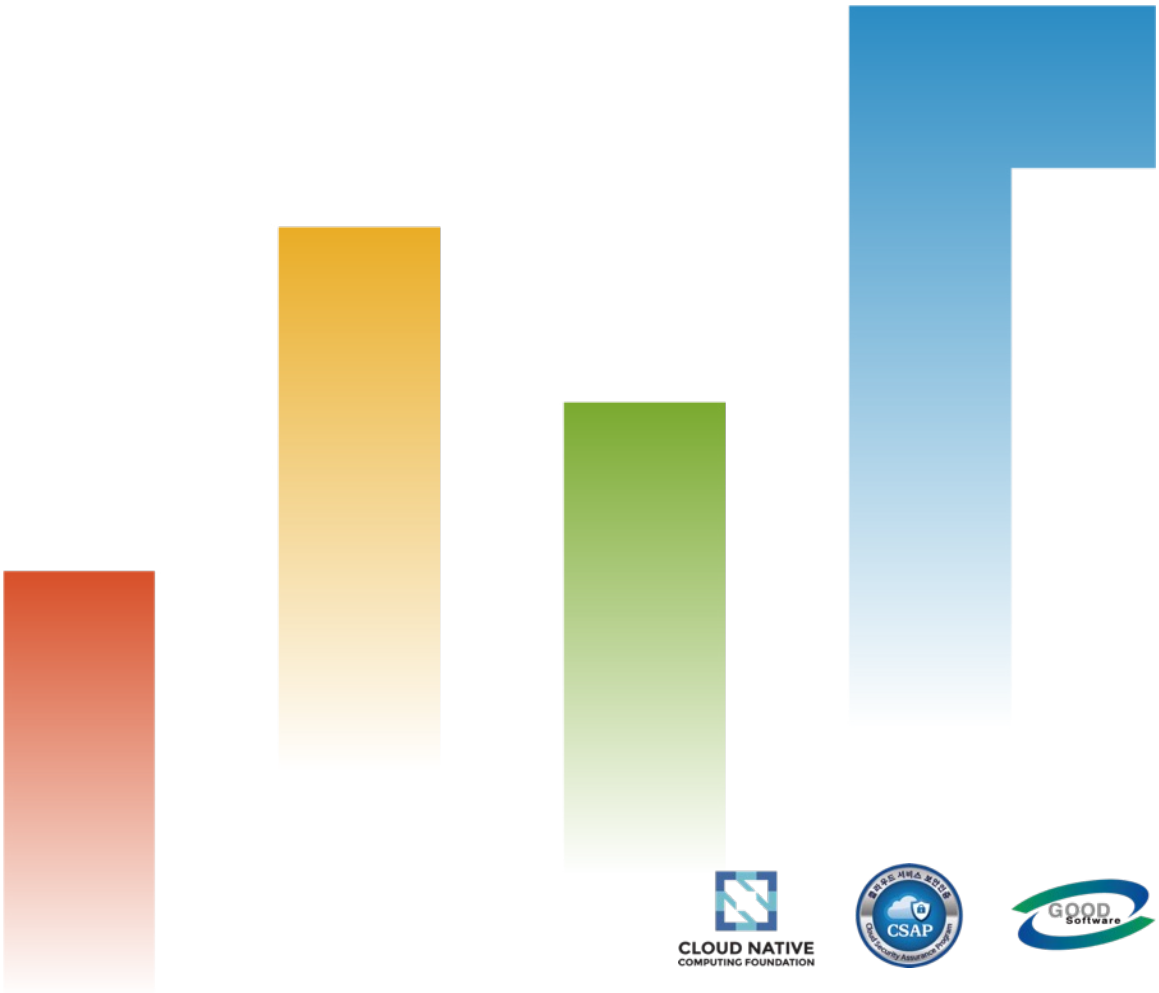
WhaTap

Log 모니터링

기술 문서 2024.04.02



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 특장점

- **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 알림과 특정 태그가 포함된 로그의 건수 추이를 기준으로 알림을 받는 복합 로그 알림을 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 테일에 대한 자세한 내용은 다음 문서를 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 트렌드에 대한 자세한 내용은 다음 문서를 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 검색에 대한 자세한 내용은 다음 문서를 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 버전을 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

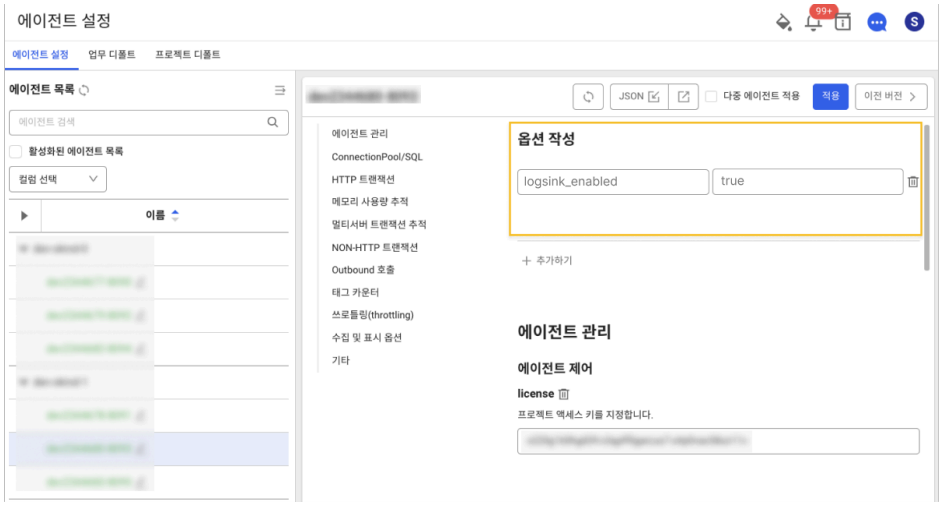
자바 에이전트 2.1.1 버전부터 가능합니다. 업데이트 방법은 다음 문서를 참조하세요.

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 입력을 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.conf에 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 추적할때 사용하세요.

