

SingleStore Monitoring

release date. 2026. 09. 11.

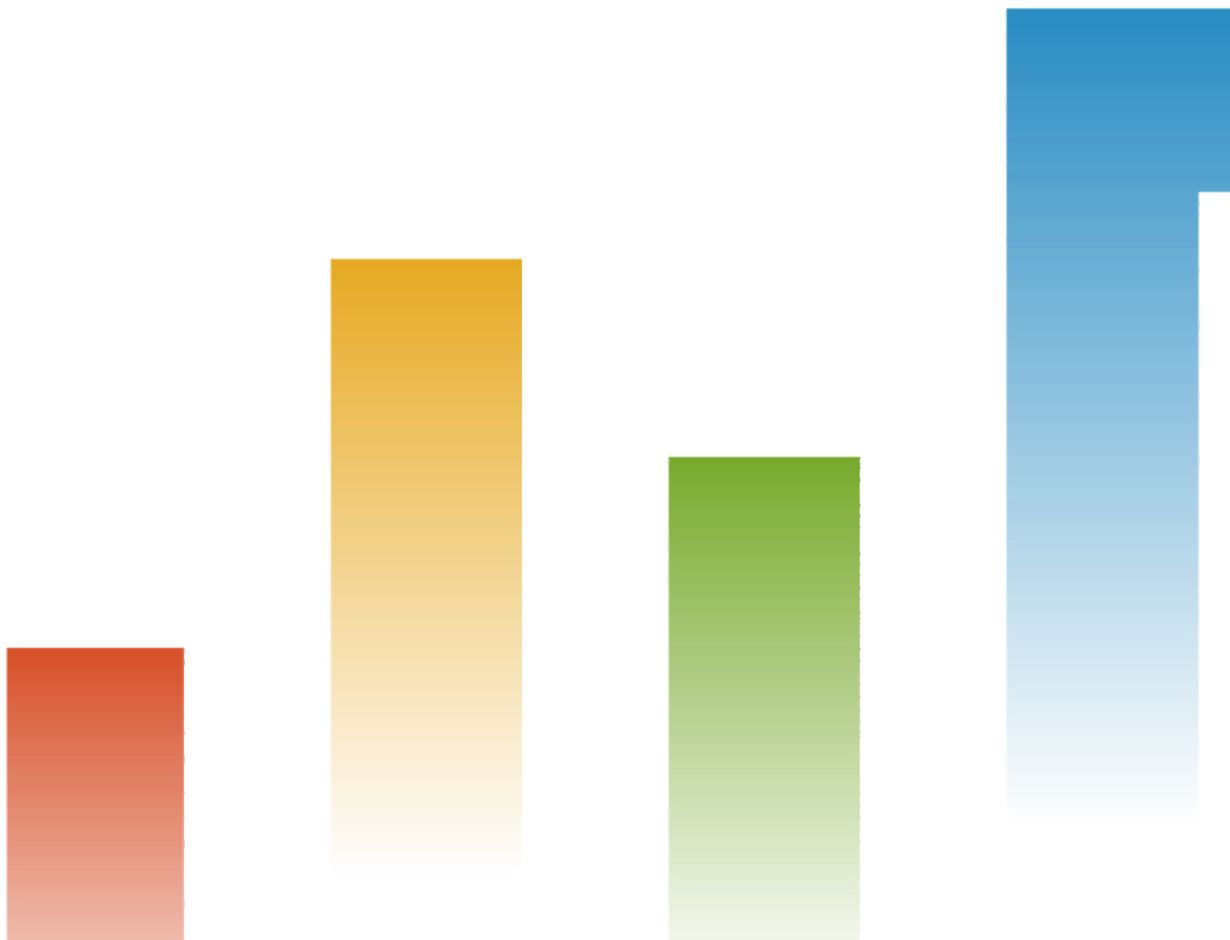


Table of Contents

• SingleStore モニタリング	4
◦ はじめに	6
◦ インストール	
▪ 手動インストール	8
◦ 設定	
▪ DBXエージェント設定	11
◦ ダッシュボード	12
▪ インスタンスリスト	13
▪ インスタンスモニタリング	16
▪ マルチインスタンスモニタリング	20
▪ ストレージエンジン	21
▪ Flexボード	25
▪ Flexボードの使い方	28
▪ ウィジェットの管理	39
◦ 分析	44
▪ 推移比較	45
▪ ロックツリー	48
▪ セッション履歴	51
▪ パーティション	54
▪ パイプライン	58
▪ データベースパラメーター	62
▪ メトリクスチャート	65
▪ メトリクストレンド分析	86
◦ 統計/レポート	89

▪ Top SQL.....	90
▪ データベースサイズ.....	94
▪ レポート	95
◦ ログ	98
▪ ライブテール	100
▪ ログエクスプローラー.....	112
▪ ログトレンド	119
▪ ログの設定.....	127
◦ OpenMetrics.....	160
▪ テンプレート一覧.....	161
▪ エクスプローラー	164
▪ エージェントのインストール.....	167
◦ アラート通知.....	169
▪ イベント設定	170
▪ メトリクスイベント	176
▪ 複合メトリクスイベント.....	197
▪ 異常検知イベント.....	204
▪ リアルタイムログ.....	208
▪ 複合ログ	220
▪ 通知設定	234
▪ 通知フォーマット.....	256
▪ イベント履歴	264
▪ イベント一時停止	272
◦ 実験室	273
▪ MXQLデータ照会	274
▪ アラートメッセージ	275

SingleStoreモニタリング

SingleStoreは、複数のノードにデータを分散して保存する分散SQLデータベースです。ノード数が増えるほど、どのノードに負荷が集中しているか、データが一方に偏っていないかを一目で把握することが難しくなります。WhaTapデータベースモニタリングは、クラスター全体の状態とノード別の指標、SQLパフォーマンスをまとめて表示します。SingleStoreを運用するDBAとデータプラットフォーム担当者が、負荷ポイントとデータの偏りを素早く見つけるのに役立ちます。

WhaTapは、**DBXエージェント**がSingleStoreクラスターに接続して指標を収集する方式で動作します。アグリゲーターノード1か所のみエージェントをインストールすると、`MV_NODES` でリーフノードを自動検出してクラスター全体を収集するため、すべてのノードにエージェントをインストールする必要はありません。詳しい開始方法は[はじめに](#)のドキュメントを参照してください。

SingleStoreクラスター構成

SingleStoreクラスターは、役割の異なるノードで構成されます。インスタンスリストの `ROLE` 列をはじめ画面のあちこちでノードの役割が表示されるため、先に把握しておく役立ちます。

ROLE	Name	Description
MA	Master Aggregator	クラスターメタデータの管理、クエリのルーティングを担当する代表アグリゲーター
CA	Child Aggregator	クエリの分散処理を補助する補助アグリゲーター
Leaf	Leaf	実際のデータを保存し演算を実行するリーフノード

簡単に言うと、アグリゲーター（MA、CA）は要求を受け取って振り分ける窓口であり、リーフ（Leaf）はデータを持って処理を行う作業者に近い存在です。

モニタリング画面の構成

SingleStoreモニタリングは、分散環境でよく確認する項目を中心に画面を提供します。

画面	説明
インスタンスモニタリング	ノード単位のCPU・メモリ・ディスク・ネットワーク指標とアクティブセッションをリアルタイムで確認
マルチインスタンスモニタリング	複数ノードの指標を1つのダッシュボードにまとめて比較
ストレージエンジン	Rowstore・Columnstoreのメモリ・ディスク使用量とデータの偏り（skew）を確認
パーティション	テーブルパーティションがノードに均等に分散されているかを偏差で確認
パイプライン	データ取り込みパイプラインのスループット・遅延・エラーを確認
データベースサイズ	データベース別の容量推移を確認
Top SQL	負荷の大きいSQLを指標と推移チャートで分析
セッション履歴	過去のアクティブセッションを時系列で照会
ロックツリー	ロック待機とデッドロックをツリーで確認

サポート環境

公式インストールガイドを基準に、次の環境をサポートします。

- SingleStore 9.0以上
- アグリゲーターノードへのDBXエージェントのインストール（リーフノードは `MV_NODES` で自動検出）
- モニタリングアカウントの権限 `grant select, process, cluster on *.*`

SingleStoreモニタリングのはじめに

このドキュメントは、SingleStoreモニタリングを初めて設定する方のための全体的な流れの案内です。クラスターにモニタリング用アカウントを作成してDBXエージェントを接続すると、数分以内に指標の収集が始まります。

SingleStoreを運用するDBAとインフラ担当者が対象読者です。

インストールは次の順序で進めます。SingleStoreのインストール画面はMySQLのインストール画面を基に作成されているため、流れが似ています。

1. Access Keyの確認
2. 構成図の確認
3. DBアカウントの作成
4. DBXエージェントのダウンロード
5. DBXエージェントの設定
6. モニタリングの開始

Access Keyの確認

WhaTapプロジェクトを作成すると、**Access Key**が発行されます。このキーは、エージェントがどのプロジェクトヘッダーを送信するかを識別する値です。whatap.confファイルの `license` 項目に入力します。

構成図の確認

インストール画面では、SingleStoreクラスターの構成図を表示します。アグリゲーター（MA、CA）とリーフ（Leaf）ノードがどのように接続されるか、DBXエージェントがどの地点に接続するかを確認できます。DBXエージェントはアグリゲーターノードに接続し、リーフノードは `MV_NODES` で自動検出されて一緒に収集されます。ノードの役割についての説明は[SingleStoreモニタリング](#)のドキュメントを参照してください。

DBアカウントの作成

DBXエージェントがクラスターの指標を照会するには、モニタリング専用のアカウントが必要です。次の権限を付与してください。

```
grant select, process, cluster on *.* to '{モニタリング_アカウント}'@'%';
```

ここで混乱しやすいのは権限の構成です。MySQLやMariaDBのインストール案内に出てくる一部の専用権限はSingleStoreでは使用せず、上記の3つの権限で十分であるとインストールガイドに案内されています。

DBXエージェントのダウンロードと設定

DBXエージェントをアグリゲーターノードにダウンロードしてインストールした後、[whatap.conf](#) ファイルを設定します。db_ip には、接続するアグリゲーターノードのアドレスを入力します。リーフノードは個別に指定しなくてもMV_NODES で自動検出されます。SingleStoreは次の基本設定を使用します。

whatap.conf

```
license={AccessKey}  
whatap.server.host={WhaTap_Server_アドレス}  
dbms=singlestore  
db_ip={Aggregator_ノード_IP}  
db_port={DB_Server_Port}
```

設定項目の詳しい説明は[手動インストール](#)と[DBXエージェント設定](#)のドキュメントを参照してください。

ファイアウォールは、DBXエージェントからWhaTap Serverへ向かう 6600 ポートのOutboundを許可する必要があります。

モニタリングの開始

設定を終えてエージェントを実行すると、指標の収集が始まります。収集が正常に行われると、[SingleStoreモニタリング](#)の各画面でデータを確認できます。

手動インストール

WhaTapデータベースモニタリングは、DBXエージェントがSingleStoreクラスターに接続して指標を収集します。エージェントはアグリゲーターノード1か所にのみインストールすればよく、リーフノードは `MV_NODES` で自動検出されてクラスター全体と一緒に収集されます。すべてのノードにエージェントをインストールする必要はありません。このドキュメントは、エージェントを手動でインストールし、whatap.conf ファイルを設定する基本的な方法を案内します。SingleStore 9.0以上の環境を対象とします。

モニタリングアカウントの作成

DBXエージェントが使用するモニタリング専用アカウントを作成し、次の権限を付与してください。

```
grant select, process, cluster on *.* to '{モニタリング_アカウント}'@'%';
```

Privilege	Description
<code>select</code>	モニタリングに必要なシステムビュー・テーブルの照会
<code>process</code>	実行中のセッション・クエリ情報の照会
<code>cluster</code>	クラスターノードの構成と分散状態の照会

MySQLやMariaDBの案内に含まれる一部の専用権限は、SingleStoreでは必要ありません。

DBXエージェントのダウンロード

インストール画面で、オペレーティングシステムに合ったDBXエージェントをダウンロードしてください。SingleStoreのインストールはManual（手動）方式を使用します。

whatap.confの基本設定

エージェントをインストールしたディレクトリの`whatap.conf`ファイルに、次の項目を設定してください。

whatap.conf

```
license={AccessKey}
whatap.server.host={WhaTap_Server_アドレス}
dbms=singlestore
db_ip={DB_Server_IP}
db_port={DB_Server_Port}
```

Option	Description
license	プロジェクトのAccess Key
whatap.server.host	データを送信するWhaTap Serverのアドレス
dbms	singlestore に固定
db_ip	接続するSingleStoreアグリゲーターノードのIP
db_port	接続ポート

ここで混乱しやすいのは `dbms` の値です。MySQLは `dbms=mysql` ですが、SingleStoreは必ず `singlestore` に設定する必要があります、これによりSingleStore専用画面が有効になるとインストールガイドに案内されています。

設定オプションの詳しい説明は[DBXエージェント設定](#)のドキュメントを参照してください。

ファイアウォール設定

DBXエージェントからWhaTap Serverへ向かう `6600` ポートのOutboundを許可する必要があります。

区分	方向	ポート
DBXエージェント → WhaTap Server	Outbound	6600

モニタリングの開始

設定を終えた後にエージェントを実行すると、指標の収集が始まります。

DBXエージェント設定

DBXエージェントに必要な設定は [whatap.conf](#) ファイルに記述します。このドキュメントでは、SingleStore監視で使用する設定オプションについて説明します。

基本オプション

Option	Type	Description
<code>license</code>	<code>string</code>	プロジェクトのAccess Key
<code>whatap.server.host</code>	<code>string</code>	データを送信するWhaTap Serverのアドレス
<code>dbms</code>	<code>string</code>	<code>singlestore</code> 固定
<code>db_ip</code>	<code>string</code>	接続するSingleStoreノードのIP
<code>db_port</code>	<code>integer</code>	接続ポート

whatap.conf

```
license={AccessKey}
whatap.server.host={WhaTap_Server_アドレス}
dbms=singlestore
db_ip={DB_Server_IP}
db_port={DB_Server_Port}
```

追加オプション

ダッシュボード

ダッシュボードは、SingleStoreクラスターの状況を一目で把握する出発点です。アグリゲーターとリーフノードを併せて確認してクラスター全体の状態を見渡し、異常のあるノードへすぐに入って詳細な指標とセッションを確認できます。

画面構成

画面	説明
インスタンスリスト	クラスターに属するノードの状態・役割（MA・CA・Leaf）と主要指標を表で一目で確認
インスタンスモニタリング	1つのノードのCPU・メモリ・ディスク・ネットワーク指標とアクティブセッションをリアルタイムで確認
マルチインスタンスモニタリング	複数ノードの主要指標を1つの画面に並べて比較
ストレージエンジン	Rowstore・Columnstoreの使用状況と危険・過多テーブルを分析
Flexボード	必要なウィジェットを組み合わせるユーザー定義ダッシュボードを構成

各画面へ入って、ノード別の詳細な指標とセッションを分析できます。

インスタンスリスト

インスタンスリスト画面は、SingleStoreクラスターに属するノードを1行ずつ表にまとめて表示します。アグリゲーターとリーフノードを1つの画面で併せて確認できるため、クラスター全体の状態を素早く見渡し、異常のあるノードへすぐに入る出発点になります。

サマリー領域

表の上部には、全体のノード数と状態別の集計を表示します。

Item	Description
全体	収集中の全体ノード数
危険	危険状態に分類されたノード数
警告	警告状態に分類されたノード数
正常	正常状態のノード数

ノードリスト表

各行が1つのノードに対応します。デフォルトで提供される列は次のとおりです。

Item	Description
状態	ノードの収集・状態表示
サーバー名	ノード名（例: 1-MA-150、LF-152）。クリックすると該当する インスタンスモニタリング へ移動
IP	ノードのIPアドレス

Item	Description
ポート	接続ポート（デフォルト 3306）
データベース	ノードが担当するデータベースの一覧
ROLE	ノードの役割。MA（Master Aggregator）、CA（Child Aggregator）、Leaf
Cluster Name	ノードが属するクラスター名
Threads_running	実行中のスレッド数
Questions	処理したクエリ数
innodb_buffer_pool_read_requests	バッファプールの読み取り要求数
lock_wait_sessions	ロック待機中のセッション数

① SingleStoreは、アグリゲーターノードにのみDBXエージェントをインストールすると、MV_NODES でリーフノードを自動検出してクラスター全体がリストに表示されます。ノード名の MA ・ CA ・ LF の接頭辞で役割を素早く区別できます。

表の操作

- **列の選択:** 表に表示する列を追加したり非表示にしたりできます。
- **マルチビュー:** 複数のノードを選択して、併せて比較する画面に切り替えます。
- ノードを選択した後、詳細画面へ移動して指標とセッションを詳しく確認できます。

データ解釈ガイド

確認ポイント	説明
特定ノードの <code>Threads_running</code> の急増	該当ノードに負荷・競合が集中している疑い
<code>lock_wait_sessions</code> の累積	ロック待機が発生、 ロックツリー で原因を追跡
Leafノード間の指標の偏差	データの偏り（Skew）の可能性、 パーティション で配置を点検

インスタンスモニタリング

インスタンスモニタリング画面では、SingleStoreの1つのノードの主要指標をリアルタイムで確認できます。CPUとメモリの使用量が急に上がったり、特定のノードにセッションが集中したりするとき、どのノードで何が起きているかを素早く把握するのに役立ちます。SingleStoreを運用するDBAが対象読者です。

基本画面の案内

画面上部のインスタンスセレクトアーで照会するノードを選択します。ノード名には役割も併せて表れます。インスタンスリストの `ROLE` 列で `MA`（Master Aggregator）、`CA`（Child Aggregator）、`Leaf` の値からノードの役割を区別できます。時間領域はLIVE基準でデフォルト10分の範囲で照会され、指標は5秒周期で更新されます。

画面上部には、ノードの状態を素早く見るKPIタイルが配置されます。

Item	Description
Threads Running	実行中のスレッド数
Connections	接続数
Queries	クエリ処理量
Successful Read Queries	成功した読み取りクエリ数
Failed Read Queries	失敗した読み取りクエリ数
Failed Write Queries	失敗した書き込みクエリ数

KPIタイルの下には、リソース使用量のチャートウィジェットが構成されます。

Widget	Metric
CPU	<code>cpu_user_pct</code> ・ <code>cpu_system_pct</code> ・ <code>cpu_iowait_pct</code> ・ <code>cpu_idle_pct</code>
Memory	<code>host_total_mb</code> ・ <code>host_used_mb</code>

Widget	Metric
Disk Usage	<code>os_mount_total_mb</code> ・ <code>os_mount_used_mb</code>
Network Bandwidth	ノードのネットワークIN ・ OUT

画面下部には、アクティブセッションとロックツリーをタブで切り替えて見る領域、そしてLock Wait sessionsウィジェットが配置されます。

アクティブセッション領域

画面下部のアクティブセッションテーブルで、現在クラスターで実行中のセッションを確認できます。SingleStoreは1つのクエリが複数のノードに分かれて実行されるため、アクティブセッションをアグリゲーター作業（Aggregator activity）単位でまとめて表示します。これにより、クラスターが今どのような作業を実行中かを作業単位で把握できます。

テーブルの列は次のとおりです。

Column	Description
<code>instance</code>	セッションが実行中のノード
<code>node_id</code>	ノード識別子
<code>database</code>	対象データベース
<code>session_id</code>	セッション識別子
<code>user</code>	セッションユーザー
<code>state</code>	セッション状態（例: <code>executing</code> ）
<code>command</code>	実行中のコマンドの種類（例: <code>Query</code> ）
<code>activity</code>	作業名

Column	Description
<code>raw_task</code>	実行中のSQL原文
<code>sql_param</code>	SQLパラメータ
<code>aggregator_activity</code>	まとめの基準となるアグリゲーター作業名
<code>elapsed(ms)</code> ・ <code>avg elapsed(ms)</code>	実行時間（最大・平均）
<code>cpu(ms)</code> ・ <code>cpu wait(ms)</code>	CPU使用・待機時間
<code>lock wait(ms)</code>	ロック待機時間
<code>network(ms)</code>	ネットワーク時間
<code>disk i/o(ms)</code>	ディスクI/O時間
<code>disk spilling</code> ・ <code>avg spilling</code>	ディスクスピリング量（最大・平均）
<code>part rows</code>	処理したパーティションの行数
<code>conn</code>	接続数
<code>memory</code> ・ <code>avg memory</code>	メモリ使用量（最大・平均）

`node_id` ・ `aggregator_activity` ・ `part rows` ・ `disk spilling` は、分散実行環境でのみ意味を持つSingleStore固有の列です。

アクティブセッションで特定のセッションのSQLをクリックすると、詳細情報ウィンドウが開きます。SQL詳細ウィンドウは[Top SQL](#)ドキュメントのSQL詳細表示の説明を参照してください。

セッションの停止

SingleStoreでは、アクティブセッションを選択して停止（Kill）できます。停止対象はセッションID（`session_id`）で識別します。

⚠ セッションの停止は、実行中のクエリを強制的に終了します。影響範囲を確認したうえで慎重に使用してください。

マルチインスタンスモニタリング

マルチインスタンスモニタリング画面では、クラスターに属する複数ノードの指標を1つのダッシュボードにまとめて比較できます。分散環境では特定のノードにのみ負荷が集中する場合がありますが、ノード別の指標を並べて見ることで偏りを素早く見つけられます。

基本画面の案内

基本ダッシュボード（Defaultプリセット）は、ノード別の主要指標をまとめたチャートとアクティブセッションテーブルで構成されます。インスタンスモニタリングと同様に、ノード名の前に **MA** ・ **CA** ・ **LF** の役割タグが表示されます。

ウィジェットの追加

マルチインスタンスダッシュボードは、ウィジェットパレットからSingleStore専用ウィジェットを追加して構成できます。ウィジェットを追加・編集・削除する方法は、データベース共通のダッシュボード編集方式と同じです。

アクティブセッション領域

ダッシュボード下部のアクティブセッションテーブルで、クラスター全般のセッションを確認できます。列の案内とSQL詳細表示は[インスタンスモニタリング](#)と[Top SQL](#)のドキュメントを参照してください。

ストレージエンジン

ストレージエンジン画面では、SingleStoreがデータを保存する2つの方式であるRowstoreとColumnstoreのメモリ・ディスク使用状況を確認できます。分散環境では、特定のノードにデータが集中する偏り（skew）が性能低下につながりますが、この画面はノード間の分布を一目で表示し、偏りを素早く見つけれられるよう支援します。SingleStoreを運用するDBAが対象読者です。

RowstoreとColumnstore

SingleStoreはデータを2つの方式で保存します。まず2つの概念を知っておくと画面が読みやすくなります。

- **Rowstore** はデータをメモリに行単位で保存します。高速な読み取り・書き込みに有利ですが、メモリを多く使用します。簡単に言うと、よく取り出して使う物を机の上に置いておく方式に近いです。
- **Columnstore** はデータをディスクに列単位で圧縮して保存します。大容量分析に有利で、ディスク効率が高いです。あまり使わない物を圧縮して倉庫に入れておく方式に近いです。

画面はこの2つを分けて表示します。

要約情報

画面上部で照会するクラスター（例: `memsql_cluster`）を選択すると、RowstoreとColumnstoreの状態を2つの要約カードで表示します。各カードには、注意が必要な状態のときに **WARN** バッジが表示されます。

Card	Description
Rowstore要約情報	Total in Memory, Max Node Mem, Avg Memory Deviation, Worst skew table
Columnstore要約情報	Total on Disk, Compression, Avg Disk Deviation, Worst skew table

`Avg Memory Deviation` ・ `Avg Disk Deviation` はノード間の使用量偏差を倍数で表します。値が大きいほど特定のノードにデータが集中しているという意味です。 `Worst skew table` は偏りが最も激しいテーブルを併せて示します。

Rowstore領域

Rowstoreはメモリを使用するため、メモリ使用量とノード別の分布が主要指標です。

Widget	Description
ノード別メモリ使用率	ノード別のホストメモリ使用率をゲージで表示
Memory Trend	Table Memory (Rowstore) と Server Memory (Process) の時間推移
Memory-Risk Tables (TOP 5)	メモリ危険度が高いテーブルの上位5個

ノード別メモリゲージは、ホストメモリ使用率を使用量と全体容量（例: 2.4 / 3.7 GB）、パーセンテージと併せて表示します。 <80%、80-90%、>90% の区間を色で区別し、アグリゲーター（MA/CA）ノードはデフォルトで折りたたまれており、展開して見るができます。

Memory-Risk Tables (TOP 5)は次のカラムで構成されます。

Column	Description
Table	テーブル名とデータベース
Worst Node	使用量が最も大きいノード
Size (Total)	全体のメモリ使用量と行数
Parts	パーティション数
Skew	ノード間の偏り倍数

Columnstore領域

Columnstoreはディスクを使用するため、ディスク使用量とセグメント状態が重要です。

Widget	Description
ノード別ディスク使用率	ノード別のディスク使用量をバーで表示
Segment Group推移	セグメントグループ数（group_cnt）の日次比較と上位テーブル
Size Top 5	ディスクを多く占めるテーブルの上位5個

