

Server Monitoring

release date. 2026. 09. 11.

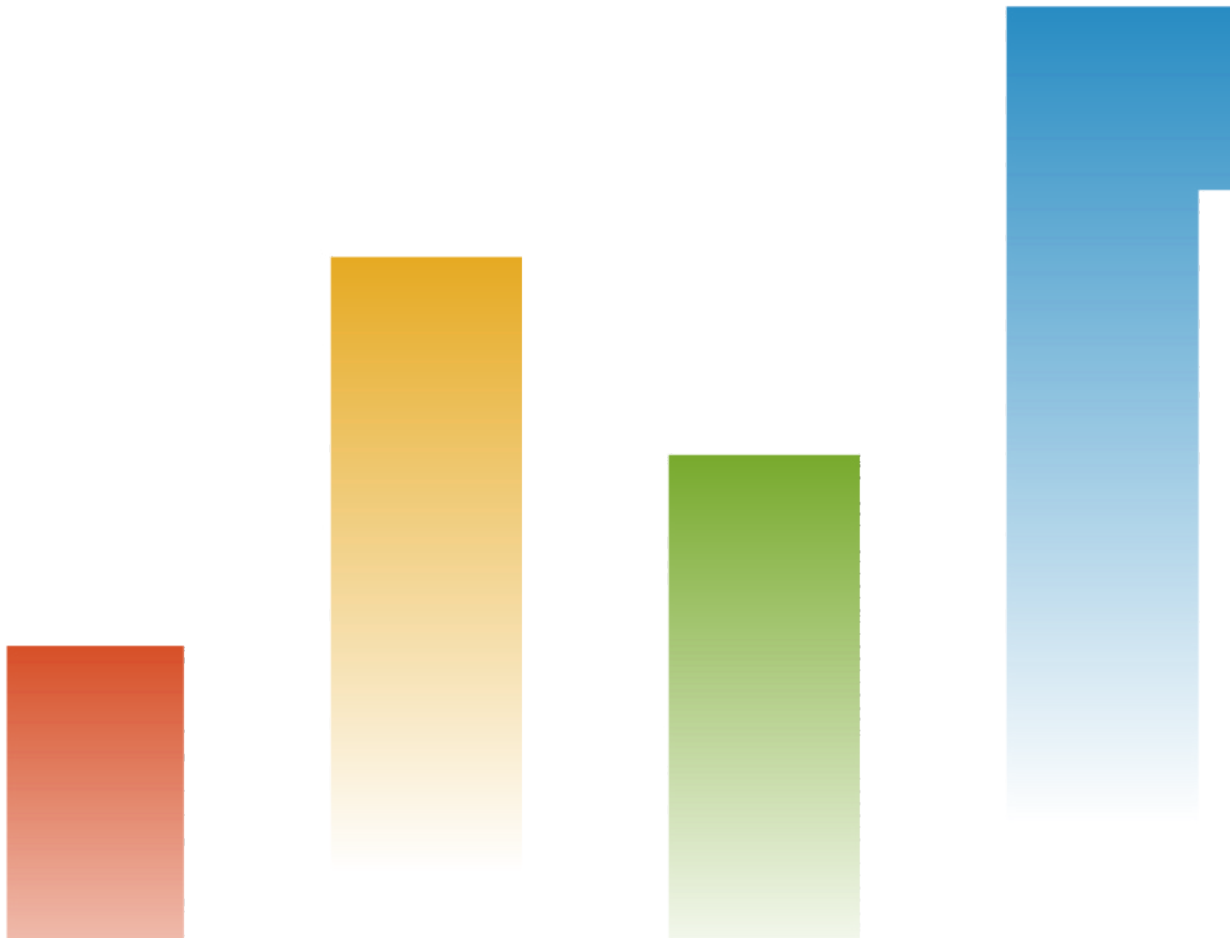


Table of Contents

• Serverモニタリング	5
◦ はじめに	7
◦ サポート環境	9
◦ インストール	
▪ インストールの概要	15
▪ 環境別インストールガイド	
▪ Linux	17
▪ Unix	20
▪ Windows	30
▪ サーバー以外の場合	33
▪ Elastic Beanstalk	34
▪ インストールの確認	37
▪ エージェントのアップデート	39
▪ エージェント削除	42
◦ 設定	
▪ 基本設定	44
▪ Windows性能カウンターの設定	49
▪ 拡張機能	50
▪ GPU機能	76
◦ ダッシュボード	
▪ リソースボード	78
▪ コンパウンドアイ	84
▪ サーバーインベントリマップ	87
▪ サーバーインベントリマップの詳細	100

▪ サーバーインベントリマップのグループ化	106
▪ Flexボード	111
▪ Flexボードの使用手法.....	114
▪ ウィジェットの管理.....	125
◦ サーバーリスト	
▪ サーバーインベントリ.....	130
▪ サーバーリスト.....	138
▪ サーバー詳細	147
▪ プロセスグループの追加	151
◦ GPU.....	155
▪ GPUダッシュボード	160
▪ GPUインベントリ	164
▪ GPUパフォーマンスサマリー	166
▪ GPU詳細	169
◦ 分析	
▪ キューブ.....	174
▪ メトリクス異常検出	177
◦ メトリクス	180
▪ サーバーメトリクス.....	183
▪ サーバーメトリクス V2.....	197
▪ インベントリ収集項目.....	259
▪ VMware収集項目	265
▪ GPUメトリクス	300
▪ メトリクスチャート	348
▪ メトリクス照会.....	351

◦ Logモニタリング	353
◦ レポート	0
▪ サーバーレポート	0
▪ 統合レポート	0
◦ アラート通知	0
▪ イベント設定	0
▪ メトリクス	0
▪ ログファイル	0
▪ 複合メトリクス	0
▪ 異常値	0
▪ リアルタイムログ	0
▪ 複合ログ	0
▪ イベント設定	0
▪ 通知設定	0
▪ イベント通知フォーマット	0
▪ イベント履歴	0
▪ リアルタイムアラート	0
▪ システムイベント	0
◦ 実験室	0
▪ メトリクスエクスプローラー	0
▪ プロセスグループ設定	0
▪ ファイルシステム運用情報	0
▪ NIC構成情報	0
▪ 時刻同期情報	0
▪ OS Parameter情報	0

サーバーモニタリング

WhaTapサーバーモニタリングサービスは1分以内にインストールでき、実務担当者の観点から迅速に導入可能です。CPUやディスクI/Oなど、しきい値を超える可能性のある指標は5秒間隔で収集し、平均値による検出の限界を克服します。また、20秒間隔のプロセスモニタリングも提供しています。

統合モニタリングのための複数のダッシュボードを提供しており、システム全体の状況を簡単に把握できます。クラウド環境に適した指標に対応しており、スケールアウト環境にも適用可能です。

WhaTapのサーバーモニタリングサービスを利用すると、運用担当者がいなくてもサーバーを安定して運用できます。

主な機能

- 多様な規模のサーバーモニタリング

さまざまな種類のダッシュボードを通じて、システム全体の状況をリアルタイムで確認できます。

- サーバーインベントリ管理

表示したい項目を選択して表示できるテーブル形式でサーバーリストを管理し、リアルタイムモニタリングが可能です。

- リアルタイム統合アラート

リソースの推移モニタリングや異常指標の検出にとどまらず、リアルタイムの統合アラート履歴を通じて障害に迅速に対応できます。サーバー、プロセス、キーワードに基づくアラートに対応しています。

- システム担当者向けのWhaTapレポート

運用担当者に対してさまざまな種類のレポートを提供し、手作業の負担を軽減します。必要なレポートはフィードバックに基づいて追加することができます。

- クラウド性能の脆弱性の検知

クラウド環境のアプリケーションで発生し得る脆弱性を自動的に検出し、アラートを提供します。

- 最適なシステム規模の予測

サーバー規模の変化をリアルタイムでモニタリングし、最適な規模を予測することができます。

- プロセス性能の自動収集

すべてのプロセスのCPU、メモリ、I/O使用量を20秒単位で自動的に収集します。

- **マルチチャネルと個人用設定の通知**

電子メール、SMS、3rd Party Plugin を使用して、パーソナライズされた通知サービスを提供します。

- **クラウド、物理サーバー、ハイブリッド環境に対応**

クラウドおよび物理サーバー環境の両方に適した指標を提供し、スケールアウト環境でも活用できます。

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

OS別のサポート環境

WhaTapのサーバーモニタリングエージェントをインストールする前に、サポート環境を確認してください。X86ベースで動作するLinux、AIX、Windowsに適用されます。

 最終更新: 2025-12-10

Linux

エージェントバージョン	RHEL 5.8+	CentOS 6+	Rocky Linux 8.6+	SUSE 10.1+	Amazon Linux	Ubuntu 12.04+	Debian 6.0+
v2.9.5	✓	✓	✓	✓	✓	✓	✓

CentOSは最小サポートバージョンが6に引き上げられました。CentOS 6では一部の機能のみをサポートし、すべての機能はCentOS 7以上でサポートします。

RHELのサポートバージョンは変更されておらず、従来どおり5.8以上をサポートします。

Unix

エージェントバージョン	AIX 6.1+	Oracle Solaris 10+	Oracle Solaris 11.2+	HP-UX 11.23+
v1.4.4	✓	✓	✓	✓

FreeBSDはサポート対象から除外しました。エージェントのインストール画面でもFreeBSD項目を提供しません。

Windows

エージェントバージョン	Windows 2008 R2+
v2.9.5	

❗ 使用環境がサポート一覧に含まれていない場合は、support@whatap.io までお問い合わせください。

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。

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。

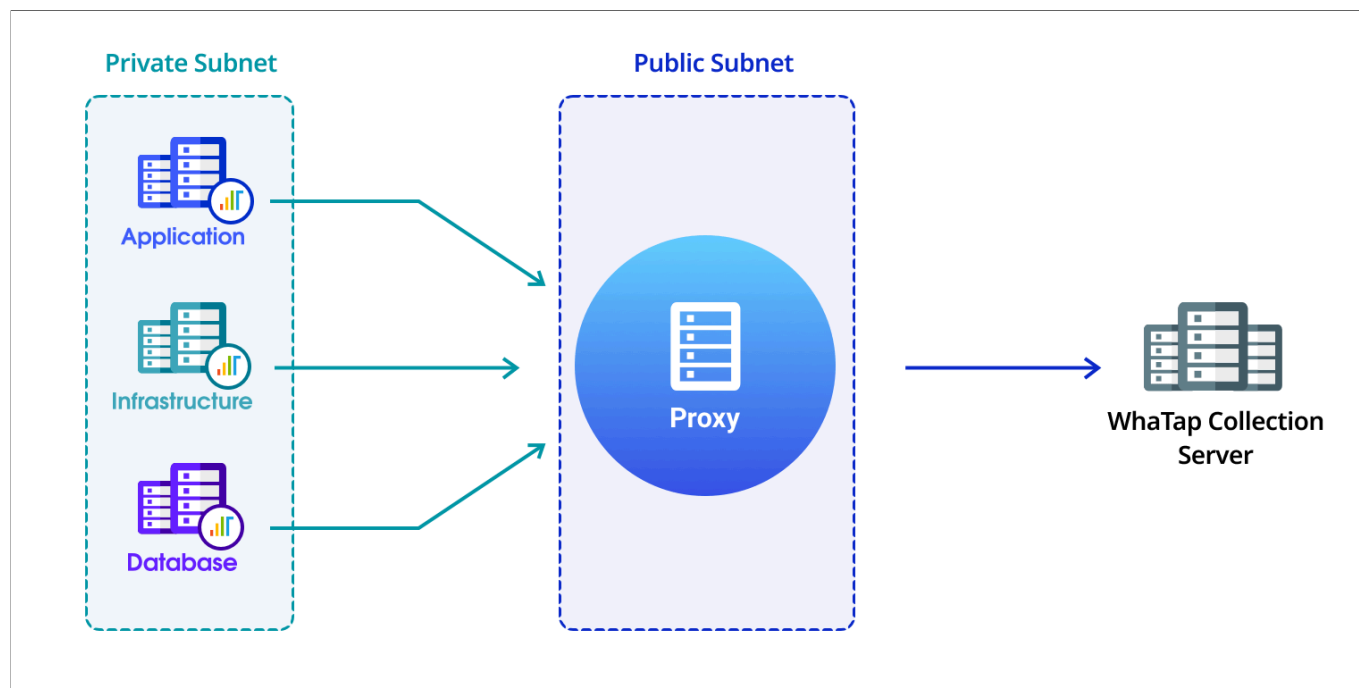
ファイアウォール

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。



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

インストールの概要

WhaTapサーバーモニタリングエージェントのインストール手順を案内します。

インストール前の確認事項

エージェントをインストールする前に、次の点を確認してください。

- [はじめに](#)でプロジェクト作成とアクセスキーの発行を完了しているか確認してください。
- [サポート環境](#)で使用中のオペレーティングシステムがサポートされているか確認してください。

基本インストール手順

1. エージェントインストール画面で、監視対象サーバーのオペレーティングシステムを選択します。
2. オペレーティングシステム別の詳細ガイドに従って、エージェントパッケージをダウンロードしてインストールします。
3. 設定ファイル([whatap.conf](#))にプロジェクトアクセスキーと収集サーバー情報を入力します。
4. エージェントを起動します。

✔ エージェントインストール画面に移動していない場合は、左側のメニューから**全プロジェクト**>該当プロジェクトを選択してください。

エージェントファイル構成

オペレーティングシステム別のエージェントファイル構成は次のとおりです。

- 共通ファイル
 - [ChangeLog.txt](#)：エージェントの変更履歴です。
 - [whatap.conf](#)：サーバーのデータを収集するために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

が入力されるファイルです。

- **Linux/FreeBSD**

- `whatap_infrad`：データ収集と送信エージェントです。
- `whatap_infrad.pid`：実行中のエージェントのPID値を記録するファイルです。
- `VERSION`：現在インストールされているエージェントのバージョンを記録するファイルです。

- **Windows**

- `whatap_infra.exe`：データ収集と送信用エージェントです。
- `unins000.`：エージェントの削除ファイルです。
- `whatap.ico`：WhaTapインフラのアイコン画像です。

環境別インストールガイド

使用中の環境に合ったインストールガイドを選択してください。

Linux

❗ サーバーモニタリングエージェントのインストール時に `sudo` 権限のあるユーザーアカウントまたはrootアカウントでインストールを進めてください。

新規で作成したサーバーモニタリングプロジェクトを選択すると、エージェントインストール画面が表示されます。プロジェクトの管理>エージェントインストールメニューからでもできます。

エージェントインストール

< オペレーティングシステムの選択



Ubuntu 20.04 LTS

64-bit (amd64)

amd64 (outbound)

インストールの案内

▼ 開く

チャットでのお問い合わせ

動画チュートリアル

▶ 1. アクセスキーの確認

▶ 2. WhaTapリポジトリの追加

▶ 3. サーバーモニタリングパッケージのインストール

▶ 4. サーバーモニタリングの開始

▶ 5. エージェントのアップデート

エージェントインストール画面から対象OSを選択し、プロジェクトのアクセスキーを確認した後、次のようにインストールします。

1. WhaTap リポジトリを登録します。

WhaTapリポジトリの追加タブから該当するコマンドをコピーして入力します。

- [Debian / Ubuntu](#) SUSE CentO6 Amazon Linux

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

```
sudo rpm --import https://repo.whatap.io/suse/release.gpg
echo "[whatap]" | sudo tee /etc/zypp/repos.d/whatap.repo > /dev/null
echo "name=whatap packages for enterprise linux" | sudo tee -a /etc/zypp/repos.d/whatap.repo > /dev/null
echo "baseurl=https://repo.whatap.io/suse/12/x86_64" | sudo tee -a /etc/zypp/repos.d/whatap.repo > /dev/null
echo "enabled=1" | sudo tee -a /etc/zypp/repos.d/whatap.repo > /dev/null
echo "gpgcheck=1" | sudo tee -a /etc/zypp/repos.d/whatap.repo > /dev/null
sudo zypper refresh
```

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

```
sudo rpm --import https://repo.whatap.io/centos/release.gpg
echo "[whatap]" | sudo tee /etc/yum/repos.d/whatap.repo > /dev/null
echo "name=whatap packages for enterprise linux" | sudo tee -a /etc/yum/repos.d/whatap.repo > /dev/null
echo "baseurl=https://repo.whatap.io/centos/latest/\$basearch" | sudo tee -a /etc/yum/repos.d/whatap.repo > /dev/null
echo "enabled=1" | sudo tee -a /etc/yum/repos.d/whatap.repo > /dev/null
echo "gpgcheck=0" | sudo tee -a /etc/yum/repos.d/whatap.repo > /dev/null
```

2. 次のコマンドを実行し、パッケージをインストールします。

サーバーモニタリングパッケージのインストールタブでコマンドをコピーして入力します。

- [Debian / Ubuntu](#) SUSE CentOS / Amazon Linux

```
sudo apt-get install whatap-infra
```

```
sudo zypper install whatap-infra
```

```
sudo yum install whatap-infra
```

3. 設定スクリプトを実行してください。

設定スクリプトを実行しサーバーモニターデモンを開始してください。タブに移動してコマンドを作成してコピーするか、下部のコマンドにプロジェクトアクセスキーとサーバーIPを追加して実行します。

```
echo "license=[発行されたプロジェクトアクセスキー]" |sudo tee /usr/whatap/infra/conf/whatap.conf
echo "whatap.server.host=[割り当てられたWhaTapサーバーIP]" |sudo tee -a /usr/whatap/infra/conf/whatap.conf
echo "createdtime=`date +%s%N`" |sudo tee -a /usr/whatap/infra/conf/whatap.conf
sudo service whatap-infra restart
```

ⓘ 注意事項

データ転送用にTCPアウトバウンド**6600 PORT**が開放されている必要があります。

① サーバー エージェントファイルの構成

ⓘ

• 共通ファイル

- **ChangeLog.txt**：エージェントの変更履歴です。
- **whatap.conf**：サーバーのデータを収集するために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が入力されるファイルです。

• Linux/FreeBSD

- **whatap_infrad**：データ収集と送信エージェントです。
- **whatap_infrad.pid**：実行中のエージェントのPID値を記録するファイルです。
- **VERSION**：現在インストールされているエージェントのバージョンを記録するファイルです。

Unix

FreeBSD

❗ FreeBSDのサポート終了

FreeBSD用のサーバーモニタリングエージェントはサポートを終了しました。**エージェントインストール画面**のオペレーティングシステム選択リストにFreeBSD項目を提供せず、サーバーインベントリ機能もサポートしません。以下の手順は、以前にインストールした環境のための参考資料です。

新規作成したサーバーモニタリングプロジェクトを選択すると、**エージェントインストール画面**が表示されます。プロジェクト**管理**>**エージェントインストールメニュー**を通じても可能です。

エージェントインストール

🔊 🔔 📁 ⋮ 👤

◀ オペレーティングシステムの選択



Project Name

Project Description

Project ID (outbound)

インストールの案内

▼ 開く

💬 チャットでのお問い合わせ

🎥 動画チュートリアル

▶ 1. アクセスキーの確認

▶ 2. WhaTapリポジトリの追加

▶ 3. サーバーモニタリングパッケージのインストール

▶ 4. サーバーモニタリングの開始

▶ 5. エージェントのアップデート

エージェントインストール画面から対象OSを選択し、プロジェクトのアクセスキーを確認した後、次のようにインストールします。

1. WhaTap リポジトリを登録します。

WhaTapリポジトリの追加タブから該当するコマンドをコピーして入力します。

```
wget https://repo.whatap.io/freebsd/10/whatap-infra.txz
```

2. 次のコマンドを実行し、パッケージをインストールします。

サーバーモニタリングパッケージのインストールタブでコマンドをコピーして入力します。

```
pkg install whatap-infra.txz
```

3. 設定スクリプトを実行してください。

設定スクリプトを実行しサーバーモニターデモンを開始してください。タブに移動してコマンドを作成してコピーするか、下部のコマンドにプロジェクトアクセスキーとサーバーIPを追加して実行します。

```
echo "license=[発行されたプロジェクトアクセスキー]" | sudo tee /usr/whatap/infra/conf/whatap.conf
echo "whatap.server.host=[割り当てられたWhaTapサーバーIP]" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
echo "createdtime=`date +%s%N`" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
sudo service whatap-infra restart
```

ⓘ 注意事項

データ転送用にTCPアウトバウンド6600 PORTが開放されている必要があります。



サーバーエージェントファイルの構成



• 共通ファイル

- **ChangeLog.txt**：エージェントの変更履歴です。
- **whatap.conf**：サーバーのデータを収集するために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が入力されるファイルです。

• Linux/FreeBSD

- **whatap_infrad**：データ収集と送信エージェントです。
- **whatap_infrad.pid**：実行中のエージェントのPID値を記録するファイルです。
- **VERSION**：現在インストールされているエージェントのバージョンを記録するファイルです。

- 新規作成したサーバーモニタリングプロジェクトを選択すると、エージェントインストール画面が表示されます。プロジェクト管理>エージェントインストールメニューを通じても可能です。

エージェントインストールメニューのOSの選択画面でAIXを選択し、プロジェクトアクセスキーを確認した後、次の手順に進みインストールします。

1. インストールファイルのダウンロードタブで[whatap-infra-latest.noarch.rpm](#)ボタンを選択して、エージェントのインストールファイルをダウンロードします。
2. インストールファイルの実行タブに移動し、次の実行コマンドを確認してから、パッケージを実行します。

```
rpm -Uvh whatap-infra-latest.noarch.rpm
```

⚠ サーバーセキュリティのため、インストーラーはダウンロードでのみ提供します。

エージェント実行

次のコマンドを実行して、サーバーモニタリングを開始します。アプリケーションサーバーが実行されると、エージェントがモニタリング情報を収集します。

```
echo "license=x4t2322hcqshs-x1q9rv0b9rjvs6-x4jnrqfl5ce5g" |tee /usr/whatap/infra/conf/whatap.conf
echo "whatap.server.host=127.0.0.1" |tee -a /usr/whatap/infra/conf/whatap.conf
echo "createdtime=date +%s%S" |tee -a /usr/whatap/infra/conf/whatap.conf
stopsrc -s whatap-infra
startsrc -s whatap-infra
```

注意事項

WhaTap AIXエージェント1.3.3以下のバージョンをインストールする際、次のような追加オプションの設定が必要です。

1. サーバーリストメニューで**コラム設定**ボタンを選択した後、サーバー情報の**OID**項目を有効にします。
2. サーバーリストで対象サーバーの**OID**コラム情報を確認します。
3. 次のようにOID固定オプションを追加します。

```
echo "oid=[サーバーのoid]" >> /usr/whatap/infra/conf/whatap.conf
```

Oracle Solaris

- ① • WhaTap Oracle Solarisエージェント1.3.3以下のバージョンをインストールする際、追加オプションの設定が必要です。 [次の文書](#)を参照してください。
- サポートするバージョン：Oracle Solaris 10、11.2、11.3、11.4

新規作成したサーバーモニタリングプロジェクトを選択すると、**エージェントインストール**画面が表示されます。プロジェクト**管理**>**エージェントインストール**メニューを通じても可能です。

エージェントインストール

< OS選択



Oracle Solaris
 サポートバージョン: Oracle Solaris 11.2 以降
 WhaTapサーバー 127.0.0.1へデータを転送のためには、6600番ポートの開放が必要です。(TCP Outbound)

インストールの案内

開く
チャットでのお問い合わせ
動画チュートリアル

▶ 1. アクセスキーの確認

▼ 2. インストールファイルのダウンロード

プロジェクトアクセスキーが発行された場合にのみ、インストールファイルのダウンロードが可能です。

下の「ダウンロードコマンド」を実行するか、インストールファイルをダウンロードします。

ダウンロードコマンド

```
wget https://repo.whatap.io/sunos/11/whatap-infra.latest.SPARC.pkg.tar.gz
```

コピー

インストールファイルのダウンロード

 whatap_infra.zip

▶ 3. インストールファイルの実行

▶ 4. サーバー監視の開始

▶ 5. エージェントを更新する場合

エージェントインストールメニューのOSの選択画面で**Oracle Solaris**選択後、プロジェクトアクセスキーを確認したら、次の案内通りにインストールを進めてください。

1. ダウンロードコマンドを実行するか**インストールファイルのダウンロード**タブでバージョンを選択し、インストールファイルをダウンロードします。

- 次のコマンドを使用して、エージェントのインストールファイルをダウンロードします。

```
wget https://repo.whatap.io/sunos/11/whatap-infra.latest.SPARC.pkg.tar.gz
```

- **whatap_infra.zip**ボタンを選択して、エージェントのインストールファイルをダウンロードします。

2. インストールファイルの実行タブに移動し、次の実行コマンドを確認してから、パッケージを実行します。

```
tar xzvf whatap-infra.latest.SPARC.pkg.tar.gz
pkgadd -d .
```

エージェント実行

次のコマンドを実行して、サーバーモニタリングを開始します。アプリケーションサーバーが実行されると、エージェントがモニタリング情報を収集します。

```
echo "license=x4t2322hcqshs-x1q9rv0b9rjvs6-x4jnrqfl5ce5g" |tee /usr/whatap/infra/conf/whatap.conf
echo "whatap.server.host=127.0.0.1" |tee -a /usr/whatap/infra/conf/whatap.conf
echo "createdtime=`date +%s%S`" |tee -a /usr/whatap/infra/conf/whatap.conf
/etc/init.d/whatap-infra start
```

注意事項

WhaTap Oracle Solarisエージェント1.3.3以下のバージョンをインストールする際、次のような追加オプションの設定が必要です。

1. サーバーリストメニューで**コラム設定**ボタンを選択した後、サーバー情報の**OID**項目を有効にします。
2. サーバーリストで対象サーバーの**OID**コラム情報を確認します。
3. 次のようにOID固定オプションを追加します。

```
echo "oid=[サーバーのoid]" >> /usr/whatap/infra/conf/whatap.conf
```

❗ Oracle Enterprise Edition駆動サーバー

Oracle Enterprise Editionが駆動中のサーバーにインストールする場合は、次を参照してプロセスの収集オプションを無効にします。

```
echo "task_proc=false" >> /usr/whatap/infra/conf/whatap.conf
/etc/init.d/whatap-infra restart
```

エージェントの障害処理

Oracle SolarisエージェントでNo Dataが誤って検知された場合の処理方法を次のようにご案内します。

OIDの設定確認

`/usr/whatap/infra/conf/whatap.conf` ファイルで `oid` オプションが設定されていることを確認します。

- エージェントバージョン1.3.3以下では、OIDを手動で設定する必要があります。設定方法は、[次の文書](#)を参照してください。
- エージェントバージョン1.3.4以降では、OIDが自動的に設定されます。

エージェントバージョンが1.3.3以下であり、Oracle Enterprise Editionを使用する時

Oracle Enterprise Editionが駆動中のサーバーでは、プロセスの情報収集はサポートされていません。

1. `/usr/whatap/infra/conf/whatap.conf` ファイルに `task_proc=false` オプションが設定されていることを確認します。
2. もし設定されていない場合は、次のコマンドを実行してオプションを設定した後、エージェントを再起動します。

```
echo "task_proc=false" >> /usr/whatap/infra/conf/whatap.conf
/etc/init.d/whatap-infra restart
```

このプロセスを通じてプロセスの収集オプションが無効になり、Oracle Enterprise Editionが駆動される環境でのエージェントの動作を保証します。

HP-UX

- ① • HP-UX Itanium 11.23バージョンから対応します。
- HP PA-RISC-UX 11.23バージョンから対応します。

新規作成したサーバーモニタリングプロジェクトを選択すると、エージェントインストール画面が表示されます。プロジェクト管理 > エージェントインストールメニューを通じても可能です。

エージェントインストール

< OS選択

HP-UX
バージョン: HP-UX Itanium : 11.23, HP PA-RISC-UX : 11.23
WhaTapサーバー 127.0.0.1へデータを転送するためには、6600番ポートの開放が必要です。(TCP Outbound)

インストールの案内 ▼ 開く チャットでのお問い合わせ 動画チュートリアル

IA64 PA-RISC

▶ 1. アクセスキーの確認

▼ 2. インストールファイルのダウンロード

プロジェクトアクセスキーが発行された場合にのみ、インストールファイルのダウンロードが可能です。
以下のインストールファイルをダウンロードしてください。

11.23 バージョン	11.31 バージョン
whatap_infra.zip	whatap_infra.zip

▶ 3. インストールファイルの実行

▶ 4. サーバー監視の開始

▶ 5. エージェントを更新する場合

エージェントインストールメニューのオペレーティングシステムの選択画面でHP-UXを選択します。ユーザーのHP-UXサーバーアーキテクチャに従って、上部のタブで **IA64** または **PA-RISC** の中から選択した後、プロジェクトアクセスキーを確認します。その後、次の手順とおりインストールします。

• **IA64** PA-RISC

1. インストールファイルのダウンロードタブで適切なバージョンの [whatap_infra.zip](#) ボタンを選択して、エージェントのインストールファイルをダウンロードします。
2. インストールファイルの実行タブに移動し、次の実行コマンドを確認してから、パッケージを実行します。


```
gunzip -c whatap-infra.latest.ia64.tar.gz | tar xvf -  
./whatap-infra/install.sh x4t2322hcqshs-x1q9rv0b9rjvs6-x4jnrqfl5ce5g 127.0.0.1
```

1. インストールファイルのダウンロードタブで`whatap_infra.zip`ボタンを選択して、エージェントのインストールファイルをダウンロードします。
2. インストールファイルの実行タブに移動し、次の実行コマンドを確認してから、パッケージを実行します。

```
gunzip -c whatap-infra.latest.pa.tar.gz | tar xvf -  
./whatap-infra/install.sh x4t2322hcqshs-x1q9rv0b9rjvs6-x4jnrqfl5ce5g 127.0.0.1
```

エージェント実行

次のコマンドを実行して、サーバーモニタリングを開始します。アプリケーションサーバーが実行されると、エージェントがモニタリング情報を収集します。

```
/sbin/init.d/whatap-infra start
```

Windows

新規で作成したサーバーモニタリングプロジェクトを選択すると、エージェントインストール画面が表示されます。プロジェクトの**管理**>**エージェントインストール**メニューからでもできます。

エージェントインストール

＜ オペレーティングシステムの選択



Windows

対応OS：Windows Server 2008 R2以降

WhaTapサーバー 127.0.0.1へデータを転送のためには、6600番ポートの開放が必要です。(TCP Outbound)

インストールの案内

▼ 開く

チャットでのお問い合わせ

動画チュートリアル

▶ 1. アクセスキーの確認

▼ 2. インストールファイルのダウンロード

whatap_infra.exe

whatap_infra.zip

リンクをクリックすると、Windowsサーバー向けのインストールファイル（whatap.exe/ whatap.zip）がダウンロードされます。

セキュリティ設定により.exe形式のファイルがダウンロードできないユーザーのために、.zip形式のファイルもダウンロードできます。

*セキュリティ向上のため、ブラウザから直接インストールするより、インストールファイルをダウンロードしてから実行する方をお勧めします。

▶ 3. インストールファイルの実行

▶ 4. エージェントのアップデート

エージェントインストールメニューのOSの選択画面で**Windows**を選択し、プロジェクトアクセスキーを確認した後、次の手順に進みインストールします。

1. エージェントファイルをダウンロードします。

インストールファイルのダウンロード' タブで **whatap_infra.exe** または、 **whatap_infra.zip** ボタンを選択して、エージェントのインストールファイルをダウンロードします。

- ❗ • セキュリティ設定により_.exe_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_形式のファイルも提供します。
- サーバーのセキュリティのために、ブラウザから直接インストールするのではなく、ダウンロードしたインストールファイルで実行することをお勧めします。

2. モニタリング対象サーバーに接続してエージェントファイルをアップロードしてください。
3. ダウンロードしたインストール ファイルをダブルクリックして実行してください。
4. ③ インストールファイルの実行 タブに移動し、発行されたプロジェクトアクセスキーとサーバーIPを確認します。
5. 画面の指示に従って、[License Key](#)項目にプロジェクトアクセスキーを入力し、[WhaTap IP](#)の項目に、WhaTapサーバーのIPアドレスを入力します。
6. [Next](#) ボタンをクリックします。
7. 次の画面で [Install](#) ボタンをクリックします。インストールを続行します。
8. [Finish](#) ボタンをクリックして、インストールを終了してください。

閉域網環境におけるインストールファイルの署名検証

インターネットから分離された閉域網のサーバーでは、Windowsがルート証明書の自動更新を受け取れないため、正常に署名されたインストールファイルでも署名検証に失敗する場合があります。インストーラーはオペレーティングシステムの信頼ストアに依存せず、インストーラーに含まれるルート証明書のフィンガープリントと署名証明書チェーンを直接比較する方式で検証します。サーバーの証明書ストアを変更しないため、閉域網でも別途の対応なくインストールを進められます。

署名・ハッシュが破損したファイルや、期限切れ・失効した証明書で署名されたファイルは、引き続きインストールを拒否します。

① サーバー エージェントファイルの構成

- ❗ • 共通ファイル
 - [ChangeLog.txt](#)：エージェントの変更履歴です。
 - [whatap.conf](#)：サーバーのデータを収集するためにサーバーのアドレスとサーバーのプロジェクト



アクセスキーが入力されるファイルです。

- **Windows**

- [whatap_infra.exe](#) : データ収集と送信用エージェントです。
- [unins000.](#) : エージェントの削除ファイルです。
- [whatap.ico](#) : WhaTapインフラのアイコン画像です。

サーバー以外の場合

ラップトップなどのサーバーコンピューターではなくパソコンを使用している場合、IPアドレスを変更して、Wi-Fiを使用する環境では、次のオプションを適用してください。

デフォルト値の変更案内

エージェント2.9.21バージョンから、`ipreg` オプションのデフォルト値は `false` です。そのため、IPアドレスが頻繁に変わる環境でも、別途の設定なしに最初に決定されたエージェント識別子をそのまま維持します。以下の設定は、デフォルト値を明示的に指定したい場合にのみ使用してください。

オートスケール環境は例外です。`autoscale` オプションを使用するか、`autoscale.group` の値を指定すると、エージェントは `ipreg` の値を `true` に切り替えます。オートスケール環境のサーバーは寿命が短く、起動のたびに現在のIPアドレスを基準に再登録する必要があるためです。

- **Linux** Windows

```
echo "ipreg=false" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
sudo service whatap-infra restart
```

SH

```
// 管理者権限のPowerShellで次のコマンドを実行してください。
Add-Content "c:\Program Files\WhatapInfra\whatap.conf" "ipreg=false"
Restart-Service "Whatap Infra"
```

ⓘ IPが変更されるたびに自動的に再登録されることがないため、便利に使用できます。

Elastic Beanstalk

Elastic Beanstalkを使用してデプロイする場合、WhaTapエージェントを適用します。

1. Linuxのインストール環境に合わせ、以下をElastic Beanstalkの **インストールスクリプト**に追加します。

❗ `whatap.server.host` と `license` は**プロジェクトアクセスキー**をユーザーに合わせて入力します。

- [Debian / Ubuntu](#) **CentOS** [Amazon Linux](#)

```
```bash
wget https://repo.whatap.io/debian/release.gpg -O -|sudo apt-key add -
wget https://repo.whatap.io/debian/whatap-repo_1.0_all.deb
sudo dpkg -i whatap-repo_1.0_all.deb
sudo apt-get update
sudo apt-get install whatap-infra
echo "license={LICENSE_INFO}" |sudo tee /usr/whatap/infra/conf/whatap.conf
echo "whatap.server.host={HOST_IP}" |sudo tee -a /usr/whatap/infra/conf/whatap.conf
echo "createdtime=`date +%s%N`" |sudo tee -a /usr/whatap/infra/conf/whatap.conf
sudo service whatap-infra restart
```
```

```
```bash
sudo rpm --import https://repo.whatap.io/centos/release.gpg
sudo rpm -Uvh https://repo.whatap.io/centos/5/noarch/whatap-repo-1.0-1.noarch.rpm
sudo yum install whatap-infra
echo "license={LICENSE_INFO}" |sudo tee /usr/whatap/infra/conf/whatap.conf
echo "whatap.server.host={HOST_IP}" |sudo tee -a /usr/whatap/infra/conf/whatap.conf
echo "createdtime=`date +%s%N`" |sudo tee -a /usr/whatap/infra/conf/whatap.conf
sudo service whatap-infra restart
```
```

```
```bash
sudo rpm --import https://repo.whatap.io/centos/release.gpg
echo "[whatap]" | sudo tee /etc/yum.repos.d/whatap.repo > /dev/null
echo "name=whatap packages for enterprise linux" | sudo tee -a /etc/yum.repos.d/whatap.repo > /dev/null
```

```

echo "baseurl=https://repo.whatap.io/centos/latest/\$basearch" | sudo tee -a /etc/yum.repos.d/whatap.repo > /dev/null
echo "enabled=1" | sudo tee -a /etc/yum.repos.d/whatap.repo > /dev/null
echo "gpgcheck=0" | sudo tee -a /etc/yum.repos.d/whatap.repo > /dev/null
sudo yum install whatap-infra
echo "license={LICENSE_INFO}" | sudo tee /usr/whatap/infra/conf/whatap.conf
echo "whatap.server.host={HOST_IP}" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
echo "createdtime=date +%s%N" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
sudo service whatap-infra restart
```

```

• SUSE FreeBSD

```

```bash
sudo rpm --import https://repo.whatap.io/suse/release.gpg
echo "[whatap]" | sudo tee /etc/zypp/repos.d/whatap.repo > /dev/null
echo "name=whatap packages for enterprise linux" | sudo tee -a /etc/zypp/repos.d/whatap.repo > /dev/null
echo "baseurl=https://repo.whatap.io/suse/12/x86_64" | sudo tee -a /etc/zypp/repos.d/whatap.repo > /dev/null
echo "enabled=1" | sudo tee -a /etc/zypp/repos.d/whatap.repo > /dev/null
echo "gpgcheck=1" | sudo tee -a /etc/zypp/repos.d/whatap.repo > /dev/null
sudo zypper refresh
sudo zypper install whatap-infra
echo "license={LICENSE_INFO}" | sudo tee /usr/whatap/infra/conf/whatap.conf
echo "whatap.server.host={HOST_IP}" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
echo "createdtime=`date +%s%N`" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
sudo /etc/init.d/whatap-infra restart
```

```

```

```bash
wget https://repo.whatap.io/freebsd/10/whatap-infra.txz
pkg install whatap-infra.txz
echo "license={LICENSE_INFO}" | tee /usr/whatap/infra/conf/whatap.conf
echo "whatap.server.host={HOST_IP}" | tee -a /usr/whatap/infra/conf/whatap.conf
echo "createdtime=`date +%s%N`" | tee -a /usr/whatap/infra/conf/whatap.conf
service whatap_infra restart
```

```

1. 次のコマンドを変更します。

```

echo "createdtime=date +%s%N" | sudo tee -a /usr/whatap/infra/conf/whatap.conf

```

インストール後、サーバーモニタリングをBeanstalkに含めて、アプリケーションをデプロイすると、サーバーモニタリングが繰り返される可能性があります。

WhaTapエージェントの内部IDが、上記のコマンドが実行されるたびに新しく発行されるためです。今後のデプロイ時に新しいリストが追加されないように、次のように変更します。

```
echo "createdtime=12345678" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
```


インストールの確認

サーバーモニタリングのインストールを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。

Linux及びUnix

ログ出力確認

エージェントが正常にインストールされている場合は、次のログ出力を確認できます。 接続に成功すると、connected というメッセージが表示されます。

- [Debian/Ubuntu/SUSE](#) CentOS/Amazon Linux/Unix

```
tail -10 /var/log/syslog
```

```
...
```

```
Apr 8 16:28:08 localhost systemd[1]: Started LSB: Start whatap-infra daemon.
```

```
Apr 8 16:28:08 localhost whatap_infrad[32468]: 2019/04/08 16:28:08 Config file: /usr/whatap/infra/conf/whatap.conf
```

```
Apr 8 16:28:08 localhost whatap_infrad[32468]: 2019/04/08 16:28:08 OID: 1193741647 ONAME: localhost
```

```
Apr 8 16:28:08 localhost whatap_infrad[32468]: 2019/04/08 16:28:08 connected to {whatap ip}:{whatap port}
```

```
tail -10 /var/log/messages
```

```
...
```

```
Apr 8 16:28:08 localhost systemd[1]: Started LSB: Start whatap-infra daemon.
```

```
Apr 8 16:28:08 localhost whatap_infrad[32468]: 2019/04/08 16:28:08 Config file: /usr/whatap/infra/conf/whatap.conf
```

```
Apr 8 16:28:08 localhost whatap_infrad[32468]: 2019/04/08 16:28:08 OID: 1193741647 ONAME: localhost
```

```
Apr 8 16:28:08 localhost whatap_infrad[32468]: 2019/04/08 16:28:08 connected to {whatap ip}:{whatap port}
```

ファイアウォール設定とネットワーク設定の確認

接続できない場合は、ファイアウォール設定を含むネットワーク設定を確認してください。 ネットワーク設定が反映されると、エージェントは自動的に接続されます。

Windows

正常にインストールが完了した場合、インストールの最終段階で次の画面が表示されます。 エージェントが自動的にモニタリングを開始します。

ⓘ 注意事項

データ転送用にTCPアウトバウンド**6600 PORT**が開放されている必要があります。

エージェントのアップデート

⚠ 以前のバージョンをインストールする場合は、support@whatap.io までお問い合わせください。

Linux

インストールされているエージェントを最新バージョンにアップデートするには、次のコマンドを実行してください。

- Debian / Ubuntu

```
sudo apt-get update
sudo apt-get install whatap-infra
sudo service whatap-infra restart
```

特定のバージョンをインストールする場合は、インストール時にバージョン情報を指定します。

```
sudo apt-get install whatap-infra={version}
```

- CentOS / Amazon Linux / SUSE

```
sudo yum update whatap-infra
sudo service whatap-infra restart
```

特定のバージョンをインストールする場合は、インストール時にバージョン情報を指定します。

```
sudo yum install whatap-infra-{version}
```

Unix

- FreeBSD

インストールされているエージェントを最新バージョンにアップデートするには、次のコマンドを実行してくださ

い。

```
wget https://repo.whatap.io/freebsd/10/whatap-infra.txz
pkg install whatap-infra.txz
```

• AIX

インストールされているエージェントを最新バージョンにアップデートするには、次のコマンドを実行してください。

```
stopsrc -s whatap-infra
cp /usr/whatap/infra/conf/whatap.conf /tmp/whatap.conf
rpm -e whatap-infra
rpm -Uvh https://repo.whatap.io/aix/noarch/whatap-infra-latest.noarch.rpm
cp /tmp/whatap.conf /usr/whatap/infra/conf/whatap.conf
startsrc -s whatap-infra
```

• Oracle Solaris

インストールされているエージェントを最新バージョンにアップデートするには、次のコマンドを実行してください。

```
cp /usr/whatap/infra/conf/whatap.conf /tmp
/etc/init.d/whatap-infra stop
pkgrm whatap-infra
wget https://repo.whatap.io/sunos/11/whatap-infra.latest.SPARC.pkg.tar.gz
tar xzvf whatap-infra.latest.SPARC.pkg.tar.gz
pkgadd -d .
cp /tmp/whatap.conf /usr/whatap/infra/conf/whatap.conf
/etc/init.d/whatap-infra start
```

• HP-UX

インストールされているエージェントを最新バージョンにアップデートするには、次のコマンドを実行してください。

• IA64 PA-RISC

IA64

```
cp /usr/whatap/infra/conf/whatap.conf /tmp
/sbin/init.d/whatap-infra stop
gunzip -c whatap-infra.latest.ia64.tar.gz | tar xvf -
yes n | ./whatap-infra/install.sh
cp /tmp/whatap.conf /usr/whatap/infra/conf/whatap.conf
/sbin/init.d/whatap-infra start
```

PA-RISC

```
cp /usr/whatap/infra/conf/whatap.conf /tmp
/sbin/init.d/whatap-infra stop
gunzip -c whatap-infra.latest.pa.tar.gz | tar xvf -
yes n | ./whatap-infra/install.sh
cp /tmp/whatap.conf /usr/whatap/infra/conf/whatap.conf
/sbin/init.d/whatap-infra start
```

Windows

インストール済みのエージェントを最新バージョンにアップデートするには、**管理 > エージェントインストールメニュー**に移動します。**インストールの案内**セクションの**インストールファイルのダウンロード**の指示に従って、Windows サーバー用のインストーラーをダウンロードし、**whatap_infra.exe**ファイルを実行します。エージェントのアップデート後、サービスが再起動されます。

❗ セキュリティ設定により、**.exe** 形式のファイルがダウンロードできないユーザーは、**.zip** 形式のファイルを提供します。詳しい内容は [次の文書](#)を参照してください。

エージェント削除

Linux

インストールされたエージェントを削除するには、次のコマンドを実行してください。

- Debian / Ubuntu

```
sudo apt-get remove whatap-infra
```

- CentOS / Amazon Linux / SUSE

```
sudo yum remove whatap-infra
```

Unix

- FreeBSD

```
pkg delete whatap-infra
```

- AIX

```
stopsrc -s whatap-infra  
rpm -e whatap-infra  
rm -rf /usr/whatap/infra
```

- Oracle Solaris

```
pkgrm whatap-infra  
rm -rf /usr/whatap/infra
```

- HP-UX

IA64 / PA-RISC

```
swremove whatap-infra
```

Windows

- サーバーモニタリングエージェントの削除コマンドを管理者権限のcommandウィンドウで実行します。

```
"C:\Program Files\WhatapInfra\unins000.exe"
```

- コントロールパネルのプログラム削除機能を使用することができます。

基本設定

WhaTapサーバーモニタリングエージェントは、[whatap.conf](#)設定ファイルを通じて動作を制御します。このドキュメントでは、エージェントの基本設定を案内します。

❗ 設定ファイルの場所

- **Unix/Linux:** `$WHATAP_HOME/whatap.conf`
- **Windows:** `%WHATAP_HOME%\whatap.conf`

設定変更後、変更事項を適用するにはエージェントを再起動する必要があります。

エージェント名の識別

WhaTapは、モニタリング情報の収集対象となるインフラストラクチャサーバーの識別のために、サーバーから収集した情報を使用します。既定値は、サーバーのホスト名(hostname)です。

- ❗ • エージェント名は、プロジェクトごとに一意である必要があります。
- エージェントID／名前を変更しても、古いデータには関連付けられません。

- ❗ • ユーザーが設定したエージェント名を [WhaTapのモニタリングサービス](#)を確認するには、サーバーを再起動してください。

ユーザーフレンドリーな名前を指定する場合、次のように設定ファイルに指定できます。

• Linux Shell

```
export WHATAP_SERVER_NAME=ユーザーフレンドリーな名前  
  
echo "oname=$WHATAP_SERVER_NAME" |sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

• Windows Power Shell


```
# 管理者権限が必要です。
```

```
$WHATAP_SERVER_NAME="ユーザーフレンドリーな名前"
```

```
Add-Content "C:\Program Files\WhaTapInfra\whatap.conf" "oname=$WHATAP_SERVER_NAME"
```

ネットワーク設定

WhaTapは、エージェントにサーバー通信でTCP接続してからモニタリングデータを送信します。

WhaTapエージェントのネットワーク

エージェントは、1つのTCPセッションを介してデータ送信とサーバーの制御要求を処理します。ノードエージェントはUDPを使用しません。ノードエージェントからWhaTap収集サーバーの通信はファイアウォールを開きます。

収集サーバーのアドレスとポート

WhaTapサーバーは、データリージョンサーバーとフロントサーバー、ユーレカなどに区分します。データリージョンにはProxy、Yard、Gateway、Keeperなどがあります。エージェントは、Proxyサーバーと通信します。

NodeエージェントにWhaTapサーバのproxyサーバのアドレスを設定します。(ex,

`whatap.server.host=10.0.3.1/10.0.3.2`)サーバアドレスを設定する場合、proxyサーバの数を入力します。WhaTapサーバは、インストール方法によって、proxyサーバを1つまたは複数使用できます。

WhaTap Proxyサーバは6600番ポートでリスニング(Listening)します。エージェントで何も設定しない場合、エージェントは6600番ポートへの接続を試みます。

whatap.conf

```
whatap.server.port=6600
```

- ⓘ 2つのProxyサーバーが異なるポートを使用することはできません。複数のProxyサーバーを使用している場合は、(Listening) ポートが同じである必要があります。

通信接続およびセキュリティ

WhaTapは、パブリックネットワークでモニタリングデータを収集することを前提に設計されています。そのため、すべてのモニタリングデータを暗号化してサーバーに送信します。WhaTapは、オーバーヘッドを最小限に抑えるため、データを選択的に暗号化します。エージェントとサーバー間の通信プロセスは次のとおりです。

1. プロジェクト作成時に**プロジェクトアクセスキー**を生成してコピーします。
2. **プロジェクトアクセスキー**には秘密鍵が含まれているため、外部に露出しないように注意してください。
3. エージェントを起動すると、WhaTap収集サーバーにTCPセッションを接続します。
4. **プロジェクトアクセスキー**に含まれる通信用秘密鍵でデータを暗号化し、新しいセッション用セキュリティキーをリクエストします。
5. サーバーは、エージェントがリクエストしたセッション用セキュリティキーを生成してエージェントに渡します。
6. その後、エージェントはテキスト、数値などのデータを暗号化してサーバーに送信します。

❗ 変更を有効にするには、サーバーを再起動してください。

エージェントリソース制限

Linux及びWindowsサーバーで使用するWhaTapのサーバーモニタリングエージェントは、過負荷発生時にサーバーの安定性を維持し、資源使用量の影響を最小限にするため、次のようなエージェント設定を提供します。

Linux / Windows

メモリ使用量の保護

WhaTapエージェントは、メモリの使用量が臨界点(100MB)を超える場合、自動的にプロセスを再起動し、ユーザーサーバーの利用可能なメモリを保護します。

```
memory.usage.limit=104857600 #メモリ使用量の臨界値(100MB、バイト単位)
```

自動的再起動

WhaTapエージェントは1日1回、自動的に再起動されます。該当サイクルはユーザー設定を通じて調整可能です。この機能は、データ収集の障害と一時的なプロセスの誤動作を解消するために提供されます。

```
housekeeping.enabled=true      #自動的な再起動機能の活性化(デフォルト:true)
housekeeping.hour=2            #再起動時間(サーバー時間基準、デフォルト:2時)
housekeeping.exitoncheckfail=true #収集障害の発生時、自動的に再起動(デフォルト:true)
```

再起動の時刻は、時間単位のほかに分単位でも指定できます。housekeeping.minute オプションをあわせて設定すると、エージェントは housekeeping.hour と housekeeping.minute が指す時刻以降に再起動します。サーバーが多い環境では、再起動の時刻が正時に集中しないよう、サーバーごとに分の値を分けて指定できます。

```
housekeeping.hour=2            #再起動時間(サーバー時間基準、デフォルト:2時)
housekeeping.minute=30         #再起動の分(デフォルト:0)
```

| Item | Description |
|---------------------|--|
| housekeeping.hour | 再起動時刻の時 (hour) 。デフォルト値 2 |
| housekeeping.minute | 再起動時刻の分 (minute) 。デフォルト値 0。0 の場合は従来と同じく、指定した時 (hour) 内に再起動 |

サポートするエージェントバージョンは、Linux・Windowsは2.9.22以上、Unix (AIX・HP-UX・Solaris) は1.4.13以上です。

CPU使用量の保護

CPUの使用量が臨界値を超える場合、WhaTapエージェントは実行速度を自動的に調整してサーバーのCPU可用性を保護します。デフォルトでは非アクティブになっており、必要に応じてアクティブにできます。

```
cpu.limit.enabled=false        #CPU使用量の保護機能を非アクティブにする(デフォルト:false)
cpu.usage.limit=50             #CPU使用量の臨界値(単一コア基準 50%)
```

Windows

Handle使用量の保護

Windows環境では、WhaTapエージェントが使用するHandleの数が臨界点(1000個)を超える場合、自動的に再起動してユーザサーバーの利用可能なHandleを保護します。

```
windows.handle.threshold=1000 # Handle使用量の臨界値(既定値：1000個)
```

ウォッチドッグの通信方式

Windows環境のエージェントは、監視プロセス（ウォッチドッグ）と収集プロセスが互いに状態をやり取りします。この通信にはデフォルトで名前付きパイプ（named pipe）を使用し、パイプへの書き込みが失敗して通信が切断される環境では、ローカルTCPソケット方式に変更できます。

```
housekeeping.rpc.mode=socket #ウォッチドッグの通信方式(デフォルト：pipe)
housekeeping.rpc.port=6601 #socket方式で使用するポート(デフォルト：6601)
```

| Item | Description |
|-----------------------|--|
| housekeeping.rpc.mode | ウォッチドッグの通信方式。socket を指定するとローカルTCPソケットを使用。デフォルトは名前付きパイプ |
| housekeeping.rpc.port | socket 方式で使用するTCPポート。デフォルト値 6601 |

socket 方式はサーバー内部（ローカル）の通信にのみ使用するため、外部のファイアウォールを開放する必要はありません。ただし、指定したポートを他のプログラムが使用していないか確認してください。

Windows性能カウンターの設定

任意のWindows性能カウンターを収集できます。WhaTapのサーバーモニタリング設定ファイルに性能カウンターセット名を追加します。

- 性能カウンターセット名を検索できます。

Windows Powershell

```
Get-Counter -ListSet *
```

- 設定ファイルに性能カウンターセットを追加できます。

Windows Powershell

```
Add-Content -Path "C:\Program Files\WhatapInfra\whatap.conf" -Value "performance.counter.$(Get-Date -uformat %s)=検索する性能カウンターセット名"
```

- 追加した性能カウンターは分析 > メトリクス照会 メニューの カテゴリ `performance_counter_{性能カウンターセット名}` で照会できます。

ⓘ 変更を有効にするには、サーバーを再起動してください。

拡張機能

拡張パックの設定

通常のインストール後に拡張パックの機能を使用するには、構成ファイルを作成し、次のようにエージェントを再起動します。

MySQLサーバーリスト

MySQL/MariaDB モニタリングエージェントが利用可能です。

Web URLの性能チェック

WhaTapインフラエージェントは、与えられたWebアドレスに接続し、接続有無および応答時間を収集します。収集されたWeb URLの性能はカテゴリ `server_webcheck` で確認できます。次のコマンドでチェックするWebアドレスを追加します。URLモニタリングサービスの詳細については、[次の文書](#)を参照してください。

- [Linux Shell](#) Windows Powershell

```
echo "チェックするウェブアドレス" | sudo tee -a /usr/whatap/infra/conf/webcheck.conf
echo "webcheck.enabled=true" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
sudo service whatap-infra restart
```

```
Add-Content -Path "C:\Program Files\WhatapInfra\webcheck.conf" -Value "チェックするウェブアドレス"
Add-Content -Path "C:\Program Files\WhatapInfra\whatap.conf" -Value "webcheck.enabled=true"
Restart-Service "Whatap Infra"
```

Redisインスタンス

WhaTapインフラエージェントは、特定のRedisアドレスに接続し、接続数を含む複数の性能指数を収集します。収集された性能情報は、カテゴリ `server_redis` で確認できます。次のコマンドでチェックするRedisサーバーの接続情報を追加できます。

- [Linux Shell](#) Windows Powershell

```
sudo echo "addr=Redisアドレス:ポート番号" | sudo tee /usr/whatap/infra/conf/redis.conf
sudo echo "password=Redisパスワード" | sudo tee -a /usr/whatap/infra/conf/redis.conf
sudo service whatap-infra restart
```

```
Add-Content -Path "C:\Program Files\WhatapInfra\redis.conf" -Value "addr=Redisアドレス:ポート番号"
Add-Content -Path "C:\Program Files\WhatapInfra\redis.conf" -Value "password=Redisパスワード"
Restart-Service "Whatap Infra"
```

Memcachedインスタンス

WhaTapインフラエージェントは、特定のMemcachedアドレスに接続し、接続数を含む複数の性能指数を収集します。収集された情報は、カテゴリ `server_memcached` で確認できます。次のコマンドでチェックするMemcachedサーバーの接続情報を追加できます。

- [Linux Shell](#) Windows Powershell

```
sudo echo "addr=Memcachedアドレス:ポート番号" | sudo tee /usr/whatap/infra/conf/memcached.conf
sudo echo "password=Memcachedパスワード" | sudo tee -a /usr/whatap/infra/conf/memcached.conf
sudo service whatap-infra restart
```

