

Network Management System

release date. 2026. 09. 11.



Table of Contents

• Network管理システム	5
◦ 始める	9
◦ インストール	
▪ サポート環境	11
▪ マネージャーのインストール	17
◦ ネットワークインサイト	
▪ トポロジー	21
▪ デバイス Overview	28
▪ グループナビゲーター	31
▪ Flexボード	37
▪ Flexボードの使用法	40
▪ ウィジェットの管理	51
◦ デバイスの状態	
▪ インターフェース状態	56
▪ デバイス推移	58
▪ ヘルスチェックステータス	66
◦ デバイス管理	
▪ デバイスインベントリ	70
▪ グループ管理	75
◦ Network自動化	
▪ タスク設定	79
▪ タスク状況	84
▪ 設定変更履歴	87
▪ 予防点検プロファイル	90

▪ 予防点検ルール.....	94
▪ 予防点検レポート	97
◦ SNMP OID管理	100
◦ アラート通知.....	101
▪ イベント設定	0
▪ メトリクス	107
▪ 複合メトリクス	128
▪ リアルタイムログ.....	135
▪ 複合ログ	147
▪ 通知設定	161
▪ イベント通知フォーマット	183
▪ イベント履歴	191
▪ リアルタイムアラート	199
▪ システムイベント.....	202
◦ ◇◇	
▪ 使用量分析.....	204
◦ Log Monitoring.....	209
◦ デバイス資産管理	0
◦ 設定	
▪ SNMP Trap設定	0
▪ Syslog設定.....	0
▪ General Config	0
◦ 分析	
▪ ◇◇◇◇◇	0
◦ 管理	

■ マネージャー情報	0
------------------	---

ネットワーク管理システム

ネットワーク管理システム（Network Management System、以下NMS）は、ルーター、スイッチ、サーバー、ファイアウォール、無線APなどのネットワーク機器を中央で統合監視し、性能と安定性を維持するシステムです。トラフィック、機器状態、帯域幅使用量などをリアルタイムで確認し、障害発生時に原因を迅速に把握できます。

NMSは障害予防と問題検知に重点を置き、性能低下を最小化し、安定したサービス品質（QoS）を保証します。WhaTap NMSを使用すると、ITインフラを効率的に運用し、ビジネス継続性を維持できます。

主な特長

- 広範囲なマルチベンダー対応

標準プロトコルであるSNMPをベースに、特定メーカーに限定されない強力な互換性を提供します。Cisco、Juniperなどのグローバルベンダーから国産機器まで、SNMPに対応するすべてのネットワーク機器をWhaTap NMS一つで統合管理できる柔軟な運用環境を支援します。

- 効率的なMIB管理とデータ照会

直感的なMIB（Management Information Base）ブラウザを内蔵し、各ネットワーク機器が提供する膨大なデータを簡単に確認・検証できます。特に、システムでデフォルトで提供されない特定メーカーのプライベートMIBや新規機器のMIBファイルが必要な場合、ユーザーが直接ファイルをアップロードして管理できる機能を支援します。

- OIDリストの提供

運用現場で活用頻度の高いコアOID（Object Identifier）項目を体系的に選別し、リスト形式で提供します。管理者が複雑なMIB構造内で個別OIDを直接探索・検証する手間を最小化し、機器およびインターフェース別しきい値設定に必須の性能指標を迅速に識別・適用できるよう支援することで、管理最適化と運用効率性を最大化します。

- 柔軟なインストール環境とハイブリッドインフラ対応

多様なオペレーティングシステム（OS）に対応し、インストール環境の制約を最小化しました。オンプレミスとクラウドなど、お客様のインフラ環境に最適化された構築方式を提供します。これにより、閉鎖的な内部ネットワークだけでなく、複雑なハイブリッドクラウド環境でも中断のない監視体制を構築でき、企業のセキュリティポリシーとネットワーク構造に最適化された柔軟な配置モデルを支援します。

主な機能

- 機器と性能のリアルタイム監視 (SNMP Polling)

ネットワーク機器のコア稼働指標と性能データを定期的に収集し、最適な運用状態を維持します。CPU負荷、メモリ使用量、セッション占有率などのハードウェアリソースの状態を精密に監視し、インターフェース別データ流入・流出量 (Throughput) とポートの物理的接続状態 (Link Up/Down) をリアルタイムで把握することで、ネットワーク性能のボトルネック現象を事前に防止します。

- 階層構造とトポロジマップ (Hierarchy & Topology)

ネットワーク資産の所属関係と接続状態を視覚化し、管理の直感性を提供します。機器を地域、建物、業務サービス単位のツリー構造で体系化して管理する一方、機器間の物理的・論理的接続関係をトポロジマップで実装することで、全体的なネットワーク構成と障害発生時の影響範囲を即座に把握できます。

- 可用性と品質チェック (Health Check)

ネットワーク機器と運用サービスが正常に動作しているかを応答性に基づいて常時チェックします。ICMP (Ping) およびTCPプロトコルを通じて機器のリアルタイム生存状態 (Alive) を確認し、応答時間 (RTT) とネットワーク遅延変動 (JITTER) 数値を分析することで、ユーザーサービス品質 (SLA) が低下しないよう管理します。

- リアルタイムイベントとログ管理

機器から発生するSNMP TrapとSyslogメッセージをリアルタイムで分析し、障害状況を管理者に即座に伝達します。保存されたイベント履歴に基づいて特定時点の障害原因を精密に検索・追跡できる分析環境を支援します。

- 自動検出 (Auto Discovery)

複雑で膨大なネットワーク環境を一つ一つ手動で登録する手間なく、システムが自ら識別します。SNMPプロトコルを活用してネットワーク内の機器をスキャンし、機器タイプとインターフェース構成、詳細仕様情報を自動的にデータベース化することで、初期構築時間を短縮します。

データ収集範囲

**WhaTap NMS (Network Management System) **は、次のようなネットワークデータ収集方式に対応しています。

- SNMP Polling

ネットワーク機器の状態と性能データを定期的に要求して収集し、`SNMP v1/v2c/v3` プロトコルをすべて対応しま

す。

- **SNMP Trap**

ネットワーク機器から発生するイベントと通知情報を収集・処理し、`SNMP Trap v1/v2c/v3` プロトコルに対応します。

- **Syslog**

ネットワーク機器から生成されるログデータを収集し、リアルタイムで分析します。

- **ICMP**

ICMPプロトコルを使用して機器の**Alive**、**RTT**、**Jitter**などを測定します。

- **TCP**

TCPポートをベースに機器またはサービスの**Alive**と**RTT**などを測定します。

マネージャー主要サービス

NMSはマネージャーでエージェントデータを収集・精製し、WhaTap連動前の事前設定とテストを実行します。

Web-based Management Console & APIs

`uvicorn.service` は管理UIおよびAPIサービスで、NMS設定管理、システム状態確認、設定バックアップ・復旧などの運用管理機能全般をローカル環境で提供します。

❗ 一般的にNMS運用時、マネージャーへのアクセスは必要ありません。アクセスが必要な場合は、WhaTap技術チームにお問い合わせください。

- **使用ポート**：HTTP 5000、HTTPS 8443（設定時）

- **サービスの起動と停止**：次のコマンドで `uvicorn.service` を起動、停止、または再起動できます。

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

NMSエンジン

`nmscore.service` は、ネットワーク管理システム（NMS）のエンジン役割を果たすサービスです。ネットワーク機器とトラフィック監視、管理、イベント処理機能を提供します。

- 使用ポート：
 - **SNMP Polling** : UDP 161 (default)
 - **SNMP Trap** : UDP 162 (default)
 - **Syslog** : UDP 514 (default)
- サービスの起動と停止：次のコマンドで `nmscore.service` を起動、停止、または再起動できます。

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

Health Check

`icmptcphealthd.service` は、ネットワーク機器を対象にICMPおよびTCPベースのHealth Checkを実行し、定期的な状態チェックを通じて機器の可用性と接続状態を継続的に監視します。

- サービスの起動と停止：次のコマンドで `icmptcphealthd.service` を起動、停止、または再起動できます。

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


始める

WhaTapモニタリングを開始するために必要な手順を案内します。

[Step 1. 会員登録](#)

[Step 2. 製品を選択](#)

[Step 3. プロジェクトを作成](#)

サポート環境を確認した後、[マネージャーのインストール](#) 手順に進んでください。

Step 1. 会員登録

WhaTapモニタリングサービスを利用するには、まず[会員登録](#)が必要です。会員登録の詳細については、[アカウント管理 > 会員登録](#)文書を参照してください。

Step 2. 製品を選択

1. [WhaTapモニタリングサービス](#)にログインします。
2.  **プロジェクト全体** > **+** **Project** ボタンをクリックします。
3.  **商品選択**画面で、モニタリングする製品の**作成する**ボタンをクリックしてください。

Step 3. プロジェクトを作成

モニタリングする製品を選択したら、エージェントをインストールする前にまずプロジェクトを作成します。

1.  **プロジェクト作成**画面で、プロジェクトを作成するには次の項目を入力または選択してください。
 - **プロジェクト名**（必須）：プロジェクトの名前を入力します。
 - **データサーバーリージョン**（必須）：データサーバーが位置するリージョン（地域）を選択します。リージョンはクラウドサービスを提供するデータセンターの集まりです。選択したリージョンにユーザーのデータが保存されます。

- **プロジェクトタイムゾーン（必須）**：通知とレポート作成時の基準となる時間を設定します。
- **通知言語の設定（必須）**：プロジェクトで発生する警告通知メッセージの言語を設定します。（韓国語、英語対応）
- **プロジェクトグループ**：複数のプロジェクトをグループにまとめて管理できます。所属するグループがあれば選択してください。ない場合は、グループ追加ボタンをクリックしてグループを追加できます。
- **プロジェクト説明**：プロジェクトに関する追加説明を入力します。

2. すべての設定を完了したら、**プロジェクトを作成する**ボタンをクリックしてください。

① 組織を選択した状態でプロジェクトを追加する場合、**組織下位のグループ**を必須で設定する必要があります。グループの詳細については、[次の文書](#)を参照してください。

サポート環境

WhaTap Network Control Management Systemは、Standalone方式で単独の仮想マシン（VM）にインストールされます。これにより、ネットワーク管理システムが独立して動作し、ネットワークモニタリングおよび管理に必要なすべての機能を安定的に提供します。

システム要求仕様

WhaTap Network Management Systemの安定した性能を保証するための推奨最小仕様です。

項目	仕様
CPU	4core（最小2core）
Memory	最小16GB以上（最小8G）
Disk	50G以上SSD推奨（最小30G）
Network Interface	1Gbps以上

OS別対応

OS	Pythonバージョン	対応状況
Ubuntu 22.04	3.10	対応、推奨
Ubuntu 23.04	3.11	対応
Ubuntu 24.04	3.12	対応
Rocky 9.4	3.9	対応、推奨

OS	Pythonバージョン	対応状況
Rocky 8.10	3.11	対応
Redhat 8.10	3.11	対応、推奨

Pythonバージョン別対応

OS種類に関係なく、Pythonバージョンに応じて対応可能です。ただし、できるだけ推奨OSの使用を推奨します。

系列	対応Pythonバージョン
Debian系列	Python 3.10、3.11、3.12
Redhat系列	Python 3.9、3.10、3.11、3.12

使用TCP/UDPポート

明記されたTCP、IPポート番号は、該当サービスが使用するデフォルトポートであり、お客様の環境に合わせて変更できます。

区分	TCP	UDP	説明	方向	その他
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	デフォルトhttp、https使用时8443ポート 許可が必要
whatap 収集	6600	-	データ転送	Outbound	-

区分	TCP	UDP	説明	方向	その他
サーバー					
ICMP	-	-	ICMP health Check	-	ICMPプロトコル許可が必要
TCP	-	-	TCPベースhealth Check	In/Out	モニタリング対象TCPポート番号接続許可が必要 (Options)

サービス提供形態

WhaTapモニタリングは、SaaSまたはオンプレミス（インストール型）方式でご利用いただけます。どちらを選択しても、同じエージェントで同じモニタリング機能をご利用いただけます。

Deployment	Support	Description
SaaS		WhaTapが運用する収集サーバーに接続。リージョン別アドレスはファイアウォール項目を参照
オンプレミス（インストール型）		収集サーバーを自社で構築して運用（閉域網環境に対応）。導入範囲は営業担当者と協議

❗ インターネットに接続しない閉域網環境でも、オンプレミスで構築できます。

提供形態による機能の違い

どの形態を選択しても、モニタリング機能は同じです。モバイルアプリのみが例外で、service.whatap.io SaaSでのみご利用いただけます。

❗ オンプレミス環境で一部の機能をご利用いただくには、別途契約が必要です。

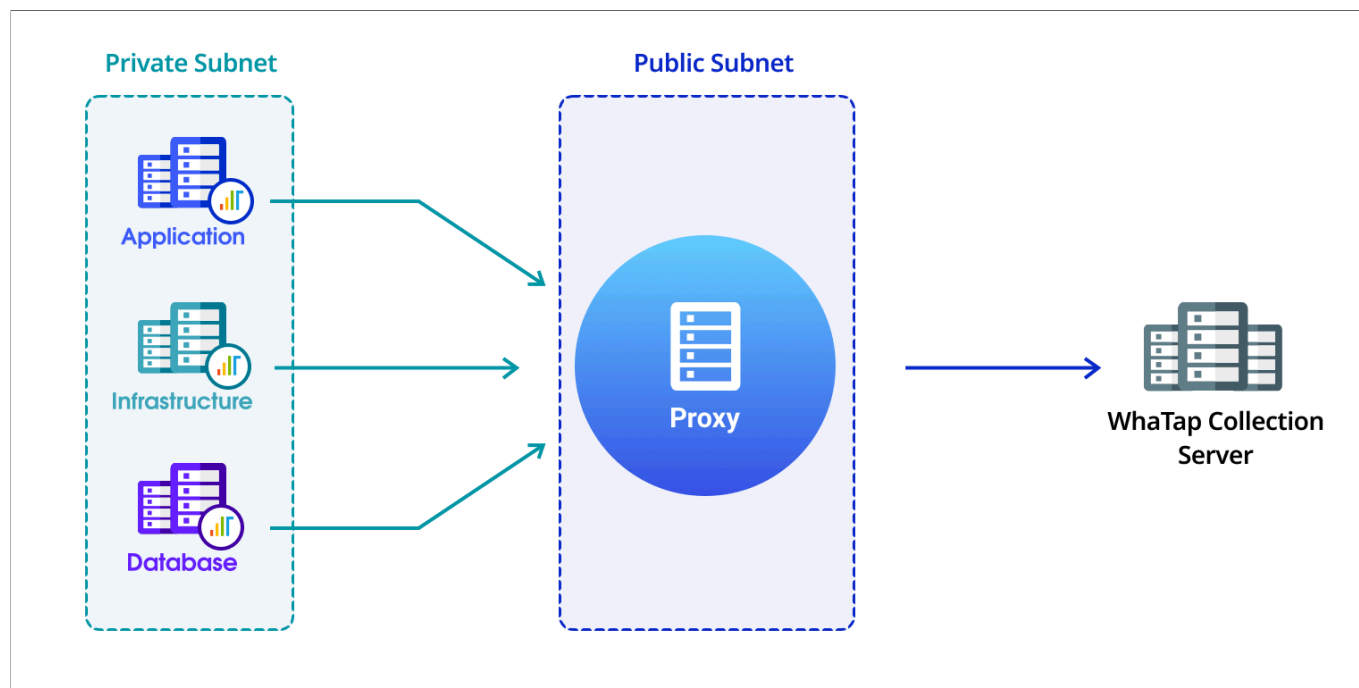
ファイアウォール

WhaTap エージェントは、収集サーバーの **TCP 6600** ポートにアクセスする必要があります。監視対象に最も近い収集サーバーのアドレスを許可してください。

出発地：WhaTapエージェント

クラウド	目的地	目的地IP	ポート番号
AWS	WhaTapソウル収集サーバー	13.124.11.223 / 13.209.172.35	TCP 6600
	WhaTap東京収集サーバー	52.68.36.166 / 52.193.60.176	TCP 6600
	WhaTapシンガポール収集サーバー	18.138.0.93 / 18.139.67.236	TCP 6600
	WhaTapジャカルタ収集サーバー	108.136.91.69 / 108.137.158.44	TCP 6600
	WhaTapタイ収集サーバー	43.209.109.219 / 43.209.48.86	TCP 6600
	WhaTapムンバイ収集サーバー	13.127.125.69 / 13.235.15.118	TCP 6600
	WhaTapカリフォルニア収集サーバー	52.8.223.130 / 52.8.239.99	TCP 6600
	WhaTapバージニア収集サーバー	107.23.220.101 / 54.236.221.105	TCP 6600
	WhaTapフランクフルト収集サーバー	3.125.142.162 / 3.127.76.140	TCP 6600
Azure	WhaTapソウル収集サーバー	52.231.66.38 / 20.194.5.115	TCP 6600
	WhaTap東京収集サーバー	52.246.169.54 / 20.210.27.232	TCP 6600
Kakao	WhaTapソウル収集サーバー	61.109.237.237 / 61.109.238.166	TCP 6600

エージェントから収集サーバーに直接接続できない場合は、提供するProxyモジュールを使用して経由します。



主要サービス構成要素とポート

NMS Control Manager Web-Based U/I

`uvicorn.service` は、ローカル環境で実行される管理UIおよびAPIサービスで、NMS設定管理、システム状態確認、設定バックアップ・復旧などの運用管理機能全般を提供します。

- 使用ポート：HTTP 5000、HTTPS 8443（設定時）
- サービスの起動と停止：次のコマンドで `uvicorn.service` を起動、停止、または再起動できます。

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

❗ マネージャーアクセス情報は、WhaTap技術チームにお問い合わせください。

NMSエンジン

`nmscore.service` は、ネットワーク管理システム（NMS）のエンジン役割を果たすサービスです。ネットワーク機器とトラフィック監視、管理、イベント処理機能を提供します。

- 使用ポート：
 - **SNMP Trap** : UDP 162 (default)
 - **Syslog** : UDP 514 (default)
- サービスの起動と停止：次のコマンドで `nmscore.service` を起動、停止、または再起動できます。

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

Health Check

`icmptcphealthd.service` は、ネットワーク機器を対象にICMPおよびTCPベースのHealth Checkを実行し、定期的な状態チェックを通じて機器の可用性と接続状態を継続的に監視します。

- サービスの起動と停止：次のコマンドで `icmptcphealthd.service` を起動、停止、または再起動できます。

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


マネージャーのインストール

WhaTap NMS(Network Management System) エージェントであるNMS Managerのインストール方法を案内します。インストールを進める前に、以下の事項を必ず確認してください。

- ❗ マネージャーのインストール前に、WhaTap会員登録とプロジェクト作成が完了している必要があります。詳細は[始める](#)文書を参照してください。
 - システム要求事項は、[サポート環境](#)文書で確認できます。

マネージャーのインストール

プロジェクトアクセスキーの確認

アクセスキーは、WhaTapサービスを有効にするための固有IDです。アクセスキーを自動的に発行された後、次の手順を進めます。

1. インストールガイドセクションで、**プロジェクトアクセスキーの発行**ボタンをクリックしてください。
2. 発行されたアクセスキーを**コピー**ボタンをクリックしてコピーします。アクセスキーは再確認できます。

- ✔ プロジェクトを作成すると、自動的に**エージェントインストール**ページに移動します。エージェントインストールページに移動しない場合は、画面左側のメニューから**管理 > マネージャーのインストール**を選択してください。

インストールコマンドの実行

管理 > マネージャーのインストールガイドセクションで、プロジェクトアクセスキーを確認した後、順番に該当するOSに合わせてインストールを進めてください。

Red Hat-based Linux

❗ WhaTap Network Management Systemは、Rocky、Redhat Linux環境に対応しています。

1. 次のコマンドを実行して、WhaTap リポジトリを登録してください。

```
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. 次のコマンドを実行して、パッケージをインストールしてください。

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

3. 次のコマンドを実行してください。アクセスキーを入力し、WhaTapサーバーホストを設定します。

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

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

Whatap-nms access key manager tool

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

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

4. インストール完了後、次のコマンドを実行してNMSマネージャーが正常に実行されているか確認してください。

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

Debian-based Linux

❗ WhaTap Network Management Systemは、Ubuntu環境に対応しています。

1. 次のコマンドを実行して、WhaTap リポジトリを登録してください。

```
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. 次のコマンドを実行して、パッケージをインストールしてください。

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

3. 次のコマンドを実行してください。アクセスキーを入力し、WhaTapサーバーホストを設定します。

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

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

Whatap-nms access key manager tool

optional arguments:

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

-a LICENSE, --accesskey LICENSE

Access key for project

-s HOST, --server HOST

Whatap host ip address for data transfer

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

example:

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

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

4. インストール完了後、次のコマンドを実行してNMSマネージャーが正常に実行されているか確認してください。

```
sudo service uvicorn status
```

```
sudo service nmscore status
```

```
sudo service icmptcphealthd status
```

NMSサービスへのアクセス

インストールが完了したら、<https://service.whatap.io>にアクセスしてNMSモニタリングを開始します。

トポロジー

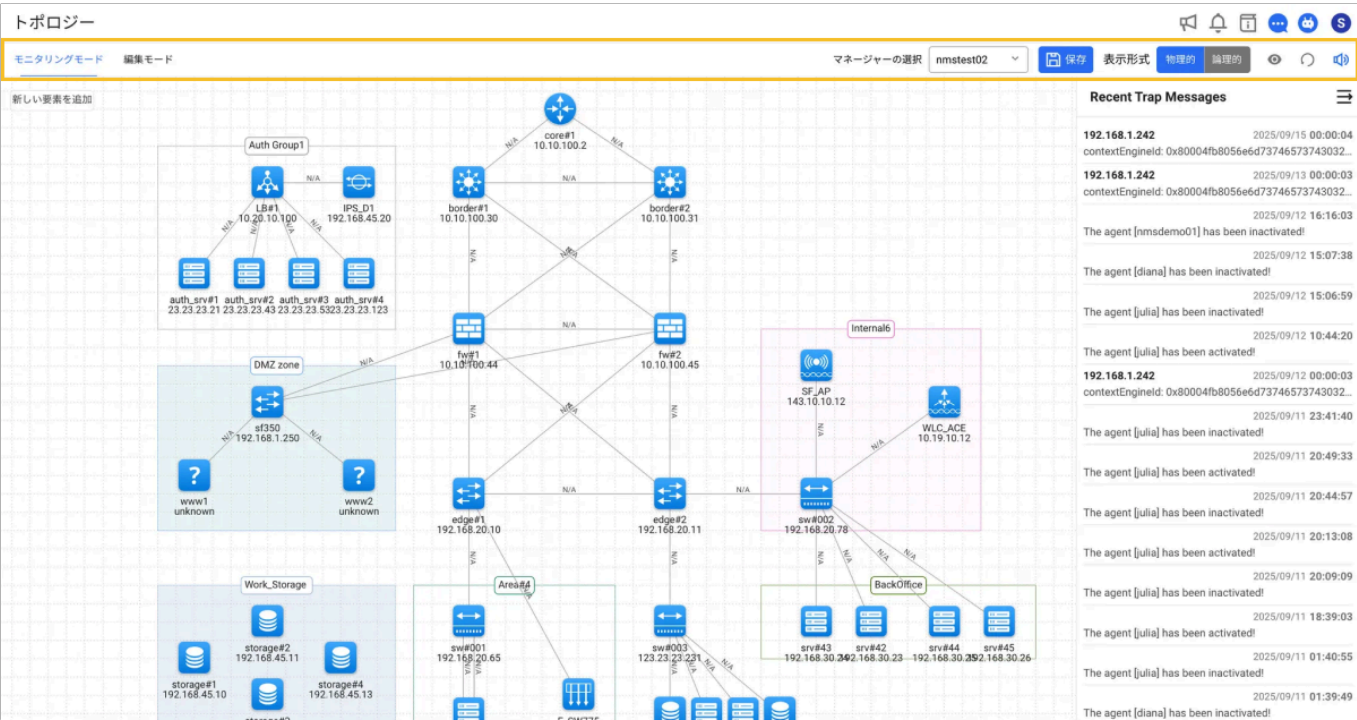
ネットワークインサイトのトポロジーは、ネットワーク機器とリンク構造を視覚的に表示します。

単に構造を見るだけでなく、リンクダウンなどリアルタイムで発生するイベントが即時に反映されるため、管理者はネットワーク状態を素早く把握できます。トポロジーは2つのモードを提供します。

- ・ **モニタリングモード**: ネットワーク全体構造を確認し、リアルタイムイベントを監視する閲覧モード
- ・ **編集モード**: 領域の作成、ノードの追加・削除・編集、リンク接続の機能を提供して画面レイアウトを管理

基本画面と設定

トポロジー画面上部では、モード切替、マネージャー選択、表示形式変更など主要な制御機能を利用できます。



メニュー	説明
モード選択	モニタリングモード または 編集モード タブを選択

メニュー	説明
	- モニタリングモード: ネットワーク全体構造を確認し、リアルタイムイベントを監視 - 編集モード: 領域を作成したり、ノードの追加・削除・編集、リンク接続の機能を提供
マネージャー選択	接続された NMS マネージャーを選択
 保存	ユーザーが調整した機器および領域位置を保存
表示形式	物理 または 論理 トポロジーに切替 - 物理: 実際に機器間で接続されたすべてのポートを確認 - 論理: 機器間の論理的な接続構造を中心に確認
	ノード IP 表示の有無を選択
	すべての画面設定を初期値に戻す
	ON / OFF でトポロジーに異常があるときサウンドで通知するかを設定

Topology Map アイコン

アイコン	ノードタイプ	説明
	Router	ネットワークトラフィックを他のネットワークにルーティングする機器
	L3 Switch	Layer 3 スイッチ、ルーティング機能を持つスイッチ
	L2 Switch	Layer 2 スイッチ、VLAN 等のデータリンク層機器
	Firewall	ネットワークトラフィックをフィルタリングするセキュリティ機器
	Load Balancer	トラフィックを複数のサーバーに分散するロードバランサー
	Hub	シンプルなネットワーク分配機器（非インテリジェント）

アイコン	ノードタイプ	説明
	IPS	侵入防止システム (Intrusion Prevention System)
	WAF	Web アプリケーションファイアウォール (Web Application Firewall)
	WLC	無線 LAN コントローラー (Wireless LAN Controller)
	Access Point	無線アクセスポイント
	Server	サービスやデータを提供するサーバー
	Storage	データ保存機器 (NAS、SAN 等)
	IP Phone	VoIP ベースの音声通話機器
	Appliance	特定目的のネットワーク機器 (例: Proxy、UTM 等)
	Unknown	分類されていない、または未確認の機器

共通機能

- ・ パン: 画面の空白部分をドラッグして移動
- ・ ズームイン/ズームアウト: マウスホイールで拡大・縮小

モニタリングモード

モニタリングモードでは、ネットワーク構造をリアルタイムで確認し、イベント変化を即座に把握できます。

1. ネットワークインサイト>トポロジー に移動します。
2. モニタリングモード タブをクリックし、メイントポロジービューと Recent Trap Messages を確認します。

メイントポロジービュー

- ネットワーク機器はアイコンで表示されます。ルーター・スイッチ・ファイアウォールなど機器タイプによってアイコンの形が異なります。
- 機器間の接続は線で表示され、状態によってスタイルが変化します。
 - 正常（灰色の実線）
 - Throughput がある場合、SNMP 設定を通じてアニメーションでデータフローが表示されます。SNMP 設定が必要です。
 - リンクダウン（赤色の実線）
- 機器の電源がオフになるか、ネットワークから切断されると、警告アイコン（)が表示され、状態を即座に確認できます。
- 領域を分けて機器をグループ化するカスタム機能を提供します。

Recent Trap Messages

画面右側のパネルに、収集された Trap メッセージがリアルタイムで順次表示されます。機器やリンクのイベントをテキストログ形式で確認できます。

- 例: 特定リンクダウン、機器の有効化または無効化

編集モード

編集モード タブでノードの追加/編集、領域の追加/編集、リンクの追加/編集ができます。

1. ネットワークインサイト > トポロジー に移動します。
2. 編集モード タブをクリックし、画面右側で希望のモードを選択して編集します。
 -  Topology Edit: 修正モード
 -  Add Device: 機器追加モード
 -  Add Area: 領域追加モード
 -  Add Link: リンク追加モード

修正モード

修正モードでは、配置された要素を編集できます。

- ノードと領域をドラッグして位置を変更できます。
- 要素をクリックするとプロパティを編集できます。

領域の編集

作成された領域のプロパティを編集できます。

- 領域の背景色と枠線色を変更して視覚的に区別しやすくなります。
- 領域名は  アイコンをクリックして入力または変更します。
- 不要な領域は  削除 ボタンをクリックして削除します。

ノードの編集

ネットワーク機器（ノード）を選択すると、名前とデバイスタイプを編集できます。

- ネットワークノード情報は  アイコンをクリックして入力または変更します。
- ノードを削除する場合は  削除 ボタンをクリックして削除します。
- 提供されるデバイスタイプ: router, switch, hub, host, ap, phone, firewall, unknown

機器追加モード

機器追加モードでは、トポロジーにノードを追加できます。機器タイプを選択後、トポロジーの空白部分をクリックしてノードを追加できます。

領域追加モード

領域追加モードでは、トポロジーに新しい領域を追加できます。トポロジーの空白部分をドラッグして新しい領域を追加します。

リンク追加モード

リンク追加モードでは、ノードとノードを接続できます。ノードを1つクリックした後、別のノードをクリックするとリンクを接続できます。

編集履歴

上段オプションバー右側の編集履歴では、編集ツールで実行した作業を元に戻したり、再度適用したりできます。

Item	Description
元に戻す	直前の編集作業を取り消し。ショートカットキー <code>Ctrl+Z</code>
やり直し	取り消した作業を再適用。ショートカットキー <code>Ctrl+Shift+Z</code> または <code>Ctrl+Y</code>

元に戻す作業がない場合、各ボタンは非活性状態で表示されます。

- 元に戻せる作業：領域の追加・編集・削除、ノードと領域のドラッグ移動およびサイズ変更、ページガイドの追加・移動・削除
- 元に戻せない作業：ノードとリンクの追加・修正・削除（保存時にサーバーへ即時反映）、画面移動と拡大・縮小

❗ 編集履歴は最大50段階まで保管し、ドラッグ中は動作しません。短時間に連続して発生した同一対象の変更は、1段階にまとめられます。

自動巡回再生バー

トポロジーを複数の区画に分けた場合、自動巡回再生バーが表示されます。再生バーでは、区画間の移動と自動巡回をあわせて制御できます。

Item	Description
ページ表示	区画数と現在位置を表示。項目を選択するとその区画へ即座に移動

Item	Description
再生・停止	自動巡回の開始・停止。アイコン右上に現在の間隔（秒）が表示される
間隔選択	自動巡回の間隔を選択。プリセットは3・5・10・30秒で、直接入力1秒から120秒まで
進行バー	次の区画へ移動するまでの残り時間を表示

再生バーは、区画が2つ以上の場合にのみ表示されます。

デバイス Overview

デバイス概要は **共通オプション** と **ウィジェット** で構成されたダッシュボードで、プロジェクト内のネットワークデバイスの状態や性能指標を一目で確認できます。管理者はインターフェース状態、トラフィック処理状況、HealthCheck、Syslog、Trap イベント、リアルタイムログなどの主要運用データをウィジェット形式で確認できます。

ⓘ デバイスダッシュボードは、リアルタイムモニタリング専用画面で、過去の特定時点を選択して照会する機能を提供しません。

共通オプション

Overview 画面全体に共通適用される機能で、データ参照範囲、マネージャ選択、ウィジェット配置保存などを設定できます。

- **プリセット選択:** 保存されたウィジェット配置を呼び出し、同じレイアウトで使用
- **プリセット保存:** 現在の画面構成を保存し、後で再利用可能
- **ウィジェット管理:** ウィジェットの追加、削除、配置変更、サイズ調整が可能
 - **ウィジェット削除:** 削除するウィジェットを右クリックし、表示される **削除** ボタンで削除
 - **ウィジェット追加:** ウィジェットのない空白部分を右クリックし、追加したいウィジェットを選択

ウィジェット

ダッシュボードに表示される様々なウィジェットを通じて、ネットワーク状態を直感的に確認できます。

デバイス状態

使用中のインターフェース数(**Connected**) / 全体インターフェース数(**Total Interfaces**)として表示され、デバイスで有効になっているインターフェース数を確認できます。デバイスにマウスオーバーすると状態情報が表示され、デバイスをクリックするとインターフェース情報がある場合は **インターフェース状態** に、ない場合は **使用状況** に移動します。

- 例: 8 / 22 → 全 22 個のうち 8 個が有効

❗ インターフェース情報は SNMP の ifTable(1.3.6.1.2.1.2.2) または ifXTable(1.3.6.1.2.1.31.1.1) データを収集する必要があります。機器によっては未対応または異なる場合があります。

HealthCheck

HealthCheck ウィジェットはネットワークジッタと最大往復時間 (Max RTT) をグラフで表示します。状態が異常な場合、対象 IP アドレスを **赤色** で表示します。モニタリング結果は直近 10 分単位で更新されます。

1. デバイスインベントリに移動し、設定するデバイスの  をクリックします。
2. デバイス設定画面の **Health Check** タブで設定できます。

本日の Syslog

本日発生した Syslog イベントは重大度別に円グラフで表示され、Emergency から Debug までのレベルに分類されます。これによりログの頻度と重大度の分布を直感的に確認できます。

Trap 発生量 TOP 10

直近 24 時間で Trap メッセージが最も多く発生したデバイスを表示し、イベント発生頻度順に降順で並び替えます。これによりイベントが集中する機器を素早く把握できます。

最大 Throughput インターフェース

直近 24 時間で最大 Throughput を記録したインターフェースを表示し、トラフィック量の多い順に降順で並びます。

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

最大 PPS インターフェース

直近 24 時間で最大 Packets Per Second (PPS) を記録したインターフェースを表示します。

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

リアルタイムログイベント

プロジェクト内で発生したログをリアルタイムテーブルで確認でき、時間、ホスト、ログ内容が表示されます。新しいログは Live tail 形式ですぐに反映されます。リアルタイムでログを分析することで、システム障害や異常兆候を迅速に検知できます。

グループナビゲーター

グループナビゲーターでは、ネットワーク機器とインターフェースを階層構造で探索しながら、パフォーマンス指標をリアルタイムで確認できます。📍 Site → 🏠 Building → 🏢 Floor → 📄 Device → 🌐 Interface の順にドリルダウンし、各段階でその範囲のトラフィック、状態、エラー情報を可視化します。

グループナビゲーターでは、以下の作業でネットワーク状態をリアルタイムにモニタリングできます。

- 目的の場所まで素早く移動
- 各階層のデバイスおよびインターフェースの状態サマリーを確認
- デバイスまたはインターフェースのトラフィック・エラー指標を詳細分析

基本画面と設定

グループナビゲーター画面上部のオプションバーで照会条件を設定し、左パネルでモニタリング対象を選択します。

時間選択

上部オプションバーの**時間選択**で照会時間範囲を設定できます。

LIVEモードは5秒間隔でデータを更新し、最大31日まで照会できます。デフォルトのライブ範囲は1時間です。

マネージャー選択

上部オプションバーの**マネージャー選択**で、データを収集するNMSマネージャーを選択してパフォーマンス指標を確認できます。

Group Selection

Group Selectionパネルはツリー構造で📍 Site → 🏠 Building → 🏢 Floor → 📄 Device → 🌐 Interface の順に階層を探索できます。

項目	説明
— すべて閉じる	ツリー全体を閉じる
+ すべて開く	ツリー全体を開く
☰ / ☲	パネルを閉じる/開く

パス表示 (Breadcrumb)

Breadcrumbナビゲーションが表示されます。選択したノードのパスが上部に表示されます。各パスをクリックして上位レベルに移動できます。

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

ⓘ 現在の選択位置はURLパラメーター（ nodeKey ）として保存され、ブックマークや共有が可能です。

グループレベルサマリー

項目	説明
Devices	選択範囲内の全デバイス数
Interfaces	選択範囲内の全インターフェース数
グループカード	サブグループごとのデバイス/インターフェース数。クリックすると該当グループにドリルダウン

デバイスの状態とトラフィック情報の確認

特定のデバイスを選択すると、そのデバイスに属するインターフェースの状態とトラフィック情報を確認できます。

NMS group-navigator

フィルターオプション

画面右上のHide Logical Interfaces、Hide Unused Interfacesオプションのオン/オフを切り替えられます。

項目	説明
Hide Logical Interfaces	VLAN、Loopbackなどの論理インターフェースをリストから非表示にする。物理ポート（ethernetCsmacd、fastEtherなど）のみ表示
Hide Unused Interfaces	照会期間内にトラフィックがないインターフェースをリストから非表示にする

❗ フィルター設定はブラウザに保存され、次回アクセス時も維持されます。

インターフェースサマリーパネル

項目	説明
Total	全インターフェース数
Link Up	リンクが接続されたインターフェース数
Link Down	リンクが切断されたインターフェース数
Admin Down	管理者が無効化したインターフェース数

❗ 各状態のカウントをクリックすると詳細リストモーダルが表示されます。モーダルで該当状態のインターフェースリストを確認できます。

チャート

チャート名	説明
Peak Throughput Interface (Time Range)	照会期間内に最大トラフィックを記録したインターフェースとその推移。クリックで該当インターフェースに移動
Peak Throughput Interface (Current)	現在時点での最大トラフィックインターフェースとその推移
Total Throughput	デバイス全体のトラフィック推移（ラインチャート）
Throughput (Inbound / Outbound)	インターフェース別のインバウンド/アウトバウンドトラフィック推移。インターフェースごとに色分け（スタックラインチャート）
Inbound by Interface	インターフェース別インバウンドトラフィック比較（横棒グラフ）
Outbound by Interface	インターフェース別アウトバウンドトラフィック比較（横棒グラフ）

Interface Status

カラム	説明
Status	インターフェース状態アイコン（  Connected、  Link Down、  Admin Down、  Unavailable)
Interface	インターフェース名とifIndex
Link Status	リンク接続状態（up/down）
Admin Status	管理状態（up/down）
Inbound	インバウンドトラフィック（Kbps）
Outbound	アウトバウンドトラフィック（Kbps）

カラム	説明
Inbound PPS	1秒あたりのインバウンドパケット数
Outbound PPS	1秒あたりのアウトバウンドパケット数
Utilization	帯域幅使用率 (%)
Error Ratio	エラー率 (%)
Max Link Speed	インターフェース最大速度
Interface Type	インターフェースタイプ (例: ethernetCsmacd)
Last Seen Time	最後のデータ受信時刻

インターフェースのパフォーマンス指標分析

特定のインターフェースを選択すると、そのインターフェースの詳細なパフォーマンス指標を確認できます。

NMS group-navigator

インターフェース情報

項目	説明
ifIndex	インターフェース識別番号
Link Status	リンク状態バッジ (Link Up / Link Down / Admin Down)
Admin	管理状態 (UP/DOWN)
Oper	運用状態 (UP/DOWN)

項目	説明
Speed	インターフェース速度（例: 1Gbps）
Type	インターフェースタイプ（例: ethernetCsmacd）

チャート

チャート名	説明
Throughput (Inbound / Outbound)	インバウンド/アウトバウンドトラフィック時系列グラフ（スタック）
Packets Per Second (In/Out)	1秒あたりのパケット数時系列グラフ
Errors (In/Out)	インバウンド/アウトバウンドエラー発生推移

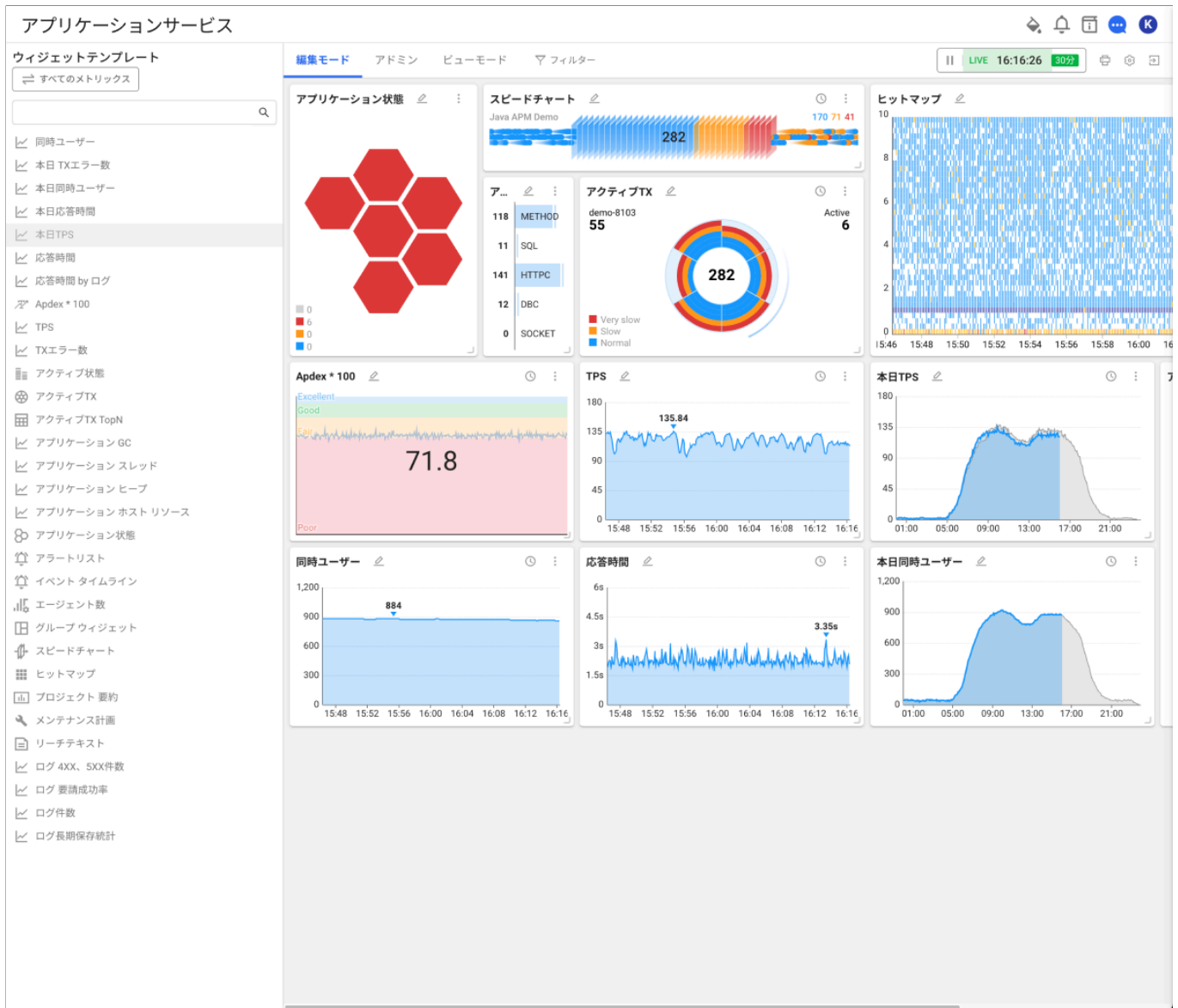
統計カード

区分	項目	説明
Total Throughput	Current / Max / Avg	全トラフィックの現在値、最大値、平均値（Kbps）
Inbound Throughput	Current / Max / Avg	インバウンドトラフィック統計
Outbound Throughput	Current / Max / Avg	アウトバウンドトラフィック統計
PPS In	Current / Max / Avg	インバウンド1秒あたりパケット数統計
PPS Out	Current / Max / Avg	アウトバウンド1秒あたりパケット数統計
Error In	Current / Max / Avg	インバウンドエラー統計
Error Out	Current / Max / Avg	アウトバウンドエラー統計

Flexボード

Flexボードはユーザー定義型の統合ダッシュボードです。アプリケーション、サーバー、データベース、コンテナなどのプロジェクトのデータを使用して、リアルタイムのダッシュボードが作成できます。

事前構成されたテンプレートで初期設定を迅速に完了し、希望する形式のダッシュボードを作成できます。データウィジェットを追加したりプロパティを修正したりして、必要な形式で表示することができ、フィルタリング機能によって監視対象を絞り込むこともできます。時間範囲を指定すれば特定の時点のデータを確認でき、補助チャートを活用することで多様な方法で分析できます。ダッシュボードはお気に入りに登録して簡単にアクセスでき、カスタマイズしたダッシュボードは他のアカウントにコピーして再利用することも可能です。



Flexボードは、次のアクセスパスによってさまざまな用途があります。

- ホーム画面 > 統合Flexボード

- ウィジェットを作成すると、表示可能なすべてのプロジェクトを選択オプションとして提供します。
- ユーザーアカウントにダッシュボードが保存され、他のユーザーにコピーする機能を使用して共有できます。
- 個人アカウントダッシュボードで、権限による影響はありませんが、読み取り専用として共有されたダッシュボードの場合は修正できません。

- ホーム画面 > プロジェクト選択 > **ダッシュボード** > **Flexボード**
 - ウィジェットを作成すると対応するプロジェクトの情報が自動入力されます。
 - プロジェクトメンバーで作成したFlexボードは、自動共有されます。
 - プロジェクト**修正権限**、または**プロジェクトのFlexボードの修正権限**、**Site Admin**権限を持つユーザーが修正できます。

✔ Flexボードの編集権限を持つユーザーは、以下の機能を利用できます。

- ダッシュボードをJSONファイルとしてエクスポート/インポート
- ダッシュボード内のデータリクエストおよびレスポンス内容を確認
- ウィジェット設定オプションをJSON形式で参照および修正

❗ プロジェクト内の**Flexボード**メニューでは、ダッシュボードの変更権限のあるユーザーのみが**編集モード**および**アドミンモード**、**フィルター**機能にアクセスできます。

- アクセス可能なメンバー権限
 - プロジェクト**修正権限**
 - **プロジェクトのFlexボードの修正権限**
 - **Site Admin**権限
- **ビューモード**および**フィルター**機能の詳細については、[次の文書](#)を参照してください。
- メンバー権限の詳細については、[次の文書](#)を参照してください。

Flexボードの使用方法

- 🟢 ダッシュボードはメトリクスウィジェットを含むさまざまなウィジェットテンプレートを活用して構成できます。
- 各テンプレートの特徴と使用方法については、[ウィジェットテンプレート](#) ドキュメントで詳しく確認できます。

事前テンプレートを適用する

事前構成テンプレートで初期設定を素早く進め、必要に応じて修正して活用してください。

1. **Flexボード** メニューを選択します。
2. 左側の **テンプレート** 一覧から使用するテンプレートを選択します。
3. **Flexボード管理** ウィンドウが表示されたら、**名前変更** に希望の名前を入力します。
 - **レイアウト** でウィジェットを選択し、ドラッグして希望の位置へ移動できます。
4. **保存** ボタンをクリックします。選択したテンプレートを基準に Flex ボードを作成します。
 - 作成したボードは **Flexボード** のボード一覧で確認できます。

Flex ボードを作成する

Flex ボードを作成し、ウィジェットを配置して自分だけのダッシュボードを作れます。

1. **Flexボード** で右上の **ダッシュボード生成** ボタンをクリックします。
2. **ダッシュボード生成** ウィンドウが表示されたら、入力ボックスにダッシュボードの **名前** を入力します。
3. ウィジェットの配置方式を選択し、**ダッシュボード生成** ボタンをクリックします。
 - **固定レイアウトFlexボード**: ピクセル基準の自由配置
 - **レスポンシブFlexボード**: ブラウザサイズ基準のグリッドレスポンシブレイアウト

(グリッドを設定してから **ダッシュボード生成** ボタンをクリック)

4. **ウィジェットテンプレート** 選択画面で、ダッシュボードに配置するウィジェットを選択します。

- メトリクスウィジェットを追加する場合は、**ウィジェットテンプレート** の右側にある **すべてのメトリクス** ボタンをクリックします。

- ❗ **ウィジェットテンプレート**: 一般的な監視状況で重要となる指標を要約し、事前定義されたウィジェット一覧から選択できます。
- **すべてのメトリクス**: ユーザーのプロジェクトで収集中のすべてのメトリクスデータを基準にウィジェットを作成します。メトリクスウィジェットの詳細は[次のドキュメント](#)を参照してください。

5. 配置したウィジェットの位置を移動したりサイズを調整します。

- ウィジェット上部で十字カーソルが表示されたら、クリックしたままドラッグして位置を移動します。
- ウィジェット右下で矢印カーソルが表示されたら、クリックしたままドラッグしてサイズを調整します。

6. 追加するウィジェットの配置が完了したら、**ビューモード** を選択してレイアウトを確認します。レイアウトを再編集する場合は、**編集モード** を選択してウィジェット配置を変更します。

7. すべての工程が完了したら、右上の (**リストへ**) アイコンをクリックします。

- **Flexボードのダッシュボードリスト** で作成したボードを確認できます。作成したボードを選択して新しいFlexボードを確認してください。

- ❗ お客様のご要望を反映してダッシュボードテンプレートやウィジェットの追加を検討しています。必要なテンプレートまたはウィジェットがあれば support@whatap.io までご連絡ください。

Flex ボードを編集する

- ❗ **Flex ボード編集権限**



- **ホーム > 統合Flexボード:** 個人アカウントのダッシュボードで権限の影響はありませんが、閲覧専用で共有されたダッシュボードは編集できません。
- **ホーム > プロジェクト選択 > ダッシュボード > Flexボード:** プロジェクトの編集権限、プロジェクトのフレックスボード編集権限、または Site Admin 権限のユーザーが編集できます。

メンバー権限の詳細は[次のドキュメント](#)を参照してください。

1. **Flexボードのダッシュボードリスト**で、 編集アイコンをクリックします。画面右側に **Flex ボード管理** ウィンドウが表示されます。
2. **Flex ボード管理** ウィンドウで、名前、プロジェクト、レイアウト、widget.json、option.json を設定します。
 - **名前変更:** ダッシュボード名を編集します。
 - **プロジェクト:** ダッシュボードのウィジェットがデータを取得するプロジェクトを選択します。



プロジェクト オプションは **ホーム > 統合Flexボード** メニューでのみ設定できます。

統合Flexボード から入った場合は、ウィジェットごとにデータ取得元のプロジェクトを選択できます。

1. ウィジェット右上の ボタンをクリックし、目的のプロジェクトを検索して単一または複数選択します。
2. プロジェクトを選択したら **適用** ボタンをクリックします。

• レイアウト

- ウィジェットをドラッグして位置を移動します。
- ウィジェット右下をマウスでクリックしたままドラッグしてサイズを調整します。
- ウィジェットを削除するには、ウィジェット右上の アイコンをクリックします。
- **ウィジェット.json:** ダッシュボードのウィジェット設定を JSON 形式で読み込みます。 アイコンをクリックすると JSON をコピーします。
- **オプション.json:** ダッシュボードのオプション設定を JSON 形式で読み込みます。 アイコンをクリックすると JSON をコピーします。

Flex ボードを削除する

1. Flexボード>ダッシュボードリスト で、削除する項目の  アイコンをクリックします。
2. 確認メッセージで **削除** ボタンをクリックします。

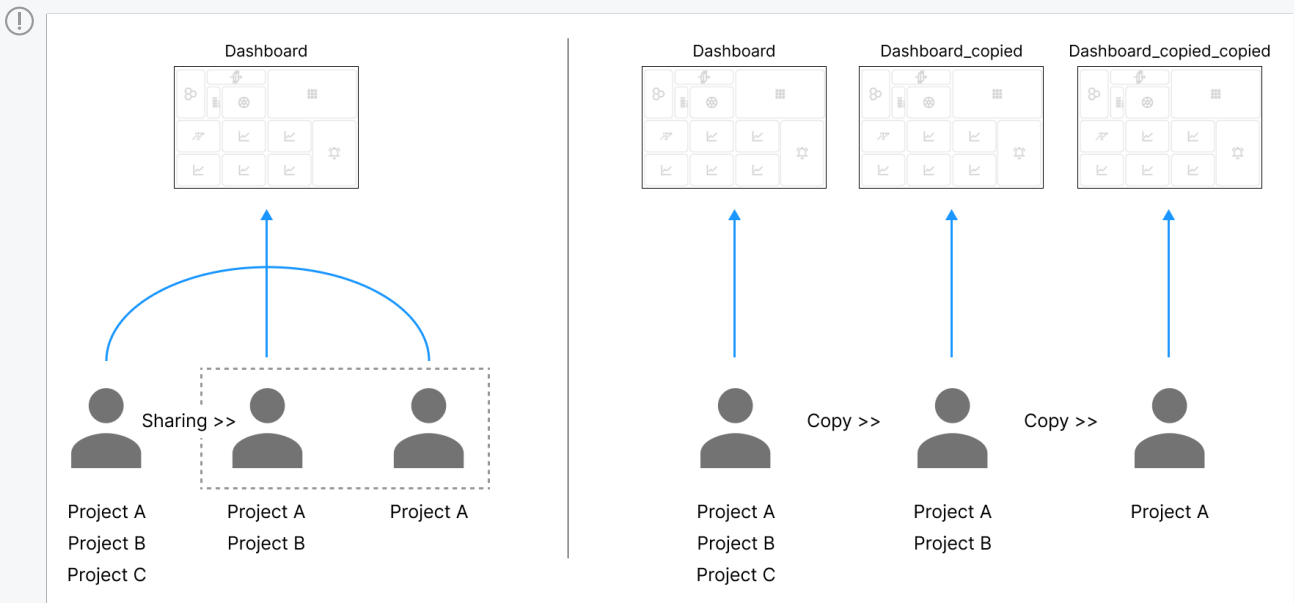
 ダッシュボードの削除は所有者と共有を受けたユーザーで動作が異なります。

- ダッシュボード所有者がダッシュボードを削除すると、共有されたすべてのユーザーアカウントでもそのダッシュボードが削除されます。
- 共有を受けたユーザーがダッシュボードを削除すると、そのユーザーの **ダッシュボードリスト** のみから削除されます。元のダッシュボードは維持されます。

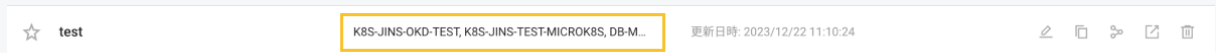
Flex ボードを共有する

 Flex ボードの共有機能は **ホーム>統合Flexボード** メニューでのみ使用できます。
プロジェクトの **Flexボード** メニューでは提供されません。

 共有とコピーの違い



- 共有: 共有されたメンバーは同じダッシュボードを閲覧します。
- コピー: ダッシュボードを他のメンバーまたは自分にコピーすると、コピーされた別個のダッシュボードを閲覧します。
- 読取り専用 で共有/コピーされたダッシュボードは編集できません。編集モード で共有/コピーされた場合のみ編集できます。
- 読取り専用 で共有を受けたメンバーも、そのダッシュボードを 閲覧専用で再共有 したり コピー できます。
- ダッシュボードに含まれるプロジェクトのうち **少なくとも1つ** のプロジェクトに所属しているメンバーにのみ共有できます。共有またはコピー先のメンバーがプロジェクトに所属しているか確認してください。



統合Flexボード で作成した Flex ボードを他のメンバーと共有できます。所有者が共有されたダッシュボードを編集すると、共有を受けたすべてのメンバーに同じ変更が反映されます。

1. 統合Flexボード の **ダッシュボードリスト** で、共有するダッシュボードの アイコンをクリックします。
2. **ダッシュボード共有** ウィンドウが表示されたら、共有するメンバーを1名または複数名選択するか、アカウントを直接入力します。
 - **読取り専用** を選択すると、共有を受けたメンバーはダッシュボードを編集できません。

- 共有対象は、ダッシュボードに含まれるプロジェクトのうち少なくとも1つのプロジェクトに所属している必要があります。

3. 共有 ボタンをクリックします。

- 共有された項目には **共有** タグが表示されます。**共有** タグにマウスを載せると、共有したメンバー情報を確認できます。
- 閲覧専用で共有された項目には **読取り専用** タグが表示されます。

ダッシュボードを共有で受け取った場合	ダッシュボードを共有した場合（ダッシュボード
 ダッシュボード所有者 owner@whatap.io 更新日時: 2023/06/14 10:22:05 共有 RUM ページ 5 ダッシュボード共有メンバーリスト 更新日時: 2023/06/14 10:19:52 共有 読取り専用 更新日時: 2023/06/05 16:41:36	 ダッシュボード所有者 demoowner@whatap.io 更新日時: 2023/07/06 16:25:06 共有 demoowner@whatap.io ダッシュボード共有メンバーリスト 更新日時: 2023/06/14 10:22:05 共有 更新日時: 2023/06/14 10:19:52

✓ ダッシュボード共有の条件

- ダッシュボード共有機能は **ホーム > 統合Flexボード** のみで提供します。
- だれでも自分のダッシュボードを共有でき、共有で受けたダッシュボードを再共有やコピーできます。
- 読取り専用** で受けたダッシュボードは編集できませんが、**編集モード** で受けた場合は編集できます。
- 所有者** がダッシュボードを削除すると、共有を受けたすべてのアカウントで該当ダッシュボードが削除されます。
- 共有を受けたユーザー** が削除した場合は、そのユーザーの **ダッシュボードリスト** のみから削除され、元のダッシュボードは維持されます。
- 共有で受けたダッシュボードに含まれるプロジェクトのうち、**ビュー** 権限がないプロジェクトはデータを参照できません。

Flex ボードをコピーする

ユーザーは Flex ボードをコピーして他のメンバーに渡せます。

1. 統合Flexボード のダッシュボードリスト で、 アイコンをクリックします。
2. コピーオプションを選択します。
 - **自分にコピー:** 自分のアカウントにコピーします。
 - a. `_copied` 接尾辞が付いた項目が **ダッシュボードリスト** に追加されます。
 - **他人にコピー:** 他のメンバーのアカウントにコピーします。
 - a. **+** **アカウント** をクリックします。
 - b. コピー先メンバーのメールを選択し、**ダッシュボードコピー** ボタンをクリックします。
 - c. そのメンバーの **ダッシュボードリスト** に `_copied` 接尾辞が付いた項目が追加されます。

JSON ファイルで共有する

Flex ボードの設定を JSON ファイルとして他のメンバーに渡したり、他のメンバーの設定を取り込みます。

エクスポート

1. 統合Flexボード またはプロジェクトの **Flexボード** メニューに移動します。
2. **ダッシュボードリスト** で  ボタンをクリックします。
3. エクスポートオプションを選択します。
 - **プロジェクト情報を含む:** ダッシュボードに設定されたプロジェクト情報を JSON ファイルに含めて共有
 - **プロジェクト情報を含まない:** ダッシュボードに設定されたプロジェクト情報を JSON ファイルに含めずに共有
4. JSON ファイルをダウンロードし、共有先のメンバーに渡します。

インポート

1. 統合Flexボード またはプロジェクトの Flexボード メニューに移動します。
2. 画面右上の  インポート ボタンをクリックします。
3. ダウンロードした JSON ファイルを選択します。

❗ この機能は、プロジェクトの 編集 権限を持つメンバーのみ利用できます。

Flex ボードの画面モード

Flex ボードの画面モードに応じて提供機能が異なります。

❗ アクセス可能なメンバー権限

プロジェクト内の Flexボード メニューでは、編集権限のあるユーザーのみが編集モード、アドミン、フィルター 機能にアクセスできます。メンバー権限の詳細は[次のドキュメント](#)を参照してください。

- プロジェクト編集 権限
- プロジェクトのFlexボードの修正 権限
- Site Admin 権限

モード種類

Flexボード は画面モードにより設定できる機能が異なります。

- **編集モード:** ウィジェットテンプレート一覧からレイアウトにウィジェットを配置し、ウィジェットの編集、削除、位置調整ができます。
- **アドミン:** ウィジェットの詳細プロパティを JSON 形式で管理できます。レイアウトに配置したウィジェット右上の  ボタンを選択します。
- **ビューモード:** ウィジェットの配置、サイズ調整、詳細オプションなどの設定を完了後、ダッシュボードのように各ウィジェットのデータをリアルタイムで監視できます。

共通機能

- データフィルタリング
- リアルタイムデータの参照範囲設定
- 印刷モード
- Flex ボード管理
- データ結合オプション

データフィルタリング

データフィルタリングで監視対象を絞り、効率的な Flex ボードを構成できます。

1. 画面上部の **▽ フィルター** タブをクリックします。
2. 画面右に表示される **フィルター** ウィンドウでフィルタリング対象を選択します。すべて選択するには **すべて選択** を選択します。
 - **エージェント オプション**: エージェント種別またはアプリケーション一覧を選択、**検索** 機能あり
 - **メトリクス オプション**: プロジェクトまたはエージェント種別を選択、**+ And** 条件の追加や、**含む**、**除外** による文字列ベースの自動選択が可能
3. フィルタリング対象を選択したら、**適用** ボタンをクリックします。
4. よく使う条件は **フィルター保存** ボタンで保存します。
 - a. フィルター名を入力し、**保存** を選択します。**保存フィルター** は **フィルター** ウィンドウ下部に表示されます。

フィルタリング条件

フィルタリング条件はエージェントタイプとメトリクスタイプに分かれます。

エージェントは基本的な監視対象のみ選択肢として提供し、メトリクスはプロジェクトで収集したすべてのメトリクスデータのタグを選択肢として提供します。メトリクスタイプは、非エージェント形式でデータを収集し、その後フィルタリングを適用する場合に有用です。メトリクスの詳細は[次のドキュメント](#)を参照してください。

タイプ	エージェント	メトリクス
選択オプション	WhaTap プロジェクトの監視対象 (アプリケーション、サーバー、データベース、 コンテナ、Kubernetes の POD と NODE)	エージェントを含むすべてのメトリクスタグ
適用範囲	すべてのウィジェット	メトリクスデータを使用するすべてのウィジェット
フィルタリング方式	チェックボックス	一致, 含む, 除外

参照時間を設定する

Flexボード の画面右上の時間セクターで、ウィジェットのデータ参照時間を設定できます。

- ||: リアルタイムモードを停止して特定の参照時間に設定
- 🕒: リアルタイムモードに戻す

印刷する

Flex ボード画面を PDF で保存して印刷できます。

- Flex ボード画面の右上にある  アイコンをクリックして印刷モードに切り替えます。
- オプションを設定します。
 - フィルターオプション表示:** 画面のフィルターオプションを表示/非表示に切り替え
 - {mode}方向に切換え / {mode}方向に切換え:** 画面を横向きまたは縦向きに変更
- 完了後、**PDFダウンロード** を選択します。
- 印刷モードを終了するには、右上の **× 印刷モード終了** をクリックします。

Flex ボード管理

Flex ボードのレイアウト変更、ウィジェットの位置移動やサイズ調整、名称変更などの管理機能を提供します。Flex ボード管理 機能は、**ダッシュボード > Flexボード メニューのダッシュボードリスト**で  アイコンをクリックして入

