

Network Performance Monitoring

release date. 2026. 09. 11.

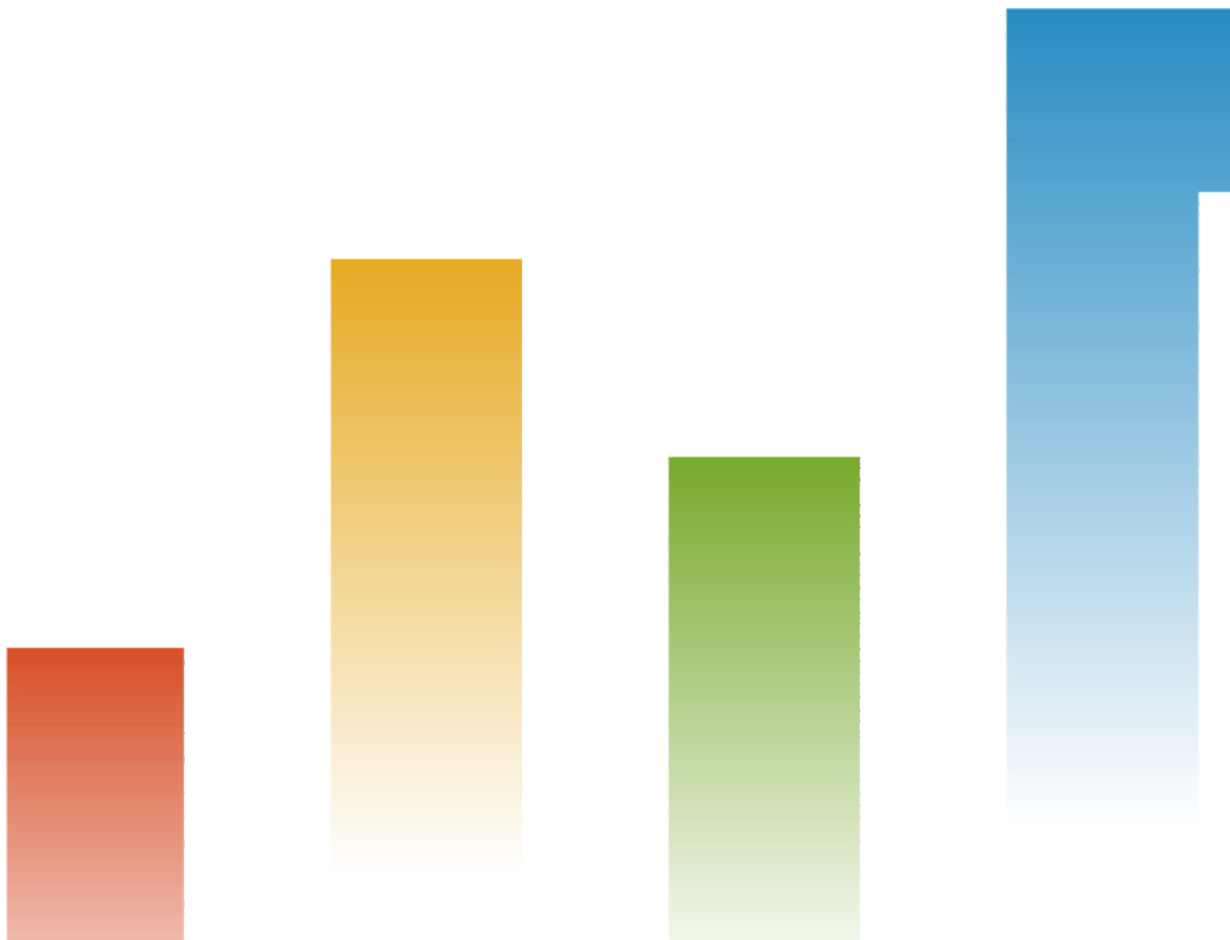


Table Of Contents

• Network Performance Monitoring.....	3
◦ Getting started.....	8
◦ Support Environment.....	10
◦ Agent Installation	13
■ Options for collection of AWS resource data	16
◦ Setting the tagRule.....	19
◦ Dashboard	
■ Network topology	27
■ Network trend (TCP).....	38
◦ Analysis	
■ TCP session/UDP session	43
◦ Metrics.....	50
■ Network performance metrics	52
■ Metrics Search	57
◦ Alert	59
■ Event Configuration	60
■ Metrics	64
■ Event Notification Settings.....	86
■ Event Notification Format.....	108
■ Event History and Monitoring	116
■ Real-time Notifications.....	124
■ System Events	127
◦ Laboratory	130

Network Performance Monitoring

The **Network Performance Monitoring (NPM)** solution collects and visualizes network communication data for processes to identify any congestions and failures between networks and uses them to improve the network performance.

Needs for Network Performance Monitoring

Changes in network environment

Network monitoring must change from traditional equipment-centric monitoring to process-centric monitoring. In the past, network monitoring was operated by obtaining and visualizing data dependent on servers and network equipment through the SNMP protocol. Recently, the network market is growing in the framework for **Cloud** and **Virtualization**, which makes it difficult to determine failure situations and factors by existing monitoring methods.

- **Cloud**

It is changing from an on-premise environment where services were operated through existing servers and network equipment to the environment where services are operated in a virtual environment provided by cloud service providers (CSPs). In the cloud environment where there are no physical entities, important monitoring targets are the **processes** that perform actual works.

- **Virtualization**

In a container-based virtualization environment, multiple containers run on a single machine. Each container has an independent network stack, and communication between multiple containers exists on a single device. It is difficult to identify problematic containers and processes by the traditional equipment-based network monitoring.

Through Network Function Virtualization (NFV), the efforts to virtualize network functions implemented in existing independent hardware by using software are ongoing.

Cloud and **virtualization** have created gray zones that traditional network performance monitoring methods cannot trace. WhaTap **NPM** can respond to environmental changes for **cloud** and **virtualization** because it traces network behaviors for **processes**.

Increase in network complexity

Micro Service Architecture (MSA)-based services are increasing, and network relationships are becoming complex due to flexibility and scalability. Tasks to stabilize services, such as High Availability (HA) configuration or Scale Out, also affect the network complexity. As the relationship becomes more complex, the process of recognizing whether any load occurs and identifying each section becomes increasingly difficult.

WhaTap **NPM** traces the network operations performed by each process and visualizes complex components and status intuitively through the topology.

Expected results

The following benefits can be expected through the metrics collected by process.

- Network metrics monitoring at the process level
- Identifying and improving the service dependencies
- Network cost optimization
- Reduced MTTD and MTTR for network failures
 - **MTTD** (Mean Time To Detect): Time taken to recognize a failure
 - **MTTR** (Mean Time To Repair): Time taken to recover from a failure after recognizing it

Main features

It groups complex networks to quickly monitor the performance metrics for each section. Through the topology dashboard that allows you to quickly respond to network failures, you can quickly identify network failures by using the grouped and simplified network information.

- **Reliable and detailed data collection**

WhaTap **NPM** collects data by using the eBPF technology. The eBPF technology hooks various events occurring in the kernel and performs additional actions in the sandbox environment. Because it hooks kernel events, the detailed information at the process level can be obtained, and stable operation is possible as it is based on the sandbox.

- **Visibility via tag options**

Network monitoring products can provide various complex network data for ease of understanding. WhaTap **NPM** supports the tag options to display network components according to your purpose and intention. Various customizations are possible according to the characteristics of customer services.

- **Troubleshooting through raw data**

Even if you do not access a server, you can check the network status based on the metrics at a specific time point even after a failure situation has been resolved, and support to identify problems such as related servers and processes.

❗ For more information about the menu that uses raw data, see [the following](#).

- **Custom charts of various criteria through the Flex Board**

Custom charts can be created based on various criteria through the collected data.

Guide to key metrics

The network performances are monitored through five network metrics.

- **Quality metrics**

The **latency** and **jitter** metrics are provided as criteria for determining performance issues and failures. It can be collected while using the TCP-based network communication.

- **Latency:** Metric that indicates the network response time. A high response time zone can directly provide a poor experience for end users.
- **Jitter:** Metric that indicates the variability in network response time. A high **Jitter** value can be interpreted as network congestion in the zone and frequent changes in the packet moving path. Failure of a specific network zone can be suspected, and the order of packet arrival is distorted, resulting in packet retransmission, leakage, and poor overall service quality.

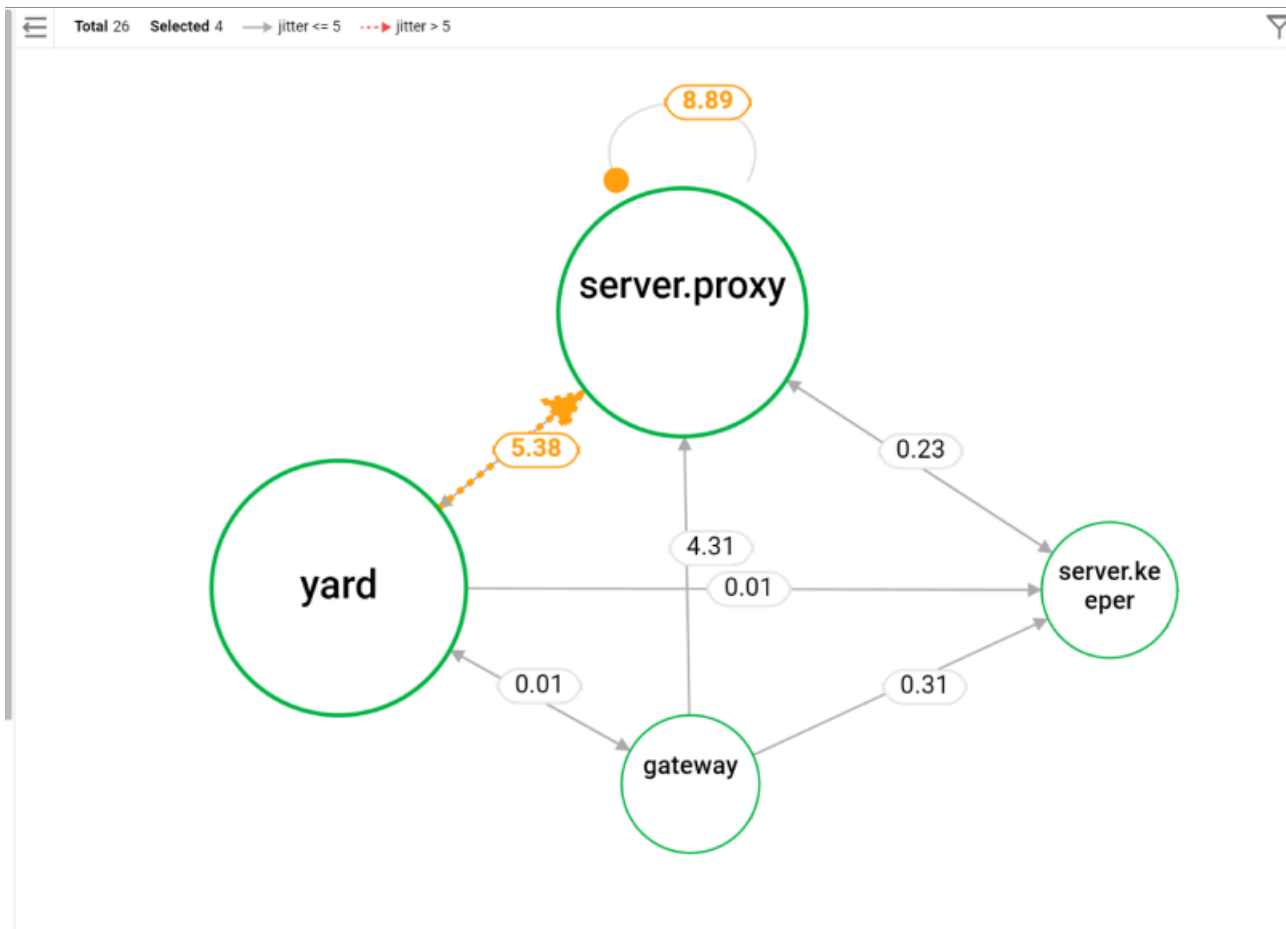
- **Network usage metrics**

bps, **pps**, and **session count** provide the network usage data based on three things, and can be used to optimize the cloud environment through influx of unintended external traffic (DDoS, etc.) or traffic patterns.

- **bps**: Metric that indicates bits per second (bps).
- **pps**: Metric that indicates packets per second (pps).
- **session count**: Metric that indicates the unique session count.

Guide to use metrics

- Network metrics are better to have the target thresholds similar to the server's CPU usage.
 - For service reliability, SLI (Service Level Indicator) and SLO (Service Level Objective) must be defined and based on this, a specific level of service must be consistently provided.
 - If the target value is unclear, collect data based on the initial criteria provided by WhaTap, set the goal later, and then attempt to improve the service.
- Currently, WhaTap applies default thresholds as follows. It can be changed according to user environment and SLO target value.
 - **Jitter**: 30 ms
 - **Latency**: 200 ms
 - **bps**: 128 Mib/s
 - **pps**: 50k
 - **session count**: 100
- By applying the threshold to the topology, you can quickly identify the sections that have exceeded the threshold and support improvement decisions.



- You can send a notification when each metric exceeds the threshold and check the event data.
- For network metrics, a flat and horizontal chart is expected generally. The metrics that rapidly change from the mean value can determine failures and identify each section.

Getting Started

WhaTap monitoring starts with the following steps:

[Step 1. Sign up](#)

[Step 2. Select a product](#)

[Step 3. Create a project](#)

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

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

Sign up

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

Select a product

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

Create a project

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

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

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

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

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

Check the access key

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

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

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

Support Environment

To use WhaTap's **NPM**, install **NPM Agent** on the running servers. Because **NPM** uses the eBPF technology provided by the OS kernel, be sure to check the OS version.

- The versions other than the following list require testing.
- Currently, Windows and mac OS are not supported.

Linux

Minimum version applicable for each OS distribution

Red Hat

REHL	Supportable or not	Default kernel version
Previous Version	X	-
REHL 7.x	X	3.10
REHL 8.x	O	4.18
REHL 9.x	O	5.14

CentOS	Supportable or not	Default kernel version
Previous Version	X	-
CentOS 7.x	X	3.10
CentOS 8.x	X	4.18

CentOS	Supportable or not	Default kernel version
CentOS Stream 8.x	O	4.18
CentOS Stream 9.x	O	5.14

Amzon Linux	Supportable or not	Default kernel version
Previous Version	X	-
Amazon Linux 2.0.20220121.0	X	4.14
Amazon Linux 2.0.20220207.0	O	5.10

Debian

Debian	Supportable or not	Default kernel version
Previous Version	X	-
Debian 10 (buster)	X	4.19
Debian 11 (bullseye)	O	5.10
Debian 12 (bookworm)	O	6.1

Ubuntu	Supportable or not	Default kernel version
Previous Version	X	-
Ubuntu 16.04	X	4.4.0
Ubuntu 18.04	X	4.15.0
Ubuntu 20.04	O	5.4

Ubuntu	Supportable or not	Default kernel version
Ubuntu 22.04	O	5.15

Agent Installation

Installation in the Linux environment

In the [Install guide](#) section, select the [Linux](#) tab and then follow the on-screen instructions to install the agent.