```
Add-Content -Path "C:\Program Files\WhatapInfra\memcached.conf" -Value "addr=Memcachedアドレス"
Add-Content -Path "C:\Program Files\WhatapInfra\memcached.conf" -Value "password=Memcachedパスワード"
Restart-Service "Whatap Infra"
```

TCPポートモニタリング

ネットワークデーモンの受信ポートが無効になった場合に通知を受け取ることができます。

ホーム画面 > プロジェクトの選択 > アラート通知 > イベント設定 > サーバータブを選択して、+ イベント設定追加ボタンを選択します。

イベント設定

× イベント設定追加

全体 サーバー プロセス

サーバー

題名 * 最大100文字まで入力できます。

▼ 通知種類の選択

☒ サーバー ☐ プロセス ☐ ログ

▼ アラート通知条件

| メトリクス | 条件 | レベル | 持続時間 | 活性化 |
|--------------|---|-------|---------|---|
| 再起動 ① | - | 危険 | - | ☒ |
| 未受信 ① | - | 警告 | 10 分 | ☐ |
| ポート ① | - | 警告 | 1 分 | ☒ |
| ネットワークIOPS ① | 警告 > 45,000 pps 危険 > 50,000 pps | 警告 危険 | 5 分 5 分 | ☒ ☒ |
| ネットワークBPS ① | 警告 > 150,000,000 bps 危険 > 200,000,000 bps | 警告 危険 | 5 分 5 分 | ☒ ☒ |
| ディスクI/O ① | 90% 95% | 警告 危険 | 5 分 5 分 | ☒ ☒ |
| ディスク使用量 ① | 90% 95% | 警告 危険 | 5 分 5 分 | ☒ ☒ |

サーバーリスト ①

サーバー

☐ すべて選択

☐ demo-k8s-master (10.21.1.149)

☐ demo-k8s-worker-01 (10.21.1.229)

☐ demo-k8s-worker-02 (10.21.1.157)

☐ demo-k8s-worker-03 (10.21.1.23)

☐ demo-k8s-worker-04 (10.21.1.210)

☐ dotnet-official-demo (10.21.1.51)

☐ go-official-demo (10.21.1.118)

☐ mysql-official-demo-01 (10.21.1.86)

☐ mysql-official-demo-02 (10.21.1.136)

☐ mysql-official-demo-02 (10.21.1.136)

☐ mysql-official-demo-03 (10.21.1.236)

☐ node-official-demo (10.21.1.98)

☐ python-demo-attack (10.21.1.254)

☐ python-demo-target (10.21.1.43)

☐ rum-official-demo (10.21.1.151)

2 保存

- ① ポート指標のトグルボタンをクリックして、**使用**状態に変更します。
- ② 保存ボタンを選択して保存します。
- 対象サーバーに、次のコマンドを追加します。

Linux Shell Windows Powershell

```
#以下の変数にモニタリング対象IPを指定します。
export TARGET_IP=127.0.0.1
#以下の変数にモニタリング対象ポート番号を指定します。
export TARGET_PORT=80
```



```
echo "tcp.check.$TARGET_PORT=tcp://$TARGET_IP:$TARGET_PORT" |sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

```
#以下の変数にモニタリング対象IPを指定します。
$TARGET_IP="127.0.0.1"
#以下の変数にモニタリング対象ポート番号を指定します。
$TARGET_PORT="80"
Add-Content -Path "C:\Program Files\WhatapInfra\whatap.conf" -Value
"tcp.check.${TARGET_PORT}=tcp://${TARGET_IP}:${TARGET_PORT}"
```

❗ マルチポートモニタリング

複数のポートをモニタリングするためには`whatap.conf`ファイル内の追加設定が必要です。次の例を参考にしてください。

whatap.conf

```
# port 8080, port 80
tcp.check.8080=tcp://127.0.0.1:8080
tcp.check.80=tcp://127.0.0.1:80
```

プロセスFile Descriptor情報の収集

プロセスFile Descriptor情報は、サーバーリスト>サーバー 詳細画面のプロセスウィジェットで確認できます。

• Linux Shell Windows Powershell

```
echo "process.fdcheck=true" |sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

```
# 管理者権限が必要です。
Add-Content -Path "C:\Program Files\WhatapInfra\whatap.conf" -Value "process.fdcheck=true"
```

サーバースペック収集

CPU、MEMORY、DISK、NICの仕様とインストールされたパッケージおよび仮想マシンのメタ情報を収集します。各

カテゴリで、次の内容を確認できます。

- `server_package` : インストールされているパッケージです。
- `server_inventory` : CPU、MEMORY、DISK、NICの仕様です。
- `server_pending_security_update` : Linuxのセキュリティパッチの待機リストです。

- **Linux Shell** Windows Powershell

```
echo "inventory.product.enabled=true" |sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

管理者権限が必要です。

```
Add-Content -Path "C:\Program Files\WhatapInfra\whatap.conf" -Value "inventory.product.enabled=true"
```

Linuxコンテナの性能収集

LinuxコンテナのCPU、MEMORY、DISK、NIC性能を収集します。収集された性能情報は、**カテゴリ** `server_container` で確認できます。

Linux Shell

```
echo "container.enabled=true" |sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

Windowsサーバーサービスの動作状態を収集する

ウィンドウサーバーサービスの運用状態を収集します。収集されたサービスの運用状態は**カテゴリ** `server_windows_service` で確認できます。

Windows Powershell

管理者権限が必要です。

```
Add-Content -Path "C:\Program Files\WhatapInfra\whatap.conf" -Value "winservice.enabled=true"
```

ファイルシステムの収集除外

収集する必要のないファイルシステムを正規表現で指定して除外できます。スナップショットマウントのように使用率が常に100%に近く報告されるファイルシステムを除外すると、不要なアラートとデータを減らせます。

`filesystem.exclude.pattern` オプションに正規表現を入力してください。マウントポイントまたはデバイス名が正規表現と一致するファイルシステムは、`server_disk` と `infra_filesystem` の2つのカテゴリの両方から除外します。

whatap.conf

```
filesystem.exclude.pattern=^/snap/
```

| Item | Description |
|---|--|
| <code>filesystem.exclude.pattern</code> | 収集から除外するファイルシステムのマウントポイント・デバイス名の正規表現。デフォルト値は空で、空の場合は除外しません |

❗ 正規表現が誤っている場合、エージェントはエラーをログに残し、オプションを適用しません。ファイルシステムの収集自体は継続して動作します。

サポートするエージェントバージョンは、Linux・Windowsは2.9.23以上、Unix（AIX・HP-UX・Solaris）は1.4.14以上です。設定を変更した後は、エージェントを再起動してください。

ファイルモニタリング

ファイルシステム上に存在または存在する可能性のあるファイルおよびディレクトリをモニタリングできます。

Linux Shell Windows Powershell

```
echo "filecheck.enabled=true" |sudo tee -a /usr/whatap/infra/conf/whatap.conf
echo "モニタリングするファイルまたはディレクトリのフルパス" |sudo tee -a /usr/whatap/infra/conf/filesystem.conf
```

```
Add-Content -Path "C:\Program Files\WhatapInfra\whatap.conf" -Value "filecheck.enabled=true"
Add-Content -Path "C:\Program Files\WhatapInfra\filesystem.conf" -Value "モニタリングするファイルまたはディレクトリの全
```

体パス"

監視パスの日付置換

監視パスに日付形式の文字を入れると、エージェントが収集時点の日付に置換して監視します。日付ごとにファイル名が変わるログのように、パスが毎日変わる対象を1つの設定で監視できます。ログ監視機能と同じ方式です。

filesystem.conf

```
/var/log/app/access_%Y%m%d.log
```

| Item | Description |
|------|-------------|
| %Y | 年（4桁） |
| %m | 月（2桁） |
| %d | 日（2桁） |
| %H | 時（2桁） |

日付が変わって監視対象のパスが変わった場合、以前のパスの状態と比較せず、新たに監視を開始します。

サポートするエージェントバージョンは、Linux・Windowsは2.9.23以上、Unix（AIX・HP-UX・Solaris）は1.4.14以上です。

WhaTapエージェントのログオプション

ログの保存場所

WhaTapエージェントログ(`whatap_infrad.log`、`whatap_infra.log`、`whatap_infrad.fork.stdout.log`)のパスを変更します。指定パスがない場合は、WhaTapエージェントは指定パスの作成を試みます。エージェント2.0.6バージョン以降に対応されています。

- [Linux Shell](#) Windows Powershell

```
echo "agent.log.prefix=変更するディレクトリ" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

```
Add-Content -Path "C:\Program Files\WhatapInfra\whatap.conf" -Value "agent.log.prefix=変更するディレクトリ"
```

❗ Windowsの場合、パスの区切り文字を `\\` と入力できます。

ログ出力制御オプション

サーバーモニタリングエージェントのログは、デフォルトで `/var/log` ディレクトリ配下に保存されます。以下のオプションを使用して、ログファイルのサイズ上限およびバックアップファイル数を調整できます。

• Linux / Windows Unix (AIX, HPUX, Solaris)

- Linux / Windows
 - agent.log.size
 - 既定値：10（単位：MB）
 - agent.log.backupfile
 - 既定値：2（単位：個数）
- Unix (AIX、HPUX、Solaris)
 - log.size
 - 既定値：4（単位：MB）
 - log.backup
 - 既定値：3（単位：個数）
- AIX 追加ログオプション（errpt 収集ログ）
 - aix.errpt.log.size=4
 - 既定値：4（単位：MB）
 - aix.errpt.log.backup=3
 - 既定値：3（単位：個数）

Netstatモニタリング

netstatコマンドが入力された場合、1分間隔で収集され、カテゴリ `server_netstat` (netstat connection統計)、`server_netstat_s` (netstat -sコマンドの結果)がアップロードされます。

- Linux Shell Windows Powershell

```
echo "netstats.enabled=true" |sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

```
Add-Content -Path "C:\Program Files\WhatapInfra\whatap.conf" -Value "netstats.enabled=true"
```

ユーザースクリプトモニタリング

- Linux Shell Windows Powershell

Linuxサーバーで実行可能なユーザースクリプトを定期的に行って結果をアップロードします。ユーザースクリプトモニタリング機能は、決められたサイクルに従ってスクリプトを実行し、その結果を収集サーバーにアップロードします。30秒周期間隔でスクリプトを実行して結果を収集します。

データはスクリプト実行が完了した時点に基づいて収集され、実行するスクリプト内容によって実際の収集時刻とデータ反映時刻には一部差が生じることがあります。次の例を参考にして、ユーザースクリプトを作成します。

1. スクリプトを次のように作成して実行してください。

Linux Shell

```
#!/bin/bash

urls=("https://www.whatap.io" "https://blog.whatap.io" "https://service.whatap.io")

for url in ${urls[*]}; do

echo "M $url url $url"
curl -w @- -o /dev/null -s "$url" <<'EOF'
M %{url_effective} url %{url_effective}\n
H %{url_effective} time_namelookup %{time_namelookup}\n
```

```

H %{url_effective} time_connect %{time_connect}\n
H %{url_effective} time_appconnect %{time_appconnect}\n
H %{url_effective} time_pretransfer %{time_pretransfer}\n
H %{url_effective} time_redirect %{time_redirect}\n
H %{url_effective} time_starttransfer %{time_starttransfer}\n
H %{url_effective} time_total %{time_total}\n
EOF

done

```

2. 次のように出力されるか確認してください。

Linux Shell

```

$ ./curl.sh
M https://www.whatap.io/ url https://www.whatap.io/
H https://www.whatap.io/ time_namelookup 0.007289
H https://www.whatap.io/ time_connect 0.010702
H https://www.whatap.io/ time_appconnect 0.033637
H https://www.whatap.io/ time_pretransfer 0.033831
H https://www.whatap.io/ time_redirect 0.000000
H https://www.whatap.io/ time_starttransfer 0.043230
H https://www.whatap.io/ time_total 0.043312
M https://blog.whatap.io/ url https://blog.whatap.io/
H https://blog.whatap.io/ time_namelookup 0.000000
H https://blog.whatap.io/ time_connect 0.000000
H https://blog.whatap.io/ time_appconnect 0.000000
H https://blog.whatap.io/ time_pretransfer 0.000000
H https://blog.whatap.io/ time_redirect 0.000000
H https://blog.whatap.io/ time_starttransfer 0.000000
H https://blog.whatap.io/ time_total 0.005654
M https://service.whatap.io/ url https://service.whatap.io/
H https://service.whatap.io/ time_namelookup 0.004296
H https://service.whatap.io/ time_connect 0.007282
H https://service.whatap.io/ time_appconnect 0.038404
H https://service.whatap.io/ time_pretransfer 0.038607
H https://service.whatap.io/ time_redirect 0.000000
H https://service.whatap.io/ time_starttransfer 0.055226
H https://service.whatap.io/ time_total 0.055307

```

3. スクリプトの正常収集を確認し、次のようにWhaTapサーバーのモニタリングエージェントにスクリプトを登録してください。

Linux Shell

```
export USER_SCRIPT=実行するユーザースクリプトのフルパス
suco chmod +x $USER_SCRIPT
sudo mkdir /usr/whatap/infra/ext/
sudo cp -r $USER_SCRIPT /usr/whatap/infra/ext/
export RUNAS_USER=ユーザースクリプトを実行するアカウント、rootアカウントを除く
sudo WHATAP_HOME=/usr/whatap/infra/conf /usr/whatap/infra/whatap_infrad --user=$RUNAS_USER init-script
sudo service whatap-infra restart
```

収集されたデータは、**分析 > メトリクスチャートのカテゴリ** `server_ext_フォルダ_実行スクリプト` で確認できます。

Windowsサーバーで実行可能なユーザースクリプトを定期的に行って結果をアップロードします。ユーザースクリプトモニタリング機能は、決められたサイクルに従ってスクリプトを実行し、その結果を収集サーバーにアップロードします。30秒周期間隔でスクリプトを実行して結果を収集します。

データはスクリプト実行が完了した時点に基づいて収集され、実行するスクリプト内容によって実際の収集時刻とデータ反映時刻には一部差が生じることがあります。次の例を参考にして、ユーザースクリプトを作成します。

• BAT PowerShell

BATスクリプト実行

1. スクリプトを次のように作成して実行してください。

BAT

```
@echo off
setlocal enabledelayedexpansion

set urls=https://www.whatap.io https://blog.whatap.io https://service.whatap.io

for %%u in (%urls%) do (
    echo M %%u url %%u

    rem Use curl to fetch the URL and get the total time taken for the request
```



```

for /f "tokens=*" %%i in ('curl -o nul -s -w "M %{url_effective} url %{url_effective}" %%u') do (
    echo %%i
)

rem Measure the start time
set startTime=!time!

rem Perform the curl request and measure the end time
curl -o nul -s %%u

set endTime=!time!

rem Parse the start time
for /F "tokens=1-4 delims=.,," %%a in ("!startTime!") do (
    set /A "startH=%%a, startM=%%b, startS=%%c, startMS=%%d"
)

rem Parse the end time
for /F "tokens=1-4 delims=.,," %%a in ("!endTime!") do (
    set /A "endH=%%a, endM=%%b, endS=%%c, endMS=%%d"
)

rem Calculate the elapsed time in milliseconds
set /A "elapsedMS=(endH*3600000 + endM*60000 + endS*1000 + endMS) - (startH*3600000 + startM*60000 + startS*1000 + startMS)"

rem Convert milliseconds to seconds and milliseconds part
set /A "elapsedSec=elapsedMS/1000"
set /A "elapsedMSPart=elapsedMS %% 1000"

echo H %%u time_total !elapsedSec!.!elapsedMSPart!
)

endlocal

```

2. 次のように出力されるか確認してください。

BAT

```
>webcheck.bat
M https://www.whatap.io url https://www.whatap.io
M https://www.whatap.io/ url https://www.whatap.io/
H https://www.whatap.io time_total 0.38
M https://blog.whatap.io url https://blog.whatap.io
M https://blog.whatap.io/ url https://blog.whatap.io/
H https://blog.whatap.io time_total 0.1
M https://service.whatap.io url https://service.whatap.io
M https://service.whatap.io/ url https://service.whatap.io/
H https://service.whatap.io time_total 0.922
```

3. スクリプトの正常収集を確認し、次のようにWhaTapサーバーのモニタリングエージェントにスクリプトを登録してください。

BAT

```
cd "\Program Files\WhatapInfra"
whatap_infra.exe init-script
sc stop "Whatap Infra"
sc start "Whatap Infra"
```

PowerShellスクリプト実行

1. スクリプトを次のように作成して実行してください。

PowerShell

```
$urls = @("https://www.whatap.io", "https://blog.whatap.io", "https://service.whatap.io")

# Hide progress bar
$ProgressPreference = 'SilentlyContinue'

foreach ($url in $urls) {
    Write-Output "M $url url $url"

    $startTime = Get-Date
    try {
```

```

$response = Invoke-WebRequest -Uri $url -UseBasicParsing
$endTime = Get-Date

$timeTotal = ($endTime - $startTime).TotalSeconds

Write-Output "M $($response.BaseResponse.ResponseUri) url $($response.BaseResponse.ResponseUri)"
Write-Output ("H {0} time_total {1}" -f $url, $timeTotal)
} catch {
    Write-Output "Failed to access $url"
}
}

```

2. 次のように出力されるか確認してください。

PowerShell

```

> .\webcheck.ps1
M https://www.whatap.io url https://www.whatap.io
M url
H https://www.whatap.io time_total 0.376979
M https://blog.whatap.io url https://blog.whatap.io
Failed to access https://blog.whatap.io
M https://service.whatap.io url https://service.whatap.io
Failed to access https://service.whatap.io

```

3. スクリプトの正常収集を確認し、次のようにWhaTapサーバーのモニタリングエージェントにスクリプトを登録してください。

PowerShell

```

cd "\Program Files\WhatapInfra"
.\whatap_infra.exe init-script
Restart-Service "Whatap Infra"

```

サーバー時間同期化モニタリング

ⓘ 事前確認

- OS : Linux
- WhaTapサーバーモニタリングエージェントバージョン : 2.5.4以降

次のオプションを使用してサーバー時間の同期化(NTP) モニタリング機能を活性化することができます。

```
echo "ntp.enabled=true" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

追加指標の案内

サーバー時間の同期化モニタリング機能を活性化する時に追加されるメトリクスは以下の通りです。

server_ntpq

Tags

| タグ名 | 説明 | 備考 |
|--------|---|----|
| refid | 当該リモート(<code>remote</code>)の時間同期化ソースを意味します。 | - |
| remote | ホストが時間同期化を実行する対象サーバーを意味します。 | - |

Fields

| フィールド名 | 単位 | 説明 | 備考 |
|--------|----|---|----|
| delay | ms | サーバーが送信したクエリへのレスポンスとして返信パケットを返すのにかった時間を意味します。 | - |

| フィールド名 | 単位 | 説明 | 備考 |
|-------------|--------|--|----|
| jitter | - | 2つのサンプル間のオフセット測定の違いから推定した誤差の境界値を意味します。 | - |
| offset | ms | サーバー設定時間とクライアント設定時間の差を意味します。 | - |
| poll | second | ntp.confファイルで minpoll 値として定義されたリモートホストへのポーリング間隔を意味します。 | - |
| reach | - | サーバーに到達する試みがどれほど成功しているかを確認できます。2^0の位置に最新のクエリの成否を記録し、8ビットシフトレジスタで動作します。 | - |
| st | - | リモートホストのストラタムレベルを意味します。 | - |
| sync_client | - | 1：同期化サーバーが存在します。 | - |
| | | 0：同期化サーバーが存在しません。 | |
| t | - | 使用可能なタイプは次のとおりです。 | - |
| | | l：ローカル(例：GPS時計) | |
| | | u：ユニキャスト(一般的なタイプ) | |
| | | m：マルチキャスト | |
| | | b：ブロードキャスト | |
| when | second | リモートホストの応答から過ぎた時間(秒)を意味します。 | - |

Linuxシステムログモニタリング

Linuxシステムログをリアルタイムでアップロードして、障害発生時点のログを確認できます。収集対象のログファイルは次のとおりです。

- `/var/log/syslog`
- `/var/log/messages`

設定方法は次のとおりです。

Linux Shell

```
echo "systemlog.enabled=true" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

ログモニタリングプラグイン

ランダムなログを収集できます。次の設定の場合、エージェントの再起動が必要です。

Linux Shell

- 基本インストール

Linux Shell

```
export LOGFILES=/some/path/file1,/some/other/file2
echo "logsink.files=$LOGFILES" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

- カテゴリ付きインストール

Linux Shell

```
1 cd /usr/whatap/infra
2 sudo mkdir extension
3
4 cat <<EOL | sudo tee extension/logsink.conf >> /dev/null
5 [[inputs.logsink]]
6   category = "serverlog"
7   ## ログ発生量統計の別途データとしての送信有無
8   stats_enabled = true
9   ## 対数発生量の統計カテゴリ
10  stats_category = "logsink_stats"
11  ## ログファイルパス(path)にアスタリスク(*)が含まれ、除外するログ非対象ファイル名を設定
```

```

12  excludeNames = [ ".gz", ".zip" ]
13  [[inputs.logsink.file]]
14  ## ログファイルの指定時、日付パターン(strftime.org)指定可能
15  path = "/some/path/%Y-%m-%d/.log"
16  disabled = false
17  encoding = "utf-8"
18
19  [[inputs.logsink.file]]
20  path = "/some/other/log"
21  disabled = false
22  encoding = "utf-8"
23
24  [[inputs.logsink.file]]
25  ## 行単位ログで該当キーワードを検索する時、以前のログにマージ
26  nowrap_keywords = ["Caused by:", "Test"]
27
28  [[inputs.logsink.file]]
29  ## プロジェクトコード及びプロジェクトライセンスの入力時、ログを同じリージョンの希望するプロジェクトに転送可
   能
30  # pcode = プロジェクトコード
31  # license = "プロジェクトライセンス"
32
33  [[inputs.logsink.file]]
34  # whatap_host_ip = "収集サーバーIP1/収集サーバーIP2"
35  # whatap_host_port = 6600
36
37  [[inputs.logsink.file]]
38  path = "/tmp/mixed.log"
39  disabled = false
40  encoding = "utf-8"
41  ## [{"A":1,"B":2},{ "C":3,"D":4},...] 形態をそれぞれのログに分離できる{"A":1,"B":2} {"C":3,"D":4}
42  multiline_pattern = "simple_json_array"
43  EOL
44
45  sudo service whatap-infra restart

```

Windows Powershell

- 基本インストール

Windows Powershell

```
$LOGFILES="c:\\whatap\\logs\\%Y-%m-%d\\*.log,c:\\whatap\\logs\\*.log"
Add-Content "c:\\Program Files\\WhatapInfra\\whatap.conf" -Value "logsink.files=$LOGFILES"
```

- カテゴリ付きインストール

Windows Powershell

```
1 # 管理者権限が必要
2 New-Item -type "Directory" -Path "C:\\Program Files\\WhatapInfra\\extension"
3
4 $contentToAdd = @"
5 [[inputs.logsink]]
6 category = "serverlog"
7 ## ログ発生量統計の別途データとしての送信有無
8 stats_enabled = true
9 ## 対数発生量の統計カテゴリ
10 stats_category = "logsink_stats"
11 ## ログファイルパス(path)にアスタリスク(*)が含まれ、除外するログの非対象ファイル名を設定
12 excludeNames = [ ".gz", ".zip" ]
13 [[inputs.logsink.file]]
14 ## ログ ファイルの指定時、日付パターン(strftime.org)指定可能
15 path = "c:\\whatap\\logs%Y-%m-%d_.log"
16 disabled = false
17 encoding = "utf-8"
18
19 [[inputs.logsink.file]]
20 ## 行単位ログで該当キーワードを検索する時、以前のログにマージ
21 nowrap_keywords = ["Caused by:", "Test"]
22
23 [[inputs.logsink.file]]
24 ## プロジェクトコード及びプロジェクトライセンスの入力時、ログを同じリージョンの希望するプロジェクトに転送可
   能
25 # pcode = プロジェクトコード
```



```

26 # license = "プロジェクトライセンス"
27
28 [[inputs.logsink.file]]
29 # whatap_host_ip = "収集サーバーIP1/収集サーバーIP2"
30 # whatap_host_port = 6600
31
32 [[inputs.logsink.file]]
33 path = "/tmp/mixed.log"
34 disabled = false
35 encoding = "utf-8"
36 ## [{"A":1,"B":2},{ "C":3,"D":4},...] 形態をそれぞれのログに分離することができる。
37 {"A":1,"B":2} {"C":3,"D":4}
38 multiline_pattern = "simple_json_array"
39
40 "@
41
42 New-Item -path "C:\Program Files\WhatapInfra\extension" -name "logsink.conf" -type "file" -value $contentToAdd
  -Force
43
44 Restart-Service "Whatap Infra"

```

オプション設定

- **stats_enabled** : 収集ステータスデータの収集有無を設定します。(既定値: `false`)
 - `true` に設定する必要がある、**stats_category** で設定したカテゴリ（`logsink_stats`）に統計データが生成されます。
- **stats_category** : 収集ステータスデータを保存するメトリクスカテゴリを設定します。 `logsink_stats` に設定する必要があります。統計データのフィールドは次のとおりです。

保存される統計データフィールド: `file` `checkInterval` `encoding` `filepos` `checkedLocalTime`
`lastupdatedLocalTime` `fileSize` `error` `firstCheck` `transferBytes`

- **excludeNames** : ログファイルのパス（`path`）にアスタリスク（`*`）が含まれている場合、ログ収集対象外のファイル名を設定して除外することができます。カンマ（`,`）を区切り文字として使用することで、複数の値を設定できます。

Example

```
excludeNames = [ ".gz", ".zip" ]
```

- **nowrap_keywords** : 行単位のログ検索時に、このオプションで指定されたキーワードが検出されると、前のログと結合されます。
- **pcode** : ログを送信する同じリージョンのプロジェクトコードを入力します。
- **license** : ログを送信する同じリージョンのプロジェクトのライセンスコードを入力します。

❗ **pcode**、**license** オプションの場合、サーバーエージェント2.7.4バージョン以降に対応します。

Windowsイベントログのオプション設定

Windowsイベントログ収集時、次のようにオプションを設定することができます。

```

1  # 管理者権限が必要
2  New-Item -type "Directory" -Path "C:\Program Files\WhatapInfra\extension"
3
4  $contentToAdd = @"
5  [[inputs.win_eventlog]]
6      category = "win_event_log"
7      stats_category = "win_event_log_stats"
8      stats_enabled = true
9      enabled = true
10 [[inputs.win_eventlog.file]]
11     #true | false
12     enabled = true
13     # Application, Security, Setup, System, ForwardedEvents
14     file = "Application"
15     #1: Information, 2: Warning 3: Error 4: Audit Success 5 Audit Fail
16     #event_type =
17     #event_id
18     #event_id =
19     #event source name
20     #source_name = ""
21     #プロジェクトコード及びプロジェクトライセンスの入力時、ログを同じリージョンの希望するプロジェクトに転送可能

```

```

22     #pcode = プロジェクトコード
23     #license = "プロジェクトライセンス"
24     #whatap_host_ip = "収集サーバーIP1/収集サーバーIP2"
25     #whatap_host_port = 6600
26
27     "@
28
29     New-Item -path "C:\Program Files\WhatapInfra\extension" -name "win_eventlog.conf" -type "file" -value $contentToAdd
30     -Force
31
32     Restart-Service "Whatap Infra"

```

- カテゴリ指定(`category`) 必須

例) `win_event_log`

- 統計カテゴリ指定(`stats_category`) 必須

例) `win_event_log_stats`

- 統計カテゴリOn/Off(`stats_enabled`) 必須

例) `true` または `false`

- 収集機能On/Off(`enabled`) 必須

例) `true` または `false`

- ファイル別収集機能On/Off(`enabled`) 必須

例) `true` または `false`

- ファイル(`file`) 必須

例) `Application`、`Security`、`Setup`、`System`、`Forwarded`

- イベントタイプ(`event_type`) 非必須

例) `1`、`2`、`3`、`4`、`5`

① イベントタイプ

①

1. Information
2. Warning
3. Error
4. Audit Success
5. Audit Fail

- イベントID(`event_id`) 非必須
- イベントソース名(`source_name`) 非必須
- プロジェクトコード(`pcode`) 非必須
- プロジェクトライセンス(`license`) 非必須

❗ エージェント対応バージョン

- ウィンドウイベントログ収集の場合、サーバーエージェント2.5.2バージョン以降に対応します。
- ウィンドウイベントログオプションの中で `pcode` 、 `license` オプションの場合、サーバーエージェント2.7.4バージョン以降に対応します。

ログ複数ファイルの指定と分離

複数のファイル指定

複数のログファイルを同じカテゴリに設定するには、各ログファイルのパスを `[[inputs.logsink.file]]` 項目に追加して、`path` 設定により、ファイルパスを指定します。また、`category`、`stats_enabled`、`stats_category` などのオプションを使用して、ログ発生量の統計設定などの付加的な設定が可能です。

`/root/test1` および `/root/test2` ファイルを同じカテゴリ (`serverlog`) に指定した例です。

```
[[inputs.logsink]]
  category = "serverlog"
  stats_enabled = true
```

```
stats_category = "logsink_stats"
excludeNames = [ ".gz", ".zip" ]
```

```
[[inputs.logsink.file]]
```

```
path = "/root/test1"
```

```
disabled = false
```

```
encoding = "utf-8"
```

```
[[inputs.logsink.file]]
```

```
path = "/root/test2"
```

```
disabled = false
```

```
encoding = "utf-8"
```

❗ category、stats_enabled、stats_category、nowrap_keywords などのオプションに関する詳細は、[オプション設定](#) を参照してください。

この例は、**ログTail** メニューで次のように確認できます。

| serverlog | | ▼ | | ▼ | |
|-----------|--------|------------|--------------|------------------|--|
| ▼ | oname | 時間 | | 内容 | |
| ▼ | APPSVR | 2024-10-11 | 18:14:30.325 | file /root/test1 | pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709
kdjfhakdhgldkjggha;dfghad;fkjggha;dfkjggha;dfgjha;fkghj;fgjh |
| ▼ | APPSVR | 2024-10-11 | 18:14:30.325 | file /root/test1 | pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709
kdjfhakdhgldkjggha;dfghad;fkjggha;dfkjggha;dfgjha;fkghj;fgjh |
| ▼ | APPSVR | 2024-10-11 | 18:14:30.325 | file /root/test1 | pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709
kdjfhakdhgldkjggha;dfghad;fkjggha;dfkjggha;dfgjha;fkghj;fgjh |
| ▼ | APPSVR | 2024-10-11 | 18:14:30.325 | file /root/test1 | pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709
kdjfhakdhgldkjggha;dfghad;fkjggha;dfkjggha;dfgjha;fkghj;fgjh |
| ▼ | APPSVR | 2024-10-11 | 18:14:30.325 | file /root/test1 | pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709
kdjfhakdhgldkjggha;dfghad;fkjggha;dfkjggha;dfgjha;fkghj;fgjh |
| ▼ | APPSVR | 2024-10-11 | 18:14:30.325 | file /root/test1 | pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709
kdjfhakdhgldkjggha;dfghad;fkjggha;dfkjggha;dfgjha;fkghj;fgjh |
| ▼ | APPSVR | 2024-10-11 | 18:14:40.326 | file /root/test2 | pcode 34 oname APPSVR agenttime 1728638079521 oid 1988910709
sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbvcvmbn.bcmn |

ファイル分離

異なるカテゴリにログファイルを割り当てるには、`logsink{数字}.conf` ファイルをそれぞれ作成し、各ファイルの `category` 項目に異なる値を設定してください。

`logsink.conf` と `logsink1.conf` を使用して、異なるログカテゴリを設定した例です。

logsink.conf

```
# cat logsink.conf
[[inputs.logsink]]
  category = "serverlog1"
  stats_enabled = true
  stats_category = "logsink_stats"
  excludeNames = [ ".gz", ".zip" ]

[[inputs.logsink.file]]
  path = "/root/test1"
  disabled = false
  encoding = "utf-8"
```

logsink1.conf

```
#cat logsink1.conf
[[inputs.logsink]]
  category = "serverlog2"
  stats_enabled = true
  stats_category = "logsink_stats"
  excludeNames = [ ".gz", ".zip" ]

[[inputs.logsink.file]]
  path = "/root/test2"
  disabled = false
  encoding = "utf-8"
```

❗ `category`、`stats_enabled`、`stats_category`、`nowrap_keywords` などのオプションに関する詳細は、[オプション設定](#) を参照してください。

この例は、**ログTail**メニューで次のように確認できます。

| 検索条件 | | 絞り込み | |
|----------|--------|-------------------------|--|
| All logs | | 絞り込み条件 | |
| ▼ | oname | 取得日時 | ログ内容 |
| ▼ | APPSVR | 2024-10-11 18:20:55.084 | file /root/test1 pcode 34 oname APPSVR agenttime 1728638454313 oid 1988910709 category serverlog1
kdjfhakdhglfdkjg ha,dfghad;fkjg ha;dfkjg ha;dfgjha;fkjgh;fgjh |
| ▼ | APPSVR | 2024-10-11 18:20:55.087 | file /root/test1 pcode 34 oname APPSVR agenttime 1728638454313 oid 1988910709 category serverlog1
kdjfhakdhglfdkjg ha,dfghad;fkjg ha;dfkjg ha;dfgjha;fkjgh;fgjh |
| ▼ | APPSVR | 2024-10-11 18:21:05.103 | file /root/test2 pcode 34 oname APPSVR agenttime 1728638464315 oid 1988910709 category serverlog2
sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbcvmbn.bcmn |
| ▼ | APPSVR | 2024-10-11 18:21:05.104 | file /root/test2 pcode 34 oname APPSVR agenttime 1728638464315 oid 1988910709 category serverlog2
sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbcvmbn.bcmn |
| ▼ | APPSVR | 2024-10-11 18:21:05.104 | file /root/test2 pcode 34 oname APPSVR agenttime 1728638464315 oid 1988910709 category serverlog2
sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbcvmbn.bcmn |
| ▼ | APPSVR | 2024-10-11 18:21:05.104 | file /root/test2 pcode 34 oname APPSVR agenttime 1728638464315 oid 1988910709 category serverlog2
sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbcvmbn.bcmn |
| ▼ | APPSVR | 2024-10-11 18:21:05.104 | file /root/test2 pcode 34 oname APPSVR agenttime 1728638464315 oid 1988910709 category serverlog2
sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbcvmbn.bcmn |

GPU機能

以下は、GPUモニタリング機能を有効にするためのエージェントの対応環境およびGPUオプションの案内です。

GPUモニタリング対応環境

基本的に `nvidia-smi` を利用してパフォーマンスデータおよびインベントリ情報を収集できますが、`nvidia-dcgm` がインストールされている場合は、追加のメトリクスも収集可能です。`nvidia-dcgm` がインストールされた環境では、`nvidia-dcgm` サービスが有効化されている必要があります。

- `systemctl status nvidia-dcgm` コマンドを使用して、`nvidia-dcgm` サービスが正常に稼働しているかを確認してください。
- 収集可能なメトリック項目は、今後も継続的に追加される予定です。

収集ツール別のメトリクス項目の詳細は[GPUメトリクス](#)を参照してください。

GPU機能

GPUインベントリおよびGPUパフォーマンスサマリー機能を使用するには、以下のエージェントバージョン以上へのアップデートおよび設定が必要です。

✔ サポートバージョン

Linux 最小 2.9.3、推奨 2.9.16 以上

- Amazon Linux, RHEL, Fedora, Oracle Linux, CentOS, Rocky Linux, SUSE

```
sudo yum update whatap-infra
```

- Debian, Ubuntu

```
sudo apt-get update
```



```
sudo apt-get install whatap-infra
```

GPUオプション

GPUインベントリ機能を有効にするには、以下のオプションを有効にする必要があります。

- **nvidiaiav2.enabled** Boolean

既定値： false

NVIDIA GPUメトリクス収集オプションで、物理GPU構成情報およびリソース使用量情報を収集します。

- **nvidiaiav2.mig.enabled** Boolean

既定値： false

NVIDIA GPU MIG関連のメトリクス収集オプションで、MIG構成情報およびリソース使用量情報を収集します。

nvidiaiav2.enabled オプションが true に設定されている必要があります。

- **nvidiaiav2.proc.enabled** Boolean

既定値： false

NVIDIA GPU割り当てプロセス情報の収集オプションです。**nvidiaiav2.enabled** オプションが true に設定されている必要があります。

- **nvidiaiav2.dcp.enabled** Boolean

既定値： true

NVIDIA DCP（Data Center Profiling）メトリクス収集オプションです。**nvidiaiav2.enabled** オプションが true に設定されている必要があります。

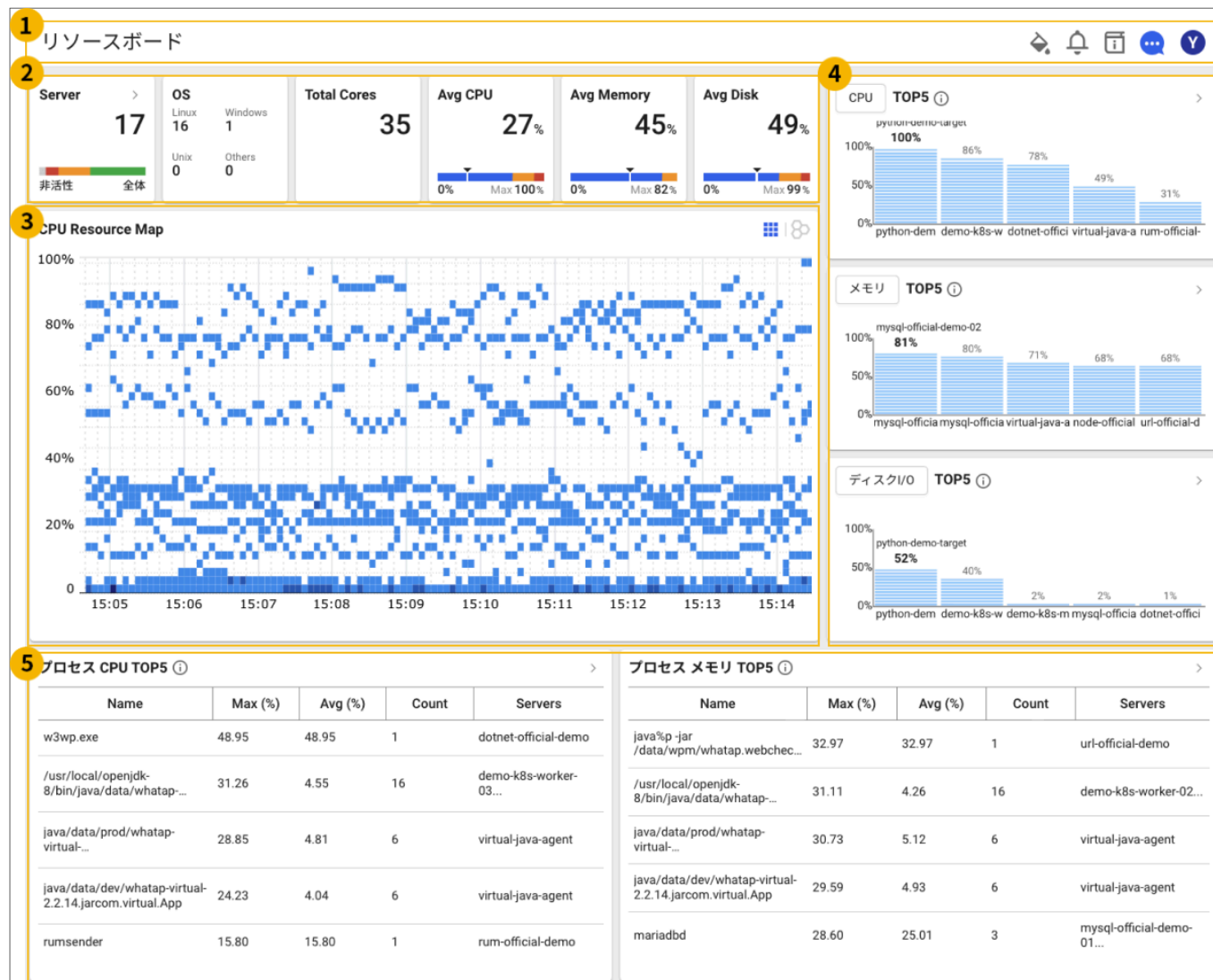
- **nvidiaiav2.interval.sec**

既定値： 30秒

NVIDIAメトリクス収集間隔を設定します。

リソースボード

WhaTapモニタリングサービスの初期画面でプロジェクトを選択した後、**ダッシュボード** > **リソースボード**を選択します。



リソースボードから1つのプロジェクトに登録されているすべてのサーバーをモニタリングできます。

プロジェクト内のすべてのサーバーの概要とリアルタイムのリソース使用状況の変化を確認できる **CPU Resource Map** を提供します。全体リソース、CPU、メモリ、プロセス使用率の **Top 5** を表示します。リソースボードを通じて、トラ

ブルの状況をすぐ把握し、対応できます。

1 固定メニュー

-  テーマ：現在のページのテーマを変更できます。デフォルトはLightモードです。
-  リアルタイムアラート：最近発生したイベントを確認できます。切り替えメニューをクリックしてブラウザ通知をオンまたはオフにすることができます。
-  顧客サポート：オンラインで顧客サポートをご利用頂けます。
-  プロフィールアイコン：右端のアイコンを選択します。アカウント管理、組織生成、組織管理、ユーザー言語を選択できる機能を提供します。

2 情報パネル

プロジェクトに登録されているすべてのサーバー概要メトリクスを提供します。10秒単位で更新されます。

• Server

全体のサーバー数とトラブルのあるサーバーの数を提供します。領域を選択するとサーバーリスト ページに移動します。

- 例外状態：危険、警告
- 正常なサーバー：通常, 非活性

• OS

プロジェクト内のlinuxとWindowsOSの数です。

• Total Cores

全体のサーバーのコア(vCPU) の合計です。

• Avg CPU

全体のサーバーのCPU平均使用率(%)です。下部のゲージは、平均値、最大値、最小値を示します。

• Avg Memory

全体のサーバーのメモリ平均使用率(%)です。下部のゲージは、平均値、最大値、最小値を示します。

- Avg Disk

全体のサーバーのディスクデバイスの平均使用率(%)です。下部のゲージは、平均値、最大値、最小値を示します。

3 CPU Resource Map

全体のサーバーのCPU使用量を示す分布図です。10分間のデータを表示し、10秒ごとに更新されます。セルの色が濃いほどその領域のリソース使用量に該当するサーバーの数が多いことを意味します。

- 詳細情報提供

セル領域をドラッグすると、詳細情報が表示されます。



- サーバリストは、範囲内で収集されたデータの最大値でソートされます。
- 基本の5つのサーバーが選択され、選択されたサーバーの使用状況の傾向をマルチラインチャートで表示します。
- リフレッシュボタンをクリックすると、現時点のデータに手動で更新できます。

❗ マルチラインチャート

1つのチャートに複数の線を表示するチャートです。

4 リソースイコライザー

CPU、メモリ、ディスクI/O、ディスクIOPSの上位5つのサーバーの一覧をリアルタイムで表示します。

例えば、Disk I/O(%) メトリクスは、5秒間のディスク使用率を示します。Disk I/O(%)が80%を超えると、システムの性能に影響を与える可能性があります。警告となる既定値は 90%です。Disk I/O(%)が100%の場合、ディスクが常時動作していることを意味します。

- イコライザーチャート領域を選択すると、対象のサーバー 詳細ページに移動します。
- > ボタンを選択するとリソースイコライザページに移動します。すべてのサーバーに対するリアルタイム使用量が確認できます。

5 Process Top 5

CPU、メモリの最大占有率による上位5つのプロセス一覧を提供します。 > ボタンを選択すると、次のようにサーバー全体のプロセスリスト一覧が確認できます。

プロセスリスト

Process Name, User

| 名前 | ユーザー | エージェント名 | 数 | CPU | メモリ | IO |
|-------------------|-----------------------|----------------------|---|-------|-------|----|
| java | root | demo-k8s-worker-04 | 6 | 66.8% | 17.1% | 0% |
| w3wp.exe | IIS APPPOOL\smarts... | dotnet-official-demo | 1 | 49.4% | 17% | 0% |
| java | root | demo-k8s-worker-02 | 7 | 29.1% | 30% | 0% |
| java | root | demo-k8s-worker-02 | 7 | 29.1% | 30.7% | 0% |
| java | whatap | virtual-java-agent | 6 | 28.8% | 29.7% | 0% |
| java | whatap | virtual-java-agent | 6 | 26.6% | 30.9% | 0% |
| rumsender | root | rum-official-demo | 1 | 20% | 2.4% | 0% |
| node /home/ubun | ubuntu | node-official-demo | 3 | 16.4% | 19.6% | 0% |
| rumstats | root | rum-official-demo | 1 | 9.5% | 4% | 0% |
| w3wp.exe | IIS APPPOOL\demo4... | dotnet-official-demo | 1 | 6.8% | 24% | 0% |
| whatap_dotnet.exe | NT AUTHORITY\SYS... | dotnet-official-demo | 1 | 5.9% | 0.4% | 0% |
| whatap_agent | root | go-official-demo | 4 | 5.6% | 0.7% | 0% |
| node.exe | EC2AMAZ-NO1BAVA... | dotnet-official-demo | 1 | 4.6% | 0.5% | 0% |
| http_server | root | go-official-demo | 2 | 3.2% | 0.9% | 0% |
| grpc_server | root | go-official-demo | 2 | 2.5% | 0.8% | 0% |
| sqlservr.exe | NT SERVICE\MSSQL... | dotnet-official-demo | 1 | 2.3% | 5.1% | 0% |
| kubelet | root | demo-k8s-master | 1 | 2% | 1.7% | 0% |
| cadvisor_helper | root | demo-k8s-worker-02 | 1 | 1.8% | 0.6% | 0% |
| kuber | root | go-official-demo | 1 | 1.8% | 0.6% | 0% |
| conhost.exe | EC2AMAZ-NO1BAVA... | dotnet-official-demo | 2 | 1.6% | 0.2% | 0% |
| echo | root | go-official-demo | 1 | 1.6% | 0.5% | 0% |
| echov4 | root | go-official-demo | 1 | 1.6% | 0.5% | 0% |
| kube-apiserver | root | demo-k8s-master | 1 | 1.6% | 9.4% | 0% |
| grpc_client | root | go-official-demo | 1 | 1.3% | 0.4% | 0% |

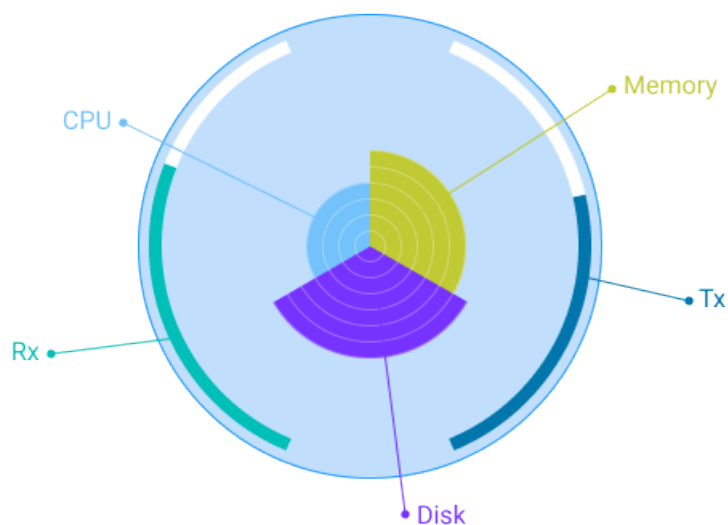
コンパウンドアイ

WhaTapモニタリングサービスの初期画面でプロジェクトを選択した後、**ダッシュボード**>**コンパウンドアイ**を選択します。



コンパウンドアイにより、WhaTapエージェントがインストールされているすべてのサーバーのビューを確認でき、大規模サーバーのリソース状況を一目で確認できます。サンプリングまたは要約された結果でなく、視覚的に可視化されたビューを提供します。

提供情報

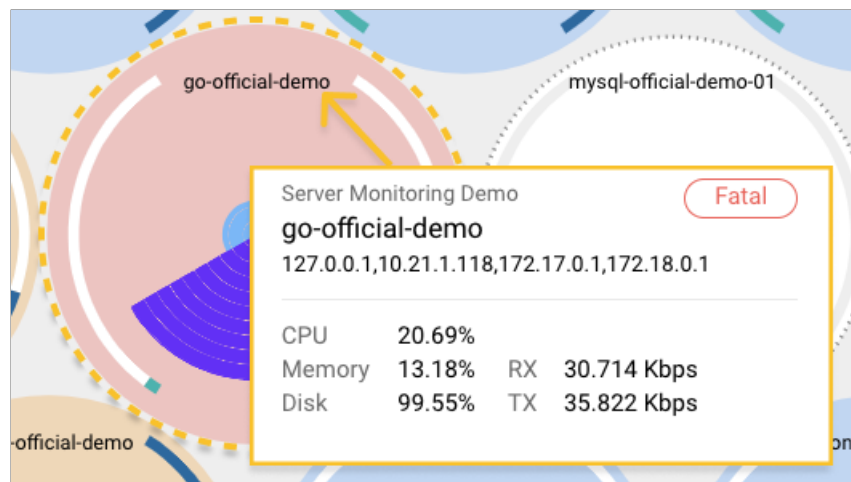


ひとつの目(Eye)です。全部で5つの情報を提供します。

- CPU：CPU使用量
- Memory：メモリ使用量
- Disk：Disk使用量
- Rx：ネットワークのRx(受信量)
- Tx：ネットワークのTx(送信量)

⚠ ネットワーク Rx/Tx 使用量のメトリクスを表示して、DDoSなどの外部攻撃が複数のサーバーで同時に発生しているかを確認できます。

異常現象発生



サーバーに異常現象が発生した場合、個々のアイ(Eye、目)は、色でステータスを表現します。

- 赤：危険ステータス
- オレンジ：アラートステータス
- グレー：モニタリングの一時停止

さらに、サーバー上にカーソルを置くと、数値情報を含むポップアップメッセージが表示されます。サーバーをクリックすると、そのサーバーの要約ページに移動し、詳細を把握できます。

Traffic Max Valueオプション

ネットワーク環境によってトラフィック量が増える可能性があるため、トラフィックの最大値を調整できます。トラフィックの最大値を設定すると、値に応じてRx/Txグラフが変更します。

| | | | | | |
|---------|-------|-------|---------|---------|-------|
| チャート最大値 | 1Kbps | 1Mbps | 100Mbps | 500Mbps | 1Gbps |
|---------|-------|-------|---------|---------|-------|

サーバーインベントリマップ

WhaTapモニタリングサービスの初期画面でプロジェクトを選択した後、ダッシュボードメニューの下にあるサーバーインベントリマップメニューを選択します。サーバーインベントリマップはサーバーインベントリに基づいて、オペレーターがモニタリングの目的に合った分類基準に従ってサーバーをグループ化して構成できる視覚化ダッシュボードです。

WhaTapはサーバーインベントリマップこれにより、ユーザーがサーバーの運用状況を直感的に確認し、分析できるようにサポートします。運用者は業務分類、担当者、サーバー位置などのユーザー定義情報をカスタムコラムで追加して管理でき、これを基に視覚化したダッシュボードを簡単に生成できます。サーバーインベントリマップは、モニタリング目的に応じた様々な視点を満たすために、グループ化機能を提供します。サーバーインベントリマップを通じて、サーバーの運用管理の効率を向上させます。

要求事項

- ① サーバーインベントリマップダッシュボードを使用するためにはサーバーインベントリ機能活性化とサーバーインベントリマップ機能の活性化がそれぞれ必要です。サーバーインベントリとともに新しいサーバーインベントリマップダッシュボードを活用します。サーバーインベントリ活性化についての詳細は、[次の文書](#)を参照してください。

サポートするエージェント

サーバーインベントリマップメニューは、オペレーティングシステムごとに次のバージョン以降でサポートされます。

- **Linux** : 2.7.2以降

アップデートが必要な場合は、オペレーティングシステムごとに次のコマンドを確認します。

- [Debian/Ubuntu](#) Amazon Linux/RHEL/Fedora/Oracle Linux/CentOS/Rocky Linux/SUSE

```
sudo apt-get update
sudo apt-get install whatap-infra
```

```
sudo yum update whatap-infra
```

- Unix : 1.3.7以降

- [AIX](#) Solaris

アップデートが必要な場合は、次のコマンドを確認します。

```
stopsrc -s whatap-infra
cp /usr/whatap/infra/conf/whatap.conf /tmp/whatap.conf
rpm -e whatap-infra
rpm -Uvh https://repo.whatap.io/aix/noarch/whatap-infra-latest.noarch.rpm
cp /tmp/whatap.conf /usr/whatap/infra/conf/whatap.conf
startsrc -s whatap-infra
```

アップデートが必要な場合は、次のコマンドを確認します。

```
cp /usr/whatap/infra/conf/whatap.conf /tmp
/etc/init.d/whatap-infra stop
gunzip -c whatap-infra.latest.SPARC.pkg.tar.gz | tar xvf -
yes n | ./whatap-infra/install.sh
cp /tmp/whatap.conf /usr/whatap/infra/conf/whatap.conf
/etc/init.d/whatap-infra start
```

- Windows : 2.7.2以降

次の[リンク](#)でインストールファイルをダウンロードして実行します。エージェントアップデートの後、サービスが再起動します。

活性化オプション

サーバーインベントリマップメニューの照会機能を有効にするには、次の設定が必要です。

1. [whatap.conf](#)ファイル内の次のオプションを有効にします。

```
categoryv2.enabled=true
```

2. 環境ごとにオプションを追加設定した後、エージェントを再起動します。

- Linux

- オプション追加コマンド エージェントの再起動

```
```bash
grep -q '^categoryv2.enabled' /usr/whatap/infra/conf/whatap.conf || echo 'categoryv2.enabled=true' | sudo tee -a /usr/
whatap/infra/conf/whatap.conf
```
```

```
```bash
sudo service whatap-infra restart
```
```

***Unix**

- オプション追加コマンド エージェントの再起動

```
```bash
grep -q '^categoryv2.enabled' /usr/whatap/infra/conf/whatap.conf || echo 'categoryv2.enabled=true' | tee -a /usr/whatap/
infra/conf/whatap.conf
```
```

***AIX**

```
```bash title='AIX'
stopsrc -s whatap-infra
startsrc -s whatap-infra
```
```

***Solaris**

```
```bash title='Solaris'
/etc/init.d/whatap-infra restart
```
```

***Windows**

- オプション追加コマンド エージェント再起動

```
```bash
if (-not (Select-String -Path "C:\Program Files\WhatapInfra\whatap.conf" -Pattern "^categoryv2.enabled" -Quiet)) { Add-Content -Path "C:\Program Files\WhatapInfra\whatap.conf" -Value "categoryv2.enabled=true" }
```

```bash
Restart-Service -Name "Whatap Infra"
```
```

基本画面ガイド

サーバーインベントリマップ New

1時間

グループ化

ラベル

フィルター

10:44:20

一次グループ

二次グループ

アイコンラベル

適用されたフィルターがありません

機能活性化ガイド

2

TotalActiveCore

822793684

OS

SunOSLinuxWindows

Active / Total

5 / 5466 / 6918 / 77

Core

2403088356

3

Servers

TotalCriticalWarningNormalInactiveCores

82200797433684

Metrics

Avg

Max

Max Server

CPU(%)

7.32%12.04%

server148

Memory(%)

25.55%65.2%

server105

Swap(%)

4.68%46.29%

server101

Disk Busy(%)

0.38%6.64%

server141

Network RX

32.1Mib168.7Mib

server126

Network TX

10.3Mib15.4Mib

server167

1 ユーザー設定

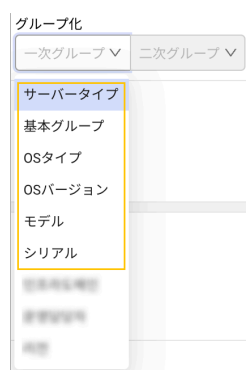
サーバーインベントリマップが提供する複数のユーザー設定により、好きなようにダッシュボードを構成できます。利用できる機能は次の通りです。

リアルタイム照会および一時停止

サーバーインベントリマップは基本的にリアルタイムの照会ベースです。リアルタイム照会および一時停止状態の変更は、画面上部左側の時間選択者を利用します。

| 参照ステータス | 説明 |
|----------------|-------------------|
| リアルタイム照会(Live) | 基本モード
インターバル5秒 |
| 一時停止照会(Pause) | リアルタイム状態変更OFF |

グループ化



サーバーインベントリマップは、サーバーを体系的に分類できるグループ化機能を提供します。モニタリングの目的と環境に基づいてグループ基準を設定して、サーバーを効果的に管理します。

サーバーインベントリベースで照会可能なカラムのうち、基本収集項目とユーザー定義項目がグループ化一覧に表示されます。基本収集項目はサーバータイプ、基本グループ、OSタイプ、OSバージョン、モデル、シリアルです。例示画像で確認できるその他の項目は、ユーザー定義項目であり、カスタムカラム(custom)です。

1次グループと2次グループを順次選択してサーバーを分類できます。1次と2次グループ化によって3領域で1次グ

ループはカード方式でデータを分類し2次グループは、カード内のチャート領域でサブグループ形式で各グループ化されたデータを表現します。

❗ グループ化についての詳細は、[次の文書](#)を参照してください。

ラベル

サーバーインベントリマップは、サーバ情報を明確に確認できるよう **ラベル**オプションを提供します。希望するラベル オプションを選択すると、チャートでサーバー別の該当ラベル情報を確認できます。

| ラベル | 説明 |
|--------------|------------------------------|
| サーバー名 | 各サーバーの実際のホスト名をラベル表示します。 |
| サーバーエイリアス | ユーザーが指定したエイリアスをラベルで表示します。 |
| IP Address | 該当サーバーのIPアドレスをラベルで表示します。 |
| CPU(%) | 現在のCPU使用率(%)をラベルで表示します。 |
| Memory(%) | 現在のメモリ使用率(%)をラベルで表示します。 |
| Swap(%) | 現在のスワップメモリ使用率(%)をラベルで表示します。 |
| Disk Busy(%) | 現在のディスク使用率(%)をラベルで表示します。ディスク |
| Network | ネットワーク状態をラベルで表示します。 |