ノード別ディスクバーは、SingleStoreが使用するディスクを領域別に分けて表示します。バーをクリックすると、ノード別の詳細構成を確認できます。

Area	Description
Data	カラムストアデータ
Snapshot	スナップショット
Log	トランザクションログ
Temp	一時データ
Etc	パーティション外の領域
Others	その他のOS使用量
Free	残りの空き容量

Size Top 5は、テーブルごとに圧縮後のサイズ（Size (Total)）、圧縮率（Compression）、行数（Rows）と、使用量が最も大きいノード（Worst Node）を表示します。

ここで混同しやすい部分はSegment Group推移です。SingleStoreはColumnstoreデータをセグメントで管理し、バックグラウンドのマージャー（merger）が小さなセグメントを統合して整理します。Segment Group推移はクラスターの group_cnt の合計を前日と比較して表示し、現在 group_cnt が大きいテーブルの上位5個を24時間の変化量（ $\Delta 24h$ ）・パーティション数と併せて表で提供します。group_cnt が継続的に右肩上がりになる場合は、自動マージャーがINSERT速度に追いついていないという信号と見ることができ、この場合は OPTIMIZE 作業を検討することになります。

データの偏り（skew）確認

分散データベースでデータが特定のノードに偏ると、そのノードだけが負荷を抱えることになります。ストレージエンジン画面は偏りを次の指標で表示します。

Metric	Description
Max Node Mem	ノードの中で最も高いメモリ使用率
Avg Memory Deviation	Rowstoreメモリ使用量のノード間平均偏差（倍数）
Avg Disk Deviation	Columnstoreディスク使用量のノード間平均偏差（倍数）
Skew	テーブル単位のノード間偏り倍数
Worst skew table	偏りが最も激しいテーブル

偏りが激しいテーブル行をクリックすると詳細ドロワーが開き、ノード別の分布と併せて **OPTIMIZE** 推奨の案内を確認できます。

OPTIMIZE推奨の案内

テーブル詳細ドロワーでは、データ整理（**OPTIMIZE**）が必要かどうかを段階別に案内します。案内は推奨レベルに応じて分かります。

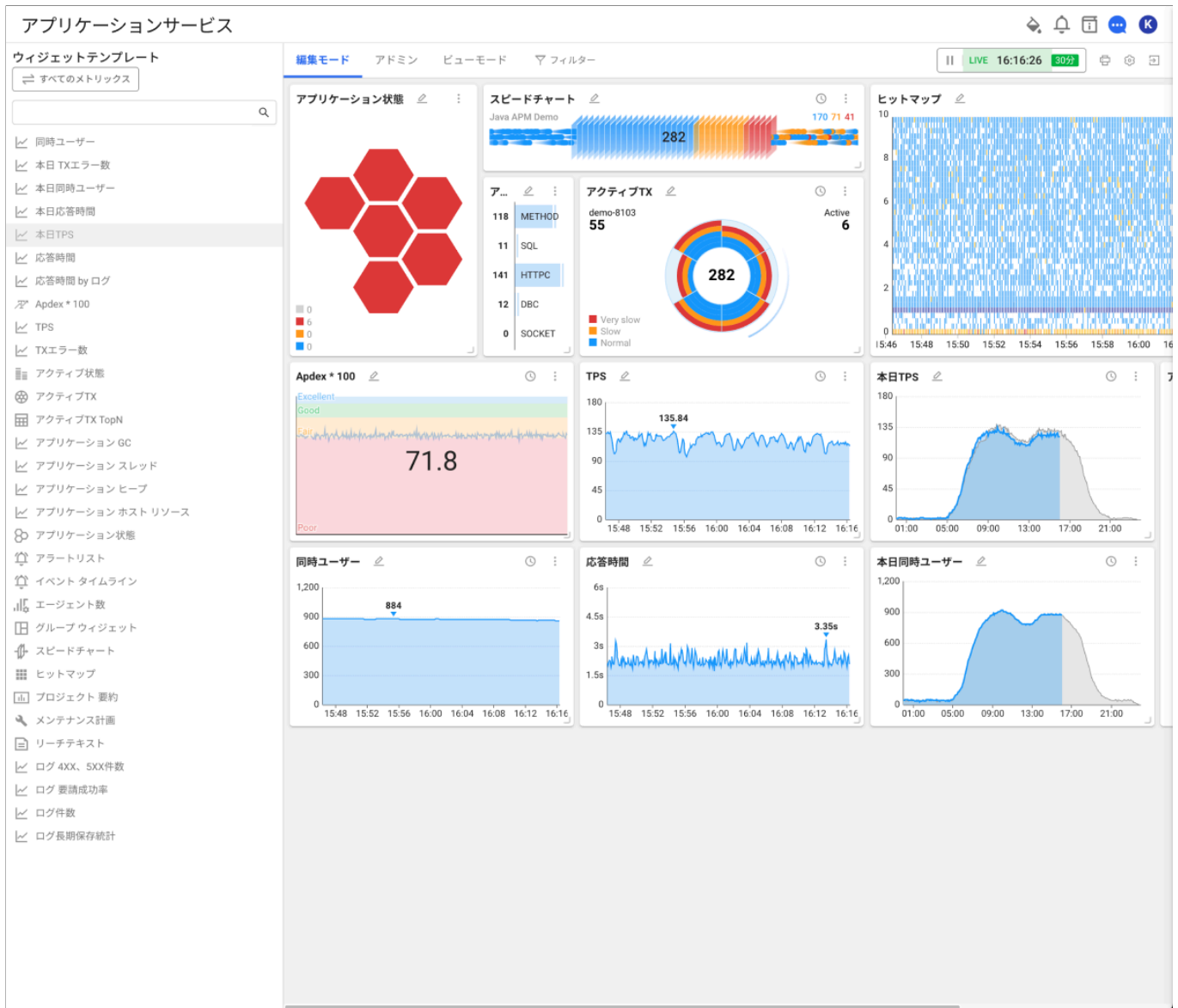
照会時点

画面はリアルタイムタイムセレクターを使用します。収集周期に合わせて最近の収集値を表示し、Memory Trendは最近1時間、クラスター要約は最近7日の範囲をデフォルトで照会します。

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ボードの使い方

- ✔ 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。

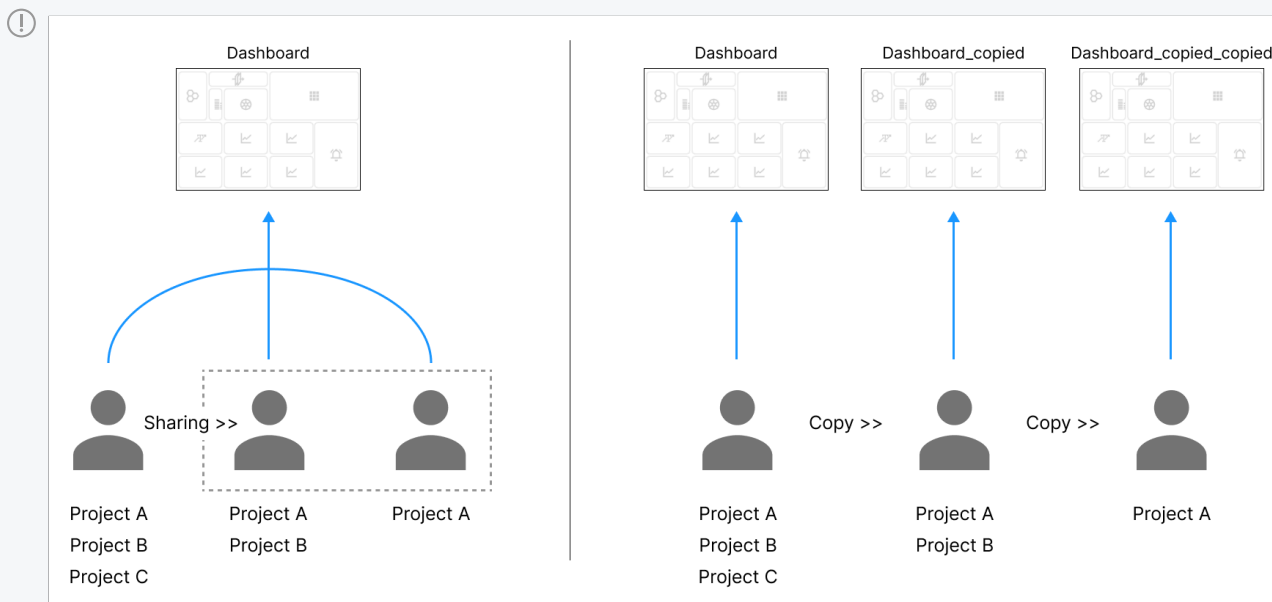
 ダッシュボードの削除は所有者と共有を受けたユーザーで動作が異なります。

- 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。

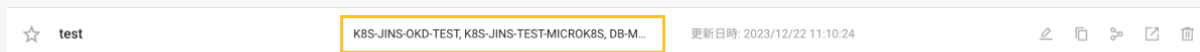
Flex ボードを共有する

 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 読取り専用 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。

1. 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。
2. 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
3. 完了後、**PDFダウンロード** を選択します。
4. 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

することもできます。

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

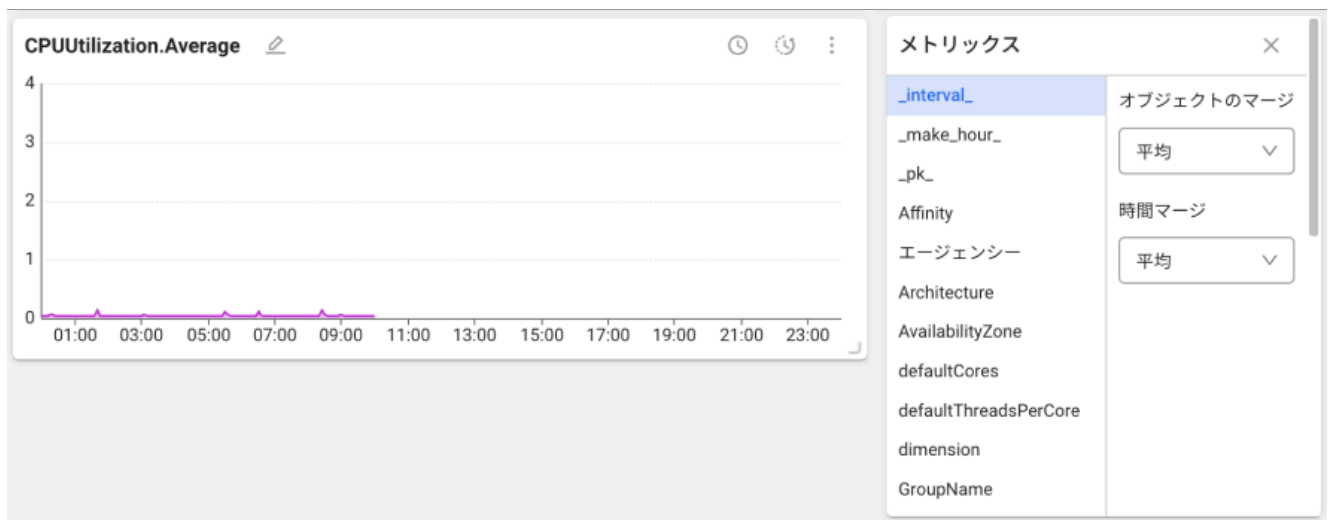
左側で選択したタグ(例：エージェント名)に基づいてチャートデータをグループ化するために使用します。この場合、異なるフィールド(例：CPU)値を持つデータ間でタグが一致する場合、そのデータは結合されます。

• 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。

分析

分析メニューでは、ダッシュボードで見つけた異常の原因を深く掘り下げます。セッションとロック、分散構造（パーティション・パイプライン）、メトリクスの推移をさまざまな角度から見て、根本原因を突き止めることができます。

画面構成

画面	説明
推移比較	2つの時点の主要指標とセッションの流れを並べて比較
ロックツリー	ロック待機関係をツリーで追跡し、ブロッキングの原因を特定
セッション履歴	過去のアクティブセッションを時系列で照会・分析
パーティション	データの偏り（Skew）とShard Keyの適切性を点検
パイプライン	Pipelineの取り込み状況（処理率・失敗・バックログ）を追跡
データベースパラメーター	パラメーター値の照会・日付別の比較
メトリクスチャート	メトリクスデータをチャートで照会
メトリクス推移分析	長期メトリクスの推移分析

推移比較

推移比較画面では、異なる2つの時点を並べて主要指標とセッションの流れを比較できます。普段と異なる日の負荷を見比べたり、変更作業の前後を比較して何が変わったかを確認したりするときに役立ちます。

比較条件の設定

画面上部で比較する2つの時点と対象を指定します。

項目	説明
基準日	比較の基準となる日付
比較日	基準と見比べる日付
インスタンス	基準・比較それぞれの対象ノード（ <code>oname</code> ）を選択
データベース	選択したインスタンスが担当するデータベースを表示
プリセット	よく見るチャート構成を保存して呼び出し（ <code>Default</code> を提供）

基準と比較のインスタンスを異なるように指定すると、異なるノードを同じ日付で見比べることも可能です。

KPI比較チャート

基準時点と比較時点の主要指標を同じ軸に重ねて5分単位で表示します。

Metric	Description
Threads Running	実行中のスレッド数
Connections	接続数

Metric	Description
Queries	処理したクエリ数
Successful Queries	成功したクエリ数
Failed Queries	失敗したクエリ数
CPU	CPU使用率
Engine Memory	エンジンが使用するメモリ
Disk Usage	ディスク使用量
Network Bandwidth	ネットワーク帯域幅

各チャートで基準と比較時点の曲線を重ねて見るため、同じ時間帯に負荷がどれだけ異なっていたかを一目で確認できます。

ⓘ Engine Memory は、インスタンスモニタリング画面の Memory ウィジェットと同じメモリ指標を、推移比較画面のラベルで表記したものです。

基準・比較セッションテーブル

チャートの下には、基準時点と比較時点のセッション一覧を左右に並べて表示します。上部の時間バーで特定の時刻を選択すると、その時点に収集されたセッションを両方で一緒に確認できます。

2つのテーブルは同じカラムを使用します。

Column	Description
instance	セッションが実行されたノード。クリックすると該当の インスタンスモニタリング 画面へ移動
id	セッション識別子

Column	Description
user	セッションを実行したユーザー
host	接続ホスト
db	対象データベース
command	セッションが実行中のコマンドの種類（Query など）
runtime	実行時間
state	セッションの状態（executing など）
query	実行中のSQL
query_param	バインドされたパラメーター値
type	セッションのタイプ
connection_type	接続タイプ

データ解釈ガイド

確認ポイント	説明
同じ時間帯の指標急増	比較時点に比べて負荷が増えた区間。変更・イベントの影響を疑う
一方にのみ偏ったFailed Queries	特定の日付に集中したエラー。デプロイ・データ変更との関連を確認
セッション数・実行時間の増加	クエリパターンの変化や競合の増加を疑い、セッションテーブルで原因クエリを追跡

ロックツリー

ロックツリー画面では、ロック（Lock）によって互いに待機しているセッションをツリー形式で確認できます。どのセッションがリソースを保持しており（holder）、どのセッションがそれを待っているか（waiter）を親子関係で表示するため、デッドロックの原因となるセッションを素早く見つけるのに役立ちます。

ロックとロックツリー

簡単に言うと、ロックは同じデータを同時に変更できないようにかける施錠装置です。あるセッションがデータを修正している間、他のセッションは待たなければなりません。待機するセッションが増えて互いに絡み合うと、デッドロックになります。ロックツリーはこの待機関係を木の形に展開し、一番上でリソースを保持しているセッション（原因）を見つけられるようにします。

基本画面の案内

画面上部でインスタンスとデータベースを選択します。まずLock Wait Sessionsチャートでロック待機が発生した時点を選択すると、その時点のLock TreeとTotal Locksを確認できます。数分以上持続したロックを示してくれるため、長く拘束されているロックを素早く見つけられます。

領域	説明
Lock Wait Sessions	時間帯別のロック待機セッション数チャート。照会する時点を選択
Lock Tree	選択時点のロック待機関係をツリーで表示
Total Locks	選択時点の全ロック数

カラム案内

リソースを保持しているセッション（holder）と待機しているセッション（waiter）を、次のカラムで表示します。

Column	Description
instance	セッションが実行中のノード
node_id	ノード識別子
session_id	セッションID
db	使用中のデータベース
user	接続ユーザー
tx_state	トランザクション状態
lock_type	ロックタイプ
row_locks	行ロック数
partition_locks	パーティションロック数
activity	作業名
raw_task	実行中のSQL原文
sql_param	SQLパラメーター
command	実行中のコマンドの種類
elapsed_time_ms	実行時間（ミリ秒）

ここで混同しやすいのはセッションの識別方法です。MySQLはセッションID1つで識別しますが、SingleStoreは分散環境のため、ノード識別子とセッションIDを合わせて（`node_id` + `session_id`）マッチングキーとして使用します。同じセッションIDでもノードが異なれば別のセッションだからです。`row_locks`・`partition_locks`は、分散環境でロックが行単位かパーティション単位かを区別してくれます。

ロックの解消

原因セッション（holder）を確認した後、必要に応じてそのセッションを停止できます。セッションの停止方法は[セッション履歴](#)と[インスタンスモニタリング](#)のドキュメントを参照してください。

AIで分析する

画面で**WhaTap AI**ボタンをクリックすると、WhaTap AIチャットウィンドウが開き、照会した画面データを要約して分析した結果が対話形式で表示されます。結果を読んだ後、同じ対話で続けて質問できます。

- 分析に使用するデータは照会範囲全体の推移、30分区間の集計、選択時点のロックツリースナップショットの3つです。
- 分析対象は画面に照会されたデータです。照会条件を変更してから再度分析すると、変更後のデータを基準に分析します。
- 対話履歴には **AI分析 - {画面名}** 形式で記録されます。

セッション履歴

セッション履歴画面では、過去に収集されたセッション情報を時系列で照会できます。特定の時間帯にどのセッションがどのSQLを実行したか、リソースをどれだけ使用したかを遡って分析できます。障害が過ぎた後に原因を振り返るときに役立ちます。

データはアクティブセッションのスナップショット（db_singlestore_active_session）をもとに提供します。

基本オプション

上部フィルター領域で照会条件を設定します。

項目	説明
時間	照会時間範囲を選択
インスタンス	照会対象のノード（oname）を選択
フィルター	フィールドごとに条件を追加。複数条件はANDロジックが適用されます
ダウンロード	CSV形式でエクスポート

セッション推移チャート

照会期間中のアクティブセッション数をバーチャートで表示します。X軸は時間、Y軸はセッション数です。

- チャート領域をマウスでドラッグすると、その区間に絞り込んで詳細分析できます。
- チャートのバーをクリックすると、その時点（±5分）の[インスタンスモニタリング](#)画面へ移動します。セッションが多かった時点のノード状態も一緒に確認できます。

長時間実行セッション

セッション推移とともに、長時間実行セッション領域を提供します。照会期間中に長く実行されたセッションをまとめて表示するため、非効率なクエリや停止したトランザクションを素早く選び出せます。

セッション一覧テーブル

収集されたセッション情報を時系列で表示します。上部のフィールド・フィルターで条件を設定でき、下部のページサイズ設定で一度に表示する行数を調整できます。

カラムは[インスタンスモニタリング](#)のアクティブセッションテーブルと同じ分散実行指標（`instance`・`node_id`・`session_id`・`state`・`elapsed(ms)`・`cpu(ms)`・`memory`・`aggregator_activity` など）を共有し、過去の照会に合わせて次のカラムを追加して表示します。

Column	Description
<code>time</code>	セッションが収集された時刻
<code>sql_hash</code>	同一SQLをまとめるハッシュ値

`sql_hash` で同じクエリの繰り返し実行をまとめて見ることができ、特定のSQLが繰り返しリソースを多く使っているかを把握するのに役立ちます。

セッションの停止

セッションを選択して停止（Kill）できます。停止対象はセッションID（`session_id`）で識別し、ノード識別子（`node_id`）は数値に正規化して処理します。

ⓘ セッションの停止は実行中のクエリを強制終了します。影響範囲を確認したうえで慎重に使用してください。

データ解釈ガイド

確認ポイント	説明
実行時間が長いセッション	長時間実行中のセッション。ロック競合・非効率クエリ・未完了トランザクションを疑う
待機状態のセッションが多数	特定リソースの競合が発生。ロック原因の分析が必要
特定ノードへのセッション集中	データの偏りやルーティングの偏りを疑う

パーティション

パーティション画面では、テーブルのデータがクラスターノードにどれだけ均等に分かれているかを確認できます。SingleStoreはテーブルを複数のパーティションに分割してノードに分散しますが、この分散が一方に偏ると特定のノードだけが多くの処理を担うことになります。この画面は偏りを平均との偏差で表示し、バランスが崩れたテーブルを見つけられるよう支援します。

パーティションとは

簡単に言うと、パーティションは大きなテーブルを複数の断片に分けてノードに散らしておく単位です。データが均等に散らばると、ノードが処理を分担できるため高速です。逆に1つのノードに断片が集中すると、そのノードがボトルネックになります。そのため、分散データベースではパーティションが均等に広がっているかが重要です。

パーティション配置図（ホスト別）

画面上部でクラスターを選択すると、データベースごとにパーティションがどのホスト（リーフノード）に配置されているかをグリッドで表示します。データベースごとに全体のパーティション数（例: PARTITIONS=16）が表示され、各パーティションのセルの色で偏り状態を区別します。全ホスト・全DBフィルターで範囲を絞り込めます。

状態	意味
Hot	平均の2倍以上
Warning	平均の1.5倍以上
Normal	正常範囲
Empty	行がないパーティション（rows=0）
Offline	オフラインパーティション

Table-level Partition Distribution

画面中央にはテーブルごとのパーティション分散状況の表があります。各テーブルがノードにどれだけ均等に分散されているかを **Avg Deviation** で表示します。**Avg Deviation** は **Max / Avg**、つまり最も大きいパーティションが平均の何倍かを表す倍数です。値が1倍に近いほど均等に分散された状態で、大きいほど特定のパーティションに偏っているという意味です。表はデフォルトで **Avg Deviation** を基準に降順で並べ替えられ、最も偏ったテーブルが上に上がってきます。

表のカラムは次のとおりです。

Column	Description
Table	データベース.テーブル 名
Storage	ストレージエンジン (ROWSTORE / COLUMNSTORE)
Shard Key	データをノードに分ける基準カラム
Cardinality	Shard Keyの固有値の数
Partitions	全体のパーティション数
Used Parts	データが入っているパーティション数
Total Rows	全体の行数
Total Size	全体のサイズ
Max Part Size	最も大きいパーティションのサイズ
Avg Deviation	ノード間の偏り倍数 (Max / Avg)

Shard Key と **Cardinality** を併せて見ると、偏りの原因を突き止められます。Shard Keyの固有値が少ない（低い Cardinality）と、同じ値が1つのパーティションに集中して偏りが生じやすくなります。

状態は **Avg Deviation** の値で次のように区別します。

状態	基準
Healthy	< 1.5x
Warning	1.5x ~ 2x
Critical	≥ 2x または空のパーティションが存在

ノード別の統計収集基準に満たないテーブルは分散を評価しにくいいため、N/Aとして処理し、表から除外します。信頼できるデータだけを比較するための動作です。全体状態・Top 5フィルタで表示範囲を調整できます。

Row Count Growth (Top 5 Hot Partitions)

行数が急速に増えているパーティションの上位5個を推移で表示します。各項目は

P#パーティション番号 テーブル(ノード) の形式で表示されます(例: P#9 merge_active_demo (LF-153))。データが急激に増えるパーティションは、まもなく分散バランスが崩れる可能性があるため、事前に確認しておく役立ちます。

パーティション詳細ドロワー

表でテーブル行をクリックすると、パーティション詳細ドロワーが開きます。ドロワーはディスクとメモリの使用量を2つの領域に分けてゲージで表示し、行数・サイズ・スキューなどの主要指標(KPI)を併せて表示します。

照会時点

画面は範囲タイムセレクター(RangeTimeSelector)を使用し、デフォルト範囲は当日(00:00から翌日00:00まで)です。Quickボタンで6時間・12時間・当日・前日・2日前・7日前・30日前を素早く選択できます。

ⓘ パーティションデータは1時間単位で収集されます。照会範囲を1時間より短く設定するとデータが表示されないことがあるため、1時間以上に設定することをおすすめします。

照会範囲が1時間未満または24時間を超えると、画面に案内ボックスが表示されます。表示される値は範囲内の最後の

収集値 (LAST-ONLY) です。

パイプライン

パイプライン画面では、SingleStoreのデータ取り込みパイプラインがどれだけ正常に動作しているかを確認できます。パイプラインが遅延したりエラーが発生したりすると、データが時間どおりに取り込まれません。この画面はスループット・遅延・エラーをまとめて表示し、問題箇所をすばやく特定できるように支援します。

