trigger Conditions and Target Selection Guide

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

Level Behavior Guide

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

1. Priority-based Event Triggering

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

Example

Configuration:

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

Current state: CPU 95%

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

2. Level Escalation

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

Example

Configuration:

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

Scenario:

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

3. Level De-escalation

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

Example

Configuration:

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

Scenario:

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

4. Execution Flow

- Warning: CPU > 70%

- Critical: CPU > 90%

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

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

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

Condition Configuration Guide

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

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

Examples using `${}` :

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

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



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

1. Comparison Operators

Numeric Comparison

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

String Comparison

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

2. Arithmetic Operators

- Basic arithmetic operations

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

- Controlling precedence with parentheses

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

- Negative values

```
cpu > -100
```

3. Logical Operators

- AND operator (&&)

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

- OR operator (| |)

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

- Combined logical operations

```
(cpu > 50 && memory > 50) | | disk < 20  
cpu > 80 && (memory > 1000 | | disk > 500)
```

4. Pattern Matching Operators

- LIKE operator

```
oname like 'prod-*'  
url like '*error*'  
message like 'WARN%'
```

- NOT LIKE operator

```
oname not like 'test-*'  
url not like '*debug*'
```

5. Built-in Functions

- Null check functions

```

isNull(value)      # Checks whether the value is null
isNotNull(value)   # Checks whether the value is not null
nvl(value, 0)      # Returns a default value if null
isEmpty(str)       # Checks whether the string is empty
isNotEmpty(str)    # Checks whether the string is not empty

```

- Aggregate functions

```

sum(cpu, memory, disk)    # Sum
avg(cpu, memory)          # Average
max(cpu, memory, disk)    # Maximum
min(cpu, memory, disk)    # Minimum
count(value1, value2, value3) # Count

```

- Math functions

```

round(cpu, 2)    # Rounds to 2 decimal places

```

- String functions

```

length(str)      # String length
startsWith(str, 'prefix') # Checks prefix
endsWith(str, 'suffix') # Checks suffix
indexOf(str, 'search') # String index
substring(str, 0, 10) # Substring
trim(str)        # Trims whitespace
replace(str, 'old', 'new') # String replacement
hasStr(str, 'search') # Checks string containment

```

- Conditional functions

- **if:** A conditional function that returns the `trueValue` if the condition evaluates to `true`, or the `falseValue` if it evaluates to `false`

Syntax

```

if(condition, trueValue, falseValue)

```

Example

```
if(value >= 90, 'High', 'Medium') == 'High'
```

- **decode:** Compares a value against conditions and returns the result of the matching condition, or a default value if no match is found

Syntax

```
decode(value, condition1, result1, condition2, result2, ..., conditionN, resultN, defaultValue)
```

Example

```
decode(value, 1, 'Low', 2, 'Medium', 3, 'High', 'Unknown') == 'Unknown'
```

- **in:** Returns `true` if the value matches any of the specified candidates; otherwise returns `false`

Syntax

```
in(value, candidate1, candidate2, ..., candidateN)
```

Example

```
in(status, 200, 201, 204) == false
```

! Writing Guidelines

- Recommended
 - Use simple variable names without `${}` (e.g. `cpu`, `memory`)
 - Always use `${}` when special characters are included
 - Use parentheses to clearly separate complex expressions
 - Enter function names exactly as defined (case-sensitive)
- Avoid



- Incomplete expressions (e.g. `cpu > , memory && )`
- Mismatched parentheses (e.g. `(cpu > 80 && cpu > 70) )`
- Consecutive or invalid operators (e.g. `cpu >> 80 , cpu >< 80 )`