フィルター

サーバーインベントリマップは、ダッシュボードに表示するサーバー種類のフィルター機能を提供します。フィルターを介して適用されたデータは、サーバー グループチャート、要約ビュー、および詳細ビューに反映されます。

- **フィルタキー**：フィルターはサーバー インベントリメニューで提供される基本収集カラムとユーザーが定義したカスタムカラムを基準に設定できます。

- 基本収集カラム：サーバー インベントリで自動収集されたデータ項目であり、サーバータイプ、基本グループ、OSタイプ、OSバージョン、モデル、シリアルカラム項目です。
- カスタムカラム：ユーザーがプロジェクトごとに追加して管理する項目です。
- 条件: フィルターの条件は、 $\geq$ 、 $\leq$ 、 $>$ 、 $<$ などの数値型条件と一致、不一致、包含、不包含などの文字列条件で設定できます。

インベントリマップ設定

サーバーインベントリマップはインベントリマップの設定オプションを提供します。右上で⚙️アイコンを選択し、次のオプションの活性化有無を設定します。

- 一次グループなし表示: グループ化する時に選択した1次グループの設定のないサーバーグループカードの表示有無を選択します。デフォルト設定は表示します。
- グループ下段メトリック領域の表示: サーバーグループカードの下部で、メトリクス情報の表示有無を選択します。デフォルト設定は表示します。

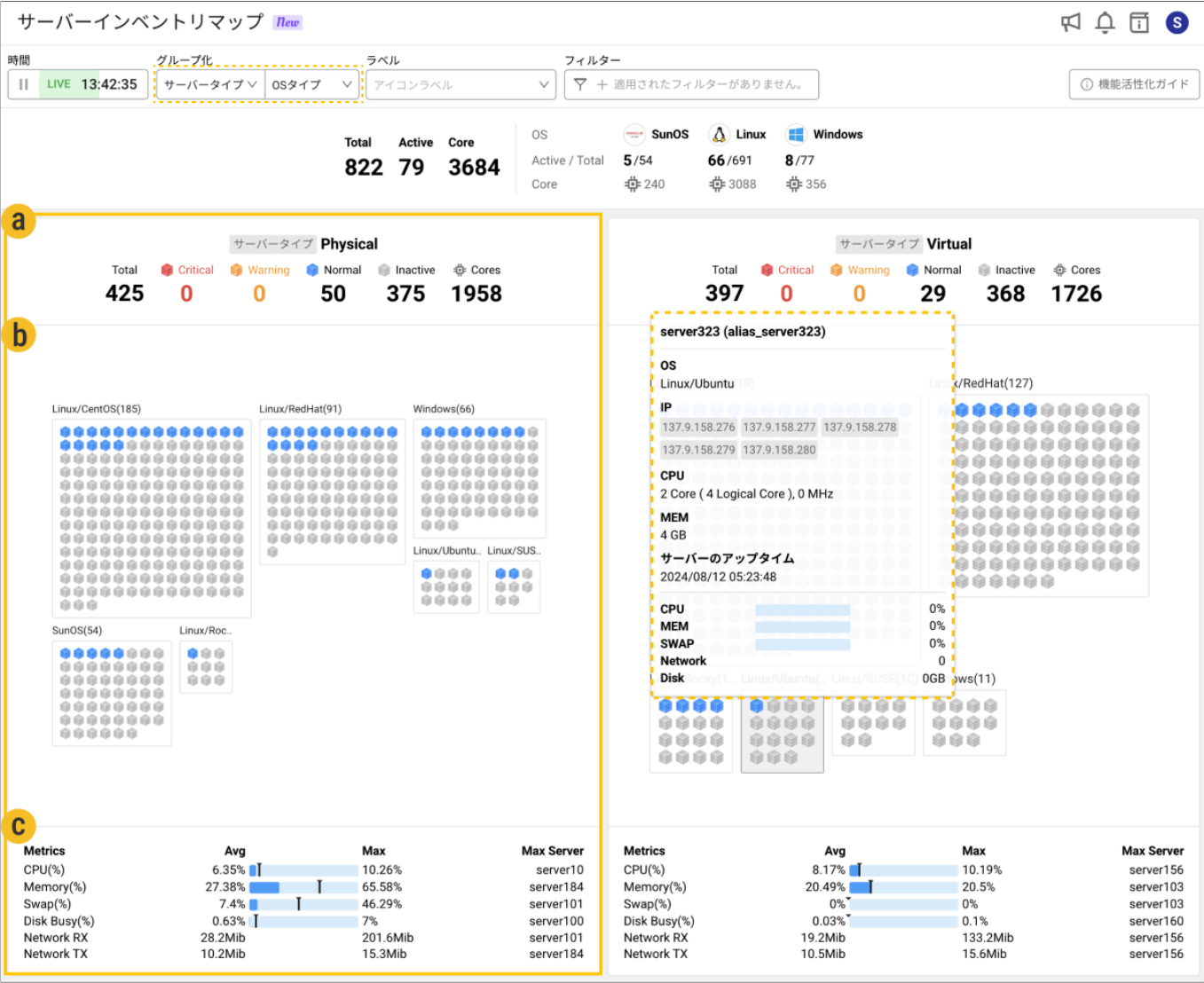
2 サーバー構成状況

サーバーインベントリマップは、ダッシュボードの上部で当該プロジェクトのサーバー運営体制別の構成状態を一目で確認できるサーバー構成状況情報を提供します。これにより、ユーザーはプロジェクト内のサーバーの主要な情報を簡単かつ直感的に把握できます。

- OS：サーバーのオペレーティングシステムを示し、OSアイコンとともにOSの名前を表示します。事前に定義されていないOSが含まれている場合は、デフォルトでインフラアイコンを表示します。
- Total / Active：プロジェクトに含まれているサーバー全体の数と、現在有効なサーバー数を意味します。
- Core：プロジェクトに含まれるすべてのサーバーの物理コアの合計を表示します。

3 サーバーグループカード

サーバーインベントリマップは、グループ化されたサーバー構成情報に基づいて個別のカードを提供します。サーバーインベントリマップのカードは、次の3つの主要な要素で構成されます。



a グループ状況

グループ名およびグループに属するサーバーの状態別サーバー数の情報を提供します。

| 区分 | 説明 |
|-------|--|
| Total | そのグループに含まれるサーバー全体の数を示します。サーバーは目的に合わせて分類され、フィルタリングされた状態で集計されます。 |

| 区分 | 説明 |
|----------|---|
| Critical | 危険度Critical(危険)に該当するイベントを発生させたサーバー数を示します。 |
| Warning | 危険度Warning(警告)に該当するイベントを発生させたサーバー数を示します。 |
| Normal | 危険度CriticalまたはWarningイベントが発生していない、正常な状態のサーバー数を示します。 |
| Inactive | サーバーDown、AgentDown、ネットワーク通信障害などにより、正常なデータ収集ができないサーバー数を示します。 |
| Cores | グループ内の各サーバーの物理コア数を合計したコア数を示します。 |

b サーバーグループチャート

グループ内のサーバーの状態と性能データを視覚化して提供します。2次グループ化が適用された場合、チャート内でサブグループ形式でデータがさらに区切られて表示されます。また、サブグループにマウスオーバーすると、そのグループに含まれたサーバーの主要状態情報をポップオーバー形式で簡単に確認できます。

c メトリクス

グループごとの主要なメトリクス情報を簡単に提供します。各メトリクスの詳細については、次のグラフを参照してください。

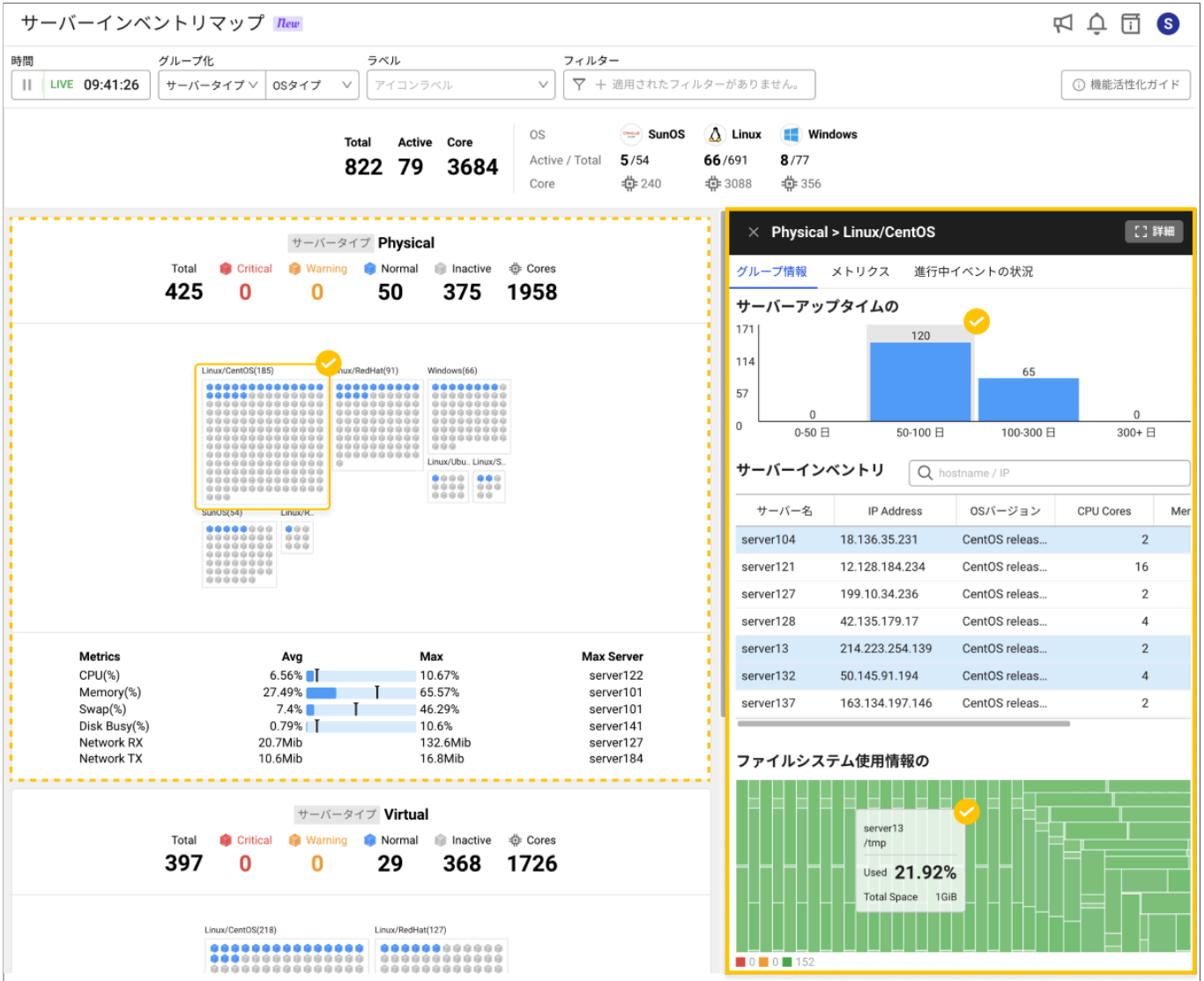
| 区分 | 説明 |
|--------------|---|
| CPU(%) | 全CPU使用率のうち、ユーザーモード(User)とカーネルモード(Sys)での使用率の合計を表示します。 |
| Memory(%) | ユーザープロセスとカーネルが使用中のメモリの割合を表示し、バッファとキャッシュ領域は除外されます。 |
| Swap(%) | 現在使用中のSwap領域のサイズをパーセンテージで表示します。 |
| Disk Busy(%) | 単位時間当たりの各ディスクが作業した時間の割合であり、サーバーで最も使用率の高いディスクの値を表示します。 |
| Network RX | 受信(Rx)されたデータの量をbps単位で表示します。 |

| 区分 | 説明 |
|------------|-----------------------------|
| Network TX | 送信(Tx)されたデータの量をbps単位で表示します。 |

- **Avg**：グループに属するすべてのサーバーの平均メトリクス値を表示します。
- **Max**：当該メトリクスの最大値を表示します。
- **Max Server**：最大値を記録したサーバーの名前を表示します。

概要を表示

サーバーインベントリのマップチャートでグループを選択する場合、右側の領域で**要約表示**パネルを確認できます。要約表示パネルは**グループ情報**タブと**メトリクス**タブを提供します。



 詳細

要約表示パネルの右上に「詳細を見る」ボタンをクリックします。詳細を見るについての詳細は、[次の文書](#)を参照してください。

グループ情報

グループ情報タブで、次のように選択したサーバーグループの主要な運用状態とリソース情報を効果的に確認できま

す。

サーバーアップタイムの

サーバーが起動した後、運用期間を基準に区間を分けて、該当区間に属しているサーバーの台数をバーチャートの形で視覚化して表示します。バーチャート選択時、当該区間に属するサーバーの詳細情報が下段のサーバーインベントリ一覧でハイライトされます。同じバーチャートをクリックすると、選択が解除されます。

サーバーインベントリ

選択したサーバーグループのサーバー関連の主要情報を一覧形式で照会できます。右側の入力画面でHostnameまたはIPアドレスを入力してフィルタリングできます。サーバー名、IP Address、OSバージョン、CPU Cores、Memory(GB)、サーバーアップタイムカラムを提供します。

ファイルシステム使用情報の

サーバーのファイルシステムの状態を直感的に照会できます。各サーバーのマウントポイントは1つのブロックで表現されます。ブロック色は、当該マウントポイントの使用率(Used、%)を示します。また、同じ色の範囲内でも使用率の数値が高くなるほど、色の強度が高くなります。

- ・ **赤色**：使用率が90%以上の場合を意味します。
- ・ **オレンジ色**：使用率が80%以上90%未満の場合を意味します。
- ・ **緑色**：使用率が80%未満の場合を意味します。

① マウントポイントブロックの上にマウスオーバーすると、そのサーバー名、マウントポイント、使用率、および全容量情報を確認できます。

メトリクス

メトリクスタブで主要サーバーの性能メトリクスをチャート形式で照会できます。グループごとのリソースの状態を直感的に確認できます。

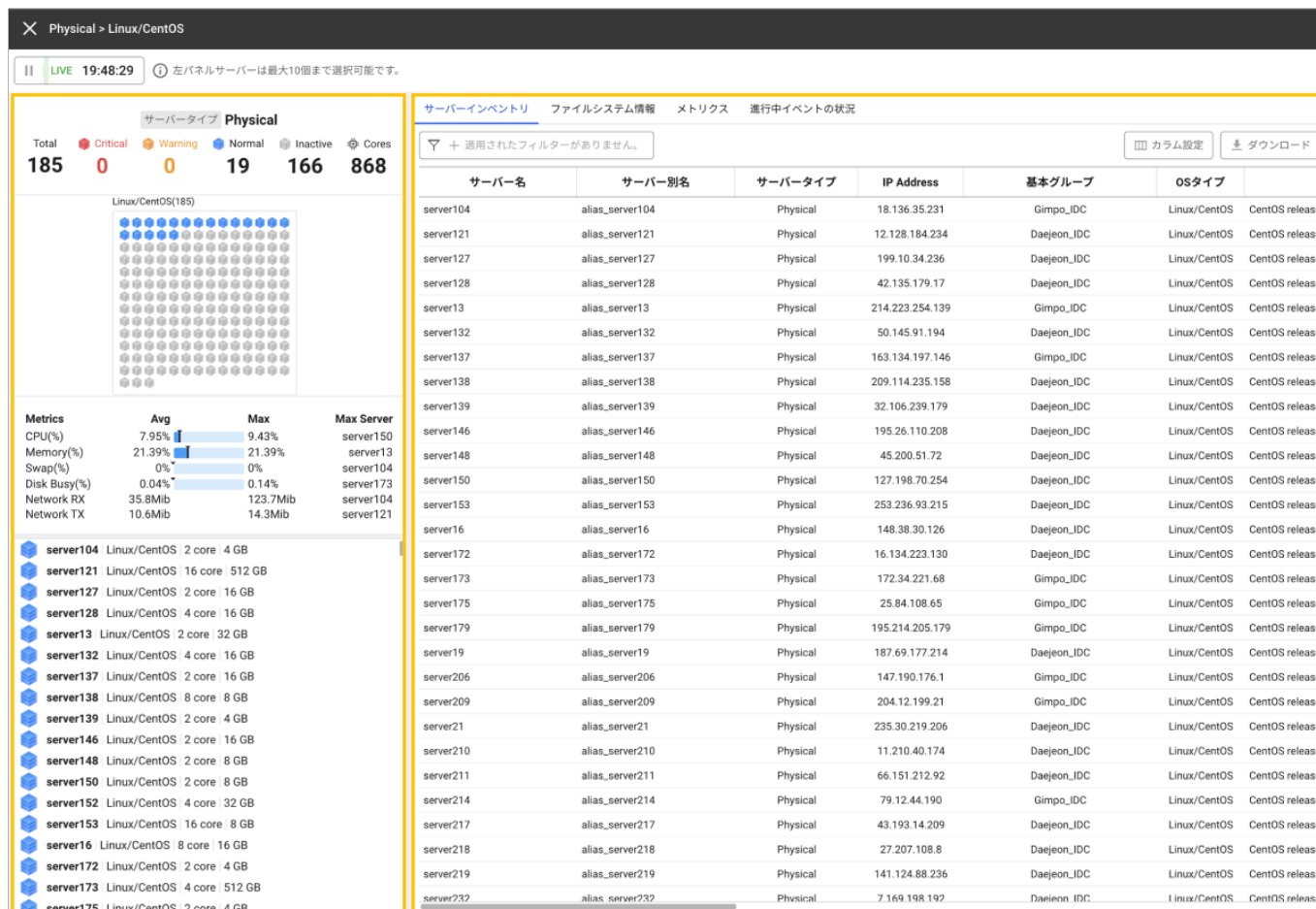
| 区分 | 説明 |
|----------------------|---|
| [CPU] User + Sys (%) | 全CPU使用率のうち、ユーザーモード(User)とカーネルモード(Sys)での使用率の合計を表示します。これにより、CPU資源全体の活用度を示します。 |
| [MEM] Used (%) | ユーザープロセスまたはカーネルによって使用されたメモリの割合を表示します。バッファとキャッシュ領域を除き、純粋なメモリ使用量のみが反映されます。 |
| [SWAP] Used (%) | 現在使用中のSwapメモリサイズをパーセンテージで表示した値です。 |
| [NET] Rx (bps) | ネットワークで受信(Rx)されたデータの量をbps(秒当たりビット)単位で表示します。 |
| [NET] Tx (bps) | ネットワークを通じて送信(Tx)されたデータの量をbps(秒当たりビット)単位で表示します。 |
| [Disk] Read (Bytes) | ディスク全体の1秒当たりの読み取り速度の合計をBytes単位で表示します。 |
| [Disk] Write (Bytes) | ディスク全体の1秒当たりの書き込み速度の合計をBytes単位で表示します。 |

進行中のイベント現況

進行中イベントの状況タブで選択したサーバーグループで進行中のイベントのステータスリストを確認できます。

サーバーインベントリマップの詳細

サーバーインベントリマップメニューで選択したサーバーグループの詳細情報を詳細を見る画面で確認できます。要約表示パネル上段の右上に「詳細を見る」ボタンをクリックします。詳細ビュー内のサーバーグループ情報はリアルタイムで更新されます。



- 上段時間セレクトターにより、グループデータの照会時点と更新周期を確認でき、データの更新を中止または再開できます。
- 左の領域でサーバーグループカードとサーバー一覧を確認できます。
- 右側の個別タブエリアで、サーバーインベントリ、ファイルシステム情報、メトリクス情報を確認できます。

サーバーグループカードと一覧

選択したサーバーグループの主要な要約情報は、サーバーグループのカードと一覧から確認できます。

- サーバーグループカード内のチャート領域でサーバーの上にマウスを置くと、選択したサーバーの要約情報をポップオーバー形式で簡単に確認できます。
- サーバーグループカード内のチャート領域とサーバー一覧から照会したい対象サーバーを特定できます。
- サーバー一覧でサーバーを選択すると、すべての選択またはすべて解除できます。
- サーバー選択時に選択したサーバーの情報を右側の個別タブで確認できます。

サーバーインベントリ

選択したサーバーの詳細構成情報をサーバーインベントリタブで一覧形式で確認できます。サーバーを選択していない場合、そのサーバーグループ内のすべてのサーバーに対するサーバー構成情報が表示されます。サーバーインベントリメニューで照会できる情報と構成が同じです。

フィルター

サーバーインベントリメニューで設定したカラム一覧に基づいてサーバーフィルター機能を提供します。

- **フィルタキー**：フィルターはサーバーインベントリメニューで提供される基本収集カラムとユーザーが定義したカスタムカラムを基準に設定できます。
 - **基本収集カラム**：サーバーインベントリで自動収集されたデータ項目であり、サーバータイプ、基本グループ、OSタイプ、OSバージョン、モデル、シリアルカラム項目です。
 - **カスタムカラム**：ユーザーがプロジェクトごとに追加して管理する項目です。
- **条件**：フィルターの条件は、 $\geq$ 、 $\leq$ 、 $>$ 、 $<$ などの数字型条件と一致、不一致、包含、不包含などの文字列条件で設定できます。

カラム設定

サーバーインベントリマップの詳細を見る内のサーバーインベントリタブのカラム設定の場合は、一覧内のカラムの表示可否と順序を設定できます。当該表示の有無と手順はサーバーインベントリメニューと個別に設定されます。

❗ カスタムカラムの追加と修正はサーバー インベントリメニューでできます。

CSVダウンロード

上段の  ダウンロードボタンをクリックして、収集されたサーバー構成情報をCSVファイル形式でダウンロードできます。

ファイルシステム情報

左側のサーバーグループカードまたは一覧で選択したサーバーのファイルシステム情報をファイルシステム情報タブで一覧形式で照会できます。サーバーを選択していない場合、そのサーバーグループ内のすべてのサーバーに対するファイルシステム情報が表示されます。

| 区分 | 説明 |
|-----------------|--|
| Mount Point | Mountされたファイルシステムの名前を表示します。Windows環境では、ドライブパーティションの名前を示します。 |
| Total Space(GB) | ファイルシステムに割り当てられた完全なストレージ容量をGB単位で表示します。 |
| Used Space(GB) | ファイルシステムで現在使用中のストレージ容量をGB単位で表示します。 |
| Used(%) | ファイルシステムの全ストレージ容量に対する使用中のストレージ容量の割合をパーセンテージで表示します。 |
| i-node Used(%) | ファイルシステムに割り当てられたi-nodeのうち、使用中のi-nodeの割合をパーセンテージで表示します。 |
| Free(GB) | ファイルシステムで現在使用可能な空き容量をGB単位で表示します。 |

❗ i-node



i-nodeはファイルシステムでファイルとディレクトリに対する情報を保存する空間であり、この使用率が100%になると、**Used(%)**が100%でなくても、これ以上ファイルを使えません。

フィルター

サーバーフィルター機能を提供します。**フィルターキー**には、**サーバー名**と**Mount Point**が提供されます。フィルターの**条件**は、数値条件のほか、一致・不一致・含む・含まないなどの文字列条件で設定できます。

CSVダウンロード

上段の **ダウンロード** ボタンをクリックして、収集されたファイルシステム情報を**CSV**ファイル形式でダウンロードできます。

メトリクス

左側のサーバーグループカードまたは一覧で選択したサーバーの性能メトリクスチャートを**メトリクスタブ**で照会できます。サーバーを選択しなかった場合、そのサーバーグループ内の上位50台のサーバーに対する性能メトリクスチャートが表示されます。

| 名前 | 説明 | 備考 |
|----------------------|--|----|
| [CPU] User + Sys (%) | 全CPU使用率のうち、ユーザーモード(User)とカーネルモード(Sys)での使用率の合計を表示し、全体のCPUリソースの活用度を示します。 | - |
| [CPU] User (%) | ユーザーモードで実行中のプロセスが占めるCPU比率です。 | - |
| [CPU] Sys (%) | カーネルモードで実行中のプロセスが占めるCPU比率です。 | - |
| [CPU] Wait (%) | CPUがディスクやネットワークのようなI/O作業を待ちながらアイドル状態にある時間の割合です。 | - |
| [System] Runqueue | 実行準備ができていますが、まだCPUを割り当てられていないプロセス(またはThread)の数です。 | - |

| 名前 | 説明 | 備考 |
|---------------------------|--|----------------------------------|
| [System]
Blockqueue | I/O、ページング等のためにキューにあるプロセス(またはThread)数を意味します。 | Windows除外 |
| [System] Forks | 1秒当たりの新しいプロセスを作成するタスク数を表示します。 | Windows除外 |
| [System]
Interrupts | 1秒当たりのCPUがハードウェア割り込みを処理した回数を表示します。 | - |
| [System]
SystemCall | 1秒当たりのカーネルがシステム呼び出しを処理した回数を表示します。 | Linux除外 |
| [System]
ContextSwitch | 1秒当たりのプロセス間の切り替えが発生した回数を表示します。 | - |
| [MEM]
Used+Cache(%) | 全メモリのうち、UsedメモリとCachedメモリの合計比率を表示します。 | Windowsは
[MEM] Used(%)
に表示 |
| [MEM] Used(%) | メモリがユーザープロセスまたはカーネルによって使用されたメモリの使用率を意味し、バッファおよびキャッシュ領域を除いて表示します。 | - |
| [MEM]
Cache(%) | 頻繁にアクセスされるファイルやデータを素早く提供するために、キャッシュされたメモリの使用率を表示します。 | Windows除外 |
| [Swap]
Used(%) | 現在使用中のSwapの大きさをパーセンテージで表示した値です。 | - |
| [MEM] SwapIn | ディスクのスワップ(ページングスペース)領域からメモリに移動したページ数を表示します。 | - |
| [MEM]
SwapOut | メモリでディスクスワップ(ページングスペース)領域に移動したページ数を表示します。 | - |
| [MEM]
FilesystemIn | ファイルシステムの読み取り操作に応じて、メモリにロードしたページ数を表示します。 | - |

| 名前 | 説明 | 備考 |
|--------------------------------|--|----|
| [MEM]
FilesystemOut | ファイルシステムの書き込み操作に応じて、ディスクに記録したページ数を表示します。 | - |
| [NET] Rx+Tx
(bps) | 受信(Rx)と送信(Tx)されるデータの合計をbps単位で表示した値です。 | - |
| [NET] Rx+Tx
(pps) | 受信(Rx)と送信(Tx)されるパケットの合計を1秒当たりのパケット(pps)単位で表示した値です。 | - |
| [Disk] Read +
Write (bytes) | ディスクの読み込みと書き込みデータの合計をバイト単位で表示します。 | - |
| [Disk] Read +
Write (IOPS) | ディスク読み込みと書き込み操作の回数をIOPS(Input/Output Operations Per Second)単位で表示します。 | - |
| [Process]
TotalCount | 現在のプロセス全体数を表示します。 | - |
| [Thread]
TotalCount | 現在の全体スレッド数を表示します。 | - |
| [Defunct]
TotalCount | 現在defunctプロセスの数を表示します。 | - |

進行中のイベント現況

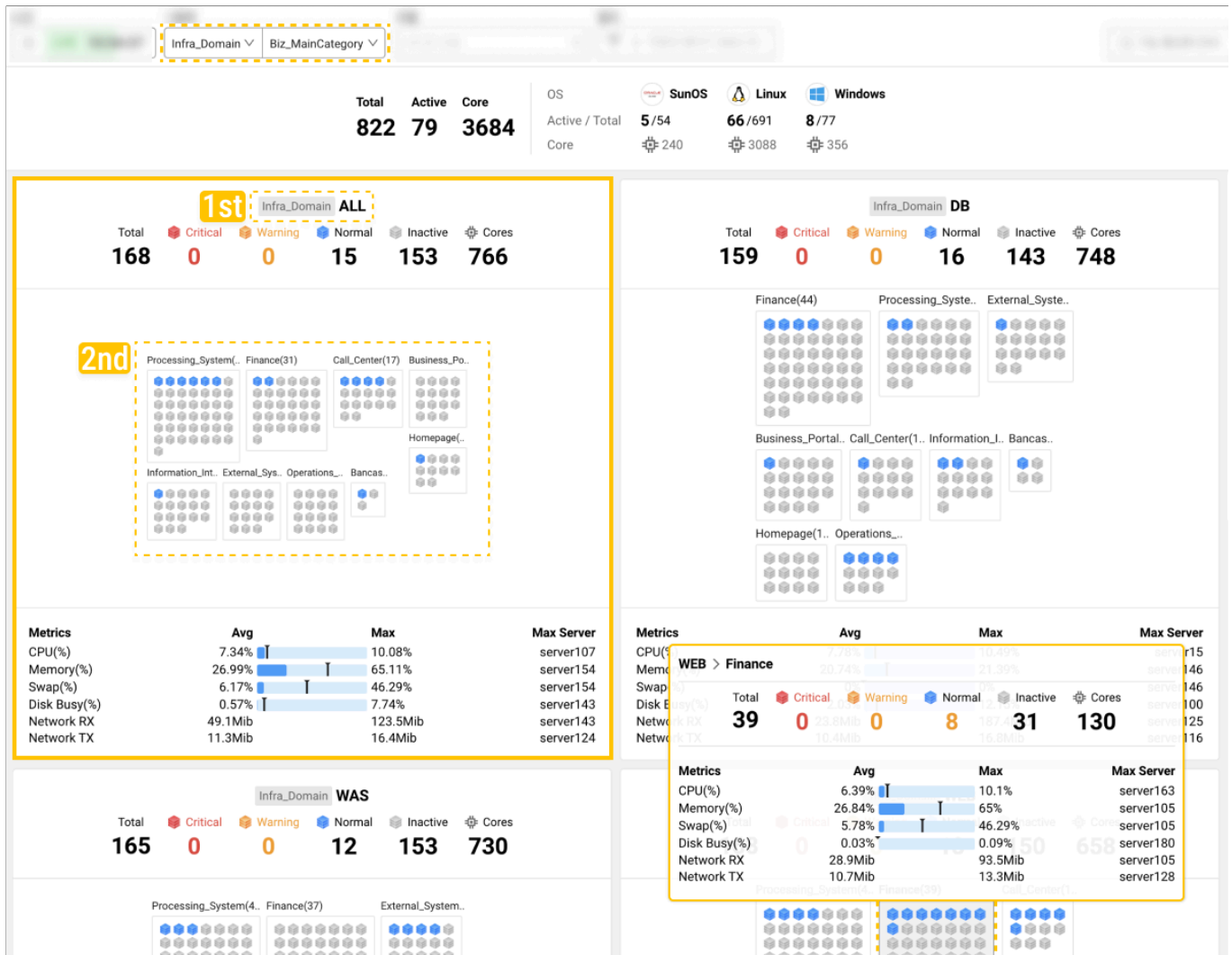
左側のサーバーグループカードまたは一覧から選択したサーバー内の進行中のイベント状況を照会できます。 目録形式で イベント名、アラート発生時刻、サーバー名及びメッセージが確認できます。

サーバーインベントリマップのグループ化

サーバーインベントリマップはサーバー インベントリメニューでユーザーが設定したカラム情報に基づいて、すべてのサーバー情報を一目で確認できるダッシュボードです。しかし、サーバーの状態と情報をモニタリングする際、ユーザーごとに重要視する基準は異なる場合があります。これを反映してサーバーインベントリマップは、ユーザーの関心事に応じてデータをグループ化できる機能を提供します。

例えば、インフラ担当者は、サーバーのハードウェア構成情報とリソース使用率に主に関心を持つのに対し、アプリケーション担当者は、特定のサービスに関連するサーバーグループや個々のサーバー状態に集中します。オペレーターは、特定の期間におけるリソースの変化や主要なイベントに基づいてサーバーの状態を分析しようとする場合があります。

このように多様な観点と必要を満たすためにサーバーインベントリマップは、柔軟なグループ化機能を提供します。これにより、ユーザーは関心事に基づいてデータを再構成し、サーバーの状態をより効率的にモニタリングおよび管理できます。



グループ化 & カード

サーバーインベントリマップは、グループ化したサーバー構成情報ごとにカードを提供します。グループ化を適用していない場合、サーバー全体の情報が1つの大きなカード内に表示されます。グループ化を適用すると、各グループ単位でカードを構成します。

グループ化適用時1次グループと2次グループを順次選択してサーバーを分類できます。1次と2次グループ化によって1次グループはカード方式でデータを分類し2次グループは、カード内のチャート領域でサブグループ形式で各グループ化されたデータを表現します。

- **1次グループ**：1次グループは**グループ区分**と**グループ名**情報に基づいて表示されます。

例、`Infra_domain` ALL

- **2次グループ**：2次グループは**グループ名**と**グループ内のサーバー数**情報に基づいて表示されます。

例、**Finance(31)**

- ❗ • サーバークラスまたはサーバーにマウスオーバーすると、そのグループおよびサーバーの主要状態情報をポップオーバー形式で簡単に確認できます。
- グループ化選択項目のうち**未設定**項目を選択した時には、グループ化指定が初期化されます。

主なグループ化の属性

サーバー インベントリベースで照会可能なカラムのうち、基本収集項目とユーザー定義項目が**グループ化**一覧に表示されます。基本収集項目は**サーバータイプ**、**基本グループ**、**OSタイプ**、**OSバージョン**、**モデル**、**シリアル**です。

例示画像で確認できる**インフラドメイン**(`Infra_Domain`)と**業務別大分類**(`Biz_MainCategory`)などのその他の項目は、**サーバー インベントリメニュー**でカスタムカラム(`custom`)を通じて追加されたカスタム項目です。

カスタム項目により、サーバーを物理的または論理的構成に従って**インフラドメイン**で**1次グループ化**後、業務の目的に応じて**業務別大分類基準**として**2次グループ化**を適用して、ビューを細分化できます。

| | Freq(MHz) | Memory(GB) | All IP | Time Zone | | Infra_Domain <small>custom</small> | Biz_MainCategory <small>custom</small> |
|-----------|-----------|------------|-----------------------------|-----------|---------------------|------------------------------------|--|
| server758 | 4,250 | 8 | 54.142.159.829,54.142.1... | KST-9 | 2024-08-04 02:40:59 | ALL | External_System |
| server885 | 4,250 | 4 | 254.186.171.1093,254.1... | KST-9 | 2024-08-23 12:59:43 | WEBWAS | Homepage |
| server902 | 4,250 | 32 | 135.175.32.952,135.175... | KST-9 | 2024-08-30 08:53:12 | ALL | Homepage |
| server0 | 4,250 | 4 | 210.4.178.230,210.4.178... | KST-9 | 2024-08-26 07:55:20 | DB | Processing_System |
| server9 | 4,250 | 4 | 246.216.137.957,246.21... | KST-9 | 2024-08-30 19:45:12 | WEBWAS | Finance |
| server958 | 4,250 | 8 | 118.4.94.1209,118.4.94.1... | KST-9 | 2024-08-22 20:36:20 | DB | Finance |
| server975 | 4,250 | 16 | 248.61.3.1003,248.61.3.1... | KST-9 | 2024-08-05 22:08:48 | DB | External_System |
| server993 | 4,250 | 4 | 153.144.222.1237,153.1... | KST-9 | 2024-08-15 03:44:03 | WAS | Finance |
| server373 | 4,250 | 16 | 79.4.116.362,79.4.116.36... | KST-9 | 2024-08-05 05:54:49 | WEB | Processing_System |
| server659 | 4,250 | 32 | 241.234.162.736,241.23... | KST-9 | 2024-08-05 19:08:40 | WEBWAS | Bancassurance |
| server667 | 4,250 | 16 | 220.224.107.784,220.22... | KST-9 | 2024-08-04 19:36:34 | WEB | Homepage |

例示画像はサーバー インベントリメニューでインフラドメイン項目をDB、WAS、WEB、WEBWAS、そしてユーザーが定義したインフラドメインを含むALLなどで項目値を分類しました。 また業務別大分類項目をExternal_System、Processing_System、Financeなどで項目値を分類しました。

このような情報をもとにサーバーインベントリマップダッシュボードを構成して全体の運用状況をモニタリングできます。

カード別メトリクスデータ

各カードの下には、グループ化されたサーバーに関する主要なメトリクス情報を簡単に提供します。 各メトリクスの詳細については、次のグラフを参照してください。

| 区分 | 説明 |
|-----------|--|
| CPU(%) | 全CPU使用率のうち、ユーザーモード(User)とカーネルモード(Sys)での使用率の合計を表示します。 |
| Memory(%) | ユーザープロセスとカーネルが使用中のメモリの割合を表示し、バッファとキャッシュ領域は除外されます。 |
| Swap(%) | 現在使用中のSwap領域のサイズをパーセンテージで表示します。 |
| Disk | 単位時間当たりの各ディスクが作業した時間の割合であり、サーバーで最も使用率の高いディスクの値 |

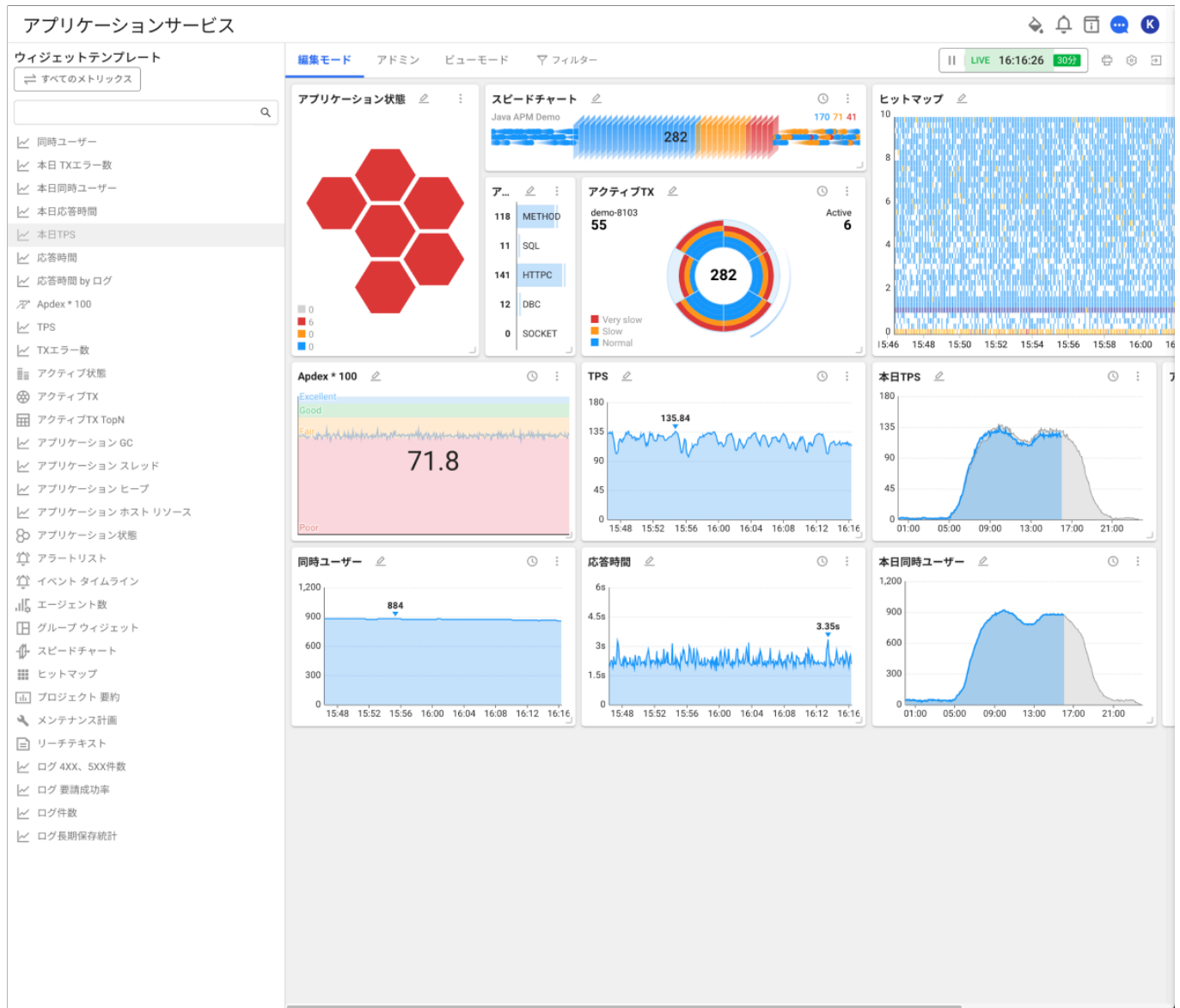
| 区分 | 説明 |
|------------|-----------------------------|
| Busy(%) | を表示します。 |
| Network RX | 受信(Rx)されたデータの量をbps単位で表示します。 |
| Network TX | 送信(Tx)されたデータの量をbps単位で表示します。 |

- **Avg**：グループに属するすべてのサーバーの平均メトリクス値を表示します。
- **Max**：当該メトリクスの最大値を表示します。
- **Max Server**：最大値を記録したサーバーの名前を表示します。

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。

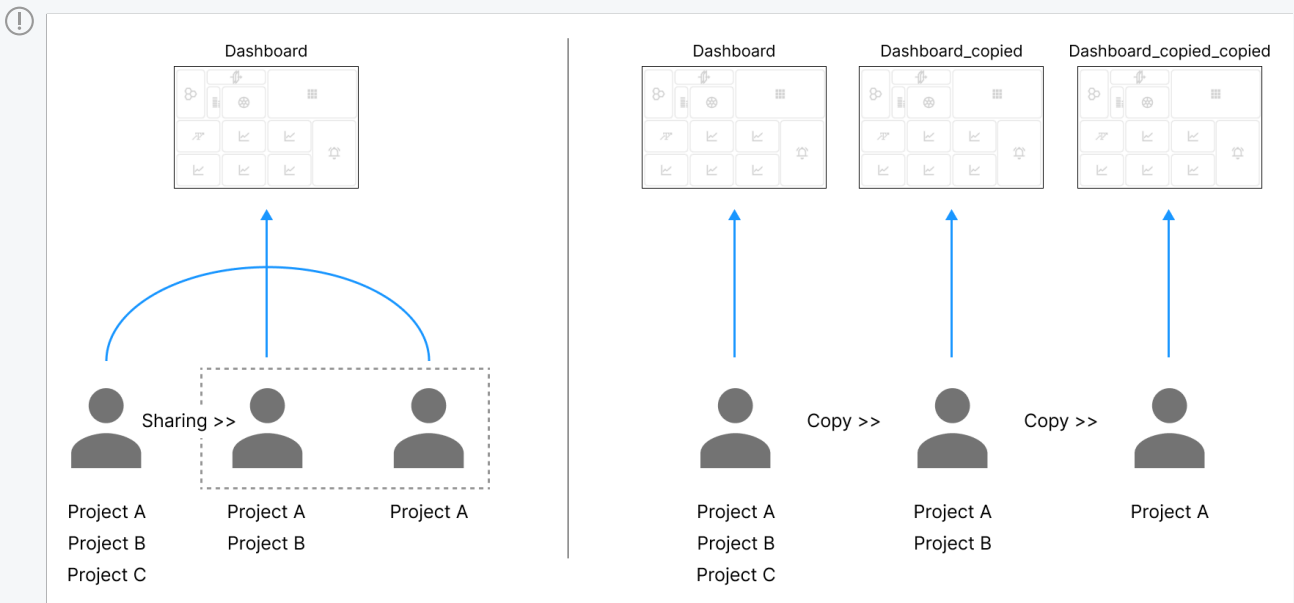
 ダッシュボードの削除は所有者と共有を受けたユーザーで動作が異なります。

- 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。

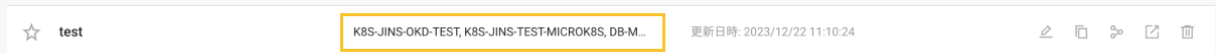
Flex ボードを共有する

 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 |
|--|--|
|  <p>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</p> |  <p>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</p> |

✓ ダッシュボード共有の条件

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

Flex ボードをコピーする

ユーザーは Flex ボードをコピーして他のメンバーに渡せます。

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

JSON ファイルで共有する

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

エクスポート

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

インポート

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

❗ この機能は、プロジェクトの 編集 権限を持つメンバーのみ利用できます。

Flex ボードの画面モード

Flex ボードの画面モードに応じて提供機能が異なります。

❗ アクセス可能なメンバー権限

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

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

モード種類

Flexボード は画面モードにより設定できる機能が異なります。

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

共通機能

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

データフィルタリング

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

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

フィルタリング条件

フィルタリング条件はエージェントタイプとメトリクスタイプに分かれます。

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

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

参照時間を設定する

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

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

印刷する

Flex ボード画面を PDF で保存して印刷できます。

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

Flex ボード管理

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

することもできます。

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

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

2. すべての設定を完了し、**保存** ボタンをクリックします。

ダッシュボードをお気に入りに登録する

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

ウィジェットの管理

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

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

ウィジェット追加

作成済みのFlexボードにウィジェットを追加できます。

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

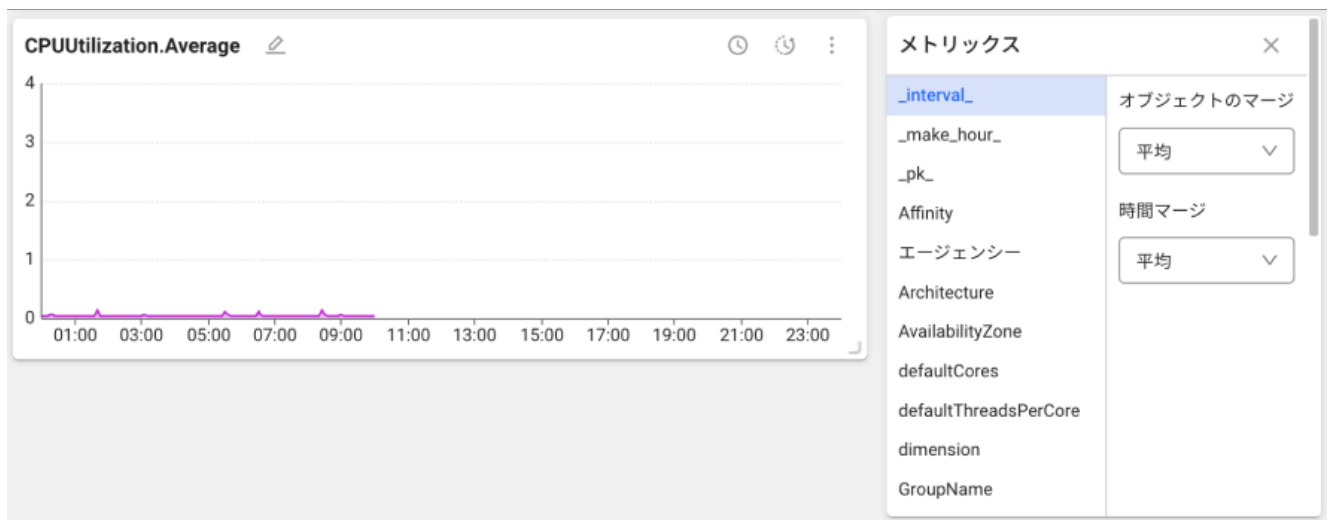
左側で選択したタグ(例：エージェント名)に基づいてチャートデータをグループ化するために使用します。この場合、異なるフィールド(例：CPU)値を持つデータ間でタグが一致する場合、そのデータは結合されます。

• 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。

サーバーインベントリ

WhaTapモニタリングサービスの初期画面でプロジェクトを選択した後、**サーバーリストメニュー**の下にある**サーバーインベントリメニュー**を選択します。**サーバー インベントリ**は、サーバー運営に必要な構成情報を提供し、管理の利便性のために手動で管理項目を追加できます。

サーバー インベントリは、サーバーの物理的かつ仮想的特性、運用環境などを体系的に管理するためのメニューです。この機能により、自動的に収集されたサーバーの構成要素とユーザー定義項目を使用してサーバーの構成を詳細に把握し、管理できます。**サーバー インベントリ**は、サーバーの性能分析と問題解決に不可欠なデータを提供します。

❗ サポートエージェントバージョン

サーバー インベントリメニューは、オペレーティングシステムごとに次のバージョン以降でのみ対応しています。

- **Linux** : 2.6.6以降

アップデートが必要な場合は、オペレーティング システムごとに次のコマンドを確認します。

- **Debian/Ubuntu** Amazon Linux/RHEL/Fedora/Oracle Linux/CentOS/Rocky Linux/SUSE

```
sudo apt-get update
sudo apt-get install whatap-infra
```

```
sudo yum update whatap-infra
```

- **Unix** : 1.3.4以降

アップデートが必要な場合は、オペレーティング システムごとに次のコマンドを確認します。

- **AIX** Oracle Solaris

```
stopsrc -s whatap-infra
cp /usr/whatap/infra/conf/whatap.conf /tmp/whatap.conf
rpm -e whatap-infra
rpm -Uvh https://repo.whatap.io/aix/noarch/whatap-infra-latest.noarch.rpm
cp /tmp/whatap.conf /usr/whatap/infra/conf/whatap.conf
```



```
cp /usr/whatap/infra/conf/whatap.conf /tmp
/etc/init.d/whatap-infra stop
pkgrm whatap-infra
wget https://repo.whatap.io/sunos/11/whatap-infra.latest.SPARC.pkg.tar.gz
tar xzvf whatap-infra.latest.SPARC.pkg.tar.gz
pkgadd -d .
cp /tmp/whatap.conf /usr/whatap/infra/conf/whatap.conf
```

- **Windows** : 2.6.6以降

次の[リンク](#)でインストールファイルをダウンロードして実行します。エージェントアップデートの後、サービスが再起動します。

活性化オプション

サーバー インベントリメニューの照会機能を有効にするには、次の設定が必要です。

1. [whatap.conf](#)ファイル内の次のオプションを有効にします。

```
hostinfov2.enabled=true
```

2. 環境ごとにオプションを追加設定した後、エージェントを再起動します。

- **Linux**

- オプション追加コマンド エージェントの再起動

```
```bash
grep -q '^hostinfov2.enabled' /usr/whatap/infra/conf/whatap.conf || echo 'hostinfov2.enabled=true' | sudo tee -a /usr/
whatap/infra/conf/whatap.conf
```
```

```
```bash
sudo service whatap-infra restart
```
```

```
***Unix**
```

- [オプション追加コマンド](#) エージェントの再起動

```
```bash title='AIX/Oracle Solaris'
grep -q '^hostinfov2.enabled' /usr/whatap/infra/conf/whatap.conf || echo 'hostinfov2.enabled=true' | tee -a /usr/whatap/infra/conf/whatap.conf
```
```

```
```bash title='AIX'
stopsrc -s whatap-infra
startsrc -s whatap-infra
```

```bash title='Oracle Solaris'
/etc/init.d/whatap-infra restart
```
```

```
***Windows**
```

- [オプション追加コマンド](#) エージェント再起動

```
```bash
if (-not (Select-String -Path "C:\Program Files\WhatapInfra\whatap.conf" -Pattern "^hostinfov2.enabled" -Quiet)) { Add-Content -Path "C:\Program Files\WhatapInfra\whatap.conf" -Value "hostinfov2.enabled=true" }
```
```

```
```bash
Restart-Service -Name "Whatap Infra"
```
```

基本画面ガイド

サーバー インベントリメニューは、サーバーの主な構成情報を一覧形式で提供します。自動的に収集したサーバーの運用および管理に必要な必須情報とユーザー定義項目をともに管理できます。これにより、サーバー管理者はより体系的かつ効率的にインフラをモニタリングするとともに、運用できます。フィルターとソート機能を活用して、必要な情報を簡単に検索してみてください。

| サーバー インベントリ | | | | | | | | | |
|-------------|------------|------------------------------|-----------------|---------------------|----------------|---------------|------------|-----------------------------|-----|
| 2025/09/23 | | 合計 | 5件 | + 適用されたフィルターがありません。 | | | | | |
| OS Type | > | Model | > | Serial | | 機能活性化ガイド | 変更履歴の照会 | カラム設定 | CSV |
| History | Connection | Host Name | Alias Name | Server Type | External IP | Default Group | OS Type | OS | |
| | | ip-172-31-36-165.ap-north... | | Virtual | 172.31.36.165 | | Linux/A... | Amazon 2 5.10.237-230.94 | |
| | ✓ | rocky9arm | 리눅스_운영_ARM_01 | Virtual | 192.168.12.128 | production | Linux/R... | Rocky 9.4 5.14.0-427.28.1.ε | |
| | ✓ | rocky9-vm | 리눅스_운영_서버_01 | Virtual | 192.168.1.84 | production | Linux/R... | Rocky 9.4 5.14.0-427.31.1.ε | |
| | ✓ | nmstest | | Virtual | 192.168.1.76 | | Linux\U... | Ubuntu 22.04 5.15.0-144-ge | |
| | ✓ | KHUNLEE-LAPTOP | 테스트용_windows_랩탑 | Physical | 192.168.10.117 | test | Windows | Windows 11 2009 (Version | |

フィルター

フィルター入力欄をクリックし、目的の **フィルターキー** と **条件** を選択して値を入力し、**適用** ボタンをクリックしてください。サーバーインベントリー覧領域でフィルタリングされた一覧を確認できます。

- **フィルタキー**：フィルターはサーバー インベントリメニューで提供される基本収集カラムとユーザーが定義したカスタムカラムを基準に設定できます。
 - 基本収集カラム：サーバー インベントリで自動収集されたデータ項目であり、**サーバータイプ**、**基本グループ**、**OSタイプ**、**OSバージョン**、**モデル**、**シリアル**カラム項目です。
 - カスタムカラム：ユーザーがプロジェクトごとに追加して管理する項目です。
- **条件**：フィルターの条件は、**≥**、**≤**、**>**、**<**などの数字型条件と一致、不一致、包含、不包含などの文字列条件で設定できます。

ソート

ソートオプションによって最大3段階のマルチソートが可能です。カスタムカラムを含め、希望する項目を基準にソートできます。デフォルトのソート設定は**OSタイプ**>**モデル**>**シリアル**です。

ⓘ メニューの移動と更新時にソートは初期化されます。

ヒストリー照会

サーバーインベントリの過去データ照会、変更履歴照会、日別比較を通じてサーバーの変化過程を追跡できます。

過去データ照会

毎日午前0時基準で保存されたスナップショットデータを読み出し、過去データや特定フィールドの変更履歴を確認できます。

1. YYYY/MM/DD  ボタンをクリックします。
2. 照会する過去の日付を選択し、**確認** ボタンをクリックして照会します。

 過去データ照会時、**修正**、**CSVアップロード**、**カラム設定** 機能は使用できません。
テーブルの **Connection** フィールドは自動的に非表示になります。

変更履歴照会

選択したサーバーの特定フィールド値が照会区間の間、日ごとにどのように変更されたかを確認でき、そのフィールドの生成および削除履歴もあわせて照会できます。

1. **サーバー インベントリ**で  **変更履歴照会** ボタンをクリックします。
2. **インベントリ変更履歴検索** ウィンドウで照会する日付、サーバー、カラム名を選択します。
3. 選択した条件に従って日別の変更履歴を確認します。

日別比較

選択したサーバーの2つの日付を指定し、データ変更内容やフィールドの生成・削除有無を比較できます。

1. 比較するサーバーの **History**  アイコンをクリックします。
2. **ヒストリー照会**で **基準日** と **比較日** を選択してデータを比較します。

カラム設定

カラム設定 ボタンをクリックしてください。 次のようにカラムを選択してカスタムカラムを追加した後、下にある**確認**ボタンをクリックしてカラムの設定を保存します。

カラム設定

表示するカラムを選択してください。

☐ すべて選択

+ カラム追加

初期化

☐

カラム名

 custom

✎

✕

☐

カラム名

 custom

✎

✕

☐

カラム名

 custom

✎

✕

☒ サーバー名
 ☒ サーバー別名
 ☒ サーバータイプ
 ☒ IP Address
 ☒ 基本グループ
 ☒ OSタイプ
 ☒ OSバージョン
 ☒ モデル
 ☒ シリアル
 ☒ ファームウェア
 ☒ Numa Node
 ☒ X86 Socket
 ☒ CPU Type
 ☒ CPU Cores
 ☒ Logical Cores

カラム名で検索

表示項目(20)

サーバー名

サーバー別名

サーバータイプ

IP Address

基本グループ

OSタイプ

OSバージョン

モデル

シリアル

ファームウェア

Numa Node

X86 Socket

CPU Type

CPU Cores

Logical Cores

キャンセル

確認

・ カラム選択

ユーザーはテーブルに表示するカラムを選択できます。 **初期化**ボタンを選択すると、デフォルト項目の選択状態に戻ります。

- ① 選択した **カラム** はブラウザのクッキーに保存され、ページを更新しても状態が維持されます。クッキーが削除されたり、他の理由で設定エラーが発生した場合は、デフォルト項目の選択状態に初期化します。

- **カラム追加**

ユーザーは + **カラム追加** ボタンを選択した後、基本提供項目に加えて、自分が望む項目を追加してカスタムカラム(**custom**)を構成できます。必要に応じてカラムを追加し、サーバーの状態とパフォーマンスをより細かくモニタリングしてみてください。