  Java

```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.conf에 `hooklog_enabled` 옵션이 설정되어 있으면 본 옵션을 통해 로그 모니터링의 On/Off를 동적으로 제어할 수 있습니다.

- **logsink_trace_enabled** Boolean

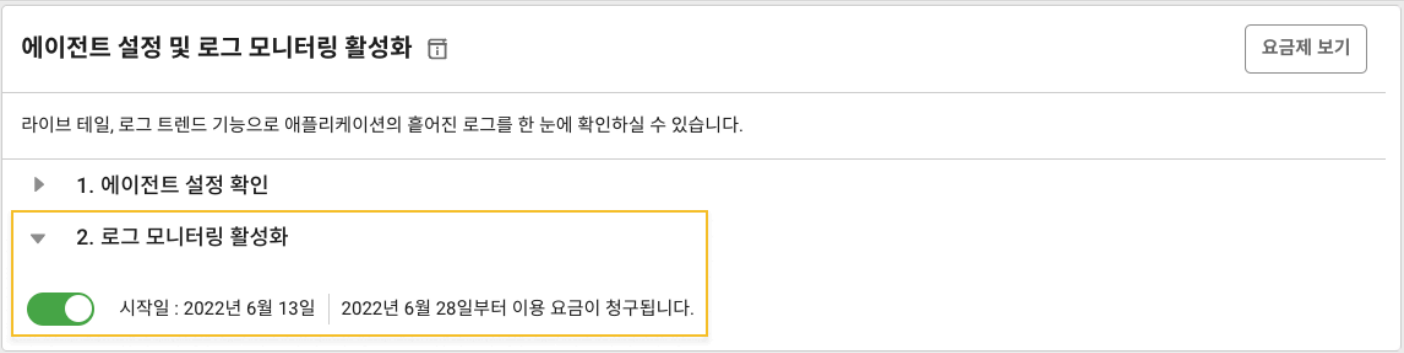
  기본값 `false`

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.



- 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 문서를 참조하세요.

PHP

PHP 애플리케이션에서 로그를 수집하려면 다음을 확인하세요.

에이전트 업데이트

PHP 에이전트 2.3.2 버전부터 가능합니다. 업데이트 방법은 다음 문서를 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-sysvsem' '--enable-sysvshm' '--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.

- 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 문서를 참조하세요.

Python

Python 애플리케이션에서 로그를 수집하려면 다음을 확인하세요.

에이전트 업데이트

Python 에이전트 1.2.2 버전부터 가능합니다. 업데이트 방법은 다음 문서를 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.conf를 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.

- 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 문서를 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.

-  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 문서를 참조하세요.

Server

서버 애플리케이션에서 로그를 수집하려면 다음을 확인하세요.

에이전트 업데이트

서버 에이전트 2.1.2 버전부터 가능합니다. 업데이트 방법은 다음 문서를 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(Powersehll))를 선택하세요. 기본 설치 또는 카테고리와 함께 설치를 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
```

```
cat >extension/logsink.conf<<EOL
[[inputs.logsink]]
 category = "serverlog"
 ## 로그 발생량 통계 별도 데이터로 전송 여부
 stats_enabled = true
 ## 로그 발생량 통계 카테고리
 stats_category = "logsink_stats"
 ## 로그 파일 경로(path)에 별표(*)가 포함되어 제외할 로그 비대상 파일명 설정
 excludeNames = [ ".gz",".zip" ]
 [[inputs.logsink.file]]
   ## 로그 파일 지정 시, 날짜 패턴(strftime.org) 지정 가능
   path = "/some/path/%Y-%m-%d/.log"
   disabled = false
   encoding = "euc-kr"

 [[inputs.logsink.file]]
   path = "/some/other/log"
   disabled = false
   encoding = "utf-8"

 [[inputs.logsink.file]]
   ## 줄 단위 로그에서 해당 키워드 검색 시, 이전 로그에 병합
   nowrap_keywords = ["Caused by:", "Test"]
EOL

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
```

```
# 관리자 권한 필요
New-Item -type "Directory" -Path "C:\Program Files\WhatapInfra\extension"

$contentToAdd = @"
[[inputs.logsink]]
category = "serverlog"
## 로그 발생량 통계 별도 데이터로 전송 여부
stats_enabled = true
## 로그 발생량 통계 카테고리
stats_category = "logsink_stats"
## 로그 파일 경로(path)에 별표()가 포함되어 제외할 로그 비대상 파일명 설정
excludeNames = [ ".gz",".zip" ]
[[inputs.logsink.file]]
## 로그 파일 지정 시, 날짜 패턴(strftime.org) 지정 가능
path = "c:\\whatap\\logs%Y-%m-%d_.log"
disabled = false
encoding = "euc-kr"

[[inputs.logsink.file]]
## 줄 단위 로그에서 해당 키워드 검색 시, 이전 로그에 병합
nowrap_keywords = ["Caused by:", "Test"]

"@

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

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 메트릭스 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.

- 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 문서를 참조하세요.

Kubernetes

쿠버네티스 컨테이너와 컨테이너 내부 애플리케이션의 로그를 수집하려면 다음을 확인하세요.

에이전트 업데이트

쿠버네티스 에이전트 1.1.35 버전부터 가능합니다. 업데이트 방법은 다음 문서를 참조하세요.

에이전트 설정 확인

홈 화면 > 프로젝트 선택 > 로그 > 로그 설정

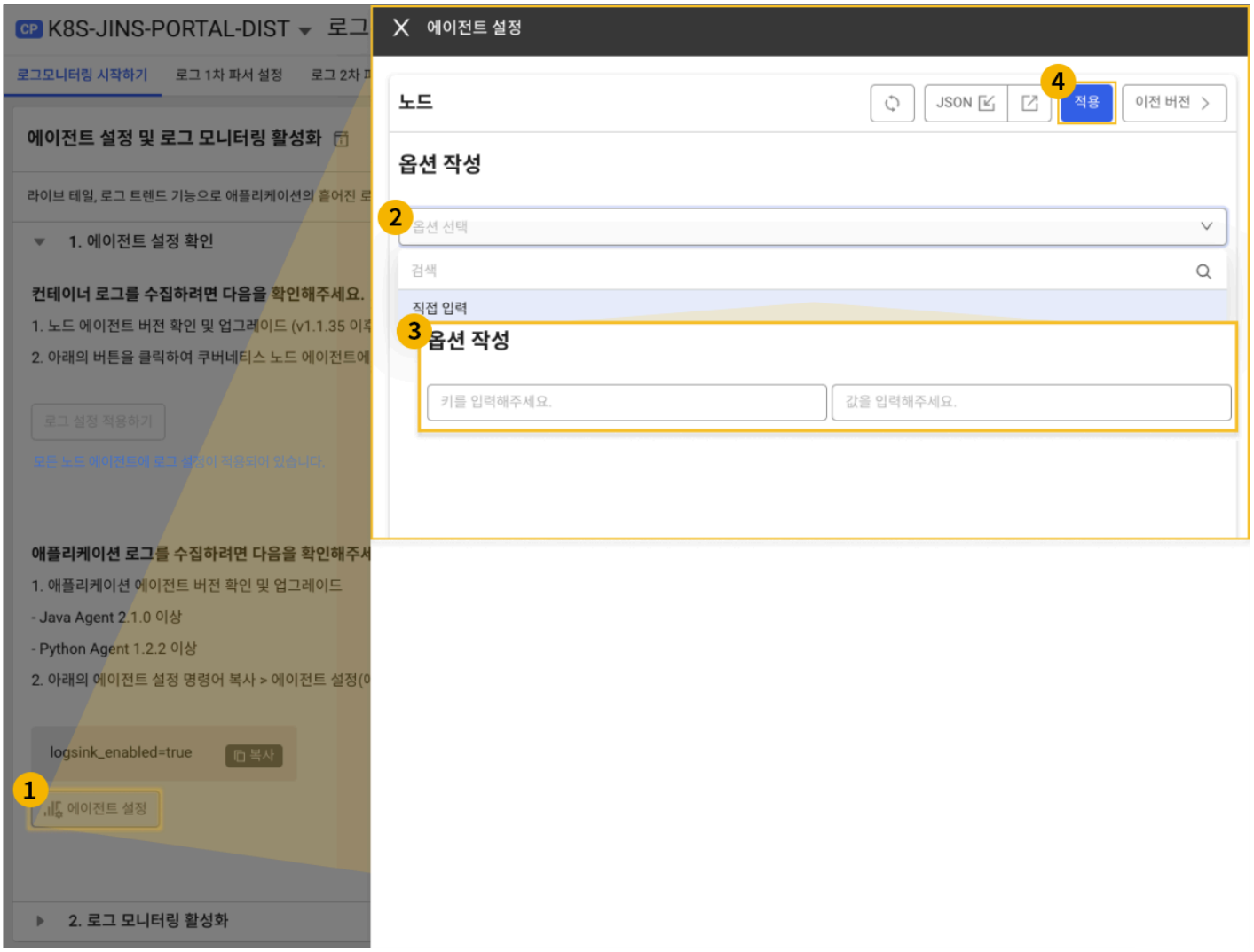
와탭 모니터링 서비스 초기 화면에서 프로젝트를 선택한 다음 프로젝트 메뉴 하위에 로그 > 로그 설정 메뉴를 선택하세요. 에이전트 설정 및 로그 모니터링 활성화 섹션의 에이전트 설정 확인 탭의 안내를 참조해 진행하세요.

컨테이너 로그 수집 활성화

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.



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. 4 적용 버튼을 선택하세요. 쿠버네티스 컨테이너 내 애플리케이션의 로그를 수집할 수 있습니다.

> ⓘ
> - Java 애플리케이션 로그 수집에 대한 자세한 내용은 다음 문서를 참조하세요.
> - Python 애플리케이션 로그 수집에 대한 자세한 내용은 다음 문서를 참조하세요.
> - Go 애플리케이션 로그 수집에 대한 자세한 내용은 다음 문서를 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.

- 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 문서를 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`	• 쿠버네티스에서 발생하는 이벤트가 저장된 로그 • 사용자 설정과 무관하게 기본 생성
`#WhatapEvent`	• 와탭 이벤트 설정에 의해 발생한 이벤트가 저장된 로그 • 사용자 설정과 무관하게 기본 생성
`containerStdout`	• 컨테이너 Standard Out 로그 • 사용자 설정 시 생성 • 노드 에이전트에 `logsink_enabled=true` 설정 추가 시
`AppLog`	• 컨테이너 내 애플리케이션 로그 • 사용자 설정 시 생성 • 애플리케이션 에이전트에 `logsink_enabled=true` 설정 추가 시

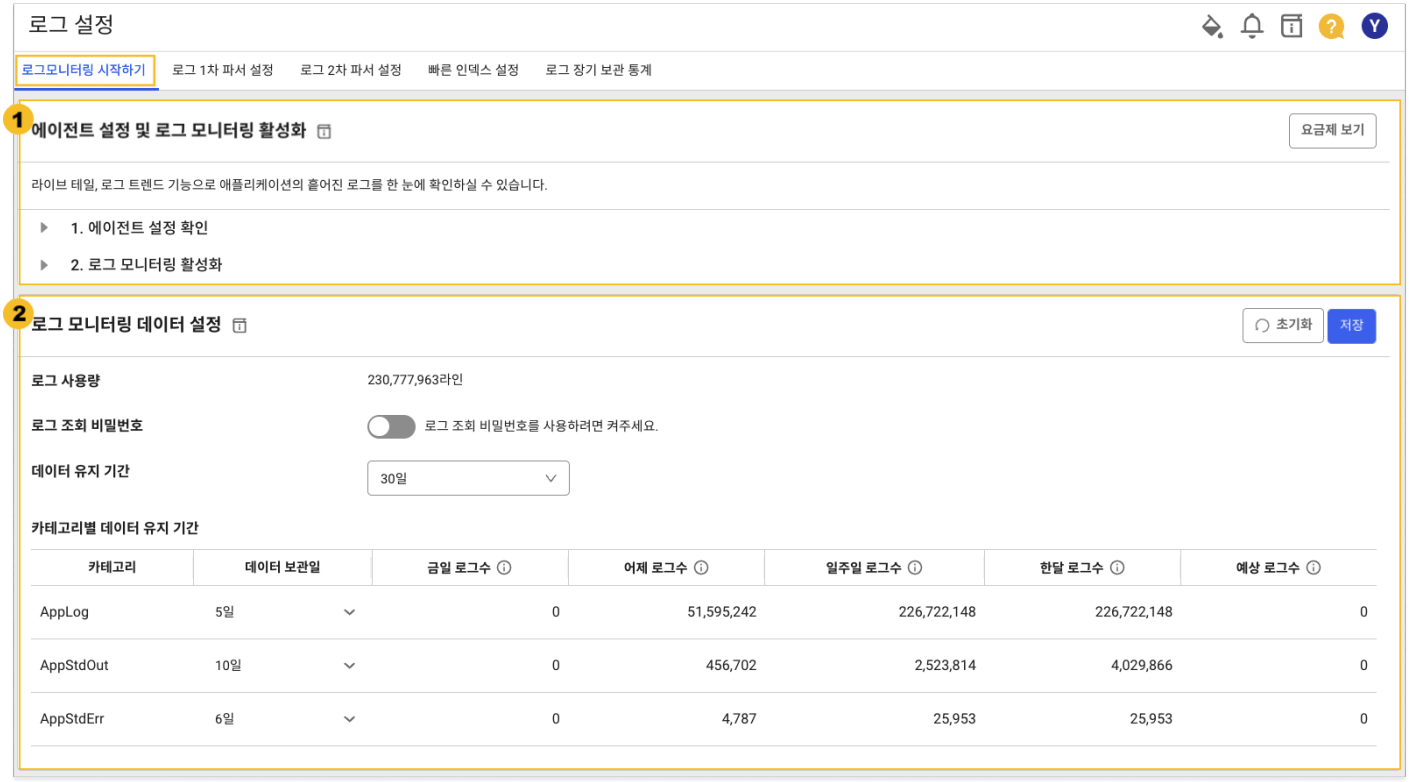
로그 설정

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.

> ⓘ
> - 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



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 문서를 참조하세요. 안내대로 whatap.conf 에 로그 감시 대상 파일 설정을 추가하세요.

- **쿠버네티스 모니터링**

  적용하기 메뉴 하위에 개별 적용 안내를 확인하세요. 다음 문서를 참조하세요.

로그 모니터링 활성화

로그 모니터링 활성화 메뉴를 선택하여 로그 모니터링 활성화 및 비활성화 여부를 설정하세요.

- 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 사용량을 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 수는 하루 동안 쌓인 로그 라인 개수, 예상 로그 수는 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 비밀번호를 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 GROK과 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 불가한 예약어**
>
> 다음 예약어의 경우 파서를 등록하더라도 인덱스가 생성되지 않습니다.
>
> `timestamp` , `message` , `pcode` , `category` , `content` , `logContent`

> 로그 파서에 대한 자세한 내용은 다음 문서를 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

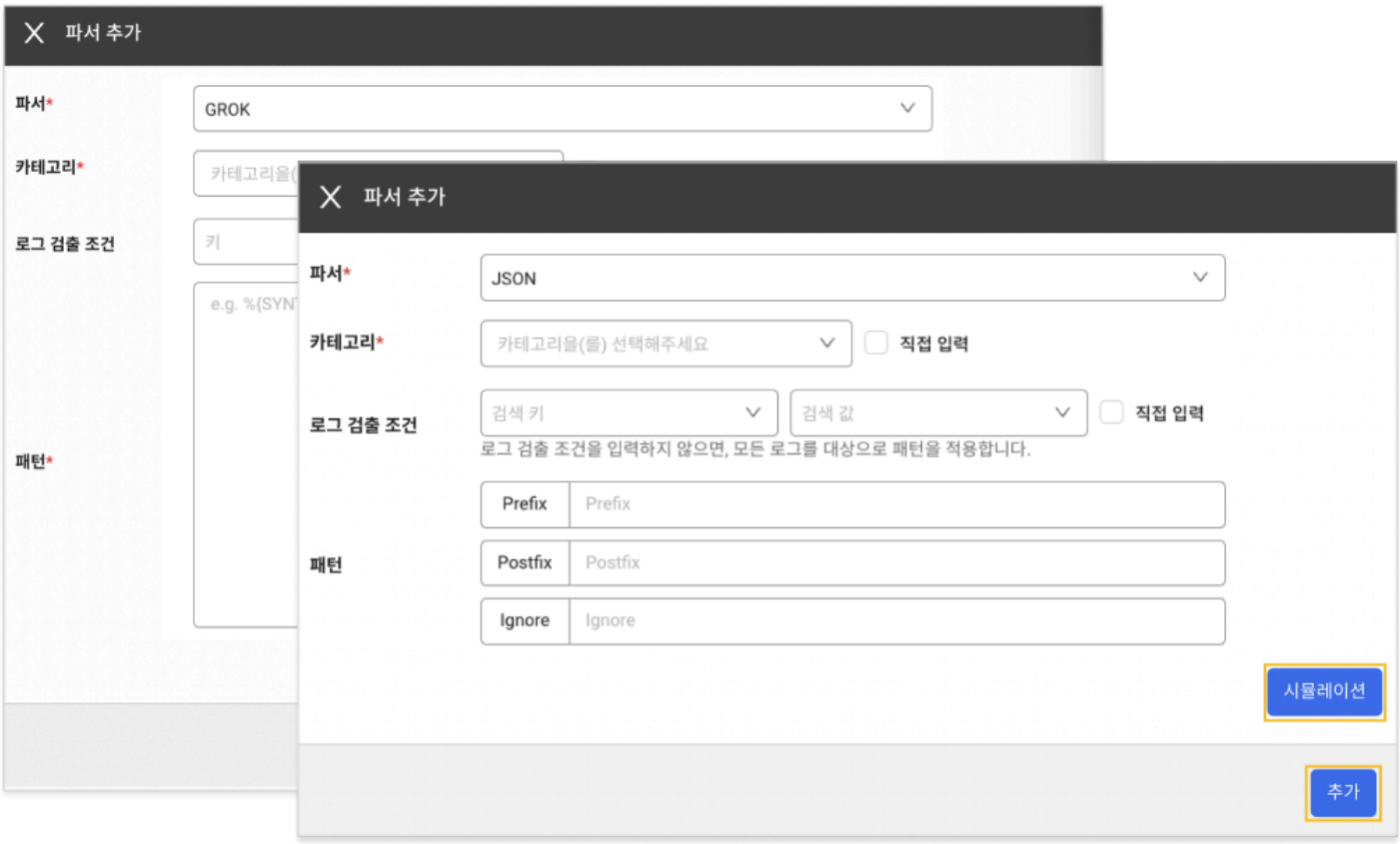
파서 목록

로그 설정 메뉴 상단에서 로그 1차 파서 설정 탭을 선택하면 등록한 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 등록한 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.