ることもできます。

1. Flex ボード画面の右上の  アイコンをクリックすると、**Flexボード管理** ウィンドウが開きます。

- **名前変更:** Flex ボード名の変更
- **レイアウト:** ウィジェットの位置・サイズ調整および削除
- **他のユーザーの修正を許可しない:** 変更制限オプション
 - 編集権限のあるメンバーは編集・削除・変更が可能で、オプションを有効化すると **他のユーザーの修正を許可しない: On** に変更されます
- **ウィジェット.json:** Flex ボードに含まれるウィジェットを JSON 形式で編集・管理
- **オプション.json:** Flex ボードの設定を JSON 形式で編集・管理（プロジェクト情報、Flex ボードフィルター、時間選択などの設定値）

 **ウィジェット.json と オプション.json** 機能は、ダッシュボード管理者権限のユーザーにのみ提供します。

2. すべての設定を完了し、**保存** ボタンをクリックします。

ダッシュボードをお気に入りに登録する

作成した Flex ボードはお気に入りに登録して素早くアクセスできます。**ダッシュボード > Flexボード** の **ダッシュボードリスト** で、お気に入り登録するダッシュボードの ☆ ボタンをクリックすると、★ に変わります。

ウィジェットの管理

Flexボードに配置したウィジェットを管理して、ダッシュボードをユーザーがカスタマイズします。

- ✓ ダッシュボードはメトリクスウィジェットを含むさまざまなウィジェットテンプレートを活用して構成できます。
各テンプレートの特徴と使用方法については、[ウィジェットテンプレート](#) ドキュメントで詳しく確認できます。

ウィジェット追加

作成済みのFlexボードにウィジェットを追加できます。

1. Flexボードメニューのダッシュボードリストで、ウィジェットを追加するダッシュボードを選択します。
 2. 画面左上の編集モードを選択します。
 3. 左側のウィジェットテンプレート一覧から目的のウィジェットを選択します。メトリクスウィジェットを追加するには、すべてのメトリクスを選択してから、目的のウィジェットをクリックします。
- ホーム画面の統合Flexボードを選択し、ウィジェットを追加した場合は、プロジェクト選択ボタンをクリックして、収集対象のプロジェクトを選択します。
 - 追加するウィジェットがある場合は、同じプロセスを繰り返してください。
4. すべての手順が完了したら、画面上部のビューモードを選択してレイアウトを確認し、 (リストヘ) ボタンをクリックします。

ウィジェットの属性変更

Flexボードメニューのダッシュボードリストで、ウィジェットのプロパティを変更するボードを選択します。編集モードに入ります。

ウィジェット名の変更

1. 名前を変更するウィジェットの名前の右側の  ボタンをクリックします。
2. ウィジェットの題名、フォントサイズ、色を設定し、**保存**ボタンを選択します。
 - 保存する際に、**すべてのウィジェットに適用**トグルボタンの機能を活性化すると、フォントサイズと色が他のウィジェットにも適用されます。
 - ウィジェットのタイトルをロックするには  ボタンを選択し、**保存**ボタンをクリックします。

時間設定

1. 時間を設定するウィジェットの右上の  ボタンを選択します。
2. **時間選択**ウィンドウで時間を設定してください。
 - ダッシュボード画面で設定した時間を適用するには、**ダッシュボード設定に従う**をチェックします。ダッシュボードの時間設定は右上にあります。
 - 特定の時間を設定する場合は、**ダッシュボード設定に従う**のチェックを外します。＜または＞ボタンを使用して照会する時間を設定します。
3. 時間設定が終了したら  ボタンをクリックします。

 ウィジェットのデータタイプによっては、時間設定機能をサポートしていない場合があります。

出力データオプションの設定

チャート型ウィジェットの出力データオプションを設定して、ユーザーが必要なデータを選択できます。

1. ウィジェットの右上にある  アイコンをクリックして、出力データのオプションを設定します。
 - プロジェクト、エージェント、アプリケーションなどを選択してデータをフィルタリングできます。
 - 個々のデータまたはマージされたデータを選択して、チャートに表示されるグラフのタイプを変更できます。
 -  >  を選択します。**チャート設定**画面で詳細オプションを変更できます。設定できるオプションは次

のとおりです。

- **チャートタイプ**：集計する現在の数値をチャートに表示するオプションです。
 - **y軸 チャート最大値**：Y軸にチャートの最大値を自動または固定で選択できます。
 - **水平線設定**：追加ボタンを選択し、しきい値または範囲を水平線として表示できます。複数を追加して適用できます。水平線を追加した後は、**適用**ボタンを選択してチャートに反映してください。
 - **チャートの最大値を表示**：チャートに表示されるグラフの最大値を表示します。
 - **サブチャート**：ウィジェットのメインチャートにサブチャートを追加できます。サブチャートの種類を選択し、レイアウトとサイズ、データのマージ有無を選択します。他のウィジェットにも適用する場合は、**すべてのウィジェットに適用**ボタンを選択します。サブチャートは、データをさまざまな方法で確認するとき便利です。
2. オプション設定がすべて完了したら、**チャート設定**画面の左上の×ボタンをクリックするか、**チャート設定**領域の外側をクリックします。

❗ ウィジェットのデータタイプによって選択できるオプションは異なる場合があります。

メトリクスウィジェットデータの変更

メトリクスウィジェットのデータ照会の条件を変更できます。

1. **Flexボード > ダッシュボードリスト**で、ウィジェットデータを変更するダッシュボードを選択します。
2. **編集モード**で、変更したいウィジェットの右上にある  アイコンをクリックします。
3.  アイコンをクリックすると、データ設定編集ウィンドウが表示されます。
4. 次を参照して設定を変更するには、**適用アイコンウィジェットに適用**ボタンをクリックします。
 - ウィジェットを作成すると、デフォルトで生成されるメトリクスのオプションがタブに表示されます。
 - メトリクス オプションには、**カテゴリ**と**フィールド**、**タグ**が含まれます。
 - **カテゴリ**項目は現在、変更を加える機能を制限しています。
 - **フィールド**、**タグ**項目は複数選択できます。選択したタグオプションでチャートデータをグループ化します。
 -  ボタンをクリックすると、元のデータを表示できます。

- オブジェクトのマージおよび時間マージ項目の詳細については、[データマージオプション](#)を参照してください。

データマージオプション

Flexボードのすべてのメトリクス一覧に配置されたマトリクスウィジェットでは、データのマージオプションを提供します。データのマージは、オブジェクトのマージと時間マージ方法を提供します。

• オブジェクトのマージ

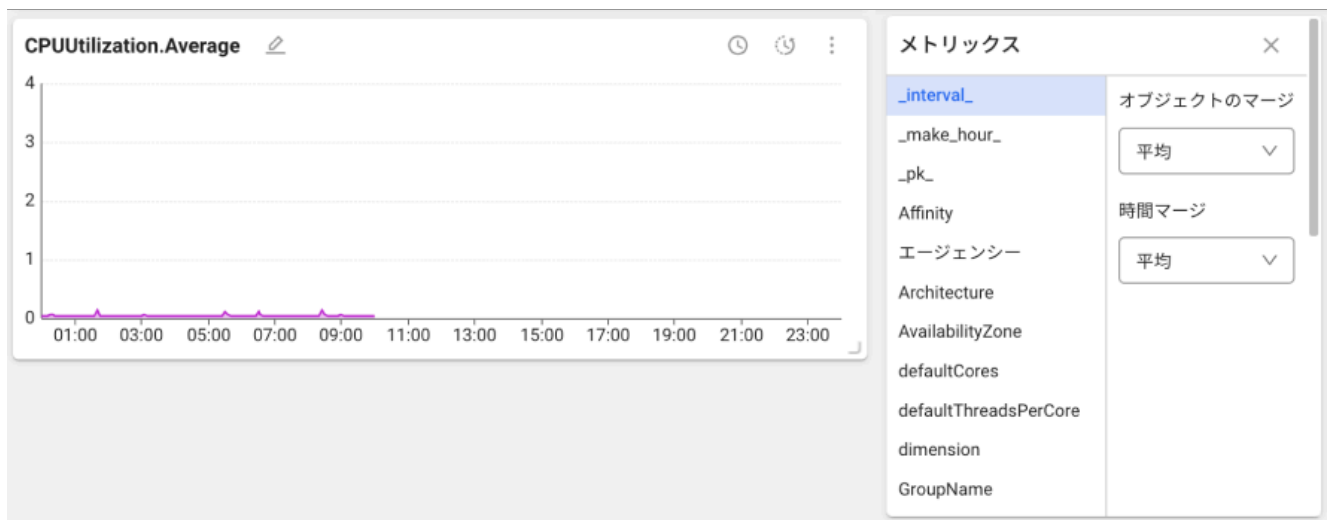
左側で選択したタグ(例：エージェント名)に基づいてチャートデータをグループ化するために使用します。この場合、異なるフィールド(例：CPU)値を持つデータ間でタグが一致する場合、そのデータは結合されます。

• 時間マージ

主に検索時間が長い場合に使用します。ソースデータとフィールド値が同じデータを時間範囲に基づいて一定の時間間隔(5分または1時間)でデータを結合します。この結合方法は、時間結合と呼ばれます。

• AWS CloudWatchメトリクス

AWSモニタリング指標の場合、統計手法はフィールド名の後にサフィックス(接尾辞)として追加されます。データマージの既定値は、このサフィックスを参照しています。



1. 編集モードですべてのメトリクスボタンを選択し、ウィジェットテンプレート一覧をすべてのメトリクス一覧に変更します。
2. メトリクスウィジェットをレイアウトに配置します。

3. メトリクス ウィジェットの右上にある  ボタンを選択します。
4. タグ(例: エージェント名)オプションを選択すると、データ結合オプションが表示されます。ウィジェットのサイズによっては、メトリクス オプションの位置が異なる場合があります。

ウィジェットのコピー

1. ウィジェットの右上にある  ボタンをクリックします。
2.  ボタンをクリックします。
3. コピー画面が表示されたら、**+ ウィジェット追加**を選択します。
4. 一覧にあるウィジェットの名前を変更します。
5. **適用**ボタンを選択します。
6. **編集モード**画面でコピーしたウィジェットで確認できます。

ウィジェットの削除

1. ウィジェットの右上にある  ボタンをクリックします。
2.  ボタンをクリックします。
3. 確認メッセージの画面が表示されると、**削除**ボタンを選択します。削除を取り消すには**キャンセル**ボタンをクリックします。

インターフェース状態

インターフェース状態メニューでデバイスのネットワークインターフェースの状態をリアルタイムでモニタリングできます。インターフェースの接続状態を視覚的に表示し、各インターフェースに関する詳細な情報を提供することで、ネットワークの性能を簡単に分析できます。

基本画面と設定

インターフェース状態画面は左インターフェースリスト領域と右上インターフェース状態、右下インターフェース詳細領域で構成されています。インターフェースリストで照会するインターフェースを選択すると、右側の領域でインターフェースの状態および詳細を確認できます。

Interface Status

1. インターフェース状態上部オプションバーの**時間選択**で、照会時間範囲を設定してください。
 - **LIVE**モードは直近30分のデータを自動的に更新し、過去の時間照会をサポートしていません。
2. 上部オプションバーの**マネージャー選択**で、データを収集するNMSマネージャーを選択してインターフェース状態を確認できます。

インターフェース状態

インターフェースの接続状態を確認できます。

- **Connected** : インターフェースが正常に接続された状態です。Link StatusとAdmin Statusともに"up"の時に表示されます。
- **Link Down** : ネットワークリンクがダウンした状態です。Link Statusは"down"、Admin Statusは"up"状態の時に表示されます。
- **Admin Down** : 管理者がそのインターフェースを非活性化した状態です。Link StatusとAdmin Statusともに"down"の時に表示されます。
- **Unavailable** : 物理的に活性化されていない仮想インターフェース、ループバックインターフェース、またはSFPモジュールが未挿入されたFiberインターフェースなど、使用できないインターフェースの数を示します。

インターフェース詳細

各インターフェースの詳細情報を一覧形式で表示し、インターフェースをクリックすると該当デバイスの推移ページに移動してより具体的な状態を確認できます。

デバイス推移

使用状況でデバイスの状態変化に関連するデータをリアルタイムで確認できます。デバイスとインターフェイスの指標を視覚的に提供することで、ネットワーク性能の変化を即座に把握できます。

基本画面と設定

- 1. 上部オプションバーの**時間選択**で照会時点を選択できます。選択した時点基準で直近10分のデータを表示します。
- 2. 上部オプションバーの**マネージャー選択**で、データを収集するNMSマネージャーを選択して使用状況を確認できます。
- 3. **デバイス選択領域**で分析するデバイスまたは特定インターフェイスを選択します。

選択	表示されるビュー
デバイスのみ選択	Deviceレベルビュー（全インターフェイストレンド）
デバイス>インターフェイス選択	Interfaceレベルビュー（単一インターフェイス詳細）

- 4. 選択したデバイスまたはインターフェイスの使用状況を確認できます。

インターフェイス表示形式

デバイスを選択すると、インターフェイスの表示形式を選択できます。

インターフェイス表示形式

Item	Description
デバイス	実際の機器の前面と同じ形でポートを配置して表示
状態	インターフェイスの状態をリスト形式で表示

物理ポート情報がない機器は、フレームの代わりに 収集されたインターフェイスポート情報がありません。 という案内が表示され、ポート配置設定への入口も表示されません。

ポート配置設定

デバイス形式では、画面に表示するポート配置を機器の実物に合わせて調整できます。

1.  アイコンをクリックしてください。ポート配置設定ウィンドウが開きます。
2. フレームエリアで機器の規格を選択してください。

Item	Description
幅	1行が収容するポート数。 24ポート または 48ポート
高さ	フレームの行数。 1 から 3 まで
SFPポート	各行の右側に予備ポートスロットを4つ追加

3. ポートをドラッグするか、ポートをクリックした後に移動先をクリックして位置を変更してください。
4. 適用ボタンをクリックして保存してください。元に戻す場合はキャンセルボタンをクリックしてください。
 - 基本配置に戻すには、基本配置に戻すボタンをクリックしてください。

❗ フレームの容量が不足している場合は、
{count}個のポートがフレームの外に残っています。幅または高さを大きくしてください。 という案内が表示されます。すべてのポートが配置されると、配置されたポート数と残りのスロット数が表示されます。

❗ 状態形式である場合や編集する物理ポートがない場合は、ポート配置設定ボタンが非活性状態が表示され、その理由がツールチップで案内されます。

使用状況 - Device

デバイスを選択すると、そのデバイスの全インターフェイストラフィック推移をラインチャートで表示します。

Usage status device

チャートパネル

パネル	説明
Total Throughput	全インターフェイス合算処理量。画面全体の幅で表示される
Inbound Throughput	インターフェイスごとのインバウンドトラフィック。各インターフェイスが個別ラインで表示される
Outbound Throughput	インターフェイスごとのアウトバウンドトラフィック
Top N (Daily)	日間最大処理量基準のインターフェイスランキングテーブル
Top N (10分)	直近10分の最大処理量基準のインターフェイスランキングテーブル

Top N テーブルカラム

カラム	説明
Interface	インターフェイス名
Today / Recent 10 Min	該当期間内の最大処理量（bps単位）
Current	現在の処理量（bps単位）

ⓘ Top N テーブルは処理量基準の降順で並び替えられ、最もトラフィックの多いインターフェイスを素早く特定できます。

Private MIB ウィジェット

デバイスにカスタム OID（Private MIB）が設定されている場合、追加ウィジェットが表示されます。

項目	説明
表示条件	AllInterfaces 以外のOIDが設定されている場合
ウィジェット内容	OIDごとのカスタム指標チャート

Private MIBチャートのカスタマイズ

Private MIBウィジェットの右上にある  アイコンをクリックすると、**Chart Setting**ウィンドウが開きます。**Chart Setting**ウィンドウは3つのエリアで構成されます。

エリア	説明
Chart Preview	現在の設定でチャートがどのように表示されるかをプレビュー
OID Information	該当OIDの詳細情報
	OID: 収集対象のOID（例：1.3.6.1.4.1.9.6.1.101.1.8.0） MIB Info: MIBモジュールとシンボル情報（例：CISCO-SB-MIB::rxCpuUtilDuringLastMinute） Node Type: MIBノードタイプ（例：Integer32、Counter64） Description: MIBファイルに定義されたOIDの説明
Chart Setting	チャートタイプ、単位などの設定オプション

Chart Settingオプション

Chart Settingオプションである**時間範囲**、**チャートタイプ**、**単位**を設定します。

Time Range（時間範囲）

オプション	説明	使用可能なチャート
Recent 30 Min	直近30分のデータを時系列で表示	Line、Bar
Latest	最新の値のみ表示	Text、Table

ⓘ Time Rangeを変更すると、使用可能なChart Typeが自動的に変更されます。

Chart Type（チャートタイプ）

タイプ	チャート	説明
Time Rangeが Recent 30 Min の場合	Line	時系列ラインチャート。トレンド分析に適する
	Bar	時系列棒チャート。区間別の比較に適する
Time Rangeが Latest の場合	Text	最新の値を大きなテキストで表示。単一指標のモニタリングに適する
	Table	テーブル形式で表示。複数のインデックス値の比較に適する

Unit（単位）

単位	説明	使用例
Count	一般的な数値（デフォルト）	パケット数、セッション数
Byte	バイト単位で自動変換（KB、MB、GB）	メモリ使用量、ファイルサイズ
Bit	ビット単位で自動変換（Kb、Mb、Gb）	ストレージ容量

単位	説明	使用例
bps	秒あたりビットで自動変換（Kbps、Mbps、Gbps）	帯域幅、スループット
Percent (0-100)	パーセント（0～100の範囲）	CPU使用率、メモリ使用率
Percent (0-1)	パーセント（0～1の範囲、100を掛けて表示）	一部機器の使用率
Severity	カスタム状態値のマッピング	機器の状態、アラームレベル

Severityのカスタマイズ

UnitでSeverityを選択すると、数値を意味のある状態ラベルにマッピングできます。

デフォルトのSeverity設定

Value	Label
0	Normal
1	Warning
2	Critical

Severityの設定方法

- Unitドロップダウンで**Severity**を選択します。
- デフォルトの3つの状態（Normal、Warning、Critical）が表示されます。
- 各状態の設定を修正します。
 - Label:** 画面に表示される状態名（例：正常、警告、危険）
 - Value:** その状態として認識するOIDの値（整数）
- Add Severity**ボタンで新しい状態を追加します。
- X**ボタンをクリックして不要な状態を削除します。

✔ Severityは、SNMP機器の状態コードを人が読みやすいラベルに変換する際に便利です。

Severityの使用例

機器の運用状態のモニタリング

Value	Label	意味
1	Running	正常運用中
2	Standby	待機状態
3	Down	障害状態

ポート状態のモニタリング

Value	Label	意味
1	Up	有効
2	Down	無効
3	Testing	テスト中

使用状況 - Interface

特定インターフェイスを選択すると、そのポートの詳細指標が4つのチャートパネルで表示されます。

Usage status interface

チャートパネル

パネル	指標	単位	説明
Throughput In/Out	bpsIn, bpsOut	bps	インバウンド/アウトバウンド処理量
Discard In/Out	discardIn, discardOut	count	廃棄されたパケット数
Error In/Out	errorIn, errorOut	count	エラー発生パケット数
PPS In/Out	ppsIn, ppsOut	count	1秒あたりのパケット数

統計情報

各チャート下部に Input/Output 統計が表示されます。

項目	説明
Current	現在値（最新データポイント）
Max	照会期間内の最大値
Avg	照会期間内の平均値

ヘルスチェックステータス

ヘルスチェックステータスでは、ヘルスチェックの結果をリアルタイムでモニタリングできます。各対象の応答状態、RTT、Jitter、パケットロスなどの詳細指標を確認します。

基本画面と設定

Health check status

時間選択

上部オプションバーの時間選択でリアルタイムデータの更新時間が表示されます。

マネージャー選択

上部オプションバーのマネージャー選択で、データを収集するNMSマネージャーを選択してヘルスチェック結果を確認できます。

ヘルスチェック対象の選択

左パネルで照会するデバイスまたはヘルスチェック対象を選択します。

選択レベル	説明
ALL [n]	すべてのヘルスチェック結果。括弧内の数字はAlive/Dead数
デバイス名	特定デバイスに登録されたヘルスチェックのみ表示
対象 (IP/FQDN)	特定対象の詳細結果のみ表示

ステータス表示

各項目の横にヘルスチェックステータス結果が 全体数[正常応答数/未応答数] の形式で表示されます。

- 緑色: Alive（応答あり）
- 赤色: Dead（応答なし）

ヘルスチェック結果

チャート

選択した対象の指標を時系列チャートで表示します。

チャート	説明
Jitter	ジッター推移（ms）。ICMPタイプで提供
Max RTT	最大RTT（Round Trip Time）推移（ms）。すべてのタイプで提供

時間範囲

- 固定10分範囲のデータを表示します。
- 10秒間隔で自動更新されます。

ヘルスチェックリスト

カラム	説明
Alive	応答状態 - ●: Alive（正常応答） - ●: Dead（応答なし）
Type	ヘルスチェックタイプ（ICMP、TCPなど）
IP	ヘルスチェック対象のIPアドレス
FQDN	Fully Qualified Domain Name（ドメイン名）

カラム	説明
Port	TCPポート番号（TCPタイプの場合）
Avg RTT	平均Round Trip Time（ms）
Max RTT	最大Round Trip Time（ms）
Packet Loss	パケットロス率（%）
Jitter	ジッター値（ms）
Error	エラーメッセージ
Last Seen Time	最後の応答受信時刻

付録

指標

タイプ別提供指標	ICMP	TCP
Alive	0	0
Avg RTT	0	-
Max RTT	0	0
Jitter	0	-
Packet Loss	0	-
Port	-	0
Error	0	0

- RTT (Round Trip Time)

指標	説明
Avg RTT	平均往復時間 - 応答遅延時間の平均
Max RTT	最大往復時間 - 最も遅い応答時間

- Packet Loss

送信されたパケットのうち、失われたパケットの割合（%）です。

- Jitter

ネットワーク遅延時間の変動幅です。Jitterが高いとネットワーク品質が不安定であることを示します。

データ更新周期

ページは10秒間隔で自動更新されます。

項目	値
更新周期	10秒
時間範囲	直近10分

対応ヘルスチェックタイプ

タイプ	説明
ICMP	ICMP Pingベースの接続状態確認
TCP	TCPポート接続状態確認

デバイスインベントリ

デバイスインベントリはネットワーク上の機器登録と監視設定を管理します。機器はマネージャが提供する Auto Discovery 機能で自動検出するか、必要に応じて手動で追加できます。登録された各機器は SNMP ベースの監視と Health Check を設定して、リアルタイム状態を確認できます。これによりネットワーク管理システムで監視対象デバイスを一元管理できます。

基本画面と設定

デバイスインベントリでは、登録されたすべてのネットワーク機器の一覧をテーブル形式で確認できます。上部メニューでは、機器の登録と管理に関連する主要機能を提供します。

Device inventory

マネージャー選択

接続されたNMS Managerインスタンスを選択します。

デバイス追加

+ デバイス追加ボタンをクリックして、新しいネットワーク機器を手動で追加します。詳細は[デバイス追加](#)を参照してください。

SNMP Polling一括設定

+ SNMP Polling一括設定ボタンをクリックして、複数のデバイスにSNMP Polling設定を一括適用します。

状態サマリー

項目	説明
Total	登録された全デバイス数

項目	説明
SNMP Enabled	SNMP Pollingが有効なデバイス数
SNMP Disabled	SNMP Pollingが無効なデバイス数

ⓘ 状態サマリーの項目をクリックすると、その状態のデバイスのみをフィルタリングして照会できます。

デバイス一覧

デバイス一覧項目	説明
	デバイス設定の修正。クリックするとデバイス設定Drawerが開く
Alias	機器エイリアス
Host	機器のIPアドレス
Hostname	機器のホスト名
Description	機器の説明（機器のモデル名など）
Manufacturer	製造元（例：Cisco Systems）
Location	設置場所
Contact	担当者の連絡先
Host Type	ホストタイプ（例：Switch、Router）
Role	機器の役割（例：Border Router、Edge Switch）
Serial No.	機器のシリアル番号
Firmware	ファームウェアバージョン

デバイス一覧項目	説明
SNMP Polling	SNMP Pollingの状態と収集OID数
Health Check	Health Checkの状態と設定数

+ デバイス追加

新しいネットワーク機器を手動で登録できます。

1. デバイスインベントリ 画面で + デバイスの追加 ボタンをクリック。
2. デバイスの追加 の Device Info タブで情報を入力。
 - Host (必須): 機器の IP アドレス
 - Host Name: 機器のホスト名
 - Manufacturer: 製造元情報
 - Contact: 担当者情報
 - Role: ネットワーク上の役割
 - Alias: 管理用エイリアス
 - Description: 機器詳細説明
 - Location: 物理設置場所
 - Host Type: 機器タイプ
 - Serial No.: シリアル番号
3. 追加 ボタンをクリック。

デバイス詳細管理

1. 登録済み機器の  をクリック。
2. 詳細情報画面の Device Info, SNMP Polling, Health Check タブで情報を確認または修正し、保存 ボタンをクリック。

Device Info タブ

機器の基本情報を設定。

SNMP Polling タブ

SNMP プロトコルを使って機器の性能と状態を定期的に収集する設定を管理。修正後、**保存** ボタンで反映。

- **Port** (必須): SNMP ポート (デフォルト: 161)
- **Community** (必須): SNMP v1/v2c コミュニティ文字列 (デフォルト: public)
- **Version** (必須): SNMP バージョン (v1, v2c, v3)
- **User Name**: SNMPv3 ユーザー名
- **Security Level**: セキュリティレベル (noAuthNoPriv, authNoPriv, authPriv)
- **Authentication Protocol**: 認証プロトコル
 - **Authentication Key**: 認証キー
- **Privacy Protocol**: 暗号化プロトコル
 - **Privacy Key**: 暗号化キー

OID 選択と管理

1. **Edit OID** ボタンをクリックし、OID リストから収集する MIB 情報を選択。

OID リスト項目	説明
OID	SNMP OID 値
MIB Information	MIB 名称と情報
Manufacturer	製造元
Category	指標カテゴリ
Description	詳細説明

2. OK ボタンをクリック。

収集間隔設定

- **Custom Polling Interval:** データ収集間隔を設定 (秒単位、デフォルト: 60)
- **Activate:** SNMP Polling の有効/無効

Health Check タブ

ネットワーク機器の可用性をリアルタイムで監視。ヘルスチェック対象を追加することもできます。

Health Check 項目	説明
Activate	ヘルスチェック有効状態
Target Host	監視対象 IP アドレスまたは FQDN
Protocol	ヘルスチェックプロトコル (ICMP など)
Memo	メモや説明
Actions	監視対象の編集 (✎)、削除 (🗑)

ヘルスチェック対象の追加

1. Health Check タブで + 追加 ボタンをクリック。
2. ヘルスチェック対象追加 ポップアップで情報を入力。
 - **Target Host:** IP アドレスまたは FQDN を入力
 - **Protocol:** ICMP を選択 (ドロップダウン)
 - **Memo:** 任意のメモ入力
 - **Activate:** 即時有効化の有無を選択
3. OK ボタンをクリックして保存。

グループ管理

グループ管理メニューでは、デバイスを📍 Site → 🏠 Building → 🏢 Floor の構造で管理できます。グループ単位でデバイスを整理すると、大規模ネットワーク環境での管理・モニタリングが便利になります。

基本画面と設定

グループ管理

🔊 🔔 📄 💬 🤖 👤

マネージャーの選択

nmsdevu2204

▼

+ Add Location

NAME	DESCRIPTION	DEVICES	
📍 Seoul HQ	-	-	+ 追加 ✎ 修正 🗑 削除
🏠 SparkPlus	-	-	+ 追加 ✎ 修正 🗑 削除
🏢 13F	-	View Devices	✎ 修正 🗑 削除
📍 Tokyo Office	-	-	+ 追加 ✎ 修正 🗑 削除
🏠 Nakayama B/D	-	-	+ 追加 ✎ 修正 🗑 削除
🏢 11F	-	View Devices	✎ 修正 🗑 削除

1. グループ管理画面上部のマネージャー選択から、グループ管理を行うマネージャーを選択してください。選択したマネージャーを基準にグループリストが表示されます。
2. 選択したマネージャーを基準に表示されたグループリストを確認・追加・削除できます。📍 Site → 🏠 Building → 🏢 Floor のツリー形式で表示されます。

表 | グループリスト

カラム	説明
Name	グループ名（場所/建物/フロア）
Description	グループの説明

カラム	説明
Devices	グループに含まれるデバイスの表示
アクション	グループの追加/編集/削除

グループの追加

Locationの追加

1. 画面上部の**+ Add Location**ボタンをクリックしてください。
2. **Add Location**ダイアログで名前とタイプを入力してください。
3. **Save**ボタンをクリックすると新しいLocationが作成されます。

Buildingの追加

1. Buildingを追加するLocationの**+ 追加**ボタンをクリックしてください。
 - 画面上部の**+ Add Location**ボタンをクリックして追加することもできます。
2. **Add building**ダイアログで名前を入力してください。
3. **Save**ボタンをクリックすると新しいBuildingが作成されます。

Floorの追加

1. Floorを追加するBuildingの**+ 追加**ボタンをクリックしてください。
 - 画面上部の**+ Add Location**ボタンをクリックして追加することもできます。
2. **Add floor**ダイアログで名前を入力してください。
3. **Save**ボタンをクリックすると新しいFloorが作成されます。
4. **View Devices**ボタンをクリックして割り当てられたデバイスを確認できます。

グループの編集

1. 編集するグループの  編集ボタンをクリックしてください。
2. グループ名または説明を変更します。
3. **Save** ボタンをクリックして変更内容を反映します。

グループの削除

1. 削除するグループ右側の  削除ボタンをクリックしてください。
2. 削除確認ポップアップで削除をクリックすると、該当グループが削除されます。

デバイスの割り当て

グループ管理リストでFloorの**View Devices**ボタンをクリックすると、デバイス割り当て画面が開きます。

デバイスの追加/削除

- + 追加ボタンをクリックして未割り当てデバイスを選択すると、即座に割り当てられます。
-  アイコンをクリックして個別デバイスの割り当てを解除します。

一括編集

複数のデバイスを一度に管理できます。

1. Floorの**View Devices**ボタンをクリックして、デバイス割り当て画面を開きます。
2.  編集ボタンをクリックすると一括編集画面に移動します。

パネル	説明
Unassigned (左)	未割り当てリストで、***をクリックして割り当て
Assigned (右)	割り当てリストで、**-**をクリックして割り当て解除

- 一括編集画面で**保存**ボタンをクリックして変更内容を保存します。

タスク設定

Networkオートメーションを使用すると、ネットワークデバイスにSSHで接続してコマンドを自動実行できます。たとえば、ルーターの設定ファイルを毎日バックアップしたり、特定のイベントが発生したときに診断コマンドを自動実行するタスクを登録できます。

タスクを追加するには、対象デバイスにSSHで接続できるアカウント情報（ユーザー名・パスワードまたはSSHキーファイル）が必要です。

タスク一覧の確認

Networkオートメーション>タスク設定に移動すると、登録済みのタスク一覧を表示できます。画面上部のマネージャー選択ドロップダウンでNMSマネージャーを選択し、検索フィールドにデバイスエイリアス、ホスト、ユーザー名、メモを入力してタスクをすばやく検索できます。

画面上部にステータス別のタスク数が表示されます。チップをクリックすると、該当ステータスのタスクのみ絞り込まれます。

チップ	説明
全体	登録済みタスクの合計数
有効	現在有効化されて実行中のタスク数
無効	一時停止中のタスク数
スケジュール済み	定期的に自動実行されるタスク数

一覧の主要情報

タスク一覧で確認できる主要情報です。

カラム	説明
番号	タスクの順番
有効	緑の点（点滅）は有効、グレーの点は無効状態
エイリアス	デバイスエイリアス。クリックすると該当タスクの実行履歴へ移動
ホスト	デバイスのIPアドレスまたはホスト名
ユーザー名	SSHログインアカウント名
ポート	SSH接続ポート
認証方式	パスワード または キーファイル
スケジュール	manual（手動）、every N分（定期実行）、detector（イベントトリガー）
コマンド	タスクに登録されたコマンド数
リトライ	失敗時のリトライ回数
キーファイル	キーファイル認証使用時のファイル名
タイムアウト	コマンド実行の制限時間
最終ステータス	最終実行結果： success、failure、pending
最終実行時刻	最終実行時刻
次回実行時刻	次回の予約実行時刻（manualの場合は表示なし）
メモ	タスクの説明メモ

タスクの追加

1. 右上のタスク追加ボタンをクリックします。
2. ポップアップで各項目を設定し、**保存**をクリックします。

ステップ1：基本情報の入力

どのデバイスにどのアカウントで接続するかを設定します。

フィールド	必須	説明
デバイス	必須	コマンドを実行する対象デバイスを選択
ユーザー名	必須	SSHログインアカウント名
SSHポート	必須	SSHポート。デフォルト（22）以外の場合のみ変更
デバイスタイプ	必須	CLIドライバーのタイプ。不明な場合は自動検出をオンにすると、タスク設定の保存時にサーバーが自動判別
有効化		タスク設定の有効/無効
リトライ回数	必須	ネットワークが不安定な環境では1～3回の設定を推奨
タイムアウト (秒)	必須	応答が遅いデバイスの場合はデフォルト値より高く設定
メモ		タスク情報のメモ

ステップ2：実行タイミングの選択（スケジュール）

このタスクをいつ実行するかを決定します。

スケジュールタイプ	使用場面
Manual	必要なときに手動で実行ボタンを押す方式。自動実行が不要な場合
Scheduler	毎N分ごと、または毎日特定の時刻に自動実行。定期バックアップ・収集に適切
Detector	特定のイベントや条件が検出されたときに自動実行。障害対応の自動化に適切

ステップ3：SSH認証方式の選択

認証方式	使用場面
パスワード	SSHパスワードを直接入力。すぐに開始したい場合
キーファイル	SSHキーファイルで認証。パスワードなしで安全に接続したい場合。キーファイルは事前にSSHキー管理でアップロードが必要

ステップ4：実行コマンドの登録

実行するコマンドを順番に追加します。コマンドは1つ以上必要です。

1. + コマンド追加ボタンをクリックしてコマンドを入力します。
2. ↑↓ボタンで実行順序を調整します。
3. コマンドごとに説明を記入しておく、後から確認しやすくなります。

保存前の接続テスト

保存前に接続確認を行うことを推奨します。

1. 接続テストボタンをクリックします。
2. 結果がポップアップ下部に表示されます。
 - 成功：接続プロンプトのプレビュー
 - 失敗：エラーの種類と原因メッセージ

タスクの編集・即時実行・削除

一覧右側のアクションボタンで各操作を実行します。

ボタン	説明
編集	設定ポップアップが開き、既存の値を修正できます
即時実行	確認後すぐにタスクを実行。結果はタスク状況で確認できます
削除	タスクを削除。削除すると実行履歴も合わせて削除されます

SSHキーファイル管理

キーファイル認証を使用するには、事前にキーファイルを登録する必要があります。右上のSSHキー管理ボタンをクリックしてください。

操作	方法
アップロード	.pem などのSSH秘密鍵ファイルを選択してファイル名を入力。パスフレーズ付きのキーの場合はパスフレーズも入力
削除	一覧から使用しなくなったキーファイルを削除

タスク状況

タスク状況では、オートメーションタスクの実際の実行履歴と各コマンドの出力結果を確認できます。タスクが想定どおりに動作しているかの確認や、失敗原因の調査に使用します。タスク設定画面でデバイスエイリアスをクリックすると、該当タスクの実行履歴がフィルタリングされた状態で開きます。

結果の検索（フィルター）

実行履歴が多い場合はフィルターで範囲を絞ります。すべてのフィルターをリセットするにはリセットボタンをクリックします。

フィルター	使用方法
マネージャー選択	NMSマネージャーを選択
タスク	特定タスクの結果のみ表示したい場合に選択
コマンド	コマンド名で検索
ステータス	成功または失敗のみ絞り込んで表示したい場合に選択
開始日・終了日	特定期間の実行履歴のみ照会
表示件数	一度に読み込む最大件数（100 / 500 / 1000 / 5000）

実行結果サマリー

フィルターの下に現在の照会結果のサマリーが表示されます。

項目	説明
全体	照会された実行件数の合計

項目	説明
成功	成功で完了した件数
失敗	失敗で終了した件数

実行履歴一覧

最新の実行順に一覧が表示されます。

カラム	説明
実行時刻	タスクが実行された時刻
ホスト	実行対象デバイスのホスト名
エイリアス	デバイスエイリアス
コマンド	実行されたコマンド
ステータス	成功（緑） / 失敗（赤）
所要時間	コマンド実行にかかった時間（例：1.234s）
エラー	失敗時のエラーメッセージ（長い場合は省略記号で表示。カーソルを合わせると全文確認可能）

実行結果の詳細表示

- 一覧で行をクリックすると、該当コマンドの全出力が下に展開されます。
- 出力内容を活用します。
 - コピー：クリップボードにコピー
 - ダウンロード：テキストファイルとして保存（ファイル名形式：

automation_YYYY-MM-DD_エイリアス_ID.txt)

3. ステータスが 失敗 の行をクリックすると、エラーメッセージとともにコマンドがどこまで実行されたかを出力で確認できます。

設定変更履歴

設定変更履歴では、オートメーションタスクが収集したデバイス設定ファイルのスナップショットを照会し、以前の状態と比較して何が変わったかを確認できます。たとえば、ルーターの設定バックアップタスクを毎日実行している場合、この画面で「昨日と今日の設定がどのように異なるか」を行単位で確認できます。

設定変更履歴は、タスク作成時に設定変更トラッキングオプションが有効化されたタスクでのみ収集されます。

フィルター

画面上部で照会範囲を設定します。

フィルター	使用方法
マネージャー選択	NMSマネージャーを選択
タスク	特定タスクの履歴のみ表示したい場合に選択
開始日/終了日	照会する日付範囲 - データ保存期間内の日付のみ選択可能。デフォルトでは直近30日以内のデータを照会できます
表示件数	一度に読み込む最大件数（100 / 500 / 1000 / 5000）
範囲	変更のみ：設定が実際に変更されたスナップショットのみ表示 全体：変更の有無に関わらず全件表示

変更状況概要

フィルターの下の変更状況概要パネルで全体の状況をすばやく把握できます。ヘッダー右側の矢印でパネルの折りたたみ/展開ができ、パネルと一覧の間の区切り線をドラッグして高さを調整できます。

統計

項目	説明
全体	照会期間に収集されたスナップショットの合計数
変更あり	前のスナップショットと比較して設定が変更されたスナップショット数

サマリーテーブル

どのデバイス・コマンド・日付で変更が集中したかを、タブごとに上位5件で確認できます。

タブ	内容
変更が多いホスト	設定変更回数が最も多いデバイス一覧。頻繁に変更される機器の把握に利用
コマンド別の影響	最も多くのデバイスに影響を与えたコマンド一覧。変更範囲が広い作業の確認に利用
変更上位日付	設定変更が最も多く発生した日付。特定日に大規模な変更があったかの把握に利用

日別変更チャート

日付別の設定変更件数を棒グラフで表示します。**特定の日付の棒をクリック**すると、その日付のスナップショットのみ一覧に表示されます。全体に戻るには**戻る**ボタンをクリックしてください。

設定スナップショット一覧

収集されたスナップショットの一覧です。各行はタスクが1回実行されたときにキャプチャされた設定ファイルの状態を表します。

カラム	説明
番号	スナップショットの順番

カラム	説明
キャプチャ時刻	スナップショットがキャプチャされた時刻
ホスト	対象デバイスのホスト名
エイリアス	デバイスエイリアス
コマンド	設定を収集したCLIコマンド
追加	前のスナップショットより増えた行数（緑）
削除	前のスナップショットから削除された行数（赤）
変更	<code>modified</code> （変更あり、オレンジ） / <code>unchanged</code> （変更なし、グレー） / <code>initial</code> （初回収集）
詳細	照会ボタンで変更内容の詳細を確認

変更内容の詳細表示

1. 一覧で照会ボタンをクリックするとポップアップが開きます。
2. ポップアップ上部でホスト、エイリアス、コマンド、変更ステータスを確認します。上部サマリーは矢印をクリックして折りたたむことができます。
3. 見やすい比較モードを選択します。

比較モード

モード	説明
Unified	追加（緑の+）・削除（赤の-）行を1つのビューに順番に表示。 <code>git diff</code> と同様の形式
Split	以前の設定と現在の設定を左右に並べて比較。全体のコンテキストを同時に確認したい場合
Simple	変更された行のみ色で強調してシンプルに表示。素早く確認したい場合

予防点検プロファイル

予防点検は、ネットワーク自動化タスクに登録されたコマンドの一部を点検項目として指定し、各項目に判定ルールをマッピングして実行結果を自動的に点検する機能です。タスクが実行されるたびに、マッピングされたルールに従って正常・警告・重大の状態を自動判定したレポートが生成されるため、繰り返し行う点検項目を標準化し、しきい値ベースの異常有無を手で確認しなくても把握できます。ネットワーク機器を繰り返し点検するネットワーク管理者やインフラエンジニアを対象としています。

プロファイルは、この予防点検の点検テンプレートです。どのオートメーションタスクのコマンドを点検対象にするか、各コマンドの結果にどの項目ラベルと判定ルールを適用するかを定義します。

プロフィール一覧の確認

ネットワーク自動化 > 予防点検プロファイルに進むと、登録されたプロフィールの一覧を確認できます。画面上部のマネージャー選択ドロップダウンでNMSマネージャーを先に選択しないと一覧は表示されません。

一覧の主な情報

カラム	説明
番号	一覧の順番
プロフィール	プロフィール名。クリックすると編集ポップアップが開く
オートメーションタスク	プロフィールが連携するオートメーションタスクのデバイスエイリアスまたはホスト
対象	タスクが実際に接続するデバイスアドレス
コマンド	プロフィールに登録された点検コマンドの数
最新レポート	直近に生成されたレポートの状態(正常・警告・重大・不明)バッジと生成時刻
プロフィール有効	有効化の可否を有効化・無効化バッジで表示。一覧から直接切り替えることはできず、編集ポッ

カラム	説明
化	プアップでのみ変更可能
アクション	詳細表示・修正・削除アイコン。詳細表示と修正は同じ編集ポップアップを開きます

❗ 検索欄にプロファイル名を入力すると、一覧をすぐに絞り込めます。

プロファイルの追加・修正

1. 右上のプロファイル追加ボタンをクリックします。既存のプロファイルを修正する場合は、一覧の修正アイコンをクリックしてください。
2. ポップアップで各項目を設定し、プロファイル保存ボタンをクリックします。

ステップ1: 基本情報の入力

フィールド	必須	説明
プロファイル名	必須	点検テンプレートを区別する名前
オートメーションタスク	必須	点検対象にするオートメーションタスクを選択。すでに他のプロファイルで使用中のタスクは一覧から除外されます
プロファイル有効化		有効化トグル。デフォルトは有効化
メモ		プロファイルの説明メモを記入

オートメーションタスクを選択すると、選択したタスクのCLIドライバー・スケジュール・直近の実行結果・コマンド数をサマリーカードで確認できます。

ステップ2: 点検項目のマッピング

選択したオートメーションタスクに登録されたコマンドが、実行順にテーブルへ表示されます。各行でコマンドごとの点検方法を設定します。

カラム	フィールド	説明
使用	チェックボックス	チェックを外したコマンドはプロファイルに保存されません
オートメーションコマンド	テキスト(読み取り専用)	タスクに登録された元のコマンド
項目ラベル	入力フィールド	レポートに表示する点検項目名を入力してください
パーサー使用	ドロップダウン	下のマッチフィールドを選択するには 使用 を選択する必要があります
マッチフィールド	ドロップダウン	コマンドの実行結果をパースしたカラムのうち、判定に使うカラムを選択してください。パースに失敗したコマンドは直接入力してください
適用ルール	ドロップダウン	この項目に適用する判定ルールを選択してください。ルールがない場合は ルールなし を選択してください

右上の**ルール管理**ボタンを選択すると、ルール編集ポップアップがプロファイル編集ポップアップの上に重なって開きます。新しいルールを登録した後、すぐに**適用ルール**ドロップダウンで選択できます。

-  コマンドの実行結果が表形式でパースされると、**マッチフィールド**ドロップダウンに実際のカラム名が自動的に入力されます。パースに失敗した場合は、**マッチフィールド**に値を直接入力してください。

プロフィールの削除

1. 一覧の削除アイコンを選択すると、確認ダイアログが表示されます。
2. 確認を押すとプロフィールが削除されます。

予防点検ルール

ルールは、[予防点検プロファイル](#)の点検項目ごとに適用する判定基準です。コマンドの実行結果がルールの条件を満たすと、警告または重大の状態に自動判定されます。1つのルールを複数のプロファイルの点検項目で再利用できるため、しきい値や判定条件をルール1つだけ変更すれば、連携するすべての項目に反映されます。

ルール一覧の確認

ネットワーク自動化> 予防点検ルールに進むと、登録されたルールの一覧を確認できます。画面上部のマネージャー選択ドロップダウンでNMSマネージャーを先に選択しないと一覧は表示されません。

一覧の主な情報

カラム	説明
番号	一覧の順番
ルール名	ルール名
判定方式	<code>threshold</code> (しきい値) ・ <code>count</code> (件数) ・ <code>contains</code> (文字列包含) ・ <code>regex</code> (正規表現)のいずれかをバッジで表示
警告条件	警告と判定する条件。 <code>contains</code> ・ <code>regex</code> 方式では使用しないと表示
重大条件	重大と判定する条件。 <code>contains</code> ・ <code>regex</code> 方式では値のみ表示(例: <code>down</code>)
単位	しきい値の単位。 <code>contains</code> ・ <code>regex</code> 方式では使用しないと表示
アクション	修正 ・ 削除アイコン

ルールの追加・修正

1. 右上のルール追加ボタンをクリックします(既存のルールを修正する場合は、一覧の修正アイコンをクリックしてください)。
2. ポップアップで各項目を設定し、保存ボタンをクリックします。

フィールド	必須	説明
名前	必須	ルールを区別する名前
判定方式	必須	下の表を参照し、点検結果に合った方式を選択してください
警告条件		判定方式がしきい値・件数の場合のみ演算子と値を入力。文字列包含・正規表現は値のみ入力
重大条件		警告条件と同じ入力ルール
単位		判定方式がしきい値・件数の場合のみ入力
説明		ルールの説明メモ。任意項目

判定方式別の動作

判定方式を変更すると、入力フィールドが自動的に切り替わります。

判定方式	演算子	値	単位	判定基準
threshold (しきい値)	>= ・ > ・ == ・ != から選択	数値として解釈される文字列	使用	結果値が指定した数値条件を満たすかを判定
count (件数)	>= ・ > ・ == ・ != から選択	数値として解釈される文字列	使用	条件に一致する結果行の件数で判定
contains (文字列包含)	使用しない	検索する文字列	使用しない	実行結果に指定した文字列が含まれるかを判定

判定方式	演算子	値	単位	判定基準
regex (正規表現)	使用しない	正規表現パターン	使用しない	実行結果が正規表現パターンに一致するかを判定

ルールの削除

一覧の削除アイコンを選択すると、次の確認メッセージが表示されます。

 このルールを削除しますか？

このルールを使用中のプロファイルのマッピングはルールなし状態になります。続行しますか？

確認を押すとルールが削除され、このルールを使用していたプロファイルの点検項目はルールの連携のみが解除されます。項目自体はそのまま維持されます。

予防点検レポート

予防点検プロファイルに連携するオートメーションタスクが実行されるたびに、マッピングされたルールに従って判定したレポートが自動的に生成されます。レポートを確認すると、どのデバイスのどの点検項目が異常状態かを一目で把握できます。プロファイルごとに直近2件のレポートのみが保持され、最新レポートには直前のレポートと比較した状態変化の情報も併せて表示されます。

レポート一覧の確認

ネットワーク自動化> 予防点検レポートに進むと、プロファイルごとの最新レポート一覧を確認できます。画面上部のマネージャー選択ドロップダウンでNMSマネージャーを先に選択しないと一覧は表示されません。

ⓘ 一覧は自動的に更新されません。初回アクセス時とマネージャーを変更したときのみ自動で照会され、それ以降は画面上部の更新ボタンを選択しないと最新状態に更新されません。

上部サマリーカード

一覧の上に、状態別のプロファイル数を要約したカードが表示されます。カードを選択すると一覧が該当の状態でフィルタリングされ、選択したカードは枠線で強調されます。

カード	説明
点検対象	レポート生成対象となる全プロファイル数
報告済み	今回の照会期間にレポートが生成されたプロファイル数
未報告	まだレポートが生成されていないプロファイル数。選択するとカラム構成が異なる別の一覧に切り替わります
正常	正常と判定されたプロファイル数

カード	説明
警告	警告と判定されたプロファイル数
重大	重大と判定されたプロファイル数
不明	判定できない状態のプロファイル数

一覧の主な情報

カラム	説明
番号	一覧の順番
デバイス	レポート対象デバイス。クリックするとマネージャー情報画面に移動
プロファイル	レポートを生成したプロファイル名。クリックするとレポート詳細ポップアップが開く
生成時刻	レポートが生成された時刻
点検項目数	レポートに含まれる点検項目の数
結果サマリー	正常・警告・重大・不明の項目数を色分けして要約表示
トリガー	レポートを生成した実行方式(scheduler・manual・detector)バッジ
アクション	詳細表示アイコン

❗ 未報告カードを選択すると、テーブルにはまだレポートがないプロファイルの一覧が代わりに表示され、プロファイル名・連携するオートメーションタスク・点検項目数のみが表示されます。

レポート詳細の確認

1. 一覧でプロファイルをクリックすると、レポート詳細ポップアップが開きます。
2. 上部に**全体項目数/正常/警告/重大/不明**の件数がカードで表示され、下には点検項目ごとの詳細結果が並びます。
3. 各項目は、実行結果のパス成否によって表示が異なります。
 - **パス成功:** 点検項目の結果を表形式で表示し、適用されたルールの判定条件文言(例: **警告** ≥ 10 / **重大** ≥ 30)と判定理由、直前のレポートと比較した状態変化を併せて表示します。**元データ表示**を選択すると、コマンドの元の実行結果を確認できます。
 - **パス失敗:** 「サポートしていないか、パスできません」という案内とともに、元の実行結果をそのまま表示します。

直前のレポートとの比較

各点検項目には、直前のレポートと比較した情報も併せて表示されます。

状況	表示内容
比較する直前のレポートがない	直前のレポートがない旨の案内
直前のレポートと状態が同じ	状態変化なしの案内
直前のレポートと状態が異なる	直前の状態から現在の状態に変わったことを強調表示(例: 警告 → 重大)

SNMP OID管理

ホーム画面 > プロジェクト選択 > 設定 > SNMP OID 管理

SNMP OID 管理メニューでSNMP Pollingを通じて収集するOIDを登録できます。OIDは、ネットワーク機器の様々な性能指標を収集するための識別子です。

基本画面

基本的にOIDは、システムにあらかじめ登録されており、特定デバイスの専用指標を収集するために追加できます。追加されたOIDは、デバイス管理画面で該当デバイスに接続してSNMP Pollingを通じてデータを収集するために使用されます。

OID追加

特定の機器が提供するユーザー定義指標を収集するには、OIDを手動で追加できます。

1. 左上でエージェントを選択します。
2. 右上で+ OIDの追加ボタンをクリックした後OIDの追加画面で次の情報を入力します。

OID, Description, Manufacture, Category

❗ **Category**は、各OIDが収集するリソースを定義するために使用されます。これにより、OIDが収集する指標を分類し、管理できます。

OID修正

OIDリストの左側Editコラムで✎修正アイコンを選択して、関連情報を修正できます。

警告アラート

監視対象のシステムまたはアプリケーションで問題が発生した際に、あらかじめ設定した条件に基づいてユーザーへ通知を送信する機能です。通知は、メール、SMS、メッセージャー、アプリのプッシュ通知など、さまざまなチャネルを通じて配信されます。

たとえば、CPU 使用率、メモリ使用量、ディスク I/O、ネットワークトラフィック、トランザクション数、エラー発生、レスポンスタイムの遅延などの主要なパフォーマンス指標にアラート基準を設定しておく、その基準を超過した場合や異常な兆候が検出された際に通知が送信されます。

WhaTap の AI ベースのアラート機能を使用すると、複雑な条件を手動で設定する必要はありません。AI がアプリケーションの正常な動作パターンを学習し、異常パターンを自動的に検知して通知します。また、タグカウントアラート機能を活用することで、特定のタグを基準に集計された値に条件を設定でき、複雑な状況でも高精度な検知が可能です。

主な機能

- ・ **イベント設定:** 閾値ベースのアラート条件および通知チャネルの設定
- ・ **通知設定:** ユーザーごとの通知チャネルおよび時間帯設定
- ・ **イベント履歴:** アラート発生履歴の確認

権限

イベントを追加または設定するには、**アラート設定権限** が必要です。

- ・ **閲覧:** メトリクスイベント設定を確認するには、**閲覧・分析権限** が必要です。
- ・ **追加／編集／削除:** 設定を変更するには、**アラート設定権限** が必要です。
- ・ **通知受信:** 通知を受信するには、**通知受信権限** が必要です。

📌 参考資料

詳細については、[メンバー権限](#) を参照してください。

イベント設定

ホーム画面 > プロジェクト選択 >  アラート通知 > イベント設定

イベント設定では、監視対象のシステムやアプリケーションで発生する可能性のある異常兆候を基準に、イベントを設定・管理できます。設定した条件が満たされると、メール、SMS、メッセージャー、アプリのプッシュ通知など、希望するチャンネルで通知を受信できます。監視の目的に応じて、イベントを柔軟に構成できます。

メトリクス

メトリクスイベントは、リアルタイムデータを基にシステムおよびアプリケーションのパフォーマンス指標を監視できます。

複合メトリクス

複合メトリクス機能では、複雑なルールを活用してイベントを作成し、警告アラートを送信できます。

リアルタイムログ

リアルタイムで収集されたログから設定したイベント条件が検出された場合、警告アラートを送信します。

複合ログ

ログの内容を基準に警告通知を発生させる複合ログイベントを設定します。

ホーム画面 > プロジェクト選択 >  アラート通知 > イベント設定

イベント設定では、監視対象のシステムやアプリケーションで発生する可能性のある異常兆候を基準に、イベントを設定・管理する機能を提供します。設定した条件を満たすと、メール、SMS、メッセージャー、アプリプッシュなど、希望するチャンネルで通知を受信できます。監視目的に応じてイベント構成を設計できます。

メトリクス

メトリクスイベントは、リアルタイムデータを基にシステムおよびアプリケーションのパフォーマンス指標を監視できます。

複合メトリクス

複合メトリクス機能では、複雑なルールを活用してイベントを作成し、警告アラートを送信できます。

リアルタイムログ

リアルタイムで収集されたログから設定したイベント条件が検出された場合、警告アラートを送信します。

複合ログ

ログの内容を基準に警告通知を発生させる複合ログイベントを設定します。

参考

- イベント設定時は、不要なイベント発生を防ぐために適切なしきい値を設定してください。
- 通知設定では、問題解消時に通知される回復通知もあわせて検討すると、運用対応に役立ちます。

共通機能

すべてのイベント設定は **JSON または Excel 形式** でダウンロードできます。同じ種類のプロダクト設定を共有することで、繰り返し発生するイベント設定作業を削減できます。

- **JSON 一括編集:** すべてのイベント条件を JSON 形式で一括編集できます。
- **JSON 一括ダウンロード:** 現在登録されているイベント条件を JSON ファイルとして保存できます。

- **Excel 一括ダウンロード:** イベント一覧を Excel ファイルとしてダウンロードし、外部レポートやバックアップに活用できます。

JSON 一括編集

1. 画面上部の [JSON 一括編集] ボタンをクリックします。
2. **JSON 一括ダウンロード** 機能でダウンロードした JSON ファイルを読み込むか、直接編集します。
3. [上書き] ボタンをクリックして保存します。
4. 確認メッセージが表示されたら、[上書き] ボタンをクリックします。

❗ 上書き後は、以前のイベント設定に戻すことはできません。

- `productType` または `platform` プロパティの値を任意に変更すると、他のプロジェクトでイベントが正常に動作しなくなる可能性があります。
- JSON 編集画面には検証機能が組み込まれています。形式や値が正しくない場合、編集画面下部にエラーメッセージが表示され、[上書き] ボタンは無効になります。

```

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

```

❗ 「criticalEnabled」には、「string」タイプではなく、「boolean」タイプの値が必要です。

読み込み キャンセル 適用

JSON データ構造



```

{
  "productType": "{productType}",
  "platform": "{platform}",
  "events": {
    "HITMAP": {
      ...
    },

```




```

"LOG_REALTIME": [
  {...}
],
"METRICS": [
  {...}
],
"COMPOSITE_LOG": [
  {...}
],
"BASIC": [
  {...}
],
"COMPOSITE_METRICS": [
  {...}
],
"ANOMALY": [
  {...}
]
}
}

```

JSON フィールド	説明
productType	プロダクトタイプ（例: APM、Infra など）
platform	プラットフォーム情報（例: java、node など）
events	イベントデータ
└ HITMAP	ヒットマップパターン
└ LOG_REALTIME	リアルタイムログイベント
└ METRICS	メトリクス
└ COMPOSITE_LOG	複合ログイベント



JSON フィールド	説明
└ BASIC	基本イベント
└ COMPOSITE_METRICS	複合メトリクス
└ ANOMALY	異常値

JSON 一括ダウンロード

画面上部の [JSON 一括ダウンロード] ボタンをクリックします。

- JSON ファイル名は `integrated-event-YYYYMMDD.json` 形式です。
- JSON データの構造や `events` 属性配下のサブ属性は、プロダクト（ `platform` ）またはプロダクトタイプ（ `productType` ）によって異なる場合があります。

⚠ JSON データ内の `productType` または `platform` プロパティの値を任意に変更すると、他のプロジェクトでイベントが正常に動作しなくなる可能性があります。

Excel 一括ダウンロード

画面上部の [Excel 一括ダウンロード] ボタンをクリックします。

メトリクス

ホーム > プロジェクト選択 >  アラート通知 > イベント設定 > メトリクス タブ

プロジェクトに設定されているすべてのメトリクスベースのイベント一覧を確認できます。設定済みのメトリクスイベントを確認、修正、削除したり、新しいイベントを追加したりできます。

基本オプション

- **イベントレベル:** イベントの深刻度を示し、正常（Info）、警告（Warning）、危険（Critical）の3段階に分類されます。
- **エージェント重複アラート抑止:** 同じ名前のエージェントが同時に2つ以上動作している場合、選択した時間（30秒、1分、3分、5分、10分）の間はイベントが発生しません。
- **検索:** イベント名を基準に検索します。
- **JSON ダウンロード／アップロード:** JSON エディタでイベントルールを直接編集するか、ファイルとしてダウンロードして編集後に再アップロードできます。
- **+ イベント追加:** 新しいメトリクスイベントを追加します。
- **カラムサイズ調整:** 各カラムの境界をドラッグして幅を調整できます。

表 | メトリクスイベント一覧構成

項目	説明
No.	イベントの番号
	イベントの有効化状態 – 有効: 条件を満たすとイベントが発生 – 無効: イベントは動作せず、条件も評価されません
	イベント設定の編集および削除
イベント名	ユーザーが指定したイベント名 – 最大255文字

項目	説明
ルール	イベント発生条件
対象	イベントが適用される監視対象
発生回数	イベント発生の基準となる期間と回数 - 選択した時間内に設定回数分条件を満たすとイベントが発生
一時停止	アラート発生後、同一イベントの発生を一定時間停止 - 選択可能時間: 使用しない、5分、10分、15分、20分、30分、1時間、2時間、3時間、6時間、12時間、1日 - 回復通知が有効な場合、RECOVERED（正常）通知後、選択した時間は同一イベントが発生しても通知されません
回復通知	Critical および Warning レベルのイベントが解消された際に、RECOVERED（正常）通知を受信するかどう - 有効: 進行中から正常状態に遷移すると RECOVERED 通知を送信し、イベント履歴で進行中／解消状態を区別して確認可能 - 無効: しきい値を超えるたびに単発イベントが発生
イベント受信	該当イベント通知を受信するユーザーまたはグループ（受信タグ）

イベント設定

メトリクスイベントは、監視対象で発生する事象を条件に基づいて定義し、効率的に通知を受信できるよう設定するための機能です。

イベント追加

メトリクスイベントを追加するには、**イベント設定** > **メトリクス** タブに移動し、右上の [+ イベント追加] ボタンをクリックします。

メトリクスイベント追加手順
Step 1. テンプレート選択: イベントの基本構成を選択します。
Step 2. イベント条件定義: どの条件でイベントを発生させるかを設定します。
Step 3. イベント対象選択: イベントが適用される監視対象を選択します。
Step 4. 基本情報および通知設定: イベント名、メッセージ、受信対象を設定します。

テンプレート選択

1. イベントの構成方法に応じて、画面左側の3つのテンプレートのいずれかを選択します。
 - **新規作成:** カテゴリやメトリクスを一から自由に構成できます。複雑な条件や詳細な監視ルールが必要な上級ユーザーに適しています。
 - **クイック設定:** あらかじめ定義されたカテゴリ、メトリクス、基本しきい値が提供され、しきい値のみを調整して素早く適用できるため、初心者に適しています。
 - **高度な設定:** あらかじめ定義されたカテゴリやメトリクスを基に、条件を追加したり自由に変更したりできます。

❗ メトリクスイベントでは、さまざまな設定方法をサポートしています。利用する監視プラットフォームによって、提供されるテンプレートは異なる場合があります。

イベント条件定義

イベント条件定義のステップでは、イベント発生の判断に使用するメトリクス設定、発生回数、一時停止、回復通知、イベント動作時間を設定します。

指標設定

1. 検索欄にカテゴリを入力するか、カテゴリー一覧からカテゴリ（指標）を選択します。
指標設定を進めるには、カテゴリの選択が必要です。

- カテゴリ一覧では、カテゴリ名、データ収集間隔、キーを確認できます。直近3時間にプロジェクトで収集されたメトリクスデータが表示されます。

2. 一覧にない指標を使用する場合は、**直接入力**を選択してカテゴリを手動で入力します。

❗ カテゴリや指標が不明な場合は、メトリクス照会を活用してください。

初めて指標を設定する場合、メトリクス照会を利用すると効率的に指標を見つけられます。

- メトリクス照会で指標を検索すると、関連するカテゴリや詳細情報を確認できます。
- 検索結果から必要なメトリクスの[選択]ボタンをクリックすると、選択した値がイベント設定画面に自動的に反映されます。

メトリクス検索

All 13件 / 全 149 件

カテゴリ	名前	単位	タイプ	詳細	マージ	
ApplicationHostResource	CpuSys	pct	field	System領域のCPU使用率	OM: avg TM: avg	選択
ApplicationHostResource	CpuIrq	pct	field	Interrupt Request (IRQ)を使用したCPU使用率	OM: avg TM: avg	選択
ApplicationHostResource	CpuSteal	pct	field	実際にCPUを待機する時間を%で表示した値	OM: avg TM: avg	選択
ApplicationHostResource	CpuCores	count	field	CPUコア数	OM: avg TM: avg	選択
ApplicationHostResource	CpuUser	pct	field	User領域のCPU使用率	OM: avg TM: avg	選択
ApplicationHostResource	CpuProc	pct	field	Proc領域のCPU使用率	OM: avg TM: avg	選択
ApplicationHostResource	Cpu	pct	field	CPU使用率	OM: avg TM: avg	選択
ApplicationHostResource	CpuWait	pct	field	ディスク入出力を待つ間(wait)に使用したCPU使用率	OM: avg TM: avg	選択
ProcessPrivateMemory	PrivateMemory	count	field	Number of Bytes Private		