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

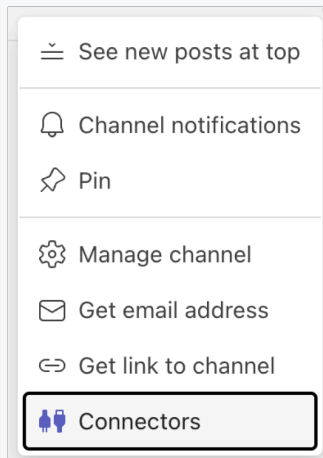


- `/remove` : Enter the project code for which you want to stop receiving alerts
- `/list` : View the list of project codes currently receiving alerts

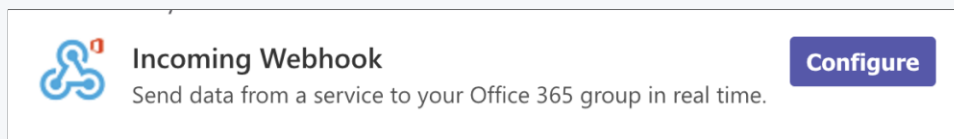
Teams



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

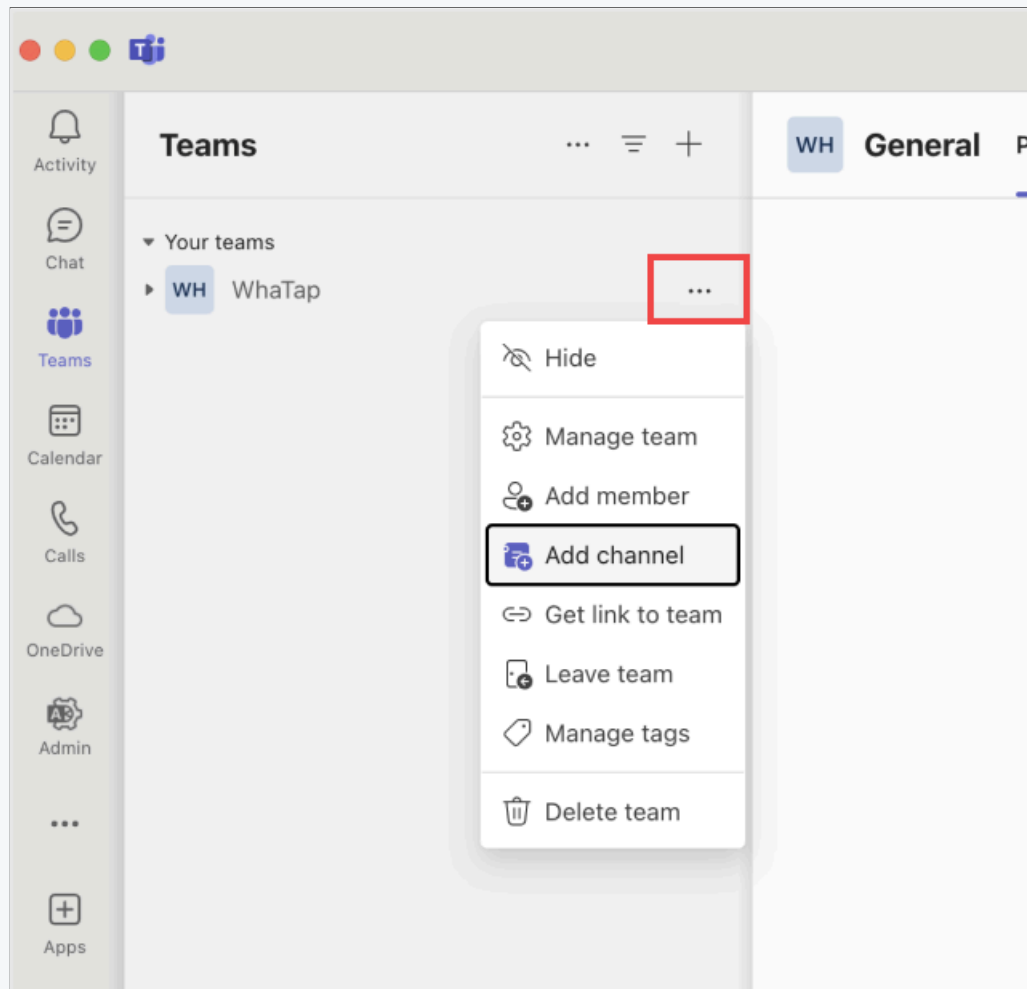
5. Return to the **Add a third-party plug-in** window in the WhaTap Monitoring service, and enter values for **Channel Name** and **Webhook URL** at the bottom of the **Teams** tab.
6. Click the [**Registration**] button.