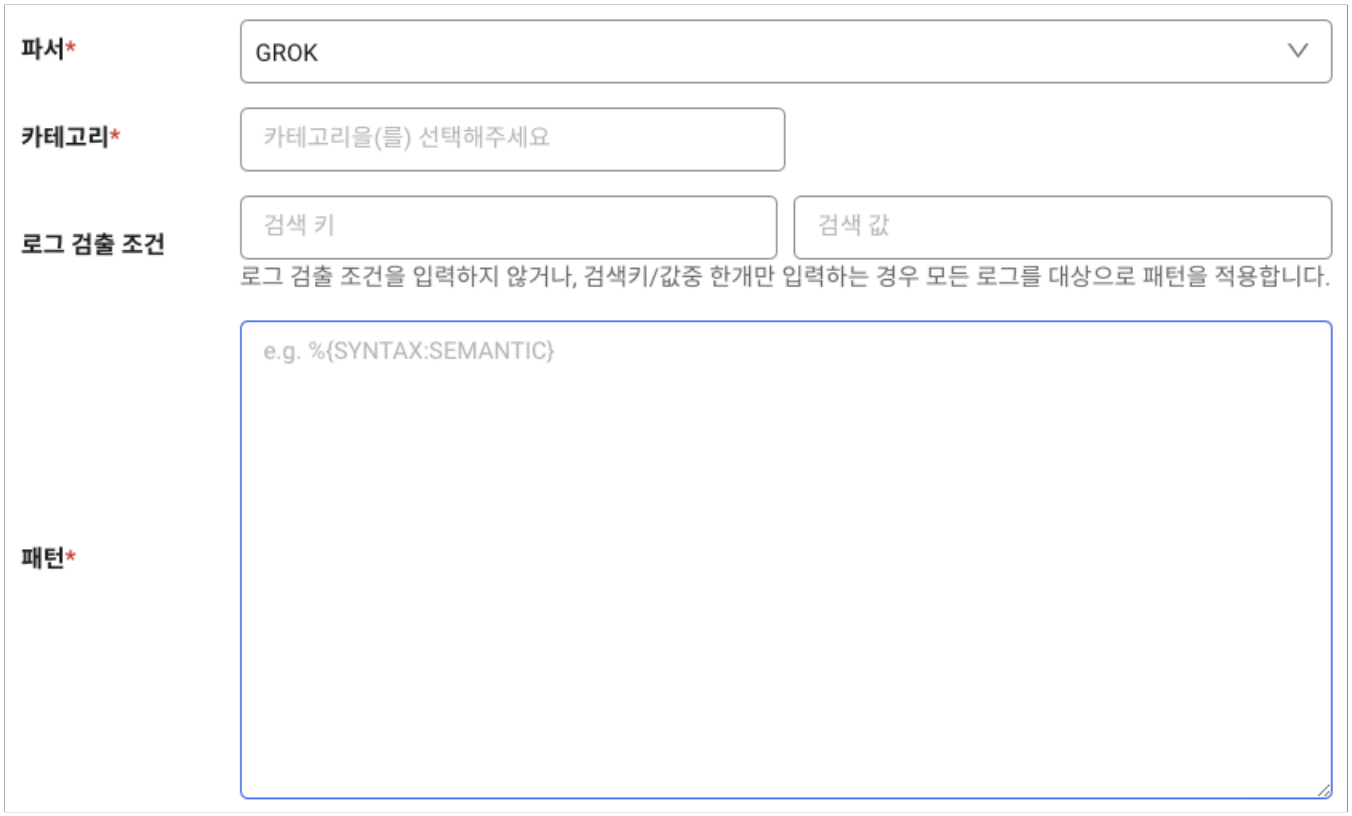
1. + 추가하기 버튼을 선택하면 파서 추가 창이 나타납니다.
2. 파서 선택 창에서 파서를 선택하세요. 각 파서 및 패턴 등록에 관한 자세한 내용은 다음 문서를 참조하세요.
   - GROK 파서 및 패턴 등록
   - JSON 파서 및 패턴 등록
3. 카테고리 선택 창에서 카테고리를 선택하거나 직접 입력하세요.
4. 로그 검출 조건으로 활용할 검색 키와 검색 값을 선택하거나 직접 입력하세요.

   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 문서를 참조하세요.
7. 시뮬레이션 결과가 정상적이라면 추가 버튼을 선택해 파서를 등록하세요.

> ⓘ 로그 파서 등록 시 동일한 카테고리에 파서를 중복 등록할 수 없습니다.

GROK 파서 패턴 등록



기본 문법은 `%{SYNTAX:SEMANTIC}` 입니다. GROK 파서에 대한 자세한 내용은 다음 문서를 참조하세요.

- **SYNTAX**

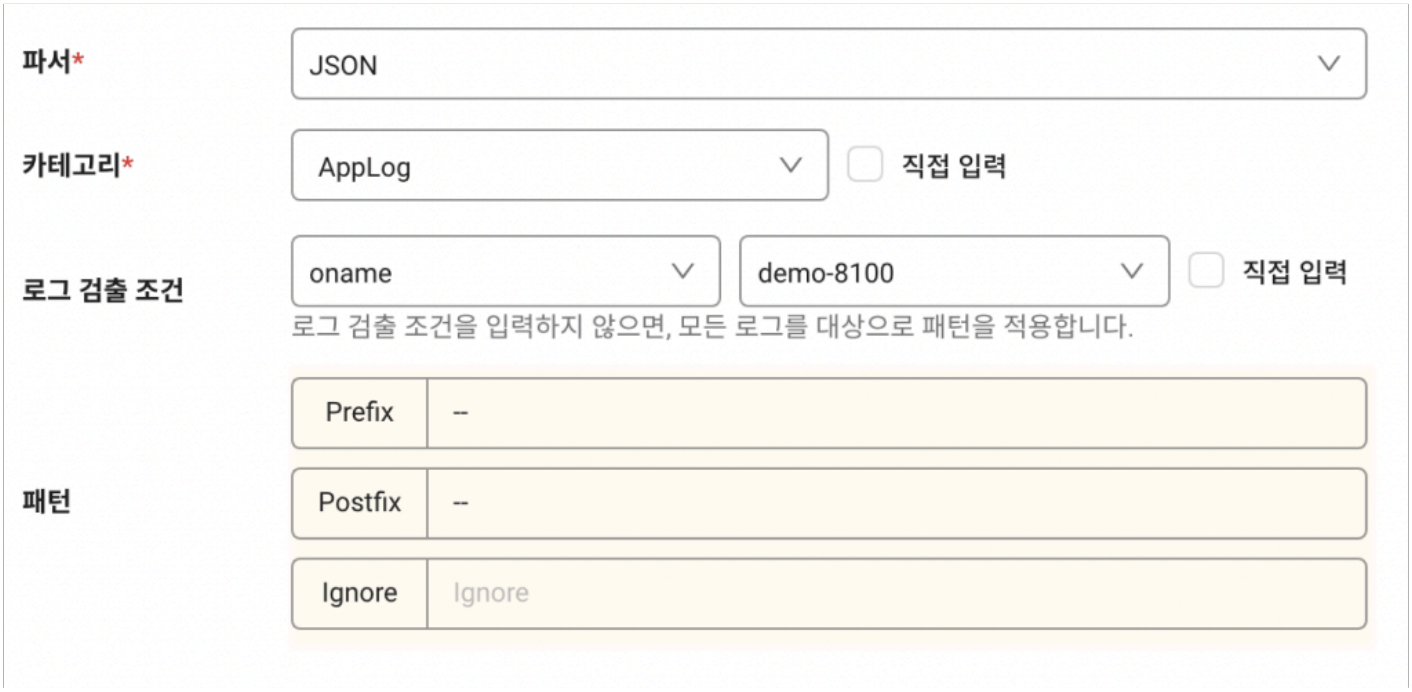
  GROK 정의 패턴입니다.

- **SEMANTIC**

  파싱된 데이터에 할당할 키입니다.

> ⓘ SEMANTIC에는 예약어 등이 사용되지 않도록 조합어 사용을 권장합니다.

JSON 포맷 파서 패턴 등록



로그 전체 혹은 일부가 JSON 형태로 출력되는 경우 JSON 포맷 파서를 통해 JSON으로 출력된 부분을 파싱할 수 있습니다. 로그 중 JSON 형태로 출력된 부분을 검출하기 위하여 Prefix, Postfix 옵션을 조합해 로그의 어느 부분을 JSON으로 인식해 파싱할지 지정합니다. JSON 파서에 대한 자세한 내용은 다음 문서를 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
- Reponse 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

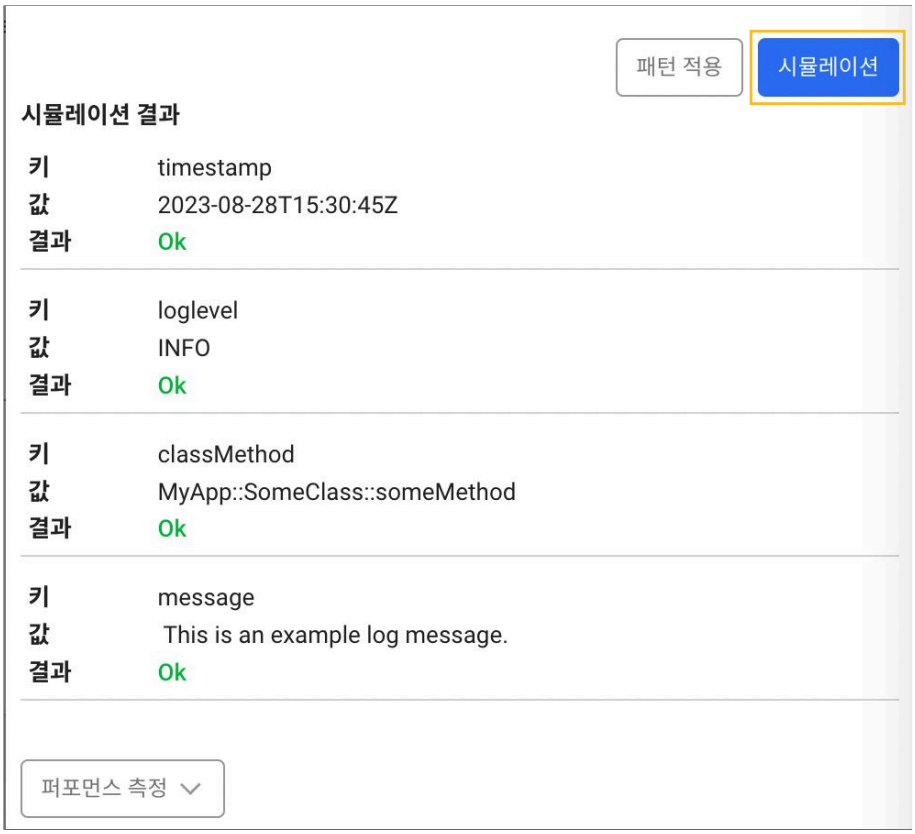
```
io.whatap.logsink.parser.JsonFormatParser {prefix: "Response : "}
```

파서 시뮬레이션

1. 파서 추가 화면에서 패턴을 입력한 후 시뮬레이션 버튼을 선택하세요. 파서 시뮬레이션 창이 나타납니다.
2. 파서 시뮬레이션 창에서 로그를 입력하세요.
3. 입력한 로그와 패턴을 확인하세요.

4. 시뮬레이션 버튼을 선택해 등록하려는 패턴으로 파싱에 성공하는지 확인하세요.

- **시뮬레이션 성공 화면**



- **시뮬레이션 실패 화면**

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.

파싱된 키는 라이브 테일, 로그 검색, 로그 트렌드에서 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 파서와 상태 코드 성공률 파서를 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 파서**가 **등록**되어 있어야 합니다.

파서 목록

로그 설정 메뉴 상단에서 로그 2차 파서 설정 탭을 선택하면 등록한 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 등록한 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.

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 조건을 선택하거나 직접 입력하세요.
5. 제외할 상태 코드를 입력하세요.
6. 추가 버튼을 선택해 파서를 등록하세요.

4xx, 5xx 상태 코드 파서 제외할 상태 코드 등록

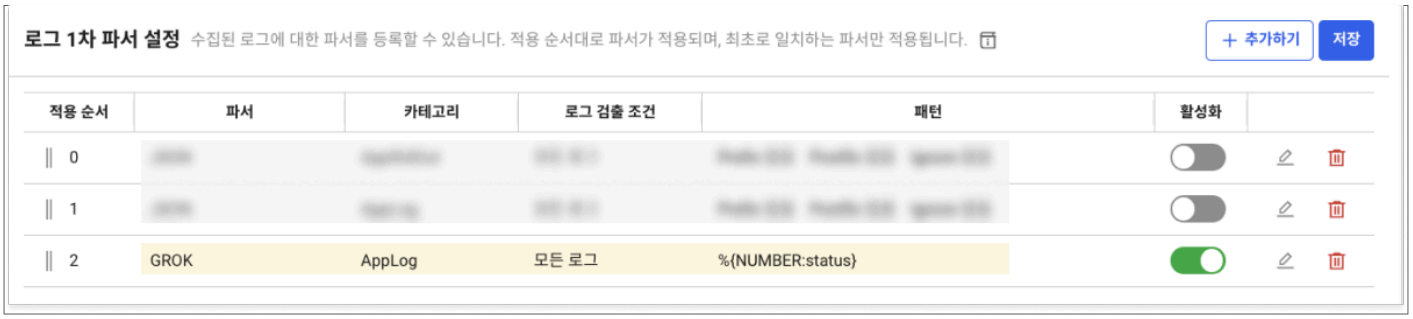
4xx, 5xx 상태 코드 파서는 status가 이미 파싱된 경우 사용할 수 있는 파서입니다. 파싱된 status를 이용하여 추가적으로 4xx, 5xx 상태 코드를 파싱합니다. 파싱한 데이터로 4xx, 5xx 건수 데이터를 생성할 수 있습니다. 제외할 상태 코드로 4xx, 5xx 상태 코드를 입력 또는 선택할 수 있습니다. 입력된 상태 코드는 로그에서 4xx, 5xx 상태 코드를 파싱할 때 제외됩니다.

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

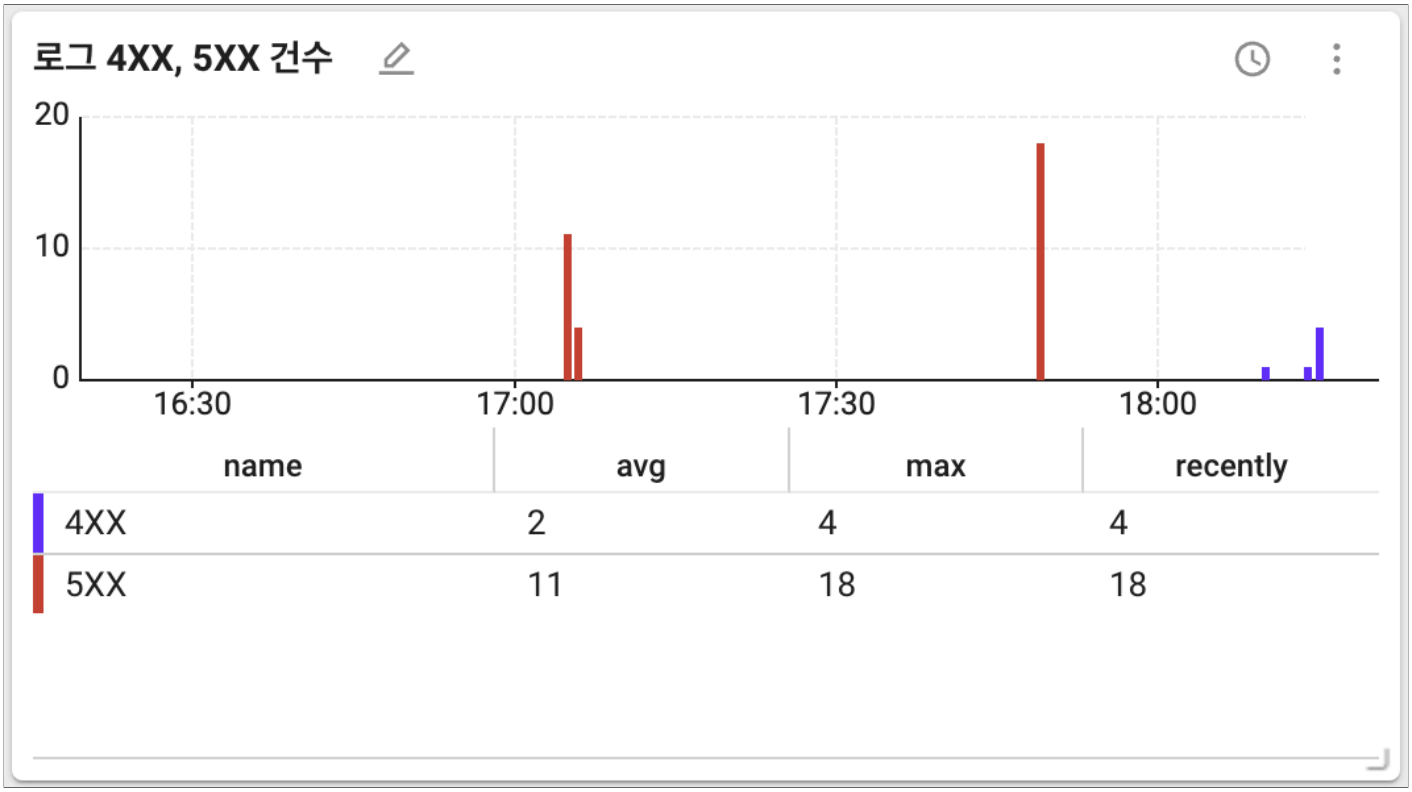


유입되는 로그가 `{"msg":"message","status":404}`이고 예시처럼 GROK 파서로 status를 파싱한다면, `status: 404`와 같이 파싱됩니다. status가 정상적으로 파싱되는 것을 확인했다면 4XX,5XX 상태 코드 파서에서 제외할 상태 코드를 등록하세요.

데이터 조회

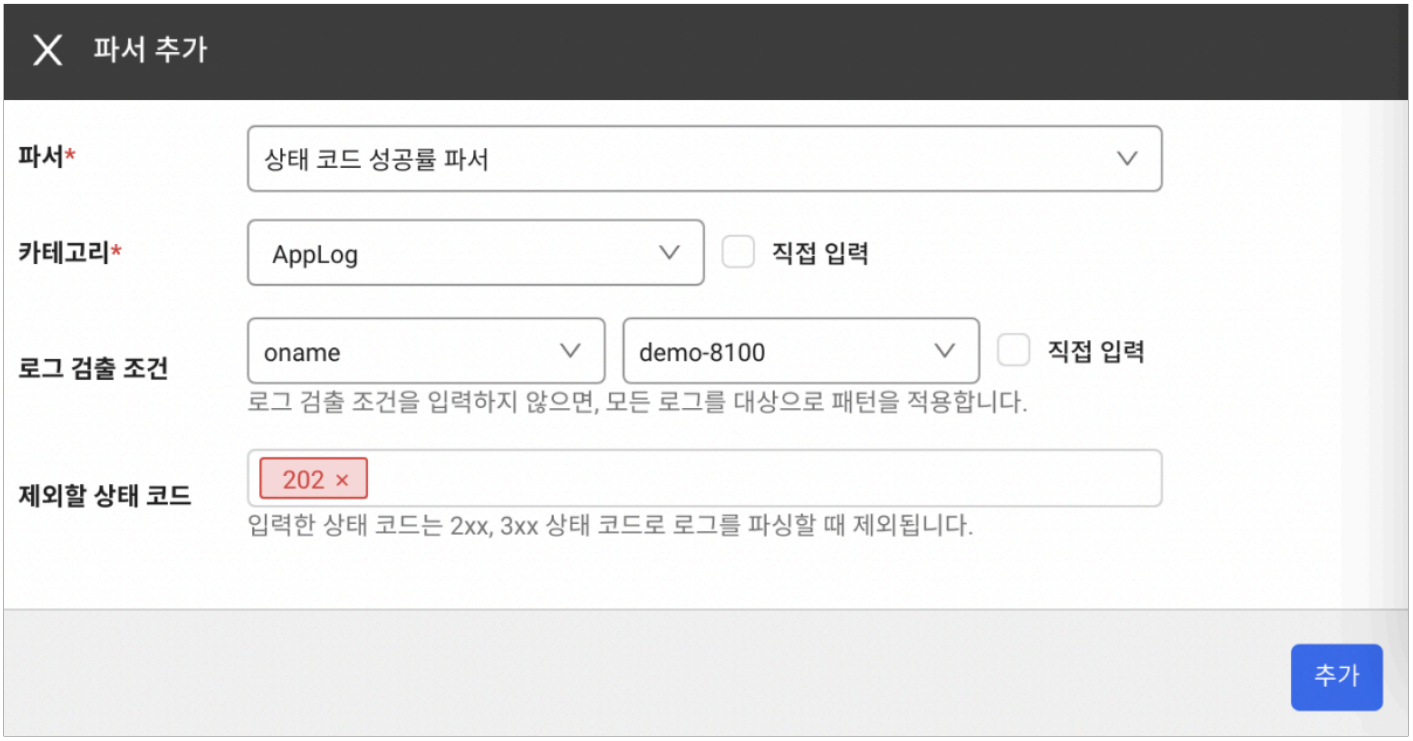
파서를 모두 등록하면 Flex 보드로 이동해 로그 4XX, 5XX 건수 위젯을 생성하세요.

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



상태 코드 성공률 파서는 status가 이미 파싱된 경우 사용할 수 있는 파서입니다. status 파싱에 관한 내용은 다음 문서를 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 보드로 이동해 로그 요청 성공률 위젯을 생성하세요.

위젯을 생성하면 다음과 같이 데이터를 확인할 수 있습니다.

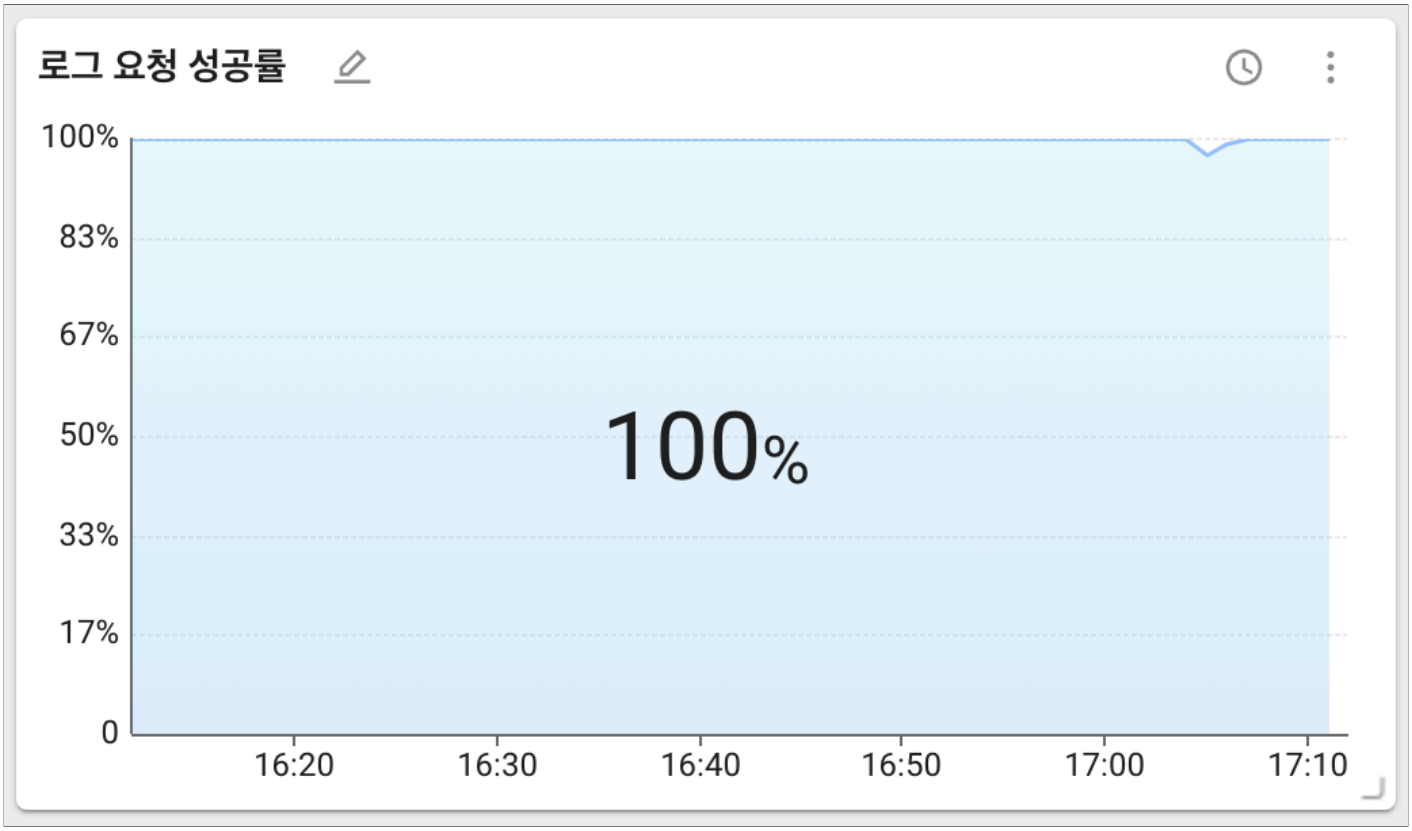


차트 위 데이터는 조회 기간에 대한 통계를 나타냅니다. 통계 방법을 최근값, 최댓값, 평균값 등으로 선택할 수 있습니다. 최근값이 기본으로 선택되어 있습니다.

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.

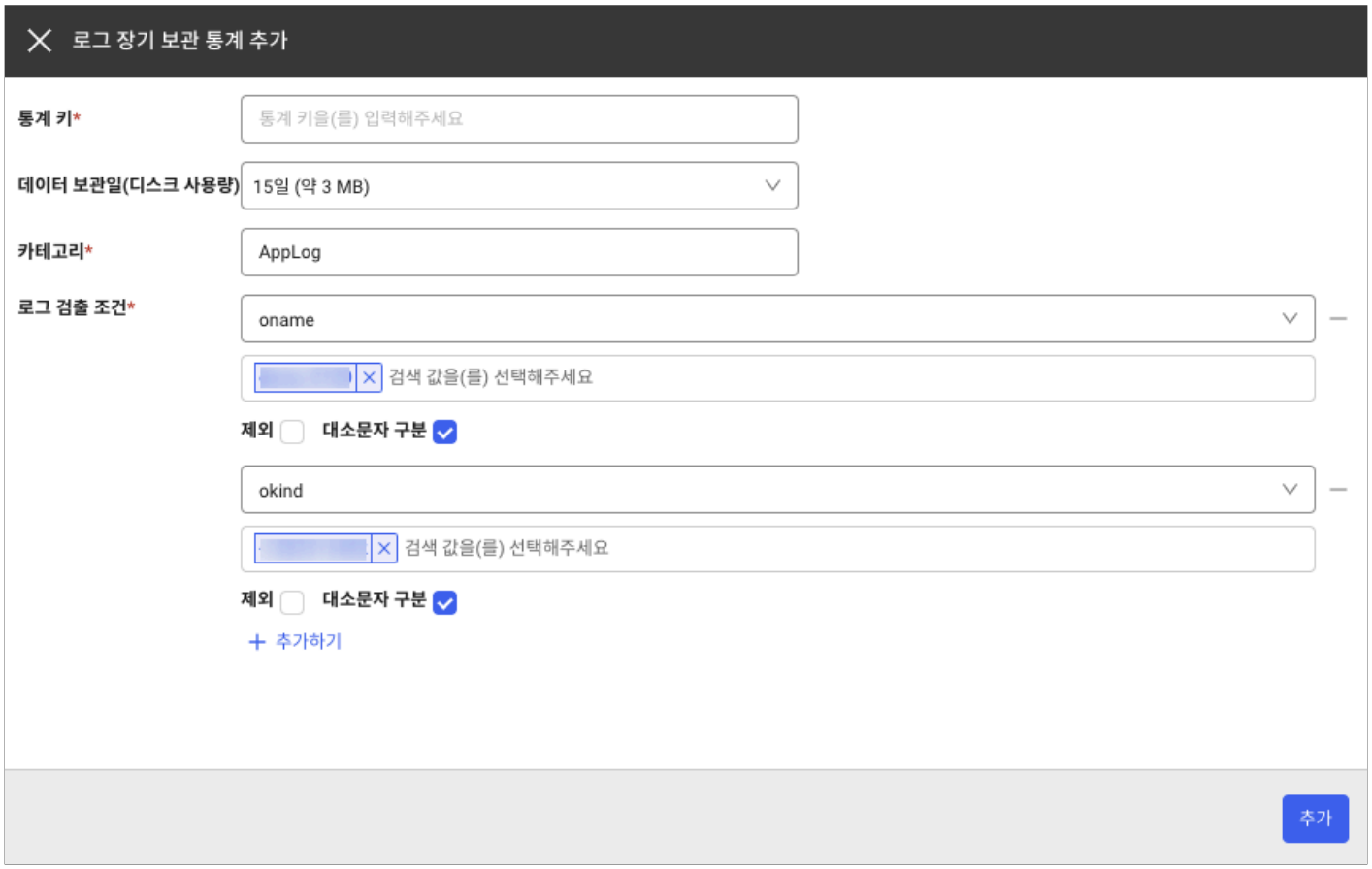
1. 하나의 프로젝트에 파서 설정 및 빠른 인덱스 설정을 추가하세요.
2. 각 설정 탭에서 화면 오른쪽 위에 JSON 버튼을 선택하세요.
3. JSON 내보내기 창이 나타나면 화면 오른쪽 위에 내보내기 버튼을 선택하세요.
4. JSON 설정 파일이 사용자 PC에 저장됩니다.
5. 다른 프로젝트로 이동한 다음 로그 > 로그 설정 메뉴로 이동하세요.
6. 앞서 JSON 설정 파일을 내보낸 설정 탭을 선택한 다음 버튼을 선택하세요.
7. 파일 선택 창이 나타나면 사용자의 PC에 저장한 JSON 설정 파일을 선택하세요.
8. JSON 가져오기 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 저장**할 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 탭에서 + 추가하기 버튼을 선택하면 로그 장기 보관 통계 추가 창이 나타납니다. + 추가하기 버튼을 통해 규칙을 추가하거나 생성한 규칙을 - 아이콘을 통해 삭제할 수 있습니다.

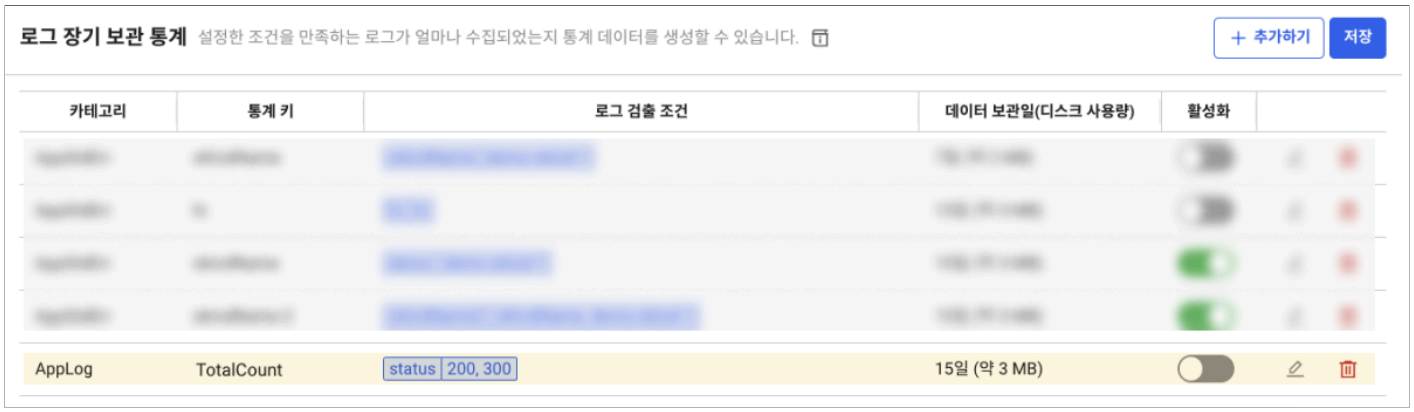
설정 항목

필드	설명
카테고리	규칙을 적용할 카테고리 입니다.
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 검출 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.

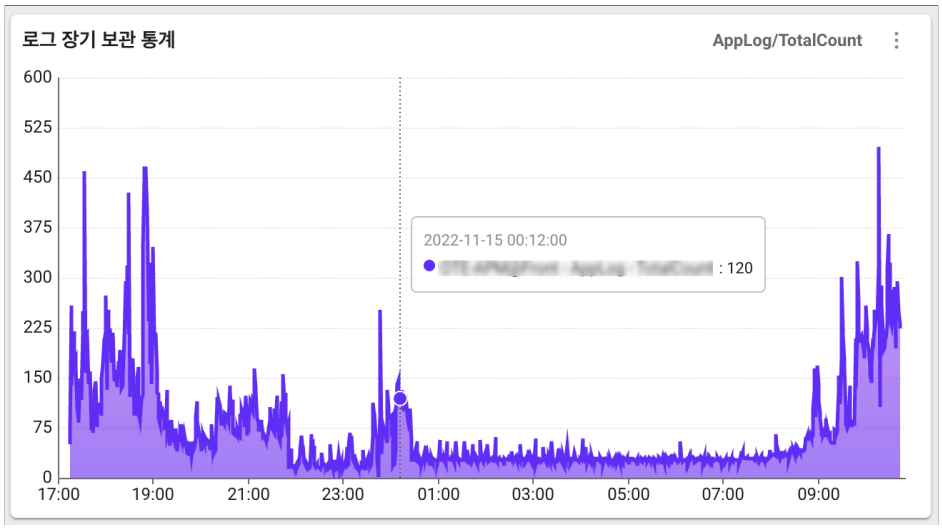


데이터 조회

1. Flex 보드의 위젯 템플릿에서 로그 장기 보관 통계를 검색해 위젯을 생성하세요.

2. 데이터를 조회할 카테고리와 키를 지정한 뒤 적용 버튼을 선택합니다.

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.

> ⓘ **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 다음을 참조하세요.
   - **SYNTAX**: GROK이 제공하는 named regular expressions를 지정합니다.
   - **SEMANTIC**: 매칭되는 값에 부여할 이름을 지정합니다.

   > ⓘ **named regular expressions**
   >
   > GROK에서 제공하는 문법입니다. 복잡한 정규 표현식에 이름을 부여해 사용할 수 있도록 GROK에서 제공하는 기능입니다.
   >
   > | name | regular expression |
   > | --- | --- |
   > | WORD | `\b\w+\b` |
   > | SPACE | `\s*` |
   > | NOTSPACE | `\S+` |
   > | UUID | `[A-Fa-f0-9]{8}-(?:[A-Fa-f0-9]{4}-){3}[A-Fa-f0-9]{12}` |
   >
   > 와탭에서 제공하는 모든 named regular expressions 확인을 원한다면 다음 링크를 참조하세요.

2. `(?<SEMANTIC>REGX)`: 정규 표현식의 **named capturing group** 문법입니다. 정규 표현식을 활용해서 사용자의 의도에 맞게 태그를 추출할 수 있습니다. 활용 예시는 다음을 참조하세요.
   - **SEMANTIC**: 매칭되는 값에 부여할 이름을 지정합니다.
   - **REGX**: 매칭에 사용할 정규 표현식을 입력합니다.

   > ⓘ **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 logCategiry 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 로그에서 `%{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 logCategiry 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(\{, \, \})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),\scity=(?<cityEnum>\d)\}\s(?<dexBuildElapsed>\d{2})ms
```