パイプラインとは

SingleStoreのパイプライン（Pipeline）は、外部ソース（ファイル、メッセージキューなど）からデータを自動的に取得してテーブルに取り込む機能です。簡単に言えば、データを絶えず運び続けるコンベアベルトに近いものです。ベルトが遅くなったり止まったりするとデータが蓄積されるため、処理速度とエラーを監視することが重要です。

基本画面の案内

画面上部で照会するクラスターを選択してください。画面はステータスサマリー、KPIカード、推移チャート、パイプライン詳細表、最近のエラーで構成されます。

KPIカード

パイプライン全体の主要指標をカードで表示します。

Card	Description
PIPELINES	全パイプライン数
FAILING PIPELINES	失敗が発生中のパイプライン数
BATCH SUCCESS RATE	バッチ成功率
FAILED BATCHES	失敗したバッチ数
BATCHES	処理したバッチ数（間隔あたりのバッチ数）

各カードは `rows/s (avg)`、`batches per interval`、`milliseconds (avg)` などの補助単位もあわせて表示します。

推移チャート

パイプラインの処理状態を2つの時系列チャートで表示します。

Chart	Description
RPS by Pipeline	パイプラインごとの秒あたり処理行数 (rows per second)
Batch Success / Failure	バッチの成功・失敗の推移

チャートで特定のパイプラインをクリックすると、チャートと下の表の両方を該当パイプライン基準でフィルタリングします。

Pipeline Details 表

個々のパイプラインの処理状況を表で表示します。上部の検索ボックスでパイプライン、ソース、テーブル名で検索できます。

Column	Description
Pipeline	パイプライン名
Source	データソース
Target Table	取り込み先テーブル
Type	ソースの種類
Kind	パイプラインの種別
RPS (avg)	秒あたり処理行数 (平均)

Column	Description
Rows Total	取り込んだ全行数
Batches OK	成功したバッチ数
Failed	失敗したバッチ数
Queued	待機中のバッチ数（バックログ）

表でパイプラインの行をクリックすると、バッチ単位の詳細ドロワーが開きます。ドロワーでは、選択したパイプラインのバッチ指標チャートと最近のエラーをあわせて確認できます。

最近のエラー (Recent Pipeline Errors)

画面下部で、最近発生したパイプラインのエラーを確認できます。

Column	Description
Error Time	エラー発生時刻
Pipeline	エラーが発生したパイプライン
Batch	バッチ識別子
Code	エラーコード
Message	エラーメッセージ
Host	発生ホスト
Instance	発生インスタンス

- バッチドロワーを開くと、最近のエラーを自動的に照会します。
- エラー一覧はページを分けて表示します。

- 検索ボックスでパイプライン、タイプ、コード、メッセージで検索できます。

照会時点

画面右上で最終収集時刻を確認できます。

データベースパラメーター

ホーム画面 > プロジェクト選択 > 分析 > パラメータ

データベース設定値の参照機能を提供し、過去の日付の時点でのデータベース設定を表示することができます。比較機能を使用すると、データベースのパラメータ値を日付別に比較できます。デフォルトでは、現在時刻のデータが表示されます。

データベースにパラメータ値が原因で問題が発生した場合、データベースパラメータ比較機能を使用すると、すばやく原因を特定できます。

パラメータ		
基準日	比較日	インスタンス
2023/10/04	2023/10/10	demo-01
変更を表示		
Key	2023/10/04 Value	2023/10/10 Value
wsrep_ready(stat)	ON	OFF
wsrep_provider_version(stat)	4.9(rcece3ba2)	4.9(rcece3ba2)
wsrep_provider_vendor(stat)	Codership Oy <info@codership.com>	Codership Oy <info@codership.com>
wsrep_provider_name(stat)	Galera	Galera
wsrep_provider_capabilities(stat)	:MULTI_MASTER:CERTIFICATION:PARALLEL_APPLYING:TRX_REPLAY:ISOLATION:P AUSE:CAUSAL_READS:INCREMENTAL_WRITESET:UNORDERED:PREORDERED:STRE AMING:NBO:	:MULTI_MASTER:CERTIFICATION:PARALLEL_APPLYING:TRX_REPLAY:ISOLATION:P AUSE:CAUSAL_READS:INCREMENTAL_WRITESET:UNORDERED:PREORDERED:STRE AMING:NBO:
wsrep_connected(stat)	ON	ON
wsrep_cluster_status(stat)	Primary	non-Primary
wsrep_cluster_state_uuid(stat)	37ea72c5-ee15-11ed-8f3e-67510a6d46e9	37ea72c5-ee15-11ed-8f3e-67510a6d46e9
wsrep_cluster_capabilities(stat)		
wsrep_gcomm_uuid(stat)	c094ae4d-56c3-11ee-8772-57dd9d06a011	c094ae4d-56c3-11ee-8772-57dd9d06a011
wsrep_evs_state(stat)	OPERATIONAL	OPERATIONAL
wsrep_evs_rep_latency(stat)	0.000372136/0.000778795/0.0157565/0.00107258/1859	0/0/0/0/0
wsrep_evs_evict_list(stat)		
wsrep_evs_delayed(stat)		
wsrep_incoming_addresses(stat)	10.21.1.236:0,10.21.1.86:0,10.21.1.136:0	10.21.1.86:0
wsrep_local_state_comment(stat)	Synced	Initialized
wsrep_flow_control_requested(stat)	false	false
wsrep_flow_control_active(stat)	false	false
wsrep_local_state_uuid(stat)	37ea72c5-ee15-11ed-8f3e-67510a6d46e9	37ea72c5-ee15-11ed-8f3e-67510a6d46e9
Ssl_version(stat)		
Ssl_session_cache_mode(stat)	NONE	NONE
Ssl_server_not_before(stat)		
Ssl_server_not_after(stat)		
Ssl_cipher_list(stat)		
Ssl_cipher(stat)		
Slave_running(stat)	OFF	OFF
Rpl_status(stat)	AUTH_MASTER	AUTH_MASTER
Rpl_semi_sync_slave_status(stat)	OFF	OFF
Rpl_semi_sync_master_status(stat)	OFF	OFF
InnoDB_have_punch_hole(stat)	ON	ON
InnoDB_have_snappy(stat)	ON	ON
InnoDB_have_bzip2(stat)	OFF	OFF
InnoDB_have_lzma(stat)	OFF	OFF
InnoDB_have_lzo(stat)	OFF	OFF
InnoDB_have_lz4(stat)	ON	ON
InnoDB_buffer_pool_load_incomplete(stat)	OFF	OFF

1. 基準日と比較日を設定します。
2. インスタンス項目で目的のインスタンスを選択します。
3.  ボタンをクリックします。

現在と選択した過去の日付との変更点を一目で確認する場合は、**変更を表示**ボタンを選択します。

パラメータ

基準日: 2023/10/04 比較日: 2023/10/10 インスタンス: demo-01

変更を表示

Key	2023/10/04 Value	2023/10/10 Value
wsrep_ready(stat)	ON	OFF
wsrep_cluster_status(stat)	Primary	non-Primary
wsrep_evs_repl_latency(stat)	0.000372136/0.000778795/0.0157565/0.00107258/1859	0/0/0/0/0
wsrep_incoming_addresses(stat)	10.21.1.236:0,10.21.1.86:0,10.21.1.136:0	10.21.1.86:0
wsrep_local_state_comment(stat)	Synced	Initialized
auto_increment_offset	2	1
auto_increment_increment	3	1

🟢 今日の日付のデータベースパラメータを比較する

パラメータ

基準日と**比較日**をすべて今日の日付に設定すると、リアルタイムデータと保存された最後のデータを照会して比較できます。データの最終保存時刻は、データベースサーバーの環境によって異なる場合があります。

メトリクスチャート

ホーム画面 > プロジェクト選択 > 分析 > メトリクスチャート *New*

メトリクスチャート *New* メニューは、WhaTapモニタリングソリューションの主要機能であり、様々なモニタリング対象から収集したデータを時系列チャートで視覚化して提供します。これにより、ユーザーはシステムの性能を効果的にモニタリングし、異常をすばやく識別して、問題解決に必要なインサイトを確認できます。

- 様々なメトリクスを時系列チャートを通じて視覚的に確認でき、障害発生時点の様々なメトリクスを一度に分析できます。
- 特定の時間範囲を選択して過去のデータを照会し、その期間の性能を分析できます。
- 特定の時間帯や条件に合ったデータをフィルタリングすることで、より正確な分析ができます。
- ユーザーは、目的のチャートを画面に配置し、レイアウトを自由に調整できます。
- ユーザーが希望するメトリクスを配置し、プリセットとして保存し、必要に応じて読み込みできます。

❗ 既存のメトリクスチャートメニューとの違い

Service 2.8.0 アップデート以降の変更点は以下の通りです。アップデート後の変更事項を画面で確認するには、右上のチュートリアルボタンを選択します。

- ユーザーが時間、対象、インターバルオプションを設定した後、モニタリングする対象のメトリクスを特定し、チャートを追加できるようにユーザー経験(UX)を改善しました。
- ダッシュボードに配置されたウィジェットを削除することなく、チャートの照会時間の範囲を変更できます。
- ダッシュボードに配置したすべてのウィジェットのオプションを一括で適用できる**一括変更機能**を提供します。
- プリセット機能により、ダッシュボードに配置されたウィジェットの情報を保存し、読み込みできます。
- 提供する様々なオプションにより、ダッシュボードのレイアウトやウィジェットの機能を調整できます。

チャートウィジェットを追加する

ダッシュボードにメトリクスをウィジェットとして追加するには、画面左上の**チャート追加**ボタンを選択します。

照会時間の設定

時間でメトリクスを照会する日付と時間を設定します。

対象を選択する

プロジェクトに含まれるエージェントの中から、対象を選択します。個々のエージェントを選択するか、エージェント設定で分類されたグループ単位で選択できます。



- **エージェント**: 個別エージェントまたはすべてを選択できます。
- **種類別**: エージェント設定で `whatap.okind` に分類されたグループ単位でエージェントをモニタリングします。
- **サーバー別**: エージェント設定で `whatap.onode` に分類されたグループ単位でエージェントをモニタリングします。

- ❗ 設定した時間と日付によって、選択できる対象が変更される場合があります。
- エージェントの一覧からマウスをクリックして、対象を選択または解除できます。Shift キーを使用して複数のエージェントを選択できます。
- **すべて選択**または**すべて解除**ボタンを選択すると、関連する下位対象をすべて選択または解除できます。



す。

- 希望のエージェントが一覧に表示されない場合は、**リフレッシュ**ボタンを選択します。
- **すべて折りたたむ**または**すべて開く**ボタンを選択してグループ単位で一覧を隠したり、展開したりできます。

指標を選択する

モニタリングする対象エージェントを選択した後、**メトリック**パネルに選択できる一覧が表示されます。一覧からご希望のメトリクスを選択します。

選択したメトリクスに対応するチャートウィジェットが右側のダッシュボードに配置されます。他のメトリクスを選択し、チャートウィジェットを追加できます。チャート領域を拡大して見るには、**時間**オプションの右にある**×**ボタンを選択します。**対象とメトリック**パネルが消え、チャート領域のみが画面に表示されます。



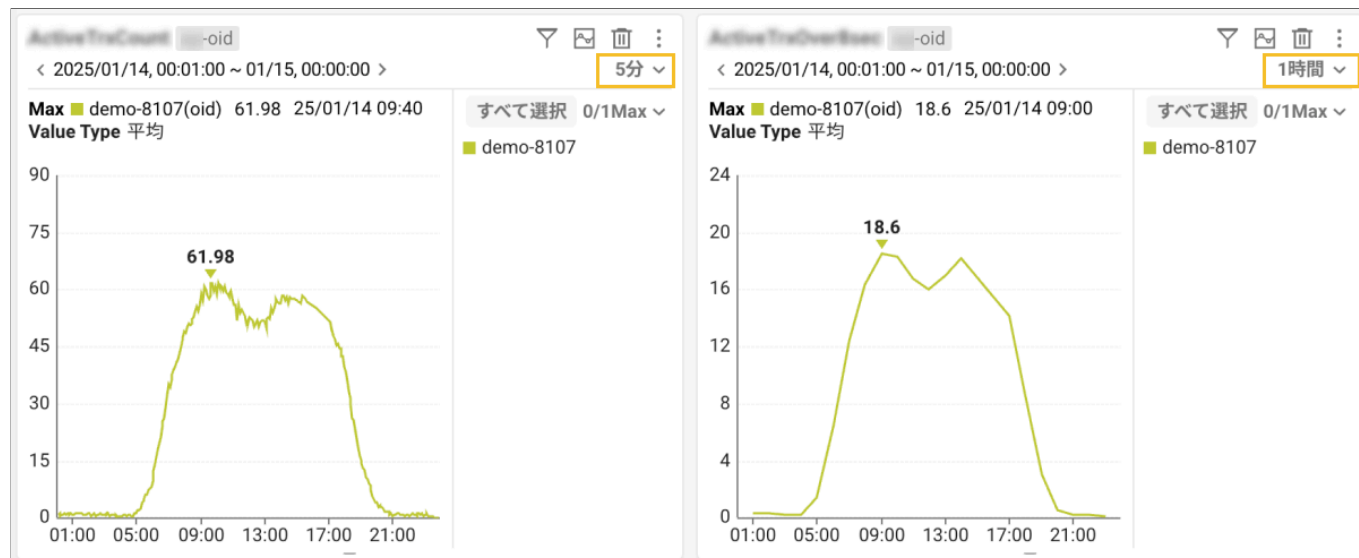
- **指標検索**入力欄に文字列を入力すると、希望のメトリクスをすばやく検索できます。
- **すべて折りたたむ**または**すべて開く**ボタンを選択して、カテゴリ単位でメトリクス一覧を非表示または表示できます。
- 希望するメトリクス項目が一覧に表示されない場合は、**リフレッシュ**ボタンを選択します。

インターバルを設定する

チャートごとにインターバルを設定でき、データの集計単位を調整して、様々な時間間隔のデータを可視化できます。**メトリック**パネルの右上にある**🕒**ボタンを選択すると、**インターバル**オプションを選択できます。

メトリクスごとにデフォルトで設定されたインターバル時間が異なり、照会時間の範囲によってインターバル時間が変更されます。

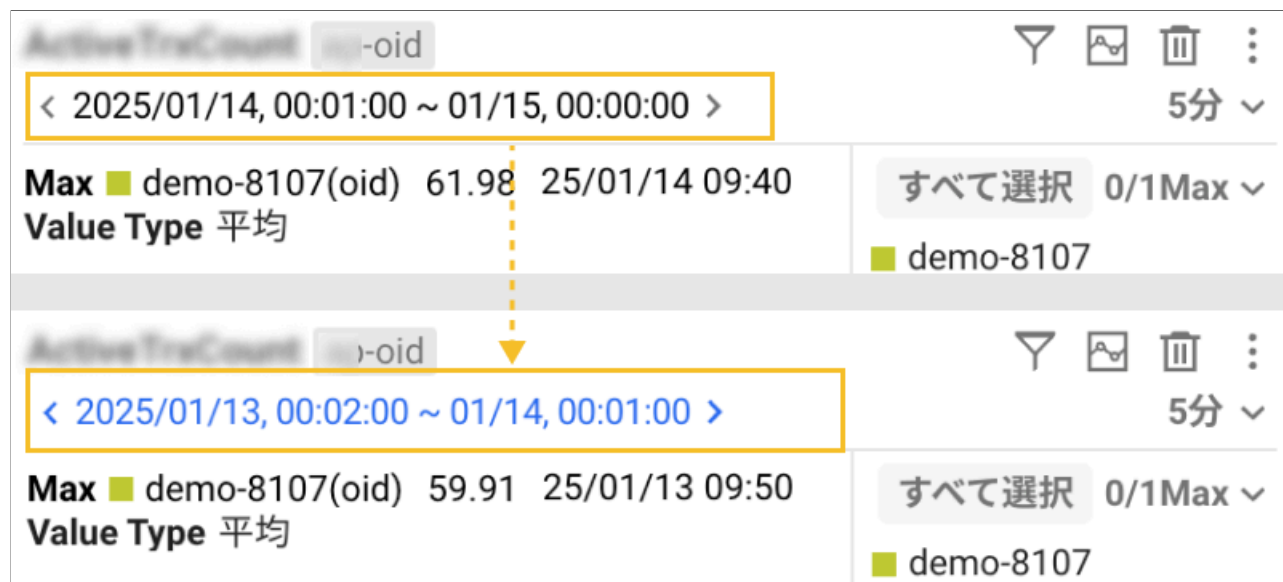
例えば、**5分間**インターバルは5分単位の平均値を表示し、**1時間**インターバルは、1時間単位の平均値を表示します。



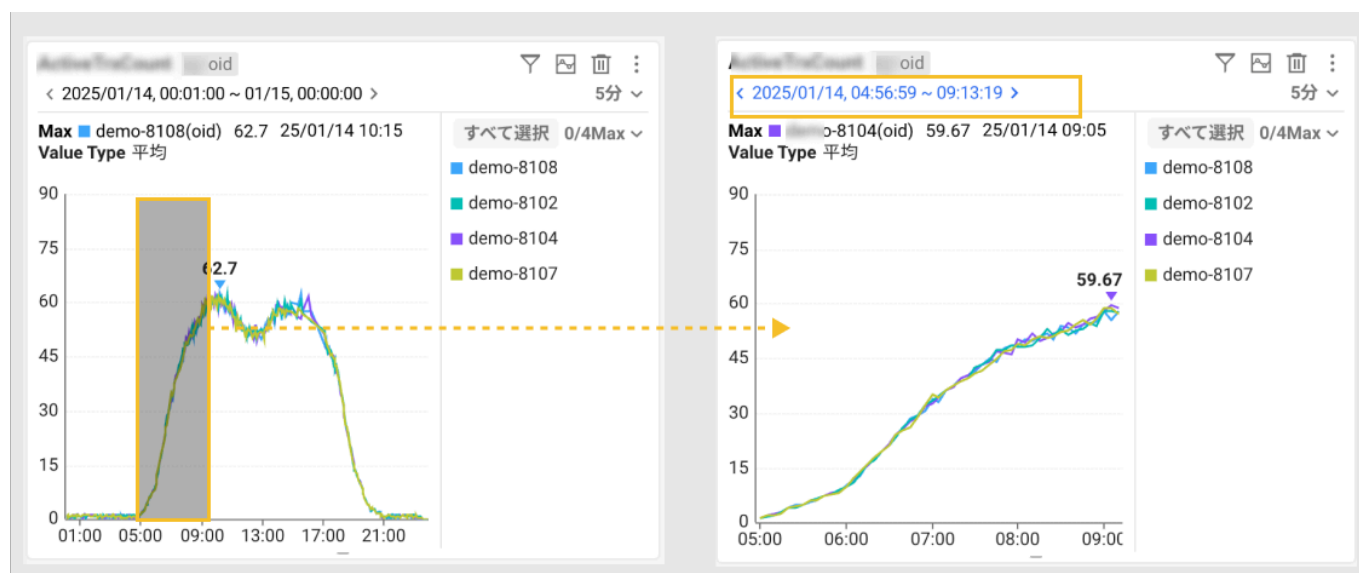
- ✓ インターバルオプションを調整し、短い間隔の詳細データから長い間隔の全体的な推移まで、多様な観点からデータを分析できます。

照会時間を変更する

ウィジェットのチャート照会時間の範囲を変更するには、ウィジェット上部の < または > ボタンを選択します。時間変更範囲は、時間オプションに設定された時間基準と同じです。例えば、時間オプションで1日間に設定されている時、< または > ボタンを選択すると、時間を1日単位で変更できます。



またはチャートの特定領域をドラッグすると、ドラッグした範囲に時間を変更して照会できます。



- ✓ 画面の上部にある**チャート時間の一括適用**オプションを有効にして、ウィジェットの時間を変更すると、すべてのウィジェットの時間を変更できます。



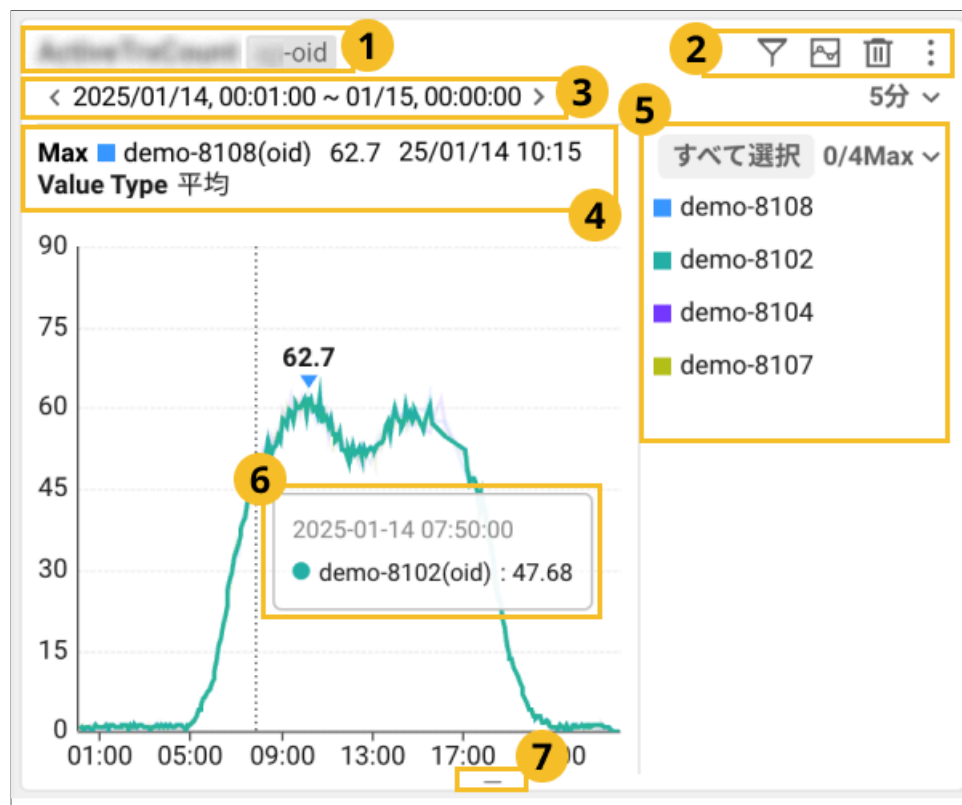
- 照会時間の範囲を変更した後、直近の時間に再度変更するには、 ボタンを選択します。

もし画面の上部にある**チャート時間の一括適用**オプションを有効にした場合、 **時間一括初期化**ボタンが表示されます。このボタンを選択すると、すべてのウィジェットの時間を初期化できます。

- 一括変更機能**を利用してウィジェット全体の時間を変更し、モニタリング対象とインターバルも修正できます。詳細については、[次の文書](#)を参照してください。

チャートウィジェットの詳細

チャートウィジェットに表示される各アイテムの詳細を確認します。



- **① メトリクス名とカテゴリ:** チャートウィジェットのメトリクス名を表示します。メトリクスの右側には、照会対象のカテゴリをタグ形式で表示します。ご利用の商品によりカテゴリ名称は異なる場合がございます。
 - `*oid` : 個々のエージェントを選択した時に表示されます。
 - `project` : プロジェクト単位で対象を選択した時に表示されます。
 - `okind` : エージェント設定で `whatap.okind` で分類されたグループを選択した時に表示されます。
 - `onode` : エージェント設定で、`whatap.onode` で分類されたグループを選択した時に表示されます。
- **② ウィジェットオプション:** チャートウィジェットのオプションメニューです。詳細については、[次の文書](#)を参照してください。インターバルオプションの詳細については、[次の文書](#)を参照してください。
- **③ 時間:** チャートのデータを照会する時間範囲を表示します。 < または > ボタンを選択して照会時間範囲を調整できます。
- **④ データ:** モニタリング対象のうち照会したデータの最大値(Max)とデータ結合方式(Value Type)を確認できます。
- **⑤ 凡例:** モニタリング対象を凡例として表示します。凡例表示の詳細については[次の文書](#)を参照してください。
- **⑥ チャート:** 照会したデータを時系列グラフで表示します。マウスをグラフの上にかざすと、詳細な情報を確認できます。チャートの特定領域をドラッグすると、ドラッグした範囲に時間を変更して照会できます。

