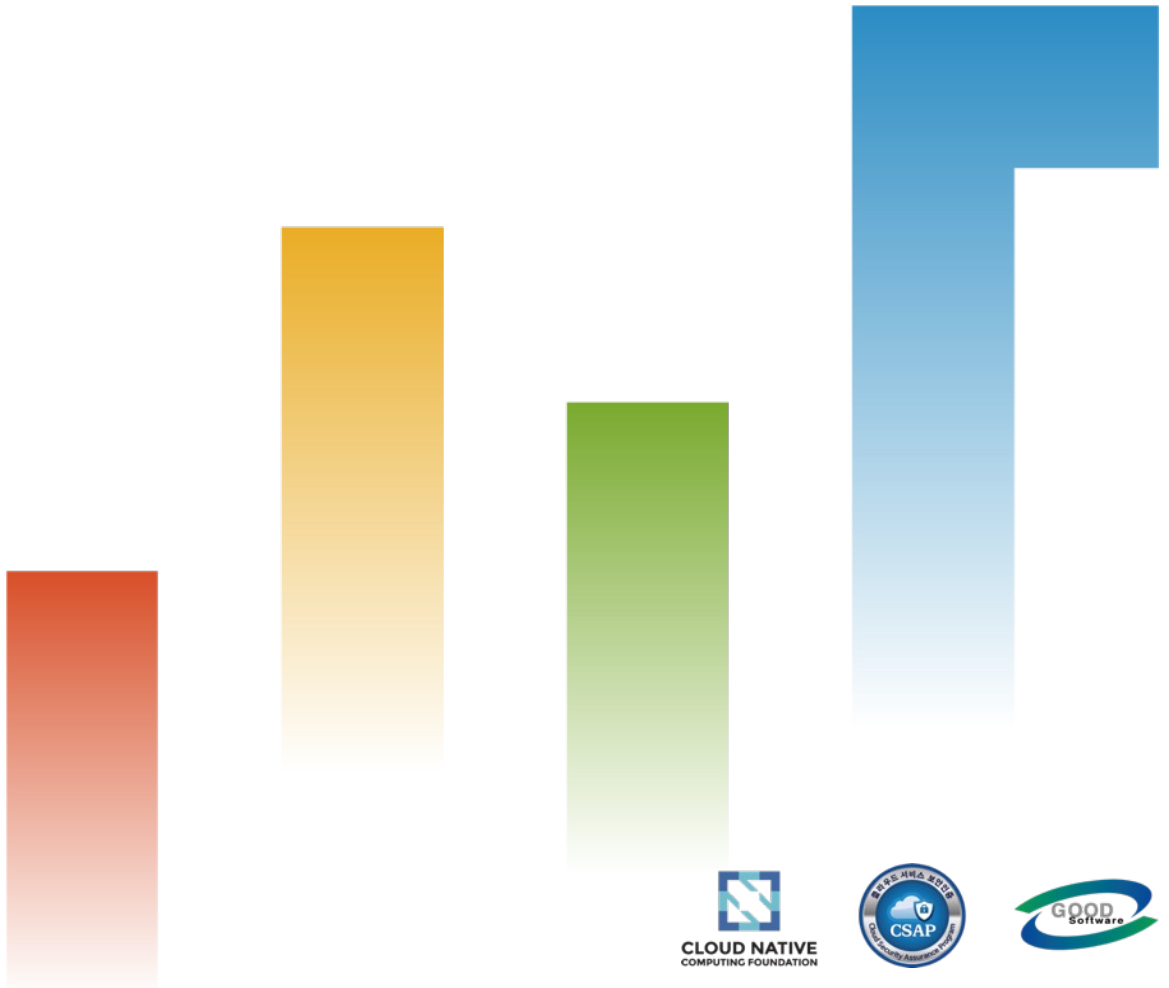


Server 모니터링

기술 문서 2024.04.02



Server 모니터링

와탭 서버 모니터링 서비스는 1분 이내 설치가 가능하며 실무자 관점으로 빠르게 적용할 수 있어 쉽게 모니터링 가능합니다. CPU, Disk I/O와 같이 순간적으로 임계 구간을 넘어설 수 있는 지표에 대해 5초 단위 수집으로 평균화 검출 방식의 한계를 극복합니다. 또한 20초 간격의 프로세스 모니터링을 제공합니다. 통합 모니터링을 위한 복수 대시보드를 제공하여 시스템 전체 현황 파악이 용이합니다. 클라우드 환경 모니터링에 적합한 지표를 제공하며 스케일아웃 환경에도 적용 가능합니다.

와탭 서버 모니터링 서비스를 활용하면 운영자 없이 서버를 안정적으로 운영할 수 있습니다.

주요 특징점

- **다양한 규모의 서버 모니터링**

통합 모니터링을 위한 다양한 유형의 대시보드를 제공하여, 시스템 전체 현황을 실시간으로 조망 가능합니다.

- **서버 인벤토리 관리**

관리 대상 서버 목록을 사용자가 표시하고 싶은 항목을 선택 가능한 테이블 형태로 제공하여, 중소 규모의 서버의 목록 관리 뿐만 아니라 실시간 모니터링도 가능합니다.

- **실시간 통합 알림**

자원 추이를 사용자가 모니터링하여 이상 지표를 검출해내야 하는 능동적 대처에서 자유로워지도록, 실시간 통합 알림 내역을 제공하여 알림 내역 기반으로 장애 대처가 가능하도록 지원합니다. 서버, 프로세스, 키워드 검출 방식의 알림을 제공합니다.

- **운영자를 위한 와탭 보고서**

다수의 자원을 안정적으로 운영해야 하는 운영자에게 있어 보고를 위한 자료를 수작업으로 만드는 일의 노고를 절감하고자, 다양한 유형의 보고서를 제공합니다. 사용자가 필요로 하는 보고서가 있다면, 피드백 기반으로 보고서 유형을 추가하여 제공합니다.

- **클라우드 성능 취약점 감지**

클라우드 환경 애플리케이션에서 발생할 수 있는 취약점에 대한 자동 감지와 알림 기능을 제공합니다.

- **적정 수준의 시스템 규모 판단 가능**

매년 필요한 서버의 규모는 다릅니다. 클라우드를 사용하고 있다면 이는 매월, 매주에서 실시간으로 달라질 수도 있습니다. 이를 모니터링을 통해 예측하고, 적정 수준의 규모를 산정합니다.

- **프로세스 성능 자동 수집**

자동으로 모든 프로세스의 CPU, 메모리, IO 사용량을 20초 단위로 수집합니다.

- **멀티 채널 및 개인화 알림**

이메일, SMS, 3rd Party Plugin을 이용한 개인화된 알림 서비스를 제공합니다.

- **클라우드, 물리 서버, Hybrid 환경까지**

물리 서버를 넘어서 클라우드 환경 모니터링에 적합한 지표를 제공하며, 스케일아웃 환경에도 적용 가능합니다.

지원 환경

운영체제별 지원 환경

와탭 서버 모니터링 에이전트를 설치하기 전에 지원 환경을 확인하세요. X86 기반에서 동작하는 **Linux, FreeBSD, Windows** 에 적용할 수 있습니다.

- **Linux**
 - CentOS 5 이상
 - Red Hat Server 5.0 이상(RHEL 또는 RHEL 기반 배포 버전 지원)
 - Rocky Linux 8.6 이상
 - SUSE 10.1 이상
 - Amazon Linux 모든 버전
 - Ubuntu 12.04 이상
 - Debian 6.0 이상
 - XenServer 6.0 이상
- **Unix**
 - FreeBSD 10 이상
- **Windows**
 - Windows 2008 R2 이상
 - Windows 7 SP1 버전 이상

① 지원 리스트에 포함되지 않는 환경이라면 support@whatap.io로 문의해 주세요.

브라우저 지원

와탭 모니터링 서비스는 웹브라우저와 모바일 앱에서 이용할 수 있습니다.

브라우저	권장여부	지원버전
Google Chrome	O	84 이상
Mozilla FireFox	X	최신 버전
Edge	X	최신 버전
Safari	X	최신 버전

- ① • 브라우저 호환성과 성능을 이유로 Chrome 최신 버전 사용을 권장합니다.
- 사용자 인터페이스(User Interface, UI)는 HTML5 표준 기술로 구현하여 Internet Explorer는 지원하지 않습니다.

방화벽

와탭 에이전트는 수집 서버 **TCP 6600** 포트로 접속 가능해야 합니다. 모니터링 대상과 가까운 수집 서버 주소를 허용하세요.

출발지: 와탭 에이전트

목적지	목적지 IP	포트
와탭 서울 수집 서버	13.124.11.223 / 13.209.172.35	TCP 6600
와탭 도쿄 수집 서버	52.68.36.166 / 52.193.60.176	TCP 6600


목적지	목적지 IP	포트
와탭 싱가포르 수집 서버	18.138.0.93 / 18.139.67.236	TCP 6600
와탭 뭄바이 수집 서버	13.127.125.69 / 13.235.15.118	TCP 6600
와탭 캘리포니아 수집 서버	52.8.223.130 / 52.8.239.99	TCP 6600
와탭 프랑크푸르트 수집 서버	3.125.142.162 / 3.127.76.140	TCP 6600

에이전트에서 수집 서버로 직접 접속할 수 없다면 제공하는 Proxy 모듈을 이용해 경유하세요.

Proxy

모바일 앱

와탭 모바일 앱은 안드로이드와 iOS 환경을 지원합니다. 다음 링크로 이동하거나 QR 코드를 스캔해 앱을 설치할 수 있습니다. 모바일 앱에 대한 자세한 설명은 [다음 문서](#)를 참조하세요.

iOS	Android
 <p>iOS 12 버전 이상</p>	 <p>Android 5.0 버전 이상</p>

설치하기

와탭 서버 모니터링 서비스 이용을 위한 기본 설치 방법을 안내합니다.

와탭 모니터링 서비스를 사용하기 위해서는 [회원 가입](#) 후 프로젝트를 생성하고 대상 서버에 에이전트를 설치해야 합니다. 회원 가입에 관한 자세한 내용은 [다음 문서](#)를 참조하세요.

다음 동영상 가이드를 참조하세요.

프로젝트 생성하기

에이전트를 설치하기 전에 먼저 프로젝트를 생성하세요.

1. [와탭 모니터링 서비스](#)로 이동한 다음 로그인하세요.
2. 프로젝트를 생성하려면 화면 왼쪽 사이드 메뉴에서 [전체 프로젝트](#) > [+ 프로젝트](#) 버튼을 선택하세요.
3. [상품 선택](#) 화면에서 프로젝트에 설치할 상품을 선택하세요.
4. [프로젝트 이름](#), [데이터 서버 지역](#), [타임 존](#) 등의 항목을 차례로 설정하세요.

프로젝트 이름 *

프로젝트 이름을(를) 입력해주세요

데이터 서버 지역 * AWS demo Azure Kakao Huawei 가까운 지역의 서버를 선택하세요 ▼

데이터 서버 지역을(를) 선택해주세요

데이터 서버 지역은 리전(클라우드 서비스를 제공하기 위해 설치한 데이터 센터의 묶음)을 의미합니다. 특정 리전을 선택하면 해당 리전에 속해있는 데이터 센터에 사용자의 데이터가 저장됩니다.

타임 존 * (GMT +9:00) Seoul, Tokyo, Yakutsk ▼

타임존은 알림, 보고서를 생성할 시 기준시간이 됩니다.

프로젝트 그룹 그룹 없음 ▼ ➕ 그룹 추가

여러개의 프로젝트를 그룹으로 묶어서 관리할 수 있습니다. 생성할 프로젝트가 속할 그룹이 있으면 선택해주세요.

프로젝트 설명

5. 모든 설정을 완료한 다음에는 [프로젝트 생성하기](#) 버튼을 선택하세요.

ⓘ • [데이터 서버 지역](#)은 리전(클라우드 서비스를 제공하기 위해 설치한 데이터 센터의 묶음)을 의미합니다. 특정 리전을

- ① 선택하면 해당 리전에 속한 데이터 센터에 사용자의 데이터를 저장합니다.
 - **타임 존**은 알림, 보고서를 생성하는 기준 시간입니다.
 - 여러 개의 프로젝트를 그룹으로 묶어 관리하려면 **프로젝트 그룹**에서 그룹을 선택하거나 그룹을 추가하세요. 그룹에 대한 자세한 설명은 **다음 문서**를 참조하세요.
 - 조직을 선택한 상태에서 프로젝트를 추가할 경우 **조직 하위 그룹**을 필수로 설정해야 합니다.

프로젝트 액세스 키 확인

프로젝트 액세스 키는 와탭 서비스 활성화를 위한 고유 ID입니다.

설치 안내 섹션에서 **프로젝트 액세스 키 발급받기** 버튼을 선택하세요. **프로젝트 액세스 키**를 자동으로 발급 받은 후 다음 단계를 진행합니다.

- ✔ 프로젝트를 생성한 다음에는 자동으로 **에이전트 설치** 페이지로 이동합니다. **에이전트 설치** 페이지로 이동하지 않는다면 왼쪽 메뉴에서 **전체 프로젝트**를 선택한 다음 새로 생성한 프로젝트를 선택하세요.

환경별 에이전트 설치

> 서버 에이전트 파일 구성

- **공통 파일**
 - **ChangeLog.txt**: 에이전트 변경 내역입니다.
 - **whatap.conf**: 서버의 데이터를 수집할 서버의 주소와 서버의 프로젝트 액세스 키가 입력되는 파일입니다.
- **Linux/FreeBSD**
 - **whatap_infrad**: 데이터 수집 및 전송용 에이전트입니다.
 - **whatap_infrad.pid**: 실행 중인 에이전트의 PID 값을 기록한 파일입니다.
 - **VERSION**: 현재 설치된 에이전트의 버전이 기록된 파일입니다.
- **Windows**
 - **whatap_infra.exe**: 데이터 수집 및 전송용 에이전트입니다.
 - **unins000**: 에이전트 삭제 파일입니다.

- [whatap.ico](#): 와탭 인프라의 아이콘 이미지입니다.

프로젝트 생성과 프로젝트 액세스 키 확인은 공통 과정입니다.

사용하는 환경에 따른 설치 방법을 다음과 같이 제공합니다. 에이전트를 설치하고 적용하기 전에 [지원 환경](#)을 먼저 확인하세요.

Linux 및 Unix

Linux와 Unix 환경에서 와탭 서버 모니터링 에이전트를 설치하는 방법을 제공합니다.

AIX

AIX 환경에서 에이전트를 설치하는 방법을 제공합니다.

Windows

Windows 환경에서 와탭 서버 모니터링 에이전트를 설치하는 방법을 제공합니다.

서버 컴퓨터 이외의 경우

서버 컴퓨터가 아닌 환경에서 와탭 서버 모니터링 에이전트를 설치하는 방법을 제공합니다.

Elastic Beanstalk

Elastic Beanstalk 환경에서 와탭 서버 모니터링 에이전트를 설치하는 방법을 제공합니다.

Linux 및 Unix

신규 생성한 서버 모니터링 프로젝트를 선택하면 [에이전트 설치](#) 화면이 나타납니다. 프로젝트 [관리](#) > [에이전트 설치](#) 메뉴를 통해서도 가능합니다.

에이전트 설치

Debian/Ubuntu RedHat Amazon Linux Windows SUSE FreeBSD XenServer

1



Debian/Ubuntu

지원 버전: Debian 7.0/Ubuntu 12.04 이상

WhaTap Server 15.165.146.117로 데이터 전송을 위해 6600 포트가 열려 있어야 합니다. (TCP Outbound)

설치 안내

▼ 펼치기

🔍 채널 문의

📺 영상 가이드

▶ 1. 프로젝트 액세스 키 확인

▼ 2. 와탭 리포지토리 추가

2

와탭 리포지토리 구성을 위해 아래 명령어를 실행하세요.

```
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
```

복사

▼ 3. 와탭 서버 모니터링 패키지 설치

3

와탭 서버 모니터링 패키지 설치를 위해 아래 명령어를 실행하세요.

```
sudo apt-get install whatap-infra
```

복사

▼ 4. 서버 모니터링 시작하기

4

설정 스크립트를 실행하여 와탭 서버 모니터링을 시작합니다.

▼ 일반 설치

```
echo "license=x463v23ua3jf1-x2mkoluc0fcbq2-x4g8145u0ov2h4" |sudo tee /usr/whatap/infra/conf/whatap.conf
echo "whatap.server.host=127.0.0.1" |sudo tee -a /usr/whatap/infra/conf/whatap.conf
echo "createdtime=`date +%s%N`" |sudo tee -a /usr/whatap/infra/conf/whatap.conf
sudo service whatap-infra restart
```

복사

▶ AWS Elastic Beanstalk



1. 와탭 리포지토리를 등록하세요.

1 관리 > 에이전트 설치 화면 상단 영역의 OS 탭에서 서버 OS를 선택하세요. 2 와탭 리포지토리 추가 탭에서 해당하는 명령어를 복사하여 입력합니다.

Debian / Ubuntu

CentOS

Amazon Linux

SH

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

SH

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

SH

```
sudo rpm --import http://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=http://repo.whatap.io/centos/latest/\$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
```

SUSE

FreeBSD

XenServer

SH

```
sudo rpm --import http://repo.whatap.io/suse/release.gpg
echo "[whatap]" | sudo tee /etc/zypp/repos.d/whatap.repo > /dev/null
echo "name=whatap packages for enterprise linux" | sudo tee -a /etc/zypp/repos.d/whatap.repo > /dev/null
echo "baseurl=http://repo.whatap.io/suse/12/x86_64" | sudo tee -a /etc/zypp/repos.d/whatap.repo > /dev/null
echo "enabled=1" | sudo tee -a /etc/zypp/repos.d/whatap.repo > /dev/null
echo "gpgcheck=1" | sudo tee -a /etc/zypp/repos.d/whatap.repo > /dev/null
```

```
sudo zypper refresh
```

```
SH
```

```
wget http://repo.whatap.io/freebsd/10/whatap-infra.txz
```

```
SH
```

```
sudo rpm --import http://repo.whatap.io/centos/release.gpg
sudo rpm -Uvh http://repo.whatap.io/centos/python/5/noarch/whatap-repo-1.0-1.noarch.rpm
```

2. 다음 명령어를 통해 **패키지**를 설치하세요.

3 와탭 서버 모니터링 패치 설치 탭에서 해당하는 명령어를 복사해 입력합니다.

[Debian / Ubuntu](#)

[SUSE](#)

[FreeBSD](#)

[CentOS / Amazon Linux / XenServer](#)

```
SH
```

```
sudo apt-get install whatap-infra
```

```
SH
```

```
sudo zypper install whatap-infra
```

```
SH
```

```
pkg install whatap-infra.txz
```

```
SH
```

```
sudo yum install whatap-infra
```

3. 설정 스크립트를 실행하세요.

4 서버 모니터링 시작하기 탭으로 이동해 명령어를 발급받거나, 하단의 명령어에 프로젝트 액세스 키와 서버 IP를 추가해

실행하세요.

```
echo "license=[발급된 프로젝트 액세스 키]" | sudo tee /usr/whatap/infra/conf/whatap.conf
echo "whatap.server.host=[활당된 와탭 서버 IP]" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
echo "createdtime= `date +%s%N`" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
sudo service whatap-infra restart
```

ⓘ 주의 사항

데이터 전송을 위해 TCP 아웃바운드 **6600 PORT**가 열려 있어야 합니다.

> 서버 에이전트 파일 구성

• 공통 파일

- **ChangeLog.txt**: 에이전트 변경 내역입니다.
- **whatap.conf**: 서버의 데이터를 수집할 서버의 주소와 서버의 프로젝트 액세스 키가 입력되는 파일입니다.

• Linux/FreeBSD

- **whatap_infrad**: 데이터 수집 및 전송용 에이전트입니다.
- **whatap_infrad.pid**: 실행 중인 에이전트의 PID 값을 기록한 파일입니다.
- **VERSION**: 현재 설치된 에이전트의 버전이 기록된 파일입니다.

AIX

! AIX 6.X 버전 이상부터 지원합니다.

신규 생성한 서버 모니터링 프로젝트를 선택하면 [에이전트 설치](#) 화면이 나타납니다. 프로젝트 [관리](#) > [에이전트 설치](#) 메뉴를 통해서도 가능합니다.

1. [관리](#) > [에이전트 설치](#) 화면 상단 영역의 ① OS 탭에서 [AIX](#)를 선택하세요.
2. ② [설치 파일 다운로드](#) 탭에서 [whatap-infra-latest.noarch.rpm](#) 버튼을 선택해 에이전트 설치 파일을 다운로드하세요.
3. ③ [설치 파일 실행](#) 탭으로 이동해 다음의 실행 명령어를 확인 후 패키지를 실행하세요.

```
rpm -Uvh whatap-infra-latest.noarch.rpm
```

! 서버 보안을 위해 [설치 파일](#)은 다운로드 형식으로만 제공합니다.

에이전트 실행

다음 명령어를 실행해 서버 모니터링을 시작하세요. 애플리케이션 서버가 실행되면 에이전트가 모니터링 정보를 수집하기 시작합니다.

```
echo "license=x4t2322hcqshs-x1q9rv0b9rjvs6-x4jnrqfl5ce5g" | tee /usr/whatap/infra/conf/whatap.conf
echo "whatap.server.host=127.0.0.1" | tee -a /usr/whatap/infra/conf/whatap.conf
echo "createdtime=date +%s%S" | tee -a /usr/whatap/infra/conf/whatap.conf
stopsrc -s whatap-infra
startsrc -s whatap-infra
```

Windows

신규 생성한 서버 모니터링 프로젝트를 선택하면 [에이전트 설치](#) 화면이 나타납니다. 프로젝트 [관리](#) > [에이전트 설치](#) 메뉴를 통해서도 가능합니다.

Debian/Ubuntu RedHat Amazon Linux **Windows** SUSE FreeBSD XenServer

Windows

지원 버전: Windows 2008 Sp2 이상
 WhaTap Server 15.165.146.117로 데이터 전송을 위해 6600 포트가 열려 있어야 합니다. (TCP Outbound)

설치 안내
[펼치기](#) [채널 문의](#) [영상 가이드](#)

▶ 1. 프로젝트 액세스 키 확인

▼ 2. 설치 파일 다운로드 2

프로젝트 액세스 키를 발급받은 경우에만 설치 파일 다운로드가 가능합니다.

whatap_infra.exe
whatap_infra.zip
Silent Install

링크를 클릭하시면 윈도우 서버 운영체제용 설치 파일 (whatap.exe / whatap.zip) 가 다운로드 됩니다.
 보안 설정으로 인해 .exe 형식의 파일이 받아지지 않는 사용자를 위해 .zip 형식의 파일도 함께 제공됩니다.
 * 서버 보안을 위해 브라우저를 통한 직접 설치 보다 다운로드 받은 설치 파일을 실행하시는 것을 권장합니다.

▼ 3. 설치 파일 실행 3

설치 파일을 더블클릭 하고 화면의 안내에 따라 프로젝트 액세스 키를 입력합니다.

프로젝트 액세스 키

x463v23ua3jf1-x2mkoluc0fcbq2-x4g8145u0ov2h4
복사

WhaTap IP

127.0.0.1
복사

1. 에이전트 파일을 다운로드하세요.

관리 > 에이전트 설치 화면 상단 영역의 ❶ OS 탭에서 서버 OS를 선택하세요. ❷ 설치 파일 다운로드 탭에서 `whatap_infra.exe` 혹은 `whatap_infra.zip` 버튼을 선택해 에이전트 설치 파일을 다운로드 하세요.

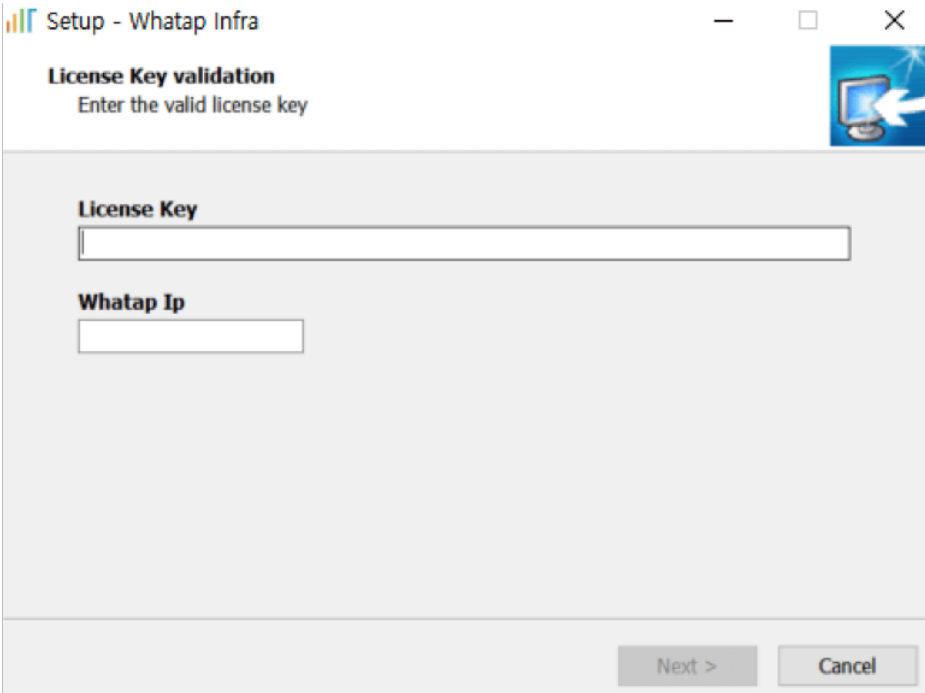
- ❗ • 보안 설정으로 인해 .exe 형식의 파일이 받아지지 않는 사용자를 위해 .zip 형식의 파일도 함께 제공합니다.
- 서버 보안을 위해 브라우저를 통한 직접 설치 보다 다운로드 받은 설치 파일을 실행하는 것을 권장합니다.

2. 모니터링 대상 서버에 접속해 에이전트 파일을 업로드 하세요.

3. 다운로드한 설치 파일을 두 번 클릭해 실행하세요.

4. ❸ 설치 파일 실행 탭으로 이동하여 발급받은 프로젝트 액세스 키와 서버 IP를 확인하세요.

5. 화면의 안내에 따라 License Key 항목에는 프로젝트 액세스 키를, WhaTap IP 항목에는 와탭 서버의 IP 주소를 입력하세요.



Setup - Whatap Infra

License Key validation
Enter the valid license key

License Key

Whatap Ip

Next > Cancel

6. Next 버튼을 클릭하세요.

7. 다음 화면에서 Install 버튼을 클릭하세요. 설치를 진행합니다.

8. Finish 버튼을 클릭해 설치를 완료하세요.

> 서버 에이전트 파일 구성

- **공통 파일**

- [ChangeLog.txt](#): 에이전트 변경 내역입니다.
- [whatap.conf](#): 서버의 데이터를 수집할 서버의 주소와 서버의 프로젝트 액세스 키가 입력되는 파일입니다.

- **Windows**

- [whatap_infra.exe](#): 데이터 수집 및 전송용 에이전트입니다.
- [unins000.](#): 에이전트 삭제 파일입니다.
- [whatap.ico](#): 와탭 인프라의 아이콘 이미지입니다.

서버 컴퓨터 이외의 경우

노트북과 같이 서버 컴퓨터가 아닌 개인용 컴퓨터 및 와이파이를 사용하는 환경에서는 다음 옵션을 적용하세요.

- Linux
- Windows

```
SH
echo "ipreg=false" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
sudo service whatap-infra restart
```

```
SH
// 관리자 권한 파워셸에서 다음 명령을 실행하세요.
Add-Content "c:\Program Files\WhatapInfra\whatap.conf" "ipreg=false"
Restart-Service "Whatap Infra"
```

ⓘ IP가 변경될 때마다 자동으로 다시 등록되지 않아 편리하게 사용할 수 있습니다.

Elastic Beanstalk

Elastic Beanstalk를 이용해 배포할 경우 와탭 에이전트를 적용하는 방법입니다.

- Linux 설치 환경에 따라 다음의 내용을 Elastic Beanstalk **설치 스크립트**에 추가하세요.

! whatap.server.host 와 license 즉 프로젝트 액세스 키는 사용자에게 맞게 입력합니다.

Debian / Ubuntu

CentOS

Amazon Linux

```
wget http://repo.whatap.io/debian/release.gpg -O - | sudo apt-key add -
wget http://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-infra
echo "license={LICENSE_INFO}" | sudo tee /usr/whatap/infra/conf/whatap.conf
echo "whatap.server.host={HOST_IP}" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
echo "createdtime=`date +%s%N`" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
sudo service whatap-infra restart
```

```
sudo rpm --import http://repo.whatap.io/centos/release.gpg
sudo rpm -Uvh http://repo.whatap.io/centos/5/noarch/whatap-repo-1.0-1.noarch.rpm
sudo yum install whatap-infra
echo "license={LICENSE_INFO}" | sudo tee /usr/whatap/infra/conf/whatap.conf
echo "whatap.server.host={HOST_IP}" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
echo "createdtime=`date +%s%N`" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
sudo service whatap-infra restart
```

```
sudo rpm --import http://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=http://repo.whatap.io/centos/latest/`$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-infra
echo "license={LICENSE_INFO}" | sudo tee /usr/whatap/infra/conf/whatap.conf
echo "whatap.server.host={HOST_IP}" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
echo "createdtime=date +%s%N" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

```
sudo service whatap-infra restart
```

SUSE

FreeBSD

XenServer

```
sudo rpm --import http://repo.whatap.io/suse/release.gpg
echo "[whatap]" | sudo tee /etc/zypp/repos.d/whatap.repo > /dev/null
echo "name=whatap packages for enterprise linux" | sudo tee -a /etc/zypp/repos.d/whatap.repo > /dev/null
echo "baseurl=http://repo.whatap.io/suse/12/x86_64" | sudo tee -a /etc/zypp/repos.d/whatap.repo > /dev/null
echo "enabled=1" | sudo tee -a /etc/zypp/repos.d/whatap.repo > /dev/null
echo "gpgcheck=1" | sudo tee -a /etc/zypp/repos.d/whatap.repo > /dev/null
sudo zypper refresh
sudo zypper install whatap-infra
echo "license={LICENSE_INFO}" | sudo tee /usr/whatap/infra/conf/whatap.conf
echo "whatap.server.host={HOST_IP}" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
echo "createdtime=`date +%s%N`" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
sudo /etc/init.d/whatap-infra restart
```

```
wget http://repo.whatap.io/freebsd/10/whatap-infra.txz
pkg install whatap-infra.txz
echo "license={LICENSE_INFO}" | tee /usr/whatap/infra/conf/whatap.conf
echo "whatap.server.host={HOST_IP}" | tee -a /usr/whatap/infra/conf/whatap.conf
echo "createdtime=`date +%s%N`" | tee -a /usr/whatap/infra/conf/whatap.conf
service whatap_infra restart
```

```
sudo rpm --import http://repo.whatap.io/centos/release.gpg
sudo rpm -Uvh http://repo.whatap.io/centos/python/5/noarch/whatap-repo-1.0-1.noarch.rpm
sudo yum install whatap-infra
echo "license={LICENSE_INFO}" | sudo tee /usr/whatap/infra/conf/whatap.conf
echo "whatap.server.host={HOST_IP}" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
echo "createdtime=`date +%s%N`" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
sudo service whatap_infra restart
```

2. 다음 명령어를 수정하세요.

```
echo "createdtime=date +%s%N" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

설치 후 서버 모니터링을 Beanstalk에 포함해 애플리케이션 배포 시 서버 모니터링 신규 목록이 반복적으로 생성될 수 있습니다.

와탭 에이전트 내부 아이디가 위의 명령이 실행될 때마다 새로 발급되기 때문입니다. 추후 배포 시 신규 목록이 추가로 발생하지 않도록 다음과 같이 수정하세요.

```
echo "createdtime=12345678" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

설치 점검 사항

서버 모니터링 설치를 모두 완료했습니다. 설치 후 확인 사항을 점검하세요.

Linux 및 Unix

로그 출력 확인

에이전트가 정상적으로 설치되면 다음과 같은 로그 출력을 확인하실 수 있습니다. 성공적으로 접속이 되면 connected 문구가 표시됩니다.

[Debian/Ubuntu/SUSE](#)
[CentOS/Amazon Linux/Unix](#)

SH

```
tail -10 /var/log/syslog
```

```
...
Apr 8 16:28:08 localhost systemd[1]: Started LSB: Start whatap-infra daemon.
Apr 8 16:28:08 localhost whatap_infrad[32468]: 2019/04/08 16:28:08 Config file : /usr/whatap/infra/conf/whatap.conf
Apr 8 16:28:08 localhost whatap_infrad[32468]: 2019/04/08 16:28:08 OID: 1193741647 ONAME: localhost
Apr 8 16:28:08 localhost whatap_infrad[32468]: 2019/04/08 16:28:08 connected to {whatap ip}:{whatap port}
```

SH

```
tail -10 /var/log/messages
```

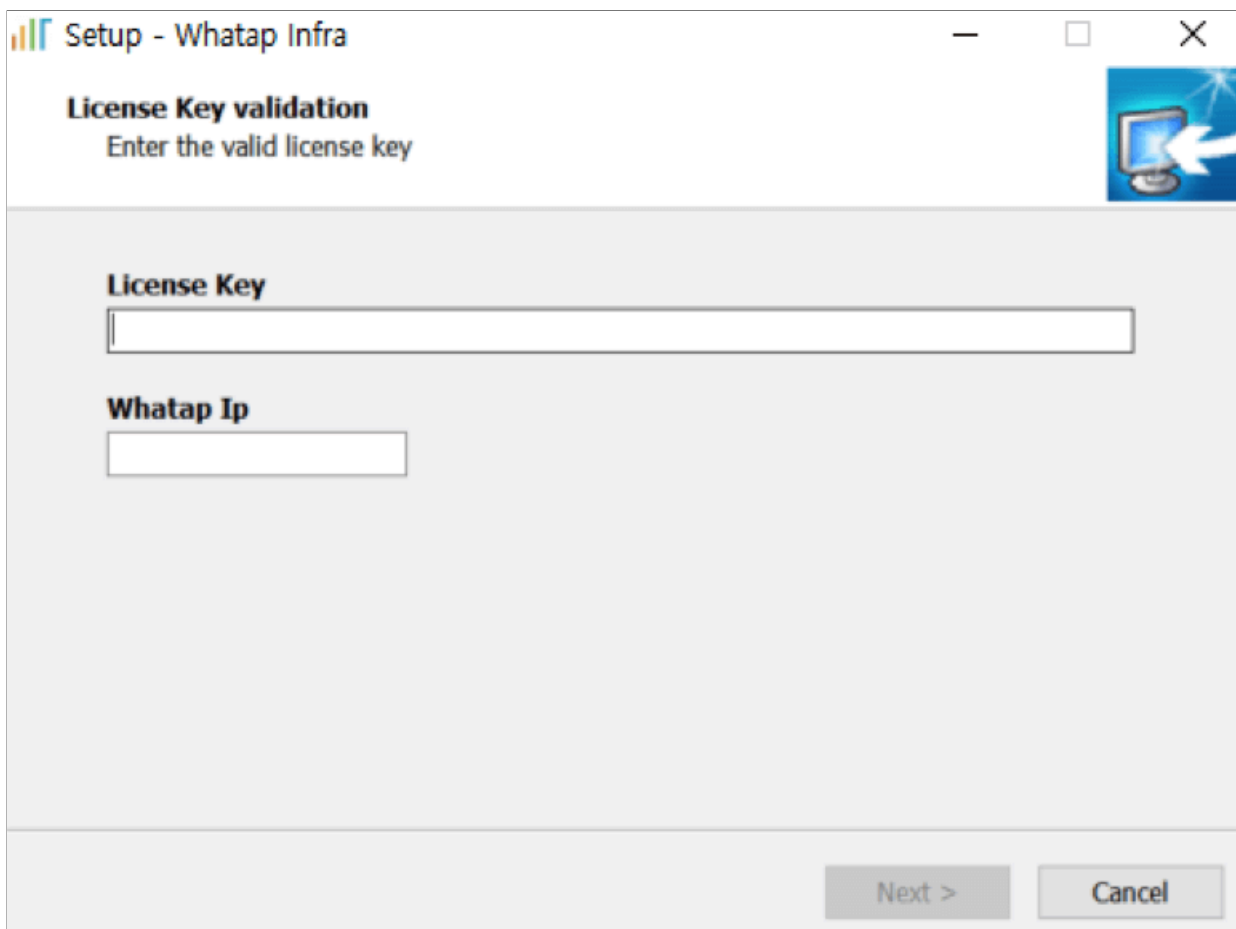
```
...
Apr 8 16:28:08 localhost systemd[1]: Started LSB: Start whatap-infra daemon.
Apr 8 16:28:08 localhost whatap_infrad[32468]: 2019/04/08 16:28:08 Config file : /usr/whatap/infra/conf/whatap.conf
Apr 8 16:28:08 localhost whatap_infrad[32468]: 2019/04/08 16:28:08 OID: 1193741647 ONAME: localhost
Apr 8 16:28:08 localhost whatap_infrad[32468]: 2019/04/08 16:28:08 connected to {whatap ip}:{whatap port}
```

방화벽 설정 및 네트워크 설정 확인

접속이 되지 않으면 방화벽 설정을 포함해 네트워크 설정을 확인하세요. 네트워크 설정이 반영되면 에이전트는 자동 접속됩니다.

Windows

정상적으로 설치가 완료된 경우 설치 최종 단계에서 다음과 같은 화면을 볼 수 있습니다. 에이전트가 자동으로 모니터링을 시작합니다.



ⓘ 주의 사항

데이터 전송을 위해 TCP 아웃바운드 **6600 PORT**가 열려 있어야 합니다.

설정하기

와탭 에이전트는 에이전트 별 필요한 설정을 `whatap.conf` 파일에 작성합니다. 에이전트는 환경변수를 통해 설정 파일의 위치를 파악하고 로딩합니다. `whatap.conf` 파일을 통해 설정할 수 있는 옵션은 다음과 같습니다.

📄 에이전트 이름 식별

모니터링 대상을 식별하기 위해 에이전트 이름 설정 방법을 제공합니다.

📄 에이전트 통신 설정

에이전트와 서버 간의 연결에 관한 설정입니다.

📄 윈도우 성능 카운터 설정

윈도우 성능 카운터 설정을 안내합니다.

에이전트 이름 식별

와탭은 모니터링 정보 수집 대상인 인프라 서버 식별을 위해 기본적으로 서버로부터 수집한 정보를 활용합니다. 기본값은 서버의 호스트 명(hostname)입니다.

- ❗ • 에이전트 이름은 프로젝트 단위로 고유해야 합니다.
- 에이전트 아이디/이름을 변경하면 이전 데이터와 연결되지 않습니다.

① 사용자가 설정한 에이전트 이름을 [와탭 모니터링 서비스](#)에서 확인하려면 서버를 재시작하세요.

사용자 친화적인 이름을 지정할 경우 다음과 같이 설정 파일에 지정 가능합니다.

• Linux Shell

SH

```
export WHATAP_SERVER_NAME=사용자 친화적인 이름
```

```
echo "oname=$WHATAP_SERVER_NAME" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

• Windows Power Shell

SH

```
# 관리자 권한이 필요합니다.
```

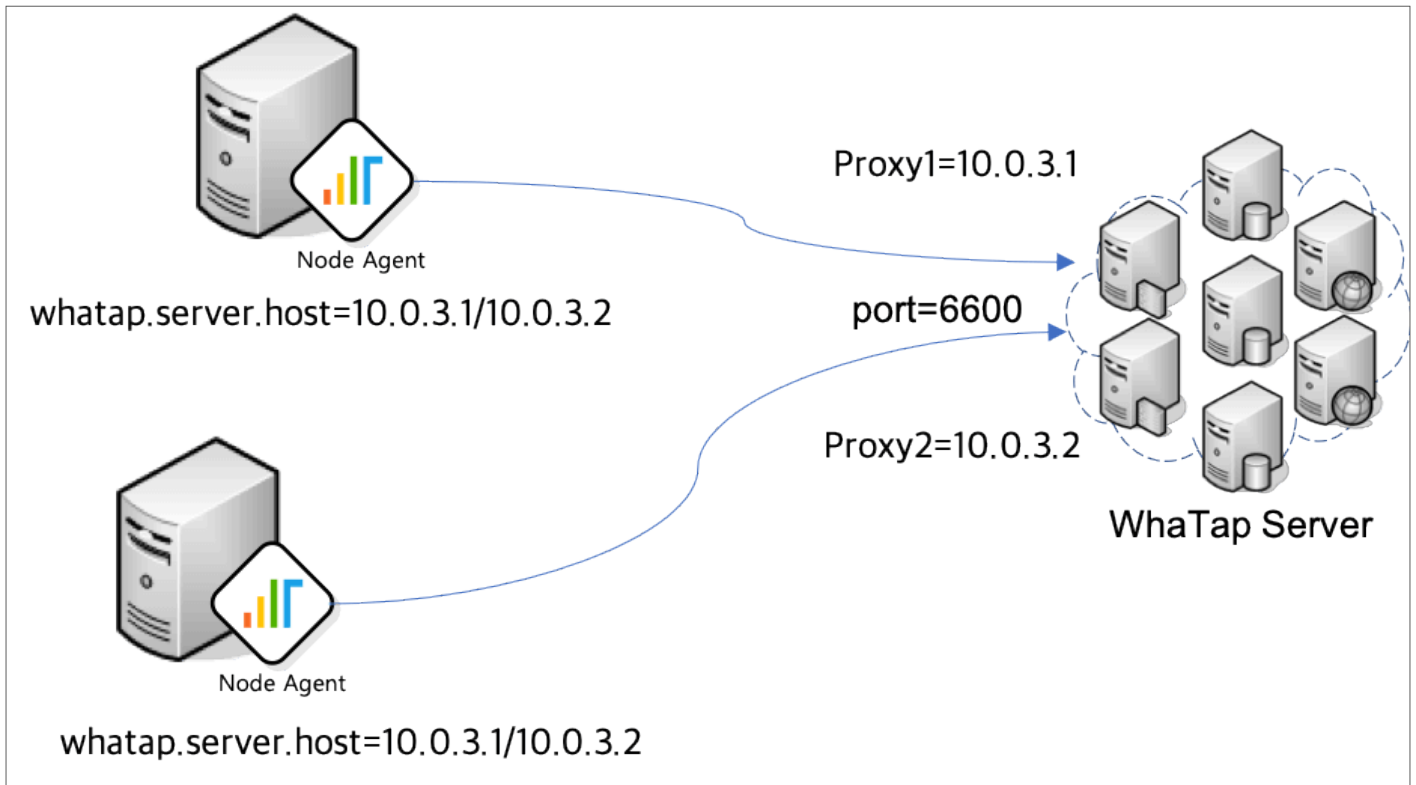
```
$WHATAP_SERVER_NAME="사용자 친화적인 이름"
```

```
Add-Content "C:\Program Files\WhatapInfra\whatap.conf" "oname=$WHATAP_SERVER_NAME"
```

에이전트 통신 설정

Network & security

와탭은 에이전트에 서버 방향을 TCP 연결 후 모니터링 데이터를 전송합니다.



에이전트는 하나의 TCP 세션을 통해서 데이터 전송과 서버의 제어 요청을 처리합니다. Node 에이전트는 UDP를 사용하지 않습니다. Node 에이전트에서 와탭 수집 서버 방향으로 방화벽을 개방합니다.

수집 서버 주소와 포트

와탭 서버는 데이터 리전 서버와 프론트 서버, 유레카 등으로 구분합니다. 데이터 리전에는 다시 Proxy, Yard, Gateway, Keeper 등이 있습니다. 에이전트는 그중에 Proxy 서버와 통신을 합니다.

Node 에이전트에 와탭 서버의 proxy 서버의 주소를 설정합니다.(예, `whatap.server.host=10.0.3.1/10.0.3.2`) 서버 주소를 설정할 때는 proxy 서버 숫자만큼 입력합니다. 와탭 서버는 설치 방식에 따라서 proxy 서버를 1개 또는 여러 개를 사용할 수 있습니다.

와탭 Proxy 서버는 6600 포트에서 리스닝(Listening)합니다. 에이전트에서 별도 설정을 하지 않으면 에이전트는 6600 포트에 접속을 시도합니다.

```
whatap.conf
```

```
whatap.server.port=6600
```

- ⓘ 두 개의 Proxy 서버가 서로 상이한 포트를 사용할 수 없습니다. 여러 대의 Proxy 서버를 사용하는 경우 리스닝(Listening) 포트는 동일해야 합니다.

통신 연결 및 보안

와탭은 퍼블릭 네트워크에서 모니터링 데이터를 수집하는 것을 전제로 설계했습니다. 따라서 모든 모니터링 데이터를 암호화해 서버로 전송합니다. 많은 데이터를 암호화 전송하면 오버헤드를 유발할 수도 있습니다. 와탭은 데이터를 선별적으로 암호화합니다. 에이전트와 서버 사이의 통신 과정은 다음과 같습니다.

1. 프로젝트 생성 메뉴에서 **프로젝트 액세스 키**를 생성하고 복사하세요.
2. **프로젝트 액세스 키**에는 비밀키를 포함합니다. 외부에 알려지지 않도록 주의하세요.
3. 애플리케이션 서버를 다시 시작하세요.
4. 와탭 에이전트는 서버로 TCP 세션을 연결합니다.
5. **프로젝트 액세스 키**에 포함된 통신용 비밀키를 가지고 데이터를 암호화해 새로운 세션용 보안 키를 요청합니다.
6. 서버는 에이전트가 요청한 세션용 보안 키를 새로 만들어 에이전트에 내려보냅니다.
7. 세션용 보안키는 2개의 암호 키를 포함하고 있습니다. ASC 알고리즘용 암호 키와 단순 암호를 위한 암호 키입니다.
8. 이후에 에이전트는 텍스트와 제어 등 중요한 데이터는 ASC 암호 키를 사용합니다. 숫자 데이터와 같이 상대적으로 안전한 데이터는 단순 암호화를 거쳐 데이터를 서버에 전송합니다.

- ⓘ 변경 사항을 적용하려면 서버를 재시작하세요.

윈도우 성능 카운터 설정

임의의 윈도우 성능 카운터를 수집할 수 있습니다. 와탭 서버 모니터링 설정 파일에 성능 카운터 세트 이름을 추가합니다.

- 성능 카운터 세트 이름을 조회할 수 있습니다.

Windows Powershell

```
Get-Counter -ListSet *
```

- 설정 파일에 성능 카운터 세트를 추가할 수 있습니다.

Windows Powershell

```
Add-Content -Path "C:\Program Files\WhatapInfra\whatap.conf" -Value "performance.counter.$(Get-Date -uformat %s)=조회할 성능 카운터 세트 이름"
```

- 추가한 성능 카운터는 [분석 > 메트릭스 조회](#) 메뉴에서 [카테고리](#) `performance_counter_{성능 카운터 세트 이름}` 으로 조회할 수 있습니다.

ⓘ 변경 사항을 적용하려면 서버를 재시작하세요.

고급 기능

확장팩 설정

정상적으로 설치 후 확장팩 기능을 사용하려면 다음과 같이 설정 파일을 생성하고 에이전트를 다시 시작하세요.

MySQL 서버 목록

MySQL/MariaDB 모니터링 에이전트를 이용할 수 있습니다.

웹 URL 성능 체크

와탭 인프라 에이전트가 주어진 웹 주소로 접속하여 접속 여부 및 응답 시간을 수집합니다. 수집된 웹 URL 성능은 [카테고리](#)

`server_webcheck` 에서 확인할 수 있습니다. 다음 명령으로 체크할 웹 주소를 추가하세요. URL 모니터링 서비스에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

Linux Shell

Windows Powershell

SH

```
echo "체크할 웹 주소" | sudo tee -a /usr/whatap/infra/conf/webcheck.conf
echo "webcheck.enabled=true" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
sudo service whatap-infra restart
```

SH

```
Add-Content -Path "C:\Program Files\WhatapInfra\webcheck.conf" -Value "체크할 웹 주소"
Add-Content -Path "C:\Program Files\WhatapInfra\whatap.conf" -Value "webcheck.enabled=true"
Restart-Service "Whatap Infra"
```

Redis 서버 목록

와탭 인프라 에이전트가 주어진 Redis 주소로 접속하여 연결 개수를 포함한 여러 개의 성능 지수를 수집합니다. 수집된 성능 정보는 [카테고리](#) `server_redis` 에서 확인할 수 있습니다. 다음 명령으로 체크할 Redis 서버의 접속 정보를 추가할 수 있습니다.

Linux Shell

Windows Powershell

SH

```
sudo echo "addr=Redis 주소:포트" | sudo tee /usr/whatap/infra/conf/redis.conf
sudo echo "password=Redis 패스워드" | sudo tee -a /usr/whatap/infra/conf/redis.conf
sudo service whatap-infra restart
```

SH

```
Add-Content -Path "C:\Program Files\WhatapInfra\redis.conf" -Value "addr=Redis 주소:포트"
Add-Content -Path "C:\Program Files\WhatapInfra\redis.conf" -Value "password=Redis 패스워드"
Restart-Service "Whatap Infra"
```

Memcached 서버 목록

와탭 인프라 에이전트가 주어진 Memcached 주소로 접속하여 연결 개수를 포함한 여러 개의 성능 지수를 수집합니다. 수집된 정보는 [카테고리](#) `server_memcached` 에서 확인할 수 있습니다. 다음 명령으로 체크할 Memcached 서버의 접속 정보를 추가할 수 있습니다.

Linux Shell

Windows Powershell

SH

```
sudo echo "addr=Memcached 주소:포트" | sudo tee /usr/whatap/infra/conf/memcached.conf
sudo echo "password=Memcached 패스워드" | sudo tee -a /usr/whatap/infra/conf/memcached.conf
sudo service whatap-infra restart
```

SH

```
Add-Content -Path "C:\Program Files\WhatapInfra\memcached.conf" -Value "addr=Memcached 주소"
Add-Content -Path "C:\Program Files\WhatapInfra\memcached.conf" -Value "password=Memcached 패스워드"
Restart-Service "Whatap Infra"
```

TCP 포트 감시

네트워크 데몬의 수신 포트 비활성화 시 알림을 받을 수 있습니다.

홈 화면 > 프로젝트 선택 > 경고 알림 > 이벤트 설정 > 서버 탭을 선택하고 + 이벤트 추가 버튼을 선택하세요.

이벤트 설정

이벤트 추가

제목 *

이벤트 타입 선택

서버 프로세스 로그

이벤트 발행 조건

지표	조건	레벨	지속 시간	활성화
재시작	-	위험	-	<input checked="" type="checkbox"/>
미수신	-	경고	10 분	<input type="checkbox"/>
포트	-	경고	1 분	<input checked="" type="checkbox"/>
네트워크 IOPS	경고 > 45,000 pps	위험 > 50,000 pps	5 분	<input checked="" type="checkbox"/>
			위험 5 분	<input checked="" type="checkbox"/>
네트워크 BPS	경고 > 150,000,000 bps	위험 > 200,000,000 bps	5 분	<input checked="" type="checkbox"/>
			위험 5 분	<input checked="" type="checkbox"/>
디스크 I/O	90%	95%	5 분	<input checked="" type="checkbox"/>
			위험 5 분	<input checked="" type="checkbox"/>
디스크 사용량	90%	95%	5 분	<input checked="" type="checkbox"/>
			위험 5 분	<input checked="" type="checkbox"/>

서버 목록

전체 선택

- demo-k8s-master (10.21.1.149)
- demo-k8s-worker-01 (10.21.1.229)
- demo-k8s-worker-02 (10.21.1.157)
- demo-k8s-worker-03 (10.21.1.23)
- demo-k8s-worker-04 (10.21.1.210)
- dotnet-official-demo (10.21.1.51)
- go-official-demo (10.21.1.118)
- mysql-official-demo-01 (10.21.1.86)
- mysql-official-demo-02 (10.21.1.136)
- mysql-official-demo-02 (10.21.1.136)
- mysql-official-demo-03 (10.21.1.236)
- node-official-demo (10.21.1.98)
- python-demo-attack (10.21.1.254)
- python-demo-target (10.21.1.43)
- rum-official-demo (10.21.1.151)

2 저장

- 1 포트 지표 토글 버튼을 클릭하여 사용 상태로 변경하세요.
- 2 저장 버튼을 선택하여 저장하세요.

- 대상 서버에서 다음 명령을 추가하세요.

Linux Shell

Windows Powershell

SH

```
#아래 변수에 모니터링 대상 아이피를 지정합니다.
export TARGET_IP=127.0.0.1
#아래 변수에 모니터링 대상 포트를 지정합니다.
export TARGET_PORT=80
echo "tcp.check.$TARGET_PORT=tcp://$TARGET_IP:$TARGET_PORT" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

SH

```
#아래 변수에 모니터링 대상 아이피를 지정합니다.
$TARGET_IP="127.0.0.1"
#아래 변수에 모니터링 대상 포트를 지정합니다.
$TARGET_PORT="80"
Add-Content -Path "C:\Program Files\WhatapInfra\whatap.conf" -Value
"tcp.check.$TARGET_PORT=tcp://$TARGET_IP:$TARGET_PORT"
```

프로세스 네트워크 성능 측정

프로세스 네트워크 성능은 [서버 목록](#) > [서버 상세](#) 화면의 [프로세스](#) 위젯에서 확인할 수 있습니다.

Linux Shell

Windows Powershell

SH

```
echo "process.fdcheck=true" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

SH

```
# 관리자 권한이 필요합니다.
Add-Content -Path "C:\Program Files\WhatapInfra\whatap.conf" -Value "process.fdcheck=true"
```

서버 스펙 수집

CPU, MEMORY, DISK, NIC의 스펙과 설치된 패키지 및 가상 머신의 메타 정보를 수집합니다. 각 [카테고리](#)에서 다음 내용을 확인하실 수 있습니다.

- `server_package` : 설치된 패키지입니다.
- `server_inventory` : CPU, MEMORY, DISK, NIC의 스펙입니다.
- `server_pending_security_update` : 리눅스의 보안 패치 대기 목록입니다.

Linux Shell

Windows Powershell

SH

```
echo "inventory.product.enabled=true" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

SH

```
# 관리자 권한이 필요합니다.
Add-Content -Path "C:\Program Files\WhatapInfra\whatap.conf" -Value "inventory.product.enabled=true"
```

리눅스 컨테이너 성능 수집

리눅스 컨테이너의 CPU, MEMORY, DISK, NIC 성능을 수집합니다. 수집된 성능 정보는 [카테고리](#) `server_container`에서 확인할 수 있습니다.

Linux Shell

```
echo "container.enabled=true" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

윈도우 서버 서비스 운영 상태 수집

윈도우 서버 서비스 운영 상태를 수집합니다. 수집된 서비스 운영 상태는 [카테고리](#) `server_windows_service`에서 확인할 수 있습니다.

Windows Powershell

관리자 권한이 필요합니다.

Add-Content -Path "C:\Program Files\WhatapInfra\whatap.conf" -Value "winservice.enabled=true"

파일 감시

파일 시스템상에 존재하거나 존재할 가능성이 있는 파일 및 디렉터리를 감시할 수 있습니다.

Linux Shell

Windows Powershell

SH

```
echo "filecheck.enabled=true" | sudo tee -a /usr/whatap/infra/conf/filesystem.conf
echo "감시를 원하는 파일 혹은 디렉터리 전체 경로" | sudo tee -a /usr/whatap/infra/conf/filesystem.conf
```

SH

```
Add-Content -Path "C:\Program Files\WhatapInfra\whatap.conf" -Value "filecheck.enabled=true"
Add-Content -Path "C:\Program Files\WhatapInfra\filesystem.conf" -Value "감시를 원하는 파일 혹은 디렉터리 전체 경로"
```

Nvidia GPU 모니터링

`nvidia-smi` 명령이 탑재된 경우 GPU 성능을 5초 간격으로 수집해 와탭으로 업로드합니다. 수집된 정보는 매트릭스 [카테고리](#) `server_nvdiasm` 로 수집됩니다.

Linux Shell

Windows Powershell

SH

```
echo "nvdiasm.enabled=true" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

SH


```
Add-Content -Path "C:\Program Files\WhatapInfra\whatap.conf" -Value "nvidiasmi.enabled=true"
```

- category server_nvidiasmi

메트릭스	비고
DecoderUtil	gauge, Decoder utilization (in %)
EncoderUtil	gauge, Encoder utilization (in %)
FreeFbMemoryUsageGpu	gauge, Framebuffer memory free (in MiB).
UsedFbMemoryUsageGpu	gauge, Framebuffer memory used (in MiB).
GpuTemp	gauge, GPU temperature (in C).
GpuUtil	gauge, GPU utilization (in %).
MemClock	gauge, Memory clock frequency (in MHz).
MemoryUtil	gauge, Memory utilization (in %).
SmClock	gauge, SM clock frequency (in MHz).

와탭 에이전트 로그 위치 변경

와탭 에이전트 로그(`whatap_infrad.log` , `whatap_infra.log` , `whatap_infrad.fork.stdout.log`)의 경로를 변경합니다. 지정 경로가 없는 경우 와탭 에이전트가 생성을 시도합니다. 에이전트 버전 2.0.6 이상 지원됩니다.

Linux Shell

Windows Powershell

```
SH
```

```
echo "agent.log.prefix=변경을 원하는 디렉터리" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

SH

```
Add-Content -Path "C:\Program Files\WhatapInfra\whatap.conf" -Value "agent.log.prefix=변경을 원하는 디렉터리"
```

❗ 윈도우의 경우 경로 구분자를 `\\` 로 입력할 수 있습니다.

Netstat 모니터링

netstat 명령이 탑재된 경우 1분 간격으로 수집하여 [카테고리](#) `server_netstat` (netstat connection 통계), `server_netstat_s` (netstat -s 명령 실행 결과)로 업로드됩니다.

Linux Shell

Windows Powershell

SH

```
echo "netstats.enabled=true" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

SH

```
Add-Content -Path "C:\Program Files\WhatapInfra\whatap.conf" -Value "netstats.enabled=true"
```

사용자 스크립트 모니터링

리눅스 서버에서 실행 가능한 사용자 스크립트를 주기적으로 실행하여 결과를 업로드합니다. 다음 예시를 참조하여 사용자 스크립트를 작성하세요.

1. 스크립트를 다음과 같이 작성 후 실행하세요.

Linux Shell

```
#!/bin/bash
```

```
urls=("https://www.whatap.io" "https://blog.whatap.io" "https://service.whatap.io")
```

```

for url in ${urls[*]}; do

echo "M $url url $url"
curl -w @- -o /dev/null -s "$url" <<'EOF'
M %{url_effective} url %{url_effective}\n
H %{url_effective} time_namelookup %{time_namelookup}\n
H %{url_effective} time_connect %{time_connect}\n
H %{url_effective} time_appconnect %{time_appconnect}\n
H %{url_effective} time_pretransfer %{time_pretransfer}\n
H %{url_effective} time_redirect %{time_redirect}\n
H %{url_effective} time_starttransfer %{time_starttransfer}\n
H %{url_effective} time_total %{time_total}\n
EOF

done

```

2. 다음과 같이 출력되는지 확인하세요.

Linux Shell

```

$ ./curl.sh
M https://www.whatap.io/ url https://www.whatap.io/
H https://www.whatap.io/ time_namelookup 0.007289
H https://www.whatap.io/ time_connect 0.010702
H https://www.whatap.io/ time_appconnect 0.033637
H https://www.whatap.io/ time_pretransfer 0.033831
H https://www.whatap.io/ time_redirect 0.000000
H https://www.whatap.io/ time_starttransfer 0.043230
H https://www.whatap.io/ time_total 0.043312
M https://blog.whatap.io/ url https://blog.whatap.io/
H https://blog.whatap.io/ time_namelookup 0.000000
H https://blog.whatap.io/ time_connect 0.000000
H https://blog.whatap.io/ time_appconnect 0.000000
H https://blog.whatap.io/ time_pretransfer 0.000000
H https://blog.whatap.io/ time_redirect 0.000000
H https://blog.whatap.io/ time_starttransfer 0.000000
H https://blog.whatap.io/ time_total 0.005654
M https://service.whatap.io/ url https://service.whatap.io/
H https://service.whatap.io/ time_namelookup 0.004296
H https://service.whatap.io/ time_connect 0.007282
H https://service.whatap.io/ time_appconnect 0.038404
H https://service.whatap.io/ time_pretransfer 0.038607
H https://service.whatap.io/ time_redirect 0.000000

```

```
H https://service.whatap.io/ time_starttransfer 0.055226
H https://service.whatap.io/ time_total 0.055307
```

3. 스크립트 정상 수집을 확인하고 다음과 같이 와탭 서버 모니터링 에이전트에 스크립트를 등록하세요.

Linux Shell

```
export USER_SCRIPT=실행할 사용자 스크립트 절대 경로
sudo chmod +x $USER_SCRIPT
sudo mkdir /usr/whatap/infra/ext/
sudo cp -r $USER_SCRIPT /usr/whatap/infra/ext/
export RUNAS_USER=사용자 스크립트를 실행할 계정. root 계정 제외
sudo WHATAP_HOME=/usr/whatap/infra/conf /usr/whatap/infra/whatap_infrad --user=$RUNAS_USER init-script
sudo service whatap-infra restart
```

수집된 데이터는 [분석 > 매트릭스 차트](#)에서 [카테고리](#) `server_ext_폴더_실행스크립트` 에서 찾을 수 있습니다.

서버 시간 동기화 모니터링

ⓘ 사전 확인

- 운영체제: 리눅스
- 와탭 서버 모니터링 에이전트 버전: 2.5.4 이상

다음 옵션을 통해 서버 시간 동기화(NTP) 모니터링 기능을 활성화 할 수 있습니다.

```
echo "ntp.enabled=true" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

추가 지표 안내

서버 시간 동기화 모니터링 기능 활성화 시 추가되는 메트릭은 다음과 같습니다.

server_ntpq

Tags

태그명	설명	비고
refid	해당 리모트(remote)의 시간 동기화 소스를 의미합니다.	-
remote	호스트가 시간 동기화를 수행할 대상 서버를 의미합니다.	-

Fields

필드명	단위	설명	비고
delay	ms	서버가 보낸 쿼리에 대한 응답으로 회신 패킷을 반환하는데 걸린 시간을 의미합니다.	-
jitter	-	두 샘플 간의 오프셋 측정 차이로 추정된 오차 경계치를 의미합니다.	-
offset	ms	서버 설정 시간과 클라이언트 설정 시간 간의 차이를 의미합니다.	-
poll	second	ntp.conf 파일에서 minpoll 값으로 정의된 원격 호스트로의 폴링 간격을 의미합니다.	-
reach	-	서버에 도달하는 시도가 얼마나 성공적인지 확인할 수 있습니다. 2^0 위치에 가장 최근 질의 성공 여부를 기록하고 8 비트 쉬프트 레지스터로 작동합니다.	-
st	-	원격 호스트의 스트래텀 레벨을 의미합니다.	-
sync_client	-	1: 동기화 서버가 존재합니다. 0: 동기화 서버가 존재하지 않습니다.	-
t	-	사용 가능한 유형은 다음과 같습니다. l : 로컬(예 GPS시계)	-

필드명	단위	설명	비고
		u: 유니캐스트(일반적인 유형)	
		m: 멀티캐스트	
		b: 브로드캐스트	
when	second	원격 호스트 응답 이후 지난 초 수를 의미합니다.	-

리눅스 시스템 로그 모니터링

리눅스 시스템 로그를 실시간 업로드하여 장애 시 해당 시간에 발생한 로그를 확인할 수 있습니다. 수집 대상 로그 파일은 다음과 같습니다.

- [/var/log/syslog](#)
- [/var/log/messages](#)

설정 방법은 다음과 같습니다.

Linux Shell

```
echo "systemlog.enabled=true" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

로그 모니터링 플러그인

임의의 로그를 수집할 수 있습니다. 다음 설정은 에이전트 재시작이 필요합니다.

Linux Shell

Linux Shell

```

1 cd /usr/whatap/infra
2 sudo mkdir extension
3
4 cat >extension/logsink.conf<<EOL
5 [[inputs.logsink]]
6   category = "serverlog"
7   ## 로그 발생량 통계 별도 데이터로 전송 여부
8   stats_enabled = true
9   ## 로그 발생량 통계 카테고리
10  stats_category = "logsink_stats"
11  ## 로그 파일 경로(path)에 별표(*)가 포함되어 제외할 로그 비대상 파일명 설정
12  excludeNames = [ ".gz", ".zip" ]
13  [[inputs.logsink.file]]
14  ## 로그 파일 지정 시, 날짜 패턴(strftime.org) 지정 가능
15  path = "/some/path/%Y-%m-%d/.log"
16  disabled = false
17  encoding = "euc-kr"
18
19  [[inputs.logsink.file]]
20  path = "/some/other/log"
21  disabled = false
22  encoding = "utf-8"
23
24  [[inputs.logsink.file]]
25  ## 줄 단위 로그에서 해당 키워드 검색 시, 이전 로그에 병합
26  nowrap_keywords = ["Caused by:", "Test"]
27 EOL
28
29 sudo service whatap-infra restart

```

Windows Powershell

Windows Powershell

```

1 # 관리자 권한 필요
2 New-Item -type "Directory" -Path "C:\Program Files\WhatapInfra\extension"
3
4 $contentToAdd = @"
5 [[inputs.logsink]]
6   category = "serverlog"

```

```

7  ## 로그 발생량 통계 별도 데이터로 전송 여부
8  stats_enabled = true
9  ## 로그 발생량 통계 카테고리
10 stats_category = "logsink_stats"
11 ## 로그 파일 경로(path)에 별표()가 포함되어 제외할 로그 비대상 파일명 설정
12 excludeNames = [ ".gz", ".zip" ]
13 [[inputs.logsink.file]]
14 ## 로그 파일 지정 시, 날짜 패턴(strftime.org) 지정 가능
15 path = "c:\\whatap\\logs%Y-%m-%d_.log"
16 disabled = false
17 encoding = "euc-kr"
18 [[inputs.logsink.file]]
19 ## 줄 단위 로그에서 해당 키워드 검색 시, 이전 로그에 병합
20 nowrap_keywords = ["Caused by:", "Test"]
21 "@
22
23 New-Item -path "C:\Program Files\WhatapInfra\extension" -name "logsink.conf" -type "file" -value $contentToAdd -Force
24
25 Restart-Service "Whatap Infra"

```

옵션 설정

- `stats_enabled` : 수집 현황 데이터의 수집 여부를 설정합니다. 기본값은 `false` 입니다. 값을 `true` 로 설정해야 합니다. `true` 로 설정하면 다음 `stats_category` 에서 설정한 카테고리(`logsink_stats`)로 통계 데이터가 발생합니다.
- `stats_category` : 수집 현황 데이터를 저장할 매트릭스 카테고리를 설정합니다. 값을 `logsink_stats` 로 설정해야 합니다. 통계 데이터 필드는 다음과 같습니다.
 - `file`
 - `checkInterval`
 - `encoding`
 - `filepos`
 - `checkedLocalTime`
 - `lastupdatedLocalTime`
 - `fileSize`
 - `error`
 - `firstCheck`

- `transferBytes`
- `excludeNames`: 로그 파일 경로(path)에 별표(*)를 포함한 경우 로그 비대상 파일을 제외하도록 파일명을 설정할 수 있습니다. 심표(.)를 구분자로 이용해 복수 설정할 수 있습니다.

Example

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

- `nowrap_keywords`: 줄 단위 로그 검색 시 해당 옵션값으로 지정한 키워드가 검색될 경우 이전 로그에 병합합니다.

윈도우 이벤트 로그 옵션 설정

윈도우 이벤트 로그 수집 시 다음과 같이 옵션을 설정할 수 있습니다.

```
# 관리자 권한 필요
```

```
New-Item -type "Directory" -Path "C:\Program Files\WhatapInfra\extension"
```

```
$contentToAdd = @"
```

```
[[inputs.win_eventlog]]
```

```
category = "win_event_log"
```

```
stats_category = "win_event_log_stats"
```

```
stats_enabled = true
```

```
enabled = true
```

```
[[inputs.win_eventlog.file]]
```

```
#true | false
```

```
enabled = true
```

```
# Application, Security, Setup, System, Forwarded
```

```
file = "Application"
```

```
#1: Information, 2: Warning 3: Critical 4: Audit Success 5 Audit Fail
```

```
#event_type =
```

```
#event id
```

```
#event_id =
```

```
#event source name
```

```
#source_name = ""
```

```
"@"
```

```
New-Item -path "C:\Program Files\WhatapInfra\extension" -name "win_eventlog.conf" -type "file" -value $contentToAdd -Force
```

```
Restart-Service "Whatap Infra"
```

- ❗ • 지원 버전 2.5.2
- 운영체제: Windows

- 카테고리 지정(`category`) 필수
| 예, `win_event_log`
- 통계 카테고리 지정(`stats_category`) 필수
| 예, `win_event_log_stats`
- 통계 카테고리 On/Off(`stats_enabled`) 필수
| 예, `true` 혹은 `false`
- 수집 기능 On/Off(`enabled`) 필수
| 예, `true` 혹은 `false`
- 파일별 수집 기능 On/Off(`enabled`) 필수
| 예, `true` 혹은 `false`
- 파일(`file`) 필수
| 예, `Application` , `Security` , `Setup` , `System` , `Forwarded`
- 이벤트 타입(`event_type`) 비필수
| 예, `1` , `2` , `3` , `4` , `5`

❗ 이벤트 타입

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

- 이벤트 아이디(`event_id`) 비필수
- 이벤트 소스 이름(`source_name`) 비필수

에이전트 업데이트

! 이전 버전을 설치하려면 support@whatap.io로 문의해 주세요.

Linux 및 Unix

설치된 에이전트를 최신 버전으로 업데이트하려면 다음 명령어를 실행하세요.

• Debian / Ubuntu

SH

```
sudo apt-get update
sudo apt-get install whatap-infra
sudo service whatap-infra restart
```

특정 버전을 설치하려면 설치 시 버전 정보를 다음과 같이 명시하세요.

```
sudo apt-get install whatap-infra={version}
```

• CentOS / Amazon Linux / SUSE / XenServer

SH

```
sudo yum update whatap-infra
sudo service whatap-infra restart
```

특정 버전을 설치하려면 설치 시 버전 정보를 다음과 같이 명시하세요.

```
sudo yum install whatap-infra-{version}
```

• FreeBSD

SH

```
wget http://repo.whatap.io/freebsd/10/whatap-infra.txz
pkg install whatap-infra.txz
```

AIX

설치된 에이전트를 최신 버전으로 업데이트하려면 다음 명령어를 실행하세요.

```
stopsrc -s whatap-infra
cp /usr/whatap/infra/conf/whatap.conf /tmp/whatap.conf
rpm -e whatap-infra
rpm -Uvh http://repo.whatap.io/aix/noarch/whatap-infra-latest.noarch.rpm
cp /tmp/whatap.conf /usr/whatap/infra/conf/whatap.conf
startsrc -s whatap-infra
```

Windows

설치된 에이전트를 최신 버전으로 업데이트하려면 [관리 > 에이전트 설치](#) 메뉴로 이동하세요. [설치 안내](#) 섹션의 [설치 파일 다운로드](#) 안내에 따라 윈도우 서버 운영 체제용 설치 파일을 다운로드 후 `whatap_infra.exe` 파일을 실행하세요. 에이전트 업데이트 후 서비스가 재시작됩니다.

ⓘ 보안 설정 때문에 `.exe` 형식의 파일이 받아지지 않는 사용자를 위해 `.zip` 형식의 파일도 함께 제공합니다. 자세한 내용은 [다음 문서](#)를 참조하세요.

에이전트 삭제

Linux

설치된 에이전트를 삭제하려면 다음 명령어를 실행하세요.

- Debian / Ubuntu

```
SH
```

```
sudo apt-get remove whatap-infra
```

- CentOS / Amazon Linux / SUSE / XenServer

```
SH
```

```
sudo yum remove whatap-infra
```

- FreeBSD

```
SH
```

```
pkg delete whatap-infra
```

Windows

- 서버 모니터링 에이전트 삭제 명령을 관리자 권한의 command 창에서 실행합니다.