CSVダウンロードとアップロード

CSVダウンロード

⬇ **ダウンロード** ボタンを選択して、収集されたサーバーインベントリを **CSV** ファイル形式でダウンロードできます。

CSVアップロード

サーバー構成情報を大量に入力する必要がある場合、個々のデータを手作業で入力するのに多くの時間がかかります。**CSVファイル**アップロード機能により、大量のデータ入力を効率的に処理できます。ダウンロードした**CSV**ファイルを修正してアップロード機能を活用してみてください。

1. ⬆ **CSV アップロード** ボタンをクリックし、アップロードする **CSV** ファイルを選択してください。
2. **CSV検証** ウィンドウで、アップロードされたデータの検証結果を確認してください。
 - 変更される項目及びエラー項目の件数を確認できます。

| X CSV 保証 | | | | | | | | | | | |
|----------|------------|-----------------|---------|-------------|------------|--------------|--------------|-------------|--------------|---|--|
| 保証結果 | | | | | | | | | | | |
| 変更件数 1 | | | | | | | | | | | |
| Error 0 | | | | | | | | | | | |
| No. | id | | | | | | | | | | |
| 1 | 1906460792 | virtual-gpu-a- | Virtual | 10.21.1.26 | APM DEMO | Linux/Ubuntu | Ubuntu 22.04 | Amazon EC2 | c2v5fa4.33- | - | |
| 2 | 1816982090 | mysql-official- | Virtual | 10.21.3.69 | DPF DEMO | Linux/Ubuntu | Ubuntu 22.04 | Amazon EC2 | c2v1arf7-0- | | |
| 3 | 2142472185 | mysql-official- | Virtual | 10.21.1.247 | DPF DEMO | Linux/Ubuntu | Ubuntu 22.04 | Amazon EC2 | c2v637b-e0- | | |
| 4 | 780292294 | mysql-official- | Virtual | 10.21.1.223 | DPF DEMO | Linux/Ubuntu | Ubuntu 22.04 | Amazon EC2 | c2v682d4-c- | | |
| 5 | 643422279 | go-official-de- | Virtual | 10.21.1.118 | APM DEMO | Linux/Ubuntu | Ubuntu 22.04 | Amazon EC2 | c2v581c-80f- | | |
| 6 | 1786431657 | qa-php-demo | Virtual | 10.21.3.75 | APM QA | Linux/Ubuntu | Ubuntu 22.04 | Amazon EC2 | c2v328D-79- | | |
| 7 | 1413588424 | php-official-d- | Virtual | 10.21.3.223 | APM DEMO | Linux/Ubuntu | Ubuntu 22.04 | Amazon EC2 | c2v7d6a5-9- | | |
| 8 | 478184937 | ip-10-21-1-200 | Virtual | 10.21.1.200 | | | | Amazon EC2 | c2v618e6-8f- | | |
| 9 | 84695083 | rum-official-d- | Virtual | 10.21.1.151 | BROWSER DE | Linux/Ubuntu | Ubuntu 22.04 | Amazon EC2 | c2v473e-f24- | | |
| 10 | 868519645 | wpm-official- | Virtual | 10.21.1.181 | WPM DEMO | Linux/Ubuntu | Ubuntu 22.04 | Amazon EC2 | c2v4c67d-a5- | | |
| 11 | 1393962412 | qa-node-demo | Virtual | 10.21.1.241 | APM QA | Linux/Ubuntu | Ubuntu 22.04 | Amazon EC2 | c2v30c91-6- | | |
| 12 | 1341918756 | node-official- | Virtual | 10.21.1.98 | APM DEMO | Linux/Ubuntu | Ubuntu 22.04 | Amazon EC2 | c2v4014a-65- | | |
| 13 | 332295967 | python-demo- | Virtual | 10.21.1.254 | APM DEMO | Linux/Ubuntu | Ubuntu 22.04 | Amazon EC2 | c2v29f4-db- | | |
| 14 | 2078406413 | python-demo- | Virtual | 10.21.1.43 | APM DEMO | Linux/Ubuntu | Ubuntu 22.04 | Xen (HVM do | c2v113a-c5- | | |
| 15 | 1187373871 | EC2AMAZ-J7- | Virtual | 10.21.1.227 | | Windows | Microsoft Wi | Amazon EC2 | c2v024D-90- | | |

- エラー項目をクリックすると、右側の変更データ一覧内でエラーが発生した項目に移動し、エラー項目はハイライトされます。

| X CSV 验证 | | | | | | | | | |
|--|----|------------|------------------|---------|-------------|--------------|--------------|---------------|-------------------------------|
| 验证结果 | | | | | | | | | |
| 变更行数 0 | | | | | | | | | |
| Error 2 | | | | | | | | | |
| 16.8 / rd
数据库 L7.5.0. (round update pk0.) | 2 | 1816482090 | mysql-official.. | Virtual | 10.21.3.69 | DPM DEMO | Linux/ubuntu | Ubuntu 22.04. | Amazon EC2 ... ec2i8ff47-07.. |
| 16.8 / rd
数据库 L7.5.0. (round update pk0.) | 3 | 2142472185 | mysql-official.. | Virtual | 10.21.1.247 | DPM DEMO | Linux/ubuntu | Ubuntu 22.04. | Amazon EC2 ... ec2a37b8-0e.. |
| 16.8 / rd
数据库 L7.5.0. (round update pk0.) | 4 | 780329242 | mysql-official.. | Virtual | 10.21.1.223 | DPM DEMO | Linux/ubuntu | Ubuntu 22.04. | Amazon EC2 ... ec483224-c3.. |
| 16.8 / rd
数据库 L7.5.0. (round update pk0.) | 5 | 64332279 | go-official-dm.. | Virtual | 10.21.1.118 | APM DEMO | Linux/ubuntu | Ubuntu 22.04. | Amazon EC2 ... ec2581f4-d9.. |
| 16.8 / rd
数据库 L7.5.0. (round update pk0.) | 6 | 1786431637 | go-php-dm-dm.. | Virtual | 10.21.3.73 | APM QA | Linux/ubuntu | Ubuntu 22.04. | Amazon EC2 ... ec222807-79.. |
| 16.8 / rd
数据库 L7.5.0. (round update pk0.) | 7 | 1413588424 | php-official-d.. | Virtual | 10.21.3.223 | APM DEMO | Linux/ubuntu | Ubuntu 22.04. | Amazon EC2 ... ec2788a8-9f.. |
| 16.8 / rd
数据库 L7.5.0. (round update pk0.) | 8 | 978189497 | ip-10-21-1.200 | Virtual | 10.21.1.200 | | Linux/ubuntu | Ubuntu 22.04. | Amazon EC2 ... ec2408b8-8f.. |
| 16.8 / rd
数据库 L7.5.0. (round update pk0.) | 9 | 844956083 | rum-official-d.. | Virtual | 10.21.1.151 | BROWSER DE.. | Linux/ubuntu | Ubuntu 22.04. | Amazon EC2 ... ec2a73fe-f24.. |
| 16.8 / rd
数据库 L7.5.0. (round update pk0.) | 10 | 86851965 | wpm-official-d.. | Virtual | 10.21.1.181 | WPM DEMO | Linux/ubuntu | Ubuntu 22.04. | Amazon EC2 ... ec24c670-45.. |
| 16.8 / rd
数据库 L7.5.0. (round update pk0.) | 11 | 1393964262 | q4-node-dm-dm.. | Virtual | 10.21.2.241 | APM QA | Linux/ubuntu | Ubuntu 22.04. | Amazon EC2 ... ec230c90-1a.. |
| 16.8 / rd
数据库 L7.5.0. (round update pk0.) | 12 | 1341918756 | node-official.. | Virtual | 10.21.1.98 | APM DEMO | Linux/ubuntu | Ubuntu 22.04. | Amazon EC2 ... ec240248-65.. |
| 16.8 / rd
数据库 L7.5.0. (round update pk0.) | 13 | 332299567 | python-dm-dm.. | Virtual | 10.21.1.254 | APM DEMO | Linux/ubuntu | Ubuntu 22.04. | Amazon EC2 ... ec2a29c4-0b.. |
| 16.8 / rd
数据库 L7.5.0. (round update pk0.) | 14 | 207840643 | python-dm-dm.. | Virtual | 10.21.1.43 | APM DEMO | Linux/ubuntu | Ubuntu 22.04. | Xen (PVM do... ec2c8113a-c5.. |
| 16.8 / rd
数据库 L7.5.0. (round update pk0.) | 15 | 1187373871 | EC2MAZ-J7.. | Virtual | 10.21.1.227 | | Windows | Microsoft W.. | Amazon EC2 ... ec20420-90.. |
| 16.8 / rd
数据库 L7.5.0. (round update pk0.) | 16 | 978189497 | ip-10-21-1.200 | Virtual | 10.21.1.200 | | Linux/ubuntu | Ubuntu 22.04. | Amazon EC2 ... ec2c8188-8f.. |

3. データの検証後、問題がなければ **適用** ボタンをクリックして、選択した **CSV** ファイルのサーバー構成情報を適用してください。

- ① • CSVアップロード時**サーバー別名**、**基本グループ**及びカスタムカラム(**custom**)の変更点のみ適用します。
- CSVアップロード時に、事前に登録していないカラムは反映しません。

修正

✎ **修正** ボタンを選択して、サーバーインベントリ一覧を修正できます。

- ・ **サーバー別名と基本グループカラム**の内容を設定できます。
- ・ ユーザーが追加した**カスタムカラム**(**custom**)の内容を設定できます。

サーバーリスト

WhaTapモニタリングサービスの初期画面でプロジェクトを選択し、**サーバーリスト**>**サーバーリスト**メニューを選択します。**サーバーリスト**は、収集サーバーの全体状況を表示し、サーバーの管理機能およびサーバー間の比較機能を提供します。

サーバーリスト

|| LIVE 08:25:52

全体 11

非活性 3

警告 7

正常 1

1

エージェント名, IP

Q

2

▽

適用されたフィルターがありません。

☆

3

カラム設定

リフレッシュ

移動

CSV

比較

管理

| | | サーバー情報 | CPU | メモリ | ディスク ▾ | | ネットワーク ▾ | その他 |
|----|----|-----------------|----------------------|----------------------------|--------------------|-------------------|-----------|---------------------|
| 状態 | 詳細 | エージェント名 | CPU Used % | メモリ使用量% | ディスク使用%(最大) | ディスクI/O率(最大) | トラフィック(i) | PRIVATE_IP |
| ⚠ | 🔍 | 25fd76273a2 | > 37.9% <div></div> | 32.1% (4.9G) <div></div> | 79.05% <div></div> | 0.06% <div></div> | lo 0 | 127.0.0.1 |
| ⚠ | 🔍 | 64311a6a8bb1 | > 38.03% <div></div> | 32.1% (4.9G) <div></div> | 79.05% <div></div> | 0.06% <div></div> | lo 0 | 127.0.0.1 |
| ⚠ | 🔍 | 9ae35ad8c03b | > 38.12% <div></div> | 32.1% (4.9G) <div></div> | 79.05% <div></div> | 0.02% <div></div> | lo 0 | 127.0.0.1 |
| ⚠ | 🔍 | 9e6a0322b3a2 | > 38.03% <div></div> | 32.1% (4.9G) <div></div> | 79.05% <div></div> | 0.06% <div></div> | lo 0 | 127.0.0.1 |
| ⚠ | 🔍 | d374f2cebf49 | > 38.03% <div></div> | 32.1% (4.9G) <div></div> | 79.05% <div></div> | 0.06% <div></div> | lo 0 | 127.0.0.1 |
| ⚠ | 🔍 | qa-compose-demo | > 38.06% <div></div> | 32.1% (4.9G) <div></div> | 79.05% <div></div> | 0.06% <div></div> | ens5 1M | 10.21.11.118 / 1... |
| ⚠ | 🔍 | qa-region | > 12.05% <div></div> | 86.78% (26.6G) <div></div> | 85.47% <div></div> | 1.92% <div></div> | lo 8.3M | 10.21.11.187 / 1... |
| ✅ | 🔍 | qa-node-demo | > 11.96% <div></div> | 15.51% (1.1G) <div></div> | 47.59% <div></div> | 0.06% <div></div> | lo 30.7M | 10.21.1.241 / 12... |
| 🔍 | 🔍 | | > 0% <div></div> | 0% <div></div> | 0% <div></div> | 0% <div></div> | 0 | 10.21.1.241 |

1 データ更新・サーバーステータス・検索

データ更新

サーバーリストページのデータは60秒ごとに自動で更新されます。ユーザーは停止した自動更新を再開することができます。

- || 一時停止：該当エージェントのイベント発生を一時停止します。サーバーリストでは一時停止状態として表示されます。

-  **再起動**：一時停止されたイベントを再開します。対象エージェントでイベントの発生を確認できます。

サーバー状態

収集サーバーのステータスを表示します。ステータス情報は1分間隔で自動的に更新されます。

-  **非活性**：エージェントは、そのサーバーからデータを収集できない状態です。
-  **危険**：収集サーバーで危険イベントが発生した状態です。
-  **警告**：収集サーバーで警告イベントが発生した状態です。
-  **正常**：エージェントが収集サーバーで正常に動作している状態です。
-  **アラート停止**：選択されたサーバーのイベント発生が一時停止された状態です。

検索

右上の  検索ボックスを使って、エージェント名やIPを検索できます。

2 フィルター

入力画面に値を直接入力するか、フィルターを追加するようにフィルターを指定できます。フィルタータグは **フィルターキー**、**条件**、**検索値** の順に入力します。

フィルターキー、条件、検索値を入力

- **フィルターキー** 入力時エージェント名、CPU Used %、Memory Used %、Disk Used %、Disk I/O %、Network Traffic、private_ipオプションを提供します。
- **条件** 入力時 >、<、<=、>=、==、!= 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。

フィルタータグの削除

- Backspaceで削除することができます。
- タグのXアイコン選択時にタグを削除できます。
- 入力ウィンドウの全体削除、Xアイコンを選択すると、タグ全体を削除できます。

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、除去および既存のお気に入りを選択できます。

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 条件キー 、 検索値 は入力できません。
- 条件キー 、 検索値 のいずれか一つでもないタグが存在する場合は検索できません。無効なタグの場合 灰色で表示します。

3 サーバーステータス

エージェントが割り当てられたサーバー全体のステータスを示します。エージェント名の一覧からエージェントを選択すると、サーバー 詳細ページに移動します。サーバー 詳細メニューの詳細については、[次の文書](#)を参照してください。

ファイルシステム情報

ファイルシステム情報は、ファイルシステムを詳しく見たいエージェント名の左側🔍アイコンをクリックすると確認できます。

カラム設定

- カラム設定

3 領域の上部の **カラム設定** ボタンをクリックすると、テーブルに表示するカラムを選択できます。

カラム設定
リフレッシュ
フィルター
移動
CSV
比較
管理

すべて選択
すべて解除
初期化(既定値)

Default

| CPU | ディスク | メモリ | ネットワーク | サーバー情報 | その他 |
|--|--|---|--|--|--|
| ☐ CPU Idle
☐ CPU I/O待ち
☐ CPU IRQ使用率
☐ CPU平均負荷1分
☐ CPU平均負荷15分
☐ CPU平均負荷5分
☐ CPU nice値使用率
☐ CPU SOFT IRQ
☐ CPU Steal使用率
☐ CPUシステム使用率
☒ CPU Used %
☐ CPUユーザー使用率 | ☐ ディスクブロックサイズ
☐ ディスクフリー率
☐ ディスクフリースペース
☐ ディスク Inode Total
☐ ディスク Inode Used
☐ ディスク Inode Used %
☐ ディスクI/O率
☒ ディスクI/O率(最大)
☐ ディスクキューサイズ
☐ ディスク読取りBps
☐ ディスク読取りIOPS
☐ ディスク容量
☐ ディスク使用%
☒ ディスク使用%(最大)
☐ ディスク使用量
☐ ディスク書き込みBps
☐ ディスク書き込みIOPS | ☐ メモリバッファ
☐ キャッシュメモリ
☐ フリーメモリ
☐ メモリページフォルト
☐ 共有メモリ
☐ トータルスワップメモリ
☐ スワップメモリ使用量
☐ 合計メモリ
☒ メモリ使用量% | ☐ ネットワークドロップ(インバウンド)
☐ ネットワークドロップ(アウトバウンド)
☐ ネットワークエラー(インバウンド)
☐ ネットワークエラー(アウトバウンド)
☐ ネットワークIP
☐ ネットワークパケット(インバウンド)
☐ ネットワークパケット(アウトバウンド)
☐ ネットワークトラフィック
☒ ネットワークトラフィック(最大)
☐ ネットワークトラフィック(インバウンド)
☐ ネットワークトラフィック(アウトバウンド) | ☐ CPUコア
☐ OID
☐ ホスト名
☐ OSアーキテクチャ
☐ OS CPUベンダー
☐ OSメモリ
☐ OS名
☐ OSバージョン | ☐ エージェント作成からの経過時間
☒ IP
☐ ファイル記述子
☐ パブリックIP
☐ サーバー時間
☐ タグ
☐ 起動後経過時間
☐ エージェントバージョン |

① 選択したカラムは、ブラウザのクッキー値として保存されます。また、ページの更新後もステータスが維持されます。クッキーの削除またはその他の理由で設定エラーが発生した場合、すべて選択に初期化されます。

- カラム幅設定

カラムタイトルの端をドラッグして、カラム幅を設定できます。

- カラムソート

カラムのタイトルをクリックすると、昇順または降順の並べ替えが可能です。

① カラム幅 および カラムソート 設定値は、ブラウザクッキーとして保存され、ページの更新後もステータ

- ① スが維持されます。クッキーの削除またはその他の理由で設定にエラーが発生した場合は、未設定状態でリセットされます。

プリセット管理

サーバーリスト > サーバーリストで  カラム設定ボタンをクリックすると、プリセットを管理・共有できます。

選択したカラムの組み合わせはプリセットで保存でき、同一プロジェクトにアクセスした他のユーザーと共有されます。最近使用したプリセットは個人ブラウザに保存され、再接続時に自動的に読み込まれます。最近プリセットが削除された場合、基本プリセット(デフォルト)に初期化されます。プリセットの設定方法は[次の文書](#)を参照してください。

- ・ カラムごとの幅とソート状態は、ユーザーのブラウザに保存され、メニューへの再接続時に自動的に適用されます。この設定はユーザー個人にのみ適用され、他のユーザーと共有することはできません。

 **プロジェクトの修正権限を持つユーザーのみがプリセットを保存・削除できます。**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。

リフレッシュ

 リフレッシュボタンをクリックすると、現在の時刻を基準にデータを更新できます。

エージェント移動

 移動ボタンを選択して、エージェントを他のプロジェクトに移転できます。

エージェント移動



i サーバープロジェクトにインストールされたエージェントを他のプロジェクトに移動できます。 ×
A、Bプロジェクトと移動対象エージェントを選択してから、真ん中の→(移動)ボタンをクリックしてください。

Server Monitoring Demo (29763)

エージェント検索

選択済エージェント: 0

- ☐ 全体
- ☐ rum-official-demo
- ☐ demo-k8s-master
- ☐ demo-k8s-worker-01
- ☐ mysql-official-demo-02
- ☐ node-official-demo
- ☐ virtual-java-agent
- ☐ go-official-demo
- ☐ url-official-demo
- ☐ python-demo-target
- ☐ python-demo-attack
- ☐ demo-k8s-worker-03
- ☐ demo-k8s-worker-04

β. プロジェクト選択

> <

エージェントを移動してから10分が経たない内に再度同一エージェントを移動する場合、衝突現象が発生する場合があります。(非同期処理)

⇐ 保存

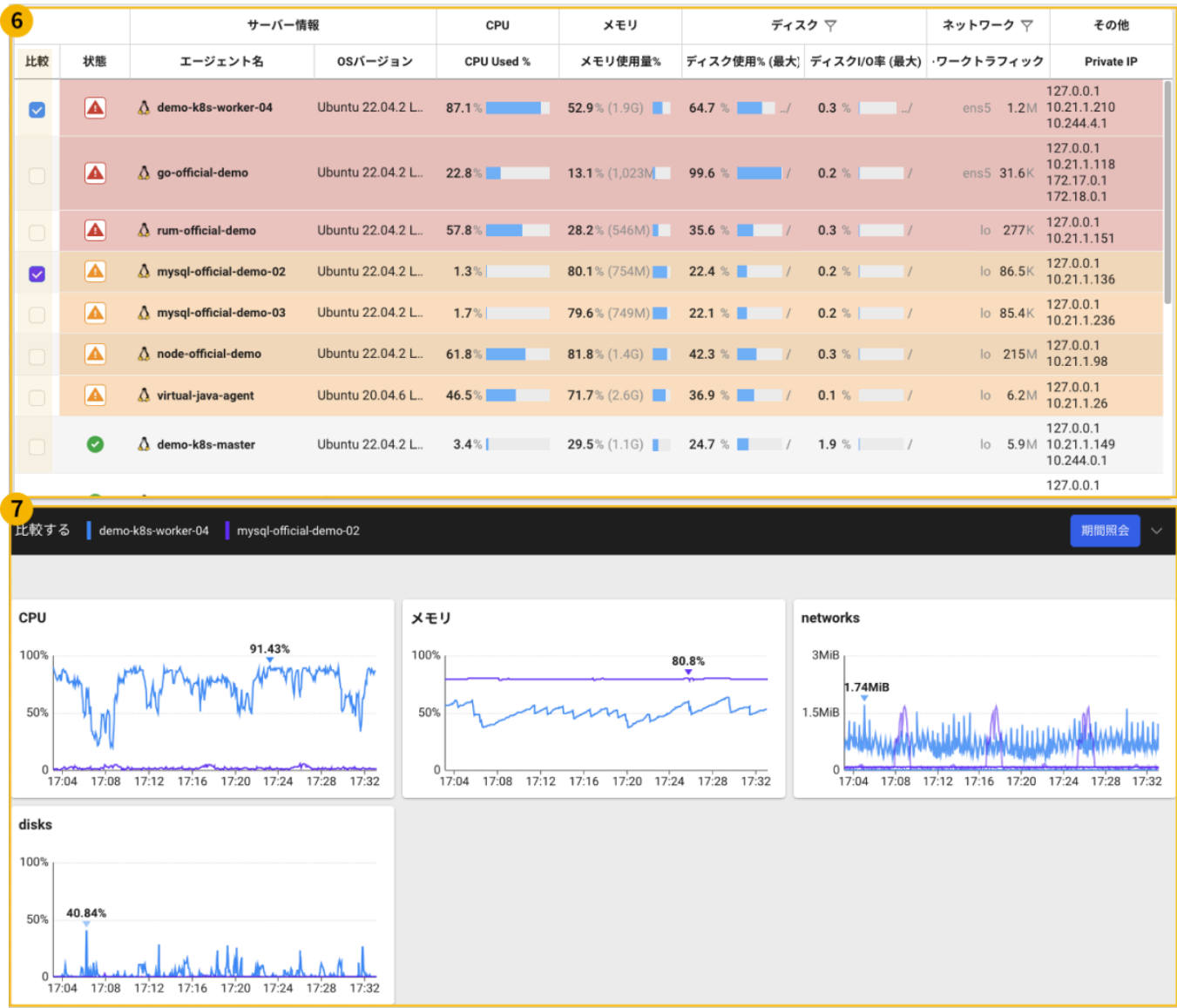
1. 右側の画面で、移動する対象プロジェクトを選択します。
2. 左側の画面で、移動するエージェントを選択します。
3. > 右矢印 ボタンをクリックして、対象プロジェクトに移動します。
4. 保存ボタンをクリックすると移転が完了します。

i • 実行から10分以内に同じエージェントを再度移動する場合、クラッシュが発生する可能性があります。

- ❗ 収集されたデータは移動されません。履歴データを参照するために、既存のプロジェクトは削除しないでください。

サーバー間の比較

🔗 比較ボタンをクリックすると、サーバー間の比較チャートが次のように提供されます。



1.  比較ボタンを選択します。
2.  をサーバーリストの左側に比較カラムが追加されます。
3. 比較カラムで比較するサーバーを選択します。
4. 比較機能を有効にすると  領域で比較チャートを参照することができます。

-  ・ 比較サーバーは最大5つまで選択できます。
- ・ サーバーごとに色が割り当てられます。色は  比較する でサーバーを区別するために使用されます。
- ・ 期間照会ボタンをクリックすると、履歴データを照会できます。

モニタリング管理

エージェントコマンドを通じてサーバーを管理する機能です。 管理 ボタンをクリックすると、管理機能を適用するサーバーを選択できます。その後、 通知停止、 通知 再起動、 除外 ボタンが有効になります。

- ・  通知停止：選択したサーバーでのイベント発生を一時的に停止します。
- ・  通知 再起動：選択されたサーバーのうち、通知停止状態のサーバーに対してイベント通知を再度有効化します。該当エージェントのイベント発生を確認できるようになります。
- ・  除外：選択されたサーバーの動作を停止します。サーバー一覧から除外され、サーバーのステータスは確認できなくなります。

非アクティブエージェントの保持期間

非アクティブエージェントの保持期間は、データ収集が停止したエージェントをサーバー一覧から自動的に削除するまでの期間です。サーバー一覧画面上部のステータス要約（全体・非アクティブ・危険・正常）領域の横で設定し、設定した期間にわたって非アクティブ状態が続くと、該当エージェントはサーバー一覧から自動的に削除されます。保持期間を短く設定すると、使用しなくなったサーバーが一覧に残る時間を短縮できます。

この設定はプロジェクト単位で適用され、選択できる保持期間は次のとおりです。

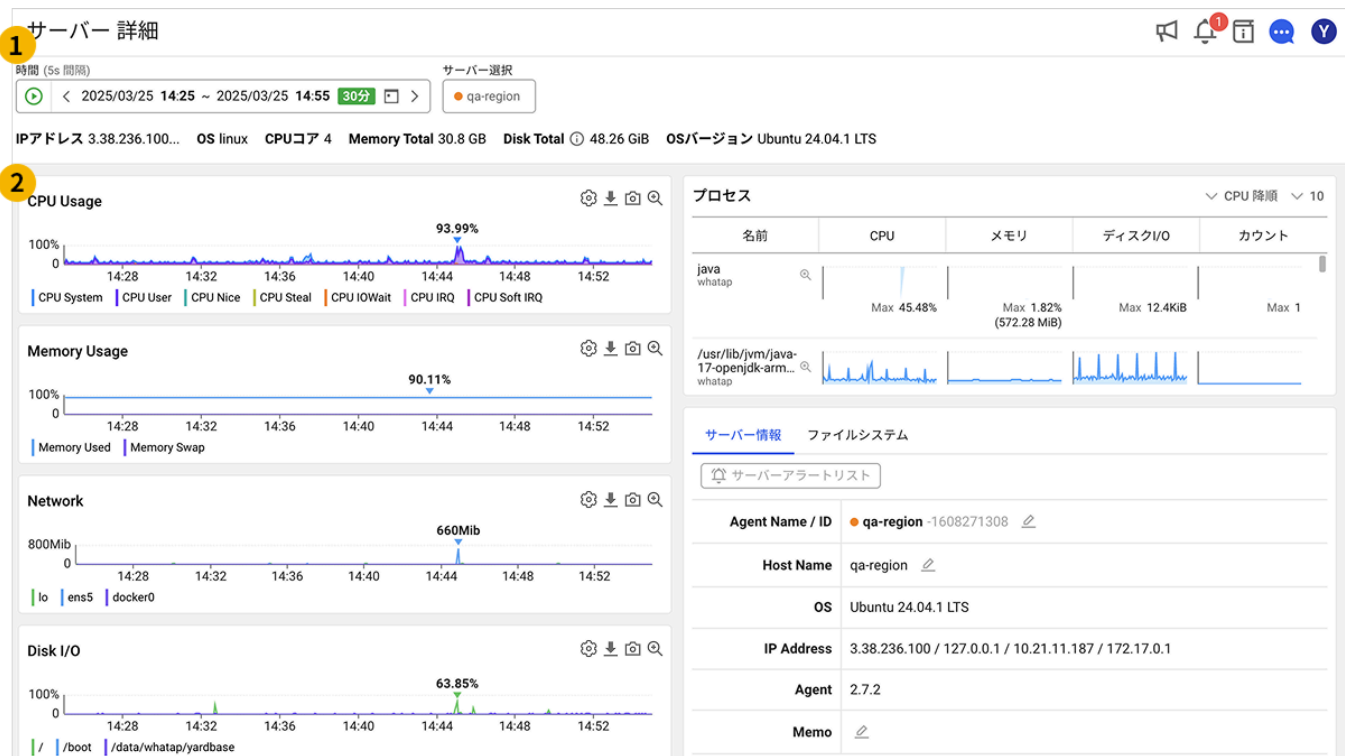
| Option | Description |
|--------|--------------------|
| 1日 | 非アクティブ状態が1日続くと自動削除 |

| Option | Description |
|--------|---------------------------------|
| 3日 | 非アクティブ状態が3日続くと自動削除 |
| 7日 | 非アクティブ状態が7日続くと自動削除 |
| 1か月 | 非アクティブ状態が1か月続くと自動削除 |
| 削除しない | 非アクティブエージェントを自動削除せず一覧に保持（デフォルト） |

- ⓘ • プロジェクトの修正権限を持つユーザーのみ、非アクティブエージェントの保持期間を設定できます。
- 上記の選択肢にない値がすでに設定されている場合、その値が一時オプションとして表示されます。

サーバー詳細

WhaTapモニタリングサービスの初期画面でプロジェクトを選択し、**サーバーリストメニューのサーバー 詳細**を選択します。**サーバー 詳細**は、サーバーのリソース状況と実行プロセスの詳細情報を提供します。



1 上部オプション

上部の **1** エリアでは、**データ更新時間** と参照対象の **サーバー** を指定できます。**データ更新時間** および **サーバー** の指定オプションとあわせて、該当サーバーの **サマリー情報** を確認できます。

データ更新時間

サーバー詳細ページのデータは5秒ごとに自動的に更新されます。

- 一時停止：該当エージェントのイベント発生を一時停止します。サーバーリストでは一時停止状態として表示さ

れます。

-  **再起動**：一時停止されたイベントを再開します。対象エージェントでイベントの発生を確認できます。

サーバー選択

サーバー選択オプションを使用すると、詳細を表示するサーバーを指定できます。リスト照会時**非アクティブサーバー**の表示可否を設定できます。選択画面の一覧から照会するサーバーを選択すると、次の②領域でサーバーリソースの状況や実行プロセスの詳細情報を確認できます。

②サーバー詳細

サーバーリソースの状態

②の領域では、CPU Usage、Memory Usage、Network、Disk I/Oチャートを使用して、サーバーのリソース状況を確認できます。

-  : チャート設定でY軸の最大値を指定できます。
-  : チャートの記録をCSVファイルとして保存できます。
-  : チャートの画面をイメージファイルで保存できます。
-  : CPU使用率、メモリ使用率、ネットワーク、ディスクI/Oの各詳細チャートを確認できます。
 - CPU使用率
CPU Usage, CPU Idle, CPU Nice, CPU I/O Wait, CPU Steal, CPU IRQ, CPU Soft IRQ, CPU Load
 - メモリ使用率
Memory Usage, Memory Available, Memory SReclaimable, Memory SUNreclaim, Memory Slab, Memory Swap Used, Memory Page Faults
 - ネットワーク
Traffic In/Out, Packet In/Out, Error In/Out, Dropped In/Out
 - ディスクI/O
Disk I/O, IOPS Read/Write, Disk Bph Read/Write, Used Space, Queue Length, Inode Used, Free Space

プロセスリスト

ソート

- プロセス一覧の上から指標を選択し、降順または昇順でソートおよび照会できます。
- プロセス一覧の上から指標を選択し、上位の10個、20個、30個、全体のプロセスを指定して確認できます。

グループ化

プロセスグループは、一つのインスタンスから同じく動作する複数のプロセスをまとめたものです。グループ化ボタンを選択し、プロセスグループを追加できます。プロセスのグループ化の詳細については、[次の文書](#)を参照してください。

サーバー情報パネル

サーバー情報 パネルで確認できる内容は次のとおりです。Agent Name および Memo は、サーバー情報 パネルでのみ編集可能です。

- **サーバーアラートリスト**

サーバー情報 パネル上部の  **サーバーアラートリスト** ボタンを選択すると、現在のサーバーに割り当てられているアラートを確認できます。

- **Agent Name / ID**

選択したサーバーの[エージェント名](#)(ONAMEのエイリアス)と[サーバーID](#)(OID)を確認できます。 ボタンを選択すると、[エージェント名](#)を変更できます。

 ONAMEは、デフォルトでホスト名が設定されます。

- **OS**

選択したサーバーのOS情報を確認できます。

- **IP Address**

選択したサーバーのIPアドレスを確認できます。

- **Agent**

選択したサーバーのエージェントのバージョンを確認できます。

- **Memo**

作成したメモを確認するか  ボタンを選択してメモを編集および追加できます。

プロセスグループの追加

プロセスグループとは？

プロセスグループは、インスタンスに対して同じアクションを実行する複数のプロセスのグループです。個別のプロセスではなく、グループ単位でモニタリングまたは通知を受け取る場合は、プロセスグループを使用してください。

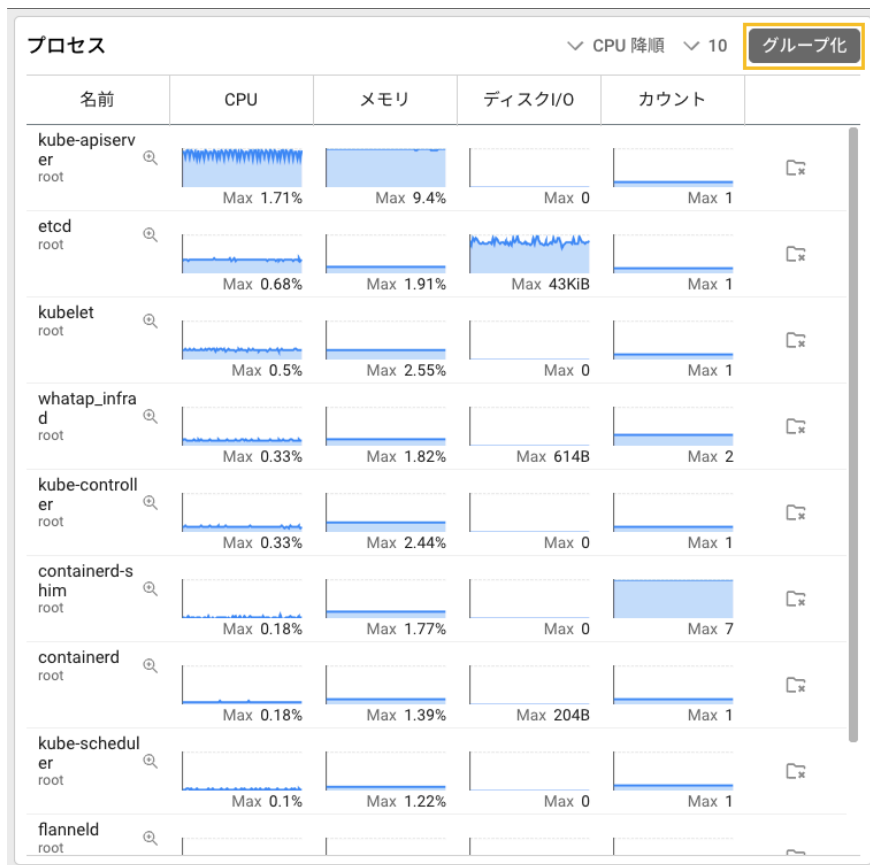
プロセスグループのメニューでは、既存の各プロセスのリソース使用量の合計を一目で確認できます。個々のプロセスのリソース使用量を計算する必要はありません。

プロセスグループのリソース使用量の合計が特定のしきい値を超えたときに通知されるように指定できます。通知の設定に関する詳細は、[次の文書](#)を参照してください。

プロセスグループの追加

❗ プロジェクト修正権限または通知設定権限が必要です。権限の詳細については、[次の文書](#)を参照してください。

1. ホーム画面> プロジェクト選択> サーバーリスト> サーバー 詳細に移動した後、プロセス一覧でグループ化ボタンをクリックします。



- プロセスグループ設定ウィンドウが表示されたら、グループに含めるプロセス名パターンをパターンに、前後のアスタリスク(*)を含めて入力します。

例) whatap → *whatap*

Process Group

Pattern

ex) *whatap*

Pattern 別名

i プロセスのパターン名を別称として変更します。

入力後、右側の **Q** ボタンを選択します。そのパターンに該当するプロセスの一覧を照会できます。プロセス名は、画面に表示されるプロセス名を基準とします。

3. **Pattern**別名にプロセスグループ名を入力し、右側の**適用**ボタンを選択します。グループ化は**設定したプロジェクトのすべてのサーバー**で実行されます。

プロセスグループの例

- プロセスグループ化適用

次の画面は、**Pattern**に*tomcat*を入力し、**Pattern**別名をtest_groupとして適用した例です。



Process Group

Pattern

tomcat

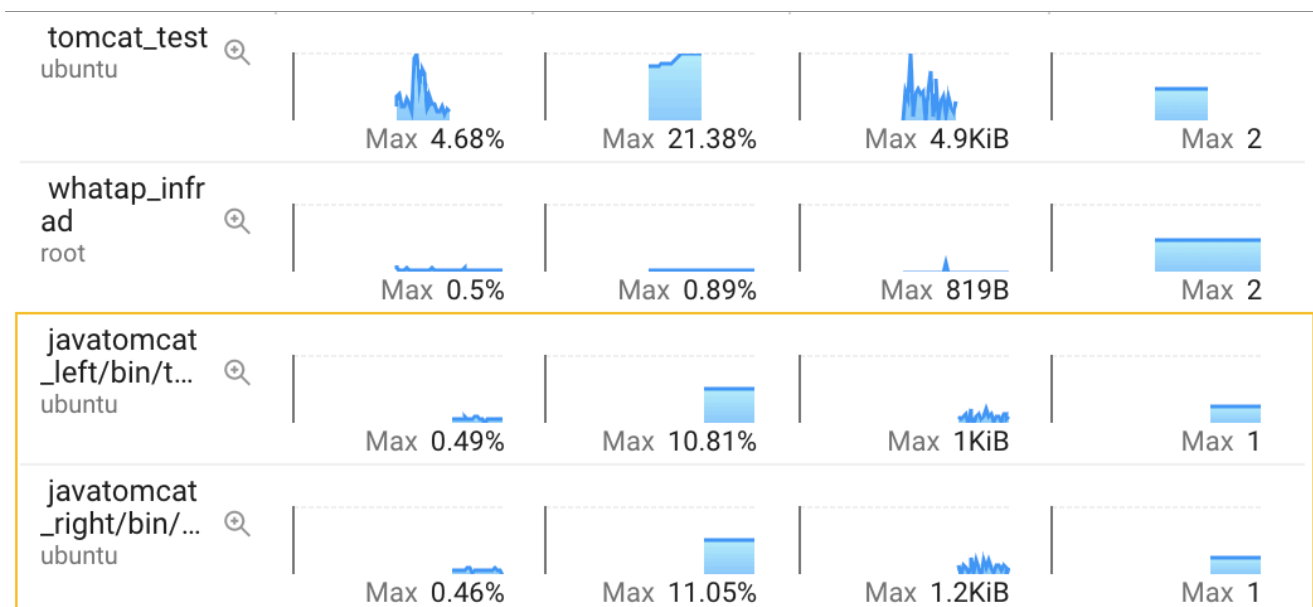
Pattern 別名

test_group

適用

i プロセスのパターン名を別称として変更します。

- プロセスグループ化以前のプロセス一覧



パターンに合わせてグループ化するプロセス一覧は次のとおりです。

- 例) javatomcat_left/bin/test.jarcom.virtual.App
- 例) javatomcat_right/bin/test.jarcom.virtual.App

• プロセスグループ化登録確認

新しいプロセスグループtest_groupが、次のようにプロセス一覧に登録されていることが確認できます。

プロセスグループ化登録確認

- ① グループ化の適用後、プロセスグループで各プロセスに対応するデータの計算された数値を確認できます。
- グループ化以前のデータを確認する場合、プロセス別にデータを確認する必要があります。

WhaTap GPU モニタリング

WhaTap GPU モニタリングは、サーバーおよびKubernetes環境全体にわたって、GPUリソースの状態と活用状況を統合的に分析できるよう支援します。GPUはサーバーを構成するリソースの一つですが、CPUやメモリと比べてコストが高く、AI/ML、LLM、HPCワークロードのパフォーマンスに直接影響を与える重要なリソースです。

単にGPUが搭載されていて、正常に動作しているかを確認するだけでなく、現在どの程度活用されているか、どのタスクが占有しているか、異常な兆候はないか、リソース配置は適切かまでを確認する必要があります。

WhaTap GPU モニタリング範囲

❗ WhaTap GPU モニタリング対応環境

- Server環境でのGPUモニタリング
- Kubernetes環境でのGPUモニタリング

サーバー環境

- GPU サーバーモニタリングは、GPU使用率、メモリ使用量、温度、電力、クロック、エラー、PCIe/NVLink通信状態などの主要指標を定期的に収集・保存し、サーバーインフラの観点からGPUデバイスの状態を総合的に把握できるよう支援します。
- GPUを使用しているプロセスの占有状況も合わせて提供するため、どのタスクがどのGPUをどの程度使用しているかを把握できます。これにより、単純なデバイス状態の確認を超えて、サーバー内のGPUリソースの実際の活用方法まで分析できます。
- モニタリングにより、過熱、スロットリング、電力制限、異常エラー、PCIe/NVLink通信異常などの兆候を早期に検出でき、障害予防と迅速な対応体制を整えることができます。これはサービスの安定性確保と運用効率の向上に直接貢献します。

Kubernetes環境

- Kubernetes環境では、GPUは主にAI学習/推論ワークロード、バッチジョブ、高性能演算アプリケーションに割り当てて使用されます。この場合、ノード単位のGPU状態のみを確認するだけでは、実際の運用状況を十分に把握す

ることが難しい場合があります。

- WhaTapのKubernetes GPUモニタリングは、クラスター、ノード、Pod/コンテナ単位でGPUリソースの使用状況を確認できるよう支援します。これにより、どのワークロードがGPUを占有しているか、特定のノードに使用が偏っていないか、GPUリクエスト/割り当てに対して実際の使用効率はどうかなどを把握できます。
- Kubernetesの観点からのGPUモニタリングは、スケジューリングの適切性、リソースの偏り、過少/過大割り当ての有無を分析するうえでも有用です。結果的に、GPUベースのワークロード運用の安定性を高め、クラスター全体のリソース活用効率を改善できます。

エンタープライズ環境

- エンタープライズ環境では、多数のGPUサーバーとKubernetesクラスターが共同で運用されます。単一のサーバーや個別のKubernetes環境単位のGPUモニタリングだけでは、リソース全体の状態と活用状況を一目で把握することが難しいため、統合的な管理体制が必要です。
- 数百～数千枚規模のGPUを運用する企業では、チームや業務ごとに割り当てられたGPUリソースがどれほど効果的に活用されているかを継続的に確認したいと考えています。このようなデータがあってこそ、遊休リソースの再配置、新規リソースの増設、追加購入の要否などに関する合理的な意思決定に役立てることができます。
- 複数のKubernetesベースのGPU環境とベアメタルGPUサーバー環境を単一のモニタリング体制に統合することで、分散したGPUリソースを一つの視点で管理できます。これにより、組織全体のGPUリソース状況を統合的に把握し、Capacity Planningにまで連携できるエンタープライズ型GPUモニタリングを提供します。

WhaTap GPU モニタリングの提供価値

GPUリソースの可視化

サーバー、クラスター、ノード、Pod、プロセスレベルまでGPUの使用状況を多角的に把握できます。

障害の早期検知と迅速な対応

温度上昇、電力制限、クロック低下、エラー発生、通信異常などの兆候を素早く特定し、障害に発展する前に対応できます。

GPU活用率の最適化

遊休GPU、偏った使用、過少活用リソースを確認し、再配置および運用の最適化が可能です。

運用効率の向上

サーバーとKubernetes環境を分離して管理するのではなく、統合的に管理することで運用の複雑さを軽減できます。

合理的な増設・投資判断の支援

実際の使用データをもとにGPU増設の必要性を検討し、予算・購入計画の根拠資料として活用できます。

Capacity Planning支援

短期的な障害対応だけでなく、中長期的なリソース需要予測と運用戦略の策定にまで連携できます。

GPUデバイス異常検知方法

GPUデバイスおよびワークロードで発生し得る異常の兆候を検知する方法です。

1. Xidベースの異常検知

NVIDIA GPUは、障害または異常状態が発生した際にXidイベントをログに記録します。そのため、システムログやドライバーログでXidキーワードおよびコードの発生有無を検知することで、GPUデバイスの異常を比較的迅速に特定できます。

例えば、特定のXidはGPU演算エラー、メモリアクセス問題、ドライバー/ハードウェア異常、リセット発生などの兆候を示す場合があるため、運用環境ではXidイベントを重要な障害シグナルとして活用できます。

2. 状態指標ベースの異常検知

GPU異常は、必ずしもエラーログだけに現れるとは限りません。実際の運用環境では、GPU使用率、メモリ使用量、温度、電力、クロック、PCIe/NVLink通信状態といった主要な状態指標の変化パターンを合わせてモニタリングすることで、異常の兆候をより早期に検知できます。

ただし、これらの指標は絶対値だけで判断するのではなく、業務特性、タスクの種類、時間帯別パターン、平常時のベースラインを合わせて考慮して解釈することが重要です。例えば、学習、推論、バッチ処理、データ前処理といったワークロードは、それぞれ正常動作時のGPU使用パターンが異なるため、同じ数値でも業務の文脈によって意味が変わる場合があります。

この観点から、以下のようなパターンの変化は主要な点検対象となります。

- 通常の業務パターンと比較してGPU使用率が過度に高い、あるいは逆に割り当てられたリソースが十分に活用されていない状態が続いている場合
- タスク終了後もメモリ占有が異常に維持されていたり、特定の時点からメモリ使用量が急激に増加している場合
- 温度が継続的に上昇して通常の運用水準を超えたり、長時間にわたって高温状態が維持されている場合
- 電力使用量が制限値付近に長時間とどまり、電力制限による性能制約が疑われる場合
- 負荷水準に対してクロックが期待値より低く維持され、スロットリングまたは異常な制御状態が疑われる場合
- PCIe/NVLink通信量が業務特性に比べて異常に増減したり、InfiniBandにエラー指標が同時に観測される場合

状態指標を個別の数値ではなく、業務の文脈における変化パターンとして解釈することで、単純な使用状況の把握を超えて、パフォーマンス低下、過熱、スロットリング、電力制限、通信ボトルネック、異常動作といった問題をより正確に特定できます。

3. プロセス/ワークロード観点の異常検知

GPUを占有しているプロセス、Pod、Containerなどのワークロード情報を合わせて確認することで、デバイス指標だけでは把握しにくい異常状況をより明確に解釈できます。ただし、これもまた単純な占有有無だけで判断するのではなく、業務の種類、実行段階、繰り返し周期、平常時の占有パターンを合わせて考慮する必要があります。

学習、推論、バッチ処理、データ前処理といったワークロードはGPUの使用方法がそれぞれ異なるため、同じ占有状態であっても、どのような業務かによって正常・異常の基準が変わる場合があります。

この観点から、以下のようなパターンは主要な点検対象となります。

- タスクの特性に比べて特定のプロセスやワークロードがGPUメモリを過度に占有したまま、予想より長い時間解放しない場合
- GPU使用率は低いのにメモリ占有のみが長時間維持され、タスクの停滞・異常待機・メモリリークの可能性が疑われる場合
- 特定のタスクが繰り返し再起動または失敗し、GPUリソースを非効率に占有している場合
- 一部のGPUにのみ特定のワークロードが継続的に集中し、使用の不均衡や局所的な過熱が発生している場合

- 同種の業務と比較して、特定のプロセスのみが過度に長い実行時間、高いメモリ占有、異常な占有パターンを示している場合
- PodまたはContainerの再配置後にGPU占有パターンが急激に変化し、スケジューリングの非効率やリソースの偏りが疑われる場合

これらのパターンは、単純なデバイス異常だけでなく、アプリケーションまたはワークロードの運用上の問題を合わせて特定するのに役立ちます。

GPUダッシュボード

GPUダッシュボードは、GPU資源構成、活用効率、問題履歴を1つの画面で統合的に照会するAIインフラ運用ダッシュボードです。GPUサーバーが複数台に増えると、個々のサーバーを1つずつ確認するのは困難です。GPUダッシュボードは、GPU資源全体をモデル別・サーバー別にまとめて表示し、活用状況と異常の兆候を素早く把握できるように支援します。

⚠ サポート環境

サーバー環境のGPUモニタリングの概要は、[WhaTap GPUモニタリングドキュメント](#)を参照してください。

基本画面の案内

GPUダッシュボードは2つのタブで構成されます。

- **GPU運用状況**：GPU資源の保有状況、活用効率、電力消費、問題をウィジェット単位でまとめて表示します。
- **GPUリソースボード**：全GPUの割り当て・活用状態をサマリーバーとマップ形式で俯瞰します。

オプションバー

画面上部のオプションバーで照会条件を調整できます。

- **時間選択**：照会する時間範囲を指定します。
- **フィルタ**：特定のモデル、サーバーなど条件に合うGPUのみ照会するようフィルタを指定します。
- **表示切り替え**：ウィジェットの表示形式を切り替えます。
- **プリセット(Preset)**：よく使うフィルタとTop 5指標選択の組み合わせをプリセットとして保存し、再度読み込むことができます。

GPU運用状況タブ

GPU運用状況タブは、次のウィジェットを提供します。

GPUインベントリ(モデル別)

保有しているGPUをモデル別に集計し、ドーナツ形式で表示します。ドーナツのモデル部分または凡例をクリックすると、該当モデルでフィルタが適用された[GPUインベントリ](#)が新しいタブで開きます。

GPU電力消費推移

GPUの電力消費推移を時間の流れに沿って表示します。

 表示される電力消費量は、GPU指標を基に算出した推定値であり、実際の電力計測定値と差がある場合があります。

GPUモデル別サーバー重大度分布

GPUモデル別に、該当モデルが搭載されたサーバーの進行中イベント状況と代表重大度分布を積み上げ棒グラフ形式で表示します。発生 x / 全体 y サーバーは、該当GPUモデルが搭載された全サーバーのうち、現在1つ以上のイベントが発生しているサーバー数を意味します。各サーバーの重大度は、該当サーバーで進行中のイベントのうち最も高い重大度を基準に分類し、危険・警告・情報・正常別のサーバー数で表示します。総イベント n件は、イベントが発生したサーバーで現在進行中の全イベント数を意味します。項目をクリックすると、該当GPUモデルが搭載されたサーバーを対象に進行中のイベント一覧をドロワーで確認できます。

Top 5 Server / Top 5 GPU

指定した指標を基準に、上位5つのサーバー(Top 5 Server)とGPU(Top 5 GPU)をそれぞれ別のパネルで表示します。デフォルトの基準指標は、サーバーがGPU使用率、GPUが電力制限違反率です。項目をクリックすると、該当対象の最近の推移を確認できるドロワーが開きます。基準指標はオプションバーまたはプリセットで変更できます。

Xid

GPUで発生したXidイベントの履歴を表示します。Xidイベントを活用した異常検知の方法は、[WhaTap GPUモニタリングドキュメント](#)を参照してください。

GPUリソースボードタブ

GPUリソースボードタブは、全GPUの割り当て・活用状態をサマリーバーとマップ形式で俯瞰します。個々のGPUがどれだけ割り当て・使用されているか、どのGPUがアイドル状態またはメモリ不足に近づいているかを一目で把握できます。

サマリーバー

全GPUの割り当て・活用状態をカード単位で要約します。各カードは物理GPU(Physical)とMIGインスタンス数を一緒に表示します。

| Item | Description |
|---------------|----------------------------|
| Total GPU | 全GPU数 |
| Allocated GPU | 割り当てられたGPU数と割り当て率 |
| Idle GPU | 割り当てられているが使用されていないアイドルGPU数 |
| Active GPU | 使用中のGPU数 |
| Effective GPU | 効率的に使用中のGPU数 |

サマリーバーのカード名称は英語(Total GPU、Allocated GPU、Idle GPU、Active GPU、Effective GPU)で表示されます。アイドル・アクティブ・効率の区分はGPU使用率を基準とし、使用率1%未満はアイドル(Idle)、1%以上50%未満はアクティブ(Active)、50%以上は効率(Effective)です。

GPU Resource Map

全GPUを使用率基準で配置した散布図(scatter)です。各GPUをアイドル(Idle)・アクティブ(Active)・効率(Effective)区間に分けて分布を表示し、メモリ使用率が高くメモリ不足に近づいたGPU(FB使用率95%以上)を区別して表示します。マップで特定の領域を選択すると、該当GPUの最近の推移を確認できるGPUタイムラインドロワー(drawer)が開きます。

GPUモデル別活用状況

GPUをモデル別に集計し、アイドル(Idle)・アクティブ(Active)・効率(Effective)・未割り当て(Unallocated)区間の割合を表示します。モデル別に割り当て・活用状態がどのように分布するかを比較できます。

サーバー別GPU活用状況

サーバー別に保有しているGPUをスロットグリッド形式で表示します。各スロットは物理GPU1つを表し、MIGで分割されたGPUはスロット内部をインスタンス単位で分けて表示します。

ⓘ サーバー別GPU活用状況は、GPUサーバーが20台以下の環境で自動的に表示されます。

GPUインベントリ

GPUインベントリでは、サーバーに搭載されたGPUの仕様や状態を体系的に管理できます。

⚠ サポートエージェントバージョン

Linuxでのみサポートされており、エージェントバージョン 2.9.3 以上が必要です。

基本画面ガイド

GPUインベントリは、システムに割り当てられたGPUおよびMIG（Multi-Instance GPU）リソースの全リストをモニタリングします。各GPUインスタンスの詳細情報を確認できます。

- 検索ボックスでキーワード検索が可能です。
- 表示結果の項目名をクリックすると、昇順または降順に並べ替えが可能です。

▽ キーワード検索フィルター

フィルター検索機能を活用すると、希望の条件に合った GPU インスタンスだけを素早く確認できます。

▽ 検索ボックスにフィルターを入力し、Enter を押して検索してください。

▣ カラム設定

画面右上の **列設定** ボタンをクリックすると、表示する列を選択できます。カラム設定ウィンドウでカラムの選択およびカスタムカラムの追加後、**確認** ボタンをクリックして設定を保存してください。表示項目からドラッグしてカラムの順序を変更できます。

• カラム選択

ユーザーはテーブルに表示するカラムを選択できます。**初期化** をクリックすると、デフォルトのカラム選択状態に戻ります。

- ① 選択した カラム はブラウザのクッキーに保存され、ページを更新しても状態が維持されます。クッキーが削除されたり、他の理由で設定エラーが発生した場合は、デフォルト項目の選択状態に初期化します。

• カラム追加

+ カラム追加 ボタンを選択し、基本項目以外に任意のカラムを追加してカスタムカラム（ custom ）を構成できます。必要に応じてカラムを追加し、サーバーの状態や性能をより詳細にモニタリングしてください。

CSVのダウンロードとアップロード

1.  CSVダウンロード ボタンをクリックして、現時点のGPUインベントリ情報をダウンロードします。
2. ダウンロードしたファイルを開いて、カラムの内容を修正します。
3.  CSVアップロード ボタンをクリックして、修正したファイルをアップロードすると、値が一括で更新されます。
 - 変更件数、エラー、未反映の件数を確認できます。
4. 適用 ボタンをクリックすると、GPUインベントリ一覧に反映されます。

① 反映されない項目

インベントリに存在しないカラムは反映されません。

- 新しいカラムを追加するには、インベントリ一覧の + カラム追加 ボタンを使用してください。GPUの追加・削除は反映されません。

修正

 修正 ボタンをクリックすると、GPUインベントリリストを編集できます。

- サーバー別名と基本グループのカラム内容を設定可能です。
- ユーザーが追加したカスタムカラム（ custom ）の内容も設定できます。

GPUパフォーマンスサマリー

システムに接続されたGPUの状態およびパフォーマンス指標をリアルタイムでモニタリング・管理できます。物理GPUとMIGインスタンスの情報を同時に確認でき、各項目を並び替えたりフィルターして効率的に使用できます。

ⓘ サポートエージェントバージョン

Linuxでのみサポートされており、エージェントバージョン 2.9.3 以上が必要です。

基本画面案内

Live をクリックすると、リアルタイムデータの表示・一時停止ができます。検索ボックスでGPU情報を検索できます。

データリスト内の項目名をクリックすると、昇順または降順に並べ替えることができます。

- **Total:** 全GPUインスタンス数（Physical + MIG含む）
- **Physical:** 実GPUデバイス数
- **MIG:** MIG（Multi-Instance GPU）インスタンス数

GPU情報

| カラム名 | 説明 |
|----------|---|
| Status | 該当GPUインスタンスの現在の状態 <ul style="list-style-type: none">- N/A: GPU 状態表示は Physical GPU のみ対象となり、GPU Type が MIG の場合は N/A と表示されます- Allocated: 既存の Active 状態と同一です- Unallocated: 既存の Inactive 状態と同一です- Active: Allocated 状態で、5 分平均の GPU Utilization が 1% 以上の場合- Idle: Allocated 状態で、5 分平均の GPU Utilization が 1% 未満の場合- Effective: Allocated 状態で、5 分平均の GPU Utilization が 50% を超える場合 |
| HostName | GPUが接続されているサーバーのホスト名 |

| カラム名 | 説明 |
|------------|---|
| GPU Index | 物理GPUまたはMIGインスタンスの固有インデックス（MIGインスタンスは 0/6/0 などの形式で表示） |
| Model Name | GPUモデル名（例：NVIDIA A100-SXM4など） |
| GPU Type | Physical または MIG のうち、該当インスタンスの種類 |

