

MongoDB Monitoring

release date. 2026. 09. 11.



Table of Contents

• MongoDBモニタリング	5
◦ はじめに	9
◦ サポート環境	11
◦ インストール	
▪ エージェントのインストール	18
▪ インストールチェックリスト	29
▪ インストール問題の解決	31
◦ 設定	33
▪ DBXエージェントの設定	36
▪ XOSエージェント設定	42
▪ クラウドエージェント	47
◦ 管理	55
◦ ダッシュボード	59
▪ インスタンスリスト	61
▪ インスタンスモニタリング	64
▪ マルチインスタンス	84
▪ Flexボード	105
▪ Flexボードの使用方法	108
▪ ウィジェットの管理	119
◦ 分析	
▪ カウント推移の比較	124
▪ データベースパラメータ	131
◦ メトリクス	133
▪ MONGODBメトリクス	135

▪ メトリクスチャート	144
▪ メトリクスチャート	167
▪ メトリクス照会.....	170
▪ メトリクス異常検出	172
▪ メトリクストレンド分析	175
◦ 統計/レポート	
▪ データベースのサイズ	178
◦ ログ	181
▪ 適用方法	183
▪ ライブテール	185
▪ ログエクスプローラー	197
▪ ログトレンド	204
▪ ログの検索.....	212
▪ ログの設定.....	227
▪ ログパーシング.....	260
◦ アラート通知.....	275
▪ イベント設定	0
▪ メトリクス	282
▪ 複合メトリクス	303
▪ 異常値.....	310
▪ リアルタイムログ.....	314
▪ 複合ログ	326
▪ イベント設定	340
▪ 通知設定	344
▪ イベント通知フォーマット	366
▪ イベント履歴	374

▪ リアルタイムアラート	382
▪ システムイベント	385
◦ 実験室	387
▪ OpenMetricsエクスプローラー	388

MongoDBモニタリング

データベースのパフォーマンス管理は、データベースのパフォーマンスをリアルタイムでモニタリングし、問題点を診断、分析します。問題のあるSQLをチューニングして適用し、問題が解決されたかをリアルタイムでモニタリングします。

WhaTapデータベースモニタリングサービスは、これら一連のタスクを循環管理できるように設計されています。データベースの動作をモニタリング、診断、分析し、可用性とパフォーマンスを一定のレベルに維持できるように構成されています。データベースに問題が発生した場合、担当者にアラームを送信して状況を認識し、収集されたデータからデータベースの状況をよりに分析することで、Root Causeを明確にする支援サービスです。

❗ データベースプラットフォームごとの対応機能の詳細については、[次の文書](#)を参照してください。

MongoDBモニタリングの特長

- リアルタイムDBモニタリング

リアルタイムのDBパフォーマンス指標と実行中のclient(アクティブセッション)の情報を収集します。稼働状況を一目で確認しながら負荷発生状況をすぐ検知できるし、通知設定で問題発生をすぐに認識できます。

- 特定時点の分析

指標の短期推移、長期推移、指標比較などの機能を提供し、過去の状況を分析できます。データベースのパラメータ変更履歴を追跡します。

- 大容量規模でも効率的な構造

複数のDBサーバーを管理する場合でも、一元化された性能データ収集および効率的なデータストレージ構造により、最適な分析環境を提供します。

- クラウドDBモニタリング可能

クエリベースのモニタリングデータ収集方式で、DBサーバーの種類に制限があり暗線。AWS、GCP、Azureおよび、OCI環境のDBもモニタリングができ、クラウドのリソース指標との統合モニタリングにも対応しています。

- 統合モニタリング

Application、Server、Databaseモニタリング製品をすべてインストールすると、連携されたビューを使用して障

害の原因を素早く分析し特定できます。

- WhaTap SaaS

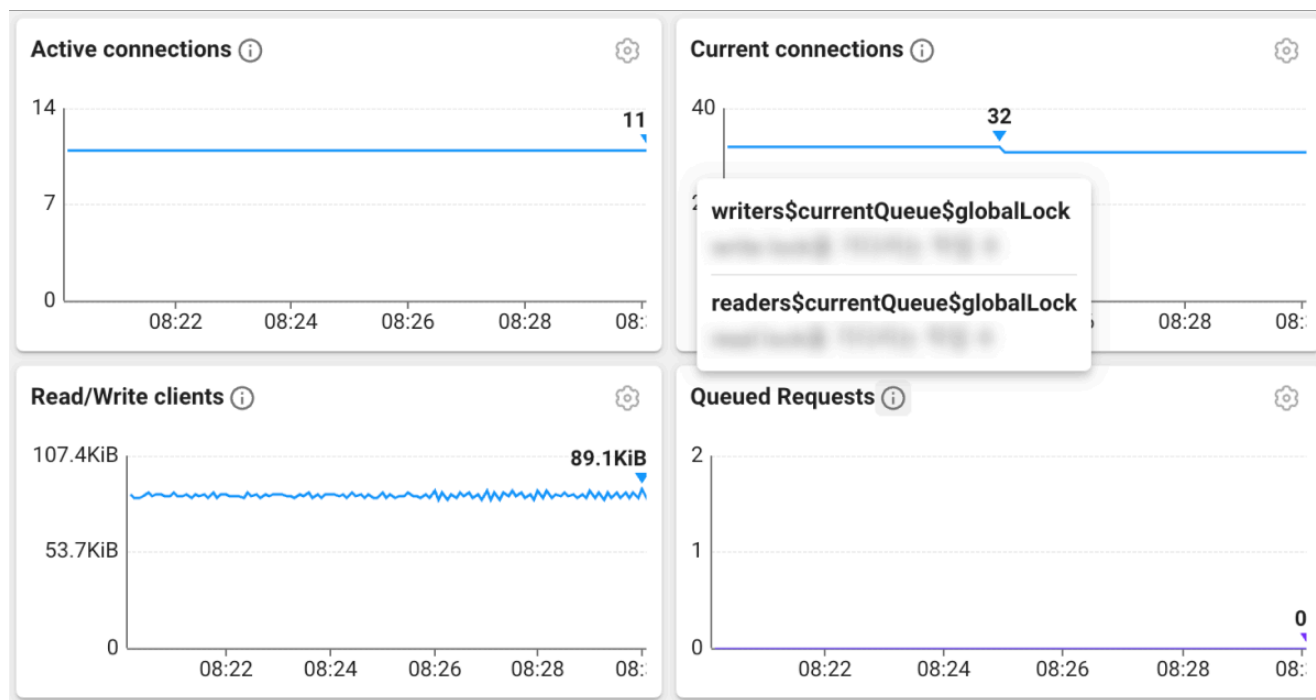
多様なDatabase製品を選択でき、サブスクリプションで利用期間を自由に設定できます。(オンプレミスタイプも提供可能)

データベースモニタリングの新機能

チャートおよび収集機能を強化したMongoDBモニタリングをアップデートしました。最新の機能を利用するには、エージェントをアップデートしてください。

❗ MongoDBモニタリングを利用するエージェントの最小バージョンは1.7.0です。エージェント更新の詳細については、[次の文書](#)を参照してください。

- DB性能指標の情報提供



指標のヘルプとチューニングに関するヒントを追加し、ユーザーが数多くの指標を簡単に理解できるようにカテゴリ化して利便性を提供します。(多言語に対応予定)

・ダッシュボード機能の改善

ダッシュボードでは、1つのチャートに複数の指標を追加する機能が追加されました。また、プリセット機能を追加してユーザーが必要な指標を素早く確認できます。

・UI改善

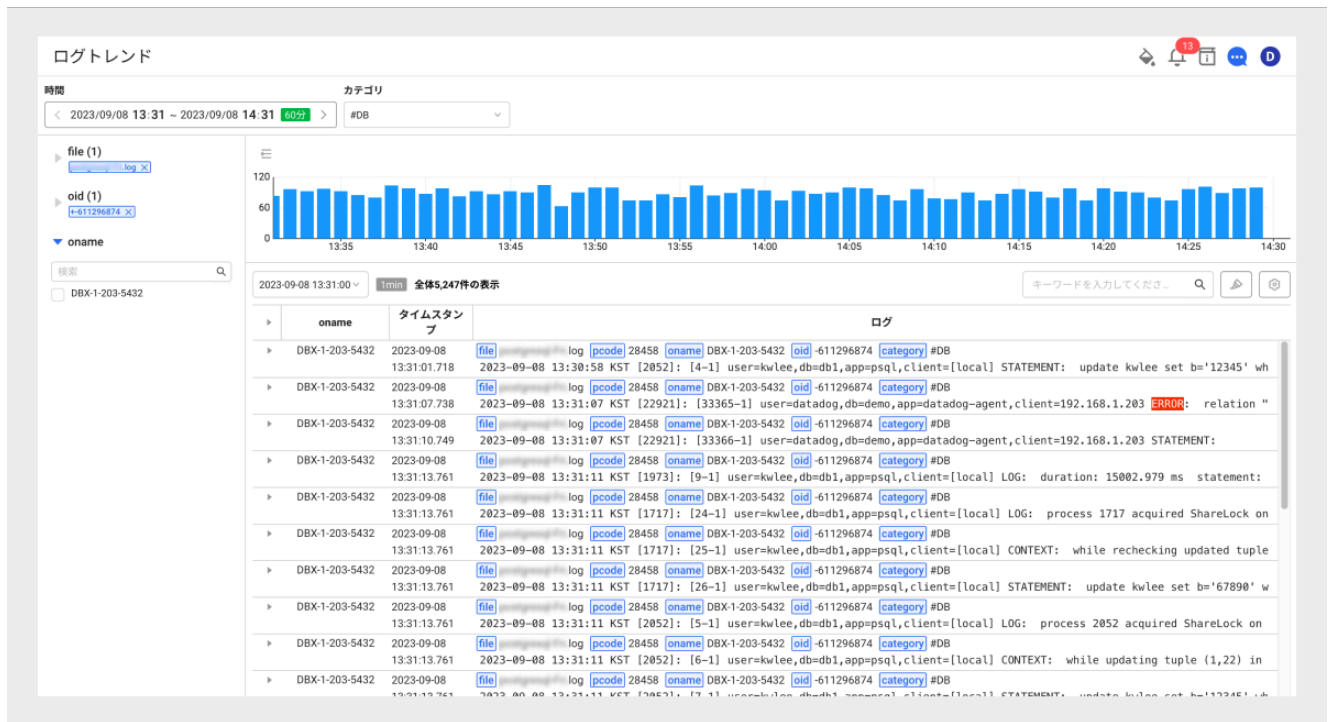
インスタンスモニタリングフィルター機能の改善

The screenshot illustrates the improvement of the instance monitoring filter function. The top part shows the filter controls, which include a dropdown menu for 'opid' and a 'Filter' button. The bottom part shows the resulting table of active sessions, which includes columns for 'opid', 'type', 'host', 'desc', 'active', 'currentOpTime', 'op', 'ns', 'numYields', and 'waitingForL'.

opid	type	host	desc	active	currentOpTime	op	ns	numYields	waitingForL
12381028	op	k8s-node1.27021	conn42	true	2024-03-19T08:56:45...	command	admin.\$cmd	0	false
12381022	op	k8s-node1.27021	conn41	true	2024-03-19T08:56:45...	command	admin.\$cmd	0	false
12381065	op	k8s-node1.27021	conn44	true	2024-03-19T08:56:45...	command	admin.\$cmd	0	false

The bottom part of the screenshot shows the resulting table of active sessions, which includes columns for 'opid', 'type', 'host', 'desc', 'active', 'currentOpTime', 'op', 'ns', 'numYields', and 'waitingForL'. The table is filtered to show only 'command' operations. A blue arrow points from the filter controls to the resulting table.

・ログ



ログTailとログトレンド、ログ検索、ログ通知機能で、DBログを検索して推移を確認できるし、ログ関連の通知を受信できます。

はじめに

WhaTapモニタリングは次の手順で開始します。

[ステップ1. 会員登録](#)

[ステップ2. 製品選択](#)

[ステップ3. プロジェクト作成](#)

[ステップ4. アクセスキー確認](#)

その後、サポート環境を確認してからエージェントのインストール手順に進みます。

会員登録

WhaTapモニタリングサービスを利用するには、まず[会員登録](#)が必要です。会員登録に関する詳細は、[アカウント管理](#)
> [会員登録](#)ドキュメントを参照してください。

製品選択

1. [WhaTapモニタリングサービス](#)にログインします。
2. ≡ [プロジェクト全体](#) > [+ Project](#)ボタンをクリックします。
3. [商品選択](#)画面でモニタリングするGo製品を選択してから作成ボタンをクリックしてください。

プロジェクト作成

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

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

- **プロジェクトタイムゾーン(必須):** アラートおよびレポート生成時の基準となる時間を設定します。
- **通知言語の設定(必須):** プロジェクトで発生する警告通知メッセージの言語を設定します(韓国語、英語対応)。
- **プロジェクトグループ:** 複数のプロジェクトをグループにまとめて管理できます。所属するグループがあれば選択してください。
- **プロジェクト説明:** プロジェクトに関する追加説明を入力します。

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

❗ 組織を選択した状態でプロジェクトを追加する場合、**組織下位のグループ**を必須で設定する必要があります。グループに関する詳細は、[次のドキュメント](#)を参照してください。

アクセスキー確認

アクセスキーは、WhaTapサービスを有効化するための固有IDです。

インストールガイドセクションで**プロジェクトアクセスキーの発行ボタン**を選択してください。**アクセスキー**を自動的に発行した後、次のステップに進みます。

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

サポート環境

MongoDBモニタリングを開始する前に、次のサポート環境を確認してください。

データベース対応バージョン

MongoDB 4.2バージョン以降に対応します。

- ❗ エージェントをインストールするサーバーには、Java 8以降のインストールが必要です。
- データベースサーバーは、DBXエージェントがDBポートにアクセスできるように、Inbound接続を許可する必要があります。
- DBXエージェントがWhaTapサーバーにデータを転送できるように、6600ポートのOutboundを開く必要があります。

エージェントの最小インストール仕様

- CPU:** 1コアあたり約20個のエージェントのインストールが可能(DBサーバーの負荷によって変動可能)
- メモリー:** 200MB
- ディスク:** 100MB(エージェントスペース50MB + ログファイル作成スペース50MB)

❗ エージェント数による最小インストール仕様

エージェントインストール数	CPU	メモリ	ディスク
10個	1コア	2GB	1GB
20個	1コア	4GB	2GB
40個	2コア	8GB	4GB

エージェント方式

DBエージェントは、次のような方式で基本動作します。

- 遂行周期: 5秒(既定値)
- 実行クエリ数: 5~6個
- 速度: サーバーの負荷が正常な場合、1秒以内に終了
- 最大2つのセッション(5秒収集セッション、その他の情報収集セッション)

収集クエリのタイムアウトが発生すると、DBエージェントは負荷を最小化するために次の方法で動作します。

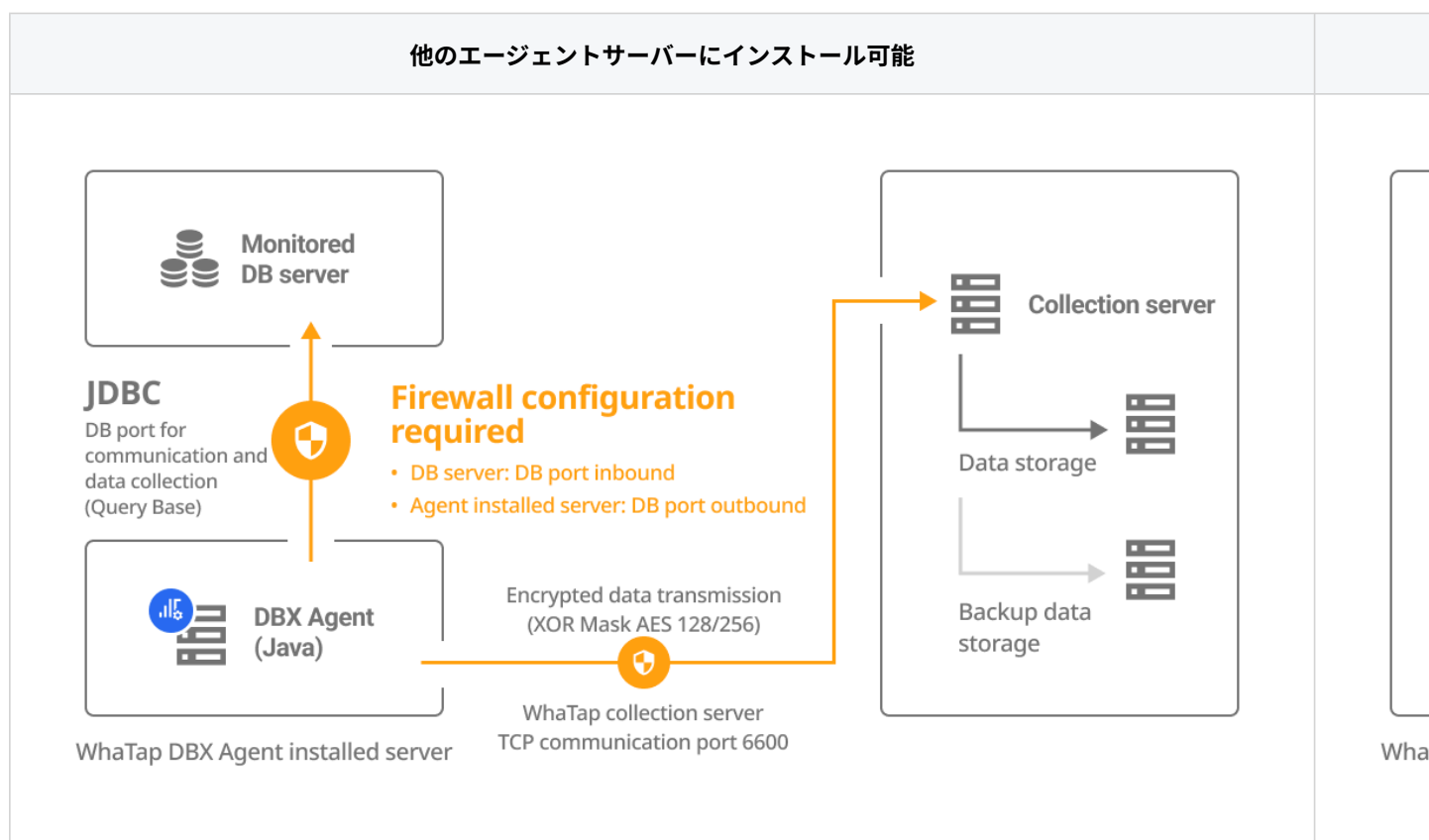
- 以前の収集クエリが終了するまで、新しい収集クエリを実行しません。
- タイムアウトが12秒を超えた場合(リフレッシュ周期が2回を超えた場合)は、セッション終了後に再接続します。
- 3回以上タイムアウトが発生した場合は、10秒待機してから再試行します。

❗ DBサーバーの負荷状態によって収集クエリの結果がWhaTapモニタリングサービス画面に出力されるまでに長い時間がかかったり、タイムアウトが発生することがあります。

エージェント構成

WhaTapのデータベースモニタリングサービスは、エージェントと収集サーバーで構成され、エージェントと収集サーバーの間でセキュリティのためにデータを暗号化します。外部ライブラリを使用していないため、インストールやアップデートのためにシステムを再起動する必要はありません。

- WhaTapデータベースモニタリングサービスは、データベースサーバーにエージェントをインストールしなくても、別のエージェントサーバーでモニタリングすることができます。ユーザーの環境に柔軟に対応できます。



- XOSエージェントは、データベースサーバーのプロセス使用状況をモニタリングできる付加オプションエージェントです。データベースサーバーでプロセス使用状況をモニタリングする場合は、データベースサーバーに別のエージェントを起動してデータを収集できます。
- エージェントとサーバーは、バイナリベースの通信プロトコルを使用します。また、データを選択的に暗号化することで、データのセキュリティを確保しながら、暗号化の負荷を低減します。

- ⓘ
- モニタリング対象のデータベースサーバーとネットワーク通信が可能なサーバーにWhaTapエージェントをインストールする必要があります。
 - WhaTap DBXエージェントサーバには、**Java 8バージョン以降のJDK**をインストールする必要があります。

サービス提供形態

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

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

❗ インターネットに接続しない閉域網環境でも、オンプレミスで構築できます。

提供形態による機能の違い

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

❗ オンプレミス環境で一部の機能をご利用いただくには、別途契約が必要です。

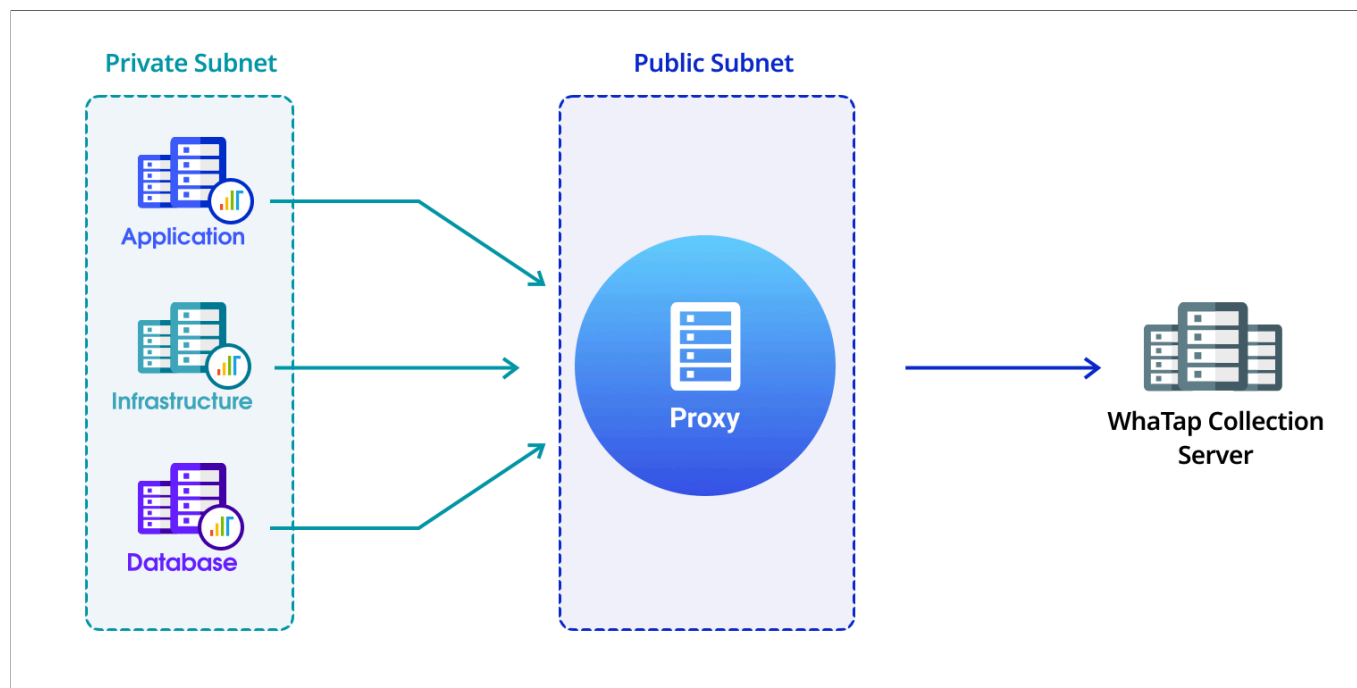
ファイアウォール

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

出発地：WhaTapエージェント

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

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



対応ブラウザ

WhaTapモニタリングサービスは、ウェブブラウザとモバイルアプリで利用できます。

Webブラウザ	推奨	対応バージョン
Google Chrome	O	111以降
Mozilla FireFox	X	最新バージョン
Edge	X	最新バージョン
Safari	X	最新バージョン

ⓘ サポート案内

- ブラウザの互換性および性能の観点から、Chrome の最新バージョンの使用を推奨します。
- ユーザーインターフェース（User Interface, UI）は HTML5 標準技術で実装されているため、Internet



Explorer はサポートしていません。

⚠ 制約事項

WhaTap の Web インターフェースはモバイルブラウザをサポートしていません。モバイル端末から WhaTap にアクセスするには、Android または iOS 用の WhaTap アプリをインストールしてください。WhaTap モバイルアプリはモバイル環境に最適化されています。WhaTap モバイルアプリの詳細については、[こちらのドキュメント](#)を参照してください。

モバイルアプリ

WhaTap モバイルアプリは、Android および iOS 環境をサポートしています。リンクへ移動するか、QR コードをスキャンして WhaTap アプリをインストールできます。モバイルアプリの詳細な説明は、[次の文書](#)を参照してください。

iOS	Android
	
iOS 12バージョン以降	Android 5.0バージョン以降

エージェントのインストール

WhaTapデータベースモニタリングサービスを使用するための基本的なインストール方法について説明します。

WhaTapデータベースエージェントのダウンロード

1. エージェントファイルをダウンロードしてください。次の2つの方法を利用してください。
 - WhaTapモニタリングサービス画面で**Download**ボタンをクリックしてダウンロードすることができます。
 - Linux wget方式でダウンロードできます。次のコマンドを使用してください。

```
wget -O whatap.agent.database.tar.gz "https://service.whatap.io/download/dbx_agent?type=mongodb&format=tar.gz"
```

❗ セキュリティ設定により、tar形式のファイルをダウンロードできないユーザーのために、ZIP形式のファイルも一緒に提供します。インストール画面で**.zip ダウンロード**ボタンを選択します。

2. ダウンロードしたファイルを分析するサーバーにコピーし、解凍してください。(Windows、Linux共通)

エージェント構成ファイル



ファイル名	説明
whatap.conf	データベースサーバーのデータを収集する収集サーバーのアドレスとサーバーのプロジェクトアクセスキーを入力するファイルです。エージェント設定の詳細については、 次の文書 を参照してください。
alert/alert.conf	収集するモニタリング項目にしきい値を設定するファイルです。しきい値を超えると通知イベントが発生します。



ファイル名	説明
<code>scripts/</code>	リモートでSQLスクリプトを実行できるスクリプトのディレクトリです。
<code>ps.sh</code>	プロセスIDを読み込むスクリプトです。エージェントプロセスを終了する場合は、そのIDを参照します。
<code>stop.sh</code>	エージェントプロセスを終了するときに使用するスクリプトです。
<code>uid.sh (uid.bat)</code>	データベースの接続情報を組み合わせて暗号化されたUIDを生成するためのシェルスクリプトファイルです。 <code>db.user</code> ファイルを作成します。最初に一度だけ設定すると、暗号化されたUIDを通じてモニタリング対象データベースサーバーからデータが収集されます。 モニタリング用アカウント作成の詳細については、 次の文書 を参照ください。
<code>start.sh (start.bat)</code>	エージェント実行用のシェルスクリプトファイルです。エージェントを実行すると、データベースサーバーからのモニタリング情報の収集が開始されます。
<code>startd.sh (startd.bat)</code>	エージェント実行用のシェルスクリプトファイルでバックグラウンドで実行できます。
<code>whatap.agent.dbx-X.Y.Z.jar</code>	Tracerプログラムは、データベースサーバーの情報を収集し、収集した情報をサーバーに送信するプログラムです。
<code>jdbc</code>	データベースサーバー接続のために参照するライブラリを収集するディレクトリです。エージェントをデータベースサーバーに接続するためのライブラリを直接ダウンロードし、javaのclasspathオプションにパスを設定して使用します。

ファイル名	説明
<code>xos/</code>	データベースサーバーのプロセス使用量をモニタリングできるオプションのエージェントを含むディレクトリです。
<code>_xos.conf</code>	データベースサーバーのプロセス使用状況のデータを収集およびデータ転送をするためのエージェントサーバーのアドレスと通信ポートを入力するファイルです。
<code>*xcub/</code>	CUBRIDデータベースのSQLテキスト収集と指標計算を実行する追加のエージェントファイルが含まれているディレクトリです。
<code>_xcub.conf</code>	CUBRIDデータベースおよび追加のエージェント接続情報を入力するファイルです。

ⓘ *`:xcub`パスのファイルは、CUBRIDモニタリングの専用ファイルです。

3. 解凍したフォルダの中から`whatap.conf`ファイルを確認してください。`whatap.conf`ファイルにプロジェクトのアクセスキー情報、WhaTapサーバー情報、DB接続情報を入力します。

whatap.conf

```
license={Access_Key}
whatap.server.host=13.124.11.223/13.209.172.35 # WhaTap server information

dbms=mongodb
db={Database_name} # sid
db_ip={DB_server_IP_address}
db_port={DB_server_port}
```

4. 次のディレクトリにJDBCドライバーをダウンロードしてください。`/圧縮を解凍したフォルダ/jdbc`
データベースサーバーのOSとバージョンに合わせてJDBCドライバをダウンロードします。

MongoDB JDBC Drivers : <https://github.com/mongodb/mongo-jdbc-driver>

- ① • DB構成によっては、[whatap.conf](#)ファイルの追加設定が必要になる場合があります。詳細については、[次の文書](#)を参照してください。
- DBサーバーのリソースを追加でモニタリングするには、XOSエージェントを使用する必要があります。詳細については、[次の文書](#)を参照してください。
- [/解凍されたフォルダ/jdbc/README.md](#)ファイルで各データベースのJDBCドライバのインストールパスを確認することができます。

アカウント生成

データベースモニタリングをするために必要な権限を持つアカウントを作成します。root(admin) アカウントでログインしてアカウントを作成してください。

- ① • 既に存在するアカウントを使用する場合は、[DBユーザーファイルの作成](#)に進みます。権限がない場合は、モニタリングを開始できません。
- コード例で `whatap` は、DBユーザーアカウント名です。ユーザーが利用するユーザーアカウント名に変更してください。
- コード例の `DB_Password` には、ユーザーパスワードを入力します。

```
db.createUser(  
  {  
    user: "whatap",  
    pwd: "DB_Password",  
    roles: [  
      { "role": "clusterMonitor", "db": "admin" },  
    ]  
  }  
)
```

- ❗ user と pwd 値に特殊文字を含めると、パーセントエンコード(percent encoding)を適用して変換する必要があります。例えば、パスワードが whatap@# だったら whatap%40%23 に変換して入力する必要があります。詳細は、[次のリンク](#)を参照してください。
- MongoDB環境のアカウント作成の詳細については、[次のリンク](#)を参照してください。

DBユーザーの作成とパスワードの変更

- ✔ userとpasswordを使用しない場合(認証なしでMongoDBに接続可能な場合) [DBユーザーファイル生成](#)する手順をスキップできます。

データベース接続用に暗号化されたUIDを作成します。usernameとpasswordを入力し、シェルスクリプト(またはバッチファイル)を実行してください。

- ✔ パスワードを変更する場合も、変更するパスワードを入力して同じ方法で進めてください。

• [Linux](#) [Windows](#)

```
./uid.sh {DB_USER} {DB_PASSWORD}
```

```
uid.bat {DB_USER} {DB_PASSWORD}
```

- ❗ 最初に一度設定すると、その後は暗号化されたUIDを通じて監視対象データベースサーバーからデータ収集を行います。
- DBユーザーファイルを作成するには、プロジェクトアクセスキーが[whatap.conf](#)ファイルに入力されている必要があります。 [アクセスキーの確認](#)

特殊文字を含む場合の処理方法

MongoDB環境で DB_USER または DB_PASSWORD に特殊文字が含まれる場合、次の手順で処理する必要があります。

す。

ステップ1:パーセントエンコーディングの適用(必須)

MongoDBは特殊文字が含まれる場合、パーセントエンコーディング(Percent Encoding)を先に適用する必要があります。

例

- 元のパスワード: whatap@#
- パーセントエンコーディング適用後: whatap%40%23

✔ パーセントエンコーディング規則の詳細については、[MongoDB Connection String URI Format](#)公式ドキュメントを参照してください。

ステップ2:エスケープ文字の適用(必要な場合)

パーセントエンコーディング適用後もシェルで解釈される特殊文字(!、\、\$ など)が含まれる場合、エスケープ文字(\)を追加で適用する必要があります。

例

基本的な使用

```
./uid.sh whatap whatap%40%23
```

シェル解釈の問題が発生した場合

```
./uid.sh whatap whatap\%40\%23
```

- ❗ • MongoDBは特殊文字を含む場合、パーセントエンコーディングが優先です。
- 適用順序:パーセントエンコーディング → 必要に応じてエスケープ文字
- パーセントエンコーディングを適用しないと、UID生成は成功してもDB接続が失敗する可能性があります。

モニタリングの開始

エージェントをインストールしたパスからシェルスクリプト(またはバッチファイル)を実行してください。

- [Linux](#) Windows

```
./start.sh
```

デーモンのように使用する場合、次のコマンドを実行してください。ただし、**nohup**をインストールした環境のみで動作します。

```
./startd.sh
```

```
start.bat
```

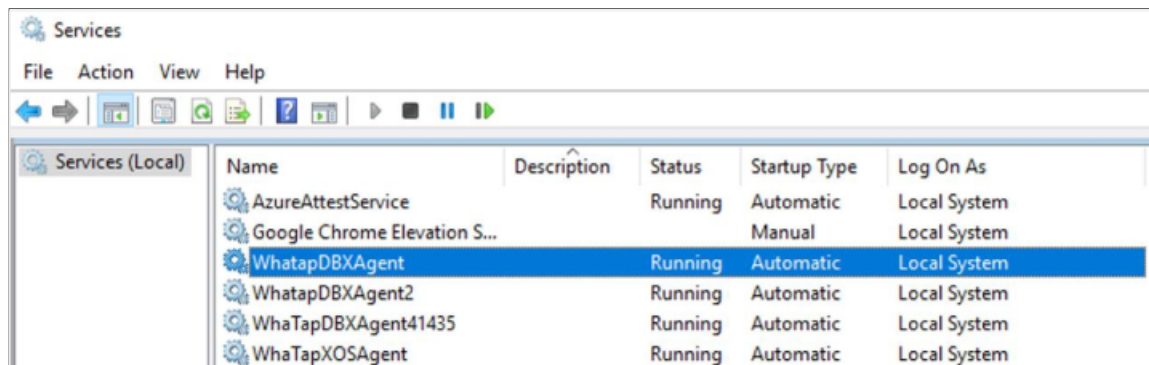
画面に表示された実行ログにエラーがないか確認し、ダッシュボード画面(**インスタンスリスト**)にチャートが正常に表示されることを確認します。異常がなければCtrl+Cを押して実行を終了し、次の手順に従ってウィンドウサービスに登録します。

サービスを登録する

次のコマンドを実行して、サービスを登録します。

```
install_WindowsService.bat create WhatapDBXAgent
```

サービスを登録すると、Windowsのサービス管理ツールで以下のように確認できます。該当サービスを探して右クリックし、スタート(Start) オプションを選択してサービスを開始します。



① コントロールパネル > Windows ツール > サービス (services.msc) で WhatapDBXAgent サービスを開始または停止できます。使用する Windows バージョンによってサービス経路は異なる場合があります。

サービスを削除する

次のコマンドを実行して、サービスを削除できます。

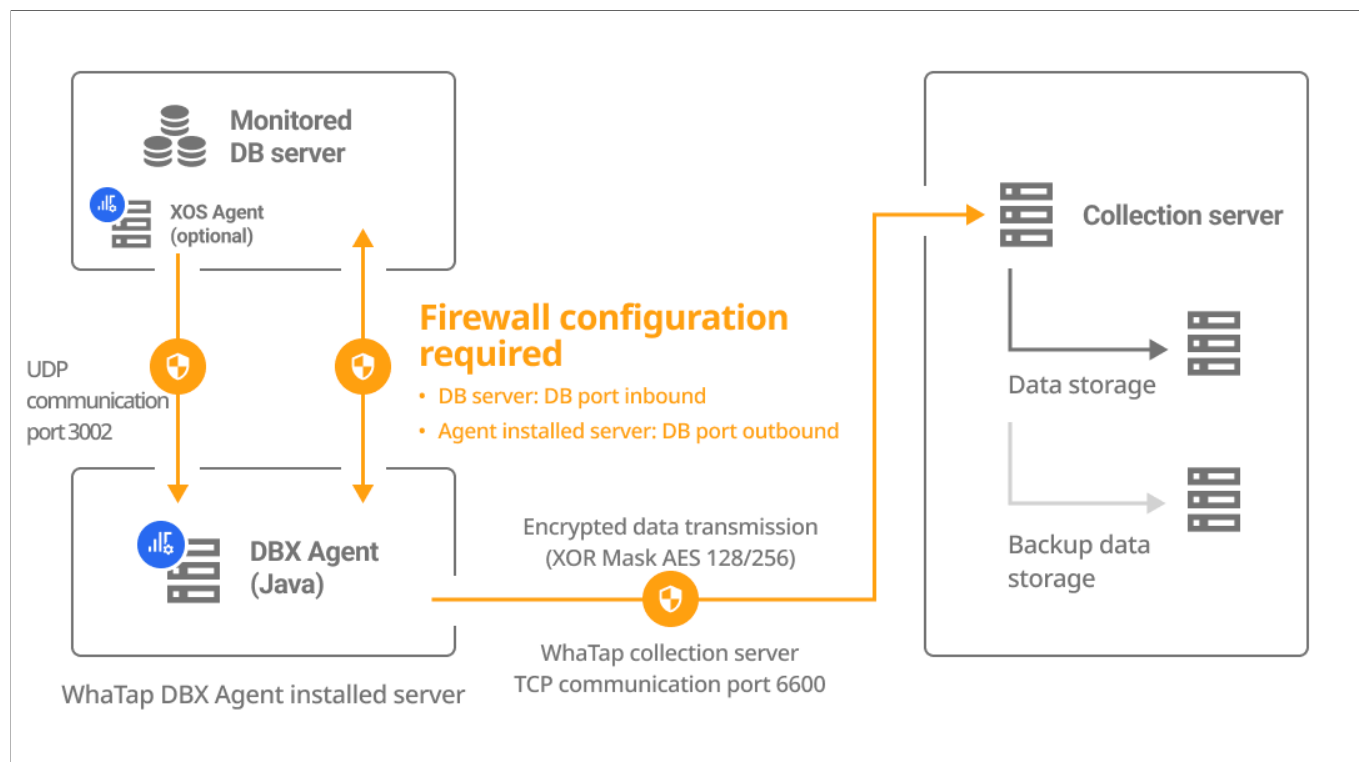
```
install_WindowsService.bat delete WhatapDBXAgent
```

データベースモニタリングのエージェントのインストールが完了しました。[次の文書](#)でインストール後、チェックリストを確認してください。

XOSエージェントのインストール及びその他のオプションを適用する

データベースサーバーのリソースをさらにモニタリングする場合は、データベースサーバーに別のXOSエージェントを実行してデータを収集できます。

- ① • x86アーキテクチャで動作するOS環境にのみ適用されます。
- 追加エージェントのインストールは、必須ではなく選択事項です。
- XOSエージェント設定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。



whatap.confファイルを設定する

DBXエージェントがインストールされたパスの`whatap.conf`ファイルに次のオプションを設定します。

whatap.conf

```
xos=1
xos_port=3002
```

`xos`フォルダー(/解凍されたフォルダ/`xos/`)をデータベースサーバーに移動してください。

xos.confファイルを設定する

データベースサーバーに移動し、`xos`パスの`xos.conf`ファイルに次のオプションを設定します。

xos.conf

```
dbx_ip={DB_Agent_IP}
```

```
dbx_port=3002 # default 3002
cpu_limit=0
mem_limit=10240
```

- ✓ エージェントインストールメニューのDB Agent IP、DB Agent Port項目にDB情報を入力すると、エージェントオプションを自動生成できます。

XOSエージェントを実行する

XOSエージェントを実行します。

```
./start.sh
```

- ⓘ
- DBXエージェントでモニタリングしたデータを転送するために dbx_port に設定したポート(default 3002)が開いている必要があります。(UDP Outbound)
 - XOSエージェントをバックグラウンドで実行するには*./startd.sh*ファイルを実行します。

次のステップ

インストールの点検

プロジェクトの作成やエージェントのインストール、基本エージェントのオプションまですべて適用した場合は、[次の文書](#)で点検事項を確認します。

インストール問題の解決

エージェントをインストールする際に発生する可能性がある問題と、これを解決するための具体的なガイドを提供します。詳細については、[次の文書](#)を参照してください。

エージェント設定

エージェント設定([whatap.conf](#))ファイルにオプションを適用して、モニタリングのための様々な機能を提供します。詳細については、[次の文書](#)を参照してください。

データベースのサーバーリソースを追加で監視するには、追加のエージェント(XOS)に追加オプションを設定します。詳細については、[次の文書](#)を参照してください。

モニタリングの開始

すべての設定を完了したら、エージェントがデータベースサーバーのメトリクスに対する情報収集を開始します。まず、**インスタンスリスト**メニューでモニタリングデータが収集されていることを確認します。**インスタンスリスト**の詳細については、[次の文書](#)を参照してください。

インストールチェックリスト

データベースモニタリングのインストールがすべて完了しました。インストール後に確認事項をチェックしてください。

エージェントのインストールチェック

データベースエージェントをインストールしたパスから、**start.sh**シェルスクリプトファイルまたは**start.bat**バッチファイルを実行します。エージェントを実行すると、データベースのモニタリング情報の収集が開始されます。シェルスクリプトを実行した後、ターミナルにWhaTapロゴが出力されている場合は、正常に実行されている状態です。

start.sh

```
$ ./start.sh
```

```

_      _      _
||/||| _ _/_ _||_
||/||_ \_`|||_`/_\
|_|_|_|/||\_,||\_,_|
      ||

```

Just Tap, Always Monitoring

WhaTap DBX version X.Y.Z YYYYMMDD

① デーモンのように使用したい場合は、`startd.sh` コマンドを実行してください。ただし、**nohup**をインストールされている環境のみで動作します。

ログの確認

- [whatap.log](#)

エージェントの起動および収集に関するすべてのログは、`$WHATAP_HOME /logs/whatap.log`ファイルで確認できます。

毎日0時(UTC)になると、既存のwhatap.logファイルはwhatap_ yymmdd .log形式に自動的にリネームされて日付

別に保存され、新しいwhatap.logファイルが作成されてログが記録されます。

日付別に保存されたログファイルは、7日が経過すると自動的に削除されます。

- xos.log

XOSの起動に関するログは、\$XOSのインストール先 /xos yymmdd .logファイルに記録され、日付別に自動生成されます。

エージェントプロセスの確認

次のコマンドを使用して、動作中のWhaTap DBXエージェントプロセスを確認できます。

```
$ ps -ef | grep dbx
```

モニタリングの確認

サーバーで正常にログが確認され、コンソールに正しく登録されたことを確認するには、WhaTapモニタリングサービスの初期画面に移動します。確認するプロジェクトを選択し、画面の左側の管理 > エージェントリストメニューを選択します。エージェントリストからデータベースサーバーの名前を確認できます。データベースサーバーの名前を別途設定する場合、次の文書を参照してください。

エージェントリスト											
Csv Download											
Agent Name, OID											
ステータス	名前 (初期)	ID	開始時間	活性 / 非活性	エージェントバージョン	Agent IP	DB IPアドレス	DB ポート	DB バージョン	CPU コア	
● 活性	DBX-2-60-6379	2122651642	2024-03-13 18:36:35	2024-03-13 18:36:35	1.6.32 20240306	172.17.0.1	192.168.2.60	6379	7.0.11	1	📄 🗑
● 活性	DBX-2-60-6380	-2134789231	2024-03-13 18:36:10	2024-03-13 18:36:10	1.6.32 20240306	172.17.0.1	192.168.2.60	6380	7.0.11	0	📄 🗑
● 活性	DBX-2-60-6381	-137985273	2024-03-13 18:36:15	2024-03-13 18:36:15	1.6.32 20240306	172.17.0.1	192.168.2.60	6381	7.0.11	0	📄 🗑
● 活性	DBX-2-60-6382	1859113661	2024-03-13 18:36:20	2024-03-13 18:36:20	1.6.32 20240306	172.17.0.1	192.168.2.60	6382	7.0.11	0	📄 🗑

インストール問題の解決

データベースエージェントのインストール時に発生する問題を確認してください。

ファイアウォール設定の確認

ファイアウォールのブロックを解除してください。WhaTapサーバーのTCPアウトバウンドファイアウォールが設定されていると、モニタリング情報をサーバーに転送できません。

ファイアウォールを確認する方法

telnet コマンドを実行し、接続関連情報をが正常に表示します。(telnet[サーバーIP][サーバーポート])

Example

```
$ telnet 52.193.60.176 6600
Trying 52.193.60.176...
Connected to 52.193.60.176.
Escape character is '^]'.
```

❗ WhaTapの収集サーバー情報は、**管理** > **エージェントインストール**メニューから確認できます。

制約事項

複数リージョンを1つのプロジェクトとして選択することはできません。

- [WhaTapモニタリングサービス](#)サイトでプロジェクトを作成する時にリージョンは重複選択できず、複数のリージョンを活用する場合は別途のプロジェクトを作成する必要があります。
- クラウド環境に複数のリージョン(Region)にサーバが存在する場合、ネットワークのlatencyなどパフォーマンス情報収集の制約を回避するために、リージョン(Region) 単位で収集サーバをインストールする必要があります。

- WhaTapは、顧客のニーズを満たすためにリージョン(Region)ごとに収集サーバーを構築します

エージェント名(ONAME) は重複使用できません

WhaTap DBXモニタリングは、エージェントを認識するために、エージェントのIPアドレスとポート(Port)情報を使用します。ユーザー環境でモニタリングするデータベースサーバーが同一IP、同一ポート(Port)を使用している場合、WhaTapサーバーのサーバーインスタンスを区分できません。

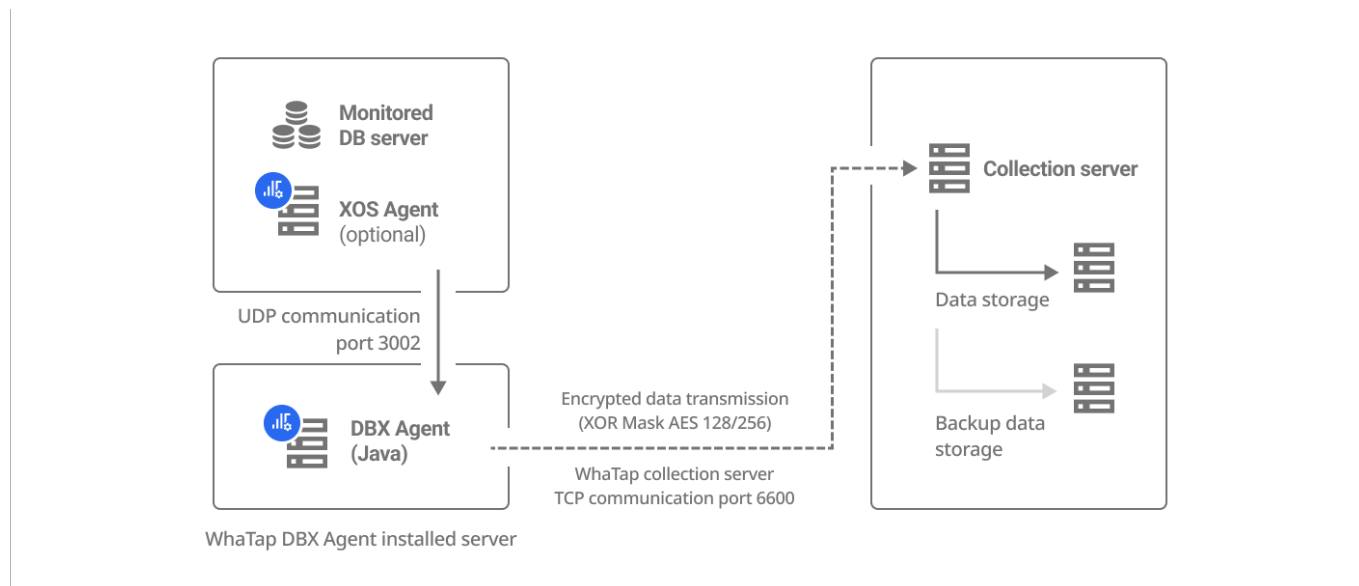
- サーバーインスタンスが動的に容量を可変に拡張される環境でない場合は、[次の文書](#)を参照してデータベース識別用の名前を直接変更することで、サーバーインスタンスを迂回できます。
- モニタリングするデータベースのinternal addressまたはネットワーク仮想化により重複したIPを使用している場合は、[次の文書](#)を参照して、別のデータベース名のパターンを使用してください。

設定

このページでは、WhaTapエージェントの構成について説明し、各種機能の設定方法について解説します。また、モニタリング対象となるDBサーバーのリソースを監視するためのオプション機能についても紹介します。

エージェント構成

以下は、WhaTapエージェントの構成図です。



• 収集サーバー

エージェントが収集したデータベースのパフォーマンスデータを収集および保存、統計情報を抽出し、これをユーザーに効率的な形式で提供します。収集サーバーはリージョン（Region）別に設定できます。リージョンごとに収集サーバーのアドレスが異なるように割り当てます。ユーザーが選択したリージョンによって収集サーバーのアドレスは異なる場合があります。プロジェクトを作成する際、リージョンも設定します。

• DBX エージェント(デフォルトエージェント)

Queryベースで性能データを収集し、サーバーに送信します。モニタリング対象データベースサーバーにエージェントを直接インストールしなくても、別のエージェントサーバーを使用してモニタリングすることができます。

• XOSエージェント(追加エージェント)

XOSエージェントは、データベースサーバーのプロセス使用量をモニタリングできる追加のオプションエージェントです。データベースサーバーのプロセス使用量をモニタリングしたい場合は、データベースサーバーにXOSエージェントを実行してデータを収集できます。

① XOSエージェントは、x86アーキテクチャベースで動作するOS環境のみ適用できます。

• ネットワーク

- 基本エージェント：WhaTapのモニタリングエージェントは、収集したモニタリング情報をWhaTap収集サーバーに転送するために外部通信（TCP）6600番ポートを使用します。
- XOSエージェント：エージェントをインストールしたサーバーとデータベースサーバーの間に外部通信（UDP）3002番ポートを使用します。ポートが重複する場合は、`dbx_port` オプションを使用してポートを変更します。

エージェント設定

エージェント設定の詳細については、次の文書を参照してください。

DBXエージェントの設定

MongoDBデータベースでwhatap.confファイルに設定できるオプションについて案内します。

XOSエージェント設定

MongoDBデータベースサーバーのリソースを追加でモニタリングするための設定方法を提供します。

クラウドエージェント

MongoDBデータベースクラウドエージェントの設定方法について案内します。

DBXエージェントの設定

DBXエージェントに必要な設定は、[whatap.conf](#)ファイルに作成されます。設定できるオプションについては、次を参照してください。

基本オプション

- **license** *String*

エージェントのインストール時にサーバーから付与されたプロジェクトアクセスキーを設定します。プロジェクトアクセスキーには、エージェントが属するプロジェクトとセキュリティ通信のためのパスワードキーが含まれています。