Download agent

Download the agent file to a target monitoring server.

- [Amazon Linux](#) [Debian/Ubuntu](#) [Red Hat/CentOS](#)

```
sudo rpm --import https://repo.whatap.io/centos/release.gpg
echo "[whatap]" | sudo tee /etc/yum.repos.d/whatap.repo > /dev/null
echo "name=whatap packages for enterprise linux" | sudo tee -a /etc/yum.repos.d/whatap.repo > /dev/null
echo "baseurl=https://repo.whatap.io/centos/9/^\$basearch" | sudo tee -a /etc/yum.repos.d/whatap.repo > /dev/null
echo "enabled=1" | sudo tee -a /etc/yum.repos.d/whatap.repo > /dev/null
echo "gpgcheck=0" | sudo tee -a /etc/yum.repos.d/whatap.repo > /dev/null
sudo yum install whatap-npmd
```

For installation, the gnupg2 package is required.

```
wget https://repo.whatap.io/debian/release.gpg -O - | sudo apt-key add -
wget https://repo.whatap.io/debian/whatap-repo_1.0_all.deb
sudo dpkg -i whatap-repo_1.0_all.deb
sudo apt-get update
sudo apt-get install whatap-npmd
```

```
sudo rpm -Uvh https://repo.whatap.io/centos/5/noarch/whatap-repo-1.0-1.noarch.rpm
sudo yum install whatap-npmd
```

ⓘ To collect resource information in the AWS EC2 environment, see [the following](#).

Compatibility checking and configuration

Check the compatibility of the server in which the agent has been downloaded, and then enter the required settings.

```
sudo /usr/whatap/whatap-npmd/install.sh {Project access key} {Collection server IP}
```

You can see the compatibility result and incoming messages as follows.

```
Supported kernel version : 5.15. OK.
Supported CPU Arch : aarch64, OK.
Move package files
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total     Spent    Left     Speed
100  14 100  14    0    0    65    0    0:00:00  0:00:00  0:00:00    65
Start service
Installation complete!
```

Installation in the Kubernetes environment

In the [Install guide](#) section, select the [Kubernetes](#) tab and then follow the on-screen instructions to install the agent.

ⓘ To collect resource information in the AWS EKS environment, see [the following](#).

Agent Creation

1. To create an agent, select **Download** and then download the YAML file.
2. Upload the downloaded YAML file to the master node.
3. Execute the following command in the master node to create an agent.

```
kubectl apply -f whatap_npmd.yaml
```

4. Execute the following command and then check whether the agent's status (**STATUS**) is **RUNNING**.

```
kubectl get pod -n whatap-npm-ns
```

```
ubuntu@Dev-Modules:~/YJH_TESTS$ kubectl get pod -n whatap-npm-ns
NAME                                READY    STATUS    RESTARTS   AGE
whatap-npm-ds-6jgdr                1/1     Running   0           31s
whatap-npm-ds-br795                1/1     Running   0           31s
```

Setting the TagRule option (optional)

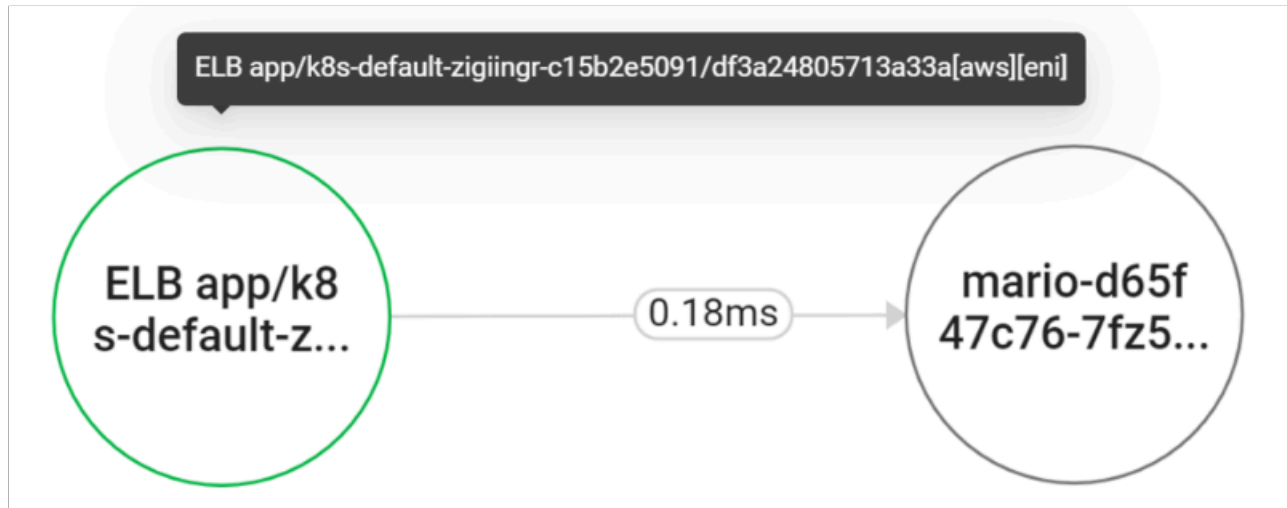
NPM can collect irregular and diverse data through the **tagRule** settings and display the data in a topography or chart. For more details, see [the following](#).

Starting the monitoring

When the agent works, it starts collecting the monitoring data. To check the collected data on the service screen, select **Network topology** at the lower right of the screen.

Options For Collection Of AWS Resource Data

To use the network performance monitoring in the AWS environment, you can collect data on the EC2 network interface (ENI) connected to each resource (e.g. LB) and then represent it in the topology. Because the agent cannot be installed directly as an AWS element, the associated ENI is displayed after checking based on the collected IP.



When traffic is applied internally through AWS's ELB, it can appear in the topology through the data displayed in ENI, as shown in the figure. It appears based on the `Description` field in AWS's ENI. If you do not leave any data in the `Description` field, the `NetworkInterfaceId` property is provided.

Configuring the AWS resource roles in the EC2 environment

When you install the **NPM** agent on AWS EC2, you can collect resource data from AWS based on the IAM settings.

[AWS configuration guide](#)

Configuring the AWS IAM

AWS IAM requires you to specify minimum roles during policy configuration. To collect the AWS resource data from NPM, the `ec2:DescribeNetworkInterfaces` role is required.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        //...
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource": "*"
    }
  ]
}
```

! For more information about the policy and authorization, see [the following link](#).

Configuring the AWS resource roles in the EKS environment

While installing the NPM agent on AWS EKS, you can collect resource data from AWS through ServiceAccount.

! [AWS configuration guide](#)

Configuring the AWS IAM

AWS IAM requires you to specify minimum roles during policy configuration. To collect the AWS resource data from NPM, the `ec2:DescribeNetworkInterfaces` role is required.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        //...
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource": "*"
    }
  ]
}
```

ⓘ For more information about the policy and authorization, see [the following link](#).

Configuring the service account

During the AWS EKS configuration, connect IAM to the Kubernetes service account. To collect AWS resource data from **NPM**, connect IAM to the NPM service account.

For **NPM**, use the following service account.

```
namespace : whatap-npm-ns
service_account : whatap-npm
```

example

```
kubectl annotate serviceaccount -n whatap-npm-ns whatap-npm eks.amazonaws.com/role-
arn=arn:aws:iam::$account_id:role/$role
```

Setting The TagRule

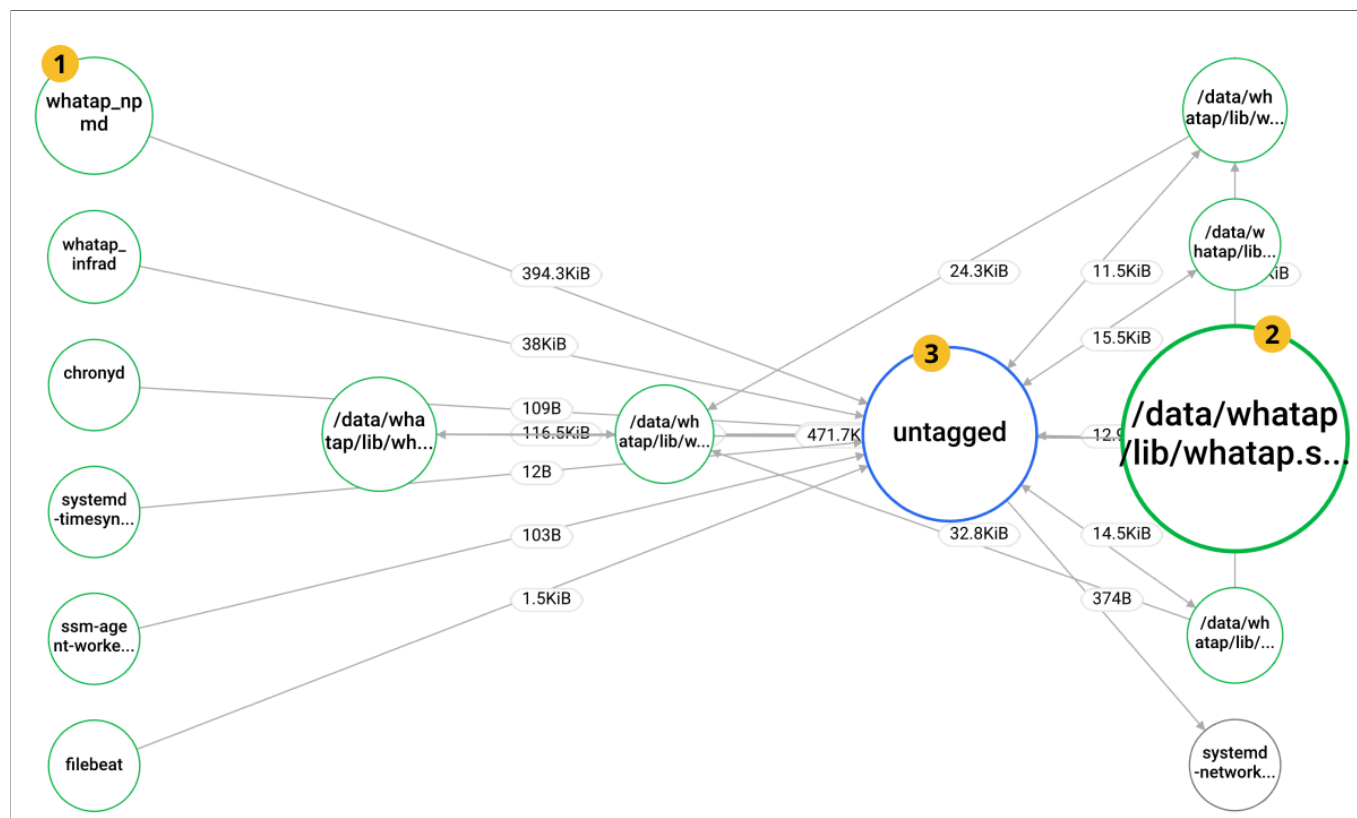
Tag is a criterion for expressing the data collected from the monitored servers in group units. The most important factor in **NPM** is visibility. Grouping is essential to secure visibility in an environment where irregular and diverse data is pouring into the network.

The agent collects the IP addresses, ports (Source, Target), host names, and process names in raw data with keys. Based on the collected data, you can set the group units for the nodes to be displayed in a topology or charts.

Along with the tags collected by agents, the rules have been created to be easily changed and applied. The options can be applied by modifying the `tagRule.yaml` file in the agent installation path (`/usr/whatap/whatap-npmd`).

tagRule option

The result of the **tagRule** option appears in [Dashboard > Network Topology](#). Grouping simplifies the correlation between complex and irregular networks and allows you to visualize the performance of abstracted networks for monitoring.



- It is the **1** node with the **tagRule** option applied. It simplifies long and complex process names to display on nodes.
- It is the **2** node to which the **tagRule** option is not applied. Because it is hard to identify the process, be sure to apply the **tagRule** option to simplify the process name, such as **1** node.
- The **3** node cannot acquire its host and process data. For more information, see [the following](#).

Simplifying the process name

Option: `processRegex`

It simplifies long process names that are obscure. For example, Java processes include JVM launch options and the like as follows.

zookeeper process name

```
java -Dzookeeper.log.dir=/data/wpm/zookeeper/bin/..logs -Dzookeeper.log.file=zookeeper-whatap-server-Dev-Modules.log
```

```
-XX:+HeapDumpOnOutOfMemoryError -XX:OnOutOfMemoryError=kill -9 %p -cp /data/wpm/zookeeper/bin/../zookeeper-server/target/classes:/data/wpm/zookeeper/bin/../build/classes:/data/wpm/zookeeper/bin/../zookeeper-server/target/lib/*:/data/wpm/zookeeper/bin/../build/lib/*:/data/wpm/zookeeper/bin/../lib/zookeeper-prometheus-metrics-3.8.0.jar:/data/wpm/zookeeper/bin/../lib/zookeeper-jute-3.8.0.jar:/data/wpm/zookeeper/bin/../lib/zookeeper-3.8.0.jar:/data/wpm/zookeeper/bin/../lib/snappy-java-1.1.7.7.jar:/data/wpm/zookeeper/bin/../lib/slf4j-api-1.7.30.jar:/data/wpm/zookeeper/bin/../lib/simpleclient-servlet-0.9.0.jar:/data/wpm/zookeeper/bin/../lib/simpleclient-hotspot-0.9.0.jar:/data/wpm/zookeeper/bin/../lib/simpleclient-common-0.9.0.jar:/data/wpm/zookeeper/bin/../lib/simpleclient-0.9.0.jar:/data/wpm/zookeeper/bin/../lib/netty-transport-native-unix-common-4.1.73.Final.jar:/data/wpm/zookeeper/bin/../lib/netty-transport-native-epoll-4.1.73.Final.jar:/data/wpm/zookeeper/bin/../lib/netty-transport-classes-epoll-4.1.73.Final.jar:/data/wpm/zookeeper/bin/../lib/netty-transport-4.1.73.Final.jar:/data/wpm/zookeeper/bin/../lib/netty-tcnative-classes-2.0.48.Final.jar:/data/wpm/zookeeper/bin/../lib/netty-tcnative-2.0.48.Final.jar:/data/wpm/zookeeper/bin/../lib/netty-resolver-4.1.73.Final.jar:/data/wpm/zookeeper/bin/../lib/netty-handler-4.1.73.Final.jar:/data/wpm/zookeeper/bin/../lib/netty-common-4.1.73.Final.jar:/data/wpm/zookeeper/bin/../lib/netty-codec-4.1.73.Final.jar:/data/wpm/zookeeper/bin/../lib/netty-buffer-4.1.73.Final.jar:/data/wpm/zookeeper/bin/../lib/metrics-core-4.1.12.1.jar:/data/wpm/zookeeper/bin/../lib/logback-core-1.2.10.jar:/data/wpm/zookeeper/bin/../lib/logback-classic-1.2.10.jar:/data/wpm/zookeeper/bin/../lib/jline-2.14.6.jar:/data/wpm/zookeeper/bin/../lib/jetty-util-ajax-9.4.43.v20210629.jar:/data/wpm/zookeeper/bin/../lib/jetty-util-9.4.43.v20210629.jar:/data/wpm/zookeeper/bin/../lib/jetty-servlet-9.4.43.v20210629.jar:/data/wpm/zookeeper/bin/../lib/jetty-server-9.4.43.v20210629.jar:/data/wpm/zookeeper/bin/../lib/jetty-security-9.4.43.v20210629.jar:/data/wpm/zookeeper/bin/../lib/jetty-io-9.4.43.v20210629.jar:/data/wpm/zookeeper/bin/../lib/jetty-http-9.4.43.v20210629.jar:/data/wpm/zookeeper/bin/../lib/javax.servlet-api-3.1.0.jar:/data/wpm/zookeeper/bin/../lib/jackson-databind-2.13.1.jar:/data/wpm/zookeeper/bin/../lib/jackson-core-2.13.1.jar:/data/wpm/zookeeper/bin/../lib/jackson-annotations-2.13.1.jar:/data/wpm/zookeeper/bin/../lib/commons-io-2.11.0.jar:/data/wpm/zookeeper/bin/../lib/commons-cli-1.4.jar:/data/wpm/zookeeper/bin/../lib/audience-annotations-0.12.0.jar:/data/wpm/zookeeper/bin/../zookeeper-*.jar:/data/wpm/zookeeper/bin/../zookeeper-server/src/main/resources/lib/*:/data/wpm/zookeeper/bin/../conf: -Xmx1000m -Dcom.sun.management.jmxremote -Dcom.sun.management.jmxremote.local.only=false org.apache.zookeeper.server.quorum.QuorumPeerMain /data/wpm/zookeeper/bin/../conf/zoo.cfg
```