```
SH
```

```
"C:\Program Files\WhatapInfra\unins000.exe"
```

- 제어판의 프로그램 삭제 기능을 사용할 수도 있습니다.

주요 메뉴 알아보기

와탭 에이전트 설치를 완료했다면 [와탭 모니터링 서비스](#)에 로그인하세요. 와탭 모니터링 서비스는 원활한 서비스 제공과 안정적 운영, 이상 징후 감시 및 파악을 위한 정보를 제공합니다.

서버 모니터링은 실시간 수집으로 장애 원인 도출에 용이합니다. 운영 편리성을 높이기 위해 보고서 기능을 강화했으며, 선호하는 알림 수단을 선택할 수 있습니다.

와탭 서버 모니터링 서비스는 다음의 주요 기능을 제공합니다.

• 실시간 통합 모니터링

- 300대 이하 서버 자원의 실시간 사용량 정보
- 전체 서버 요약 지표 제공
- CPU, Memory, Disk I/O, IOPS 사용량 기준으로 상위 5개 서버 목록 제공
- CPU, Memory 최대 점유율 기준으로 상위 5개 프로세스 목록 제공

• 성능 분석

- 수집 서버 전체의 현황 정보
- 1분에 10회 이상 수집된 CPU, Memory, Disk, Network 성능 정보
- 최대 5개 서버 간 메트릭스 차트로 성능 비교 정보
- 프로세스 그룹화 적용 후 멀티 프로세스 자원 사용량 합계치 정보

• 이벤트 알림

- 이메일, 문자, SNS(Telegram, Slack) 발송
- 이벤트 지속 기간 및 임계치 설정에 의한 이벤트 발생 및 과거 데이터 기반 이벤트 시뮬레이션
- 무음 설정 시간 등록 및 키워드 반복으로 인한 동일 이벤트 알림 억제 기능
- 개별 알림을 묶어 Policy로 제공 후 특정 서버에 자동 적용 기능
- 재시작 여부, 통신 장애 지속시간, 자원 사용량에 따른 서버 이벤트 설정 알림
- 프로세스 개수 증감, CPU 사용량, Memory 사용량에 따른 프로세스 이벤트 설정 알림
- 파일 로그 키워드에 의한 이벤트 설정 및 이벤트 위험도 설정 알림

• 통계 및 보고

- 서버 일간/주간 보고서

- 서버 월간 보고서

- **관리 기능**

- 권한 관리
- 에이전트 삭제
- 정비 계획 사전 입력

리소스 보드

홈 화면 > 프로젝트 선택 > 대시보드 > 리소스 보드

와탭 모니터링 서비스 초기 화면에서 프로젝트를 선택한 다음 **프로젝트 메뉴** 하위에 **대시보드 > 리소스 보드**를 선택하세요.

1 리소스보드
🔍 🔔 📄 ⋮ 👤

2 **Server** > 17

OS: Linux 16, Windows 1, Unix 0, Others 0

비활성 전체

Total Cores 35

Avg CPU 21%

0% Max 88%

Avg Memory 45%

0% Max 82%

Avg Disk 49%

0% Max 99%

4 **CPU TOP5**

메모리 TOP5

디스크 I/O TOP5

3 **CPU Resource Map**

5 **프로세스 CPU TOP5**

Name	Max (%)	Avg (%)	Count	Servers
/usr/local/openjdk-8/bin/java/data/whatap...	69.87	6.28	20	demo-k8s-worker-04...
w3wp.exe	48.91	48.91	1	dotnet-official-demo
java/data/prod/whatap-virtual...	29.25	4.87	6	virtual-java-agent
java/data/dev/whatap-virtual-2.2.14.jarcom.virtual.App	29.09	4.85	6	virtual-java-agent
rumsender	16.24	16.24	1	rum-official-demo

프로세스 메모리 TOP5

Name	Max (%)	Avg (%)	Count	Servers
java%p jar /data/wpm/whatap.webche...	32.97	32.97	1	url-official-demo
java/data/prod/whatap-virtual...	30.73	5.12	6	virtual-java-agent
/usr/local/openjdk-8/bin/java/data/whatap...	30.43	4.22	20	demo-k8s-worker-02...
java/data/dev/whatap-virtual-2.2.14.jarcom.virtual.App	29.61	4.94	6	virtual-java-agent
mysql-official-demo-03...	26.88	26.14	2	mysql-official-demo-03...

리소스 보드에서 하나의 프로젝트에 등록된 모든 서버를 모니터링할 수 있습니다.

프로젝트 내 모든 서버의 요약 정보와 실시간 자원 사용량의 변화를 확인할 수 있는 **CPU Resource Map**을 제공합니다. 전체 자원의

규모, CPU, 메모리, 프로세스의 사용률 Top 5를 보여줍니다. 리소스 보드를 통해 장애 상황을 즉시 인지하고 대응할 수 있습니다.

1 고정 메뉴

- **🏠 테마:** 현재 페이지의 테마를 변경할 수 있습니다. 기본값은 **Light** 모드입니다.
- **🔔 실시간 알림:** 최근 발생한 이벤트를 확인할 수 있습니다. 토글 메뉴를 클릭해 브라우저 알림을 켜거나 끌 수 있습니다.
- **💬 고객 지원:** 온라인 고객 지원을 받을 수 있습니다.
- **프로필 아이콘:** 가장 오른쪽에 위치한 아이콘을 선택하세요. **계정 관리**, **조직 생성**, **조직 관리**, 사용자 언어를 선택할 수 있는 기능을 제공합니다.

2 인포 패널

프로젝트에 등록된 전체 서버들에 대한 요약 지표들을 제공합니다. 10초 단위로 갱신됩니다.

• Servers

전체 서버 수와 문제가 있는 서버의 수를 함께 제공합니다. 영역을 선택하면 **서버 목록** 페이지로 이동합니다.

- 예외 상태: **위험**, **경고**
- 정상 서버: **보통**, **비활성**

• Total Cores

전체 서버들의 코어(vCPU) 합입니다.

• Avg CPU

전체 서버들의 CPU 평균 사용량(%)입니다. 아래 게이지는 평균값, 최댓값, 최솟값을 나타냅니다.

• Avg Memory

전체 서버들의 메모리 평균 사용량(%)입니다. 아래 게이지는 평균값, 최댓값, 최솟값을 나타냅니다.

• Avg Disk

전체 서버들의 디스크 디바이스들의 평균 사용량(%)입니다. 아래 게이지는 평균값, 최댓값, 최솟값을 나타냅니다.

• OS

프로젝트 내 linux와 windows 운영체제 수입니다.

3 CPU Resource Map

전체 서버들의 CPU 사용량을 나타내는 분포도입니다. 10분 동안의 데이터를 보여주고 10초 주기로 갱신됩니다. 셀 색상의 진하기는 해당 영역에 서버들의 자원 사용량이 많이 분포되어 있음을 의미합니다.

• 상세 정보 제공

셀 영역을 드래그하면 상세 정보를 제공합니다.



- 서버 목록은 범위에서 수집된 데이터의 최댓값을 기준으로 정렬됩니다.

- 기본 5개의 서버가 선택되어 있으며 선택된 서버들의 사용량 추이를 멀티 라인 차트로 제공합니다.
- **새로 고침** 버튼을 수동으로 클릭하여 현재 시점의 데이터로 갱신이 가능합니다.

❗ 멀티 라인 차트

한 차트에 라인 여러 개가 보이는 차트입니다.

4 리소스 이퀄라이저

CPU, Memory, Disk I/O, Disk IOPS의 항목에 대해 상위 5개 서버 목록을 실시간으로 보여줍니다.

예를 들어 Disk I/O(%) 지표는 5초 동안의 디스크 사용률을 보여줍니다. Disk I/O(%)가 80%를 넘으면 시스템 성능에 영향을 줄 수 있습니다. 기본 경고 값은 90%입니다. Disk I/O(%)가 100% 라면 디스크가 쉬지 않고 일하고 있다는 의미입니다.

- 이퀄라이저 차트 영역을 선택하면 대상 **서버 상세** 페이지로 이동합니다.
- > 버튼을 선택하면 **리소스 이퀄라이저** 페이지로 이동합니다. 전체 서버에 대한 실시간 사용량을 볼 수 있습니다.

5 Process Top 5

CPU, Memory의 최대 점유율 기준으로 상위 5개의 프로세스 목록을 제공합니다. > 버튼을 선택하면 다음과 같이 전체 서버에 대한 **프로세스 목록**을 확인할 수 있습니다.

프로세스 목록

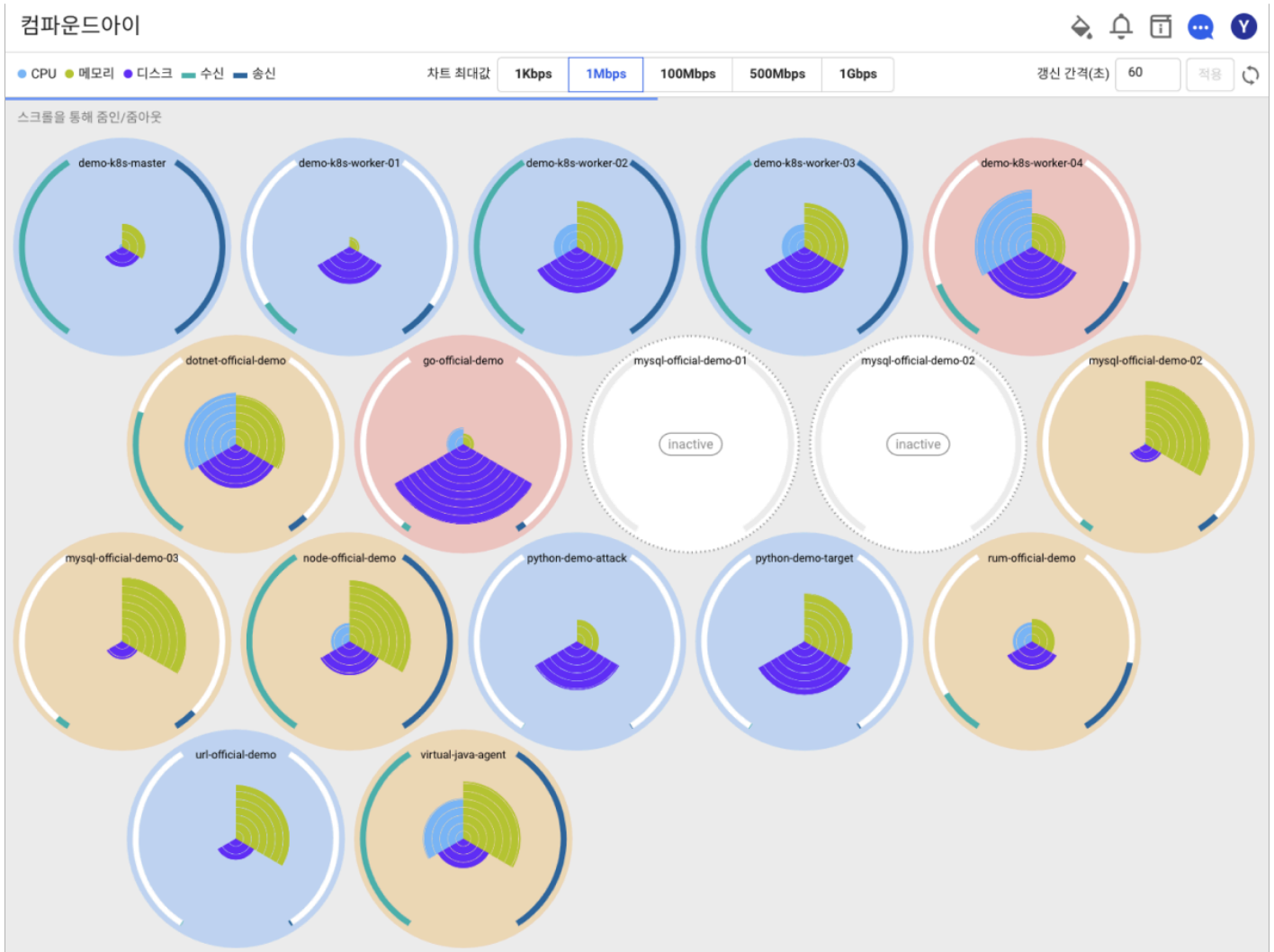
Process Name, User

이름	사용자	에이전트 명	건수	CPU ↑	메모리	IO
java	root	demo-k8s-worker-04	6	69.8%	20.3%	0%
w3wp.exe	IIS APPPOOL\smarts...	dotnet-official-demo	1	48.7%	16.1%	0%
java	root	demo-k8s-worker-02	7	30.1%	30.1%	0%
java	root	demo-k8s-worker-02	7	29.3%	30.6%	0%
java	whatap	virtual-java-agent	6	26.4%	29.7%	0%
java	whatap	virtual-java-agent	6	20.8%	30.9%	0%
node /home/ubun	ubuntu	node-official-demo	3	14.2%	20.5%	0%
rumsender	root	rum-official-demo	1	10.3%	2.2%	0%
rumstats	root	rum-official-demo	1	9.7%	3.8%	0%
w3wp.exe	IIS APPPOOL\demo4...	dotnet-official-demo	1	7.7%	24%	0%
whatap_dotnet.exe	NT AUTHORITY\SYS...	dotnet-official-demo	1	6%	0.4%	0%
whatap_agent	root	go-official-demo	4	5.8%	0.7%	0%
node.exe	EC2AMAZ-NO1BAVA...	dotnet-official-demo	1	5.2%	0.5%	0%
http_server	root	go-official-demo	2	3.4%	0.9%	0%
grpc_server	root	go-official-demo	2	2.5%	0.8%	0%
sqlservr.exe	NT SERVICE\MSSQL...	dotnet-official-demo	1	2%	5.1%	0%
cadvisor_helper	root	demo-k8s-worker-02	1	1.9%	0.6%	0%
whatap_infra.exe	NT AUTHORITY\SYS...	dotnet-official-demo	2	1.9%	0.4%	0%
kuber	root	go-official-demo	1	1.9%	0.6%	0%
echov4	root	go-official-demo	1	1.7%	0.5%	0%
kube-apiserver	root	demo-k8s-master	1	1.7%	9.4%	0%
echo	root	go-official-demo	1	1.6%	0.5%	0%
kubelet	root	demo-k8s-master	1	1.5%	1.7%	0%
conhost.exe	EC2AMAZ-NO1BAVA...	dotnet-official-demo	2	1.4%	0.2%	0%
grpc_client	root	go-official-demo	1	1.3%	0.4%	0%

컴파운드 아이

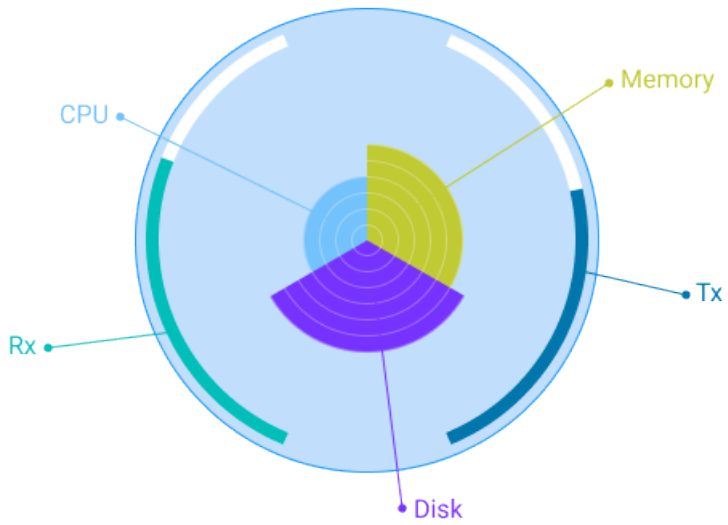
홈 화면 > 프로젝트 선택 > 대시보드 > 컴파운드 아이

와탭 모니터링 서비스 초기 화면에서 프로젝트를 선택한 다음 프로젝트 메뉴 하위에 대시보드 > 컴파운드 아이를 선택하세요.



컴파운드 아이를 통해 와탭 에이전트가 설치된 모든 서버를 빈틈없이 볼 수 있습니다. 대규모 서버의 자원 상황을 한눈에 확인 가능합니다. 대규모 서버 자원에 대해 샘플링 혹은 요약된 결과가 아닌 시각적으로 가시화 된 뷰를 제공합니다

제공 정보

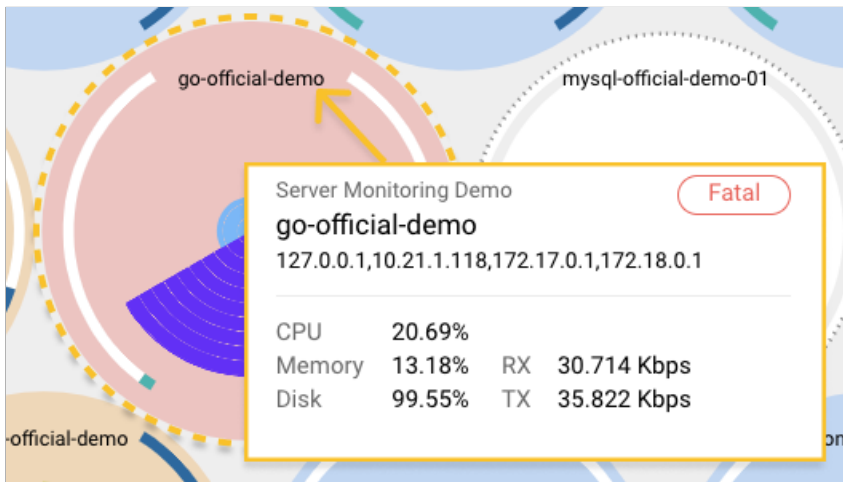


하나의 눈(Eye)입니다. 총 5 가지 정보를 제공합니다.

- CPU: CPU 사용량
- Memory: Memory 사용량
- Disk: Disk 사용량
- Rx: 네트워크의 Rx (수신량)
- Tx: 네트워크의 Tx (송신량)

ⓘ 네트워크 Rx/Tx 사용량 지표를 보고 DDoS와 같은 외부 공격이 여러 서버에서 일제히 발생하는지 확인할 수 있습니다.

이상 현상 발생



서버에 이상 현상이 발생한 경우 개별 아이(Eye, 눈)는 색상으로 그 상태를 표현합니다.

- **빨간색:** 위험 상태
- **주황색:** 경고 상태
- **회색:** 모니터링 일시정지

추가적으로 서버 위에 마우스를 위치하게 될 경우 개별 정보가 수치화된 팝업 메시지가 뜹니다. 서버 클릭 시 해당 서버의 요약 페이지로 이동하게 되어 자세한 내용을 파악할 수 있습니다.

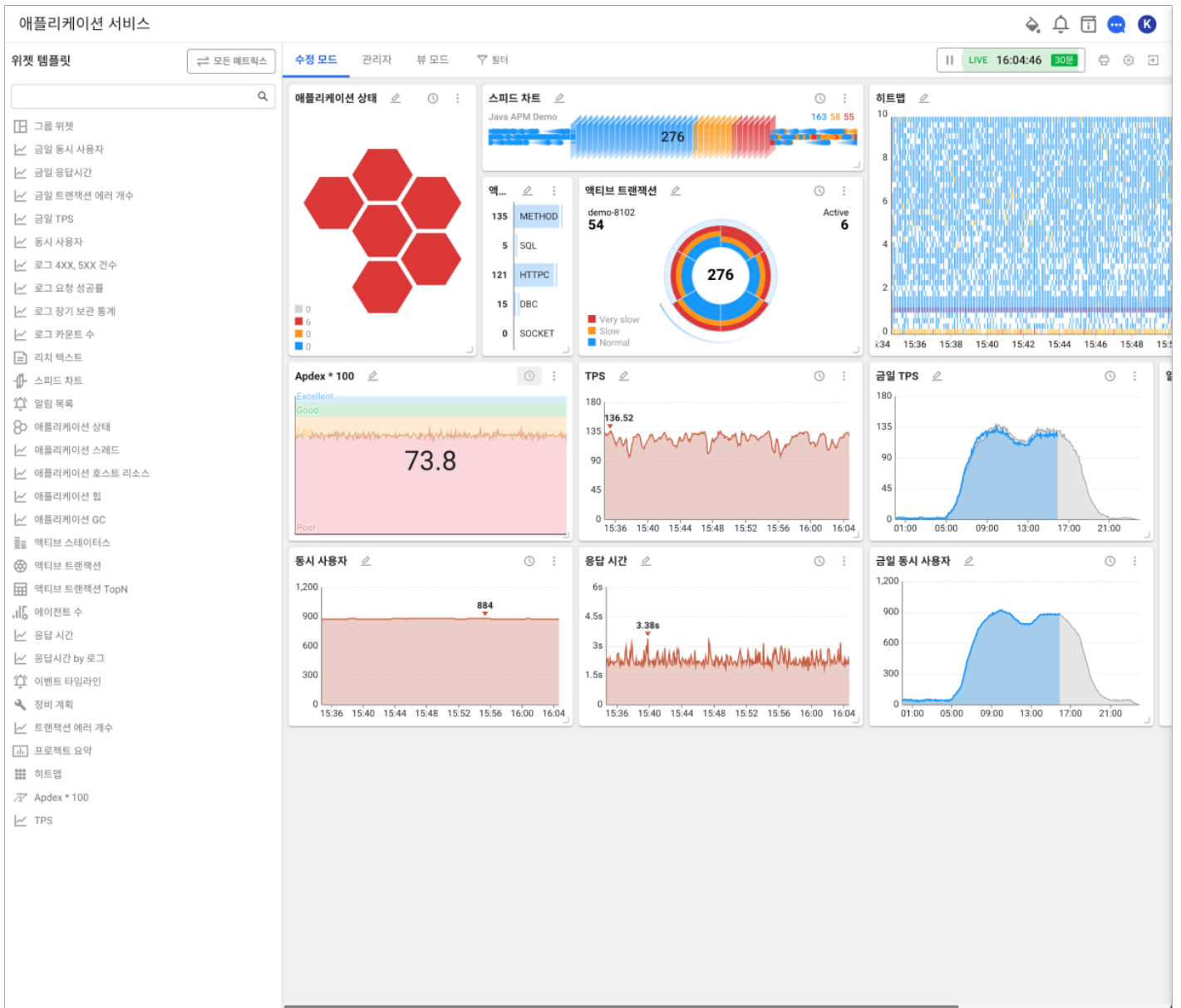
Traffic Max Value 옵션

네트워크 환경에 따라 트래픽 양이 변화할 수 있기 때문에 트래픽의 최댓값을 조정할 수 있습니다. 희망하는 트래픽 최댓값을 설정하면 값에 따라 Rx/Tx 그래프가 변경됩니다.



Flex 보드

Flex 보드는 사용자 정의형 통합 대시보드입니다. 애플리케이션, 서버, 데이터베이스, 컨테이너 등 프로젝트의 데이터로 실시간 대시보드를 만들 수 있습니다.



- 사전 구성된 템플릿을 제공해 초기 설정을 손쉽게 진행할 수 있습니다. 이를 통해 사용자가 원하는 다양한 대시보드를 구성할 수

있습니다.

- 다양한 형태의 데이터 위젯을 추가할 수 있고, 개별 위젯의 속성을 수정해 사용자가 원하는 데이터 형식을 표시할 수 있습니다.
- 데이터 필터링을 통해 사용자가 원하는 모니터링 대상을 간추릴 수 있습니다.
- 시간 범위를 설정해 중요 시간의 데이터를 확인할 수 있습니다.
- 보조 차트를 활용해 다양한 방법으로 데이터를 확인할 수 있습니다.
- 대시보드를 즐겨 찾는 메뉴로 등록할 수 있습니다.
- 개인화된 대시보드를 타 계정에 복사해 활용할 수 있습니다.

Flex 보드는 다음의 진입 경로에 따라 활용 범위가 달라집니다.

- 홈 화면 > [Flex 보드](#)
 - 위젯 생성 시 조회 가능한 모든 프로젝트를 선택 옵션으로 제공합니다.
 - 사용자 계정에 대시보드가 저장되며 다른 사용자에게 복사하기 기능을 이용해 공유할 수 있습니다.
 - 개인 계정 대시보드로 권한에 따른 영향은 없으나 읽기 전용으로 공유된 대시보드의 경우 수정할 수 없습니다.
- 홈 화면 > 프로젝트 선택 > [대시보드](#) > [Flex 보드](#)
 - 위젯 생성 시 해당 프로젝트 정보를 자동 입력합니다.
 - 프로젝트 멤버들에게 생성한 Flex 보드가 자동 공유됩니다.
 - 프로젝트 수정 권한 또는 **프로젝트 플렉스보드 편집** 권한, **Site Admin** 권한을 가진 사용자가 수정할 수 있습니다.

✔ Flex 보드를 수정할 수 있는 사용자는 다음의 주요 기능을 이용할 수 있습니다.

- 대시보드를 json 파일 형식으로 내보내거나 가져올 수 있습니다.
- 대시보드 내의 데이터 요청 및 응답 내용을 확인할 수 있습니다.
- 위젯의 설정 옵션을 json 파일 형식으로 조회하고 수정할 수 있습니다.

ⓘ 프로젝트 내 [Flex 보드](#) 메뉴에서는 대시보드 수정 권한이 있는 사용자만이 [수정 모드](#) 및 [관리자 모드](#), [필터](#) 기능에 접근할 수 있습니다. 접근할 수 있는 멤버 권한은 다음과 같습니다.

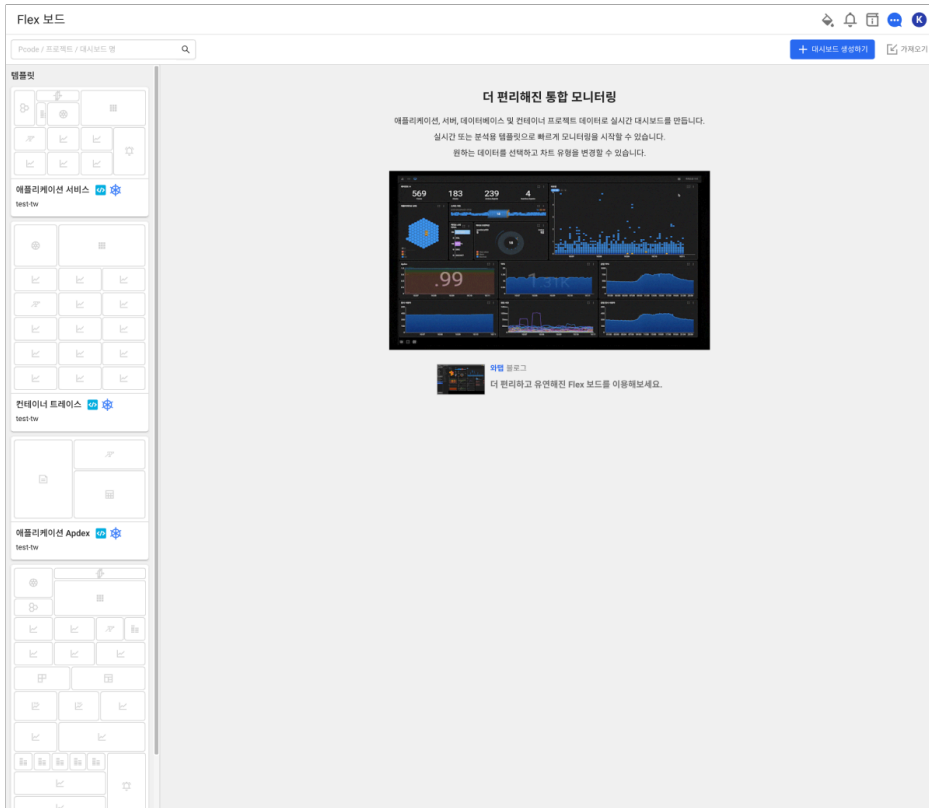
- 프로젝트 수정 권한
- **프로젝트 플렉스보드 편집** 권한
- **Site Admin** 권한
- **화면 모드** 및 **필터** 기능에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

- ⓘ • 멤버 권한에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

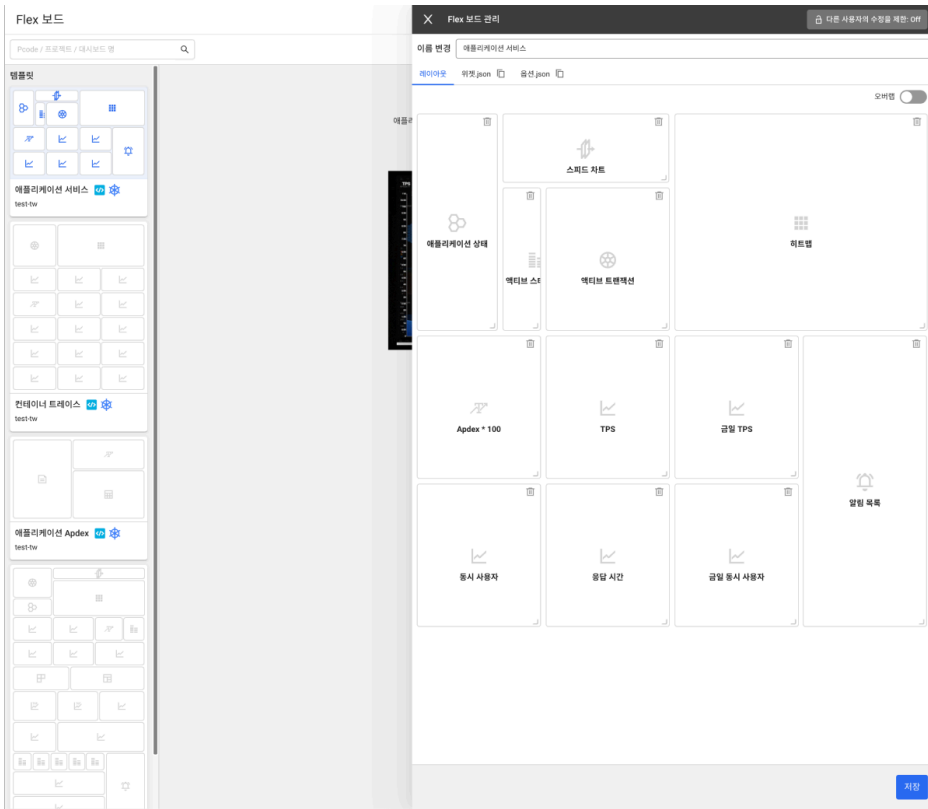
사전 템플릿 적용

제공된 사전 구성 템플릿을 이용하세요. 초기 설정을 손쉽게 진행하고 설정을 변경해 활용할 수 있습니다.

1. Flex 보드 메뉴를 선택하세요.
2. 왼쪽 템플릿 목록에서 원하는 템플릿을 선택하세요.



3. Flex 보드 관리 창이 나타나면 이름 변경에 원하는 이름을 입력하세요.



- 레이아웃 항목에 위젯을 마우스로 선택한 다음 원하는 위치로 드래그해 이동할 수 있습니다.
- 오버랩 토글 버튼을 선택해 옵션을 활성화하면 위젯을 서로 겹치게 배치할 수 있습니다.

4. 저장 버튼을 선택하세요.

선택한 템플릿 기준의 Flex 보드를 생성합니다. Flex 보드 메뉴에서 생성한 보드 목록을 확인할 수 있습니다.

Flex 보드 만들기


대시보드 생성

Flex 보드를 생성하고 위젯을 배치해 자신만의 대시보드를 만들 수 있습니다.

1. Flex 보드 메뉴에서 오른쪽 위에 **+ 대시보드 생성하기** 버튼을 선택하세요.
2. **대시보드 생성하기** 창이 나타나면 **이름** 입력 텍스트 상자에 대시 보드 이름을 입력하세요.
3. 위젯 배치 방법을 선택해 **대시보드 생성하기** 버튼을 클릭하세요.
 - **고정 레이아웃 플렉스 보드**: 픽셀 기반으로 자유롭게 위젯을 배치할 수 있습니다.
 - **반응형 플렉스 보드**: 브라우저 사이즈 기준으로 그리드 반응형 레이아웃을 제공합니다. **반응형 플렉스 보드**를 선택하면 그리드를 설정한 다음 **대시보드 생성하기** 버튼을 선택하세요.
4. **위젯 템플릿** 선택 화면에서 대시보드에 배치할 위젯을 선택하세요. 매트릭스 위젯을 추가하려면 **위젯 템플릿**의 오른쪽에 **모든 매트릭스** 버튼을 선택하세요.

- ❗ **위젯 템플릿**: 일반적인 모니터링 상황에서 중요하게 다뤄지는 지표를 간추려 사전 정의된 위젯 목록을 선택할 수 있습니다.
- **모든 매트릭스**: 사용자의 프로젝트에서 수집 중인 모든 매트릭스 데이터를 기준으로 위젯을 생성할 때 사용합니다. 매트릭스 위젯에 대한 자세한 설명은 [다음 문서](#)를 참조하세요.

5. 배치한 위젯의 위치를 이동하거나 크기를 조절하세요.
 - 배치한 위젯의 위쪽으로 마우스 커서를 이동하세요. 커서 모양이 십자 형태로 변경되면 위젯을 마우스로 클릭한 상태에서 드래그하세요. 위치를 이동할 수 있습니다.
 - 배치한 위젯의 오른쪽 아래로 마우스 커서를 이동하세요. 커서 모양이 화살표 형태로 변경되면 위젯을 마우스로 클릭한 상태로 드래그하세요. 원하는 크기로 조절할 수 있습니다.
6. 추가할 위젯을 모두 배치를 완료한 다음 **뷰 모드**를 선택해 레이아웃을 확인하세요. 레이아웃을 다시 수정하려면 **수정 모드**를 선택해 위젯의 배치를 변경하세요.


모든 과정을 완료했다면 오른쪽 위에  (**목록으로 가기**) 버튼을 선택하세요. Flex 보드 메뉴의 **보드** 목록에서 생성한 보드를 확인할 수 있습니다. 생성한 보드를 선택해 새로 생성한 Flex 보드를 확인할 수 있습니다.

- ❗ 고객의 의견을 반영해 대시보드 템플릿 또는 위젯을 추가하려고 합니다. 필요한 대시보드 템플릿 또는 위젯이 있다면

ⓘ support@whatap.io로 문의해 주세요.

Flex 보드 관리하기

Flex 보드 편집하기

Flex 보드 메뉴의 [대시보드 목록](#)에서  버튼을 선택하세요. 화면 오른쪽에 Flex 보드 관리 창이 나타납니다.

ⓘ Flex 보드 편집 기능 권한 안내

- 홈 화면 > [Flex 보드](#)
개인 계정 대시보드로 권한에 따른 영향은 없으나 읽기 전용으로 공유된 대시보드의 경우 수정할 수 없습니다.
- 홈 화면 > 프로젝트 선택 > [대시보드](#) > [Flex 보드](#)
프로젝트 수정 권한 또는 [프로젝트 플렉스보드 편집](#) 권한, **Site Admin** 권한을 가진 사용자가 수정할 수 있습니다.
- 멤버 권한에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.


The image displays the Flex Board management interface. On the left, the 'Flex 보드' (Flex Board) section shows a search bar for 'Pcode / 프로젝트 / 대시보드 명' and a list of dashboard templates. The right pane, titled 'Flex 보드 관리' (Flex Board Management), shows a search bar for '이름 변경' and a list of layouts. The main area displays a preview of a dashboard layout with various widgets: '스피드 차트' (Speed Chart), '애플리케이션 상태' (Application Status), '히트맵' (Heatmap), 'Apdex * 100', 'TPS', '금일 TPS', '동시 사용자' (Concurrent Users), '응답 시간' (Response Time), '금일 동시 사용자' (Concurrent Users Today), and '알림 목록' (Alert List). A '저장' (Save) button is visible at the bottom right.

설정할 수 있는 속성은 다음과 같습니다.



- **이름 변경:** 대시보드의 이름을 수정할 수 있습니다.
- **프로젝트:** 대시보드 위젯에 데이터를 가져올 프로젝트를 선택할 수 있습니다.

❗ 이 옵션은 홈 화면 > Flex 보드 메뉴에서만 설정할 수 있습니다.

• 레이아웃

- 위젯을 선택하고 드래그하여 위치를 이동할 수 있습니다.
- 위젯 오른쪽 아래를 마우스로 선택한 다음 드래그해 위젯의 크기를 조절할 수 있습니다.
- 위젯을 삭제하려면 위젯 오른쪽 위에  버튼을 선택하세요.
- **오버랩** 토글 버튼을 활성화하면 위젯의 배치를 겹쳐진 상태로 배치할 수 있습니다.

❗ 홈 화면 > Flex 보드 메뉴로 진입한 경우, 각 위젯마다 데이터를 가져올 프로젝트를 선택할 수 있습니다. 위젯 오른쪽 위에 + 버튼을 클릭한 다음 원하는 프로젝트를 선택하세요. 프로젝트를 검색해 선택할 수 있고, 다중 선택할 수 있습니다. 선택을 완료한 다음 **적용** 버튼을 선택하세요.

- **위젯.json**: 대시보드의 위젯 설정을 json 형식으로 불러올 수 있습니다.  버튼을 선택하면 json 내용을 복사합니다.
- **옵션.json**: 대시보드에 설정된 옵션을 json 형식으로 불러올 수 있습니다.  버튼을 선택하면 json 내용을 복사합니다.

Flex 보드 삭제하기

Flex 보드 > 대시보드 목록에서 삭제하려는 항목의 오른쪽에  버튼을 선택하세요. 확인 메시지가 나타나면 **삭제** 버튼을 선택하세요.

- ❗ • 대시보드 소유자가 대시보드를 삭제하는 경우 대시보드를 공유한 모든 사용자 계정에서도 해당 대시보드를 삭제합니다.
- 대시보드를 공유 받은 사용자가 대시보드를 삭제하면, 해당 사용자의 **대시보드 목록**에서만 삭제합니다. 원본 대시보드는 그대로 유지합니다.

메트릭스 위젯

메트릭스란?

프로젝트에서 수집 중인 숫자로된 성능 지표를 **메트릭스**라고 부릅니다. 메트릭스는 '카테고리'로 분류되며, 카테고리별 태그를 이용해 데이터를 탐색할 수 있습니다.

- **카테고리(Category)**: 관련한 지표들을 묶는 단위
- **태그(Tags)**: 수집 대상을 구분할 수 있는 고유 정보가 포함된 데이터
- **필드(Fields)**: 에이전트로부터 수집한 지표

메트릭스에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

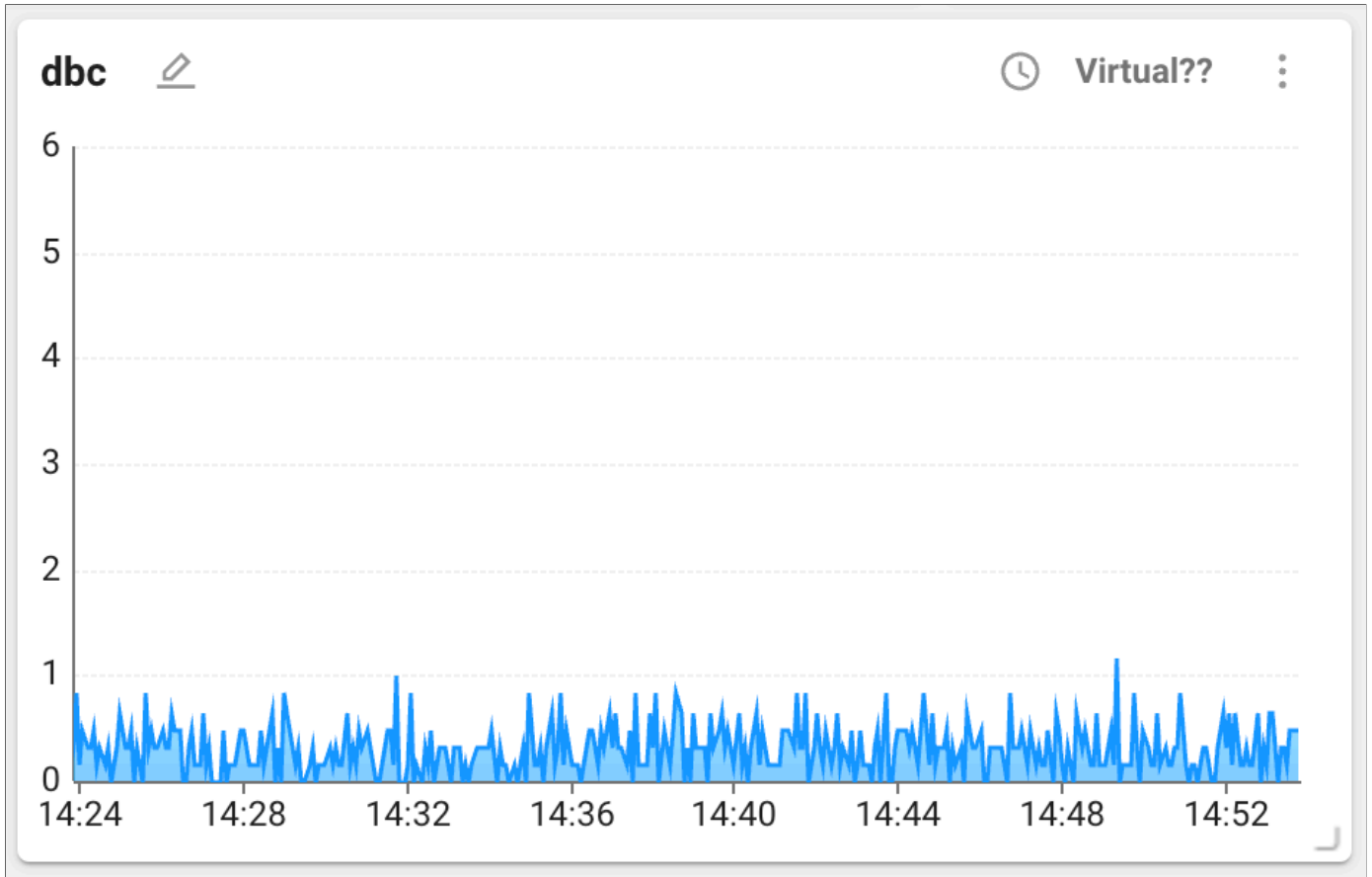
메트릭스 위젯 종류

모든 **메트릭스**에서 추가할 수 있는 위젯 유형은 카테고리에 대한 태그와 필드 정보를 나열한 테이블 형식의 위젯, 단일 필드에 대한 추이 그래프로 나뉩니다.

- **테이블 위젯**: 선택한 메트릭스 카테고리에 대한 데이터를 표 형식으로 제공합니다.

container	containerKey	host_ip	okindName	oname	onodeName	pid	Project	type	dbc	httpc	method	socket	sql	oid
prod-agent.service	1204611323	10.21.2.34	demo-okind-0	demo-8102	node-0	3788129	W_JAVA_DEMO	java	0.36	9.6	11	-	3.05	1387800924
prod-agent.service	1204611323	10.21.2.34	demo-okind-1	demo-8103	node-1	3788128	W_JAVA_DEMO	java	0.33	9.66	10.55	-	3.14	633280970
prod-agent.service	1204611323	10.21.2.34	demo-okind-1	demo-8105	node-1	3788134	W_JAVA_DEMO	java	0.3	9.19	11.37	-	2.91	-857948929
prod-agent.service	1204611323	10.21.2.34	demo-okind-1	demo-8101	node-1	3788130	W_JAVA_DEMO	java	0.28	9.93	10.82	-	3.07	-877561626
prod-agent.service	1204611323	10.21.2.34	demo-okind-0	demo-8100	node-0	3788127	W_JAVA_DEMO	java	0.34	9.71	11.38	-	2.88	-1128904592
prod-agent.service	1204611323	10.21.2.34	demo-okind-0	demo-8104	node-0	3788126	W_JAVA_DEMO	java	0.29	9.69	10.96	-	3.11	-1143239575

- **시리즈 위젯**: 선택한 메트릭스 카테고리의 선택 필드에 대한 데이터를 시리즈 차트 형식으로 제공합니다.



① 메트릭스 위젯 설정에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.


위젯 관리하기

Flex 보드에 배치한 위젯 관리를 통해 대시보드를 사용자가 원하는 대로 꾸밀 수 있습니다.

위젯 추가

이미 만들어진 Flex 보드에 위젯을 추가할 수 있습니다.

1. Flex 보드 메뉴의 **보드** 목록에서 위젯을 추가할 대시보드를 선택하세요.
2. 화면 왼쪽 위에 **수정 모드**를 선택하세요.
3. 왼쪽에 **위젯 템플릿** 목록에서 원하는 위젯을 선택하세요. 매트릭스 위젯을 추가하려면 **모든 매트릭스**를 선택한 다음 원하는 위젯을 클릭하세요.
 - 홈 화면의 Flex 보드 메뉴로 진입한 경우 위젯을 추가했다면 **+ 프로젝트 선택** 버튼을 클릭해 수집 대상 프로젝트를 선택하세요.
 - 추가할 위젯이 있다면 같은 과정을 반복하세요.


모든 과정을 완료했다면 화면 위에 **뷰 모드**를 선택해 레이아웃을 확인한 다음  (**목록으로 가기**) 버튼을 선택하세요.

위젯 속성 변경


Flex 보드 메뉴의 **보드** 목록에서 위젯 속성을 변경할 보드를 선택하세요. **수정 모드**로 진입합니다.

위젯 이름 변경

이름을 변경할 위젯의 이름 오른쪽에  버튼을 선택하세요. 위젯의 **제목**, **폰트 크기**, **색상**을 설정한 다음 **저장** 버튼을 선택하세요.

- ✔ • 저장 시 **전체 위젯에 적용** 토글 버튼의 기능을 활성화하면 폰트 크기와 색상을 다른 위젯에도 적용합니다.
 - 위젯의 제목을 잠금 설정하려면  버튼을 선택한 다음 **저장** 버튼을 클릭하세요.

시간 설정

시간을 설정하려는 위젯의 오른쪽 위에  버튼을 선택하세요. **시간 선택** 창이 나타납니다.

- 대시보드 화면에 설정한 시간을 적용하려면 **대시보드 설정을 따름**을 체크하세요. 대시보드의 시간 설정은 오른쪽 상단에 위치합니다.
- 사용자가 원하는 시간을 설정을 적용하려면 **대시보드 설정을 따름**을 체크 해제하세요. < 또는 > 버튼을 이용해 원하는 시간을 설정하세요.

시간 설정을 완료했다면 ✕ 버튼을 선택하세요.

ⓘ 위젯의 데이터 유형에 따라서 시간 설정 기능을 지원하지 않을 수 있습니다.

출력 데이터 옵션 설정

차트형 위젯의 출력 데이터 옵션을 설정해 사용자가 원하는 데이터를 선택할 수 있습니다. 위젯의 오른쪽 위에 ⋮ 버튼을 선택하세요.

- 프로젝트, 에이전트, 애플리케이션 등의 종류를 선택해 데이터를 필터링할 수 있습니다.
- 개별, 병합 데이터를 선택해 차트에 표시되는 그래프의 유형을 변경할 수 있습니다.
- ⋮ > ⚙️을 선택하세요. **차트 설정** 창을 통해 세부 옵션을 변경할 수 있습니다. 설정할 수 있는 옵션은 다음과 같습니다.
 - **차트 유형**: 집계하는 현재 수치를 차트에 표시할 수 있는 옵션입니다.
 - **y축 차트 최대값**: y축에 차트 최대값을 **자동** 또는 **고정**으로 선택할 수 있습니다.
 - **수평선 설정**: **+ 추가** 버튼을 선택해 임계치 또는 범위를 수평선으로 표시할 수 있습니다. 여러 개를 추가해 적용할 수 있습니다. 수평선을 추가한 다음에는 **적용** 버튼을 선택해야 차트에 반영됩니다.
 - **차트 최대값 표시**: 차트에 표시되는 그래프의 최대값을 표시합니다.
 - **보조 차트**: 위젯의 주요 차트에 보조 차트를 추가 설정할 수 있습니다. 보조 차트의 종류를 선택한 다음 레이아웃, 크기, 데이터 병합 여부를 선택하세요. 다른 위젯에도 공통 적용하려면 **전체 위젯에 적용** 버튼을 선택하세요. 보조 차트는 데이터를 다양한 방법으로 보고 싶을 때 유용합니다.

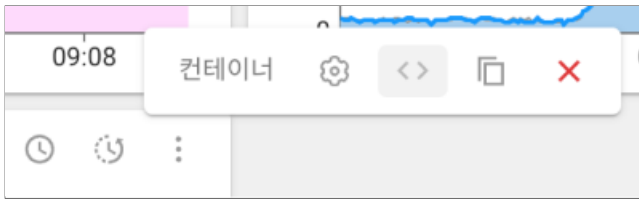
옵션 설정을 모두 완료했다면 **차트 설정** 창의 왼쪽 위에 ✕ 버튼을 클릭하거나 **차트 설정** 창 영역 밖을 클릭하세요.

ⓘ 위젯의 데이터 유형에 따라서 선택할 수 있는 옵션은 다를 수 있습니다.

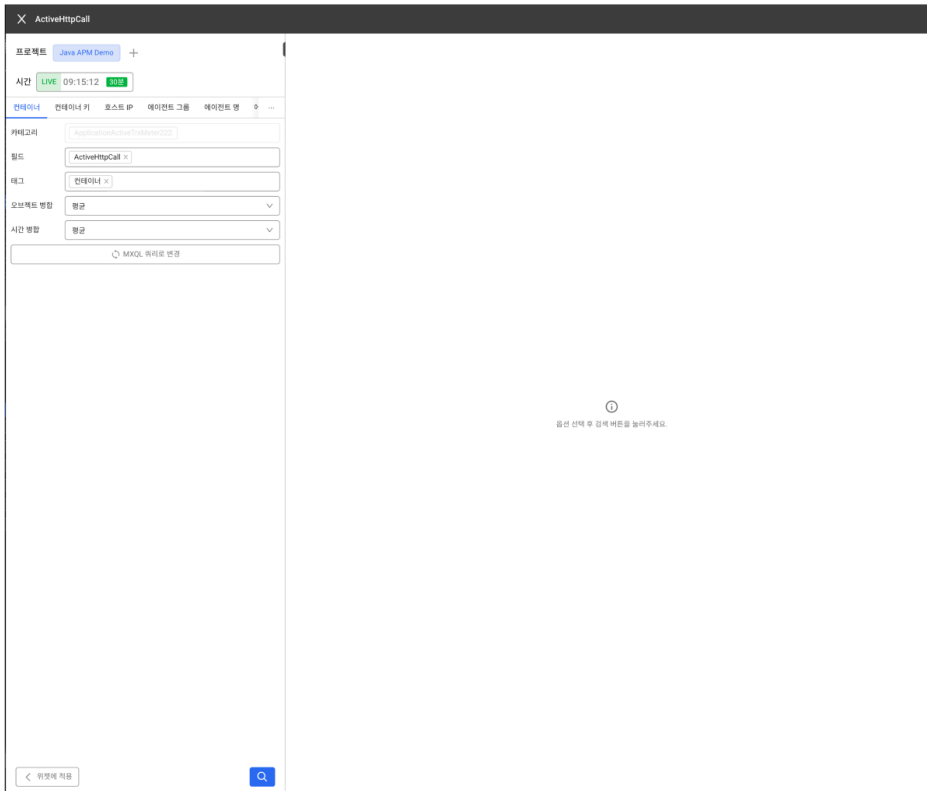
메트릭스 위젯 데이터 변경

메트릭스 위젯의 데이터 조회 조건을 변경할 수 있습니다.

1. Flex 보드 > 수정 모드에서 변경할 위젯의 오른쪽 위에 ⋮ 버튼을 선택하세요.




2. <> 버튼을 선택하세요. 데이터 설정 편집 창이 나타납니다.



3. 다음을 참조해 설정을 변경한 다음 < 위젯에 적용 > 버튼을 선택하세요.
 - 위젯 생성 시 기본 생성되는 메트릭스 옵션이 탭에 표시됩니다.
 - 메트릭스 옵션에는 **카테고리**와 **필드**, **태그**가 있습니다.
 - **카테고리** 항목은 현재 변경 기능을 제한합니다.
 - **필드**, **태그** 항목은 복수 선택할 수 있습니다. 선택한 태그 옵션으로 차트 데이터를 그룹화합니다.
 - 🔍 버튼을 선택해 원본데이터를 조회할 수 있습니다.
 - **오브젝트 병합** 및 **시간 병합** 항목에 대한 자세한 내용은 [데이터 병합 옵션](#)을 참조하세요.

데이터 병합 옵션

Flex 보드의 [모든 메트릭스](#) 목록에서 배치한 메트릭스 위젯은 데이터 병합 옵션을 제공합니다.

1. 수정 모드에서 [모든 메트릭스](#) 버튼을 선택해 [위젯 템플릿](#) 목록을 [모든 메트릭스](#) 목록으로 변경하세요.
2. 메트릭스 위젯을 레이아웃에 배치하세요.
3. 메트릭스 위젯 오른쪽 위에  버튼을 선택하세요.
4. 태그(예: 에이전트 명) 옵션을 선택하면 데이터 병합 옵션이 나타납니다. 위젯의 크기에 따라 메트릭스 옵션의 위치가 다를 수 있습니다.



데이터 병합은 [오브젝트 병합](#)과 [시간 병합](#) 방법을 제공합니다.

- **오브젝트 병합**

좌측에서 선택한 태그(예: 에이전트 명)를 기준으로 차트 데이터를 그룹화할 때 사용합니다. 이때 서로 다른 필드(예: CPU)값을 가진 데이터들 중에서 태그가 일치하는 경우 해당 데이터를 병합하는 방법입니다.

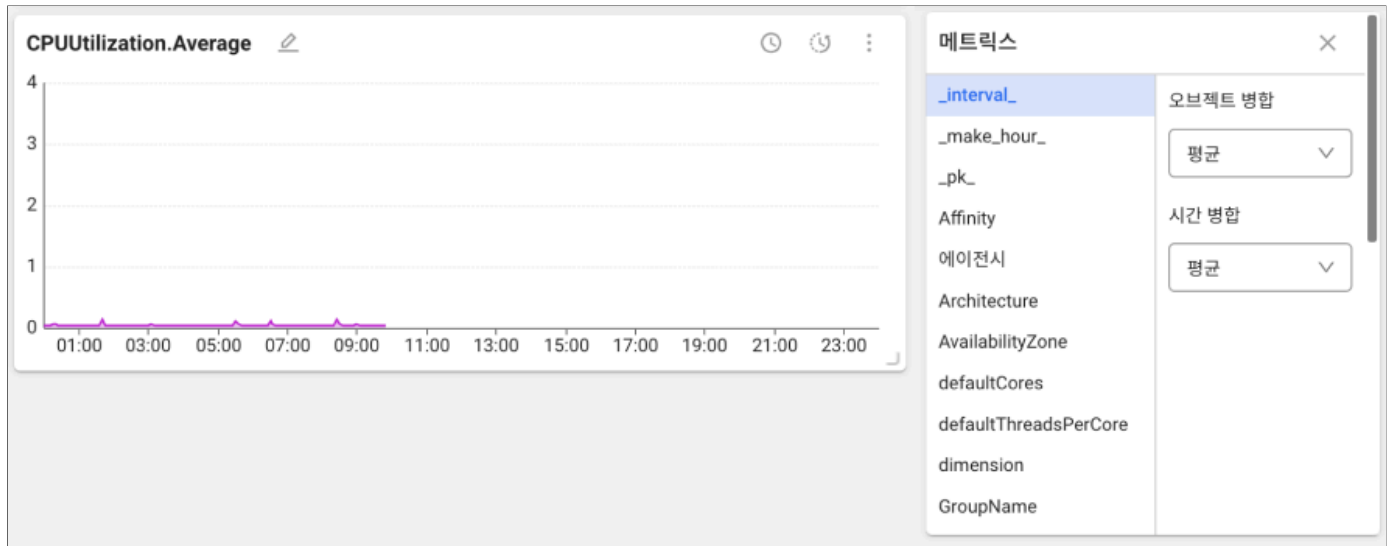
- **시간 병합**

조회 시간이 긴 경우 주로 사용합니다. 원본 데이터에서 필드 값이 같은 데이터끼리 시간 범위에 따라 일정한 시간 간격(5분 또는 1시간)으로 데이터를 병합합니다. 이 병합 방법을 시간 병합이라고 합니다.

- **AWS CloudWatch 메트릭스**

AWS 모니터링 지표의 경우 통계 방식이 필드명 뒤에 suffix(접미사) 형식으로 추가됩니다. 데이터 병합 기본값은 이 suffix를

참조하고 있습니다.



위젯 복사

1. 위젯의 오른쪽 위에 버튼을 선택하세요.
2. 버튼을 선택하세요.
3. 복사 창이 나타나면 + 위젯 추가를 선택하세요.
4. 목록에 위젯의 이름을 변경하세요.
5. 적용 버튼을 선택하세요.

수정 모드 화면에서 복사한 위젯을 확인할 수 있습니다.

위젯 삭제

1. 위젯의 오른쪽 위에 버튼을 선택하세요.
2. 버튼을 선택하세요.
3. 확인 메시지 창이 나타나면 삭제 버튼을 선택하세요. 삭제를 취소하려면 취소 버튼을 선택하세요.


Flex 보드 화면 모드

Flex 보드의 화면 모드에 따라 제공하는 기능을 설명합니다.

- ❗ • 프로젝트 내 **Flex 보드** 메뉴에서는 대시보드 수정 권한이 있는 사용자만이 **수정 모드** 및 **관리자** 모드, **필터** 기능에 접근할 수 있습니다. 접근할 수 있는 멤버 권한은 다음과 같습니다.
 - 프로젝트 수정 권한
 - 프로젝트 플렉스보드 편집 권한
 - **Site Admin** 권한
- 멤버 권한에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

화면 모드

Flex 보드는 다음과 같은 화면 모드를 제공합니다. 화면 모드에 따라 설정할 수 있는 기능이 다릅니다.

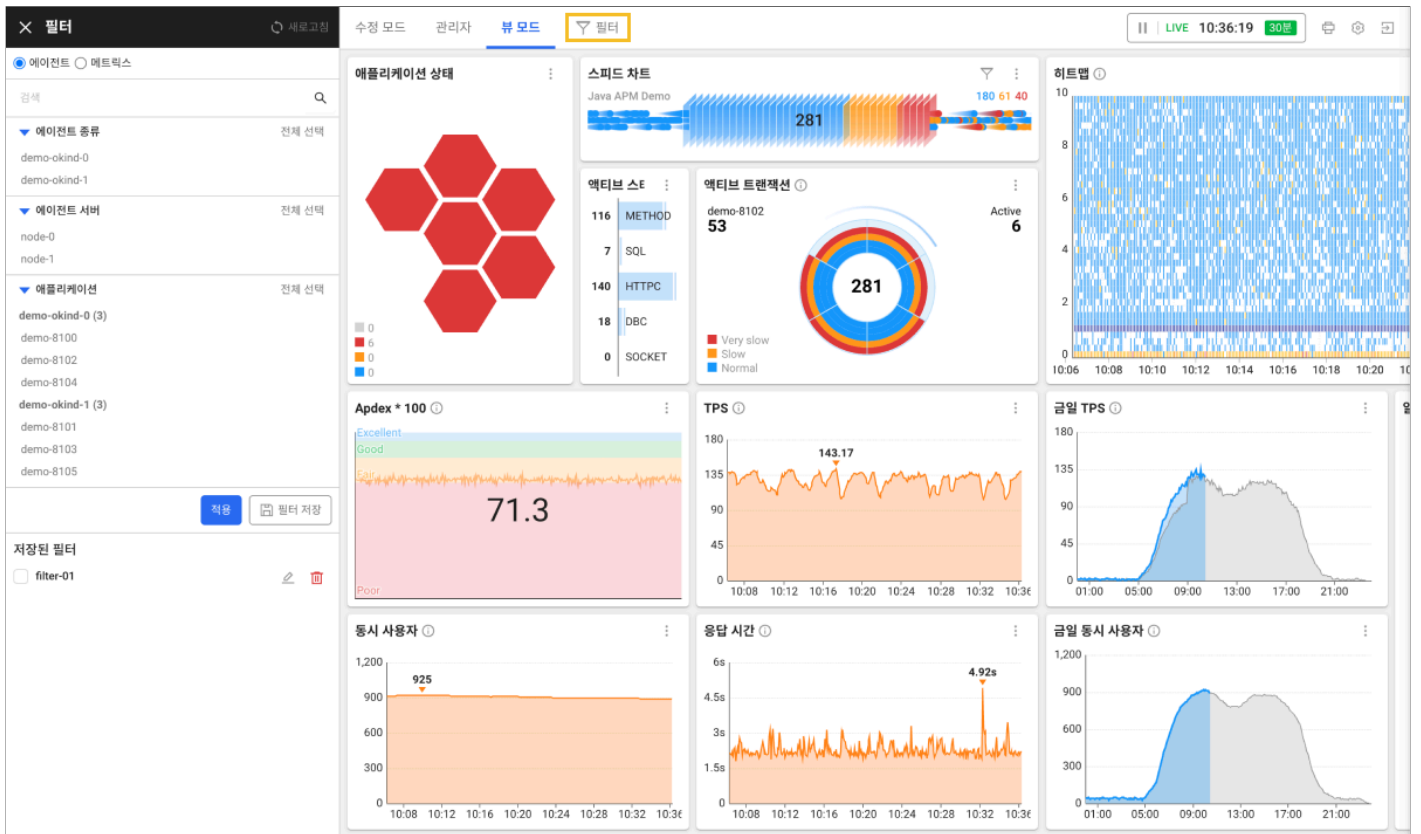
- **수정 모드**: 위젯 템플릿 목록에서 Flex 보드의 레이아웃에 위젯을 배치하거나 위젯을 수정, 삭제, 위치 조정할 수 있습니다.
- **관리자**: 위젯의 세부 속성을 json 형태로 관리할 수 있습니다. 레이아웃에 배치한 위젯의 오른쪽 위에 위치한  버튼을 선택하세요.
- **뷰 모드**: 위젯 배치, 크기 조절, 세부 옵션 등의 설정을 완료한 다음 대시보드와 같이 각 위젯의 데이터를 실시간으로 모니터링할 수 있습니다.

Flex 보드에서는 다음의 공통 기능을 사용할 수 있습니다.

- 데이터 필터링
- 실시간 데이터 조회 범위 설정
- 인쇄 모드
- Flex 보드 관리
- 데이터 병합 옵션

데이터 필터링

Flex 보드는 수백 가지의 종류의 데이터를 다룹니다. 데이터 필터링 기능을 이용해 모니터링하려는 대상을 간추려 Flex 보드를 구성하세요.



1. 화면 위에 ① 필터를 선택하세요.

2. 화면 왼쪽으로 ② 필터 창이 나타납니다.

- 에이전트 옵션을 선택했다면 에이전트 종류 또는 애플리케이션 목록 기준으로 필터링 대상을 선택할 수 있습니다. 필터링 대상을 모두 선택하려면 전체 선택을 선택하세요. 필요한 경우 검색 기능을 이용해 선택할 수 있습니다.
- 매트릭스 옵션을 선택했다면 카테고리 옵션에서 프로젝트, 에이전트 유형에 따라 필터링 대상을 선택할 수 있습니다. 카테고리 옵션은 + And를 선택해 추가할 수 있습니다. 포함, 제외 옵션을 선택하면 문자열로 필터링 대상을 자동 선택합니다.

3. 필터링 대상 선택을 완료했다면 적용 버튼을 선택하세요.

사용자가 설정한 필터링 설정을 저장해 이용하려면 필터 저장 버튼을 선택하세요. 필터 이름을 입력하고 저장을 선택하세요. ③ 저장된 필터는 필터 창 하단에 나타납니다.

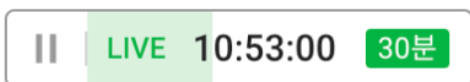
필터링 조건은 에이전트 타입과 매트릭스 타입으로 구분합니다.

타입	에이전트	메트릭스
선택 옵션	와탭 프로젝트 모니터링 대상 (애플리케이션, 서버, 데이터베이스, 컨테이너 및 쿠버네티스 POD와 NODE)	에이전트를 포함한 모든 메트릭스 태그
적용 범위	모든 위젯	메트릭스 데이터를 사용하는 모든 위젯
필터링 조건	체크박스	일치 , 포함 , 제외 방식

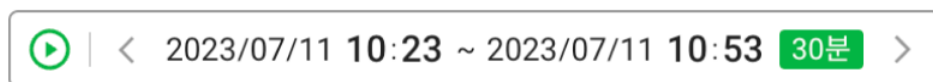
- ① • 에이전트 타입은 기본적인 모니터링 대상만을 선택 옵션으로 제공합니다.
 - 메트릭스 타입은 프로젝트에서 수집 중인 모든 메트릭스 데이터의 태그를 선택 옵션으로 제공합니다. 메트릭스 타입은 클라우드 모니터링과 같이 에이전트가 아닌 형태로 데이터를 수집한 후 필터링을 적용할 때 유용합니다.
 - 메트릭스에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

실시간 데이터 조회 범위 설정

Flex 보드 메뉴의 화면 오른쪽 위에 UI 요소를 이용해 위젯에 데이터를 출력하는 시간을 설정할 수 있습니다.




II 버튼을 선택하면 실시간 데이터 조회를 일시 정지하고 다음과 같이 조회 시간을 설정할 수 있습니다.



- 가장 오른쪽의 녹색 배경의 시간 버튼을 선택하세요. 다양한 시간 설정을 선택할 수 있는 옵션이 나타납니다. 원하는 시간 설정을 선택하세요.
- < 또는 > 버튼을 클릭하면 설정된 시간 범위 만큼 조절할 수 있습니다.
- 날짜와 시간 텍스트 영역을 클릭하면 날짜와 시간을 선택할 수 있는 옵션이 나타납니다.
- 조회 시간 설정을 모두 완료했다면 ▶ 버튼을 선택하세요. 실시간 데이터 조회를 시작합니다.


인쇄하기


Flex 보드 화면을 PDF로 저장해 인쇄할 수 있습니다. Flex 보드 화면의 오른쪽 위에  버튼을 선택하세요. 화면을 인쇄 모드로 전환합니다. 다음의 옵션을 설정한 다음 [PDF 다운로드](#)를 선택하세요.

- **필터 옵션 보기**: 화면에 필터 옵션을 켜거나 끌 수 있습니다.
- **가로/세로 방향으로 변환**: 화면을 가로 또는 세로로 변환할 수 있습니다.


인쇄 모드를 종료하려면 오른쪽 위에 **×** [인쇄모드 종료](#)를 선택하세요.

Flex 보드 관리

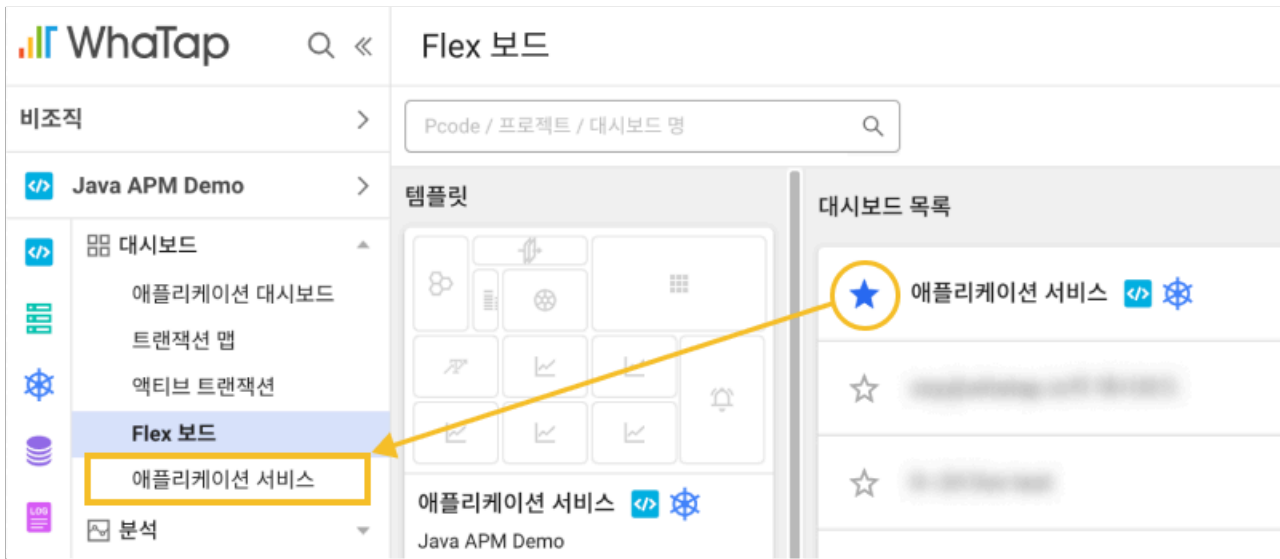
Flex 보드의 레이아웃을 변경하거나 위젯의 위치 변경, 크기 조절, 이름 변경 등의 관리 기능을 제공합니다. Flex 보드 화면의 오른쪽 위에  버튼을 선택하세요. [Flex 보드 관리](#) 창이 나타납니다.

- **이름 변경**: Flex 보드의 이름을 변경할 수 있습니다. 변경하려는 이름을 입력하세요.
- **레이아웃**: 위젯의 배치를 변경하거나 위치 및 크기를 조절할 수 있습니다. 배치한 위젯을 삭제하려면  버튼을 클릭하세요. [오버랩](#) 토글 버튼을 선택해 옵션을 활성화하면 위젯을 서로 겹치게 배치할 수 있습니다.
- **다른 사용자의 수정을 제한**: 다른 사용자가 해당 Flex 보드의 수정을 할 수 없도록 설정합니다. 수정 권한이 있는 멤버만 수정 또는 삭제, 위젯을 편집할 수 있습니다. 버튼을 클릭하면 [다른 사용자의 수정을 제한](#): on으로 변경됩니다.
- **위젯 json**: Flex 보드에 포함된 위젯을 json 형태로 편집해 관리할 수 있습니다.
- **옵션 json**: Flex 보드의 설정을 json 형태로 편집해 관리할 수 있습니다. 프로젝트 정보, Flex 보드 필터, 시간 선택 등의 설정값을 편집할 수 있습니다.

모든 설정을 완료한 다음에는 화면 오른쪽 아래에 [저장](#) 버튼을 클릭하세요.

- ① • **위젯 json, 옵션 json** 기능은 대시보드 관리자 권한의 사용자에게만 제공합니다.
 - [Flex 보드 관리](#) 기능은 [대시보드](#) > [Flex 보드](#) 메뉴에서 [보드 목록](#)의  버튼을 선택해 진입할 수도 있습니다.

대시보드 즐겨찾기로 등록

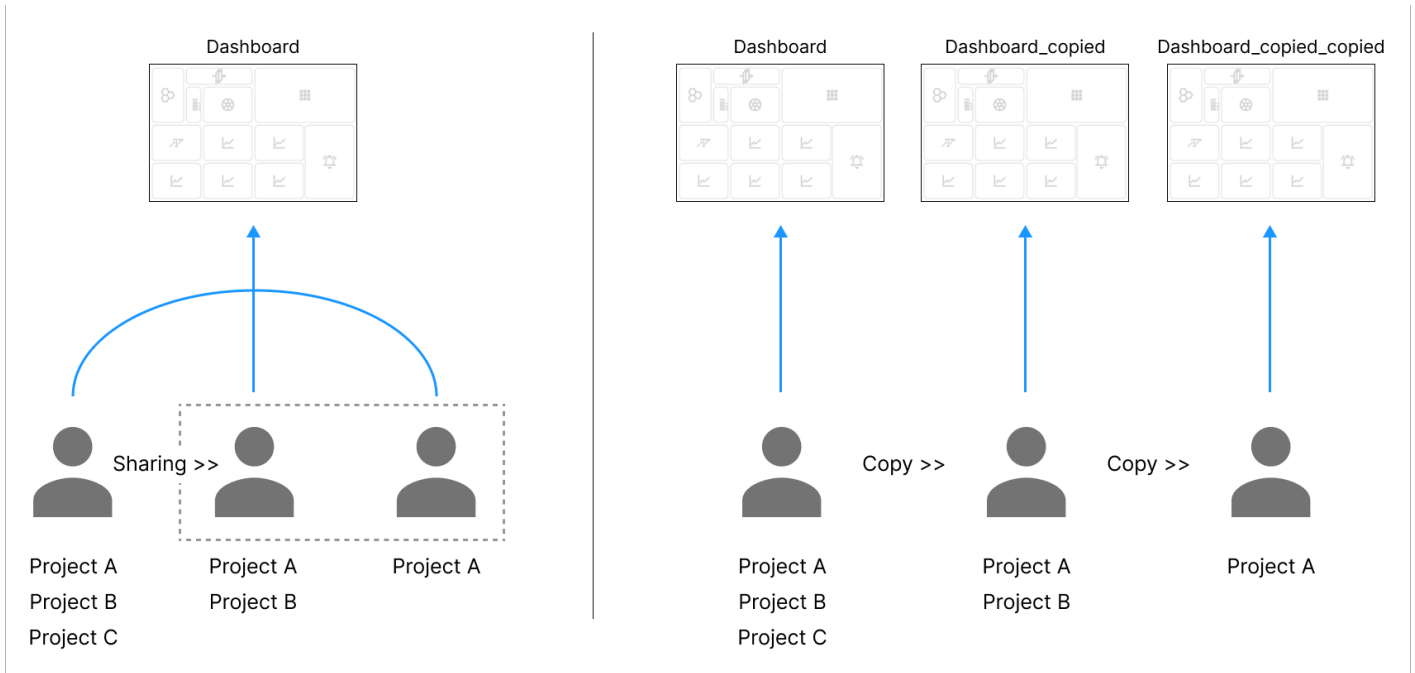


사용자가 생성한 Flex 보드는 [대시보드](#) 메뉴 하위에 즐겨찾는 메뉴로 등록할 수 있습니다. [대시보드](#) > [Flex 보드](#) 메뉴에서 [대시보드 목록](#)의 ☆ 버튼을 선택하세요. 즐겨찾기로 설정된 항목은 ★으로 변경됩니다.

Flex 보드 공유하기

통합 Flex 보드 메뉴에서 생성한 대시보드를 다른 멤버와 공유하거나 복사해 재사용할 수 있습니다.

공유와 복사의 차이



- 대시보드를 공유한 경우 공유한 멤버는 모두 같은 대시보드를 볼 수 있습니다.
- 대시보드를 다른 멤버 또는 나에게 복사한 경우 복사된 별도의 대시보드를 볼 수 있습니다.
- **읽기 전용**으로 대시보드를 공유 또는 복사 받은 멤버는 대시보드를 수정할 수 없지만 **수정 모드**로 공유 또는 복사된 대시보드는 수정할 수 있습니다.
- **읽기 전용**으로 대시보드를 공유받은 멤버는 읽기 전용으로 대시보드를 공유할 수 있으며 복사할 수 있습니다.
- 대시보드에 포함된 프로젝트 중 최소 1개 프로젝트에 초대된 멤버에게 대시보드를 공유할 수 있습니다. 공유 또는 복사 받을 멤버가 프로젝트에 소속되어 있는지 확인하세요.




ⓘ 대시보드 공유 및 복사 기능이 업데이트됐습니다

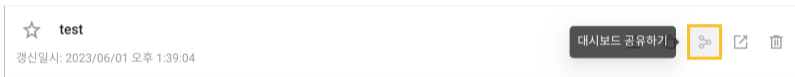
이전에는 공유 또는 복사 받을 멤버에게 수정 권한이 있어야 했지만, [Service 2.3.0 릴리스](#) 이후 권한에 상관없이 프로젝트에 소속되어 있기만 한다면 복사 또는 공유할 수 있습니다. 단, 공유 받은 대시보드의 프로젝트 중 **조회 분석** 권한이 없는 프로젝트는 데이터를 조회할 수 없습니다. 멤버 권한에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

Flex 보드 공유하기

사용자가 생성한 Flex 보드를 다른 멤버와 공유해 동일한 대시보드를 볼 수 있습니다. 이를 통해 업무를 공유할 수 있습니다. 공유한 대시보드를 수정한 경우 공유받은 모든 멤버는 동일한 대시보드를 확인할 수 있습니다.

ⓘ 이 기능은 **통합 Flex 보드** 메뉴에서만 이용할 수 있습니다. 프로젝트의 **Flex 보드** 메뉴에서는 이용할 수 없습니다.

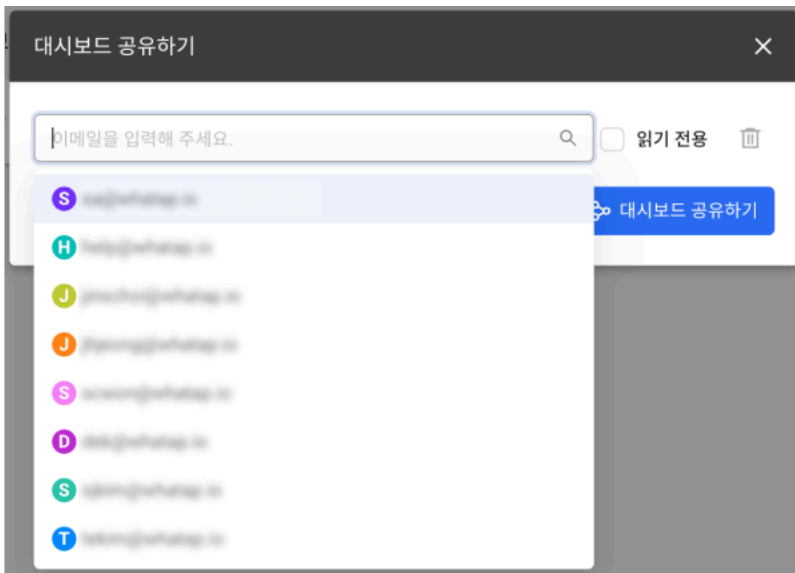
1. **통합 Flex 보드** 메뉴의 **대시보드 목록**에서 공유하려는 대시보드의  버튼을 선택하세요.



2. **대시보드 공유하기** 창이 나타나면 **+ 계정** 버튼을 선택하세요.



3. 대시보드를 공유할 멤버를 선택하세요.



- 공유 대상을 추가하려면 + **계정** 버튼을 선택하세요. 멤버를 추가로 선택할 수 있습니다.
- 대시보드에 포함된 프로젝트 중 최소 1개 프로젝트에 초대된 멤버에게 대시보드를 공유할 수 있습니다. 공유 또는 복사 받을 멤버가 프로젝트에 소속되어 있는지 확인하세요.

4. **대시보드 공유하기** 버튼을 선택하세요.



- **읽기 전용**을 선택하면 공유받은 멤버는 대시보드를 수정할 수 없습니다.
- 공유받을 멤버 모두에게 읽기 전용으로 공유하려면 **읽기 전용(전체)**를 선택하세요.

대시보드를 공유한 항목은 **대시보드 목록**에서 **공유** 태그가 표시된 것을 확인할 수 있습니다. **공유** 태그에 마우스를 오버하면 대시보드를 공유한 멤버에 대한 정보를 확인할 수 있습니다. 읽기 전용으로 공유한 멤버에게는 **읽기 전용** 태그가 표시됩니다.

대시보드를 공유받은 경우	대시보드를 공유한 경우(대시보드 소유자)
	

✔ 대시보드 공유 조건

- 대시보드 공유 기능은 홈 화면 > [통합 Flex 보드](#) 메뉴에서만 이용할 수 있습니다.
- 누구나 자신의 대시보드를 공유할 수 있으며, 공유받은 대시보드를 다시 공유하거나 복사할 수 있습니다.
- [읽기 전용](#)으로 대시보드를 공유받은 멤버는 대시보드를 수정할 수 없지만 [수정 모드](#)로 공유받은 대시보드는 수정할 수 있습니다.
- 대시보드 소유자가 대시보드를 삭제하면 대시보드를 공유받은 모든 멤버 계정에서도 해당 대시보드가 삭제됩니다.
- 대시보드를 공유받은 멤버가 대시보드를 삭제하면, 해당 멤버의 [대시보드 목록](#)에서만 삭제됩니다. 원본 대시보드는 그대로 유지합니다.
- 공유 받은 대시보드의 프로젝트 중 [조회 분석](#) 권한이 없는 프로젝트는 데이터를 조회할 수 없습니다.

Flex 보드 복사하기

사용자가 생성한 Flex 보드를 복사해 다른 멤버에게 전달할 수 있습니다.

[통합 Flex 보드](#) 메뉴의 [대시보드 목록](#)에서  버튼을 선택하세요. [나에게 복사](#) 또는 [다른 사람에게 복사](#) 옵션을 선택하세요.

- [나에게 복사](#) 옵션을 선택하면 [대시보드 목록](#)에 '_copied' 접미어가 붙은 항목이 추가됩니다.
- [다른 사람에게 복사](#) 옵션을 선택하면 + [계정](#)을 선택하세요.




다른 멤버의 이메일을 선택한 다음 [대시보드 복사하기](#) 버튼을 클릭하세요. 복사 받은 멤버의 [대시보드 목록](#) 목록에 '_copied' 접미어가 붙은 항목이 추가됩니다.

JSON 파일로 공유하기


Flex 보드 설정을 JSON 파일로 저장하고 다른 멤버에서 전달하거나 다른 멤버의 설정을 가져올 수 있습니다.

내보내기

1. [통합 Flex 보드](#) 또는 프로젝트의 [Flex 보드](#) 메뉴로 이동하세요.
2. [대시보드 목록](#)에서  버튼을 선택하세요.
3. JSON 파일이 다운로드되면 공유할 다른 멤버에게 전달하세요.

가져오기

1. [통합 Flex 보드](#) 또는 프로젝트의 [Flex 보드](#) 메뉴로 이동하세요.

2. 화면 오른쪽 위에  가져오기 버튼을 선택하세요.
3. 다운로드한 JSON 파일을 선택하세요.

ⓘ 이 기능은 프로젝트의 수정 권한을 소유한 멤버만 이용할 수 있습니다.

메트릭스

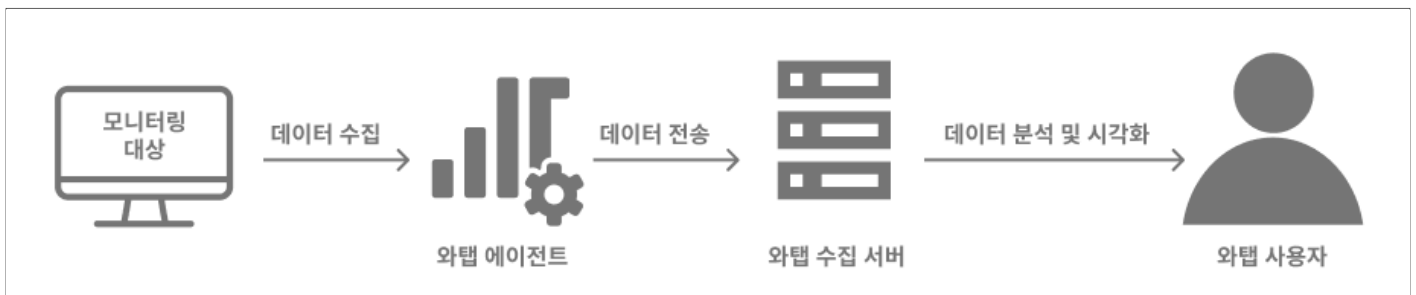
메트릭스란?

와탭은 모니터링 대상으로부터 데이터를 수집해서 사용자에게 제공합니다. 에이전트로부터 수집되는 데이터를 **메트릭스**라고 표기합니다.

메트릭스는 사용자 환경을 한 눈에 살펴볼 수 있는 기준 요소를 제공합니다. 예를 들어 서버별 메모리 사용률 평균, DB 평균 연결 시간 등을 원본 데이터 목록이나 시각화한 차트 뷰를 통해 간편하게 확인할 수 있습니다. 문제 요소를 찾은 후에는 로그와 트레이스 등을 통해 상세 분석을 확인할 수 있습니다.

메트릭스는 또한 사용자 환경의 스케일을 조절하는 것에도 도움을 줍니다. 자원 사용량 통계를 통해 필요 자원량을 확정하는 것은 성능 향상과 비용 효율성 측면에서 중요한 기준입니다.

와탭의 메트릭스 수집 방식



와탭 에이전트는 모니터링 대상으로부터 모니터링 지표를 수집해 메트릭 데이터의 형태로 와탭 수집 서버에 전송합니다. 와탭 수집 서버는 관련 데이터를 카테고리별로 저장하고 관리합니다.

와탭의 수집 서버는 다양한 모니터링 대상에서 메트릭스를 수집합니다. 사용자는 원하는 메트릭스에 접근하기 위해 해당 상품별 안내 화면으로 이동해 기술된 과정을 따라야 합니다.

예를 들어 [Server](#)를 모니터링하고 싶다면 먼저 와탭 에이전트를 설치해야 합니다. [다음 문서](#)를 참조하세요. 관련 메트릭스 지표 안내 또한 [다음의 상품별 페이지](#)에서 확인할 수 있습니다.

와탭의 메트릭스 구성 요소

와탭의 **메트릭스**는 다음의 정보들로 구성되어 있습니다.

- **Category:** 관련된 지표들을 묶는 단위로 메트릭스를 구분하는 Key를 의미합니다.
- **Tags:** 수집 대상을 구분할 수 있는 고유 정보를 포함하는 데이터입니다. 변경이 드문 IP, Oname, Host 정보 등의 항목을 저장합니다. Map 형태로 Multi Tag가 존재합니다.
- **Fields:** 에이전트로부터 수집된 모든 지표 값을 저장합니다. Map 형태로 Multi Field가 존재합니다.
- **Time:** 메트릭스가 수집된 시간입니다.
- **Oid:** 메트릭스를 수집한 에이전트의 고유 번호입니다.
- **Oname:** 메트릭스를 수집한 에이전트의 명칭입니다.

메트릭스 데이터 조회 및 시각화

와탭은 사용자가 지정한 조건에 따라 수집한 원본 데이터 목록과 편의성을 위해 다양하게 시각화한 차트를 다음과 같이 제공합니다. 메트릭스의 원본 데이터를 조회할 수 있는 **메트릭스 조회**, 시각화한 차트를 통해 메트릭스 데이터를 조회할 수 있는 **메트릭스 차트**, 시가 학습한 메트릭스 지표의 패턴과 비교해 예상 패턴을 벗어난 이상을 탐지할 수 있는 **메트릭스 이상 탐지** 메뉴를 확인해 보세요.

The screenshot displays the Metrics tool interface, divided into several sections:

- 메트릭스 조회 (Metrics Query):** A table listing metrics with columns for Time, Oid, Tags (alias, container, containerKey, host_ip, okindName, oname, onodeName, pid, type), and Fields (dbc, http, method, socket, sql, s/s). It includes search filters and a CSV export button.
- 메트릭스 이상 탐지 (Metrics Anomaly Detection):** A panel for detecting anomalies in metrics like ApplicationActiveStat, DbConnection, HttpCall, and Socket.
- 메트릭스 차트 (Metrics Chart):** A central area with an 'Overlay Chart' and several sub-charts: TPS (Transaction Per Second), 인스턴스 응답 시간 (Instance Response Time), Think Time, 서비스 시간 (Service Time), Call, and Sql. Each chart shows a time-series plot with a peak value highlighted (e.g., 22.05 for TPS, 92.87% for Think Time).
- Left Sidebar:** A navigation menu with categories like 트랜잭션 (Transaction), TPS, 인스턴스 응답 시간, Think Time, 서비스 시간, TX 건수, TX Error 건수, 트랜잭션별 SQL 시간, 트랜잭션별 HTTP 호출 시간, 트랜잭션별 DB 연결 시간, 액티브 트랜잭션, 액티브 스태티스, SQL, HTTP 호출, 사용자, CPU, 메모리, 힙, GC, and 디스크.

서버 지표

서버 모니터링 지표를 다음과 같이 안내합니다.

server_base

서버 자원 지표입니다.

- 수집 간격 : 5초
- 통계 데이터 : 5분, 1시간

Tags

태그명	설명	비고
cpu_cores	서버 코어 수	-
host_ip	서버 IP	-
oname	서버 이름	-
okindName	서버 종류명	-
os	OS 유형 linux 또는 window	-

Fields

필드명	단위	설명	비고
cpu	퍼센트	CPU 전체 사용률	공통
cpu_c1	퍼센트	cpu c1 state 사용률	윈도우

필드명	단위	설명	비고
cpu_c2	퍼센트	cpu c2 state 사용률	윈도우
cpu_c3	퍼센트	cpu c3 state 사용률	윈도우
cpu_ctxt	소수	context switching 사용률	리눅스
cpu_dpc	퍼센트	CPU DPC 시간 비율	윈도우
cpu_idle	퍼센트	CPU idle 비율	공통
cpu_interrupt	퍼센트	cpu interrupt	리눅스
cpu_iowait	퍼센트	CPU iowait 비율	리눅스
cpu_irq	퍼센트	CPU IRQ 사용률	리눅스
cpu_load1	소수	1분 평균 Load Average	리눅스
cpu_load5	소수	5분 평균 Load Average	리눅스
cpu_load15	소수	15분 평균 Load Average	리눅스
cpu_new_procs_forked	정수	os process fork 호출	리눅스
cpu_procs_blocked	정수	프로세스 blocked 상태 개수	리눅스
cpu_procs_running	정수	프로세스 Running 상태 개수	리눅스
cpu_softirq	퍼센트	CPU softirq 사용률	리눅스
cpu_steal	퍼센트	CPU steal 사용률	리눅스
cpu_sys	퍼센트	CPU system 사용률	공통
cpu_usr	퍼센트	CPU user 사용률	공통

필드명	단위	설명	비고
epochtime	정수	메트릭이 수집된 시간의 epoch time	공통
memory_available	바이트	메모리 available 크기	공통
memory_buffers	바이트	메모리 buffers 크기	리눅스
memory_cached	바이트	메모리 cached 크기	공통
memory_free	바이트	메모리 free 크기	공통
memory_pageFaults	정수	메모리 page fault 횟수	공통
memory_pavailble	퍼센트	메모리 available 사용률	공통
memory_pused	퍼센트	메모리 사용률	공통
memory_shared	바이트	메모리 shared 크기	리눅스
memory_slab	바이트	메모리 slab 크기	리눅스
memory_sreclaimable	바이트	메모리 slab reclaimable 크기	리눅스
memory_sunreclaim	바이트	메모리 slab cclaimable 크기	리눅스
memory_swappused	퍼센트	스왑 사용률	공통
memory_swaptotal	바이트	스왑 전체 크기	공통
memory_swapused	바이트	스왑 사용량	공통
memory_total	바이트	메모리 전체 크기	공통
memory_used	바이트	메모리 사용량	공통
processorQueueLength	정수	프로세서 큐 길이	윈도우

필드명	단위	설명	비고
uptime	정수	부팅 후 서버의 가동 시간(TimeStamp)	공통

server_cpu_core

서버 CPU 코어별 지표입니다.

- 수집 간격 : 5초
- 통계 데이터 : -

Tags

태그명	설명	비고
cpu	서버 코어 번호	-
ip	서버 IP	-
oname	서버 이름	-
os	OS 유형 linux 또는 window	-

Fields

필드명	단위	설명	비고
idle	퍼센트	코어 idle 비율	공통
iowait	퍼센트	코어 iowait 비율	윈도우

필드명	단위	설명	비고
irq	퍼센트	코어 irq 사용률	리눅스
load1	소수	코어 1분 평균 Load Average	리눅스
load5	소수	코어 5분 평균 Load Average	리눅스
load15	소수	코어 15분 평균 Load Average	리눅스
nice	퍼센트	코어 nice 사용률	공통
processorQueueLength	정수	코어 프로세스 큐 길이	윈도우
softirq	퍼센트	코어 softirq 사용률	리눅스
steal	퍼센트	코어 steal 사용률	리눅스
sys	퍼센트	코어 sys 사용률	리눅스
usr	퍼센트	코어 usr 사용률	리눅스

server_disk

각 서버에 마운트 된 파일 시스템별 지표입니다.

- 수집 간격 : 5초
- 통계 데이터 : 5분, 1시간

Tags

태그명	설명	비고
deviceId	디바이스 ID	-
deviceIdHash	디바이스 ID 해시 값	-
fileSystem	파일 시스템 유형	-
mountPoint	파일 시스템 마운트 포인트	-
mountPointHash	파일 시스템 마운트 포인트 해시	-
oname	서버 이름	-
os	OS 유형 linux 또는 window	-

Fields

필드명	단위	설명	비고
blksize	바이트	블록 사이즈	리눅스
count	정수	와탭 전용	공통
freePercent	퍼센트	파일 시스템 잔여율	리눅스
freeSpace	바이트	파일 시스템 잔여량	리눅스
ioPercent	퍼센트	IO 사용률 일부 디스크 유형에서는 부정확한 값이 측정될 수 있습니다.	리눅스
ioutilOrder	정수	와탭 전용	리눅스
queueLength	실수	Queue Length	공통

필드명	단위	설명	비고
totalInode	정수	Inode 전체 개수	리눅스
totalSpace	바이트	파일 시스템 전체 크기	리눅스
usedPercent	퍼센트	파일 시스템 사용률	리눅스
usedInode	정수	Inode 사용 개수	리눅스
usedInodePercent	퍼센트	Inode 사용률	리눅스
userSpaceOrder	정수	와탭 전용	공통
readBps	바이트	초당 읽은 바이트 수	공통
writeBps	바이트	초당 쓴 바이트 수	공통
readIops	소수	초당 읽은 수	공통
writeIops	소수	초당 쓴 수	공통

server_network

각 서버의 네트워크 인터페이스 지표입니다.

- 수집 간격 : 5초
- 통계 데이터 : 5분, 1시간

Tags

태그명	설명	비고
desc	네트워크 인터페이스 이름	-
descHash	네트워크 인터페이스 해시 값	-
hwAddr	MAC 주소	-
ip	인터페이스 IP 주소	-
oname	서버 이름	-
os	OS 유형 linux 또는 window	-

Fields

필드명	단위	설명	비고
bandwidthOrder	정수	와탭 전용	-
count	정수	와탭 전용	공통
droppedIn	정수	인바운드 드랍	-
droppedOut	정수	아웃바운드 드랍	-
errorIn	정수	인바운드 에러	-
errorOut	정수	아웃바운드 에러	-
packetIn	pps	인바운드 패킷	-
packetOut	pps	아웃바운드 패킷	-

필드명	단위	설명	비고
trafficIn	bps	인바운드 트래픽	-
trafficInAcct	정수	와탭 전용	-
trafficOut	bps	아웃바운드 트래픽	-
trafficOutAcct	정수	와탭 전용	-

server_netstat

각 서버별 네트워크 프로토콜 통계 정보입니다.

- 수집 간격 : 5초
- 통계 데이터 : 5분, 1시간

Tags

태그명	설명	비고
oname	서버 이름	-
os_arch	OS 아키텍처 이름	-
os_cpucore	서버 CPU 코어 수	-
os_cpusocket	서버 CPU 소켓 수	-
os_cpuvendor	서버 CPU 벤더 이름	-
os_ip	서버 IP	-

태그명	설명	비고
os_memory	서버 메모리 크기	-
os_nameOS 유형 linux 또는 window	-	
os_public_ip	서버 공인 IP	-
os_release	서버 OS 릴리즈명	-
whatap_build	와탭 에이전트 빌드 해시값	-
whatap_home	와탭 에이전트 홈 경로	-
whatap_product	와탭 상품 유형	-
whatap_version	와탭 에이전트 버전	-

Fields

필드명	단위	설명	비고
netstat_Close_Wait	정수	CLOSE_WAIT 상태 소켓 수	공통
netstat_Closing	정수	CLOSING 상태 소켓 수	공통
netstat_Established	정수	Established 상태 소켓 수	공통
netstat_Fin_Wait1	정수	FIN_WAIT1 상태 소켓 수	공통
netstat_Fin_Wait2	정수	FIN_WAIT2 상태 소켓 수	공통
netstat_Last_Ack	정수	LASK_ASK 상태 소켓 수	공통
netstat_Listen	정수	LISTEN 상태 소켓 수	공통

필드명	단위	설명	비고
netstat_Syn_Recv	정수	SYN_RECV 상태 소켓 수	공통
netstat_Syn_Sent	정수	SYN_SENT 상태 소켓 수	공통
netstat_Time_Wait	정수	TIME_WAIT 상태 소켓 수	공통
netstat_Unknown	정수	Unknown 상태 소켓 수	공통
Server_FileDescriptors	정수	OS file descriptor 개수	공통

server_process

서버 프로세스 정보입니다.

- 수집 간격 : 20초
- 통계 데이터 : 5분

Tags

태그명	설명	비고
alias	서버 별칭	-
cmd1	프로세스 실행 명령어1	-
cmd2	프로세스 실행 파라미터	-
hash	프로세스 해시 값	-
name	프로세스명	-

태그명	설명	비고
oname	서버 이름	-
user	프로세스를 실행한 리눅스 사용자명	-

Fields

필드명	단위	설명	비고
count	정수	프로세스 개수	공통
cpu	퍼센트	CPU 사용률	공통
cpuAccumulated	퍼센트	와탭 전용	공통
cpuOrder	순서	와탭 전용	공통
memOrder	순서	와탭 전용	공통
memory	퍼센트	메모리 사용률	공통
memoryAccumulated	퍼센트	와탭 전용	공통
openFileDescriptors	정수	open file descriptor 개수	공통
rbps	바이트	디스크 초당 읽은 바이트 수	공통
rbpsAccmulated	바이트	와탭 전용	공통
riops	정수	디스크 초당 읽은 수	공통
riopsAccmulated	정수	와탭 전용	공통
wbps	바이트	디스크 초당 쓴 바이트 수	공통
wbpsAccmulated	바이트	와탭 전용	공통

필드명	단위	설명	비고
wiops	정수	디스크 초당 쓴 수	공통
wiopsAccmulated	정수	와탭 전용	공통
rss	바이트	메모리 RSS 크기	공통
rssAccmulated	바이트	와탭 전용	공통

참고 자료

- [윈도우 지수 자료](#)
- [리눅스 지수 자료](#)

메트릭스 조회

홈 화면 > 프로젝트 선택 > 분석 > 메트릭스 조회

메트릭스 조회 메뉴에서 태그 기반으로 특정 메트릭스를 조회할 수 있습니다.

The screenshot shows the '메트릭스 조회' (Metrics Search) interface. It is divided into three main sections:

- 1 시간 선택 (Time Selection):** Includes a date range selector (2023/08/17 07:56 ~ 2023/08/17 08:56), a '최대 개수' (Max Count) dropdown set to 100, and a '카테고리' (Category) dropdown set to 'app_counter'.
- 2 태그 전체 (Tag Selection):** A list of tags is displayed, including 'container', 'containerKey', 'host_ip', 'okindName', 'oname', 'onodeName', 'pid', and 'type'. A search filter '태그값으로 필터링' is available. Below the tags, a list of fields is shown, with 'active_tx_3', 'arrival_rate', 'sql_time', 'tps', and 'tx_error' highlighted.
- 3 Table:** A table with columns for 'Time', 'Oid', 'Tags', and 'Fields'. The 'Fields' column lists metrics like 'active_tx_3', 'arrival_rate', 'sql_time', 'tps', and 'tx_error'.

	Time	Oid	Tags							Fields					
			container	containerKey	host_ip	okindName	oname	onodeName	pid	type	active_tx_3	arrival_rate	sql_time	tps	tx_error
1	2023-08-17 07:56:45	-877561626	agent.service	1395943798	10.21.1.26	demo-okind-1	demo-8101	node-1	3284967	java	11	24.390244	5.7834587	20.68982	1
2	2023-08-17 07:56:45	-1128904592	agent.service	1395943798	10.21.1.26	demo-okind-0	demo-8100	node-0	3284934	java	5	15.993603	9.613368	18.623732	0

1 시간과 카테고리 선택

1 영역에서 메트릭스가 수집된 시간과 최대 개수 및 카테고리를 지정할 수 있습니다. 시간과 카테고리는 반드시 지정해야 합니다.

- 시간:** 메트릭스가 수집된 시간을 지정해 조회할 수 있습니다. 기본값은 1시간 입니다. 기본 옵션으로 제공하는 조회 시간 외 사용자가 직접 시간 탭을 선택해 날짜와 시간을 지정할 수 있습니다.
- 최대 개수:** 3 목록에 조회할 메트릭스 최대 개수를 지정할 수 있습니다. 10, 50, 100, 200, 300, 1000, 2000, 3000 개까지 설정할 수 있습니다.
- 카테고리:** 유관 지표들의 분류 단위입니다. 카테고리 탭을 선택해 원하는 카테고리를 지정할 수 있습니다.
- 새로 고침:** 새로 고침 아이콘을 선택하면 카테고리, 태그 및 필드 옵션을 다시 불러올 수 있습니다.

2 태그와 필드 선택

2 영역에서 태그와 필드를 선택합니다. 사용자가 개별적으로 지정하지 않는다면 기본 설정은 전체 선택입니다.

- 태그:** 수집된 대상을 구분할 수 있는 고유 정보 데이터입니다.

- **필드**: 모니터링 대상으로부터 수집된 지표입니다.
- **필터**: ▾ **태그값으로 필터링** 버튼을 선택하고 태그 값을 설정해 필터링할 수 있습니다.
예시, `oname` 의 값을 `demo-8101` 로 설정해 필터링한 데이터를 조회할 수 있습니다.
- 🔍 **검색**: 조건을 설정 후 **검색** 아이콘을 선택하면 ③ 영역에서 해당 메트릭스의 원본 데이터를 조회할 수 있습니다.
- 📄 **CSV 다운로드**: **CSV 다운로드** 버튼을 선택해 해당 메트릭스 원본 데이터를 CSV 파일로 다운로드할 수 있습니다.

3 메트릭스 테이블

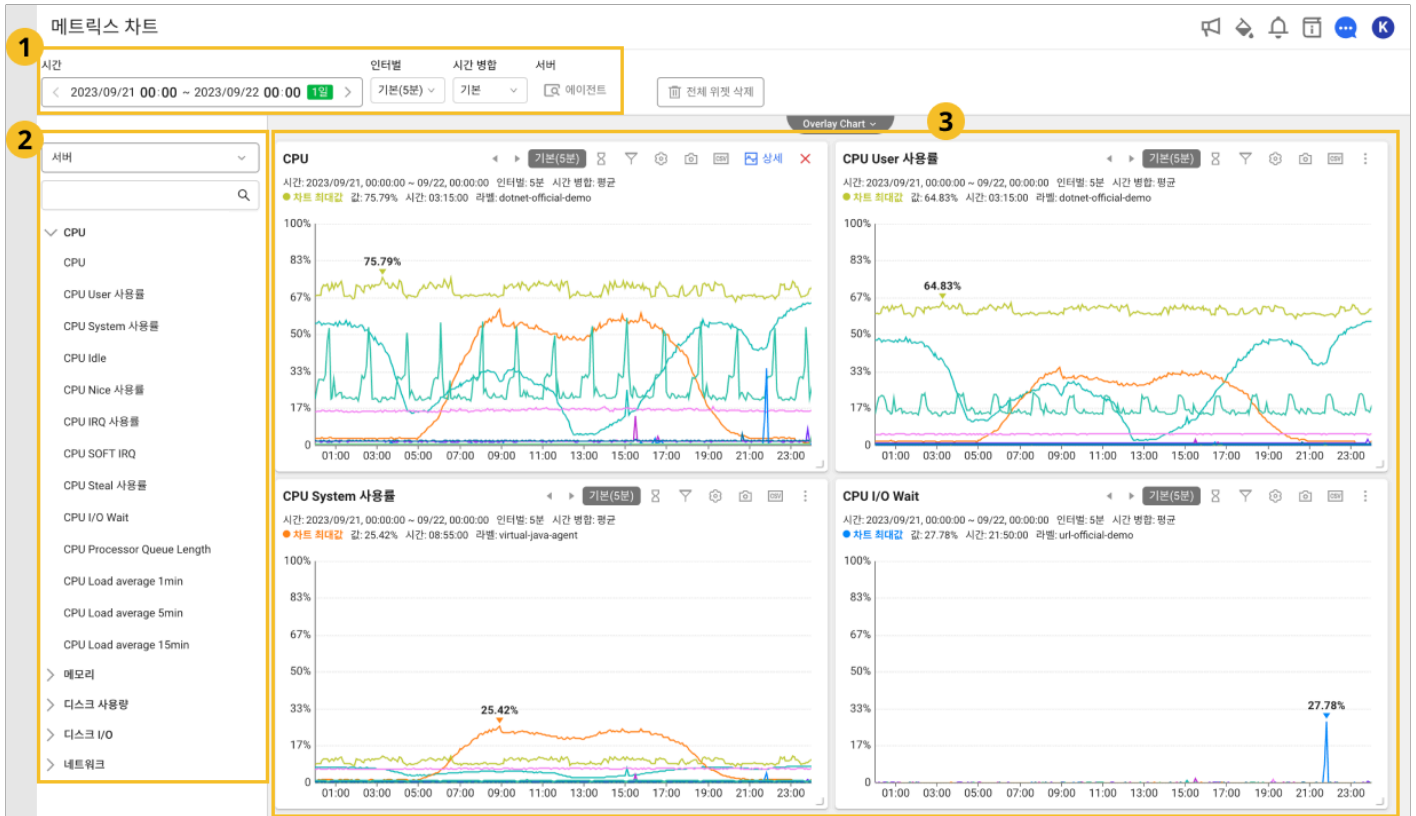
수집되는 메트릭스를 사전에 특정할 수 없기에 수집 중인 모든 메트릭스의 원본 데이터를 확인하는 것이 중요합니다. 위의 조건 영역에서 원하는 조건을 설정 후 ③ 영역에서 해당 메트릭스의 원본 데이터를 테이블 형식으로 조회할 수 있습니다. 사용자가 **태그**와 **필드** 각 조건을 지정함에 따라 테이블의 컬럼이 변경됩니다.

- ① • 메트릭스 조회 시 **시간**과 **카테고리**는 반드시 지정해야 합니다.
- 메트릭스 조회 시 **태그**와 **필드** 지정은 선택 사항입니다.

메트릭스 차트

홈 화면 > 프로젝트 선택 > 분석 > 메트릭스 차트

메트릭스 차트 메뉴에서 모니터링 대상에서 수집된 메트릭스 데이터를 다음과 같이 차트로 조회할 수 있습니다. 시간과 지표를 지정하는 것은 필수입니다.



상단 옵션

1 영역의 메트릭스 차트의 상단 옵션을 통해 차트의 시간 범위와 모니터링 대상 에이전트를 지정할 수 있습니다.

- **시간**: 시간의 총 범위로 X축의 시작과 끝을 지정할 수 있습니다.
- **인터벌**: 시간 간격으로 X축 데이터 간격을 지정할 수 있습니다.
- **시간 병합**: 데이터 병합 방식 중 하나로 인터벌로 지정한 시간 내의 데이터를 병합할 수 있습니다.

예, **평균**은 1시간 안 데이터의 평균값을 말합니다.

- ☑ **에이전트**: 조회할 에이전트를 지정할 수 있습니다. 지정하지 않으면 전체가 조회됩니다.

지표 목록

2 영역은 옵션을 조회할 지표 목록입니다. 먼저 **카테고리**를 선택하세요. 선택한 **카테고리** 하위의 지표를 조회한 후 원하는 지표를 선택하세요. **카테고리**와 지표를 선택하면 1 영역의 상단 메뉴에서 지정한 시간 범위의 데이터를 기준으로 3 영역에서 차트 위젯을 통해 데이터를 조회할 수 있습니다.

ⓘ 데이터 병합

데이터 병합은 **시간 병합**과 **오브젝트 병합**을 제공합니다.

- **시간 병합**은 원본 데이터에서 필드 값이 같은 데이터끼리 일정한 간격으로 데이터를 병합합니다.
- **오브젝트 병합**은 서로 다른 필드 값을 가진 데이터들 중에서 태그가 일치하는 경우 해당 데이터를 병합합니다.

차트 위젯

3 영역 차트 위젯의 좌측 상단에서 지표명을 확인할 수 있습니다. 차트 위젯의 우측 상단에서 다음과 같은 옵션을 확인할 수 있습니다.




- 시간 이동: ◀ ▶ 왼쪽 화살표 또는 오른쪽 화살표 버튼을 통해 선택한 시간 범위만큼 -1, +1 씩 이동 가능합니다.

예, 시간 범위가 2월 13일 00:00~2월 14일 00:00일 때, ▶ 오른쪽 화살표를 선택하면 2월 12일 00:00~2월 13일 00:00 데이터를 조회할 수 있습니다.

- 인터벌/시간 병합: 1 상단 메뉴에서 지정한 인터벌과 시간 병합을 수정할 수 있습니다.
- 모니터링 대상: ⚙ 아이콘을 선택해 모니터링 대상을 지정할 수 있습니다. 선택하지 않으면 전체를 대상으로 조회합니다.
- 시간 비교: 📏 아이콘을 선택하면 동일한 지표의 이전 시간대의 추이를 비교할 수 있습니다.
- 스냅샷: 📷 아이콘을 선택해 위젯의 옵션을 제외한 차트를 스냅샷 할 수 있습니다.
- CSV: 📄 아이콘을 선택해 차트를 그리는 데이터를 CSV 파일로 다운로드할 수 있습니다.
- 상세 보기: 🔍 아이콘을 선택해 상세 조회가 가능합니다. 모니터링 대상이 많은 경우 유용하며, 모니터링 대상의 지표 추이를 개별로 확인 할 수 있습니다.

① 메트릭스 차트 위젯 상단에서 옵션이 보이지 않을 경우 ⋮ 아이콘을 선택하세요.

위젯 삭제하기

화면에 배치한 모든 위젯을 삭제하려면 화면 위에 위치한  **전체 위젯 삭제** 버튼을 선택하세요.

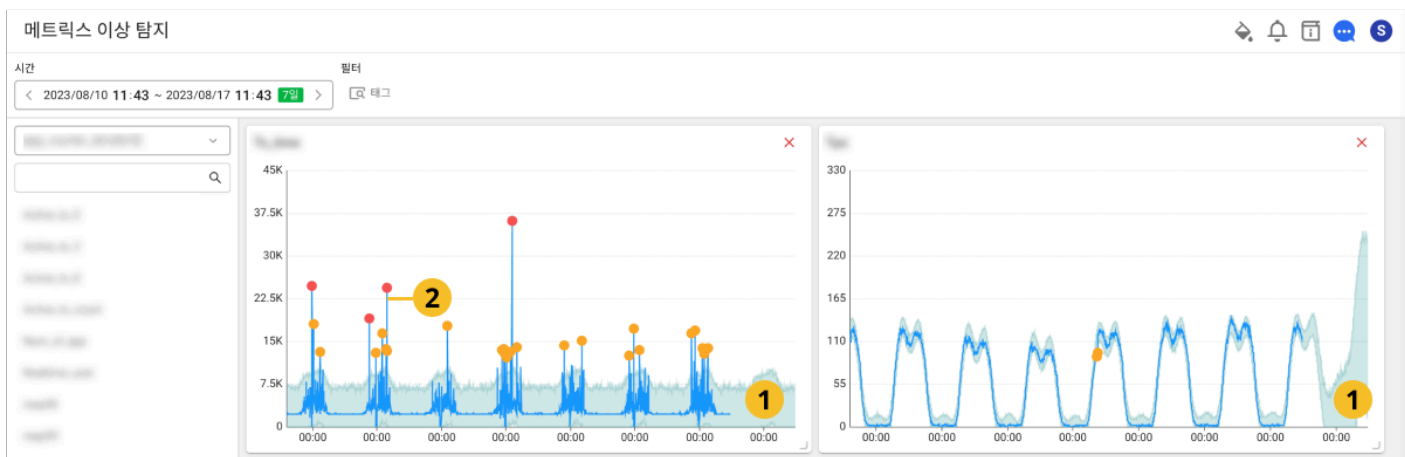
메트릭스 이상 탐지

홈 화면 > 프로젝트 선택 > 분석 > 메트릭스 이상 탐지

다양한 메트릭스 지표의 패턴을 시가 학습한 예상 패턴과 비교해 볼 수 있습니다. 예상 패턴을 벗어난 이상 탐지를 그래프 차트를 통해 확인할 수 있습니다. 과거 데이터를 바탕으로 반복되는 패턴을 확인하고 향후 지표 값 예측에 활용할 수 있습니다.

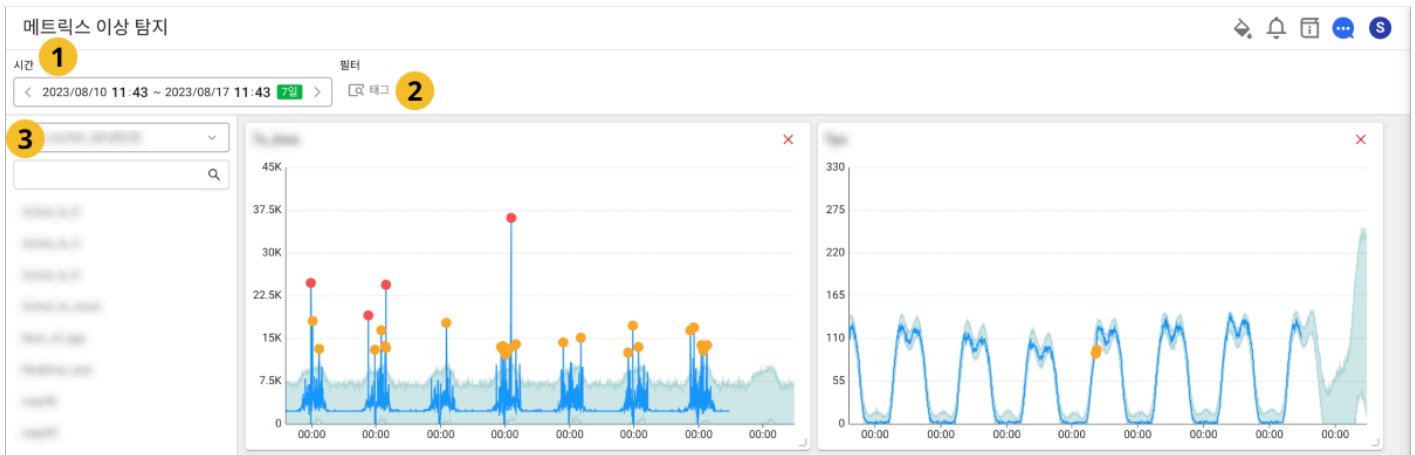
- ❗ • 화면에 배치한 위젯은 다른 메뉴로 이동할 경우 저장되지 않고 초기화합니다.
- 패턴 표시와 이상치 표시 기능을 제외하면 **분석 > 메트릭스 차트** 메뉴와 유사합니다.
- **이상치 탐지(Anomaly Detection)** 경고 알림 기능의 기술 근간은 **메트릭스 이상 탐지**입니다. **이상치 탐지** 경고 알림 설정에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

위젯 확인하기



- ❶ 밝은 색상의 그래프 영역은 시가 분석한 예상 패턴입니다.
- ❷ 파랑색 그래프는 프로젝트의 메트릭스 지표 추이입니다.
- 시가 분석한 예상 패턴을 벗어나면 **주황색**, **빨간색**의 단계로 그래프에 점을 표시합니다. 예상 패턴 범위를 크게 벗어난 값을 **빨간색**으로 표시합니다.

위젯 배치하기

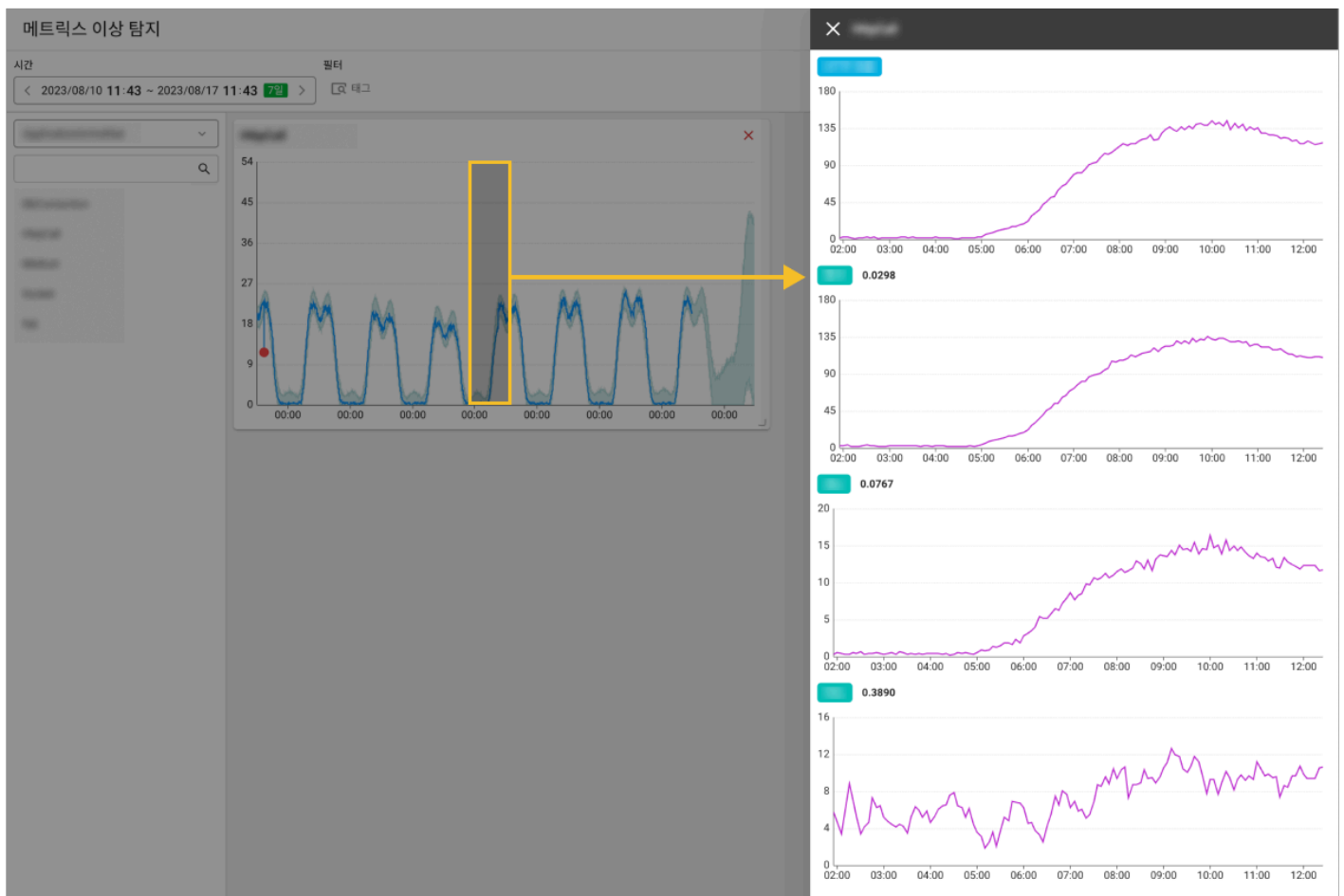


1. ① **시간**에서 원하는 시간 간격을 설정하세요. 최대 1개월 간격까지 설정할 수 있습니다.
2. ② **필터**에서 메트릭스 지표의 범위를 선택하세요.
3. 아래 목록에서 모니터링하길 원하는 메트릭스 지표를 선택하세요.

선택한 메트릭스 지표를 화면 오른쪽에 배치합니다.

- ⓘ • 모니터링 대상을 선택해 메트릭스 지표를 구분해서 확인하려면 ② **태그**를 선택하세요. 화면 오른쪽에 태그 선택 목록이 나타납니다. 원하는 항목을 선택한 다음 위젯을 추가하세요.
 - 화면에 배치한 위젯은 **시간** 또는 **태그** 값을 변경해도 차트에 반영되지 않습니다.
 - 화면에 배치한 위젯을 삭제하려면 위젯 오른쪽 위에 **×** 버튼을 선택하세요.
 - 위젯의 왼쪽 위를 선택한 상태에서 드래그해 위젯 위치를 변경할 수 있습니다.
 - 위젯 오른쪽 아래를 선택한 상태에서 드래그해 위젯 크기를 조절할 수 있습니다.

연관 지표 확인하기



위젯에서 차트의 일부 영역을 드래그하세요. 선택한 영역에서 해당 메트릭스 지표와 관련한 지표를 같이 확인할 수 있습니다.

서버 목록

홈 화면 > 프로젝트 선택 > 서버 목록 > 서버 목록

와탭 모니터링 서비스 초기 화면에서 프로젝트를 선택한 다음 프로젝트 메뉴 하위에 **서버 목록 > 서버 목록** 메뉴를 선택하세요. **서버 목록**은 수집 서버의 전체 현황을 나타내며 서버 관리기능 및 서버 간 비교 기능을 제공합니다.

상태	에이전트 명	OS 버전	CPU Used %	메모리 Memory Used %	디스크 Disk Used % (Max)	디스크 I/O % (Max)	네트워크 Network Traffic (Max)	기타 Private IP
⚠	demo-k8s-worker-04	Ubuntu 22.04.2 LTS	66.5%	45.1% (1.6G)	64.7%	0.4%	ens5 369K	127.0.0.1 10.21.1.210 10.244.4.1
⚠	go-official-demo	Ubuntu 22.04.2 LTS	22.8%	13.1% (1G)	99.6%	0.3%	ens5 40.4K	127.0.0.1 10.21.1.118 172.17.0.1 172.18.0.1
⚠	mysql-official-demo-02	Ubuntu 22.04.2 LTS	3%	80% (753M)	22.4%	0.5%	ens5 171K	127.0.0.1 10.21.1.136
⚠	mysql-official-demo-03	Ubuntu 22.04.2 LTS	3.4%	79.9% (752M)	22.1%	0.8%	ens5 191K	127.0.0.1 10.21.1.236
⚠	node-official-demo	Ubuntu 22.04.2 LTS	26.8%	77.6% (1.4G)	42.2%	0.3%	lo 71.9M	127.0.0.1 10.21.1.98
⚠	rum-official-demo	Ubuntu 22.04.2 LTS	23.5%	27.6% (535M)	35.6%	0.1%	lo 288K	127.0.0.1 10.21.1.151
⚠	virtual-java-agent	Ubuntu 20.04.6 LTS	50.7%	71.6% (2.6G)	36.8%	0.2%	lo 7.6M	127.0.0.1 10.21.1.26
✅	demo-k8s-master	Ubuntu 22.04.2 LTS	3.3%	29.3% (1.1G)	24.7%	1.7%	lo 6.1M	127.0.0.1 10.21.1.149 10.244.0.1

1 서버 상태

수집 서버의 상태별 현황을 나타냅니다. 상태는 1분 간격으로 갱신합니다.

- ⚠ 비활성 : 에이전트가 해당 서버의 데이터 수집이 불가능한 상태입니다.
- ⚠ 위험 : 수집 서버에서 위험 이벤트가 발생한 상태입니다.
- ⚠ 경고 : 수집 서버에서 경고 이벤트가 발생한 상태입니다.
- ✅ 정상 : 에이전트가 수집 서버에서 정상적으로 작동 중인 상태입니다.
- ⏸ 일시정지 : 에이전트에서 데이터 수집을 일시적으로 중지한 상태입니다.

2 데이터 갱신

서버 목록 페이지의 데이터는 60초마다 자동으로 갱신합니다.

- || **일시정지** : 사용자는 데이터의 자동 갱신을 중지할 수 있습니다.
- ▶ **재생** : 사용자는 중지한 자동 갱신을 재시작할 수 있습니다.
- ↻ **새로고침** : 사용자는 현재 시간을 기준으로 데이터를 갱신할 수 있습니다.

3 서버 현황

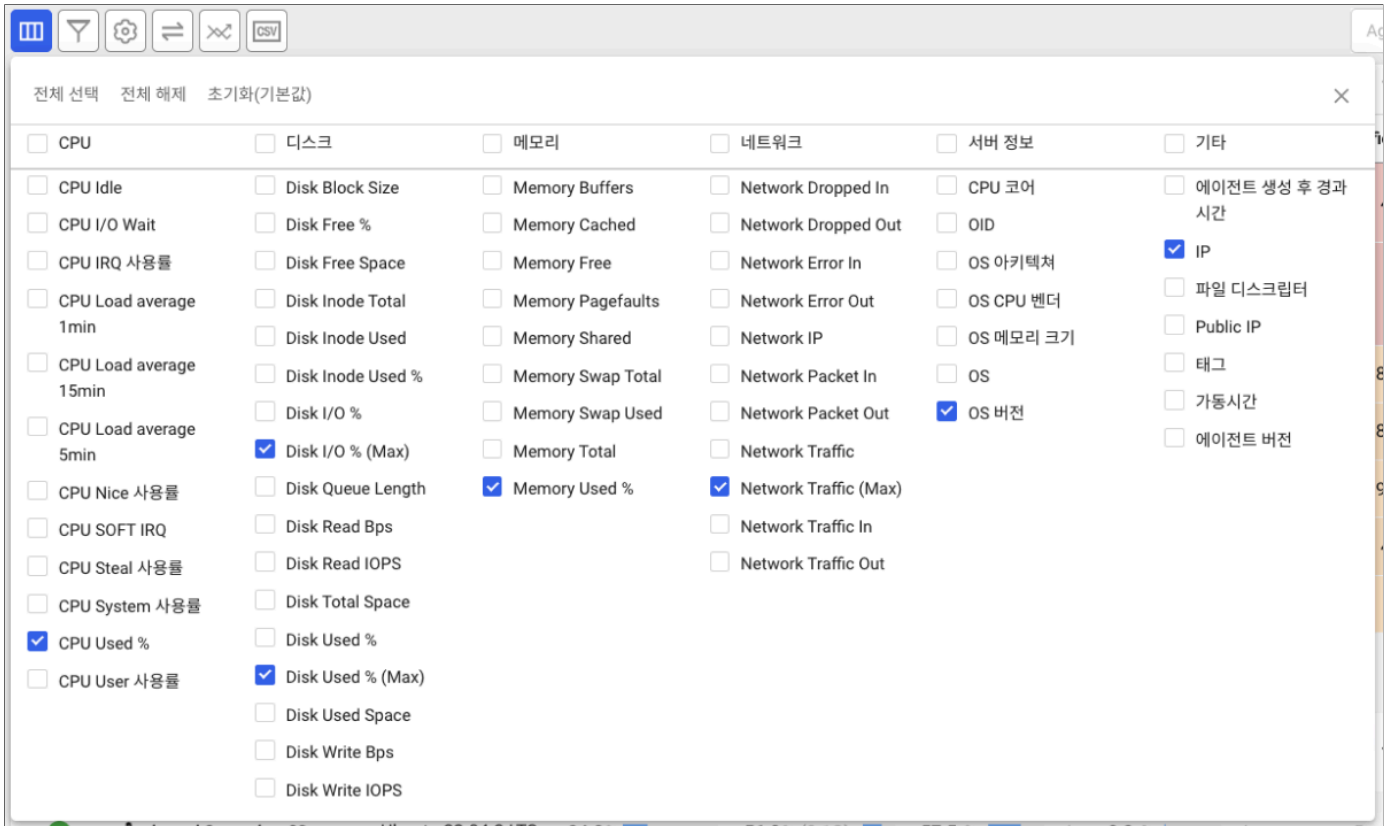
에이전트가 할당된 전체 서버의 현황을 나타냅니다. 목록에서 에이전트를 선택하면 [서버 상세](#) 페이지로 이동합니다. [서버 상세](#) 메뉴에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

검색

- 3 영역 상단 오른쪽 **검색창**을 활용해 서버 이름(ONAME), 서버 아이디(OID), 태그 중에서 입력값이 포함된 서버 목록을 필터링할 수 있습니다.

컬럼

- ☐ **컬럼 선택**
 - 3 영역 상단 메뉴에서 ☐ **컬럼 선택** 버튼을 클릭하면 다음과 같이 테이블에 표시할 컬럼을 선택할 수 있습니다.



① 선택한 컬럼은 브라우저 쿠키값으로 저장되어 페이지 새로 고침 후에도 상태가 유지됩니다. 쿠키 삭제 또는 기타 이유로 설정 간 오류가 발생하면 전체 선택 상태로 초기화합니다.

• 컬럼 너비 설정

컬럼 제목의 가장자리를 드래그해 컬럼 너비를 설정할 수 있습니다.

• 컬럼 정렬

컬럼 제목을 클릭해 오름차순 또는 내림차순 정렬이 가능합니다.

① 컬럼 너비 및 컬럼 정렬 설정값은 브라우저 쿠키로 저장되어 페이지 새로 고침 후에도 상태가 유지됩니다. 쿠키 삭제 또는 기타 이유로 설정 간 오류가 발생하면 미 설정 상태로 초기화합니다.

필터

3 영역 상단 메뉴에서 **필터** 버튼을 클릭하면 태그를 통해 서버를 필터링할 수 있습니다.

태그는 에이전트를 설치할 때 자동으로 부여됩니다. 사용자 입력값을 추가할 수 있습니다. 태그를 통해 수집 서버를 식별하거나 서버 현황을 필터링합니다.

4

meta:public-ipv4=43.201.249.150 (1) meta:instance-id=i-07e7516e45b47f239 (1) ftp (2) meta:local-ipv4=10.21.1.23 (1) meta:hostname=ip-10-21-1-236.ap-northeast-2.compute.internal (1)

meta:local-ipv4=10.21.1.151 (1) meta:security-groups=Demo-WPM (1) meta:reservation-id=r-088d02659bdf67048 (1) meta:public-ipv4=54.180.137.72 (1) meta:ami-id=ami-029ba909398cde220 (3)

meta:reservation-id=r-0d8918b6cf200678e (1) meta:reservation-id=r-0ed734eb24bc78ef4 (1) meta:public-hostname=ec2-43-201-54-111.ap-northeast-2.compute.amazonaws.com (2)

meta:public-ipv4=3.35.137.79 (1) meta:local-hostname=ip-10-21-1-51.ap-northeast-2.compute.internal (1) meta:public-ipv4=13.125.198.227 (1) meta:local-ipv4=10.21.1.157 (1)

meta:ami-id=ami-0c6a76b08ece4b045 (1) meta:reservation-id=r-05ced84247e60e9f8 (1) meta:instance-type=t3.micro (4) meta:local-hostname=ip-10-21-1-210.ap-northeast-2.compute.internal (1)

meta:mac=02:05:0f:92:ec:0c (1) meta:reservation-id=r-0fb020761f1642019 (1) meta:security-groups=mysql-official-demo (4) meta:instance-id=i-0cefd1cfeafef04f (1)

meta:instance-id=i-0e9c4b2322821b0e3 (2) meta:local-hostname=ip-10-21-1-236.ap-northeast-2.compute.internal (1) meta:reservation-id=r-0810528ffde66bceb (2) meta:local-ipv4=10.21.1.149 (1)

meta:reservation-id=r-092d310dc1702d1d9 (1) network:172.17.0.0/16 (1) mysql (1) meta:public-hostname=ec2-3-35-137-79.ap-northeast-2.compute.amazonaws.com (1) network:172.18.0.0/16 (1)

meta:local-ipv4=10.21.1.26 (1) meta:local-hostname=ip-10-21-1-98.ap-northeast-2.compute.internal (1) meta:instance-type=m6i.xlarge (1) meta:local-ipv4=10.21.1.43 (1)

meta:mac=02:d3:06:2f:c5:24 (1) meta:public-ipv4=43.201.6.83 (1) meta:public-hostname=ec2-3-35-168-178.ap-northeast-2.compute.amazonaws.com (1) meta:public-ipv4=13.125.62.87 (1)

meta:public-ipv4=3.36.69.13 (1) meta:public-hostname=ec2-43-201-249-150.ap-northeast-2.compute.amazonaws.com (1) meta:local-hostname=ip-10-21-1-136.ap-northeast-2.compute.internal (2)

상태	에이전트 명	OS 버전	CPU	메모리	디스크	네트워크	기타
			CPU Used %	Memory Used %	Disk Used % (Max)	Disk I/O % (Max)	Network Traffic (Max)
	demo-k8s-worker-04	Ubuntu 22.04.2 LTS	80.3%	57% (2.1G)	64.7%	0.8%	ens5 784K 127.0.0.1 10.21.1.210 10.244.4.1

태그 입력 / 엔터

5

meta:reservation-id=r-0810528ffde66bceb meta:public-ipv4=43.201.6.83 meta:local-ipv4=10.21.1.210 meta:hostname=ip-10-21-1-210.ap-northeast-2.compute.internal

meta:public-hostname=ec2-43-201-6-83.ap-northeast-2.compute.amazonaws.com meta:ami-manifest-path=(unknown) meta:ami-launch-index=0 meta:instance-type=c6i.large

network:10.0.0.0/8 share meta:instance-action=none python meta:mac=02:2a:91:a3:4e:02 meta:local-hostname=ip-10-21-1-210.ap-northeast-2.compute.internal

meta:public-ipv4=3.38.98.50 meta:instance-type=t3.medium meta:public-hostname=ec2-3-38-98-50.ap-northeast-2.compute.amazonaws.com meta:security-groups=demo-k8s-node

meta:instance-id=i-06712d49e meta:profile=default-hvm meta:ami-id=ami-07e02e4beb31bf4d5 meta:instance-life-cycle=on-demand meta:system=nitro

/var/lib/kubelet/pods/3fed1399-6c95-46a0-ab8b-f6cb89cb052/volume-subpaths/start-script-volume/whatap-master-agent/0

/var/lib/kubelet/pods/cc40b595-d44f-47a9-a831-1956a48fd2d8/volume-subpaths/start-script-volume/whatap-node-agent/1

상태	에이전트 명	OS 버전	CPU	메모리	디스크	네트워크	기타
			CPU Used %	Memory Used %	Disk Used % (Max)	Disk I/O % (Max)	Network Traffic (Max)
	virtual-java-agent	Ubuntu 20.04.6 LTS	39.9%	71.5% (2.6G)	36.8%	0.8%	lo 5.8M 127.0.0.1 10.21.1.26

meta:reservation-id=r-088d02659bdf67048 meta:security-groups=Dev-Office-SG-Demo-Agent-Server meta:instance-id=i-0909a78ddd704547 meta:ami-manifest-path=(unknown)

meta:ami-launch-index=0 meta:instance-type=c6g.large network:10.0.0.0/8 meta:instance-action=none meta:local-hostname=ip-10-21-1-26.ap-northeast-2.compute.internal python

meta:ami-id=ami-0c6a76b08ece4b045 meta:public-hostname=ec2-52-78-115-130.ap-northeast-2.compute.amazonaws.com meta:public-ipv4=52.78.115.130 ftp meta:profile=default-hvm

meta:instance-life-cycle=on-demand meta:local-ipv4=10.21.1.26 meta:hostname=ip-10-21-1-26.ap-northeast-2.compute.internal meta:system=nitro meta:mac=02:05:0f:92:ec:0c

태그 입력 / 엔터

- 4 영역에서 태그를 선택하여 서버 현황을 필터링할 수 있습니다.
- 에이전트별 태그를 입력하여 새로운 태그 기능을 활성화 할 수 있습니다. 5 영역 입력창을 확인하세요.

모니터링 관리

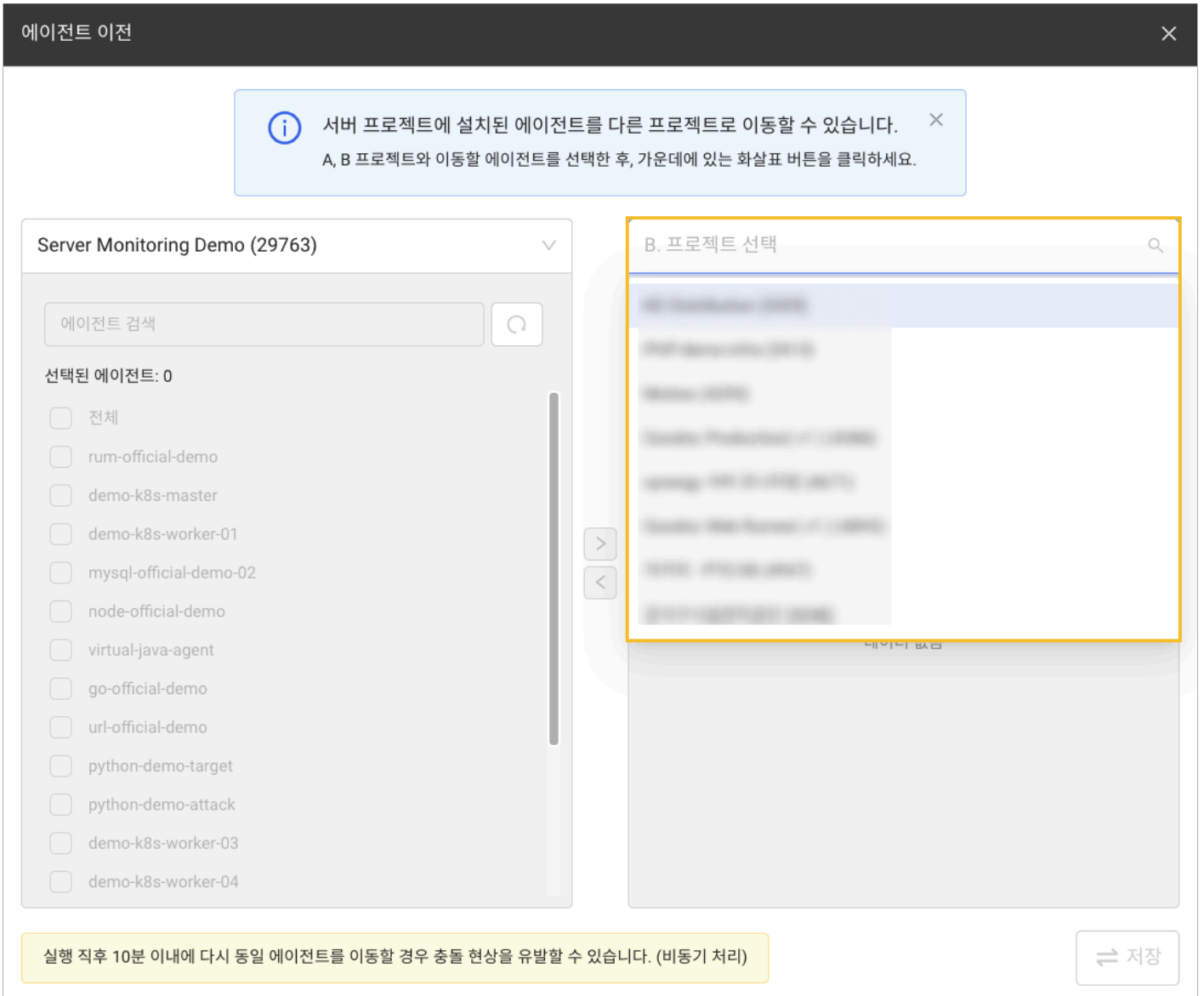
에이전트 명령을 통해 서버를 관리하는 기능입니다. **관리** 버튼을 클릭하고 목록에서 관리 기능을 적용할 서버를 선택하세요.

오른쪽에 [일시정지](#), [재시작](#), [해지하기](#) 버튼이 활성화됩니다.

- **|| 일시정지** : 해당 에이전트의 데이터 수집을 일시 중지합니다. 서버 목록에서 일시 중지 상태로 표시됩니다.
- **▶ 재시작** : 에이전트를 다시 시작합니다.
- **⏏ 해지하기** : 에이전트의 작동을 중지합니다. 서버 목록에서 제외되며 서버 현황을 확인할 수 없습니다.

에이전트 이전

⇒ [에이전트 이전](#) 버튼을 선택해 에이전트를 다른 프로젝트로 이전할 수 있습니다.



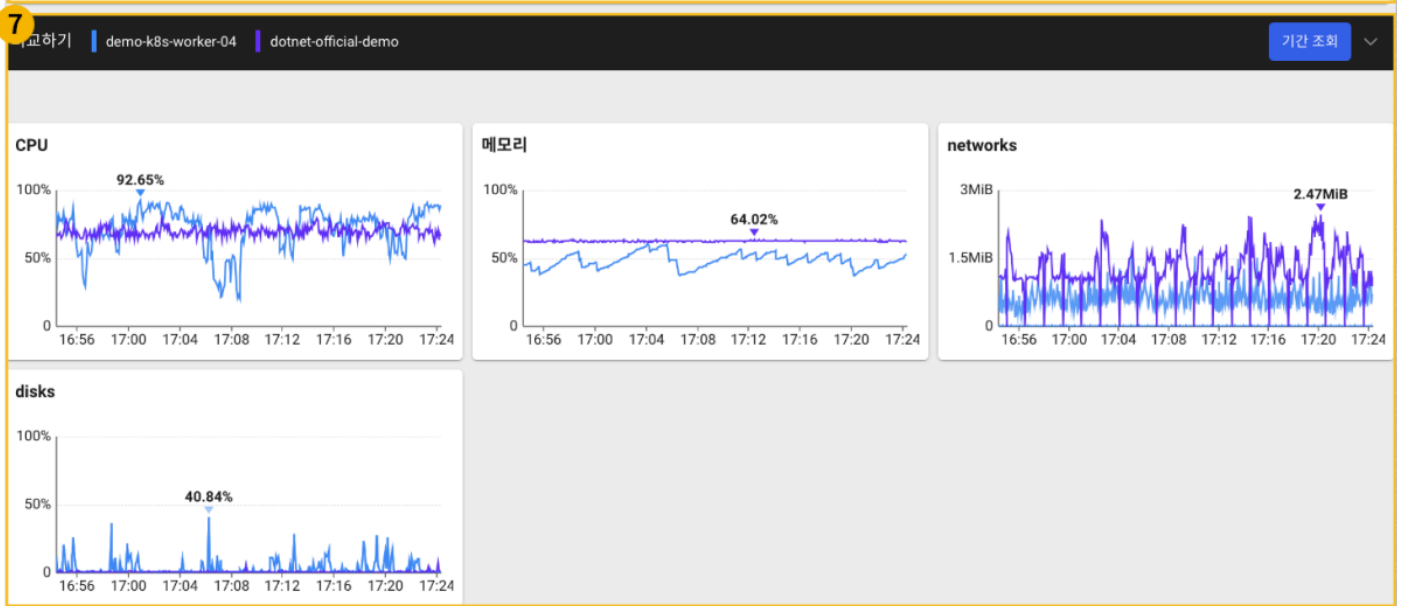
1. 오른쪽 화면에서 이전할 대상 프로젝트를 선택합니다.
2. 왼쪽 화면에서 이전할 에이전트를 선택하세요.
3. > **오른쪽 화살표** 버튼을 클릭해 대상 프로젝트로 이전합니다.
4. **저장** 버튼을 누르면 이전이 완료됩니다.

- ① • 실행 직후 10분 이내에 다시 동일 에이전트를 이동할 경우 충돌 현상을 유발할 수 있습니다.
- 수집된 데이터는 이전되지 않습니다. 과거 데이터 조회를 위해 기존 프로젝트는 당분간 삭제하지 마세요.

서버 간 비교

서버 간 비교 차트를 다음과 같이 제공합니다.

비교		서버 정보		CPU	메모리	디스크		네트워크	기타
비교	상태	에이전트명	OS 버전	CPU Used %	Memory Used %	Disk Used % (Max)	Disk I/O % (Max)	Network Traffic (Max)	Private IP
<input checked="" type="checkbox"/>		demo-k8s-worker-04	Ubuntu 22.04.2 L...	89.8%	53.1% (1.9G)	64.7%	0.6%	ens5 746K	127.0.0.1 10.21.1.210 10.244.4.1
<input type="checkbox"/>		go-official-demo	Ubuntu 22.04.2 L...	22.6%	13.1% (1G)	99.6%	0.3%	ens5 62.6K	127.0.0.1 10.21.1.118 172.17.0.1 172.18.0.1
<input checked="" type="checkbox"/>		dotnet-official-demo	Microsoft Windo...	66.6%	62.6% (9.8G)	55%	1.3%	Amazon ... 1M	10.21.1.51
<input type="checkbox"/>		mysql-official-demo-02	Ubuntu 22.04.2 L...	1.4%	80% (753M)	22.4%	0.1%	lo 84.5K	127.0.0.1 10.21.1.136
<input type="checkbox"/>		mysql-official-demo-03	Ubuntu 22.04.2 L...	0.8%	80.3% (756M)	22.1%	0.2%	lo 80.9K	127.0.0.1 10.21.1.236
<input type="checkbox"/>		node-official-demo	Ubuntu 22.04.2 L...	50.6%	79.4% (1.4G)	42.3%	0.5%	lo 157M	127.0.0.1 10.21.1.98
<input type="checkbox"/>		rum-official-demo	Ubuntu 22.04.2 L...	30.7%	27.4% (531M)	35.6%	0.1%	lo 873K	127.0.0.1 10.21.1.151
<input type="checkbox"/>		virtual-java-agent	Ubuntu 20.04.6 L...	44.6%	71.5% (2.6G)	36.9%	0.2%	lo 6.5M	127.0.0.1 10.21.1.26
<input type="checkbox"/>		demo-k8s-master	Ubuntu 22.04.2 L...	3.2%	29.6% (1.1G)	24.7%	1.5%	lo 5.3M	127.0.0.1 10.21.1.149 10.244.0.1



1. 비교하기 버튼을 선택하세요.
2. 6과 같이 서버 목록 왼쪽에 비교 컬럼이 추가된 것을 확인하세요.
3. 비교 컬럼에서 비교를 원하는 서버를 선택하세요.
4. 비교 기능이 활성화되면 7 영역에서 비교 차트를 조회할 수 있습니다.

- ① • 비교 서버는 5개까지 선택 가능합니다.
- 서버별 고유색이 할당됩니다. 고유색은 7 비교 차트에서 서버 구별을 위해 사용됩니다.
- 기간 조회 버튼을 선택하면 과거 데이터를 조회할 수 있습니다.

서버 상세

홈 화면 > 프로젝트 선택 > [서버 목록](#) > [서버 상세](#)

와탭 모니터링 서비스 초기 화면에서 프로젝트를 선택한 다음 [서버 목록](#) 메뉴 하위에 [서버 상세](#) 메뉴를 선택하세요. [서버 상세](#)는 서버의 자원 현황과 실행 프로세스의 상세 정보를 제공합니다.

서버 상세



1 시간 (5초 인터벌) 서버 선택

|| LIVE 12:02:04 30분
● whatap-server-demo-4

IP 주소: 222.237.239.142... 운영체제: windows CPU 코어: 4 Memory Total: 8 GB OS 버전: Microsoft Windows Server 2012 R2 Standard 6.3.9600

2

CPU Usage

CPU System | CPU User

Memory Usage

Memory Swap | Memory Used

Network

Intel(R) 82574L...

Disk I/O

C:

프로세스

▼ CPU 내림차순 ▼ 10 그룹화

이름	CPU	메모리	디스크 I/O	개수
WmiPrvSE.exe NT AUTHORITY\SYSTEM	Max 0.93%	Max 0.38%	Max 144KiB	Max 1
whatap_infra.exe NT AUTHORITY\SYSTEM	Max 0.55%	Max 0.56%	Max 71B	Max 2
svchost.exe NT AUTHORITY\SYSTEM	Max 0.39%	Max 0.73%	Max 302.2KiB	Max 4
WmiPrvSE.exe NT AUTHORITY\NETWORK S...	Max 0.18%	Max 0.18%	Max 146B	Max 1
IpOverUsbSvc.exe NT AUTHORITY\SYSTEM	Max 0%	Max 0.14%	Max 0	Max 1

서버 정보

[서버 알림 목록](#)

Display Name / ID	● whatap-server-demo-4 1973980398
OS	Microsoft Windows Server 2012 R2 Standard 6.3.9600
IP Address	222.237.239.142 / 192.168.178.244
Agent	2.2.3
Memo	테스트

1 상단 옵션

상단 1 영역에서 **데이터 갱신 시간** 및 조회할 **서버**를 지정할 수 있습니다. **데이터 갱신 시간** 및 **서버** 지정 옵션과 함께 해당 서버의 **요약 정보**를 확인할 수 있습니다.

데이터 갱신 시간

서버 상세 페이지의 데이터는 5초마다 자동으로 갱신합니다.

- || **일시정지** : 사용자는 데이터의 자동 갱신을 중지할 수 있습니다.
- ⏪ **재생** : 사용자는 중지한 자동 갱신을 재시작할 수 있습니다.
- ↺ **새로고침** : 사용자는 현재 시간을 기준으로 데이터를 갱신할 수 있습니다.

서버 선택

서버 선택 옵션을 통해 상세 내용을 조회할 서버를 지정할 수 있습니다. 선택창의 목록에서 조회할 서버를 선택하면 다음 2 영역에서 서버 자원 현황과 실행 프로세스의 상세 정보 등을 확인할 수 있습니다.

2 서버 상세

서버 자원 현황

2 영역에서 **CPU Usage**, **Memory Usage**, **Network**, **Disk I/O** 차트를 통해 해당 서버의 자원 현황을 확인할 수 있습니다.

- 📄: **CSV** 아이콘을 선택하면 차트 기록을 CSV 파일로 저장할 수 있습니다.
- 📷: **카메라** 아이콘을 선택하면 이미지 형식으로 차트 화면을 저장할 수 있습니다.
- 🔍: **상세** 아이콘을 선택하면 CPU 사용률, 메모리 사용률, 네트워크, 디스크 입출력 각 상세 차트를 확인할 수 있습니다.
 - CPU 사용률
CPU Usage, CPU Idle, CPU Nice, CPU I/O Wait, CPU Steal, CPU IRQ, CPU Soft IRQ, CPU Load
 - 메모리 사용률

Memory Usage, Memory Available, Memory SReclaimable, Memory SUnreclaim, Memory Slab, Memory Swap Used, Memory Page Faults

- 네트워크

Traffic In/Out, Packet In/Out, Error In/Out, Dropped In/Out

- 디스크 입출력

Disk I/O, IOPS Read/Write, Disk Bph Read/Write, Used Space, Queue Length, Inode Used, Free Space

프로세스 목록

정렬

- 프로세스 목록 상단에서 선택한 지표에 따라 내림차순 또는 오름차순 정렬을 지정해 조회할 수 있습니다.
- 프로세스 목록 상단에서 선택한 지표에 따라 상위 10개, 20개, 30개, 전체 프로세스를 지정해 확인할 수 있습니다.


그룹화

프로세스 그룹은 하나의 인스턴스에서 동일한 동작을 하는 여러 프로세스를 묶은 것입니다. 그룹화 버튼을 선택해 프로세스 그룹을 추가할 수 있습니다. 프로세스 그룹화에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.


서버 정보 패널


서버 정보 패널에서 확인할 수 있는 내용은 다음과 같습니다. 디스플레이 이름과 메모의 경우 서버 정보 패널에서만 편집이 가능합니다.

-  서버 알림 목록

서버 정보 패널 상단의  서버 알림 목록 버튼을 선택하면 현재 서버에 할당된 알림을 확인할 수 있습니다.

- Display Name/ID

선택한 서버의 디스플레이 이름(ONAME의 별칭)과 서버 아이디(OID)를 확인할 수 있습니다.  수정 아이콘을 선택하면 디스플레이 이름을 수정할 수 있습니다.

 ONAME은 디폴트로 호스트 이름이 설정됩니다.

- OS

선택한 서버의 OS 정보를 확인할 수 있습니다.

- IP Address

선택한 서버의 IP 주소를 확인할 수 있습니다.

- Agent

선택한 서버의 에이전트 버전을 확인할 수 있습니다.

- Memo

작성한 메모를 확인하거나 ✎ 수정 아이콘을 선택해 메모를 수정 및 추가 작성할 수 있습니다.

프로세스 그룹 추가

프로세스 그룹이란?

프로세스 그룹이란 하나의 인스턴스에서 동일한 동작을 하는 여러 개의 프로세스를 묶은 것입니다. 개별 프로세스가 아닌 그룹 단위로 모니터링하거나 알림을 받고 싶을 때 프로세스 그룹을 사용해 보세요.

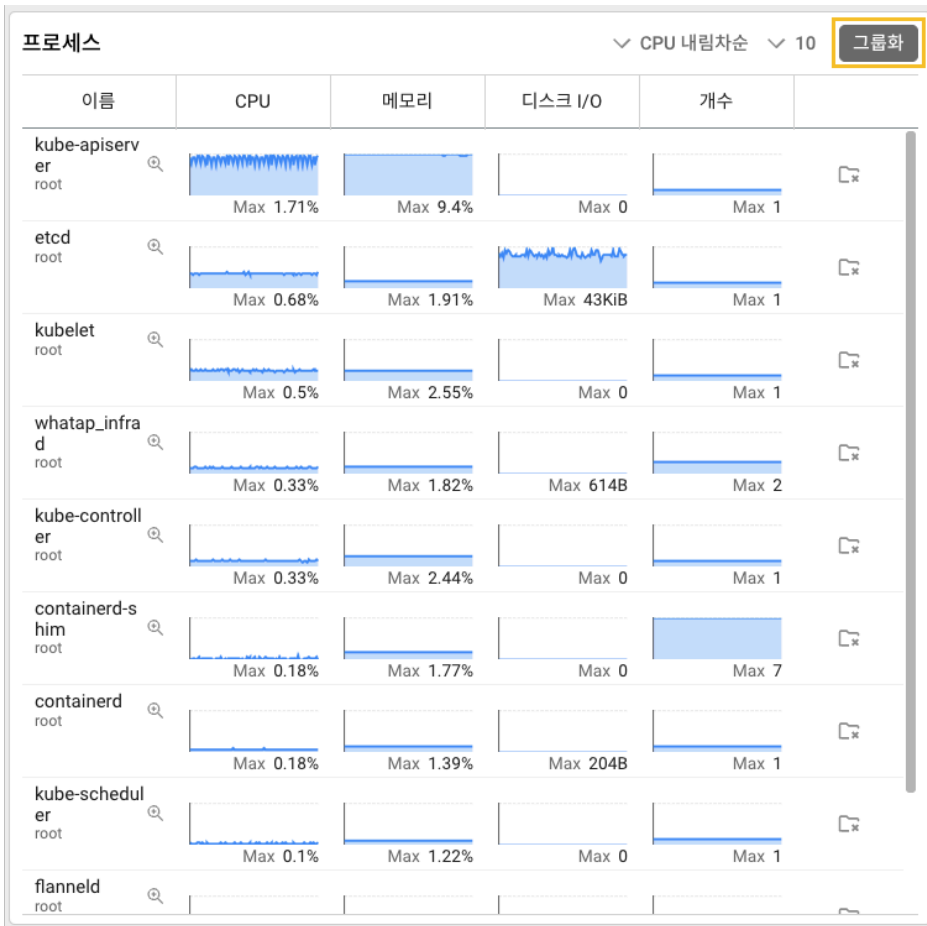
프로세스 그룹 메뉴에서 기존에 나뉘져 있던 각 프로세스의 자원 사용량 합계치를 한눈에 확인해 볼 수 있습니다. 개별 프로세스의 자원 사용량을 일일이 계산할 필요가 없어집니다.

프로세스 그룹의 자원 사용량 합계치가 특정 기준을 넘으면 알림을 받도록 지정할 수 있습니다. 알림 설정에 관한 자세한 설명은 [다음 문서](#)를 참조하세요.

프로세스 그룹 추가하기

❗ 프로젝트 수정 권한 또는 **알림 설정** 권한이 필요합니다. 권한에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

1. 홈 화면 > 프로젝트 선택 > **서버 목록** > **서버 상세**로 이동한 후 프로세스 목록에서 **그룹화** 버튼을 클릭하세요.



- 프로세스 그룹 설정창이 뜨면 **Pattern**에 해당 그룹에 포함할 프로세스 명칭 패턴을 앞뒤 별표(*)를 포함해서 입력하세요.
예시, whatap → *whatap*

Process Group

Pattern

ex) *whatap*

Pattern 별칭

적용

프로세스 패턴 명을 별칭으로 변경합니다

입력 후 오른쪽의 🔍 **돋보기** 버튼을 선택하세요. 해당 패턴에 해당하는 프로세스 목록을 조회할 수 있습니다. 프로세스 명칭은 화면 상에 표시되는 프로세스 명을 기준으로 합니다.

3. **Pattern 별칭**에 프로세스 그룹 이름을 입력하고 오른쪽의 **적용** 버튼을 선택하세요. 그룹화 설정 시 **설정된 프로젝트의 모든 서버**에 해당 그룹화가 진행됩니다.

프로세스 그룹 예시

• 프로세스 그룹화 적용

다음 화면은 **Pattern**에 *tomcat*을 입력하고, **Pattern 별칭**을 test_group으로 적용한 예시입니다.

Process Group

Pattern

tomcat

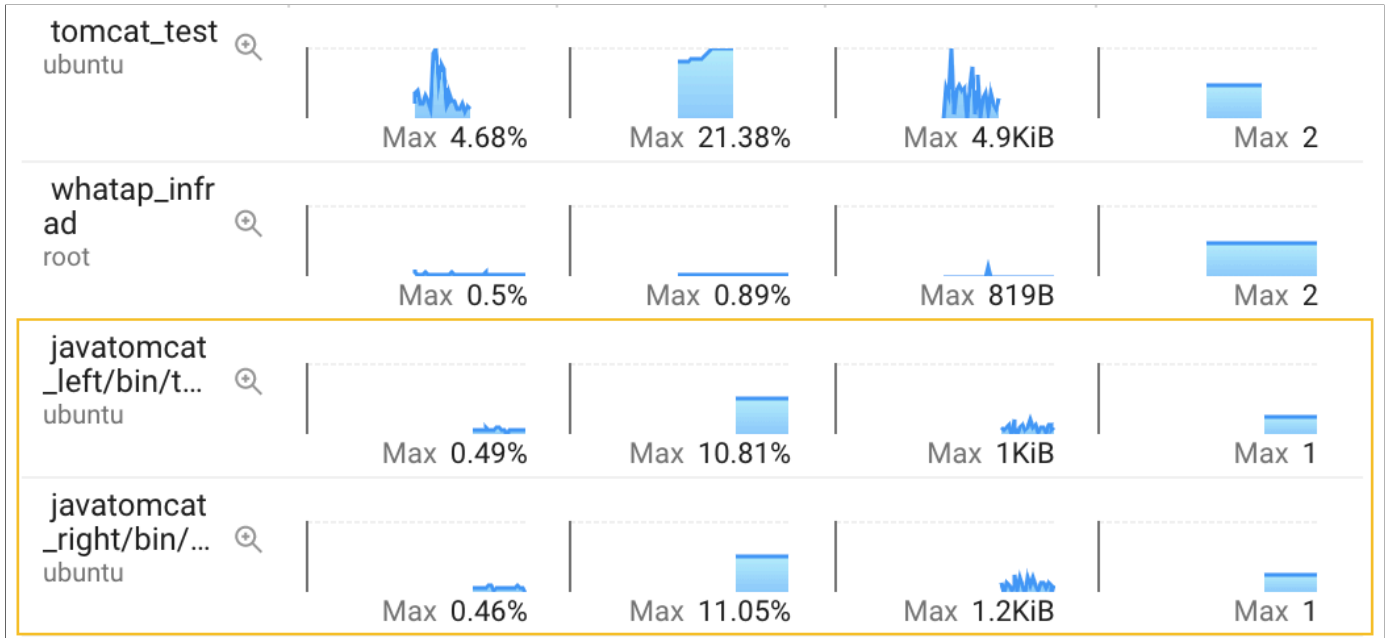
Pattern 별칭

test_group

적용

프로세스 패턴 명을 별칭으로 변경합니다

• 프로세스 그룹화 이전 프로세스 목록



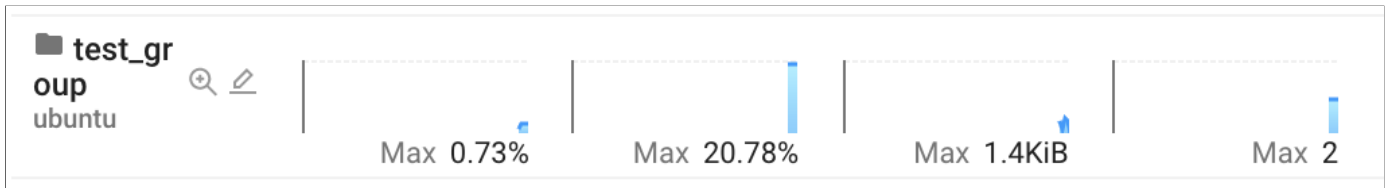
Pattern에 맞게 그룹화할 프로세스 목록은 다음과 같습니다.



- 예시, javatomcat_left/bin/test.jarcom.virtual.App
- 예시, javatomcat_right/bin/test.jarcom.virtual.App

• 프로세스 그룹화 등록 확인

새로운 프로세스 그룹 test_group이 다음과 같이 프로세스 목록에 등록된 것을 확인할 수 있습니다.



- ⓘ • 그룹화 적용 이후 프로세스 그룹에서 각 프로세스에 해당하는 데이터를 합산한 수치를 확인할 수 있습니다.
- 그룹화 이전의 데이터를 확인하려면 프로세스별로 데이터를 확인하세요.

큐브

홈 화면 > 프로젝트 선택 > 분석 > 큐브

와탭 모니터링 서비스 초기 화면에서 프로젝트를 선택한 다음 [프로젝트 메뉴](#) 하위에 [분석 > 큐브](#)를 선택하세요.

큐브란?

와탭은 5분 단위로 만든 성능 통계를 **큐브**라고 부릅니다. 큐브 분석은 큐브에 저장된 5분 단위 성능 데이터를 활용한 분석 기능입니다.



1 큐브 셀렉트 패널

왼쪽의 큐브 셀렉트 패널에서 특정 시간 기준으로 큐브를 선택하세요. 큐브는 5분 단위로 저장되어 있기 때문에 특정 시간을 선택해야 합니다.

• 패널 관심 지표

서버 큐브 셀렉트 패널의 관심 지표는 CPU와 메모리입니다.

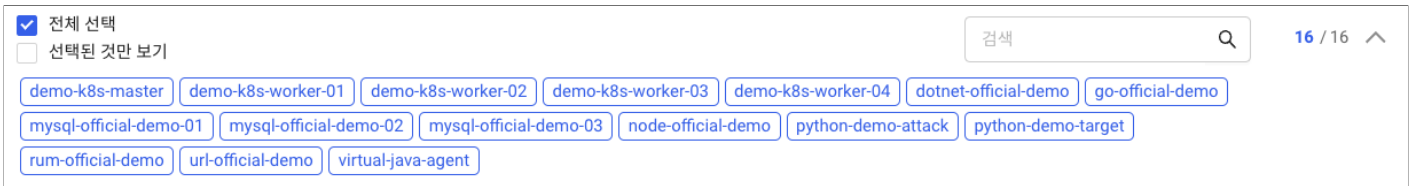
• 큐브 표시색

큐브는 선택된 지표의 수치에 따라 다른 색으로 표현됩니다.

- 남색: 높은 수치
- 하늘색: 낮은 수치

2 애플리케이션 선택자

상단 2 영역의 애플리케이션 선택자 옵션을 통해 특정 애플리케이션의 데이터를 선택할 수 있습니다. 오른쪽의 ∨ 버튼을 선택하면 다음과 같이 선택 가능한 전체 애플리케이션을 확인할 수 있습니다.



- 전체 선택: 모든 애플리케이션을 조회합니다. 기본은 전체 선택과 활성 애플리케이션이 선택되어있습니다.
- 선택된 것만 보기: 애플리케이션 중 사용자가 지정한 해당 애플리케이션만 조회합니다.
- 검색: 애플리케이션이 많은 경우 입력창을 통해 해당 애플리케이션을 검색할 수 있습니다.
- 숫자/숫자: 지정한 애플리케이션 개수/전체 애플리케이션 개수를 표시합니다.

3 큐브 데이터

- ① • 차트 상단 오른쪽의 📊 아이콘을 선택하면 바형 차트를 제공합니다.
 - 차트 상단 오른쪽의 📈 아이콘을 선택하면 선형 차트를 제공합니다.

3 영역에서 해당 큐브 데이터를 CPU, 메모리, 디스크, 네트워크 등의 차트를 통해 확인할 수 있습니다.

- CPU
 - 프로젝트 내 애플리케이션을 CPU 사용량이 많은 순서대로 정렬해 표시합니다.
- 메모리

프로젝트 내 애플리케이션을 메모리 사용량이 많은 순서대로 정렬해 표시합니다.

- [디스크](#)

프로젝트 내 애플리케이션을 디스크 사용량이 많은 순서대로 정렬해 표시합니다.

- [네트워크](#)

프로젝트 내 애플리케이션을 네트워크 입출력 트래픽량이 많은 순서대로 정렬해 표시합니다.

ⓘ WhaTap uses the IP2Location LITE database for [IP geolocation](#).

보고서

홈 화면 > 프로젝트 선택 > [보고서](#)

보고서는 개별 프로젝트에 대해 서비스 이용 현황과 장애 발생 기록을 보고하는 문서입니다. 서비스 모니터링 담당자는 보고서를 통해 관련 부서 담당자들과 현황을 공유합니다.

모니터링 데이터 분석은 서비스의 개선 방향을 정하는 지표가 되기 때문에 중요합니다. 하지만 여러 대시보드의 데이터를 취합해서 문서화하는 일은 번거롭습니다.

와탭의 [보고서](#) 메뉴는 [보고서 작성 업무 자동화](#)를 지원합니다. 매주 보고서를 작성해야 하는 일, 정해진 시간에 보고서를 공유하는 일, 여러 가지 서식을 관리하는 일 모두 [보고서](#) 메뉴에서 할 수 있습니다.

✔ [보고서](#)를 다운로드하거나 인쇄, 메일 발송 예약을 원하면 해당 버튼을 클릭하세요. HTML 형식으로 다운로드할 수 있습니다.

보고서와 통합 보고서의 차이

- [보고서](#)는 하나의 프로젝트에 대한 보고서를 생성하는 메뉴입니다. 따라서 프로젝트를 선택한 다음 사이드 메뉴의 [보고서](#) 메뉴를 통해 진입할 수 있습니다.
- [통합 보고서](#)는 여러 프로젝트에 대한 보고서를 생성하는 메뉴입니다. 프로젝트를 선택하지 않고 홈 화면의 사이드 메뉴에서 진입할 수 있습니다. [통합 보고서](#)에 대한 자세한 내용은 [다음 문서](integrated-report)에서 확인할 수 있습니다.

보고서의 종류

기본 보고서는 대기업, 공공기관 및 IT 서비스 기업에서 실제로 사용하고 있는 양식입니다. 원하는 양식이 있으면 support@whatap.io로 요청해 주세요. 요청한 보고서는 [보고서](#) 목록에 추가됩니다.

보고서 양식 추가

- 요청 양식이 범용성이 있을 경우 [보고서](#) 목록에 추가로 제공합니다.
- 요청 시 HTML 및 CSS 양식이 함께 제공될 경우 추가가 용이합니다.

> [요청 양식 예시](#)

보고서 양식 추가 요청 시 예시와 같이 원하는 HTML 및 CSS 양식 첨부를 권장합니다. 세부 사항은 다음 예시 파일을 참조하세요.

- [예시 파일](#): 다운로드 후 ZIP 형식의 압축을 풀어 HTML 형식의 예시 파일을 확인하세요. 파일 내 주석에 커스터마이징을 위한 CSS 영역과 HTML 영역 안내가 기술되어있습니다.

메일 발송 예약

정기적으로 보고서를 이메일로 받으려면 [보고서 메일 발송 예약](#)을 선택하세요. 출근 직후 수행하던 여러 가지 서비스 점검 절차를 메일 확인으로 대체할 수 있습니다.

보고서 메일 발송 예약
×

① 등록 다음날 부터 04~06시에 리포트가 발송됩니다.

② 최대 5건의 리포트 메일 설정이 가능합니다.

보고서 종류 리포트

발송 요일 Mon Tue Wed Thu Fri Sat Sun

보고 시간 00:00 ~ 23:59

메일 + 저장

서버 보고서

홈 화면 > 프로젝트 선택 > 보고서

와탭 모니터링 서비스 초기 화면에서 프로젝트를 선택한 다음 프로젝트 메뉴 하위에 [보고서](#)를 선택하세요. 보고서 화면에서 ∨ 버튼을 클릭하면 일간, 주간, 월간으로 분류된 각종 분석 보고서를 확인할 수 있습니다.

일간 서버 보고서

[일간 서버 보고서](#)는 하루 동안의 서버 자원 사용량을 확인할 수 있는 보고서입니다. 시작일, 시작 시간, 종료 시간을 직접 설정하여 조회할 수 있습니다.

개요

프로젝트명	호스트 건수 (증감건)	알림 건수 (증감건)
Server Monitoring Demo	16 (-)	30 (-5)

프로젝트 이름과 호스트 수, 발생한 알림 건수를 요약해서 볼 수 있습니다. 호스트 건수와 알림 건수의 경우 전날과 비교하여 얼마나 변동이 있었는지를 함께 확인할 수 있습니다.

- **호스트 건수** : 조회 기간 동안의 총 서버 개수입니다.
- **알림 건수** : 조회 기간 동안 발생한 알림의 전체 건수입니다.

서버 목록

서버그룹명 (uptime)		CPU코어	메모리 정보	CPU(%) 평균	CPU(%) 최대	메모리 (%) 평균	메모리(%) 최대	알림 건수		
								D-day	D-1	D-7
demo-k8s-master (111일 5시간 54분)	2	4 Gb	3.9	55.73 (18:25 ~ 18:30)	29.57	30.62 (18:25 ~ 18:30)	0	0	0	
demo-k8s-worker-01 (25일 10시간 13분)	2	8 Gb	5.05	56.81 (11:25 ~ 11:30)	19.88	28.17 (11:25 ~ 11:30)	0	0	0	
demo-k8s-worker-02 (39일 6시간 34분)	2	4 Gb	9.47	60.73 (18:25 ~ 18:30)	44.25	56.99 (09:55 ~ 10:00)	0	0	0	
demo-k8s-worker-03 (39일 7시간 23분)	2	4 Gb	8.03	67.42 (15:35 ~ 15:40)	43.61	55.89 (10:40 ~ 10:45)	0	0	0	
demo-k8s-worker-04 (25일 13시간 14분)	2	4 Gb	21.86	80.89 (09:05 ~ 09:10)	44.87	53.63 (09:05 ~ 09:10)	2	10	13	
dotnet-official-demo (19일 11시간 41분)	4	16 Gb	67.45	92.34 (12:40 ~ 12:45)	61.01	84.95 (23:45 ~ 23:50)	2	3	4	
go-official-demo (68일 13시간 14분)	2	8 Gb	19.02	26.18 (17:00 ~ 17:05)	14.45	15.34 (18:05 ~ 18:10)	0	1	2	
mysql-official-demo-01 (0일 0시간 0분)		0 Gb	0.0	0.0 (00:00 ~ 00:00)	0.0	0.0 (00:00 ~ 00:00)	0	0	0	
mysql-official-demo-02 (119일 10시간 29분)	2	1 Gb	1.94	64.25 (15:30 ~ 15:35)	80.96	90.38 (15:30 ~ 15:35)	0	0	1	
mysql-official-demo-03 (113일 13시간 7분)	2	1 Gb	2.09	56.32 (17:25 ~ 17:30)	80.22	89.3 (17:25 ~ 17:30)	0	0	0	
node-official-demo (113일 8시간 26분)	2	2 Gb	31.99	80.48 (19:00 ~ 19:05)	77.05	89.81 (19:20 ~ 19:25)	9	5	2	
python-demo-attack (81일 8시간 42분)	2	2 Gb	0.6	60.82 (15:05 ~ 15:10)	26.84	32.03 (15:05 ~ 15:10)	0	0	0	
python-demo-target (81일 8시간 42분)	1	1 Gb	1.89	100.0 (09:10 ~ 09:15)	58.68	69.35 (15:20 ~ 15:25)	1	0	0	
rum-official-demo (97일 7시간 31분)	2	2 Gb	26.62	93.33 (15:15 ~ 15:20)	27.95	29.3 (23:25 ~ 23:30)	15	13	13	
url-official-demo (63일 6시간 58분)	2	1 Gb	0.81	52.23 (20:25 ~ 20:30)	73.62	81.62 (20:25 ~ 20:30)	0	0	1	
virtual-java-agent (166일 8시간 31분)	2	4 Gb	27.07	93.33 (15:50 ~ 15:55)	70.15	73.68 (15:50 ~ 15:55)	1	3	0	

서버별로 일간 주요 지표들을 확인할 수 있습니다. CPU 최댓값(CPU Max)과 메모리 최댓값(MEM Max)의 경우 해당 수치가 발생한 시간을 함께 표시합니다.

알림 건수는 7일 전, 1일 전, 조회 당일을 함께 조회하여 비교해 볼 수 있습니다.

ⓘ CPU, 메모리의 평균, 최댓값이 90% 이상인 경우 **빨간색**으로 표시됩니다.

알림 기록

생성시간	등급	서버명	설명
23:55	Critical	rum-official-demo	CPU Steal > 10 %
22:12	Critical	rum-official-demo	CPU Steal > 10 %
20:33	Critical	rum-official-demo	CPU Steal > 10 %
18:37	Critical	rum-official-demo	CPU Steal > 10 %
16:55	Critical	rum-official-demo	CPU Steal > 10 %
15:50	Warning	dotnet-official-demo	Memory Used > 70 %
15:24	Warning	python-demo-target	CPU Used > 70 %
15:14	Warning	node-official-demo	Memory Used > 70 %
15:06	Critical	rum-official-demo	CPU Steal > 10 %
15:04	Warning	node-official-demo	Memory Used > 70 %
14:00	Warning	dotnet-official-demo	CPU Used > 70 %
13:33	Critical	rum-official-demo	CPU Steal > 10 %
13:20	Warning	node-official-demo	Memory Used > 70 %
11:35	Critical	rum-official-demo	CPU Steal > 10 %
10:26	Warning	node-official-demo	Memory Used > 70 %
10:05	Critical	rum-official-demo	CPU Steal > 10 %
08:57	Warning	node-official-demo	Memory Used > 70 %

조회한 시간 동안 발생한 알림 기록에 대해 발생 시간, 등급, 발생한 서버 이름, 해당 알림이 발생한 원인을 확인할 수 있습니다. 각 알림에 대한 상세 정보는 [경고 알림 > 이벤트 기록](#) 메뉴에서 조회할 수 있습니다. 해당 프로젝트에 대해 알림 기록이 없는 경우 '해당 기간에 데이터가 존재하지 않습니다'라는 안내 문구가 뜰 수 있습니다.

ⓘ 알림의 레벨에 따라 **Critical**은 **빨간색**, **Warning**은 **주황색**, **Info**는 **회색**으로 표시됩니다.

주간 서버 보고서

주간 서버 보고서는 일주일간 서버의 CPU, Memory 사용량을 확인할 수 있는 보고서입니다. 시작일을 직접 설정할 수 있으며, 조회 당일 기준 7일 전부터 조회 가능합니다. 시작일로부터 7일간의 데이터를 조회합니다.

전체 자원 사용 목록

CPU

그룹명	서버명	항목	사용률							
			08/31	09/01	09/02	09/03	09/04	09/05	09/06	
	demo-k8s-master	CPU(%)	평균	3.4 %	3.42 %	3.39 %	3.37 %	3.52 %	3.87 %	3.9 %
			최대 95%	5.63 %	5.67 %	5.42 %	5.32 %	5.78 %	7.28 %	6.06 %
			최대	56.5 %	15.5 %	56.16 %	37.32 %	53.0 %	42.66 %	55.73 %
	demo-k8s-worker-01	CPU(%)	평균	1.0 %	0.99 %	0.99 %	0.99 %	0.99 %	1.09 %	5.05 %
			최대 95%	1.77 %	1.8 %	1.77 %	1.71 %	1.76 %	4.44 %	17.7 %
			최대	44.28 %	43.49 %	37.84 %	47.96 %	32.79 %	73.75 %	56.81 %
	demo-k8s-worker-02	CPU(%)	평균	14.34 %	13.92 %	13.13 %	12.2 %	13.47 %	14.22 %	9.47 %
			최대 95%	32.77 %	31.21 %	29.56 %	27.57 %	31.4 %	32.62 %	33.11 %
			최대	78.72 %	43.24 %	59.2 %	71.86 %	79.01 %	83.0 %	60.73 %
	demo-k8s-worker-03	CPU(%)	평균	12.34 %	11.33 %	10.28 %	11.79 %	11.34 %	12.27 %	8.03 %
			최대 95%	27.9 %	27.95 %	23.28 %	28.46 %	27.11 %	31.3 %	27.64 %
			최대	80.54 %	45.85 %	67.52 %	76.83 %	44.53 %	75.89 %	67.42 %
	demo-k8s-worker-04	CPU(%)	평균	31.56 %	29.83 %	25.58 %	22.32 %	24.96 %	30.78 %	21.86 %
			최대 95%	93.33 %	92.22 %	71.68 %	56.43 %	61.17 %	92.62 %	56.99 %
			최대	100.0 %	100.0 %	94.16 %	76.97 %	85.68 %	95.86 %	80.89 %
	dotnet-official-demo	CPU(%)	평균	68.7 %	68.22 %	68.87 %	72.38 %	70.05 %	69.24 %	67.45 %
			최대 95%	84.38 %	83.39 %	83.88 %	88.22 %	86.52 %	85.97 %	79.49 %
			최대	87.73 %	91.08 %	96.25 %	99.65 %	96.1 %	92.26 %	92.34 %
	go-official-demo	CPU(%)	평균	21.51 %	20.23 %	16.03 %	16.88 %	18.43 %	19.26 %	19.02 %
			최대 95%	27.69 %	26.62 %	22.06 %	21.7 %	23.18 %	24.41 %	23.1 %
			최대	30.92 %	28.35 %	47.81 %	23.19 %	41.99 %	51.59 %	26.18 %
mysql-official-demo-01	CPU(%)	평균	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	
		최대 95%	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	
		최대	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	

조회 기간 동안 각 서버의 CPU 사용률을 일별로 조회합니다. 조회되는 항목으로는 CPU 평균, 최대 95%, 최댓값이 있으며, 각 수치는 백분율로 표시됩니다.

⚠ 최대 95%

상위 5% 데이터를 제외한 최댓값을 의미합니다. 서버 재기동 등의 이유로 인해 순간적으로 높게 나온 수치를 제외하고 보기 위함입니다.

메모리

그룹명	서버명	항목	사용률							
			08/31	09/01	09/02	09/03	09/04	09/05	09/06	
demo-k8s-master	메모리(%)	평균	29.27 %	29.31 %	29.2 %	29.21 %	29.13 %	29.35 %	29.57 %	
		최대	31.1 %	29.98 %	31.04 %	31.19 %	30.51 %	32.51 %	30.62 %	
demo-k8s-worker-01	메모리(%)	평균	11.95 %	11.94 %	11.93 %	11.93 %	11.96 %	12.39 %	19.88 %	
		최대	12.56 %	12.59 %	12.61 %	12.25 %	13.29 %	15.0 %	28.17 %	
demo-k8s-worker-02	메모리(%)	평균	54.16 %	53.76 %	53.59 %	53.33 %	53.76 %	53.81 %	44.25 %	
		최대	57.59 %	56.59 %	56.0 %	56.61 %	57.08 %	57.44 %	56.99 %	
demo-k8s-worker-03	메모리(%)	평균	53.19 %	53.71 %	53.33 %	53.09 %	53.45 %	53.11 %	43.61 %	
		최대	59.6 %	56.77 %	56.48 %	56.57 %	56.33 %	56.32 %	55.89 %	
demo-k8s-worker-04	메모리(%)	평균	56.71 %	57.37 %	57.96 %	57.07 %	57.82 %	55.8 %	44.87 %	
		최대	72.3 %	70.45 %	71.37 %	59.56 %	61.72 %	71.89 %	53.63 %	
dotnet-official-demo	메모리(%)	평균	60.68 %	42.38 %	48.59 %	50.0 %	48.93 %	62.02 %	61.01 %	
		최대	85.33 %	86.56 %	67.42 %	78.0 %	67.41 %	86.34 %	84.95 %	
go-official-demo	메모리(%)	평균	14.98 %	15.0 %	14.39 %	14.37 %	14.35 %	14.41 %	14.45 %	
		최대	15.62 %	15.93 %	14.74 %	14.77 %	14.73 %	14.95 %	15.34 %	
mysql-official-demo-01	메모리(%)	평균	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	
		최대	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	
mysql-official-demo-02	메모리(%)	평균	80.06 %	80.08 %	80.73 %	80.93 %	80.73 %	80.75 %	80.96 %	
		최대	87.76 %	87.88 %	87.68 %	88.16 %	88.27 %	85.88 %	90.38 %	
mysql-official-demo-03	메모리(%)	평균	79.66 %	79.7 %	80.25 %	80.21 %	80.15 %	80.26 %	80.22 %	
		최대	87.93 %	88.51 %	88.33 %	89.17 %	82.4 %	86.93 %	89.3 %	

조회 기간 동안 각 서버의 메모리 사용량을 일별로 조회합니다. 조회되는 항목으로는 메모리 사용 평균값, 최댓값이 있으며, 각 수치는 백분율로 표시됩니다.

디스크

그룹명	서버명	마운트 위치	전체 디스크	사용률						
				08/31	09/01	09/02	09/03	09/04	09/05	09/06
	demo-k8s-master	/ (/dev/root)	19.2 Gb	25.35 %	25.09 %	25.09 %	25.09 %	25.09 %	25.04 %	25.31 %
	dotnet-official-demo	C: (C:)	128.0 Gb	55.84 %	56.45 %	57.67 %	58.15 %	58.96 %	59.64 %	60.21 %
	go-official-demo	/ (/dev/root)	19.2 Gb	100.0 %	100.0 %	100.0 %	100.0 %	100.0 %	100.0 %	100.0 %
	mysql-official-demo-01	/ (/dev/root)	19.2 Gb	24.31 %	24.62 %	24.71 %	24.75 %	24.82 %	24.91 %	25.27 %
	mysql-official-demo-02	/ (/dev/root)	19.2 Gb	23.13 %	24.23 %	23.46 %	23.49 %	23.58 %	23.77 %	25.87 %
	mysql-official-demo-03	/ (/dev/root)	19.2 Gb	22.82 %	24.49 %	23.14 %	23.16 %	23.39 %	23.28 %	23.45 %
	node-official-demo	/ (/dev/root)	19.21 Gb	46.58 %	44.74 %	44.7 %	44.25 %	44.7 %	45.18 %	46.76 %
	python-demo-attack	/ (/dev/root)	7.58 Gb	65.05 %	63.04 %	63.72 %	63.75 %	62.72 %	63.79 %	68.33 %
	python-demo-target	/ (/dev/root)	7.57 Gb	69.64 %	68.08 %	68.48 %	68.56 %	69.64 %	69.89 %	74.64 %
	rum-official-demo	/ (/dev/root)	19.2 Gb	38.95 %	36.25 %	36.44 %	36.28 %	35.96 %	36.11 %	36.22 %
	url-official-demo	/ (/dev/root)	19.21 Gb	27.26 %	26.51 %	26.54 %	26.62 %	26.67 %	27.11 %	27.21 %
	virtual-java-agent	/ (/dev/root)	19.21 Gb	37.45 %	39.01 %	38.33 %	38.28 %	38.38 %	38.48 %	40.24 %

조회 기간 동안 각 서버에 마운트 된 파일 시스템별 지표입니다. 마운트 위치와 전체 디스크, 사용률을 조회하며 각 수치는 백분율로 표시됩니다.

- ① 수치가 90% 이상인 경우 빨간색으로 표시됩니다.
- 그룹명에는 `okindName` 이 표시되며, `okindName` 을 설정하지 않은 경우 빈칸으로 표시될 수 있습니다.

월간 서버 보고서

월간 서버 보고서는 한 달 동안의 서버의 자원 사용량 및 정보를 확인할 수 있는 보고서입니다. 시작일을 직접 설정할 수 있으며, 조회 당일 기준 30일 전부터 조회 가능합니다.

개요

전체 호스트	전체 코어	전체 디스크	전체 디스크 사용량	전체 메모리	전체 메모리 사용량	전체 알립
18	31	450.40G	175.53G	48.11G	22.43G	6275

한 달 동안 서버의 전체 자원 사용 내역을 취합하여 볼 수 있습니다.

- **전체 호스트** : 조회 기간 동안의 총 서버 개수입니다.
- **전체 코어** : 조회 기간 동안 사용된 총 코어 개수입니다.
- **전체 디스크** : 조회 기간 동안 마운트 된 총 파일 시스템 크기입니다.
- **전체 알림** : 조회 기간 동안 발생한 알림의 전체 건수입니다.

서버 정보

서버명	IP 주소	OS 정보	CPU 정보	메모리 정보
demo-k8s-master		Ubuntu 22.04.2 LTS	Intel(R) Xeon(R) Platinum 8375C CPU @ 2.90GHz 2 core	3.75G