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**.

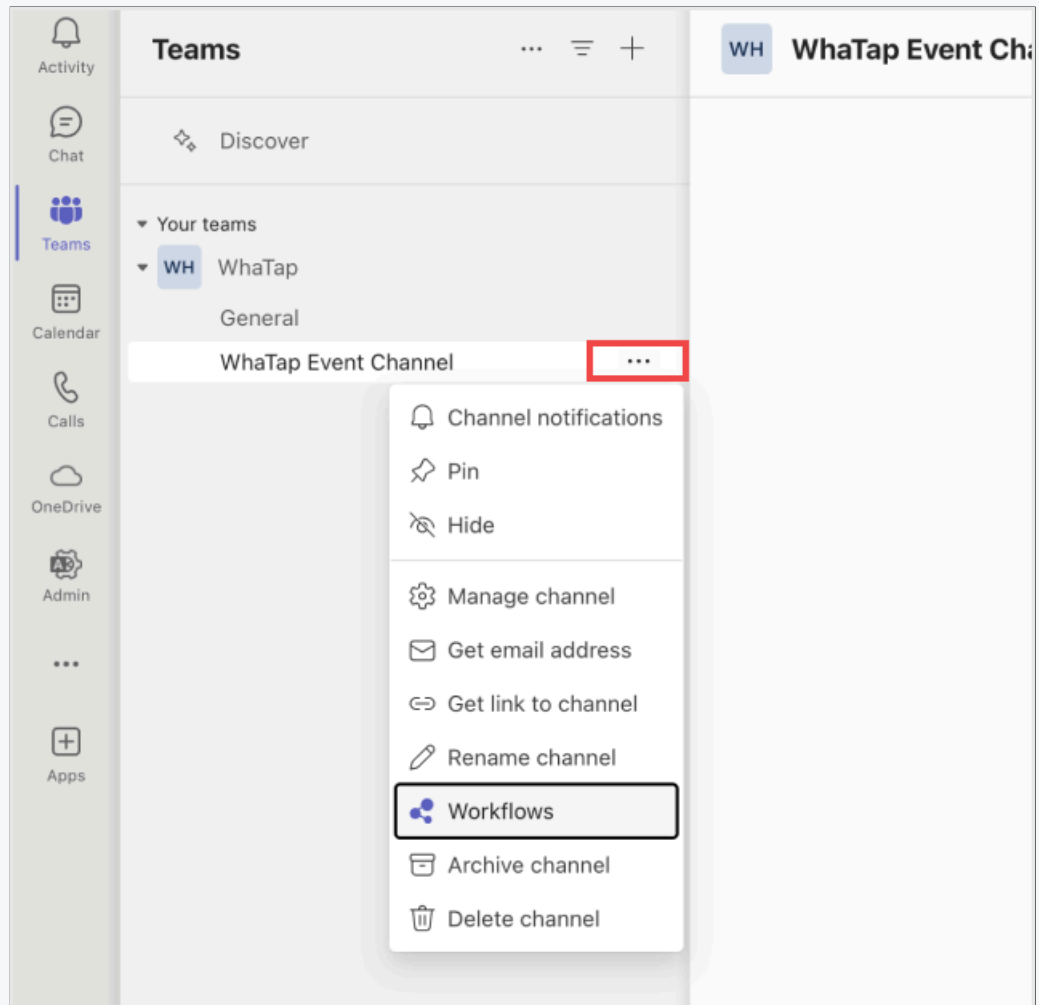


2. In the **Create a channel** window, enter the **Channel name** and **Description**. For **Channel type**, select **Standard**, then click the [Create] button.

