

Network Management System

release date. 2026. 09. 10.

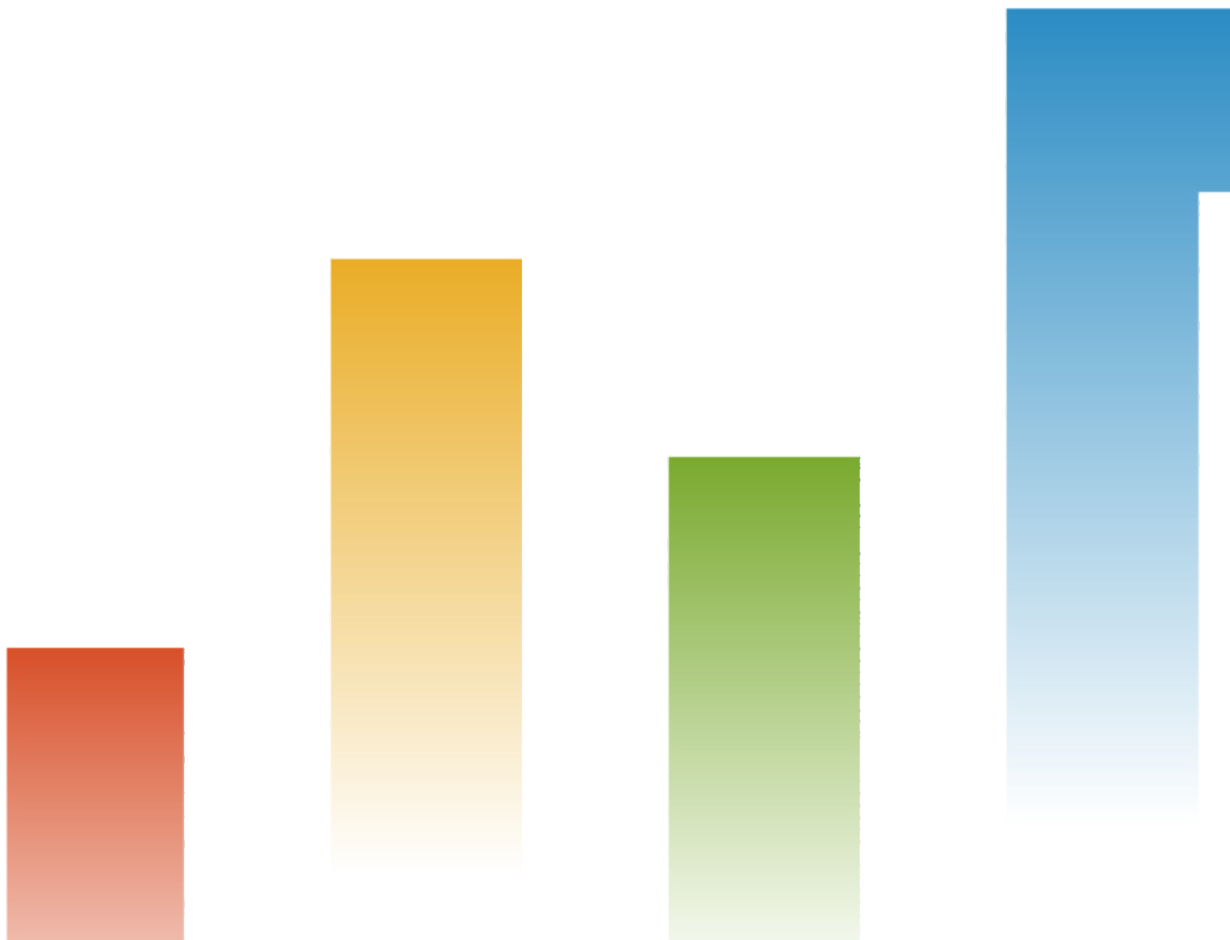


Table of Contents

• Network 관리 시스템	5
◦ 시작하기	9
◦ 설치하기	
▪ 지원 환경	11
▪ 매니저 설치	17
◦ 네트워크 인사이트	
▪ 토폴로지	21
▪ 디바이스 Overview	28
▪ 그룹 내비게이터	31
▪ Flex 보드	38
▪ Flex 보드 사용하기	41
▪ 위젯 관리하기	51
◦ 디바이스 상태	
▪ 인터페이스 상태	56
▪ 사용량 현황	58
▪ 헬스 체크 상태	68
◦ 디바이스 관리	
▪ 디바이스 인벤토리	73
▪ 그룹 관리	79
◦ Network 자동화	
▪ 태스크 설정	83
▪ 태스크 현황	88
▪ 설정 변경 이력	90
▪ 예방 점검 프로파일	93

▪ 예방점검 규칙	96
▪ 예방점검 리포트	99
◦ SNMP OID 관리	102
◦ 경고 알림	104
▪ 이벤트 설정	0
▪ 메트릭스	109
▪ 복합 메트릭스	130
▪ 실시간 로그	137
▪ 복합 로그	150
▪ 이벤트 수신 설정	164
▪ 이벤트 수신 포맷	187
▪ 이벤트 기록 및 모니터링	195
▪ 실시간 알림	203
▪ 시스템 이벤트	206
◦ 통계	
▪ 네트워크 대역폭 사용량	208
◦ 로그	213
◦ 자산 관리	0
◦ 설정	
▪ SNMP Trap 설정	0
▪ Syslog 설정	0
▪ General Config	0
◦ 분석	
▪ 메트릭스 조회	0
◦ 관리	

▪ 매니저 정보.....	0
---------------	---

네트워크 관리 시스템

네트워크 관리 시스템(Network Management System, 이하 NMS)은 라우터, 스위치, 서버, 방화벽, 무선 AP 등 네트워크 장비를 중앙에서 통합 모니터링하여 성능 및 안정성을 유지하는 시스템입니다. 트래픽, 장비 상태, 대역폭 사용량 등을 실시간으로 확인하고, 장애 발생 시 원인을 신속히 파악할 수 있습니다.

NMS는 장애 예방과 문제 탐지에 중점을 두어 성능 저하를 최소화하고 안정적인 서비스 품질(QoS)을 보장합니다. 와탭 NMS를 사용하면 IT 인프라를 효율적으로 운영하고 비즈니스 연속성을 유지할 수 있습니다.

주요 특징점

- 광범위한 멀티 벤더 지원

표준 프로토콜인 SNMP를 기반으로 특정 제조사에 국한되지 않는 강력한 호환성을 제공합니다. 시스코(Cisco), 주니퍼(Juniper) 등 글로벌 벤더부터 국산 장비까지, SNMP를 지원하는 모든 네트워크 장비를 와탭 NMS 하나로 통합 관리할 수 있는 유연한 운영 환경을 지원합니다.

- 효율적인 MIB 관리 및 데이터 조회

직관적인 MIB(Management Information Base) 브라우저를 내장하여 각 네트워크 장비가 제공하는 방대한 데이터를 손쉽게 확인하고 검증할 수 있습니다. 특히 시스템에서 기본으로 제공하지 않는 특정 제조사의 사설(Private) MIB이나 신규 장비의 MIB 파일이 필요한 경우, 사용자가 직접 파일을 업로드하여 관리할 수 있는 기능을 지원합니다.

- OID 리스트 제공

운영 현장에서 활용 빈도가 높은 핵심 OID(Object Identifier) 항목들을 체계적으로 선별하여 리스트 형태로 제공합니다. 관리자가 복잡한 MIB 구조 내에서 개별 OID를 직접 탐색하고 검증해야 하는 번거로움을 최소화하며, 장비 및 인터페이스별 임계치 설정에 필수적인 성능 지표를 신속하게 식별하고 적용할 수 있도록 지원하여 관리 최적화와 운영 효율성을 극대화합니다.

- 유연한 설치 환경 및 하이브리드 인프라 지원

다양한 운영체제(OS)를 지원하여 설치 환경의 제약을 최소화하였으며, 온프레미스(On-premise)와 클라우드 등 고객의 인프라 환경에 최적화된 구축 방식을 제공합니다. 이를 통해 폐쇄적인 내부망뿐만 아니라 복잡한 하이브리드 클라우드 환경에서도 중단 없는 모니터링 체계를 구축할 수 있으며, 기업의 보안 정책과 네트워크 구조에 최적화된 유연한 배치 모델을 지원합니다.

주요 기능

- 장비 및 성능 실시간 모니터링 (SNMP Polling)

네트워크 장비의 핵심 가동 지표와 성능 데이터를 주기적으로 수집하여 최적의 운영 상태를 유지합니다. CPU 부하, 메모리 사용량, 세션 점유율 등 하드웨어 자원의 상태를 정밀하게 모니터링하며, 인터페이스별 데이터 유입·유출량(Throughput)과 포트의 물리적 연결 상태(Link Up/Down)를 실시간으로 파악하여 네트워크 성능 병목 현상을 사전에 방지합니다.

- 계층 구조 및 토폴로지 맵 (Hierarchy & Topology)

네트워크 자산의 소속 관계와 연결 상태를 시각화하여 관리의 직관성을 제공합니다. 장비를 지역, 건물, 업무 서비스 단위의 트리 구조로 체계화하여 관리하는 한편, 장비 간의 물리적, 논리적 연결 관계를 토폴로지 맵으로 구현함으로써 전체적인 네트워크 구성과 장애 발생 시 영향 범위를 즉각적으로 파악할 수 있습니다.

- 가용성 및 품질 점검 (Health Check)

네트워크 장비와 운영 서비스가 정상적으로 동작하고 있는지 응답성을 기반으로 상시 점검합니다. ICMP(Ping) 및 TCP 프로토콜을 통해 장비의 실시간 생존 여부(Alive)를 확인하고, 응답 시간(RTT)과 네트워크 지연 변이(JITTER) 수치를 분석하여 사용자 서비스 품질(SLA)이 저하되지 않도록 관리합니다.

- 실시간 이벤트 및 로그 관리

장비에서 발생하는 SNMP Trap과 Syslog 메시지를 실시간으로 분석하여 장애 상황을 관리자에게 즉시 전달하며, 저장된 이벤트 히스토리를 바탕으로 특정 시점의 장애 원인을 정밀하게 검색하고 추적할 수 있는 분석 환경을 지원합니다.

- 자동 탐지(Auto Discovery)

복잡하고 방대한 네트워크 환경을 일일이 수동으로 등록하는 번거로움 없이 시스템이 스스로 식별합니다. SNMP 프로토콜을 활용해 네트워크 내 장비를 스캔하고, 장비 유형 및 인터페이스 구성, 상세 스펙 정보를 자동으로 데이터베이스화하여 초기 구축 시간을 단축시킵니다.

데이터 수집 범위

WhaTap NMS(Network Management System)은 다음과 같은 네트워크 데이터 수집 방식을 지원합니다.

- SNMP Polling

네트워크 장비 상태 및 성능 데이터를 주기적으로 요청하여 수집하며 **SNMP v1/v2c/v3** 프로토콜을 모두 지원합니다.

- SNMP Trap

네트워크 장비에서 발생하는 이벤트 및 알림 정보를 수집, 처리하며, **SNMP Trap v1/v2c/v3** 프로토콜을 지원합니다.

- **Syslog**

네트워크 장비에서 생성되는 로그 데이터를 수집하여 실시간으로 분석합니다.

- **ICMP**

ICMP 프로토콜을 사용하여 장비의 **Alive, RTT, Jitter** 등을 측정합니다.

- **TCP**

TCP 포트를 기반으로 장비 또는 서비스의 **Alive** 및 **RTT** 등을 측정합니다.

매니저 주요 서비스

NMS는 매니저에서 에이전트 데이터를 수집·정제하며, 와탭 연동 전 사전 설정과 테스트를 수행합니다.

Web-based Management Console & APIs

uvicorn.service 는 관리 UI 및 API 서비스로 NMS 설정 관리, 시스템 상태 확인, 그리고 설정 백업, 복구와 같은 운영 관리 기능 전반을 로컬 환경에서 제공합니다.

❗ 일반적으로 NMS 운영 시 매니저 접속은 필요하지 않습니다. 접속이 필요할 경우 와탭 기술팀에 문의하십시오.

- **사용 포트:** HTTP 5000, HTTPS 8443(설정 시)

- **서비스 시작 및 중지:** 다음 명령어를 통해 **uvicorn.service** 를 시작, 중지 또는 재시작 할 수 있습니다.

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

NMS 엔진

nmscore.service 는 네트워크 관리 시스템(NMS)의 엔진 역할을 하는 서비스입니다. 네트워크 장비 및 트래픽 모니터링, 관리 및 이벤트 처리 기능을 제공합니다.

- **사용 포트:**

- **SNMP Polling:** UDP 161 (default)
- **SNMP Trap:** UDP 162 (default)
- **Syslog:** UDP 514 (default)
- **서비스 시작 및 중지:** 다음 명령어를 통해 `nmscore.service` 를 시작, 중지 또는 재시작 할 수 있습니다.

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

Health Check

`icmptcphealthd.service` 는 네트워크 장비를 대상으로 ICMP 및 TCP 기반의 Health Check를 수행하며, 주기적인 상태 점검을 통해 장비의 가용성과 연결 상태를 지속적으로 모니터링합니다

- **서비스 시작 및 중지:** 다음 명령어를 통해 `icmptcphealthd.service` 를 시작, 중지 또는 재시작 할 수 있습니다.

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

시작하기

와탭 모니터링을 시작하기 위해 필요한 단계를 안내합니다.

[Step 1. 회원 가입하기](#)

[Step 2. 제품 선택하기](#)

[Step 3. 프로젝트 생성하기](#)

이후 지원 환경을 확인한 후 [매니저 설치](#) 단계로 이동합니다.

회원 가입하기

와탭 모니터링 서비스를 사용하려면 먼저 [회원 가입](#)이 필요합니다. 회원 가입에 관한 자세한 내용은 [계정 관리 > 회원 가입](#) 문서를 참고하세요.

제품 선택하기

1. [와탭 모니터링 서비스](#)에 로그인합니다.
2. ≡ [전체 프로젝트](#) > + [프로젝트](#) 버튼을 클릭합니다.
3. ❶ [상품 선택](#) 화면에서 모니터링할 제품의 [생성하기](#) 버튼을 클릭하세요.

프로젝트 생성하기

모니터링할 제품을 선택했다면, 에이전트를 설치하기 전에 먼저 프로젝트를 생성합니다.

1. ❷ [프로젝트 생성](#) 화면에서 프로젝트를 생성하려면 다음 항목을 입력하거나 선택하세요.
 - [프로젝트 이름](#)(필수): 프로젝트의 이름을 입력합니다.
 - [데이터 서버 지역](#)(필수): 데이터 서버가 위치한 리전(지역)을 선택합니다. 리전은 클라우드 서비스를 제공하는 데이터 센터의 묶음입니다. 선택한 리전에 사용자의 데이터가 저장됩니다.
 - [타임 존](#)(필수): 알림 및 보고서 생성 시 기준이 되는 시간을 설정합니다.

- **알림 언어 설정**(필수): 프로젝트에서 발생하는 경고 알림 메시지의 언어를 설정합니다. (한글, 영어 지원)
- **프로젝트 그룹**: 여러 프로젝트를 그룹으로 묶어 관리할 수 있습니다. 소속될 그룹이 있으면 선택하세요. 없다면 그룹 추가 버튼을 클릭해 그룹을 추가할 수 있습니다.
- **프로젝트 설명**: 프로젝트에 대한 추가 설명을 입력합니다.

2. 모든 설정을 완료하면 **프로젝트 생성하기** 버튼을 클릭하세요.

❗ 조직을 선택한 상태에서 프로젝트를 추가할 경우 **조직 하위 그룹**을 필수로 설정해야 합니다. 그룹에 대한 자세한 설명은 [다음 문서](#)를 참고하세요.

지원 환경

와탭 Network Control Management System은 Standalone 방식으로 단독 가상 머신(VM)에 설치됩니다. 이를 통해 네트워크 관리 시스템이 독립적으로 동작하며, 네트워크 모니터링 및 관리에 필요한 모든 기능을 안정적으로 제공합니다.

시스템 요구 사양

와탭 Network Management System의 안정적인 성능을 보장하기 위해 권장되는 최소 사양입니다.

항목	사양
CPU	4core(최소 2core)
Memory	최소 16GB 이상(최소 8G)
Disk	50G 이상 SSD 권장(최소 30G)
Network Interface	1Gbps 이상

OS별 지원

OS	Python 버전	지원 여부
Ubuntu 22.04	3.10	지원, 권장
Ubuntu 23.04	3.11	지원
Ubuntu 24.04	3.12	지원
Rocky 9.4	3.9	지원, 권장
Rocky 8.10	3.11	지원

OS	Python 버전	지원 여부
Redhat 8.10	3.11	지원, 권장

Python 버전별 지원

OS 종류에 관계 없이 Python 버전에 따라 지원이 가능합니다. 단, 가급적 권장 OS 사용을 권고합니다.

계열	지원 Python 버전
Debian 계열	Python 3.10, 3.11, 3.12
Redhat 계열	Python 3.9, 3.10, 3.11, 3.12

사용 TCP/UDP 포트

명시된 TCP, IP Port번호는 해당 서비스가 사용하는 기본 포트로 고객의 환경에 맞게 변경할 수 있습니다.

구분	TCP	UDP	설명	방향	기타
SNMP	-	161	polling	Outbound	Default port
SNMP Trap	-	162	trap message	Inbound	Default port
syslog	-	514	syslog message	Inbound	Default port
manager U/I	5000(http) 8443(https)	-	NMS Control Manager GUI	Inbound	기본 http, https 사용 시 8443 포트 허용 필요
whatap 수집서버	6600	-	데이터 전송	Outbound	-
ICMP	-	-	ICMP health Check	-	ICMP 프로토콜 허용 필요

구분	TCP	UDP	설명	방향	기타
TCP	-	-	TCP 기반 health Check	In/Out	모니터링 대상 TCP 포트 번호 연결 허용 필요(Options)

서비스 제공 형태

와탭 모니터링은 SaaS 또는 온프레미스(설치형) 방식으로 이용할 수 있습니다. 어느 쪽을 선택해도 같은 에이전트로 같은 모니터링 기능을 사용합니다.

Deployment	Support	Description
SaaS	✓	와탭이 운영하는 수집 서버에 연결. 리전별 주소는 방화벽 항목 참조
온프레미스(설치형)	✓	수집 서버를 직접 구축해 운영(폐쇄망 환경 지원). 도입 범위는 영업 담당자와 협의

❗ 인터넷에 연결하지 않는 폐쇄망 환경에서도 온프레미스로 구축할 수 있습니다.

제공 형태에 따른 기능 차이

어느 형태를 선택해도 모니터링 기능은 같습니다. 모바일 앱만 예외로 service.whatap.io SaaS에서만 사용할 수 있습니다.

❗ 온프레미스에서 일부 기능을 사용하려면 별도 계약이 필요합니다.

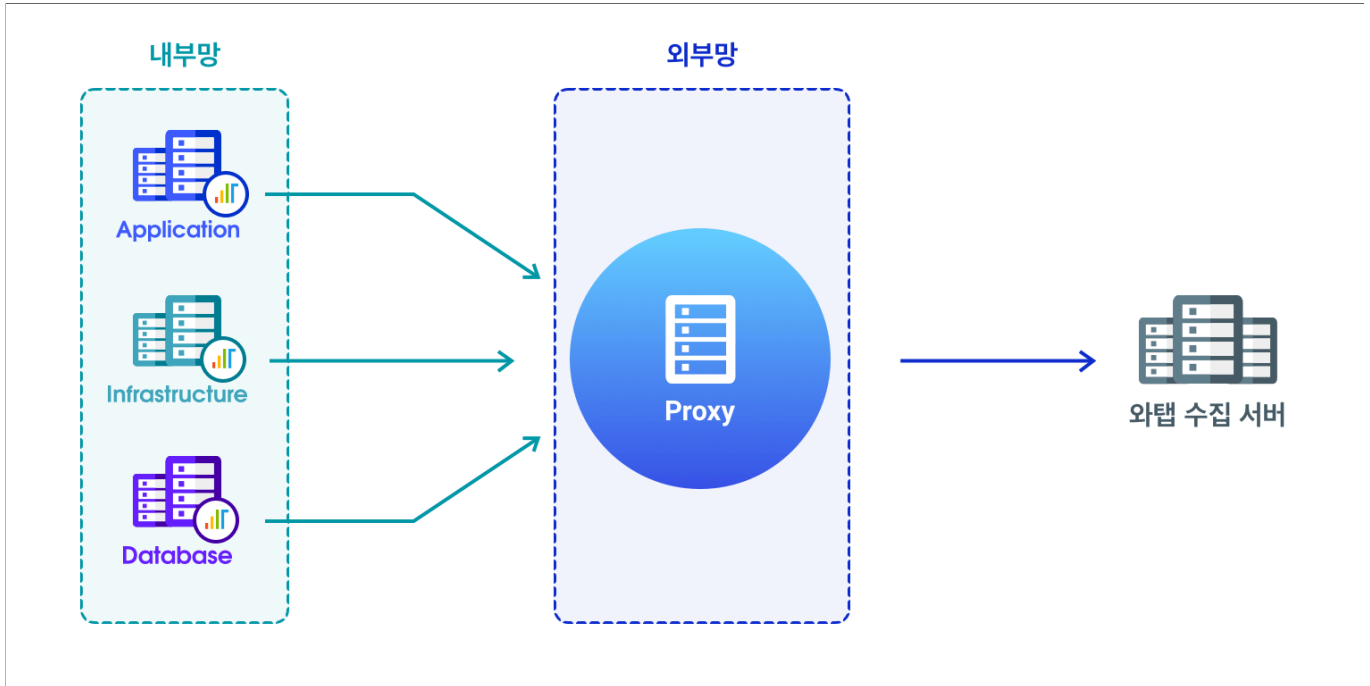
방화벽

와탭 에이전트는 수집 서버 **TCP 6600** 포트로 접근할 수 있어야 합니다. 모니터링 대상과 가까운 수집 서버 주소를 허용하세요.

출발지: 와탭 에이전트

클라우드	목적지	목적지 IP	포트
AWS	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
	와탭 싱가포르 수집 서버	18.138.0.93 / 18.139.67.236	TCP 6600
	와탭 자카르타 수집 서버	108.136.91.69 / 108.137.158.44	TCP 6600
	와탭 태국 수집 서버	43.209.109.219 / 43.209.48.86	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 버지니아 수집 서버	107.23.220.101 / 54.236.221.105	TCP 6600
	와탭 프랑크푸르트 수집 서버	3.125.142.162 / 3.127.76.140	TCP 6600
Azure	와탭 서울 수집 서버	52.231.66.38 / 20.194.5.115	TCP 6600
	와탭 도쿄 수집 서버	52.246.169.54 / 20.210.27.232	TCP 6600
Kakao	와탭 서울 수집 서버	61.109.237.237 / 61.109.238.166	TCP 6600

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



주요 서비스 구성 요소 및 포트

NMS Control Manager Web-Based U/I

`uvicorn.service` 는 로컬 환경에서 실행되는 관리 UI 및 API 서비스로, NMS 설정 관리, 시스템 상태 확인, 그리고 설정 백업·복구와 같은 운영 관리 기능 전반을 제공합니다.

- **사용 포트:** HTTP 5000, HTTPS 8443(설정 시)
- **서비스 시작 및 중지:** 다음 명령어를 통해 `uvicorn.service` 를 시작, 중지 또는 재시작할 수 있습니다.

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

❗ 매니저 접속 정보는 와탭 기술팀에 문의하시기 바랍니다.

NMS 엔진

`nmscore.service` 는 네트워크 관리 시스템(NMS)의 엔진 역할을 하는 서비스입니다. 네트워크 장비 및 트래픽 모니터링, 관리 및 이벤트 처리 기능을 제공합니다.

- **사용 포트:**
 - **SNMP Trap:** UDP 162 (default)
 - **Syslog:** UDP 514 (default)
- **서비스 시작 및 중지:** 다음 명령어를 통해 `nmscore.service` 를 시작, 중지 또는 재시작할 수 있습니다.

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

Health Check

`icmptcphealthd.service` 는 네트워크 장비를 대상으로 ICMP 및 TCP 기반의 Health Check를 수행하며, 주기적인 상태 점검을 통해 장비의 가용성과 연결 상태를 지속적으로 모니터링합니다

- **서비스 시작 및 중지:** 다음 명령어를 통해 `icmptcphealthd.service` 를 시작, 중지 또는 재시작할 수 있습니다.

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

매니저 설치

와탭 NMS(Network Management System) 에이전트인 **NMS Manager** 설치 방법을 안내합니다. 설치를 진행하기 전에 아래 사항을 반드시 확인해주세요.

- ❗ 매니저 설치 전, 와탭 회원 가입과 프로젝트 생성이 완료되어야 합니다. 자세한 내용은 [시작하기](#) 문서를 참고하시기 바랍니다.
 - 시스템 요구 사항은 [지원 환경](#) 문서에서 확인할 수 있습니다.

매니저 설치

프로젝트 액세스 키 확인

액세스 키는 와탭 서비스 활성화를 위한 고유 ID입니다. 액세스 키를 자동으로 발급받은 후 다음 단계를 진행합니다.

- 설치 안내 섹션에서 **프로젝트 액세스 키 발급받기** 버튼을 클릭하세요.
- 발급된 액세스 키를 **복사** 버튼을 클릭해 복사합니다. 액세스 키는 재확인 할 수 있습니다.

- ✅ 프로젝트를 생성한 후, 자동으로 **에이전트 설치** 페이지로 이동합니다. **에이전트 설치** 페이지로 이동하지 않는다면 화면 왼쪽 메뉴에서 **관리 > 매니저 설치**를 선택하세요.

설치 명령어 실행

관리 > 매니저 설치 안내 섹션에서 프로젝트 액세스 키 확인 후 순서대로 운영체제에 맞는 설치를 진행하세요.

Red Hat-based Linux

- ❗ WhaTap Network Management System은 Rocky, Redhat Linux 환경을 지원합니다.

1. 다음 명령어를 실행하여 와탭 리포지토리를 등록하세요.

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

2. 다음 명령어를 실행하여 패키지를 설치하세요.

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

3. 다음 명령어를 실행하세요. 액세스 키를 입력하고 와탭 서버 호스트를 설정합니다.

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

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

Whatap-nms access key manager tool

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

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

4. 설치가 완료된 후 다음 명령어를 실행하여 NMS 매니저가 정상적으로 실행 중인지 확인하세요.

```
sudo service uvicorn status
sudo service nmsscore status
sudo service icmptcphealthd status
```

Debian-based Linux

ⓘ WhaTap Network Management System은 Ubuntu 환경을 지원합니다.

1. 다음 명령어를 실행하여 와탭 리포지토리를 등록하세요.

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

2. 다음 명령어를 실행하여 패키지를 설치하세요.

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

3. 다음 명령어를 실행하세요. 액세스 키를 입력하고 와탭 서버 호스트를 설정합니다.