- **7 サイズ調整:** チャートウィジェットの真ん中の下部領域をドラッグすると、ウィジェットのサイズを調整できます。

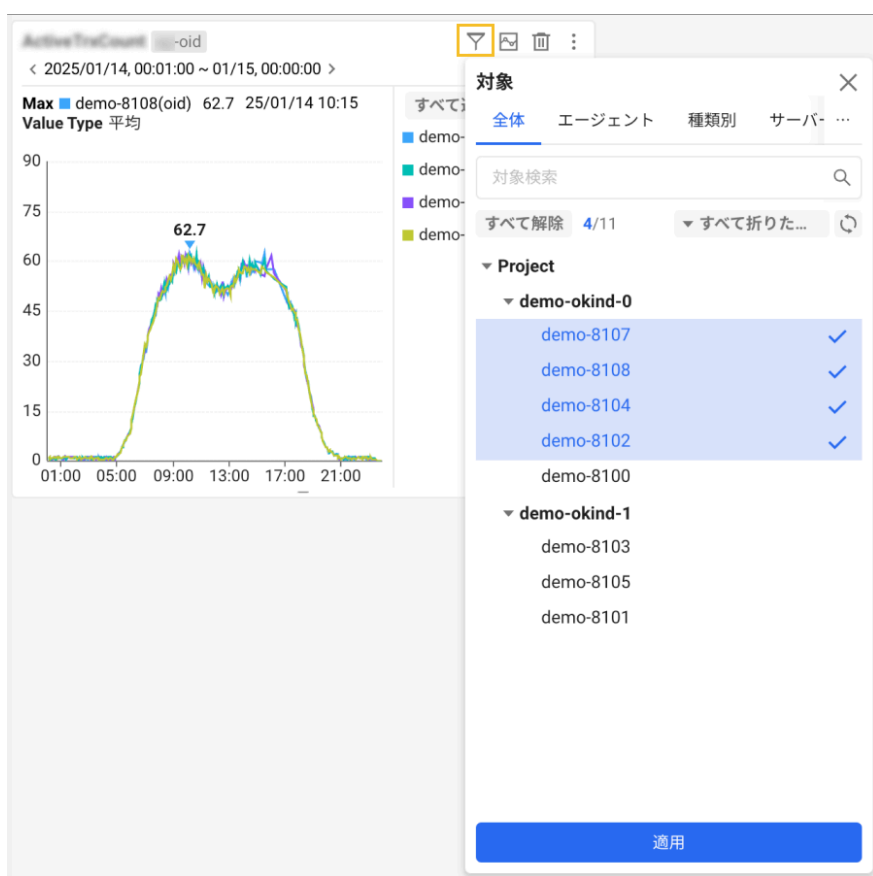
チャートウィジェットオプションを利用する

チャートウィジェットの右上にあるオプションボタンを使用すると、様々な機能が利用できます。

▽対象をフィルタリングする

画面に追加したチャートウィジェットに、モニタリング対象を追加または除外できます。

1. ▽ボタンを選択すると、モニタリング対象を選択できる画面メニューが表示されます。



2. 画面の案内に従って希望する対象を選択します。

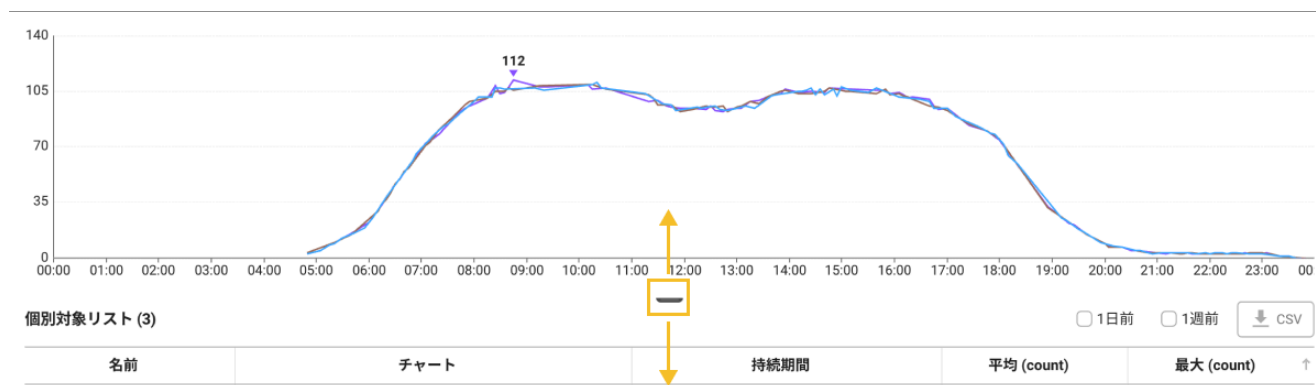
3. 適用ボタンを選択します。

詳細を照会する

チャートのデータをより広い画面で詳細情報を確認するにはボタンを選択します。詳細検索画面が表示されます。個々の対象に対するチャートと平均および最大値を照会できます。



- **1日前**: 1日前のデータと比較して確認できます。
- **1週間前**: 1週間前のデータと比較して確認できます。
- **↓ CSV**: 照会したデータをCSV形式のファイルとしてダウンロードできます。
- グラフチャートの下部にあるアイコンをドラッグすると、チャートのサイズを調整できます。

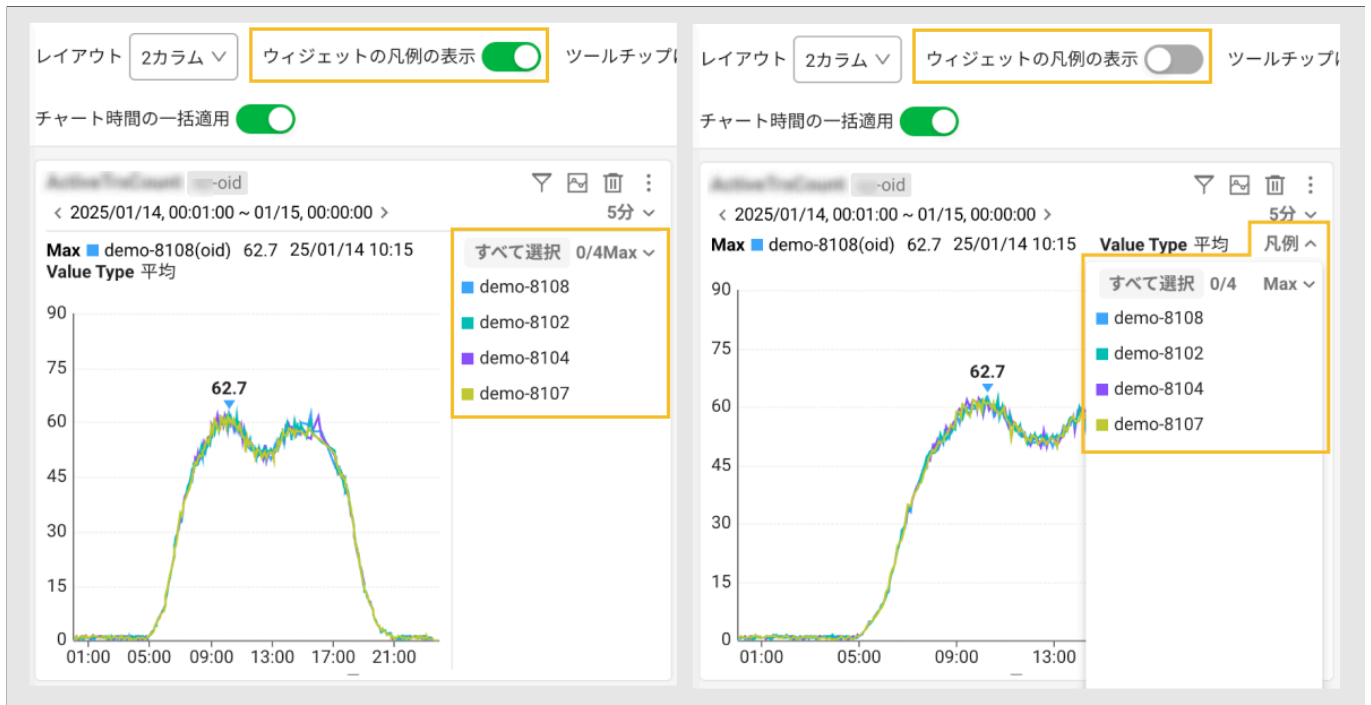


🗑️ チャートウィジェットを削除する

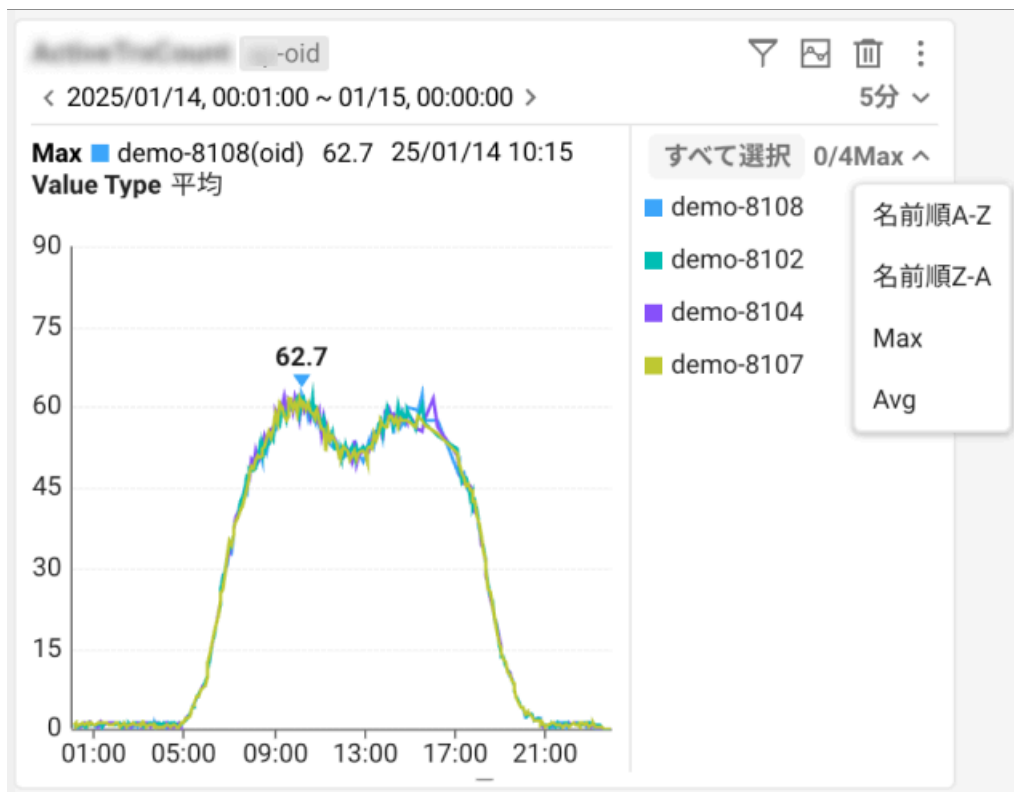
画面に配置したチャートウィジェットを削除するには、🗑️ ボタンを選択します。

凡例を活用する

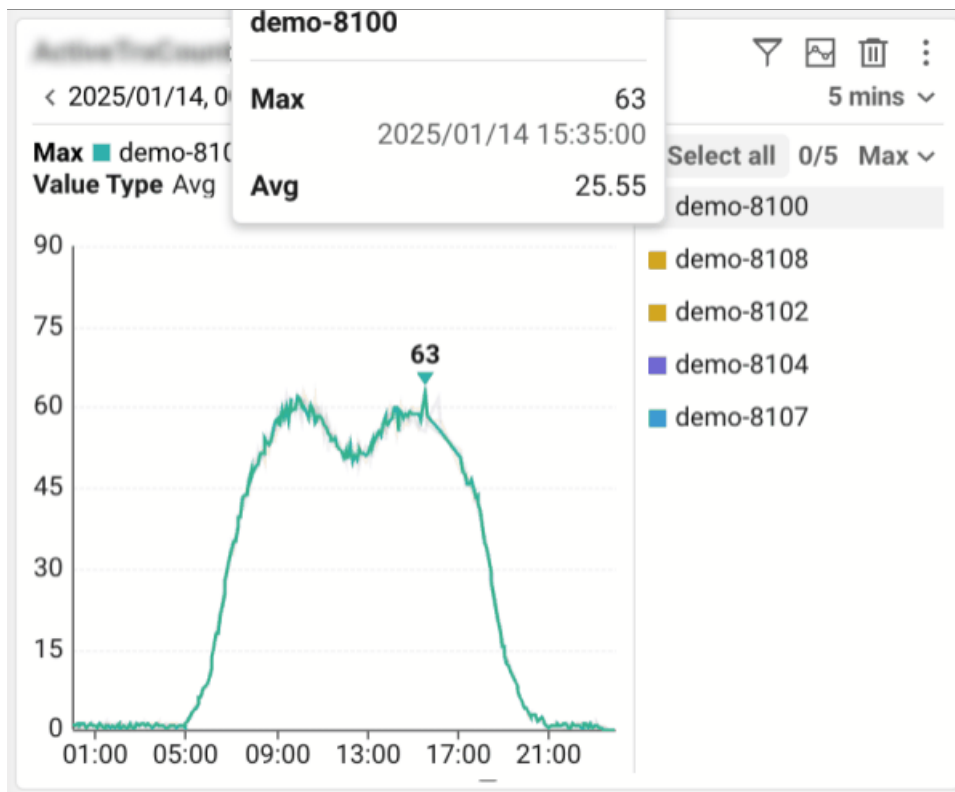
凡例を通じてチャートに表示されるモニタリング対象を確認し、希望する基準で整列したりフィルタリングできます。画面上部のウィジェットの**凡例の表示オプション**をオンまたはオフにすると、ウィジェットのチャートの右側に凡例を表示・非表示できます。オプションをオフにした状態では**凡例**をクリックしてモニタリング対象を確認して選択できます。



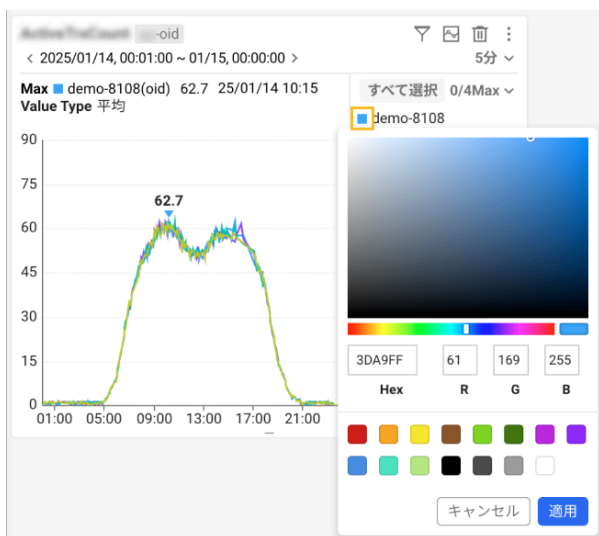
- すべて選択/すべて解除ボタンを選択してモニタリング対象を選択または解除できます。
- 凡例一覧では、モニタリング対象を名前順、最大値、平均値に基づいてソートできます。



- 凡例一覧の各項目にマウスをオーバーすると、そのモニタリング対象に対するグラフを強調して確認でき、Max値が記録された特定時間をツールチップで表示します。または、凡例一覧の対象を選択してもフィルタリングできます。



凡例色を変更する



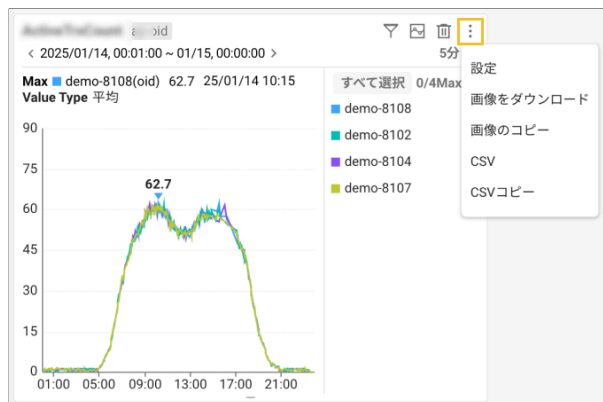
モニタリング対象に該当するグラフの色を変更できます。凡例一覧から色を変更したい対象の左側にある四角い箱

を選択します。希望する色を選択した後**適用**ボタンをクリックします。

- ❗ 設定した色は、プリセット機能によって保存されません。この機能は、今後のアップデートで提供される予定です。

追加オプションを利用する

チャートウィジェット右上にある  ボタンを選択すると、次の追加オプションが利用できます。



- **設定**
 - **自動Y軸を使用:** 照会したデータ範囲内でY軸の大きさを自動調整できます。
 - **最大値表示:** チャートのグラフ領域に最大値を表示できます。
- **画像をダウンロード:** チャートを画像形式のファイルとしてダウンロードできます。
- **画像のコピー:** チャートを画像形式でクリップボードにコピーできます。
- **CSV:** チャートで照会したデータをCSV形式のファイルにダウンロードできます。
- **CSVコピー:** チャートで照会したデータをCSV形式でクリップボードにコピーできます。

プリセットを設定する

ダッシュボードからユーザーが設定したウィジェットの設定とレイアウト状態を保存して読み込むことができます。ウィジェットのサイズを調整し、希望する場所に配置して新しいプリセットを作成できます。

- ❗ プロジェクト修正権限のあるメンバーのみがプリセットを保存または変更できます。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。

新しいプリセットを作成する

1. ダッシュボードから、希望する形にウィジェットを配置してみてください。サイズを変更して、頻繁に確認するウィジェットのみを配置することもできます。
2. 画面の右上に🏠ボタンを選択します。
3. 新しいプリセット名を入力します。



4. 保存ボタンを選択します。

プリセット一覧から新しく保存したプリセットを確認できます。

- ❗
- 新しく作成したプリセットに変更が加えられた場合は、再度プリセットを保存してください。🏠ボタンを選択し、同じ名前でプリセットを保存します。既存のプリセットに変更を上書きします。
 - ダッシュボードの変更を保存せずに別のメニューに移動すると、変更は保存されません。
 - プリセットはプロジェクト単位で保存され、他のユーザーと共有できます。
 - プリセットに保存される対象は、ダッシュボードのレイアウトとダッシュボードに配置したウィジェット、ウィジェットで修正したオプション(対象, 間隔)です。画面上部の時間オプションは保存されません。

- ❗ プリセットを読み込んでからウィジェットの照会時間を変更するには、**一括変更機能**を利用します。詳細については、[次の文書](#)を参照してください。

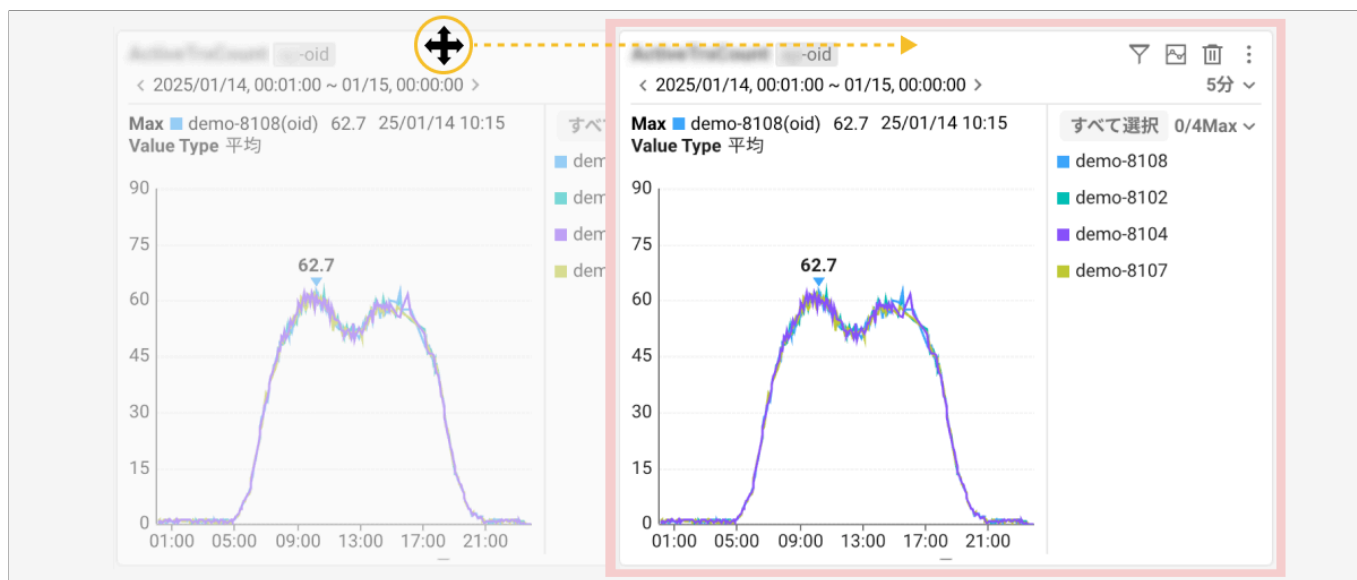
プリセットを削除する

使用していないプリセットは、プリセット一覧から削除できます。プリセット一覧から削除する項目の右側にある×ボタンを選択します。

ダッシュボードウィジェットの編集

ダッシュボードに配置したウィジェットをユーザーが希望する場所に配置したり、サイズを調整できます。

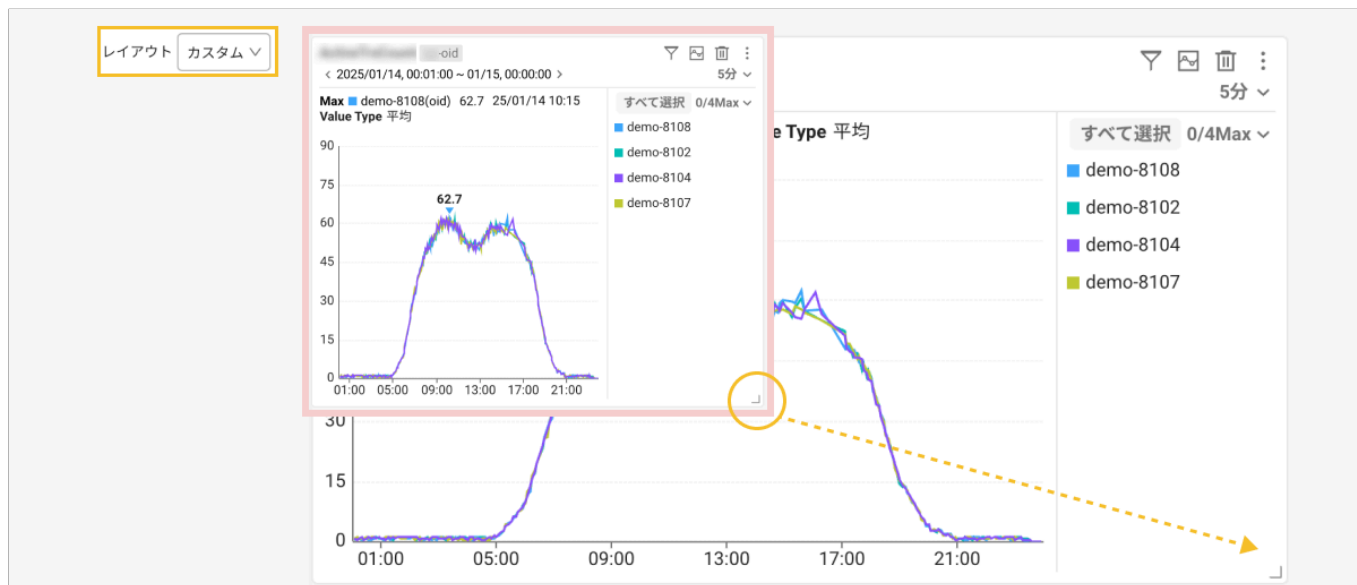
ウィジェットの移動



ウィジェットの上部にマウスをかざすと、**+**に変更されます。この時、クリックしたまま希望の位置にドラッグするとウィジェットを移動できます。

ウィジェットのサイズ変更

ダッシュボードオプションのレイアウトがカスタムに設定されていると、ウィジェットのサイズを調整できます。



ウィジェットの右下にある「」をマウスでクリックした状態で希望するサイズにドラッグします。

- ⓘ レイアウトがカスタムに設定されていない場合は、ウィジェットの高さだけを調整できます。ウィジェットの真ん中の下部領域をマウスでクリックしたままサイズを調整します。

ダッシュボードオプションを利用する

画面上部にあるオプションメニューを利用して、チャートウィジェットに適用された様々な設定を一度に適用できます。また、ダッシュボードのレイアウトを希望する形に設定できます。



チャートウィジェットオプションを一括変更する

画面に配置されたチャートウィジェットに、詳細オプションを一度に適用できる機能を提供します。画面左上に**一括変更**ボタンを選択します。一括変更画面が表示されたら、オプションを設定し、**適用**ボタンを選択します。