위와 같은 문법으로 파싱을 하면 다음과 같이 태그를 추출할 수 있습니다.

Tag extraction

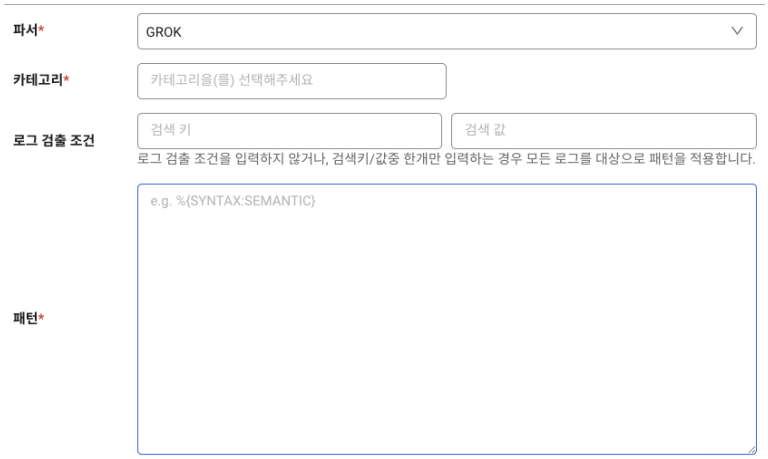
- projectCode : 8
- logCategory : VirtualLog
- dexBuildStartTime : 20230808 02:01:00.000
- areaEnum : 4
- cityEnum : 5
- dexBuildElapsed : 56

GROK 적용하기

로그 설정 > 로그 1차 파서 설정

1. GROK 패턴 파서를 적용하려면 로그 설정 메뉴의 로그 1차 파서 설정 탭으로 이동하세요.

2. + 추가하기를 선택 후 파서 입력란에서 GROK 파서를 선택하세요.



3. 카테고리 및 로그 검출 조건, 패턴을 입력하세요. 파서 추가 창의 구성 요소는 다음과 같습니다.

- 카테고리

  로그 카테고리를 선택하세요. 카테고리는 필수로 입력해야 합니다.

- 로그 검출 조건
  - 조건에 만족하는 로그만 파서가 적용됩니다.
  - 검색 키와 검색 값을 선택하거나 직접 입력하세요.
  - 로그 검출 조건은 모든 파서가 수행되기 전에 적용됩니다. 즉 파서의 결과로 추가되는 태그를 사용할 수 없습니다.

- 패턴

  GROK 패턴을 지정하세요. 필수로 입력해야 합니다.

4. 추가 버튼을 선택해 파서를 등록하세요.

ⓘ
- 로그 파서 목록에서 해당 파서의 적용 순서를 변경하거나 활성화 및 수정, 삭제할 수 있습니다.
- 파서를 등록하기 전에 시뮬레이션을 통해 등록하려는 패턴이 정상적인지 확인할 수 있습니다.