- **whatap.server.host** *String*

既定値 `127.0.0.1,127.0.0.1`

エージェントが収集したデータを送信するWhaTap収集サーバーのIPアドレスを設定します。収集サーバーの冗長化で2つ以上のIPを所有する場合は、コンマ(,)を区切り文字として使用します。設定したIPアドレスには、収集サーバーproxyデーモンがリスニング状態でサービスされる必要があります。

- **whatap.server.port** *String*

既定値 `6600`

収集サーバーのポート(port)を設定します。ポートは1つのみ設定ができるので、`whatap_server_host` に設定した収集サーバーは同一ポートを使用する必要があります。

- **dbms** *String*

`mongodb`

⚠ 別のオプション値を入力すると、モニタリングのデータ収集が正常に動作しない場合があります。

- **db_ip** *String*

モニタリングするデータベースサーバーのIPアドレスを設定します。

- **db_port** *String*

データベースが通信に使用するポート番号を設定します。

クラスター構成

- **cluster_name** String

クラスターセットを定義するオプションで、同じ `cluster_name` のオプション値を持つデータベースは、**ダッシュボード > インスタンスリスト**メニューでツリー構造で表示されます。**マルチインスタンス**メニューのエージェント選択オプションで**クラスター別エージェント**項目を選択してクラスターを構成するインスタンス同士がダッシュボードに表現され、一目でモニタリングできます。一部のウィジェットは、クラスター単位の情報を提供します。詳細については、[次の文書](#)を参照してください。

データ収集

- **db_param_enabled** Boolean

既定値 `true`

DBパラメータの収集有無を設定します。

- **conn_fail_count** Int

既定値 `15`

15回連続コネクションエラーが発生した時に通知を送信します。希望する回数を入力して、通知の発生基準を調整できます。

- **collections** Boolean

既定値 `true`

コレクションサイズ情報の保存有無を設定します。保存しないためには、`false` に変更します。

① このオプションに関する**DBサイズ**メニューの詳細については、[次の文書](#)を参考にしてください。

- **collections_hour** Int

既定値 `5`

コレクション情報を保存するために情報を収集する時刻を設定します。既定値は 5 で、午前5時に収集を始めます。

① このオプションに関するDBサイズメニューの詳細については、[次の文書](#)を参考にしてください。

ユーザーメトリック収集 (SQLMON)

SQLMON は、ユーザー定義の SQL 結果を定期的に収集し、メトリクスとして保存します。数値を返し、負荷が低いクエリに適しています。

- **sqlmon** Int

既定値: 1

- 1 : dbx と sqlmon を同時に実行
- 2 : sqlmon のみ実行

対応バージョン: 2.3.5 以上

設定

1. dbx エージェント配下に **sqlmon** ディレクトリを作成し、収集したいクエリを **<filename>.sql** ファイルとして作成します。

```
dbx/
├── sqlmon/
│   ├── active_sessions.sql
│   └── lock_count.sql
```

2. 収集するクエリを **<filename>.sql** ファイルとして保存します。

.sql ファイルの**1行目**に実行オプションを、**2行目以降**に SQL 文を記述します。

オプション形式

```
周期(分);動作時間;タグ名
SQL文
```

項目	説明	例
周期	実行周期（分単位）、最小値 1	1 → 1分ごとに実行
動作時間	HHMM-HHMM 形式、カンマ（,）で複数の時間帯を指定可能。0 の場合は常時実行	0900-1100 → 09:00～11:00のみ実行
タグ名	メトリクスに保存するタグ名。省略時はファイル名がタグ名として使用されます	whatap

例：1分周期、09:00～11:00動作、タグ名 whatap

```
1;0900-1100;whatap
SELECT count(*) FROM active_sessions
```

例：1分周期、常時動作、タグ名はファイル名を使用

```
1;0
SELECT count(*) FROM active_sessions
```

- ⓘ 動作時間は日付をまたいで設定できます。（例：2300-0100 → 23:00～翌日01:00）
- タグ名を省略する場合、動作時間の後にセミコロン（;）を付けないでください。
- SQL 文の末尾にセミコロン（;）を付けないでください。

- whatap.conf で SQLMON を有効化します。
- エージェントを再起動します。
- 🔗 サイトマップ > メトリクス照会 メニューで、sqlmon カテゴリを確認します。

```
# whatap.conf
sqlmon=1
```

AES256暗号化の適用

WhaTap DBXエージェントは、収集されたデータを暗号化してサーバーに送信します。データの重要度や設定によって変更できます。基本的にXOR演算とAESアルゴリズムによる暗号化を使用し、平文を128ビット単位に分割して暗号化、復号を行います。ユーザー設定により、256ビットまで拡張できます。

WhaTap DBXエージェントをインストールしたパスで、[whatap.conf](#)ファイルを次のオプションに追加します。

```
whatap.conf
```

```
1 cypher_level=256
```

設定を追加してから、エージェントを再起動してください。

エージェント名の設定

自動設定する

エージェント設定([whatap.conf](#))で名前を設定しないと、エージェント名はIP アドレスとポート番号が結合されて自動指定されます。例えば、IPアドレスが**10.11.12.13**であり、ポート番号が**3000**であれば、エージェント名は**DBX-12-13-3000**に設定されます。

エージェント名を決定する主な変数については、以下を参照してください。

設定	説明
<code>{type}</code>	DBX値を使います。
<code>{ip0}</code>	IPv4アドレスのうち、第1オクテットを使用します。(例：10.11.12.13のうち 10)
<code>{ip1}</code>	IPv4アドレスのうち、第2オクテットを使用します。(例：10. 11 .12.13のうち 11)
<code>{ip2}</code>	IPv4アドレスのうち、第3オクテットを使用します。(例：10.11. 12 .13のうち 12)
<code>{ip3}</code>	IPv4アドレスのうち、第4オクテットを使用します。(例：10.11.12. 13 のうち 13)

設定	説明
{port}	データベースサーバのポート

❗ RDSのようにIPアドレスが数字でなければDBX- {ip0} - {hash} - {port} 形式で名前が設定されます。ここで {hash} 値は、IPアドレスを4桁の16進数に変換した値です。

手動設定する

エージェント名を直接設定したい場合は、[whatap.conf](#)ファイルで `whatap.name` または `object_name` オプションに目的の名前を入力します。ユーザーが入力した名前がエージェント名として設定されます。

whatap.conf

```
whatap.name=agent-1234
# or
object_name=agent-1234
```

XOSエージェント設定

データベースサーバーのリソースをさらにモニタリングする場合は、データベースサーバーに別のXOSエージェントを実行してデータを収集できます。

- ❗ • x86アーキテクチャで動作するOS環境にのみ適用されます。
- XOSエージェントのインストールについての詳細は、[次の文書](#)を参照してください。

whatap.confファイルの設定

XOSエージェントを実行する前に、[whatap.conf](#)ファイルで、以下のオプションを設定します。

- **xos** **Int**

既定値 0

XOSエージェントを使用するかどうかを設定します。0 に設定するとXOSからのデータは収集されません。1 に設定するとすべてのXOSからのデータを収集します。IPアドレスを設定する場合、そのIPアドレスが一致するXOSからのデータのみ収集します。

- **xos_port** **String**

既定値 3002

XOSエージェントと通信するポートを設定します。XOSエージェントはUDPで通信します。ファイアウォールでUDPポートがブロックされている場合は、該当ポートを開放してください。

- **xos_cpu_iowait** **Int**

既定値 1

XOSエージェントから収集したCPU使用率にiowaitを追加できます。1 に設定するとiowaitが追加され、0 に設定するとiowaitは追加されません。

- **xos_mem_buffcache** **Int**

既定値 0

XOSエージェントから収集したメモリ使用率にbuffcacheを追加できます。1 に設定するとbuffcacheが追加され、

0 に設定するとbuffcacheは追加されません。

xos.confファイルの設定

xosディレクトリをデータベースサーバーにコピーし、xos.confファイルにエージェントサーバー情報を入力して追加オプションを設定してください。

- **dbx_ip** String

DBXエージェントをインストールしたサーバーのIPアドレスを入力します。

- **dbx_port** String

既定値 3002

DBXエージェントと通信するポートを設定します。

DBXエージェントは、UDPで通信します。ファイアウォールでUDPポートがブロックされている場合は、該当ポートを開放してください。

- **cpu_limit** Int

既定値 0

limitの設定値より大きい値を持つプロセス情報を収集します。1/100%単位で1.23%の場合、123として設定します。

- **mem_limit** Int

既定値 10240

limitの設定値より大きい値を持つプロセス情報を収集します。単位は「KB」で既定値である10240は、10MBになります。(1024 KB = 1 MB)

- **disk_usage_interval** Second

既定値 60

インスタンス別のディスク使用率と使用可能サイズ、全体サイズ情報を表示します。値が'0'の場合、ディスク使用率は収集しません。

- **port_check** String

接続状態をチェックするサーバーとポートを指定します。IP:Portの形式で設定し、コンマ(,)で区切って複数登録が

可能です。接続ができないサーバーとポートの一覧は、`db_port_check` カテゴリに保存されます。

xos.conf

```
port_check=192.168.122.113:3333,192.168.122.113:3334
```

接続ができなかったサーバーとポートの一覧を確認する場合、**分析>メトリクス照会メニュー**で `db_port_check` カテゴリを選択します。

-	Time	Oid	Tags	Fields	
			oname	error_count 	port_list
1	2025-01-17 18:39:41	1064156037	DBX-5-112-1521	2	192.168.122.113:3333,192.168.122.113:3334
2	2025-01-17 18:39:41	1064156037	DBX-5-112-1521	2	192.168.122.113:3333,192.168.122.113:3334
3	2025-01-17 18:39:51	1064156037	DBX-5-112-1521	2	192.168.122.113:3333,192.168.122.113:3334
4	2025-01-17 18:39:51	1064156037	DBX-5-112-1521	2	192.168.122.113:3333,192.168.122.113:3334

• process_check String

プロセスの実行状態をモニタリングできます。オプション値でプロセス名を入力します。コンマ(,)を区切り文字として使用し、複数登録することができます。

xos.conf

```
process_check=pmon,smon,tnslsnr,melong,haha
```

指定された文字列を含むプロセス名が検知されない場合、`db_process_check` カテゴリにその文字列の一覧を保存します。例えば、**melong**、**haha**の2つのプロセスがない場合、**分析>メトリクス照会メニュー**で `db_process_check` カテゴリを選択した後、確認できます。

-	Time	Oid	Tags	Fields	
			oname	error_count 	process_name
1	2025-01-17 18:35:06	1064156037	DBX-5-112-1521	2	melong,haha
2	2025-01-17 18:35:06	1064156037	DBX-5-112-1521	2	melong,haha
3	2025-01-17 18:35:12	1064156037	DBX-5-112-1521	2	melong,haha
4	2025-01-17 18:35:12	1064156037	DBX-5-112-1521	2	melong,haha

- ① `process_check` オプションを使用して、データベースで実行されているプロセスが終了した場合はアラート通知を送信できます。詳細は[次の文書](#)を参照してください。

- **process_check_interval** Second

既定値 `6`

`process_check` オプションに設定されたプロセスの実行状況を確認する間隔を設定します。(単位：秒)

- **iplist_interval** Second

既定値 `0` (off)

DBサーバーのIP一覧を収集する間隔を設定します。(単位：秒、3以上で設定)

- ① [whatap.conf](#)のファイルに `xos_dbip=true` オプションを設定すると `db_ip_list` のカテゴリに転送します。[分析 > メトリクス照会](#)メニューで `db_ip_list` カテゴリを選択した後、確認することができます。

- **file** String

[ログメニュー](#)([ログTail](#)、[ログトレンド](#)、[ログ検索](#)、[ログ設定](#))を使用するには、`file` オプションにモニタリングするログファイル名のフルパスを入力します。

`xos.conf`

```
file=/var/log/mongodb/mongodb.log
```

- ✓ モニタリングするログファイルを追加するには `file`、`file1`、`file2` といった方法でオプションを追加します。

`xos.conf`

```
file={log_file_path1}
file1={log_file_path2}
file2={log_file_path3}
file3={log_file_path4}
```

ユーザーメトリクス収集 (SHMON)

SHMONはユーザー定義のシェルスクリプトの実行結果を定期的に収集し、メトリクスとして保存します。

- **shmon** Int

既定値: 1

対応バージョン: dbx 2.55.01以降 & xos 1.2.0f以降

設定

1. エージェントのインストールパスに `shmon` ディレクトリを作成します。
2. 収集するスクリプトを `.sh` ファイルとして保存します。
3. `xos.conf` でSHMONを有効にします。
4. エージェントを再起動します。
5. [🔍 サイトマップ](#) > [メトリクス照会](#) メニューで、`shmon` カテゴリを確認します。

```
# xos.conf
shmon=1
```

- ❗ • `file` オプションは、DBXエージェントの1.7.0バージョン以降に対応しています。
- ログメニューの詳細は[次の文書](#)を参照してください。

XOSエージェントの実行

データベースサーバーで次のバッチファイルを実行してください。

```
$ ./start.sh

# または

$ ./startd.sh #バックグラウンドで実行する場合
```

クラウドエージェント

この文書は、AWS環境でWhaTapクラウドエージェントを設定するためのガイドです。主要設定項目、フィールドの説明、権限構成、実行コマンドまで含めて、運用環境にすぐに適用できるように構成されています。

エージェント設定

AWS DocumentDBエージェントの設定方法です。

AWS DocumentDBエージェント

config.yaml

```
input:
  csp: "aws" # クラウドサービスのプロバイダーを入力します。
  namespace: "docdb"
  region: "ap-northeast-1" # インスタンスが位置するリージョンを設定します。
  instances: # 指定したインスタンスは常に収集されます。クラスター内のインスタンスをここに指定すると、オートスケールに関係なく収集されます。
    - name: "docdb-instance-name" # インスタンス名
      slow_query: true # スロークエリページを利用する場合は true に設定してください。
  clusters:
    autoscale:
      enabled: false # オートスケールが有効な場合、スケーリングされたインスタンスを収集対象に追加または削除します。
      interval: 60 # 指定したクラスターのオートスケール確認間隔です。（単位: 秒）
    names:
      - "docdb-cluster-name"
  metrics: # 収集するメトリクスを入力します。
    - "CPUUtilization"
    - "FreeStorageSpace"
    - "FreeableMemory"
    - "ReadLatency"
    - "WriteLatency"
  logs:
    enabled: false # ログ収集の有無を設定します。true/falseで設定できます。
    groups: # 収集するAWSロググループを入力します。
```

```
- "/aws/rds/cluster/docdb-cluster-name/error"
- "/aws/lambda/MyLambda"
```

output: # 収集したメトリックデータを受信するWhaTap情報を入力します。

```
license: "abcdefg-higjkgjk-zxcvnbmbmc"
```

```
host: "127.0.0.1"
```

フィールド	説明
csp	クラウドサービスの提供者として aws (Amazon Web Services)を意味
namespace	収集対象サービスのネームスペース - AWS DocumentDB設定時固定値で docdb 入力
region	AWSリージョンコード - 例: ap-northeast-1 (東京リージョン)
instances	常に収集するインスタンスの一覧で、オートスケール有無に関係なく、指定されたインスタンスは無条件に収集する
instances[].name	DocumentDBインスタンス名 - 例 docdb-2025-04-08-01-21-05
clusters	DocumentDBクラスター関連設定
clusters.autoscale.enabled	クラスターオートスケール収集有無 - true: 自動的にインスタンスを追加/削除して収集 - false: instances に直接入力したインスタンスのみ収集対象に含める
clusters.autoscale.interval	オートスケール有無を感知する周期(単位:秒)
clusters.names	オートスケール有無をチェックするクラスター名の一覧
metrics	収集するメトリック項目のリスト - 例 CPUUtilization、FreeableMemory など - 参考 Amazon DocumentDB指標公式文書
output.license	収集されたデータを転送するWhaTapのライセンスキー

フィールド	説明
output.host	収集データを転送するWhaTapサーバーのホストアドレス(IP)

① クロスアカウントモニタリング（マルチAWSアカウント）

- ① 単一のクラウドエージェントで複数のAWSアカウントのDocumentDBをモニタリングできます。マルチアカウント（環境別分離、パートナーアカウントなど）を使用する場合、アカウントごとにエージェントをインストールする必要はなく、1つのエージェントからSTS AssumeRoleで他のアカウントのリソースを照会します。

項目	内容
対応対象	AWS DocumentDB
認証方式	EC2 Instance Profile + STS AssumeRole

設定方式の選択

クラスター設定には2つの方式があり、同時に使用することはできません。

- **names** : 単一アカウント専用（エージェントがインストールされたEC2のIAM Roleで自アカウントのみ照会）
- **account_configs** : クロスアカウント対応（STS AssumeRoleを通じて複数アカウントを照会）

account_configs 設定

config.yaml

```
input:
  csp: "aws"
  namespace: "docdb"
  region: "ap-northeast-2"
clusters:
  autoscale:
    enabled: true
    interval: 300
```



```

account_configs:
  # ローカルアカウント
  - clusters: ["local-docdb-cluster"]

  # 別のアカウント
  - assume_role_arn: "arn:aws:iam::111111111111:role/DBXCRole"
    clusters: ["partner-docdb-cluster"]
metrics:
  - "CPUUtilization"
  - "FreeableMemory"
  - "ReadLatency"
  - "WriteLatency"
  - "DatabaseConnections"

output:
  license: "your-license-key"
  host: "127.0.0.1"

```

表 | account_configs フィールド

フィールド	必須	説明
assume_role_arn	X	STS AssumeRole ARN。省略するとローカルアカウントを使用
clusters	O	DocumentDBクラスター名。所属インスタンスを自動検出
instances	X	クラスターに属さないスタンドアロンインスタンス名

❗ clusters と instances の違い

	clusters	instances
対象	DocumentDBクラスター	クラスターなしで単独運用される インスタンス

	clusters	instances
動作	クラスター名で所属インスタンスを自動ディスカバリー	インスタンス名を直接指定
オートスケール	インスタンスの追加/削除時に自動反映	該当なし

権限設定

エージェントが正常に動作するには、サービスごとに必要な権限を設定する必要があります。

AWS DocumentDB権限

クラウドエージェントはDocumentDBに対して、次の機能を実行します。

- DocumentDBインスタンスとクラスター情報の照会
- CloudWatchメトリック収集

DocumentDB用IAMインラインポリシー

JSONポリシーをIAMユーザーまたは役割にインラインポリシーで追加します。EC2でエージェントを実行する場合、当該EC2インスタンスに接続されたIAMの役割に付与します。

- Resource項目は、すべてのDocumentDBリソースを対象に指定されており、セキュリティポリシーによって必要な場合、リソースARNを制限できます。
- エージェントは照会(Read-only) APIのみ使用します。データベースに影響を与える権限は含まれません。

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```

{
  "Sid": "DocDBPermissions",
  "Effect": "Allow",
  "Action": [
    "docdb:DescribeDBInstances",
    "docdb:DescribeDBClusters"
  ],
  "Resource": "*"
},
{
  "Sid": "CloudWatchMetricsPermissions",
  "Effect": "Allow",
  "Action": [
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics"
  ],
  "Resource": "*"
},
{
  "Sid": "CloudWatchLogsPermissions",
  "Effect": "Allow",
  "Action": [
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "logs:FilterLogEvents",
    "logs:GetLogEvents"
  ],
  "Resource": [
    "arn:aws:logs:*:*:log-group:/aws/docdb/*"
  ]
}
]
}

```

クロスアカウントIAM権限



account_configs を使用してクロスアカウントモニタリングを設定するには、追加のIAM権限が必要です。



エージェントEC2 Instance Profile

エージェントが実行されるEC2に、対象アカウントのRoleをAssumeできる権限を付与します。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": [
        "arn:aws:iam::111111111111:role/DBXCRole",
        "arn:aws:iam::222222222222:role/QARole"
      ]
    }
  ]
}
```

対象アカウントのCross-Account Role

対象アカウントでエージェントアカウントからのアクセスを許可するRoleを作成します。

- **Trust Relationship:** エージェントアカウントを許可

```
{
  "Principal": {
    "AWS": "arn:aws:iam::<エージェントアカウントID>:role/DBXC-EC2-Instance-Role"
  },
  "Action": "sts:AssumeRole"
}
```

- **Permission Policy:** RDS/CloudWatch照会権限

```
{
  "Effect": "Allow",
  "Action": [
    "rds:DescribeDBInstances",
    "rds:DescribeDBClusters",
  ]
}
```



```
"cloudwatch:GetMetricData",
"logs:FilterLogEvents"
],
"Resource": "*"
}
```

料金案内

- ❗ クラウドモニタリングエージェントは無料ですが、クラウドサービスの使用によっては別途料金が発生することがありますので、確認が必要です。

AWS料金

クラウドモニタリングエージェントは別途のSaaS料金なしで提供され、エージェントのインストールだけでモニタリング機能を使用できます。ただ、AWS CloudWatchなどクラウドサービスのAPIを通じてメトリックを収集するため、CloudWatch使用量によって別途料金がかかる場合があります。

本エージェントは、基本的に1分周期でGetMetricData APIを呼び出ししてメトリックを収集し、呼び出し頻度と収集対象によって料金が増加することがあるので注意が必要です。

詳しい料金ポリシーは[AWS公式文書のAmazon CloudWatch料金](#)ページを参照してください。

- ❗
- names と account_configs は同時に使用できません。エージェント起動時にバリデーションエラーが発生します。
 - ARN形式を厳密に検証します。arn:aws:iam::<12桁の数字>:role/<名前> — コロン2つ(::)を省略しないよう注意してください。
 - 各 account_config には最低1つのclusterが必要です。
 - autoscale.enabled: true でないとクラスターディスカバリーが動作しません。

管理

エージェントのアップデート

最新バージョンにアップデートする

ホーム画面 > プロジェクト選択 > 管理 > エージェントアップデート

エージェントアップデート

エージェントアップデートのご案内

「アップデート」ボタンをクリックすると、最新のエージェントファイルがエージェントのインストール場所にダウンロードされ、自動的に再起動されます。アップデートには1分がかかります。完了すると、該当のエージェントのバージョンが最新バージョンに変更されます。

① Windows環境にインストールされたエージェントは、自己更新機能を提供していません。 [詳細](#)

② 更新が正しく行われない場合は、[WhaTap Docs](#) を参考してください。

エージェントリスト

最新エージェントのバージョン 2.3.3 [すべてのエージェントを最新バージョンに更新](#) [旧バージョン](#)

no.	id	ip	name	agent path	version	update
1	704779695	192.168.1.101	WhaTap-001	C:\Program Files\WhaTap\agent.exe	2.2.8 20241212	アップデート
2	1652207373	192.168.1.102	WhaTap-002	C:\Program Files\WhaTap\agent.exe	2.2.8 20241212	アップデート
3	755606486	192.168.1.103	WhaTap-003	C:\Program Files\WhaTap\agent.exe	2.1.4 20241101	アップデート

エージェントをアップデートすると、最新バージョンのエージェントファイルをエージェントインストールパス ([agent path](#))に自動的にダウンロードして再起動します。エージェントのアップデートには約1分かかり、アップデート過程でダウンロードとアップデートの成功メッセージが画面上に順番に表示されます。アップデートを完了すると、そのエージェントのバージョンが自動的に最新バージョンに変更されます。

- アップデートできるエージェントは、**アップデート**ボタンが活性化されます。
- エージェントを個別にアップデートするには、各エージェント項目の右側にある**アップデート**ボタンを選択します。
- すべてのエージェントを一度に更新するには、**すべてのエージェントを最新バージョンに更新**ボタンを選択します。

✔ エージェントのアップデート中に別のメニューに移動する場合は、進行状況を確認することはできず、1つのエージェントをアップデートしながら別のエージェントを同時にアップデートすることはできません。

- ❗ Windows環境にインストールされたエージェントは、自動更新機能をサポートしていません。手動で最新のエージェントに再インストールするか、最新の `whatap.agent.dbx-*.jar` ファイルを既存のエージェントパスに入れて、サービスを再登録します。

```
# 1. Delete Windows service
install_WindowsService.bat delete WhatapDBXAgent # existing service name

# 2. Create Windows service
install_WindowsService.bat create WhatapDBXAgent # existing service name
```

アップデートに失敗した場合

エージェントが再起動しない場合

アップデート中にダウンロード成功メッセージが表示されても、エージェントのバージョンが最新に自動的にアップデートされない場合は、手動でエージェントを再起動する必要があります。エージェントのインストールパス([agent path](#))で`stop.sh`、`startd.sh`バッチファイルを順番に実行します。

エージェント手動ダウンロード

ダウンロードができない環境の場合は、次の手順でエージェントのインストールを進めてください。

1. 管理 > エージェントインストールメニューに移動します。
2. インストールの案内セクションの2番項目で**Download**ボタンを選択し、最新バージョンのエージェントをダウンロードします。
3. ダウンロードしたファイルを解凍します。
4. `whatap.agent.dbx-X.Y.Z.jar` ファイルだけをエージェントインストールパス([agent path](#))にアップロードします。
5. `stop.sh`、`startd.sh`バッチファイルを順番に実行して、エージェントを再起動します。

前のバージョンに戻す

1. 画面右上の旧バージョンボタンを選択します。

2. ダウンロード可能なエージェントの一覧が表示されます。
3. 希望するバージョンを選択します。
4. 選択したバージョンに戻すエージェント項目で **ダウンロード** ボタンを選択します。
5. 選択したエージェントのインストールパスでエージェントファイルをダウンロードします。
6. エージェントのインストールパスで上位バージョンの `whatap.agent.dbx-X.Y.Z.jar` ファイルを削除します。
7. `stop.sh`、`startd.sh` バッチファイルを順番に実行して、エージェントを再起動します。

❗ バッチファイルがエージェントのインストールパスで最も高いバージョンのエージェントファイルを実行するように設定されているため、上位バージョンのJARファイルを削除しないと、以前のバージョンのエージェントを実行できません。

エージェント削除

エージェントがインストールされたサーバーから削除する

• [Linux](#) [Windows](#)

サーバー上で起動されるJavaプロセスから、`whatap.agent.dbx` 文字列を含むプロセスを終了します。エージェントをインストールしたパスから`stop.sh`を実行します。その後、エージェントファイルとエージェントに登録したUser権限を削除します。

サーバー上で起動するJavaプロセスからエージェントファイル名のjarファイルで起動中のプロセスを見つけて停止します。もし、batファイルをForegroundで実行中の場合は、そのbat実行スクリプトを終了します。その後、エージェントファイルとエージェントに登録したUser権限を削除します。

サービス画面から削除する

WhaTapモニタリングサービスからエージェントを削除するには、**エージェントリスト**メニューに移動します。エージェントを削除する前に、エージェントをインストールしたサーバーでエージェントプロセスを終了する必要があります。

1. プロジェクトリストからエージェントを削除するプロジェクトを選択します。

2. 左側のメニューから**管理** > **エージェントリスト**を選択します。
3. **エージェントリスト**で削除するエージェントで右側の  ボタンをクリックします。

- ⓘ • 非活性化状態のエージェントのみ削除できます。

ステータス	名前 (初期)	ID
 活性	 	
 非活性	 	
 活性	 	

- エージェントのバージョンによっては、削除機能をサポートしていない場合があります。最新バージョンのエージェントに更新します。

ダッシュボード

WhaTapエージェントのインストールが完了しましたら、[WhaTapモニタリングサービス](#)にログインしてください。初期画面はプロジェクトリストです。プロジェクトリストで作成したプロジェクトを確認できます。プロジェクトリストで作成したプロジェクトを選択すると、[インスタンスリスト](#)が表示されます。

WhaTapデータベースモニタリングサービスでダッシュボードは、プロジェクトの全体のステータスを一目で確認できる機能です。モニタリングされているリソース全体の使用量を確認でき、リアルタイムダッシュボードでモニタリング対象のリソースをフィルタリングできます。

- 主なパフォーマンス指標とステータスを表示するように構成されています。パフォーマンス指標は5秒間隔で更新されます。
- 現在使用中のアクティブセッション(Queryを含む)、ロック情報および、プロセス情報を確認することができます。Public CloudとPrivate Cloudの両方に対応するために、クエリベースのモニタリングを使用して構成しました。
- 1つのインスタンスで複数のDBをフィルタリングできます。
- 収集したデータに基づいて、特定の1日あたりの全体的なトレンドを分析できる機能を提供します。特定の時間に進行中だったセッションを特定し、低速なQueryを分析することができます。

インスタンスリスト

エージェントをインストールしたデータベースサーバーの一覧を確認できます。主なパフォーマンス指標と状態(Status)を表示できるように構成されています。パフォーマンス指標は5秒間隔で更新され、一覧のカラムは設定を使用して目的のカラムに配置できます。詳細については、[次の文書](#)を参照してください。

インスタンスモニタリング

- データベースサーバーの主要メトリクスとアクティブセッションに関する詳細情報をリアルタイムでモニタリングし、問題になる可能性のあるアラートを確認できます。関心のある重要メトリクスを選択して、全体的なシステム状況をモニタリングできます。
- リアルタイムモニタリングは、5秒間隔でパフォーマンス指標をモニタリングします。実行中の**アクティブセッション**、**ロックツリー**、**プロセス情報**を確認できます。

詳細については、[次の文書](#)を参照してください。

マルチインスタンス

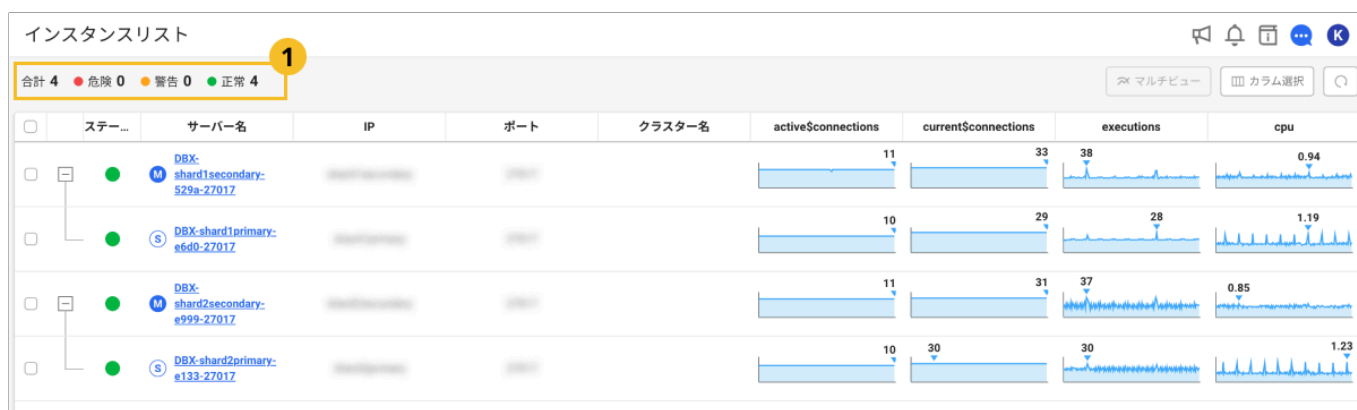
プロジェクトに登録されたすべてのインスタンスを5秒間隔でリアルタイムでモニタリングします。特定のインスタンスにフィルタリングしてモニタリングすることもできます。詳細については、[次の文書](#)を参照してください。

インスタンスリスト

ホーム画面 > プロジェクト選択 > ダッシュボード > インスタンスリスト

エージェントをインストールしたデータベースサーバーの一覧を表示し、各インスタンスの主要なパフォーマンス指標と状態が把握できます。パフォーマンス指標は、5秒間隔で更新されるし、カラム選択ボタンで表示する指標を選択できます。

基本画面ガイド



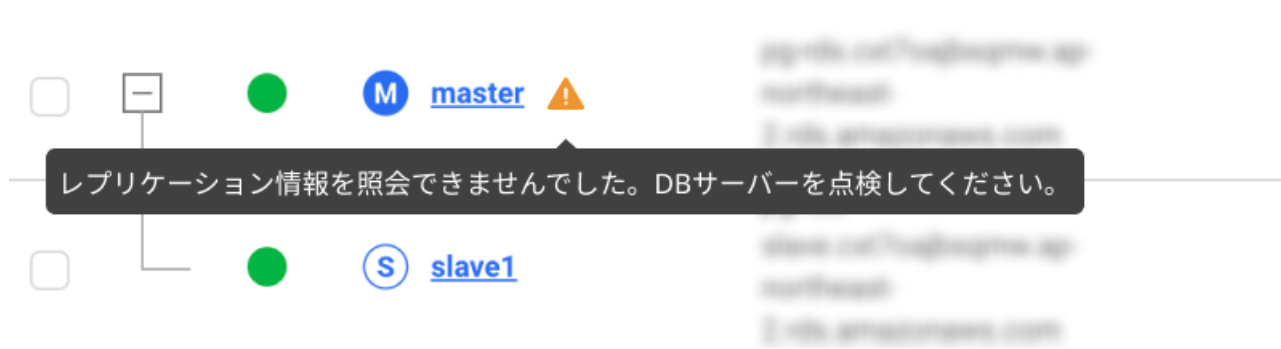
- ① 領域は、プロジェクトに設定されているインスタンスの状態を表示します。合計にはテーブルに表示中のインスタンスの数、危険、警告、正常にはステータスカラムの各ステータスの数が表示されます。
- ステータスカラムで正常ではない状態のアイコンをクリックするとイベント画面が表示されます。そのインスタンスで発生したイベントの履歴を確認できます。
- 各インスタンスを選択すると、**インスタンスモニタリング**メニューが表示されます。選択したインスタンスの詳細をリアルタイムでモニタリングできます。

❗ インスタンスモニタリングメニューの詳細については、[次の文書](#)を参考にしてください。

- 主要なパフォーマンス指標をグラフチャート形式で提供します。最も高い数値をチャートに表示します。チャートにカーソルを合わせると、その場所の数値が表示されます。パフォーマンス指標の詳細については、[次の文書](#)を参照してください。

- インスタンスリストでサーバー名カラムに表示された **M**、**S**、**C** は、それぞれMaster、Slave、Clusterを意味します。Replicationで構成したDBの場合に表示します。

Replicationインスタンスが異常な状態の場合  アイコンが表示されます。



- 画面右上の  ボタンをクリックすると、リアルタイムの通知が確認できます。通知設定の詳細については、[次の文書](#)を参照してください。

① 画面上部にある固定領域の詳細については、[次の文書](#)を参照してください。

- ✓ インスタンスリストのサーバー名を変更するには、エージェント設定(whatap.conf)で `object_name` オプションを利用します。詳細については、[次の文書](#)を参照してください。

インスタンス性能指標の比較

2つ以上のインスタンスを選択して、性能指標を比較できます。性能指標を比較するインスタンスを一覧から選択すると、画面右上のマルチビューボタンが活性化されます。マルチビューボタンを選択すると、マルチインスタンスメニューに移動します。主要な性能指標のデータを比較したグラフチャートとアクティブセッション、ロックツリーに関する詳細情報を確認できます。

- ① マルチインスタンスメニューの詳細については、[次の文書](#)を参考にしてください。

カラム表示または非表示

インスタンスリストのパフォーマンス指標カラムを表示または非表示できます。画面右上の**カラム選択**ボタンをクリックします。目的の項目を選択、または解除します。カラムを表示または非表示できます。

インスタンスモニタリング

ホーム画面 > プロジェクト選択 > **ダッシュボード** > インスタンスモニタリング

インスタンスモニタリングメニューでは、データベースサーバーのコア指標とアクティブセッションに関する詳細情報をリアルタイムでモニタリングし、問題のあるアラートを特定できます。デフォルトでは、過去10分間の収集データをリアルタイムで表示します。収集データは5秒間隔で更新します。

基本画面ガイド



1 検索時間と検索先を選択します。

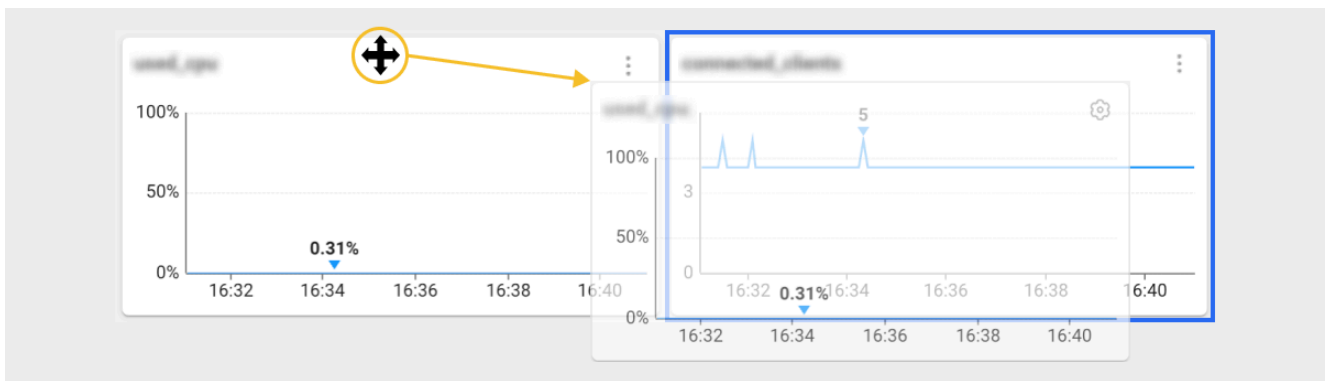
基本的に、直近10分間の収集されたデータをリアルタイムで表示します。時間とインスタンス項目から時間と対象を選択すると、収集データが2 グラフチャートと4 のアクティブセッションテーブルに自動的に反映されます。

- 過去のデータを照会するには、**時間**で緑のボタンをクリックし、希望の照会時間を選択します。過去3週間までのデータを表示できます。
- 任意の日時を照会するには**時間**で **II** ボタンを選択します。日付と時間テキスト領域をクリックして、日付と時間を選択するオプションを表示します。再度、リアルタイムでデータを検索します **▶** ボタンを選択します。
- 他のエージェントのデータを照会するには、**インスタンス**をクリックし、目的のエージェント名を選択します。

2 グラフチャートセクション

3 Default プリセットで保存された16個の指標をグラフチャート形式のウィジェットで表示します。横軸は時間、縦軸は各指標の数値です。各指標の意味を知りたい場合は、名前の横の ⓘ ボタンを選択するか、[次の文書](#)を参照してください。

- 他のウィジェットの位置を変更する場合は、ウィジェットの上部を選択した状態でドラッグします。ただし、ウィジェットのサイズは変更できません。



- 時間の**リアルタイム照会**モードを停止し、ウィジェットでチャートの特定時間をクリックすると、選択した時間の実行したセッション情報を **4 アクティブセッションテーブル**で確認できます。その後、**アクティブセッションテーブル**の上に、5秒単位でデータを照会できるタイムバーが表示されます。

- ① ◦ 選択した時間は、**アクティブセッションテーブル**の右上で確認できます。
- **アクティブセッションテーブル**一覧の文字の色は黒 → オレンジ → 赤の順にセッションの実行速度が遅いことを意味します。

- リアルタイム照会モードを停止した後、ウィジェットの右上の ⓘ ボタンをクリックすると、チャートデータをCSVファイルにダウンロードできます。

4 アクティブセッション / ロックツリー / プロセス情報

リアルタイムで実行中のアクティブセッションおよびロックツリー、プロセス情報を照会できます。ウィジェットのチャートで特定の時間を選択すると、**リアルタイム参照モード**が停止し、選択した時間に実行したセッション情報がテーブルに表示します。テーブルの上には5秒単位でデータを検索できる時間選択ボタンが表示されます。

• アクティブセッション

リアルタイムで実行中のセッションを照会することができます。詳しい内容は、[次の文書](#)を参考にしてください。

• ロックツリー

ロックセッションに関する情報やHolderとWaiter情報をリアルタイムで照会できます。テーブルのカラムの詳細については、[次の文書](#)を参照してください。

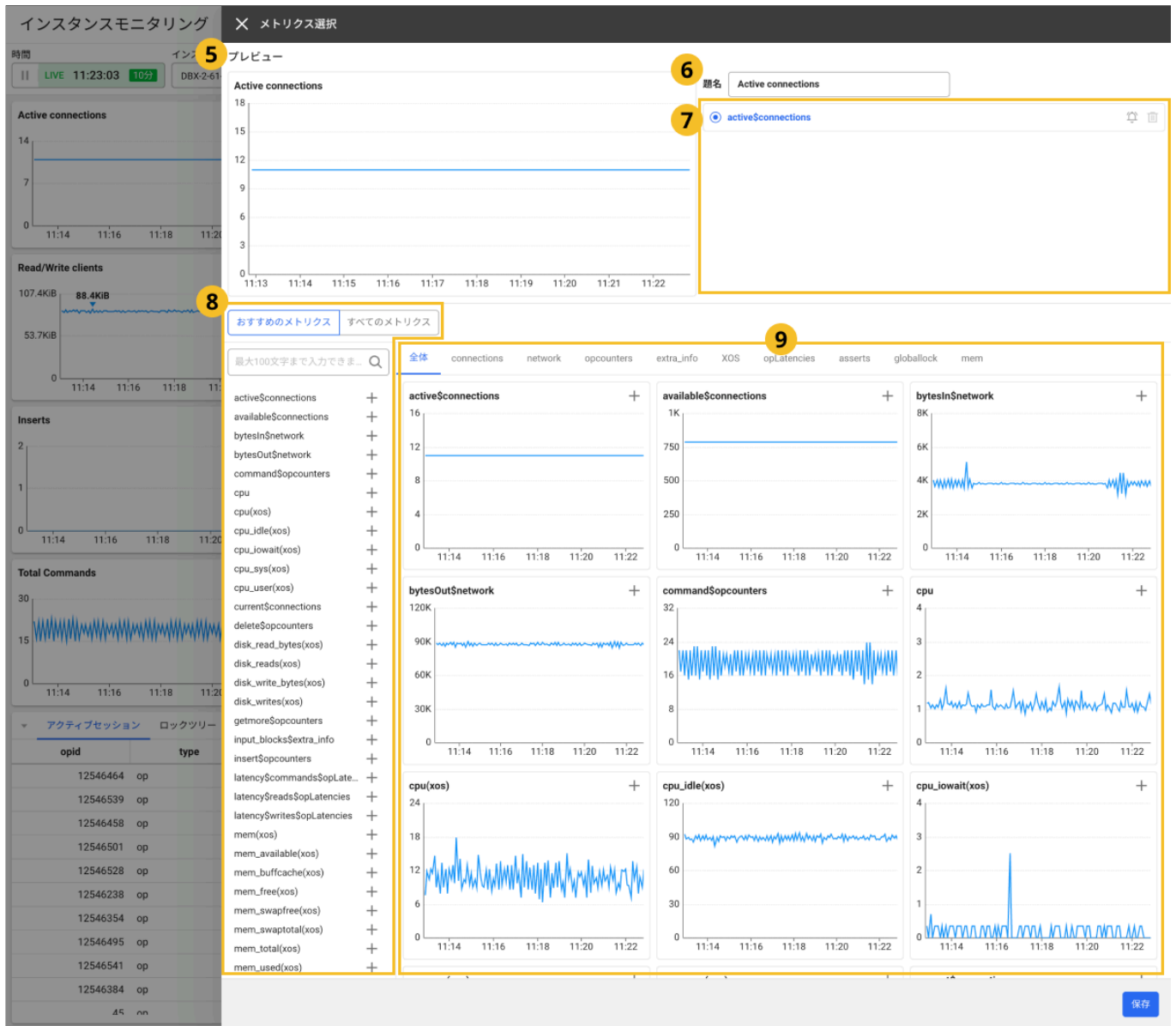
• プロセス情報

データベースサーバーのリソース使用量をリアルタイムで表示できます。

- ① • テーブル一覧の文字の色は黒 → **オレンジ** → **赤**順にセッションの実行速度が遅いことを意味します。
- **プロセス情報**は、XOSエージェントをインストールしないと確認できません。詳細については、[次の文書](#)を参照してください。

メトリクスを選択する

ウィジェットに指標グラフを追加または置換するには、**⋮** ボタンを選択します。**メトリクス選択画面**が表示されます。設定を完了して**保存**ボタンを選択します。



- **5 プレビュー**：選択した指標のグラフのプレビューを確認できます。
- **6 題名**：ウィジェット名を入力します。
- **7** 現在選択されているウィジェットのチャートで表示されるメトリクス項目が表示されます。最大4つのメトリクスを選択できます。

① メトリクス項目の右側に🔔ボタンを選択すると、そのメトリクスに基づいてアラート通知を設定できるイ

① **ベント設定** *New* メニューに移動できます。

- **8** **おすすめのメトリクス / すべてのメトリクス**：おすすめのメトリクスを選択すると、データベースモニタリングで頻繁に表示される指標のリストが表示されます。一覧に表示されている指標をウィジェットの指標に変更または追加できます。
- **9** 領域で指標の推移をグラフで確認し、ウィジェットの追加または変更することができます。目的のタブを選択して、メトリクスのリストをカテゴリ別に絞り込むことができます。

指標の追加

ウィジェットに2つ以上の指標を追加できます。最大4つまで追加できます。

1. 指標を追加するウィジェットの右上の **⋮** ボタンを選択します。
2. **メトリクス選択** ウィンドウが表示されると、**8** メトリクス一覧または **9** グラフ一覧で追加する指標の右側にある **+** ボタンを選択します。
3. 指標をさらに追加する場合は、2の手順を繰り返します。
4. ウィジェットを簡単に識別できるように **6** 題名を変更します。
5. 画面の右下にある **保存** ボタンを選択します。

指標を追加したウィジェットに追加した指標の数に対してチャートが作成されます。ウィジェット名の横にある **①** ボタンを選択すると、追加した指標の名前と内容を確認できます。また、チャートにカーソルを合わせると、ツールチップから数値を確認できます。

❗ ① ボタンのツールチップ機能は多言語ではサポートされていません。

指標の変更

ウィジェットの指標を別の指標に変更できます。

1. 指標を変更するウィジェットの右上の **⋮** ボタンを選択します。
2. **メトリクス選択** ウィンドウが表示されると、**7** 領域で変更する指標を選択します。

3. ⑧ メトリクス一覧または ⑨ グラフ一覧から目的の指標を選択します。
4. ⑦ 領域で選択した指標の名前が変更されたことを確認してください。
5. 画面の右下にある**保存**ボタンを選択します。

指標の削除

ウィジェットに複数の指標を設定されている場合は、不要な指標を削除できます。

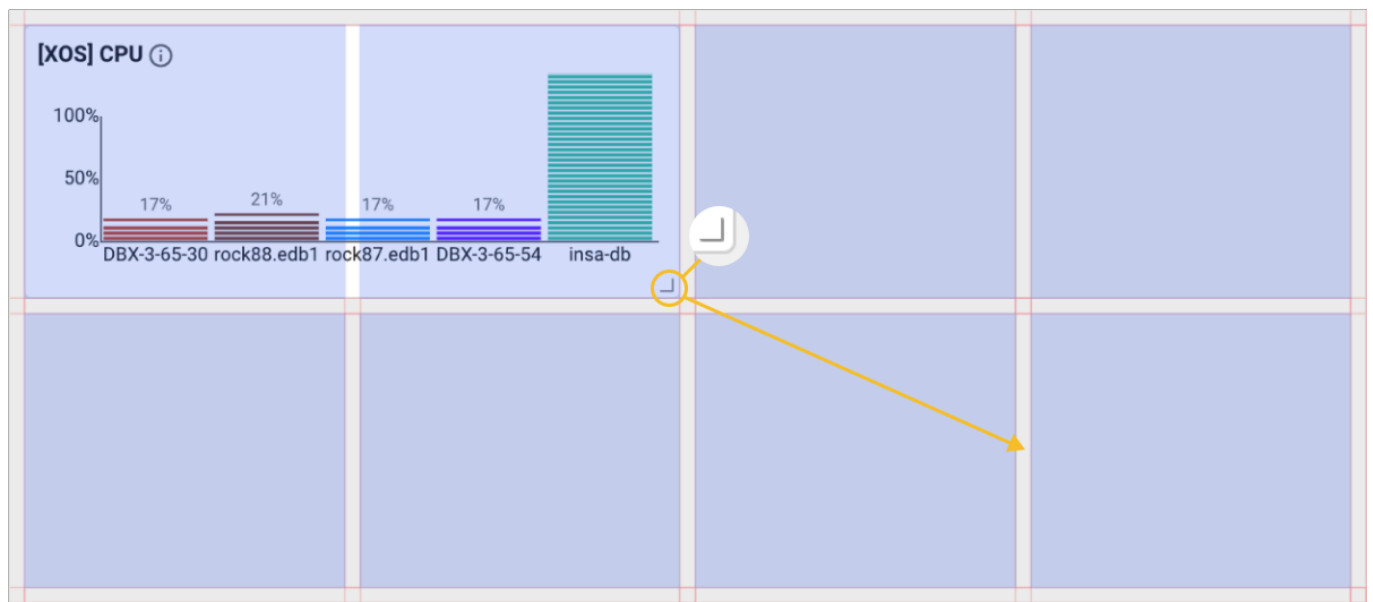
1. 指標を削除するウィジェットの右上の ⋮ ボタンを選択します。
2. **メトリクス選択**ウィンドウが表示されると、⑦ 領域から削除する指標の右側の  ボタンを選択します。
3. 画面の右下にある**保存**ボタンを選択します。