GPUパフォーマンス指標

各メトリクスの詳細説明は[GPUメトリクス](#)を参照してください。

↓ CSVダウンロード

検索結果をCSVファイルとしてダウンロードできます。

☐ カラム設定

画面右上の ☐ カラム設定 ボタンをクリックすると、**カラム設定** ウィンドウが開きます。
このウィンドウで、テーブルに表示するカラムを選択できます。

- ✓ **全選択**: すべてのカラムを選択
- ↺ **デフォルト順にリセット**: カラム順を初期状態に戻す
- ↺ **デフォルト選択にリセット**: 選択状態を初期設定に戻す

❗ 選択したカラムはブラウザのクッキーに保存され、ページを更新しても保持されます。
クッキーが削除された場合や設定エラーが発生した場合は、初期状態にリセットされます。

1. **カラム設定** ウィンドウで、**GPU情報** および **GPUパフォーマンス指標** の表示カラムを選択してください。
 - カラムはグループ単位で選択したり、表示順を調整することができます。

❗ GPU情報のうち、Status と HostName は削除できません。

2. **適用** ボタンをクリックして、設定を保存してください。

フィルターを追加する

フィルター条件を追加することで、目的のGPUを素早く見つけることができます。

1. **▽ フィルター** 検索バーをクリックすると、**フィルターを追加** ウィンドウが表示されます。
2. **フィルターを追加** で、GPU条件（フィルターキーと条件）を選択し、**適用** ボタンをクリックします。

GPUを比較する

複数のGPUを選択すると、GPUリストの下にある **比較** パネルで、チャートによる視覚的な比較が可能になります。直近10分間のデータトレンドを追跡し、パフォーマンスの異常やボトルネックを特定できます。

- 比較できる項目は最大20個までです。

GPU詳細

GPU詳細ページでは、特定サーバーのGPU使用状況を時系列チャートでモニタリングし、GPUを占有しているプロセスをリアルタイムで確認できます。物理GPU（Physical）とMIG（Multi-Instance GPU）インスタンスの情報を1つの画面でまとめて確認でき、どのワークロードがどのGPUリソースをどの程度使用しているかを素早く把握できます。

⚠ 対応エージェントバージョン

Linuxのみ対応しており、エージェント 2.9.16 以上を推奨します。

メイン画面

画面上部のオプションバーで照会時間範囲とサーバーを選択できます。選択したサーバーのインライン情報（IP、OS Type、CPU Cores、Memory Total、OS Version）と機能有効化ガイドボタンが表示されます。オプションバー下部でGPUを選択し、画面に表示する対象をフィルタリングできます。

各項目の使用方法は次のとおりです。

- **時間範囲:** 照会する時間区間を選択します。左右の矢印ボタンで区間を移動できます。
- **サーバー選択:** モニタリングするサーバーをドロップダウンから選択します。ホスト名とIPが一緒に表示されます。
- **GPU選択:** 画面に表示するGPUをフィルタリングします。選択ボックスをクリックするとGPU選択モーダルが開きます。デフォルトは *** (Select All)** で、サーバーに接続されているすべての物理GPUとMIGインスタンスが選択されます。
- **機能有効化ガイド:** クリックするとGPUモニタリングの対応環境と収集可能なメトリクス一覧を案内するパネルが開きます。

GPUインデックスは、チャートの凡例とプロセステーブル全体で次の形式で表記されます。

- **物理GPU:** 0、1、4 などの整数
- **MIGインスタンス:** 7/1/0、6/4/0、5/8/0 などのスラッシュ表記（Physical/GI/CI）

GPUメトリクスチャート

画面左側に選択したサーバーのGPU使用状況が5つの時系列チャートカードで表示されます。ラインチャート2つ（物理GPU + MIGインスタンス両方）とスタック/ライン切り替えチャート3つ（物理GPUのみ）で構成されます。

各カード右上のトグルボタンでラインモードに切り替えられます。

| チャート | タイプ | 説明 |
|---------------------|----------|-------------------|
| GPU Utilization (%) | ライン | GPUコア使用率 |
| FB Memory Used (%) | ライン | GPUフレームバッファメモリ使用率 |
| Power Usage | スタック/ライン | GPU消費電力 |
| PCIe TX+RX | スタック/ライン | PCIe送受信帯域幅 |
| NVLink TX+RX | スタック/ライン | NVLink送受信帯域幅 |

各チャートカード右上のアイコンからデータをCSVファイルとしてダウンロードしたり、チャートを画像として保存したりできます。拡大アイコンをクリックすると、そのメトリクスカテゴリの**チャート詳細ドロワー**が開きます。

ⓘ 各メトリクスの詳細な定義については、[GPUメトリクスドキュメント](#)を参照してください。

チャート詳細（ドロワー）

各チャートカード右上の拡大アイコンをクリックすると、そのメトリクスカテゴリの詳細指標をまとめて確認できるドロワーが右側から開きます。ドロワー内では、時間範囲とGPU選択をメイン画面とは独立して変更できます。

ドロワー下部の**解釈ガイド**セクションでは、各メトリクスの意味とモニタリングポイントを確認できます。

| ドローワー | 含まれるメトリクス |
|-------------------|--|
| GPU Utilization詳細 | GPUコア活用率、SM Active/Occupancy、FP・Tensor・DRAM活性度 など |
| GPU Memory詳細 | FB Total/Used/Free/Reserved、FB Used (%）、メモリコピー活用度 など |
| 電力/温度詳細 | Power Limit/Usage、電力違反率、GPU温度、温度違反率 など |
| PCIeトラフィック詳細 | PCIe TX+RX、PCIe TX、PCIe RX、NVLink TX+RX など |
| NVLinkトラフィック詳細 | NVLink TX+RX、NVLink TX、NVLink RX、PCIe TX+RX など |

GPUプロセステーブル

画面右上のGPUプロセステーブルには、選択したサーバーでGPUを占有しているプロセスの一覧が表示されます。各プロセスのGPU・CPU・メモリ使用状況を一目で確認でき、テーブル右上の検索ボックスでプロセス名によるフィルタリングができます。

各メトリクスセルには、照会期間中の時系列ミニチャートと最大値（Max）が表示されます。

| カラム | 説明 |
|---------------------|--|
| プロセス情報 | プロセス名、実行コマンド、PID xxxx・アカウント の3行 |
| GPU Utilization (%) | プロセスがバインドされているGPUデバイス全体のGPU Utilization。プロセスごとに直接測定した値ではなく、接続されているGPU全体の使用率を表示するため、同一GPUを使用する複数のプロセスに同一または類似した値が表示される場合があります。ミニチャート + Max N% |
| FB Used (MiB) | プロセスが占有しているGPUフレームバッファメモリのサイズ。ミニチャート + Max N MiB |
| CPU (%) | プロセスのCPU使用率。ミニチャート + Max N% |
| RSS (byte) | プロセスのホストシステムメモリ使用量（Resident Set Size）。ミニチャート + Max N GiB |

| カラム | 説明 |
|----------------------------------|--|
| Process IO
Total
(bytes/s) | プロセスのI/O帯域幅。ミニチャート + Max N KiB/s。収集データがない場合は - と表示 |
| GPU Index | プロセスが占有しているGPUインデックス。Physicalは整数（0、1）、MIGはスラッシュ表記（5/8/0） |

❗ VLLM::Worker_TP0、VLLM::EngineCore、python3 app.pyなどは、ユーザー環境で実際に実行中のプロセス名です。テーブルにはGPUを占有しているすべてのプロセスが表示されます。

サーバー情報・GPUインベントリパネル

画面右下のパネルでサーバー情報またはGPUインベントリタブを選択すると、現在照会中のサーバーの詳細情報を確認できます。GPUプロセステーブルとこのパネルの間のドラッグハンドルで上下の比率を調整できます。

サーバー情報

| 項目 | 説明 |
|-----------------|---|
| Host name (oid) | ホスト名とOID |
| OS | オペレーティングシステムの種類とバージョン |
| GPU model | GPUモデル名（例: A100-40GB） |
| GPU count | サーバーに接続されているGPU数（Physical N / MIG M 形式） |
| Server memory | サーバー全体のメモリ |
| Agent | インストールされているエージェントバージョン |

GPUインベントリ

サーバーに接続されている物理GPUとMIGインスタンスの一覧を次のカラムで確認できます。タブ右側の詳細表示ボタンをクリックすると、すべてのカラムを表示するドロワーが開きます。

ⓘ 現時点のインベントリのみ照会できます。過去の時点の照会はGPUインベントリメニューから行えます。

| カラム | 説明 |
|-----------------------|--|
| GPU Index | Physicalは整数（0、1）、MIGはスラッシュ表記（5/7/0、5/8/0） |
| GPU Type | Physical または MIG |
| Model Name | 正式なGPUモデル名（例: NVIDIA A100-SXM4-40GB） |
| Model Family | GPUモデルファミリー（例: A100） |
| GPU Memory Size (MiB) | GPUメモリサイズ。Physicalは全メモリ、MIGは分割されたフラグメントサイズ |

インベントリメニュー自体と活用方法については、[GPUインベントリ](#)ページを参照してください。

キューブ

WhaTapモニタリングサービスの初期画面でプロジェクトを選択した後、**分析**>**キューブ**を選択します。

キューブとは？

WhaTapは5分単位で作成されたパフォーマンス統計を**キューブ**と呼びます。キューブ分析は、キューブに保存された5分単位のパフォーマンスデータを利用する分析機能です。



1 キューブのセレクトパネル

左側のキューブセレクトパネルで、特定の時間を基準にキューブを選択します。キューブは5分単位で保存されるため、任意の時間を選択する必要があります。

- パネル関心メトリクス

サーバーキューブセレクトパネルで関心のあるメトリクスは、**CPU**と**メモリ**です。

- キューブ表示色

キューブは、選択された関心指標の数値に応じて異なる色で表示されます。

- 紺色：高い数値
- 水色：低い数値

2 アプリケーションセクター

上部②領域のアプリケーションセクターオプションを使用して、特定のアプリケーションのデータを選択することができます。右側の▽ボタンをクリックすると、次のように選択可能なアプリケーション全体を確認できます。

The screenshot shows the 'Application Selector' interface. At the top left, there are two checkboxes: 'すべて選択' (Select All) which is checked, and '選択のみ表示' (Show Selected Only) which is unchecked. To the right is a search bar with the placeholder text '検索' (Search) and a magnifying glass icon. Further right, it displays '16 / 16' with a chevron icon. Below these elements is a grid of application names, each enclosed in a light blue rounded rectangle. The applications are arranged in three rows: Row 1: demo-k8s-master, demo-k8s-worker-01, demo-k8s-worker-02, demo-k8s-worker-03, demo-k8s-worker-04, dotnet-official-demo, go-official-demo. Row 2: mysql-official-demo-01, mysql-official-demo-02, mysql-official-demo-03, node-official-demo, python-demo-attack, python-demo-target. Row 3: rum-official-demo, url-official-demo, virtual-java-agent.

- **すべて選択**：すべてのアプリケーションを表示します。既定値は**すべて選択**と**活性アプリケーション**が選択されています。
- **選択のみ表示**：アプリケーションからユーザーが指定したアプリケーションのみを表示します。
- **検索**：アプリケーションが多数の場合は、入力ウィンドウからそのアプリケーションを検索できます。
- **数字/数字**：指定されたアプリケーション数/全体のアプリケーション数を表示します。

3 キューブデータ

- ① • チャート右上の  アイコンを選択すると、バーチャートが表示します。
- チャート右上の  アイコンを選択すると、線形チャートを提供します。

3 領域で該当するキューブデータをCPU、メモリ、ディスク、ネットワークなどのチャートから確認できます。

- CPU

プロジェクト内のアプリケーションをCPU使用量が多い順にソートして表示します。

- メモリ

プロジェクト内のアプリケーションをメモリ使用量が多い順にソートして表示します。

- ディスク

プロジェクト内のアプリケーションをディスク使用量が多い順にソートして表示します。

- ネットワーク

プロジェクト内のアプリケーションをネットワークの入出力トラフィック量が多い順にソートして表示します。

- ① WhaTap uses the IP2Location LITE database for [IP geolocation](#).

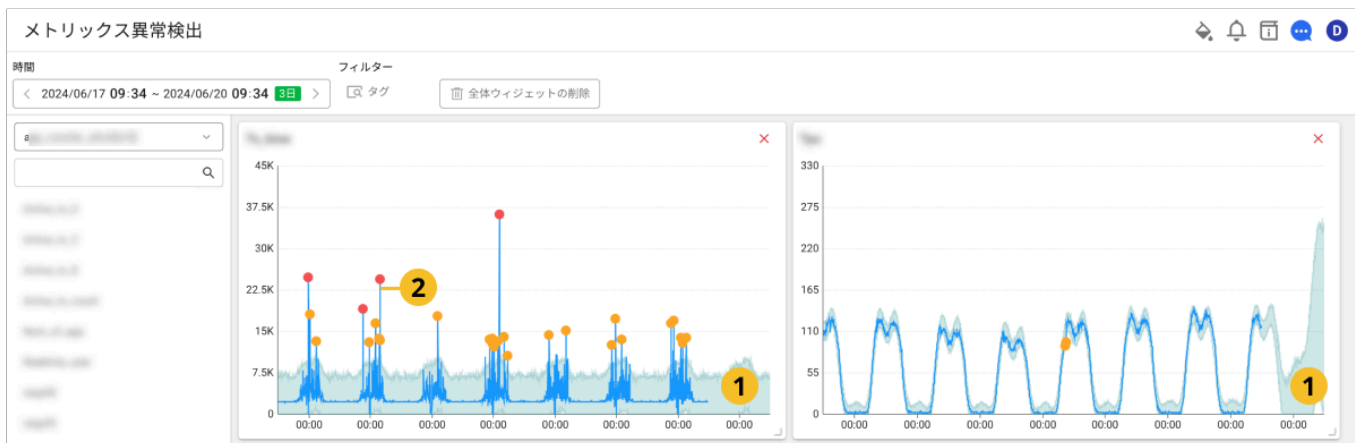
メトリクス異常検出

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。

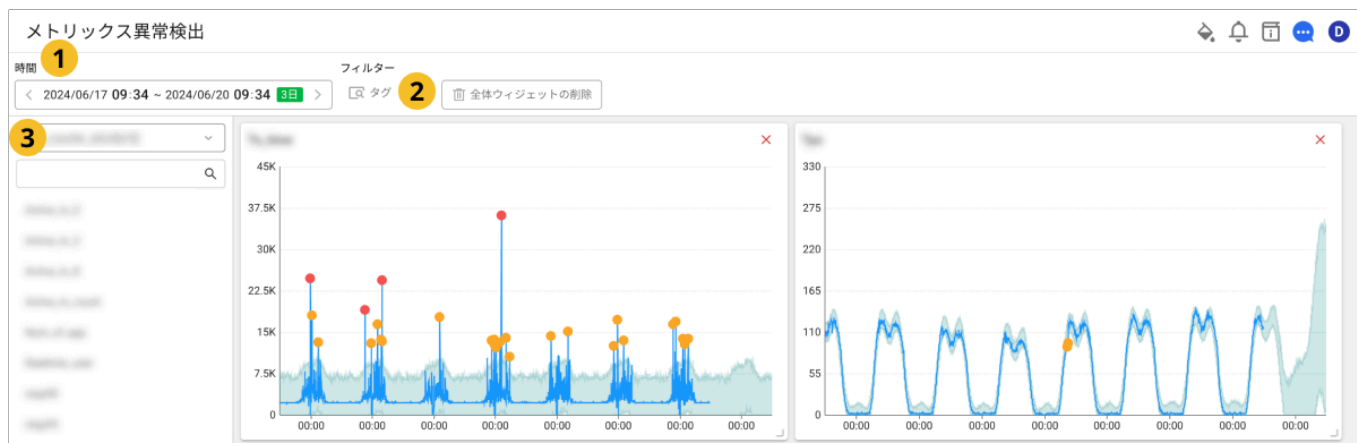
- ❗ 画面に配置したウィジェットは、別のメニューに移動すると保存されずに初期化されます。
- パターン分析と異常値検出機能を除くと分析 > メトリクスチャートメニューに似ています。
- 異常値(Anomaly Detection)アラート通知機能の技術的根拠は、メトリクス異常値です。異常値アラート通知設定の詳細については、[次の文書](#)を参照してください。

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。

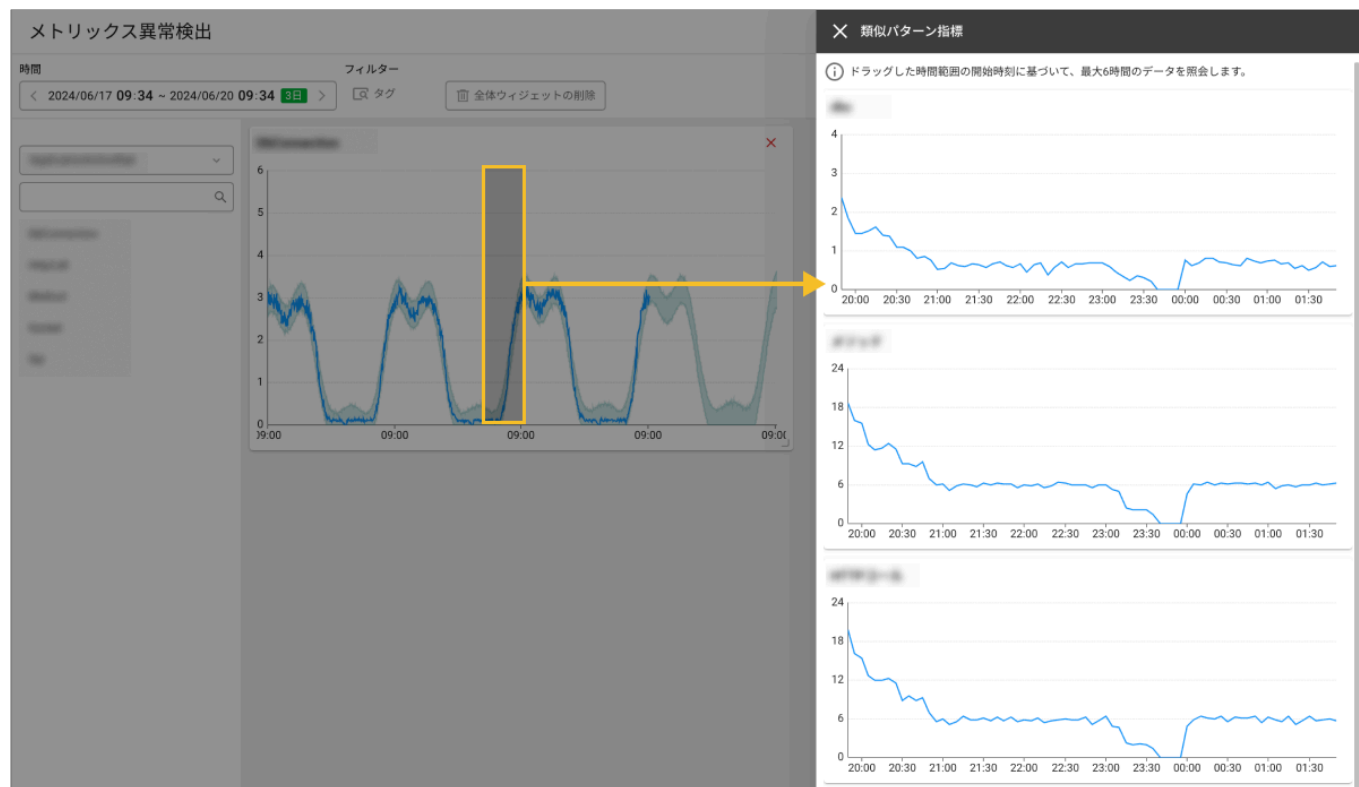
選択したメトリクスを画面の右側に配置します。

- 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

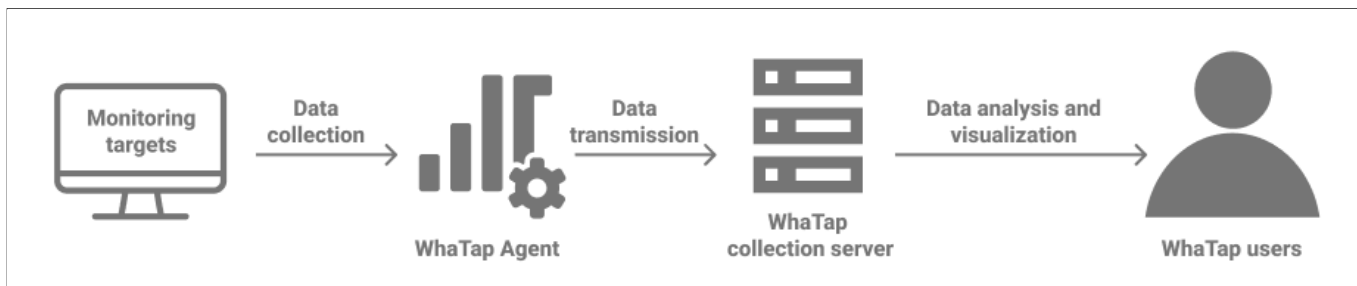
メトリクスとは？

メトリクスはモニタリング対象の状態を数値で表現した時系列データです。WhaTapエージェントがモニタリング対象から収集した性能データを加工した結果です。

メトリクスを通じてサーバー別メモリ使用率、DB接続時間などの主要な性能指標を一目で把握できます。問題を発見した後はログとトレースを通じて詳細分析ができます。

リソース使用量の統計を基に必要なリソース量を算定でき、コスト効率化にも活用できます。

WhaTapのメトリクス収集方式



メトリクスを収集するにはモニタリング対象にWhaTapエージェントをインストールする必要があります。エージェントが送信したメトリクスはWhaTap収集サーバーに保存されます。

例えばServerをモニタリングするにはまず[エージェントをインストール](#)してください。収集可能なメトリクスは[サーバーメトリクス](#)で確認できます。

WhaTapのメトリクス構成要素

WhaTapのメトリクスは以下の要素で構成されています。

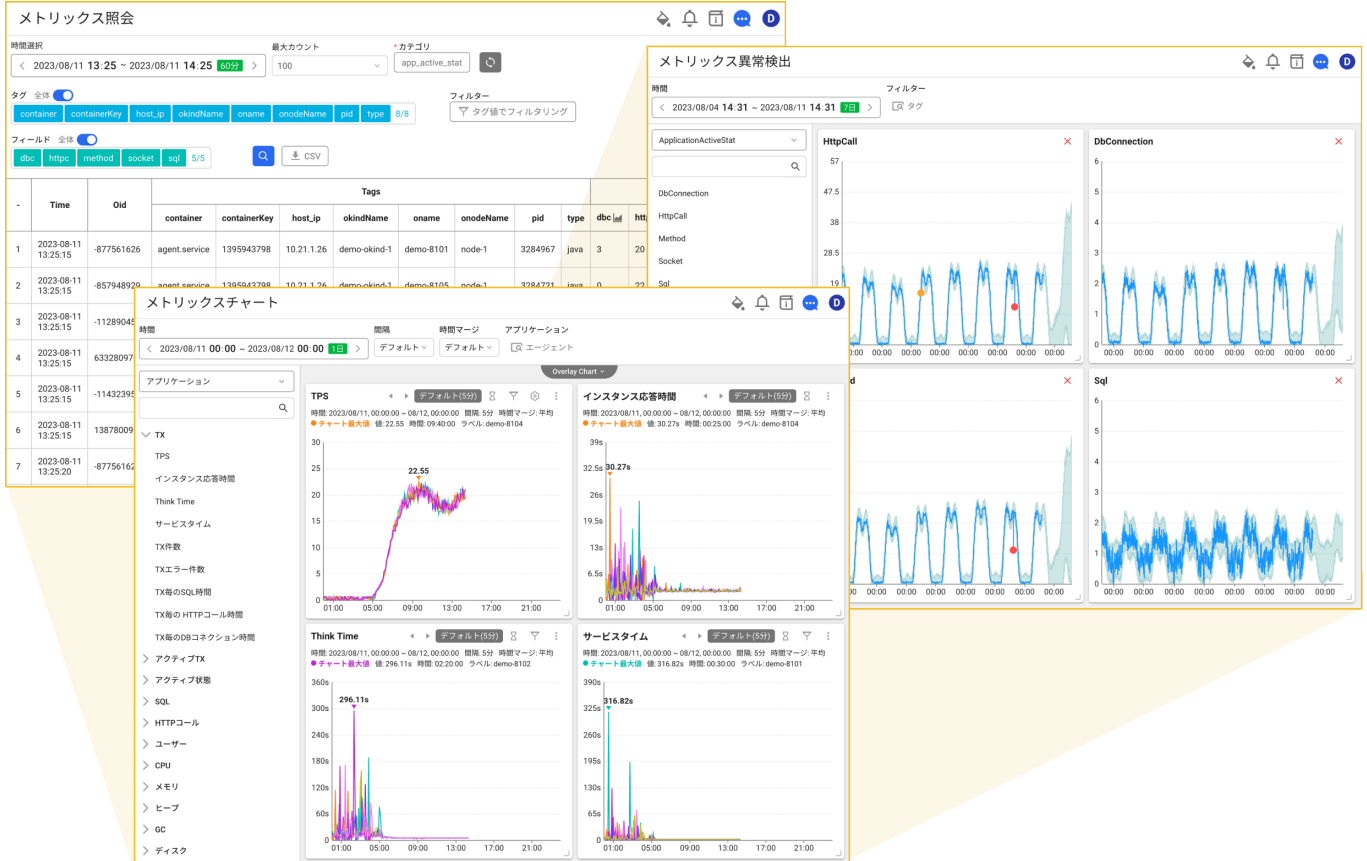
- **Category:** 関連メトリクスを1つのグループにまとめる名前です。

- **Tags:** 収集対象を識別するラベルです。IP、Oname、Hostなど変更の少ない固有情報を保存します。1つのメトリクスに複数のタグが含まれることがあります。
- **Fields:** 実際の測定値を保存します。1つのメトリクスに複数のフィールドが含まれることがあります。
- **Time:** メトリクスを収集した時間です。
- **Oid:** メトリクスを収集したエージェントの固有番号です。
- **Oname:** メトリクスを収集したエージェントの名前です。

メトリクスデータの照会と可視化

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。

- **メトリクス照会:** メトリクスの原本データを照会します。
- **メトリクスチャート:** 可視化したチャートを通じてメトリクスデータを照会します。
- **メトリクス異常検出:** AIが学習したメトリクスパターンと比較して予想パターンを外れた異常を探知します。



サーバーメトリクス

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検索できるメトリクスです。メトリクスは以下の情報を含みます。一部のメトリクスにはタグ情報がない場合があります。

- **Tags:** 収集対象を識別する情報（エージェント名、IPなど）
- **Fields:** 実際の測定値（CPU使用率、応答時間など）

ⓘ CategoryV2メトリクスはサーバーメトリクスV2で案内します。

Category V1

agent_status_summary

- エージェント状態関連メトリクスを収集
- 収集間隔: 10秒

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 | - | - | 現在のエージェントの活性状態有無(true / false) |
| isRebooted | - | - | サーバーが最近再起動したかどうか(true / false) |
| 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 (0 : 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 |

| Field | Type | Unit | Description |
|-----------|------|---------|-------------------------|
| 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 |
| status | - | - | 現在のエージェントの状態 |
| uptime | - | 秒(sec) | サーバーが稼働している時間 |

- ❗ status フィールドの値は、次のように区切ります。
- ok : サーバーが有効になっている正常な状態です。
 - inactive : サーバーが無効になっている状態です。
 - warning : サーバーに警告(warning) イベントが進行中の状態です。
 - fatal : サーバーに危険(critical) イベントが進行中の状態です。
 - paused : エージェントがデータの収集を一時停止した状態です。

server_base

- サーバーリソースメトリクスを収集
- 収集間隔: 5秒
- 統計データ: 5分、1時間

Tags

| Tag | Description | Remarks |
|-----------|-------------|---------|
| cpu_cores | サーバーコア数 | - |
| host_ip | サーバーIP | - |
| oname | サーバー名 | - |
| okindName | サーバー種類名 | - |

| Tag | Description | Remarks |
|-----|----------------------|---------|
| os | OSタイプ linuxまたはwindow | - |

Fields

| Field | Unit | Description | Remarks |
|----------------------|-------|-----------------------|---------|
| cpu | パーセント | CPU全体使用率 | 共通 |
| cpu_c1 | パーセント | cpu c1 state 使用率 | window |
| cpu_c2 | パーセント | cpu c2 state 使用率 | window |
| cpu_c3 | パーセント | cpu c3 state 使用率 | window |
| cpu_ctxt | 少数 | context switching 使用率 | linux |
| cpu_dpc | パーセント | CPU DPC 時間比率 | window |
| cpu_idle | パーセント | CPU idle 比率 | 共通 |
| cpu_interrupt | パーセント | cpu interrupt | linux |
| cpu_iowait | パーセント | CPU iowait 比率 | linux |
| cpu_irq | パーセント | CPU IRQ 使用率 | linux |
| cpu_load1 | 少数 | 1分平均Load Average | linux |
| cpu_load5 | 少数 | 5分平均Load Average | linux |
| cpu_load15 | 少数 | 15分平均Load Average | linux |
| cpu_new_procs_forked | 整数 | os process fork呼び出し | linux |
| cpu_procs_blocked | 整数 | プロセス blocked ステータス個数 | linux |

| Field | Unit | Description | Remarks |
|---------------------|-------|--------------------------|---------|
| cpu_procs_running | 整数 | プロセス Running ステータス個数 | linux |
| cpu_softirq | パーセント | CPU softirq 使用率 | linux |
| cpu_steal | パーセント | CPU steal 使用率 | linux |
| cpu_sys | パーセント | CPU system 使用率 | 共通 |
| cpu_usr | パーセント | CPU user 使用率 | 共通 |
| epochtime | 整数 | メトリクスが収集された時間のepoch time | 共通 |
| memory_available | バイト | メモリ available サイズ | 共通 |
| memory_buffers | バイト | メモリ buffers サイズ | linux |
| memory_cached | バイト | メモリ cached サイズ | 共通 |
| memory_free | バイト | メモリ free サイズ | 共通 |
| memory_pageFaults | 整数 | メモリ page fault 回数 | 共通 |
| memory_pavailble | パーセント | メモリ available 使用率 | 共通 |
| memory_pused | パーセント | メモリ使用率 | 共通 |
| memory_shared | バイト | メモリ shared サイズ | linux |
| memory_slab | バイト | メモリ slab サイズ | linux |
| memory_sreclaimable | バイト | メモリ slab reclaimable サイズ | linux |
| memory_sunreclaim | バイト | メモリ slab cclaimable サイズ | linux |
| memory_swappused | パーセント | スワップ使用率 | 共通 |

| Field | Unit | Description | Remarks |
|----------------------|------|--------------------------|---------|
| memory_swaptotal | バイト | スワップの全体サイズ | 共通 |
| memory_swapused | バイト | スワップ使用量 | 共通 |
| memory_total | バイト | メモリの全体サイズ | 共通 |
| memory_used | バイト | メモリ使用量 | 共通 |
| processorQueueLength | 整数 | プロセッサキューの長さ | window |
| uptime | 整数 | 起動後サーバーの稼働時間 (TimeStamp) | 共通 |

server_cpu_core

- サーバーCPUコア別メトリクスを収集
- 収集間隔: 5秒
- 統計データ: -

Tags

| Tag | Description | Remarks |
|-------|----------------------|---------|
| cpu | サーバーコア番号 | - |
| IP | サーバーIP | - |
| oname | サーバー名 | - |
| os | OSタイプ linuxまたはwindow | - |

Fields

| Field | Unit | Description | Remarks |
|----------------------|-------|----------------------|---------|
| idle | パーセント | コアidle比率 | 共通 |
| iowait | パーセント | コアiowait比率 | window |
| irq | パーセント | コアirq使用率 | linux |
| load1 | 少数 | コア1分平均 Load Average | linux |
| load5 | 少数 | コア5分平均 Load Average | linux |
| load15 | 少数 | コア15分平均 Load Average | linux |
| nice | パーセント | コアnice使用率 | 共通 |
| processorQueueLength | 整数 | コアプロセスキューの長さ | window |
| softirq | パーセント | コアsoftirq使用率 | linux |
| steal | パーセント | コアsteal使用率 | linux |
| sys | パーセント | コアsys使用率 | linux |
| usr | パーセント | コアusr使用率 | linux |

server_disk

- ファイルシステム別ディスクメトリクスを収集
- 収集間隔: 5秒
- 統計データ: 5分、1時間

Tags

| Tag | Description | Remarks |
|----------------|----------------------|---------|
| deviceId | デバイスID | - |
| deviceIdHash | デバイスIDハッシュ値 | - |
| fileSystem | ファイルシステムタイプ | - |
| mountPoint | ファイルシステムのマウントポイント | - |
| mountPointHash | ファイルシステムマウントポイントハッシュ | - |
| oname | サーバー名 | - |
| os | OSタイプ linuxまたはwindow | - |

Fields

| Field | Unit | Description | Remarks |
|-------------|-----------|--|---------|
| blksize | バイト | ブロックサイズ | linux |
| count | 整数 | WhaTap専用 | 共通 |
| freePercent | パーセン
ト | ファイルシステム残存率 | linux |
| freeSpace | バイト | ファイルシステム残存量 | linux |
| ioPercent | パーセン
ト | IO使用率 「一部のディスクタイプでは不正確な値が測定されることがあります」 | linux |
| ioutilOrder | 整数 | WhaTap専用 | linux |

| Field | Unit | Description | Remarks |
|------------------|-------|---------------|---------|
| queueLength | 実数 | Queue Length | 共通 |
| totalInode | 整数 | Inode全体個数 | linux |
| totalSpace | バイト | ファイルシステム全体サイズ | linux |
| usedPercent | パーセント | ファイルシステム使用率 | linux |
| usedInode | 整数 | Inode使用個数 | linux |
| usedInodePercent | パーセント | Inode使用率 | linux |
| userSpaceOrder | 整数 | WhaTap専用 | 共通 |
| readBps | バイト | 毎秒読み込みバイト数 | 共通 |
| writeBps | バイト | 毎秒書き込みバイト数 | 共通 |
| readIops | 少数 | 毎秒読み込み数 | 共通 |
| writeIops | 少数 | 毎秒書き込み数 | 共通 |

server_network

- ネットワークインターフェースメトリクスを収集
- 収集間隔: 5秒
- 統計データ: 5分、1時間

Tags

| Tag | Description | Remarks |
|----------|----------------------|---------|
| desc | ネットワークインターフェース名 | - |
| descHash | ネットワークインターフェースハッシュ値 | - |
| hwAddr | MACアドレス | - |
| IP | インターフェースIPアドレス | - |
| oname | サーバー名 | - |
| os | OSタイプ linuxまたはwindow | - |

Fields

| Field | Unit | Description | Remarks |
|----------------|------|-------------|---------|
| bandwidthOrder | 整数 | WhaTap専用 | - |
| count | 整数 | WhaTap専用 | 共通 |
| droppedIn | 整数 | インバウンドドロップ | - |
| droppedOut | 整数 | アウトバウンドドロップ | - |
| errorIn | 整数 | インバウンドエラー | - |
| errorOut | 整数 | アウトバウンドエラー | - |
| packetIn | pps | インバウンドパケット | - |
| packetOut | pps | アウトバウンドパケット | - |

| Field | Unit | Description | Remarks |
|----------------|------|---------------|---------|
| trafficIn | bps | インバウンドトラフィック | - |
| trafficInAcct | 整数 | WhaTap専用 | - |
| trafficOut | bps | アウトバウンドトラフィック | - |
| trafficOutAcct | 整数 | WhaTap専用 | - |

server_netstat

- ネットワークプロトコル統計情報を収集
- 収集間隔: 5秒
- 統計データ: 5分、1時間

Tags

| Tag | Description | Remarks |
|-----------------------------|--------------|---------|
| oname | サーバー名 | - |
| os_arch | OSアーキテクチャ名 | - |
| os_cpucore | サーバーCPUコア数 | - |
| os_cpusocket | サーバーCPUソケット数 | - |
| os_cpuvendor | サーバーCPUベンダー名 | - |
| os_ip | サーバーIP | - |
| os_memory | サーバーメモリサイズ | - |
| os_nameOSタイプ linuxまたはwindow | - | |

| Tag | Description | Remarks |
|----------------|----------------------|---------|
| os_public_ip | サーバーパブリックIP | - |
| os_release | サーバーOSリリース名 | - |
| whatap_build | WhaTapエージェントビルドハッシュ値 | - |
| whatap_home | WhaTapエージェントホームパス | - |
| whatap_product | WhaTap製品タイプ | - |
| whatap_version | WhaTapエージェントバージョン | - |

Fields

| Field | Unit | Description | Remarks |
|---------------------|------|------------------------|---------|
| netstat_Close_Wait | 整数 | CLOSE_WAITステータスソケット数 | 共通 |
| netstat_Closing | 整数 | CLOSINGステータスのソケット数 | 共通 |
| netstat_Established | 整数 | Establishedステータスのソケット数 | 共通 |
| netstat_Fin_Wait1 | 整数 | FIN_WAIT1ステータスのソケット数 | 共通 |
| netstat_Fin_Wait2 | 整数 | FIN_WAIT2ステータスのソケット数 | 共通 |
| netstat_Last_Ack | 整数 | LASK_ASKステータスソケット数 | 共通 |
| netstat_Listen | 整数 | LISTENステータスソケット数 | 共通 |
| netstat_Syn_Recv | 整数 | SYN_RECVステータスソケット数 | 共通 |
| netstat_Syn_Sent | 整数 | SYN_SENTステータスソケット数 | 共通 |
| netstat_Time_Wait | 整数 | TIME_WAITステータスソケット数 | 共通 |

| Field | Unit | Description | Remarks |
|------------------------|------|----------------------|---------|
| netstat_Unknown | 整数 | Unknownステータスソケット数 | 共通 |
| Server_Filedescriptors | 整数 | OS file descriptor個数 | 共通 |

server_process

- サーバプロセス情報を収集
- 収集間隔: 20秒
- 統計データ: 5分

Tags

| Tag | Description | Remarks |
|-------|---------------------|---------|
| alias | サーバー別名 | - |
| cmd1 | プロセス実行コマンド1 | - |
| cmd2 | プロセス実行パラメータ | - |
| hash | プロセスハッシュ値 | - |
| name | プロセス名 | - |
| oname | サーバー名 | - |
| ユーザー | プロセスを実行したLinuxユーザー名 | - |

Fields

| Field | Unit | Description | Remarks |
|-------|------|-------------|---------|
| count | 整数 | プロセス個数 | 共通 |

| Field | Unit | Description | Remarks |
|---------------------|-------|------------------------|---------|
| cpu | パーセント | CPU使用率 | 共通 |
| cpuAccumulated | パーセント | WhaTap専用 | 共通 |
| cpuOrder | 順序 | WhaTap専用 | 共通 |
| memOrder | 順序 | WhaTap専用 | 共通 |
| memory | パーセント | メモリ使用率 | 共通 |
| memoryAccumulated | パーセント | WhaTap専用 | 共通 |
| openFileDescriptors | 整数 | open file descriptor個数 | 共通 |
| rbps | バイト | ディスク毎秒読み込みバイト数 | 共通 |
| rbpsAccmulated | バイト | WhaTap専用 | 共通 |
| riops | 整数 | ディスク毎秒読み込み数 | 共通 |
| riopsAccmulated | 整数 | WhaTap専用 | 共通 |
| wbps | バイト | ディスク毎秒書き込みバイト数 | 共通 |
| wbpsAccmulated | バイト | WhaTap専用 | 共通 |
| wiops | 整数 | ディスク毎秒の書き込み数 | 共通 |
| wiopsAccmulated | 整数 | WhaTap専用 | 共通 |
| rss | バイト | メモリRSSサイズ | 共通 |
| rssAccmulated | バイト | WhaTap専用 | 共通 |

参考資料

- [ウィンドウインデックスデータ](#)
- [linuxメトリクス資料](#)

サーバーメトリクス V2

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検索できるメトリクスです。メトリクスは以下の情報を含みます。一部のメトリクスにはタグ情報がない場合があります。

- **Tags:** 収集対象を識別する情報（エージェント名、IPなど）
- **Fields:** 実際の測定値（CPU使用率、応答時間など）

WhaTap サーバーモニタリングの CategoryV2 メトリクスは、運用環境のサーバーリソースをドメイン単位で標準化したメトリクス体系です。CPU、メモリ、Swap、カーネルのようなコアシステムリソースから、ディスクデバイス I/O、ファイルシステム、ネットワークトラフィック、NIC 構成、NTP 同期、プロセス、Windows サービス、InfiniBand、ZFS、Veritas LV などの主要なインフラ指標を、Linux、Windows、Unix（HP-UX、AIX、Solaris）ベースのオンプレミスおよびクラウドサーバー環境全般にわたって一貫した構造で提供します。

CategoryV2 は、サーバー全体のリソース使用状況を比較するカテゴリと、サーバーごとの構成要素を詳細なインスタンス単位で分析するカテゴリをあわせて提供します。運用者はこれを通じて、インフラ全体のリソース分布や異常の兆候を素早く把握し、問題が発生したサーバーの詳細な構成要素まで段階的に追跡できます。

従来の CategoryV1 が複数のドメインの指標を一部のカテゴリにまとめて提供していたのに対し、CategoryV2 はドメインごとのカテゴリ分離と、指標特性に応じた収集周期の差別化によって、分析構造と収集効率を改善しました。収集した CategoryV2 メトリクスはメトリクスエクスプローラーと連携するため、ユーザーは必要な指標を直接照会し、さまざまな条件で詳細に分析できます。

ⓘ CategoryV2 は、エージェント設定で `categoryv2.enabled=true` オプションを有効にすると使用できます。

CategoryV2メトリクス詳細

infra_cpu

サーバー全体の CPU リソースの使用状態を収集するカテゴリです。ユーザーモード、カーネルモード、I/O 待機、idle、interrupt、steal、load average など、CPU 全般の使用率と負荷レベルを確認するための指標を提供します。サ

サーバーの全般的な CPU ボトルネックの有無やシステム負荷状態を把握するときに使用します。

- カテゴリ: CPU
- デフォルト収集周期: 2秒

| Field | Title | Unit | Description | OS |
|-------|----------|------|--|---|
| cpu | CPU | % | 100%からアイドル(idle)率を除いた全体のCPU使用率を意味します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| user | User | % | 全CPU時間の中でユーザーモードで一般的なアプリケーション/プロセスを実行するために使用された割合を意味します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| sys | Sys | % | 全CPU時間のうち、カーネルモード (System mode) でのシステムコール処理、カーネル作業、ドライバ処理などに使用された割合を意味します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| nice | Nice | % | 全体のCPU時間の中で、低優先度(niced)のユーザープロセスの実行に使用された割合を意味します。通常の優先度のユーザープロセスの使用率は、一般的にuser(%)に含まれます。 | HP-UX,
AIX,
Solaris,
Linux |
| wait | Wait | % | 全CPU時間の中でCPUがI/Oの完了を待ってアイドル状態にあった割合 (I/O待機) を意味します。CPUが実際に計算を行った時間ではなく、ディスクやネットワークなどの外部リソースからの応答を待っていた時間として解釈されます。 | HP-UX,
AIX,
Solaris,
Linux |
| total | User+Sys | % | 全体のCPU使用率の中で、ユーザーモード(user)とカーネルモード(sys)で使用された割合の合計を意味します。一般的にI/O待機(wait)、irq、softirq、stealなどは除外された純粋 | HP-UX,
AIX,
Solaris, |

| Field | Title | Unit | Description | OS |
|------------|---------------|-------|---|---|
| | | | なCPU実行使用率として解釈されます。 | Linux,
Windows |
| total_wait | User+Sys+Wait | % | 全CPU時間のuser + sys + waitの合計を意味します。つまり、ユーザー処理、カーネル処理、I/O待機を含む使用指標です。 | HP-UX,
AIX,
Solaris,
Linux |
| idle | Idle | % | 全CPU時間の中でCPUが何の作業も行わずアイドル状態にあった割合を意味します。値が高いほどCPUに余裕がある状態を示します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| lCores | Logical Cores | count | OSが認識する論理CPU（論理コア）の数を意味します。物理コアの数とは異なる場合があります、Hyper-Threading/SMTが有効な場合、論理コアの数がより大きく表示されることがあります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| irq | Irq | % | 全CPU時間の中で割り込み要求(IRQ)を処理するために使用された割合を意味します。ネットワークカード、ディスク、その他のハードウェアイベント処理の負担が高いときに増加することがあります。 | Linux |
| softirq | Softirq | % | 全CPU時間の中でソフトウェア割り込み要求(SoftIRQ)を処理するために使用された割合を意味します。ネットワークパケット処理やブロックI/O後処理など、カーネルの遅延処理作業が多いときに増加することがあります。 | Linux |
| steal | Steal | % | 仮想化環境において、ハイパーバイザーが他の仮想CPUを優先的に処理している間、現在の仮想CPUが実行されずに奪われた時間の割合を意味します。値が高い場合、VMに割り当てられたCPUリソースが不足しているか、過剰競合状態である可能性があります。 | Linux |

| Field | Title | Unit | Description | OS |
|-------------|----------------|-------|--|-------------------------------------|
| procUtil | Processor Util | % | Windows専用の指標で、システム全体のプロセッサの総合CPU使用率を意味します。Windowsタスクマネージャーで確認できる全体のCPU使用率と同様です。 | Windows |
| loadavg_1m | LoadAvg 1m | count | 最近1分間の平均システム負荷(load average)を意味します。実行中または実行待機中のタスク、割り込み要求不可待機状態のタスクなどを反映し、CPU使用率とは異なる概念です。 | HP-UX,
AIX,
Solaris,
Linux |
| loadavg_5m | LoadAvg 5m | count | 最近5分間の平均システム負荷(load average)を意味します。短期的な変動よりも少し緩やかな傾向を見るために使用されます。 | HP-UX,
AIX,
Solaris,
Linux |
| loadavg_15m | LoadAvg 15m | count | 最近15分間の平均システム負荷(load average)を意味します。システム負荷の長期的な傾向を確認するために使用されます。 | HP-UX,
AIX,
Solaris,
Linux |

infra_mem

サーバー全体のメモリ使用状態を収集するカテゴリです。全体メモリ容量、使用量、使用率、cache、buffer、available memory、slab、page fault、swap in/out など、メモリ全般の使用状況と圧迫状態を確認するための指標を提供します。メモリ不足、reclaim、paging、cache 活用状態を把握するときに使用します。

- カテゴリ: MEMORY
- デフォルト収集周期: 2秒

| Field | Title | Unit | Description | OS |
|-------|-------|------|--|--|
| pUsed | Used | % | 全体メモリに対する現在使用中のメモリの割合を意味します。Linuxは通常、MemAvailableを基準にused = total - availableに近いと解釈します。ページキャッシュや再利用可能な一部のメモリは余剰メモリと見なされます。Windowsは一般的に | AIX, HP-UX,
Solaris,
Linux,
Windows |

| Field | Title | Unit | Description | OS |
|--------------|------------|------|---|--|
| | | | Availableを除いた使用量を基準に解釈します。
AIX / HP-UX / SolarisはLinuxのMemAvailableと同じ概念がないため、通常はOSが提供するused値を基準に算出します。 | |
| used | Used | byte | 現在使用中のメモリ使用量を意味します。Linuxは通常、MemTotal - MemAvailableの値を基にバイト単位で換算して使用します。Windowsは一般的にAvailableを除いた使用量を基準として解釈します。AIX / HP-UX / SolarisはLinuxのようにMemAvailableの基準がないため、OSが提供するusedの値を基に算出します。 | AIX, HP-UX,
Solaris,
Linux,
Windows |
| pCache | Cache | % | 全メモリの中でキャッシュ領域が占める割合を意味します。Linuxでは一般的に/proc/meminfoのCached値を基準とし、ページキャッシュ性質のメモリを指すが、バッファやSReclaimableは含まれません。AIX、HP-UX、SolarisはLinuxのMemAvailableと同じ概念がないため、通常はOSが提供するキャッシュ値を基準に算出します。 | HP-UX,
AIX,
Solaris,
Linux |
| cache | Cache | byte | キャッシュとして使用されるメモリのサイズを意味します。Linuxでは一般的に/proc/meminfoのCached値を基準とし、ページキャッシュ性のメモリを指しますが、BuffersやSReclaimableは含まれません。AIX、HP-UX、SolarisにはLinuxのMemAvailableと同じ概念がないため、通常はOSが提供するキャッシュ値を基準に算出します。 | HP-UX,
AIX,
Solaris,
Linux |
| buffer | Buffer | byte | 全メモリの中でI/Oバッファとして使用されるメモリ使用量をバイト単位で示した値です。Linux専用の指標であり、/proc/meminfoのBuffers値を基準としています。 | Linux |
| pUsed_pCache | Used+Cache | % | 現在の使用率(pUsed)とキャッシュ比率(pCache)を同時に示す指標です。ユーザー/カーネルが実際 | HP-UX,
AIX, |

| Field | Title | Unit | Description | OS |
|--------------|--------------|------|---|---|
| | | | に使用しているメモリとキャッシュ領域の比率を一緒に確認するための参考指標であり、標準的なメモリ指標というよりは運用解釈のための合成指標です。 | Solaris,
Linux |
| shared | Shared Size | byte | サーバ全体で使用されている共有メモリのサイズをバイト単位で示した値です。Linux専用の指標であり、tmpfs、shared memory、一部のshared mapping領域などが含まれることがあります。 | Linux |
| size | Total Size | byte | システムに割り当てられた全体の物理メモリサイズをバイト単位で示した値です。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| available | Available | byte | 現在使用可能なメモリサイズをバイト単位で示した値です。Linuxでは/proc/meminfoのMemAvailableを意味し、単純なフリーメモリだけでなく、再利用可能なキャッシュも一部反映した「即時利用可能な推定値」に近いです。瞬間的な値も重要ですが、時間とともに持続的に減少し、pageMajFaults、swapIn、swapOutが共に増加するパターンは、実際のメモリ圧迫が大きくなっていることを示唆することがあります。 | Linux |
| sreclaimable | Sreclaimable | byte | カーネルslab cacheの中で、必要に応じて回収(reclaim)可能な領域のサイズをバイト単位で示した値です。メモリの圧迫時には一部が回収される可能性があります。値が大きいからといって必ずしも問題があるわけではなく、現在のキャッシュの利用状況を示す意味もあります。ただし、時間が経過しても過度に増加したり、利用可能なメモリが減少し、回収が適切に行われていない場合は、追加の確認が必要かもしれません。 | Linux |

| Field | Title | Unit | Description | OS |
|---------------|-------------------|----------|---|-------|
| sunreclaim | Sunreclaim | byte | カーネルのスラブキャッシュにおける回収不可能な領域のサイズをバイト単位で示した値です。カーネルが引き続き保持しなければならないメモリであるため、SReclaimableよりもメモリ圧迫の観点でより直接的な意味を持ちます。値が持続的に増加するパターンは、カーネルメモリの使用拡大または異常な蓄積の可能性を解釈するのに役立ちます。 | Linux |
| slab | Slab | byte | カーネルがオブジェクトキャッシュ用に使用するスラブメモリの全体のサイズをバイト単位で示した値です。一般的には/proc/meminfoのSlabを意味し、SReclaimable + SUNreclaimの合計として解釈されます。現在の値も重要ですが、時間とともに持続的に増加する場合、カーネルメモリ使用の拡大を意味する可能性があり、特にSUNreclaimの増加が伴う場合は、回収可能なキャッシュの増加ではなく、実際のカーネルメモリの圧迫の可能性を検討する必要があります。 | Linux |
| pageFaults | Page Faults | counts/s | システム全体で発生したメモリアクセスプロセスにおける全ページフォルトの件数を1秒あたりの値で示した指標です。マイナーフォルトとメジャーフォルトの両方を含み、必ずしもディスクI/Oを伴うわけではありません。瞬間的な増加自体が問題とは見なされませんが、値が持続的に高くなったり、pageMajFaults、scanned、swapIn/Outの増加とともに現れる場合、メモリの圧迫やページキャッシュミスの増加の可能性を解釈するのに役立ちます。 | Linux |
| pageMajFaults | Page Major Faults | counts/s | システムで必要なページをディスク/ストレージから実際に読み込む必要があったメジャーページフォルトの件数を1秒あたりの値で示した指標です。読み込むソースはファイルシステムのファイルバックページである場合もあれば、スワップ領 | Linux |

| Field | Title | Unit | Description | OS |
|------------|------------|---------|--|-------------------------------------|
| | | | 域である場合もあります。値が持続的に高いか、増加傾向を示す場合は単なるメモリアクセスの増加ではなく、実際のI/Oを伴うメモリの圧迫の可能性を示唆し、応答遅延と直接的に関連することもあります。swapIn、fsIn、availableと一緒に見ることが重要です。 | |
| scanned | Page Scan | pages/s | システムがメモリを確保するためにスキャンしたページ数を意味します。値が高くなるほど、メモリ確保のためのリクレーン活動が活発であることを示し、持続的に高いレベルを示す場合はメモリ圧迫が増していることを示唆します。一時的な上昇よりも長時間の持続と freed、steal、swapIn/Out との関係と一緒に解釈することが重要です。 | HP-UX,
AIX,
Solaris,
Linux |
| freed | Page Free | pages/s | ページの回収やページの解放などによって確保されたフリーページ数を意味します。システムのリクレーンまたはメモリ返却活動の結果を示す指標です。値そのものよりも、スキャンされたページとの関係、そして持続的な増加の有無と一緒に確認することが重要です。スキャンされたページが高いのに解放されたページが十分に追いつかない場合、メモリ確保の効率が低下していることを示唆する可能性があります。 | HP-UX,
AIX,
Solaris,
Linux |
| steal | Page Steal | pages/s | Linuxにおけるページリクレーンプロセスで実際に回収されたページ数を意味します。メモリ不足の状況でページキャッシュや非アクティブページなどを確保するプロセスに関連しています。値が一時的に増加するのは正常なリクレーン動作である可能性がありますが、持続的に高く維持される場合は、システムが引き続きメモリ圧迫状態でページを回収していることを意味する可能性があります。 | Linux |
| stealRatio | Page Steal | % | Linuxでスキャンしたページの中で、実際に回収 | Linux |

| Field | Title | Unit | Description | OS |
|---------|---------------|---------|---|---|
| | Ratio | | <p>されたページの割合を意味します。一般的には $\text{steal} / \text{scanned} * 100$ で計算され、値が高いほどスキャンに対する回収効率が高く、値が低いほどアクティブページの比率が高く、回収がうまくいかない状況である可能性があります。(0は意味がありません) ただし、ワークロードの特性により解釈が異なる場合があるため、scanned、freed、availableと一緒に確認することが重要です。</p> | |
| swapIn | Swap In | pages/s | <p>ディスクのスワップ（ページングスペース）領域からメモリに毎秒再読み込みされるページ数を意味します。値が持続的に発生したり増加傾向を示す場合、メモリ不足によりスワップ依存度が高まっていることを示唆し、応答遅延に直接つながる可能性があります。一時的な発生よりも持続性の有無を重視することが望ましいです。</p> | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| swapOut | Swap Out | pages/s | <p>メモリからディスクのスワップ（ページングスペース）領域に毎秒出力されるページ数を意味します。値が持続的に発生する場合、システムがメモリを確保するためにページをスワップに押し出していることを示します。スワップインとともに持続的に高いパターンが見られる場合、パフォーマンスの低下の可能性が高いメモリ圧迫状態を示唆することがあります。</p> | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| fsIn | Filesystem In | pages/s | <p>ファイルシステムの読み取り操作によってメモリに取り込まれたページ数を意味します。Swap Inとは異なり、ファイルシステムI/Oによってロードされたページを指します。現在の値も意味がありますが、pageMajFaults、プロセスのrdisklo、availableと共に増加するパターンは、実際のファイルベースのページイン活動が増加していることを解釈するのに役立ちます。</p> | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| fsOut | Filesystem | pages/s | <p>ファイルシステムの書き込み操作によってディス</p> | HP-UX, |

| Field | Title | Unit | Description | OS |
|---------------------|-----------------------|------|---|---------------------------------------|
| | Out | | クに記録されたページ数を意味します。スワップアウトとは異なり、ファイルシステムのwriteback/flush性質のページ記録量として解釈するのが適切です。値の持続的な増加や周期的な急騰パターンは、flush/writeback/checkpointなどの作業特性と関連付けて解釈できます。 | AIX,
Solaris,
Linux,
Windows |
| poolPaged | Pool Paged | byte | Windows専用の指標で、ページプール（Paged Pool）のバイトサイズを示します。必要に応じてディスクにページングされる可能性のあるカーネルメモリ領域を意味します。 | Windows |
| poolNonPaged | Pool Nonpaged | byte | Windows専用指標で、ノンページプールのバイトサイズを示します。常に物理メモリに常駐しなければならないカーネルメモリ領域を意味します。 | Windows |
| systemCacheResident | System Cache Resident | byte | Windows専用の指標で、現在物理メモリに常駐しているシステムキャッシュメモリのバイトサイズを示します。ファイルシステムキャッシュに関連するカーネルメモリの使用量を反映しています。 | Windows |

infra_swap

サーバー全体の swap または paging space 使用状態を収集するカテゴリです。全体 swap サイズ、使用量、使用率などを通じて、ディスクベースの仮想メモリ使用レベルを把握できます。メモリ不足による swap 使用の有無や、全般的な仮想メモリ圧迫状態を確認するときに使用します。