< 1 > 50件 / ページ

3. イベントレベル（Critical、Warning、Info）を選択します。1つの指標に対して複数のレベルを設定できます。

❗ イベントレベルの動作

複数の条件を満たしても、最も優先度の高いレベル（Critical → Warning → Info）のみがイベントとして発生します。詳細は [レベル動作ガイド](#) を参照してください。

- イベントレベルは、危険（Critical）、警告（Warning）、正常（Info）に分類されます。
- 同一指標に対して段階的なしきい値でレベルを設定することを推奨します。

4. 選択したイベントレベルのフィールド、演算子、値を入力します。

a. + 追加 をクリックすると条件を追加できます。

- && : すべての条件を同時に満たした場合 にイベントが発生
- || : いずれか 1 つ以上の条件を満たした場合 にイベントが発生

b. - をクリックすると、その条件が削除されます。

❗ 条件式の書き方や対応する演算子については、[条件設定ガイド](#) を参照してください。

発生回数

条件が何回満たされた場合にイベントを発生させるかを設定します。継続的な問題のみを検知したい場合に有効です。

1. 発生頻度を選択します。

- 連続: 設定した回数分、イベントが連続して発生した場合にイベントを発生
- 直近: 選択した時間内に、設定した回数分イベントが発生した場合にイベントを発生
 - 選択可能時間: 5秒, 10秒, 15秒, 30秒, 1分, 2分, 3分, 4分, 5分, 10分, 30分, 1時間

2. 発生回数を入力します。

- Interval の値は、選択したカテゴリのデータ収集間隔を示します。(Interval: 10s)

一時停止

過剰なイベント発生を防ぐため、イベント動作を一時停止する時間を選択してください。イベント発生後、設定した時間が経過するまで同一イベントは発生しません。

- 選択可能時間: 使用しない, 5分, 10分, 15分, 20分, 30分, 1時間, 2時間, 3時間, 6時間, 12時間, 1日

❗ 解消通知が有効な場合

正常状態の通知 (RECOVERED) を受信した時点から、設定した時間が経過するまで、同一イベントが再発しても通知は送信されません。

解消通知

解消通知機能を有効にすると、イベント発生後の状態変化（進行中 → 解消）を追跡できます。イベント履歴メニューでは、進行中のイベントとして表示されます。

- 解消通知は **Critical** および **Warning** レベルにのみ適用されます。Info レベルは常に単発イベントとして動作します。
- **Critical** または **Warning** レベルのイベントが解消されると、正常（RECOVERED）状態の通知が送信されます。
- トグルボタンをクリックして **有効化** または **無効化** してください。
 -  **有効**: イベントは状態ベースで動作します。しきい値を超えると進行中となり、値がしきい値未満に回復すると解消状態に遷移します。
 -  **無効**: しきい値を超えるたびに単発イベントが発生します。

イベント動作時間

イベントが特定の時間帯（勤務時間／非勤務時間／点検時間など）にのみ動作するよう、タグを設定してください。タグを設定しない場合、イベントが有効な状態では 24 時間常時動作します。

1. **+ 追加** をクリックします。
2. イベント動作時間で **+ 新しいタグを作成** をクリックします。
3. **イベント動作時間タグ作成** で **タグ名、曜日、時間、色** を選択し、[適用] ボタンをクリックします。
4. 作成したタグはタグ一覧で確認でき、チェックボックスを選択すると適用されます。
5. タグを修正または削除するには、 をクリックし、**イベント動作時間タグ修正** で修正または削除してください。

 タグを削除すると、そのタグが適用されているすべてのユーザーからタグが削除されます。ただし、イベントルールで使用中のタグは削除できません。

シミュレーション

シミュレーション機能では、設定したイベント条件を過去データに基づいて事前にテストできます。想定されるイベント件数が多いすぎる、または少なすぎる場合は、条件を調整して最適なしきい値を見つけることができます。

- **ルール検証:** 新しく作成したイベントルールを過去データに適用した場合の結果を確認できます。
- **しきい値チューニング:** イベントが頻発する、またはまったく発生しない場合に、適切なレベルへしきい値を調整します。

シミュレーション開始

1. イベント条件の設定が完了したら、[シミュレーション] ボタンをクリックします。
2. 想定イベント件数と可視化された結果を確認します。

シミュレーション結果の理解

1. 時系列データ

指標の時間帯別変化と各レベルのしきい線がグラフで表示され、イベント発生タイミングを直感的に確認できます。

2. レベル別発生状況

画面右側に Critical、Warning、Info レベルごとのイベント発生回数が表示され、全体の分布や頻度を把握できます。

3. 対象別詳細情報

グラフ上の特定ポイントにマウスを合わせると、その時点の正確な指標値と監視対象が表示されます。複数の対象がある場合は色で区別され、対象ごとにパターンが異なる場合はフィルタリング機能で個別分析が可能です。

4. ピーク区間の特定

指標が急激に上昇する時間帯を確認し、問題が頻発する時間帯やパターンを把握できます。

🟢 シミュレーション活用のヒント

• 複数時間帯でのシミュレーション

平日／週末、ピーク／非ピーク時間帯をそれぞれシミュレーションし、時間帯ごとの最適なしきい値を設定してください。



- 実際の障害期間を含める

過去に障害が発生した期間を含めてシミュレーションを実行し、現在のルールが障害を正しく検知できるか確認しましょう。

- 対象フィルタリングの追加

監視対象が多い場合、結果が複雑になります。フィルタリング機能を使って特定の対象のみを選択し、明確な結果を確認してください。

- しきい値を段階的に調整

一度に大きく変更するのではなく、10 パーセント単位で段階的に調整しながら最適値を探すことをおすすめします。

イベント対象選択

イベント対象を指定しない場合、プロジェクト内のすべての対象に対してイベントが発生し、多数のイベントが生成される可能性があります。そのため、イベントを適用する対象を明確に設定することを推奨します。

❗ イベント対象を変更すると、イベント件数が変わる場合があります。シミュレーション ボタンをクリックして再実行し、想定イベント件数を確認してください。

対象選択

イベントを適用する対象は、**選択入力** または **直接入力** の方法で指定できます。

- **選択入力** 直接入力

1. タグ、演算子、値を選択または入力してください。
 - a. タグが見つけない場合は、**メトリクス照会** を使ってタグを検索できます。
2. **+ 追加** をクリックして、条件（**&&**、**||**）でイベント対象を追加してください。

監視対象のタグ、演算子、値を直接入力してください。

- 直接入力を選択すると、入力欄の下に使用可能なタグ一覧（**タグ選択入力**）が表示されます。

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

 入力方法を変更すると、作成中の内容は初期化されます。

基本情報および通知設定

イベント名、メッセージ、受信対象を設定します。設定した内容はイベント履歴や実際の通知メッセージにそのまま表示されるため、識別しやすく分かりやすい名称にすることが重要です。

イベント有効化

設定した条件を満たした際にイベントを発生させるかどうかを設定します。

-  **有効**: 設定した条件を満たすとイベントが発生します。
-  **無効**: 条件を判定しません。

イベント名

イベントのタイトルとして使用するイベント名を入力してください。設定したイベント名は **イベント一覧** および **イベント履歴** メニューに表示され、この名前で検索することができます。

メッセージ

イベントメッセージを入力してください。入力したメッセージは、イベント履歴および通知に使用されます。 をクリックすると、過去に作成したメッセージ履歴を確認できます。メッセージには変数を使用して、イベント発生時点の実際の値を含めることができます。

- **変数の使用ルール**
 - 変数形式: `${指標名}`
 - 設定した **カテゴリ** と同一カテゴリ内の指標のみを変数として使用できます。
 - 複数の変数を組み合わせて、より詳細なメッセージを作成できます。
 - 使用可能な変数一覧は **メトリクス照会** メニューで確認できます。

- 変数の使用例

	イベント設定	イベント発生時
タイトル	Disk 使用量増加	Disk 使用量増加
メッセージ	Disk = \${disk}%	Disk = 89.9%

イベント受信

イベント通知を受信するメンバーを指定します。

- 全体受信** タグ選択受信

プロジェクトで通知設定が有効になっているすべての対象（メンバー、チャンネル）に通知が送信されます。

指定したタグを持つプロジェクトメンバーに通知が送信されます。

1. **タグ選択受信** を選択します。
2. **受信タグ** 項目で [+ タグ追加] または [+] ボタンをクリックします。
3. **イベント受信タグ** 画面の下にある + **新しいタグを作成** をクリックします。
4. **タグ作成** 画面でタグ名を入力し、色を選択した後、[タグ作成] ボタンをクリックしてタグを作成します。
5. 作成したタグは、**タグ一覧** の  をクリックして修正または削除できます。
6. **イベント受信タグ** 画面の **タグ一覧** から希望するタグを選択すると適用されます。

ⓘ 受信タグ

受信タグは、通知を受け取るユーザーやチャンネルを **グループ単位で管理するための機能** です。イベントに受信タグを設定すると、そのタグが付与されたユーザーにのみ通知が送信されます。受信タグを設定しない場合、プロジェクト内のすべてのユーザーに通知が送信されます。

イベント修正／削除

1. **警告アラート** > **イベント設定** の **メトリクス** タブに移動します。

2. イベント一覧で、修正または削除したいイベントの  をクリックします。
3. イベントルール修正 画面でオプションを修正し、[保存] ボタンをクリックします。
 - a. 選択したイベントを削除する場合は、イベントルール修正 画面右上の [削除] ボタンをクリックします。

イベント共有

メトリクスイベント設定を JSON ファイルとして保存し、他のユーザーと設定を共有したり、他のユーザーの設定を取り込んだりすることができます。

- JSON ファイル名: `event-rules-YYYYMMDD.json`

エクスポート

1. 画面右上の [JSON ] ボタンをクリックします。
2. JSON 編集画面が表示されたら、[ エクスポート] ボタンをクリックします。
 - イベントを検索した状態でエクスポート機能を使用すると、検索結果のみが JSON ファイルとしてダウンロードされます。
3. JSON ファイルがダウンロードされたら、共有したい他のユーザーに渡してください。

インポート

1. 画面右上の [] ボタンをクリックします。
2. エクスポート 機能でダウンロードした JSON ファイルを選択します。
3. JSON 編集画面が表示されたら、[一覧に追加] または [上書き] を選択します。

 同じ種類の製品間での利用を推奨します。異なる製品のプロジェクトからイベント設定を取り込むことは可能ですが、正常に動作しない場合があります。

JSON 形式で編集する

1. 画面右上の [JSON ] ボタンをクリックします。

2. 編集画面が表示されたら、JSON 形式に従って内容を修正してください。
3. 修正が完了したら、画面下部の [保存] ボタンをクリックします。

❗ 修正した内容が JSON 形式に合っていない場合、画面下部にエラーメッセージが表示され、保存できません。表示されるエラーメッセージは、形式エラーの内容によって異なる場合があります。

JSON error

JSON データ構造

```
{
  "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"
  ]
}
}

```

表 | JSON データ構造

JSON フィールド	型	説明	備考
version	Integer	イベントルールのバージョン	変更制限
eventId	String	イベントルールの一意識別子	
enabled	boolean	イベントの有効／無効	
stateful	boolean	状態ベースイベントかどうか	
title	String	ユーザーが設定したイベントルール名	
message	String	ユーザーが設定したイベントルールメッセージ	
category	String	データカテゴリ	
alertLabel	List<String>	イベント状態管理のため、カテゴリごとに指定される基本識別子（プライマリキー）値	変更制限
repeatCount	Integer	繰り返し回数	
repeatDuration	Long	繰り返し期間	
silent	Integer	一時停止時間	
receiver	List<String>	受信タグのキー値一覧	

JSON フィールド	型	説明	備考
timeTag	List<String>	動作時間タグのキー値一覧	
selectString	String	対象選択	
conditions	List<Object>	レベル別の発生条件一覧	
└ level	byte	レベル値	Critical: 30、Warning: 20、Info: 10
└ enabled	boolean	レベルの有効／無効	
└ rule	String	レベル発生条件	
createTime	Long	イベントルールの初回作成時刻	
lastModifiedTime	Long	イベントルールの最終修正時刻	
lastModifiedUser	String	イベントルールを最後に修正したアカウント	
basic	boolean	クイック設定で作成されたイベントかどうか	変更制限
metald	String	クイック設定テンプレートの一意識別子	変更制限: この値はクイック設定で作成されたイベントにのみ存在します (basic=true)。
selectCondition	Object	クイック設定の対象選択値	この値はクイック設定で作成されたイベントにのみ存在します (basic=true)。

❗ 「変更制限」と表示されたフィールドはイベント動作に影響を与える可能性があるため、値を変更しないことを推奨します。

付録

発生条件・対象選択ガイド

メトリクスアラートにおけるイベントの発生条件とイベント対象の選択は、同一の構文を使用します。ただし、イベント発生条件ではフィールド（Field）のキーを変数として使用し、イベント対象の選択ではタグ（Tag）のキーを変数として使用します。

レベル動作ガイド

イベントレベルは、危険（Critical）、警告（Warning）、正常（Info）の3段階に分類されます。

1. 優先順位に基づくイベント発生

複数のレベル条件を同時に満たした場合、最も優先度の高いイベントのみが発生します。

例

```
設定:  
- Warning: CPU > 70%  
- Critical: CPU > 90%  
  
現在の状態: CPU 95%  
→ 結果: Critical イベントのみ発生（Warning は抑制される）
```

2. レベル上昇

進行中状態を持つイベントにおいて、低いレベルのイベントが進行中の状態で高いレベルの条件を満たすと、両方のレベルが進行中状態になります。

例

```
設定:  
- Warning: CPU > 70%  
- Critical: CPU > 90%  
  
シナリオ:
```

- 1) CPU 80% → Warning 発生 (進行中)
- 2) CPU 95% → Warning (進行中)、Critical (進行中)

3. レベル下降

進行中状態を持つイベントで、高いレベルから低いレベルへ遷移した場合、高いレベルは解消され、低いレベルが維持されます。

例

設定:

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

シナリオ:

- 1) CPU 97% → Critical 発生
- 2) CPU 85% → Critical 解消、Warning 維持
- 3) CPU 65% → Warning 解消

4. 動作フロー

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

メトリクス値: 60% → 75% → 92% → 85% → 60%

状態: 正常 Warning Critical Warning 正常

 (発生) (発生) (維持) (解消)

 Warning

 (維持)

ⓘ 進行中状態を持つイベントは、条件が満たされている間は継続して有効となり、条件が解除されるまで維持されます。

条件設定ガイド

❗ メトリクス名が数字で始まる場合、または特殊文字を含む場合は、`${メトリクス名}` の形式で記述する必要があります。

- 括弧 `()`, `[]`
- 演算子 `+`, `-`, `*`, `/`, `%`
- 区切り文字 `:`, `@`, `#`, `,`, `,`, (空白)
- その他の特殊文字 `!`, `^`, `&`, `|`, `~`, ````, =`

`${}` 使用例:

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

`${}` なしで使用可能: 英字、アンダースコア (`_`)、ドット (`.`) のみを含む場合

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

1. 比較演算子

数値比較

```
より大きい:  cpu > 80
以上:        cpu >= 80
より小さい:  memory < 1000
以下:        memory <= 1000
等しい:      status == 200
等しくない:  error != 0
```

文字列比較

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

2. 算術演算子

- 基本的な算術演算

```
加算:   cpu + 10 >= 90
減算:   memory - 100 >= 500
乗算:   cpu * 2 >= 100
除算:   disk / 1024 >= 100
剰余:   value % 10 == 0
```

- 括弧による優先順位の制御

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

- 負の値の表現

```
cpu > -100
```

3. 論理演算子

- AND 演算 (&&)

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

- OR 演算 (||)

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

- 複合論理演算

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

4. パターンマッチング演算子

- LIKE 演算子

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

- NOT LIKE 演算子

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

5. 組み込み関数

- Null チェック関数

```
isNull(value)      # null かどうかを確認
isNotNull(value)   # null でないかを確認
nvl(value, 0)      # null の場合に既定値を返す
isEmpty(str)       # 空文字列かどうかを確認
isNotEmpty(str)    # 空文字列でないかを確認
```

- 集計関数

```
sum(cpu, memory, disk)    # 合計
avg(cpu, memory)          # 平均
max(cpu, memory, disk)    # 最大値
min(cpu, memory, disk)    # 最小値
count(value1, value2, value3) # 件数
```

- 数学関数

```
round(cpu, 2)    # 四捨五入（小数点以下2桁）
```

- 文字列関数

```
length(str)      # 文字列の長さ
startsWith(str, 'prefix') # 接頭辞の確認
endsWith(str, 'suffix') # 接尾辞の確認
indexOf(str, 'search') # 文字列の位置
substring(str, 0, 10) # 部分文字列
trim(str)        # 空白の削除
replace(str, 'old', 'new') # 文字列の置換
hasStr(str, 'search') # 文字列の包含判定
```

- 条件関数

- **if:** 条件式が `true` の場合は `true値` を返し、`false` の場合は `false値` を返す条件関数

形式

```
if(条件, true値, false値)
```

例

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

- **decode:** 値と条件を比較し、一致した条件の結果を返します。一致しない場合は既定値を返します

形式

```
decode(値, 条件1, 結果1, 条件2, 結果2, ..., 条件N, 結果N, 既定値)
```

例

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

- **in:** 値が指定した候補値のいずれかと一致した場合は `true` 、それ以外は `false` を返します

形式

```
in(値, 候補値1, 候補値2, ..., 候補値N)
```

例

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

❗ 記述時の注意事項

- 推奨事項
 - 簡単な変数名は `${}` を使わずに記述（例: `cpu`, `memory`）
 - 特殊文字を含む場合は必ず `${}` を使用
 - 複雑な演算は括弧で明確に区切る
 - 関数名は正確に入力（大文字と小文字を区別）
- 避けるべき事項
 - 不完全な式の記述（例: `cpu >` , `memory &&` ）
 - 括弧の不一致（例: `(cpu > 80 && cpu > 70)` ）
 - 演算子の連続使用(例: `cpu >> 80` , `cpu >< 80`)

複合メトリクス

ホーム > プロジェクト選択 >  アラート通知 > イベント設定 > 複合指標 タブ

複雑なルールを利用してイベントを作成し、警告通知を送信できます。

基本オプション

- **検索:** イベント名またはイベント受信タグを選択して、目的のイベントを検索します
- **JSON ダウンロード／アップロード:** JSON エディタでイベントルールを直接編集するか、ファイルとしてダウンロードして編集後に再アップロードできます
- **通知メッセージ設定:** 受信するメッセージの詳細項目を選択し、項目ごとに内容を編集します
- **+ イベント追加:** 新しい複合メトリクスイベントを追加します

 権限

複合指標 イベントを設定するには **アラート設定** 権限が必要です。この権限は **ホーム > プロジェクト選択 > 管理 > 統合メンバー管理** で、対象メンバーの  をクリックして付与できます。

表 | 複合メトリクスイベント一覧の構成

項目	説明
イベントタイトル	ユーザーが指定したイベント名 - 最大 255 バイトまで入力可能
条件	イベント発生条件
イベント状態が解消された場合の追加通知	Critical および Warning レベルのイベントが解消された際に、RECOVERED（正常）状態の通知を受信するかどうか - 有効: 進行中 → 正常状態に切り替わると RECOVERED 通知を送信し、イベント履歴で進行中／解消状態を区別して確認できます - 無効: しきい値を超えるたびに単発のイベントが発生します

項目	説明
イベント受信タグ	該当イベントの通知を受信するユーザーまたはグループ
	イベントの修正および削除
	イベントの有効／無効状態 - 有効: 条件を満たすとイベントが発生 - 無効: イベントは動作せず、条件も評価されません

イベント設定

複合指標 イベントは、メトリクスデータのクエリ言語である **MXQL** を基にイベント条件を作成します。**チャートから作成** 機能では、MXQL の自動補完を支援するコンボボックス機能を提供します。

イベント追加

1.  **アラート通知** > **イベント設定** から **複合指標** タブをクリックします。
2. 画面右側の **[+ イベント追加]** ボタンをクリックします。
3. **複合指標** 画面で **チャートから作成** をクリックします。
 - a. 提供されているテンプレートを利用できます。
4. **イベント設定** 画面で、先にイベントデータを取得し、その後イベント条件を設定します。

イベントデータ照会

イベントデータを照会してチャートを構成します。**イベント設定** 画面右側の **イベントデータ照会** で、**ウィジェット** または **テキスト** オプションを選択してイベントを設定します。

• ウィジェット テキスト

時系列チャートを構成するオプションを使用して、イベント設定に利用する **MXQL** を自動補完できます。

1. データを照会する日付を選択します。
2. データを照会する **カテゴリ** (対象) を選択します。

3. **フィルター** 項目の **+フィルター追加** をクリックしてイベント条件を作成します。
 - a. フィルター画面で、演算式、タグ、フィルター値を選択します。
 - b. **+追加** をクリックして条件を追加できます。
 - c. 条件を削除する場合は、条件の横にある **-** をクリックします。
4. **グループ化** 項目で、グループ化されたメトリクスデータを選択します。複数選択が可能です。
5. **タイムユニット** 項目で、**秒**、**分**、**時間** 単位のいずれかを選択し、データを分割する時間基準を設定します。
6. **フィールド** 項目で、イベント発生条件に使用するフィールドを選択します。複数選択が可能です。

 テキストモードで入力した MXQL は、ウィジェットモードと互換性がありません。

MXQL を直接編集できるエディタが表示されます。

1. **MXQL** を直接修正し、**照会** ボタンをクリックします。
2. 日付を選択すると、該当内容をチャートまたはグラフで確認できます。

通知

警告通知設定の基本情報を入力します。

- **イベント有効化**: トグルボタンを有効にすると、イベントが動作します。
- **レベル**: イベントレベル（Critical、Warning、Info）を選択します。
 - **イベント状態が解消された場合の追加通知**: トグルを有効にすると、イベントが解消され、正常（RECOVERED）状態の通知が送信されます。
- **タイトル**: イベントルールのタイトルを入力します。
- **メッセージ**: イベント発生時に受信する通知メッセージの内容を入力します。メッセージ内で変数を使用すると、イベント発生時点の実際の値を含めることができます。

Message example

 変数使用ルール



- 変数形式: \${メトリクス名}
- 設定した **カテゴリ**と同一**カテゴリ** 内のメトリクスのみ変数として使用できます。
- 複数の変数を組み合わせて、詳細なメッセージを構成できます。
- 使用可能な変数一覧は **メトリクス照会** で確認できます。

イベント発行条件

- **データ照会範囲**: リアルタイムデータの照会範囲を選択します。
 - 選択可能な範囲: 30秒, 1分, 2分, 5分, 10分, 30分, 1時間, 2時間, 3時間
- **条件**: イベント発行条件を入力します。イベントデータ照会に含まれるフィールドのみ使用できます。

付加情報

- **インターバル**: 選択した時間間隔（1分, 5分, 10分, 30分, 1時間, 12時間）ごとにアラート条件を確認します。
- **サイレンス**: イベント発生後、選択した時間（unset, 1分, 5分, 10分, 30分, 1時間, 12時間）の間、同一イベントは発生しません。
- **イベント動作時間**: 勤務時間、非勤務時間、点検時間など、特定の時間帯にイベントが動作するようタグを設定します。タグを設定しない場合、イベントは有効な状態で24時間常時動作します。
 1. **+追加** をクリックします。
 2. **イベント動作時間で+新しいタグ作成** をクリックします。
 3. **イベント動作時間タグ作成** で **タグ名**、**曜日**、**時間**、**色** を選択し、**[適用]** ボタンをクリックします。
 4. 作成したタグはタグ一覧で確認でき、チェックボックスを選択すると適用されます。
 5. 修正または削除するタグの をクリックし、**イベント動作時間タグ修正** で編集または削除できます。



タグを削除すると、そのタグが適用されているすべてのユーザーから削除されます。ただし、イベントルールで使用中のタグは削除できません。

- **イベント受信タグ**: 受信タグを設定すると、該当タグを持つプロジェクトメンバーに通知が送信されます。受信タグを設定しない場合、プロジェクト内のすべてのユーザーに通知が送信されます。

1. **+タグ追加** または **+** をクリックします。
2. **イベント受信タグ** 画面下部の **+新しいタグ作成** をクリックします。
3. **タグ作成** 画面でタグ名を入力し、色を選択した後、**[タグ作成]** ボタンをクリックします。
4. 作成したタグは、**タグ一覧** の  をクリックして修正または削除できます。
5. **イベント受信タグ** 画面の **タグ一覧** から適用したいタグを選択します。

✔ イベント設定時にイベント受信タグを選択すると、該当タグを持つプロジェクトメンバーおよび 3rd-party プラグインに通知を送信できます。**アラート通知 > 通知設定** で、それぞれにタグを割り当てることができます。

イベントルールテスト

設定した条件を過去データに基づいてテストし、どの程度のイベントが発生するかを予測できます。

1. イベントルールをテストする日付を選択し、**[確認]** ボタンをクリックします。
2. **[実行]** ボタンをクリックして、イベント発生件数を確認します。

イベント修正／削除

1. **アラート通知 > 通知設定** の **複合指標** タブに移動します。
2. 複合メトリクス一覧で、修正または削除したいイベントの  をクリックします。
3. **通知設定** 画面でオプションを修正し、**[保存]** ボタンをクリックします。
 - a. 選択したイベントを削除する場合は、**通知設定** 画面右上の **[削除]** ボタンをクリックします。

イベント共有

メトリクスイベント設定を JSON ファイルとして保存し、他のユーザーと設定を共有したり、他のユーザーの設定を取り込んだりすることができます。

- JSON ファイル名: **event-rules-YYYYMMDD.json**

エクスポート

1. 画面右上の [JSON ] ボタンをクリックします。
2. JSON 編集画面が表示されたら、[ エクスポート] ボタンをクリックします。
 - イベントを検索した状態でエクスポート機能を使用すると、検索結果のみが JSON ファイルとしてダウンロードされます。
3. JSON ファイルがダウンロードされたら、共有したい他のユーザーに渡してください。

インポート

1. 画面右上の [] ボタンをクリックします。
2. エクスポート 機能でダウンロードした JSON ファイルを選択します。
3. JSON 編集画面が表示されたら、[一覧に追加] または [上書き] を選択します。

 同じ種類の製品間での利用を推奨します。異なる製品のプロジェクトからイベント設定を取り込むことは可能ですが、正常に動作しない場合があります。

JSON 形式で編集する

1. 画面右上の [JSON ] ボタンをクリックします。
2. 編集画面が表示されたら、JSON 形式に従って内容を修正してください。
3. 修正が完了したら、画面下部の [保存] ボタンをクリックします。

 修正した内容が JSON 形式に合っていない場合、画面下部にエラーメッセージが表示され、保存できません。表示されるエラーメッセージは、形式エラーの内容によって異なる場合があります。

JSON error

通知メッセージ設定

受信するメッセージの詳細項目を選択し、項目ごとに内容を編集できます。

付録

MXQL 文法ガイド

複合指標 は MXQL クエリを基に動作します。詳細な文法については、[MXQL 文法ガイド](#) を参照してください。

リアルタイムログイベント

ホーム > プロジェクト選択 >  アラート通知 > イベント設定 > リアルタイムログ タブ

収集したログデータを条件に合わせてフィルタリングして警告通知を設定できます。ログイベントを使用するには、ログモニタリングを有効化する必要があります。**ログモニタリングの有効化**については、各製品のログドキュメントを参照してください。

- ・ **リアルタイムログイベント**: リアルタイムで収集したログで、設定したイベント条件が満たされるとイベントが発生します。

基本オプション

- ・ **検索**: イベント名またはイベント受信タグを選択して目的のイベントを検索
- ・ **JSONダウンロード/アップロード**: イベントルールはJSONエディタで直接編集するか、ファイルにダウンロードして修正後に再アップロード可能
- ・ **通知メッセージ設定**: 受信するメッセージの詳細項目を選択し、項目ごとに内容を編集
- ・ **+ イベント追加**: 新しいログイベントを追加

表 | リアルタイムログイベント一覧構成

項目	説明
イベント名	通知タイトルとして使用されるイベント名 - 最大255バイトまで入力可能
カテゴリ	ログ分類名（ログフォルダ名）
検索キー	ログデータで検索したい項目 - 例: HTTPレスポンスステータスコードの値にアクセスする場合、検索キー <code>status</code>
検索値	検索キーに対応する実際のデータ。ログに入力した文字列が含まれる場合に警告通知を送信 - 例: 検索キー <code>status</code> 、検索値 <code>200</code> を設定した場合、HTTPステータスコード200を含むログデータ収集時に警告通知が発生

項目	説明
イベント発生一時停止	イベント通知発生後、同じイベントの発生を一定時間停止 - 選択可能時間: 使用しない、5分、10分、15分、20分、30分、1時間、2時間、3時間、6時間、12時間、1日 - 解消通知が有効な場合、正常（RECOVERED）状態の通知受信後、選択した時間中は同じイベントが発生しても通知されない
イベント対象フィルタリング	イベントが適用される対象の条件 - 対象条件を設定しない場合、収集されるすべてのデータに対して通知を判断 - 選択入力: タグ、演算子、値を選択して条件を構成 - 直接入力: 条件を直接入力して対象を指定
イベント受信タグ	イベント通知を受け取るユーザーまたはグループ（受信タグ）
	イベントの編集と削除
	イベントの有効化状態 - 有効: 条件を満たすとイベント発生 - 無効: イベントが動作せず、条件をチェックしない

イベント設定

ログイベントは、リアルタイムで収集されるログ、または特定条件を満たすログが一定数蓄積された際に警告通知を設定できる機能です。

リアルタイムログイベントの追加

1. アラート通知 > イベント設定のリアルタイムログタブをクリックしてください。
2. 画面右側の [+ イベント追加] ボタンをクリックしてください。
3. イベントルール追加ウィンドウでログイベント条件を設定してください。
 - イベント名: イベントタイトルとして使用する名前を入力してください。

- **イベント有効化:** トグルボタンを有効にすると、条件を満たしたときにイベントが発生します。
- **レベル:** イベントレベル (**Critical**、**Warning**、Info) を選択してください。
- **メッセージ:** イベント発生時に受け取る通知メッセージを入力してください。メッセージに変数を使用して、イベント発生時点の実際の値を含めることができます。

✔ 変数使用ルール

- 変数形式: \${指標名}
- 設定したカテゴリと同じカテゴリ内の指標のみ変数として使用できます。
- 複数の変数を組み合わせて詳細なメッセージを構成できます。
- 使用可能な変数一覧は**メトリクス照会**で確認できます。

- **カテゴリ:** ログ分類名（ログフォルダ名）をリストから選択するか、直接入力してください。カテゴリを選択してから検索キーと検索値を入力できます。
- **検索キー:** ログデータで検索したい項目を入力してください。
 - 例: HTTPレスポンスステータスコードの値にアクセスする場合、**検索キー** status
- **検索値:** 検索キーに対応する実際のデータを入力してください。ログに入力した文字列が含まれる場合に警告通知を送信します。
 - 例: **検索キー** status、**検索値** 200 を設定した場合、HTTPステータスコード200を含むログデータ収集時に警告通知が発生
- **イベント対象フィルタリング:** イベントが適用される対象の条件を入力してください。入力値がない場合、収集されるすべてのデータに対して通知を判断します。
 - **選択入力:** タグ、演算子、値を選択して対象条件を設定してください。

❗ 条件式の記述方法とサポートされる演算子については、[条件設定ガイド](#)を参照してください。

- **直接入力:** 条件を直接入力してください。
- **イベント発生一時停止:** 通知を一時停止する時間を選択してください。イベント発生後、設定した時間中は同じイベントが発生しません。

- 選択可能時間: 使用しない、1分、2分、3分、5分、10分、20分、30分、1時間、3時間、6時間、12時間
- イベント動作時間: 特定の時間帯（業務/非業務/メンテナンス時間など）にイベントが動作するようにタグを設定してください。タグを設定しない場合、イベントが有効な状態で24時間常時動作します。
 1. + 追加をクリックしてください。
 2. イベント動作時間で**+新しいタグを作成**をクリックしてください。
 3. イベント動作時間タグの作成でタグ名、曜日、時間、色を選択し、[適用] ボタンをクリックしてください。
 4. 作成したタグはタグリストで確認でき、チェックボックスを選択すると適用されます。
 5. 変更または削除するタグの  アイコンをクリックして、イベント動作時間タグの編集でタグを編集または削除できます。

 タグを削除すると、そのタグが適用されているすべてのユーザーのタグが削除されます。ただし、イベントルールで使用中のタグは削除できません。

- イベント受信タグ: イベントに受信タグを設定すると、そのタグを持つプロジェクトメンバーに通知が送信されます。受信タグを設定しない場合、プロジェクト内のすべてのユーザーに通知が送信されます。
 1. + タグ追加または+をクリックしてください。
 2. イベント受信タグウィンドウ下部の**+ 新しいタグを作成**をクリックしてください。
 3. タグ作成ウィンドウでタグ名を入力し、色を選択してから、[タグ作成] ボタンをクリックしてタグを作成してください。
 4. 作成されたタグはタグリストの  アイコンをクリックして編集または削除してください。
 5. イベント受信タグウィンドウのタグリストから目的のタグを選択すると適用されます。

 イベント設定時にイベント受信タグを選択して、そのタグを持つプロジェクトメンバーとサードパーティプラグインに通知を送信できます。アラート通知 > 通知設定でプロジェクトメンバーとサードパーティプラグインにそれぞれタグを指定できます。

4. イベントルール追加ウィンドウで設定が完了したら、[保存] ボタンをクリックしてください。

イベントの編集/削除

1. アラート通知 > イベント設定のリアルタイムログタブに移動してください。
2. ログイベントリストで編集または削除するイベントの  アイコンをクリックしてください。
3. イベント設定画面でオプションを変更し、[保存] ボタンをクリックしてください。
 - a. 選択したイベントを削除するには、イベント設定画面の右上の [削除] ボタンをクリックしてください。

イベントの共有

メトリクスイベント設定を JSON ファイルとして保存し、他のユーザーと設定を共有したり、他のユーザーの設定を取り込んだりすることができます。

- JSON ファイル名: `event-rules-YYYYMMDD.json`

エクスポート

1. 画面右上の [JSON ] ボタンをクリックします。
2. JSON 編集画面が表示されたら、[ エクスポート] ボタンをクリックします。
 - イベントを検索した状態でエクスポート機能を使用すると、検索結果のみが JSON ファイルとしてダウンロードされます。
3. JSON ファイルがダウンロードされたら、共有したい他のユーザーに渡してください。

インポート

1. 画面右上の [] ボタンをクリックします。
2. エクスポート 機能でダウンロードした JSON ファイルを選択します。
3. JSON 編集画面が表示されたら、[一覧に追加] または [上書き] を選択します。

 同じ種類の製品間での利用を推奨します。異なる製品のプロジェクトからイベント設定を取り込むことは可能ですが、正常に動作しない場合があります。

JSON 形式で編集する

1. 画面右上の [JSON 

❗ 修正した内容が JSON 形式に合っていない場合、画面下部にエラーメッセージが表示され、保存できません。表示されるエラーメッセージは、形式エラーの内容によって異なる場合があります。

JSON error

付録

発生条件・対象選択ガイド

メトリクスアラートにおけるイベントの発生条件とイベント対象の選択は、同一の構文を使用します。ただし、イベント発生条件ではフィールド（Field）のキーを変数として使用し、イベント対象の選択ではタグ（Tag）のキーを変数として使用します。

レベル動作ガイド

イベントレベルは、危険（Critical）、警告（Warning）、正常（Info）の3段階に分類されます。

1. 優先順位に基づくイベント発生

複数のレベル条件を同時に満たした場合、最も優先度の高いイベントのみが発生します。

例

設定:

- Warning: CPU > 70%

- Critical: CPU > 90%

現在の状態: CPU 95%
→ 結果: Critical イベントのみ発生 (Warning は抑制される)

2. レベル上昇

進行中状態を持つイベントにおいて、低いレベルのイベントが進行中の状態で高いレベルの条件を満たすと、両方のレベルが進行中状態になります。

例

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

シナリオ:
1) CPU 80% → Warning 発生 (進行中)
2) CPU 95% → Warning (進行中)、Critical (進行中)

3. レベル下降

進行中状態を持つイベントで、高いレベルから低いレベルへ遷移した場合、高いレベルは解消され、低いレベルが維持されます。

例

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

シナリオ:
1) CPU 97% → Critical 発生
2) CPU 85% → Critical 解消、Warning 維持
3) CPU 65% → Warning 解消

4. 動作フロー

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

```

メトリクス値: 60% → 75% → 92% → 85% → 60%
状態:   正常   Warning   Critical   Warning   正常
        (発生)   (発生)   (維持)   (解消)
           Warning
           (維持)

```

- ❗ 進行中状態を持つイベントは、条件が満たされている間は継続して有効となり、条件が解除されるまで維持されます。

条件設定ガイド

- ❗ メトリクス名が数字で始まる場合、または特殊文字を含む場合は、`${メトリクス名}` の形式で記述する必要があります。

- 括弧 `()`, `[]`
- 演算子 `+`, `-`, `*`, `/`, `%`
- 区切り文字 `:`, `@`, `#`, `,`, ``` (空白)
- その他の特殊文字 `!`, `^`, `&`, `|`, `~`, ````, `=`

`${}` 使用例:

```

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

```

`${}` なしで使用可能: 英字、アンダースコア (`_`)、ドット (`.`) のみを含む場合

```

cpu > 80
cpu_usage > 50
CPUUtilization.Average > 0.8

```

1. 比較演算子

数値比較

```
より大きい:  cpu > 80
以上:        cpu >= 80
より小さい:  memory < 1000
以下:        memory <= 1000
等しい:      status == 200
等しくない:  error != 0
```

文字列比較

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

2. 算術演算子

- 基本的な算術演算

```
加算:  cpu + 10 >= 90
減算:  memory - 100 >= 500
乗算:  cpu * 2 >= 100
除算:  disk / 1024 >= 100
剰余:  value % 10 == 0
```

- 括弧による優先順位の制御

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

- 負の値の表現

```
cpu > -100
```

3. 論理演算子

- AND 演算 (&&)

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

- OR 演算 (||)

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

- 複合論理演算

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

4. パターンマッチング演算子

- LIKE 演算子

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

- NOT LIKE 演算子

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

5. 組み込み関数

- Null チェック関数

```
isNull(value)      # null かどうかを確認
isNotNull(value)   # null でないかを確認
nvl(value, 0)      # null の場合に既定値を返す
isEmpty(str)       # 空文字列かどうかを確認
isNotEmpty(str)    # 空文字列でないかを確認
```

- 集計関数


```
sum(cpu, memory, disk)    # 合計
avg(cpu, memory)          # 平均
max(cpu, memory, disk)    # 最大値
min(cpu, memory, disk)    # 最小値
count(value1, value2, value3) # 件数
```

- 数学関数

```
round(cpu, 2)    # 四捨五入（小数点以下2桁）
```

- 文字列関数

```
length(str)      # 文字列の長さ
startsWith(str, 'prefix') # 接頭辞の確認
endsWith(str, 'suffix') # 接尾辞の確認
indexOf(str, 'search') # 文字列の位置
substring(str, 0, 10) # 部分文字列
trim(str)        # 空白の削除
replace(str, 'old', 'new') # 文字列の置換
hasStr(str, 'search') # 文字列の包含判定
```

- 条件関数

- **if:** 条件式が `true` の場合は `true値` を返し、`false` の場合は `false値` を返す条件関数

形式

```
if(条件, true値, false値)
```

例

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

- **decode:** 値と条件を比較し、一致した条件の結果を返します。一致しない場合は既定値を返します

形式

```
decode(値, 条件1, 結果1, 条件2, 結果2, ..., 条件N, 結果N, 既定値)
```

例

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

- **in**: 値が指定した候補値のいずれかと一致した場合は `true`、それ以外は `false` を返します

形式

```
in(値, 候補値1, 候補値2, ..., 候補値N)
```

例

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

❗ 記述時の注意事項

- 推奨事項
 - 簡単な変数名は `${}` を使わずに記述（例: `cpu`, `memory`）
 - 特殊文字を含む場合は必ず `${}` を使用
 - 複雑な演算は括弧で明確に区切る
 - 関数名は正確に入力（大文字と小文字を区別）
- 避けるべき事項
 - 不完全な式の記述（例: `cpu >` , `memory &&` ）
 - 括弧の不一致（例: `(cpu > 80 && cpu > 70)` ）
 - 演算子の連続使用(例: `cpu >> 80` , `cpu >< 80`)

複合ログイベント設定

ホーム > プロジェクト選択 >  アラート通知 > イベント設定 > 複合ログ タブ

収集したログデータを条件に合わせてフィルタリングして警告通知を設定できます。ログイベントを使用するには、ログモニタリングを有効化する必要があります。**ログモニタリングの有効化**については、各製品のログドキュメントを参照してください。

- **複合ログイベント**: 設定したデータ照会範囲内のログを基準に、ログ検索条件を満たすログ数が閾値以上の場合にイベントが発生します。

ⓘ 権限

複合メトリクスイベントを設定するには**通知設定権限**が必要です。通知設定権限は、**ホーム画面 > プロジェクト選択 > 管理 > 統合メンバー管理**で、権限を付与するメンバーの  アイコンをクリックして設定できます。

基本オプション

- **検索**: イベント名またはイベント受信タグを選択して目的のイベントを検索
- **JSONダウンロード/アップロード**: イベントルールはJSONエディタで直接編集するか、ファイルにダウンロードして修正後に再アップロード可能
- **通知メッセージ設定**: 受信するメッセージの詳細項目を選択し、項目ごとに内容を編集
- **+ イベント追加**: 新しいログイベントを追加

表 | 複合ログイベント一覧構成

項目	説明
イベント名	通知タイトルとして使用されるイベント名
テンプレート	複合ログテンプレート

項目	説明
カテゴリ	ログ分類名（ログフォルダ名）
ルール	イベントが発生する条件
イベント状態が解消されたら追加通知	CriticalとWarningレベルのイベントが解消されたとき、正常（RECOVERED）状態の通知を受信するかどうか - 有効: 進行中 → 正常状態に移行したときRECOVERED通知を送信し、イベント履歴で進行中/解消状態を区別して確認可能 - 無効: 閾値を超えるたびに単発のイベントが発生
イベント発生一時停止	イベント通知発生後、同じイベントの発生を一定時間停止 - 選択可能時間: 使用しない、5分、10分、15分、20分、30分、1時間、2時間、3時間、6時間、12時間、1日 - 解消通知が有効な場合、正常（RECOVERED）状態の通知受信後、選択した時間中は同じイベントが発生しても通知されない
インターバル	ログデータを照会する時間範囲
イベント受信タグ	イベント通知を受け取るユーザーまたはグループ（受信タグ）
	イベントの編集と削除
	イベントの有効化状態 - 有効: 条件を満たすとイベント発生 - 無効: イベントが動作せず、条件をチェックしない

イベント設定

設定したデータ照会範囲内のログを基準に、ログ検索条件を満たすログ数が閾値以上の場合に警告通知を設定できる機能です。

複合ログイベントの追加

1. アラート通知 > イベント設定の複合ログ タブをクリックしてください。
2. 画面右側の [+ イベント追加] ボタンをクリックしてください。
3. イベントルール追加ウィンドウでログイベント条件を設定してください。詳細については、[基本設定](#)、[詳細設定](#)、[追加設定](#)を参照してください。

複合ログイベントの追加

4. イベントルール追加ウィンドウで設定が完了したら、[保存] ボタンをクリックしてください。

基本設定

- イベント名: イベントタイトルとして使用する名前を入力してください。
- イベント有効化: トグルボタンを有効にすると、条件を満たしたときにイベントが発生します。
- レベル: イベントレベル (Critical、Warning、Info) を選択してください。

詳細設定

[テンプレート \(プリセット\)](#)、[メッセージ](#)、[カテゴリ](#)、[フィルター](#)、[イベント発行条件](#)を設定します。

テンプレート (プリセット)

定義済みのプリセットを選択すると、[フィルター](#)、[クエリタイプ](#)、[イベント発行条件](#)が自動的に設定されます。プリセットを選択後、必要に応じて変更できます。

複合ログテンプレートの種類



プリセット	クエリタイプ	デフォルトルール
使用しない	none	rows > 10
2xxステータスコード件数	count	count > 10



プリセット	クエリタイプ	デフォルトルール
3xxステータスコード件数	count	count > 10
4xxステータスコード件数	count	count > 10
5xxステータスコード件数	count	count > 10
正常ステータスコード (2xx, 3xx) 件数	count_v2	include_minus_exclude_count > 10
エラーステータスコード (4xx, 5xx) 件数	count_v2	include_minus_exclude_count > 10
エラー受信件数	count	count > 10
例外受信件数	count	count > 10
毎秒ログ発生件数	rps	rps > 100
フィールド集計 (Aggregation)	aggr	avg > 1000
比率 (Rate)	rate	rate > 10
ユニーク値数 (Cardinality)	cardinality	cardinality > 100
パーセンタイル (Percentile)	percentile	p99 > 3000

メッセージ

イベント発生時に受け取る通知メッセージを入力してください。メッセージに変数を使用して動的なメッセージを構成できます。

- 例示: メッセージ `${host}` でエラー `${count}` 件発生 → 通知メッセージ web-01 でエラー15件発生

表 | メッセージ変数

変数	説明	使用条件
<code>\${count}</code>	条件に一致するログ件数	常に使用可能
<code>\${groupField}</code>	グループ化フィールド名	グループ化通知のみ
<code>\${groupValue}</code>	グループ化フィールド値	グループ化通知のみ
<code>\${フィールド名}</code>	グループ化フィールド値（フィールド名で直接参照）	グループ化通知のみ

❗ `${count}` 変数はグループ化の有無に関わらず、すべての通知で使用できます。 `${groupField}`、`${groupValue}`、`${フィールド名}` 変数はグループ化フィールドが設定されている場合のみ置換されます。

カテゴリ

ログ分類名（ログフォルダ名）をリストから選択するか、直接入力してください。カテゴリを選択してから検索キーと検索値を入力できます。

フィルター

Luceneクエリ構文でログ検索条件を入力します。2種類の入力モードをサポートします。

- **フィルターモード** [🔍](#): フィールドと値を選択してクエリを構成します。
- **コードモード** [<>](#): Luceneクエリを直接入力します。

表 | Luceneクエリ例

クエリ	説明
<code>level:ERROR</code>	levelフィールドがERRORのログ
<code>status_nxx:status_4xx OR status_nxx:status_5xx</code>	4xxまたは5xxステータスコード
<code>appender:accessLog</code>	accessLog appenderのログ
<code>response_time.n:*</code>	response_time.nフィールドが存在するログ

クエリ	説明
host:web-01 AND level:ERROR	web-01ホストのエラーログ

イベント発行条件

クエリタイプ別に設定します。選択したテンプレート（プリセット）またはクエリタイプに応じて、追加設定項目が表示されます。

表 | イベント発行条件キーの意味

キー	意味
rows / count	フィルター条件に一致するログ件数
rps	毎秒ログ発生件数（件数 / インターバル秒）
avg	対象フィールド値の平均
sum	対象フィールド値の合計
min	対象フィールド値の最小値
max	対象フィールド値の最大値
rate	分子件数 / 分母件数 × 100（%）
cardinality	対象フィールドのユニーク値数
p99 / p95 / p90 / p75 / p50	対象フィールドのパーセンタイル値
include_minus_exclude_count	含むフィルター件数 - 除外フィルター件数

- **件数（count / none）**：設定したフィルター条件に一致するログの件数をカウントします。

表 | 件数設定項目

設定項目	説明
フィルター	ログ検索条件（Luceneクエリ）
イベント発行条件	件数 または 条件に一致するログ {演算子} {閾値}（例: count > 10）

- **毎秒ログ発生件数（rps）**：設定したフィルター条件に一致するログの毎秒発生件数（Requests Per Second）を計算します。インターバル時間中の総件数をインターバル秒数で割って算出します。

表 | 毎秒ログ発生件数設定項目

設定項目	説明
フィルター	ログ検索条件（Luceneクエリ）
イベント発行条件	RPS {演算子} {閾値}（例: rps > 0.5）

- **フィールド集計（aggr）**：指定した数値フィールドの集計値（平均、合計、最小値、最大値）を計算します。イベント発行条件で集計方式をドロップダウンから選択できます。

表 | フィールド集計設定項目

設定項目	説明
フィルター	ログ検索条件（Luceneクエリ）
対象フィールド	集計対象の数値フィールド（例: response_time.n）
イベント発行条件	平均 / 合計 / 最小値 / 最大値 {演算子} {閾値}（例: avg > 1000）

- **比率（rate）**：分子フィルターと分母フィルターの件数比率（%）を計算します。全ログに対する特定条件の比率を監視する際に有用です。

表 | 比率設定項目

設定項目	説明
フィルター（分子）	比率計算の分子となるログ条件（例: <code>level:ERROR</code> ）
分母フィルター	比率計算の分母となるログ条件（例: <code>level:*</code> ）
イベント発行条件	比率（%） {演算子} {閾値}（例: <code>rate > 10</code> ）

- 例示: フィルター `level:ERROR`、分母フィルター `level:*`、ルール `rate > 10` → 全ログ中のエラー比率が10%を超えると通知が発生
- **ユニーク値数（cardinality）** : 指定したフィールドのユニーク値数を計算します。異常に多くの種類の値が発生する場合を検出する際に有用です。

表 | ユニーク値数設定項目

設定項目	説明
フィルター	ログ検索条件（Luceneクエリ）
対象フィールド	ユニーク値を計算するフィールド（例: <code>host</code> ）
イベント発行条件	ユニーク値数 {演算子} {閾値}（例: <code>cardinality > 100</code> ）

- **パーセンタイル（percentile）** : 指定した数値フィールドのパーセンタイル値を計算します。レスポンスタイムのテールレイテンシを監視する際に有用です。パーセンタイルの選択を変更すると、イベント発行条件のキーが自動的に更新されます。

表 | パーセンタイル設定項目

設定項目	説明
フィルター	ログ検索条件（Luceneクエリ）
対象フィールド	パーセンタイルを計算する数値フィールド（例: <code>response_time.n</code> ）
パーセンタイル	P99、P95、P90、P75、P50から選択

設定項目	説明
イベント発行条件	P99 / P95 / ... {演算子} {閾値} (例: p99 > 3000)

表 | パーセンタイルの意味

パーセンタイル	意味
P50	中央値。全データの50%がこの値以下
P75	全データの75%がこの値以下
P90	全データの90%がこの値以下
P95	全データの95%がこの値以下
P99	全データの99%がこの値以下

- 含む/除外件数 (count_v2) : 含むフィルターの件数から除外フィルターの件数を引いた純件数を計算します。

表 | 含む/除外件数設定項目

設定項目	説明
フィルター (含む)	含むログ条件 (例: status_nxx:status_4xx OR status_nxx:status_5xx)
フィルター除外	除外するログ条件 (例: status_nxx:status_4xx)
分母フィルター	比率計算用の分母 (任意)
イベント発行条件	含む-除外件数 {演算子} {閾値} (例: include_minus_exclude_count > 10)

- 例示: フィルター status_nxx:status_4xx OR status_nxx:status_5xx、フィルター除外 status_nxx:status_4xx
→ 4xx+5xxから4xxを除いた純5xx件数が10を超えると通知が発生

グループ化フィールド（Group By）

グループ化フィールドを設定すると、そのフィールドの値ごとに独立して通知条件が判定されます。ドロップダウンからグループ化するフィールドを選択します。ドロップダウンをクリックすると、現在のカテゴリで使用可能なフィールド一覧がオートコンプリートで表示されます。

- 例示: フィルター `level:ERROR`、グループ化フィールド `host`、ルール `rows > 3`

表 | グループ化設定の比較

項目	グループ化なし	グループ化あり
判定単位	全ログを1つに集計	グループ値ごとに独立して集計
通知発生	1件	条件を満たすグループ数分
通知タイトル	イベントタイトル	[グループ値] イベントタイトル
Stateful	全体基準での状態遷移	グループごとに独立した状態遷移

- `[web-01]` エラー通知 — `web-01`でエラー8件 → 通知発生
- `[web-02]` エラー通知 — `web-02`でエラー5件 → 通知発生
- `[api-01]` エラー通知 — `api-01`でエラー2件 → 条件未達、通知なし

❗ イベント状態が解消されたら追加通知を有効にした場合、グループごとに独立してABNORMAL → RECOVERED状態が遷移します。例えば `web-01` のエラーが解消されると `[web-01] RECOVERED` 通知が発生し、他のホストの状態には影響しません。

追加設定

- **インターバル:** 選択した時間（`unset`、`1分`、`5分`、`10分`、`30分`、`1時間`、`12時間`）間隔で通知条件を確認します。
- **無音:** イベント発生後、選択した時間（`unset`、`1分`、`5分`、`10分`、`30分`、`1時間`、`12時間`）中は同じイベントが発生しません。

- **イベント動作時間:** 特定の時間帯（業務/非業務/メンテナンス時間など）にイベントが動作するようにタグを設定してください。タグを設定しない場合、イベントが有効な状態で24時間常時動作します。
 1. **+追加**をクリックしてください。
 2. **イベント動作時間で**+新しいタグを作成****をクリックしてください。
 3. **イベント動作時間タグの作成でタグ名、曜日、時間、色**を選択し、**[適用]** ボタンをクリックしてください。
 4. 作成したタグはタグリストで確認でき、チェックボックスを選択すると適用されます。
 5. 変更または削除するタグの  アイコンをクリックして、**イベント動作時間タグの編集**でタグを編集または削除できます。

 タグを削除すると、そのタグが適用されているすべてのユーザーのタグが削除されます。ただし、イベントルールで使用中のタグは削除できません。

- **イベント受信タグ:** イベントに受信タグを設定すると、そのタグを持つプロジェクトメンバーに通知が送信されます。受信タグを設定しない場合、プロジェクト内のすべてのユーザーに通知が送信されます。
 1. **+タグ追加**または**+**をクリックしてください。
 2. **イベント受信タグウィンドウ下部の**+新しいタグを作成****をクリックしてください。
 3. **タグ作成ウィンドウ**でタグ名を入力し、色を選択してから、**[タグ作成]** ボタンをクリックしてタグを作成してください。
 4. 作成されたタグはタグリストの  アイコンをクリックして編集または削除してください。
 5. **イベント受信タグウィンドウのタグリスト**から目的のタグを選択すると適用されます。

 イベント設定時にイベント受信タグを選択して、そのタグを持つプロジェクトメンバーとサードパーティプラグインに通知を送信できます。**アラート通知 > 通知設定**でプロジェクトメンバーとサードパーティプラグインにそれぞれタグを指定できます。

シミュレーション

通知を保存する前に、過去のデータでシミュレーションして通知発生予測件数を確認できます。

1. 通知設定を完了後、下部の時間範囲を選択してください。
2. [シミュレーション] ボタンをクリックしてください。
3. チャートに時間帯別データと通知発生回数が表示されます。

❗ シミュレーション時間範囲を調整して、さまざまな時間帯の通知発生パターンを確認できます。直近1~2分のデータはインデックスビルド遅延により照会されない場合があります。

4. イベントルール追加ウィンドウで設定が完了したら、[保存] ボタンをクリックしてください。

ログエクスプローラーから通知を作成

ログエクスプローラーから直接通知を作成できます。

1. ログ > ログ検索メニューに移動してください。
2. カテゴリと検索クエリを設定してください。
3. 画面右上の[イベント追加] ボタンをクリックしてください。
4. Drawerで通知設定フォームが開き、現在のカテゴリと検索クエリが自動的に入力されます。
5. 追加設定を完了し、[保存] ボタンをクリックしてください。
6. 保存完了後、[移動] ボタンをクリックすると通知一覧に移動します。

イベントの編集/削除

1. アラート通知 > イベント設定の複合ログタブに移動してください。
2. ログイベントリストで編集または削除するイベントの✎アイコンをクリックしてください。
3. イベント設定画面でオプションを変更し、[保存] ボタンをクリックしてください。
 - a. 選択したイベントを削除するには、イベント設定画面の右上の[削除] ボタンをクリックしてください。

イベントの共有

メトリクスイベント設定を JSON ファイルとして保存し、他のユーザーと設定を共有したり、他のユーザーの設定を取り込んだりすることができます。

- JSON ファイル名: `event-rules-YYYYMMDD.json`

エクスポート

1. 画面右上の [JSON ] ボタンをクリックします。
2. JSON 編集画面が表示されたら、[ エクスポート] ボタンをクリックします。
 - イベントを検索した状態でエクスポート機能を使用すると、検索結果のみが JSON ファイルとしてダウンロードされます。
3. JSON ファイルがダウンロードされたら、共有したい他のユーザーに渡してください。

インポート

1. 画面右上の [] ボタンをクリックします。
2. エクスポート 機能でダウンロードした JSON ファイルを選択します。
3. JSON 編集画面が表示されたら、[一覧に追加] または [上書き] を選択します。

 同じ種類の製品間での利用を推奨します。異なる製品のプロジェクトからイベント設定を取り込むことは可能ですが、正常に動作しない場合があります。

JSON 形式で編集する

1. 画面右上の [JSON ] ボタンをクリックします。
2. 編集画面が表示されたら、JSON 形式に従って内容を修正してください。
3. 修正が完了したら、画面下部の [保存] ボタンをクリックします。

- ❗ 修正した内容が JSON 形式に合っていない場合、画面下部にエラーメッセージが表示され、保存できません。表示されるエラーメッセージは、形式エラーの内容によって異なる場合があります。

JSON error

通知設定

ホーム > プロジェクト選択 >  アラート通知 > 通知設定

ユーザー別アラート受信設定

 **ユーザー別アラート受信設定** における他メンバーの情報は、**メンバー管理** 権限を持つメンバーのみが確認できます。それ以外のメンバーには、必須情報がマスキングされて表示されます。

- イベント通知の一括受信設定およびアクセス設定のためのモバイル端末管理は、**アカウント情報** で行うことができます。
- メンバー権限の詳細については、[こちらのドキュメント](#) を参照してください。

通知手段の設定

メール、**SMS**、**WhatsApp**、**モバイル** による通知を提供します。

ユーザー別アラート受信設定 セクションで、受信したい通知手段のチェックボックスを選択すると警告アラートを受信できます。通知手段のチェックボックスを解除すると、その手段ではアラートは送信されません。

 プロジェクトの最高管理者を除き、すべてのユーザーは自分自身の受信設定のみ変更できます。

メール通知

メール通知は、会員登録時に入力したメールアドレス宛に送信されます。

SMS通知

SMSで通知を受信できます。

 SMS通知機能は、有料プロジェクトでのみ利用できます。

1. 画面右上の **プロフィールアイコン** をクリックし、**アカウント管理** に移動します。
2. **アカウント情報** の **ユーザー電話番号** セクションで、[一般携帯電話] ボタンをクリックします。
3. 認証番号を受信する **電話番号** を入力します。
 - SMS通知を受信できる電話番号は、**韓国の携帯電話番号のみ**対応しています。
4. [保存] ボタンをクリックします。

✔ 登録した電話番号の変更および削除

- 電話番号を変更する場合は、[変更] ボタンをクリックしてください。SMS認証が必要です。
- 電話番号を削除する場合は、[削除] ボタンをクリックしてください。削除後は、SMSによる通知を受信できなくなります。

WhatsApp通知

WhatsAppを通じて通知を受信できます。

ⓘ WhatsApp通知機能は、有料プロジェクトでのみ利用できます。

1. 画面右上の **プロフィールアイコン** をクリックし、**アカウント管理** に移動します。
2. **アカウント情報** の **ユーザー電話番号** セクションで、[WhatsApp] ボタンをクリックします。
3. 認証番号を受信する **電話番号** を入力します。
4. [認証番号送信] ボタンをクリックします。
5. WhatsAppアプリケーションに送信された6桁の認証番号を入力します。
 - 10分以内に認証番号を受信できなかった場合は、[認証番号再送信] ボタンをクリックしてください。
6. [認証] ボタンをクリックします。

モバイル通知

モバイル通知を受信するには、モバイル端末にWhaTapアプリケーションをインストールし、ログインする必要があります。

- WhaTapアプリケーションをダウンロード – [Android](#)
- WhaTapアプリケーションをダウンロード – [iOS](#)

繰り返し通知（エスカレーション）設定

アラート発生後も状況が解消されない場合、初回アラート発生時刻を基準に通知を繰り返す間隔を設定できます。この設定は **Critical** レベルのアラートにのみ適用されます。

例えば、初回アラート発生から即時（0分）、1時間後、1日後に通知を繰り返す場合は、**繰り返し通知（エスカレーション）** カラムに `0,1H,1D` と入力します。

1. **アラート通知 > 通知設定** に移動し、**ユーザー別アラート受信設定** セクションを開きます。
2. **繰り返し通知（エスカレーション）** 項目で設定します。
 - **M**: 分、**H**: 時間、**D**: 日。単位を省略した場合は分単位として扱われます。
 - 数値、または 数値+単位（**M**, **H**, **D**）の形式で入力してください。入力形式が正しくない場合はメッセージが表示されます。
3. [保存] ボタンをクリックしてください。保存しない場合、設定は反映されません。

イベント受信タグ

イベント設定時に **イベント受信タグ** を選択すると、そのタグを持つプロジェクトメンバーや 3rd-party プラグインに通知を送信できます。イベント受信タグを設定しない場合、**すべてのプロジェクトメンバー** に警告アラートが送信されます。

イベント受信タグの追加・編集・削除

 イベントに **適用中のイベント受信タグ** は削除できません。

1. **アラート通知 > 通知設定** に移動します。
2. **ユーザー別アラート受信設定** セクションのユーザー一覧で、**+ タグ追加** または **+** をクリックします。
3. **イベント受信タグ** 画面で **+ 新しいタグ作成** をクリックします。
4. **タグ作成** 画面でタグ名を入力し、色を選択して [タグ作成] ボタンをクリックします。

5. 作成されたタグは、タグ一覧の  をクリックして編集または削除できます。
6. イベント受信タグ画面の **タグ一覧** から使用したいタグを選択すると適用されます。

イベント受信タグを解除する

1. アラート通知 > 通知設定 に移動し、**ユーザー別アラート受信設定** セクションを開きます。
2. イベント受信タグを解除したいユーザーの **イベント受信タグ** 項目にある + をクリックします。
3. イベント受信タグ画面で、解除したいタグの X をクリックすると、そのタグが解除されます。

受信タグ未設定のアラートを受信する

イベント設定時にイベント受信タグを選択すると、そのタグを持つプロジェクトメンバーや 3rd-party プラグインに通知を送信できます。

- イベント受信タグが設定されていないアラートを受信するには、**受信タグ未設定のアラートを受信** オプションを有効にしてください。
- イベント受信タグが設定されているアラートのみ受信したい場合は、このオプションを無効にしてください。