❗ ウィジェットには、少なくとも 1つの指標を選択する必要があります。ウィジェットのすべての指標を削除できません。

ダッシュボードウィジェットの編集

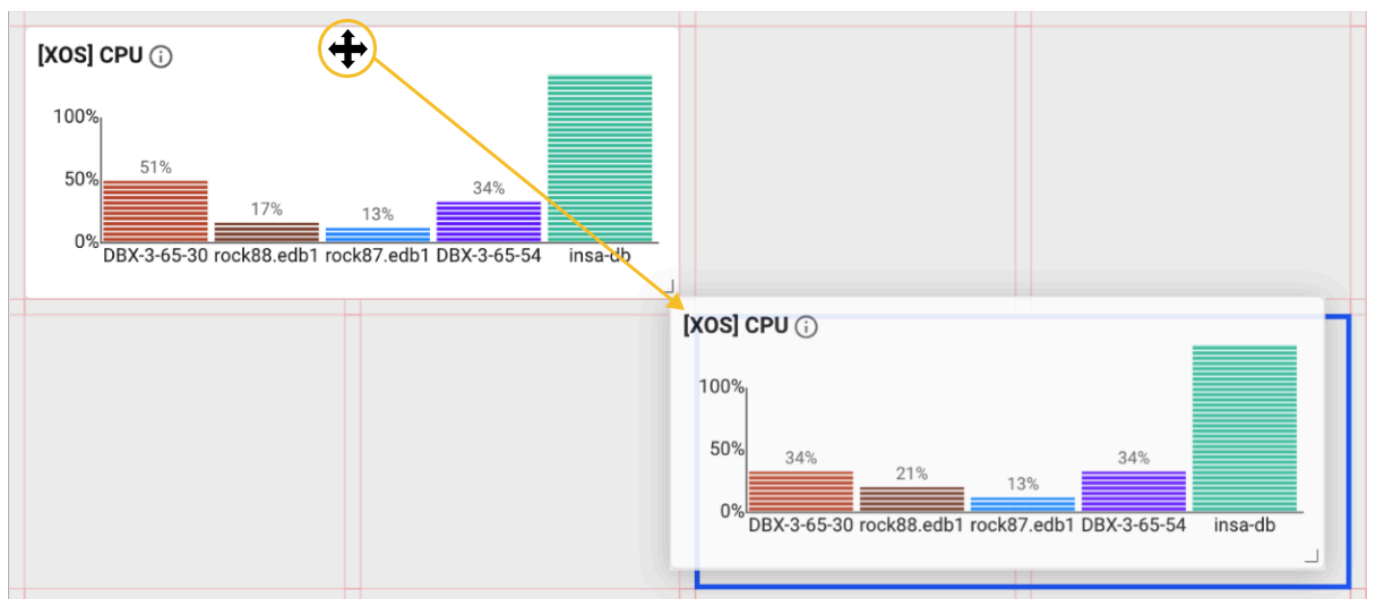
ダッシュボードに配置したウィジェットは、ユーザーが希望するサイズに調整でき、任意の位置に配置できます。るウィジェットは削除したり、再度追加したりすることもできます。

ウィジェットのサイズ変更



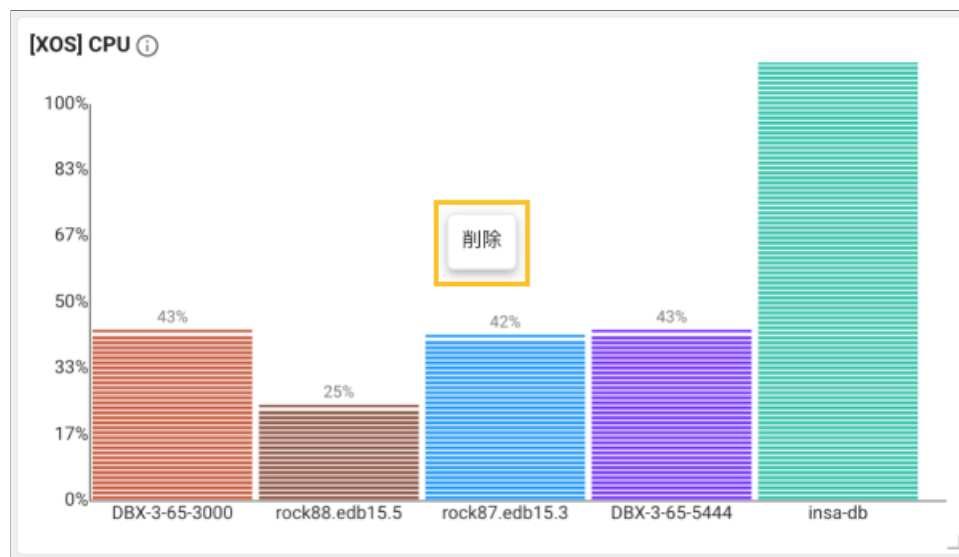
ウィジェットの右下にある「」をマウスでクリックした状態で希望するサイズにドラッグします。幅と高さの比率が均一なグリッドが表示され、グリッド単位でウィジェットのサイズを調整できます。

ウィジェットの移動



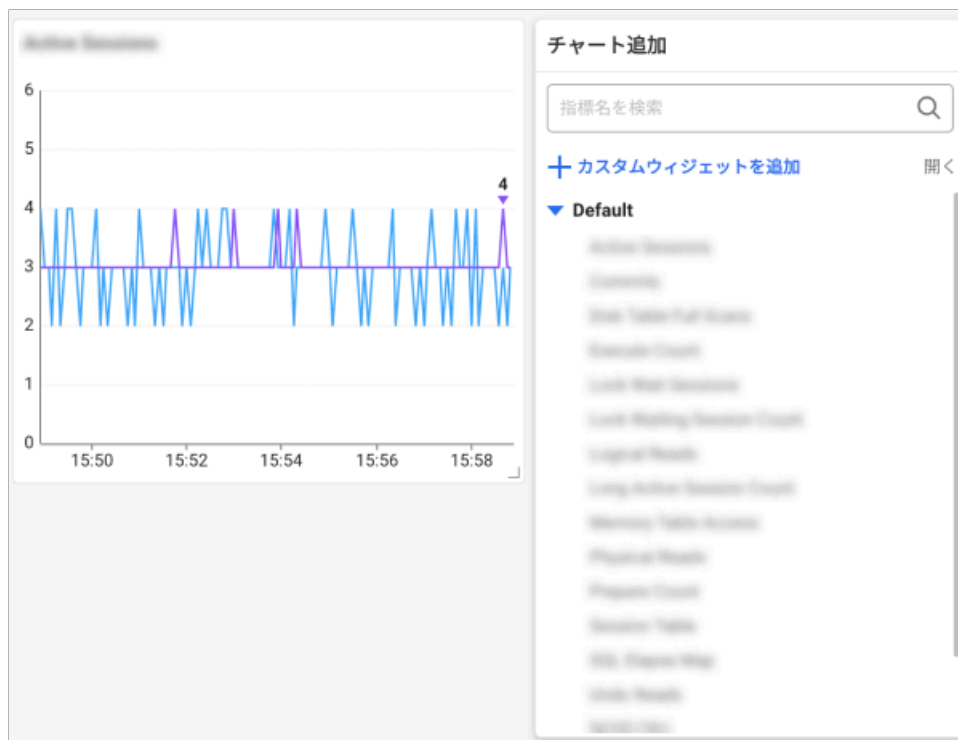
ウィジェットの上部にマウスカーソルを位置すると、カーソルの形が $\oplus$ の形に変更されます。この時、マウスの左ボタンをクリックした状態で希望する位置にドラッグすると、ウィジェットを移動することができます。

ウィジェットを削除する



削除するウィジェットで右クリックします。**削除**ボタンをクリックすると、ウィジェットがダッシュボードから削除されます。

ウィジェットを追加する



ダッシュボードから空白エリアにマウスカーソルを移動し、マウスの右ボタンをクリックします。ポップアップメニューから追加するウィジェットを選択します。希望する場所にウィジェットを配置してサイズを変更します。

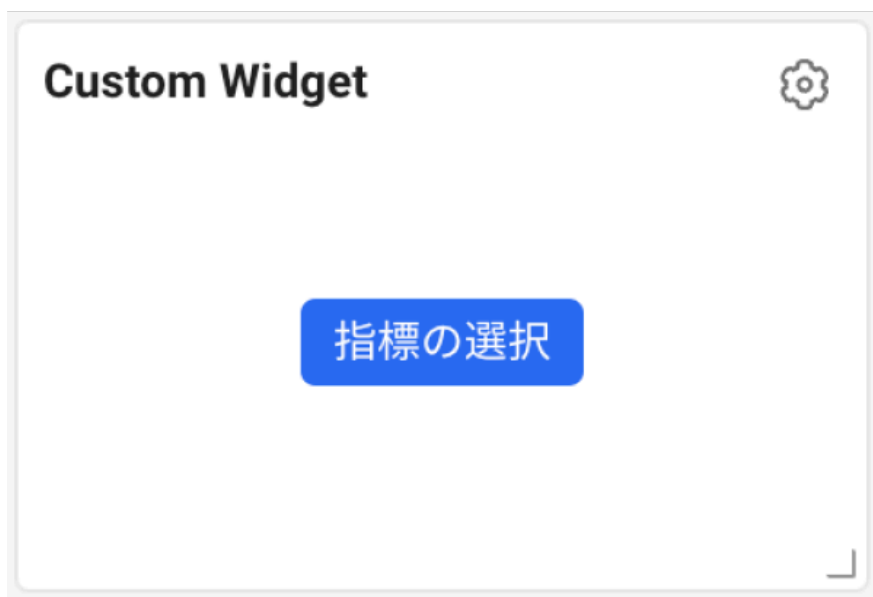
カスタムウィジェット

カスタムウィジェットは、ダッシュボードでデフォルトに提供されるメトリクスの他に、ユーザーがメトリクスを追加できる機能です。デフォルトで提供するメトリクスの他に、ダッシュボードで継続的にモニタリングしたいメトリクスがある場合は、カスタムウィジェット機能を利用できます。

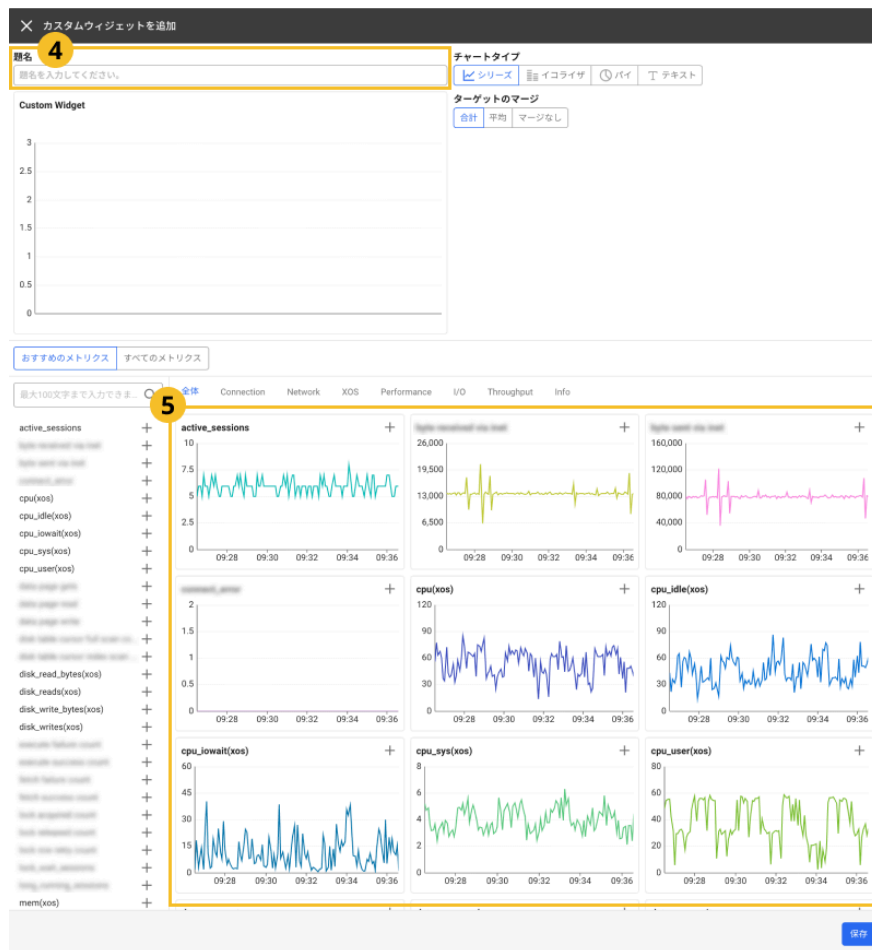
追加する

1. ダッシュボードの空のスペースで、右クリックします。
2. ポップアップメニューで**カスタムウィジェットを追加**を選択します。

3. ダッシュボードに**Custom Widget**が生成されたら、**指標の選択**ボタンを選択します。



4. 画面の右側から **カスタムウィジェット**を追加画面が現れると、**題名項目**にウィジェットの名前を入力します。



5. 画面下のメトリクス一覧から、追加するメトリクスの右上にある＋ボタンを選択します。

6. メトリクスをすべて追加したら**保存**ボタンを選択します。

- ① 最大4つのメトリクスを追加できます。メトリクスを追加する時は、＋ボタンを選択します。
- メトリクスを変更する時は、メトリクス一覧で別のメトリクス項目を選択します。＋ボタンを選択すると、そのメトリクスが追加されます。
- ウィジェットのタイトルを入力しないと、Custom Widgetと保存されます。

チャートタイプを選択する

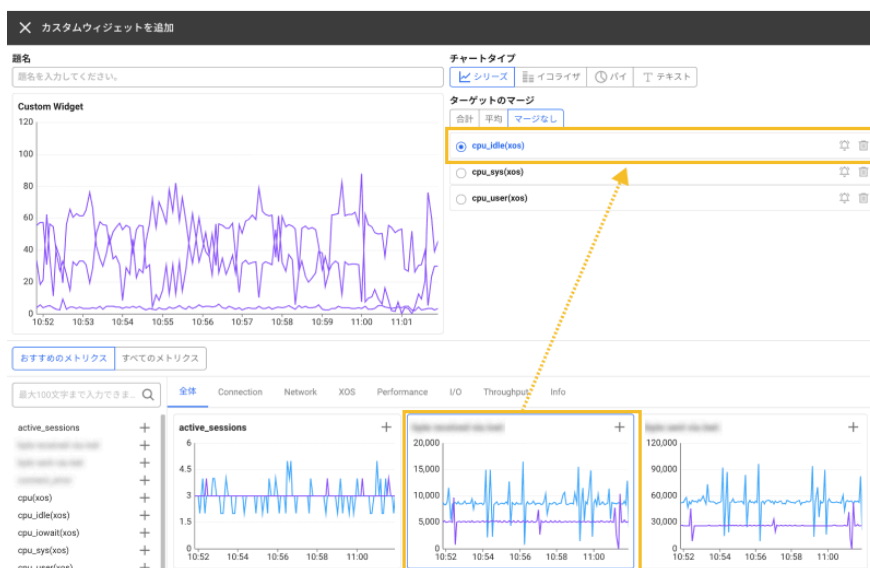
カスタムウィジェットを追加画面のチャートタイプでは、次の形式のチャートを選択できます。

-  シリーズ: 時間の経過によるメトリクスの変化を確認できる時系列形式のチャートです。
-  イコライザ: 複数のメトリクスの性能を比較できる棒グラフ形式のチャートです。様々なメトリクスを1つの画面に視覚的に表現することで、全体的な性能状態を簡単に把握できます。
-  パイ: 複数のメトリクスの全体に対する部門構成比率を確認するのに役立つ円形チャートです。
-  テキスト: メトリクスに対する数値をテキスト形式で表示します。

指標の変更

ユーザー定義ウィジェットに追加したメトリクスを、他のメトリクスに変更または追加できます。

1. ダッシュボードに追加したユーザー定義ウィジェットの右上に  ボタンを選択します。
2. 画面の右側でカスタムウィジェットを追加画面が表示されたら、変更するメトリクスを選択します。



3. 画面下のメトリクスの一覧で変更するメトリクスを選択します。メトリクスを追加する場合、追加するメトリクスの右上に  ボタンを選択します。
4. メトリクスを全て変更したのであれば保存ボタンを選択します。

✓ 追加または変更したメトリクス一覧に表示されたアイコンボタンの機能は、次のとおりです。

-  : 該当メトリクスをカスタムウィジェットから除外できます。
-  : 該当メトリクスに対するアラート通知を設定できます。 ボタンを選択すると、**アラート通知 > イベント設定**メニューに移動します。 **メトリクスイベント**設定の詳細については、[次の文書](#)を参考にしてください。

ウィジェットオプション

ウィジェットに表示されているアイコンボタンの機能は次のとおりです。

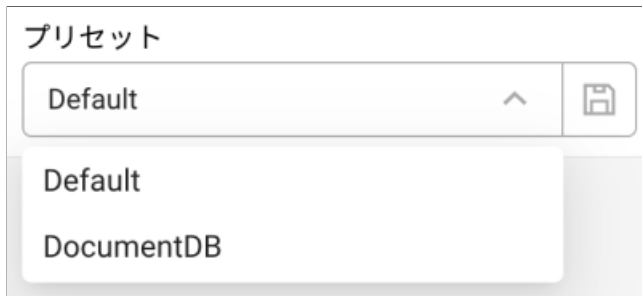
-  : 主要ウィジェットに関する機能と情報が確認できます。(多言語に対応予定)
-  /  : チャートの縦軸範囲を拡大または縮小できます。
-  : 該当ウィジェットのデータを広い画面に開いて表示します。
-  : 該当ウィジェットのデータをエージェントごとに区分して照会できる詳細画面が表示されます。

ⓘ ウィジェットによって使用可能なオプションは異なる場合があります。

プリセット

ユーザーが設定したウィジェットの設定とアクティブセッションテーブルの配置状態をプリセットで保存して読み込むことができます。 **Default**プリセットは、変更できません。

- **Default** : 主要DB指標で構成されています。
- **DocumentDB**: 主なDocumentDB指標(現在の接続数、使用可能な接続、挿入/照会/更新/削除の作業回数、トランザクション状態、オープンカーソル、返却された文書数など)で構成されています。



プリセット保存

プリセット一覧から保存した項目を選択して、設定を呼び出すことができます。

1. ウィジェットの指標を追加または変更します。
2. 画面の右上に  ボタンを選択します。
3. **プリセット保存**で名前を変更した上で**保存**ボタンを選択します。

- ❗
- **Default**プリセットは、変更できません。
 - データベース環境によって、一部のプリセットはサポートされない場合があります。
 - ユーザー定義プリセットは、変更した指標グラフだけでなく、アクティブセッションのカラム順序、カラム幅、フィルター適用内容も一緒に適用されます。
 - **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。

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  アイコンをクリックします。
3. 新しいプリセット名を入力します。
4. **保存**ボタンをクリックします。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。

- ① • 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。📁 アイコンをクリックし、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。

プリセット削除

画面の右上ある**プリセット**を選択すると、プリセット一覧が表示されます。削除するプリセット項目の右側にある **×** ボタンを選択します。

アクティブセッションのセクションを活用

画面の下にある**アクティブセッションセクション**からリアルタイムで実行中のセッション情報を確認できます。ここでは、テーブルの右上にあるボタン機能を説明します。

- ▼：テーブルのカラムヘッダー項目に基づいて一覧をフィルタリングできます。
- 🔄：テーブルのリストを更新できます。
- ☐：テーブル内のカラムヘッダー項目を表示または非表示にすることができます。
- ↓：テーブルの内容をCSVファイルとしてダウンロードできます。
- 🔍：別ウィンドウで開き、より大きな画面でリストを確認できます。

グラフチャートセクションを拡大する

現在見ている画面が小さくてウィジェットを確認しづらい場合は、より広い画面でグラフチャートウィジェットを確認することができます。画面下段に**アクティブセッションセクション**の ▼ ボタンを選択します。**アクティブセッションセクション**は縮小され、**グラフチャートウィジェットセクション**は拡大します。

グラフチャートウィジェットセクションを縮小するには、画面下部に**アクティブセッションセクション**の ▲ ボタンを選択します。

テーブルカラムの設定

テーブルヘッダーカラムを非表示にしたり、希望する項目を追加できます。カラムの順序を変更することもできます。
☐ ボタンをクリックします。

- ① • 設定を完了した後は、**確認**ボタンを選択すると、設定事項がテーブルに反映されます。
- ③ 検索バーにテキストを入力し、カラム項目を検索できます。入力したテキストと一致するカラム項目が表示されます。
- 画像は、製品またはプロジェクト、メニューによって異なる場合があります。

カラムを追加する

① 一覧でテーブルヘッダーカラムに追加する項目を選択します。すべての項目を追加するには、**すべて選択**を選択します。

カラムを削除する

① 一覧から削除するカラム項目のチェックボックスのチェックを解除します。または② 一覧から削除する項目の右側の×ボタンを選択します。

カラムの順序の変更

② 一覧で順序を変更するアイテムをドラッグして、希望する位置に移動できます。

設定事項の初期化

変更事項をすべてキャンセルし、初期化するには、🔄 **初期化**ボタンを選択します。

テーブルデータのフィルタリング

1. テーブルの右上にある▽ボタンを選択します。
2. テーブルのカラムヘッダー項目と条件を選択します。
3. 条件を入力してください。テキストボックスに条件を入力します。
4. 保存ボタンを選択します。

カラム情報ガイド

- [Active session](#) Lock tree Process information

次は、アクティブセッションセクションのテーブルに表示されるカラム情報です。 `currentOp` コマンドで収集されたデータです。

項目	説明
<code>opid</code>	operationの固有識別子(identifier)
<code>type</code>	値が <code>op</code> の場合、 <code>op</code> フィールドで作業タイプを確認可能
<code>host</code>	サーバー名
<code>desc</code>	<code>connectionId</code> を含むクライアント説明
<code>active</code>	作業が始まる場合は <code>true</code> 、idleの場合は <code>false</code>

項目	説明
currentOpTime	operationの開始時間
op	operationタイプ(none、update、insert、query、command、getmore、remove など)
ns	ネームスペース名で Database.Collection で表示
numYields	作業が行われた数
waitingForLock	ロック(lock)を待機している場合は true、ロック(lock)を取得した場合は false
waitingForFlowControl	flowcontrol を待機している場合は true

項目	説明
holder type	holder セッションの type (transaction id、tupleなど)
lock mode	holder_mode (exclusive lock、shared lockなど)
waiter type	waiter セッションの type (transaction id、tupleなど)
lock request	waiter_mode (exclusive lock、shared lockなど)

次の項目は、XOSエージェントをインストールした場合に収集される指標です。

項目	説明	単位
pid	プロセスID	-
cpuusage	プロセスが使用するCPU使用率	%
cputime	プロセスがこれまでに使用した累積CPU時間	秒
elapse	プロセスが実行されてからの経過時間	秒

項目	説明	単位
vsize	Virtual memory size. 全体の仮想メモリ使用量（RAM + Swap + 予約）	KB
rss	Resident Set Size. 現在のプロセスが占有している実際の物理メモリサイズ	KB
pss	Proportional Set Size. 共有メモリを含む実際の物理メモリ使用量	KB
state	プロセスの現在の状態コード（例：R、S、D、T、Z など）	-
ioread	累積読み込みバイト数（read_bytes）	バイト（B）
iowrite	累積書き込みバイト数（write_bytes）	バイト（B）
uid	このプロセスを実行したユーザーID	-
cmd	実行されたコマンドの短縮形式	-
longcmd	実行されたコマンドの完全な形式（フルパスおよび引数を含む）	-

マルチインスタンス

ホーム画面 > プロジェクト選択 > ダッシュボード > マルチインスタンス

インスタンスモニタリングメニューでは、1つのエージェント(インスタンス)だけをモニタリングすると、マルチインスタンスは、複数のエージェント(インスタンス)を同時に監視して管理できる機能を提供します。

各インスタンスで発生する主な性能指標を、一目で比較して分析できます。実行中の各エージェントの数、すべてのアクティブセッションの合計、トランザクション数などのデータを集計して、効果的にモニタリングできます。ユーザーは、グラフチャートを通じて時間によるメトリクス値の変化と各インスタンスの高い性能メトリクスを簡単に確認できます。

また、最も長く続くアクティブセッションに関する情報を確認でき、ユーザーはシステム性能のボトルネック現象を診断し、解決できる根拠資料として活用できます。



✔ **ダッシュボード > インスタンスリストメニュー**で比較しようとするエージェントを選択し**マルチビュー**ボタンを選択すると**マルチインスタンスメニュー**に入ります。

照会時間設定

ダッシュボードではリアルタイムモニタリング機能を基本的に提供しますが、画面上部のタイムセクターを利用して過去の時間のデータを照会できます。タイムセクターで || ボタンを選択して時間を設定します。ユーザーが設定した時間に基づいて、ダッシュボードに配置したウィジェットのデータを更新します。

エージェント確認

エージェント接続状態を確認する



画面の左上のタイムピッカーの右側には、プロジェクトに関連したエージェントの状態を確認できる情報が表示されます。この機能で、モニタリング対象サーバーの動作有無がすぐに確認できます。

- **Total**: プロジェクトに関連付けられているすべてのエージェントの数
- **Active**: 活性化されたエージェントの数
- **Inactive**: 非活性化状態のエージェント数
- : 非活性化されたエージェントを表示または非表示します。

エージェント別モニタリング



基本的に、ダッシュボードにはすべてのエージェントから収集した指標をチャートとして表示しますが、エージェントを選択してデータを表示することもできます。タイムピッカーの下にあるエージェントを1つ以上選択します。選択したエージェントの指標でダッシュボードに配置されたウィジェットのデータを更新します。

- ✓ エージェントを1つ以上選択した状態で再度すべてのエージェントを選択するには、選択を解除するか、**Total**をクリックします。

- ⓘ プロジェクトに接続されたエージェントの数が多い場合は、エージェント名を短く設定することをお勧めします。エージェント名の設定に関する詳細は、[次の文書](#)を参照してください。

分類別エージェントモニタリング



エージェント設定で分類されたグループ単位でエージェントを選択してモニタリングできます。

- **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。
- **クラスタ別エージェント**: クラスターで構成されるデータベースの場合、クラスターごとにエージェントをモニタリングできます。

- ⓘ **クラスタ別エージェント**項目を利用するには、DBXエージェント([whatap.conf](#))の次のオプションを設定する必要があります。詳細については、[次の文書](#)を参照してください。

whatap.conf

```
cluster_name={cluster_name}
```

ウィジェット編集

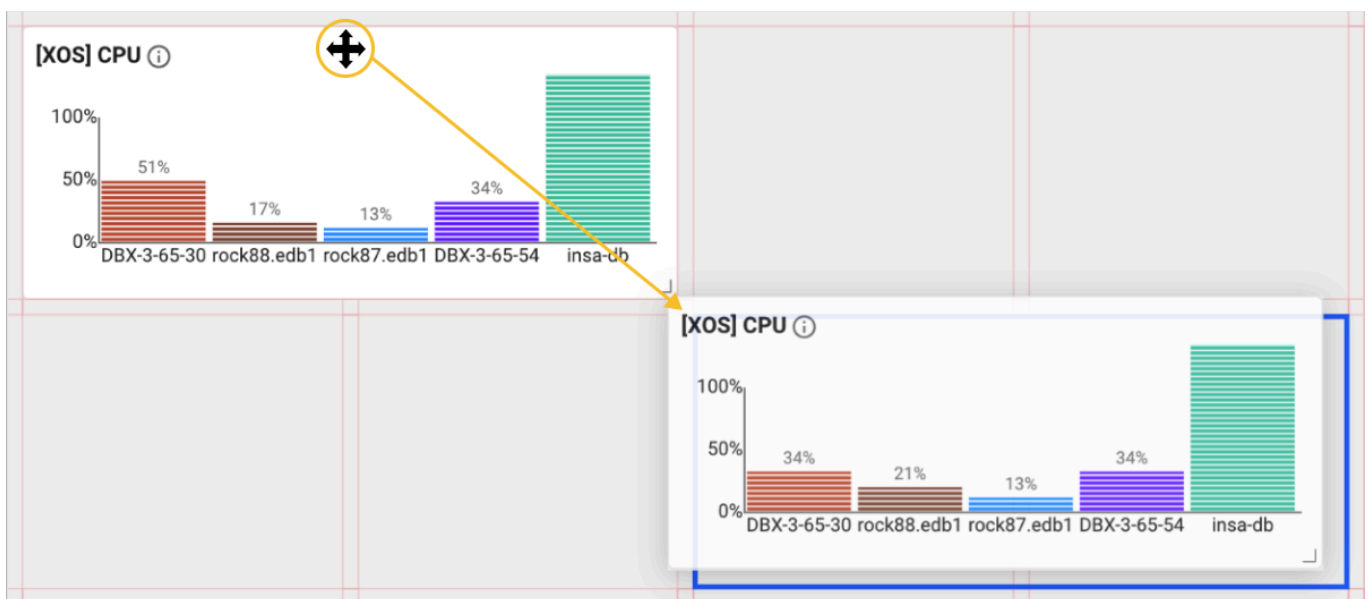
ダッシュボードに配置したウィジェットは、ユーザーが希望するサイズに調整でき、任意の位置に配置できます。ウィジェットは削除したり、再度追加したりすることもできます。

ウィジェットのサイズ変更



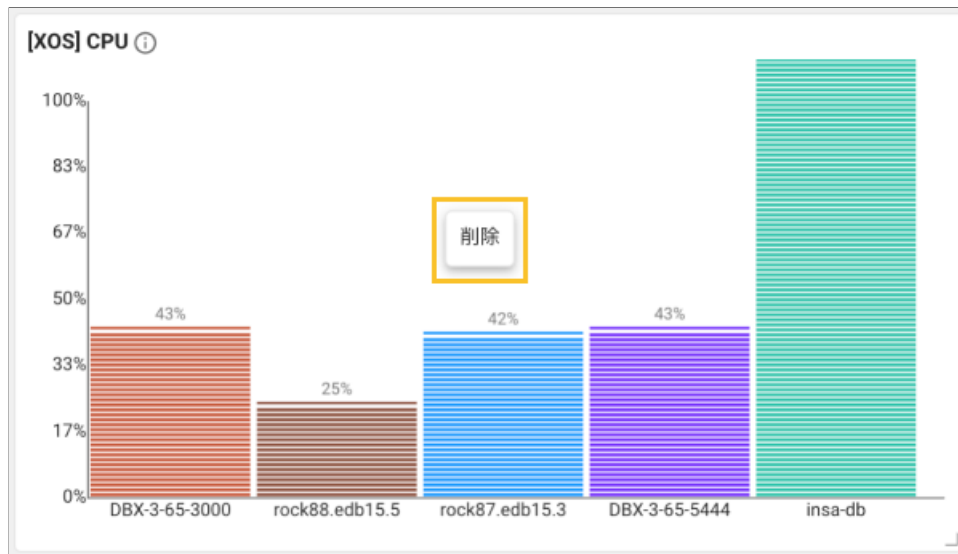
ウィジェットの右下にある「」をマウスでクリックした状態で希望するサイズにドラッグします。幅と高さの比率が均一なグリッドが表示され、グリッド単位でウィジェットのサイズを調整できます。

ウィジェットの移動



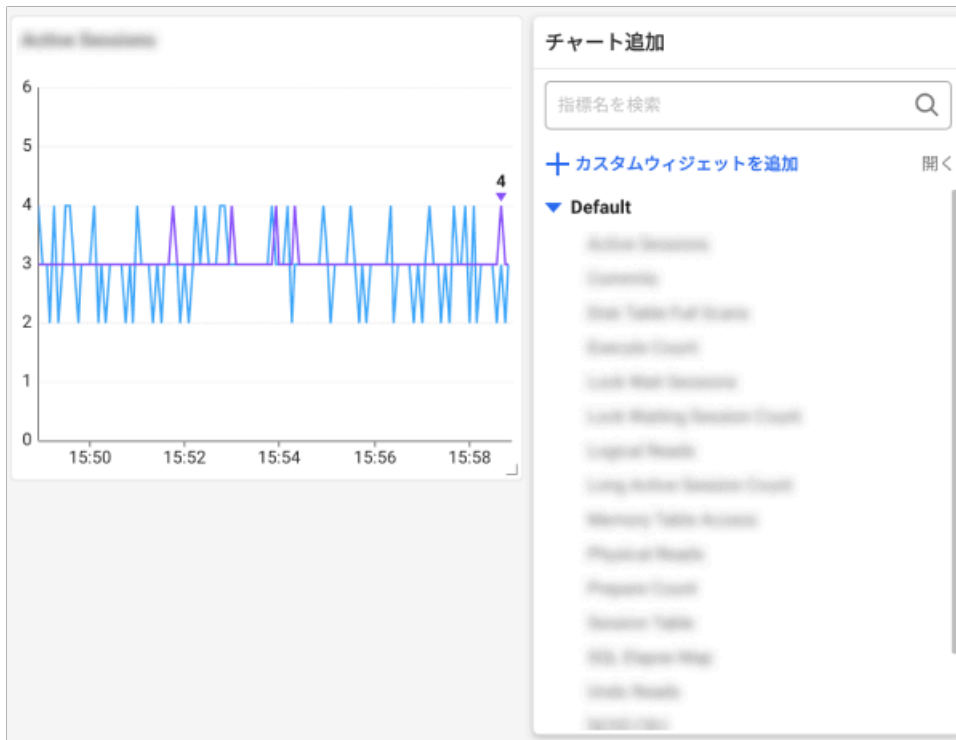
ウィジェットの上部にマウスカーソルを位置すると、カーソルの形が $\oplus$ の形に変更されます。この時、マウスの左ボタンをクリックした状態で希望する位置にドラッグすると、ウィジェットを移動することができます。

ウィジェットを削除する



削除するウィジェットで右クリックします。**削除**ボタンをクリックすると、ウィジェットがダッシュボードから削除されます。

ウィジェットを追加する



ダッシュボードから空白エリアにマウスカーソルを移動し、マウスの右ボタンをクリックします。ポップアップメニューから追加するウィジェットを選択します。希望する場所にウィジェットを配置してサイズを変更します。

- ❗ • ダッシュボードに配置できるウィジェットの詳細については、[次の文書](#)を参考にしてください。
- ダッシュボードで基本的に提供されるメトリクスの他に、ユーザーが希望するメトリクスを追加できます。ユーザー定義ウィジェットの詳細については、[次の文書](#)を参照してください。

カスタムウィジェット

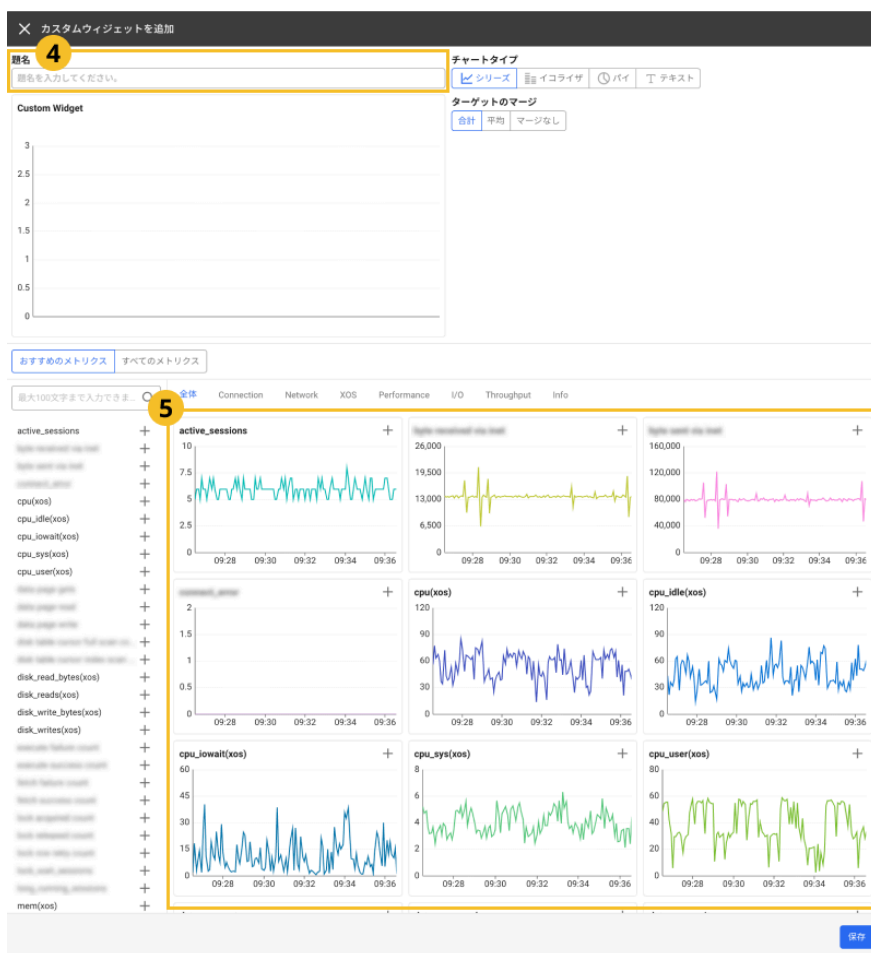
カスタムウィジェットは、ダッシュボードでデフォルトに提供されるメトリクスの他に、ユーザーがメトリクスを追加できる機能です。デフォルトで提供するメトリクスの他に、ダッシュボードで継続的にモニタリングしたいメトリクスがある場合は、カスタムウィジェット機能を利用できます。

追加する

1. ダッシュボードの空のスペースで、右クリックします。
2. ポップアップメニューでカスタムウィジェットを追加を選択します。
3. ダッシュボードにCustom Widgetが生成されたら、指標の選択ボタンを選択します。



4. 画面の右側から カスタムウィジェットを追加画面が現れると、題名項目にウィジェットの名前を入力します。



5. 画面下のメトリクス一覧から、追加するメトリクスの右上にある＋ボタンを選択します。

6. メトリクスをすべて追加したら**保存**ボタンを選択します。

- ① 最大4つのメトリクスを追加できます。メトリクスを追加する時は、＋ボタンを選択します。
- メトリクスを変更する時は、メトリクス一覧で別のメトリクス項目を選択します。＋ボタンを選択すると、そのメトリクスが追加されます。
- ウィジェットのタイトルを入力しないと、Custom Widgetと保存されます。

チャートタイプを選択する

カスタムウィジェットを追加画面のチャートタイプでは、次の形式のチャートを選択できます。

-  **シリーズ**: 時間の経過によるメトリクスの変化を確認できる時系列形式のチャートです。
-  **イコライザ**: 複数のメトリクスの性能を比較できる棒グラフ形式のチャートです。様々なメトリクスを1つの画面に視覚的に表現することで、全体的な性能状態を簡単に把握できます。
-  **パイ**: 複数のメトリクスの全体に対する部門構成比率を確認するのに役立つ円形チャートです。
-  **テキスト**: メトリクスに対する数値をテキスト形式で表示します。

データマージ方式を選択する

カスタムウィジェットを追加画面の対象のマージでは、エージェントから収集されたメトリクスを表示する方法を選択できます。

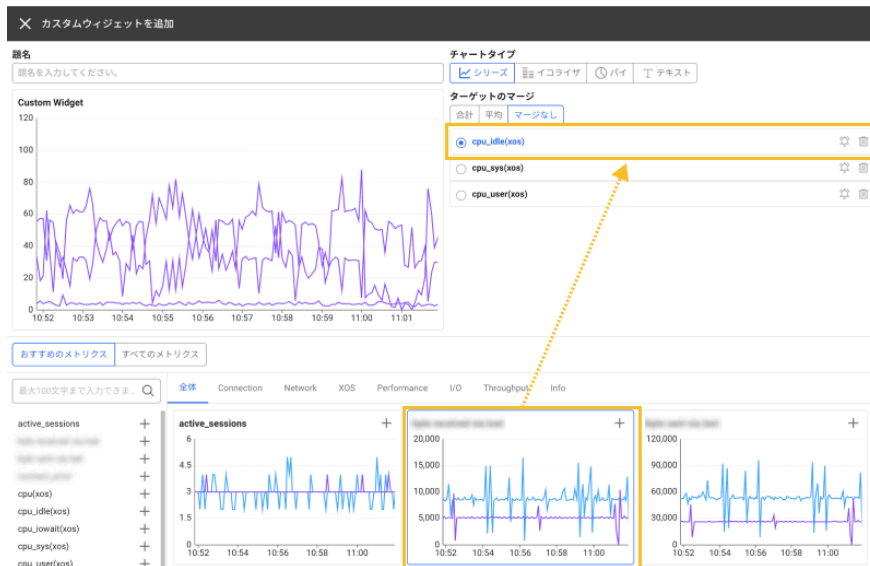
- **合計**: 複数のエージェントから収集されたメトリクス値を合計して、1つの値として表示します。このオプションは、複数のエージェントのデータを統合して全体的な合計を表示する場合に役立ちます。
- **平均**: 複数のエージェントから収集されたメトリクス値を平均して、1つの値として表示します。このオプションは、エージェント全体の平均性能や状態を把握するのに役立ちます。
- **最大値**: 複数のエージェントから収集された指標値の中から最大の値を選択して、一つの値として表示します。このオプションは、エージェントの中で最もパフォーマンスが消耗した状況や最悪の状態を把握するのに役立ちます。
- **マージなし**: 各エージェントのメトリクスを個別に表示します。

 チャートのタイプによって選択できるマージ方式は異なる場合があります。

指標の変更

ユーザー定義ウィジェットに追加したメトリクスを、他のメトリクスに変更または追加できます。

1. ダッシュボードに追加したユーザー定義ウィジェットの右上に  ボタンを選択します。
2. 画面の右側で **カスタムウィジェットを追加画面**が表示されたら、変更するメトリクスを選択します。



3. 画面下のメトリクスの一覧で変更するメトリクスを選択します。メトリクスを追加する場合、追加するメトリクスの右上に+ ボタンを選択します。
4. メトリクスを全て変更したのであれば保存ボタンを選択します。

✓ 追加または変更したメトリクス一覧に表示されたアイコンボタンの機能は、次のとおりです。

- 🗑️ : 該当メトリクスをカスタムウィジェットから除外できます。
- 🔔 : 該当メトリクスに対するアラート通知を設定できます。ボタンを選択すると、**アラート通知 > イベント設定**メニューに移動します。メトリクスイベント設定の詳細については、[次の文書](#)を参考にしてください。

ウィジェットオプション

ウィジェットに表示されているアイコンボタンの機能は次のとおりです。

- ⓘ : 主要ウィジェットに関する機能と情報が確認できます。(多言語に対応予定)
- ⤴ / ⤵ : チャートの縦軸範囲を拡大または縮小できます。
- ⌵ : 該当ウィジェットのデータを広い画面に開いて表示します。
- 🔍 : 該当ウィジェットのデータをエージェントごとに区分して照会できる詳細画面が表示されます。

❗ ウィジェットによって使用可能なオプションは異なる場合があります。

プリセット設定

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。



- **Default** : 主要DB指標で構成されたプリセットです。
- **DocumentDB**: 主なDocumentDB指標(現在の接続数、使用可能な接続、挿入/照会/更新/削除の作業回数、トランザクション状態、オープンカーソル、返却された文書数など)で構成されています。

- ❗
- プリセットに保存できるダッシュボードの設定は次のとおりです。
 - ウィジェットのサイズ、位置
 - ユーザー定義ウィジェットに定義された設定
 - **Session Table**ウィジェットに定義されたテーブルの幅とフィルター、選択したカラム値
 - 基本プリセット(デフォルト)は変更できません。
 - データベース環境によって、一部のプリセットはサポートされない場合があります。
 - **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。



エージェント選択履歴と一緒に保存するには、**エージェント選択履歴を含む**を選択します。

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。

- ① 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したい項目の右側に **×** ボタンをクリックします。

- ① **Default** プリセットは削除できません。

主なウィジェットを調べる

ダッシュボードに配置できるウィジェットの種類は次のとおりです。

XOSウィジェット

- [XOS] CPU

エージェント別のCPU使用率をリアルタイムで確認できます。

- [XOS] Memory

エージェント別のメモリ使用率をリアルタイムで確認できます。

- [XOS] Disk Usage

エージェント別のディスク使用率と使用可能サイズ、全体サイズ情報を表示します。

- : **ディスク使用量の詳細**ポップアップが表示されます。時間帯別のディスク使用量を表示するチャートを確認できます。インスタンスごとに確認でき、**Size**、**Free**、**Used**ボタンを選択すると、全体のサイズ、残りのサイズ、使用中のサイズが確認できます。
- : ウィジェットに表示されたテーブルをより広い画面で確認できます。

✔ データが表示されない場合は、`xos.conf`ファイルに次の設定を追加します。

`xos.conf`

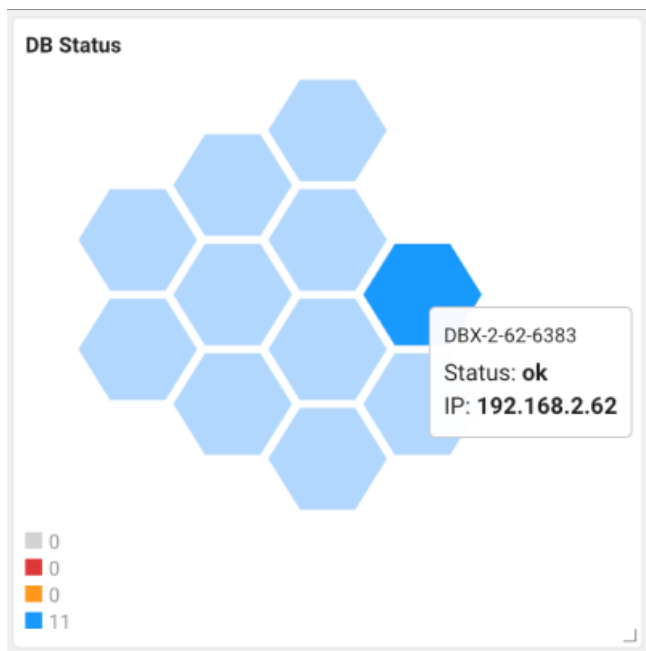
```
# disk usage 0ならばoff、単位: 秒
disk_usage_interval=60
```

Databaseウィジェット

提供するウィジェットを通じて、データベース性能分析の主要メトリクスとして、CPU、メモリ、ディスクI/Oなど多様なシステムリソースの状態を確認できます。

- DB Status

プロジェクトに含まれたエージェント(インスタンス)の状況を確認できます。個別エージェントを六角形に表示し、マウスオーバーすると、今の状況とIPアドレスを確認できます。



エージェントのステータスは、次のように区別されます。

- **正常**：定常状態のエージェントの数です。
- **非活性化されたエージェント**：接続が解除されているエージェントの数です。

• Read requests

1秒あたりの読み取り要請数を測定したウィジェットです。読み取り要請は、データベース内のデータを照会または検索するクエリ、集計タスク、インデックススキャンなどに関するタスクです。データベースの利用パターンの変化を検出するのに役立ちます。

算出方式： `query$opcounters` + `getmore$opcounters`

• Write requests

1秒あたりの書き込み要請数を測定したウィジェットです。書き込み要請は、データベースに新しいデータを追加したり、アップデート、削除に関する作業です。データベースの利用パターンの変化を検出するのに役立ちます。

算出方式： `insert$opcounters` + `update$opcounters` + `delete$opcounters`

• Read Latency (`latency$reads$opLatencies`)

読み取り作業の遅延時間(microsecond)を測定したウィジェットで、クライアントが読み取り作業を要請し、データベースでその作業を実行する際にかかった時間です。読み取り作業の遅延が長い場合は、インデックスを最適化

するか、クエリを改善するなど、性能を向上させる方法を検討してください。

- **Write Latency** (`latency$writes$opLatencies`)

書き込み作業の遅延時間(microsecond)を測定したウィジェットで、クライアントが書き込み作業を要請し、データベースでその作業を実行する際にかかった時間です。書き込み作業の遅延が長い場合は、インデックスを最適化するか、書き込み作業をバッチ処理するなど、性能を向上させる方法を検討してください。

- **Page Faults** (`page_faults$extra_info`)

ページフォールト(page faults)が発生した回数を測定したウィジェットです。ページフォールトは、メモリ管理で発生する問題で、プロセスが要請したメモリページが物理的なメモリにないため、ディスクから該当ページを読み込む必要があるときに発生します。この時、ディスクI/Oが発生して作業が遅延することがあります。通常、システムのメモリ不足の状態を意味します。

データベースの読み書き作業がディスクI/Oに依存しているかを確認し、メモリの不足が性能問題の原因になっているかを把握できます。

① Page faultsの詳細については、[次のリンク](#)を参考にしてください。

- **Active Connections** (`active$connections`)

作業中のクライアントの接続数を測定したウィジェットです。データベースサーバーで同時に処理できるクライアントの接続数をモニタリングできます。高い接続数は、サーバー容量を増設する必要があることを意味します。逆の場合、問題が発生した可能性がありますので、直ちにシステムの状況を把握する必要があります。

- **Read Clients** (`readers$activeClients$globalLock`)

MongoDBのグローバルロック(global lock)で読み取り作業を行っているクライアントの数を測定したウィジェットです。データベースサーバーが読み取り作業のために処理しているクライアントの数を把握できます。データベースの性能をモニタリングし、応答時間を追跡するために役立つ指標です。過度な読み取り作業が発生すると、性能低下の原因になります。

- **Write Clients** (`writers$activeClients$globalLock`)

MongoDBのグローバルロック(global lock)で書き込み作業を行っているクライアントの数を測定するウィジェットです。データベースサーバーが書き込み作業のために処理しているクライアントの数を把握できます。データベースの性能をモニタリングし、応答時間を追跡するために役立つ指標です。過度な書き込み操作が発生すると、性能低下の原因になります。

- **Queued Read Requests** (`readers$currentQueue$globalLock`)

システムで待機中の読み取り作業を処理するために、グローバルロック(global lock)を待っているクライアントの数を測定するウィジェットです。データベースの性能と拡張性を評価できる情報を提供します。待機中の読み取り要請作業が多いほど、クライアントの要請に対する応答時間が長くなる可能性があり、処理量が限界に達する恐れがあります。

待機中の読み込み作業が急に増加する場合、サーバーのリソース増設を検討するか、待機中の読み込み作業の原因を分析し、クエリの最適化およびインデックスのチューニングなどの対策を通じてボトルネックを解決できます。

- **Queued Write Requests** (`writers$currentQueue$globalLock`)

システムで待機中の書き込み作業を処理するために、グローバルロック(global lock)を待っているクライアントの数を測定するウィジェットです。データベースの性能を評価し、最適化するための必須指標です。待機中の書き込み作業が増えると、システムの性能が低下するか、応答時間が長くなる可能性があります。

リソースの増設を検討するか、どのような作業がボトルネックを引き起こすかを把握してみる必要があります。

- **Resident Memory** (`resident$mem`)

システムでプロセスが使用しているメモリのサイズ(MB)です。どれだけのメモリを使用しているかを把握できます。メモリ使用量の追跡により、メモリ使用量を最適化して性能を向上させ、メモリリソースを効率的に活用するために必要な指標です。また、より多くのメモリが必要なのか、シャードを追加するべきかを決定するのに役立ちます。

- **Virtual Memory** (`virtual$mem`)

システムでプロセスが使用している仮想メモリのサイズ(MB)です。実行中の環境でどれだけのメモリリソースを必要としているかを把握できます。仮想メモリのサイズを把握すると、物理メモリの増設または、仮想メモリの使用量を減らすなどの判断に役立ちます。

- **Network Out** (`bytesOut$network`)

クライアントまたはその他のインスタンスの接続を介してサーバーが送信した総バイト数です。データベースサーバーが外部からのリクエストを受けて応答を返すときに送信したデータの総量を意味します。データベースサーバーから発生するネットワークトラフィックを把握できるため、ネットワークの帯域幅やサーバーリソースの使用に対する最適化を行えます。さらに、高いネットワークトラフィックは、応答時間の増加などの性能問題に関連しています。

- **Network In** (`bytesIn$network`)