demo-k8s-worker-01		Ubuntu 22.04.2 LTS	Intel(R) Xeon(R) Platinum 8375C CPU @ 2.90GHz 2 core	7.61G
demo-k8s-worker-02		Ubuntu 22.04.2 LTS	Intel(R) Xeon(R) Platinum 8375C CPU @ 2.90GHz 2 core	3.74G
demo-k8s-worker-03		Ubuntu 22.04.2 LTS	Intel(R) Xeon(R) Platinum 8375C CPU @ 2.90GHz 2 core	3.74G
demo-k8s-worker-04		Ubuntu 22.04.2 LTS	Intel(R) Xeon(R) Platinum 8175M CPU @ 2.50GHz 2 core	3.76G
dotnet-official-demo		Microsoft Windows Server 2022 Datacenter 1 0.0.20348	Intel(R) Xeon(R) Platinum 8375C CPU @ 2.90GHz 4 core	15.73G
go-official-demo		Ubuntu 22.04.2 LTS	Intel(R) Xeon(R) Platinum 8175M CPU @ 2.50GHz 2 core	7.65G
mysql-official-demo-01		Ubuntu 22.04.3 LTS	Intel(R) Xeon(R) Platinum 8259CL CPU @ 2.50GHz 2 core	941.21M
mysql-official-demo-01			core	-
mysql-official-demo-02		Ubuntu 22.04.2 LTS	Intel(R) Xeon(R) Platinum 8259CL CPU @ 2.50GHz 2 core	941.21M
mysql-official-demo-02		Ubuntu 22.04.2 LTS	Intel(R) Xeon(R) Platinum 8259CL CPU @ 2.50GHz 2 core	941.21M
mysql-official-demo-03		Ubuntu 22.04.2 LTS	Intel(R) Xeon(R) Platinum 8175M CPU @ 2.50GHz 2 core	941.21M
node-official-demo		Ubuntu 22.04.2 LTS	N/A 2 core	1.81G
python-demo-attack		Ubuntu 22.04.2 LTS	N/A 2 core	1.80G
python-demo-target		Ubuntu 22.04.2 LTS	Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz 1 core	965.74M
rum-official-demo		Ubuntu 22.04.2 LTS	Intel(R) Xeon(R) Platinum 8259CL CPU @ 2.50GHz 2 core	1.89G
url-official-demo		Ubuntu 22.04.1 LTS	N/A 2 core	918.28M
virtual-java-agent		Ubuntu 20.04.6 LTS	N/A 2 core	3.73G

조회 기간 동안 가동된 서버의 IP 주소, OS 정보, CPU 정보, 메모리 사용량을 보여줍니다.

알림 내역

총 알림건수 :6275		1주 (08.07-08.13)					2주 (08.14-08.20)					3주 (08.21-08.27)					4주 (08.28-09.03)					5주 (09.04-09.06)				
demo-k8s-master		0					0					0					0					0				
demo-k8s-worker-01		8					0					0					0					0				
demo-k8s-worker-02		0					0					0					0					0				
demo-k8s-worker-03		0					0					0					0					0				
demo-k8s-worker-04		7					63					72					68					14				
dotnet-official-demo		4184					1131					34					28					11				
go-official-demo		15					7					9					17					3				
mysql-official-demo-01		0					0					0					0					0				
mysql-official-demo-01		0					0					0					0					0				
mysql-official-demo-02		0					1					0					1					0				
mysql-official-demo-02		0					0					0					0					0				
mysql-official-demo-03		0					1					0					0					0				
node-official-demo		2					29					29					13					15				
python-demo-attack		0					0					0					0					0				
python-demo-target		0					0					0					0					1				
rum-official-demo		11					81					105					98					41				
url-official-demo		4					18					10					8					0				
virtual-java-agent		43					36					37					16					4				

조회 기간의 전체 서버에 대한 총 알림 건수를 확인할 수 있으며, 서버별로 발생한 알림을 주 단위로 나누어 볼 수 있습니다.

서버 사용 목록

서버명	항목	08/07	08/08	08/09	08/10	08/11	08/12	08/13	08/14	08/15	08/16	08/17	08/18	08/19	08/20	08/21	08/22	08/23	08/24	08/25	08/26	08/27	08/28	08/29	08/30	08/31	09/01	09/02	09/03	09/04	09/05	09/06	
demo-k8s-master	CPU(%) 평균	3.79	3.76	3.78	3.76	3.6	3.4	3.45	3.37	3.38	3.46	3.4	3.39	3.36	3.35	3.35	3.38	3.35	3.38	3.39	3.38	3.36	3.36	3.38	3.38	3.42	3.4	3.42	3.39	3.37	3.52	3.87	3.9
	CPU(%) 최대	21.8	48.8	55.5	21.4	47.5	60.0	42.4	19.9	57.0	54.8	47.4	53.6	56.2	41.1	45.3	54.9	54.6	54.4	54.7	50.8	37.5	19.5	55.2	60.7	56.5	15.5	56.1	37.3	53.0	42.6	55.73	
	디스크(%) 평균	24.6	24.6	24.6	24.6	24.7	24.7	24.5	24.5	24.6	24.7	24.7	24.7	24.7	24.7	24.7	24.7	24.7	24.7	24.6	24.6	24.6	24.6	24.6	24.6	24.6	24.6	24.7	24.7	24.7	24.7	24.7	24.79
	디스크(%) 최대	24.9	24.9	24.9	24.9	24.9	26.9	24.9	24.9	25.1	24.9	25.0	25.0	25.0	25.0	25.1	25.0	25.1	24.9	24.9	24.9	24.9	24.9	24.9	24.9	24.9	24.9	25.3	25.0	25.0	25.0	25.0	25.04
	메모리(%) 평균	29.4	29.3	29.3	29.4	29.4	29.4	29.5	29.5	29.5	29.5	29.5	29.6	29.5	29.4	29.4	29.5	29.3	29.5	29.4	29.3	29.3	29.3	29.3	29.3	29.4	29.4	29.2	29.3	29.3	29.3	29.3	29.5
	메모리(%) 최대	30.2	31.4	30.6	30.1	31.6	31.4	1	1	30.5	30.6	30.5	30.8	30.9	30.5	31.2	30.9	30.1	32.3	30.4	30.2	30.1	31.2	30.4	31.9	32.4	31.1	29.9	31.0	31.1	30.5	32.5	30.62
demo-k8s-worker-01	CPU(%) 평균	18.9	19.5	20.7	18.2	10.6	1.01	0.99	0.99	1.0	0.99	0.99	0.99	0.99	0.98	0.99	1.0	0.99	0.99	0.99	0.99	0.99	1.0	0.99	1.0	1.01	1.0	0.99	0.99	0.99	1.09	5.05	
	CPU(%) 최대	89.0	94.6	86.1	87.6	68.9	55.7	46.3	15.7	53.8	50.4	45.1	37.3	50.6	16.5	37.7	51.6	51.7	31.1	44.4	11.43	51.7	41.4	46.8	56.5	44.2	43.4	37.8	47.9	32.7	73.7	56.81	
	디스크(%) 평균	37.4	37.5	37.4	37.5	40.0	46.4	46.3	46.3	46.3	46.3	46.3	46.3	46.3	46.3	46.3	46.3	46.3	46.3	46.3	46.3	46.3	46.3	46.3	46.3	46.3	46.4	46.5	46.5	46.6	48.2	52.54	
	디스크(%) 최대	41.7	41.9	42.0	42.2	48.4	46.4	46.4	46.6	46.6	46.6	46.4	46.5	46.4	46.6	46.3	46.4	46.6	46.3	46.3	46.3	46.3	46.3	46.3	46.3	46.3	46.3	46.6	46.7	46.7	46.7	52.5	52.95
	메모리(%) 평균	73.1	73.4	73.7	73.4	46.7	11.48	11.82	11.84	11.88	11.88	11.93	11.94	11.95	11.97	11.97	11.97	11.96	11.97	11.98	11.97	11.98	12.0	11.98	12.0	11.95	11.94	11.93	11.93	11.96	12.3	19.88	
	메모리(%) 최대	78.5	79.2	79.3	78.9	77.6	12.8	12.4	12.0	12.3	12.3	12.5	13.1	12.2	12.2	13.0	12.7	12.2	12.9	12.2	12.2	13.0	12.9	12.2	12.9	13.2	12.5	12.6	12.2	13.2	13.2	15.0	28.17
demo-k8s-worker-02	CPU(%) 평균	7.55	7.96	8.23	8.14	10.3	12.9	12.1	13.6	14.5	14.7	14.4	14.0	12.9	12.0	13.4	14.1	14.6	14.4	13.9	12.9	12.0	13.4	14.2	14.7	14.3	13.9	13.1	12.2	13.4	14.2	9.47	
	CPU(%) 최대	37.6	63.4	70.3	65.3	70.6	64.6	79.0	51.1	83.2	84.4	79.8	81.7	77.3	73.4	57.6	80.0	84.4	54.8	50.4	56.5	71.5	81.5	60.4	84.8	78.7	43.2	59.2	71.8	79.0	83.0	60.73	
	디스크(%) 평균	51.9	52.3	52.8	53.4	54.0	54.9	55.4	55.6	56.3	56.9	57.3	58.0	57.8	57.5	57.4	57.3	57.5	57.5	57.5	57.8	57.6	57.3	57.6	57.3	57.8	58.2	58.0	57.9	58.0	58.5	63.72	
	디스크(%) 최대	52.1	52.5	53.1	53.8	54.3	55.5	57.4	55.9	56.9	57.2	57.6	58.3	58.3	58.2	57.7	57.8	58.1	58.1	58.1	58.1	57.9	57.6	57.9	57.6	57.9	60.0	58.1	58.5	58.3	58.5	64.4	64.96
	메모리(%) 평균	39.7	39.8	40.1	40.11	45.2	52.11	52.1	53.1	53.4	53.7	53.4	53.3	53.0	52.8	53.1	53.4	53.6	53.3	53.0	52.9	52.6	53.1	53.3	53.8	54.1	53.7	53.5	53.3	53.7	53.8	44.25	
	메모리(%) 최대	41.7	43.0	42.3	42.8	60.6	54.6	57.4	56.1	58.1	58.5	56.8	56.4	56.2	55.2	56.0	57.7	57.3	56.1	55.8	55.3	55.3	57.1	56.1	60.8	57.5	56.5	56.0	56.6	57.0	57.4	56.99	

서버별 CPU 평균, 최댓값과 메모리 평균, 최댓값을 일자별로 한눈에 확인할 수 있습니다.

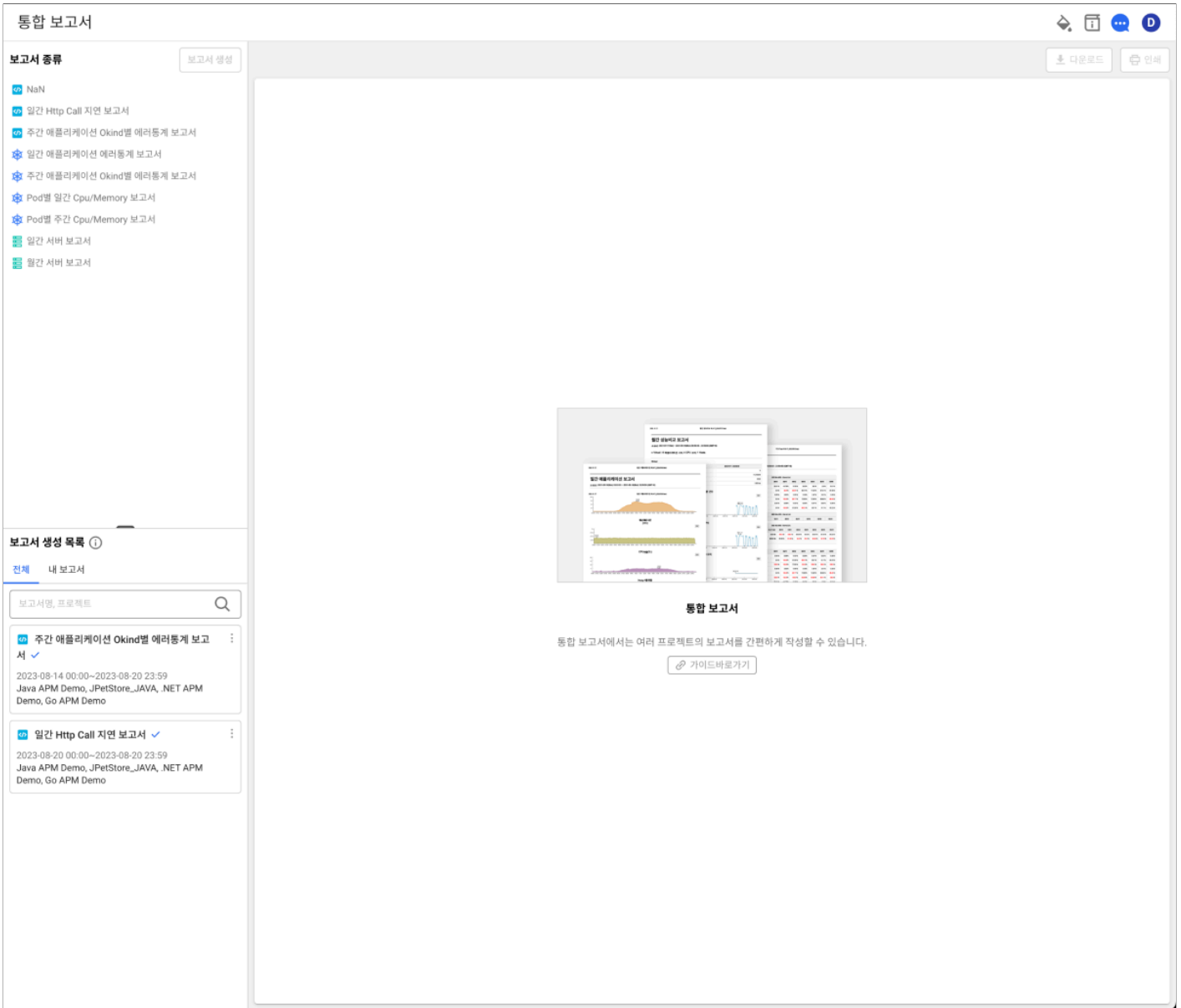
ⓘ 수치가 90% 이상인 경우 **빨간색**으로 표시됩니다.

통합 보고서

홈 화면 > [통합 보고서](#)

와탭 모니터링 서비스 초기 화면에서 프로젝트를 선택하지 않고 기본 [메뉴](#) 하위에 [통합 보고서](#)를 선택하세요. [통합 보고서](#)는 여러 프로젝트에 대한 보고서를 간편하게 생성할 수 있습니다.

보고서 종류와 원하는 프로젝트를 선택하여 보고서를 생성할 수 있고, 보고서 생성 목록에서 작업 진행 상태를 확인할 수 있습니다. 보고서 생성 중 특정 프로젝트에서 에러가 발생한 경우 에러 내용을 확인할 수 있습니다. 작업이 완료된 보고서를 바로 조회하거나, 다운로드 및 인쇄 기능을 통해 다른 사람에게 보고서를 공유할 수 있습니다.



통합 보고서의 기능은 다음과 같습니다.

- 멀티 프로젝트 지원

통합 보고서 메뉴에서 여러 프로젝트를 선택해 한 번에 보고서를 생성할 수 있어 편리합니다. 기존 보고서 메뉴는 프로젝트마다 보고서를 생성해야 했습니다.

- 업무 단위 보고서 생성

보고서 생성 메뉴에서 업무 단위로 프로젝트를 선택해 템플릿으로 저장할 수 있습니다. 보통 업무 단위로 프로젝트를 나누어 사용하는 마이크로 서비스 아키텍처(MSA, Micro Service Architecture) 환경에서 유용한 기능입니다.

- **대용량 데이터 최적화**

통합 보고서 메뉴는 보고서 생성 시간이 획기적으로 줄어들었습니다. 그리고 일부 프로젝트 보고서 작성 과정에서 오류가 발생하더라도 보고서 결과를 조회할 수 있습니다.

- **보고서 생성 중 동시 작업 가능**

통합 보고서 메뉴에서 보고서를 생성하는 동시에 다른 업무를 보는 것이 가능합니다. 기존 **보고서** 메뉴는 생성 작업이 완료될 때까지 기다려야만 했습니다.

통합 보고서 메뉴에서 보고서 생성을 시작한 후 다른 페이지로 이동할 수 있습니다. 또한 보고서 결과 목록에서 진행 상태와 완료된 보고서를 조회할 수 있습니다.

- **보고서 작업 공유**

동일 프로젝트 권한을 가진 사용자라면 누구든 생성한 보고서를 조회할 수 있습니다. 관련 보고서가 이미 생성됐는지 확인할 수 있어 중복으로 작성하지 않을 수 있습니다.

보고서와 통합 보고서의 차이

보고서는 하나의 프로젝트에 대한 보고서를 생성하는 메뉴입니다. 따라서 프로젝트를 선택 후 좌측의 **통계/보고서** 메뉴를 통해 접근이 가능합니다.

통합 보고서는 여러 프로젝트에 대한 보고서를 생성하는 메뉴입니다. 프로젝트를 선택하지 않고 기본 메뉴에서 접근이 가능합니다. **보고서**의 상세 내용은 [다음 문서](#)에서 확인할 수 있습니다.

보고서 생성 방법

1. 보고서 종류 선택

보고서 종류

보고서 생성

 **일간 Http Call 지연 보고서**

 주간 애플리케이션 Okind별 에러통계 보고서

 일간 애플리케이션 에러통계 보고서

 주간 애플리케이션 Okind별 에러통계 보고서




 Pod별 일간 Cpu/Memory 보고서

 Pod별 주간 Cpu/Memory 보고서

 일간 서버 보고서

 월간 서버 보고서

보고서 종류 메뉴에서 원하는 보고서 유형을 선택하면 **보고서 생성** 버튼이 활성화됩니다. 보고서 이름 앞의 **아이콘**은 보고서의 양식이 지원하는 프로젝트 플랫폼을 의미합니다.

-  애플리케이션 프로젝트 플랫폼을 나타냅니다.
-  쿠버네티스 프로젝트 플랫폼을 나타냅니다.
-  서버 프로젝트 플랫폼을 나타냅니다.

2. 상세 설정

✕
보고서 생성

타입

⌵
일간 Http Call 지연 보고서
⌵

제목

일간 Http Call 지연 보고서

시간

⏪
2023/08/22 00:00 ~ 2023/08/22 23:59
1일
⏩

프로젝트

검색
🔍

▼ 프로젝트
전체 선택

⌵
[30092] .NET APM Demo

⌵
[31130] Go APM Demo

⌵
[5490] Java APM Demo

⌵
[6969] Node.js APM Demo

⌵
[31324] PHP APM Demo

⌵
[29744] Python APM Demo

보고서 양식 저장

보고서 생성

보고서 종류 선택 후 [보고서 생성](#) 버튼을 클릭하세요. 다음과 같이 상세 설정을 할 수 있습니다.

- **보고서 제목**

같은 타입의 보고서가 여러 개인 경우 이름을 지정하면 보고서 결과를 구분하기 쉽습니다.

- **시간**

보고서에 사용될 데이터의 기간을 선택하세요. 기간은 보고서 타입(일, 주, 월)에 따라 달라집니다.

- 프로젝트 선택

보고서를 작성할 프로젝트를 선택하세요. 그룹 및 개별 프로젝트 단위로 선택이 가능합니다.

- 보고서 양식 저장과 불러오기

지금 입력된 보고서의 설정을 템플릿으로 저장하고 다음 생성 시 타입 목록에서 불러올 수 있습니다. 업무 단위로 프로젝트를 자주 사용하시는 분들에게 유용한 기능입니다.

3. 보고서 생성

설정을 완료했다면 [보고서 생성](#) 버튼을 눌러 보고서를 생성하세요.

작업 목록 확인

보고서 생성 목록 (i)

[전체](#) [내 보고서](#)

🔍

<>
일간 Http Call 지연 보고서 ✓
⋮

2023-08-22 00:00~2023-08-22 23:59

Java APM Demo, .NET APM Demo, Go APM Demo

[보고서 생성 목록](#)에서 이전에 만들었던 보고서와 현재 작업 중인 보고서를 확인할 수 있습니다.

[전체](#) 목록에서는 내가 생성한 보고서 외에도 나와 같은 권한을 가진 사람이 생성한 보고서를 함께 볼 수 있습니다. [내 보고서](#) 목록에서는 내가 생성한 보고서만 필터링하여 볼 수 있습니다.

에러 없이 생성된 보고서는 ✓ **체크** 아이콘으로 표시되며, 에러가 포함된 경우는 △ **경고** 아이콘이 함께 표시됩니다. △ **경고** 아이콘을 클릭하시면 어떤 프로젝트에서 에러가 발생했는지 확인할 수 있습니다.

조회 및 공유

↓ 다운로드
☰ 인쇄

일간 Http Call 지연 보고서

조회조건 :2023-08-22(Tue) 00:00:00 ~ 2023-08-22(Tue) 23:59:59 (GMT+9)

[5490] Java APM Demo

일간 Http Call 지연 보고서

조회조건 2023-08-22(Tue) 00:00:00 ~ 2023-08-22(Tue) 23:59:59 (GMT+9)

Http Call 지연 Top 5 (1초 이상)

번호	URL	호출 URL	호스트	포트	전체	에러	평균 시간(ms)	합계 시간(ms)	최대 시
1	/remote/account/save/dept/kwangj u	/account/load/dept/daejun	127.0.0.1	8105	2264	0	1247	2823259	

보고서는 3가지 방식으로 제공됩니다.

- **화면 조회**

작업 목록에서 생성한 보고서를 선택하면 화면에서 바로 조회하여 볼 수 있습니다.

- **다운로드**

[다운로드](#) 버튼을 클릭하면 바로 보기의 보고서와 같은 파일이 html 형식으로 다운로드 됩니다. 모니터링 관리 권한이 없는 사람에게 보고서를 공유할 수 있습니다.

- **인쇄 및 PDF 저장**

[인쇄](#) 버튼을 누르면 컴퓨터에 연결된 프린터로 인쇄하거나 또는 PDF 형식으로 저장할 수 있습니다.

알림 설정하기

이벤트 조건을 설정하고 이메일, SMS, 메신저, App Push 등 다양한 경로로 알림을 수신할 수 있습니다.

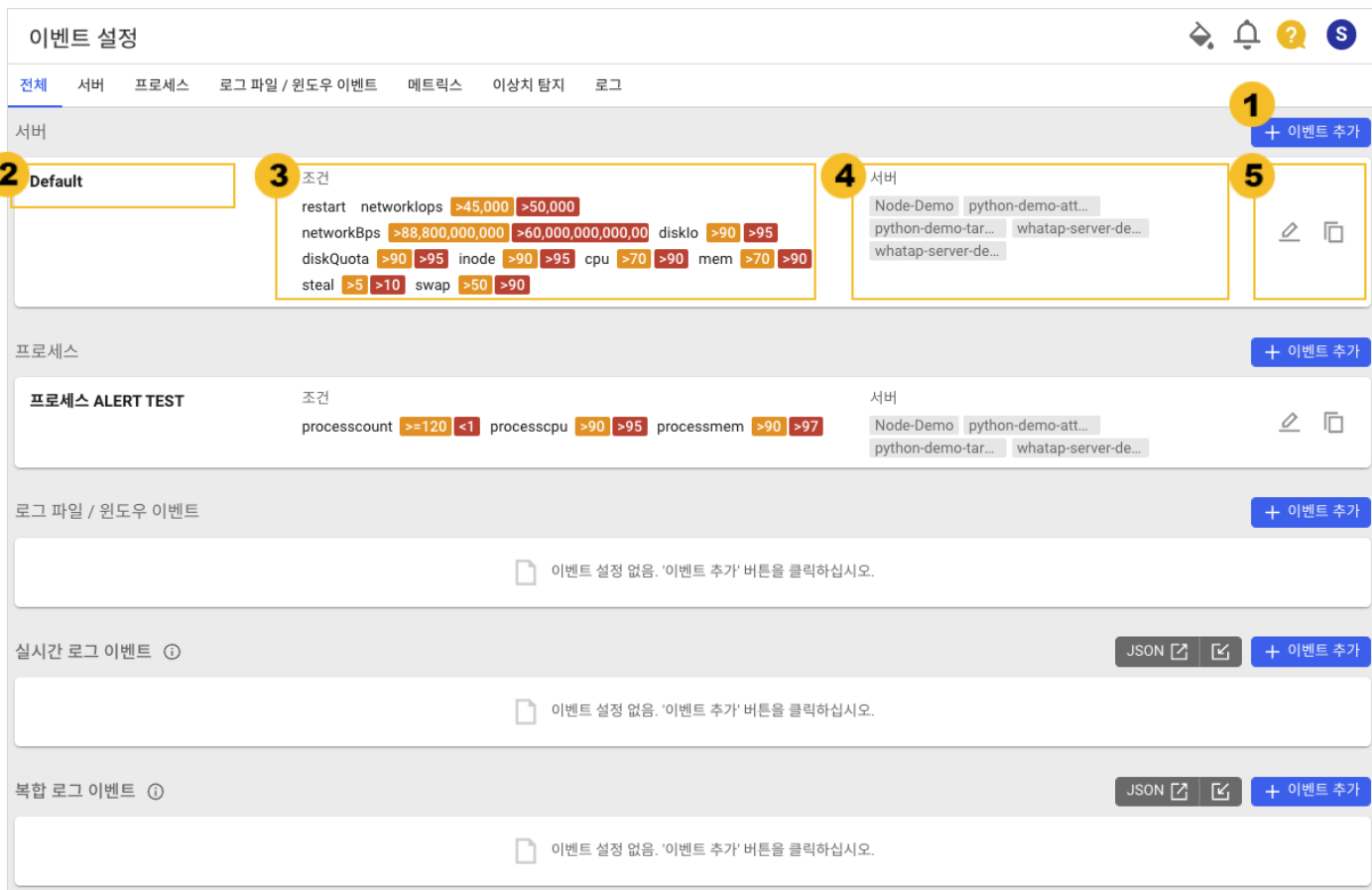
- 에이전트와 수집 서버의 통신 두절 및 자원 사용률, 액티브 트랜잭션, 에러, 응답 지연, 응답 분포 이상에 대한 알림 설정이 가능합니다.
- 어려운 조건의 알림 설정은 태그 카운트 알림 기능을 통해 제공합니다.
- 머신 러닝 기반 AI 알림 설정을 통해 히트맵 패턴을 감지해 알림 기능을 제공합니다. AI 모듈이 애플리케이션 실행 분포 패턴을 판단해 알림을 보냅니다. 복잡한 조건 없이 이슈 상황을 빠르고 정확하게 인지할 수 있습니다.
- [이벤트 설정](#) 메뉴를 통해 임계치 기반 알림 조건 및 수신 설정을 할 수 있습니다.
- [이벤트 수신 설정](#) 메뉴에서는 개인별 알림 수신 채널 및 시간대를 설정할 수 있습니다.
- [이벤트 기록](#) 메뉴에서는 알림 발생 기록을 조회할 수 있습니다.

- ① • 다른 계정에 대한 알림을 설정하려면 [수정](#), [알림 설정](#), [멤버 관리](#) 권한 중 하나가 있어야 합니다.
 - 이벤트를 추가하거나 설정하려면 알림 설정 권한이 있어야 합니다. 권한 체계에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.
 - 경고 알림과 관련해 모니터링 플랫폼별 지원되는 이벤트 종류를 확인하려면 [다음 문서](#)를 참조하세요.

서버 경고 알림

홈 화면 > 프로젝트 선택 > 경고 알림 > 이벤트 설정

서버, 프로세스, 로그 파일 및 윈도우 이벤트 등의 이벤트 정책을 생성, 수정, 삭제할 수 있습니다. 이벤트 타입을 선택해 서버 재시작 여부, 에이전트의 통신 장애 지속 시간, 자원 사용량 등에 따라 이벤트를 설정할 수 있습니다.





- **1 + 이벤트 추가**
해당 이벤트를 추가할 수 있습니다.
- **2 이름**
해당 이벤트의 이름을 표시합니다
- **3 조건**

해당 이벤트의 조건을 표시합니다.

- **4 서버**

해당 이벤트가 설정된 서버를 표시합니다.

- **5 수정과 복사**

-  버튼을 선택해 저장된 이벤트 설정을 **수정**할 수 있습니다.
-  버튼을 선택해 다른 인프라에 해당 이벤트를 **복사**할 수 있습니다.

- ⓘ • **메트릭스** 이벤트 추가는 [다음 문서](#)를 참조하세요.
- **이상치 탐지** 이벤트 추가는 [다음 문서](#)를 참조하세요.
- **로그** 이벤트 추가는 [다음 문서](#)를 참조하세요.

서버 이벤트 추가

홈 화면 > 프로젝트 선택 > 경고 알림 > 이벤트 설정 > 서버 탭 > + 이벤트 추가 버튼 선택

특정 서버에 대한 전반적인 이벤트를 설정할 수 있습니다.

✕ 이벤트 추가

1

제목 *

이벤트 타입 선택

서버
 프로세스
 로그

3

이벤트 발행 조건

지표	조건	레벨	지속 시간	활성화
재시작	-	위험	-	<input checked="" type="checkbox"/>
미수신	-	경고	10 분	<input type="checkbox"/>
포트	-	경고	1 분	<input type="checkbox"/>
네트워크 IOPS	경고 > <input type="text" value="45,000 pps"/> 위험 > <input type="text" value="50,000 pps"/>	경고	5 분	<input checked="" type="checkbox"/>
		위험	5 분	<input checked="" type="checkbox"/>
네트워크 BPS	경고 > <input type="text" value="150,000,000 bps"/> 위험 > <input type="text" value="200,000,000 bps"/>	경고	5 분	<input checked="" type="checkbox"/>
		위험	5 분	<input checked="" type="checkbox"/>
디스크 I/O	<input type="text" value="90%"/> <input type="text" value="95%"/>	경고	5 분	<input checked="" type="checkbox"/>
		위험	5 분	<input checked="" type="checkbox"/>
디스크 사용량	<input type="text" value="90%"/> <input type="text" value="95%"/>	경고	5 분	<input checked="" type="checkbox"/>
		위험	5 분	<input checked="" type="checkbox"/>

2

서버 목록

- 전체 선택
- demo-k8s-master (10.21.1.149)
- demo-k8s-worker-01 (10.21.1.229)
- demo-k8s-worker-02 (10.21.1.157)
- demo-k8s-worker-03 (10.21.1.23)
- demo-k8s-worker-04 (10.21.1.210)
- dotnet-official-demo (10.21.1.51)
- go-official-demo (10.21.1.118)
- mysql-official-demo-01 (10.21.1.86)
- mysql-official-demo-02 (10.21.1.136)
- mysql-official-demo-02 (10.21.1.136)
- mysql-official-demo-03 (10.21.1.236)
- node-official-demo (10.21.1.98)
- python-demo-attack (10.21.1.254)
- python-demo-target (10.21.1.43)
- rum-official-demo (10.21.1.151)
- url-official-demo (10.21.1.181)

4

이벤트 수신 태그

전체 멤버 수신

이벤트 타입이 서버, 프로세스일 경우 이벤트 수신 태그를 사용할 수 있습니다.
이벤트 설정 시 이벤트 수신 태그를 선택하여 해당 태그를 가진 프로젝트 멤버와 3rd-party 플러그인에 알림을 전송할 수 있습니다.
이벤트 수신 설정 메뉴에서 프로젝트 멤버와 3rd-party 플러그인에 각각 태그를 지정할 수 있습니다

[프로젝트 이벤트 수신설정 메뉴](#)

이벤트 설정 시 태그를 선택하지 않은 경우 프로젝트 이벤트 수신 설정 메뉴의 나머지 수신 조건(활성화 여부 등)에 따라 알림이 발생합니다.

5
저장

1. 이벤트 추가 창이 뜨면 ① 이벤트 제목을 입력하세요.
2. ② 서버 목록을 확인하거나 검색창을 통해 모니터링을 원하는 서버를 선택하세요.
3. ③ 이벤트 발행 조건 탭에서 원하는 지표의 조건, 레벨, 지속 시간, 활성화 여부를 설정하세요.

- **레벨**: 경고 혹은 위험 수준을 선택할 수 있습니다.
- **지속 시간**: 설정한 **지속 시간** 이후 서버의 상태가 **경고**, **위험** 수준으로 변경됩니다.

지표 안내는 다음을 참고하세요.

- **재시작**: 서버 재시작 시 발생하는 이벤트입니다.
- **미수신**: 에이전트로부터 **지속 시간**동안 정상적인 데이터를 수신하지 못했을 경우 발생하는 통신 장애 이벤트입니다.
- **포트**: 포트 접속 불가 이벤트입니다. 프로젝트 내 등록된 에이전트는 **10120 포트**를 통해 서로의 상태를 확인합니다. **지속 시간**동안 통신이 이루어지지 않을 경우 발생하는 이벤트입니다.
- **CPU, Memory, 스왑**: CPU, Memory, SWAP 메모리 등의 사용량에 대한 이벤트를 설정합니다.
- **Steal**: CPU Steal Time에 대한 이벤트를 설정합니다. 리눅스 계열 OS만 설정할 수 있습니다.
- **Disk**: 디스크 사용량과 I/O 사용량 및 Inode 사용량을 기반으로 이벤트를 설정합니다.
- **Network**: 네트워크 사용량과 관련한 이벤트를 설정합니다. 트래픽 양과 초당 패킷을 기준으로 설정할 수 있습니다.

4. **4** **이벤트 수신 태그**를 설정하세요.

- 이벤트 수신 태그를 선택하면 해당 태그를 가진 프로젝트 멤버와 3rd-party 플러그인에 알림을 전송할 수 있습니다. 이벤트 수신 태그를 선택하지 않으면 프로젝트 전체 멤버에게 경고 알림을 보냅니다.
- **+ 태그 추가**를 클릭한 다음 **태그 목록**에서 경고 알림 수신 대상을 선택하세요. **+ 새 태그 생성**을 선택해 태그를 추가할 수도 있습니다.
- **경고 알림 > 이벤트 수신 설정** 메뉴에서 프로젝트 멤버와 3rd-party 플러그인에 태그를 설정할 수 있습니다. **이벤트 수신 설정** 메뉴에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

5. 이벤트 설정을 마쳤으면 **5** **저장** 버튼을 선택하세요.

! 하나의 서버에 하나의 이벤트를 할당할 수 있습니다.

> 서버 이벤트 기본 설정

와탭 서버 모니터링 서비스는 에이전트 설치와 동시에 다음과 같은 기본 이벤트 설정을 제공합니다.

Default	조건
restart	networklops >45,000 >50,000 networkBps >500,000,000 >700,000,000
disklo >90 >95	diskQuota >90 >95 inode >90 >95 cpu >70 >90
mem >70 >90	steal >5 >10 swap >50 >90

- 재시작: 활성화
- 네트워크 IOPS
 - 경고: 45,000 pps / 지속 시간: 5분
 - 위험: 50,000 pps / 지속 시간: 5분
- 네트워크 BPS
 - 경고: 5000,000,000 bps / 지속 시간: 5분
 - 위험: 7000,000,000 bps / 지속 시간: 5분
- 디스크 I/O
 - 경고: 90% / 지속 시간: 5분
 - 위험: 95% / 지속 시간: 5분
- 디스크 사용량
 - 경고: 90% / 지속 시간: 5분
 - 위험: 95% / 지속 시간: 5분
- inode
 - 경고: 90% / 지속 시간: 5분
 - 위험: 95% / 지속 시간: 5분
- CPU
 - 경고: 70% / 지속 시간: 1분
 - 위험: 90% / 지속 시간: 1분
- 메모리
 - 경고: 70% / 지속 시간: 1분
 - 위험: 90% / 지속 시간: 1분
- steal
 - 경고: 5% / 지속 시간: 1분
 - 위험: 10% / 지속 시간: 1분
- 스왑
 - 경고: 50% / 지속 시간: 1분
 - 위험: 90% / 지속 시간: 1분

프로세스 이벤트 추가

홈 화면 > 프로젝트 선택 > 경고 알림 > 이벤트 설정 > 프로세스 탭 > + 이벤트 추가 버튼 선택

특정 프로세스에 대한 이벤트 정책을 설정할 수 있습니다.

✕ 이벤트 추가

1

제목 *

▼ 이벤트 타입 선택

서버 프로세스 로그

2

▼ 이벤트 발행 조건

서버 목록

프로세스

프로세스 소유자

생략하면 소유자와 관계없이 같은 이름의 모든 프로세스에 설정이 적용됩니다. 단 이벤트 조건은 소유자를 생략한 경우라도 소유자-프로세스 단위로 동작합니다.

지표	조건	레벨	지속 시간	활성화
프로세스 수 <input type="text" value="1"/>	위험 < 1 경고 >= 2	경고	1 분	<input checked="" type="checkbox"/>
		위험	1 분	<input checked="" type="checkbox"/>
프로세스 CPU <input type="text" value="90%"/>	<div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px 5px; margin-right: 5px;">90%</div> <div style="flex-grow: 1; border: 1px solid #ccc; position: relative;"> <div style="background-color: #ccc; width: 100%; height: 10px;"></div> <div style="background-color: orange; width: 80%; height: 10px; position: absolute; left: 0;"></div> <div style="background-color: red; width: 20%; height: 10px; position: absolute; left: 80%;"></div> </div> <div style="border: 1px solid #ccc; padding: 2px 5px; margin-left: 5px;">95%</div> </div>	경고	1 분	<input checked="" type="checkbox"/>
		위험	1 분	<input checked="" type="checkbox"/>
프로세스 메모리 <input type="text" value="90%"/>	<div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px 5px; margin-right: 5px;">90%</div> <div style="flex-grow: 1; border: 1px solid #ccc; position: relative;"> <div style="background-color: #ccc; width: 100%; height: 10px;"></div> <div style="background-color: orange; width: 80%; height: 10px; position: absolute; left: 0;"></div> <div style="background-color: red; width: 20%; height: 10px; position: absolute; left: 80%;"></div> </div> <div style="border: 1px solid #ccc; padding: 2px 5px; margin-left: 5px;">95%</div> </div>	경고	1 분	<input checked="" type="checkbox"/>
		위험	1 분	<input checked="" type="checkbox"/>

3

▼ 이벤트 수신 태그


전체 멤버 수신

이벤트 타입이 서버, 프로세스일 경우 이벤트 수신 태그를 사용할 수 있습니다.
이벤트 설정 시 이벤트 수신 태그를 선택하여 해당 태그를 가진 프로젝트 멤버와 3rd-party 플러그인에 알림을 전송할 수 있습니다.
이벤트 수신 설정 메뉴에서 프로젝트 멤버와 3rd-party 플러그인에 각각 태그를 지정할 수 있습니다

이벤트 설정 시 태그를 선택하지 않은 경우 프로젝트 이벤트 수신 설정 메뉴의 나머지 수신 조건(활성화 여부 등)에 따라 알림이 발생합니다.

4

1. 이벤트 추가 창이 뜨면 1 이벤트 제목을 입력하세요.
2. 2 이벤트 발행 조건 탭에서 서버 목록의 선택된 에이전트가 없습니다 버튼을 클릭해 서버 목록 창에서 서버를 선택하세요.

❗ 프로젝트 기본 정책 옵션 토글  활성화 시 프로젝트가 관리하는 서버에 기본 알림 정책을 적용합니다.

3. 프로세스 선택창에서 프로세스 혹은 프로세스 그룹을 선택하세요.

❗ 프로세스 그룹 추가 방법에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

4. 프로세스 소유자를 선택하세요.

- 프로세스 소유자를 지정하지 않을 시 소유자와 관계없이 같은 이름의 모든 프로세스에 해당 설정이 적용됩니다.
- 이벤트 조건은 프로세스 소유자를 생략한 경우라도 소유자-프로세스 단위로 동작합니다.

5. 원하는 지표의 레벨, 지속 시간, 활성화 여부를 설정하세요.

- 레벨: 경고 혹은 위험 수준을 선택할 수 있습니다.
- 지속 시간: 설정한 임계값의 지속 시간 이후 서버의 상태가 경고, 위험 수준으로 변경됩니다.

지표 안내는 다음을 참고하세요.

- 프로세스 수: 동일한 이름의 프로세스의 개수에 대한 이벤트를 설정할 수 있습니다. 위험과 경고 조건의 개수를 지정하세요.
- 프로세스 CPU: CPU 사용량에 따라 이벤트를 설정할 수 있습니다.
- 프로세스 메모리: 메모리 사용량에 따라 이벤트를 설정할 수 있습니다.

6. 3 이벤트 수신 태그를 설정하세요.

- 이벤트 수신 태그를 선택하면 해당 태그를 가진 프로젝트 멤버와 3rd-party 플러그인에 알림을 전송할 수 있습니다. 이벤트 수신 태그를 선택하지 않으면 프로젝트 전체 멤버에게 경고 알림을 보냅니다.
- + 태그 추가를 클릭한 다음 태그 목록에서 경고 알림 수신 대상을 선택하세요. + 새 태그 생성을 선택해 태그를 추가할 수도 있습니다.
- 경고 알림 > 이벤트 수신 설정 메뉴에서 프로젝트 멤버와 3rd-party 플러그인에 태그를 설정할 수 있습니다. 이벤트 수신 설정 메뉴에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

7. 이벤트 설정을 마쳤으면 4 저장 버튼을 선택하세요.

- ❗
- 프로세스 알림 조건을 잘못 설정한 경우 해당 알림을 비활성화하거나 알림 조건을 재설정하세요.
 - 프로세스 및 프로세스 소유자를 잘못 지정한 경우 해당 알림을 비활성화해 진행 중인 알림을 해소한 후 알림 조건을 재설정하세요.

로그 파일 및 윈도우 이벤트 추가

홈 화면 > 프로젝트 선택 > 경고 알림 > 이벤트 설정 > 로그 파일/윈도우 이벤트 탭 > + 이벤트 추가 버튼 선택

특정 로그 파일과 윈도우 이벤트 설정을 관리할 수 있습니다.

로그 파일

[로그 파일](#) 이벤트를 추가하려면 다음을 참고해 [이벤트 발생 조건](#)을 지정하세요.

X 이벤트 추가

1 제목 *

이벤트 타입 선택

- 서버
- 프로세스
- 로그

3 이벤트 발행 조건

로그 종류 로그 파일 ⓘ 윈도우 이벤트 ⓘ

파일 경로

* 파일 이름에는 날짜/시간이 들어갈 수 있습니다.(참조 http://strftime.org/)
Ex.)/var/log/mylogfile_%Y-%m-%d_%H:%M:%S.log

검색 키워드

* 검색 키워드는 복수개로 입력할 수 있습니다. Ex) keyword1|keyword2|keyword3 윈도우 이벤트뷰어 키워드 항목에는 적용되지 않습니다.

검출 제외 문자열

* Agent 버전 1.2.7 이상 지원됩니다.
검출 제외 문자열은 복수개로 입력할 수 있습니다. Ex) keyword1|keyword2|keyword3

반복 (회)

기간 (초)

위험도 위험 경고

조건에 충족되면 경고를 받을 수 있습니다.

— 삭제

+ 로그 이벤트 조건 추가

? 자동등록 스크립트 사용법

2

서버 목록 ⓘ

프로젝트 기본 정책으로 ⓘ

- 전체 선택
- dev-agency (10.21.1.59)
- dev-front (10.21.1.99)
- dev-yard (10.21.1.55)
- ip-10-20-3-83 (10.20.3.83)
- ip-10-20-3-144 (10.20.3.144)
- ip-10-20-3-212 (10.20.3.212)
- ip-10-20-60-5 (10.20.60.5)
- ip-10-20-60-11 (10.20.60.11)
- ip-10-20-60-13 (10.20.60.13)
- ip-10-20-60-14 (10.20.60.14)
- ip-10-20-60-16 (10.20.60.16)
- ip-10-20-60-17 (10.20.60.17)
- ip-10-20-60-19 (10.20.60.19)
- ip-10-20-60-23 (10.20.60.23)
- ip-10-20-60-24 (10.20.60.24)
- ip-10-20-60-36 (10.20.60.36)
- ip-10-20-60-39 (10.20.60.39)
- ip-10-20-60-73 (10.20.60.73)
- ip-10-20-60-80 (10.20.60.80)
- ip-10-20-60-87 (10.20.60.87)
- ip-10-20-60-95 (10.20.60.95)

4 저장

1. 이벤트 추가 창이 뜨면 ① 이벤트 제목을 입력하세요.
2. ② 서버 목록을 확인하거나 검색창을 통해 모니터링을 원하는 서버를 선택하세요.

❗ 프로젝트 기본 정책 옵션 토글 활성화 시 프로젝트가 관리하는 서버에 기본 알림 정책을 적용합니다.

3. ③ 이벤트 발행 조건 탭에서 로그 종류를 로그 파일로 선택하세요.
4. 예시를 참고해 파일 경로를 정규식대로 입력하세요.
예시, `/var/log/mylogfile%Y-%m-%d%H:%M:%S.log`
5. 이벤트를 발생시킬 검색 키워드를 입력하세요. 복수 개 지정할 수 있습니다.
6. 알림에서 제외할 검출 제외 문자열을 입력하세요. 복수 개 지정할 수 있습니다.
7. 몇 초 동안 몇 회 지정한 키워드 검출 시 알림을 받을 지 반복 횟수와 기간을 입력하세요.
8. 이벤트의 위험도를 선택하세요. 위험 혹은 경고 수준을 선택할 수 있습니다.
9. ④ 저장 버튼을 선택하세요.

윈도우 이벤트

윈도우 이벤트를 추가하려면 다음을 참고해 이벤트 발행 조건을 지정하세요. Windows 환경에서만 사용 가능합니다.

X 이벤트 추가

1 제목 *

이벤트 타입 선택

서버 프로세스 로그

3 이벤트 발행 조건

로그 종류 로그 파일 ⓘ 윈도우 이벤트 ⓘ

로그명

수준

원본

이벤트 ID

* 숫자만 입력 가능합니다.

검색 키워드

* 검색 키워드는 복수개로 입력할 수 있습니다. Ex) keyword1|keyword2|keyword3 윈도우 이벤트뷰어 키워드 항목에는 적용되지 않습니다.

검출 제외 문자열

* Agent 버전 1.2.7 이상 지원됩니다.
검출 제외 문자열은 복수개로 입력할 수 있습니다. Ex) keyword1|keyword2|keyword3

위험도 위험 경고

조건에 충족되면 경고를 받을 수 있습니다.

2 서버 목록 ⓘ

프로젝트 기본 정책으로 ⓘ

전체 선택

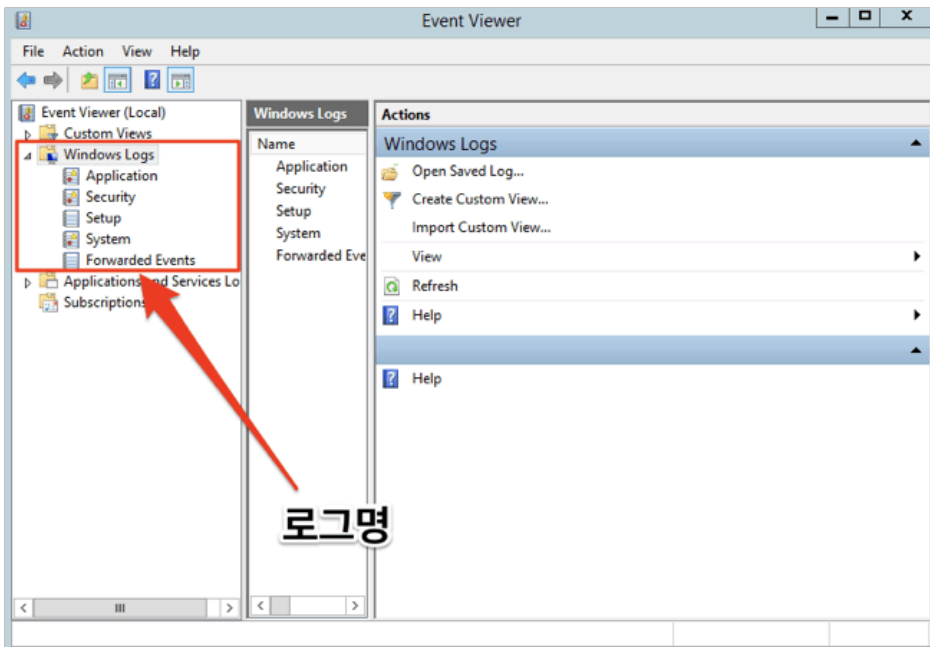
- dev-agency (10.21.1.59)
- dev-front (10.21.1.99)
- dev-yard (10.21.1.55)
- ip-10-20-3-83 (10.20.3.83)
- ip-10-20-3-144 (10.20.3.144)
- ip-10-20-3-212 (10.20.3.212)
- ip-10-20-60-5 (10.20.60.5)
- ip-10-20-60-11 (10.20.60.11)
- ip-10-20-60-13 (10.20.60.13)
- ip-10-20-60-14 (10.20.60.14)
- ip-10-20-60-16 (10.20.60.16)
- ip-10-20-60-17 (10.20.60.17)
- ip-10-20-60-19 (10.20.60.19)
- ip-10-20-60-23 (10.20.60.23)
- ip-10-20-60-24 (10.20.60.24)
- ip-10-20-60-36 (10.20.60.36)
- ip-10-20-60-39 (10.20.60.39)
- ip-10-20-60-73 (10.20.60.73)
- ip-10-20-60-80 (10.20.60.80)
- ip-10-20-60-87 (10.20.60.87)
- ip-10-20-60-95 (10.20.60.95)

4

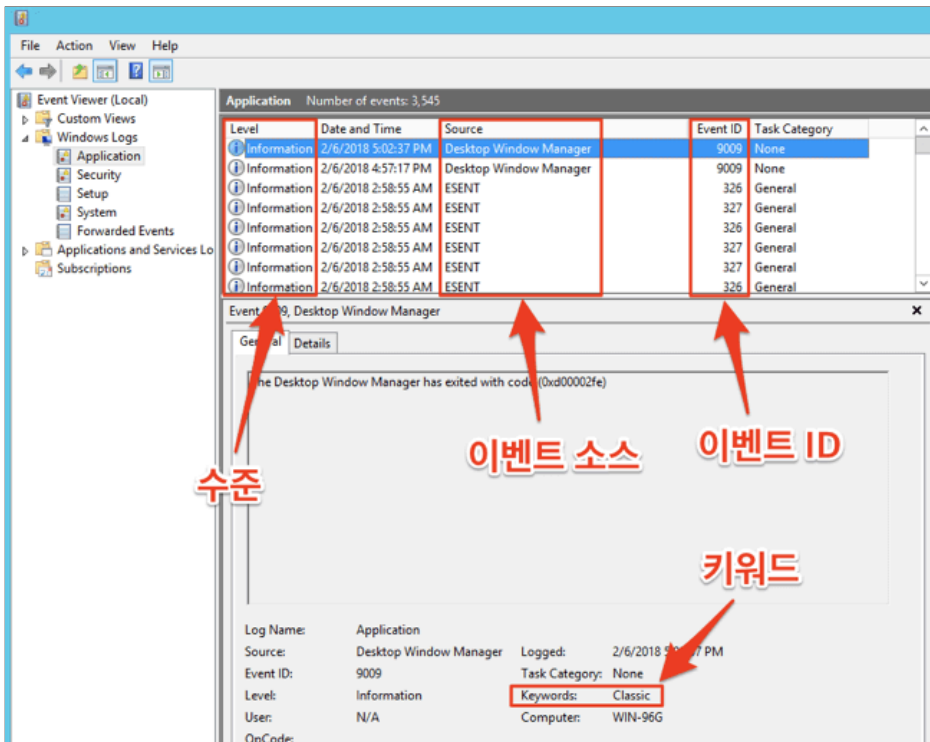
1. 이벤트 추가 창이 뜨면 ❶ 이벤트 제목을 입력하세요.
2. ❷ 서버 목록을 확인하거나 검색창을 통해 모니터링을 원하는 서버를 선택하세요.

❸ 프로젝트 기본 정책 옵션 토글 활성화 시 프로젝트가 관리하는 서버에 기본 알림 정책을 적용합니다.

3. ❸ 이벤트 발행 조건 탭에서 로그 종류를 윈도우 이벤트로 선택하세요.
4. 다음 예시를 참고해 로그명을 선택하세요.



5. 다음 예시를 참고해 수준, 원본(이벤트 소스), 이벤트 ID, 검색 키워드를 지정하세요. 검색 키워드는 복수 개 지정할 수 있습니다.



6. 알림에서 제외할 **검출 제외 문자열**을 입력하세요. 복수 개 지정할 수 있습니다.
7. 이벤트의 **위험도**를 선택하세요. **위험** 혹은 **경고** 수준을 선택할 수 있습니다.
8. **4 저장** 버튼을 선택하세요.

로그 파일 처리량

로그 파일 처리량은 로그 라인 기준으로 다음과 같이 설정되어 있습니다. 로그 과다 발생 시 와탭 서버 모니터링 에이전트 CPU 과다 사용 방지를 위해서입니다. 초과량은 처리하지 않습니다.

- 버전 1.3.6 이하 : 약 2초당 60 라인을 처리합니다.
- 버전 1.3.7 이상 : 약 2초당 1000 라인을 처리합니다.

다음 옵션으로 2초당 초과량을 조절할 수 있습니다.


• Linux

`/usr/whatap/infra/conf/whatap.conf` 파일에 `log.skip.threshold=2초당 처리 가능 라인 수`

• Windows


`C:\Program Files\WhatapInfra\whatap.conf` 파일에 `log.skip.threshold=2초당 처리 가능 라인 수`

이벤트 수정


1. 이벤트 목록 오른쪽의  수정 아이콘을 선택하세요.
2. 이벤트 발행 조건 탭에서 원하는 지표의 조건, 레벨, 지속 시간, 활성화 여부를 수정하세요.
3. 이벤트 수정을 마쳤으면 저장 버튼을 선택하세요.

- ⓘ • 이벤트 수정 시 특정 지표에 대한 변경 사항이 있는 경우 해당 지표에 걸려있던 진행 중 알림은 Disabled 됩니다.
 - 수정 후 조건에 맞는 데이터가 유입되면 새로운 알림이 발생합니다.
 - 프로세스 알림의 제목, 프로세스, 프로세스 소유자 중 하나 이상의 값을 수정하는 경우 해당 조건에 걸린 모든 알림이 Disabled 됩니다.

이벤트 삭제

1. 이벤트 목록 오른쪽의  수정 아이콘을 선택하세요.
2. 수정 화면 상단 오른쪽의  삭제 아이콘을 선택하세요.

이벤트 복사

1. 이벤트 목록 오른쪽의  복사 아이콘을 선택하세요.
2. 이벤트 설정 복사 창이 뜨면 원하는 프로젝트를 선택하거나 하단의 현재 프로젝트에 복사를 선택하세요.
3. 이벤트 설정을 복사할 프로젝트를 지정했으면 복사 버튼을 선택하세요.

- ⓘ • 동일 프로젝트 내 이벤트 중복 복사 시 복사 횟수만큼 이벤트가 생성됩니다.
 - 복사한 이벤트명은 접미사 (copy) 표기가 추가됩니다.
 - 예, 기존 이벤트명 Default → 복사 이벤트명 Default(copy)

이벤트 설정

홈 화면 > 프로젝트 선택 >  사이트맵 > 경고 알림 > 이벤트 설정 New






새로운 **이벤트 설정** 메뉴는 카테고리(Category)가 아닌 필드(Field) 중심의 사용자 경험을 강화한 메뉴입니다. 메트릭스 이벤트 설정과 같은 강력한 기능을 모두 필요치 않거나 단순한 알림 조건을 반복해서 사용하는 사용자에게 빠르게 경고 알림을 적용할 수 있는 이벤트 기능입니다. 생성한 프로젝트의 상품에 적합한 기본 이벤트 템플릿을 제공하여 빠르고 쉽게 원하는 경고 알림 이벤트를 설정할 수 있습니다.

카테고리가 아니라 필드를 먼저 선택해 사용자가 인지하는 지표와 이벤트 설정의 불일치를 해소합니다. 시뮬레이션이 주는 시각적 직관성을 결합하여 빠르고 정확하게 이벤트설정을 완료할 수 있습니다.

- ① • 신규 프로젝트는 별도의 설정없이 이 기능을 이용할 수 있으나 이미 생성된 프로젝트에서는 **이벤트 템플릿 생성** 버튼을 선택하세요. 새로운 기능에 최적화된 이벤트 목록을 자동으로 생성합니다.
- 상품에 따라 제공하는 이벤트 템플릿은 다를 수 있습니다.
- 이 기능은 알림 설정 권한이 있는 멤버만 이용할 수 있습니다. 멤버 권한에 대한 자세한 설명은 [다음 문서](#)를 참조하세요.

기본 이벤트 템플릿

생성한 프로젝트의 상품에 따라 기본 이벤트 템플릿을 제공합니다. 이벤트 목록의 가장 왼쪽에 **활성화** 버튼을 선택해 원하는 이벤트를 활성화할 수 있습니다.

활성화	수정	이벤트 이름 ↑	지표 이름	지표	대상	연속 ①	일시 중지	해결된 알림	이벤트 수신
<input type="checkbox"/>		CPU	CPU (%)	● > 70 ● > 90	전체	사용 안함	1분	사용	전체 수신
<input type="checkbox"/>		CPU Steal	CPU Steal (%)	● > 5 ● > 10	전체	사용 안함	1분	사용	전체 수신
<input type="checkbox"/>		Disk	Disk (%)	● > 90 ● > 95	전체	사용 안함	5분	사용	전체 수신
<input type="checkbox"/>		Disk I/O	Disk I/O (%)	● > 90 ● > 95	전체	사용 안함	5분	사용	전체 수신
<input type="checkbox"/>		Disk Inode	Disk Inode (%)	● > 90 ● > 95	전체	사용 안함	1분	사용	전체 수신
<input type="checkbox"/>		Memory	Memory (%)	● > 70 ● > 90	전체	사용 안함	1분	사용	전체 수신
<input type="checkbox"/>		Network BPS	Network BPS (bps)	● > 150,000,000 ● > 200,000,000	전체	사용 안함	5분	사용	전체 수신
<input type="checkbox"/>		Network IOPS	Network IOPS (pps)	● > 45,000 ● > 50,000	전체	사용 안함	5분	사용	전체 수신
<input type="checkbox"/>		Process CPU	Process CPU (%)	● > 90 ● > 95	전체	사용 안함	사용 안함	사용 안함	전체 수신
<input type="checkbox"/>		Process Count	Process Count (count)	● >= 2 ● < 1	전체	사용 안함	사용 안함	사용 안함	전체 수신
<input type="checkbox"/>		Process Memory	Process Memory (%)	● > 90 ● > 95	전체	사용 안함	사용 안함	사용 안함	전체 수신
<input type="checkbox"/>		Swap Memory	Swap Memory (%)	● > 70 ● > 90	전체	사용 안함	5분	사용	전체 수신

제공하는 이벤트 템플릿은 다음과 같습니다. [지표](#) 항목에 설정된 기본값은 사용자가 원하는 값으로 수정할 수 있습니다.

- CPU

카테고리: `server_base`

CPU 사용률(`cpu`)이 70%를 초과하면 경고(Warning) 수준의 알림을, 90%를 초과하면 위험(Critical) 수준의 알림을 보냅니다.

- CPU Steal

카테고리: `server_base`

CPU steal 사용률(`cpu_steal`)이 5를 초과하면 경고(Warning) 수준의 알림을, 10을 초과하면 위험(Critical) 수준의 알림을 보냅니다.

- Disk

카테고리: `server_disk`

파일 시스템 사용률(`usedPercent`)이 90%를 초과하면 경고(Warning) 수준의 알림을, 95%를 초과하면 위험(Critical) 수준의 알림을 보냅니다.

- Disk I/O

카테고리: `server_disk`

Disk I/O 사용률(`ioPercent`)이 90%를 초과하면 경고(Warning) 수준의 알림을, 95%를 초과하면 위험(Critical) 수준의 알림을 보냅니다.

- Disk Inode

카테고리: `server_disk`

Disk Inode 사용률(`usedInodePercent`)이 90%를 초과하면 경고(Warning) 수준의 알림을, 95%를 초과하면 위험(Critical) 수준의 알림을 보냅니다.

- Memory

카테고리: `server_base`

메모리 사용률(`memory_pused`)이 70%를 초과하면 경고(Warning) 수준의 알림을, 90%를 초과하면 위험(Critical) 수준의 알림을 보냅니다.

- Network BPS

카테고리: `server_network`

네트워크 인바운드 트래픽(`trafficIn`)과 아웃바운드 트래픽(`trafficOut`)의 합이 150,000,000byte(150MB)를 초과하면 경고(Warning) 수준의 알림을, 200,000,000byte(200MB)를 초과하면 위험(Critical) 수준의 알림을 보냅니다.

- Network IOPS

카테고리: `server_network`

네트워크 인바운드 패킷(`packetIn`)과 아웃바운드 패킷(`packetOut`)의 합이 45000byte를 초과하면 경고(Warning) 수준의 알림을, 50000byte를 초과하면 위험(Critical) 수준의 알림을 보냅니다.

- **Process CPU**

카테고리: `server_process`

CPU 전체 사용률(`cpu`)이 90%를 초과하면 경고(Warning) 수준의 알림을, 95%를 초과하면 위험(Critical) 수준의 알림을 보냅니다.

- **Process Count**

카테고리: `server_process`

프로세스의 수(`count`)가 2개 이상이면 경고(Warning) 수준의 알림을, 1개 미만이면 위험(Critical) 수준의 알림을 보냅니다.

- **Process Memory**

카테고리: `server_process`

프로세스 메모리 사용률(`memory`)이 90%를 초과하면 경고(Warning) 수준의 알림을, 95%를 초과하면 위험(Critical) 수준의 알림을 보냅니다.


- **Swap Memory**

카테고리: `server_base`

스왑 메모리 사용률(`memory_swappused`)이 70%를 초과하면 경고(Warning) 수준의 알림을, 90%를 초과하면 위험(Critical) 수준의 알림을 보냅니다.

ⓘ 기본 이벤트 템플릿에 적용된 필드에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

이벤트 수정하기

기본 이벤트 템플릿에 적용된 지표값을 수정해 경고 알림이 발생 기준을 변경할 수 있습니다. 그 외에도 다양한 옵션 설정을 통해 알림 발생 기준을 변경할 수 있습니다. 수정하려는 이벤트 항목에서  버튼을 선택하면 이벤트 수정 화면으로 이동합니다. 다음의 항목을 차례로 수정한 다음 [저장](#) 버튼을 선택하세요.

이벤트 조건 정의

이벤트 발생 조건 기준을 설정할 수 있습니다.

1 이벤트 조건 정의

< 2024/02/06 10:46 ~ 2024/02/06 11:46 60분 > 실행

①
조건 설정 후 실행 버튼을 누르면 이벤트를 시뮬레이션 할 수 있습니다.

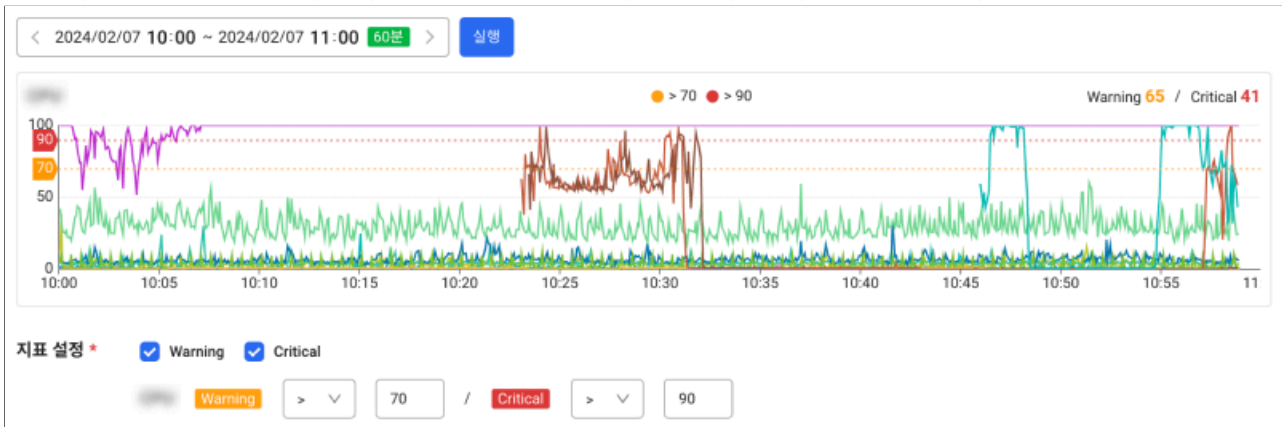
지표 설정 * Warning Critical
Warning > 70 / Critical > 90

연속 사용 안함 연속 1 회 발생 (1분에 최대 N회 발생)

일시 중지 1분
알림 수신 후 선택한 시간 동안 이벤트가 발생하지 않습니다.
단, "이벤트 상태가 해결되면 추가 알림" 기능을 활성화한 경우에는 RECOVERED 알림 수신 후 선택한 시간 동안 이벤트가 발생하지 않습니다.

해결된 알림
Critical과 Warning 레벨의 이벤트가 해결되면 RECOVERED 상태의 알림을 수신합니다.

- 실행: 이벤트 조건을 설정한 다음 버튼을 선택하면 설정한 이벤트를 시뮬레이션할 수 있습니다.



- 지표 설정: Warning 또는 Critical 알림에 대한 임계값을 설정할 수 있습니다. 연산자를 설정하고 임계값을 입력하세요.
 - 연산자 종류: > (보다 큼), >= (보다 크거나 같음), < (보다 작음), <= (보다 작거나 같음), == (같음)
 - 임계값으로 양수, 음수, 0을 입력할 수 있지만, 선택한 이벤트 템플릿에 따라 음수 입력 여부는 다를 수 있습니다.

- ⓘ 제공되는 이벤트 템플릿에 따라 설정할 수 있는 알림 수준(Level)은 다를 수 있습니다.
- Warning 또는 Critical 수준 하나만 선택할 수 있지만, 두 항목을 모두 비활성화할 수는 없습니다.

- **연속**: 설정한 이벤트 조건을 충족하는 횟수에 따라 알림을 보낼 수 있습니다.
 - **사용 안함**: 이벤트가 발생할 때마다 알림을 보냅니다.
 - **연속**: 입력한 횟수만큼 이벤트가 발생하면 알림을 보냅니다.
- **일시 중지**: 알림 수신 후 선택한 시간 동안 이벤트가 발생하지 않습니다.
- **해결된 알림**: 이벤트가 해결되면 **RECOVERED** 상태의 알림을 보냅니다.

☑ 다음 조건에 따라 알림을 보내는 기준이 달라집니다.

연속	해결된 알림	동작
사용 안함	On	설정된 이벤트 조건을 충족하거나 해결되면 알림을 보냅니다.
	Off	설정된 조건을 충족할 때마다 알림을 보냅니다.
연속 N 회 발생	On	N 회 이상 조건을 충족하거나 N 회 이상 이벤트가 해결되면 알림을 보냅니다.
	Off	N 회 이상 설정한 이벤트 조건을 충족하면 알림을 보냅니다. 알림을 보낸 후 횟수를 초기화해 횟수를 다시 집계합니다.

이벤트 대상 선택

특정 에이전트에서만 발생하는 이벤트를 알림으로 보내도록 설정할 수 있습니다. **에이전트 (서버)** 항목을 클릭한 다음 원하는 에이전트를 선택하세요.

2 이벤트 대상 선택

대상 선택 전체 대상이 포함됩니다.

에이전트 (서버)

위 항목들을 설정하지 않으면 프로젝트에 포함된 전체 에이전트를 대상으로 이벤트가 실행되며 많은 알림이 발생할 수 있습니다.

이벤트 대상에 대한 자세한 설명은 가이드 문서를 참고하세요. [가이드 문서 >](#)

이벤트를 시뮬레이션하려면 화면 최상단에 '이벤트 조건 정의' 항목에서 [실행 버튼](#)을 선택하세요.

- ① • 제공되는 템플릿에 따라 선택할 수 있는 대상은 다를 수 있습니다.
- 선택한 대상에 대한 이벤트 발생 현황을 확인하려면 [이벤트 조건 정의](#)에서 [실행](#) 버튼을 선택하세요.
- 대상을 선택하지 않으면 프로젝트에 포함된 전체 에이전트를 대상으로 알림을 보냅니다. 전체 에이전트를 대상으로 이벤트가 실행되면 많은 알림이 발생할 수 있습니다.

기본 정보 및 수신 설정

알림으로 수신되는 이벤트의 제목과 메시지를 작성하고, 수신 대상을 선택할 수 있습니다.

3 기본 정보 및 수신 설정

이벤트 활성화


이벤트 이름 *

메시지 * 

\$를 입력하면 변수를 입력할 수 있습니다.
ex) \$(active_tx_8) \$(time)에 예러가 발생했습니다.

수신 테스트

이벤트 수신 전체 수신 태그 선택 수신

- **이벤트 활성화:** 현재 이벤트를 활성화할 수 있습니다.
- **이벤트 이름:** 기본 제공된 템플릿의 이벤트 이름이 입력되어 있습니다. 사용자가 원하는 이벤트 이름으로 편집할 수 있습니다.
- **메시지:** 기본 제공된 템플릿의 메시지가 입력되어 있습니다. 사용자가 원하는 메시지로 편집할 수 있습니다.  버튼을 클릭하면 이전에 입력한 메시지 기록을 확인할 수 있습니다.

✓ 메시지 입력 창에 `#{Tag}` 또는 `#{Field}` 변수를 입력해 메시지를 작성할 수 있습니다.
 분석 > 매트릭스 조회 메뉴에서 **카테고리**를 선택한 다음 입력할 수 있는 `#{Tag}` 또는 `#{Field}` 변수를 확인하세요.
 현재 이벤트 템플릿의 **카테고리** 이름은 [다음 문서](#)의 **카테고리** 항목을 참조하세요.

- **수신 테스트**: 현재 이벤트로 발생하는 알림 수신 시 입력한 이벤트 이름과 메시지를 사전 점검할 수 있습니다. 필수 항목([지표 설정](#), [이벤트 이름](#), [메시지](#))을 모두 입력해야 테스트할 수 있습니다.

ⓘ 테스트 중에는 실제 매트릭스 값이나 변수에 대한 치환 기능이 작동하지 않으며, 수신자 태그가 설정된 사용자에게만 알림을 보낼 수 없습니다.

- **이벤트 수신**: 현재 이벤트로 발생하는 알림을 수신할 멤버를 선택할 수 있습니다.
 - **전체 수신**: 프로젝트에 소속된 멤버 전원에게 알림을 보냅니다.
 - **태그 선택 수신**: 선택한 태그를 가진 프로젝트 멤버와 3rd-party 플러그인에 알림을 보냅니다. [태그 추가](#) 또는 + 버튼을 클릭해 태그 목록에서 원하는 태그를 선택하세요.

ⓘ [경고 알림](#) > [이벤트 수신 설정](#) 메뉴에서 프로젝트 멤버와 3rd-party 플러그인에 태그를 설정할 수 있습니다. 자세한 내용은 [다음 문서](#)를 참조하세요.

이벤트 추가하기

기본 제공되는 이벤트 템플릿을 편집해 사용자가 원하는 알림을 추가할 수 있습니다.

1. 화면 오른쪽 위에 [이벤트 추가](#) 버튼을 선택하세요.
2. 템플릿 목록에서 추가하려는 이벤트 항목을 선택하세요.
3. [이벤트 대상 선택](#) 및 [이벤트 대상 선택](#), [기본 정보 및 수신 설정](#) 섹션의 옵션을 차례로 설정하세요.
4. 모든 설정을 완료한 다음 화면 오른쪽 위에 [저장](#) 버튼을 선택하세요.


이벤트 목록에서 새로 추가한 이벤트를 확인할 수 있습니다.

ⓘ • 기본 제공되는 이벤트 템플릿과 구별하여 사용하려면 [이벤트 이름](#) 항목을 편집해 저장하세요.

- ① 기본 제공하는 이벤트 템플릿에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.
- 이벤트 조건 설정의 각 섹션에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

이벤트 삭제하기


기본 제공된 이벤트 또는 새로 추가한 이벤트를 삭제할 수 있습니다.

- 이벤트 목록에서 삭제하려는 이벤트 항목에서  버튼을 선택하세요.
- 이벤트 수정 화면으로 이동하면 화면 오른쪽 위에 **삭제** 버튼을 선택하세요.
- 삭제 확인 메시지가 나타나면 다시 한번 **삭제** 버튼을 선택하세요.

- ① 삭제한 이벤트는 복구할 수 없습니다.

JSON 형식으로 수정하기

이벤트 설정을 JSON 형식으로 수정할 수 있습니다.

- 화면 오른쪽 위에 **JSON**  버튼을 선택하세요.
- 편집 창이 나타나면 JSON 형식에 맞춰 내용을 수정하세요.
- 수정을 완료하면 화면 오른쪽 위에 **저장** 버튼을 선택하세요.

- ① 수정한 내용이 JSON 형식에 맞지 않으면 화면 아래에 에러 메시지가 표시되며, 저장할 수 없습니다. 표시되는 에러 메시지는 형식에 따라 다를 수 있습니다.

Expected ', or }' after property value in JSON at position 1964 (line 80 column 42)

JSON 데이터의 구조는 다음과 같습니다.