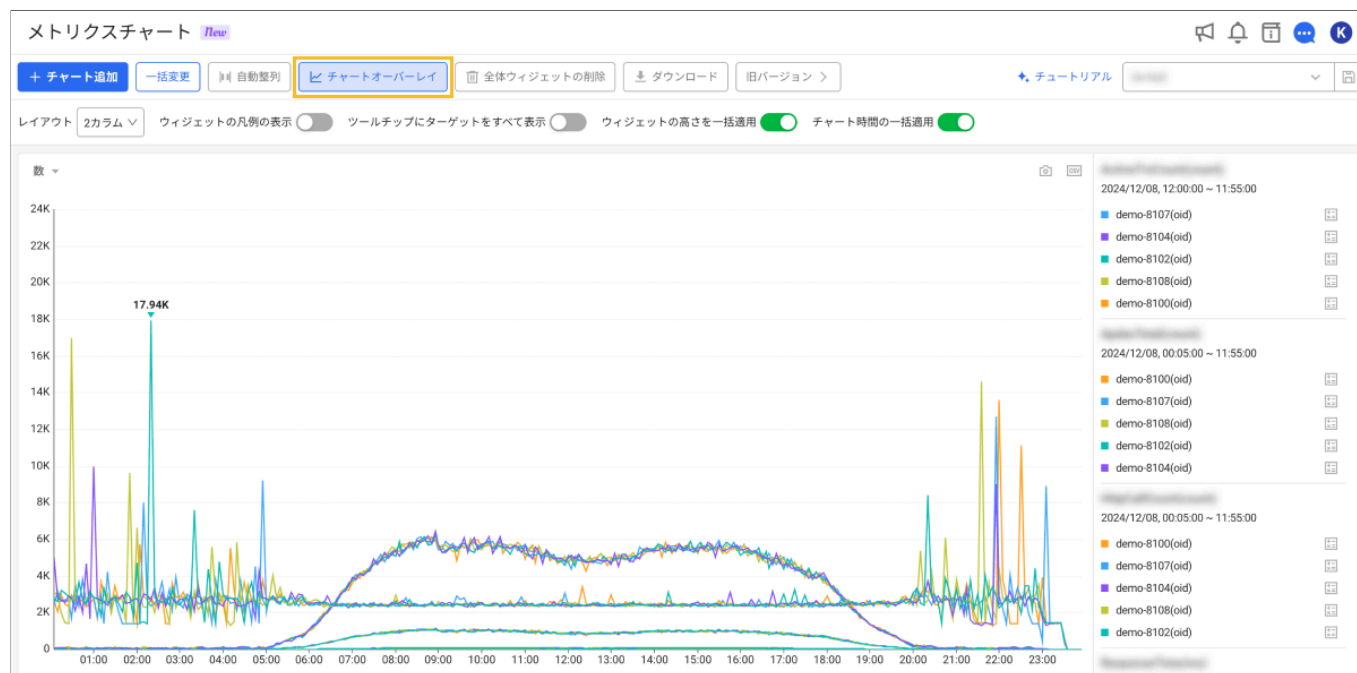
- **時間**: チャートのデータ照会範囲を設定できます。
- **対象**: モニタリング対象を選択します。個々のエージェントを選択したり、エージェント設定を通じて分類したグループ単位で選択できます。
 - **エージェント**: 個別エージェントまたはすべてを選択できます。
 - **種類別**: エージェント設定で `whatap.okind` に分類されたグループ単位でエージェントをモニタリングします。
 - **サーバー別**: エージェント設定で `whatap.onode` に分類されたグループ単位でエージェントをモニタリングします。
- **間隔**: 様々な時間間隔でデータの集計単位を調整できます。
- **適用ウィジェット**: 変更するオプションを適用するチャートウィジェットを選択します。選択したウィジェットに変更したオプションを一度に適用できます。

ダッシュボードを自動ソートする

ダッシュボードに配置したウィジェットの位置を自動的にソートするには**自動整列**ボタンを選択します。ウィジェットの幅、高さが小さい順にウィジェットの配置を自動的にソートします。幅が同じであれば、高さが小さい順にソートします。

複数のチャートを比較する

ダッシュボードに配置した複数のチャートデータを1つのチャートで確認できる機能です。この機能により、同時間帯の様々なメトリクス情報を他のメトリクスと比較しながら確認できます。**チャートオーバーレイ**ボタンを選択します。画面にオーバーレイチャートを配置できます。



- オーバーレイチャート左上の**数**を選択すると、x軸チャートのデータ基準を変更できる一覧が表示されます。希望する項目を選択して、チャートのデータを比較できます。
- : 照会中のデータに基づいて、チャートを画像形式のファイルとしてダウンロードできます。
- : 照会中のデータに基づいて、チャートをCSV形式のファイルとしてダウンロードできます。
- 右側のセクションでは、メトリクスごとのエージェントの一覧を確認できます。個々のエージェントの色は、チャートのグラフの色と一致します。

配置されたウィジェットを一括削除する

ダッシュボードに配置された複数のウィジェットを一度に削除できます。 **全体ウィジェットの削除**ボタンを選択します。確認メッセージが表示されたら削除ボタンを選択します。

CSVファイルでダウンロードする

ダッシュボードに配置したウィジェットのデータをCSV形式のファイルとしてダウンロードできます。 **ダウンロード > CSV**を選択します。時間帯のメトリクスのデータを確認できます。

イメージファイルでダウンロードする

ダッシュボードに配置されたすべてのウィジェットを1つのイメージファイルでダウンロードできます。 **ダウンロード** > **画像をダウンロード** を選択します。 ダッシュボード画面をそのままイメージで保存できます。

以前のバージョンを利用する

以前のバージョンのメトリクスチャートメニューを利用するには、**旧バージョン**ボタンを選択します。 または **サイトマップ** > **分析** > **メトリクスチャート** **Old** メニューパスで確認できます。

❗ メトリクスチャート **Old** メニューの詳細は、[次の文書](#)を参照してください。

その他のオプションを利用する

次のその他のオプションで、ダッシュボードのレイアウトを調整したり、ウィジェットに適用されたオプションを簡単に一括設定できます。

レイアウト **2カラム** ▼ ウィジェットの凡例の表示 ☒ ツールチップにターゲットをすべて表示 ☐ ウィジェットの高さを一括適用 ☒ チャート時間の一括適用 ☒

- **レイアウト**: ダッシュボードで列の数、つまり1行に配置できるウィジェットの数を設定できます。 最大4列まで設定できます。 **カスタム**を選択すると、列の数に関係なくウィジェットを配置できます。

❗ **カスタム**では、ウィジェットの幅と高さを自由に調整できます。 他のオプションを選択すると、ウィジェットの高さだけを調整できます。

- **ウィジェットの凡例の表示**: オプションをオンまたはオフにすると、ウィジェットのチャートの右側に凡例を表示・非表示できます。 オプションをオフにした状態では**凡例**をクリックしてモニタリング対象を確認して選択できます。 凡例の活用についての詳細は[次の文書](#)を参照してください。
- **ツールチップにターゲットをすべて表示**: チャートにマウスかざすと、そのグラフの位置に該当する値を確認できます。 マウスが位置した時間帯のすべての対象のデータを確認するにはオプションをオンにします。
- **ウィジェットの高さを一括適用**: オプションをオンにすると、すべてのウィジェットの高さを同じく設定できます。

- **チャート時間の一括適用:** チャートウィジェットのデータ照会時間を変更する時、他のウィジェットのチャート時間も一緒に変更するにはオプションをオンにします。

チュートリアルを利用する

画面の右上のチュートリアルボタンを選択すると、[Service 2.8.0](#) アップデート以降の変更を確認できます。

メトリクストレンド分析

メトリクス推移分析 は、過去 30 日以内のメトリクス変化を可視化し、トレンドを比較・分析できる機能です。データベースの主要なパフォーマンス指標を期間別または時間別に照会し、特定の時点や時間帯のパターンを迅速に把握できます。

基本画面

メトリクス推移分析 は、上部の **オプションバー** と下部の **チャート領域** で構成されています。オプションバーで照会範囲と表示メトリクスを選択すると、条件に合ったトレンドグラフが自動的に表示されます。

オプションバー

オプションバーでは、時間範囲の設定、メトリクス選択、プリセット管理などの機能を提供します。

Time Window

特定の時間帯のみのデータを表示したい場合に使用します。
トグルを有効にすると時間範囲入力フィールドが有効になります。デフォルトは無効です。

たとえば、業務時間（09:00～18:00）のデータを分析する場合は、Time Window をオンにして該当時間を指定します。

インスタンス

照会するデータベースインスタンスを選択します。
プロジェクトに接続されたインスタンス一覧が表示され、検索ボックスを使用してインスタンスをすばやく見つけることができます。

メトリクス

表示するメトリクスを選択します。
カテゴリ別にフィールドが一覧表示され、必要な項目を選択して照会できます。

プリセット

頻繁に使用するチャート構成を保存または呼び出すことができます。

- 上部の日付別チャートのクリック状態はプリセットに保存されます。
- 下部の日別トレンドチャートのクリック状態は保存されません。

プリセットの保存

ダッシュボードで設定した指標とレイアウトをプリセットとして保存します。

1. **Time Window**、**メトリクス**などを希望の形で設定します。
2. 画面右上の  アイコンをクリックします。
3. **プリセットとして保存** ウィンドウで名前を入力し、**保存** ボタンをクリックします。

プリセットの呼び出し

1. プリセットドロップダウンリストから保存済みプリセットを選択します。
2. 保存された **Time Window**、**メトリクス**、**チャート**などの設定がそのまま適用されます。

✔ プリセットを保存すると、繰り返し設定することなくすぐに照会できます。

チャート

メトリクス推移分析のチャート領域では、選択したメトリクスの変化を可視化します。

特定期間のトレンド、平均値、最大値などを比較でき、必要に応じて新しいチャートを追加したり不要なチャートを削除できます。

チャートの追加

1. （任意）上部オプションバーで **Time Window** を指定します。
2. **メトリクス** から希望するフィールドを選択します。
3. 画面右上の **+ チャート追加** ボタンをクリックします。

チャートの削除

削除するチャートの右上にある  アイコンをクリックします。

ウィジェット

メトリクス推移分析 の下部チャートは **Interval** と **リンクを開く** 機能を提供します。

これにより特定期間のデータをより詳細に分析したり、該当時間帯の詳細モニタリング画面へ直接移動することができます。

Interval

チャートに表示されるデータの集計単位を変更します。

データを1時間単位または5分単位で照会できます。

デフォルトでは1時間単位の集計データが表示され、より詳細なデータを確認したい場合は5分単位表示に切り替えます。

リンクを開く

チャートの特定時間区間のバーをクリックすると、その時間に移動して該当区間の詳細モニタリングページを開きます。

❗ **リンクを開く** > ボタンは、特定の時間区間のバーをクリックしたときのみ有効になります。
選択した時間帯の詳細な指標を確認できます。

統計/レポート

統計/レポートメニューでは、一定期間累積されたデータをまとめてSQL実行とデータベースサイズの傾向を把握し、運用状況を定期レポートとして受け取ることができます。

画面構成

画面	説明
Top SQL	リソースを多く使用したSQLを実行回数・時間基準で分析
データベースサイズ	データベース容量の増加推移を確認
レポート	サービス利用状況と障害記録を日・週・月単位でレポート

Top SQL

照会期間中のTop SQL一覧を提供します。エージェントが収集したアクティブセッション内のSQLをもとに、WhaTapが実行回数、実行時間などの指標を独自に算出したSQL統計です。負荷の大きいSQLを見つけてチューニングの優先順位を決めるのに役立ちます。

推移チャートで特定の時間帯のSQL発生パターンを視覚的に把握でき、リテラル値を除いたSQLを基準に統計を算出します。

基本オプション

上部フィルター領域で照会条件を設定します。

項目	説明
時間	照会時間範囲を選択
クラスター	照会対象のクラスターを選択
ソート順	Top SQLの選定基準となる指標を選択
照会件数	テーブルに表示する件数を設定
フィールド・フィルター	SQL Textなどのフィールドで条件を設定して一覧を絞り込み

ここで混同しやすいのは上部のセレクターです。MySQL Top SQLは対象**インスタンス**を選びますが、SingleStore Top SQLは対象**クラスター**を選びます。SingleStoreはクラスター単位でSQLを分散処理するため、クラスター基準で統計を集計します。

分析基準タブ

分析基準タブで、Top SQLをどの基準でまとめて見るかを選択します。

タブ	説明
ALL	SQL単位ですぐに確認
DB	データベース単位でSQL負荷を分析
USER	ユーザーアカウント基準でSQL負荷を分析
NODE	ノード（ <code>node_id</code> ）基準でSQL負荷を分析

Top SQL Trendsチャート

選択した指標を基準に、上位SQLの推移を時系列チャートで表示します。どのSQLがどの時間帯に負荷が高いかを一目で確認できます。凡例やチャートをクリックすると、該当するSQLのラインが強調されます。

SQL Listテーブル

照会期間中のTop SQL一覧をテーブルで表示します。

Column	Description
SQL Text	SQL全文（リテラル値を除いた形式）
SQL Hash Value	同一SQLをまとめるハッシュ値
User	実行ユーザー
Execute Count	実行回数
Elapsed Time	累積実行時間
Avg Elapsed Time	平均実行時間
Max Elapsed Time	最大実行時間

クエリ別チャート

テーブル項目の展開ボタンをクリックすると、個別クエリの実行回数と平均実行時間のチャートを確認できます。チャートのバーをクリックすると、その時間帯の[インスタンスモニタリング](#)画面へ移動し、その時点のノード状態とアクティブセッションと一緒に確認できます。

SQL詳細表示

SQLをクリックすると詳細ポップアウトが開きます。ポップアウトは次の領域で構成されます。

領域	説明
Query	SQL全文
SQL Statistics	実行回数・実行時間などの統計
Elapsed Time Trends	実行時間の推移
Plan	実行計画

Plan（実行計画）

Plan領域では、SQLの実行計画をツリーテーブルで表示します。各段階の処理行数（Rows）、ノードコスト（Node Cost）、実行計画（Plans）を段階別に確認できます。

簡単に言うと、実行計画はデータベースがSQLをどのような順序で処理するかを立てた作業計画書です。コストの大きい段階を見つければ、どこで時間がかかっているかを推し量ることができます。

データ解釈ガイド

指標	意味	解釈ポイント
Execute Count	SQLの呼び出し回数	高いほど頻繁に呼び出されるため、最適化の効果が大きい
Elapsed Time	累積実行時間	高いほど全体の負荷が大きいSQL
Avg Elapsed Time	1回あたりの平均実行時間	高いほど個別の実行が遅く、チューニングの優先対象
Max Elapsed Time	最大実行時間	平均との差が大きい場合は断続的な性能低下を疑う

データベースサイズ

データベースサイズ画面では、SingleStoreのデータベースごとの容量が時間に応じてどのように変化するかを確認できます。どのデータベースが急速に大きくなっているかを事前に把握すると、容量計画を立てるのに役立ちます。

基本画面の説明

画面上部で照会するクラスターと期間を選択します。デフォルトの照会範囲は最近7日で、最大3週間まで照会できます。

Item	Description
クラスターセクター	照会対象のクラスターを選択
期間セクター	照会期間を選択（デフォルト最近7日、最大3週間）
データ単位セクター	表示単位を選択（byteベース）
ダウンロード	CSV・Excel形式でエクスポート

サイズ推移チャート

全体容量（TOTAL）とデータベースごとの容量をラインチャートで表示します。単位はデータサイズに合わせてbyteベースで自動表示されます。

詳細表

データベースごとの容量指標を表で表示します。各指標は照会期間の開始値、終了値、変化量を併せて表示し、増減を一目で比較できます。全体合計（TOTAL）行は強調して表示します。

レポート

ホーム画面 > プロジェクト選択 > 統計/レポート > レポート

画面の上に**レポート**で▽ボタンをクリックすると、日刊、週刊、月刊に分類された各種分析レポートを確認できます。希望するレポート様式を選択し、照会したい日付と時間、フィルターオプションを設定してください。 ボタンを選択すると、選択したレポートを確認できます。

レポートは、個々のプロジェクトのサービスの使用状況と障害の発生履歴を報告する文書です。サービスモニタリング担当者は、レポートを通じて関連部署の担当者とステータスを共有します。

モニタリングデータ分析は、サービスの改善方向を定める指標となるため、極めて重要です。ただし、複数のダッシュボードからデータを収集して文書化するには煩雑な場合があります。

WhaTapの**レポートメニュー**は、**レポート作成業務の自動化**をサポートします。毎週報告書を作成すること、決まった時間に報告書を共有すること、様々な書式を管理することなど、すべて**レポートメニュー**から解決できます。

✔ レポートダウンロード

レポートのダウンロード、印刷またはメール送信の予約を希望する場合は ダウンロードボタンをクリックしてください。html形式でダウンロードできます。

レポートの種類

基本レポートは、大手企業、公共機関やITサービス企業などで実際に使用しているフォームです。ご要望のフォームを作成したい場合は、support@whatap.ioまでお問い合わせください。要望されたレポートは、**統計/レポート > レポート一覧**に追加されます。

メール送信予約

定期的にレポートをメールで受信する場合は、**レポートのメール送信予約**を選択します。出社直後行っていたサービスのチェック作業をメール確認で代わりにできます。

レポートのメール送信予約

×

① 登録した翌日の04~06時にレポートが送信されます。

② 最大5件までのレポート送信が予約できます。

レポートタイプ

レポート時刻

00:00

~

23:59

送信曜日

☒ Mon

☒ Tue

☒ Wed

☒ Thu

☒ Fri

☐ Sat

☐ Sun

メール

メールを入力してからEnterする

×

+ 保存

目次レポート：データベース

日次データベースレポートは、1日あたりのデータベースのパフォーマンスを数値とチャートで確認できるレポートです。レポート作成時に必要に応じて開始日、開始時間、終了時間を設定することができます。特定のインスタンスのみ選択して表示することができます。すべてを選択すると、すべてのインスタンスを一度に表示します。

性能推移チャート

データベースインスタンスごとに指標チャートを確認できます。各指標の最大値を円形で表示し、最大値が発生した時間をまとめて表示します。

- ① チャートで表現される指標は、Config設定によって異なる場合があります。
- 各チャートの右上にあるCSVボタンを使用して、データをエクセルファイルとしてダウンロードすることができます。

SQL TOP 10

検索期間中に全体または選択したインスタンスが実行したSQLクエリ統計を確認できます。クエリ実行時間の最大値を降順にソートし、上位10項目のみ表示します。

週次レポート：データベース

週次データベースレポートは、1週間のデータベースのパフォーマンスを数値とチャートで確認できるレポートです。開始日を直接設定することができ、参照日の7日前から表示できます。

性能推移チャート

データベースインスタンスごとに、週間指標を数値およびチャートで比較できます。検索期間の最大値を円形で表示し、その数値が発生した時間も表示されます。

- ① • チャートで表現される指標は、Config設定によって異なる場合があります。
- 各チャートの右上にある[CSV](#)ボタンを使用して、データをエクセルファイルとしてダウンロードすることができます。

SQL TOP 10

検索期間に全体または選択したインスタンスが実行したSQLクエリ統計を確認できます。クエリ実行時間の最大値(elapse max)を降順にソートし、上位10項目のみを表示します。

月次レポート：データベース

月間のデータベースの性能を数値とチャートで確認できるレポートです。開始日を設定でき、開始日から30日まで表示できます。月間の各指標別の変化量をインスタンス別に確認することができ、検索期間中に実行した上位10項目のSQLクエリ統計も確認できます。

ログ

WhaTapのログモニタリングは、システム統合を通じて、優れた利便性とログデータへのスムーズなアクセスを提供します。独自の技術力による確実なデータ収集を強みとし、ライブテール、ログトレンド、ログ検索、イベント通知、パーサーなどの主要機能をより効率的に活用いただけます。

ログメニューは、照会およびクエリの分析とオプション設定などの機能を提供します。イベント設定メニューでは、ログ関連のイベント通知が設定できます。

- ホーム画面 > プロジェクト選択 > ログ

WhaTapモニタリングサービスのメイン画面からプロジェクトを選択し、プロジェクトメニューにあるログメニューを選択します。次の機能を活用すると、複雑なログにより簡単にアクセスができ、様々な条件でリアルタイムに確認および分析ができます。

- ログTail
- ログトレンド
- ログ検索

- 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

WhaTapモニタリングサービスのメイン画面でプロジェクトを選択し、プロジェクトメニューにあるアラート通知メニューを選択し、イベント設定メニューを開きます。イベント条件を設定し、メール、SMS、メッセージャー、App Pushなどの様々な方法で通知を受信できます。

WhaTapログモニタリングサービスの主要なメニューガイドを次のように提供します。

ライブテール

ログモニタリングのライブテールについて説明します。

ログエクスプローラー

ログモニタリングのログエクスプローラーメニューについて案内します。

ログトレンド

ログモニタリングのログトレンドメニューについて案内します。

ログの設定

ログモニタリングの設定方法について説明します。

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

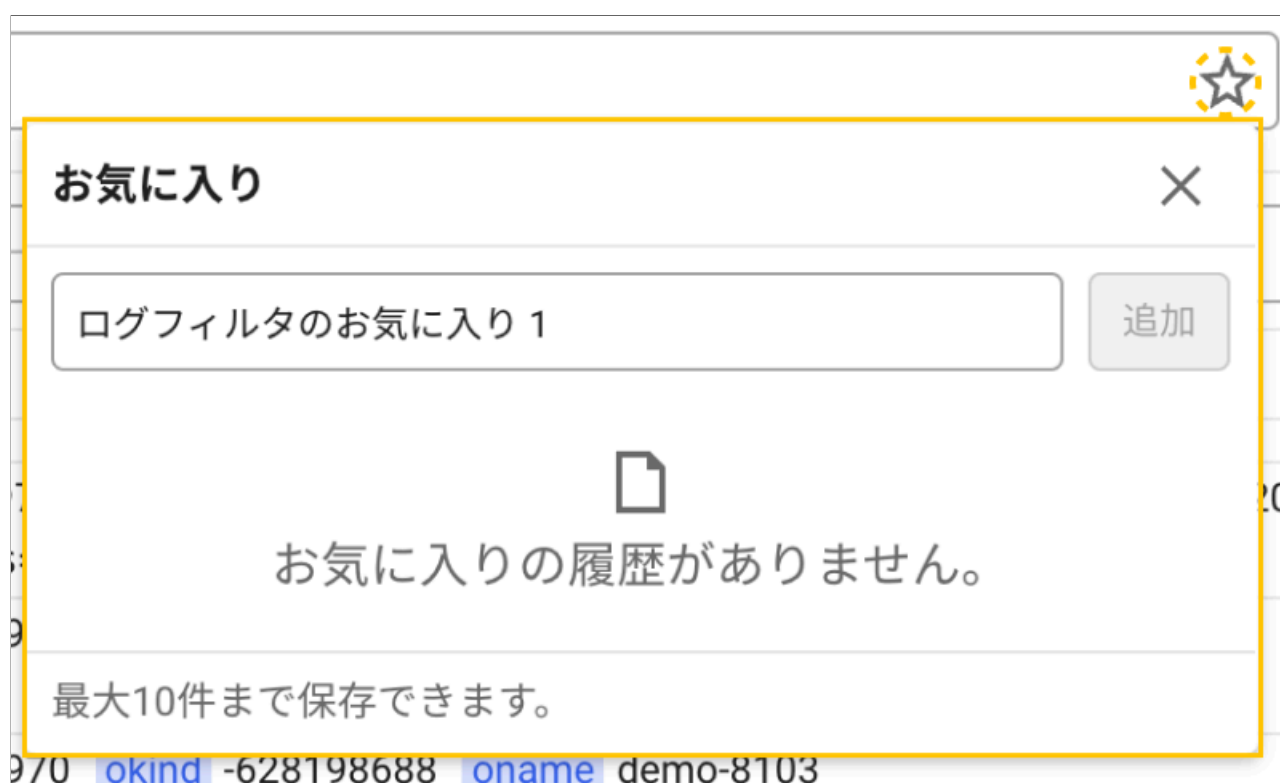
入力フィールドにテキストを入力し、Enter または Tab キーを押すか、入力欄下のガイド UI で推奨値をクリックまたは矢印キーで選択して追加できます。

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。

パーシ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。

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)