クライアントまたはその他のインスタンスの接続を介してサーバーが受信した合計バイト数です。データベースサーバーが外部から受信した要請とデータの総量を意味し、クライアントがデータベースサーバーに要請を送り、応答を受ける時に発生するデータ転送量を含みます。特定のアプリケーションまたはタスクとデータベースがどのように通信を使用するかを把握できます。また、ネットワークトラフィックの推移を把握して、システムの容量を計

画し、拡張性を評価できます。

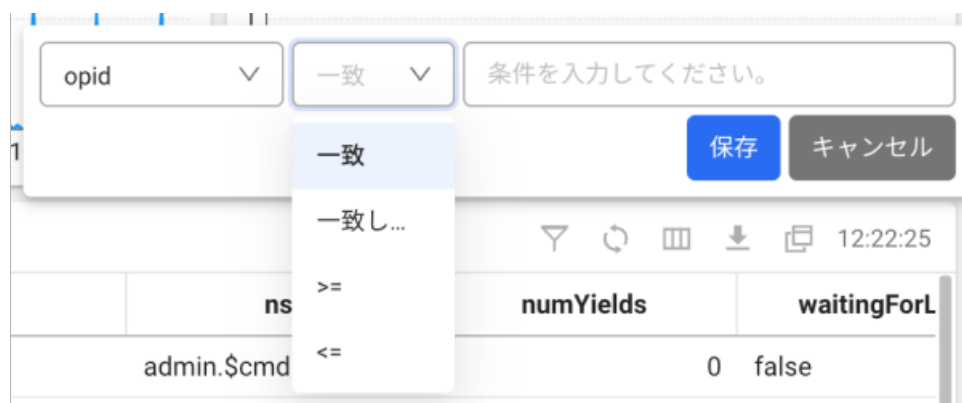
❗ グローバルロック(global lock)は、MongoDBでデータの一貫性を維持するために使用されるメカニズムです。読み取りと書き込みの両方に適用され、タスクを実行しようとするクライアントは、グローバルロックを取得する必要があります。

Session Tableウィジェット

画面下段のSession Tableウィジェットでは、リアルタイムで実行されているアクティブセッションを照会できます。

❗ テーブル一覧の文字の色は黒 → オレンジ → 赤順にセッションの実行速度が遅いことを意味します。

テーブルデータのフィルタリング



1. テーブルの右上にある🔍ボタンを選択します。
2. テーブルのカラムヘッダー項目と条件を選択します。
3. 条件を入力してください。テキストボックスに条件を入力します。
4. 保存ボタンを選択します。

テーブルカラムの設定

テーブルヘッダーカラムを非表示にしたり、希望する項目を追加できます。カラムの順序を変更することもできます。 ボタンをクリックします。

- ❗ • 設定を完了した後は、**確認**ボタンを選択すると、設定事項がテーブルに反映されます。
- ③ 検索バーにテキストを入力し、カラム項目を検索できます。入力したテキストと一致するカラム項目が表示されます。
- 画像は、製品またはプロジェクト、メニューによって異なる場合があります。

カラムを追加する

① 一覧でテーブルヘッダーカラムに追加する項目を選択します。すべての項目を追加するには、**すべて選択**を選択します。

カラムを削除する

① 一覧から削除するカラム項目のチェックボックスのチェックを解除します。または② 一覧から削除する項目の右側の×ボタンを選択します。

カラムの順序の変更

② 一覧で順序を変更するアイテムをドラッグして、希望する位置に移動できます。

設定事項の初期化

変更事項をすべてキャンセルし、初期化するには、 **初期化**ボタンを選択します。

カラム情報ガイド

- Active session Lock tree Process information

次は、**アクティブセッション**セクションのテーブルに表示されるカラム情報です。 `currentOp` コマンドで収集された

データです。

項目	説明
opid	operationの固有識別子(identifier)
type	値が op の場合、 op フィールドで作業タイプを確認可能
host	サーバー名
desc	connectionId を含むクライアント説明
active	作業が始まる場合は true、idleの場合は false
currentOpTime	operationの開始時間
op	operationタイプ(none、update、insert、query、command、getmore、remove など)
ns	ネームスペース名で Database.Collection で表示
numYields	作業が行われた数
waitingForLock	ロック(lock)を待機している場合は true、ロック(lock)を取得した場合は false
waitingForFlowControl	flowcontrol を待機している場合は true

項目	説明
holder type	holder セッションの type (transaction id、tupleなど)
lock mode	holder_mode (exclusive lock、shared lockなど)
waiter type	waiter セッションの type (transaction id、tupleなど)
lock request	waiter_mode (exclusive lock、shared lockなど)

次の項目は、XOSエージェントをインストールした場合に収集される指標です。

項目	説明	単位
pid	プロセスID	-
cpuusage	プロセスが使用するCPU使用率	%
cputime	プロセスがこれまでに使用した累積CPU時間	秒
elapsed	プロセスが実行されてからの経過時間	秒
vsize	Virtual memory size. 全体の仮想メモリ使用量（RAM + Swap + 予約）	KB
rss	Resident Set Size. 現在のプロセスが占有している実際の物理メモリサイズ	KB
pss	Proportional Set Size. 共有メモリを含む実際の物理メモリ使用量	KB
state	プロセスの現在の状態コード（例：R、S、D、T、Z など）	-
ioread	累積読み込みバイト数（read_bytes）	バイト（B）
iowrite	累積書き込みバイト数（write_bytes）	バイト（B）
uid	このプロセスを実行したユーザーID	-
cmd	実行されたコマンドの短縮形式	-
longcmd	実行されたコマンドの完全な形式（フルパスおよび引数を含む）	-

照会リストをダウンロードする

現在照会中の[Session Table](#)リストをCSVファイルでダウンロードできます。[Session Table](#)セクションの右上の  ボタンを選択します。

ダウンロードしたファイル名の形式は次のとおりです。

- アクティブセッション: [activeSession_HH_MM_SS.csv](#)
- ロックツリー: [lockTree_HH_MM_SS.csv](#)

アクティブセッション: `activeSession_HH_MM_SS.csv`

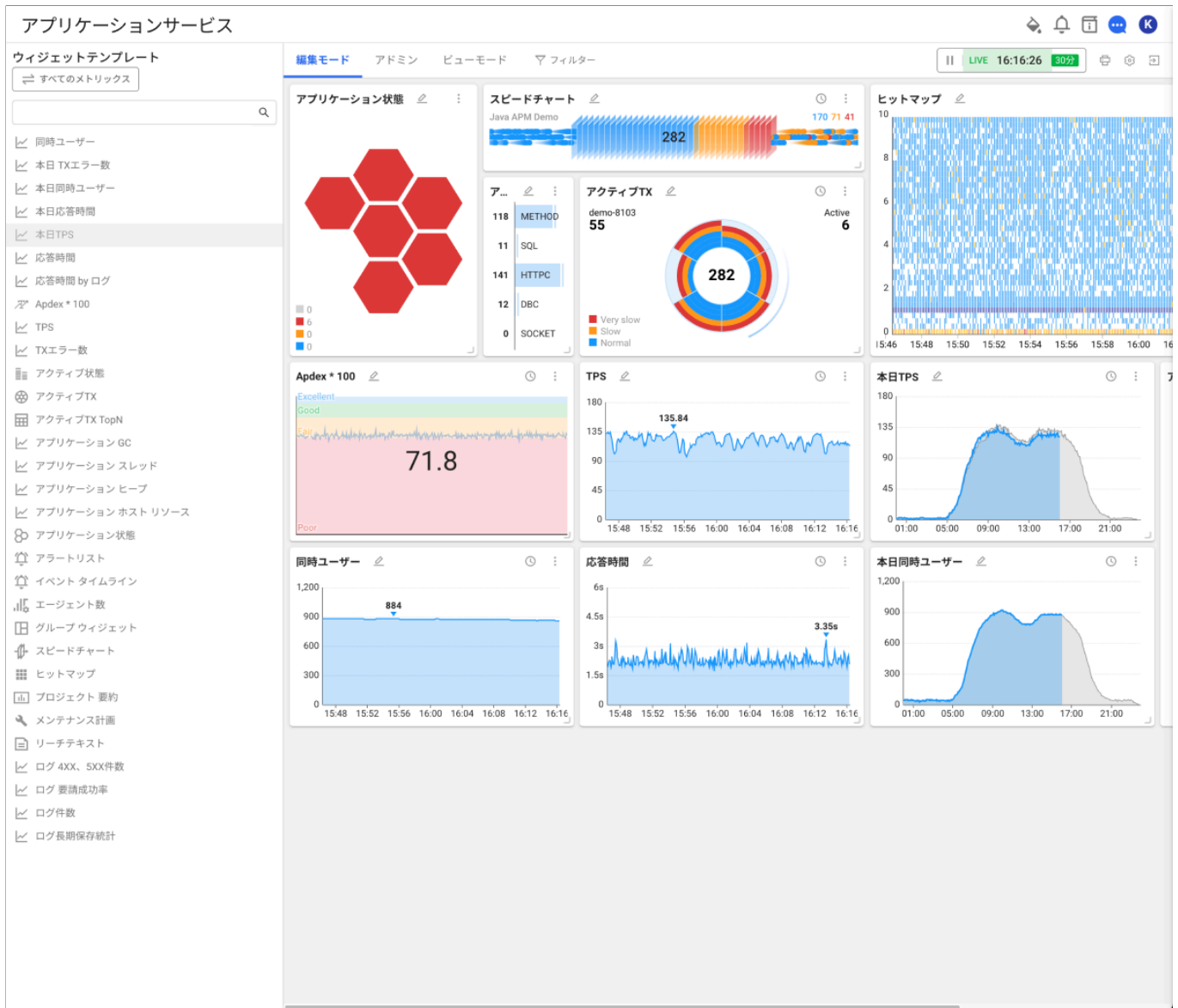
別ウィンドウで見る

`Session Table` リストを別ウィンドウで開き、より広い画面で確認できます。`Session Table` セクションの右上の  ボタンを選択します。

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ボードの使用方法

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

事前テンプレートを適用する

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

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

Flex ボードを作成する

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

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

(グリッドを設定してから **ダッシュボード生成** ボタンをクリック)

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

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

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

5. 配置したウィジェットの位置を移動したりサイズを調整します。

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

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

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

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

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

Flex ボードを編集する

- ❗ **Flex ボード編集権限**



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

メンバー権限の詳細は[次のドキュメント](#)を参照してください。

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



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

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

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

• レイアウト

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

Flex ボードを削除する

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

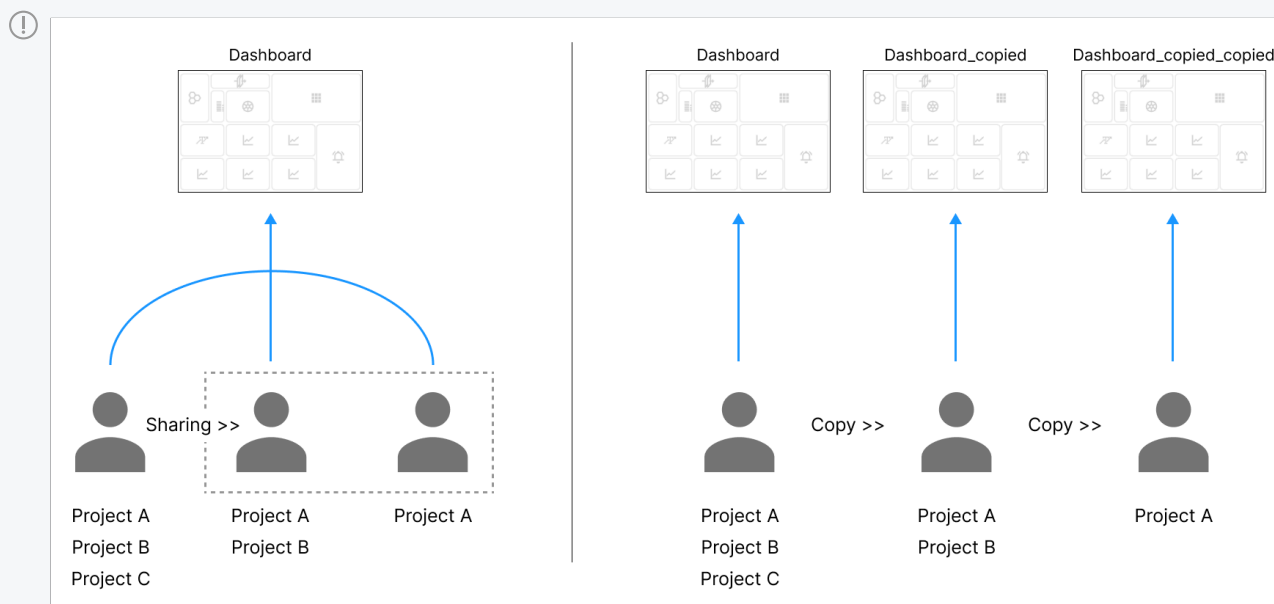
 ダッシュボードの削除は所有者と共有を受けたユーザーで動作が異なります。

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

Flex ボードを共有する

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

 共有とコピーの違い



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



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

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

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

3. 共有 ボタンをクリックします。

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

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

✓ ダッシュボード共有の条件

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

Flex ボードをコピーする

ユーザーは Flex ボードをコピーして他のメンバーに渡せます。

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

JSON ファイルで共有する

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

エクスポート

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

インポート

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

❗ この機能は、プロジェクトの 編集 権限を持つメンバーのみ利用できます。

Flex ボードの画面モード

Flex ボードの画面モードに応じて提供機能が異なります。

❗ アクセス可能なメンバー権限

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

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

モード種類

Flexボード は画面モードにより設定できる機能が異なります。

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

共通機能

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

データフィルタリング

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

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

フィルタリング条件

フィルタリング条件はエージェントタイプとメトリクスタイプに分かれます。

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

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

参照時間を設定する

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

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

印刷する

Flex ボード画面を PDF で保存して印刷できます。

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

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

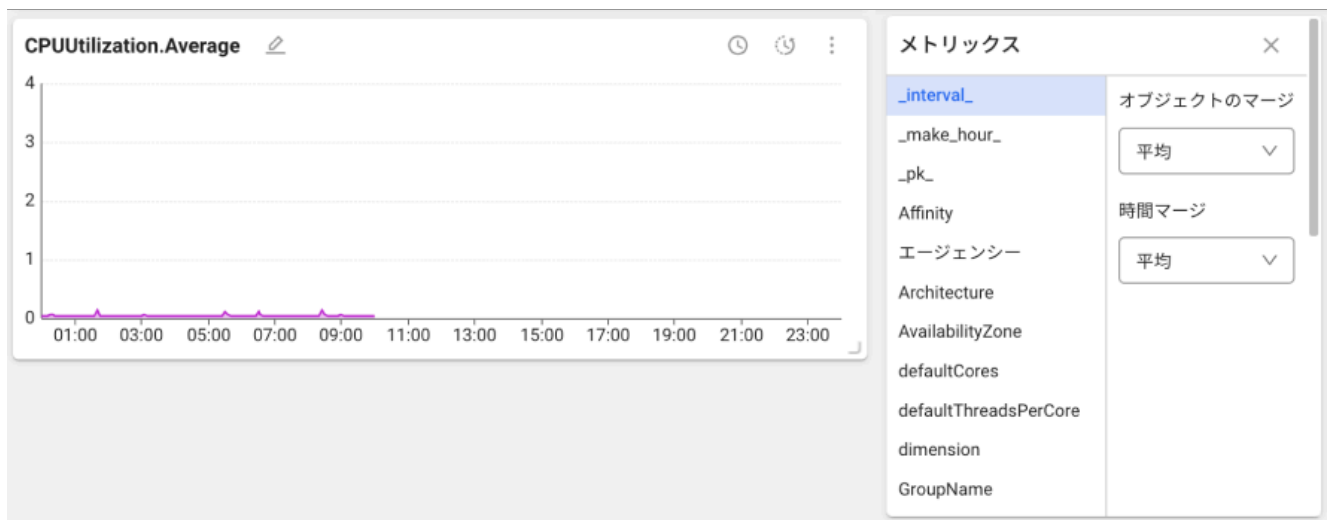
左側で選択したタグ(例：エージェント名)に基づいてチャートデータをグループ化するために使用します。この場合、異なるフィールド(例：CPU)値を持つデータ間でタグが一致する場合、そのデータは結合されます。

• 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。

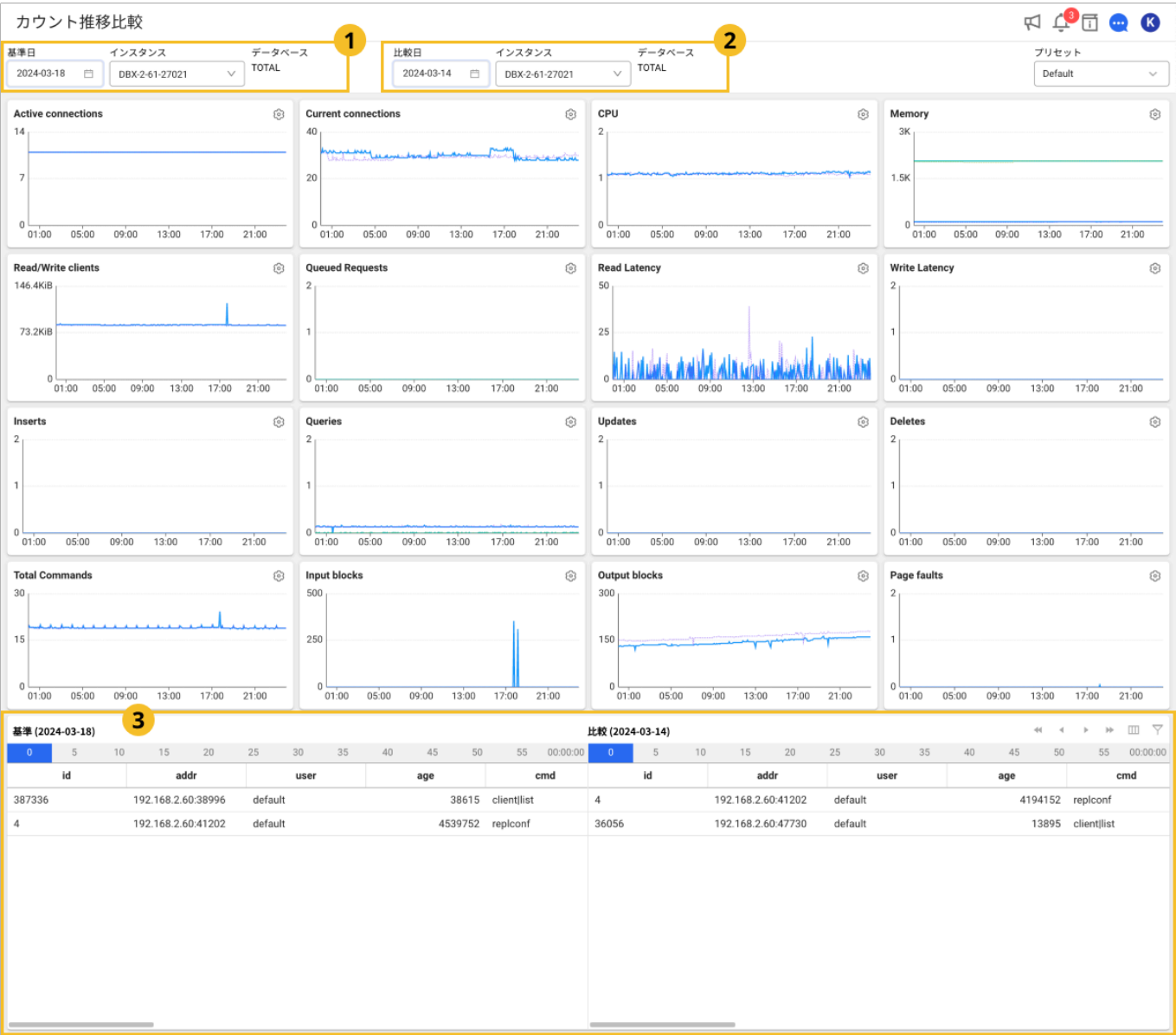
カウント推移の比較

ホーム画面 > プロジェクト選択 > 分析 > カウント推移比較

分析 > 推移比較 で、データベースの主要指標を時間帯ごとに確認し、パフォーマンスの変化を追跡します。

異なる日付の指標を比較することで、運用の傾向を分析できます。アクティブセッション テーブルでは、現在実行中のセッションと長時間実行中のセッションの両方を確認できます。

基本画面ガイド



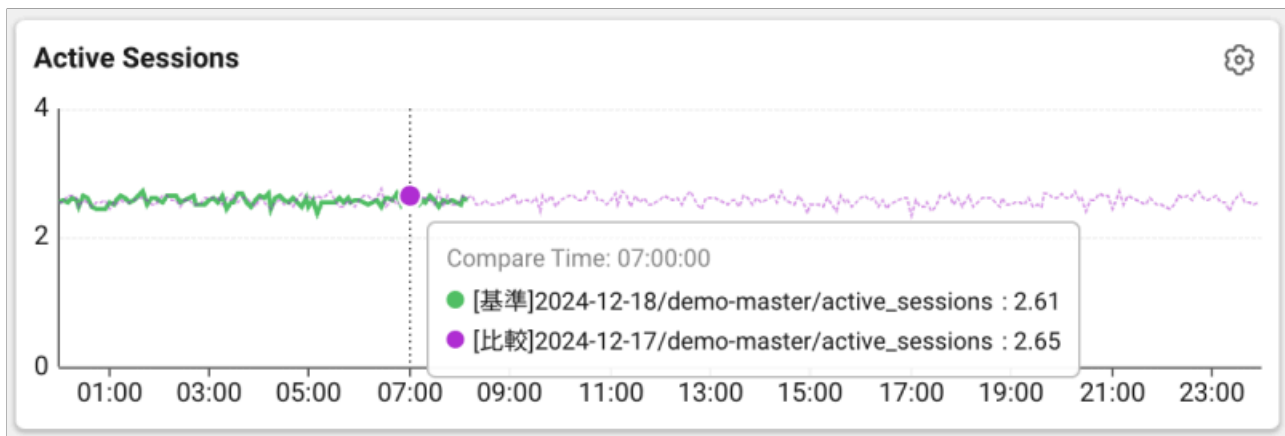
- ① 基準日、② 比較日、インスタンス項目を選択すると、すべてのウィジェットに選択した項目を基準に、データが自動的に反映されます。
- ウィジェットに表示されている指標の意味を知りたい場合は、名前の横の ⓘ ボタンを選択するか、[次の文書](#)を参照してください。

① ⓘ ボタンのツールチップ機能は多言語ではサポートされていません。

- 他のウィジェットの位置を変更する場合は、ウィジェットの上部を選択した状態でドラッグします。ただし、ウィジェットのサイズは変更できません。
- ③ アクティブセッションテーブルの左側には、**基準日**、右側には、**比較日**に該当するデータを表示します。
- ③ アクティブセッションテーブル一覧の文字の色は黒 → オレンジ → 赤の順でセッションの実行速度が遅いことを意味します。

比較対象の選択

① **基準日、インスタンス**を選択し、② **比較日、インスタンス**を選択します。チャートの上にマウスをオーバーすると表示されるツールチップを通じて、その時点の詳細データを確認できます。ツールチップの内容は、マウスの位置に応じて値が更新されます。



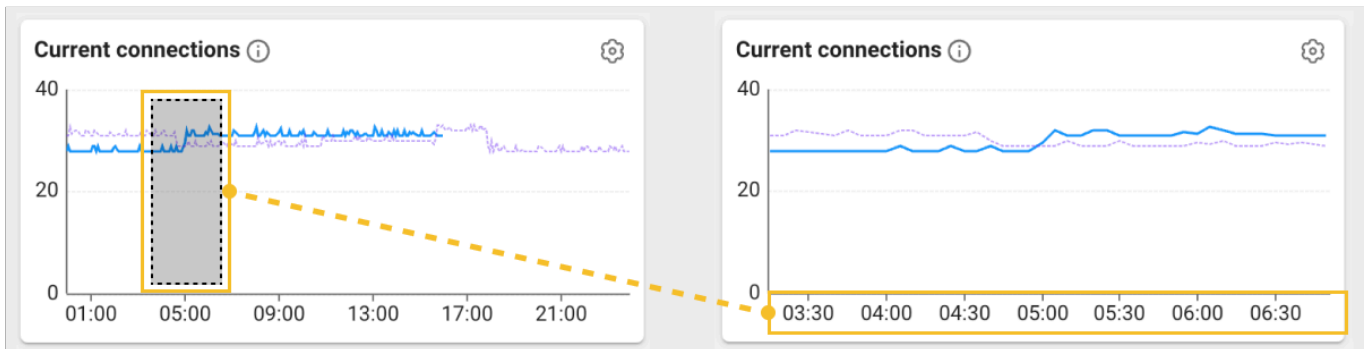
- シリーズごとに固有の色が表示され、視覚的に簡単に区別できます。実線は**基準日**のデータ、点線は**比較日**のデータを意味します。
- **Compare Time**は、現在マウスポインターが存在するデータの時間値を表示します。
- 選択したデータ時点のメトリクス値を表示し、シリーズごとに区別して提供します。各シリーズには、データポイントの日付とエージェント(インスタンス)名、指標名、値が含まれます。

アクティブセッション情報の比較

基準 (2024-03-18)						比較 (2024-03-14)					
0	5	10	15	20	25	0	5	10	15	20	25
id	addr	user	age	cmd		id	addr	user	age	cmd	
387336	192.168.2.60:38996	default	38615	clientlist		4	192.168.2.60:41202	default	4194152	replconf	
4	192.168.2.60:41202	default	4539752	replconf		36056	192.168.2.60:47730	default	13895	clientlist	

- データを表示した時間帯は、**4**で確認できます。
- アクティブセッションデータは5秒単位で収集され、テーブル上の5秒単位で移動できるボタンを選択すると、その時間のデータを表示することができます。
- 右上にある◀または▶を選択すると、1分単位でデータを表示できます。5秒単位で移動するには、◀または▶ボタンを選択します。
- アクティブセッションテーブル一覧の文字の色は黒 → オレンジ → 赤の順にセッションの実行速度が遅いことを意味します。
- グラフチャートの特定の時点をクリックすると、**(3)**その時点を赤い線で表示して収集されたアクティブセッションを確認できます。

特定時間の比較



特定の時間を拡大してデータを比較できます。画面に配置されたウィジェットから目的の時間帯を選択して、チャートをドラッグしてください。すべてのウィジェットとアクティブセッションテーブルに、ドラッグした特定の時間帯の

データを表示します。

プリセット

インスタンスモニタリングメニューから、ユーザーが設定したウィジェットの設定とアクティブセッションテーブルの配置状態をプリセットとして読み込むことができます。

❗ プリセット設定の詳細については、[次の文書](#)を参考にしてください。

カラム情報ガイド

- Active session Lock tree Process information

次は、アクティブセッションセクションのテーブルに表示されるカラム情報です。currentOp コマンドで収集されたデータです。

項目	説明
opid	operationの固有識別子(identifier)
type	値がopの場合、opフィールドで作業タイプを確認可能
host	サーバー名
desc	connectionIdを含むクライアント説明
active	作業が始まる場合はtrue、idleの場合はfalse
currentOpTime	operationの開始時間
op	operationタイプ(none、update、insert、query、command、getmore、removeなど)
ns	ネームスペース名でDatabase.Collectionで表示

項目	説明
numYields	作業が行われた数
waitingForLock	ロック(lock)を待機している場合は true、ロック(lock)を取得した場合は false
waitingForFlowControl	flowcontrol を待機している場合は true

項目	説明
holder type	holder セッションの type (transaction id、tuple など)
lock mode	holder_mode (exclusive lock、shared lock など)
waiter type	waiter セッションの type (transaction id、tuple など)
lock request	waiter_mode (exclusive lock、shared lock など)

次の項目は、XOSエージェントをインストールした場合に収集される指標です。

項目	説明	単位
pid	プロセスID	-
cpuusage	プロセスが使用するCPU使用率	%
cputime	プロセスがこれまでに使用した累積CPU時間	秒
elapsed	プロセスが実行されてからの経過時間	秒
vsize	Virtual memory size. 全体の仮想メモリ使用量 (RAM + Swap + 予約)	KB
rss	Resident Set Size. 現在のプロセスが占有している実際の物理メモリサイズ	KB
pss	Proportional Set Size. 共有メモリを含む実際の物理メモリ使用量	KB
state	プロセスの現在の状態コード (例: R、S、D、T、Z など)	-

項目	説明	単位
ioread	累積読み込みバイト数（read_bytes）	バイト（B）
iowrite	累積書き込みバイト数（write_bytes）	バイト（B）
uid	このプロセスを実行したユーザーID	-
cmd	実行されたコマンドの短縮形式	-
longcmd	実行されたコマンドの完全な形式（フルパスおよび引数を含む）	-

データベースパラメータ

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		
2024/06/14	2024/06/13	DBX-2-61-27024		
			変更を表示	
Key	2024/06/14 12:28:33 本日	2024/06/13 00:00:00		
	Value	Value		
oldestRequiredTimestampForCrashRecovery\$storageEngine	Timestamp(value=7380015139048652801, seconds=1718293675, inc=1)	Timestamp(value=7379644101118918658, seconds=1718207286, inc=2)		
supportsCommittedReads\$storageEngine	true	true		
name\$storageEngine	wiredTiger	wiredTiger		
clientSupported\$tcpFastOpen\$network	false	false		
serverSupported\$tcpFastOpen\$network	true	true		
lastTransactionReaperJobTimestamp\$logicalSessionRecordCache	Fri Jun 14 00:44:45 KST 2024	Thu Jun 13 00:44:45 KST 2024		
lastSessionsCollectionJobTimestamp\$logicalSessionRecordCache	Fri Jun 14 00:44:45 KST 2024	Thu Jun 13 00:44:45 KST 2024		
state\$freeMonitoring	undecided	undecided		
isLagged\$flowControl	false	false		
targetRateLimit\$flowControl	1000000000	1000000000		
enabled\$flowControl	true	true		
localTime	Fri Jun 14 00:48:55 KST 2024	Thu Jun 13 00:48:54 KST 2024		
uptimeEstimate	4444751	4358350		
uptimeMillis	4444751231	4358350324		

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

2024/06/14

比較日

2024/06/13

インスタンス

DBX-2-61-27024

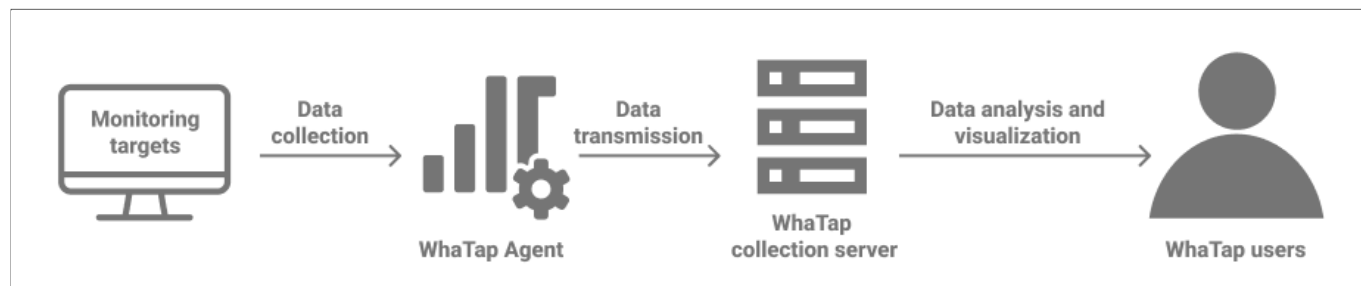
変更を表示

Key	2024/06/14 12:28:33 本日	2024/06/13 00:00:00
	Value	Value
oldestRequiredTimestampForCrashRecovery\$storageEngine	Timestamp(value=7380015139048652801, seconds=1718293675, inc=1)	Timestamp(value=7379644101118918658, seconds=1718207286, inc=2)
lastTransactionReaperJobTimestamp\$logicalSessionRecordCache	Fri Jun 14 00:44:45 KST 2024	Thu Jun 13 00:44:45 KST 2024
lastSessionsCollectionJobTimestamp\$logicalSessionRecordCache	Fri Jun 14 00:44:45 KST 2024	Thu Jun 13 00:44:45 KST 2024
localTime	Fri Jun 14 00:48:55 KST 2024	Thu Jun 13 00:48:54 KST 2024
uptimeEstimate	4444751	4358350
uptimeMillis	4444751231	4358350324
uptime	4444752.0	4358351.0
operationTime	Timestamp(value=7380015396746690561, seconds=1718293735, inc=1)	Timestamp(value=7379644281507545089, seconds=1718207328, inc=1)
clusterTime\$\$clusterTime	Timestamp(value=7380015396746690561, seconds=1718293735, inc=1)	Timestamp(value=7379644281507545089, seconds=1718207328, inc=1)
ts\$opTime\$\$configServerState	Timestamp(value=7380015370976886785, seconds=1718293729, inc=1)	Timestamp(value=7379644272917610499, seconds=1718207326, inc=3)
lastCommittedOpTime	Timestamp(value=7380015353797017601, seconds=1718293725, inc=1)	Timestamp(value=7379644281507545089, seconds=1718207328, inc=1)

メトリクス

メトリクスとは？

WhaTapは、モニタリング対象からデータを収集し、ユーザーに提供します。エージェントから収集されるデータをメトリクスと呼びます。



メトリクスは、次の情報で構成されています。

- **Category**：関連する指標をバインドする単位
- **Tags**：収集対象を特定できる個別情報を含むデータ
- **Fields**：エージェントから収集された指標
- **Time**：メトリクスが収集された時間
- **Oid**：メトリクスを収集したエージェントの固有番号

収集したデータを表示するには、ホーム画面でプロジェクトを選択し、[サイトマップ](#) > [メトリクス表示](#)を選択します。

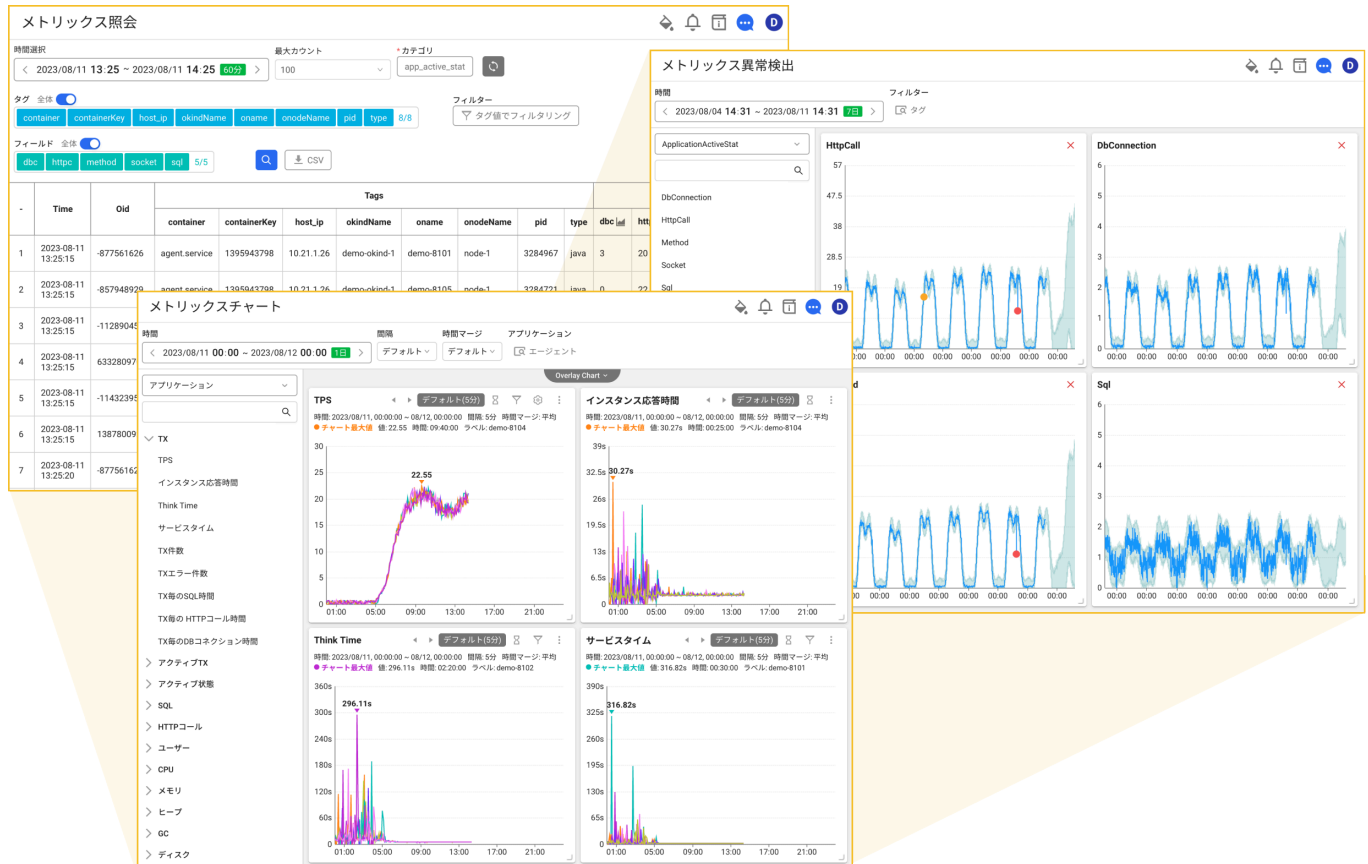
例えば、`db_mongodb_counter` という名前のカテゴリを選択し、関連する指標を検索すると、次のようにカテゴリに対応するタグ(**Tags**)とフィールド(**Fields**)項目を表示できます。

.

メトリクスデータの検索と可視化

WhaTapは収集したメトリクスをさまざまな方式で照会できるメニューを提供します。メトリクスの原本データを照会

できるメトリクス照会、可視化したチャートでメトリクスデータを照会できるメトリクスチャート、AIが学習したメトリクスのパターンと比較して予想パターンを外れた異常を探知できるメトリクス異常検出メニューを確認してください。



MONGODBメトリクス

データベースメトリクスは、データベースの作業量とリソース使用量を包括的に収集したデータです。WhaTapモニタリングサービスは、継続的にメトリクスを収集してデータベースのボトルネックを特定し、性能問題の根本原因を特定するのに役立つデータを提供します。

MongoDBでは `db.serverStatus` から主要指標を収集し、以下は収集する主要指標についての説明です。その他の指標の詳細については、[次の文書](#)を参照してください。

agent_status_summary

エージェントの状態に関するメトリクスを10秒間隔で収集したカテゴリです。

Fields

Field	Type	Unit	Description
inActTime	-	ミリ秒(ms)	エージェントが無効になったままの時間
isActive	Boolean	-	現在のエージェントの活性化状態
isRestart	Boolean	-	エージェントが最近再起動したかどうか (<code>true</code> / <code>false</code>)
lastActTime	-	ミリ秒(ms)	最後にエージェントが活性化された状態の時刻 (<code>0</code> : 非活性化された場合)
oid	-	-	プロジェクトに含まれる各エージェントの固有の識別子
startTime	-	ミリ秒(ms)	エージェントが開始された時点でのタイムスタンプ

db_mongodb_counter

Tags

次は db_mongodb_counter カテゴリに収集されるタグ値の案内です。

Tag	説明	備考
oname	エージェント名です。	一意の値

Field

次は db_mongodb_counter カテゴリに収集されるフィールド値の案内です。

Metrics	Description
accepted\$tcpFastOpen\$network	TCP Fast Openを通じて受け入れられたネットワーク接続の数です。
active\$connections	現在作業が進行中のアクティブクライアント接続の数です。
available\$connections	使用できるネットワーク接続の数です。
awaitingTopologyChanges\$connections	トポロジー変更を待っている接続の数です。
bytesIn\$compressor\$snappy\$compression\$network	Snappy圧縮によって受信されたネットワークバイトの数です。
bytesIn\$compressor\$zlib\$compression\$network	zlib圧縮によって受信されたネットワークバイトの数です。
bytesIn\$compressor\$zstd\$compression\$network	zstd圧縮によって受信されたネットワークバイトの数です。
bytesIn\$decompressor\$snappy\$compression\$network	Snappy圧縮解除によって受信されたネットワークバイトの数です。

Metrics	Description
n\$network	す。
bytesIn\$decompressor\$zlib\$compression\$network	zlib圧縮解除によって受信されたネットワークバイトの数です。
bytesIn\$decompressor\$zstd\$compression\$network	zstd圧縮解除によって受信されたネットワークバイトの数です。
bytesIn\$network	MongoDBクライアントまたはその他のインスタンスの接続を通じてサーバーが受信したネットワークバイトの合計数です。
bytesOut\$compressor\$snappy\$compression\$network	Snappy圧縮によって送信されたネットワークバイトの数です。
bytesOut\$compressor\$zlib\$compression\$network	zlib圧縮によって送信されたネットワークバイトの数です。
bytesOut\$compressor\$zstd\$compression\$network	zstd圧縮によって送信されたネットワークバイトの数です。
bytesOut\$decompressor\$snappy\$compression\$network	Snappy圧縮解除によって送信されたネットワークバイトの数です。
bytesOut\$decompressor\$zlib\$compression\$network	zlib圧縮解除によって送信されたネットワークバイトの数です。
bytesOut\$decompressor\$zstd\$compression\$network	zstd圧縮解除によって送信されたネットワークバイトの数です。
bytesOut\$network	MongoDBクライアントまたはその他のインスタンスの接続を通じてサーバーが送信したネットワークバイトの合計数です。
clientsInTotal\$fixed\$serviceExecutors\$network	固定サービスExecutorで処理されたクライアントの合計数です。
clientsInTotal\$passthrough\$serviceExecutors\$network	パススルーサービスExecutorで処理されたクライアントの合計数です。

Metrics	Description
<code>clientsRunning\$fixed\$serviceExecutors\$network</code>	固定サービスExecutorで実行中のクライアントの数です。
<code>clientsRunning\$passthrough\$serviceExecutors\$network</code>	パススルーサービスExecutorで実行中のクライアントの数です。
<code>clientsWaitingForData\$fixed\$serviceExecutors\$network</code>	固定サービスExecutorでデータ待機中のクライアント数です。
<code>clientsWaitingForData\$passthrough\$serviceExecutors\$network</code>	パススルーサービスExecutorでデータ待機中のクライアント数です。
<code>command\$opcounters</code>	データベースで実行されたコマンドの合計数です。
<code>connect_error</code>	接続エラーの数です。
<code>cpu</code>	<code>extra_info</code> メトリクスの <code>user_time_us</code> および <code>system_time_us</code> 値で計算したCPU使用率です。
<code>cpu_cores</code>	使用可能なCPUコアの数です。
<code>cpu_sys</code>	システムで使用されたCPU時間です。
<code>cpu_user</code>	ユーザー作業に使用されたCPU時間です。
<code>current\$connections</code>	現在サーバーに接続されているクライアントの合計数です。
<code>delete\$opcounters</code>	処理された削除コマンドの数です。
<code>exhaustHello\$connections</code>	<code>exhaustHello</code> メッセージに関連する接続数です。
<code>exhaustIsMaster\$connections</code>	<code>exhaustIsMaster</code> メッセージに関連する接続数です。
<code>fatal count</code>	クリティカルなエラー発生の回数です。
<code>getmore\$opcounters</code>	処理された <code>getMore</code> 作業数です。

Metrics	Description
input_blocks\$extra_info	システムの入力ブロック値です。
insert\$opcounters	処理されたInsertコマンド数です。
involuntary_context_switches\$extra_info	強制コンテキストスイッチの発生回数に関する追加情報です。
kernelSetting\$tcpFastOpen\$network	TCP Fast Openに対するカーネル設定のステータスです。
latency\$commands\$opLatencies	データベースコマンドの待ち時間です。
latency\$reads\$opLatencies	読み取り作業に費やされた遅延時間です。
latency\$transactions\$opLatencies	トランザクション処理に費やされた遅延時間です。
latency\$writes\$opLatencies	書き込み作業に費やされた遅延時間です。
maximum_resident_set_kb\$extra_info	最大居住セットサイズ(KB)に関連する追加情報です。
msg\$asserts	発生したメッセージ表明(assert)の数です。
node_state	ノードの現在状態です。
numRequests\$network	サーバーが受信したネットワークの合計リクエスト数です。
numSlowDNSOperations\$network	遅いDNS作業の数です。
numSlowSSLOperations\$network	遅いSSL作業の数です。
ops\$commands\$opLatencies	コマンド作業の処理回数です。
ops\$reads\$opLatencies	読み取り作業の処理回数です。
ops\$transactions\$opLatencies	トランザクション作業の処理回数です。
ops\$writes\$opLatencies	書き込み作業の処理回数です。

Metrics	Description
output_blocks\$extra_info	システムの実出力ブロック値です。
page_faults\$extra_info	ページのフォールトに関する追加情報です。
page_reclaims\$extra_info	ページの再取得に関する追加情報です。
physicalBytesIn\$network	受信した物理バイト数です。
physicalBytesOut\$network	送信された物理バイトの数です。
query\$opcounters	処理されたクエリコマンドの数です。
readers\$activeClients\$globalLock	活性化された読み取りクライアントの数(global lock)です。
readers\$currentQueue\$globalLock	現在待機中の読み取りクライアントの数(global lock)です。
regular\$asserts	発生した一般表明(assert)の数です。
replication_delay_max	複製の最大遅延時間です。
resident\$mem	使用中の実際メモリサイズです。
rollovers\$asserts	発生したロールオーバー表明(assert)の数です。
system_time_us\$extra_info	システム時間(マイクロ秒)に関連する追加情報です。
threaded\$connections	スレッドベースの接続数です。
threadsRunning\$fixed\$serviceExecutors\$network	固定サービスExecutorで実行中のスレッドの数です。
threadsRunning\$passthrough\$serviceExecutors\$network	パススルーサービスExecutorで実行中のスレッドの数です。
total\$activeClients\$globalLock	活性化されたクライアントの合計数(global lock)です。

Metrics	Description
<code>total\$currentQueue\$globalLock</code>	待機中のクライアントの合計数(global lock)です。
<code>totalCreated\$connections</code>	生成された接続の合計数です。
<code>totalTime\$globalLock</code>	グローバルロック(global lock)でかかった合計時間です。
<code>tripwire\$asserts</code>	発生したトリップワイヤ表明(assert)の数です。
<code>update\$opcounters</code>	処理されたアップデートコマンドの数です。
<code>user\$asserts</code>	発生したユーザー表明(assert)の数です。
<code>user_time_us\$extra_info</code>	ユーザー時間(マイクロ秒)に関連する追加情報です。
<code>virtual\$mem</code>	使用中の仮想メモリサイズです。
<code>voluntary_context_switches\$extra_info</code>	自発的なコンテキストスイッチの発生回数に関する追加情報です。
<code>warning count</code>	警告メッセージの数です。
<code>warning\$asserts</code>	発生した警告表明(assert)の数です。
<code>writers\$activeClients\$globalLock</code>	活性化された書き込みクライアントの数(global lock)です。
<code>writers\$currentQueue\$globalLock</code>	待機中の書き込みクライアントの数(global lock)です。

ⓘ WhaTapは、クライアントに関する情報をデフォルトで保存します。

XOS関連メトリクス

XOSエージェントから収集されるメトリクスについての説明です。

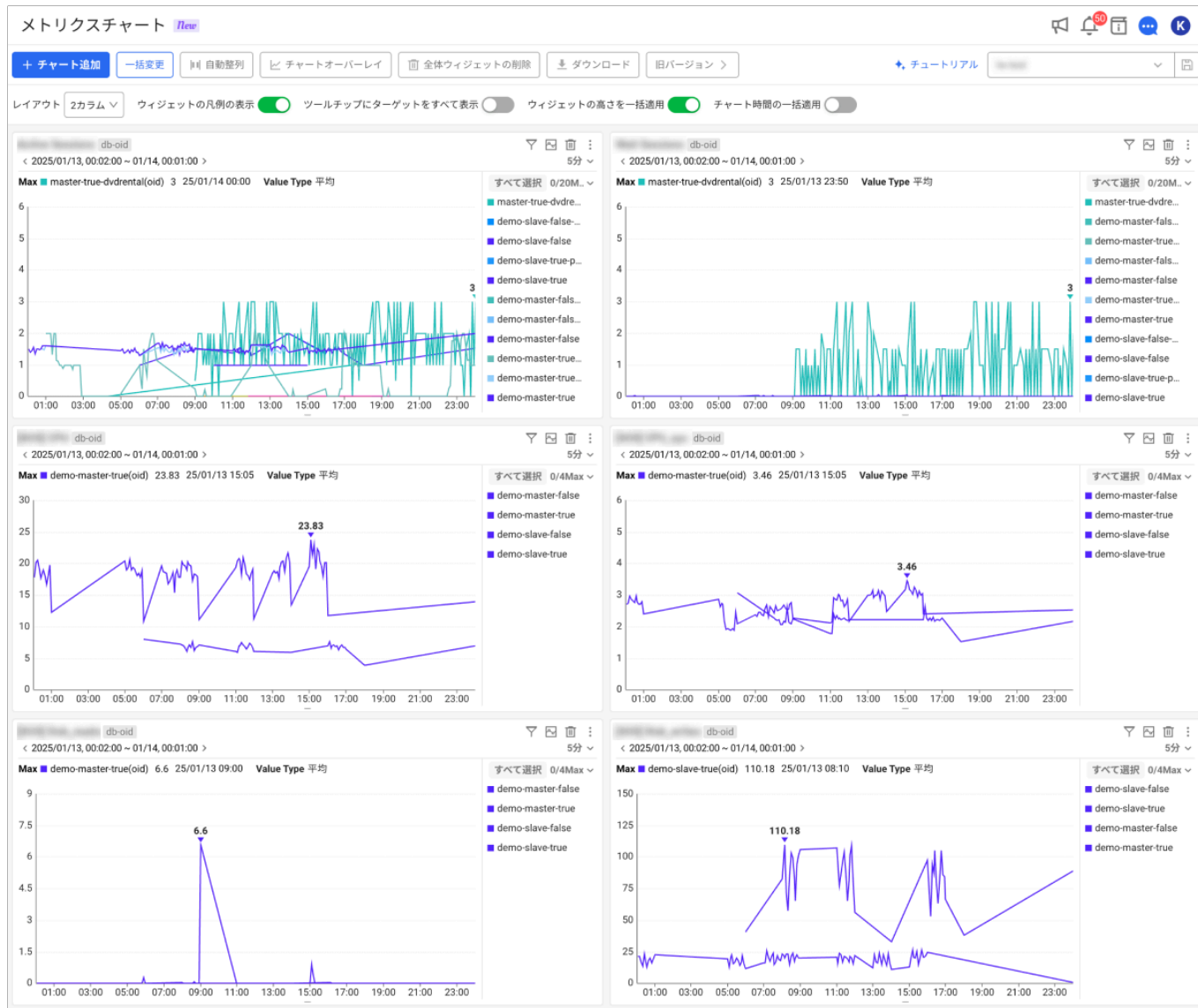
Metric	Unit	Description
<code>cpu(xos)</code>	pct	CPU使用率 <code>cpu_user</code> + <code>cpu_sys</code> + <code>cpu_iowait</code> の合計
<code>cpu_idle(xos)</code>	pct	CPUが遊休状態の時間
<code>cpu_iowait(xos)</code>	pct	CPUがI/O作業を待機した時間
<code>cpu_sys(xos)</code>	pct	CPUがカーネルコードの実行に使用された時間
<code>cpu_user(xos)</code>	pct	CPUがユーザーコードの実行に使用された時間
<code>disk_read_bytes(xos)</code>	バイト	ディスクから読み取ったデータ量
<code>disk_reads(xos)</code>	block	ディスクで読み取られたブロック数
<code>disk_write_bytes(xos)</code>	バイト	ディスクに記録されたデータ量
<code>disk_writes(xos)</code>	block	ディスクに記録されたブロック数
<code>mem(xos)</code>	pct	メモリ使用率
<code>mem_available(xos)</code>	MB	使用可能なメモリサイズ
<code>mem_buffcache(xos)</code>	MB	buff/cache用途に使用中のメモリサイズ
<code>mem_free(xos)</code>	MB	使用していないメモリサイズ
<code>mem_swapfree(xos)</code>	MB	未使用のスワップ領域サイズ スワップはディスク領域を使用するため、使用時に性能が低下する可能性がある
<code>mem_swaptotal(xos)</code>	MB	全体スワップ(Swap)サイズ 物理メモリ不足時に使用