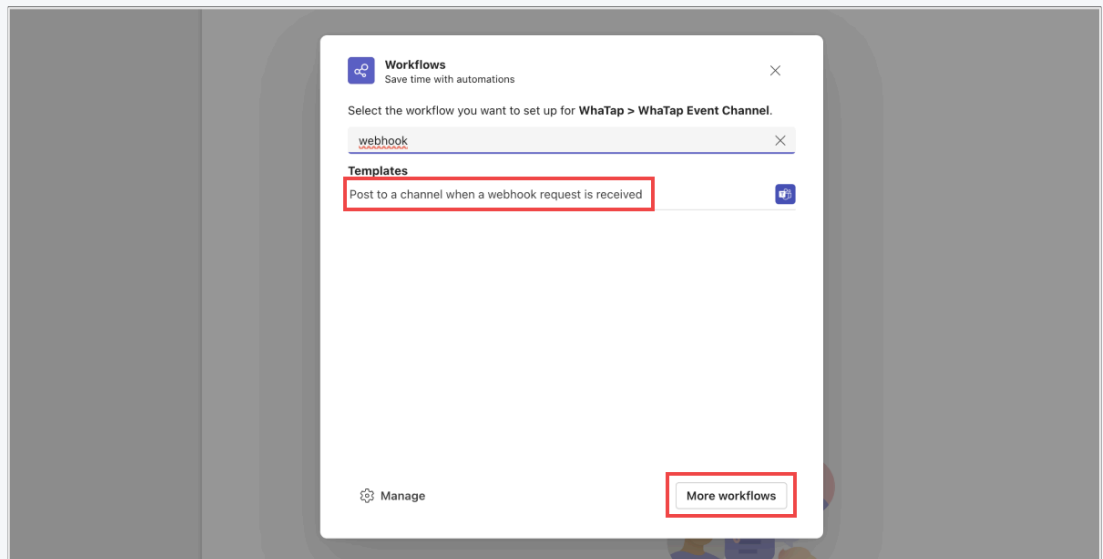


⚠ If you select **Shared** as the channel type, workflows cannot be used. If you select **Private**, workflows can be added but notifications cannot be received.

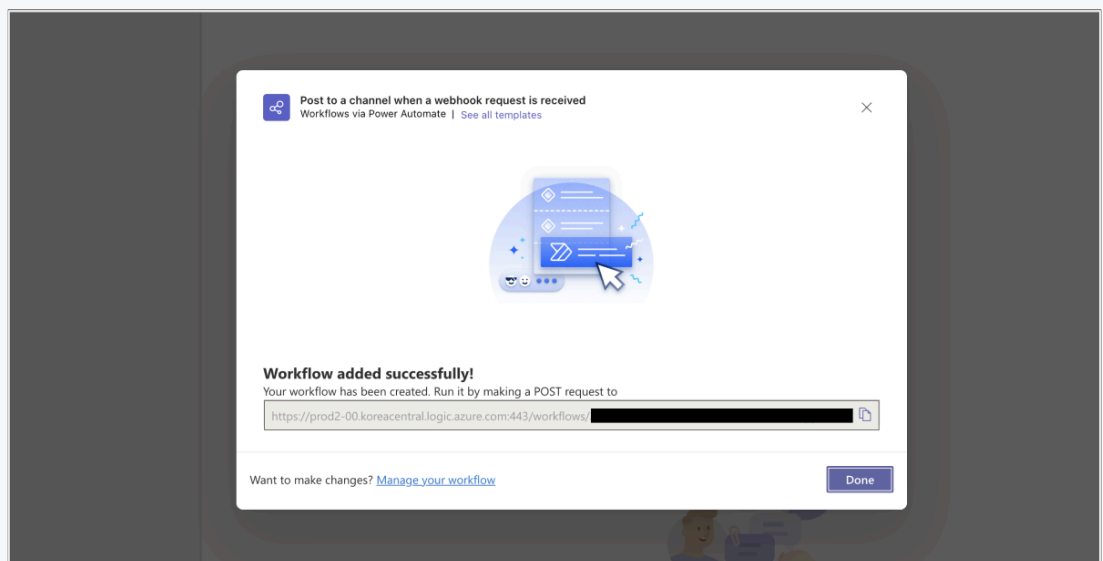
3. Click **More actions (...)** of the created channel, then select **Workflows**.