ⓘ **GROK 파서 주의사항**
- GROK 파서는 `%{SYNTAX:SEMANTIC}` , `%{SYNTAX:SEMANTIC}` 두 가지 패턴을 지원합니다.
- `%{SYNTAX:SEMANTIC}` 패턴 사용 시 `SEMANTIC` 을 반드시 입력해야합니다.
- `%{SYNTAX:SEMANTIC}` 패턴 사용 시 `SEMANTIC` 은 하나의 파서 안에서 unique 해야합니다.
- `(?<SEMANTIC>REGX)` 패턴 사용 시 `SEMANTIC` 은 문자(a-z, A-Z)와 숫자(0-9) 그리고 지정된 특수문자(`.` , `_` , `-`)만 올 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 로그와 패턴을 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{2}\.\d{3})\s\{area=(?<areaEnum>\d),\scity=(?<cityEnum>\d)\}\s(?<dexBuildElapsed>\d{2})ms
```

1. 파서 추가 창에서 시뮬레이션 버튼을 선택하세요.
2. 파서 시뮬레이션 창에서 로그와 패턴을 입력하세요.
3. 로그와 패턴 입력 후 시뮬레이션 버튼을 선택하세요. 다음과 같이 시뮬레이션 결과를 확인할 수 있습니다.

JSON 파서

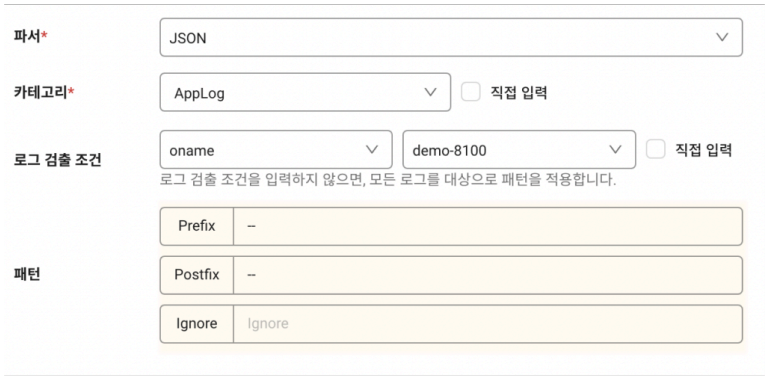
로그가 JSON 포맷으로 수집될 경우 JSON 파서를 사용해 쉽고 편리하게 파싱할 수 있습니다.

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.



3. 카테고리 및 로그 검출 조건, 패턴을 입력하세요. 파서 추가 창의 구성 요소는 다음과 같습니다.
   - 카테고리

     로그 카테고리를 선택하세요. 카테고리는 필수로 입력해야 합니다.

   - 로그 검출 조건
     - 조건에 만족하는 로그만 파서가 적용됩니다.
     - 검색 키와 검색 값을 선택하거나 직접 입력하세요.
     - 로그 검출 조건은 모든 파서가 수행되기 전에 적용됩니다. 즉 파서의 결과로 추가되는 태그를 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 Prefix와 Postfix를 `--`로 지정하고 Ignore에 `--`를 지정 시 `host`, `method`, `status` 3개의 태그만 생성됩니다.

4. 추가 버튼을 선택해 파서를 등록하세요.

ⓘ
- 로그 파서 목록에서 해당 파서의 적용 순서를 변경하거나 활성화 및 수정, 삭제할 수 있습니다.
- 파서를 등록하기 전에 시뮬레이션을 통해 등록하려는 패턴이 정상적인지 확인할 수 있습니다. GROK 파서 등록 시뮬레이션 과정과 동일합니다. 다음 문서를 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 태그를 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 Prefix와 Postfix를 지정해 주세요. 와탭 로그 모니터링은 Prefix와 Postfix 사이의 영역을 JSON 포맷으로 인식 후 파싱합니다.

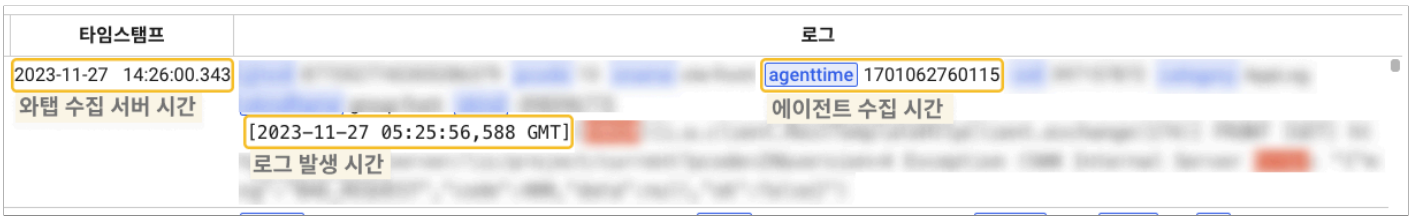
Tag extraction

- 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



로그 타임스탬프 기준 시간이 **와탭 에이전트가 로그를 수집한 시간**에서 **와탭 수집 서버의 로그 처리 시간**으로 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 시간**을 기준으로 동작합니다. 이에 따라 **에이전트 수집 시간**과 **와탭 수집 서버 시간**에 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.

> ⓘ 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.

     > ⓘ 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

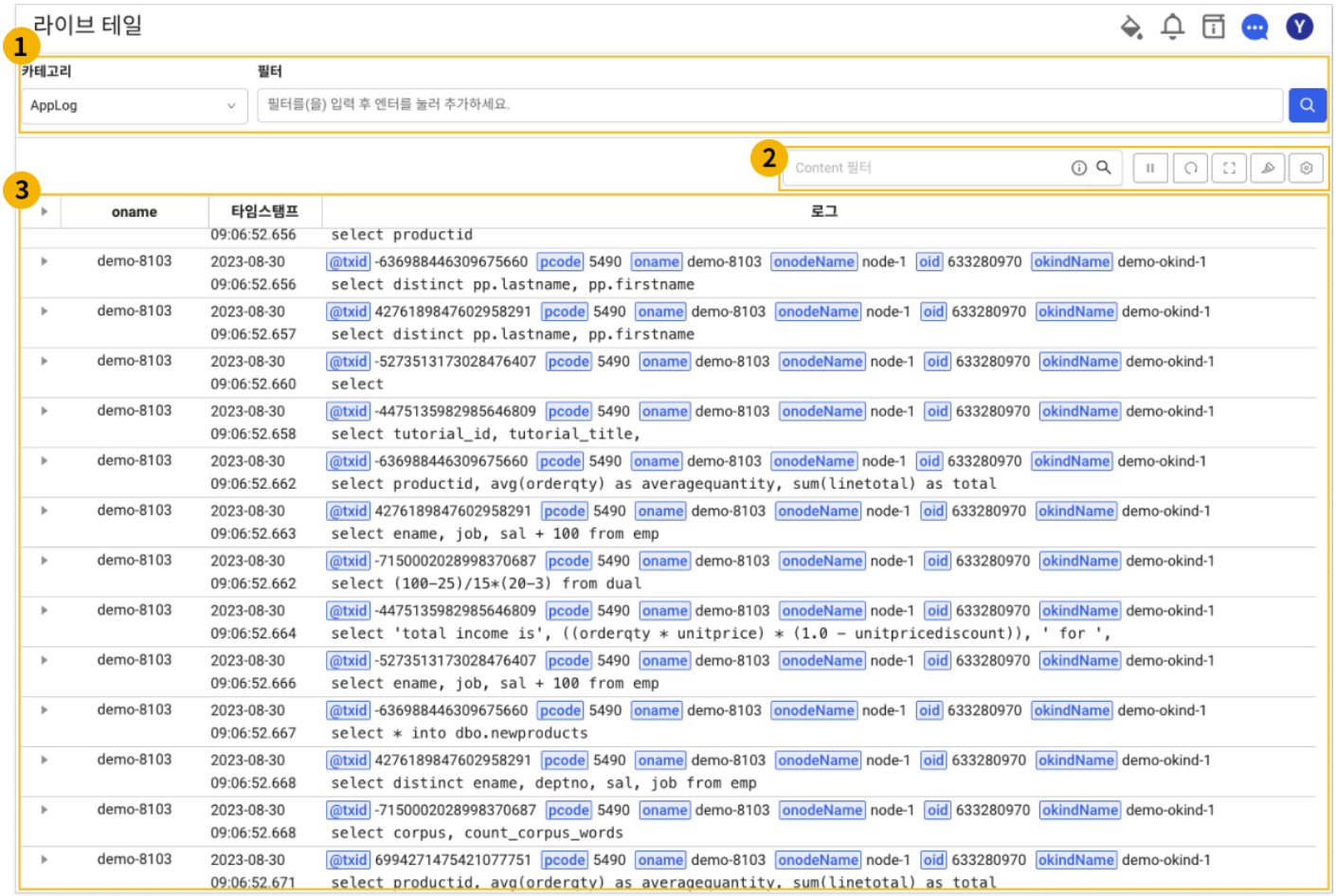
이벤트 기록 메뉴를 통해 발생한 경고 알림 이력을 확인할 수 있습니다.

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.



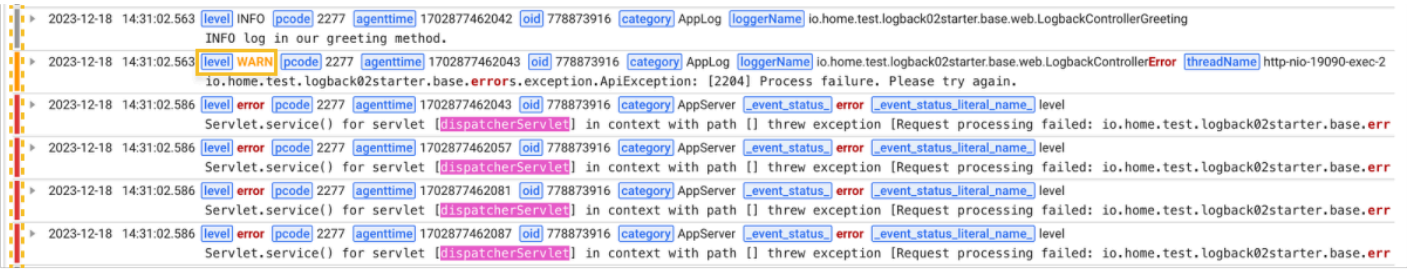
라이브 테일 메뉴에서 복잡한 로그들도 손쉽게 접근 가능합니다. 필요에 따라 필터 혹은 하이라이트 등의 기능을 활용해 실시간으로 조회할 수 있습니다. 로그 데이터 조회 주기는 2초입니다. 주요 용어는 다음과 같습니다.

- **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.



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

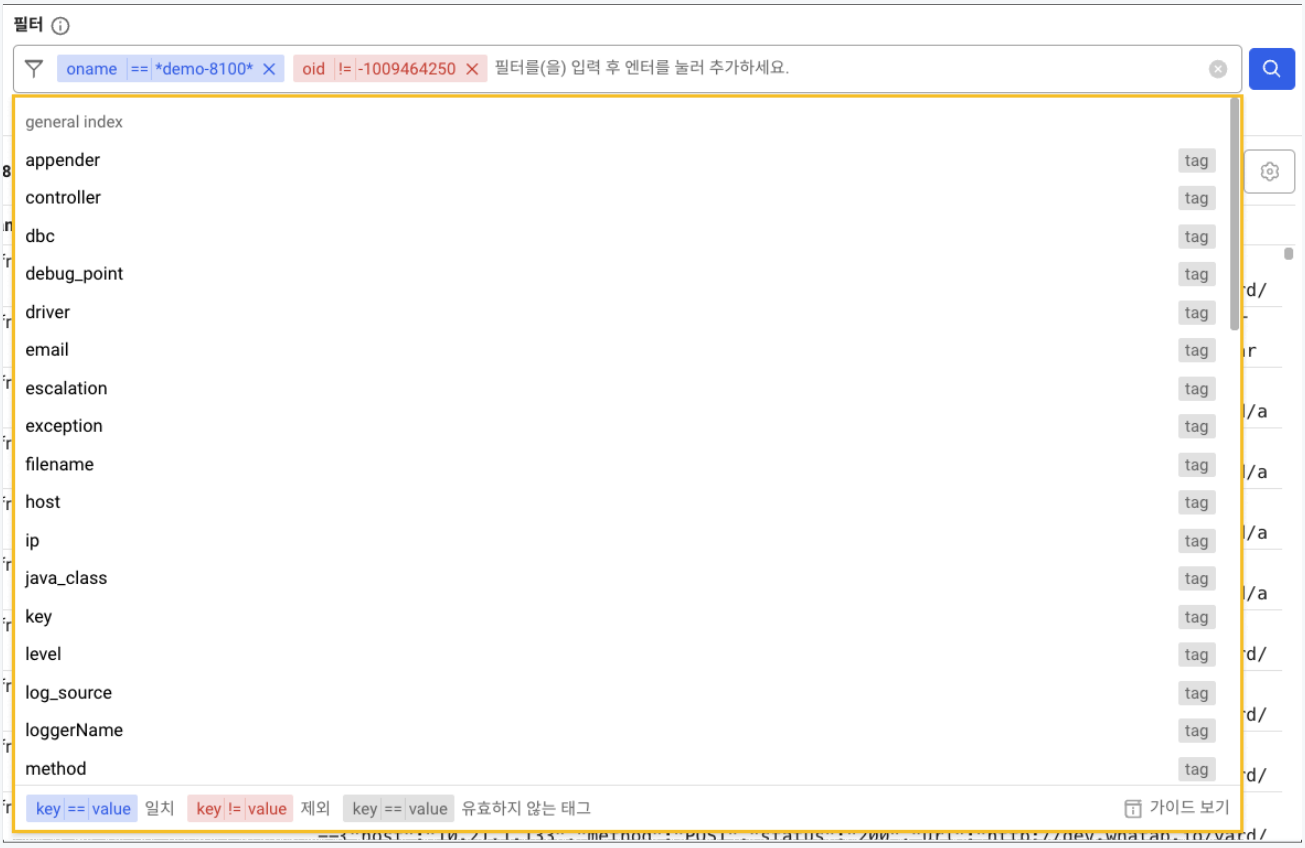
필터 적용

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.

가이드 UI

다음과 같이 입력 창 아래 **가이드 UI**를 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.

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 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.

> ⓘ
> - 라이브 테일 `검색 키` 로 `category` 를 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 설정을 통해 인덱스 키 값을 활용해 검색하는 것을 권장합니다.

1. 카테고리를 선택하세요.
2. 필터 입력창에 `content` 기준 띄어쓰기 후 검색을 원하는 키워드를 입력하세요.

   > 예시, `content *select*`

3. 검색 버튼을 클릭해 로그를 조회하세요.

> ⓘ
> - 라이브 테일의 경우 모든 로그 검색이 가능해 카테고리를 지정할 필요가 없습니다.
> - 파서 설정에 대한 자세한 내용은 다음 문서를 참조하세요.

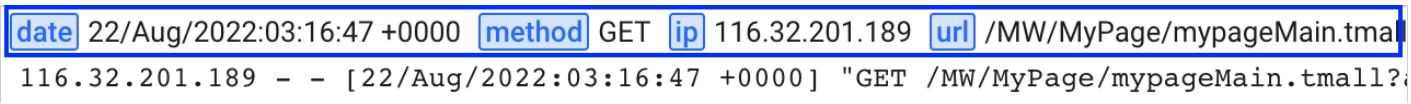
필터 수정

필터에 값을 입력한 뒤 입력한 값을 클릭하면 해당 값을 수정할 수 있습니다.

- 입력 창에 텍스트 재입력해 수정할 수 있습니다.
- 입력 창 아래 **가이드 UI**를 통해 추천 값을 선택해 수정할 수 있습니다.

검색 키(Search Key)

다음 이미지에서 파란색 박스 부분은 파싱(parsing)된 검색 키입니다. 검색 키는 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.

검색 키 종류

검색 키 종류	검색 키 포멧	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
==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:{regexr}	정규표현식에 매칭되는 로그를 검색합니다.	caller==re:^i\.w\.a\.w\.s\.v\.r\.
**	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.

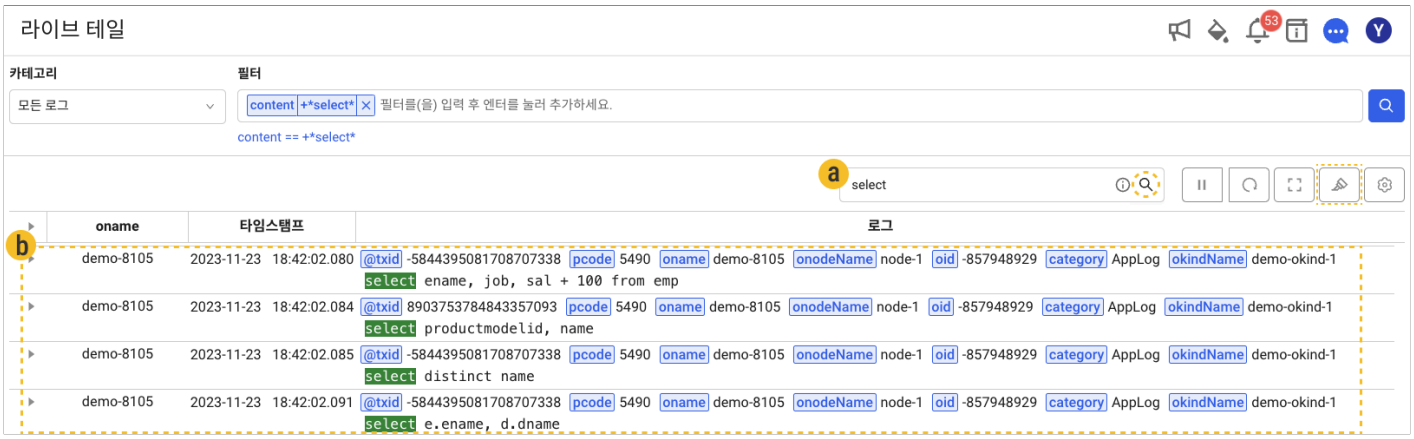
  > 예, `+>searchValue` 는 유효하지 않습니다.