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

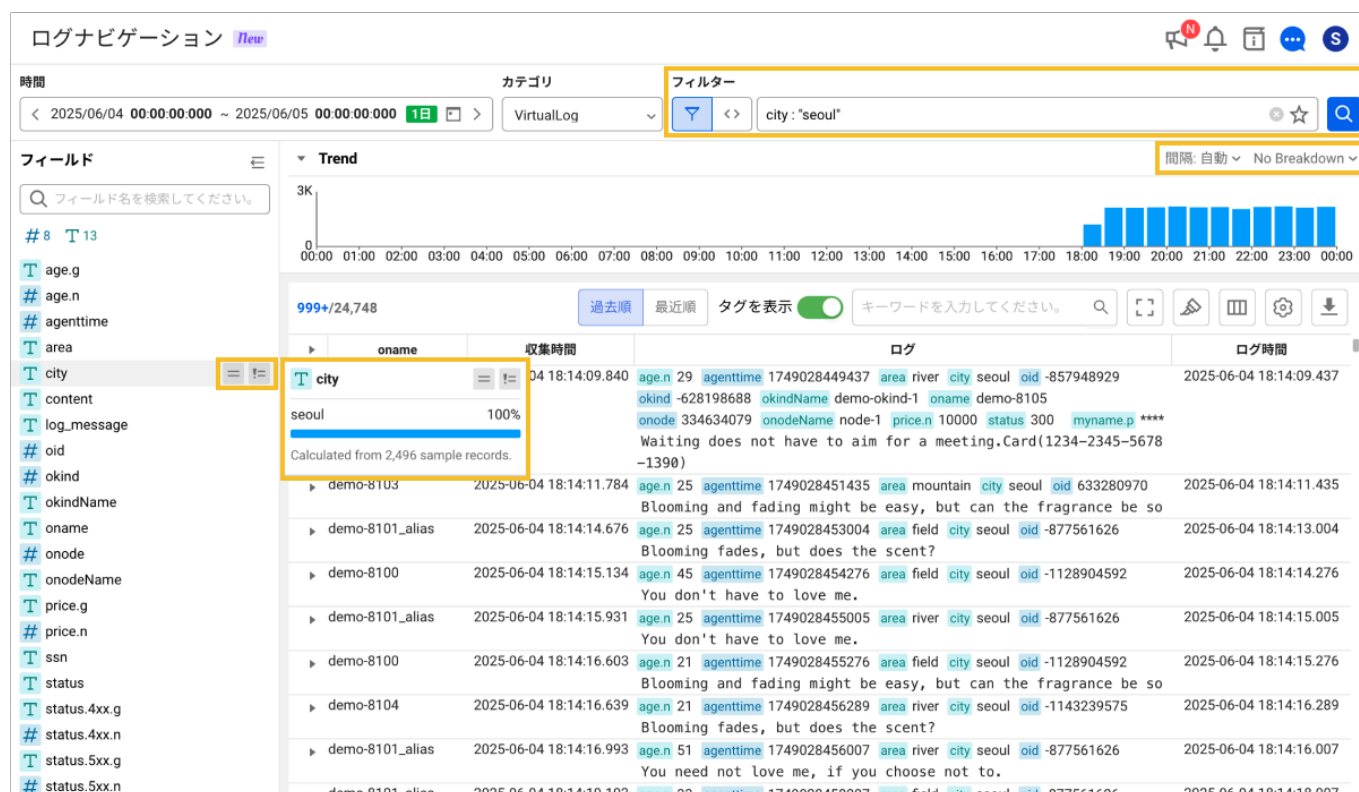
ⓘ ログ参照権限がない場合は、そのメニューにアクセスできません。

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**タイムセクター**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
 - `↑ / ↓` 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。

ログトレンド

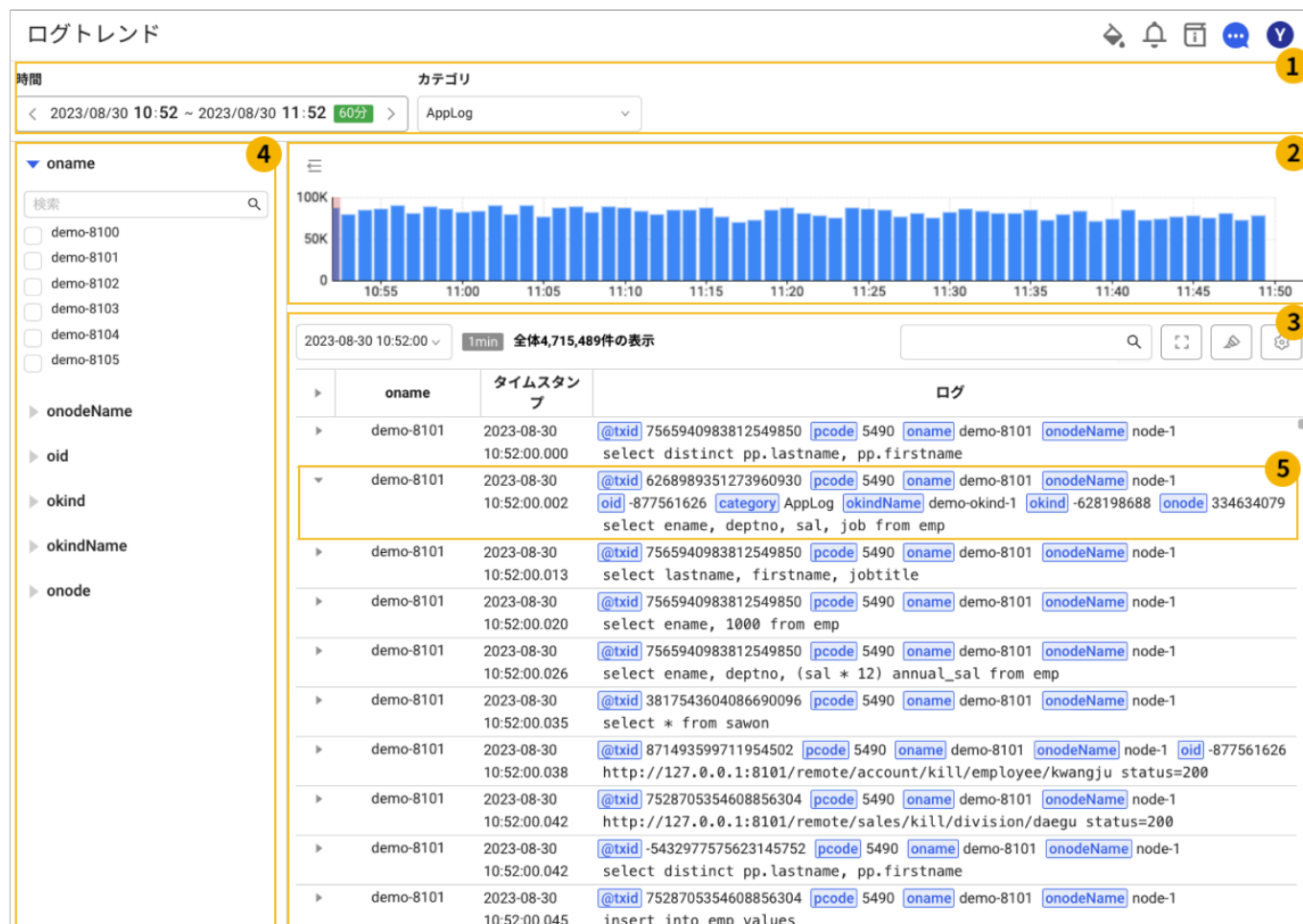
ⓘ ログ参照権限がない場合は、そのメニューにアクセスできません。

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。

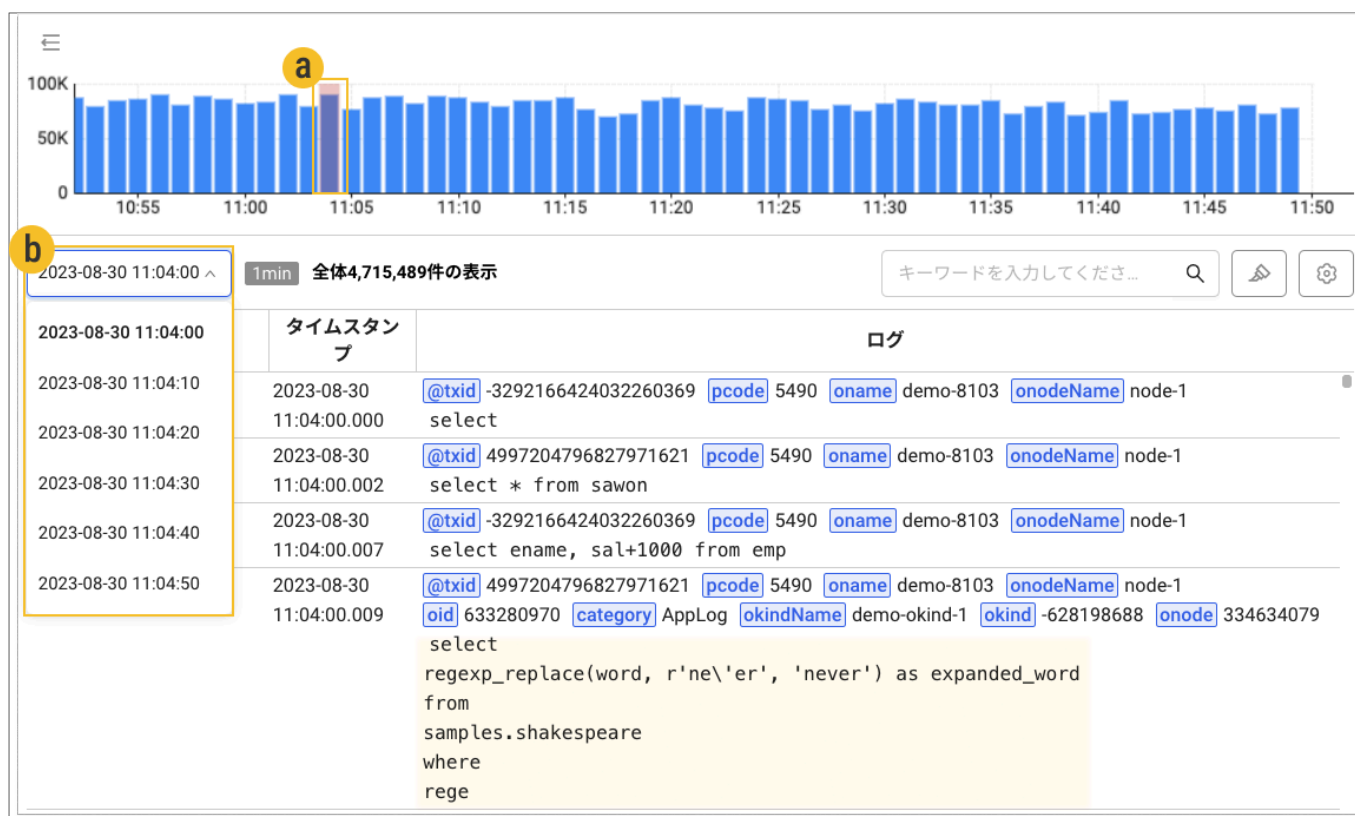
入力文字列	説明	結果
a b c	各キーワードをスペースで区切ります。	a, b, c
"Whatap is good."	キーワードにスペースを含める場合は、" または "" で囲みます。	Whatap is good.
"Whatap\\ is good."	""で囲まれたキーワードに、\ を含める場合は、\\ と入力する必要があります。	Whatap\\ is good.

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

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

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日を選択できます。

- **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。

ログプライマリパーサ設定

ログ設定 上部の **ログプライマリパーサ設定** タブを選択して、収集されたログに対するパーサーを登録できます。

ログプライマリパーサは**GROK**と**JSON**パーサを提供し、タイプ別ログ発生数の集計や特定ログの検索に必須のパーサです。パターン条件に一致する検索キーと検索値を抽出し、パーシングされたキーはログのタイプ分類と検索インデ

ックスに活用します。

- **GROK**：基本的には、正規表現ベースのパーシングに対応します。予約キーワードベースのパーシングを提供します。
- **JSON**：ログからJSONで出力された部分に対して一括パーシング機能を提供します。

✓ パーシングロジックが未登録時に検索可能なkey

category , oid , oname , okind , okindName , @txid , @login , httphost

パーサで登録できない予約語

timestamp , message , pcode , category , content , logContent

- 次の予約語の場合、パーサを登録してもインデックスは作成されません。

❗ ログパーサに関する詳細は[こちらの文書](#)をご覧ください。

設定項目

設定値	説明	その他
カテゴリ	パターンを適用する対象のカテゴリです。	required
ログ検出条件	フィルターとして使用する検索キーと検索値を入力します。 - ログ検出条件に一致するログデータにのみパターンが適用されます。検出条件を入力しない場合、すべてのログにパターンが適用されます。	optional
パターン	ログをパースするためのパターンです。 - 作成したパターンに従ってログをパースし、インデックスを生成します。 GROKおよび正規表現の構文をサポートしています。	required

パーサー一覧

登録済みのパーサーを確認でき、追加や編集が可能です。適用順にパーサーが評価され、最初に一致したパーサーのみが適用されます。

- 右上の*****追加する**ボタンをクリックすると、**パーサ 追加画面**が表示されます。
- 優先順位カラムの📌アイコンをドラッグしてパーサの設定手順を変更できます。
-  **活性化**トグルでパーサの活性化有無を指定できます。
-  **修正**及び  **削除**アイコンで登録したパーサを修正または削除できます。

パーサー登録

以下はパーサーを登録する共通の手順です。

1. **ログプライマリパーサ設定** で **+ 追加する** ボタンをクリックしてください。
2. **パーサ 追加画面**でパーサを選択してください。

❗ パーサーおよびパターンの登録方法

- [GROK パーサおよびパターン登録](#)
- [JSON パーサおよびパターン登録](#)

3. パーサーを選択すると、**パターン登録**ボタンが有効になります。 **パターン登録**ボタンをクリックした後、**パーサーシミュレーション**ウィンドウでパターンとログを入力します。

a. **パターン**を入力してください。

b. **ログのカテゴリ**と**シミュレーション用のパースログ**を入力してください。 **ログ検索**ボタンをクリックした後、検索結果の一覧から目的のログの右側にある**選択**ボタンをクリックすると、ログが自動的に入力されます。

❗ **ログ検索**を使用して、収集されたログの中からサンプルログを選択できます。選択したログはシミュレーション入力欄に自動的に反映され、コピーや貼り付けなしですぐにテストできます。

c. 登録するパターンが正しいかどうかを確認するには、**シミュレーション**ボタンをクリックして、シミュレ

ーションとパターンのパフォーマンスを測定してください。

❗ シミュレーションと性能測定についての詳細は、[次の文書](#)を参照してください。

4. 正常にパースされるかどうかシミュレーション結果を確認した後、**パターン適用**ボタンをクリックしてください。
5. **追加**ボタンをクリックすると、パーサーが追加されます。

❗ 個人情報の非識別化

パーサー登録時に検索キー名を `検索キー.p` に指定すると非識別化の対象になります（例：`myname.p` **）。WhaTapは**個人情報の非識別化**タブで非識別化を管理する方式を勧めます。詳細は[個人情報の非識別化](#)を参照してください。

GROKパーサパターン登録

基本文法は、`%{SYNTAX:SEMANTIC}` です。GROKパーサの詳細は、[次の文書](#)を参照してください。パターン登録とシミュレーションが必須です。

- SYNTAX

GROK定義パターンです。

- SEMANTIC

パーシングされたデータに割り当てるキーです。

❗ SEMANTICでは、予約語ではなく、組み合わせでの使用を推奨します。

JSONフォーマットのパーサパターン登録

ログ全体または一部がJSON形式で出力される場合、JSONフォーマットのパーサを使用して、JSONに出力された部分をパーシングできます。ログのうちJSON形式として出力された部分を検出するために、**Prefix**、**Postfix**オプションを組み合わせでログのどの部分をJSONとして認識してパーシングするかを指定します。JSONパーサの詳細は、[次の文書](#)を参照してください。シミュレーションが必須です。

オプション	説明
Prefix	JSON文字列の先頭の前にある文字列を指定します。未指定時、ログ出力文の先頭からJSON文字列として識別します。
Postfix	JSON文字列の最後の部分の文字列を指定します。未指定時、ログ出力文の最後までをJSON文字列として識別します。
Ignore	JSON出力部分のうちキー抽出を除外するフィールドを指定します。

• 登録例

Log

```
[2022-10-25 10:15:34:145]...(改行)
Request: {"key1":"value1","key2":"value2",...}(改行)
Response: {"key3":"value3","key4":"value4",...}
```

例のように流入されるログがRequest JSON、Response JSONをすべてパーシングする場合、次の2つのパターンを登録します。

- Requestパーシング用のパターン

"Request : "と"Response"間の文字列 {"key1":"value1","key2":"value2",...} 対象

- Responseパーシング用のパターン

"Response : "からログの最後まで文字列 {"key3":"value3","key4":"value4",...} 対象

• JSONカスタムパターンの登録

ログの一部がJSON形式で出力される場合、JSONで出力された部分をカスタムパーサを使用してパーシングできます。パターンを次のように入力します。

```
io.whatap.logsink.parser.JsonFormatParser{}
```

ログのうちJSON形式として出力された部分を検出するために、**Prefix**、**Postfix**オプションを組み合わせでログのどの部分をJSONとして認識してパーシングするかを指定します。

JsonFormatParser{} の {} にオプションを指定します。

登録例

Log

```
[2022-10-25 10:15:34:145]...(改行)
Request:{"key1":"value1","key2":"value2",...}(改行)
Response:{"key3":"value3","key4":"value4",...}
```

例のように流入されるログがRequest JSON、Response JSONをすべてパーシングする場合、次の2つのパターンを登録します。

Requestパーシング用のパターン

"Request："と"Response"間の文字列 {"key1":"value1","key2":"value2",...} 対象

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

Responseパーシング用のパターン

"Response："からログの最後まで文字列 {"key3":"value3","key4":"value4",...} 対象

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

パーサーシミュレーションと性能測定

パーサーシミュレーション後、パターンを登録できます。パフォーマンス測定は、シミュレーション実行対象文字列に対してパーサーの反復パーシング所要時間を測定します。

1. パターンとログを入力します。ログ検索ボタンをクリックした後、検索結果の一覧から目的のログの右側にある選択ボタンをクリックすると、ログが自動的に入力されます。
2. シミュレーションボタンをクリックして、登録しようと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。
3. 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。
4. 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。

パーシングの成功

パーシング ロジックを登録し、キー(key)が生成されたら、ログを照会する際に該当キーでパーシングされた値が追加されます。次のログTailメニュー例のように、パーシングされたキーと値が追加されます。

Timestamp	ログ
2022-08-17 14:28:00.612	oname dev949400-8093 onodeName node-1 oid 413390913 category AppStdOut okindName dev-okind-1 load 52

パーシングされたキーはログTail、ログ検索、ログトレンドで確認できます。

ログセカンダリーパーサ設定

ログ設定メニューの上部にあるログセカンダリーパーサの設定タブを選択してログパーサを登録できます。

ログのセカンダリーパーサは、プライマリーパーサ(GROKまたはJSON)で抽出した値を加工して統計データや新しいフィールドを生成します。HTTPステータスコードベースの統計パーサとともに、キーワードフィルタ、フィールド加工、応答時間分類、GeoIP変換など、さまざまなプロセッサを提供します。

❗ ログのセカンダリーパーサは、1次でパーシングされた結果に対して、追加での2次パーシング機能を提供します。セカンダリーパーサを使用するには、プライマリーパーサを登録する必要があります。

パーサー一覧

ログ設定						
ログモニタリングの開始 ログプライマリーパーサ設定 ログセカンダリーパーサの設定 高速インデックス設定 ログ長期保存統計 1時間の統計ウィジェットのデータ設定のログ						
ログセカンダリーパーサの設定 Grok、またはJSON/パーサがすでに解析された場合に使用できるパーサです。 + 追加する 保存						
優先順位	パーサ	カテゴリ	ログ検出条件	パターン	活性化	
0	4xx、5xx状態コードパーサ	AppStdErr	すべてのログ		☒	✎ ✖
1	状態コード成功率パーサ	AppLog	すべてのログ		☒	✎ ✖

登録したパーサを確認でき、追加および編集が可能です。

パーサの追加、順序変更、活性化トグル、修正および削除などの操作方法はプライマリーパーサー一覧と同一です。

パーサ登録手順

次に、パーサ登録の共通の手順を説明します。

×

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。

パーサを選択してください。

除外する状態コード

パーサを選択してください。

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。

カテゴリを選択してください。

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。

検索キー

検索値

追加

1. **+追加する**ボタンを選択すると**パーサ 追加**画面が表示されます。
2. **パーサ**選択画面からパーサを選択します。各パーサの設定項目の詳細については、次の文書を参照してください。
 - [4xx、5xx状態コードパーサ 設定項目](#)
 - [状態コード成功率パーサ 設定項目](#)
3. **除外する状態コード**を入力します。
4. **カテゴリ**選択画面からカテゴリを選択するか、直接入力します。

5. ログ検出条件を選択するか、直接入力します。
6. 追加ボタンを選択してパーサを登録します。

4xx、5xxステータスコードパーサ設定項目

4xx、5xx状態コードパーサ はプライマリーパーサでパースングされたstatus値を基に4xx、5xx件数データを生成します。特定のステータスコードを除外する場合は、除外するステータスコードを入力してください。

設定項目

設定値	説明	その他
カテゴリ	4xx、5xxの件数データを生成するカテゴリです。	required
ログ検出条件	フィルターとして適用する検索キー、検索値を入力します。ログ検出条件を満たすログデータに対して、4xx、5xxのデータを生成します。ログ検出条件を入力しない場合は、すべてのログのデータを生成します。	optional
除外するステータスコード	統計データの作成時に除外するステータスコードです。入力がなければ、4xx・5xxに該当するすべてのエラーステータスコードを対象に4xx、5xxの件数データを生成します。	optional

statusパーサの登録例

ログプライマリパーサ設定 収集したログに対してパーサを登録することができます。パーサは、順番通り適用され、最初にマッチしたパーサのみが適用されます。 + 追加する 保存						
優先順位	パーサ	カテゴリ	ログ検出条件	パターン	活性化	
0					☐	編集 削除
1					☒	編集 削除
2	GROK	AppLog	すべてのログ	%{NUMBER:status}	☒	編集 削除

流入されるログが `{"msg":"message","status":404}` で、例のようにGROKパーサでstatusをパースングする場合、`status: 404` のようにパースングされます。statusが正しくパースングされることを確認したら、4xx、5xxのステータスコードのパーサから除外するステータスコードを登録します。

データ参照

パーサをすべて登録すると、統合Flexボードに移動してログ 4XX、5XX件数ウィジェットを作成します。

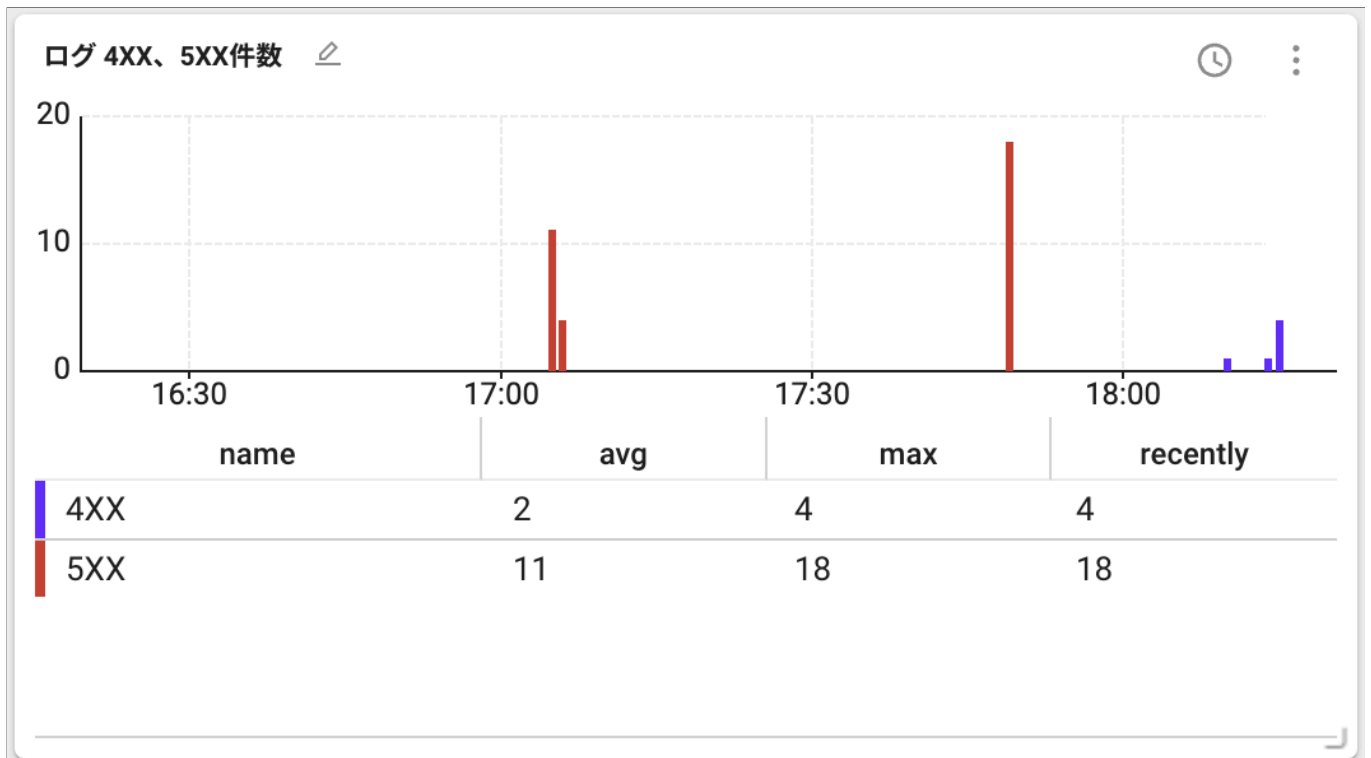
ウィジェットテンプレート

⇒ すべてのメトリックス

4xx

ログ 4XX、5XX件数

ウィジェットを作成すると、次のようにデータを確認できます。



- **avg**：照会期間のデータで平均値です。
- **max**：照会期間のデータで最大値です。
- **recently**：照会期間のデータで最後の値です。

ステータスコード成功率パーサ設定項目

状態コード成功率パーサはプライマリーパーサでパースされたstatus値を基にHTTPリクエスト成功率データを生成します。特定のステータスコードを除外する場合は、除外するステータスコードを入力してください。statusパースに関する内容は、[4xx](#)、[5xxステータスコードパーサ設定項目](#)を参照してください。