❗ すべての警告アラートを受信しない場合は、このオプションを無効にし、**イベント受信タグ** が一つも選択されていない状態にしてください。

イベント受信モードの選択

ユーザー別アラート受信設定 セクションで、メンバーまたはサードパーティチャネルごとにイベント通知の受信範囲を次の3つのモードから選択できます。受信モードは、各メンバーまたはチャネル行の**イベント受信タグ**列で選択します。

Mode	Description
すべての通知を受信	イベント受信タグに関係なく、すべての警告通知を受信
選択したタグのみ通知を受信	選択したイベント受信タグを持つ警告通知のみ受信。タグを最低1つ以上選択
すべての通知を受信しない	いかなるイベント通知も受信しない。選択したタグは削除されずそのまま保存

- 選択したタグのみ通知を受信モードでは、タグ選択領域で通知を受信するタグを1つ以上選択してください。
- イベント受信タグが指定されていない警告通知まで受信するには、タグ選択領域で**未分類仮想タグ**を選択してください。**未分類タグ**は通常のタグと同様に選択または解除でき、タグ自体を編集・削除することはできません。

❗ すべての通知を受信しないモードでは、該当メンバーまたはチャネルがイベント通知をまったく受信しません。このとき選択したタグは削除されず保存されるため、再び**選択したタグのみ通知を受信モード**に切り替えると、以前に選択したタグ設定をそのまま使用できます。

通知受信言語の選択

ユーザーが受信するアラート通知の言語を選択できます。

1. アラート通知 > 通知設定 に移動します。
2. ユーザー別アラート受信設定 セクションのユーザー一覧で、言語を設定したいユーザーの一番左にある ► ボタンをクリックします。
3. 通知受信言語 を選択します。

曜日・時間別通知設定

ユーザーごとに、曜日および時間帯別の通知受信可否を設定できます。

1. アラート通知 > 通知設定 に移動します。
2. ユーザー別アラート受信設定 セクションのユーザー一覧で、曜日・時間別通知を設定したいユーザーの一番左にある ► ボタンをクリックします。
3. 警告アラートを受信したい曜日を選択するか、時間帯を入力します。
 - 通知手段ごとに設定できます。

サードパーティプラグイン

外部アプリケーションを通じて警告アラートを受信できます。

- 対応アプリケーション: Slack、Telegram、Teams、Teams Workflows、Jandi、AlertNow、Webhook、Webhook

JSON、Opsgenie、PagerDuty、LINE、ilert

❗ WhaTap のサポート範囲に含まれない社内メッセンジャーは、標準の **Webhook** または **Webhook JSON** を使用して連携できます。

表 | サードパーティプラグイン一覧

項目	説明
プラグイン名	プラグインの名称
認証キー	認証キー
認証値	認証値
受信レベル	警告、全体、危険のいずれか
繰り返し通知（エスカレーション）	問題が解消されない場合、初回通知時刻から再通知する間隔 - Critical レベルのアラートにのみ適用
Smart メッセージ（AI）	Telegram プラグイン追加時に AI 通知機能を提供 - 対応言語：韓国語、英語、日本語
イベント受信タグ	プロジェクト内の特定メンバーまたはチームに対する通知受信設定
削除	サードパーティプラグインの削除

サードパーティプラグインの追加

1. アラート通知 > 通知設定 に移動します。
2. サードパーティプラグイン セクションで **追加** ボタンをクリックします。
3. サードパーティプラグイン追加 画面で、使用するサービスのタブを選択します。
4. 選択したサービスの案内（[サードパーティプラグイン通知の追加方法](#)）に従って設定します。
5. 受信テスト ボタンをクリックして設定を確認します。

- すべて完了したら **追加** または **登録** ボタンをクリックします。

サードパーティプラグイン通知の追加方法

Slack

- サードパーティプラグイン追加 画面の **Slack** タブで、[**Slackに登録**] ボタンをクリックすると、Slack のチームおよびチャンネルに **WhaTapNotiBot** を登録できます。

Telegram

- Telegramで @WhaTapApmNotiBot を検索してください。

- ボットを選択し、[開始] ボタンをクリックします。
- チャット画面に `/license` コマンドと、通知を受信したいプロジェクトのアクセスキーを入力してください。



① 使用可能なコマンド一覧

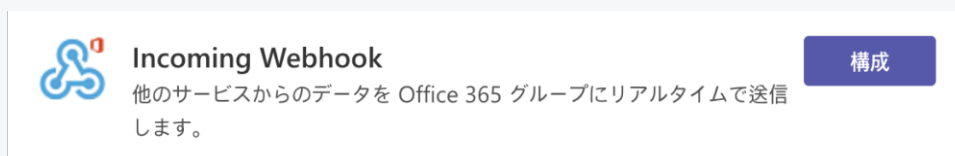
- `/help` : コマンド一覧を表示
- `/license` : 通知を受信するプロジェクトのアクセスキーを入力
- `/remove` : 通知を受信しないプロジェクトコードを入力
- `/list` : 現在通知を受信しているプロジェクトコードを表示

Teams

- 通知を受信したいチャンネルの **コネクタ** に移動します。



2. Webhook を追加し、[構成] ボタンをクリックします。



3. Webhook 名を入力し、[作成] ボタンをクリックします。



Incoming Webhook

フィードバックの送信

Incoming Webhook コネクタを利用すると、トラッキング対象の活動についての通知を外部サービスから受け取ることができます。このコネクタを使うには、別サービスで設定を作成する必要があります。そのサービスが、Office 365 コネクタ形式 対応の Web フックをサポートしている必要があります。

* が付いているフィールドは必須です

着信 Web フック (Incoming Webhook) をセットアップするには、名前を入力して [作成] を選んでください。*

この着信 Web フック (Incoming Webhook) からのデータに関連付ける画像をカスタマイズします。

イメージをアップロードします。



既定のイメージ

作成

キャンセル

4. 生成された Webhook URL をコピーします。

以下の URL をコピーしてクリップボードに保存してから、[保存] を選んでください。この URL は、グループへのデータ送信元となるサービスの画面で必要になります。

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



URL は最新です。

完了

削除

5. WhaTap モニタリングサービスの サードパーティプラグインの追加 画面に戻り、Teams タブ下部の Channel Name と Webhook URL に値を入力します。

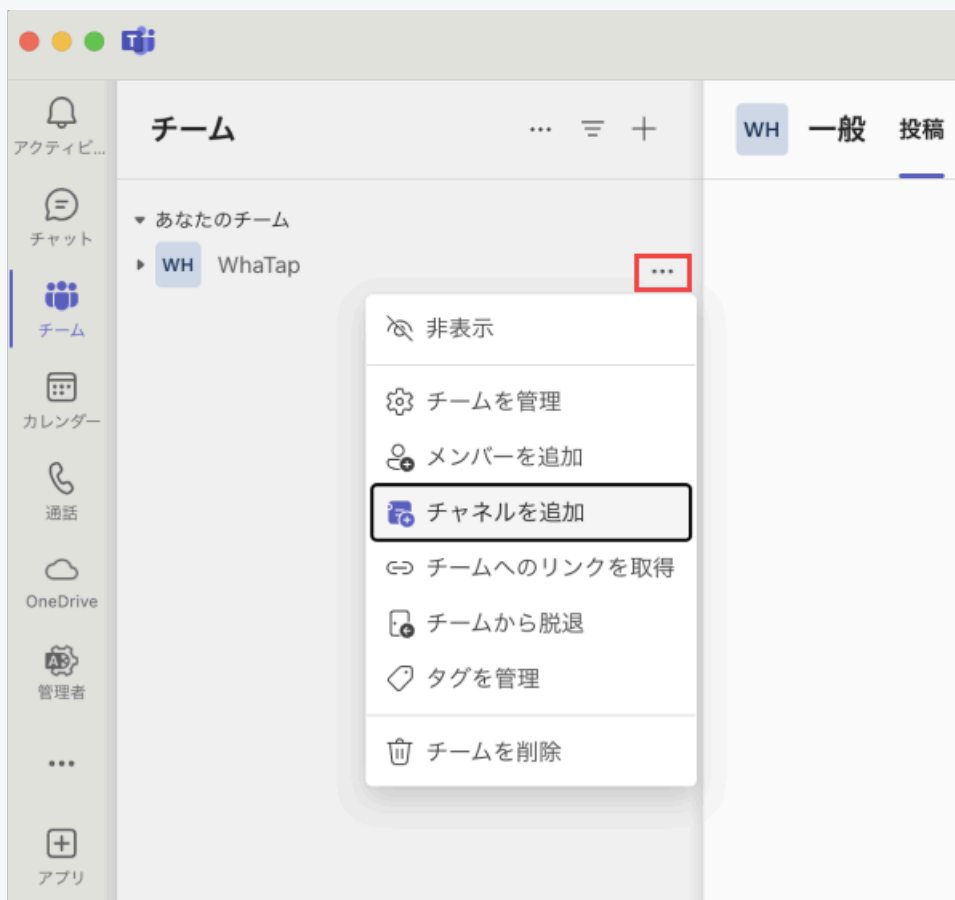
6. [登録] ボタンをクリックします。

Teams Workflows



- ① ワークフローを使用するには、**Microsoft Teams** にアクセス可能なアカウントと **ビジネスプランのサブスクリプション**が必要です。

1. チーム メニューの **その他の操作 (...)** > **チャンネルを追加** をクリックします。



2. チャンネルの作成 画面で **チャンネル名** と **説明** を入力します。チャンネルの種類 は **標準** を選択し、[作成] ボタンをクリックします。



チャンネルの作成

チャンネル名 *

WhaTapのイベントチャンネル

説明

他のユーザーが、適切なチャンネルを見つけられるように説明を入力します

チャンネルの種類を選択する * ⓘ

選択

☒ 標準
チームの全員がアクセスできます。

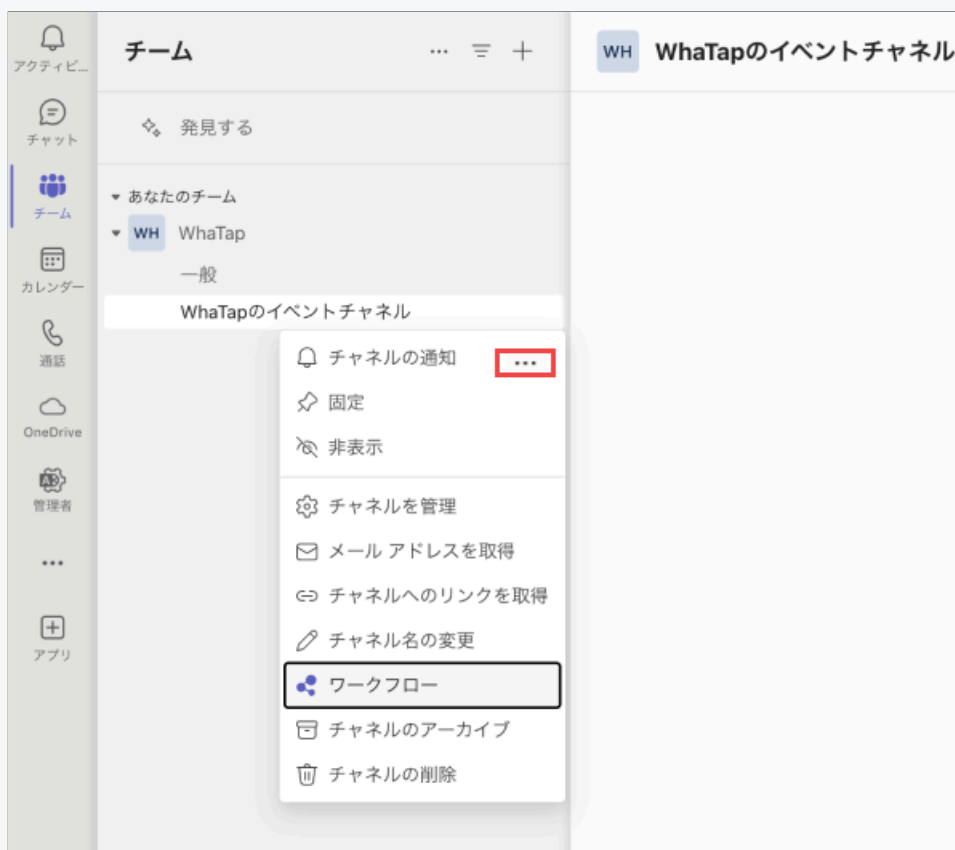
☐ 共有
組織内または組織外の人またはチームがアクセスできます。

☐ プライベート
チームの特定のユーザーがアクセスできます。

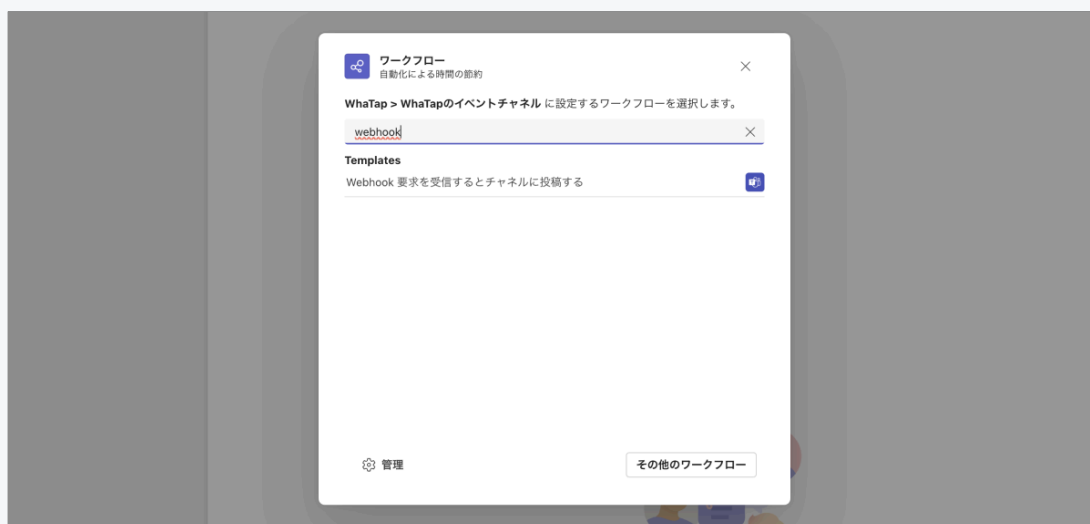
キャンセル 作成

❗ チャンネルの種類を **共有** にするとワークフローは使用できません。**プライベート** を選択した場合、ワークフローは追加できますが通知は受信できません。

- 作成したチャンネルの **その他の操作 (...)** > **ワークフロー** をクリックします。



4. ワークフロー ダイアログの一覧から Webhook 要求を受信したらチャンネルに投稿 を選択し、[ワークフローを追加] ボタンをクリックします。



5. 名前と接続の状態を確認し、[次へ] ボタンをクリックします。
6. 詳細を確認後、[ワークフローを追加] ボタンをクリックします。
7. ワークフローが追加されました。生成された URL をコピーします。



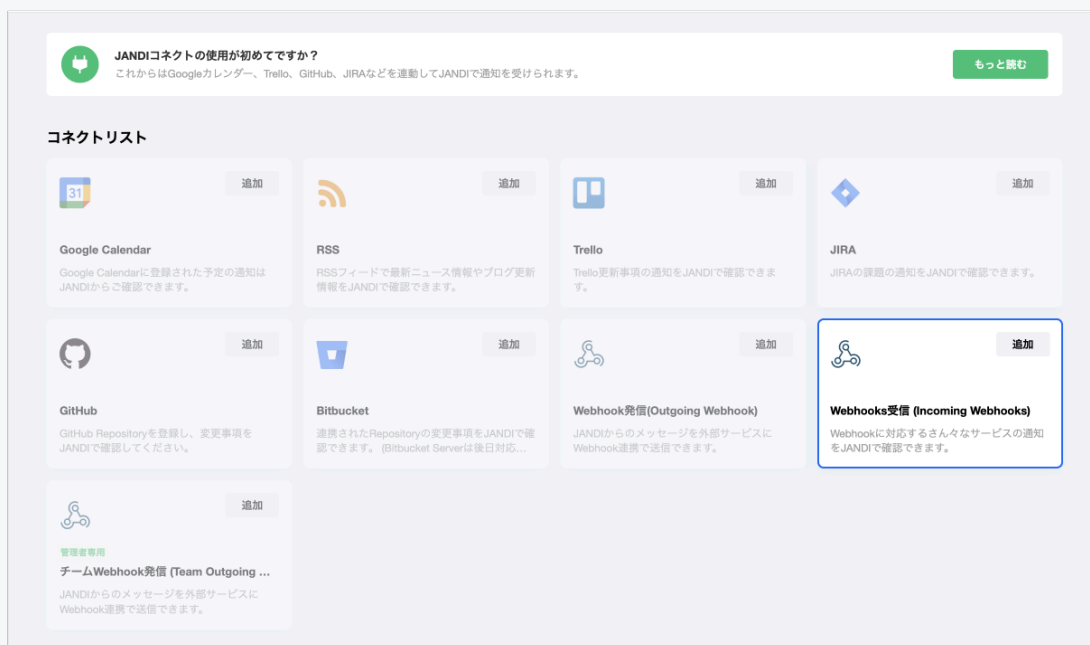
8. WhaTap モニタリングサービスの **サードパーティプラグインの追加** 画面に戻り、Teams **Workflows** タブ下部の **Channel Name** と **Webhook URL** に値を入力します。
9. [登録] ボタンをクリックします。

Jandi





1. 通知を受信するトピックまたはチャットで、**Jandi Connect 設定** に移動します。
2. **コネクト一覧** から **Webhook 受信 (Incoming Webhook)** を選択し、[連携する] ボタンをクリックします。



3. [Webhook 受信を追加] ボタンをクリックします。
4. **Webhook URL 登録** 項目に表示される Webhook URL をコピーします。



5. WhaTap モニタリングサービスの **サードパーティプラグインの追加** 画面に戻り、**Jandi** タブ下部の **Channel Name** と **Webhook URL** に値を入力します。
6. [登録] ボタンをクリックします。



1. AlertNow サービスにアクセスし、設定 > Integration メニューに移動します。



2. Integration 画面で [Integration 作成] ボタンをクリックします。
3. Integration タイプの中から **WhaTap** を選択します。
4. Integration 作成 画面で、名前 および 命名規則 を設定します。

5. [確認] ボタンをクリックすると、Integration が作成されます。
6. 作成された Integration の一覧を確認し、該当する Integration を選択します。



インテグレーション

インテグレーションの作成 検索語を入力 最後のアップデート: 2024-02-21 11:25:10

統合名	統合タイプ	統合キー	サービス名
ワットテスト	ワタップ		ワットテスト

7. 詳細画面で、URL 右側のコピーアイコンをクリックして URL をコピーします。

← **インテグレーション**

ワットテスト

基本情報

統合タイプ	ワタップ
統合キー	fda527a5140
URL	https://alertnowitgr.opsnow.com/integration/whatap/v1/
コンストラクタ	リサ

クリップボードにコピーする

8. Whatap モニタリングサービスの **サードパーティプラグインの追加** 画面に戻り、AlertNow タブ下部の **Channel Name** と **Webhook URL** に値を入力します。
9. [登録] ボタンをクリックします。

Webhook



1. 通知を受信する Webhook を登録します。登録した URL に対して、通知の **title** と **text** が POST メソッドで送信されます。

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

2. **Webhook Name** と **Webhook URL** の項目を入力します。
3. [登録] ボタンをクリックします。

Webhook JSON



1. 通知を受信する Webhook を登録します。登録した URL に対して、通知データが **JSON 形式**で **POST** メソッドにより送信されます。JSON に含めることができる置換変数については、**使用可能な変数**を参照してください。

- `${something}` は WhaTap が提供する置換値を表します。対応する全一覧と意味については、**使用可能な変数**を参照してください。
- イベント状態（`status`）は、**イベント発生**（`on`）と**イベント解消**（`off`）に区別されます。
- `level` は `None`、`Info`、`Warning`、`Critical` に区別されます。

```
{
  "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}"
}
```

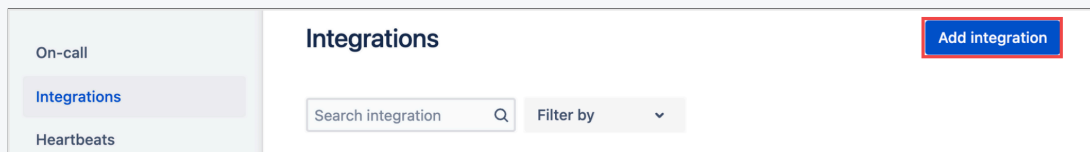
2. **Webhook Name** と **Webhook URL** の項目を入力してください。
3. ヘッダー値を追加するには、**ユーザーヘッダー値の追加** の + 追加 をクリックし、key と value を入力してください。
4. [登録] ボタンをクリックしてください。

Opsgenie

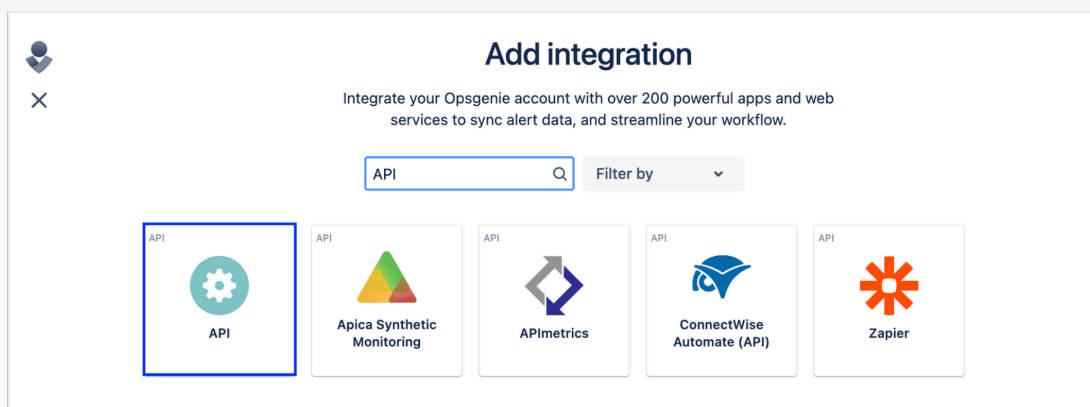




1. **Teams** メニューで、アラートを受信するチームを選択してください。
2. **Integration** メニューに移動し、[Add Integration] ボタンをクリックしてください。



3. インテグレーション一覧で **API** を検索し、選択してください。



4. API 名を設定し、チームを割り当て、各権限を設定した後、[Save Integration] ボタンをクリックしてください。



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: ☐

[Save Integration](#) [Cancel](#)

5. Whatap モニタリングサービスの **サードパーティプラグインの追加** 画面に戻り、Opsgenie タブ下部の **Name** と **API Key** を入力してください。
6. [登録] ボタンをクリックしてください。



PagerDuty



1. [PagerDuty](#) アカウントを登録し、ログインしてください。
2. PagerDuty で **Services > Service Directory** メニューに移動し、[+ New Service] ボタンをクリックしてください。
3. サービス情報 (Name) を入力し、[Next] ボタンをクリックしてください。
4. **Escalation Policy** を設定し、[Next] ボタンをクリックしてください。



PagerDuty

5. **Alert Grouping** と **Transient Alerts** を設定し、[Next] ボタンをクリックしてください。

PagerDuty

6. **Integrations** で **Event API V2** を選択し、[Create Service] ボタンをクリックしてください。

PagerDuty

7. 作成されたサービス画面で **Integration Name** と **Integration Key** の値をコピーしてください。

PagerDuty

8. WhaTap モニタリングサービスの **サードパーティプラグインの追加** 画面に戻り、**Integration Name** と **Integration Key** を入力してください。
9. [登録] ボタンをクリックしてください。

❗ メッセージを受信できない、またはプラグインが登録されない場合は、**Integration Name** または **Integration Key** の値が正しいか確認してください。

LINE



1. LINE アプリをインストールしてください。
2. 以下の QR コードをスキャンして、**WhaTapLabs** 公式チャンネルを友だち追加してください。

LINE 3rd パーティプラグイン追加

3. 次のコマンドを使用して、プロジェクトを LINE と連携し、通知を設定してください。

コマンド

```
/help # 使用可能なコマンド一覧を表示
/list # 連携されているプロジェクト一覧を表示
/license [アクセスキー] # 新しいプロジェクト連携を追加
```



```
/remove [プロジェクトコード] # プロジェクト連携を解除
/language [ko|ja|en] # 通知言語を設定（韓国語／日本語／英語）
```

- プロジェクトのアクセスキーは **管理 > プロジェクト管理** で確認できます。
- LINE 内で `/language` コマンドを使用した場合、その設定は **該当する LINE チャットルーム内のみ** に適用されます。他の 3rd パーティプラグインやプロジェクトの通知言語は変更されません。

使用例

```
/license XXXXXXXXXX # プロジェクトを連携
/language ko # 言語を韓国語に設定
/list # 連携済みプロジェクトを確認
```



- プロジェクトアクセスキー:** WhaTap プロジェクト内の **管理 > プロジェクト管理** で確認できます。
- 言語設定:** `/language` コマンドは LINE チャットルーム内でのみ有効で、他の通知チャンネルの言語は変更されません。

ilert



- ilert コンソールの **Alert sources** 画面右上にある **[+ Create alert source]** をクリックします。
- Integration type** ステップ下部の **Filter integrations** 検索欄に **WhaTap** を入力して検索します。
- 検索結果から **WhaTap** タイルを選択し、**[Next]** ボタンをクリックします。
- アラートソース名を入力し、チームを指定した後、**[Next]** ボタンをクリックします。
 - エスカレーションポリシーは、新規作成または既存のものを選択できます。
- アラートのグループ化方式を選択し、**[Continue setup]** ボタンをクリックします。
 - 最初に選択した **Do not group alerts** は後から変更可能です。
- 次の画面で **アラートテンプレートや優先度などの追加設定** を行うことができます。ここでは [



Finish setup] ボタンをクリックして設定を完了します。

7. 設定が完了すると、完了画面で **API キー** または **Webhook URL** が生成されます。
8. **Webhook JSON** タブで生成された **Webhook URL** をコピーし、下部の **Webhook URL** 入力欄に貼り付けます。
9. [登録] ボタンをクリックします。

大量アラート発生の防止

短時間に大量のアラートが発生した場合、指定した時間だけアラート通知を一時的に停止します。たとえば、5 分間に 20 件のイベントが発生すると、その後 5 分間は警告アラートが送信されません。設定した **停止時間** が経過すると、大量アラート防止機能は自動的に解除されます。

1. 次の画面に移動してください。 **アラート通知** > **通知設定** > **大量アラート通知発生防止** セクション
2. トグルボタンをクリックして **有効化** または **無効化** します。
 -  **有効**: 大量アラートを検知した場合、一時的に通知を停止
 -  **無効**: アラート通知を再開
3. **検知時間**, **検知回数**, **停止時間** を設定してください。
 - **検知時間** 内に **検知回数** 以上のイベントが発生すると、**停止時間** の間、警告アラートが停止されます。



大量アラートによってブロックされた場合、ブロック案内ボックスが表示されます。大量アラート防止機能をすぐに解除するには、ボックス内の **大量アラート発生中止** ボタンをクリックしてください。

イベント通知フォーマット

共通アラートテンプレート

共通テンプレートは、ほとんどのケースで適用できます。さまざまな環境において、同一のフォーマットでアラートを受信できます。

- プロダクトタイプ: アプリケーション、データベース、Kubernetes
- イベントタイプ: アプリケーションアラート、データベースアラート、メトリクスアラート
- イベントチャネル: SMS、Mobile、3rd-party プラグイン、プラグイン

イベントタイトル

Event title format

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

Event title example

```
[Info][JAVA][アプリケーションプロジェクト][TC-0-1-8081][CRITICAL_HIGH_MEMORY]
```

❗ ApplicationName が設定されていない場合、イベントタイトルから省略されます。

- Platform は以下のいずれかで表示されます。
 - 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

イベントメッセージ

イベントメッセージに含めることができる情報です。 `optional` が `false` の場合、常にメッセージに含まれます。
`optional` が `true` の場合、該当データが確認できるときのみ表示されます。

イベントメッセージ例

```
Project Name : アプリケーションプロジェクト  
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

表 | イベントメッセージ構成要素

En	Ko	対応するアラートタイプ	説明
Project Name	プロジェクト名	全て	-
Project Code	プロジェクトコード	全て	-
Agent Name	エージェント名	全て (optional)	oname
Message	イベントメッセージ	全て	-
Alert Type	イベント種別	全て	下記の AlertType 表を参照
Event Time	イベント発生時間	全て	2022-04-13 10:40:49 +0900 の +0900 は GMT オフセット
Event Off Time	イベント解除時間	全て (optional)	2022-04-13 10:40:49 +0900 の +0900 は GMT オフセット
Metric Name	メトリクス名	全て (optional)	イベント条件判定に使用されるメトリクス名
Metric Value	メトリクス値	全て (optional)	メトリクス値が閾値を超えた場合に含まれる
Metric Threshold	メトリクス閾値	全て (optional)	メトリクス条件の閾値

En	Ko	対応するアラートタイプ	説明
Stateful	復旧イベント通知	全て (optional)	復旧通知が有効な場合 <code>true</code> 、それ以外は <code>false</code>
Event Rule	イベント発生条件	メトリクスアラート	-
Target Filter	イベント対象選択	メトリクスアラート	特定対象から収集されたメトリクスのみ評価
Repeat Count	イベント繰り返し回数	メトリクスアラート	繰り返し時間内に指定回数条件を満たすと発生
Repeat Duration	イベント繰り返し時間	メトリクスアラート	繰り返し回数を評価する時間
Receiver	受信者	メトリクスアラート	-
Query	MXQL クエリ	複合メトリクスアラート	-
Rule	イベント発生条件	複合メトリクスアラート	-
Query Period	クエリ期間	複合メトリクスアラート	-
Query Interval	クエリ間隔	複合メトリクスアラート	-
Silent Time	サイレント時間	複合メトリクスアラート	-
Query	URL	Exception アラート	例外を発生させたリクエストの URL
TXID	トランザクション ID	Exception アラート	-

En	Ko	対応するアラートタイプ	説明
Class	エラークラス名	Exception アラート	-
Log Message	ログメッセージ	サーバーファイル ログアラート	-
Log File	ログファイルパス	サーバーファイル ログアラート	-
IP	IP	サーバーアラート全 体	-
CPU	CPU	サーバーアラート全 体	イベント発生時のスナップショット
CPU_load1	CPU_load1	サーバーアラート全 体	イベント発生時のスナップショット
CPU_loadPerCore	CPU_loadPerCore	サーバーアラート全 体	イベント発生時のスナップショット
Memory	メモリ	サーバーアラート全 体	イベント発生時のスナップショット
Swap	スワップ	サーバーアラート全 体	イベント発生時のスナップショット
Disk Name Used Percent Free Size IO Percent	ディスクパフォー マンス	サーバーアラート全 体	イベント発生時のスナップショット
Name Bps Pps	トラフィックパフ ォーマンス	サーバーアラート全 体	イベント発生時のスナップショット
Message Time Name	処理履歴メッセー ジ	サーバーアラート全 体	-

❗ このセクションでは、該当するイベントで提供可能な情報を最大限に表示します。

- **AlertType** は以下のいずれかの値で表示されます。

AlertType	説明
APPLICATION_CPU	アプリケーション CPU アラート
APPLICATION_MEMORY	アプリケーション メモリアラート
APPLICATION_DISK	アプリケーション ディスクアラート
APPLICATION_ACTIVE_TRANSACTION	アプリケーション アクティブTXアラート
APPLICATION_ERROR_TRANSACTION	アプリケーション エラートランザクションアラート
APPLICATION_SLOW_TRANSACTION	アプリケーション トランザクション応答時間アラート
METRICS	メトリクスアラート
COMPOSITE_METRICS	複合メトリクスアラート
ANOMALY	異常値アラート
LOG_REALTIME	リアルタイムログアラート
COMPOSITE_LOG	複合ログアラート
SERVER_REBOOT	サーバー 再起動アラート
SERVER_NO_DATA	サーバー データ未受信アラート
SERVER_PORT	サーバー ポートアラート
SERVER_NETWORK_IOPS	サーバー ネットワーク IOPS アラート
SERVER_NETWORK_BPS	サーバー ネットワーク BPS アラート



AlertType	説明
SERVER_DISK_IO	サーバー ディスク I/O アラート
SERVER_DISK_QUOTA	サーバー ディスク使用量アラート
SERVER_DISK_INODE	サーバー inode アラート
SERVER_CPU	サーバー CPU アラート
SERVER_MEMORY	サーバー メモリアラート
SERVER_CPU_STEAL	サーバー CPU steal アラート
SERVER_MEMORY_SWAP	サーバー スワップメモリアラート
SERVER_LOG_FILE	サーバー ログファイルアラート
SERVER_WINDOW_EVENT	サーバー Windows イベントアラート
SERVER_OFF	サーバー アラート OFF 通知
SERVER_ACKNOWLEDGE	サーバー 処理確認通知
SERVER_PROCESS_COUNT	サーバー プロセス数アラート
SERVER_PROCESS_CPU	サーバー プロセス CPU アラート
SERVER_PROCESS_MEMORY	サーバー プロセス メモリアラート
SERVER_PROCESS_OFF	サーバー プロセスアラート OFF 通知
AGENT_ACTIVE	エージェント 有効化アラート
AGENT_INACTIVE	エージェント 無効化アラート



AlertType	説明
AGENT_REACTIVATED	エージェント 再有効化アラート
URL	URL アラート
TOO_MANY_EVENT	イベント多発アラート
CLOUD_WATCH	CloudWatch アラート
EXCEPTION	例外アラート

イベント履歴

ホーム > プロジェクト選択 > 🔍 アラート通知 > イベント履歴

イベント履歴では、プロジェクトで発生したさまざまなイベントを確認し、詳細情報を分析できます。Elasticsearch DSL クエリをサポートしており、指定した条件に一致するイベントを迅速かつ正確に検索できます。

イベント履歴の確認

検索結果でイベントタイトルをクリックすると、そのイベントが発生した時間帯の詳細データを分析できる画面に移動します。これにより、イベント発生前後の状況を総合的に把握できます。

1. アラート通知 > イベント履歴 に移動してください。
2. イベント履歴 画面の 時間選択 で、イベント履歴を確認する期間を設定してください。
3. フィルター入力欄にクエリを入力し、[虫眼鏡] ボタンをクリックしてください。
 - クエリを入力しない場合、すべてのイベントが表示されます。

🔧 カラム設定

表示するカラムや非表示にするカラムを設定できます。

1. イベント履歴 画面の左上にある [🔧 カラム設定] ボタンをクリックしてください。
2. カラム設定 画面で、表示または非表示にするカラムを選択してください。
 - 表示項目 でカラムの順序を変更できます。
 - カラム名検索 欄で目的のカラムを検索できます。

カラム項目	説明
イベント名	イベントのタイトル
メッセージ	イベントのメッセージまたはスナップショット情報

カラム項目	説明
イベント状態	イベントの現在の状態
エージェント名	イベントが発生した対象エージェントの名前 (Oname) - 特定のエージェントに紐づかないイベントの場合は空欄で表示されます
エージェントグループ	イベントが発生した対象エージェントの種類 (OkindName) - 特定のエージェントに紐づかないイベントの場合は空欄で表示されます
エージェントノード	イベントが発生した対象エージェントのサーバー (OnodeName) - 特定のエージェントに紐づかないイベントの場合は空欄で表示されます
イベント発生時刻	イベントが発生した時刻
イベント解消時刻	イベントが解消された時刻 - 解消状態を持たないイベントの場合は - と表示されます

3. 設定が完了したら、[確認] ボタンをクリックしてカラム設定を反映してください。

↓ CSV ダウンロード

検索結果を CSV ファイル形式でダウンロードできます。

1. アラート通知 > イベント履歴 で [CSV] ボタンをクリックしてください。
2. 現在のフィルター条件に一致するイベント一覧が CSV ファイルとして保存されます。

進行中のイベントのみ表示

現在進行中の状態のイベントのみを表示できます。

1. アラート通知 > イベント履歴 で [進行中のイベントのみ表示] ボタンをクリックしてください。
2. フィルタークエリに次の条件が自動的に追加され、検索が実行されます。


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

イベント検索

- **正確な検索:** 必要なイベントだけを取得できるよう、条件を正確に指定
- **複合条件:** 複数のフィールドを同時に検索し、複雑な条件も一度に処理
- **柔軟なパターン:** ワイルドカードや部分一致など、さまざまな検索方式をサポート
- **高速パフォーマンス:** インデックス化されたデータを活用した高速検索

検索可能なフィールド

フィールド名および値は大文字と小文字を区別しません。

- **フィールド名タグ:** フィールドがサポートされるイベントタイプ
- **フィールドタイプ:** フィールドのデータ型
 -  #: Number
 -  T: String
 -  C: Boolean
 -  D: Date

イベント情報フィールド

フィールド名	タイプ	説明	例
Title	String	イベントタイトル	"Database Connection Error"
OffTitle	String	イベント解消タイトル	"RECOVERED: Database Connection Error"
Message	String	イベントメッセージ	"Connection timeout occurred"
OffMessage	String	イベント解消メッセージ	"RECOVERED: Connection timeout occurred"

フィールド名	タイプ	説明	例
Level	String	現在のイベントレベル	Critical, Warning, Info
OriginLevel	String	元のイベントレベル	Critical, Warning, Info
Status	String	イベント状態	ON, OFF, CANCEL, ACKNOWLEDGE, MAINTENANCE, DISABLED
ActCount	Number	発生回数	2
MetricName	String	指標名	"memory"
MetricValue	String	指標値	"85.5"
OffValue	String	解消時の値	"72.8"
MetricThreshold	String	閾値	"80"
alertType	String	イベント種別	"BASIC", "METRICS", "TRANSACTION" など
alertId	String	イベントルールの一意識別子	"zf3uoj0fv4v7"

イベントタイプ別対応フィールド

ⓘ 特定のイベントタイプでのみサポートされるフィールドです。該当しないイベントタイプの場合、値が存在しないことがあります。

フィールド名	タイプ	イベント種別	説明	例
eventRule	String	基本、メト	イベント発生	"memory ≥ 80"

フィールド名	タイプ	イベント種別	説明	例
		リクス	ルール	
field	String	リアルタイムログ	ログ検索キー	"content"
keyword	String	リアルタイムログ	ログ検索値	"Error"
logCategory	String	リアルタイムログ	ログカテゴリ	"AppLog"
logContent	String	リアルタイムログ	ログ内容	"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."

対象フィールド

フィールド名	タイプ	説明	例
Oid	Number	エージェントの一意識別子	-98765432
Oname	String	エージェント名	"web-server-01"
Okind	Number	エージェント種別の一意識別子	867318026

フィールド名	タイプ	説明	例
OkindName	String	エージェント種別名	"web-server"
Onode	Number	エージェントノードの一意識別子	334634079
OnodeName	String	エージェントノード名	"production-node-1"

イベント固有値フィールド

フィールド名	タイプ	説明	例
Id	Number	イベントの一意識別子	5768121
UUID	String	イベント固有識別子	"550e8400-e29b-41d4-a716"

状態／フラグフィールド

フィールド名	タイプ	説明	例
Stateful	Boolean	状態ベースイベントかどうか	true, false
Disabled	Boolean	無効化されたイベントかどうか	true, false
Escalation	Boolean	エスカレーション有無	true, false
SystemEvent	Boolean	システムイベントかどうか	true, false

検索タイプ別クエリ構文

① 検索の基本構文については、[WhaTap ログ検索クエリ構文](#) ドキュメントを参照してください。

1. キーワード検索

「Database Connection」という文字列を含むイベント

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

2. 複数値検索

指定した複数の値のうち、いずれかを含むイベントを検索します。

```
title: Database Connection
```

現在のイベントレベルが Info または Warning のイベント

```
level: info warning
```

3. パターン検索

ワイルドカードを使用してパターン検索ができます。

名前パターンで特定のエージェントで発生したイベントを検索

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

タイトルが Connection で終わるイベントを検索

```
title: *Connection
```

4. 複合条件検索

複数の条件を組み合わせて、より正確に検索できます。

レベルが Critical で、タイトルに Database を含むイベント

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

特定のエージェントにおける Warning または Critical のイベント

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

5. OR 条件検索

複数の条件のうち、**いずれか一つでも満たす**イベントを検索します。

タイトルまたはメッセージに特定のキーワードを含むイベント

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

6. 除外条件

特定の条件を除外して検索できます。

Info レベルを除いたすべてのイベント

```
not level: info
```

リアルタイムアラート

リアルタイムアラート機能は、イベント設定で設定したイベントが発生した際に、ポップアップ形式で表示されます。イベント発生と同時に通知を受け取ることで、問題を迅速に把握し、対応することができます。また、すでに発生した通知や見逃した通知の履歴を確認することで、リアルタイム対応が難しかった状況を把握し、解決に役立てることができます。

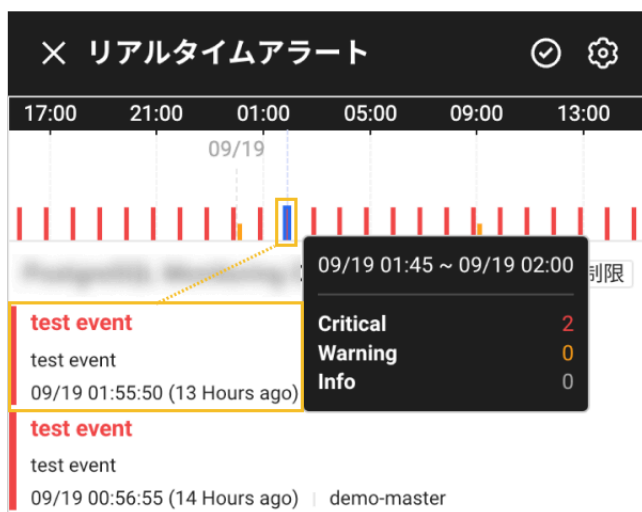
リアルタイムアラートを確認する

リアルタイムアラートは、画面右上にポップアップとして表示されます。通知が発生した時刻、タイトル、メッセージを確認できます。

- 個別の通知を閉じるには、メッセージ右上の ✕ ボタンをクリックしてください。
- 画面に表示されているすべてのポップアップ通知を閉じるには、**すべての通知を閉じる** をクリックしてください。

通知履歴を確認する

1. プロジェクトを選択して表示される画面の最上部にある 🔔 をクリックしてください。
2. リアルタイムアラート ウィンドウが表示されます。
 - 現在のプロジェクトについて、直近24時間以内の通知を最大100件まで確認できます。
 - 個別のイベント項目を選択すると、関連するメニューに移動します。
 - リアルタイムアラート ウィンドウ内の時間別チャートで任意の時間帯を選択すると、該当するイベント項目に移動します。



- すべての通知履歴を確認するには、**全体の通知履歴** ボタンをクリックしてください。**アラート通知 > イベント履歴** メニューに移動します。

❗ リアルタイムアラート の一覧が空の場合、**全体の通知履歴** ボタンが表示されます。受信タグ未設定の通知を受け取る オプションを無効にしてください。

イベントを一括で解消する

リアルタイムアラート の一覧から、進行中のすべてのイベントを一括で解消できます。

イベント解消が完了するまでに、約30秒～1分程度かかる場合があります。

- イベント一括処理** 機能を使用すると、現在進行中のイベントに対する解消通知が大量に発生する可能性があります。
- イベント一括処理** 機能を使用した後でも、イベントルールが有効であり、データが引き続きしきい値を超えている場合、イベントは再度発生することがあります。
- イベント解消通知は、**アラート通知 > イベント設定** メニューでイベントを編集し、**イベントが解消されたときに追加通知** または **解消通知** オプションを無効にすることで停止できます。

使用方法:

1. プロジェクトを選択して表示される画面上部の  をクリックします。
2. リアルタイムアラート ウィンドウが表示されたら、右上の  をクリックします。
3. リアルタイムアラートリストの進行中イベントを一括で解消します。 というメッセージが表示されたら、解消 ボタンをクリックします。

リアルタイムアラートを設定する

1. プロジェクトを選択して表示される画面上部の  をクリックします。
2. リアルタイムアラート ウィンドウが表示されたら、右上の  をクリックします。
3. リアルタイムアラート設定画面で各項目を設定します。
 - ポップアップ通知: リアルタイムアラート ウィンドウが閉じている状態でも、ポップアップ形式で通知を表示します。
 - 解消済みイベントを表示: リアルタイムアラート 一覧に解消済みイベントも含めて表示します。
 - 通知音の試聴: ブラウザで再生される通知音を事前に確認できます。Critical または Warning の横にある  をクリックしてください。音が再生されない場合は、ブラウザの設定をご確認ください。

システムイベント

WhaTap モニタリングは、プラットフォーム全体で自動的に検知・生成される共通イベントを提供します。本ドキュメントでは、システムによって発生するイベントの種類、発生条件、および対応方法について説明します。

EVENT_BLOCKED_BY_SYSTEM

プロジェクト内で短時間に過剰な数のイベントが発生した場合、WhaTap システムがこれを検知し、イベントの発生を一時的にブロックします。イベントがブロックされると、システムは次のメッセージをユーザーに通知します。このイベントが発生した場合は、イベント設定内容を確認し、必要に応じて調整してください。

 **Critical**



イベントメッセージ

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

プロジェクト番号	8
プロジェクト名	new server
対象	server agent
イベント名	EVENT_BLOCKED_BY_SYSTEM
イベント日時	(GMT+0900) 2024-11-18 18:03:18

WhaTapにログイン

new serverプロジェクトのserver agentから過度なイベントが検知されたため、イベント発生が遮断されます。server agentから一定期間の間にイベントが発生しなくなると、遮断が自動で解除されます。

ブロック基準

イベントは次の基準に基づいてブロックされます。

1. エージェント単位のブロック

1つのエージェントで **1分以内に10件** のイベントが発生した場合、そのエージェントから発生する以降のイベントはブロックされます。

2. 複数エージェントによる全体ブロック

条件 **1** によりイベントがブロックされたエージェントが **1分以内に3件以上** 発生した場合、プロジェクト全体のイベントがブロックされます。

3. プロジェクト単位のブロック

1つのプロジェクトで **1分以内に100件** のイベントが発生した場合、プロジェクト全体のイベントがブロックされます。

ブロック解除方法

システムによってイベントがブロックされた場合、対象のエージェントまたはプロジェクトで **1分間** イベントが発生しない状態を維持する必要があります。

- ・ **アラート通知 > イベント設定** メニューから設定されているすべてのイベントを無効化してください。 **イベント設定** を見直し、過剰なイベントが発生しないように閾値を調整する必要があります。
- ・ イベントを設定する前に、**シミュレーション** 機能を活用してイベント発生回数を事前に予測できます。

使用量分析

ネットワーク帯域幅使用量メニューでは、デバイスおよびインターフェースの過去のトラフィック推移を照会できます。最大31日間の履歴データを分析して長期トレンドを把握します。

基本画面と設定



1. 使用状況分析上部オプションバーの時間選択で照会する時間範囲を選択してください。最大31日まで設定可能です。

- **1分** をクリックするとデータ照会区間を変更できます。

クイック選択オプション	説明
直近5分	直近5分のデータを照会
直近10分	直近10分のデータを照会
直近1時間	直近1時間のデータを照会
直近1日	直近24時間のデータを照会（デフォルト）
直近7日	直近7日のデータを照会
直近21日	過去21日のデータを照会
本日 (0~24h)	本日00時から23:59までを照会
1日前 (0~24h)	1日前の00時から23:59までを照会
7日前 (0~24h)	7日前の00時から23:59までを照会

2. 上部オプションバーの**マネージャー選択**でデータを収集するNMSマネージャーを選択してください。

3. **デバイス選択**エリアで照会するデバイスまたはインターフェースを選択して使用量を分析できます。

- **デバイスリスト**: 登録されたデバイスが名前順に並んで表示されます。各デバイスを展開すると、そのデバイスのインターフェースリストが表示されます。

選択レベル	説明
デバイス	デバイス全体のトラフィック推移を表示
インターフェース	特定インターフェースの詳細推移を表示

チャートオプション

- 単位表示

トラフィックデータは自動的に適切な単位に変換されます。

値の範囲	単位
0 ~ 1,000	bps
1,000 ~ 1,000,000	Kbps
1,000,000 ~ 1,000,000,000	Mbps
1,000,000,000以上	Gbps

- ツールチップ

チャート上にマウスを重ねると、その時点の詳細な値を確認できます。複数シリーズの値が同時に表示されます。

使用量分析 - デバイス

デバイス選択エリアでデバイスを選択すると、そのデバイスの全トラフィック推移がチャートで表示されます。

基本チャート

チャート	説明
Total Throughput	全処理量（全幅）
Inbound Throughput	インバウンドトラフィック
Outbound Throughput	アウトバウンドトラフィック

Private MIBウィジェット

デバイスにカスタムOIDが設定されている場合、該当指標のチャートが追加表示されます。ウィジェット設定はローカルストレージに保存されます。

使用量分析 - インターフェース

デバイス選択エリアで特定のインターフェースを選択すると、そのインターフェースの詳細推移が表示されます。[使用量現況](#)のインターフェースビューと同じレイアウトです。

チャート

- トラフィック推移 (bps)
- PPS推移 (packets per second)
- エラー推移

照会結果のダウンロード

照会した画面をファイルとして保存できます。

1. 上段オプションバー右側の**ダウンロード**ボタンをクリックしてください。
2. ドロップダウンで保存形式を選択してください。

Item	Description
PDF	画面をA4規格の文書として保存。内容が長い場合は複数ページに分割
PNG	画面を1枚の画像として保存

キャプチャ範囲は右側のチャートエリアで、左側の**デバイス選択**パネルは含まれません。スクロールによって画面に表示されていないエリアも一緒に保存されます。

保存したファイルの上部には、次の情報が一緒に記録されます。

- 日付（照会期間）
- プロジェクト名
- Manager
- 対象（デバイスまたはインターフェース）

❗ 照会するデータがない場合、ダウンロードボタンは非活性状態で表示されます。保存に失敗した場合は、ファイルまたは画像のダウンロード失敗の案内が表示されます。

URLパラメーター

ページURLにパラメーターを含めることで、特定条件に直接アクセスできます。

パラメーター	説明
oid	NMSマネージャーOID
host	デバイスのHost IP
idx	インターフェースIndex
stime	開始時刻（タイムスタンプ）
etime	終了時刻（タイムスタンプ）

Logモニタリング

ログは、アプリケーションやシステムで発生するイベントやメッセージを記録するファイルです。異常を特定してシステムの劣化を防いだり、発生したトラブルの原因を確認する場合は、ログを確認することが重要です。

最近のITサービス構築環境は、MSA（マイクロサービスアーキテクチャ）やKubernetesベースへと移行が進んでおり、管理対象が増加しています。一般的なログモニタリングでは、サーバーに接続して `tail` コマンドやエディタを使ってログを確認します。しかし、個別のサーバーに逐一接続するような単純な方法では対応が困難です。では、数百～数千台のサーバーから発生するログを、どのようにして確認すればよいのでしょうか？

WhaTapログモニタリングサービスを使用すると、数多くのログを簡単に管理できます。

❗ Linuxの `tail` コマンドは、時間の経過とともにコンテンツを追加するログを確認するためによく使用されます。

主な機能

- 中央統合管理

WhaTapは、大量のログを中央で一元管理します。個別のサーバーにアクセスしなくても、中央からログを確認できるため、利便性に優れています。

- すべてのログを収集

ログを選別して収集する場合、重要なデータが欠落する可能性があります。WhaTapはすべてのログを収集し、収集されたログは **ライブテール** でリアルタイムに確認できます。

- 可視性確保

WhaTapのさまざまなチャートからログを確認できます。これにより、エラーや問題に関する情報へのアクセス性が向上し、障害の早期検知が可能になります。

- 柔軟な容量管理

個別のサーバーにログを保存する場合、ログによってファイルシステムの容量が過剰に占有される問題が発生する可能性があります。WhaTapを利用してログを中央に集約すれば、各サーバーでログファイルを保持する必要はなく、中央に保存されたログデータの保持期間のみを管理すれば済みます。

- 複数の分析的視点

障害の状況を把握し予測するためには、さまざまな観点からログを分析する必要があります。WhaTapでは、特定のタグを含むログ件数の推移を確認したり、フィルターを適用して分析したりすることができます。よく使うパターンはチャートとして保存し、いつでも呼び出して確認できます。

- パターン通知

障害のパターンをアラートとして設定することで、問題を予防したり迅速に把握したりすることができます。

WhaTapでは、個別のログに特定のキーワードが含まれている場合に通知を受け取る **リアルタイムログアラート** と、特定のタグを含むログ件数の推移を基準に通知を受け取る **複合ログアラート** を提供しています。

ログ分析

ライブテール

ライブテールメニューでは、リアルタイムで収集されたログを `tail` コマンドのように画面上で流れる形式で確認できます。

① 詳しくは、[ライブテール](#) のドキュメントを参照してください。

ログトレンド

ログトレンドメニューでは、収集されたすべてのログ、または特定のタグを含むログの件数推移を確認できます。ログの発生件数は障害の発生および解消のタイミングと密接に関連しているため、ログ件数の推移を通じて障害の原因を分析し、対応のスピードを向上させることができます。

① 詳しくは、[ログトレンド](#) のドキュメントを参照してください。

ログの検索

ログ検索メニューでは、収集されたすべてのログ、または特定のタグを含むログを照会できます。特定の時間帯やサーバーで発生したログをタグを基準にして検索・確認することができます。隣接ログ機能を使用すれば、特定のError

やException発生の前後に記録されたログをあわせて確認し、原因分析に活用できます。

① 詳しくは、[ログ検索](#) のドキュメントを参照してください。

ログエクスプローラー

ログエクスプローラー メニューを使用すると、ログデータを迅速に検索、フィルタリング、分析できます。フィールド構造を把握し、クエリベースのフィルタリングによって必要なログを効率的に検索し、その結果をデータとして可視化することができます。ログエクスプローラー機能は、Luceneインデックスを基盤として動作します。

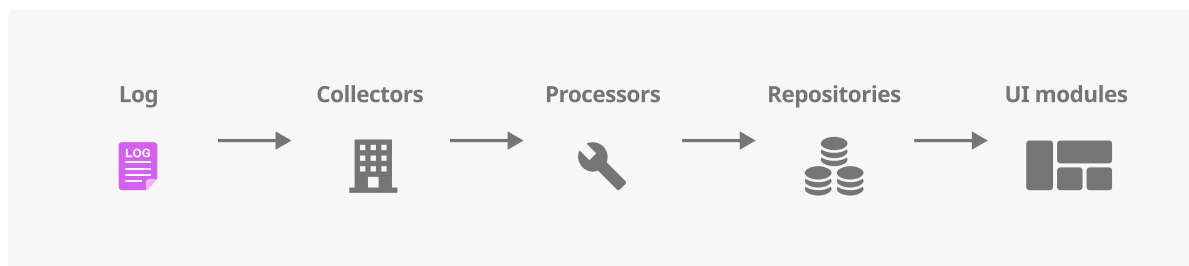
① 詳しくは、[ログエクスプローラー](#) のドキュメントを参照してください。

ログモニタリングを適用する

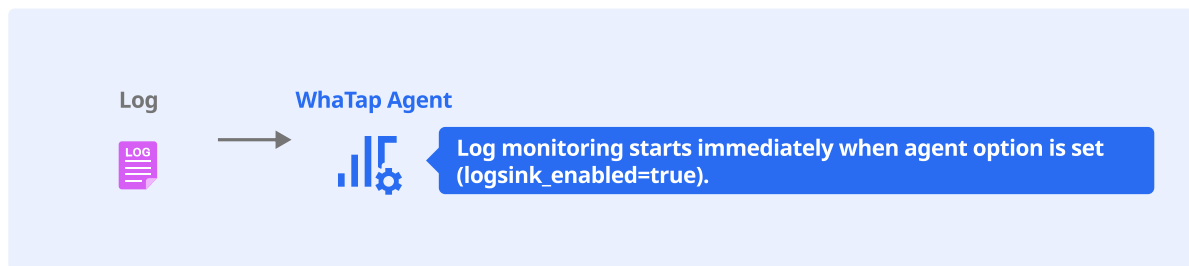
WhaTapログモニタリングサービスを利用するための基本的な使用方法について説明します。WhaTapログモニタリングは、追加のエージェントを構成やログのパーサを適用する必要はありません。簡単な設定で迅速に起動できます。

ログモニタリングの動作原理

Common log integration services



WhaTap log monitoring service



一般的なログ統合サービスは収集機、処理機、ストレージ、UIモジュールで構成されています。段階別設定と構成作業が必要なため、それぞれのモジュールを構築する過程が煩わしく、追加費用が発生します。

WhaTapログモニタリングは簡単に適用できます。既存のモニタリングエージェントがコレクターとして機能するため、エージェントオプションをオンにするだけでログモニタリングを開始できます。

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

- 出力されたファイルからログを読まずに、Javaアプリケーションのログライブラリに渡されるログを直接収集します。
- ログを直接収集するため、ファイルI/Oを引き起こさず、システムに与える性能への影響が非常に低いです。
- トランザクショントレースとログの接続を追跡する特徴を確保し、トレースからログを確認できます。

❗ Javaログのライブラリ

典型的なJavaログライブラリはApache Log4j、Logbackです。

❗ Java Agent2.1.1バージョンから使用できます。

- 既存のエージェントにログ収集機能を追加しました。モニタリングエージェントがログファイルから追加で出力されたログを読み取り読み取り収集する方法を利用します。

❗ PHP Agent2.3.2バージョンから使用できます。

- 既存のエージェントにログ収集機能を追加しました。モニタリングエージェントがログファイルから追加で出力されたログを読み取り読み取り収集する方法を利用します。
- ログにトランザクションIDを出力すると、トランザクショントレースとログの接続追跡性を確保し、トレースからログを確認できます。

❗ Python Agent1.2.2バージョンから使用できます。

- 既存のエージェントにログ収集機能を追加しました。モニタリングエージェントがログファイルから追加で出力されたログを読み取り読み取り収集する方法を利用します。
- 既存のエージェントにログ収集機能を追加しました。モニタリングエージェントがログファイルから追加で出力されたログを読み取り読み取り収集する方法を利用します。

❗ Server Agent2.1.2バージョンから使用できます。

- Kubernetesコンテナにログを収集できます。

- Kubernetesコンテナ内のアプリケーションからログを収集できます。

 Kubernetes Agent1.1.35バージョンから使用できます。

ログモニタリングを適用する

使用するアプリケーションに応じた適用方法は以下のとおりです。ログモニタリングを適用する前に、[対応バージョン](#)を必ずご確認ください。

1. 対応するエージェントのバージョンを確認し、**アップデート**してください。
2. ログモニタリング**オプション**を設定してください。
3. ログモニタリングを**有効**にしてください。

Java

Javaアプリケーションでログを収集する方法について案内します。

PHP

PHPアプリケーションからログを収集する方法について説明します。

Node.js

Node.jsアプリケーションでログを収集する方法を案内します。

 Python

Pythonアプリケーションからログを収集する方法について説明します。

 Go

Goアプリケーションからログを収集する方法について説明します。

 Server

サーバーアプリケーションからログを収集する方法について説明します。

 Kubernetes

Kubernetesコンテナとコンテナ内部のアプリケーションのログを収集する方法について説明します。

Java

Javaアプリケーションでログを収集するための設定方法を案内します。

エージェントのアップデート

Javaエージェントのバージョン2.1.1以降で利用可能です。アップデート方法については、[次のドキュメント](#)を参照してください。

エージェント設定の確認

ホーム画面 > プロジェクト選択 > ログ > ログ設定

1. WhaTapモニタリングサービスの初期画面でプロジェクトを選択した後、**ログ > ログ設定** メニューに移動してください。
2. **ログモニタリング開始タブの 1. エージェント設定の確認** の案内に従って、エージェント設定を確認してください。

エージェント設定

1. プロジェクトの **管理 > エージェントの設定** メニューをクリックしてください。
2. **オプション作成** の **オプション選択** ドロップダウンリストから **直接入力** をクリックし、`logsink_enabled=true` オプションを入力して **適用** ボタンをクリックして追加してください。
 - キー入力欄に `logsink_enabled` を入力してください。
 - 値入力欄に `true` を入力してください。
3. ログモニタリングを適用するには、アプリケーションを再起動します。

主なオプション

- `hooklog_enabled` `Boolean`

既定値 `false`

Logライブラリをフックして、ログモニタリングを有効化します。

- ① アプリケーションを実行する前に、[whatap.conf](#) オプションを有効にして、その後にログモニタリングの On/Off を `logsink_enabled` 設定で動的に制御できます。アプリケーションを起動する前に `logsink_enabled` オプションを `true` に設定する場合、このオプションを個別に設定しなくてもログモニタリングが可能です。

今後ログモニタリングを活用する可能性がある場合は、事前にこのオプションを設定することをお勧めします。

- **hooklog_custom_methods**

カスタムログを登録します。特定のログフレームワークの内容を収集します。サイトで個別に作成したログモジュールのログを追跡する際に利用してください。

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

既定値 `false`

Logモニタリング機能をOn/Offします。

- ① アプリケーションが起動する前に[whatap.conf](#)に `hooklog_enabled` オプションが設定されている場合、このオプションを使用すると、ログモニタリングのOn/Offを動的に制御することができます。

- **logsink_trace_enabled** Boolean

既定値 false

LogにトランザクションIDを挿入して、トランザクショントレースのログタブの表示有無を指定します。

ログモニタリングの活性化

ホーム画面 > プロジェクト選択 > ログ > ログ設定

ログモニタリングを開始する タブの 2. ログモニタリング機能の活性化 で、WhaTapログモニタリングを有効化または無効化できます。

-  ログモニタリングの有効化：トグルボタンをオンにするとログモニタリングが有効になり、有効化した日から15日間は無料でお試しいただけます。
-  ログモニタリングの無効化：トグルボタンをオフにするとログモニタリングが無効になり、以降ログは保存されません。

ⓘ ログモニタリングの有効化権限

エージェントをインストールした後、プロジェクトに対して編集権限を持つユーザーのみがログモニタリングを有効化できます。権限の詳細については、[次のドキュメント](#)を参照してください。

PHP

PHPアプリケーションでログを収集するための設定方法を案内します。

エージェントのアップデート

PHPエージェント2.3.2バージョンから可能です。アップデート方法は[次の文書](#)を参照してください。

エージェント設定の確認

ホーム画面 > プロジェクト選択 > ログ > ログ設定

1. WhaTapモニタリングサービスの初期画面でプロジェクトを選択した後、**ログ > ログ設定** メニューに移動してください。
2. **ログモニタリングを開始する** タブの **1. エージェント設定の確認** の案内に従って、エージェント設定を確認してください。

設定ファイルパスの確認

ログモニタリングするファイルの**設定ファイルパス**を確認してください。CLI環境または、ウェブで確認することができます。

CLI環境で確認する

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

❗ パスが"(None)"の場合、設定ファイルのパスは*/usr/whatap/php*です。

ウェブで確認する

CLI環境とApache環境でPHPの設定が異なる場合は、Web上で `phpinfo()` 関数の結果を確認してください。

コマンド入力

設定ファイルパスを含むコマンドを入力すると、ログモニタリングが開始されます。