Metric	Unit	Description
<code>mem_total(xos)</code>	MB	全体メモリのサイズ
<code>mem_used(xos)</code>	MB	使用中のメモリサイズ
<code>net_rcv_bytes(xos)</code>	バイト	ネットワークから受信したデータ量
<code>net_rcv_packets(xos)</code>	count	ネットワークから受信したパケット数
<code>net_send_bytes(xos)</code>	バイト	ネットワークで送信したデータ量
<code>net_send_packets(xos)</code>	count	ネットワークで送信したパケット数

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

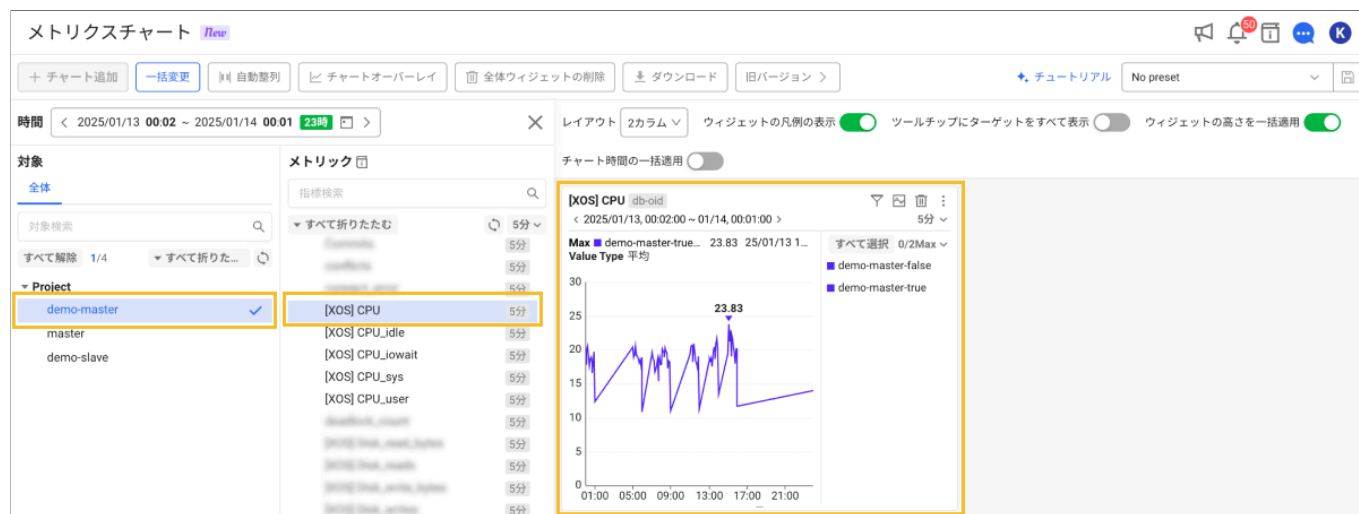
ト設定で分類されたグループ単位で選択できます。

- **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。
 - 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。

- ① **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。
- メトリクスのカテゴリとフィールド名に基づいても検索できます。カテゴリおよびフィールドの詳細については、[次の文書](#)を参照してください。
- 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。

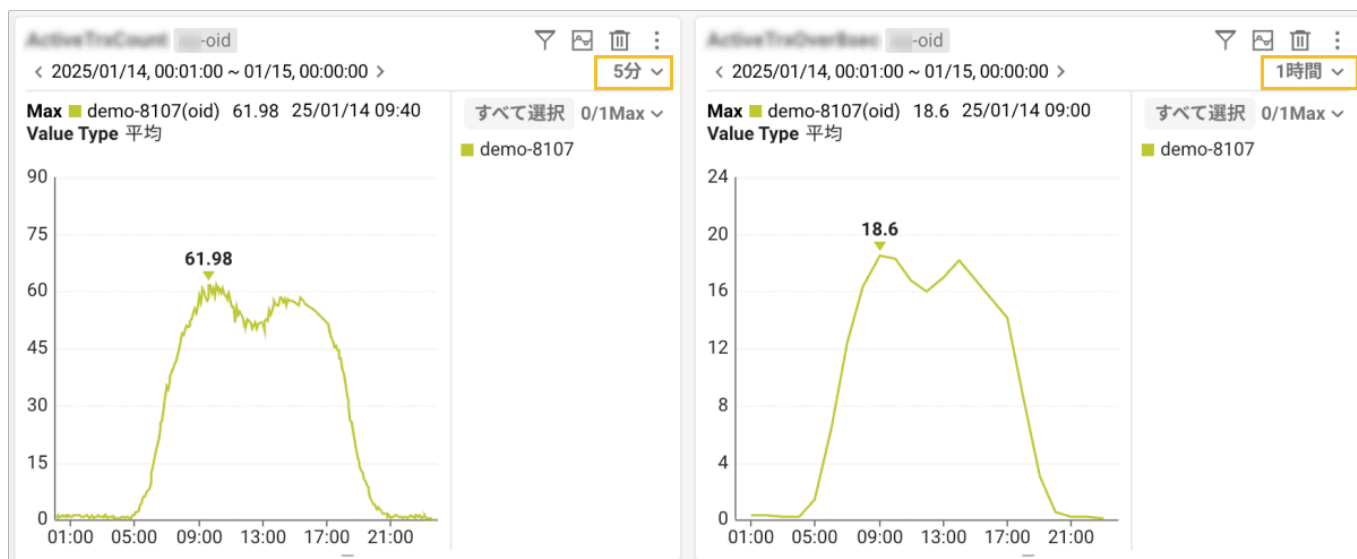
インターバルを設定する



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。

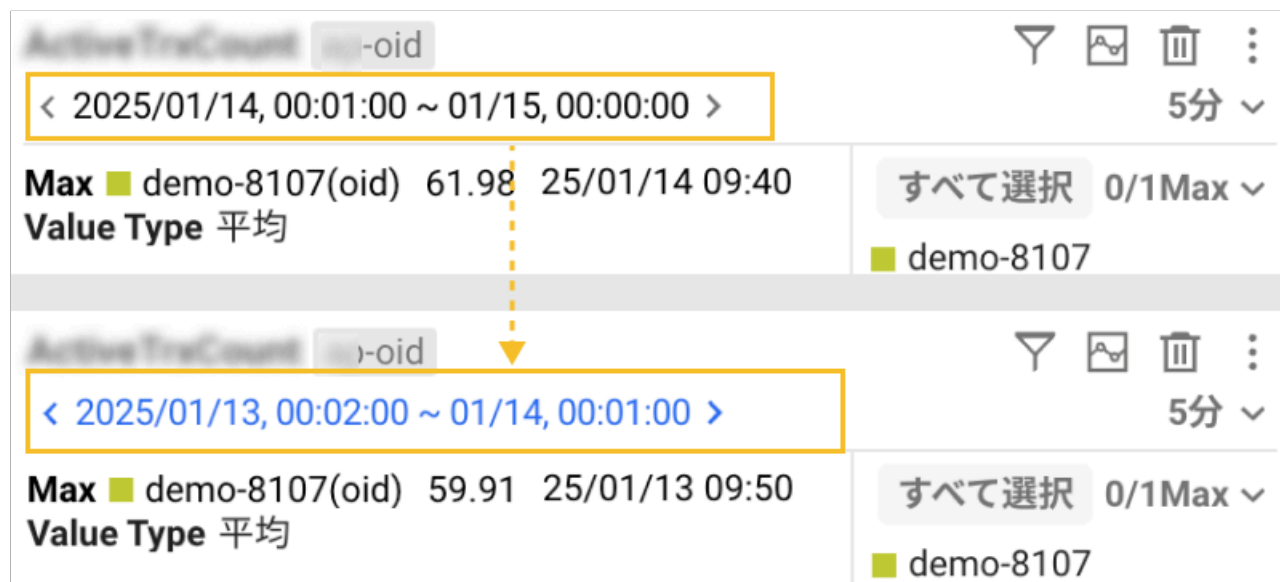
例えば、**5分間**インターバルは5分単位の平均値を表示し、**1時間**インターバルは、1時間単位の平均値を表示します。



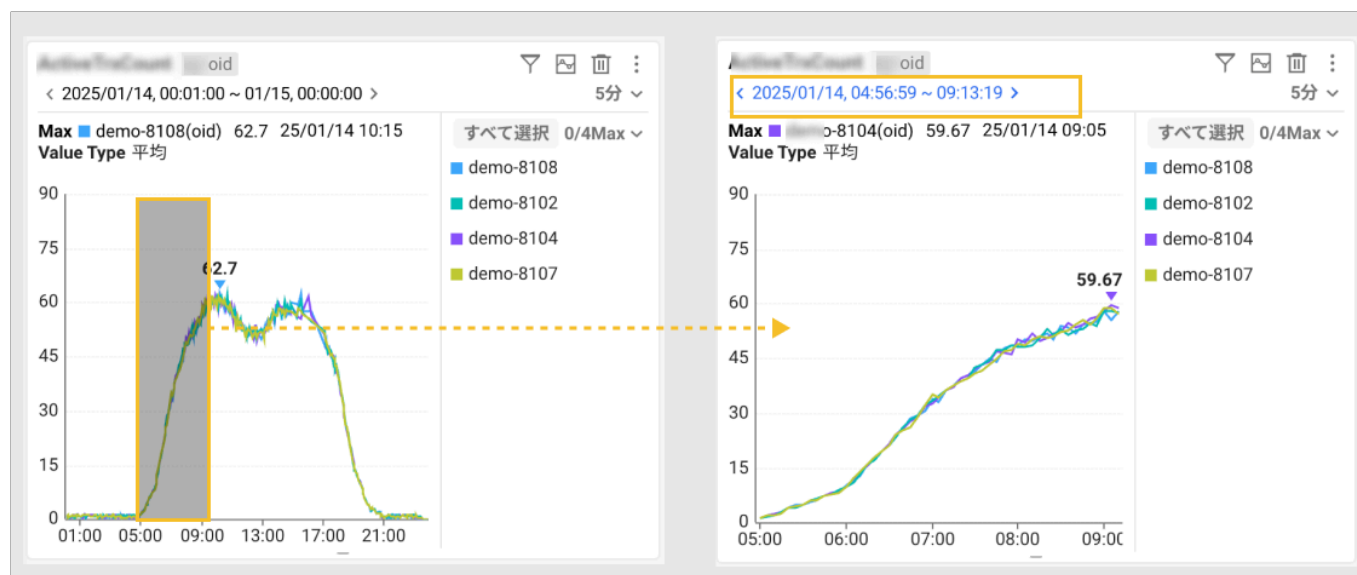
- ☑ インターバルオプションを調整し、短い間隔の詳細データから長い間隔の全体的な推移まで、多様な観点からデータを分析できます。

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。

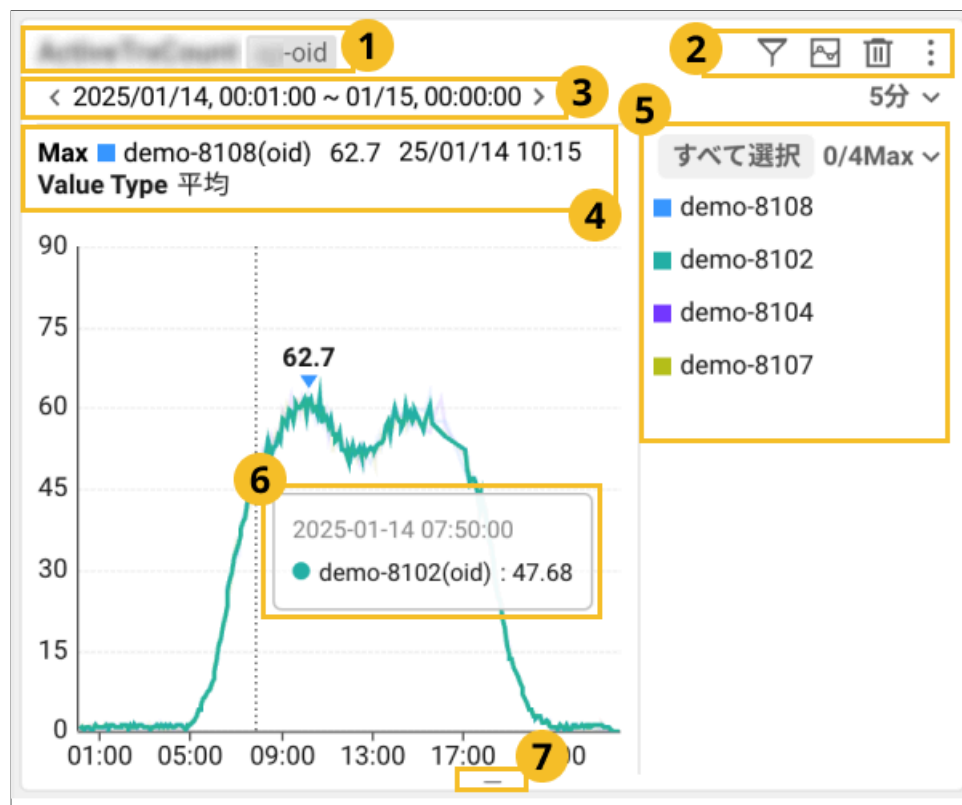


- 照会時間の範囲を変更した後、直近の時間に再度変更するには、 ボタンを選択します。
- もし画面の上部にある**チャート時間の一括適用**オプションを有効にした場合、 **時間バッチ初期化**ボタンが表示されます。このボタンを選択すると、すべてのウィジェットの時間を初期化できます。

-  **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。

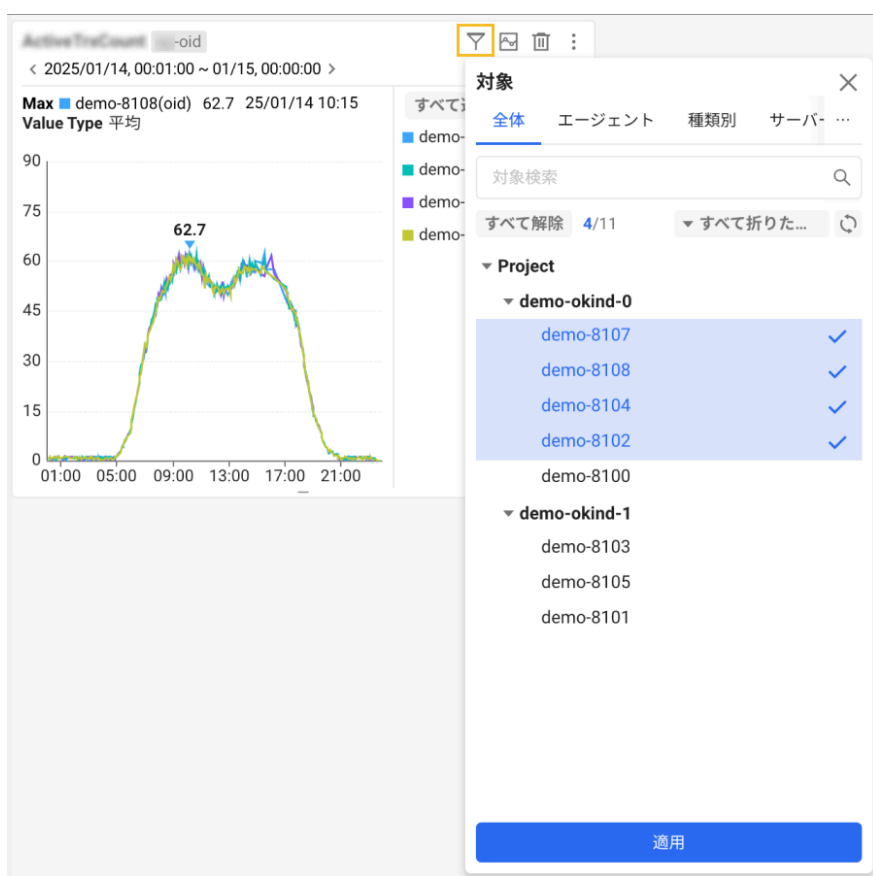
チャートウィジェットオプションを利用する

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。

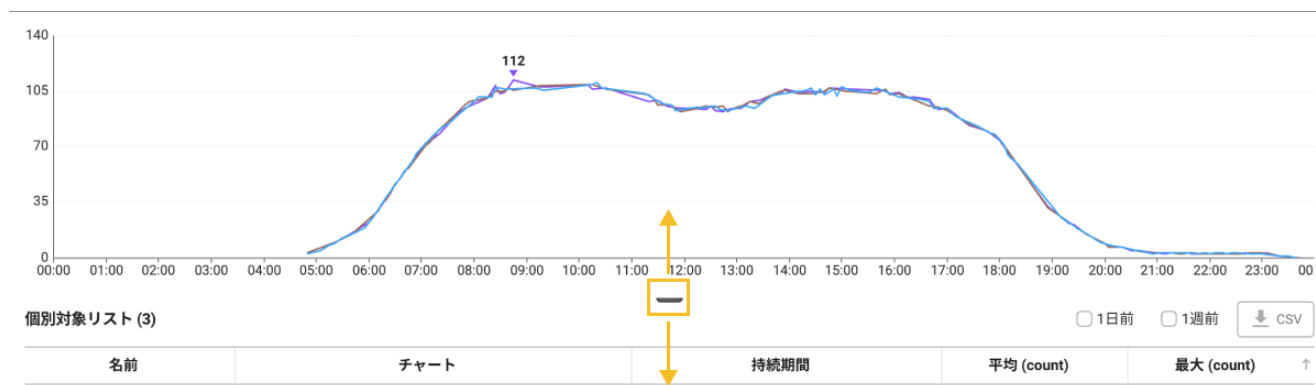
3. 適用ボタンを選択します。

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。

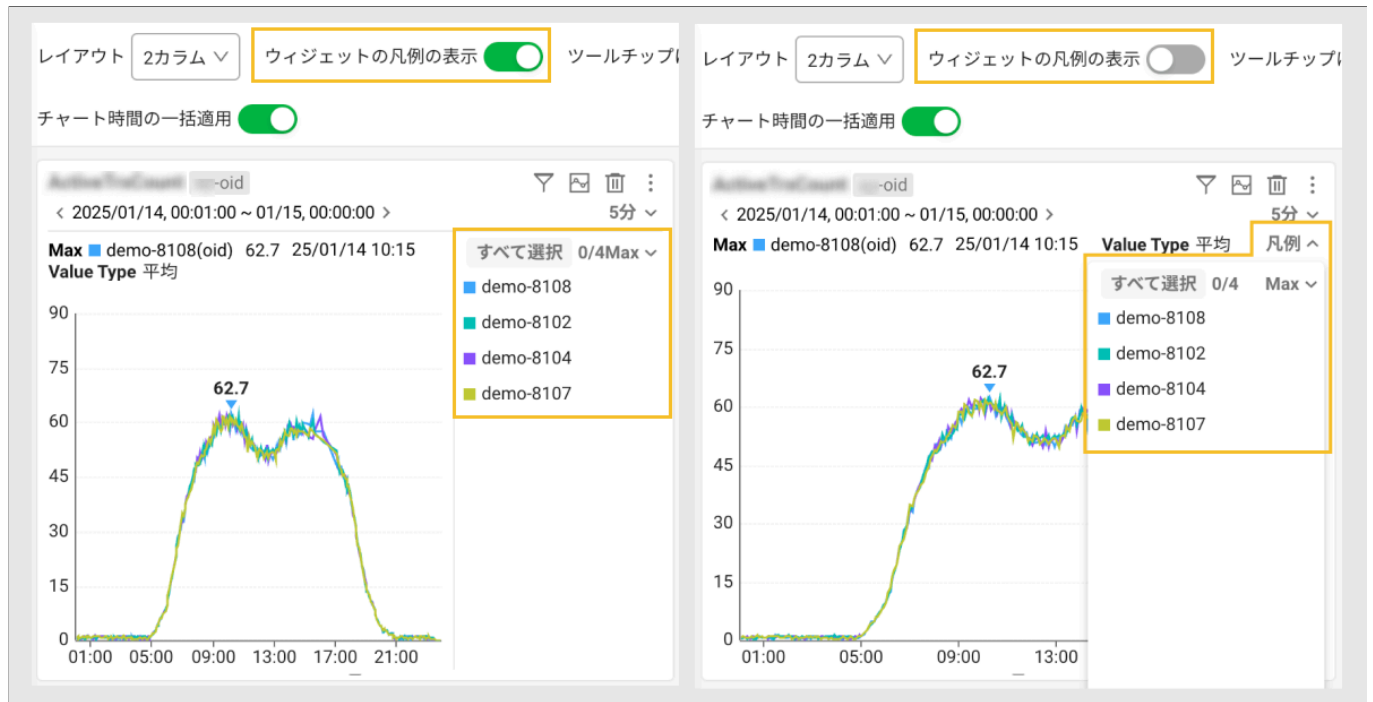


🗑️ チャートウィジェットを削除する

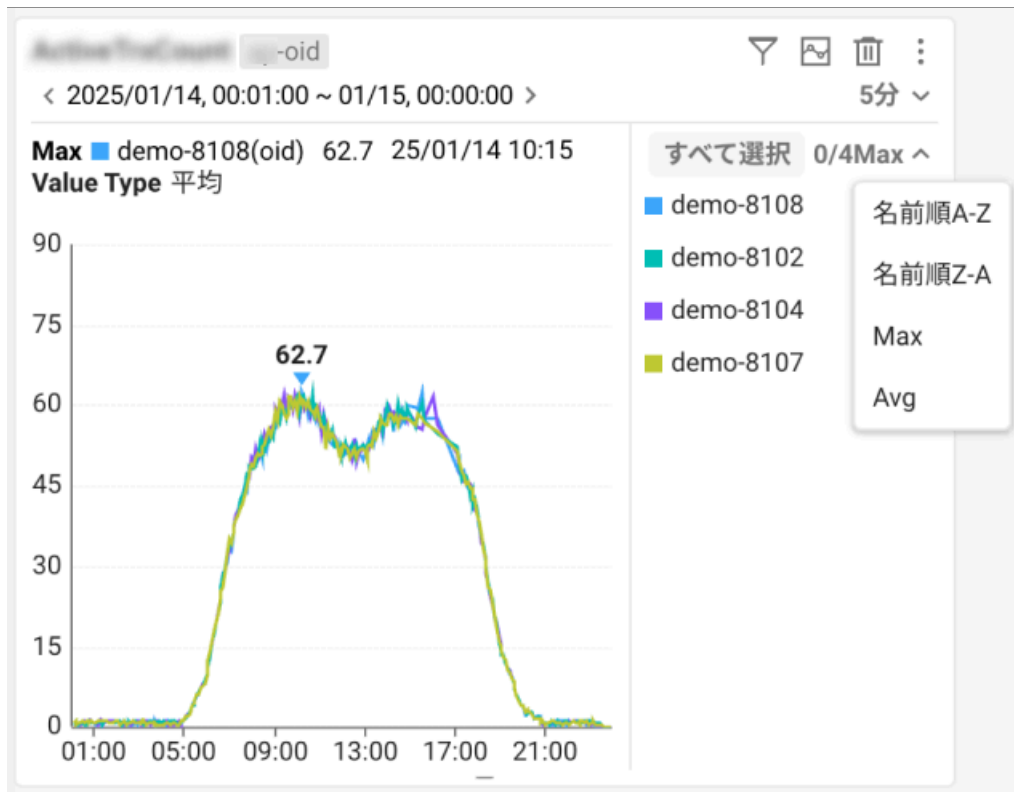
画面に配置したチャートウィジェットを削除するには、🗑️ ボタンを選択します。

凡例を活用する

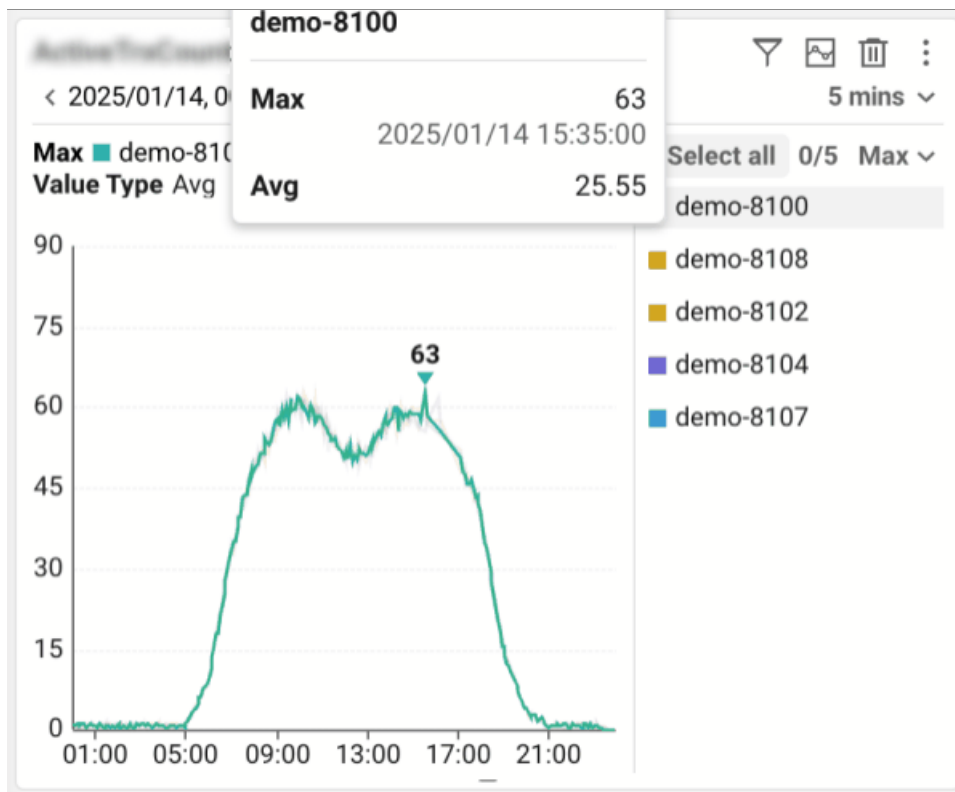
凡例を通じてチャートに表示されるモニタリング対象を確認し、希望する基準で整列したりフィルタリングできます。画面上部のウィジェットの**凡例の表示**オプションをオンまたはオフにすると、ウィジェットのチャートの右側に凡例を表示・非表示できます。オプションをオフにした状態では**凡例**をクリックしてモニタリング対象を確認して選択できます。



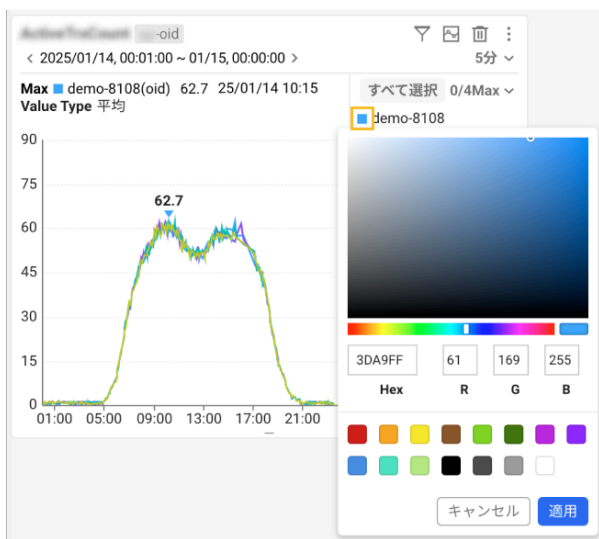
- すべて選択/すべて解除ボタンを選択してモニタリング対象を選択または解除できます。
- 凡例一覧では、モニタリング対象を名前順、最大値、平均値に基づいてソートできます。



- 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



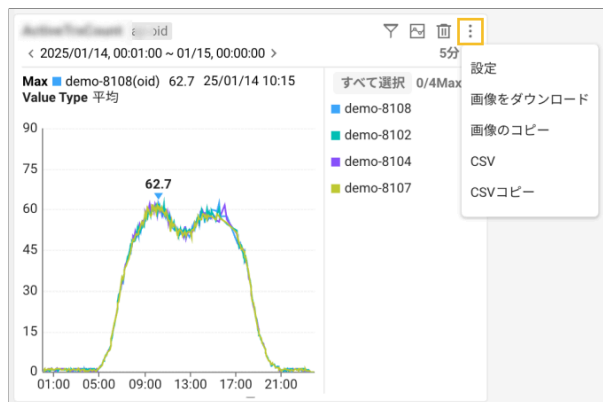
モニタリング対象に該当するグラフの色を変更できます。凡例一覧から色を変更したい対象の左側にある四角い箱

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。

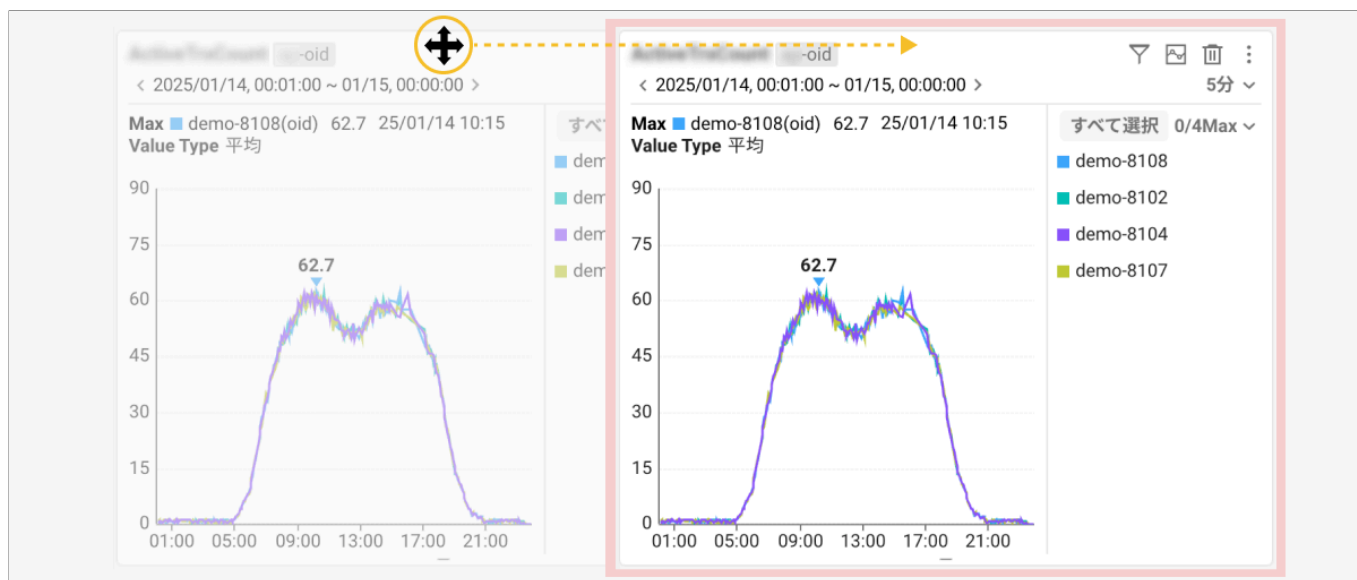
プリセットを削除する

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。

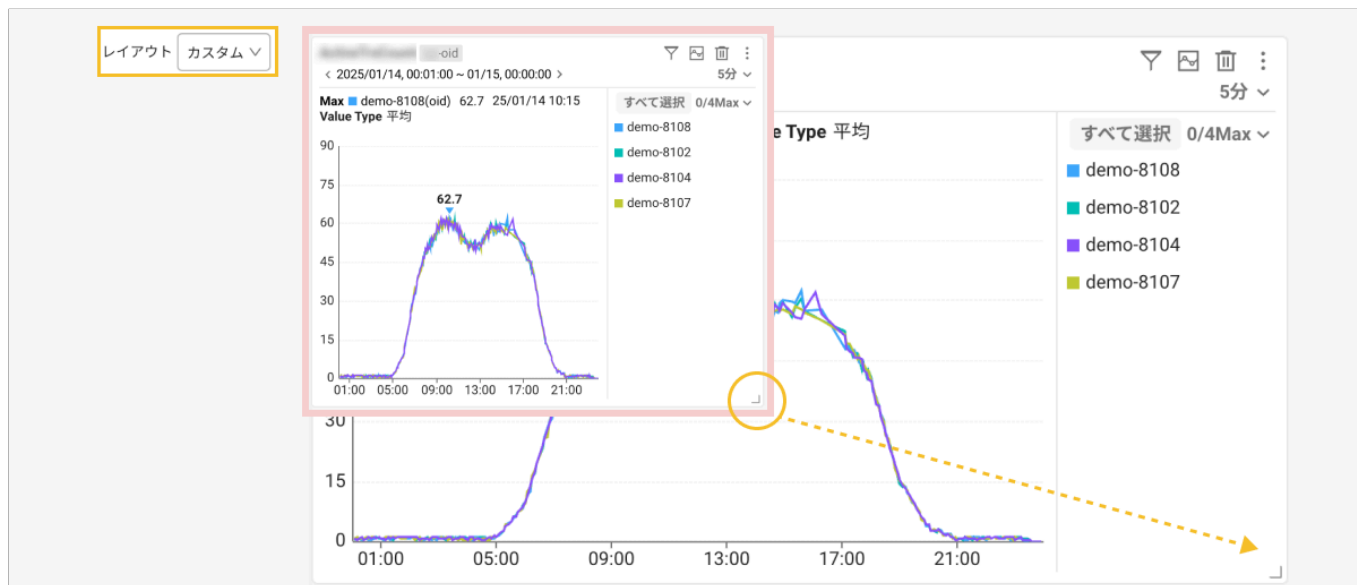
ウィジェットの移動



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。

一括変更

時間

< 2025/01/15 00:00 ~ 2025/01/15 23:59 23時

>

対象

全体

対象検索

すべて解除 1/4

すべて折りたたむ

▼ Project

demo-master

master

demo-slave

適用ウィジェット

すべて選択

☐ Active Sessions

2025/01/13, 00:02:00 ~ 01/14, 00:01:00 db-oid 5分

☐ Wait Sessions

2025/01/13, 00:02:00 ~ 01/14, 00:01:00 db-oid 5分

☐ [XOS] CPU

2025/01/13, 00:02:00 ~ 01/14, 00:01:00 db-oid 5分

☐ [XOS] CPU_sys

2025/01/13, 00:02:00 ~ 01/14, 00:01:00 db-oid 5分

☐ [XOS] Disk_reads

2025/01/13, 00:02:00 ~ 01/14, 00:01:00 db-oid 5分

☐ [XOS] Disk_writes

2025/01/13, 00:02:00 ~ 01/14, 00:01:00 db-oid 5分

間隔

変更しない

5分

1時間

キャンセル

適用

- **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。

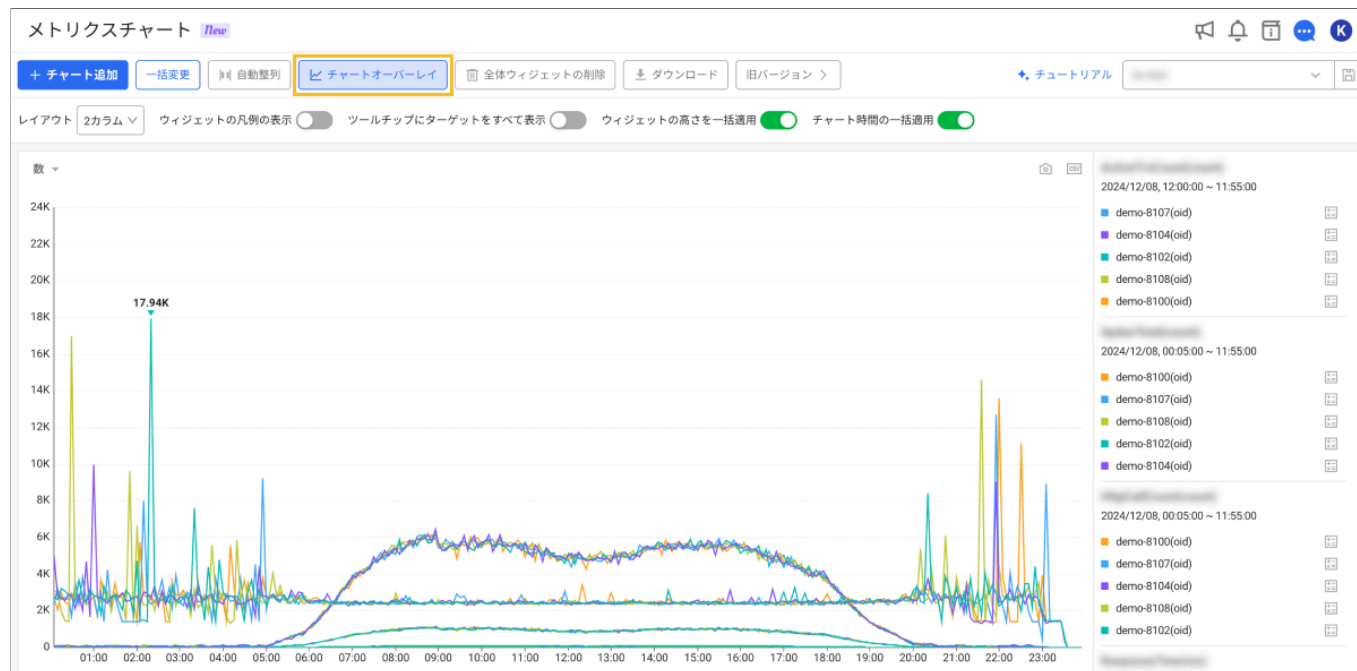
- **エージェント**: 個別エージェントまたはすべてを選択できます。
- **種類別**: エージェント設定で `whatap.okind` に分類されたグループ単位でエージェントをモニタリングします。
- **サーバー別**: エージェント設定で `whatap.onode` に分類されたグループ単位でエージェントをモニタリングします。
- **間隔**: 様々な時間間隔でデータの集計単位を調整できます。
- **適用ウィジェット**: 変更するオプションを適用するチャートウィジェットを選択します。選択したウィジェットに変更したオプションを一度に適用できます。

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。

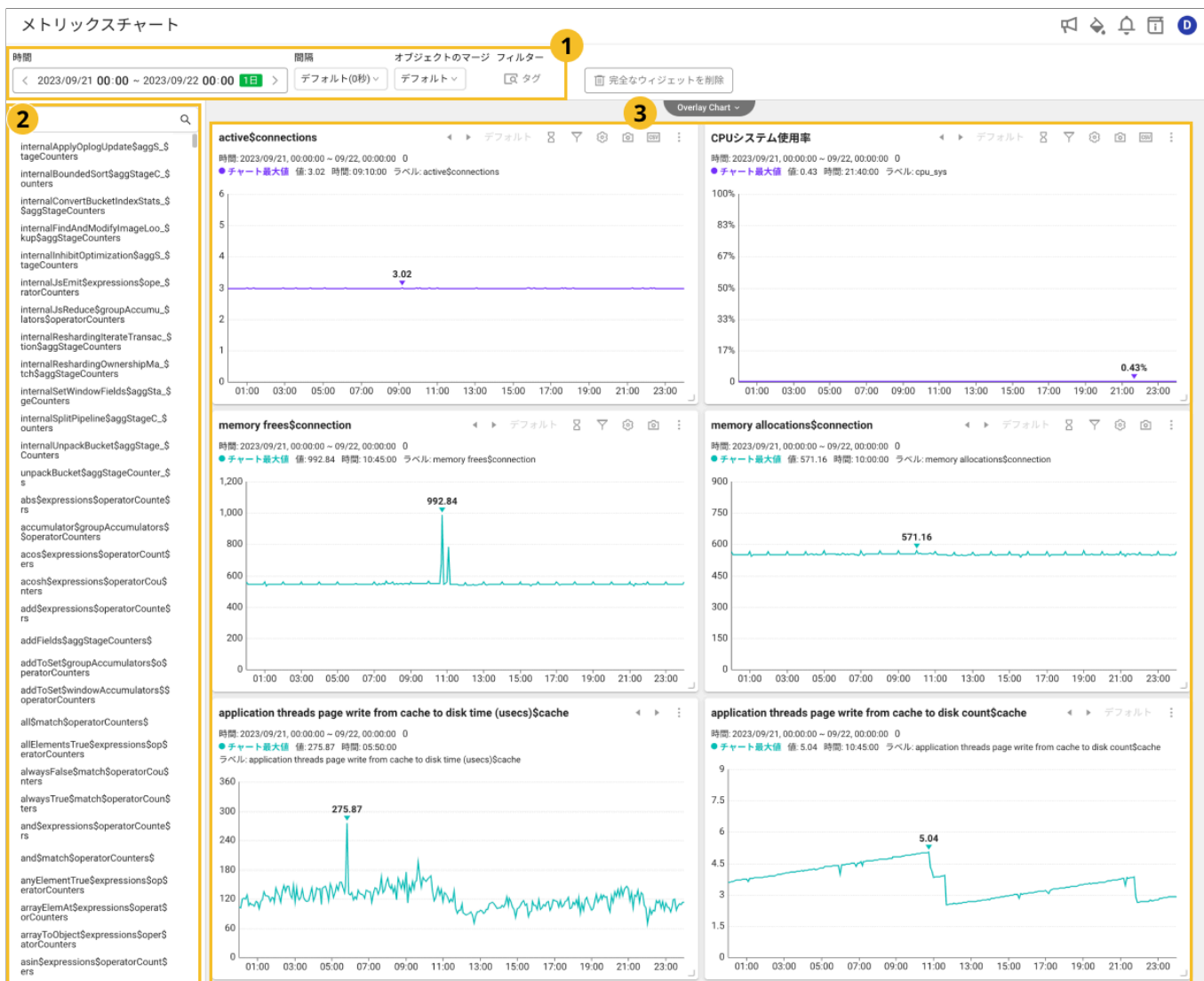
チュートリアルを利用する

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。

メトリクスチャート

🔍 サイトマップ > 分析 > メトリクスチャート Old

メトリクスチャートメニューでは、モニタリング対象から収集されたメトリクスデータを次のようにチャートで照会できます。時間と指標の指定が必須です。



上部オプション

① 領域のメトリクスチャートの上部オプションからチャートの時間範囲とモニタリング対象エージェントを指定できます。

- **時間**：時間の範囲でX軸の開始と終了を指定できます。
- **間隔**：時間間隔でX軸データの間隔を指定できます。
- **時間マージ**：データマージ方式の1つを選んで、指定した時間間隔内のデータをマージできます。

例) 平均は、1時間のデータ平均値を意味します。

-  **エージェント**：照会するエージェントを指定できます。指定しない場合は、すべてを対象に照会します。

指標一覧

② 領域は、オプションを検索する指標のリストです。まず、**カテゴリ**を選択します。**カテゴリ**を選択すると、そのカテゴリに含まれる指標が表示されます。目的の指標を選択してください。**カテゴリ**と指標を選択すると、① 領域のトップメニューから指定した時間範囲のデータに基づいて③ 領域のチャートウィジェットからデータを照会できます。

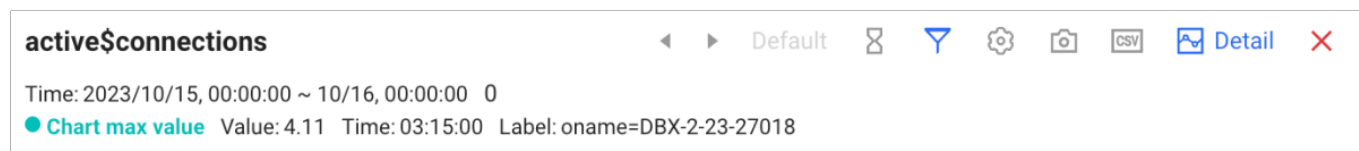
① データ結合

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。

- **時間マージ**は、ソースデータからフィールド値が同じデータを一定の間隔でマージします。
- **オブジェクトのマージ**は、異なるフィールド値を持つデータの中からタグが一致する場合、そのデータをマージします。

チャートウィジェット

③ 領域のチャートウィジェットの左上で指標名を確認できます。チャートウィジェットの右上で次のオプションを確認できます。



- タイムシフト：◀ ▶ 左矢印または右矢印ボタンを使用して、選択した時間範囲だけ-1または、+1ずつ移動することができます。

例えば、時間範囲が2月13日00:00~2月14日00:00の場合、◀ 左矢印を選択すると、2月12日00:00~2月13日00:00までのデータが表示できます。

- 間隔/時間のマージ：① トップメニューで指定した間隔と時間のマージを修正できます。
- モニタリング対象：▼ アイコンを選択して、モニタリング対象を指定できます。選択しない場合は、すべて表示されます。
- 時間比較：📊 アイコンを選択すると、同じ指標の以前の時間帯の推移を比較できます。
- スナップショット：📷 アイコンを選択すると、ウィジェットのオプションを除くチャートのスナップショットを取得できます。
- CSV：📄 アイコンを選択して、チャートを描画したデータをCSVファイルとしてダウンロードできます。
- 詳細：🔍 アイコンを選択して詳細を表示します。モニタリング対象が多い場合、モニタリング対象の指標推移を特定して確認できるため便利です。

❗ メトリクスチャートウィジェットの上部にオプションが表示されない場合は、⋮ アイコンを選択します。

ウィジェットを削除する

画面に配置したすべてのウィジェットを削除するには、🗑 全体ウィジェットの削除ボタンを選択します。

メトリクス照会

ホーム画面 > プロジェクト選択 > 分析 > メトリクス照会

メトリクス照会メニューからタグベースで特定のメトリクスを照会できます。

メトリクス照会

1

時間選択
< 2023/08/17 08:04 ~ 2023/08/17 09:04 1時 >
最大カウント
100
カテゴリ
app_counter

2

タグ 全体
container containerKey host_ip okindName oname onodeName pid type 8/8
フィルター
タグ値でフィルタリング
フィールド 全体
_clock_delta active_tx_0 active_tx_3 active_tx_8 active_tx_count apdex_satisfied apdex_tolerated apdex_total arrival_rate httpc_count httpc_error httpc_time metering resp10 resp15 resp_time sql_count
sql_error sql_fetch_count sql_fetch_time sql_time tps tx_count tx_dbc_time tx_error tx_http_time tx_sql_time tx_time tx_time_sqr_sum 5/29
CSV

3

	Time	Old	Tags								Fields				
			container	containerKey	host_ip	okindName	oname	onodeName	pid	type	active_tx_3	arrival_rate	sql_time	tps	tx_error
1	2023-08-17 08:04:30	-877561626	agent.service	1395943798	10.21.1.26	demo-okind-1	demo-8101	node-1	3284967	java	13	19.554815	9.995699	19.008858	1
2	2023-08-17 08:04:30	1387800924	agent.service	1395943798	10.21.1.26	demo-okind-0	demo-8102	node-0	3285018	java	10	21.37008	5.108556	19.723042	1

1 時間とカテゴリの選択

1 領域でメトリクスが収集された時間選択と最大カウントおよびカテゴリを指定できます。時間選択とカテゴリは、必ず指定してください。

- 時間選択：メトリクスが収集された時間を指定して照会できます。既定値は 1時間 です。基本オプションとして提供する照会時間以外に、ユーザーが時間選択タブを選択して日付と時間を指定できます。

① 時間選択オプションの利用方法の詳細については。

- 最大カウント：3 一覧から参照するメトリクスの最大数を指定できます。10、50、100、200、300、1000、2000、3000 個まで設定できます。
- カテゴリ：関連指標の分類単位です。カテゴリタブを選択し、カテゴリを指定できます。
- 🔄 カテゴリ、タグ、フィールドオプションの更新：カテゴリ、タグおよびフィールドオプションを再読み込みできます。

2 タグとフィールドの選択

2 領域でタグとフィールドを選択します。ユーザーが個別に指定しない場合、デフォルト設定が完全な選択になります。

- **タグ**：収集された対象を区分できる固有情報データです。
- **フィールド**：モニタリング対象から収集された指標です。
- **フィルター**：▼タグ値でフィルタリングボタンを選択し、タグ値を設定してフィルタリングできます。

例) oname の値を demo-8101 に設定すると、フィルタリングしたデータを表示することができます。

- 🔍 **検索**：条件を設定して検索アイコンを選択すると、3 領域でそのメトリクスの原本データを検索できます。
- 📄 **CSV**：メトリクスの原本データをCSVファイルとしてダウンロードできます。

3 メトリクステーブル

収集されるメトリクスを事前に特定できないため、収集されるすべてのメトリクスの原本データを確認することが重要です。上記の条件領域で目的の条件を設定した後 3 領域で、そのメトリクスの原本データをテーブル形式で検索できます。ユーザーがタグとフィールドの各条件を指定することによって、テーブルのカラムが変更されます。

- ❗ • メトリクスの参照時、**時間選択**と**カテゴリ**を指定する必要があります。
- メトリクス参照時、**タグとフィールド**の指定はオプションです。