```
{
```

```

"metaId": "infra001",
"displayName": "CPU",
"stateful": true,
"selectCondition": {},
"warningEnabled": true,
"criticalEnabled": true,
"receiver": [],
"warningThreshold": "cpu > 70",
"criticalThreshold": "cpu > 90",
"repeatCount": 1,
"silentPeriod": 60000,
"enabled": false,
"message": "CPU = ${cpu}"
},

```

JSON 데이터의 필드는 이벤트 설정에서 다음 옵션 항목과 연결됩니다.



JSON 필드	옵션
metaId	사용자가 선택한 템플릿의 고유 식별자 값
displayName	이벤트 이름
stateful	해결된 알림
selectCondition	대상 선택
warningEnabled	Warning 이벤트 활성화 여부
criticalEnabled	Critical 이벤트 활성화 여부
receiver	이벤트 수신 > 태그 선택 수신 옵션의 수신 태그 키값 목록
warningThreshold	Warning 이벤트의 임계값 설정
criticalThreshold	Critical 이벤트의 임계값 설정

JSON 필드	옵션
repeatCount	연속 N 회 발생
silentPeriod	일시 중지
enabled	이벤트 활성화
message	메시지

JSON 파일로 공유하기


이벤트 설정을 JSON 파일로 저장해 다른 사용자와 설정을 공유하거나 다른 사용자의 설정을 가져올 수 있습니다.


내보내기

1. 화면 오른쪽 위에 [JSON](#)  버튼을 선택하세요.
2. JSON 편집 창이 나타나면 [내보내기](#)  버튼을 선택하세요.
3. JSON 파일이 다운로드되면 공유할 다른 사용자에게 전달하세요.

 JSON 파일 이름은 event-rules---.json 형식입니다.

가져오기

1. 화면 오른쪽 위에  버튼을 선택하세요.
2. [내보내기](#) 기능을 통해 다운로드한 JSON 파일을 선택하세요.
3. JSON 편집 창이 나타나면 [목록에 추가하기](#) 또는 [덮어쓰기](#) 버튼을 선택하세요.

 이 기능은 같은 종류의 상품 간에 이용할 것을 권장합니다. 다른 상품의 프로젝트로부터 이벤트 설정을 가져올 수는 있지만 정상 작동하지 않습니다.

이벤트 검색하기

이벤트 목록에서 이벤트 이름 또는 지표를 기준으로 검색할 수 있습니다. 검색 입력란에 문자열을 입력한 다음 🔍 버튼을 선택하세요.

메트릭스 경고 알림

홈 화면 > 프로젝트 선택 > 경고 알림 > 이벤트 설정 > 메트릭스 탭 선택

메트릭스 이벤트란?

메트릭스 이벤트는 기본 이벤트(애플리케이션 이벤트, 서버 이벤트 등)보다 구체적이고 복잡한 이벤트를 설정할 때 사용합니다. 프로젝트에서 실시간으로 수집 중인 메트릭스 데이터를 기반으로 이벤트를 설정할 수 있습니다. 사용에 따라 두 가지 설정 방법 중 하나를 선택해 이벤트를 설정할 수 있습니다.

- 메트릭스 이벤트
- 복합 메트릭스 이벤트

ⓘ 메트릭스에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

메트릭스 이벤트

경고 알림 > 이벤트 설정 메뉴에서 화면 위에 [메트릭스](#)를 선택하세요. 화면 오른쪽 위에 [이벤트 추가](#)를 선택하세요. [메트릭스 이벤트](#) 창이 나타납니다.

× 메트릭스 이벤트

이벤트명 *

이벤트 활성화

템플릿 사용 안 함 ▼

카테고리 * 카테고리를 선택해 주세요. ▼

레벨 * Critical Warning Info 이벤트 상태가 해결되면 추가 알림 ⓘ

메시지 * 카테고리를 먼저 선택해 주세요. 🔊

ex. \${active_tx_8} \${time}에 에러가 발생했습니다.

수신 테스트 🔔 수신 테스트

수신 테스트를 이용하려면 필수 항목(이벤트 명, 카테고리, 레벨, 메시지)에 값을 입력하거나 선택하세요.

발생 조건 & 대상 설정

이벤트 발생조건과 대상 입력시 특수문자(~!@#%*&*()_+=[])가 포함되거나 숫자로 시작하는 필드명을 입력하면 오류가 발생할 수 있습니다.
직접 입력 옵션을 선택한 다음 예시와 같이 중괄호({})로 묶어서 입력하세요.

이벤트 발생 조건 * 선택 입력 직접 입력

필드를 선택해 주세요.

>

값

+ 추가

이벤트 대상 필터링 선택 입력 직접 입력

태그를 선택해 주세요.

>

값

+ 추가

🔗 가이드바로가기

▶ 이벤트 수신 설정

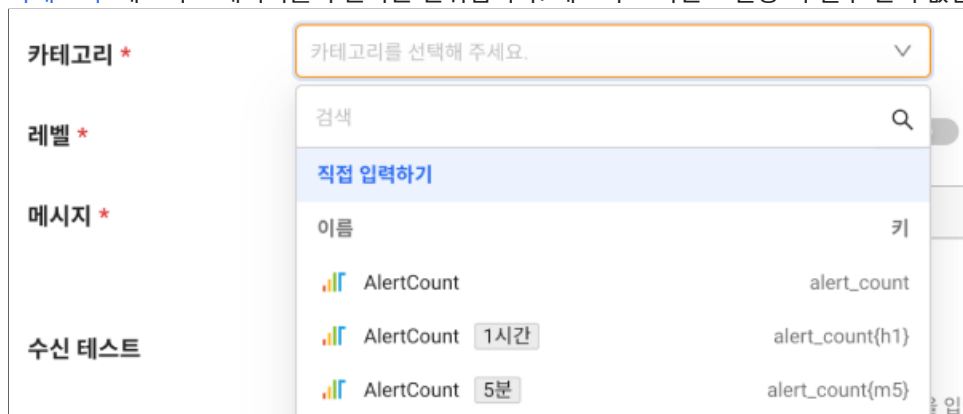
▶ 알림 규칙 테스트

저장

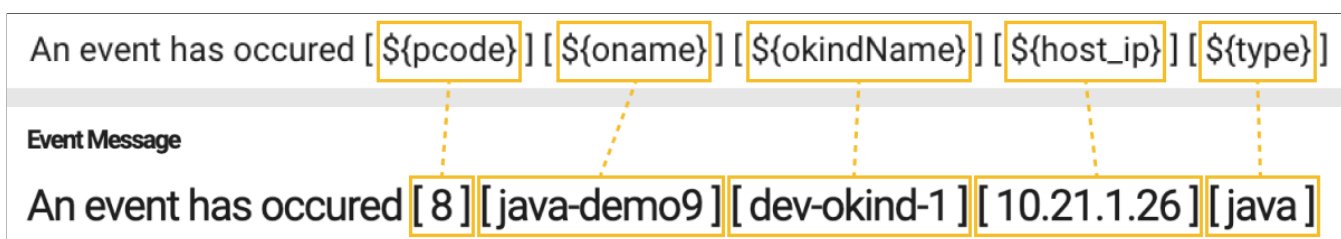
기본 정보 입력

- **이벤트명**: 추가하려는 이벤트 이름을 입력하세요.

- **이벤트 활성화:** 이벤트를 활성화 여부를 선택하세요.
- **템플릿:** 만들어진 템플릿을 선택해 빠르고 쉽게 이벤트를 설정할 수 있습니다. 템플릿을 사용하지 않을 경우 **사용 안 함**을 선택하세요.
- **카테고리:** 메트릭스 데이터를 구분하는 단위입니다. 메트릭스 이벤트 설정 시 필수 선택 값입니다.



- **카테고리** 선택 옵션에는 ① **이름**과 ② **데이터 수집 간격**, ③ **키** 정보를 표시합니다. 이벤트 설정 시 해당 카테고리의 키 값을 사용합니다.
- **카테고리**는 최근 3시간 범위 내 프로젝트에서 수집 중인 메트릭스 데이터를 조회해 목록에 표시합니다. **카테고리** 선택 옵션에 수집 간격이 표시되지 않는 경우 **직접 입력하기** 옵션을 선택해 카테고리 키를 입력할 수 있습니다.
- **레벨**
 - 이벤트 발생 시 경고 수준을 나타냅니다. **Critical**, **Warning**, **Info** 수준으로 나눕니다. **Critical**, **Warning** 레벨 설정 시 **이벤트 상태가 해결되면 추가 알림** 선택 옵션이 활성화됩니다.
 - **이벤트 상태가 해결되면 추가 알림:** 이벤트 항목 중 발생한 이벤트 상태가 해결되면 추가 알림 송신 여부를 선택할 수 있습니다. 토글 버튼을 선택해 기능을 켜거나 끌 수 있습니다.
- **메시지**
 - 이벤트 발생 시 출력하는 알림 메시지를 입력합니다. `{Tag}` 또는 `{Field}` 입력으로 메시지에 변수를 적용할 수 있습니다. 변수에 입력할 키는 선택한 메트릭스 데이터 **카테고리**에 포함된 값이어야 합니다. **메트릭스 조회** 메뉴에서 입력할 수 있는 태그 또는 필드키를 확인할 수 있습니다.



- 버튼을 클릭하면 이전에 입력한 메시지 기록을 확인할 수 있습니다.

• 수신 테스트

필수 항목인 **이벤트명**, **카테고리**, **레벨**, **메시지** 정보를 기준으로 알림을 발생시켜 메시지를 점검하는 기능입니다.

❗ 수신 테스트를 이용하려면 필수 항목(**이벤트명**, **카테고리**, **레벨**, **메시지**)에 값을 입력하거나 선택해야 합니다.

• 이벤트 발생 조건

이벤트 발생 조건 * 선택 입력 직접 입력

4 cpu > 70 && mem > 80 5 6

cpu	Cpu (pct) ▾	>	70
&& ▾	mem Memory (pct) ▾	>	80

+ 추가

4 필드, 5 연산자 선택, 6 임계값을 입력해 이벤트 발생 조건을 설정하세요.

• 이벤트 대상 필터링

이벤트 대상 필터링 선택 입력 직접 입력

7 8 9

태그를 선택해 주세요. ▾	>	값
----------------	---	---

+ 추가

7 태그, 8 연산자 선택, 9 필터링값을 입력해 대상을 필터링합니다. 입력값이 없을 경우 전체 에이전트를 대상으로 경고 알림을 보냅니다.

- ❗ 이벤트 발생 조건과 이벤트 대상 필터링에서 사용할 수 있는 기본 문법과 연산자 목록은 [다음 문서](#)를 참조하세요.
- 이벤트 발생 조건과 이벤트 대상 필터링 옵션은 **선택 입력** 또는 **직접 입력** 옵션을 선택할 수 있습니다.
- 이벤트 설정 내용이 저장된 이후에는 해당 옵션값은 **직접 입력** 옵션으로 관리합니다. 이후 **선택 입력** 옵션으로 전환하면 옵션값이 초기화될 수 있습니다.
- 이벤트 발생 조건과 대상 입력 시 특수 문자(`~!@#%$%^&*()_+=[]'`)를 포함하거나 숫자로 시작하는 필드명을 입력하면 오류가 발생할 수 있습니다. 이런 경우 **직접 입력** 옵션을 선택한 다음 예시와 같이 중괄호(`{ }`)로 묶어서 입력하세요.

```

    ${4xxErrorType} == '401'
    
```

이벤트 수신 설정

▼ 이벤트 수신 설정

발생 횟수 최근 동안 회 발생

선택 시간 동안 설정한 이벤트가 입력 횟수만큼 발생할 때 알림을 수신합니다.
 선택 시간이 "사용 안 함"인 경우에는 지정한 횟수만큼 연속적으로 발생할 때 알림을 수신합니다.
 "이벤트 상태가 해결되면 추가 알림"을 사용하는 경우, 선택 시간은 "사용 안 함"을 권장합니다.
 선택한 카테고리의 수집 주기는 5초입니다.

이벤트 발생 일시 중지

알림 수신 후 선택한 시간 동안 이벤트가 발생하지 않습니다.
 단, "이벤트 상태가 해결되면 추가 알림" 기능을 활성화한 경우에는 RECOVERED 알림 수신 후 선택한 시간 동안 이벤트가 발생하지 않습니다.

이벤트 수신 태그 전체 멤버 수신

이벤트 설정 시 이벤트 수신 태그를 선택하여 해당 태그를 가진 프로젝트 멤버와 3rd-party 플러그인에 알림을 전송할 수 있습니다.
 이벤트 수신 설정 메뉴에서 프로젝트 멤버와 3rd-party 플러그인에 각각 태그를 지정할 수 있습니다

이벤트 설정 시 태그를 선택하지 않은 경우 프로젝트 이벤트 수신 설정 메뉴의 나머지 수신 조건(활성화 여부 등)에 따라 알림이 발생합니다.

- **발생 횟수:** 선택한 시간 동안 **이벤트 발생 조건**에서 설정한 이벤트가 입력 횟수만큼 발생하면 경고 알림을 보냅니다.

- ① ○ 선택 시간을 **사용 안 함**으로 설정하면 입력한 횟수만큼 연속 발생할 때 알림을 보냅니다.
- **이벤트 상태가 해결되면 추가 알림** 옵션을 활성화한 경우 선택 시간은 **사용 안 함**으로 선택할 것을 권장합니다.
- **카테고리** 옵션에서 선택한 항목의 수집 주기는 5초입니다.

- **이벤트 발생 일시 중지:** 과도한 경고 알림 발생을 방지할 수 있는 옵션입니다. 첫번째 경고 알림 이후 선택한 시간 동안 경고 알림을 보내지 않습니다. 또한 **이벤트 기록** 메뉴에 기록되지 않습니다.
- **관련 카테고리:** 관련 카테고리를 5개까지 설정하고 알림 조회 시 참조합니다.
- **이벤트 수신 태그:** 이벤트 수신 태그를 선택하면 해당 태그를 가진 프로젝트 멤버와 3rd-party 플러그인에 알림을 전송할 수 있습니다. 이벤트 수신 태그를 선택하지 않으면 프로젝트 전체 멤버에게 경고 알림을 보냅니다.

- ① **경고 알림 > 이벤트 수신 설정** 메뉴에서 프로젝트 멤버와 3rd-party 플러그인에 태그를 설정할 수 있습니다.

알림 규칙 테스트



선택한 시간 동안 설정한 이벤트 조건을 실행해 몇 번의 경고 알림이 발생했는지 확인할 수 있습니다. 실행 버튼을 선택하면 알림 발생 건수 정보를 알 수 있으며, 이벤트 발생 조건에서 선택한 필드와 임계치를 차트상에 표시합니다.

복합 메트릭스 이벤트

복합 메트릭스 이벤트를 이용하려면 다음의 개념에 대한 이해가 필요합니다.

- [메트릭스란?](#)
- [MXQL](#)

복합 메트릭스 이벤트는 메트릭스 데이터에 보다 복잡한 규칙을 활용해 이벤트를 생성하고 경고 알림을 보낼 수 있습니다. 복합 메트릭스는 다음과 같은 상황에서 효과적으로 사용할 수 있습니다.

- 여러 에이전트에서 수신된 데이터에 대해 종합적인 이벤트 판정을 해야할 때
- 과거 데이터와 현재 데이터를 비교해 이벤트 판정을 해야할 때

메트릭스 이벤트는 에이전트로부터 메트릭스를 수신할 때마다 이벤트 판정을 합니다. 반면, 복합 메트릭스 이벤트는 각 에이전트에서 수집한 메트릭스들을 데이터베이스에 저장합니다. 그리고 다시 조회해서 이벤트 판정을 합니다. 이와 같은 특성 때문에 여러 에이전트의 데이터를 종합적으로 활용하거나 과거의 데이터를 활용할 수 있습니다. 하지만 **MXQL**이라는 와탭 고유의 데이터 조회 언어를 사용해야한다는 진입장벽이 존재합니다. 따라서 사용자들이 기초적인 **MXQL**만 이해하더라도 효과적으로 이벤트를 설정할 수 있도록 이벤트 템플릿을 제공합니다. MXQL 기초 사용자는 이벤트 대상 필터링과 이벤트 조건에 대한 쿼리만 수정해서 이벤트를 적용할 수 있습니다.

1. [경고 알림 > 이벤트 설정](#) 메뉴에서 화면 위에 [메트릭스](#)를 선택하세요.
2. [복합 메트릭스](#) 섹션에서 오른쪽에 [이벤트 추가](#)를 선택하세요.

3. 복합 메트릭스 창이 나타나면 **차트로 생성하기**를 선택하세요.

이벤트 설정 창이 나타납니다.

name	sum	avg	max	recently
633280970	10285	85.70833333333333	122	81
1387800924	10363	86.35833333333333	121	101
-1128904592	10824	90.2	117	100
-1143239575	10038	83.65	124	107
-857948929	10388	86.56666666666666	115	102
-877561626	10278	85.65	127	102

❗ 복합 메트릭스에 이벤트 템플릿에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

이벤트 데이터 조회

복합 메트릭스 이벤트는 메트릭스 데이터 질의 언어인 **MXQL**을 기반으로 이벤트 조건을 생성합니다. **차트로 생성하기** 기능은 **MXQL**의 자동완성을 위한 콤보박스 기능을 제공합니다. 이벤트 데이터를 조회하여 차트를 구성한 다음 이벤트 발행 조건을 직접

입력하기 위한 템플릿입니다. [위젯](#) 또는 [텍스트](#) 옵션을 선택해 이벤트를 설정하세요.



시계열 차트를 구성하는 옵션을 통해 이벤트 설정 시 사용할 **MXQL**을 자동완성할 수 있습니다.

이벤트 데이터 조회

위젯 텍스트

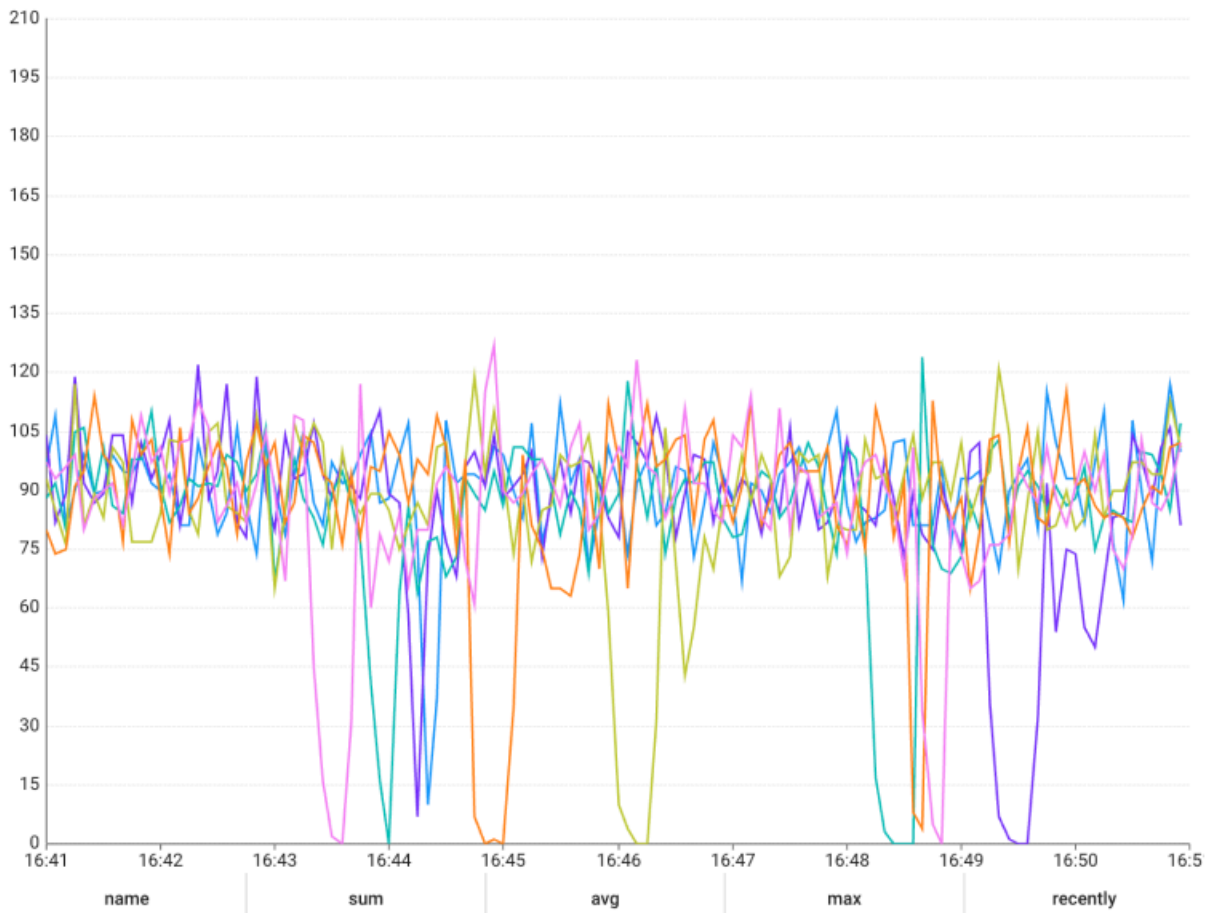
< 2023/08/23 16:41 ~ 2023/08/23 16:51 10분 >

카테고리

필터 + 필터 추가

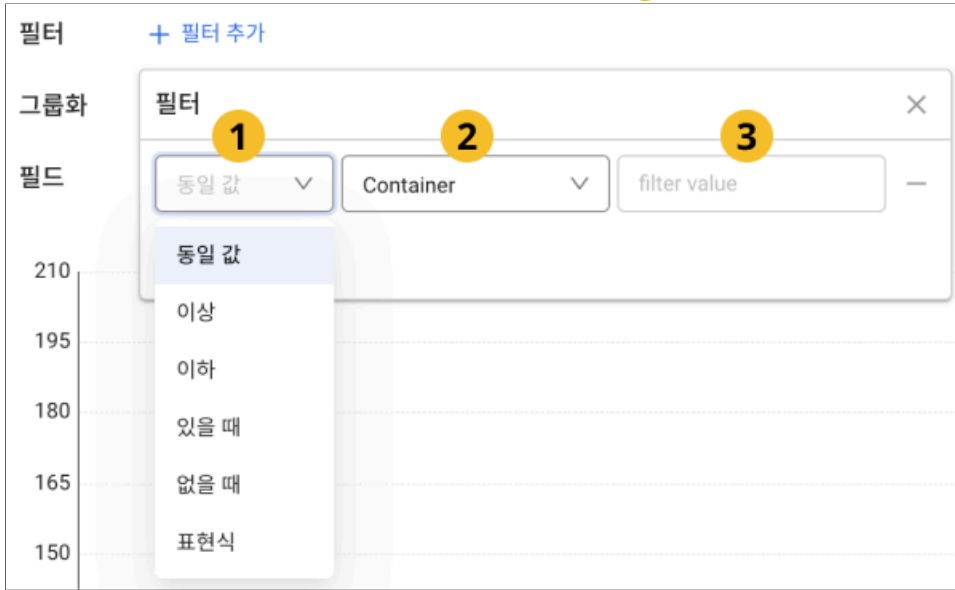
그룹화 타임 유닛 5 초

필드



name	sum	avg	max	recently
633280970	10285	85.70833333333333	122	81
1387800924	10363	86.35833333333333	121	101
-1128904592	10824	90.2	117	100

- **필터**: 이벤트 조건 대상을 선택합니다. ① 연산식, ② 태그, ③ 필터링값을 입력해 필터링 조건을 생성합니다.



- **그룹화**: 그룹화된 메트릭스 데이터를 선택합니다. 다중 선택할 수 있습니다.
- **타임 유닛**: 그룹화된 데이터를 나눌 시간 기준을 설정합니다. 초, 분, 시간 단위로 선택하고 설정할 수 있습니다.
- **필드**: 이벤트 발행 조건에 사용할 필드를 선택합니다. 다중 선택할 수 있습니다.

MXQL을 평문 그대로 수정할 수 있는 편집창이 나타납니다.

이벤트 데이터 조회

위젯 텍스트

```

INJECT timepast
HEADER { "httpc_count$":"COUNT" }
OIDSET { oid:$oid, okind:$okind, onode:$onode }
CATEGORY {"app_counter":6h, "app_counter{m5}":3d, "app_counter{h1}":unlimit }
TAGLOAD
INJECT default
UPDATE {key: httpc_count, value: avg}
FILTER {key: container, exist: true}
GROUP {pk:[oid], timeunit: 5000}
UPDATE {key: httpc_count, value: avg}
CREATE {key: _id_, expr:"oid"}
CREATE {key: _name_, expr:"oname"}
SELECT [_name_, _id_, time, oid, httpc_count]
    
```

조회

< 2023/08/23 16:51 ~ 2023/08/23 17:01 10분 >



httpc_count	_name_	_id_	time	oid
89	demo-8105	-857948929	2023/08/23 16:51:00	-857948929
82	demo-8100	-1128904592	2023/08/23 16:51:00	-1128904592
98	demo-8101	-877561626	2023/08/23 16:51:00	-877561626
81	demo-8102	1387800924	2023/08/23 16:51:00	1387800924
90	demo-8104	-1143239575	2023/08/23 16:51:00	-1143239575
107	demo-8103	633280970	2023/08/23 16:51:00	633280970
107	demo-8105	-857948929	2023/08/23 16:51:05	-857948929
85	demo-8100	-1128904592	2023/08/23 16:51:05	-1128904592
97	demo-8101	-877561626	2023/08/23 16:51:05	-877561626
94	demo-8102	1387800924	2023/08/23 16:51:05	1387800924
86	demo-8104	-1143239575	2023/08/23 16:51:05	-1143239575
85	demo-8103	633280970	2023/08/23 16:51:05	633280970
88	demo-8105	-857948929	2023/08/23 16:51:10	-857948929
6	demo-8100	-1128904592	2023/08/23 16:51:10	-1128904592
79	demo-8101	-877561626	2023/08/23 16:51:10	-877561626
84	demo-8102	1387800924	2023/08/23 16:51:10	1387800924
77	demo-8104	-1143239575	2023/08/23 16:51:10	-1143239575
70	demo-8103	633280970	2023/08/23 16:51:10	633280970
86	demo-8105	-857948929	2023/08/23 16:51:15	-857948929
5	demo-8100	-1128904592	2023/08/23 16:51:15	-1128904592

이전

페이지 1 of 4

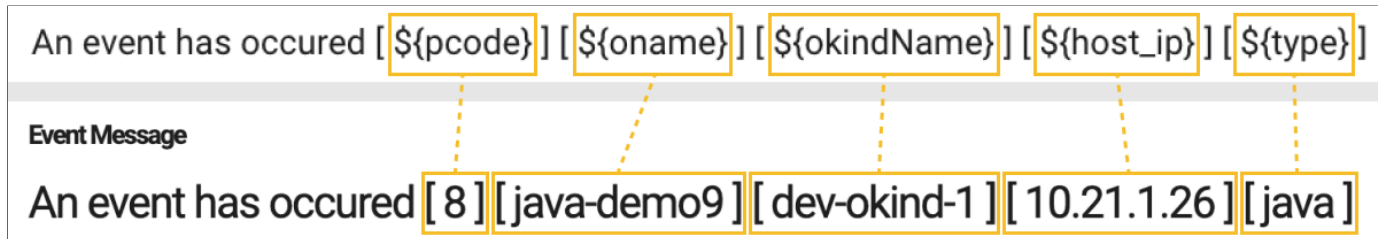
다음

저장

알림

경고 알림 설정의 기본 정보를 입력합니다.

- **이벤트 활성화:** 토글 버튼을 클릭해 이벤트를 활성화할 여부를 선택할 수 있습니다.
- **레벨:** 위험(Critical), 경고(Warning), 정보 수준 중 하나의 레벨을 선택하세요. **이벤트 상태가 해결되면 추가 알림:** 이벤트 항목 중 발생한 이벤트 상태가 해결되면 추가 알림 송신 여부를 선택할 수 있습니다. 토글 버튼을 선택해 기능을 켜거나 끌 수 있습니다.
- **제목:** 경고 알림의 제목을 입력하세요.
- **메시지:** 이벤트 발생 시 출력하는 알림 메시지를 입력합니다. `${Tag}` 또는 `${Field}` 입력으로 메시지에 변수를 적용할 수 있습니다. 변수에 입력할 키는 선택한 메트릭스 데이터 **카테고리**에 포함된 값이어야 합니다. **메트릭스 조회** 메뉴에서 입력할 수 있는 태그 또는 필드키를 확인할 수 있습니다.



알림 정책

경고 알림을 보낼 조건을 입력합니다.

- **데이터 조회 범위:** 이벤트 조건에 사용할 **MXQL**의 실시간 데이터 조회 범위를 설정합니다. 이벤트 데이터 조회에 포함된 필드만 사용할 수 있습니다.
복합 메트릭스 이벤트는 DB에 저장된 메트릭스를 조회해서 활용합니다. 따라서 데이터를 조회할 시간 범위를 먼저 지정해야 합니다. 데이터 조회 시간을 5분으로 선택하면 최근 5분동안 수집된 데이터를 조회해서 이벤트 발생 조건을 확인합니다. 최근 데이터에 대해서 이벤트를 설정할 때에는 짧게, 넓은 시간에 대해서 통계적으로 접근하고 싶을 때에는 길게 설정할 수 있습니다. 실제 사용 예시는 [다음 문서](#)를 참조하세요.
- **조건:** MXQL에 반영한 필드와 연산 규칙, 임계치를 입력합니다.

부가 정보

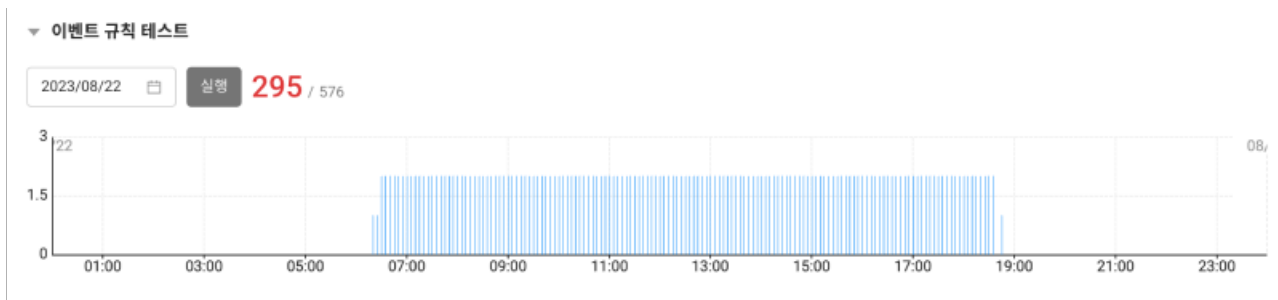
경고 알림 수신과 관련한 부가적인 옵션을 설정합니다.

- **인터벌:** 선택한 시간 간격으로 알림 조건을 확인합니다.
- **무음:** 과도한 경고 알림 발생을 방지할 수 있는 옵션입니다. 첫번째 경고 알림 이후 선택한 시간 동안 경고 알림을 보내지 않습니다. 또한 **이벤트 기록** 메뉴에 기록되지 않습니다.

- **이벤트 수신 태그:** 이벤트 수신 태그를 선택하면 해당 태그를 가진 프로젝트 멤버와 3rd-party 플러그인에 알림을 전송할 수 있습니다. 이벤트 수신 태그를 선택하지 않으면 프로젝트 전체 멤버에게 경고 알림을 보냅니다.

ⓘ 경고 알림 > 이벤트 수신 설정 메뉴에서 프로젝트 멤버와 3rd-party 플러그인에 태그를 설정할 수 있습니다.

이벤트 규칙 테스트



선택한 시간 동안 설정한 이벤트 조건을 실행해 몇 번의 경고 알림이 발생했는지 확인할 수 있습니다. 실행 버튼을 선택하면 알림 발생 건수 정보를 알 수 있으며, 이벤트 발생 조건에서 선택한 필드와 임계치를 차트상에 표시합니다.

이벤트 설정에 포함된 대부분의 내용들이 **MXQL**을 사용해서 지정됩니다. **MXQL**이 적절하게 작성되었는지 시뮬레이션할 수 있는 기능을 제공합니다. 시뮬레이션 기능은 과거의 24시간 데이터를 조회해서 이벤트 판정을 한 다음 몇 건의 메트릭스가 조회되었고 그 중 몇 건에서 이벤트 판정이 성공했는지 알려줍니다.

메트릭스 이벤트 수정 및 삭제

1. 경고 알림 > 이벤트 설정 메뉴로 이동한 다음 **메트릭스** 탭을 선택하세요.
2. 이벤트 목록에서 수정 또는 삭제하려는 항목의 가장 오른쪽에 버튼을 선택하세요.
3. 메트릭스 또는 복합 메트릭스 이벤트 설정 창이 나타나면 각 옵션을 수정한 다음 **저장** 버튼을 선택하세요.
 선택한 이벤트를 삭제하려면 이벤트 설정 창의 오른쪽 위에 **삭제** 버튼을 선택하세요.

발생 조건, 대상 선택 가이드

메트릭스 경고 알림의 이벤트 발생 조건과 이벤트 대상 선택은 동일한 문법을 사용합니다. 단, 이벤트 발생 조건은 태그(Tag)의 Key를 변수로 사용하고, 이벤트 대상 선택은 필드(Field)의 Key를 변수로 사용합니다.

기본 문법

- 문자열을 그냥 입력하면 변수, 작은 따옴표(') 또는 큰 따옴표("")로 감싸면 text로 인식합니다.

```
oid == "oid"
```

- oid : 변수
- == : 함수
- "oid" : text

```
// oname가 ott-1235일 경우
```

```
// 정상적인 경우
```

```
onname = 'ott-1235' 또는 onname = "ott-1235"
```

```
// 비정상적인 경우, 알림이 동작하지 않습니다.
```

```
onname = ott-1235
```

- 숫자를 그냥 입력하면 number, 작은 따옴표(') 또는 큰 따옴표("")로 감싸면 text로 인식합니다.

```
oid == 123
```

- oid : 변수
- == : 함수
- 123 : number

```
// oid가 123일 경우
```

```
// 정상적인 경우
```

```
oid = 123
```

```
// 비정상적인 경우, 알림이 동작하지 않습니다.
```

```
id == '123' 또는 oid == "123"
```

사용 가능한 연산자 목록

연산자	사용법	설명
==	operand1 == operand2	operand1과 operand2의 값이 동일한지 확인합니다.
!=	operand1 != operand2	operand1과 operand2의 값이 다른지 확인합니다.
>	operand1 > operand2	operand1의 값이 operand2의 값보다 큰지 확인합니다.
>=	operand1 >= operand2	operand1의 값이 operand2의 값보다 크거나 같은지 확인합니다.
<	operand1 < operand2	operand1의 값이 operand2의 값보다 작은지 확인합니다.
<=	operand1 <= operand2	operand1의 값이 operand2의 값보다 작거나 같은지 확인합니다.
like	operand1 like operand2	operand1에 operand2가 포함되어 있는지를 패턴으로 검색합니다.
&&	expression1 && expression2	expression1과 expression2이 모두 true인지 확인합니다.
and	expression1 and expression2	expression1과 expression2이 모두 true인지 확인합니다. &&와 동일한 역할을 수행하는 연산자입니다.
	expression1 expression2	expression1 또는 expression2이 true인지 확인합니다.
or	expression1 or expression2	expression1 또는 expression2이 true인지 확인합니다. 와 동일한 역할을 수행하는 연산자입니다.

like 사용법

와일드카드(*****)를 통해 포함 문자열을 편리하게 검색할 수 있습니다.

- 특정 키워드로 시작하는 문자열 검색

Key like "Value*"

- 특정 키워드로 끝나는 문자열 검색

```
Key like "*Value"
```

- 특정 키워드가 포함된 문자열 검색

```
Key like "*Value*"
```

- 키워드 중간에 와일드카드(`*`)를 사용할 수 없습니다.

```
// 지원하지 않는 문법
Key like "Va*lue"
```

- `like` 연산자에서 와일드카드(`*`)를 생략하는 경우 `equals(==)`로 동작합니다.

```
// 아래의 두 문장은 완전히 같은 결과를 가집니다.
Key like "Value"
Key == "Value"
```

사용 가능한 함수 목록

함수	사용법	설명
startsWith	<code>startsWith(param1, param2)</code>	param1을 Key로 하는 Value가 param2로 시작하면 <code>true</code> , 반대의 경우 <code>false</code>

함수	사용법	설명
endsWith	endsWith(param1, param2)	param1을 Key로 하는 Value가 param2로 끝나면 true, 반대의 경우 false
isNull	isNull(param1)	param1이 null이면 true, 반대의 경우 false
isNotNull	isNotNull(param1)	param1이 null이 아니면 true, 반대의 경우 false
isEmpty	isEmpty(param1)	param1이 null 또는 EmptyString("") 이면 true, 반대의 경우 false
isNotEmpty	isNotEmpty(param1)	param1이 null도 아니고 EmptyString("") 도 아니면 true, 반대의 경우 false

startsWith

```
startsWith(Key, "Value")
```

endsWith

```
endsWith(Key, "Value")
```

isNull

```
isNull(Key)
```

isNotNull

```
isNotNull(Key)
```

isEmpty

```
isEmpty(Key)
```

isNotEmpty

```
isNotEmpty(Key)
```

복합 메트릭스 이벤트 템플릿

복합 메트릭스 이벤트 추가 시 + [차트로 생성하기](#) 외 템플릿을 선택해 사용할 수 있습니다. CPU, Disk I/O, Network I/O 지표가 설정한 임계치 기준에 따라 알림을 발생시키는 템플릿을 제공합니다.

✕
복합 메트릭스

템플릿

+
차트로 생성하기

+
CPU % is too high

+
CPU User % is too high

+
The number of agents with high CPU SYS % is too large

+
The Disk I/O is too high

+
The Disk Used % is too high

+
Network Traffic I/O is too high

+
Network Packet I/O is too high

+
Network Error I/O is too high

CPU

ⓘ CPU 관련 지표는 다음과 같습니다. `cpu` , `user_cpu` , `system_cpu`

CPU % is too high

최근 1분 동안 가장 높게 측정된 CPU 관련 지표가 임계치 설정값(`$_rule_`)의 조건(`>` , `<` , `=`)과 일치 시 알림이 발생합니다. 해당 알림은 에이전트(`oname`)별로 발생합니다. [메시지](#) 예시는 다음과 같습니다.

CPU utilization rate of the `$_oname_` in the last minute > `$_rule_` %

CPU User % is too high

최근 1분 동안 가장 높게 측정된 `user_cpu` 지표가 임계치 설정값(`$_rule_`)의 조건(`>`, `<`, `=`)과 일치 시 알림이 발생합니다. 해당 알림은 에이전트(`oname`)별로 발생합니다. **메시지** 예시는 다음과 같습니다.

```
CPU User utilization rate of the $_oname in the last minute > $_rule_ %
```

The number of agents with high CPU SYS % is too large

`system_cpu` 지표가 70% 이상인 서버의 개수가 관련 지표가 임계치 설정값(`$_rule_`)의 조건(`>`, `<`, `=`)과 일치 시 알림이 발생합니다. 해당 알림은 에이전트(`oname`)별로 발생합니다. **메시지** 예시는 다음과 같습니다.

```
The number of agents with a CPU SYS of 70% or more in the last minute > $_rule_
```

Disk

The Disk I/O is too high

최근 1분 동안 가장 높게 측정된 Disk I/O가 관련 지표가 임계치 설정값(`$_rule_`)의 조건(`>`, `<`, `=`)과 일치 시 알림이 발생합니다. 해당 알림은 에이전트(`oname`)별로 발생합니다. **메시지** 예시는 다음과 같습니다.

```
In the last minute, $_oname's Disk I/O > $_rule_ %
```

The Disk Used % is too high

최근 1분 동안 가장 높게 측정된 Disk User I/O가 관련 지표가 임계치 설정값(`$_rule_`)의 조건(`>`, `<`, `=`)과 일치 시 알림이 발생합니다. 해당 알림은 에이전트(`oname`)별로 발생합니다. **메시지** 예시는 다음과 같습니다.

```
In the last minute, $_oname's Disk Used > $_rule_ %
```

Network

Network Traffic I/O is too high

최근 1분 동안 가장 높게 측정된 Network I/O 지표가 임계치 설정값(`$_rule_`)의 조건(`>`, `<`, `=`)과 일치 시 알림이 발생합니다. 해당 알림은 에이전트(`oname`)별로 발생합니다. **메시지** 예시는 다음과 같습니다.

```
In the last minute, $_oname's Network Traffic I/O > $_rule_ %
```

Network Packet I/O is too high

최근 1분 동안 가장 높게 측정된 Network Packet I/O 지표가 임계치 설정값(`$_rule_`)의 조건(`>`, `<`, `=`)과 일치 시 알림이 발생합니다. 해당 알림은 에이전트(`oname`)별로 발생합니다. [메시지](#) 예시는 다음과 같습니다.

In the last minute, `$_oname_`'s Network Packet I/O > `$_rule_` %

Network Error I/O is too high

최근 1분 동안 가장 높게 측정된 Network Error I/O 지표가 임계치 설정값(`$_rule_`)의 조건(`>`, `<`, `=`)과 일치 시 알림이 발생합니다. 해당 알림은 에이전트(`oname`)별로 발생합니다. [메시지](#) 예시는 다음과 같습니다.

In the last minute, The maximum value of the `$_oname_`'s Network Error I/O > `$_rule_` %

알림 메시지 사용자 정의

홈 화면 > 프로젝트 선택 > 경고 알림 > 이벤트 설정 > 메트릭스 탭 선택

프로젝트 멤버에게 메일 또는 서드 파티 플러그인을 통해 전달하는 경고 알림 메시지를 수정할 수 있는 사용자 정의 기능을 제공합니다. 화면 오른쪽 위에 **알림 메시지 설정** 버튼을 선택하세요. 수신할 메시지에서 불필요하다고 생각되는 항목을 감추거나 사용자가 원하는 특별한 내용을 추가할 수 있습니다.

이벤트 설정

애플리케이션 **메트릭스** 히트맵 패턴 이상치 탐지 로그

메트릭스 JSON 📄 **알림 메시지 설정** + 이벤트 추가

이벤트 이름	카테고리	대상	규칙	이벤트 상태가 해결되면 추가 알림	이벤트 수신 태그	설정
메트릭스 값이 1 이상 증가할 때	app_proc_counter	*	gc_oldgen_count >= 1	Off	이벤트 수신 태그 전체 멤버 수신	📄 <input checked="" type="checkbox"/>
신입 사용자 가입이 5분 동안 5명 이상 증가할 때	app_counter 5분	endsWith(okindN..)	(write_time > 3000 read_time > 30...	Off	이벤트 수신 태그 A팀 수신자	📄 <input type="checkbox"/>

복합 메트릭스 JSON 📄 **알림 메시지 설정** + 이벤트 추가

이벤트 이름	조건	이벤트 상태가 해결되면 추가 알림	이벤트 수신 태그	설정
TPS has changed by more than 50% compared to the previous week	one_week_diff_abs > current_tps * 0.3	On	이벤트 수신 태그 전체 멤버 수신	📄 <input type="checkbox"/>

- ① 이 기능은 **메트릭스**, **복합 메트릭스** 경고 알림에만 적용할 수 있습니다.
- 이 기능은 프로젝트 선택 > **실험실** > **알림 메시지** 설정 메뉴 경로로도 진입할 수 있습니다.
- 이 기능은 **알림 설정** 권한을 가진 멤버가 설정할 수 있습니다. 자세한 내용은 [다음 문서](#)를 참조하세요.

기본 화면 안내

알림 메시지

알림 메시지
수신할 메시지의 상세 항목을 선택하고, 항목 별 내용을 편집할 수 있습니다.

다른 프로젝트에 복사 | 전체 초기화 | 전체 저장

전체 | 발생 | 해결 | 검색

전체 펼치기 | 발생 | 이벤트 발생 메시지 | 해결 | 이벤트 해결 메시지

기본 설정 | 초기화 | 미리보기 | 저장 | 전체 활성화

1	메트릭스 발생	상태	ex) 상태:OCCURED/SOLVED	3	4	5
		알림 레벨	ex) 알림 레벨:Warning		수정	ON
		프로젝트 번호	ex) 프로젝트 번호:101		수정	ON
		프로젝트 이름	ex) 프로젝트 이름:Example Project		수정	ON
		애플리케이션 이름	ex) 애플리케이션 이름:Whatap-Front-01		수정	ON
		메시지	ex) 메시지:Message		수정	ON
		이벤트 발생 시각	ex) 이벤트 발생 시각:2022-09-08 14:23:17 +0900		수정	ON
		이벤트 발생 조건	ex) 이벤트 발생 조건:tps > 20		수정	ON
		이벤트 대상 필터링	ex) 이벤트 대상 필터링:oid == 800488350		수정	ON
		해결된 이벤트 알림 기능	ex) 해결된 이벤트 알림 기능:ON/OFF		수정	ON
		알림 종류	ex) 알림 종류:METRICS		수정	ON
		알림 라벨	ex) 알림 라벨:oid(800488350)		수정	ON
		지표	ex) 지표:tps		수정	ON
		현재값	ex) 현재값:25		수정	ON
		임계값	ex) 임계값:20		수정	ON
		현재값(복수)	ex) 현재값(복수):tps=23.39, tx_error=7		수정	ON
		반복 횟수	ex) 반복 횟수:5		수정	ON
		반복 시간	ex) 반복 시간:5 minutes		수정	ON
		무음 시간	ex) 무음 시간:10 minutes		수정	ON


메트릭스 해결 | 기본 설정 | 초기화 | 미리보기 | 저장 | 전체 활성화

복합 메트릭스 발생 | 기본 설정 | 초기화 | 미리보기 | 저장 | 전체 활성화


복합 메트릭스 해결 | 기본 설정 | 초기화 | 미리보기 | 저장 | 전체 활성화

- 알림 메시지의 종류는 **발생** 과 **해결** 로 분류할 수 있습니다. **발생** 은 이벤트가 발생했을 때 전달되는 알림이며, **해결** 은 이벤트가 해소되었을 때 전달되는 알림입니다.
- 1 영역은 수신할 메시지의 상세 항목입니다. 2 영역은 수신할 메시지의 상세 항목에 대한 내용입니다. 3 **미리보기** 버튼을

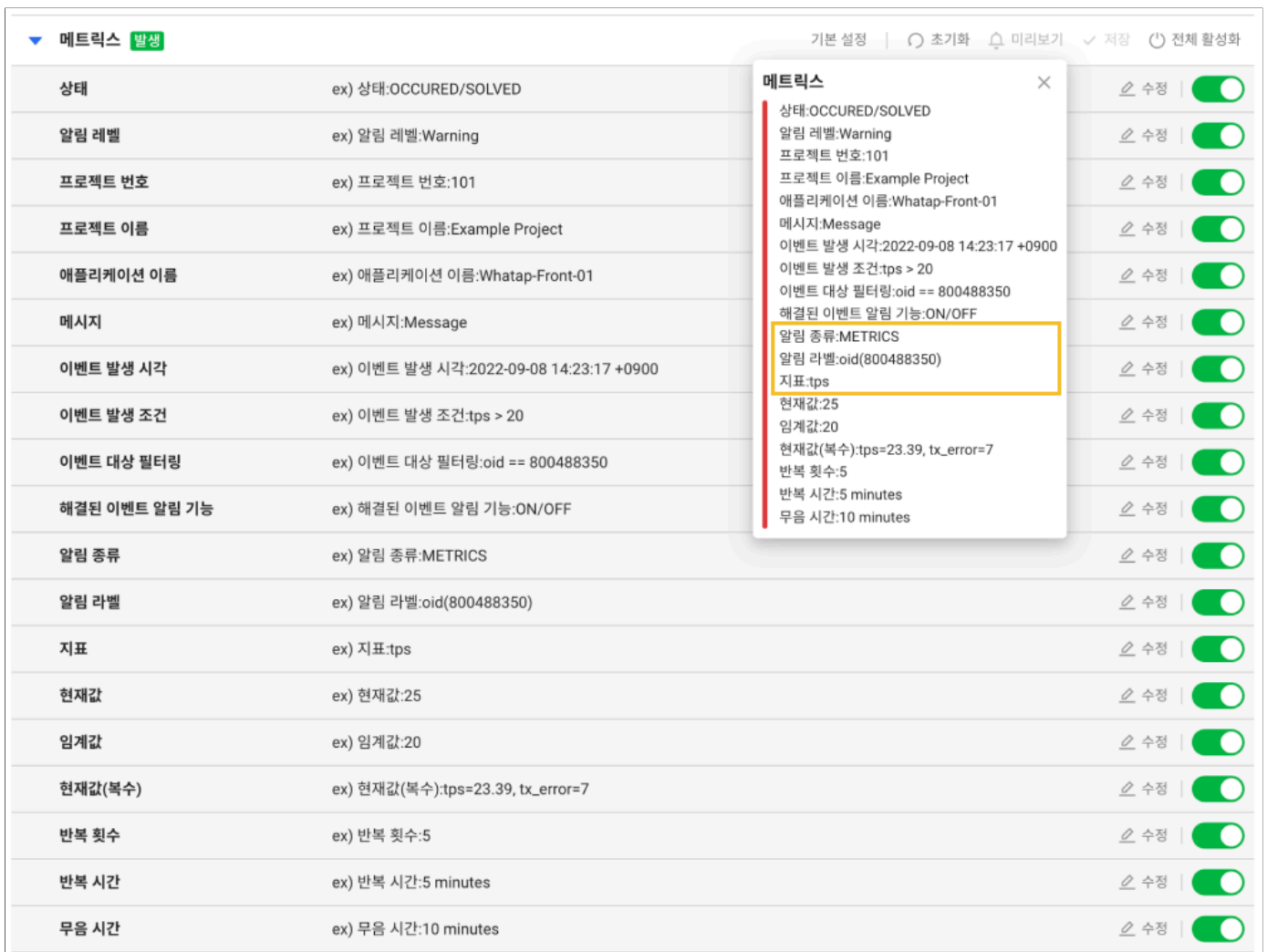
선택하면 수신할 메시지의 내용을 미리 확인할 수 있습니다.

- 수신한 메시지의 내용을 수정하려면 ④  수정 버튼을 선택하세요.
- 수신한 메시지의 상세 항목을 감추려면 ⑤  토글 버튼을 선택해 비활성화하세요.

수신 메시지 상세 항목 감추기

수신 메시지의 내용 중 불필요하다고 생각되는 항목을 감출 수 있습니다. 각 상세 항목의 가장 오른쪽의 토글 버튼을 선택해 해당 항목을 수신 메시지에서 감추거나 보이도록 설정할 수 있습니다.  미리보기 버튼을 선택해 수신할 메시지의 내용을 미리 확인할 수 있습니다.

- 상세 항목 활성화 예시



항목	예시	활성화
상태	ex) 상태:OCCURED/SOLVED	<input checked="" type="checkbox"/>
알림 레벨	ex) 알림 레벨:Warning	<input checked="" type="checkbox"/>
프로젝트 번호	ex) 프로젝트 번호:101	<input checked="" type="checkbox"/>
프로젝트 이름	ex) 프로젝트 이름:Example Project	<input checked="" type="checkbox"/>
애플리케이션 이름	ex) 애플리케이션 이름:Whatap-Front-01	<input checked="" type="checkbox"/>
메시지	ex) 메시지:Message	<input checked="" type="checkbox"/>
이벤트 발생 시간	ex) 이벤트 발생 시간:2022-09-08 14:23:17 +0900	<input checked="" type="checkbox"/>
이벤트 발생 조건	ex) 이벤트 발생 조건:tps > 20	<input checked="" type="checkbox"/>
이벤트 대상 필터링	ex) 이벤트 대상 필터링:oid == 800488350	<input checked="" type="checkbox"/>
해결된 이벤트 알림 기능	ex) 해결된 이벤트 알림 기능:ON/OFF	<input checked="" type="checkbox"/>
알림 종류	ex) 알림 종류:METRICS	<input checked="" type="checkbox"/>
알림 라벨	ex) 알림 라벨:oid(800488350)	<input checked="" type="checkbox"/>
지표	ex) 지표:tps	<input checked="" type="checkbox"/>
현재값	ex) 현재값:25	<input checked="" type="checkbox"/>
임계값	ex) 임계값:20	<input checked="" type="checkbox"/>
현재값(복수)	ex) 현재값(복수):tps=23.39, tx_error=7	<input checked="" type="checkbox"/>
반복 횟수	ex) 반복 횟수:5	<input checked="" type="checkbox"/>
반복 시간	ex) 반복 시간:5 minutes	<input checked="" type="checkbox"/>
무음 시간	ex) 무음 시간:10 minutes	<input checked="" type="checkbox"/>

• 상세 항목 비활성화 예시

메트릭스 발생
기본 설정 | 초기화 | 미리보기 | 저장 | 전체 활성화


상태	ex) 상태:OCCURED/SOLVED	수정	<input checked="" type="checkbox"/>
알림 레벨	ex) 알림 레벨:Warning	수정	<input checked="" type="checkbox"/>
프로젝트 번호	ex) 프로젝트 번호:101	수정	<input checked="" type="checkbox"/>
프로젝트 이름	ex) 프로젝트 이름:Example Project	수정	<input checked="" type="checkbox"/>
애플리케이션 이름	ex) 애플리케이션 이름:Whatap-Front-01	수정	<input checked="" type="checkbox"/>
메시지	ex) 메시지:Message	수정	<input checked="" type="checkbox"/>
이벤트 발생 시각	ex) 이벤트 발생 시각:2022-09-08 14:23:17 +0900	수정	<input checked="" type="checkbox"/>
이벤트 발생 조건	ex) 이벤트 발생 조건:tps > 20	수정	<input checked="" type="checkbox"/>
이벤트 대상 필터링	ex) 이벤트 대상 필터링:oid == 800488350	수정	<input checked="" type="checkbox"/>
해결된 이벤트 알림 기능	ex) 해결된 이벤트 알림 기능:ON/OFF	수정	<input checked="" type="checkbox"/>
알림 종류	ex) 알림 종류:METRICS	수정	<input type="checkbox"/>
알림 라벨	ex) 알림 라벨:oid(800488350)	수정	<input type="checkbox"/>
지표	ex) 지표:tps	수정	<input type="checkbox"/>
현재값	ex) 현재값:25	수정	<input checked="" type="checkbox"/>
임계값	ex) 임계값:20	수정	<input checked="" type="checkbox"/>
현재값(복수)	ex) 현재값(복수):tps=23.39, tx_error=7	수정	<input checked="" type="checkbox"/>
반복 횟수	ex) 반복 횟수:5	수정	<input checked="" type="checkbox"/>
반복 시간	ex) 반복 시간:5 minutes	수정	<input checked="" type="checkbox"/>
무음 시간	ex) 무음 시간:10 minutes	수정	<input checked="" type="checkbox"/>

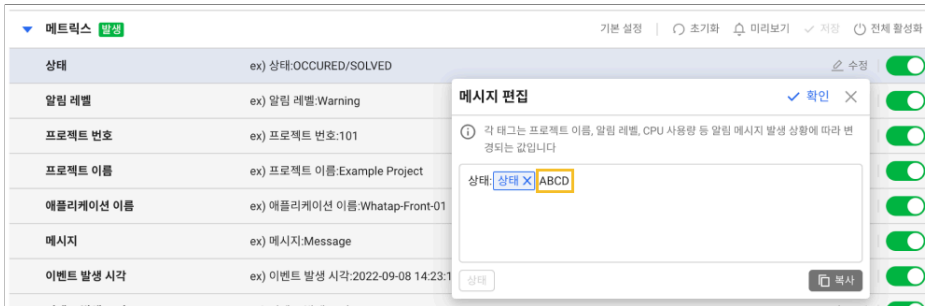
변경 사항을 반영하려면 ✓ **저장** 버튼을 선택하세요. 다른 카테고리의 변경 사항을 한번에 모두 반영하려면 화면 오른쪽 위에 **전체 저장** 버튼을 선택하세요.


- ⓘ • 감춘 상세 항목을 수신 메시지에 다시 추가하려면 해당 항목의 토글 버튼을 선택해 활성화하세요.
- 모든 상세 항목을 수신 메시지에 추가하려면 ☹ **전체 활성화** 버튼을 선택하세요.

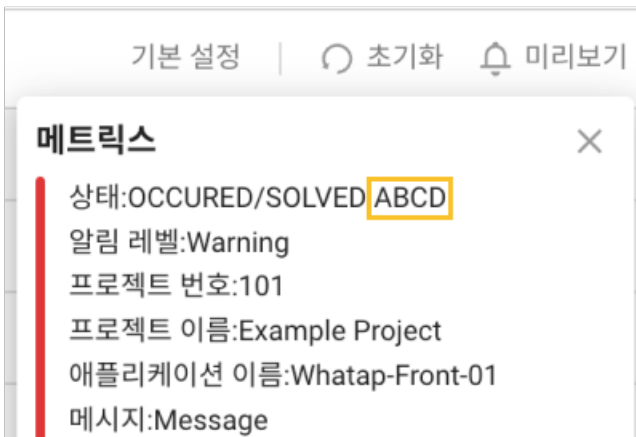
상세 항목 내용 수정하기


상세 항목의 내용에 사용자가 원하는 특별한 내용을 추가할 수 있습니다.

1. 각 상세 항목 가장 오른쪽에  수정 버튼을 선택하세요.
2. **메시지 편집** 창이 나타나면 추가할 내용을 입력하세요.

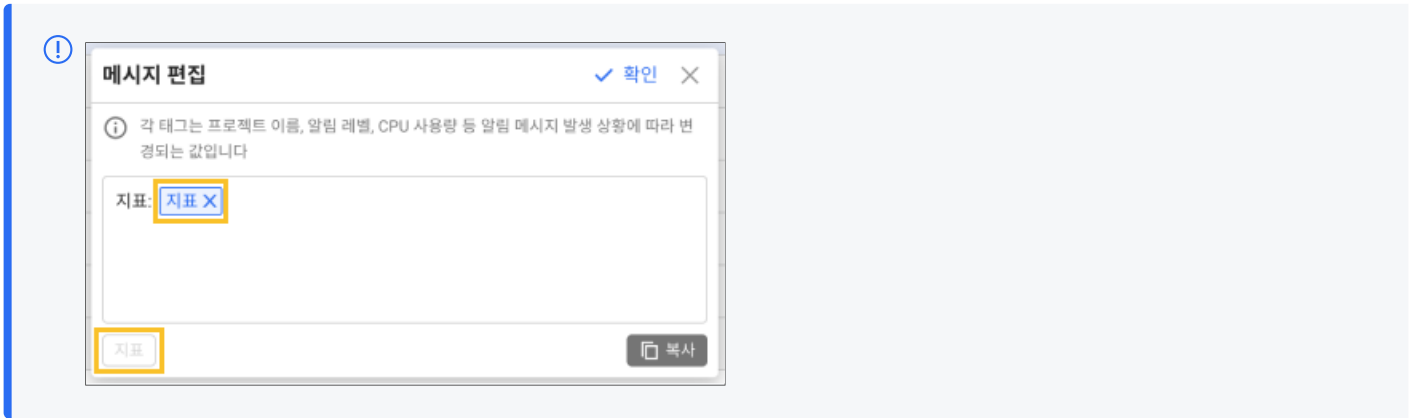


3. **확인** 버튼을 선택하세요.
4.  **미리보기** 버튼을 선택해 수신할 메시지의 내용을 미리 확인하세요.



변경 사항을 반영하려면  **저장** 버튼을 선택하세요. 다른 카테고리의 변경 사항을 한번에 모두 반영하려면 화면 오른쪽 위에 **전체 저장** 버튼을 선택하세요.

- ⓘ **메시지 편집** 창에서 텍스트 블록은 알림 발생 상황에 따라 변경되어 출력되는 변수입니다. 텍스트 블록을 드래그해서 위치를 변경할 수 있습니다. 텍스트 블록을 삭제했다면 창 아래에 텍스트 블록 버튼을 선택해 다시 추가할 수 있습니다.



- ⚠ 사용자에 의해 내용을 수정하기 전의 메시지는 사용자의 언어 상태에 따라 번역되어 전송되나, 내용 수정 이후에는 언어 상태와 관계 없이 사용자 정의된 포맷으로만 알림을 전송합니다.

다른 프로젝트에 설정 복사하기

사용자가 설정한 내용을 다른 프로젝트에 복사할 수 있습니다.

1. 화면 오른쪽 위에 [다른 프로젝트에 복사](#) 버튼을 선택하세요.
2. [프로젝트 적용](#) 창이 나타나면 설정 내용을 복사할 프로젝트를 선택하세요. 모든 프로젝트를 선택하려면 [전체 선택](#)을 선택하세요.
3. [적용](#) 버튼을 선택하세요.

- ⚠ 현재 프로젝트와 동일한 제품 타입만 선택할 수 있습니다.

초기화하기

사용자가 설정한 모든 변경 사항을 초기화하려면 [초기화](#) 버튼을 선택하세요. 모든 카테고리의 변경 사항을 초기화하려면 화면 오른쪽 위에 [전체 초기화](#) 버튼을 선택하세요. 확인 메시지 창이 나타나면 [확인](#) 버튼을 선택하세요.

- ⚠ 초기화된 설정은 복구할 수 없습니다.

이상치 탐지 경고 알림

홈 화면 > 프로젝트 선택 > 경고 알림 > 이벤트 설정 > 이상치 탐지 탭 선택

이상치 탐지(Anomaly Detection)란 데이터 안에서 anomaly, outlier, abnormal과 같이 예상치 못한 패턴을 찾는 일련의 활동입니다. 사용자는 매트릭스의 데이터를 기반으로 상승 패턴과 하락 패턴의 움직임이 평소와 같지 않을 경우 경고 알림을 보내도록 설정할 수 있습니다.

이벤트 설정
🔍 🔔 📄 ⋮ D

애플리케이션
메트릭스
히트맵 패턴
이상치 탐지
로그

이상치 탐지
+ 이벤트 추가

	카테고리	필드	필터	상승/하락 패턴	
	app_counter(m5)	tx_error	없음	보통 / 보통	✎ 🗑️ 🏸
	java_memory(m5)	heap_used	없음	민감 / 민감	✎ 🗑️ 🏸
	app_host_resource(m5)	swap	없음	보통 / 보통	✎ 🗑️ 🏸
	app_counter	tps	없음	민감 / 민감	✎ 🗑️ 🟢
	app_counter(m5)	tx_count	demo-8100 demo-8101 demo-8102 demo-8103	비활성 / 보통	✎ 🗑️ 🏸

+ 이벤트 추가 버튼을 선택해 이상치 탐지 이벤트 설정을 진행할 수 있습니다. 모든 설정을 완료한 다음 저장 버튼을 선택하세요. 이상치 탐지 창의 제목 오른쪽에 토글 버튼을 선택해 활성화 여부를 선택할 수 있습니다.

이상치 탐지 이벤트 생성

이벤트 설정

애플리케이션 메트릭스 히트맵 패턴 **이상치 탐지** 로그

이상치 탐지

이벤트 이름	카테고리	필드
...	app_counter(m5)	tx_error
...	java_memory(m5)	heap_used
...	app_host_resource(m5)	swap
...	app_counter	tps
...	app_counter(m5)	tx_count

✕ 이상치 탐지
● 꺼짐

▼ 이벤트 기본 정보

레벨 정보 경고 위험

* 메시지
알림 발생 시 알림 내용에 포함됩니다.

▼ 메트릭스

* 카테고리

* 필드

필터
이벤트 대상을 필터링합니다.

오브젝트 병합 없음 합산 평균

▼ 이상치 탐지

상승 패턴 둔감 보통 민감

하락 패턴 둔감 보통 민감

저장

이벤트 기본 정보

이상치 탐지 이벤트의 기본 정보를 입력하세요.

- **레벨**: 정보, **경고**, **위험** 수준 중 하나의 레벨을 선택하세요.
- **메시지**: 이벤트 발생 시 출력하는 알림 메시지를 입력합니다. `${태그 또는 필드키}` 입력으로 메시지에 변수를 적용할 수 있습니다. 변수에 입력할 키는 선택한 메트릭스 데이터 **카테고리**에 포함된 값이어야 합니다.

메트릭스

이벤트 발생 대상을 선택하세요.

- **카테고리**: 메트릭스 데이터를 구분하는 단위입니다. 메트릭스 이벤트 설정 시 필수 선택 값입니다.
- **필드**: 이벤트 발행 조건에 사용할 필드를 선택합니다. 다중 선택할 수 있습니다.
- **필터**: 이벤트 조건 대상을 선택합니다. 다중 선택할 수 있습니다.
- **오브젝트 병합**: 오브젝트 병합 방법을 선택할 수 있습니다.

이상치 탐지

상승 패턴 또는 하락 패턴의 민감도를 선택할 수 있습니다. 각 항목의 토글 버튼을 선택해 기능을 켜거나 끌 수 있습니다.

이상치 탐지 이벤트 수정

1. 경고 알림 > 이벤트 설정 메뉴에서 이상치 탐지 탭을 선택하세요.
2. 이상치 탐지 목록에서 수정하려는 항목의 오른쪽에 ✎ 버튼을 선택하세요.
3. 이상치 탐지 설정 창이 나타납니다. 수정이 필요한 항목을 수정한 다음 저장 버튼을 선택하세요.

이상치 탐지 이벤트 삭제

경고 알림 > 이벤트 설정 메뉴에서 이상치 탐지 탭을 선택하세요. 목록에서 삭제하려는 항목의 오른쪽에 🗑 버튼을 선택하세요. 확인 팝업 메시지가 나타나면 삭제 버튼을 선택하세요.

로그 경고 알림

- ❗ 이 기능은 로그 모니터링을 활성화해야 이용할 수 있습니다. **로그 모니터링 활성화**에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.
- 로그 모니터링의 주요 메뉴에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

홈 화면 > 프로젝트 선택 > 경고 알림 > 이벤트 설정 > 로그 탭

수집한 로그 데이터를 조건에 맞춰 필터링해 경고 알림을 설정할 수 있습니다. **+ 이벤트 추가** 버튼을 선택해 로그 이벤트 경고 알림을 설정하세요. 모든 설정을 완료한 다음 **저장** 버튼을 선택하세요.

이벤트 설정

실시간 로그 이벤트 ①
JSON [] [] + 이벤트 추가

이벤트 이름	카테고리	검색 키	검색 값	이벤트 발생 일시 중지	이벤트 대상 필터링	이벤트 수신 태그	설정
실시간 로그 이벤트	AppLog	onodeName	node-0	20분	onode == '334634079' && okindName != 'demo-okind-1'	test-tag	🗑️ <input type="checkbox"/>
이벤트 테스트	AppLog	oid	-1128904592	사용 안 함	사용 안 함	전체 멤버 수신	🗑️ <input checked="" type="checkbox"/>
test	AppLog	oname	demo-8100	사용 안 함	oname && 'demo-8100'	전체 멤버 수신	🗑️ <input checked="" type="checkbox"/>

복합 로그 이벤트 ①
JSON [] [] + 이벤트 추가

이벤트 이름	템플릿	카테고리	규칙	이벤트 상태가 해결되면 추가 알림	이벤트 발생 일시 중지	인터벌	이벤트 수신 태그	설정
이벤트 이름_테스트	2xx 상태코드 건수 <code>count</code>	AppLog	include_minus_exclude_count > 10	Off	1분	5분	전체 멤버 수신	🗑️ <input checked="" type="checkbox"/>
retreter	사용 안 함	#WhatapEvent	rows > 10	Off	1분	5분	전체 멤버 수신	🗑️ <input checked="" type="checkbox"/>
test	사용 안 함	*	rows > 10	Off	1분	5분	전체 멤버 수신	🗑️ <input checked="" type="checkbox"/>

추가할 수 있는 로그 이벤트 다음과 같습니다.

- 실시간 로그 이벤트** : 실시간으로 수집한 로그에서 검색 값이 등장하면 경고 알림을 보냅니다.
- 복합 로그 이벤트** : 최근에 수집한 로그 중 일정 조건을 만족하는 로그가 일정 개수 이상 수집한 경우에 경고 알림을 보냅니다.

- ① 이 이벤트를 추가하거나 설정하려면 **알림 설정** 권한이 있어야 합니다. 사용자별 권한에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.
- 경고 알림과 관련해 모니터링 플랫폼별 지원되는 이벤트 종류를 확인하려면 [다음 문서](#)를 참조하세요.

이벤트 추가 공통 옵션

다음은 이벤트 추가 시 공통으로 설정할 수 있는 옵션입니다.

- 이벤트 이름** : 추가하려는 이벤트 이름을 입력하세요.
- 이벤트 활성화** : 토글 버튼을 클릭해 경고 알림 활성화 여부를 선택할 수 있습니다.
- 레벨** : **위험**, **경고**, 정보 중 하나의 레벨을 선택하세요.
- 메시지** : 이벤트 발생 시 출력하는 알림 메시지를 입력합니다. `#{태그 또는 필드키}` 입력으로 메시지에 변수를 적용할 수 있습니다. 변수에 입력할 키는 선택한 매트릭스 데이터 **카테고리**에 포함된 값이어야 합니다.
- 카테고리** : 로그 구분 명칭(로그 폴더명)을 목록에서 선택하거나 직접 입력할 수 있습니다.
- 이벤트 발생 일시 중지** : 과도한 경고 알림 발생을 방지할 수 있는 옵션입니다. 첫 번째 경고 알림 이후 선택한 시간 동안 경고 알림을 보내지 않습니다. 또한 **이벤트 기록** 메뉴에 기록되지 않습니다.
- 이벤트 수신 태그** : 이벤트 수신 태그를 선택하면 해당 태그를 가진 프로젝트 멤버와 3rd-party 플러그인에 알림을 전송할 수 있습니다. 이벤트 수신 태그를 선택하지 않으면 프로젝트 전체 멤버에게 경고 알림을 보냅니다.

태그를 추가하지 않으면 전체 멤버에게 경고 알림을 보냅니다. **+ 태그 추가**를 클릭한 다음 **태그 목록**에서 경고 알림 수신 대상을 선택하세요. **+ 새 태그 생성**을 선택해 태그를 추가할 수도 있습니다.

- ① **경고 알림 > 이벤트 수신 설정** 메뉴에서 프로젝트 멤버와 3rd-party 플러그인에 태그를 설정할 수 있습니다. **이벤트 수신 설정** 메뉴에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

실시간 로그 이벤트 추가

이벤트 추가

이벤트 이름 * 제목

이벤트 활성화

레벨 * 위험 경고 정보

메시지 * 메시지

카테고리 ⓘ * 카테고리(를) 선택해주세요

검색 키 * 카테고리(를) 먼저 선택해 주세요.

검색 값 * 카테고리(를) 먼저 선택해 주세요.

입력된 단어가 일치하는 경우 알림이 발생합니다.

이벤트 대상 필터링 ⓘ

선택 입력
 직접 입력

+ 추가

ex. oid == '12345678' && level == 'ERROR'

이벤트 발생 일시 중지 * 사용 안 함

알림 수신 후 선택한 시간 동안 이벤트가 발생하지 않습니다. 단, "이벤트 상태가 해결되면 추가 알림" 기능을 활성화한 경우에는 RECOVERED 알림 수신 후 선택한 시간 동안 이벤트가 발생하지 않습니다.

이벤트 수신 태그 ⓘ 전체 멤버 수신 + 태그 추가

[프로젝트 이벤트 수신설정 메뉴 바로가기](#)

저장

- **검색 키** : 로그 데이터 내에서 특정 값에 접근하기 위한 식별자를 의미합니다. 목록에서 선택하거나 직접 입력할 수 있습니다.

예시, HTTP 응답 상태 코드를 나타내는 값에 접근하고자 할 경우 **검색 키** `status`

- **검색 값** : **검색 키**에 해당하는 실제 데이터를 의미합니다. 로그에서 입력한 단어를 포함할 경우 경고 알림을 보냅니다. 목록에서 선택하거나 직접 입력할 수 있습니다.

예시, **검색 키** `status` **검색 값** `200`을 설정한 경우 HTTP 응답 상태 코드 200을 포함하는 로그 데이터 수집 시 경고 알림 발생

- **이벤트 대상 필터링** : **선택 입력** 옵션을 통해 **검색 키**와 **연산자**, **검색 값**을 선택해 대상을 필터링하거나 **직접 입력** 옵션을 선택할 수 있습니다. 입력값이 없을 경우 실시간으로 수집하는 데이터 전체에 대한 알림 발생 여부를 판단합니다.

예시, `AppLog` 카테고리의 로그 중 `level` 이 `ERROR`인 로그를 찾습니다. 일치하는 로그 중에서 `oid`가 `12345678`인 경우 경고 알림을 보냅니다.

복합 로그 이벤트 추가

×
이벤트 추가

***이벤트 이름**

이벤트 활성화

레벨 위험 경고 정보 이벤트 상태가 해결되면 추가 알림 ⓘ

템플릿 사용 안 함

***메시지**

***카테고리 ⓘ** 카테고리(를) 선택해주세요

데이터 조회 범위 최근에 1 분 ▼
선택 시간동안 수집된 로그를 조회합니다.

로그 검색 조건 ⓘ 선택 입력 직접 입력
검색 키 ▼ 검색 값 ▼ 제외 —
+ 추가
이벤트 발행 조건을 입력하기 위해서 카테고리를 먼저 선택해 주세요.

***이벤트 발행 조건** 조건에 맞는 로그 > ▼ 10

인터벌 ⓘ 5 분 ▼

무음 ⓘ 1 분 ▼

이벤트 수신 태그 ⓘ 전체 멤버 수신 + 태그 추가
🔗 프로젝트 이벤트 수신설정 메뉴 바로가기

사용 안 함

2xx 상태코드 건수 count

3xx 상태코드 건수 count

4xx 상태코드 건수 count

5xx 상태코드 건수 count

정상 상태코드(2xx,3xx) 건수 count

에러 상태코드(4xx,5xx) 건수 count

에러 수신 건수 count

저장

- **템플릿** : 복합 로그 템플릿을 제공합니다.
- **로그 검색 조건**
 - **검색 키**에서 이벤트 발생 조건 대상을 선택할 수 있습니다. 선택한 **검색 키**에 해당하는 검색 값을 선택할 수 있습니다.
 - **검색 키**에서 동일한 항목을 추가할 경우 'OR' 조건으로, 다른 항목을 추가할 경우 'AND' 조건으로 동작합니다.
 - **제외** 체크 박스를 선택해 선택한 검색 값을 이벤트 발행 조건에서 제외할 수 있습니다.
 - **+ 추가**를 선택해 여러개의 이벤트 발행 조건을 추가 또는 제외 설정할 수 있습니다.
- **데이터 조회 범위** : 선택한 시간동안 수집한 로그를 조회합니다. 데이터 조회 시간을 5분으로 선택하면 최근 5분 동안 수집한 데이터를 조회해서 이벤트 발생 조건을 확인합니다.
- **이벤트 발행 조건** : 이벤트가 입력한 횟수와 선택한 연산자의 조건과 같이 발생할 때 경고 알림을 보냅니다.

예시, AppLog 카테고리의 로그 중 조건 입력에 해당하는 로그를 필터링 합니다. 조건 입력에서 제외를 체크한 경우 해당 조건으로 찾은 로그를 제외하겠다는 의미입니다. 따라서 level 이 ERROR 인 로그는 제외합니다. 최근 10분 동안 수집한 로그 중 이벤트가 5 보다 작을 경우 경고 알림을 보냅니다.

로그 이벤트 설정 수정하기

1. 경고 알림 > 이벤트 설정 메뉴로 이동하세요.
2. 로그 탭을 선택하세요.
3. 로그 이벤트 목록 중 수정하려는 이벤트 항목에서 오른쪽에 ✎ 버튼을 선택하세요.
4. 이벤트 설정 창이 나타나면 옵션을 수정한 다음 저장 버튼을 선택하세요.

선택한 로그 이벤트를 삭제하려면 이벤트 설정 창에서 오른쪽 위에 삭제 버튼을 선택하세요.




로그 이벤트 끄기

1. 경고 알림 > 이벤트 설정 메뉴로 이동하세요.
2. 로그 탭을 선택하세요.
3. 로그 이벤트 목록 중 경고 알림을 끄려는 이벤트 항목의 가장 오른쪽에 토글 버튼을 선택하세요.

다시 토글 버튼을 선택하면 해당 경고 알림이 활성화됩니다.

로그 이벤트 내보내기/불러오기

로그 이벤트의 설정 내용을 json 파일로 저장한 다음 불러와 재사용할 수 있습니다.

1. 경고 알림 > 이벤트 설정 메뉴로 이동하세요.
2. 로그 탭을 선택하세요.
3. 로그 이벤트 목록 위에 JSON  버튼을 선택하세요. JSON 내보내기 창이 나타납니다.
4. 내보내기 할 항목을 수정 또는 편집하세요.
5. 오른쪽 위에  내보내기 버튼을 선택하세요. 브라우저에서 json 파일을 다운로드합니다.
6. 로그 이벤트 목록 위에  버튼을 선택하세요.
7. 파일 선택 창이 나타나면 앞서 다운로드 받은 json 파일을 선택하세요.
8. JSON 가져오기 창이 나타나면 내용을 수정한 다음 + 목록에 추가하기 버튼을 선택하세요.

❗ 이벤트에 id가 존재합니다. id를 제거한 뒤 다시 시도하세요.

- 메시지가 나타나면 JSON 가져오기 창에서 id 항목을 삭제한 다음 + 목록에 추가하기 버튼을 선택하세요.
- 기존의 이벤트 항목에 덮어쓰기를 하려면 id 항목을 삭제한 다음 덮어쓰기 버튼을 선택하세요.

경고 알림 수신 설정

홈 화면 > 프로젝트 선택 > 경고 알림 > 이벤트 수신 설정

프로젝트 멤버들의 경고 알림 수신과 관련한 다양한 기능을 설정할 수 있습니다.

이벤트 수신 설정



▼ 사용자별 이벤트 수신 설정 (64)

이벤트 알림의 일괄 수신설정 및 접근 설정을 위한 모바일 기기 관리는 [계정 정보 메뉴](#)에서 가능합니다. [계정 정보 >](#)

이름	이메일 알림	SMS 알림	WhatsApp 알림	모바일 알림	반복 알림 (에스컬레이션)	이벤트 수신 태그
JH	<input checked="" type="checkbox"/> 수신 레벨: 위임	<input type="checkbox"/> 수신 레벨: 위임	등록된 번호가 없습니다.	<input type="checkbox"/> 모바일 기기 6대 수신 레벨: 전체	0 저장	<input type="checkbox"/> 수신 태그 미설정 알림 받기 testtag 테스트 태그 +
JT	<input checked="" type="checkbox"/> 수신 레벨: 전체	<input type="checkbox"/> 수신 레벨: 전체	등록된 번호가 없습니다.	<input type="checkbox"/> 등록된 기기가 없습니다.	0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 + 태그 추가
JU	<input checked="" type="checkbox"/> 수신 레벨: 전체	등록된 번호가 없습니다.	등록된 번호가 없습니다.	등록된 기기가 없습니다.	0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 + 태그 추가
KJ	<input type="checkbox"/> 수신 레벨: 전체	<input type="checkbox"/> 수신 레벨: 전체	등록된 번호가 없습니다.	등록된 기기가 없습니다.	0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 + 태그 추가
KY	<input checked="" type="checkbox"/> 수신 레벨: 전체	<input type="checkbox"/> 수신 레벨: 전체	등록된 번호가 없습니다.	등록된 기기가 없습니다.	0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 + 태그 추가
	<input checked="" type="checkbox"/>	<input type="checkbox"/>			0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기

3rd 파티 플러그인

Slack, Telegram, Teams, Jandi, Webhook 등을 이용하여 알림 메시지를 받으실 수 있습니다.

플러그인 이름	인증 키	인증 값	반복 알림 (에스컬레이션)	이벤트 수신 태그
SLACK			0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 + 태그 추가
SLACK			0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 + 태그 추가
SLACK			0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 + 태그 추가
SLACK			0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 + 태그 추가
TELEGRAM			0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 PREV_TEST +
WEBHOOK_JSON			0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 + 태그 추가

➕ 추가하기

대량 알림 발생 방지

알림이 대량으로 발생하면 지정된 시간 동안 알림이 일시적으로 중지됩니다. 대량 알림 차단 기능을 해제하려면 (이메일 주소 옆의) '중단 해제' 버튼을 눌러주세요.

활성화

탐지 시간: 5분

탐지 횟수: 10

정지 시간: 3시간

저장

수신 수단 선택하기

이메일 알림 이외에 SMS, 모바일 알림을 선택할 수 있습니다. 원하는 알림 수신 수단의 체크 박스를 체크하면 경고 알림을 받을 수 있습니다. 알림 수신 수단의 체크 박스를 해제하면 경고 알림을 보내지 않습니다.

- ① • 이메일 알림은 회원 가입 시 입력한 이메일 주소로 알림을 보냅니다.
- 프로젝트 최고 관리자를 제외한 모든 사용자는 자신의 수신 설정만 변경할 수 있습니다.

SMS 알림 수신 추가하기

SMS 알림 수신이 필요한 경우 [계정 관리](#)에서 사용자 전화번호를 설정하세요.

사용자 전화번호

전화번호는 경고 알림 문자에 사용됩니다. 전화번호를 변경하려면 SMS 인증이 필요합니다.

전화번호

일반 휴대전화는 **한국 휴대전화 번호만 등록** 가능합니다.

1. 화면 오른쪽 위에 프로필 아이콘을 선택하세요.
2. 팝업 메뉴가 나타나면 [계정 관리](#) 버튼을 선택하세요.
3. [사용자 전화번호](#) 섹션에서 [일반 휴대전화](#) 버튼을 선택하세요.
4. [전화번호](#)에 인증번호를 수신할 전화번호를 입력하세요.
5. [인증번호 전송](#) 버튼을 선택하세요.
6. 사용자의 휴대전화로 전송된 인증 번호를 입력하세요.
7. [인증하기](#) 버튼을 선택하세요.

- ① • 등록된 전화번호를 변경하려면 [번호 변경하기](#) 버튼을 선택한 다음 위의 과정을 반복하세요.
- SMS를 알림으로 수신할 수 있는 전화번호는 **한국 휴대전화 번호만** 등록할 수 있습니다.

WhatsApp 알림 수신 추가하기

WhatsApp을 통해 알림을 수신할 수 있습니다.

사용자 전화번호

전화번호는 경고 알림 문자에 사용됩니다. 전화번호를 변경하려면 SMS 인증이 필요합니다.

일반 휴대전화 **WhatsApp**

전화번호 KR (+82) 인증번호 전송

1. 화면 오른쪽 위에 프로필 아이콘을 선택하세요.
2. 팝업 메뉴가 나타나면 **계정 관리** 버튼을 선택하세요.
3. **사용자 전화번호** 섹션에서 **WhatsApp** 버튼을 선택하세요.
4. **전화번호**에 인증번호를 수신할 전화번호를 입력하세요.
5. **인증번호 전송** 버튼을 선택하세요.
6. WhatsApp 애플리케이션으로 전송된 인증번호 6자리를 입력하세요.
7. **인증하기** 버튼을 선택하세요.

ⓘ 등록된 전화번호를 변경하려면 **번호 변경하기** 버튼을 선택한 다음 위의 과정을 반복하세요.

수신 레벨 선택하기

경고 알림 레벨에 따라 알림 수신 여부를 선택할 수 있습니다. **사용자별 이벤트 수신 설정** 섹션의 사용자 목록에서 **수신 레벨**을 **전체** 또는 **위험**을 선택하세요.

- **전체**: 모든 경고 알림을 수신할 수 있습니다.
- **위험**: 위험 레벨의 경고 알림만 수신할 수 있습니다.

요일 및 시간별 알람 설정하기

요일별, 시간별 알림 수신 여부를 선택할 수 있습니다. **사용자별 이벤트 수신 설정** 섹션의 사용자 목록에서 가장 왼쪽에 ▾ 버튼을 선택하세요. 경고 알림 수신을 원하는 요일을 선택하거나 시간을 입력하세요. 알림 수신 수단별로 설정할 수 있습니다.

▼ 사용자별 이벤트 수신 설정 (64)

이벤트 알림의 일괄 수신설정 및 접근 설정을 위한 모바일 기기 관리는 [계정 정보 메뉴에서](#) 가능합니다. [계정 정보 >](#)

이름	이메일 알림	SMS 알림	WhatsApp 알림	모바일 알림	반복 알림 (에스컬레이션)	이벤트 수신 태그
HS	<input checked="" type="checkbox"/> 수신 레벨: 전체	<input type="checkbox"/> 0***** 등록된 번호가 없습니다.	<input type="checkbox"/>	<input type="checkbox"/> 모바일 기기 2대 수신 레벨: 전체	0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 + 태그 추가
알림 수신 언어	요일 <input checked="" type="checkbox"/> 월 <input checked="" type="checkbox"/> 화 <input checked="" type="checkbox"/> 수 <input checked="" type="checkbox"/> 목 <input checked="" type="checkbox"/> 금 <input checked="" type="checkbox"/> 토 <input checked="" type="checkbox"/> 일 시간 00:00 ~ 00:00	요일 <input checked="" type="checkbox"/> 월 <input checked="" type="checkbox"/> 화 <input checked="" type="checkbox"/> 수 <input checked="" type="checkbox"/> 목 <input checked="" type="checkbox"/> 금 <input checked="" type="checkbox"/> 토 <input checked="" type="checkbox"/> 일 시간 00:00 ~ 00:00	요일 <input checked="" type="checkbox"/> 월 <input checked="" type="checkbox"/> 화 <input checked="" type="checkbox"/> 수 <input checked="" type="checkbox"/> 목 <input checked="" type="checkbox"/> 금 <input checked="" type="checkbox"/> 토 <input checked="" type="checkbox"/> 일 시간 00:00 ~ 00:00	모바일 기기 테스트	테스트	

경고 알림 반복 설정하기

경고 알림 발생 시간으로부터 알림 발생 상황이 해소되지 않을 경우 최초 알림 발생 시각으로부터의 알림 반복 간격을 설정할 수 있습니다. 예를 들어, 경고 알림 발생 시간으로부터 0분(즉시), 1시간 후, 1일 후에 경고 알림을 반복하려면 '0,1H,1D'를 [반복 알림 \(에스컬레이션\)](#) 컬럼 항목에 입력하세요.

반복 알림 (에스컬레이션) ⓘ

0,1H,1D

저장

- ⓘ • 이 기능은 **Critical** (또는 **위험**) 등급의 모든 이벤트를 대상으로 합니다. 이벤트 추가 시 설정한 **레벨** 항목을 참조하세요.
- **M**: 분, **H**: 시간, **D**: 일, 단위를 생략하면 분 단위로 시간을 설정합니다.
- **저장** 버튼을 선택하지 않으면 설정을 완료할 수 없습니다.
- 숫자 또는 숫자+단위(**M**, **H**, **D**)로 입력하세요. 입력이 올바르지 않으면 메시지가 표시됩니다.

팀별, 사용자별 알림 설정하기

프로젝트의 멤버 중 특정 멤버 또는 팀을 대상으로 알림 수신 여부를 설정합니다. [메트릭스](#) 및 [이상치 탐지](#), [로그](#) 이벤트 설정의 [이벤트 수신 태그](#) 항목에서 태그를 추가하세요. 이벤트별로 경고 알림을 수신하는 멤버 또는 팀을 선택할 수 있습니다.

반대로 이벤트 수신 태그를 설정하지 않으면 전체 멤버에게 경고 알림을 보낼 수 있습니다.

> 이벤트 수신 태그 사용 예시

이벤트 수신 태그에 대한 사용 예시를 통해 팀별 또는 사용자별로 경고 알림을 전송하는 설정 방법에 대해 알아봅니다. 다음과 같이 팀 별로 서로 다른 경고 알림을 전송하도록 설정합니다.

알림 종류	서버팀 수신 여부	데브옵스팀 수신 여부
메트릭스 경고 알림	O	X
이상치 탐지 경고 알림	O	O
로그 실시간 경고 알림	X	O

1. 이벤트 수신 설정하기 (경고 알림 > 이벤트 수신 설정)

▼ 사용자별 이벤트 수신 설정 (64)

이벤트 알림의 일괄 수신설정 및 접근 설정을 위한 모바일 기기 관리는 [계정 정보 메뉴에서](#) 가능합니다. [계정 정보 >](#)

이름	이메일 알림	SMS 알림	WhatsApp 알림	모바일 알림	반복 알림 (에스컬레이션)	이벤트 수신 태그
DE	<input checked="" type="checkbox"/> 수신 레벨: 전체	등록된 번호가 없습니다.	등록된 번호가 없습니다.	등록된 기기가 없습니다.	0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 Server +
DE	<input checked="" type="checkbox"/> 수신 레벨: 전체	등록된 번호가 없습니다.	등록된 번호가 없습니다.	등록된 기기가 없습니다.	0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 DevOps +

프로젝트에 속한 멤버들 중 서버팀 소속은 [서버팀](#), 데브옵스팀 소속은 [데브옵스팀](#) 으로 이벤트 수신 태그를 설정하세요.

2. 메트릭스 경고 알림 설정하기 (경고 알림 > 이벤트 설정 > 메트릭스 > 이벤트 추가 > 이벤트 수신 설정)

이벤트 수신 태그 Server +

이벤트 설정 시 이벤트 수신 태그를 선택하여 해당 태그를 가진 프로젝트 멤버와 3rd-party 플러그인에 알림을 전송할 수 있습니다.
이벤트 수신 설정 메뉴에서 프로젝트 멤버와 3rd-party 플러그인에 각각 태그를 지정할 수 있습니다

[프로젝트 이벤트 수신설정 메뉴](#)

이벤트 설정 시 태그를 선택하지 않은 경우 프로젝트 이벤트 수신 설정 메뉴의 나머지 수신 조건(활성화 여부 등)에 따라 알림이 발생합니다.

태그 추가 또는 **+** 버튼을 클릭하세요. 태그 목록에서 원하는 태그를 선택하거나 새 태그를 생성하세요. 메트릭스 이벤트에 대한 알림을 `서버팀`으로 설정한 경우입니다.

3. 로그 실시간 경고 알림 설정 (경고 알림 > 이벤트 설정 > 로그 > 이벤트 추가 > 이벤트 수신 태그)

이벤트 수신 태그 ⓘ DevOps +

[프로젝트 이벤트 수신설정 메뉴 바로가기](#)

태그 추가 또는 **+** 버튼을 클릭하세요. 태그 목록에서 원하는 태그를 선택하거나 새 태그를 생성하세요. 로그 실시간 이벤트에 대한 알림을 `데브옵스팀`으로 설정한 경우입니다.

4. 이상치 탐지 이벤트는 전체 멤버에게 경고 알림을 전송하므로 이벤트 수신 태그를 설정하지 않습니다.

이벤트 수신 태그 추가하기

1. **사용자별 이벤트 수신 설정** 섹션의 사용자 목록에서 **태그 추가** 또는 **+** 버튼을 선택하세요.
2. **이벤트 수신 태그** 팝업 창이 나타나면 태그 입력란에 태그 이름을 입력한 다음 엔터를 입력하거나 **새 태그 생성**을 선택하세요.
3. 태그 색상을 선택하세요.
4. **태그 생성** 버튼을 선택하세요.

태그 목록에서 생성한 태그를 확인할 수 있습니다. 생성한 태그를 적용하려면 해당 태그를 선택하세요.

이벤트 수신 태그 해제하기

1. **사용자별 이벤트 수신 설정** 섹션의 사용자 목록에서 **+** 버튼을 선택하세요.
2. **이벤트 수신 태그** 팝업 창이 나타나면 적용된 태그 옆에 **×** 버튼을 선택하세요.
3. **이벤트 수신 태그** 팝업 창을 닫으세요.

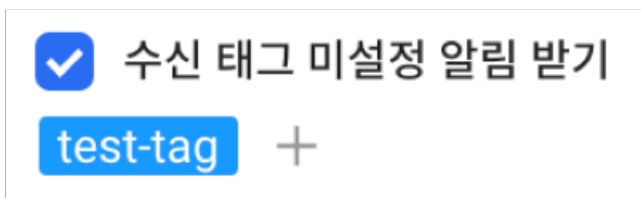
이벤트 수신 태그를 해제합니다.

이벤트 수신 태그 수정 및 삭제하기

1. **사용자별 이벤트 수신 설정** 섹션의 사용자 목록에서 **태그 추가** 또는 **+** 버튼을 선택하세요.
2. **이벤트 수신 태그** 팝업 창이 나타나면 **태그 목록**에서 수정 또는 삭제할 항목의 **✎** 버튼을 선택하세요.
3. 태그 이름을 수정하거나 색상을 변경한 다음 **적용** 버튼을 선택하세요.
태그를 삭제하려면 **🗑️ 태그 삭제** 버튼을 선택하세요.

❗ 이벤트에 적용 중인 **이벤트 수신 태그** 항목은 삭제할 수 없습니다.

수신 태그 미설정 알림



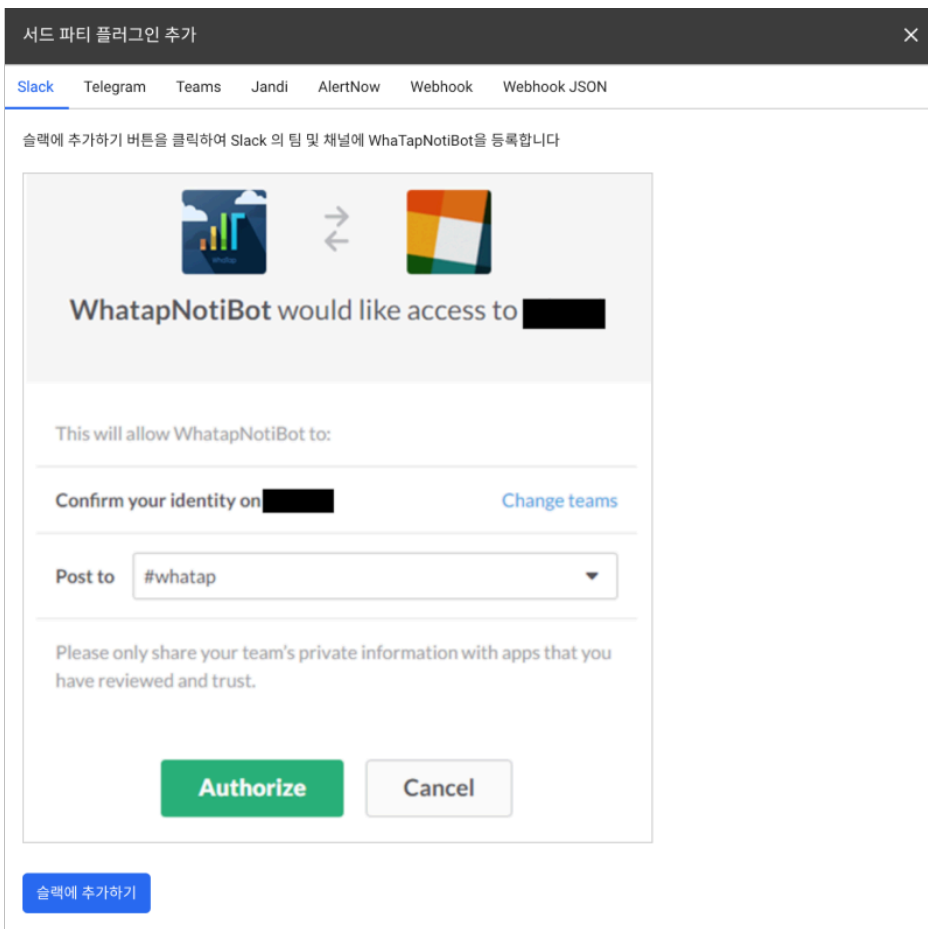
이벤트 수신 태그가 설정되지 않은 경고 알림을 받으려면 **수신 태그 미설정 알림 받기** 옵션을 선택하세요. **이벤트 수신 태그**가 설정된 경고 알림만 받고 싶다면 선택을 해제하세요.

❗ 모든 경고 알림을 받지 않으려면 해당 옵션을 해제하고 선택한 **이벤트 수신 태그**가 없어야 합니다.

3rd 파티 플러그인 알림 추가하기

Slack, Telegram, Teams, Jandi, Webhook 등의 외부 애플리케이션을 통해 경고 알림을 받을 수 있습니다.

1. **경고 알림 > 이벤트 수신 설정** 메뉴에서 **3rd 파티 플러그인** 섹션의 **추가하기** 버튼을 선택하세요.
2. 원하는 서비스를 선택하세요.



3. 선택한 서비스의 화면 안내에 따라 설정을 진행하세요.
4. 모든 과정을 완료했다면 추가 버튼을 선택하세요.

ⓘ 와탭랩스의 지원 범위에 포함하지 않는 사내 메신저는 표준 Webhook, webhook json을 통해 연동할 수 있습니다.

대량 알림 발생 방지

알림이 대량으로 발생하면 설정한 시간 동안 경고 알림을 일시적으로 중단합니다. [경고 알림](#) > [이벤트 수신 설정](#) 메뉴에서 [대량 알림 발생 방지](#) 섹션으로 이동하세요.

대량 알림 발생 방지

알림이 대량으로 발생하면 지정한 시간 동안 알림이 일시적으로 중지됩니다.
대량 알림 차단 기능을 해제하려면 (이메일 주소 옆의) '중단 해제' 버튼을 눌러주세요.

활성화



탐지 시간

5분



탐지 횟수

10

정지 시간

3시간



저장

- **활성화** 토글 버튼을 선택해 기능을 켜거나 끌 수 있습니다.
- **탐지 시간** 동안 **탐지 횟수** 이상의 이벤트가 발생하면 **정지 시간** 동안 경고 알림을 중지합니다.

예를 들어, 5분 동안 20회의 이벤트가 발생하면 5분 동안 경고 알림을 중지합니다. 설정한 **정지 시간** 시간이 지나면 대량 알림 발생 방지 기능은 해제됩니다.

❗ 문자 메시지 알림이 하루 200건 이상 발생하면 일시 중지하며 다음 메시지를 표시합니다. 문자 알림 중단 기능을 해제하려면 **문자알림 중단 해제** 버튼을 선택하세요.

다량의 문자메시지가 전송되었습니다. (200건 / 일)

- ① 프로젝트에서 발생한 많은 양의 문자 메시지로 인해 문자 메시지 알림이 중지됩니다.
- 시작 시간 : 2024-02-02 18:40:01

문자알림 중단 해제

경고 알림 사용자 설정하기

계정 관리 메뉴에서 사용자 개인의 알림 수신 레벨, 수신 수단, 요일 및 시간 등을 설정할 수 있습니다.

1. 화면의 오른쪽 위에 프로필 아이콘을 선택하세요.
2. 팝업 메뉴가 나타나면 **계정 관리** 버튼을 선택하세요.

3. 화면을 아래로 스크롤해 [알림 수신 설정](#) 섹션으로 이동하세요.
4. 수신 레벨, 수신 수단, 요일 및 시간을 설정한 다음 [저장](#) 버튼을 선택하세요.

경고 알림 언어 설정

프로젝트에서 발생하는 경고 알림 메시지의 언어를 변경할 수 있습니다.

1. 홈 화면에서 경고 알림 메시지의 언어를 변경할 프로젝트를 선택하세요.
2. 화면 왼쪽 메뉴에서 [관리](#) > [프로젝트 관리](#)를 선택하세요.
3. [알림 언어 관리](#) 섹션에서 원하는 언어를 선택하세요.
4. 화면 오른쪽 아래에 [저장](#) 버튼을 선택하세요.

이벤트 기록

홈 화면 > 프로젝트 선택 > 경고 알림 > 이벤트 기록

경고 알림이 발생한 이력을 확인할 수 있습니다. 발생한 모든 이벤트 내역 리스트 조회가 가능합니다.

1 2023/02/27 00:00 ~ 2023/02/28 00:00 1일 >		서버 이름 또는 이벤트 이름 검색		Q	<input type="checkbox"/> 진행 중인 이벤트만 보기	<input type="checkbox"/> 이벤트 해소 시각 표시	CSV
이벤트 이름	이벤트 발생 시각	서버	스냅샷				
Memory Used > 70 %	2023/02/27 14:22:15 진행 중 + 처리내역	ip-10-21-1-191	CPU 0.3% CPU User 사용률 0.1% CPU System 사용률 0.2%	Memory Used % 70.1% Used Size 646M Free 32M Cached 280M Pagefaults 0 Swap Used% 0% Swap Used 0	디스크 44.8% Used Size 2.6G Free 94.5M Cached 953M Pagefaults 266B Swap Used% 0% Swap Used 0	네트워크 / ens5 19.4K lo 0B	
CPU Used > 70 %	2023/02/27 14:10:45 + 처리내역	virtual-java-agent	CPU 71.4% CPU User 사용률 43.5% CPU System 사용률 26.7%	Memory Used % 70% Used Size 2.6G Free 94.5M Cached 953M Pagefaults 266B Swap Used% 0% Swap Used 0	디스크 72.9% Used Size 2.5G Free 174M Cached 943M Pagefaults 515B Swap Used% 0% Swap Used 0	네트워크 / lo 7.1M ens5 1.3M	
CPU Used > 70 %	2023/02/27 13:13:00 + 처리내역	virtual-java-agent	CPU 71.7% CPU User 사용률 46.4% CPU System 사용률 24.1%	Memory Used % 68.2% Used Size 2.5G Free 174M Cached 943M Pagefaults 515B Swap Used% 0% Swap Used 0	디스크 72.8% Used Size 2.5G Free 174M Cached 943M Pagefaults 515B Swap Used% 0% Swap Used 0	네트워크 / lo 7M ens5 1.3M	
Memory Used > 70 %	2023/02/27 12:05:50 + 처리내역	ip-10-21-1-191	CPU 0.7% CPU User 사용률 0.2% CPU System 사용률 0.5%	Memory Used % 70.1% Used Size 646M Free 32.8M Cached 285M Pagefaults 0B Swap Used% 0% Swap Used 0	디스크 44.8% Used Size 646M Free 32.8M Cached 285M Pagefaults 0B Swap Used% 0% Swap Used 0	네트워크 / ens5 19.7K lo 0B	

1 상단 옵션

시간 선택

- 오른쪽에 위치한 녹색 버튼을 선택해 조회 시간을 선택할 수 있습니다. 기본 설정은 12시간 입니다.
- < 또는 > 버튼을 선택해 선택한 조회 시간 만큼 간격을 이동할 수 있습니다.
- 세부 시간을 선택하려면 날짜 또는 시간 영역을 선택하세요. 세부 시간을 설정한 다음 **확인** 버튼을 선택하세요.

입력창

입력창에서 서버 이름 혹은 이벤트 이름으로 검색할 수 있습니다.

- [진행 중인 이벤트만 보기](#)

이벤트 기록 목록에서 [진행 중인 이벤트](#)만 조회할 수 있습니다.

- [이벤트 해소 시각 표시](#)

이벤트 기록 목록에 [이벤트 해소 시각](#) 컬럼을 추가할 수 있습니다.

❗ 진행 중인 이벤트는 [이벤트 해소 시각](#)을 조회하지 않습니다.

- [CSV](#)

조회한 이벤트 기록 결과를 csv 파일로 저장할 수 있습니다. [최대 CSV 라인 수](#)를 입력한 다음 [다운로드](#) 버튼을 선택하세요.

- **2 이벤트 기록 목록**

- [위험도](#)

위험도는 [Fatal](#)(위험), [Warning](#)(경고) 색깔로 표시됩니다.

- [이벤트 이름](#)

이벤트 정책에서 설정한 값을 바탕으로 발생한 이벤트 이름입니다.

- [이벤트 발생 시각](#)

이벤트 발생 시간입니다.

- [+ 처리내역](#)

이벤트 처리 내역을 추가할 수 있습니다.

- [서버](#)

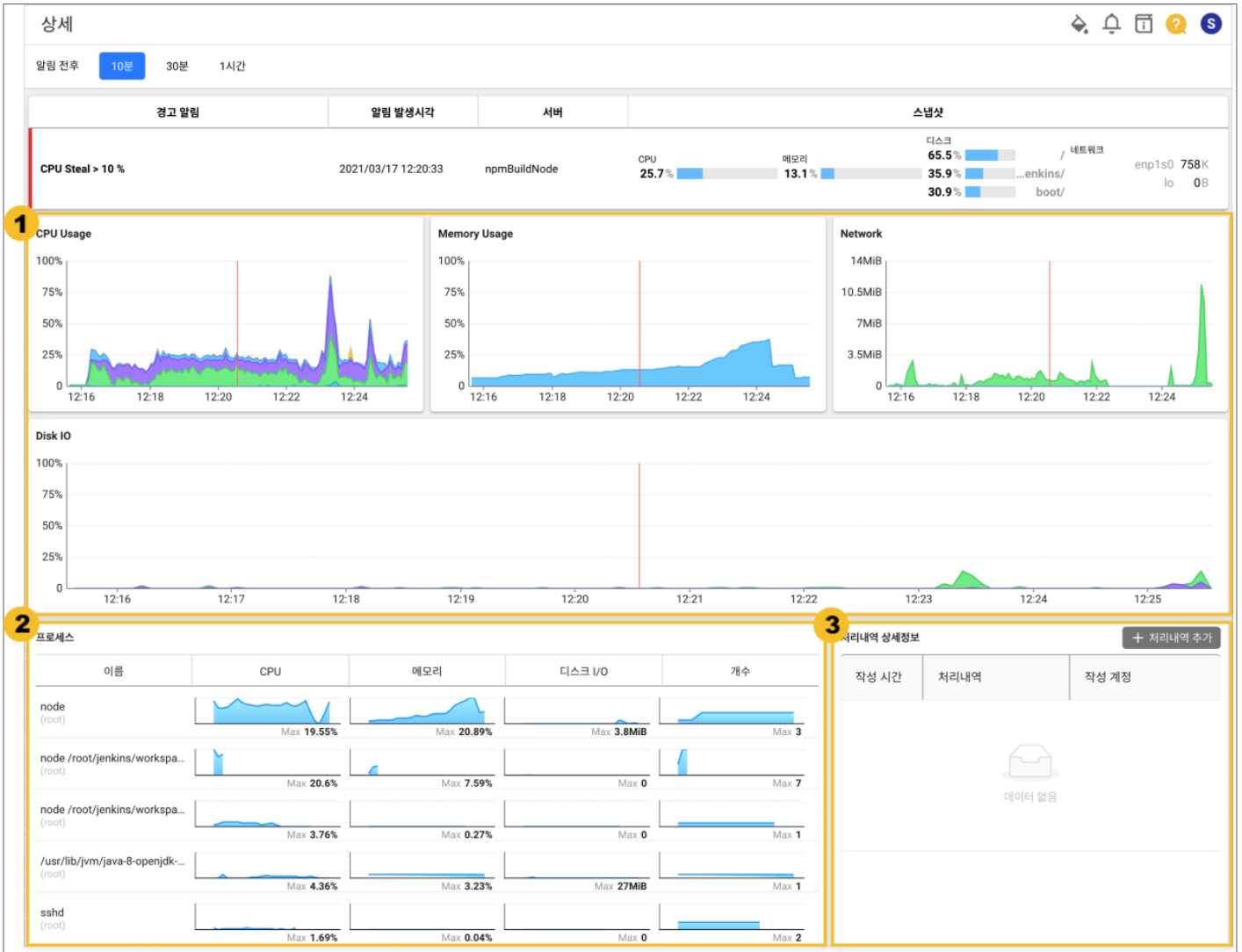
서버 이름입니다.

- [스냅샷](#)

발생한 이벤트에 대한 [CPU](#), [Memory Used](#), [디스크](#), [네트워크](#)에 대한 스냅샷 정보입니다.

이벤트 상세 정보

이벤트 기록 목록에서 해당 [이벤트 이름](#)을 선택하면 이벤트 발생 전후 5분간의 [상세](#) 정보로 이동합니다.



• 1 차트 위젯

알람 발생 전후 5분간의 CPU, Memory Usage, Disk I/O, Network 차트를 보여줍니다. 이벤트에 해당하는 부분의 위험도를 색깔로 표시합니다.

• 2 프로세스

이벤트에 해당하는 프로세스 상위 10개 정보를 조회할 수 있습니다.

• 3 처리 내역 상세 정보

이벤트에 대한 처리 내역을 조회할 수 있습니다. 처리 내역 추가 버튼을 선택하면 내역을 작성하고 저장할 수 있습니다.

이벤트 수신 포맷

서버 알림 템플릿

서버 모니터링은 예외적으로 알림 템플릿이 다릅니다.

- Product Type : 서버
- Event Type : 서버 알림, 프로세스 알림, 로그 파일 / 윈도우 이벤트 알림
- Event Channel : SMS, Mobile, 3rd party plugin , Plugin

이벤트 제목

Event title format

[Level][INFRA] ProjectName ServerName EventTitle

Event title example

[Info][INFRA] 서버 프로젝트 TC-0-1-8081 CPU Used > 70%

ⓘ ServerName이 지정되지 않은 경우 이벤트 제목에서 생략됩니다.

이벤트 메시지

이벤트 메시지에 포함될 수 있는 정보입니다. `optional` 이 `false` 인 경우 항상 메시지에 포함됩니다. `optional` 이 `true` 인 경우 해당 데이터를 확인할 수 있으면 보여줍니다.

Event message example

Project Name : 애플리케이션 프로젝트
Project Code : 3
Server Name : TC-0-1-8081