```
export LOGFILES=/some/path/file1,/some/other/file2
echo "whatap.logsink_enabled=true" | sudo tee -a [設定ファイルパス]/whatap.ini
echo "whatap.logsink.files=$LOGFILES" | sudo tee -a [設定ファイルパス]/whatap.ini
```

ログモニタリングの活性化

ホーム画面 > プロジェクト選択 > ログ > ログ設定

ログモニタリングを開始する タブの 2. ログモニタリングの有効化 で、WhaTapのログモニタリングを有効または無効に設定できます。

-  ログモニタリングの有効化：トグルボタンをオンにするとログモニタリングが有効になり、有効化した日から15日間は無料でお試しいただけます。
-  ログモニタリングの無効化：トグルボタンをオフにするとログモニタリングが無効になり、以降ログは保存されません。

ⓘ ログモニタリングの有効化権限

エージェントをインストールした後、プロジェクトに対して編集権限を持つユーザーのみがログモニタリングを有効化できます。権限の詳細については、[次のドキュメント](#)を参照してください。

Node.js

Node.jsアプリケーションでログを収集するための設定方法を案内します。

エージェントのアップデート

Node.jsエージェント0.5.1バージョンから可能です。アップデート方法は、[次の文書](#)を参照してください。

エージェント設定の確認

ホーム画面 > プロジェクト選択 > ログ > ログ設定

1. Whatapモニタリングサービスの初期画面でプロジェクトを選択した後、**ログ > ログ設定** メニューに移動してください。
2. ログモニタリング開始タブの **1. エージェント設定の確認** の案内に従って、エージェント設定を確認してください。

エージェント設定

1. プロジェクトの **管理 > エージェントの設定** メニューをクリックしてください。
2. オプション作成 の オプション選択 ドロップダウンリストから **直接入力** をクリックし、`logsink_enabled=true` オプションを入力して **適用** ボタンをクリックして追加してください。
 - キー入力欄に `logsink_enabled` を入力してください。
 - 値入力欄に `true` を入力してください。
3. ログモニタリングを適用するには、アプリケーションを再起動します。

主なオプション

- `logsink_enabled` Boolean

既定値 `false`

ログモニタリングの活性化有無を設定します。

- `logsink_trace_txid_enabled` Boolean

既定値 `true`

ログにトランザクションIDを挿入して、トランザクション トレースのログタブの表示有無を指定します。

- `logsink_limit_content_enabled` Boolean

既定値 `true`

ログメッセージの最大サイズの制限有無を設定します。

- `logsink_limit_content_length` Number

既定値 `10,000`

ログメッセージの最大長さを設定します。この値は、`logsink_limit_content_enabled` オプションが `true` に設定された場合にのみ適用されます。

ログモニタリングの活性化

ホーム画面 > プロジェクト選択 > ログ > ログ設定

ログモニタリングを開始するセクションのログモニタリングを有効にするタブのトグルボタンで、WhaTapログモニタリングの有効または無効にできます。

-  ログモニタリングの有効化：トグルボタンをオンにするとログモニタリングが有効になり、有効化した日から15日間は無料でお試しいただけます。
-  ログモニタリングの無効化：トグルボタンをオフにするとログモニタリングが無効になり、以降ログは保存されません。

ⓘ ログモニタリングの有効化権限

エージェントをインストールした後、プロジェクトに対して編集権限を持つユーザーのみがログモニタリングを有効化できます。権限の詳細については、[次のドキュメント](#)を参照してください。

Python

Pythonアプリケーションでログを収集するための設定方法を案内します。

エージェントのアップデート

Pythonエージェント1.2.2バージョン以降で可能です。アップデート方法は[次の文書](#)を参照してください。

エージェント設定の確認

ホーム画面 > プロジェクト選択 > ログ > ログ設定

1. WhaTapモニタリングサービスの初期画面でプロジェクトを選択した後、**ログ > ログ設定** メニューに移動してください。
2. **ログモニタリングを開始する** タブの **1. エージェント設定の確認** の案内に従って、エージェント設定を確認してください。

ログ収集の活性化

設定ファイルパス(**WHATAP_HOME**)を含むコマンドを入力すると、ログ収集がすぐに開始されます。

```
export LOGFILES={ログファイル全体パス},...  
echo "logsink_enabled=true" | sudo tee -a {設定ファイルパス}/whatap.conf  
echo "logsink.files=$LOGFILES" | sudo tee -a {設定ファイルパス}/whatap.conf
```

ログとウェブトランザクションの連動

1.3.6 以降バージョン

1.3.6バージョンから次の方法でトランザクションとログの連動を設定できます。現在、WhaTapはPythonのlogging、loguruライブラリを対応しています。使用するPython Logライブラリに従って**whatap.conf**を構成してください。

- loggingモジュール

logging

```
echo "trace_logging_enabled=true" | sudo tee -a{設定ファイルパス}/whatap.conf
```

- loguruモジュール

loguru

```
echo "trace_loguru_enabled=true" | sudo tee -a{設定ファイルパス}/whatap.conf
```

1.3.6以前バージョン

トランザクションごとに発生したログを個別に照会できるように、ログにトランザクションID `{txid}` を出力します。WhaTapモニタリングでは、PythonのLogRecordに `{txid}` を自動的に注入し、フォーマッタを設定することでログファイルに `{txid}` を出力できるようにします。

```
settings.py
...
LOGGING = {
...
    'formatters': {
        ...
    },
    'handlers': {
        ...
    },
    'loggers': {
        ...
        '{ロガー名}': {
            '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'][ロガー名]['handlers'].append('whatap')
except:
    pass
...

```

ログモニタリングの活性化

ホーム画面 > プロジェクト選択 > ログ > ログ設定

ログモニタリングを開始する タブの 2. ログモニタリングの有効化 で、WhaTapのログモニタリングを有効または無効に設定できます。

-  ログモニタリングの有効化：トグルボタンをオンにするとログモニタリングが有効になり、有効化した日から15日間は無料でお試しいただけます。
-  ログモニタリングの無効化：トグルボタンをオフにするとログモニタリングが無効になり、以降ログは保存されません。

ⓘ ログモニタリングの有効化権限

エージェントをインストールした後、プロジェクトに対して編集権限を持つユーザーのみがログモニタリングを有効化できます。権限の詳細については、[次のドキュメント](#)を参照してください。

Go

Goアプリケーションでログを収集するための設定方法を案内します。

エージェント設定の確認

ホーム画面 > プロジェクト選択 > ログ > ログ設定

1. Whatapモニタリングサービスの初期画面でプロジェクトを選択した後、**ログ > ログ設定** メニューに移動してください。
2. **ログモニタリングを開始する** タブの **1. エージェント設定の確認** の案内に従って、エージェント設定を確認してください。

ログ収集の活性化

次のコマンドを入力すると、すぐにログの収集が開始されます。

```
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
```

ログモニタリングの活性化

ホーム画面 > プロジェクト選択 > ログ > ログ設定

ログモニタリングを開始する タブの **2. ログモニタリングの有効化** で、Whatapのログモニタリングを有効または無効に設定できます。

-  ログモニタリングの有効化：トグルボタンをオンにするとログモニタリングが有効になり、有効化した日から15日間は無料でお試しいただけます。
-  ログモニタリングの無効化：トグルボタンをオフにするとログモニタリングが無効になり、以降ログは保存されません。

ⓘ ログモニタリングの有効化権限

エージェントをインストールした後、プロジェクトに対して**編集権限**を持つユーザーのみがログモニタリングを有効化できます。権限の詳細については、[次のドキュメント](#)を参照してください。

Server

サーバーアプリケーションでログを収集するための設定方法を案内します。

エージェントのアップデート

サーバーエージェントのバージョン2.1.2以降で利用可能です。アップデート方法は [次の文書](#) を参照してください。

エージェント設定の確認

ホーム画面 > プロジェクト選択 > ログ > ログ設定

1. Whatapモニタリングサービスの初期画面でプロジェクトを選択した後、**ログ > ログ設定** メニューに移動してください。
2. ログモニタリングを始めるの1. エージェント設定の確認にある**OS選択**タブで、**Linux (shell) または Windows (PowerShell、管理者権限) **を選択してください。
3. **基本インストール**または**カテゴリ付きインストール**を参考にして、エージェント設定を確認してください。

⚠ 次の設定は、エージェントを再起動する必要があります。

Linux Shell

• 基本インストール

Linux Shell

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

• カテゴリ付きインストール

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  ## ログ発生量統計の別途データとしての送信有無
8  stats_enabled = true
9  ## 対数発生量の統計カテゴリ
10 stats_category = "logsink_stats"
11 ## ログファイルパス(path)にアスタリスク(*)が含まれ、除外するログ非対象ファイル名を設定
12 excludeNames = [ ".gz", ".zip" ]
13 [[inputs.logsink.file]]
14 ## ログファイルの指定時、日付パターン(strftime.org)指定可能
15 path = "/some/path/%Y-%m-%d/.log"
16 disabled = false
17 encoding = "utf-8"
18
19 [[inputs.logsink.file]]
20 path = "/some/other/log"
21 disabled = false
22 encoding = "utf-8"
23
24 [[inputs.logsink.file]]
25 ## 行単位ログで該当キーワードを検索する時、以前のログにマージ
26 nowrap_keywords = ["Caused by:", "Test"]
27
28 [[inputs.logsink.file]]
29 ## プロジェクトコード及びプロジェクトライセンスの入力時、ログを同じリージョンの希望するプロジェクトに転送可能
30 # pcode = プロジェクトコード
31 # license = "プロジェクトライセンス"
32
33 [[inputs.logsink.file]]
34 # whatap_host_ip = "収集サーバーIP1/収集サーバーIP2"
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},...] 形態をそれぞれのログに分離できる{"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

• 基本インストール

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"

```

• カテゴリ付きインストール

Windows Powershell

```

1  # 管理者権限が必要
2  New-Item -type "Directory" -Path "C:\\Program Files\\WhatapInfra\\extension"
3
4  $contentToAdd = @"
5  [[inputs.logsink]]
6  category = "serverlog"
7  ## ログ発生量統計の別途データとしての送信有無
8  stats_enabled = true
9  ## 対数発生量の統計カテゴリ
10 stats_category = "logsink_stats"
11 ## ログファイルパス(path)にアスタリスク(*)が含まれ、除外するログの非対象ファイル名を設定
12 excludeNames = [ ".gz", ".zip" ]
13 [[inputs.logsink.file]]
14 ## ログ ファイルの指定時、日付パターン(strftime.org)指定可能
15 path = "c:\\whatap\\logs%Y-%m-%d_.log"
16 disabled = false

```

```

17 encoding = "utf-8"
18
19 [[inputs.logsink.file]]
20 ## 行単位ログで該当キーワードを検索する時、以前のログにマージ
21 nowrap_keywords = ["Caused by:", "Test"]
22
23 [[inputs.logsink.file]]
24 ## プロジェクトコード及びプロジェクトライセンスの入力時、ログを同じリージョンの希望するプロジェクトに転送可能
25 # pcode = プロジェクトコード
26 # license = "プロジェクトライセンス"
27
28 [[inputs.logsink.file]]
29 # whatap_host_ip = "収集サーバーIP1/収集サーバーIP2"
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},...] 形態をそれぞれのログに分離することができる。
37 {"A":1,"B":2} {"C":3,"D":4}
38 multiline_pattern = "simple_json_array"
39
40 "@"
41
42 New-Item -path "C:\Program Files\WhatapInfra\extension" -name "logsink.conf" -type "file" -value $contentToAdd -Force
43
44 Restart-Service "Whatap Infra"

```

オプション設定

- `stats_enabled` : 収集ステータスデータの収集有無を設定します。(既定値: `false`)
 - `true` に設定する必要がある、`stats_category` で設定したカテゴリ（`logsink_stats`）に統計データが生成されます。
- `stats_category` : 収集ステータスデータを保存するメトリクスカテゴリを設定します。 `logsink_stats` に設定す

る必要があります。統計データのフィールドは次のとおりです。

保存される統計データフィールド: `file` `checkInterval` `encoding` `filepos` `checkedLocalTime`
`lastupdatedLocalTime` `fileSize` `error` `firstCheck` `transferBytes`

- **excludeNames** : ログファイルのパス (`path`) にアスタリスク (`*`) が含まれている場合、ログ収集対象外のファイル名を設定して除外することができます。カンマ (`,`) を区切り文字として使用することで、複数の値を設定できます。

Example

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

- **nowrap_keywords** : 行単位のログ検索時に、このオプションで指定されたキーワードが検出されると、前のログと結合されます。
- **pcode** : ログを送信する同じリージョンのプロジェクトコードを入力します。
- **license** : ログを送信する同じリージョンのプロジェクトのライセンスコードを入力します。

❗ `pcode` 、 `license` オプションの場合、サーバーエージェント2.7.4バージョン以降に対応します。

Windowsイベントログのオプション設定

Windowsイベントログ収集時、次のようにオプションを設定することができます。

```
1 # 管理者権限が必要
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     #プロジェクトコード及びプロジェクトライセンスの入力時、ログを同じリージョンの希望するプロジェクトに転送可能
22     #pcode = プロジェクトコード
23     #license = "プロジェクトライセンス"
24     #whatap_host_ip = "収集サーバーIP1/収集サーバーIP2"
25     #whatap_host_port = 6600
26
27 "@
28
29 New-Item -path "C:\Program Files\WhatapInfra\extension" -name "win_eventlog.conf" -type "file" -value $contentToAdd
   -Force
30
31 Restart-Service "Whatap Infra"

```

- カテゴリ指定(`category`) 必須
例) `win_event_log`
- 統計カテゴリ指定(`stats_category`) 必須
例) `win_event_log_stats`
- 統計カテゴリOn/Off(`stats_enabled`) 必須
例) `true` または `false`
- 収集機能On/Off(`enabled`) 必須
例) `true` または `false`
- ファイル別収集機能On/Off(`enabled`) 必須
例) `true` または `false`
- ファイル(`file`) 必須

例) Application、Security、Setup、System、Forwarded

- イベントタイプ(event_type) 非必須

例) 1、2、3、4、5

① イベントタイプ

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

- イベントID(event_id) 非必須
- イベントソース名(source_name) 非必須
- プロジェクトコード(pcode) 非必須
- プロジェクトライセンス(license) 非必須

① エージェント対応バージョン

- ウィンドウイベントログ収集の場合、サーバーエージェント2.5.2バージョン以降に対応します。
- ウィンドウイベントログオプションの中で pcode 、 license オプションの場合、サーバーエージェント2.7.4バージョン以降に対応します。

複数のファイルを指定および分離

複数のファイル指定

複数のログファイルを同じカテゴリに設定するには、各ログファイルのパスを `[[inputs.logsink.file]]` 項目に追加して、`path` 設定により、ファイルパスを指定します。また、`category`、`stats_enabled`、`stats_category` などのオプションを使用して、ログ発生量の統計設定などの付加的な設定が可能です。

/root/test1 および /root/test2 ファイルを同じカテゴリ（serverlog）に指定した例です。

```
[[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 などのオプションに関する詳細は、[オプション設定](#) を参照してください。

この例は、**ログTail** メニューで次のように確認できます。

serverlog			
▼	oname	時刻	
▼	APPSVR	2024-10-11 18:14:30.325	file /root/test1 pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709 kdjfhakdhgldkjggha;dfghad;fkjggha;dfkjggha;dfgjha;fkghj;fgjh
▼	APPSVR	2024-10-11 18:14:30.325	file /root/test1 pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709 kdjfhakdhgldkjggha;dfghad;fkjggha;dfkjggha;dfgjha;fkghj;fgjh
▼	APPSVR	2024-10-11 18:14:30.325	file /root/test1 pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709 kdjfhakdhgldkjggha;dfghad;fkjggha;dfkjggha;dfgjha;fkghj;fgjh
▼	APPSVR	2024-10-11 18:14:30.325	file /root/test1 pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709 kdjfhakdhgldkjggha;dfghad;fkjggha;dfkjggha;dfgjha;fkghj;fgjh
▼	APPSVR	2024-10-11 18:14:30.325	file /root/test1 pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709 kdjfhakdhgldkjggha;dfghad;fkjggha;dfkjggha;dfgjha;fkghj;fgjh
▼	APPSVR	2024-10-11 18:14:30.325	file /root/test1 pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709 kdjfhakdhgldkjggha;dfghad;fkjggha;dfkjggha;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

ファイル分離

異なるカテゴリにログファイルを割り当てるには、`logsink{数字}.conf` ファイルをそれぞれ作成し、各ファイルの `category` 項目に異なる値を設定してください。

`logsink.conf` と `logsink1.conf` を使用して、異なるログカテゴリを設定した例です。

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 などのオプションに関する詳細は、[オプション設定](#) を参照してください。

この例は、**ログTail**メニューで次のように確認できます。

検索条件		絞り込み	
All logs			
▼	oname	時刻	ログ内容
▼	APPSVR	2024-10-11 18:20:55.084	file /root/test1 pcode 34 oname APPSVR agenttime 1728638454313 oid 1988910709 category serverlog1 kdjfhakdhgldkjg ha,dfghad;fkjgha;dfkjgha;dfgjha;fkgjha;fgjh
▼	APPSVR	2024-10-11 18:20:55.087	file /root/test1 pcode 34 oname APPSVR agenttime 1728638454313 oid 1988910709 category serverlog1 kdjfhakdhgldkjg ha,dfghad;fkjgha;dfkjgha;dfgjha;fkgjha;fgjh
▼	APPSVR	2024-10-11 18:21:05.103	file /root/test2 pcode 34 oname APPSVR agenttime 1728638464315 oid 1988910709 category serverlog2 sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbcvmbn.bcmn
▼	APPSVR	2024-10-11 18:21:05.104	file /root/test2 pcode 34 oname APPSVR agenttime 1728638464315 oid 1988910709 category serverlog2 sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbcvmbn.bcmn
▼	APPSVR	2024-10-11 18:21:05.104	file /root/test2 pcode 34 oname APPSVR agenttime 1728638464315 oid 1988910709 category serverlog2 sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbcvmbn.bcmn
▼	APPSVR	2024-10-11 18:21:05.104	file /root/test2 pcode 34 oname APPSVR agenttime 1728638464315 oid 1988910709 category serverlog2 sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbcvmbn.bcmn
▼	APPSVR	2024-10-11 18:21:05.104	file /root/test2 pcode 34 oname APPSVR agenttime 1728638464315 oid 1988910709 category serverlog2 sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbcvmbn.bcmn

ログモニタリングの活性化

ホーム画面 > プロジェクト選択 > ログ > ログ設定

ログモニタリングを開始するセクションのログモニタリングを有効にするタブのトグルボタンで、WhaTapログモニタリングの有効または無効にできます。

-  ログモニタリングの有効化：トグルボタンをオンにするとログモニタリングが有効になり、有効化した日から15日間は無料でお試しいただけます。
-  ログモニタリングの無効化：トグルボタンをオフにするとログモニタリングが無効になり、以降ログは保存されません。

ⓘ ログモニタリングの有効化権限

エージェントをインストールした後、プロジェクトに対して編集権限を持つユーザーのみがログモニタリングを有効化できます。権限の詳細については、[次のドキュメント](#)を参照してください。

Kubernetes

Kubernetesコンテナおよびコンテナ内のアプリケーションのログを収集するための設定方法を案内します。

エージェントのアップデート

Kubernetesエージェント1.1.35バージョン以降で使用可能です。アップデート方法は[次の文書](#)を参照してください。

エージェント設定の確認

ホーム画面 > プロジェクト選択 > ログ > ログ設定

1. WhaTapモニタリングサービスの初期画面でプロジェクトを選択した後、**ログ > ログ設定** メニューに移動してください。
2. **ログモニタリングを開始する** タブの **エージェント設定およびログモニタリングの有効化** にある **1. エージェント設定の確認** の案内を参考にして、エージェント設定を確認してください。

コンテナログ収集の有効化

Kubernetesコンテナでログを収集するには、**1. エージェント設定の確認** で **ログ設定を適用** ボタンをクリックしてください。

コンテナの内部アプリケーションログ収集の有効化

Java 2.1.1、Python 1.2.2以降のバージョンで利用可能です。Kubernetesコンテナ上で実行されるアプリケーションのログを収集するには、以下を参考にしてください。

1. **ログ > ログ設定 > ログモニタリングを開始する** タブに移動してください。
2. **1. エージェント設定の確認** の下部にある  **エージェント設定** ボタンをクリックしてください。
3. **エージェント設定** で、**オプション作成** のオプション選択ドロップダウンリストから **直接入力** をクリックしてください。

4. エージェント設定コマンドのキー `logsink_enabled` と値 `true` を入力欄に入力してください。

```
logsink_enabled=true
```

5. 適用ボタンを選択します。Kubernetesコンテナ内のアプリケーションからログを収集できます。

- ① • Javaアプリケーションのログ収集に関する詳細は、[次のドキュメント](#)を参考にしてください。
- Pythonアプリケーションのログ収集に関する詳細は、[次のドキュメント](#)を参考にしてください。
- Goアプリケーションのログ収集に関する詳細は、[次のドキュメント](#)を参考にしてください。

ログモニタリングの活性化

ホーム画面 > プロジェクト選択 > ログ > ログ設定

ログモニタリングを開始するセクションのログモニタリングを有効にするタブのトグルボタンで、WhaTapログモニタリングの有効または無効にできます。

- ログモニタリングの有効化：トグルボタンをオンにするとログモニタリングが有効になり、有効化した日から15日間は無料でお試しいただけます。
- ログモニタリングの無効化：トグルボタンをオフにするとログモニタリングが無効になり、以降ログは保存されません。

① ログモニタリングの有効化権限

エージェントをインストールした後、プロジェクトに対して編集権限を持つユーザーのみがログモニタリングを有効化できます。権限の詳細については、[次のドキュメント](#)を参照してください。

Kubernetesログモニタリングのカテゴリガイド

Kubernetesに関するさまざまなログを確認できます。WhaTap Kubernetesでは、モニタリングカテゴリを提供しています。

⚠ 設定によって重複したログ内容が保存される場合があるため、重複がないか必ず確認してください。

カテゴリ	説明
#K8sEvent	- Kubernetesで発生したイベントがデフォルトで保存および作成されるログ - ユーザー設定に関係なく基本作成
#WhatapEvent	- WhaTapイベント設定によって発生したイベントが格納されるログ - ユーザー設定に関係なく、デフォルトで作成されます
containerStdout	- コンテナ標準出力ログ - ユーザー設定時に作成 - ノードエージェントに <code>logsink_enabled=true</code> 設定を追加したした場合
AppLog	- コンテナ内アプリケーションログ - ユーザー設定時に作成 - アプリケーションエージェントに <code>logsink_enabled=true</code> 設定の追加時

containerStdOutログフィルターの設定

ホーム画面 > プロジェクト選択 > 管理 > エージェント設定

Kubernetesログで必要な情報を選別するためのフィルタリングオプションを案内します。フィルタリングにより、許可または除外するログを設定できます。

1. 管理 > エージェント設定 に移動してください。
2. プロジェクトデフォルト タブで、オプション作成 方式から 直接入力 をクリックしてください。



ログネーミングのルール

Kubernetes containerStdOutログはノードの*/var/log/containers/*パスの下位に生成されます。次のようなネーミングルールに従っています。

```
<podName>_<namespace>_<containerName>-<containerId>.log
```

ログフィルターオプション

- **log_filter_enabled** bool

既定値 false

ログフィルターの使用有無を設定します。

- **log_filter_allow_list** list

許可するログの一覧を設定します。フィルタリングの適用時に含める項目を意味します。

- **log_filter_deny_list** list

除外するログの一覧を設定します。フィルタリングの適用時に除外する項目を意味します。

ログフィルター動作

`log_filter_enabled` オプションが有効になっている場合にのみ、ログフィルターが動作します。該当オプションの値が `true` に設定された状態で、`log_filter_allow_list` および `log_filter_deny_list` を通じてログを選択的に収集できます。

ログフィルターはブラックリストベースで動作します。例えば、`log_filter_enabled` 活性化した後 `log_filter_allow_list` オプションに追加する項目を設定しない場合、デフォルトではすべてのコンテナのログ収集がブロックされます。また、ログフィルターはallowルールよりdenyルールの優先順位が高いです。同一の項目がallowとdenyの両方に設定されている場合、denyルールが優先的に適用され、そのログは収集されません。

ログフィルターの例

単一ネームスペースログの収集

- 許容 `log_filter_allow_list` `*_infra_*`

`infra` ネームスペースに存在するすべてのコンテナが収集対象として特定されます。

マルチネームスペースログの収集

- 許容 `log_filter_allow_list` `*_infra_*`、`*_monitoring_*`

`infra`、`monitoring` ネームスペースに存在するすべてのコンテナが収集対象として特定されます。

特定の単語を含むPodを除く

- 許容 `log_filter_allow_list` `*_*_*`
- 除外 `log_filter_deny_list` `*prod*_*_*`

すべてのコンテナが収集対象として特定されますが、`podName` に `prod` が含まれているログは除外されます。

特定の単語を含むPodログの収集

- 許容 `log_filter_allow_list` `*prod*_*_*`

`podName` に `prod` が含まれるPodのログのみが収集されます。

マルチネームスペースログの収集と特定の単語を含むPodを除く

- 許容 `log_filter_allow_list` `*_infra_*`、`*_monitoring_*`
- 除外 `log_filter_deny_list` `*prod*_**`

`infra`、`monitoring` ネームスペースのログが収集され、`podName` に `prod` が含まれているログは除外されます。

コンテナ名内の特定の単語で始まるコンテナログを除外

- 許容 `log_filter_allow_list` `*_*_db-*`

すべてのネームスペースで `containerName` が `db` で始まるコンテナのログは除外されます。

ライブテール

ⓘ ログ参照権限がない場合は、そのメニューにアクセスできません。

ホーム画面 > プロジェクト選択 > ログ > ログTail

ログTail メニューでは、サーバーコンソールに接続せずに、ログデータストリームをモニタリング画面上で直接確認できます。複雑で大量のログも、フィルター と ハイライト 機能を活用して絞り込み、素早く把握できます。ログデータの取得周期は2秒です。

主な用語は次のとおりです。

- **Category**：ログの収集および照会単位
- **Content**：ログメッセージ
- **Search Key**：ログパーサーの設定によって生成される検索キー
- **Tag**：収集されたログを検索できるタグ

ⓘ ログテーブルカラムの端をドラッグしてカラムの幅を修正できます。

エージェントオプション

エージェントオプションが設定されている場合、ログレベルを収集し、各ログの左側に色付きの縦線が次のように表示されます。

2023-12-18 14:31:02.563	level	INFO	pcode	2277	agenttime	1702877462042	oid	778873916	category	AppLog	loggerName	io.home.test.logback02starter.base.web.LogbackControllerGreeting
												INFO log in our greeting method.
2023-12-18 14:31:02.563	level	WARN	pcode	2277	agenttime	1702877462043	oid	778873916	category	AppLog	loggerName	io.home.test.logback02starter.base.web.LogbackControllerError
											threadName	http-nio-19090-exec-2
												io.home.test.logback02starter.base.errors.exception.ApiException: [2204] Process failure. Please try again.
2023-12-18 14:31:02.586	level	error	pcode	2277	agenttime	1702877462043	oid	778873916	category	AppServer	event_status	error
											event_status_literal_name	level
												Servlet.service() for servlet [dispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.error
2023-12-18 14:31:02.586	level	error	pcode	2277	agenttime	1702877462057	oid	778873916	category	AppServer	event_status	error
											event_status_literal_name	level
												Servlet.service() for servlet [dispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.error
2023-12-18 14:31:02.586	level	error	pcode	2277	agenttime	1702877462081	oid	778873916	category	AppServer	event_status	error
											event_status_literal_name	level
												Servlet.service() for servlet [dispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.error
2023-12-18 14:31:02.586	level	error	pcode	2277	agenttime	1702877462087	oid	778873916	category	AppServer	event_status	error
											event_status_literal_name	level
												Servlet.service() for servlet [dispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.error

❗ エージェントのオプション設定

```
# whatap.conf
weaving=log4j-2.17
weaving=logback-1.2.8
```

- Javaエージェント2.2.22バージョンからウィービング設定にlog4j-2.17またはlogback-1.2.8設定時に使用できます。エージェントの再起動が必要です。
- ログレベルは、パーシングされたキーワードの中で level 、 type 基準で判別します。 level 、 type にパーシングされたキーが存在し、パーシングの値がFATAL、CRITICAL、ERROR、WARN、WARNING、INFOを含む場合は、ログレベルの色を表示します。

1 フィルター領域

フィルター適用

フィルターを適用すると、入力した条件に合ったログをフィルタリングします。複数のフィルターを入力できます。フィルターのタグが同じ場合、OR(||)、そうでない場合はAND(&&)が適用されます。

入力欄に文字を直接入力するか、**フィルター**入力欄をクリックしてフィルターを指定します。フィルタータグは **検索キー**、**オペレーター**、**検索値** の順に入力します。🔍 **検索** ボタンを選択すると、フィルターが適用されたデータをログ一覧で確認できます。

❗ ガイドUI

次のように入力ウィンドウの下に**ガイドUI**を提供します。入力画面またはフィルタータグにマウスカースールがある場合、**ガイドUI**を閉じる時はESCキーで操作できます。



検索キー、オペレーター、検索値の入力

- **検索キー** 入力時、一般インデックス、予約語インデックス、数字のみ入力できるインデックスを区分して推奨値を提供します。
- **オペレーター** 入力時、一般インデックス検索キーの場合は、`==`、`!=` オプションが下に表示されます。数字のみ入力できるインデックスの場合、`>`、`<`、`<=`、`>=`、`==`、`!=` オプションを提供します。
- **検索値** 入力時の一致検索(`>`、`<`、`<=`、`>=`、`==`)の時は青色で、除外検索(`!=`)の時は赤色でハイライトします。 **検索値** 入力時に大文字と小文字の区分オプションを活用して検索することができます。

- ⓘ
- フィルタータグが2行以上長くなる場合へ **折りたたみ**アイコンを選択して折りたたむことができます。
 - フィルタータグを入力した後、入力画面でShiftとTabキーを同時に使用して、以前のフィルタータグに移動できます。
 - フィルタータグを入力した後、入力画面でTABキーを通じて次のフィルタータグに移動できます。

フィルタータグ追加

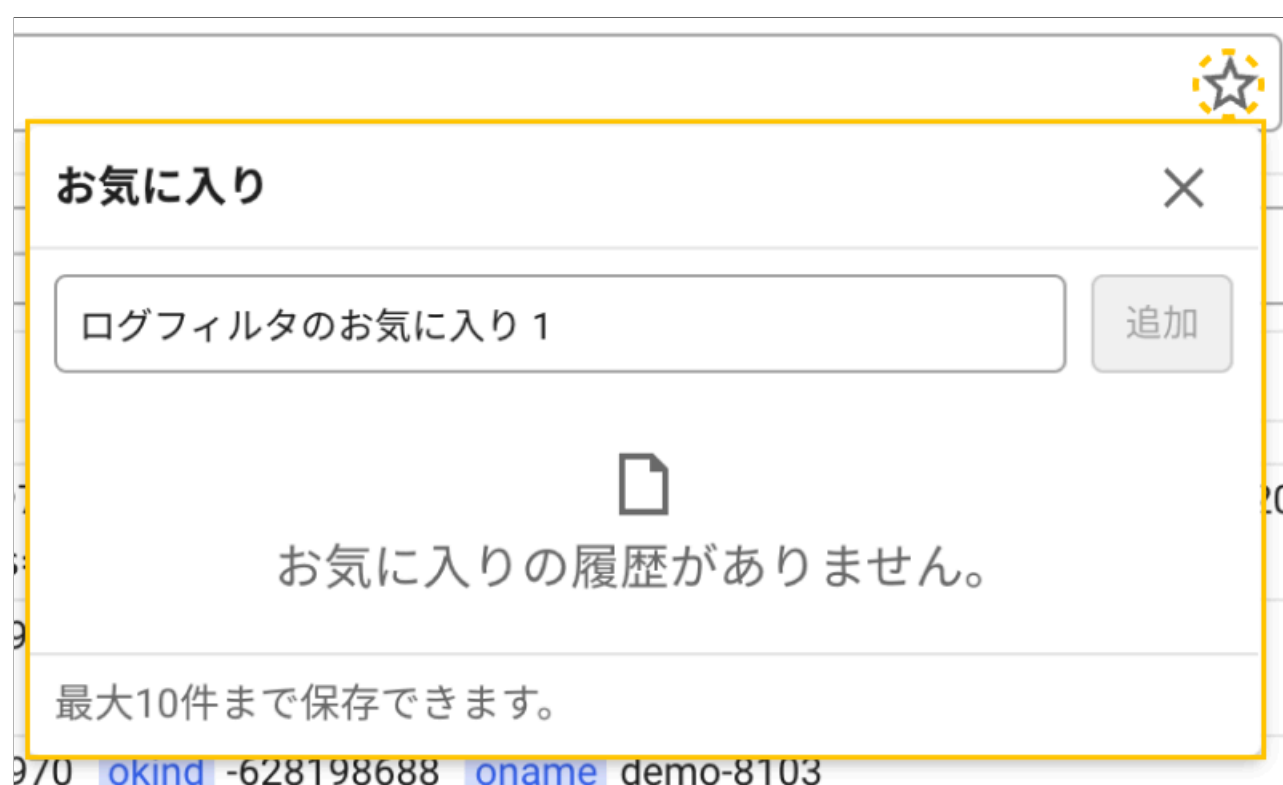
入力フィールドにテキストを入力し、Enter または Tab キーを押すか、入力欄下のガイド UI で推奨値をクリックまたは矢印キーで選択して追加できます。

フィルタータグの削除

単一のタグを削除するには、**Backspace** キーを押すか、タグ上の **X** アイコンをクリックします。すべてのタグを一度に削除するには、入力フィールド右側の **X** アイコンをクリックします。

フィルターのお気に入り

フィルターお気に入り機能を提供します。入力画面の右側にある ☆ お気に入り アイコンを選択して、目的のフィルター検索条件をお気に入りに追加、削除および既存のお気に入りを選択できます。お気に入りは最大50個まで保存されます。



フィルター適用の例外状況

- 数字のみ入力できるインデックス(.n で終わる 検索キー)を入力したタグで、 検索値 は数字のみ入力できます。
- 重複した 検索キー 、 検索値 は入力できません。
- 検索キー 、 検索値 いずれかのタグが存在しない場合は、検索できません。有効でないタグの場合、灰色と表示します。

❗ **ログTail** 検索キー として category は入力できません。

入力フィルター値の下にある数式(expression)は、ログデータを表示するときに適用されるフィルター式のプレビューです。

パースングされていないキーワードのフィルター適用

ログからパースングされていない、つまりインデックスが作成されていないキーワードを含むログを照会できます。この場合、指定範囲内のすべてのログをFull Scanします。そのため、インデックスが生成されたキーに比べて検索速度が多少落ちる可能性があります。定型化されたログデータの場合、**ログパーサの設定**を通じてインデックスキーを活用した検索をお勧めします。

フィルター ⓘ

▽

content

==

select

×

フィルターを入力してから「Enter」キーを押して追加

×

content == *select*

1. カテゴリを選択します。
2. フィルター入力欄に content を選択後、検索キーワードを入力します。
例) content *select*
3. 🔍 検索ボタンをクリックしてログを照会します。

- ❗ **ログTail**の場合、すべてのログ検索が可能であるため、カテゴリを指定する必要はありません。
- パーサ設定の詳細については、[次の文書](#)を参考にしてください。

フィルター修正

フィルターに値を入力し、入力した値をクリックすると、その値を修正できます。

The screenshot shows the 'フィルター' (Filter) interface. At the top, there's a search bar with a magnifying glass icon and a list of active filters: 'oname == ote-account', 'key == aws.base:index', and 'appender != fileAppender'. To the right of the filters is a text input field with the placeholder 'フィルターを入力してから「Enter」キーを押して追加' (Enter the filter and press 'Enter' to add it). Below the search bar, there's a checkbox labeled '大小文字を区別する' (Distinguish case) and a text input field labeled 'filterAppender'. To the right of this field is a table with search value options:

searchValue*	検索値で始まるログを検索します。 ex key!=searchValue*
*searchValue	検索値で終わるログを検索します。 ex key!=*searchValue
searchValue	検索値を含むログを検索します。 ex key!=*searchValue*
*search*Value*	検索値を含むログを検索します。 ex key!=*search*Value*
re:searchValue	正規表現に一致するログを検索します。 ex key!=re:searchValue
**	検索語に該当するすべてのログを検索します。 ex key!=**

At the bottom of the interface, there's a legend for the filter syntax: 'key == value' (一致) for '一致', 'key != value' (除外) for '除外', and 'key == value' (無効なタグです) for '無効なタグです'. There's also a 'ガイド表示' (Show guide) button.

- フィルター入力欄にテキストを書き換えて修正できます。
- フィルター入力欄の下に表示されるガイドUIから推奨値を選択して修正できます。

検索キー(Search Key)

次の画像で青いボックス部分はパーシング(parsing)された検索キーです。検索キーはログ設定のログパーサの設定タブでパーシングロジックを登録し、設定できます。

検索キー

フィルター入力の文法

タグは検索キーと検索値で構成されています。次の例で、検索キーは `exception`、検索値は `UnknownHostException` となります。この例は、収集したログデータのうち、IPアドレスとドメインアドレスが一致せず、サーバーをホストに接続できない場合に発生する例外(`UnknownHostException`)が含まれたログデータを照会

します。

exception == UnknownHostException

×

検索キーの種類

検索キーの種類	検索キーフォーマット	意味	検索キーと検索値の例	検索例
文字列キーワード	keyword	ファイル名	- キー: fileName - 値: /data/whatap/logs/yard.log	fileName:/data/whatap/logs/yard.log
数字キーワード	keyword.n	レスポンス時間	- キー: response_time.n - 値: 2945	response_time.n>=2945
予約語キーワード (辞書定義キーワード)	@keyword	TXID	- キー: @txid - 値: 85459614215434144	-
ログ本文キーワード	content	ログ本文	- キー: content - 値: ユーザー入力値	content: *ERROR*

ⓘ Content検索キー

- Content検索キーは、インデックスされていないログの本文を対象に検索します。例えば、`content *ERROR*` のように入力する場合は、ログ本文中で ERROR を含めたログを検索します。
- どのキーワードでインデックスをかけるべきかわからない場合は、Content検索キーを活用して問題となるキーワードを含むログを識別します。その後、**ログ設定メニュー**のログパーサ設定を通じて、該当キーワードでパーサを設定し、インデックスを生成する方式で、検索速度を早くできます。

共通文法

文法の種類	説明	例
<code>==searchValue</code>	検索値と一致するログを検索します。	<code>exception==RuntimeExceptionexception</code>
<code>!=searchValue</code>	検索値を除いたログを検索します。	<code>exception!=RuntimeException</code>
<code>*searchValue</code>	検索値で終わるログを検索します。	<code>word==*hello</code>
<code>searchValue*</code>	検索値で始まるログを検索します。	<code>word==hello*</code>
<code>*searchValue*</code>	検索値として中間に含まれるログを検索します。	<code>word==*hello*</code>
<code>*search*Value*</code>	検索値として含まれるログを検索します。	<code>word==*he*llo*</code>
<code>re:{正規表現}</code>	正規表現にマッチングされるログを検索します。	<code>caller==re:^(i\.w\.a\.w\.s\.v\.r\.</code>
<code>**</code>	検索語に該当するすべてのログを検索します。	

検索キーが数字キーワード(keyword.n)の場合の文法

次の文法は検索キーが、`keyword.n` 形式の場合のみに対応します。

- 検索値は数字のみ使えます。
- `.n` キーワードの値にはPrefixを付けません。`.n` 以外のキーワードは、すべてPrefixを付ける必要があります。

例) `+>searchValue` は有効ではありません。

文法の種類	説明	例
<code>>searchValue</code>	検索値よりも大きな値を含むログを照会します。	<code>response_time.n>3000</code>
<code>>=searchValue</code>	検索値よりも大きい、同じ値を含むログを照会します。	<code>response_time.n>=3000</code>
<code>==searchValue</code>	検索値と同じ値を含むログを照会します。	<code>response_time.n==3000</code>

文法の種類	説明	例
<code>!=searchValue</code>	検索値とは異なる値を含むログを照会します。	<code>response_time.n!=3000</code>
<code><searchValue</code>	検索値より小さい値を含むログを照会します。	<code>response_time.n<3000</code>
<code><=searchValue</code>	検索値より小さいか、同じ値を含むログを照会します。	<code>response_time.n<=3000</code>

個人情報の照会

ログの個人情報照会権限がある場合**個人情報の表示**  トグルボタンの活性化を通じて非識別化処理した個人情報を表示することができます。

- ① ログの個人情報照会権限についての詳細は[次の文書](#)を参照してください。
- ログ個人情報の非識別化機能についての詳細は[次の文書](#)を参照してください。

2 コンテンツハイライト領域

ログのコンテンツ内で目的のキーワードを簡単に識別できるよう、ハイライト機能を提供します。単一または複数のキーワードでフィルタリングできます。

ログTail

カテゴリー

AppLog

フィルター

content

+select*

×

フィルターを入力してから「Enter」キーを押して追加します。

content == +select*

act

🔍

⏸

🔄

🔍

⚙

	oname	タイムスタンプ	ログ
▶	demo-8102	2023-11-24 14:06:43.648	@txid 4785826165275137961 pcode 5490 oname demo-8102 onodeName node-0 oid 1387800924 okindName demo-okind-0 okind -1383513482 select distinct ename, deptno, sal, job from emp
▶	demo-8102	2023-11-24 14:06:43.654	@txid 4785826165275137961 pcode 5490 oname demo-8102 onodeName node-0 oid 1387800924 okindName demo-okind-0 okind -1383513482 select ename, 1000 from emp
▶	demo-8102	2023-11-24 14:06:43.659	@txid -240363117644553212 pcode 5490 oname demo-8102 onodeName node-0 oid 1387800924 okindName demo-okind-0 okind -1383513482 select distinct pp.lastname, pp.firstname
▶	demo-8102	2023-11-24 14:06:43.659	@txid 4785826165275137961 pcode 5490 oname demo-8102 onodeName node-0 oid 1387800924 okindName demo-okind-0 okind -1383513482 select 'total income is', ((orderqty * unitprice) * (1.0 - unitpricediscount)), ' for '

1. ハイライトしたいキーワードをキーワード入力欄に入力します。

- 例: `select`

2. 検索したキーワードがログリストのContent内でハイライト表示されます。

-  **拡大表示** アイコンをクリックすると、**ログ** と **タイムスタンプ** を全画面で確認できます。
- ハイライトされたキーワード間の移動はショートカットで操作できます。
 - `Enter` : 次の行へ移動
 - `Shift+Enter` : 前の行へ移動
 - `↑ / ↓` アイコン: 行の移動
 - `Cmd + F` (Mac) / `Ctrl + F` (Windows): キーワード検索

複数キーワード条件

複数キーワードでハイライトする場合は、次のように作成します。

入力文字列	説明	結果
<code>a b c</code>	各キーワードをスペースで区切ります。	a, b, c
<code>"Whatap is good."</code>	キーワードにスペースを含める場合は、 <code>"</code> または <code>"</code> で囲みます。	Whatap is good.
<code>"Whatap\\ is good."</code>	<code>"</code> で囲まれたキーワードに、 <code>\</code> を含める場合は、 <code>\\</code> と入力する必要があります。	Whatap\ is good.

ハイライトカラー設定

ハイライトするキーワードおよび色を設定できます。

- デフォルトでは、ログレベルに応じたハイライト (**FATAL**、**ERROR**、**WARN**、**SEVERE**、**CRITICAL**) が適用されています。
- 設定した内容は**プロジェクト単位**で保存されます。

1.  アイコンをクリックします。

2. **ハイライト** ウィンドウで、色を設定するキーワードを入力欄に追加してください。
3. 入力欄の左側の色をクリックすると、色を選択できます。

テーブル設定

カラム設定

2 領域の右で  **カラム設定** ボタンを選択します。カラムを追加したり、順序を設定できます。

- **カラム追加**

タグを選択してテーブルにカラムを追加できます。**log**カラム選択を解除する場合**ログ表示詳細設定**が確認できません。必ず1つ以上のカラムを選択します。

- **カラム順序設定**

カラムを追加すると**表示項目**に該当カラムが追加されます。希望のカラムをドラッグしてカラムの順序を変更します。

ログ表示詳細設定

2 領域右で  **ログ表示詳細設定** ボタンを選択します。デフォルトで**content**、**タグ**すべてチェックされており、両方の項目を表示します。**content**と**タグ**どちらかは必ず選択します。

チェックが解除されたアイテムはテーブルに表示されません。次のように**タグ**を解除する場合、テーブルでログの**タグ**は表示されません。

ログテーブルコンテンツタグ非表示

タグ管理一覧にタグを追加すると、追加した順にログのタグがソートされます。タグの順序はドラッグして変更できます。追加したタグを無効にすると、無効にしたタグはログのタグに表示されません。

❗ **カラムおよびログ表示設定の適用範囲**

- **カラム設定**と**ログ表示詳細設定**は、**ログTail**、**ログ検索**、**ログトレンド**で使用できます。
- 同一プロジェクト内の**ログTail**、**ログ検索**、**ログトレンド**は、**カラム設定**と**ログ表示詳細設定**を共有します。

ログファイルのダウンロード

検索したログの結果を **CSV** または **TXT** ファイル形式でダウンロードできます。

1. 画面中央右側の **↓ ダウンロード** ボタンをクリックします。
2. **CSVダウンロード** または **Logダウンロード** をクリックして、希望の形式のファイルをダウンロードします。

ログエクスプローラー

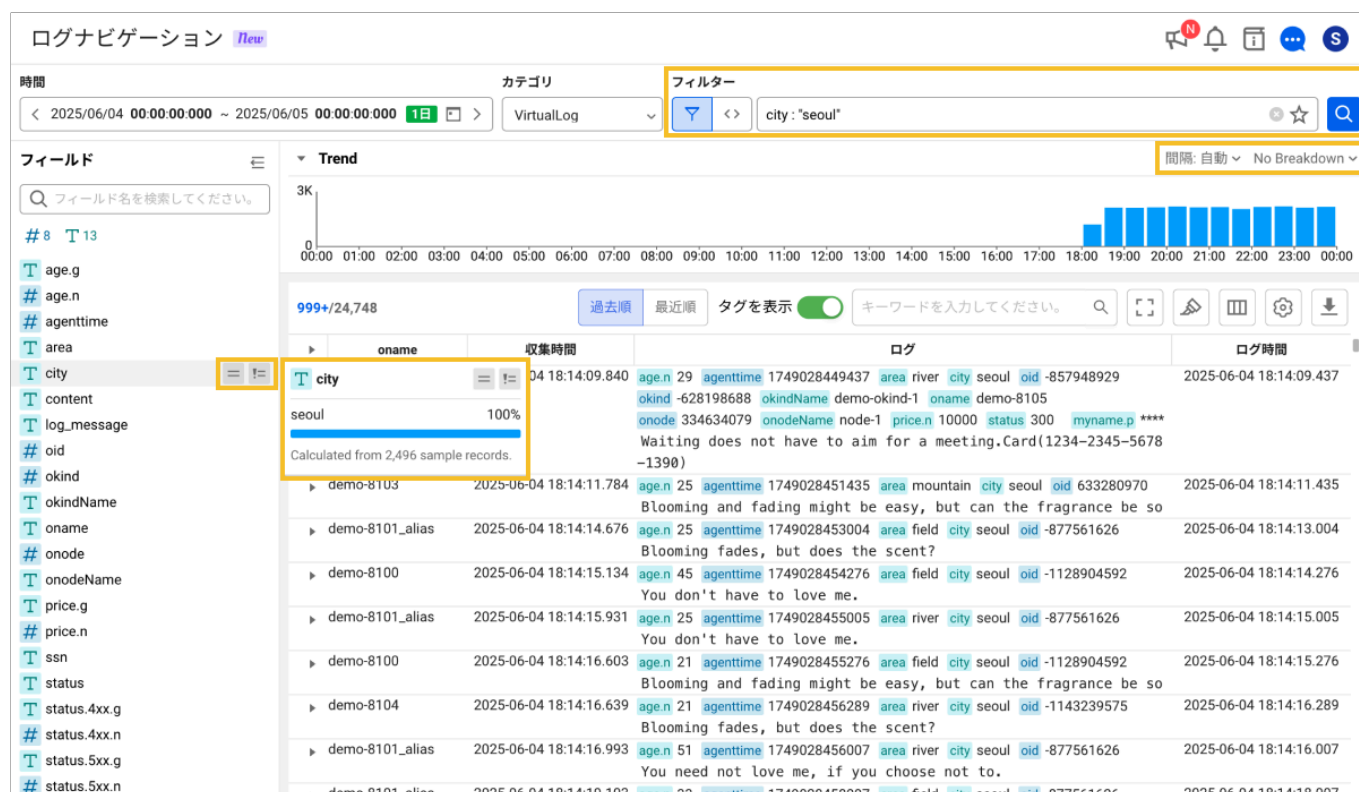
ⓘ ログ参照権限がない場合は、そのメニューにアクセスできません。

ホーム画面 > プロジェクト選択 > ログ > ログエクスプローラー *New*

ログエクスプローラー (Log Explorer) 機能は、ログデータを迅速に検索、フィルタリング、分析します。フィールド構造に関する情報を把握し、クエリベースのフィルタリングによって必要なログを効率的に検索し、結果をデータの可視化を通じて確認できます。本機能はLuceneインデックスをベースに動作し、主な特徴は以下のとおりです。

1. **ログトレンド分析および検索:** ログのトレンドと検索機能を同時にサポートし、時間経過によるログの変化傾向を把握できます。
2. **高速検索およびフィルタリング:** ユーザーは簡単なキーワード入力だけで、問題のあるログを迅速に検索できます。WhaTapログ検索クエリおよびLuceneクエリ言語に対応しており、さまざまな検索条件を設定できます。
3. **オートコンプリート機能:** クエリ入力時にオートコンプリート機能が提供され、ユーザーが簡単にクエリを作成し、習得できるようサポートします。
4. **データ可視化:** スタックグラフを活用して時系列のログ件数データを視覚的に表示し、ドリルダウン機能を通じて特定のログを深く分析できます。
5. **お気に入りと共有:** よく使うフィルターはお気に入りとして保存でき、URLを通じて他のユーザーと簡単に共有できます。

基本画面ガイド



時間設定

上部のオプションバーにある**タイムセレクト**を使用して、ログ検索の時間範囲を設定できます。

カテゴリ

上部のオプションバーにある**カテゴリ選択**で、探索したいログの種類を選択します。（例：AppLogなど）

フィルター

上部オプションバーの**フィルター**でクエリ言語を選択し、検索条件を入力してフィルターを適用します。
検索クエリ構文は、WhaTapログ検索クエリとLuceneクエリの両方をサポートしています。

-  : WhaTapログ検索クエリ
-  : Luceneクエリ

検索クエリ構文

WhaTap log search query

WhaTapのログ検索クエリはオートコンプリート機能を提供しており、簡単なキーワード入力だけで問題のログを迅速に検索できます。and、orなどのさまざまな構文を活用して、さまざまな検索条件を入力できます。

- 例、検索フィルターに `error` と入力するだけで、content（ログ本文）を検索できます。
 1. 上部オプションバーでフィルターアイコンをクリックした後、クエリ検索ウィンドウでフィールド（選択した時間とカテゴリに応じたリストが表示されます）を選択してください。
 2. 演算子を選択してください。
 - a. 基本: `:`、`*`、`and`、`or`
 - b. 選択したフィールドが `Number` 型の場合（基本 + `<=`、`>=`、`<`、`>`）
 - c. 選択したフィールドが `String` の場合（基本のみ）
 3. 値（選択した時間、カテゴリ、フィールドに一致するリストが表示されます）を選択してください。

検索インデックスフィールドタイプ

サポートされているフィールドタイプは、`Number`、`String`、`Boolean` の3種類のみです。

- `Number` : Long、double、float 型の数値
- `String` : メール本文のような全文テキスト
- `Boolean` : True または False の値

 WhaTapログ検索クエリの構文に関する詳細は[次の文書](#)を参照してください。

Lucene

Apache Lucene 8.11.1バージョンのオープンソースの構文がそのまま利用可能です。ただし、自動補完機能は提供していません。

❗ LuceneのQueryParserクラシックパッケージに関する詳細は[公式ドキュメント](#)を参照してください。

フィールド一覧

ドリルダウン分析に活用できます。

フィールド情報のフィルターを反映する

フィールド一覧でフィールド名を確認し、`=` または `!=` ボタンをクリックして条件をフィルターに適用してください。

- フィールドにマウスオーバーすると、`=`、`!=` ボタンが表示され、クリックするとフィルターに反映されます。
- フィールド検索機能を使って、目的のフィールドを素早く見つけることができます。

Trendチャート

Trendチャートでインターバルやブレイクダウンを適用して、ログをグラフで確認できます。

- グラフィインタラクション:** マウสดラッグや  ボタンで時間のズームイン、バークリックで該当領域のログを確認可能
- インターバル:** 自動、1秒、5秒、30秒、1分、5分、10分、30分、1時間から選択可能
- Breakdown:** 特定のフィールドを基準にTop 3 + Othersの値を分布として可視化し、ドリルダウンフィルターの適用が可能

breakdown

Breakdownは、ログ件数の推移を特定のフィールドで分析する可視化機能です。

- 特定のフィールドのTop 3の値とOthers（その他の値）を区別して、スタックグラフで分布を表示します。
- ドリルダウン分析に活用でき、凡例やスタックグラフの特定領域（部分グラフ）をクリックして、特定の値のみを

強調したり、フィルター条件を追加することができます。

ログの確認

検索条件に一致するログの一覧を確認でき、フィールド一覧ではフィールド情報とログタグが同じ色で表示されます。

コンテンツハイライト

ログのコンテンツ内で目的のキーワードを簡単に識別できるよう、ハイライト機能を提供します。単一または複数のキーワードでフィルタリングできます。

1. ハイライトしたいキーワードをキーワード入力欄に入力します。
 - 例: `select`
2. 検索したキーワードがログリストのContent内でハイライト表示されます。
 -  **拡大表示** アイコンをクリックすると、**ログ** と **タイムスタンプ** を全画面で確認できます。
 - ハイライトされたキーワード間の移動はショートカットで操作できます。
 - `Enter` : 次の行へ移動
 - `Shift+Enter` : 前の行へ移動
 - `^ / v` アイコン: 行の移動
 - `Cmd + F (Mac) / Ctrl + F (Windows)`: キーワード検索

複数キーワード条件

複数キーワードでハイライトする場合は、次のように作成します。

入力文字列	説明	結果
<code>a b c</code>	各キーワードをスペースで区切ります。	a, b, c
<code>"Whatap is good."</code>	キーワードにスペースを含める場合は、 <code>"</code> または <code>"</code> で囲みます。	Whatap is good.

入力文字列	説明	結果
"Whatap\\ is good."	""で囲まれたキーワードに、\を含める場合は、\\と入力する必要があります。	Whatap\ is good.

ハイライトカラー設定

ハイライトするキーワードおよび色を設定できます。

- デフォルトでは、ログレベルに応じたハイライト（FATAL、ERROR、WARN、SEVERE、CRITICAL）が適用されています。
- 設定した内容はプロジェクト単位で保存されます。
 - 🔗アイコンをクリックします。
 - ハイライト ウィンドウで、色を設定するキーワードを入力欄に追加してください。
 - 入力欄の左側の色をクリックすると、色を選択できます。

カラム設定

☐ ボタンをクリックして、カラムを追加したり順序を設定することができます。

カラム追加

カラム追加：タグを選択して、テーブルにカラムを追加できます。

⚠ ログカラムの選択を解除すると、ログ表示詳細設定を確認できません。必ず1つ以上のカラムを選択します。

カラム順序設定

カラム設定でカラムを追加すると、表示項目に該当カラムが追加されます。希望するカラムをドラッグして、カラムの順序を変更してください。

ログ表示詳細設定

⚙ ボタンをクリックして、ログの表示を詳細に設定します。デフォルトでは **content**、**タグ** の両方がチェックされており、両方の項目が表示されます。

- **content**と**タグ**のいずれかを必ず選択してください。
- **タグ管理**リストにタグを追加すると、追加した順にログのタグが表示されます。タグの順序はドラッグで変更できます。追加したタグを無効にすると、無効にしたタグはログのタグに表示されません。
- チェックが解除された項目は、テーブルに表示されません。次のように**タグ**を解除する場合、テーブルからログの**タグ**は表示されません。

log table contents remove tag sc

ⓘ カラムおよびログ表示設定の適用範囲

- **カラム設定**と**ログ表示詳細設定**は、**ログTail**、**ログ検索**、**ログトレンド**で使用できます。
- 同一プロジェクト内の**ログTail**、**ログ検索**、**ログトレンド**は、**カラム設定**と**ログ表示詳細設定**を共有します。

ログファイルのダウンロード

検索したログの結果を **CSV** または **TXT** ファイル形式でダウンロードできます。

1. 画面中央右側の **↓ ダウンロード** ボタンをクリックします。
2. **CSVダウンロード** または **Logダウンロード** をクリックして、希望の形式のファイルをダウンロードします。

WhaTap log search query 文法

👍 これは、WhaTapログエクスプローラーで使えるWhaTapログ検索クエリ構文に関するドキュメントです。

1. Equal

- `field : value`

2. Not

- `not field : value`

3. Wildcard (`String` タイプのフィールドのみ使用可能、検索値の前後に `"` は不)

- `field : val*`

4. Exist

- `field : *`

5. Range (`Number` タイプのフィールドのみ使用可能)

- `<` , `>` , `<=` , `>=` が使用可能
- 例: `field < 30 and field >= 10`

6. Combining Multiple Queries

- AND 例: `field < 30 and field >= 10`
- OR 例: `field < 30 or field >= 10`

7. Grouping

- 例: `(field < 30 or field >= 10) and other : 70`

8. Escaping Special Characters

- Luceneでエスケープが必要な特殊文字一覧: `&` `&` `|` `|` `!` `()` `{}` `^` `"` `~` `*` `?` `:` `\` `/`
- 文字の前に `\` を付けてエスケープする
- 例: `(1+1):2` を検索するには `\(1\+1\)\:2`

検索インデックスフィールドタイプ

サポートされるフィールドタイプは `Number` と `String` の2種類のみです。

- `Number` : Long、double、floatタイプの数値値
 - 使用例 : `field : "value"`
- `String` : メール本文のような全文テキスト
 - 使用例 : `field : value`
- `Boolean` : True または False
 - `field : true` または `field : false` の形式で使します

ログトレンド

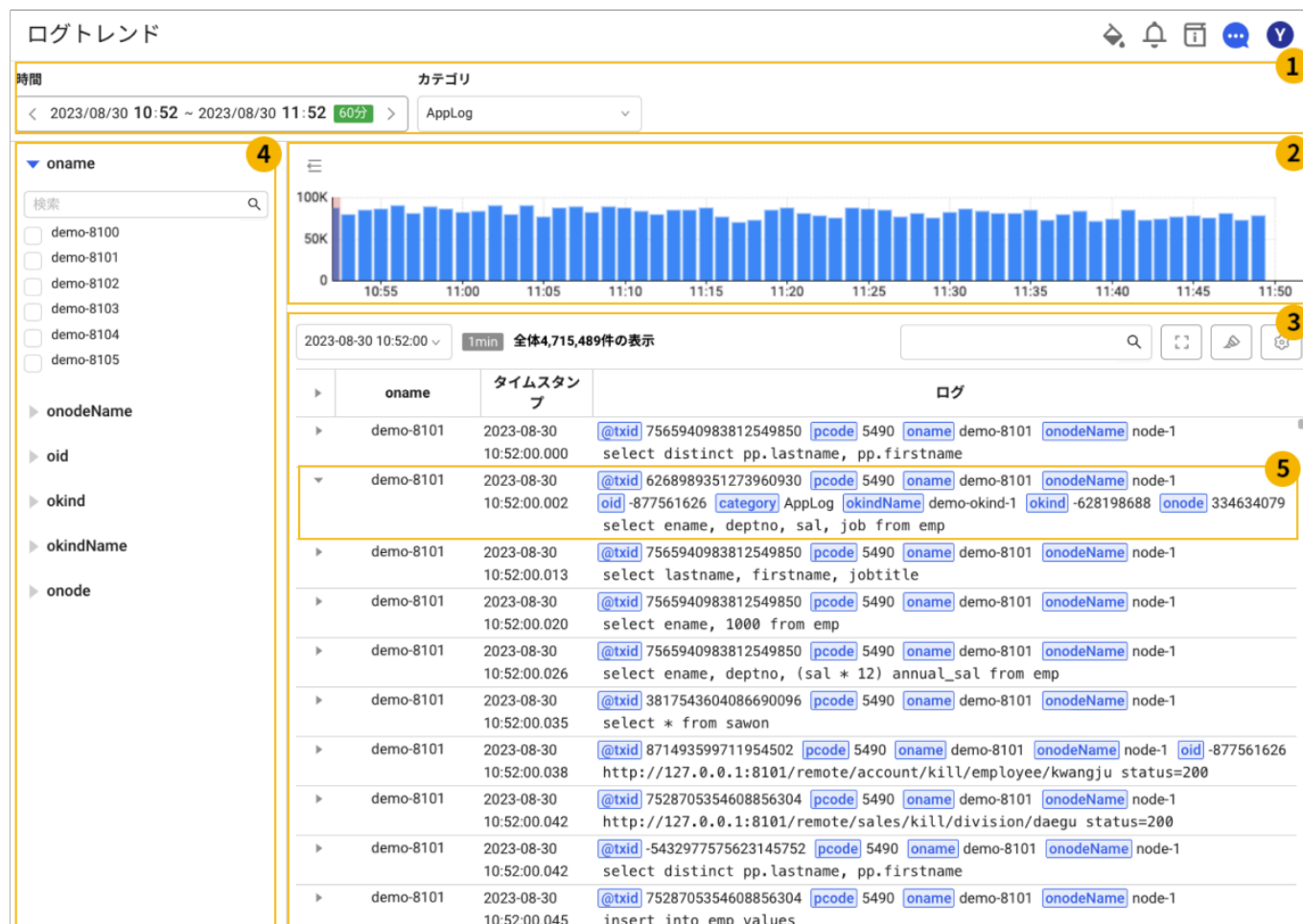
ⓘ ログ参照権限がない場合は、そのメニューにアクセスできません。

ホーム画面 > プロジェクト選択 > ログ > ログトレンド

ログトレンドでは、タイプ別に分類されたログの発生件数の推移を通じて、特定エラータイプの発生パターンを確認し、時間別の詳細ログデータを確認できます。ハイライト機能により、目的のログをすばやく識別できます。カテゴリ別に収集されたログの推移を照会できます。

主な用語は次のとおりです。

- **Category**：ログの収集および照会単位
- **Content**：ログメッセージ
- **Search Key**：ログパーサーの設定によって生成される検索キー
- **Tag**：収集されたログを検索できるタグ



データ参照

- 下部までスクロールすると、次のデータを表示します。
- 1で検索するログデータの時間と収集単位としてカテゴリを指定します。
- カテゴリを変更すると、選択されたカテゴリに対応するログを表示します。2バーチャートと3ログテーブルで確認できます。
- 2棒グラフのバーをクリックすると、バーの時間範囲に対応するログを検索します。
- 3ログテーブルの左上から照会されたログの総数を確認できます。
- 3 ログテーブル上段の右の「全画面」アイコンを選択すると、ログと収集時間を全画面で確認できます。
- 4 サイドメニューからタグでフィルタリングすることでログを確認できます。検索キーは最大2つまで選択でき、

検索値は複数選択できます。

- エージェントオプションが設定されている場合、ログレベルを収集し、各ログの左側に色付きの縦線が次のように表示されます。

2023-12-18 14:31:02.563	level	INFO	pcode	2277	agenttime	1702877462042	oid	778873916	category	AppLog	loggerName	io.home.test.logback02starter.base.web.LogbackControllerGreeting
												INFO log in our greeting method.
2023-12-18 14:31:02.563	level	WARN	pcode	2277	agenttime	1702877462043	oid	778873916	category	AppLog	loggerName	io.home.test.logback02starter.base.web.LogbackControllerError
											threadName	http-nio-19090-exec-2
												io.home.test.logback02starter.base.errors.exception.ApiException: [2204] Process failure. Please try again.
2023-12-18 14:31:02.586	level	error	pcode	2277	agenttime	1702877462043	oid	778873916	category	AppServer	event_status	error
											event_status_literal_name	level
												Servlet.service() for servlet [DispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.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	level
												Servlet.service() for servlet [DispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.err
2023-12-18 14:31:02.586	level	error	pcode	2277	agenttime	1702877462081	oid	778873916	category	AppServer	event_status	error
											event_status_literal_name	level
												Servlet.service() for servlet [DispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.err
2023-12-18 14:31:02.586	level	error	pcode	2277	agenttime	1702877462087	oid	778873916	category	AppServer	event_status	error
											event_status_literal_name	level
												Servlet.service() for servlet [DispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.err

❗ エージェントのオプション設定