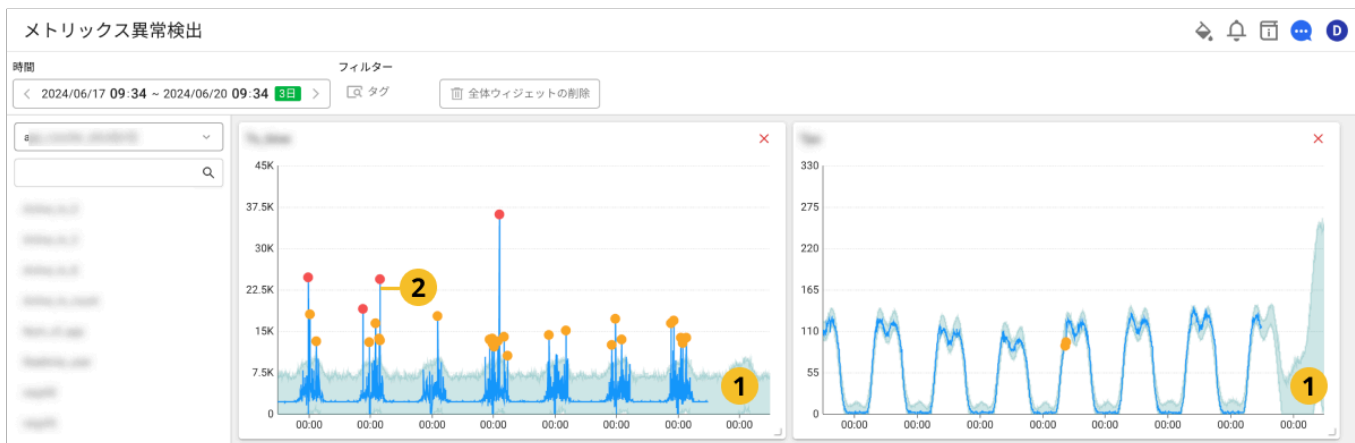
メトリクス異常検出

ホーム画面 > プロジェクト選択 > 分析 > メトリクス異常検出

さまざまなメトリクスのパターンをAIが学習した予想パターンと比較できます。予想パターンを外れた異常探知をグラフチャートで確認できます。過去のデータに基づいて繰り返されるパターンを確認し、今後の指標値の予測に活用できます。

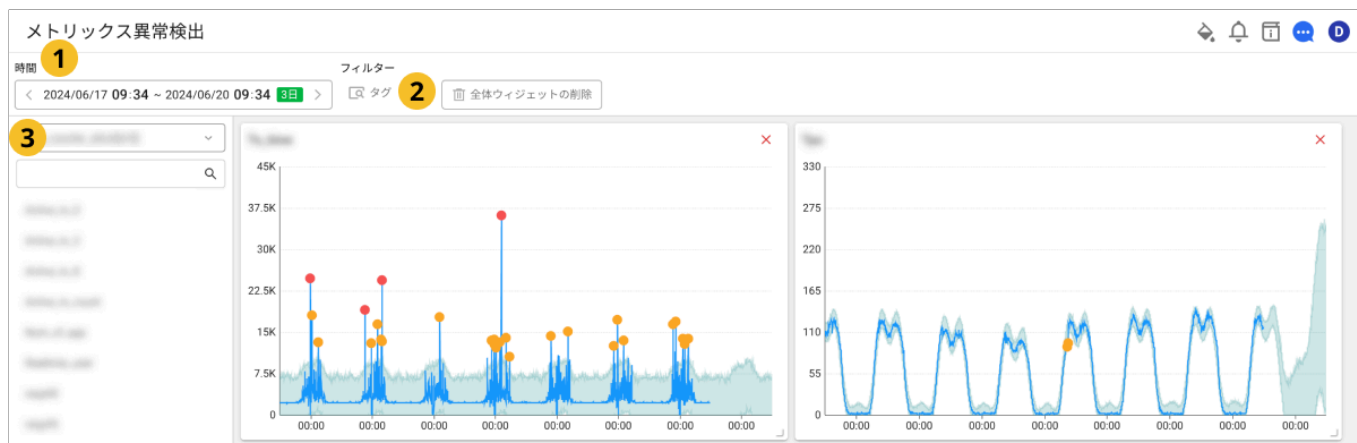
- ❗ 画面に配置したウィジェットは、別のメニューに移動すると保存されずに初期化されます。
- パターン分析と異常値検出機能を除くと分析 > メトリクスチャートメニューに似ています。
- 異常値(Anomaly Detection)アラート通知機能の技術的根拠は、メトリクス異常値です。異常値アラート通知設定の詳細については、[次の文書](#)を参照してください。

ウィジェットを確認する



- ① 明るい色のグラフ領域は、AIによって分析した予想されるパターンです。
- ② 青色グラフは、プロジェクトのメトリクスの推移です。
- AIによって分析された予想パターンから外れるとオレンジ色と、赤色のステップでグラフにドットが表示されます。予想されるパターンの範囲から大幅に外れた値を赤色として表示します。

ウィジェットを配置する



1. ① 時間で、目的の時間間隔を設定してください。最大1か月間隔まで設定できます。
2. ② フィルターでメトリクスの範囲を選択します。
3. 以下の一覧でモニタリングするメトリクスを選択します。

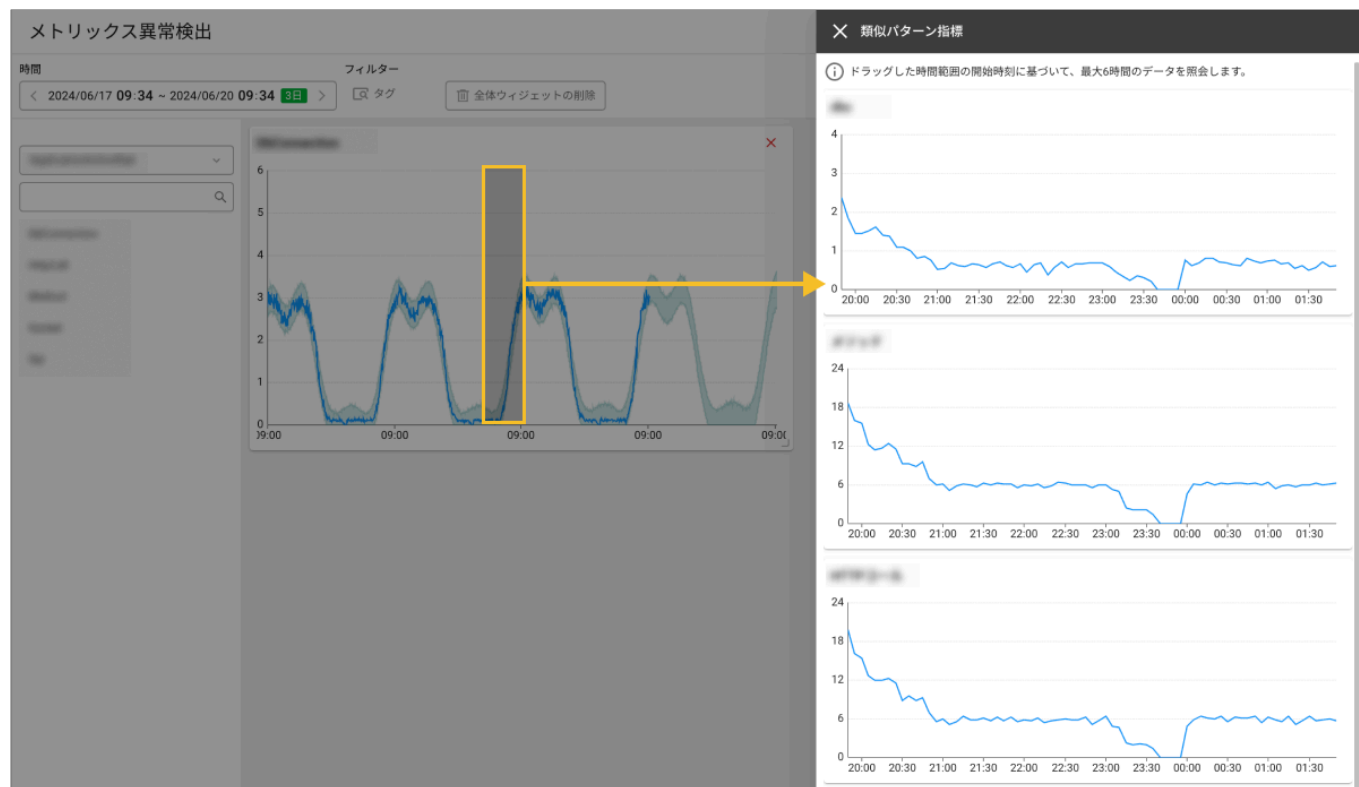
選択したメトリクスを画面の右側に配置します。

- ① モニタリング対象を選択してメトリクスを絞り込んで確認するには、② タグを選択します。画面右側にタグ選択リストが表示されます。目的の項目を選択し、ウィジェットを追加します。
- 画面に配置したウィジェットは、時間またはタグ値を変更してもチャートに反映されません。
- 画面に配置したウィジェットを削除するには、ウィジェット右上の✕ボタンを選択します。
- ウィジェットの左上を選択した状態でドラッグすると、ウィジェットの位置を変更できます。
- ウィジェットの右下を選択した状態でドラッグすると、ウィジェットのサイズを変更できます。

ウィジェットを削除する

画面に配置したすべてのウィジェットを削除するには、 全体ウィジェットの削除ボタンを選択します。

関連メトリクスを確認する



ウィジェットでチャートの一部の領域をドラッグします。画面の右側に**類似パターン指標**画面が表示されます。ドラッグした時間範囲の開始時刻に基づいて、最大6時間の関連メトリクスを照会できます。

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。

データベースのサイズ

ホーム画面 > プロジェクト選択 > 統計/レポート > DBサイズ

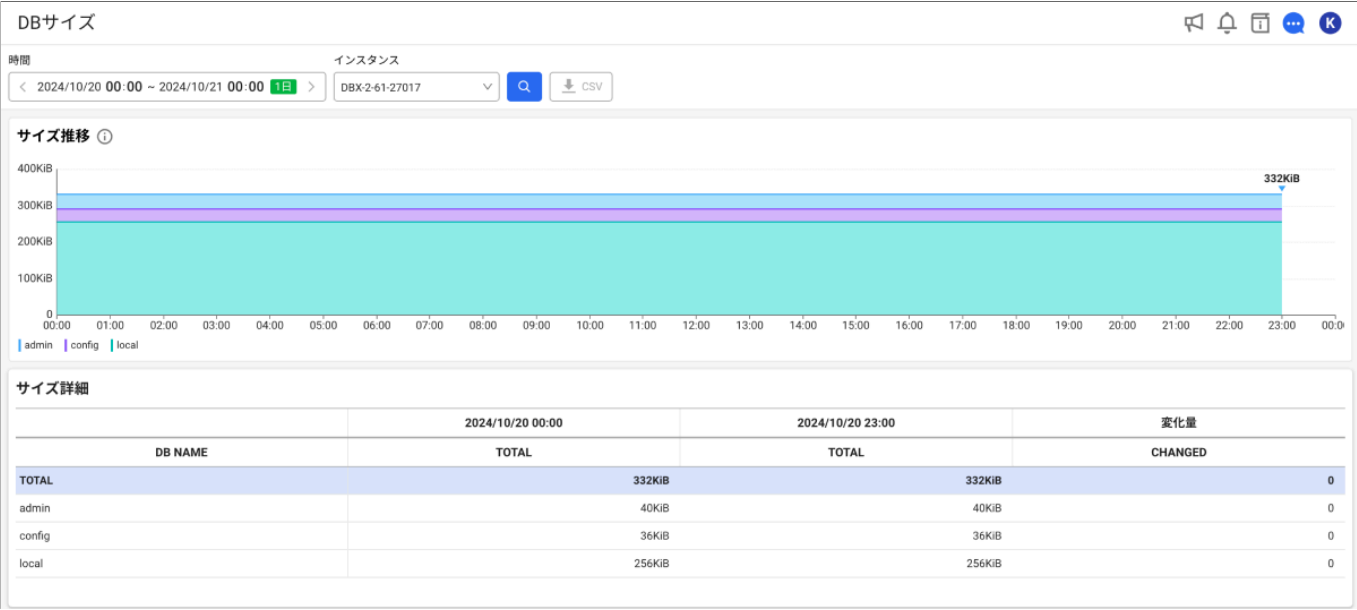
データベースごとのテーブルのサイズを集計し、推移情報をチャートで提供します。データベースの容量が増加する傾向を識別して管理できます。容量が急速に増加する場合を事前に把握して備えられます。

データベースのサイズは、性能にも大きな影響を与える可能性があります。サイズの増加により、クエリの実行時間が長くなる可能性があるため、性能問題の解決を準備できます。間違ったクエリやデータベース構造によりサイズが増加する可能性のある問題を事前に把握して予防することも必要です。

データベースサイズの推移により、使用量のパターンとデータの成長が理解できます。将来の容量要件を予測し、対策を講じられます。これらの変化をモニタリングすることは、リソースとコストを最適化するのに役立ちます。

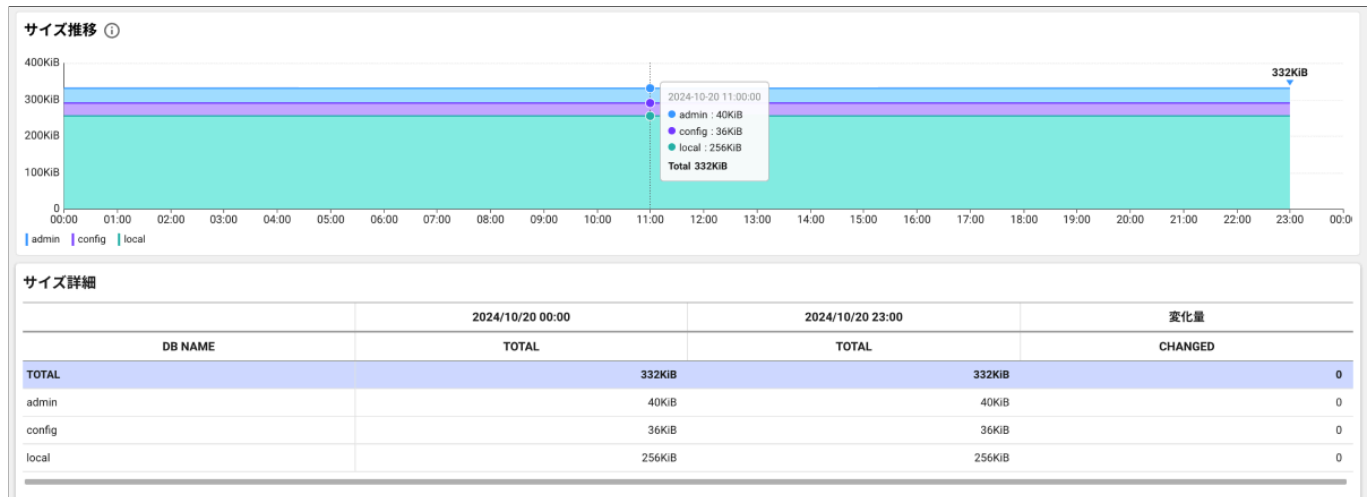
使用する前に

基本画面ガイド



1. 時間で照会したい時間を設定します。緑のボタンを選択して照会時間を選択することもできます。
2. インスタンスで照会したい対象を選択します。
3.  ボタンを選択します。

時間別変化量を確認する



・ サイズ推移

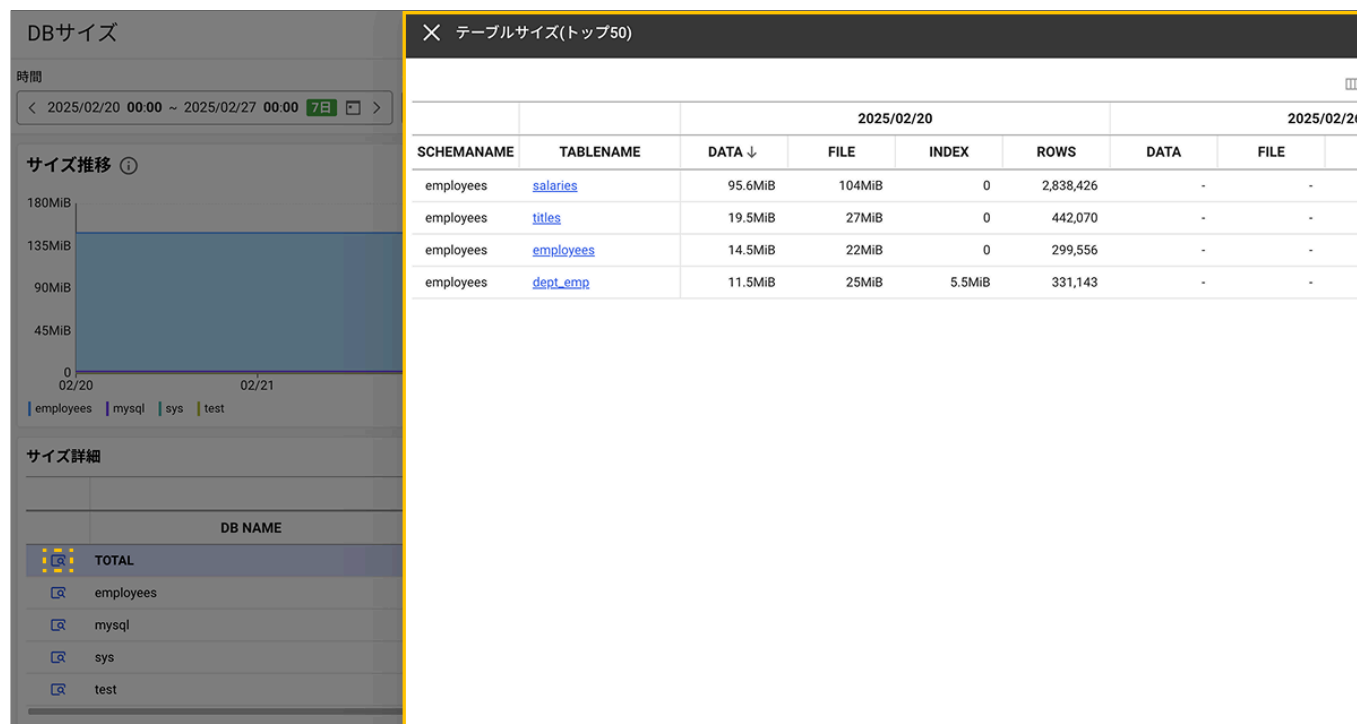
時間帯ごとに、データベースの全体的なサイズと使用量の変化を視覚的に確認できます。チャートで各データベースのサイズを色分けして表示し、マウスをチャートの上にオーバーした状態で左右に移動します。特定の時点の各データベースサイズをツールチップで詳細に確認できます。

・ サイズ詳細

データベースごとの容量の詳細をテーブル形式で提供します。各データベースの名前(DB NAME)および合計容量(TOTAL)、変更量(CHANGED)を確認できます。特定のデータベースを選択すると、テーブルサイズ(トップ50)セクションで詳細情報を確認できます。

テーブル別のサイズを確認する

サイズ詳細セクションでデータベースを選択すると、そのデータベース内のサイズTOP50に該当するテーブルごとのサイズを一覧で確認できます。



- ⓘ この機能は、DBXエージェント1.7.0バージョン以降に対応しています。関連するエージェント設定の詳細については、[次の文書](#)を参照してください。
- テーブルサイズ(トップ50)セクションでテーブルカラムの順番を変更したり、特定のカラムを非表示にするには、右上に☐ボタンを選択します。カラム設定の詳細については、[次の文書](#)を参照してください。

照会データのダウンロード

照会したデータをCSV形式のファイルでダウンロードできます。[📄 CSV](#) ボタンを選択した後サイズ詳細またはテーブルサイズ(トップ50)を選択します。

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。

適用方法

データベースとAWS RDSのログを収集する方法をご案内します。

 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。

 ログの検索

ログモニタリングのログ検索メニューについて説明します。

 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。

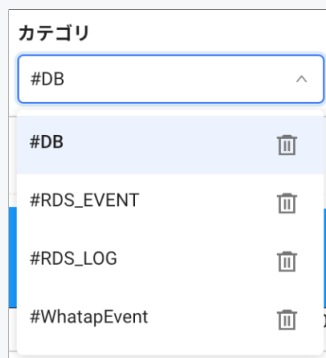
 ログパーシング

WhaTapが提供するログパーサについて案内します。

適用方法

WhaTapは、データベースのログモニタリングを提供します。サーバーインストール型データベースと、クラウドサービスであるAWS RDSのログを収集できます。これにより、WhaTapのログモニタリング機能である**ログTail**、**ログトレンド**メニューからデータベースの散在したログをひと目で確認できます。

- ✔ ログモニタリングを適用した後、各メニューの**カテゴリ**項目とログ一覧からインストール型DBは `#DB`、AWS RDSは `#RDS_LOG` および `#RDS_EVENT` と表示されます。



サーバーインストール型DBに適用する

サーバーにインストールされたデータベースのログをモニタリングするには、WhaTapの`xos.conf`ファイルに次のオプションを適用します。

`xos.conf`

```
file=/var/log/mongodb/mongodb.log
```

- ⓘ 適用する前に、XOSエージェントをインストールしてエージェント設定を行う必要があります。詳細については、[次の文書](#)を参照してください。

ログモニタリングを開始する

すべての設定を完了した後、ログ>ログ設定メニューにアクセスし、ログモニタリングを活性化します。

エージェントの設定とログモニタリング活性化

ログTail、ログトレンド、ログ検索機能で、アプリケーションに点在するログをまとめて確認することができます。

ログモニタリングの設定方法

[インストール型DB](#) AWS RDS

1. XOSエージェントのインストール

LinuxファイルシステムにインストールされたDBのログは、WaタブのXOSエージェントで収集します。
下記のガイドリンクからインストールを進めてください。

[エージェントインストールガイド >](#)

2. xos.confファイルにオプション適用

xos.confファイルに次のオプションを適用してください。

```
log_monitoring: true
log_monitoring_options:
  log_monitoring: true
  log_monitoring_options: true
```

📋 コピー

3. ログモニタリング機能の活性化

設定完了後、ログ監視を有効にするトグルボタンをクリックしてください。



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.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。

- ① フィルタータグが2行以上長くなる場合へ **折りたたみ**アイコンを選択して折りたたむことができます。
- フィルタータグを入力した後、入力画面でShiftとTabキーを同時に使用して、以前のフィルタータグに移動できます。
- フィルタータグを入力した後、入力画面でTABキーを通じて次のフィルタータグに移動できます。

フィルタータグ追加

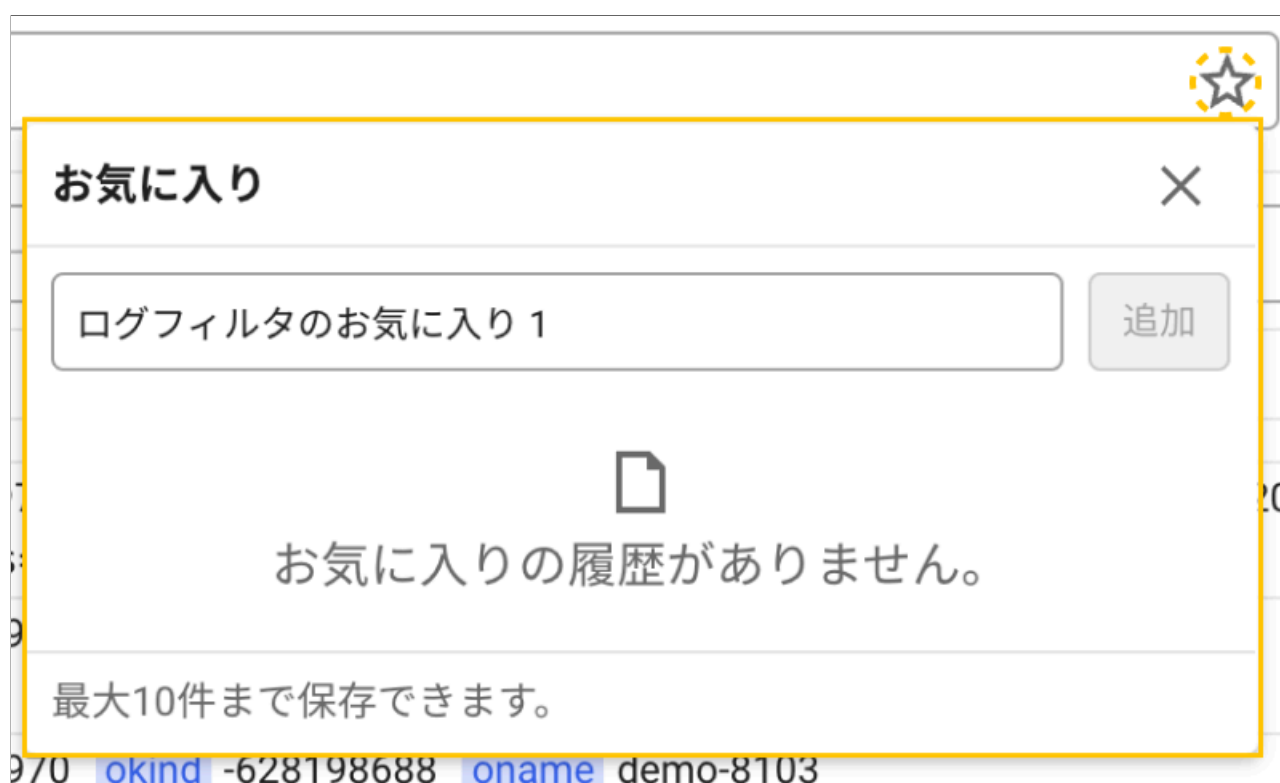
入力フィールドにテキストを入力し、Enter または Tab キーを押すか、入力欄下のガイド UI で推奨値をクリックまたは矢印キーで選択して追加できます。

フィルタータグの削除

単一のタグを削除するには、**Backspace** キーを押すか、タグ上の **X** アイコンをクリックします。すべてのタグを一度に削除するには、入力フィールド右側の **X** アイコンをクリックします。

フィルターのお気に入り

フィルターお気に入り機能を提供します。入力画面の右側にある ☆ お気に入り アイコンを選択して、目的のフィルター検索条件をお気に入りに追加、削除および既存のお気に入りを選択できます。お気に入りは最大50個まで保存されます。



フィルター適用の例外状況

- 数字のみ入力できるインデックス(.n で終わる 検索キー)を入力したタグで、 検索値 は数字のみ入力できます。
- 重複した 検索キー 、 検索値 は入力できません。
- 検索キー 、 検索値 いずれかのタグが存在しない場合は、検索できません。有効でないタグの場合、灰色と表示します。

❗ **ログTail** 検索キー として category は入力できません。

入力フィルター値の下にある数式(expression)は、ログデータを表示するときに適用されるフィルター式のプレビューです。

パースングされていないキーワードのフィルター適用

ログからパースングされていない、つまりインデックスが作成されていないキーワードを含むログを照会できます。この場合、指定範囲内のすべてのログをFull Scanします。そのため、インデックスが生成されたキーに比べて検索速度が多少落ちる可能性があります。定型化されたログデータの場合、**ログパーサの設定**を通じてインデックスキーを活用した検索をお勧めします。

フィルター ⓘ

▼
content == *select* ×
フィルターを入力してから「Enter」キーを押して追加
×

content == *select*

1. カテゴリを選択します。
2. フィルター入力欄に content を選択後、検索キーワードを入力します。
例) content *select*
3. 🔍 検索ボタンをクリックしてログを照会します。

- ❗
- **ログTail**の場合、すべてのログ検索が可能であるため、カテゴリを指定する必要はありません。
 - パーサ設定の詳細については、[次の文書](#)を参考にしてください。

フィルター修正

フィルターに値を入力し、入力した値をクリックすると、その値を修正できます。

フィルター ⓘ

🔍 oname == aws-base:index X key == aws-base:index X appender != fileAppender X フィルターを入力してから「Enter」キーを押して追加 X

☐ 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

AppLog

フィルター

content

+=select*

×

フィルターを入力してから「Enter」キーを押して追加します。

content == +=select*

act

🔍

⏸

🔄

📄

⚙

	oname	タイムスタンプ	ログ
▶	demo-8102	2023-11-24 14:06:43.648	@txid 4785826165275137961 pcode 5490 oname demo-8102 onodeName node-0 oid 1387800924 okindName demo-okind-0 okind -1383513482 select distinct ename, deptno, sal, job from emp
▶	demo-8102	2023-11-24 14:06:43.654	@txid 4785826165275137961 pcode 5490 oname demo-8102 onodeName node-0 oid 1387800924 okindName demo-okind-0 okind -1383513482 select ename, 1000 from emp
▶	demo-8102	2023-11-24 14:06:43.659	@txid -240363117644553212 pcode 5490 oname demo-8102 onodeName node-0 oid 1387800924 okindName demo-okind-0 okind -1383513482 select distinct pp.lastname, pp.firstname
▶	demo-8102	2023-11-24 14:06:43.659	@txid 4785826165275137961 pcode 5490 oname demo-8102 onodeName node-0 oid 1387800924 okindName demo-okind-0 okind -1383513482 select 'total income is', ((orderqty * unitprice) * (1.0 - unitpricediscount)), ' for '

1. ハイライトしたいキーワードをキーワード入力欄に入力します。

- 例: `select`

2. 検索したキーワードがログリストのContent内でハイライト表示されます。

-  **拡大表示** アイコンをクリックすると、**ログ** と **タイムスタンプ** を全画面で確認できます。
- ハイライトされたキーワード間の移動はショートカットで操作できます。
 - `Enter` : 次の行へ移動
 - `Shift+Enter` : 前の行へ移動
 - `↑ / ↓` アイコン: 行の移動
 - `Cmd + F` (Mac) / `Ctrl + F` (Windows): キーワード検索

複数キーワード条件

複数キーワードでハイライトする場合は、次のように作成します。

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

ハイライトカラー設定

ハイライトするキーワードおよび色を設定できます。

- デフォルトでは、ログレベルに応じたハイライト (**FATAL**、**ERROR**、**WARN**、**SEVERE**、**CRITICAL**) が適用されています。
- 設定した内容は**プロジェクト単位**で保存されます。

1.  アイコンをクリックします。

2. **ハイライト** ウィンドウで、色を設定するキーワードを入力欄に追加してください。
3. 入力欄の左側の色をクリックすると、色を選択できます。

テーブル設定

カラム設定

2 領域の右で  **カラム設定** ボタンを選択します。カラムを追加したり、順序を設定できます。

- **カラム追加**

タグを選択してテーブルにカラムを追加できます。**log**カラム選択を解除する場合**ログ表示詳細設定**が確認できません。必ず1つ以上のカラムを選択します。

- **カラム順序設定**

カラムを追加すると**表示項目**に該当カラムが追加されます。希望のカラムをドラッグしてカラムの順序を変更します。

ログ表示詳細設定

2 領域右で  **ログ表示詳細設定** ボタンを選択します。デフォルトで**content**、**タグ**すべてチェックされており、両方の項目を表示します。**content**と**タグ**どちらかは必ず選択します。

チェックが解除されたアイテムはテーブルに表示されません。次のように**タグ**を解除する場合、テーブルでログの**タグ**は表示されません。

ログテーブルコンテンツタグ非表示

タグ管理一覧にタグを追加すると、追加した順にログのタグがソートされます。タグの順序はドラッグして変更できます。追加したタグを無効にすると、無効にしたタグはログのタグに表示されません。

❗ **カラムおよびログ表示設定の適用範囲**

- **カラム設定**と**ログ表示詳細設定**は、**ログTail**、**ログ検索**、**ログトレンド**で使用できます。
- 同一プロジェクト内の**ログTail**、**ログ検索**、**ログトレンド**は、**カラム設定**と**ログ表示詳細設定**を共有します。

ログファイルのダウンロード

検索したログの結果を **CSV** または **TXT** ファイル形式でダウンロードできます。

1. 画面中央右側の **↓ ダウンロード** ボタンをクリックします。
2. **CSVダウンロード** または **Logダウンロード** をクリックして、希望の形式のファイルをダウンロードします。

ログエクスプローラー

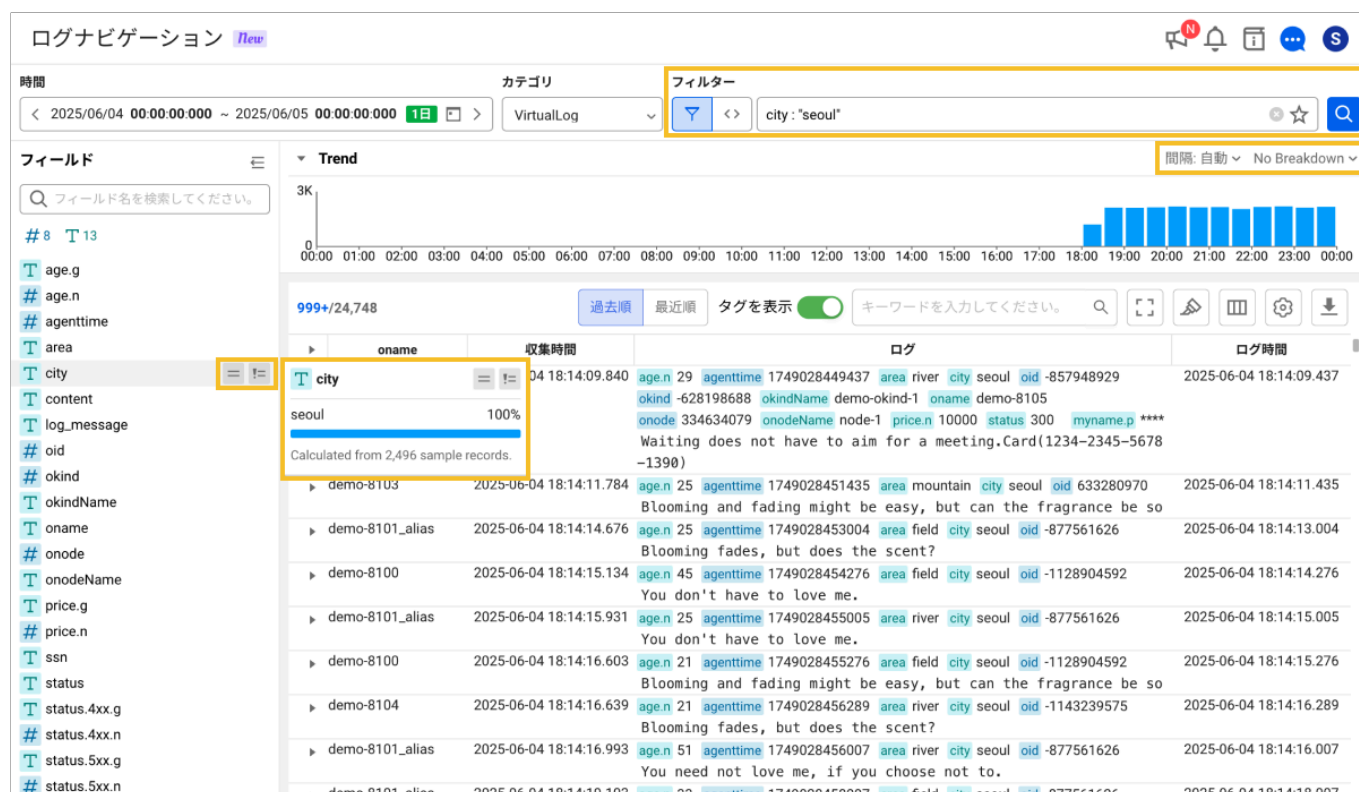
ⓘ ログ参照権限がない場合は、そのメニューにアクセスできません。

ホーム画面 > プロジェクト選択 > ログ > ログエクスプローラー *New*

ログエクスプローラー (Log Explorer) 機能は、ログデータを迅速に検索、フィルタリング、分析します。フィールド構造に関する情報を把握し、クエリベースのフィルタリングによって必要なログを効率的に検索し、結果をデータの可視化を通じて確認できます。本機能はLuceneインデックスをベースに動作し、主な特徴は以下のとおりです。

1. **ログトレンド分析および検索:** ログのトレンドと検索機能を同時にサポートし、時間経過によるログの変化傾向を把握できます。
2. **高速検索およびフィルタリング:** ユーザーは簡単なキーワード入力だけで、問題のあるログを迅速に検索できます。WhaTapログ検索クエリおよびLuceneクエリ言語に対応しており、さまざまな検索条件を設定できます。
3. **オートコンプリート機能:** クエリ入力時にオートコンプリート機能が提供され、ユーザーが簡単にクエリを作成し、習得できるようサポートします。
4. **データ可視化:** スタックグラフを活用して時系列のログ件数データを視覚的に表示し、ドリルダウン機能を通じて特定のログを深く分析できます。
5. **お気に入りと共有:** よく使うフィルターはお気に入りとして保存でき、URLを通じて他のユーザーと簡単に共有できます。

基本画面ガイド



時間設定

上部のオプションバーにある**タイムセレクター**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

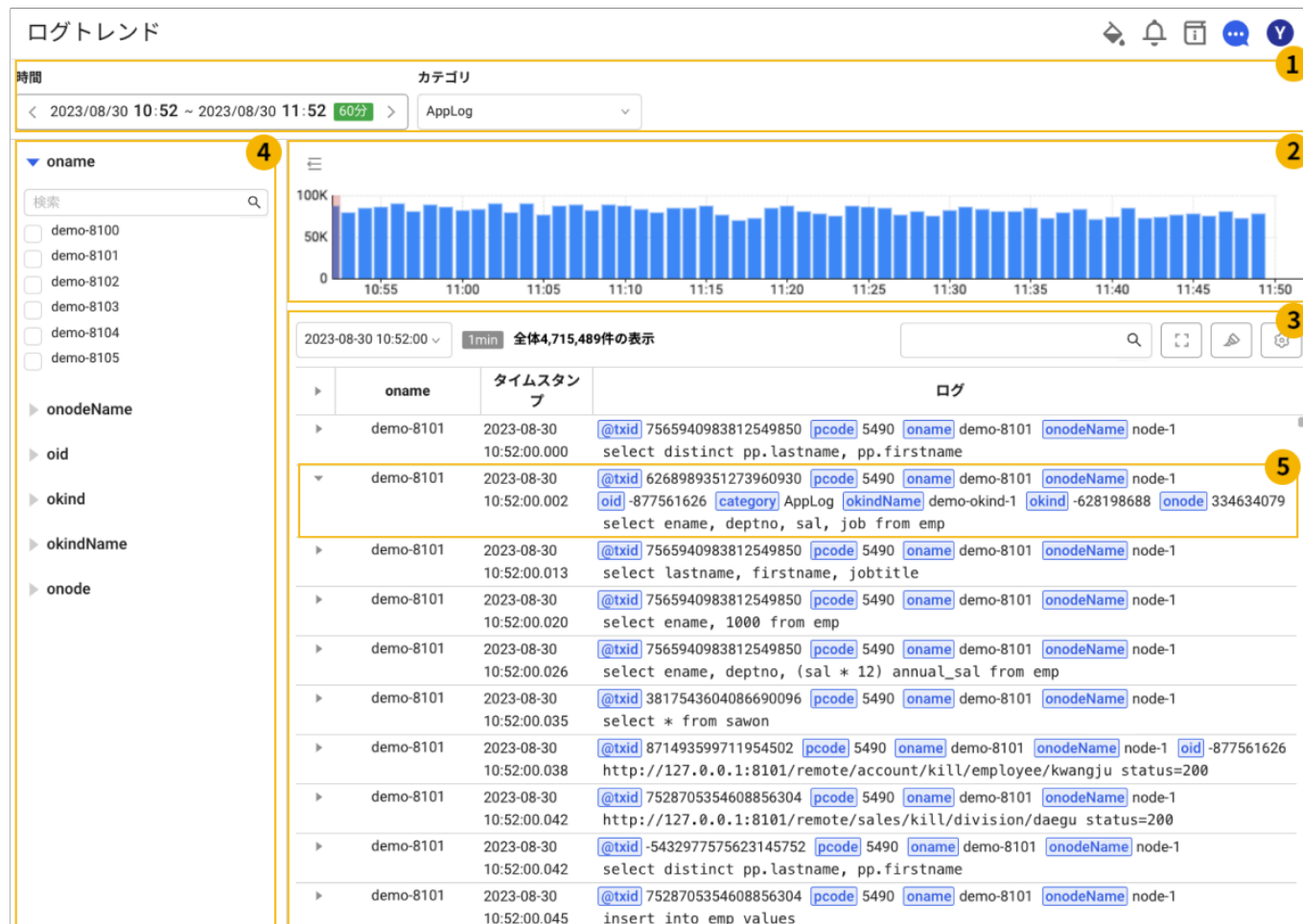
ⓘ ログ参照権限がない場合は、そのメニューにアクセスできません。

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
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
2023-12-18 14:31:02.586	level	error	pcode	2277	agenttime	1702877462043	oid	778873916	category	AppServer	event_status	error
2023-12-18 14:31:02.586	level	error	pcode	2277	agenttime	1702877462057	oid	778873916	category	AppServer	event_status	error
2023-12-18 14:31:02.586	level	error	pcode	2277	agenttime	1702877462081	oid	778873916	category	AppServer	event_status	error
2023-12-18 14:31:02.586	level	error	pcode	2277	agenttime	1702877462087	oid	778873916	category	AppServer	event_status	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、パースされたキーワードの中で level 、 type 基準で判別します。 level 、 type にパースされたキーが存在し、パースの値がFATAL、CRITICAL、ERROR、WARN、WARNING、INFOを含む場合は、ログレベルの色を表示します。

- ❗ ログテーブルカラムの端をドラッグしてカラムの幅を修正できます。

個人情報の照会

ログの個人情報照会権限がある場合個人情報の表示  トグルボタンの活性化を通じて非識別化処理した個人情報を表示することができます。

- ❗ ログの個人情報照会権限についての詳細は次の文書を参照してください。
- ログ個人情報の非識別化機能についての詳細は次の文書を参照してください。

ログContentの確認

Content はログメッセージです。ログカラムの1行目には、パースされたキーと値が表示され、2行目にはContent（ログメッセージ）が表示されます。

- **3** ログテーブルの行(ログ)ごとに ▶ 詳細ボタンがあります。 ▶ 詳細ボタンを選択すると **5** のように、ログの全体 contentを確認できます。

ハイライト設定

目的のキーワードを簡単に識別できるように、ハイライト機能を提供しています。🔍 アイコンをクリックし、キーワードを入力してからEnterキーを押して追加してください。

コンテンツハイライト

ログのコンテンツ内で目的のキーワードを簡単に識別できるよう、ハイライト機能を提供します。単一または複数のキーワードでフィルタリングできます。

1. ハイライトしたいキーワードをキーワード入力欄に入力します。
 - 例: `select`
2. 検索したキーワードがログリストのContent内でハイライト表示されます。
 - **[] 拡大表示** アイコンをクリックすると、**ログ** と **タイムスタンプ** を全画面で確認できます。
 - ハイライトされたキーワード間の移動はショートカットで操作できます。
 - `Enter` : 次の行へ移動
 - `Shift+Enter` : 前の行へ移動
 - `^ / v` アイコン: 行の移動
 - `Cmd + F (Mac) / Ctrl + F (Windows)`: キーワード検索

複数キーワード条件

複数キーワードでハイライトする場合は、次のように作成します。

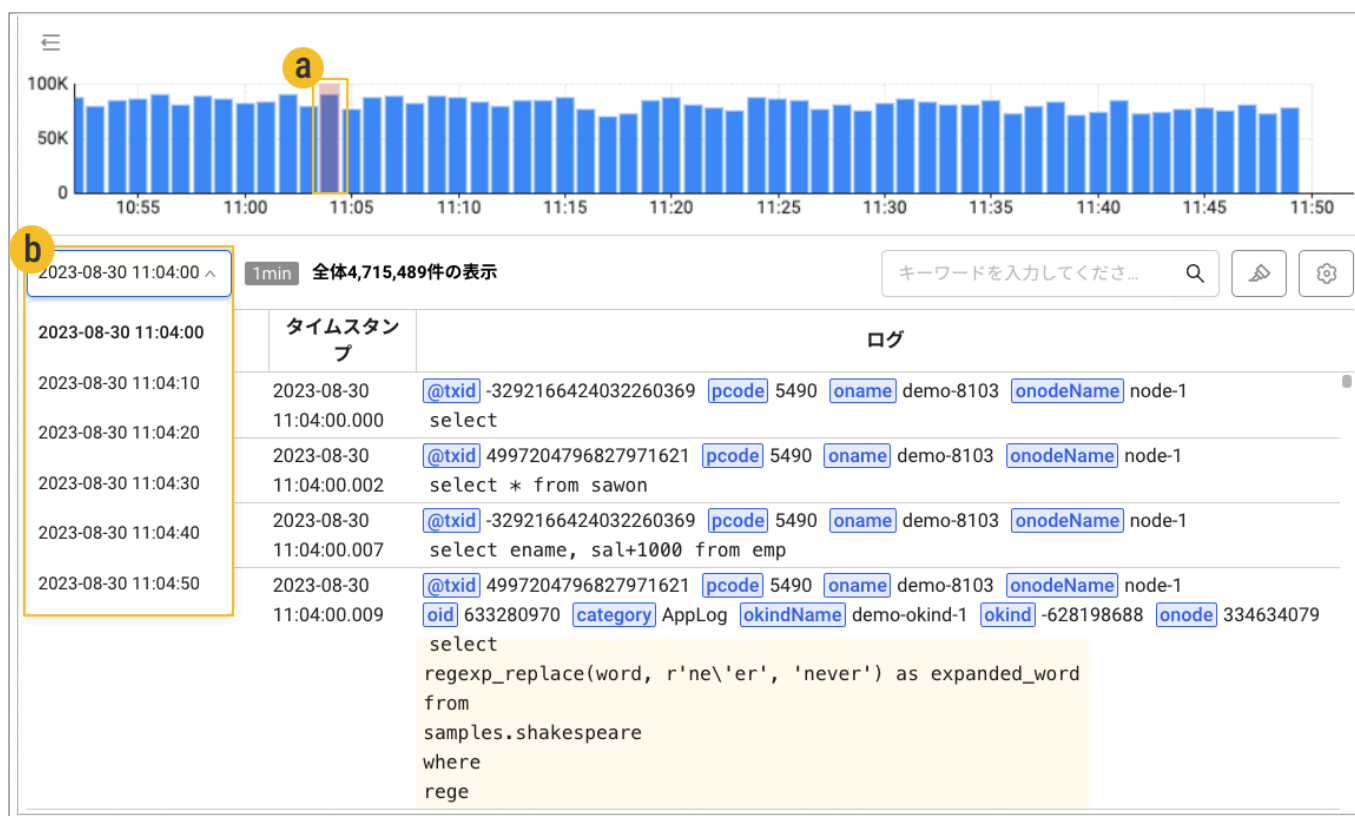
入力文字列	説明	結果
a b c	各キーワードをスペースで区切ります。	a, b, c
"Whatap is good."	キーワードにスペースを含める場合は、" または "" で囲みます。	Whatap is good.
"Whatap\\ is good."	""で囲まれたキーワードに、\ を含める場合は、\\ と入力する必要があります。	Whatap\\ is good.