In the above case, even if the name is displayed on a topology or chart,, it is difficult to recognize. Only the required parts are extracted from agents as much as possible. Apply the options by referring to the following example.

tagRule.yaml

```
processRegex:
  - zookeeper
  - whatap_[a-zA-Z]*
```

The `processRegex` option extracts names via the following rules.

- **Java** is the executable JAR file name or method name.

- **Python** is the name of the executable script.

However, if the process name is long enough even after extraction, it can be shortened through the option. It can be input in the form of regular expression. If there are multiple rules, the longest matched string is selected.

❗ If you use numerous short rules, you can tag wrong processes unintentionally. Use a unique naming rule.

Process white list

Option: `processWhiteList`

Set the list of processes to be collected. All data other data than the process specified through the option are ignored.

tagRule.yaml

```
processWhiteList:
- zookeeper
- whatap_[a-zA-Z]*
```

❗ If you use the `processRegEx` option, the name matching the regular expression takes precedence over the OS name.

Process black list

Option: `processBlackList`

It sets the list of processes to exclude from collection. The process data specified through the option is ignored. If both `processWhiteList` and `processBlackList` are in use, data is collected except for the list corresponding to `processBlackList` among the `processWhiteList`.

For example, when three processes (zookeeper, whatap_npmd, and whatap_infrad) are running, the following option is applied to collect data for two processes: zookeeper and whatap_infrad.

tagRule.yaml

```
processWhiteList:
- zookeeper
- whatap_[a-zA-Z]*

processBlackList:
- whatap_npm
```

⚠ If you use the `processRegex` option, the name matching the regular expression takes precedence over the OS name.

Setting the process type

Option: `processType`

The `processType` option is a tag for the most basic group represented in topologies and charts. The main purpose is to express processes that play the same role as a single node when the same process is expressed slightly differently depending on the version or OS.

The process name is used as a key and the matching type is specified. For the processes that are not defined with the option, the process name is automatically applied as the process type.

```
processType:
  apache:
    - httpd
    - apache2
  mysql:
    - mysqld
    - mysqld_safe
```

⚠ If you use the `processRegex` option, the name matching the regular expression takes precedence over the OS name.

Setting the App name

Option: `appName`

The `appName` option expresses the topology or chart in a form that is easy to understand. In case of the `processType` option above, the same process is merged into a single node regardless of your intention. For `appName`, you can express the node in your desired form by specifying the node to express separately and the node to merge through a key combination.

Let's assume the case in which the network configuration of proxy → msa_process → msa_process2 → db is divided into three purposes: **operation stage**, **development stage**, and **testing stage**.

- In case of visualization with the `processType` option
- In case the processes with the same name are divided into **operation stage**, **development stage**, and **testing stage** with the `appName` option

tagRule.yaml

```
appName:
  prod_proxy: # Operation stage
    - host_tag: prod_proxy
      process_type: proxy
  prod_msa1: # Operation stage
    - host_tag: prod_msa
      process_type: msa_process1
  prod_msa2: # Operation stage
    - host_tag: prod_msa
      process_type: msa_process2
  dev_proxy: # Development stage
    - host_tag: dev_proxy
      process_type: proxy
  dev_msa: # Development stage
    - host_tag: dev_msa
      process_type: msa_process1
    - host_tag: dev_msa
      process_type: msa_process2
  test: # Testing stage
    - host_tag: test
  db:
```

```
- process_type: mysql
```

- The keys available by `appName` are `host_tag` , `process_type` , `ip` , and `port` .
- The keys that have not been entered are applied as wild cards.

If the `appName` option is not met, the field or value specified in the `appNameDefault` option is applied.

- In `appNameDefault` , enter the key to be used by default.
- If you enter any of `host_tag` and `process_type` , the field data is automatically assigned to `appName` . If you enter a string other than that, it is fixed to the value.

tagRule.yaml

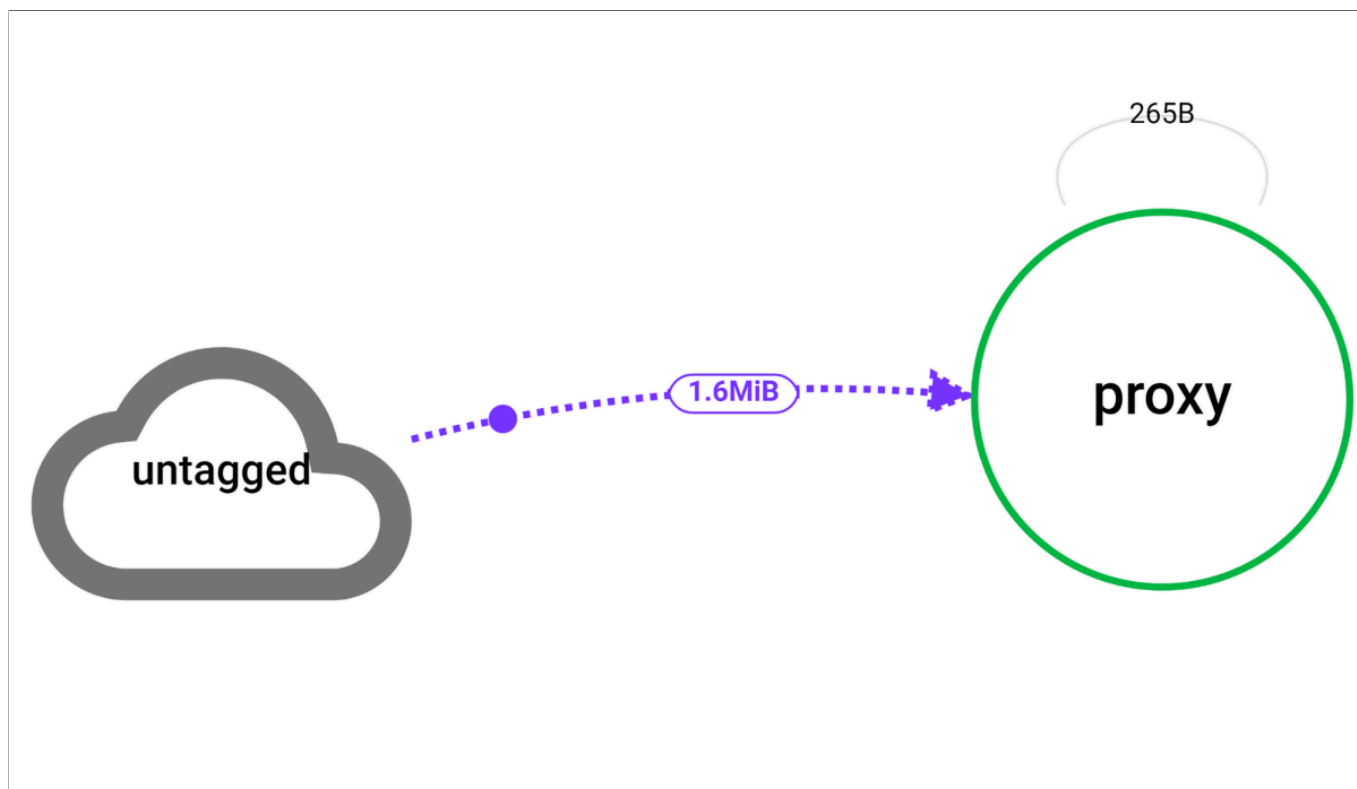
```
appNameDefault: host_tag # host_tag, process_type, custom string
```

Identification of unclear targets

Option: `untagOption`

When communicating with a target that does not have an agent installed, such as ELB provided by a Cloud Service Provider (CSP) or external API, the host and process data cannot be acquired. Tags can be set based on the IP and port that you know (or the target to be managed).

If the agent has not been installed and communication is made with the IP or port that has not been defined with the option, it is displayed as an **untagged** node on the topology.



Set the tag with the IP and port as keys. In case of inbound traffic, set it to `0` because the external port is the client port and is not the fixed service port.

tagRule.yaml

```
untagOption:  
  15.165.146.117:  
    6600: "whatap-proxy"  
  172.31.24.16:  
    0: "ELB app/New-gitlab/5fe1a93082df3495"
```

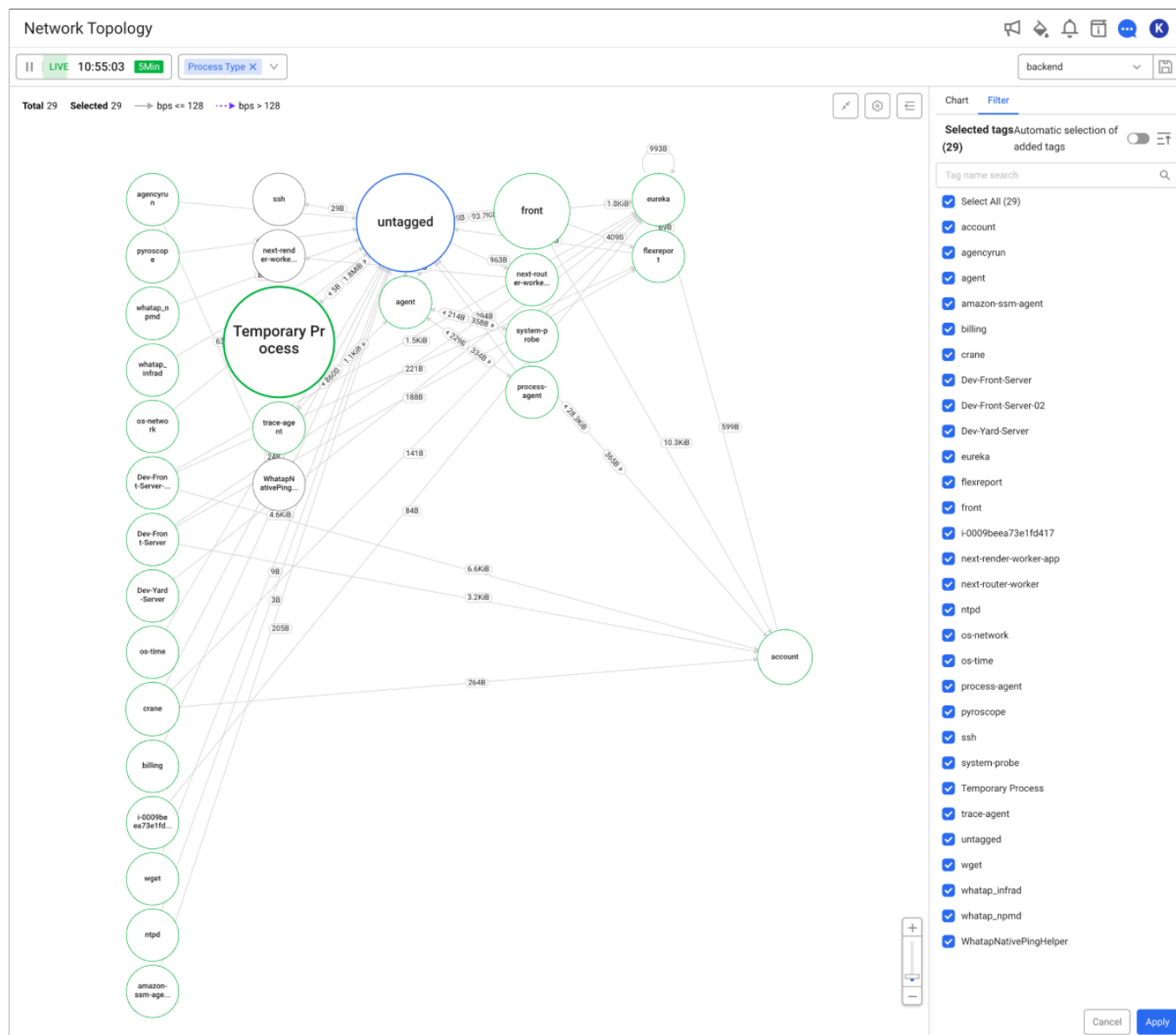
Network Topology

Home > Select Project > **Dashboard** > **Network topology**

In **Network topology**, you can see the relationship between nodes at a glance through the topology chart, and quickly see the performances for each network section that relate the line charts for each metric. Real-time and historical data can be viewed, and the performances of abstracted networks can be visualized and monitored based on the process type or application tags.

Basic screen guide

Topology shapes the network with **nodes** and **edges**. In parallel with the time series charts for each performance metric, the network bottlenecks or failure sections can be identified more easily.



- **Node** is a criterion for expressing the data collected from the monitored servers in group units. This element is expressed as a circle in the chart.
- **Edge** means the node-to-node communication. For more information, see [the following](#).
- You can move the screen to a desired position by clicking and dragging an empty area of the topology chart.
- You can zoom in or out the topology chart by scrolling the mouse wheel. You can also use the slide tools at the lower right corner.
- You can move each node by clicking and dragging it to a desired position.