```
# whatap.conf
weaving=log4j-2.17
weaving=logback-1.2.8
```

- Javaエージェント2.2.22バージョンからウィービング設定にlog4j-2.17またはlogback-1.2.8設定時に使用できます。エージェントの再起動が必要です。
- ログレベルは、パースされたキーワードの中で level 、 type 基準で判別します。 level 、 type にパースされたキーが存在し、パースの値がFATAL、CRITICAL、ERROR、WARN、WARNING、INFOを含む場合は、ログレベルの色を表示します。

- ❗ ログテーブルカラムの端をドラッグしてカラムの幅を修正できます。

個人情報の照会

ログの個人情報照会権限がある場合個人情報の表示  トグルボタンの活性化を通じて非識別化処理した個人情報を表示することができます。

- ❗ ログの個人情報照会権限についての詳細は次の文書を参照してください。
- ログ個人情報の非識別化機能についての詳細は次の文書を参照してください。

ログContentの確認

Content はログメッセージです。ログカラムの1行目には、パースされたキーと値が表示され、2行目にはContent（ログメッセージ）が表示されます。

- **3** ログテーブルの行(ログ)ごとに ▶ 詳細ボタンがあります。 ▶ 詳細ボタンを選択すると **5** のように、ログの全体 contentを確認できます。

ハイライト設定

目的のキーワードを簡単に識別できるように、ハイライト機能を提供しています。🔍 アイコンをクリックし、キーワードを入力してからEnterキーを押して追加してください。

コンテンツハイライト

ログのコンテンツ内で目的のキーワードを簡単に識別できるよう、ハイライト機能を提供します。単一または複数のキーワードでフィルタリングできます。

1. ハイライトしたいキーワードをキーワード入力欄に入力します。
 - 例: `select`
2. 検索したキーワードがログリストのContent内でハイライト表示されます。
 - **[] 拡大表示** アイコンをクリックすると、**ログ** と **タイムスタンプ** を全画面で確認できます。
 - ハイライトされたキーワード間の移動はショートカットで操作できます。
 - `Enter` : 次の行へ移動
 - `Shift+Enter` : 前の行へ移動
 - `^ / v` アイコン: 行の移動
 - `Cmd + F (Mac) / Ctrl + F (Windows)`: キーワード検索

複数キーワード条件

複数キーワードでハイライトする場合は、次のように作成します。

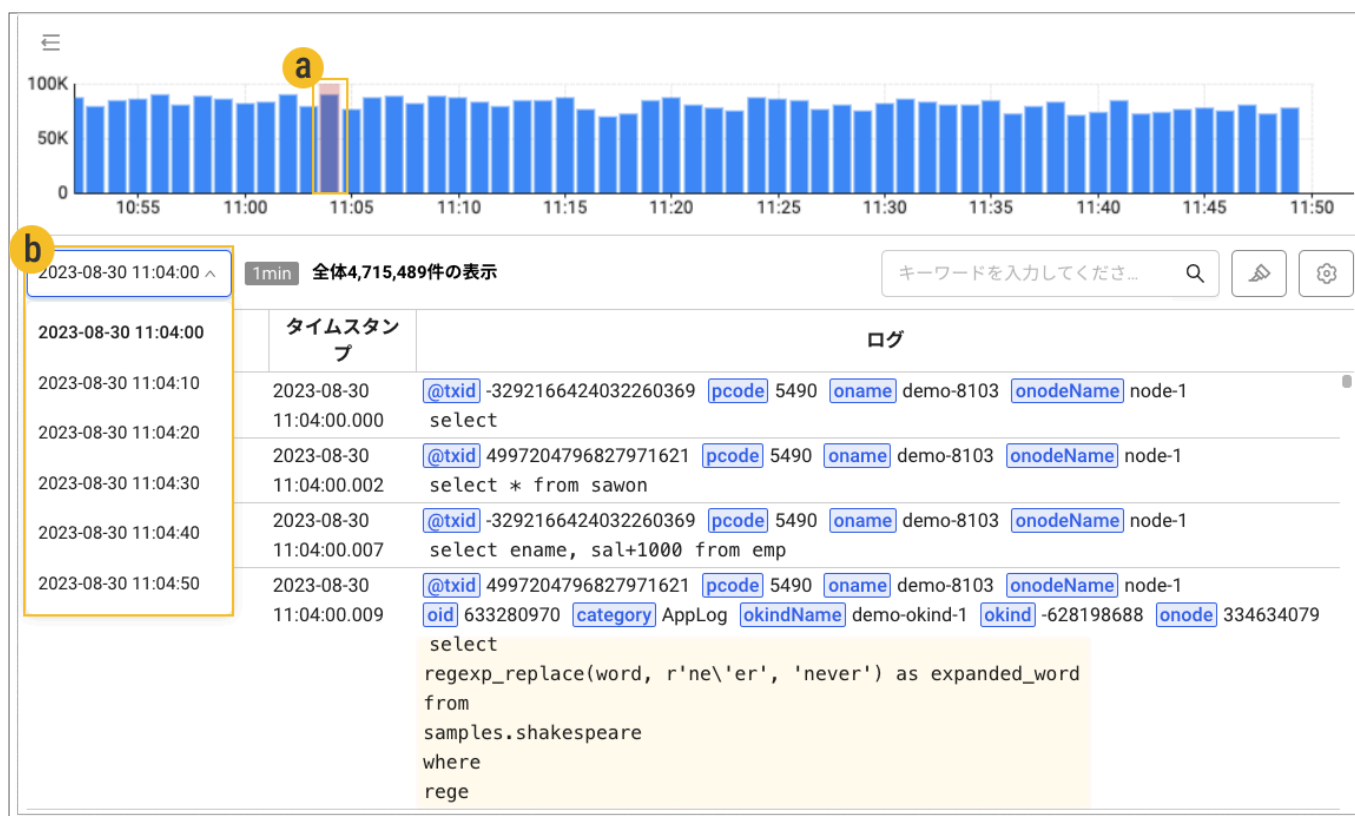
入力文字列	説明	結果
a b c	各キーワードをスペースで区切ります。	a, b, c
"Whatap is good."	キーワードにスペースを含める場合は、" または "" で囲みます。	Whatap is good.
"Whatap\\ is good."	""で囲まれたキーワードに、\ を含める場合は、\\ と入力する必要があります。	Whatap\\ is good.

ハイライトカラー設定

ハイライトするキーワードおよび色を設定できます。

- デフォルトでは、ログレベルに応じたハイライト（FATAL、ERROR、WARN、SEVERE、CRITICAL）が適用されています。
- 設定した内容はプロジェクト単位で保存されます。
 -  アイコンをクリックします。
 - ハイライト ウィンドウで、色を設定するキーワードを入力欄に追加してください。
 - 入力欄の左側の色をクリックすると、色を選択できます。

ログをチャートで検索



- バーチャートで **a** 目的の時間領域バーをクリックまたはドラッグして、その時間範囲のログを確認できます。
- 棒チャートの下ログテーブル上部左側の **b** 時間選択オプションを使用して、次のように選択した時間帯でより詳細なログ検索が可能です。
 - 1min : interval (チャート内の棒の間隔)
 - 時間選択オプション : 選択された時間範囲を6つの間隔に分割した時間帯

テーブル設定

カラム設定

3 領域の右で  **カラム設定** ボタンを選択します。カラムを追加したり、順序を設定できます。

- **カラム追加**

タグを選択してテーブルにカラムを追加できます。**log**カラム選択を解除する場合**ログ表示詳細設定**が確認できません。必ず1つ以上のカラムを選択します。

- **カラム順序設定**

カラムを追加すると**表示項目**に該当カラムが追加されます。希望のカラムをドラッグしてカラムの順序を変更します。

ログ表示詳細設定

3 領域右で  **ログ表示詳細設定** ボタンを選択します。デフォルトで**content**、**タグ**すべてチェックされており、両方の項目を表示します。**content**と**タグ**どちらかは必ず選択します。

チェックが解除されたアイテムはテーブルに表示されません。次のように**タグ**を解除する場合、テーブルでログの**タグ**は表示されません。

ログテーブルコンテンツタグ非表示

タグ管理一覧にタグを追加すると、追加した順にログのタグがソートされます。タグの順序はドラッグして変更できます。追加したタグを無効にすると、無効にしたタグはログのタグに表示されません。

ⓘ カラムおよびログ表示設定の適用範囲

- **カラム設定**と**ログ表示詳細設定**は、**ログTail**、**ログ検索**、**ログトレンド**で使用できます。
- 同一プロジェクト内の**ログTail**、**ログ検索**、**ログトレンド**は、**カラム設定**と**ログ表示詳細設定**を共有します。

ログファイルのダウンロード

検索したログの結果を **CSV** または **TXT** ファイル形式でダウンロードできます。

1. 画面中央右側の **↓ ダウンロード** ボタンをクリックします。
2. **CSVダウンロード** または **Logダウンロード** をクリックして、希望の形式のファイルをダウンロードします。

ログの検索

❗ ログ参照権限がない場合は、そのメニューにアクセスできません。

ホーム画面 > プロジェクト選択 > ログ > ログ検索

ログ検索メニューから収集された大量のログをさまざまな条件で検索し、ユーザーが必要なログを指定できます。複数の検索条件をパーシングされたキーとバリューで指定できるため、目的の条件に一致するログデータのみを抽出します。

動的ページで取得したログデータは、設定された行単位で取得され、スクロールで画面の下まで移動すると自動的に次のデータが取得されて表示されます。

主な用語は次のとおりです。

- **Category**：ログの収集および照会単位
- **Content**：ログメッセージ
- **Search Key**：ログパーサーの設定によって生成される検索キー
- **Tag**：収集されたログを検索できるタグ

1 ログ検索

時間 2023/08/30 11:28 ~ 2023/08/30 12:28 60分

フィルター ① category AppLog フィルターを入力してから「Enter」キーを押して追加します。 category == AppLog

2

AppLog (4,404,050)

AppStdErr (438)

AppStdOut (19,489)

3 全体4,424,485件の中、9999+件が検索条件に合致します。 過去 最近 タグを表示 キーワードを入力してください。

▶	oname	タイムスタンプ	ログ
▶	demo-8102	2023-08-30 11:28:00.003	@txid -8737177787317841782 pcode 5490 oname demo-8102 onodeName node-0 select productid, specialofferid, avg(unitprice) as [average price],
▶	demo-8102	2023-08-30 11:28:00.012	@txid 8009922019355005360 pcode 5490 oname demo-8102 onodeName node-0 select distinct pp.lastname, pp.firstname
▶	demo-8102	2023-08-30 11:28:00.008	@txid -8737177787317841782 pcode 5490 oname demo-8102 onodeName node-0 select ename, sal+1000 from emp
▼	demo-8102	2023-08-30 11:28:00.017	@txid -8737177787317841782 pcode 5490 oname demo-8102 onodeName node-0 oid 1387800924 category AppLog okindName demo-okind-0 okind -1383513482 onode 1693789385 select e.ename ' departments's name is:' d.dname from emp e, dept d where e.deptno=d.deptno
▶	demo-8102	2023-08-30 11:28:00.017	@txid 5677524395951858637 pcode 5490 oname demo-8102 onodeName node-0 http://127.0.0.1:8102/remote/account/kill/division/daegu status=200
▶	demo-8102	2023-08-30 11:28:00.019	@txid 8009922019355005360 pcode 5490 oname demo-8102 onodeName node-0 select ename, sal=sal+1000 from emp
▶	demo-8102	2023-08-30 11:28:00.030	@txid 8009922019355005360 pcode 5490 oname demo-8102 onodeName node-0 select employeeid, lastname, salary
▶	demo-8102	2023-08-30 11:28:00.025	@txid 8009922019355005360 pcode 5490 oname demo-8102 onodeName node-0 select productid, sum(linetotal) as total
▶	demo-8102	2023-08-30 11:28:00.033	@txid -8302816252130563957 pcode 5490 oname demo-8102 onodeName node-0 http://127.0.0.1:8102/remote/order/delete/dept/jeju status=200
▶	demo-8102	2023-08-30 11:28:00.041	@txid 8009922019355005360 pcode 5490 oname demo-8102 onodeName node-0 select pp.lastname, pp.firstname, e.jobtitle
▶	demo-8102	2023-08-30 11:28:00.036	@txid 8009922019355005360 pcode 5490 oname demo-8102 onodeName node-0 select * from emp

4

データ参照

- 画面の下までスクロールすると、次のデータを検索します。一度に、10,000個のログを参照できます。
- 3 ログテーブルの左上に検索されたログの総数を確認することができます。
- ログデータを時間の順と逆順で照会できます。3 ログテーブルの右上の古い順と新しい順の中から照会方式を選択します。
- 時間範囲を指定した後適用ボタンを選択して照会時間を設定し、🔍 検索ボタンを選択してデータを照会します。
- 3 ログテーブルの右上の🔍 拡大表示アイコンを選択すると、ログとタイムスタンプを全画面で確認できます。
- エージェントオプションが設定されている場合、ログレベルを収集し、各ログの左側に色付きの縦線が次のように表示されます。

2023-12-18 14:31:02.563	INFO	2277	1702877462042	778873916	AppLog	io.home.test.logback02starter.base.web.LogbackControllerGreeting	
	INFO log in our greeting method.						
2023-12-18 14:31:02.563	WARN	2277	1702877462043	778873916	AppLog	io.home.test.logback02starter.base.web.LogbackControllerError	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	error	2277	1702877462043	778873916	AppServer		
	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	error	2277	1702877462057	778873916	AppServer		
	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	error	2277	1702877462081	778873916	AppServer		
	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	error	2277	1702877462087	778873916	AppServer		
	Servlet.service() for servlet [DispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.error]						

① エージェントのオプション設定

```
# whatap.conf
weaving=log4j-2.17
weaving=logback-1.2.8
```

- Javaエージェント2.2.22バージョンからウィービング設定にlog4j-2.17またはlogback-1.2.8設定時に使用できます。エージェントの再起動が必要です。
- ログレベルは、パースされたキーワードの中で level 、 type 基準で判別します。 level 、 type にパースされたキーが存在し、パースの値がFATAL、CRITICAL、ERROR、WARN、WARNING、INFOを含む場合は、ログレベルの色を表示します。

① ログテーブルカラムの端をドラッグしてカラムの幅を修正できます。

ログContentの確認

Content はログメッセージです。ログカラムの1行目には、パースされたキーと値が表示され、2行目にはContent（ログメッセージ）が表示されます。

- ③ ログテーブルの行(ログ)ごとに ▶ 詳細ボタンがあります。 ▶ 詳細ボタンを選択すると ④ のように、ログの全体Contentを確認できます。
- ログのタグを選択すると、コピー, 検索, 除外検索, 隣接ログを検索できるドロップダウンメニューが表示されます。

フィルター

フィルター適用

① 左側の**時間選択バー**で時間範囲を指定できます。右側から、フィルターを適用すると、入力した条件に合ったログをフィルタリングします。複数のフィルターを入力できます。フィルターのタグが同じ場合、OR(||)、そうでない場合はAND(&&)が適用されます。

入力欄に文字を直接入力するか、**フィルター**入力欄をクリックしてフィルターを指定します。フィルタータグは **検索キー**、**オペレーター**、**検索値** の順に入力します。🔍 **検索** ボタンを選択すると、フィルターが適用されたデータをログ一覧で確認できます。

📌 ガイドUI

次のように入力ウィンドウの下に**ガイドUI**を提供します。入力画面またはフィルタータグにマウスカーソルがある場合、**ガイドUI**を閉じる時はESCキーで操作できます。



検索キー、オペレーター、検索値の入力

- **検索キー** 入力時、一般インデックス、予約語インデックス、数字のみ入力できるインデックスを区分して推奨値を提供します。
- **オペレーター** 入力時、一般インデックス検索キーの場合は、`==`、`!=` オプションが下に表示されます。数字のみ入力できるインデックスの場合、`>`、`<`、`<=`、`>=`、`==`、`!=` オプションを提供します。
- **検索値** 入力時の一致検索(`>`、`<`、`<=`、`>=`、`==`)の時は青色で、除外検索(`!=`)の時は赤色でハイライトします。 **検索値** 入力時に大文字と小文字の区分オプションを活用して検索することができます。

- ⓘ
- フィルタータグが2行以上長くなる場合へ **折りたたみ**アイコンを選択して折りたたむことができます。
 - フィルタータグを入力した後、入力画面でShiftとTabキーを同時に使用して、以前のフィルタータグに移動できます。
 - フィルタータグを入力した後、入力画面でTABキーを通じて次のフィルタータグに移動できます。

フィルタータグ追加

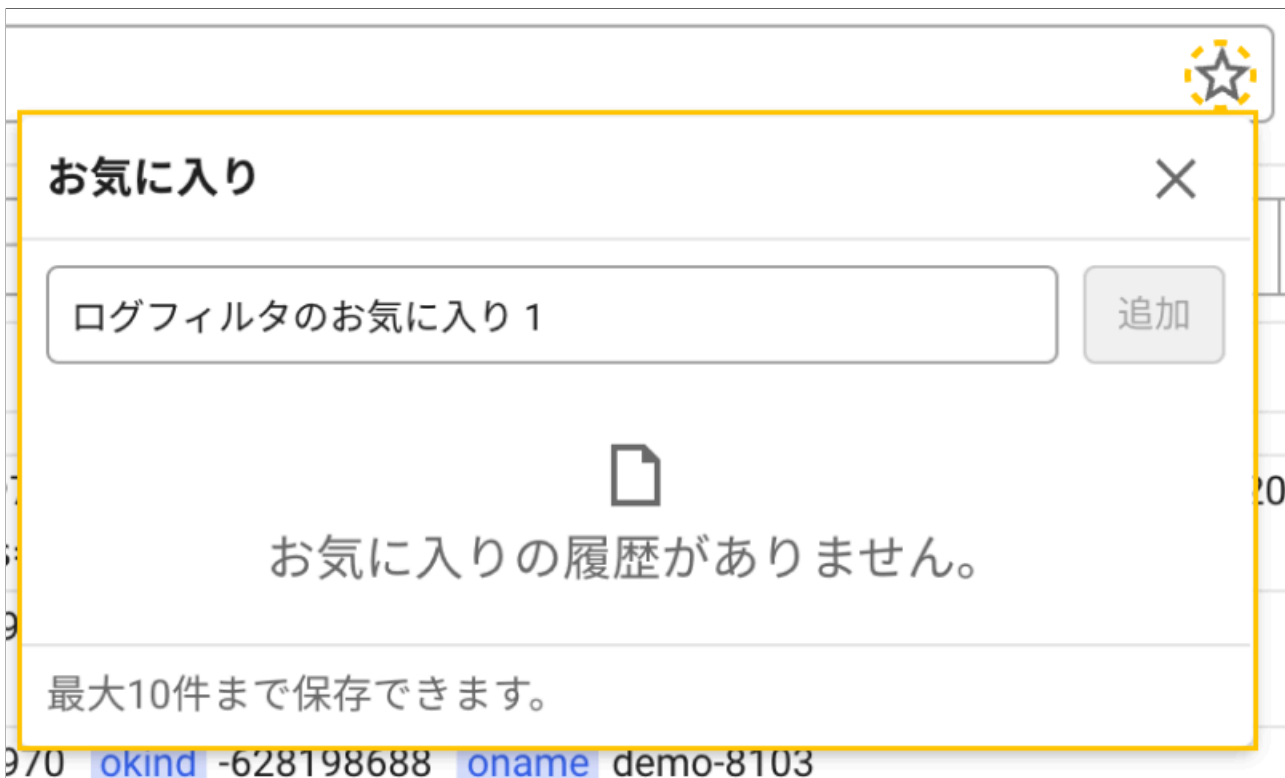
入力フィールドにテキストを入力し、Enter または Tab キーを押すか、入力欄下のガイド UI で推奨値をクリックまたは矢印キーで選択して追加できます。

フィルタータグの削除

単一のタグを削除するには、**Backspace** キーを押すか、タグ上の **X** アイコンをクリックします。すべてのタグを一度に削除するには、入力フィールド右側の **X** アイコンをクリックします。

フィルターのお気に入り

フィルターお気に入り機能を提供します。入力画面の右側にある ☆ お気に入り アイコンを選択して、目的のフィルター検索条件をお気に入りに追加、削除および既存のお気に入りを選択できます。お気に入りは最大50個まで保存されます。



フィルター適用の例外状況

- 数字のみ入力できるインデックス(.n で終わる 検索キー)を入力したタグで、 検索値 は数字のみ入力できます。
- 重複した 検索キー 、 検索値 は入力できません。
- 検索キー 、 検索値 いずれかのタグが存在しない場合は、検索できません。有効でないタグの場合、灰色と表示します。

構文解析されていないキーワードのフィルター適用

ログからパーシングされていない、つまりインデックスが作成されていないキーワードを含むログを照会できます。この場合、指定範囲内のすべてのログをFull Scanします。そのため、インデックスが生成されたキーに比べて検索速度が多少落ちる可能性があります。定型化されたログデータの場合、**ログパーサの設定**を通じてインデックスキーを活用した検索をお勧めします。

フィルター ⓘ

🔍 content == *select* ✕

フィルターを入力してから「Enter」キーを押して追加

✕

content == *select*

1. **カテゴリ**を選択します。カテゴリ指定が必須です。
2. **フィルター**入力欄に **content** を選択後、検索キーワードを入力します。
例) content *select*
3. 🔍 **検索**ボタンをクリックしてログを照会します。ログ全体の一部を先に照会します。1回あたりの検索結果は最大1万件です。
4. スクロールを下げて下段の**追加照会**ボタンを選択すると、つづけて照会できます。



- ❗ 全体ログのうち、サーバー照会範囲当たり1万件ずつ照会します。サーバー照会範囲の場合、基本20万件ですが、ログ全体の量によって比率が変わることがあります。
- パーサ設定の詳細については、[次の文書](#)を参考にしてください。

フィルター修正

フィルターに値を入力し、入力した値をクリックすると、その値を修正できます。

フィルター ⓘ

🔍 oname == ote-account × key == aws.base:index × appender != fileAppender × フィルターを入力してから「Enter」キーを押して追加 ×

☐ 大小文字を区別する

fileAppender

searchValue*	検索値で始まるログを検索します。 ex key!=searchValue*
*searchValue	検索値で終わるログを検索します。 ex key!=*searchValue
searchValue	検索値を含むログを検索します。 ex key!=*searchValue*
*search*Value*	検索値を含むログを検索します。 ex key!=*search*Value*
re:searchValue	正規表現に一致するログを検索します。 ex key!=re:searchValue
**	検索語に該当するすべてのログを検索します。 ex key!=**

key == value 一致 key != value 除外 key == value 無効なタグです。 ⓘ ガイド表示

- ・ フィルター入力欄にテキストを書き換えて修正できます。
- ・ フィルター入力欄の下に表示されるガイドUIから推奨値を選択して修正できます。

検索キー(Search Key)

検索キーは、ログデータ内で希望する特定の値にアクセスするための識別子を意味します。検索キーに該当する実際のデータが検索値です。左側の②領域のタグはカテゴリ別にパーシング(parsing)された検索キーです。タグを選択してフィルターを入力します。オレンジ色タグはカテゴリで、青色タグは検索キーです。

例えば②領域のAppLogとAppStdOutはカテゴリであり、その下のoidなどのタグは、パーシング(parsing)された検索キーです。検索キーはログ>ログ設定のログパーサの設定タブでパーシングロジックを登録し、設定できます。

フィルター入力文法

タグは検索キーと検索値で構成されています。次の例で、検索キーは `exception`、検索値は `UnknownHostException` となります。この例は、収集したログデータのうち、IPアドレスとドメインアドレスが一致せず、サーバーをホストに接続できない場合に発生する例外(`UnknownHostException`)が含まれたログデータを照会します。

exception == UnknownHostException

×

検索キーの種類

検索キーの種類	検索キーフォーマット	意味	検索キーと検索値の例	検索例
文字列キーワード	keyword	ファイル名	- キー: fileName - 値: /data/whatap/logs/yard.log	fileName:/data/whatap/logs/yard.log
数字キーワード	keyword.n	レスポンス時間	- キー: response_time.n - 値: 2945	response_time.n>=2945
予約語キーワード (辞書定義キーワード)	@keyword	TXID	- キー: @txid - 値: 85459614215434144	-

共通文法

文法の種類	説明	例
<code>==searchValue</code>	検索値と一致するログを検索します。	<code>exception==RuntimeExceptionexception</code>
<code>!=searchValue</code>	検索値を除いたログを検索します。	<code>exception!=RuntimeException</code>
<code>*searchValue</code>	検索値で終わるログを検索します。	<code>word==*hello</code>
<code>searchValue*</code>	検索値で始まるログを検索します。	<code>word==hello*</code>
<code>*searchValue*</code>	検索値として中間に含まれるログを検索します。	<code>word==*hello*</code>
<code>*search*Value*</code>	検索値として含まれるログを検索します。	<code>word==*he*llo*</code>

文法の種類	説明	例
re:{正規表現}	正規表現にマッチングされるログを検索します。	caller==re:^i\.w\.a\.w\.s\.v\.r\.
**	検索語に該当するすべてのログを検索します。	

検索キーが数字キーワード(keyword.n)の場合の文法

次の文法は検索キーが、 keyword.n 形式の場合のみに対応します。

- 検索値は数字のみ使えます。
- .n キーワードの値にはPrefixを付けません。 .n 以外のキーワードは、すべてPrefixを付ける必要があります。

例) +>searchValue は有効ではありません。

文法の種類	説明	例
>searchValue	検索値よりも大きな値を含むログを照会します。	response_time.n>3000
>=searchValue	検索値よりも大きいか、同じ値を含むログを照会します。	response_time.n>=3000
==searchValue	検索値と同じ値を含むログを照会します。	response_time.n==3000
!=searchValue	検索値とは異なる値を含むログを照会します。	response_time.n!=3000
<searchValue	検索値より小さい値を含むログを照会します。	response_time.n<3000
<=searchValue	検索値より小さいか、同じ値を含むログを照会します。	response_time.n<=3000

個人情報の照会

ログの個人情報照会権限がある場合**個人情報の表示**  トグルボタンの活性化を通じて非識別化処理した個人情報を表示することができます。

- ❗ ・ ログの個人情報照会権限についての詳細は[次の文書](#)を参照してください。

- ・ ログ個人情報の非識別化機能についての詳細は[次の文書](#)を参照してください。

ログのタグオプション

ログのタグを選択すると、ドロップダウンメニューが表示されます。検索、除外検索、隣接ログ、トランザクション情報オプションが確認できます。

≡

全体90,699件の表示

過去順

最近順

キーワードを入力してください。

🔍

🔄

📄

🏠

⚙️

▶	oname	タイムスタンプ	ログ
▶	java-demo3	2025-04-17 09:17:13.018	@txid 7759974649447934516 pcode 8 onodeName node-0 oid -278185929 okind 1152715164 oname java-demo3 eException: random exception
▶	java-demo3	2025-04-17 09:17:13.018	demo3 onodeName node-0 agentime 1744849031927 oid -278185929 category AppStdErr okindName dev-okind-0 rtual.web.Simula.exec(Simula.java:79)
▶	java-demo3	2025-04-17 09:17:13.018	demo3 onodeName node-0 agentime 1744849031927 oid -278185929 category AppStdErr okindName dev-okind-0 ion: java.lang.RuntimeException: random exception
▶	java-demo3	2025-04-17 09:17:13.018	demo3 onodeName node-0 agentime 1744849031928 oid -278185929 category AppStdErr okindName dev-okind-0 rtual.web.VExec.doFilter(VExec.java:16)

コピー

検索

除外検索

隣接ログ

トランザクション...

ログタグ オプション メニュー	説明
コピー	該当するタグのログをコピーします。
検索	フィルターには、該当のタグを含む ('==') 条件で入力されます。
除外検索	フィルターには、該当のタグを除外する ('!=') 条件で入力されます。
隣接ログ	隣接ログの詳細画面では、選択したログのサーバーを対象に、選択したログと隣接する時間帯のログを照会できます。時間を選択して、周辺の時間帯に発生したログを確認することも可能です。基準となるログは青い背景で表示されます。
トランザクション 情報	ログに @txid や @mtid タグが含まれている場合は、トランザクション情報をクリックすると、トランザクション情報の詳細画面で内容を確認できます。

コンテンツハイライト

ログのコンテンツ内で目的のキーワードを簡単に識別できるよう、ハイライト機能を提供します。単一または複数のキーワードでフィルタリングできます。

1. ハイライトしたいキーワードをキーワード入力欄に入力します。
 - 例: `select`
2. 検索したキーワードがログリストのContent内でハイライト表示されます。
 -  **拡大表示** アイコンをクリックすると、**ログ** と **タイムスタンプ** を全画面で確認できます。
 - ハイライトされたキーワード間の移動はショートカットで操作できます。
 - `Enter` : 次の行へ移動
 - `Shift+Enter` : 前の行へ移動
 - `↑ / ↓` アイコン: 行の移動
 - `Cmd + F` (Mac) / `Ctrl + F` (Windows): キーワード検索

複数キーワード条件

複数キーワードでハイライトする場合は、次のように作成します。

入力文字列	説明	結果
<code>a b c</code>	各キーワードをスペースで区切ります。	a, b, c
<code>"Whatap is good."</code>	キーワードにスペースを含める場合は、 <code>"</code> または <code>"</code> で囲みます。	Whatap is good.
<code>"Whatap\\ is good."</code>	<code>"</code> で囲まれたキーワードに、 <code>\</code> を含める場合は、 <code>\\</code> と入力する必要があります。	Whatap\ is good.

ハイライトカラー設定

ハイライトするキーワードおよび色を設定できます。

- デフォルトでは、ログレベルに応じたハイライト（**FATAL**、**ERROR**、**WARN**、**SEVERE**、**CRITICAL**）が適用されています。
- 設定した内容はプロジェクト単位で保存されます。
 -  アイコンをクリックします。
 - ハイライト ウィンドウで、色を設定するキーワードを入力欄に追加してください。
 - 入力欄の左側の色をクリックすると、色を選択できます。

テーブル設定

カラム設定

3 領域の右で  **カラム設定** ボタンを選択します。カラムを追加したり、順序を設定できます。

- カラム追加

タグを選択してテーブルにカラムを追加できます。logカラム選択を解除する場合**ログ表示詳細設定**が確認できません。必ず1つ以上のカラムを選択します。

- カラム順序設定

カラムを追加すると**表示項目**に該当カラムが追加されます。希望のカラムをドラッグしてカラムの順序を変更します。

ログ表示詳細設定

3 領域右で  **ログ表示詳細設定** ボタンを選択します。デフォルトで**content**、**タグ**すべてチェックされており、両方の項目を表示します。**content**と**タグ**どちらかは必ず選択します。

チェックが解除されたアイテムはテーブルに表示されません。次のように**タグ**を解除する場合、テーブルでログの**タグ**は表示されません。

ログテーブルコンテンツタグ非表示

タグ管理一覧にタグを追加すると、追加した順にログのタグがソートされます。タグの順序はドラッグして変更できます。追加したタグを無効にすると、無効にしたタグはログのタグに表示されません。

ⓘ カラムおよびログ表示設定の適用範囲

- カラム設定とログ表示詳細設定は、ログTail、ログ検索、ログトレンドで使用できます。
- 同一プロジェクト内のログTail、ログ検索、ログトレンドは、カラム設定とログ表示詳細設定を共有します。

ログファイルのダウンロード

検索したログの結果を CSV または TXT ファイル形式でダウンロードできます。

1. 画面中央右側の  ダウンロード ボタンをクリックします。
2. CSVダウンロード または Logダウンロード をクリックして、希望の形式のファイルをダウンロードします。

ログの設定

ホーム画面 > プロジェクト選択 > ログ > ログ設定

ログ設定 の上部タブからログモニタリングを設定できます。 エージェント設定の確認、ログモニタリングの有効化設定、ログデータの保持期間および照会パスワードの設定、ログパーサーの登録、クイックインデックスの設定、個人情報のマスキング管理などを行うことができます。

！ 権限

- ・ **ログモニタリング機能の活性化** を使用するには、**プロジェクト修正** 権限が必要です。
- ・ **ログエディター** 権限があれば、**ログモニタリング機能の活性化** のほか、**ログ設定** メニューを編集できます。

ログモニタリングを開始する

ログモニタリングの開始 ログフィルター設定 ログプライマリパーサ設定 ログセカンダリパーサの設定 高速インデックス設定 ログ長期保存統計 個人情報の非属別化

エージェントの設定とログモニタリング活性化 料金プラン表示

ログTail、ログトレンド、ログ検索機能で、アプリケーションに点在するログをまとめて確認することができます。

▼ 1. エージェント設定の確認

Javaアプリケーションからログを収集するには、次の点を確認してください。
1. エージェントバージョンを確認して、必要だったらアップデートしてください。（v2.1.1以降のバージョンから可能）
2. エージェント設定 > オプション作成 > オプション選択 > 直接入力 > 下のエージェント設定コマンドを入力してください。
3. 再起動してください。

エージェント設定

logsink_enabled=true コピー

▶ 2. ログモニタリング機能の活性化

ログモニタリングデータの設定 初期化 保存

ログ照会パスワード ☐ ログ照会の際にパスワードを入力するようにするには、オンにしてください。

ログ保存期間(初期値) 最小1日から最大40日まで入力できます。

ログ使用量

カテゴリ	データ保存期間	累積ログ数(保存期間基準)	平均ログ数(日)	ログ数(前日)	予想ログ数(1週間)	予想ログ数(1月間)
Total		3,523,236,480	234,882,433	124,084,216	1,644,177,010	7,046,472,900
AppLog	15日	3,494,072,628	232,938,175	123,070,829	1,630,567,225	6,988,145,250
AppStdErr	15日	338,233	22,548	12,222	157,836	676,440
AppStdOut	15日	13,911,268	927,417	483,168	6,491,919	27,822,510
VirtualLog	15日	14,914,351	994,290	517,997	6,960,030	29,828,700

1. ログ > ログ設定 の ログモニタリングの開始 タブをクリックしてください。
2. ⓘ ガイド表示アイコンと 料金プラン表示ボタンを選択すると、案内画面に移動します。

エージェント設定とログモニタリングの有効化

- ① 領域でエージェント設定を確認し、ログモニタリングの有効化または無効化を設定できます。

エージェントの設定確認

ログモニタリングを開始するために、エージェントのバージョンと設定情報を確認してください。1. エージェント設定の確認 の案内に従って進めてください。

- アプリケーションモニタリング

アプリケーション別の適用方法については、[Java](#)、[PHP](#)、[Node.js](#)、[Python](#)、[Go](#) のドキュメントを参照してください。

- サーバーモニタリング

サーバーモニタリングの適用方法については、[Server](#) ドキュメントを参照してください。指示に従って [whatap.conf](#) にログモニタリング対象ファイルの設定を追加します。

- Kubernetesモニタリング

Kubernetesモニタリングの適用方法については、[Kubernetes](#) ドキュメントを参照してください。

ログモニタリングの有効化

ログモニタリングを有効化または無効化できます。2. ログモニタリング機能の活性化 でログモニタリングの有効／無効を設定してください。

-  ログモニタリングの有効化：トグルボタンをオンにするとログモニタリングが有効になり、有効化した日から15日間は無料でお試しいただけます。
-  ログモニタリングの無効化：トグルボタンをオフにするとログモニタリングが無効になり、以降ログは保存されません。

ログモニタリングのデータ設定

2 領域でログ使用量が確認できます。またログ保存期間とログ照会パスワード設定を変更できます。

ログ参照パスワード

セキュリティを強化するため、**ログ照会パスワード**を設定してください。ログ検索パスワードの指定はオプションです。ログ検索パスワードを使用中の場合は、ログ画面に入るときは必ずパスワードを入力します。

❗ パスワードを忘れた場合

ログ編集権限を持つユーザーは、**ログ設定** で新しいパスワードに変更できます。

ログ保存期間

共通に適用する基本(default) データ保持期間です。

- 最小1日から最大40日まで入力できます。未指定の場合、既定値は1日です。ログ保存期間の選択オプションの他に、ユーザーが希望する期間を入力できます。
- **ログ使用量**一覧で別に設定しない場合、このログデータの保存期間がデフォルトで適用されます。**ログ使用量** リストでカテゴリごとのデータ保持期間を設定し、**初期化** ボタンをクリックすると、デフォルトのデータ保持期間に初期化されます。

ログ使用量

ログ使用量一覧でカテゴリ別のログデータの保存期間を指定できます。ログ数は、当該期間中に蓄積されたログの件数を意味します。例えば、**日間ログ数**は、1日にたまったログ件数、**予想ログ数**は、データ保持日に今日のログ数を掛けたログ件数を意味します。

ログデータの保存期間を次のように指定できます。期間指定により、古いデータを削除してスペースを確保できます。

- **トライアルプロジェクト**
データ保存期間として1日、2日、3日を選択できます。
- **有料プロジェクト**

データの保存期間として1日、2日、3日、4日、5日、6日、7日、10日、30日、40日が選択できます。

- **保存量基準課金**

データの保存期間によってコストが異なります。

例、1日平均200万ログ件数が蓄積され、データ保存期間を3日に指定した場合、平均600万ログ件数が収集サーバーに保持され、課金の対象となります。

ログフィルター設定

ログフィルター設定は、ユーザーが指定したフィルター条件に一致するログのみを保存する機能です。必要なログだけを保存することでコストを削減できます。

ⓘ 権限

ログ編集権限を持つユーザーのみ設定できます。

ログフィルター設定の追加

新しいフィルター設定を追加する方法です。ログフィルターを設定する際は、フィルター名、ライブテール表示有無、カテゴリ、フィルター条件が必須入力項目です。

保存しないログであっても、ライブテール表示有無トグルを有効にするとライブテールで確認できます。

ⓘ カテゴリごとに設定できるフィルターは1つのみです。

1. ログ > ログ設定 > ログフィルター設定 タブに移動します。
2. + 追加 ボタンをクリックして新しいフィルター設定を作成します。
3. ログフィルター設定追加で フィルター名、ライブテール表示有無、カテゴリ、フィルター条件 を入力します。
 - フィルター名: フィルターを識別する名前
 - ライブテール表示有無: 保存の有無に関係なくライブテールに表示するかを選択
 - カテゴリ: フィルターを適用するログカテゴリ (複数選択可能)
 - フィルター条件: フィルターに保存するログの条件

ⓘ フィルター条件の詳細については [WhaTap log search query 構文](#) を参照してください。

- 例
 - 含む: `oid:123`
 - oid が 123 のログだけを収集します。
 - 含まない: `not oid:123`
 - oid が 123 ではない ログだけを収集します。
 - すべて含む: フィルター条件を未入力
 - すべて含まない: `not content:*`

4. 追加 ボタンをクリックすると、登録結果プレビューで各フィルター設定を確認・修正できます。

5. 確認が完了したら、適用 ボタンをクリックしてログフィルター設定を保存します。

シミュレーション

入力したカテゴリとフィルター条件でログを事前に検索し、ログフィルターを適用する前に結果を確認できます。

シミュレーション ボタンをクリックすると、フィルターが適用された **ログ検索** 画面が表示されます。

ログフィルター設定の修正

登録済みのログフィルターは編集アイコンをクリックして修正できます。

ログフィルター設定修正 画面では既存の値が表示され、必要な項目を変更して適用できます。

 ログフィルターを修正する際、選択できるカテゴリは1つのみです。

ログフィルター設定の削除

登録したフィルターは削除アイコンをクリックして削除できます。削除後は必ず **保存** ボタンをクリックしてください。

❗ 変更を保存しないとフィルターは削除されません。

ログフィルター設定のJSONインポート/エクスポート

ログフィルター設定はJSON形式でインポート/エクスポートできます。
他のプロジェクトに同じログフィルターを適用したい場合に便利です。

JSONエクスポート

1. 画面右上の ☒ JSON をクリックします。
2. JSONエクスポート ウィンドウが開いたら、エクスポート ボタンをクリックします。
3. ログフィルター設定がJSONファイルとしてダウンロードされます。

JSONインポート

1. 画面右上の ☐ をクリックします。
2. インポートするJSONファイルを選択します。
3. JSONインポート ウィンドウで リストに追加 または 上書き を選択してログフィルター設定をインポートします。
4. 保存 ボタンをクリックして変更を反映します。

バリデーション条件

設定を保存する際のバリデーションは次の通りです。

- type: GENERAL のみサポート
- category: 必須、string タイプのみサポート
- condition
 - language: jsonDsl , lucene のみサポート
 - description: 無効なフィルター条件は保存できません

- **showLiveTail:** `boolean` タイプのみサポート
- **name:** 必須、`string` タイプのみサポート

ログパースング

ログパーサを使用すると、不規則な形のログをクエリが可能な構造化された形に変更できます。WhaTapログモニタリングは、次の2つのタイプのパーサを提供します。

- **GROKパーサ**：任意の形で収集されるログを正規表現とGROKを活用してパースングします。
- **JSONパーサ**：JSON形式で収集されるログをパースングします。

ⓘ 共通の注意事項

- 同じカテゴリに複数のパーサが登録されている場合、最初にマッチングされるパーサのみが適用されます。
- WhaTapはWhaTapサービスの安定性に影響を与えるパーサを無効にする場合があります。。

GROKパーサ

ログが不規則な形で収集される場合、GROKパーサを使用してログをパースングできます。GROKパターンは、named regular expressionsを提供し、正規表現をより簡単かつ便利に使用できます。

GROKを開始する

GROKは2種類の文法を提供します。

1. `%{SYNTAX:SEMANTIC}`：GROKライブラリーが提供するパターンです。**named regular expressions**を活用してタグを抽出できます。活用例は[次のリンク](#)を参照してください。
 - **SYNTAX**：GROKが提供するnamed regular expressionsを指定します。
 - **SEMANTIC**：マッチングされる値に付ける名前を指定します。

ⓘ named regular expressions

GROKが提供するパターンです。複雑な正規表現に名前を付けて使用できるよう、GROKが提供す

❗ る機能です。

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>

WhaTapで提供するすべてのnamed regular expressionsを確認したい場合は、次の[リンク](#)を参考にしてください。

2. `(?<SEMANTIC>REGX)` : 正規表現の**named capturing group**文法です。正規表現を活用して、ユーザーの意図に合わせてタグを抽出できます。活用例は[次のリンク](#)を参照してください。

- **SEMANTIC** : マッチングされる値に付ける名前を指定します。
- **REGX** : マッチングに使用する正規表現を入力します。

❗ named capturing group

正規表現の文法です。

- capturing group: 複数のトークンを1つにまとめて1つのマッチング単位で使用する機能を意味します。
- named capturing group: capturing groupに名前を付けたものです。
- 文字列マッチングの例を見てみましょう。 dev@whatap.io
 - 例1 : `(\w+)@(\w+\.\w+)`
 - 例2 : Eメール全体のマッチング、およびusernameとdomainを追加でマッチングする場合 `(?<username>\w+)@(?<domain>\w+\.\w+)`

%{SYNTAX:SEMANTIC} 活用の例

次は %{SYNTAX:SEMANTIC} を活用する例です。

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
```

サンプルログを見て、各単語が意味する内容を推測できます。各部分をsemanticな単語に置き換えると、次のように表現できます。

semantic replace

```
[date][logLevel][caller] projectCode logCategory dexBuildStartTime {area=areaEnum, city=cityEnum} dexBuildElapsed
```

semanticな単語すべて、正規表現に書き換えることができます。GROKパーサを使用すると、事前に定義されたnamed regular expressionsを活用できます。ここで使われた `TIMESTAMP_ISO8601`、`LOGLEVEL`、`DATA` は、GROKが提供するnamed regular expressionsです。これらの値は、それぞれ次の正規表現に置き換えられてマッチングされます。

- name: `TIMESTAMP_ISO8601`
 - regular expression: `%{YEAR}-%{MONTHNUM}-%{MONTHDAY}[T|t]%{HOUR}:%{MINUTE}(:%{SECOND})?%{ISO8601_TIMEZONE}?`
- name: `LOGLEVEL`
 - regular expression: `LOGLEVEL`
`([Aa]lert|ALERT|[Tt]race|TRACE|[Dd]ebug|DEBUG|[Nn]otice|NOTICE|[Ii]nfo|INFO|[Ww]arn?(?:ing)?|WARN?(?:ING)?|[Ee]rr?(?:or)?|ERR?(?:OR)?|[Cc]rit?(?:ical)?|CRIT?(?:ICAL)?|[Ff]atal|FATAL|[Ss]evere|SEVERE|EMERG(?:ENCY)?|[Ee]merg(?:ency)?)`
- name: `DATA`
 - regular expression: `.*`

GROK parsing pattern

```
\[%{TIMESTAMP_ISO8601:date}\sGMT\]\[%{LOGLEVEL:level}\s\]\[%{DATA:caller}\]
```

上記の内容でパースングすると、次のようにタグを抽出できます。このようにGROKの `%{SYNTAX:SEMANTIC}` パター

ンは、複雑で長い正規表現を簡単に適用できる機能を提供します。

Tag extraction

```
- date : 2023-08-08 02:02:30,101
- caller : i.w.y.l.c.LogSinkDexScheduleThread.realProcess(159)
- level : LEVEL
```

(?<SEMANTIC>REGX) 活用の例

named regular expressionsでマッチングされない部分は (?<SEMANTIC>REGX) パターンを使ってパースできます。上記の[サンプルログ](#)から `%{SYNTAX:SEMANTIC}` パターンだけでパースされない領域は次の通りです。

Unparsed area

```
8 VirtualLog 20230808 02:01:00.000 {area=4, city=5} 56ms
```

該当ログの各部分をsemanticな単語に置き換えると、次のように表現できます。

semantic replace

```
projectCode logCategory dexBuildStartTime {area=areaEnum, city=cityEnum} dexBuildElapsed
```

このように不規則な形の文字列は、次のような (?<SEMANTIC>REGX) パターンを使ってパースできます。

サンプルログパースキーワード別にマッチングされる正規表現

パースキーワード	(?<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)

パースングキーワード	(?<SEMANTIC>REGX)
56 ms	(?<dexBuildElapsed>\d{2})ms

正規表現の基本文法



文法	意味	別名
<code>?</code>	0 or 1	-
<code>+</code>	1 or more	-
<code>*</code>	0 or more	-
<code>a{5}</code>	exactly 5	-
<code>\w</code>	word character	<code>[a-zA-Z_0-9]</code>
<code>\s</code>	white space	-
<code>.</code>	any character except newline	
<code>[abc]</code>	any of	-
<code>[^abc]</code>	not a,b, or c	-
<code>[a-z]</code>	character between a and z	-
<code>[1-3[7-9]]</code>	union (combining two or more character classes)	-
<code>[1-6&&[3-9]]</code>	intersection (共通集合)	-
<code>[0-9&&[^2468]]</code>	subtraction (差集合)	-
<code>a{2,}</code>	2 or more	-
<code>a{1,3}</code>	between 1 and 3	-



文法	意味	別名
<code>a+?</code>	match as few as possible	-
<code>{2,3}?</code>	match as few as possible	-
<code>(abc)</code>	capturing group (複数の文字列をsingle unitで処理する)	-
<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	-

このようにパースングされたキーワードをスペース(`\s`)と、特殊文字escape(`\{`、`\,`、`\}`)で接続すると、次のようにパターンを適用できます。

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
```

上記の内容でパースングすると、次のようにタグを抽出できます。

Tag extraction

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

GROKを適用する

ログ設定 > ログプライマリパーサ設定

1. GROKパターンパーサを適用するには、**ログ設定**メニューの**ログプライマリパーサ設定**タブに移動します。
2. **+ 追加する**を選択した後**パーサ入力欄**で**GROK**パーサを選択します。
3. **パターン登録**ボタンを選択すると、右側にパターン登録とシミュレーション画面が表示されます。
4. **パターン**と**ログ**入力後、**シミュレーション**ボタンをクリックして、適用するパターンでパーシングに成功することを確認します。

パターン 例:

```
[%{TIMESTAMP_ISO8601:date}\sGMT][%{LOGLEVEL:level}\s][%{DATA:caller}]\s(?:<projectCode>\d)\s(?:<logCategory>\d{2}:\d{2}:\d{2}\.\d{3})\s\s{area=(?:<areaEnum>\d),\scity=(?:<cityEnum>\d)}\s(?:<dexBuildElapsed>\d{2})ms
```

ログ例:

```
[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. シミュレーションの成功時**シミュレーション結果**と**性能測定の結果**を照会できます。
6. シミュレーション後、**パターン適用**ボタンをクリックすると、選択したパーサーに入力したパターンが適用されます。
7. パターン適用後、**カテゴリ**と**ログ検出条件**、**パターン**を入力します。

×

パーサ 追加

パーサ*

WhaTap Monitoringには、サービスの信頼性に影響を与える可能性があるパーサーを無効にできる権限があります。

GROK

パーサーパターン*

入力したパターンでログが正常に解析されるかどうかをシミュレートし、パターンを登録します。

成功しました。

```

\[%{TIMESTAMP_ISO8601:date}\sGMT\}\[%{LOGLEVEL:level}\s\}\[%{DATA:caller}\}\s(?:<projectCode>\d)\s(?:
<logCategory>w*)\s(?:<dexBuildStartTime>\d{8}\s\d{2}:\d{2}:\d{2})\s\{area=(?:<areaEnum>\d),\scity=(?
<cityEnum>\d)\}\s(?:<dexBuildElapsed>\d{2})ms

```

パーサーパターンの修正

カテゴリ*

同じカテゴリに複数のパーサーが登録されている場合、最初に一致するパーサーのみが適用されます。

AppLog

ログ検出条件

フィルタを入力しなかった場合、または検索キー／値を1つだけ入力した場合、そのパターンはすべてのログに適用される。

oname

demo-8100

追加

• カテゴリ

ログカテゴリを選択します。 **カテゴリ**は必須入力項目です。

• ログ検出条件

- 条件を満たすログのみパーサが適用されます。
- 検索キーと検索値を選択するか、直接入力します。
- ログ検出条件は、すべてのパーサが実行される前に適用されます。つまり、パーサの結果として追加されるタグを使用できません。

8. 追加ボタンを選択してパーサを登録します。

- !

 ログパーサー一覧から該当パーサの優先順位を変更するか、**活性化**および**修正**、**削除**できます。
- パーサーシミュレーション後、パターンを登録できます。

304

❗ GROKパーサの注意事項

- GROKパーサは `%{SYNTAX:SEMANTIC}` 、 `%{SYNTAX:SEMANTIC}` 二つのパターンをサポートします。
- `%{SYNTAX:SEMANTIC}` パターンを使用する時、 `SEMANTIC` を必ず入力します。
- `%{SYNTAX:SEMANTIC}` パターンを使用する時、 `SEMANTIC` は一つのパーサの中でユニークである必要があります。
- `(?<SEMANTIC>REGX)` パターンを使用する時、 `SEMANTIC` は文字(a-z、A-Z)、数字(0-9)、および指定された特殊文字(`.` 、 `_` 、 `-`)のみが使えます。
- `SEMANTIC` は文字(a-z、A-Z)で始めなければなりません。
- `SEMANTIC` は文字(a-z、A-Z)または数字(0-9)で終わる必要があります。

GROK追加パターンの選択

GROKパーサのシミュレーション時に、基本パターン(`WORD` 、 `NUMBER` 、 `IP` など)以外に特定のログ形式に合った追加パターンを選択できます。Java、Nginx、MySQLなど32個のパターンタイプが11個のカテゴリにグループ化されて提供されます。

追加パターンカテゴリのドロップダウン

1. パーサのシミュレーション画面で**追加パターン (選択)**領域のドロップダウンをクリックしてください。
2. カテゴリ別にグループ化されたパターンタイプ一覧から、必要なパターンタイプを選択してください。検索入力欄にパターンタイプ名または説明を入力して検索することもできます。
3. 選択したパターンタイプは、シミュレーション時に基本パターンとともにロードされます。

❗ 基本パターン(Core)は常に自動的に含まれます。追加パターンの選択は任意です。

カテゴリ別パターンタイプ一覧

カテゴリ	パターンタイプ
Web Servers	haproxy, httpd, iis, nginx, squid

カテゴリ	パターンタイプ
Application Servers & Frameworks	java, log4j, rails, ruby, springboot
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

活用例

Tomcat Catalina 8のログをパースングするには、**java**パターンタイプを追加で選択した後、`%{CATALINA8_LOG}` パターンを使用してください。

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
```

パターン詳細表示

選択した追加パターンタイプにどのパターンが含まれているかを詳細画面で確認できます。パターン定義(正規表現)とサンプルログを照会し、シミュレーションにすぐに適用できます。

パターン詳細表示

追加パターンタイプを選択した後、選択されたパターンタイプのタグをクリックすると、右側に詳細画面が開きます。詳細画面はシミュレーションフォームを隠さずに並んで表示されるため、パターン定義を確認しながらシミュレーションを進めることができます。

各パターン項目で次の機能を使用できます。

ボタン	機能	説明
サンプル	サンプルログ入力	該当パターンにマッチングする例ログをシミュレーションパーシングログ入力欄に自動的に入力します。
選択	パターン挿入	<code>%{パターン名}</code> 形式でパターン入力欄に挿入します。該当パターンタイプも自動的に選択されます。
コピー	クリップボードコピー	<code>%{パターン名}</code> 形式をクリップボードにコピーします。

- ① パターン項目をクリックすると、パターン定義(正規表現)が展開されます。複数のパターンを同時に展開して定義を比較できます。
- パターン定義に含まれる `%{PATTERN:field}` 参照は、パターン名、フィールド名、リテラル文字がそれぞれ異なる色で区別されて表示されます。
- サンプルボタンで入力されたログでそのままシミュレーションを実行してパーシング結果を確認できます。

シミュレーションサンプルログの保存

シミュレーションに使用したログは、パーサ設定とともに自動的に保存されます。パーサを修正する際に、以前に使用したサンプルログがシミュレーション画面に自動的に復元され、毎回ログを再入力する必要がありません。

JSONパーサ

ログがJSONフォーマットで収集される場合、JSONパーサを使用して簡単かつ便利にパーシングできます。

JSONを適用する

ログ設定 > ログプライマリパーサ設定

1. JSONパターンパーサを適用するには**ログ設定**メニューの**ログプライマリパーサ設定**タブに移動します。
2. **+ 追加する**を選択した後パーサ入力欄で**JSON**パーサを選択します。
3. **パターン登録**ボタンを選択すると、右側にパターン登録とシミュレーション画面が表示されます。
4. **パターン**と**ログ**入力後、**シミュレーション**ボタンをクリックして、適用するパターンでパーシングに成功することを確認します。

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"} --
```

例のログで**Prefix**と**Postfix**を `--` に指定し、**Ignore**に `url` を指定時 `host`、`method`、`status` 3つ**タグ**のみ生成します。

- **Prefix** ログでJSONフォーマットが開始する場所を指定します。ログ全体がJSONフォーマットの場合は、空の値に設定します。
 - **Postfix** ログでJSONフォーマットが終わる位置を指定します。ログ全体がJSONフォーマットの場合は、空の値に設定します。
 - **Ignore** JSONフォーマットの中でタグを生成しないキーを指定します。
5. シミュレーションの成功時**シミュレーション結果**と**性能測定の結果**を照会できます。

×

パーサ シミュレーション

ガイド表示

パターン

agenttime, category, content, logContent, message, pcode, time, timestamp は予約語です。
予約語はログ検出条件、パターンで登録しても動作しません。

Prefix

-

Postfix

-

Ignore

url

ログ

ログシミュレーションは必須ですする必要があり、
シミュレーションの結果に応じてパターン登録が必要になる場合があります。

2023-08-08 02:43:28.615 -
{"host":"10.21.3.24","method":"POST","status":"200","url":"http://devote.whatap.io/yard/api/flush"} -
-

シミュレーション

シミュレーション結果 成功しました。

キー	値	結果
method	POST	Ok
host	10.21.3.24	Ok
status	200	Ok

性能測定の結果 成功しました。

シミュレーション数	最小時間(ns)	最大時間(ns)	平均時
1	4,491	4,491	4,491
10	3,322	3,930	3,525
100	2,662	177,949	8,084
1,000	2,654	476,818	4,305
10,000	2,648	311,233	3,823
100,000	2,650	60,522,941	3,713
1,000,000	2,647	44,113,067	3,014

パターン適用

6. シミュレーション後、パターン適用ボタンをクリックすると、選択したパーサーに入力したパターンが適用されます。

7. パターン適用後、カテゴリとログ検出条件、パターンを入力します。

309

×

パーサ 追加

パーサ*

WhaTap Monitoringには、サービスの信頼性に影響を与える可能性があるパーサーを無効にできる権限があります。

JSON

パーサーパターン*

ログが正常に解析されるかどうかをシミュレートします。シミュレーションは必須でなければならず、シミュレーション結果によってはパターン登録がさらに必要になる場合があります。

✔ 成功しました。

Prefix --

Postfix --

Ignore url

シミュレーション検証とパターン修正

カテゴリ*

同じカテゴリに複数のパーサーが登録されている場合、最初に一致するパーサーのみが適用されます。

AppLog

ログ検出条件

フィルタを入力しなかった場合、または検索キー／値を1つだけ入力した場合、そのパターンはすべてのログに適用される。

oname

demo-8100

追加

• カテゴリ

ログカテゴリを選択します。 **カテゴリ**は必須入力項目です。

• ログ検出条件

- 条件を満たすログのみパーサが適用されます。
- 検索キー**と**検索値**を選択するか、直接入力します。
- ログ検出条件**は、すべてのパーサが実行される前に適用されます。つまり、パーサの結果として追加される**タグ**を使用できません。

8. 追加ボタンを選択してパーサを登録します。

- ⓘ ログパーサー一覧から該当パーサの**優先順位**を変更するか、**活性化**および**修正**、**削除**できます。
- パーサを登録する前に**シミュレーション**を通じて登録するパターンが正常であるか確認できます。GROK

310



パーサ登録シミュレーションプロセスと同じです。 [次の文書](#)を参考にしてください。

JSONフォーマット活用例

Sample log

```
{"host":"10.21.3.24","method":"POST","status":"200","url":"http://dev.whatap.io/yard/api/flush"}
```

上記のようなサンプルログが収集された場合パーサ 追加画面でJSONパーサを選択します。複雑なパーシングロジックを作成する必要なく、ログ分析に必要なタグを次のように抽出できます。

Tag extraction

```
- host : 10.21.3.24
- method : POST
- status : 200
- url : http://dev.whatap.io/yard/api/flush
```

JSONフォーマットを一部構成する時の活用例

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"}
--
```

もし、例のようにログの一部のみがJSONフォーマットで構成されている場合はPrefixとPostfixを指定してください。WhaTapログモニタリングはPrefixとPostfix間の領域をJSONフォーマットで認識してからパーシングします。

Tag extraction