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

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

Whatap-nms access key manager tool

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

example:
# wtinitset -a znun32arkonto-76rbkt4ftlrwh9-1234ogewww1lhs -s 192.168.10.100
# wtinitset -a znun32arkonto-76rbkt4ftlrwh9-1234wogewww1lhs -s 10.10.10.10/10.10.10.20
```

4. 설치가 완료된 후 다음 명령어를 실행하여 NMS 매니저가 정상적으로 실행 중인지 확인하세요.

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

NMS 서비스 접속

설치가 완료되면 <https://service.whatap.io>에 접속하여 NMS 모니터링을 시작합니다.

토폴로지

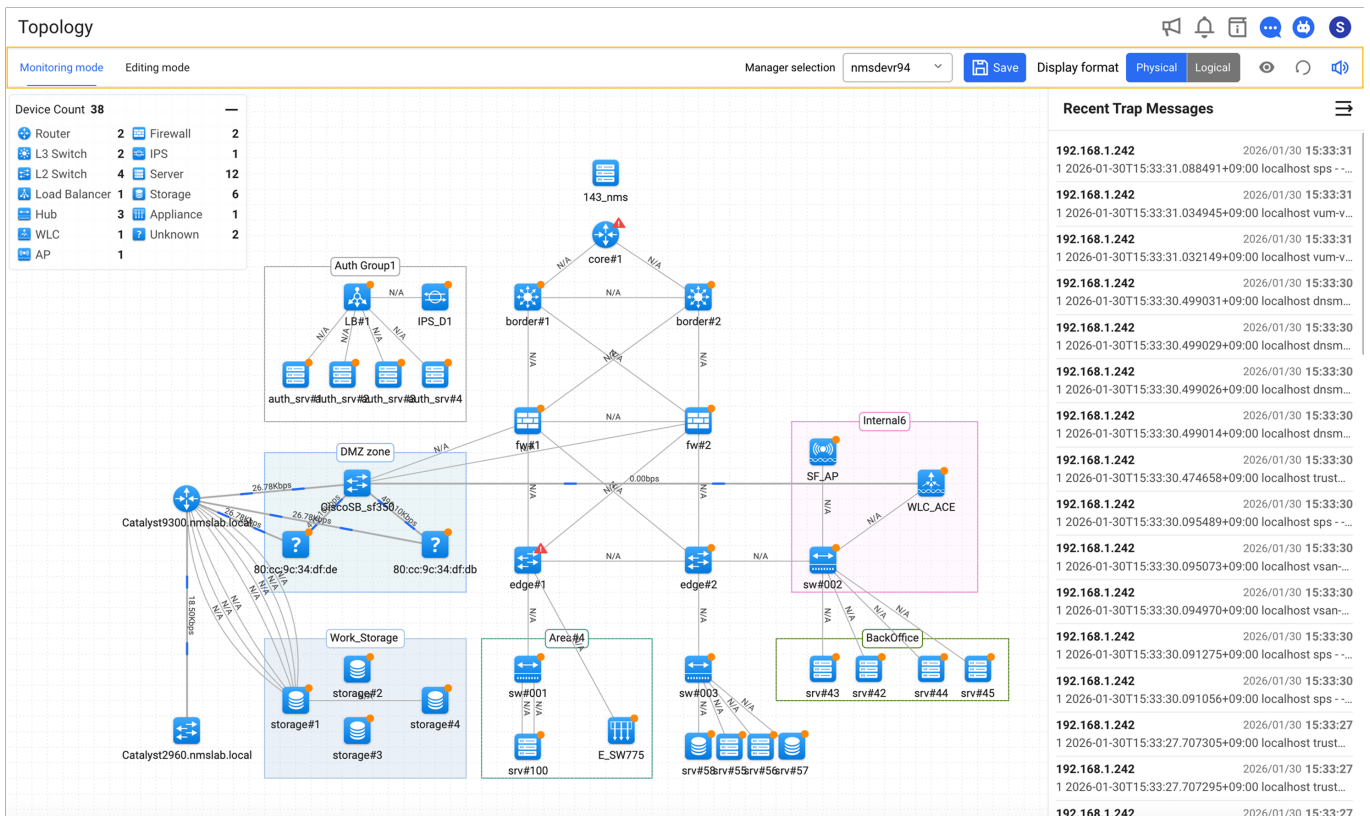
네트워크 인사이트의 토폴로지는 네트워크 장비와 링크 구조를 시각적으로 보여줍니다.

화면에서 단순히 구조만 보는 것이 아니라 링크 다운 등 실시간으로 발생하는 이벤트가 즉시 반영합니다. 따라서 관리자가 네트워크 상태를 빠르게 파악할 수 있습니다. 토폴로지는 두 가지 모드를 제공합니다.

- **모니터링 모드:** 보기 모드로 네트워크 전체 구조를 확인하고 실시간 이벤트를 모니터링합니다.
- **편집 모드:** 영역을 생성하거나 노드 속성을 수정해 화면 배치를 관리합니다.

기본 화면 및 설정

토폴로지 화면 상단에 모드 전환, 매니저 선택, 표시 형식 변경 등 주요 제어 기능을 제공합니다.



메뉴	설명
모드 선택	모니터링 모드 또는 편집 모드 탭 선택 - 모니터링 모드: 보기 모드로 네트워크 전체 구조를 확인하고 실시간 이벤트 모니터링 - 편집 모드: 영역을 생성하거나 노드의 추가, 삭제, 편집, 링크 연결의 기능 제공
매니저 선택	연결된 NMS 매니저 선택
 저장	사용자가 조정한 장비 및 영역 위치 저장
표시 형식	물리적 또는 논리적 토폴로지로 전환 - 물리적: 실제 장치간 연결된 모든 포트를 확인 - 논리적: 장치간 논리적으로 연결 구조 위주로 확인
	노드 IP 표시 여부 선택
	모든 화면 설정을 기본값으로 되돌림
	ON / OFF로 토폴로지에 이상이 있을 때 알림을 알리는 사운드 재생 여부 설정

Topology Map 아이콘

아이콘	노드 타입	설명
	Router	네트워크 트래픽을 다른 네트워크로 라우팅하는 장치
	L3 Switch	Layer 3 스위치, 라우팅 기능을 가진 스위치
	L2 Switch	Layer 2 스위치, VLAN 등 데이터 링크 계층 장치
	Firewall	네트워크 트래픽을 필터링하는 보안 장비
	Load Balancer	트래픽을 여러 서버에 분산하는 부하 분산 장치

아이콘	노드 타입	설명
	Hub	단순 네트워크 분배 장치 (비지능형)
	IPS	침입 방지 시스템 (Intrusion Prevention System)
	WAF	웹 애플리케이션 방화벽 (Web Application Firewall)
	WLC	무선 LAN 컨트롤러 (Wireless LAN Controller)
	Access Point	무선 액세스 포인트
	Server	서비스나 데이터를 제공하는 서버
	Storage	데이터 저장 장치 (NAS, SAN 등)
	IP Phone	VoIP 기반 음성 통화 장치
	Appliance	특정 목적의 네트워크 장비 (예: Proxy, UTM 등)
	Unknown	분류되지 않은 또는 미확인 장비

공통 기능

- 시점 이동: 화면의 빈 부분을 드래그해 이동함
- 줌인/줌아웃: 마우스 휠로 화면을 확대하거나 축소함

모니터링 모드

모니터링 모드에서 네트워크 구조를 실시간으로 확인하고, 이벤트 변화를 즉시 파악할 수 있습니다.

1. 네트워크 인사이트 > 토폴로지로 이동합니다.
2. 모니터링 모드 탭을 클릭해, 메인 토폴로지 뷰와 Recent Trap Messages를 확인합니다.

메인 토폴로지 뷰

- 네트워크 장비는 아이콘으로 표시되며, 라우터·스위치·방화벽 등 장비 종류에 따라 아이콘 모양이 다릅니다.
- 장비 간 연결은 선으로 표현되며, 상태에 따라 스타일이 달라집니다.
 - 정상(회색 실선)
 - Throughput이 있을 경우, SNMP 설정을 통해 애니메이션으로 데이터 흐름을 표시합니다. SNMP 설정이 필요합니다.
 - 링크 다운(붉은색 실선)
- 장비가 꺼지거나 네트워크에서 연결이 끊기면 경고 아이콘 (▲)이 표시되어 상태를 즉시 확인할 수 있습니다.
- 장비를 영역별로 그룹화하는 커스텀 기능을 제공합니다.

Recent Trap Messages

화면 오른쪽의 패널에 실시간으로 수집된 Trap 메시지가 순차적으로 표시됩니다. 장비와 링크의 이벤트를 텍스트 로그 형태로 확인할 수 있습니다.

- 예: 특정 링크 다운, 장비 활성화 또는 비활성화

편집 모드

편집 모드 탭에서 노드 추가/편집, 영역 추가/편집, 링크 추가/편집할 수 있습니다.

1. 네트워크 인사이트 > 토폴로지로 이동합니다.
2. 편집 모드 탭을 클릭해, 화면 오른쪽에서 원하는 모드를 선택해 편집합니다.
 -  Topology Edit: 수정 모드
 -  Add Device: 장비 추가 모드
 -  Add Area: 영역 추가 모드
 -  Add Link: 링크 추가 모드

수정 모드

수정 모드에서는 배치된 요소를 편집할 수 있습니다.

- 노드와 영역을 드래그하여 위치를 변경할 수 있습니다.
- 요소를 클릭하면 속성을 편집할 수 있습니다.

영역 편집

생성된 영역의 속성을 편집할 수 있습니다.

- 영역의 **배경 색상**과 **테두리 색상**을 변경할 수 있어 시각적으로 구분하기 쉽습니다.
- 영역 이름은  아이콘을 클릭해 입력하거나 수정합니다.
- 필요 없는 영역은  **삭제** 버튼을 클릭해 제거합니다.

노드 편집

네트워크 장비(노드)를 선택하면 이름과 디바이스 타입을 수정할 수 있습니다.

- 네트워크 노드 정보는  아이콘을 클릭해 입력하거나 수정합니다.
- 노드를 삭제하고 싶다면  **삭제** 버튼을 클릭해 제거합니다.
- 제공되는 디바이스 타입: router, switch, hub, host, ap, phone, firewall, unknown

장비 추가 모드

장비 추가 모드에서 토폴로지에 노드를 추가할 수 있습니다. 장비 타입을 선택 후 토폴로지에 빈 공간을 클릭하여 노드 추가할 수 있습니다.

영역 추가 모드

영역 추가 모드에서 토폴로지에 새로운 영역을 추가할 수 있습니다. 토폴로지의 빈 공간을 드래그해 새로운 영역을 추가합니다.

링크 추가 모드

링크 추가 모드에서 노드와 노드를 연결할 수 있습니다. 노드를 하나 클릭한 후, 다른 노드를 클릭하면 링크의 연결할 수 있습니다.

편집 이력

상단 옵션 바 오른쪽 **편집 이력**에서 편집 도구로 수행한 작업을 되돌리거나 다시 적용할 수 있습니다.

Item	Description
실행 취소	직전 편집 작업 취소. 단축키 Ctrl+Z
다시 실행	취소한 작업 다시 적용. 단축키 Ctrl+Shift+Z 또는 Ctrl+Y

되돌릴 작업이 없으면 각 버튼은 비활성 상태로 표시됩니다.

- 되돌릴 수 있는 작업: 영역 추가·편집·삭제, 노드와 영역의 드래그 이동 및 크기 변경, 페이지 가이드 추가·이동·삭제
- 되돌릴 수 없는 작업: 노드와 링크의 추가·수정·삭제(저장 시 서버에 바로 반영됨), 화면 이동과 확대·축소

❗ 편집 이력은 최대 50단계까지 보관하며, 드래그 중에는 동작하지 않습니다. 짧은 시간 안에 연속으로 발생한 같은 대상의 변경은 한 단계로 묶입니다.

자동 순회 재생 바

토폴로지를 여러 구획으로 나눈 경우, 자동 순회 재생 바가 표시됩니다. 재생 바에서 구획 사이 이동과 자동 순회를 함께 제어할 수 있습니다.

Item	Description
페이지 표시	구획 개수와 현재 위치 표시. 항목 선택 시 해당 구획으로 즉시 이동
재생·정지	자동 순회 시작·정지. 아이콘 오른쪽 위에 현재 간격(초)이 표시됨

Item	Description
간격 선택	자동 순회 간격 선택. 프리셋은 3 · 5 · 10 · 30 초이며, 직접 입력은 1 초부터 120 초까지
진행 막대	다음 구획으로 이동하기까지 남은 시간 표시

재생 바는 구획이 2개 이상일 때만 표시됩니다.

디바이스 Overview

디바이스 Overview는 **공통 옵션**과 **위젯**으로 구성된 프로젝트 내 네트워크 디바이스의 상태와 성능 지표를 한눈에 확인할 수 있는 대시보드입니다. 관리자는 인터페이스 상태, 트래픽 처리 현황, HealthCheck, Syslog, Trap 이벤트, 실시간 로그 등 주요 운영 데이터를 위젯 형태로 확인할 수 있습니다.

❗ 디바이스 대시보드는 실시간 모니터링 전용 화면으로 과거 특정 시점을 선택하여 조회하는 기능을 제공하지 않습니다.

공통 기능

디바이스 Overview 화면 전체에 공통 적용되는 기능으로 데이터 조회 범위, 매니저 선택, 위젯 배치 저장 등을 설정할 수 있습니다.

- **프리셋 선택**: 저장된 위젯 배치를 불러와 동일한 레이아웃으로 사용
- **프리셋 저장**: 현재 화면 구성을 저장하여 이후 재사용 가능
- **위젯 관리**: 위젯 추가, 삭제, 배치 변경, 크기 조절 가능
 - **위젯 삭제**: 삭제할 위젯을 우클릭하면 나타나는 **삭제** 버튼으로 삭제합니다.
 - **위젯 추가**: 위젯이 없는 공간에 마우스 우클릭 후 원하는 위젯을 선택해 추가합니다.

위젯

대시보드에 표시되는 다양한 위젯을 통해 네트워크 상태를 직관적으로 확인할 수 있습니다.

디바이스 상태

사용 중인 인터페이스 수(**Connected**) / 전체 인터페이스 수(**Total Interfaces**)로 표시되어 디바이스의 활성화된 인터페이스 수를 확인할 수 있습니다. 디바이스에 마우스 오버 시 상태 정보가 표시되고, 디바이스를 클릭 시 인터페이스 정보가 있으면 인터페이스 상태, 없으면 **사용량 현황**으로 이동합니다.

- 예: 8 / 22 → 전체 22개 중 8개 활성화

❗ 인터페이스 정보는 SNMP의 ifTable(1.3.6.1.2.1.2.2) 또는 ifXTable(1.3.6.1.2.1.31.1.1) 데이터를 수집해야 합니다. 장비별로 지원하지 않거나 다를 수 있습니다.

HealthCheck

HealthCheck 위젯은 네트워크 지연 변동성(jitter)과 왕복 시간(Max RTT)을 그래프로 제공합니다. 상태가 비정상일 경우 해당 IP 주소를 **빨간색**으로 표시합니다. 모니터링 결과는 최근 10분 단위로 확인할 수 있습니다.

1. 디바이스 인벤토리로 이동한 후, 설정할 디바이스의  아이콘을 클릭하세요.
2. 디바이스 설정 화면의 **Health Check** 탭에서 설정할 수 있습니다.

금일 Syslog

금일 발생한 Syslog 이벤트는 심각도별 원형 차트로 표시되며, Emergency부터 Debug까지 레벨별로 분류됩니다. 이를 통해 로그 발생 빈도와 심각도 분포를 직관적으로 확인할 수 있습니다.

Trap 발생량 TOP 10

최근 24시간 동안 Trap 메시지가 가장 많이 발생한 디바이스를 표시하며, 이벤트 발생 빈도 기준으로 내림차순 정렬합니다. 이를 통해 이벤트가 집중되는 장비를 빠르게 파악할 수 있습니다.

최대 Throughput 인터페이스

최근 24시간 기준으로 최대 Throughput을 기록한 인터페이스를 표시하며, 트래픽이 가장 높은 순서대로 내림차순 정렬됩니다.

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

최대 PPS 인터페이스

최근 24시간 기준 최대 Packets Per Second(PPS) 기록 인터페이스를 표시합니다.

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

실시간 로그 이벤트

프로젝트 내에서 발생하는 로그를 실시간 테이블로 확인할 수 있으며, 시간, 호스트, 로그 내용이 함께 표시됩니다. 새로운 로그는 Live tail 형식으로 실시간으로 표시합니다. 로그를 실시간으로 분석하여 시스템 장애 및 이상 징후를 빠르게 감지할 수 있습니다.

그룹 내비게이터

그룹 내비게이터에서 네트워크 장비와 인터페이스를 계층 구조로 탐색하며 성능 지표를 실시간으로 확인할 수 있습니다.  **Site** →  **Building** →  **Floor** →  **Device** →  **Interface** 순으로 드릴다운하며, 각 단계에서 해당 범위의 트래픽, 상태, 오류 정보를 시각화합니다.

그룹 내비게이터에서 다음 작업을 통해 네트워크 상태를 실시간으로 모니터링할 수 있습니다.

- 원하는 위치까지 빠르게 탐색
- 각 계층의 디바이스 및 인터페이스 상태 요약 확인하기
- 디바이스 또는 인터페이스의 트래픽·오류 지표 상세 분석하기

기본 화면 및 설정

그룹 내비게이터 화면 상단 옵션바에서 조회 조건을 설정하고, 왼쪽 패널에서 모니터링 대상을 선택합니다.

시간 선택

상단 옵션 바 **시간 선택**에서 조회 시간 범위를 설정할 수 있습니다.

 **LIVE** 모드는 5초 간격으로 데이터를 갱신하며, 최대 31일까지 조회할 수 있습니다. 기본 라이브 범위는 1시간입니다.

매니저 선택

상단 옵션 바 **매니저 선택**에서 데이터를 수집하는 NMS 매니저를 선택해 성능 지표를 확인할 수 있습니다.

Group Selection

Group Selection 패널은 트리 구조로  **Site** →  **Building** →  **Floor** →  **Device** →  **Interface** 순으로 계층을 탐색할 수 있습니다.

항목	설명
— 전체 접기	트리 전체 접기
+ 전체 펼치기	트리 전체 펼치기
☰ / ☱	패널 닫기/열기

경로 표시 (Breadcrumb)

Breadcrumb 내비게이션이 표시됩니다. 선택한 노드의 경로가 상단에 표시됩니다. 각 경로를 클릭하여 상위 레벨로 이동할 수 있습니다.

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

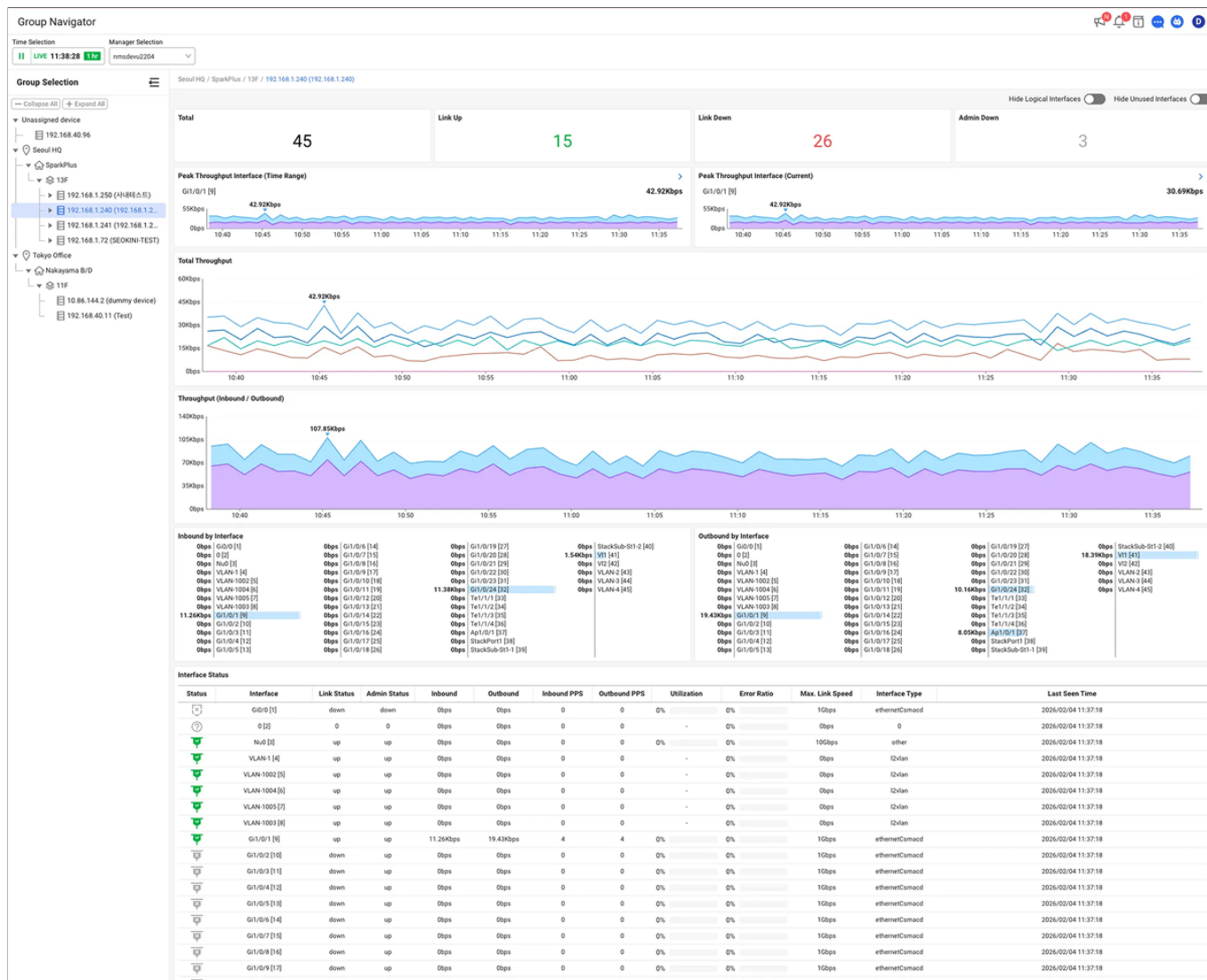
❗ 현재 선택 위치는 URL 파라미터(nodeKey)로 저장되어 북마크하거나 공유할 수 있습니다.

그룹 레벨 요약

항목	설명
Devices	선택 범위 내 전체 디바이스 수
Interfaces	선택 범위 내 전체 인터페이스 수
그룹 카드	하위 그룹별 디바이스/인터페이스 개수로 클릭 시 해당 그룹으로 드릴다운함

디바이스 상태 및 트래픽 정보 확인

특정 디바이스를 선택 시, 해당 디바이스에 속한 인터페이스들의 상태와 트래픽 정보를 확인할 수 있습니다.



필터 옵션

화면 오른쪽 상단에 **Hide Logical Interfaces**, **Hide Unused Interfaces** 옵션을 켜고 끌 수 있습니다.

항목	설명
Hide Logical Interfaces	VLAN, Loopback 등 논리 인터페이스를 목록에서 숨김, 물리 포트(ethernetCsmacd, fastEther 등)만 표시됨

항목	설명
Hide Unused Interfaces	조회 기간 내 트래픽이 없는 인터페이스를 목록에서 숨김

❗ 필터 설정은 브라우저에 저장되어 다음 접속 시 유지됩니다.

인터페이스 요약 패널

항목	설명
Total	전체 인터페이스 수
Link Up	링크가 연결된 인터페이스 수
Link Down	링크가 끊어진 인터페이스 수
Admin Down	관리자가 비활성화한 인터페이스 수

❗ 각 상태 카운트를 클릭하면 상세 목록 모달이 표시됩니다. 모달에서 해당 상태의 인터페이스 목록을 확인할 수 있습니다.

차트

차트명	설명
Peak Throughput Interface (Time Range)	조회 기간 내 최대 트래픽을 기록한 인터페이스와 추이로 클릭 시 해당 인터페이스로 이동함
Peak Throughput Interface (Current)	현재 시점 기준 최대 트래픽 인터페이스와 추이
Total Throughput	디바이스 전체 트래픽 추이(Line Chart)

차트명	설명
Throughput (Inbound / Outbound)	인터페이스별 인바운드/아웃바운드 트래픽 추이로 인터페이스별로 색상이 구분됨(Stacked Line Chart)
Inbound by Interface	인터페이스별 인바운드 트래픽 비교(Horizontal Bar Chart)
Outbound by Interface	인터페이스별 아웃바운드 트래픽 비교(Horizontal Bar Chart)

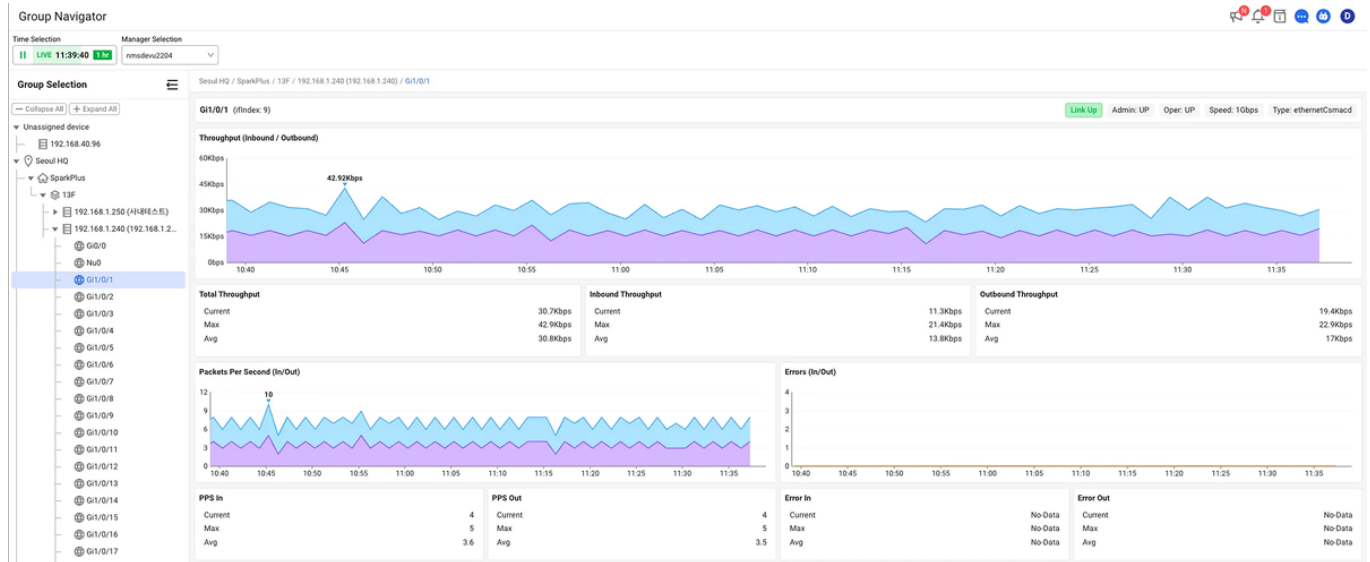
Interface Status

컬럼	설명
Status	인터페이스 상태 아이콘(🟢 Connected, 🛑 Link Down, 🛑 Admin Down, 🤔 Unavailable)
Interface	인터페이스 이름 및 ifIndex
Link Status	링크 연결 상태(up/down)
Admin Status	관리 상태(up/down)
Inbound	인바운드 트래픽(Kbps)
Outbound	아웃바운드 트래픽(Kbps)
Inbound PPS	초당 인바운드 패킷 수
Outbound PPS	초당 아웃바운드 패킷 수
Utilization	대역폭 사용률(%)
Error Ratio	오류 비율(%)
Max Link Speed	인터페이스 최대 속도
Interface Type	인터페이스 타입 (예: ethernetCsmacd)

컬럼	설명
Last Seen Time	마지막 데이터 수신 시간

인터페이스 성능 지표 분석

특정 인터페이스를 선택 시, 해당 인터페이스의 상세 성능 지표를 확인할 수 있습니다.



인터페이스 정보

항목	설명
ifIndex	인터페이스 식별 번호
Link Status	링크 연결 상태 배지(Link Up / Link Down / Admin Down)
Admin	관리 상태(UP/DOWN)
Oper	운영 상태(UP/DOWN)

항목	설명
Speed	인터페이스 속도(예: 1Gbps)
Type	인터페이스 타입(예: ethernetCsmacd)

차트

차트명	설명
Throughput (Inbound / Outbound)	인바운드/아웃바운드 트래픽 시계열 그래프(Stacked)
Packets Per Second (In/Out)	초당 패킷 수 시계열 그래프
Errors (In/Out)	인바운드/아웃바운드 오류 발생 추이

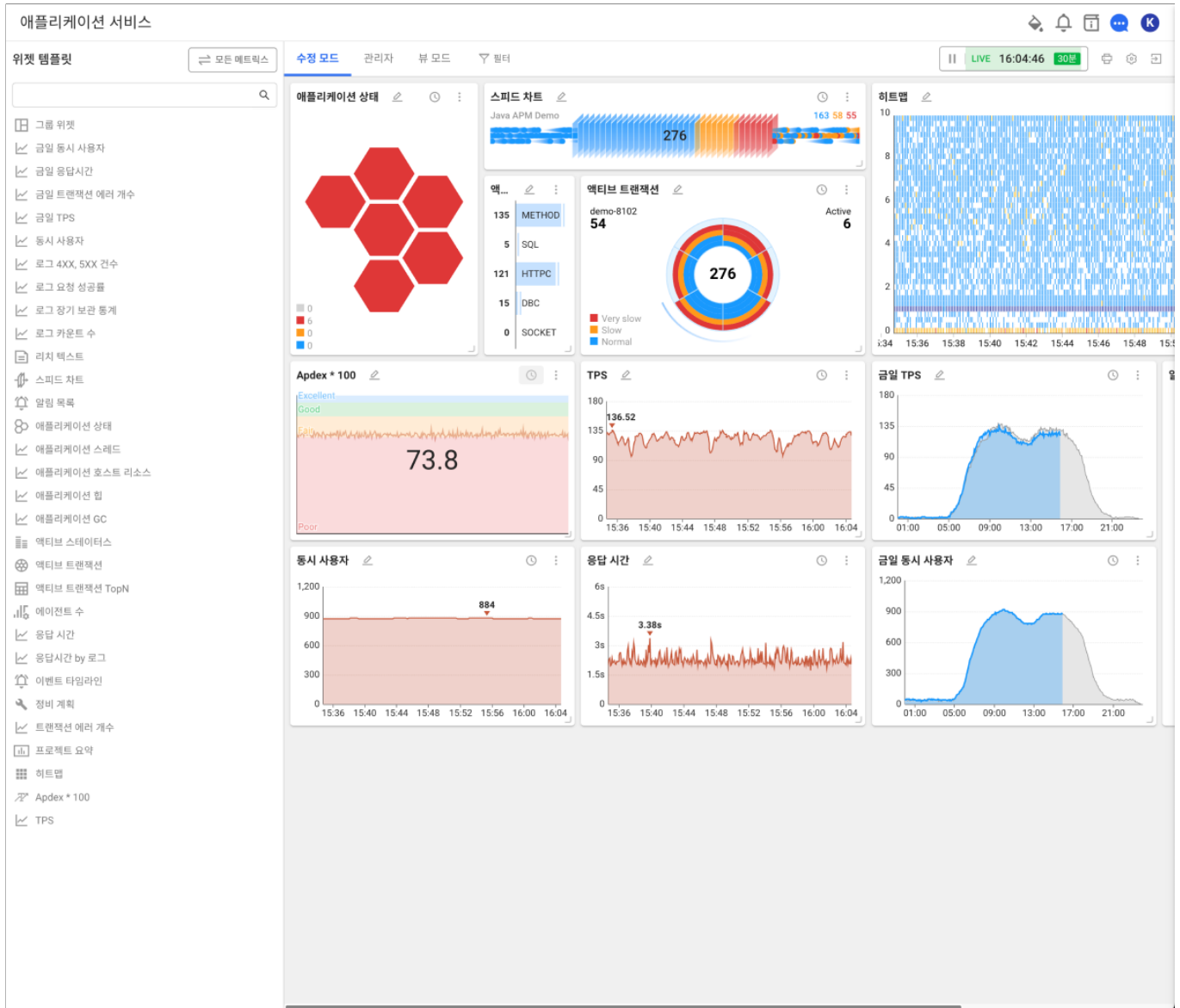
통계 카드

구분	항목	설명
Total Throughput	Current / Max / Avg	전체 트래픽의 현재값, 최대값, 평균값(Kbps)
Inbound Throughput	Current / Max / Avg	인바운드 트래픽 통계
Outbound Throughput	Current / Max / Avg	아웃바운드 트래픽 통계
PPS In	Current / Max / Avg	인바운드 초당 패킷 수 통계
PPS Out	Current / Max / Avg	아웃바운드 초당 패킷 수 통계
Error In	Current / Max / Avg	인바운드 오류 통계
Error Out	Current / Max / Avg	아웃바운드 오류 통계

Flex 보드

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

사전 구성된 템플릿으로 초기 설정을 빠르게 마치고 원하는 형태의 대시보드를 만들 수 있습니다. 데이터 위젯을 추가하거나 속성을 수정해 필요한 형식으로 표시할 수 있으며, 필터링 기능으로 모니터링 대상을 간추릴 수도 있습니다. 시간 범위를 지정하면 특정 시점의 데이터를 확인할 수 있고, 보조 차트를 활용해 다양한 방식으로 분석할 수 있습니다. 대시보드는 즐겨찾기에 등록해 쉽게 접근할 수 있으며, 개인화한 대시보드는 다른 계정으로 복사해 재사용할 수 있습니다.



홈 화면 > 통합 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 보드의 수정 권한이 있는 사용자는 다음 기능을 이용할 수 있습니다.

- 대시보드를 JSON 파일로 내보내기/가져오기
- 대시보드 내의 데이터 요청 및 응답 내용 확인
- 위젯 설정 옵션을 JSON 형식으로 조회 및 수정

❗ 프로젝트 내 Flex 보드 메뉴에서는 대시보드 수정 권한이 있는 사용자만 수정 모드 및 관리자 모드, 필터 기능에 접근할 수 있습니다.

- 접근 가능 멤버 권한
 - 프로젝트 수정 권한
 - 프로젝트 플렉스보드 편집 권한
 - Site Admin 권한
- 뷰 모드 및 필터 기능에 대한 자세한 내용은 [다음 문서](#)를 참고하세요.
- 멤버 권한에 대한 자세한 내용은 [다음 문서](#)를 참고하세요.

Flex 보드 사용하기

- ✔ 대시보드를 매트릭스 위젯을 포함해 다양한 위젯 템플릿을 활용해 구성할 수 있습니다.
각 템플릿의 특징과 사용법은 [위젯 템플릿](#) 문서에서 자세히 확인할 수 있습니다.

사전 템플릿 적용하기

사전 구성 템플릿으로 초기 설정을 빠르게 진행하고 필요에 따라 수정해 활용하세요.

1. **Flex 보드** 메뉴를 선택하세요.
2. 왼쪽 **템플릿** 목록에서 원하는 템플릿을 선택하세요.
3. **Flex 보드 관리** 창이 나타나면 **이름 변경**에 원하는 이름을 입력하세요.
 - 레이아웃에서 위젯을 선택 후, 드래그하여 원하는 위치로 이동할 수 있습니다.
4. **저장** 버튼을 클릭세요. 선택한 템플릿 기준의 Flex 보드를 생성합니다.
 - **Flex 보드**의 보드 목록에서 생성한 보드를 확인할 수 있습니다.

Flex 보드 만들기

Flex 보드를 생성하고 위젯을 배치해 자신만의 대시보드를 만들 수 있습니다.

1. **Flex 보드**에서 오른쪽 위의 **대시보드 생성하기** 버튼을 클릭하세요.
2. **대시보드 생성하기** 창이 나타나면 입력 상자에 대시보드 **이름**을 입력하세요.
3. 위젯 배치 방식을 선택한 후, **대시보드 생성하기** 버튼을 클릭하세요.
 - 고정 레이아웃 플렉스보드: 픽셀 기반으로 위젯 자유 배치
 - 반응형 플렉스보드: 브라우저 크기 기준 그리드 반응형 레이아웃 (그리드 설정한 뒤 **대시보드 생성하기** 버튼 클릭)
4. **위젯 템플릿** 선택 화면에서 대시보드에 배치할 위젯을 선택하세요.

- 매트릭스 위젯을 추가하려면 **위젯 템플릿**의 오른쪽 **모든 매트릭스** 버튼을 클릭하세요.

- ❗ • **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 생성합니다. 매트릭스 위젯에 대한 자세한 설명은 [다음 문서](#)를 참고하세요.

5. 배치한 위젯의 위치를 이동하거나 크기를 조절하세요.

- 위젯의 위쪽에 커서를 올려 십자 커서가 보이면, 위젯을 클릭한 채 드래그하여 위치를 이동합니다.
- 위젯 오른쪽 아래에 커서를 올려 화살표 커서가 보이면, 위젯을 클릭한 채 드래그하여 크기를 조절합니다.

6. 추가할 위젯 배치를 완료하면 **뷰 모드**를 선택해 레이아웃을 확인하세요. 레이아웃을 다시 수정하려면 **수정 모드**를 선택해 위젯의 배치를 변경하세요.

7. 모든 과정을 완료했다면 오른쪽 위 (**목록으로 가기**) 아이콘을 클릭하세요.

- **Flex 보드의 대시보드 목록**에서 생성한 보드를 확인할 수 있습니다. 생성한 보드를 선택해 새로 생성한 Flex 보드를 확인할 수 있습니다.

❗ 고객님의 의견을 반영해 대시보드 템플릿 또는 위젯을 추가하려고 합니다. 필요한 대시보드 템플릿 또는 위젯이 있다면 support@whatap.io로 문의해 주세요.

Flex 보드 편집하기

❗ Flex 보드 편집 권한

- **홈 화면 > 통합 Flex 보드**: 개인 계정 대시보드로 권한 영향은 없으나 읽기 전용으로 공유된 대시보드는 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 참고하세요.

1. Flex 보드의 대시보드 목록에서  수정 아이콘을 클릭하세요. 화면 오른쪽에 Flex 보드 관리 창이 나타납니다.
2. Flex 보드 관리 창에서 이름, 프로젝트, 레이아웃, 위젯.json, 옵션.json을 설정합니다.
 - **이름 변경:** 대시보드의 이름을 수정합니다.
 - **프로젝트:** 대시보드 위젯에 데이터를 가져올 프로젝트를 선택합니다.

 프로젝트 옵션은 홈 화면 > 통합 Flex 보드 메뉴에서만 설정할 수 있습니다.

통합 Flex 보드 메뉴로 진입한 경우, 위젯마다 데이터를 가져올 프로젝트를 선택할 수 있습니다.

1. 위젯 오른쪽 위 + 버튼을 클릭하고 원하는 프로젝트를 검색해 하나 또는 다중 선택하세요.
2. 프로젝트를 선택한 후 적용 버튼을 클릭하세요.

- **레이아웃**
 - 위젯을 드래그하여 위치를 이동합니다.
 - 위젯 오른쪽 아래를 마우스로 클릭한 상태로 드래그해 위젯의 크기를 조절합니다.
 - 위젯을 삭제하려면 위젯 오른쪽 위에  아이콘을 클릭하세요.
- **위젯.json:** 대시보드의 위젯 설정을 JSON 형식으로 불러올 수 있습니다.  아이콘을 클릭하면 JSON 내용을 복사합니다.
- **옵션.json:** 대시보드에 설정된 옵션을 JSON 형식으로 불러올 수 있습니다.  아이콘을 클릭하면 JSON 내용을 복사합니다.

Flex 보드 삭제하기

1. Flex 보드 > 대시보드 목록에서 삭제할 항목의  아이콘을 클릭하세요.
2. 확인 메시지에서 삭제 버튼을 클릭하세요.

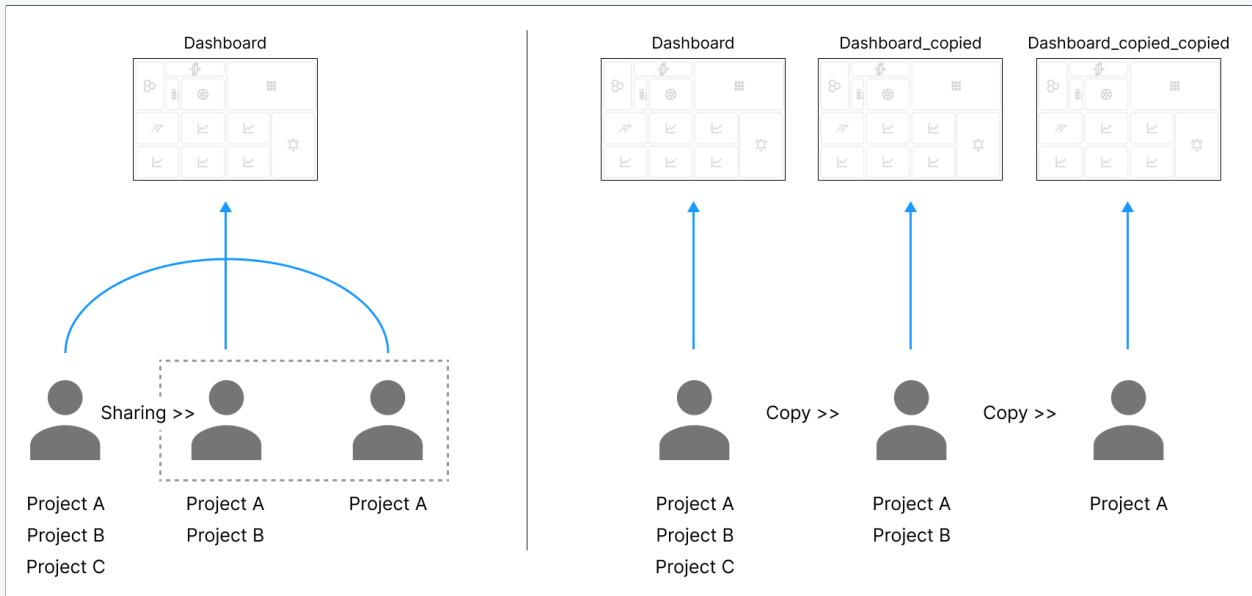
 대시보드 삭제는 소유자와 공유받은 사용자에게 따라 다르게 적용됩니다.

- 대시보드 소유자가 대시보드를 삭제하면, 공유된 모든 사용자 계정에서도 해당 대시보드를 삭제됩니다.
- 대시보드를 공유받은 사용자가 대시보드를 삭제하면, 해당 사용자의 대시보드 목록에서만 삭제됩니다. 원본 대시보드는 유지됩니다.

Flex 보드 공유하기

- ❗ Flex 보드 공유 기능은 **홈 화면 > 통합 Flex 보드** 메뉴에서만 사용할 수 있습니다.
프로젝트의 **Flex 보드** 메뉴에서는 제공되지 않습니다.

❗ 공유와 복사의 차이



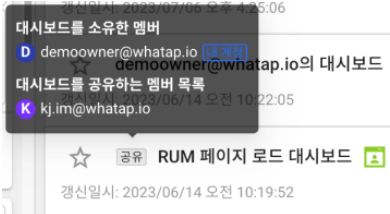
- 공유: 공유한 멤버는 모두 같은 대시보드를 볼 수 있습니다.
- 복사: 대시보드를 다른 멤버 또는 나에게 복사하면, 복사된 별도의 대시보드를 볼 수 있습니다.
- 읽기 전용: 공유/복사받은 대시보드는 수정할 수 없습니다. 단, 수정 모드로 공유/복사된 경우는 수정할 수 있습니다.
- 읽기 전용: 공유받은 멤버도 해당 대시보드를 읽기 전용으로 재공유하거나 복사할 수 있습니다.
- 대시보드에 포함된 프로젝트 중 최소 1개 프로젝트에 초대된 멤버에게만 공유할 수 있습니다. 공유 또는 복사 받을 멤버의 프로젝트 소속 여부를 확인하세요.



통합 Flex 보드에서 생성한 Flex 보드를 다른 멤버와 공유할 수 있습니다. 소유자가 공유된 대시보드를 수정하면, 공유받은 모든

멤버에게 동일하게 반영됩니다.

1. **통합 Flex 보드의 대시보드 목록**에서 공유할 대시보드의  아이콘을 클릭하세요.
2. **대시보드 공유하기** 창이 나타나면 입력창에 공유할 멤버를 한 명 또는 여러명을 선택하거나 계정을 직접 입력하세요.
 - 읽기 전용을 선택하면 공유받은 멤버는 대시보드를 수정할 수 없습니다.
 - 공유 대상은 대시보드에 포함된 프로젝트 중 최소 1개 프로젝트에 소속되어 있어야 합니다.
3. **공유** 버튼을 클릭하세요.
 - 공유된 항목은 **공유** 태그가 표시됩니다. **공유** 태그에 마우스를 올리면 공유한 멤버 정보를 확인할 수 있습니다.
 - 읽기 전용으로 공유한 항목은 **읽기 전용** 태그가 표시됩니다.

대시보드를 공유받은 경우	대시보드를 공유한 경우(대시보드 소유자)
	

✔ 대시보드 공유 조건

- 대시보드 공유 기능은 **홈 화면 > 통합 Flex 보드**에서만 제공합니다.
- 누구나 자신의 대시보드를 공유할 수 있으며, 공유받은 대시보드를 다시 공유하거나 복사할 수 있습니다.
- **읽기 전용**으로 공유받은 대시보드는 수정할 수 없지만, **수정 모드**로 공유받은 대시보드는 수정할 수 있습니다.
- **소유자**가 대시보드를 삭제하면, 공유받은 모든 계정에서 해당 대시보드가 삭제됩니다.
- **공유받은 사용자**가 삭제하면, 해당 사용자의 **대시보드 목록**에서만 삭제되며 원본은 유지됩니다.
- 공유받은 대시보드의 프로젝트 중 **조회 분석** 권한이 없는 프로젝트는 데이터를 조회할 수 없습니다.

Flex 보드 복사하기

사용자가 Flex 보드를 복사해 다른 멤버에게 전달할 수 있습니다.

1. 통합 Flex 보드의 대시보드 목록에서  아이콘을 클릭하세요.
2. 복사 옵션을 선택하세요.
 - **나에게 복사:** 자신의 계정으로 복사합니다.
 - a. `_copied` 접미어가 붙은 항목이 **대시보드 목록**에 추가됩니다.
 - **다른 사람에게 복사:** 다른 멤버 계정으로 복사합니다.
 - a. **+** 계정을 클릭하세요.
 - b. 복사할 멤버의 이메일을 선택하고 **대시보드 복사하기** 버튼을 클릭하세요.
 - c. 해당 멤버의 **대시보드 목록**에 `_copied` 접미어가 붙은 항목이 추가됩니다.

JSON 파일로 공유하기

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

내보내기

1. 통합 Flex 보드 또는 프로젝트의 Flex 보드 메뉴로 이동하세요.
2. 대시보드 목록에서  버튼을 클릭하세요.
3. 내보내기 옵션을 선택하세요.
 - **프로젝트 정보 포함:** 대시보드에 설정된 프로젝트 정보를 JSON 파일에 포함해 공유
 - **프로젝트 정보 미포함:** 대시보드에 설정된 프로젝트 정보를 JSON 파일에 포함하지 않고 공유
4. JSON 파일을 다운로드하고 공유할 멤버에게 전달하세요.

가져오기

1. 통합 Flex 보드 또는 프로젝트의 Flex 보드 메뉴로 이동하세요.

2. 화면 오른쪽 위  가져오기 버튼을 클릭하세요.
3. 다운로드한 JSON 파일을 선택하세요.

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

Flex 보드 화면 모드

Flex 보드의 화면 모드에 따라 제공하는 기능을 설명합니다.

❗ 접근 가능한 멤버 권한

프로젝트 내 **Flex 보드** 메뉴에서 수정 권한이 있는 사용자만 수정 모드, 관리자, 필터 기능에 접근할 수 있습니다. 멤버 권한에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

- 프로젝트 수정 권한
- 프로젝트 플렉스보드 편집 권한
- Site Admin 권한

모드 종류

Flex 보드는 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.

공통 기능

- 데이터 필터링

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

데이터 필터링

데이터 필터링을 통해 모니터링 대상을 간추려 효율적인 Flex 보드를 구성할 수 있습니다.

1. 화면 위  **필터** 탭을 클릭하세요.
2. 화면 오른쪽에 나타나는 **필터** 창에서 필터링 대상을 선택하세요. 필터링 대상을 모두 선택하려면 **전체 선택**을 선택하세요.
 - **에이전트** 옵션: 에이전트 종류 또는 애플리케이션 목록 선택, **검색** 기능 제공
 - **메트릭스** 옵션: 프로젝트 또는 에이전트 유형 선택, + **And** 조건 추가하거나 **포함**, **제외**로 문자열 기반 자동 선택 가능
3. 필터링 대상을 선택했다면 **적용** 버튼을 클릭하세요.
4. 자주 사용하는 조건은 **필터 저장** 버튼으로 저장하세요.
 - a. 필터 이름을 입력하고 **저장**을 선택하세요. **저장된 필터**는 **필터** 창 하단에 나타납니다.

필터링 조건

필터링 조건은 에이전트 타입과 메트릭스 타입으로 구분합니다.

에이전트는 기본 모니터링 대상만 선택 옵션으로 제공하며, 메트릭스는 프로젝트에서 수집한 모든 메트릭스 데이터의 태그를 선택 옵션으로 제공합니다. 메트릭스 타입은 에이전트가 아닌 형태로 데이터를 수집한 후 필터링을 적용할 때 유용합니다. 메트릭스에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

타입	에이전트	메트릭스
선택 옵션	와탭 프로젝트 모니터링 대상 (애플리케이션, 서버, 데이터베이스, 컨테이너, 쿠버네티스 POD와 NODE)	에이전트를 포함한 모든 메트릭스 태그
적용 범위	모든 위젯	메트릭스 데이터를 사용하는 모든 위젯

타입	에이전트	메트릭스
필터링 조건	체크박스	일치, 포함, 제외 방식

조회 시간 설정하기

Flex 보드의 화면 오른쪽 위 시간 선택자를 이용해 위젯에 데이터 조회 시간을 설정할 수 있습니다.

- : 실시간 모드 멈추고 특정 조회 시간으로 설정
- : 다시 실시간 모드로 전환

인쇄하기

Flex 보드 화면을 PDF로 저장해 인쇄할 수 있습니다.

1. Flex 보드 화면의 오른쪽 위  아이콘을 클릭해 인쇄 모드로 전환합니다.
2. 옵션을 설정합니다.
 - **필터 옵션 보기**: 화면에 필터 옵션 켜거나 끄기
 - **{mode} 방향으로 변환 / {mode} 방향으로 변환**: 화면을 가로 또는 세로로 변환
3. 완료 후 **PDF다운로드**를 선택하세요.
4. 인쇄 모드를 종료하려면 오른쪽 위  **인쇄모드 종료**를 클릭하세요.

Flex 보드 관리

Flex 보드의 레이아웃을 변경하거나 위젯의 위치 변경, 크기 조절, 이름 변경 등의 관리 기능을 제공합니다. **Flex 보드 관리** 기능은 **대시보드 > Flex 보드 메뉴의 대시보드 목록**에서  아이콘을 클릭해 진입할 수도 있습니다.

1. Flex 보드 화면의 오른쪽 위  아이콘을 클릭하면 **Flex 보드 관리** 창이 열립니다.
 - **이름 변경**: Flext 보드의 이름 변경
 - **레이아웃**: 위젯의 위치 및 크기조절 및 삭제
 - **다른 사용자의 수정을 제한**: 수정 제한 옵션
 - 수정 권한이 있는 멤버는 수정, 삭제, 편집할 수 있으며 옵션을 활성화하면 **다른 사용자의 수정을 제한: On**으로

변경됨

- **위젯.json**: Flex 보드에 포함된 위젯을 JSON 형태로 편집 및 관리
- **옵션.json**: Flex 보드의 설정을 JSON 형태로 편집 및 관리(프로젝트 정보, Flex 보드 필터, 시간 선택 등 설정값 편집)

 **위젯.json, 옵션.json** 기능은 대시보드 관리자 권한의 사용자에게만 제공됩니다.

2. 모든 설정을 완료하고 **저장** 버튼을 클릭하세요.

대시보드 즐겨찾기로 등록

사용자가 생성한 Flex 보드는 즐겨찾기에 등록해 빠르게 접근할 수 있습니다. **대시보드 > Flex 보드의 대시보드 목록**에서 즐겨찾기로 등록할 대시보드의 ☆ 버튼을 클릭하면 ★으로 변경됩니다.

위젯 관리하기

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

- ✓ 대시보드를 매트릭스 위젯을 포함해 다양한 위젯 템플릿을 활용해 구성할 수 있습니다.
각 템플릿의 특징과 사용법은 [위젯 템플릿](#) 문서에서 자세히 확인할 수 있습니다.

위젯 추가

이미 만들어진 Flex 보드에 위젯을 추가할 수 있습니다.

1. Flex 보드 메뉴의 **대시보드 목록**에서 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 **통합 Flex 보드**로 진입한 경우 위젯을 추가했다면 **프로젝트 선택** 버튼을 클릭해 수집 대상 프로젝트를 선택하세요.
 - 추가할 위젯이 있다면 같은 과정을 반복하세요.
4. 모든 과정을 완료했다면 화면 위에 **뷰 모드**를 선택해 레이아웃을 확인한 후,  (**목록으로 가기**) 버튼을 클릭하세요.

위젯 속성 변경

Flex 보드 메뉴의 **대시보드 목록**에서 위젯 속성을 변경할 보드를 선택하세요. **수정 모드**로 진입합니다.

위젯 이름 변경

1. 이름을 변경할 위젯의 이름 오른쪽에  아이콘을 클릭하세요.
2. 위젯의 **제목**, **폰트 크기**, **색상**을 설정한 후, **저장** 버튼을 클릭하세요.

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

시간 설정

1. 시간을 설정하려는 위젯의 오른쪽 위에  버튼을 클릭하세요.
2. **시간 선택** 창에서 시간을 설정하세요.
 - 대시보드 화면에 설정한 시간을 적용하려면 **대시보드 설정을 따름**을 체크하세요. 대시보드의 시간 설정은 오른쪽 상단에 위치합니다.
 - 사용자가 원하는 시간 설정을 적용하려면 **대시보드 설정을 따름**을 체크 해제하세요. < 또는 > 버튼을 이용해 원하는 시간을 설정하세요.
3. 시간 설정을 완료했다면 ✕ 버튼을 클릭하세요.

 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.

1. 위젯의 오른쪽 위에  아이콘을 클릭해, 출력 데이터 옵션을 설정하세요.
 - 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 최댓값을 **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 최댓값을 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.
2. 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 > 대시보드 목록**에서 위젯 데이터를 변경할 대시보드를 선택하세요.
2. **수정 모드**에서 변경할 위젯의 오른쪽 위에 **⋮** 아이콘을 클릭하세요.
3. **<>** 아이콘을 클릭하면, 데이터 설정 편집 창이 나타납니다.
4. 다음을 참조해 설정을 변경한 다음 **< 위젯에 적용** 버튼을 클릭해 적용하세요.
 - 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. 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: CPU값)를 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.



1. 수정 모드에서 모든 메트릭스 버튼을 클릭해 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.

위젯 복사

1. 위젯의 오른쪽 위에 ⋮ 버튼을 클릭하세요.
2. □ 버튼을 클릭하세요.
3. 복사 창이 나타나면 + 위젯 추가 버튼을 클릭하세요.
4. 목록에 위젯의 이름을 변경하세요.

5. 적용 버튼을 클릭하세요.
6. 수정 모드 화면에서 복사한 위젯을 확인할 수 있습니다.

위젯 삭제

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

인터페이스 상태

인터페이스 상태 메뉴에서 디바이스의 네트워크 인터페이스 상태를 실시간으로 모니터링할 수 있습니다. 인터페이스의 연결 상태를 시각적으로 표시하고, 각 인터페이스에 대한 상세한 정보를 제공하여 네트워크 성능을 쉽게 분석할 수 있습니다.

기본 화면 및 설정

인터페이스 상태 화면은 왼쪽 인터페이스 목록 영역, 오른쪽 상단 인터페이스 상태와 오른쪽 하단 인터페이스 상세 영역으로 구성되어 있습니다. 인터페이스 목록에서 조회를 원하는 인터페이스 선택 시 오른쪽 영역에서 인터페이스 상태 및 상세를 확인할 수 있습니다.

Interface Status

Time selector

Manager selection

LIVE 18:21:39

nmsdevu2204

Device selection

사내테스트 (192.168.1.250)

dummy device (10.86.144.2)

Test (192.168.40.11)

192.168.1.241

192.168.1.240

SEOKINI-TEST (192.168.1.72)

192.168.40.96

Interface status

Interface display format

Device

Total Port

Connected

Link Down

Admin Down

30

3

26

1

Interface information

Display logical interface

Last checked time: 2026/02/04 18:21:18

Status	Interface Name	Link Status	Admin Status	Inbound Throughput	Outbound Throughput	Inbound PPS	Outbound PPS	Utilization	Error Ratio
	Gi0/0	down	down	0bps	0bps	0	0	-	-
	Gi1/0/1	up	up	9.56Kbps	18.59Kbps	4	4	0%	-
	Gi1/0/2	down	up	0bps	0bps	0	0	-	-
	Gi1/0/3	down	up	0bps	0bps	0	0	-	-
	Gi1/0/4	down	up	0bps	0bps	0	0	-	-
	Gi1/0/5	down	up	0bps	0bps	0	0	-	-
	Gi1/0/6	down	up	0bps	0bps	0	0	-	-
	Gi1/0/7	down	up	0bps	0bps	0	0	-	-
	Gi1/0/8	down	up	0bps	0bps	0	0	-	-
	Gi1/0/9	down	up	0bps	0bps	0	0	-	-
	Gi1/0/10	down	up	0bps	0bps	0	0	-	-
	Gi1/0/11	down	up	0bps	0bps	0	0	-	-

1. 인터페이스 상태의 상단 옵션 바 시간 선택에서 조회 시간 범위를 설정하세요.

- || LIVE 모드는 최근 30분 데이터를 자동으로 갱신하고 과거 시간 조회는 지원하지 않습니다.

2. 상단 옵션 바 매니저 선택에서 데이터를 수집하는 NMS 매니저를 선택해 인터페이스 상태를 확인할 수 있습니다.

인터페이스 상태

인터페이스의 연결 상태를 확인할 수 있습니다.

- **Connected** : 인터페이스가 정상적으로 연결된 상태입니다. Link Status와 Admin Status 모두 "up"일 때 표시됩니다.
- **Link Down** : 네트워크 링크가 다운된 상태입니다. Link Status는 "down", Admin Status는 "up" 상태일 때 나타납니다.
- **Admin Down** : 관리자가 해당 인터페이스를 비활성화한 상태입니다. Link Status와 Admin Status 모두 "down"일 때 표시됩니다.
- **Unavailable** : 물리적으로 활성화되지 않은 가상 인터페이스, 루프백 인터페이스, 또는 SFP 모듈이 미삽입된 Fiber 인터페이스 등 사용할 수 없는 인터페이스 수를 나타냅니다.

인터페이스 상세

각 인터페이스의 상세 정보를 목록 형식으로 표시하며, 사용자가 인터페이스를 클릭하면 해당 디바이스의 추이 페이지로 이동하여 더 구체적인 상태를 확인할 수 있습니다.

사용량 현황

사용량 현황에서 디바이스의 상태 변화와 관련된 데이터를 실시간으로 확인할 수 있습니다. 디바이스와 인터페이스에 대한 지표를 시각적으로 제공하여 네트워크 성능 변화를 즉각적으로 파악할 수 있습니다.

기본 화면 및 설정

- 1. 상단 옵션 바 시간 선택에서 조회 시점을 선택할 수 있습니다. 선택한 시점 기준 최근 10분 데이터를 표시합니다.
- 2. 상단 옵션 바 매니저 선택에서 데이터를 수집하는 NMS 매니저를 선택해 사용량 현황을 확인할 수 있습니다.
- 3. 디바이스 선택 영역에서 분석할 디바이스 또는 특정 인터페이스를 선택합니다.

선택	표시되는 뷰
디바이스만 선택	Device 레벨 뷰(전체 인터페이스 트렌드)
디바이스 > 인터페이스 선택	Interface 레벨 뷰(단일 인터페이스 상세)

- 4. 선택한 디바이스 또는 인터페이스 사용량 현황을 확인할 수 있습니다.

인터페이스 표시 형식

디바이스를 선택하면 인터페이스 표시 형식을 선택할 수 있습니다.

Device Status

WhaTap AI

Summarize critical / warning alerts from the last 24 hours.

Time selector

LIVE 10:37:30

Manager selection

nmsdevr94

Device selection

Flat

Group

Search

Catalyst2960 (192.168.1.241)

Catalyst9300 (192.168.1.240)

dummy device (10.86.144.2)

huawei5720 (192.168.1.248)

Test4 (192.168.40.11)

WhaTap Office (192.168.1.250)

yamaha sw1 (192.168.1.239)

Overview

Interface information

Seoul HQ / SparkPlus / 13F / Catalyst2960 (192.168.1.241)

Catalyst2960 (192.168.1.241)

Total 52

Connected 1

Link Down 51

Admin Down 0

Device

Status

Gi0/1

Gi0/2

Gi0/3

Gi0/4

Gi0/5

Gi0/6

Gi0/7

Gi0/8

Gi0/9

Gi0/10

Gi0/11

Gi0/12

Gi0/13

Gi0/14

Gi0/15

Gi0/16

Gi0/17

Gi0/18

Gi0/19

Gi0/20

Gi0/21

Gi0/22

Gi0/23

Gi0/24

Gi0/25

Gi0/26

Gi0/27

Gi0/28

Gi0/29

Gi0/30

Gi0/31

Gi0/32

Gi0/33

Gi0/34

Gi0/35

Gi0/37

Gi0/38

Gi0/39

Gi0/40

Gi0/41

Gi0/42

Gi0/43

Gi0/44

Gi0/49

Gi0/50

Gi0/51

Gi0/52

Hostname

Catalyst2960.nmslab.local

Vendor

ciscoSystems

Serial No

FCW2456A2PJ

Firmware

15.2(6)E

Location

whatap-office13F

Item	Description
디바이스	실제 장비 전면과 같은 형태로 포트를 배치해 표시
상태	인터페이스 상태를 목록 형태로 표시

물리 포트 정보가 없는 장비는 프레임 대신 수집된 인터페이스 포트 정보가 없습니다. 안내가 표시되며, 포트 배치 설정 진입점도 노출되지 않습니다.

포트 배치 설정

디바이스 형식에서는 화면에 표시할 포트 배치를 장비 실물에 맞게 조정할 수 있습니다.

- 아이콘을 클릭하세요. 포트 배치 설정 창이 열립니다.
- 프레임 영역에서 장비 규격을 선택하세요.

Item	Description
폭	한 행이 수용하는 포트 수. 24포트 또는 48포트

Item	Description
높이	프레임 행 수. 1 부터 3 까지
SFP 포트	각 행 오른쪽에 여분 포트 슬롯 4개 추가

3. 포트를 드래그하거나, 포트를 클릭한 뒤 옮길 자리를 클릭해 위치를 바꾸세요.
4. 적용 버튼을 클릭해 저장하세요. 되돌리려면 취소 버튼을 클릭하세요.
 - 기본 배치로 돌아가려면 기본 배치로 되돌리기 버튼을 클릭하세요.

❗ 프레임 용량이 부족하면 {count}개 포트가 프레임 밖에 남았습니다. 폭이나 높이를 키우세요. 안내가 표시됩니다.
모든 포트가 배치되면 배치된 포트 수와 남은 슬롯 수가 표시됩니다.

❗ 상태 형식이거나 편집할 물리 포트가 없으면 포트 배치 설정 버튼이 비활성 상태로 표시되고, 사유가 톨팁으로 안내됩니다.

사용량 현황 - Device

디바이스를 선택하면 해당 디바이스의 전체 인터페이스 트래픽 추이를 라인 차트로 표시합니다.

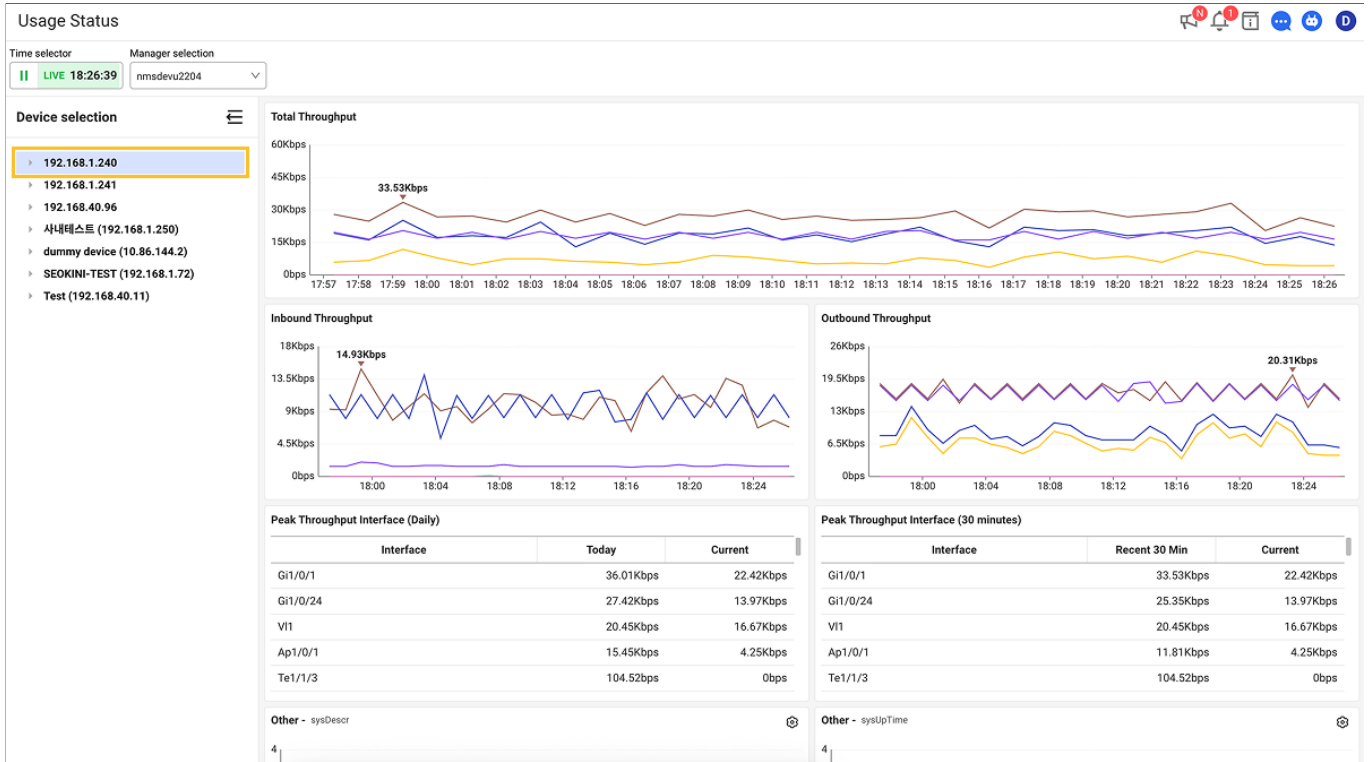


차트 패널

패널	설명
Total Throughput	전체 인터페이스 합산 처리량으로 화면 전체 너비로 표시됨
Inbound Throughput	인터페이스별 인바운드 트래픽으로 각 인터페이스가 개별 라인으로 표시됨
Outbound Throughput	인터페이스별 아웃바운드 트래픽
Top N (Daily)	일간 최대 처리량 기준 인터페이스 순위 테이블
Top N (10분)	최근 10분 최대 처리량 기준 인터페이스 순위 테이블

Top N 테이블 컬럼

컬럼	설명
Interface	인터페이스 이름
Today / Recent 10 Min	해당 기간 내 최대 처리량(bps 단위)
Current	현재 처리량(bps 단위)

ⓘ Top N 테이블은 처리량 기준 내림차순으로 정렬되어 가장 많은 트래픽을 사용하는 인터페이스를 빠르게 식별할 수 있습니다.

Private MIB 위젯

디바이스에 커스텀 OID(Private MIB)가 설정된 경우, 추가 위젯이 표시됩니다.

항목	설명
표시 조건	AllInterfaces 외의 OID가 설정된 경우
위젯 내용	OID별 커스텀 지표 차트

Private MIB 차트 커스터마이징

Private MIB 위젯 오른쪽 위의 ⚙ 아이콘을 클릭하면 **Chart Setting** 창이 열립니다. **Chart Setting** 창은 세 영역으로 구성됩니다.

영역	설명
Chart Preview	현재 설정으로 차트가 어떻게 표시되는지 미리 확인
OID Information	해당 OID의 상세 정보

영역	설명
	OID: 수집 대상 OID (예: 1.3.6.1.4.1.9.6.1.101.1.8.0) MIB Info: MIB 모듈과 심볼 정보 (예: CISCO-SB-MIB::rxCpuUtilDuringLastMinute) Node Type: MIB 노드 타입 (예: Integer32, Counter64) Description: MIB 파일에 정의된 OID 설명
Chart Setting	차트 유형, 단위 등 설정 옵션

Chart Setting 옵션

Chart Setting 옵션인 시간 범위, 차트 유형, 단위를 설정합니다.

Time Range(시간 범위)

옵션	설명	사용 가능한 차트
Recent 30 Min	최근 30분 데이터를 시계열로 표시	Line, Bar
Latest	가장 최근 값만 표시	Text, Table

ⓘ Time Range를 변경하면 사용 가능한 Chart Type이 자동으로 변경됩니다.

Chart Type(차트 유형)

유형	차트	설명
Time Range가 Recent 30 Min인 경우	Line	시계열 라인 차트. 트렌드 분석에 적합
	Bar	시계열 막대 차트. 구간별 비교에 적합
Time Range가 Latest인 경우	Text	최신 값을 큰 텍스트로 표시. 단일 지표 모니터링에 적합
	Table	테이블 형태로 표시. 여러 인덱스 값 비교에 적합

Unit(단위)

단위	설명	사용 예시
Count	일반 숫자(기본값)	패킷 수, 세션 수
Byte	바이트 단위 자동 변환(KB, MB, GB)	메모리 사용량, 파일 크기
Bit	비트 단위 자동 변환(Kb, Mb, Gb)	저장 용량
bps	초당 비트 자동 변환(Kbps, Mbps, Gbps)	대역폭, 처리량
Percent (0-100)	퍼센트(0~100 범위)	CPU 사용률, 메모리 사용률
Percent (0-1)	퍼센트(0~1 범위, 100 곱해서 표시)	일부 장비의 사용률
Severity	커스텀 상태값 매핑	장비 상태, 알람 수준

Severity 커스터마이징

Unit을 Severity로 선택하면 숫자 값을 의미 있는 상태 레이블로 매핑할 수 있습니다.

기본 Severity 설정

Value	Label
0	Normal
1	Warning
2	Critical

Severity 설정 방법

1. Unit 드롭다운에서 **Severity**를 선택합니다.
2. 기본 3개의 상태 (Normal, Warning, Critical)가 표시됩니다.

3. 각 상태의 설정을 수정합니다.

- **Label:** 화면에 표시될 상태명 (예: 정상, 경고, 위험)
- **Value:** 해당 상태로 인식할 OID 값 (정수)

4. **Add Severity** 버튼으로 새 상태를 추가합니다.

5. **X** 버튼을 클릭해 불필요한 상태를 삭제합니다.

✔ Severity는 SNMP 장비의 상태 코드를 사람이 읽기 쉬운 레이블로 변환할 때 유용합니다.

Severity 사용 예시

장비 운영 상태 모니터링

Value	Label	의미
1	Running	정상 운영 중
2	Standby	대기 상태
3	Down	장애 상태

포트 상태 모니터링

Value	Label	의미
1	Up	활성
2	Down	비활성
3	Testing	테스트 중

사용량 현황 - Interface

특정 인터페이스를 선택하면 해당 포트의 상세 지표를 4개 차트 패널로 표시합니다.



차트 패널

패널	지표	단위	설명
Throughput In/Out	bpsIn, bpsOut	bps	인바운드/아웃바운드 처리량
Discard In/Out	discardIn, discardOut	count	폐기된 패킷 수
Error In/Out	errorIn, errorOut	count	에러 발생 패킷 수
PPS In/Out	ppsIn, ppsOut	count	초당 패킷 수

통계 정보

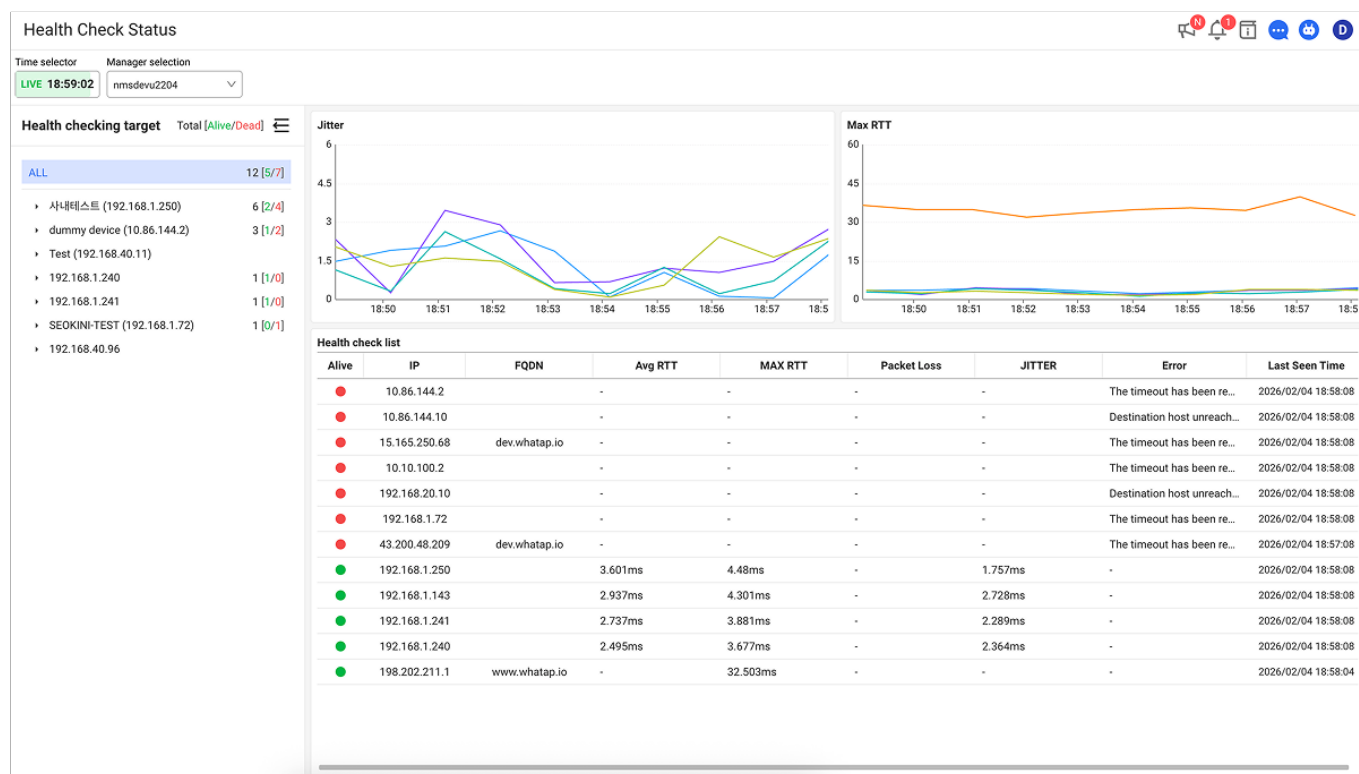
각 차트 하단에 Input/Output 통계가 표시됩니다.

항목	설명
Current	현재 값(가장 최근 데이터 포인트)
Max	조회 기간 내 최대값
Avg	조회 기간 내 평균값

헬스 체크 상태

헬스 체크 상태에서 헬스 체크 결과를 실시간으로 모니터링할 수 있습니다. 각 대상의 응답 상태, RTT, Jitter, 패킷 로스 등 상세 지표를 확인합니다.

기본 화면 및 설정



시간 선택

상단 옵션 바 시간 선택에서 실시간 데이터 갱신 시간을 표시합니다.

매니저 선택

상단 옵션 바 매니저 선택에서 데이터를 수집하는 NMS 매니저를 선택해 헬스 체크 결과를 확인할 수 있습니다.

헬스 체크 대상 선택

좌측 패널에서 조회할 디바이스 또는 헬스 체크 대상을 선택합니다.

선택 레벨	설명
ALL [n]	모든 헬스 체크 결과로 괄호 안의 숫자는 Alive/Dead 개수
디바이스명	특정 디바이스에 등록된 헬스 체크만 표시
대상 (IP/FQDN)	특정 대상의 상세 결과만 표시

상태 표시

각 항목 옆에 헬스 체크 상태 결과가 전체 수[정상 응답 수/미응답 수] 형식으로 표시됩니다.

- **녹색**: Alive(응답 있음)
- **빨간색**: Dead(응답 없음)

헬스 체크 결과

차트

선택한 대상의 지표를 시계열 차트로 표시합니다.

차트	설명
Jitter	지터(Jitter) 추이(ms)로 ICMP 타입에서 제공됨
Max RTT	최대 RTT(Round Trip Time) 추이(ms)로 모든 타입에서 제공됨

시간 범위

- 고정 10분 범위의 데이터를 표시합니다.
- 10초 간격으로 자동 갱신됩니다.

헬스 체크 목록

컬럼	설명
Alive	응답 상태 - ●: Alive(정상 응답) - ●: Dead(응답 없음)
Type	헬스 체크 타입(ICMP, TCP 등)
IP	헬스 체크 대상 IP 주소
FQDN	Fully Qualified Domain Name(도메인명)
Port	TCP 포트 번호(TCP 타입인 경우)
Avg RTT	평균 Round Trip Time(ms)
Max RTT	최대 Round Trip Time(ms)
Packet Loss	패킷 손실률(%)
Jitter	지터 값(ms)
Error	오류 메시지
Last Seen Time	마지막 응답 수신 시간

부록

지표

타입별 제공 지표	ICMP	TCP
Alive	O	O
Avg RTT	O	-
Max RTT	O	O
Jitter	O	-
Packet Loss	O	-
Port	-	O
Error	O	O

• RTT(Round Trip Time)

지표	설명
Avg RTT	평균 왕복 시간 - 응답 지연 시간의 평균
Max RTT	최대 왕복 시간 - 가장 느린 응답 시간

• Packet Loss

전송된 패킷 중 손실된 패킷의 비율(%)입니다.

• Jitter

네트워크 지연 시간의 변동폭입니다. Jitter가 높으면 네트워크 품질이 불안정함을 의미합니다.

데이터 갱신 주기

페이지는 10초 간격으로 자동 갱신됩니다.

항목	값
갱신 주기	10초
시간 범위	최근 10분

지원 헬스 체크 타입

타입	설명
ICMP	ICMP Ping 기반 연결 상태 확인
TCP	TCP 포트 연결 상태 확인

디바이스 인벤토리

디바이스 인벤토리는 네트워크상의 장비를 등록하고 모니터링 설정을 관리합니다. 장비는 매니저에서 제공하는 Auto Discovery 기능을 통해 자동으로 탐지하거나, 필요에 따라 수동으로 추가할 수 있습니다. 등록된 각 장비는 SNMP 기반 모니터링과 Health Check를 설정하여 실시간 상태를 확인할 수 있습니다. 이를 통해 네트워크 관리 시스템에서 모니터링할 디바이스를 통합적으로 관리할 수 있습니다.

기본 화면 및 설정

디바이스 인벤토리에서 등록된 모든 네트워크 장비 목록을 테이블 형태로 확인할 수 있습니다. 상단 메뉴에서 장비 등록 및 관리와 관련된 주요 기능을 제공합니다.

Device Inventory

Manager selection

nmsdevu2204

+ Add device

+ Bulk configuration for SNMP polling

Total: 7 SNMP Enabled: 5 SNMP Disabled: 2

	Alias	Host	Hostname	Description	Manufacturer	Location	Contact	Host Type	Role	Serial No.	Firmware
	사내테스트	192.168.1.250	hsnamdev	SF350-08 8-Port 10/100 Managed Switch	ciscoSystems	13F		switch			
	dummy device	10.86.144.2	demo#001	demo test	ciscoSystems	usa					
	Test	192.168.40.11	Test		unknown						
		192.168.1.240	Catalyst9300.nmslab.L...	Cisco IOS Software [Dublin], Catalyst L3 S...	ciscoSystems	whatap-office13F	jdson				
		192.168.1.241	Catalyst2960.nmslab.L...	Cisco IOS Software, C2960L Software (C2...	ciscoSystems	whatap-office13F	jdson				
	SEOKINI-TEST	192.168.1.72	testui-MacBookPro.local			13F					
		192.168.40.96	v3 test								

매니저 선택

연결된 NMS Manager 인스턴스를 선택합니다.

디바이스 추가

+ 디바이스 추가 버튼을 클릭해, 새로운 네트워크 장비를 수동으로 추가합니다. 자세한 내용은 [디바이스 추가](#)를 참고하시기 바랍니다.

SNMP Polling 일괄설정

+ SNMP Polling 일괄설정 버튼을 클릭해, 여러 디바이스에 SNMP Polling 설정을 일괄 적용합니다.

상태 요약

항목	설명
Total	전체 등록된 디바이스 수
SNMP Enabled	SNMP Polling이 활성화된 디바이스 수
SNMP Disabled	SNMP Polling이 비활성화된 디바이스 수

! 상태 요약 항목을 클릭하면 해당 상태의 디바이스만 필터링하여 조회할 수 있습니다.

디바이스 목록

디바이스 목록 구성	설명
	디바이스 설정 수정, 클릭 시 디바이스 설정 Drawer가 열림
Alias	장비 별칭
Host	장비 IP 주소
Hostname	장비의 호스트명
Description	장비 설명(장미 모델명 등)
Manufacturer	제조사(예: Cisco Systems)
Location	설치 위치
Contact	담당자 연락처
Host Type	호스트 유형(예: Switch, Router)

디바이스 목록 구성	설명
Role	장비 역할(예: Border Router, Edge Switch)
Serial No.	장비 시리얼 번호
Firmware	펌웨어 버전
SNMP Polling	SNMP Polling 상태 및 수집 OID 개수
Health Check	Health Check 상태 및 설정 개수

+ 디바이스 추가

새로운 네트워크 장비를 수동으로 등록할 수 있습니다.

1. 디바이스 인벤토리 화면의 + 디바이스 추가 버튼을 클릭하세요.
2. 디바이스 추가에서 디바이스 정보 탭에 정보를 입력하세요.
 - **Host(필수)**: 장비의 IP 주소
 - **Host Name**: 장비의 호스트명
 - **Manufacturer**: 제조사 정보
 - **Contact**: 담당자 정보
 - **Role**: 네트워크에서의 역할
 - **Alias**: 관리용 별칭
 - **Description**: 장비 상세 설명
 - **Location**: 물리적 설치 위치
 - **Host Type**: 장비 유형
 - **Serial No.**: 시리얼 번호
3. 추가 버튼을 클릭하면 장비가 추가됩니다.

디바이스 상세 관리

1. 등록된 장비의 를 클릭하세요.
2. 상세 정보창의 디바이스 정보, SNMP Polling, 헬스 체크 탭에서 상세 정보를 확인 또는 수정하고 저장 버튼을 클릭하세요.

디바이스 정보 탭

장비의 기본 정보를 설정합니다.

SNMP Polling 탭

SNMP 프로토콜을 사용하여 주기적으로 장비의 성능 및 상태 정보를 수집하는 설정을 관리합니다. 정보를 수정한 후 저장 버튼을 클릭하여 설정합니다.

- Port(필수): SNMP 포트(기본값: 161)
- Community(필수): SNMP v1/v2c Community String(기본값: public)
- Version(필수): SNMP 버전 선택(v1, v2c, v3)
- User Name: SNMPv3 사용자명
- Security Level: 보안 수준(noAuthNoPriv, authNoPriv, authPriv)
- Authentication Protocol: 인증 프로토콜
 - Authentication Key: 인증 키
- Privacy Protocol: 암호화 프로토콜
 - Privacy Key: 암호화 키

OID 선택 및 관리

1. Edit OID 버튼을 클릭하여 OID 목록에서 수집할 MIB 정보를 선택합니다.

OID List 구성	설명
OID	SNMP OID 값
MIB Information	MIB 이름 및 정보
Manufacturer	제조사
Category	지표 종류
Description	상세 설명

2. OK 버튼을 클릭하세요.

수집 주기 설정

- **Custom Polling Interval:** 데이터 수집 주기 설정(단위: 초, 기본값: 60)
- **Activate:** SNMP Polling 활성화/비활성화

헬스 체크 탭

네트워크 장비의 가용성을 실시간으로 모니터링합니다. 헬스 체크 대상을 추가할 수도 있습니다.

Health Check 목록 구성	설명
Activate	헬스체크 기능 활성화 상태
Target Host	모니터링 대상 IP 주소 또는 FQDN
Protocol	헬스체크 프로토콜(ICMP 등)
Memo	메모 또는 설명
Actions	헬스체크 대상 수정(✎), 삭제(🗑)

헬스 체크 대상 추가하기

1. Health Check 탭에서 + 추가 버튼을 클릭하세요.
2. 헬스체크 대상 추가 팝업창에서 정보를 입력하세요.
 - **Target Host:** IP 주소 또는 FQDN 입력
 - **Protocol:** ICMP 선택 (드롭다운)
 - **Memo:** 선택적 메모 입력
 - **Activate:** 즉시 활성화 여부 선택
3. 확인 버튼을 클릭해 저장합니다.

그룹 관리

홈 화면 > 프로젝트 선택 > 디바이스 관리 > 그룹 관리

그룹 관리 메뉴에서 디바이스를  Site →  Building →  Floor 구조로 관리할 수 있습니다. 그룹을 기준으로 디바이스를 구조화하면 대규모 네트워크 환경에서 관리 및 모니터링이 편리해집니다.

기본 화면 및 설정

그룹 관리



매니저 선택

nmsdevu2204

+ Add Location

NAME	DESCRIPTION	DEVICES	
 Seoul HQ	-	-	+ 추가 ✎ 수정 🗑 삭제
 SparkPlus	-	-	+ 추가 ✎ 수정 🗑 삭제
 13F	-	View Devices	✎ 수정 🗑 삭제
 Tokyo Office	-	-	+ 추가 ✎ 수정 🗑 삭제
 Nakayama B/D	-	-	+ 추가 ✎ 수정 🗑 삭제
 11F	-	View Devices	✎ 수정 🗑 삭제

1. 그룹 관리 화면 상단의 매니저 선택에서 그룹 관리를 할 매니저를 선택하세요. 선택한 매니저 기준으로 그룹 목록이 표시됩니다.
2. 선택한 매니저 기준으로 표시된 그룹 목록을 확인, 추가, 삭제할 수 있습니다.  Site →  Building →  Floor의 트리 형태로 표시됩니다.

표 | 그룹 목록

컬럼	설명
Name	그룹 이름(위치/건물/층)

컬럼	설명
Description	그룹 설명
Devices	해당 그룹에 포함된 디바이스 보기
작업	그룹 추가/수정/삭제

그룹 추가

Location 추가

1. 화면 위의 **+ Add Location** 버튼을 클릭하세요.
2. **Add Location** 창에서 이름과 타입을 입력하세요.
3. **Save** 버튼을 클릭하면 새로운 Location이 생성됩니다.

Building 추가

1. Building을 추가할 Location의 **+ 추가** 버튼을 클릭하세요.
 - 화면 위의 **+ Add Location** 버튼을 클릭해 추가할 수도 있습니다.
2. **Add building** 창에서 이름을 입력하세요.
3. **Save** 버튼을 클릭하면 새로운 Building이 생성됩니다.

Floor 추가

1. Floor를 추가할 Building의 **+ 추가** 버튼을 클릭하세요.
 - 화면 위의 **+ Add Location** 버튼을 클릭해 추가할 수도 있습니다.
2. **Add floor** 창에서 이름을 입력하세요.

3. **Save** 버튼을 클릭하면 새로운 Building이 생성됩니다.
4. **View Devices** 버튼을 클릭해 할당된 장비를 확인할 수 있습니다.

그룹 수정

1. 수정할 그룹의  수정 버튼을 클릭하세요.
2. 그룹 이름 또는 설명을 변경합니다.
3. **Save** 버튼을 클릭해 변경 사항을 반영합니다.

그룹 삭제

1. 삭제할 그룹 우측의  삭제 버튼을 클릭하세요.
2. 삭제 확인 팝업에서 **삭제**를 클릭하면 해당 그룹이 삭제됩니다.

디바이스 할당

그룹 관리 목록에서 Floor의 **View Devices** 버튼을 클릭하면 디바이스 할당창이 열립니다.

디바이스 추가/삭제

- + 추가 버튼을 클릭해 미할당 디바이스를 선택하면 즉시 할당됩니다.
-  아이콘을 클릭해 개별 디바이스를 해제합니다.

일괄 편집

여러 디바이스를 한 번에 관리할 수 있습니다.

1. Floor의 **View Devices** 버튼을 클릭해 디바이스 할당 창이 열립니다.
2.  수정 버튼을 클릭하면 일괄 편집 창으로 이동합니다.

패널	설명
Unassigned (왼쪽)	미할당 목록이며 + 클릭해 할당
Assigned (오른쪽)	할당 목록이며 - 클릭해 할당 해제

3. 일괄 편집 화면에서 **저장** 버튼을 클릭해 변경사항을 저장합니다.

태스크 설정

Network 자동화를 사용하면 네트워크 디바이스에 SSH로 접속해 명령어를 자동으로 실행할 수 있습니다. 예를 들어, 라우터 설정 파일을 매일 백업하거나, 특정 이벤트가 발생했을 때 자동으로 진단 명령을 실행하는 작업을 등록할 수 있습니다.

태스크를 추가하려면 대상 디바이스에 SSH로 접속할 수 있는 계정 정보(사용자명·비밀번호 또는 SSH 키 파일)가 필요합니다.

태스크 목록 확인

네트워크 자동화 > 태스크 설정에 진입하면 등록된 태스크 목록을 볼 수 있습니다. 화면 상단의 **매니저 선택** 드롭다운에서 NMS 매니저를 선택하고, 검색창에 디바이스 별칭, 호스트, 사용자명, 메모를 입력하면 태스크를 바로 찾을 수 있습니다.

화면 상단에 상태별 태스크 수가 표시됩니다. 칩을 클릭하면 해당 상태의 태스크만 필터링됩니다.

칩	설명
전체	등록된 태스크 전체 수
활성	현재 활성화되어 실행 중인 태스크 수
비활성	일시 중단된 태스크 수
예약됨	주기적으로 자동 실행되는 태스크 수

목록 주요 정보

목록에서 확인할 수 있는 주요 정보입니다.

컬럼	설명
번호	태스크 순번
활성	초록색 점(깜박임)은 활성, 회색 점은 비활성 상태

컬럼	설명
별칭	디바이스 별칭. 클릭하면 해당 태스크의 실행 이력으로 이동
호스트	디바이스 IP 또는 호스트명
사용자명	SSH 접속 계정명
포트	SSH 접속 포트
인증 방식	비밀번호 또는 키 파일
스케줄	manual (수동), every N분 (주기 실행), detector (이벤트 트리거)
명령어	태스크에 등록된 명령어 개수
재시도	실패 시 재시도 횟수
키 파일	키 파일 인증 사용 시 파일명
타임아웃	명령어 실행 제한 시간
마지막 상태	마지막 실행 결과: success, failure, pending
마지막 실행 시각	마지막 실행 시각
다음 실행 시각	다음 예약 실행 시각 (manual 이면 표시 없음)
메모	태스크 설명 메모

태스크 추가하기

1. 우상단 태스크 추가 버튼을 클릭합니다.
2. 팝업에서 각 항목을 설정하고 저장을 클릭합니다.

1단계: 기본 정보 입력

어떤 디바이스에 어떤 계정으로 접속할지 설정합니다.

필드	필수	설명
디바이스	필수	명령어를 실행할 대상 디바이스 선택
사용자명	필수	SSH 접속 계정명
SSH 포트	필수	SSH 포트, 기본값(22)이 아닌 경우에만 변경
디바이스 유형	필수	CLI 드라이버 유형, 잘 모른다면 자동 감지를 켜면 태스크 설정 저장 시 서버가 자동으로 판별
활성화		태스크 설정 사용 여부(활성화/비활성화)
재시도 횟수	필수	네트워크가 불안정한 환경이라면 1~3회 설정을 권장
타임아웃(초)	필수	응답이 늦은 디바이스라면 기본값보다 높게 설정
메모		태스크 정보 메모 작성

2단계: 실행 시점 선택(스케줄)

언제 이 태스크를 실행할지 결정합니다.

스케줄 유형	언제 사용하나요?
Manual	필요할 때 직접 실행 버튼을 누르는 방식, 자동 실행이 필요 없을 때
Scheduler	매 N분마다 또는 매일 특정 시각에 자동 실행, 정기 백업·수집에 적합
Detector	특정 이벤트나 조건이 감지됐을 때 자동 실행, 장애 대응 자동화에 적합

3단계: SSH 인증 방식 선택

인증 방식	언제 사용하나요?
비밀번호	SSH 비밀번호를 직접 입력, 빠르게 시작하고 싶은 경우
키 파일	SSH 키 파일로 인증 및 비밀번호 없이 안전하게 접속하고 싶은 경우, 키 파일을 미리 SSH 키 관리에서 업로드 해야 함

4단계: 실행할 명령어 등록

실행할 명령어를 순서대로 추가합니다. 명령어는 1개 이상 필요합니다.

1. + 명령어 추가 버튼을 클릭해 명령어를 입력합니다.
2. ↑ ↓ 버튼으로 실행 순서를 조정합니다.
3. 명령어마다 설명을 함께 적어두면 나중에 알아보기 쉽습니다.

저장 전 연결 테스트

저장하기 전에 접속이 되는지 먼저 확인하는 것을 권장합니다.

1. 연결 테스트 버튼을 클릭합니다.
2. 결과가 팝업 하단에 표시됩니다.
 - 성공: 접속 프롬프트 미리보기
 - 실패: 오류 유형 및 원인 메시지

태스크 편집·즉시 실행·삭제

목록 우측 액션 버튼으로 각 동작을 수행합니다.

버튼	설명
편집	설정 팝업이 열리며 기존 값을 수정할 수 있음
즉시 실행	확인 후 바로 태스크 실행, 결과는 태스크 현황 에서 확인 가능
삭제	태스크 삭제, 삭제하면 실행 이력도 함께 사라짐

SSH 키 파일 관리

키 파일 인증을 사용하려면 먼저 키 파일을 등록해야 합니다. 우상단 **SSH 키 관리** 버튼을 클릭하세요.

동작	방법
업로드	.pem 등 SSH 개인 키 파일을 선택하고 파일명 입력, 패스프레이즈가 있는 키라면 함께 입력
삭제	목록에서 더 이상 사용하지 않는 키 파일 삭제

태스크 현황

태스크 현황에서 자동화 태스크가 실제로 실행된 이력과 각 명령어의 출력 결과를 확인할 수 있습니다. 태스크가 예상대로 동작하는지 확인하거나, 실패 원인을 찾을 때 사용합니다. 태스크 설정 화면에서 디바이스 별칭을 클릭하면 해당 태스크의 실행 이력이 바로 필터링된 상태로 열립니다.

원하는 결과 찾기(필터)

실행 이력이 많을 때는 필터로 범위를 좁힙니다. 필터를 모두 초기화하려면 초기화 버튼을 클릭합니다.

필터	사용 방법
매니저 선택	NMS 매니저를 선택
태스크	특정 태스크의 결과만 보고 싶을 때 선택
명령어	특정 명령어 이름으로 검색
상태	성공/실패만 골라서 보고 싶을 때 선택
시작일~종료일	특정 기간의 실행 이력만 조회
표시 개수	한 번에 불러올 최대 건수 (100 / 500 / 1000 / 5000)

실행 결과 요약

필터 아래에 현재 조회 결과의 요약이 표시됩니다.

항목	설명
전체	조회된 전체 실행 건수
성공	성공으로 완료된 건수

항목	설명
실패	실패로 종료된 건수

실행 이력 목록

최근 실행 순으로 목록이 표시됩니다.

컬럼	설명
실행 시각	태스크가 실행된 시각
호스트	실행 대상 디바이스 호스트명
별칭	디바이스 별칭
명령어	실행된 명령어
상태	성공 (초록) / 실패 (빨강)
소요 시간	명령어 실행에 걸린 시간 (예: 1.234s)
오류	실패 시 오류 메시지 (길면 말줄임표로 표시, 커서를 올리면 전체 확인 가능)

실행 결과 상세 보기

- 목록에서 행을 클릭하면 해당 명령어의 전체 출력이 아래로 펼쳐집니다.
- 출력 내용을 활용합니다.
 - 복사:** 클립보드에 복사
 - 다운로드:** 텍스트 파일로 저장 (파일명 형식: automation_YYYY-MM-DD_별칭_ID.txt)
- 상태가 실패 인 행을 클릭하면 오류 메시지와 함께 명령어가 어디까지 실행됐는지 출력에서 확인할 수 있습니다.

설정 변경 이력

설정 변경 이력에서 자동화 태스크가 수집한 디바이스 설정 파일의 스냅샷을 조회하고, 이전 상태와 비교해 무엇이 바뀌었는지 확인할 수 있습니다. 예를 들어, 라우터 설정 백업 태스크를 매일 실행한다면 이 화면에서 "어제와 오늘 설정이 어떻게 달라졌는지"를 라인 단위로 볼 수 있습니다.

설정 변경 이력은 태스크 생성 시 **설정 변경 추적** 옵션이 활성화된 태스크에서만 수집됩니다.

필터

화면 상단에서 조회 범위를 설정합니다.

필터	사용 방법
매니저 선택	NMS 매니저를 선택
태스크	특정 태스크의 이력만 보려면 선택
시작일/종료일	조회할 날짜 범위 - 데이터 보존 기간 내의 날짜만 선택할 수 있으며, 기본적으로 최근 30일 이내의 데이터를 조회할 수 있음
표시 개수	한 번에 불러올 최대 건수 (100 / 500 / 1000 / 5000)
범위	변경만: 설정이 실제로 바뀐 스냅샷만 표시 전체: 변경 여부에 관계없이 전체 표시

변경 현황 개요

필터 아래 **변경 현황 개요** 패널에서 전체 상황을 빠르게 파악할 수 있습니다. 헤더 우측 화살표로 패널을 접거나 펼칠 수 있고, 패널과 목록 사이 구분선을 드래그해 영역 높이를 조절할 수 있습니다.

통계

항목	설명
전체	조회 기간에 수집된 전체 스냅샷 수
변경됨	이전 스냅샷과 비교해 설정이 바뀐 스냅샷 수

요약 테이블

어떤 디바이스·명령어·날짜에서 변경이 집중됐는지 상위 5개를 탭별로 확인할 수 있습니다.

탭	내용
많이 변경된 호스트	설정 변경 횟수가 가장 많은 디바이스 목록으로 자주 바뀌는 장비를 파악하는 경우
명령어별 영향	가장 많은 디바이스에 영향을 준 명령어 목록으로 변경 범위가 넓은 작업을 확인하는 경우
변경 상위 날짜	설정 변경이 가장 많이 발생한 날짜로 특정 날 대규모 변경이 있었는지 파악하는 경우

일별 변경 차트

날짜별 설정 변경 건수를 막대 차트로 보여줍니다. **특정 날짜 막대를 클릭하면** 그 날짜의 스냅샷만 목록에 표시됩니다. 다시 전체로 돌아가려면 **뒤로 가기** 버튼을 클릭하세요.

설정 스냅샷 목록

수집된 스냅샷 목록입니다. 각 행은 태스크가 한 번 실행될 때 캡처된 설정 파일 상태를 나타냅니다.

컬럼	설명
번호	스냅샷 순번

컬럼	설명
캡처 시각	스냅샷이 캡처된 시각
호스트	대상 디바이스 호스트명
별칭	디바이스 별칭
명령어	설정을 수집한 CLI 명령어
추가	이전 스냅샷보다 늘어난 줄 수(초록색)
삭제	이전 스냅샷에서 사라진 줄 수(빨간색)
변경	modified (변경됨, 주황) / unchanged (변경 없음, 회색) / initial (최초 수집)
상세	조회 버튼으로 변경 내용 상세 확인

변경 내용 상세 보기

1. 목록에서 조회 버튼을 클릭하면 팝업이 열립니다.
2. 팝업 상단에서 호스트, 별칭, 명령어, 변경 상태를 확인합니다. 상단 요약은 화살표를 클릭해 접을 수 있습니다.
3. 보기 편한 비교 모드를 선택합니다.

비교 모드

모드	설명
Unified	추가(초록 +)·제거(빨강 -) 줄을 하나의 뷰에서 순서대로 표시해 git diff와 유사한 형식
Split	이전 설정과 현재 설정을 좌우로 나란히 비교해 전체 맥락을 함께 보고 싶은 경우
Simple	변경된 줄만 색상으로 강조해 단순하게 표시해 빠르게 훑어볼 경우

예방 점검 프로파일

예방 점검은 네트워크 자동화 태스크에 등록된 명령어 중 일부를 골라 점검 항목으로 지정하고, 각 항목에 판정 규칙을 매핑해 실행 결과를 자동으로 점검하는 기능입니다. 태스크가 실행될 때마다 매핑한 규칙에 따라 정상·경고·심각 상태를 자동 판정한 리포트가 생성되므로, 반복 점검 항목을 표준화하고 임계 기반 이상 여부를 사람이 직접 확인하지 않아도 파악할 수 있습니다. 네트워크 장비를 반복 점검하는 네트워크 관리자와 인프라 엔지니어를 대상으로 합니다.

프로파일은 이 예방 점검의 점검 템플릿입니다. 어떤 자동화 태스크의 명령어를 점검 대상으로 쓸지, 각 명령어 결과에 어떤 항목 라벨과 판정 규칙을 적용할지 정의합니다.

프로파일 목록 확인

네트워크 자동화 > 예방 점검 프로파일에 진입하면 등록된 프로파일 목록을 볼 수 있습니다. 화면 상단의 매니저 선택 드롭다운에서 NMS 매니저를 먼저 선택해야 목록이 표시됩니다.

목록 주요 정보

컬럼	설명
번호	목록 순번
프로파일	프로파일 이름. 클릭하면 편집 팝업이 열림
자동화 태스크	프로파일이 연결한 자동화 태스크의 디바이스 별칭 또는 호스트
대상	태스크가 실제로 접속하는 디바이스 주소
명령어	프로파일에 등록된 점검 명령어 개수
최신 리포트	가장 최근 생성된 리포트의 상태(정상·경고·심각·알 수 없음) 배지와 생성 시각
프로파일 활성화	활성화 여부를 활성화·비활성화 배지로 표시. 목록에서 직접 토글할 수 없고 편집 팝업에서만 변경 가능
액션	자세히 보기·수정·삭제 아이콘. 자세히 보기와 수정은 동일한 편집 팝업을 엽니다

! 검색창에 프로파일 이름을 입력하면 목록을 바로 좁힐 수 있습니다.

프로파일 추가·수정하기

1. 우상단 **프로파일 추가** 버튼을 클릭합니다. 기존 프로파일을 고치려면 목록에서 **수정** 아이콘을 클릭하세요.
2. 팝업에서 각 항목을 설정하고 **프로파일 저장** 버튼을 클릭합니다.

1단계: 기본 정보 입력

필드	필수	설명
프로파일 이름	필수	점검 템플릿을 구분할 이름
자동화 태스크	필수	점검 대상으로 쓸 자동화 태스크 선택. 이미 다른 프로파일이 사용 중인 태스크는 목록에서 제외됨
프로파일 활성화		활성화 토글, 기본값은 활성화
메모		프로파일 설명 메모 작성

자동화 태스크를 선택하면 선택한 태스크의 **CLI 드라이버·스케줄·최근 실행 결과·명령어 개수**를 요약 카드로 확인할 수 있습니다.

2단계: 점검 항목 매핑

선택한 자동화 태스크에 등록된 명령어가 실행 순서대로 표에 나타납니다. 각 행에서 명령어별 점검 방식을 설정합니다.

컬럼	필드	설명
사용	체크박스	선택 해제한 명령어는 프로파일에 저장되지 않음
자동화 명령어	텍스트(읽기 전용)	태스크에 등록된 원본 명령어
항목 라벨	입력 필드	리포트에 표시할 점검 항목 이름을 입력하세요

컬럼	필드	설명
파서 사용	드롭다운	사용 을 선택해야 아래 매치 필드 를 선택할 수 있음
매치 필드	드롭다운	명령어 실행 결과를 파싱한 컬럼 중 판정에 쓸 컬럼을 선택하세요. 파싱에 실패한 명령어는 직접 입력하세요
적용 규칙	드롭다운	이 항목에 적용할 판정 규칙을 선택하세요. 규칙이 없으면 규칙 없음 을 선택하세요

우측 상단 **규칙 관리** 버튼을 선택하면 규칙 편집 팝업이 프로파일 편집 팝업 위에 겹쳐서 열립니다. 새 규칙을 등록한 뒤 바로 **적용 규칙** 드롭다운에서 선택할 수 있습니다.

- ✔ 명령어 실행 결과가 표 형태로 파싱되면 **매치 필드** 드롭다운에 실제 컬럼명이 자동으로 채워집니다. 파싱에 실패했다면 **매치 필드**에 값을 직접 입력하세요.

프로파일 삭제

1. 목록의 **삭제** 아이콘을 선택하면 확인 다이얼로그가 나타납니다.
2. 확인을 누르면 프로파일이 삭제됩니다.

예방점검 규칙

규칙은 [예방 점검 프로파일](#)의 점검 항목마다 적용하는 판정 기준입니다. 명령어 실행 결과가 규칙의 조건을 만족하면 **경고** 또는 **심각** 상태로 자동 판정합니다. 하나의 규칙을 여러 프로파일의 점검 항목에서 재사용할 수 있어, 임계값이나 판정 조건을 규칙 하나만 바꾸면 연결된 모든 항목에 반영됩니다.

규칙 목록 확인

네트워크 자동화 > 예방점검 규칙에 진입하면 등록된 규칙 목록을 볼 수 있습니다. 화면 상단의 **매니저 선택** 드롭다운에서 NMS 매니저를 먼저 선택해야 목록이 표시됩니다.

목록 주요 정보

컬럼	설명
번호	목록 순번
규칙 이름	규칙 이름
판정 방식	<code>threshold</code> (임계값) · <code>count</code> (개수) · <code>contains</code> (문자열 포함) · <code>regex</code> (정규식) 중 하나를 뱃지로 표시
경고 조건	경고로 판정하는 조건. <code>contains</code> · <code>regex</code> 방식은 사용 안 함 으로 표시
심각 조건	심각으로 판정하는 조건. <code>contains</code> · <code>regex</code> 방식은 값만 표시(예: <code>down</code>)
단위	임계값의 단위. <code>contains</code> · <code>regex</code> 방식은 사용 안 함 으로 표시
액션	수정·삭제 아이콘

규칙 추가·수정하기

1. 우상단 규칙 추가 버튼을 클릭합니다(기존 규칙을 고치려면 목록에서 수정 아이콘을 클릭하세요).

2. 팝업에서 각 항목을 설정하고 저장 버튼을 클릭합니다.

필드	필수	설명
이름	필수	규칙을 구분할 이름
판정 방식	필수	아래 표를 참조해 점검 결과에 맞는 방식을 선택하세요
경고 조건		판정 방식이 임계값·개수일 때만 연산자와 값을 입력. 문자열 포함·정규식 은 값만 입력
심각 조건		경고 조건과 동일한 입력 규칙
단위		판정 방식이 임계값·개수일 때만 입력
설명		규칙 설명 메모, 선택 사항

판정 방식별 동작

판정 방식을 바꾸면 입력 필드가 자동으로 바뀝니다.

판정 방식	연산자	값	단위	판정 기준
threshold (임계값)	>= > == != 중 선택	숫자로 해석되는 문자열	사용	결과값이 지정한 숫자 조건을 만족하는지 판정
count (개수)	>= > == != 중 선택	숫자로 해석되는 문자열	사용	조건에 매칭되는 결과 행의 개수로 판정
contains (문자열 포함)	사용 안 함	검사할 문자열	사용 안 함	실행 결과에 지정한 문자열이 포함되는지 판정
regex (정규식)	사용 안 함	정규식 패턴	사용 안 함	실행 결과가 정규식 패턴에 매치되는지 판정

규칙 삭제

목록의 **삭제** 아이콘을 선택하면 확인 문구가 나타납니다.

 이 규칙을 삭제하시겠습니까?

이 규칙을 사용 중인 프로파일 매핑은 **규칙 없음** 상태가 됩니다. 계속할까요?

확인을 누르면 규칙이 삭제되고, 이 규칙을 쓰던 프로파일의 점검 항목은 규칙 연결만 해제됩니다. 항목 자체는 그대로 유지됩니다.

예방점검 리포트

예방 점검 [프로파일](#)에 연결된 자동화 태스크가 실행될 때마다, 매핑한 [규칙](#)에 따라 판정한 리포트가 자동으로 생성됩니다. 리포트를 확인하면 어떤 장비의 어떤 점검 항목이 이상 상태인지 한눈에 파악할 수 있습니다. 프로파일마다 최근 2건의 리포트만 유지되며, 최신 리포트에는 바로 이전 리포트와 비교한 상태 변화 정보도 함께 표시됩니다.

리포트 목록 확인

네트워크 자동화 > 예방점검 리포트에 진입하면 프로파일별 최신 리포트 목록을 볼 수 있습니다. 화면 상단의 매니저 선택 드롭다운에서 NMS 매니저를 먼저 선택해야 목록이 표시됩니다.

❗ 목록은 자동으로 새로고침되지 않습니다. 최초 진입 시와 매니저를 변경했을 때만 자동으로 조회하며, 이후에는 화면 상단의 새로고침 버튼을 선택해야 최신 상태로 갱신됩니다.

상단 요약 카드

목록 위에 상태별 프로파일 수를 요약하는 카드가 표시됩니다. 카드를 선택하면 목록이 해당 상태로 필터링되고, 선택한 카드는 테두리로 강조됩니다.

카드	설명
점검 대상	리포트 생성 대상인 전체 프로파일 수
보고됨	이번 조회 기간에 리포트가 생성된 프로파일 수
미보고	아직 리포트가 생성되지 않은 프로파일 수. 선택하면 표 컬럼 구성이 다른 별도 목록으로 전환됨
정상	정상으로 판정된 프로파일 수
경고	경고로 판정된 프로파일 수
심각	심각으로 판정된 프로파일 수

카드	설명
알 수 없음	판정할 수 없는 상태의 프로파일 수

목록 주요 정보

컬럼	설명
번호	목록 순번
디바이스	리포트 대상 디바이스. 클릭하면 매니저 정보 화면으로 이동
프로파일	리포트를 생성한 프로파일 이름. 클릭하면 리포트 상세 팝업이 열림
생성 시각	리포트가 생성된 시각
점검 항목 수	리포트에 포함된 점검 항목 개수
결과 요약	정상·경고·심각·알 수 없음 항목 수를 색상으로 구분해 요약 표시
트리거	리포트를 생성시킨 실행 방식(scheduler · manual · detector) 배지
액션	상세 보기 아이콘

ⓘ 미보고 카드를 선택하면 표에는 리포트가 아직 없는 프로파일 목록이 대신 나타나며, 프로파일 이름·연결된 자동화 태스크·점검 항목 수만 표시됩니다.

리포트 상세 확인

1. 목록에서 프로파일을 클릭하면 리포트 상세 팝업이 열립니다.
2. 상단에 전체 항목 수/정상/경고/심각/알 수 없음 개수가 카드로 표시되고, 아래에는 점검 항목별 상세 결과가 나열됩니다.

3. 각 항목은 실행 결과 파싱 성공 여부에 따라 다르게 표시됩니다.

- **파싱 성공:** 점검 항목의 결과를 표 형태로 보여주고, 적용된 규칙의 판정 조건 문구(예: 경고 ≥ 10 / 심각 ≥ 30)와 판정 사유, 이전 리포트와 비교한 상태 변화를 함께 표시합니다. 원본 보기를 선택하면 명령어의 원본 실행 결과를 확인할 수 있습니다.
- **파싱 실패:** "지원하지 않거나 파싱할 수 없음" 안내와 함께 원본 실행 결과를 바로 보여줍니다.

이전 리포트와의 비교

각 점검 항목에는 바로 이전 리포트와 비교한 정보가 함께 표시됩니다.

상황	표시 내용
비교할 이전 리포트가 없음	이전 리포트 없음 안내
이전 리포트와 상태가 같음	상태 변화 없음 안내
이전 리포트와 상태가 다름	이전 상태에서 현재 상태로 바뀌었음을 강조 표시(예: 경고 → 심각)

기본 화면

OID 관리

메이스트 선택

nmstest02

+ OID 추가

OID	Manufacture	Category	Description	Edit
1.3.6.1.2.1.2.2	Standard	AllInterfaces	All Interfaces(32bit)	
1.3.6.1.2.1.31.1.1	Standard	AllInterfaces	All Interfaces(64bit)	
1.3.6.1.2.1.1.1.0	Standard	Other	System Description	
1.3.6.1.2.1.1.3.0	Standard	Other	System Uptime	
1.3.6.1.2.1.1.5.0	Standard	Other	System Name	
1.3.6.1.4.1.2021.11	Net-SNMP	CPU	net-snmp systemstats(cpu)	
1.3.6.1.4.1.2021.4	Net-SNMP	Memory	net-snmp memory usage	
1.3.6.1.4.1.2021.9	Net-SNMP	Disk	net-snmp disk usage	
1.3.6.1.4.1.9.9.109.1.1.1.5.19	Cisco	CPU	The overall CPU busy percentage in the last 5 minute period(%). 12.0(3)T - 12.2(3.5) ios	
1.3.6.1.4.1.9.9.109.1.1.1.1.8	Cisco	CPU	The overall CPU busy percentage in the last 5 minute period(%). 12.2(3.5) or later ios	
1.3.6.1.4.1.9.9.109.1.1.1.1.12	Cisco	Memory	The overall CPU wide system memory which is currently under use(KB)	
1.3.6.1.4.1.9.9.109.1.1.1.1.13	Cisco	Memory	The overall CPU wide system memory which is currently free(KB)	

OID 추가

1. 왼쪽 상단에서 에이전트를 선택하세요.
2. 오른쪽 상단에서 + **OID** 추가 버튼을 클릭 후 **OID** 추가 창에서 다음 정보를 입력하세요.

OID, Description, Manufacture, Category

❗ **Category**는 각 OID가 수집하는 리소스를 정의하는 데 사용됩니다. 이를 통해 OID가 수집하는 지표를 분류하고 관리할 수 있습니다.

OID 수정

OID 목록 왼쪽 **Edit** 컬럼에서  수정 아이콘을 선택하여 관련 정보를 수정할 수 있습니다.

경고 알림

모니터링 대상 시스템 또는 애플리케이션에서 문제가 발생했을 때, 미리 설정한 조건에 따라 사용자에게 알림을 전달하는 기능입니다. 알림은 이메일, SMS, 메신저, 앱 푸시 등 다양한 채널로 전송됩니다.

예를 들어, CPU 사용률, 메모리 사용량, 디스크 I/O, 네트워크 트래픽, 트랜잭션 수, 오류 발생, 응답 시간 지연 등 주요 성능 지표에 알림 기준을 설정해두면, 해당 기준을 초과하거나 이상 징후가 감지될 때 알림이 전송됩니다.

와탭의 AI 기반 알림 기능을 사용하면 복잡한 조건을 직접 설정하지 않아도 됩니다. AI는 애플리케이션의 정상적인 동작 패턴을 학습해 이상 패턴을 자동으로 감지하여 알려줍니다. 태그 카운트 알림 기능을 활용하면 특정 태그 기반으로 집계된 값에 조건을 설정하여 복잡한 상황도 정밀하게 감지할 수 있습니다.

주요 기능

- **이벤트 설정:** 임계치 기반 알림 조건과 수신 채널 설정
- **이벤트 수신 설정:** 사용자별 수신 채널, 시간대 설정
- **이벤트 기록:** 알림 발생 기록 조회

권한

이벤트를 추가하거나 설정하려면 **알림 설정 권한**이 필요합니다.

- **조회:** 메트릭스 이벤트 설정 내용을 확인하려면 **조회 분석 권한**이 필요합니다.
- **추가/수정/삭제:** 설정을 변경하려면 **알림 설정 권한**이 필요합니다.
- **알림 수신:** 알림을 수신하려면 **알림 수신 권한**이 필요합니다.

❗ 참고 문서

자세한 내용은 [멤버 권한](#)을 참고하시기 바랍니다.

이벤트 설정

홈 화면 > 프로젝트 선택 >  경고 알림 > 이벤트 설정

이벤트 설정에서 모니터링 대상 시스템 또는 애플리케이션에서 발생할 수 있는 이상 징후를 기준으로 이벤트를 설정하고 관리하는 기능을 제공합니다. 설정된 조건이 충족되면 이메일, SMS, 메신저, 앱 푸시 등 원하는 채널로 알림을 받을 수 있습니다. 모니터링 목적에 따라 이벤트를 구성할 수 있습니다.

메트릭스

메트릭스 이벤트는 실시간 데이터를 기반으로 시스템 및 애플리케이션의 성능 지표를 모니터링할 수 있습니다.

복합 메트릭스

복합 메트릭스 기능은 복잡한 규칙을 활용해 이벤트를 생성하고 경고 알림을 보낼 수 있습니다.

실시간 로그

실시간으로 수집한 로그에서 설정한 이벤트 조건이 발견되면 경고 알림을 보냅니다.

복합 로그

로그 내용을 기준으로 경고 알림을 발생시키는 복합 로그 이벤트를 설정합니다.

참고

- 이벤트 설정 시 적정 임계값을 사용하여 불필요한 이벤트 발생을 방지하세요.
- 알림 설정 시 해소 알림(문제 해결 시 알림) 여부도 함께 고려하면 운영 대응에 도움이 됩니다.

공통 기능

모든 이벤트 설정을 **JSON** 또는 **Excel** 형식으로 다운로드할 수 있습니다. 같은 유형의 제품 설정을 공유하면 반복되는 이벤트 설정 작업을 줄일 수 있습니다.

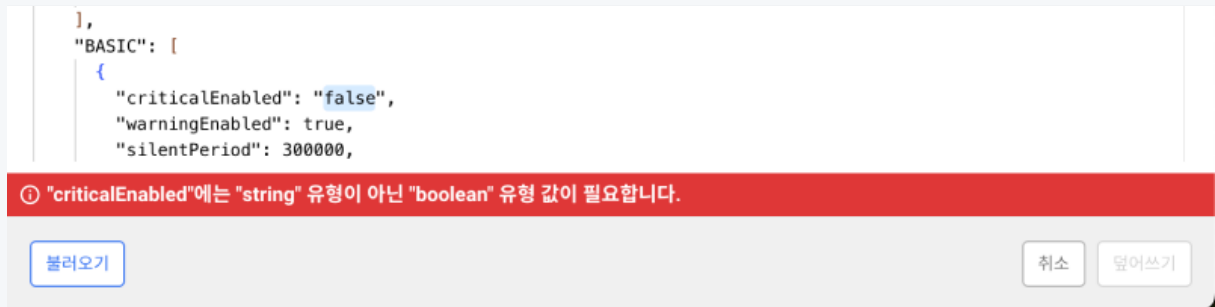
- **JSON 일괄 수정**: 모든 이벤트 조건을 JSON 형식으로 일괄 수정할 수 있습니다.
- **JSON 일괄 다운로드**: 현재 등록된 이벤트 조건을 JSON 파일로 저장할 수 있습니다.
- **Excel 일괄 다운로드**: 이벤트 목록을 Excel 파일로 내려받아 외부 보고나 백업에 활용할 수 있습니다.

JSON 일괄 수정

1. 화면 상단의 [JSON 일괄 수정] 버튼을 클릭하세요.
2. **JSON 일괄 다운로드** 기능을 통해 다운로드 받은 JSON 파일을 가져오거나 직접 수정하세요.
3. [덮어쓰기] 버튼을 클릭해 저장합니다.
4. 확인 메시지가 나타나면 [덮어쓰기] 버튼을 클릭하세요.

! 덮어쓰기 후 이전의 이벤트 설정으로 복구할 수 없습니다.

- `productType` 또는 `platform` 속성의 값을 임의로 수정하면 다른 프로젝트에서 이벤트가 정상 동작하지 않을 수 있습니다.
- JSON 편집창은 JSON 검증(Validation) 기능이 내장되어 있습니다. 형식이나 값이 올바르지 않은 경우, 편집창 아래에 오류 메시지가 표시되며 [덮어쓰기] 버튼은 비활성화됩니다.



JSON 데이터 구조