ハイライトカラー設定

ハイライトするキーワードおよび色を設定できます。

- デフォルトでは、ログレベルに応じたハイライト（FATAL、ERROR、WARN、SEVERE、CRITICAL）が適用されています。
- 設定した内容はプロジェクト単位で保存されます。
 -  アイコンをクリックします。
 - ハイライト ウィンドウで、色を設定するキーワードを入力欄に追加してください。
 - 入力欄の左側の色をクリックすると、色を選択できます。

ログをチャートで検索



- バーチャートで **a** 目的の時間領域バーをクリックまたはドラッグして、その時間範囲のログを確認できます。
- 棒チャートの下ログテーブル上部左側の **b** 時間選択オプションを使用して、次のように選択した時間帯でより詳細なログ検索が可能です。
 - 1min : interval (チャート内の棒の間隔)
 - 時間選択オプション : 選択された時間範囲を6つの間隔に分割した時間帯

テーブル設定

カラム設定

3 領域の右で  **カラム設定** ボタンを選択します。カラムを追加したり、順序を設定できます。

- **カラム追加**

タグを選択してテーブルにカラムを追加できます。**log**カラム選択を解除する場合**ログ表示詳細設定**が確認できません。必ず1つ以上のカラムを選択します。

- **カラム順序設定**

カラムを追加すると**表示項目**に該当カラムが追加されます。希望のカラムをドラッグしてカラムの順序を変更します。

ログ表示詳細設定

3 領域右で  **ログ表示詳細設定** ボタンを選択します。デフォルトで**content**、**タグ**すべてチェックされており、両方の項目を表示します。**content**と**タグ**どちらかは必ず選択します。

チェックが解除されたアイテムはテーブルに表示されません。次のように**タグ**を解除する場合、テーブルでログの**タグ**は表示されません。

ログテーブルコンテンツタグ非表示

タグ管理一覧にタグを追加すると、追加した順にログのタグがソートされます。タグの順序はドラッグして変更できます。追加したタグを無効にすると、無効にしたタグはログのタグに表示されません。

ⓘ カラムおよびログ表示設定の適用範囲

- **カラム設定**と**ログ表示詳細設定**は、**ログTail**、**ログ検索**、**ログトレンド**で使用できます。
- 同一プロジェクト内の**ログTail**、**ログ検索**、**ログトレンド**は、**カラム設定**と**ログ表示詳細設定**を共有します。

ログファイルのダウンロード

検索したログの結果を **CSV** または **TXT** ファイル形式でダウンロードできます。

1. 画面中央右側の **↓ ダウンロード** ボタンをクリックします。
2. **CSVダウンロード** または **Logダウンロード** をクリックして、希望の形式のファイルをダウンロードします。

ログの検索

ⓘ ログ参照権限がない場合は、そのメニューにアクセスできません。

ホーム画面 > プロジェクト選択 > ログ > ログ検索

ログ検索メニューから収集された大量のログをさまざまな条件で検索し、ユーザーが必要なログを指定できます。複数の検索条件をパーシングされたキーとバリューで指定できるため、目的の条件に一致するログデータのみを抽出します。

動的ページで取得したログデータは、設定された行単位で取得され、スクロールで画面の下まで移動すると自動的に次のデータが取得されて表示されます。

主な用語は次のとおりです。

- **Category**：ログの収集および照会単位
- **Content**：ログメッセージ
- **Search Key**：ログパーサーの設定によって生成される検索キー
- **Tag**：収集されたログを検索できるタグ

1 ログ検索

時間 2023/08/30 11:28 ~ 2023/08/30 12:28 60分

フィルター ① category AppLog フィルターを入力してから「Enter」キーを押して追加します。 category == AppLog

2

3 全体4,424,485件の中、9999+件が検索条件に合致します。 過去 最近 タグを表示 キーワードを入力してください。

4

▶	oname	タイムスタンプ	ログ
▶	demo-8102	2023-08-30 11:28:00.003	@txid -8737177787317841782 pcode 5490 oname demo-8102 onodeName node-0 select productid, specialofferid, avg(unitprice) as [average price],
▶	demo-8102	2023-08-30 11:28:00.012	@txid 8009922019355005360 pcode 5490 oname demo-8102 onodeName node-0 select distinct pp.lastname, pp.firstname
▶	demo-8102	2023-08-30 11:28:00.008	@txid -8737177787317841782 pcode 5490 oname demo-8102 onodeName node-0 select ename, sal+1000 from emp
▼	demo-8102	2023-08-30 11:28:00.017	@txid -8737177787317841782 pcode 5490 oname demo-8102 onodeName node-0 oid 1387800924 category AppLog okindName demo-okind-0 okind -1383513482 onode 1693789385 select e.ename ' departments's name is:' d.dname from emp e, dept d where e.deptno=d.deptno
▶	demo-8102	2023-08-30 11:28:00.017	@txid 5677524395951858637 pcode 5490 oname demo-8102 onodeName node-0 http://127.0.0.1:8102/remote/account/kill/division/daegu status=200
▶	demo-8102	2023-08-30 11:28:00.019	@txid 8009922019355005360 pcode 5490 oname demo-8102 onodeName node-0 select ename, sal=sal+1000 from emp
▶	demo-8102	2023-08-30 11:28:00.030	@txid 8009922019355005360 pcode 5490 oname demo-8102 onodeName node-0 select employeeid, lastname, salary
▶	demo-8102	2023-08-30 11:28:00.025	@txid 8009922019355005360 pcode 5490 oname demo-8102 onodeName node-0 select productid, sum(linetotal) as total
▶	demo-8102	2023-08-30 11:28:00.033	@txid -8302816252130563957 pcode 5490 oname demo-8102 onodeName node-0 http://127.0.0.1:8102/remote/order/delete/dept/jeju status=200
▶	demo-8102	2023-08-30 11:28:00.041	@txid 8009922019355005360 pcode 5490 oname demo-8102 onodeName node-0 select pp.lastname, pp.firstname, e.jobtitle
▶	demo-8102	2023-08-30 11:28:00.036	@txid 8009922019355005360 pcode 5490 oname demo-8102 onodeName node-0 select * from emp

AppLog (4,404,050)
AppLog @txid oid okind okindName oname onode onodeName

AppStdErr (438)
AppStdErr @txid oid okind okindName oname onode onodeName

AppStdOut (19,489)
AppStdOut oid okind okindName oname onode onodeName

データ参照

- 画面の下までスクロールすると、次のデータを検索します。一度に、10,000個のログを参照できます。
- 3 ログテーブルの左上に検索されたログの総数を確認することができます。
- ログデータを時間の順と逆順で照会できます。3 ログテーブルの右上の古い順と新しい順の中から照会方式を選択します。
- 時間範囲を指定した後適用ボタンを選択して照会時間を設定し、🔍 検索ボタンを選択してデータを照会します。
- 3 ログテーブルの右上の🔍 拡大表示アイコンを選択すると、ログとタイムスタンプを全画面で確認できます。
- エージェントオプションが設定されている場合、ログレベルを収集し、各ログの左側に色付きの縦線が次のように表示されます。

2023-12-18 14:31:02.563	INFO	2277	1702877462042	778873916	AppLog	io.home.test.logback02starter.base.web.LogbackControllerGreeting	
INFO log in our greeting method.							
2023-12-18 14:31:02.563	WARN	2277	1702877462043	778873916	AppLog	io.home.test.logback02starter.base.web.LogbackControllerError	http-nio-19090-exec-2
io.home.test.logback02starter.base.errors.exception.ApiException: [2204] Process failure. Please try again.							
2023-12-18 14:31:02.586	error	2277	1702877462043	778873916	AppServer	Servlet.service() for servlet [dispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.errors.exception.ApiException: [2204] Process failure. Please try again.]	level
2023-12-18 14:31:02.586	error	2277	1702877462057	778873916	AppServer	Servlet.service() for servlet [dispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.errors.exception.ApiException: [2204] Process failure. Please try again.]	level
2023-12-18 14:31:02.586	error	2277	1702877462081	778873916	AppServer	Servlet.service() for servlet [dispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.errors.exception.ApiException: [2204] Process failure. Please try again.]	level
2023-12-18 14:31:02.586	error	2277	1702877462087	778873916	AppServer	Servlet.service() for servlet [dispatcherServlet] in context with path [] threw exception [Request processing failed: io.home.test.logback02starter.base.errors.exception.ApiException: [2204] Process failure. Please try again.]	level

① エージェントのオプション設定

```
# whatap.conf
weaving=log4j-2.17
weaving=logback-1.2.8
```

- Javaエージェント2.2.22バージョンからウィービング設定にlog4j-2.17またはlogback-1.2.8設定時に使用できます。エージェントの再起動が必要です。
- ログレベルは、パースされたキーワードの中で level 、 type 基準で判別します。 level 、 type にパースされたキーが存在し、パースの値がFATAL、CRITICAL、ERROR、WARN、WARNING、INFOを含む場合は、ログレベルの色を表示します。

① ログテーブルカラムの端をドラッグしてカラムの幅を修正できます。

ログContentの確認

Content はログメッセージです。ログカラムの1行目には、パースされたキーと値が表示され、2行目にはContent（ログメッセージ）が表示されます。

- ③ ログテーブルの行(ログ)ごとに ▶ 詳細ボタンがあります。 ▶ 詳細ボタンを選択すると ④ のように、ログの全体Contentを確認できます。
- ログのタグを選択すると、コピー、検索、除外検索、隣接ログを検索できるドロップダウンメニューが表示されます。

フィルター

フィルター適用

① 左側の**時間選択バー**で時間範囲を指定できます。右側から、フィルターを適用すると、入力した条件に合ったログをフィルタリングします。複数のフィルターを入力できます。フィルターのタグが同じ場合、OR(||)、そうでない場合はAND(&&)が適用されます。

入力欄に文字を直接入力するか、**フィルター**入力欄をクリックしてフィルターを指定します。フィルタータグは **検索キー**、**オペレーター**、**検索値** の順に入力します。🔍 **検索** ボタンを選択すると、フィルターが適用されたデータをログ一覧で確認できます。

❗ ガイドUI

次のように入力ウィンドウの下に**ガイドUI**を提供します。入力画面またはフィルタータグにマウスカーソルがある場合、**ガイドUI**を閉じる時はESCキーで操作できます。



検索キー、オペレーター、検索値の入力

- **検索キー** 入力時、一般インデックス、予約語インデックス、数字のみ入力できるインデックスを区分して推奨値を提供します。
- **オペレーター** 入力時、一般インデックス検索キーの場合は、`==`、`!=` オプションが下に表示されます。数字のみ入力できるインデックスの場合、`>`、`<`、`<=`、`>=`、`==`、`!=` オプションを提供します。
- **検索値** 入力時の一致検索(`>`、`<`、`<=`、`>=`、`==`)の時は青色で、除外検索(`!=`)の時は赤色でハイライトします。 **検索値** 入力時に大文字と小文字の区分オプションを活用して検索することができます。

- ① フィルタータグが2行以上長くなる場合へ **折りたたみ**アイコンを選択して折りたたむことができます。
- フィルタータグを入力した後、入力画面でShiftとTabキーを同時に使用して、以前のフィルタータグに移動できます。
- フィルタータグを入力した後、入力画面でTABキーを通じて次のフィルタータグに移動できます。

フィルタータグ追加

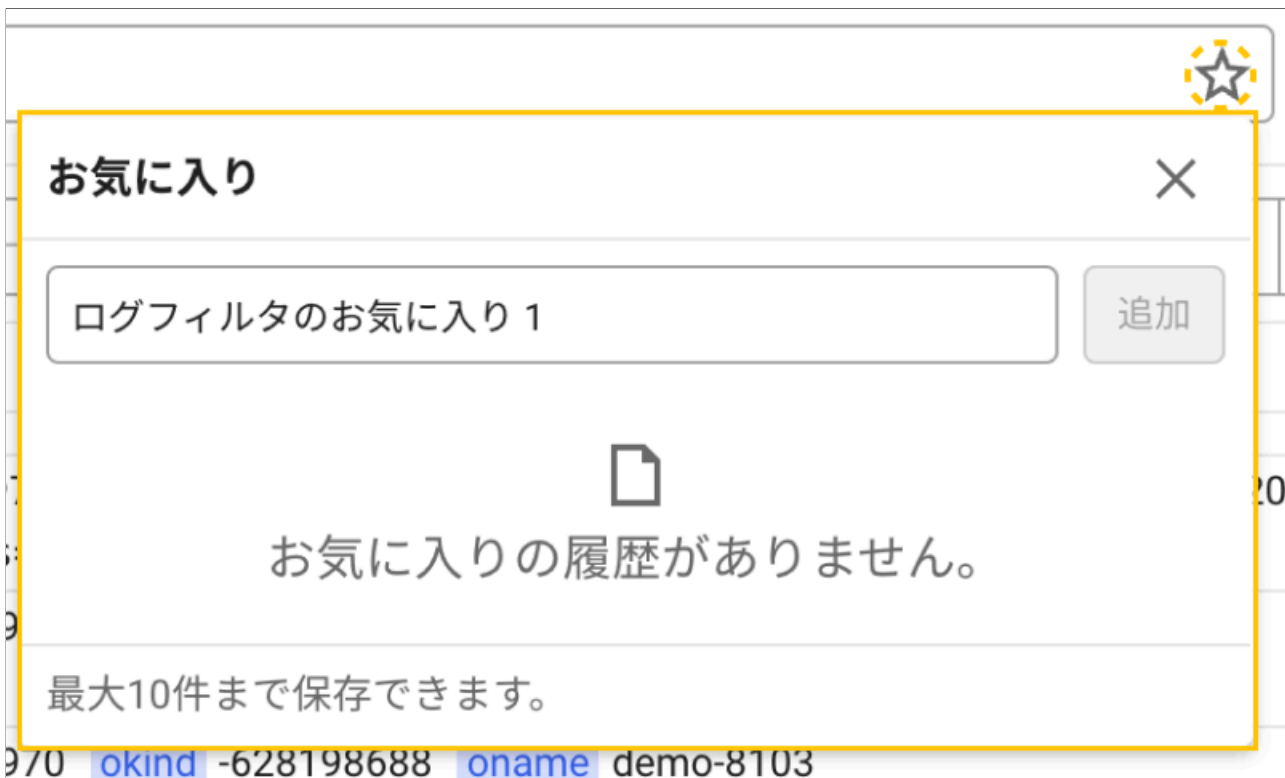
入力フィールドにテキストを入力し、Enter または Tab キーを押すか、入力欄下のガイド UI で推奨値をクリックまたは矢印キーで選択して追加できます。

フィルタータグの削除

単一のタグを削除するには、**Backspace** キーを押すか、タグ上の **X** アイコンをクリックします。すべてのタグを一度に削除するには、入力フィールド右側の **X** アイコンをクリックします。

フィルターのお気に入り

フィルターお気に入り機能を提供します。入力画面の右側にある ☆ お気に入り アイコンを選択して、目的のフィルター検索条件をお気に入りに追加、削除および既存のお気に入りを選択できます。お気に入りは最大50個まで保存されます。



フィルター適用の例外状況

- 数字のみ入力できるインデックス(.n で終わる 検索キー)を入力したタグで、 検索値 は数字のみ入力できます。
- 重複した 検索キー 、 検索値 は入力できません。
- 検索キー 、 検索値 いずれかのタグが存在しない場合は、検索できません。有効でないタグの場合、灰色と表示します。

構文解析されていないキーワードのフィルター適用

ログからパーシングされていない、つまりインデックスが作成されていないキーワードを含むログを照会できます。この場合、指定範囲内のすべてのログをFull Scanします。そのため、インデックスが生成されたキーに比べて検索速度が多少落ちる可能性があります。定型化されたログデータの場合、**ログパーサの設定**を通じてインデックスキーを活用した検索をお勧めします。

フィルター ⓘ

🔍 content == *select* ✕

フィルターを入力してから「Enter」キーを押して追加

✕

content == *select*

1. **カテゴリ**を選択します。カテゴリ指定が必須です。
2. **フィルター**入力欄に **content** を選択後、検索キーワードを入力します。
例) content *select*
3. 🔍 **検索**ボタンをクリックしてログを照会します。ログ全体の一部を先に照会します。1回あたりの検索結果は最大1万件です。
4. スクロールを下げて下段の**追加照会**ボタンを選択すると、つづけて照会できます。



- ❗ 全体ログのうち、サーバー照会範囲当たり1万件ずつ照会します。サーバー照会範囲の場合、基本20万件ですが、ログ全体の量によって比率が変わることがあります。
- パーサ設定の詳細については、[次の文書](#)を参考にしてください。

フィルター修正

フィルターに値を入力し、入力した値をクリックすると、その値を修正できます。

フィルター ⓘ

🔍 oname == ote-account × key == aws.base:index × appender != fileAppender × フィルターを入力してから「Enter」キーを押して追加 ×

☐ 大小文字を区別する

fileAppender

searchValue*	検索値で始まるログを検索します。 ex key!=searchValue*
*searchValue	検索値で終わるログを検索します。 ex key!=*searchValue
searchValue	検索値を含むログを検索します。 ex key!=*searchValue*
*search*Value*	検索値を含むログを検索します。 ex key!=*search*Value*
re:searchValue	正規表現に一致するログを検索します。 ex key!=re:searchValue
**	検索語に該当するすべてのログを検索します。 ex key!=**

key == value 一致 key != value 除外 key == value 無効なタグです。 ⓘ ガイド表示

- ・ フィルター入力欄にテキストを書き換えて修正できます。
- ・ フィルター入力欄の下に表示されるガイドUIから推奨値を選択して修正できます。

検索キー(Search Key)

検索キーは、ログデータ内で希望する特定の値にアクセスするための識別子を意味します。検索キーに該当する実際のデータが検索値です。左側の②領域のタグはカテゴリ別にパーシング(parsing)された検索キーです。タグを選択してフィルターを入力します。オレンジ色タグはカテゴリで、青色タグは検索キーです。

例えば②領域のAppLogとAppStdOutはカテゴリであり、その下のoidなどのタグは、パーシング(parsing)された検索キーです。検索キーはログ>ログ設定のログパーサの設定タブでパーシングロジックを登録し、設定できます。

フィルター入力文法

タグは検索キーと検索値で構成されています。次の例で、検索キーは `exception`、検索値は `UnknownHostException` となります。この例は、収集したログデータのうち、IPアドレスとドメインアドレスが一致せず、サーバーをホストに接続できない場合に発生する例外(`UnknownHostException`)が含まれたログデータを照会します。

exception == UnknownHostException

×

検索キーの種類

検索キーの種類	検索キーフォーマット	意味	検索キーと検索値の例	検索例
文字列キーワード	keyword	ファイル名	- キー: fileName - 値: /data/whatap/logs/yard.log	fileName:/data/whatap/logs/yard.log
数字キーワード	keyword.n	レスポンス時間	- キー: response_time.n - 値: 2945	response_time.n>=2945
予約語キーワード (辞書定義キーワード)	@keyword	TXID	- キー: @txid - 値: 85459614215434144	-

共通文法

文法の種類	説明	例
<code>==searchValue</code>	検索値と一致するログを検索します。	<code>exception==RuntimeExceptionexception</code>
<code>!=searchValue</code>	検索値を除いたログを検索します。	<code>exception!=RuntimeException</code>
<code>*searchValue</code>	検索値で終わるログを検索します。	<code>word==*hello</code>
<code>searchValue*</code>	検索値で始まるログを検索します。	<code>word==hello*</code>
<code>*searchValue*</code>	検索値として中間に含まれるログを検索します。	<code>word==*hello*</code>
<code>*search*Value*</code>	検索値として含まれるログを検索します。	<code>word==*he*llo*</code>

文法の種類	説明	例
re:{正規表現}	正規表現にマッチングされるログを検索します。	caller==re:^i\.w\.a\.w\.s\.v\.r\.
**	検索語に該当するすべてのログを検索します。	

検索キーが数字キーワード(keyword.n)の場合の文法

次の文法は検索キーが、`keyword.n` 形式の場合のみに対応します。

- 検索値は数字のみ使えます。
- .n キーワードの値にはPrefixを付けません。 .n 以外のキーワードは、すべてPrefixを付ける必要があります。

例) `+>searchValue` は有効ではありません。

文法の種類	説明	例
>searchValue	検索値よりも大きな値を含むログを照会します。	response_time.n>3000
>=searchValue	検索値よりも大きいか、同じ値を含むログを照会します。	response_time.n>=3000
==searchValue	検索値と同じ値を含むログを照会します。	response_time.n==3000
!=searchValue	検索値とは異なる値を含むログを照会します。	response_time.n!=3000
<searchValue	検索値より小さい値を含むログを照会します。	response_time.n<3000
<=searchValue	検索値より小さいか、同じ値を含むログを照会します。	response_time.n<=3000

個人情報の照会

ログの個人情報照会権限がある場合**個人情報の表示**  トグルボタンの活性化を通じて非識別化処理した個人情報を表示することができます。

- ❗ ・ ログの個人情報照会権限についての詳細は[次の文書](#)を参照してください。

- ・ ログ個人情報の非識別化機能についての詳細は次の文書を参照してください。

ログのタグオプション

ログのタグを選択すると、ドロップダウンメニューが表示されます。検索、除外検索、隣接ログ、トランザクション情報オプションが確認できます。

≡

全体90,699件の表示

過去順

最近順

キーワードを入力してください。

🔍

🔗

📄

🏠

⚙️

▶	oname	タイムスタンプ	ログ	
▶	java-demo3	2025-04-17 09:17:13.018	@txid 7759974649447934516 pcode 8 onodeName node-0 oid -278185929 okind 1152715164 oname java-demo3	
			コピー	eException: random exception
▶	java-demo3	2025-04-17 09:17:13.018	検索	demo3 onodeName node-0 agentime 1744849031927 oid -278185929 category AppStdErr okindName dev-okind-0 rtual.web.Simula.exec(Simula.java:79)
▶	java-demo3	2025-04-17 09:17:13.018	除外検索	demo3 onodeName node-0 agentime 1744849031927 oid -278185929 category AppStdErr okindName dev-okind-0
			隣接ログ	ion: java.lang.RuntimeException: random exception
▶	java-demo3	2025-04-17 09:17:13.018	トランザクション...	demo3 onodeName node-0 agentime 1744849031928 oid -278185929 category AppStdErr okindName dev-okind-0 rtual.web.VExec.doFilter(VExec.java:16)

ログタグ オプション メニュー	説明
コピー	該当するタグのログをコピーします。
検索	フィルターには、該当のタグを含む ('==') 条件で入力されます。
除外検索	フィルターには、該当のタグを除外する ('!=') 条件で入力されます。
隣接ログ	隣接ログの詳細画面では、選択したログのサーバーを対象に、選択したログと隣接する時間帯のログを照会できます。時間を選択して、周辺の時間帯に発生したログを確認することも可能です。基準となるログは青い背景で表示されます。
トランザクション 情報	ログに @txid や @mtid タグが含まれている場合は、トランザクション情報をクリックすると、トランザクション情報の詳細画面で内容を確認できます。

コンテンツハイライト

ログのコンテンツ内で目的のキーワードを簡単に識別できるよう、ハイライト機能を提供します。単一または複数のキーワードでフィルタリングできます。

1. ハイライトしたいキーワードをキーワード入力欄に入力します。
 - 例: `select`
2. 検索したキーワードがログリストのContent内でハイライト表示されます。
 -  **拡大表示** アイコンをクリックすると、**ログ** と **タイムスタンプ** を全画面で確認できます。
 - ハイライトされたキーワード間の移動はショートカットで操作できます。
 - `Enter` : 次の行へ移動
 - `Shift+Enter` : 前の行へ移動
 - `↑ / ↓` アイコン: 行の移動
 - `Cmd + F` (Mac) / `Ctrl + F` (Windows): キーワード検索

複数キーワード条件

複数キーワードでハイライトする場合は、次のように作成します。

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

ハイライトカラー設定

ハイライトするキーワードおよび色を設定できます。

- デフォルトでは、ログレベルに応じたハイライト（**FATAL**、**ERROR**、**WARN**、**SEVERE**、**CRITICAL**）が適用されています。
- 設定した内容はプロジェクト単位で保存されます。
 -  アイコンをクリックします。
 - ハイライト ウィンドウで、色を設定するキーワードを入力欄に追加してください。
 - 入力欄の左側の色をクリックすると、色を選択できます。

テーブル設定

カラム設定

3 領域の右で  **カラム設定** ボタンを選択します。カラムを追加したり、順序を設定できます。

- カラム追加

タグを選択してテーブルにカラムを追加できます。logカラム選択を解除する場合**ログ表示詳細設定**が確認できません。必ず1つ以上のカラムを選択します。

- カラム順序設定

カラムを追加すると**表示項目**に該当カラムが追加されます。希望のカラムをドラッグしてカラムの順序を変更します。

ログ表示詳細設定

3 領域右で  **ログ表示詳細設定** ボタンを選択します。デフォルトで**content**、**タグ**すべてチェックされており、両方の項目を表示します。**content**と**タグ**どちらかは必ず選択します。

チェックが解除されたアイテムはテーブルに表示されません。次のように**タグ**を解除する場合、テーブルでログの**タグ**は表示されません。

ログテーブルコンテンツタグ非表示

タグ管理一覧にタグを追加すると、追加した順にログのタグがソートされます。タグの順序はドラッグして変更できます。追加したタグを無効にすると、無効にしたタグはログのタグに表示されません。

ⓘ カラムおよびログ表示設定の適用範囲

- カラム設定とログ表示詳細設定は、ログTail、ログ検索、ログトレンドで使用できます。
- 同一プロジェクト内のログTail、ログ検索、ログトレンドは、カラム設定とログ表示詳細設定を共有します。

ログファイルのダウンロード

検索したログの結果を CSV または TXT ファイル形式でダウンロードできます。

1. 画面中央右側の  ダウンロード ボタンをクリックします。
2. CSVダウンロード または Logダウンロード をクリックして、希望の形式のファイルをダウンロードします。

ログの設定

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。

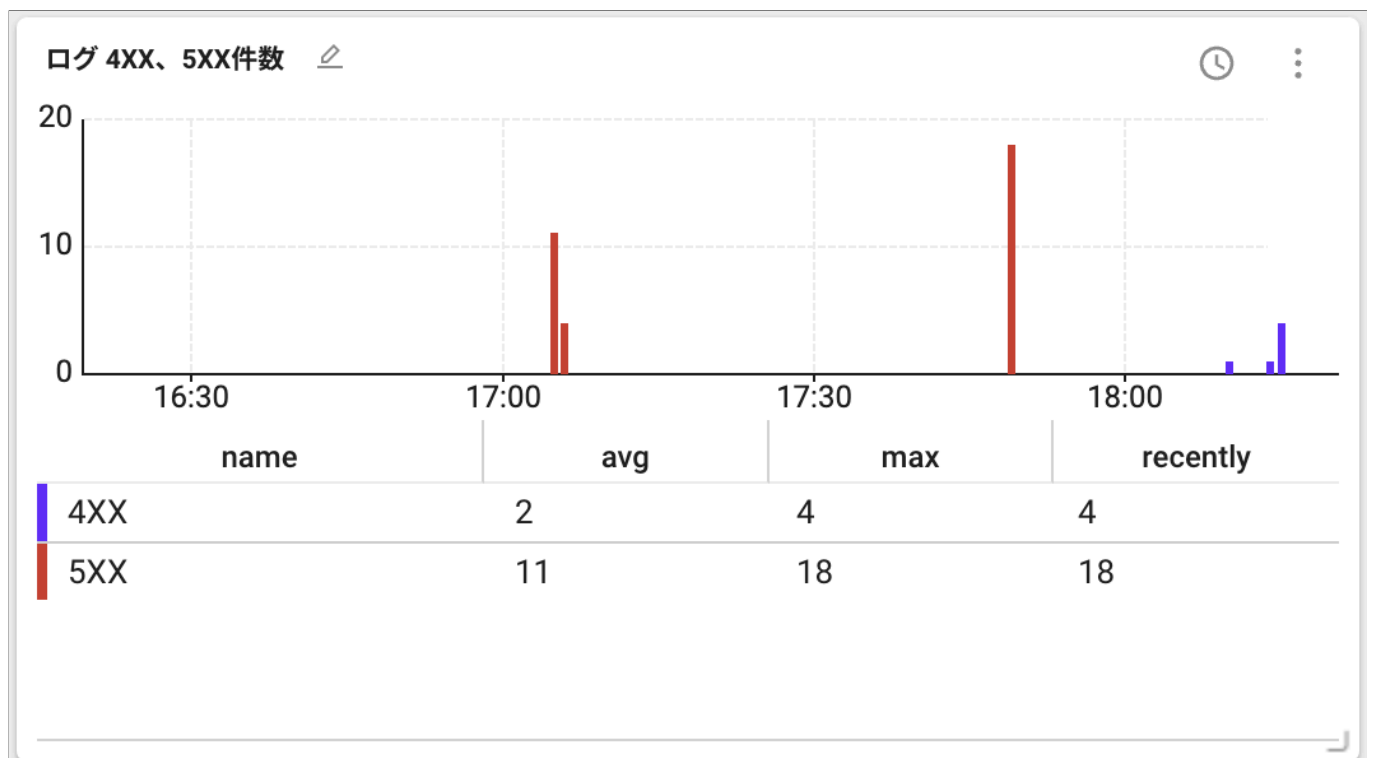
ウィジェットテンプレート

⇒ 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

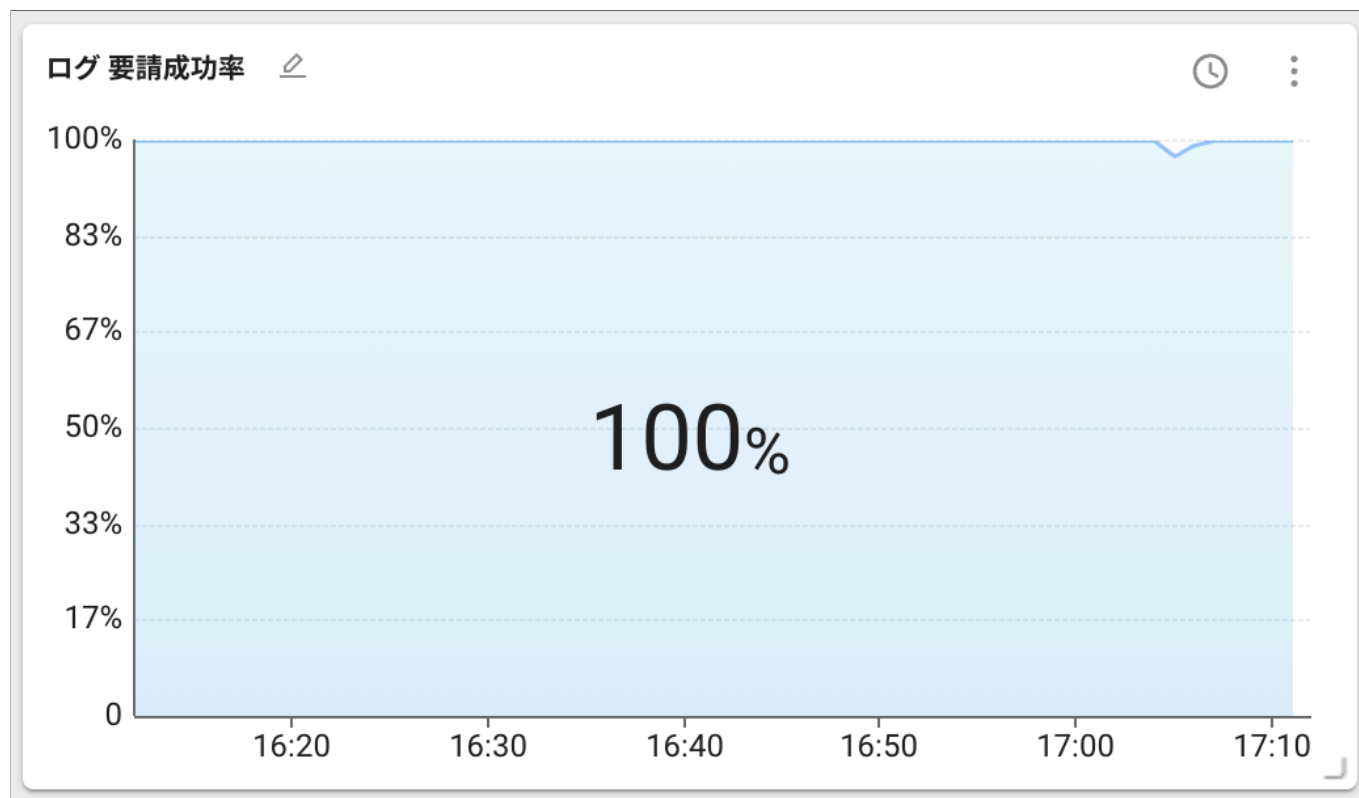
成功率

🔍

📉

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。

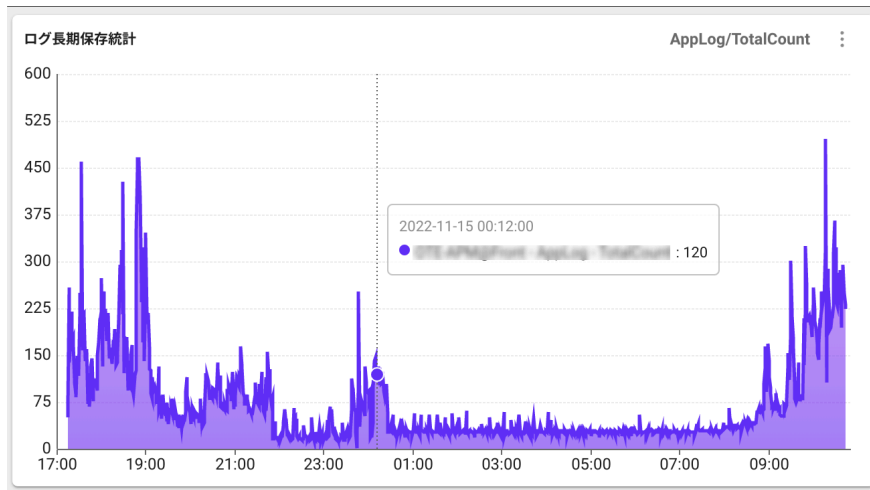
該当ウィジェットに表示するデータ収集のためにはログ長期保存統計 設定が必要です。

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		
☒	VirtualLog	status		
☒	AppLog	agenttime		

- 非識別化処理された検索キーの場合、ログコンテンツ内の **検索キー.pii** 形式で出力されます。
- 個人情報の非識別化一覧内の活性化カラムで非識別化項目を ☒ 活性化にできます。
- 個人情報の非識別化一覧内の編集カラムで 修正及び 除去できます。

- ✔ **ログプライマリパーサ設定**タブで検索キー名を **検索キー.p** に指定すると、非識別化対象として自動登録されます。自動登録された項目は**個人情報の非識別化**タブで**カテゴリ**選択後、**指定された検索キー**で確認または解除できます。

パーサーで .p 接尾辞を指定する方式よりも、**個人情報の非識別化**タブで直接設定することを推奨します。

個人情報の表示

非識別化されたデータは**ログTail**、**ログトレンド**、**ログ検索メニュー**でマスキング状態で表示されます。**ログの個人情報照会権限**のあるユーザーはログ一覧内の**個人情報の表示** ☒ ボタンをクリックすると元のデータを確認できます。

▼	java-demo2	2024-12-16 16:06:49.988	area river privacy true status.pii *** pcode 8 city seoul onodeName node-0 myname.p *** oid -1737750367 okind 1152715164 price.n 12000 oname java-demo2 age.n 33 agenttime 1734332809555 category VirtualLog okindName dev-okind-0 onode 1693789385 You need not love me, if you choose not to.
▶	java-demo1	2024-12-16 16:06:49.993	area mountain privacy true status.pii *** pcode 8 city junju onodeName node-1 myname.p **** Waiting does not have to aim for a meeting.
▼	java-demo2	2024-12-16 16:06:49.988	area river privacy true status.pii 500 pcode 8 city seoul onodeName node-0 myname.p lee oid -1737750367 okind 1152715164 price.n 12000 oname java-demo2 age.n 33 agenttime 1734332809555 category VirtualLog okindName dev-okind-0 onode 1693789385 You need not love me, if you choose not to.
▶	java-demo1	2024-12-16 16:06:49.993	area mountain privacy true status.pii 200 pcode 8 city junju onodeName node-1 myname.p hong Waiting does not have to aim for a meeting.
▶	java-demo6	2024-12-16 16:06:50.064	area sea privacy true status.pii 200 pcode 8 city daegu onodeName node-1 myname.p song Waiting does not have to aim for a meeting.

❗ **個人情報の非識別化タブ**で指定した検索キーは、ログメニュー内のログコンテンツから **検索キー.pii** 形式で表示されます。

例: **status.pii** 例 ***

ログの個人情報の非識別化点検

❗ **ログ個人情報の非識別チェック機能**を通じて既存のデータを置き換える場合、そのデータは元に戻すことができません。

ログ個人情報の非識別チェックは既存のログデータ内の個人情報を識別し、ユーザーが指定した**置換値**に置き換えます。

対象キー指定による置換

対象キーを指定すると、該当キーに保存された値のみを置換し、残りのログ内容はそのまま維持します。対象キーはログの **field** 値と **tag** 値の両方に適用されます。対象キーを指定しない場合、従来と同様にログコンテンツ全体から個人情報を識別して置換します。

❗ 置換は保存されたログデータにのみ適用されます。検索インデックスには、置換後も元の値が残っている場合があります。

対象キーは、ログ個人情報の非識別化点検フォームの**対象キー**入力欄で指定し、画面では **field** と **tag** を区別せず、1つの対象キーとして入力します。

ログ個人情報の非識別チェック

収集されてあるログを非識別化します。

☒ チェック履歴の確認

時間 < 2025/03/21 12:26 ~ 2025/03/21 13:26 1時 カテゴリ VirtualLog 個人情報項目 個人識別番号 個人情報パターン (?<!\w)\d{2}(0[1-9] 1[0-2])([0-2][0-9] 3[0-1]){1-4}\d{6}(?!w) 置換の適用有無 ☐ 置換値 ***** チェック開始 チェック中止	カテゴリ VirtualLog 検索開始時刻 2025/03/21 12:26 検索終了時刻 2025/03/21 13:26 個人情報項目 個人識別番号 個人情報パターン (?<!\w)\d{2}(0[1-9] 1[0-2])([0-2][0-9] 3[0-1]){1-4}\d{6}(?!w) 置換値 ***** パターンのマッチング結果 0 ☒ 結果の確認 チェック作業の開始時刻 2025/03/21 13:28 チェック作業の終了時刻 2025/03/21 13:28 置換の適用有無 No チェック作業の結果 SUCCESS
--	--

1. 開始時間と終了時間を設定してください。
2. カテゴリを設定します。
3. 個人情報項目を例の中から選択または直接入力を選択します。

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

4. 置換の適用有無トグルで個人情報が識別された場合、該当情報の置換有無を選択します。
5. 既存のログで正規表現式パターンに識別された文字列を変更する置換値を入力します。

- ❗
- 置換値は元の値より長くしてはなりません。
 - 置換の適用有無トグルの活性化時に、必ず置換値を入力する必要があります。

6. 条件を入力した後、チェック開始ボタンを選択します。

❗ 点検中の場合はいつでもチェック中止ボタンで点検過程を中止できます。

7. 置き換えを適用する時個人情報の非識別チェックの開始確認画面で置き換え入力後確認ボタンをクリックします。

個人情報の非識別チェックの開始



選択した個人情報パターンに一致する値を置き換えます。

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。

 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)	*****_ *****

ログパーシング

ログパーサを使用すると、不規則な形のログをクエリが可能な構造化された形に変更できます。WhaTapログモニタリングは、次の2つのタイプのパーサを提供します。

- **GROKパーサ**：任意の形で収集されるログを正規表現とGROKを活用してパーシングします。
- **JSONパーサ**：JSON形式で収集されるログをパーシングします。

ⓘ 共通の注意事項

- 同じカテゴリに複数のパーサが登録されている場合、最初にマッチングされるパーサのみが適用されます。
- WhaTapはWhaTapサービスの安定性に影響を与えるパーサを無効にする場合があります。。

GROKパーサ

ログが不規則な形で収集される場合、GROKパーサを使用してログをパーシングできます。GROKパターンは、named regular expressionsを提供し、正規表現をより簡単かつ便利に使用できます。

GROKを開始する

GROKは2種類の文法を提供します。

1. `%{SYNTAX:SEMANTIC}`：GROKライブラリーが提供するパターンです。**named regular expressions**を活用してタグを抽出できます。活用例は[次のリンク](#)を参照してください。
 - **SYNTAX**：GROKが提供するnamed regular expressionsを指定します。
 - **SEMANTIC**：マッチングされる値に付ける名前を指定します。

ⓘ named regular expressions

GROKが提供するパターンです。複雑な正規表現に名前を付けて使用できるよう、GROKが提供す

❗ る機能です。

name	regular expression
WORD	<code>\b\w+\b</code>
SPACE	<code>\s*</code>
NOTSPACE	<code>\S+</code>
UUID	<code>[A-Fa-f0-9]{8}-(?:[A-Fa-f0-9]{4}-){3}[A-Fa-f0-9]{12}</code>

WhaTapで提供するすべてのnamed regular expressionsを確認したい場合は、次の[リンク](#)を参考にしてください。

2. `(?<SEMANTIC>REGX)` : 正規表現の**named capturing group**文法です。正規表現を活用して、ユーザーの意図に合わせてタグを抽出できます。活用例は[次のリンク](#)を参照してください。

- **SEMANTIC** : マッチングされる値に付ける名前を指定します。
- **REGX** : マッチングに使用する正規表現を入力します。

❗ named capturing group

正規表現の文法です。

- capturing group: 複数のトークンを1つにまとめて1つのマッチング単位で使用する機能を意味します。
- named capturing group: capturing groupに名前を付けたものです。
- 文字列マッチングの例を見てみましょう。 dev@whatap.io
 - 例1 : `(\w+)@(\w+\.\w+)`
 - 例2 : Eメール全体のマッチング、およびusernameとdomainを追加でマッチングする場合 `(?<username>\w+)@(?<domain>\w+\.\w+)`

%{SYNTAX:SEMANTIC} 活用の例

次は %{SYNTAX:SEMANTIC} を活用する例です。

Sample log

```
[2023-08-08 02:02:30,101 GMT][INFO ][i.w.y.l.c.LogSinkDexScheduleThread.realProcess(159)] 8 VirtualLog 20230808
02:01:00.000 {area=4, city=5} 56ms
```

サンプルログを見て、各単語が意味する内容を推測できます。各部分をsemanticな単語に置き換えると、次のように表現できます。

semantic replace

```
[date][logLevel][caller] projectCode logCategory dexBuildStartTime {area=areaEnum, city=cityEnum} dexBuildElapsed
```

semanticな単語すべて、正規表現に書き換えることができます。GROKパーサを使用すると、事前に定義されたnamed regular expressionsを活用できます。ここで使われた `TIMESTAMP_ISO8601`、`LOGLEVEL`、`DATA` は、GROKが提供するnamed regular expressionsです。これらの値は、それぞれ次の正規表現に置き換えられてマッチングされます。

- name: `TIMESTAMP_ISO8601`
 - regular expression: `%{YEAR}-%{MONTHNUM}-%{MONTHDAY}[T|t]%{HOUR}:%{MINUTE}(:%{SECOND})?%{ISO8601_TIMEZONE}?`
- name: `LOGLEVEL`
 - regular expression: `LOGLEVEL`
`([Aa]lert|ALERT|[Tt]race|TRACE|[Dd]ebug|DEBUG|[Nn]otice|NOTICE|[Ii]nfo|INFO|[Ww]arn(?:ing)?|WARN(?:ing)?|`
`NG)?|[Ee]rr(?:or)?|ERR(?:OR)?|[Cc]rit(?:ical)?|CRIT(?:ICAL)?|[Ff]atal|FATAL|[Ss]evere|SEVERE|EMERG(?:enc`
`Y)?|[Ee]merg(?:ency)?`
- name: `DATA`
 - regular expression: `.*`

GROK parsing pattern

```
\[%{TIMESTAMP_ISO8601:date}\sGMT\]\[%{LOGLEVEL:level}\s\]\[%{DATA:caller}\]
```

上記の内容でパースングすると、次のようにタグを抽出できます。このようにGROKの `%{SYNTAX:SEMANTIC}` パター

ンは、複雑で長い正規表現を簡単に適用できる機能を提供します。

Tag extraction

```
- date : 2023-08-08 02:02:30,101
- caller : i.w.y.l.c.LogSinkDexScheduleThread.realProcess(159)
- level : LEVEL
```

(?<SEMANTIC>REGX) 活用の例

named regular expressionsでマッチングされない部分は (?<SEMANTIC>REGX) パターンを使ってパースできます。上記の[サンプルログ](#)から `%{SYNTAX:SEMANTIC}` パターンだけでパースされない領域は次の通りです。

Unparsed area

```
8 VirtualLog 20230808 02:01:00.000 {area=4, city=5} 56ms
```

該当ログの各部分をsemanticな単語に置き換えると、次のように表現できます。

semantic replace

```
projectCode logCategory dexBuildStartTime {area=areaEnum, city=cityEnum} dexBuildElapsed
```

このように不規則な形の文字列は、次のような (?<SEMANTIC>REGX) パターンを使ってパースできます。

サンプルログパースキーワード別にマッチングされる正規表現

パースキーワード	(?<SEMANTIC>REGX)
8	(?<projectCode>\d)
VirtualLog	(?<logCategory>\w*)
20230808 02:01:00.000	(?<dexBuildStartTime>\d{8}\s\d{2}:\d{2}:\d{2}\.\d{3})
area=4	area=(?<areaEnum>\d)
city=5	city=(?<cityEnum>\d)

パースングキーワード	(?<SEMANTIC>REGX)
56 ms	(?<dexBuildElapsed>\d{2})ms

正規表現の基本文法



文法	意味	別名
<code>?</code>	0 or 1	-
<code>+</code>	1 or more	-
<code>*</code>	0 or more	-
<code>a{5}</code>	exactly 5	-
<code>\w</code>	word character	<code>[a-zA-Z_0-9]</code>
<code>\s</code>	white space	-
<code>.</code>	any character except newline	
<code>[abc]</code>	any of	-
<code>[^abc]</code>	not a,b, or c	-
<code>[a-z]</code>	character between a and z	-
<code>[1-3[7-9]]</code>	union (combining two or more character classes)	-
<code>[1-6&&[3-9]]</code>	intersection (共通集合)	-
<code>[0-9&&[^2468]]</code>	subtraction (差集合)	-
<code>a{2,}</code>	2 or more	-
<code>a{1,3}</code>	between 1 and 3	-



文法	意味	別名
<code>a+?</code>	match as few as possible	-
<code>{2,3}?</code>	match as few as possible	-
<code>(abc)</code>	capturing group (複数の文字列をsingle unitで処理する)	-
<code>\d</code>	digit	<code>[0-9]</code>
<code>\D</code>	non-digit	<code>[^0-9]</code>
<code>\W</code>	non-word character	-
<code>\S</code>	non-white space	-

このようにパースングされたキーワードをスペース(`\s`)と、特殊文字escape(`\{`、`\,`、`\}`)で接続すると、次のようにパターンを適用できます。

GROK parsing pattern

```
(?<projectCode>\d)\s(?<logCategory>\w*)\s(?<dexBuildStartTime>\d{8})\s\d{2}:\d{2}:\d{2}\.\d{3})\s\{area=(?<areaEnum>\d),\scity=(?<cityEnum>\d)\}\s(?<dexBuildElapsed>\d{2})ms
```

上記の内容でパースングすると、次のようにタグを抽出できます。

Tag extraction

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

GROKを適用する

ログ設定 > ログプライマリパーサ設定

1. GROKパターンパーサを適用するには、**ログ設定**メニューの**ログプライマリパーサ設定**タブに移動します。
2. **+ 追加する**を選択した後**パーサ**入力欄で**GROK**パーサを選択します。
3. **パターン登録**ボタンを選択すると、右側にパターン登録とシミュレーション画面が表示されます。
4. **パターン**と**ログ**入力後、**シミュレーション**ボタンをクリックして、適用するパターンでパーシングに成功することを確認します。

パターン 例:

```
[%{TIMESTAMP_ISO8601:date}\sGMT][%{LOGLEVEL:level}\s][%{DATA:caller}]\s(?:<projectCode>\d)\s(?:<logCategory>\d{2}:\d{2}:\d{2}\.\d{3})\s\s{area=(?:<areaEnum>\d),\scity=(?:<cityEnum>\d)\}\s(?:<dexBuildElapsed>\d{2})ms
```

ログ例:

```
[2023-08-08 02:02:30,101 GMT][INFO ][i.w.y.l.c.LogSinkDexScheduleThread.realProcess(159)] 8  
VirtualLog 20230808 02:01:00.000 {area=4, city=5} 56ms
```

5. シミュレーションの成功時**シミュレーション結果**と**性能測定の結果**を照会できます。
6. シミュレーション後、**パターン適用**ボタンをクリックすると、選択したパーサーに入力したパターンが適用されます。
7. パターン適用後、**カテゴリ**と**ログ検出条件**、**パターン**を入力します。

×

パーサ 追加

パーサ*

WhaTap Monitoringには、サービスの信頼性に影響を与える可能性があるパーサーを無効にできる権限があります。

GROK

パーサーパターン*

入力したパターンでログが正常に解析されるかどうかをシミュレートし、パターンを登録します。

成功しました。

```

\[%{TIMESTAMP_ISO8601:date}\sGMT\}\[%{LOGLEVEL:level}\s\}\[%{DATA:caller}\}\s(?<projectCode>\d)\s(?
<logCategory>w*)\s(?<dexBuildStartTime>\d{8}\s\d{2}:\d{2}:\d{2})\s\{area=(?<areaEnum>\d),\scity=(?
<cityEnum>\d)\}\s(?<dexBuildElapsed>\d{2})ms

```

パーサーパターンの修正

カテゴリ*

同じカテゴリに複数のパーサーが登録されている場合、最初に一致するパーサーのみが適用されます。

AppLog

ログ検出条件

フィルタを入力しなかった場合、または検索キー／値を1つだけ入力した場合、そのパターンはすべてのログに適用される。

oname

demo-8100

追加

• カテゴリ

ログカテゴリを選択します。 **カテゴリ**は必須入力項目です。

• ログ検出条件

- 条件を満たすログのみパーサが適用されます。
- 検索キーと検索値を選択するか、直接入力します。
- ログ検出条件は、すべてのパーサが実行される前に適用されます。つまり、パーサの結果として追加されるタグを使用できません。

8. 追加ボタンを選択してパーサを登録します。

- !