```

Event Message : [TEST] RECOVERED: Memory is too high. less than 10%
Event ON Time : 2022-04-12 18:53:24 +0900
Event OFF Time : 2022-04-12 18:53:24 +0900
Alert Type :
Metric Name : memory
Metric Value : 20
Metric Threshold : 10
Stateful : true

```

다음은 이벤트 메시지 구성 요소입니다.

En	Ko	Optional	설명
Project Name	프로젝트 이름	false	-
Project Code	프로젝트 Code	false	-
Server Name	에이전트 이름	true	oname
Event Message	이벤트 메시지	false	-
Event ON Time	이벤트 발생 시간	false	2022-04-13 10:40:49 +0900에서 +0900는 GMT를 의미합니다.
Event OFF Time	이벤트 해제 시간	true	2022-04-13 10:40:49 +0900에서 +0900는 GMT를 의미합니다.
Elapsed Time	이벤트 발생 지속 시간	true	-
Alert Type	이벤트 종류	true	-
Policy Name	알림 정책 이름	true	-
Metric Name	메트릭스 이름	true	이벤트 조건 판단에서 사용하는 메트릭스의 이름입니다.
Metric Value	메트릭스 값	true	메트릭스 값이 메트릭스 임계치를 넘으면 이벤트 발생 조건이 만족한 경우입니다.

En	Ko	Optional	설명
Metric Threshold	메트릭스 임계치	true	메트릭스 값이 메트릭스 임계치를 넘으면 이벤트 발생 조건이 만족한 경우입니다.
Event Rule	이벤트 발생 조건	true	-
Alert Type	이벤트 종류	true	이벤트 종류를 특정하기 위한 필드입니다.
Event Target Filter	이벤트 대상 선택	true	(메트릭스 알림) 특정 대상에서 수집된 메트릭스에 대해서만 이벤트 조건을 확인합니다.
Stateful	해결된 이벤트 알림	true	해결된 이벤트 알림 기능 사용 중이면 true, 아니면 false
Repeat Count	이벤트 반복 횟수	true	(메트릭스 알림) 이벤트 조건이 이벤트 반복 시간동안 이벤트 반복 횟수만큼 만족해야 이벤트가 발생합니다.
Repeat Duration	이벤트 반복 시간	true	(메트릭스 알림) 이벤트 조건이 이벤트 반복 시간동안 이벤트 반복 횟수만큼 만족해야 이벤트가 발생합니다. 해결된 이벤트 알림입니다.
IP	IP	true	-
Log Content	Log Content	true	-
Log Source	Log Source	true	-
CPU	CPU	true	-
CPU_load1	CPU_load1	true	-
CPU_loadPerCore	CPU_load1	true	-
Memory	Memory	true	-

En	Ko	Optional	설명
Swap	Swap	true	-
Disk Name / Used Percent / Free Size / IO Percent	Disk Name / Used Percent / Free Size / IO Percent	true	-
Traffic Name / Bps / Pps	Name / Bps / Pps	true	-
Acknowledge Message / Time / Name	Acknowledge Message / Time / Name	true	-

서버 알림 제목과 메시지

서버 알림은 Event Title 없이 Event Message만 제공됩니다.

서버 알림

Event Type	Event Level	Event Message	Event Off Message
재시작	Critical	System Rebooted"	미지원
미수신	Warning	Agent No Data"	미지원
포트	Warning	Port \${port} is down"	"Port \${port} is up"
포트(IP를 알 수 있는 경우)	Warning	IP \${ip} Port \${port} is down"	"IP \${ip} Port \${port} is up"
네트워크 IOPS	Warning or Critical	NETWORK \${deviceId} pps > \${value} pps"	-

Event Type	Event Level	Event Message	Event Off Message
네트워크 BPS	Warning or Critical	NETWORK \${deviceId} bps > \${value} ps"	-
디스크 I/O	Warning or Critical	Disk \${mountPoint} IO Usage > \${value} %"	-
디스크 사용량	Warning or Critical	Disk \${mountPoint} Used > \${value} %"	-
inode	Warning or Critical	Disk \${mountPoint} inode usage > \${value} %"	-
CPU	Warning or Critical	CPU Used > \${value} %"	-
메모리	Warning or Critical	Memory Used > \${value} %"	-
steal	Warning or Critical	CPU Steal > \${value} %"	-
스왑	Warning or Critical	Swap Used > \${value} %"	-

프로세스 알림

Event Type	Event Level	Event Message	Event Off Message
프로세스 수 경고	Warning or Critical	Process \${processName} Count >= \${value}"	"Process \${groupName} Count < \${value}"
프로세스 수 위험	Warning or Critical	Process \${processName} Count < \${value}"	"Process \${groupName} Count >= \${value}"

Event Type	Event Level	Event Message	Event Off Message
프로세스 CPU	Warning or Critical	Process \${processName} CPU > \${value}"	-
프로세스 메모리	Warning or Critical	Process \${processName} Memory > \${value}"	-

로그 파일과 윈도우 이벤트

Event Type	Event Level	Event Message	Event Off Message
Event Type	Event Level	Event Message	Event Off Message
LOG_DEFAULT	Warning or Critical	LOG \${logContent}"	-
LOG_FILE	Warning or Critical	LOG File: \${filePath}, Keyword : \${keyword}, [Event] \${logContent}"	-
LOG_WINDOW_EVENT	Warning or Critical	LOG \${logContent}"	-
LOG_AUDIT	Warning or Critical	AUDIT \${logContent}"	-
LOG_SCRIPT	Warning or Critical	SCRIPT \${logContent}"	-

Log 모니터링

로그는 애플리케이션 및 시스템에서 발생하는 이벤트와 메시지 등을 기록한 파일입니다. 이상 징후를 파악해 시스템 악화를 막거나 발생한 장애의 원인을 이해하고자 한다면 로그를 확인하는 것이 중요합니다.

현대 IT 서비스 구축 환경은 MSA 또는 Kubernetes 환경으로 변화하고 있는 추세이며 이로 인해 관리 대상이 증가하고 있습니다. 일반적인 로그 모니터링은 서버에 접속해 `tail` 명령어나 편집기를 통해 확인합니다. 하지만 이러한 환경에서는 개별 서버에 일일이 접속하는 등의 단순한 방법을 사용하기 어렵습니다. 경우에 따라 수백 또는 수천 대의 서버에서 발생하는 로그를 어떻게 확인할 수 있을까요?

와탭 로그 모니터링 서비스를 통해 수많은 로그를 보다 쉽게 관리할 수 있습니다.

❗ 리눅스 `tail` 명령어는 시간에 따라 내용이 추가되는 로그 등을 확인하기 위한 용도로 많이 사용됩니다.

주요 특징점

• 중앙 통합 관리

와탭은 대량의 로그를 중앙에서 통합 관리할 수 있습니다. 개별 서버에 접근하지 않고 중앙에서 로그의 내용을 확인할 수 있어 편리합니다.

• 모든 로그 수집

로그를 선별해서 수집하는 경우 중요한 데이터가 누락될 수 있습니다. 와탭은 모든 로그를 수집합니다. 이렇게 수집되는 로그들은 [라이브 테일](#) 메뉴를 통해 실시간으로 확인할 수 있습니다.

• 가시성 확보

와탭이 제공하는 다양한 차트에서 로그를 확인할 수 있습니다. 이를 통해 가시성을 확보해 에러 및 이슈 정보에 대한 접근성을 높이고 장애 상황을 조기에 감지할 수 있게 합니다.

• 유연한 용량 관리

개별 서버에 로그 적재 시 로그로 인해 파일 시스템 용량이 과도하게 점유되는 문제가 발생할 수 있습니다. 하지만 와탭을 통해 로그를 중앙에 모은다면 개별 서버에서 발생하는 로그 파일을 유지할 필요 없이 중앙에 적재된 로그 데이터의 유지 기간만 관리하면 됩니다.

• 다양한 분석 관점

장애 상황을 파악하고 예측하기 위해서는 다양한 관점으로 로그를 분석할 수 있어야 합니다. 와탭은 특정 태그가 포함된 로그의 건수 추이 또는 특정 태그가 포함된 로그만 필터링해 확인할 수 있습니다. 자주 사용하는 패턴이라면 차트로 저장해 언제든지 조회할 수

있도록 설정할 수 있습니다.

- **패턴 알림**

장애의 패턴을 파악했다면 이를 알림으로 설정해 문제를 예방하거나 최대한 빠르게 인지할 수 있습니다. 와탭은 개별 로그를 기준으로 특정 키워드가 포함되면 알림을 받는 [실시간 로그 알림](#)과 특정 태그가 포함된 로그의 건수 추이를 기준으로 알림을 받는 [복합 로그 알림](#)을 제공합니다.

로그 분석

라이브 테일

[라이브 테일](#) 메뉴를 통해 실시간으로 수집된 로그는 `tail` 명령어를 사용한 것과 마찬가지로 화면을 통해 흘러가는 로그를 조회할 수 있습니다. [라이브 테일](#)에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

로그 트렌드

[로그 트렌드](#) 메뉴를 통해 수집되는 전체 로그 또는 특정 태그가 포함된 로그의 건수 추이를 확인할 수 있습니다. 로그 발생 건수가 장애 발생 및 해소 시점과 밀접한 연관을 가진 경우, 로그 발생 건수 추이를 통해 장애의 원인 분석과 대응이 빨라질 수 있습니다. [로그 트렌드](#)에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

로그 검색

[로그 검색](#) 메뉴를 통해 수집되는 전체 로그 또는 특정 태그가 포함된 로그를 조회할 수 있습니다. 특정 시간대 또는 특정 서버에서 발생한 로그를 태그를 기준으로 조회하고 확인할 수 있습니다. 선택한 로그의 앞뒤에 발생한 로그를 확인하는 인접 로그 기능은 특정 Error 또는 Exception이 발생한 전후 상황 파악 시 활용할 수 있습니다. [로그 검색](#)에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

로그 모니터링 적용하기

와탭 로그 모니터링 서비스 이용을 위한 기본 적용 방법을 안내합니다. 와탭 로그 모니터링은 추가적인 에이전트를 구성하거나 로그에 맞추어 parser를 적용할 필요가 없습니다. 간단한 설정으로 빠르게 시작할 수 있습니다.

로그 모니터링의 작동 원리



일반적인 로그 통합 서비스는 수집기, 처리기, 저장소 그리고 UI 모듈로 이루어져 있습니다. 단계별 설정과 구성 작업을 필요로 하기에 각각의 모듈을 구축하는 과정이 번거로우며 추가 비용이 발생합니다.

와탭 로그 모니터링은 적용이 간단합니다. 기존의 모니터링 에이전트가 수집기 역할을 하기에 에이전트 옵션을 켜는 것만으로 로그 모니터링을 시작할 수 있습니다.

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

- 출력된 파일에서 로그를 읽지 않고 Java 애플리케이션의 로그 라이브러리로 전달되는 로그를 직접 수집합니다.
- 로그를 직접 수집하기 때문에 파일 I/O를 유발하지 않아 시스템에 미치는 성능 영향이 매우 낮습니다.
- 트랜잭션 트레이스와 로그의 연결 추적성을 확보하여 트레이스에서 로그를 확인할 수 있습니다.

❗ Java 로그 라이브러리

대표적인 Java 로그 라이브러리는 Apache Log4j, Logback 입니다.

❗ Java Agent 2.1.1 버전부터 사용할 수 있습니다.

- 기존의 에이전트에 로그 수집 기능을 추가했습니다. 모니터링 에이전트가 로그 파일에 추가로 출력된 로그를 읽어 수집하는 방식을 활용합니다.

❗ PHP Agent 2.3.2 버전부터 사용할 수 있습니다.

- 기존의 에이전트에 로그 수집 기능을 추가했습니다. 모니터링 에이전트가 로그 파일에 추가로 출력된 로그를 읽어 수집하는 방식을 활용합니다.
- 로그에 트랜잭션 ID를 출력하면, 트랜잭션 트레이스와 로그의 연결 추적성을 확보하여 트레이스에서 로그를 확인할 수 있습니다.

❗ Python Agent 1.2.2 버전부터 사용할 수 있습니다.

- 기존의 에이전트에 로그 수집 기능을 추가했습니다. 모니터링 에이전트가 로그 파일에 추가로 출력된 로그를 읽어 수집하는 방식을 활용합니다.
- 기존의 에이전트에 로그 수집 기능을 추가했습니다. 모니터링 에이전트가 로그 파일에 추가로 출력된 로그를 읽어 수집하는 방식을 활용합니다.

❗ Server Agent 2.1.2 버전부터 사용할 수 있습니다.

- 쿠버네티스 컨테이너에 로그를 수집할 수 있습니다.

- 쿠버네티스 컨테이너 내부 애플리케이션의 로그를 수집할 수 있습니다.

 Kubernetes Agent 1.1.35 버전부터 사용할 수 있습니다.

로그 모니터링 적용하기

사용하는 애플리케이션에 따른 적용 방법을 다음과 같이 제공합니다. 로그 모니터링을 적용하기 전에 [지원 버전](#)을 먼저 확인하세요.

1. 지원하는 에이전트 버전을 확인하고 **업데이트**하세요.
2. 로그 모니터링 **옵션**을 설정하세요.
3. 로그 모니터링을 **활성화**하세요.

Java

Java 애플리케이션에서 로그를 수집하는 방법을 안내합니다.

PHP

PHP 애플리케이션에서 로그를 수집하는 방법을 안내합니다.

Python

Python 애플리케이션에서 로그를 수집하는 방법을 안내합니다.

Go

Go 애플리케이션에서 로그를 수집하는 방법을 안내합니다.

Server

Server 애플리케이션에서 로그를 수집하는 방법을 안내합니다.

Kubernetes

쿠버네티스 컨테이너와 컨테이너 내부 애플리케이션의 로그를 수집하는 방법을 안내합니다.

Java

자바 애플리케이션에서 로그를 수집하려면 다음 3단계를 모두 완료해야 합니다.

에이전트 업데이트

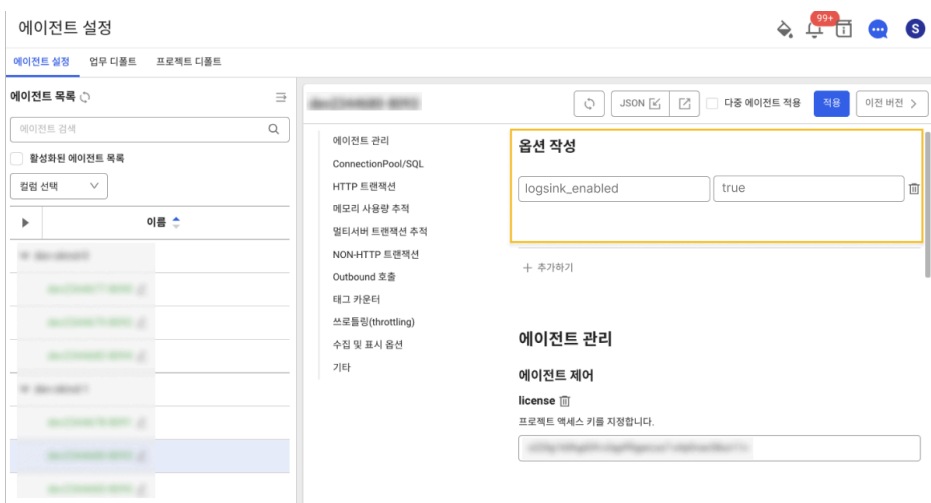
자바 에이전트 2.1.1 버전부터 가능합니다. 업데이트 방법은 [다음 문서](#)를 참조하세요.

에이전트 설정 확인

홈 화면 > 프로젝트 선택 > [로그](#) > [로그 설정](#)

와탭 모니터링 서비스 초기 화면에서 프로젝트를 선택한 다음 프로젝트 메뉴 하위에 [로그](#) > [로그 설정](#) 메뉴를 선택하세요. [로그 모니터링 시작하기](#) 섹션의 [에이전트 설정 확인](#) 탭의 안내를 참조해 진행하세요.

1. 프로젝트 메뉴 하위에 [관리](#) > [에이전트 설정](#) 메뉴를 선택하세요.
2. [옵션 작성](#) 탭에서 [직접 입력](#)을 선택하세요. 입력창에 다음과 같이 `logsink_enabled=true` 옵션을 추가하세요.



3. 로그 모니터링을 적용하기 위해 애플리케이션을 다시 시작하세요.

주요 옵션

- `hooklog_enabled` **Boolean**

기본값 `false`

Log 라이브러리를 hooking 하여 로그 모니터링을 활성화합니다.

! 애플리케이션 실행 전에 [whatap.conf](#)에 본 옵션이 활성화되어 있어야 이후 로그 모니터링의 On/Off를 `logsink_enabled` 설정을 통해 동적으로 제어할 수 있습니다. 애플리케이션 실행 전에 `logsink_enabled` 옵션이 `true`로 설정된 경우 본 옵션을 별도로 설정하지 않아도 로그 모니터링이 가능합니다.

! 앞으로 로그 모니터링을 활용할 가능성이 있다면 사전에 본 옵션을 꼭 설정할 것을 권장합니다.

• hooklog_custom_methods

사용자 정의 로그를 등록합니다. 임의의 로그 프레임워크 내용을 전달합니다. 사이트에서 개별로 만든 로그 모듈의 로그를 추적할 때 사용하세요.

Java

```
package io.home.test;

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

whatap.conf

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

• logsink_enabled Boolean

기본값 `false`

Log 모니터링 기능을 On/Off 합니다.

! 애플리케이션 실행 전에 [whatap.conf](#)에 `hooklog_enabled` 옵션이 설정되어 있으면 본 옵션을 통해 로그 모니터링의 On/Off를 동적으로 제어할 수 있습니다.

• logsink_trace_enabled Boolean

기본값 `false`

Log에 트랜잭션 ID를 삽입하여, 트랜잭션 트레이스의 로그 탭을 노출할지 여부를 지정합니다.

로그 모니터링 활성화

홈 화면 > 프로젝트 선택 > 로그 > 로그 설정

로그 모니터링 시작하기 섹션의 로그 모니터링 활성화 탭에서 토글 버튼으로 와탭 로그 모니터링을 활성화 또는 비활성화 할 수 있습니다.

에이전트 설정 및 로그 모니터링 활성화 ⓘ
요금제 보기

라이브 테일, 로그 트렌드 기능으로 애플리케이션의 흠어진 로그를 한 눈에 확인하실 수 있습니다.

- ▶ 1. 에이전트 설정 확인
- ▼ 2. 로그 모니터링 활성화

시작일 : 2022년 6월 13일 | 2022년 6월 28일부터 이용 요금이 청구됩니다.

- 토글 버튼을 켜면 로그 모니터링이 활성화됩니다. 활성화한 날부터 15일 동안 무료로 체험하실 수 있습니다.
- 토글 버튼을 끄면 로그 모니터링이 비활성화됩니다. 로그를 더 이상 저장하지 않습니다.

ⓘ 권한

에이전트 설치 후 프로젝트에 대한 수정 권한이 있는 경우에만 로그 모니터링을 활성화할 수 있습니다. 권한에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

PHP

PHP 애플리케이션에서 로그를 수집하려면 다음을 확인하세요.

에이전트 업데이트

PHP 에이전트 2.3.2 버전부터 가능합니다. 업데이트 방법은 [다음 문서](#)를 참조하세요.

에이전트 설정 확인

홈 화면 > 프로젝트 선택 > [로그](#) > [로그 설정](#)

와탭 모니터링 서비스 초기 화면에서 프로젝트를 선택한 다음 프로젝트 메뉴 하위에 [로그](#) > [로그 설정](#) 메뉴를 선택하세요. [로그 모니터링 시작하기](#) 섹션의 [에이전트 설정 확인](#) 탭의 안내를 참조해 진행하세요.

설정 파일 경로 확인

로그 모니터링을 원하는 파일의 [설정 파일 경로](#)를 확인하세요. CLI 환경에서 확인하거나 웹에서 확인할 수 있습니다.

CLI 환경에서 확인하기

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

ⓘ 해당 경로가 "(None)"인 경우 설정 파일의 경로는 [/usr/whatap/php](#) 입니다.

웹에서 확인하기

CLI 환경과 Apache 환경의 PHP 설정이 다르면 웹에서 `phpinfo()` 함수의 결과 내용을 확인하세요.

PHP Version 8.0.12



System	Linux cent6default.com 2.6.32-754.35.1.el6.x86_64 #1 SMP Sat Nov 7 12:42:14 UTC 2020 x86_64
Build Date	Oct 26 2021 16:35:28
Build System	Linux cent6default.com 2.6.32-754.35.1.el6.x86_64 #1 SMP Sat Nov 7 12:42:14 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
Configure Command	'./configure' '--prefix=/usr/php8.0.12' '--bindir=/usr/bin' '--with-config-file-path=/etc/php8.0.12' '--program-prefix=' '--program-suffix=8.0.12' '--with-config-file-scan-dir=/etc/php8.0.d' '--with-libdir=lib64' '--with-apxs2' '--enable-fpm' '--with-curl' '--with-iconv' '--with-pdo-mysql' '--with-mysqli' '--with-pdo-oci' '--with-oci8' '--without-pgsql' '--without-pdo-pgsql' '--with-openssl' '--with-mhash' '--with-xsl' '--with-libxml' '--enable-sockets' '--enable-syssem' '--enable-sysshm' '--enable-soap' '--enable-gd' '--without-sqlite3' '--without-pdo-sqlite' 'PKG_CONFIG_PATH=/usr/local/lib/pkgconfig'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php8.0.12
Loaded Configuration File	(none)
Scan this dir for additional .ini files	/etc/php8.0.d

명령어 입력


설정 파일 경로를 포함한 명령어를 입력하면 로그 모니터링이 시작됩니다.

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

로그 모니터링 활성화

홈 화면 > 프로젝트 선택 > 로그 > 로그 설정

로그 모니터링 시작하기 섹션의 로그 모니터링 활성화 탭에서 토글 버튼으로 와탭 로그 모니터링을 활성화 또는 비활성화 할 수 있습니다.

에이전트 설정 및 로그 모니터링 활성화 

요금제 보기



라이브 테일, 로그 트렌드 기능으로 애플리케이션의 흠어진 로그를 한 눈에 확인하실 수 있습니다.


▶ 1. 에이전트 설정 확인

▼ 2. 로그 모니터링 활성화



시작일 : 2022년 6월 13일 | 2022년 6월 28일부터 이용 요금이 청구됩니다.

-  토글 버튼을 켜면 로그 모니터링이 활성화됩니다. 활성화한 날부터 15일 동안 무료로 체험하실 수 있습니다.
-  토글 버튼을 끄면 로그 모니터링이 비활성화됩니다. 로그를 더 이상 저장하지 않습니다.

 권한

에이전트 설치 후 프로젝트에 대한 **수정 권한**이 있는 경우에만 로그 모니터링을 활성화할 수 있습니다. 권한에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

Python

Python 애플리케이션에서 로그를 수집하려면 다음을 확인하세요.

에이전트 업데이트

Python 에이전트 1.2.2 버전부터 가능합니다. 업데이트 방법은 [다음 문서](#)를 참조하세요.

에이전트 설정 확인

홈 화면 > 프로젝트 선택 > [로그](#) > [로그 설정](#)

와탭 모니터링 서비스 초기 화면에서 프로젝트를 선택한 다음 프로젝트 메뉴 하위에 [로그](#) > [로그 설정](#) 메뉴를 선택하세요. [로그 모니터링 시작하기](#) 섹션의 [에이전트 설정 확인](#) 탭의 안내를 참조해 진행하세요.

로그 수집 활성화

설정 파일 경로(WHATAP_HOME)를 포함한 명령어를 입력하면 로그 수집이 바로 시작됩니다.

```
export LOGFILES={로그파일전체경로},...
echo "logsink_enabled=true" | sudo tee -a {설정파일경로}/whatap.conf
echo "logsink.files=$LOGFILES" | sudo tee -a {설정파일경로}/whatap.conf
```

로그와 웹 트랜잭션 연동

1.3.6 이후 버전

1.3.6 버전부터 다음의 방법으로 트랜잭션과 로그 연동을 설정할 수 있습니다. 현재 와탭은 Python의 logging, loguru 라이브러리를 지원하고 있습니다. 사용하는 Python Log 라이브러리에 따라 [whatap.conf](#)를 구성하세요.

- logging 모듈

```
logging
```

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

- loguru 모듈

```
loguru
```

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

1.3.6 미만 버전

트랜잭션 별로 발생한 로그를 별도로 조회 가능하도록 트랜잭션 아이디 `{txid}` 를 로그에 출력합니다. 와탭 모니터링에서는 Python LogRecord에 `{txid}` 를 자동 주입하여 포매터 설정 시 로그 파일에 `{txid}` 를 출력할 수 있도록 합니다.

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

try:
import whatap.trace.mod.logging as whatap_logging
if whatap_logging.logging_injection_processed:
    LOGGING['formatters']['whatap.formatter']={
        '(): 'django.utils.log.ServerFormatter',
        'format': '[{server_time}] -- {{ "@txid" : "{txid}" }} -- {message}',
```

```

        'style': '{',
    }
    LOGGING['handlers']['whatap']={
        'level': 'DEBUG',
        'class': 'logging.handlers.RotatingFileHandler',
        'filename': os.path.join(BASE_DIR, 'logs','whatap_log.log'),
        'formatter': 'whatap.formatter',
    }
    LOGGING['loggers'][{로거이름}]['handlers'].append('whatap')
except:
    pass
...

```

로그 모니터링 활성화

홈 화면 > 프로젝트 선택 > [로그](#) > [로그 설정](#)

[로그 모니터링 시작하기](#) 섹션의 [로그 모니터링 활성화](#) 탭에서 토글 버튼으로 와탭 로그 모니터링을 활성화 또는 비활성화 할 수 있습니다.

에이전트 설정 및 로그 모니터링 활성화 ⓘ
요금제 보기

라이브 테일, 로그 트렌드 기능으로 애플리케이션의 출어진 로그를 한 눈에 확인하실 수 있습니다.

- ▶ 1. 에이전트 설정 확인
- ▼ 2. 로그 모니터링 활성화

시작일 : 2022년 6월 13일 | 2022년 6월 28일부터 이용 요금이 청구됩니다.

- 토글 버튼을 켜면 로그 모니터링이 활성화됩니다. 활성화한 날부터 15일 동안 무료로 체험하실 수 있습니다.
- 토글 버튼을 끄면 로그 모니터링이 비활성화됩니다. 로그를 더 이상 저장하지 않습니다.

ⓘ 권한

에이전트 설치 후 프로젝트에 대한 **수정 권한**이 있는 경우에만 로그 모니터링을 활성화할 수 있습니다. 권한에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

Go

Go 애플리케이션에서 로그를 수집하려면 다음을 확인하세요.

에이전트 설정 확인

홈 화면 > 프로젝트 선택 > 로그 > 로그 설정

와탭 모니터링 서비스 초기 화면에서 프로젝트를 선택한 다음 프로젝트 메뉴 하위에 [로그](#) > [로그 설정](#) 메뉴를 선택하세요. [로그 모니터링 시작하기](#) 섹션의 [에이전트 설정 확인](#) 탭의 안내를 참조해 진행하세요.

로그 수집 활성화

다음 명령어를 입력하면 로그 수집이 바로 시작됩니다.

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

로그 모니터링 활성화

홈 화면 > 프로젝트 선택 > 로그 > 로그 설정

[로그 모니터링 시작하기](#) 섹션의 [로그 모니터링 활성화](#) 탭에서 토글 버튼으로 와탭 로그 모니터링을 활성화 또는 비활성화 할 수 있습니다.

에이전트 설정 및 로그 모니터링 활성화 ⓘ
요금제 보기

라이브 테일, 로그 트렌드 기능으로 애플리케이션의 흩어진 로그를 한 눈에 확인하실 수 있습니다.

- ▶ 1. 에이전트 설정 확인
- ▼ 2. 로그 모니터링 활성화

시작일 : 2022년 6월 13일 | 2022년 6월 28일부터 이용 요금이 청구됩니다.

- 토글 버튼을 켜면 로그 모니터링이 활성화됩니다. 활성화한 날부터 15일 동안 무료로 체험하실 수 있습니다.
- 토글 버튼을 끄면 로그 모니터링이 비활성화됩니다. 로그를 더 이상 저장하지 않습니다.

ⓘ 권한

에이전트 설치 후 프로젝트에 대한 **수정 권한**이 있는 경우에만 로그 모니터링을 활성화할 수 있습니다. 권한에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

Server

서버 애플리케이션에서 로그를 수집하려면 다음을 확인하세요.

에이전트 업데이트

서버 에이전트 2.1.2 버전부터 가능합니다. 업데이트 방법은 [다음 문서](#)를 참조하세요.

에이전트 설정 확인

홈 화면 > 프로젝트 선택 > [로그](#) > [로그 설정](#)

와탭 모니터링 서비스 초기 화면에서 프로젝트를 선택한 다음 프로젝트 메뉴 하위에 [로그](#) > [로그 설정](#) 메뉴를 선택하세요. [에이전트 설정 확인](#) 탭 상단의 OS 선택 탭에서 서버 OS([리눅스\(shell\)](#), [윈도우\(Powershell\)](#))를 선택하세요. [기본 설치](#) 또는 [카테고리와 함께 설치](#)를 참조해 진행하세요.

ⓘ 다음 설정은 에이전트 재시작이 필요합니다.

Linux Shell

- [기본 설치](#)

Linux Shell

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

- [카테고리와 함께 설치](#)

Linux Shell

```
1 cd /usr/whatap/infra
2 sudo mkdir extension
3
```

```

4 cat >extension/logsink.conf<<EOL
5 [[inputs.logsink]]
6   category = "serverlog"
7   ## 로그 발생량 통계 별도 데이터로 전송 여부
8   stats_enabled = true
9   ## 로그 발생량 통계 카테고리
10  stats_category = "logsink_stats"
11  ## 로그 파일 경로(path)에 별표(*)가 포함되어 제외할 로그 비대상 파일명 설정
12  excludeNames = [ ".gz", ".zip" ]
13  [[inputs.logsink.file]]
14  ## 로그 파일 지정 시, 날짜 패턴(strftime.org) 지정 가능
15  path = "/some/path/%Y-%m-%d/.log"
16  disabled = false
17  encoding = "euc-kr"
18
19  [[inputs.logsink.file]]
20  path = "/some/other/log"
21  disabled = false
22  encoding = "utf-8"
23
24  [[inputs.logsink.file]]
25  ## 줄 단위 로그에서 해당 키워드 검색 시, 이전 로그에 병합
26  nowrap_keywords = ["Caused by:", "Test"]
27 EOL
28
29 sudo service whatap-infra restart

```

Windows Powershell

- 기본 설치

Windows Powershell

```

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

```

- 카테고리와 함께 설치

Windows Powershell

```

1 # 관리자 권한 필요
2 New-Item -type "Directory" -Path "C:\Program Files\WhatapInfra\extension"
3
4 $contentToAdd = @"
5 [[inputs.logsink]]
6 category = "serverlog"
7 ## 로그 발생량 통계 별도 데이터로 전송 여부
8 stats_enabled = true
9 ## 로그 발생량 통계 카테고리
10 stats_category = "logsink_stats"
11 ## 로그 파일 경로(path)에 별표(*)가 포함되어 제외할 로그 비대상 파일명 설정
12 excludeNames = [ ".gz", ".zip" ]
13 [[inputs.logsink.file]]
14 ## 로그 파일 지정 시, 날짜 패턴(strftime.org) 지정 가능
15 path = "c:\whatap\logs%Y-%m-%d_.log"
16 disabled = false
17 encoding = "euc-kr"
18
19 [[inputs.logsink.file]]
20 ## 줄 단위 로그에서 해당 키워드 검색 시, 이전 로그에 병합
21 nowrap_keywords = ["Caused by:", "Test"]
22
23 "@
24
25 New-Item -path "C:\Program Files\WhatapInfra\extension" -name "logsink.conf" -type "file" -value $contentToAdd -Force
26
27 Restart-Service "Whatap Infra"

```

옵션 설정

- `stats_enabled` : 수집 현황 데이터의 수집 여부를 설정합니다. 기본값은 `false` 입니다. 값을 `true` 로 설정해야 합니다. `true` 로 설정하면 다음 `stats_category` 에서 설정한 카테고리(`logsink_stats`)로 통계 데이터가 발생합니다.
- `stats_category` : 수집 현황 데이터를 저장할 매트릭스 카테고리를 설정합니다. 값을 `logsink_stats` 로 설정해야 합니다. 통계 데이터 필드는 다음과 같습니다.
 - `file`
 - `checkInterval`
 - `encoding`
 - `filepos`

- `checkedLocalTime`
 - `lastupdatedLocalTime`
 - `fileSize`
 - `error`
 - `firstCheck`
 - `transferBytes`
- `excludeNames`: 로그 파일 경로(path)에 별표(*)를 포함한 경우 로그 비대상 파일을 제외하도록 파일명을 설정할 수 있습니다. 쉼표(,)를 구분자로 이용해 복수 설정할 수 있습니다.

Example

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

- `nowrap_keywords`: 줄 단위 로그 검색 시 해당 옵션값으로 지정한 키워드가 검색될 경우 이전 로그에 병합합니다.

윈도우 이벤트 로그 옵션 설정

윈도우 이벤트 로그 수집 시 다음과 같이 옵션을 설정할 수 있습니다.

```
# 관리자 권한 필요
New-Item -type "Directory" -Path "C:\Program Files\WhatapInfra\extension"

$contentToAdd = @"
[[inputs.win_eventlog]]
  category = "win_event_log"
  stats_category = "win_event_log_stats"
  stats_enabled = true
  enabled = true
[[inputs.win_eventlog.file]]
  #true | false
  enabled = true
  # Application, Security, Setup, System, Forwarded
  file = "Application"
  #1: Information, 2: Warning 3: Critical 4: Audit Success 5 Audit Fail
  #event_type =
  #event_id =
  #event_id =
  #event source name
```

```
#source_name = ""

"@
New-Item -path "C:\Program Files\WhatapInfra\extension" -name "win_eventlog.conf" -type "file" -value $contentToAdd -Force
Restart-Service "Whatap Infra"
```

- ❗ • 지원 버전 2.5.2
- 운영체제: Windows

- 카테고리 지정(`category`) 필수
 - | 예, `win_event_log`
- 통계 카테고리 지정(`stats_category`) 필수
 - | 예, `win_event_log_stats`
- 통계 카테고리 On/Off(`stats_enabled`) 필수
 - | 예, `true` 혹은 `false`
- 수집 기능 On/Off(`enabled`) 필수
 - | 예, `true` 혹은 `false`
- 파일별 수집 기능 On/Off(`enabled`) 필수
 - | 예, `true` 혹은 `false`
- 파일(`file`) 필수
 - | 예, `Application` , `Security` , `Setup` , `System` , `Forwarded`
- 이벤트 타입(`event_type`) 비필수
 - | 예, `1` , `2` , `3` , `4` , `5`

❗ 이벤트 타입

1. Information



2. Warning
3. Critical
4. Audit Success
5. Audit Fail

- 이벤트 아이디(`event_id`) 비필수
- 이벤트 소스 이름(`source_name`) 비필수

로그 모니터링 활성화

홈 화면 > 프로젝트 선택 > 로그 > 로그 설정

로그 모니터링 시작하기 섹션의 로그 모니터링 활성화 탭에서 토글 버튼으로 와탭 로그 모니터링을 활성화 또는 비활성화 할 수 있습니다.

에이전트 설정 및 로그 모니터링 활성화 ⓘ
요금제 보기

라이브 테일, 로그 트렌드 기능으로 애플리케이션의 흩어진 로그를 한 눈에 확인하실 수 있습니다.

- ▶ 1. 에이전트 설정 확인
- ▼ 2. 로그 모니터링 활성화

시작일 : 2022년 6월 13일 | 2022년 6월 28일부터 이용 요금이 청구됩니다.

- 토글 버튼을 켜면 로그 모니터링이 활성화됩니다. 활성화한 날부터 15일 동안 무료로 체험하실 수 있습니다.
- 토글 버튼을 끄면 로그 모니터링이 비활성화됩니다. 로그를 더 이상 저장하지 않습니다.

ⓘ 권한

에이전트 설치 후 프로젝트에 대한 수정 권한이 있는 경우에만 로그 모니터링을 활성화할 수 있습니다. 권한에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

Kubernetes

쿠버네티스 컨테이너와 컨테이너 내부 애플리케이션의 로그를 수집하려면 다음을 확인하세요.

에이전트 업데이트

쿠버네티스 에이전트 1.1.35 버전부터 가능합니다. 업데이트 방법은 [다음 문서](#)를 참조하세요.

에이전트 설정 확인

홈 화면 > 프로젝트 선택 > [로그](#) > [로그 설정](#)

와탭 모니터링 서비스 초기 화면에서 프로젝트를 선택한 다음 프로젝트 메뉴 하위에 [로그](#) > [로그 설정](#) 메뉴를 선택하세요. [에이전트 설정 및 로그 모니터링 활성화](#) 섹션의 [에이전트 설정 확인](#) 탭의 안내를 참조해 진행하세요.

컨테이너 로그 수집 활성화

CP K8S-JINS-PORTAL-DIST ▾ 로그 설정

[로그모니터링 시작하기](#) [로그 1차 파서 설정](#) [로그 2차 파서 설정](#) [빠른 인덱스 설정](#) [로그 장기 보관 통계](#) [로그 1시간 통계 위젯 데이터 설정](#)

에이전트 설정 및 로그 모니터링 활성화 ⓘ

라이브 테일, 로그 트렌드 기능으로 애플리케이션의 흩어진 로그를 한 눈에 확인하실 수 있습니다.

▼ 1. 에이전트 설정 확인

컨테이너 로그를 수집하려면 다음을 확인해주세요.

1. 노드 에이전트 버전 확인 및 업그레이드 (v1.1.35 이후 버전부터 가능)
2. 아래의 버튼을 클릭하여 쿠버네티스 노드 에이전트에 로그 설정(logsink_enabled=true)을 전체 적용합니다.

[로그 설정 적용하기](#)

쿠버네티스 컨테이너에 로그를 수집하려면 [에이전트 설정 확인](#) 탭에서 [로그 설정 적용하기](#) 버튼을 선택하세요.

컨테이너 내부 애플리케이션 로그 수집 활성화

Java 2.1.1, Python 1.2.2 버전부터 가능합니다. 쿠버네티스 컨테이너 상에서 실행되는 애플리케이션의 로그를 수집할 수 있도록 다음을 참조하세요.

The screenshot shows the '에이전트 설정' (Agent Settings) page. On the left, there is a sidebar with '에이전트 설정 및 로그 모니터링 활성화' (Activate Agent Settings and Log Monitoring) and '1. 에이전트 설정 확인' (Check Agent Settings). The main content area shows '에이전트 설정' (Agent Settings) with a '로그 설정 적용하기' (Apply Log Settings) button and a '복사' (Copy) button. Below that, there is a '2. 로그 모니터링 활성화' (Activate Log Monitoring) section. On the right, the '에이전트 설정' (Agent Settings) form is shown. It has a '노드' (Node) dropdown, a 'JSON' button, a '복사' (Copy) button, and a '적용' (Apply) button. Below that, there is a '옵션 작성' (Option Creation) section with a search bar and a '직접 입력' (Direct Input) option. The '직접 입력' (Direct Input) section has two input fields: '키를 입력해주세요.' (Please enter the key) and '값을 입력해주세요.' (Please enter the value).

1. 에이전트 설정 확인 탭 하단의 1. 에이전트 설정 버튼을 선택하세요.
2. 애플리케이션 에이전트 설정 메뉴로 이동 후 2. 옵션 작성 창에서 직접 입력을 선택하세요.
3. 다음의 에이전트 설정 명령어의 키 `logsink_enabled` 와 값 `true` 를 3. 입력창에 입력하세요.