- Select the  button on the upper right of the screen to sort the canvas positions so that all nodes are visible on the screen. It is useful for quickly seeing all nodes after filtering tags and repositioning nodes.
- Just above the topology chart, you can see the summary information such as the total node count, number of tag-filtered nodes, and threshold settings.

Total 25 Selected 24  bps <= 128  bps > 128

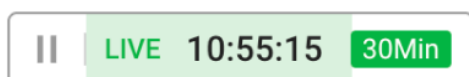
- To hide the filter panel on the right and zoom in the topology screen, select  on the right of the chart.

The topology chart options

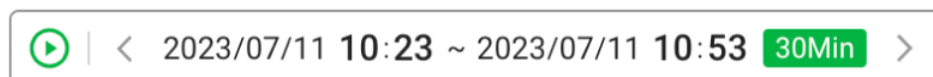
You can view and analyze data by setting what to display on the topology chart.

Setting the lookup time

- **Realtime mode:** Searches the data for the time set on the green button in real time.

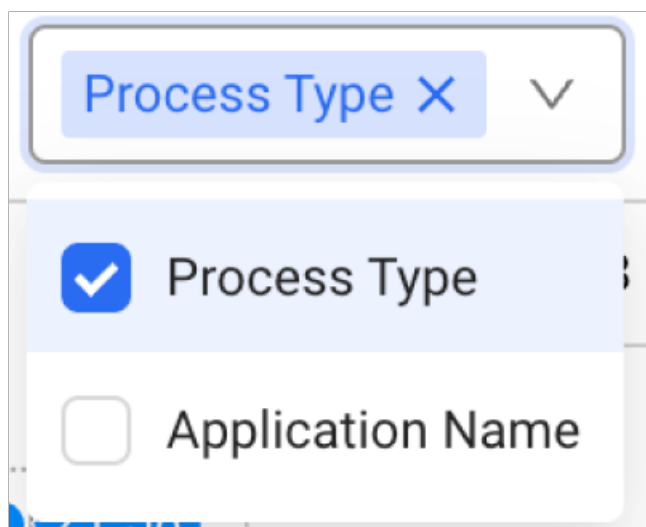


- You can click the green button to select a desired time.
- Click **II** to pause the real-time data search and then search the data for a desired time.
- **Time setting mode:** You can see the data by setting a desired time.



- Click the green button to select a time from various values.
- By selecting **<** or **>**, you can move by the time set on the green button.
- If you click the text range for date and time, the option appears to select the date and time.
- To switch to the Realtime mode, select .

Selecting a node type

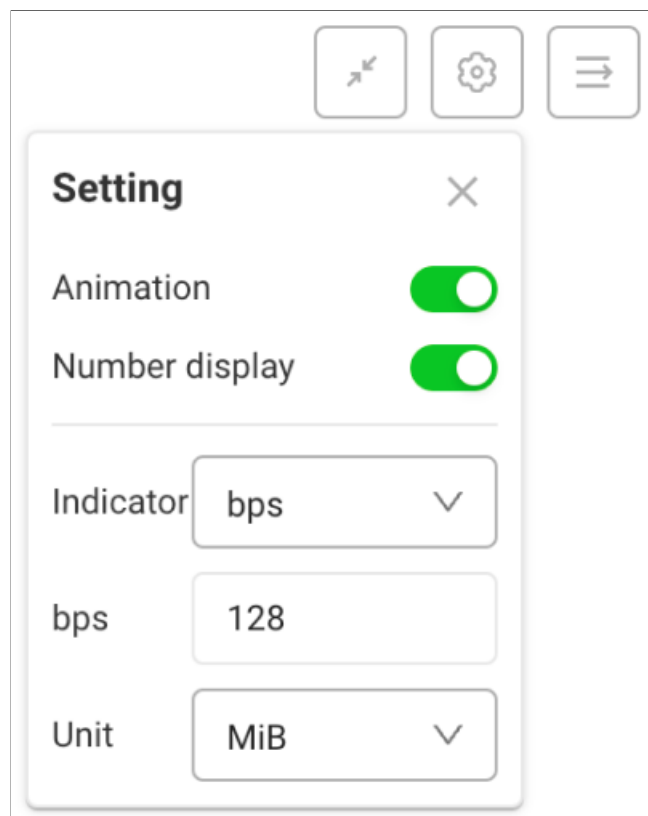


You can select a node type displayed on the chart. Each corresponds to a single tag. Tags are collected depending on the **tagRule** options you set in the [tagRule.yaml](#) file. Nodes can be expressed as **Process type** and **Application name** or a combination of the two.

ⓘ For more information about the **tagRule** options, see [the following](#).

Setting the visual information of the chart

Among the data displayed on the chart, only the required data can be visually exposed. Select ⚙ on the upper right of the screen.



Default options

- **Animation:** Set whether or not to display the animation when the threshold is exceeded.
- **Number display:** Set whether or not to display the edge labels.

Setting the edge label

Edge means the node-to-node communication and the labels for each edge display the selected performance metrics.

Edge

You can select a type of the value to display on the edge of the topology chart. In **Indicator**, you can select a desired metric. The types of performance metrics that can be displayed on the edge are as follows.

- [jitter](#)
- [latency](#)

- [bps](#)(bit per second)
- [pps](#)(packet per second)
- [sessions](#)

- ! • In **Edge**, the second item is also changed according to the selected metric type. In the second item, you can set the thresholds for the selected metric.

Indicator	jitter
jitter	30
Unit	ms

- The weight of the node size is automatically set depending on the value selected in the **Indicator** item.

Setting the threshold

In the second item and **Unit**, you can set the thresholds and units for the metric set to Edge. The edges that exceed the threshold are highlighted on the topology.

The thresholds and units are set as follows, unless there is a separate setting procedure.

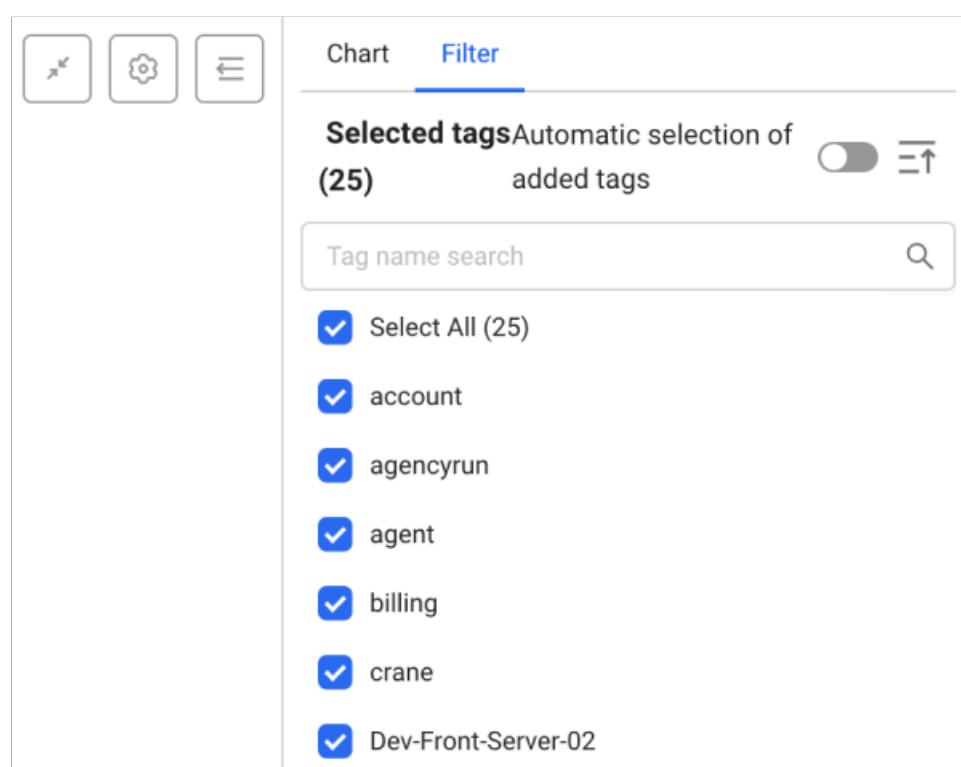
- latency > 200 (ms)
- jitter > 30 (ms)
- bps > 128 (Mib/s)
- pps > 50 (K/s)
- sessions > 100

The settings can be checked in the summary on the upper left of the chart.

Total 25 **Selected 24** $\longrightarrow$ bps $\leq$ 128 $\dashrightarrow$ bps $>$ 128

Filtering the tags

If the network configuration is too vast and complicated, you can configure a sub network view by selecting some nodes. In the panel on the right of the screen, select the **Filter** tab. When the tag list set through the **tagRule** option appears, select the nodes to display on the screen.



Only the communication performance data between the selected tag nodes and the target node appears on the topology chart. If you exclude the nodes merged by **untagged** from the topology and time series charts, or there are no nodes for analysis, uncheck them.

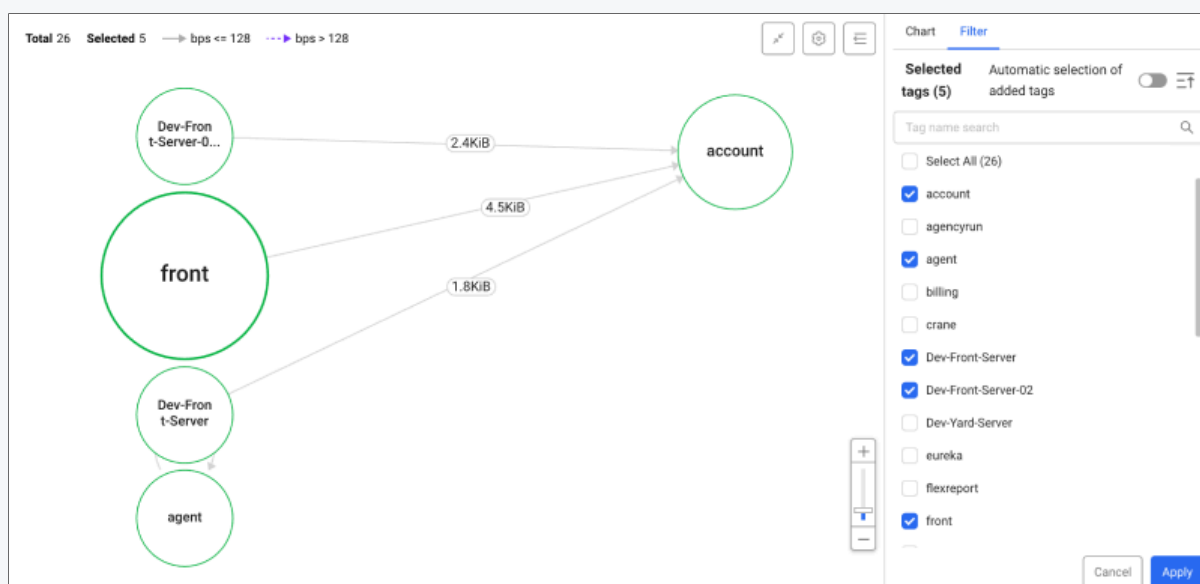
The information configured in this way can be saved through the **preset** function and then recalled for analysis.

- Only the tags collected during the data lookup period are displayed in the list.
- To automatically select new added nodes, select the **Automatic selection of added tags** option.
- For more information about the **preset** menu, see [the following](#).

Usage example

To display only some nodes out of all nodes, follow the steps below.

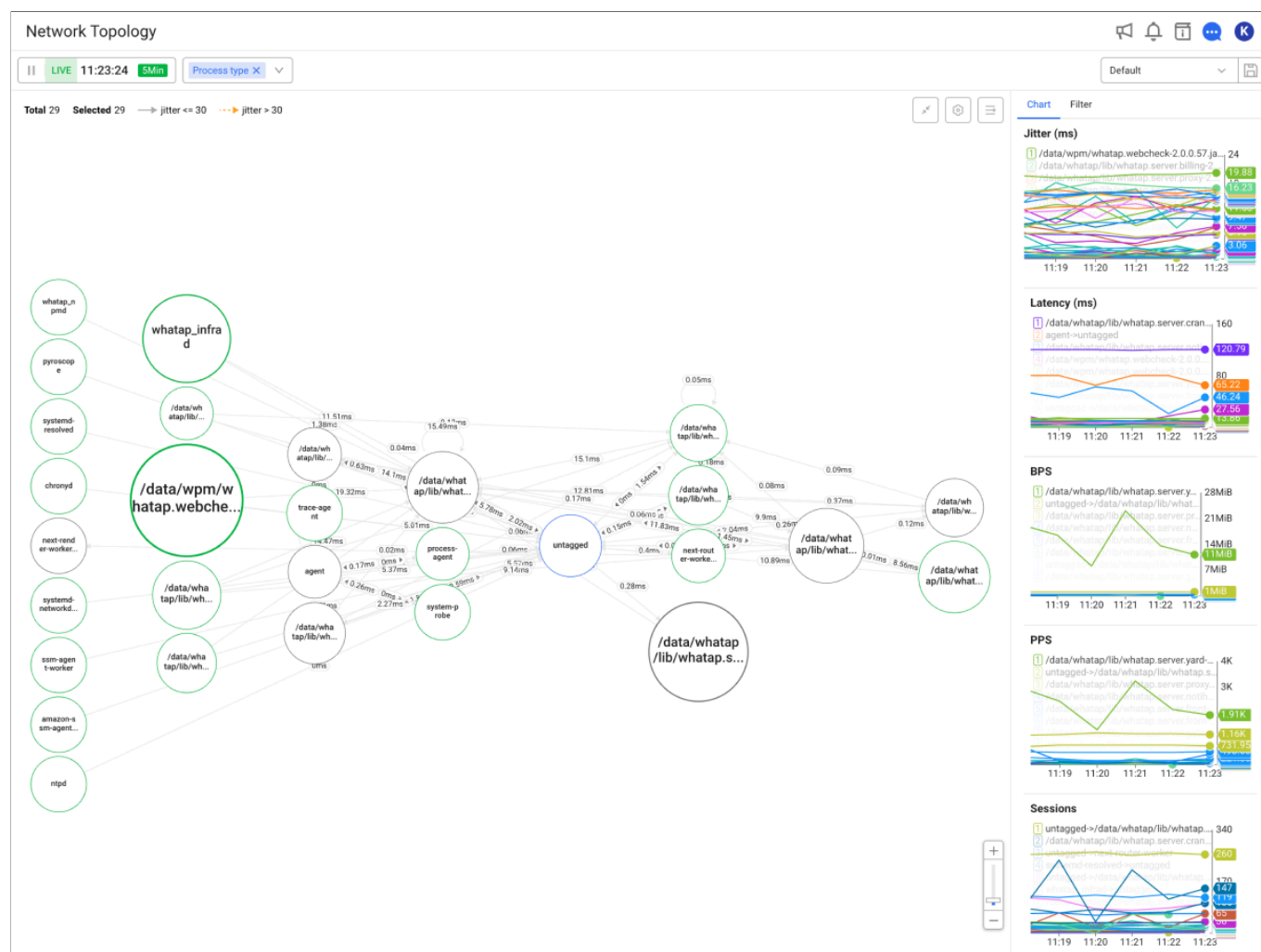
1. In the panel on the right of the screen, select the **Filter** tab.
2. Release the **Select all** option and then disable the **Automatic selection of added tags** option.
3. Select or deselect nodes in the topology chart. You can easily find the desired node by searching for the tag name or using the sorting function (⇅↑).
4. At the bottom of the screen, select **Apply**.