 ログパーサー一覧から該当パーサの優先順位を変更するか、**活性化**および**修正**、**削除**できます。
- パーサーシミュレーション後、パターンを登録できます。

267

❗ GROKパーサの注意事項

- GROKパーサは `%{SYNTAX:SEMANTIC}` 、 `%{SYNTAX:SEMANTIC}` 二つのパターンをサポートします。
- `%{SYNTAX:SEMANTIC}` パターンを使用する時、 `SEMANTIC` を必ず入力します。
- `%{SYNTAX:SEMANTIC}` パターンを使用する時、 `SEMANTIC` は一つのパーサの中でユニークである必要があります。
- `(?<SEMANTIC>REGX)` パターンを使用する時、 `SEMANTIC` は文字(a-z、A-Z)、数字(0-9)、および指定された特殊文字(`.` 、 `_` 、 `-`)のみが使えます。
- `SEMANTIC` は文字(a-z、A-Z)で始めなければなりません。
- `SEMANTIC` は文字(a-z、A-Z)または数字(0-9)で終わる必要があります。

GROK追加パターンの選択

GROKパーサのシミュレーション時に、基本パターン(`WORD` 、 `NUMBER` 、 `IP` など)以外に特定のログ形式に合った追加パターンを選択できます。Java、Nginx、MySQLなど32個のパターンタイプが11個のカテゴリにグループ化されて提供されます。

追加パターンカテゴリのドロップダウン

1. パーサのシミュレーション画面で**追加パターン (選択)**領域のドロップダウンをクリックしてください。
2. カテゴリ別にグループ化されたパターンタイプ一覧から、必要なパターンタイプを選択してください。検索入力欄にパターンタイプ名または説明を入力して検索することもできます。
3. 選択したパターンタイプは、シミュレーション時に基本パターンとともにロードされます。

❗ 基本パターン(Core)は常に自動的に含まれます。追加パターンの選択は任意です。

カテゴリ別パターンタイプ一覧

カテゴリ	パターンタイプ
Web Servers	haproxy, httpd, iis, nginx, squid

カテゴリ	パターンタイプ
Application Servers & Frameworks	java, log4j, rails, ruby, springboot
Databases	mongodb, mysql, oracle, postgresql, redis
Cloud	aws
System & Infrastructure	docker, kubernetes, linux-syslog
Messaging & Search	elasticsearch, kafka
Network & Security	bind, bro, firewalls, junos, zeek
Mail	exim, postfix
Monitoring & Backup	bacula, mcollective, nagios
Build Tools	maven

活用例

Tomcat Catalina 8のログをパースングするには、**java**パターンタイプを追加で選択した後、`%{CATALINA8_LOG}` パターンを使用してください。

Sample log

```
31-Jul-2020 16:40:38 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Server version name: Apache Tomcat/8.5.57
```

GROK parsing pattern

```
%{CATALINA8_LOG}
```

Tag extraction

```
- log_timestamp : 31-Jul-2020 16:40:38
- log.level : INFO
```

```
- java.log.origin.thread.name : main
- java.log.origin.class.name : org.apache.catalina.startup.VersionLoggerListener
- log.origin.function : log
- log_message : Server version name: Apache Tomcat/8.5.57
```

パターン詳細表示

選択した追加パターンタイプにどのパターンが含まれているかを詳細画面で確認できます。パターン定義(正規表現)とサンプルログを照会し、シミュレーションにすぐに適用できます。

パターン詳細表示

追加パターンタイプを選択した後、選択されたパターンタイプのタグをクリックすると、右側に詳細画面が開きます。詳細画面はシミュレーションフォームを隠さずに並んで表示されるため、パターン定義を確認しながらシミュレーションを進めることができます。

各パターン項目で次の機能を使用できます。

ボタン	機能	説明
サンプル	サンプルログ入力	該当パターンにマッチングする例ログをシミュレーションパーシングログ入力欄に自動的に入力します。
選択	パターン挿入	<code>%{パターン名}</code> 形式でパターン入力欄に挿入します。該当パターンタイプも自動的に選択されます。
コピー	クリップボードコピー	<code>%{パターン名}</code> 形式をクリップボードにコピーします。

- ① パターン項目をクリックすると、パターン定義(正規表現)が展開されます。複数のパターンを同時に展開して定義を比較できます。
- パターン定義に含まれる `%{PATTERN:field}` 参照は、パターン名、フィールド名、リテラル文字がそれぞれ異なる色で区別されて表示されます。
- サンプルボタンで入力されたログでそのままシミュレーションを実行してパーシング結果を確認できます。

シミュレーションサンプルログの保存

シミュレーションに使用したログは、パーサ設定とともに自動的に保存されます。パーサを修正する際に、以前に使用したサンプルログがシミュレーション画面に自動的に復元され、毎回ログを再入力する必要がありません。

JSONパーサ

ログがJSONフォーマットで収集される場合、JSONパーサを使用して簡単かつ便利にパースングできます。

JSONを適用する

ログ設定 > ログプライマリパーサ設定

1. JSONパターンパーサを適用するには**ログ設定**メニューの**ログプライマリパーサ設定**タブに移動します。
2. **+ 追加する**を選択した後**パーサ**入力欄で**JSON**パーサを選択します。
3. **パターン登録**ボタンを選択すると、右側にパターン登録とシミュレーション画面が表示されます。
4. **パターン**と**ログ**入力後、**シミュレーション**ボタンをクリックして、適用するパターンでパースングに成功することを確認します。

Example

```
2023-08-08 02:43:28,615 -- {"host":"10.21.3.24","method":"POST","status":"200","url":"http://dev.whatap.io/yard/api/flush"} --
```

例のログで**Prefix**と**Postfix**を `--` に指定し、**Ignore**に `url` を指定時 `host`、`method`、`status` 3つ**タグ**のみ生成します。

- **Prefix** ログでJSONフォーマットが開始する場所を指定します。ログ全体がJSONフォーマットの場合は、空の値に設定します。
 - **Postfix** ログでJSONフォーマットが終わる位置を指定します。ログ全体がJSONフォーマットの場合は、空の値に設定します。
 - **Ignore** JSONフォーマットの中でタグを生成しないキーを指定します。
5. シミュレーションの成功時**シミュレーション結果**と**性能測定の結果**を照会できます。

×

パーサ シミュレーション

ガイド表示

パターン

agenttime, category, content, logContent, message, pcode, time, timestamp は予約語です。
予約語はログ検出条件、パターンで登録しても動作しません。

Prefix

-

Postfix

-

Ignore

url

ログ *

ログシミュレーションは必須ですする必要があり、
シミュレーションの結果に応じてパターン登録が必要になる場合があります。

2023-08-08 02:43:28.615 -
{"host":"10.21.3.24","method":"POST","status":"200","url":"http://devote.whatap.io/yard/api/flush"} -
-

シミュレーション

シミュレーション結果 成功しました。

キー	値	結果
method	POST	Ok
host	10.21.3.24	Ok
status	200	Ok

性能測定の結果 成功しました。

シミュレーション数	最小時間(ns)	最大時間(ns)	平均時
1	4,491	4,491	4,491
10	3,322	3,930	3,525
100	2,662	177,949	8,084
1,000	2,654	476,818	4,305
10,000	2,648	311,233	3,823
100,000	2,650	60,522,941	3,713
1,000,000	2,647	44,113,067	3,014

パターン適用

6. シミュレーション後、パターン適用ボタンをクリックすると、選択したパーサーに入力したパターンが適用されます。

7. パターン適用後、カテゴリとログ検出条件、パターンを入力します。

272

×

パーサ 追加

パーサ*

WhaTap Monitoringには、サービスの信頼性に影響を与える可能性があるパーサーを無効にできる権限があります。

JSON

パーサーパターン*

ログが正常に解析されるかどうかをシミュレートします。シミュレーションは必須でなければならず、シミュレーション結果によってはパターン登録がさらに必要になる場合があります。

✔ 成功しました。

Prefix --

Postfix --

Ignore url

シミュレーション検証とパターン修正

カテゴリ*

同じカテゴリに複数のパーサーが登録されている場合、最初に一致するパーサーのみが適用されます。

AppLog

ログ検出条件

フィルタを入力しなかった場合、または検索キー／値を1つだけ入力した場合、そのパターンはすべてのログに適用される。

oname

demo-8100

追加

• カテゴリ

ログカテゴリを選択します。 **カテゴリ**は必須入力項目です。

• ログ検出条件

- 条件を満たすログのみパーサが適用されます。
- 検索キー**と**検索値**を選択するか、直接入力します。
- ログ検出条件**は、すべてのパーサが実行される前に適用されます。つまり、パーサの結果として追加される**タグ**を使用できません。

8. 追加ボタンを選択してパーサを登録します。

- ⓘ ログパーサー一覧から該当パーサの**優先順位**を変更するか、**活性化**および**修正**、**削除**できます。
- パーサを登録する前に**シミュレーション**を通じて登録するパターンが正常であるか確認できます。GROK

273



パーサ登録シミュレーションプロセスと同じです。 [次の文書](#)を参考にしてください。

JSONフォーマット活用例

Sample log

```
{"host":"10.21.3.24","method":"POST","status":"200","url":"http://dev.whatap.io/yard/api/flush"}
```

上記のようなサンプルログが収集された場合パーサ 追加画面でJSONパーサを選択します。複雑なパーシングロジックを作成する必要なく、ログ分析に必要なタグを次のように抽出できます。

Tag extraction

```
- host : 10.21.3.24
- method : POST
- status : 200
- url : http://dev.whatap.io/yard/api/flush
```

JSONフォーマットを一部構成する時の活用例

Some JSON format sample log

```
2023-08-08 02:43:28,615 -- {"host":"10.21.3.24","method":"POST","status":"200","url":"http://dev.whatap.io/yard/api/flush"}
--
```

もし、例のようにログの一部のみがJSONフォーマットで構成されている場合はPrefixとPostfixを指定してください。WhaTapログモニタリングはPrefixとPostfix間の領域をJSONフォーマットで認識してからパーシングします。

Tag extraction

```
- host : 10.21.3.24
- method : POST
- status : 200
- url : http://dev.whatap.io/yard/api/flush
```

警告アラート

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

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

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

主な機能

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

権限

イベントを追加または設定するには、**アラート設定権限** が必要です。

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

📌 参考資料

詳細については、[メンバー権限](#) を参照してください。

イベント設定

ホーム画面 > プロジェクト選択 >  アラート通知 > イベント設定

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

メトリクス

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

複合メトリクス

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

異常値

異常値機能では、想定外のパターンを検出して警告アラートを送信するよう設定できます。

リアルタイムログ

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

複合ログ

ログの内容を基準に警告通知を発生させる複合ログイベントを設定します。

ホーム画面 > プロジェクト選択 >  **アラート通知** > **イベント設定**

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

メトリクス

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

複合メトリクス

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

異常値

異常値機能では、想定外のパターンを検出して警告アラートを送信するよう設定できます。

リアルタイムログ

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

複合ログ

ログの内容を基準に警告通知を発生させる複合ログイベントを設定します。

参考

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

共通機能

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

- **JSON 一括編集**: すべてのイベント条件を JSON 形式で一括編集できます。
- **JSON 一括ダウンロード**: 現在登録されているイベント条件を JSON ファイルとして保存できます。
- **Excel 一括ダウンロード**: イベント一覧を Excel ファイルとしてダウンロードし、外部レポートやバックアップに活用できます。

JSON 一括編集

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

上書き後は、以前のイベント設定に戻すことはできません。

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



- JSON 編集画面には検証機能が組み込まれています。形式や値が正しくない場合、編集画面下部にエラーメッセージが表示され、[上書き] ボタンは無効になります。

```

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

```

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

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

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

基本オプション

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

表 | メトリクスイベント一覧構成

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

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

イベント設定

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

イベント追加

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

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

テンプレート選択

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

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

イベント条件定義

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

指標設定

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

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

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

❗ カテゴリや指標が不明な場合は、メトリクス照会を活用してください。

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

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

メトリクス検索

All 13件 / 全 149件

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

< 1 > 50件 / ページ

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

❗ イベントレベルの動作

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

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

4. 選択したイベントレベルのフィールド、演算子、値を入力します。

a. + 追加 をクリックすると条件を追加できます。

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

b. - をクリックすると、その条件が削除されます。

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

発生回数

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

1. 発生頻度を選択します。

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

2. 発生回数を入力します。

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

一時停止

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

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

❗ 解消通知が有効な場合

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

解消通知

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

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

イベント動作時間

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

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

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

シミュレーション

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

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

シミュレーション開始

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

シミュレーション結果の理解

1. 時系列データ

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

2. レベル別発生状況

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

3. 対象別詳細情報

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

4. ピーク区間の特定

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

🟢 シミュレーション活用のヒント

• 複数時間帯でのシミュレーション

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



- 実際の障害期間を含める

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

- 対象フィルタリングの追加

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

- しきい値を段階的に調整

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

イベント対象選択

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

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

対象選択

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

- **選択入力** 直接入力

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

監視対象のタグ、演算子、値を直接入力してください。

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

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

❗ 入力方法を変更すると、作成中の内容は初期化されます。

基本情報および通知設定

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

イベント有効化

設定した条件を満たした際にイベントを発生させるかどうかを設定します。

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

イベント名

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

メッセージ

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

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

- 変数の使用例

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

イベント受信

イベント通知を受信するメンバーを指定します。

- 全体受信** タグ選択受信

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

指定したタグを持つプロジェクトメンバーに通知が送信されます。

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

ⓘ 受信タグ

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

イベント修正／削除

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

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

イベント共有

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

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

エクスポート

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

インポート

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

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

JSON 形式で編集する

1. 画面右上の [JSON ] ボタンをクリックします。

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

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

JSON error

JSON データ構造

```
{
  "version": 2,
  "eventId": "zcef7s7f27rum1",
  "enabled": true,
  "stateful": false,
  "title": "Active Transaction",
  "message": "Active Transaction = ${active_tx_count}",
  "category": "app_counter",
  "alertLabel": [
    "oid"
  ],
  "repeatCount": 1,
  "repeatDuration": 0,
  "silent": 300000,
  "receiver": [],
  "timeTag": [],
  "selectString": "",
  "conditions": [
    {
      "level": 20,
      "enabled": true,
      "rule": "active_tx_count > 100"
    }
  ],
  "createTime": 1763632674345,
  "lastModifiedTime": 1763632674347,
  "lastModifiedUser": "support@whatap.io",
  "basic": true,
  "metaId": "java004",
}
```

```

"selectCondition":{
  "oid":[
    "-1010758404",
    "-250906941"
  ]
}
}

```

表 | JSON データ構造

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

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

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

付録

発生条件・対象選択ガイド

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

レベル動作ガイド

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

1. 優先順位に基づくイベント発生

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

例

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

2. レベル上昇

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

例

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

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

3. レベル下降

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

例

設定:

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

シナリオ:

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

4. 動作フロー

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

メトリクス値: 60% → 75% → 92% → 85% → 60%

状態: 正常 Warning Critical Warning 正常

 (発生) (発生) (維持) (解消)

 Warning

 (維持)

- ① 進行中状態を持つイベントは、条件が満たされている間は継続して有効となり、条件が解除されるまで維持されます。

条件設定ガイド

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

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

`${}` 使用例:

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

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

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

1. 比較演算子

数値比較

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

文字列比較

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

2. 算術演算子

- 基本的な算術演算

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

- 括弧による優先順位の制御

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

- 負の値の表現

```
cpu > -100
```

3. 論理演算子

- AND 演算 (&&)

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

- OR 演算 (||)

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

- 複合論理演算

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

4. パターンマッチング演算子

- LIKE 演算子

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

- NOT LIKE 演算子

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

5. 組み込み関数

- Null チェック関数

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

- 集計関数

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

- 数学関数


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

- 文字列関数

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

- 条件関数

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

形式

```
if(条件, true値, false値)
```

例

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

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

形式

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

例

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

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

形式

```
in(値, 候補値1, 候補値2, ..., 候補値N)
```

例

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

❗ 記述時の注意事項

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

複合メトリクス

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

複雑なルールを利用してイベントを作成し、警告通知を送信できます。

基本オプション

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

 権限

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

表 | 複合メトリクスイベント一覧の構成

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

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

イベント設定

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

イベント追加

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

イベントデータ照会

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

• ウィジェット テキスト

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

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

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

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

MXQL を直接編集できるエディタが表示されます。

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

通知

警告通知設定の基本情報を入力します。

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

Message example

 変数使用ルール



- 変数形式: \${メトリクス名}
- 設定した **カテゴリ**と**同一カテゴリ** 内のメトリクスのみ変数として使用できます。
- 複数の変数を組み合わせて、詳細なメッセージを構成できます。
- 使用可能な変数一覧は **メトリクス照会** で確認できます。

イベント発行条件

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

付加情報

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



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

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

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

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

イベントルールテスト

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

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

イベント修正／削除

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

イベント共有

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

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

エクスポート

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

インポート

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

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

JSON 形式で編集する

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

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

JSON error

通知メッセージ設定

受信するメッセージの詳細項目を選択し、項目ごとに内容を編集できます。

付録

MXQL 文法ガイド

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

異常値

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 

❗ 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)

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

- 画面右上の [JSON ] ボタンをクリックします。
- 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。
- 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

- 画面右上の [] ボタンをクリックします。
- 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。
- 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

- 画面右上の [JSON ] ボタンをクリックします。
- 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。
- 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

データベース

ホーム > プロジェクト選択 >  **アラート通知** > **イベント設定** classic

データベースの指標ごとにイベント条件を設定し、アラート通知を送信します。指標ごとにしきい値を入力することで、**危険** および **警告** レベルに分けて通知できます。

基本オプション

データベースインスタンスの主要指標を基準にイベント条件を設定できます。

- ・ **インスタンス**: イベント条件を設定するデータベースエージェント
- ・ **データベース**: モニタリング対象のデータベース
- ・ **エージェント非アクティブ警告**: 設定した時間後に応答がない場合、エージェントから警告通知を送信

表 | データベースイベント設定画面の構成

項目	説明
メトリクス	イベント条件を設定するデータベース指標
危険	Critical レベルのしきい値
警告	Warning レベルのしきい値
検知回数	指標が 5 秒ごとに収集される際、しきい値を連続して超過した回数 - 例: 3 回に設定した場合、5 秒 × 3 回連続 条件で通知
状態解消時の追加通知	イベント発生後、正常状態に復旧したことを知らせる追加通知 - DBX エージェント 1.6.30 以上対応
	イベント削除
	イベントの有効 / 無効 - 有効: 条件を満たすとイベント発生

項目	説明
	- 無効: イベントは動作せず条件も評価されません

イベント追加

選択した **メトリクス** 項目に基づき、入力した **危険** および **警告** 条件が **検知回数** 分だけ発生すると、アラート通知を送信するよう設定できます。

1. アラート通知 > イベント設定 **classic** に移動します。
2. インスタンス でアラートを設定するエージェントを選択します。
3. [+ イベント追加] ボタンをクリックします。
4. **メトリクス** から目的の指標を選択します。
5. **危険** と **警告** の比較演算子 (**<**, **≤**, **>**, **≥**) を選択し、数値を入力します。
 - 設定値を超過するとアラートが発生します。
6. **検知回数** に希望する数値を入力します。
 - 5 秒間隔で設定回数連続発生すると通知されます。
 - 例: 検知回数が 3 の場合
5 秒 (1 回目) - 5 秒 (2 回目) - 5 秒 (3 回目) → 合計 15 秒 → 通知
7. **状態解消時の追加通知** を有効にすると、イベントが解消 (RECOVERED) された際に追加通知が送信されます。

❗ 状態解消時の追加通知 機能は DBX エージェント バージョン 1.6.30 以上 で対応しています。
8. 右端のトグルボタンを有効 (🟢) にするとアラート通知が送信されます。
 - a. イベントを削除する場合は、該当イベントの 🗑️ をクリックしてください。

アラート複製

現在選択しているインスタンスに作成したアラートイベントを、他のインスタンスに複製できます。

1. アラート通知 > イベント設定 **classic** に移動します。
2. [アラート複製] ボタンをクリックします。
3. アラート複製 画面で複製先インスタンスを選択します。すべてのインスタンスに複製する場合は **全体選択** を選択してください。
4. [複製] ボタンをクリックしてアラートを複製します。

❗ 複製先インスタンスに既存のアラートイベントがある状態で **アラート複製** 機能を使用すると、既存のアラートイベントは削除されます。

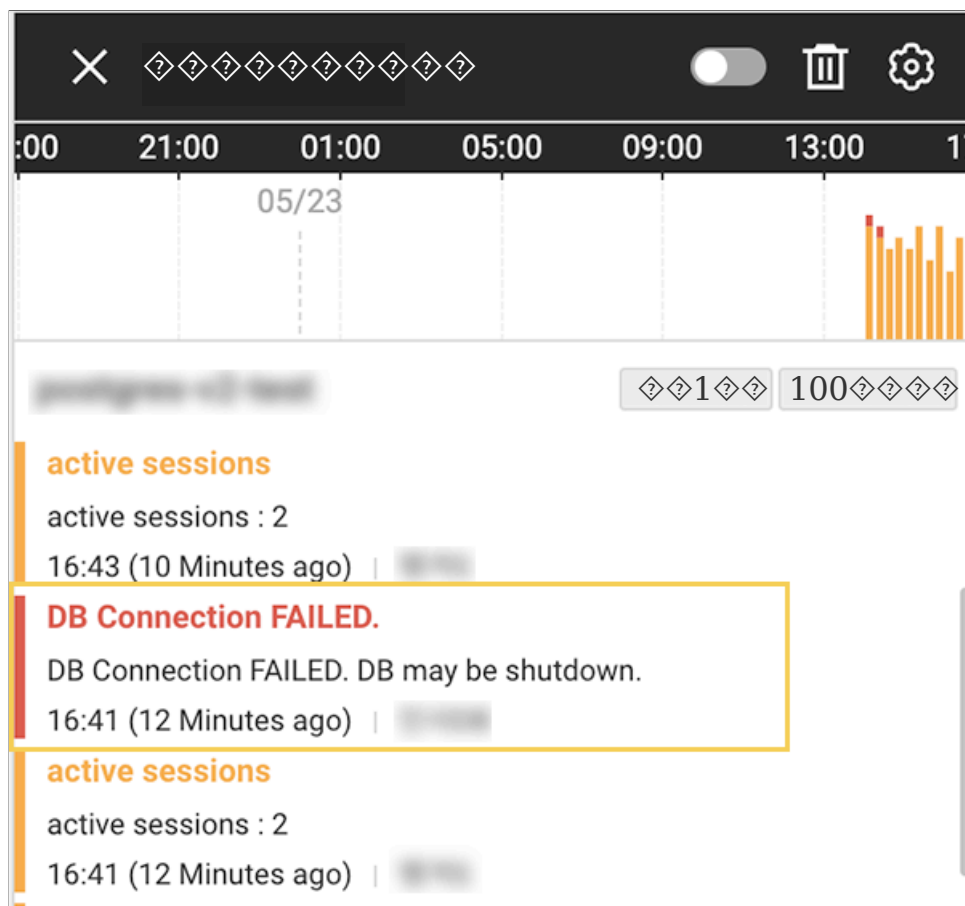
エージェント非アクティブ警告

設定した時間後に応答がない場合、エージェントから警告通知を送信します。

1. アラート通知 > イベント設定 **classic** に移動します。
2. エージェント非アクティブ警告 で希望する時間（ **30秒** , **1分** , **2分** , **3分** , **5分** , **10分** , **30分** ）を選択します。
3. 右側のトグルボタンをクリックして有効化します。
 -  **有効**: 設定した時間中にエージェントからデータを受信できない場合、**INACTIVE MONITORING AGENT** イベントが発生します。

基本アラート: Connection FAILED

イベントルールを別途設定しなくても、エージェントが DB 接続に 15 回以上失敗した場合、アラートが送信されます。DB シャットダウンやネットワーク障害、アカウントまたは権限の問題が原因となる場合があります。



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

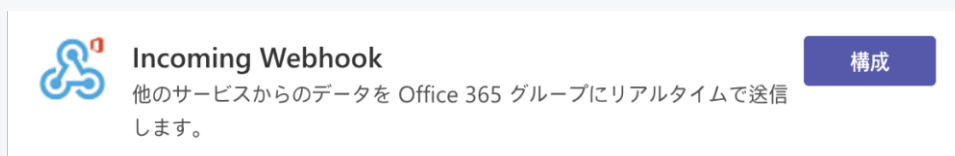
- `/help` : コマンド一覧を表示
- `/license` : 通知を受信するプロジェクトのアクセスキーを入力
- `/remove` : 通知を受信しないプロジェクトコードを入力
- `/list` : 現在通知を受信しているプロジェクトコードを表示

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。

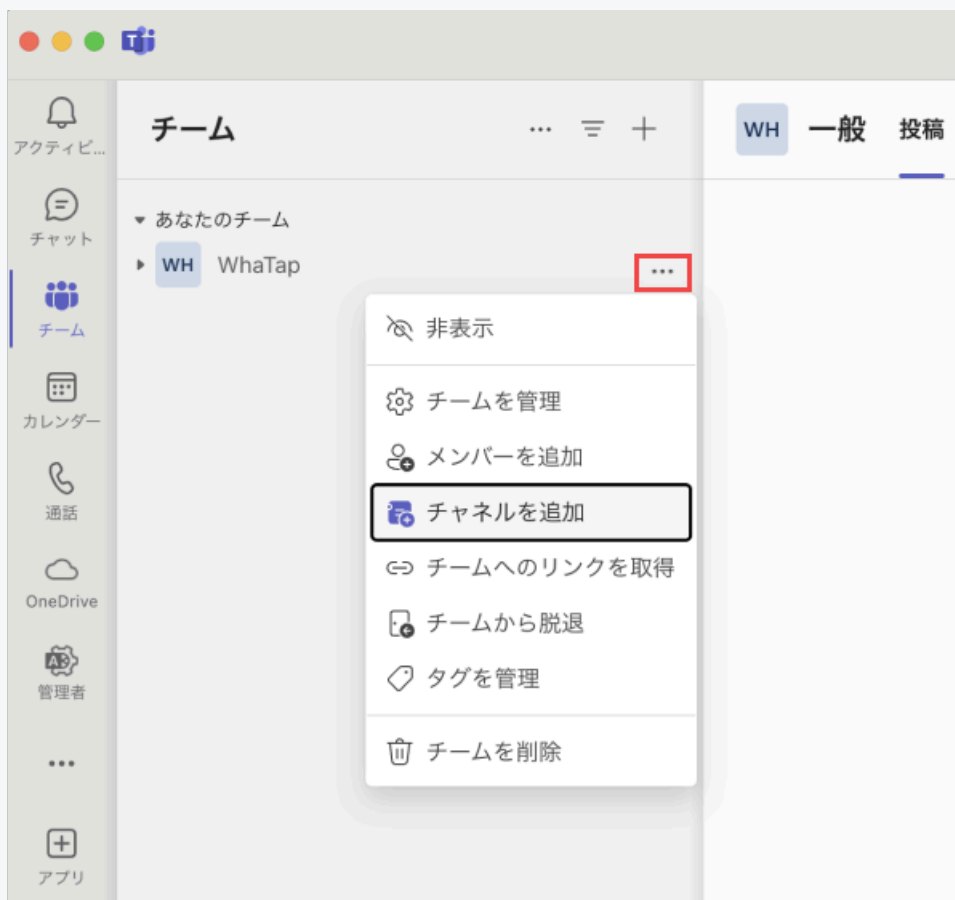
6. [登録] ボタンをクリックします。



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。

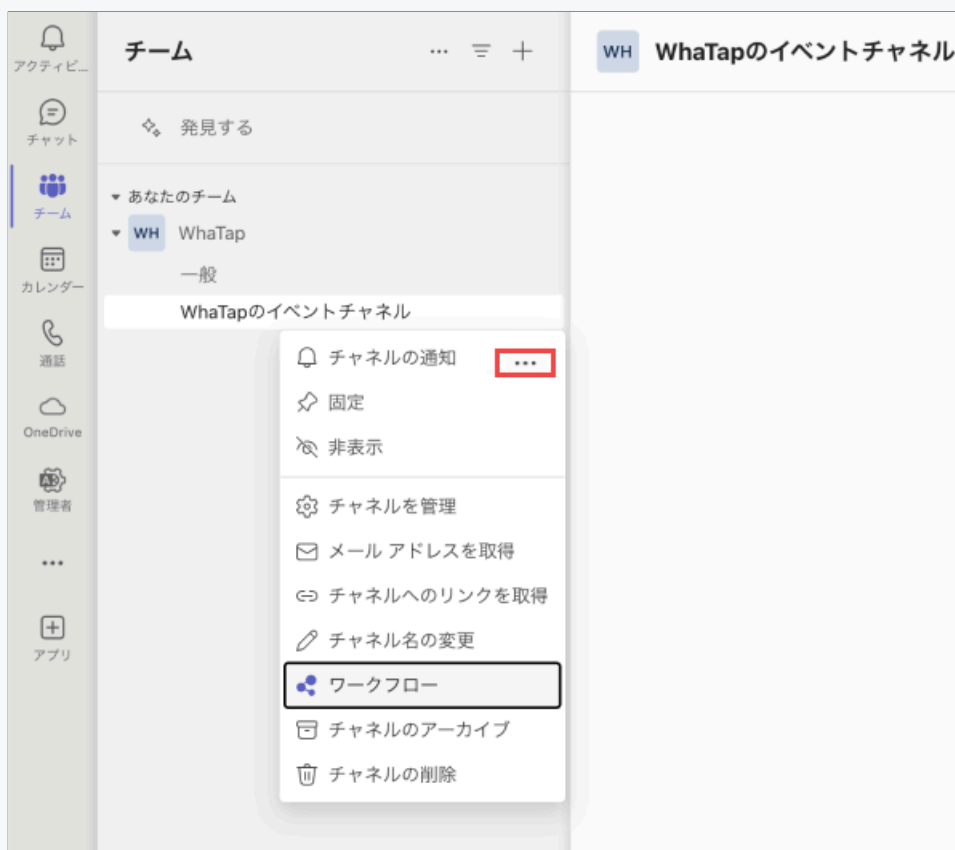
☐ 共有
組織内または組織外の人またはチームがアクセスできます。

☐ 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。

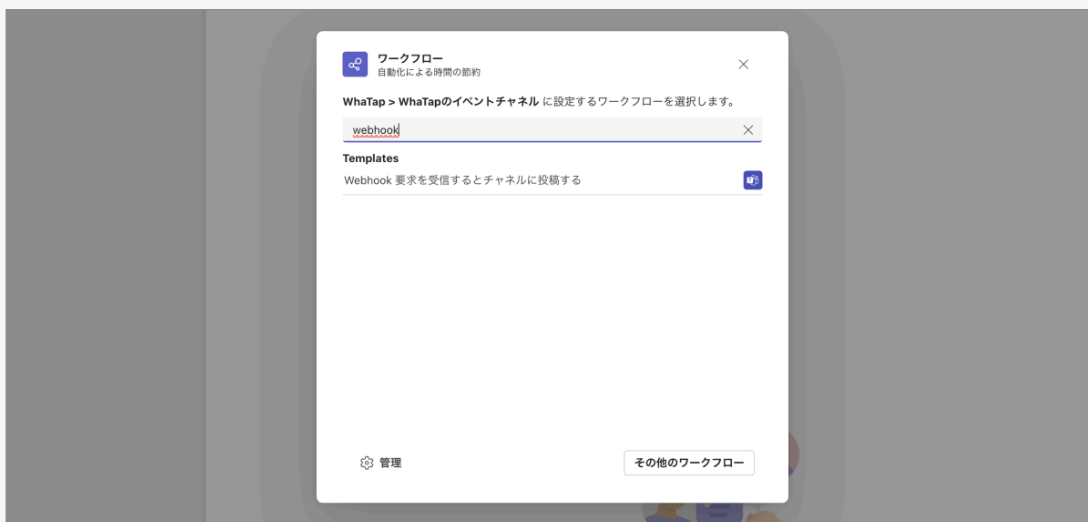
キャンセル 作成

❗ 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。



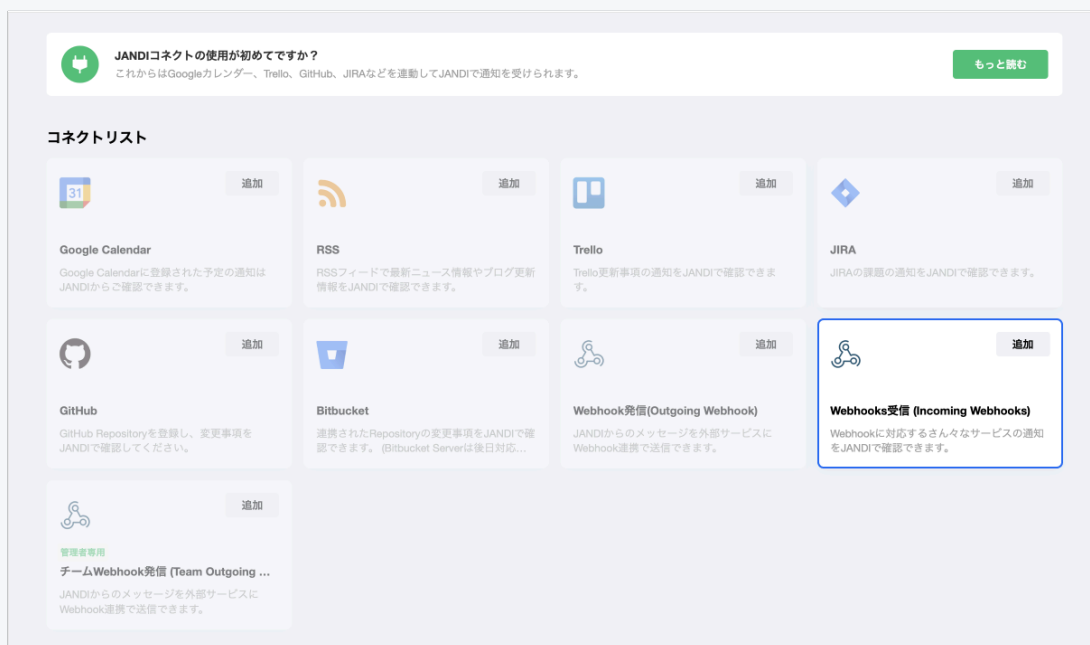
8. WhaTap モニタリングサービスの **サードパーティプラグインの追加** 画面に戻り、Teams **Workflows** タブ下部の **Channel Name** と **Webhook URL** に値を入力します。
9. [登録] ボタンをクリックします。

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}"
}
```

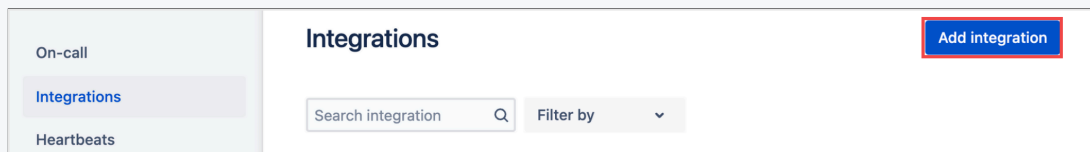
2. **Webhook Name** と **Webhook URL** の項目を入力してください。
3. ヘッダー値を追加するには、**ユーザーヘッダー値の追加**の+追加をクリックし、key と value を入力してください。
4. [**登録**] ボタンをクリックしてください。

Opsgenie

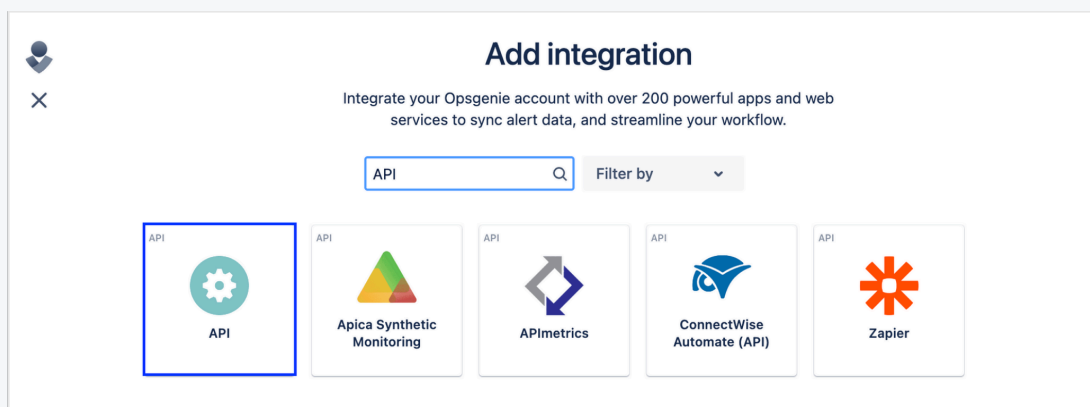




1. **Teams** メニューで、アラートを受信するチームを選択してください。
2. **Integration** メニューに移動し、[Add Integration] ボタンをクリックしてください。



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
- イベントチャンネル: SMS、Mobile、3rd-party プラグイン、プラグイン

イベントタイトル

Event title format

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

Event title example

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

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

- Platform は以下のいずれかで表示されます。
 - JAVA
 - NODEJS
 - PYTHON
 - PHP
 - DOTNET
 - GO
 - POSTGRESQL



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

イベントメッセージ

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

イベントメッセージ例

```
Project Name : アプリケーションプロジェクト  
Project Code : 3  
Agent Name : TC-0-1-8081  
Message : RECOVERED: Memory is too high. less than 10%  
Event Time : 2022-04-12 18:53:24 +0900
```

Event OFF Time : 2022-04-12 18:53:24 +0900
 Alert Type : APPLICATION_MEMORY
 Metric Name : memory
 Metric Value : 20
 Metric Threshold : 10
 Stateful : true

表 | イベントメッセージ構成要素

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

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

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

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

- **AlertType** は以下のいずれかの値で表示されます。

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



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



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

イベント履歴

ホーム > プロジェクト選択 >  アラート通知 > イベント履歴

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

イベント履歴の確認

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

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

カラム設定

表示するカラムや非表示にするカラムを設定できます。

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

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

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

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

↓ CSV ダウンロード

検索結果を CSV ファイル形式でダウンロードできます。

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

進行中のイベントのみ表示

現在進行中の状態のイベントのみを表示できます。

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

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

イベント検索

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

検索可能なフィールド

フィールド名および値は大文字と小文字を区別しません。

- **フィールド名タグ:** フィールドがサポートされるイベントタイプ
- **フィールドタイプ:** フィールドのデータ型
 -  #: Number
 -  T: String
 -  C: Boolean
 -  D: Date

イベント情報フィールド

フィールド名	タイプ	説明	例
Title	String	イベントタイトル	"Database Connection Error"
OffTitle	String	イベント解消タイトル	"RECOVERED: Database Connection Error"
Message	String	イベントメッセージ	"Connection timeout occurred"
OffMessage	String	イベント解消メッセージ	"RECOVERED: Connection timeout occurred"

フィールド名	タイプ	説明	例
Level	String	現在のイベントレベル	Critical, Warning, Info
OriginLevel	String	元のイベントレベル	Critical, Warning, Info
Status	String	イベント状態	ON, OFF, CANCEL, ACKNOWLEDGE, MAINTENANCE, DISABLED
ActCount	Number	発生回数	2
MetricName	String	指標名	"memory"
MetricValue	String	指標値	"85.5"
OffValue	String	解消時の値	"72.8"
MetricThreshold	String	閾値	"80"
alertType	String	イベント種別	"BASIC", "METRICS", "TRANSACTION" など
alertId	String	イベントルールの一意識別子	"zf3uojer0fv4v7"

イベントタイプ別対応フィールド

ⓘ 特定のイベントタイプでのみサポートされるフィールドです。該当しないイベントタイプの場合、値が存在しないことがあります。

フィールド名	タイプ	イベント種別	説明	例
eventRule	String	基本、メト	イベント発生	"memory ≥ 80"

フィールド名	タイプ	イベント種別	説明	例
		リクス	ルール	
field	String	リアルタイムログ	ログ検索キー	"content"
keyword	String	リアルタイムログ	ログ検索値	"Error"
logCategory	String	リアルタイムログ	ログカテゴリ	"AppLog"
logContent	String	リアルタイムログ	ログ内容	"00:00000:00009:2025/04/06 23:03:52.55 server Error: 1601, Severity: 17, State: 3\n00:00000:00009:2025/04/06 23:03:52.55 server There are not enough 'user connections' available to start a new process."

対象フィールド

フィールド名	タイプ	説明	例
Oid	Number	エージェントの一意識別子	-98765432
Oname	String	エージェント名	"web-server-01"
Okind	Number	エージェント種別の一意識別子	867318026

フィールド名	タイプ	説明	例
OkindName	String	エージェント種別名	"web-server"
Onode	Number	エージェントノードの一意識別子	334634079
OnodeName	String	エージェントノード名	"production-node-1"

イベント固有値フィールド

フィールド名	タイプ	説明	例
Id	Number	イベントの一意識別子	5768121
UUID	String	イベント固有識別子	"550e8400-e29b-41d4-a716"

状態／フラグフィールド

フィールド名	タイプ	説明	例
Stateful	Boolean	状態ベースイベントかどうか	true, false
Disabled	Boolean	無効化されたイベントかどうか	true, false
Escalation	Boolean	エスカレーション有無	true, false
SystemEvent	Boolean	システムイベントかどうか	true, false

検索タイプ別クエリ構文

① 検索の基本構文については、[WhaTap ログ検索クエリ構文](#) ドキュメントを参照してください。

1. キーワード検索

「Database Connection」という文字列を含むイベント

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

2. 複数値検索

指定した複数の値のうち、いずれかを含むイベントを検索します。

```
title: Database Connection
```

現在のイベントレベルが Info または Warning のイベント

```
level: info warning
```

3. パターン検索

ワイルドカードを使用してパターン検索ができます。

名前パターンで特定のエージェントで発生したイベントを検索

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

タイトルが Connection で終わるイベントを検索

```
title: *Connection
```

4. 複合条件検索

複数の条件を組み合わせて、より正確に検索できます。

レベルが Critical で、タイトルに Database を含むイベント

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

特定のエージェントにおける Warning または Critical のイベント


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

5. OR 条件検索

複数の条件のうち、**いずれか一つでも満たす**イベントを検索します。

タイトルまたはメッセージに特定のキーワードを含むイベント

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

6. 除外条件

特定の条件を除外して検索できます。

Info レベルを除いたすべてのイベント

```
not level: info
```

リアルタイムアラート

リアルタイムアラート機能は、イベント設定で設定したイベントが発生した際に、ポップアップ形式で表示されます。イベント発生と同時に通知を受け取ることで、問題を迅速に把握し、対応することができます。また、すでに発生した通知や見逃した通知の履歴を確認することで、リアルタイム対応が難しかった状況を把握し、解決に役立てることができます。

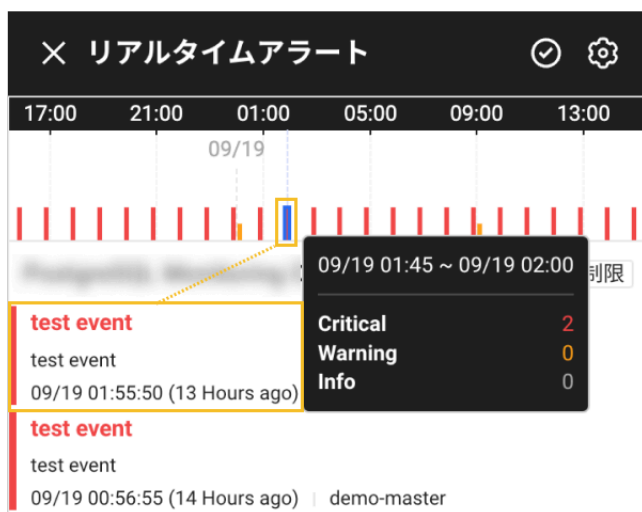
リアルタイムアラートを確認する

リアルタイムアラートは、画面右上にポップアップとして表示されます。通知が発生した時刻、タイトル、メッセージを確認できます。

- 個別の通知を閉じるには、メッセージ右上の ✕ ボタンをクリックしてください。
- 画面に表示されているすべてのポップアップ通知を閉じるには、**すべての通知を閉じる** をクリックしてください。

通知履歴を確認する

1. プロジェクトを選択して表示される画面の最上部にある 🔔 をクリックしてください。
2. リアルタイムアラート ウィンドウが表示されます。
 - 現在のプロジェクトについて、直近24時間以内の通知を最大100件まで確認できます。
 - 個別のイベント項目を選択すると、関連するメニューに移動します。
 - リアルタイムアラート ウィンドウ内の時間別チャートで任意の時間帯を選択すると、該当するイベント項目に移動します。



- すべての通知履歴を確認するには、**全体の通知履歴** ボタンをクリックしてください。**アラート通知 > イベント履歴** メニューに移動します。

❗ リアルタイムアラート の一覧が空の場合、**全体の通知履歴** ボタンが表示されます。受信タグ未設定の通知を受け取る オプションを無効にしてください。

イベントを一括で解消する

リアルタイムアラート の一覧から、進行中のすべてのイベントを一括で解消できます。

イベント解消が完了するまでに、約30秒～1分程度かかる場合があります。

- **イベント一括処理** 機能を使用すると、現在進行中のイベントに対する解消通知が大量に発生する可能性があります。
- **イベント一括処理** 機能を使用した後でも、イベントルールが有効であり、データが引き続きしきい値を超えている場合、イベントは再度発生することがあります。
- イベント解消通知は、**アラート通知 > イベント設定** メニューでイベントを編集し、**イベントが解消されたときに追加通知** または **解消通知** オプションを無効にすることで停止できます。

使用方法:

1. プロジェクトを選択して表示される画面上部の  をクリックします。
2. リアルタイムアラート ウィンドウが表示されたら、右上の  をクリックします。
3. リアルタイムアラートリストの進行中イベントを一括で解消します。 というメッセージが表示されたら、解消 ボタンをクリックします。

リアルタイムアラートを設定する

1. プロジェクトを選択して表示される画面上部の  をクリックします。
2. リアルタイムアラート ウィンドウが表示されたら、右上の  をクリックします。
3. リアルタイムアラート設定画面で各項目を設定します。
 - ポップアップ通知: リアルタイムアラート ウィンドウが閉じている状態でも、ポップアップ形式で通知を表示します。
 - 解消済みイベントを表示: リアルタイムアラート 一覧に解消済みイベントも含めて表示します。
 - 通知音の試聴: ブラウザで再生される通知音を事前に確認できます。Critical または Warning の横にある  をクリックしてください。音が再生されない場合は、ブラウザの設定をご確認ください。

システムイベント

WhaTap モニタリングは、プラットフォーム全体で自動的に検知・生成される共通イベントを提供します。本ドキュメントでは、システムによって発生するイベントの種類、発生条件、および対応方法について説明します。

EVENT_BLOCKED_BY_SYSTEM

プロジェクト内で短時間に過剰な数のイベントが発生した場合、WhaTap システムがこれを検知し、イベントの発生を一時的にブロックします。イベントがブロックされると、システムは次のメッセージをユーザーに通知します。このイベントが発生した場合は、イベント設定内容を確認し、必要に応じて調整してください。

 **Critical**



イベントメッセージ

Excessive events detected, event blocked for stability. name: server agent

プロジェクト番号	8
プロジェクト名	new server
対象	server agent
イベント名	EVENT_BLOCKED_BY_SYSTEM
イベント日時	(GMT+0900) 2024-11-18 18:03:18

WhaTapにログイン

new serverプロジェクトのserver agentから過度なイベントが検知されたため、イベント発生が遮断されます。server agentから一定期間の間にイベントが発生しなくなると、遮断が自動で解除されます。

ブロック基準

イベントは次の基準に基づいてブロックされます。

1. エージェント単位のブロック

1つのエージェントで **1分以内に10件** のイベントが発生した場合、そのエージェントから発生する以降のイベントはブロックされます。

2. 複数エージェントによる全体ブロック

条件 **1** によりイベントがブロックされたエージェントが **1分以内に3件以上** 発生した場合、プロジェクト全体のイベントがブロックされます。

3. プロジェクト単位のブロック

1つのプロジェクトで **1分以内に100件** のイベントが発生した場合、プロジェクト全体のイベントがブロックされます。

ブロック解除方法

システムによってイベントがブロックされた場合、対象のエージェントまたはプロジェクトで **1分間** イベントが発生しない状態を維持する必要があります。

- **アラート通知 > イベント設定** メニューから設定されているすべてのイベントを無効化してください。**イベント設定** を見直し、過剰なイベントが発生しないように閾値を調整する必要があります。
- イベントを設定する前に、**シミュレーション** 機能を活用してイベント発生回数を事前に予測できます。

実験室

ユーザーに新機能または試験的な機能を提供します。サイドメニューの  **実験室** または **サイトマップ** からアクセスできます。商品によって提供する機能が異なる場合があります。

✔ サイトマップから実験室メニューにアクセスする

サイドメニューに  **実験室** が表示されていない場合は、 **サイトマップ** からアクセスできます。

1. 画面左下の  **サイトマップ** アイコンをクリックしてください。
2. **サイトマップ** ウィンドウの右下にある **実験室** セクションで、目的のメニューを選択してください。

⚠ 注意

実験室の機能は現在開発中のベータ版であり、予期せぬ挙動やエラーが発生する可能性があります。十分な検証の上でご利用ください。重要なデータがある環境や運用環境では使用を推奨しません。フィードバックや問題点に対するお問い合わせは、サポートチーム(support@whatap.io)までご連絡ください。

MXQL Data

MXQLは、WhaTapの性能データ(メトリクス)を柔軟に検索するためのクエリ言語です。プロジェクトに含まれる複数のエージェントから収集したメトリクスを統合的に照会・活用するために使います。**MXQL**の詳細については、[次のドキュメント](#)をご参照ください。

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。

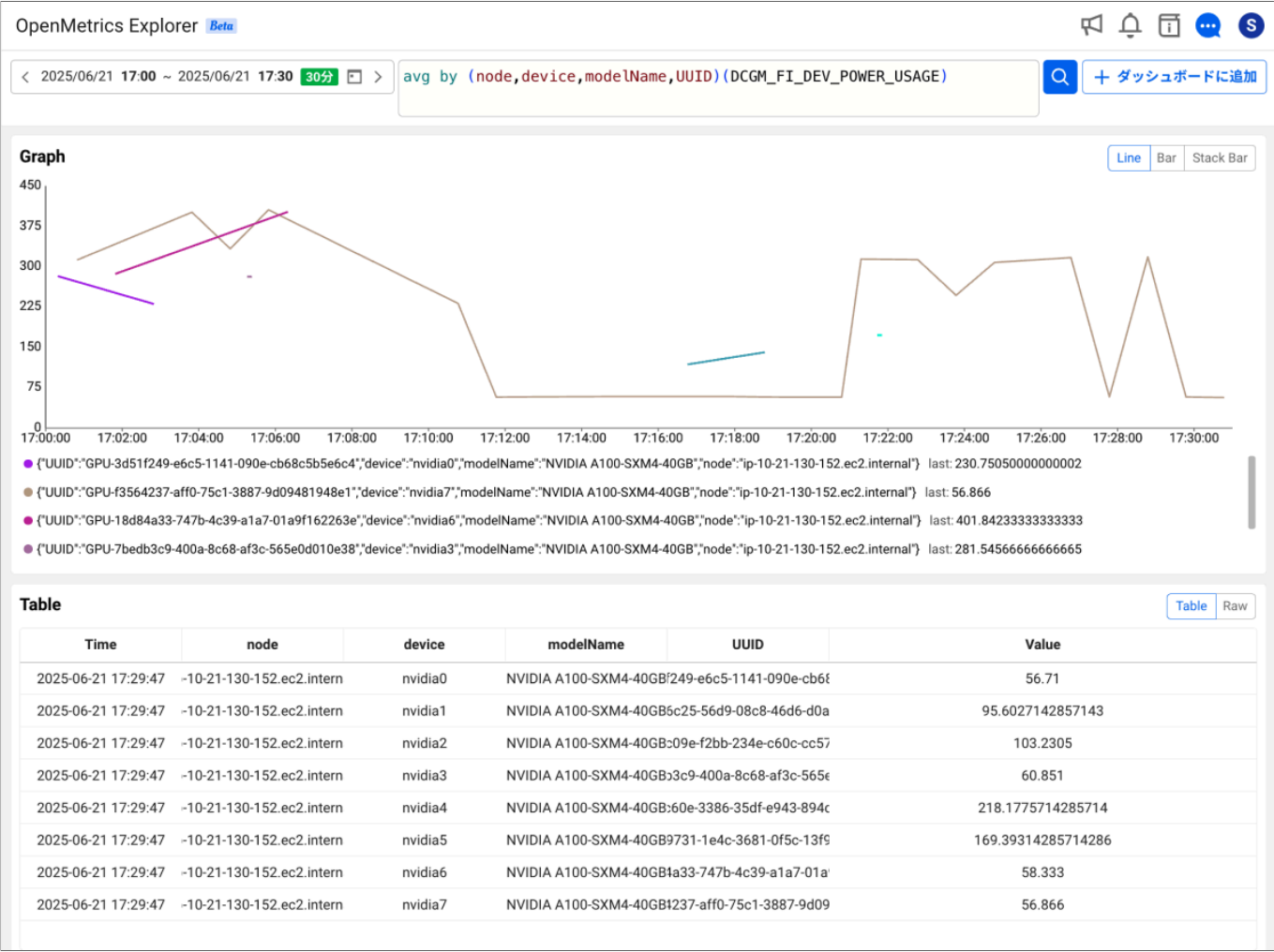
この機能を利用することで、必要なメトリクスを自由に照会し、有意義なデータを抽出したり、ダッシュボードに連携して継続的にモニタリングできます。

❗ OpenMetricsエクスプローラーを利用するには、Open Agent のインストールが必要です。

- [WhaTap Operator のインストール](#) ドキュメントを参照してください。

PromQL で探索する

OpenMetricsエクスプローラーでは、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。



グラフ

- **Line:** デフォルトの時系列折れ線グラフ
- **Bar:** 棒グラフ形式で可視化
- **StackBar:** 積み上げ値を表示するスタック型棒グラフ

テーブル / Raw

- **Table:** 各時系列の値を時間順に並べて表形式で表示
- **Raw:** Prometheus API の応答 (JSON 形式) をそのまま確認可能

PromQL 文法サポートとオートコンプリート

`node_cpu_seconds_total` や `container_memory_usage_bytes` などを入力すると、オートコンプリート機能でメトリクスや演算子の候補が提示されます。

`{pod="example"}` 形式のラベルフィルタリングにも対応しています。

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、対象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。
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、新しい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、指定したダッシュボードにウィジェットが追加されます。
 - 追加され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。
 - ウィジェットは Flex ボードのグリッドレイアウトで自由に配置でき、PromQL を修正できます。