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.



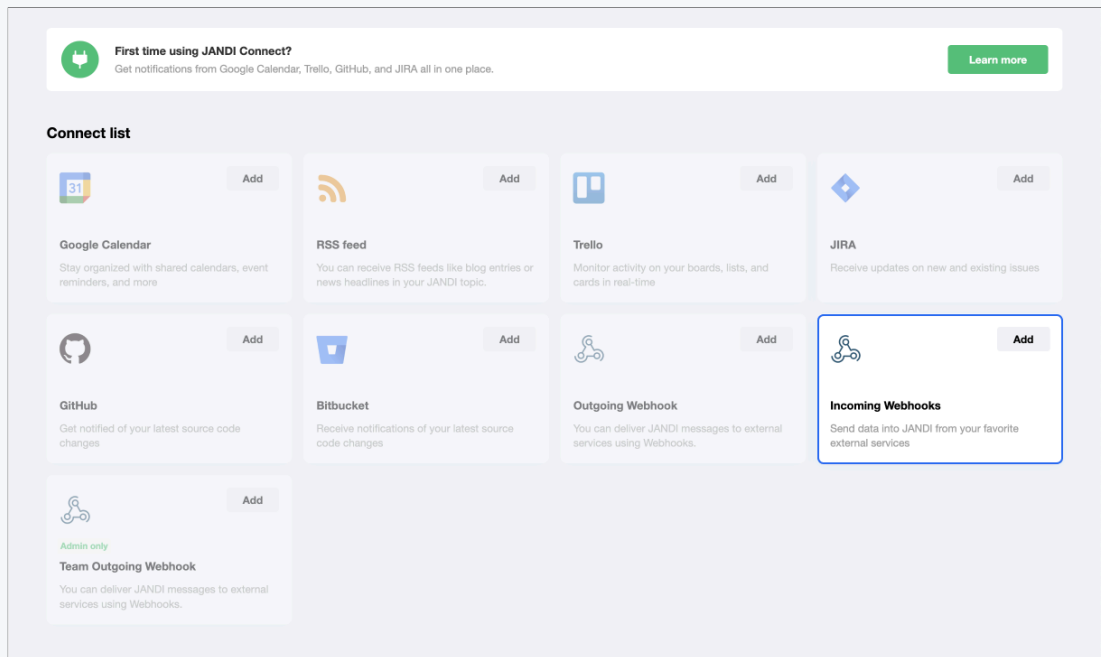
9. Click the [**Registration**] button.



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...>

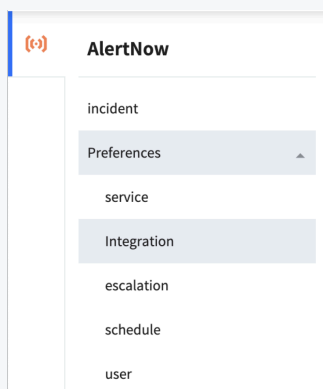
Copy

- 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**.

5. Click the [Confirm] button to create the integration.
6. Check the list of created integrations and select the newly created integration.

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.