```
{
  "productType": "{productType}",
  "platform": "{platform}",
  "events": {
    "HITMAP": {
      ...
    },
    "LOG_REALTIME": [
      {...}
    ],
    "METRICS": [
      {...}
    ],
    "COMPOSITE_LOG": [
      {...}
    ],
    "BASIC": [
      {...}
    ],
    "COMPOSITE_METRICS": [
      {...}
    ],
    "ANOMALY": [
      {...}
    ]
  ]
}
```

JSON 필드	설명
productType	제품 타입(예: APM, Infra 등)
platform	플랫폼 정보(예: java, node 등)
events	이벤트 데이터
└ HITMAP	히트맵 패턴

JSON 필드	설명
└ LOG_REALTIME	실시간 로그 이벤트
└ METRICS	메트릭스
└ COMPOSITE_LOG	복합 로그 이벤트
└ BASIC	기본 이벤트
└ COMPOSITE_METRICS	복합 메트릭스
└ ANOMALY	이상치 탐지

JSON 일괄 다운로드

화면 상단의 [JSON 일괄 다운로드] 버튼을 클릭하세요.

- JSON 파일 이름은 `integrated-event-YYYYMMDD.json` 형식입니다.
- JSON 데이터의 구조와 `events` 속성의 하위 속성은 제품(`platform`) 또는 제품 유형(`productType`)에 따라 다를 수 있습니다.

⚠ JSON 데이터의 속성 중 `productType` 또는 `platform` 속성의 값을 임의로 수정하면 다른 프로젝트에서 이벤트가 동작하지 않을 수 있습니다.

Excel 일괄 다운로드

화면 상단의 [Excel 일괄 다운로드] 버튼을 클릭하세요.

메트릭스

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

프로젝트에 설정된 모든 메트릭스 기반 이벤트 목록을 확인할 수 있습니다. 사용자가 설정한 메트릭스 이벤트를 확인, 수정, 삭제하거나, 새로운 이벤트를 추가할 수 있습니다.

기본 옵션

- **이벤트 레벨:** 이벤트의 심각도를 의미하며 정상(Info), 경고(Warning), 위험(Critical) 세 단계로 구분
- **에이전트 중복 알림:** 설정한 시간(30초, 1분, 3분, 5분, 10분)에 같은 이름의 에이전트가 동시에 2개 이상 동작하는 경우, 선택한 시간 동안 이벤트 발생 안함
- **검색:** 이벤트 이름을 기준으로 검색
- **JSON 다운로드/업로드:** 이벤트 규칙은 JSON 편집기를 통해 바로 수정하거나, 파일로 다운로드하여 수정 후 다시 업로드 가능
- **+ 이벤트 추가:** 새로운 메트릭스 이벤트 추가
- **컬럼 크기 조정:** 각 컬럼의 경계를 드래그하여 너비 조정 가능

표 | 메트릭스 이벤트 목록 구성

항목	설명
No.	이벤트의 순번
	이벤트의 활성화 여부 - 활성화: 조건을 충족하면 이벤트 발생 - 비활성화: 이벤트가 동작하지 않으며, 조건을 검사하지 않음
	이벤트 설정 편집 및 삭제
이벤트 이름	사용자가 지정한 이벤트명 - 최대 255자까지 입력 가능
규칙	이벤트 발생 조건

항목	설명
대상	이벤트가 적용되는 모니터링 대상
발생 횟수	이벤트 발생 기준이 되는 기간과 횟수 - 선택한 시간 동안 설정한 횟수만큼 조건을 충족하면 이벤트 발생
일시 중지	이벤트 알림 발생 후, 같은 이벤트 발생을 일정 시간 동안 멈춤 - 선택 가능 시간: 사용 안 함, 5분, 10분, 15분, 20분, 30분, 1시간, 2시간, 3시간, 6시간, 12시간, 1일 - 해소된 알림이 활성화된 경우, 정상(RECOVERED) 상태 알림을 받은 후 선택한 시간 동안 같은 이벤트가 발생해도 알림이 발생하지 않음
해소된 알림	Critical 과 Warning 레벨의 이벤트가 해소되면 RECOVERED(정상) 상태의 알림 수신 여부 - 활성화: 진행 중 → 정상 상태로 전환되면 RECOVERED 알림을 보내고, 이벤트 기록에서 진행 중/해소 상태를 구분해 볼 수 있음 - 비활성화: 임계값을 초과할 때마다 단발성 이벤트 발생
이벤트 수신	해당 이벤트 알림을 받을 사용자 또는 그룹(수신 태그)

이벤트 설정

메트릭스 이벤트는 모니터링 대상에서 발생하는 이벤트를 조건에 따라 정의하고, 효율적으로 알림을 받을 수 있도록 설정할 수 있는 기능을 제공합니다.

이벤트 추가

메트릭스 이벤트를 추가하려면 **이벤트 설정 > 메트릭스** 탭으로 이동한 후, 오른쪽 상단의 [+ 이벤트 추가] 버튼을 클릭하세요.

메트릭스 이벤트 추가 방법
Step 1. 템플릿 선택: 이벤트의 기본 구조를 선택합니다.
Step 2. 이벤트 조건 정의: 이벤트를 어떤 기준으로 발생시킬지 조건을 설정합니다.

메트릭스 이벤트 추가 방법

Step 3. 이벤트 대상 선택: 이벤트가 발생하는 모니터링 대상을 선택합니다.

Step 4. 기본 정보 및 수신 설정: 이벤트 이름 및 메시지, 수신 대상을 설정합니다.

템플릿 선택

1. 이벤트를 어떻게 구성할지에 따라 화면 왼쪽의 3가지 템플릿 중 하나를 선택하세요.

- **새로 만들기:** 카테고리 and 지표를 처음부터 자유롭게 구성할 수 있으며, 복잡한 조건이나 세밀한 모니터링 규칙이 필요한 고급 사용자에게 적합
- **빠른 설정:** 사전 정의된 카테고리, 지표, 기본 임계치가 제공되며, 임계값만 조정하여 빠르게 적용할 수 있어 초급 사용자에게 적합
- **고급 설정:** 사전 정의된 카테고리 and 지표를 기반으로 조건을 추가하거나 자유롭게 변경

① 메트릭스 이벤트에서는 다양한 설정 방식을 지원합니다. 모니터링 플랫폼에 따라 제공하는 템플릿은 다를 수 있습니다.

이벤트 조건 정의

이벤트 조건 정의 단계에서 이벤트가 언제 발생할지 결정하는 지표 설정, 발생 횟수, 일시 중지, 해소된 알림, 이벤트 동작 시간을 설정합니다.

지표 설정

1. 검색창에서 카테고리를 입력하거나, 카테고리 목록에서 카테고리(지표)를 선택하세요.

카테고리를 선택해야 이후 지표 설정을 진행할 수 있습니다.

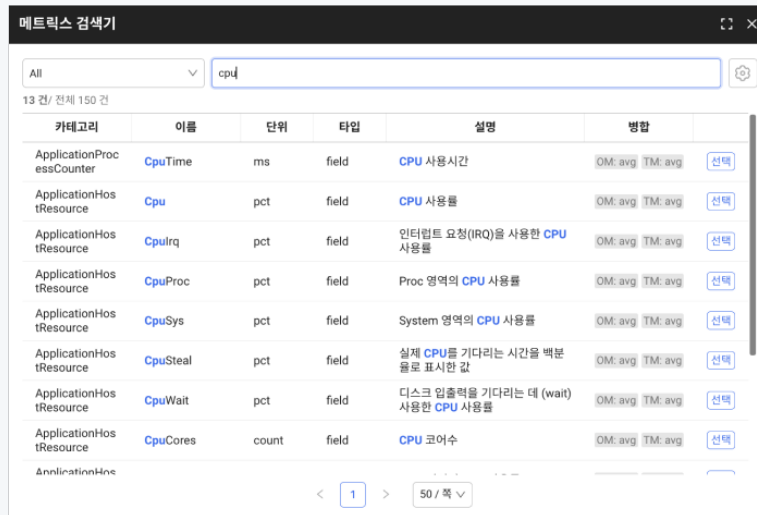
- 카테고리 목록은 카테고리 이름, 데이터 수집 주기, 키를 확인할 수 있습니다. 최근 3시간 동안 프로젝트에서 수집된 메트릭스 데이터가 표시됩니다.

2. 목록에 없는 지표를 사용하려면 **직접 입력하기**를 선택하여 카테고리를 직접 입력하세요.

❗ 카테고리나 지표를 모르는 경우 메트릭스 검색기를 활용하세요.

처음 지표를 설정하는 경우 메트릭스 검색기를 활용하면 더 빠르게 지표를 찾을 수 있습니다.

- 메트릭스 검색기에서 원하는 지표를 검색하면 관련 카테고리나 상세 정보를 확인할 수 있습니다.
- 검색 결과에서 필요한 메트릭스의 [선택] 버튼을 클릭하면, 선택한 값이 이벤트 설정 화면에 자동 반영됩니다.



3. 이벤트 레벨(Critical, Warning, Info)을 선택하세요. 하나의 지표에 여러 레벨을 설정할 수 있습니다.

❗ 이벤트 레벨 동작

여러 조건을 만족하더라도 가장 높은 우선 순위(Critical → Warning → Info)의 레벨만 이벤트가 발생합니다. 레벨 동작 방식은 [레벨 동작 가이드](#)를 참고하세요.

- 이벤트 레벨 수준은 위험(Critical)과 경고(Warning), 정상(Info)으로 구분합니다.
- 같은 지표로 레벨을 설정하고 단계별 임계치를 설정하는 것을 권장합니다.

4. 선택한 이벤트 레벨의 필드, 연산자, 값을 입력하세요.

a. + 추가를 클릭해 조건을 추가할 수 있습니다.

- && : 모든 조건을 동시에 만족해야 이벤트 발생

- **|||** : 하나 이상의 조건만 만족하면 이벤트 발생

b. — 를 클릭하면 해당 조건이 삭제됩니다.

❗ 조건식 작성 방법과 지원되는 연산자는 [조건 설정 가이드](#)를 참고하세요.

발생 횟수

조건이 몇 번 충족되었을 때 이벤트를 발생시킬지 설정합니다. 지속적인 문제만 감지하고 싶을 때 유용합니다.

1. 발생 빈도를 선택하세요.

- **연속**: 설정한 횟수만큼 이벤트가 연속으로 발생하는 경우 이벤트 발생
- **최근**: 선택한 시간 내에 설정한 횟수만큼 이벤트가 발생하는 경우 이벤트 발생
 - 선택 가능 시간: 5초, 10초, 15초, 30초, 1분, 2분, 3분, 4분, 5분, 10분, 30분, 1시간

2. 발생 횟수를 입력하세요.

- **Interval** 값은 선택한 카테고리의 데이터 수집 간격입니다. (Interval: 10s)

일시 중지

과도한 이벤트 발생을 방지하기 위해, 이벤트 동작을 일시 중지할 시간을 선택하세요. 이벤트 발생 후 설정한 시간 동안 동일한 이벤트가 발생하지 않습니다.

- 선택 가능 시간: 사용 안 함, 5분, 10분, 15분, 20분, 30분, 1시간, 2시간, 3시간, 6시간, 12시간, 1일

❗ 해소된 알림 활성화 시

알림은 정상 상태 알림(RECOVERED)을 받은 시점을 기준으로 설정한 시간이 지나기 전까지 동일한 이벤트가 발생해도 알림이 발생하지 않습니다.

해소된 알림

해소된 알림 기능을 활성화하면, 이벤트 발생 이후 상태 변화(진행 중 → 해소됨)를 추적할 수 있습니다. **이벤트 기록** 메뉴에서 진행

중인 이벤트로 표시됩니다.

- 해소된 알림은 **Critical**과 **Warning** 레벨에만 적용되며, Info 레벨은 항상 단발성 이벤트로 동작합니다.
- **Critical**과 **Warning** 레벨의 이벤트가 해소되면, 정상(RECOVERED) 상태의 알림이 전송됩니다.
- 토크 버튼을 클릭해 **활성화** 또는 **비활성화**하세요.
 -  **활성화**: 이벤트는 상태 기반으로 동작하며, 임계치 초과 시 진행 중, 임계치 이하로 복구 시 해소 상태로 전환됨
 -  **비활성화**: 임계값을 초과할 때마다 단발성 이벤트 발생

이벤트 동작 시간

이벤트가 특정 시간대(근무/비근무/점검 시간 등)에 동작하도록 태그를 설정하세요. 태그를 설정하지 않으면 이벤트가 활성화된 상태에서 24시간 상시 동작합니다.

1. **+ 추가**를 클릭하세요.
2. 이벤트 동작 시간에서 **+새로운 태그 생성**을 클릭하세요.
3. **이벤트 동작 시간 태그 생성**에서 **태그 이름, 요일, 시간, 색상**을 선택하고 [적용] 버튼을 클릭하세요.
4. 생성한 태그는 태그 목록에서 확인할 수 있으며, 체크 박스를 선택하면 적용됩니다.
5. 수정 또는 삭제할 태그의  아이콘을 클릭해 **이벤트 동작 시간 태그 수정**에서 태그를 수정하거나 태그 삭제할 수 있습니다.

 태그 삭제 시 해당 태그가 적용된 모든 사용자의 태그가 삭제됩니다. 단, 이벤트 규칙에서 사용 중인 태그는 삭제할 수 없습니다.

시뮬레이션

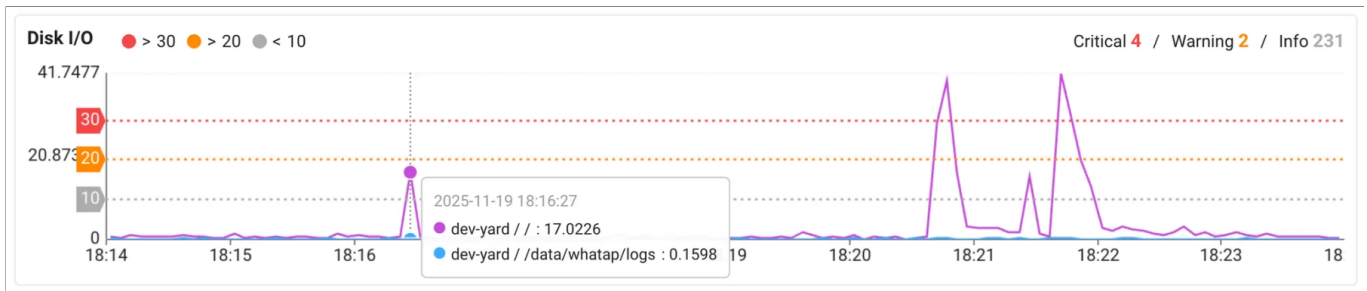
시뮬레이션 기능은 설정한 이벤트 조건을 과거 데이터에 기반으로 사전 테스트 할 수 있습니다. 예상 이벤트 수가 지나치게 많거나 부족하다면 조건을 조정해 최적의 임계값을 찾을 수 있습니다.

- **규칙 검증**: 새로운 이벤트 규칙을 만들었을 때, 과거 데이터에 적용하면 어떤 결과가 나오는지 확인 가능
- **임계값 튜닝**: 이벤트가 자주 발생하거나 전혀 발생하지 않을 때 적절한 수준으로 임계값 조정

시뮬레이션 시작하기

1. 이벤트 조건 설정이 완료되면 [시뮬레이션] 버튼을 클릭하세요.
2. 예상 이벤트 건수와 시각화된 결과를 확인합니다.

시뮬레이션 결과 이해하기



1. 시계열 데이터

지표의 시간대별 변화와 각 레벨의 임계선이 그래프로 표시되어 이벤트 발생 시점을 직관적으로 확인할 수 있습니다.

2. 레벨별 발생 현황

화면 우측에 Critical, Warning, Info 레벨의 이벤트 발생 횟수가 표시됩니다. 전체 이벤트 분포와 빈도를 파악할 수 있습니다.

3. 대상별 상세 정보

차트의 특정 지점에 마우스를 올리면 해당 시점의 정확한 지표 값과 모니터링 대상이 표시됩니다. 여러 대상이 있는 경우 색상으로 구분되며, 대상별 패턴이 다른 경우 필터링 기능을 사용해 개별적으로 분석할 수 있습니다.

4. 피크 구간 식별

그래프에서 지표가 급격히 상승하는 시간을 확인하여 문제가 자주 발생하는 시간대나 패턴을 파악할 수 있습니다.

✓ 시뮬레이션 활용 팁

• 다양한 시간대 시뮬레이션

평일/주말, 피크/비피크 시간대를 각각 시뮬레이션하여 시간대별 최적 임계값을 설정하세요.

• 실제 장애 기간 포함

과거 장애가 발생했던 기간을 포함하여 시뮬레이션을 실행하면 현재 규칙이 장애를 정확히 감지하는지 확인하세요.

• 대상 필터링 추가



모니터링 대상이 많으면 시뮬레이션 결과가 복잡해집니다. 필터링 기능으로 특정 대상만 선택하여 명확한 결과를 확인할 수 있습니다.

- **임계값 단계적 조정**

임계값을 한 번에 크게 변경하기보다 10% 단위로 점진적으로 조정하면서 최적값을 탐색하는 것이 좋습니다.

이벤트 대상 선택

이벤트 대상을 지정하지 않으면, 프로젝트에 포함된 전체 대상으로 이벤트가 발생되어 많은 이벤트가 발생할 수 있습니다. 따라서 이벤트가 적용될 대상을 명확히 설정하는 것을 권장합니다.



이벤트 대상을 변경한 경우, 이벤트 건수가 달라질 수 있습니다. **시뮬레이션** 버튼을 클릭한 후, 다시 실행해 예상 이벤트 수를 확인하세요.

대상 선택

이벤트가 적용될 대상을 **선택 입력** 또는 **직접 입력** 방식으로 지정할 수 있습니다.

- **선택 입력** **직접 입력**

1. 태그, 연산자, 값을 선택 또는 입력하세요. a. 태그를 찾기 어렵다면, **메트릭스 검색기**에서 태그를 검색할 수 있습니다.
2. **+ 추가**를 클릭해 조건(**&&** , **||**)으로 이벤트 대상을 추가하세요.

모니터링할 대상의 태그, 연산자, 값을 직접 입력하세요.

- 직접 입력을 선택하면 입력란 아래에 사용 가능한 태그 목록(**태그 선택 입력**)이 함께 제공됩니다.

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



입력 방법을 변경하면, 작성한 내용이 초기화됩니다.

대상 선택 연산자 목록

선택 입력 방식에서 문자열 태그를 선택하면 연산자 목록에 다음 두 항목이 함께 표시됩니다. 목록에 나타나는 이름은 함수 표기 그대로이며, `startsWith(key, 'match_text')` 와 같은 기존 항목과 형태가 같습니다.

- `equalsIgnoreCase(key, 'match_text')`
- `notEqualsIgnoreCase(key, 'match_text')`

두 연산자는 대소문자를 구분하지 않고 값을 비교합니다. **직접 입력** 방식에서는 같은 함수를 조건식에 직접 작성해 사용할 수 있습니다. 조건식 문법과 지원되는 함수 전체 목록은 [조건 설정 가이드](#)를 참고하세요.

❗ 이벤트 발생 조건과 이벤트 대상 선택은 같은 문법을 사용하므로 두 함수를 양쪽 조건식에 모두 작성할 수 있습니다.

기본 정보 및 수신 설정

이벤트의 이름, 메시지, 수신 대상을 설정합니다. 설정한 내용은 이벤트 기록과 실제 알림 메시지에 그대로 표시되므로, 식별하기 쉽고 명확하게 작성하는 것이 중요합니다.

이벤트 활성화

설정한 조건을 충족했을 때 이벤트 발생 여부를 설정합니다.

-  **활성화**: 설정한 조건을 충족하면 이벤트가 발생됨
-  **비활성화**: 조건을 검사하지 않음

이벤트 이름

이벤트 제목으로 사용될 이벤트 이름을 입력하세요. 설정한 이벤트 이름은 **이벤트 목록** 및 **이벤트 기록** 메뉴에 표시되며, 해당 이름으로 검색할 수 있습니다.

메시지

이벤트 메시지를 입력하세요. 입력한 메시지는 이벤트 기록 및 알림에 사용됩니다. ⓘ을 클릭하면 이전에 작성한 메시지 기록을 확인할 수 있습니다. 메시지에 변수를 사용하여 이벤트 발생 시점의 실제 값을 포함할 수 있습니다.

- **변수 사용 규칙**
 - 변수 형식: `${지표명}`

- 설정한 **카테고리**와 **동일한 카테고리** 내 지표만 변수로 사용할 수 있습니다.
- 여러 변수를 조합해 상세한 메시지를 구성할 수 있습니다.
- 사용 가능한 변수 목록은 **메트릭스 조회** 메뉴에서 확인할 수 있습니다.

• 변수 활용 예시

	이벤트 설정	이벤트 발생 시
제목	Disk 사용량 증가	Disk 사용량 증가
메시지	Disk = \${disk}%	Disk = 89.9%

이벤트 수신

이벤트 알림을 받을 멤버를 지정합니다.

• 전체 수신 태그 선택 수신

프로젝트에서 이벤트 수신 설정이 활성화된 모든 대상(멤버, 채널)에게 알림을 전송합니다.

해당 태그를 가진 프로젝트 멤버에게 알림을 전송합니다.

1. 태그 선택 수신을 선택하세요.
2. 수신 태그 항목에서 [+ 태그 추가] 또는 [+] 버튼을 클릭하세요.
3. 이벤트 수신 태그 창 아래의 + 새 태그 생성을 클릭하세요.
4. 태그 생성 창에서 태그 이름을 입력하고, 색상을 선택한 후, [태그 생성] 버튼을 클릭해 태그를 생성하세요.
5. 생성된 태그는 태그 목록의  아이콘을 클릭해 수정 또는 삭제하세요.
6. 이벤트 수신 태그 창에서 태그 목록에서 원하는 태그를 선택하면 적용됩니다.

❗ 수신 태그

수신자 태그는 알림을 받을 사용자 또는 채널을 그룹 단위로 관리하기 위한 기능입니다. 이벤트에 수신자 태그를 설정하면, 해당 태그가 포함된 사용자에게만 알림이 전달됩니다. 수신 태그를 설정하지 않으면 프로젝트 내 모든 사용자에게 알림이 전송됩니다.

이벤트 수정/삭제

1. 경고 알림 > 이벤트 설정의 메트릭스 탭으로 이동하세요.
2. 이벤트 목록에서 수정 또는 삭제하려는 이벤트의  아이콘을 클릭하세요.
3. 이벤트 규칙 수정 창에서 옵션을 수정하고, [저장] 버튼을 클릭하세요.
 - a. 선택한 이벤트를 삭제하려면 이벤트 규칙 수정 창의 오른쪽 위의 [삭제] 버튼을 클릭하세요.

이벤트 공유

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

- JSON 파일명: event-rules-YYYYMMDD.json

내보내기

1. 화면 오른쪽 위에 [JSON ] 버튼을 클릭하세요.
2. JSON 편집 창이 나타나면 [ 내보내기] 버튼을 클릭하세요.
 - 이벤트를 검색 후 내보내기 기능을 이용하면 검색한 목록만 JSON 파일로 다운받을 수 있습니다.
3. JSON 파일이 다운로드되면 공유할 다른 사용자에게 전달하세요.

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.

 같은 종류의 제품 간에 이용할 것을 권장합니다. 다른 제품의 프로젝트로부터 이벤트 설정을 가져올 수는 있지만 정상 작동하지 않습니다.

Json 형식으로 수정하기

1. 화면 오른쪽 위에 [JSON ] 버튼을 클릭하세요.
2. 편집 창이 나타나면 JSON 형식에 맞춰 내용을 수정하세요.
3. 수정을 완료하면 화면 아래 [저장] 버튼을 선택하세요.

❗ 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 데이터 구조

```
{
  "version": 2,
  "eventId": "zcef7s7f27rum1",
  "enabled": true,
  "stateful": false,
  "title": "Active Transaction",
  "message": "Active Transaction = ${active_tx_count}",
  "category": "app_counter",
  "alertLabel": [
    "oid"
  ],
  "repeatCount": 1,
  "repeatDuration": 0,
  "silent": 300000,
  "receiver": [],
  "timeTag": [],
  "selectString": "",
  "conditions": [
    {
      "level": 20,
      "enabled": true,
      "rule": "active_tx_count > 100"
    }
  ]
}
```

```

    }
  ],
  "createTime": 1763632674345,
  "lastModifiedTime": 1763632674347,
  "lastModifiedUser": "support@whatap.io",
  "basic": true,
  "metaId": "java004",
  "selectCondition": {
    "oid": [
      "-1010758404",
      "-250906941"
    ]
  }
}

```

표 | JSON 데이터 구조

JSON 필드	타입	설명	비고
version	Integer	이벤트 규칙의 버전	변경 제한
eventId	String	이벤트 규칙의 고유 식별자	
enabled	boolean	이벤트 활성화 여부	
stateful	boolean	상태 기반 이벤트 여부	
title	String	사용자가 설정한 이벤트 규칙 이름	
message	String	사용자가 설정한 이벤트 규칙 메시지	
category	String	데이터 카테고리	
alertLabel	List<String>	이벤트의 상태 관리를 위해 카테고리마다 지정되는 기본 식별자(primary key) 값	변경 제한
repeatCount	Integer	반복 횟수	
repeatDuration	Long	반복 기간	

JSON 필드	타입	설명	비고
silent	Integer	일시 중지 시간	
receiver	List<String>	수신자 태그의 키값 목록	
timeTag	List<String>	동작시간 태그의 키값 목록	
selectString	String	대상 선택	
conditions	List<Object>	레벨별 발생 조건 목록	
└ level	byte	레벨 값	Critical : 30 Warning : 20 Info : 10
└ enabled	boolean	레벨 활성화 여부	
└ rule	String	레벨 발생 조건	
createTime	Long	이벤트 규칙 최초 생성 시간	
lastModifiedTime	Long	이벤트 규칙 마지막 수정 시간	
lastModifiedUser	String	이벤트 규칙 마지막 수정 계정	
basic	boolean	빠른 설정으로 생성한 이벤트 여부	변경 제한
metaId	String	빠른 설정 템플릿 고유 식별자	변경 제한: 이 값은 빠른 설정으로 생성한 이벤트에만 존재합니다. (basic=true)
selectCondition	Object	빠른 설정 대상 선택값	이 값은 빠른 설정으로 생성한 이벤트에만 존재합니다. (basic=true)

❗ '변경 제한'으로 표시된 필드는 이벤트 동작에 영향을 줄 수 있으므로 값을 변경하지 않는 것을 권장합니다.

부록

발생 조건, 대상 선택 가이드

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

레벨 동작 가이드

이벤트 레벨은 위험(Critical)과 경고(Warning), 정상(Info)으로 구분합니다.

1. 우선순위 기반 이벤트 발생

여러 레벨의 조건을 동시에 충족할 경우, 가장 높은 우선순위의 이벤트만 발생합니다.

예시

설정:

- Warning: CPU > 70%

- Critical: CPU > 90%

현재 상태: CPU 95%

→ 결과: Critical 이벤트만 발생 (Warning은 억제됨)

2. 레벨 상승

진행중 상태를 갖는 이벤트에서 낮은 레벨 이벤트가 진행 중일 때 높은 레벨 조건을 충족하면, 두 레벨 모두 진행 중 상태가 됩니다.

예시

설정:

- Warning: CPU > 70%

- Critical: CPU > 90%

시나리오:

1) CPU 80% → Warning 발생 (진행 중)

2) CPU 95% → Warning (진행 중), Critical (진행 중)

3. 레벨 하강

진행중 상태를 갖는 이벤트에서 높은 레벨에서 낮은 레벨로 전환되면 높은 레벨은 해소되고 낮은 레벨이 유지됩니다.

예시

설정:

- Warning: CPU > 70%

- Critical: CPU > 90%

시나리오:

1) CPU 97% → Critical 발생

2) CPU 85% → Critical 해소, Warning 유지

3) CPU 65% → Warning 해소

4. 동작 흐름도

- Warning: CPU > 70%

- Critical: CPU > 90%

메트릭 값: 60% → 75% → 92% → 85% → 60%

상태:	정상	Warning (발생)	Critical (발생)	Warning (유지)	정상 (해소)
			Warning (유지)		

ⓘ 진행 중 상태를 갖는 이벤트는 조건이 충족되는 동안 계속 활성화 상태를 유지하며, 조건이 해제될 때까지 지속됩니다.

조건 설정 가이드

ⓘ 지표명이 숫자로 시작하거나 특수문자가 포함된 경우 \${지표명} 형태로 작성해야 합니다.

- 괄호 (), []



- 연산자 `+`, `-`, `*`, `/`, `%`
- 구분자 `:`, `@`, `#`, `,`, `,` (공백)
- 기타 특수문자 `!`, `^`, `&`, `|`, `~`, ```, `=`

`${}` 사용 예시:

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

`${}` 없이 사용 가능: 영문자, 언더스코어(`_`), 점(`.`)만 포함된 경우

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

1. 비교 연산자

숫자 비교

```
크다:      cpu > 80
크거나 같다:  cpu >= 80
작다:      memory < 1000
작거나 같다:  memory <= 1000
같다:      status == 200
같지 않다:   error != 0
```

문자열 비교

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

2. 산술 연산자

- 기본 산술 연산

```
덧셈:  cpu + 10 >= 90
뺄셈:  memory - 100 >= 500
곱셈:  cpu * 2 >= 100
나눗셈: disk / 1024 >= 100
나머지: value % 10 == 0
```

- 괄호를 이용한 우선순위 제어

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

- 음수 표현

```
cpu > -100
```

3. 논리 연산자

- AND 연산 (&&)

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

- OR 연산 (||)

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

- 복합 논리 연산

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

4. 패턴 매칭 연산자

- LIKE 연산자

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

- NOT LIKE 연산자

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

5. 내장 함수

- Null 체크 함수

```
isNull(value)      # null인지 확인
isNotNull(value)   # null이 아닌지 확인
nvl(value, 0)      # null이면 기본값 반환
isEmpty(str)       # 빈 문자열인지 확인
isNotEmpty(str)    # 빈 문자열이 아닌지 확인
```

- 집계 함수

```
sum(cpu, memory, disk)    # 합계
avg(cpu, memory)          # 평균
max(cpu, memory, disk)    # 최대값
min(cpu, memory, disk)    # 최소값
count(value1, value2, value3) # 개수
```

- 수학 함수

```
round(cpu, 2)            # 반올림 (소수점 2자리)
```

- 문자열 함수

```
length(str)             # 문자열 길이
startsWith(str, 'prefix') # 접두사 확인
```

```
endsWith(str, 'suffix') # 접미사 확인
indexOf(str, 'search') # 문자열 위치
substring(str, 0, 10) # 부분 문자열
trim(str) # 공백 제거
replace(str, 'old', 'new') # 문자열 치환
hasStr(str, 'search') # 문자열 포함 여부
```

문자열 함수

```
equalsIgnoreCase(str, 'match_text') # 대소문자를 구분하지 않는 일치 비교
notEqualsIgnoreCase(str, 'match_text') # 대소문자를 구분하지 않는 불일치 비교
```

`==` 와 `!=` 는 대소문자를 구분하므로 `WebServer` 와 `webserver` 를 다른 값으로 판단합니다. 표기가 일정하지 않은 태그나 필드를 비교할 때 위 두 함수를 사용하면 대소문자 차이를 무시하고 값을 맞출 수 있습니다.

예시

```
equalsIgnoreCase(ocindName, 'WebServer')
notEqualsIgnoreCase(container, 'PROD.billing')
```

이벤트 발생 조건과 이벤트 대상 선택은 같은 문법을 사용하므로 두 함수를 양쪽 조건식에 모두 작성할 수 있습니다.

- 조건 함수

- **if:** 조건식이 참(`true`)이면 `true값` 을 반환하고, 거짓(`false`)이면 `false값` 을 반환하는 조건 함수

형식

```
if(조건, true값, false값)
```

예시

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

- **decode:** 값과 조건을 비교하여 일치하는 조건의 결과를 반환, 없으면 기본값 반환

형식

```
decode(값, 조건1, 결과1, 조건2, 결과2, ..., 조건N, 결과N, 기본값)
```

예시

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

- **in:** 값이 지정한 후보값 중 하나와 일치하면 `true` , 아니면 `false`

형식

```
in(값, 후보값1, 후보값2, ..., 후보값N)
```

예시

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

❗ 작성 시 주의사항

- 권장사항
 - 간단한 변수명은 `${}` 없이 사용 (예: `cpu`, `memory`)
 - 특수문자 포함 시 반드시 `${}` 사용
 - 복잡한 연산은 괄호로 명확하게 구분
 - 함수명은 정확히 입력 (대소문자 구분)
- 피해야 할 사항
 - 불완전한 표현식 작성 (예: `cpu > , memory && )`
 - 괄호 미스매칭 (예: `(cpu > 80 && cpu > 70) )`
 - 연속된 연산자 사용 (예: `cpu >> 80 , cpu >< 80 )`

복합 메트릭스

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

복잡한 규칙을 활용해 이벤트를 생성하고 경고 알림을 보낼 수 있습니다.

기본 옵션

- **검색:** 이벤트 이름 또는 이벤트 수신 태그를 선택해 원하는 이벤트 검색
- **JSON 다운로드/업로드:** 이벤트 규칙은 JSON 편집기를 통해 바로 수정하거나, 파일로 다운로드하여 수정 후 다시 업로드 가능
- **알림 메시지 설정:** 수신할 메시지의 상세 항목 선택 및 항목 별 내용 편집
- **+이벤트 추가:** 새로운 복합 메트릭스 이벤트 추가

! 권한

복합 메트릭스 이벤트를 설정하려면 **알림 설정** 권한이 있어야 합니다. 알림 설정 권한은 **홈 > 프로젝트 선택 > 관리 > 통합 멤버 관리**에서 권한을 부여할 멤버의  아이콘을 클릭해 설정할 수 있습니다.

표 | 복합 메트릭스 이벤트 목록 구성

항목	설명
이벤트 제목	사용자가 지정한 이벤트명 - 최대 255byte까지 입력 가능
조건	이벤트 발생 조건
이벤트 상태가 해소되면 추가 알림	Critical 과 Warning 레벨의 이벤트가 해소되면 RECOVERED(정상) 상태의 알림 수신 여부 - 활성화: 진행 중 → 정상 상태로 전환되면 RECOVERED 알림을 보내고, 이벤트 기록에서 진행 중/해소 상태를 구분해 볼 수 있음 - 비활성화: 임계값을 초과할 때마다 단발성 이벤트 발생
이벤트 수신 태그	해당 이벤트 알림을 받을 사용자 또는 그룹(수신 태그)

항목	설명
	이벤트 수정 및 삭제
	이벤트의 활성화 여부 - 활성화: 조건을 충족하면 이벤트 발생 - 비활성화: 이벤트가 동작하지 않으며, 조건을 검사하지 않음

이벤트 설정

복합 메트릭스 이벤트는 메트릭스 데이터 질의 언어인 **MXQL**을 기반으로 이벤트 조건을 생성합니다. **차트로** 생성하기 기능은 **MXQL**의 자동완성을 위한 콤보박스 기능을 제공합니다.

이벤트 추가

- 🔔 경고 알림 > 이벤트 설정에서 복합 메트릭스 탭을 클릭하세요.
- 화면 오른쪽의 [+ 이벤트 추가] 버튼을 클릭하세요.
- 복합 메트릭스 창에서 차트로 생성하기를 클릭하세요.
 - 제공하는 템플릿을 활용할 수 있습니다.
- 이벤트 설정 화면에서 먼저 이벤트 데이터를 조회하고, 이벤트 조건을 설정하세요.

이벤트 데이터 조회

이벤트 데이터를 조회하여 차트를 구성합니다. 이벤트 설정 화면의 오른쪽 이벤트 데이터 조회의 위젯 또는 텍스트 옵션을 선택해 이벤트를 설정하세요.

• 위젯 텍스트

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

- 데이터를 조회할 날짜를 선택하세요.
- 데이터를 조회할 카테고리(대상)를 선택하세요.
- 필터 항목의 + 필터 추가를 클릭해 이벤트 조건을 생성하세요.

- a. 필터 창에서 연산식, 태그, 필터 값을 선택하세요.
 - b. + 추가를 클릭해 조건을 추가할 수 있습니다.
 - c. 조건을 삭제하고 싶다면 조건 옆의 - 를 클릭하세요.
4. 그룹화 항목에서 그룹화된 메트릭스 데이터를 선택하세요. 다중 선택할 수 있습니다.
 5. 타임 유닛 항목에서 초, 분, 시간 단위로 그룹화된 데이터를 나눌 시간 기준을 설정하세요.
 6. 필드 항목에서 이벤트 발행 조건에 사용할 필드를 선택하세요. 다중 선택할 수 있습니다.

❗ 텍스트 모드로 입력한 mxql은 위젯 모드와 호환되지 않습니다.

MXQL을 그대로 수정할 수 있는 편집창이 나타납니다.

1. MXQL을 직접 수정하고 조회 버튼을 클릭하세요.
2. 날짜를 선택하면 해당 내역을 차트 또는 그래프로 확인할 수 있습니다.

알림

경고 알림 설정의 기본 정보를 입력합니다.

- **이벤트 활성화:** 토글 버튼을 활성화하면 이벤트가 동작합니다.
- **레벨:** 이벤트 레벨(Critical, Warning, Info)을 선택하세요.
 - **이벤트 상태가 해소되면 추가 알림:** 토글 버튼을 활성화하면 이벤트가 해소되어 정상(RECOVERED) 상태의 알림이 전송됩니다.
- **제목:** 이벤트 규칙의 제목을 입력하세요.
- **메시지:** 이벤트 발생 시 전달받을 알림 메시지의 내용을 입력하세요. 메시지에 변수를 사용하여 이벤트 발생 시점의 실제 값을 포함할 수 있습니다.

An event has occurred [\${pcode}] [\${oname}] [\${okindName}] [\${host_ip}] [\${type}]

Event Message

An event has occurred [8] [java-demo9] [dev-okind-1] [10.21.1.26] [java]

✓ 변수 사용 규칙

- 변수 형식: \${지표명}
- 설정한 **카테고리**와 **동일한 카테고리** 내 지표만 변수로 사용 가능합니다.
- 여러 변수를 조합해 상세한 메시지를 구성할 수 있습니다.
- 사용 가능한 변수 목록은 **메트릭스 조회**에서 확인할 수 있습니다.

이벤트 발행 조건

- **데이터 조회 범위:** 실시간 데이터 조회 범위를 선택하세요.
 - 조회 가능 범위: 30초, 1분, 2분, 5분, 10분, 30분, 1시간, 2시간, 3시간
- **조건:** 이벤트 발생 조건을 입력하세요. 이벤트 데이터 조회에 포함된 필드만 사용할 수 있습니다.

부가정보

- **인터벌:** 선택한 시간(1분, 5분, 10분, 30분, 1시간, 12시간) 간격으로 알림 조건을 확인합니다.
- **무음:** 이벤트가 발생한 후, 선택한 시간(unset, 1분, 5분, 10분, 30분, 1시간, 12시간) 동안 같은 이벤트가 발생되지 않습니다.
- **이벤트 동작 시간:** 이벤트가 특정 시간대(근무/비근무/점검 시간 등)에 동작하도록 태그를 설정하세요. 태그를 설정하지 않으면 이벤트가 활성화된 상태에서 24시간 상시 동작합니다.
 1. + 추가를 클릭하세요.
 2. 이벤트 동작 시간에서 + 새로운 태그 생성을 클릭하세요.
 3. 이벤트 동작 시간 태그 생성에서 태그 이름, 요일, 시간, 색상을 선택하고 [적용] 버튼을 클릭하세요.
 4. 생성한 태그는 태그 목록에서 확인할 수 있으며, 체크 박스를 선택하면 적용됩니다.
 5. 수정 또는 삭제할 태그의  아이콘을 클릭해 이벤트 동작 시간 태그 수정에서 태그를 수정하거나 태그 삭제할 수 있습니다.

 태그 삭제 시 해당 태그가 적용된 모든 사용자의 태그가 제거됩니다. 단, 이벤트 규칙에서 사용 중인 태그는 삭제할 수 없습니다.

- **이벤트 수신 태그:** 이벤트에 수신 태그를 설정하면, 해당 태그를 가진 프로젝트 멤버에게 알림을 전송합니다. 수신 태그를

설정하지 않으면 프로젝트 내 모든 사용자에게 알림이 전송됩니다.

1. + 태그 추가 또는 +를 클릭하세요.
2. 이벤트 수신 태그 창 아래의 + 새 태그 생성을 클릭하세요.
3. 태그 생성 창에서 태그 이름을 입력하고 색상을 선택한 후, [태그 생성] 버튼을 클릭해 태그를 생성하세요.
4. 생성된 태그는 태그 목록의  아이콘을 클릭해 수정 또는 삭제하세요.
5. 이벤트 수신 태그 창에서 태그 목록에서 원하는 태그를 선택하면 적용됩니다.

✔ 이벤트 설정 시 이벤트 수신 태그를 선택하여 해당 태그를 가진 프로젝트 멤버와 3rd-party 플러그인에 알림을 전송할 수 있습니다. 경고 알림 > 이벤트 수신 설정에서 프로젝트 멤버와 3rd-party 플러그인에 각각 태그를 지정할 수 있습니다.

이벤트 규칙 테스트

설정한 조건을 과거 데이터에 기반으로 테스트를 진행해, 몇 건의 이벤트가 발생할지 예측할 수 있습니다.

1. 이벤트 규칙을 테스트할 날짜를 선택하고 [확인] 버튼을 클릭하세요.
2. [실행] 버튼을 클릭해 이벤트 발생 건수를 확인하세요.

이벤트 수정/삭제

1. 경고 알림 > 이벤트 수신 설정의 복합 메트릭스 탭으로 이동하세요.
2. 복합 메트릭스 목록에서 수정 또는 삭제하려는 이벤트의  아이콘을 클릭하세요.
3. 이벤트 수신 설정 화면에서 옵션을 수정하고, [저장] 버튼을 클릭하세요.
 - a. 선택한 이벤트를 삭제하려면 이벤트 수신 설정 화면의 오른쪽 위의 [삭제] 버튼을 클릭하세요.

이벤트 공유

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

- JSON 파일명: event-rules- YYYYMMDD .json

내보내기

1. 화면 오른쪽 위에 [JSON ] 버튼을 클릭하세요.
2. JSON 편집 창이 나타나면 [ 내보내기] 버튼을 클릭하세요.
 - 이벤트를 검색 후 내보내기 기능을 이용하면 검색한 목록만 JSON 파일로 다운받을 수 있습니다.
3. JSON 파일이 다운로드되면 공유할 다른 사용자에게 전달하세요.

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.

 같은 종류의 제품 간에 이용할 것을 권장합니다. 다른 제품의 프로젝트로부터 이벤트 설정을 가져올 수는 있지만 정상 작동하지 않습니다.

Json 형식으로 수정하기

1. 화면 오른쪽 위에 [JSON ] 버튼을 클릭하세요.
2. 편집 창이 나타나면 JSON 형식에 맞춰 내용을 수정하세요.
3. 수정을 완료하면 화면 아래 [저장] 버튼을 선택하세요.

 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)

알림 메시지 설정

수신할 메시지의 상세 항목을 선택하고, 항목별 내용을 편집할 수 있습니다.

부록

MXQL 문법 가이드

복합 매트릭스는 MXQL 쿼리를 기반으로 동작합니다. 자세한 문법은 [MXQL 문법 가이드](#)를 참고하시기 바랍니다.

실시간 로그 이벤트

홈 > 프로젝트 선택 >  경고 알림 > 이벤트 설정 > 실시간 로그 탭

수집한 로그 데이터를 조건에 맞춰 필터링하려 경고 알림을 설정할 수 있습니다. 로그 이벤트를 사용하려면 로그 모니터링이 활성화되어야 합니다. **로그 모니터링 활성화**에 대한 자세한 내용은 각 제품 로그 문서를 참고하세요.

- **실시간 로그 이벤트:** 실시간으로 수집한 로그에서 설정한 이벤트 조건이 충족되면 이벤트가 발생합니다.

기본 옵션

- **검색:** 이벤트 이름 또는 이벤트 수신 태그를 선택해 원하는 이벤트 검색
- **JSON 다운로드/업로드:** 이벤트 규칙은 JSON 편집기를 통해 바로 수정하거나, 파일로 다운로드하여 수정 후 다시 업로드 가능
- **알림 메시지 설정:** 수신할 메시지의 상세 항목 선택 및 항목 별 내용 편집
- **+ 이벤트 추가:** 새로운 로그 이벤트 추가

표 | 실시간 로그 이벤트 목록 구성

항목	설명
이벤트 이름	알림 제목으로 사용되는 이벤트 이름 - 최대 255byte까지 입력 가능
카테고리	로그 구분 명칭(로그 폴더명)
검색 키	로그 데이터에서 찾고 싶은 항목 - 예: HTTP 응답 상태 코드를 나타내는 값에 접근하고자 할 경우 검색 키 <code>status</code>
검색 값	검색 키에 해당하는 실제 데이터로 로그에서 입력한 단어를 포함할 경우 경고 알림을 보냄 - 예: 검색 키 <code>status</code> 검색 값 <code>200</code> 을 설정한 경우 HTTP 응답 상태 코드 200을 포함하는 로그 데이터 수집 시 경고 알림 발생
이벤트 발생 일시 중지	이벤트 알림 발생 후, 같은 이벤트 발생을 일정 시간 동안 멈춤 - 선택 가능 시간: 사용 안 함, 5분, 10분, 15분, 20분, 30분, 1시간, 2시간, 3시간, 6시간, 12시간, 1일 - 해소된 알림이 활성화된 경우, 정상(RECOVERED) 상태 알림을 받은 후 선택한 시간 동안 같은 이벤트가

항목	설명
	발생해도 알림이 발생하지 않음
이벤트 대상 필터링	이벤트가 적용될 대상의 조건 - 대상 조건을 설정하지 않으면 수집되는 모든 데이터에 대해 알림 여부 판단 - 선택 입력: 태그, 연산자, 값을 선택해 조건 구성 - 직접 입력: 조건을 직접 입력해 대상 지정
이벤트 수신 태그	해당 이벤트 알림을 받을 사용자 또는 그룹(수신 태그)
	이벤트 수정 및 삭제
	이벤트의 활성화 여부 - 활성화: 조건을 충족하면 이벤트 발생 - 비활성화: 이벤트가 동작하지 않으며, 조건을 검사하지 않음

이벤트 설정

로그 이벤트는 실시간 로그 또는 일정 조건을 만족하는 로그가 누적될 때 경고 알림을 설정할 수 있는 기능입니다.

실시간 로그 이벤트 추가

1. 경고 알림 > 이벤트 설정의 실시간 로그 탭을 클릭하세요.
2. 화면 오른쪽의 [+ 이벤트 추가] 버튼을 클릭하세요.
3. 이벤트 규칙 추가 창에서 로그 이벤트 조건을 설정하세요.
 - **이벤트 이름:** 이벤트 제목으로 사용할 이름을 입력하세요.
 - **이벤트 활성화:** 토글 버튼 활성화 시, 토글 버튼 활성화 시, 조건을 충족하면 이벤트 발생합니다.
 - **레벨:** 이벤트 레벨(Critical, Warning, Info)을 선택하세요.
 - **메시지:** 이벤트 발생 시 전달받을 알림 메시지를 입력하세요. 메시지에 변수를 사용하여 이벤트 발생 시점의 실제 값을 포함할 수 있습니다.

✓ 변수 사용 규칙

- 변수 형식: \${지표명}
- 설정한 **카테고리**와 **동일한 카테고리** 내 지표만 변수로 사용할 수 있습니다.
- 여러 변수를 조합해 상세한 메시지를 구성할 수 있습니다.
- 사용 가능한 변수 목록은 **메트릭스 조회**에서 확인할 수 있습니다.

- **카테고리**: 로그 구분 명칭(로그 폴더명)을 목록에서 선택하거나 직접 입력하세요. 카테고리를 선택해야 검색 키와 검색 값을 입력할 수 있습니다.
- **검색 키**: 로그 데이터에서 찾고 싶은 항목을 입력하세요.
 - 예: HTTP 응답 상태 코드를 나타내는 값에 접근하고자 할 경우 **검색 키** status
- **검색 값**: 검색 키에 해당하는 실제 데이터를 입력하세요. 로그에서 입력한 단어를 포함할 경우 경고 알림을 보냅니다.
 - 예: **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**: 이벤트가 적용될 대상의 조건을 입력하세요. 입력값이 없으면, 수집되는 모든 데이터에 대해 알림 여부 판단합니다.
 - **선택 입력**: 태그, 연산자, 값을 선택해 대상 조건을 설정하세요.

❗ 조건식 작성 방법과 지원되는 연산자는 [조건 설정 가이드](#)를 참고하세요.

- **직접 입력**: 조건을 직접 입력하세요.
- **이벤트 발생 일시 중지**: 알림을 일시 중지할 시간을 선택하세요. 이벤트 발생 후 설정한 시간 동안 동일한 이벤트가 발생하지 않습니다.
 - 선택 가능 시간: 사용 안 함 , 1분 , 2분 , 3분 , 5분 , 10분 , 20분 , 30분 , 1시간 , 3시간 , 6시간 , 12시간
- **이벤트 동작 시간**: 이벤트가 특정 시간대(근무/비근무/점검 시간 등)에 동작하도록 태그를 설정하세요. 태그를 설정하지 않으면 이벤트가 활성화된 상태에서 24시간 상시 동작합니다.

1. + 추가를 클릭하세요.
2. 이벤트 동작 시간에서 +새로운 태그 생성을 클릭하세요.
3. 이벤트 동작 시간 태그 생성에서 태그 이름, 요일, 시간, 색상을 선택하고 [적용] 버튼을 클릭하세요.
4. 생성한 태그는 태그 목록에서 확인할 수 있으며, 체크 박스를 선택하면 적용됩니다.
5. 수정 또는 삭제할 태그의  아이콘을 클릭해 이벤트 동작 시간 태그 수정에서 태그를 수정하거나 태그 삭제할 수 있습니다.

 태그 삭제 시 해당 태그가 적용된 모든 사용자의 태그가 제거됩니다. 단, 이벤트 규칙에서 사용 중인 태그는 삭제할 수 없습니다.

- **이벤트 수신 태그:** 이벤트에 수신 태그를 설정하면, 해당 태그를 가진 프로젝트 멤버에게 알림을 전송합니다. 수신자 태그를 설정하지 않으면 프로젝트 내 모든 사용자에게 알림이 전송됩니다.

1. + 태그 추가 또는 +를 클릭하세요.
2. 이벤트 수신 태그 창 아래의 + 새 태그 생성을 클릭하세요.
3. 태그 생성 창에서 태그 이름을 입력하고, 색상을 선택한 후, [태그 생성] 버튼을 클릭해 태그를 생성하세요.
4. 생성된 태그는 태그 목록의  아이콘을 클릭해 수정 또는 삭제하세요.
5. 이벤트 수신 태그 창의 태그 목록에서 원하는 태그를 선택하면 적용됩니다.

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

4. 이벤트 규칙 추가 창에서 설정이 완료되면 [저장] 버튼을 클릭하세요.

이벤트 수정/삭제

1. 경고 알림 > 이벤트 설정의 실시간 로그 탭으로 이동하세요.

2. 로그 이벤트 목록에서 수정 또는 삭제하려는 이벤트의  아이콘을 클릭하세요.
3. **이벤트 설정** 화면에서 옵션을 수정하고, [저장] 버튼을 클릭하세요.
 - a. 선택한 이벤트를 삭제하려면 **이벤트 설정** 화면의 오른쪽 위의 [삭제] 버튼을 클릭하세요.

이벤트 공유

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

- JSON 파일명: `event-rules-YYYYMMDD.json`

내보내기

1. 화면 오른쪽 위에 [JSON ] 버튼을 클릭하세요.
2. JSON 편집 창이 나타나면 [ 내보내기] 버튼을 클릭하세요.
 - 이벤트를 검색 후 내보내기 기능을 이용하면 검색한 목록만 JSON 파일로 다운받을 수 있습니다.
3. JSON 파일이 다운로드되면 공유할 다른 사용자에게 전달하세요.

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.

 같은 종류의 제품 간에 이용할 것을 권장합니다. 다른 제품의 프로젝트로부터 이벤트 설정을 가져올 수는 있지만 정상 작동하지 않습니다.

Json 형식으로 수정하기

1. 화면 오른쪽 위에 [JSON ] 버튼을 클릭하세요.
2. 편집 창이 나타나면 JSON 형식에 맞춰 내용을 수정하세요.

- 수정을 완료하면 화면 아래 [저장] 버튼을 선택하세요.

❗ 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)

부록

발생 조건, 대상 선택 가이드

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

레벨 동작 가이드

이벤트 레벨은 위험(Critical)과 경고(Warning), 정상(Info)으로 구분합니다.

1. 우선순위 기반 이벤트 발생

여러 레벨의 조건을 동시에 충족할 경우, 가장 높은 우선순위의 이벤트만 발생합니다.

예시

설정:

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

현재 상태: CPU 95%

→ 결과: Critical 이벤트만 발생 (Warning은 억제됨)

2. 레벨 상승

진행중 상태를 갖는 이벤트에서 낮은 레벨 이벤트가 진행 중일 때 높은 레벨 조건을 충족하면, 두 레벨 모두 진행 중

상태가 됩니다.

예시

설정:

- Warning: CPU > 70%

- Critical: CPU > 90%

시나리오:

1) CPU 80% → Warning 발생 (진행 중)

2) CPU 95% → Warning (진행 중), Critical (진행 중)

3. 레벨 하강

진행중 상태를 갖는 이벤트에서 높은 레벨에서 낮은 레벨로 전환되면 높은 레벨은 해소되고 낮은 레벨이 유지됩니다.

예시

설정:

- Warning: CPU > 70%

- Critical: CPU > 90%

시나리오:

1) CPU 97% → Critical 발생

2) CPU 85% → Critical 해소, Warning 유지

3) CPU 65% → Warning 해소

4. 동작 흐름도

- Warning: CPU > 70%

- Critical: CPU > 90%

메트릭 값: 60% → 75% → 92% → 85% → 60%

상태:	정상	Warning	Critical	Warning	정상
		(발생)	(발생)	(유지)	(해소)

Warning
(유지)

⚠ 진행 중 상태를 갖는 이벤트는 조건이 충족되는 동안 계속 활성화 상태를 유지하며, 조건이 해제될 때까지 지속됩니다.

조건 설정 가이드

⚠ 지표명이 숫자로 시작하거나 특수문자가 포함된 경우 `${지표명}` 형태로 작성해야 합니다.

- 괄호 `()`, `[]`
- 연산자 `+`, `-`, `*`, `/`, `%`
- 구분자 `:`, `@`, `#`, `,`, `,` (공백)
- 기타 특수문자 `!`, `^`, `&`, `|`, `~`, `"`, `=`

`${}` 사용 예시:

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

`${}` 없이 사용 가능: 영문자, 언더스코어(`_`), 점(`.`)만 포함된 경우

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

1. 비교 연산자

숫자 비교

```
크다:      cpu > 80
크거나 같다:  cpu >= 80
작다:      memory < 1000
작거나 같다:  memory <= 1000
같다:      status == 200
```

```
같지 않다: error != 0
```

문자열 비교

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

2. 산술 연산자

- 기본 산술 연산

```
덧셈: cpu + 10 >= 90
뺄셈: memory - 100 >= 500
곱셈: cpu * 2 >= 100
나눗셈: disk / 1024 >= 100
나머지: value % 10 == 0
```

- 괄호를 이용한 우선순위 제어

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

- 음수 표현

```
cpu > -100
```

3. 논리 연산자

- AND 연산 (&&)

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

- OR 연산 (||)

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

- 복합 논리 연산

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

4. 패턴 매칭 연산자

- LIKE 연산자

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

- NOT LIKE 연산자

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

5. 내장 함수

- Null 체크 함수

isNull(value)	# null인지 확인
isNotNull(value)	# null이 아닌지 확인
nvl(value, 0)	# null이면 기본값 반환
isEmpty(str)	# 빈 문자열인지 확인
isNotEmpty(str)	# 빈 문자열이 아닌지 확인

- 집계 함수

sum(cpu, memory, disk)	# 합계
avg(cpu, memory)	# 평균
max(cpu, memory, disk)	# 최대값

```
min(cpu, memory, disk)      # 최소값
count(value1, value2, value3) # 개수
```

- 수학 함수

```
round(cpu, 2)      # 반올림 (소수점 2자리)
```

- 문자열 함수

```
length(str)      # 문자열 길이
startsWith(str, 'prefix') # 접두사 확인
endsWith(str, 'suffix') # 접미사 확인
indexOf(str, 'search') # 문자열 위치
substring(str, 0, 10) # 부분 문자열
trim(str)        # 공백 제거
replace(str, 'old', 'new') # 문자열 치환
hasStr(str, 'search') # 문자열 포함 여부
```

문자열 함수

```
equalsIgnoreCase(str, 'match_text') # 대소문자를 구분하지 않는 일치 비교
notEqualsIgnoreCase(str, 'match_text') # 대소문자를 구분하지 않는 불일치 비교
```

`==` 와 `!=` 는 대소문자를 구분하므로 `WebServer` 와 `webserver` 를 다른 값으로 판단합니다. 표기가 일정하지 않은 태그나 필드를 비교할 때 위 두 함수를 사용하면 대소문자 차이를 무시하고 값을 맞출 수 있습니다.

예시

```
equalsIgnoreCase(okindName, 'WebServer')
notEqualsIgnoreCase(container, 'PROD.billing')
```

이벤트 발생 조건과 이벤트 대상 선택은 같은 문법을 사용하므로 두 함수를 양쪽 조건식에 모두 작성할 수 있습니다.

- 조건 함수

- **if:** 조건식이 참(`true`)이면 `true값` 을 반환하고, 거짓(`false`)이면 `false값` 을 반환하는 조건 함수

형식

```
if(조건, true값, false값)
```

예시

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

- **decode:** 값과 조건을 비교하여 일치하는 조건의 결과를 반환, 없으면 기본값 반환

형식

```
decode(값, 조건1, 결과1, 조건2, 결과2, ..., 조건N, 결과N, 기본값)
```

예시

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

- **in:** 값이 지정한 후보값 중 하나와 일치하면 `true`, 아니면 `false`

형식