設定項目

設定値	説明	その他
カテゴリ	要請成功率データを生成するカテゴリです。	required
ログ検出条件	フィルターとして適用する検索キー、検索値を入力します。ログの検出条件を満たすログデータのみで要請成功率データを生成します。ログ検出条件を入力しない場合は、すべてのログのデータを生成します。	optional
除外するステータスコード	要請成功率データを生成する際に除外するステータスコードです。入力がない場合は、2xx・3xxに該当するすべての成功ステータスコードを対象に要請成功率のデータを生成します。	optional

データ参照

パーサをすべて登録したら、**統合Flexボード**に移動し、ログ要請の成功率ウィジェットを作成します。

ウィジェットテンプレート

⇌ すべてのメトリックス

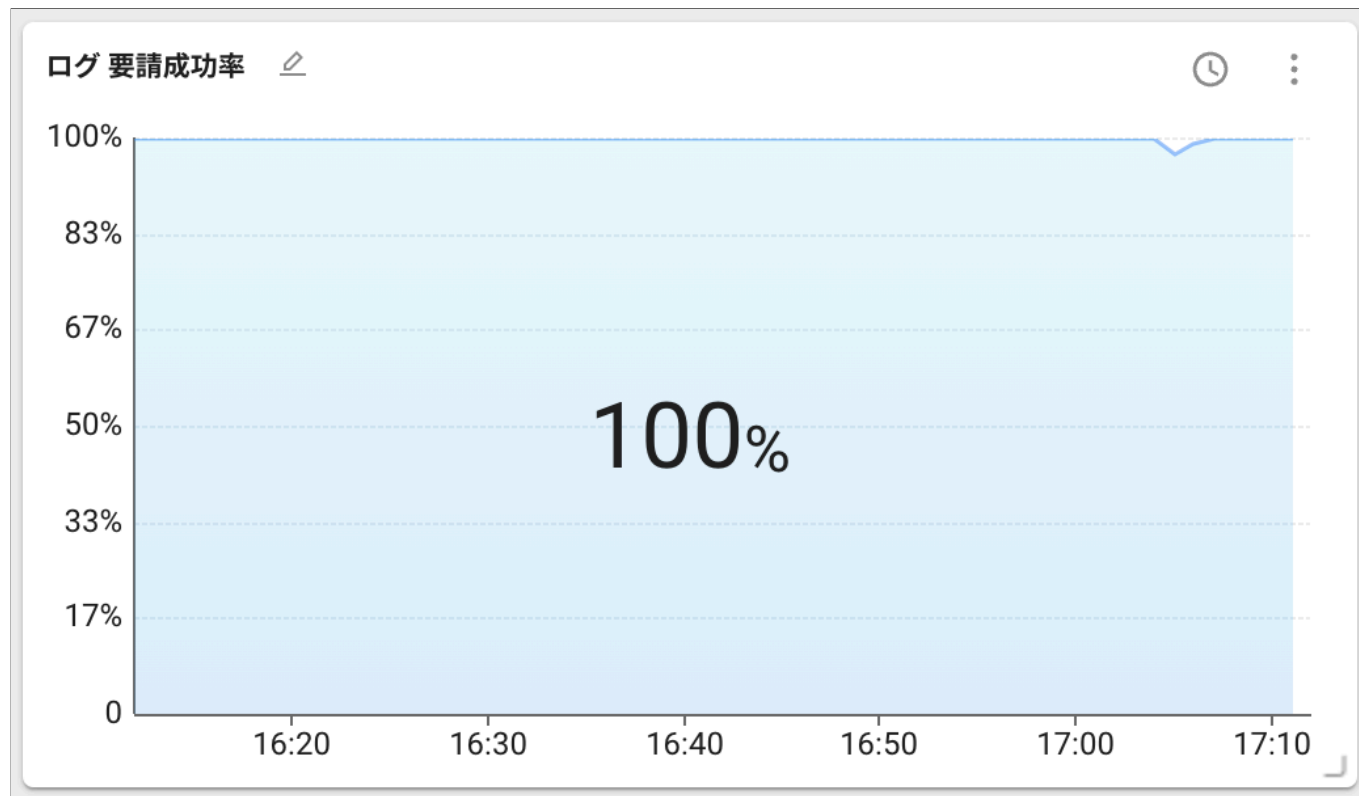
成功率

🔍

📉

ログ 要請成功率

ウィジェットを作成すると、次のようにデータを確認できます。



チャート上のデータは、照会期間に関する統計を示します。統計方法としては最近値、最大値、平均値などを選択できます。最近使った値がデフォルトで選択されています。

セカンダリーパーサプロセッサ

ログのセカンダリーパーサは、4xx、5xx状態コードパーサ と状態コード成功率パーサ のほかにも、次のようなフィールド加工プロセッサを提供します。

ログのセカンダリーパーサプロセッサ一覧

プロセッサ	説明
すべてのキーワード含有フィルタ	指定したすべてのキーワードが含まれるログにフラグフィールドを追加します。
一部キーワード含有フィルタ	指定したキーワードのうち1つでも含まれるログにフラグフィールドを追加します。

プロセッサ	説明
フィールド名変更	既存のフィールド名を別の名前に変更します。
ステータスコードグループ分類	HTTPステータスコードを2xx/3xx/4xx/5xxグループに自動分類します。
URL静的/動的分類	URLに拡張子(.)があれば静的コンテンツ、なければ動的サブリットに分類します。
URLパラメータ除去	URLから?以降のクエリパラメータを除去した値を保存します。
応答時間分類	応答時間(ms)をfast/normal/slow/critical区間に自動分類します。
JSONフィールド抽出	JSON文字列フィールドから特定のキーを抽出して新しいフィールドとして保存します。
GeoIP変換	IPアドレスを国/都市情報に変換します。
直接入力	FQNクラス名でプロセッサを直接登録します。

すべてのキーワード含有フィルタ

指定したすべてのキーワードが含まれるログにフラグフィールドを追加します。

設定値	説明	デフォルト値
入力フィールド	キーワードを検索するフィールド名	content
保存フィールド	結果を保存するフィールド名	has_str_all
keyword	検索するキーワード一覧(カンマで区切って入力)	required

活用例: 入力フィールドを content 、キーワードを error, timeout, database に設定すると、3つのキーワードがすべて含まれるログにのみ has_str_all フィールドが追加されます。

一部キーワード含有フィルタ

指定したキーワードのうち1つでも含まれるログにフラグフィールドを追加します。

設定値	説明	デフォルト値
入力フィールド	キーワードを検索するフィールド名	content
保存フィールド	結果を保存するフィールド名	has_str_any
keyword	検索するキーワード一覧(カンマで区切って入力)	required

活用例: 入力フィールドを `content`、キーワードを `reboot, shutdown, restart` に設定すると、キーワードのうち1つでも含まれるログに `has_str_any` フィールドが追加されます。

フィールド名変更

既存のフィールド名を別の名前に変更します。対象のフィールド名がすでに存在する場合は上書きしません。

設定値	説明	デフォルト値
元のフィールド	変更する既存のフィールド名	required
新しいフィールド名	変更後のフィールド名	required

ステータスコードグループ分類

HTTPステータスコードを `status_2xx`、`status_3xx`、`status_4xx`、`status_5xx` グループに自動分類します。

設定値	説明	デフォルト値
入力フィールド	ステータスコードが入ったフィールド名	status
保存フィールド	グループ分類結果を保存するフィールド名	status_nxx

活用例: `status` 値が `404` の場合、`status_nxx` フィールドに `status_4xx` が保存されます。

URL静的/動的分類

URLに拡張子(.)が含まれていれば静的コンテンツ、含まれていなければ動的サブレットに分類します。

設定値	説明	デフォルト値
入力フィールド	URLが入ったフィールド名	url
保存フィールド	分類結果を保存するフィールド名	url_type

URLパラメータ除去

URLから ? 以降のクエリパラメータを除去したパスのみを保存します。

設定値	説明	デフォルト値
入力フィールド	URLが入ったフィールド名	url
保存フィールド	パラメータ除去結果を保存するフィールド名	url_without_params

活用例: /api/v1/users?page=1&size=20 → url_without_params フィールドに /api/v1/users が保存されます。

応答時間分類

応答時間(ms)を区間別に自動分類します。区間のしきい値を直接設定できます。

設定値	説明	デフォルト値
入力フィールド	応答時間(ms)が入ったフィールド名	elapsed
保存フィールド	分類結果を保存するフィールド名	response_class
Fast上限(ms)	fast区間の上限値	100
Normal上限(ms)	normal区間の上限値	500

設定値	説明	デフォルト値
Slow上限(ms)	slow区間の上限値	2000

デフォルト値基準の分類結果は次のとおりです。

応答時間	分類
0 ~ 100ms	fast
101 ~ 500ms	normal
501 ~ 2000ms	slow
2001ms以上	critical

活用例: ログ探索で `response_class: critical` でフィルタリングすると、応答時間が2秒を超えるログのみを照会できます。

JSONフィールド抽出

プライマリーパーサで抽出したフィールドにJSON文字列が含まれる場合、該当のJSONから特定のキーを抽出して新しいフィールドとして保存します。

設定値	説明	デフォルト値
入力フィールド	JSON文字列が入ったフィールド名	payload
抽出するキー	抽出するJSONキー一覧(カンマで区切って入力)	required
保存プレフィックス	抽出されたキー名の前に付けるプレフィックス(例: <code>json_</code>)	optional

- ① ログ全体がJSONの場合、1次JSONパーサが自動的にパーシングします。このプロセッサは、**GROK 1次パーサ**使用時にテキストログ内に含まれるJSON部分を追加でパーシングする際に便利です。
- パフォーマンス保護のため、JSONフィールドサイズが10KBを超えるとパーシングをスキップします。

活用例

1次GROKパーシング結果

```
payload = {"user": "alice", "action": "purchase", "product": "laptop", "amount": 45000}
```

入力フィールド `payload`、抽出するキー `user, action`、保存プレフィックス `pay_` を設定すると、次のように抽出されます。

JSONフィールド抽出結果

```
pay_user = alice
pay_action = purchase
```

GeoIP変換

IPアドレスを国および都市情報に変換します。IP2Locationデータベースを活用して、アクセスログの地域別分析が可能です。

設定値	説明	デフォルト値
入力フィールド	IPアドレスが入ったフィールド名	<code>client_ip</code>
保存プレフィックス	結果フィールド名のプレフィックス	<code>geo</code>

結果として `{プレフィックス}_country`、`{プレフィックス}_city` の2つのフィールドが生成されます。

活用例: 入力フィールド `client_ip` の値が `223.130.195.200` で、保存プレフィックスが `geo` の場合:

GeoIP変換結果

```
geo_country = KR
geo_city = Seongnam
```

直接入力

一覧にないプロセッサをFQN(Fully Qualified Name)クラス名で直接登録できます。

直接入力形式

```
io.whatap.logsink.processor.ClassName{"param1":"value1","param2":"value2"}
```

- ❗ クラス名とパラメータ形式が正確である必要があります。誤った入力の場合、プロセッサが動作しないことがあります。

セカンダリーパーサのチェイニング

同一カテゴリに複数のセカンダリーパーサを登録してチェイニングできます。各プロセッサは登録順に実行されます。

元のログ

```
2026-04-23T10:30:00.123+0900|INFO|api-01|192.168.1.10|/api/v1/orders?detail=true|200|1234|{"user":"alice","action":"purchase"}|Request processed
```

順序	パーサ	入力 → 出力
1次	GROK	timestamp, level, host, client_ip, url, status, elapsed, payload, content
2次-1	JSONフィールド抽出	payload → user, action
2次-2	応答時間分類	elapsed → response_class (slow)
2次-3	ステータスコードグループ分類	status → status_nxx (status_2xx)
2次-4	URLパラメータ除去	url → url_without_params (/api/v1/orders)
2次-5	GeoIP変換	client_ip → geo_country (KR), geo_city (Seoul)

- ❗ セカンダリーパーサの**カテゴリ**は、プライマリーパーサと同一に設定する必要があります。異なるカテゴリに設定すると、該当のログにセカンダリーパーサが適用されません。

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 true)

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。
- 各設定タブで画面右上にJSON  ボタンを選択します。
- 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。
- JSON設定ファイルがユーザーPCに保存されます。
- 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。
- 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。
- 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。

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。 					
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)	☐	 
AppLog	TotalCount	status 200, 300	15日 (約 3 MB)	☐	 
AppLog	TotalCount	status 200, 300	15日 (約 3 MB)	☒	 
AppLog	TotalCount	status 200, 300	15日 (約 3 MB)	☒	 
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

⇒ すべてのメトリックス

ログ長期保存統計



📈 ログ長期保存統計

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。

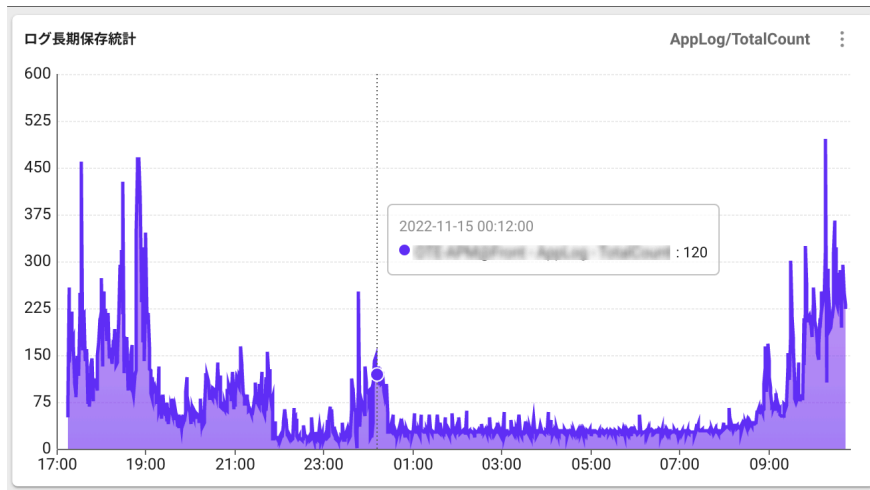
該当ウィジェットに表示するデータ収集のためにはログ長期保存統計 設定が必要です。

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。



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、当該データを非識別化します。

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
[]

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。			
活性化	カテゴリ	検索キー	修正
☐	VirtualLog	age.n	編集 削除
☒	VirtualLog	status	編集 削除
☒	AppLog	agenttime	編集 削除

- 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 [編集](#) 及び [削除](#) 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 ⓘ

カテゴリ

検索開始時刻

検索終了時刻

個人情報項目

個人情報パターン

置換値

パターンのマッチング結果

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

VirtualLog

2025/03/21 12:26

2025/03/21 13:26

個人識別番号

(?<!\w)\d(2)(0[1-9]|1[0-2])|([0-2][0-9]|3[0-1])-[1-4]\d(6)(?\w)

0 ✓ 結果の確認

2025/03/21 13:28

2025/03/21 13:28

No

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。

① **直接入力**選択時に個人情報を識別するための正規表現式パターンを直接入力します。

- 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。
- 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。

① 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。

①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。

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	M1234567	([MSRODTC][0-9]{7}\b)	*****

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
スポーツ番号			
運転免許証番号	01-23-456789-00	(?<!w)d{2}-d{2}-d{6}-d{2}(?!w)	***_**_ *****_**
外国人登録番号	987654-1234567	(?<!w)d{6}-?[5-8]d{6}(?!w)	*****_ *****
クレジット	1234-5678-9012-3456	(?<!w)d{4}-d{4}-d{4}-d{4}(?!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
カード番号			
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,})	***@***.***
銀行口座番号	123456-01-654321	(?<!w)d{6}-d{2}-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
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)	*****_ *****

OpenMetrics

OpenMetricsメニューでは、OpenAgentでPrometheusエンドポイントのカスタムメトリクスを収集し、PromQLで直接探索したり、事前定義されたテンプレートですばやく可視化したりできます。

画面構成

画面	説明
テンプレート一覧	Nginx・Istioなど事前定義された可視化テンプレートを提供
OpenMetricsエクスプローラー	PromQLでカスタムメトリクスを照会・可視化
エージェントのインストール	メトリクス収集のためのOpenAgentをインストール

OpenMetricsテンプレート一覧

OpenMetrics を初めて使用するユーザーが複雑な設定プロセスなしですばやくメトリクスを収集・可視化できるように、基本テンプレートと事前定義されたテンプレートを提供します。これにより、よく使われるオープンソースメトリクスを簡単に適用でき、初期導入の障壁を下げ、運用者が拡張可能なモニタリング環境を構築できるよう支援します。

テンプレート一覧

テンプレート一覧 は基本のオープンソーステンプレートカードを提供します。各カードには簡単な説明、テンプレートへの移動、収集案内が含まれています。

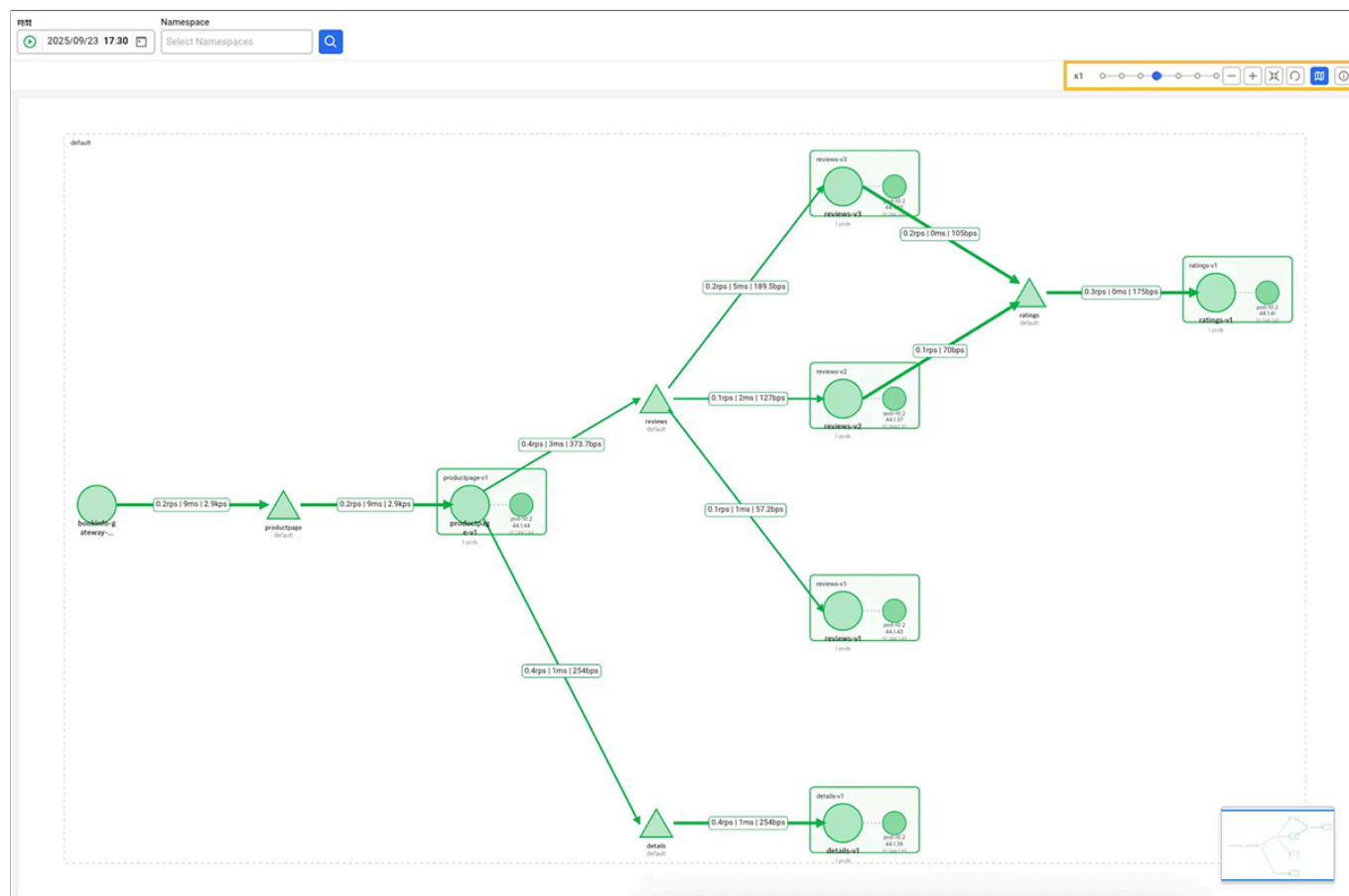
- → テンプレート アイコンをクリックすると、該当するテンプレート画面に直接移動します。
- ⓘ 収集案内 アイコンをクリックすると、データ収集の設定方法を案内します。

Nginxテンプレート

Nginxモニタリングで、Webサーバーのパフォーマンスをリアルタイムで追跡・分析できます。

Istioテンプレート

Istioサービスメッシュ環境におけるサービス間の関係とトラフィックの流れを視覚的に表現し、WhaTap APMデータと連携して統合モニタリング環境をテンプレートとして提供します。画面右上のボタンをクリックすると、テンプレートを拡大または縮小できます。



凡例

画面右上の ⓘ ボタンをクリックすると、凡例を確認できます。

ノードの形状

- 三角形はKubernetesサービス
- 円はワークロード
- 四角形はアプリケーション
- 小さい円はPod（パッド）

ノードの状態

HTTPリクエスト/レスポンス全体のうちエラー（4xx、5xx）の割合

- 緑色 はエラー率5%未満
- オレンジ色 はエラー率5%以上
- 赤色 はエラー率10%以上
- グレーはリクエスト数なし

Podノードの状態

Kubernetes PodのPhase

- 緑色 はRunning状態のPod
- オレンジ色 はPending状態のPod
- 赤色 はFailed状態のPod

エッジの色

2つのノード間のHTTPリクエストで発生したエラー（4xx、5xx）の割合

- 緑色 はエラー率10%未満
- オレンジ色 はエラー率10%以上
- 赤色 はエラー率20%以上
- 青色 はTCP通信
- グレーは状態不明

OpenMetricsエクスプローラー

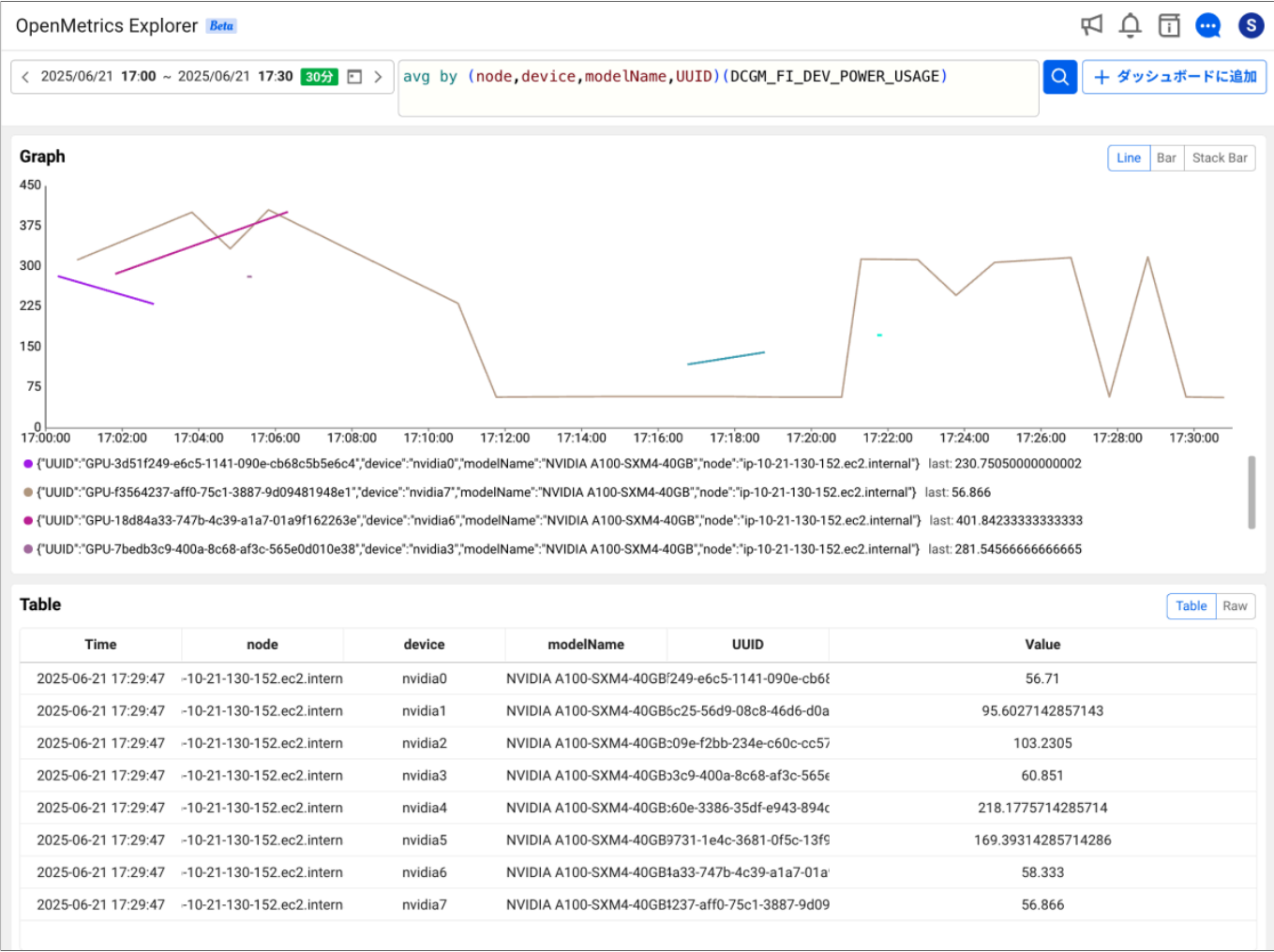
OpenMetrics エクスプローラー は、PrometheusベースのカスタムメトリクスをPromQLで直接探索し、さまざまな形式で可視化してメトリクスの状態を確認したりインサイトを得たりできる機能です。