```
logsink_enabled=true
```

4. **적용** 버튼을 선택하세요. 쿠버네티스 컨테이너 내 애플리케이션의 로그를 수집할 수 있습니다.

- Java 애플리케이션 로그 수집에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.
- Python 애플리케이션 로그 수집에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.
- Go 애플리케이션 로그 수집에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

로그 모니터링 활성화

홈 화면 > 프로젝트 선택 > [로그](#) > [로그 설정](#)

[로그 모니터링 시작하기](#) 섹션의 [로그 모니터링 활성화](#) 탭에서 토글 버튼으로 와탭 로그 모니터링을 활성화 또는 비활성화 할 수 있습니다.

에이전트 설정 및 로그 모니터링 활성화 요금제 보기

라이브 테일, 로그 트렌드 기능으로 애플리케이션의 흩어진 로그를 한 눈에 확인하실 수 있습니다.

▶ 1. 에이전트 설정 확인

▼ 2. 로그 모니터링 활성화

시작일 : 2022년 6월 13일 | 2022년 6월 28일부터 이용 요금이 청구됩니다.

- 토글 버튼을 켜면 로그 모니터링이 활성화됩니다. 활성화한 날부터 15일 동안 무료로 체험하실 수 있습니다.
- 토글 버튼을 끄면 로그 모니터링이 비활성화됩니다. 로그를 더 이상 저장하지 않습니다.

ⓘ 권한

에이전트 설치 후 프로젝트에 대한 **수정 권한**이 있는 경우에만 로그 모니터링을 활성화할 수 있습니다. 권한에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

쿠버네티스 로그 모니터링 카테고리 안내

쿠버네티스 관련 다양한 로그를 확인할 수 있습니다. 와탭 쿠버네티스에서 제공하는 모니터링 카테고리는 다음과 같습니다. 설정에 따라 중복된 로그 내용이 저장될 수 있으니 반드시 중복 여부를 확인하세요.

카테고리	설명
#K8sEvent	<ul style="list-style-type: none"> 쿠버네티스에서 발생하는 이벤트가 저장된 로그 사용자 설정과 무관하게 기본 생성
#WhatapEvent	<ul style="list-style-type: none"> 와탭 이벤트 설정에 의해 발생한 이벤트가 저장된 로그 사용자 설정과 무관하게 기본 생성
containerStdout	<ul style="list-style-type: none"> 컨테이너 Standard Out 로그 사용자 설정 시 생성 노드 에이전트에 <code>logsink_enabled=true</code> 설정 추가 시
AppLog	<ul style="list-style-type: none"> 컨테이너 내 애플리케이션 로그 사용자 설정 시 생성 애플리케이션 에이전트에 <code>logsink_enabled=true</code> 설정 추가 시

로그 설정

홈 화면 > 프로젝트 선택 > 로그 > 로그 설정

로그 설정 메뉴에서 로그 모니터링 관련 설정을 할 수 있습니다. 상단의 탭을 통해 에이전트 설정 확인, 로그 모니터링의 활성화 여부 결정, 로그 데이터의 유지 기간 및 조회 비밀번호 설정, 로그 파서 등록, 빠른 인덱스 설정 등의 메뉴를 사용할 수 있습니다.

- ① • 로그 모니터링 활성화 기능을 사용하려면 프로젝트 수정 권한이 필요합니다.
- 로그 편집 권한을 통해 로그 모니터링 활성화 기능 외 로그 설정 메뉴를 수정할 수 있습니다.

로그 모니터링 시작하기

로그 설정
🔍 🔔 📄 ? 📄

로그모니터링 시작하기
로그 1차 파서 설정
로그 2차 파서 설정
빠른 인덱스 설정
로그 장치 보관 통계

1 에이전트 설정 및 로그 모니터링 활성화 📄
요금제 보기

라이브 테일, 로그 트렌드 기능으로 애플리케이션의 흩어진 로그를 한 눈에 확인하실 수 있습니다.

- ▶ 1. 에이전트 설정 확인
- ▶ 2. 로그 모니터링 활성화

2 로그 모니터링 데이터 설정 📄
초기화
저장

로그 사용량 230,777,963라인

로그 조회 비밀번호 로그 조회 비밀번호를 사용하려면 켜주세요.

데이터 유지 기간 30일 ▼

카테고리별 데이터 유지 기간

카테고리	데이터 보관일	금일 로그수 ①	어제 로그수 ①	일주일 로그수 ①	한달 로그수 ①	예상 로그수 ①
AppLog	5일 ▼	0	51,595,242	226,722,148	226,722,148	0
AppStdOut	10일 ▼	0	456,702	2,523,814	4,029,866	0
AppStdErr	6일 ▼	0	4,787	25,953	25,953	0

상단에서 로그 모니터링 시작하기 탭을 선택하세요. 📄 가이드 보기 아이콘과 요금제 보기 버튼을 선택하면 관련 안내 화면으로 이동합니다.

에이전트 설정 및 로그 모니터링 활성화

- 1 영역에서 에이전트 설정을 확인하고 [로그 모니터링 활성화](#) 토글 버튼으로 로그 모니터링 활성화 및 비활성화 여부를 설정하세요.

에이전트 설정 확인

로그 모니터링을 시작하기 위해 에이전트 버전과 설정 정보를 확인하세요. [에이전트 설정 확인](#) 메뉴를 선택하여 안내대로 과정을 진행하세요.

• 애플리케이션 모니터링

[적용하기](#) 메뉴 하위에 애플리케이션별 적용 안내를 확인하세요. 다음 설명서 [Java](#), [PHP](#), [Python](#), [Go](#) 등을 참조하세요.

• 서버 모니터링

[적용하기](#) 메뉴 하위에 개별 적용 안내를 확인하세요. [다음 문서](#)를 참조하세요. 안내대로 [whatap.conf](#) 에 로그 감시 대상 파일 설정을 추가하세요.

• 쿠버네티스 모니터링

[적용하기](#) 메뉴 하위에 개별 적용 안내를 확인하세요. [다음 문서](#)를 참조하세요.

로그 모니터링 활성화

[로그 모니터링 활성화](#) 메뉴를 선택하여 로그 모니터링 활성화 및 비활성화 여부를 설정하세요.

에이전트 설정 및 로그 모니터링 활성화 📄
요금제 보기

라이브 테일, 로그 트렌드 기능으로 애플리케이션의 흩어진 로그를 한 눈에 확인하실 수 있습니다.

- ▶ 1. 에이전트 설정 확인
- ▼ 2. 로그 모니터링 활성화

시작일 : 2022년 6월 13일 | 2022년 6월 28일부터 이용 요금이 청구됩니다.

- 토글 버튼을 켜면 로그 모니터링이 활성화됩니다. 활성화한 날부터 15일 동안 무료로 체험하실 수 있습니다.
- 토글 버튼을 끄면 로그 모니터링이 비활성화됩니다. 로그를 더 이상 저장하지 않습니다.

로그 모니터링 데이터 설정

2 영역에서 **로그 사용량**을 확인할 수 있습니다. 또한 **데이터 유지 기간** 및 **로그 조회 비밀번호** 설정을 변경할 수 있습니다.

데이터 유지 기간

공통으로 적용할 기본(default) 데이터 유지 기간입니다. 미지정 시 기본값은 1일입니다. 카테고리별 데이터 유지 기간을 별도로 설정하지 않으면 이 데이터 유지 기간이 기본적으로 적용됩니다. 카테고리별 데이터 유지 기간을 설정하고 **초기화** 버튼을 선택하면 기본 데이터 유지 기간으로 초기화됩니다.

카테고리별 데이터 유지 기간

카테고리별 로그 데이터 유지 기간을 지정할 수 있습니다. **로그 수**는 해당 기간 동안 쌓인 로그 라인을 의미합니다. 예를 들어 **금일 로그 수**는 하루 동안 쌓인 로그 라인 개수, **예상 로그 수**는 데이터 보관일에 금일 로그 수를 곱한 로그 라인 개수를 의미합니다.

로그 데이터 유지 기간을 다음과 같이 지정할 수 있습니다. 기간 지정에 따라 오래된 데이터를 삭제해 공간을 확보할 수 있습니다.

- **트라이얼 프로젝트**

데이터 유지 기간으로 1일, 2일, 3일을 선택할 수 있습니다.

- **유료 프로젝트**

데이터 유지 기간으로 1일, 2일, 3일, 4일, 5일, 6일, 7일, 10일, 30일, 40일을 선택할 수 있습니다.

- **저장량 기준 과금**

데이터 유지 기간에 따라 비용이 달라집니다.

예시, 일 평균 200만 로그 라인이 쌓이고 데이터 유지 기간을 3일로 지정한 경우라면 평균 600만 로그 라인이 수집 서버에 유지되고 과금 대상이 됩니다.

로그 조회 비밀번호

보안을 강화하기 위해 **로그 조회 비밀번호**를 설정하세요. 로그 조회 비밀번호 지정은 선택 사항입니다. 로그 조회 비밀번호를 사용 중이라면 로그 화면 진입 시 반드시 비밀번호를 입력해야 합니다.

ⓘ 비밀번호 분실

로그 편집 권한이 있는 경우 **로그 설정** 메뉴에서 새 비밀번호로 수정할 수 있습니다.

로그 1차 파서 설정

로그 설정 메뉴 상단에서 [로그 1차 파서 설정](#) 탭을 선택해 로그 파서를 등록 및 수정할 수 있습니다. 로그 1차 파서는 [GROK](#)과 [JSON](#) 파서를 제공합니다. 수집된 로그를 대상으로 패턴의 조건과 일치하는 키 정보 즉 검색 키와 검색 값을 추출합니다. 파싱된 로그 키는 로그의 유형을 분류하기 위한 용도 및 특정 로그를 검색하기 위한 인덱싱 용도로 활용합니다. 유형별 로그 발생 수를 집계하거나 특정 로그를 빠르게 찾아내기 위해 등록하는 필수 파서입니다.

- **GROK**: 기본은 정규 표현식 기반 파싱에 해당합니다. 예약 키워드 기반의 파싱을 제공합니다.
- **JSON**: 로그 중 JSON으로 출력된 부분에 대해서 일괄 파싱을 제공합니다.

❗ 파싱 로직 미등록 시 검색 가능한 key

category , oid , oname , okind , okineName , @txid , @login , httphost

❗ 파서 등록이 불가능한 예약어

다음 예약어의 경우 파서를 등록하더라도 인덱스가 생성되지 않습니다.

timestamp , message , pcode , category , content , logContent

❗ 로그 파서에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

설정 항목

설정 값	설명	기타
카테고리	패턴을 적용할 카테고리입니다.	required
로그 검출 조건	필터로 적용할 검색 키, 검색 값을 입력합니다. 로그 검출 조건에 맞는 로그 데이터에만 패턴을 적용합니다. 로그 검출 조건을 입력하지 않으면 모든 로그를 대상으로 패턴을 적용합니다.	optional
패턴	로그를 파싱(parsing)할 패턴입니다. 작성한 패턴에 맞추어서 파싱을 하고 인덱스를 생성합니다. GROK, 정규 표현식 문법을 지원합니다.	required

파서 목록

로그 설정

로그모니터링 시작하기 **로그 1차 파서 설정** 로그 2차 파서 설정 빠른 인덱스 설정 로그 장치 보관 통계

로그 1차 파서 설정 수집된 로그에 대한 파서를 등록할 수 있습니다. 적용 순서대로 파서가 적용되며, 최초로 일치하는 파서만 적용됩니다. + 추가하기 저장

적용 순서	파서	카테고리	필터	패턴	활성화	
0	GROK	AppLog	모든 로그	\[%{TIMESTAMP_ISO8601:timestamp}\]\[%{LOGLEVEL:loglevel}\}s*\]\[%{(GREEDYDATA:classMethod)}\]\[%{(GREEDYDATA:message)}\]	<input checked="" type="checkbox"/>	
1	JSON	AppLog	category:Applog	Prefix 없음 Postfix 없음 Ignore 없음	<input type="checkbox"/>	

로그 설정 메뉴 상단에서 **로그 1차 파서 설정** 탭을 선택하면 등록된 파서를 조회하고 추가 및 편집이 가능한 **파서 목록** 화면을 확인할 수 있습니다.

- 상단 오른쪽 **+ 추가하기** 버튼을 선택하면 **파서 추가** 창이 나타납니다.
- 파서 목록 **적용 순서** 컬럼의 **||** 아이콘을 드래그해 파서 설정 순서를 변경할 수 있습니다.
- 파서 목록 **활성화** 토글을 통해 파서 활성화 여부를 지정할 수 있습니다.
- 파서 목록 **수정** 및 **삭제** 아이콘을 통해 등록된 파서를 수정 및 삭제할 수 있습니다.

파서 등록 순서

로그 설정 메뉴 상단에서 **로그 1차 파서 설정** 탭을 선택해 로그 파서를 등록 및 수정할 수 있습니다. 다음은 파서 등록 시 공통 순서를 안내합니다.

The image shows a 'Add Parser' (파서 추가) dialog box. The background form has the following fields:

- 파서*: GROK
- 카테고리*: 카테고리들()
- 로그 검출 조건: 키, e.g. %(SYN
- 패턴*

 The foreground dialog box has the following fields:

- 파서*: JSON
- 카테고리*: 카테고리들() 선택해주세요, 직접 입력
- 로그 검출 조건: 검색 키, 검색 값, 직접 입력
- 패턴: Prefix, Postfix, Ignore

 A '시뮬레이션' (Simulation) button is highlighted in yellow at the bottom right of the dialog. A '추가' (Add) button is also visible at the bottom right of the background form.

1. + 추가하기 버튼을 선택하면 파서 추가 창이 나타납니다.
2. 파서 선택 창에서 파서를 선택하세요. 각 파서 및 패턴 등록에 관한 자세한 내용은 다음 문서를 참조하세요.
 - [GROK 파서 및 패턴 등록](#)
 - [JSON 파서 및 패턴 등록](#)
3. 카테고리 선택 창에서 카테고리를 선택하거나 직접 입력하세요.
4. 로그 검출 조건으로 활용할 검색 키와 검색 값을 선택하거나 직접 입력하세요.
필터 조건에 맞는 로그 데이터에만 패턴을 적용합니다. 로그 검출 조건을 지정하지 않으면 모든 로그를 대상으로 패턴을 적용합니다.
5. 패턴을 입력하세요.
6. 등록하려는 패턴이 정상적인지 시뮬레이션 버튼을 선택해 시뮬레이션 및 패턴의 퍼포먼스를 측정하세요.
시뮬레이션과 퍼포먼스 측정에 관한 자세한 내용은 [다음 문서](#)를 참조하세요.
7. 시뮬레이션 결과가 정상적이라면 추가 버튼을 선택해 파서를 등록하세요.

❗ 로그 파서 등록 시 동일한 **카테고리**에 파서를 중복 등록할 수 없습니다.

GROK 파서 패턴 등록

파서*	GROK ▼	
카테고리*	카테고리를(를) 선택해주세요	
로그 검출 조건	검색 키	검색 값
	로그 검출 조건을 입력하지 않거나, 검색키/값중 한개만 입력하는 경우 모든 로그를 대상으로 패턴을 적용합니다.	
패턴*	<p>e.g. %{SYNTAX:SEMANTIC}</p>	

기본 문법은 `%{SYNTAX:SEMANTIC}` 입니다. GROK 파서에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

- **SYNTAX**

GROK 정의 패턴입니다.

- **SEMANTIC**

파싱된 데이터에 할당할 키입니다.

❗ SEMANTIC에는 예약어 등이 사용되지 않도록 조합어 사용을 권장합니다.

JSON 포맷 파서 패턴 등록

파서*	JSON ▼	
카테고리*	AppLog ▼	<input type="checkbox"/> 직접 입력
로그 검색 조건	oname ▼	demo-8100 ▼ <input type="checkbox"/> 직접 입력
	로그 검색 조건을 입력하지 않으면, 모든 로그를 대상으로 패턴을 적용합니다.	
패턴	Prefix	--
	Postfix	--
	Ignore	ignore

로그 전체 혹은 일부가 JSON 형태로 출력되는 경우 JSON 포맷 파서를 통해 JSON으로 출력된 부분을 파싱할 수 있습니다. 로그 중 JSON 형태로 출력된 부분을 검색하기 위하여 [Prefix](#), [Postfix](#) 옵션을 조합해 로그의 어느 부분을 JSON으로 인식해 파싱할지 지정합니다. JSON 파서에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

옵션	설명
Prefix	JSON 문자열의 시작 부분 앞의 문자열을 지정합니다. 미지정 시 로그 출력문의 맨 앞부터 JSON 문자열로 식별합니다.
Postfix	JSON 문자열의 종료 부분 뒤의 문자열을 지정합니다. 미지정 시 로그 출력문의 맨 뒤 까지를 JSON 문자열로 식별합니다.
Ignore	JSON 출력부 중 키 추출을 제외할 필드를 지정합니다.

• 등록 예시

Log

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

예시처럼 유입되는 로그가 Request JSON, Response JSON을 모두 파싱하고자 하는 경우 다음의 2가지 패턴을 등록합니다.

- Request 파싱용 패턴

"Request : " 와 "Response" 사이의 문자열 `{"key1":"value1","key2":"value2",...}` 대상

- Response 파싱용 패턴

"Response : " 부터 로그의 마지막 까지의 문자열 `{"key3":"value3","key4":"value4",...}` 대상

- JSON 커스텀 패턴 등록

로그 중 일부가 JSON 형태로 출력되는 경우 JSON으로 출력된 부분을 전용 커스텀 파서를 통해 파싱할 수 있습니다. 패턴을 다음과 같이 입력하세요.

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

로그 중 JSON 형태로 출력된 부분을 검출하기 위해 [Prefix](#), [Postfix](#) 옵션을 조합해 로그의 어느 부분을 JSON으로 인식하여 파싱할지 지정하세요.

`JsonFormatParser{}` 의 `{}` 에 옵션을 지정합니다.

- 등록 예시

Log

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

예시처럼 유입되는 로그가 Request JSON, Response JSON을 모두 파싱하고자 하는 경우 다음의 2가지 패턴을 등록합니다.

- Request 파싱용 패턴

"Request : " 와 "Response" 사이의 문자열 `{"key1":"value1","key2":"value2",...}` 대상

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

- Reponse 파싱용 패턴

"Response : " 부터 로그의 마지막 까지의 문자열 `{"key3":"value3","key4":"value4",...}` 대상

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

파서 시뮬레이션

1. 파서 추가 화면에서 패턴을 입력한 후 **시뮬레이션** 버튼을 선택하세요. **파서 시뮬레이션** 창이 나타납니다.
2. **파서 시뮬레이션** 창에서 **로그**를 입력하세요.
3. 입력한 **로그**와 **패턴**을 확인하세요.

✕
파서 시뮬레이션

! 입력한 패턴으로 로그가 성공적으로 파싱되는지 시뮬레이션합니다.

로그

2022-08-28T15:00:00Z This is a sample log.

패턴

2022-08-28T15:00:00Z This is a sample log.

시뮬레이션

4. **시뮬레이션** 버튼을 선택해 등록하려는 패턴으로 파싱에 성공하는지 확인하세요.

- 시뮬레이션 성공 화면

패턴 적용 시뮬레이션

시뮬레이션 결과

키	timestamp
값	2023-08-28T15:30:45Z
결과	Ok

키	loglevel
값	INFO
결과	Ok

키	classMethod
값	MyApp::SomeClass::someMethod
결과	Ok

키	message
값	This is an example log message.
결과	Ok

퍼포먼스 측정 ▼

- 시뮬레이션 실패 화면

시뮬레이션 결과

결과 Fail

상세 원인 파싱에 실패하였습니다.

5. **패턴 적용** 버튼 클릭 시 선택한 파서에 입력한 패턴이 적용됩니다.

퍼포먼스 측정

시뮬레이션 성공 후 [퍼포먼스 측정](#) 버튼을 선택해 파서에 대한 퍼포먼스를 측정할 수 있습니다. 시뮬레이션 수행 대상 문자열에 대하여 파서의 반복 파싱 소요 시간을 측정 후 다음과 같이 측정 결과를 확인하세요.

시뮬레이션 횟수	결과	최소 시간(ns)	최대 시간(ns)	평균 시간(ns)
1	SUCCESS	29,522	29,522	29,522
10	SUCCESS	5,752	29,628	11,145
100	SUCCESS	4,931	97,550	7,305
1,000	SUCCESS	2,215	178,706	4,431
10,000	SUCCESS	1,575	195,436	2,037
100,000	SUCCESS	451	604,623	1,286
1,000,000	SUCCESS	328	59,273,046	625

파싱 성공

파싱 로직을 등록해 키(key)가 생성되면 로그 조회 시 해당 키로 파싱된 값이 추가됩니다. 다음 [라이브 테일](#) 메뉴 예시와 같이 파싱된 키와 값이 추가됩니다.

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

파싱된 키는 [라이브 테일](#), [로그 검색](#), [로그 트렌드](#)에서 확인할 수 있습니다.

로그 2차 파서 설정

[로그 설정](#) 메뉴 상단에서 [로그 2차 파서 설정](#) 탭을 선택해 로그 파서를 등록 및 수정할 수 있습니다. [4xx, 5xx 상태 코드 파서](#)와 [상태 코드 성공률 파서](#)를 제공합니다. 로그 2차 파서는 GROK 또는 JSON과 같은 1차 파서가 파싱된 경우 사용할 수 있는 파서입니다. 1차 파서로 추출한 값을 가공해 통계 데이터를 생성합니다. 웹 혹은 API 응답 로그에 대해 Http Status Code를 기반으로 2차 통계를 추출합니다.

- **4xx, 5xx 상태 코드 파서**: 비정상 응답에 대한 건수 정보를 집계합니다.
- **상태 코드 성공률 파서**: 전체 건수 대비 비정상 응답 비율을 추출합니다.

❗ 로그 2차 파서는 1차 파싱된 결과에 대하여 특수 목적의 2차 파싱 기능을 제공합니다. 2차 파서를 사용하기 위해서는 **1차 파서가 등록되어** 있어야 합니다.

파서 목록

적용 순서	파서	카테고리	필터	패턴	활성화
0	4xx, 5xx 상태 코드 파서	AppLog	없음		<input checked="" type="checkbox"/>
1	상태 코드 성공률 파서	AppLog	없음		<input checked="" type="checkbox"/>

로그 설정 메뉴 상단에서 **로그 2차 파서 설정** 탭을 선택하면 등록된 파서를 조회하고 추가 및 편집이 가능한 **파서 목록** 화면을 확인할 수 있습니다.

- 상단 오른쪽 **+ 추가하기** 버튼을 선택하면 **파서 추가** 창이 나타납니다.
- 파서 목록 **적용 순서** 컬럼의 아이콘을 드래그해 파서 설정 순서를 변경할 수 있습니다.
- 파서 목록 **활성화** 토글을 통해 파서 활성화 여부를 지정할 수 있습니다.
- 파서 목록 **수정** 및 **삭제** 아이콘을 통해 등록된 파서를 수정 및 삭제할 수 있습니다.

파서 등록 순서

로그 설정 메뉴 상단에서 **로그 2차 파서 설정** 탭을 선택해 로그 파서를 등록 및 수정할 수 있습니다. 다음은 파서 등록 시 공통 순서를 안내합니다.

X 파서 추가

파서*	파서(을) 선택해주세요 v
카테고리*	<p>4xx, 5xx 상태 코드 파서</p> <p>status가 파싱된 경우, 추가적으로 4xx, 5xx 상태 코드를 파싱하여 "4xx, 5xx 건수 데이터"를 생성함</p> <p>4xx, 5xx 건수 데이터 생성</p>
로그 검출 조건	<p>상태 코드 성공률 파서</p> <p>status가 파싱된 경우, 추가적으로 2xx,3xx 상태 코드를 파싱하여 "요청 성공률 데이터"를 생성함</p> <p>요청 성공률 데이터 생성</p>

1. **+ 추가하기** 버튼을 선택하면 **파서 추가** 창이 나타납니다.
2. **파서** 선택 창에서 파서를 선택하세요. 각 파서 설정 항목 및 제외할 상태 코드 등록에 관한 자세한 내용은 다음 문서를 참조하세요.
 - [4xx, 5xx 상태 코드 파서 설정 항목 및 제외할 상태 코드 등록](#)
 - [상태 코드 성공률 파서 설정 항목 및 제외할 상태 코드 등록](#)
3. **카테고리** 선택 창에서 카테고리를 선택하거나 직접 입력하세요.
4. **로그 검출 조건**을 선택하거나 직접 입력하세요.
5. **제외할 상태 코드**를 입력하세요.
6. **추가** 버튼을 선택해 파서를 등록하세요.

4xx, 5xx 상태 코드 파서 제외할 상태 코드 등록

X 파서 추가

파서* 4xx, 5xx 상태 코드 파서 ▼

카테고리* AppLog ▼ 직접 입력

로그 검출 조건 oname ▼ demo-8100 ▼ 직접 입력
로그 검출 조건을 입력하지 않으면, 모든 로그를 대상으로 패턴을 적용합니다.

제외할 상태 코드 400 × 404 ×
입력한 상태 코드는 4xx, 5xx 상태 코드로 로그를 파싱할 때 제외됩니다.

추가

4xx, 5xx 상태 코드 파서는 status가 이미 파싱된 경우 사용할 수 있는 파서입니다. 파싱된 status를 이용하여 추가적으로 4xx, 5xx 상태 코드를 파싱합니다. 파싱한 데이터로 4xx, 5xx 건수 데이터를 생성할 수 있습니다. 제외할 상태 코드로 4xx, 5xx 상태 코드를 입력 또는 선택할 수 있습니다. 입력된 상태 코드는 로그에서 4xx, 5xx 상태 코드를 파싱할 때 제외됩니다.

설정 항목

설정 값	설명	기타
카테고리	4xx, 5xx건수 데이터를 생성할 카테고리입니다.	required
로그 검출 조건	필터로 적용할 검색 키, 검색 값을 입력합니다. 로그 검출 조건에 맞는 로그 데이터에 대해서만 4xx, 5xx건수 데이터를 생성합니다. 로그 검출 조건을 입력하지 않으면 모든 로그를 대상으로 데이터를 생성합니다.	optional
제외할	통계 데이터 생성 시 제외할 상태 코드입니다. 입력하지 않으면 4xx~5xx에 해당하는 전체 오류 상태	optional

설정 값	설명	기타
상태 코드	코드를 대상으로 4xx, 5xx건수 데이터를 생성합니다.	

status 파서 등록 예시

로그 1차 파서 설정 수집된 로그에 대한 파서를 등록할 수 있습니다. 적용 순서대로 파서가 적용되며, 최초로 일치하는 파서만 적용됩니다. + 추가하기 저장

적용 순서	파서	카테고리	로그 검출 조건	패턴	활성화	
0	REGEX	AppLog	모든 로그	%(NUMBER:status)	<input type="checkbox"/>	✎ ✖
1	REGEX	AppLog	모든 로그	%(NUMBER:status)	<input type="checkbox"/>	✎ ✖
2	GROK	AppLog	모든 로그	%(NUMBER:status)	<input checked="" type="checkbox"/>	✎ ✖

유입되는 로그가 `{"msg": "message", "status": 404}` 이고 예시처럼 GROK 파서로 status를 파싱한다면, `status: 404` 와 같이 파싱됩니다. status가 정상적으로 파싱되는 것을 확인했다면 4XX,5XX 상태 코드 파서에서 제외할 상태 코드를 등록하세요.

데이터 조회

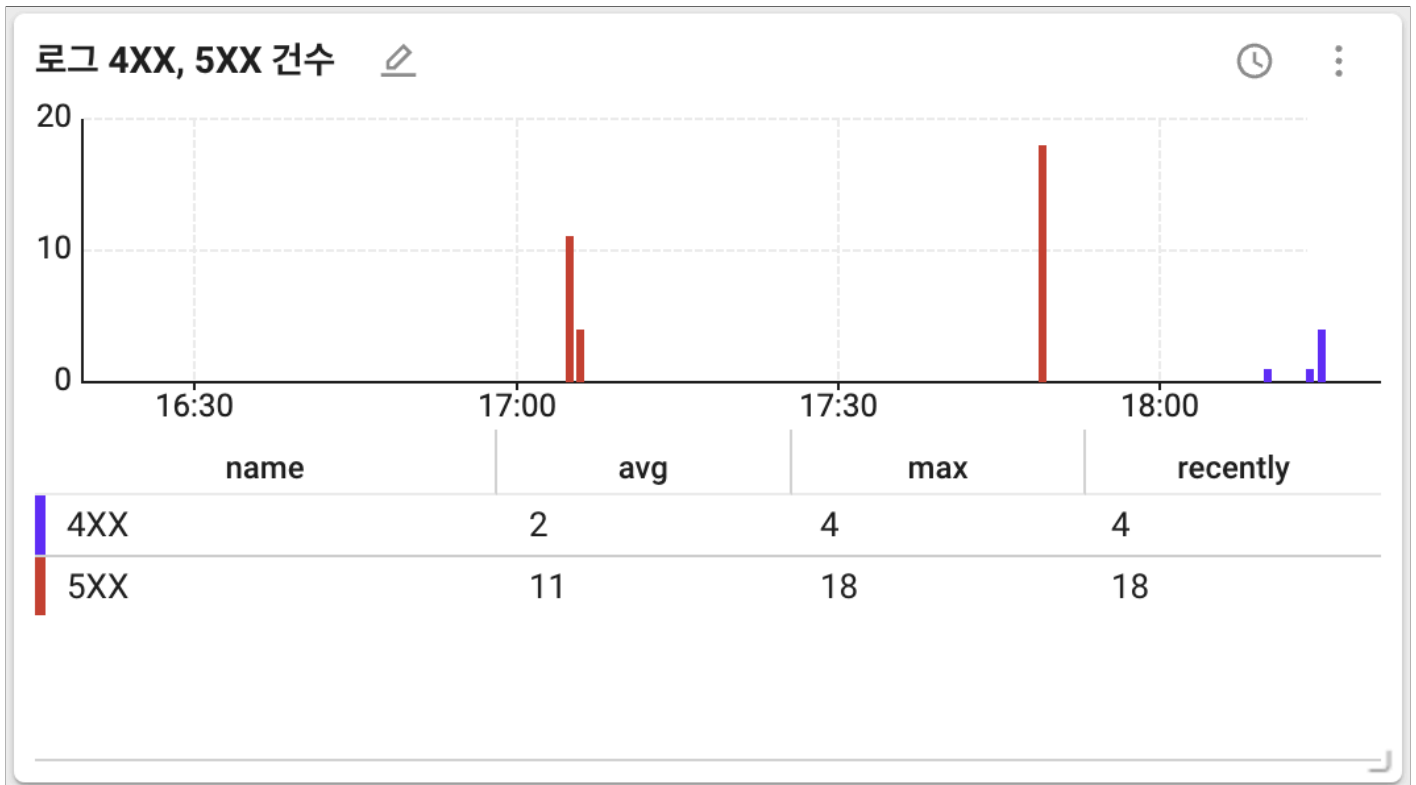
파서를 모두 등록하면 [Flex 보드](#)로 이동해 [로그 4XX, 5XX 건수](#) 위젯을 생성하세요.

위젯 템플릿 ⇌ 모든 메트릭스

🔍

📈 로그 4XX, 5XX 건수

위젯을 생성하면 다음과 같이 데이터를 확인할 수 있습니다.



- **avg**: 조회 기간 데이터 평균값입니다.
- **max**: 조회 기간 데이터 중 최댓값입니다.
- **recently**: 조회 기간 데이터 중 마지막 값입니다.

상태 코드 성공률 파서 제외할 상태 코드 등록

✕
파서 추가

파서*

카테고리* 직접 입력

로그 검출 조건 직접 입력
로그 검출 조건을 입력하지 않으면, 모든 로그를 대상으로 패턴을 적용합니다.

제외할 상태 코드
입력한 상태 코드는 2xx, 3xx 상태 코드로 로그를 파싱할 때 제외됩니다.

추가

상태 코드 성공률 파서는 status가 이미 파싱된 경우 사용할 수 있는 파서입니다. status 파싱에 관한 내용은 [다음 문서](#)를 참조하세요. 파싱된 status를 이용해 추가로 2xx, 3xx 상태 코드를 파싱합니다. 파싱한 데이터로 HTTP 요청 성공률 데이터를 생성할 수 있습니다. 제외할 상태 코드에는 2xx, 3xx 상태 코드를 입력 또는 선택할 수 있습니다. 입력된 상태 코드는 로그에서 2xx, 3xx 상태 코드를 파싱할 때 제외됩니다.

설정 항목

설정 값	설명	기타
카테고리	요청 성공률 데이터를 생성할 카테고리입니다.	required
로그 검출 조건	필터로 적용할 검색 키, 검색 값을 입력합니다. 로그 검출 조건에 맞는 로그 데이터에 대해서만 요청 성공률 데이터를 생성합니다. 로그 검출 조건을 입력하지 않으면 모든 로그를 대상으로 데이터를 생성합니다.	optional

설정 값	설명	기타
제외할 상태 코드	요청 성공률 데이터 생성 시 제외할 상태 코드입니다. 입력하지 않으면 2xx~3xx에 해당하는 전체 성공 상태 코드를 대상으로 요청 성공률 데이터를 생성합니다.	optional

데이터 조회

파서를 모두 등록하면 [Flex 보드](#)로 이동해 로그 요청 성공률 위젯을 생성하세요.

위젯 템플릿 ⇌ 모든 매트릭스

요청 성공률 🔍

📄 로그 요청 성공률

위젯을 생성하면 다음과 같이 데이터를 확인할 수 있습니다.

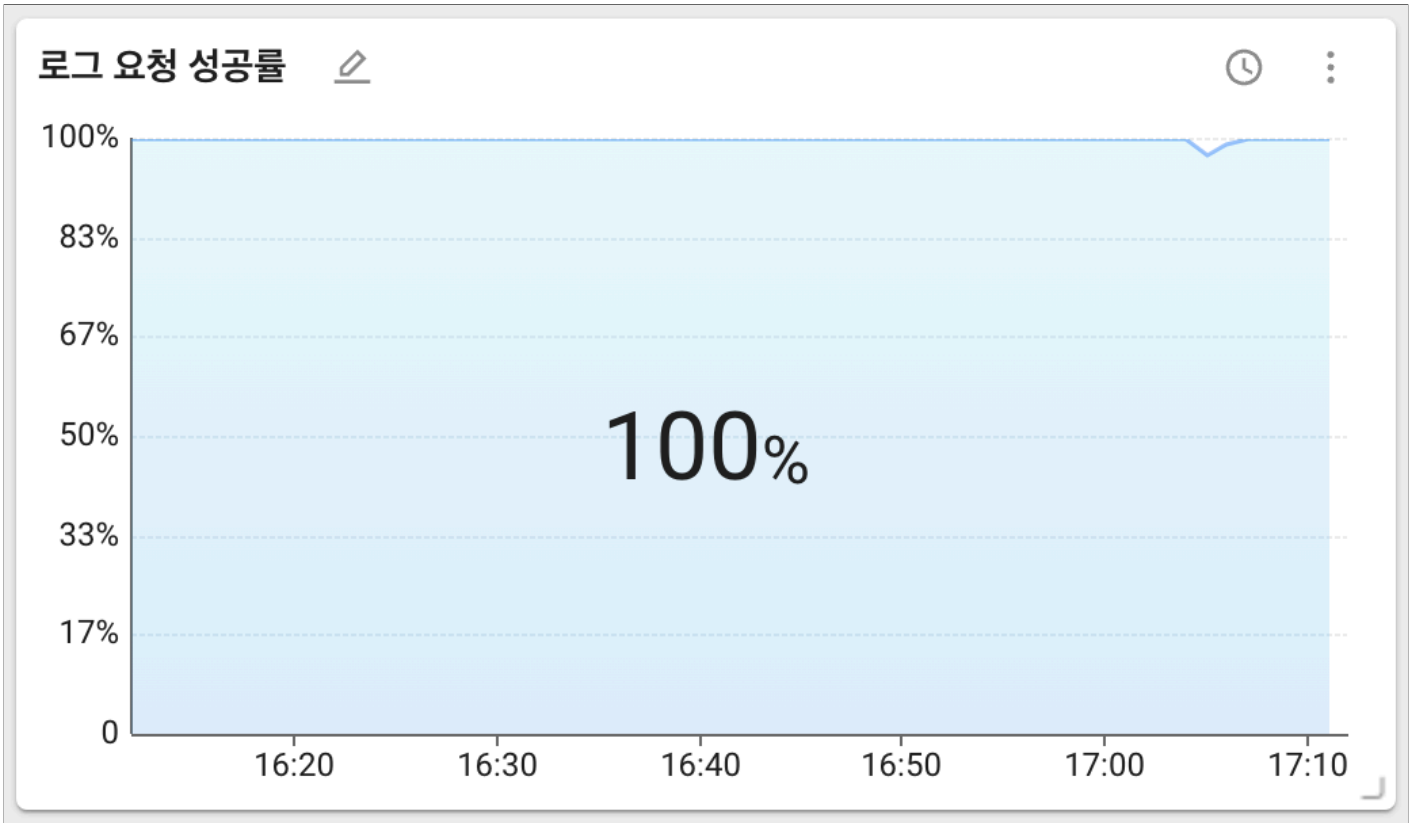


차트 위 데이터는 조회 기간에 대한 통계를 나타냅니다. 통계 방법을 최근값, 최댓값, 평균값 등으로 선택할 수 있습니다. 최근값이 기본으로 선택되어 있습니다.

빠른 인덱스 설정



[로그 설정](#) 메뉴 상단에서 [빠른 인덱스 설정](#) 탭을 선택하세요. 대량의 로그를 수집할 경우 로그 검색 성능이 현저하게 저하될 수 있습니다. 자주 사용하는 검색 조건을 **인덱스(index)**로 생성하면 로그 검색 성능을 개선해 빠른 탐색이 가능합니다. 설정 항목은 다음과 같습니다.


설정 값	필수 여부	설명
카테고리	필수	빠른 인덱스를 설정할 카테고리
검색 키	필수	빠른 인덱스를 설정할 검색 키

설정 값	필수 여부	설명
대소문자 구분 안 함	옵션	대소문자를 구분 여부
규칙	필수	* 한 개 이상 포함 필수
활성	필수	활성 또는 비활성 여부(기본값 true)

로그 설정 가져오기/내보내기

공통된 파서 설정 및 빠른 인덱스 설정 내용을 JSON 파일 형식으로 저장하고, 다른 프로젝트에서 JSON 파일을 가져와 적용할 수 있습니다. 프로젝트마다 여러 번 반복해서 설정을 작성하는 번거로움을 줄일 수 있습니다.

1. 하나의 프로젝트에 파서 설정 및 빠른 인덱스 설정을 추가하세요.
2. 각 설정 탭에서 화면 오른쪽 위에 **JSON**  버튼을 선택하세요.
3. **JSON 내보내기** 창이 나타나면 화면 오른쪽 위에 **내보내기** 버튼을 선택하세요.
4. JSON 설정 파일이 사용자 PC에 저장됩니다.
5. 다른 프로젝트로 이동한 다음 **로그** > **로그 설정** 메뉴로 이동하세요.
6. 앞서 JSON 설정 파일을 내보낸 설정 탭을 선택한 다음  버튼을 선택하세요.
7. 파일 선택 창이 나타나면 사용자의 PC에 저장한 JSON 설정 파일을 선택하세요.
8. **JSON 가져오기** 창이 나타나면 설정 내용을 확인한 다음 **목록에 추가하기** 또는 **덮어쓰기** 버튼을 선택하세요.
9. 화면 오른쪽 위에 **저장** 버튼을 선택하세요.

 JSON 설정 파일을 가져온 다음 **저장** 버튼을 선택하지 않으면 가져온 설정 내용을 저장할 수 없습니다.

로그 장기 보관 통계 설정

로그 설정 메뉴 상단에서 **로그 장기 보관 통계** 탭을 선택하세요. 로그 데이터는 용량이 매우 커서 장기간 보관하기가 어렵습니다. 따라서 로그 통계 데이터 설정 기능을 사용하여 **특정 조건을 만족하는 로그 데이터가 5분마다 몇 건씩 수집되었는지에 대한 정보를 저장할 수** 있습니다. 장기간 시 실제 로그 데이터는 삭제되어도 해당 조건을 만족하는 로그가 얼마나 수집되었는지 추이를 확인할 수 있습니다.

로그 장기 보관 통계 추가

×
로그 장기 보관 통계 추가

통계 키*

데이터 보관일(디스크 사용량) ▼

카테고리*

로그 검출 조건*

▼

X 검색 값을(를) 선택해주세요

제외 대소문자 구분

▼

X 검색 값을(를) 선택해주세요

제외 대소문자 구분

[+ 추가하기](#)

로그 장기 보관 통계 탭에서 + 추가하기 버튼을 선택하면 로그 장기 보관 통계 추가 창이 나타납니다. + 추가하기 버튼을 통해 규칙을 추가하거나 생성한 규칙을 - 아이콘을 통해 삭제할 수 있습니다.

설정 항목

필드	설명
카테고리	규칙을 적용할 카테고리입니다.
통계 키(key)	규칙을 만족하는 로그 발생 시 저장할 키 값으로 동일한 키를 중복으로 설정할 수 없습니다.
로그 검출	로그 통계 데이터를 생성할 조건입니다. 이 조건을 만족하는 로그가 얼마나 수집되었는지를 기반으로 통계

필드	설명
조건	데이터를 생성합니다.
제외	제외를 체크하면 입력한 조건에 해당하지 않는 값으로 통계 데이터를 생성합니다.
대소문자 구분	입력한 로그 검색 조건의 값에 대해서 대소문자 구분 여부를 지정합니다.
활성	활성 또는 비활성 여부(기본값 true)

예시

다음과 같이 설정을 추가한 경우 수집된 로그 중 status가 200, 300 인 로그를 대상으로 TotalCount라는 키값으로 통계 데이터를 생성합니다.

로그 장기 보관 통계 설정한 조건을 만족하는 로그가 얼마나 수집되었는지 통계 데이터를 생성할 수 있습니다. + 추가하기 저장

카테고리	통계 키	로그 검색 조건	데이터 보관일(디스크 사용량)	활성화	
AppLog	TotalCount	status 200, 300	15일 (약 3 MB)	<input type="checkbox"/>	✖
AppLog	TotalCount	status 200	15일 (약 3 MB)	<input type="checkbox"/>	✖
AppLog	TotalCount	status 200, 300	15일 (약 3 MB)	<input checked="" type="checkbox"/>	✖
AppLog	TotalCount	status 200, 300	15일 (약 3 MB)	<input checked="" type="checkbox"/>	✖

데이터 조회

1. Flex 보드의 위젯 템플릿에서 로그 장기 보관 통계를 검색해 위젯을 생성하세요.

위젯 템플릿 ⇌ 모든 메트릭스

🔍

로그 장기 보관 통계

2. 데이터를 조회할 **카테고리**와 **키**를 지정한 뒤 **적용** 버튼을 선택합니다.

로그 장기 보관 통계 ✎

i 카테고리, 키를 선택해 주세요.

해당 위젯이 나타낼 데이터 수집을 위해서는 **로그 장기 보관 통계 설정**이 필요합니다.
 해당 설정을 하지 않은 경우,
[가이드](#)를 참고하여 **로그 장기 보관 통계 설정**을 해주세요.
[로그 설정](#)

카테고리 변경

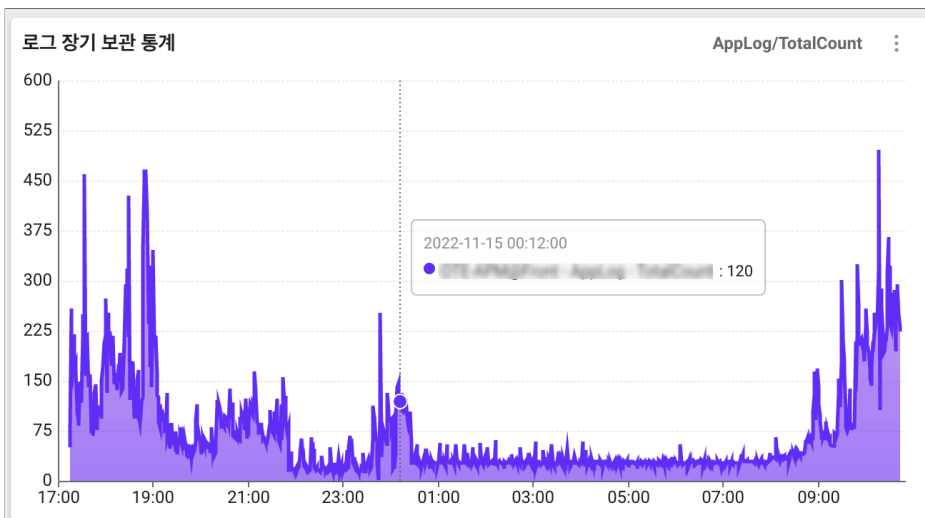
AppLog ▼

통계 키

TotalCount ▼

취소
적용

3. 추가한 설정값으로 **로그 장기 보관 통계** 데이터를 다음처럼 확인할 수 있습니다.



로그 파싱하기

로그 파서를 사용하면 불규칙한 형태의 로그를 쿼리가 가능한 구조화된 형태로 변경할 수 있습니다. 와탭 로그 모니터링은 다음과 같이 두 가지 유형의 파서를 제공합니다.

- **GROK 파서:** 임의의 형태로 수집되는 로그를 정규 표현식과 GROK 문법을 활용해 파싱합니다.
- **JSON 파서:** JSON 형태로 수집되는 로그를 파싱합니다.

① 공통 주의사항

- 같은 카테고리에 여러 개의 파서가 등록되어 있는 경우 첫 번째로 매칭되는 파서만 적용됩니다.
- 와탭은 와탭 서비스의 안정성에 영향을 줄 수 있는 파서를 비활성화할 수 있는 권한을 가집니다.

GROK 파서

로그가 불규칙한 형태로 수집되는 경우 GROK 파서를 사용해 로그를 파싱할 수 있습니다. GROK 문법은 named regular expressions를 제공해 정규 표현식을 보다 쉽고 편리하게 사용할 수 있습니다.

GROK 파서 패턴 등록에 관해 다음 동영상 가이드를 참조하세요.

GROK 시작하기

GROK은 두 가지 형태의 문법을 제공합니다.

1. `%{SYNTAX:SEMANTIC}`: GROK 라이브러리에서 제공하는 문법입니다. **named regular expressions**를 활용해 태그를 추출할 수 있습니다. 활용 예시는 [다음](#)을 참조하세요.
 - **SYNTAX:** GROK이 제공하는 named regular expressions를 지정합니다.
 - **SEMANTIC:** 매칭되는 값에 부여할 이름을 지정합니다.

① named regular expressions

GROK에서 제공하는 문법입니다. 복잡한 정규 표현식에 이름을 부여해 사용할 수 있도록 GROK에서 제공하는 기능입니다.

name	regular expression
WORD	<code>\b\w+\b</code>
SPACE	<code>\s*</code>
NOTSPACE	<code>\S+</code>
UUID	<code>[A-Fa-f0-9]{8}-(?:[A-Fa-f0-9]{4}-){3}[A-Fa-f0-9]{12}</code>

와탭에서 제공하는 모든 named regular expressions 확인을 원한다면 다음 [링크](#)를 참조하세요.

2. `?<SEMANTIC>REGX`: 정규 표현식의 **named capturing group** 문법입니다. 정규 표현식을 활용해서 사용자의 의도에 맞게 태그를 추출할 수 있습니다. 활용 예시는 [다음](#)을 참조하세요.
 - **SEMANTIC:** 매칭되는 값에 부여할 이름을 지정합니다.
 - **REGX:** 매칭에 사용할 정규 표현식을 입력합니다.

① named capturing group

정규 표현식에서 제공하는 문법입니다.

- capturing group: 여러 개의 토큰을 하나로 묶어 하나의 매칭 단위로 사용하는 기능을 의미합니다.
- named capturing group: capturing group에 이름을 부여한 것입니다.
- 문자열 매칭 예시를 살펴보겠습니다. [dev@whatap.io](#)

- 예시 1 `(\w+)@(\w+\.\w+)`

- 예시 2 이메일 전체 매칭 및 username과 domain 추가 매칭 시 `(?<username>\w+)@(?<domain>\w+\.\w+)`

%(SYNTAX:SEMANTIC) 활용 예시

다음은 %(SYNTAX:SEMANTIC) 문법을 활용하는 예시입니다.

Sample log

```
[2023-08-08 02:02:30,101 GMT][INFO ][i.w.y.l.c.LogSinkDexScheduleThread.realProcess(159)] 8 VirtualLog 20230808 02:01:00.000 {area=4, city=5} 56ms
```

샘플 로그를 보고 각 단어가 의미하는 내용을 유추할 수 있습니다. 각 부분을 semantic한 단어로 치환 시 다음과 같이 표현할 수 있습니다.

semantic replace

```
[date][logLevel][caller] projectCode logCategory dexBuildStartTime {area=areaEnum, city=cityEnum} dexBuildElapsed
```

semantic한 단어 모두 정규 표현식으로 대체할 수 있습니다. GROK 파서를 사용하면 사전 정의된 named regular expressions를 활용할 수 있습니다. 여기서 사용된 `TIMESTAMP_ISO8601`, `LOGLEVEL`, `DATA` 는 GROK에서 제공하는 named regular expressions입니다. 이 값들은 각각 다음의 정규 표현식으로 대체되어 매칭됩니다.

- name: `TIMESTAMP_ISO8601`
 - regular expression: `%(YEAR)-%(MONTHNUM)-%(MONTHDAY)[T]%(HOUR):?(MINUTE):?(?:?(SECOND))?(?:%(ISO8601_TIMEZONE)?`
- name: `LOGLEVEL`
 - regular expression: `LOGLEVEL`
`[(Aa)lert|ALERT|[Tt]race|TRACE|[Dd]ebug|DEBUG|[Nn]otice|NOTICE|[Ii]nfo|INFO|[Ww]arn?:?ing)?|WARN?:?(?:ING)?|[Ee]rr?:?(?:or)?|ERR?:?(?:OR)?|[Cc]rit?:?(?:ical)?|CRIT?:?(?:ICAL)?|[Ff]atal|FATAL|[Ss]evere|SEVERE|EMERG(?::ENCY)?|[Ee]merg(?::ency)?`
- name: `DATA`
 - regular expression: `.*`

GROK parsing pattern

```
\[(TIMESTAMP_ISO8601:date)\sGMT\]\[(LOGLEVEL:level)\s\]\[(DATA:caller)\]
```

위와 같은 문법으로 파싱을 하면 다음과 같이 태그를 추출할 수 있습니다. 이렇게 GROK의 %(SYNTAX:SEMANTIC) 문법은 복잡하고 긴 정규 표현식을 쉽고 간결하게 적용할 수 있도록 도와주는 역할을 합니다.

Tag extraction

```
- date : 2023-08-08 02:02:30,101
- caller : i.w.y.l.c.LogSinkDexScheduleThread.realProcess(159)
- level : LEVEL
```

(?<SEMANTIC>REGX) 활용 예시

named regular expressions로 매칭되지 않는 부분은 (?<SEMANTIC>REGX) 패턴을 사용해서 파싱할 수 있습니다. 위의 [샘플 로그](#)에서 %(SYNTAX:SEMANTIC) 문법만으로 파싱되지 않는 영역은 다음과 같습니다.

Unparsed area

```
8 VirtualLog 20230808 02:01:00.000 {area=4, city=5} 56ms
```

해당 로그의 각 부분을 semantic한 단어로 치환 시 다음과 같이 표현할 수 있습니다.

semantic replace

```
projectCode logCategory dexBuildStartTime {area=areaEnum, city=cityEnum} dexBuildElapsed
```

이렇게 불규칙한 형태의 문자열은 다음과 같은 (?<SEMANTIC>REGX) 문법을 사용해 파싱할 수 있습니다.

샘플 로그 파싱 키워드별 매칭되는 정규 표현식

파싱 키워드	(?<SEMANTIC>REGX)
8	(?<projectCode>\d)
VirtualLog	(?<logCategory>\w*)
20230808 02:01:00.000	(?<dexBuildStartTime>\d{8}\s\d{2}:\d{2}:\d{2}\.\d{3})
area=4	area=(?<areaEnum>\d)
city=5	city=(?<cityEnum>\d)
56ms	(?<dexBuildElapsed>\d{2})ms

> 기본 정규 표현식 문법

문법	의미	별칭
?	0 or 1	-
+	1 or more	-
*	0 or more	-
a{5}	exactly 5	-
\w	word character	[a-zA-Z_0-9]
\s	white space	-
.	any character except newline	-
[abc]	any of	-
[^abc]	not a,b, or c	-
[a-z]	character between a and z	-
[1-3[7-9]]	union (combining two or more character classes)	-
[1-6&&[3-9]]	intersection (교집합)	-
[0-9&&[^2468]]	subtraction (차집합)	-
a{2,}	2 or more	-
a{1,3}	between 1 and 3	-
a+?	match as few as possible	-
{2,3}?	match as few as possible	-
(abc)	capturing group (여러 개의 문자열을 single unit으로 처리함)	-
\d	digit	[0-9]

문법	의미	별칭
\D	non-digit	[^0-9]
\W	non-word character	-
\S	non-white space	-

이렇게 파싱된 키워드를 띄어쓰기(\s)와 특수 문자 escape(\x, \., \y)로 연결하면 다음과 같이 패턴을 적용할 수 있습니다.

```
GROK parsing pattern
(?<projectCode>d)s(?<logCategory>\w*)s(?<dexBuildStartTime>d{8})\s
d(2):d(2):d(2)\.d(3))\s(area=?<areaEnum>d)\,s(city=?<cityEnum>d)\)\s(?<dexBuildElapsed>d(2))ms
```

위와 같은 문법으로 파싱을 하면 다음과 같이 태그를 추출할 수 있습니다.

```
Tag extraction
- projectCode : 8
- logCategory : VirtualLog
- dexBuildStartTime : 20230808 02:01:00.000
- areaEnum : 4
- cityEnum : 5
- dexBuildElapsed : 56
```

GROK 적용하기

로그 설정 > 로그 1차 파서 설정

1. GROK 패턴 파서를 적용하려면 **로그 설정** 메뉴의 **로그 1차 파서 설정** 탭으로 이동하세요.



2. **+ 추가하기**를 선택 후 **파서** 입력란에서 **GROK** 파서를 선택하세요.

파서*

카테고리*

로그 검출 조건
로그 검출 조건을 입력하지 않거나, 검색키/값중 한개만 입력하는 경우 모든 로그를 대상으로 패턴을 적용합니다.

패턴*

3. **카테고리** 및 **로그 검출 조건**, **패턴**을 입력하세요. **파서 추가** 창의 구성 요소는 다음과 같습니다.

- **카테고리**
로그 카테고리를 선택하세요. **카테고리**는 필수로 입력해야 합니다.
- **로그 검출 조건**
 - 조건에 만족하는 로그만 파서가 적용됩니다.
 - **검색 키**와 **검색 값**을 선택하거나 직접 입력하세요.
 - **로그 검출 조건**은 모든 파서가 수행되기 전에 적용됩니다. 즉 파서의 결과로 추가되는 **태그**를 사용할 수 없습니다.
- **패턴**
GROK 패턴을 지정하세요. 필수로 입력해야 합니다.

4. **추가** 버튼을 선택해 파서를 등록하세요.

① • 로그 파서 목록에서 해당 파서의 **적용 순서**를 변경하거나 **활성화** 및 **수정**, **삭제**할 수 있습니다.
 • 파서를 등록하기 전에 **시뮬레이션**을 통해 등록하려는 패턴이 정상적인지 확인할 수 있습니다.

① **GROK 파서 주의사항**

- GROK 파서는 `%(SYNTAX:SEMANTIC)`, `%(SYNTAX:SEMANTIC)` 두 가지 패턴을 지원합니다.
- `%(SYNTAX:SEMANTIC)` 패턴 사용 시 `SEMANTIC` 을 반드시 입력해야 합니다.
- `%(SYNTAX:SEMANTIC)` 패턴 사용 시 `SEMANTIC` 은 하나의 파서 안에서 **unique** 해야 합니다.
- `(?<SEMANTIC>REGX)` 패턴 사용 시 `SEMANTIC` 은 문자(a-z, A-Z)와 숫자(0-9) 그리고 지정된 특수문자(`.`, `_`, `-`)만 을 수 있습니다.
- `SEMANTIC` 은 문자(a-z, A-Z)로 시작해야 합니다.
- `SEMANTIC` 은 문자(a-z, A-Z) 또는 숫자(0-9)로 끝나야 합니다.

시뮬레이션

파서 시뮬레이션 창에서 **로그**와 **패턴**을 입력해 파싱 결과를 미리 확인할 수 있습니다.

로그 예시: `[2023-08-08 02:02:30,101 GMT][INFO][i.w.y.l.c.LogSinkDexScheduleThread.realProcess(159)] 8 VirtualLog 20230808 02:01:00.000 {area=4, city=5} 56ms`

패턴 예시:

```
\\[%{TIMESTAMP_ISO8601:date}\sGMT\\]\[%{LOGLEVEL:level}\s\\]\[%{DATA:caller}\]\s(?:<projectCode>\d)\s(?:<logCategory>\w*)\s(?:<dexBuildStartTime>\d{8})\s\d{2}:\d{2}:\d{3}\s\{area=(?:<areaEnum>\d),\s\city=(?:<cityEnum>\d)\}\s(?:<dexBuildElapsed>\d{2})ms
```

1. **파서 추가** 창에서 **시뮬레이션** 버튼을 선택하세요.
2. **파서 시뮬레이션** 창에서 **로그**와 **패턴**을 입력하세요.
3. **로그**와 **패턴** 입력 후 **시뮬레이션** 버튼을 선택하세요. 다음과 같이 **시뮬레이션 결과**를 확인할 수 있습니다.

✕
파서 시물레이션

① 입력한 패턴으로 로그가 성공적으로 파싱되는지 시물레이션합니다.

로그

```
[2023-08-08 02:02:30,101 GMT][INFO ][i.w.y.l.c.LogSinkDexScheduleThread.realProcess(159)] 8 VirtualLog 20230808 02:01:00.000 {area=4, city=5} 56ms
```

패턴

```
[\%(TIMESTAMP_ISO8601:date)\sGMT\s\%\%(LOGLEVEL:level)\s\%\%(DATA.caller)\s\%(?<projectCode>d)\s\%(?<logCategory>w*)\s\?(<dexBuildStartTime>d(8)\s\d(2)\s\d(2)\s\d(3))\s\%(area=?<areaEnum>d)\s\%(city=?<cityEnum>d)\s\?(<dexBuildElapsed>d(2))ms
```

패턴 적용
시물레이션

시물레이션 결과

키	date
값	2023-08-08 02:02:30,101
결과	Ok
키	caller
값	i.w.y.l.c.LogSinkDexScheduleThread.realProcess(159)
결과	Ok
키	cityEnum
값	5
결과	Ok
키	level
값	INFO
결과	Ok
키	projectCode
값	8
결과	Ok
키	areaEnum
값	4
결과	Ok
키	dexBuildStartTime
값	20230808 02:01:00.000
결과	Ok
키	dexBuildElapsed
값	56
결과	Ok
키	logCategory
값	VirtualLog
결과	Ok

JSON 파서

로그가 JSON 포맷으로 수집될 경우 JSON 파서를 사용해 쉽고 편리하게 파싱할 수 있습니다.

JSON 적용하기

[로그 설정](#) > [로그 1차 파서 설정](#)

1. JSON 패턴 파서를 적용하려면 [로그 설정](#) 메뉴의 [로그 1차 파서 설정](#) 탭으로 이동하세요.



2. + 추가하기를 선택 후 파서 입력란에서 JSON 파서를 선택하세요.

파서*

카테고리* 직접 입력

로그 검색 조건 직접 입력
로그 검색 조건을 입력하지 않으면, 모든 로그를 대상으로 패턴을 적용합니다.

패턴

Prefix

Postfix

Ignore

3. 카테고리 및 로그 검색 조건, 패턴을 입력하세요. 파서 추가 창의 구성 요소는 다음과 같습니다.

- **카테고리**
로그 카테고리를 선택하세요. **카테고리**는 필수로 입력해야 합니다.
- **로그 검색 조건**
 - 조건에 만족하는 로그만 파서가 적용됩니다.
 - **검색 키**와 **검색 값**을 선택하거나 직접 입력하세요.
 - **로그 검색 조건**은 모든 파서가 수행되기 전에 적용됩니다. 즉 파서의 결과로 추가되는 **태그**를 사용할 수 없습니다.
- **패턴**
 - **Prefix**
로그에서 JSON 포맷이 시작하는 위치를 지정합니다. 로그 전체가 JSON 포맷인 경우 빈 값으로 설정합니다.
 - **Postfix**
로그에서 JSON 포맷이 끝나는 위치를 지정합니다. 로그 전체가 JSON 포맷인 경우 빈 값으로 설정합니다.
 - **Ignore**
JSON 포맷 중 태그를 생성하지 않을 키를 지정합니다.
 - JSON 패턴 예시

```
Example
2023-08-08 02:43:28,615 -- ("host":"10.21.3.24","method":"POST","status":"200","url":"http://devote.whatap.io/yard/api/flush") --
```

예시 로그에서 **Prefix**와 **Postfix**를 --로 지정하고 **Ignore**에 --를 지정 시 `host`, `method`, `status` 3개의 **태그**만 생성됩니다.

4. 추가 버튼을 선택해 파서를 등록하세요.

- ① • 로그 파서 목록에서 해당 파서의 **적용 순서**를 변경하거나 **활성화** 및 **수정**, **삭제**할 수 있습니다.
- 파서를 등록하기 전에 **시뮬레이션**을 통해 등록하려는 패턴이 정상적인지 확인할 수 있습니다. GROK 파서 등록 시뮬레이션 과정과 동일합니다. [다음 문서](#)를 참조하세요.

JSON 포맷 활용 예시

Sample log

```
{"host": "10.21.3.24", "method": "POST", "status": "200", "url": "http://devote.whatap.io/yard/api/flush"}
```

위와 같은 샘플 로그가 수집된 경우 **파서 추가** 창에서 **JSON** 파서를 선택하세요. 복잡한 파싱 로직을 작성할 필요없이 로그 분석에 필요한 **태그**를 다음과 같이 추출할 수 있습니다.

Tag extraction

```
- host : 10.21.3.24
- method : POST
- status : 200
- url : http://dev.whatap.io/yard/api/flush
```

JSON 포맷 일부 구성 시 활용 예시

Some JSON format sample log

```
2023-08-08 02:43:28,615 -- {"host": "10.21.3.24", "method": "POST", "status": "200", "url": "http://devote.whatap.io/yard/api/flush"} --
```

만약 예시와 같이 로그의 일부만 JSON 포맷으로 구성되어있다면 **Prefix**와 **Postfix**를 지정해 주세요. 와탭 로그 모니터링은 **Prefix**와 **Postfix** 사이의 영역을 JSON 포맷으로 인식 후 파싱합니다.

Tag extraction

```
- host : 10.21.3.24
- method : POST
- status : 200
- url : http://dev.whatap.io/yard/api/flush
```

로그 타임스탬프 기준

본 문서는 로그 모니터링 과정 중 처리(Processing) 단계에서 로그 타임스탬프 기준 시간에 대해 안내합니다.

타임스탬프 기준 시간

타임스탬프	로그
2023-11-27 14:26:00.343 와탭 수집 서버 시간	agenttime 1701062760115 에이전트 수집 시간
	[2023-11-27 05:25:56,588 GMT] 로그 발생 시간

로그 타임스탬프 기준 시간이 와탭 에이전트가 로그를 수집한 시간에서 와탭 수집 서버의 로그 처리 시간으로 변경되었습니다.

일반적인 상황에서는 변경 전과 큰 차이없이 기존 방식과 동일하게 로그를 검색할 수 있습니다. 변경 후 다음의 경우에도 사용자의 추가적인 수정 없이 로그 모니터링을 일관적으로 사용할 수 있습니다.

- NTP 사용 시, 모니터링 대상의 서버 시간이 표준 시간보다 과거 또는 미래 시간으로 설정되어있는 경우
- NTP 미사용 시, 2개 이상인 모니터링 대상의 서버 시간이 서로 다른 경우

타임셀렉터 조회 범위 지정

타임스탬프 기준 시간 변경으로 타임셀렉터 역시 와탭 수집 서버 시간을 기준으로 동작합니다. 이에 따라 에이전트 수집 시간과 와탭 수집 서버 시간에 차이가 생겨 조회 범위에 포함되지 않는 로그가 발생할 수 있습니다. 이 경우 조회 범위를 넓게 지정 시 조회가 가능합니다.

로그 트렌드

로그 트렌드 추이 차트의 X축은 최소 1분 기준입니다. 로그 기준 시간이 변경된 후에도 차트를 통한 전체적인 추이 파악에는 영향을 주지 않습니다.

로그 검색

로그 메시지에 로그 생성 시간을 나타내는 인덱스 agenttime 이 추가되었습니다. agenttime 값을 통해 에이전트 수집 시간을 확인하세요.

- ① UTC를 따르는 **와탭 수집 서버 시간**은 사용자 브라우저 시간에 따라 변환해 표기합니다.
예시, 한국의 경우 UTC+9 기준으로 시간을 표기합니다.

단계별 기준 시간

로그는 다음의 3 단계를 거쳐 수집됩니다. 각 단계마다 서로 다른 기준 시간이 사용될 수 있습니다.

1. 로그 발생 시간

모니터링 대상의 시간 또는 Logging 정책에 따라 편차가 발생할 수 있습니다.

2. 에이전트 수집 시간

사용 중인 상품 또는 에이전트가 로그를 수집하는 방법 및 생성되는 로그에 따라 편차가 발생할 수 있습니다.

- **Application**

설정에 따라 로그 라이브러리 또는 로그 파일에서 실시간에 가깝게 로그를 수집합니다.

- ① 로그 라이브러리는 Java 상품의 경우만 지원합니다.

- **Server**

로그 파일에서 실시간에 가깝게 로그를 수집합니다.

- **AWS Log**

AWS Resource 정책에 따라 준 실시간 또는 수 분마다 로그를 수집합니다.

3. 와탭 수집 서버 시간

모니터링 대상 또는 로그 생성 방법과 상관없이 수집 서버에 저장되는 시간을 사용합니다.

와탭 에이전트 수집 시간과 **와탭 수집 서버 시간**은 큰 차이가 있습니다. 모니터링 대상의 서버 시간을 확인하세요. 모니터링 대상의 서버 시간이 과거 또는 미래 시간으로 설정된 경우 에이전트 수집 시간에 영향을 끼칩니다.

주요 메뉴 알아보기

와탭의 로그 모니터링은 통합 시스템 구축을 바탕으로 사용자 편의성과 접근성을 높였습니다. 와탭은 자체 기술력을 기반으로 탄탄한 데이터 수집을 통해 사용자들이 주로 사용하는 라이브 테일, 로그 트렌드, 로그 검색, 이벤트 알림은 물론 Parser의 효율성을 지원합니다.

[로그](#) 메뉴는 조회 및 분석과 옵션 설정 등의 기능을 제공합니다. [이벤트 설정](#) 메뉴는 로그 관련 이벤트 알림을 설정할 수 있습니다.

- 홈 화면 > 프로젝트 선택 > [로그](#)

와탭 모니터링 서비스 초기 화면에서 프로젝트를 선택한 다음 프로젝트 메뉴 하위에 [로그](#) 메뉴를 선택하세요. 다음 기능을 활용하면 복잡한 로그에 보다 손쉽게 접근하여 다양한 조건으로 실시간 확인 및 분석이 가능합니다.

- [라이브 테일](#)
- [로그 트렌드](#)
- [로그 검색](#)

- 홈 화면 > 프로젝트 선택 > [경고 알림](#) > [이벤트 설정](#)

와탭 모니터링 서비스 초기 화면에서 프로젝트를 선택한 다음 프로젝트 메뉴 하위에 [경고 알림](#) 메뉴를 선택해 [이벤트 설정](#) 메뉴에 진입하세요. 이벤트 조건을 설정하고 이메일, SMS, 메신저, App Push 등 다양한 경로로 알림을 수신할 수 있습니다.

와탭 로그 모니터링 서비스의 주요 메뉴 안내를 다음과 같이 제공합니다.

라이브 테일

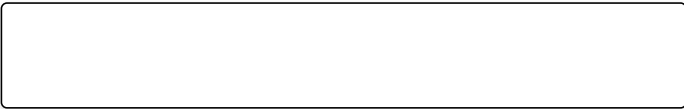
로그 모니터링 라이브 테일을 안내합니다.

로그 트렌드

로그 모니터링의 로그 트렌드 메뉴를 안내합니다.

로그 검색

로그 모니터링의 로그 검색 메뉴를 안내합니다.



알림 설정하기

로그 이벤트 알림 메뉴를 안내합니다.

경고 알림 수신 설정

프로젝트에 포함하는 멤버들의 경고 알림 수신과 관련한 다양한 기능을 설정할 수 있습니다.

이벤트 기록

이벤트 기록 메뉴를 통해 발생한 경고 알림 이력을 확인할 수 있습니다.

라이브 테일

❗ 로그 조회 권한이 없을 경우 해당 메뉴에 진입할 수 없습니다.

홈 화면 > 프로젝트 선택 > 로그 > 라이브 테일

라이브 테일 메뉴에서 서버 콘솔에 접근 없이 모니터링 화면상에서 로그 데이터 스트림을 쉽게 확인할 수 있습니다. 대량의 로그 중 필요한 로그를 선별하고 하이라이트 기능을 통해 원하는 로그를 빠르게 인지할 수 있습니다.

라이브 테일
🔍 🔔 🗄️ ⋮ 👤

1

카테고리
필터

AppLog

필터를(을) 입력 후 엔터를 눌러 추가하세요.

🔍

2

Content 필터
🔍 ⏸️ 🔍 🔄 🗑️ ⚙️

3

▶	oname	타임스탬프	로그
		09:06:52.656	select productid
▶	demo-8103	2023-08-30 09:06:52.656	@txid -636988446309675660 pcode 5490 oname demo-8103 onodeName node-1 oid 633280970 okindName demo-okind-1 select distinct pp.lastname, pp.firstname
▶	demo-8103	2023-08-30 09:06:52.657	@txid 4276189847602958291 pcode 5490 oname demo-8103 onodeName node-1 oid 633280970 okindName demo-okind-1 select distinct pp.lastname, pp.firstname
▶	demo-8103	2023-08-30 09:06:52.660	@txid -5273513173028476407 pcode 5490 oname demo-8103 onodeName node-1 oid 633280970 okindName demo-okind-1 select
▶	demo-8103	2023-08-30 09:06:52.658	@txid -4475135982985646809 pcode 5490 oname demo-8103 onodeName node-1 oid 633280970 okindName demo-okind-1 select tutorial_id, tutorial_title,
▶	demo-8103	2023-08-30 09:06:52.662	@txid -636988446309675660 pcode 5490 oname demo-8103 onodeName node-1 oid 633280970 okindName demo-okind-1 select productid, avg(orderqty) as averagequantity, sum(linetotal) as total
▶	demo-8103	2023-08-30 09:06:52.663	@txid 4276189847602958291 pcode 5490 oname demo-8103 onodeName node-1 oid 633280970 okindName demo-okind-1 select ename, job, sal + 100 from emp
▶	demo-8103	2023-08-30 09:06:52.662	@txid -7150002028998370687 pcode 5490 oname demo-8103 onodeName node-1 oid 633280970 okindName demo-okind-1 select (100-25)/15*(20-3) from dual
▶	demo-8103	2023-08-30 09:06:52.664	@txid -4475135982985646809 pcode 5490 oname demo-8103 onodeName node-1 oid 633280970 okindName demo-okind-1 select 'total income is', ((orderqty * unitprice) * (1.0 - unitpricediscount)), ' for ',
▶	demo-8103	2023-08-30 09:06:52.666	@txid -5273513173028476407 pcode 5490 oname demo-8103 onodeName node-1 oid 633280970 okindName demo-okind-1 select ename, job, sal + 100 from emp
▶	demo-8103	2023-08-30 09:06:52.667	@txid -636988446309675660 pcode 5490 oname demo-8103 onodeName node-1 oid 633280970 okindName demo-okind-1 select * into dbo.newproducts
▶	demo-8103	2023-08-30 09:06:52.668	@txid 4276189847602958291 pcode 5490 oname demo-8103 onodeName node-1 oid 633280970 okindName demo-okind-1 select distinct ename, deptno, sal, job from emp
▶	demo-8103	2023-08-30 09:06:52.668	@txid -7150002028998370687 pcode 5490 oname demo-8103 onodeName node-1 oid 633280970 okindName demo-okind-1 select corpus, count_corpus_words
▶	demo-8103	2023-08-30 09:06:52.671	@txid 6994271475421077751 pcode 5490 oname demo-8103 onodeName node-1 oid 633280970 okindName demo-okind-1 select productid, avg(orderqty) as averagequantity, sum(linetotal) as total

라이브 테일 메뉴에서 복잡한 로그들도 손쉽게 접근 가능합니다. 필요에 따라 필터 혹은 하이라이트 등의 기능을 활용해 실시간으로 조회할 수 있습니다. 로그 데이터 조회 주기는 2초입니다. 주요 용어는 다음과 같습니다.

- **Category:** 로그의 수집 및 조회 단위입니다.

- **Content:** 로그 메시지입니다.
- **Search Key:** 로그 파서 설정을 통해 생성합니다.
- **Tag:** 수집된 로그를 검색할 수 있는 검색 키입니다.

에이전트 옵션

에이전트 옵션이 설정된 경우 로그 레벨을 수집해 로그 레벨 기준 색상이 다음과 같이 표시됩니다.

```

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

! 에이전트 옵션 설정

- 에이전트 옵션은 다음과 같습니다.

```

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

- Java 에이전트 2.2.22 버전 이후부터 위빙 설정에 log4j-2.17 또는 logback-1.2.8 설정 시 사용할 수 있습니다. 에이전트 재시작이 필요합니다.
- 로그 레벨은 파싱된 키워드 중 [level], [type] 기준으로 판별합니다. [level], [type]으로 파싱된 키가 존재하고 파싱 값이 FATAL, CRITICAL, ERROR, WARN, WARNING, INFO를 포함할 경우 로그 레벨 색상을 표시합니다.

1 필터 영역

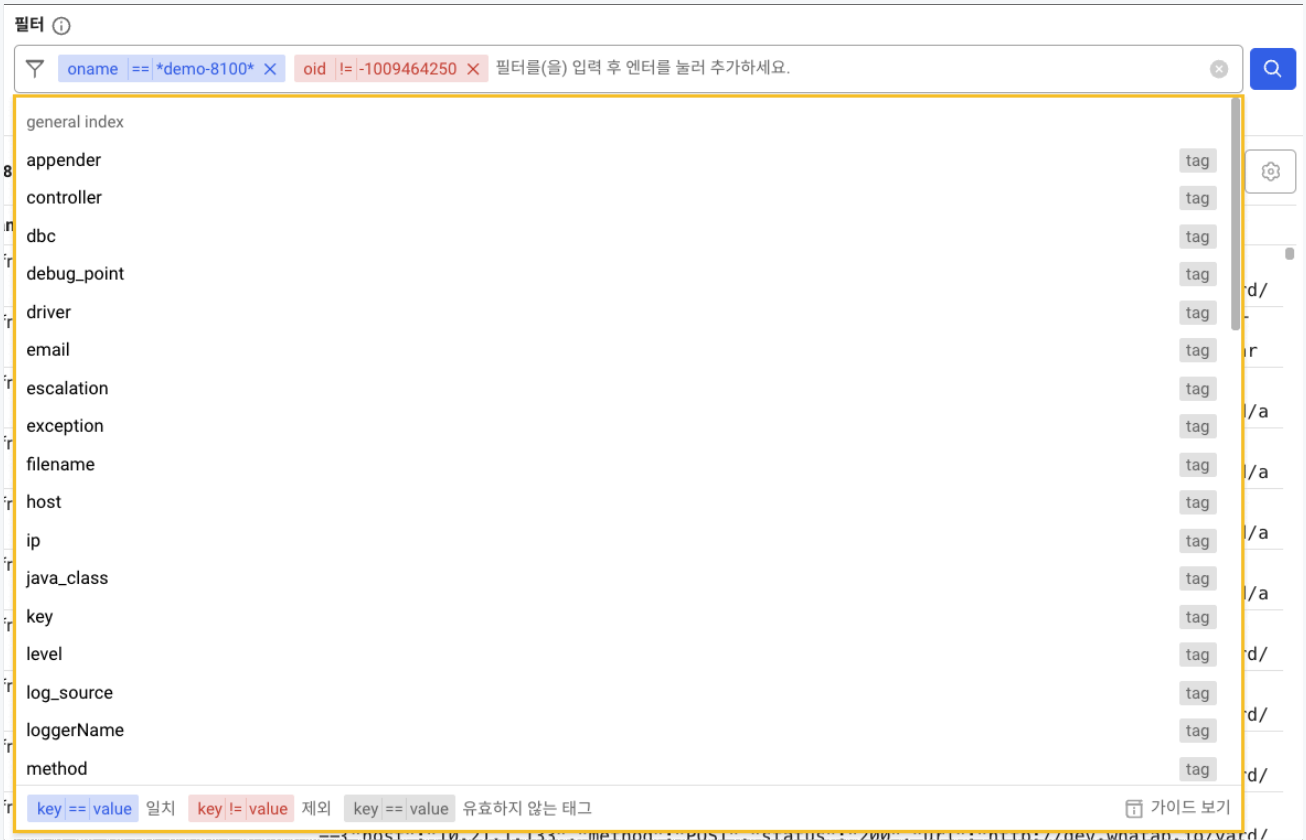
필터 적용

필터를 적용하면 입력한 조건에 맞는 로그를 필터링합니다. 복수의 필터를 입력할 수 있습니다. 필터의 태그가 같은 경우 OR(||)로, 그렇지 않은 경우는 AND(&&)로 적용됩니다.

입력 창에 값을 직접 입력하거나 필터 입력 창을 클릭해 필터를 지정할 수 있습니다. 필터 태그는 [검색 키], [연산자], [검색 값]의 순서로 입력합니다. 🔍 검색 버튼을 선택하면 필터가 적용된 데이터를 3 영역에서 조회할 수 있습니다.

① 가이드 UI

다음과 같이 입력 창 아래 가이드 UI를 제공합니다.



검색 키, 연산자, 검색 값 입력

- **검색 키** 입력 시 일반 인덱스, 예약어 인덱스, 숫자만 입력할 수 있는 인덱스를 구분해 추천 값을 제공합니다
- **연산자** 입력 시 일반 인덱스 검색 키의 경우 `==`, `!=` 옵션을 하단에 안내합니다. 숫자만 입력할 수 있는 인덱스의 경우 `>`, `<`, `<=`, `>=`, `==`, `!=` 옵션을 제공합니다.
- **검색 값** 입력 시 일치 검색(`>`, `<`, `<=`, `>=`, `==`)일 때 파란색으로, 제외 검색(`!=`)일 때 붉은색으로 하이라이팅합니다.
- **검색 값** 입력 시 대소문자 구분 옵션을 활용해 검색할 수 있습니다.

① 필터 태그가 2줄 이상 길어지는 경우 **접기** 아이콘을 선택해 접어둘 수 있습니다.

필터 태그 추가

- 입력 창에 텍스트를 입력하고 키보드의 Enter, Tab키를 통해 추가할 수 있습니다.
- 입력 창 아래 가이드 UI에서 추천 값을 클릭하여 추가할 수 있습니다.
- 입력 창 아래 가이드 UI에서 키보드의 위아래 방향키로 추천 값을 선택할 수 있고 Enter, Tab키로 태그를 추가할 수 있습니다.

필터 태그 제거

- Backspace로 삭제할 수 있습니다.
- 태그의 X 아이콘 선택 시 태그를 삭제할 수 있습니다.
- 입력 창의 전체 삭제 X 아이콘 선택 시 전체 태그를 삭제할 수 있습니다.

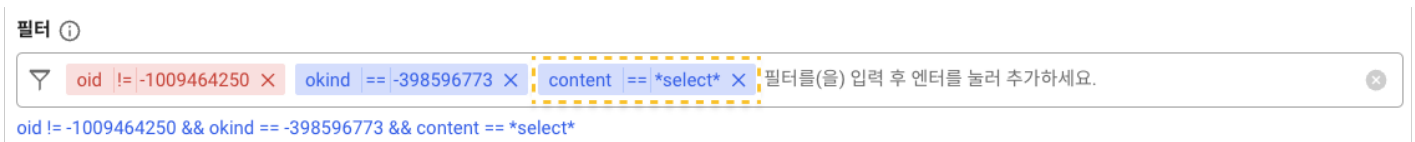
필터 적용 예외 상황

- 숫자만 입력할 수 있는 인덱스(.n으로 끝나는 검색 키)를 입력한 태그에서 검색 값은 숫자만 입력할 수 있습니다.
- 중복된 검색 키, 검색 값은 입력할 수 없습니다.
- 검색 키, 검색 값 중 하나라도 없는 태그가 존재할 때 검색할 수 없습니다. 유효하지 않는 태그의 경우 회색으로 표시합니다.

- ① 라이브 테일 검색 키로 category를 입력할 수 없습니다.
 - 입력된 필터 값 아래에 있는 수식(expression)은 로그 데이터 조회 시 적용될 필터 수식 미리 보기입니다.

미파싱 키워드 필터 적용

로그에서 파싱되지 않은 즉 인덱스가 생성되지 않은 키워드를 포함한 로그를 조회할 수 있습니다. 이 경우 지정 범위 내 모든 로그를 Full Scan합니다. 그렇기 때문에 인덱스가 생성된 키와 비교해 검색 속도가 다소 떨어질 수 있습니다. 정형화된 로그 데이터의 경우 [로그 파서 설정](#)을 통해 인덱스 키 값을 활용해 검색하는 것을 권장합니다.



1. **카테고리**를 선택하세요.
2. **필터** 입력창에 content 기준 띄어쓰기 후 검색을 원하는 키워드를 입력하세요.
 - 예시, content *select*

3. 🔍 검색 버튼을 클릭해 로그를 조회하세요.

- ① 라이브 테일의 경우 모든 로그 검색이 가능해 카테고리를 지정할 필요가 없습니다.
- 파서 설정에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

필터 수정

필터에 값을 입력한 뒤 입력한 값을 클릭하면 해당 값을 수정할 수 있습니다.



- 입력 창에 텍스트 재입력해 수정할 수 있습니다.
- 입력 창 아래 가이드 UI를 통해 추천 값을 선택해 수정할 수 있습니다.

검색 키(Search Key)

다음 이미지에서 파란색 박스 부분은 파싱(parsing)된 검색 키입니다. 검색 키는 [로그 설정](#)의 [로그 파서 설정](#) 탭에서 파싱 로직을 등록해 설정할 수 있습니다.

```

[date] 22/Aug/2022:03:16:47 +0000 [method] GET [ip] 116.32.201.189 [url] /MW/MyPage/mypageMain.tmall?
116.32.201.189 - - [22/Aug/2022:03:16:47 +0000] "GET /MW/MyPage/mypageMain.tmall?
    
```

필터 입력 문법

태그는 검색 키와 검색 값으로 구성되어있습니다. 다음의 예시에서 검색 키는 `exception`, 검색 값은 `UnknownHostException` 입니다. 해당 예시는 수집한 로그 데이터 중 IP 주소와 도메인 주소가 매칭되지 않아 서버를 호스트에 연결할 수 없을 경우 발생하는 예외(`UnknownHostException`)가 포함된 로그 데이터를 조회합니다.

```

▽ exception == UnknownHostException ×
    
```

검색 키 종류

검색 키 종류	검색 키 포맷	의미	검색 키와 검색 값 예시	검색 예시
문자열 키워드	keyword	파일 이름	- 키: fileName - 값: /data/whatap/logs/yard.log	fileName:/data/whatap/logs/yard.log
숫자 키워드	keyword.n	응답시간	- 키: response_time.n - 값: 2945	response_time.n>=2945
예약어 키워드 (사전 정의 키워드)	@keyword	트랜잭션 ID	- 키: @txid - 값: 85459614215434144	-
로그 본문 키워드	content	로그 본문	- 키: content - 값: 사용자 입력값	content: *ERROR*

ⓘ Content 검색 키

- Content 검색 키는 인덱싱되지 않은 로그의 본문을 대상으로 검색합니다. 예를 들어 `content *ERROR*` 와 같이 입력하는 경우 로그 본문 중 `ERROR` 를 포함한 로그를 검색합니다.
- 어떤 키워드로 인덱싱을 걸어야하는지 모르는 경우 Content 검색 키를 활용해 문제가 되는 키워드를 포함한 로그를 식별합니다. 이후 **로그 설정** 메뉴의 로그 파서 설정을 통해 해당 키워드로 파서를 설정해 인덱스를 생성하는 방식으로 검색 속도를 향상시킬 수 있습니다.

공통 문법

문법 종류	설명	예시
<code>==searchValue</code>	검색 값과 일치하는 로그를 검색합니다.	<code>exception==RuntimeExceptionexception</code>
<code>!=searchValue</code>	검색 값을 제외한 로그를 검색합니다.	<code>exception!=RuntimeException</code>
<code>*searchValue</code>	검색 값으로 끝나는 로그를 검색합니다.	<code>word==*hello</code>
<code>searchValue*</code>	검색 값으로 시작하는 로그를 검색합니다.	<code>word==hello*</code>
<code>*searchValue*</code>	검색 값으로 중간에 포함된 로그를 검색합니다.	<code>word==*hello*</code>
<code>*search*Value*</code>	검색 값으로 포함된 로그를 검색합니다.	<code>word==*he*llo*</code>
<code>re:{regexpr}</code>	정규표현식에 매칭되는 로그를 검색합니다.	<code>caller==re:^(i\.w\.a\.w\.s\.v\.r\.</code>
<code>**</code>	검색 키에 해당하는 모든 로그를 검색합니다.	

검색 키가 숫자 키워드(keyword.n)인 경우 문법

다음의 문법은 검색 키가 `keyword.n` 형식인 경우에만 지원합니다.

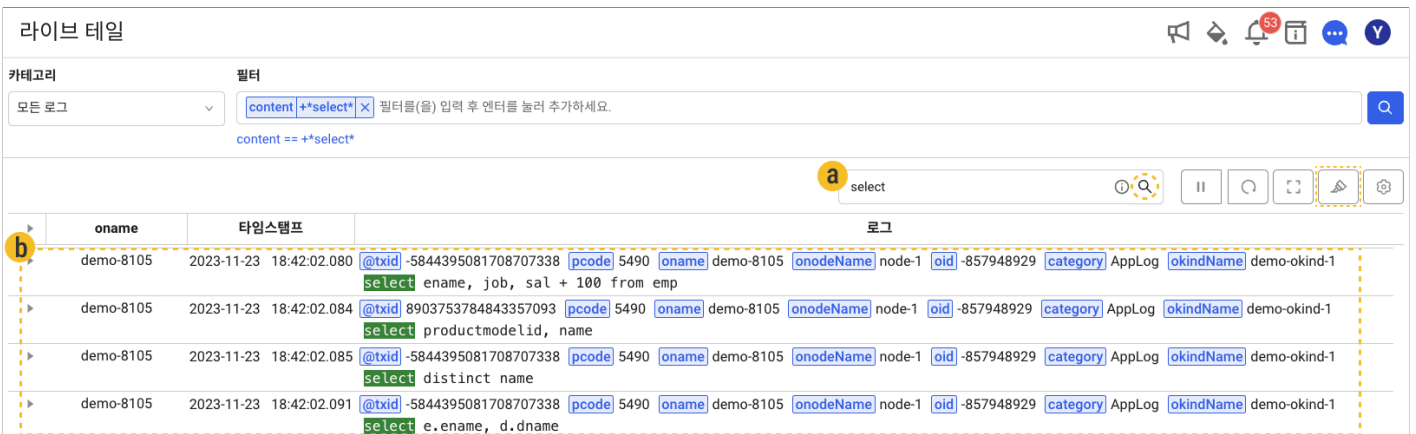
- 검색 값으로는 숫자만 올 수 있습니다.
- `.n` 키워드의 값에는 prefix를 붙이지 않습니다. `.n`이 아닌 키워드는 모두 prefix를 붙여야합니다.
예, `+>searchValue`는 유효하지 않습니다.

문법 종류	설명	예시
<code>>searchValue</code>	검색 값보다 큰 값이 포함된 로그를 조회합니다.	<code>response_time.n>3000</code>
<code>>=searchValue</code>	검색 값보다 크거나 같은 값이 포함된 로그를 조회합니다.	<code>response_time.n>=3000</code>

문법 종류	설명	예시
==searchValue	검색 값보다 같은 값이 포함된 로그를 조회합니다.	response_time.n==3000
!=searchValue	검색 값보다 다른 값이 포함된 로그를 조회합니다.	response_time.n!=3000
<searchValue	검색 값보다 작은 값이 포함된 로그를 조회합니다.	response_time.n<3000
<=searchValue	검색 값보다 작거나 같은 값이 포함된 로그를 조회합니다.	response_time.n<=3000

2 콘텐츠 하이라이트 영역

로그의 콘텐츠 중 원하는 키워드를 손쉽게 식별하기 위해 하이라이트 기능을 제공합니다.



- **a** 키워드 입력창에 하이라이트를 원하는 키워드를 입력 후 **Q 검색** 아이콘을 클릭하세요.
예시, `select`
- 예시 이미지와 같이 **b** 로그 목록에서 Content 내 키워드가 하이라이팅 됩니다.
- 단일 또는 복수 키워드로 필터를 걸 수 있습니다.
- **[] 전체 화면** 아이콘을 선택하면 **로그**와 **타임스탬프**를 전체 화면에서 확인할 수 있습니다.

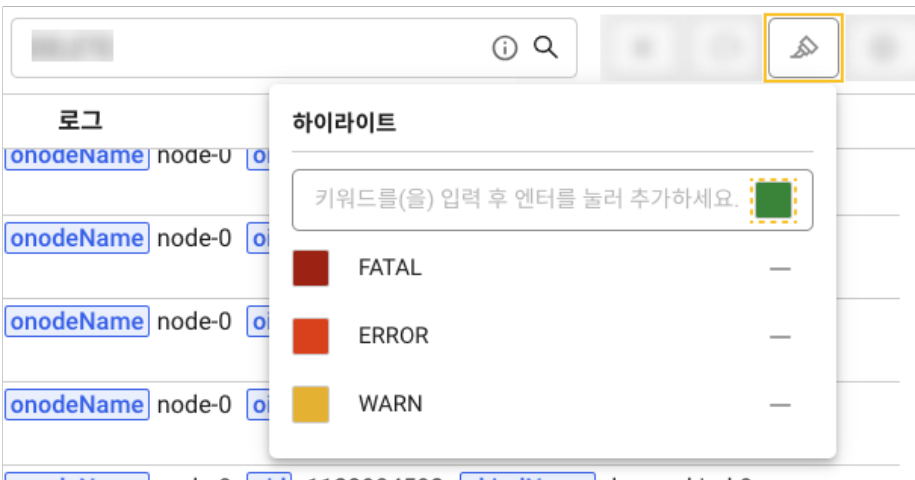
복수 키워드 조건

복수 키워드로 하이라이팅을 할 경우 다음과 같이 작성합니다.

입력 문자열	설명	결과
a b c	띄어쓰기로 각 키워드를 구분합니다.	a, b, c
"Whatap is good."	띄어쓰기를 키워드에 포함하고 싶은 경우 ' ' 또는 ""로 감쌉니다.	Whatap is good.
"Whatap\\ is good."	""로 감싸진 키워드에서 \ 를 포함할 경우, \\로 입력해야합니다.	Whatap\ is good.

하이라이트 색상 설정

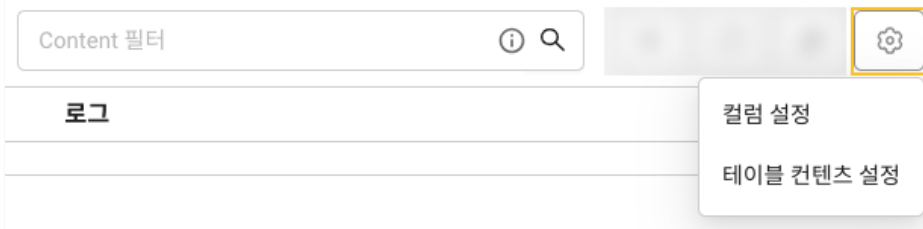
🔍 **하이라이트** 아이콘을 선택해 하이라이팅할 키워드 및 색상을 설정할 수 있습니다.



- 추가적으로 색상 설정을 원하는 키워드를 입력창에 입력하세요.
- 입력창 왼쪽 **색상** 클릭 시 선택할 수 있는 색상 메뉴가 나타납니다.
- 기본적으로 로그 레벨에 따른 하이라이팅(WARN, ERROR, FATAL)이 적용되어 있습니다.
- 설정한 내용은 **프로젝트 단위**로 저장됩니다.

테이블 설정

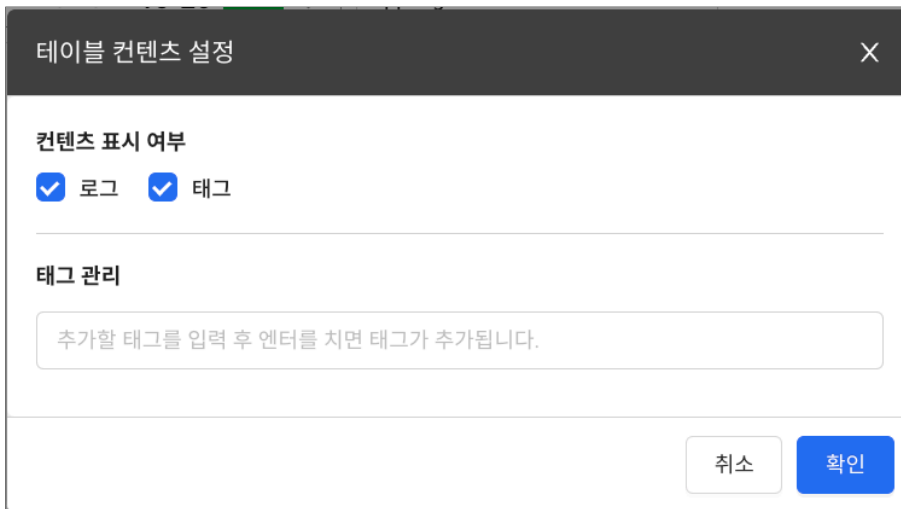
- ② 영역 오른쪽 **테이블 설정** 메뉴는 **라이브 테일**, **로그 검색**, **로그 트렌드**에서 사용할 수 있습니다.
- ⚙️ **테이블 설정** 버튼을 선택하면 **컬럼 추가**와 **테이블 콘텐츠 설정** 옵션 메뉴가 나타납니다.



1. 컬럼 설정

- **컬럼 추가:** 태그를 선택하여 테이블에 컬럼을 추가할 수 있습니다.
- **컬럼 순서 설정:** 컬럼을 추가하면 컬럼 순서 설정에 해당 컬럼이 추가됩니다. 원하는 컬럼을 드래그하여 컬럼의 순서를 변경하세요.

2. 테이블 설정



◦ **콘텐츠 표시 여부**

- 체크된 항목은 테이블에 표시되지 않습니다. 기본으로 **로그**, **태그** 모두 체크가 되어있으며 두 가지 항목 모두 표시합니다.
- 다음과 같이 **태그**를 해제할 경우 테이블에서 로그의 **태그**는 표시되지 않습니다.