문법 종류	설명	예시
>searchValue	검색 값보다 큰 값이 포함된 로그를 조회합니다.	response_time.n>3000
>=searchValue	검색 값보다 크거나 같은 값이 포함된 로그를 조회합니다.	response_time.n>=3000

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 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 로그와 타임스탬프를 전체 화면에서 확인할 수 있습니다.

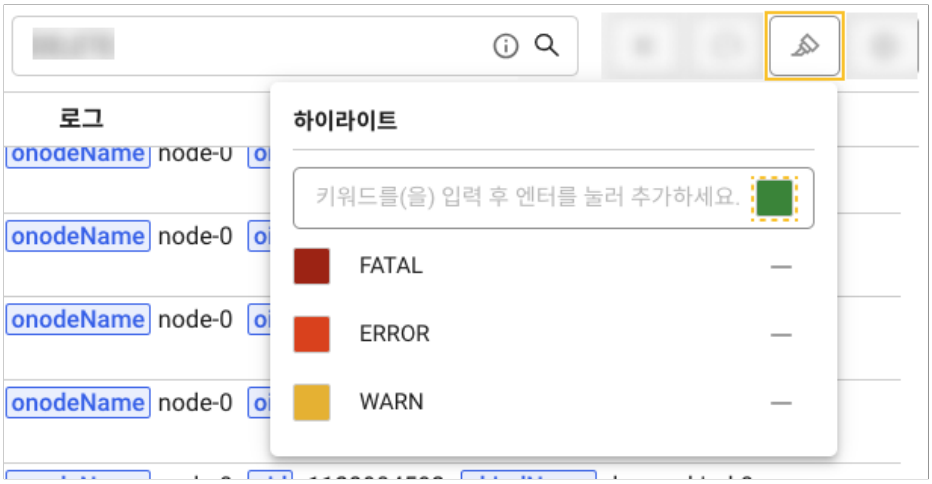
복수 키워드 조건

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

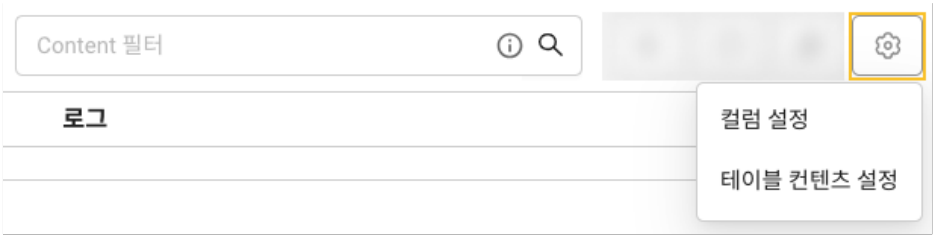
하이라이트 아이콘을 선택해 하이라이팅할 키워드 및 색상을 설정할 수 있습니다.



- 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 트렌드에서 사용할 수 있습니다.
- 테이블 설정 버튼을 선택하면 컬럼 추가와 테이블 컨텐츠 설정 옵션 메뉴가 나타납니다.

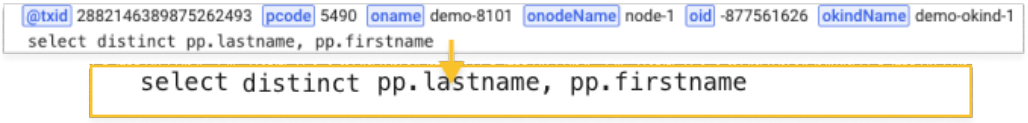


1. 컬럼 설정

- 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

- 컨텐츠 표시 여부
  - 체크된 항목은 테이블에 표시되지 않습니다. 기본으로 로그, 태그 모두 체크가 되어있으며 두 가지 항목 모두 표시합니다.
  - 다음과 같이 태그를 해제할 경우 테이블에서 로그의 태그는 표시되지 않습니다.



- 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.

ⓘ 동일한 프로젝트 내 라이브 테일, 로그 검색, 로그 트렌드 메뉴는 테이블 설정을 공유합니다.

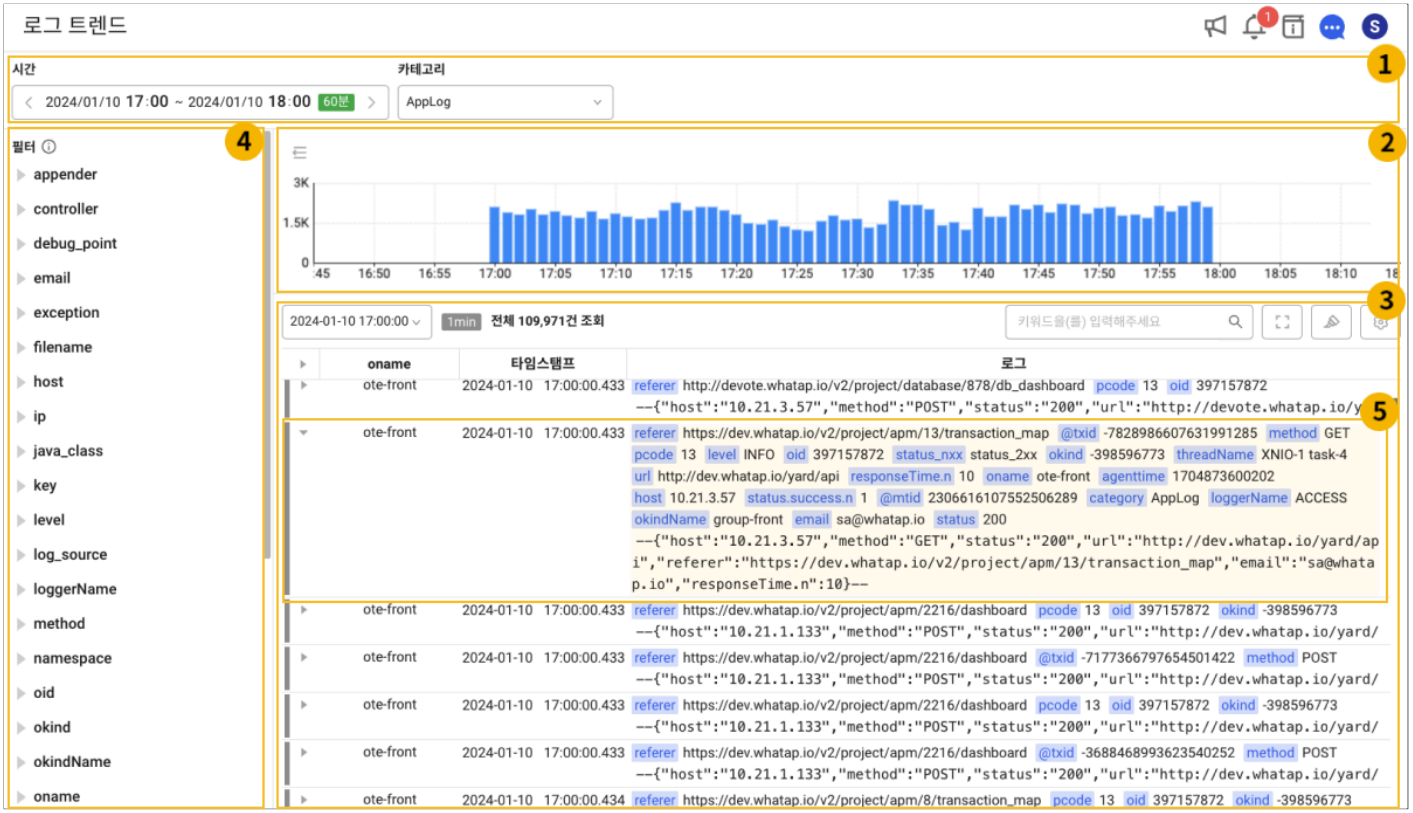
로그 트렌드

> ⓘ **로그 조회** 권한이 없을 경우 해당 메뉴에 진입할 수 없습니다.

홈 화면 > 프로젝트 선택 > 로그 > 로그 트렌드

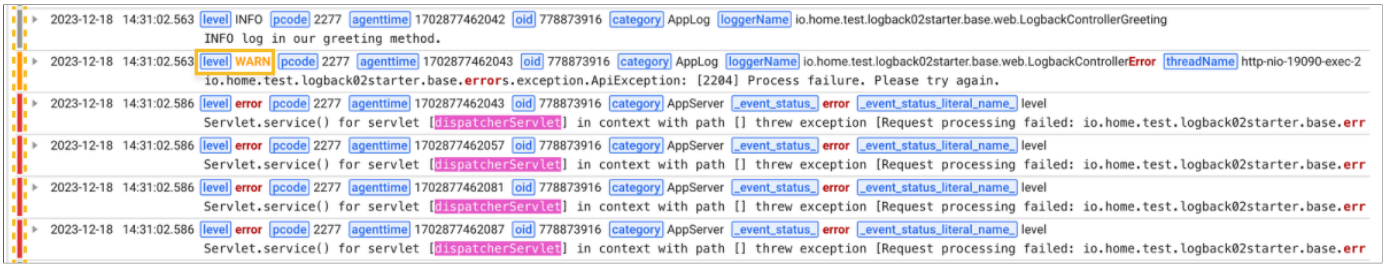
로그 트렌드 메뉴에서 유형별로 분류된 로그의 발생 건수 추이를 통해 특정 에러 유형의 발생 패턴을 확인하고 시간별 상세 로그 데이터를 확인할 수 있습니다. 하이라이트 기능을 통해 원하는 로그를 빠르게 식별할 수 있습니다. 카테고리별로 수집된 로그의 추이를 조회할 수 있습니다. 주요 용어는 다음과 같습니다.

- **Category**: 로그의 수집 및 조회 단위입니다.
- **Content**: 로그 메시지입니다.
- **Search Key**: 로그 파서 설정을 통해 생성합니다.
- **Tag**: 수집된 로그를 검색할 수 있는 검색 키입니다.



데이터 조회하기

- 스크롤이 바닥에 닿으면 다음 데이터를 조회합니다.
- 1에서 탐색할 로그 데이터의 시간과 수집 단위인 카테고리를 지정합니다.
- 카테고리를 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 로그와 타임스탬프를 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.



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

> **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.

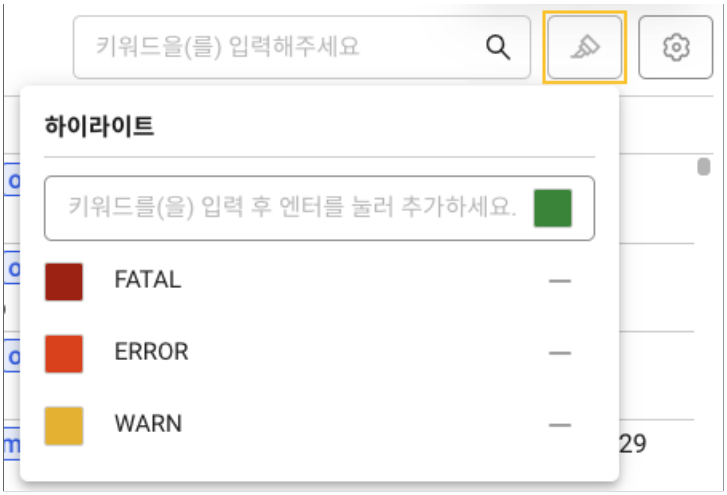
차트로 로그 조회하기

- 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

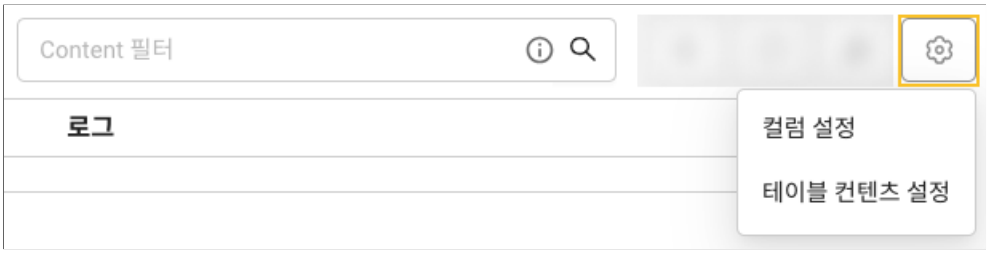
하이라이트

- 원하는 키워드를 손쉽게 식별할 수 있도록 하이라이트 기능을 제공합니다.
- 3 영역 오른쪽 입력창에 하이라이트 할 키워드를 입력하세요. 다음과 같이 하이라이팅 된 키워드를 확인할 수 있습니다.



테이블 설정하기

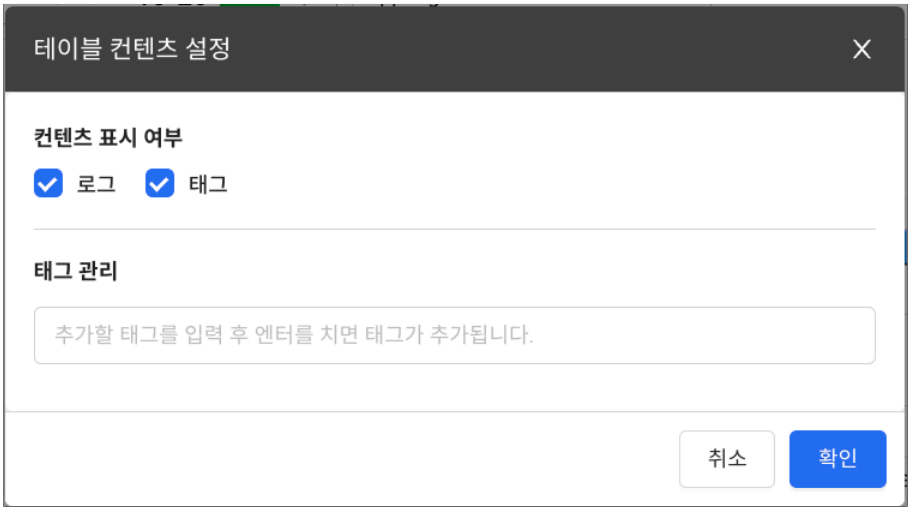
- 3 영역 오른쪽 테이블 설정 메뉴는 라이브 테일, 로그 검색, 로그 트렌드에서 사용할 수 있습니다.
- 테이블 설정 버튼을 선택하면 컬럼 추가와 테이블 컨텐츠 설정 옵션 메뉴가 나타납니다.



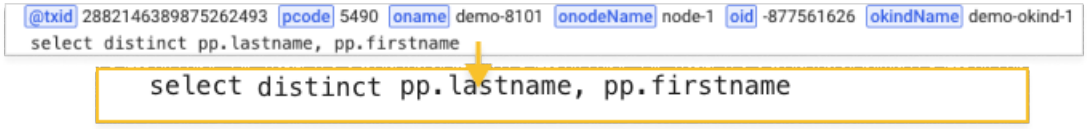
1. **컬럼 설정**

- 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



- 컨텐츠 표시 여부
  - 체크된 항목은 테이블에 표시되지 않습니다. 기본으로 로그, 태그 모두 체크가 되어있으며 두 가지 항목 모두 표시합니다.
  - 다음과 같이 태그를 해제할 경우 테이블에서 로그의 태그는 표시되지 않습니다.



- 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.

> ⓘ 동일한 프로젝트 내 라이브 테일, 로그 검색, 로그 트렌드 메뉴는 테이블 설정을 공유합니다.

로그 검색

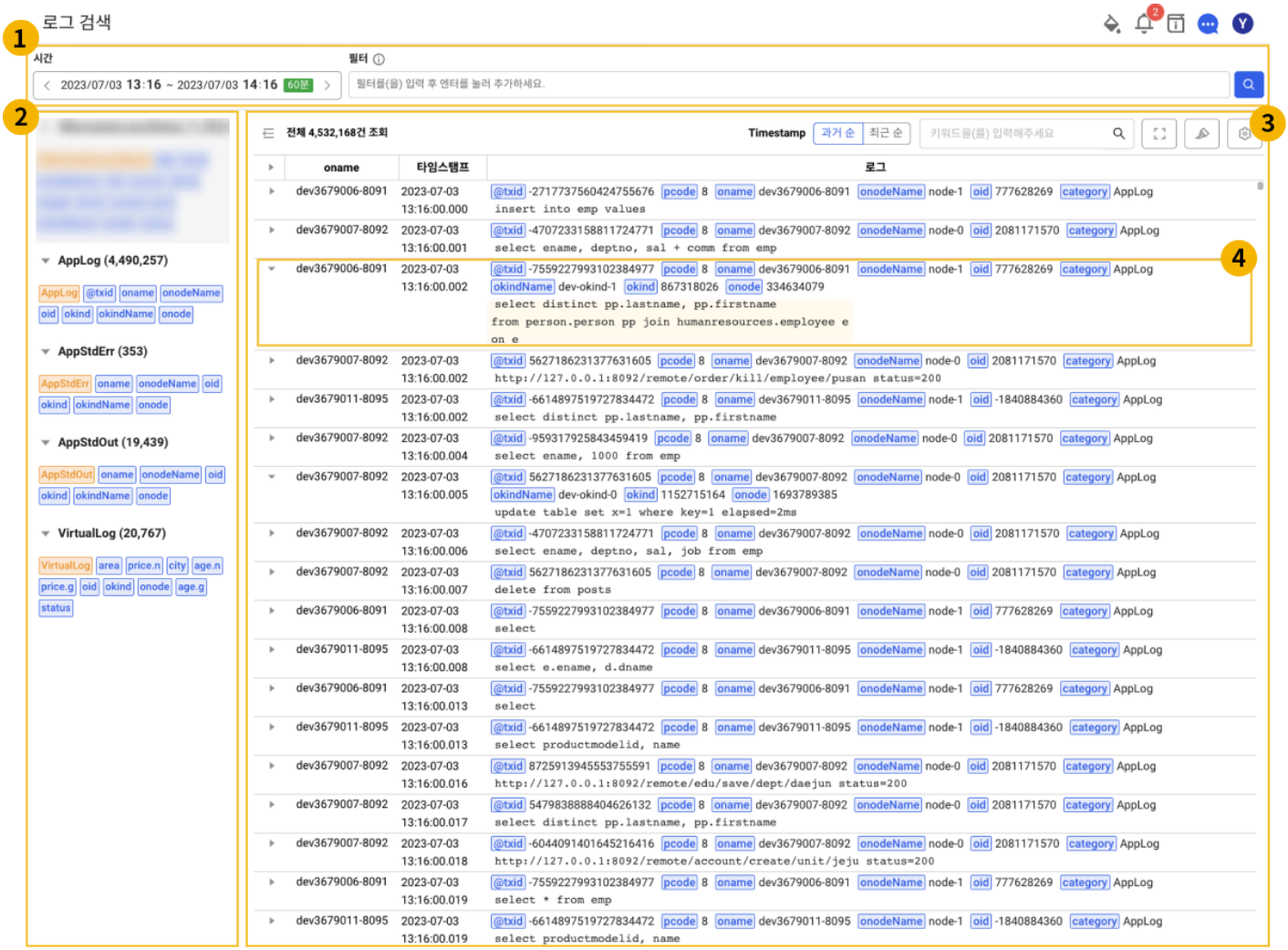
> ⓘ **로그 조회** 권한이 없을 경우 해당 메뉴에 진입할 수 없습니다.

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.

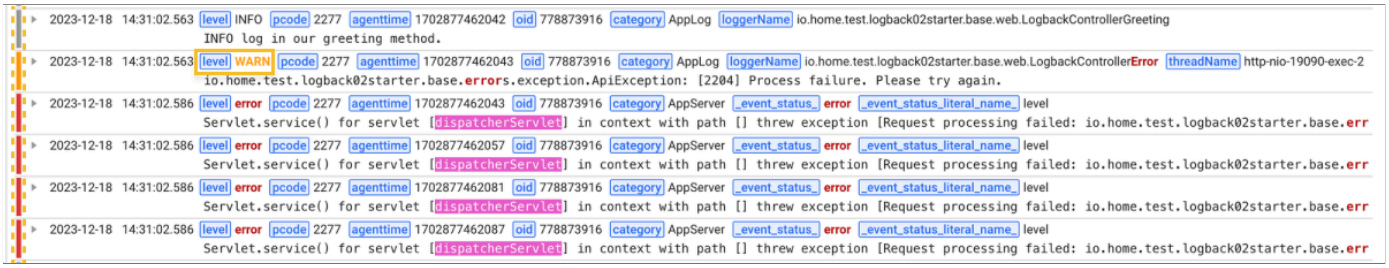
동적 페이지로 검색된 로그 데이터를 정해진 라인 단위로 가져오며, 스크롤 등에 의해 하단에 닿으면 자동으로 다음 데이터를 가져와 표시합니다. 주요 용어는 다음과 같습니다.

- **Category**: 로그의 수집 및 조회 단위입니다.
- **Content**: 로그 메시지입니다.
- **Search Key**: 로그 파서 설정을 통해 생성합니다.
- **Tag**: 수집된 로그를 검색할 수 있는 검색 키입니다.



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 검색 버튼을 선택해 데이터를 조회합니다.
- 3 로그 테이블 상단 오른쪽 전체 화면 아이콘을 선택하면 로그와 타임스탬프를 전체 화면에서 확인할 수 있습니다.
- **에이전트 옵션이 설정된 경우** 로그 레벨을 수집해 로그 레벨 기준 색상이 다음과 같이 표시됩니다.



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

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 4처럼 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 선택창에서 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.

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.

> ⓘ 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 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.

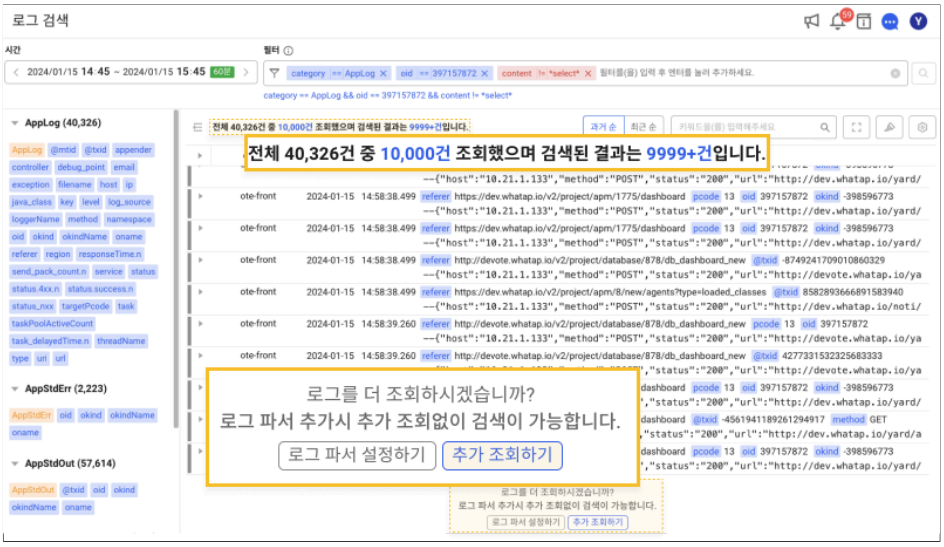
미파싱 키워드 필터 적용

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 설정을 통해 인덱스 키 값을 활용해 검색하는 것을 권장합니다.