```
in(값, 후보값1, 후보값2, ..., 후보값N)
```

예시

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

❗ 작성 시 주의사항

- 권장사항
 - 간단한 변수명은 `${}` 없이 사용 (예: `cpu`, `memory`)
 - 특수문자 포함 시 반드시 `${}` 사용
 - 복잡한 연산은 괄호로 명확하게 구분
 - 함수명은 정확히 입력 (대소문자 구분)



- 피해야 할 사항
 - 불완전한 표현식 작성 (예: `cpu > , memory &&`)
 - 괄호 미스매칭 (예: `(cpu > 80 && cpu > 70)`)
 - 연속된 연산자 사용 (예: `cpu >> 80 , cpu >< 80`)

복합 로그 이벤트 설정

홈 > 프로젝트 선택 >  경고 알림 > 이벤트 설정 > 복합 로그 탭

수집한 로그 데이터를 조건에 맞춰 필터링하려 경고 알림을 설정할 수 있습니다. 로그 이벤트를 사용하려면 로그 모니터링이 활성화되어야 합니다. **로그 모니터링 활성화**에 대한 자세한 내용은 (각 제품 로그 문서 링크)를 참고하세요.

- **복합 로그 이벤트:** 설정한 데이터 조회 범위 내 로그를 기준으로, 로그 검색 조건을 충족하는 로그 수가 임계 개수 이상일 경우 이벤트가 발생합니다.

! 권한

복합 메트릭스 이벤트를 설정하려면 **알림 설정 권한**이 필요합니다. 알림 설정 권한은 **홈 화면 > 프로젝트 선택 > 관리 > 통합 멤버 관리**에서 권한을 부여할 멤버의  아이콘을 클릭해 설정할 수 있습니다.

기본 옵션

- **검색:** 이벤트 이름 또는 이벤트 수신 태그를 선택해 원하는 이벤트 검색
- **JSON 다운로드/업로드:** 이벤트 규칙은 JSON 편집기를 통해 바로 수정하거나, 파일로 다운로드하여 수정 후 다시 업로드 가능
- **알림 메시지 설정:** 수신할 메시지의 상세 항목 선택 및 항목 별 내용 편집
- **+ 이벤트 추가:** 새로운 로그 이벤트 추가

표 | 복합 로그 이벤트 목록 구성

항목	설명
이벤트 이름	알림 제목으로 사용될 이벤트 이름
템플릿	복합 로그 템플릿
카테고리	로그 구분 명칭(로그 폴더명)
규칙	이벤트 발생하는 조건

항목	설명
이벤트 상태가 해소되면 추가 알림	Critical과 Warning 레벨의 이벤트가 해소되면 정상(RECOVERED) 상태의 알림 수신 여부 - 활성화: 진행 중 → 정상 상태로 전환될 때 RECOVERED 알림을 보내며, 이벤트 기록에서 진행 중/해소 상태를 구분해 볼 수 있음 - 비활성화: 임계값을 초과할 때 마다 단발성 이벤트 발생
이벤트 발생 일시 중지	이벤트 알림 발생 후, 같은 이벤트 발생을 일정 시간 동안 멈춤 - 선택 가능 시간: 사용 안 함, 5분, 10분, 15분, 20분, 30분, 1시간, 2시간, 3시간, 6시간, 12시간, 1일 - 해소된 알림이 활성화된 경우, 정상(RECOVERED) 상태 알림을 받은 후 선택한 시간 동안 같은 이벤트가 발생해도 알림이 발생하지 않음
인터벌	로그 데이터를 조회할 시간 범위
이벤트 수신 태그	해당 이벤트 알림을 받을 사용자 또는 그룹(수신 태그)
	이벤트 수정 및 삭제
	이벤트의 활성화 여부 - 활성화: 조건을 충족하면 이벤트 발생 - 비활성화: 이벤트가 동작하지 않으며, 조건을 검사하지 않음

이벤트 설정

복합 로그 이벤트는 설정한 데이터 조회 범위 내 로그를 기준으로, 로그 검색 조건을 충족하는 로그 수가 임계 개수 이상일 경우 경고 알림을 설정할 수 있는 기능입니다.

복합 로그 이벤트 추가

1. 경고 알림 > 이벤트 설정의 복합 로그 탭을 클릭하세요.
2. 화면 오른쪽의 [+ 이벤트 추가] 버튼을 클릭하세요.
3. 이벤트 규칙 추가 창에서 로그 이벤트 조건을 설정하세요. 자세한 내용은 [기본 설정](#), [상세 설정](#), [추가 설정](#)를 참고하세요.

X 이벤트 규칙 추가

*이벤트 이름

이벤트 활성화 ☒

레벨 위험 경고 정보 이벤트 상태가 해소되면 추가 알림 ⓘ ☐

템플릿

*메시지

*카테고리 ⓘ

*필터

*이벤트 발행 조건 조건에 맞는 로그 >

그룹화 필드

인터벌 ⓘ

무음 ⓘ

이벤트 동작 시간 [+ 추가](#)
이벤트 동작 시간 태그를 설정하면 해당 태그를 가진 알림은 해당 시간대에만 이벤트가 동작합니다.
이벤트 동작 시간 태그 설정에 대한 자세한 설명은 가이드 문서를 참고해 주세요. [가이드 문서 >](#)

이벤트 수신 태그 ⓘ 전제 멤버 수신 + 태그 추가
[프로젝트 이벤트 수신설정 메뉴 바로가기](#)

< 2026/04/21 14:11 ~ 2026/04/21 15:11 1시간 >

ⓘ

조건 설정 후 시뮬레이션 버튼을 누르면
알림 예상 건수를 확인할 수 있습니다.

저장

4. 이벤트 규칙 추가 창에서 설정이 완료되면 [저장] 버튼을 클릭하세요.

기본 설정

- **이벤트 이름:** 이벤트 제목으로 사용할 이름을 입력하세요.
- **이벤트 활성화:** 토글 버튼 활성화 시, 조건을 충족하면 이벤트 발생합니다.
- **레벨:** 이벤트 레벨(Critical, Warning, Info)을 선택하세요.

상세 설정

템플릿(프리셋), 메시지, 카테고리, 필터, 이벤트 발생 조건 항목을 설정합니다.

템플릿(프리셋)

미리 정의된 프리셋을 선택하면 필터, 쿼리 타입, 이벤트 발행 조건이 자동으로 설정됩니다. 프리셋을 선택한 후 필요에 맞게 수정할 수 있습니다.

복합 로그 템플릿 유형



프리셋	쿼리 타입	기본 규칙
사용 안 함	none	rows > 10
2xx 상태코드 건수	count	count > 10
3xx 상태코드 건수	count	count > 10
4xx 상태코드 건수	count	count > 10
5xx 상태코드 건수	count	count > 10
정상 상태코드(2xx, 3xx) 건수	count_v2	include_minus_exclude_count > 10
에러 상태코드(4xx, 5xx) 건수	count_v2	include_minus_exclude_count > 10
에러 수신 건수	count	count > 10
예외 수신 건수	count	count > 10



프리셋	쿼리 타입	기본 규칙
초당 로그 발생건수	rps	rps > 100
필드 집계 (Aggregation)	aggr	avg > 1000
비율 (Rate)	rate	rate > 10
고유값 수 (Cardinality)	cardinality	cardinality > 100
백분위 (Percentile)	percentile	p99 > 3000

메시지

이벤트 발생 시 전달받을 알림 메시지를 입력하세요. 메시지에 변수를 사용하여 동적 메시지를 구성할 수 있습니다.

- 예시: 메시지 `${host}` 에서 에러 `${count}` 건 발생 → 알림 메시지 web-01에서 에러 15건 발생

표 | 메시지 변수

변수	설명	사용 조건
<code>\${count}</code>	조건에 맞는 로그 건수	항상 사용 가능
<code>\${groupField}</code>	그룹화 필드 이름	그룹화 알림만
<code>\${groupValue}</code>	그룹화 필드 값	그룹화 알림만
<code>\${필드명}</code>	그룹화 필드 값 (필드명으로 직접 참조)	그룹화 알림만



`${count}` 변수는 그룹화 여부와 관계없이 모든 알림에서 사용할 수 있습니다. `${groupField}` , `${groupValue}` , `${필드명}` 변수는 그룹화 필드를 설정한 경우에만 치환됩니다.

카테고리

로그 구분 명칭(로그 폴더명)을 목록에서 선택하거나 직접 입력하세요. 카테고리를 선택해야 검색 키와 검색 값을 입력할 수 있습니다.

필터

Lucene 쿼리 문법으로 로그 검색 조건을 입력합니다. 두 가지 입력 모드를 지원합니다.

- **필터 모드** : 필드와 값을 선택하여 쿼리를 구성합니다.
- **코드 모드** : Lucene 쿼리를 직접 입력합니다.

표 | Lucene 쿼리 예시

쿼리	설명
<code>level:ERROR</code>	level 필드가 ERROR인 로그
<code>status_nxx:status_4xx OR status_nxx:status_5xx</code>	4xx 또는 5xx 상태코드
<code>appender:accessLog</code>	accessLog appender의 로그
<code>response_time.n:*</code>	response_time.n 필드가 존재하는 로그
<code>host:web-01 AND level:ERROR</code>	web-01 호스트의 에러 로그

이벤트 발생 조건

쿼리 타입별로 설정합니다. 선택한 템플릿(프리셋) 또는 쿼리 타입에 따라 추가 설정 항목이 표시됩니다.

표 | 이벤트 발행 조건 키 의미

키	의미
<code>rows / count</code>	필터 조건에 맞는 로그 건수
<code>rps</code>	초당 로그 발생건수 (건수 / 인터벌 초)

키	의미
avg	대상 필드 값의 평균
sum	대상 필드 값의 합계
min	대상 필드 값의 최솟값
max	대상 필드 값의 최댓값
rate	분자 건수 / 분모 건수 × 100 (%)
cardinality	대상 필드의 고유한 값 개수
p99 / p95 / p90 / p75 / p50	대상 필드의 백분위 값
include_minus_exclude_count	포함 필터 건수 - 제외 필터 건수

- **건수 (count / none):** 설정한 필터 조건에 맞는 로그의 건수를 카운트합니다.

표 | 건수 설정 항목

설정 항목	설명
필터	로그 검색 조건 (Lucene 쿼리)
이벤트 발행 조건	건수 또는 조건에 맞는 로그 {연산자} {임계값} (예: count > 10)

- **초당 로그 발생건수 (rps):** 설정한 필터 조건에 맞는 로그의 초당 발생건수(Requests Per Second)를 계산합니다. 인터벌 시간 동안의 총 건수를 인터벌 초로 나누어 산출합니다.

표 | 초당 로그 발생건수 설정 항목

설정 항목	설명
필터	로그 검색 조건 (Lucene 쿼리)
이벤트 발행 조건	RPS {연산자} {임계값} (예: rps > 0.5)

- **필드 집계 (aggr):** 지정한 숫자 필드의 집계 값(평균, 합계, 최솟값, 최댓값)을 계산합니다. 이벤트 발행 조건에서 집계 방식을 드롭다운으로 선택할 수 있습니다.

표 | 필드 집계 설정 항목

설정 항목	설명
필터	로그 검색 조건 (Lucene 쿼리)
대상 필드	집계 대상 숫자 필드 (예: response_time.n)
이벤트 발행 조건	평균 / 합계 / 최솟값 / 최댓값 {연산자} {임계값} (예: avg > 1000)

- **비율 (rate):** 분자 필터와 분모 필터의 건수 비율(%)을 계산합니다. 전체 로그 대비 특정 조건의 비율을 모니터링할 때 유용합니다.

표 | 비율 설정 항목

설정 항목	설명
필터 (분자)	비율 계산의 분자가 되는 로그 조건 (예: level:ERROR)
분모 필터	비율 계산의 분모가 되는 로그 조건 (예: level:*)
이벤트 발행 조건	비율 (%) {연산자} {임계값} (예: rate > 10)

- 예시: 필터 level:ERROR, 분모 필터 level:*, rule rate > 10 → 전체 로그 중 에러 비율이 10%를 초과하면 알림 발생

- **고유값 수 (cardinality):** 지정한 필드의 고유한 값 개수를 계산합니다. 비정상적으로 많은 종류의 값이 발생하는 경우를 감지할 때 유용합니다.

표 | 고유값 수 설정 항목

설정 항목	설명
필터	로그 검색 조건 (Lucene 쿼리)
대상 필드	고유값을 계산할 필드 (예: host)

설정 항목	설명
이벤트 발행 조건	고유값 수 {연산자} {임계값} (예: cardinality > 100)

- **백분위 (percentile):** 지정한 숫자 필드의 백분위(Percentile) 값을 계산합니다. 응답 시간의 tail latency를 모니터링할 때 유용합니다. Percentile 선택을 변경하면 이벤트 발행 조건의 키가 자동으로 업데이트됩니다.

표 | 백분위 설정 항목

설정 항목	설명
필터	로그 검색 조건 (Lucene 쿼리)
대상 필드	백분위를 계산할 숫자 필드 (예: response_time.n)
Percentile	P99, P95, P90, P75, P50 중 선택
이벤트 발행 조건	P99 / P95 / ... {연산자} {임계값} (예: p99 > 3000)

표 | 백분위 의미

백분위	의미
P50	중앙값. 전체 데이터의 50%가 이 값 이하
P75	전체 데이터의 75%가 이 값 이하
P90	전체 데이터의 90%가 이 값 이하
P95	전체 데이터의 95%가 이 값 이하
P99	전체 데이터의 99%가 이 값 이하

- **포함/제외 건수 (count_v2):** 포함 필터의 건수에서 제외 필터의 건수를 뺀 순수 건수를 계산합니다.

표 | 포함/제외 건수 설정 항목

설정 항목	설명
필터 (포함)	포함할 로그 조건 (예: <code>status_nxx:status_4xx OR status_nxx:status_5xx</code>)
필터 제외	제외할 로그 조건 (예: <code>status_nxx:status_4xx</code>)
분모 필터	비율 계산용 분모 (선택사항)
이벤트 발행 조건	포함-제외 건수 {연산자} {임계값} (예: <code>include_minus_exclude_count > 10</code>)

- 예시: 필터 `status_nxx:status_4xx OR status_nxx:status_5xx`, 필터 제외 `status_nxx:status_4xx` → `4xx+5xx`에서 `4xx`를 제외한 순수 `5xx` 건수가 10을 초과하면 알림 발생

그룹화 필드(Group By)

그룹화 필드를 설정하면 해당 필드의 값별로 독립적으로 알림 조건을 판정합니다. 드롭다운에서 그룹화할 필드를 선택합니다. 드롭다운을 클릭하면 현재 카테고리에서 사용 가능한 필드 목록이 자동완성됩니다.

- 예시: 필터 `level:ERROR`, 그룹화 필드 `host`, rule `rows > 3`

표 | 그룹화 설정 비교

항목	그룹화 없음	그룹화 사용
판정 단위	전체 로그를 하나로 집계	그룹 값별 독립 집계
알림 발생	1건	조건 충족 그룹 수만큼
알림 제목	이벤트 제목	[그룹 값] 이벤트 제목
Stateful	전체 기준 상태 전이	그룹별 독립 상태 전이

- [web-01] 에러 알림 — web-01에서 에러 8건 → 알림 발생
- [web-02] 에러 알림 — web-02에서 에러 5건 → 알림 발생
- [api-01] 에러 알림 — api-01에서 에러 2건 → 조건 미충족, 알림 미발생

- ① 이벤트 상태가 해소되면 추가 알림을 활성화한 경우, 그룹별로 독립적으로 ABNORMAL → RECOVERED 상태가 전이됩니다. 예를 들어 web-01 에서 에러가 해소되면 [web-01] RECOVERED 알림이 발생하며, 다른 호스트의 상태에는 영향을 미치지 않습니다.

추가 설정

- **인터벌:** 선택한 시간(unset , 1분 , 5분 , 10분 , 30분 , 1시간 , 12시간) 간격으로 알림 조건을 확인합니다.
- **무음:** 이벤트 발생 후, 선택한 시간(unset , 1분 , 5분 , 10분 , 30분 , 1시간 , 12시간) 동안 같은 이벤트가 발생되지 않습니다.
- **이벤트 동작 시간:** 이벤트가 특정 시간대(근무/비근무/점검 시간 등)에 동작하도록 태그를 설정하세요. 태그를 설정하지 않으면 이벤트가 활성화된 상태에서 24시간 상시 동작합니다.
 1. + 추가를 클릭하세요.
 2. 이벤트 동작 시간에서 +새로운 태그 생성을 클릭하세요.
 3. 이벤트 동작 시간 태그 생성에서 태그 이름, 요일, 시간, 색상을 선택하고 [적용] 버튼을 클릭하세요.
 4. 생성한 태그는 태그 목록에서 확인할 수 있으며, 체크 박스를 선택하면 적용됩니다.
 5. 수정 또는 삭제할 태그의 ✎ 아이콘을 클릭해 이벤트 동작 시간 태그 수정에서 태그를 수정하거나 태그 삭제할 수 있습니다.

- ❗ 태그 삭제 시 해당 태그가 적용된 모든 사용자의 태그가 제거됩니다. 단, 이벤트 규칙에서 사용 중인 태그는 삭제할 수 없습니다.

- **이벤트 수신 태그:** 이벤트에 수신 태그를 설정하면, 해당 태그를 가진 프로젝트 멤버에게 알림을 전송합니다. 수신자 태그를 설정하지 않으면 프로젝트 내 모든 사용자에게 알림이 전송됩니다.
 1. + 태그 추가 또는 +를 클릭하세요.
 2. 이벤트 수신 태그 창 아래의 + 새 태그 생성을 클릭하세요.
 3. 태그 생성 창에서 태그 이름을 입력하고, 색상을 선택한 후, [태그 생성] 버튼을 클릭해 태그를 생성하세요.
 4. 생성된 태그는 태그 목록의 ✎ 아이콘을 클릭해 수정 또는 삭제하세요.
 5. 이벤트 수신 태그 창의 태그 목록에서 원하는 태그를 선택하면 적용됩니다.

- ✓ 이벤트 설정 시 이벤트 수신 태그를 선택하여 해당 태그를 가진 프로젝트 멤버와 3rd-party 플러그인에 알림을 전송할 수 있습니다. **경고 알림 > 이벤트 수신 설정**에서 프로젝트 멤버와 3rd-party 플러그인에 각각 태그를 지정할 수 있습니다.

시뮬레이션

알림을 저장하기 전에 과거 데이터로 시뮬레이션하여 알림 발생 예상 건수를 확인할 수 있습니다.

1. 알림 설정을 완료한 후 하단의 시간 범위를 선택하세요.
2. [시뮬레이션] 버튼을 클릭하세요.
3. 차트에 시간대별 데이터와 알림 발생 횟수가 표시됩니다.

ⓘ 시뮬레이션 시간 범위를 조절하여 다양한 시간대의 알림 발생 패턴을 확인할 수 있습니다. 최근 1~2분의 데이터는 인덱스 빌드 지연으로 조회되지 않을 수 있습니다.

4. 이벤트 규칙 추가 창에서 설정이 완료되면 [저장] 버튼을 클릭하세요.

로그 탐색기에서 알림 생성

로그 탐색기에서 직접 알림을 생성할 수 있습니다.

1. 로그 > 로그 탐색 메뉴로 이동하세요.
2. 카테고리 및 검색 쿼리를 설정하세요.
3. 화면 오른쪽 위의 [이벤트 추가] 버튼을 클릭하세요.
4. Drawer에서 알림 설정 폼이 열리며, 현재 카테고리 및 검색 쿼리가 자동으로 채워집니다.
5. 추가 설정을 완료하고 [저장] 버튼을 클릭하세요.
6. 저장 완료 후 [이동] 버튼을 클릭하면 알림 목록으로 이동합니다.

이벤트 수정/삭제

1. 경고 알림 > 이벤트 설정의 복합 로그 탭으로 이동하세요.
2. 로그 이벤트 목록에서 수정 또는 삭제하려는 이벤트의  아이콘을 클릭하세요.
3. 이벤트 설정 화면에서 옵션을 수정하고, [저장] 버튼을 클릭하세요.
 - a. 선택한 이벤트를 삭제하려면 이벤트 설정 화면의 오른쪽 위의 [삭제] 버튼을 클릭하세요.

이벤트 공유

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

- JSON 파일명: event-rules- YYYYMMDD .json

내보내기

1. 화면 오른쪽 위에 [JSON ] 버튼을 클릭하세요.
2. JSON 편집 창이 나타나면 [ 내보내기] 버튼을 클릭하세요.
 - 이벤트를 검색 후 내보내기 기능을 이용하면 검색한 목록만 JSON 파일로 다운받을 수 있습니다.
3. JSON 파일이 다운로드되면 공유할 다른 사용자에게 전달하세요.

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.

 같은 종류의 제품 간에 이용할 것을 권장합니다. 다른 제품의 프로젝트로부터 이벤트 설정을 가져올 수는 있지만 정상 작동하지 않습니다.

Json 형식으로 수정하기

1. 화면 오른쪽 위에 [JSON ] 버튼을 클릭하세요.
2. 편집 창이 나타나면 JSON 형식에 맞춰 내용을 수정하세요.
3. 수정을 완료하면 화면 아래 [저장] 버튼을 선택하세요.

❗ 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)

이벤트 수신 설정

홈 > 프로젝트 선택 >  경고 알림 > 이벤트 수신 설정

사용자별 이벤트 수신 설정

 **사용자별 이벤트 수신 설정** 의 다른 멤버의 정보는 **멤버 관리** 권한을 가진 멤버만 확인할 수 있습니다. 그 외 멤버에게는 필수 정보가 마스킹 처리됩니다.

- 이벤트 알림의 일괄 수신설정 및 접근 설정을 위한 모바일 기기 관리는 **계정 정보**에서 할 수 있습니다.
- 멤버 권한에 대한 자세한 설명은 [다음 문서](#)를 참고하세요.

수신 수단 설정

이메일, SMS, WhatsApp, 모바일 알림을 제공합니다.

사용자별 이벤트 수신 설정 섹션에서 원하는 알림 수신 수단의 체크 박스를 선택하면 경고 알림을 받을 수 있습니다. 알림 수신 수단의 체크 박스를 해제하면 경고 알림을 보내지 않습니다.

 프로젝트 최고 관리자를 제외한 모든 사용자는 자신의 수신 설정만 변경할 수 있습니다.

이메일 알림

이메일 알림은 회원 가입 시 입력한 이메일 주소로 알림을 보냅니다.

SMS 알림

SMS로 알림을 수신할 수 있습니다.

 SMS 알림 기능은 유료 프로젝트에 한정됩니다.

1. 화면 오른쪽 위의 **자신의 프로필 아이콘** > **계정 관리**로 이동하세요.
2. **계정 정보의 사용자 전화번호** 섹션에서 [일반 휴대전화] 버튼을 클릭하세요.
3. **전화번호**에 인증번호를 수신을 전화번호를 입력하세요.
 - SMS를 알림으로 수신할 수 있는 전화번호는 **한국의 휴대전화 번호만** 등록할 수 있습니다.
4. [저장] 버튼을 클릭하세요.

✔ 등록된 전화번호 변경 및 삭제

- 전화번호를 변경할 경우, [변경] 버튼을 클릭하세요. SMS 인증이 필요합니다.
- 전화번호를 삭제할 경우, [삭제] 버튼을 클릭하세요. 전화번호 삭제 시 SMS로 수신받는 알림은 수신할 수 없습니다.

WhatsApp 알림

WhatsApp을 통해 알림을 수신할 수 있습니다.

❗ WhatsApp 알림 기능은 유료 프로젝트에 한정됩니다.

1. 화면 오른쪽 위의 **자신의 프로필 아이콘** > **계정 관리**로 이동하세요.
2. **계정 정보의 사용자 전화번호** 섹션에서 [WhatsApp] 버튼을 클릭하세요.
3. 인증번호를 받을 **전화번호**를 입력하세요.
4. [인증번호 전송] 버튼을 클릭하세요.
5. WhatsApp 애플리케이션으로 전송된 인증번호 6자리를 입력하세요.
 - 10분 내로 인증번호를 받지 못했다면, [인증번호 재전송] 버튼을 클릭하세요.
6. [인증하기] 버튼을 클릭하세요.

모바일 알림

모바일 알림 수신이 필요한 사용자는 모바일 기기에 와탭 애플리케이션을 설치한 후 로그인해야 합니다.

- 와탭 애플리케이션 다운로드 - [안드로이드](#)
- 와탭 애플리케이션 다운로드 - [iOS](#)

반복 알림(에스컬레이션) 설정

경고 알림 발생 시간으로부터 알림 발생 상황이 해소되지 않을 경우 최초 알림 발생 시각으로부터의 알림 반복 간격을 설정할 수 있습니다. 위험(**Critical**) 레벨의 알림만 적용됩니다.

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.

1. **경고 알림 > 이벤트 수신 설정의 사용자별 이벤트 수신 설정** 섹션으로 이동하세요.
2. **반복 알림(에스컬레이션)** 항목에서 설정하세요.
 - **M**: 분, **H**: 시간, **D**: 일, 단위를 생략하면 분 단위로 시간을 설정합니다.
 - 숫자 또는 숫자+단위(**M, H, D**)로 입력하세요. 입력이 올바르지 않으면 메시지가 표시됩니다.
3. [저장] 버튼을 클릭하세요. 저장하지 않으면 설정되지 않습니다.

이벤트 수신 태그

이벤트 설정 시 이벤트 수신 태그를 선택하여 해당 태그를 가진 프로젝트 멤버와 3rd-party 플러그인에 알림을 전송할 수 있습니다. 이벤트 수신 태그를 설정하지 않으면 전체 멤버에게 경고 알림이 전송됩니다.

이벤트 수신 태그 추가/수정/삭제하기

 이벤트에 적용 중인 이벤트 수신 태그 항목은 삭제할 수 없습니다.

1. **경고 알림 > 이벤트 수신 설정**으로 이동하세요.
2. **사용자별 이벤트 수신 설정** 섹션의 사용자 목록에서 **+ 태그 추가** 또는 **+** 를 클릭하세요.
3. **이벤트 수신 태그** 창에서 **+ 새 태그 생성**을 클릭하세요.
4. **태그 생성** 창에서 태그 이름을 입력하고, 색상을 선택한 후, [태그 생성] 버튼을 클릭해 태그를 생성하세요.
5. 생성된 태그는 태그 목록의  아이콘을 클릭해 수정 또는 삭제하세요.
6. **이벤트 수신 태그** 창의 **태그 목록**에서 원하는 태그를 선택하면 적용됩니다.

이벤트 수신 태그 해제하기

1. 경고 알림 > 이벤트 수신 설정의 사용자별 이벤트 수신 설정 섹션으로 이동하세요.
2. 이벤트 수신 태그를 해제할 사용자의 이벤트 수신 태그 항목의 + 를 클릭하세요.
3. 이벤트 수신 태그 창에서 해제할 태그의 X 를 클릭하면 해당 태그가 해제됩니다.

수신 태그 미설정 알림 받기

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

- 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.

이벤트 수신 모드 선택하기

사용자별 이벤트 수신 설정 섹션에서 멤버 또는 3rd 파티 채널별로 이벤트 알림 수신 범위를 다음 네 가지 모드 중에서 선택할 수 있습니다. 수신 모드는 각 멤버 또는 채널 행의 이벤트 수신 태그 옆에서 라디오 버튼으로 선택하세요.

수신 모드	설명
모든 알림 받기	이벤트 수신 태그와 무관하게 모든 경고 알림 수신
선택한 태그만 받기	선택한 이벤트 수신 태그를 가진 경고 알림만 수신. 태그를 최소 한 개 이상 선택
선택한 태그만 제외하기	선택한 이벤트 수신 태그를 가진 경고 알림만 제외하고 나머지 전부 수신. 제외 태그를 최소 한 개 이상 선택
모든 알림 받지 않기	어떤 이벤트 알림도 받지 않음. 선택해 둔 태그는 삭제되지 않고 그대로 보존

- 이벤트 수신 태그가 지정되지 않은 경고 알림까지 받으려면 태그 선택 영역에서 미분류 가상 태그를 선택하세요. 미분류 태그는 일반 태그와 동일하게 선택하거나 해제할 수 있으며, 태그 자체를 수정하거나 삭제할 수는 없습니다.

❗ **모든 알림 받지 않기** 모드에서는 해당 멤버 또는 채널이 이벤트 알림을 전혀 받지 않습니다. 이때 선택해 둔 태그는 삭제되지 않고 보존되므로, 다시 **선택한 태그만 받기** 모드로 전환하면 이전에 선택한 태그 설정을 그대로 사용할 수 있습니다.

선택한 태그만 받기

1. **사용자별 이벤트 수신 설정** 섹션에서 설정할 멤버 또는 3rd 파티 채널 행의 **이벤트 수신 태그** 옆을 클릭하세요.
2. **선택한 태그만 받기** 라디오 버튼을 선택하세요.
3. 태그 선택 영역에서 알림을 받을 태그를 하나 이상 선택하세요.

❗ **선택한 태그만 받기** 모드에서 태그를 하나도 선택하지 않았을 때 나타나는 완전 차단 경고는 **선택한 태그만 제외하기** 모드에는 표시되지 않습니다. 제외 태그가 없는 상태는 알림을 전부 차단하는 상태가 아니라 전부 수신하는 상태이기 때문입니다.

선택한 태그만 제외하기

경고 알림을 대부분 받되 특정 분류만 걸러 내고 싶을 때 사용합니다. 받을 태그를 하나씩 고르는 **선택한 태그만 받기**와 방향이 반대입니다.

1. **사용자별 이벤트 수신 설정** 섹션에서 설정할 멤버 또는 3rd 파티 채널 행의 **이벤트 수신 태그** 옆을 클릭하세요.
2. **선택한 태그만 제외하기** 라디오 버튼을 선택하세요.
3. 아래 태그 선택 영역에서 알림을 받지 않을 태그를 하나 이상 선택하세요.
 - 이벤트에 붙은 태그와 제외 태그가 하나라도 겹치면 해당 경고 알림은 전송되지 않습니다. 겹치는 태그가 없는 알림은 모두 수신합니다.
 - 제외 태그는 최소 한 개 이상 선택해야 합니다. 제외 태그가 하나도 없는 상태는 **모든 알림 받기**와 결과가 같아지므로, 마지막 태그는 제거할 수 없고 제외 태그가 비어 있는 동안 **최소한 하나의 태그를 선택해 주세요.** 안내가 표시됩니다.
 - 제외 태그 목록은 **선택한 태그만 받기** 모드의 수신 태그 목록과 별도로 저장됩니다. 두 모드를 번갈아 선택해도 각 모드에서 고른 태그가 그대로 남습니다.
 - **미분류** 가상 태그도 제외 대상으로 선택할 수 있으며, 태그 한 개로 계산됩니다.

알림 수신 언어 선택

사용자의 알림 수신 언어를 선택할 수 있습니다.

1. 경고 알림 > 이벤트 수신 설정으로 이동하세요.
2. 사용자별 이벤트 수신 설정 섹션의 사용자 목록에서 언어를 설정할 사용자의 가장 왼쪽에 ► 버튼을 클릭하세요.
3. 알림 수신 언어를 선택하세요.

요일 및 시간별 알림 설정

사용자의 요일별, 시간별 알림 수신 여부를 선택할 수 있습니다.

1. 경고 알림 > 이벤트 수신 설정으로 이동하세요.
2. 사용자별 이벤트 수신 설정 섹션의 사용자 목록에서 요일 및 시간별 알림을 설정할 사용자의 가장 왼쪽에 ► 버튼을 클릭하세요.
3. 경고 알림 수신을 원하는 요일을 선택하거나 시간을 입력하세요.
 - 알림 수신 수단별로 설정할 수 있습니다.

3rd 파티 플러그인

외부 애플리케이션을 통해 경고 알림을 받을 수 있습니다.

- 지원 애플리케이션: Slack, Telegram, Teams, Teams Workflows, Jandi, AlertNow, Webhook, Webhook JSON, Opsgenie, PagerDuty, LINE, ilert

❗ 와탭랩스의 지원 범위에 포함하지 않는 사내 메신저는 표준 Webhook, Webhook json을 통해 연동할 수 있습니다.

표 | 3rd 파티 플러그인 목록 구성

항목	설명
플러그인 이름	플러그인의 이름

항목	설명
인증 키	인증 키
인증 값	인증값
수신 레벨	경고, 전체, 위험으로 구분
반복 알림(에스컬레이션)	알림 발생 시간으로부터 알림 발생 상황이 해소되지 않았을 경우, 최초 알림 발생 시각으로부터의 알림 재발행 주기 - 위험(Critical) 단계의 알림에만 적용되는 기능
Smart 메시지(AI)	Telegram 3rd 파티 플러그인 추가 시 AI 알림 기능 제공 - 지원 언어: 한국어, 영어, 일본어
이벤트 수신 태그	프로젝트의 멤버 중 특정 멤버 또는 팀을 대상으로 알림 수신 여부
삭제	3rd 파티 플러그인 삭제

3rd 파티 플러그인 추가

1. 경고 알림 > 이벤트 수신 설정으로 이동하세요.
2. 3rd 파티 플러그인 섹션의 [추가하기] 버튼을 클릭하세요.
3. 서드 파티 플러그인 추가 창에서 원하는 서비스 탭으로 선택하세요.
4. 선택한 서비스의 안내(3rd 파티 플러그인 알림 추가 방법)에 따라 설정을 진행하세요.
5. [수신 테스트] 버튼을 클릭해 설정이 잘 되었는지 확인하세요.
6. 모든 과정을 완료하면 [추가하기] 또는 [등록] 버튼을 클릭하세요.

3rd 파티 플러그인 알림 추가 방법

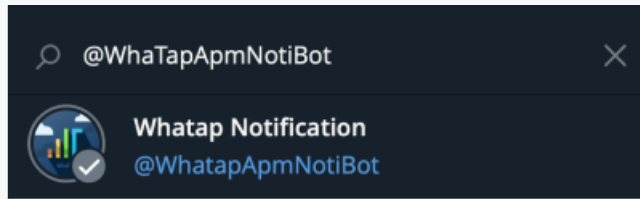
Slack

 서드 파티 플러그인 추가의 Slack 탭 화면의 [슬랙에 추가하기] 버튼을 클릭하면 Slack의 팀 및 채널에 WhaTapNotiBot을 등록할 수 있습니다.

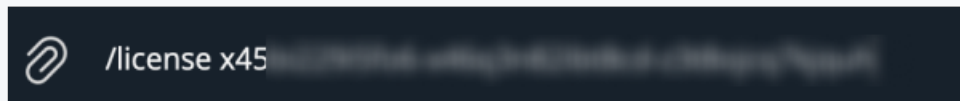
Telegram



1. Telegram에서 @WhaTapApmNotiBot을 검색하세요.



2. Bot을 선택하고 [시작] 버튼을 클릭하세요.
3. 채팅창에 `/license` 명령어와 알림을 받을 프로젝트의 액세스 키를 채팅창에 입력하세요.



① 사용할 수 있는 명령어 목록

- `/help` : 명령어 목록 보기
- `/license` : 알림 받을 프로젝트의 액세스 키 입력
- `/remove` : 알림을 받지 않을 프로젝트 코드 입력
- `/list` : 현재 알림을 받고 있는 프로젝트 코드 보기

Teams



1. 알림을 받을 채널의 커넥터로 이동하세요.



≡ 새 게시물 맨 위에 표시(최신순 정렬)

🔔 채널 알림

📌 고정

⚙️ 채널 관리

✉️ 전자 메일 주소 가져오기

↔️ 채널 링크 받기

👤 커넥터

2. Webhook을 추가하고 [구성] 버튼을 클릭하세요.

 **Incoming Webhook** 구성

서비스의 데이터를 Office 365 그룹에 실시간으로 보냅니다.

3. Webhook 이름을 입력하고 [만들기] 버튼을 클릭하세요.

 **Incoming Webhook** 피드백 보내기

수신 Webhook 커넥터를 사용하면 추적을 원하는 활동에 대한 알림을 외부 서비스로부터 받을 수 있습니다. 이 커넥터를 사용하려면 Office 365 커넥터 형식과(와) 호환되는 Webhook을 지원해야 하는 다른 서비스에서 특정 설정을 만들어야 합니다.

* 표시된 필드는 필수입니다.

Incoming Webhook를 설정하려면 이름을 지정하고 [만들기]를 선택합니다. *

이 Incoming Webhook의 데이터와 연결할 이미지를 사용자 지정합니다.

이미지 업로드



기본 이미지

만들기 취소



4. 생성된 Webhook URL을 복사하세요.

아래 URL을 복사하여 클립보드에 저장한 다음 [저장]을 선택합니다. 사용자 그룹에 데이터를 전송하려는 서비스로 이동할 때 이 URL이 필요합니다.

`https://whatap.webhook.office.com/webt`



URL이 최신 상태입니다.

완료

제거

5. 와탭 모니터링 서비스의 **서드 파티 플러그인 추가** 창으로 돌아와 Teams 탭 하단의 **Channel Name**과 **Webhook URL** 항목을 입력하세요.

6. [등록]버튼을 클릭하세요.

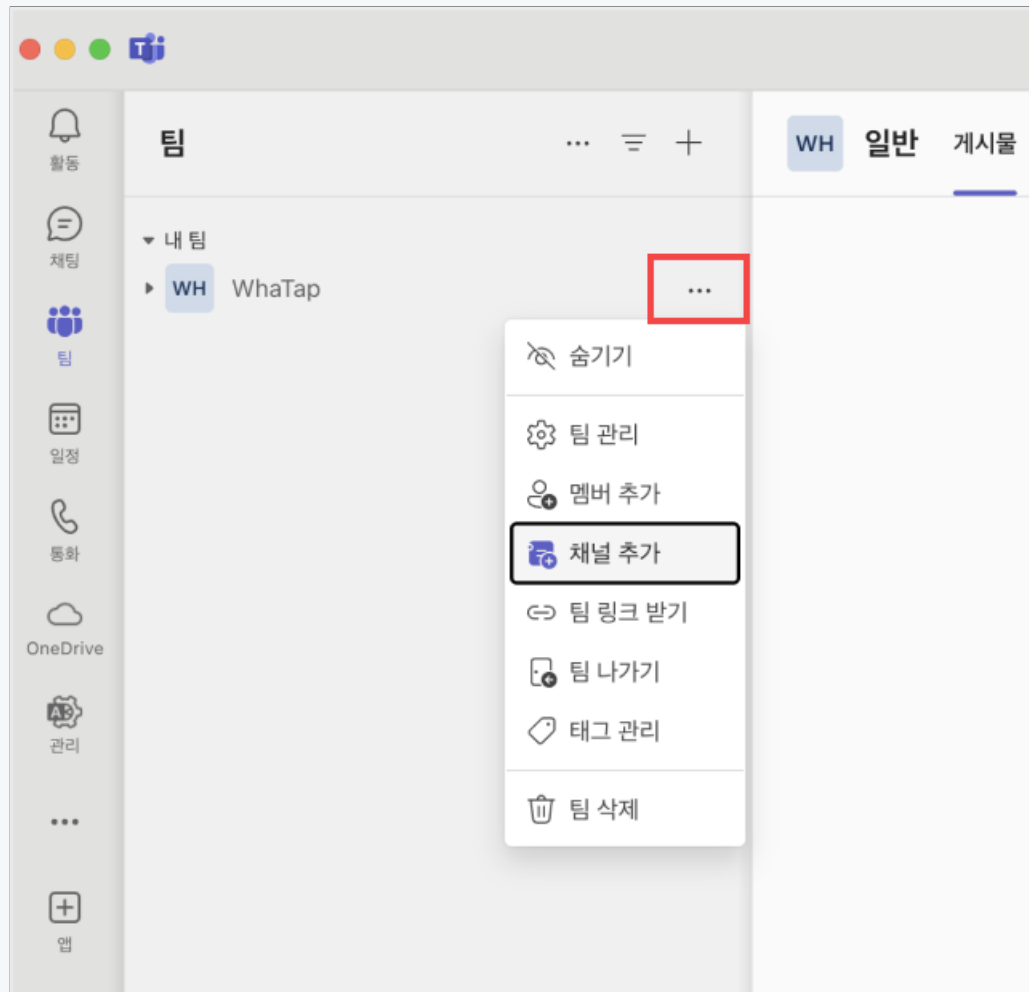


Teams Workflows



워크플로를 사용하려면 **Microsoft Teams**에 액세스할 수 있는 계정과 비즈니스 플랜 구독이 필요합니다.

1. 팀 메뉴의 더보기(...) > 채널 추가를 클릭하세요.



2. 채널 만들기 창에서 채널 이름과 설명을 입력하고, 채널 유형 선택 항목은 표준으로 선택한 후, [만들기] 버튼을 클릭하세요.



채널 만들기

채널 이름 *

WhaTap 알림 채널

설명

사람들이 올바른 채널을 찾을 수 있도록 설명을 입력하세요.

채널 유형 선택 *

①

선택

표준

팀의 모든 사람이 액세스할 수 있습니다.

공유

조직 내 또는 조직 외부의 사람이나 팀이 액세스할 수 있습니다.

비공개

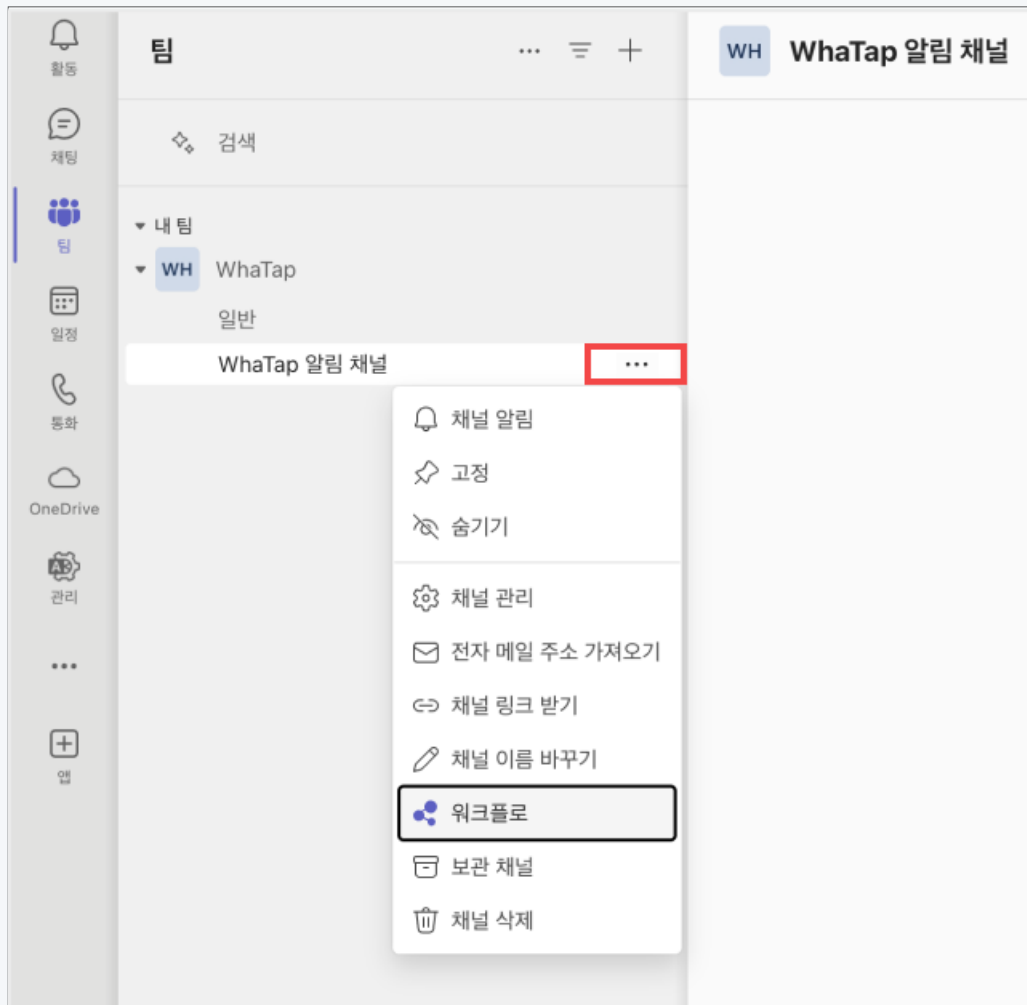
팀의 특정 사용자가 액세스할 수 있습니다.

취소

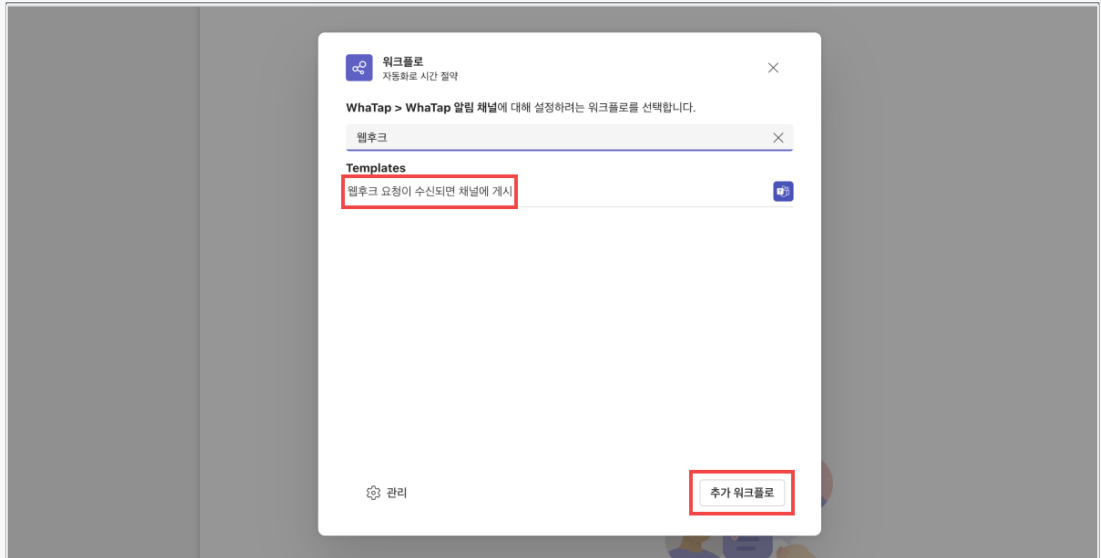
만들기

❗ 채널 유형을 공유로 선택하면 워크플로를 사용할 수 없으며, 비공개를 선택하면 워크플로를 추가할 수 있지만 알림을 수신할 수 없습니다.

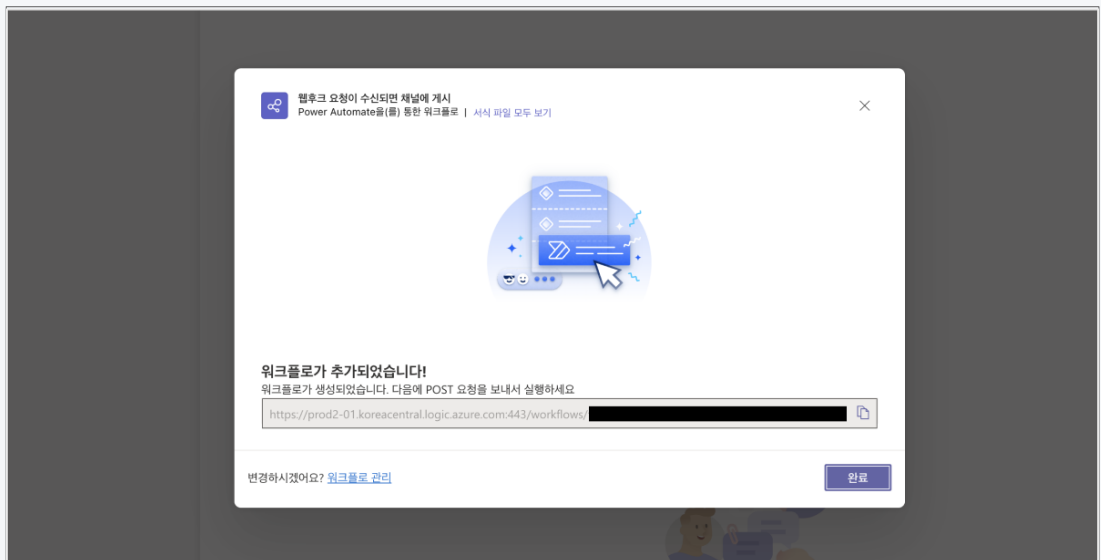
3. 생성한 채널의 더보기(...) > 워크플로를 클릭하세요.



4. 워크플로 대화상자의 워크플로의 목록에서 웹훅 요청이 수신되면 채널에 게시를 선택 후, [추가 워크플로] 버튼을 클릭하세요.



5. 이름과 연결 상태를 확인한 후, [다음] 버튼을 클릭하세요.
6. 세부 정보를 확인한 후, [워크플로 추가] 버튼을 클릭하세요.
7. 워크플로가 추가되었습니다. 생성된 주소를 복사하세요.

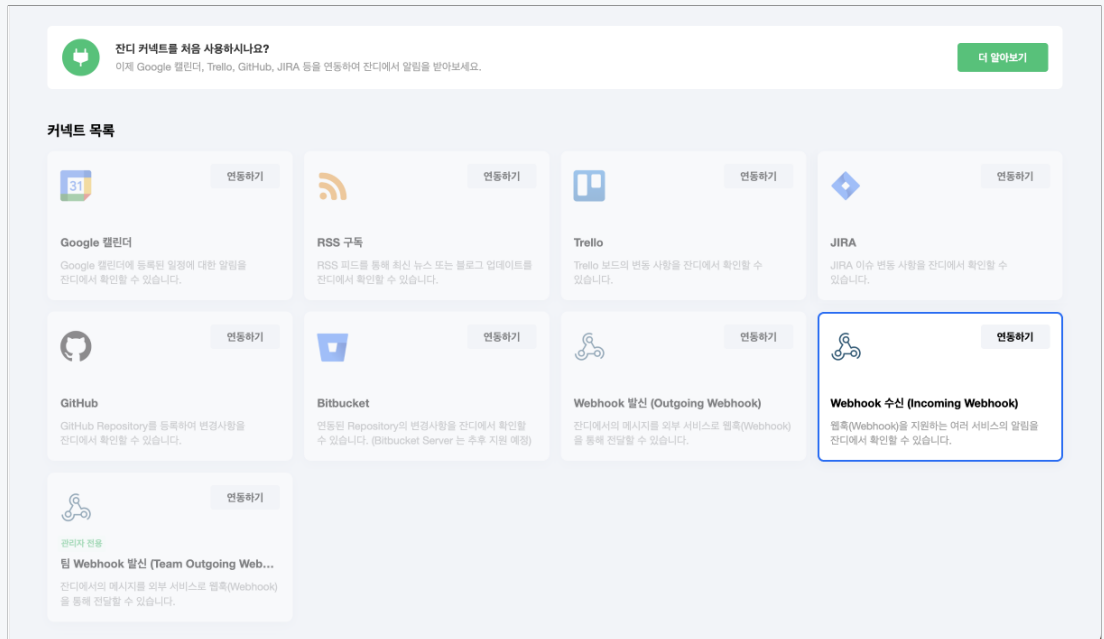


8. 와탭 모니터링 서비스의 **서드 파티 플러그인 추가** 창으로 돌아와 **Teams Workflows** 탭 안내 하단의 **Channel Name**과 **Webhook URL** 항목을 입력하세요.
9. [등록] 버튼을 선택하세요.

잔디(jandi)



1. 알림을 받을 토픽 또는 채팅에서 잔디 커넥트 설정으로 이동하세요.
2. 커넥트 목록에서 **Webhook 수신 (Incoming Webhook)** 항목에서 [연동하기] 버튼을 클릭하세요.



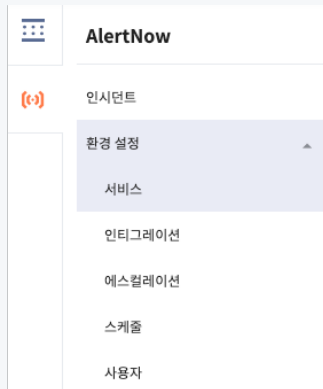
3. [Webhook 수신 추가] 버튼을 클릭하세요.
4. Webhook URL 등록 항목에 Webhook URL을 복사하세요.



5. 와탭 모니터링 서비스의 **서드 파티 플러그인 추가** 창으로 돌아와 Jandi 탭 안내 하단의 **Channel Name**과 **Webhook URL** 항목을 입력하세요.
6. [등록] 버튼을 클릭하세요.



1. AlerNow 서비스를 접속한 후, **환경 설정 > Integration** 메뉴로 이동하세요.



2. 인티그레이션 화면에서 [인티그레이션 생성] 버튼을 클릭하세요.
3. Integration 유형 중 **WhaTap**을 선택하세요.
4. 인티그레이션 생성 화면에서 이름 및 이름 지정 규칙을 설정하세요.

5. [확인] 버튼을 클릭하면 Integration이 생성됩니다.
6. 생성된 인티그레이션 목록을 확인하고 생성된 Integration 항목을 선택하세요.



인티그레이션 ?

인티그레이션 생성 검색어 입력 🔍 🔄 마지막 업데이트: 2020-07-02 16:51:44

인티그레이션 이름	인티그레이션 유형	인티그레이션 키	서비스 이름
Whatap - APM	WhaTap	46c1982c7	Whatap - APM

- 상세 화면에서 URL 오른쪽의 복사 아이콘을 클릭해 URL을 복사하세요.

← **인티그레이션**

Whatap - APM ✎

기본 정보

인티그레이션 유형	WhaTap
인티그레이션 키	46c1982c7
URL	https://alertnowitgr.opsnow.com/integration/whatap/v1/46c1982c7

- 와탭 모니터링 서비스의 **서드 파티 플러그인 추가** 창으로 돌아와 **AlertNow** 탭 안내 하단의 **Channel Name**과 **Webhook URL** 항목을 입력하세요.
- [등록] 버튼을 클릭하세요.

Webhook



- 알림을 받을 Webhook을 등록하세요. 등록된 URL에 POST Method로 알림의 **title** , **text** 가 전송됩니다.

```
{
  "title": "Alert Title",
  "text": "Sample warning message"
}
```

- Webhook Name**과 **Webhook URL** 항목을 입력하세요.
- [등록] 버튼을 클릭하세요.

Webhook JSON





1. 알림을 받을 Webhook을 등록하세요. 등록된 URL에 POST Method로 알림 데이터가 JSON 형태로 전송됩니다. JSON 내에 포함 시킬 수 있는 대체 변수에 대해선 **사용 가능 변수** 부분을 참고하세요.
 - `${something}` 은 와탭에서 제공하는 대체될 값입니다. 지원하는 전체 목록과 의미는 사용 가능 변수를 참고하세요.
 - 이벤트 상태(`status`)는 이벤트 발생(`on`), 이벤트 해소(`off`)로 구분할 수 있습니다.
 - `level` 은 `None` , `Info` , `Warning` , `Critical` 로 구분합니다.

```
{
  "pcode": "${pcode}",
  "projectName": "${projectName}",
  "time": "${time}",
  "oid": "${oid}",
  "oname": "${oname}",
  "title": "${title}",
  "message": "${message}",
  "level": "${level}",
  "status": "${status}",
  "metricName": "${metricName}",
  "metricValue": "${metricValue}",
  "metricThreshold": "${metricThreshold}",
  "uuid": "${uuid}",
  "okind": "${okind}",
  "onode": "${onode}"
}
```

2. **Webhook Name**과 **Webhook URL** 항목을 입력하세요.
3. Header 값을 추가하려면 **사용자 Header 값 추가**의 + 추가를 클릭해 key, value을 추가하세요.
4. [등록] 버튼을 클릭하세요.

Opsgenie



1. **Teams** 메뉴에서 알림을 수신할 팀을 선택하세요.
2. **Integration** 메뉴로 이동해 [Add Integration] 버튼을 클릭하세요.



On-call
Integrations
Heartbeats

Integrations

3. Integration 목록에서 'API' 검색 후 선택하세요.

X

Add integration

Integrate your Opsgenie account with over 200 powerful apps and web services to sync alert data, and streamline your workflow.

API

API

API

Apica Synthetic Monitoring

API

APImetrics

API

ConnectWise Automate (API)

API

Zapier

4. API 명과 Team을 할당하고 각 권한을 설정한 후, [Save Integration] 버튼을 클릭하세요.

Forwarding rules
Your on-call schedule

ON-CALL
Global policies
All schedules
All escalations

CONNECTED APPS
Atlassian products

INTEGRATIONS
Integrations
Heartbeats
Slack
GitLab

Settings

Name:

Assigned to Team: ?

API Key: ?

Read Access: ?
☒

Create and Update Access: ?
☒

Delete Access: ?
☒

Restrict Configuration Access: ?
☐

Enabled: ?
☒

Suppress Notifications: ?
☐



5. 와탭 모니터링 서비스의 **서드 파티 플러그인 추가** 창으로 돌아와, **Opsgenie** 탭 안내 하단의 **Name**과 **API Key** 항목을 입력하세요.
6. [등록] 버튼을 선택하세요.

PagerDuty



1. [PagerDuty](#) 계정에 등록하고 로그인하세요.
2. PagerDuty에서 **Services > Service Directory** 메뉴에서 [+ New Service] 버튼을 클릭하세요.

PagerDuty

3. Service 정보(**Name**)를 입력한 후 [Next] 버튼을 클릭하세요.

PagerDuty

4. Escalation Policy를 설정 후 [Next] 버튼을 클릭하세요.

PagerDuty

5. **Alert Grouping**과 **Transient Alerts** 항목을 설정한 후 [Next] 버튼을 클릭하세요.

PagerDuty

6. **Integrations**에서 **Event API V2**를 선택한 후 [Create Service] 버튼을 클릭하세요.

PagerDuty

7. 생성한 Service 화면에서 **Integration Name**과 **Integration Key** 값을 복사하세요.

PagerDuty

8. 와탭 모니터링 서비스의 **서드 파티 플러그인 추가** 화면으로 돌아와 **Integration Name**과 **Integration Key** 항목을 입력하세요.

9. [등록] 버튼을 클릭하세요.

ⓘ 메시지를 수신하지 못했거나 플러그인이 등록되지 않았다면 **Integration Name** 또는 **Integration Key**값이 올바른지 확인하세요.

LINE



1. LINE 앱을 설치합니다.
2. 아래 QR 코드를 스캔하여 WhaTapLabs 공식 채널을 친구로 추가합니다.



3. 다음 명령어를 사용하여 프로젝트를 라인과 연동하고 알림을 설정하세요.

명령어

```
/help # 사용 가능한 명령어 안내
/list # 연동된 프로젝트 목록 조회
/license [엑세스키] # 새 프로젝트 연동 추가
/remove [프로젝트코드] # 프로젝트 연동 해제
/language [ko|ja|en] # 알림 언어 설정 (한국어/일본어/영어)
```

- 프로젝트 액세스 키는 **관리 > 프로젝트 관리**에서 확인하실 수 있습니다.
- 라인 내에서 `/language` 명령어를 사용하는 것은 라인 내 채팅방에만 적용됩니다. 다른 3rd 플러그인이나 프로젝트의 알림 수신 언어가 변경되는 것은 아닙니다.

사용 예시

```
/license XXXXXXXXXX # 프로젝트 연동
/language ko # 한국어로 언어 설정
```



```
/list # 연동된 프로젝트 확인
```



- 프로젝트 액세스 키: WhaTap 프로젝트 내 **관리 > 프로젝트 관리**에서 확인할 수 있음
- 언어 설정: `/language` 명령어는 LINE 채팅방 내에서만 적용되며, 다른 알림 채널의 언어는 변경되지 않음

ilert



1. ilert 콘솔에서 **Alert sources** 화면의 오른쪽 위의 [+ Create alert source]를 클릭하세요.
2. **Integration type** 단계의 하단에 있는 **Filter integrations** 검색창에 WhaTap 을 입력해 검색합니다.
3. 검색 결과에서 **WhaTap** 타일을 선택한 후 [Next] 버튼을 클릭합니다.
4. 알림 소스 이름을 입력하고 팀을 지정한 후 [Next] 버튼을 클릭합니다.
 - **에스컬레이션 정책**은 새 정책을 생성하거나 기존 정책을 선택할 수 있습니다.
5. 알림 그룹화 방식을 선택한 후 [Continue setup] 버튼을 클릭합니다.
 - 우선 선택한 **Do not group alerts**는 이후 변경할 수 있습니다.
6. 다음 화면에서 **알림 템플릿**, **우선순위** 등 추가 설정을 할 수 있습니다. 우선 [Finish setup] 버튼을 클릭해 설정을 완료합니다.
7. 설정이 완료되면 완료 화면에서 **API 키** 또는 **Webhook URL**이 생성됩니다.
8. **Webhook JSON** 탭에서 생성된 **Webhook URL**을 복사해 아래의 **Webhook URL** 입력란에 붙여넣습니다.
9. [등록] 버튼을 클릭하세요.

대량 알림 발생 방지

알림이 대량으로 발생하면 지정한 시간 동안 알림이 일시적으로 중지됩니다. 예를 들어, 5분 동안 20회의 이벤트가 발생하면 5분

동안 경고 알림을 중지합니다. 설정한 **정지 시간** 시간이 지나면 대량 알림 발생 방지 기능은 해제됩니다.

1. **경고 알림 > 이벤트 수신 설정의 대량 알림 발생 방지** 섹션으로 이동하세요.
2. 토글 버튼을 클릭해 **활성화** 또는 **비활성화** 할 수 있습니다.
 -  **활성화**: 대량 알림 일시적 중지
 -  **비활성화**: 대량 알림 재개
3. **탐지 시간, 탐지 횟수, 정지 시간**을 설정하세요.
 - **탐지 시간** 동안 **탐지 횟수** 이상의 이벤트가 발생하면 **정지 시간** 동안 경고 알림을 중지합니다.

❗ 대량 알림으로 차단되는 경우 차단 안내 박스가 표시됩니다. 대량 알림 차단 기능을 해제하려면 박스의 [대량 알림 발생 중지] 버튼을 클릭하세요.

이벤트 수신 포맷

공용 알림 템플릿

공통 템플릿은 대부분의 경우 적용 가능합니다. 다양한 환경에서 동일한 포맷으로 알림을 받을 수 있습니다.

- Product Type: 애플리케이션, 데이터베이스, 쿠버네티스
- Event Type: 애플리케이션 알림, 데이터베이스 알림, 메트릭스 알림
- Event Channel: sms, mobile, 3rd party plugin, plugin

이벤트 제목

Event title format

```
[Level][Platform][ProjectName][ApplicationName][EventTitle]
```

Event title example

```
[Info][JAVA][애플리케이션 프로젝트][TC-0-1-8081][CRITICAL_HIGH_MEMORY]
```

ⓘ ApplicationName을 설정하지 않은 경우 이벤트 제목에서 생략합니다.

- Platform은 다음 중 한 가지로 표시합니다.
 - JAVA
 - NODEJS
 - PYTHON
 - PHP
 - DOTNET
 - GO
 - POSTGRESQL
 - ORACLE



- MYSQL
- MSSQL
- BSM_JAVA
- CLOUDWATCH
- TIBERO
- KUBERNETES
- KUBE_NS
- URLCHECK
- URLCHECK_ADMIN
- CUBRID
- ALTIBASE
- CLUSTER
- REDIS
- MONGODB
- VR
- RUM

이벤트 메시지

이벤트 메시지에 포함할 수 있는 정보입니다. `optional` 이 `false` 인 경우 항상 메시지에 포함합니다. `optional` 이 `true` 인 경우 해당 데이터를 확인할 수 있으면 표시합니다.

Event message example

```
Project Name : 애플리케이션 프로젝트
Project Code : 3
Agent Name : TC-0-1-8081
Message : RECOVERED: Memory is too high. less than 10%
Event Time : 2022-04-12 18:53:24 +0900
Event OFF Time : 2022-04-12 18:53:24 +0900
Alert Type : APPLICATION_MEMORY
```

Metric Name : memory
 Metric Value : 20
 Metric Threshold : 10
 Stateful : true

표 | 이벤트 메시지 구성 요소

En	Ko	지원되는 알림 타입	설명
Project Name	프로젝트 이름	전체	-
Project Code	프로젝트 Code	전체	-
Agent Name	에이전트 이름	전체(optional)	oname
Message	이벤트 메시지	전체	-
Alert Type	이벤트 종류	전체	아래의 AlertType 종류 표 참고
Event Time	이벤트 발생 시간	전체	2022-04-13 10:40:49 +0900에서 +0900는 GMT를 의미합니다.
Event Off Time	이벤트 해제 시간	전체(optional)	2022-04-13 10:40:49 +0900에서 +0900는 GMT를 의미합니다.
Metric Name	메트릭스 이름	전체(optional)	이벤트 조건 판단에서 사용하는 메트릭스의 이름
Metric Value	메트릭스 값	전체(optional)	메트릭스 값이 메트릭스 임계치를 넘으면 이벤트 발생 조건이 만족한 경우입니다.
Metric Threshold	메트릭스 임계치	전체(optional)	메트릭스 값이 메트릭스 임계치를 넘으면 이벤트 발생 조건이 만족한 경우입니다.
Stateful	해소된 이벤트 알림	전체(optional)	해소된 이벤트 알림 기능 사용 중이면 true, 아니면 false
Event Rule	이벤트 발생 조건	메트릭스 알림	-

En	Ko	지원되는 알림 타입	설명
Target Filter	이벤트 대상 선택	메트릭스 알림	특정 대상에서 수집된 메트릭스에 대해서만 이벤트 조건을 확인합니다.
Repeat Count	이벤트 반복 횟수	메트릭스 알림	이벤트 조건이 이벤트 반복 시간동안 이벤트 반복 횟수만큼 만족해야 이벤트가 발생합니다.
Repeat Duration	이벤트 반복 시간	메트릭스 알림	이벤트 조건이 이벤트 반복 시간동안 이벤트 반복 횟수만큼 만족해야 이벤트가 발생합니다.
Receiver	수신자	메트릭스 알림	-
Query	MXQL 쿼리	복합 메트릭스 알림	-
Rule	이벤트 발생 조건	복합 메트릭스 알림	-
Query Period	쿼리 기간	복합 메트릭스 알림	-
Query Interval	쿼리 간격	복합 메트릭스 알림	-
Silent Time	무음 시간	복합 메트릭스 알림	-
Query	URL	Exception 알림	Exception을 발생시킨 요청의 URL
TXID	트랜잭션 ID	Exception 알림	-
Class	에러 클래스 이름	Exception 알림	-

En	Ko	지원되는 알림 타입	설명
Log Message	로그 메시지	서버 - 파일 로그 알림	-
Log File	로그 파일 경로	서버 - 파일 로그 알림	-
IP	IP	서버 알림 전체	-
CPU	CPU	서버 알림 전체	이벤트 발생 당시의 Snapshot
CPU_load1	CPU_load1	서버 알림 전체	이벤트 발생 당시의 Snapshot
CPU_loadPerCore	CPU_loadPerCore	서버 알림 전체	이벤트 발생 당시의 Snapshot
Memory	Memory	서버 알림 전체	이벤트 발생 당시의 Snapshot
Swap	Swap	서버 알림 전체	이벤트 발생 당시의 Snapshot
Disk Name Used Percent Free Size IO Percent	디스크 퍼포먼스	서버 알림 전체	이벤트 발생 당시의 Snapshot
Name Bps Pps	트래픽 퍼포먼스	서버 알림 전체	이벤트 발생 당시의 Snapshot
Message Time Name	처리내역 메시지	서버 알림 전체	-

ⓘ 해당 이벤트에서 제공할 수 있는 최대한 많은 정보를 보여줍니다.

- AlertType은 다음 중 한 가지로 표시합니다.

AlertType	설명
APPLICATION_CPU	애플리케이션 CPU 알림
APPLICATION_MEMORY	애플리케이션 MEMORY 알림



AlertType	설명
APPLICATION_DISK	애플리케이션 DISK 알림
APPLICATION_ACTIVE_TRANSACTION	애플리케이션 액티브 트랜잭션 알림
APPLICATION_ERROR_TRANSACTION	애플리케이션 에러 트랜잭션 알림
APPLICATION_SLOW_TRANSACTION	애플리케이션 트랜잭션 응답시간 알림
METRICS	메트릭스 알림
COMPOSITE_METRICS	복합 메트릭스 알림
ANOMALY	이상치 탐지 알림
LOG_REALTIME	로그 실시간 알림
COMPOSITE_LOG	복합 로그 알림
SERVER_REBOOT	서버 - 재시작 알림
SERVER_NO_DATA	서버 - 미수신 알림
SERVER_PORT	서버 - 포트 알림
SERVER_NETWORK_IOPS	서버 - 네트워크 IOPS 알림
SERVER_NETWORK_BPS	서버 - 네트워크 BPS 알림
SERVER_DISK_IO	서버 - 디스크 I/O 알림
SERVER_DISK_QUOTA	서버 - 디스크 사용량 알림
SERVER_DISK_INODE	서버 - inode 알림



AlertType	설명
SERVER_CPU	서버 - CPU 알림
SERVER_MEMORY	서버 - 메모리 알림
SERVER_CPU_STEAL	서버 - steal 알림
SERVER_MEMORY_SWAP	서버 - 스왑 알림
SERVER_LOG_FILE	서버 - 로그 파일 알림
SERVER_WINDOW_EVENT	서버 - 윈도우 이벤트 알림
SERVER_OFF	서버 - 알림 OFF 알림
SERVER_ACKNOWLEDGE	서버 - 처리내역 알림
SERVER_PROCESS_COUNT	서버 - 프로세스 수 알림
SERVER_PROCESS_CPU	서버 - 프로세스 CPU 알림
SERVER_PROCESS_MEMORY	서버 - 프로세스 메모리 알림
SERVER_PROCESS_OFF	서버 - 프로세스 알림 OFF 알림
AGENT_ACTIVE	에이전트 활성화 알림
AGENT_INACTIVE	에이전트 비활성화 알림
AGENT_REACTIVATED	에이전트 재활성화 알림
URL	URL 알림
TOO_MANY_EVENT	너무 많은 이벤트 발생 알림



AlertType	설명
CLOUD_WATCH	Cloud Watch 알림
EXCEPTION	Exception 알림

이벤트 기록 및 모니터링

홈 > 프로젝트 선택 >  경고 알림 > 이벤트 기록

이벤트 기록은 프로젝트에서 발생한 여러 이벤트를 조회하고 상세 정보를 분석할 수 있습니다. Elasticsearch DSL 쿼리를 지원하며, 원하는 조건에 맞는 이벤트를 정확하고 빠르게 찾을 수 있습니다.

이벤트 기록 조회하기

검색 결과에서 **이벤트 제목**을 클릭하면 해당 이벤트가 발생한 시간대의 상세 데이터를 분석할 수 있는 화면으로 이동합니다. 이를 통해 이벤트 발생 전후 상황을 종합적으로 파악할 수 있습니다.

1. 경고 알림 > 이벤트 기록으로 이동하세요.
2. 이벤트 기록 화면의 시간 선택에서 이벤트 기록을 조회할 기간을 설정하세요.
3. 필터 입력 창에 쿼리를 입력하고 [돋보기] 버튼을 클릭하세요.
 - 쿼리를 입력하지 않으면 전체 이벤트가 조회됩니다.

컬럼 설정

원하는 컬럼을 표시하거나 숨길 수 있습니다.

1. 이벤트 기록 화면의 왼쪽 위 [ 컬럼 설정] 버튼을 클릭하세요.
2. 컬럼 설정 창에서 표시하거나 숨길 컬럼을 선택하세요.
 - 표시 항목에서 컬럼의 순서를 변경할 수 있습니다.
 - 컬럼명 검색창에 원하는 컬럼 항목을 검색할 수 있습니다.

컬럼 항목	설명
이벤트 이름	이벤트의 제목
메시지	이벤트의 메시지 또는 스냅샷 정보

컬럼 항목	설명
이벤트 상태	이벤트의 현재 상태
에이전트 명	이벤트가 발생한 대상 에이전트의 이름(Oname) - 특정 에이전트에 대해 발생한 이벤트가 아닌 경우 빈칸으로 표시됨
에이전트 그룹	이벤트가 발생한 대상 에이전트의 종류(OkindName) - 특정 에이전트에 대해 발생한 이벤트가 아닌 경우 빈칸으로 표시됨
에이전트 노드	이벤트가 발생한 대상 에이전트의 서버(OnodeName) - 특정 에이전트에 대해 발생한 이벤트가 아닌 경우 빈칸으로 표시됨
이벤트 발생 시각	이벤트가 발생한 시간
이벤트 해소 시각	이벤트가 해소된 시간 상태가 없는 이벤트의 경우 - 로 표시됨

3. 설정을 완료한 후, [확인] 버튼을 클릭해 컬럼 설정을 반영합니다.

↓ CSV 다운로드

조회 결과를 CSV 파일 형식으로 다운로드할 수 있습니다.

1. 경고 알림 > 이벤트 기록에서 [CSV] 버튼을 클릭하세요.
2. 현재 필터 조건에 맞는 이벤트 목록이 CSV 파일로 저장됩니다.

진행 중인 이벤트만 보기

현재 진행 중인 상태의 이벤트만 조회할 수 있습니다.

1. 경고 알림 > 이벤트 기록에서 [진행 중인 이벤트만 보기] 버튼을 클릭하세요.
2. 필터 쿼리에 다음 조건이 자동으로 추가되어 검색됩니다.

```
Stateful: true and Status : "ON"
```

이벤트 검색

- **정확한 검색:** 원하는 조건을 정확히 지정하여 필요한 이벤트만 조회
- **복합 조건:** 여러 필드를 동시에 검색하여 복잡한 조건도 한 번에 처리
- **유연한 패턴:** 와일드카드, 부분 검색 등 다양한 검색 방식 지원
- **빠른 성능:** 인덱싱된 데이터를 활용한 고속 검색

검색 가능한 필드

필드와 값에 대해 대소문자를 구분하지 않습니다.

- **필드명 태그:** 필드가 지원되는 이벤트 타입
- **필드 타입:** 필드의 데이터의 타입
 - : Number
 - : String
 - : Boolean
 - : Date

이벤트 정보 필드

필드명	타입	설명	예시 값
Title	String	이벤트 제목	"Database Connection Error"
OffTitle	String	이벤트 해소 제목	"RECOVERED: Database Connection Error"
Message	String	이벤트 메시지	"Connection timeout occurred"
OffMessage	String	이벤트 해소 메시지	"RECOVERED: Connection timeout occurred"
Level	String	현재 이벤트 레벨	Critical, Warning, Info

필드명	타입	설명	예시 값
OriginLevel	String	원본 이벤트 레벨	Critical, Warning, Info
Status	String	이벤트 상태	ON, OFF, CANCEL, ACKNOWLEDGE, MAINTENANCE, DISABLED
ActCount	Number	처리내역 개수	2
MetricName	String	지표 이름	"memory"
MetricValue	String	지표 값	"85.5"
OffValue	String	해소 값	"72.8"
MetricThreshold	String	임계치	"80"
alertType	String	이벤트 종류	"BASIC", "METRICS", "TRANSACTION" 등
alertId	String	이벤트 규칙의 고유식별자	"zf3uojer0fv4v7"

이벤트 타입별 지원 필드

ⓘ 특정 이벤트 타입에서만 지원되는 필드입니다. 해당 이벤트 타입이 아닌 경우 값이 없을 수 있습니다.

필드명	타입	이벤트 종류	설명	예시 값
eventRule	String	기본, 메트릭스	이벤트 발생 규칙	"memory ≥ 80"
field	String	실시간 로그	로그 검색 키	"content"

필드명	타입	이벤트 종류	설명	예시 값
keyword	String	실시간 로그	로그 검색 값	"Error"
logCategory	String	실시간 로그	로그 카테고리	"AppLog"
logContent	String	실시간 로그	로그 내용	"00:00000:00009:2025/04/06 23:03:52.55 server Error: 1601, Severity: 17, State: 3\n00:00000:00009:2025/04/06 23:03:52.55 server There are not enough 'user connections' available to start a new process."

대상 필드

필드명	타입	설명	예시 값
Oid	Number	에이전트 고유식별자	-98765432
Oname	String	에이전트 이름	"web-server-01"
Okind	Number	에이전트 종류 고유식별자	867318026
OkindName	String	에이전트 종류명	"web-server"
Onode	Number	에이전트 서버 고유식별자	334634079
OnodeName	String	에이전트 서버명	"production-node-1"

이벤트 고유값 필드

필드명	타입	설명	예시 값
Id	Number	이벤트의 고유식별자	5768121

필드명	타입	설명	예시 값
UUID	String	이벤트 고유식별자	"550e8400-e29b-41d4-a716"

상태/플래그 필드

필드명	타입	설명	예시 값
Stateful	Boolean	상태 기반 이벤트 여부	true, false
Disabled	Boolean	종료된 이벤트 여부	true, false
Escalation	Boolean	에스컬레이션 여부	true, false
SystemEvent	Boolean	시스템 이벤트 여부	true, false

검색 유형별 문법

❗ 검색 기본 문법은 [WhaTap log search query 문법](#) 문서를 참고하시기 바랍니다.

1. 키워드 검색

Database Connection 문자열이 포함된 이벤트

```
title: "Database Connection"
```

2. 여러 값 검색

여러 옵션 중 하나라도 포함되는 이벤트를 조회합니다.