この機能により、希望するメトリクスを自由に照会し、有意義なデータを抽出したり、ダッシュボードと連携して継続的にモニタリングしたりできます。

ⓘ **OpenMetrics エクスプローラー** を使用するには、OpenAgentのインストールが必要です。

PromQLで探索する

OpenMetrics エクスプローラー でPromQLを実行し、さまざまな可視化オプションで結果を確認できます。



PromQL構文のサポートと自動補完

`node_cpu_seconds_total`、`container_memory_usage_bytes`などのメトリクスを入力すると、自動補完機能でメトリクスおよび演算子の一覧を提示します。

`{pod="example"}`形式のラベルフィルタリングもサポートします。

ダッシュボードに追加する

照会したPromQLクエリをダッシュボードウィジェットとして保存し、希望するメトリクスを継続的にモニタリングできます。

追加方法

1. **OpenMetrics エクスプローラー** 画面右上の **+ダッシュボードに追加** ボタンをクリックします。**ダッシュボードに追加** ウィンドウが開きます。
2. **ダッシュボードに追加** ウィンドウで既存のダッシュボードを選択するか、新規ダッシュボードを作成します。
3. **適用** ボタンをクリックすると、該当ウィジェットを指定したダッシュボードに追加します。
 - 追加したダッシュボードでウィジェット名と説明を入力できます。
 - 追加したウィジェットは、FlexボードのGridレイアウトで自由に位置を調整し、PromQLを編集できます。

OpenMetricsエージェントのインストール

OpenAgentは、Prometheusエンドポイントからメトリクスを収集してWhatapサーバーに送信するエージェントです。SingleStoreプロジェクトでOpenMetricsエクスプローラーとテンプレートを使用するには、まずOpenAgentをインストールする必要があります。

OpenAgentの動作には、次の3つのファイルが同じディレクトリに必要です。

File	Description
<code>openagent</code>	メトリクスの収集・送信を行う実行ファイル
<code>whatap.conf</code>	ライセンス・収集サーバーアドレスなどの基本設定
<code>scrape_config.yaml</code>	スクレイピング対象（エンドポイント）の定義

インストール手順の概要

1. インストールディレクトリを作成後、アーキテクチャに合ったバイナリをダウンロードします（AMD64/ARM64）。

```
mkdir -p /opt/whatap/openagent
cd /opt/whatap/openagent
wget https://repo.whatap.io/openagent/latest/amd/openagent
chmod +x openagent
```

2. `whatap.conf` にライセンス・サーバーアドレス・ポートを入力します。

```
echo "WHATAP_LICENSE=your-whatap-license" >> whatap.conf
echo "WHATAP_HOST=your-whatap-host" >> whatap.conf
echo "WHATAP_PORT=your-whatap-port" >> whatap.conf
```

3. `scrape_config.yaml` に収集対象エンドポイントを定義します（修正時は自動的に再読み込みされ、再起動は不要です）。

4. standaloneモードで実行します。

```
./openagent standalone
```

❗ インストール手順全体・実行モード・ `scrape_config.yaml` の詳細オプション（StaticEndpoints・params・metricRelabelConfigs）と設定項目については、[OpenAgentのインストール](#) および [OpenAgentの設定](#) ドキュメントを参照してください。Kubernetes環境については [OpenAgent Kubernetes構成](#) に従います。

❗ macOS Apple Siliconはサポートされていません。Linux AMD64またはARM64でのみ動作します。

SingleStore 警告アラートの概要

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、イベントを構成できます。

メトリクスイベント

SingleStore のメトリクスに基づくイベント条件を設定し、警告アラートを発生させる方法を説明します。

複合メトリクスイベント

複数のメトリクスを組み合わせてイベント条件を設定する複合メトリクスイベント機能を説明します。

異常検知イベント

SingleStore のメトリクスの異常パターンを自動的に検知し、警告アラートを発生させるイベント設定を説明します。

リアルタイムログ

SingleStore のログ内容を基準に警告通知を発生させるログイベントを設定します。

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。

メトリクスイベント

SingleStore のメトリクスに基づくイベント条件を設定し、警告アラートを発生させる方法を説明します。

複合メトリクスイベント

複数のメトリクスを組み合わせてイベント条件を設定する複合メトリクスイベント機能を説明します。

異常検知イベント

SingleStore のメトリクスの異常パターンを自動的に検知し、警告アラートを発生させるイベント設定を説明します。

リアルタイムログ

SingleStoreのログ内容を基準に警告通知を発生させるログイベントを設定します。

📄 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,

```

① 「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
└ 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 > 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生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（プライマリーキー）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`)

複合メトリクスイベント設定

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。

異常検知イベント設定

ホーム > プロジェクト選択 >  アラート通知 > イベント設定 > 異常検知 タブ

異常検知 は、メトリクスデータから異常な上昇または下降パターンを検出し、通常とは異なる動きが検知された場合にイベントを発生させる機能です。

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。
- **+ イベントルール追加:** 新しい異常値イベントを追加します。

表 | 異常値イベント一覧の構成

項目	説明
イベントメッセージ	イベント発生時に送信されるメッセージ
カテゴリ	メトリクスデータを分類する単位で、メトリクスイベント設定の基準となるカテゴリ
フィールド	異常を検知する指標（メトリクスフィールド）
フィルター	異常値の対象となるデータ範囲を制限する条件
上昇／下降パターン	上昇または下降パターンの感度
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
	イベント設定の修正
	イベントの削除
	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

メトリクスデータを基に、値の動きが通常とは異なり上昇または下降した場合に、警告通知を送信するよう設定できます。

イベントルール追加

1. 画面右側の [+ イベントルール追加] ボタンをクリックします。
2. イベント基本情報, メトリクス, 異常値, 付加情報 を順に設定します。

イベント基本情報

1. イベントレベル (Critical, Warning, Info) を選択します。
 - イベントの重要度および通知レベルが決定されます。
2. イベント発生時に受信する通知メッセージを入力します。
 - 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。

❗ 使用可能な変数

- \$pcode : プロジェクトコード
- \$category : カテゴリ
- \$field : フィールド
- \$value : 発生値
- \$oname : イベント対象

メトリクス

1. カテゴリ を選択します。
 - 異常を検知するメトリクスデータの基準となるカテゴリです。

2. 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。
3. イベント対象を絞り込むための **フィルター** を選択します。複数選択が可能です。

異常値

1. **上昇パターン** と **下降パターン** の感度を選択します。
2. 各パターンのトグルボタンをクリックして、有効または無効を切り替えます。
 - 上昇パターンのみを検知する場合: 上昇パターン **ON**, 下降パターン **OFF**
 - 下降パターンのみを検知する場合: 下降パターン **ON**, 上昇パターン **OFF**

付加情報

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

イベント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。

イベント修正

1. アラート通知 > イベント設定 の 異常検知 タブに移動します。
2. 異常値 一覧で、修正するイベントの右側にある  をクリックします。
3. 異常値 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。

イベント削除

1. アラート通知 > イベント設定 の 異常検知 タブに移動します。
2. 異常値 一覧で、削除するイベントの右側にある  をクリックします。
3. 削除確認画面で [削除] ボタンをクリックします。

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ージャーは、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

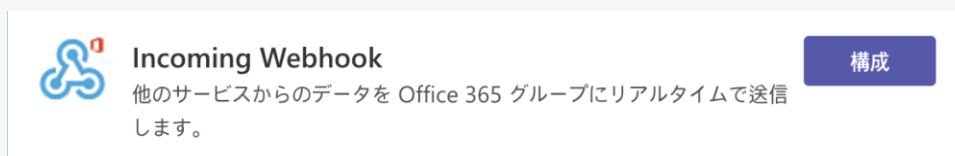
- `/help` : コマンド一覧を表示
- `/license` : 通知を受信するプロジェクトのアクセスキーを入力
- `/remove` : 通知を受信しないプロジェクトコードを入力
- `/list` : 現在通知を受信しているプロジェクトコードを表示

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。

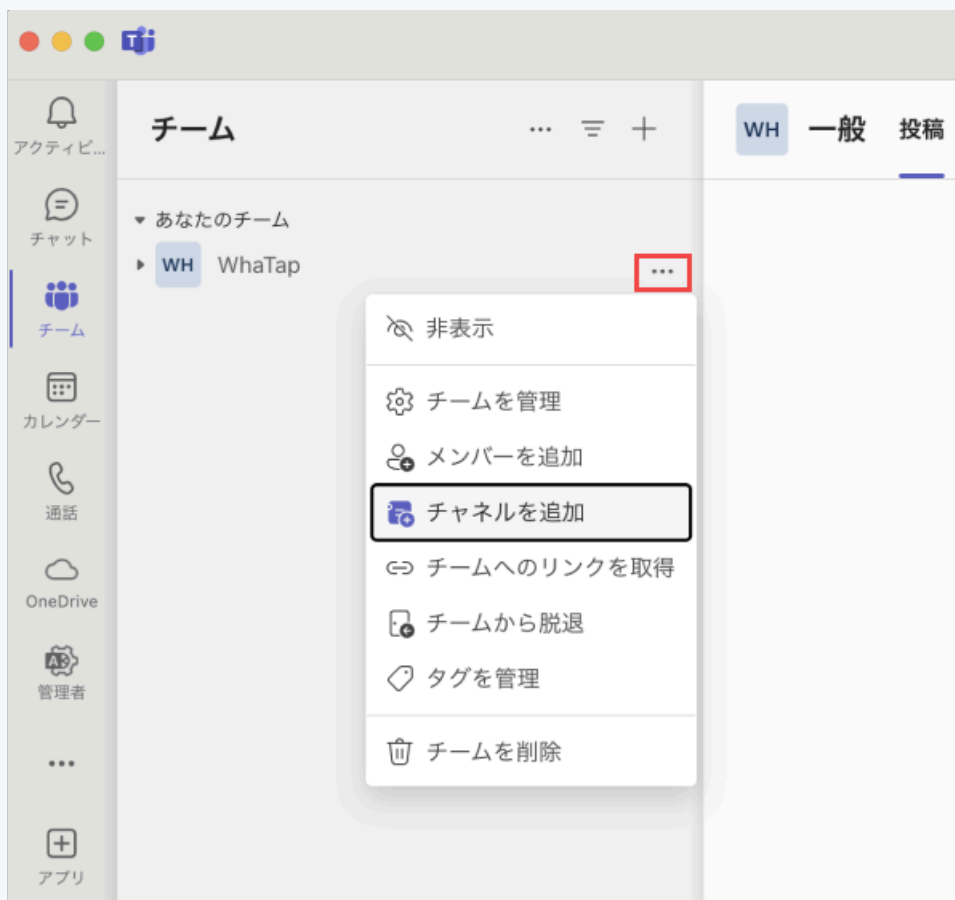
6. [登録] ボタンをクリックします。



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。

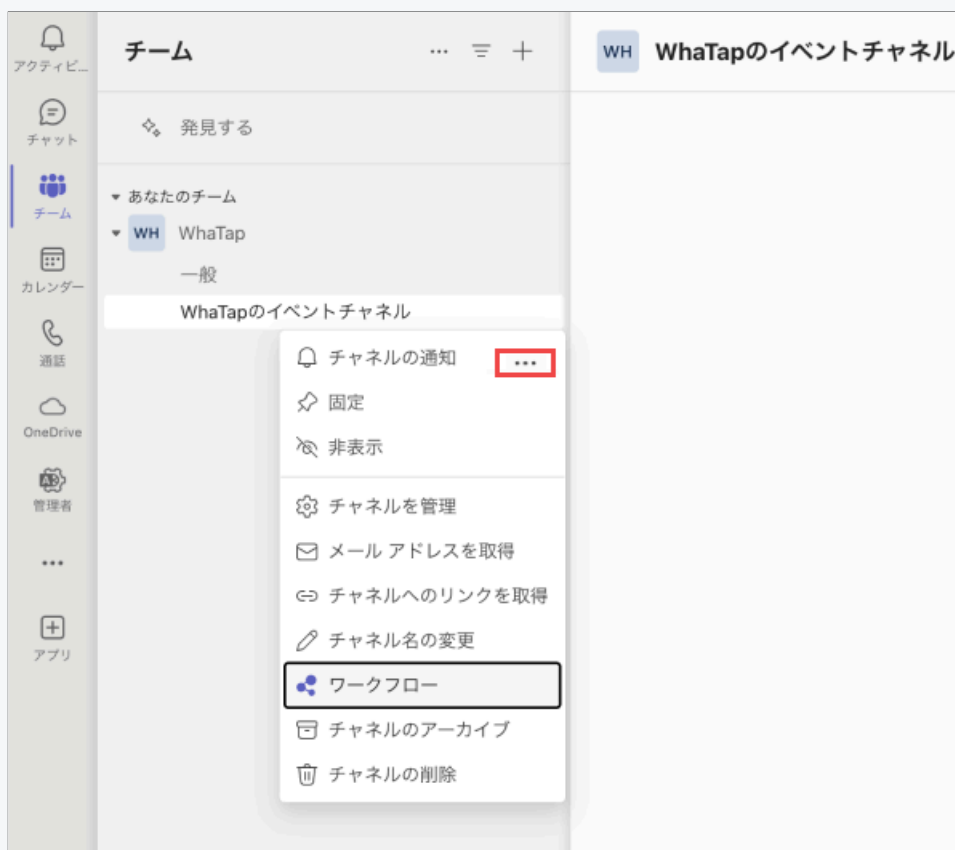
☐ 共有
組織内または組織外の人またはチームがアクセスできます。

☐ 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。

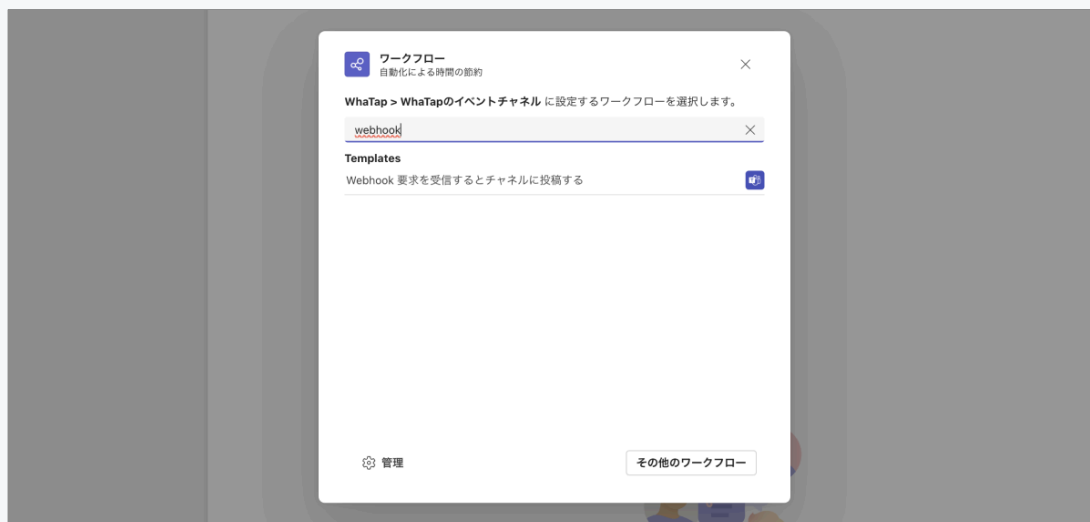
キャンセル 作成

❗ 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。



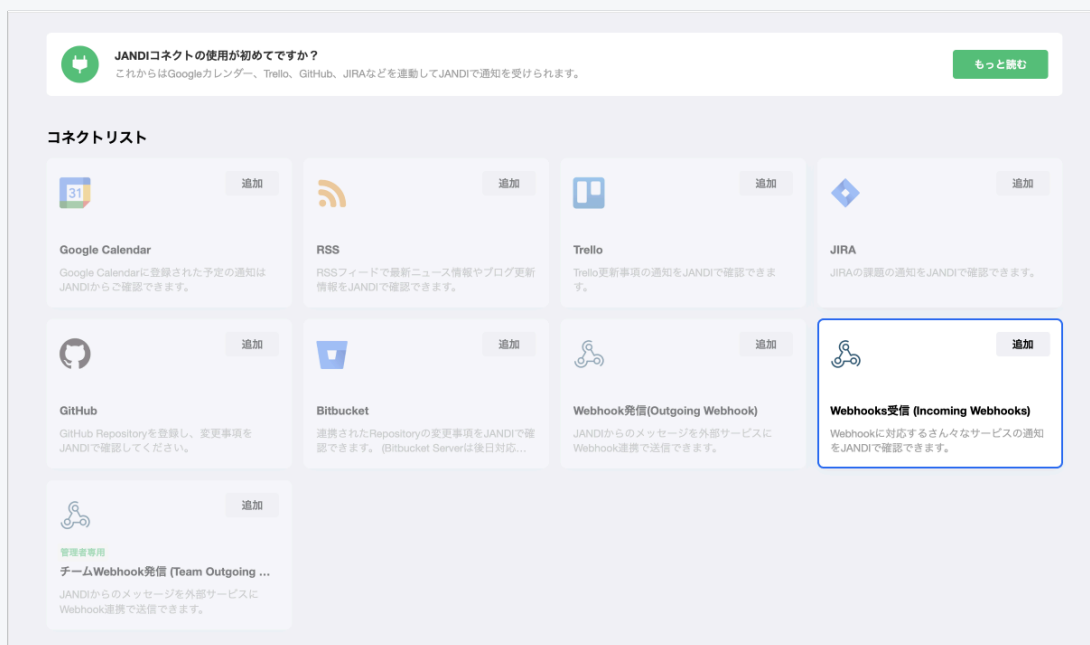
8. WhaTap モニタリングサービスの **サードパーティプラグインの追加** 画面に戻り、**Teams Workflows** タブ下部の **Channel Name** と **Webhook URL** に値を入力します。
9. [登録] ボタンをクリックします。

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}"
}
```

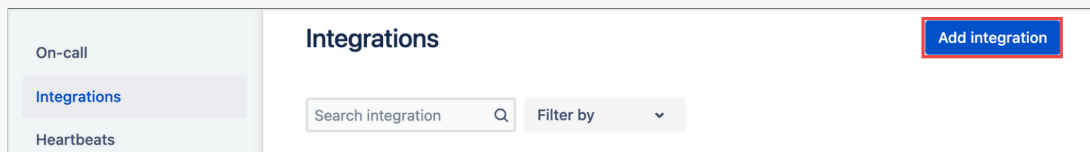
2. **Webhook Name** と **Webhook URL** の項目を入力してください。
3. ヘッダー値を追加するには、**ユーザーヘッダー値の追加** の + 追加 をクリックし、key と value を入力してください。
4. [**登録**] ボタンをクリックしてください。

Opsgenie

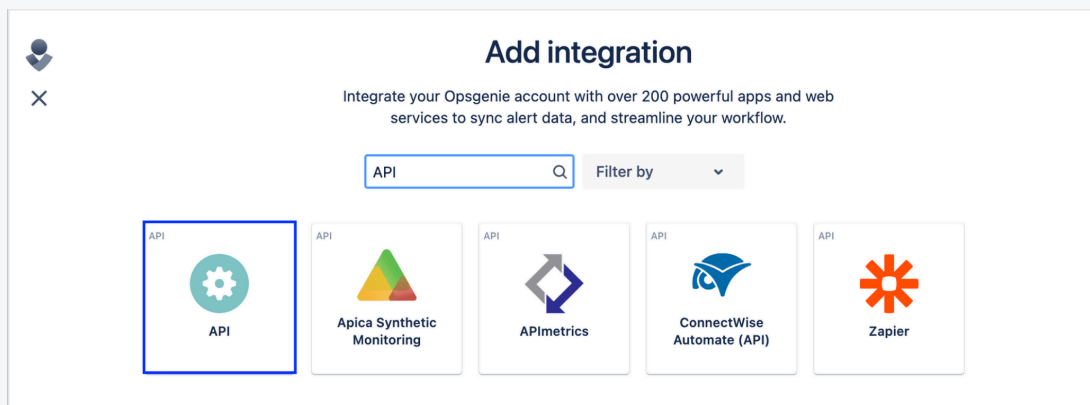




1. **Teams** メニューで、アラートを受信するチームを選択してください。
2. **Integration** メニューに移動し、[Add Integration] ボタンをクリックしてください。



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

❗ 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
```

イベント一時停止

ホーム画面 > プロジェクト選択 >  アラート通知 > イベント一時停止

イベント一時停止は、イベントルールを一時的に停止してイベントの発生を制限する機能です。メンテナンス作業や点検のように通知が不要な期間に使用すると、不要な通知を減らすことができます。

ⓘ 一時停止ルールは一度作成すると修正できず、設定した期間が終了すると自動的に削除されます。

画面構成

Item	Description
進行中の一時停止ルール	現在適用中の一時停止ルール数
イベント一時停止リスト	作成した一時停止ルールのリスト

一時停止ルールの追加

- 一時停止ルールの追加ボタンをクリックします。
- 一時停止する対象と期間を設定します。
- 保存すると、その期間中は対象イベントルールの通知が停止され、期間が終了するとルールが自動的に削除されます。

実験室

実験室メニューでは、基本画面以外にデータを直接扱ったり、アラートを細かく調整したりする付加機能を提供します。

画面構成

画面	説明
MXQLデータ照会	MXQLで収集データを直接照会・可視化
アラートメッセージ	イベント発生・解消アラートメッセージの項目と内容を編集

MXQLデータ照会

MXQLデータ照会画面では、ワタップが収集したデータをMXQL（WhaTapデータ問い合わせ言語）で直接照会できます。基本画面が提供しない形でデータを抽出したり、収集値を直接確認したりするときに使用します。

❗ MXQLの文法と関数は [MXQLガイド](#) で確認できます。

使い方

1. **時間** セレクターで照会する時間範囲を選択します（例: 最近1日）。
2. **MXQLエディター** に照会するクエリを入力します。たとえば
`CATEGORY db_real_counter TAGLOAD SELECT` の形でカテゴリとタグを指定してデータを読み込みます。
3. **照会行数** フィールドで一度に取得する行数を選択します（例: Up to 100 lines）。
4. オプションを設定した後に検索を実行すると、結果を表示します。**メトリクス探索** ボタンをクリックすると、メトリクスデータを探索することもできます。

アラートメッセージ

アラートメッセージ画面では、イベントが発生または解消されたときに受信するメッセージの詳細項目を選択し、項目ごとの内容を編集できます。アラートに必要な情報のみを含めてメッセージを簡潔に整える際に使用します。

画面構成

Item	Description
発生 / 解消	イベント発生メッセージと解消メッセージを区別して編集
アラート種類	メトリクス・複合メトリクスなど、アラート種類別にメッセージを個別に構成
全体 / 発生 / 解消、検索	メッセージ項目を状態別にフィルタリングするか、名前で検索

上部の他のプロジェクトにコピー・全体初期化・全体保存で設定を一括管理できます。各アラート種類セクションでは、初期化・プレビュー・保存・全体有効化を提供します。

メッセージ項目の編集

各項目は修正スイッチでメッセージへの含有可否をオン・オフでき、表示内容を直接編集できます。提供される項目は次のとおりです。

Item	Example
状態	<code>OCCURED / SOLVED</code>
アラートレベル	<code>Warning</code>
プロジェクト番号 / 名前	<code>101 / Example Project</code>
エージェント名	<code>Whatap-Front-01</code>

Item	Example
メッセージ	Message
イベント発生時刻	2022-09-08 14:23:17 +0900
イベント発生条件	tps > 20
イベント対象フィルタリング	oid == 800488350
解消されたイベント通知機能	ON / OFF
アラート種類 / ラベル	METRICS / oid(800488350)
指標 / 現在値 / しきい値	tps / 25 / 20
現在値（複数）	tps=23.39, tx_error=7
繰り返し回数 / 繰り返し時間 / 無音時間	5 / 5 minutes / 10 minutes
処理内容	- Disk Cleanup (20250101 08:30:00+0900, support@whatap.io)
ショートカット	https://service.whatap.io/link/event

項目を編集した後、**プレビュー**で実際のメッセージ形式を確認し、**保存**します。