⚠ If you select the **Select all** option and then unselect some nodes, **Select all** is automatically deselected.

Checking the chart

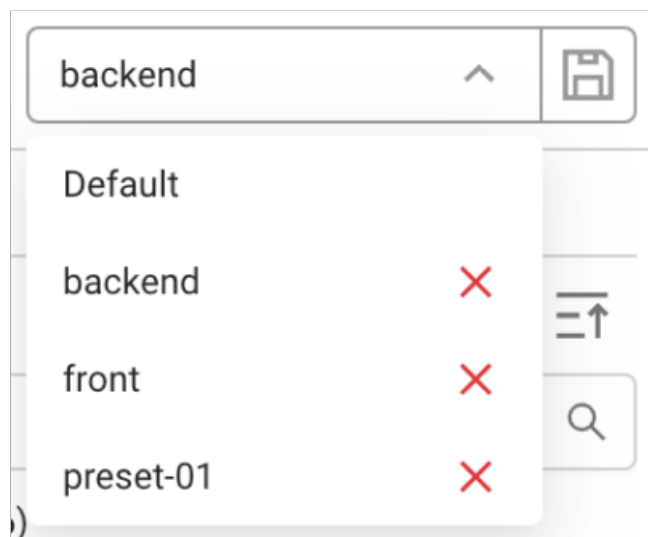
You can quickly check the performance of the network section by integrating with the line charts for each metric. In the panel on the right, select the **Chart** tab.



- The items displayed in the **Chart** tab are the tags selected in the **Filter** tab.
- Hover your mouse over the chart to see the network performance over time.

Preset

Through the **preset** function, you can save the sub network topology view by relating the tag filter function. If there are too many nodes and edges in the topology view, it is recommended to divide and filter the network part and save it as a preset for analysis.

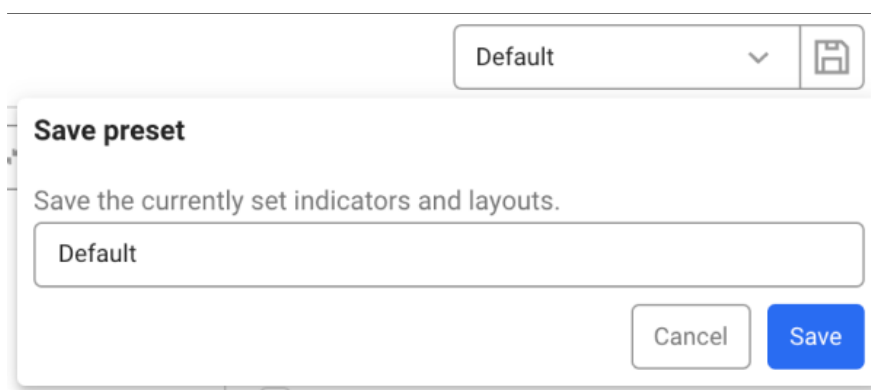


The data saved in the preset is as follows.

- Node display type
- Edge display type
- Threshold value
- Tag filter
- Positions for each tag on the topology

Creating a preset

1. Set the topology chart options as you want.
2. On the upper right of the screen, select .
3. When the **Save preset** window appears, enter the name of the preset to save.



4. After entering the preset name, select **Save**.

Modifying a preset

With a preset selected, modify the options of the topology chart. To update the current preset, save it with the same name as the previous preset.

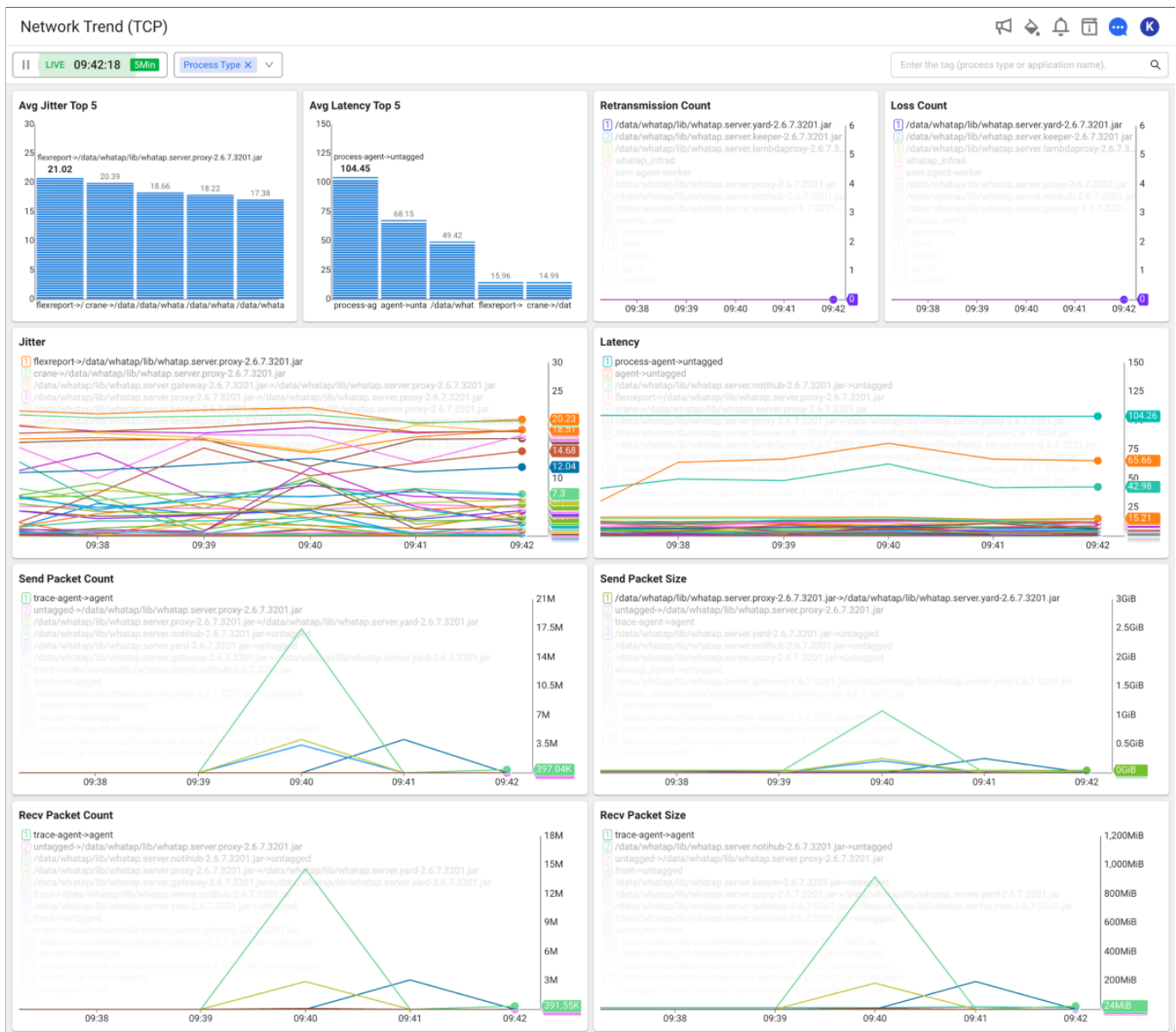
! You can also save the preset with another name.

Deleting presets

To delete unused presets, select **×** in the preset list.

Network Trend (TCP)

Home > Select Project > [Dashboard](#) > [Network Trend \(TCP\)](#)



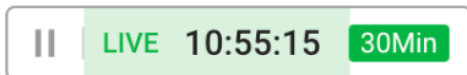
While the [Network Topology](#) menu mainly visualizes the network configuration, the [Network Trend \(TCP\)](#) menu allows you to see the performances in a dense manner on a single screen. The performances over time can be

displayed in real time, and the performances in the past can be displayed and used as the data to analyze problems.

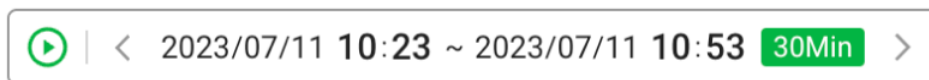
Configuring the chart options

Setting the lookup time

- **Realtime mode:** Searches the data for the time set on the green button in real time.

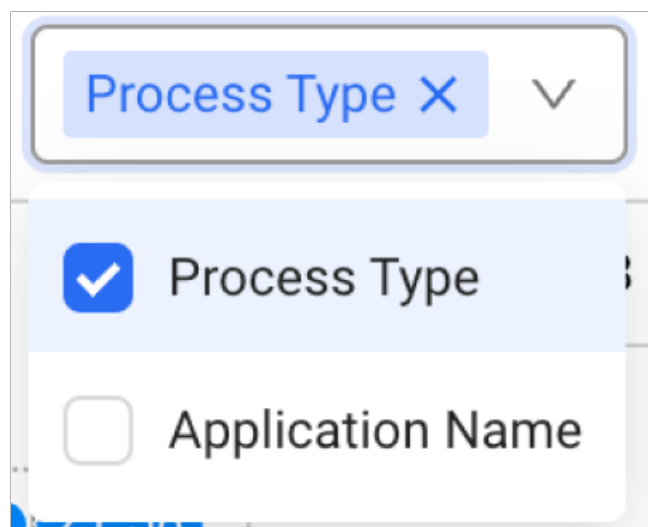


- You can click the green button to select a desired time.
- Click **II** to pause the real-time data search and then search the data for a desired time.
- **Time setting mode:** You can see the data by setting a desired time.



- Click the green button to select a time from various values.
- By selecting **<** or **>**, you can move by the time set on the green button.
- If you click the text range for date and time, the option appears to select the date and time.
- To switch to the Realtime mode, select **▶**.

Selecting a node type



You can select a node type displayed on the chart. Each corresponds to a single tag. Tags are collected depending on the **tagRule** options you set in the [tagRule.yaml](#) file. Nodes can be expressed as **Process type** and **Application name** or a combination of the two.

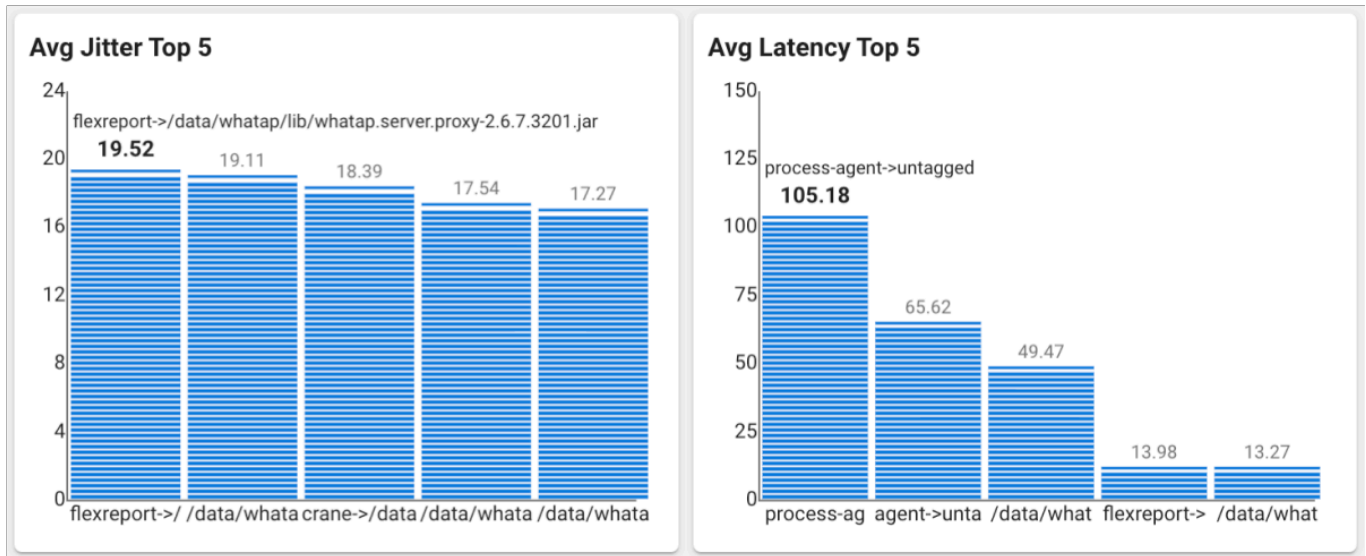
! For more information about the **tagRule** options, see [the following](#).

Searching the node

The search bar on the upper right of the screen allows you to filter the nodes displayed on the chart. The items that do not meet the search word do not appear on the chart.

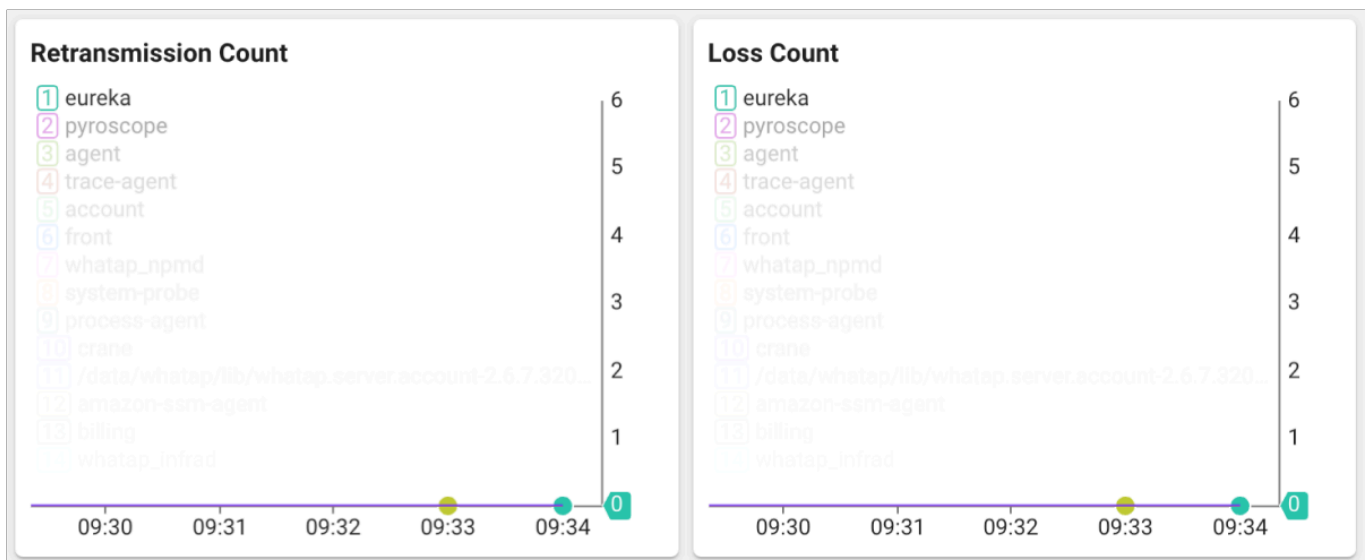
! This is useful when checking only the communication related to specific tags.