Basic Information	
Integration type	WhaTap
Integration key	fda527a5140
URL	https://alertnowitgr.opsnow.com/integration/whatap/v1/
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}",
}
```



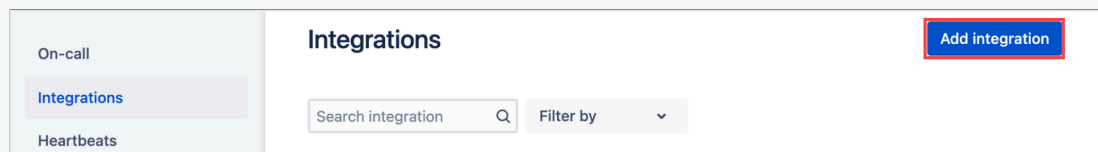
```
"metricName": "${metricName}",
"metricValue": "${metricValue}",
"metricThreshold": "${metricThreshold}",
"uuid": "${uuid}",
"okind": "${okind}",
"onode": "${onode}"
}
```

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.

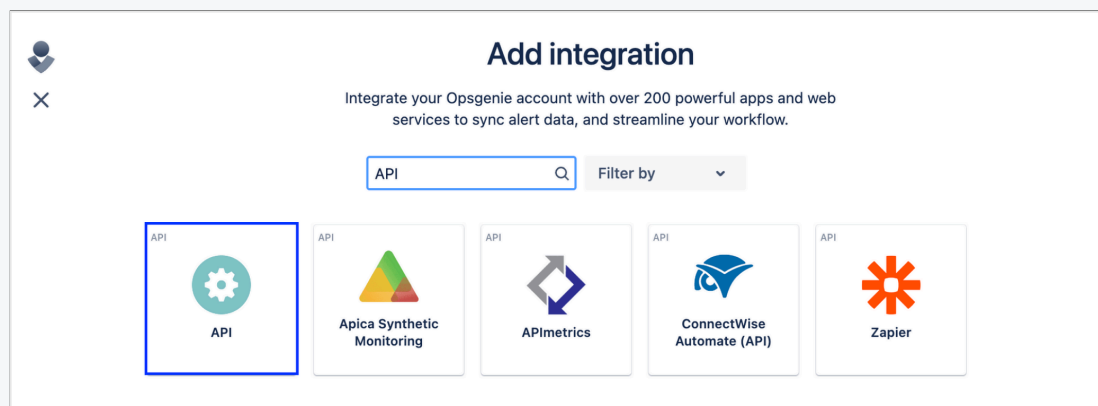
Opsgenie



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
```

Real-time Notifications

The **Alert status** feature displays pop-up notifications when events configured in **Event Configuration** occur. You can receive alerts immediately when an event is triggered, allowing you to quickly recognize issues and respond. You can also review notifications that have already occurred or were missed, helping you understand and resolve situations where real-time response was difficult.

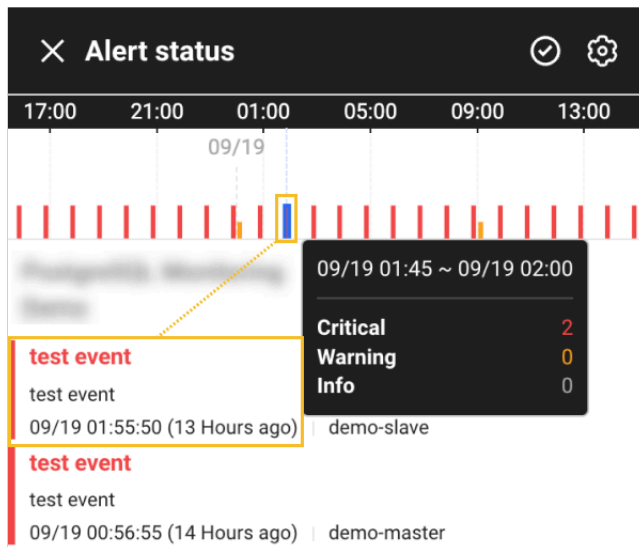
Viewing Real-time Notifications

Real-time notifications appear as pop-ups in the upper-right corner of the screen. You can check the time, title, and message of each notification.