1. 카테고리를 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.



> ⓘ
> - 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 문서를 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 UI**를 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(`UnknowHostException`)가 포함된 로그 데이터를 조회합니다.

검색 키 종류

검색 키 종류	검색 키 포멧	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:{regexr}`	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.

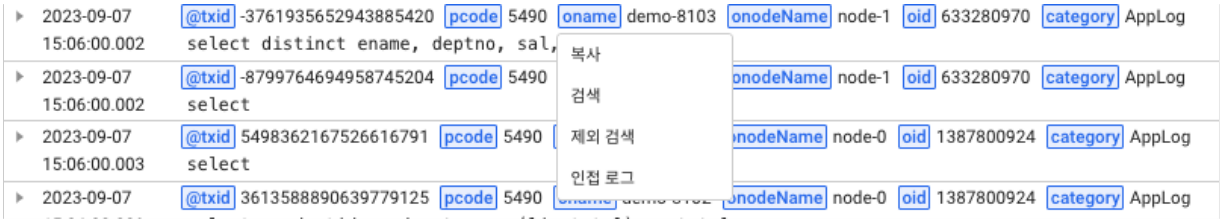
- 검색 값으로는 숫자만 올 수 있습니다.
- `.n` 키워드의 값에는 prefix를 붙이지 않습니다. `.n`이 아닌 키워드는 모두 prefix를 붙여야합니다.

  > 예, `+>searchValue`는 유효하지 않습니다.

문법 종류	설명	예시
>searchValue	검색 값보다 큰 값이 포함된 로그를 조회합니다.	response_time.n>3000
>=searchValue	검색 값보다 크거나 같은 값이 포함된 로그를 조회합니다.	response_time.n>=3000
==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

로그 태그 옵션

로그 태그 선택 시 다음과 같이 드롭다운 메뉴가 나타납니다. 검색, 제외 검색, 인접 로그 옵션을 확인할 수 있습니다.



- **검색**

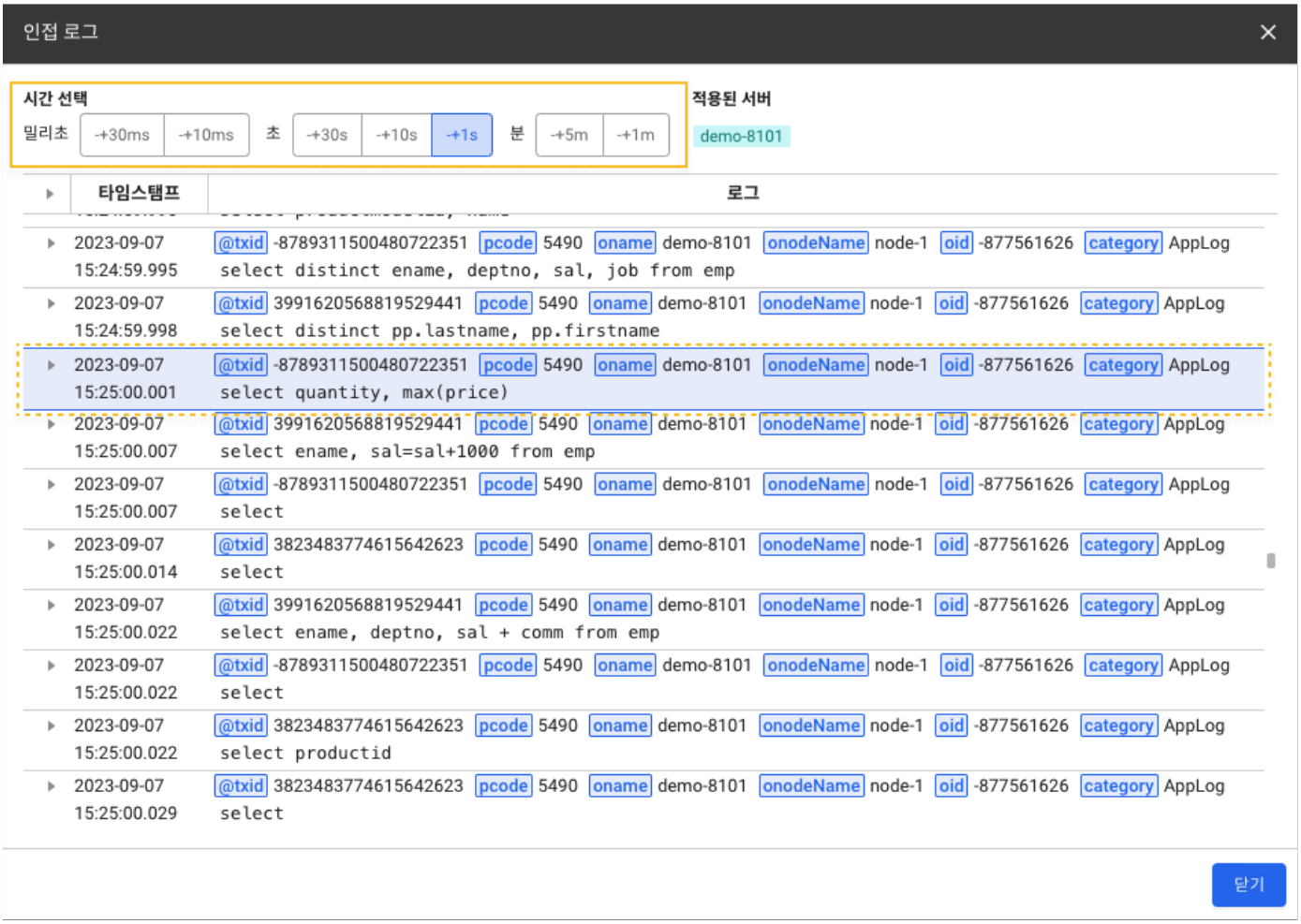
  검색 옵션을 선택하면 필터에 해당 태그가 포함('==') 조건으로 입력됩니다.

- **제외 검색**

  제외 검색 옵션을 선택하면 필터에 해당 태그가 제외('!=') 조건으로 입력됩니다.

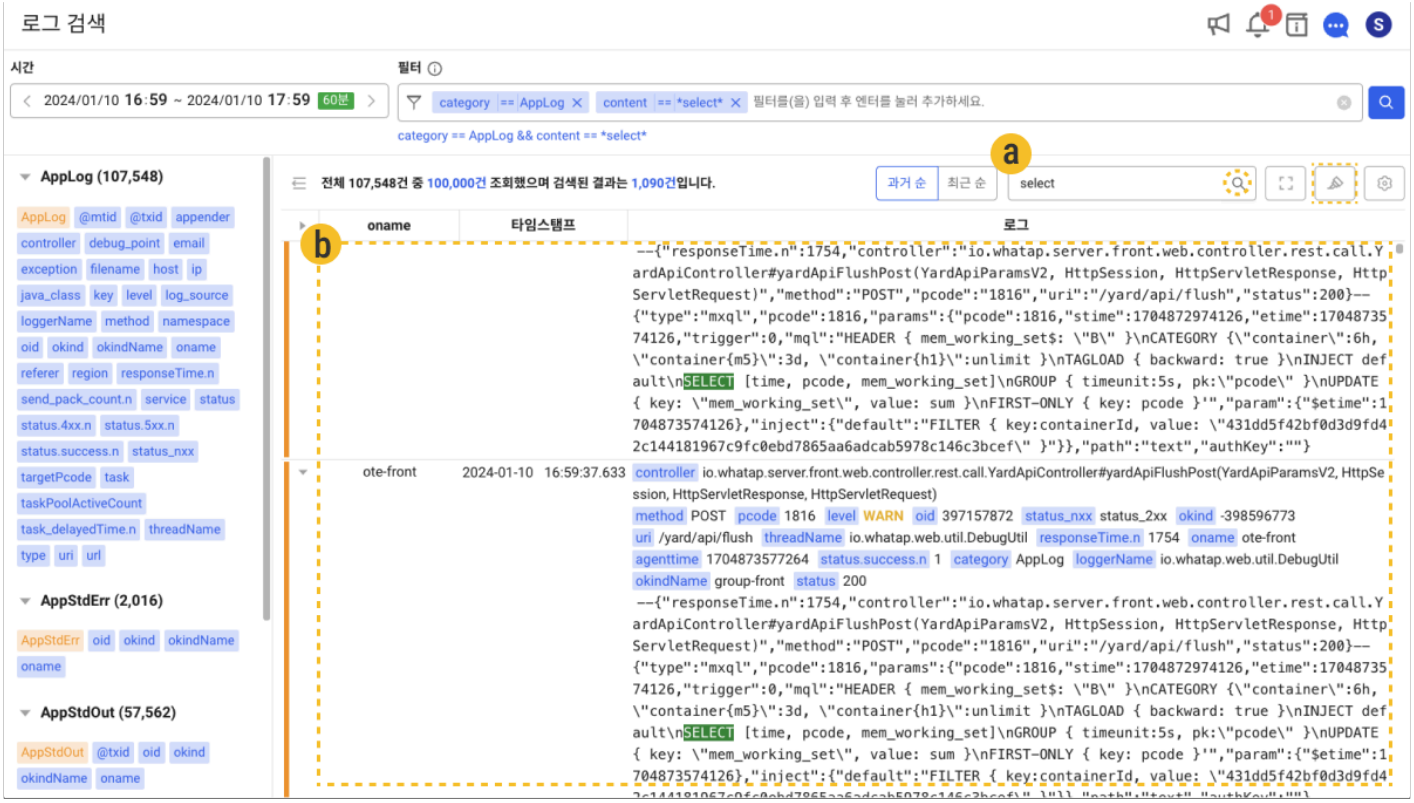
- **인접 로그**

  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. 기준 로그는 파란색 바탕으로 표시됩니다.



콘텐츠 하이라이트

로그의 콘텐츠 중 원하는 키워드를 손쉽게 식별하기 위해 하이라이트 기능을 제공합니다.



- a 키워드 입력창에 하이라이트를 원하는 키워드를 입력 후 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 로그와 타임스탬프를 전체 화면에서 확인할 수 있습니다.

복수 키워드 조건

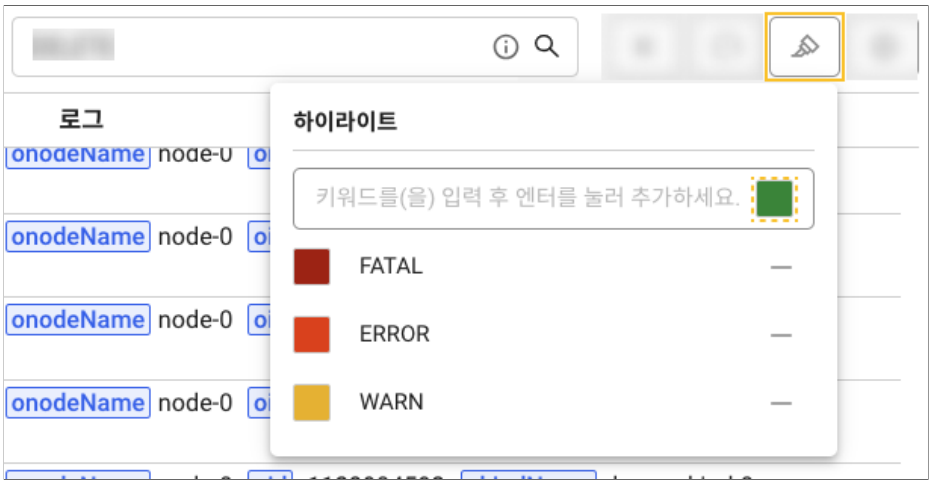
복수 키워드로 하이라이팅을 할 경우 다음과 같이 작성합니다.

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 입력해야합니다.	Whatap\ is good.

하이라이트 색상 설정

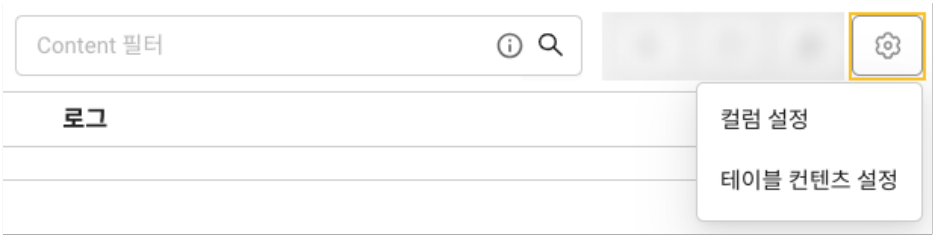
하이라이트 아이콘을 선택해 하이라이팅할 키워드 및 색상을 설정할 수 있습니다.



- 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 설정하기

- 3 영역 오른쪽 테이블 설정 메뉴는 라이브 테일, 로그 검색, 로그 트렌드에서 사용할 수 있습니다.
- 테이블 설정 버튼을 선택하면 컬럼 추가와 테이블 컨텐츠 설정 옵션 메뉴가 나타납니다.

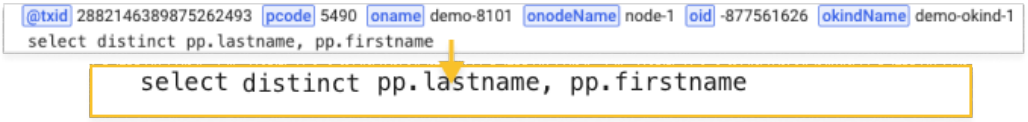


1. 컬럼 설정

- 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

- 컨텐츠 표시 여부
  - 체크된 항목은 테이블에 표시되지 않습니다. 기본으로 로그, 태그 모두 체크가 되어있으며 두 가지 항목 모두 표시합니다.
  - 다음과 같이 태그를 해제할 경우 테이블에서 로그의 태그는 표시되지 않습니다.



- 태그 관리
  - 태그 관리 목록에 태그를 추가하면 추가한 순서대로 로그의 태그가 나열됩니다. 태그의 순서는 드래그하여 변경할 수 있습니다.

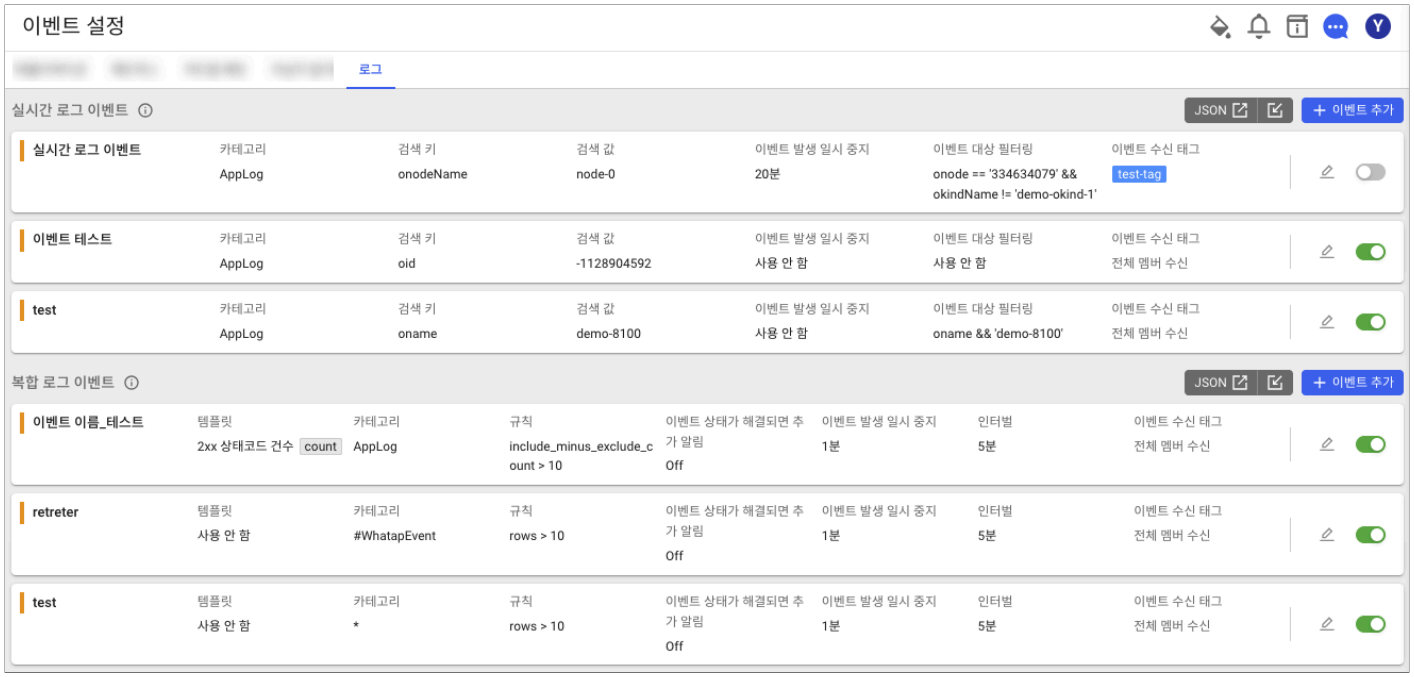
- 추가한 태그를 비활성화하면 비활성화한 태그는 로그의 태그에 노출되지 않습니다.

ⓘ 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.



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 있어야합니다. 사용자별 권한에 대한 자세한 내용은 다음 문서를 참조하세요.
> - 경고 알림과 관련해 모니터링 플랫폼별 지원되는 이벤트 종류를 확인하려면 다음 문서를 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 메트릭스 데이터 카테고리에 포함된 값이여야 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 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 문서를 참조하세요.

실시간 로그 이벤트 추가


이벤트 추가
이벤트 이름 *
제목
이벤트 활성화
레벨 *
위험
경고
정보
메시지 *
메시지
카테고리 *
카테고리을(를) 선택해주세요
검색 키 *
카테고리를 먼저 선택해 주세요.
검색 값 *
카테고리를 먼저 선택해 주세요.
입력된 단어가 일치하는 경우 알림이 발생합니다.
이벤트 대상 필터링
선택 입력
직접 입력
입력값이 없을 경우, 실시간으로 수
선택 입력
직접 입력
검색 키
연산자
검색 값
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`

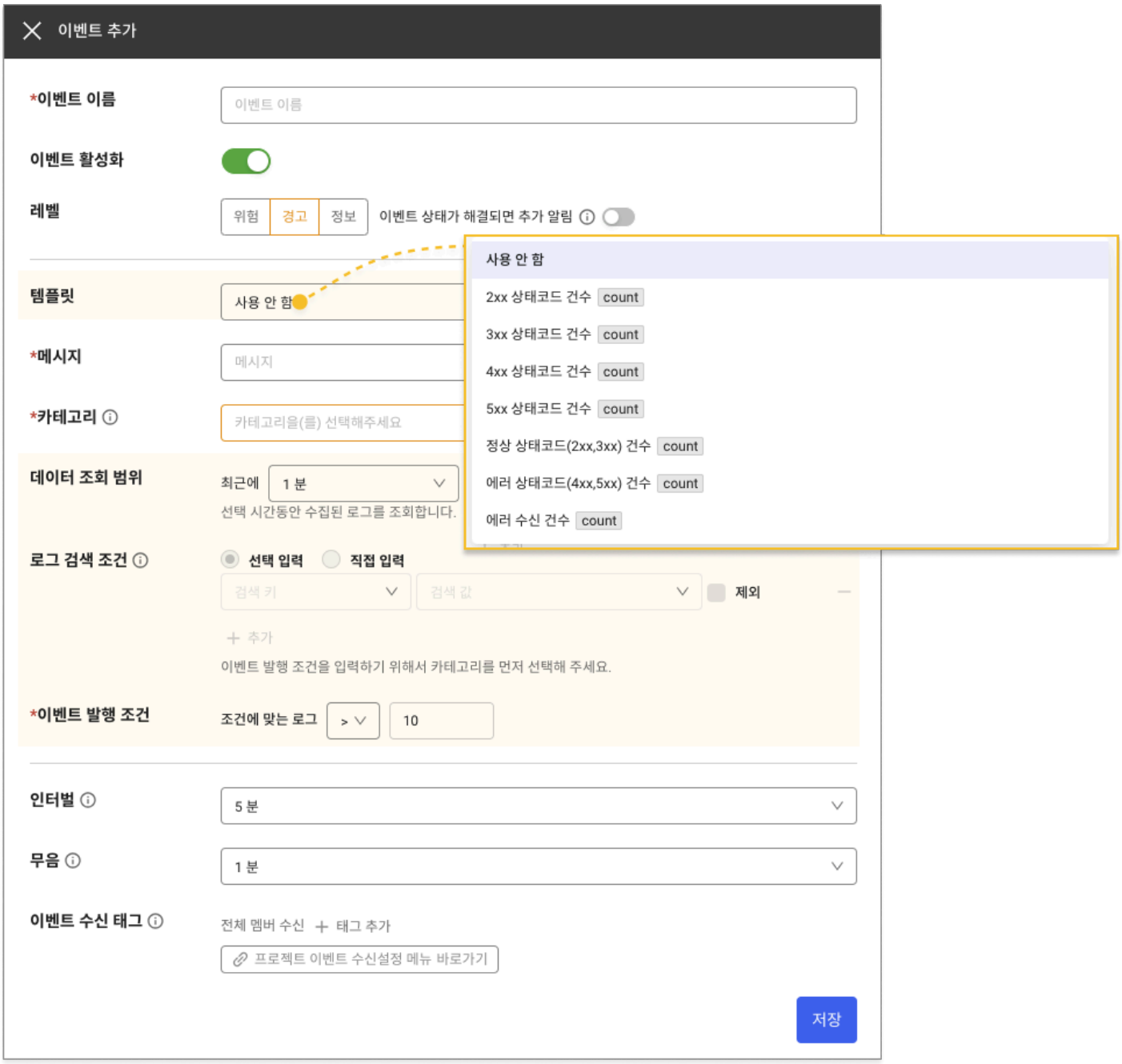
- 검색 값 : 검색 키에 해당하는 실제 데이터를 의미합니다. 로그에서 입력한 단어를 포함할 경우 경고 알림을 보냅니다. 목록에서 선택하거나 직접 입력할 수 있습니다.

  > 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 키와 연산자, 검색 값을 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 oid가 **12345678**인 경우 경고 알림을 보냅니다.

복합 로그 이벤트 추가


이벤트 추가
*이벤트 이름
이벤트 이름
이벤트 활성화
레벨
위험
경고
정보
이벤트 상태가 해결되면 추가 알림
템플릿
사용 안 함
*메시지
메시지
*카테고리
카테고리을(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
저장
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

- 템플릿 : 복합 로그 템플릿을 제공합니다.
- 로그 검색 조건
  - 검색 키에서 이벤트 발생 조건 대상을 선택할 수 있습니다. 선택한 검색 키에 해당하는 검색 값을 선택할 수 있습니다.
  - 검색 키에서 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.
  - + 추가를 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 입력`에 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.