Top 5 Charts



It charts **jitter** and **latency**, which are key metrics for communication failures on the network, in the top-five order.

Packet retransmission and loss metrics



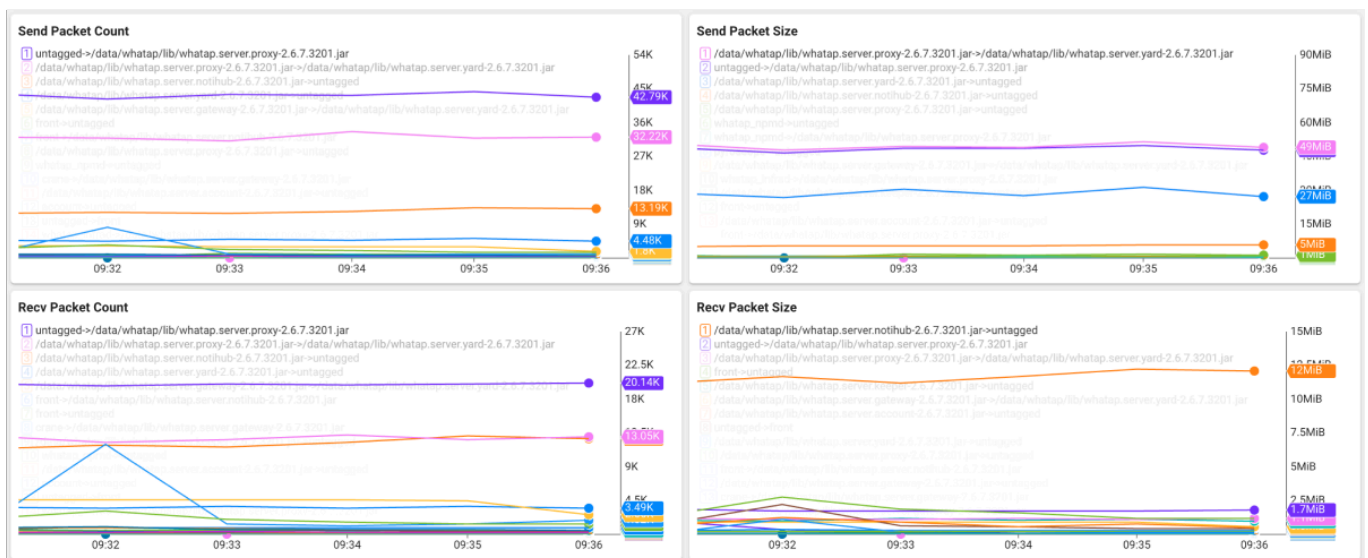
It displays the number of retransmissions in a specific communication section as a chart. In connection with the packet loss count that can cause retransmission, you can check the retransmissions for packet loss.

Latency metric



Network reliability can be evaluated based on the latency and changes in latency.

Data throughput metric



It charts the data throughput (bps or pps) metrics broken down from the send/receive perspective.

TCP Session/UDP Session

Home > Select Project > Analysis > TCP session or UDP session

The session data collected by agents can be used to identify failure points in detail. It provides the filters that allow you to set multiple conditions to efficiently identify data. The identified data can be downloaded in CSV format for other purposes.

< 2024/01/05 14:14 ~ 2024/01/05 15:14 60Min >

Direction In Out

Enter Filter and press enter to add.

Column Settings CSV

No	Time	Local Process Type	Local App Name	IP	Port	Foreign IP	Foreign Port	PID	Foreign Process Type
1	24/01/05 15:13:05	front	dev-front-02	10.21.1.187	0	10.21.13.216	6379	3487158	untagged
2	24/01/05 15:13:05	eureka	dev-front-02	10.21.1.187	0	10.21.1.99	6761	3417880	eureka
3	24/01/05 15:13:05	front	dev-front-02	10.21.1.187	0	10.21.1.187	18080	3487158	account
4	24/01/05 15:13:05	process-agent	dev-front-02	10.21.1.187	0	34.160.150.109	443	1875864	untagged
5	24/01/05 15:13:05	front	dev-front-02	10.21.1.187	0	10.21.1.99	6761	3487158	eureka
6	24/01/05 15:13:05	agent	dev-front-02	10.21.1.187	0	35.190.51.116	443	1875863	untagged
7	24/01/05 15:13:05	front	dev-front-02	10.21.1.187	0	75.2.37.199	443	3487158	untagged
8	24/01/05 15:13:05	trace-agent	dev-front-02	127.0.0.1	0	127.0.0.1	5001	1875865	agent
9	24/01/05 15:13:05	agent	dev-front-02	10.21.1.187	0	35.244.255.175	443	1875863	untagged
10	24/01/05 15:13:05	agent	dev-front-02	127.0.0.1	0	127.0.0.1	5001	1875863	agent
11	24/01/05 15:13:05	account	dev-front-02	10.21.1.187	0	10.21.1.187	6761	3559745	eureka
12	24/01/05 15:13:05	process-agent	dev-front-02	127.0.0.1	0	127.0.0.1	5001	1875864	agent
13	24/01/05 15:13:05	eureka	dev-front-02	10.21.1.187	0	15.165.146.117	6600	3417880	proxy
14	24/01/05 15:13:05	eureka	dev-front-02	10.21.1.187	0	10.21.1.187	6761	3417880	eureka
15	24/01/05 15:13:05	front	dev-front-02	10.21.1.187	0	10.21.1.187	6761	3487158	eureka
16	24/01/05 15:13:05	system-probe	dev-front-02	127.0.0.1	0	127.0.0.1	5001	1875862	agent
17	24/01/05 15:13:05	front	dev-front-02	10.21.1.187	0	10.21.1.99	18080	3487158	account
18	24/01/05 15:13:05	pyroscope	dev-front-02	10.21.1.187	0	10.20.1.185	4040	1057434	untagged
19	24/01/05 15:13:05	front	dev-front-02	10.21.1.187	0	15.165.146.117	6600	3487158	proxy
20	24/01/05 15:13:05	whatap_npm	dev-front-02	10.21.1.187	0	3.39.176.158	6600	3564600	untagged
21	24/01/05 15:13:05	account	dev-front-02	10.21.1.187	0	15.165.146.117	6600	3559745	proxy
22	24/01/05 15:13:05	account	dev-front-02	10.21.1.187	0	10.21.1.183	3306	3559745	untagged
23	24/01/05 15:13:05	front	dev-front-02	10.21.1.187	0	10.21.1.55	8800	3487158	gateway

Set a desired 1 time, and then select 2 . The table displays the data that meets the set conditions.

- !
- After setting new data search conditions, select to output the target data.
 - This function uses raw data. It provides up to 5 cases per minute based on one agent.

Setting the lookup time

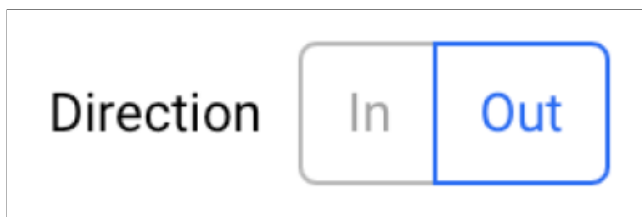
You can see the data by setting a desired time.



- You can click the green button to select a desired time. It can be set up to 1 hour.
- By selecting < or >, you can move by the time set on the green button.
- If you click the text range for date and time, the option appears to select the date and time.

Setting for the session data search

Configuring the inbound/outbound conditions



Before setting the search conditions, select the following traffic types.

- **In**: Inbound traffic
- **Out**: Outbound traffic

Setting the filter conditions

You can see the data by setting multiple filter conditions for tag and field values. Conditions are added by the **&&** (and) condition. For example, to search the session data with the **ProcessType** tag value of "agencyrun" and the **Session Count** field value greater than 2, set as follows.


 Local Process Type == agencyrun X Session Count > 2 X Enter Filter and press enter to add.
 

- ✓ You can filter with the || (or) condition when duplicate tags or field values have been set as follows:

Local Process Type == agencyrun, Local Process Type == dev-yard

1. Select the Filter field to see the list of available filters.

You can select the string format (text) and the numeric format (numeric).

 Enter Filter and press enter to add.

Text	
Local IP	text
Local Port	text
Foreign IP	text
Foreign Port	text
Local Process Type	text
Local App Name	text
Foreign Process Type	text
Foreign App Name	text
Numeric	
Send Packet Count	numeric
Send Packet Size	numeric
Receive Packet Count	numeric
Receive Packet Size	numeric
Session Count	numeric

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

2. Select a filter and then select **Operator**(Operator).

Depending on the string format and numeric format, the operator you can select may differ.

- String format

Local Process Type Enter Filter and press enter to add.

Operator

== operator

!= operator

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

- Numeric format

Session Count Enter Filter and press enter to add.

Operator

== operator

!= operator

> operator

>= operator

< operator

<= operator

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

3. If a string format is selected, the list of available values appears. Select a desired value. In case of a numeric format, enter it directly.

Local Process Type == Enter Filter and press enter to add.

Local Process Type

Temporary Process Process Type

account Process Type

agencyrun Process Type

agent Process Type

amazon-ssm-agent Process Type

billing Process Type

crane Process Type

4. Select a desired value or enter a number. To add filters, press Enter and then repeat the above steps.
5. Select  to the right of the Filter field.

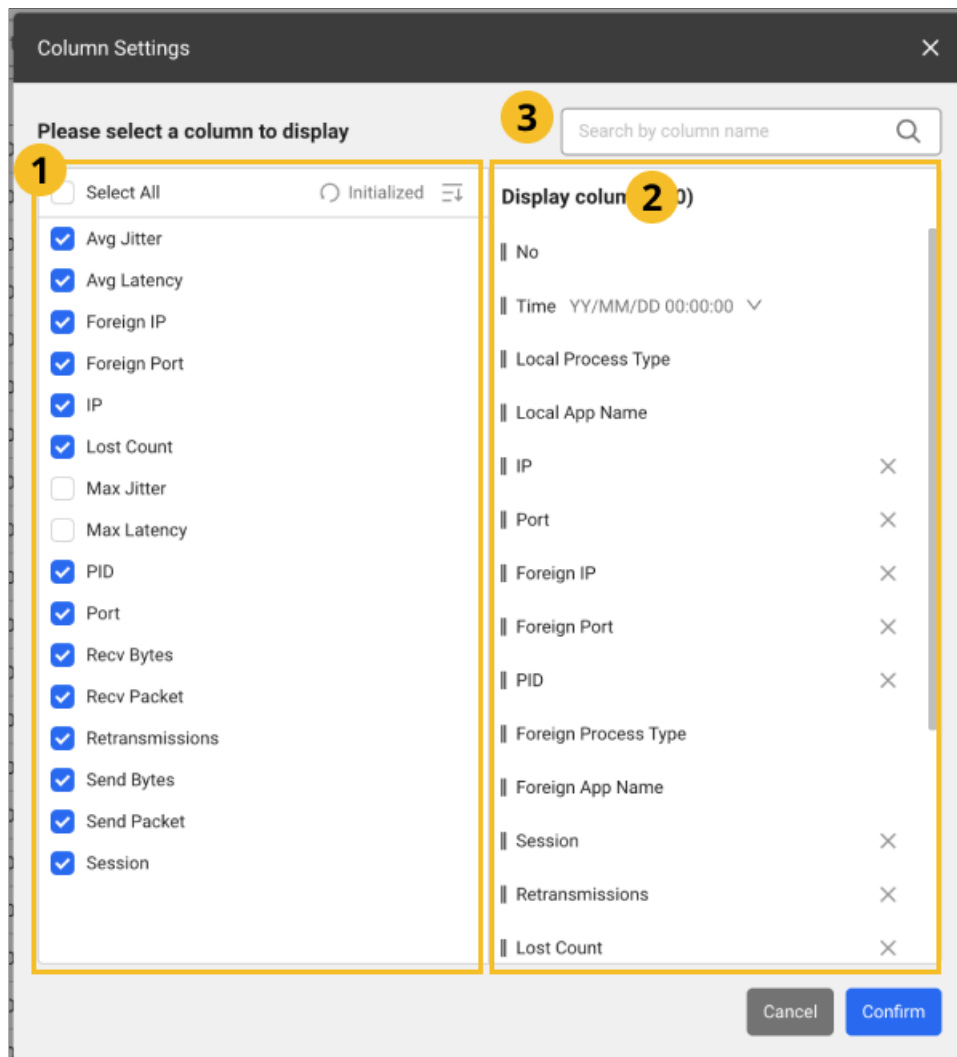
Operator types

Type	Operator	Description
Text/Numeric	<code>==</code>	Filters the strings that match the value of the selected filter.
	<code>!=</code>	Filters the strings that exclude the value of the selected filter.
Numeric	<code>></code>	Filters the cases that are greater than the value of the selected filter.
	<code>>=</code>	Filters the cases that are greater than or equal to the value of the selected filter.
	<code><</code>	Filters the cases that are less than the value of the selected filter.
	<code><=</code>	Filters the cases that are less than or equal to the value of the selected filter.

Additional options

Setting the table columns

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



- After configuration, select **Confirm** to apply the settings in the table.
- In the (3) search bar, enter text to search the desired columns. Only the columns that meet the entered text are displayed.

Adding columns

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

Deleting columns

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

Changing the column order

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

Initializing the configuration

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

Downloading the viewed data

To download the data output in the table in CSV format, select .