- カテゴリ: SWAP
- デフォルト収集周期: 2秒

| Field | Title | Unit | Description | OS |
|-------|------------|------|---|----------------------------|
| size | Total Size | byte | システムに構成された全体のスワップ領域のサイズをバイト単位で示した値です。UNIX/Linux系ではスワップ/ページングスペースの総サイズを意味し、Windowsではページファイルに基づく仮想メモリ領域の総サイズに相当しま | HP-UX,
AIX,
Solaris, |

| Field | Title | Unit | Description | OS |
|-------|-------|------|--|---|
| | | | す。 | Linux,
Windows |
| pUsed | Used | % | 全体のスワップ領域に対する現在使用中のスワップ比率を意味します。used / size * 100で計算します。値が高いほど、メモリ不足によりディスクベースの仮想メモリ使用割合が高まった可能性を示します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| used | Used | byte | 現在使用中のスワップ領域のサイズをバイト単位で示した値です。UNIX/Linux系ではスワップ/ページングスペースで実際に占有されているスペースを意味し、Windowsではページファイルの使用量に相当する値を意味します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |

infra_kernel

OS カーネルおよびシステム動作状態を収集するカテゴリです。run queue、block queue、context switch、interrupt、syscall、fork、exec など、カーネルおよびスケジューラー観点の動作指標を提供します。CPU 競合、I/O 待機、スケジューリング負荷、カーネル進入頻度などを把握するときに使用します。

- カテゴリ: System Kernel
- デフォルト収集周期: 2秒

| Field | Title | Unit | Description | OS |
|-------|----------|-------|--|---|
| runq | RunQueue | count | 実行準備が完了しましたが、まだCPUを割り当てられていないため、実行待機キューにあるプロセスまたはスレッドの数を意味します。値が高いほど、CPU競合があるか、実行可能な作業がCPUリソースよりも多いことを示唆します。実行待機キューはCPU使用率と共に確認することが重要です。CPU使用率が高く、実行待機キューも高い場合、CPUボトルネックの可能性が大きく、CPU使用率が低いのに実行待機キューが高い場合は、ロック、スケジューリング、優先順位の問題を疑うことができます。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |

| Field | Title | Unit | Description | OS |
|----------|--------------|----------|---|-------------------------------------|
| blockq | BlockQueue | count | I/O、ページング、リソース待機などのために即時実行できない状態で待機中のプロセスまたはスレッドの数を意味します。一般的にディスクI/O、メモリ待機、リソース競合が多いときに増加する可能性があります。値が高いということは、CPU不足よりもI/O、ページング、リソース待機に関連するボトルネックの可能性を示唆します。ディスク性能指標とスワップ指標を一緒に確認することを推奨します。 | HP-UX,
AIX,
Solaris,
Linux |
| pendingq | PendingQueue | count | AIX専用の指標で、一般的にraw device I/Oリクエストに対してまだ完了応答を受け取っていない待機中のスレッド数を意味します。ストレージ応答の遅延やraw I/Oの競合が大きいときに増加する可能性があります。 | AIX |
| waitq | WaitQueue | count | HP-UX / Solaris系の指標で、主にスワップアウトされたり、一時的にスケジューリング対象から除外されて待機中のプロセスまたはスレッドの数を意味します。単純なrun queueとは異なり、即座にCPUを受け取って実行可能な状態とは区別されます。 | HP-UX,
Solaris |
| fork | Fork | counts/s | 秒あたりのfork()呼び出し回数を意味します。forkは、現在のプロセスを複製して新しい子プロセスを生成するシステムコールです。値が高い場合、短命のプロセスが頻繁に生成される環境である可能性があります。シェルスクリプト、バッチジョブ、CGI/プロセス型アプリケーションのように、プロセスを頻繁に生成する環境では自然に高くなるため、通常と比べて急増しているかどうかにより重要です。 | HP-UX,
AIX,
Solaris,
Linux |
| exec | Exec | counts/s | 秒当りのexec()の呼び出し回数を示します。execは、現在のプロセスのPIDを保持したまま、プロセスのメモリイメージと実行内容を新しいプログラムに置き換えるシステムコールです。forkのように新しいプロセスを生成するのではなく、既存のプロセスを別のプログラムに置き換えます。シェルスクリプト、バッチジョブ、CGI/プロセス型アプリケーションのようにプログラムの置き換えが頻繁に行われる環境では、自然に高くなる可能性があるため、通常と比べて急増しているかどうかにより重要です。 | HP-UX,
AIX,
Solaris |

| Field | Title | Unit | Description | OS |
|-----------|---------------|----------|---|---|
| interrupt | Interrupt | counts/s | CPUが1秒間にハードウェア割り込みを処理した回数を意味します。ネットワーク、ディスク、タイマー、その他のデバイスイベントが多いほど増加する可能性があります。値が高い場合は、ネットワークパケットの処理量の増加、ストレージI/Oの増加、特定のデバイスの割り込みの偏りなどを一緒に分析することを推奨します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| syscall | SystemCall | counts/s | カーネルが1秒間に処理したシステムコールの回数を意味します。ユーザープロセスがファイルI/O、ネットワーク、プロセス制御などのカーネルサービスを要求する際に増加します。値が高いからといって必ずしも異常ではありませんが、ワークロードの特性の変化やカーネルへのエントリ頻度の増加を反映する可能性があります。ファイル/ソケットI/Oが多いアプリケーションでは高くなる可能性があります。 | HP-UX,
AIX,
Solaris,
Windows |
| ctxswitch | ContextSwitch | counts/s | 秒あたりのコンテキストスイッチの回数を意味します。実行中のプロセスまたはスレッドから他の作業にCPUが切り替わると増加します。値が高いほど、マルチタスク、スレッド競合、ロック競合、短い作業単位の処理が多い可能性があります。ctxswitchが非常に高い場合、CPUが実際の作業を行うよりもスケジューリングの切り替えコストに多くの時間を費やしている可能性があるためrunq、syscall、interrupt、ロック競合の状況と一緒に確認することを推奨します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |

infra_disk

サーバーに接続された全体物理ディスクの集計パフォーマンスを収集するカテゴリです。読み取り/書き込みスループット (Byte/s)、IOPS など、サーバー全体のディスク I/O 規模を確認するための指標を提供します。サーバー全般のディスク負荷レベルを把握するときに使用します。

- カテゴリ: DISK
- デフォルト収集周期: 2秒

| Field | Title | Unit | Description | OS |
|-----------|---------------|----------|--|---|
| read | Read | bytes/s | サーバーのすべての物理ディスクから毎秒読み取られたデータ処理量の合計をByte/s単位で示した値です。つまり、サーバー全体の物理ディスクの読み取りスループットの集計値です。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| write | Write | bytes/s | サーバーのすべての物理ディスクからの1秒あたりの書き込みデータ処理量の合計をByte/s単位で示した値です。つまり、サーバー全体の物理ディスクの書き込みスループットの集計値です。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| total | IO
Total | bytes/s | サーバーのすべての物理ディスクからの毎秒の読み取りおよび書き込みスループットを合算した全体のデータスループットをByte/s単位で示した値です。read + writeに該当するサーバー全体のディスクI/Oスループットの集計値です。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| readIops | Read
IOPS | counts/s | サーバーのすべての物理ディスクで毎秒処理された読み取りI/O作業数の合計をIOPS単位で示した値です。つまり、サーバー全体の物理ディスクの読み取りIOPS集計値です。IOPSはディスクが毎秒処理したI/Oリクエストの件数を示す指標であり、データサイズ自体は反映されません。したがって、小さなブロックI/Oが多い環境ではIOPSが高く、スループット（Byte/s）は相対的に低くなる可能性があり、大きなブロックI/Oが多い環境ではIOPSが低くてもスループット（Byte/s）は高くなる可能性があります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| writeIops | Write
IOPS | counts/s | サーバーのすべての物理ディスクで毎秒処理された書き込みI/O作業数の合計をIOPS単位で示した値です。つまり、サーバー全体の物理ディスクの書き込みIOPS集計値です。IOPSはディスクが毎秒処理したI/Oリクエストの件数を示す指標であり、データサイズ自体は反映されません。したがって、小さなブロックI/Oが多い環境ではIOPSが高く、スループット（Byte/s）は相対的に低くなる可能性があります。一方、大きなブロックI/Oが多い環境ではIOPSが低くてもスループット（Byte/s）は高くなる可能性があります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |

| Field | Title | Unit | Description | OS |
|-----------|------------|----------|---|---|
| totalIops | Total IOPS | counts/s | サーバーのすべての物理ディスクで毎秒処理された読み取りと書き込みI/O作業数を合算した全体のI/O作業数をIOPS単位で示した値です。readIops + writeIopsに相当するサーバー全体のディスクI/O作業数の集計値です。IOPSはディスクが毎秒処理したI/Oリクエストの件数を示す指標であり、データのサイズ自体は反映されません。したがって、小さなブロックI/Oが多い環境ではIOPSが高く、スループット(Byte/s)は相対的に低くなる可能性があり、大きなブロックI/Oが多い環境ではIOPSが低くてもスループット(Byte/s)は高くなる場合があります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| busyMax | Busy Max | % | サーバーに接続されたすべての物理ディスクの中で、収集期間中に最も高いbusy(%)値を持つディスクの使用率を示します。つまり、サーバー全体のディスクの中で最も忙しく動作しているディスクのbusyレベルを意味します。値が高いほど、特定のディスクにI/O負荷が集中しているか、ボトルネックの可能性を示す場合があります。ただし、この値は基本的に2秒ごとに収集され、個別のディスク性能指標におけるbusy値は基本的に5秒ごとに収集されるため、同じ時刻のチャートでも個別ディスクのbusy値と完全に一致しない場合があります。特に低いbusy期間や瞬間的な負荷増加期間では、収集期間とサンプリング時点の違いにより値の差が大きく見えることがあります。したがって、この値はサーバーユニットのディスク負荷の兆候を迅速に確認するための代表的な指標として活用し、実際のボトルネックディスクの確認はディスクごとの詳細指標を併せて確認することを推奨します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| diskName | Busy Disk | string | サーバーに接続されているすべての物理ディスクの中で、最も高いbusy(%)値を持つディスク名を表示した値です。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |

infra_network

サーバー全体のネットワーク使用量とインターフェースごとの使用レベルを集計して提供するカテゴリです。

Loopbackを除いたNICの送受信bps、送受信pps、全体トラフィック、最大NIC使用率および該当NIC名を収集します。これにより、サーバー全体のネットワーク負荷の推移を確認し、ネットワーク使用率が最も高いインターフェース

を識別できます。

- カテゴリ: NETWORK
- デフォルト収集周期: 2秒

| Field | Title | Unit | Description | OS |
|----------|-----------|----------|--|---|
| rxbps | Net Rx | bps | サーバーのすべてのNIC（ループバックを除く）を通じて、1秒あたりに受信（Rx）された全データ転送量の合計をbps(bit per second)単位で示した値です。つまり、サーバー全体のネットワーク受信帯域幅の集計値です。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| txbps | Net Tx | bps | サーバーのすべてのNIC（ループバックを除く）を通じて、1秒あたりに送信された全データ転送量の合計をbps(bit per second)単位で示した値です。つまり、サーバー全体のネットワーク送信帯域幅の集計値です。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| totalbps | Net Total | bps | サーバーのすべてのNIC（ループバックを除く）を通じて、1秒あたりに受信（Rx）および送信（Tx）された全データ転送量の合計をbps(bit per second)単位で示した値です。rxbps + txbpsに該当するサーバー全体のネットワーク帯域幅の集計値です。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| rxpps | Rx PPS | counts/s | サーバーのすべてのNIC（ループバックを除く）を通じて、1秒あたりに受信（Rx）されたパケット数の合計をpps(packets per second)、またはcount/s単位で示した値です。つまり、サーバー全体のネットワーク受信パケット処理量の集計値です。ppsは転送量の大きさに関係なくパケット数に基づくため、小さなパケットが多い場合、ppsは高く、bpsは相対的に低くなる可能性があります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| txpps | Tx PPS | counts/s | サーバーのすべてのNIC（ループバックを除く）を通じて、1秒あたりに送信されたパケット数の合計をpps(packets per second)、またはcount/s単位で示した値です。つまり、サーバー全体のネットワーク送信パケット処理量の集計値です。ppsは転送量の大きさに関係なくパケット数に基づくため、小さなパケットが多い場 | HP-UX,
AIX,
Solaris,
Linux,
Windows |

| Field | Title | Unit | Description | OS |
|--------------|--------------------|----------|--|---|
| | | | 合、ppsは高く、bpsは相対的に低くなる可能性があります。 | |
| totalpps | Total PPS | counts/s | サーバーのすべてのNIC（ループバックを除く）を通じて、1秒あたりに受信（Rx）および送信（Tx）された全パケット数を合算した値をpps(packets per second)、またはcount/s単位で示したものです。rxpps + txppsに該当するサーバー全体のネットワークパケット処理量の集計値です。ppsは転送量の大きさに関係なくパケット数に基づくため、小さなパケットが多い場合、ppsは高く、bpsは相対的に低くなる可能性があります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| linkUsageMax | NIC Max Usage | % | サーバーに存在するすべてのNIC（ループバックを除く）の中で、リンク使用率（linkUsage）が最も高いNICの使用率をパーセンテージ（%）で示した値です。サーバー全体のネットワークインターフェースの中で、どのNICが最も高い負荷状態にあるかを迅速に確認するための指標です。一般的に各NICのlinkUsage値の最大値に相当し、linkSpeed情報を確認できないNICは計算対象から除外されるか、値が反映されない場合があります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| nicName | Max Usage NIC Name | string | サーバーに存在するすべてのNIC（ループバックを除く）の中で、リンク使用率（linkUsage）が最も高いNICの名前を示す値です。linkUsageMax値がどのNICで発生したかを識別するための項目です。例えば、Linuxのeth0、ens192、bond0、Windowsのアダプタ名などが表示される可能性があります。計算可能なNICがない場合、値は空になることがあります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |

infra_netstat

サーバーの TCP ネットワーク接続状態を状態別に集計した情報です。

- カテゴリ: Network State Summary
- デフォルト収集周期: 60秒
- 最小サポートエージェント: Linux 2.9.18+, Windows 2.9.18+, AIX 1.4.9+, Solaris 1.4.9+, HP-UX 1.4.9+

| Field | Title | Unit | Description | OS |
|---------------------|-------------|-------|---|-------------------------------------|
| netstat_Listen | Listen | count | 現在のサーバーで外部接続要求を受け付けるために待機中のLISTEN状態のTCPソケットの数です。主にサービスポートが正常に開いているか確認する際に使用されます。 | HP-UX,
AIX,
Solaris,
Linux |
| netstat_Established | Established | count | 現在のサーバーで正常に確立されたデータ送受信が可能なESTABLISHED状態のTCP接続の数です。実際に通信中のセッション数を示します。 | HP-UX,
AIX,
Solaris,
Linux |
| netstat_Close_Wait | Close_Wait | count | リモート側から接続終了が要求されましたが、まだローカルアプリケーションがソケットを完全に閉じていないCLOSE_WAIT状態のTCP接続の数です。この値が継続的に多い場合は、アプリケーションのソケットクリーンアップの遅延またはリークの可能性を確認する必要があります。 | HP-UX,
AIX,
Solaris,
Linux |
| netstat_Closing | Closing | count | 両方の接続がCLOSING状態で終了手続きを進めているTCP接続の数です。一般的に短く表示されますが、持続的または過度に増加する場合は異常な終了処理の確認が必要です。 | HP-UX,
AIX,
Solaris,
Linux |
| netstat_Fin_Wait1 | Fin_Wait1 | count | ローカル側が接続終了を開始し、FINを送信した後、相手側の応答を待っているFIN_WAIT1状態のTCP接続数です。接続終了手続きの初期段階に該当します。 | HP-UX,
AIX,
Solaris,
Linux |
| netstat_Fin_Wait2 | Fin_Wait2 | count | ローカル側が接続終了要求に対する応答を受け取った後、リモート側の最終終了信号を待っているFIN_WAIT2状態のTCP接続の数です。この状態が長く続く場合、終了遅延または相手側の処理問題の可能性が疑われます。 | HP-UX,
AIX,
Solaris,
Linux |
| netstat_Time_Wait | Time_Wait | count | 接続終了後の遅延パケット処理と同様のソケット再利用の競合を防ぐために、一定時間保持されるTIME_WAIT状態のTCP接続の数です。短い接続が非常に多い環境では、この値が大きく増加する可能性があります。 | HP-UX,
AIX,
Solaris,
Linux |

| Field | Title | Unit | Description | OS |
|------------------|----------|-------|---|-------------------------------------|
| netstat_Syn_Recv | Syn_Recv | count | リモート側からの接続要求(SYN)を受信し、応答した後、最終確認を待っているSYN_RECV状態のTCP接続の数です。値が急激に増加すると、接続要求の急増やSYN Floodの性質についても確認する必要があります。 | HP-UX,
AIX,
Solaris,
Linux |
| netstat_Syn_Sent | Syn_Sent | count | ローカル側が接続要求(SYN)を送信した後、相手側の応答を待っているSYN_SENT状態のTCP接続の数です。リモートサーバーの応答遅延、ネットワーク経路の問題、ファイアウォールの問題などがある場合に増加する可能性があります。 | HP-UX,
AIX,
Solaris,
Linux |
| netstat_Last_Ack | Last_Ack | count | リモート側からの終了要求を受信した後、ローカル側も終了応答を送り、最後の確認を待っているLAST_ACK状態のTCP接続の数です。一般的に短期間保持され、継続的に多い場合は終了処理の遅延の有無を確認する必要があります。 | HP-UX,
AIX,
Solaris,
Linux |
| netstat_Unknown | Unknown | count | 定義された主要なTCP状態に分類されていないか、収集時点で状態を明確に識別できなかった接続の数です。一般的に値は大きくないはずで、継続的に増加する場合は収集ロジックまたはOSごとの状態マッピング基準を確認する必要があります。 | HP-UX,
AIX,
Solaris,
Linux |

infra_ntp_info

サーバーの時刻同期状態を収集するカテゴリです。NTP 使用の有無、同期デーモン、同期状態、使用中の NTP サーバー、offset、offset 方向、time zone などを提供します。システム時刻が基準時刻とどれだけ差があるか、NTP 同期が正常かを確認するときに使用します。

- カテゴリ: NTP Information
- デフォルト収集周期: 60秒
- 最小サポートエージェント: Linux 2.9.18+, Windows 2.9.18+, AIX 1.4.9+, Solaris 1.4.9+, HP-UX 1.4.9+

| Field | Title | Unit | Description | OS |
|------------|-------------|--------|--|---|
| checkTime | Check Time | string | NTP情報収集または確認が行われた時刻を意味します。該当結果が生成された時点のエージェントがインストールされたサーバーのローカルシステム時間を表示します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| ntpInUse | NTP In Use | string | このシステムでNTPベースの時間同期機能が使用されているかどうかを示します。YesはNTPまたは時間同期デーモンが設定されて使用中の状態を意味し、Noは使用されていないか、関連するデーモンが動作していない状態を示します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| ntpDaemon | NTP Daemon | string | 該当システムで使用中の時間同期デーモンまたはサービス名を示します。例えば、Linux/Unix系ではchrony、ntpd、xntpd、Windowsではw32timeなどが表示されることがあります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| timeSynced | Time Synced | string | 現在のシステムがNTPサーバーと正常に時間同期されているかどうかを示します。Yesは現在有効なNTPサーバーと同期中の状態、NoはNTPが使用中ですがまだ同期されていないか、有効な同期対象を確保できていない状態を意味します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| ntpServer | NTP Server | string | 現在の時間同期に使用されているNTPサーバーのホスト名またはIPアドレスを示します。同期が正常に行われていない場合、値が空である可能性があります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| offset | Offset (ms) | ms | 現在のシステム時間と基準NTPサーバー時間との間の差をms（ミリ秒）単位の絶対値で示したものです。速いか遅いかの方向情報はoffsetDirectionフィールドで区別します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |

| Field | Title | Unit | Description | OS |
|-----------------|------------------|--------|---|---|
| offsetDirection | Offset Direction | string | 現在のシステム時間が基準NTPサーバーの時間よりも早いか遅いかを示します。例えば、FAST(+)はローカルシステム時間が早い状態、SLOW(-)はローカルシステム時間が遅い状態を意味します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| timeZone | Time Zone | string | システムに設定されたタイムゾーン情報を示します。OSによってAsia/Tokyo、JST、Japan Standard Timeなど、異なる形式で表示されることがあります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |

infra_process

サーバー全体のプロセス状態を集計して表示するカテゴリです。全体プロセス数、スレッド数、zombie 数、runnable/sleeping 状態数、file descriptor 使用量など、プロセス/スレッド全般の状態を確認できます。プロセス数の急増、zombie の蓄積、FD 枯渇などのシステム運用状態を把握するときに使用します。

- カテゴリ: Process State Summary
- デフォルト収集周期: 2秒

| Field | Title | Unit | Description | OS |
|-------------|---------------|-------|---|---|
| procTotal | Process Total | count | OSに現在存在する全プロセス数を意味します。プロセス数が多いからといって必ずしも異常ではありません。バッチ、Webサーバーのprefork構造、短い作業単位が多い環境では自然に高くなる可能性があります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| threadTotal | Thread Total | count | OSに現在存在する全スレッド数を意味します。マルチスレッドアプリケーションが多いほど増加する可能性があり、プロセス数よりもシステム負荷をより直接的に反映する場合もあります。スレッド数はプロセス数よりも実際の同時性レベルをよりよく示すことができます。Java、WAS、DB、マルチスレッドアプリ環境では、threadTotalの傾向が重要です。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |

| Field | Title | Unit | Description | OS |
|----------------|------------------|-------|---|-------------------------------------|
| handleTotal | Handle Total | count | Windows OSで現在開いてあるか、または使用中の全ハンドル数を意味します。ファイル、レジストリキー、プロセス、スレッド、イベント、ミューテックスなどのさまざまなカーネルオブジェクトへの参照数を含みます。 | Windows |
| runnableTotal | Runnable Total | count | Linuxにおけるプロセス状態がRであるプロセス数を意味します。現在実行中であるか、実行可能だがCPUを待ちながらrun queueに載せられたプロセスを含みます。 | Linux |
| sleepingTotal | Sleeping Total | count | Linuxにおけるプロセス状態がSであるプロセスの数を意味します。割り込み可能なスリープ状態で、イベントやリソースの応答を待ちながら、信号によって目覚めることができるプロセスを含みます。一般的な待機状態のプロセスが最も多く分布する範囲です。 | Linux |
| idleTotal | Idle Total | count | Linuxにおけるプロセス状態がIであるプロセス数を意味します。カーネルスケジューラの観点からアイドル状態として表示されるタスク数を意味し、一般ユーザープロセスよりもカーネル内部のワーカーやアイドル系タスクで見られることがあります。 | Linux |
| disksleepTotal | Disk Sleep Total | count | Linuxにおけるプロセス状態がDであるプロセス数を意味します。割り込み不可能な待機状態で、主にディスクI/O、ファイルシステム、デバイス、カーネルリソースを待機しているプロセスが含まれます。値が高く持続する場合、ストレージまたはカーネル待機のボトルネックを疑うことができます。 | Linux |
| zombieTotal | Zombie Total | count | 親プロセスによってまだ回収されていないため、ゾンビ(Z)状態のまま残っているプロセスの数を意味します。継続的に増加する場合は、親プロセスの待機処理の問題やプロセス回収の遅延を疑うことができます。 | HP-UX,
AIX,
Solaris,
Linux |
| stoppedTotal | Stopped Total | count | Linuxにおけるプロセス状態がTであるプロセス数を意味します。一般的にジョブ制御信号(SIGSTOP、SIGTSTPなど)によって停止されたプロセスを示します。 | Linux |

| Field | Title | Unit | Description | OS |
|------------------|--------------------|-------|---|-------|
| tracingstopTotal | Tracing Stop Total | count | Linuxにおけるプロセス状態がtのプロセス数を意味します。一般的にデバグ（ptrace）などによってトレース停止状態で停止したプロセスを示します。 | Linux |
| deadTotal | Dead Total | count | Linuxにおけるプロセス状態がXのプロセス数を意味します。終了処理中または完全に終了した状態を意味しますが、一般的な運用環境ではほとんど観測されません。 | Linux |
| wakekillTotal | Wake Kill Total | count | Linuxにおけるプロセス状態がKのプロセス数を意味します。カーネル内部状態に分類される場合があり、一般的な運用環境ではほとんど観測されず、カーネルのバージョンによって意味が異なることがあります。 | Linux |
| wakingTotal | Waking Total | count | Linuxにおけるプロセス状態がWであるプロセスの数を意味します。目覚めている（waking）処理中の遷移状態と見なすことができ、最新のカーネルではほとんど見られないか、環境依存的にのみ観測される可能性があります。 | Linux |
| otherTotal | Other Total | count | Linuxで明示的に分離されたR/S/I/D/Z/T/t/X/K/W以外のその他のプロセス状態を持つプロセス数を意味します。カーネルバージョンの違いや観測時の遷移状態、実装の違いにより、含まれる対象が異なる場合があります。 | Linux |
| openfdCurrent | Open fd Used | count | Linux OS全体で現在使用中のファイルディスクリプタの数を意味します。ファイル、ソケット、パイプ、デバイスなど、カーネルがファイルディスクリプタで管理するオープンオブジェクトの数を含みます。 | Linux |
| openfdMax | Open fd Max | count | Linux OS全体で設定された最大ファイル記述子数を意味します。一般的にシステム全体のファイル記述子の制限（/proc/sys/fs/file-max）に基づいて解釈されます。 | Linux |
| openfdPUsed | Open fd Used | % | Linux OS全体のファイルディスクリプタ使用率を意味します。一般的にopenfdCurrent / openfdMax * 100で計算され、値が高いほどシステム全体のFD枯渇リスクが高まります。 | Linux |

infra_nic_info

サーバー内の各ネットワークインターフェースの構成情報を収集するカテゴリです。NIC 名、IP、MAC、link、state、duplex、speed、mode、driver などの静的または半静的情報を提供します。NIC 構成変更の監視、冗長化構造の確認、インターフェースの識別に使用します。

- カテゴリ: NIC Information
- デフォルト収集周期: 60秒
- 最小サポートエージェント: Linux 2.9.18+, Windows 2.9.18+, AIX 1.4.9+, Solaris 1.4.9+, HP-UX 1.4.9+

| Field | Title | Unit | Description | OS |
|------------|-------------|--------|--|---|
| nicName | NIC Name | string | OSが認識するネットワークインターフェース名で、一般的な物理NICだけでなく、エイリアスインターフェース、bond/team/bridge、EtherChannel、APA、AGGR、IPMPなどの論理インターフェースおよびその所属メンバーNICと一緒に表示されることがあります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| ipAddress | IP Address | string | このNICに設定されたIPv4アドレスであり、複数のアドレスがある場合はカンマ(,)で表示され、IPがない場合はnoneと表示されることがあります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| macAddress | MAC Address | string | 該当NICに割り当てられたMACアドレスであり、論理/集約インターフェースはOSが報告する代表的なMACが表示される場合があります、確認できない場合はnoneと表示されることがあります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| link | Link | string | OSまたはドライバーが判断したリンク接続の有無を示します。yesは接続状態、noは未接続または非アクティブ状態を意味し、実際のケーブルの状態と完全に一致しない場合があります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| state | State | string | 該当NICの現在のインターフェース状態を示します。UPは使用可 | HP-UX, |

| Field | Title | Unit | Description | OS |
|---------------|----------------|--------|--|---|
| | | | 能、DOWNは非アクティブまたは使用不可、Unknown/Unknown!は状態確認不可を意味します。 | AIX,
Solaris,
Linux,
Windows |
| duplex | Duplex | string | NICのDuplexモードを示します。Fullは全二重、Halfは半二重、unknownはオペレーティングシステム・ドライバ・デバイスの特性上確認できない状態を意味します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| speed | Speed | string | 該当NICの現在のリンク速度またはOSが報告した動作速度です。最大サポート速度ではなく、現在交渉または認識された速度を意味し、一部の集約インターフェースは合算値として表示される場合があります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| mode | Mode | string | NICの集約、冗長化またはチーミング方式に関する追加情報を示します。例えばAIXのEtherChannel:<mode>、HP-UXのAPA、Windowsのチーミングモード/負荷分散、SolarisのAGGRまたはIPMPが表示されることがあります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| windowsDriver | Windows Driver | string | Windows環境で該当NICが使用するドライバまたはアダプターの説明情報です。 | Windows |
| 二重化構成の表示方式 | | | | |

nicName と mode フィールドは、二重化構成に応じて次のように表示します。

| Item | Description |
|---------------|--|
| Linux bonding | ボンディングに属するメンバーインターフェイスは bond0_eth1 の形式で ボンディング名_メンバー名 として表示し、 mode にはそのボンディングのモードを表示 |

| Item | Description |
|--------------------|---|
| Windowsチームインターフェイス | mode に LBFO/<チームモード>/<負荷分散方式> の形式で表示（例：LBFO/SwitchIndependent/TransportPorts） |
| Windowsチームメンバー NIC | mode に LBFO_MEMBER/<設定された役割>/<動作状態> の形式で表示（例：LBFO_MEMBER/Active/Active） |

WindowsのチームメンバーNICは自身のIPアドレスを持たない非表示のアダプターであるため、以前はリストに表示されませんでしたが、現在はメンバーNICもあわせて収集します。Linuxでは、ボンディングドライバーの制御用項目（bonding_masters）をネットワークインターフェイスとして誤って表示していた問題を修正しました。

infra_process_group

サーバーで除外なく収集した全体プロセスを対象に、基本的には実行 argument が異なっても同じ User によって同じ cmd で実行されたプロセスをグループ化して、リソース使用状況を提供するカテゴリです。グループ単位で CPU、メモリ、I/O、page fault などの使用量を合算して表示するため、ユーザーは同一のプログラム系列がサーバーリソースに与える影響を一目で把握できます。また、ユーザー定義の process group 管理機能を通じて、特定のサーバー/owner/argsPattern 条件でグループを直接定義し、ユーザー指定の process group name で管理できます。

- カテゴリ: ProcessGroup
- デフォルト収集周期: 5秒

| Field | Title | Unit | Description | OS |
|-------|---------|--------|--|-------------------------------------|
| cmd | Command | string | プロセスグループに属するプロセスの実行コマンド(cmd)です。 | HP-UX, AIX, Solaris, Linux, Windows |
| name | Name | string | 基本はcmdを表示しますが、ユーザーがプロセスグループ管理メニューを通じて定義したプロセスグループの場合は、定義したプロセスグループの名前を表示します。 | HP-UX, AIX, Solaris, Linux, Windows |
| owner | Owner | string | プロセスグループに属するプロセスの実行アカウント (user) です。同一ユーザーを基準にグループ化される | HP-UX, AIX, Solaris, |

| Field | Title | Unit | Description | OS |
|---------|-----------------|--------|--|--|
| | | | め、グループ内のプロセスは同一の所有者を持ちます。 | Linux,
Windows |
| pidList | Process ID List | string | Process TopNで収集されたプロセスIDのみをリストとして提供します。したがって、表示されるプロセスIDの数はプロセス数と異なる場合があります。 | HP-UX, AIX,
Solaris,
Linux,
Windows |
| custom | Custom | string | ユーザー定義のプロセスグループかどうかをTrue/Falseで表示します。 | HP-UX, AIX,
Solaris,
Linux,
Windows |
| cpu | CPU | % | プロセスグループに属するプロセスが使用した全体のCPU使用率を意味します。ユーザーモードとシステムモードの使用率を含む値であり、時間に伴う持続的な増加、長時間の高使用率維持、周期的な急増パターンを一緒に見ること、該当グループの演算負荷特性や異常なCPU占有の有無を解釈するのに役立ちます。 | HP-UX, AIX,
Solaris,
Linux,
Windows |
| cpuUser | CPU User | % | Process Groupに属するプロセスがユーザーモードで使用したCPU使用率を意味します。アプリケーションロジックの実行に使用されたCPUの割合を確認するための指標です。現在の値だけでなく、時間に伴う持続的な増加、繰り返しの急騰パターン、procCnt/threadCntの変化との関連性を一緒に見ること、業務処理量の増加に伴う正常な負荷なのか、ユーザー領域の演算が過剰な状況なのかを解釈するのに役立ちます。 | HP-UX, AIX,
Solaris,
Linux,
Windows |
| cpuSys | CPU System | % | Process Groupに属するプロセスがカーネル/システムモードで使用したCPU使用率を意味します。システムコール、I/O処理、カーネルリソース使用に関連するCPUの割合を解釈するのに役立ちます。値が持続的に高い場合やユーザーモードに対してシステムモードの割合が過度に大きいパターンは、I/O処理の増加、カーネル呼び出しの増加、ロック競合などの影響を確認する際に役立ちます。 | HP-UX, AIX,
Solaris,
Linux,
Windows |

| Field | Title | Unit | Description | OS |
|-------|-------|------|--|-------------------------------------|
| rss | RSS | byte | Process Groupに属するプロセスのRSS (Resident Set Size) の合計です。実際の物理メモリにロードされたメモリのサイズを意味します。この値には共有メモリが含まれる可能性があるため、共有メモリを多く使用するプロセスが多いサーバーの場合、プロセスのRSSの合計は全体のメモリサイズを超えることがあります。現在の占有規模だけでなく、時間に伴う持続的な増加の有無や急激な増減パターンを一緒に見ることで、メモリリークや異常な占有の有無を判断するのに役立ちます。 | HP-UX, AIX, Solaris, Linux |
| pRss | RSS | % | プロセスグループのRSS合計がシステム全体の物理メモリに占める割合を意味します。 $\text{rss} / \text{全体の物理メモリ} * 100$ で計算します。プロセスグループのRSS合計は共有メモリを重複して含む可能性があるため、システム全体の物理メモリに対して100%を超えて見えることがあります。絶対的な使用率だけでなく、長期間にわたる上昇傾向と高点維持の有無を合わせて見ることで、該当プロセスグループのメモリ圧迫の影響度を判断するのに役立ちます。 | HP-UX, AIX, Solaris, Linux |
| vsz | VSZ | byte | Process Groupに属するプロセスが確保した全体の仮想メモリアドレス空間の合計サイズです。実際の物理メモリ使用量ではなく、割り当てられたまたは予約されたアドレス空間のサイズを意味し、ファイルマッピング、共有ライブラリ、スワップ予約などが含まれる可能性があります。したがって、現在の値自体よりも長期的な増加傾向や他の実際のメモリ指標 (RSS/PSS/USS) との違いを一緒に確認することが重要です。 | HP-UX, AIX, Solaris, Linux, Windows |
| pss | PSS | byte | Linuxにおけるプロセスグループに属するプロセスのPSS (Proportional Set Size) の合計です。共有メモリを共有しているプロセスの数で割った比重に基づく物理メモリ使用量で、RSSよりも実際の占有レベルに近いメモリ負担を把握するのに役立ちます。プロセスグループ全体の共有メモリを含む使用傾向と時間に伴う増加傾向を合わせて見ることで、メモリ使用構造の変化を解釈するのに役立ちます。Linuxでは収集コストを考慮して、各PIDの/ | Linux:
smaps_rollup
支援環境 |

| Field | Title | Unit | Description | OS |
|--------|------------------------|----------|--|--------------------------------|
| | | | proc/[pid]/smaps_rollupファイルが提供されている場合にのみ収集・合算します。Agent 2.9.20以降では、RSSが一定サイズ（既定4GiB）を超えるプロセスはPSSの計算過程で対象プロセスに負荷が発生する可能性があるため、エージェントは既定でPSSの収集を省略し、値が空になる場合があります。そのため、複数のプロセスを1つのグループに集計する場合、PSSが収集されなかったプロセスはグループ合計から除外されるため、グループの合計PSSは実際のメモリ使用量より小さく表示される場合があります。しきい値は設定で変更できます。 | |
| uss | USS | byte | Linuxにおけるプロセスグループに属するプロセスのUSS（ユニークセットサイズ）の合計です。各プロセスが単独で使用する非共有物理メモリの使用量の合計であり、プロセスグループ終了時に実際に返却される可能性が高いメモリの規模を把握するのに役立ちます。共有メモリを除いた純粋な占有メモリの増加傾向を観察することで、特定のサービスグループ自体のメモリリークの可能性を判断するのに役立ちます。Linuxでは、収集コストを考慮して、各PIDの/proc/[pid]/smaps_rollupファイルが提供されている場合にのみ収集・合算します。Agent 2.9.20以降では、RSSが一定サイズ（既定4GiB）を超えるプロセスはUSSの計算過程で対象プロセスに負荷が発生する可能性があるため、エージェントは既定でUSSの収集を省略し、値が空になる場合があります。そのため、複数のプロセスを1つのグループに集計する場合、USSが収集されなかったプロセスはグループ合計から除外されるため、グループの合計USSは実際のメモリ使用量より小さく表示される場合があります。しきい値は設定で変更できます。 | Linux:
smaps_rollup
支援環境 |
| minFlt | Page
Minor
Fault | counts/s | Process Groupに属するプロセスの秒当りのminor page fault数の合計です。ページフォールトが発生したが、ディスクI/Oなしでメモリ内部で解決されたフォールトを意味します。値自体も重要ですが、RSSの増加や作業量の増加とともに緩やかに上昇するパターンは、正常なメモリアクセスの拡大を示す可能性があり、突然の急増はアクセスパタ | Linux |

| Field | Title | Unit | Description | OS |
|-------------|------------------|----------|--|-----------------------------|
| | | | ーンの変化やメモリの再利用の増加を示唆することがあります。 | |
| majFlt | Page Major Fault | counts/s | Process Groupに属するプロセスの秒当りのmajor page fault数の合計です。必要なページをディスク/スワップ領域から実際に読み込む必要があったフォールトを意味します。一般的にファイルバックページまたはスワップ領域からの読み込みが含まれます。値が持続的に高いか、増加傾向を示す場合、メモリ圧迫、ページインの増加、応答遅延の可能性を解釈する上で重要な指標となります。 | Linux |
| workingSet | Working Set | byte | Windows専用の指標で、プロセスグループに属するプロセスのワーキングセットの合計です。現在物理メモリに常駐しているメモリのサイズを示します。瞬間的な値も重要ですが、長期間の増加傾向や急激な膨張後の回復状況を併せて見ることで、メモリの圧迫や異常な占有パターンを把握するのに役立ちます。 | Windows |
| private | Private | byte | Windows専用の指標で、プロセスグループに属するプロセスが独占的に使用するプライベートメモリの合計です。共有されない専用メモリの使用量を意味し、プロセス固有のメモリの増加を確認するための指標です。時間とともに持続的に増加し回収されないパターンは、メモリリークの兆候を解釈するのに役立つ可能性があります。 | Windows |
| poolPaged | Pool Paged | byte | Windows専用の指標で、プロセスグループに属するプロセスに関連するページプールメモリ使用量の合計です。必要に応じてディスクにページングされる可能性のあるカーネルメモリ領域を意味します。現在の値だけでなく、長期的な増加傾向や回復状況を合わせて見ることで、カーネルリソースの使用増加や異常な占有パターンを把握するのに役立ちます。 | Windows |
| totalCharlo | Process IO Total | bytes/s | プロセスグループに属するプロセスが1秒間に発生させた全体のキャラクターベースのI/O (char I/O) 処理量の合計です。ディスクだけでなく、パイプ、ターミナル、キャッシュ | HP-UX, AIX, Solaris, Linux, |

| Field | Title | Unit | Description | OS |
|---------|--------------------|---------|---|----------------|
| | | | <p>ユ、一部のバッファベースのI/Oも含まれるため、実際の物理ディスクI/Oとは異なる場合があります。現在の処理量も重要ですが、時間に伴う持続的な増加、急増期間、反復的な作業パターンを合わせて確認することで、該当グループの全体的なI/O活動の特性を解釈するのに役立ちます。</p> | Windows |
| rcharlo | Read Character IO | bytes/s | <p>Process Groupに属するプロセスが1秒あたりに発生させたread char I/O処理量の合計です。ディスクのreadだけでなく、バッファ、キャッシュ、ターミナルなどを通じた読み取り要求も含まれる可能性があります。したがって、瞬間値だけでなく、作業周期に関連する繰り返しパターン、急増時点、CPUおよびDisk I/O指標との関係と一緒に見るのが重要です。</p> | Linux, Windows |
| wcharlo | Write Character IO | bytes/s | <p>Process Groupに属するプロセスが1秒あたりに生成した書き込み文字I/O処理量の合計です。ディスクへの書き込みだけでなく、バッファ、キャッシュ、ターミナルなどを通じた書き込み要求も含まれる可能性があります。値の持続的な増加や繰り返しの急増パターンは、ログ出力の増加、バッファフラッシュ、データ処理作業との関連性を解釈するのに役立ちます。</p> | Linux, Windows |
| rdisklo | Read Disk IO | bytes/s | <p>Linux専用の指標で、プロセスグループに属するプロセスが1秒間にディスクから実際に発生させた読み取りI/O処理量の合計です。ファイルシステムキャッシュで処理された読み取りは除外されるため、rcharloよりも実際のストレージデバイスのreadに近い値となります。したがって、キャッシュヒットが多い環境ではrcharloが高くてもrdiskloは低くなる可能性があり、実際のディスク依存の読み取り負荷を把握するための指標として解釈するのが適切です。</p> | Linux |
| wdisklo | Write Disk IO | bytes/s | <p>Linux専用の指標で、プロセスグループに属するプロセスが1秒間にディスクに実際に発生させた書き込みI/O処理量の合計です。この値はプロセスが発生させた全体の書き込み要求量(wcharlo)とは異なる場合があります、ページキャッシュ/バッファキャッシュおよびwriteback動作の影響により時</p> | Linux |

| Field | Title | Unit | Description | OS |
|-----------|--------------------|-------|---|--|
| | | | 間差を持って反映されることがあります。したがって、実際のストレージに記録される書き込み負荷を確認するための指標として解釈することが適切です。 | |
| threadCnt | Thread | count | 現在のプロセスグループに属する全スレッド数を意味します。グループ内のすべてのプロセスのスレッド数を合算した値です。 | HP-UX, AIX,
Solaris,
Linux,
Windows |
| procCnt | Process | count | 現在、該当するプロセスグループに属する全プロセス数を意味します。同一ユーザーが同一コマンドで実行したプロセスの数として解釈できます。 | HP-UX, AIX,
Solaris,
Linux,
Windows |
| fdCnt | File
Descriptor | count | Linux専用の指標で、プロセスグループに属するプロセスが現在開いているファイル記述子の合計数です。ファイル、ソケット、パイプ、デバイスなどに対するオープンfdが含まれます。 | Linux |
| handleCnt | Handle | count | Windows専用の指標で、プロセスグループに属するプロセスが現在保持しているハンドルの合計数です。ファイル、プロセス、スレッド、イベント、レジストリキーなど、さまざまなカーネルオブジェクトへの参照を含みます。 | Windows |

infra_process_topn

収集時点でサーバーのリソース使用率が高い個別プロセスのみを選別して保存するカテゴリです。基本的には個別プロセスごとの CPU 使用率が 0.1% 以上のプロセスのうち上位 30 個を優先的に収集し、この条件とは別に、CPU 使用率が 0 でも RSS 20MB 以上のプロセスのうち上位 10 個まで追加収集して、最大 40 個程度のプロセスを保存します。ユーザーはこのカテゴリを通じて、実際にどの PID が CPU またはメモリを多く使用しているかを詳細分析の観点から確認できます。つまり、Process Group がリソース使用の大きな流れを見る用途であるのに対し、Process TopN は原因となる個別プロセスを具体的に追跡する用途で使います。

- カテゴリ: ProcessTopN
- デフォルト収集周期: 5秒

| Field | Title | Unit | Description | OS |
|----------|---------------------|--------|--|-------------------------------------|
| cmd | Command | string | プロセスの実行コマンドのみを抽出した値を意味します。cmdlineまたは実行ファイル名を基準にパースして使用します。 | HP-UX, AIX, Solaris, Linux, Windows |
| owner | Owner | string | このプロセスを実行したユーザーアカウントを示す値です。 | HP-UX, AIX, Solaris, Linux, Windows |
| args | Arguments | string | このプロセスの実行引数を示す値です。 | HP-UX, AIX, Solaris, Linux, Windows |
| stime | StartTime | string | このプロセスの開始時刻をエポックタイム基準で示した値です。 | HP-UX, AIX, Solaris, Linux, Windows |
| pid | PID | string | このプロセスのプロセスIDを示す値です。 | HP-UX, AIX, Solaris, Linux, Windows |
| ppid | PPID | string | このプロセスのPPID（Parent Process ID）を示す値です。つまり、このプロセスを生成した親プロセスのPIDです。 | HP-UX, AIX, Solaris, Linux, Windows |
| procInfo | Process Information | string | プロセス識別および表示のために使用される情報フィールドです。owner、pid、ppid、stime、cmd(args)などの組み合わせで構成されています。 | HP-UX, AIX, Solaris, Linux, Windows |
| cpu | CPU | % | このプロセスが使用した全体のCPU使用率を意味しま | HP-UX, AIX, |

| Field | Title | Unit | Description | OS |
|---------|------------|------|--|--|
| | | | す。ユーザーモードとシステムモードの使用率を含む値であり、マルチコア環境では全論理コア数を基準に補正され、最大100%の範囲で表示されます。つまり、システム全体のCPUリソースに対するこのプロセスの使用比率として解釈できます。瞬間的な使用率も重要ですが、持続的な高使用率の維持や周期的な急騰パターンを合わせて見ることで、CPUリソースの占有特性を解釈するのに役立ちます。 | Solaris,
Linux,
Windows |
| cpuUser | CPU User | % | このプロセスがユーザーモードで使用したCPU使用率を意味します。アプリケーションロジックの実行に使用されたCPUの割合を確認するための指標であり、時間に伴う持続的な増加や繰り返しの急増パターンと一緒に確認することで、ユーザー領域の演算負荷特性を把握するのに役立ちます。 | HP-UX, AIX,
Solaris,
Linux,
Windows |
| cpuSys | CPU System | % | このプロセスがカーネル/システムモードで使用したCPU使用率を意味します。システムコール、I/O処理、カーネルリソース使用に関連するCPUの割合を解釈するのに役立ちます。値が持続的に高い場合やユーザーに対するシステムの割合が過度に大きいパターンは、カーネル呼び出し、I/O、ロック競合などの影響を疑う手助けになります。 | HP-UX, AIX,
Solaris,
Linux,
Windows |
| rss | RSS | byte | このプロセスのRSS (Resident Set Size) 値は、現在実際に物理メモリにロードされているメモリのサイズを意味します。この値には共有メモリが含まれるため、共有メモリを多く使用するプロセスが多いサーバーの場合、プロセスのRSSの合計は全体のメモリサイズを超える可能性があります。現在の占有規模を示す代表的な指標であり、時間とともに持続的に増加する場合、メモリリークまたは異常な占有の可能性を判断するのに役立ちます。 | HP-UX, AIX,
Solaris, Linux |
| pRss | RSS | % | 対象プロセスのRSSがシステム全体の物理メモリで占める割合を意味します。絶対値自体よりも長期間にわたる上昇傾向と高値維持の有無を合わせて確認することで、特 | HP-UX, AIX,
Solaris, Linux |

| Field | Title | Unit | Description | OS |
|-------|-------|------|---|--|
| | | | <p>定のプロセスがシステムメモリの圧迫にどれほど影響を与えるかを解釈するのに役立ちます。</p> | |
| VSZ | VSZ | byte | <p>このプロセスが確保した全体の仮想メモリアドレス空間のサイズを意味します。実際の物理メモリ使用量ではなく、マッピングされたり予約された仮想アドレス空間に基づくサイズです。したがって、値自体よりもRSS/PSS/USSとの違いや、長期的な増加傾向を一緒に確認することが重要です。VSZだけが大きく、実際の占有メモリが大きくない場合もあります。</p> | <p>HP-UX, AIX,
Solaris,
Linux,
Windows</p> |
| pss | PSS | byte | <p>このプロセスのPSS（比例セットサイズ）値です。共有メモリを共有しているプロセスの数で割った比率に基づく物理メモリのサイズを意味し、RSSよりも実際の占有レベルに近いメモリ使用量を把握するのに役立ちます。共有ライブラリや共有メモリの使用が多い環境で、プロセスごとのメモリ負担を比較する際に特に有用です。Linuxでは、収集コストを考慮して、/proc/[pid]/smaps_rollupファイルが提供されている環境でのみ収集します。Agent 2.9.20以降では、RSSが一定サイズ（既定4GiB）を超えるプロセスはPSSの計算過程で対象プロセスに負荷が発生する可能性があるため、エージェントは既定でPSSの収集を省略し、値が空になる場合があります。しきい値は設定で変更できます。</p> | <p>Linux:
smaps_rollup
支援環境</p> |
| uss | USS | byte | <p>このプロセスのUSS（Unique Set Size）値です。このプロセスが単独で使用する非共有物理メモリのサイズを意味し、プロセス終了時に実際に返却される可能性が高いメモリの規模を把握するのに役立ちます。共有メモリを除いた純粋な占有メモリを確認するための指標であり、時間とともに持続的に増加し回収されないパターンは、このプロセス自体のメモリリークの可能性を判断するのに特に有用です。Linuxでは、収集コストを考慮して、/proc/[pid]/smaps_rollupファイルが提供されている環境でのみ収集します。Agent 2.9.20以降では、RSSが一定サイズ（既定4GiB）を超えるプロセスはUSSの計算過程で</p> | <p>Linux:
smaps_rollup
支援環境</p> |

| Field | Title | Unit | Description | OS |
|------------|------------------|----------|--|---------|
| | | | 対象プロセスに負荷が発生する可能性があるため、エージェントは既定でUSSの収集を省略し、値が空になる場合があります。しきい値は設定で変更できます。 | |
| minFlt | Page Minor Fault | counts/s | このプロセスの1秒あたりのマイナーページフォルト数を意味します。ページフォルトが発生したが、ディスクI/Oなしでメモリ内部で解決されたフォルトです。値自体も意味がありますが、RSSの増加や作業量の増加とともに緩やかに上昇するパターンは、正常なメモリアクセスの拡大である可能性があり、突然の急増はアクセスパターンの変化やメモリの再利用の増加を示唆することがあります。 | Linux |
| majFlt | Page Major Fault | counts/s | このプロセスの1秒あたりのメジャーページフォルト数を意味します。必要なページをディスク/スワップ領域から実際に読み込む必要があったフォルトを示します。一般的にファイルバックページまたはスワップ領域からの読み込みが含まれる可能性があります。値が持続的に高いか、増加傾向を示す場合、メモリ圧迫、ページインの増加、応答遅延の可能性を解釈する上で重要な指標となります。 | Linux |
| workingSet | Working Set | byte | Windows専用の指標で、現在そのプロセスが物理メモリに常駐して使用中のメモリのサイズを意味します。プロセスの実際のメモリ使用量を確認する代表的な指標として活用されます。現在の値も重要ですが、長時間の増加傾向や急激な膨張後の回復状況を合わせて確認することで、メモリの圧迫や異常な占有パターンを把握するのに役立ちます。 | Windows |
| private | Private | byte | Windows専用の指標であり、該当プロセスが独占的に使用するプライベートメモリのサイズを意味します。他のプロセスと共有しない専用メモリの使用量を示すため、プロセス固有のメモリの増加を確認するための指標です。時間の経過とともに持続的に増加し、回収されないパターンは、メモリリークの兆候を解釈するのに役立つ | Windows |

| Field | Title | Unit | Description | OS |
|-------------|--------------------|---------|---|--|
| | | | 場合があります。 | |
| poolPaged | Pool Paged | byte | Windows専用の指標で、該当プロセスに関連するページプールメモリの使用量を意味します。必要に応じてディスクにページングされる可能性のあるカーネルメモリ領域に関連する使用量です。現在の値だけでなく、長期的な増加傾向や回復状況を併せて確認することで、カーネルリソースの増加や異常なメモリ使用パターンを把握するのに役立ちます。 | Windows |
| totalCharlo | Process IO Total | bytes/s | このプロセスが1秒あたりに発生させる全体のキャラクターベースのI/O（char I/O）スループットを意味します。ディスクだけでなく、パイプ、ターミナル、バッファ、キャッシュ、ファイルシステムレイヤーを通じたI/Oも含まれるため、実際の物理ディスクI/Oとは異なる場合があります。現在のスループットだけでなく、時間に伴う急増期間や持続的な高使用パターンを考慮することで、プロセスのI/O活動の特性を解釈するのに役立ちます。 | HP-UX, AIX,
Solaris,
Linux,
Windows |
| rcharlo | Read Character IO | bytes/s | このプロセスが1秒あたりに発生させる読取り文字I/O処理量を意味します。ディスク読取りだけでなく、バッファ、キャッシュ、ターミナルなどを通じた読み取り要求も含まれる可能性があります。したがって、瞬間値だけでなく、作業サイクルに関連する繰り返しパターンや急増のタイミングを一緒に確認することが重要です。 | Linux,
Windows |
| wcharlo | Write Character IO | bytes/s | このプロセスが1秒間に生成する書き込みキャラクターI/Oのスループットを意味します。ディスクへの書き込みだけでなく、バッファ、キャッシュ、ターミナルなどを介した書き込み要求も含まれる可能性があります。値の持続的な増加や繰り返しの急増パターンは、ログ出力、バッファフラッシュ、データ処理作業との関連性を解釈するのに役立ちます。 | Linux,
Windows |
| rdisklo | Read Disk IO | bytes/s | Linux専用の指標で、該当プロセスが1秒あたりにディスクから実際に発生させた読み取りI/O処理量の合計です。 | Linux |

| Field | Title | Unit | Description | OS |
|-----------|-----------------|---------|---|-------------------------------------|
| | | | ファイルシステムキャッシュで処理された読み取りは除外されるため、rcharloよりも実際のストレージデバイスのreadに近い値です。したがって、キャッシュヒットが多い環境ではrcharloが高くてもrdiskloは低くなる可能性があります、実際のディスク依存の読み取り負荷を把握するための指標として解釈するのが適切です。 | |
| wdisklo | Write Disk IO | bytes/s | Linux専用の指標で、該当プロセスが1秒間にディスクに実際に発生させた書き込みI/O処理量の合計です。この値はプロセスが発生させた全体の書き込み要求量(wcharlo)とは異なる場合があります、ページキャッシュ/バッファキャッシュおよびwriteback動作の影響により時間差を持って反映されることがあります。したがって、実際のストレージに記録される書き込み負荷を確認するための指標として解釈することが適切です。 | Linux |
| threadCnt | Thread | count | このプロセスが現在保持しているスレッド数を意味します。マルチスレッドアプリケーションの同時実行レベルを把握するのに役立ちます。 | HP-UX, AIX, Solaris, Linux, Windows |
| fdCnt | File Descriptor | count | Linux専用の指標で、現在そのプロセスが開いているファイル記述子の数を意味します。ファイル、ソケット、パイプ、デバイスなどに対する開いているFDが含まれます。 | Linux |
| handleCnt | Handle | count | Windows専用の指標であり、現在そのプロセスが保持しているハンドルの数を意味します。ファイル、プロセス、スレッド、イベント、レジストリキーなど、さまざまなカーネルオブジェクトへの参照を含みます。 | Windows |

Kubernetesメタデータフィールド

コンテナランタイムが動作しているLinuxサーバーでは、プロセスが属するPodの情報もあわせて収集します。サーバーでリソースを多く使用しているプロセスを見つけた後、そのプロセスがどのPodのどのコンテナなのかをすぐに確認できます。

| Field | Title | Unit | Description | OS |
|---------------|----------------|--------|---|-------|
| namespace | Namespace | string | プロセスが属するコンテナのKubernetesネームスペース。コンテナのプロセスでない場合は空の値 | Linux |
| podName | Pod Name | string | プロセスが属するPodの名前 | Linux |
| containerName | Container Name | string | プロセスが属するコンテナの名前 | Linux |

3つのフィールドはデフォルトで収集し、`process.topn.k8s.enabled=false` に設定すると収集を中止して3つのフィールドを送信しません。コンテナランタイムがないサーバーでは値が空になります。

サポートするエージェントバージョンは、Linux 2.9.23以上です。

infra_win_service

Windows サービス単位の状態情報を収集するカテゴリです。サービス名、PID、state、status、start mode、exit code などを提供します。Windows サービスの実行状態、起動設定、異常終了の有無を確認するときに使用します。