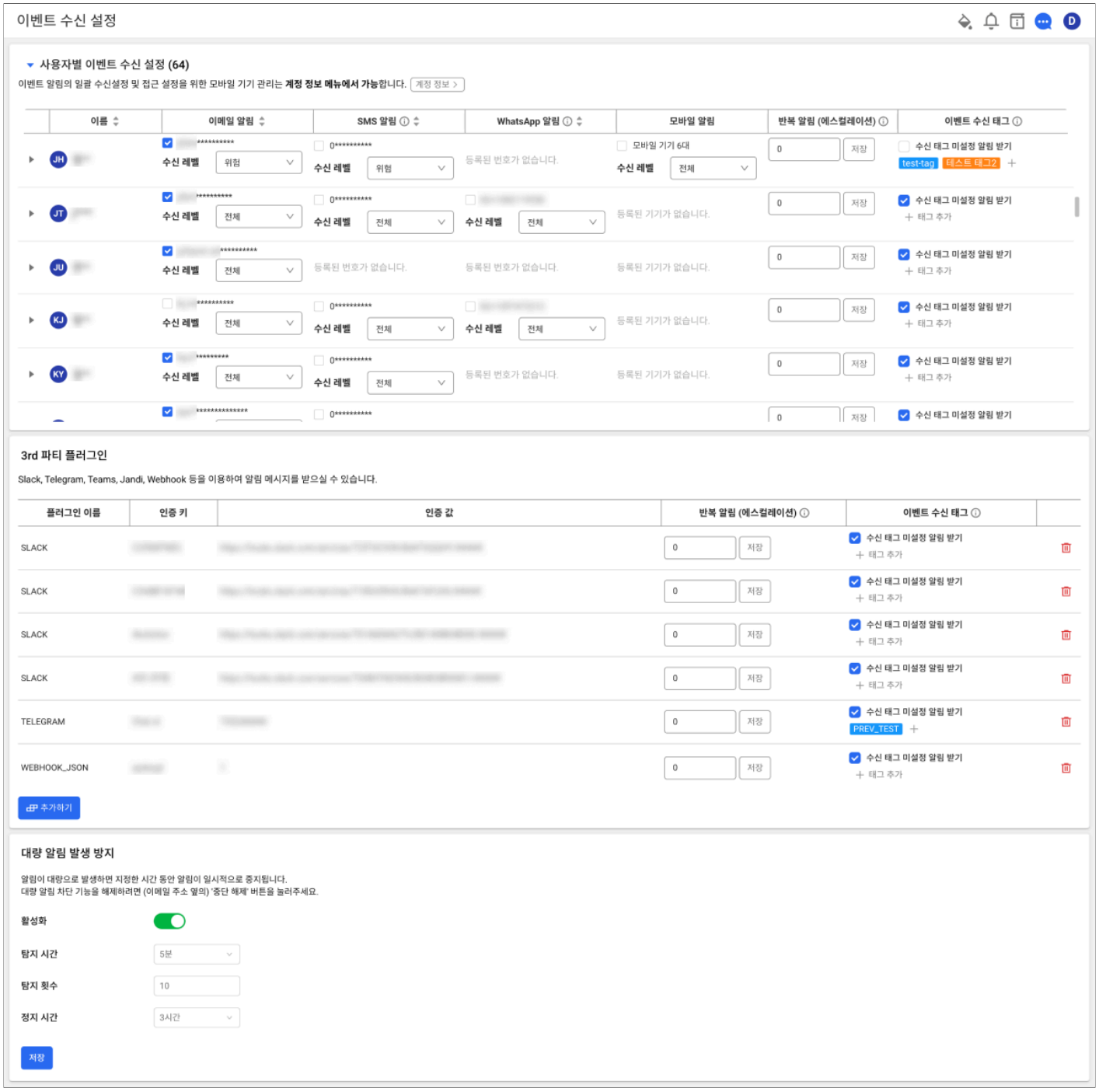
1. 경고 알림 > 이벤트 설정 메뉴로 이동하세요.
2. 로그 탭을 선택하세요.
3. 로그 이벤트 목록 위에 JSON 버튼을 선택하세요. JSON 내보내기 창이 나타납니다.
4. 내보내기 할 항목을 수정 또는 편집하세요.
5. 오른쪽 위에 내보내기 버튼을 선택하세요. 브라우저에서 json 파일을 다운로드합니다.
6. 로그 이벤트 목록 위에 버튼을 선택하세요.
7. 파일 선택 창이 나타나면 앞서 다운로드 받은 json 파일을 선택하세요.
8. JSON 가져오기 창이 나타나면 내용을 수정한 다음 + 목록에 추가하기 버튼을 선택하세요.

> **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 메뉴에서 가능합니다.
계정 정보 >
이름
이메일 알림
SMS 알림
WhatsApp 알림
모바일 알림
반복 알림 (에스컬레이션)
이벤트 수신 태그
수신 레벨
위험
전체
등록된 번호가 없습니다.
등록된 기기가 없습니다.
모바일 기기 6대
저장
수신 태그 미설정 알림 받기
test-tag
테스트 태그2
태그 추가
3rd 파티 플러그인
Slack, Telegram, Teams, Jandi, Webhook 등을 이용하여 알림 메시지를 받으실 수 있습니다.
플러그인 이름
인증 키
인증 값
SLACK
TELEGRAM
WEBHOOK_JSON
PREV_TEST
추가하기
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

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.

> ⓘ
> - 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 관리에서 사용자 전화번호를 설정하세요.

1. 화면 오른쪽 위에 프로필 아이콘을 선택하세요.
2. 팝업 메뉴가 나타나면 계정 관리 버튼을 선택하세요.
3. 사용자 전화번호 섹션에서 일반 휴대전화 버튼을 선택하세요.
4. 전화번호에 인증번호를 수신할 전화번호를 입력하세요.
5. 인증번호 전송 버튼을 선택하세요.
6. 사용자의 휴대전화로 전송된 인증 번호를 입력하세요.
7. 인증하기 버튼을 선택하세요.

> ⓘ
> - 등록한 전화번호를 변경하려면 번호 변경하기 버튼을 선택한 다음 위의 과정을 반복하세요.
> - SMS를 알림으로 수신할 수 있는 전화번호는 **한국 휴대전화 번호**만 등록할 수 있습니다.

WhatsApp 알림 수신 추가하기

WhatsApp을 통해 알림을 수신할 수 있습니다.

1. 화면 오른쪽 위에 프로필 아이콘을 선택하세요.
2. 팝업 메뉴가 나타나면 계정 관리 버튼을 선택하세요.
3. 사용자 전화번호 섹션에서 WhatsApp 버튼을 선택하세요.
4. 전화번호에 인증번호를 수신할 전화번호를 입력하세요.
5. 인증번호 전송 버튼을 선택하세요.
6. WhatsApp 애플리케이션으로 전송된 인증번호 6자리를 입력하세요.
7. 인증하기 버튼을 선택하세요.

> ⓘ 등록한 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 레벨을 전체 또는 위험을 선택하세요.

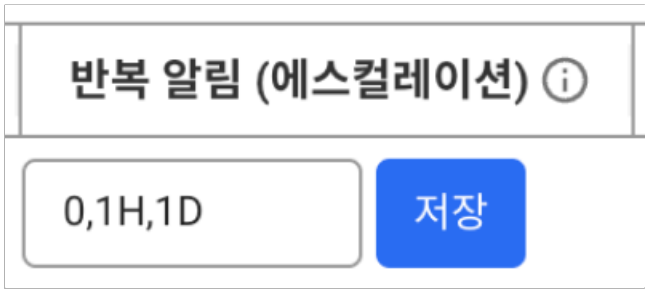
- 전체: 모든 경고 알림을 수신할 수 있습니다.
- 위험: 위험 레벨의 경고 알림만 수신할 수 있습니다.

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.

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.



- 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

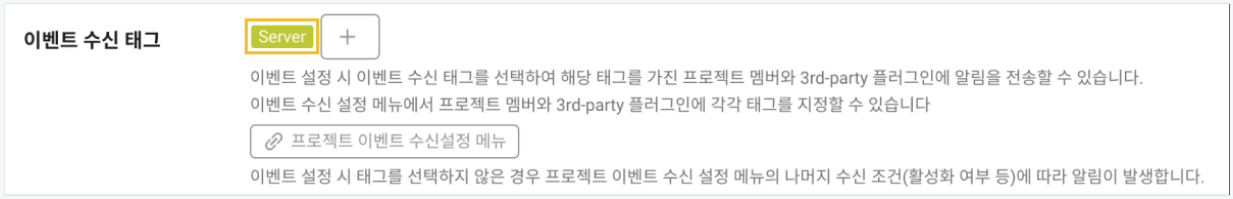
이벤트 수신 태그에 대한 사용 예시를 통해 팀별 또는 사용자별로 경고 알림을 전송하는 설정 방법에 대해 알아봅니다.
다음과 같이 팀 별로 서로 다른 경고 알림을 전송하도록 설정합니다.

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)

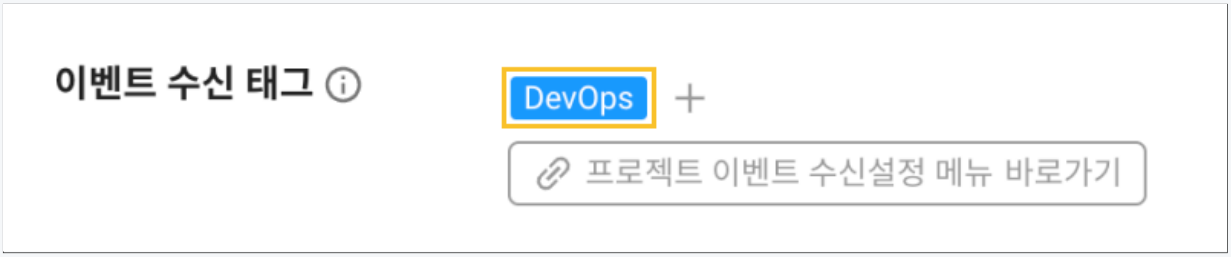
   프로젝트에 속한 멤버들 중 서버팀 소속은 `서버팀`, 데브옵스팀 소속은 `데브옵스팀`으로 이벤트 수신 태그를 설정하세요.

2. **메트릭스 경고 알림 설정하기** (경고 알림 > 이벤트 설정 > 메트릭스 > 이벤트 추가 > 이벤트 수신 설정)



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)



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 입력 란에 태그 이름을 입력한 다음 엔터를 입력하거나 새 태그 생성을 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.

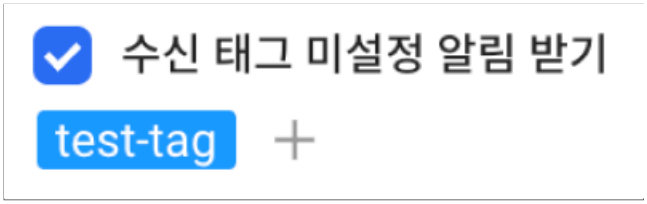
이벤트 수신 태그를 해제합니다.

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 목록에서 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



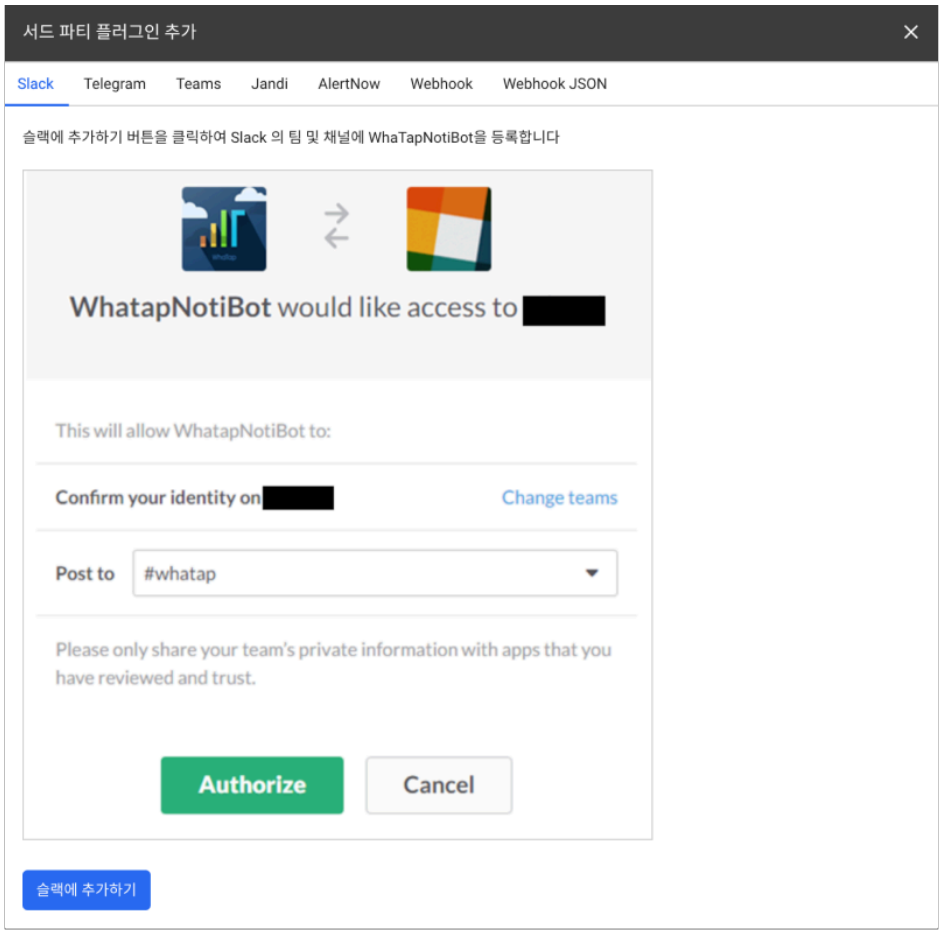
이벤트 수신 태그가 설정되지 않은 경고 알림을 받으려면 수신 태그 미설정 알림 받기 옵션을 선택하세요. 이벤트 수신 태그가 설정된 경고 알림만 받고 싶다면 선택을 해제하세요.

> ⓘ 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.

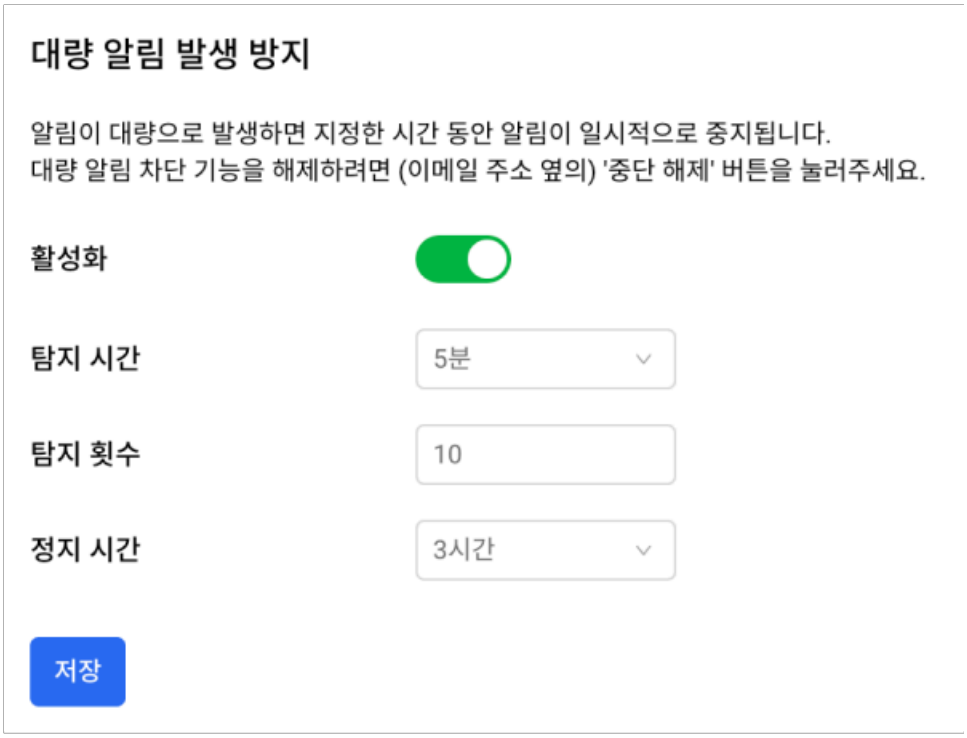


3. 선택한 서비스의 화면 안내에 따라 설정을 진행하세요.
4. 모든 과정을 완료했다면 추가 버튼을 선택하세요.

> ⓘ 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.



- 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.
>
> 
>

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

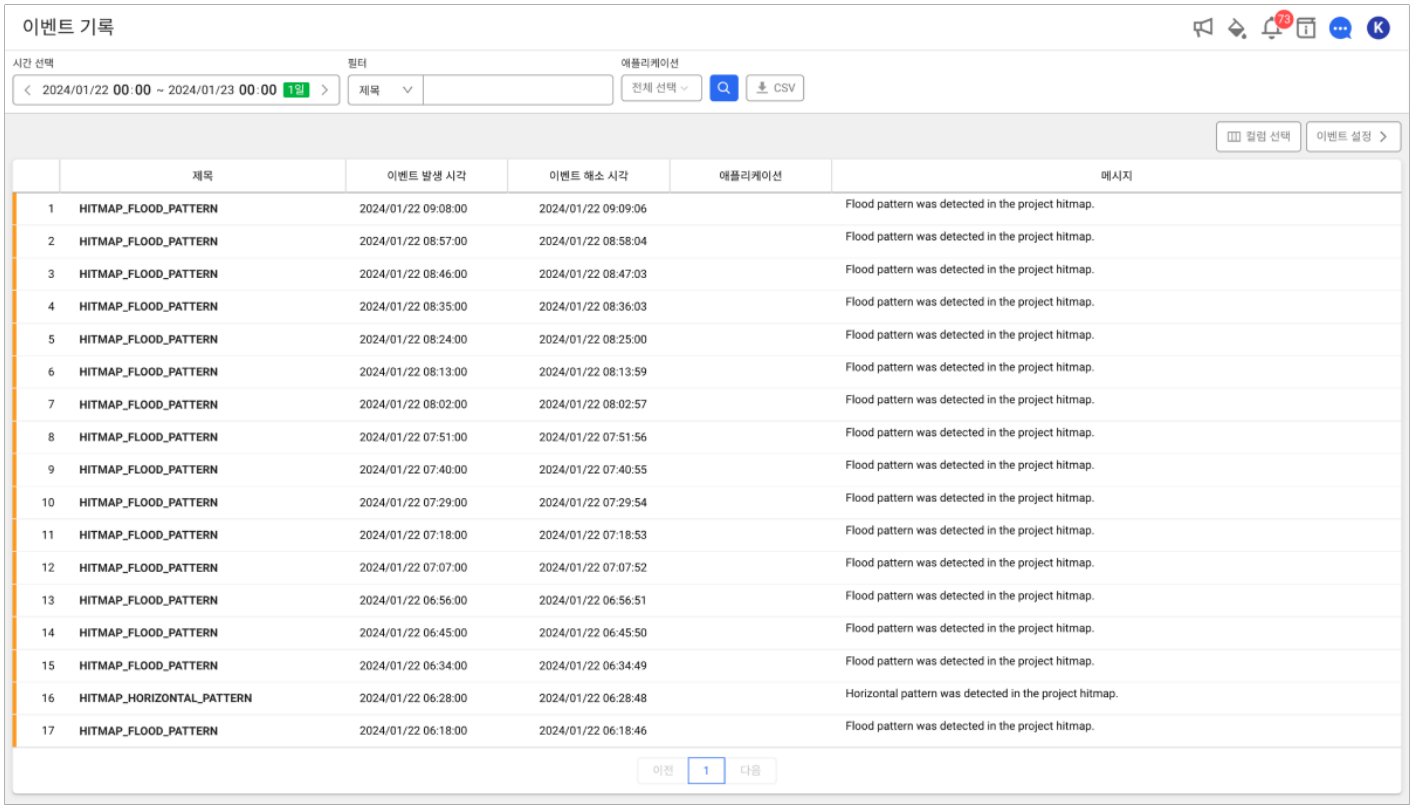
프로젝트에서 발생하는 경고 알림 메시지의 언어를 변경할 수 있습니다.

1. 홈 화면에서 경고 알림 메시지의 언어를 변경할 프로젝트를 선택하세요.
2. 화면 왼쪽 메뉴에서 관리 > 프로젝트 관리를 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.



> ⓘ 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 포함한 에이전트를 선택할 수 있습니다.
- CSV: 조회한 이벤트 기록 결과를 csv 파일로 저장할 수 있습니다. CSV 버튼을 클릭하면 최대 CSV 라인 수를 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 이벤트명과 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 계획에 대한 자세한 내용은 다음 문서를 참조하세요.

- 이벤트 해소 시각: 설정한 이벤트가 해결된 시각입니다. 만약 해당 컬럼이 보이지 않는다면 컬럼 선택 버튼을 클릭한 다음 이벤트 해소 시각을 선택하세요.
- 애플리케이션: 이벤트 설정 메뉴에서 이벤트 추가 시 이벤트 대상 필터링 항목을 설정하면 표시됩니다.