Metrics

Home > Select Project > Sitemap > Metrics Search

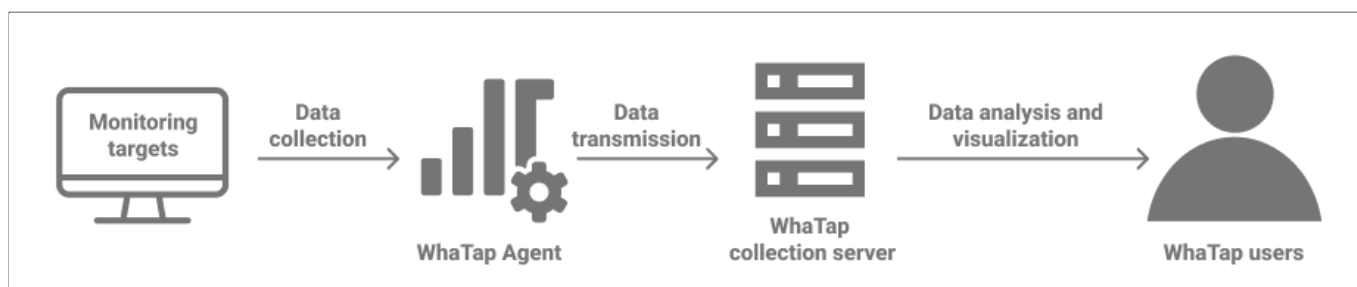
What is a metric?

A **metric** is time-series data that represents the state of a monitoring target as numerical values. It is the result of processing performance data collected by the WhaTap agent from monitoring targets.

Through metrics, you can view key performance indicators such as memory usage per server and DB connection time at a glance. After identifying a problem, you can perform detailed analysis through logs and traces.

Resource usage statistics help you estimate the required amount of resources, which can also be used for cost optimization.

How WhaTap collects metrics



To collect metrics, install the WhaTap agent on the monitoring target. Metrics sent by the agent are stored on the WhaTap collection server.

Metric components

WhaTap **metrics** consist of the following components:

- **Category:** A name that groups related metrics.

- **Tags:** Labels that identify collection targets. Stores rarely-changing unique information such as IP, Oname, and Host. A metric can contain multiple tags.
- **Fields:** Stores actual measured values. A metric can contain multiple fields.
- **Time:** The time when the metric was collected.
- **Oid:** The unique number of the agent that collected the metric.
- **Oname:** The name of the agent that collected the metric.

Viewing and visualizing metrics

WhaTap provides the **Metrics Search** menu where you can view original data collected based on user-defined conditions.

Network Performance Metrics

It describes the metrics indicators that are collected by Network Performance Monitoring. You can search in **Sitemap > Metrics Search**. Network performance metrics provide all data folded into fields.

npm_process_tag_data

It indicates the network communication metric for each session. The collection interval is 1 minute.

Field name	Unit	Description	Remarks
app_name	-	Custom identification tag for the communicating entity	Default - A single Linux server environment: Host name - Kubernetes container environment: Pod name
avg_jitter	ms	Average of packet round-trip latency fluctuations	Average jitter over the collection interval
avg_latency	ms	Average packet round-trip latency time	Average latency over the collection interval
container_name	-	Name of the container collected in the Kubernetes environment	Empty value if not in Kubernetes environment
direction	-	Session connection direction	IN (Inbound), OUT (Outbound)
foreign_container_id	-	ID of the container for local communication in the Kubernetes container	During local communication, the target cannot be identified using the IP address and port number. Therefore, additional data is provided to find the exact target.

Field name	Unit	Description	Remarks
foreign_ip	-	Target IP address	-
foreign_pod_id	-	Pod ID in case of local communication within a Kubernetes Pod	During local communication, the target cannot be identified using the IP address and port number. Therefore, additional data is provided to find the exact target.
foreign_port	-	Target port number	Client Port (Inbound - foreign_port) is displayed with data merged to 0.
host_tag	-	Source host name	-
local_ip	-	Source IP address	-
local_port	-	Source port number	Client Port (Outbound - local_port) is displayed with data merged to 0.
lost_count	count	Number of lost packets	-
max_jitter	ms	Maximum for packet round-trip latency fluctuations	Maximum for jitters collected for a certain period
max_latency	ms	Maximum packet round-trip latency time	Maximum for latencies collected for a certain period
min_jitter	ms	Minimum for packet round-trip latency fluctuations	Minimum for jitters collected for a certain period
min_latency	ms	Minimum packet round-trip latency time	Minimum for latencies collected for a certain period
pod_name	-	Pod name in case the communication source is in the Kubernetes	Empty value if not in Kubernetes environment

Field name	Unit	Description	Remarks
		environment	
process_type	-	Type of process for communication	-
protocol	-	Communication protocol type	TCP / UDP
recv_packet_count	count	Number of received packets	-
recv_packet_size	byte	Data size of the received packet	-
retransmission_count	count	Number of retransmitted packets	-
row_count	count	Session count including duplicates	-
send_packet_count	count	Number of transmitted packets	-
send_packet_size	byte	Total size of the transmitted packets	-
session_count	count	Session count excluding duplicates	The number of unique sessions is calculated as HyperLogLog⁽¹⁾ rather than a simple sum.
session_count_lobits	-	Bit data (HyperLogLog) for calculation of the unique session	It is HyperLogLog related information for statistical processing.
tot_jitter	ms	Sum of packet round-trip latency fluctuations	-

Field name	Unit	Description	Remarks
<code>tot_latency</code>	ms	Sum of packet round-trip latencies	-

❗ (1): **HyperLogLog** is a probabilistic data structure that estimates the number of elements in a set with very little memory.

npm_process_tag_list

This is internal data for processing foreign area tagging in the session.

- Tag lists for each session
- Collection interval: 1 minute

Field name	Description	Remarks
<code>foreign_app_name</code>	Custom identification value of the target	Default - A single Linux server environment: Host name - Kubernetes container environment: Pod name
<code>foreign_container_id</code>	ID of the container for local communication in the Kubernetes container	-
<code>foreign_container_name</code>	Container name in case the target is in the Kubernetes environment	-
<code>foreign_host_tag</code>	Target host name	-
<code>foreign_ip</code>	Target IP address	-
<code>foreign_pod_id</code>	Pod ID in case of local communication within a	-

Field name	Description	Remarks
	Kubernetes Pod	
foreign_pod_name	Pod name in case the communication target is in the Kubernetes environment	-
foreign_port	Target port number	-
foreign_process_type	Target process name	untagged if not identified
local_inbound_check	Checks whether the inbound communication works in the internal network.	-

Metrics Search

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

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

1

Metrics Search

Time selector

< 2023/08/17 07:57 ~ 2023/08/17 08:57 60Min >

Max count

100

Category

app_counter

2

Tags All

container

containerKey

hostIp

okindName

oname

onodeName

pid

type

8/8

Filter

Filter by tag value

Field All

_clock_delta

active_tx_0

active_tx_3

active_tx_8

active_tx_count

apdex_satisfied

apdex_tolerated

apdex_total

arrival_rate

httpc_count

httpc_error

httpc_time

meterlog

resp90

resp95

resp_time

sql_count

sql_error

sql_fetch_count

sql_fetch_time

sql_time

tps

tx_count

tx_doc_time

tx_error

tx_http_time

tx_sql_time

tx_time

tx_time_sql_sum

5/29

Download CSV

3

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

1 Time and category selection

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

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

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

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

2 Tag and field selection

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

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

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

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

 Among network performance metrics, the `npm_process_tag_data` and `npm_process_tag_list` categories do not provide the item, **Tag**.

3 Metrics table

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

-  • To search metrics, **Time selector** and **Category** must have been specified.
- To search metrics, **Tags** and **Field** are optional.
 - Among network performance metrics, the `npm_process_tag_data` and `npm_process_tag_list` categories do not provide the item, **Tag**.

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.

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.

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.

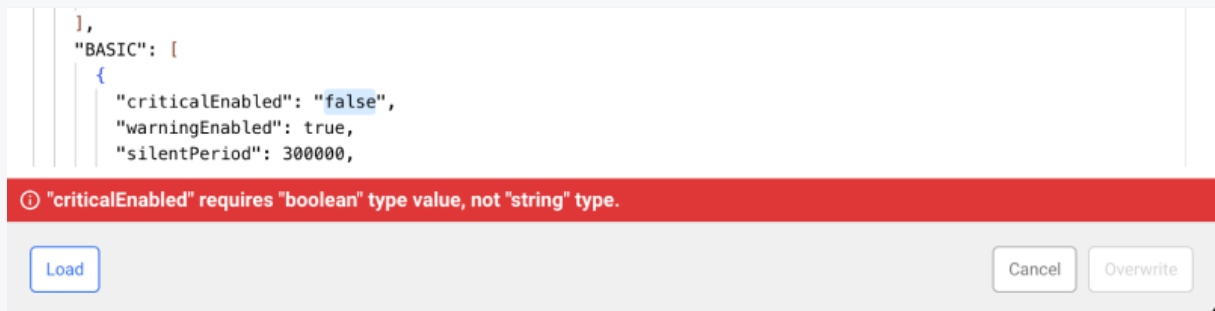
- **Batch JSON Edit:** Edit all event conditions in bulk using JSON format.
- **Batch JSON Download:** Save all currently registered event conditions as a JSON file.
- **Batch Excel Download:** Download the event list as an Excel file for external reporting or backup purposes.

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

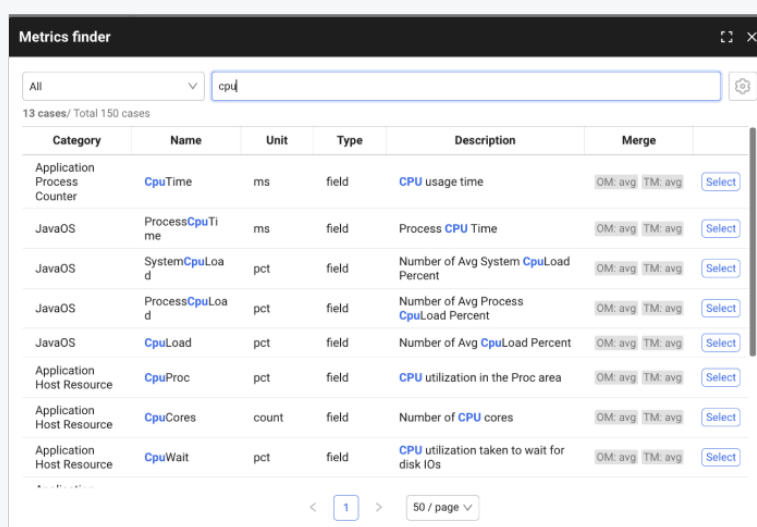
- Enter a category in the search field, or select a category (metric) from the category list. You must select a category to proceed with metric configuration.

- 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 )`)

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

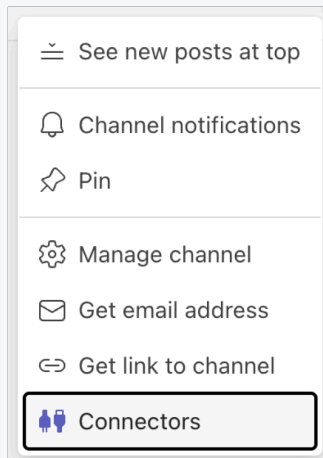


- `/remove` : Enter the project code for which you want to stop receiving alerts
- `/list` : View the list of project codes currently receiving alerts

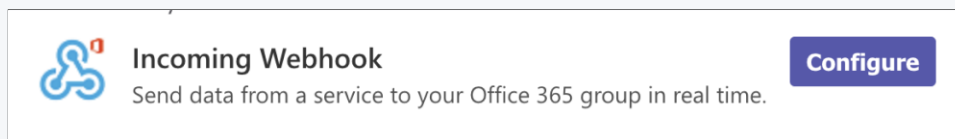
Teams



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

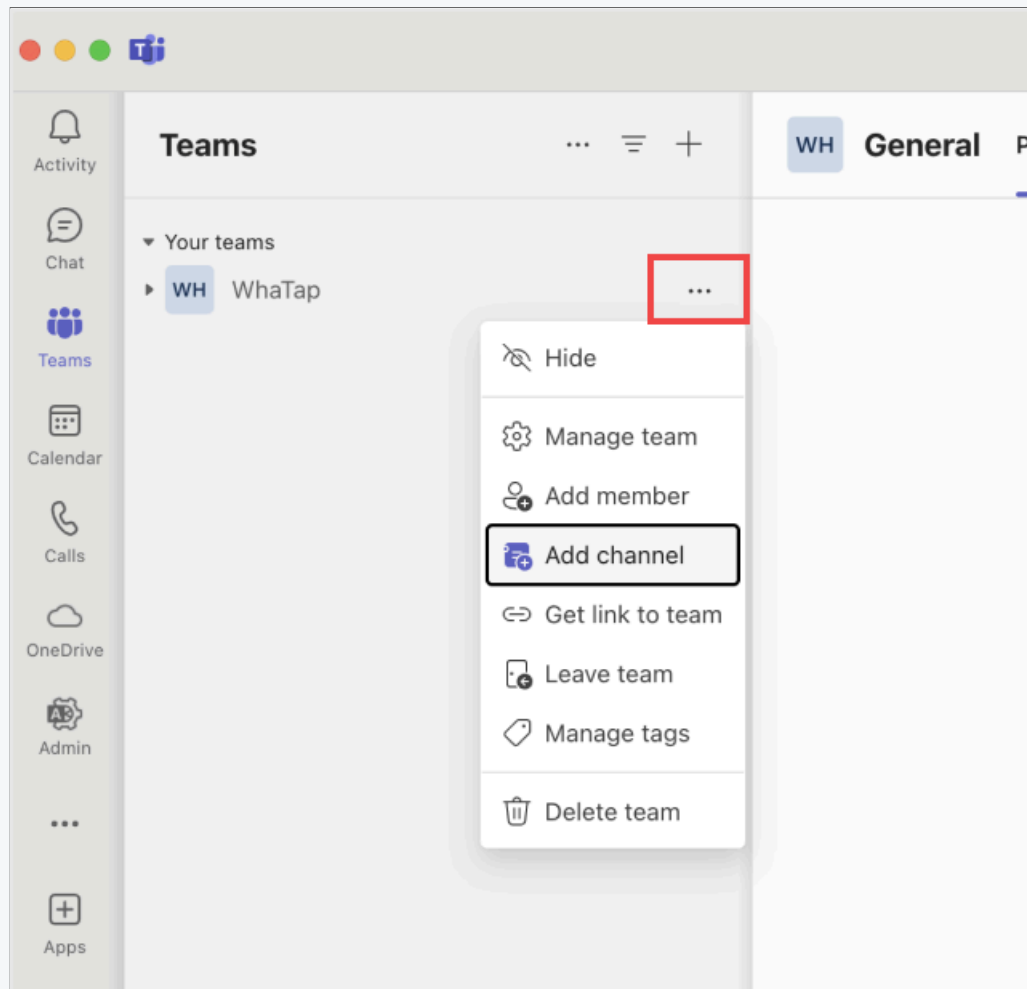
5. Return to the **Add a third-party plug-in** window in the WhaTap Monitoring service, and enter values for **Channel Name** and **Webhook URL** at the bottom of the **Teams** tab.
6. Click the [**Registration**] button.

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**.