- To close an individual notification, click the  button in the upper-right corner of the message.
- To close all pop-up notifications displayed on the screen, click **Close All Notifications**.

Viewing Notification History

1. Click the  icon at the top of the screen after selecting a project.
2. The **Alert status** window appears.
 - You can view up to 100 notifications from the past 24 hours for the current project.
 - Selecting an individual event item navigates you to the related menu.
 - In the time-based chart within the **Alert status** window, selecting a specific time range takes you to the corresponding event items.



- To view the full notification history, click **View All Notification History**. This navigates to **Alert > Event History**.

ⓘ If the **Alert status** list is empty, the **View All Notification History** button is displayed. Disable the **Receive notifications without reception tags** option.

Resolving Events in Bulk

You can resolve all ongoing events at once from the **Alert status** list. The bulk resolution process may take approximately 30 seconds to 1 minute to complete.

- When using the **Add Acknowledge** feature, a large number of recovery (resolved) notifications may be generated for currently ongoing events.
- Even after using the **Add Acknowledge** feature, events may occur again if the event rules remain enabled and the data still exceeds the threshold.
- Recovery notifications can be disabled by editing the event in **Alert > Event Configuration**. Disable **Send additional notification when the event is resolved** or **Recovered notification**.

How to use:

1. Click the  icon at the top of the screen after selecting a project.
2. When the **Real-time Notifications** window appears, click the  icon in the upper-right corner.
3. When the message `Resolve all ongoing events in the real-time notification list.` appears, click the **Resolve** button.

Configuring Real-time Notifications

1. Click the  icon at the top of the screen after selecting a project.
2. When the **Alert status** window appears, click the  icon in the upper-right corner.
3. Configure each option in the real-time notification settings window.
 - **Popup notifications:** Displays notifications as pop-ups even when the **Alert status** window is closed.
 - **Show resolved events:** Allows resolved events to be displayed in the **Alert status** list.
 - **Preview notification sound:** Lets you preview browser notification sounds. Click the  button next to **Critical** or **Warning**. If you cannot hear the sound, check your browser settings.

System Events

WhaTap Monitoring provides common system events that are automatically detected and generated across the platform. This document explains the types of events generated by the system, their trigger conditions, and recommended response actions.

EVENT_BLOCKED_BY_SYSTEM

If an excessive number of events occurs within a short period of time in a project, the WhaTap system detects this situation and blocks further events. When events are blocked, the system delivers the following message to the user. If you encounter this event, review and adjust your event configuration settings.

 **Critical**



Event Message

Excessive events detected, event blocked for stability. name: server agent

Project No	8
Project Name	new server
Target	server agent
Event Title	EVENT_BLOCKED_BY_SYSTEM
Event Time	(GMT+0900) 2024-11-18 17:58:58

Log In to WhaTap

Events are blocked as a result of excessive events in the server agent of new server project. If no events occur in server agent for a period of time, it is automatically unblocked.

Blocking Criteria

Events are blocked based on the following criteria:

1. Agent-level blocking

If **10 events** occur within **1 minute** from a single agent, all subsequent events from that agent are blocked.

2. Project-wide blocking triggered by multiple agents

If **3 or more agents** are blocked within **1 minute** according to condition 1, events from the entire project are blocked.

3. Project-level blocking

If **100 events** occur within **1 minute** in a single project, all events from that project are blocked.

How to Release the Block

When events are blocked by the system, no events must occur from the affected agent or project for **1 minute**.

- Disable all configured events from **Alert > Event Configuration**. **Review your event settings and adjust thresholds to prevent excessive event generation.**
- Before configuring events, use the **Simulation** feature to estimate how many events may occur.