```
- host : 10.21.3.24
- method : POST
- status : 200
- url : http://dev.whatap.io/yard/api/flush
```

ログ高速インデックス設定

高速インデックス設定

ログ設定メニューの上段から高速インデックス設定タブを選択します。大量のログを収集すると、ログ検索性能が低下する場合があります。よく使う検索条件は、インデックス(index)で生成すると、ログ検索がより速くなります。設定項目は次のとおりです。

設定値	必須の有無	説明
カテゴリ	必須	高速インデックスを設定するカテゴリ
検索キー	必須	高速インデックスを設定する検索キー
大文字と小文字を区別しない	オプション	大文字と小文字の区別するかどうか
ルール	必須	* を少なくとも1つ以上を含める必要あり
活性化有無	必須	活性化または非活性化の設定(既定値 <code>true</code>)

ログ長期保管統計設定

ログ長期保存統計の設定

ログ設定メニューの上段からログ長期保存統計タブを選択します。ログデータは、非常に大容量のため、長期間保存することは難しいです。したがって、ログ統計データの設定機能を使用して特定の条件を満たすログデータが5分ごとに何件収集されたかに関する情報を保存できます。長期間にあたって、実際のログデータが削除されても、条件を満たすログがどれだけ収集されているかの推移は確認できます。

ログ長期保存統計の追加

×

ログ長期保存統計 追加

統計キー*

統計キーを入力してください。

データ保存期間
(ディスク使用量)

15日 (約 3 MB) ▾

カテゴリ*

カテゴリを選択してください。

ログ検出条件*

まず、カテゴリを選択してください。 ▾

まず、カテゴリを選択してください。

除外 ☐

大小文字を区別する ☒

+ 追加する

追加

ログ長期保存統計タブで + 追加する ボタンを選択するとログ長期保存統計 追加画面が表示されます。 + 追加する ボタンでルールを追加したり、作成したルールを**-**アイコンで削除できます。

設定項目

フィールド	説明
カテゴリ	ルールが適用されるカテゴリです。
統計キー(key)	ルールを満たすログが発生した場合、保存するキーとして同じキーを重複で設定できません。
ログ検出条件	ログ統計データを生成する条件です。この条件を満たすログがどのくらい収集されたかで統計データを生成します。
除外	除外をチェックすると、入力した条件を満たさない値で統計データを作成します。
大小文字を区別する	入力したログ検出条件の値に対して大文字と小文字の区別有無を指定します。
活性化有無	活性化または非活性化の設定(既定値 true)

例

次のように設定を追加した場合、収集されたログのうち、statusが 200 , 300 のログを対象にTotalCountのキーで統計データを作成します。

ログ長期保存統計 指定した条件を満たすログがどれ程収集されたかの統計データが生成できます。 					+ 追加する	保存
カテゴリ	統計キー	ログ検出条件	データ保存期間 (ディスク使用量)	活性化		
AppLog	TotalCount	status 200, 300	15日 (約 3 MB)	☒		

データ参照

1. 統合Flexボードのウィジェットテンプレートでログ長期保存統計を検索し、ウィジェットを作成します。

ウィジェットテンプレート

2. データを照会するカテゴリと統計キーを指定して適用ボタンを選択します。

ログ長期保存統計

カテゴリ変更

AppLog

統計キー

TotalCount

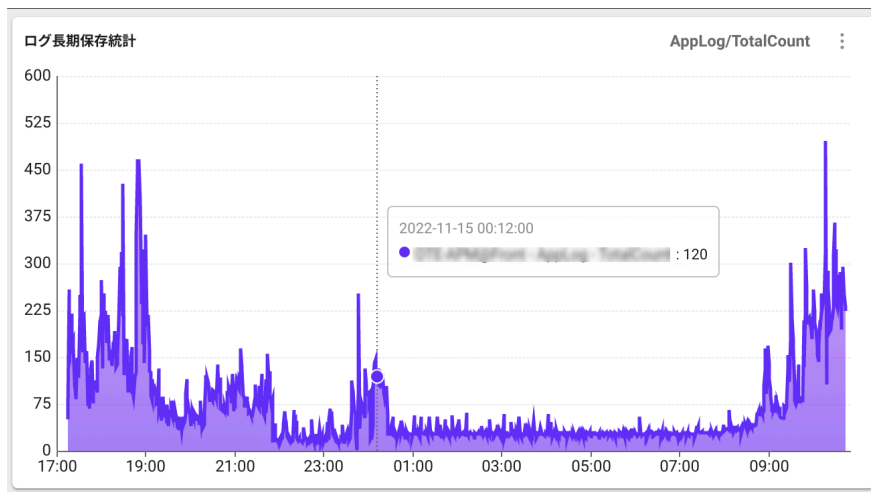
キャンセル

適用

カテゴリ、キーを選択してください。

該当ウィジェットに表示するデータ収集のためにはログ長期保存統計 設定が必要です。
 当該設定をしていない場合は、
[ガイド](#)を参考してログ長期保存統計 設定をしてください。
[ログ設定](#)

3. 追加した設定でログ長期保存統計データを次のように確認できます。



ログ個人情報非識別化設定

個人情報の非識別化

個人情報の非識別化ではログデータ内の個人情報をマスキング処理したり、安全な値に置換できます。

- 暗号化の保存：指定された機密な情報は暗号化され、データベースに保存されます。
- マスキング処理：ログ画面に表示される時、機密な情報は基本的にマスキング(*******)処理されて表示されます。
- 置換処理：機密な情報をユーザーが指定した安全な値に変更します。

個人情報の分類

一般的に個人情報として分類する項目は次のとおりです。一般の個人情報以外にも機密な情報として処理すべき項目があれば**個人情報の非識別化機能**を通じて、ログ内で必要な項目をマスキング処理または置換処理してください。

- 個人識別番号
- パスポート番号
- 運転免許証番号
- 外国人登録番号
- クレジットカード番号
- 銀行口座番号
- 生体情報

要求権限

非識別化された個人情報はマスキング処理されて表示されます。 **ログの個人情報照会権限**が付与されたユーザーのみ **個人情報の表示** トグルを通じて元のデータを確認できます。非識別化の対象検索キーの追加及び修正は、**ログ編集権限**が必要です。

❗ ログの個人情報照会権限及びログ編集権限の詳細は[次の文書](#)を確認してください。

個人情報の非識別化設定

新規のログデータにマスキング処理を適用して機密な情報を保護できます。

ログ設定

ログモニタリングの開始 ログプライマリパーサ設定 ログセカンダリーパーサの設定

個人情報の非識別化 個人情報が含まれた検索キーを追加すると、当該データを暗号化して保存し、マスキングします。

活性化 ☒ カテゴリ AppLog @txid agenttime @mt

ログ個人情報の非識別化チェック 以前に積み重ねられたログを非識別化します。

時間 < 2025/01/21 16:48 ~ 2025/01/21 17:48 1時 >

カテゴリ カテゴリを選択してください。

個人情報項目

個人情報パターン

置換を適用するかどうか ☒

置換値 ①

点検開始 チェックを中止

× 個人情報の非識別化 追加

カテゴリ *

カテゴリを選択してください。

検索キー *

暗号化保存およびマスキング処理する検索キーを選択します。

暗号化する検索キーを入力してください。

追加

1. 個人情報の非識別化タブで追加するボタンを選択します。
2. 右側の個人情報の非識別化 追加画面でカテゴリを選択し、マスキング処理する検索キーを入力します。
3. 追加ボタンをクリックして設定を追加します。
4. 個人情報の非識別化一覧で非識別化項目を確認した後、右上の保存ボタンを押して現在の設定を保存してください。

個人情報の非識別化 個人情報が含まれた検索キーを追加すると、当該データを暗号化して保存し、マスキングします。				+ 追加する	保存
活性化	カテゴリ	検索キー	修正		
☐	VirtualLog	agen	削除 編集		
☒	VirtualLog	status	削除 編集		
☒	AppLog	agenttime	削除 編集		

- 非識別化処理された検索キーの場合、ログコンテンツ内の **検索キー.pii** 形式で出力されます。

- 個人情報の非識別化一覧内の活性化カラムで非識別化項目を  活性化にできます。
- 個人情報の非識別化一覧内の編集カラムで  修正及び  除去できます。

- ✔ ログプライマリパーサ設定タブで検索キー名を **検索キー.p** に指定すると、非識別化対象として自動登録されます。自動登録された項目は**個人情報の非識別化**タブで**カテゴリ**選択後、**指定された検索キー**で確認または解除できます。

パーサーで .p 接尾辞を指定する方式よりも、**個人情報の非識別化**タブで直接設定することを推奨します。

個人情報の表示

非識別化されたデータは**ログTail**、**ログトレンド**、**ログ検索メニュー**でマスキング状態で表示されます。**ログの個人情報照会権限**のあるユーザーはログ一覧内の**個人情報の表示**  ボタンをクリックすると元のデータを確認できます。

▼	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.												

- ❗ **個人情報の非識別化**タブで指定した検索キーは、ログメニュー内のログコンテンツから **検索キー.pii** 形式で表示されます。

例: **status.pii** 例 *******

ログの個人情報の非識別化点検

- ❗ **ログ個人情報の非識別チェック**機能を通じて既存のデータを置き換える場合、そのデータは元に戻すことが

❗ できません。

ログ個人情報の非識別チェックは既存のログデータ内の個人情報を識別し、ユーザーが指定した置換値に置き換えます。

対象キー指定による置換

対象キーを指定すると、該当キーに保存された値のみを置換し、残りのログ内容はそのまま維持します。対象キーはログの field 値と tag 値の両方に適用されます。対象キーを指定しない場合、従来と同様にログコンテンツ全体から個人情報を識別して置換します。

❗ 置換は保存されたログデータにのみ適用されます。検索インデックスには、置換後も元の値が残っている場合があります。

対象キーは、ログ個人情報の非識別化点検フォームの対象キー入力欄で指定し、画面では field と tag を区別せず、1つの対象キーとして入力します。

ログ個人情報の非識別チェック

収集されてあるログを非識別化します。

[✓ チェック履歴の確認](#)

時間 < 2025/03/21 12:26 ~ 2025/03/21 13:26 1時 > カテゴリ VirtualLog 個人情報項目 個人識別番号 個人情報パターン (?<!\w)\d{2}(0[1-9] 1[0-2])([0-2][0-9] 3[0-1]){1-4}\d{6}(?!\\w) 置換の適用有無 ☐ 置換値 *****_***** ○ チェック開始 ⊗ チェック中止	カテゴリ VirtualLog 検索開始時刻 2025/03/21 12:26 検索終了時刻 2025/03/21 13:26 個人情報項目 個人識別番号 個人情報パターン (?<!\w)\d{2}(0[1-9] 1[0-2])([0-2][0-9] 3[0-1]){1-4}\d{6}(?!\\w) 置換値 *****_***** パターンのマッチング結果 0 ✓ 結果の確認 チェック作業の開始時刻 2025/03/21 13:28 チェック作業の終了時刻 2025/03/21 13:28 置換の適用有無 No チェック作業の結果 SUCCESS
---	---

1. 開始時間と終了時間を設定してください。
2. カテゴリを設定します。
3. 個人情報項目を例の中から選択または直接入力を選択します。

❗ **直接入力**選択時に個人情報を識別するための正規表現パターンを直接入力します。

4. 置換の適用有無トグルで個人情報が識別された場合、該当情報の置換有無を選択します。
5. 既存のログで正規表現パターンに識別された文字列を変更する置換値を入力します。

- ❗
- 置換値は元の値より長くしてはなりません。
 - 置換の適用有無トグルの活性化時に、必ず置換値を入力する必要があります。

6. 条件を入力した後、**チェック開始**ボタンを選択します。

❗ 点検中の場合はいつでも**チェック中止**ボタンで点検過程を中止できます。

7. 置き換えを適用する時個人情報の非識別チェックの開始確認画面で置き換え入力後確認ボタンをクリックします。

個人情報の非識別チェックの開始
×

選択した個人情報パターンに一致する値を置き換えます。

❗ 置き換え後はデータの復元ができません。

置き換えが必要な場合は "**置き換え**" を直接入力してください。

キャンセル

確認

8. 点検作業の完了後、例の画像のように右側から**チェック作業の結果**を確認できます。
 - **カテゴリ**：点検されたカテゴリ情報を表示します。
 - **検索開始時刻及び検索終了時刻**：点検が実行された時間範囲を表示します。
 - **個人情報項目**：点検された個人情報の項目を表示します。

- **個人情報パターン**：使用された正規表現式のパターンを表示します。
- **置換値**：適用された置換値を表示します。
- **パターンのマッチング結果**：識別された個人情報の数を表示します。**結果の確認**をクリックするとサンプルログを確認できます。
- **チェック作業の結果**：個人情報が識別された結果を表示します。

SUCCESS (点検成功)、FAILED (点検失敗)、STOP (点検中止)、TIMED_OUT (時間超過による点検終了)

チェック履歴の確認

ログ個人情報の非識別化点検を行った後、過去に行われた点検結果を照会するには、上段右側で**チェック履歴の確認**ボタンをクリックします。置き換え履歴、点検時点、適用された個人情報項目などを追跡できます。また**チェック履歴の確認**画面の上段右側の  **CSV** ボタンをクリックすると_CSV_ファイル形式でそのリスト情報をダウンロードできます。

チェック履歴の確認  					
< 2025/03/25 08:17 ~ 2025/03/25 09:17 1時  >		個人情報項目 			 CSV
	パターンのマッチング...	チェック作業の開始時刻	チェック作業の終了時刻	置換の適用有無	チェック作業の結果
***	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

個人情報のパターン

既存のログデータから個人情報を識別する際に使用される正規表現式のパターンの例は以下の通りです。

個人情報のパターン	個人情報の例	正規表現式パターン	置換される値
個人識別番号	123456-1234567	(?<!w)d{2}(0[1-9] 1[0-2])([0-2][0-9] 3[0-1])-[1-4]d{6}(?!w)	*****_ *****
パスポート番号	M1234567	([MSRODTC][0-9]{7}\b)	*****
運転免許証番号	01-23-456789-00	(?<!w)d{2}-d{2}-d{6}-d{2}(?!w)	**_**_ *****_**
外国人登録	987654-1234567	(?<!w)d{6}-?[5-8]d{6}(?!w)	*****_ *****

個人情報のパターン	個人情報の例	正規表現パターン	置換される値
番号			
クレジットカード番号	1234-5678-9012-3456	(?<!w)d{4}-d{4}-d{4}-d{4}(?!w)	****_****_ ****_****
携帯電話番号	010-1234-5678	(?<!w)(+82-?1[016789]-?d{3,4}-?d{4} 01[016789]-?d{3,4}-?d{4})(?!w)	***_****_ ****
メールアドレス	example@domain.com	([a-zA-Z0-9][a-zA-Z0-9._%+~]*@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,})	***@***.***

個人情報のパターン	個人情報の例	正規表現式パターン	置換される値
銀行口座番号	123456-01-654321	(?<!w)d{6}-d{2}-d{6}(?!w)	*****_**_ *****
事業者登録番号	111-11-01111	(?<!w)d{3}-d{2}-d{5}(?!w)	***_**_ *****
法人登録番号	111111-1111111	(?<!w)d{6}-?d{7}(?!w)	*****_ *****

ログ設定のインポート/エクスポート

ログ設定のインポート・エクスポート

パーサ設定、高速インデックス設定、フィルター設定の内容をJSONファイル形式で保存し、他のプロジェクトからJSONファイルをインポートして適用できます。プロジェクトごとに何度も繰り返し設定を作成する手間を減らします。

1. 1つのプロジェクトにパーサ設定、高速インデックス設定、フィルター設定を追加します。
2. 各設定タブで画面右上に**JSON**  ボタンを選択します。
3. **JSONエクスポート**画面が表示されると、画面右上にある**抽出**ボタンを選択します。
4. JSON設定ファイルがユーザーPCに保存されます。
5. 他のプロジェクトに移動してから、**ログ** > **ログ設定**メニューに移動してください。
6. まず、JSON設定ファイルをエクスポートした設定タブを選択し、 ボタンを選択します。
7. ファイル選択画面が表示されたら、ユーザーのPCに保存したJSON設定ファイルを選択します。
8. **JSONインポート**画面が表示されたら、設定内容を確認し、**リストに追加する**または**上書き**ボタンを選択します。
9. 画面右上の**保存**ボタンを選択します。

 JSON設定ファイルをインポートして、**保存**ボタンを選択しないと、インポートされた設定は保存されません。

警告アラート

監視対象のシステムまたはアプリケーションで問題が発生した際に、あらかじめ設定した条件に基づいてユーザーへ通知を送信する機能です。通知は、メール、SMS、メッセージャー、アプリのプッシュ通知など、さまざまなチャネルを通じて配信されます。

たとえば、CPU 使用率、メモリ使用量、ディスク I/O、ネットワークトラフィック、トランザクション数、エラー発生、レスポンスタイムの遅延などの主要なパフォーマンス指標にアラート基準を設定しておく、その基準を超過した場合や異常な兆候が検出された際に通知が送信されます。

WhaTap の AI ベースのアラート機能を使用すると、複雑な条件を手動で設定する必要はありません。AI がアプリケーションの正常な動作パターンを学習し、異常パターンを自動的に検知して通知します。また、タグカウントアラート機能を活用することで、特定のタグを基準に集計された値に条件を設定でき、複雑な状況でも高精度な検知が可能です。

主な機能

- ・ **イベント設定:** 閾値ベースのアラート条件および通知チャネルの設定
- ・ **通知設定:** ユーザーごとの通知チャネルおよび時間帯設定
- ・ **イベント履歴:** アラート発生履歴の確認

権限

イベントを追加または設定するには、**アラート設定権限** が必要です。

- ・ **閲覧:** メトリクスイベント設定を確認するには、**閲覧・分析権限** が必要です。
- ・ **追加／編集／削除:** 設定を変更するには、**アラート設定権限** が必要です。
- ・ **通知受信:** 通知を受信するには、**通知受信権限** が必要です。

📌 参考資料

詳細については、[メンバー権限](#) を参照してください。

イベント設定

ホーム画面 > プロジェクト選択 >  アラート通知 > イベント設定

イベント設定では、監視対象のシステムやアプリケーションで発生する可能性のある異常兆候を基準に、イベントを設定・管理できます。設定した条件が満たされると、メール、SMS、メッセージャー、アプリのプッシュ通知など、希望するチャンネルで通知を受信できます。監視の目的に応じて、イベントを柔軟に構成できます。

メトリクス

メトリクスイベントは、リアルタイムデータを基にシステムおよびアプリケーションのパフォーマンス指標を監視できます。

リアルタイムログ

リアルタイムで収集されたログから設定したイベント条件が検出された場合、警告アラートを送信します。

複合ログ

ログの内容を基準に警告通知を発生させる複合ログイベントを設定します。

ホーム画面 > プロジェクト選択 >  アラート通知 > イベント設定

イベント設定では、監視対象のシステムやアプリケーションで発生する可能性のある異常兆候を基準に、イベントを設定・管理する機能を提供します。設定した条件を満たすと、メール、SMS、メッセージャー、アプリプッシュなど、希望するチャンネルで通知を受信できます。監視目的に応じてイベント構成を設計できます。

メトリクス

メトリクスイベントは、リアルタイムデータを基にシステムおよびアプリケーションのパフォーマンス指標を監視できます。

リアルタイムログ

リアルタイムで収集されたログから設定したイベント条件が検出された場合、警告アラートを送信します。

複合ログ

ログの内容を基準に警告通知を発生させる複合ログイベントを設定します。

参考

- イベント設定時は、不要なイベント発生を防ぐために適切なしきい値を設定してください。
- 通知設定では、問題解消時に通知される回復通知もあわせて検討すると、運用対応に役立ちます。

共通機能

すべてのイベント設定は **JSON または Excel 形式** でダウンロードできます。同じ種類のプロダクト設定を共有することで、繰り返し発生するイベント設定作業を削減できます。

- **JSON 一括編集:** すべてのイベント条件を JSON 形式で一括編集できます。
- **JSON 一括ダウンロード:** 現在登録されているイベント条件を JSON ファイルとして保存できます。
- **Excel 一括ダウンロード:** イベント一覧を Excel ファイルとしてダウンロードし、外部レポートやバックアップに活用できます。

JSON 一括編集

1. 画面上部の [JSON 一括編集] ボタンをクリックします。
2. JSON 一括ダウンロード 機能でダウンロードした JSON ファイルを読み込むか、直接編集します。
3. [上書き] ボタンをクリックして保存します。
4. 確認メッセージが表示されたら、[上書き] ボタンをクリックします。

❗ 上書き後は、以前のイベント設定に戻すことはできません。

- `productType` または `platform` プロパティの値を任意に変更すると、他のプロジェクトでイベントが正常に動作しなくなる可能性があります。
- JSON 編集画面には検証機能が組み込まれています。形式や値が正しくない場合、編集画面下部にエラーメッセージが表示され、[上書き] ボタンは無効になります。



JSON データ構造



```
{
  "productType": "{productType}",
  "platform": "{platform}",
  "events": {
    "HITMAP": {
      ...
    },
    "LOG_REALTIME": [
      {...}
    ],
  },
}
```



```

"METRICS": [
  {...}
],
"COMPOSITE_LOG": [
  {...}
],
"BASIC": [
  {...}
],
"COMPOSITE_METRICS": [
  {...}
],
"ANOMALY": [
  {...}
]
}
}

```

JSON フィールド	説明
productType	プロダクトタイプ（例: APM、Infra など）
platform	プラットフォーム情報（例: java、node など）
events	イベントデータ
└ HITMAP	ヒットマップパターン
└ LOG_REALTIME	リアルタイムログイベント
└ METRICS	メトリクス
└ COMPOSITE_LOG	複合ログイベント
└ BASIC	基本イベント
└ COMPOSITE_METRICS	複合メトリクス

!	JSON フィールド	説明
	L ANOMALY	異常値

JSON 一括ダウンロード

画面上部の [JSON 一括ダウンロード] ボタンをクリックします。

- JSON ファイル名は `integrated-event-YYYYMMDD.json` 形式です。
- JSON データの構造や `events` 属性配下のサブ属性は、プロダクト（ `platform` ）またはプロダクトタイプ（ `productType` ）によって異なる場合があります。

⚠ JSON データ内の `productType` または `platform` プロパティの値を任意に変更すると、他のプロジェクトでイベントが正常に動作しなくなる可能性があります。

Excel 一括ダウンロード

画面上部の [Excel 一括ダウンロード] ボタンをクリックします。

メトリクス

ホーム > プロジェクト選択 >  アラート通知 > イベント設定 > メトリクス タブ

プロジェクトに設定されているすべてのメトリクスベースのイベント一覧を確認できます。設定済みのメトリクスイベントを確認、修正、削除したり、新しいイベントを追加したりできます。

基本オプション

- **イベントレベル:** イベントの深刻度を示し、正常（Info）、警告（Warning）、危険（Critical）の3段階に分類されます。
- **エージェント重複アラート抑止:** 同じ名前のエージェントが同時に2つ以上動作している場合、選択した時間（30秒、1分、3分、5分、10分）の間はイベントが発生しません。
- **検索:** イベント名を基準に検索します。
- **JSON ダウンロード／アップロード:** JSON エディタでイベントルールを直接編集するか、ファイルとしてダウンロードして編集後に再アップロードできます。
- **+ イベント追加:** 新しいメトリクスイベントを追加します。
- **カラムサイズ調整:** 各カラムの境界をドラッグして幅を調整できます。

表 | メトリクスイベント一覧構成

項目	説明
No.	イベントの番号
	イベントの有効化状態 – 有効: 条件を満たすとイベントが発生 – 無効: イベントは動作せず、条件も評価されません
	イベント設定の編集および削除
イベント名	ユーザーが指定したイベント名 – 最大255文字

項目	説明
ルール	イベント発生条件
対象	イベントが適用される監視対象
発生回数	イベント発生の基準となる期間と回数 – 選択した時間内に設定回数分条件を満たすとイベントが発生
一時停止	アラート発生後、同一イベントの発生を一定時間停止 – 選択可能時間: 使用しない、5分、10分、15分、20分、30分、1時間、2時間、3時間、6時間、12時間、1日 – 回復通知が有効な場合、RECOVERED（正常）通知後、選択した時間は同一イベントが発生しても通知されません
回復通知	Critical および Warning レベルのイベントが解消された際に、RECOVERED（正常）通知を受信するかどうか – 有効: 進行中から正常状態に遷移すると RECOVERED 通知を送信し、イベント履歴で進行中／解消状態を区別して確認可能 – 無効: しきい値を超えるたびに単発イベントが発生
イベント受信	該当イベント通知を受信するユーザーまたはグループ（受信タグ）

イベント設定

メトリクスイベントは、監視対象で発生する事象を条件に基づいて定義し、効率的に通知を受信できるよう設定するための機能です。

イベント追加

メトリクスイベントを追加するには、**イベント設定** > **メトリクス** タブに移動し、右上の [+ イベント追加] ボタンをクリックします。

メトリクスイベント追加手順
Step 1. テンプレート選択: イベントの基本構成を選択します。
Step 2. イベント条件定義: どの条件でイベントを発生させるかを設定します。
Step 3. イベント対象選択: イベントが適用される監視対象を選択します。
Step 4. 基本情報および通知設定: イベント名、メッセージ、受信対象を設定します。

テンプレート選択

1. イベントの構成方法に応じて、画面左側の3つのテンプレートのいずれかを選択します。
 - **新規作成:** カテゴリやメトリクスを一から自由に構成できます。複雑な条件や詳細な監視ルールが必要な上級ユーザーに適しています。
 - **クイック設定:** あらかじめ定義されたカテゴリ、メトリクス、基本しきい値が提供され、しきい値のみを調整して素早く適用できるため、初心者に適しています。
 - **高度な設定:** あらかじめ定義されたカテゴリやメトリクスを基に、条件を追加したり自由に変更したりできます。

❗ メトリクスイベントでは、さまざまな設定方法をサポートしています。利用する監視プラットフォームによって、提供されるテンプレートは異なる場合があります。

イベント条件定義

イベント条件定義のステップでは、イベント発生の判断に使用するメトリクス設定、発生回数、一時停止、回復通知、イベント動作時間を設定します。

指標設定

1. 検索欄にカテゴリを入力するか、カテゴリー一覧からカテゴリ（指標）を選択します。
指標設定を進めるには、カテゴリの選択が必要です。

- ・ カテゴリ一覧では、カテゴリ名、データ収集間隔、キーを確認できます。直近3時間にプロジェクトで収集されたメトリクスデータが表示されます。

2. 一覧にない指標を使用する場合は、**直接入力**を選択してカテゴリを手動で入力します。

❗ カテゴリや指標が不明な場合は、メトリクス照会を活用してください。

初めて指標を設定する場合、メトリクス照会を利用すると効率的に指標を見つけられます。

- ・ メトリクス照会で指標を検索すると、関連するカテゴリや詳細情報を確認できます。
- ・ 検索結果から必要なメトリクスの[選択]ボタンをクリックすると、選択した値がイベント設定画面に自動的に反映されます。

メトリクス検索

All 13件 / 全 149件

カテゴリ	名前	単位	タイプ	詳細	マージ	
ApplicationHostResource	CpuSys	pct	field	System領域のCPU使用率	OM: avg TM: avg	選択
ApplicationHostResource	CpuIrq	pct	field	Interrupt Request(Irq)を使用したCPU使用率	OM: avg TM: avg	選択
ApplicationHostResource	CpuSteal	pct	field	実際にCPUを待機する時間を%で表示した値	OM: avg TM: avg	選択
ApplicationHostResource	CpuCores	count	field	CPUコア数	OM: avg TM: avg	選択
ApplicationHostResource	CpuUser	pct	field	User領域のCPU使用率	OM: avg TM: avg	選択
ApplicationHostResource	CpuProc	pct	field	Proc領域のCPU使用率	OM: avg TM: avg	選択
ApplicationHostResource	Cpu	pct	field	CPU使用率	OM: avg TM: avg	選択
ApplicationHostResource	CpuWait	pct	field	ディスク入出力を待つ間(wait)に使用したCPU使用率	OM: avg TM: avg	選択
ProcessPrivateMemory	PrivateMemory	count	field	Number of Bytes Private		

< 1 > 50件 / ページ

3. イベントレベル（Critical、Warning、Info）を選択します。1つの指標に対して複数のレベルを設定できます。

❗ イベントレベルの動作

複数の条件を満たしても、最も優先度の高いレベル（Critical → Warning → Info）のみがイベントとして発生します。詳細は [レベル動作ガイド](#) を参照してください。

- ・ イベントレベルは、危険（Critical）、警告（Warning）、正常（Info）に分類されます。
- ・ 同一指標に対して段階的なしきい値でレベルを設定することを推奨します。

4. 選択したイベントレベルのフィールド、演算子、値を入力します。

a. + 追加 をクリックすると条件を追加できます。

- **&&** : すべての条件を同時に満たした場合 にイベントが発生
- **||** : いずれか 1 つ以上の条件を満たした場合 にイベントが発生

b. - をクリックすると、その条件が削除されます。

❗ 条件式の書き方や対応する演算子については、[条件設定ガイド](#) を参照してください。

発生回数

条件が何回満たされた場合にイベントを発生させるかを設定します。継続的な問題のみを検知したい場合に有効です。

1. 発生頻度を選択します。

- **連続**: 設定した回数分、イベントが連続して発生した場合にイベントを発生
- **直近**: 選択した時間内に、設定した回数分イベントが発生した場合にイベントを発生
 - 選択可能時間: 5秒, 10秒, 15秒, 30秒, 1分, 2分, 3分, 4分, 5分, 10分, 30分, 1時間

2. 発生回数を入力します。

- **Interval** の値は、選択したカテゴリのデータ収集間隔を示します。（Interval: 10s）

一時停止

過剰なイベント発生を防ぐため、イベント動作を一時停止する時間を選択してください。イベント発生後、設定した時間が経過するまで同一イベントは発生しません。

- 選択可能時間: 使用しない, 5分, 10分, 15分, 20分, 30分, 1時間, 2時間, 3時間, 6時間, 12時間, 1日

❗ 解消通知が有効な場合

正常状態の通知（RECOVERED）を受信した時点から、設定した時間が経過するまで、同一イベントが再発しても通知は送信されません。

解消通知

解消通知機能を有効にすると、イベント発生後の状態変化（進行中 → 解消）を追跡できます。**イベント履歴** メニューでは、進行中のイベントとして表示されます。

- 解消通知は **Critical** および **Warning** レベルにのみ適用されます。Info レベルは常に単発イベントとして動作します。
- **Critical** または **Warning** レベルのイベントが解消されると、正常（RECOVERED）状態の通知が送信されます。
- トグルボタンをクリックして **有効化** または **無効化** してください。
 -  **有効**: イベントは状態ベースで動作します。しきい値を超えると進行中となり、値がしきい値未満に回復すると解消状態に遷移します。
 -  **無効**: しきい値を超えるたびに単発イベントが発生します。

イベント動作時間

イベントが特定の時間帯（勤務時間／非勤務時間／点検時間など）にのみ動作するよう、タグを設定してください。タグを設定しない場合、イベントが有効な状態では 24 時間常時動作します。

1. **+ 追加** をクリックします。
2. イベント動作時間で **+ 新しいタグを作成** をクリックします。
3. **イベント動作時間タグ作成** で **タグ名**、**曜日**、**時間**、**色** を選択し、**[適用]** ボタンをクリックします。
4. 作成したタグはタグ一覧で確認でき、チェックボックスを選択すると適用されます。
5. タグを修正または削除するには、 をクリックし、**イベント動作時間タグ修正** で修正または削除してください。

 タグを削除すると、そのタグが適用されているすべてのユーザーからタグが削除されます。ただし、イベントルールで使用中のタグは削除できません。

シミュレーション

シミュレーション機能では、設定したイベント条件を過去データに基づいて事前にテストできます。想定されるイベント件数が多いすぎる、または少なすぎる場合は、条件を調整して最適なしきい値を見つけることができます。

- **ルール検証:** 新しく作成したイベントルールを過去データに適用した場合の結果を確認できます。
- **しきい値チューニング:** イベントが頻発する、またはまったく発生しない場合に、適切なレベルへしきい値を調整します。

シミュレーション開始

1. イベント条件の設定が完了したら、[シミュレーション] ボタンをクリックします。
2. 想定イベント件数と可視化された結果を確認します。

シミュレーション結果の理解

1. 時系列データ

指標の時間帯別変化と各レベルのしきい線がグラフで表示され、イベント発生タイミングを直感的に確認できます。

2. レベル別発生状況

画面右側に Critical、Warning、Info レベルごとのイベント発生回数が表示され、全体の分布や頻度を把握できます。

3. 対象別詳細情報

グラフ上の特定ポイントにマウスを合わせると、その時点の正確な指標値と監視対象が表示されます。複数の対象がある場合は色で区別され、対象ごとにパターンが異なる場合はフィルタリング機能で個別分析が可能です。

4. ピーク区間の特定

指標が急激に上昇する時間帯を確認し、問題が頻発する時間帯やパターンを把握できます。

✔ シミュレーション活用のヒント

• 複数時間帯でのシミュレーション

平日／週末、ピーク／非ピーク時間帯をそれぞれシミュレーションし、時間帯ごとの最適なしきい値を設定してください。



- 実際の障害期間を含める

過去に障害が発生した期間を含めてシミュレーションを実行し、現在のルールが障害を正しく検知できるか確認しましょう。

- 対象フィルタリングの追加

監視対象が多い場合、結果が複雑になります。フィルタリング機能を使って特定の対象のみを選択し、明確な結果を確認してください。

- しきい値を段階的に調整

一度に大きく変更するのではなく、10 パーセント単位で段階的に調整しながら最適値を探すことをおすすめします。

イベント対象選択

イベント対象を指定しない場合、プロジェクト内のすべての対象に対してイベントが発生し、多数のイベントが生成される可能性があります。そのため、イベントを適用する対象を明確に設定することを推奨します。

❗ イベント対象を変更すると、イベント件数が変わる場合があります。シミュレーション ボタンをクリックして再実行し、想定イベント件数を確認してください。

対象選択

イベントを適用する対象は、**選択入力** または **直接入力** の方法で指定できます。

- **選択入力** 直接入力

1. タグ、演算子、値を選択または入力してください。
 - a. タグが見つけない場合は、**メトリクス照会** を使ってタグを検索できます。
2. **+ 追加** をクリックして、条件（**&&**、**||**）でイベント対象を追加してください。

監視対象のタグ、演算子、値を直接入力してください。

- 直接入力を選択すると、入力欄の下に使用可能なタグ一覧（**タグ選択入力**）が表示されます。

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

 入力方法を変更すると、作成中の内容は初期化されます。

基本情報および通知設定

イベント名、メッセージ、受信対象を設定します。設定した内容はイベント履歴や実際の通知メッセージにそのまま表示されるため、識別しやすく分かりやすい名称にすることが重要です。

イベント有効化

設定した条件を満たした際にイベントを発生させるかどうかを設定します。

-  **有効**: 設定した条件を満たすとイベントが発生します。
-  **無効**: 条件を判定しません。

イベント名

イベントのタイトルとして使用するイベント名を入力してください。設定したイベント名は **イベント一覧** および **イベント履歴** メニューに表示され、この名前で検索することができます。

メッセージ

イベントメッセージを入力してください。入力したメッセージは、イベント履歴および通知に使用されます。 をクリックすると、過去に作成したメッセージ履歴を確認できます。メッセージには変数を使用して、イベント発生時点の実際の値を含めることができます。

- **変数の使用ルール**
 - 変数形式: `${指標名}`
 - 設定した **カテゴリ** と同一 **カテゴリ内** の指標のみを変数として使用できます。
 - 複数の変数を組み合わせて、より詳細なメッセージを作成できます。
 - 使用可能な変数一覧は **メトリクス照会** メニューで確認できます。

- 変数の使用例

	イベント設定	イベント発生時
タイトル	Disk 使用量増加	Disk 使用量増加
メッセージ	Disk = \${disk}%	Disk = 89.9%

イベント受信

イベント通知を受信するメンバーを指定します。

- 全体受信** タグ選択受信

プロジェクトで通知設定が有効になっているすべての対象（メンバー、チャンネル）に通知が送信されます。

指定したタグを持つプロジェクトメンバーに通知が送信されます。

1. **タグ選択受信** を選択します。
2. **受信タグ** 項目で [+ タグ追加] または [+] ボタンをクリックします。
3. **イベント受信タグ** 画面の下にある + **新しいタグを作成** をクリックします。
4. **タグ作成** 画面でタグ名を入力し、色を選択した後、[タグ作成] ボタンをクリックしてタグを作成します。
5. 作成したタグは、**タグ一覧** の  をクリックして修正または削除できます。
6. **イベント受信タグ** 画面の **タグ一覧** から希望するタグを選択すると適用されます。

ⓘ 受信タグ

受信タグは、通知を受け取るユーザーやチャンネルを **グループ単位で管理するための機能** です。イベントに受信タグを設定すると、そのタグが付与されたユーザーにのみ通知が送信されます。受信タグを設定しない場合、プロジェクト内のすべてのユーザーに通知が送信されます。

イベント修正／削除

1. **警告アラート** > **イベント設定** の **メトリクス** タブに移動します。

2. イベント一覧で、修正または削除したいイベントの  をクリックします。
3. イベントルール修正 画面でオプションを修正し、[保存] ボタンをクリックします。
 - a. 選択したイベントを削除する場合は、イベントルール修正 画面右上の [削除] ボタンをクリックします。

イベント共有

メトリクスイベント設定を JSON ファイルとして保存し、他のユーザーと設定を共有したり、他のユーザーの設定を取り込んだりすることができます。

- JSON ファイル名: `event-rules-YYYYMMDD.json`

エクスポート

1. 画面右上の [JSON ] ボタンをクリックします。
2. JSON 編集画面が表示されたら、[ エクスポート] ボタンをクリックします。
 - イベントを検索した状態でエクスポート機能を使用すると、検索結果のみが JSON ファイルとしてダウンロードされます。
3. JSON ファイルがダウンロードされたら、共有したい他のユーザーに渡してください。

インポート

1. 画面右上の [] ボタンをクリックします。
2. エクスポート 機能でダウンロードした JSON ファイルを選択します。
3. JSON 編集画面が表示されたら、[一覧に追加] または [上書き] を選択します。

 同じ種類の製品間での利用を推奨します。異なる製品のプロジェクトからイベント設定を取り込むことは可能ですが、正常に動作しない場合があります。

JSON 形式で編集する

1. 画面右上の [JSON ] ボタンをクリックします。

2. 編集画面が表示されたら、JSON 形式に従って内容を修正してください。
3. 修正が完了したら、画面下部の [保存] ボタンをクリックします。

❗ 修正した内容が JSON 形式に合っていない場合、画面下部にエラーメッセージが表示され、保存できません。表示されるエラーメッセージは、形式エラーの内容によって異なる場合があります。

JSON error

JSON データ構造

```
{
  "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"
  ]
}
}

```

表 | JSON データ構造

JSON フィールド	型	説明	備考
version	Integer	イベントルールのバージョン	変更制限
eventId	String	イベントルールの一意識別子	
enabled	boolean	イベントの有効／無効	
stateful	boolean	状態ベースイベントかどうか	
title	String	ユーザーが設定したイベントルール名	
message	String	ユーザーが設定したイベントルールメッセージ	
category	String	データカテゴリ	
alertLabel	List<String>	イベント状態管理のため、カテゴリごとに指定される基本識別子（プライマリキー）値	変更制限
repeatCount	Integer	繰り返し回数	
repeatDuration	Long	繰り返し期間	
silent	Integer	一時停止時間	
receiver	List<String>	受信タグのキー値一覧	

JSON フィールド	型	説明	備考
timeTag	List<String>	動作時間タグのキー値一覧	
selectString	String	対象選択	
conditions	List<Object>	レベル別の発生条件一覧	
└ level	byte	レベル値	Critical: 30、Warning: 20、Info: 10
└ enabled	boolean	レベルの有効／無効	
└ rule	String	レベル発生条件	
createTime	Long	イベントルールの初回作成時刻	
lastModifiedTime	Long	イベントルールの最終修正時刻	
lastModifiedUser	String	イベントルールを最後に修正したアカウント	
basic	boolean	クイック設定で作成されたイベントかどうか	変更制限
metald	String	クイック設定テンプレートの一意識別子	変更制限: この値はクイック設定で作成されたイベントにのみ存在します (basic=true)。
selectCondition	Object	クイック設定の対象選択値	この値はクイック設定で作成されたイベントにのみ存在します (basic=true)。

❗ 「変更制限」と表示されたフィールドはイベント動作に影響を与える可能性があるため、値を変更しないことを推奨します。

付録

発生条件・対象選択ガイド

メトリクスアラートにおけるイベントの発生条件とイベント対象の選択は、同一の構文を使用します。ただし、イベント発生条件ではフィールド（Field）のキーを変数として使用し、イベント対象の選択ではタグ（Tag）のキーを変数として使用します。

レベル動作ガイド

イベントレベルは、危険（Critical）、警告（Warning）、正常（Info）の3段階に分類されます。

1. 優先順位に基づくイベント発生

複数のレベル条件を同時に満たした場合、最も優先度の高いイベントのみが発生します。

例

```
設定:  
- Warning: CPU > 70%  
- Critical: CPU > 90%  
  
現在の状態: CPU 95%  
→ 結果: Critical イベントのみ発生（Warning は抑制される）
```

2. レベル上昇

進行中状態を持つイベントにおいて、低いレベルのイベントが進行中の状態で高いレベルの条件を満たすと、両方のレベルが進行中状態になります。

例

```
設定:  
- Warning: CPU > 70%  
- Critical: CPU > 90%  
  
シナリオ:
```

- 1) CPU 80% → Warning 発生（進行中）
- 2) CPU 95% → Warning（進行中）、Critical（進行中）

3. レベル下降

進行中状態を持つイベントで、高いレベルから低いレベルへ遷移した場合、高いレベルは解消され、低いレベルが維持されます。

例

設定:

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

シナリオ:

- 1) CPU 97% → Critical 発生
- 2) CPU 85% → Critical 解消、Warning 維持
- 3) CPU 65% → Warning 解消

4. 動作フロー

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

メトリクス値: 60% → 75% → 92% → 85% → 60%

状態: 正常 Warning Critical Warning 正常
 (発生) (発生) (維持) (解消)
 Warning
 (維持)

- ① 進行中状態を持つイベントは、条件が満たされている間は継続して有効となり、条件が解除されるまで維持されます。

条件設定ガイド

❗ メトリクス名が数字で始まる場合、または特殊文字を含む場合は、`${メトリクス名}` の形式で記述する必要があります。

- 括弧 `()`, `[]`
- 演算子 `+`, `-`, `*`, `/`, `%`
- 区切り文字 `:`, `@`, `#`, `,`, `,`, (空白)
- その他の特殊文字 `!`, `^`, `&`, `|`, `~`, ````, `=`

`${}` 使用例:

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

`${}` なしで使用可能: 英字、アンダースコア (`_`)、ドット (`.`) のみを含む場合

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

1. 比較演算子

数値比較

```
より大きい:  cpu > 80
以上:        cpu >= 80
より小さい:  memory < 1000
以下:        memory <= 1000
等しい:      status == 200
等しくない:  error != 0
```

文字列比較

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

2. 算術演算子

- 基本的な算術演算

```
加算:   cpu + 10 >= 90  
減算:   memory - 100 >= 500  
乗算:   cpu * 2 >= 100  
除算:   disk / 1024 >= 100  
剰余:   value % 10 == 0
```

- 括弧による優先順位の制御

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

- 負の値の表現

```
cpu > -100
```

3. 論理演算子

- AND 演算 (&&)

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

- OR 演算 (||)

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

- 複合論理演算

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

4. パターンマッチング演算子

- LIKE 演算子

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

- NOT LIKE 演算子

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

5. 組み込み関数

- Null チェック関数

```
isNull(value)      # null かどうかを確認
isNotNull(value)   # null でないかを確認
nvl(value, 0)      # null の場合に既定値を返す
isEmpty(str)       # 空文字列かどうかを確認
isNotEmpty(str)    # 空文字列でないかを確認
```

- 集計関数

```
sum(cpu, memory, disk)    # 合計
avg(cpu, memory)          # 平均
max(cpu, memory, disk)    # 最大値
min(cpu, memory, disk)    # 最小値
count(value1, value2, value3) # 件数
```

- 数学関数

```
round(cpu, 2)    # 四捨五入（小数点以下2桁）
```

- 文字列関数

```
length(str)      # 文字列の長さ
startsWith(str, 'prefix') # 接頭辞の確認
endsWith(str, 'suffix') # 接尾辞の確認
indexOf(str, 'search') # 文字列の位置
substring(str, 0, 10) # 部分文字列
trim(str)        # 空白の削除
replace(str, 'old', 'new') # 文字列の置換
hasStr(str, 'search') # 文字列の包含判定
```

- 条件関数

- **if:** 条件式が `true` の場合は `true値` を返し、`false` の場合は `false値` を返す条件関数

形式

```
if(条件, true値, false値)
```

例

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

- **decode:** 値と条件を比較し、一致した条件の結果を返します。一致しない場合は既定値を返します

形式

```
decode(値, 条件1, 結果1, 条件2, 結果2, ..., 条件N, 結果N, 既定値)
```

例

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

- **in:** 値が指定した候補値のいずれかと一致した場合は `true` 、それ以外は `false` を返します

形式

```
in(値, 候補値1, 候補値2, ..., 候補値N)
```

例

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

❗ 記述時の注意事項

- 推奨事項
 - 簡単な変数名は `${}` を使わずに記述（例: `cpu`, `memory`）
 - 特殊文字を含む場合は必ず `${}` を使用
 - 複雑な演算は括弧で明確に区切る
 - 関数名は正確に入力（大文字と小文字を区別）
- 避けるべき事項
 - 不完全な式の記述（例: `cpu >` , `memory &&` ）
 - 括弧の不一致（例: `(cpu > 80 && cpu > 70)` ）
 - 演算子の連続使用(例: `cpu >> 80` , `cpu >< 80`)

リアルタイムログイベント

ホーム > プロジェクト選択 >  アラート通知 > イベント設定 > リアルタイムログ タブ

収集したログデータを条件に合わせてフィルタリングして警告通知を設定できます。ログイベントを使用するには、ログモニタリングを有効化する必要があります。**ログモニタリングの有効化**については、各製品のログドキュメントを参照してください。

- ・ **リアルタイムログイベント**: リアルタイムで収集したログで、設定したイベント条件が満たされるとイベントが発生します。

基本オプション

- ・ **検索**: イベント名またはイベント受信タグを選択して目的のイベントを検索
- ・ **JSONダウンロード/アップロード**: イベントルールはJSONエディタで直接編集するか、ファイルにダウンロードして修正後に再アップロード可能
- ・ **通知メッセージ設定**: 受信するメッセージの詳細項目を選択し、項目ごとに内容を編集
- ・ **+ イベント追加**: 新しいログイベントを追加

表 | リアルタイムログイベント一覧構成

項目	説明
イベント名	通知タイトルとして使用されるイベント名 - 最大255バイトまで入力可能
カテゴリ	ログ分類名（ログフォルダ名）
検索キー	ログデータで検索したい項目 - 例: HTTPレスポンスステータスコードの値にアクセスする場合、検索キー <code>status</code>
検索値	検索キーに対応する実際のデータ。ログに入力した文字列が含まれる場合に警告通知を送信 - 例: 検索キー <code>status</code> 、検索値 <code>200</code> を設定した場合、HTTPステータスコード200を含むログデータ収集時に警告通知が発生

項目	説明
イベント発生一時停止	イベント通知発生後、同じイベントの発生を一定時間停止 - 選択可能時間: 使用しない、5分、10分、15分、20分、30分、1時間、2時間、3時間、6時間、12時間、1日 - 解消通知が有効な場合、正常（RECOVERED）状態の通知受信後、選択した時間中は同じイベントが発生しても通知されない
イベント対象フィルタリング	イベントが適用される対象の条件 - 対象条件を設定しない場合、収集されるすべてのデータに対して通知を判断 - 選択入力: タグ、演算子、値を選択して条件を構成 - 直接入力: 条件を直接入力して対象を指定
イベント受信タグ	イベント通知を受け取るユーザーまたはグループ（受信タグ）
	イベントの編集と削除
	イベントの有効化状態 - 有効: 条件を満たすとイベント発生 - 無効: イベントが動作せず、条件をチェックしない

イベント設定

ログイベントは、リアルタイムで収集されるログ、または特定条件を満たすログが一定数蓄積された際に警告通知を設定できる機能です。

リアルタイムログイベントの追加

1. アラート通知 > イベント設定のリアルタイムログタブをクリックしてください。
2. 画面右側の [+ イベント追加] ボタンをクリックしてください。
3. イベントルール追加ウィンドウでログイベント条件を設定してください。
 - イベント名: イベントタイトルとして使用する名前を入力してください。

- **イベント有効化:** トグルボタンを有効にすると、条件を満たしたときにイベントが発生します。
- **レベル:** イベントレベル (**Critical**、**Warning**、Info) を選択してください。
- **メッセージ:** イベント発生時に受け取る通知メッセージを入力してください。メッセージに変数を使用して、イベント発生時点の実際の値を含めることができます。

✔ 変数使用ルール

- 変数形式: \${指標名}
- 設定したカテゴリと同じカテゴリ内の指標のみ変数として使用できます。
- 複数の変数を組み合わせて詳細なメッセージを構成できます。
- 使用可能な変数一覧は**メトリクス照会**で確認できます。

- **カテゴリ:** ログ分類名（ログフォルダ名）をリストから選択するか、直接入力してください。カテゴリを選択してから検索キーと検索値を入力できます。
- **検索キー:** ログデータで検索したい項目を入力してください。
 - 例: HTTPレスポンスステータスコードの値にアクセスする場合、**検索キー** status
- **検索値:** 検索キーに対応する実際のデータを入力してください。ログに入力した文字列が含まれる場合に警告通知を送信します。
 - 例: **検索キー** status、**検索値** 200 を設定した場合、HTTPステータスコード200を含むログデータ収集時に警告通知が発生
- **イベント対象フィルタリング:** イベントが適用される対象の条件を入力してください。入力値がない場合、収集されるすべてのデータに対して通知を判断します。
 - **選択入力:** タグ、演算子、値を選択して対象条件を設定してください。

❗ 条件式の記述方法とサポートされる演算子については、[条件設定ガイド](#)を参照してください。

- **直接入力:** 条件を直接入力してください。
- **イベント発生一時停止:** 通知を一時停止する時間を選択してください。イベント発生後、設定した時間中は同じイベントが発生しません。

- 選択可能時間: 使用しない、1分、2分、3分、5分、10分、20分、30分、1時間、3時間、6時間、12時間
- イベント動作時間: 特定の時間帯（業務/非業務/メンテナンス時間など）にイベントが動作するようにタグを設定してください。タグを設定しない場合、イベントが有効な状態で24時間常時動作します。
 1. + 追加をクリックしてください。
 2. イベント動作時間で**+新しいタグを作成**をクリックしてください。
 3. イベント動作時間タグの作成でタグ名、曜日、時間、色を選択し、[適用] ボタンをクリックしてください。
 4. 作成したタグはタグリストで確認でき、チェックボックスを選択すると適用されます。
 5. 変更または削除するタグの  アイコンをクリックして、イベント動作時間タグの編集でタグを編集または削除できます。

 タグを削除すると、そのタグが適用されているすべてのユーザーのタグが削除されます。ただし、イベントルールで使用中のタグは削除できません。

- イベント受信タグ: イベントに受信タグを設定すると、そのタグを持つプロジェクトメンバーに通知が送信されます。受信タグを設定しない場合、プロジェクト内のすべてのユーザーに通知が送信されます。
 1. + タグ追加または+をクリックしてください。
 2. イベント受信タグウィンドウ下部の**+ 新しいタグを作成**をクリックしてください。
 3. タグ作成ウィンドウでタグ名を入力し、色を選択してから、[タグ作成] ボタンをクリックしてタグを作成してください。
 4. 作成されたタグはタグリストの  アイコンをクリックして編集または削除してください。
 5. イベント受信タグウィンドウのタグリストから目的のタグを選択すると適用されます。

 イベント設定時にイベント受信タグを選択して、そのタグを持つプロジェクトメンバーとサードパーティプラグインに通知を送信できます。アラート通知 > 通知設定でプロジェクトメンバーとサードパーティプラグインにそれぞれタグを指定できます。

4. イベントルール追加ウィンドウで設定が完了したら、[保存] ボタンをクリックしてください。

イベントの編集/削除

1. アラート通知 > イベント設定のリアルタイムログタブに移動してください。
2. ログイベントリストで編集または削除するイベントの  アイコンをクリックしてください。
3. イベント設定画面でオプションを変更し、[保存] ボタンをクリックしてください。
 - a. 選択したイベントを削除するには、イベント設定画面の右上の [削除] ボタンをクリックしてください。

イベントの共有

メトリクスイベント設定を JSON ファイルとして保存し、他のユーザーと設定を共有したり、他のユーザーの設定を取り込んだりすることができます。

- JSON ファイル名: `event-rules-YYYYMMDD.json`

エクスポート

1. 画面右上の [JSON ] ボタンをクリックします。
2. JSON 編集画面が表示されたら、[ エクスポート] ボタンをクリックします。
 - イベントを検索した状態でエクスポート機能を使用すると、検索結果のみが JSON ファイルとしてダウンロードされます。
3. JSON ファイルがダウンロードされたら、共有したい他のユーザーに渡してください。

インポート

1. 画面右上の [] ボタンをクリックします。
2. エクスポート 機能でダウンロードした JSON ファイルを選択します。
3. JSON 編集画面が表示されたら、[一覧に追加] または [上書き] を選択します。

 同じ種類の製品間での利用を推奨します。異なる製品のプロジェクトからイベント設定を取り込むことは可能ですが、正常に動作しない場合があります。

JSON 形式で編集する

1. 画面右上の [JSON ] ボタンをクリックします。
2. 編集画面が表示されたら、JSON 形式に従って内容を修正してください。
3. 修正が完了したら、画面下部の [保存] ボタンをクリックします。

❗ 修正した内容が JSON 形式に合っていない場合、画面下部にエラーメッセージが表示され、保存できません。表示されるエラーメッセージは、形式エラーの内容によって異なる場合があります。

JSON error

付録

発生条件・対象選択ガイド

メトリクスアラートにおけるイベントの発生条件とイベント対象の選択は、同一の構文を使用します。ただし、イベント発生条件ではフィールド（Field）のキーを変数として使用し、イベント対象の選択ではタグ（Tag）のキーを変数として使用します。

レベル動作ガイド

イベントレベルは、危険（Critical）、警告（Warning）、正常（Info）の3段階に分類されます。

1. 優先順位に基づくイベント発生

複数のレベル条件を同時に満たした場合、最も優先度の高いイベントのみが発生します。

例

設定:

- Warning: CPU > 70%

- Critical: CPU > 90%

現在の状態: CPU 95%
→ 結果: Critical イベントのみ発生 (Warning は抑制される)

2. レベル上昇

進行中状態を持つイベントにおいて、低いレベルのイベントが進行中の状態で高いレベルの条件を満たすと、両方のレベルが進行中状態になります。

例

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

シナリオ:
1) CPU 80% → Warning 発生 (進行中)
2) CPU 95% → Warning (進行中)、Critical (進行中)

3. レベル下降

進行中状態を持つイベントで、高いレベルから低いレベルへ遷移した場合、高いレベルは解消され、低いレベルが維持されます。

例

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

シナリオ:
1) CPU 97% → Critical 発生
2) CPU 85% → Critical 解消、Warning 維持
3) CPU 65% → Warning 解消

4. 動作フロー

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


```

メトリクス値: 60% → 75% → 92% → 85% → 60%
状態:   正常   Warning   Critical   Warning   正常
        (発生)   (発生)   (維持)   (解消)
           Warning
           (維持)

```

- ❗ 進行中状態を持つイベントは、条件が満たされている間は継続して有効となり、条件が解除されるまで維持されます。

条件設定ガイド

- ❗ メトリクス名が数字で始まる場合、または特殊文字を含む場合は、`${メトリクス名}` の形式で記述する必要があります。

- 括弧 `()`, `[]`
- 演算子 `+`, `-`, `*`, `/`, `%`
- 区切り文字 `:`, `@`, `#`, `,`, ``` (空白)
- その他の特殊文字 `!`, `^`, `&`, `|`, `~`, ````, `=`

`${}` 使用例:

```

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

```

`${}` なしで使用可能: 英字、アンダースコア (`_`)、ドット (`.`) のみを含む場合

```

cpu > 80
cpu_usage > 50
CPUUtilization.Average > 0.8

```

1. 比較演算子

数値比較

```
より大きい:  cpu > 80
以上:         cpu >= 80
より小さい:   memory < 1000
以下:         memory <= 1000
等しい:       status == 200
等しくない:   error != 0
```

文字列比較

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

2. 算術演算子

- 基本的な算術演算

```
加算:  cpu + 10 >= 90
減算:  memory - 100 >= 500
乗算:  cpu * 2 >= 100
除算:  disk / 1024 >= 100
剰余:  value % 10 == 0
```

- 括弧による優先順位の制御

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

- 負の値の表現

```
cpu > -100
```

3. 論理演算子

- AND 演算 (&&)

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

- OR 演算 (||)

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

- 複合論理演算

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

4. パターンマッチング演算子

- LIKE 演算子

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

- NOT LIKE 演算子

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

5. 組み込み関数

- Null チェック関数

```
isNull(value)      # null かどうかを確認
isNotNull(value)   # null でないかを確認
nvl(value, 0)      # null の場合に既定値を返す
isEmpty(str)       # 空文字列かどうかを確認
isNotEmpty(str)    # 空文字列でないかを確認
```

- 集計関数

```
sum(cpu, memory, disk)    # 合計
avg(cpu, memory)          # 平均
max(cpu, memory, disk)    # 最大値
min(cpu, memory, disk)    # 最小値
count(value1, value2, value3) # 件数
```

- 数学関数

```
round(cpu, 2)    # 四捨五入（小数点以下2桁）
```

- 文字列関数

```
length(str)      # 文字列の長さ
startsWith(str, 'prefix') # 接頭辞の確認
endsWith(str, 'suffix') # 接尾辞の確認
indexOf(str, 'search') # 文字列の位置
substring(str, 0, 10) # 部分文字列
trim(str)        # 空白の削除
replace(str, 'old', 'new') # 文字列の置換
hasStr(str, 'search') # 文字列の包含判定
```

- 条件関数

- **if:** 条件式が `true` の場合は `true値` を返し、`false` の場合は `false値` を返す条件関数

形式

```
if(条件, true値, false値)
```

例

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

- **decode:** 値と条件を比較し、一致した条件の結果を返します。一致しない場合は既定値を返します

形式

```
decode(値, 条件1, 結果1, 条件2, 結果2, ..., 条件N, 結果N, 既定値)
```

例

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

- **in**: 値が指定した候補値のいずれかと一致した場合は `true`、それ以外は `false` を返します

形式