- カテゴリ: Windows Service
- デフォルト収集周期: 60秒
- 最小サポートエージェント: Windows 2.9.19+

| Field | Title | Unit | Description | OS |
|---------|--------------|--------|---|---------|
| svcName | Service Name | string | Windowsサービスの固有サービス名を示す値です。サービス管理ツール(services.msc)の内部識別子またはシステムサービス名に対応し、表示名(Display Name)とは異なる場合があります。 | Windows |
| pid | PID | string | 現在実行中のサービスのプロセスID (PID) を示す値です。サービスが実行されていない場合は、空または0として表示されることがあります。svchost.exeのように、1つのプロセスで複数のサービスが同時に動作する場合、同じPIDを共有することがあります。 | Windows |
| state | State | string | サービス制御マネージャー(SCM)基準の現在のサービス状態を示す値です。例えば、Running、Stopped、Start Pending、Stop Pending、 | Windows |

| Field | Title | Unit | Description | OS |
|-----------|------------|--------|--|---------|
| | | | Paused、Pause Pending、Continue Pendingなどの状態が表示されることがあります。 | |
| startMode | Start Mode | string | このサービスがシステムの起動またはサービスの開始時にどのように開始されるかを示す値です。表示されるのは、Automatic、Manual、Disabledであり、環境によってはAutomatic (Delayed Start)が区別されて表示されることがあります。 | Windows |
| exitCode | Exit Code | string | サービスが最後に終了したり、開始/停止作業を行う過程で返された終了コードを示す値です。一般的に0は正常終了またはエラーなしと解釈され、0以外の値はサービスの開始失敗、実行エラー、異常終了などの原因を追跡する際の参考になります。 | Windows |

infra_nic_perf

個別 NIC 単位のパフォーマンス指標を収集するカテゴリです。インターフェースごとの送受信帯域幅、パケット数、error、drop、collisionなどを提供します。特定 NIC のボトルネック、packet loss、割り込み/エラーの偏りの有無を確認するときに使用します。

- カテゴリ: by NIC
- デフォルト収集周期: 5秒

| Field | Title | Unit | Description | OS |
|----------|-----------|--------|---|---|
| name | NIC Name | string | ネットワークインターフェースの名前を示す値です。例えば、Linuxのeth0、ens192、bond0、Windowsのアダプタ名などが表示されます。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| totalbps | NIC Total | bps | 該当NICを通じて1秒あたりに送信(Tx)および受信(Rx)された全データ転送量の合計をbps (bit per second) 単位で示した値です。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |

| Field | Title | Unit | Description | OS |
|-----------|---------------|----------|---|---|
| rxbps | NIC RX | bps | 指定されたNICを介して、1秒あたりに受信(Rx)されたデータ転送量をbps (bit per second) 単位で示した値です。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| txbps | NIC Tx | bps | 該当NICを通じて1秒あたりに送信(Tx)されたデータ転送量をbps (bit per second) 単位で示した値です。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| totalpps | NIC Total PPS | counts/s | 該当NICを通じて1秒あたりに受信(Rx)および送信(Tx)された全パケット数の合計をpps (packets per second) またはcount/s単位で示した値です。rxpps + txppsに該当します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| rxpps | NIC Rx PPS | counts/s | 該当NICを通じて1秒あたりに受信(Rx)されたパケット数をpps(packets per second)またはcount/s単位で示した値です。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| txpps | NIC Tx PPS | counts/s | 該当NICを通じて秒あたりに送信されたパケット数をpps (packets per second) またはcount/s単位で示した値です。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| collision | NIC Collision | counts/s | 該当NICの送信(Tx)過程で検出されたパケット衝突数を1秒あたりの平均変化率(rate)に換算した値です。主にハーフデュプレックスEthernet環境で意味があり、モダンなフルデュプレックス環境では一般的に0に近いのが正常です。 | HP-UX,
AIX,
Solaris,
Linux |
| errln | NIC Error | counts/s | 該当NICを通じて受信(Rx)されたパケットのうち、エラーが発生 | HP-UX, |

| Field | Title | Unit | Description | OS |
|-----------|-----------------|----------|--|---|
| | In | | したパケット数を1秒あたりの平均変化率(rate)に換算した値です。CRCエラー、フレームエラー、オーバーランなどの受信エラーを含む可能性があり、含まれる範囲はOS/ドライバによって異なる場合があります。 | AIX,
Solaris,
Linux,
Windows |
| errOut | NIC Error Out | counts/s | 該当NICを通じて送信(Tx)されたパケットのうち、エラーが発生したパケット数を1秒あたりの平均変化率(rate)に換算した値です。carrierエラー、abort、transmit queue問題など送信エラーを含む可能性があり、含まれる範囲はOS/ドライバによって異なる場合があります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| dropIn | NIC Drop In | counts/s | このNICを通じて受信(Rx)されたパケットのうち、カーネルまたはNIC層で処理されずにドロップされたパケット数を1秒あたりの平均変化率(rate)に換算した値です。バッファ不足、キューオーバーフロー、ドライバ処理遅延などにより増加する可能性があります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| dropOut | NIC Drop Out | counts/s | このNICを介して送信(Tx)されたパケットのうち、実際に送信される前にドロップされたパケット数を1秒あたりの平均変化率(rate)に換算した値です。送信キューのオーバーフロー、ドライバの問題、インターフェースの状態異常などにより増加する可能性があります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| linkSpeed | NIC Link Speed | bps | 該当NICのリンク速度をMbps単位で示した値です。実際の使用量ではなく、現在交渉または設定されたインターフェースの転送帯域幅の容量を意味します。ただし、OS/ドライバ/仮想インターフェースの種類によってはリンク速度を確認できない場合があります、その場合はunknownまたはnullとして収集されることがあり、この場合値が出力されないことがあります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| linkUsage | NIC Utilization | % | このNICの全送受信処理量(NIC Total)をリンク速度(NIC Link Speed)に対する割合として表した値です。NICの利用可能なリンク帯域幅に対する実際のトラフィック使用レベルを示しており、値が高いほどリンクが活発に使用されていることを意味します。ただし、リンク速度(NIC Link Speed)がunknownまたはnullの場合、使用率を計算できないため、値が出力されないことがあります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |

| Field | Title | Unit | Description | OS |
|-------|-------|------|-------------|----|
| | | | す。 | |

infra_infiniband

InfiniBand または HCA ポート単位の状態およびパフォーマンス指標を収集するカテゴリです。ポート状態、リンク層、速度、LID、送受信処理量、パケット数、symbol error、link recovery、constraint error などを提供します。IB fabric の接続状態とリンク品質、ポートごとのボトルネック/エラーを確認するときに使用します。

- カテゴリ: by Infiniband
- デフォルト収集周期: 5秒

| Field | Title | Unit | Description | OS |
|---------------|----------------|--------|---|-------|
| interfaceName | Interface Name | string | HCAデバイス名とポート番号を組み合わせた識別値です。例えば、mlx5_0:1はmlx5_0デバイスの1番ポートを意味します。 | Linux |
| linkLayer | Link Layer | string | ポートのリンク層タイプを示します。InfiniBandまたはEthernetが表示され、ポートがどのリンクモードで動作しているかを確認するために使用されます。 | Linux |
| state | State | string | ポートの論理状態を示します。例えば、Down、Init、Activeなどが表示され、ポートがIBファブリックに正常に参加しているかどうかを判断する基準となります。 | Linux |
| physState | Physical State | string | ポートの物理リンク状態を示します。例えば、ポーリング、リンクアップ、無効などが表示され、ケーブル接続および物理層の交渉状態を判断する際に使用されます。 | Linux |
| rate | Link Speed | string | ポートの現在のリンク速度を示します。例えば、100Gb/s、200Gb/sなどが表示され、リンク交渉の結果やポートの最大動作速度を確認する | Linux |

| Field | Title | Unit | Description | OS |
|---------------------|---------------------------|----------|---|-------|
| | | | ために使用されます。 | |
| lid | Local Identifier | string | InfiniBand環境における該当ポートに割り当てられたLID（ローカル識別子）を示します。IBファブリック内でポートの論理アドレスとして機能し、Ethernetモードでは意味がないか、空である可能性があります。 | Linux |
| portXmitData | Transmit Data | bytes/s | 指定されたポートで毎秒送信(Tx)されたデータの処理量をBytes/s単位で示した値です。ポート基準の送信使用量を意味します。 | Linux |
| portRcvData | Receive Data | bytes/s | 該当ポートで毎秒受信(Rx)されたデータ処理量をBytes/s単位で示した値です。ポート基準の受信使用量を意味します。 | Linux |
| portXmitPackets | Transmit Packets | counts/s | 該当ポートで1秒あたりに送信された全パケット数を示す値です。パケットサイズに関係ないpacket rate指標です。 | Linux |
| portRcvPackets | Receive Packets | counts/s | 指定されたポートで1秒あたりに受信された全パケット数を示す値です。パケットサイズに関係ないパケットレート指標です。 | Linux |
| unicastRcvPackets | Unicast Receive Packets | counts/s | 該当ポートで1秒あたりに受信されたユニキャストパケット数を示す値です。単一の対象との一般的なトラフィックフローを確認する際に役立ちます。 | Linux |
| unicastXmitPackets | Unicast Transmit Packets | counts/s | 該当ポートで毎秒転送されたユニキャストパケット数を示す値です。 | Linux |
| multicastRcvPackets | Multicast Receive Packets | counts/s | 指定されたポートで受信したマルチキャストパケットの数を示す値です。マルチキャストベースの通信やIBファブリック制御トラフィックの | Linux |

| Field | Title | Unit | Description | OS |
|-----------------------------|----------------------------|----------|--|-------|
| | | | 影響分析時に参考にできます。 | |
| multicastXmitPackets | Multicast Transmit Packets | counts/s | 該当ポートで1秒あたりに転送されたマルチキャストパケット数を示す値です。 | Linux |
| symbolError | Symbol Errors | counts/s | 物理リンク層で発生したシンボルエラーの1秒あたりの変化率を示す値です。一般的にビットエラー、ケーブル品質の問題、光モジュール/ポートの不安定などの信号である可能性があります。 | Linux |
| portRcvErrors | Port Receive Errors | counts/s | 該当ポートが受信過程で記録した全エラーカウンターの1秒あたりの変化率を示す値です。受信フレーム異常、整合性問題、プロトコルエラーなどが含まれる可能性があります。 | Linux |
| portRcvRemotePhysicalErrors | Remote Physical Errors | counts/s | 相手側ポートで発生した物理層の問題により、このポートが受信したエラーカウンターの1秒あたりの変化率を示す値です。リモートポートまたはリンクの反対側のケーブル/モジュールの状態異常が疑われます。 | Linux |
| portRcvSwitchRelayErrors | Switch Relay Errors | counts/s | スイッチがパケットを正しく中継できなかった場合に記録されるエラーカウンターの1秒あたりの変化率を示す値です。スイッチの伝送経路の問題やファブリックの異常を示唆する可能性があります。 | Linux |
| linkErrorRecovery | Link Error Recovery | counts/s | リンクエラー回復(link error recovery)イベントの1秒あたりの変化率を示す値です。リンクの再初期化またはエラー回復が頻繁に発生している可能性があります。値が持続的に増加する場合は、リンクの不安定性が疑われます。 | Linux |
| portXmitConstraintErrors | Transmit | counts/s | 送信側制約条件違反によって記録されたエラー | Linux |

| Field | Title | Unit | Description | OS |
|------------------------------|-----------------------------|----------|--|-------|
| | Constraint Errors | | の秒間変化率を示す値です。例えば、SL、VL、QoS、パーティションキーなどのファブリックポリシーの不一致が原因となることがあります。 | |
| portRcvConstraintErrors | Receive Constraint Errors | counts/s | 受信側の制約条件違反として記録されたエラーの秒間変化率を示す値です。送信側と受信側のファブリックポリシー、パーティション、QoSの不一致がある場合に増加する可能性があります。 | Linux |
| localLinkIntegrityErrors | Local Link Integrity Errors | counts/s | ローカルポート基準のリンク整合性エラーの秒間変化率を示す値です。CRC/ビットエラー、信号品質の低下、ケーブルまたはポートハードウェアの異常に関連する可能性があります。 | Linux |
| excessiveBufferOverrunErrors | Buffer Overrun Errors | counts/s | 受信バッファオーバーランによって正常に処理できなかったエラーの秒間変化率を示す値です。ポート処理能力に対してバーストラフィックが大きい場合や、システム/ドライバ/ファームウェアの処理遅延がある場合に増加する可能性があります。 | Linux |
| linkDowned | Link Down Events | counts/s | リンクがダウン状態に切り替わったイベントの1秒あたりの変化率を示す値です。ケーブルの脱着、相対ポートの無効化、リンクの不安定、機器の再起動などの状況で増加する可能性があります。 | Linux |
| portXmitDiscards | Transmit Discards | counts/s | 送信キューで実際に送信される前に破棄されたパケット数の1秒あたりの変化率を示す値です。バッファ不足、混雑、キュー制約、ポート状態異常などが原因となる可能性があります。 | Linux |
| vl15Dropped | VL15 Dropped | counts/s | VL15(サブネット管理専用バーチャルレーン)キューで破棄されたパケット数の1秒あたりの変化 | Linux |

| Field | Title | Unit | Description | OS |
|----------------------------|-----------------|--------|--|-------|
| | Packets | | 率を示す値です。サブネットマネージャー関連の制御トラフィックの混雑やファブリック管理経路の異常を示唆する可能性があります。 | |
| Field | Title | Unit | Description | OS |
| --- | --- | :--- | --- | --- |
| <code>rdmaNetDevice</code> | RDMA Net Device | string | そのRDMAデバイス・ポートに接続されたオペレーティングシステムのネットワークインターフェイス名。複数ある場合は で区切ります（例： <code>ib0</code> 、 <code>enp175s0f0</code> ）。マッピング情報がない場合は空の値 | Linux |

RDMAポートとオペレーティングシステムのネットワークインターフェイスを結び付けて確認できるため、InfiniBandポートのエラー指標と、そのインターフェイスのトラフィック指標をあわせて確認する際に使用します。純粋なInfiniBandポートのようにポート単位のマッピングを提供しない場合は、デバイス単位のマッピングを代わりに表示します。

サポートするエージェントバージョンは、Linux 2.9.23以上です。

infra_disk_perf

個別物理ディスク単位のパフォーマンス指標を収集するカテゴリです。ディスクごとの処理量、IOPS、busy、service time、wait time など詳細な I/O パフォーマンスを提供します。特定ディスクのボトルネック、遅延、queue の増加を確認するときに使用します。

- カテゴリ: by Disk
- デフォルト収集周期: 5秒

| Field | Title | Unit | Description | OS |
|-------------------|-----------|--------|--------------------|----------------------------|
| <code>name</code> | Disk Name | string | 物理ディスクの名前を表示した値です。 | HP-UX,
AIX,
Solaris, |

| Field | Title | Unit | Description | OS |
|-----------|-----------------------|----------|--|---|
| | | | | Linux,
Windows |
| busy | Disk
Busy | % | この物理ディスクが観測期間中に忙しく動作していた時間の割合を示す値です。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| total | Disk IO
Total | bytes/s | 物理ディスクの毎秒の総処理量を示す値です。読み取りと書き込みのバイト処理量を合算した値です。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| read | Disk
Read | bytes/s | 対象の物理ディスクの1秒あたりの読み取りスループットを示す値です。Bytes/sec基準で解釈します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| write | Disk
Write | bytes/s | 物理ディスクの毎秒書き込みスループットを示す値です。Bytes/sec基準で解釈します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| totallops | Disk
Total
IOPS | counts/s | 物理ディスクの秒あたりの総I/O操作数を示す値です。読み取りIOPSと書き込みIOPSを合算した値です。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| readlops | Disk
Read
IOPS | counts/s | 物理ディスクの1秒あたりの読み取りI/O操作数を示す値です。 | HP-UX,
AIX,
Solaris, |

| Field | Title | Unit | Description | OS |
|--------------|---------------------------|----------|--|---|
| | | | | Linux,
Windows |
| writelops | Disk Write IOPS | counts/s | 物理ディスクの秒あたりの書き込みI/O操作数を示す値です。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| readSvcTime | Disk Read Service Time | ms/io | この物理ディスクが1つのRead IOリクエストを処理するのにかった時間をミリ秒単位で示した値です。 | AIX,
Solaris,
Linux,
Windows |
| writeSvcTime | Disk Write Service Time | ms/io | この物理ディスクが1つのWrite IOリクエストを処理するのにかった時間をミリ秒単位で示した値です。 | AIX,
Solaris,
Linux,
Windows |
| avgWaitTime | Disk Average Wait Time | ms | HP-UX専用の指標で、IO処理要求がディスクのキューでアイドル状態で待機していた平均時間をミリ秒単位で示した値です。 | HP-UX |
| avgSvcTime | Disk Average Service Time | ms | HP-UX専用の指標で、ディスクに対する各転送要求（探索、回転待機時間、データ転送時間を含む）を処理する平均時間をミリ秒単位で示した値です。 | HP-UX |
| qLength | Disk Q-Length | count | 対象ディスクに対して待機中または処理中のI/Oリクエストのキュー長を示す指標です。値が低い場合はリクエストがスムーズに処理されていることを意味し、値が高く持続する場合はディスクがリクエストを適時に処理できていない可能性を示唆します。ただし、絶対的な基準値はディスクの種類（HDD/SSD/NVMe）、システムアーキテクチャ、ワークロードの特性によって異なるため、busy（%）、待機時間、サービス時間と合わせ | Linux,
Windows |

| Field | Title | Unit | Description | OS |
|-------|-------|------|-------------------|----|
| | | | で総合的に解釈する必要があります。 | |

infra_filesystem

ファイルシステムまたはマウントポイント単位の容量およびパフォーマンス情報を収集するカテゴリです。総容量、使用量、空き容量、使用率、inode 使用率、読み取り/書き込み処理量、IOPS、queue length などを提供します。特定ファイルシステムの空間不足、inode 枯渇、I/O 負荷を確認するときに使用します。

- カテゴリ: by Filesystem
- デフォルト収集周期: 5秒

| Field | Title | Unit | Description | OS |
|-----------|--------------------|--------|---|---|
| mountName | Mount Name | string | ファイルシステムがマウントされたパスまたは識別名を示す値です。例えば、Linux/Unixでは /、/var、/data のようなマウントポイントが、Windowsではドライブ文字やボリュームパスが表示されることがあります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| fsType | FileSystem Type | string | ファイルシステムのタイプを示す値です。例えば、ext4、xfs、zfs、vxfs、ntfsなどが表示される可能性があります。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| devName | Device Name | string | 該当ファイルシステムが実際に接続されているデバイス名またはデバイス識別パスを示す値です。LinuxではlsblkのKNAME、Unix系ではdfまたはbdfの結果のFILESYSTEM列の値に基づいて表示されます。Windowsではドライブ文字ではなく、該当ファイルシステムが接続されているデバイス識別パスに基づいて表示されます。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| pDevName | Parent Device Name | string | このデバイスが属する親デバイスの名前を示す値です。LinuxではlsblkのPKNAME値に基づいて表示され、パーティションまたは論理デバイスがどの上位ディスク階層に接続されている | Linux |

| Field | Title | Unit | Description | OS |
|-----------|---------------|------|---|---|
| | | | かを特定するのに利用できます。例えば、nvme0n1p1の場合はnvme0n1、sda1の場合はsdaのように表示されることがあります。Unix系およびWindowsでは、LinuxのPKNAMEと同様の情報を共通の方法で安定して提供することが難しいため、空であったり収集対象から除外されることがあります。 | |
| totalSize | FS Total Size | GiB | 対象ファイルシステムの全容量をバイト単位で示した値です。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| used | FS Used | GiB | このファイルシステムで現在使用中の容量をバイト単位で示した値です。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| free | FS Free | GiB | 該当ファイルシステムで現在使用可能な残りの容量をバイト単位で示した値です。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| pUsed | FS Used | % | ファイルシステムの全体容量に対する使用中の容量の割合を示す値です。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| pFree | FS Free | % | ファイルシステムの全体容量に対する使用可能な残り容量の割合を示す値です。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |

| Field | Title | Unit | Description | OS |
|------------|----------------|----------|---|--|
| pInodeUsed | FS i-node Used | % | このファイルシステムの全体のinode数に対する使用中のinodeの割合を示す値です。ファイル数が非常に多い場合、容量が残っていてもinodeが枯渇してファイルを作成できない可能性があるため、併せて確認する必要があります。 | HP-UX,
AIX,
Solaris,
Linux |
| read | FS Read | bytes/s | このファイルシステムで1秒あたりに読み取られたデータのスループットをByte/s単位で示した値です。つまり、ファイルシステム基準の読み取りスループットです。 | HHP-UX,
AIX,
Solaris,
Linux,
Windows |
| write | FS Write | bytes/s | 対象のファイルシステムで1秒あたりに記録されたデータ処理量をByte/s単位で示した値です。つまり、ファイルシステム基準の書き込みスループットです。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| ioTotal | FS IO Total | bytes/s | このファイルシステムで毎秒処理された全データのスループットをバイト/秒単位で示した値です。読み取りと書き込みのデータスループットを合算した値であり、ファイルシステム基準の総I/Oスループットを意味します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| readIops | FS Read IOPS | counts/s | このファイルシステムで1秒あたりに処理された読取りI/O作業の数を示す値です。ファイルシステム基準の読取りIOPSとして解釈します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| writeIops | FS Write IOPS | counts/s | このファイルシステムで1秒あたりに処理された書き込みI/O作業の数を示す値です。ファイルシステム基準の書き込みIOPSとして解釈します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| IopsTotal | FS Total | counts/s | このファイルシステムで1秒あたりに処理された全体のI/O作 | HP-UX, |

| Field | Title | Unit | Description | OS |
|-----------|---------------|----------|--|---|
| | IOPS | | 業数を示す値です。読み取りIOPSと書き込みIOPSを合算した値であり、ファイルシステム基準の総IOPSを意味します。 | AIX,
Solaris,
Linux,
Windows |
| iopsTotal | FS Total IOPS | counts/s | このファイルシステムで1秒あたりに処理された全体のI/O作業数を示す値です。読み取りIOPSと書き込みIOPSを合算した値で、ファイルシステム基準の総IOPSを意味します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| qLength | FS Q-Length | count | この指標は、関連するファイルシステムのI/O処理要求のキュー長レベルを示しています。待機中または処理中の要求の平均的な累積レベルとして解釈できます。値が一時的に上昇することは瞬間的な負荷の増加として正常である可能性があります。高い状態が持続する場合はファイルシステムまたは下位ストレージの処理遅延の可能性を示唆します。ただし、絶対的な基準値はファイルシステムの種類、ストレージ構造、ワークロードの特性によって異なる可能性があるため、read/write処理量、IOPS、応答時間の系列指標とともに総合的に解釈する必要があります。 | Linux,
Windows |

infra_zpool_perf

ZFS zpool および vdev 単位のパフォーマンス/状態情報を収集するカテゴリです。zpool 容量、読み取り/書き込み処理量、IOPS、queue および disk wait 系列の指標、scrub/trim/rebuild 関連の待機時間を提供します。ZFS ストレージプールの全体状態と、特定の vdev または device のボトルネック区間を確認するときに使用します。

- カテゴリ: by ZFS
- デフォルト収集周期: 5秒
- 最小サポートエージェント: Linux 2.9.15+, Solaris 1.4.9+

| Field | Title | Unit | Description | OS |
|-----------|--------------------|---------|---|----------------|
| name | Zpool Display Name | string | 表示用デバイス名です。pool名とデバイス名を組み合わせた識別値で、画面上でzpoolまたはvdevを区別するための表示名として使用されます。 | Linux, Solaris |
| poolName | Zpool Name | string | 該当デバイスが属するZFSプールの名前を示す値です。同一プール内の複数のvdevまたはリーフデバイスをグループ化して解釈する際に使用します。 | Linux, Solaris |
| devName | Zpool Device Name | string | 実際のvdevまたはleafデバイスの元の名前を示す値です。パフォーマンスボトルネックが発生したデバイスを特定する際に使用します。 | Linux, Solaris |
| devType | Zpool Device Type | string | ZFSデバイスタイプを示す値です。例えば、zpool、data、special、log、cache、spareなどのタイプで表示され、デバイスの役割の区別に使用されます。 | Linux, Solaris |
| totalSize | Total Size | byte | 対象のzpoolまたはデバイスの全体サイズ（割り当て済み+空き）をバイト単位で示した値です。 | Linux, Solaris |
| allocated | Allocated | byte | 該当のzpoolまたはデバイスに現在割り当てられている容量をバイト単位で示した値です。論理的に既に割り当てられたスペースの規模を把握する際に使用します。 | Linux, Solaris |
| free | Free | byte | 該当するzpoolまたはデバイスで現在利用可能な残りの容量をバイト単位で示した値です。利用可能なスペースが不足しているかどうかを確認する際に使用します。 | Linux, Solaris |
| pctUsed | Used | % | 指定されたzpoolまたはデバイスの全体容量に対する使用中の容量の割合をパーセンテージ(%)で示した値です。値が高いほど、空き容量が少ない状態を意味します。 | Linux, Solaris |
| readBytes | Read | bytes/s | 指定されたzpoolまたはデバイスの毎秒読み取りデータ処理量をbytes/s単位で示した値です。ZFS基準の読み取りスループット指標を意味します。 | Linux, Solaris |

| Field | Title | Unit | Description | OS |
|--------------------|-------------------|----------|---|-------------------|
| writeBytes | Write | bytes/s | 指定されたzpoolまたはデバイスの1秒あたりの書き込みデータ処理量をbytes/s単位で示した値です。ZFS基準の書き込みスループット指標を意味します。 | Linux,
Solaris |
| totalBytes | Read+Write | bytes/s | 対象のzpoolまたはデバイスの毎秒の全データ処理量をbytes/s単位で示した値です。読み取りスループットと書き込みスループットを合算した総スループット指標です。 | Linux,
Solaris |
| readOperation | Read IOPS | counts/s | 該当するzpoolまたはデバイスで1秒あたりに処理された読み取りI/Oタスクの数を示す値です。ZFS基準の読み取りIOPSを意味します。 | Linux,
Solaris |
| writeOperation | Write IOPS | counts/s | この値は、指定されたzpoolまたはデバイスで1秒あたりに処理された書き込みI/O操作の数を示します。ZFS基準の書き込みIOPSを意味します。 | Linux,
Solaris |
| totalOperation | Read+Write IOPS | counts/s | 指定されたzpoolまたはデバイスで毎秒処理された全体のI/O操作数を示す値です。読み取りIOPSと書き込みIOPSを合算した総IOPS指標です。 | Linux,
Solaris |
| asyncqReadWait_ns | Asyncq Read Wait | ns | ZFS内部の非同期キューで待機している読み取りI/Oリクエストの平均時間をナノ秒単位で示した値です。値が高いほど、非同期読み取りリクエストがキューで遅延していることを示唆します。 | Linux |
| asyncqWriteWait_ns | Asyncq Write Wait | ns | ZFS内部の非同期キューで待機している書き込みI/Oリクエストの平均待機時間をナノ秒単位で示した値です。値が高いほど、非同期書き込みリクエストがキューで遅延していることを示唆します。 | Linux |
| totalAsyncqWait_ns | Asyncq Total Wait | ns | ZFS内部の非同期キューで待機している読み書きI/Oリクエストの全体的な平均時間をナノ秒単位で示した値です。非同期キューのボトルネックレベルを総合的に確認する際に使用します。 | Linux |

| Field | Title | Unit | Description | OS |
|--------------------------------|---------------------|------|---|-------|
| <code>syncqReadWait_ns</code> | Syncq
Read Wait | ns | ZFS内部の同期キューで待機している読み取りI/Oリクエストの平均時間をナノ秒単位で示した値です。同期読み取りリクエストの処理遅延レベルを把握する際に使用します。 | Linux |
| <code>syncqWriteWait_ns</code> | Syncq
Write Wait | ns | ZFS内部の同期キューで待機している書き込みI/Oリクエストの平均時間をナノ秒単位で示した値です。同期書き込みリクエストの処理遅延レベルを把握する際に使用します。 | Linux |
| <code>totalSyncqWait_ns</code> | Syncq
Total Wait | ns | ZFS内部の同期キューで待機している読み書きI/Oリクエストの全体平均時間をナノ秒単位で示した値です。sync queueのボトルネックを総合的に確認する際に使用します。 | Linux |
| <code>diskReadWait_ns</code> | Disk Read
Wait | ns | 読み取りI/Oリクエストが実際のディスク層で処理されるのにかかる平均時間をns単位で示した値です。キュー待機後の実際のデバイス処理遅延レベルを把握する際に使用します。 | Linux |
| <code>diskWriteWait_ns</code> | Disk Write
Wait | ns | 書き込みI/Oリクエストが実際のディスク階層で処理されるのに要した平均時間をナノ秒単位で示した値です。キュー待機後の実際のデバイス処理遅延レベルを把握する際に使用します。 | Linux |
| <code>totalDiskWait_ns</code> | Disk Total
Wait | ns | 読み書きI/Oリクエストが実際のディスク階層で処理される全体の平均時間をナノ秒単位で示した値です。デバイス自体の処理遅延レベルを総合的に確認する際に使用します。 | Linux |
| <code>totalReadWait_ns</code> | Total Read
Wait | ns | 読み取りI/Oリクエストの全体的な平均遅延時間をナノ秒単位で示した値です。ZFS内部のキュー待機時間と実際のディスク処理時間の両方が含まれています。 | Linux |
| <code>totalWriteWait_ns</code> | Total Write
Wait | ns | 書き込みI/Oリクエストの全体平均遅延時間をナノ秒単位で示した値です。ZFS内部のキュー待機時間と実際の | Linux |

| Field | Title | Unit | Description | OS |
|--------------|------------|------|---|-------|
| | | | ディスク処理時間がすべて含まれています。 | |
| totalWait_ns | Total Wait | ns | 全ての読み書きI/Oリクエストの平均遅延時間をナノ秒単位で示した値です。キュー待機と実際のディスク処理時間を含む統合待機指標です。値が高いほど、該当するzpoolまたはデバイスのI/O遅延の可能性を示唆します。 | Linux |
| scrub_ns | Scrub | ns | ZFS内部キューで待機しているscrub作業の平均時間をナノ秒単位で示した値です。scrubはプール内のブロックを順次読み取り、チェックサムを検証し、データの異常を確認する作業です。 | Linux |
| trim_ns | Trim | ns | trim作業がZFS内部キューで待機した平均時間をナノ秒単位で示した値です。trimはSSDまたはthin provisioningデバイスに使用しないブロックを返す作業です。 | Linux |
| rebuild_ns | Rebuild | ns | ZFS内部キューで待機している再構築作業の平均時間をナノ秒単位で示した値です。デバイスの交換や復旧プロセスに必要なデータを再構成する作業の遅延レベルを示します。 | Linux |

infra_vxlv_perf

Veritas Volume Manager 環境で Logical Volume (vxlv) 単位の I/O パフォーマンス情報を収集したデータです。ディスクグループおよびボリュームごとに読み取り/書き込み IOPS、処理量、平均レイテンシなどの指標を提供し、ボリューム単位のパフォーマンス推移、ボトルネックの有無、読み取り/書き込みの偏り現象などを分析するのに活用します。

- カテゴリ: by VxLV
- デフォルト収集周期: 5秒
- 最小サポートエージェント: Linux 2.9.15+

| Field | Title | Unit | Description | OS |
|------------|-------------------|----------|--|-------|
| name | VxLV Display Name | string | 表示装置の名前です。Disk Group名とVxLvol名を組み合わせた識別値として使用されることがあります。 | Linux |
| diskGroup | VxLV Disk Group | string | このボリュームが属するVeritasディスクグループの名前です。複数のボリュームを論理的にまとめる管理単位であり、同じディスクグループ内のボリュームを一緒に識別または集計する際に使用されます。 | Linux |
| vxLvolName | VxLV Lvol Name | string | Veritas Volume Managerで管理されている論理ボリュームの名前です。パフォーマンス指標の測定対象となるボリューム識別子です。 | Linux |
| blockSize | VxLV Block Size | string | このボリュームのI/Oブロックサイズを示す値です。バイト単位で表現され、ブロック数ベースの指標をバイト単位のスループットに換算する際に使用します。vxprint -F %iosizeの取得値を基準とし、取得に失敗した場合や異常な値の場合は512バイトにフォールバックされます。 | Linux |
| readIops | Read IOPS | counts/s | 収集期間中に発生した読み取り操作の数を期間の時間で割った1秒あたりの平均読み取り作業数です。ボリュームの読み取り要求処理頻度を示します。 | Linux |
| writeIops | Write IOPS | counts/s | 収集期間中に発生した書き込み操作の数を期間の時間で割った1秒あたりの平均書き込み作業数です。ボリュームの書き込み要求処理頻度を示します。 | Linux |
| IopsTotal | Total IOPS | counts/s | 収集期間中に発生した全体のI/O操作数を期間の時間で割った1秒あたりの平均作業数です。読取りIOPSと書き込みIOPSの合計として解釈します。 | Linux |
| read | Read | bytes/s | 収集期間中に処理された読み取りブロック数にI/Oブロックサイズを掛け、その後、期間の時間で割った1秒あたりの平均読み取りスループットです。単位はbytes/sです。 | Linux |
| write | Write | bytes/s | 収集期間中に処理された書き込みブロック数にI/Oブロックサイズを掛け、その後、期間の時間で割った1秒あたりの平均書き込みスループットです。単位はbytes/sです。 | Linux |

| Field | Title | Unit | Description | OS |
|------------|-----------------------|---------|--|-------|
| | | | プットです。単位はbytes/sです。 | |
| total | IO Total | bytes/s | 収集期間中に処理された全体のI/Oデータ量を期間の時間で割った1秒あたりの平均処理量です。読み取り処理量と書き込み処理量の合計を意味します。 | Linux |
| readAvgMs | Read Average Latency | ms | 収集期間中に発生した読み取り作業の平均遅延時間です。各読み取りリクエストが完了するまでにかかった時間の平均値で、単位はミリ秒(ms)です。 | Linux |
| writeAvgMs | Write Average Latency | ms | 収集期間中に発生した書き込み作業の平均遅延時間です。各書き込みリクエストが完了するまでにかかった時間の平均値で、単位はミリ秒(ms)です。 | Linux |

infra_cpu_core

CPU 論理コアごとの使用状態を収集するカテゴリです。coreId 基準で user、sys、wait、idle、irq、softirq、steal、core CPU 使用率などを提供します。特定コアの偏り、IRQ の偏重、シングルスレッドのボトルネックを確認するときに使用します。

- カテゴリ: by CPU Core
- デフォルト収集周期: 5秒

| Field | Title | Unit | Description | OS |
|---------|---------|--------|--|-------------------------------------|
| coreId | Core ID | string | CPUコアを識別するためのID値です。OSが認識する論理コア番号を意味し、物理コアと1:1で対応しない場合があります。Hyper-Threading/SMTが有効な場合、1つの物理コアに複数の論理コアがマッピングされることがあります。 | HP-UX, AIX, Solaris, Linux, Windows |
| coreCpu | CPU | % | 該当Coreの全CPU使用率を意味します。100 - idleで計算され、ユーザーモード(user)、カーネルモード(sys)、nice、I/O待機(wait)、irq、softirq、stealなどの非アイドル時間をすべて含んだ使用割合として解釈されます。オペレーティングシステムに | HP-UX, AIX, Solaris, Linux, |

| Field | Title | Unit | Description | OS |
|------------|---------------|------|--|---|
| | | | よって含まれる項目は異なる場合があります。 | Windows |
| user | User | % | 対象のCoreの全CPU時間のうち、ユーザーモードで一般的なアプリケーション/プロセスを実行するために使用された割合を意味します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| sys | Sys | % | 該当Coreの全CPU時間のうち、カーネルモード（システムモード）でのシステムコール処理、カーネル作業、ドライバ処理などに使用された割合を意味します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| nice | Nice | % | 対象のCoreの全CPU時間のうち、低優先度(niced)ユーザープロセスの実行に使用された割合を意味します。一般的な優先度のユーザープロセス使用率は通常user(%)に含まれます。 | HP-UX |
| wait | Wait | % | 該当Coreの全CPU時間のうち、CPUがI/O完了を待ってアイドル状態にあった割合（I/O待ち）を意味します。CPUが実際に演算を行った時間ではなく、ディスクやネットワークなどの外部リソースの応答を待っていた時間として解釈します。 | HP-UX,
AIX,
Solaris,
Linux |
| total | User+Sys | % | 該当Coreの全CPU使用率のうち、ユーザーモード(user)とカーネルモード(sys)で使用された比率の合計を意味します。I/O待機(wait)、irq、softirq、stealなどは除外した純粋なCPU実行使用率として解釈します。 | HP-UX,
AIX,
Solaris,
Linux,
Windows |
| total_wait | User+Sys+Wait | % | 該当Coreの全CPU時間のうち、ユーザー、システム、待機の合計を意味します。つまり、ユーザー処理、カーネル処理、I/O待機を含む使用指標です。オペレーティングシステムによっては、実際の全CPU使用率と異なる場合があります。 | HP-UX,
AIX,
Solaris,
Linux |
| idle | Idle | % | 該当Coreの全CPU時間の中で、何の作業も行わずアイドル状態にあった割合を意味します。値が高いほど、該当コアの余裕が | HP-UX,
AIX, |

| Field | Title | Unit | Description | OS |
|---------|---------|------|---|-------------------------------|
| | | | 多い状態を意味します。 | Solaris,
Linux,
Windows |
| irq | Irq | % | 該当Coreの全CPU時間のうち、ハードウェアインタラプト（IRQ）を処理するために使用された割合を意味します。ネットワークカード、ディスク、その他のハードウェアイベントが特定のコアに集中する際に増加する可能性があります。 | Linux |
| softirq | Softirq | % | 該当するCoreの全CPU時間のうち、ソフトウェア割り込み（SoftIRQ）を処理するために使用された割合を意味します。ネットワークパケット処理、ブロックI/O後処理など、カーネルの遅延処理作業が特定のコアに集中する際に増加する可能性があります。 | Linux |
| steal | Steal | % | 仮想化環境において、ハイパーバイザーが他の仮想CPUを優先的に処理している間、そのコアが実行されずに奪われた時間の割合を意味します。値が高い場合、VMに割り当てられたCPUリソースが不足しているか、過剰競合状態である可能性があります。 | Linux |

| Field | Title | Unit | Description | OS |
|------------|-----------------|--------|---|-------|
| numaNodeid | NUMA
Node ID | string | その論理コアが属するNUMAノード番号。NUMA接続情報を確認できないコアは -1 | Linux |

メトリクスエクスプローラーのCPU Coreチャートの凡例は、このフィールドを使用して Core cpu1 (Node 0) の形式で表示します。値が -1 のコアと、フィールドを収集しないWindows・Unix環境では Core cpu1 の形式を維持します。

infra_os_parameter

オペレーティングシステムのカーネル・システムパラメーターの値を収集するカテゴリーです。ネットワーク、ファイルシステム、カーネル領域の主要パラメーターと現在の設定値を提供します。サーバー間の設定差異を比較したり、パフォーマンス問題の原因になり得るカーネル設定値を確認したりする際に使用します。収集した値は、ラボの [OS Parameter情報](#) 画面で照会できます。

- カテゴリー: OS Parameter
- デフォルト収集周期: 1時間

| Field | Title | Unit | Description | OS |
|-----------|-----------|--------|--|----------------------------------|
| parameter | Parameter | string | パラメーター名（例：net.ipv4.tcp_keepalive_intvl） | AIX, HP-UX,
Solaris,
Linux |
| category | Category | string | パラメーターが属する領域（例：net、fs、kernel） | AIX, HP-UX,
Solaris,
Linux |
| os | OS | string | パラメーターを収集したオペレーティングシステムの種類 | AIX, HP-UX,
Solaris,
Linux |
| value | Value | string | パラメーターの現在の設定値 | AIX, HP-UX,
Solaris,
Linux |
| custom | Custom | string | デフォルトの収集対象ではなく、ユーザーが
os.parameter.custom オプションで追加したパラメーターかどうか | AIX, HP-UX,
Solaris,
Linux |

デフォルトの収集対象以外のパラメーターを追加するには、os.parameter.custom オプションにパラメーター名をカンマ（,）で区切って入力してください。収集周期は infra_os_parameter.interval オプションで調整します。デフォルト値は3600秒です。

Windowsはこのカテゴリーを収集しません。

参考資料

- [Windows 参考資料](#)
- [Linux 参考資料](#)

サーバーインベントリの収集項目

サーバーモニタリングエージェントは、パフォーマンス指標とは別に、サーバーのハードウェア構成を定期的に収集します。パフォーマンス指標だけでは、どのデバイスがどこに接続されているかがわからないため、指標に異常が見えても原因となるデバイスを特定しにくくなります。インベントリ項目をあわせて確認すると、GPUとネットワークカードがどのNUMAノードに接続されているか、GPU同士がどのような方式で接続されているかまで確認できます。このドキュメントは、AI・HPCワークロードを運用し、デバイス構成まで点検する必要がある運用者を対象に、各インベントリ項目の収集フィールドを案内します。

インベントリ項目は、値が変わったときにのみ送信します。エージェントは1時間周期で構成を確認し、前回の収集と比較して追加・変更・削除された項目のみをサーバーへ送ります。

各表の備考列にバージョンとともに **新規** と表示したフィールドは、そのバージョンで追加された項目であり、表示のないフィールドはカテゴリが追加された時点から提供しています。

server_rdma_inventory

RDMA（InfiniBand・RoCE）デバイスとポートの構成情報です。RDMAデバイス1台のポートごとに1行を収集し、デバイスのモデル・ファームウェア・リンク速度から、接続されたオペレーティングシステムのネットワークインターフェイスまであわせて提供します。

- 収集対象: Linux
- デフォルト収集周期: 1時間

| Field | Type | Unit | Description |
|---------------|--------|------|--|
| interfaceName | string | - | RDMAデバイス名とポート番号（例：mlx5_0:1） |
| rdmaDevice | string | - | RDMAデバイス名（例：mlx5_0） |
| rdmaNetdev | string | - | デバイスに接続されたオペレーティングシステムのネットワークインターフェイス。複数ある場合は で区切ります |
| rdmaNetdevIp | string | - | ネットワークインターフェイス別のIPアドレス（CIDR表記）。複数ある場合は で区切ります |

| Field | Type | Unit | Description |
|---------------------|--------|------|--------------------------------------|
| rdmaDeviceType | string | - | デバイスのASICの種類（例：MT4123） |
| rdmaDeviceModel | string | - | デバイスのモデル名（例：ConnectX-6） |
| rdmaLinkLayer | string | - | リンク層。InfiniBand または Ethernet |
| rdmaNumaNode | string | - | デバイスが属するNUMAノード番号。確認できない場合は -1 |
| rdmaPciBusId | string | - | PCIアドレス（例：0000:81:00.0） |
| rdmaPort | string | - | ポート番号 |
| rdmaRate | string | - | ポートのリンク速度（例：100 Gb/sec (4X EDR)） |
| rdmaMtu | string | - | ポートの有効MTU |
| rdmaNetdevMtu | string | - | ネットワークインターフェイス別のMTU。複数ある場合は で区切ります |
| rdmaDriverName | string | - | カーネルドライバー名（例：mlx5_core） |
| rdmaDriverVersion | string | - | ドライバーバージョン |
| rdmaFirmwareVersion | string | - | デバイスのファームウェアバージョン |
| rdmaBondMaster | string | - | ネットワークインターフェイスが属するボンディング名 |
| rdmaNodeGuid | string | - | デバイスのNode GUID |
| rdmaPortGuid | string | - | ポートのPort GUID |
| rdmaSysImageGuid | string | - | デバイスのSystem Image GUID |
| rdmaSubnetPrefix | string | - | ポートが属するサブネットプレフィックス |
| rdmaVlanId | string | - | ネットワークインターフェイス別のVLAN ID |

| Field | Type | Unit | Description |
|--------------|--------|------|---|
| storageMount | string | - | そのネットワークインターフェイスを経由して接続されたりリモートストレージのマウントポイント |

収集の有無と周期は、次のオプションで調整します。

whatap.conf

```
rdma.inventory.enabled=true # 収集の有無 (デフォルト: true)
rdma.inventory.interval=3600 # 収集周期、秒単位 (デフォルト: 3600)
```

server_gpu_topology

GPU 2台の間の接続関係です。物理GPUのペアごとに1行を収集し、2つのGPUがどの経路で接続されており、直接データをやり取りできるかを確認する際に使用します。

- 収集対象: Linux
- デフォルト収集周期: 1時間

| Field | Type | Unit | Description |
|--------------------|--------|-------|---|
| baseGpuIndex | string | - | 基準GPUの番号 |
| targetGpuIndex | string | - | 相手GPUの番号。常に基準GPUの番号より大きい |
| topologyType | string | - | 2つのGPU間の接続段階。PIX・PXB・PHB・NODE・SYS・NVnのいずれか。値が一貫していない場合はINCONSISTENT |
| topologyConsistent | string | - | 双方向の照会結果が一致するかどうか。true または false |
| interconnectType | string | - | 接続方式。NVSwitch・NVLink・PCIe・Unknown |
| nvLinkCount | - | count | NVLink接続数。NVLink接続でない場合は0 |
| baseGpuMigMode | string | - | 基準GPUのMIG設定状態。Enabled・Disabled・NotSupported・ |

| Field | Type | Unit | Description |
|---------------------|--------|------|---|
| | | | Unknown |
| targetGpuMigMode | string | - | 相手GPUのMIG設定状態 |
| peerToPeerSupported | string | - | 2つのGPU間の直接通信（P2P）のサポート有無。true・false・unknown |
| peerToPeerStatus | string | - | P2P読み取りの状態コード（例：OK・NS・CNS） |

接続段階は PIX に近いほど2つのGPUが物理的に近く、SYS に近いほど遠くなります。同じ処理を担当するGPUを近いペアにまとめると、通信の遅延を減らせます。

whatap.conf

```
gpu.topology.inventory.enabled=true # 収集の有無 (デフォルト: true)
gpu.topology.inventory.interval=3600 # 収集周期、秒単位 (デフォルト: 3600)
```

ⓘ GPUの収集が無効な場合や、GPUドライバーにアクセスできない場合は、この項目を収集しません。GPUが1台のサーバーはペアが作られないため、収集結果は空になります。

server_system_topology

CPUソケット、NUMAノード、PCIeデバイスを親子関係でつないだ構成情報です。1つの接続関係が1行になり、サーバー全体のデバイス配置をツリー形式で確認する際に使用します。

- 収集対象: Linux, Windows
- デフォルト収集周期: 1時間

| Field | Type | Unit | Description |
|--------------|--------|------|---|
| parentDevice | string | - | 上位デバイス名（例：SYSTEM、NUMA_NODE:0、PCI_BRIDGE:0000:00:01.1） |

| Field | Type | Unit | Description |
|-------------|--------|------|---|
| childDevice | string | - | 下位デバイス名（例：CPU_SOCKET:0、GPU0、ens192） |
| deviceType | string | - | 下位デバイスの種類。CPU_SOCKET・NUMA_NODE・CPU_CORES・MEMORY・PCI_ROOT・GPU・NVSWITCH・RDMA_NIC・NIC・NVME・PCI_BRIDGE・HOST_BRIDGE・PCI_DEVICE |
| pciBusId | string | - | PCI階層のデバイスはPCIアドレス、CPU階層のデバイスは socket:0・node:0 の形式の識別子 |
| pcieDepth | string | - | PCIe経路の深さ。CPU・NUMA・メモリ階層は0 |

ツリーの最上位の名前は SYSTEM です。収集はカーネルが提供する情報（Linuxはsysfs、Windowsはデバイス情報）のみを使用するため、別途のコマンドは実行しません。

whatap.conf

```
system.topology.enabled=true # 収集の有無 (デフォルト: true)
system.topology.interval=3600 # 収集周期、秒単位 (デフォルト: 3600)
```

server_numa_inventory

NUMAノード別の構成情報です。NUMAノード1つが1行になり、ノードに属するCPUとメモリ、そして同じノードに接続されたGPU・RDMA・NVMeデバイスをあわせて提供します。

- 収集対象: Linux
- デフォルト収集周期: 1時間

| Field | Type | Unit | Description | 備考 |
|--------------|--------|-------|-----------------------------|----|
| numaNodeid | string | - | NUMAノード番号 | |
| cpuList | string | - | ノードに属するCPUのリスト（例：0-7,16-23） | |
| logicalCores | - | count | ノードに属する論理CPU数 | |

| Field | Type | Unit | Description | 備考 |
|-----------------|--------|------|---|--------------|
| memorySize | - | byte | ノードに属するメモリサイズ | |
| gpuIndexes | string | - | ノードに接続されたNVIDIA GPU番号のリスト。カンマと空白で区切ります | |
| rdmaDevices | string | - | ノードに接続されたRDMAデバイス名のリスト（例：mlx5_0, mlx5_1）。カンマと空白で区切ります | |
| rdmaNetDevs | string | - | 該当のRDMAデバイスに接続されたネットワークインターフェイスのリスト。カンマと空白で区切ります | |
| nvmeDevices | string | - | そのNUMAノードに接続されたNVMeデバイス名のリスト（例：nvme0, nvme1）。カンマと空白で区切ります | 2.9.22
新規 |
| gpuRdmaAffinity | string | - | そのNUMAノードのGPUごとに最も近いRDMAデバイスをGPU0:mlx5_0(PIX)の形式で表示。複数ある場合はカンマと空白で区切ります | 2.9.22
新規 |

gpuRdmaAffinity の括弧内の値は、GPUとRDMAデバイスの間の距離です。近い順は PIX、PXB、PHB、NODE、SYS で、GPUごとに最も近い段階のデバイスのみを表示します。GPU通信がRDMAデバイスを経由する構成で、2つのデバイスが同じノードに接続されているかを確認する際に使用します。

収集するかどうかと周期は、次のオプションで調整します。

whatap.conf

```
numa.inventory.enabled=true # 収集するかどうか（デフォルト値: true）
numa.inventory.interval=3600 # 収集周期、秒単位（デフォルト値: 3600）
```

VMware収集項目

サーバーモニタリングエージェントは、VMware APIを通じてESXiホストと仮想マシンの状態をあわせて収集します。仮想マシン内部から見たリソース使用量だけでは、パフォーマンス低下の原因を把握しにくくなります。ホストのファンが故障している場合や、1台のホストに仮想マシンが過度に集中してvCPUが互いに実行順序を待っている状況は、ゲストの指標には現れにくいからです。このドキュメントは、仮想化基盤のインフラを運用し、ホスト単位の原因まで追跡する必要がある運用者を対象に、VMware連携で収集する項目を案内します。

VMwareのデータ連携は、vCenterがなくてもESXiホストに直接連携してデータを収集できます。ただし `vm_vcenter_inventory` カテゴリは、vCenterに連携した場合にのみ収集します。

サポートするエージェントバージョンは、Linux・Windows 2.9.23以上です。各表の備考列に `2.9.23 新規` と表示したフィールドは2.9.23で追加された項目であり、表示のないフィールドは以前のバージョンから提供しています。

infra_vm_vhost_hw

ESXiホストのハードウェア状態を部位別にまとめて収集するカテゴリです。ホスト1台が1行になり、電源・冷却・メモリ・プロセッサなど部位別の状態と最高温度を提供します。ハードウェアの故障がパフォーマンス低下や障害につながる前に確認する際に使用します。2.9.23で追加したカテゴリであり、表のすべてのフィールドが新規です。

- 収集対象: VMware ESXi
- 状態の値は、次の4つに標準化します。部位別のセンサーが複数ある場合は最も深刻な状態を代表値として表示し、センサーデータが提供されない部位は `unknown` と表示します。

| Item | Description |
|----------------------|-------------|
| <code>green</code> | 正常 |
| <code>yellow</code> | 警告 |
| <code>red</code> | 障害 |
| <code>unknown</code> | 状態を確認できません |

| Field | Type | Unit | Description |
|-----------------------------|--------|------|--|
| vhostName | string | - | 収集対象のホスト名。各ハードウェア状態がどのESXiホストで収集されたかを識別する基準 |
| uuid | string | - | ホストのハードウェアUUID。ホスト名やIPが変わっても同じホストを識別する補助基準 |
| hardwareHealth | string | - | 収集可能な全ハードウェア状態のうち、最も深刻な状態を代表する総合状態 |
| powerSupplyStatus | string | - | 電源供給装置の状態 |
| powerSupplyRedundancyStatus | string | - | 電源供給装置の冗長化状態。一部の障害で冗長化が低下していないかを確認する際に使用 |
| networkDeviceStatus | string | - | 物理ネットワークデバイスとネットワークアダプターのハードウェア状態。ネットワークリンクのUp・Down状態とは区別される情報 |
| batteryStatus | string | - | 内部バッテリーまたはハードウェア管理コントローラーのバッテリーの状態。CMOSバッテリー、RAIDキャッシュバッテリーなどを含む |
| processorsStatus | string | - | 物理プロセッサとCPUソケットのハードウェア状態。CPU使用率とは無関係な物理ハードウェアの状態 |
| memoryModulesStatus | string | - | 物理メモリモジュールのハードウェア状態。DIMMエラーやモジュールの障害・警告状態を含む |
| coolingUnitStatus | string | - | ファン、ブロワーなど冷却装置の状態 |
| coolingUnitRedundancyStatus | string | - | 冷却装置の冗長化状態。一部のファンが故障しても冷却機能が維持されるかを確認する際に使用 |
| temperatureStatus | string | - | CPU、システムボード、メモリ、吸気口など温度センサーの総合状態 |

| Field | Type | Unit | Description |
|---------------------------------|---------|------|--|
| temperatureMax | - | °C | 収集時点で確認された温度センサー値のうち最も高い温度。センサーの生値にVMwareが提供する単位補正値を適用して計算し、温度センサーがない場合は空の値 |
| hardwareHealthDataAvailable | boolean | - | ホストからハードウェア状態またはセンサーデータが1つ以上提供されたかどうか |
| hardwareHealthSupportStatus | string | - | ハードウェア状態の収集をサポートするかどうか。
supported はセンサーデータが提供される状態、
unsupported はAPIがサポートされていないか、センサーが公開されていない状態 |
| hardwareHealthUnavailableReason | string | - | ハードウェア状態データを収集できない理由。Hardware Health APIの非サポート、センサーの非公開、収集エラーなどが記録され、正常に収集した場合は空の値 |
| temperatureMaxSensor | string | - | temperatureMax の値が測定された温度センサーの名前。CPU、システムボード、メモリ、吸気口のうち、実際に最も高い温度を記録したセンサーを識別 |
| temperatureUnit | string | - | temperatureMax に適用される温度単位。通常は Degrees C の形式で、センサープロバイダーによって表現方式が異なる場合があります |

infra_vm_vhost_resource_capacity

ESXiホストの物理リソースと、仮想マシンに割り当てたリソースをあわせて収集するカテゴリーです。ホスト1台が1行になり、物理容量に対する割り当て量の比率（オーバーコミット）を提供します。特定のホストに仮想マシンを過度に配置していないかを点検する際に使用します。2.9.23で追加したカテゴリーであり、表のすべてのフィールドが新規です。

- 収集対象: VMware ESXi

| Field | Type | Unit | Description |
|---------------------------|--------|-------|--|
| vhostName | string | - | 収集対象のホスト名。各リソース指標がどのESXiホストで収集されたかを識別する基準 |
| uuid | string | - | ホストのハードウェアUUID。ホスト名やIPが変わっても同じホストを識別する補助基準 |
| cpuCores | - | count | ホスト全体の物理CPUコア数。仮想マシンに割り当て可能なリソースとCPU容量算定の基準 |
| totalMemory | - | byte | ホストに搭載された全体のメモリ容量。仮想マシンを配置できる容量とメモリリソース計画の基準 |
| activeVCpu | - | count | 電源がオンの仮想マシンに割り当てられたvCPU数の合計 |
| allocatedVCpu | - | count | ホストに配置された全仮想マシンに設定されたvCPU数の合計。電源がオフ、または一時停止中の仮想マシンもすべて含む |
| activeOverCommitCore | - | - | activeVCpu を物理CPUコア数で割った値。実行中の仮想マシンを基準に、物理コア1つあたり平均で何個のvCPUが割り当てられているかを倍数で表示 |
| allocatedOverCommitCore | - | - | allocatedVCpu を物理CPUコア数で割った値。電源がオフ、または一時停止中の仮想マシンまで含めた構成基準のvCPUオーバーコミット倍数 |
| activeMemory | - | byte | 電源がオンの仮想マシンに設定されたメモリ容量の合計 |
| allocatedMemory | - | byte | ホストに配置された全仮想マシンに設定されたメモリ容量の合計。電源がオフ、または一時停止中の仮想マシンもすべて含む |
| activeOverCommitMemory | - | - | activeMemory を物理メモリ容量で割った値。実行中の仮想マシンを基準に、物理メモリに対して何倍のメモリが割り当てられているかを倍数で表示 |
| allocatedOverCommitMemory | - | - | allocatedMemory を物理メモリ容量で割った値。電源がオフ、または一時停止中の仮想マシンまで含めた構成基準のメモリオ |

| Field | Type | Unit | Description |
|--------------------------|------|-------|--|
| | | | オーバーコミット倍数 |
| vmGuestCount | - | count | ホストに接続された仮想マシンオブジェクトの数。ホストごとの配置状況と密集度を把握する際に使用 |
| poweredOffVMCount | - | count | 電源がオフの仮想マシン数。allocatedVCpu には含まれますが、activeVCpu には含まれません |
| suspendedVMCount | - | count | 一時停止状態の仮想マシン数。vCPUが設定されているため allocatedVCpu には含まれますが、実行中ではないため activeVCpu には含まれません |
| unknownPowerStateVMCount | - | count | 電源状態を確認できない、または poweredOn ・ poweredOff ・ suspended のいずれとしても識別されない仮想マシン数。vCenterの応答遅延、権限、一時的な状態の不一致で発生する場合があります |
| vcpuSkippedVMCount | - | count | vCPUの設定値を読み取れず、vCPUの合算から除外した仮想マシン数。設定情報へのアクセス失敗、権限不足、異常な構成、一時的なvCenterの応答エラーが原因の可能性があります |
| memorySkippedVMCount | - | count | メモリの設定値を読み取れず、メモリの合算から除外した仮想マシン数。原因は vcpuSkippedVMCount と同じ |