```
title: Database Connection
```

현재 이벤트 레벨이 Info이거나 Warning인 이벤트

```
level: info warning
```

3. 패턴 검색

와일드카드를 사용하여 패턴을 검색할 수 있습니다.

이름 패턴으로 특정 에이전트에서 발생한 이벤트 찾기

```
oname: web-*-prod
```

제목이 Connection으로 끝나는 이벤트 찾기

```
title: *Connection
```

4. 복합 조건 검색

여러 조건을 조합하여 정확히 검색할 수 있습니다.

Critical 레벨이면서 제목에 Database가 포함된 이벤트

```
level: critical and title: Database
```

특정 에이전트의 Warning 또는 Critical 이벤트

```
oname: web-server-01 and level: Warning Critical
```

5. OR 조건 검색

여러 조건 중 하나라도 만족하는 이벤트를 조회합니다.

제목 또는 메시지에 특정 키워드가 포함된 이벤트

```
title: Connection or message: Connection
```

6. 제외 조건

특정 조건을 제외해 검색할 수 있습니다.

Info 레벨을 제외한 모든 이벤트

not level: info

실시간 알림

실시간 알림 기능은 이벤트 설정을 통해 설정한 이벤트가 발생할 때 팝업 형태 표시됩니다. 이벤트 발생 즉시 알림을 받아 문제를 빠르게 인지하고 대응할 수 있습니다. 이미 발생했거나 놓친 알림 내역을 확인하여 실시간 대응이 어려웠던 상황을 파악하고 해결할 수 있습니다.

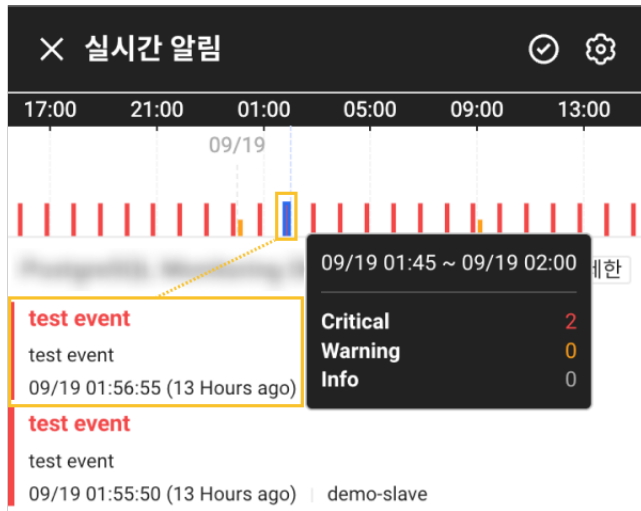
실시간 알림 확인하기

실시간 알림은 화면 오른쪽 위 팝업 형태로 표시됩니다. 알림이 발생한 시간, 제목, 메시지를 확인할 수 있습니다.

- 개별 알림을 닫으려면 메시지 오른쪽 상단의 ✕ 버튼을 클릭하세요.
- 화면에 표시된 모든 팝업 알림을 닫으려면 **전체 알림 닫기**을 클릭하세요.

알림 내역 확인하기

1. 프로젝트를 선택해 진입한 화면의 가장 위에 🔔 아이콘을 클릭하세요.
2. 실시간 알림 창이 나타납니다.
 - 현재 프로젝트의 최근 24시간 동안의 알림을 최대 100개까지 확인할 수 있습니다.
 - 개별 이벤트 항목을 선택하면 관련 메뉴로 이동합니다.
 - 실시간 알림 창의 시간별 차트에서 원하는 시간대를 선택하면 해당 이벤트 항목으로 이동할 수 있습니다.



- 전체 알림 내역을 확인하려면 **전체 알림 기록** 버튼을 선택하세요. **경고 알림 > 이벤트 기록** 메뉴로 이동합니다.

❗ **실시간 알림** 목록이 비어 있을 경우, [전체 알림 기록] 버튼이 표시됩니다. 수신 태그 미설정 알림 받기 옵션을 해제하세요.

이벤트 일괄 해소하기

실시간 알림 목록에서 진행 중인 모든 이벤트를 일괄 해소합니다. 이벤트 해소 작업 완료까지 약 30초에서 1분 정도 소요됩니다.

- **이벤트 일괄 처리** 기능을 사용하면 현재 진행 중인 이벤트에 대한 해소 알림이 다량 발생할 수 있습니다.
- **이벤트 일괄 처리** 기능을 사용한 후에도 이벤트 규칙이 활성화되어 있고, 데이터가 임계치를 초과했다면 이벤트는 다시 발생할 수 있습니다.
- 이벤트 해소 알림은 **경고 알림 > 이벤트 설정** 메뉴에서 이벤트 수정을 통해 비활성화할 수 있습니다. **이벤트 상태가 해소되면 추가 알림 또는 해소된 알림** 옵션을 비활성화하세요.

사용 방법:

1. 프로젝트를 선택해 진입한 화면 상단의 🔔 아이콘을 클릭하세요.
2. 실시간 알림 창이 나타나면 오른쪽 상단의 ⏸ 아이콘을 클릭하세요.

3. 실시간 알림 목록에서 진행중인 이벤트를 일괄 해소합니다. 메시지 창이 나타나면 [해소] 버튼을 클릭하세요.

실시간 알림 설정하기

1. 프로젝트를 선택해 진입한 화면 상단의 🔔 아이콘을 클릭하세요.
2. 실시간 알림 창이 나타나면 오른쪽 상단의 ⚙️ 아이콘을 클릭하세요.
3. 실시간 알림 설정 창에서 각 항목을 설정하세요.
 - 팝업 알림: 실시간 알림 창이 닫힌 상태에서도 알림을 팝업 형태로 제공합니다.
 - 해소된 이벤트 보기: 실시간 알림 목록에서 해소된 이벤트를 포함해 확인할 수 있습니다.
 - 알림음 미리 듣기: 브라우저에서 발생하는 알림음을 미리 들을 수 있습니다. Critical 또는 Warning 옆의 🔊 버튼을 클릭하세요. 알림음이 들리지 않으면 브라우저 설정을 확인하시기 바랍니다.

시스템 이벤트

와탭 모니터링은 플랫폼 전반에서 자동으로 탐지 및 생성되는 공용 이벤트를 제공합니다. 이 문서는 시스템에 의해 발생하는 이벤트의 유형 및 발생 조건, 대응 방법에 대해 안내합니다.

EVENT_BLOCKED_BY_SYSTEM

프로젝트에서 짧은 시간에 과도한 이벤트가 발생하면, 와탭 시스템이 이를 탐지하여 이벤트를 차단하고 다음 메시지를 사용자에게 전달합니다. 이벤트가 차단되었다면 사용자의 이벤트 설정을 점검하세요.

 위험



이벤트 메시지

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

프로젝트 번호	8
프로젝트 이름	new server
대상	server agent
이벤트 이름	EVENT_BLOCKED_BY_SYSTEM
발생 시각	(GMT+0900) 2024-11-15 18:24:15

와탭에 로그인하기

new server 프로젝트의 server agent에서 과도한 이벤트가 탐지되어 이벤트가 차단됩니다. server agent에 일정 기간 이벤트가 발생하지 않으면 자동으로 차단 해제됩니다.

차단 기준

이벤트를 차단하는 기준은 다음과 같습니다.

1. 에이전트 단위 차단

한 개의 에이전트에서 1분 내에 10개의 이벤트가 발생하면 해당 에이전트에서 발생하는 이벤트를 차단합니다.

2. 다중 에이전트 차단 시 전체 차단

1의 경우로 이벤트가 차단된 에이전트가 1분 내에 3개 이상이 되는 경우 프로젝트 전체에서 발생하는 이벤트를 차단합니다.

3. 프로젝트 단위 차단

한 개의 프로젝트에서 1분 내에 100개의 이벤트가 발생하면 프로젝트 전체에서 발생하는 이벤트를 차단합니다.

해제 방법

시스템에 의해 이벤트가 차단된 경우, 1분 동안 대상 에이전트 또는 프로젝트에서 이벤트가 발생하지 않아야 합니다.

- 경고 알림 > 이벤트 설정 메뉴에서 설정한 이벤트를 모두 비활성화하세요. 이벤트 설정을 점검하여 과도한 이벤트가 발생하지 않도록 임계치를 조정해야 합니다.
- 이벤트를 설정하기 전 시뮬레이션 기능을 활용해 이벤트 발생 횟수를 예측해볼 수 있습니다.

네트워크 대역폭 사용량

네트워크 대역폭 사용량 메뉴에서 디바이스 및 인터페이스의 과거 트래픽 추이를 조회할 수 있습니다. 최대 31일 범위의 히스토리 데이터를 분석하여 장기 트렌드를 파악합니다.

기본 화면 및 설정

1. 사용량 분석 상단 옵션 바 시간 선택에서 조회할 시간 범위를 선택하세요. 최대 31일까지 설정 가능합니다.

- 1분을 클릭하면 데이터 조회 구간을 변경할 수 있습니다.

빠른 선택 옵션	설명
최근 5분	최근 5분 데이터 조회
최근 10분	최근 10분 데이터 조회
최근 1시간	최근 1시간 데이터 조회
최근 1일	최근 24시간 데이터 조회 (기본값)
최근 7일	최근 7일 데이터 조회
최근 21일	지난 21일 데이터 조회
금일 (0~24h)	금일 00시 부터 23:59분 까지 조회
1일전 (0~24h)	1일전 00시 부터 23:59분 까지 조회
7일전 (0~24h)	7일전 00시 부터 23:59분 까지 조회

2. 상단 옵션 바 매니저 선택에서 데이터를 수집하는 NMS 매니저를 선택하세요.

3. 디바이스 선택 영역에서 조회할 디바이스 또는 인터페이스를 선택해 사용량을 분석할 수 있습니다.

- 디바이스 목록: 등록된 디바이스가 이름순으로 정렬되어 표시됩니다. 각 디바이스를 확장하면 해당 디바이스의

인터페이스 목록이 표시됩니다.

선택 레벨	설명
디바이스	디바이스 전체 트래픽 추이 표시
인터페이스	특정 인터페이스 상세 추이 표시

차트 옵션

• 단위 표시

트래픽 데이터는 자동으로 적절한 단위로 변환됩니다.

값 범위	단위
0 ~ 1,000	bps
1,000 ~ 1,000,000	Kbps
1,000,000 ~ 1,000,000,000	Mbps
1,000,000,000 이상	Gbps

• 톨팁

차트 위에 마우스를 올리면 해당 시점의 상세 값을 확인할 수 있습니다. 여러 시리즈의 값이 동시에 표시됩니다.

네트워크 대역폭 사용량 - 디바이스

디바이스 선택 영역에서 디바이스를 선택하면, 해당 디바이스의 전체 트래픽 추이가 차트로 표시됩니다.

기본 차트

차트	설명
Total Throughput	전체 처리량(전체 너비)
Inbound Throughput	인바운드 트래픽
Outbound Throughput	아웃바운드 트래픽

Private MIB 위젯

디바이스에 커스텀 OID가 설정된 경우 해당 지표의 차트가 추가로 표시됩니다. 위젯 설정은 로컬 스토리지에 저장됩니다.

네트워크 대역폭 사용량 - 인터페이스

디바이스 선택 영역에서 특정 인터페이스를 선택하면, 해당 인터페이스의 상세 추이가 표시됩니다. [사용량 현황](#)의 인터페이스 뷰와 동일한 레이아웃입니다.

차트

- 트래픽 추이 (bps)
- PPS 추이 (packets per second)
- 에러 추이

조회 결과 다운로드

조회한 화면을 파일로 저장할 수 있습니다.

1. 상단 옵션 바 오른쪽 **다운로드** 버튼을 클릭하세요.
2. 드롭다운에서 저장 형식을 선택하세요.

Item	Description
PDF	화면을 A4 규격 문서로 저장. 내용이 길면 여러 페이지로 나뉨
PNG	화면을 이미지 한 장으로 저장

캡처 범위는 오른쪽 차트 영역이며, 왼쪽 **디바이스 선택** 패널은 포함되지 않습니다. 스크롤 때문에 화면에 보이지 않는 영역까지 함께 저장됩니다.

저장한 파일 위쪽에는 다음 정보가 함께 기록됩니다.

- 날짜(조회 기간)
- 프로젝트 이름
- Manager
- 대상(디바이스 또는 인터페이스)

❗ 조회할 데이터가 없으면 **다운로드** 버튼은 비활성 상태로 표시됩니다. 저장에 실패하면 파일 또는 이미지 다운로드 실패 안내가 표시됩니다.

URL 파라미터

페이지 URL에 파라미터를 포함하여 특정 조건으로 직접 접근할 수 있습니다.

파라미터	설명
oid	NMS 매니저 OID
host	디바이스 Host IP
idx	인터페이스 Index
stime	시작 시간(timestamp)

파라미터	설명
etime	종료 시간(timestamp)

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.

최근 IT 서비스 구축 환경은 MSA(Microservice Architecture) 또는 Kubernetes 기반으로 전환되면서 관리 대상이 증가하고 있습니다. 일반적인 로그 모니터링은 서버에 접속해 `tail` 명령어나 편집기를 통해 확인합니다. 하지만 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 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 관리합니다. 개별 서버에 접근하지 않아도 중앙에서 로그를 확인할 수 있어 편리합니다.

- 모든 로그 수집

로그를 선별해서 수집하는 경우 중요한 데이터가 누락될 수 있습니다. 와탭은 모든 로그를 수집하며, 수집된 로그들은 **라이브 테일**에서 실시간으로 확인할 수 있습니다.

- 가시성 확보

와탭의 다양한 차트에서 로그를 확인할 수 있습니다. 이를 통해 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. 와탭을 통해 로그를 중앙에 모은다면, 개별 서버에서 발생하는 로그 파일을 유지할 필요없이 중앙에 적재된 로그 데이터의 유지 기간만 관리하면 됩니다.

- 다양한 분석 관점

장애 상황을 파악하고 예측하기 위해 다양한 관점으로 로그를 분석할 수 있어야 합니다. 와탭은 특정 태그를 포함한 로그 건수 추이를 확인하거나 필터링하여 분석할 수 있으며, 자주 사용하는 패턴은 차트로 저장해 언제든지 조회할 수 있습니다.

• 패턴 알림

장애 패턴을 알림으로 설정하여 문제를 예방하거나 빠르게 인지할 수 있습니다. 와탭은 개별 로그를 기준으로 특정 키워드가 포함되면 알림을 받는 **실시간 로그 알림**과, 특정 태그가 포함된 로그 건수 추이를 기준으로 알림을 받는 **복합 로그 알림**을 제공합니다.

로그 분석

라이브 테일

라이브 테일 메뉴에서 실시간으로 수집된 로그를 `tail` 명령어처럼 화면을 통해 흘러가는 로그를 조회할 수 있습니다.

❗ 자세한 내용은 [라이브 테일](#) 문서를 참고하세요.

로그 트렌드

로그 트렌드 메뉴에서 수집되는 전체 로그 또는 특정 태그가 포함된 로그의 건수 추이를 확인할 수 있습니다. 로그 발생 건수는 장애 발생 및 해소 시점과 밀접하게 연관되므로, 로그 발생 건수 추이를 통해 장애 원인을 분석하고 대응 속도를 높일 수 있습니다.

❗ 자세한 내용은 [로그 트렌드](#) 문서를 참고하세요.

로그 검색

로그 검색 메뉴에서 수집되는 전체 로그 또는 특정 태그가 포함된 로그를 조회할 수 있습니다. 특정 시간대나 서버에서 발생한 로그를 태그를 기준으로 조회하고 확인할 수 있습니다. 인접 로그 기능을 사용하면 특정 Error 또는 Exception 발생 전후의 로그를 함께 확인하여 원인 분석에 활용할 수 있습니다.

❗ 자세한 내용은 [로그 검색](#) 문서를 참고하세요.

로그 탐색

로그 탐색 메뉴를 통해 로그 데이터를 빠르게 검색, 필터링, 분석할 수 있습니다. 필드 구조를 파악하고, 쿼리 기반 필터링을 통해 필요한 로그를 효율적으로 검색해, 결과를 데이터 시각화할 수 있습니다. 로그 탐색 기능은 Lucene 인덱스 기반으로 동작합니다.

❗ 자세한 내용은 [로그 탐색](#) 문서를 참고하세요.

로그 모니터링 적용하기

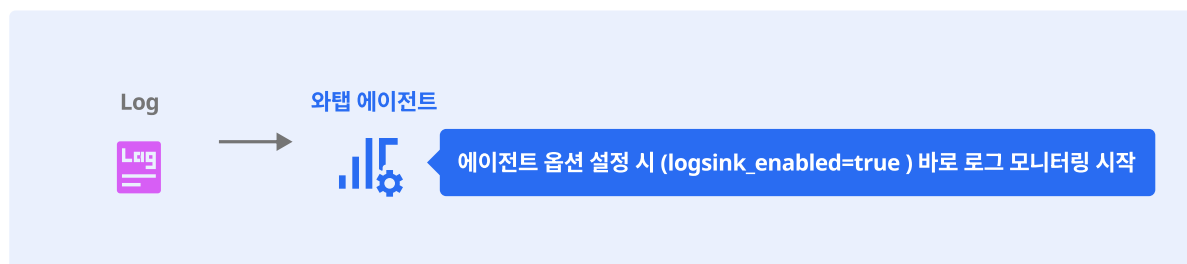
와탭 로그 모니터링 서비스 이용을 위한 기본 적용 방법을 안내합니다. 와탭 로그 모니터링은 추가적인 에이전트를 구성하거나 로그에 맞추어 parser를 적용할 필요가 없습니다. 간단한 설정으로 빠르게 시작할 수 있습니다.

로그 모니터링의 작동 원리

일반적인 로그 통합 서비스



와탭 로그 모니터링 서비스



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 수집 시간 기준

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 수집 시간 기준 시간이 와탭 에이전트가 로그를 수집한 시간에서 와탭 수집 서버의 로그 처리 시간으로 변경되었습니다.

일반적인 상황에서 변경 전과 큰 차이가 없으며, 기존 방식과 동일하게 로그를 검색할 수 있습니다. 다음과 같은 경우도 사용자의 추가적인 수정없이 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

수집 시간 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 파악에 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.
예, 한국의 경우 UTC+9 기준으로 시간을 표기합니다.

단계별 기준 시간

로그는 3단계를 거쳐 수집됩니다. 단계마다 서로 다른 기준 시간이 사용될 수 있습니다.

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.

1. 로그 발생 시간

모니터링 대상의 시간 또는 Logging 정책에 따라 편차가 발생할 수 있습니다.

2. 에이전트 수집 시간

사용 중인 제품 또는 에이전트가 로그를 수집하는 방법 및 생성되는 로그에 따라 편차가 발생할 수 있습니다.

- **Application**

설정에서 로그 라이브러리 또는 로그 파일에서 실시간에 가깝게 로그를 수집합니다.

❗ 로그 라이브러리는 Java 제품만 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.

로그 모니터링 적용하기

사용하는 애플리케이션에 따른 적용 방법은 다음과 같습니다. 로그 모니터링을 적용하기 전, [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.

Node.js

Node.js 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

Java 애플리케이션에서 로그 수집을 위한 설정 방법을 안내합니다.

에이전트 업데이트

자바 에이전트 2.1.1 버전부터 가능합니다. 업데이트 방법은 [다음 문서](#)를 참고하세요.

에이전트 설정 확인

홈 화면 > 프로젝트 선택 > 로그 > 로그 설정

1. 와탭 모니터링 서비스 초기 화면에서 프로젝트를 선택한 후, **로그 > 로그 설정** 메뉴로 이동하세요.
2. 로그 모니터링 시작하기 탭의 **1. 에이전트 설정 확인**의 안내를 참고해 에이전트 설정을 확인하세요.

에이전트 설정하기

1. 프로젝트의 **관리 > 에이전트 설정** 메뉴를 클릭하세요.
2. 옵션 작성의 **옵션 선택** 드롭 다운 목록에서 **직접 입력**을 클릭한 후, `logsink_enabled=true` 옵션을 작성하고 **적용** 버튼을 클릭해 추가하세요.
 - 키 입력창에 `logsink_enabled` 을 작성하세요.
 - 값 입력창에 `true` 을 작성하세요.
3. 로그 모니터링을 적용하기 위해 애플리케이션을 다시 시작하세요.

주요 옵션

- `hooklog_enabled` **Boolean**

기본값 `false`

Log 라이브러리를 후킹(Hooking)하여 로그 모니터링을 활성화합니다.

- ❗ 애플리케이션 실행 전, [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 사용합니다.

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 전, [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 탭의 2. 로그 모니터링 활성화에서 와탭 로그 모니터링을 활성화 또는 비활성화 할 수 있습니다.

-  로그 모니터링 활성화: 토글 버튼을 켜면 로그 모니터링이 활성화되고, 활성화한 날부터 15일 동안 무료로 체험하실 수 있습니다.
-  로그 모니터링 비활성화: 토글 버튼을 끄면 로그 모니터링이 비활성화되고, 로그를 더 이상 저장하지 않습니다.

! 로그 모니터링 활성화 권한

에이전트 설치 후 프로젝트에 대한 수정 권한이 있는 사용자만 로그 모니터링을 활성화할 수 있습니다. 권한에 대한 자세한 내용은 [다음 문서](#)를 참고하세요.

PHP

PHP 애플리케이션에서 로그 수집을 위한 설정 방법을 안내합니다.

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

1. 와탭 모니터링 서비스 초기 화면에서 프로젝트를 선택한 후, **로그 > 로그 설정** 메뉴로 이동하세요.
2. 로그 모니터링 시작하기 탭의 **1. 에이전트 설정 확인**의 안내를 참고해 에이전트 설정을 확인하세요.

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 결과를 확인하세요.

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 탭의 2. 로그 모니터링 활성화에서 와탭 로그 모니터링을 활성화 또는 비활성화할 수 있습니다.

- ☒
로그 모니터링 활성화: 토글 버튼을 켜면 로그 모니터링이 활성화되고, 활성화한 날부터 15일 동안 무료로 체험하실 수 있습니다.
- ☐
로그 모니터링 비활성화: 토글 버튼을 끄면 로그 모니터링이 비활성화되고, 로그를 더 이상 저장하지 않습니다.


로그 모니터링 활성화 권한

에이전트 설치 후 프로젝트에 대한 수정 권한이 있는 사용자만 로그 모니터링을 활성화할 수 있습니다. 권한에 대한 자세한 내용은 [다음 문서](#)를 참고하세요.

Node.js

Node.js 애플리케이션에서 로그 수집을 위한 설정 방법을 안내합니다.

에이전트 업데이트

Node.js 에이전트 0.5.1 버전부터 가능합니다. 업데이트 방법은 [다음 문서](#)를 참조하세요.

에이전트 설정 확인

홈 화면 > 프로젝트 선택 > 로그 > 로그 설정

1. 와탭 모니터링 서비스 초기 화면에서 프로젝트를 선택한 후, **로그 > 로그 설정** 메뉴로 이동하세요.
2. 로그 모니터링 시작하기 탭의 **1. 에이전트 설정 확인**의 안내를 참고해 에이전트 설정을 확인하세요.

에이전트 설정하기

1. 프로젝트의 **관리 > 에이전트 설정** 메뉴를 클릭하세요.
2. 옵션 작성의 **옵션 선택** 드롭 다운 목록에서 **직접 입력**을 클릭한 후, `logsink_enabled=true` 옵션을 작성하고 **적용** 버튼을 클릭해 추가하세요.
 - 키 입력창에 `logsink_enabled` 을 작성하세요.
 - 값 입력창에 `true` 을 작성하세요.
3. 로그 모니터링을 적용하기 위해 애플리케이션을 다시 시작하세요.

주요 옵션

- `logsink_enabled` **Boolean**

기본값 `false`

로그 모니터링 활성화 여부를 설정합니다.

- **logsink_trace_txid_enabled** Boolean

기본값 `true`

로그에 트랜잭션 ID를 삽입하여 트랜잭션 트레이스의 로그 탭 노출 여부를 설정합니다.

- **logsink_limit_content_enabled** Boolean

기본값 `true`

로그 메시지의 최대 크기 제한 여부를 설정합니다.

- **logsink_limit_content_length** Number

기본값 `10,000`

로그 메시지의 최대 길이를 설정합니다. 이 값은 `logsink_limit_content_enabled` 옵션이 `true` 로 설정된 경우에만 적용됩니다.

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 비활성화할 수 있습니다.

-  로그 모니터링 활성화: 토글 버튼을 켜면 로그 모니터링이 활성화되고, 활성화한 날부터 15일 동안 무료로 체험하실 수 있습니다.
-  로그 모니터링 비활성화: 토글 버튼을 끄면 로그 모니터링이 비활성화되고, 로그를 더 이상 저장하지 않습니다.

❗ 로그 모니터링 활성화 권한

에이전트 설치 후 프로젝트에 대한 수정 권한이 있는 사용자만 로그 모니터링을 활성화할 수 있습니다. 권한에 대한 자세한 내용은 [다음 문서](#)를 참고하세요.

Python

Python 애플리케이션에서 로그 수집을 위한 설정 방법을 안내합니다.

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

1. 와탭 모니터링 서비스 초기 화면에서 프로젝트를 선택한 후, **로그 > 로그 설정** 메뉴로 이동하세요.
2. 로그 모니터링 시작하기 탭의 **1. 에이전트 설정 확인**의 안내를 참고해 에이전트 설정을 확인하세요.

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 조회할 수 있도록 트랜잭션 아이디 {txid} 를 로그에 출력합니다. 와탭 모니터링에서 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 탭의 2. 로그 모니터링 활성화에서 와탭 로그 모니터링을 활성화 또는 비활성화할 수 있습니다.

-  로그 모니터링 활성화: 토글 버튼을 켜면 로그 모니터링이 활성화되고, 활성화한 날부터 15일 동안 무료로 체험하실 수 있습니다.
-  로그 모니터링 비활성화: 토글 버튼을 끄면 로그 모니터링이 비활성화되고, 로그를 더 이상 저장하지 않습니다.

! 로그 모니터링 활성화 권한

에이전트 설치 후 프로젝트에 대한 수정 권한이 있는 사용자만 로그 모니터링을 활성화할 수 있습니다. 권한에 대한 자세한 내용은 [다음 문서](#)를 참고하세요.

Go

Go 애플리케이션에서 로그 수집을 위한 설정 방법을 안내합니다.

에이전트 설정 확인

홈 화면 > 프로젝트 선택 > 로그 > 로그 설정

1. 와탭 모니터링 서비스 초기 화면에서 프로젝트를 선택한 후, **로그 > 로그 설정** 메뉴로 이동하세요.
2. 로그 모니터링 시작하기 탭의 **1. 에이전트 설정 확인**의 안내를 참고해 에이전트 설정을 확인하세요.

로그 수집 활성화

아래 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 탭의 **2. 로그 모니터링 활성화**에서 와탭 로그 모니터링을 활성화 또는 비활성화할 수 있습니다.

-  로그 모니터링 활성화: 토글 버튼을 켜면 로그 모니터링이 활성화되고, 활성화한 날부터 15일 동안 무료로 체험하실 수 있습니다.
-  로그 모니터링 비활성화: 토글 버튼을 끄면 로그 모니터링이 비활성화되고, 로그를 더 이상 저장하지 않습니다.

! 로그 모니터링 활성화 권한

에이전트 설치 후 프로젝트에 대한 **수정 권한**이 있는 사용자만 로그 모니터링을 활성화할 수 있습니다. 권한에 대한 자세한 내용은 [다음 문서](#)를 참고하세요.

Server

서버 애플리케이션에서 로그 수집을 위한 설정 방법을 안내합니다.

에이전트 업데이트

서버 에이전트 2.1.2 버전부터 가능합니다. 업데이트 방법은 [다음 문서](#)를 참고하세요.

에이전트 설정 확인

홈 화면 > 프로젝트 선택 > 로그 > 로그 설정

1. 와탭 모니터링 서비스 초기 화면에서 프로젝트를 선택한 후, **로그 > 로그 설정** 메뉴로 이동하세요.
2. 로그 모니터링 시작하기의 1. 에이전트 설정 확인의 OS 선택 탭에서 리눅스(shell) 또는 윈도우(Powersehll, 관리자 권한) 를 선택하세요.
3. 기본 설치 또는 카테고리 와 함께 설치를 참고해 에이전트 설정을 확인하세요.

ⓘ 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
```

• 카테고리 와 함께 설치

Linux Shell

```

1 cd /usr/whatap/infra
2 sudo mkdir extension
3
4 cat <<EOL | sudo tee extension/logsink.conf >> /dev/null
5 [[inputs.logsink]]
6   category = "serverlog"
7   ## 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
28  [[inputs.logsink.file]]
29    ## 프로젝트 코드 및 프로젝트 라이선스 입력 시, 로그를 같은 리전의 원하는 프로젝트로 전송 가능
30    # pcode = 프로젝트 코드
31    # license = "프로젝트 라이선스"
32
33  [[inputs.logsink.file]]
34    # whatap_host_ip = "수집 서버 아이피1/수집 서버 아이피2"
35    # whatap_host_port = 6600
36
37  [[inputs.logsink.file]]
38    path = "/tmp/mixed.log"
39    disabled = false

```

```

40 encoding = "utf-8"
41 ## [{"A":1,"B":2},{ "C":3,"D":4},...] 형태를 각각의 로그로 분리할 수 있다.{"A":1,"B":2} {"C":3,"D":4}
42 multiline_pattern = "simple_json_array"
43 EOL
44
45 sudo service whatap-infra restart

```

Windows Powershell

• 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"

```

• 카테고리 와 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 [[inputs.logsink.file]]
24 ## 프로젝트 코드 및 프로젝트 라이선스 입력 시, 로그를 같은 리전의 원하는 프로젝트로 전송 가능
25 # pcode = 프로젝트 코드
26 # license = "프로젝트 라이선스"
27
28 [[inputs.logsink.file]]
29 # whatap_host_ip = "수집 서버 아이피1/수집 서버 아이피2"
30 # whatap_host_port = 6600
31
32 [[inputs.logsink.file]]
33 path = "/tmp/mixed.log"
34 disabled = false
35 encoding = "utf-8"
36 ## [{"A":1,"B":2},{C":3,"D":4},...] 형태를 각각의 로그로 분리할 수 있다.{"A":1,"B":2} {"C":3,"D":4}
37 multiline_pattern = "simple_json_array"
38
39 "@
40
41 New-Item -path "C:\Program Files\WhatapInfra\extension" -name "logsink.conf" -type "file" -value $contentToAdd
42 -Force
43 Restart-Service "Whatap Infra"

```

옵션 설정

- **stats_enabled** : 수집 현황 데이터의 수집 여부를 설정합니다. (기본값: `false`)
 - `true` 로 설정해야 하며, `stats_category` 에서 설정한 카테고리(`logsink_stats`)로 통계 데이터가 발생합니다.
- **stats_category** : 수집 현황 데이터를 저장할 메트릭스 카테고리를 설정합니다. `logsink_stats` 로 값을 설정해야 합니다. 통계 데이터 필드는 다음과 같습니다.

저장되는 통계 데이터 필드: `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.
- **pcode** : 로그를 전송할 같은 리전의 프로젝트 코드를 입력합니다.
- **license** : 로그를 전송할 같은 리전의 프로젝트의 라이선스 코드를 입력합니다.

❗ **pcode** , **license** 옵션의 경우 서버 에이전트 2.7.4 버전 이상부터 지원합니다.

윈도우 이벤트 로그 옵션 설정

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

```
1 # 관리자 권한 필요
2 New-Item -type "Directory" -Path "C:\Program Files\WhatapInfra\extension"
3
4 $contentToAdd = @"
5 [[inputs.win_eventlog]]
6     category = "win_event_log"
7     stats_category = "win_event_log_stats"
8     stats_enabled = true
9     enabled = true
10 [[inputs.win_eventlog.file]]
11     #true | false
12     enabled = true
13     # Application, Security, Setup, System, ForwardedEvents
14     file = "Application"
15     #1: Information, 2: Warning 3: Error 4: Audit Success 5 Audit Fail
16     #event_type =
17     #event_id =
18     #event_id =
19     #event source name
20     #source_name = ""
```

```

21     #프로젝트 코드 및 프로젝트 라이선스 입력 시, 로그를 같은 리전의 원하는 프로젝트로 전송 가능
22     #pcode = 프로젝트 코드
23     #license = "프로젝트 라이선스"
24     #whatap_host_ip = "수집 서버 아이피1/수집 서버 아이피2"
25     #whatap_host_port = 6600
26
27     "@
28
29     New-Item -path "C:\Program Files\WhatapInfra\extension" -name "win_eventlog.conf" -type "file" -value $contentToAdd
30     -Force
31     Restart-Service "Whatap Infra"

```

- 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

① 이벤트 타입

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

- 이벤트 아이디(`event_id`) 비필수
- 이벤트 소스 이름(`source_name`) 비필수
- 프로젝트 코드(`pcode`) 비필수
- 프로젝트 라이선스 (`license`) 비필수

① 에이전트 지원 버전

- 윈도우 이벤트 로그 수집의 경우 서버 에이전트 2.5.2 버전 이상부터 지원합니다.
- 윈도우 이벤트 로그 옵션 중 `pcode` , `license` 옵션의 경우 서버 에이전트 2.7.4 버전 이상부터 지원합니다.

다중 파일 지정 및 분리

다중 파일 지정

여러 로그 파일을 동일한 카테고리로 설정하려면, 각 로그 파일 경로를 `[[inputs.logsink.file]]` 항목에 추가하고, `path` 설정을 통해 파일 경로를 지정합니다. 또한, `category` , `stats_enabled` , `stats_category` 등의 옵션을 사용하여 로그 발생량 통계 설정과 같은 부가적인 설정을 할 수 있습니다.

`/root/test1` 및 `/root/test2` 파일을 동일한 카테고리(`serverlog`)로 지정한 예시입니다.

```
[[inputs.logsink]]
  category = "serverlog"
  stats_enabled = true
```

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

```
[[inputs.logsink.file]]
```

```
path = "/root/test1"
```

```
disabled = false
```

```
encoding = "utf-8"
```

```
[[inputs.logsink.file]]
```

```
path = "/root/test2"
```

```
disabled = false
```

```
encoding = "utf-8"
```

❗ category , stats_enabled , stats_category , nowrap_keywords 등의 옵션에 대한 내용은 [옵션 설정](#)를 참고하세요.

해당 예시의 경우 **라이브 테일** 메뉴에서 다음과 같이 확인할 수 있습니다.

serverlog			
▼	oname	시간	내용
▼	APPSVR	2024-10-11 18:14:30.325	file /root/test1 pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709 kdjfhakdhgldkjgha;dfghad;fkjgha;dfkjgha;dfgjha;fkghj;fgjh
▼	APPSVR	2024-10-11 18:14:30.325	file /root/test1 pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709 kdjfhakdhgldkjgha;dfghad;fkjgha;dfkjgha;dfgjha;fkghj;fgjh
▼	APPSVR	2024-10-11 18:14:30.325	file /root/test1 pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709 kdjfhakdhgldkjgha;dfghad;fkjgha;dfkjgha;dfgjha;fkghj;fgjh
▼	APPSVR	2024-10-11 18:14:30.325	file /root/test1 pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709 kdjfhakdhgldkjgha;dfghad;fkjgha;dfkjgha;dfgjha;fkghj;fgjh
▼	APPSVR	2024-10-11 18:14:30.325	file /root/test1 pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709 kdjfhakdhgldkjgha;dfghad;fkjgha;dfkjgha;dfgjha;fkghj;fgjh
▼	APPSVR	2024-10-11 18:14:30.325	file /root/test1 pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709 kdjfhakdhgldkjgha;dfghad;fkjgha;dfkjgha;dfgjha;fkghj;fgjh
▼	APPSVR	2024-10-11 18:14:40.326	file /root/test2 pcode 34 oname APPSVR agenttime 1728638079521 oid 1988910709 sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbvcmbn.bcmn

파일 분리

서로 다른 카테고리로 로그 파일을 지정하려면, `logsink{숫자}.conf` 파일을 각각 생성한 후, 각 파일의 `category` 항목에 서로 다른값을 설정하세요.

`logsink.conf`와 `logsink1.conf`를 통해 서로 다른 로그 카테고리를 설정한 예시입니다.

logsink.conf

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

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

logsink1.conf

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

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

❗ `category` , `stats_enabled` , `stats_category` , `nowrap_keywords` 등의 옵션에 대한 내용은 [옵션 설정](#)를 참고하세요.

해당 예시의 경우 **라이브 테일** 메뉴에서 다음과 같이 확인할 수 있습니다.

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

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 비활성화할 수 있습니다.

- ☒ **로그 모니터링 활성화:** 토글 버튼을 켜면 로그 모니터링이 활성화되고, 활성화한 날부터 15일 동안 무료로 체험하실 수 있습니다.
- ☐ **로그 모니터링 비활성화:** 토글 버튼을 끄면 로그 모니터링이 비활성화되고, 로그를 더 이상 저장하지 않습니다.

❗ 로그 모니터링 활성화 권한

에이전트 설치 후 프로젝트에 대한 수정 권한이 있는 사용자만 로그 모니터링을 활성화할 수 있습니다. 권한에 대한 자세한 내용은 [다음 문서](#)를 참고하세요.

Kubernetes

쿠버네티스 컨테이너와 컨테이너 내부 애플리케이션의 로그 수집을 위한 설정 방법을 안내합니다.

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

1. 와탭 모니터링 서비스 초기 화면에서 프로젝트를 선택한 후, **로그 > 로그 설정** 메뉴로 이동하세요.
2. 로그 모니터링 시작하기 탭에서 에이전트 설정 및 로그 모니터링 활성화의 **1. 에이전트 설정 확인**의 안내를 참고해 에이전트 설정을 확인하세요.

컨테이너 로그 수집 활성화

쿠버네티스 컨테이너에 로그를 수집하려면 **1. 에이전트 설정 확인**에서 **로그 설정 적용하기** 버튼을 클릭하세요.

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 참고하세요.

1. **로그 > 로그 설정 > 로그 모니터링 시작하기** 탭으로 이동하세요.
2. **1. 에이전트 설정 확인** 하단의  **에이전트 설정** 버튼을 클릭하세요.
3. 에이전트 설정에서 **옵션 작성**의 옵션 선택 드롭 다운 목록에서 **직접 입력**을 클릭하세요.
4. 에이전트 설정 명령어의 키 `logsink_enabled` 와 값 `true` 를 입력창에 입력하세요.

```
logsink_enabled=true
```

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

- ❗ • Java 애플리케이션 로그 수집에 대한 자세한 내용은 [다음 문서](#)를 참고하세요.
- Python 애플리케이션 로그 수집에 대한 자세한 내용은 [다음 문서](#)를 참고하세요.
- Go 애플리케이션 로그 수집에 대한 자세한 내용은 [다음 문서](#)를 참고하세요.

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 비활성화할 수 있습니다.

- ☒ **로그 모니터링 활성화:** 토글 버튼을 켜면 로그 모니터링이 활성화되고, 활성화한 날부터 15일 동안 무료로 체험하실 수 있습니다.
- ☐ **로그 모니터링 비활성화:** 토글 버튼을 끄면 로그 모니터링이 비활성화되고, 로그를 더 이상 저장하지 않습니다.

❗ 로그 모니터링 활성화 권한

에이전트 설치 후 프로젝트에 대한 수정 권한이 있는 사용자만 로그 모니터링을 활성화할 수 있습니다. 권한에 대한 자세한 내용은 [다음 문서](#)를 참고하세요.

쿠버네티스 로그 모니터링 카테고리 안내

쿠버네티스 관련 다양한 로그를 확인할 수 있습니다. 와탭 쿠버네티스에서 모니터링 카테고리를 제공합니다.

- ⚠ **설정**에 따라 중복된 로그 내용이 저장될 수 있으니 반드시 중복 여부를 확인하시기 바랍니다.

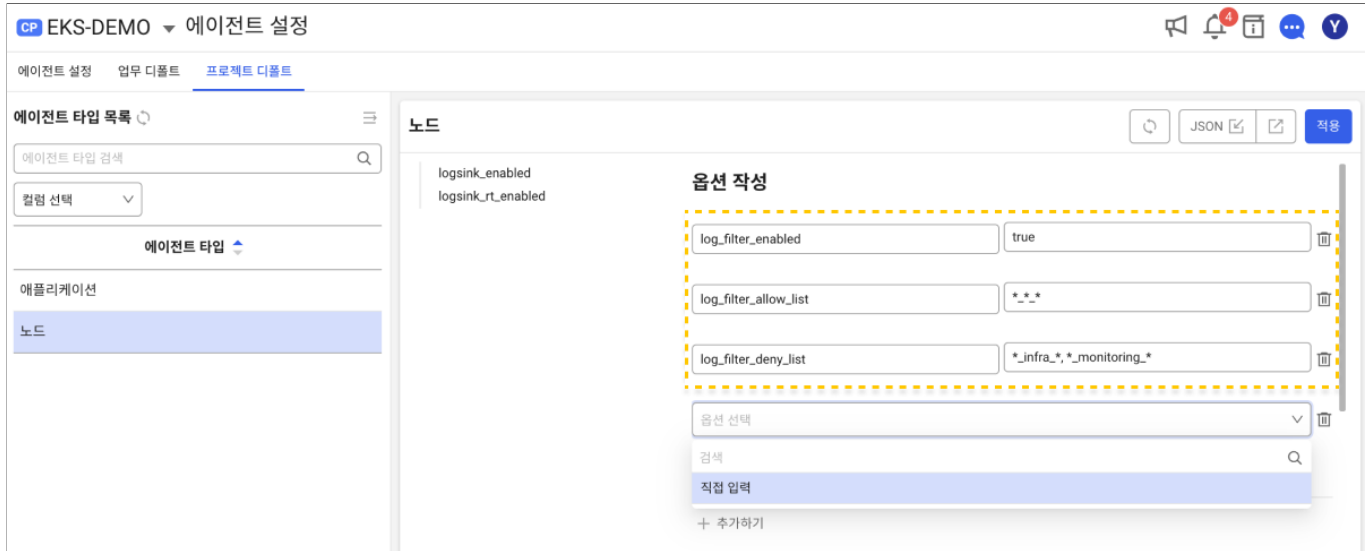
카테고리	설명
#K8sEvent	- 쿠버네티스에서 발생하는 이벤트가 저장된 로그 - 사용자 설정과 무관하게 기본 생성
#WhatapEvent	- 와탭 이벤트 설정에 의해 발생한 이벤트가 저장된 로그 - 사용자 설정과 무관하게 기본 생성
containerStdout	- 컨테이너 Standard Out 로그 - 사용자 설정 시 생성 - 노드 에이전트에 <code>logsink_enabled=true</code> 설정 추가 시
AppLog	- 컨테이너 내 애플리케이션 로그 - 사용자 설정 시 생성 - 애플리케이션 에이전트에 <code>logsink_enabled=true</code> 설정 추가 시

containerStdOut 로그 필터 설정

홈 화면 > 프로젝트 선택 > 관리 > 에이전트 설정

쿠버네티스 로그에서 필요한 정보를 선별하기 위한 필터링 옵션을 안내합니다. 필터링을 통해 허용하거나 제외할 로그를 설정할 수 있습니다.

1. 관리 > 에이전트 설정으로 이동하세요.
2. 프로젝트 디폴트 탭에서 옵션 작성 방식으로 직접 입력을 클릭하세요.



로그 네이밍 규칙

쿠버네티스 containerStdOut 로그는 노드의 `/var/log/containers/` 경로 하위에 생성됩니다. 다음과 같은 네이밍 규칙을 따르고 있습니다.

```
<podName>_<namespace>_<containerName>-<containerId>.log
```

로그 필터 옵션

- `log_filter_enabled` `bool`

기본값 `false`

로그 필터 사용 여부를 설정합니다.

- `log_filter_allow_list` `list`

허용할 로그의 리스트를 설정합니다. 필터링 적용 시 포함할 항목을 의미합니다.

- `log_filter_deny_list` `list`

제외할 로그의 리스트를 설정합니다. 필터링 적용 시 제외할 항목을 의미합니다.

로그 필터 동작

`log_filter_enabled` 옵션이 활성화된 경우만 로그 필터가 동작합니다. 해당 옵션의 값이 `true` 로 설정된 상태에서 `log_filter_allow_list` 및 `log_filter_deny_list` 를 통해 로그를 선택적으로 수집할 수 있습니다.

로그 필터는 블랙리스트 기반으로 작동합니다. 예를 들어 `log_filter_enabled` 활성화 후 `log_filter_allow_list` 옵션에 추가할 항목을 설정하지 않을 경우 기본적으로 모든 컨테이너의 로그 수집이 차단됩니다. 또한 로그 필터는 allow 규칙 보다 deny 규칙의 우선 순위가 높습니다. 동일한 항목이 allow와 deny에 모두 설정된 경우, deny 규칙이 우선 적용되어 해당 로그는 수집되지 않습니다.

로그 필터 예시

단일 네임스페이스 로그 수집

- 허용 `log_filter_allow_list` `*_infra_*`

`infra` 네임스페이스에 존재하는 모든 컨테이너가 수집 대상으로 지정됩니다.

다중 네임스페이스 로그 수집

- 허용 `log_filter_allow_list` `*_infra_*`, `*_monitoring_*`

`infra`, `monitoring` 네임스페이스에 존재하는 모든 컨테이너가 수집 대상으로 지정됩니다.

특정 단어를 포함하는 Pod 제외

- 허용 `log_filter_allow_list` `*_*_*`
- 제외 `log_filter_deny_list` `*prod*_**`

모든 컨테이너가 수집 대상으로 지정되지만, `podName` 에 `prod` 가 포함된 로그는 제외됩니다.

특정 단어를 포함하는 Pod 로그 수집

- 허용 `log_filter_allow_list` `*prod*_**`

`podName` 에 `prod` 가 포함된 파드의 로그만 수집됩니다.

다중 네임스페이스 로그 수집 및 특정 단어 포함하는 Pod 제외

- 허용 `log_filter_allow_list` `*_infra_*, *_monitoring_*`
- 제외 `log_filter_deny_list` `*prod*_**`

`infra`, `monitoring` 네임스페이스의 로그가 수집되고, `podName`에 `prod`가 포함된 로그는 제외됩니다.

컨테이너 이름 내 특정 단어로 시작하는 컨테이너 로그 제외

- 허용 `log_filter_allow_list` `*_*_db-*`

모든 네임스페이스에서 `containerName`이 `db`로 시작하는 컨테이너의 로그는 제외됩니다.

라이브 테일

❗ 로그 조회 권한이 없을 경우 해당 메뉴에 진입할 수 없습니다.

홈 화면 > 프로젝트 선택 > 로그 > 라이브 테일

라이브 테일 메뉴에서 서버 콘솔에 접속하지 않고, 로그 데이터 스트림을 모니터링 화면상에서 바로 확인할 수 있습니다. 복잡한 대량의 로그도 필터와 하이라이트 기능을 활용해 선별하고 빠르게 인지할 수 있습니다. 로그 데이터 조회 주기는 2초입니다.

주요 용어는 다음과 같습니다.

- **Category:** 로그의 수집 및 조회 단위
- **Content:** 로그 메시지
- **Search Key:** 로그 파서 설정을 통해 생성되는 검색 키
- **Tag:** 수집된 로그를 검색할 수 있는 태그

❗ 로그 테이블 컬럼 가장자리를 드래그해 컬럼 너비를 수정할 수 있습니다.

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]
Servlet.service() for servlet [dispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.err														
2023-12-18	14:31:02.586	level	error	[pcode]	2277	[agenttime]	1702877462057	[oid]	778873916	[category]	AppServer	[event_status]	error	[event_status_literal_name]
Servlet.service() for servlet [dispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.err														
2023-12-18	14:31:02.586	level	error	[pcode]	2277	[agenttime]	1702877462081	[oid]	778873916	[category]	AppServer	[event_status]	error	[event_status_literal_name]
Servlet.service() for servlet [dispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.err														
2023-12-18	14:31:02.586	level	error	[pcode]	2277	[agenttime]	1702877462087	[oid]	778873916	[category]	AppServer	[event_status]	error	[event_status_literal_name]
Servlet.service() for servlet [dispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.err														

에이전트 옵션 설정

```
# 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.

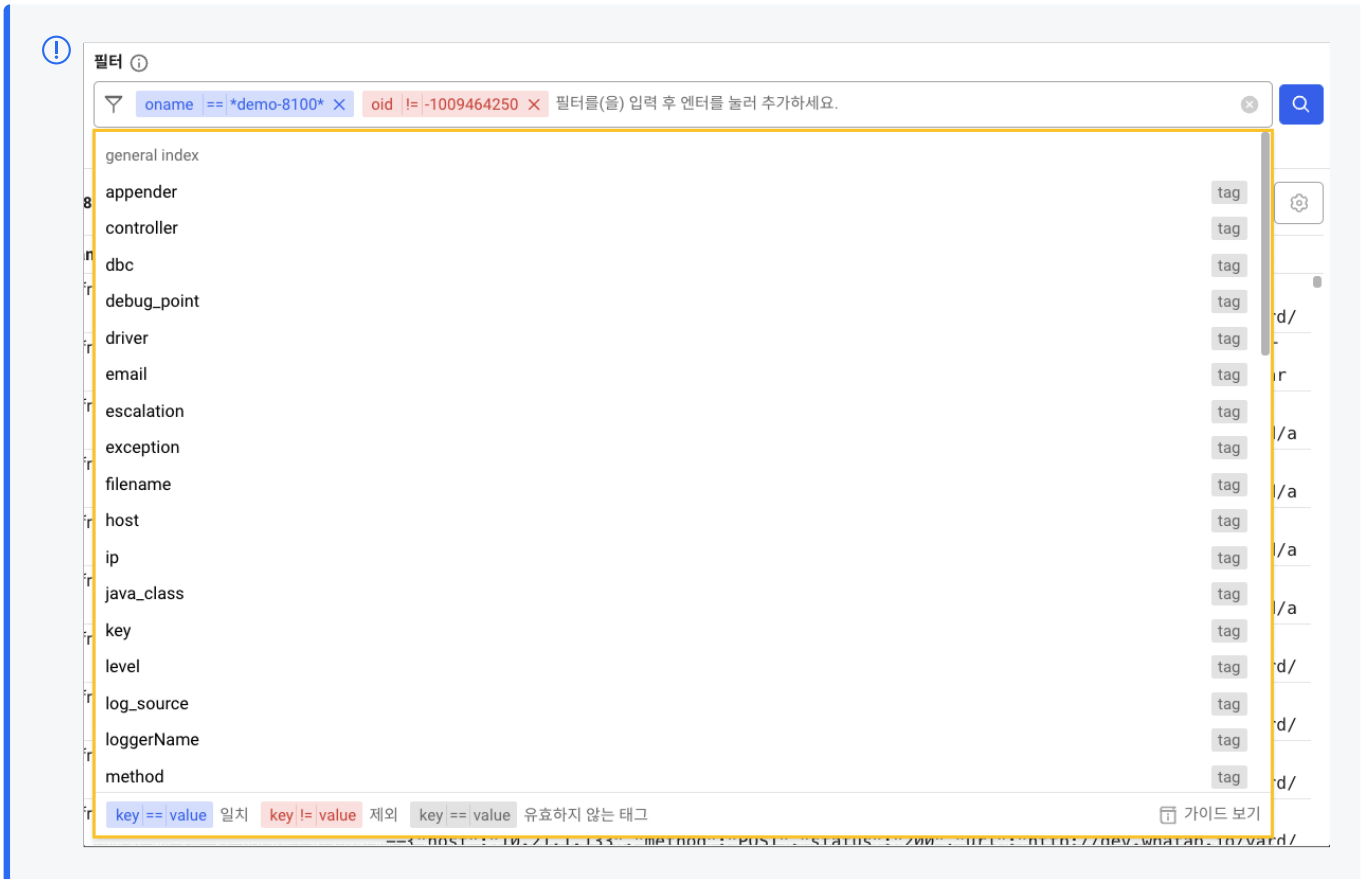
필터 적용하기

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 로그 목록에서 조회할 수 있습니다.

! 가이드 UI

다음과 같이 입력 창 아래 **가이드 UI**를 제공합니다. 입력 창 또는 필터 태그에 마우스 커서가 있을 때 ESC 키를 통해 **가이드 UI**를 닫을 수 있습니다.



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. 대소문자 구분 옵션을 활용해 검색할 수 있습니다.

- 필터 태그가 2줄 이상 길어지는 경우 **접기** 아이콘을 선택해 접어둘 수 있습니다.
- 필터 태그 입력 후 입력 창에서 Shift와 Tab 키를 동시에 사용하여 이전 필터 태그로 이동할 수 있습니다.
- 필터 태그 입력 후 입력 창에서 Tab 키를 통해 다음 필터 태그로 이동할 수 있습니다.

필터 태그 추가

입력 창에 텍스트 입력 후 Enter 또는 Tab 키를 누르거나, 입력창 하단의 가이드 UI에서 추천 값을 클릭하거나 방향키로 선택해 추가할 수 있습니다.

필터 태그 제거

Backspace 키 또는 태그의 X 아이콘을 눌러 태그를 삭제할 수 있습니다. 입력창 오른쪽의 X 아이콘을 클릭해 모든 태그를 한 번에 삭제할 수 있습니다.

필터 즐겨찾기

필터 즐겨찾기 기능을 제공합니다. 입력 창 오른쪽의 ☆ 즐겨찾기 아이콘을 선택하여 원하는 필터 검색 조건을 즐겨찾기에 추가, 제거 및 기존 즐겨찾기를 선택할 수 있습니다. 즐겨찾기는 최대 50개까지 저장됩니다.

The screenshot shows the Live Tail interface with a filter bar at the top containing tags: `area == river`, `city == kwangju`, and `level == Warning`. Below the filter bar, a SQL query is displayed: `select ename, sal+1000 from emp`. A modal window titled "즐거찾기" (Favorites) is open, showing a list of saved filters: "로그 필터 즐겨찾기 2" and "로그 필터 즐겨찾기 1". The modal also includes a "추가" (Add) button and a "전체 삭제" (Delete All) button. The background interface shows a table of log data with columns like `@txid`, `pcode`, `onodeName`, and `oid`.

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 설정**을 통해 인덱스 키 값을 활용해 검색하는 것을 권장합니다.

필터 ⓘ

🔍

oid != -1009464250 ✕

okind == -398596773 ✕

content == *select* ✕

필터를(을) 입력 후 엔터를 눌러 추가하세요.

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

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 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.

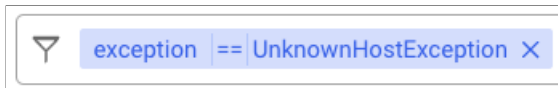
검색 키(Search Key)

다음 이미지에서 파란색 박스 부분은 파싱(parsing)된 검색 키입니다. 검색 키는 **로그 설정의 로그 파서 설정** 탭에서 파싱 로직을 등록해 설정할 수 있습니다.

검색 키

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 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>

문법 종류	설명	예시
*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:{regex}	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
==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

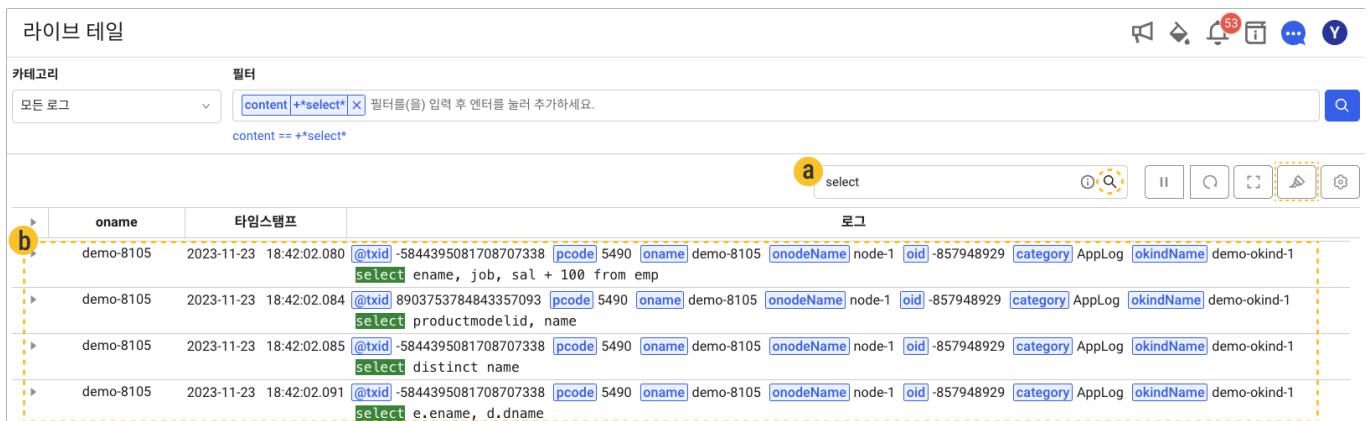
개인정보 조회

로그 개인정보 조회 권한이 있을 경우, **개인정보 표시**  토글 버튼 활성화를 통해 비식별화 처리한 개인정보를 표시할 수 있습니다.

- ❗ • 로그 개인정보 조회 권한에 대한 자세한 내용은 [다음 문서](#)를 참고하세요.
- 로그 개인정보 비식별화 기능에 대한 자세한 내용은 [다음 문서](#)를 참고하세요.

콘텐츠 하이라이트

로그의 콘텐츠 중 원하는 키워드를 손쉽게 식별하기 위해 하이라이트 기능을 제공합니다. 단일 또는 복수 키워드로 필터링할 수 있습니다.



라이브 테일

카테고리: 모든 로그

필터: content == *select*

select

▶	oname	타임스탬프	로그
b	demo-8105	2023-11-23 18:42:02.080	@txid]-5844395081708707338 [pcode] 5490 [oname] demo-8105 [onodeName] node-1 [oid]-857948929 [category] AppLog [okindName] demo-okind-1 select ename, job, sal + 100 from emp
▶	demo-8105	2023-11-23 18:42:02.084	@txid] 8903753784843357093 [pcode] 5490 [oname] demo-8105 [onodeName] node-1 [oid]-857948929 [category] AppLog [okindName] demo-okind-1 select productmodelid, name
▶	demo-8105	2023-11-23 18:42:02.085	@txid]-5844395081708707338 [pcode] 5490 [oname] demo-8105 [onodeName] node-1 [oid]-857948929 [category] AppLog [okindName] demo-okind-1 select distinct name
▶	demo-8105	2023-11-23 18:42:02.091	@txid]-5844395081708707338 [pcode] 5490 [oname] demo-8105 [onodeName] node-1 [oid]-857948929 [category] AppLog [okindName] demo-okind-1 select e.ename, d.dname

- 키워드 입력창에 하이라이트를 원하는 키워드를 입력하세요.
 - 예시, select
- 로그 목록의 Content 내 검색한 키워드가 하이라이팅 됩니다.
 - [] 로그 전체 화면 아이콘을 선택하면 로그와 타임스탬프를 전체 화면에서 확인할 수 있습니다.
 - 하이라이트된 키워드 간 이동은 단축키로 조작할 수 있습니다.
 - Enter : 다음 row로 이동
 - Shift+Enter : 이전 row로 이동

-  /  아이콘: row 이동
- **Cmd + F** (Mac) / **Ctrl + F** (Windows): 키워드 검색

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 <code>"</code> 또는 <code>'</code> 로 감쌉니다.	Whatap is good.
"Whatap\\ is good."	<code>"</code> 로 감싸진 키워드에서 <code>\</code> 를 포함할 경우, <code>\\</code> 로 입력해야 합니다.	Whatap\ is good.

하이라이트 색상 설정

하이라이팅할 키워드 및 색상을 설정할 수 있습니다.

- 기본적으로 로그 레벨에 따른 하이라이팅(**FATAL**, **ERROR**, **WARN**, **SEVERE**, **CRITICAL**)이 적용되어 있습니다.
- 설정한 내용은 **프로젝트** 단위로 저장됩니다.
 1.  아이콘을 클릭하세요.
 2. **하이라이트** 창에서 추가적으로 색상 설정을 원하는 키워드를 입력창에 입력하세요.
 3. 입력창 왼쪽 색상 클릭 시 색을 선택할 수 있습니다.

테이블 설정

컬럼 설정

컬럼을 추가하거나 순서를 설정할 수 있습니다. 화면 오른쪽에서  **컬럼 설정** 버튼을 클릭하세요.

컬럼 추가

태그를 선택하여 테이블에 컬럼을 추가할 수 있습니다. **log** 컬럼 선택을 해제할 경우 **로그 표시 상세 설정**을 확인할 수 없습니다. 반드시 한 개 이상의 컬럼을 선택하세요.

- 제공되는 컬럼: 로그, 수집 시간, content(로그 메시지)

컬럼 순서 변경

컬럼을 추가하면 **표시 항목**에 해당 컬럼이 추가됩니다. 원하는 컬럼을 드래그하여 컬럼의 순서를 변경하세요.

로그 표시 상세 설정

1. 화면의 오른쪽에서 ⚙ **로그 표시 상세 설정** 버튼을 클릭하세요.
2. **로그 표시 상세 설정** 창에서 **content**와 **태그** 중 하나는 반드시 선택하세요.
 - 기본으로 **content**, **태그** 모두 선택되어있으며 두 가지 항목 모두 표시합니다.

체크가 해제된 항목은 테이블에 표시되지 않습니다. 다음과 같이 **태그**를 해제할 경우 테이블에서 로그의 **태그**는 표시되지 않습니다.



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.

ⓘ 컬럼 및 로그 표시 설정 적용 범위

- 컬럼 설정과 로그 표시 상세 설정은 **라이브 테일**, **로그 검색**, **로그 트렌드**에서 사용할 수 있습니다.
- 동일한 프로젝트 내 **라이브 테일**, **로그 검색**, **로그 트렌드**는 컬럼 설정과 로그 표시 상세 설정을 공유합니다.

로그 파일 다운로드

검색한 로그의 결과값을 **CSV**, **TXT** 파일 형식으로 수집된 로그를 다운로드 받을 수 있습니다.

1. 화면 중앙의 오른쪽의 **↓ 다운로드** 버튼을 클릭합니다.
2. **CSV 다운로드** 또는 **Log 다운로드**를 클릭해 원하는 형태의 파일을 다운로드 받습니다.

로그 탐색

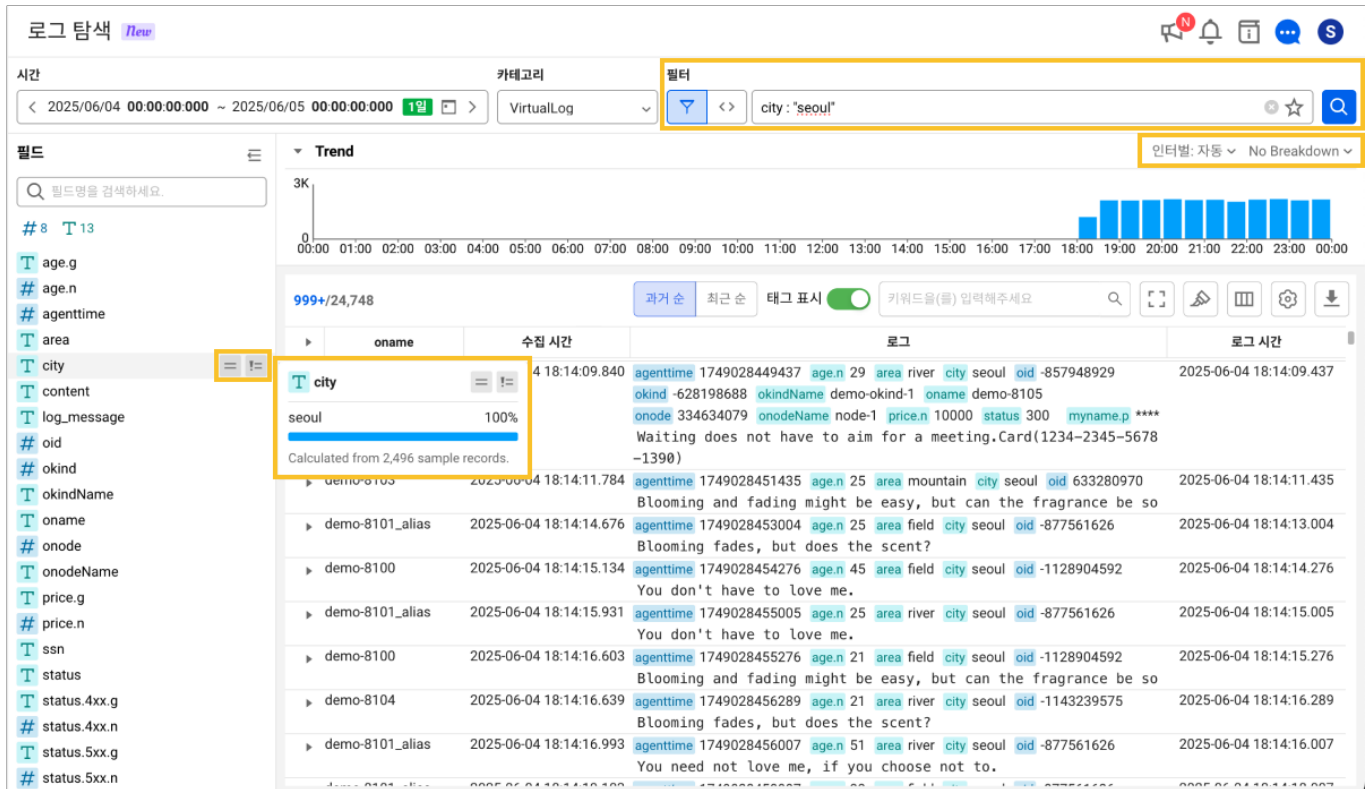
❗ 로그 조회 권한이 없을 경우 해당 메뉴에 진입할 수 없습니다.

홈 화면 > 프로젝트 선택 > 로그 > 로그 탐색 *New*

로그 탐색(Log Explorer) 기능은 로그 데이터를 빠르게 검색, 필터링, 분석합니다. 필드 구조에 대한 정보를 파악하고, 쿼리 기반 필터링을 통해 필요한 로그를 효율적으로 검색해, 결과를 데이터 시각화하여 확인할 수 있습니다. 본 기능은 Lucene 인덱스 기반으로 동작하며, 주요 특징은 다음과 같습니다.

- 로그 트렌드 분석 및 검색:** 로그 트렌드와 검색 기능을 동시에 지원하여, 시간에 따른 로그 변화 추이를 파악할 수 있습니다.
- 빠른 검색 및 필터링:** 사용자는 간단한 단어 입력만으로도 문제의 로그를 신속하게 검색할 수 있습니다. WhaTap log search query와 Lucene 쿼리 언어를 지원하여, 다양한 검색 조건을 설정할 수 있습니다.
- 자동완성 기능:** 쿼리 입력 시 자동완성 기능을 통해 사용자가 쉽게 쿼리를 작성하고 학습할 수 있도록 돕습니다.
- 데이터 시각화:** 스택 그래프를 활용하여 시계열 로그 건수 데이터를 시각적으로 표현하며, 드릴다운 기능을 통해 특정 로그를 심층 분석할 수 있습니다.
- 즐거찾기 및 공유:** 자주 사용하는 필터를 즐겨찾기로 저장하고, URL을 통해 다른 사용자와 쉽게 공유할 수 있습니다.

기본 화면 안내



시간 설정

상단 옵션바의 타임셀렉터를 통해 로그 검색 시간 범위를 설정할 수 있습니다.

카테고리

상단 옵션바의 카테고리 선택에서 탐색하고 싶은 로그 종류 선택합니다. (예: AppLog 등)

필터

상단 옵션 바의 필터에서 쿼리 언어를 선택하고 검색 조건을 입력하여 필터를 적용합니다. 검색 쿼리 문법은 WhaTap 로그 검색 쿼리와 Lucene 쿼리를 지원합니다.

-  : WhaTap 로그 검색 쿼리
-  : Lucene 쿼리

검색 쿼리 문법

WhaTap log search query

WhaTap 로그 검색 쿼리는 자동 완성 기능을 제공하며, 간단한 단어 입력만으로도 문제의 로그를 신속하게 검색할 수 있습니다. and, or 등 다양한 문법을 활용해 다양한 검색 조건을 입력할 수 있습니다.

- 예, 검색 필터에 `error` 만 입력하여 content(로그 본문) 검색할 수 있습니다.
 1. 상단 옵션 바에서 필터 아이콘을 클릭한 후, 쿼리 검색창에서 필드(선택한 시간과 카테고리에 맞는 목록 노출)를 선택하세요.
 2. 연산자를 선택하세요.
 - a. 기본: `:`, `:*`, `and`, `or`
 - b. 선택한 필드가 `Number` 인 경우(기본 + `<=`, `>=`, `<`, `>`)
 - c. 선택한 필드가 `String` 인 경우(기본)
 3. 값(선택한 시간, 카테고리, 필드에 맞는 목록 노출)을 선택하세요.

검색 인덱스 필드 타입

지원 필드 타입은 `Number`, `String`, `Boolean` 세 가지 유형만 존재합니다.

- `Number` : Long, double, float 타입의 숫자 값
- `String` : 이메일 본문과 같은 전체 텍스트
- `Boolean` : True 또는 False 값

 WhaTap log search query 문법에 대한 자세한 내용은 [다음 문서](#)를 참고하세요.

Lucene

apache lucene 8.11.1 버전 오픈소스 문법을 그대로 사용하세요. 단, 자동 완성 기능을 제공하지 않습니다.

❗ Lucene의 QueryParser 클래식 패키지에 대한 자세한 내용은 [공식 문서](#)를 참고하세요.

필드 목록

드릴 다운 분석에 활용할 수 있습니다.

필드 정보 필터 반영하기

필드 목록에서 필드명을 확인하고, `=`, `!=` 버튼을 클릭해 조건을 필터에 적용하세요.

- 필드에 마우스 호버 시 `=`, `!=` 버튼이 보이고 클릭 시 필터에 반영됩니다.
- 필드 검색 기능을 통해 원하는 필드를 빠르게 찾을 수 있습니다.

Trend 차트

Trend 차트에서 **인터벌**, **Breakdown**을 적용해 그래프로 로그를 확인할 수 있습니다.

- **그래프 인터랙션**: 마우스 드래그 및 🔍 버튼으로 시간 줌인, 바 클릭으로 해당 영역의 로그 확인 가능
- **인터벌**: 자동, 1초, 5초, 30초, 1분, 5분, 10분, 30분, 1시간 중 선택 가능
- **Breakdown**: 특정 필드를 기준으로 Top 3 + Others 값을 분포 시각화하고, 드릴다운 필터 적용 가능

breakdown

breakdown은 로그 건수 추이를 특정 필드로 분석해주는 시각화 기능입니다.

- 특정 필드의 Top 3 값과 Others(나머지 값)를 구분하여 스택 그래프로 분포를 표시합니다.
- 드릴다운 분석에 활용할 수 있으며, 범례와 스택 그래프에서 특정 영역(부분 그래프)를 클릭해 특정 값만 강조하거나 필터 조건을 추가할 수 있습니다.

로그 확인하기

검색 조건에 맞는 로그 목록을 확인할 수 있으며, **필드 목록**에서 필드 정보와 로그 태그 색이 동일하게 표시됩니다.

콘텐츠 하이라이트

로그의 콘텐츠 중 원하는 키워드를 손쉽게 식별하기 위해 하이라이트 기능을 제공합니다. 단일 또는 복수 키워드로 필터링할 수 있습니다.

- 키워드 입력창에 하이라이트를 원하는 키워드를 입력하세요.
 - 예시, `select`
- 로그 목록의 Content 내 검색한 키워드가 하이라이팅 됩니다.
 - [] **로그 전체 화면** 아이콘을 선택하면 **로그**와 **타임스탬프**를 전체 화면에서 확인할 수 있습니다.
 - 하이라이트된 키워드 간 이동은 단축키로 조작할 수 있습니다.
 - `Enter` : 다음 row로 이동
 - `Shift+Enter` : 이전 row로 이동
 - `^` / `↓` 아이콘: row 이동
 - `Cmd + F` (Mac) / `Ctrl + F` (Windows): 키워드 검색

복수 키워드 조건

복수 키워드로 하이라이팅을 할 경우 다음과 같이 작성합니다.

입력 문자열	설명	결과
<code>a b c</code>	띄어쓰기로 각 키워드를 구분합니다.	a, b, c
<code>"Whatap is good."</code>	띄어쓰기를 키워드에 포함하고 싶은 경우 <code>"</code> 또는 <code>'</code> 로 감쌉니다.	Whatap is good.
<code>"Whatap\\ is good."</code>	<code>'</code> 로 감싸진 키워드에서 <code>\</code> 를 포함할 경우, <code>\\</code> 로 입력해야 합니다.	Whatap\ is good.

하이라이트 색상 설정

하이라이팅할 키워드 및 색상을 설정할 수 있습니다.

- 기본적으로 로그 레벨에 따른 하이라이팅(**FATAL**, **ERROR**, **WARN**, **SEVERE**, **CRITICAL**)이 적용되어 있습니다.

- 설정한 내용은 **프로젝트 단위**로 저장됩니다.

1.  아이콘을 클릭하세요.
2. **하이라이트** 창에서 추가적으로 색상 설정을 원하는 키워드를 입력창에 입력하세요.
3. 입력창 왼쪽 색상 클릭 시 색을 선택할 수 있습니다.

컬럼 설정

 버튼을 클릭해, 컬럼을 추가하거나 순서를 설정할 수 있습니다.

• 컬럼 추가

컬럼 설정에서 태그를 선택하여 테이블에 컬럼을 추가할 수 있습니다.

 로그 컬럼 선택을 해제할 경우 **로그 표시 상세 설정**을 확인할 수 없습니다. 반드시 한 개 이상의 컬럼을 선택하세요.

• 컬럼 순서 설정

컬럼 설정에서 컬럼을 추가하면 **표시 항목**에 해당 컬럼이 추가됩니다. 원하는 컬럼을 드래그하여 컬럼의 순서를 변경하세요.

로그 표시 상세 설정

 버튼을 클릭해, 로그 표시를 상세 설정합니다. 기본으로 **content**, **태그** 모두 체크가 되어있으며 두 가지 항목 모두 표시합니다.

- **content**와 **태그** 중 하나는 반드시 선택하세요.
- **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.
- 체크가 해제된 항목은 테이블에 표시되지 않습니다. 다음과 같이 **태그**를 해제할 경우 테이블에서 로그의 **태그**는 표시되지 않습니다.


 select distinct pp.lastname, pp.firstname
 select distinct pp.lastname, pp.firstname

 컬럼 및 로그 표시 설정 적용 범위



- 컬럼 설정과 로그 표시 상세 설정은 라이브 테일, 로그 검색, 로그 트렌드에서 사용할 수 있습니다.
- 동일한 프로젝트 내 라이브 테일, 로그 검색, 로그 트렌드는 컬럼 설정과 로그 표시 상세 설정을 공유합니다.

로그 파일 다운로드

검색한 로그의 결과값을 CSV, TXT 파일 형식으로 수집된 로그를 다운로드 받을 수 있습니다.

1. 화면 중앙의 오른쪽의  다운로드 버튼을 클릭합니다.
2. CSV 다운로드 또는 Log 다운로드를 클릭해 원하는 형태의 파일을 다운로드 받습니다.

WhaTap log search query 문법

✓ WhaTap 로그 탐색에서 사용할 수 있는 WhaTap log search query 문법에 관한 문서입니다.

1. Equal

- `field : value`

2. Not

- `not field : value`

3. Wildcard (String 타입 필드만 사용 가능, 검색 값 앞뒤에 " 사용 금지)

- `field : val*`

4. Exist

- `field : *`

5. Range (Number 타입 필드만 사용 가능)

- `<`, `>`, `<=`, `>=` 사용 가능
- 예: `field < 30 and field >= 10`

6. Combining Multiple Queries

- AND 예: `field < 30 and field >= 10`
- OR 예: `field < 30 or field >= 10`

7. Grouping

- 예: `(field < 30 or field >= 10) and other : 70`

8. Escaping Special Characters

- Lucene의 이스케이프 지원 특수 문자 목록: `&` `&` `|` `|` `!` `(` `)` `{` `}` `^` `"` `~` `*` `?` `:` `\` `/`
- 문자 앞에 `\` 를 사용해 이스케이프함
- 예: `(1+1):2` 검색하려면, `\(1\+1\)\:2`

검색 인덱스 필드 타입

지원 필드 타입은 `Number` , `String` 두 가지 유형만 존재합니다.

- `Number` : Long, double, float 타입의 숫자 값
 - `field : "value"` 로 사용
- `String` : 이메일 본문과 같은 전체 텍스트
 - `field : value` 로 사용
- `Boolean` : True 또는 False
 - `field : true` 또는 `field : false` 로 사용

로그 트렌드

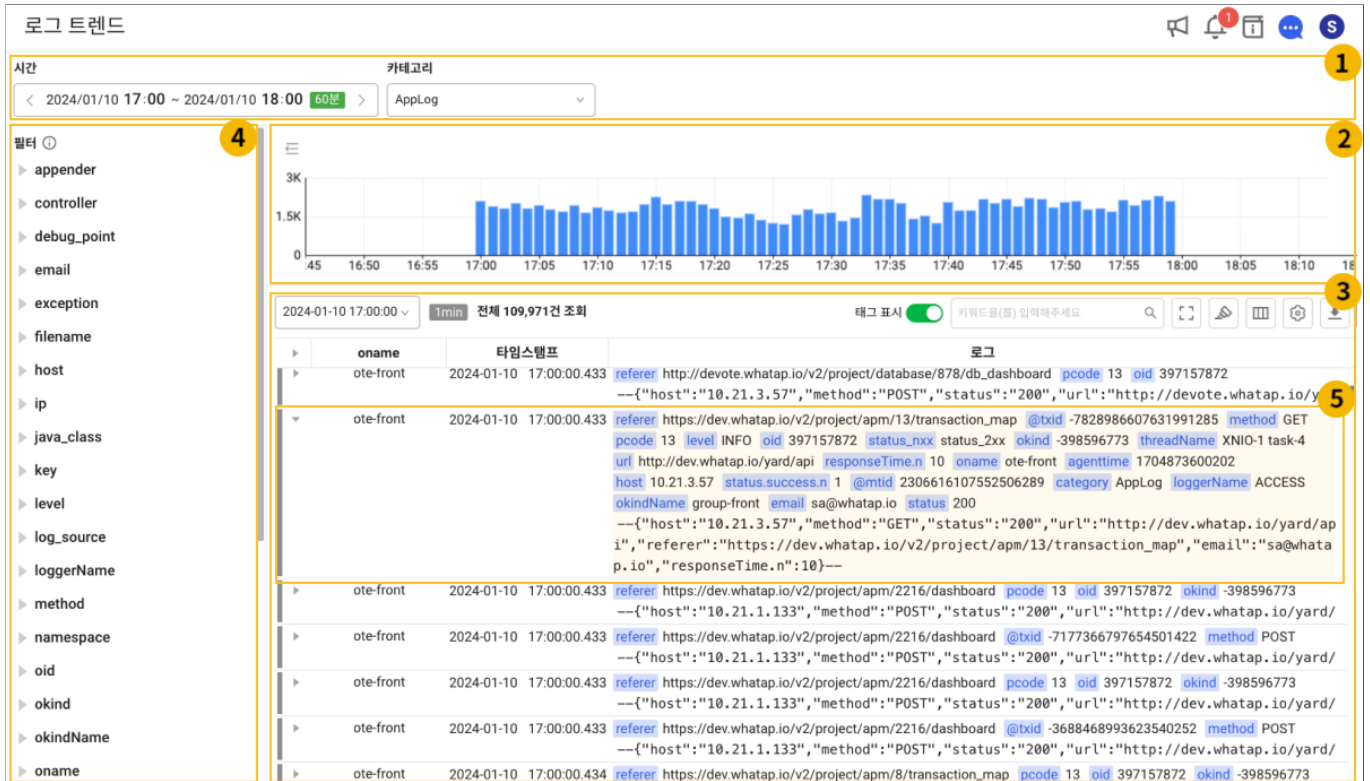
❗ 로그 조회 권한이 없을 경우 해당 메뉴에 진입할 수 없습니다.

홈 화면 > 프로젝트 선택 > 로그 > 로그 트렌드

로그 트렌드에서 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 단위
- **Content:** 로그 메시지
- **Search Key:** 로그 파서 설정을 통해 생성되는 검색 키
- **Tag:** 수집된 로그를 검색할 수 있는 태그



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 수집 시간을 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	agentime	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	agentime	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	agentime	1702877462043	oid	778873916	category	AppServer	event_status	error
Servlet.service() for servlet [DispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.error]												
2023-12-18 14:31:02.586	level	error	pcode	2277	agentime	1702877462057	oid	778873916	category	AppServer	event_status	error
Servlet.service() for servlet [DispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.error]												
2023-12-18 14:31:02.586	level	error	pcode	2277	agentime	1702877462081	oid	778873916	category	AppServer	event_status	error
Servlet.service() for servlet [DispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.error]												
2023-12-18 14:31:02.586	level	error	pcode	2277	agentime	1702877462087	oid	778873916	category	AppServer	event_status	error
Servlet.service() for servlet [DispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.error]												

에이전트 옵션 설정

```
# 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 로그 테이블 컬럼 가장자리를 드래그해 컬럼 너비를 수정할 수 있습니다.

개인정보 조회

로그 개인정보 조회 권한이 있을 경우, 개인정보 표시  토글 버튼 활성화를 통해 비식별화 처리한 개인정보를 표시할 수 있습니다.

- ① • 로그 개인정보 조회 권한에 대한 자세한 내용은 [다음 문서](#)를 참고하세요.
- 로그 개인정보 비식별화 기능에 대한 자세한 내용은 [다음 문서](#)를 참고하세요.

로그 Content 확인하기

Content는 로그 메시지입니다. 로그 컬럼의 첫 번째 줄은 로그의 파싱(parsing)된 키와 값이고 두 번째 줄은 Content입니다.

- 3 로그 테이블의 행(로그)마다 ▶ 더보기 버튼이 있습니다. ▶ 더보기 버튼을 선택하면 5처럼 해당 로그의 전체 content를 확인할 수 있습니다.

하이라이트 설정하기

원하는 키워드를 손쉽게 식별할 수 있도록 하이라이트 기능을 제공합니다.  아이콘을 클릭해 키워드를 입력 후 엔터를 눌러 추가하세요.

콘텐츠 하이라이트

로그의 콘텐츠 중 원하는 키워드를 손쉽게 식별하기 위해 하이라이트 기능을 제공합니다. 단일 또는 복수 키워드로 필터링할 수 있습니다.

1. 키워드 입력창에 하이라이트를 원하는 키워드를 입력하세요.
 - 예시, `select`
2. 로그 목록의 Content 내 검색한 키워드가 하이라이팅 됩니다.
 -  **로그 전체 화면** 아이콘을 선택하면 **로그**와 **타임스탬프**를 전체 화면에서 확인할 수 있습니다.
 - 하이라이트된 키워드 간 이동은 단축키로 조작할 수 있습니다.
 - `Enter` : 다음 row로 이동
 - `Shift+Enter` : 이전 row로 이동
 - `^ / v` 아이콘: row 이동
 - `Cmd + F` (Mac) / `Ctrl + F` (Windows): 키워드 검색

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 입력해야 합니다.	Whatap\ is good.

하이라이트 색상 설정

하이라이팅할 키워드 및 색상을 설정할 수 있습니다.