```
in(値, 候補値1, 候補値2, ..., 候補値N)
```

例

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

❗ 記述時の注意事項

- 推奨事項
 - 簡単な変数名は `${}` を使わずに記述（例: `cpu`, `memory`）
 - 特殊文字を含む場合は必ず `${}` を使用
 - 複雑な演算は括弧で明確に区切る
 - 関数名は正確に入力（大文字と小文字を区別）
- 避けるべき事項
 - 不完全な式の記述（例: `cpu >` , `memory &&` ）
 - 括弧の不一致（例: `(cpu > 80 && cpu > 70)` ）
 - 演算子の連続使用(例: `cpu >> 80` , `cpu >< 80`)

複合ログイベント設定

ホーム > プロジェクト選択 >  アラート通知 > イベント設定 > 複合ログ タブ

収集したログデータを条件に合わせてフィルタリングして警告通知を設定できます。ログイベントを使用するには、ログモニタリングを有効化する必要があります。ログモニタリングの有効化については、各製品のログドキュメントを参照してください。

- **複合ログイベント:** 設定したデータ照会範囲内のログを基準に、ログ検索条件を満たすログ数が閾値以上の場合にイベントが発生します。

ⓘ 権限

複合メトリクスイベントを設定するには通知設定権限が必要です。通知設定権限は、ホーム画面 > プロジェクト選択 > 管理 > 統合メンバー管理で、権限を付与するメンバーの  アイコンをクリックして設定できます。

基本オプション

- **検索:** イベント名またはイベント受信タグを選択して目的のイベントを検索
- **JSONダウンロード/アップロード:** イベントルールはJSONエディタで直接編集するか、ファイルにダウンロードして修正後に再アップロード可能
- **通知メッセージ設定:** 受信するメッセージの詳細項目を選択し、項目ごとに内容を編集
- **+ イベント追加:** 新しいログイベントを追加

表 | 複合ログイベント一覧構成

項目	説明
イベント名	通知タイトルとして使用されるイベント名
テンプレート	複合ログテンプレート

項目	説明
カテゴリ	ログ分類名（ログフォルダ名）
ルール	イベントが発生する条件
イベント状態が解消されたら追加通知	CriticalとWarningレベルのイベントが解消されたとき、正常（RECOVERED）状態の通知を受信するかどうか - 有効: 進行中 → 正常状態に移行したときRECOVERED通知を送信し、イベント履歴で進行中/解消状態を区別して確認可能 - 無効: 閾値を超えるたびに単発のイベントが発生
イベント発生一時停止	イベント通知発生後、同じイベントの発生を一定時間停止 - 選択可能時間: 使用しない、5分、10分、15分、20分、30分、1時間、2時間、3時間、6時間、12時間、1日 - 解消通知が有効な場合、正常（RECOVERED）状態の通知受信後、選択した時間中は同じイベントが発生しても通知されない
インターバル	ログデータを照会する時間範囲
イベント受信タグ	イベント通知を受け取るユーザーまたはグループ（受信タグ）
	イベントの編集と削除
	イベントの有効化状態 - 有効: 条件を満たすとイベント発生 - 無効: イベントが動作せず、条件をチェックしない

イベント設定

設定したデータ照会範囲内のログを基準に、ログ検索条件を満たすログ数が閾値以上の場合に警告通知を設定できる機能です。

複合ログイベントの追加

1. アラート通知 > イベント設定の複合ログ タブをクリックしてください。
2. 画面右側の [+ イベント追加] ボタンをクリックしてください。
3. イベントルール追加ウィンドウでログイベント条件を設定してください。詳細については、[基本設定](#)、[詳細設定](#)、[追加設定](#)を参照してください。

複合ログイベントの追加

4. イベントルール追加ウィンドウで設定が完了したら、[保存] ボタンをクリックしてください。

基本設定

- イベント名: イベントタイトルとして使用する名前を入力してください。
- イベント有効化: トグルボタンを有効にすると、条件を満たしたときにイベントが発生します。
- レベル: イベントレベル (**Critical**、**Warning**、Info) を選択してください。

詳細設定

[テンプレート \(プリセット\)](#)、[メッセージ](#)、[カテゴリ](#)、[フィルター](#)、[イベント発行条件](#)を設定します。

テンプレート (プリセット)

定義済みのプリセットを選択すると、[フィルター](#)、[クエリタイプ](#)、[イベント発行条件](#)が自動的に設定されます。プリセットを選択後、必要に応じて変更できます。

複合ログテンプレートの種類



プリセット	クエリタイプ	デフォルトルール
使用しない	none	rows > 10
2xxステータスコード件数	count	count > 10



プリセット	クエリタイプ	デフォルトルール
3xxステータスコード件数	count	count > 10
4xxステータスコード件数	count	count > 10
5xxステータスコード件数	count	count > 10
正常ステータスコード (2xx, 3xx) 件数	count_v2	include_minus_exclude_count > 10
エラーステータスコード (4xx, 5xx) 件数	count_v2	include_minus_exclude_count > 10
エラー受信件数	count	count > 10
例外受信件数	count	count > 10
毎秒ログ発生件数	rps	rps > 100
フィールド集計 (Aggregation)	aggr	avg > 1000
比率 (Rate)	rate	rate > 10
ユニーク値数 (Cardinality)	cardinality	cardinality > 100
パーセンタイル (Percentile)	percentile	p99 > 3000

メッセージ

イベント発生時に受け取る通知メッセージを入力してください。メッセージに変数を使用して動的なメッセージを構成できます。

- 例示: メッセージ `${host}` でエラー `${count}` 件発生 → 通知メッセージ web-01 でエラー15件発生

表 | メッセージ変数

変数	説明	使用条件
<code>\${count}</code>	条件に一致するログ件数	常に使用可能
<code>\${groupField}</code>	グループ化フィールド名	グループ化通知のみ
<code>\${groupValue}</code>	グループ化フィールド値	グループ化通知のみ
<code>\${フィールド名}</code>	グループ化フィールド値（フィールド名で直接参照）	グループ化通知のみ

❗ `${count}` 変数はグループ化の有無に関わらず、すべての通知で使用できます。 `${groupField}`、`${groupValue}`、`${フィールド名}` 変数はグループ化フィールドが設定されている場合のみ置換されます。

カテゴリ

ログ分類名（ログフォルダ名）をリストから選択するか、直接入力してください。カテゴリを選択してから検索キーと検索値を入力できます。

フィルター

Luceneクエリ構文でログ検索条件を入力します。2種類の入力モードをサポートします。

- フィルターモード [▼](#): フィールドと値を選択してクエリを構成します。
- コードモード [<>](#): Luceneクエリを直接入力します。

表 | Luceneクエリ例

クエリ	説明
<code>level:ERROR</code>	levelフィールドがERRORのログ
<code>status_nxx:status_4xx OR status_nxx:status_5xx</code>	4xxまたは5xxステータスコード
<code>appender:accessLog</code>	accessLog appenderのログ
<code>response_time.n:*</code>	response_time.nフィールドが存在するログ

クエリ	説明
host:web-01 AND level:ERROR	web-01ホストのエラーログ

イベント発行条件

クエリタイプ別に設定します。選択したテンプレート（プリセット）またはクエリタイプに応じて、追加設定項目が表示されます。

表 | イベント発行条件キーの意味

キー	意味
rows / count	フィルター条件に一致するログ件数
rps	毎秒ログ発生件数（件数 / インターバル秒）
avg	対象フィールド値の平均
sum	対象フィールド値の合計
min	対象フィールド値の最小値
max	対象フィールド値の最大値
rate	分子件数 / 分母件数 × 100（%）
cardinality	対象フィールドのユニーク値数
p99 / p95 / p90 / p75 / p50	対象フィールドのパーセンタイル値
include_minus_exclude_count	含むフィルター件数 - 除外フィルター件数

- **件数（count / none）**：設定したフィルター条件に一致するログの件数をカウントします。

表 | 件数設定項目

設定項目	説明
フィルター	ログ検索条件（Luceneクエリ）
イベント発行条件	件数 または 条件に一致するログ {演算子} {閾値}（例: count > 10）

- **毎秒ログ発生件数（rps）**：設定したフィルター条件に一致するログの毎秒発生件数（Requests Per Second）を計算します。インターバル時間中の総件数をインターバル秒数で割って算出します。

表 | 毎秒ログ発生件数設定項目

設定項目	説明
フィルター	ログ検索条件（Luceneクエリ）
イベント発行条件	RPS {演算子} {閾値}（例: rps > 0.5）

- **フィールド集計（aggr）**：指定した数値フィールドの集計値（平均、合計、最小値、最大値）を計算します。イベント発行条件で集計方式をドロップダウンから選択できます。

表 | フィールド集計設定項目

設定項目	説明
フィルター	ログ検索条件（Luceneクエリ）
対象フィールド	集計対象の数値フィールド（例: response_time.n）
イベント発行条件	平均 / 合計 / 最小値 / 最大値 {演算子} {閾値}（例: avg > 1000）

- **比率（rate）**：分子フィルターと分母フィルターの件数比率（%）を計算します。全ログに対する特定条件の比率を監視する際に有用です。

表 | 比率設定項目

設定項目	説明
フィルター（分子）	比率計算の分子となるログ条件（例: <code>level:ERROR</code> ）
分母フィルター	比率計算の分母となるログ条件（例: <code>level:*</code> ）
イベント発行条件	比率（%） {演算子} {閾値}（例: <code>rate > 10</code> ）

- 例示: フィルター `level:ERROR`、分母フィルター `level:*`、ルール `rate > 10` → 全ログ中のエラー比率が10%を超えると通知が発生
- **ユニーク値数（cardinality）** : 指定したフィールドのユニーク値数を計算します。異常に多くの種類の値が発生する場合を検出する際に有用です。

表 | ユニーク値数設定項目

設定項目	説明
フィルター	ログ検索条件（Luceneクエリ）
対象フィールド	ユニーク値を計算するフィールド（例: <code>host</code> ）
イベント発行条件	ユニーク値数 {演算子} {閾値}（例: <code>cardinality > 100</code> ）

- **パーセンタイル（percentile）** : 指定した数値フィールドのパーセンタイル値を計算します。レスポンスタイムのテールレイテンシを監視する際に有用です。パーセンタイルの選択を変更すると、イベント発行条件のキーが自動的に更新されます。

表 | パーセンタイル設定項目

設定項目	説明
フィルター	ログ検索条件（Luceneクエリ）
対象フィールド	パーセンタイルを計算する数値フィールド（例: <code>response_time.n</code> ）
パーセンタイル	P99、P95、P90、P75、P50から選択

設定項目	説明
イベント発行条件	P99 / P95 / ... {演算子} {閾値} (例: p99 > 3000)

表 | パーセンタイルの意味

パーセンタイル	意味
P50	中央値。全データの50%がこの値以下
P75	全データの75%がこの値以下
P90	全データの90%がこの値以下
P95	全データの95%がこの値以下
P99	全データの99%がこの値以下

- 含む/除外件数 (count_v2) : 含むフィルターの件数から除外フィルターの件数を引いた純件数を計算します。

表 | 含む/除外件数設定項目

設定項目	説明
フィルター (含む)	含むログ条件 (例: status_nxx:status_4xx OR status_nxx:status_5xx)
フィルター除外	除外するログ条件 (例: status_nxx:status_4xx)
分母フィルター	比率計算用の分母 (任意)
イベント発行条件	含む-除外件数 {演算子} {閾値} (例: include_minus_exclude_count > 10)

- 例示: フィルター status_nxx:status_4xx OR status_nxx:status_5xx、フィルター除外 status_nxx:status_4xx
→ 4xx+5xxから4xxを除いた純5xx件数が10を超えると通知が発生

グループ化フィールド（Group By）

グループ化フィールドを設定すると、そのフィールドの値ごとに独立して通知条件が判定されます。ドロップダウンからグループ化するフィールドを選択します。ドロップダウンをクリックすると、現在のカテゴリで使用可能なフィールド一覧がオートコンプリートで表示されます。

- 例示: フィルター `level:ERROR`、グループ化フィールド `host`、ルール `rows > 3`

表 | グループ化設定の比較

項目	グループ化なし	グループ化あり
判定単位	全ログを1つに集計	グループ値ごとに独立して集計
通知発生	1件	条件を満たすグループ数分
通知タイトル	イベントタイトル	[グループ値] イベントタイトル
Stateful	全体基準での状態遷移	グループごとに独立した状態遷移

- `[web-01] エラー通知` — web-01でエラー8件 → 通知発生
- `[web-02] エラー通知` — web-02でエラー5件 → 通知発生
- `[api-01] エラー通知` — api-01でエラー2件 → 条件未達、通知なし

❗ イベント状態が解消されたら追加通知を有効にした場合、グループごとに独立してABNORMAL → RECOVERED状態が遷移します。例えば web-01 のエラーが解消されると `[web-01] RECOVERED 通知` が発生し、他のホストの状態には影響しません。

追加設定

- **インターバル:** 選択した時間（`unset`、`1分`、`5分`、`10分`、`30分`、`1時間`、`12時間`）間隔で通知条件を確認します。
- **無音:** イベント発生後、選択した時間（`unset`、`1分`、`5分`、`10分`、`30分`、`1時間`、`12時間`）中は同じイベントが発生しません。

- **イベント動作時間:** 特定の時間帯（業務/非業務/メンテナンス時間など）にイベントが動作するようにタグを設定してください。タグを設定しない場合、イベントが有効な状態で24時間常時動作します。
 1. **+追加**をクリックしてください。
 2. **イベント動作時間で**+新しいタグを作成****をクリックしてください。
 3. **イベント動作時間タグの作成でタグ名、曜日、時間、色**を選択し、**[適用]** ボタンをクリックしてください。
 4. 作成したタグはタグリストで確認でき、チェックボックスを選択すると適用されます。
 5. 変更または削除するタグの  アイコンをクリックして、**イベント動作時間タグの編集**でタグを編集または削除できます。

 タグを削除すると、そのタグが適用されているすべてのユーザーのタグが削除されます。ただし、イベントルールで使用中のタグは削除できません。

- **イベント受信タグ:** イベントに受信タグを設定すると、そのタグを持つプロジェクトメンバーに通知が送信されます。受信タグを設定しない場合、プロジェクト内のすべてのユーザーに通知が送信されます。
 1. **+タグ追加**または**+**をクリックしてください。
 2. **イベント受信タグウィンドウ下部の**+新しいタグを作成****をクリックしてください。
 3. **タグ作成ウィンドウ**でタグ名を入力し、色を選択してから、**[タグ作成]** ボタンをクリックしてタグを作成してください。
 4. 作成されたタグはタグリストの  アイコンをクリックして編集または削除してください。
 5. **イベント受信タグウィンドウのタグリスト**から目的のタグを選択すると適用されます。

 イベント設定時にイベント受信タグを選択して、そのタグを持つプロジェクトメンバーとサードパーティプラグインに通知を送信できます。**アラート通知 > 通知設定**でプロジェクトメンバーとサードパーティプラグインにそれぞれタグを指定できます。

シミュレーション

通知を保存する前に、過去のデータでシミュレーションして通知発生予測件数を確認できます。

1. 通知設定を完了後、下部の時間範囲を選択してください。
2. [シミュレーション] ボタンをクリックしてください。
3. チャートに時間帯別データと通知発生回数が表示されます。

❗ シミュレーション時間範囲を調整して、さまざまな時間帯の通知発生パターンを確認できます。直近1~2分のデータはインデックスビルド遅延により照会されない場合があります。

4. イベントルール追加ウィンドウで設定が完了したら、[保存] ボタンをクリックしてください。

ログエクスプローラーから通知を作成

ログエクスプローラーから直接通知を作成できます。

1. ログ>ログ検索メニューに移動してください。
2. カテゴリと検索クエリを設定してください。
3. 画面右上の[イベント追加] ボタンをクリックしてください。
4. Drawerで通知設定フォームが開き、現在のカテゴリと検索クエリが自動的に入力されます。
5. 追加設定を完了し、[保存] ボタンをクリックしてください。
6. 保存完了後、[移動] ボタンをクリックすると通知一覧に移動します。

イベントの編集/削除

1. アラート通知>イベント設定の複合ログタブに移動してください。
2. ログイベントリストで編集または削除するイベントの✎アイコンをクリックしてください。
3. イベント設定画面でオプションを変更し、[保存] ボタンをクリックしてください。
 - a. 選択したイベントを削除するには、イベント設定画面の右上の[削除] ボタンをクリックしてください。

イベントの共有

メトリクスイベント設定を JSON ファイルとして保存し、他のユーザーと設定を共有したり、他のユーザーの設定を取り込んだりすることができます。

- JSON ファイル名: `event-rules-YYYYMMDD.json`

エクスポート

1. 画面右上の [JSON ] ボタンをクリックします。
2. JSON 編集画面が表示されたら、[ エクスポート] ボタンをクリックします。
 - イベントを検索した状態でエクスポート機能を使用すると、検索結果のみが JSON ファイルとしてダウンロードされます。
3. JSON ファイルがダウンロードされたら、共有したい他のユーザーに渡してください。

インポート

1. 画面右上の [] ボタンをクリックします。
2. エクスポート 機能でダウンロードした JSON ファイルを選択します。
3. JSON 編集画面が表示されたら、[一覧に追加] または [上書き] を選択します。

 同じ種類の製品間での利用を推奨します。異なる製品のプロジェクトからイベント設定を取り込むことは可能ですが、正常に動作しない場合があります。

JSON 形式で編集する

1. 画面右上の [JSON ] ボタンをクリックします。
2. 編集画面が表示されたら、JSON 形式に従って内容を修正してください。
3. 修正が完了したら、画面下部の [保存] ボタンをクリックします。

❗ 修正した内容が JSON 形式に合っていない場合、画面下部にエラーメッセージが表示され、保存できません。表示されるエラーメッセージは、形式エラーの内容によって異なる場合があります。

JSON error

通知設定

ホーム > プロジェクト選択 >  アラート通知 > 通知設定

ユーザー別アラート受信設定

 **ユーザー別アラート受信設定** における他メンバーの情報は、**メンバー管理** 権限を持つメンバーのみが確認できます。それ以外のメンバーには、必須情報がマスキングされて表示されます。

- イベント通知の一括受信設定およびアクセス設定のためのモバイル端末管理は、**アカウント情報** で行うことができます。
- メンバー権限の詳細については、[こちらのドキュメント](#) を参照してください。

通知手段の設定

メール、**SMS**、**WhatsApp**、**モバイル** による通知を提供します。

ユーザー別アラート受信設定 セクションで、受信したい通知手段のチェックボックスを選択すると警告アラートを受信できます。通知手段のチェックボックスを解除すると、その手段ではアラートは送信されません。

 プロジェクトの最高管理者を除き、すべてのユーザーは自分自身の受信設定のみ変更できます。

メール通知

メール通知は、会員登録時に入力したメールアドレス宛に送信されます。

SMS通知

SMSで通知を受信できます。

 SMS通知機能は、有料プロジェクトでのみ利用できます。

1. 画面右上の **プロフィールアイコン** をクリックし、**アカウント管理** に移動します。
2. **アカウント情報** の **ユーザー電話番号** セクションで、[一般携帯電話] ボタンをクリックします。
3. 認証番号を受信する **電話番号** を入力します。
 - SMS通知を受信できる電話番号は、**韓国の携帯電話番号のみ**対応しています。
4. [保存] ボタンをクリックします。

✔ 登録した電話番号の変更および削除

- 電話番号を変更する場合は、[変更] ボタンをクリックしてください。SMS認証が必要です。
- 電話番号を削除する場合は、[削除] ボタンをクリックしてください。削除後は、SMSによる通知を受信できなくなります。

WhatsApp通知

WhatsAppを通じて通知を受信できます。

ⓘ WhatsApp通知機能は、有料プロジェクトでのみ利用できます。

1. 画面右上の **プロフィールアイコン** をクリックし、**アカウント管理** に移動します。
2. **アカウント情報** の **ユーザー電話番号** セクションで、[WhatsApp] ボタンをクリックします。
3. 認証番号を受信する **電話番号** を入力します。
4. [認証番号送信] ボタンをクリックします。
5. WhatsAppアプリケーションに送信された6桁の認証番号を入力します。
 - 10分以内に認証番号を受信できなかった場合は、[認証番号再送信] ボタンをクリックしてください。
6. [認証] ボタンをクリックします。

モバイル通知

モバイル通知を受信するには、モバイル端末にWhaTapアプリケーションをインストールし、ログインする必要があります。

- WhaTapアプリケーションをダウンロード – [Android](#)
- WhaTapアプリケーションをダウンロード – [iOS](#)

繰り返し通知（エスカレーション）設定

アラート発生後も状況が解消されない場合、初回アラート発生時刻を基準に通知を繰り返す間隔を設定できます。この設定は **Critical** レベルのアラートにのみ適用されます。

例えば、初回アラート発生から即時（0分）、1時間後、1日後に通知を繰り返す場合は、**繰り返し通知（エスカレーション）** カラムに **0,1H,1D** と入力します。

1. **アラート通知 > 通知設定** に移動し、**ユーザー別アラート受信設定** セクションを開きます。
2. **繰り返し通知（エスカレーション）** 項目で設定します。
 - **M**: 分、**H**: 時間、**D**: 日。単位を省略した場合は分単位として扱われます。
 - 数値、または 数値+単位（**M, H, D**）の形式で入力してください。入力形式が正しくない場合はメッセージが表示されます。
3. [保存] ボタンをクリックしてください。保存しない場合、設定は反映されません。

イベント受信タグ

イベント設定時に **イベント受信タグ** を選択すると、そのタグを持つプロジェクトメンバーや 3rd-party プラグインに通知を送信できます。イベント受信タグを設定しない場合、**すべてのプロジェクトメンバー** に警告アラートが送信されます。

イベント受信タグの追加・編集・削除

 イベントに **適用中のイベント受信タグ** は削除できません。

1. **アラート通知 > 通知設定** に移動します。
2. **ユーザー別アラート受信設定** セクションのユーザー一覧で、**+ タグ追加** または **+** をクリックします。
3. **イベント受信タグ** 画面で **+ 新しいタグ作成** をクリックします。
4. **タグ作成** 画面でタグ名を入力し、色を選択して [タグ作成] ボタンをクリックします。

5. 作成されたタグは、タグ一覧の  をクリックして編集または削除できます。
6. イベント受信タグ画面の **タグ一覧** から使用したいタグを選択すると適用されます。

イベント受信タグを解除する

1. アラート通知 > 通知設定 に移動し、**ユーザー別アラート受信設定** セクションを開きます。
2. イベント受信タグを解除したいユーザーの **イベント受信タグ** 項目にある + をクリックします。
3. イベント受信タグ画面で、解除したいタグの X をクリックすると、そのタグが解除されます。

受信タグ未設定のアラートを受信する

イベント設定時にイベント受信タグを選択すると、そのタグを持つプロジェクトメンバーや 3rd-party プラグインに通知を送信できます。

- イベント受信タグが設定されていないアラートを受信するには、**受信タグ未設定のアラートを受信** オプションを有効にしてください。
- イベント受信タグが設定されているアラートのみ受信したい場合は、このオプションを無効にしてください。

❗ すべての警告アラートを受信しない場合は、このオプションを無効にし、**イベント受信タグ** が一つも選択されていない状態にしてください。

イベント受信モードの選択

ユーザー別アラート受信設定 セクションで、メンバーまたはサードパーティチャネルごとにイベント通知の受信範囲を次の3つのモードから選択できます。受信モードは、各メンバーまたはチャネル行の**イベント受信タグ**列で選択します。

Mode	Description
すべての通知を受信	イベント受信タグに関係なく、すべての警告通知を受信
選択したタグのみ通知を受信	選択したイベント受信タグを持つ警告通知のみ受信。タグを最低1つ以上選択
すべての通知を受信しない	いかなるイベント通知も受信しない。選択したタグは削除されずそのまま保存

- 選択したタグのみ通知を受信モードでは、タグ選択領域で通知を受信するタグを1つ以上選択してください。
- イベント受信タグが指定されていない警告通知まで受信するには、タグ選択領域で**未分類仮想タグ**を選択してください。**未分類タグ**は通常のタグと同様に選択または解除でき、タグ自体を編集・削除することはできません。

❗ すべての通知を受信しないモードでは、該当メンバーまたはチャネルがイベント通知をまったく受信しません。このとき選択したタグは削除されず保存されるため、再び**選択したタグのみ通知を受信モード**に切り替えると、以前に選択したタグ設定をそのまま使用できます。

通知受信言語の選択

ユーザーが受信するアラート通知の言語を選択できます。

1. アラート通知 > 通知設定 に移動します。
2. ユーザー別アラート受信設定 セクションのユーザー一覧で、言語を設定したいユーザーの一番左にある ► ボタンをクリックします。
3. 通知受信言語 を選択します。

曜日・時間別通知設定

ユーザーごとに、曜日および時間帯別の通知受信可否を設定できます。

1. アラート通知 > 通知設定 に移動します。
2. ユーザー別アラート受信設定 セクションのユーザー一覧で、曜日・時間別通知を設定したいユーザーの一番左にある ► ボタンをクリックします。
3. 警告アラートを受信したい曜日を選択するか、時間帯を入力します。
 - 通知手段ごとに設定できます。

サードパーティプラグイン

外部アプリケーションを通じて警告アラートを受信できます。

- 対応アプリケーション: Slack、Telegram、Teams、Teams Workflows、Jandi、AlertNow、Webhook、Webhook

JSON、Opsgenie、PagerDuty、LINE、ilert

❗ WhaTap のサポート範囲に含まれない社内メッセンジャーは、標準の **Webhook** または **Webhook JSON** を使用して連携できます。

表 | サードパーティプラグイン一覧

項目	説明
プラグイン名	プラグインの名称
認証キー	認証キー
認証値	認証値
受信レベル	警告、全体、危険のいずれか
繰り返し通知（エスカレーション）	問題が解消されない場合、初回通知時刻から再通知する間隔 - Critical レベルのアラートにのみ適用
Smart メッセージ（AI）	Telegram プラグイン追加時に AI 通知機能を提供 - 対応言語：韓国語、英語、日本語
イベント受信タグ	プロジェクト内の特定メンバーまたはチームに対する通知受信設定
削除	サードパーティプラグインの削除

サードパーティプラグインの追加

1. アラート通知 > 通知設定 に移動します。
2. サードパーティプラグイン セクションで **追加** ボタンをクリックします。
3. サードパーティプラグイン追加 画面で、使用するサービスのタブを選択します。
4. 選択したサービスの案内（[サードパーティプラグイン通知の追加方法](#)）に従って設定します。
5. 受信テスト ボタンをクリックして設定を確認します。

- すべて完了したら **追加** または **登録** ボタンをクリックします。

サードパーティプラグイン通知の追加方法

Slack

- サードパーティプラグイン追加 画面の **Slack** タブで、[**Slackに登録**] ボタンをクリックすると、Slack のチームおよびチャンネルに **WhaTapNotiBot** を登録できます。

Telegram

- Telegramで @WhaTapApmNotiBot を検索してください。

- ボットを選択し、[開始] ボタンをクリックします。
- チャット画面に `/license` コマンドと、通知を受信したいプロジェクトのアクセスキーを入力してください。



① 使用可能なコマンド一覧

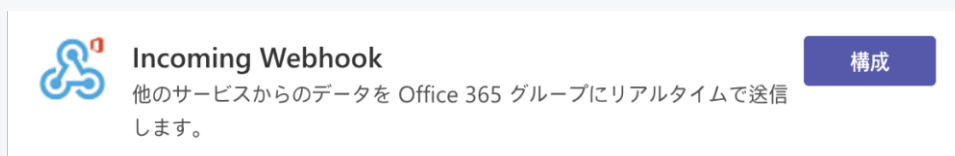
- `/help` : コマンド一覧を表示
- `/license` : 通知を受信するプロジェクトのアクセスキーを入力
- `/remove` : 通知を受信しないプロジェクトコードを入力
- `/list` : 現在通知を受信しているプロジェクトコードを表示

Teams

- 通知を受信したいチャンネルの **コネクタ** に移動します。



2. Webhook を追加し、[構成] ボタンをクリックします。



3. Webhook 名を入力し、[作成] ボタンをクリックします。



Incoming Webhook

フィードバックの送信

Incoming Webhook コネクタを利用すると、トラッキング対象の活動についての通知を外部サービスから受け取ることができます。このコネクタを使うには、別サービスで設定を作成する必要があります。そのサービスが、Office 365 コネクタ形式 対応の Web フックをサポートしている必要があります。

* が付いているフィールドは必須です

着信 Web フック (Incoming Webhook) をセットアップするには、名前を入力して [作成] を選んでください。*

この着信 Web フック (Incoming Webhook) からのデータに関連付ける画像をカスタマイズします。

イメージをアップロードします。



既定のイメージ

作成

キャンセル

4. 生成された Webhook URL をコピーします。

以下の URL をコピーしてクリップボードに保存してから、[保存] を選んでください。この URL は、グループへのデータ送信元となるサービスの画面で必要になります。

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



URL は最新です。

完了

削除

5. WhaTap モニタリングサービスの サードパーティプラグインの追加 画面に戻り、Teams タブ下部の Channel Name と Webhook URL に値を入力します。

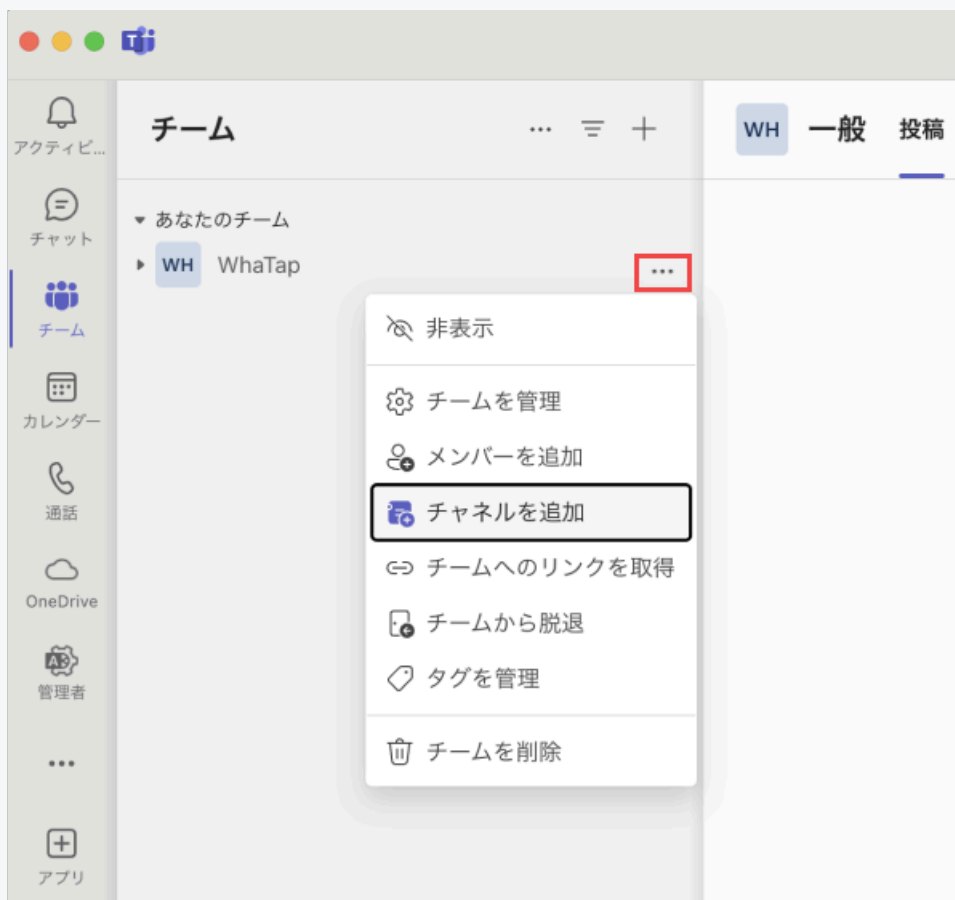
6. [登録] ボタンをクリックします。



Teams Workflows

- ① ワークフローを使用するには、**Microsoft Teams** にアクセス可能なアカウントと **ビジネスプランのサブスクリプション**が必要です。

1. チーム メニューの **その他の操作 (...)** > **チャンネルを追加** をクリックします。



2. チャンネルの作成 画面で **チャンネル名** と **説明** を入力します。チャンネルの種類 は **標準** を選択し、[作成] ボタンをクリックします。



チャンネルの作成

チャンネル名 *

WhaTapのイベントチャンネル

説明

他のユーザーが、適切なチャンネルを見つけられるように説明を入力します

チャンネルの種類を選択する * ⓘ

選択

☒ 標準
チームの全員がアクセスできます。

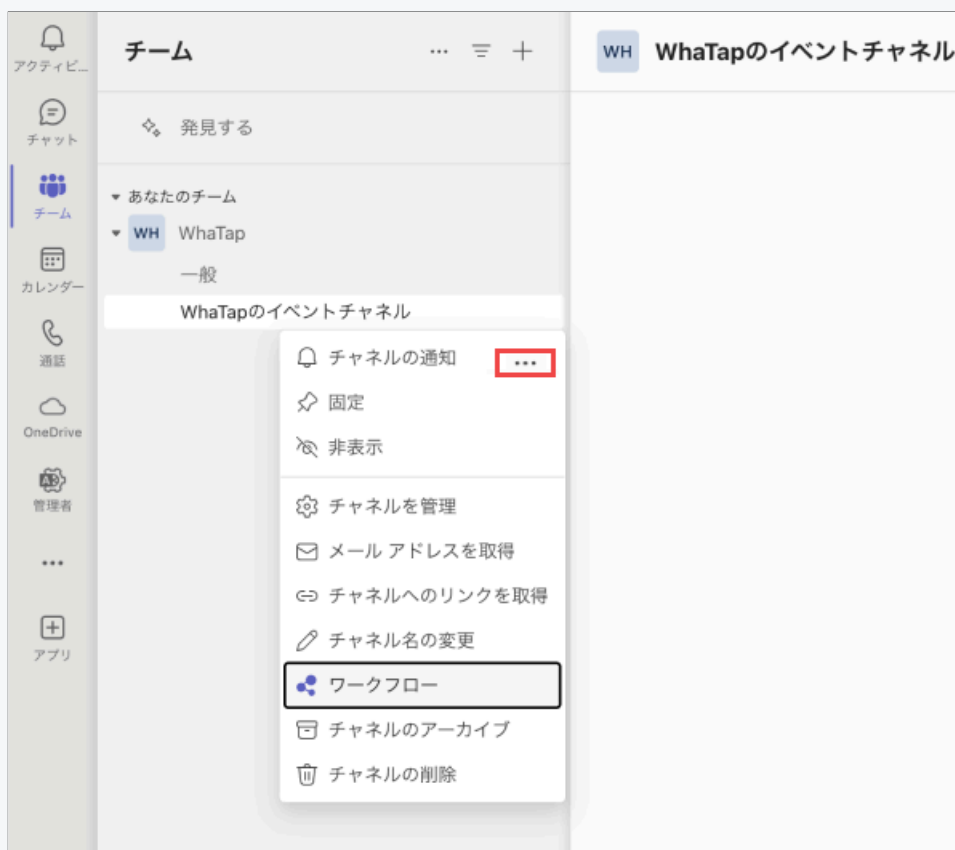
☐ 共有
組織内または組織外の人またはチームがアクセスできます。

☐ プライベート
チームの特定のユーザーがアクセスできます。

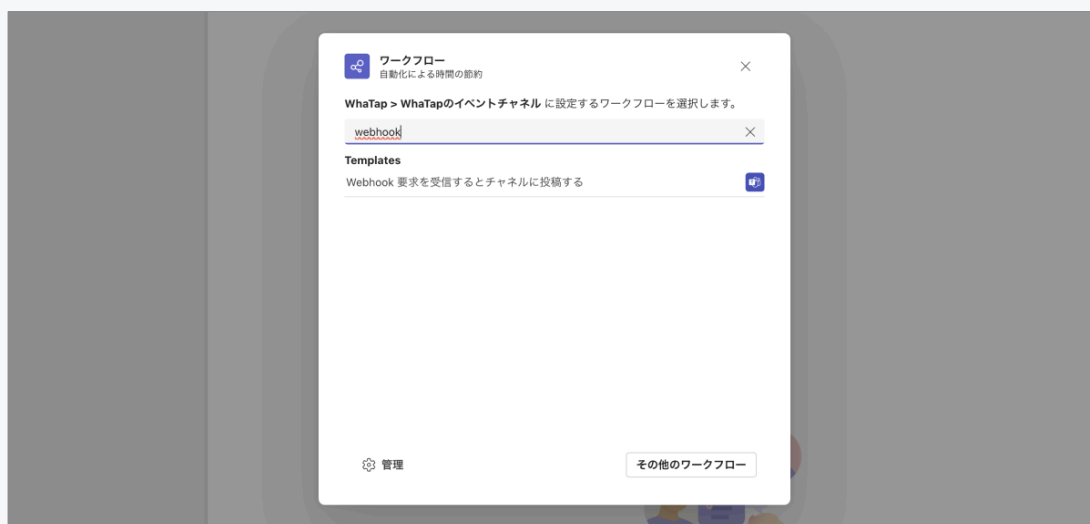
キャンセル 作成

❗ チャンネルの種類を **共有** にするとワークフローは使用できません。**プライベート** を選択した場合、ワークフローは追加できますが通知は受信できません。

- 作成したチャンネルの **その他の操作 (...)** > **ワークフロー** をクリックします。



4. ワークフロー ダイアログの一覧から Webhook 要求を受信したらチャンネルに投稿 を選択し、[ワークフローを追加] ボタンをクリックします。



5. 名前と接続の状態を確認し、[次へ] ボタンをクリックします。
6. 詳細を確認後、[ワークフローを追加] ボタンをクリックします。
7. ワークフローが追加されました。生成された URL をコピーします。



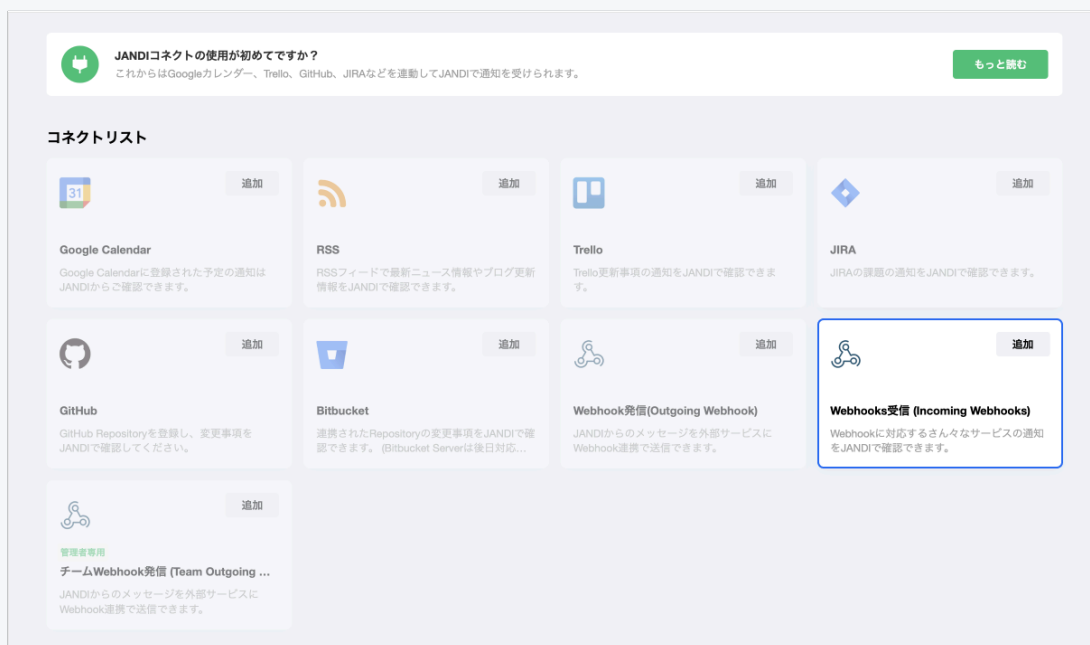
8. WhaTap モニタリングサービスの **サードパーティプラグインの追加** 画面に戻り、**Teams Workflows** タブ下部の **Channel Name** と **Webhook URL** に値を入力します。
9. [登録] ボタンをクリックします。

Jandi





1. 通知を受信するトピックまたはチャットで、**Jandi Connect 設定** に移動します。
2. **コネクト一覧** から **Webhook 受信 (Incoming Webhook)** を選択し、[連携する] ボタンをクリックします。



3. [**Webhook 受信を追加**] ボタンをクリックします。
4. **Webhook URL 登録** 項目に表示される Webhook URL をコピーします。



5. WhaTap モニタリングサービスの **サードパーティプラグインの追加** 画面に戻り、**Jandi** タブ下部の **Channel Name** と **Webhook URL** に値を入力します。
6. [**登録**] ボタンをクリックします。



1. AlertNow サービスにアクセスし、設定 > Integration メニューに移動します。



2. Integration 画面で [Integration 作成] ボタンをクリックします。
3. Integration タイプの中から **WhaTap** を選択します。
4. Integration 作成 画面で、名前 および 命名規則 を設定します。

5. [確認] ボタンをクリックすると、Integration が作成されます。
6. 作成された Integration の一覧を確認し、該当する Integration を選択します。



インテグレーション

インテグレーションの作成 検索語を入力 最後のアップデート: 2024-02-21 11:25:10

統合名	統合タイプ	統合キー	サービス名
ワットテスト	ワタップ		ワットテスト

7. 詳細画面で、URL 右側のコピーアイコンをクリックして URL をコピーします。

← **インテグレーション**

ワットテスト

基本情報

統合タイプ	ワタップ
統合キー	fda527a5140
URL	https://alertnowitgr.opsnow.com/integration/whatap/v1/
コンストラクタ	リサ

クリップボードにコピーする

8. Whatap モニタリングサービスの **サードパーティプラグインの追加** 画面に戻り、AlertNow タブ下部の **Channel Name** と **Webhook URL** に値を入力します。
9. [登録] ボタンをクリックします。

Webhook



1. 通知を受信する Webhook を登録します。登録した URL に対して、通知の **title** と **text** が POST メソッドで送信されます。

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

2. **Webhook Name** と **Webhook URL** の項目を入力します。
3. [登録] ボタンをクリックします。

Webhook JSON



1. 通知を受信する Webhook を登録します。登録した URL に対して、通知データが **JSON 形式**で **POST** メソッドにより送信されます。JSON に含めることができる置換変数については、**使用可能な変数**を参照してください。

- `${something}` は WhaTap が提供する置換値を表します。対応する全一覧と意味については、**使用可能な変数**を参照してください。
- イベント状態（`status`）は、**イベント発生**（`on`）と**イベント解消**（`off`）に区別されます。
- `level` は `None`、`Info`、`Warning`、`Critical` に区別されます。

```
{
  "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}"
}
```

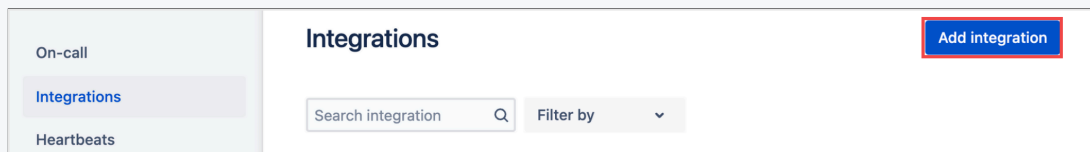
2. **Webhook Name** と **Webhook URL** の項目を入力してください。
3. ヘッダー値を追加するには、**ユーザーヘッダー値の追加** の + 追加 をクリックし、key と value を入力してください。
4. [登録] ボタンをクリックしてください。

Opsgenie

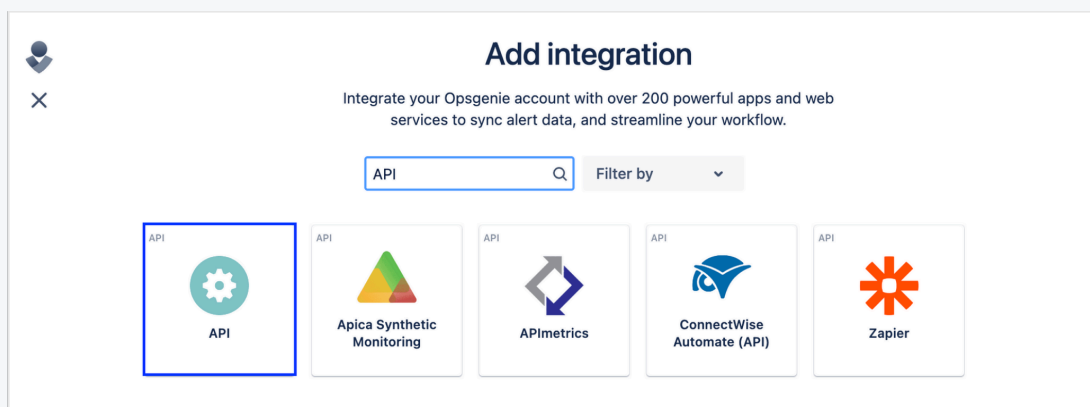




1. **Teams** メニューで、アラートを受信するチームを選択してください。
2. **Integration** メニューに移動し、[Add Integration] ボタンをクリックしてください。



3. インテグレーション一覧で **API** を検索し、選択してください。



4. API 名を設定し、チームを割り当て、各権限を設定した後、[Save Integration] ボタンをクリックしてください。



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: ☐

[Save Integration](#) [Cancel](#)

5. Whatap モニタリングサービスの **サードパーティプラグインの追加** 画面に戻り、Opsgenie タブ下部の **Name** と **API Key** を入力してください。
6. [登録] ボタンをクリックしてください。



PagerDuty



1. [PagerDuty](#) アカウントを登録し、ログインしてください。
2. PagerDuty で **Services > Service Directory** メニューに移動し、[+ New Service] ボタンをクリックしてください。
3. サービス情報 (Name) を入力し、[Next] ボタンをクリックしてください。
4. **Escalation Policy** を設定し、[Next] ボタンをクリックしてください。



PagerDuty

5. **Alert Grouping** と **Transient Alerts** を設定し、[Next] ボタンをクリックしてください。

PagerDuty

6. **Integrations** で **Event API V2** を選択し、[Create Service] ボタンをクリックしてください。

PagerDuty

7. 作成されたサービス画面で **Integration Name** と **Integration Key** の値をコピーしてください。

PagerDuty

8. WhaTap モニタリングサービスの **サードパーティプラグインの追加** 画面に戻り、**Integration Name** と **Integration Key** を入力してください。
9. [登録] ボタンをクリックしてください。

❗ メッセージを受信できない、またはプラグインが登録されない場合は、**Integration Name** または **Integration Key** の値が正しいか確認してください。

LINE



1. LINE アプリをインストールしてください。
2. 以下の QR コードをスキャンして、**WhaTapLabs** 公式チャンネルを友だち追加してください。

LINE 3rd パーティプラグイン追加

3. 次のコマンドを使用して、プロジェクトを LINE と連携し、通知を設定してください。

コマンド

```
/help # 使用可能なコマンド一覧を表示
/list # 連携されているプロジェクト一覧を表示
/license [アクセスキー] # 新しいプロジェクト連携を追加
```



```
/remove [プロジェクトコード] # プロジェクト連携を解除
/language [ko|ja|en] # 通知言語を設定（韓国語／日本語／英語）
```

- プロジェクトのアクセスキーは **管理 > プロジェクト管理** で確認できます。
- LINE 内で `/language` コマンドを使用した場合、その設定は **該当する LINE チャットルーム内のみ** に適用されます。他の 3rd パーティプラグインやプロジェクトの通知言語は変更されません。

使用例

```
/license XXXXXXXXXX # プロジェクトを連携
/language ko # 言語を韓国語に設定
/list # 連携済みプロジェクトを確認
```



- **プロジェクトアクセスキー**: WhaTap プロジェクト内の **管理 > プロジェクト管理** で確認できます。
- **言語設定**: `/language` コマンドは LINE チャットルーム内でのみ有効で、他の通知チャンネルの言語は変更されません。

ilert



1. ilert コンソールの **Alert sources** 画面右上にある [+ Create alert source] をクリックします。
2. **Integration type** ステップ下部の **Filter integrations** 検索欄に `WhaTap` を入力して検索します。
3. 検索結果から **WhaTap** タイルを選択し、[Next] ボタンをクリックします。
4. アラートソース名を入力し、チームを指定した後、[Next] ボタンをクリックします。
 - エスカレーションポリシーは、新規作成または既存のものを選択できます。
5. アラートのグループ化方式を選択し、[Continue setup] ボタンをクリックします。
 - 最初に選択した **Do not group alerts** は後から変更可能です。
6. 次の画面で **アラートテンプレートや優先度などの追加設定** を行うことができます。ここでは [



Finish setup] ボタンをクリックして設定を完了します。

7. 設定が完了すると、完了画面で **API キー** または **Webhook URL** が生成されます。
8. **Webhook JSON** タブで生成された **Webhook URL** をコピーし、下部の **Webhook URL** 入力欄に貼り付けます。
9. [登録] ボタンをクリックします。

大量アラート発生の防止

短時間に大量のアラートが発生した場合、指定した時間だけアラート通知を一時的に停止します。たとえば、5 分間に 20 件のイベントが発生すると、その後 5 分間は警告アラートが送信されません。設定した **停止時間** が経過すると、大量アラート防止機能は自動的に解除されます。

1. 次の画面に移動してください。 **アラート通知 > 通知設定 > 大量アラート通知発生防止** セクション
2. トグルボタンをクリックして **有効化** または **無効化** します。
 -  **有効**: 大量アラートを検知した場合、一時的に通知を停止
 -  **無効**: アラート通知を再開
3. **検知時間**, **検知回数**, **停止時間** を設定してください。
 - **検知時間** 内に **検知回数** 以上のイベントが発生すると、**停止時間** の間、警告アラートが停止されます。



大量アラートによってブロックされた場合、ブロック案内ボックスが表示されます。大量アラート防止機能をすぐに解除するには、ボックス内の **大量アラート発生中止** ボタンをクリックしてください。

イベント通知フォーマット

共通アラートテンプレート

共通テンプレートは、ほとんどのケースで適用できます。さまざまな環境において、同一のフォーマットでアラートを受信できます。

- プロダクトタイプ: アプリケーション、データベース、Kubernetes
- イベントタイプ: アプリケーションアラート、データベースアラート、メトリクスアラート
- イベントチャンネル: SMS、Mobile、3rd-party プラグイン、プラグイン

イベントタイトル

Event title format

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

Event title example

```
[Info][JAVA][アプリケーションプロジェクト][TC-0-1-8081][CRITICAL_HIGH_MEMORY]
```

❗ ApplicationName が設定されていない場合、イベントタイトルから省略されます。

- Platform は以下のいずれかで表示されます。
 - 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

イベントメッセージ

イベントメッセージに含めることができる情報です。 `optional` が `false` の場合、常にメッセージに含まれます。
`optional` が `true` の場合、該当データが確認できるときのみ表示されます。

イベントメッセージ例

```
Project Name : アプリケーションプロジェクト  
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

表 | イベントメッセージ構成要素

En	Ko	対応するアラートタイプ	説明
Project Name	プロジェクト名	全て	-
Project Code	プロジェクトコード	全て	-
Agent Name	エージェント名	全て (optional)	oname
Message	イベントメッセージ	全て	-
Alert Type	イベント種別	全て	下記の AlertType 表を参照
Event Time	イベント発生時間	全て	2022-04-13 10:40:49 +0900 の +0900 は GMT オフセット
Event Off Time	イベント解除時間	全て (optional)	2022-04-13 10:40:49 +0900 の +0900 は GMT オフセット
Metric Name	メトリクス名	全て (optional)	イベント条件判定に使用されるメトリクス名
Metric Value	メトリクス値	全て (optional)	メトリクス値が閾値を超えた場合に含まれる
Metric Threshold	メトリクス閾値	全て (optional)	メトリクス条件の閾値

En	Ko	対応するアラートタイプ	説明
Stateful	復旧イベント通知	全て (optional)	復旧通知が有効な場合 <code>true</code> 、それ以外は <code>false</code>
Event Rule	イベント発生条件	メトリクスアラート	-
Target Filter	イベント対象選択	メトリクスアラート	特定対象から収集されたメトリクスのみ評価
Repeat Count	イベント繰り返し回数	メトリクスアラート	繰り返し時間内に指定回数条件を満たすと発生
Repeat Duration	イベント繰り返し時間	メトリクスアラート	繰り返し回数を評価する時間
Receiver	受信者	メトリクスアラート	-
Query	MXQL クエリ	複合メトリクスアラート	-
Rule	イベント発生条件	複合メトリクスアラート	-
Query Period	クエリ期間	複合メトリクスアラート	-
Query Interval	クエリ間隔	複合メトリクスアラート	-
Silent Time	サイレント時間	複合メトリクスアラート	-
Query	URL	Exception アラート	例外を発生させたリクエストの URL
TXID	トランザクション ID	Exception アラート	-

En	Ko	対応するアラートタイプ	説明
Class	エラークラス名	Exception アラート	-
Log Message	ログメッセージ	サーバーファイル ログアラート	-
Log File	ログファイルパス	サーバーファイル ログアラート	-
IP	IP	サーバーアラート全 体	-
CPU	CPU	サーバーアラート全 体	イベント発生時のスナップショット
CPU_load1	CPU_load1	サーバーアラート全 体	イベント発生時のスナップショット
CPU_loadPerCore	CPU_loadPerCore	サーバーアラート全 体	イベント発生時のスナップショット
Memory	メモリ	サーバーアラート全 体	イベント発生時のスナップショット
Swap	スワップ	サーバーアラート全 体	イベント発生時のスナップショット
Disk Name Used Percent Free Size IO Percent	ディスクパフォー マンス	サーバーアラート全 体	イベント発生時のスナップショット
Name Bps Pps	トラフィックパフ ォーマンス	サーバーアラート全 体	イベント発生時のスナップショット
Message Time Name	処理履歴メッセー ジ	サーバーアラート全 体	-

❗ このセクションでは、該当するイベントで提供可能な情報を最大限に表示します。

- **AlertType** は以下のいずれかの値で表示されます。

AlertType	説明
APPLICATION_CPU	アプリケーション CPU アラート
APPLICATION_MEMORY	アプリケーション メモリアラート
APPLICATION_DISK	アプリケーション ディスクアラート
APPLICATION_ACTIVE_TRANSACTION	アプリケーション アクティブTXアラート
APPLICATION_ERROR_TRANSACTION	アプリケーション エラートランザクションアラート
APPLICATION_SLOW_TRANSACTION	アプリケーション トランザクション応答時間アラート
METRICS	メトリクスアラート
COMPOSITE_METRICS	複合メトリクスアラート
ANOMALY	異常値アラート
LOG_REALTIME	リアルタイムログアラート
COMPOSITE_LOG	複合ログアラート
SERVER_REBOOT	サーバー 再起動アラート
SERVER_NO_DATA	サーバー データ未受信アラート
SERVER_PORT	サーバー ポートアラート
SERVER_NETWORK_IOPS	サーバー ネットワーク IOPS アラート
SERVER_NETWORK_BPS	サーバー ネットワーク BPS アラート



AlertType	説明
SERVER_DISK_IO	サーバー ディスク I/O アラート
SERVER_DISK_QUOTA	サーバー ディスク使用量アラート
SERVER_DISK_INODE	サーバー inode アラート
SERVER_CPU	サーバー CPU アラート
SERVER_MEMORY	サーバー メモリアラート
SERVER_CPU_STEAL	サーバー CPU steal アラート
SERVER_MEMORY_SWAP	サーバー スワップメモリアラート
SERVER_LOG_FILE	サーバー ログファイルアラート
SERVER_WINDOW_EVENT	サーバー Windows イベントアラート
SERVER_OFF	サーバー アラート OFF 通知
SERVER_ACKNOWLEDGE	サーバー 処理確認通知
SERVER_PROCESS_COUNT	サーバー プロセス数アラート
SERVER_PROCESS_CPU	サーバー プロセス CPU アラート
SERVER_PROCESS_MEMORY	サーバー プロセス メモリアラート
SERVER_PROCESS_OFF	サーバー プロセスアラート OFF 通知
AGENT_ACTIVE	エージェント 有効化アラート
AGENT_INACTIVE	エージェント 無効化アラート



AlertType	説明
AGENT_REACTIVATED	エージェント 再有効化アラート
URL	URL アラート
TOO_MANY_EVENT	イベント多発アラート
CLOUD_WATCH	CloudWatch アラート
EXCEPTION	例外アラート

イベント履歴

ホーム > プロジェクト選択 >  アラート通知 > イベント履歴

イベント履歴では、プロジェクトで発生したさまざまなイベントを確認し、詳細情報を分析できます。Elasticsearch DSL クエリをサポートしており、指定した条件に一致するイベントを迅速かつ正確に検索できます。

イベント履歴の確認

検索結果でイベントタイトルをクリックすると、そのイベントが発生した時間帯の詳細データを分析できる画面に移動します。これにより、イベント発生前後の状況を総合的に把握できます。

1. アラート通知 > イベント履歴 に移動してください。
2. イベント履歴 画面の 時間選択 で、イベント履歴を確認する期間を設定してください。
3. フィルター入力欄にクエリを入力し、[虫眼鏡] ボタンをクリックしてください。
 - クエリを入力しない場合、すべてのイベントが表示されます。

カラム設定

表示するカラムや非表示にするカラムを設定できます。

1. イベント履歴 画面の左上にある [ カラム設定] ボタンをクリックしてください。
2. カラム設定 画面で、表示または非表示にするカラムを選択してください。
 - 表示項目 でカラムの順序を変更できます。
 - カラム名検索 欄で目的のカラムを検索できます。

カラム項目	説明
イベント名	イベントのタイトル
メッセージ	イベントのメッセージまたはスナップショット情報

カラム項目	説明
イベント状態	イベントの現在の状態
エージェント名	イベントが発生した対象エージェントの名前 (Oname) - 特定のエージェントに紐づかないイベントの場合は空欄で表示されます
エージェントグループ	イベントが発生した対象エージェントの種類 (OkindName) - 特定のエージェントに紐づかないイベントの場合は空欄で表示されます
エージェントノード	イベントが発生した対象エージェントのサーバー (OnodeName) - 特定のエージェントに紐づかないイベントの場合は空欄で表示されます
イベント発生時刻	イベントが発生した時刻
イベント解消時刻	イベントが解消された時刻 - 解消状態を持たないイベントの場合は - と表示されます

3. 設定が完了したら、[確認] ボタンをクリックしてカラム設定を反映してください。

↓ CSV ダウンロード

検索結果を CSV ファイル形式でダウンロードできます。

1. アラート通知 > イベント履歴 で [CSV] ボタンをクリックしてください。
2. 現在のフィルター条件に一致するイベント一覧が CSV ファイルとして保存されます。

進行中のイベントのみ表示

現在進行中の状態のイベントのみを表示できます。

1. アラート通知 > イベント履歴 で [進行中のイベントのみ表示] ボタンをクリックしてください。
2. フィルタークエリに次の条件が自動的に追加され、検索が実行されます。

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

イベント検索

- **正確な検索:** 必要なイベントだけを取得できるよう、条件を正確に指定
- **複合条件:** 複数のフィールドを同時に検索し、複雑な条件も一度に処理
- **柔軟なパターン:** ワイルドカードや部分一致など、さまざまな検索方式をサポート
- **高速パフォーマンス:** インデックス化されたデータを活用した高速検索

検索可能なフィールド

フィールド名および値は大文字と小文字を区別しません。

- **フィールド名タグ:** フィールドがサポートされるイベントタイプ
- **フィールドタイプ:** フィールドのデータ型
 -  #: Number
 -  T: String
 -  C: Boolean
 -  D: Date

イベント情報フィールド

フィールド名	タイプ	説明	例
Title	String	イベントタイトル	"Database Connection Error"
OffTitle	String	イベント解消タイトル	"RECOVERED: Database Connection Error"
Message	String	イベントメッセージ	"Connection timeout occurred"
OffMessage	String	イベント解消メッセージ	"RECOVERED: Connection timeout occurred"

フィールド名	タイプ	説明	例
Level	String	現在のイベントレベル	Critical, Warning, Info
OriginLevel	String	元のイベントレベル	Critical, Warning, Info
Status	String	イベント状態	ON, OFF, CANCEL, ACKNOWLEDGE, MAINTENANCE, DISABLED
ActCount	Number	発生回数	2
MetricName	String	指標名	"memory"
MetricValue	String	指標値	"85.5"
OffValue	String	解消時の値	"72.8"
MetricThreshold	String	閾値	"80"
alertType	String	イベント種別	"BASIC", "METRICS", "TRANSACTION" など
alertId	String	イベントルールの一意識別子	"zf3uojer0fv4v7"

イベントタイプ別対応フィールド

ⓘ 特定のイベントタイプでのみサポートされるフィールドです。該当しないイベントタイプの場合、値が存在しないことがあります。

フィールド名	タイプ	イベント種別	説明	例
eventRule	String	基本、メト	イベント発生	"memory ≥ 80"

フィールド名	タイプ	イベント種別	説明	例
		リクス	ルール	
field	String	リアルタイムログ	ログ検索キー	"content"
keyword	String	リアルタイムログ	ログ検索値	"Error"
logCategory	String	リアルタイムログ	ログカテゴリ	"AppLog"
logContent	String	リアルタイムログ	ログ内容	"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."

対象フィールド

フィールド名	タイプ	説明	例
Oid	Number	エージェントの一意識別子	-98765432
Oname	String	エージェント名	"web-server-01"
Okind	Number	エージェント種別の一意識別子	867318026

フィールド名	タイプ	説明	例
OkindName	String	エージェント種別名	"web-server"
Onode	Number	エージェントノードの一意識別子	334634079
OnodeName	String	エージェントノード名	"production-node-1"

イベント固有値フィールド

フィールド名	タイプ	説明	例
Id	Number	イベントの一意識別子	5768121
UUID	String	イベント固有識別子	"550e8400-e29b-41d4-a716"

状態／フラグフィールド

フィールド名	タイプ	説明	例
Stateful	Boolean	状態ベースイベントかどうか	true, false
Disabled	Boolean	無効化されたイベントかどうか	true, false
Escalation	Boolean	エスカレーション有無	true, false
SystemEvent	Boolean	システムイベントかどうか	true, false

検索タイプ別クエリ構文

① 検索の基本構文については、[WhaTap ログ検索クエリ構文](#) ドキュメントを参照してください。

1. キーワード検索

「Database Connection」という文字列を含むイベント

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

2. 複数値検索

指定した複数の値のうち、いずれかを含むイベントを検索します。

```
title: Database Connection
```

現在のイベントレベルが Info または Warning のイベント

```
level: info warning
```

3. パターン検索

ワイルドカードを使用してパターン検索ができます。

名前パターンで特定のエージェントで発生したイベントを検索

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

タイトルが Connection で終わるイベントを検索

```
title: *Connection
```

4. 複合条件検索

複数の条件を組み合わせて、より正確に検索できます。

レベルが Critical で、タイトルに Database を含むイベント

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

特定のエージェントにおける Warning または Critical のイベント


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

5. OR 条件検索

複数の条件のうち、**いずれか一つでも満たす**イベントを検索します。

タイトルまたはメッセージに特定のキーワードを含むイベント

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

6. 除外条件

特定の条件を除外して検索できます。

Info レベルを除いたすべてのイベント

```
not level: info
```

リアルタイムアラート

リアルタイムアラート機能は、イベント設定で設定したイベントが発生した際に、ポップアップ形式で表示されます。イベント発生と同時に通知を受け取ることで、問題を迅速に把握し、対応することができます。また、すでに発生した通知や見逃した通知の履歴を確認することで、リアルタイム対応が難しかった状況を把握し、解決に役立てることができます。

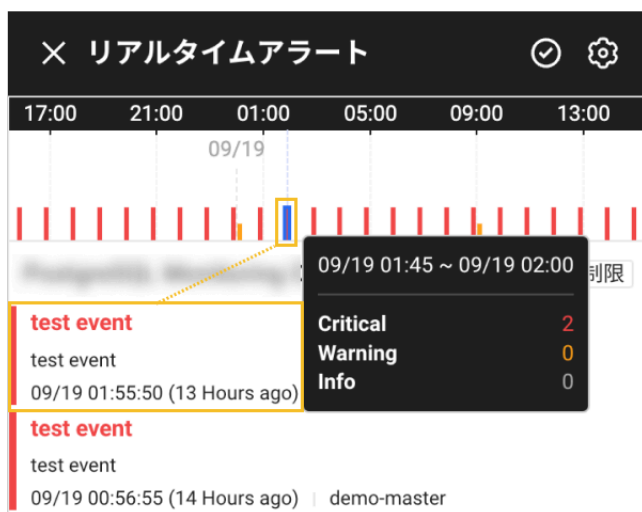
リアルタイムアラートを確認する

リアルタイムアラートは、画面右上にポップアップとして表示されます。通知が発生した時刻、タイトル、メッセージを確認できます。

- 個別の通知を閉じるには、メッセージ右上の ✕ ボタンをクリックしてください。
- 画面に表示されているすべてのポップアップ通知を閉じるには、**すべての通知を閉じる** をクリックしてください。

通知履歴を確認する

1. プロジェクトを選択して表示される画面の最上部にある 🔔 をクリックしてください。
2. リアルタイムアラート ウィンドウが表示されます。
 - 現在のプロジェクトについて、直近24時間以内の通知を最大100件まで確認できます。
 - 個別のイベント項目を選択すると、関連するメニューに移動します。
 - リアルタイムアラート ウィンドウ内の時間別チャートで任意の時間帯を選択すると、該当するイベント項目に移動します。



- すべての通知履歴を確認するには、**全体の通知履歴** ボタンをクリックしてください。**アラート通知 > イベント履歴** メニューに移動します。

❗ リアルタイムアラート の一覧が空の場合、**全体の通知履歴** ボタンが表示されます。受信タグ未設定の通知を受け取る オプションを無効にしてください。

イベントを一括で解消する

リアルタイムアラート の一覧から、進行中のすべてのイベントを一括で解消できます。

イベント解消が完了するまでに、約30秒～1分程度かかる場合があります。

- イベント一括処理** 機能を使用すると、現在進行中のイベントに対する解消通知が大量に発生する可能性があります。
- イベント一括処理** 機能を使用した後でも、イベントルールが有効であり、データが引き続きしきい値を超えている場合、イベントは再度発生することがあります。
- イベント解消通知は、**アラート通知 > イベント設定** メニューでイベントを編集し、**イベントが解消されたときに追加通知** または **解消通知** オプションを無効にすることで停止できます。

使用方法:

1. プロジェクトを選択して表示される画面上部の  をクリックします。
2. リアルタイムアラート ウィンドウが表示されたら、右上の  をクリックします。
3. リアルタイムアラートリストの進行中イベントを一括で解消します。 というメッセージが表示されたら、解消 ボタンをクリックします。

リアルタイムアラートを設定する

1. プロジェクトを選択して表示される画面上部の  をクリックします。
2. リアルタイムアラート ウィンドウが表示されたら、右上の  をクリックします。
3. リアルタイムアラート設定画面で各項目を設定します。
 - ポップアップ通知: リアルタイムアラート ウィンドウが閉じている状態でも、ポップアップ形式で通知を表示します。
 - 解消済みイベントを表示: リアルタイムアラート 一覧に解消済みイベントも含めて表示します。
 - 通知音の試聴: ブラウザで再生される通知音を事前に確認できます。Critical または Warning の横にある  をクリックしてください。音が再生されない場合は、ブラウザの設定をご確認ください。

システムイベント

WhaTap モニタリングは、プラットフォーム全体で自動的に検知・生成される共通イベントを提供します。本ドキュメントでは、システムによって発生するイベントの種類、発生条件、および対応方法について説明します。

EVENT_BLOCKED_BY_SYSTEM

プロジェクト内で短時間に過剰な数のイベントが発生した場合、WhaTap システムがこれを検知し、イベントの発生を一時的にブロックします。イベントがブロックされると、システムは次のメッセージをユーザーに通知します。このイベントが発生した場合は、イベント設定内容を確認し、必要に応じて調整してください。

 **Critical**



イベントメッセージ

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

プロジェクト番号	8
プロジェクト名	new server
対象	server agent
イベント名	EVENT_BLOCKED_BY_SYSTEM
イベント日時	(GMT+0900) 2024-11-18 18:03:18

WhaTapにログイン

new serverプロジェクトのserver agentから過度なイベントが検知されたため、イベント発生が遮断されます。server agentから一定期間の間にイベントが発生しなくなると、遮断が自動で解除されます。

ブロック基準

イベントは次の基準に基づいてブロックされます。

1. エージェント単位のブロック

1つのエージェントで **1分以内に10件** のイベントが発生した場合、そのエージェントから発生する以降のイベントはブロックされます。

2. 複数エージェントによる全体ブロック

条件 **1** によりイベントがブロックされたエージェントが **1分以内に3件以上** 発生した場合、プロジェクト全体のイベントがブロックされます。

3. プロジェクト単位のブロック

1つのプロジェクトで **1分以内に100件** のイベントが発生した場合、プロジェクト全体のイベントがブロックされます。

ブロック解除方法

システムによってイベントがブロックされた場合、対象のエージェントまたはプロジェクトで **1分間** イベントが発生しない状態を維持する必要があります。

- **アラート通知 > イベント設定** メニューから設定されているすべてのイベントを無効化してください。**イベント設定** を見直し、過剰なイベントが発生しないように閾値を調整する必要があります。
- イベントを設定する前に、**シミュレーション** 機能を活用してイベント発生回数を事前に予測できます。