```
@txid 2882146389875262493 pcode 5490 oname demo-8101 onodeName node-1 oid -877561626 okindName demo-okind-1
select distinct pp.lastname, pp.firstname
```

↓

```
select distinct pp.lastname, pp.firstname
```

◦ **태그 관리**

- 태그 관리 목록에 태그를 추가하면 추가한 순서대로 로그의 태그가 나열됩니다. 태그의 순서는 드래그하여 변경할 수 있습니다.

- 추가한 태그를 비활성화하면 비활성화한 태그는 로그의 태그에 노출되지 않습니다.

① 동일한 프로젝트 내 [라이브 테일](#), [로그 검색](#), [로그 트렌드](#) 메뉴는 테이블 설정을 공유합니다.

로그 트렌드

❗ 로그 조회 권한이 없을 경우 해당 메뉴에 진입할 수 없습니다.

홈 화면 > 프로젝트 선택 > 로그 > 로그 트렌드

로그 트렌드 메뉴에서 유형별로 분류된 로그의 발생 건수 추이를 통해 특정 에러 유형의 발생 패턴을 확인하고 시간별 상세 로그 데이터를 확인할 수 있습니다. 하이라이트 기능을 통해 원하는 로그를 빠르게 식별할 수 있습니다. 카테고리별로 수집된 로그의 추이를 조회할 수 있습니다. 주요 용어는 다음과 같습니다.

- **Category:** 로그의 수집 및 조회 단위입니다.
- **Content:** 로그 메시지입니다.
- **Search Key:** 로그 파서 설정을 통해 생성합니다.
- **Tag:** 수집된 로그를 검색할 수 있는 검색 키입니다.

로그 트렌드

시간 < 2024/01/10 17:00 ~ 2024/01/10 18:00 60분 >

카테고리 AppLog

1

필터

- > appender
- > controller
- > debug_point
- > email
- > exception
- > filename
- > host
- > ip
- > java_class
- > key
- > level
- > log_source
- > loggerName
- > method
- > namespace
- > oid
- > okind
- > okindName
- > oname

2024-01-10 17:00:00 1min 전체 109,971건 조회

키워드(를) 입력해주세요

▶	oname	타임스탬프	로그
▶	ote-front	2024-01-10 17:00:00.433	referer http://devote.whatap.io/v2/project/database/878/db_dashboard pcode 13 oid 397157872 --{"host":"10.21.3.57","method":"POST","status":"200","url":"http://devote.whatap.io/y
▼	ote-front	2024-01-10 17:00:00.433	referer https://dev.whatap.io/v2/project/apm/13/transaction_map @txid -7828986607631991285 method GET pcode 13 level INFO oid 397157872 status_nxx status_2xx okind -398596773 threadName XNIO-1 task-4 url http://dev.whatap.io/yard/api responseTime.n 10 oname ote-front agentime 1704873600202 host 10.21.3.57 status.success.n 1 @mtid 2306616107552506289 category AppLog loggerName ACCESS okindName group-front email sa@whatap.io status 200 --{"host":"10.21.3.57","method":"GET","status":"200","url":"http://dev.whatap.io/yard/ap i","referer":"https://dev.whatap.io/v2/project/apm/13/transaction_map","email":"sa@whata p.io","responseTime.n":10}--
▶	ote-front	2024-01-10 17:00:00.433	referer https://dev.whatap.io/v2/project/apm/2216/dashboard pcode 13 oid 397157872 okind -398596773 --{"host":"10.21.1.133","method":"POST","status":"200","url":"http://dev.whatap.io/yard/
▶	ote-front	2024-01-10 17:00:00.433	referer https://dev.whatap.io/v2/project/apm/2216/dashboard @txid -7177366797654501422 method POST --{"host":"10.21.1.133","method":"POST","status":"200","url":"http://dev.whatap.io/yard/
▶	ote-front	2024-01-10 17:00:00.433	referer https://dev.whatap.io/v2/project/apm/2216/dashboard pcode 13 oid 397157872 okind -398596773 --{"host":"10.21.1.133","method":"POST","status":"200","url":"http://dev.whatap.io/yard/
▶	ote-front	2024-01-10 17:00:00.433	referer https://dev.whatap.io/v2/project/apm/2216/dashboard @txid -3688468993623540252 method POST --{"host":"10.21.1.133","method":"POST","status":"200","url":"http://dev.whatap.io/yard/
▶	ote-front	2024-01-10 17:00:00.434	referer https://dev.whatap.io/v2/project/apm/8/transaction_map pcode 13 oid 397157872 okind -398596773

309

데이터 조회하기

- 스크롤이 바닥에 닿으면 다음 데이터를 조회합니다.
- ①에서 탐색할 로그 데이터의 **시간**과 수집 단위인 **카테고리**를 지정합니다.
- **카테고리**를 변경하면 선택된 카테고리에 해당하는 로그를 조회합니다. ② 바 차트와 ③ 로그 테이블에서 확인할 수 있습니다.
- ② 바 차트의 막대를 클릭하면 막대의 시간 범위에 해당하는 로그를 조회합니다.
- ③ 로그 테이블 상단 왼쪽에서 조회한 총 로그 개수를 확인할 수 있습니다.
- ③ 로그 테이블 상단 오른쪽 [] **전체 화면** 아이콘을 선택하면 **로그**와 **타임스탬프**를 전체 화면에서 확인할 수 있습니다.
- ④ 사이드 메뉴에서 태그로 필터를 걸어서 로그를 확인할 수 있습니다. 검색 키는 2개까지 선택할 수 있고, 검색값은 복수 개 선택이 가능합니다.
- **에이전트 옵션이 설정된 경우** 로그 레벨을 수집해 로그 레벨 기준 색상이 다음과 같이 표시됩니다.

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

! 에이전트 옵션 설정

- 에이전트 옵션은 다음과 같습니다.

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

- Java 에이전트 2.2.22 버전 이후부터 위빙 설정에 log4j-2.17 또는 logback-1.2.8 설정 시 사용할 수 있습니다. 에이전트 재시작이 필요합니다.
- 로그 레벨은 파싱된 키워드 중 [level], [type] 기준으로 판별합니다. [level], [type] 으로 파싱된 키가 존재하고 파싱 값이 **FATAL**, **CRITICAL**, **ERROR**, **WARN**, **WARNING**, **INFO**를 포함할 경우 로그 레벨 색상을 표시합니다.

로그 Content 확인하기

! Content란?

Content는 로그 메시지를 의미합니다.

- 로그 컬럼의 첫 번째 줄은 로그의 파싱(parsing)된 키와 값이고 두 번째 줄은 로그의 Content입니다.
- 3 로그 테이블의 행(로그)마다 ▶ **더보기** 버튼이 있습니다. ▶ **더보기** 버튼을 선택하면 5처럼 해당 로그의 전체 content를 확인할 수 있습니다.

차트로 로그 조회하기

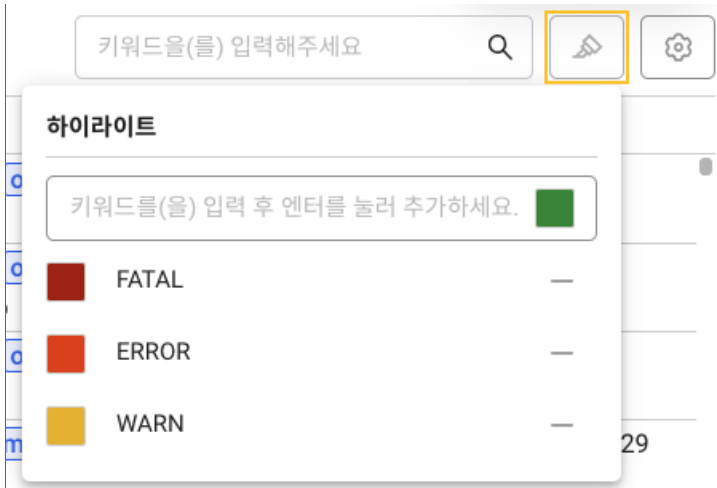


- 바 차트에서 a 원하는 시간을 클릭하여 해당 시간의 로그를 확인할 수 있습니다.
- 바 차트 아래 로그 테이블 상단 왼쪽의 b 시간 선택 옵션을 이용해 다음과 같이 선택한 시간대에서 더 세분화해 로그를 검색할 수 있습니다.

- 1min: interval (차트의 막대 사이 간격)
- 시간 선택 옵션: 선택된 시간 범위를 6개의 구간으로 나눈 시간대

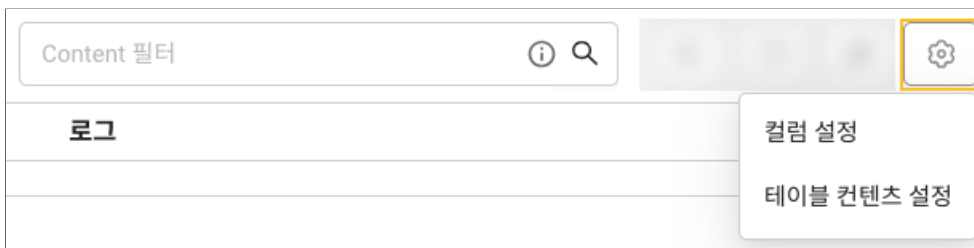
하이라이트

- 원하는 키워드를 손쉽게 식별할 수 있도록 하이라이트 기능을 제공합니다.
- **3** 영역 오른쪽 **입력창**에 하이라이트 할 키워드를 입력하세요. 다음과 같이 하이라이팅 된 키워드를 확인할 수 있습니다.



테이블 설정하기

- **3** 영역 오른쪽 **테이블 설정** 메뉴는 **라이브 테일**, **로그 검색**, **로그 트렌드**에서 사용할 수 있습니다.
- **테이블 설정** 버튼을 선택하면 **컬럼 추가**와 **테이블 콘텐츠 설정** 옵션 메뉴가 나타납니다.



1. 컬럼 설정

- **컬럼 추가**: 태그를 선택하여 테이블에 컬럼을 추가할 수 있습니다.
- **컬럼 순서 설정**: 컬럼을 추가하면 컬럼 순서 설정에 해당 컬럼이 추가됩니다. 원하는 컬럼을 드래그하여 컬럼의 순서를 변경하세요.

2. 테이블 설정



테이블 콘텐츠 설정

콘텐츠 표시 여부

로그 태그

태그 관리

추가할 태그를 입력 후 엔터를 치면 태그가 추가됩니다.

취소 확인

◦ 콘텐츠 표시 여부

- 체크된 항목은 테이블에 표시되지 않습니다. 기본으로 **로그**, **태그** 모두 체크가 되어있으며 두 가지 항목 모두 표시합니다.
- 다음과 같이 **태그**를 해제할 경우 테이블에서 로그의 **태그**는 표시되지 않습니다.

```
@txid 2882146389875262493 pcode 5490 oname demo-8101 onodeName node-1 oid -877561626 okindName demo-okind-1
select distinct pp.lastname, pp.firstname
```

↓

```
select distinct pp.lastname, pp.firstname
```

◦ 태그 관리

- 태그 관리 목록에 태그를 추가하면 추가한 순서대로 로그의 태그가 나열됩니다. 태그의 순서는 드래그하여 변경할 수 있습니다.
- 추가한 태그를 비활성화하면 비활성화한 태그는 로그의 태그에 노출되지 않습니다.

① 동일한 프로젝트 내 **라이브 테일**, **로그 검색**, **로그 트렌드** 메뉴는 테이블 설정을 공유합니다.

로그 검색

① 로그 조회 권한이 없을 경우 해당 메뉴에 진입할 수 없습니다.

홈 화면 > 프로젝트 선택 > 로그 > 로그 검색

로그 검색 메뉴에서 통합 수집된 대량의 로그를 다양한 조건으로 검색하고 사용자가 원하는 로그를 특정할 수 있습니다. 복수의 검색 조건을 파싱된 키와 밸류로 지정할 수 있어 원하는 조건에 일치하는 로그 데이터만 추출합니다.

동적 페이지로 검색된 로그 데이터를 정해진 라인 단위로 가져오며, 스크롤 등에 의해 하단에 닿으면 자동으로 다음 데이터를 가져와 표시합니다. 주요 용어는 다음과 같습니다.

- **Category:** 로그의 수집 및 조회 단위입니다.
- **Content:** 로그 메시지입니다.
- **Search Key:** 로그 파서 설정을 통해 생성합니다.
- **Tag:** 수집된 로그를 검색할 수 있는 검색 키입니다.

1 로그 검색

시간: < 2023/07/03 13:16 ~ 2023/07/03 14:16 60분 > 필터 (을) 입력 후 엔터를 눌러 추가하세요.

2 [AppLog, AppStdErr, AppStdOut, VirtualLog] 필터링 메뉴

3 전체 4,532,168건 조회 | Timestamp | 과거 순 | 최근 순 | 키워드(을) 입력해주세요

oname	타임스탬프	로그
dev3679006-8091	2023-07-03 13:16:00.000	@@txid -2717737560424755676 pcode 8 oname dev3679006-8091 onodeName node-1 oid 777628269 category AppLog insert into emp values
dev3679007-8092	2023-07-03 13:16:00.001	@@txid -4707233158811724771 pcode 8 oname dev3679007-8092 onodeName node-0 oid 2081171570 category AppLog select ename, deptno, sal + comm from emp
dev3679006-8091	2023-07-03 13:16:00.002	@@txid -7559227993102384977 pcode 8 oname dev3679006-8091 onodeName node-1 oid 777628269 category AppLog okindName dev-okind-1 okind 867318026 onode 334634079 select distinct pp.lastname, pp.firstname from person.person pp join humanresources.employee e on e
dev3679007-8092	2023-07-03 13:16:00.002	@@txid 5627186231377631605 pcode 8 oname dev3679007-8092 onodeName node-0 oid 2081171570 category AppLog http://127.0.0.1:8092/remote/order/kill/employee/pusan status=200
dev3679011-8095	2023-07-03 13:16:00.002	@@txid -6614897519727834472 pcode 8 oname dev3679011-8095 onodeName node-1 oid -1840884360 category AppLog select distinct pp.lastname, pp.firstname
dev3679007-8092	2023-07-03 13:16:00.004	@@txid -959317925843459419 pcode 8 oname dev3679007-8092 onodeName node-0 oid 2081171570 category AppLog select ename, 1000 from emp
dev3679007-8092	2023-07-03 13:16:00.005	@@txid 5627186231377631605 pcode 8 oname dev3679007-8092 onodeName node-0 oid 2081171570 category AppLog okindName dev-okind-0 okind 1152715164 onode 1693789385 update table set x=1 where key=1 elapsed=2ms
dev3679007-8092	2023-07-03 13:16:00.006	@@txid -4707233158811724771 pcode 8 oname dev3679007-8092 onodeName node-0 oid 2081171570 category AppLog select ename, deptno, sal, job from emp
dev3679007-8092	2023-07-03 13:16:00.007	@@txid 5627186231377631605 pcode 8 oname dev3679007-8092 onodeName node-0 oid 2081171570 category AppLog delete from posts
dev3679006-8091	2023-07-03 13:16:00.008	@@txid -7559227993102384977 pcode 8 oname dev3679006-8091 onodeName node-1 oid 777628269 category AppLog select
dev3679011-8095	2023-07-03 13:16:00.008	@@txid -6614897519727834472 pcode 8 oname dev3679011-8095 onodeName node-1 oid -1840884360 category AppLog select e.ename, d.dname
dev3679006-8091	2023-07-03 13:16:00.013	@@txid -7559227993102384977 pcode 8 oname dev3679006-8091 onodeName node-1 oid 777628269 category AppLog select
dev3679011-8095	2023-07-03 13:16:00.013	@@txid -6614897519727834472 pcode 8 oname dev3679011-8095 onodeName node-1 oid -1840884360 category AppLog select productmodelid, name
dev3679007-8092	2023-07-03 13:16:00.016	@@txid 8725913945553755591 pcode 8 oname dev3679007-8092 onodeName node-0 oid 2081171570 category AppLog http://127.0.0.1:8092/remote/edu/save/dept/daejun status=200
dev3679007-8092	2023-07-03 13:16:00.017	@@txid 5479838888404626132 pcode 8 oname dev3679007-8092 onodeName node-0 oid 2081171570 category AppLog select distinct pp.lastname, pp.firstname
dev3679007-8092	2023-07-03 13:16:00.018	@@txid -6044091401645216416 pcode 8 oname dev3679007-8092 onodeName node-0 oid 2081171570 category AppLog http://127.0.0.1:8092/remote/account/create/unit/jeju status=200
dev3679006-8091	2023-07-03 13:16:00.019	@@txid -7559227993102384977 pcode 8 oname dev3679006-8091 onodeName node-1 oid 777628269 category AppLog select * from emp
dev3679011-8095	2023-07-03 13:16:00.019	@@txid -6614897519727834472 pcode 8 oname dev3679011-8095 onodeName node-1 oid -1840884360 category AppLog select productmodelid, name

4 로그 내용 상세보기

데이터 조회하기

- 스크롤이 바닥에 닿으면 다음 데이터를 조회합니다. 한 번에 10,000개의 로그를 조회합니다.
- **3** 로그 테이블 상단 왼쪽에서 조회한 총 로그 개수를 확인할 수 있습니다.
- 로그 데이터를 시간 순과 역순으로 조회할 수 있습니다. **3** 로그 테이블 상단 오른쪽에서 **Timestamp** 과거 순과 **최근 순** 중 원하는 조회 방식을 선택하세요.
- 시간 범위 지정 후 **적용** 버튼을 선택 해 조회 시간을 설정하고 **Q** 검색 버튼을 선택해 데이터를 조회합니다.
- **3** 로그 테이블 상단 오른쪽 **[] 전체 화면** 아이콘을 선택하면 **로그**와 **타임스탬프**를 전체 화면에서 확인할 수 있습니다.
- **에이전트 옵션이 설정된 경우** 로그 레벨을 수집해 로그 레벨 기준 색상이 다음과 같이 표시됩니다.

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

① 에이전트 옵션 설정

- 에이전트 옵션은 다음과 같습니다.

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

- Java 에이전트 2.2.22 버전 이후부터 위빙 설정에 log4j-2.17 또는 logback-1.2.8 설정 시 사용할 수 있습니다. 에이전트 재시작이 필요합니다.
- 로그 레벨은 파싱된 키워드 중 [level], [type] 기준으로 판별합니다. [level], [type] 으로 파싱된 키가 존재하고 파싱 값이 FATAL, CRITICAL, ERROR, WARN, WARNING, INFO를 포함할 경우 로그 레벨 색상을 표시합니다.

로그 Content 확인하기

① Content란?

Content는 로그 메시지를 의미합니다.

- 로그 컬럼의 첫 번째 줄은 로그의 파싱(parsing)된 키와 값이고 두 번째 줄은 로그의 Content입니다.
- ③ 로그 테이블의 행(로그)마다 ▶ [더보기](#) 버튼이 있습니다. ▶ [더보기](#) 버튼을 선택하면 ④ 처럼 해당 로그의 전체 Content를 확인할 수 있습니다.
- 로그의 태그를 선택하면 복사, 검색, 제외 검색, 인접 로그 검색을 할 수 있는 드롭다운 메뉴가 나타납니다.

필터

필터 적용

1 왼쪽 **시간 선택창**에서 시간 범위를 지정할 수 있습니다. 오른쪽에서 필터를 적용하면 입력한 조건에 맞는 로그를 필터링합니다. 복수의 필터를 입력할 수 있습니다. 필터의 태그가 같은 경우 OR(||)로, 그렇지 않은 경우는 AND(&&)로 적용됩니다.

입력 창에 값을 직접 입력하거나 **필터** 입력 창을 클릭해 필터를 지정할 수 있습니다. 필터 태그는 **검색 키**, **연산자**, **검색 값**의 순서로 입력합니다. **검색** 버튼을 선택하면 필터가 적용된 데이터를 **3** 영역에서 조회할 수 있습니다.

가이드 UI

다음과 같이 입력 창 아래 **가이드 UI**를 제공합니다.

The screenshot shows a filter input field with the following content: `oname == *demo-8100* x oid != -1009464250 x`. Below the input field is a list of filterable fields, each with a corresponding tag:

Field Name	Tag
general index	
appender	tag
controller	tag
dbc	tag
debug_point	tag
driver	tag
email	tag
escalation	tag
exception	tag
filename	tag
host	tag
ip	tag
java_class	tag
key	tag
level	tag
log_source	tag
loggerName	tag
method	tag

At the bottom of the guide UI, there are instructions for filter syntax: `key == value` 일치, `key != value` 제외, `key == value` 유효하지 않는 태그. A "가이드 보기" (View Guide) button is also present.

검색 키, 연산자, 검색 값 입력

- **검색 키** 입력 시 일반 인덱스, 예약어 인덱스, 숫자만 입력할 수 있는 인덱스를 구분해 추천 값을 제공합니다
- **연산자** 입력 시 일반 인덱스 검색 키의 경우 `==`, `!=` 옵션을 하단에 안내합니다. 숫자만 입력할 수 있는 인덱스의 경우 `>`, `<`, `<=`, `>=`, `==`, `!=` 옵션을 제공합니다.
- **검색 값** 입력 시 일치 검색(`>`, `<`, `<=`, `>=`, `==`)일 때 **파란색**으로, 제외 검색(`!=`)일 때 **붉은색**으로 하이라이팅합니다.
- **검색 값** 입력 시 대소문자 구분 옵션을 활용해 검색할 수 있습니다.

① 필터 태그가 2줄 이상 길어지는 경우 **접기** 아이콘을 선택해 접어들 수 있습니다.

필터 태그 추가

- 입력 창에 텍스트를 입력하고 키보드의 Enter, Tab키를 통해 추가할 수 있습니다.
- 입력 창 아래 **가이드 UI**에서 추천 값을 클릭하여 추가할 수 있습니다.
- 입력 창 아래 **가이드 UI**에서 키보드의 위아래 방향키로 추천 값을 선택할 수 있고 Enter, Tab키로 태그를 추가할 수 있습니다.

필터 태그 제거

- Backspace로 삭제할 수 있습니다.
- 태그의 **X** 아이콘 선택 시 태그를 삭제할 수 있습니다.
- 입력 창의 전체 삭제 **X** 아이콘 선택 시 전체 태그를 삭제할 수 있습니다.

필터 적용 예외 상황

- 숫자만 입력할 수 있는 인덱스(`.n`으로 끝나는 **검색 키**)를 입력한 태그에서 **검색 값**은 숫자만 입력할 수 있습니다.
- 중복된 **검색 키**, **검색 값**은 입력할 수 없습니다.
- **검색 키**, **검색 값** 중 하나라도 없는 태그가 존재할 때 검색할 수 없습니다. 유효하지 않는 태그의 경우 회색으로 표시합니다.

미파싱 키워드 필터 적용

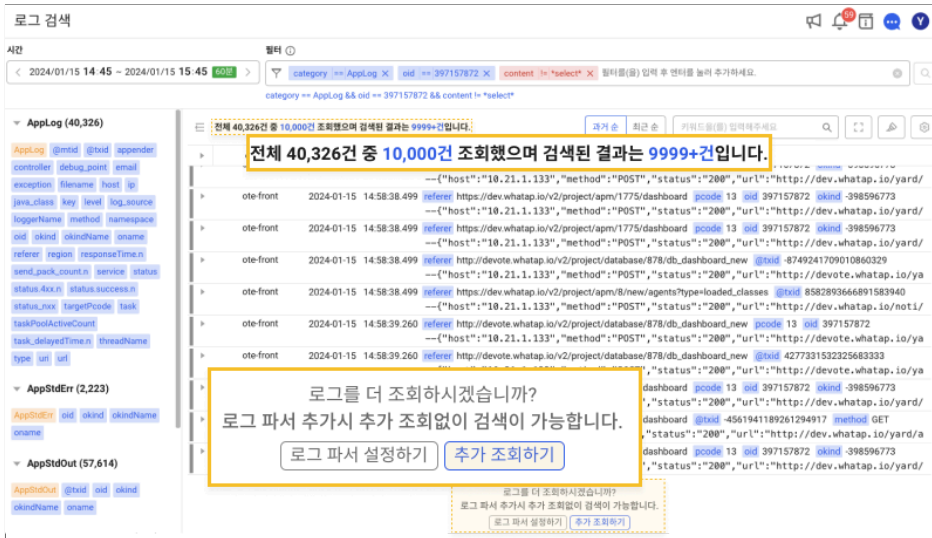
로그에서 파싱되지 않은 즉 인덱스가 생성되지 않은 키워드를 포함한 로그를 조회할 수 있습니다. 이 경우 지정 범위 내 모든 로그를 Full Scan합니다. 그렇기 때문에 인덱스가 생성된 키와 비교해 검색 속도가 다소 떨어질 수 있습니다. 정형화된 로그 데이터의 경우 **로그 파서 설정**을 통해 인덱스 키 값을 활용해 검색하는 것을 권장합니다.

필터 ⓘ

필터를(을) 입력 후 엔터를 눌러 추가하세요.

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

1. **카테고리**를 선택하세요. 카테고리 지정이 필수적입니다.
2. **필터** 입력창에 `content` 기준 띄어쓰기 후 검색을 원하는 키워드를 입력하세요.
예시, `content *select*`
3. 🔍 **검색** 버튼을 클릭해 로그를 조회하세요. 전체 로그 중 일부 먼저 조회합니다. 1회당 검색 결과는 최대 1만 건입니다.
4. 스크롤을 내려 하단의 **추가 조회하기** 버튼 선택 시 추가 조회할 수 있습니다.



- ① 전체 로그 중 서버 조회 범위 당 1만 건씩 조회합니다. 서버 조회 범위의 경우 기본 20만 건이지만 전체 로그 양에 따라 비율이 달라질 수 있습니다.
- 파서 설정에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

필터 수정

필터에 값을 입력한 뒤 입력한 값을 클릭하면 해당 값을 수정할 수 있습니다.



- 입력 창에 텍스트 재입력해 수정할 수 있습니다.
- 입력 창 아래 가이드 UI를 통해 추천 값을 선택해 수정할 수 있습니다.

검색 키(Search Key)

검색 키는 로그 데이터 내에서 원하는 특정 값에 접근하기 위한 식별자를 의미합니다. 검색 키에 해당하는 실제 데이터가 검색 값입니다. 왼쪽 2 영역에 있는 태그는 카테고리별로 파싱(parsing) 된 검색 키입니다. 태그를 선택하여 필터를 입력할 수 있습니다. 주황색 태그는 카테고리, 파란색 태그는 검색 키입니다.

예를 들어 2 영역의 AppLog와 AppStdOut은 카테고리, 그 아래 oid와 같은 태그는 파싱(parsing) 된 검색 키입니다. 검색 키는 로그 > 로그 설정의 로그 파서 설정 탭에서 파싱 로직을 등록해 설정할 수 있습니다.

필터 입력 문법

태그는 검색 키와 검색 값으로 구성되어있습니다. 다음의 예시에서 검색 키는 exception, 검색 값은 UnknownHostException 입니다. 해당 예시는 수집한 로그 데이터 중 IP 주소와 도메인 주소가 매칭되지 않아 서버를 호스트에 연결할 수 없을 경우 발생하는 예외(UnknownHostException)가 포함된 로그 데이터를 조회합니다.

exception == UnknownHostException X

검색 키 종류

검색 키 종류	검색 키 포맷	의미	검색 키와 검색 값 예시	검색 예시
문자열 키워드	keyword	파일 이름	- 키: fileName - 값: /data/whatap/logs/yard.log	fileName:/data/whatap/logs/yard.log
숫자 키워드	keyword.n	응답시간	- 키: response_time.n - 값: 2945	response_time.n>=2945
예약어 키워드 (사전 정의 키워드)	@keyword	트랜잭션 ID	- 키: @txid - 값: 85459614215434144	-

공통 문법

문법 종류	설명	예시
==searchValue	검색 값과 일치하는 로그를 검색합니다.	exception==RuntimeExceptionexception
!=searchValue	검색 값을 제외한 로그를 검색합니다.	exception!=RuntimeException
*searchValue	검색 값으로 끝나는 로그를 검색합니다.	word==*hello
searchValue*	검색 값으로 시작하는 로그를 검색합니다.	word==hello*
searchValue	검색 값으로 중간에 포함된 로그를 검색합니다.	word==*hello*
*search*Value*	검색 값으로 포함된 로그를 검색합니다.	word==*he*llo*
re:{regexpr}	정규표현식에 매칭되는 로그를 검색합니다.	caller==re:^i\.w\.a\.w\.s\.v\.r\.

문법 종류	설명	예시
**	검색 키에 해당하는 모든 로그를 검색합니다.	

검색 키가 숫자 키워드(keyword.n)인 경우 문법

다음의 문법은 검색 키가 `keyword.n` 형식인 경우에만 지원합니다.

- 검색 값으로는 숫자만 올 수 있습니다.
- `.n` 키워드의 값에는 prefix를 붙이지 않습니다. `.n` 이 아닌 키워드는 모두 prefix를 붙여야합니다.
예, `+>searchValue` 는 유효하지 않습니다.

문법 종류	설명	예시
<code>>searchValue</code>	검색 값보다 큰 값이 포함된 로그를 조회합니다.	<code>response_time.n>3000</code>
<code>>=searchValue</code>	검색 값보다 크거나 같은 값이 포함된 로그를 조회합니다.	<code>response_time.n>=3000</code>
<code>==searchValue</code>	검색 값보다 같은 값이 포함된 로그를 조회합니다.	<code>response_time.n==3000</code>
<code>!=searchValue</code>	검색 값보다 다른 값이 포함된 로그를 조회합니다.	<code>response_time.n!=3000</code>
<code><searchValue</code>	검색 값보다 작은 값이 포함된 로그를 조회합니다.	<code>response_time.n<3000</code>
<code><=searchValue</code>	검색 값보다 작거나 같은 값이 포함된 로그를 조회합니다.	<code>response_time.n<=3000</code>

로그 태그 옵션

로그 태그 선택 시 다음과 같이 드롭다운 메뉴가 나타납니다. [검색](#), [제외 검색](#), [인접 로그](#) 옵션을 확인할 수 있습니다.

▶ 2023-09-07 15:06:00.002	@txid -3761935652943885420	pcode 5490	oname demo-8103	onodeName node-1	oid 633280970	category AppLog
▶ 2023-09-07 15:06:00.002	@txid -8799764694958745204	pcode 5490		onodeName node-1	oid 633280970	category AppLog
▶ 2023-09-07 15:06:00.003	@txid 5498362167526616791	pcode 5490		onodeName node-0	oid 1387800924	category AppLog
▶ 2023-09-07	@txid 3613588890639779125	pcode 5490		onodeName node-0	oid 1387800924	category AppLog

- 검색

검색 옵션을 선택하면 **필터**에 해당 태그가 포함('=') 조건으로 입력됩니다.

- 제외 검색

제외 검색 옵션을 선택하면 **필터**에 해당 태그가 제외('!=') 조건으로 입력됩니다.

- 인접 로그

인접 로그 옵션을 선택하면 **인접 로그** 상세 창이 나타납니다. 선택한 로그의 서버를 대상으로 선택한 로그와 인접한 시간대의 로그를 조회합니다. **시간 선택** 버튼을 클릭해 인접한 시간대의 로그를 조회할 수 있습니다. 기존 로그는 파란색 바탕으로 표시됩니다.

인접 로그
✕

시간 선택

밀리초 초 분

적용된 서버

demo-8101

	타임스탬프	로그
▶	2023-09-07 15:24:59.995	@txid -8789311500480722351 pcode 5490 oname demo-8101 onodeName node-1 oid -877561626 category AppLog select distinct ename, deptno, sal, job from emp
▶	2023-09-07 15:24:59.998	@txid 3991620568819529441 pcode 5490 oname demo-8101 onodeName node-1 oid -877561626 category AppLog select distinct pp.lastname, pp.firstname
▶	2023-09-07 15:25:00.001	@txid -8789311500480722351 pcode 5490 oname demo-8101 onodeName node-1 oid -877561626 category AppLog select quantity, max(price)
▶	2023-09-07 15:25:00.007	@txid 3991620568819529441 pcode 5490 oname demo-8101 onodeName node-1 oid -877561626 category AppLog select ename, sal=sal+1000 from emp
▶	2023-09-07 15:25:00.007	@txid -8789311500480722351 pcode 5490 oname demo-8101 onodeName node-1 oid -877561626 category AppLog select
▶	2023-09-07 15:25:00.014	@txid -8789311500480722351 pcode 5490 oname demo-8101 onodeName node-1 oid -877561626 category AppLog select
▶	2023-09-07 15:25:00.022	@txid 3991620568819529441 pcode 5490 oname demo-8101 onodeName node-1 oid -877561626 category AppLog select ename, deptno, sal + comm from emp
▶	2023-09-07 15:25:00.022	@txid -8789311500480722351 pcode 5490 oname demo-8101 onodeName node-1 oid -877561626 category AppLog select
▶	2023-09-07 15:25:00.022	@txid 3823483774615642623 pcode 5490 oname demo-8101 onodeName node-1 oid -877561626 category AppLog select productid
▶	2023-09-07 15:25:00.029	@txid 3823483774615642623 pcode 5490 oname demo-8101 onodeName node-1 oid -877561626 category AppLog select

닫기

콘텐츠 하이라이트

로그의 콘텐츠 중 원하는 키워드를 손쉽게 식별하기 위해 하이라이트 기능을 제공합니다.

로그 검색

시간 < 2024/01/10 16:59 ~ 2024/01/10 17:59 60분 > 필터 ① category == AppLog X content == *select* X 필터를(을) 입력 후 엔터를 눌러 추가하세요.

category == AppLog && content == *select*

AppLog (107,548) AppStdErr (2,016) AppStdOut (57,562)

전체 107,548건 중 100,000건 조회했으며 검색된 결과는 1,090건입니다. [과거 순] [최근 순] select

oname	타임스탬프	로그
ote-front	2024-01-10 16:59:37.633	<pre> --{"responseTime.n":1754,"controller":"io.whatap.server.front.web.controller.rest.call.YardApiController#yardApiFlushPost(YardApiParamsV2, HttpSession, HttpServletResponse, HttpServletRequest)","method":"POST","pcode":"1816","uri":"/yard/api/flush","status":200}--{"type":"mxml","pcode":1816,"params":{"pcode":1816,"stime":1704872974126,"etime":1704873574126,"trigger":0,"mql":"HEADER { mem_working_set\$: \"B\" }\\nCATEGORY {\\\"container\\\":6h, \\\"container{m5}\\\":3d, \\\"container{h1}\\\":unlimit }\\nTAGLOAD { backward: true }\\nINJECT default\\nSELECT [time, pcode, mem_working_set]\\nGROUP { timeunit:5s, pk:\\\"pcode\\\" }\\nUPDATE { key: \\\"mem_working_set\\\", value: sum }\\nFIRST-ONLY { key: pcode }","param":{"stime":1704873574126},"inject":{"default":{"FILTER { key:containerId, value: \\\"431dd5f42bf0d3d9fd42c144181967c9fc0ebd7865aa6adcab5978c146c3bcef\\\" }}},"path":"text","authKey":""} </pre>

- a 키워드 입력창에 하이라이트를 원하는 키워드를 입력 후 **Q 검색** 아이콘을 클릭하세요.
 예시, select
- 예시 이미지와 같이 b 로그 목록에서 Content 내 키워드가 하이라이팅 됩니다.
- 단일 또는 복수 키워드로 필터를 걸 수 있습니다.
- [] 전체 화면 아이콘을 선택하면 **로그**와 **타임스탬프**를 전체 화면에서 확인할 수 있습니다.

복수 키워드 조건

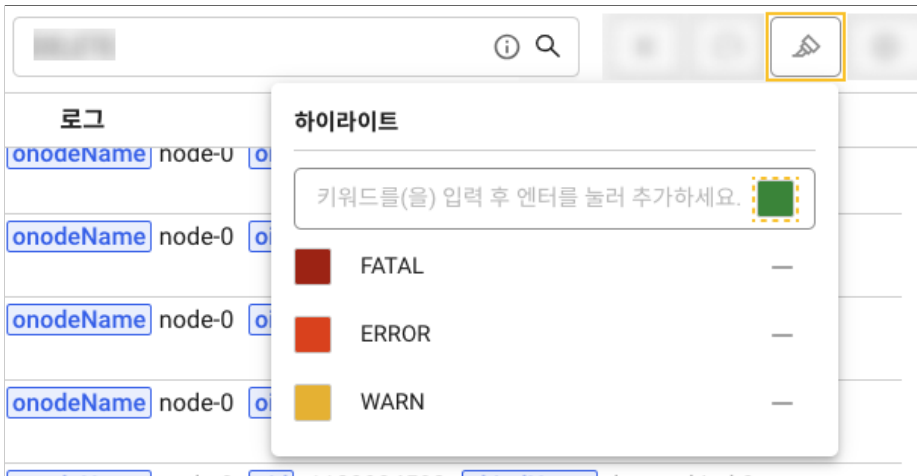
복수 키워드로 하이라이팅을 할 경우 다음과 같이 작성합니다.

입력 문자열	설명	결과
a b c	띄어쓰기로 각 키워드를 구분합니다.	a, b, c

입력 문자열	설명	결과
"Whatap is good."	띄어쓰기를 키워드에 포함하고 싶은 경우 ' ' 또는 ""로 감쌉니다.	Whatap is good.
"Whatap\\ is good."	""로 감싸진 키워드에서 \를 포함할 경우, \\로 입력해야 합니다.	Whatap\ is good.

하이라이트 색상 설정

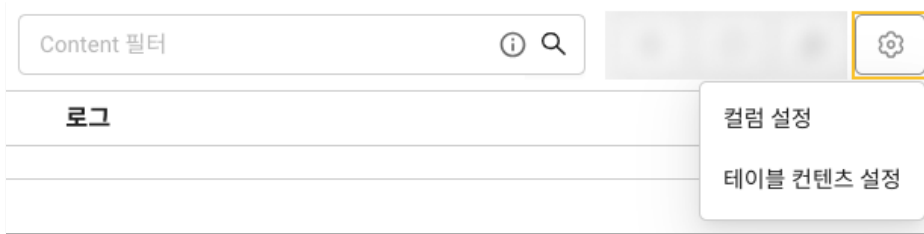
🔍 **하이라이트** 아이콘을 선택해 하이라이팅할 키워드 및 색상을 설정할 수 있습니다.



- 추가적으로 색상 설정을 원하는 키워드를 입력창에 입력하세요.
- 입력창 왼쪽 **색상** 클릭 시 선택할 수 있는 색상 메뉴가 나타납니다.
- 기본적으로 로그 레벨에 따른 하이라이팅(WARN, ERROR, FATAL)이 적용되어 있습니다.
- 설정한 내용은 **프로젝트** 단위로 저장됩니다.

테이블 설정하기

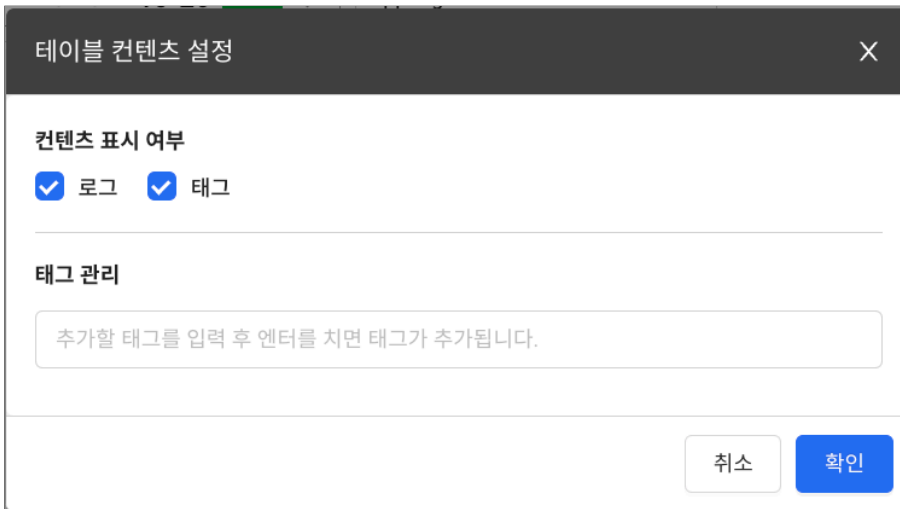
- ③ 영역 오른쪽 **테이블 설정** 메뉴는 **라이브 테일**, **로그 검색**, **로그 트렌드**에서 사용할 수 있습니다.
- ⚙️ **테이블 설정** 버튼을 선택하면 **컬럼 추가**와 **테이블 콘텐츠 설정** 옵션 메뉴가 나타납니다.



1. 컬럼 설정

- **컬럼 추가:** 태그를 선택하여 테이블에 컬럼을 추가할 수 있습니다.
- **컬럼 순서 설정:** 컬럼을 추가하면 컬럼 순서 설정에 해당 컬럼이 추가됩니다. 원하는 컬럼을 드래그하여 컬럼의 순서를 변경하세요.

2. 테이블 설정



◦ **콘텐츠 표시 여부**

- 체크된 항목은 테이블에 표시되지 않습니다. 기본으로 **로그**, **태그** 모두 체크가 되어있으며 두 가지 항목 모두 표시합니다.
- 다음과 같이 **태그**를 해제할 경우 테이블에서 로그의 **태그**는 표시되지 않습니다.

```
@txid 2882146389875262493 pcode 5490 oname demo-8101 onodeName node-1 oid -877561626 okindName demo-okind-1
select distinct pp.lastname, pp.firstname
```

↓

select distinct pp.lastname, pp.firstname

◦ **태그 관리**

- 태그 관리 목록에 태그를 추가하면 추가한 순서대로 로그의 태그가 나열됩니다. 태그의 순서는 드래그하여 변경할 수 있습니다.

- 추가한 태그를 비활성화하면 비활성화한 태그는 로그의 태그에 노출되지 않습니다.

① 동일한 프로젝트 내 [라이브 테일](#), [로그 검색](#), [로그 트렌드](#) 메뉴는 테이블 설정을 공유합니다.

알림 설정하기

홈 화면 > 프로젝트 선택 > 경고 알림 > 이벤트 설정 > 로그 탭

수집한 로그 데이터를 조건에 맞춰 필터링해 경고 알림을 설정할 수 있습니다. + 이벤트 추가 버튼을 선택해 로그 이벤트 경고 알림을 설정하세요. 모든 설정을 완료한 다음 저장 버튼을 선택하세요.

이벤트 설정

실시간 로그 이벤트
JSON
+ 이벤트 추가

이벤트 이름	카테고리	검색 키	검색 값	이벤트 발생 일시 중지	이벤트 대상 필터링	이벤트 수신 태그
실시간 로그 이벤트	AppLog	onodeName	node-0	20분	onode == '334634079' && okindName != 'demo-okind-1'	test-tag
이벤트 테스트	AppLog	oid	-1128904592	사용 안 함	사용 안 함	전체 멤버 수신
test	AppLog	oname	demo-8100	사용 안 함	oname && 'demo-8100'	전체 멤버 수신

복합 로그 이벤트
JSON
+ 이벤트 추가

이벤트 이름	템플릿	카테고리	규칙	이벤트 상태가 해결되면 추가 알림	이벤트 발생 일시 중지	인터벌	이벤트 수신 태그
이벤트 이름_테스트	2xx 상태코드 건수 count	AppLog	include_minus_exclude_count > 10	Off	1분	5분	전체 멤버 수신
retreter	사용 안 함	#WhatapEvent	rows > 10	Off	1분	5분	전체 멤버 수신
test	사용 안 함	*	rows > 10	Off	1분	5분	전체 멤버 수신

추가할 수 있는 로그 이벤트 다음과 같습니다.

- **실시간 로그 이벤트** : 실시간으로 수집한 로그에서 검색 값이 등장하면 경고 알림을 보냅니다.
- **복합 로그 이벤트** : 최근에 수집한 로그 중 일정 조건을 만족하는 로그가 일정 개수 이상 수집한 경우에 경고 알림을 보냅니다.

- ⓘ • 이벤트를 추가하거나 설정하려면 **알림 설정** 권한이 있어야 합니다. 사용자별 권한에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.
 - 경고 알림과 관련해 모니터링 플랫폼별 지원되는 이벤트 종류를 확인하려면 [다음 문서](#)를 참조하세요.

이벤트 추가 공통 옵션

다음은 이벤트 추가 시 공통으로 설정할 수 있는 옵션입니다.

- **이벤트 이름** : 추가하려는 이벤트 이름을 입력하세요.
- **이벤트 활성화** : 토글 버튼을 클릭해 경고 알림 활성화 여부를 선택할 수 있습니다.
- **레벨** : **위험**, **경고**, 정보 중 하나의 레벨을 선택하세요.
- **메시지** : 이벤트 발생 시 출력하는 알림 메시지를 입력합니다. `#{태그 또는 필드키}` 입력으로 메시지에 변수를 적용할 수 있습니다. 변수에 입력할 키는 선택한 매트릭스 데이터 **카테고리**에 포함된 값이어야 합니다.
- **카테고리** : 로그 구분 명칭(로그 폴더명)을 목록에서 선택하거나 직접 입력할 수 있습니다.
- **이벤트 발생 일시 중지** : 과도한 경고 알림 발생을 방지할 수 있는 옵션입니다. 첫 번째 경고 알림 이후 선택한 시간 동안 경고 알림을 보내지 않습니다. 또한 **이벤트 기록** 메뉴에 기록되지 않습니다.
- **이벤트 수신 태그** : 이벤트 수신 태그를 선택하면 해당 태그를 가진 프로젝트 멤버와 3rd-party 플러그인에 알림을 전송할 수 있습니다. 이벤트 수신 태그를 선택하지 않으면 프로젝트 전체 멤버에게 경고 알림을 보냅니다.

태그를 추가하지 않으면 전체 멤버에게 경고 알림을 보냅니다. **+ 태그 추가**를 클릭한 다음 **태그 목록**에서 경고 알림 수신 대상을 선택하세요. **+ 새 태그 생성**을 선택해 태그를 추가할 수도 있습니다.

ⓘ 경고 알림 > 이벤트 수신 설정 메뉴에서 프로젝트 멤버와 3rd-party 플러그인에 태그를 설정할 수 있습니다. **이벤트 수신 설정** 메뉴에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

실시간 로그 이벤트 추가

이벤트 추가

이벤트 이름 *

이벤트 활성화



레벨 *

메시지 *

카테고리 ⓘ *

검색 키 *

검색 값 *

입력된 단어가 일치하는 경우 알림이 발생합니다.

이벤트 대상 필터링 ⓘ

 선택 입력

 직접 입력

입력값이 없을 경우, 실시간으로 수정

 선택 입력

 직접 입력

+ 추가

ex. oid == '12345678' && level == 'ERROR'

이벤트 발생 일시 중지 *

알림 수신 후 선택한 시간 동안 이벤트가 발생하지 않습니다.

단, "이벤트 상태가 해결되면 추가 알림" 기능을 활성화한 경우에는 RECOVERED 알림 수신 후 선택한 시간 동안 이벤트가 발생하지 않습니다.

이벤트 수신 태그 ⓘ

전체 멤버 수신 + 태그 추가

[프로젝트 이벤트 수신설정 메뉴 바로가기](#)

저장

- **검색 키** : 로그 데이터 내에서 특정 값에 접근하기 위한 식별자를 의미합니다. 목록에서 선택하거나 직접 입력할 수 있습니다.

예시, HTTP 응답 상태 코드를 나타내는 값에 접근하고자 할 경우 **검색 키** `status`

- **검색 값** : **검색 키**에 해당하는 실제 데이터를 의미합니다. 로그에서 입력한 단어를 포함할 경우 경고 알림을 보냅니다. 목록에서 선택하거나 직접 입력할 수 있습니다.

예시, **검색 키** `status` **검색 값** `200`을 설정한 경우 HTTP 응답 상태 코드 200을 포함하는 로그 데이터 수집 시 경고 알림 발생

- **이벤트 대상 필터링** : **선택 입력** 옵션을 통해 **검색 키**와 **연산자**, **검색 값**을 선택해 대상을 필터링하거나 **직접 입력** 옵션을 선택할 수 있습니다. 입력값이 없을 경우 실시간으로 수집하는 데이터 전체에 대한 알림 발생 여부를 판단합니다.

예시, `AppLog` 카테고리의 로그 중 `level` 이 `ERROR`인 로그를 찾습니다. 일치하는 로그 중에서 `oid`가 `12345678`인 경우 경고 알림을 보냅니다.

복합 로그 이벤트 추가

✕ 이벤트 추가

***이벤트 이름**

이벤트 활성화

레벨 위험 경고 정보 이벤트 상태가 해결되면 추가 알림 ⓘ

템플릿 사용 안 함

***메시지**

***카테고리 ⓘ**

사용 안 함

- 2xx 상태코드 건수 count
- 3xx 상태코드 건수 count
- 4xx 상태코드 건수 count
- 5xx 상태코드 건수 count
- 정상 상태코드(2xx,3xx) 건수 count
- 에러 상태코드(4xx,5xx) 건수 count
- 에러 수신 건수 count

데이터 조회 범위 최근에 1 분 ▼
선택 시간동안 수집된 로그를 조회합니다.

로그 검색 조건 ⓘ **선택 입력** **직접 입력**
 ▼ ▼ **제외** —
+ 추가
이벤트 발행 조건을 입력하기 위해서 카테고리를 먼저 선택해 주세요.

***이벤트 발행 조건** 조건에 맞는 로그 > ▼ 10

인터벌 ⓘ 5 분 ▼

무음 ⓘ 1 분 ▼

이벤트 수신 태그 ⓘ 전체 멤버 수신 + 태그 추가

저장

- **템플릿** : 복합 로그 템플릿을 제공합니다.
- **로그 검색 조건**
 - **검색 키**에서 이벤트 발생 조건 대상을 선택할 수 있습니다. 선택한 **검색 키**에 해당하는 검색 값을 선택할 수 있습니다.
 - **검색 키**에서 동일한 항목을 추가할 경우 'OR' 조건으로, 다른 항목을 추가할 경우 'AND' 조건으로 동작합니다.
 - **제외** 체크 박스를 선택해 선택한 검색 값을 이벤트 발행 조건에서 제외할 수 있습니다.
 - **+ 추가**를 선택해 여러개의 이벤트 발행 조건을 추가 또는 제외 설정할 수 있습니다.
- **데이터 조회 범위** : 선택한 시간동안 수집한 로그를 조회합니다. 데이터 조회 시간을 5분으로 선택하면 최근 5분 동안 수집한 데이터를 조회해서 이벤트 발생 조건을 확인합니다.
- **이벤트 발행 조건** : 이벤트가 입력한 횟수와 선택한 연산자의 조건과 같이 발생할 때 경고 알림을 보냅니다.

예시, AppLog 카테고리의 로그 중 조건 입력에 해당하는 로그를 필터링 합니다. 조건 입력에서 **제외**를 체크한 경우 해당 조건으로 찾은 로그를 제외하겠다는 의미입니다. 따라서 level 이 ERROR 인 로그는 제외합니다. 최근 10분 동안 수집한 로그 중 이벤트가 5 보다 작을 경우 경고 알림을 보냅니다.

로그 이벤트 설정 수정하기

1. **경고 알림 > 이벤트 설정** 메뉴로 이동하세요.
2. **로그** 탭을 선택하세요.
3. 로그 이벤트 목록 중 수정하려는 이벤트 항목에서 오른쪽에 ✎ 버튼을 선택하세요.
4. **이벤트 설정** 창이 나타나면 옵션을 수정한 다음 **저장** 버튼을 선택하세요.

선택한 로그 이벤트를 삭제하려면 이벤트 설정 창에서 오른쪽 위에 **삭제** 버튼을 선택하세요.




로그 이벤트 끄기

1. **경고 알림 > 이벤트 설정** 메뉴로 이동하세요.
2. **로그** 탭을 선택하세요.
3. 로그 이벤트 목록 중 경고 알림을 끄려는 이벤트 항목의 가장 오른쪽에 토글 버튼을 선택하세요.

다시 토글 버튼을 선택하면 해당 경고 알림이 활성화됩니다.

로그 이벤트 내보내기/불러오기

로그 이벤트의 설정 내용을 json 파일로 저장한 다음 불러와 재사용할 수 있습니다.

1. 경고 알림 > 이벤트 설정 메뉴로 이동하세요.
2. 로그 탭을 선택하세요.
3. 로그 이벤트 목록 위에 JSON  버튼을 선택하세요. JSON 내보내기 창이 나타납니다.
4. 내보내기 할 항목을 수정 또는 편집하세요.
5. 오른쪽 위에  내보내기 버튼을 선택하세요. 브라우저에서 json 파일을 다운로드합니다.
6. 로그 이벤트 목록 위에  버튼을 선택하세요.
7. 파일 선택 창이 나타나면 앞서 다운로드 받은 json 파일을 선택하세요.
8. JSON 가져오기 창이 나타나면 내용을 수정한 다음 + 목록에 추가하기 버튼을 선택하세요.

❗ 이벤트에 id가 존재합니다. id를 제거한 뒤 다시 시도하세요.

- 메시지가 나타나면 JSON 가져오기 창에서 id 항목을 삭제한 다음 + 목록에 추가하기 버튼을 선택하세요.
- 기존의 이벤트 항목에 덮어쓰기를 하려면 id 항목을 삭제한 다음 덮어쓰기 버튼을 선택하세요.

경고 알림 수신 설정

홈 화면 > 프로젝트 선택 > 경고 알림 > 이벤트 수신 설정

프로젝트 멤버들의 경고 알림 수신과 관련한 다양한 기능을 설정할 수 있습니다.

이벤트 수신 설정



▼ 사용자별 이벤트 수신 설정 (64)

이벤트 알림의 일괄 수신설정 및 접근 설정을 위한 모바일 기기 관리는 [계정 정보 메뉴](#)에서 가능합니다. [계정 정보 >](#)

이름	이메일 알림	SMS 알림	WhatsApp 알림	모바일 알림	반복 알림 (에스컬레이션)	이벤트 수신 태그
JH	<input checked="" type="checkbox"/> 수신 레벨: 위임	<input type="checkbox"/> 수신 레벨: 위임	등록된 번호가 없습니다.	<input type="checkbox"/> 모바일 기기 6대 수신 레벨: 전체	0 저장	<input type="checkbox"/> 수신 태그 미설정 알림 받기 testtag 테스트 태그 +
JT	<input checked="" type="checkbox"/> 수신 레벨: 전체	<input type="checkbox"/> 수신 레벨: 전체	등록된 번호가 없습니다.	등록된 기기가 없습니다.	0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 + 태그 추가
JU	<input checked="" type="checkbox"/> 수신 레벨: 전체	등록된 번호가 없습니다.	등록된 번호가 없습니다.	등록된 기기가 없습니다.	0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 + 태그 추가
KJ	<input type="checkbox"/> 수신 레벨: 전체	<input type="checkbox"/> 수신 레벨: 전체	등록된 번호가 없습니다.	등록된 기기가 없습니다.	0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 + 태그 추가
KY	<input checked="" type="checkbox"/> 수신 레벨: 전체	<input type="checkbox"/> 수신 레벨: 전체	등록된 번호가 없습니다.	등록된 기기가 없습니다.	0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 + 태그 추가
	<input checked="" type="checkbox"/> 수신 레벨: 전체	<input type="checkbox"/> 수신 레벨: 전체	등록된 번호가 없습니다.	등록된 기기가 없습니다.	0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기

3rd 파티 플러그인

Slack, Telegram, Teams, Jandi, Webhook 등을 이용하여 알림 메시지를 받으실 수 있습니다.

플러그인 이름	인증 키	인증 값	반복 알림 (에스컬레이션)	이벤트 수신 태그
SLACK			0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 + 태그 추가
SLACK			0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 + 태그 추가
SLACK			0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 + 태그 추가
SLACK			0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 + 태그 추가
TELEGRAM			0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 PREV_TEST +
WEBHOOK_JSON			0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 + 태그 추가

➕ 추가하기

대량 알림 발생 방지

알림이 대량으로 발생하면 지정된 시간 동안 알림이 일시적으로 중지됩니다.
대량 알림 차단 기능을 해제하려면 (이메일 주소 옆의) '중단 해제' 버튼을 눌러주세요.

활성화

탐지 시간: 5분

탐지 횟수: 10

정지 시간: 3시간

저장

수신 수단 선택하기

이메일 알림 이외에 SMS, 모바일 알림을 선택할 수 있습니다. 원하는 알림 수신 수단의 체크 박스를 체크하면 경고 알림을 받을 수 있습니다. 알림 수신 수단의 체크 박스를 해제하면 경고 알림을 보내지 않습니다.

- ① • 이메일 알림은 회원 가입 시 입력한 이메일 주소로 알림을 보냅니다.
 - 프로젝트 최고 관리자를 제외한 모든 사용자는 자신의 수신 설정만 변경할 수 있습니다.

SMS 알림 수신 추가하기

SMS 알림 수신이 필요한 경우 [계정 관리](#)에서 사용자 전화번호를 설정하세요.

사용자 전화번호

전화번호는 경고 알림 문자에 사용됩니다. 전화번호를 변경하려면 SMS 인증이 필요합니다.

전화번호
 인증 완료

일반 휴대전화는 **한국 휴대전화 번호만 등록** 가능합니다.

1. 화면 오른쪽 위에 프로필 아이콘을 선택하세요.
2. 팝업 메뉴가 나타나면 [계정 관리](#) 버튼을 선택하세요.
3. [사용자 전화번호](#) 섹션에서 [일반 휴대전화](#) 버튼을 선택하세요.
4. [전화번호](#)에 인증번호를 수신할 전화번호를 입력하세요.
5. [인증번호 전송](#) 버튼을 선택하세요.
6. 사용자의 휴대전화로 전송된 인증 번호를 입력하세요.
7. [인증하기](#) 버튼을 선택하세요.

- ① • 등록된 전화번호를 변경하려면 [번호 변경하기](#) 버튼을 선택한 다음 위의 과정을 반복하세요.
 - SMS를 알림으로 수신할 수 있는 전화번호는 **한국 휴대전화 번호만** 등록할 수 있습니다.

WhatsApp 알림 수신 추가하기

WhatsApp을 통해 알림을 수신할 수 있습니다.

사용자 전화번호

전화번호는 경고 알림 문자에 사용됩니다. 전화번호를 변경하려면 SMS 인증이 필요합니다.

전화번호

1. 화면 오른쪽 위에 프로필 아이콘을 선택하세요.
2. 팝업 메뉴가 나타나면 **계정 관리** 버튼을 선택하세요.
3. **사용자 전화번호** 섹션에서 **WhatsApp** 버튼을 선택하세요.
4. **전화번호**에 인증번호를 수신할 전화번호를 입력하세요.
5. **인증번호 전송** 버튼을 선택하세요.
6. WhatsApp 애플리케이션으로 전송된 인증번호 6자리를 입력하세요.
7. **인증하기** 버튼을 선택하세요.

ⓘ 등록된 전화번호를 변경하려면 **번호 변경하기** 버튼을 선택한 다음 위의 과정을 반복하세요.

수신 레벨 선택하기

경고 알림 레벨에 따라 알림 수신 여부를 선택할 수 있습니다. **사용자별 이벤트 수신 설정** 섹션의 사용자 목록에서 **수신 레벨**을 **전체** 또는 **위험**을 선택하세요.

- **전체**: 모든 경고 알림을 수신할 수 있습니다.
- **위험**: 위험 레벨의 경고 알림만 수신할 수 있습니다.

요일 및 시간별 알람 설정하기

요일별, 시간별 알림 수신 여부를 선택할 수 있습니다. **사용자별 이벤트 수신 설정** 섹션의 사용자 목록에서 가장 왼쪽에 **▼** 버튼을 선택하세요. 경고 알림 수신을 원하는 요일을 선택하거나 시간을 입력하세요. 알림 수신 수단별로 설정할 수 있습니다.

▼ 사용자별 이벤트 수신 설정 (64)

이벤트 알림의 일괄 수신설정 및 접근 설정을 위한 모바일 기기 관리는 [계정 정보 메뉴에서](#) 가능합니다. [계정 정보 >](#)

이름	이메일 알림	SMS 알림	WhatsApp 알림	모바일 알림	반복 알림 (에스컬레이션)	이벤트 수신 태그
HS	<input checked="" type="checkbox"/> 수신 레벨: 전체	<input type="checkbox"/> 0***** 등록된 번호가 없습니다.	<input type="checkbox"/>	<input type="checkbox"/> 모바일 기기 2대 수신 레벨: 전체	0 저장	<input checked="" type="checkbox"/> 수신 태그 미설정 알림 받기 + 태그 추가
알림 수신 언어	요일 <input checked="" type="checkbox"/> 월 <input checked="" type="checkbox"/> 화 <input checked="" type="checkbox"/> 수 <input checked="" type="checkbox"/> 목 <input checked="" type="checkbox"/> 금 <input checked="" type="checkbox"/> 토 <input checked="" type="checkbox"/> 일 시간 00:00 ~ 00:00	요일 <input checked="" type="checkbox"/> 월 <input checked="" type="checkbox"/> 화 <input checked="" type="checkbox"/> 수 <input checked="" type="checkbox"/> 목 <input checked="" type="checkbox"/> 금 <input checked="" type="checkbox"/> 토 <input checked="" type="checkbox"/> 일 시간 00:00 ~ 00:00	요일 <input checked="" type="checkbox"/> 월 <input checked="" type="checkbox"/> 화 <input checked="" type="checkbox"/> 수 <input checked="" type="checkbox"/> 목 <input checked="" type="checkbox"/> 금 <input checked="" type="checkbox"/> 토 <input checked="" type="checkbox"/> 일 시간 00:00 ~ 00:00	모바일 기기 테스트	테스트	

경고 알림 반복 설정하기

경고 알림 발생 시간으로부터 알림 발생 상황이 해소되지 않을 경우 최초 알림 발생 시각으로부터의 알림 반복 간격을 설정할 수 있습니다. 예를 들어, 경고 알림 발생 시간으로부터 0분(즉시), 1시간 후, 1일 후에 경고 알림을 반복하려면 '0,1H,1D'를 [반복 알림 \(에스컬레이션\)](#) 컬럼 항목에 입력하세요.

반복 알림 (에스컬레이션) ⓘ

0,1H,1D 저장

- ⓘ • 이 기능은 **Critical** (또는 **위험**) 등급의 모든 이벤트를 대상으로 합니다. 이벤트 추가 시 설정한 **레벨** 항목을 참조하세요.
- **M**: 분, **H**: 시간, **D**: 일, 단위를 생략하면 분 단위로 시간을 설정합니다.
- **저장** 버튼을 선택하지 않으면 설정을 완료할 수 없습니다.
- 숫자 또는 숫자+단위(**M**, **H**, **D**)로 입력하세요. 입력이 올바르지 않으면 메시지가 표시됩니다.

팀별, 사용자별 알림 설정하기

프로젝트의 멤버 중 특정 멤버 또는 팀을 대상으로 알림 수신 여부를 설정합니다. [메트릭스](#) 및 [이상치 탐지](#), [로그](#) 이벤트 설정의 [이벤트 수신 태그](#) 항목에서 태그를 추가하세요. 이벤트별로 경고 알림을 수신하는 멤버 또는 팀을 선택할 수 있습니다.

반대로 이벤트 수신 태그를 설정하지 않으면 전체 멤버에게 경고 알림을 보낼 수 있습니다.

> 이벤트 수신 태그 사용 예시

이벤트 수신 태그에 대한 사용 예시를 통해 팀별 또는 사용자별로 경고 알림을 전송하는 설정 방법에 대해 알아봅니다. 다음과 같이 팀 별로 서로 다른 경고 알림을 전송하도록 설정합니다.

알림 종류	서버팀 수신 여부	데브옵스팀 수신 여부
메트릭스 경고 알림	O	X
이상치 탐지 경고 알림	O	O
로그 실시간 경고 알림	X	O

1. 이벤트 수신 설정하기 (경고 알림 > 이벤트 수신 설정)



프로젝트에 속한 멤버들 중 서버팀 소속은 **서버팀**, 데브옵스팀 소속은 **데브옵스팀** 으로 이벤트 수신 태그를 설정하세요.

2. 메트릭스 경고 알림 설정하기 (경고 알림 > 이벤트 설정 > 메트릭스 > 이벤트 추가 > 이벤트 수신 설정)

이벤트 수신 태그

Server +

이벤트 설정 시 이벤트 수신 태그를 선택하여 해당 태그를 가진 프로젝트 멤버와 3rd-party 플러그인에 알림을 전송할 수 있습니다.
이벤트 수신 설정 메뉴에서 프로젝트 멤버와 3rd-party 플러그인에 각각 태그를 지정할 수 있습니다

[프로젝트 이벤트 수신설정 메뉴](#)

이벤트 설정 시 태그를 선택하지 않은 경우 프로젝트 이벤트 수신 설정 메뉴의 나머지 수신 조건(활성화 여부 등)에 따라 알림이 발생합니다.

[태그 추가](#) 또는 + 버튼을 클릭하세요. 태그 목록에서 원하는 태그를 선택하거나 새 태그를 생성하세요. 메트릭스 이벤트에 대한 알림을 `서버팀`으로 설정한 경우입니다.

3. 로그 실시간 경고 알림 설정 (경고 알림 > 이벤트 설정 > 로그 > 이벤트 추가 > 이벤트 수신 태그)

이벤트 수신 태그 ⓘ

DevOps +

[프로젝트 이벤트 수신설정 메뉴 바로가기](#)

[태그 추가](#) 또는 + 버튼을 클릭하세요. 태그 목록에서 원하는 태그를 선택하거나 새 태그를 생성하세요. 로그 실시간 이벤트에 대한 알림을 `데브옵스팀`으로 설정한 경우입니다.

4. 이상치 탐지 이벤트는 전체 멤버에게 경고 알림을 전송하므로 이벤트 수신 태그를 설정하지 않습니다.

이벤트 수신 태그 추가하기

1. [사용자별 이벤트 수신 설정](#) 섹션의 사용자 목록에서 [태그 추가](#) 또는 + 버튼을 선택하세요.
2. [이벤트 수신 태그](#) 팝업 창이 나타나면 태그 입력란에 태그 이름을 입력한 다음 엔터를 입력하거나 [새 태그 생성](#)을 선택하세요.
3. 태그 색상을 선택하세요.
4. [태그 생성](#) 버튼을 선택하세요.

[태그 목록](#)에서 생성한 태그를 확인할 수 있습니다. 생성한 태그를 적용하려면 해당 태그를 선택하세요.

이벤트 수신 태그 해제하기

1. [사용자별 이벤트 수신 설정](#) 섹션의 사용자 목록에서 + 버튼을 선택하세요.
2. [이벤트 수신 태그](#) 팝업 창이 나타나면 적용된 태그 옆에 × 버튼을 선택하세요.
3. [이벤트 수신 태그](#) 팝업 창을 닫으세요.

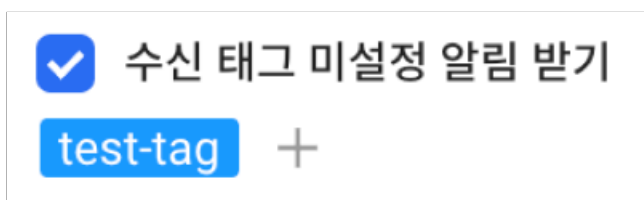
이벤트 수신 태그를 해제합니다.

이벤트 수신 태그 수정 및 삭제하기

1. 사용자별 이벤트 수신 설정 섹션의 사용자 목록에서 **태그 추가** 또는 **+** 버튼을 선택하세요.
2. 이벤트 수신 태그 팝업 창이 나타나면 **태그 목록**에서 수정 또는 삭제할 항목의 **✎** 버튼을 선택하세요.
3. 태그 이름을 수정하거나 색상을 변경한 다음 **적용** 버튼을 선택하세요.
태그를 삭제하려면 **🗑️ 태그 삭제** 버튼을 선택하세요.

❗ 이벤트에 적용 중인 이벤트 수신 태그 항목은 삭제할 수 없습니다.

수신 태그 미설정 알림



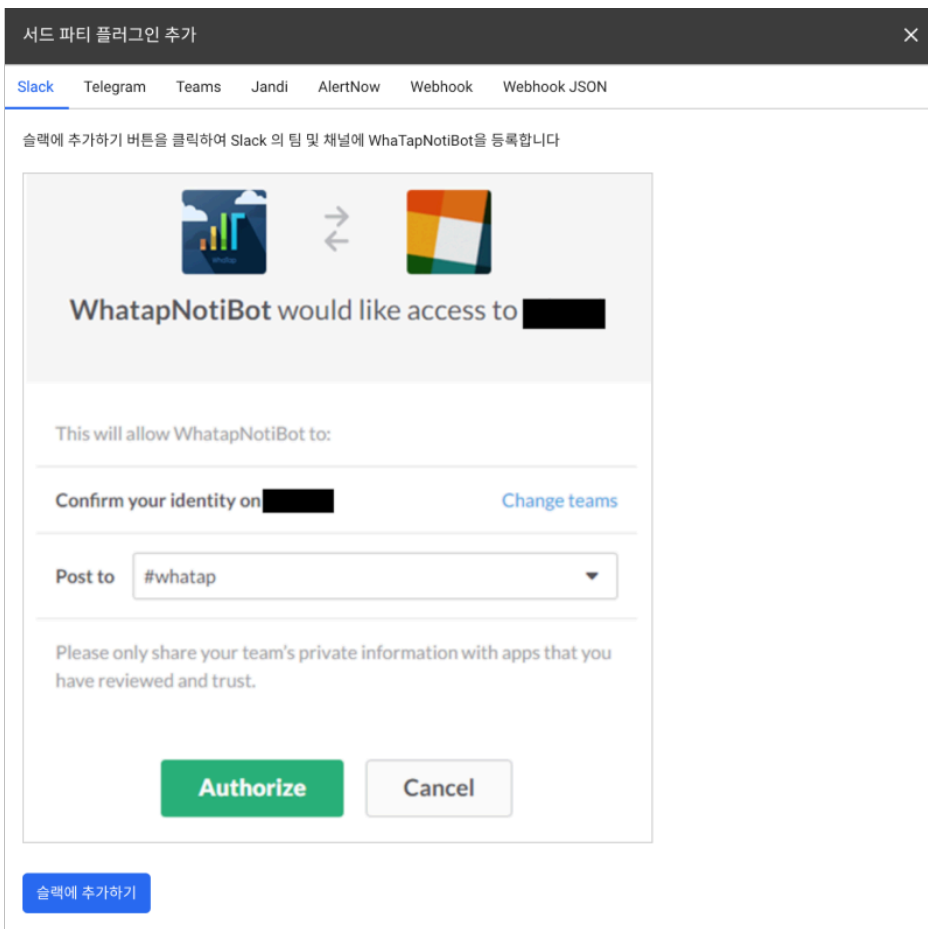
이벤트 수신 태그가 설정되지 않은 경고 알림을 받으려면 **수신 태그 미설정 알림 받기** 옵션을 선택하세요. 이벤트 수신 태그가 설정된 경고 알림만 받고 싶다면 선택을 해제하세요.

❗ 모든 경고 알림을 받지 않으려면 해당 옵션을 해제하고 선택한 이벤트 수신 태그가 없어야 합니다.

3rd 파티 플러그인 알림 추가하기

Slack, Telegram, Teams, Jandi, Webhook 등의 외부 애플리케이션을 통해 경고 알림을 받을 수 있습니다.

1. **경고 알림 > 이벤트 수신 설정** 메뉴에서 **3rd 파티 플러그인** 섹션의 **추가하기** 버튼을 선택하세요.
2. 원하는 서비스를 선택하세요.



3. 선택한 서비스의 화면 안내에 따라 설정을 진행하세요.
4. 모든 과정을 완료했다면 추가 버튼을 선택하세요.

ⓘ 와탭랩스의 지원 범위에 포함하지 않는 사내 메신저는 표준 Webhook, webhook json을 통해 연동할 수 있습니다.

대량 알림 발생 방지

알림이 대량으로 발생하면 설정한 시간 동안 경고 알림을 일시적으로 중단합니다. [경고 알림](#) > [이벤트 수신 설정](#) 메뉴에서 [대량 알림 발생 방지](#) 섹션으로 이동하세요.

대량 알림 발생 방지

알림이 대량으로 발생하면 지정한 시간 동안 알림이 일시적으로 중지됩니다.
대량 알림 차단 기능을 해제하려면 (이메일 주소 옆의) '중단 해제' 버튼을 눌러주세요.

활성화

탐지 시간

탐지 횟수

정지 시간

저장

- **활성화** 토글 버튼을 선택해 기능을 켜거나 끌 수 있습니다.
- **탐지 시간** 동안 **탐지 횟수** 이상의 이벤트가 발생하면 **정지 시간** 동안 경고 알림을 중지합니다.

예를 들어, 5분 동안 20회의 이벤트가 발생하면 5분 동안 경고 알림을 중지합니다. 설정한 **정지 시간** 시간이 지나면 대량 알림 발생 방지 기능은 해제됩니다.

ⓘ 문자 메시지 알림이 하루 200건 이상 발생하면 일시 중지하며 다음 메시지를 표시합니다. 문자 알림 중단 기능을 해제하려면 **문자알림 중단 해제** 버튼을 선택하세요.

다량의 문자메시지가 전송되었습니다. (200건 / 일)

- ① 프로젝트에서 발생한 많은 양의 문자 메시지로 인해 문자 메시지 알림이 중지됩니다.
- 시작 시간 : 2024-02-02 18:40:01

문자알림 중단 해제

경고 알림 사용자 설정하기

계정 관리 메뉴에서 사용자 개인의 알림 수신 레벨, 수신 수단, 요일 및 시간 등을 설정할 수 있습니다.

1. 화면의 오른쪽 위에 프로필 아이콘을 선택하세요.
2. 팝업 메뉴가 나타나면 **계정 관리** 버튼을 선택하세요.

3. 화면을 아래로 스크롤해 [알림 수신 설정](#) 섹션으로 이동하세요.
4. 수신 레벨, 수신 수단, 요일 및 시간을 설정한 다음 [저장](#) 버튼을 선택하세요.


경고 알림 언어 설정



프로젝트에서 발생하는 경고 알림 메시지의 언어를 변경할 수 있습니다.

1. 홈 화면에서 경고 알림 메시지의 언어를 변경할 프로젝트를 선택하세요.
2. 화면 왼쪽 메뉴에서 [관리](#) > [프로젝트 관리](#)를 선택하세요.
3. [알림 언어 관리](#) 섹션에서 원하는 언어를 선택하세요.
4. 화면 오른쪽 아래에 [저장](#) 버튼을 선택하세요.


이벤트 기록

홈 화면 > 프로젝트 선택 > 경고 알림 > 이벤트 기록

경고 알림이 발생한 이력을 확인할 수 있습니다. 최근 1년 이내의 이력까지 조회할 수 있습니다. 각 항목을 설정한 다음  버튼을 선택하세요.

이벤트 기록					
시간 선택	필터	애플리케이션			
< 2024/01/22 00:00 ~ 2024/01/23 00:00 1일 >	제목	전체 선택  			
번호	제목	이벤트 발생 시간	이벤트 해소 시간	애플리케이션	메시지
1	HITMAP_FLOOD_PATTERN	2024/01/22 09:08:00	2024/01/22 09:09:06		Flood pattern was detected in the project hitmap.
2	HITMAP_FLOOD_PATTERN	2024/01/22 08:57:00	2024/01/22 08:58:04		Flood pattern was detected in the project hitmap.
3	HITMAP_FLOOD_PATTERN	2024/01/22 08:46:00	2024/01/22 08:47:03		Flood pattern was detected in the project hitmap.
4	HITMAP_FLOOD_PATTERN	2024/01/22 08:35:00	2024/01/22 08:36:03		Flood pattern was detected in the project hitmap.
5	HITMAP_FLOOD_PATTERN	2024/01/22 08:24:00	2024/01/22 08:25:00		Flood pattern was detected in the project hitmap.
6	HITMAP_FLOOD_PATTERN	2024/01/22 08:13:00	2024/01/22 08:13:59		Flood pattern was detected in the project hitmap.
7	HITMAP_FLOOD_PATTERN	2024/01/22 08:02:00	2024/01/22 08:02:57		Flood pattern was detected in the project hitmap.
8	HITMAP_FLOOD_PATTERN	2024/01/22 07:51:00	2024/01/22 07:51:56		Flood pattern was detected in the project hitmap.
9	HITMAP_FLOOD_PATTERN	2024/01/22 07:40:00	2024/01/22 07:40:55		Flood pattern was detected in the project hitmap.
10	HITMAP_FLOOD_PATTERN	2024/01/22 07:29:00	2024/01/22 07:29:54		Flood pattern was detected in the project hitmap.
11	HITMAP_FLOOD_PATTERN	2024/01/22 07:18:00	2024/01/22 07:18:53		Flood pattern was detected in the project hitmap.
12	HITMAP_FLOOD_PATTERN	2024/01/22 07:07:00	2024/01/22 07:07:52		Flood pattern was detected in the project hitmap.
13	HITMAP_FLOOD_PATTERN	2024/01/22 06:56:00	2024/01/22 06:56:51		Flood pattern was detected in the project hitmap.
14	HITMAP_FLOOD_PATTERN	2024/01/22 06:45:00	2024/01/22 06:45:50		Flood pattern was detected in the project hitmap.
15	HITMAP_FLOOD_PATTERN	2024/01/22 06:34:00	2024/01/22 06:34:49		Flood pattern was detected in the project hitmap.
16	HITMAP_HORIZONTAL_PATTERN	2024/01/22 06:28:00	2024/01/22 06:28:48		Horizontal pattern was detected in the project hitmap.
17	HITMAP_FLOOD_PATTERN	2024/01/22 06:18:00	2024/01/22 06:18:46		Flood pattern was detected in the project hitmap.

이전 1 다음

 선택한 프로젝트에 따라 화면 이미지는 다를 수 있습니다.

• 시간 선택

- 오른쪽에 위치한 녹색 버튼을 선택해 조회 시간을 선택할 수 있습니다.
- < 또는 > 버튼을 선택해 선택한 조회 시간 만큼 간격을 이동할 수 있습니다.
- 세부 시간을 선택하려면 날짜 또는 시간 영역을 선택하세요. 세부 시간을 설정한 다음 **적용** 버튼을 선택하세요.

- **필터**: 제목 또는 메시지 내용을 기준으로 이벤트 기록을 필터링할 수 있습니다.

- **애플리케이션**: 프로젝트에 포함된 에이전트를 선택할 수 있습니다.
- **CSV**: 조회한 이벤트 기록 결과를 csv 파일로 저장할 수 있습니다. **CSV** 버튼을 클릭하면 **최대 CSV 라인 수**를 입력한 다음 **다운로드** 버튼을 선택하세요.
- **컬럼 선택**: 조회한 이벤트 기록 결과의 열 항목을 추가할 수 있습니다.
- **이벤트 설정**: **경고 알림 > 이벤트 설정** 메뉴로 이동합니다.
- **제목 / 메시지**: **이벤트 설정** 메뉴에서 추가한 이벤트의 **이벤트명**과 **메시지** 항목의 내용입니다.
- **이벤트 발생 시각**: 이벤트가 발생한 시각입니다.
 - 이벤트가 해소되지 않고 진행 중일 경우 **진행 중** 태그가 표시됩니다.
 - 정비 중인 경우 이벤트가 발생하면 **정비 중 발생** 태그가 표시됩니다.

❗ **정비 계획**에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

- **이벤트 해소 시각**: 설정한 이벤트가 해결된 시각입니다. 만약 해당 컬럼이 보이지 않는다면 **컬럼 선택** 버튼을 클릭한 다음 **이벤트 해소 시각**을 선택하세요.
- **애플리케이션**: **이벤트 설정** 메뉴에서 이벤트 추가 시 **이벤트 대상 필터링** 항목을 설정하면 표시됩니다.