- 기본적으로 로그 레벨에 따른 하이라이팅(**FATAL**, **ERROR**, **WARN**, **SEVERE**, **CRITICAL**)이 적용되어 있습니다.
- 설정한 내용은 **프로젝트 단위**로 저장됩니다.
 1.  아이콘을 클릭하세요.
 2. **하이라이트** 창에서 추가적으로 색상 설정을 원하는 키워드를 입력창에 입력하세요.
 3. 입력창 왼쪽 색상 클릭 시 색을 선택할 수 있습니다.

차트로 로그 조회하기



- 바 차트에서 **a** 원하는 시간 영역 바를 클릭하거나 드래그하여 해당 시간 범위의 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

테이블 설정하기

컬럼 설정

컬럼을 추가하거나 순서를 설정할 수 있습니다. **3** 영역 오른쪽에서 컬럼 설정 버튼을 클릭하세요.

컬럼 추가

태그를 선택하여 테이블에 컬럼을 추가할 수 있습니다. **log** 컬럼 선택을 해제할 경우 **로그 표시 상세 설정**을 확인할 수 없습니다. 반드시 한 개 이상의 컬럼을 선택하세요.

- 제공되는 컬럼: 로그, 수집 시간, content(로그 메시지)

컬럼 순서 변경

컬럼을 추가하면 **표시 항목**에 해당 컬럼이 추가됩니다. 원하는 컬럼을 드래그하여 컬럼의 순서를 변경하세요.

로그 표시 상세 설정

3 영역 오른쪽에서  **로그 표시 상세 설정** 버튼을 선택하세요. 기본으로 **content**, **태그** 모두 체크가 되어있으며 두 가지 항목 모두 표시합니다. **content**와 **태그** 중 하나는 반드시 선택하세요.

체크가 해제된 항목은 테이블에 표시되지 않습니다. 다음과 같이 **태그**를 해제할 경우 테이블에서 로그의 **태그**는 표시되지 않습니다.



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.

ⓘ 컬럼 및 로그 표시 설정 적용 범위

- 컬럼 설정과 로그 표시 상세 설정은 **라이브 테일**, **로그 검색**, **로그 트렌드**에서 사용할 수 있습니다.
- 동일한 프로젝트 내 **라이브 테일**, **로그 검색**, **로그 트렌드**는 컬럼 설정과 로그 표시 상세 설정을 공유합니다.

로그 파일 다운로드

검색한 로그의 결과값을 **CSV**, **TXT** 파일 형식으로 수집된 로그를 다운로드 받을 수 있습니다.

1. 화면 중앙의 오른쪽의 **↓ 다운로드** 버튼을 클릭합니다.
2. **CSV 다운로드** 또는 **Log 다운로드**를 클릭해 원하는 형태의 파일을 다운로드 받습니다.

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 단위
- **Content:** 로그 메시지
- **Search Key:** 로그 파서 설정을 통해 생성되는 검색 키
- **Tag:** 수집된 로그를 검색할 수 있는 태그

1 로그 검색

시간 2023/07/03 13:16 ~ 2023/07/03 14:16 60분 필터 ①

2

3 전체 4,532,168건 조회

과거 순 최근 순 태그 표시 키워드(를) 입력해주세요

4

AppLog (4,490,257)

AppStdErr (353)

AppStdOut (19,439)

VirtualLog (20,767)

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: -959317925843459491 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/daeju 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

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 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 📄 로그 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.

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

에이전트 옵션 설정

```
# 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 로그 테이블 컬럼 가장자리를 드래그해 컬럼 너비를 수정할 수 있습니다.

로그 Content 확인하기

Content는 로그 메시지입니다. 로그 컬럼의 첫 번째 줄은 로그의 파싱(parsing)된 키와 값이고 두 번째 줄은 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 로그를 검색 할 수 있는 드롭다운 메뉴가 나타납니다.

필터

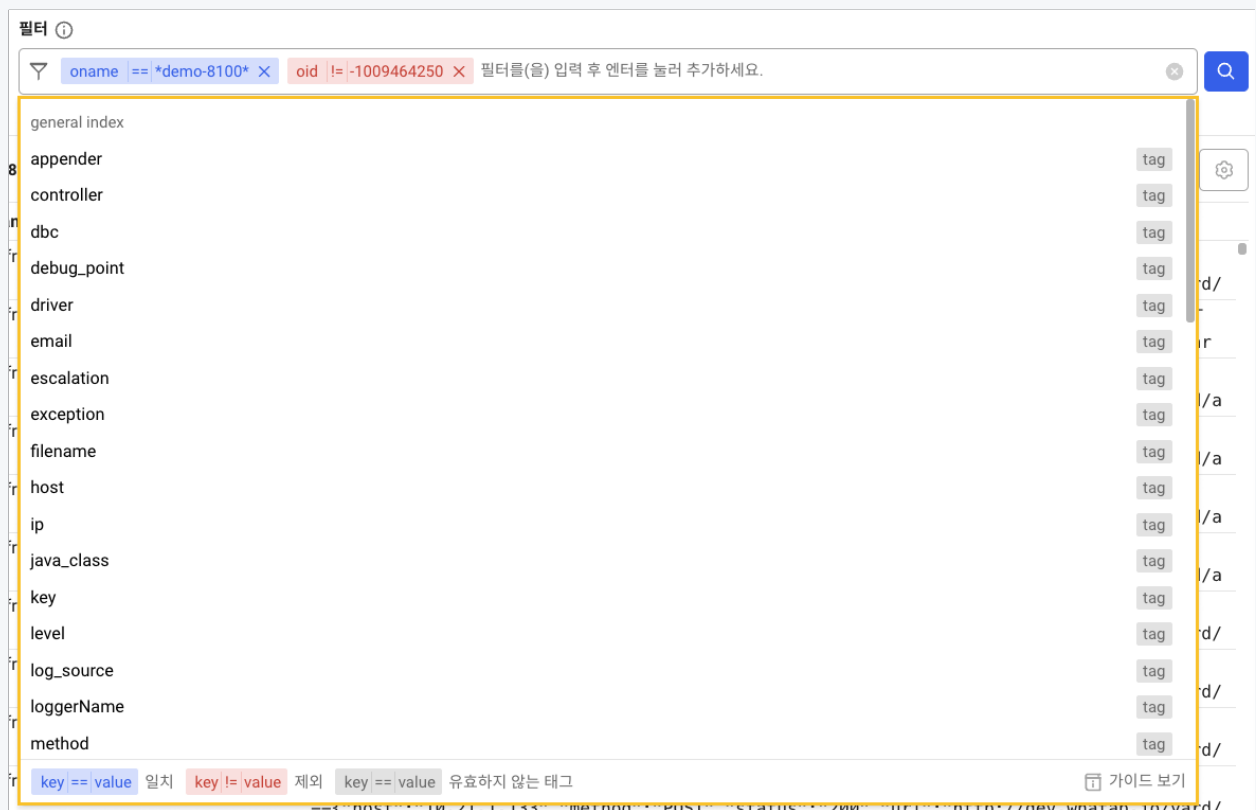
필터 적용

❶ 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 로그 목록에서 조회할 수 있습니다.

! 가이드 UI

다음과 같이 입력 창 아래 **가이드 UI**를 제공합니다. 입력 창 또는 필터 태그에 마우스 커서가 있을 때 ESC 키를 통해 **가이드 UI**를 닫을 수 있습니다.



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. 대소문자 구분 옵션을 활용해 검색할 수 있습니다.

- ❗
- 필터 태그가 2줄 이상 길어지는 경우 **접기** 아이콘을 선택해 접어들 수 있습니다.
 - 필터 태그 입력 후 입력 창에서 Shift와 Tab 키를 동시에 사용하여 이전 필터 태그로 이동할 수 있습니다.
 - 필터 태그 입력 후 입력 창에서 Tab 키를 통해 다음 필터 태그로 이동할 수 있습니다.

필터 태그 추가

입력 창에 텍스트 입력 후 Enter 또는 Tab 키를 누르거나, 입력창 하단의 가이드 UI에서 추천 값을 클릭하거나 방향키로 선택해 추가할 수 있습니다.

필터 태그 제거

Backspace 키 또는 태그의 X 아이콘을 눌러 태그를 삭제할 수 있습니다. 입력창 오른쪽의 X 아이콘을 클릭해 모든 태그를 한 번에 삭제할 수 있습니다.

필터 즐겨찾기

필터 **즐거찾기** 기능을 제공합니다. 입력 창 오른쪽의 ☆ **즐거찾기** 아이콘을 선택하여 원하는 필터 검색 조건을 즐겨찾기에 **추가**, **제거** 및 기존 즐겨찾기를 선택할 수 있습니다. **즐거찾기**는 최대 50개까지 저장됩니다.

필터

area == river X city == kwangju X level == Warning X 필터를(을) 입력 후 엔터를 눌러 추가하세요.

area == river && city == kwangju && level == Warning

키워드

로그

타임스탬프

select ename, sal+1000 from emp

10-31 15:40:17.429 @txid -7827890892800464193 pcode 5490 onodeName node-0 oid 1387800

즐거찾기

로그 필터 즐겨찾기 2

추가

로그 필터 즐겨찾기 1

최대 10개까지 저장됩니다.

X 전체 삭제

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.

필터 ⓘ

oid != -1009464250 X okind == -398596773 X content == *select* X 필터를(을) 입력 후 엔터를 눌러 추가하세요.

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

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.

로그 검색

시간: 2024/01/15 14:45 ~ 2024/01/15 15:45

필터: category: AppLog, oid: 397157872, content: *select*

전체 40,326건 중 10,000건 조회했으며 검색된 결과는 9999+건입니다.

로그를 더 조회하시겠습니까?
로그 파서 추가시 추가 조회없이 검색이 가능합니다.

로그 파서 설정하기 | 추가 조회하기

- ❗ 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 **AppLog**와 **AppStdOut**은 카테고리, 그 아래 **oid**와 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 구성되어 있습니다. 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:{regex}	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>

개인정보 조회

로그 개인정보 조회 권한이 있을 경우, 개인정보 표시  토글 버튼 활성화를 통해 비식별화 처리한 개인정보를 표시할 수 있습니다.

- ❗ • 로그 개인정보 조회 권한에 대한 자세한 내용은 [다음 문서](#)를 참고하세요.
- 로그 개인정보 비식별화 기능에 대한 자세한 내용은 [다음 문서](#)를 참고하세요.

로그 태그 옵션

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

전체 90,699건 조회	과거 순	최근 순	키워드(를) 입력해주세요	🔍	🔍	🔍	🔍	🔍
▶ oname	타임스탬프	로그						
▶ java-demo3	2025-04-17 09:17:13.018	@txid 7759974649447934516 pcode 8 onodeName node-0 oid -278185929 okind 1152715164 oname java-demo3	Exception: random exception					
▶ java-demo3	2025-04-17 09:17:13.018	복사	demo3 onodeName node-0 agentime 1744849031927 oid -278185929 category AppStdErr okindName dev-okind-0					
▶ java-demo3	2025-04-17 09:17:13.018	검색	rtual.web.Simula.exec(Simula.java:79)					
▶ java-demo3	2025-04-17 09:17:13.018	제외 검색	demo3 onodeName node-0 agentime 1744849031927 oid -278185929 category AppStdErr okindName dev-okind-0					
▶ java-demo3	2025-04-17 09:17:13.018	인접 로그	ion: java.lang.RuntimeException: random exception					
▶ java-demo3	2025-04-17 09:17:13.018	트랜잭션 정보	demo3 onodeName node-0 agentime 1744849031928 oid -278185929 category AppStdErr okindName dev-okind-0					
			rtual.web.VExec.doFilter(VExec.java:16)					

로그 태그 옵션 메뉴	설명
복사	태그에 해당하는 로그를 복사합니다.
검색	필터에 해당 태그가 포함('==') 조건으로 입력됩니다.
제외 검색	필터에 해당 태그가 제외('!=') 조건으로 입력됩니다.
인접 로그	인접 로그 상세 창에서 선택한 로그의 서버를 대상으로 선택한 로그와 인접한 시간대의 로그를 조회합니다. 시간을 선택해 인접한 시간대의 로그를 조회할 수 있습니다. 기준 로그는 파란색 바탕으로 표시됩니다.
트랜잭션 정보	로그에 @txid 및 @mtid 태그가 포함된 경우, 트랜잭션 정보를 클릭하면 트랜잭션 정보 상세창에서 정보를 확인할 수 있습니다.

콘텐츠 하이라이트

로그의 콘텐츠 중 원하는 키워드를 손쉽게 식별하기 위해 하이라이트 기능을 제공합니다. 단일 또는 복수 키워드로 필터링할 수 있습니다.

1. 키워드 입력창에 하이라이트를 원하는 키워드를 입력하세요.

- 예시, `select`

2. 로그 목록의 Content 내 검색한 키워드가 하이라이팅 됩니다.

- [] **로그 전체 화면** 아이콘을 선택하면 **로그**와 **타임스탬프**를 전체 화면에서 확인할 수 있습니다.
- 하이라이트된 키워드 간 이동은 단축키로 조작할 수 있습니다.
 - `Enter` : 다음 row로 이동
 - `Shift+Enter` : 이전 row로 이동
 - `^ / v` 아이콘: row 이동
 - `Cmd + F (Mac) / Ctrl + F (Windows)`: 키워드 검색

복수 키워드 조건

복수 키워드로 하이라이팅을 할 경우 다음과 같이 작성합니다.

입력 문자열	설명	결과
<code>a b c</code>	띄어쓰기로 각 키워드를 구분합니다.	a, b, c
<code>"Whatap is good."</code>	띄어쓰기를 키워드에 포함하고 싶은 경우 <code>"</code> 또는 <code>""</code> 로 감쌉니다.	Whatap is good.
<code>"Whatap\\ is good."</code>	<code>""</code> 로 감싸진 키워드에서 <code>\</code> 를 포함할 경우, <code>\\</code> 로 입력해야 합니다.	Whatap\ is good.

하이라이트 색상 설정

하이라이팅할 키워드 및 색상을 설정할 수 있습니다.

- 기본적으로 로그 레벨에 따른 하이라이팅(**FATAL**, **ERROR**, **WARN**, **SEVERE**, **CRITICAL**)이 적용되어 있습니다.
- 설정된 내용은 **프로젝트** 단위로 저장됩니다.
 -  아이콘을 클릭하세요.
 - 하이라이트** 창에서 추가적으로 색상 설정을 원하는 키워드를 입력창에 입력하세요.
 - 입력창 왼쪽 색상 클릭 시 색을 선택할 수 있습니다.

테이블 설정하기

컬럼 설정

컬럼을 추가하거나 순서를 설정할 수 있습니다. ③ 영역 오른쪽에서  컬럼 설정 버튼을 클릭하세요.

컬럼 추가

태그를 선택하여 테이블에 컬럼을 추가할 수 있습니다. **log** 컬럼 선택을 해제할 경우 **로그 표시 상세 설정**을 확인할 수 없습니다. 반드시 한 개 이상의 컬럼을 선택하세요.

- 제공되는 컬럼: 로그, 수집 시간, content(로그 메시지)

컬럼 순서 변경

컬럼을 추가하면 **표시 항목**에 해당 컬럼이 추가됩니다. 원하는 컬럼을 드래그하여 컬럼의 순서를 변경하세요.

로그 표시 상세 설정

③ 영역 오른쪽에서  **로그 표시 상세 설정** 버튼을 선택하세요. 기본으로 **content**, **태그** 모두 체크가 되어있으며 두 가지 항목 모두 표시합니다. **content**와 **태그** 중 하나는 반드시 선택하세요.

체크가 해제된 항목은 테이블에 표시되지 않습니다. 다음과 같이 **태그**를 해제할 경우 테이블에서 로그의 **태그**는 표시되지 않습니다.



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.

❗ 컬럼 및 로그 표시 설정 적용 범위

- 컬럼 설정과 로그 표시 상세 설정은 **라이브 테일**, **로그 검색**, **로그 트렌드**에서 사용할 수 있습니다.



- 동일한 프로젝트 내 **라이브 테일**, **로그 검색**, **로그 트렌드**는 **컬럼 설정**과 **로그 표시 상세 설정**을 공유합니다.

로그 파일 다운로드

검색한 로그의 결과값을 **CSV**, **TXT** 파일 형식으로 수집된 로그를 다운로드 받을 수 있습니다.

1. 화면 중앙의 오른쪽의 **↓ 다운로드** 버튼을 클릭합니다.
2. **CSV 다운로드** 또는 **Log 다운로드**를 클릭해 원하는 형태의 파일을 다운로드 받습니다.

로그 설정

홈 화면 > 프로젝트 선택 > 로그 > 로그 설정

로그 설정의 상단의 탭에서 로그 모니터링을 설정할 수 있습니다. 에이전트 설정 확인, 로그 모니터링의 활성화 여부 결정, 로그 데이터의 유지 기간 및 조회 비밀번호 설정, 로그 파서 등록, 빠른 인덱스 설정, 개인정보 비식별화 관리 등을 할 수 있습니다.

! 권한

- 로그 모니터링 활성화를 사용하려면 프로젝트 수정 권한이 필요합니다.
- 로그 편집 권한이 있으면 로그 모니터링 활성화 외 로그 설정 메뉴를 수정할 수 있습니다.

로그 모니터링 시작하기

[로그모니터링 시작하기](#) [로그 필터 설정](#) [로그 1차 파서 설정](#) [로그 2차 파서 설정](#) [빠른 인덱스 설정](#) [로그 장기 보관 통제](#) [개인정보 비식별화](#)

에이전트 설정 및 로그 모니터링 활성화

라이브 태일, 로그 트렌드 기능으로 애플리케이션의 출어진 로그를 한 눈에 확인하실 수 있습니다.

1. 에이전트 설정 확인

JAVA 애플리케이션에서 로그를 수집하려면 다음을 확인해주세요.
1. 에이전트 버전 확인 및 업그레이드 (v2.1.1 이상 버전부터 가능)
2. 에이전트 설정 > 직접 입력 > 아래의 에이전트 설정 명령어를 입력해주세요.
3. 다시 시작

에이전트 설정

logsink_enabled=true [📄 복사](#)

2. 로그 모니터링 활성화

로그 모니터링 데이터 설정

로그 조회 비밀번호

☐ 로그 조회 비밀번호를 사용하려면 커주세요.

로그 보존 기간 (초기값)

15일

최소 1일부터 최대 40일까지 입력이 가능합니다.

로그 사용량

카테고리	데이터 보존 기간	누적 로그 수 (보존 기간 기준)	일 평균 로그 수	현재 로그 수	일주일 예상 로그 수	한 달 예상 로그 수
Total		3,542,799,864	236,186,659	124,084,216	1,653,306,592	7,085,599,680
AppLog	15일	3,513,550,837	234,236,722	123,070,829	1,639,657,054	7,027,101,660
AppStdErr	15일	340,021	22,668	12,222	158,676	680,040
AppStdOut	15일	13,951,508	930,100	483,168	6,510,700	27,903,000
VirtualLog	15일	14,957,498	997,166	517,997	6,980,162	29,914,980

- 로그 > 로그 설정의 로그모니터링 시작하기 탭을 클릭하세요.
- [📖](#) 가이드 보기 아이콘과 [요금제 보기](#) 버튼을 클릭하면 안내 화면으로 이동합니다.

에이전트 설정 및 로그 모니터링 활성화

1 영역에서 에이전트 설정을 확인하고 로그 모니터링 활성화 및 비활성화 여부를 설정할 수 있습니다.

에이전트 설정 확인

로그 모니터링을 시작하기 위해 에이전트 버전과 설정 정보를 확인하세요. 1. **에이전트 설정 확인**에서 안내에 따라 진행하세요.

- 애플리케이션 모니터링

애플리케이션별 적용 방법은 [Java](#), [PHP](#), [Node.js](#), [Python](#), [Go](#) 문서를 참고하세요.

- 서버 모니터링

서버 모니터링 적용 방법은 [Server](#) 문서를 참고하세요. 안내에 따라 [whatap.conf](#)에 로그 감시 대상 파일 설정을 추가하세요.

- 쿠버네티스 모니터링

쿠버네티스 모니터링 적용 방법은 [Kubernetes](#) 문서를 참고하세요.

로그 모니터링 활성화

로그 모니터링을 활성화 또는 비활성화할 수 있습니다. 2. **로그 모니터링 활성화**에서 로그 모니터링 여부를 설정하세요.

-  로그 모니터링 활성화: 토글 버튼을 켜면 로그 모니터링이 활성화되고, 활성화한 날부터 15일 동안 무료로 체험하실 수 있습니다.
-  로그 모니터링 비활성화: 토글 버튼을 끄면 로그 모니터링이 비활성화되고, 로그를 더 이상 저장하지 않습니다.

로그 모니터링 데이터 설정

로그 사용량을 확인할 수 있습니다. 또한 **로그 보존 기간** 및 **로그 조회 비밀번호** 설정을 변경할 수 있습니다.

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 사용자는 **로그 설정**에서 새 비밀번호로 변경할 수 있습니다.

로그 보존 기간

공통으로 적용할 기본(default) 데이터 보존 기간입니다.

- 최소 1일부터 최대 40일까지 입력할 수 있습니다. 미지정 시 기본값은 1일입니다. 로그 보존 기간 선택 옵션 외에 사용자가 원하는 기간을 입력할 수 있습니다.
- **로그 사용량** 목록에서 별도로 설정하지 않으면 이 로그 데이터 보존 기간이 기본적으로 적용됩니다. **로그 사용량** 목록에서 카테고리별 데이터 보존 기간을 설정하고 **초기화** 버튼을 클릭하면 기본 데이터 보존 기간으로 초기화됩니다.

로그 사용량

로그 사용량 목록에서 카테고리별 로그 데이터 보존 기간을 지정할 수 있습니다. 로그 수는 해당 기간 동안 쌓인 로그 건수를 의미합니다. 예를 들어 **금일 로그수**는 하루 동안 쌓인 로그 건수, **예상 로그수**는 데이터 보관일에 금일 로그 수를 곱한 로그 건수를 의미합니다.

로그 데이터 보존 기간을 다음과 같이 지정할 수 있습니다. 기간 지정에 따라 오래된 데이터를 삭제해 공간을 확보할 수 있습니다.

- **트라이얼 프로젝트**

데이터 보존 기간으로 1일, 2일, 3일을 선택할 수 있습니다.

- **유료 프로젝트**

데이터 보존 기간으로 1일, 2일, 3일, 4일, 5일, 6일, 7일, 10일, 30일, 40일을 선택할 수 있습니다.

- **저장량 기준 과금**

데이터 보존 기간에 따라 비용이 달라집니다.

예, 일 평균 200만 로그 건수가 쌓이고 데이터 보존 기간을 3일로 지정한 경우라면 평균 600만 로그 건수가 수집 서버에 유지되고 과금 대상이 됩니다.

로그 필터 설정

로그 필터 설정은 사용자가 지정한 필터 조건에 해당하는 로그만 저장하는 기능입니다. 사용자가 필요한 로그만 저장하여 비용을 절감할 수 있습니다.

❗ 권한

로그 편집 권한이 있는 사용자만 설정할 수 있습니다.

로그 필터 설정 추가하기

새로운 필터 설정을 추가하는 방법입니다. 로그 필터 설정 시 **필터 이름**, **라이브 테일 표시 여부**, **카테고리**, **필터 조건**은 필수 입력 항목입니다.

로그 필터 설정에서 저장하지 않는 로그도 **라이브 테일 표시 여부** 토글을 활성화하면 **라이브 테일**에서 확인할 수 있습니다.

❗ 카테고리별로 하나의 필터만 설정할 수 있습니다.

1. **로그 > 로그 설정 > 로그 필터 설정** 탭으로 이동하세요.
2. 로그 필터 설정을 위해 **+ 추가하기** 버튼을 클릭하세요.
3. 로그 필터 설정 추가에서 **필터 이름**, **라이브 테일 표시 여부**, **카테고리**, **필터 조건**을 입력하세요.
 - **필터 이름**: 필터를 식별할 수 있는 이름
 - **라이브 테일 표시 여부**: 저장 여부와 관계없이 라이브 테일에 표시 여부 선택
 - **카테고리**: 필터가 적용될 로그 카테고리 (**복수 선택 가능**)
 - **필터 조건**: 필터 조건에 저장할 로그의 조건

❗ 필터 조건 설정 시, 자세한 내용은 [WhaTap log search query 문법](#)을 참고하세요.

- 예시

- **포함:** `oid : 123`
 - oid가 123인 로그만 수집합니다.
 - **불포함:** `not oid : 123`
 - oid가 123이 **아닌** 로그만 수집합니다.
 - **전체 포함:** 필터 조건 미입력
 - **전체 불포함:** `not content : *`
4. 추가 버튼을 클릭하면 **등록 결과 미리보기**에서 각 필터 설정을 확인하고 수정할 수 있습니다.
 5. 확인이 완료되었다면 **적용** 버튼을 클릭해 로그 필터 설정을 적용합니다.

시뮬레이션

사용자가 입력한 카테고리나 필터 조건으로 로그를 미리 검색하여, 로그 필터 설정을 적용하기 전에 결과를 확인할 수 있습니다.

시뮬레이션 버튼을 클릭하면 로그 필터 설정이 적용된 **로그 검색** 화면이 나타납니다.

로그 필터 설정 수정하기

등록한 로그 필터는 필요에 따라 수정 아이콘을 클릭해 수정할 수 있습니다. **로그 필터 설정 수정**에서 기존에 입력한 값이 표시되며, 원하는 항목을 변경한 뒤 적용하면 됩니다.

 로그 필터 설정을 수정할 때, 하나의 카테고리만 선택할 수 있습니다.

로그 필터 설정 삭제하기

등록한 필터는 삭제 아이콘을 클릭해 삭제할 수 있습니다. 삭제 후 반드시 **저장** 버튼을 클릭하세요.

 변경 사항을 저장하지 않으면 필터가 삭제되지 않습니다.

로그 필터 설정 JSON 가져오기/내보내기

로그 필터 설정은 JSON 형식으로 Import/Export 할 수 있습니다. 다른 프로젝트로 동일한 로그 필터 설정을 쉽게 적용할 수 있습니다. 다른 프로젝트로 로그 필터 설정 내용을 그대로 옮기고 싶은 경우 유용하게 사용할 수 있습니다.

JSON 내보내기

1. 화면 오른쪽 위의  버튼을 클릭하세요.
2. JSON 내보내기 창이 열리면, 내보내기 버튼을 클릭하세요.
3. 로그 필터 설정 내용이 JSON 형식의 파일로 다운로드됩니다.

JSON 가져오기

1. 화면 오른쪽 위의  버튼을 클릭하세요.
2. 가져올 JSON 형식의 파일을 선택하세요.
3. JSON 가져오기 창에서 목록에 추가하기 또는 덮어쓰기 버튼을 클릭해 로그 필터 설정을 가져옵니다.
4. 저장 버튼을 클릭해 변경 사항을 반영합니다.

유효성 검사 조건

설정 내용 저장 시 유효성 검사 내용은 다음과 같습니다.

- **type:** GENERAL 만 지원
- **category:** 필수값으로 string 타입 지원
- **condition**
 - **language:** jsonDsl , lucene 만 지원
 - **description:** 유효하지 않은 필터 조건이면 저장 불가
- **showLiveTail:** boolean 타입만 지원
- **name:** 필수값으로 string 타입 지원

로그 파서 설정

로그 1차 파서 설정

로그 설정 상단의 **로그 1차 파서 설정** 탭을 선택해 수집된 로그에 대한 파서를 등록할 수 있습니다.

로그 1차 파서는 **GROK**과 **JSON** 파서를 제공하며 유형별 로그 발생 수 집계나 특정 로그 탐색을 위한 필수 파서입니다. 패턴 조건에 맞는 검색 키와 검색 값을 추출하며, 파싱된 키는 로그 유형 분류 및 검색 인덱싱에 활용합니다.

- **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 , okindName , @txid , @login , httpost

파서 등록이 불가능한 예약어

timestamp , message , pcode , category , content , logContent

- 다음 예약어의 경우 파서를 등록하더라도 인덱스가 생성되지 않습니다.

❗ 로그 파서에 대한 자세한 내용은 [다음 문서](#)를 참고하세요.

설정 항목

설정 값	설명	기타
카테고리	패턴을 적용할 카테고리	required
로그 검출 조건	필터로 적용할 검색 키, 검색 값을 입력 - 로그 검출 조건에 맞는 로그 데이터에만 패턴 적용, 로그 검출 조건을 입력하지 않으면 모든 로그를 대상으로 패턴 적용	optional

설정 값	설명	기타
패턴	로그를 파싱(parsing)할 패턴 - 작성한 패턴에 맞추어서 파싱을 하고 인덱스 생성 GROK, 정규 표현식 문법 지원	required

파서 목록

등록한 파서를 조회하고, 추가 및 편집할 수 있습니다. 파서는 등록 순서대로 적용되며, 최초로 일치하는 파서만 적용됩니다.

- 상단 오른쪽 + 추가하기 버튼을 클릭하면 **파서 추가** 창이 나타납니다.
- **적용 순서** 컬럼의 ≡ 아이콘을 드래그해 파서 설정 순서를 변경할 수 있습니다.
-  **활성화** 토글로 파서 활성화 여부를 지정할 수 있습니다.
-  수정 및  삭제 아이콘을 통해 등록된 파서를 수정 및 삭제할 수 있습니다.

파서 등록

다음은 파서를 등록하는 공통 순서입니다.

1. 로그 1차 파서 설정에서 + 추가하기 버튼을 클릭하세요.
2. 파서 추가 창에서 파서를 선택하세요.

❗ 파서 및 패턴 등록 방법

- [GROK 파서 및 패턴 등록](#)
- [JSON 파서 및 패턴 등록](#)

3. 파서를 선택하면 **패턴 등록** 버튼이 활성화됩니다. **패턴 등록** 버튼을 클릭한 후, **파서 시뮬레이션** 창에서 패턴과 로그를 입력합니다.
 - a. **패턴**을 입력하세요.
 - b. 로그의 **카테고리**와 **시뮬레이션 파싱 로그**를 입력하세요. **로그 검색** 버튼을 클릭한 후, 검색된 목록에서 원하는 로그 오른쪽의 **선택** 버튼을 클릭하면 로그가 자동으로 입력됩니다.

❗ 로그 검색을 통해 수집된 로그 중 예시 로그를 선택할 수 있습니다. 선택한 로그는 시뮬레이션 입력창에 자동 반영되어 복사/붙여넣기 없이 바로 테스트할 수 있습니다.

c. 등록하려는 패턴이 정상인지 **시뮬레이션** 버튼을 클릭해 시뮬레이션 및 패턴의 퍼포먼스를 측정하세요.

❗ 시뮬레이션과 퍼포먼스 측정에 관한 자세한 내용은 [다음 문서](#)를 참고하세요.

4. 성공적으로 파싱되는지 시뮬레이션 결과를 확인한 후, **패턴 적용** 버튼을 클릭하세요.
5. **추가** 버튼을 클릭하면 파서가 추가됩니다.

❗ 개인정보 비식별화

파서 등록 시 검색 키 이름을 **검색 키.p**로 지정하면 비식별화 대상이 됩니다(예: **myname.p** **). 와탭은 **개인정보 비식별화** 탭에서 비식별화를 관리하는 방식을 권장합니다. 자세한 내용은 [개인정보 비식별화](#)를 참고하세요.

GROK 파서 패턴 등록

기본 문법은 `%{SYNTAX:SEMANTIC}` 입니다. GROK 파서에 대한 자세한 내용은 [다음 문서](#)를 참조하세요. 패턴 등록 및 시뮬레이션이 필수적입니다.

• SYNTAX

GROK 정의 패턴입니다.

• SEMANTIC

파싱된 데이터에 할당할 키입니다.

❗ SEMANTIC에는 예약어 등이 사용되지 않도록 조합어 사용을 권장합니다.

JSON 포맷 파서 패턴 등록

로그 전체 또는 일부가 JSON 형태로 출력되는 경우 해당 부분을 파싱할 수 있습니다. **Prefix, Postfix** 옵션으로 JSON 인식 범위를 지정합니다. JSON 파서에 대한 자세한 내용은 [다음 문서](#)를 참조하세요. 시뮬레이션이 필수적입니다.

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 뒤까지를 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"}
```

- Response 파싱용 패턴

"Response : " 부터 로그의 마지막까지의 문자열 {"key3":"value3","key4":"value4",...} 대상

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

파서 시뮬레이션 및 퍼포먼스 측정

파서 시뮬레이션 후 패턴을 등록할 수 있습니다. **퍼포먼스 측정**은 시뮬레이션 수행 대상 문자열에 대하여 파서의 반복 파싱 소요 시간을 측정합니다.

1. 패턴과 로그를 입력하세요. 로그 검색 버튼을 클릭한 후, 검색된 목록에서 원하는 로그 오른쪽의 선택 버튼을 클릭하면 로그가 자동으로 입력됩니다.
2. 시뮬레이션 버튼을 클릭하여 등록하려는 패턴으로 파싱에 성공하는지 확인하세요.
3. 시뮬레이션 성공 시 시뮬레이션 결과 및 퍼포먼스 측정 결과를 조회할 수 있습니다.
4. 시뮬레이션 후 패턴 적용 버튼 클릭 시 선택한 파서에 입력한 패턴이 적용됩니다.

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 등록할 수 있습니다.

로그 2차 파서는 1차 파서(GROK 또는 JSON)로 추출한 값을 가공해 통계 데이터나 새로운 필드를 생성합니다. HTTP 상태 코드 기반 통계 파서와 함께 키워드 필터, 필드 가공, 응답 시간 분류, GeoIP 변환 등 다양한 프로세서를 제공합니다.

❗ 로그 2차 파서는 1차 파싱된 결과에 대하여 특수 목적의 2차 파싱 기능을 제공합니다. 2차 파서를 사용하기 위해서는 1차 파서가 등록되어 있어야 합니다.

파서 목록

로그 설정						
로그 모니터링 시작하기 로그 1차 파서 설정 로그 2차 파서 설정 빠른 인덱스 설정 로그 장기 보관 통계 로그 1시간 통계 위젯 데이터 설정						
로그 2차 파서 설정 Grok 또는 JSON 파서가 이미 파싱된 경우 사용할 수 있는 파서입니다.						
+ 추가하기 저장						
적용 순서	파서	카테고리	필터	패턴	활성화	
0	4xx, 5xx 상태 코드 파서	AppLog	없음		☒	 
1	상태 코드 성공률 파서	AppLog	없음		☒	 

등록한 파서를 조회하고, 추가 및 편집할 수 있습니다.

파서 추가, 순서 변경, 활성화 토글, 수정 및 삭제 등의 조작 방법은 **1차 파서 목록**과 동일합니다.

파서 등록 순서

다음은 파서를 등록하는 공통 순서입니다.

×

파서 추가

파서 *

와탭은 와탭 서비스의 안정성에 영향을 줄 수 있는 파서를 비활성화할 수 있는 권한을 가집니다.

4xx, 5xx 상태 코드 파서

제외할 상태 코드

입력한 상태 코드는 4xx, 5xx 상태 코드로 로그를 파싱할 때 제외됩니다.

400 × 404 ×

카테고리 *

같은 카테고리에 여러 개의 파서가 등록되어 있는 경우 첫 번째로 매칭되는 파서만 적용됩니다.

AppLog

로그 검출 조건

로그 검출 조건을 입력하지 않거나, 검색키/값중 한개만 입력하는 경우 모든 로그를 대상으로 패턴을 적용합니다.

oname

demo-8100

추가

1. + 추가하기 버튼을 선택하면 파서 추가 창이 나타납니다.
2. 파서 선택 창에서 파서를 선택하세요. 각 파서별 설정 항목은 다음 문서를 참조하세요.
 - [4xx, 5xx 상태 코드 파서 설정 항목](#)
 - [상태 코드 성공률 파서 설정 항목](#)
3. 제외할 상태 코드를 입력하세요.
4. 카테고리 선택 창에서 카테고리를 선택하거나 직접 입력하세요.
5. 로그 검출 조건을 선택하거나 직접 입력하세요.
6. 추가 버튼을 선택해 파서를 등록하세요.

4xx, 5xx 상태 코드 파서 설정 항목

4xx, 5xx 상태 코드 파서는 1차 파서로 파싱된 status 값을 기반으로 4xx, 5xx 건수 데이터를 생성합니다. 특정 상태 코드를 제외하려면 제외할 상태 코드를 입력하세요.

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 상태 코드	통계 데이터 생성 시 제외할 상태 코드입니다. 입력하지 않으면 4xx~5xx에 해당하는 전체 오류 상태 코드를 대상으로 4xx, 5xx건수 데이터를 생성합니다.	optional

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					☐		
1					☐		
2	GROK	AppLog	모든 로그	%{NUMBER:status}	☒		

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 통합 Flex 보드로 이동해 로그 4XX, 5XX 건수 위젯을 생성하세요.

위젯 템플릿

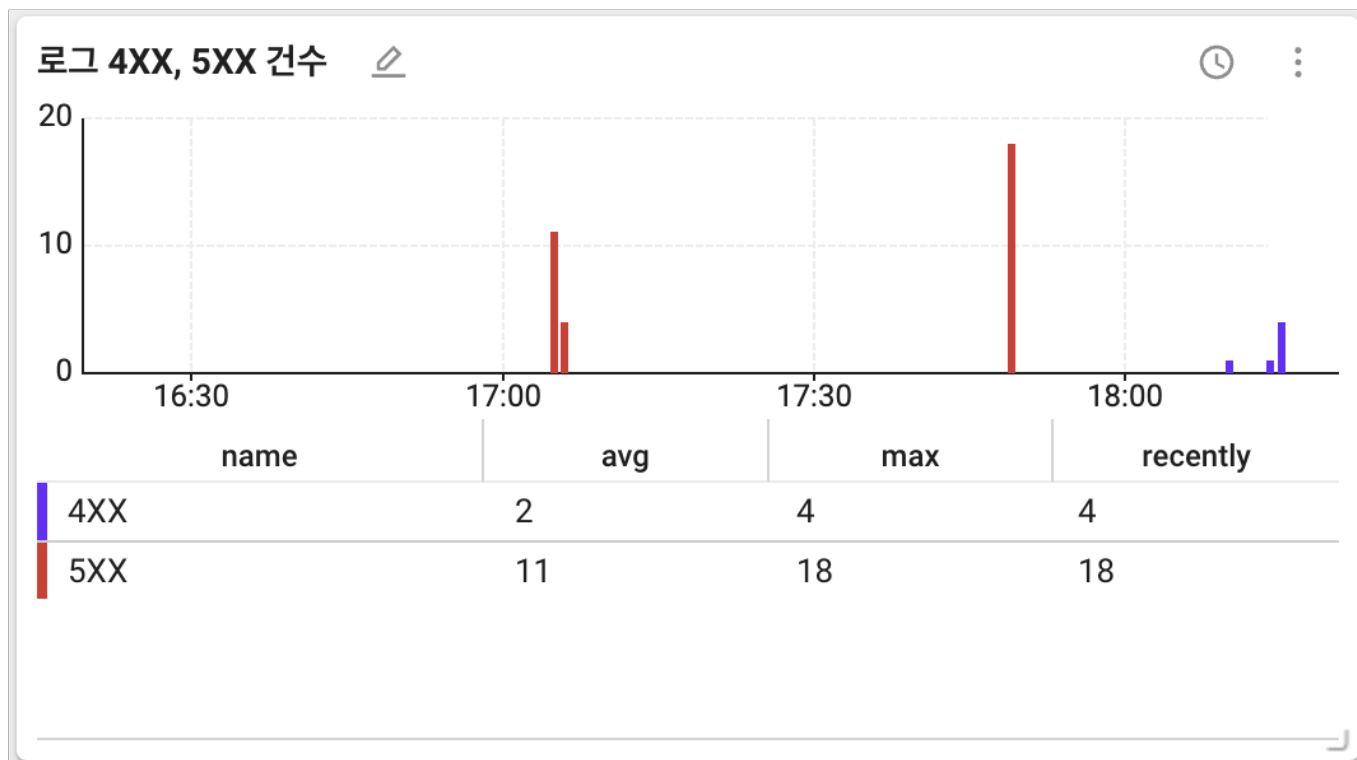
모든 메트릭스

4xx

Q

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 설정 항목

상태 코드 성공률 파서는 1차 파서로 파싱된 status 값을 기반으로 HTTP 요청 성공률 데이터를 생성합니다. 특정 상태 코드를 제외하려면 제외할 상태 코드를 입력하세요. status 파싱에 관한 내용은 [4xx, 5xx 상태 코드 파서 설정 항목](#)을 참조하세요.

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
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 **통합 Flex 보드**로 이동해 로그 요청 성공률 위젯을 생성하세요.

위젯 템플릿

⇒ 모든 메트릭스

요청 성공률

Q

로그 요청 성공률

위젯을 생성하면 다음과 같이 데이터를 확인할 수 있습니다.

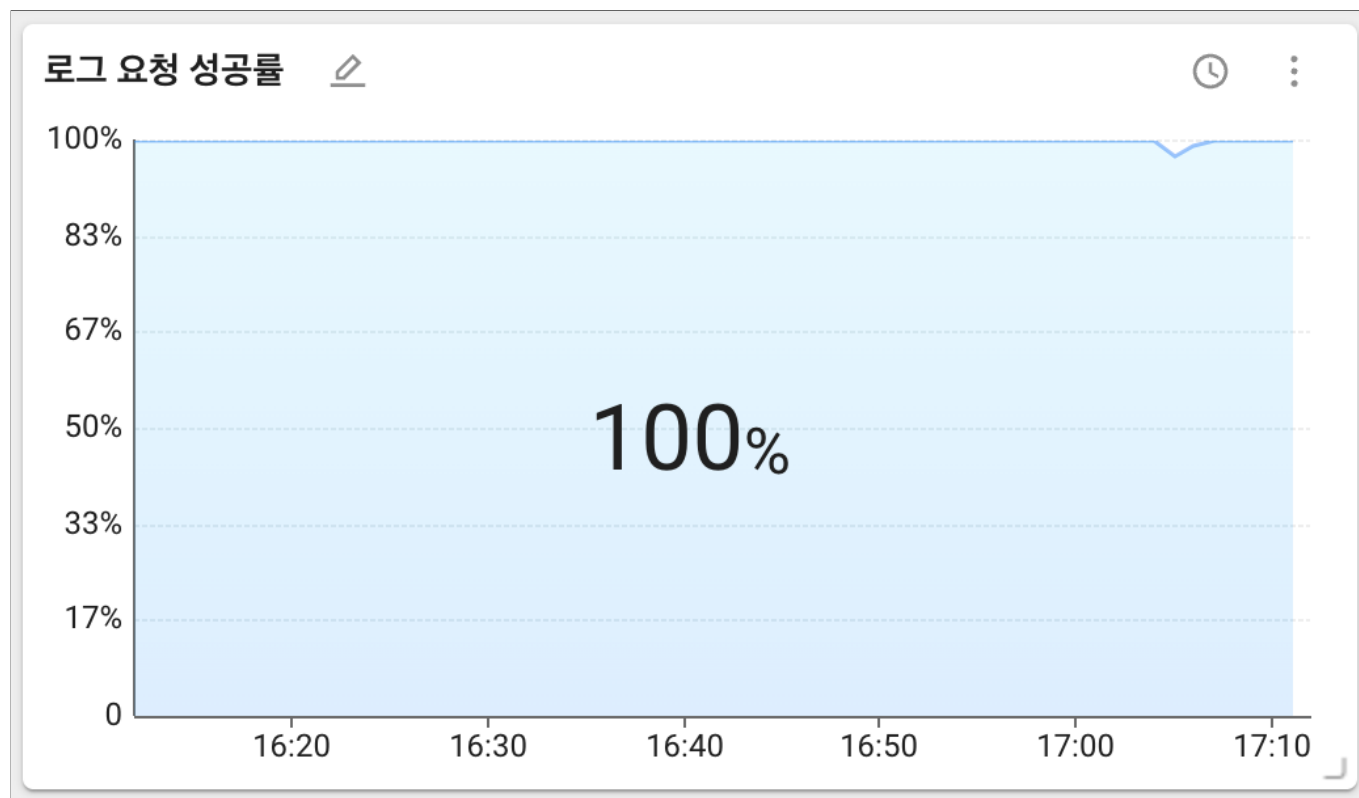


차트 위 데이터는 조회 기간에 대한 통계를 나타냅니다. 통계 방법을 최근값, 최댓값, 평균값 등으로 선택할 수 있습니다. 최근값이 기본으로 선택되어 있습니다.

2차 파서 프로세서

로그 2차 파서는 **4xx, 5xx 상태 코드 파서**와 **상태 코드 성공률 파서** 외에도 다음과 같은 필드 가공 프로세서를 제공합니다.

로그 2차 파서 프로세서 목록

프로세서	설명
모든 키워드 포함 필터	지정한 모든 키워드가 포함된 로그에 플래그 필드를 추가합니다.
일부 키워드 포함 필터	지정한 키워드 중 하나라도 포함된 로그에 플래그 필드를 추가합니다.
필드명 변경	기존 필드명을 다른 이름으로 변경합니다.

프로세서	설명
상태 코드 그룹 분류	HTTP 상태 코드를 2xx/3xx/4xx/5xx 그룹으로 자동 분류합니다.
URL 정적/동적 분류	URL에 확장자(.)가 있으면 정적 콘텐츠, 없으면 동적 서블릿으로 분류합니다.
URL 파라미터 제거	URL에서 ? 이후의 쿼리 파라미터를 제거한 값을 저장합니다.
응답 시간 분류	응답 시간(ms)을 fast/normal/slow/critical 구간으로 자동 분류합니다.
JSON 필드 추출	JSON 문자열 필드에서 특정 키를 추출하여 새 필드로 저장합니다.
GeoIP 변환	IP 주소를 국가/도시 정보로 변환합니다.
직접 입력	FQN 클래스명으로 프로세서를 직접 등록합니다.

모든 키워드 포함 필터

지정한 모든 키워드가 포함된 로그에 플래그 필드를 추가합니다.

설정 값	설명	기본값
입력 필드	키워드를 검색할 필드명	content
저장 필드	결과를 저장할 필드명	has_str_all
keyword	검색할 키워드 목록 (쉼표로 구분해 입력)	required

활용 예시: 입력 필드를 content , 키워드를 error, timeout, database 로 설정하면 세 키워드가 모두 포함된 로그에만 has_str_all 필드가 추가됩니다.

일부 키워드 포함 필터

지정한 키워드 중 하나라도 포함된 로그에 플래그 필드를 추가합니다.

설정 값	설명	기본값
입력 필드	키워드를 검색할 필드명	content
저장 필드	결과를 저장할 필드명	has_str_any
keyword	검색할 키워드 목록 (쉼표로 구분해 입력)	required

활용 예시: 입력 필드를 content , 키워드를 reboot, shutdown, restart 로 설정하면 키워드 중 하나라도 포함된 로그에 has_str_any 필드가 추가됩니다.

필드명 변경

기존 필드명을 다른 이름으로 변경합니다. 대상 필드명이 이미 존재하면 덮어쓰지 않습니다.

설정 값	설명	기본값
원본 필드	변경할 기존 필드명	required
새 필드명	변경 후 필드명	required

상태 코드 그룹 분류

HTTP 상태 코드를 status_2xx , status_3xx , status_4xx , status_5xx 그룹으로 자동 분류합니다.

설정 값	설명	기본값
입력 필드	상태 코드가 담긴 필드명	status
저장 필드	그룹 분류 결과를 저장할 필드명	status_nxx

활용 예시: status 값이 404 이면 status_nxx 필드에 status_4xx 가 저장됩니다.

URL 정적/동적 분류

URL에 확장자(.)가 포함되어 있으면 정적 콘텐츠, 포함되지 않으면 동적 서블릿으로 분류합니다.

설정 값	설명	기본값
입력 필드	URL이 담긴 필드명	url
저장 필드	분류 결과를 저장할 필드명	url_type

URL 파라미터 제거

URL에서 ? 이후의 쿼리 파라미터를 제거한 경로만 저장합니다.

설정 값	설명	기본값
입력 필드	URL이 담긴 필드명	url
저장 필드	파라미터 제거 결과를 저장할 필드명	url_without_params

활용 예시: /api/v1/users?page=1&size=20 → url_without_params 필드에 /api/v1/users 가 저장됩니다.

응답 시간 분류

응답 시간(ms)을 구간별로 자동 분류합니다. 구간 임계값을 직접 설정할 수 있습니다.

설정 값	설명	기본값
입력 필드	응답 시간(ms)이 담긴 필드명	elapsed
저장 필드	분류 결과를 저장할 필드명	response_class
Fast 상한(ms)	fast 구간 상한값	100
Normal 상한(ms)	normal 구간 상한값	500
Slow 상한(ms)	slow 구간 상한값	2000

기본값 기준 분류 결과는 다음과 같습니다.

응답 시간	분류
0 ~ 100ms	fast
101 ~ 500ms	normal
501 ~ 2000ms	slow
2001ms 이상	critical

활용 예시: 로그 탐색에서 `response_class: critical` 로 필터링하면 응답 시간이 2초를 초과하는 로그만 조회할 수 있습니다.

JSON 필드 추출

1차 파서로 추출한 필드에 JSON 문자열이 포함된 경우 해당 JSON에서 특정 키를 추출하여 새 필드로 저장합니다.

설정 값	설명	기본값
입력 필드	JSON 문자열이 담긴 필드명	payload
추출할 키	추출할 JSON 키 목록 (쉼표로 구분해 입력)	required
저장 접두사	추출된 키 이름 앞에 붙일 접두사 (예: json_)	optional

- ❗ 로그 전체가 JSON인 경우 1차 JSON 파서가 자동으로 파싱합니다. 이 프로세서는 **GROK 1차 파서** 사용 시 텍스트 로그 안에 포함된 JSON 부분을 추가로 파싱할 때 유용합니다.
- 성능 보호를 위해 JSON 필드 크기가 10KB를 초과하면 파싱을 건너웁니다.

활용 예시

1차 GROK 파싱 결과

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

입력 필드 `payload` , 추출할 키 `user, action` , 저장 접두사 `pay_` 설정 시 다음과 같이 추출됩니다.

JSON 필드 추출 결과

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

GeoIP 변환

IP 주소를 국가 및 도시 정보로 변환합니다. IP2Location 데이터베이스를 활용해 접근 로그의 지역별 분석이 가능합니다.

설정 값	설명	기본값
입력 필드	IP 주소가 담긴 필드명	client_ip
저장 접두사	결과 필드 이름의 접두사	geo

결과로 {접두사}_country, {접두사}_city 두 개의 필드가 생성됩니다.

활용 예시: 입력 필드 client_ip 값이 223.130.195.200 이고 저장 접두사가 geo 인 경우:

GeoIP 변환 결과

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

직접 입력

목록에 없는 프로세서를 FQN(Fully Qualified Name) 클래스명으로 직접 등록할 수 있습니다.

직접 입력 형식

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

❗ 클래스명과 파라미터 형식이 정확해야 합니다. 잘못된 입력 시 프로세서가 동작하지 않을 수 있습니다.

2차 파서 체이닝

동일 카테고리에 여러 2차 파서를 등록해 체이닝할 수 있습니다. 각 프로세서는 등록 순서대로 실행됩니다.

원본 로그

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

순서	파서	입력 → 출력
1차	GROK	timestamp, level, host, client_ip, url, status, elapsed, payload, content
2차-1	JSON 필드 추출	payload → user, action
2차-2	응답 시간 분류	elapsed → response_class (slow)
2차-3	상태 코드 그룹 분류	status → status_nxx (status_2xx)
2차-4	URL 파라미터 제거	url → url_without_params (/api/v1/orders)
2차-5	GeoIP 변환	client_ip → geo_country (KR), geo_city (Seoul)

❗ 2차 파서의 **카테고리**는 1차 파서와 동일하게 설정해야 합니다. 다른 카테고리로 설정하면 해당 로그에 2차 파서가 적용되지 않습니다.

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 [다음](#)을 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	<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.

❗ 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)?`
- 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

①

!

문법	의미	별칭
?	0 or 1	-
+	1 or more	-
*	0 or more	-
a{5}	exactly 5	-
\w	word character	[a-zA-Z_0-9]



문법	의미	별칭
<code>\s</code>	white space	-
<code>.</code>	any character except newline	-
<code>[abc]</code>	any of	-
<code>[^abc]</code>	not a,b, or c	-
<code>[a-z]</code>	character between a and z	-
<code>[1-3[7-9]]</code>	union (combining two or more character classes)	-
<code>[1-6&&[3-9]]</code>	intersection (교집합)	-
<code>[0-9&&[^2468]]</code>	subtraction (차집합)	-
<code>a{2,}</code>	2 or more	-
<code>a{1,3}</code>	between 1 and 3	-
<code>a+?</code>	match as few as possible	-
<code>{2,3}?</code>	match as few as possible	-
<code>(abc)</code>	capturing group (여러 개의 문자열을 single unit으로 처리함)	-
<code>\d</code>	digit	<code>[0-9]</code>
<code>\D</code>	non-digit	<code>[^0-9]</code>
<code>\W</code>	non-word character	-
<code>\S</code>	non-white space	-

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. **패턴 등록** 버튼 선택 시 오른쪽에 패턴 등록 및 시뮬레이션 창이 나타납니다.
4. **패턴**과 **로그** 입력 후 **시뮬레이션** 버튼을 클릭하여 적용하려는 패턴으로 파싱에 성공하는지 확인하세요.

패턴 예시:

```
[%{TIMESTAMP_ISO8601:date}\sGMT}\[%{LOGLEVEL:level}\s][%{DATA:caller}\s](?<projectCode>\d)\s(?<logCategory>\w*)\s\d{2}:\d{2}:\d{2}\.\d{3})\s\{area=(?<areaEnum>\d),\scity=(?<cityEnum>\d)\}\s(?<dexBuildElapsed>\d{2})ms
```

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
```

5. 시뮬레이션 성공 시 **시뮬레이션 결과** 및 **퍼포먼스 측정 결과**를 조회할 수 있습니다.
6. 시뮬레이션 후 **패턴 적용** 버튼 클릭 시 선택한 파서에 입력한 패턴이 적용됩니다.
7. 패턴 적용 후 **카테고리** 및 **로그 검색 조건**, **패턴**을 입력하세요.

X

파서 추가

파서 *

와탭은 와탭 서비스의 안정성에 영향을 줄 수 있는 파서를 비활성화할 수 있는 권한을 가집니다.

GROK

파서 패턴 *

입력한 패턴으로 로그가 성공적으로 파싱되는지 시뮬레이션 진행 후 패턴을 등록합니다.

✓ 성공

```
\{%{TIMESTAMP_ISO8601:date}\sGMT%\}%{\LOGLEVEL:.level}\s%\}%{\DATA.caller}\s(?<projectCode>\d)\s(?<logCategory>w*)\s(?<dexBuildStartTime>\d(8)\s\d(2)\s\d(2)\s\d(2)\s\d(3))\s\{area=(?<areaEnum>\d),\scity=(?<cityEnum>\d)\}\s(?<dexBuildElapsed>\d(2))ms
```

파서 패턴 수정

카테고리 *

같은 카테고리에 여러 개의 파서가 등록되어 있는 경우 첫 번째로 매칭되는 파서만 적용됩니다.

AppLog

로그 검출 조건

로그 검출 조건을 입력하지 않거나, 검색키/값중 한개만 입력하는 경우 모든 로그를 대상으로 패턴을 적용합니다.

oname

demo-8100

- 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.

8. 추가 버튼을 선택해 파서를 등록하세요.

- 로그 파서 목록에서 해당 파서의 **적용 순서**를 변경하거나 **활성화** 및 **수정**, **삭제**할 수 있습니다.
- **파서 시뮬레이션** 후 패턴을 등록할 수 있습니다.

❗ 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 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.

GROK 추가 패턴 선택하기

GROK 파서 시뮬레이션 시 기본 패턴(`WORD` , `NUMBER` , `IP` 등) 외에 특정 로그 형식에 맞는 **추가 패턴**을 선택할 수 있습니다. Java, Nginx, MySQL 등 32개 패턴 타입이 11개 카테고리로 그룹핑되어 제공됩니다.

추가 패턴 카테고리 드롭다운

1. 파서 시뮬레이션 창에서 **추가 패턴 (선택)** 영역의 드롭다운을 클릭하세요.
2. 카테고리별로 그룹핑된 패턴 타입 목록에서 필요한 패턴 타입을 선택하세요. 검색 입력란에 패턴 타입 이름 또는 설명을 입력해 검색할 수도 있습니다.
3. 선택한 패턴 타입은 시뮬레이션 시 기본 패턴과 함께 로드됩니다.

❗ 기본 패턴(Core)은 항상 자동으로 포함됩니다. 추가 패턴 선택은 선택 사항입니다.

카테고리별 패턴 타입 목록

카테고리	패턴 타입
Web Servers	haproxy, httpd, iis, nginx, squid
Application Servers & Frameworks	java, log4j, rails, ruby, springboot

카테고리	패턴 타입
Databases	mongodb, mysql, oracle, postgresql, redis
Cloud	aws
System & Infrastructure	docker, kubernetes, linux-syslog
Messaging & Search	elasticsearch, kafka
Network & Security	bind, bro, firewalls, junos, zeek
Mail	exim, postfix
Monitoring & Backup	bacula, mcollective, nagios
Build Tools	maven

활용 예시

Tomcat Catalina 8 로그를 파싱하려면 **java** 패턴 타입을 추가로 선택한 뒤 `%{CATALINA8_LOG}` 패턴을 사용하세요.

Sample log

```
31-Jul-2020 16:40:38 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Server version name: Apache Tomcat/8.5.57
```

GROK parsing pattern

```
%{CATALINA8_LOG}
```

Tag extraction

```
- log_timestamp : 31-Jul-2020 16:40:38
- log_level : INFO
- java.log.origin.thread.name : main
- java.log.origin.class.name : org.apache.catalina.startup.VersionLoggerListener
- log.origin.function : log
```

- log_message : Server version name: Apache Tomcat/8.5.57

패턴 상세 보기

선택한 추가 패턴 타입에 어떤 패턴이 포함되어 있는지 상세 창에서 확인할 수 있습니다. 패턴 정의(정규 표현식)와 샘플 로그를 조회하고 시뮬레이션에 바로 적용할 수 있습니다.

패턴 상세 보기

추가 패턴 타입을 선택한 뒤 선택된 패턴 타입 태그를 클릭하면 오른쪽에 상세 창이 열립니다. 상세 창은 시뮬레이션 폼을 가리지 않고 나란히 표시되므로, 패턴 정의를 확인하면서 시뮬레이션을 진행할 수 있습니다.

각 패턴 항목에서 다음 기능을 사용할 수 있습니다.

버튼	기능	설명
샘플	샘플 로그 입력	해당 패턴에 매칭되는 예시 로그를 시뮬레이션 파싱 로그 입력란에 자동으로 입력합니다.
선택	패턴 삽입	<code>%{패턴이름}</code> 형식으로 패턴 입력란에 삽입합니다. 해당 패턴 타입도 자동으로 선택됩니다.
복사	클립보드 복사	<code>%{패턴이름}</code> 형식을 클립보드에 복사합니다.

- ① 패턴 항목을 클릭하면 패턴 정의(정규 표현식)가 펼쳐집니다. 여러 패턴을 동시에 펼쳐 정의를 비교할 수 있습니다.
- 패턴 정의에 포함된 `%{PATTERN:field}` 참조는 패턴 이름, 필드명, 리터럴 문자가 서로 다른 색상으로 구분되어 표시됩니다.
- 샘플 버튼으로 입력된 로그로 바로 **시뮬레이션**을 실행해 파싱 결과를 확인할 수 있습니다.

시뮬레이션 샘플 로그 저장

시뮬레이션에 사용한 로그는 파서 설정과 함께 자동으로 저장됩니다. 파서를 수정할 때 이전에 사용한 샘플 로그가 시뮬레이션 창에 자동으로 복원되어 매번 로그를 다시 입력할 필요가 없습니다.

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. **+ 추가하기**를 선택 후 **파서** 입력란에서 **JSON** 파서를 선택하세요.
3. **패턴 등록** 버튼 선택 시 오른쪽에 패턴 등록 및 시뮬레이션 창이 나타납니다.
4. **패턴**과 **로그** 입력 후 **시뮬레이션** 버튼을 클릭하여 적용하려는 패턴으로 파싱에 성공하는지 확인하세요.

Example

```
2023-08-08 02:43:28,615 -- {"host":"10.21.3.24","method":"POST","status":"200","url":"http://dev.whatap.io/yard/api/flush"} --
```

예시 로그에서 **Prefix**와 **Postfix**를 `--` 로 지정하고 **Ignore**에 `url` 을 지정 시 `host` , `method` , `status` 3개의 태그만 생성됩니다.

- **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.

5. 시뮬레이션 성공 시 **시뮬레이션 결과** 및 **퍼포먼스 측정 결과**를 조회할 수 있습니다.

패턴

agenttime, category, content, logContent, message, pcode, time, timestamp는 예약어입니다.
예약어는 로그 검색 조건, 패턴으로 등록해도 동작하지 않습니다.

Prefix --

Postfix --

Ignore url

로그

로그 시뮬레이션은 필수적으로 수행되어야 하며, 시뮬레이션 결과에 따라 패턴 등록이 추가로 필요할 수 있습니다.