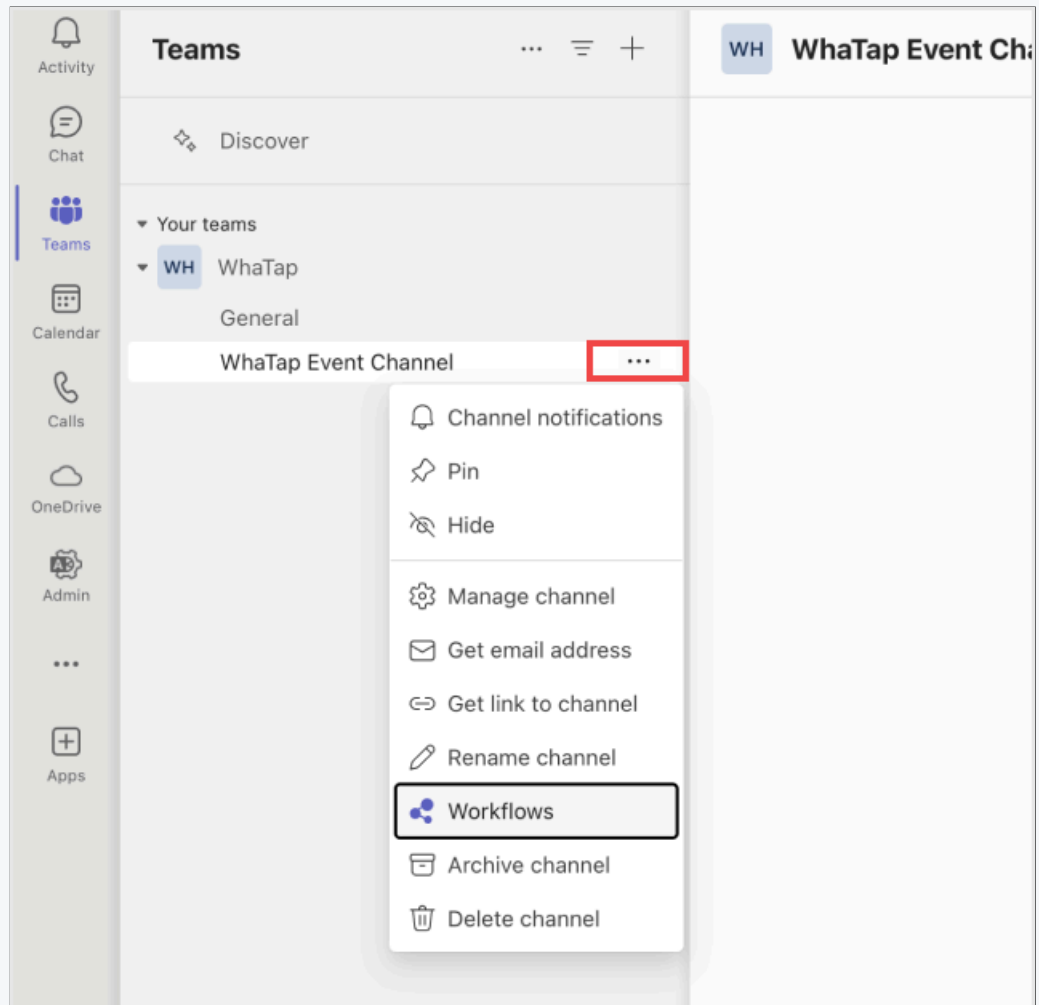


2. In the **Create a channel** window, enter the **Channel name** and **Description**. For **Channel type**, select **Standard**, then click the [Create] button.

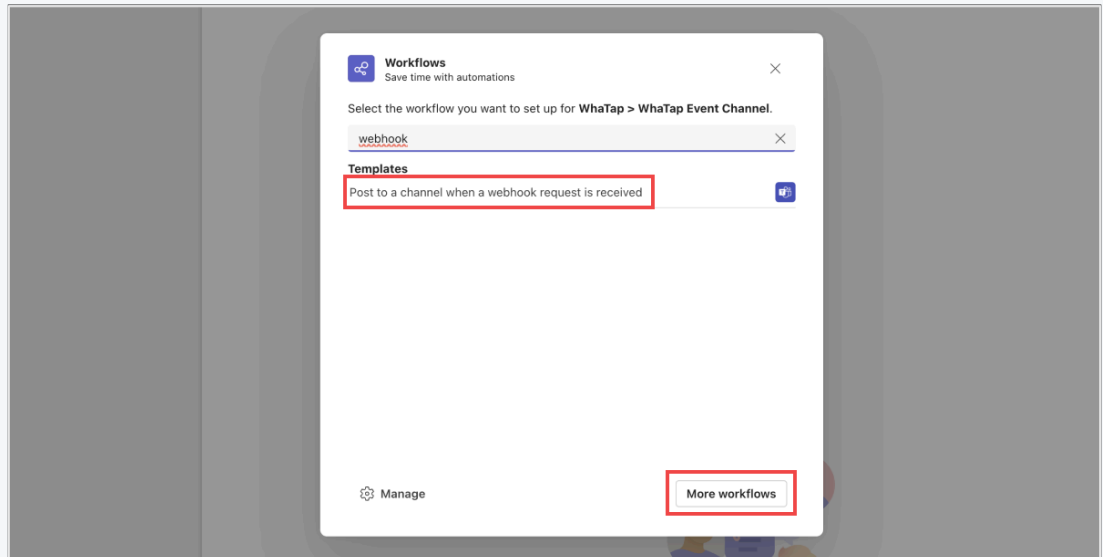


 If you select **Shared** as the channel type, workflows cannot be used. If you select **Private**, workflows can be added but notifications cannot be received.

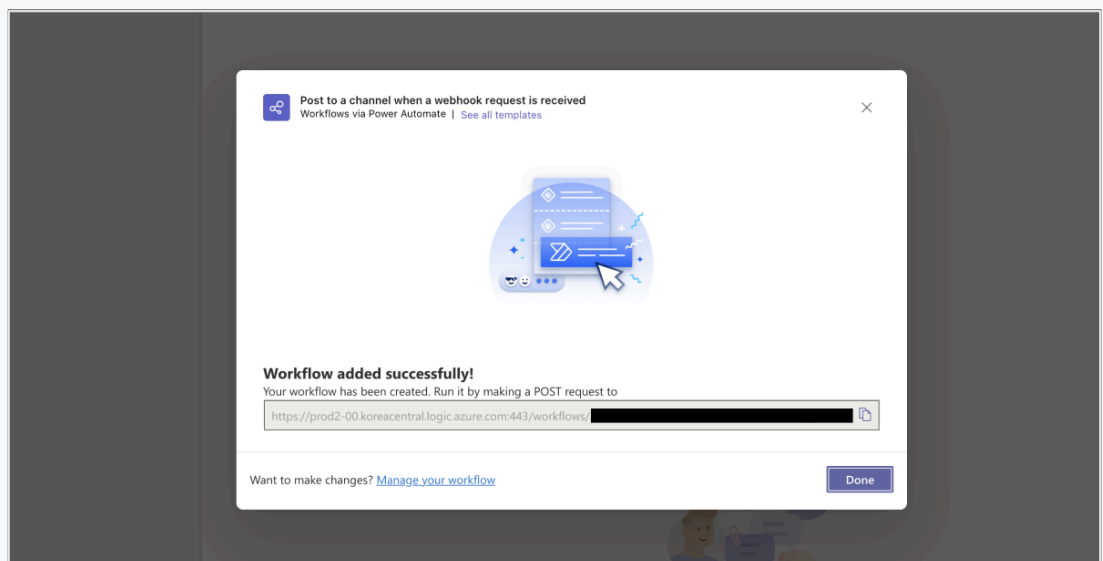
3. Click **More actions (...)** of the created channel, then select **Workflows**.



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.



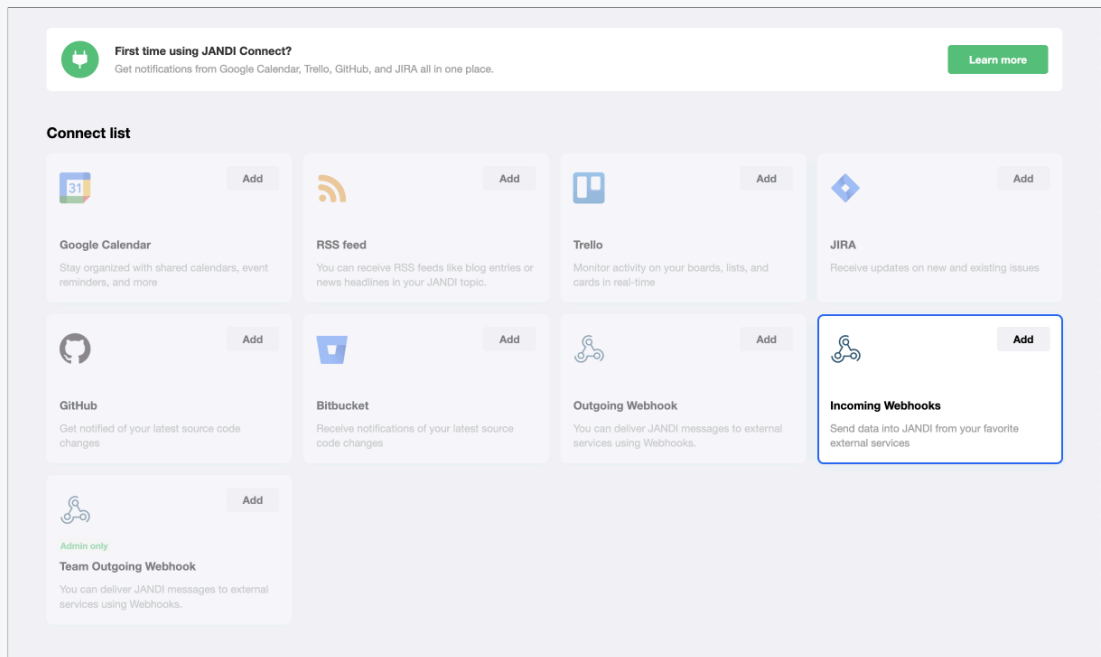
9. Click the [**Registration**] button.



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.

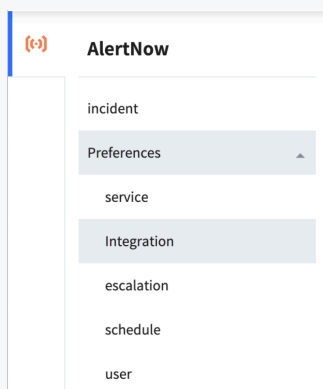
<https://wh.jandi.com/connect-api/webhook/31257583/d3...> Copy

- 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}",
}
```



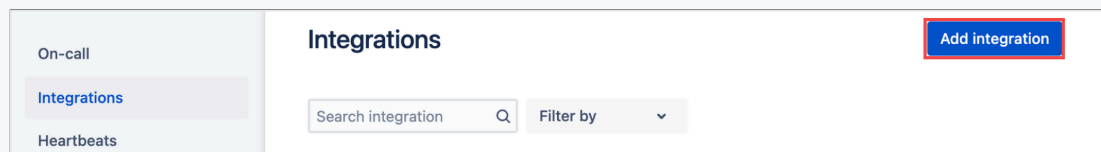
```
"metricName": "${metricName}",
"metricValue": "${metricValue}",
"metricThreshold": "${metricThreshold}",
"uuid": "${uuid}",
"okind": "${okind}",
"onode": "${onode}"
}
```

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.

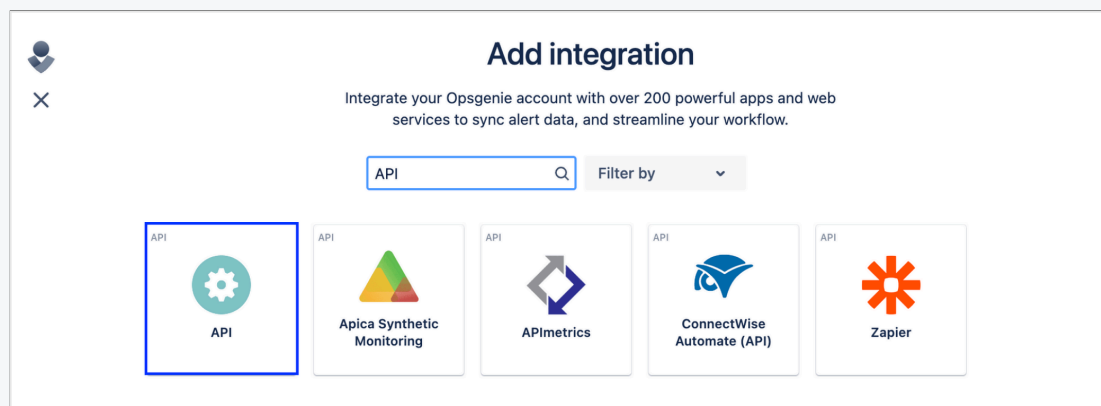
Opsgenie



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.

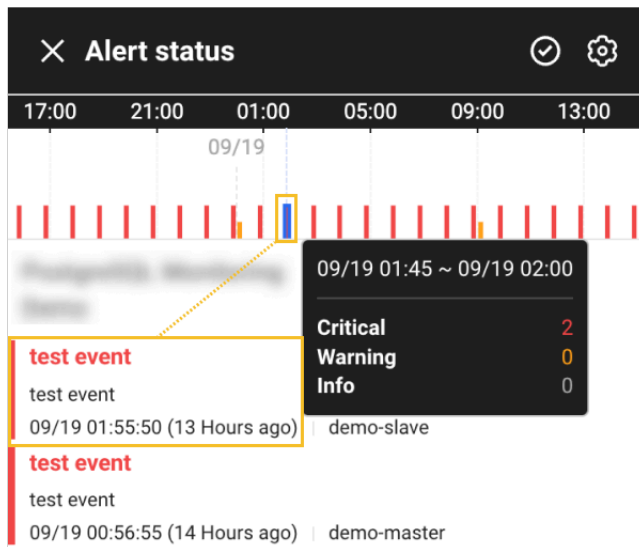
Viewing Real-time Notifications

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.

Laboratory

This menu provides new or experimental features to users. Through  **Laboratory** or **Sitemap** in the side menu, you can access it. The provided features may differ depending on the product.

 The functionality of the **Laboratory** menu is currently in Beta version and may cause unexpected errors. Be careful when using the **Laboratory** menu. It is not recommended to use the menu in handling important data or in the operating environment. If you have any feedback or issues, feel free to contact the support team at support@whatap.io.

- **Metrics Search**

You can search for specific metrics according to the categories based on fields and tags. For more information, see [the following](#).

 In the side menu, if the  **Laboratory** menu does not appear, you can access it through **Sitemap**. Under the side menu, select . If the **Sitemap** window appears, select a desired menu in the **Laboratory** section on the lower right of the window.