```
2023-08-08 02:43:28.615 -
{"host":"10.21.3.24","method":"POST","status":"200","url":"http://devote.whatsapp.io/yard/api/flush"} -

```

시뮬레이션 결과

시뮬레이션 결과

키	값	결과
method	POST	Ok
host	10.21.3.24	Ok
status	200	Ok

퍼포먼스 측정 결과

시뮬레이션 횟수	최소 시간(ns)	최대 시간(ns)	평균 시간(ns)
1	16,619	16,619	16,619
10	3,604	4,976	4,090
100	3,583	132,590	6,244
1,000	2,729	113,655	4,467
10,000	2,729	109,320	2,989
100,000	2,651	310,343	2,987
1,000,000	2,647	117,486,886	3,157

패턴 적용

6. 시뮬레이션 후 **패턴 적용** 버튼 클릭 시 선택한 파서에 입력한 패턴이 적용됩니다.
7. 패턴 적용 후 **카테고리** 및 **로그 검색 조건**, **패턴**을 입력하세요.

패서 추가

파서

와탭은 와탭 서비스의 안정성에 영향을 줄 수 있는 파서를 비활성화할 수 있는 권한을 가집니다.

JSON

파서 패턴

로그가 성공적으로 파싱되는지 시뮬레이션합니다. 시뮬레이션은 필수적으로 수행되어야 하며, 시뮬레이션 결과에 따라 패턴 등록이 추가로 필요할 수 있습니다.

성공

Prefix --

Postfix --

Ignore url

시뮬레이션 검증 및 패턴 수정

카테고리

같은 카테고리에 여러 개의 파서가 등록되어 있는 경우 첫 번째로 매칭되는 파서만 적용됩니다.

AppLog

로그 검색 조건

로그 검색 조건을 입력하지 않거나, 검색키/값 한개만 입력하는 경우 모든 로그를 대상으로 패턴을 적용합니다.

oname

demo-8100

추가

326

- 카테고리

로그 카테고리를 선택하세요. **카테고리**는 필수로 입력해야 합니다.

- 로그 검출 조건

- 조건에 만족하는 로그만 파서가 적용됩니다.
- **검색 키와 검색 값**을 선택하거나 직접 입력하세요.
- **로그 검출 조건**은 모든 파서가 수행되기 전에 적용됩니다. 즉 파서의 결과로 추가되는 **태그**를 사용할 수 없습니다.

8. 추가 버튼을 선택해 파서를 등록하세요.

- ! • 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://dev.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://dev.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 빠른 인덱스 설정

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
대소문자 구분 안 함	옵션	대소문자 구분 여부
규칙	필수	* 한 개 이상 포함 필수
활성	필수	활성 또는 비활성 여부(기본값 true)

로그 장기 보관 통계 설정

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*

통계 키를(를) 입력해주세요

데이터 보관일(디스크 사용량)

15일 (약 3 MB) ▾

카테고리*

AppLog

로그 검출 조건*

oname ▾ —

× 검색 값을(를) 선택해주세요

제외 ☐ 대소문자 구분 ☒

okind ▾ —

× 검색 값을(를) 선택해주세요

제외 ☐ 대소문자 구분 ☒

+ 추가하기

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 카테고리입니다.
통계 키(key)	규칙을 만족하는 로그 발생 시 저장할 키 값으로 동일한 키를 중복으로 설정할 수 없습니다.
로그 검출 조건	로그 통계 데이터를 생성할 조건입니다. 이 조건을 만족하는 로그가 얼마나 수집되었는지를 기반으로 통계 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 <code>true</code>)

예시

다음과 같이 설정을 추가한 경우 수집된 로그 중 status가 200 , 300 인 로그를 대상으로 TotalCount라는 키값으로 통계 데이터를 생성합니다.

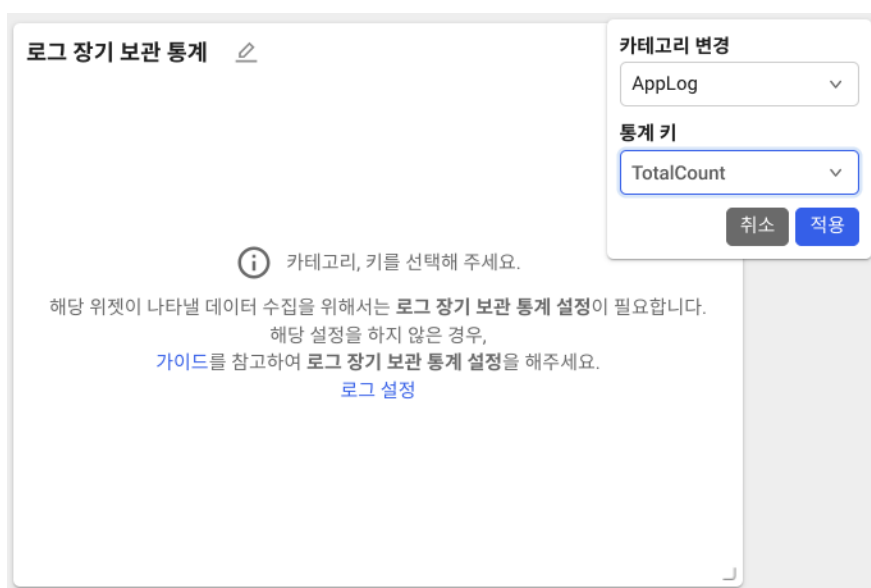
로그 장기 보관 통계 설정한 조건을 만족하는 로그가 얼마나 수집되었는지 통계 데이터를 생성할 수 있습니다. ⓘ					+ 추가하기	저장
카테고리	통계 키	로그 검출 조건	데이터 보관일(디스크 사용량)	활성화		
AppLog	TotalCount	status 200,300	15일 (약 3 MB)	☐	ⓘ	🗑
AppLog	TotalCount	status 200	15일 (약 3 MB)	☐	ⓘ	🗑
AppLog	TotalCount	status 300	15일 (약 3 MB)	☒	ⓘ	🗑
AppLog	TotalCount	status 200,300	15일 (약 3 MB)	☒	ⓘ	🗑
AppLog	TotalCount	status 200,300	15일 (약 3 MB)	☐	ⓘ	🗑

데이터 조회

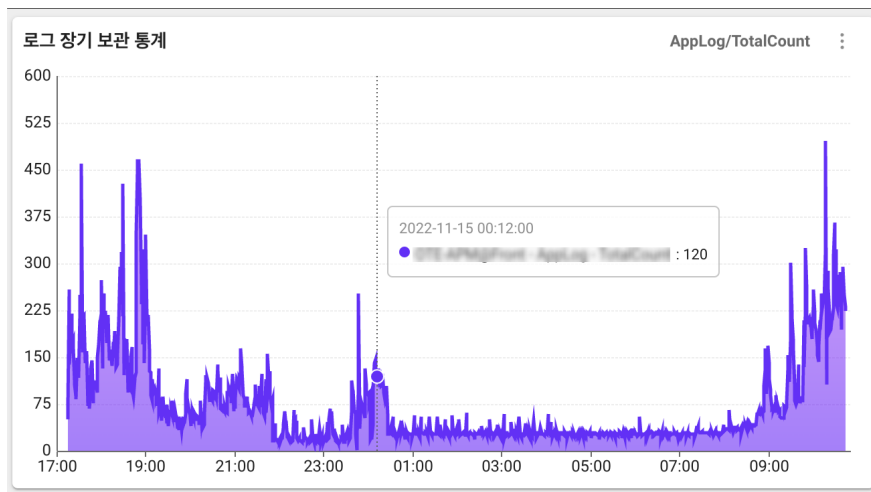
1. 통합 Flex 보드의 위젯 템플릿에서 로그 장기 보관 통계를 검색해 위젯을 생성하세요.



2. 데이터를 조회할 카테고리나 통계 키를 지정한 뒤 적용 버튼을 선택합니다.



3. 추가한 설정값으로 로그 장기 보관 통계 데이터를 다음처럼 확인할 수 있습니다.



로그 개인정보 비식별화 설정

개인정보 비식별화

개인정보 비식별화에서 로그 데이터 내 개인정보를 마스킹 처리하거나 안전한 값으로 치환할 수 있습니다.

- 암호화 저장: 지정된 민감 정보는 암호화되어 데이터베이스에 저장됩니다.
- 마스킹 처리: 로그 화면에 표시될 때 민감 정보는 기본적으로 마스킹(******) 처리되어 표시됩니다.
- 치환 처리: 민감한 정보를 사용자가 지정한 안전한 값으로 변경합니다.

개인정보 분류

일반적으로 개인정보로 분류하는 항목은 다음과 같습니다. 일반 개인정보 외에도 민감정보로 처리해야 하는 항목이 있다면 **개인정보 비식별화** 기능을 통해 로그 내에서 원하는 항목을 마스킹 처리 또는 치환 처리하세요.

- 주민등록번호
- 여권번호
- 운전면허번호
- 외국인 등록번호
- 신용카드 번호
- 계좌번호
- 생체인식 정보

요구 권한

비식별화된 개인정보는 마스킹 처리되어 표시됩니다. **로그 개인정보 조회** 권한이 있는 사용자만 **개인정보 표시** 토글을 통해 원본 데이터를 확인할 수 있습니다. 비식별화 대상 검색 키의 추가 및 수정은 **로그 편집** 권한이 필요합니다.

❗ 로그 개인정보 조회 권한 및 로그 편집 권한에 대한 자세한 내용은 [다음 문서](#)를 확인하세요.

개인정보 비식별화 설정

신규 로그 데이터에 마스킹 처리를 적용하여 민감 정보를 보호할 수 있습니다.

로그 설정

로그모니터링 시작하기 로그 1차 파서 설정 로그 2차 파서 설정 빠른 인덱스 설정 로그

개인정보 비식별화 개인정보가 포함된 검색 키를 추가하면 해당 데이터를 암호화하여 저장

활성화 카테고리

AppLog @txid agenttime @mti

로그 개인정보 비식별화 점검 이전에 생긴 로그들을 비식별화 처리합니다.

시간 < 2025/01/21 15:45 ~ 2025/01/21 16:45 1시간 >

카테고리 카테고리(들) 선택해주세요

개인정보 항목

개인정보 패턴

지환 적용 여부

지환 값

점검 시작 점검 중지

개인정보 비식별화 추가

카테고리* 카테고리(들) 선택해주세요

검색 키* 암호화 저장 및 마스킹 처리할 검색 키를 선택합니다. 암호화할 검색 키를 입력하세요.

추가

1. 개인정보 비식별화 탭에서 추가하기 버튼을 선택하세요.
2. 오른쪽 개인정보 비식별화 추가 창에서 카테고리를 선택하고, 마스킹 처리할 검색 키를 입력하세요.
3. 추가 버튼을 클릭하여 설정을 추가하세요.
4. 개인정보 비식별화 목록에서 비식별화 항목 확인 후 오른쪽 상단 저장 버튼을 눌러 현재 설정을 저장하세요.

개인정보 비식별화 개인정보가 포함된 검색 키를 추가하면 해당 데이터를 암호화하여 저장하고 마스킹 처리 합니다.				+ 추가하기	저장
활성화	카테고리	검색 키	편집		
☐	VirtualLog	age.n	🔗 🗑		
☒	VirtualLog	status	🔗 🗑		
☒	AppLog	agenttime	🔗 🗑		

- 비식별화 처리된 검색 키의 경우 로그 콘텐츠 내 검색 키.pii 형식으로 출력됩니다.
- 개인정보 비식별화 목록 내 활성화 컬럼에서 비식별화 항목을 ☒ 활성화할 수 있습니다.

- 개인정보 비식별화 목록 내 편집 컬럼에서  수정 및  제거할 수 있습니다.

🟢 로그 1차 파서 설정 탭에서 검색 키 이름을 **검색 키.p** 로 지정하면 비식별화 대상으로 자동 등록됩니다. 자동 등록된 항목은 개인정보 비식별화 탭에서 **카테고리** 선택 후 **지정된 검색 키**에서 확인하거나 해제할 수 있습니다.

파서에서 .p 접미사로 지정하는 방식보다 개인정보 비식별화 탭에서 직접 설정하는 것을 권장합니다.

개인정보 표시

비식별화된 데이터는 **라이브 테일**, **로그 트렌드**, **로그 검색** 메뉴에서 마스킹 상태로 표시됩니다. 로그 개인정보 조회 권한이 있는 사용자는 로그 목록의 **개인정보 표시**  버튼을 클릭해 원본 데이터를 확인할 수 있습니다.

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

⚠ 개인정보 비식별화 탭에서 지정한 검색 키는 로그 메뉴 내 로그 콘텐츠에서 **검색 키.pii** 형식으로 나타납니다.

예시, **status.pii** **

로그 개인정보 비식별화 점검

⚠ 로그 개인정보 비식별화 점검 기능을 통해 기존 데이터를 치환할 경우 해당 데이터는 원복이 불가능합니다.

로그 개인정보 비식별화 점검은 기존 로그 데이터 내 개인정보를 식별하여 사용자가 지정한 **치환 값**으로 대체합니다.

대상 키 지정 치환

대상 키를 지정하면 해당 키에 저장된 값만 치환하고 나머지 로그 내용은 그대로 유지합니다. 대상 키는 로그의 **field** 값과 **tag** 값 모두에 적용됩니다. 대상 키를 지정하지 않으면 기존과 동일하게 로그 콘텐츠 전체에서 개인정보를 식별해 치환합니다.

❗ 치환은 저장된 로그 데이터에만 적용됩니다. 검색 인덱스에는 치환 이후에도 원본 값이 남아 있을 수 있습니다.

대상 키는 로그 개인정보 비식별화 점검 품의 **대상 키** 입력란에 지정하며, 화면에서는 **field** 와 **tag** 를 구분하지 않고 하나의 대상 키로 입력합니다.

로그 개인정보 비식별화 점검
이전에 쌓인 로그들을 비식별화 처리합니다.

시간

< 2025/03/21 12:26 ~ 2025/03/21 13:26 1시간 >

카테고리

VirtualLog

개인정보 항목

주민등록번호

개인정보 패턴

(?<!\w)\d{2}(0[1-9]|1[0-2])([0-2][0-9]|3[0-1]){1-4}\d{6}(?!w)

치환 적용 여부

☐

치환 값

*****_*****

점검 시작

점검 중지

카테고리

VirtualLog

검색 시작 시간

2025/03/21 12:26

검색 종료 시간

2025/03/21 13:26

개인정보 항목

주민등록번호

개인정보 패턴

(?<!\w)\d{2}(0[1-9]|1[0-2])([0-2][0-9]|3[0-1]){1-4}\d{6}(?!w)

치환 값

*****_*****

패턴 매칭 결과

0 결과 확인

점검 작업 시작 시간

2025/03/21 13:28

점검 작업 종료 시간

2025/03/21 13:28

치환 적용 여부

No

점검 작업 결과

SUCCESS

1. 시작 시간 및 종료 시간을 설정하세요.
2. 카테고리를 설정하세요.
3. 개인정보 항목을 예시 중 선택 또는 직접 입력을 선택하세요.

❗ 직접 입력 선택 시 개인정보를 식별하기 위한 정규표현식 패턴을 직접 입력합니다.

4. 치환 적용 여부 토글을 통해 개인정보가 식별된 경우 이를 치환할지 여부를 선택하세요.
5. 기존 로그에서 정규표현식 패턴으로 식별된 문자열을 변경할 **치환 값**을 입력하세요.

- ❗ **치환 값**은 원본 값보다 길어서는 안됩니다.
- 치환 적용 여부** 토글 활성화 시 반드시 **치환 값**을 입력해야 합니다.

6. 조건 입력 후 **점검 시작** 버튼을 선택하세요.

- ❗ 점검 중인 경우 언제든지 **점검 중지** 버튼을 통해 점검 과정을 중지할 수 있습니다.

7. 치환 적용 시 **개인정보 비식별화 점검 시작** 확인 창에서 **치환하기** 입력 후 **확인** 버튼을 클릭하세요.

개인정보 비식별화 점검 시작

선택하신 개인정보 패턴에 매칭되는 값을 치환합니다.

❗ 치환 이후 데이터 원복은 되지 않습니다.

치환을 원하신다면 아래 "치환하기"를 직접 입력하세요.

치환하기

취소

확인

8. 점검 작업 완료 후 예시 이미지와 같이 오른쪽에서 **점검 작업 결과**를 확인할 수 있습니다.

- 카테고리**: 점검된 카테고리 정보를 표시합니다.
- 검색 시작 시간** 및 **검색 종료 시간**: 점검이 실행된 시간 범위를 표시합니다.
- 개인정보 항목**: 점검된 개인정보 항목을 표시합니다.
- 개인정보 패턴**: 사용된 정규표현식 패턴을 표시합니다.
- 치환 값**: 적용된 치환 값을 표시합니다.
- 패턴 매칭 결과**: 식별된 개인정보 개수를 표시합니다. **결과 확인** 클릭 시 샘플 로그를 확인할 수 있습니다.
- 점검 작업 결과**: 개인정보가 식별된 결과를 표시합니다.

SUCCESS (점검 성공), FAILED (점검 실패), STOP (점검 중지), TIMED_OUT (시간 초과로 점검 종료)

점검 이력 확인

로그 개인정보 비식별화 점검을 진행한 후 과거에 수행된 점검 결과를 조회하려면 상단 오른쪽에서 **점검 이력 확인** 버튼을

클릭하세요. 치환 내역, 점검 시점, 적용된 개인정보 항목 등을 추적할 수 있습니다. 또한 **점검 이력 확인** 창 상단 오른쪽에서 **↓ CSV** 버튼 클릭 시 **CSV** 파일 형식으로 해당 목록 정보를 다운로드할 수 있습니다.

점검 이력 확인

< 2025/03/25 08:17 ~ 2025/03/25 09:17 1시간 >

개인정보 항목

↓ CSV

값	패턴 매칭 결과	점검 작업 시작 시간	점검 작업 종료 시간	치환 적용 여부	점검 작업 결과
*****	0	2025/03/25 09:16	2025/03/25 09:16	No	SUCCESS
*****	0	2025/03/25 09:16	2025/03/25 09:16	No	SUCCESS
*****	0	2025/03/25 09:16	2025/03/25 09:16	No	SUCCESS

개인정보 패턴

기존 로그 데이터에서 개인정보를 식별할 때 사용되는 정규표현식 패턴 예시는 다음과 같습니다.

개인정보 패턴	개인정보 예시	정규식 패턴	치환 값
주민등록번호	123456-1234567	(?<!w)d{2}(0[1-9] 1[0-2])([0-2][0-9] 3[0-1])-[1-4]d{6}(?!w)	*****_ *****
여권번호	M1234567	([MSRODTC][0-9]{7}\b)	*****
운전면허번호	01-23-456789-00	(?<!w)d{2}-d{2}-d{6}-d{2}(?!w)	**_**_ *****_**
외국인등록번호	987654-1234567	(?<!w)d{6}-?[5-8]d{6}(?!w)	*****_ *****
신용카드번호	1234-5678-9012-3456	(?<!w)d{4}-d{4}-d{4}-d{4}(?!w)	****_*_*_*_ ****_*_*_*

개인정보 패턴	개인정보 예시	정규식 패턴	치환 값
전화번호	010-1234-5678	(?<!w)(+82-?1[016789]-?d{3,4}-?d{4} 01[016789]-?d{3,4}-?d{4})(?!w)	**-***_ ****
이메일 주소	example@domain.com	([a-zA-Z0-9][a-zA-Z0-9._%+-]*@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,})	**@**.*
계좌번호	123456-01-654321	(?<!w)d{6}-d{2}-d{6}(?!w)	*****_ *****
사업자등록번호	111-11-01111	(?<!w)d{3}-d{2}-d{5}(?!w)	**-*_* *****
법인등록번호	111111-1111111	(?<!w)d{6}-?d{7}(?!w)	*****_ *****

로그 설정 가져오기/내보내기

로그 설정 가져오기/내보내기

파서 설정, 빠른 인덱스 설정, 필터 설정 내용을 JSON 파일로 내보내고, 다른 프로젝트에서 가져와 적용할 수 있습니다. 프로젝트마다 반복해서 설정을 작성하는 번거로움을 줄일 수 있습니다.

1. 하나의 프로젝트에 파서 설정, 빠른 인덱스 설정, 필터 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.

경고 알림

모니터링 대상 시스템 또는 애플리케이션에서 문제가 발생했을 때, 미리 설정한 조건에 따라 사용자에게 알림을 전달하는 기능입니다. 알림은 이메일, SMS, 메신저, 앱 푸시 등 다양한 채널로 전송됩니다.

예를 들어, CPU 사용률, 메모리 사용량, 디스크 I/O, 네트워크 트래픽, 트랜잭션 수, 오류 발생, 응답 시간 지연 등 주요 성능 지표에 알림 기준을 설정해두면, 해당 기준을 초과하거나 이상 징후가 감지될 때 알림이 전송됩니다.

와탭의 AI 기반 알림 기능을 사용하면 복잡한 조건을 직접 설정하지 않아도 됩니다. AI는 애플리케이션의 정상적인 동작 패턴을 학습해 이상 패턴을 자동으로 감지하여 알려줍니다. 태그 카운트 알림 기능을 활용하면 특정 태그 기반으로 집계된 값에 조건을 설정하여 복잡한 상황도 정밀하게 감지할 수 있습니다.

주요 기능

- **이벤트 설정:** 임계치 기반 알림 조건과 수신 채널 설정
- **이벤트 수신 설정:** 사용자별 수신 채널, 시간대 설정
- **이벤트 기록:** 알림 발생 기록 조회

권한

이벤트를 추가하거나 설정하려면 **알림 설정 권한**이 필요합니다.

- **조회:** 메트릭스 이벤트 설정 내용을 확인하려면 **조회 분석 권한**이 필요합니다.
- **추가/수정/삭제:** 설정을 변경하려면 **알림 설정 권한**이 필요합니다.
- **알림 수신:** 알림을 수신하려면 **알림 수신 권한**이 필요합니다.

❗ 참고 문서

자세한 내용은 [멤버 권한](#)을 참고하시기 바랍니다.

이벤트 설정

홈 화면 > 프로젝트 선택 >  경고 알림 > 이벤트 설정

이벤트 설정에서 모니터링 대상 시스템 또는 애플리케이션에서 발생할 수 있는 이상 징후를 기준으로 이벤트를 설정하고 관리하는 기능을 제공합니다. 설정된 조건이 충족되면 이메일, SMS, 메신저, 앱 푸시 등 원하는 채널로 알림을 받을 수 있습니다. 모니터링 목적에 따라 이벤트를 구성할 수 있습니다.

메트릭스

메트릭스 이벤트는 실시간 데이터를 기반으로 시스템 및 애플리케이션의 성능 지표를 모니터링할 수 있습니다.

실시간 로그

실시간으로 수집한 로그에서 설정한 이벤트 조건이 발견되면 경고 알림을 보냅니다.

복합 로그

로그 내용을 기준으로 경고 알림을 발생시키는 복합 로그 이벤트를 설정합니다.

참고

- 이벤트 설정 시 적정 임계값을 사용하여 불필요한 이벤트 발생을 방지하세요.
- 알림 설정 시 해소 알림(문제 해결 시 알림) 여부도 함께 고려하면 운영 대응에 도움이 됩니다.

공통 기능

모든 이벤트 설정을 **JSON** 또는 **Excel** 형식으로 다운로드할 수 있습니다. 같은 유형의 제품 설정을 공유하면 반복되는 이벤트 설정 작업을 줄일 수 있습니다.

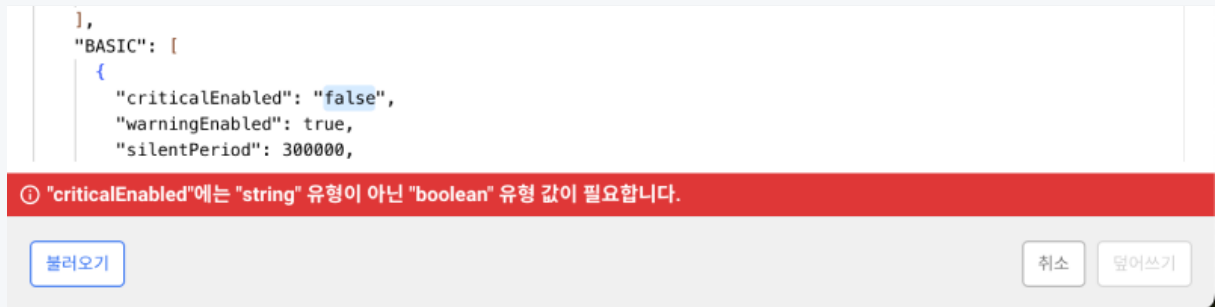
- **JSON 일괄 수정**: 모든 이벤트 조건을 JSON 형식으로 일괄 수정할 수 있습니다.
- **JSON 일괄 다운로드**: 현재 등록된 이벤트 조건을 JSON 파일로 저장할 수 있습니다.
- **Excel 일괄 다운로드**: 이벤트 목록을 Excel 파일로 내려받아 외부 보고나 백업에 활용할 수 있습니다.

JSON 일괄 수정

1. 화면 상단의 [JSON 일괄 수정] 버튼을 클릭하세요.
2. **JSON 일괄 다운로드** 기능을 통해 다운로드 받은 JSON 파일을 가져오거나 직접 수정하세요.
3. [덮어쓰기] 버튼을 클릭해 저장합니다.
4. 확인 메시지가 나타나면 [덮어쓰기] 버튼을 클릭하세요.

! 덮어쓰기 후 이전의 이벤트 설정으로 복구할 수 없습니다.

- `productType` 또는 `platform` 속성의 값을 임의로 수정하면 다른 프로젝트에서 이벤트가 정상 동작하지 않을 수 있습니다.
- JSON 편집창은 JSON 검증(Validation) 기능이 내장되어 있습니다. 형식이나 값이 올바르지 않은 경우, 편집창 아래에 오류 메시지가 표시되며 [덮어쓰기] 버튼은 비활성화됩니다.



JSON 데이터 구조





```
{
  "productType": "{productType}",
  "platform": "{platform}",
  "events": {
    "HITMAP": {
      ...
    },
    "LOG_REALTIME": [
      {...}
    ],
    "METRICS": [
      {...}
    ],
    "COMPOSITE_LOG": [
      {...}
    ],
    "BASIC": [
      {...}
    ],
    "COMPOSITE_METRICS": [
      {...}
    ],
    "ANOMALY": [
      {...}
    ]
  ]
}
```

JSON 필드	설명
productType	제품 타입(예: APM, Infra 등)
platform	플랫폼 정보(예: java, node 등)
events	이벤트 데이터
└ HITMAP	히트맵 패턴

JSON 필드	설명
└ LOG_REALTIME	실시간 로그 이벤트
└ METRICS	메트릭스
└ COMPOSITE_LOG	복합 로그 이벤트
└ BASIC	기본 이벤트
└ COMPOSITE_METRICS	복합 메트릭스
└ ANOMALY	이상치 탐지

JSON 일괄 다운로드

화면 상단의 [JSON 일괄 다운로드] 버튼을 클릭하세요.

- JSON 파일 이름은 `integrated-event-YYYYMMDD.json` 형식입니다.
- JSON 데이터의 구조와 `events` 속성의 하위 속성은 제품(`platform`) 또는 제품 유형(`productType`)에 따라 다를 수 있습니다.

⚠ JSON 데이터의 속성 중 `productType` 또는 `platform` 속성의 값을 임의로 수정하면 다른 프로젝트에서 이벤트가 동작하지 않을 수 있습니다.

Excel 일괄 다운로드

화면 상단의 [Excel 일괄 다운로드] 버튼을 클릭하세요.

메트릭스

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

프로젝트에 설정된 모든 메트릭스 기반 이벤트 목록을 확인할 수 있습니다. 사용자가 설정한 메트릭스 이벤트를 확인, 수정, 삭제하거나, 새로운 이벤트를 추가할 수 있습니다.

기본 옵션

- **이벤트 레벨:** 이벤트의 심각도를 의미하며 정상(Info), 경고(Warning), 위험(Critical) 세 단계로 구분
- **에이전트 중복 알림:** 설정한 시간(30초, 1분, 3분, 5분, 10분)에 같은 이름의 에이전트가 동시에 2개 이상 동작하는 경우, 선택한 시간 동안 이벤트 발생 안함
- **검색:** 이벤트 이름을 기준으로 검색
- **JSON 다운로드/업로드:** 이벤트 규칙은 JSON 편집기를 통해 바로 수정하거나, 파일로 다운로드하여 수정 후 다시 업로드 가능
- **+ 이벤트 추가:** 새로운 메트릭스 이벤트 추가
- **컬럼 크기 조정:** 각 컬럼의 경계를 드래그하여 너비 조정 가능

표 | 메트릭스 이벤트 목록 구성

항목	설명
No.	이벤트의 순번
	이벤트의 활성화 여부 - 활성화: 조건을 충족하면 이벤트 발생 - 비활성화: 이벤트가 동작하지 않으며, 조건을 검사하지 않음
	이벤트 설정 편집 및 삭제
이벤트 이름	사용자가 지정한 이벤트명 - 최대 255자까지 입력 가능
규칙	이벤트 발생 조건

항목	설명
대상	이벤트가 적용되는 모니터링 대상
발생 횟수	이벤트 발생 기준이 되는 기간과 횟수 - 선택한 시간 동안 설정한 횟수만큼 조건을 충족하면 이벤트 발생
일시 중지	이벤트 알림 발생 후, 같은 이벤트 발생을 일정 시간 동안 멈춤 - 선택 가능 시간: 사용 안 함, 5분, 10분, 15분, 20분, 30분, 1시간, 2시간, 3시간, 6시간, 12시간, 1일 - 해소된 알림이 활성화된 경우, 정상(RECOVERED) 상태 알림을 받은 후 선택한 시간 동안 같은 이벤트가 발생해도 알림이 발생하지 않음
해소된 알림	Critical 과 Warning 레벨의 이벤트가 해소되면 RECOVERED(정상) 상태의 알림 수신 여부 - 활성화: 진행 중 → 정상 상태로 전환되면 RECOVERED 알림을 보내고, 이벤트 기록에서 진행 중/해소 상태를 구분해 볼 수 있음 - 비활성화: 임계값을 초과할 때마다 단발성 이벤트 발생
이벤트 수신	해당 이벤트 알림을 받을 사용자 또는 그룹(수신 태그)

이벤트 설정

메트릭스 이벤트는 모니터링 대상에서 발생하는 이벤트를 조건에 따라 정의하고, 효율적으로 알림을 받을 수 있도록 설정할 수 있는 기능을 제공합니다.

이벤트 추가

메트릭스 이벤트를 추가하려면 **이벤트 설정 > 메트릭스** 탭으로 이동한 후, 오른쪽 상단의 [+ 이벤트 추가] 버튼을 클릭하세요.

메트릭스 이벤트 추가 방법
Step 1. 템플릿 선택: 이벤트의 기본 구조를 선택합니다.
Step 2. 이벤트 조건 정의: 이벤트를 어떤 기준으로 발생시킬지 조건을 설정합니다.

메트릭스 이벤트 추가 방법

Step 3. 이벤트 대상 선택: 이벤트가 발생하는 모니터링 대상을 선택합니다.

Step 4. 기본 정보 및 수신 설정: 이벤트 이름 및 메시지, 수신 대상을 설정합니다.

템플릿 선택

1. 이벤트를 어떻게 구성할지에 따라 화면 왼쪽의 3가지 템플릿 중 하나를 선택하세요.

- **새로 만들기:** 카테고리 and 지표를 처음부터 자유롭게 구성할 수 있으며, 복잡한 조건이나 세밀한 모니터링 규칙이 필요한 고급 사용자에게 적합
- **빠른 설정:** 사전 정의된 카테고리, 지표, 기본 임계치가 제공되며, 임계값만 조정하여 빠르게 적용할 수 있어 초급 사용자에게 적합
- **고급 설정:** 사전 정의된 카테고리 and 지표를 기반으로 조건을 추가하거나 자유롭게 변경

① 메트릭스 이벤트에서는 다양한 설정 방식을 지원합니다. 모니터링 플랫폼에 따라 제공하는 템플릿은 다를 수 있습니다.

이벤트 조건 정의

이벤트 조건 정의 단계에서 이벤트가 언제 발생할지 결정하는 지표 설정, 발생 횟수, 일시 중지, 해소된 알림, 이벤트 동작 시간을 설정합니다.

지표 설정

1. 검색창에서 카테고리를 입력하거나, 카테고리 목록에서 카테고리(지표)를 선택하세요.

카테고리를 선택해야 이후 지표 설정을 진행할 수 있습니다.

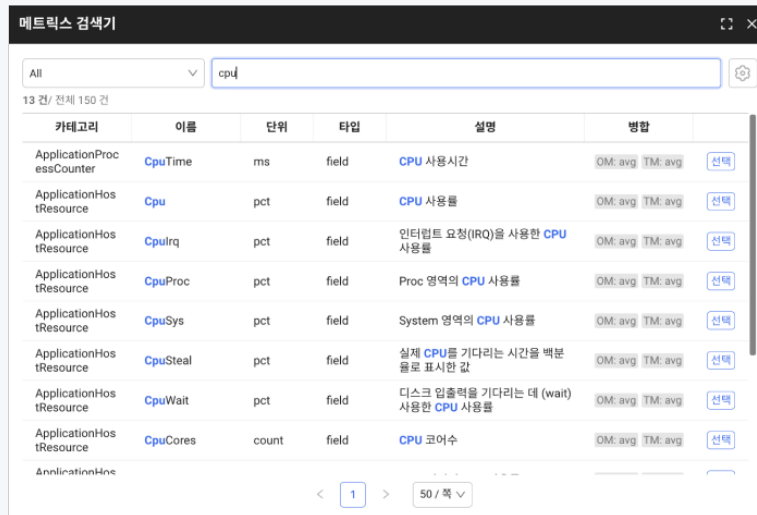
- 카테고리 목록은 카테고리 이름, 데이터 수집 주기, 키를 확인할 수 있습니다. 최근 3시간 동안 프로젝트에서 수집된 메트릭스 데이터가 표시됩니다.

2. 목록에 없는 지표를 사용하려면 **직접 입력하기**를 선택하여 카테고리를 직접 입력하세요.

❗ 카테고리나 지표를 모르는 경우 메트릭스 검색기를 활용하세요.

처음 지표를 설정하는 경우 메트릭스 검색기를 활용하면 더 빠르게 지표를 찾을 수 있습니다.

- 메트릭스 검색기에서 원하는 지표를 검색하면 관련 카테고리나 상세 정보를 확인할 수 있습니다.
- 검색 결과에서 필요한 메트릭스의 [선택] 버튼을 클릭하면, 선택한 값이 이벤트 설정 화면에 자동 반영됩니다.



3. 이벤트 레벨(Critical, Warning, Info)을 선택하세요. 하나의 지표에 여러 레벨을 설정할 수 있습니다.

❗ 이벤트 레벨 동작

여러 조건을 만족하더라도 가장 높은 우선 순위(Critical → Warning → Info)의 레벨만 이벤트가 발생합니다. 레벨 동작 방식은 [레벨 동작 가이드](#)를 참고하세요.

- 이벤트 레벨 수준은 위험(Critical)과 경고(Warning), 정상(Info)으로 구분합니다.
- 같은 지표로 레벨을 설정하고 단계별 임계치를 설정하는 것을 권장합니다.

4. 선택한 이벤트 레벨의 필드, 연산자, 값을 입력하세요.

a. + 추가를 클릭해 조건을 추가할 수 있습니다.

- && : 모든 조건을 동시에 만족해야 이벤트 발생

- **|||** : 하나 이상의 조건만 만족하면 이벤트 발생

b. — 를 클릭하면 해당 조건이 삭제됩니다.

❗ 조건식 작성 방법과 지원되는 연산자는 [조건 설정 가이드](#)를 참고하세요.

발생 횟수

조건이 몇 번 충족되었을 때 이벤트를 발생시킬지 설정합니다. 지속적인 문제만 감지하고 싶을 때 유용합니다.

1. 발생 빈도를 선택하세요.

- **연속**: 설정한 횟수만큼 이벤트가 연속으로 발생하는 경우 이벤트 발생
- **최근**: 선택한 시간 내에 설정한 횟수만큼 이벤트가 발생하는 경우 이벤트 발생
 - 선택 가능 시간: 5초, 10초, 15초, 30초, 1분, 2분, 3분, 4분, 5분, 10분, 30분, 1시간

2. 발생 횟수를 입력하세요.

- **Interval** 값은 선택한 카테고리의 데이터 수집 간격입니다. (Interval: 10s)

일시 중지

과도한 이벤트 발생을 방지하기 위해, 이벤트 동작을 일시 중지할 시간을 선택하세요. 이벤트 발생 후 설정한 시간 동안 동일한 이벤트가 발생하지 않습니다.

- 선택 가능 시간: 사용 안 함, 5분, 10분, 15분, 20분, 30분, 1시간, 2시간, 3시간, 6시간, 12시간, 1일

❗ 해소된 알림 활성화 시

알림은 정상 상태 알림(RECOVERED)을 받은 시점을 기준으로 설정한 시간이 지나기 전까지 동일한 이벤트가 발생해도 알림이 발생하지 않습니다.

해소된 알림

해소된 알림 기능을 활성화하면, 이벤트 발생 이후 상태 변화(진행 중 → 해소됨)를 추적할 수 있습니다. **이벤트 기록** 메뉴에서 진행

중인 이벤트로 표시됩니다.

- 해소된 알림은 **Critical**과 **Warning** 레벨에만 적용되며, Info 레벨은 항상 단발성 이벤트로 동작합니다.
- **Critical**과 **Warning** 레벨의 이벤트가 해소되면, 정상(RECOVERED) 상태의 알림이 전송됩니다.
- 토크 버튼을 클릭해 **활성화** 또는 **비활성화**하세요.
 -  **활성화**: 이벤트는 상태 기반으로 동작하며, 임계치 초과 시 진행 중, 임계치 이하로 복구 시 해소 상태로 전환됨
 -  **비활성화**: 임계값을 초과할 때마다 단발성 이벤트 발생

이벤트 동작 시간

이벤트가 특정 시간대(근무/비근무/점검 시간 등)에 동작하도록 태그를 설정하세요. 태그를 설정하지 않으면 이벤트가 활성화된 상태에서 24시간 상시 동작합니다.

1. **+ 추가**를 클릭하세요.
2. 이벤트 동작 시간에서 **+새로운 태그 생성**을 클릭하세요.
3. **이벤트 동작 시간 태그 생성**에서 **태그 이름**, **요일**, **시간**, **색상**을 선택하고 [적용] 버튼을 클릭하세요.
4. 생성한 태그는 태그 목록에서 확인할 수 있으며, 체크 박스를 선택하면 적용됩니다.
5. 수정 또는 삭제할 태그의  아이콘을 클릭해 **이벤트 동작 시간 태그 수정**에서 태그를 수정하거나 태그 삭제할 수 있습니다.

 태그 삭제 시 해당 태그가 적용된 모든 사용자의 태그가 삭제됩니다. 단, 이벤트 규칙에서 사용 중인 태그는 삭제할 수 없습니다.

시뮬레이션

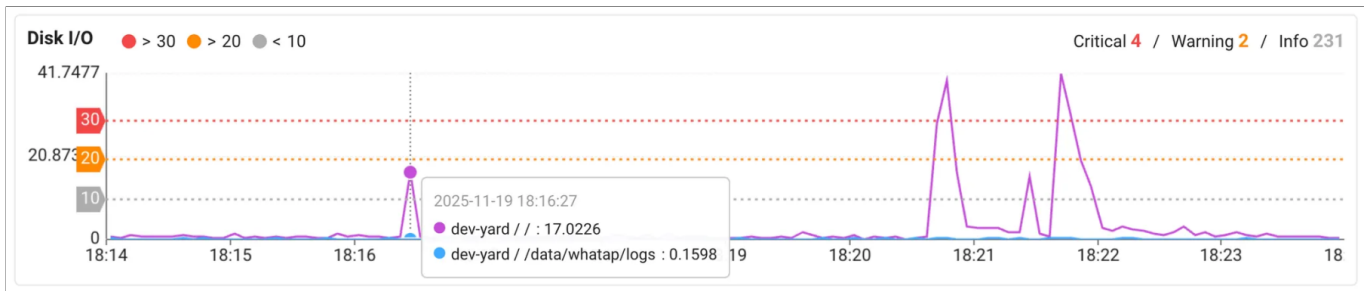
시뮬레이션 기능은 설정한 이벤트 조건을 과거 데이터에 기반으로 사전 테스트 할 수 있습니다. 예상 이벤트 수가 지나치게 많거나 부족하다면 조건을 조정해 최적의 임계값을 찾을 수 있습니다.

- **규칙 검증**: 새로운 이벤트 규칙을 만들었을 때, 과거 데이터에 적용하면 어떤 결과가 나오는지 확인 가능
- **임계값 튜닝**: 이벤트가 자주 발생하거나 전혀 발생하지 않을 때 적절한 수준으로 임계값 조정

시뮬레이션 시작하기

1. 이벤트 조건 설정이 완료되면 [시뮬레이션] 버튼을 클릭하세요.
2. 예상 이벤트 건수와 시각화된 결과를 확인합니다.

시뮬레이션 결과 이해하기



1. 시계열 데이터

지표의 시간대별 변화와 각 레벨의 임계선이 그래프로 표시되어 이벤트 발생 시점을 직관적으로 확인할 수 있습니다.

2. 레벨별 발생 현황

화면 우측에 Critical, Warning, Info 레벨의 이벤트 발생 횟수가 표시됩니다. 전체 이벤트 분포와 빈도를 파악할 수 있습니다.

3. 대상별 상세 정보

차트의 특정 지점에 마우스를 올리면 해당 시점의 정확한 지표 값과 모니터링 대상이 표시됩니다. 여러 대상이 있는 경우 색상으로 구분되며, 대상별 패턴이 다른 경우 필터링 기능을 사용해 개별적으로 분석할 수 있습니다.

4. 피크 구간 식별

그래프에서 지표가 급격히 상승하는 시간을 확인하여 문제가 자주 발생하는 시간대나 패턴을 파악할 수 있습니다.

✓ 시뮬레이션 활용 팁

• 다양한 시간대 시뮬레이션

평일/주말, 피크/비피크 시간대를 각각 시뮬레이션하여 시간대별 최적 임계값을 설정하세요.

• 실제 장애 기간 포함

과거 장애가 발생했던 기간을 포함하여 시뮬레이션을 실행하면 현재 규칙이 장애를 정확히 감지하는지 확인하세요.

• 대상 필터링 추가



모니터링 대상이 많으면 시뮬레이션 결과가 복잡해집니다. 필터링 기능으로 특정 대상만 선택하여 명확한 결과를 확인할 수 있습니다.

- **임계값 단계적 조정**

임계값을 한 번에 크게 변경하기보다 10% 단위로 점진적으로 조정하면서 최적값을 탐색하는 것이 좋습니다.

이벤트 대상 선택

이벤트 대상을 지정하지 않으면, 프로젝트에 포함된 전체 대상으로 이벤트가 발생되어 많은 이벤트가 발생할 수 있습니다. 따라서 이벤트가 적용될 대상을 명확히 설정하는 것을 권장합니다.



이벤트 대상을 변경한 경우, 이벤트 건수가 달라질 수 있습니다. **시뮬레이션** 버튼을 클릭한 후, 다시 실행해 예상 이벤트 수를 확인하세요.

대상 선택

이벤트가 적용될 대상을 **선택 입력** 또는 **직접 입력** 방식으로 지정할 수 있습니다.

- **선택 입력** 직접 입력

1. 태그, 연산자, 값을 선택 또는 입력하세요. a. 태그를 찾기 어렵다면, **메트릭스 검색기**에서 태그를 검색할 수 있습니다.
2. **+ 추가**를 클릭해 조건(**&&** , **||**)으로 이벤트 대상을 추가하세요.

모니터링할 대상의 태그, 연산자, 값을 직접 입력하세요.

- 직접 입력을 선택하면 입력란 아래에 사용 가능한 태그 목록(**태그 선택 입력**)이 함께 제공됩니다.

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



입력 방법을 변경하면, 작성한 내용이 초기화됩니다.

대상 선택 연산자 목록

선택 입력 방식에서 문자열 태그를 선택하면 연산자 목록에 다음 두 항목이 함께 표시됩니다. 목록에 나타나는 이름은 함수 표기 그대로이며, `startsWith(key, 'match_text')` 와 같은 기존 항목과 형태가 같습니다.

- `equalsIgnoreCase(key, 'match_text')`
- `notEqualsIgnoreCase(key, 'match_text')`

두 연산자는 대소문자를 구분하지 않고 값을 비교합니다. **직접 입력** 방식에서는 같은 함수를 조건식에 직접 작성해 사용할 수 있습니다. 조건식 문법과 지원되는 함수 전체 목록은 [조건 설정 가이드](#)를 참고하세요.

❗ 이벤트 발생 조건과 이벤트 대상 선택은 같은 문법을 사용하므로 두 함수를 양쪽 조건식에 모두 작성할 수 있습니다.

기본 정보 및 수신 설정

이벤트의 이름, 메시지, 수신 대상을 설정합니다. 설정한 내용은 이벤트 기록과 실제 알림 메시지에 그대로 표시되므로, 식별하기 쉽고 명확하게 작성하는 것이 중요합니다.

이벤트 활성화

설정된 조건을 충족했을 때 이벤트 발생 여부를 설정합니다.

- ☒ **활성화**: 설정한 조건을 충족하면 이벤트가 발생됨
- ☐ **비활성화**: 조건을 검사하지 않음

이벤트 이름

이벤트 제목으로 사용될 이벤트 이름을 입력하세요. 설정한 이벤트 이름은 **이벤트 목록** 및 **이벤트 기록** 메뉴에 표시되며, 해당 이름으로 검색할 수 있습니다.

메시지

이벤트 메시지를 입력하세요. 입력한 메시지는 이벤트 기록 및 알림에 사용됩니다. ⓘ을 클릭하면 이전에 작성한 메시지 기록을 확인할 수 있습니다. 메시지에 변수를 사용하여 이벤트 발생 시점의 실제 값을 포함할 수 있습니다.

- **변수 사용 규칙**
 - 변수 형식: `${지표명}`

- 설정한 **카테고리**와 **동일한 카테고리** 내 지표만 변수로 사용할 수 있습니다.
- 여러 변수를 조합해 상세한 메시지를 구성할 수 있습니다.
- 사용 가능한 변수 목록은 **메트릭스 조회** 메뉴에서 확인할 수 있습니다.

• 변수 활용 예시

	이벤트 설정	이벤트 발생 시
제목	Disk 사용량 증가	Disk 사용량 증가
메시지	Disk = \${disk}%	Disk = 89.9%

이벤트 수신

이벤트 알림을 받을 멤버를 지정합니다.

• 전체 수신 태그 선택 수신

프로젝트에서 이벤트 수신 설정이 활성화된 모든 대상(멤버, 채널)에게 알림을 전송합니다.

해당 태그를 가진 프로젝트 멤버에게 알림을 전송합니다.

1. 태그 선택 수신을 선택하세요.
2. 수신 태그 항목에서 [+ 태그 추가] 또는 [+] 버튼을 클릭하세요.
3. 이벤트 수신 태그 창 아래의 + 새 태그 생성을 클릭하세요.
4. 태그 생성 창에서 태그 이름을 입력하고, 색상을 선택한 후, [태그 생성] 버튼을 클릭해 태그를 생성하세요.
5. 생성된 태그는 태그 목록의  아이콘을 클릭해 수정 또는 삭제하세요.
6. 이벤트 수신 태그 창에서 태그 목록에서 원하는 태그를 선택하면 적용됩니다.

❗ 수신 태그

수신자 태그는 알림을 받을 사용자 또는 채널을 **그룹 단위로 관리하기 위한 기능**입니다. 이벤트에 수신자 태그를 설정하면, 해당 태그가 포함된 사용자에게만 알림이 전달됩니다. 수신 태그를 설정하지 않으면 프로젝트 내 모든 사용자에게 알림이 전송됩니다.

이벤트 수정/삭제

1. 경고 알림 > 이벤트 설정의 메트릭스 탭으로 이동하세요.
2. 이벤트 목록에서 수정 또는 삭제하려는 이벤트의  아이콘을 클릭하세요.
3. 이벤트 규칙 수정 창에서 옵션을 수정하고, [저장] 버튼을 클릭하세요.
 - a. 선택한 이벤트를 삭제하려면 이벤트 규칙 수정 창의 오른쪽 위의 [삭제] 버튼을 클릭하세요.

이벤트 공유

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

- JSON 파일명: event-rules-YYYYMMDD.json

내보내기

1. 화면 오른쪽 위에 [JSON ] 버튼을 클릭하세요.
2. JSON 편집 창이 나타나면 [ 내보내기] 버튼을 클릭하세요.
 - 이벤트를 검색 후 내보내기 기능을 이용하면 검색한 목록만 JSON 파일로 다운받을 수 있습니다.
3. JSON 파일이 다운로드되면 공유할 다른 사용자에게 전달하세요.

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.

 같은 종류의 제품 간에 이용할 것을 권장합니다. 다른 제품의 프로젝트로부터 이벤트 설정을 가져올 수는 있지만 정상 작동하지 않습니다.

Json 형식으로 수정하기

1. 화면 오른쪽 위에 [JSON ] 버튼을 클릭하세요.
2. 편집 창이 나타나면 JSON 형식에 맞춰 내용을 수정하세요.
3. 수정을 완료하면 화면 아래 [저장] 버튼을 선택하세요.

❗ 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 데이터 구조

```
{
  "version": 2,
  "eventId": "zcef7s7f27rum1",
  "enabled": true,
  "stateful": false,
  "title": "Active Transaction",
  "message": "Active Transaction = ${active_tx_count}",
  "category": "app_counter",
  "alertLabel": [
    "oid"
  ],
  "repeatCount": 1,
  "repeatDuration": 0,
  "silent": 300000,
  "receiver": [],
  "timeTag": [],
  "selectString": "",
  "conditions": [
    {
      "level": 20,
      "enabled": true,
      "rule": "active_tx_count > 100"
    }
  ]
}
```

```

    }
  ],
  "createTime": 1763632674345,
  "lastModifiedTime": 1763632674347,
  "lastModifiedUser": "support@whatap.io",
  "basic": true,
  "metaId": "java004",
  "selectCondition": {
    "oid": [
      "-1010758404",
      "-250906941"
    ]
  }
}

```

표 | JSON 데이터 구조

JSON 필드	타입	설명	비고
version	Integer	이벤트 규칙의 버전	변경 제한
eventId	String	이벤트 규칙의 고유 식별자	
enabled	boolean	이벤트 활성화 여부	
stateful	boolean	상태 기반 이벤트 여부	
title	String	사용자가 설정한 이벤트 규칙 이름	
message	String	사용자가 설정한 이벤트 규칙 메시지	
category	String	데이터 카테고리	
alertLabel	List<String>	이벤트의 상태 관리를 위해 카테고리마다 지정되는 기본 식별자(primary key) 값	변경 제한
repeatCount	Integer	반복 횟수	
repeatDuration	Long	반복 기간	

JSON 필드	타입	설명	비고
silent	Integer	일시 중지 시간	
receiver	List<String>	수신자 태그의 키값 목록	
timeTag	List<String>	동작시간 태그의 키값 목록	
selectString	String	대상 선택	
conditions	List<Object>	레벨별 발생 조건 목록	
└ level	byte	레벨 값	Critical : 30 Warning : 20 Info : 10
└ enabled	boolean	레벨 활성화 여부	
└ rule	String	레벨 발생 조건	
createTime	Long	이벤트 규칙 최초 생성 시간	
lastModifiedTime	Long	이벤트 규칙 마지막 수정 시간	
lastModifiedUser	String	이벤트 규칙 마지막 수정 계정	
basic	boolean	빠른 설정으로 생성한 이벤트 여부	변경 제한
metaId	String	빠른 설정 템플릿 고유 식별자	변경 제한: 이 값은 빠른 설정으로 생성한 이벤트에만 존재합니다. (basic=true)
selectCondition	Object	빠른 설정 대상 선택값	이 값은 빠른 설정으로 생성한 이벤트에만 존재합니다. (basic=true)

❗ '변경 제한'으로 표시된 필드는 이벤트 동작에 영향을 줄 수 있으므로 값을 변경하지 않는 것을 권장합니다.

부록

발생 조건, 대상 선택 가이드

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

레벨 동작 가이드

이벤트 레벨은 위험(Critical)과 경고(Warning), 정상(Info)으로 구분합니다.

1. 우선순위 기반 이벤트 발생

여러 레벨의 조건을 동시에 충족할 경우, 가장 높은 우선순위의 이벤트만 발생합니다.

예시

설정:

- Warning: CPU > 70%

- Critical: CPU > 90%

현재 상태: CPU 95%

→ 결과: Critical 이벤트만 발생 (Warning은 억제됨)

2. 레벨 상승

진행중 상태를 갖는 이벤트에서 낮은 레벨 이벤트가 진행 중일 때 높은 레벨 조건을 충족하면, 두 레벨 모두 진행 중 상태가 됩니다.

예시

설정:

- Warning: CPU > 70%

- Critical: CPU > 90%

시나리오:

1) CPU 80% → Warning 발생 (진행 중)

2) CPU 95% → Warning (진행 중), Critical (진행 중)

3. 레벨 하강

진행중 상태를 갖는 이벤트에서 높은 레벨에서 낮은 레벨로 전환되면 높은 레벨은 해소되고 낮은 레벨이 유지됩니다.

예시

설정:

- Warning: CPU > 70%

- Critical: CPU > 90%

시나리오:

1) CPU 97% → Critical 발생

2) CPU 85% → Critical 해소, Warning 유지

3) CPU 65% → Warning 해소

4. 동작 흐름도

- Warning: CPU > 70%

- Critical: CPU > 90%

메트릭 값: 60% → 75% → 92% → 85% → 60%

상태:	정상	Warning (발생)	Critical (발생)	Warning (유지)	정상 (해소)
			Warning (유지)		

ⓘ 진행 중 상태를 갖는 이벤트는 조건이 충족되는 동안 계속 활성화 상태를 유지하며, 조건이 해제될 때까지 지속됩니다.

조건 설정 가이드

ⓘ 지표명이 숫자로 시작하거나 특수문자가 포함된 경우 \${지표명} 형태로 작성해야 합니다.

- 괄호 (), []



- 연산자 `+`, `-`, `*`, `/`, `%`
- 구분자 `:`, `@`, `#`, `,`, `,` (공백)
- 기타 특수문자 `!`, `^`, `&`, `|`, `~`, ```, `=`

`${}` 사용 예시:

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

`${}` 없이 사용 가능: 영문자, 언더스코어(`_`), 점(`.`)만 포함된 경우

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

1. 비교 연산자

숫자 비교

```
크다:      cpu > 80
크거나 같다:  cpu >= 80
작다:      memory < 1000
작거나 같다:  memory <= 1000
같다:      status == 200
같지 않다:   error != 0
```

문자열 비교

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

2. 산술 연산자

- 기본 산술 연산

```
덧셈:  cpu + 10 >= 90
뺄셈:  memory - 100 >= 500
곱셈:  cpu * 2 >= 100
나눗셈: disk / 1024 >= 100
나머지: value % 10 == 0
```

- 괄호를 이용한 우선순위 제어

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

- 음수 표현

```
cpu > -100
```

3. 논리 연산자

- AND 연산 (&&)

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

- OR 연산 (||)

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

- 복합 논리 연산

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

4. 패턴 매칭 연산자

- LIKE 연산자

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

- NOT LIKE 연산자

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

5. 내장 함수

- Null 체크 함수

```
isNull(value)      # null인지 확인
isNotNull(value)   # null이 아닌지 확인
nvl(value, 0)      # null이면 기본값 반환
isEmpty(str)       # 빈 문자열인지 확인
isNotEmpty(str)    # 빈 문자열이 아닌지 확인
```

- 집계 함수

```
sum(cpu, memory, disk)    # 합계
avg(cpu, memory)          # 평균
max(cpu, memory, disk)    # 최대값
min(cpu, memory, disk)    # 최소값
count(value1, value2, value3) # 개수
```

- 수학 함수

```
round(cpu, 2)            # 반올림 (소수점 2자리)
```

- 문자열 함수

```
length(str)             # 문자열 길이
startsWith(str, 'prefix') # 접두사 확인
```

```
endsWith(str, 'suffix') # 접미사 확인
indexOf(str, 'search') # 문자열 위치
substring(str, 0, 10) # 부분 문자열
trim(str) # 공백 제거
replace(str, 'old', 'new') # 문자열 치환
hasStr(str, 'search') # 문자열 포함 여부
```

문자열 함수

```
equalsIgnoreCase(str, 'match_text') # 대소문자를 구분하지 않는 일치 비교
notEqualsIgnoreCase(str, 'match_text') # 대소문자를 구분하지 않는 불일치 비교
```

`==` 와 `!=` 는 대소문자를 구분하므로 `WebServer` 와 `webserver` 를 다른 값으로 판단합니다. 표기가 일정하지 않은 태그나 필드를 비교할 때 위 두 함수를 사용하면 대소문자 차이를 무시하고 값을 맞출 수 있습니다.

예시

```
equalsIgnoreCase(ocindName, 'WebServer')
notEqualsIgnoreCase(container, 'PROD.billing')
```

이벤트 발생 조건과 이벤트 대상 선택은 같은 문법을 사용하므로 두 함수를 양쪽 조건식에 모두 작성할 수 있습니다.

- 조건 함수

- **if:** 조건식이 참(`true`)이면 `true값` 을 반환하고, 거짓(`false`)이면 `false값` 을 반환하는 조건 함수

형식

```
if(조건, true값, false값)
```

예시

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

- **decode:** 값과 조건을 비교하여 일치하는 조건의 결과를 반환, 없으면 기본값 반환

형식

```
decode(값, 조건1, 결과1, 조건2, 결과2, ..., 조건N, 결과N, 기본값)
```

예시

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

- **in:** 값이 지정한 후보값 중 하나와 일치하면 `true`, 아니면 `false`

형식

```
in(값, 후보값1, 후보값2, ..., 후보값N)
```

예시

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

❗ 작성 시 주의사항

- 권장사항
 - 간단한 변수명은 `${}` 없이 사용 (예: `cpu`, `memory`)
 - 특수문자 포함 시 반드시 `${}` 사용
 - 복잡한 연산은 괄호로 명확하게 구분
 - 함수명은 정확히 입력 (대소문자 구분)
- 피해야 할 사항
 - 불완전한 표현식 작성 (예: `cpu >`, `memory &&`)
 - 괄호 미스매칭 (예: `(cpu > 80 && cpu > 70)`)
 - 연속된 연산자 사용 (예: `cpu >> 80`, `cpu >< 80`)

실시간 로그 이벤트

홈 > 프로젝트 선택 >  경고 알림 > 이벤트 설정 > 실시간 로그 탭

수집한 로그 데이터를 조건에 맞춰 필터링하려 경고 알림을 설정할 수 있습니다. 로그 이벤트를 사용하려면 로그 모니터링이 활성화되어야 합니다. **로그 모니터링 활성화**에 대한 자세한 내용은 각 제품 로그 문서를 참고하세요.

- **실시간 로그 이벤트:** 실시간으로 수집한 로그에서 설정한 이벤트 조건이 충족되면 이벤트가 발생합니다.

기본 옵션

- **검색:** 이벤트 이름 또는 이벤트 수신 태그를 선택해 원하는 이벤트 검색
- **JSON 다운로드/업로드:** 이벤트 규칙은 JSON 편집기를 통해 바로 수정하거나, 파일로 다운로드하여 수정 후 다시 업로드 가능
- **알림 메시지 설정:** 수신할 메시지의 상세 항목 선택 및 항목 별 내용 편집
- **+ 이벤트 추가:** 새로운 로그 이벤트 추가

표 | 실시간 로그 이벤트 목록 구성

항목	설명
이벤트 이름	알림 제목으로 사용되는 이벤트 이름 - 최대 255byte까지 입력 가능
카테고리	로그 구분 명칭(로그 폴더명)
검색 키	로그 데이터에서 찾고 싶은 항목 - 예: HTTP 응답 상태 코드를 나타내는 값에 접근하고자 할 경우 검색 키 <code>status</code>
검색 값	검색 키에 해당하는 실제 데이터로 로그에서 입력한 단어를 포함할 경우 경고 알림을 보냄 - 예: 검색 키 <code>status</code> 검색 값 <code>200</code> 을 설정한 경우 HTTP 응답 상태 코드 200을 포함하는 로그 데이터 수집 시 경고 알림 발생
이벤트 발생 일시 중지	이벤트 알림 발생 후, 같은 이벤트 발생을 일정 시간 동안 멈춤 - 선택 가능 시간: 사용 안 함, 5분, 10분, 15분, 20분, 30분, 1시간, 2시간, 3시간, 6시간, 12시간, 1일 - 해소된 알림이 활성화된 경우, 정상(RECOVERED) 상태 알림을 받은 후 선택한 시간 동안 같은 이벤트가

항목	설명
	발생해도 알림이 발생하지 않음
이벤트 대상 필터링	이벤트가 적용될 대상의 조건 - 대상 조건을 설정하지 않으면 수집되는 모든 데이터에 대해 알림 여부 판단 - 선택 입력: 태그, 연산자, 값을 선택해 조건 구성 - 직접 입력: 조건을 직접 입력해 대상 지정
이벤트 수신 태그	해당 이벤트 알림을 받을 사용자 또는 그룹(수신 태그)
	이벤트 수정 및 삭제
	이벤트의 활성화 여부 - 활성화: 조건을 충족하면 이벤트 발생 - 비활성화: 이벤트가 동작하지 않으며, 조건을 검사하지 않음

이벤트 설정

로그 이벤트는 실시간 로그 또는 일정 조건을 만족하는 로그가 누적될 때 경고 알림을 설정할 수 있는 기능입니다.

실시간 로그 이벤트 추가

1. 경고 알림 > 이벤트 설정의 실시간 로그 탭을 클릭하세요.
2. 화면 오른쪽의 [+ 이벤트 추가] 버튼을 클릭하세요.
3. 이벤트 규칙 추가 창에서 로그 이벤트 조건을 설정하세요.
 - **이벤트 이름:** 이벤트 제목으로 사용할 이름을 입력하세요.
 - **이벤트 활성화:** 토글 버튼 활성화 시, 토글 버튼 활성화 시, 조건을 충족하면 이벤트 발생합니다.
 - **레벨:** 이벤트 레벨(Critical, Warning, Info)을 선택하세요.
 - **메시지:** 이벤트 발생 시 전달받을 알림 메시지를 입력하세요. 메시지에 변수를 사용하여 이벤트 발생 시점의 실제 값을 포함할 수 있습니다.

✓ 변수 사용 규칙

- 변수 형식: \${지표명}
- 설정한 **카테고리**와 **동일한 카테고리** 내 지표만 변수로 사용할 수 있습니다.
- 여러 변수를 조합해 상세한 메시지를 구성할 수 있습니다.
- 사용 가능한 변수 목록은 **메트릭스 조회**에서 확인할 수 있습니다.

- **카테고리**: 로그 구분 명칭(로그 폴더명)을 목록에서 선택하거나 직접 입력하세요. 카테고리를 선택해야 검색 키와 검색 값을 입력할 수 있습니다.
- **검색 키**: 로그 데이터에서 찾고 싶은 항목을 입력하세요.
 - 예: HTTP 응답 상태 코드를 나타내는 값에 접근하고자 할 경우 **검색 키** status
- **검색 값**: 검색 키에 해당하는 실제 데이터를 입력하세요. 로그에서 입력한 단어를 포함할 경우 경고 알리를 보냅니다.
 - 예: **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**: 이벤트가 적용될 대상의 조건을 입력하세요. 입력값이 없으면, 수집되는 모든 데이터에 대해 알림 여부 판단합니다.
 - **선택 입력**: 태그, 연산자, 값을 선택해 대상 조건을 설정하세요.

❗ 조건식 작성 방법과 지원되는 연산자는 [조건 설정 가이드](#)를 참고하세요.

- **직접 입력**: 조건을 직접 입력하세요.
- **이벤트 발생 일시 중지**: 알리를 일시 중지할 시간을 선택하세요. 이벤트 발생 후 설정한 시간 동안 동일한 이벤트가 발생하지 않습니다.
 - 선택 가능 시간: 사용 안 함 , 1분 , 2분 , 3분 , 5분 , 10분 , 20분 , 30분 , 1시간 , 3시간 , 6시간 , 12시간
- **이벤트 동작 시간**: 이벤트가 특정 시간대(근무/비근무/점검 시간 등)에 동작하도록 태그를 설정하세요. 태그를 설정하지 않으면 이벤트가 활성화된 상태에서 24시간 상시 동작합니다.

1. + 추가를 클릭하세요.
2. 이벤트 동작 시간에서 +새로운 태그 생성을 클릭하세요.
3. 이벤트 동작 시간 태그 생성에서 태그 이름, 요일, 시간, 색상을 선택하고 [적용] 버튼을 클릭하세요.
4. 생성한 태그는 태그 목록에서 확인할 수 있으며, 체크 박스를 선택하면 적용됩니다.
5. 수정 또는 삭제할 태그의  아이콘을 클릭해 이벤트 동작 시간 태그 수정에서 태그를 수정하거나 태그 삭제할 수 있습니다.

 태그 삭제 시 해당 태그가 적용된 모든 사용자의 태그가 제거됩니다. 단, 이벤트 규칙에서 사용 중인 태그는 삭제할 수 없습니다.

- 이벤트 수신 태그: 이벤트에 수신 태그를 설정하면, 해당 태그를 가진 프로젝트 멤버에게 알림을 전송합니다. 수신자 태그를 설정하지 않으면 프로젝트 내 모든 사용자에게 알림이 전송됩니다.

1. + 태그 추가 또는 +를 클릭하세요.
2. 이벤트 수신 태그 창 아래의 + 새 태그 생성을 클릭하세요.
3. 태그 생성 창에서 태그 이름을 입력하고, 색상을 선택한 후, [태그 생성] 버튼을 클릭해 태그를 생성하세요.
4. 생성된 태그는 태그 목록의  아이콘을 클릭해 수정 또는 삭제하세요.
5. 이벤트 수신 태그 창의 태그 목록에서 원하는 태그를 선택하면 적용됩니다.

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

4. 이벤트 규칙 추가 창에서 설정이 완료되면 [저장] 버튼을 클릭하세요.

이벤트 수정/삭제

1. 경고 알림 > 이벤트 설정의 실시간 로그 탭으로 이동하세요.

2. 로그 이벤트 목록에서 수정 또는 삭제하려는 이벤트의  아이콘을 클릭하세요.
3. **이벤트 설정** 화면에서 옵션을 수정하고, [저장] 버튼을 클릭하세요.
 - a. 선택한 이벤트를 삭제하려면 **이벤트 설정** 화면의 오른쪽 위의 [삭제] 버튼을 클릭하세요.

이벤트 공유

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

- JSON 파일명: **event-rules-**YYYYMMDD **.json**

내보내기

1. 화면 오른쪽 위에 [JSON ] 버튼을 클릭하세요.
2. JSON 편집 창이 나타나면 [ 내보내기] 버튼을 클릭하세요.
 - 이벤트를 검색 후 내보내기 기능을 이용하면 검색한 목록만 JSON 파일로 다운받을 수 있습니다.
3. JSON 파일이 다운로드되면 공유할 다른 사용자에게 전달하세요.

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.

 같은 종류의 제품 간에 이용할 것을 권장합니다. 다른 제품의 프로젝트로부터 이벤트 설정을 가져올 수는 있지만 정상 작동하지 않습니다.

Json 형식으로 수정하기

1. 화면 오른쪽 위에 [JSON ] 버튼을 클릭하세요.
2. 편집 창이 나타나면 JSON 형식에 맞춰 내용을 수정하세요.

- 수정을 완료하면 화면 아래 [저장] 버튼을 선택하세요.

❗ 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)

부록

발생 조건, 대상 선택 가이드

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

레벨 동작 가이드

이벤트 레벨은 위험(Critical)과 경고(Warning), 정상(Info)으로 구분합니다.

1. 우선순위 기반 이벤트 발생

여러 레벨의 조건을 동시에 충족할 경우, 가장 높은 우선순위의 이벤트만 발생합니다.

예시

설정:

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

현재 상태: CPU 95%

→ 결과: Critical 이벤트만 발생 (Warning은 억제됨)

2. 레벨 상승

진행중 상태를 갖는 이벤트에서 낮은 레벨 이벤트가 진행 중일 때 높은 레벨 조건을 충족하면, 두 레벨 모두 진행 중

상태가 됩니다.

예시

설정:

- Warning: CPU > 70%

- Critical: CPU > 90%

시나리오:

1) CPU 80% → Warning 발생 (진행 중)

2) CPU 95% → Warning (진행 중), Critical (진행 중)

3. 레벨 하강

진행중 상태를 갖는 이벤트에서 높은 레벨에서 낮은 레벨로 전환되면 높은 레벨은 해소되고 낮은 레벨이 유지됩니다.

예시

설정:

- Warning: CPU > 70%

- Critical: CPU > 90%

시나리오:

1) CPU 97% → Critical 발생

2) CPU 85% → Critical 해소, Warning 유지

3) CPU 65% → Warning 해소

4. 동작 흐름도

- Warning: CPU > 70%

- Critical: CPU > 90%

메트릭 값: 60% → 75% → 92% → 85% → 60%

상태: 정상 Warning Critical Warning 정상
 (발생) (발생) (유지) (해소)

Warning
(유지)

⚠ 진행 중 상태를 갖는 이벤트는 조건이 충족되는 동안 계속 활성화 상태를 유지하며, 조건이 해제될 때까지 지속됩니다.

조건 설정 가이드

⚠ 지표명이 숫자로 시작하거나 특수문자가 포함된 경우 `${지표명}` 형태로 작성해야 합니다.

- 괄호 (), []
- 연산자 +, -, *, /, %
- 구분자 :, @, #, ,, (공백)
- 기타 특수문자 !, ^, &, |, ~, ", =

`${}` 사용 예시:

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

`${}` 없이 사용 가능: 영문자, 언더스코어(_), 점(.)만 포함된 경우

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

1. 비교 연산자

숫자 비교

```
크다:      cpu > 80
크거나 같다:  cpu >= 80
작다:      memory < 1000
작거나 같다:  memory <= 1000
같다:      status == 200
```

```
같지 않다: error != 0
```

문자열 비교

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

2. 산술 연산자

- 기본 산술 연산

```
덧셈: cpu + 10 >= 90
뺄셈: memory - 100 >= 500
곱셈: cpu * 2 >= 100
나눗셈: disk / 1024 >= 100
나머지: value % 10 == 0
```

- 괄호를 이용한 우선순위 제어

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

- 음수 표현

```
cpu > -100
```

3. 논리 연산자

- AND 연산 (&&)

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

- OR 연산 (||)

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

- 복합 논리 연산

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

4. 패턴 매칭 연산자

- LIKE 연산자

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

- NOT LIKE 연산자

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

5. 내장 함수

- Null 체크 함수

isNull(value)	# null인지 확인
isNotNull(value)	# null이 아닌지 확인
nvl(value, 0)	# null이면 기본값 반환
isEmpty(str)	# 빈 문자열인지 확인
isNotEmpty(str)	# 빈 문자열이 아닌지 확인

- 집계 함수

sum(cpu, memory, disk)	# 합계
avg(cpu, memory)	# 평균
max(cpu, memory, disk)	# 최대값

```
min(cpu, memory, disk)      # 최소값
count(value1, value2, value3) # 개수
```

- 수학 함수

```
round(cpu, 2)      # 반올림 (소수점 2자리)
```

- 문자열 함수

```
length(str)      # 문자열 길이
startsWith(str, 'prefix') # 접두사 확인
endsWith(str, 'suffix') # 접미사 확인
indexOf(str, 'search') # 문자열 위치
substring(str, 0, 10) # 부분 문자열
trim(str)        # 공백 제거
replace(str, 'old', 'new') # 문자열 치환
hasStr(str, 'search') # 문자열 포함 여부
```

문자열 함수

```
equalsIgnoreCase(str, 'match_text') # 대소문자를 구분하지 않는 일치 비교
notEqualsIgnoreCase(str, 'match_text') # 대소문자를 구분하지 않는 불일치 비교
```

`==` 와 `!=` 는 대소문자를 구분하므로 `WebServer` 와 `webserver` 를 다른 값으로 판단합니다. 표기가 일정하지 않은 태그나 필드를 비교할 때 위 두 함수를 사용하면 대소문자 차이를 무시하고 값을 맞출 수 있습니다.

예시

```
equalsIgnoreCase(okindName, 'WebServer')
notEqualsIgnoreCase(container, 'PROD.billing')
```

이벤트 발생 조건과 이벤트 대상 선택은 같은 문법을 사용하므로 두 함수를 양쪽 조건식에 모두 작성할 수 있습니다.

- 조건 함수

- **if**: 조건식이 참(`true`)이면 `true값` 을 반환하고, 거짓(`false`)이면 `false값` 을 반환하는 조건 함수

형식

```
if(조건, true값, false값)
```

예시

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

- **decode:** 값과 조건을 비교하여 일치하는 조건의 결과를 반환, 없으면 기본값 반환

형식

```
decode(값, 조건1, 결과1, 조건2, 결과2, ..., 조건N, 결과N, 기본값)
```

예시

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

- **in:** 값이 지정한 후보값 중 하나와 일치하면 `true`, 아니면 `false`

형식

```
in(값, 후보값1, 후보값2, ..., 후보값N)
```

예시

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

❗ 작성 시 주의사항

- 권장사항
 - 간단한 변수명은 `${}` 없이 사용 (예: `cpu`, `memory`)
 - 특수문자 포함 시 반드시 `${}` 사용
 - 복잡한 연산은 괄호로 명확하게 구분
 - 함수명은 정확히 입력 (대소문자 구분)



- 피해야 할 사항
 - 불완전한 표현식 작성 (예: `cpu > , memory &&`)
 - 괄호 미스매칭 (예: `(cpu > 80 && cpu > 70)`)
 - 연속된 연산자 사용 (예: `cpu >> 80 , cpu >< 80`)

복합 로그 이벤트 설정

홈 > 프로젝트 선택 >  경고 알림 > 이벤트 설정 > 복합 로그 탭

수집한 로그 데이터를 조건에 맞춰 필터링하려 경고 알림을 설정할 수 있습니다. 로그 이벤트를 사용하려면 로그 모니터링이 활성화되어야 합니다. **로그 모니터링 활성화**에 대한 자세한 내용은 (각 제품 로그 문서 링크)를 참고하세요.

- **복합 로그 이벤트:** 설정한 데이터 조회 범위 내 로그를 기준으로, 로그 검색 조건을 충족하는 로그 수가 임계 개수 이상일 경우 이벤트가 발생합니다.

 권한

복합 메트릭스 이벤트를 설정하려면 **알림 설정 권한**이 필요합니다. 알림 설정 권한은 **홈 화면 > 프로젝트 선택 > 관리 > 통합 멤버 관리**에서 권한을 부여할 멤버의  아이콘을 클릭해 설정할 수 있습니다.

기본 옵션

- **검색:** 이벤트 이름 또는 이벤트 수신 태그를 선택해 원하는 이벤트 검색
- **JSON 다운로드/업로드:** 이벤트 규칙은 JSON 편집기를 통해 바로 수정하거나, 파일로 다운로드하여 수정 후 다시 업로드 가능
- **알림 메시지 설정:** 수신할 메시지의 상세 항목 선택 및 항목 별 내용 편집
- **+ 이벤트 추가:** 새로운 로그 이벤트 추가

표 | 복합 로그 이벤트 목록 구성

항목	설명
이벤트 이름	알림 제목으로 사용될 이벤트 이름
템플릿	복합 로그 템플릿
카테고리	로그 구분 명칭(로그 폴더명)
규칙	이벤트 발생하는 조건

항목	설명
이벤트 상태가 해소되면 추가 알림	Critical과 Warning 레벨의 이벤트가 해소되면 정상(RECOVERED) 상태의 알림 수신 여부 - 활성화: 진행 중 → 정상 상태로 전환될 때 RECOVERED 알림을 보내며, 이벤트 기록에서 진행 중/해소 상태를 구분해 볼 수 있음 - 비활성화: 임계값을 초과할 때 마다 단발성 이벤트 발생
이벤트 발생 일시 중지	이벤트 알림 발생 후, 같은 이벤트 발생을 일정 시간 동안 멈춤 - 선택 가능 시간: 사용 안 함, 5분, 10분, 15분, 20분, 30분, 1시간, 2시간, 3시간, 6시간, 12시간, 1일 - 해소된 알림이 활성화된 경우, 정상(RECOVERED) 상태 알림을 받은 후 선택한 시간 동안 같은 이벤트가 발생해도 알림이 발생하지 않음
인터벌	로그 데이터를 조회할 시간 범위
이벤트 수신 태그	해당 이벤트 알림을 받을 사용자 또는 그룹(수신 태그)
	이벤트 수정 및 삭제
	이벤트의 활성화 여부 - 활성화: 조건을 충족하면 이벤트 발생 - 비활성화: 이벤트가 동작하지 않으며, 조건을 검사하지 않음

이벤트 설정

복합 로그 이벤트는 설정한 데이터 조회 범위 내 로그를 기준으로, 로그 검색 조건을 충족하는 로그 수가 임계 개수 이상일 경우 경고 알림을 설정할 수 있는 기능입니다.

복합 로그 이벤트 추가

1. 경고 알림 > 이벤트 설정의 복합 로그 탭을 클릭하세요.
2. 화면 오른쪽의 [+ 이벤트 추가] 버튼을 클릭하세요.
3. 이벤트 규칙 추가 창에서 로그 이벤트 조건을 설정하세요. 자세한 내용은 [기본 설정](#), [상세 설정](#), [추가 설정](#)를 참고하세요.

이벤트 규칙 추가

*이벤트 이름

이벤트 이름

이벤트 활성화

레벨

위험

경고

정보

이벤트 상태가 해소되면 추가 알림

템플릿

사용 안 함

*메시지

메시지

*카테고리

카테고리(들) 선택해주세요

*필터

<>

Please enter Search Query Syntax

*이벤트 발행 조건

조건에 맞는 로그

>

10

그룹화 필드

선택 안 함 (전체 집계)

인터벌

5 분

무음

1 분

이벤트 동작 시간

+ 추가

이벤트 동작 시간 태그를 설정하면 해당 태그를 가진 알림은 해당 시간대에만 이벤트가 동작합니다. 이벤트 동작 시간 태그 설정에 대한 자세한 설명은 가이드 문서를 참고해 주세요. [가이드 문서](#) >

이벤트 수신 태그

전체 멤버 수신 + 태그 추가

프로젝트 이벤트 수신설정 메뉴 바로가기

< 2026/04/21 14:11 ~ 2026/04/21 15:11 1시간

시뮬레이션

조건 설정 후 시뮬레이션 버튼을 누르면
알림 예상 건수를 확인할 수 있습니다.

저장

4. 이벤트 규칙 추가 창에서 설정이 완료되면 [저장] 버튼을 클릭하세요.

기본 설정

- **이벤트 이름:** 이벤트 제목으로 사용할 이름을 입력하세요.
- **이벤트 활성화:** 토글 버튼 활성화 시, 조건을 충족하면 이벤트 발생합니다.
- **레벨:** 이벤트 레벨(Critical, Warning, Info)을 선택하세요.

상세 설정

템플릿(프리셋), 메시지, 카테고리, 필터, 이벤트 발생 조건 항목을 설정합니다.

템플릿(프리셋)

미리 정의된 프리셋을 선택하면 필터, 쿼리 타입, 이벤트 발행 조건이 자동으로 설정됩니다. 프리셋을 선택한 후 필요에 맞게 수정할 수 있습니다.

복합 로그 템플릿 유형

!

프리셋	쿼리 타입	기본 규칙
사용 안 함	none	rows > 10
2xx 상태코드 건수	count	count > 10
3xx 상태코드 건수	count	count > 10
4xx 상태코드 건수	count	count > 10
5xx 상태코드 건수	count	count > 10
정상 상태코드(2xx, 3xx) 건수	count_v2	include_minus_exclude_count > 10
에러 상태코드(4xx, 5xx) 건수	count_v2	include_minus_exclude_count > 10
에러 수신 건수	count	count > 10
예외 수신 건수	count	count > 10



프리셋	쿼리 타입	기본 규칙
초당 로그 발생건수	rps	rps > 100
필드 집계 (Aggregation)	aggr	avg > 1000
비율 (Rate)	rate	rate > 10
고유값 수 (Cardinality)	cardinality	cardinality > 100
백분위 (Percentile)	percentile	p99 > 3000

메시지

이벤트 발생 시 전달받을 알림 메시지를 입력하세요. 메시지에 변수를 사용하여 동적 메시지를 구성할 수 있습니다.

- 예시: 메시지 `${host}` 에서 에러 `${count}` 건 발생 → 알림 메시지 web-01에서 에러 15건 발생

표 | 메시지 변수

변수	설명	사용 조건
<code>\${count}</code>	조건에 맞는 로그 건수	항상 사용 가능
<code>\${groupField}</code>	그룹화 필드 이름	그룹화 알림만
<code>\${groupValue}</code>	그룹화 필드 값	그룹화 알림만
<code>\${필드명}</code>	그룹화 필드 값 (필드명으로 직접 참조)	그룹화 알림만



`${count}` 변수는 그룹화 여부와 관계없이 모든 알림에서 사용할 수 있습니다. `${groupField}` , `${groupValue}` , `${필드명}` 변수는 그룹화 필드를 설정한 경우에만 치환됩니다.

카테고리

로그 구분 명칭(로그 폴더명)을 목록에서 선택하거나 직접 입력하세요. 카테고리를 선택해야 검색 키와 검색 값을 입력할 수 있습니다.

필터

Lucene 쿼리 문법으로 로그 검색 조건을 입력합니다. 두 가지 입력 모드를 지원합니다.

- **필터 모드** : 필드와 값을 선택하여 쿼리를 구성합니다.
- **코드 모드** : Lucene 쿼리를 직접 입력합니다.

표 | Lucene 쿼리 예시

쿼리	설명
<code>level:ERROR</code>	level 필드가 ERROR인 로그
<code>status_nxx:status_4xx OR status_nxx:status_5xx</code>	4xx 또는 5xx 상태코드
<code>appender:accessLog</code>	accessLog appender의 로그
<code>response_time.n:*</code>	response_time.n 필드가 존재하는 로그
<code>host:web-01 AND level:ERROR</code>	web-01 호스트의 에러 로그

이벤트 발생 조건

쿼리 타입별로 설정합니다. 선택한 템플릿(프리셋) 또는 쿼리 타입에 따라 추가 설정 항목이 표시됩니다.

표 | 이벤트 발행 조건 키 의미

키	의미
<code>rows / count</code>	필터 조건에 맞는 로그 건수
<code>rps</code>	초당 로그 발생건수 (건수 / 인터벌 초)

키	의미
avg	대상 필드 값의 평균
sum	대상 필드 값의 합계
min	대상 필드 값의 최솟값
max	대상 필드 값의 최댓값
rate	분자 건수 / 분모 건수 × 100 (%)
cardinality	대상 필드의 고유한 값 개수
p99 / p95 / p90 / p75 / p50	대상 필드의 백분위 값
include_minus_exclude_count	포함 필터 건수 - 제외 필터 건수

- **건수 (count / none):** 설정한 필터 조건에 맞는 로그의 건수를 카운트합니다.

표 | 건수 설정 항목

설정 항목	설명
필터	로그 검색 조건 (Lucene 쿼리)
이벤트 발행 조건	건수 또는 조건에 맞는 로그 {연산자} {임계값} (예: count > 10)

- **초당 로그 발생건수 (rps):** 설정한 필터 조건에 맞는 로그의 초당 발생건수(Requests Per Second)를 계산합니다. 인터벌 시간 동안의 총 건수를 인터벌 초로 나누어 산출합니다.

표 | 초당 로그 발생건수 설정 항목

설정 항목	설명
필터	로그 검색 조건 (Lucene 쿼리)
이벤트 발행 조건	RPS {연산자} {임계값} (예: rps > 0.5)

- **필드 집계 (aggr):** 지정한 숫자 필드의 집계 값(평균, 합계, 최솟값, 최댓값)을 계산합니다. 이벤트 발행 조건에서 집계 방식을 드롭다운으로 선택할 수 있습니다.

표 | 필드 집계 설정 항목

설정 항목	설명
필터	로그 검색 조건 (Lucene 쿼리)
대상 필드	집계 대상 숫자 필드 (예: response_time.n)
이벤트 발행 조건	평균 / 합계 / 최솟값 / 최댓값 {연산자} {임계값} (예: avg > 1000)

- **비율 (rate):** 분자 필터와 분모 필터의 건수 비율(%)을 계산합니다. 전체 로그 대비 특정 조건의 비율을 모니터링할 때 유용합니다.

표 | 비율 설정 항목

설정 항목	설명
필터 (분자)	비율 계산의 분자가 되는 로그 조건 (예: level:ERROR)
분모 필터	비율 계산의 분모가 되는 로그 조건 (예: level:*)
이벤트 발행 조건	비율 (%) {연산자} {임계값} (예: rate > 10)

◦ 예시: 필터 level:ERROR, 분모 필터 level:*, rule rate > 10 → 전체 로그 중 에러 비율이 10%를 초과하면 알림 발생

- **고유값 수 (cardinality):** 지정한 필드의 고유한 값 개수를 계산합니다. 비정상적으로 많은 종류의 값이 발생하는 경우를 감지할 때 유용합니다.

표 | 고유값 수 설정 항목

설정 항목	설명
필터	로그 검색 조건 (Lucene 쿼리)
대상 필드	고유값을 계산할 필드 (예: host)

설정 항목	설명
이벤트 발행 조건	고유값 수 {연산자} {임계값} (예: cardinality > 100)

- **백분위 (percentile):** 지정한 숫자 필드의 백분위(Percentile) 값을 계산합니다. 응답 시간의 tail latency를 모니터링할 때 유용합니다. Percentile 선택을 변경하면 이벤트 발행 조건의 키가 자동으로 업데이트됩니다.

표 | 백분위 설정 항목

설정 항목	설명
필터	로그 검색 조건 (Lucene 쿼리)
대상 필드	백분위를 계산할 숫자 필드 (예: response_time.n)
Percentile	P99, P95, P90, P75, P50 중 선택
이벤트 발행 조건	P99 / P95 / ... {연산자} {임계값} (예: p99 > 3000)

표 | 백분위 의미

백분위	의미
P50	중앙값. 전체 데이터의 50%가 이 값 이하
P75	전체 데이터의 75%가 이 값 이하
P90	전체 데이터의 90%가 이 값 이하
P95	전체 데이터의 95%가 이 값 이하
P99	전체 데이터의 99%가 이 값 이하

- **포함/제외 건수 (count_v2):** 포함 필터의 건수에서 제외 필터의 건수를 뺀 순수 건수를 계산합니다.

표 | 포함/제외 건수 설정 항목

설정 항목	설명
필터 (포함)	포함할 로그 조건 (예: <code>status_nxx:status_4xx OR status_nxx:status_5xx</code>)
필터 제외	제외할 로그 조건 (예: <code>status_nxx:status_4xx</code>)
분모 필터	비율 계산용 분모 (선택사항)
이벤트 발행 조건	포함-제외 건수 {연산자} {임계값} (예: <code>include_minus_exclude_count > 10</code>)

- 예시: 필터 `status_nxx:status_4xx OR status_nxx:status_5xx`, 필터 제외 `status_nxx:status_4xx` → `4xx+5xx`에서 `4xx`를 제외한 순수 `5xx` 건수가 10을 초과하면 알림 발생

그룹화 필드(Group By)

그룹화 필드를 설정하면 해당 필드의 값별로 독립적으로 알림 조건을 판정합니다. 드롭다운에서 그룹화할 필드를 선택합니다. 드롭다운을 클릭하면 현재 카테고리에서 사용 가능한 필드 목록이 자동완성됩니다.

- 예시: 필터 `level:ERROR`, 그룹화 필드 `host`, rule `rows > 3`

표 | 그룹화 설정 비교

항목	그룹화 없음	그룹화 사용
판정 단위	전체 로그를 하나로 집계	그룹 값별 독립 집계
알림 발생	1건	조건 충족 그룹 수만큼
알림 제목	이벤트 제목	[그룹 값] 이벤트 제목
Stateful	전체 기준 상태 전이	그룹별 독립 상태 전이

- [web-01] 에러 알림 — web-01에서 에러 8건 → 알림 발생
- [web-02] 에러 알림 — web-02에서 에러 5건 → 알림 발생
- [api-01] 에러 알림 — api-01에서 에러 2건 → 조건 미충족, 알림 미발생

- ① 이벤트 상태가 해소되면 추가 알림을 활성화한 경우, 그룹별로 독립적으로 ABNORMAL → RECOVERED 상태가 전이됩니다. 예를 들어 web-01 에서 에러가 해소되면 [web-01] RECOVERED 알림이 발생하며, 다른 호스트의 상태에는 영향을 미치지 않습니다.

추가 설정

- **인터벌:** 선택한 시간(unset , 1분 , 5분 , 10분 , 30분 , 1시간 , 12시간) 간격으로 알림 조건을 확인합니다.
- **무음:** 이벤트 발생 후, 선택한 시간(unset , 1분 , 5분 , 10분 , 30분 , 1시간 , 12시간) 동안 같은 이벤트가 발생되지 않습니다.
- **이벤트 동작 시간:** 이벤트가 특정 시간대(근무/비근무/점검 시간 등)에 동작하도록 태그를 설정하세요. 태그를 설정하지 않으면 이벤트가 활성화된 상태에서 24시간 상시 동작합니다.
 1. + 추가를 클릭하세요.
 2. 이벤트 동작 시간에서 +새로운 태그 생성을 클릭하세요.
 3. 이벤트 동작 시간 태그 생성에서 태그 이름, 요일, 시간, 색상을 선택하고 [적용] 버튼을 클릭하세요.
 4. 생성한 태그는 태그 목록에서 확인할 수 있으며, 체크 박스를 선택하면 적용됩니다.
 5. 수정 또는 삭제할 태그의 ✎ 아이콘을 클릭해 이벤트 동작 시간 태그 수정에서 태그를 수정하거나 태그 삭제할 수 있습니다.

- ❗ 태그 삭제 시 해당 태그가 적용된 모든 사용자의 태그가 제거됩니다. 단, 이벤트 규칙에서 사용 중인 태그는 삭제할 수 없습니다.

- **이벤트 수신 태그:** 이벤트에 수신 태그를 설정하면, 해당 태그를 가진 프로젝트 멤버에게 알림을 전송합니다. 수신자 태그를 설정하지 않으면 프로젝트 내 모든 사용자에게 알림이 전송됩니다.
 1. + 태그 추가 또는 +를 클릭하세요.
 2. 이벤트 수신 태그 창 아래의 + 새 태그 생성을 클릭하세요.
 3. 태그 생성 창에서 태그 이름을 입력하고, 색상을 선택한 후, [태그 생성] 버튼을 클릭해 태그를 생성하세요.
 4. 생성된 태그는 태그 목록의 ✎ 아이콘을 클릭해 수정 또는 삭제하세요.
 5. 이벤트 수신 태그 창의 태그 목록에서 원하는 태그를 선택하면 적용됩니다.

- ✓ 이벤트 설정 시 이벤트 수신 태그를 선택하여 해당 태그를 가진 프로젝트 멤버와 3rd-party 플러그인에 알림을 전송할 수 있습니다. **경고 알림 > 이벤트 수신 설정**에서 프로젝트 멤버와 3rd-party 플러그인에 각각 태그를 지정할 수 있습니다.

시뮬레이션

알림을 저장하기 전에 과거 데이터로 시뮬레이션하여 알림 발생 예상 건수를 확인할 수 있습니다.

1. 알림 설정을 완료한 후 하단의 시간 범위를 선택하세요.
2. [시뮬레이션] 버튼을 클릭하세요.
3. 차트에 시간대별 데이터와 알림 발생 횟수가 표시됩니다.

❗ 시뮬레이션 시간 범위를 조절하여 다양한 시간대의 알림 발생 패턴을 확인할 수 있습니다. 최근 1~2분의 데이터는 인덱스 빌드 지연으로 조회되지 않을 수 있습니다.

4. 이벤트 규칙 추가 창에서 설정이 완료되면 [저장] 버튼을 클릭하세요.

로그 탐색기에서 알림 생성

로그 탐색기에서 직접 알림을 생성할 수 있습니다.

1. 로그 > 로그 탐색 메뉴로 이동하세요.
2. 카테고리 및 검색 쿼리를 설정하세요.
3. 화면 오른쪽 위의 [이벤트 추가] 버튼을 클릭하세요.
4. Drawer에서 알림 설정 폼이 열리며, 현재 카테고리 및 검색 쿼리가 자동으로 채워집니다.
5. 추가 설정을 완료하고 [저장] 버튼을 클릭하세요.
6. 저장 완료 후 [이동] 버튼을 클릭하면 알림 목록으로 이동합니다.

이벤트 수정/삭제

1. 경고 알림 > 이벤트 설정의 복합 로그 탭으로 이동하세요.
2. 로그 이벤트 목록에서 수정 또는 삭제하려는 이벤트의  아이콘을 클릭하세요.
3. 이벤트 설정 화면에서 옵션을 수정하고, [저장] 버튼을 클릭하세요.
 - a. 선택한 이벤트를 삭제하려면 이벤트 설정 화면의 오른쪽 위의 [삭제] 버튼을 클릭하세요.

이벤트 공유

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

- JSON 파일명: event-rules- YYYYMMDD .json

내보내기

1. 화면 오른쪽 위에 [JSON ] 버튼을 클릭하세요.
2. JSON 편집 창이 나타나면 [ 내보내기] 버튼을 클릭하세요.
 - 이벤트를 검색 후 내보내기 기능을 이용하면 검색한 목록만 JSON 파일로 다운받을 수 있습니다.
3. JSON 파일이 다운로드되면 공유할 다른 사용자에게 전달하세요.

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.

 같은 종류의 제품 간에 이용할 것을 권장합니다. 다른 제품의 프로젝트로부터 이벤트 설정을 가져올 수는 있지만 정상 작동하지 않습니다.

Json 형식으로 수정하기

1. 화면 오른쪽 위에 [JSON ] 버튼을 클릭하세요.
2. 편집 창이 나타나면 JSON 형식에 맞춰 내용을 수정하세요.
3. 수정을 완료하면 화면 아래 [저장] 버튼을 선택하세요.

❗ 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)

이벤트 수신 설정

홈 > 프로젝트 선택 >  경고 알림 > 이벤트 수신 설정

사용자별 이벤트 수신 설정

 **사용자별 이벤트 수신 설정** 의 다른 멤버의 정보는 **멤버 관리** 권한을 가진 멤버만 확인할 수 있습니다. 그 외 멤버에게는 필수 정보가 마스킹 처리됩니다.

- 이벤트 알림의 일괄 수신설정 및 접근 설정을 위한 모바일 기기 관리는 **계정 정보**에서 할 수 있습니다.
- 멤버 권한에 대한 자세한 설명은 [다음 문서](#)를 참고하세요.

수신 수단 설정

이메일, SMS, WhatsApp, 모바일 알림을 제공합니다.

사용자별 이벤트 수신 설정 섹션에서 원하는 알림 수신 수단의 체크 박스를 선택하면 경고 알림을 받을 수 있습니다. 알림 수신 수단의 체크 박스를 해제하면 경고 알림을 보내지 않습니다.

 프로젝트 최고 관리자를 제외한 모든 사용자는 자신의 수신 설정만 변경할 수 있습니다.

이메일 알림

이메일 알림은 회원 가입 시 입력한 이메일 주소로 알림을 보냅니다.

SMS 알림

SMS로 알림을 수신할 수 있습니다.

 SMS 알림 기능은 유료 프로젝트에 한정됩니다.

1. 화면 오른쪽 위의 **자신의 프로필 아이콘** > **계정 관리**로 이동하세요.
2. **계정 정보의 사용자 전화번호** 섹션에서 [일반 휴대전화] 버튼을 클릭하세요.
3. **전화번호**에 인증번호를 수신을 전화번호를 입력하세요.
 - SMS를 알림으로 수신할 수 있는 전화번호는 **한국의 휴대전화 번호만** 등록할 수 있습니다.
4. [저장] 버튼을 클릭하세요.

✔ 등록된 전화번호 변경 및 삭제

- 전화번호를 변경할 경우, [변경] 버튼을 클릭하세요. SMS 인증이 필요합니다.
- 전화번호를 삭제할 경우, [삭제] 버튼을 클릭하세요. 전화번호 삭제 시 SMS로 수신받는 알림은 수신할 수 없습니다.

WhatsApp 알림

WhatsApp을 통해 알림을 수신할 수 있습니다.

ⓘ WhatsApp 알림 기능은 유료 프로젝트에 한정됩니다.

1. 화면 오른쪽 위의 **자신의 프로필 아이콘** > **계정 관리**로 이동하세요.
2. **계정 정보의 사용자 전화번호** 섹션에서 [WhatsApp] 버튼을 클릭하세요.
3. 인증번호를 받을 **전화번호**를 입력하세요.
4. [인증번호 전송] 버튼을 클릭하세요.
5. WhatsApp 애플리케이션으로 전송된 인증번호 6자리를 입력하세요.
 - 10분 내로 인증번호를 받지 못했다면, [인증번호 재전송] 버튼을 클릭하세요.
6. [인증하기] 버튼을 클릭하세요.

모바일 알림

모바일 알림 수신이 필요한 사용자는 모바일 기기에 와탭 애플리케이션을 설치한 후 로그인해야 합니다.

- 와탭 애플리케이션 다운로드 - [안드로이드](#)
- 와탭 애플리케이션 다운로드 - [iOS](#)

반복 알림(에스컬레이션) 설정

경고 알림 발생 시간으로부터 알림 발생 상황이 해소되지 않을 경우 최초 알림 발생 시각으로부터의 알림 반복 간격을 설정할 수 있습니다. 위험(**Critical**) 레벨의 알림만 적용됩니다.

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.

1. **경고 알림 > 이벤트 수신 설정의 사용자별 이벤트 수신 설정** 섹션으로 이동하세요.
2. **반복 알림(에스컬레이션)** 항목에서 설정하세요.
 - **M**: 분, **H**: 시간, **D**: 일, 단위를 생략하면 분 단위로 시간을 설정합니다.
 - 숫자 또는 숫자+단위(**M, H, D**)로 입력하세요. 입력이 올바르지 않으면 메시지가 표시됩니다.
3. [저장] 버튼을 클릭하세요. 저장하지 않으면 설정되지 않습니다.

이벤트 수신 태그

이벤트 설정 시 이벤트 수신 태그를 선택하여 해당 태그를 가진 프로젝트 멤버와 3rd-party 플러그인에 알림을 전송할 수 있습니다. 이벤트 수신 태그를 설정하지 않으면 전체 멤버에게 경고 알림이 전송됩니다.

이벤트 수신 태그 추가/수정/삭제하기

 이벤트에 적용 중인 이벤트 수신 태그 항목은 삭제할 수 없습니다.

1. **경고 알림 > 이벤트 수신 설정**으로 이동하세요.
2. **사용자별 이벤트 수신 설정** 섹션의 사용자 목록에서 **+ 태그 추가** 또는 **+** 를 클릭하세요.
3. **이벤트 수신 태그** 창에서 **+ 새 태그 생성**을 클릭하세요.
4. **태그 생성** 창에서 태그 이름을 입력하고, 색상을 선택한 후, [태그 생성] 버튼을 클릭해 태그를 생성하세요.
5. 생성된 태그는 태그 목록의  아이콘을 클릭해 수정 또는 삭제하세요.
6. **이벤트 수신 태그** 창의 **태그 목록**에서 원하는 태그를 선택하면 적용됩니다.

이벤트 수신 태그 해제하기

1. 경고 알림 > 이벤트 수신 설정의 사용자별 이벤트 수신 설정 섹션으로 이동하세요.
2. 이벤트 수신 태그를 해제할 사용자의 이벤트 수신 태그 항목의 + 를 클릭하세요.
3. 이벤트 수신 태그 창에서 해제할 태그의 X 를 클릭하면 해당 태그가 해제됩니다.

수신 태그 미설정 알림 받기

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

- 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.

이벤트 수신 모드 선택하기

사용자별 이벤트 수신 설정 섹션에서 멤버 또는 3rd 파티 채널별로 이벤트 알림 수신 범위를 다음 네 가지 모드 중에서 선택할 수 있습니다. 수신 모드는 각 멤버 또는 채널 행의 이벤트 수신 태그 열에서 라디오 버튼으로 선택하세요.

수신 모드	설명
모든 알림 받기	이벤트 수신 태그와 무관하게 모든 경고 알림 수신
선택한 태그만 받기	선택한 이벤트 수신 태그를 가진 경고 알림만 수신. 태그를 최소 한 개 이상 선택
선택한 태그만 제외하기	선택한 이벤트 수신 태그를 가진 경고 알림만 제외하고 나머지 전부 수신. 제외 태그를 최소 한 개 이상 선택
모든 알림 받지 않기	어떤 이벤트 알림도 받지 않음. 선택해 둔 태그는 삭제되지 않고 그대로 보존

- 이벤트 수신 태그가 지정되지 않은 경고 알림까지 받으려면 태그 선택 영역에서 미분류 가상 태그를 선택하세요. 미분류 태그는 일반 태그와 동일하게 선택하거나 해제할 수 있으며, 태그 자체를 수정하거나 삭제할 수는 없습니다.

❗ **모든 알림 받지 않기** 모드에서는 해당 멤버 또는 채널이 이벤트 알림을 전혀 받지 않습니다. 이때 선택해 둔 태그는 삭제되지 않고 보존되므로, 다시 **선택한 태그만 받기** 모드로 전환하면 이전에 선택한 태그 설정을 그대로 사용할 수 있습니다.

선택한 태그만 받기

1. **사용자별 이벤트 수신 설정** 섹션에서 설정할 멤버 또는 3rd 파티 채널 행의 **이벤트 수신 태그** 옆을 클릭하세요.
2. **선택한 태그만 받기** 라디오 버튼을 선택하세요.
3. 태그 선택 영역에서 알림을 받을 태그를 하나 이상 선택하세요.

❗ **선택한 태그만 받기** 모드에서 태그를 하나도 선택하지 않았을 때 나타나는 완전 차단 경고는 **선택한 태그만 제외하기** 모드에는 표시되지 않습니다. 제외 태그가 없는 상태는 알림을 전부 차단하는 상태가 아니라 전부 수신하는 상태이기 때문입니다.

선택한 태그만 제외하기

경고 알림을 대부분 받되 특정 분류만 걸러 내고 싶을 때 사용합니다. 받을 태그를 하나씩 고르는 **선택한 태그만 받기**와 방향이 반대입니다.

1. **사용자별 이벤트 수신 설정** 섹션에서 설정할 멤버 또는 3rd 파티 채널 행의 **이벤트 수신 태그** 옆을 클릭하세요.
2. **선택한 태그만 제외하기** 라디오 버튼을 선택하세요.
3. 아래 태그 선택 영역에서 알림을 받지 않을 태그를 하나 이상 선택하세요.
 - 이벤트에 붙은 태그와 제외 태그가 하나라도 겹치면 해당 경고 알림은 전송되지 않습니다. 겹치는 태그가 없는 알림은 모두 수신합니다.
 - 제외 태그는 최소 한 개 이상 선택해야 합니다. 제외 태그가 하나도 없는 상태는 **모든 알림 받기**와 결과가 같아지므로, 마지막 태그는 제거할 수 없고 제외 태그가 비어 있는 동안 **최소한 하나의 태그를 선택해 주세요.** 안내가 표시됩니다.
 - 제외 태그 목록은 **선택한 태그만 받기** 모드의 수신 태그 목록과 별도로 저장됩니다. 두 모드를 번갈아 선택해도 각 모드에서 고른 태그가 그대로 남습니다.
 - **미분류** 가상 태그도 제외 대상으로 선택할 수 있으며, 태그 한 개로 계산됩니다.

알림 수신 언어 선택

사용자의 알림 수신 언어를 선택할 수 있습니다.

1. 경고 알림 > 이벤트 수신 설정으로 이동하세요.
2. 사용자별 이벤트 수신 설정 섹션의 사용자 목록에서 언어를 설정할 사용자의 가장 왼쪽에 ► 버튼을 클릭하세요.
3. 알림 수신 언어를 선택하세요.

요일 및 시간별 알림 설정

사용자의 요일별, 시간별 알림 수신 여부를 선택할 수 있습니다.

1. 경고 알림 > 이벤트 수신 설정으로 이동하세요.
2. 사용자별 이벤트 수신 설정 섹션의 사용자 목록에서 요일 및 시간별 알림을 설정할 사용자의 가장 왼쪽에 ► 버튼을 클릭하세요.
3. 경고 알림 수신을 원하는 요일을 선택하거나 시간을 입력하세요.
 - 알림 수신 수단별로 설정할 수 있습니다.

3rd 파티 플러그인

외부 애플리케이션을 통해 경고 알림을 받을 수 있습니다.

- 지원 애플리케이션: Slack, Telegram, Teams, Teams Workflows, Jandi, AlertNow, Webhook, Webhook JSON, Opsgenie, PagerDuty, LINE, ilert

❗ 와탭랩스의 지원 범위에 포함하지 않는 사내 메신저는 표준 Webhook, Webhook json을 통해 연동할 수 있습니다.

표 | 3rd 파티 플러그인 목록 구성

항목	설명
플러그인 이름	플러그인의 이름

항목	설명
인증 키	인증 키
인증 값	인증값
수신 레벨	경고, 전체, 위험으로 구분
반복 알림(에스컬레이션)	알림 발생 시간으로부터 알림 발생 상황이 해소되지 않았을 경우, 최초 알림 발생 시각으로부터의 알림 재발행 주기 - 위험(Critical) 단계의 알림에만 적용되는 기능
Smart 메시지(AI)	Telegram 3rd 파티 플러그인 추가 시 AI 알림 기능 제공 - 지원 언어: 한국어, 영어, 일본어
이벤트 수신 태그	프로젝트의 멤버 중 특정 멤버 또는 팀을 대상으로 알림 수신 여부
삭제	3rd 파티 플러그인 삭제

3rd 파티 플러그인 추가

1. 경고 알림 > 이벤트 수신 설정으로 이동하세요.
2. 3rd 파티 플러그인 섹션의 [추가하기] 버튼을 클릭하세요.
3. 서드 파티 플러그인 추가 창에서 원하는 서비스 탭으로 선택하세요.
4. 선택한 서비스의 안내([3rd 파티 플러그인 알림 추가 방법](#))에 따라 설정을 진행하세요.
5. [수신 테스트] 버튼을 클릭해 설정이 잘 되었는지 확인하세요.
6. 모든 과정을 완료하면 [추가하기] 또는 [등록] 버튼을 클릭하세요.

3rd 파티 플러그인 알림 추가 방법

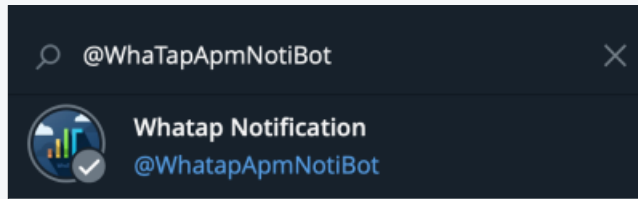
Slack

 서드 파티 플러그인 추가의 Slack 탭 화면의 [슬랙에 추가하기] 버튼을 클릭하면 Slack의 팀 및 채널에 WhaTapNotiBot을 등록할 수 있습니다.

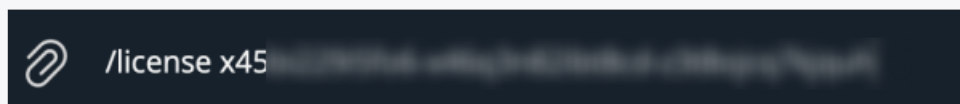
Telegram



1. Telegram에서 @WhaTapApmNotiBot을 검색하세요.



2. Bot을 선택하고 [시작] 버튼을 클릭하세요.
3. 채팅창에 `/license` 명령어와 알림을 받을 프로젝트의 액세스 키를 채팅창에 입력하세요.



① 사용할 수 있는 명령어 목록

- `/help` : 명령어 목록 보기
- `/license` : 알림 받을 프로젝트의 액세스 키 입력
- `/remove` : 알림을 받지 않을 프로젝트 코드 입력
- `/list` : 현재 알림을 받고 있는 프로젝트 코드 보기

Teams



1. 알림을 받을 채널의 커넥터로 이동하세요.



≡ 새 게시물 맨 위에 표시(최신순 정렬)

🔔 채널 알림

📌 고정

⚙️ 채널 관리

✉️ 전자 메일 주소 가져오기

↔️ 채널 링크 받기

👤 커넥터

2. Webhook을 추가하고 [구성] 버튼을 클릭하세요.

 **Incoming Webhook** 구성

서비스의 데이터를 Office 365 그룹에 실시간으로 보냅니다.

3. Webhook 이름을 입력하고 [만들기] 버튼을 클릭하세요.

 **Incoming Webhook** 피드백 보내기

수신 Webhook 커넥터를 사용하면 추적을 원하는 활동에 대한 알림을 외부 서비스로부터 받을 수 있습니다. 이 커넥터를 사용하려면 Office 365 커넥터 형식과(와) 호환되는 Webhook을 지원해야 하는 다른 서비스에서 특정 설정을 만들어야 합니다.

* 표시된 필드는 필수입니다.

Incoming Webhook를 설정하려면 이름을 지정하고 [만들기]를 선택합니다. *

Name

이 Incoming Webhook의 데이터와 연결할 이미지를 사용자 지정합니다.

이미지 업로드



기본 이미지

만들기 취소



4. 생성된 Webhook URL을 복사하세요.

아래 URL을 복사하여 클립보드에 저장한 다음 [저장]을 선택합니다. 사용자 그룹에 데이터를 전송하려는 서비스로 이동할 때 이 URL이 필요합니다.

`https://whatap.webhook.office.com/webhook`



URL이 최신 상태입니다.

완료

제거

5. 와탭 모니터링 서비스의 **서드 파티 플러그인 추가** 창으로 돌아와 Teams 탭 하단의 **Channel Name**과 **Webhook URL** 항목을 입력하세요.

6. [등록]버튼을 클릭하세요.

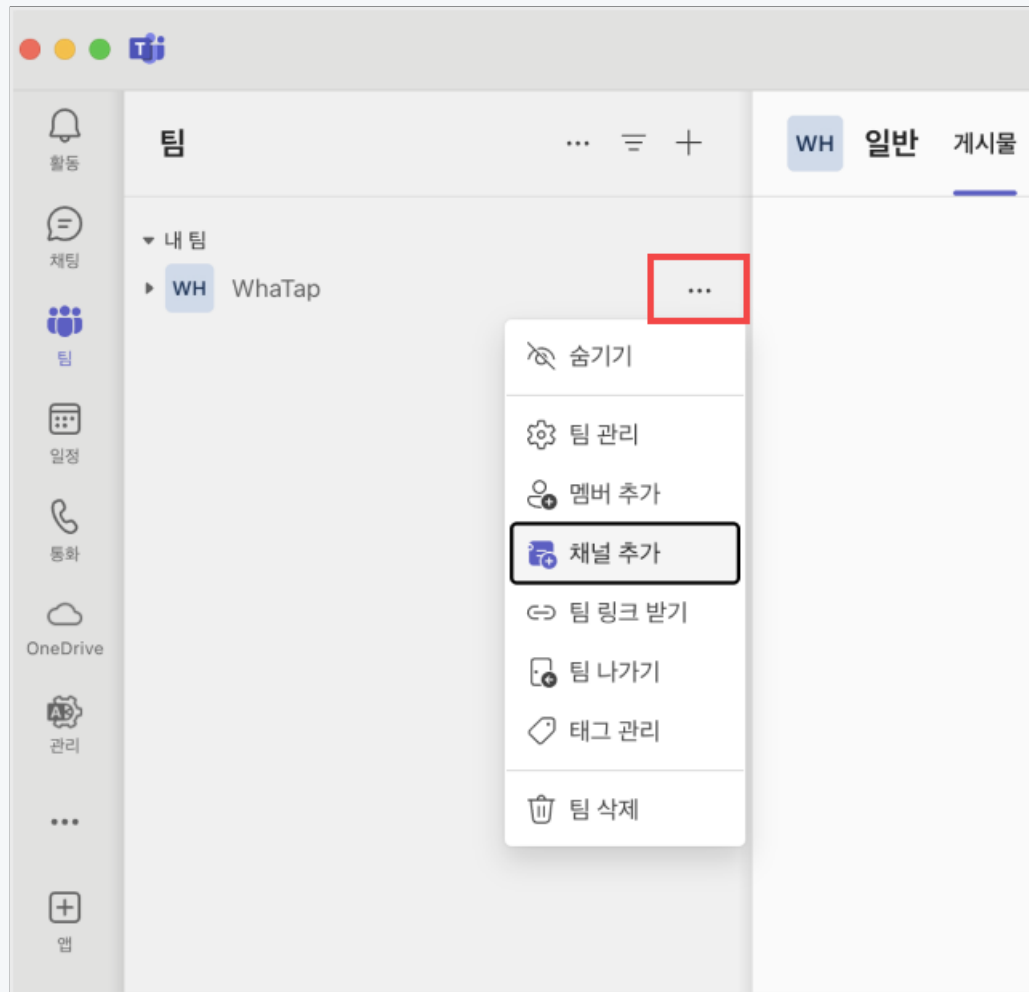


Teams Workflows



워크플로를 사용하려면 **Microsoft Teams**에 액세스할 수 있는 계정과 비즈니스 플랜 구독이 필요합니다.

1. 팀 메뉴의 더보기(...) > 채널 추가를 클릭하세요.



2. 채널 만들기 창에서 채널 이름과 설명을 입력하고, 채널 유형 선택 항목은 표준으로 선택한 후, [만들기] 버튼을 클릭하세요.



채널 만들기

채널 이름 *

WhaTap 알림 채널

설명

사람들이 올바른 채널을 찾을 수 있도록 설명을 입력하세요.

채널 유형 선택 *

①

선택

표준

팀의 모든 사람이 액세스할 수 있습니다.

공유

조직 내 또는 조직 외부의 사람이나 팀이 액세스할 수 있습니다.

비공개

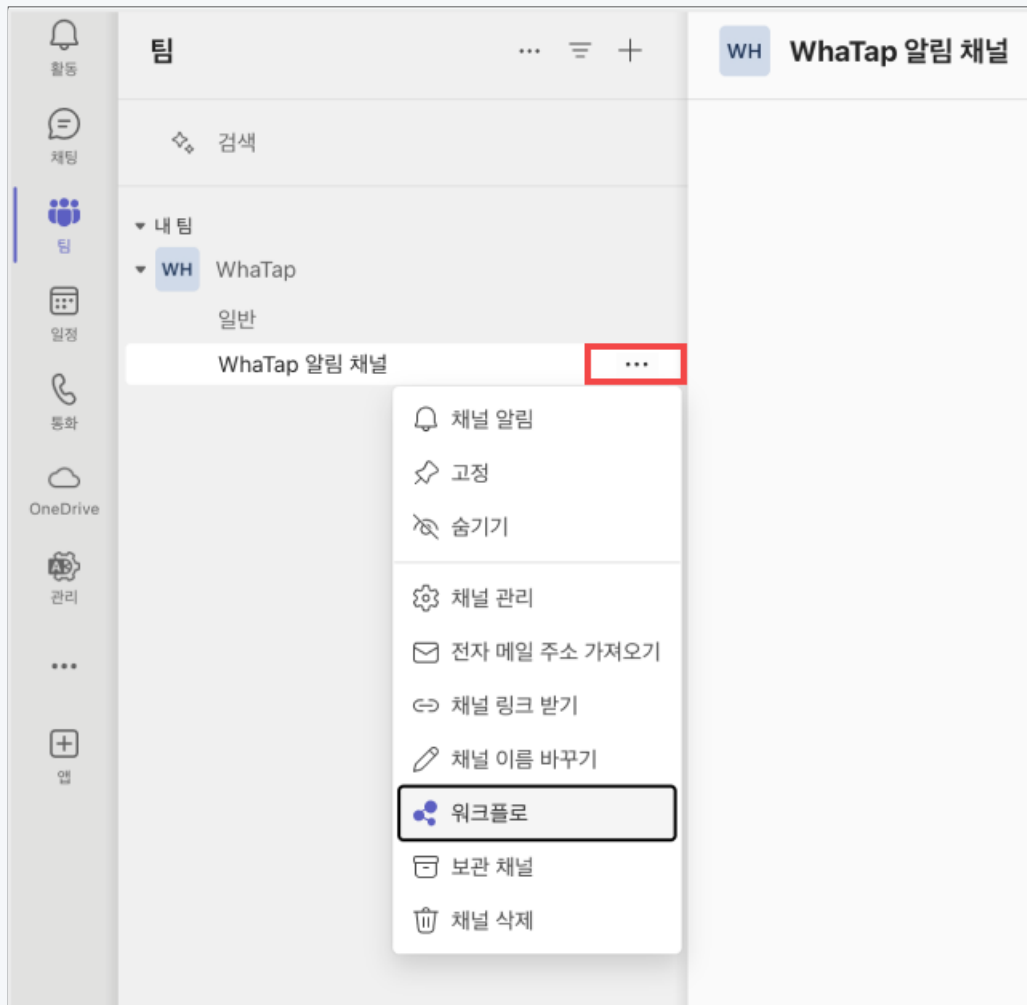
팀의 특정 사용자가 액세스할 수 있습니다.

취소

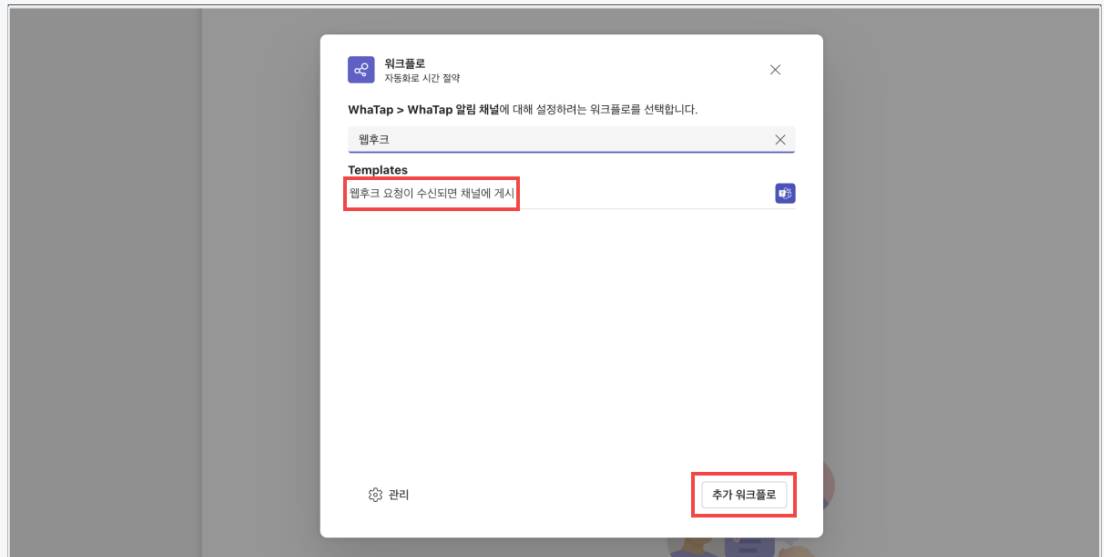
만들기

❗ 채널 유형을 공유로 선택하면 워크플로를 사용할 수 없으며, 비공개를 선택하면 워크플로를 추가할 수 있지만 알림을 수신할 수 없습니다.

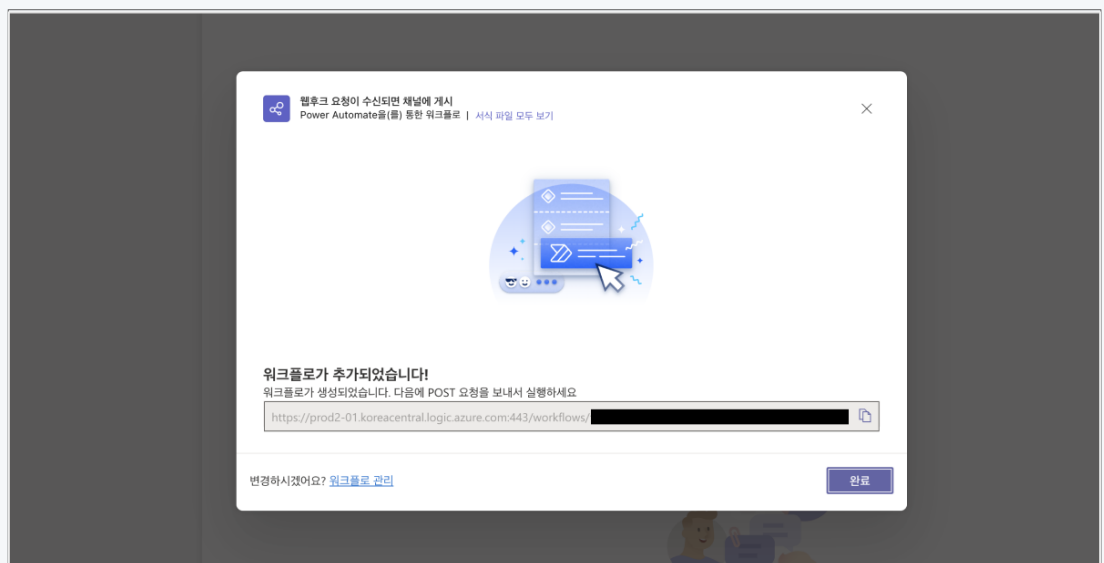
3. 생성한 채널의 더보기(...) > 워크플로를 클릭하세요.



4. 워크플로 대화상자의 워크플로의 목록에서 웹훅 요청이 수신되면 채널에 게시를 선택 후, [추가 워크플로] 버튼을 클릭하세요.



5. 이름과 연결 상태를 확인한 후, [다음] 버튼을 클릭하세요.
6. 세부 정보를 확인한 후, [워크플로 추가] 버튼을 클릭하세요.
7. 워크플로가 추가되었습니다. 생성된 주소를 복사하세요.

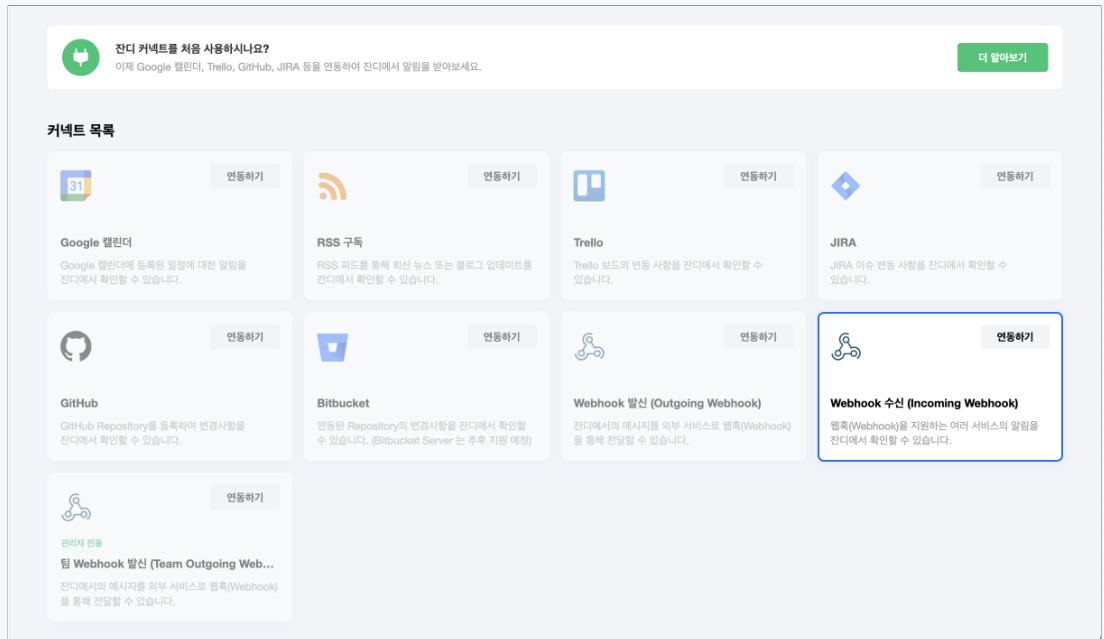


8. 와탭 모니터링 서비스의 **서드 파티 플러그인 추가** 창으로 돌아와 **Teams Workflows** 탭 안내 하단의 **Channel Name**과 **Webhook URL** 항목을 입력하세요.
9. [등록] 버튼을 선택하세요.

잔디(jandi)



1. 알림을 받을 토픽 또는 채팅에서 잔디 커넥트 설정으로 이동하세요.
2. 커넥트 목록에서 **Webhook 수신 (Incoming Webhook)** 항목에서 [연동하기] 버튼을 클릭하세요.



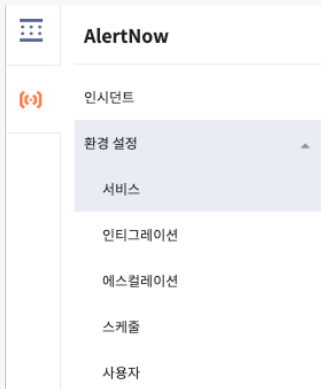
3. [Webhook 수신 추가] 버튼을 클릭하세요.
4. **Webhook URL 등록** 항목에 Webhook URL을 복사하세요.



5. 와탭 모니터링 서비스의 **서드 파티 플러그인 추가** 창으로 돌아와 Jandi 탭 안내 하단의 **Channel Name**과 **Webhook URL** 항목을 입력하세요.
6. [등록] 버튼을 클릭하세요.



1. AlerNow 서비스를 접속한 후, **환경 설정 > Integration** 메뉴로 이동하세요.



2. 인티그레이션 화면에서 [인티그레이션 생성] 버튼을 클릭하세요.
3. Integration 유형 중 **WhaTap**을 선택하세요.
4. 인티그레이션 생성 화면에서 이름 및 이름 지정 규칙을 설정하세요.

5. [확인] 버튼을 클릭하면 Integration이 생성됩니다.
6. 생성된 인티그레이션 목록을 확인하고 생성된 Integration 항목을 선택하세요.



인티그레이션 ?

인티그레이션 생성

검색어 입력

Q

🔄

마지막 업데이트: 2020-07-02 16:51:44

인티그레이션 이름	인티그레이션 유형	인티그레이션 키	서비스 이름
Whatap - APM	WhaTap	46c1982c7	Whatap - APM

- 상세 화면에서 URL 오른쪽의 복사 아이콘을 클릭해 URL을 복사하세요.

← 인티그레이션

Whatap - APM

기본 정보

인티그레이션 유형	WhaTap
인티그레이션 키	46c1982c7
URL	https://alertnowitgr.opsnow.com/integration/whatap/v1/46c1982c7

- 와탭 모니터링 서비스의 **서드 파티 플러그인 추가** 창으로 돌아와 **AlertNow** 탭 안내 하단의 **Channel Name**과 **Webhook URL** 항목을 입력하세요.
- [등록] 버튼을 클릭하세요.

Webhook



- 알림을 받을 Webhook을 등록하세요. 등록된 URL에 POST Method로 알림의 **title** , **text** 가 전송됩니다.

```
{
  "title": "Alert Title",
  "text": "Sample warning message"
}
```

- Webhook Name**과 **Webhook URL** 항목을 입력하세요.
- [등록] 버튼을 클릭하세요.

Webhook JSON





1. 알림을 받을 Webhook을 등록하세요. 등록된 URL에 POST Method로 알림 데이터가 JSON 형태로 전송됩니다. JSON 내에 포함 시킬 수 있는 대체 변수에 대해선 **사용 가능 변수** 부분을 참고하세요.
 - `${something}` 은 와탭에서 제공하는 대체될 값입니다. 지원하는 전체 목록과 의미는 사용 가능 변수를 참고하세요.
 - 이벤트 상태(`status`)는 이벤트 발생(`on`), 이벤트 해소(`off`)로 구분할 수 있습니다.
 - `level` 은 `None` , `Info` , `Warning` , `Critical` 로 구분합니다.

```
{
  "pcode": "${pcode}",
  "projectName": "${projectName}",
  "time": "${time}",
  "oid": "${oid}",
  "oname": "${oname}",
  "title": "${title}",
  "message": "${message}",
  "level": "${level}",
  "status": "${status}",
  "metricName": "${metricName}",
  "metricValue": "${metricValue}",
  "metricThreshold": "${metricThreshold}",
  "uuid": "${uuid}",
  "okind": "${okind}",
  "onode": "${onode}"
}
```

2. **Webhook Name**과 **Webhook URL** 항목을 입력하세요.
3. Header 값을 추가하려면 **사용자 Header 값 추가**의 + 추가를 클릭해 key, value을 추가하세요.
4. [등록] 버튼을 클릭하세요.

Opsgenie



1. **Teams** 메뉴에서 알림을 수신할 팀을 선택하세요.
2. **Integration** 메뉴로 이동해 [Add Integration] 버튼을 클릭하세요.



On-call
Integrations
Heartbeats

Integrations

3. Integration 목록에서 'API' 검색 후 선택하세요.

X

Add integration

Integrate your Opsgenie account with over 200 powerful apps and web services to sync alert data, and streamline your workflow.

API

API

API

Apica Synthetic Monitoring

API

APImetrics

API

ConnectWise Automate (API)

API

Zapier

4. API 명과 Team을 할당하고 각 권한을 설정한 후, [Save Integration] 버튼을 클릭하세요.

Forwarding rules
Your on-call schedule

ON-CALL
Global policies
All schedules
All escalations

CONNECTED APPS
Atlassian products

INTEGRATIONS
Integrations
Heartbeats
Slack
GitLab

Settings

Name:

Assigned to Team: ?

API Key: ?

Read Access: ?
☒

Create and Update Access: ?
☒

Delete Access: ?
☒

Restrict Configuration Access: ?
☐

Enabled: ?
☒

Suppress Notifications: ?
☐



5. 와탭 모니터링 서비스의 **서드 파티 플러그인 추가** 창으로 돌아와, **Opsgenie** 탭 안내 하단의 **Name**과 **API Key** 항목을 입력하세요.
6. [등록] 버튼을 선택하세요.

PagerDuty



1. [PagerDuty](#) 계정에 등록하고 로그인하세요.
2. PagerDuty에서 **Services > Service Directory** 메뉴에서 [+ New Service] 버튼을 클릭하세요.

PagerDuty

3. Service 정보(**Name**)를 입력한 후 [Next] 버튼을 클릭하세요.

PagerDuty

4. Escalation Policy를 설정 후 [Next] 버튼을 클릭하세요.

PagerDuty

5. **Alert Grouping**과 **Transient Alerts** 항목을 설정한 후 [Next] 버튼을 클릭하세요.

PagerDuty

6. **Integrations**에서 **Event API V2**를 선택한 후 [Create Service] 버튼을 클릭하세요.

PagerDuty

7. 생성한 Service 화면에서 **Integration Name**과 **Integration Key** 값을 복사하세요.

PagerDuty

8. 와탭 모니터링 서비스의 **서드 파티 플러그인 추가** 화면으로 돌아와 **Integration Name**과 **Integration Key** 항목을 입력하세요.

9. [등록] 버튼을 클릭하세요.

ⓘ 메시지를 수신하지 못했거나 플러그인이 등록되지 않았다면 **Integration Name** 또는 **Integration Key**값이 올바른지 확인하세요.

LINE



1. LINE 앱을 설치합니다.
2. 아래 QR 코드를 스캔하여 WhaTapLabs 공식 채널을 친구로 추가합니다.



3. 다음 명령어를 사용하여 프로젝트를 라인과 연동하고 알림을 설정하세요.

명령어

```
/help # 사용 가능한 명령어 안내
/list # 연동된 프로젝트 목록 조회
/license [엑세스키] # 새 프로젝트 연동 추가
/remove [프로젝트코드] # 프로젝트 연동 해제
/language [ko|ja|en] # 알림 언어 설정 (한국어/일본어/영어)
```

- 프로젝트 액세스 키는 **관리 > 프로젝트 관리**에서 확인하실 수 있습니다.
- 라인 내에서 `/language` 명령어를 사용하는 것은 라인 내 채팅방에만 적용됩니다. 다른 3rd 플러그인이나 프로젝트의 알림 수신 언어가 변경되는 것은 아닙니다.

사용 예시

```
/license XXXXXXXXXX # 프로젝트 연동
/language ko # 한국어로 언어 설정
```



```
/list # 연동된 프로젝트 확인
```



- 프로젝트 액세스 키: WhaTap 프로젝트 내 **관리 > 프로젝트 관리**에서 확인할 수 있음
- 언어 설정: `/language` 명령어는 LINE 채팅방 내에서만 적용되며, 다른 알림 채널의 언어는 변경되지 않음

ilert



1. ilert 콘솔에서 **Alert sources** 화면의 오른쪽 위의 [+ Create alert source]를 클릭하세요.
2. **Integration type** 단계의 하단에 있는 **Filter integrations** 검색창에 WhaTap 을 입력해 검색합니다.
3. 검색 결과에서 **WhaTap** 타일을 선택한 후 [Next] 버튼을 클릭합니다.
4. 알림 소스 이름을 입력하고 팀을 지정한 후 [Next] 버튼을 클릭합니다.
 - 에스컬레이션 정책은 새 정책을 생성하거나 기존 정책을 선택할 수 있습니다.
5. 알림 그룹화 방식을 선택한 후 [Continue setup] 버튼을 클릭합니다.
 - 우선 선택한 **Do not group alerts**는 이후 변경할 수 있습니다.
6. 다음 화면에서 **알림 템플릿**, **우선순위** 등 추가 설정을 할 수 있습니다. 우선 [Finish setup] 버튼을 클릭해 설정을 완료합니다.
7. 설정이 완료되면 완료 화면에서 **API 키** 또는 **Webhook URL**이 생성됩니다.
8. **Webhook JSON** 탭에서 생성된 **Webhook URL**을 복사해 아래의 **Webhook URL** 입력란에 붙여넣습니다.
9. [등록] 버튼을 클릭하세요.

대량 알림 발생 방지

알림이 대량으로 발생하면 지정한 시간 동안 알림이 일시적으로 중지됩니다. 예를 들어, 5분 동안 20회의 이벤트가 발생하면 5분

동안 경고 알림을 중지합니다. 설정한 **정지 시간** 시간이 지나면 대량 알림 발생 방지 기능은 해제됩니다.

1. **경고 알림 > 이벤트 수신 설정의 대량 알림 발생 방지** 섹션으로 이동하세요.
2. 토글 버튼을 클릭해 **활성화** 또는 **비활성화** 할 수 있습니다.
 -  **활성화**: 대량 알림 일시적 중지
 -  **비활성화**: 대량 알림 재개
3. **탐지 시간, 탐지 횟수, 정지 시간**을 설정하세요.
 - **탐지 시간** 동안 **탐지 횟수** 이상의 이벤트가 발생하면 **정지 시간** 동안 경고 알림을 중지합니다.

❗ 대량 알림으로 차단되는 경우 차단 안내 박스가 표시됩니다. 대량 알림 차단 기능을 해제하려면 박스의 [대량 알림 발생 중지] 버튼을 클릭하세요.

이벤트 수신 포맷

공용 알림 템플릿

공통 템플릿은 대부분의 경우 적용 가능합니다. 다양한 환경에서 동일한 포맷으로 알림을 받을 수 있습니다.

- Product Type: 애플리케이션, 데이터베이스, 쿠버네티스
- Event Type: 애플리케이션 알림, 데이터베이스 알림, 메트릭스 알림
- Event Channel: sms, mobile, 3rd party plugin, plugin

이벤트 제목

Event title format

```
[Level][Platform][ProjectName][ApplicationName][EventTitle]
```

Event title example

```
[Info][JAVA][애플리케이션 프로젝트][TC-0-1-8081][CRITICAL_HIGH_MEMORY]
```

ⓘ ApplicationName을 설정하지 않은 경우 이벤트 제목에서 생략합니다.

- Platform은 다음 중 한 가지로 표시합니다.
 - JAVA
 - NODEJS
 - PYTHON
 - PHP
 - DOTNET
 - GO
 - POSTGRESQL
 - ORACLE



- MYSQL
- MSSQL
- BSM_JAVA
- CLOUDWATCH
- TIBERO
- KUBERNETES
- KUBE_NS
- URLCHECK
- URLCHECK_ADMIN
- CUBRID
- ALTIBASE
- CLUSTER
- REDIS
- MONGODB
- VR
- RUM

이벤트 메시지

이벤트 메시지에 포함할 수 있는 정보입니다. `optional` 이 `false` 인 경우 항상 메시지에 포함합니다. `optional` 이 `true` 인 경우 해당 데이터를 확인할 수 있으면 표시합니다.

Event message example

```
Project Name : 애플리케이션 프로젝트
Project Code : 3
Agent Name : TC-0-1-8081
Message : RECOVERED: Memory is too high. less than 10%
Event Time : 2022-04-12 18:53:24 +0900
Event OFF Time : 2022-04-12 18:53:24 +0900
Alert Type : APPLICATION_MEMORY
```

Metric Name : memory
 Metric Value : 20
 Metric Threshold : 10
 Stateful : true

표 | 이벤트 메시지 구성 요소

En	Ko	지원되는 알림 타입	설명
Project Name	프로젝트 이름	전체	-
Project Code	프로젝트 Code	전체	-
Agent Name	에이전트 이름	전체(optional)	oname
Message	이벤트 메시지	전체	-
Alert Type	이벤트 종류	전체	아래의 AlertType 종류 표 참고
Event Time	이벤트 발생 시간	전체	2022-04-13 10:40:49 +0900에서 +0900는 GMT를 의미합니다.
Event Off Time	이벤트 해제 시간	전체(optional)	2022-04-13 10:40:49 +0900에서 +0900는 GMT를 의미합니다.
Metric Name	메트릭스 이름	전체(optional)	이벤트 조건 판단에서 사용하는 메트릭스의 이름
Metric Value	메트릭스 값	전체(optional)	메트릭스 값이 메트릭스 임계치를 넘으면 이벤트 발생 조건이 만족한 경우입니다.
Metric Threshold	메트릭스 임계치	전체(optional)	메트릭스 값이 메트릭스 임계치를 넘으면 이벤트 발생 조건이 만족한 경우입니다.
Stateful	해소된 이벤트 알림	전체(optional)	해소된 이벤트 알림 기능 사용 중이면 true, 아니면 false
Event Rule	이벤트 발생 조건	메트릭스 알림	-

En	Ko	지원되는 알림 타입	설명
Target Filter	이벤트 대상 선택	메트릭스 알림	특정 대상에서 수집된 메트릭스에 대해서만 이벤트 조건을 확인합니다.
Repeat Count	이벤트 반복 횟수	메트릭스 알림	이벤트 조건이 이벤트 반복 시간동안 이벤트 반복 횟수만큼 만족해야 이벤트가 발생합니다.
Repeat Duration	이벤트 반복 시간	메트릭스 알림	이벤트 조건이 이벤트 반복 시간동안 이벤트 반복 횟수만큼 만족해야 이벤트가 발생합니다.
Receiver	수신자	메트릭스 알림	-
Query	MXQL 쿼리	복합 메트릭스 알림	-
Rule	이벤트 발생 조건	복합 메트릭스 알림	-
Query Period	쿼리 기간	복합 메트릭스 알림	-
Query Interval	쿼리 간격	복합 메트릭스 알림	-
Silent Time	무음 시간	복합 메트릭스 알림	-
Query	URL	Exception 알림	Exception을 발생시킨 요청의 URL
TXID	트랜잭션 ID	Exception 알림	-
Class	에러 클래스 이름	Exception 알림	-

En	Ko	지원되는 알림 타입	설명
Log Message	로그 메시지	서버 - 파일 로그 알림	-
Log File	로그 파일 경로	서버 - 파일 로그 알림	-
IP	IP	서버 알림 전체	-
CPU	CPU	서버 알림 전체	이벤트 발생 당시의 Snapshot
CPU_load1	CPU_load1	서버 알림 전체	이벤트 발생 당시의 Snapshot
CPU_loadPerCore	CPU_loadPerCore	서버 알림 전체	이벤트 발생 당시의 Snapshot
Memory	Memory	서버 알림 전체	이벤트 발생 당시의 Snapshot
Swap	Swap	서버 알림 전체	이벤트 발생 당시의 Snapshot
Disk Name Used Percent Free Size IO Percent	디스크 퍼포먼스	서버 알림 전체	이벤트 발생 당시의 Snapshot
Name Bps Pps	트래픽 퍼포먼스	서버 알림 전체	이벤트 발생 당시의 Snapshot
Message Time Name	처리내역 메시지	서버 알림 전체	-

ⓘ 해당 이벤트에서 제공할 수 있는 최대한 많은 정보를 보여줍니다.

- AlertType은 다음 중 한 가지로 표시합니다.

AlertType	설명
APPLICATION_CPU	애플리케이션 CPU 알림
APPLICATION_MEMORY	애플리케이션 MEMORY 알림



AlertType	설명
APPLICATION_DISK	애플리케이션 DISK 알림
APPLICATION_ACTIVE_TRANSACTION	애플리케이션 액티브 트랜잭션 알림
APPLICATION_ERROR_TRANSACTION	애플리케이션 에러 트랜잭션 알림
APPLICATION_SLOW_TRANSACTION	애플리케이션 트랜잭션 응답시간 알림
METRICS	메트릭스 알림
COMPOSITE_METRICS	복합 메트릭스 알림
ANOMALY	이상치 탐지 알림
LOG_REALTIME	로그 실시간 알림
COMPOSITE_LOG	복합 로그 알림
SERVER_REBOOT	서버 - 재시작 알림
SERVER_NO_DATA	서버 - 미수신 알림
SERVER_PORT	서버 - 포트 알림
SERVER_NETWORK_IOPS	서버 - 네트워크 IOPS 알림
SERVER_NETWORK_BPS	서버 - 네트워크 BPS 알림
SERVER_DISK_IO	서버 - 디스크 I/O 알림
SERVER_DISK_QUOTA	서버 - 디스크 사용량 알림
SERVER_DISK_INODE	서버 - inode 알림



AlertType	설명
SERVER_CPU	서버 - CPU 알림
SERVER_MEMORY	서버 - 메모리 알림
SERVER_CPU_STEAL	서버 - steal 알림
SERVER_MEMORY_SWAP	서버 - 스왑 알림
SERVER_LOG_FILE	서버 - 로그 파일 알림
SERVER_WINDOW_EVENT	서버 - 윈도우 이벤트 알림
SERVER_OFF	서버 - 알림 OFF 알림
SERVER_ACKNOWLEDGE	서버 - 처리내역 알림
SERVER_PROCESS_COUNT	서버 - 프로세스 수 알림
SERVER_PROCESS_CPU	서버 - 프로세스 CPU 알림
SERVER_PROCESS_MEMORY	서버 - 프로세스 메모리 알림
SERVER_PROCESS_OFF	서버 - 프로세스 알림 OFF 알림
AGENT_ACTIVE	에이전트 활성화 알림
AGENT_INACTIVE	에이전트 비활성화 알림
AGENT_REACTIVATED	에이전트 재활성화 알림
URL	URL 알림
TOO_MANY_EVENT	너무 많은 이벤트 발생 알림



AlertType	설명
CLOUD_WATCH	Cloud Watch 알림
EXCEPTION	Exception 알림

이벤트 기록 및 모니터링

홈 > 프로젝트 선택 >  경고 알림 > 이벤트 기록

이벤트 기록은 프로젝트에서 발생한 여러 이벤트를 조회하고 상세 정보를 분석할 수 있습니다. Elasticsearch DSL 쿼리를 지원하며, 원하는 조건에 맞는 이벤트를 정확하고 빠르게 찾을 수 있습니다.

이벤트 기록 조회하기

검색 결과에서 **이벤트 제목**을 클릭하면 해당 이벤트가 발생한 시간대의 상세 데이터를 분석할 수 있는 화면으로 이동합니다. 이를 통해 이벤트 발생 전후 상황을 종합적으로 파악할 수 있습니다.

1. 경고 알림 > 이벤트 기록으로 이동하세요.
2. 이벤트 기록 화면의 시간 선택에서 이벤트 기록을 조회할 기간을 설정하세요.
3. 필터 입력 창에 쿼리를 입력하고 [돋보기] 버튼을 클릭하세요.
 - 쿼리를 입력하지 않으면 전체 이벤트가 조회됩니다.

컬럼 설정

원하는 컬럼을 표시하거나 숨길 수 있습니다.

1. 이벤트 기록 화면의 왼쪽 위 [ 컬럼 설정] 버튼을 클릭하세요.
2. 컬럼 설정 창에서 표시하거나 숨길 컬럼을 선택하세요.
 - 표시 항목에서 컬럼의 순서를 변경할 수 있습니다.
 - 컬럼명 검색창에 원하는 컬럼 항목을 검색할 수 있습니다.

컬럼 항목	설명
이벤트 이름	이벤트의 제목
메시지	이벤트의 메시지 또는 스냅샷 정보

컬럼 항목	설명
이벤트 상태	이벤트의 현재 상태
에이전트 명	이벤트가 발생한 대상 에이전트의 이름(Oname) - 특정 에이전트에 대해 발생한 이벤트가 아닌 경우 빈칸으로 표시됨
에이전트 그룹	이벤트가 발생한 대상 에이전트의 종류(OkindName) - 특정 에이전트에 대해 발생한 이벤트가 아닌 경우 빈칸으로 표시됨
에이전트 노드	이벤트가 발생한 대상 에이전트의 서버(OnodeName) - 특정 에이전트에 대해 발생한 이벤트가 아닌 경우 빈칸으로 표시됨
이벤트 발생 시각	이벤트가 발생한 시간
이벤트 해소 시각	이벤트가 해소된 시간 상태가 없는 이벤트의 경우 - 로 표시됨

3. 설정을 완료한 후, [확인] 버튼을 클릭해 컬럼 설정을 반영합니다.

↓ CSV 다운로드

조회 결과를 CSV 파일 형식으로 다운로드할 수 있습니다.

1. 경고 알림 > 이벤트 기록에서 [CSV] 버튼을 클릭하세요.
2. 현재 필터 조건에 맞는 이벤트 목록이 CSV 파일로 저장됩니다.

진행 중인 이벤트만 보기

현재 진행 중인 상태의 이벤트만 조회할 수 있습니다.

1. 경고 알림 > 이벤트 기록에서 [진행 중인 이벤트만 보기] 버튼을 클릭하세요.
2. 필터 쿼리에 다음 조건이 자동으로 추가되어 검색됩니다.

```
Stateful: true and Status : "ON"
```

이벤트 검색

- **정확한 검색:** 원하는 조건을 정확히 지정하여 필요한 이벤트만 조회
- **복합 조건:** 여러 필드를 동시에 검색하여 복잡한 조건도 한 번에 처리
- **유연한 패턴:** 와일드카드, 부분 검색 등 다양한 검색 방식 지원
- **빠른 성능:** 인덱싱된 데이터를 활용한 고속 검색

검색 가능한 필드

필드와 값에 대해 대소문자를 구분하지 않습니다.

- **필드명 태그:** 필드가 지원되는 이벤트 타입
- **필드 타입:** 필드의 데이터의 타입
 - : Number
 - : String
 - : Boolean
 - : Date

이벤트 정보 필드

필드명	타입	설명	예시 값
Title	String	이벤트 제목	"Database Connection Error"
OffTitle	String	이벤트 해소 제목	"RECOVERED: Database Connection Error"
Message	String	이벤트 메시지	"Connection timeout occurred"
OffMessage	String	이벤트 해소 메시지	"RECOVERED: Connection timeout occurred"
Level	String	현재 이벤트 레벨	Critical, Warning, Info

필드명	타입	설명	예시 값
OriginLevel	String	원본 이벤트 레벨	Critical, Warning, Info
Status	String	이벤트 상태	ON, OFF, CANCEL, ACKNOWLEDGE, MAINTENANCE, DISABLED
ActCount	Number	처리내역 개수	2
MetricName	String	지표 이름	"memory"
MetricValue	String	지표 값	"85.5"
OffValue	String	해소 값	"72.8"
MetricThreshold	String	임계치	"80"
alertType	String	이벤트 종류	"BASIC", "METRICS", "TRANSACTION" 등
alertId	String	이벤트 규칙의 고유식별자	"zf3uojer0fv4v7"

이벤트 타입별 지원 필드

ⓘ 특정 이벤트 타입에서만 지원되는 필드입니다. 해당 이벤트 타입이 아닌 경우 값이 없을 수 있습니다.

필드명	타입	이벤트 종류	설명	예시 값
eventRule	String	기본, 메트릭스	이벤트 발생 규칙	"memory ≥ 80"
field	String	실시간 로그	로그 검색 키	"content"

필드명	타입	이벤트 종류	설명	예시 값
keyword	String	실시간 로그	로그 검색 값	"Error"
logCategory	String	실시간 로그	로그 카테고리	"AppLog"
logContent	String	실시간 로그	로그 내용	"00:00000:00009:2025/04/06 23:03:52.55 server Error: 1601, Severity: 17, State: 3\n00:00000:00009:2025/04/06 23:03:52.55 server There are not enough 'user connections' available to start a new process."

대상 필드

필드명	타입	설명	예시 값
Oid	Number	에이전트 고유식별자	-98765432
Oname	String	에이전트 이름	"web-server-01"
Okind	Number	에이전트 종류 고유식별자	867318026
OkindName	String	에이전트 종류명	"web-server"
Onode	Number	에이전트 서버 고유식별자	334634079
OnodeName	String	에이전트 서버명	"production-node-1"

이벤트 고유값 필드

필드명	타입	설명	예시 값
Id	Number	이벤트의 고유식별자	5768121

필드명	타입	설명	예시 값
UUID	String	이벤트 고유식별자	"550e8400-e29b-41d4-a716"

상태/플래그 필드

필드명	타입	설명	예시 값
Stateful	Boolean	상태 기반 이벤트 여부	true, false
Disabled	Boolean	종료된 이벤트 여부	true, false
Escalation	Boolean	에스컬레이션 여부	true, false
SystemEvent	Boolean	시스템 이벤트 여부	true, false

검색 유형별 문법

❗ 검색 기본 문법은 [WhaTap log search query 문법](#) 문서를 참고하시기 바랍니다.

1. 키워드 검색

Database Connection 문자열이 포함된 이벤트

```
title: "Database Connection"
```

2. 여러 값 검색

여러 옵션 중 하나라도 포함되는 이벤트를 조회합니다.

```
title: Database Connection
```

현재 이벤트 레벨이 Info이거나 Warning인 이벤트

```
level: info warning
```

3. 패턴 검색

와일드카드를 사용하여 패턴을 검색할 수 있습니다.

이름 패턴으로 특정 에이전트에서 발생한 이벤트 찾기

```
oname: web-*-prod
```

제목이 Connection으로 끝나는 이벤트 찾기

```
title: *Connection
```

4. 복합 조건 검색

여러 조건을 조합하여 정확히 검색할 수 있습니다.

Critical 레벨이면서 제목에 Database가 포함된 이벤트

```
level: critical and title: Database
```

특정 에이전트의 Warning 또는 Critical 이벤트

```
oname: web-server-01 and level: Warning Critical
```

5. OR 조건 검색

여러 조건 중 하나라도 만족하는 이벤트를 조회합니다.

제목 또는 메시지에 특정 키워드가 포함된 이벤트

```
title: Connection or message: Connection
```

6. 제외 조건

특정 조건을 제외해 검색할 수 있습니다.

Info 레벨을 제외한 모든 이벤트

not level: info

실시간 알림

실시간 알림 기능은 이벤트 설정을 통해 설정한 이벤트가 발생할 때 팝업 형태 표시됩니다. 이벤트 발생 즉시 알림을 받아 문제를 빠르게 인지하고 대응할 수 있습니다. 이미 발생했거나 놓친 알림 내역을 확인하여 실시간 대응이 어려웠던 상황을 파악하고 해결할 수 있습니다.

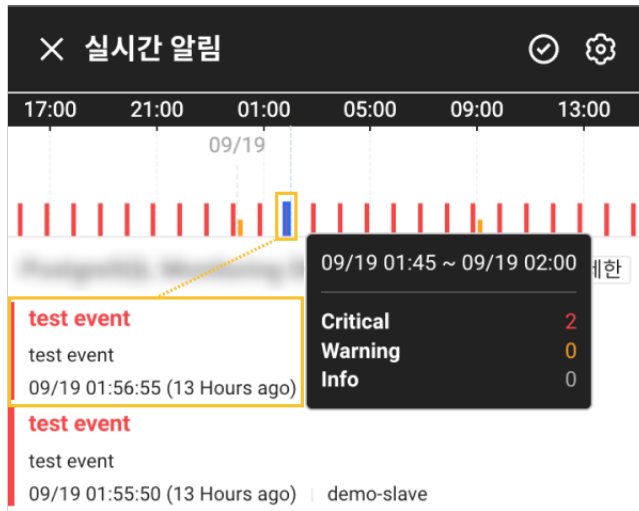
실시간 알림 확인하기

실시간 알림은 화면 오른쪽 위 팝업 형태로 표시됩니다. 알림이 발생한 시간, 제목, 메시지를 확인할 수 있습니다.

- 개별 알림을 닫으려면 메시지 오른쪽 상단의 ✕ 버튼을 클릭하세요.
- 화면에 표시된 모든 팝업 알림을 닫으려면 **전체 알림 닫기**을 클릭하세요.

알림 내역 확인하기

1. 프로젝트를 선택해 진입한 화면의 가장 위에 🔔 아이콘을 클릭하세요.
2. 실시간 알림 창이 나타납니다.
 - 현재 프로젝트의 최근 24시간 동안의 알림을 최대 100개까지 확인할 수 있습니다.
 - 개별 이벤트 항목을 선택하면 관련 메뉴로 이동합니다.
 - 실시간 알림 창의 시간별 차트에서 원하는 시간대를 선택하면 해당 이벤트 항목으로 이동할 수 있습니다.



- 전체 알림 내역을 확인하려면 **전체 알림 기록** 버튼을 선택하세요. **경고 알림 > 이벤트 기록** 메뉴로 이동합니다.

❗ **실시간 알림** 목록이 비어 있을 경우, [전체 알림 기록] 버튼이 표시됩니다. 수신 태그 미설정 알림 받기 옵션을 해제하세요.

이벤트 일괄 해소하기

실시간 알림 목록에서 진행 중인 모든 이벤트를 일괄 해소합니다. 이벤트 해소 작업 완료까지 약 30초에서 1분 정도 소요됩니다.

- **이벤트 일괄 처리** 기능을 사용하면 현재 진행 중인 이벤트에 대한 해소 알림이 다량 발생할 수 있습니다.
- **이벤트 일괄 처리** 기능을 사용한 후에도 이벤트 규칙이 활성화되어 있고, 데이터가 임계치를 초과했다면 이벤트는 다시 발생할 수 있습니다.
- 이벤트 해소 알림은 **경고 알림 > 이벤트 설정** 메뉴에서 이벤트 수정을 통해 비활성화할 수 있습니다. **이벤트 상태가 해소되면 추가 알림 또는 해소된 알림** 옵션을 비활성화하세요.

사용 방법:

1. 프로젝트를 선택해 진입한 화면 상단의 🔔 아이콘을 클릭하세요.
2. 실시간 알림 창이 나타나면 오른쪽 상단의 ⏸ 아이콘을 클릭하세요.

3. 실시간 알림 목록에서 진행중인 이벤트를 일괄 해소합니다. 메시지 창이 나타나면 [해소] 버튼을 클릭하세요.

실시간 알림 설정하기

1. 프로젝트를 선택해 진입한 화면 상단의 🔔 아이콘을 클릭하세요.
2. 실시간 알림 창이 나타나면 오른쪽 상단의 ⚙️ 아이콘을 클릭하세요.
3. 실시간 알림 설정 창에서 각 항목을 설정하세요.
 - 팝업 알림: 실시간 알림 창이 닫힌 상태에서도 알림을 팝업 형태로 제공합니다.
 - 해소된 이벤트 보기: 실시간 알림 목록에서 해소된 이벤트를 포함해 확인할 수 있습니다.
 - 알림음 미리 듣기: 브라우저에서 발생하는 알림음을 미리 들을 수 있습니다. Critical 또는 Warning 옆의 🔊 버튼을 클릭하세요. 알림음이 들리지 않으면 브라우저 설정을 확인하시기 바랍니다.

시스템 이벤트

와탭 모니터링은 플랫폼 전반에서 자동으로 탐지 및 생성되는 공용 이벤트를 제공합니다. 이 문서는 시스템에 의해 발생하는 이벤트의 유형 및 발생 조건, 대응 방법에 대해 안내합니다.

EVENT_BLOCKED_BY_SYSTEM

프로젝트에서 짧은 시간에 과도한 이벤트가 발생하면, 와탭 시스템이 이를 탐지하여 이벤트를 차단하고 다음 메시지를 사용자에게 전달합니다. 이벤트가 차단되었다면 사용자의 이벤트 설정을 점검하세요.

 위험



이벤트 메시지

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

프로젝트 번호	8
프로젝트 이름	new server
대상	server agent
이벤트 이름	EVENT_BLOCKED_BY_SYSTEM
발생 시각	(GMT+0900) 2024-11-15 18:24:15

와탭에 로그인하기

new server 프로젝트의 server agent에서 과도한 이벤트가 탐지되어 이벤트가 차단됩니다. server agent에 일정 기간 이벤트가 발생하지 않으면 자동으로 차단 해제됩니다.

차단 기준

이벤트를 차단하는 기준은 다음과 같습니다.

1. 에이전트 단위 차단

한 개의 에이전트에서 1분 내에 10개의 이벤트가 발생하면 해당 에이전트에서 발생하는 이벤트를 차단합니다.

2. 다중 에이전트 차단 시 전체 차단

1의 경우로 이벤트가 차단된 에이전트가 1분 내에 3개 이상이 되는 경우 프로젝트 전체에서 발생하는 이벤트를 차단합니다.

3. 프로젝트 단위 차단

한 개의 프로젝트에서 1분 내에 100개의 이벤트가 발생하면 프로젝트 전체에서 발생하는 이벤트를 차단합니다.

해제 방법

시스템에 의해 이벤트가 차단된 경우, 1분 동안 대상 에이전트 또는 프로젝트에서 이벤트가 발생하지 않아야 합니다.

- 경고 알림 > 이벤트 설정 메뉴에서 설정한 이벤트를 모두 비활성화하세요. 이벤트 설정을 점검하여 과도한 이벤트가 발생하지 않도록 임계치를 조정해야 합니다.
- 이벤트를 설정하기 전 시뮬레이션 기능을 활용해 이벤트 발생 횟수를 예측해볼 수 있습니다.