オーバーコミット比率は小数点第2位まで表示します。値が 1 を超えると、物理リソースより多くのリソースを仮想マシンに割り当てた状態です。仮想化環境では一定水準のオーバーコミットが一般的であるため、絶対値よりも同じクラスター内のホスト間の偏差と、時間経過に伴う増加傾向をあわせて確認することをおすすめします。

収集するかどうかは、次のオプションで調整します。

whatap.conf

```
vm.vhost.perf.resource_capacity.enabled=true # 収集するかどうか（デフォルト値: true）
```

infra_vm_vhost_cpu

ESXiホストのCPU使用量と待機時間を集計するカテゴリです。ホスト1台が1行になり、ホスト上の全仮想マシンのCPU使用と競合をあわせて提供します。

- 収集対象: VMware ESXi

| Field | Type | Unit | Description | 備考 |
|---------------|--------|---------|--|----|
| vhostName | string | - | 収集対象のホスト名。各CPU指標がどのESXiホストで収集されたかを識別する基準 | |
| uuid | string | - | ホストのハードウェアUUID。ホスト名やIPが変わっても同じホストを識別する補助基準 | |
| usage | - | percent | ホスト全体のCPUリソースのうち、実際に使用された割合。ホストのCPU負荷レベルを確認する基本的な指標 | |
| usageMhz | - | MHz | ホストで実際に使用中のCPUリソース量。CPU容量が異なるホストを比較する際は usage とあわせて確認 | |
| totalCapacity | - | MHz | ホストが提供できる全体のCPU容量。使用率・使用量・要求量・予約容量を解釈するための基準値 | |
| demand | - | MHz | ホストの仮想マシンが実際に使用しようと要求したCPUリソース量 | |
| readiness | - | percent | 仮想マシンが実行可能な状態でありながら、物理CPUをすぐに割り当てられなかった割合。ホストのCPU競合を判断する中心的な指標 | |
| ready | - | ms/s | 実行可能な状態で物理CPUを割り当てられず待機した時間 | |
| latency | - | percent | CPUリソースを要求してから実際に実行されるまでの遅延レベル | |
| costop | - | ms/s | 複数のvCPUを持つ仮想マシンが、同時にスケジューリングされ | |

| Field | Type | Unit | Description | 備考 |
|------------------|------|---------|---|--------------|
| | | | るのを待って停止していた時間 | |
| wait | - | ms/s | CPUが実際の演算を行わずに待機した時間。アイドル、I/O待ち、スワップ待ちをすべて含む | |
| swapwait | - | ms/s | メモリのスワップ処理によってCPUの実行が遅延した時間 | |
| idle | - | ms/s | CPUがアイドル状態だった時間 | |
| reservedCapacity | - | MHz | 予約で確保したCPU容量。全体容量に対して大きいと、実際に使用できるCPUの余裕が減ります | |
| demandPct | - | percent | demand を totalCapacity で割った割合 | 2.9.23
新規 |
| costopPct | - | percent | costop を割合に換算した値 (1,000ms/s = 100%) | 2.9.23
新規 |

CPU競合の有無は、単一の指標で判断せず組み合わせて確認することをおすすめします。usage が高く、readiness ・ ready もあわせて高い場合は、CPU競合の可能性が高くなります。逆に usage が低いのに readiness が高い場合は、vCPUの過剰割り当て、リソース制限、スケジューリングポリシーもあわせて確認してください。usageMhz より demand が継続して高い場合、仮想マシンが要求した分のCPUを受け取れていない可能性があります。

wait にはアイドル状態とI/O待ち、スワップ待ちがすべて含まれるため、値が高いことだけでCPU不足と断定してはいけません。idle 、 swapwait と分けて確認してください。swapwait はCPU指標として表示されますが、原因はメモリ不足やメモリ競合の可能性があるので、値が増えた場合はホストと仮想マシンのメモリ使用率、バレーニング、スワップの発生有無もあわせて確認する必要があります。

ms/s 単位の指標は、収集周期が変わっても同じ基準で比較できるよう、秒あたりの値に換算して提供します。

demandPct と costopPct は、ホスト上のすべての仮想マシンvCPUを合算した値であるため100%を超える場合があります、別途上限は適用しません。costopPct が継続して高い場合、仮想マシンに割り当てたvCPU数がホストの容量に対して多い状態である可能性があります。

infra_vm_vhost_mem

ESXiホストのメモリ使用量と回収動作を集計するカテゴリーです。ホスト1台が1行になり、実際の占有量とワーキングセットから、バレーニング・圧縮・スワップといったメモリ回収の指標まであわせて提供します。

- 収集対象: VMware ESXi

| Field | Type | Unit | Description |
|---------------------|--------|---------|---|
| vhostName | string | - | 収集対象のホスト名。各メモリ指標がどのESXiホストで収集されたかを識別する基準 |
| uuid | string | - | ホストのハードウェアUUID。ホスト名やIPが変わっても同じホストを識別する補助基準 |
| consumed | - | byte | ホストが実際に消費中の物理メモリ量。仮想マシン、VMkernel、ESXiシステム領域が占有するメモリをすべて含む |
| active | - | byte | ホスト上の仮想マシンが最近実際に活発に使用したメモリ量。実質的なワーキングセットに近い値 |
| activeConsumedRatio | - | percent | activeをconsumedで割った割合。消費中のメモリのうち、実際に活発に使用された割合 |
| granted | - | byte | ホストが仮想マシンに割り当てたメモリ量 |
| latency | - | percent | メモリのアクセスや割り当ての過程で発生する遅延レベル |
| vmmemctl | - | byte | バルーンドライバーが仮想マシンから回収したメモリ量 |
| swapped | - | byte | ホストでスワップへ退避されたメモリ量 |
| swapInRate | - | bytes/s | スワップ領域からメモリへ読み戻す速度 |
| swapOutRate | - | bytes/s | メモリページがスワップ領域へ退避される速度 |

| Field | Type | Unit | Description |
|-----------------|------|---------|-------------------------------------|
| compressed | - | byte | メモリ圧縮によって圧縮されたメモリ量 |
| compressionRate | - | bytes/s | メモリ圧縮が発生する速度 |
| shared | - | byte | 仮想マシン間、またはメモリページ間で共有されているメモリ量 |
| overhead | - | byte | 仮想マシンを実行するためにESXiが追加で使用するメモリオーバーヘッド |
| sysUsage | - | byte | ESXiシステム領域で使用中のメモリ量 |
| heapFree | - | byte | ESXiのHeap領域のうち使用可能な空きメモリ量 |

consumed が高いのに active が低い場合は、割り当てと占有は多いものの、実際の使用が少ない仮想マシンが多い状態です。2つの値の関係は activeConsumedRatio ですぐに確認できます。

メモリ不足の有無を1つの指標で判断しないでください。ESXiはメモリ逼迫が強まると、バルーニング、圧縮、スワップの順で回収の段階を上げます。vmmemctl が増えた後に compressed と compressionRate が上がり、swapped と swapOutRate まで発生する場合は、メモリ競合がかなり進行した状態です。latency もあわせて高い場合は、実際に仮想マシンのパフォーマンスに影響が出ている可能性が高くなります。

swapInRate が高い場合は、仮想マシンが必要とするページがスワップにあり読み戻している状態を意味し、パフォーマンスの遅延につながる可能性があります。

shared 、 overhead 、 sysUsage 、 heapFree は単独で問題を示すものではありません。shared はメモリ削減効果を参考にする補助指標であり、overhead は仮想マシン数が多いほど、また仮想デバイス構成が複雑なほど大きくなります。sysUsage や heapFree が異常に変化する場合は、ESXiのシステム状態を別途点検してください。

infra_vm_vhost_disk

ESXiホストのディスクI/Oを集計するカテゴリーです。ホスト1台が1行になり、ホストに接続された全ディスクを合算したスループットと、最も高いレイテンシを提供します。

- 収集対象: VMware ESXi

| Field | Type | Unit | Description |
|-----------------|--------|---------|--|
| vhostName | string | - | 収集対象のホスト名。各ディスク指標がどのESXiホストで収集されたかを識別する基準 |
| uuid | string | - | ホストのハードウェアUUID。ホスト名やIPが変わっても同じホストを識別する補助基準 |
| usage | - | bytes/s | ホストで発生した全体のディスクI/Oスループット。読み取りと書き込みを合算した値 |
| read | - | bytes/s | ホストで発生したディスク読み取りのスループット |
| write | - | bytes/s | ホストで発生したディスク書き込みのスループット |
| maxTotalLatency | - | ms | ホストに接続されたディスク・デバイスのうち、最も高いディスクI/Oのレイテンシ |

usage が継続して高い場合、該当ホストの仮想マシンで多くのディスクI/Oが発生している状態です。

maxTotalLatency とあわせて確認し、単なるスループットの増加なのか、ストレージのボトルネックなのかを見分けてください。

read が高く、レイテンシもあわせて増加する場合は、読み取りI/Oの競合、キャッシュミス、バックエンドストレージの応答遅延を確認します。write が高くレイテンシが増加する場合は、書き込みI/Oの競合、ストレージコントローラーの遅延、RAID・キャッシュ・同期の遅延を確認してください。

maxTotalLatency は、特定のディスク、データストア、LUN、ストレージパスで遅延が発生すると高くなります。ホスト全体のスループットが高くなってもこの値が高い場合は、一部のストレージパスや特定の仮想マシンのI/O遅延を確認することをおすすめします。

infra_vm_vhost_disk_perf

ESXiホストに接続されたディスクデバイス別のパフォーマンスです。ディスク1台が1行になり、スループットとリクエスト数、層別のレイテンシをあわせて提供します。どのディスクでボトルネックが発生しているかを絞り込む際に使用します。

- 収集対象: VMware ESXi

| Field | Type | Unit | Description |
|-------------------|--------|----------|---|
| vhostName | string | - | 収集対象のホスト名。各ディスク指標がどのESXiホストで収集されたかを識別する基準 |
| uuid | string | - | ホストのハードウェアUUID。ホスト名やIPが変わっても同じホストを識別する補助基準 |
| diskName | string | - | 指標が収集されたディスクまたはデバイスの名前。ホストに接続された個々のディスク、LUN、ローカルディスク、ストレージデバイスを区別する基準 |
| usage | - | bytes/s | 該当ディスクの全体的なI/Oスループット。read と write の合計 |
| read | - | bytes/s | 該当ディスクの読み取りスループット |
| write | - | bytes/s | 該当ディスクの書き込みスループット |
| numberTotal | - | counts/s | 全体のI/Oリクエスト数。numberRead と numberWrite の合計 |
| numberRead | - | counts/s | 読み取りI/Oのリクエスト数 |
| numberWrite | - | counts/s | 書き込みI/Oのリクエスト数 |
| totalLatency | - | ms | 全体のI/Oリクエスト処理にかかった平均レイテンシ。カーネル・デバイス・キューの遅延の影響をすべて含む代表的な指標 |
| totalReadLatency | - | ms | 読み取りI/Oリクエストの処理にかかった平均レイテンシ |
| totalWriteLatency | - | ms | 書き込みI/Oリクエストの処理にかかった平均レイテンシ |
| deviceLatency | - | ms | 物理ディスクまたはバックエンドストレージデバイスでI/Oを処理するのににかかった平均レイテンシ |
| queueLatency | - | ms | I/Oリクエストが処理される前にキューで待機した平均時間 |
| kernelLatency | - | ms | ESXi VMkernel層でI/Oを処理する間に発生した平均レイテンシ |

| Field | Type | Unit | Description |
|---------------|------|----------|--------------------------------|
| maxQueueDepth | - | count | 該当ディスクで使用できる、または観測された最大キュー深度 |
| busResets | - | counts/s | 該当ディスクまたはストレージバスで発生したバスリセットの回数 |

スループット（`usage`、`read`、`write`）とリクエスト数（`numberTotal`、`numberRead`、`numberWrite`）をあわせて見ると、I/Oのブロックサイズを推測できます。リクエスト数は多いのにスループットが低い場合は、小さいブロックのI/Oが多い状態です。

レイテンシがどこで発生しているかは、レイテンシ指標を分けて確認すると絞り込めます。

| 高い指標 | 確認する箇所 |
|---------------|--|
| deviceLatency | ストレージデバイス、LUN、アレイ、SAN・NASなどバックエンドストレージ層 |
| kernelLatency | ホスト内部のI/O処理、ドライバー、HBA・ストレージアダプター、VMkernelストレージスタック |
| queueLatency | リクエストの処理速度が追いつかず待ち行列が溜まっている状態。 <code>maxQueueDepth</code> 、リクエスト数とあわせて確認 |

`busResets` が0以外の状態で繰り返し発生する場合は、ストレージバスの安定性、HBA・コントローラーのログ、ESXiのイベントもあわせて確認してください。

ホスト全体を合算した値は `infra_vm_vhost_disk` で確認します。

infra_vm_vhost_storageadapter_perf

ESXiホストのストレージアダプター（HBA）別のパフォーマンスです。アダプター1つが1行になり、アダプターに接続されたディスクとLUNのパフォーマンスを合算して提供します。どのHBAに負荷が集中しているかを確認する際に使用します。

- 収集対象: VMware ESXi

| Field | Type | Unit | Description |
|---------------------|--------|----------|---|
| vhostName | string | - | 収集対象のホスト名。各アダプター指標がどのESXiホストで収集されたかを識別する基準 |
| uuid | string | - | ホストのハードウェアUUID。ホスト名やIPが変わっても同じホストを識別する補助基準 |
| memberCount | - | count | 該当アダプターの集計に含まれるcanonicalディスクまたはLUNインスタンスの数。値が大きいほど、多くのディスク・LUNの性能値が1つのアダプターとして合算された結果 |
| memberPathNames | string | - | 該当アダプターにマッピングされたディスク・LUNパスの一覧。アダプターの性能値がどのパスを基準に集計されたかを確認する際に使用 |
| adapterName | string | - | 性能値が集計されたストレージアダプター名。通常は vmhba0 のようなHBAまたはストレージコントローラー名 |
| total | - | bytes/s | 該当アダプターの全体的なI/Oスループット。 read と write の合計 |
| read | - | bytes/s | 該当アダプターで読み取ったデータのスループット。配下のディスク・LUNの読み取りスループットを合算した値 |
| write | - | bytes/s | 該当アダプターで書き込んだデータのスループット。配下のディスク・LUNの書き込みスループットを合算した値 |
| numberTotalAveraged | - | counts/s | 該当アダプターで発生した全体の平均I/O数。
numberReadAveraged と numberWriteAveraged の合計 |
| numberReadAveraged | - | counts/s | 該当アダプターで発生した平均読み取りI/O数 |
| numberWriteAveraged | - | counts/s | 該当アダプターで発生した平均書き込みI/O数 |
| commandsAveraged | - | counts/s | 該当アダプターに接続されたディスク・LUNで発生した全体のI/Oコマンド数 |
| totalReadLatency | - | ms | 該当アダプターの読み取りI/Oの平均レイテンシ。配下のディスク・ |

| Field | Type | Unit | Description |
|-------------------|------|------|---|
| | | | LUNの読み取りレイテンシを、読み取りリクエスト数で加重平均した値 |
| totalWriteLatency | - | ms | 該当アダプターの書き込みI/Oの平均レイテンシ。配下のディスク・LUNの書き込みレイテンシを、書き込みリクエスト数で加重平均した値 |

このカテゴリーの値は、アダプター配下のディスク・LUNを合算した結果です。スループットとリクエスト数は単純な合計であり、レイテンシはリクエスト数を重みとした平均です。memberCount が大きい場合は、それだけ多くのディスク・LUNが1つの値にまとめられているという意味であり、特定のディスクだけが遅くてもアダプターの平均には現れにくいことがあります。

アダプターのレイテンシが高く見える場合は、memberPathNames でどのパスがまとめられているかを確認したうえで、infra_vm_vhost_storagepath_perf でパス単位、infra_vm_vhost_disk_perf でディスク単位へと絞り込んでください。

infra_vm_vhost_storagepath_perf

ESXiホストのストレージパス別のパフォーマンスです。パス1つが1行になり、アダプター・ターゲット・LUNの情報とあわせて、パス単位のスループットとレイテンシを提供します。マルチパス構成で特定のパスだけが遅くなる状況を見つける際に使用します。

- 収集対象: VMware ESXi

| Field | Type | Unit | Description |
|-----------|--------|------|--|
| vhostName | string | - | 収集対象のホスト名。各パス指標がどのESXiホストで収集されたかを識別する基準 |
| uuid | string | - | ホストのハードウェアUUID。ホスト名やIPが変わっても同じホストを識別する補助基準 |
| pathName | string | - | ストレージパスの表示名。アダプター、ターゲット、LUN、canonicalディスクの情報を組み合わせたパス名 |

| Field | Type | Unit | Description |
|---------------------|--------|----------|--|
| canonicalDiskName | string | - | ホストが認識するSCSI LUNのcanonical名（例: naa.*、t10.*、mpx.*）。パフォーマンスカウンターのインスタンスとマッピングされる基準 |
| adapterName | string | - | 該当パスが接続されたストレージアダプター名。通常は vmhba0 のようなHBAまたはストレージコントローラー名 |
| targetName | string | - | アダプターとターゲットを組み合わせた名前（例: vmhba0:T0）。アダプター配下のターゲットパスを識別する際に使用 |
| targetId | string | - | ESXi SCSIトポロジーで該当パスが接続されたターゲット番号。同じアダプター内の複数ターゲットを区別する際に使用 |
| lunId | string | - | 該当パスが接続されたLUN番号 |
| adapterKey | string | - | vSphere内部でストレージアダプターを識別するキー。APIのマッピングや長期データの整合性確認に使用 |
| total | - | bytes/s | 該当パスの全体的なI/Oスループット。read と write の合計 |
| read | - | bytes/s | 該当パスで読み取ったデータのスループット |
| write | - | bytes/s | 該当パスで書き込んだデータのスループット |
| numberTotalAveraged | - | counts/s | 該当パスで発生した全体の平均I/O数。numberReadAveraged と numberWriteAveraged の合計 |
| numberReadAveraged | - | counts/s | 該当パスで発生した平均読み取りI/O数 |
| numberWriteAveraged | - | counts/s | 該当パスで発生した平均書き込みI/O数 |
| commandsAveraged | - | counts/s | 該当パスで発生した全体のI/Oコマンド数。読み取りと書き込みを含むストレージコマンドの負荷 |
| totalReadLatency | - | ms | 該当パスの読み取りI/Oの平均レイテンシ |

| Field | Type | Unit | Description |
|-------------------|------|------|----------------------|
| totalWriteLatency | - | ms | 該当パスの書き込みI/Oの平均レイテンシ |

パスを識別するフィールドが複数あるのは、問題を絞り込む単位がそれぞれ異なるためです。adapterName はHBA単位、targetId は同じアダプター内のターゲット単位、lunId はLUN単位です。同じLUNに複数のパスがある場合、どのパスだけが遅いかを比較すると、パス障害とストレージデバイスの問題を切り分けられます。

totalReadLatency や totalWriteLatency が継続して高い場合は、該当パスのHBA、ターゲット、LUN、SAN区間を確認してください。同じ canonicalDiskName を使うすべてのパスで高い場合は、パスではなくバックエンドストレージ側の問題である可能性が高くなります。

infra_vm_vhost_datastore_perf

ESXiホストがアクセスするデータストア別のパフォーマンスと容量です。データストア1つが1行になり、I/Oのスループットとレイテンシに加えて、容量の使用状況もあわせて提供します。

- 収集対象: VMware ESXi

| Field | Type | Unit | Description |
|----------------------|--------|------|--|
| vhostName | string | - | 収集対象のホスト名。各データストア指標がどのESXiホストで収集されたかを識別する基準 |
| uuid | string | - | ホストのハードウェアUUID。ホスト名やIPが変わっても同じホストを識別する補助基準 |
| datastoreName | string | - | パフォーマンスと容量の情報が収集されたデータストア名。VMFS、NFS、vSANなどvSphereが認識する表示名 |
| datastoreInstancelId | string | - | パフォーマンスカウンターのインスタンスとマッピングされるデータストア識別子。データストアURLから抽出したVMFSボリュームUUIDなどで、名前の変更や重複の可能性がある環境で安定して紐づける際に使用 |
| datastoreType | string | - | データストアの種類（例: VMFS、NFS、vSAN）。ストレージバ |

| Field | Type | Unit | Description |
|---------------------|---------|----------|---|
| | | | ックエンドの種類を区別する際に使用 |
| accessible | boolean | - | ホストから該当データストアにアクセスできるかどうか |
| datastoreUrl | string | - | データストアのvSphere内部URL。VMFSボリュームUUIDやアクセスパスを含む |
| total | - | bytes/s | データストアの全体的なI/Oスループット。read と write の合計 |
| read | - | bytes/s | データストアから読み取ったデータのスループット |
| write | - | bytes/s | データストアへ書き込んだデータのスループット |
| numberTotalAveraged | - | counts/s | データストアで発生した全体の平均I/O数。
numberReadAveraged と numberWriteAveraged の合計 |
| numberReadAveraged | - | counts/s | データストアで発生した平均読み取りI/O数 |
| numberWriteAveraged | - | counts/s | データストアで発生した平均書き込みI/O数 |
| totalReadLatency | - | ms | データストアの読み取りI/Oの平均レイテンシ |
| totalWriteLatency | - | ms | データストアの書き込みI/Oの平均レイテンシ |
| capacity | - | byte | データストアの全体容量 |
| allocated | - | byte | 割り当て基準の領域。used と uncommitted を合算した値 |
| used | - | byte | 実際の使用量。全体容量から空き容量を引いた値 |
| uncommitted | - | byte | Thin Provisioning環境で、まだ実際には使用されていないものの、今後使用される可能性がある未確定の割り当て領域 |
| free | - | byte | データストアの空き容量 |
| usedPct | - | percent | used を capacity で割った使用率 |

容量のフィールドは、次の関係になっています。

- `capacity` = `used` + `free`
- `allocated` = `used` + `uncommitted`

`allocated` が `capacity` を超える場合は、Thin Provisioningによって実際の容量より多くの領域を約束しているオーバーコミット状態です。仮想マシンのディスクが大きくなるにつれて `uncommitted` が実際の使用量に変わるため、`usedPct` だけを見るのではなく、`allocated` と `capacity` の関係もあわせて確認してください。

`accessible` が `false` の場合は、ホストとデータストア間の接続、ストレージパス、SAN・NASネットワーク、権限、データストアの障害有無を確認する必要があります。

レイテンシが継続して高い場合は、ストレージの応答遅延、パスの問題、バックエンドストレージの負荷、ストレージネットワークの遅延を確認してください。同じデータストアを複数のホストで共有している場合は、他のホストでも同じレイテンシが見られるかを比較すると、ホスト側の問題とバックエンド側の問題を切り分けられます。

infra_vm_vhost_network

ESXiホストのネットワーク使用量を集計するカテゴリです。ホスト1台が1行になり、ホストの全物理ネットワークインターフェイスを合算した値を提供します。

- 収集対象: VMware ESXi

| Field | Type | Unit | Description | 備考 |
|------------------------|---------------------|----------------------|--|----|
| <code>vhostName</code> | <code>string</code> | - | 収集対象のホスト名。各ネットワーク指標がどのESXiホストで収集されたかを識別する基準 | |
| <code>uuid</code> | <code>string</code> | - | ホストのハードウェアUUID。ホスト名やIPが変わっても同じホストを識別する補助基準 | |
| <code>usage</code> | - | <code>bytes/s</code> | ホスト全体のネットワーク使用量。受信と送信のトラフィックを合算した値 | |
| <code>bytesRx</code> | - | <code>bytes/s</code> | ホストがネットワークを通じて受信したデータのスループット。仮想マシン、VMkernel、管理ネットワークをすべて含む | |

| Field | Type | Unit | Description | 備考 |
|--------------|------|----------|--|--------------|
| bytesTx | - | bytes/s | ホストがネットワークを通じて送信したデータのスループット。仮想マシン、VMkernel、管理ネットワークをすべて含む | |
| packetsTotal | - | counts/s | 受信パケット（packetsRx）と送信パケット（packetsTx）の合計 | |
| packetsRx | - | counts/s | ホストが受信したネットワークパケット数 | |
| packetsTx | - | counts/s | ホストが送信したネットワークパケット数 | |
| errorsRx | - | counts/s | 受信の過程で発生したエラー数 | |
| errorsTx | - | counts/s | 送信の過程で発生したエラー数 | |
| droppedRx | - | counts/s | 受信中にドロップされたパケット数 | |
| droppedTx | - | counts/s | 送信中にドロップされたパケット数 | |
| errorsRxTx | - | counts/s | 受信エラー（errorsRx）と送信エラー（errorsTx）の合計 | 2.9.23
新規 |
| droppedRxTx | - | counts/s | 受信ドロップ（droppedRx）と送信ドロップ（droppedTx）の合計 | 2.9.23
新規 |

errorsRx が継続して増える場合は、物理NIC、ケーブル、スイッチポート、ドライバー、MTU設定の問題が考えられます。errorsTx が増える場合は、物理NIC、スイッチポート、リンク状態、ドライバー、ネットワークの輻輳を確認してください。

droppedRx は、受信キューの不足、ネットワークの輻輳、NIC・ドライバーの問題、vSwitchの処理遅延が原因の可能性あります。droppedTx は、送信キューの不足、ネットワークの輻輳、物理NICまたはvSwitchの処理遅延を確認する際に使用します。

errorsRxTx と droppedRxTx は、送受信を分けずにホスト単位の総量のみを確認する際に使用します。

infra_vm_vhost_nic_perf

ESXiホストの物理ネットワークインターフェイス別の使用量です。インターフェイス1つが1行になり、どのインターフェイスでエラーや破棄が発生しているかを確認する際に使用します。

- 収集対象: VMware ESXi

| Field | Type | Unit | Description | 備考 |
|--------------|--------|----------|--|----|
| vhostName | string | - | 収集対象のホスト名。各NIC指標がどのESXiホストで収集されたかを識別する基準 | |
| uuid | string | - | ホストのハードウェアUUID。ホスト名やIPが変わっても同じホストを識別する補助基準 | |
| nicName | string | - | 指標が収集されたネットワークインスタンス名。通常は vmnic0、vmnic1 のような物理NIC名で、環境によっては別の名前が表示される場合があります | |
| usage | - | bytes/s | 該当NICの全体的なネットワークスループット。受信と送信を合算した値 | |
| bytesRx | - | bytes/s | 該当NICで受信したデータのスループット | |
| bytesTx | - | bytes/s | 該当NICで送信したデータのスループット | |
| packetsTotal | - | counts/s | 受信パケット（packetsRx）と送信パケット（packetsTx）の合計 | |
| packetsRx | - | counts/s | 該当NICが受信したネットワークパケット数 | |
| packetsTx | - | counts/s | 該当NICが送信したネットワークパケット数 | |
| errorsRx | - | counts/s | 受信の過程で発生したエラー数 | |
| errorsTx | - | counts/s | 送信の過程で発生したエラー数 | |

| Field | Type | Unit | Description | 備考 |
|-------------|------|----------|--|--------------|
| droppedRx | - | counts/s | 受信中にドロップされたパケット数 | |
| droppedTx | - | counts/s | 送信中にドロップされたパケット数 | |
| errorsRxTx | - | counts/s | 受信エラー（errorsRx）と送信エラー（errorsTx）の合計 | 2.9.23
新規 |
| droppedRxTx | - | counts/s | 受信ドロップ（droppedRx）と送信ドロップ（droppedTx）の合計 | 2.9.23
新規 |

特定のNICだけでエラーやドロップが増える場合は、そのNICのケーブル、スイッチポート、ドライバー、MTU設定を先に確認してください。ホスト全体を合算した値は `infra_vm_vhost_network` で確認します。

`errorsRxTx` と `droppedRxTx` は、送受信を分けずにインターフェイス単位の総量のみを確認する際に使用します。

infra_vm_vhost_vmguest_perf

ESXiホストで実行中の仮想マシンのパフォーマンス指標です。電源がオンの仮想マシン1台が1行になり、ホストの観点から見た仮想マシンのCPU・メモリ・ディスク・ネットワークの使用量を提供します。

- 収集対象: VMware ESXi

| Field | Type | Unit | Description | 備考 |
|----------------|--------|------|---|----|
| vHostName | string | - | 仮想マシンが実行中のホスト名 | |
| uuid | string | - | 仮想マシンが実行中のESXiホストのハードウェアUUID。ホスト名やIPが変わっても同じホストを識別する補助基準 | |
| vmName | string | - | パフォーマンス情報が収集された仮想マシン名。vCenterインベントリに表示される名前 | |
| vmInstanceUuid | string | - | vCenter内で仮想マシンインスタンスを識別するUUID。名前の変更やvMotionに関係なく、同じ仮想マシンを追跡する主要な識別子 | |

| Field | Type | Unit | Description | 備考 |
|---------------------|------|---------|--|--------------|
| cpuUsage | - | percent | 仮想マシンのCPU使用率。vSphereの <code>cpu.usage.average</code> 値をパーセントに変換した値 | |
| cpuUsagemhz | - | MHz | 仮想マシンが実際に使用中のCPUリソース。使用率とあわせて実際の消費量を確認する際に使用 | |
| cpuCostop | - | ms | SMP仮想マシンで複数のvCPUが同時にスケジューリングされず待機した時間 | |
| cpuCostopPct | - | percent | <code>cpuCostop</code> をサンプリング間隔で割って割合に換算した値。esxtopでVMグループ単位で参照した際の <code>%CSTP</code> と一致 | 2.9.23
新規 |
| cpuCostopPctPerVcpu | - | percent | <code>cpuCostopPct</code> をvCPU数で割った、vCPUあたりの平均割合。常に0から100の間 | 2.9.23
新規 |
| cpuReadiness | - | ms | 仮想マシンがCPUを使用する準備を終えたにもかかわらず、物理CPUリソースの不足でスケジューリングされず待機した時間 | |
| cpuReadinessPct | - | percent | <code>cpuReadiness</code> をサンプリング間隔で割って割合に換算した値。esxtopでVMグループ単位で参照した際の <code>%RDY</code> と一致 | 2.9.23
新規 |
| cpuReadinessPerVcpu | - | percent | vCPUあたりの平均待機割合。vSphereの <code>cpu.readiness.average</code> カウンターから直接提供され、常に0から100の間 | 2.9.23
新規 |
| cpuMaxlimited | - | percent | CPU limit設定などにより、使用できたにもかかわらず制限されたCPU時間の割合 | |
| memConsumed | - | MB | 仮想マシンがホストメモリから実際に消費したメモリ | |
| memVmmemctl | - | KB | バルーンドライバー (vmmemctl) が回収した仮想マシンのメモリ | |

| Field | Type | Unit | Description | 備考 |
|--------------------|------|------|---|----|
| memActive | - | KB | 最近実際に活発に使用したと判断されるメモリ。実質的なワーキングセットを推定する際に使用 | |
| memGranted | - | KB | ホストが仮想マシンに付与したメモリ | |
| memSwapped | - | KB | ホストが仮想マシンのメモリの一部をスワップ処理した量 | |
| memSwapoutRate | - | KB/s | 仮想マシンのメモリがホストのスワップへ退避される速度 | |
| memCompressed | - | KB | ホストが仮想マシンのメモリを圧縮して保持している量 | |
| memCompressionRate | - | KB/s | 仮想マシンのメモリが圧縮される速度 | |
| diskUsage | - | KB/s | ゲスト観点の全体的なディスク使用量。読み取りと書き込みを合算した値 | |
| networkUsage | - | KB/s | ゲスト観点の全体的なネットワーク使用量。受信と送信を合算した値 | |

cpuCostopPct と cpuReadinessPct は、マルチvCPUの仮想マシンではvCPU数の分だけ値が大きくなり、100%を超える場合があります。しきい値を判断する際はvCPU数もあわせて考慮するか、vCPU 1つ基準に換算した cpuCostopPctPerVcpu 、 cpuReadinessPerVcpu を使用してください。vCPU基準の値は常に0から100の間になるため、vCPU数が異なる仮想マシン同士を同じ基準で比較できます。

VMware公式ガイドの判断基準は次のとおりです。

| 指標 | 正常 | 注意 | 深刻 |
|---------------------|------|-------|-------|
| cpuCostopPctPerVcpu | 3%以下 | 3～10% | 10%以上 |
| cpuReadinessPerVcpu | 5%以下 | 5～10% | 10%以上 |

cpuCostopPctPerVcpu が深刻な水準の場合は、仮想マシンに割り当てたvCPU数を減らすか、別のホストへ移すことを検討してください。cpuReadinessPerVcpu が深刻な水準の場合は、ホストのCPUリソース不足または仮想マシンの再配置を検討します。

`memVmmemctl`、`memSwapped`、`memCompressed` が増える場合は、ホストのメモリ逼迫が考えられます。圧縮は通常スワップより先に発生するため、`memCompressed` が増加した後に `memSwapped` まで増える場合は、メモリ不足が深刻化している状態です。

vCenterが提供していないカウンターは、空の値として収集します。

vm_vcenter_inventory

vCenterサーバー自体の構成情報です。管理対象オブジェクト数、アクティブなアラーム数、証明書とライセンスの有効期限情報を提供します。vCenter証明書の期限切れのように、あらかじめ備える必要のある項目を点検する際に使用します。2.9.23で追加したカテゴリーであり、表のすべてのフィールドが新規です。

- 収集対象: VMware vCenter

| Field | Type | Unit | Description |
|--------------------------------|--------|-------|---|
| <code>vCenterHostname</code> | string | - | vCenterサーバーのホスト名。vCenterを識別する代表的な名前 |
| <code>fqdn</code> | string | - | vCenterサーバーのFQDN（正規ドメイン名）。DNSに登録されている場合にのみ収集 |
| <code>ip</code> | string | - | vCenterサーバーの代表IPアドレス |
| <code>allIPs</code> | string | - | vCenterサーバーに接続可能なすべてのIPアドレスの一覧 |
| <code>connectionAddress</code> | string | - | エージェントがvCenter APIへの接続に使用したアドレス（IPまたはホスト名） |
| <code>uuid</code> | string | - | vCenterサーバーの固有識別子。サーバーの移行や名前の変更に関係なく、同じインスタンスを識別 |
| <code>overallHealth</code> | string | - | vCenterインベントリ全体の総合状態。 <code>green</code> ・ <code>yellow</code> ・ <code>red</code> のうち最も高い深刻度を表示 |
| <code>redAlarmCount</code> | string | count | 現在有効になっている危険（Red）アラームの数 |
| <code>yellowAlarmCount</code> | string | count | 現在有効になっている警告（Yellow）アラームの数 |

| Field | Type | Unit | Description |
|--------------------------|--------|-------|--|
| alarmCount | string | count | 現在有効になっている全アラームの数 |
| hostCount | string | count | vCenterで管理中のESXiホスト数 |
| vmCount | string | count | vCenterで管理中の仮想マシン数 |
| datacenterCount | string | count | 登録されたデータセンター数 |
| clusterCount | string | count | 登録されたクラスター数 |
| datastoreCount | string | count | 登録されたデータストア数 |
| networkCount | string | count | 登録されたネットワーク数 |
| resourcePoolCount | string | count | 登録されたリソースプール数 |
| folderCount | string | count | vCenterインベントリのフォルダー数 |
| certificateDaysRemaining | string | count | vCenter HTTPS証明書の期限切れまでの残り日数 |
| certificateExpiration | string | - | vCenter HTTPS証明書の期限切れ日時 |
| certificateValidFrom | string | - | vCenter HTTPS証明書の発行開始日時 |
| certificateSubject | string | - | vCenter HTTPSサーバー証明書のサブジェクト（DN）情報 |
| certificateIssuer | string | - | vCenter HTTPSサーバー証明書を発行したIssuer（CA）情報 |
| certificateThumbprint | string | - | vCenter HTTPS証明書のSHA-256フィンガープリント |
| licenseExpiration | string | - | vCenterライセンスの期限切れ日時。永久ライセンスの場合は空の可能性あります |
| licenseEdition | string | - | 適用されたvCenterライセンスのエディション |
| licenseName | string | - | 適用されたvCenterライセンスの名前 |

| Field | Type | Unit | Description |
|----------------|--------|-------|--|
| licenseTotal | string | count | ライセンスが提供する総割り当て数量 |
| licenseUsed | string | count | 現在使用中のライセンス数量 |
| version | string | - | vCenterサーバーのバージョン |
| build | string | - | vCenterサーバーのビルド番号 |
| fullName | string | - | VMwareが提供する製品名とバージョンの完全な文字列 |
| apiVersion | string | - | vSphere Web Services APIのバージョン |
| deploymentType | string | - | vCenterのデプロイ形態（例: Embedded PSC） |
| timeZone | string | - | vCenterアプライアンスに設定された標準時間帯 |
| agentName | string | - | VMware情報を収集しているエージェントがインストールされたサーバーのホスト名 |

一部の項目は、vSphere 7以上のアプライアンスAPIでのみ提供します。該当のAPIを使用できない環境では、値が空であるか、代替値として表示します。

収集するかどうかは、次のオプションで調整します。

whatap.conf

```
vm.inventory.vcenter.enabled=true # 収集するかどうか（デフォルト値: true）
```

vm_vhost_inventory

ESXiホストの構成情報です。ホスト1台が1行になり、値が変わったときにのみ送信します。ホストがどのvCenter・データセンター・クラスターに属するかから、CPU・メモリ・GPU・ネットワークの構成と運用状態まであわせて提供します。

- 収集対象: VMware ESXi

| Field | Type | Unit | Description |
|--------------------|--------|------|--|
| vCenterServerIp | string | - | 該当のESXiホスト情報を収集したvCenterサーバーのIPアドレス。複数のvCenterを統合収集する環境で、ホストがどのvCenterに属するかを区別する基準 |
| dataCenterName | string | - | vCenterインベントリ構造上、ホストが含まれるデータセンター名 |
| clusterName | string | - | ホストが所属するクラスター名。単独ホストの場合やクラスターに含まれない場合は、空の値または None |
| folder | string | - | vSphereインベントリでホストが位置するホストフォルダーのパス。データセンター配下のホストフォルダー、またはユーザーが作成した管理フォルダーを基準に表示し、クラスター・リソースプール・データストアなど実際のリソース構成位置とは別に解釈します |
| vHostName | string | - | vCenterで識別されるESXiホスト名または接続アドレス。通常はホストIPまたはFQDNの形式 |
| esxiHostNameFqdn | string | - | ESXiホストの完全修飾ドメイン名。DNSまたはホスト名の設定に応じて表示 |
| esxiHostNameShort | string | - | ESXiホストの短いホスト名。FQDNからドメインを除いた名前 |
| esxiHostNameDomain | string | - | ESXiホスト名に設定されたドメイン領域。ドメインが設定されていない場合は空の値 |
| esxiManagementIp | string | - | ESXiホストの管理用IPアドレス。vCenter接続、管理ネットワーク、API通信などに使用する代表管理IP |
| esxiVmlps | string | - | ホストに構成されたVMkernelインターフェイスのIP情報。管理・vMotion・vSAN・iSCSI/NFSなどのネットワーク用途で使用 |
| manufacturer | string | - | ホストハードウェアのメーカー（例: HP、Dell、Lenovo） |
| model | string | - | ホストハードウェアのモデル名。サーバーモデルまたはワークステーションモデルを表示 |

| Field | Type | Unit | Description |
|-----------------------|--------|-------|--|
| hostType | string | - | ホストの構成形態。クラスターに属する場合は cluster、単独ホストの場合は standalone |
| serialNumber | string | - | ホスト機器のシリアル番号。資産管理、保守契約、ベンダーサポート依頼時の識別情報として使用 |
| uuid | string | - | ホストシステムの固有識別子。名前が同じ場合やIPが変わった場合でも、機器を識別する補助情報 |
| cpuModel | string | - | ホストに搭載されたCPUのモデル名（例: Intel Xeon、Intel Core、AMD EPYC） |
| cpuSockets | string | - | 物理CPUソケット数。ライセンス、容量の算定、物理CPU構成の確認に使用 |
| cpuCores | string | - | ホスト全体の物理CPUコア数。仮想マシンに割り当て可能なリソースとCPU容量算定の基準 |
| cpuThreads | string | - | ハイパースレッディングなどを含む論理CPUスレッド数。実際に仮想マシンをスケジューリングできる論理CPU単位 |
| hyperThreadingEnabled | string | - | ホストでハイパースレッディングが有効かどうか。cpuCores と cpuThreads の値の差を解釈する際に使用 |
| cpuTotalMhz | string | MHz | ホスト全体のCPUの総処理容量。CPUコア数とクロック情報を基に算定 |
| totalMemoryGb | string | GiB | ホストに搭載された全体のメモリ容量。仮想マシンを配置できる容量とメモリリソース計画の基準 |
| gpuCount | string | count | ホストで確認された物理GPUデバイス数。PCIデバイス情報のうちVGA・3D Controller・Display Controller系のデバイスを基準に算定 |
| gpuDevices | string | - | ホストで確認されたGPUデバイスの一覧。メーカー、モデル名、PCIデバイス識別子を表示（例: NVIDIA A100、NVIDIA T4、NVIDIA L40） |

| Field | Type | Unit | Description |
|-----------------|--------|------|---|
| gpuProfiles | string | - | ホストで確認可能なvGPUプロファイル、またはShared Passthrough GPUタイプの候補一覧。NVIDIA vGPU Manager、ESXi・vCenterのバージョン、ライセンスおよびAPIの公開方式によっては値がない場合があります |
| vmGuestCount | string | - | 該当のESXiホストに接続された仮想マシンオブジェクトの数。ホストごとの仮想マシン配置状況と密集度を把握する際に使用 |
| datastoreCount | string | - | ホストからアクセス可能なデータストア数。ホストが使用できるストレージ接続数と構成規模を把握する際に使用 |
| dataStores | string | - | ホストがアクセス可能なデータストアの一覧。仮想マシンのディスクを保存できるストレージリソースの一覧 |
| totalCapacityGb | string | GiB | ホストからアクセス可能なデータストアの総容量。共有データストアが含まれる場合があるため、ホスト単独の容量と断定しないよう注意が必要 |
| networkCount | string | - | ホストに接続されたネットワークまたはポートグループの数 |
| networks | string | - | ホストに接続されたネットワークまたはポートグループの一覧。仮想マシンのネットワーク接続可能範囲を確認する際に使用 |
| nicCount | string | - | ホストに構成された物理NICの数。管理・仮想マシン・vMotion・ストレージの各ネットワークにおける物理接続規模を確認する基準 |
| nics | string | - | ホストに構成された物理NICの一覧 |
| vSwitchCount | string | - | ホストに構成された仮想スイッチの数。標準vSwitchまたは分散スイッチの使用有無と、ネットワーク構成規模を把握する際に使用 |
| vSwitchs | string | - | ホストに構成されたvSwitchの一覧 |
| networkInfo | string | - | ホストに構成されたvSwitchまたはネットワークの構成情報 |
| vMotionEnabled | string | - | ホストでvMotion機能が有効かどうか。仮想マシンを無停止で移動で |

| Field | Type | Unit | Description |
|-----------------|--------|------|---|
| | | | きるかどうかを判断する際に使用 |
| haEnabled | string | - | ホストが属するクラスターでHA機能が有効かどうか。単独ホストの場合やクラスターHAが無効の場合は None または false |
| productVersion | string | - | ESXi製品のバージョン。パッチ水準、機能のサポート有無、互換性の判断に使用 |
| buildNumber | string | - | ESXiのビルド番号。詳細なパッチバージョンの確認、セキュリティ脆弱性への対応、互換性の検討における基準 |
| license | string | - | ホストに適用されたVMwareライセンスの種類。使用できる機能の範囲と運用上の制約を判断する際に使用 |
| bootTime | string | - | ホストが最後に起動した時刻。長期運用の有無や、障害後の復旧時点の確認に使用 |
| upTime | string | - | ホストが最後の起動以降、継続して稼働している時間。長期間再起動していないサーバーの識別に使用 |
| timezone | string | - | ホストまたはvCenter基準のタイムゾーン情報。イベント発生時刻やパフォーマンスデータの時刻を解釈する基準 |
| connectionState | string | - | vCenter基準のホスト接続状態。connected ・ disconnected ・ notResponding などに表示し、収集の可否と直接関係します |
| powerState | string | - | ホストの電源状態。通常は poweredOn が正常な運用状態 |
| overallStatus | string | - | vCenterが判断したホストの総合状態。green ・ yellow ・ red ・ gray などに表示し、警告・障害の有無を素早く判断する際に使用 |
| maintenanceMode | string | - | ホストがメンテナンスモードかどうか。true の場合、仮想マシンの移動やパッチ作業などのため運用投入が制限されている状態の可能性があります |

vm_vmguest_inventory の vHostKey で、仮想マシンの一覧とこの表のホストの一覧を紐づけできます。

vm_vmguest_inventory

仮想マシンの構成情報です。仮想マシン1台が1行になり、値が変わったときにのみ送信します。

- 収集対象: VMware ESXi

| Field | Type | Unit | Description | 備考 |
|-------------------|--------|------|--|--------------|
| vHostKey | - | - | 仮想マシンが実行中のESXiホストの識別キー。
vm_vhost_inventoryのキーと同じ値 | 2.9.23
新規 |
| vmName | string | - | vCenterまたはESXiで管理される仮想マシンの表示名。運用者がvSphere環境で識別する代表的な名前 | |
| guestHostname | string | - | ゲストオペレーティングシステム内部で認識されるホスト名。VMware Toolsを通じて収集するため、Toolsの状態やゲストの設定によっては値がない場合があります | |
| vCenterServerInfo | string | - | 該当の仮想マシン情報を収集したvCenterサーバー情報。複数のvCenterを統合収集する環境で、仮想マシンがどのvCenterに属するかを区別する基準 | |
| datacenter | string | - | 仮想マシンが含まれるvCenterデータセンター名 | |
| folder | string | - | vSphereインベントリで仮想マシンが位置するVMフォルダーのパス。VMs and Templates観点の論理的なフォルダー位置であり、ホスト・クラスター・リソースプールのような実行位置やリソース割り当て位置とは別のもの | |
| cluster | string | - | 仮想マシンが属するESXiクラスター名。独立したホスト環境の場合やクラスターに含まれない場合は、値がない場合があります | |
| vHostInfo | string | - | 仮想マシンが実行中、または登録されているESXiホストの情報。収集基準によって、ホスト名・IP・FQDNなど表示形式が異なる場合があります | |

| Field | Type | Unit | Description | 備考 |
|----------------|--------|-------|---|----|
| resourcePool | string | - | 仮想マシンが属するリソースプール名。リソースポリシー、割り当て構造、サービス単位のグループを把握する際に使用 | |
| ipAddress | string | - | ゲストオペレーティングシステムで確認される代表IPアドレス。VMware Toolsの状態、ネットワーク設定、複数NIC構成によっては、値がないか代表IPのみ表示される場合があります | |
| guestOS | string | - | 仮想マシンに設定されたゲストオペレーティングシステムの種類。vSphereで選択したOSタイプが基準のため、実際のOS情報と異なる場合があります | |
| guestFullName | string | - | ゲストオペレーティングシステムの詳細名。VMware Toolsまたは仮想マシンの設定情報で確認 | |
| guestId | string | - | vSphereで使用するゲストオペレーティングシステムの識別子（例: rhel8_64Guest、windows9Server64Guest） | |
| vcpu | string | count | 仮想マシンに割り当てられた仮想CPU数 | |
| sockets | string | count | 仮想マシンに設定された仮想CPUソケット数。vCPUの構成方式と、ゲストオペレーティングシステムのCPU認識構造を確認する際に使用 | |
| coresPerSocket | string | count | 仮想マシンに設定されたソケットあたりのコア数。ゲストオペレーティングシステムが認識するCPUトポロジーとライセンスポリシーの確認に使用 | |
| totalMemory | string | MiB | 仮想マシンに割り当てられた総メモリ容量。リソース割り当て規模とメモリ増設の要否を判断する基準 | |
| vGpuCount | string | count | 仮想マシンに割り当てられたvGPU数。Virtual PCI Passthroughデバイスとして接続されたvGPU数を基準に算定し、割り当てられていない仮想マシンは0 | |

| Field | Type | Unit | Description | 備考 |
|------------------|--------|------|---|----|
| vGpuProfiles | string | - | 仮想マシンに割り当てられたvGPUプロファイル情報（例: <code>grid_a100-1-5c</code> 、 <code>grid_t4-2q</code> ）。vCenter・ESXiのバージョン、NVIDIA vGPU Managerの構成、APIの公開方式によっては、値がないか表示形式が異なる場合があります | |
| provisionedSpace | string | GiB | 仮想マシンにプロビジョニングされた全体のストレージ容量。Thin Provisioning環境では実際の使用量より大きい場合があります | |
| usedSpace | string | GiB | 仮想マシンが実際に使用中のストレージ容量。データストア使用量の分析と容量管理に使用 | |
| datastore | string | - | 仮想マシンが使用中のデータストアの一覧。ディスクファイルと設定ファイルが位置するストレージ構成を確認する際に使用 | |
| network | string | - | 仮想マシンに接続されたネットワークまたはポートグループの情報。ネットワーク接続構成と、サービス網・管理網の区分を確認する際に使用 | |
| vmPathName | string | - | 仮想マシンの構成ファイルが位置するデータストアのパス。通常は <code>[datastore] path/vm.vmx</code> の形式 | |
| vmToolsVersion | string | - | 仮想マシンにインストールされたVMware Toolsのバージョン。ゲスト情報の収集、IPの確認、ハートビート状態の確認可否に関係します | |
| template | string | - | 該当のオブジェクトがVMテンプレートかどうか。 <code>true</code> の場合は、実行中の仮想マシンではなくデプロイ用のテンプレート | |
| firmware | string | - | 仮想マシンのファームウェアの種類。 <code>bios</code> または <code>efi</code> で表示し、起動方式、セキュアブート、互換性の確認に使用 | |
| version | string | - | 仮想マシンの仮想ハードウェアバージョン。ESXi・vCenterの互換性、サポート機能、マイグレーションの可否を判断 | |

| Field | Type | Unit | Description | 備考 |
|---------------------|--------|-------|--|----|
| | | | する際に使用 | |
| cpuHotAddEnabled | string | - | 仮想マシンの実行中にvCPUを追加する機能が有効かどうか。trueの場合は、電源を切らずにCPUを追加できます | |
| cpuHotRemoveEnabled | string | - | 仮想マシンの実行中にvCPUを削除する機能が有効かどうか。サポート対象のオペレーティングシステムと設定によって、実際の動作可否が異なる場合があります | |
| memoryHotAddEnabled | string | - | 仮想マシンの実行中にメモリを追加する機能が有効かどうか。trueの場合は、電源を切らずにメモリを増設できます | |
| maxMksConnections | string | count | 仮想マシンのコンソールに同時接続できる最大MKS接続数。コンソール接続の制限と運用アクセス制御を確認する際に使用 | |
| creationDate | string | - | 仮想マシンが作成された日時。ライフサイクル管理と新規作成された仮想マシンの追跡に使用 | |
| uuid | string | - | 仮想マシンのBIOS UUID。ゲストオペレーティングシステム内部からも参照でき、複製や再作成の方式によっては重複する可能性があります | |
| instanceUuid | string | - | vCenterが仮想マシンインスタンスを識別するために使用するUUID。同一vCenter内で仮想マシンを識別する主要な基準 | |
| annotation | string | - | vSphereの仮想マシン設定に入力した説明またはメモ | |
| powerState | string | - | 仮想マシンの電源状態。poweredOn・poweredOff・suspendedなどで表示 | |
| overallStatus | string | - | 仮想マシンオブジェクトの全体状態。green・yellow・red・grayなどで表示し、アラームや構成上の問題の有無を素早く確認する際に使用 | |

| Field | Type | Unit | Description | 備考 |
|----------------------|--------|------|--|----|
| vmGuestState | string | - | VMware Toolsまたはゲストオペレーティングシステムの観点で確認される状態。 <code>running</code> ・ <code>notRunning</code> ・ <code>shuttingDown</code> ・ <code>standby</code> などに表示 | |
| guestHeartbeatStatus | string | - | VMware Toolsで確認されるゲストオペレーティングシステムのハートビート状態。 <code>green</code> ・ <code>yellow</code> ・ <code>red</code> ・ <code>gray</code> などに表示 | |

`vHostKey` で、仮想マシンの一覧とホストの一覧を紐づけできます。特定のホスト上の仮想マシンを一度に探す際に使用します。

- ❗ 既存のvCenterモニタリング（フィーチャプロジェクト）は2026年12月31日をもってサービスを終了し、サーバーモニタリング製品のvCenter機能に置き換えられる予定です。詳細は[vCenterモニタリングドキュメント](#)を参照してください。

GPUメトリクス

WhaTapサーバーモニタリングのGPUパフォーマンスメトリクスは、NVIDIA GPU環境においてGPUサーバー、個別GPU、GPU使用プロセス、GPU障害イベントの観点からパフォーマンスおよび状態情報を収集して提供します。GPU使用率、演算リソース活用度、メモリ使用量、電力、温度、クロック、PCIe/NVLink転送量、ECCエラー、パフォーマンス制限状態、Xidイベントなどを確認でき、GPUサーバー全体の活用水準の把握から個別GPUのボトルネック分析、プロセス単位の原因追跡、ドライバー・ハードウェアの異常イベント確認まで段階的に分析できます。一部の指標はPhysical GPUのみで収集され、MIG環境では収集対象と解釈基準が異なる場合があるため、GPU Typeと収集対象を併せて確認することをお勧めします。また、XidイベントはNVIDIAドライバーがシステムログに記録した障害/イベント履歴に基づいて収集します。原因分析の際は、イベント発生時刻、GPU識別情報、Xid Code、PID、Task Name、詳細メッセージを併せて確認してください。

❗ GPUモニタリングを有効にするには、エージェント設定が必要です。詳細は[GPU機能設定](#)を参照してください。

GPUパフォーマンスメトリクスは分析の観点に応じて、サーバー全体のGPU集計、個別GPU詳細、GPU使用プロセス、GPU Xidイベント基準の4つのカテゴリで提供します。

- **infra_gpu**

サーバーに搭載されたすべてのGPUのステータスを集計し、**GPUサーバー全体の観点からパフォーマンスと状態を確認できるカテゴリ**です。GPU使用率、メモリ、電力、温度、クロック、PCIe/NVLink、ECC、Violation状態を平均・合計・最大値基準で提供し、GPUサーバー全体の活用水準とボトルネックの可能性を素早く確認できます。

- **infra_gpu_id**

個別GPU単位のパフォーマンスと状態を提供するカテゴリです。GPU別の使用率、演算リソース活用度、メモリ、温度、電力、クロック、PCIe/NVLink、ECC、Violation状態を確認し、特定のGPUで発生するボトルネックや制約状態を分析できます。Physical GPUとMIGインスタンスによって収集可能な指標が異なる場合があるため、GPU Typeと収集対象を併せて確認する必要があります。

- **infra_gpu_process**

GPUを使用するプロセス単位のリソース使用情報を提供するカテゴリです。PID、プロセス名、ユーザー、GPU UUIDとともにSM使用率、メモリコントローラー使用率、エンコーダー/デコーダー使用率、FBメモリ使用量などを確認し、どのプロセスがGPUリソースを使用しているかを追跡できます。ただし、一部のプロセス別GPU使用率指標はGPU全体の指標と測定基準が異なる場合があるため、個別プロセスの寄与度を判断する際はGPU全体の指標と

合わせて解釈することをお勧めします。

• **infra_gpu_xid**

NVIDIAドライバが記録したGPU Xidイベント情報を提供するカテゴリです。 `/var/log/messages` またはシステムログに記録された `NVRM: Xid` ログを基に、Xid Code、GPU Index、PCI Bus ID、発生時刻、PID、Task Name、詳細メッセージを収集し、GPUドライバー、ハードウェア、PCIe、メモリ、アプリケーションエラーなどのGPU異常イベントを追跡できます。すべてのXidイベントが直ちにハードウェア障害を意味するわけではないため、Xid Codeの意味、発生頻度、同時点のGPUパフォーマンス指標、プロセス情報、システムログを併せて確認して解釈することをお勧めします。

GPUメトリクス詳細

カテゴリ別の収集指標の詳細内容は次のとおりです。

infra_gpu

サーバーに搭載されたGPU全体を集計した使用状態を収集するカテゴリです。GPU使用率、メモリ使用量、電力、温度、クロック、PCIe/NVLink処理量、ECC、violation状態などをサーバー全体のGPU観点で平均、合計、最大値などに再構成して提供します。GPUサーバー全体の活用水準とボトルネック、制約状態を把握する際に使用します。

- DCP（Datacenter Profiling）指標の収集には、nvidia-dcgmサービス（またはnv-hostengineプロセス）が起動している必要があります。
- Agent 2.9.16以上のバージョンでnvidiaav2.collector=trueを設定すると、接続可能なNVML、DCGM Libraryを通じてメトリクスデータを自動的に収集します。（nvidia-smiまたはdcgmcliクエリは使用しません。）
- デフォルト収集周期：30s

| Field
カテゴリフィールド名 | Title
パフォーマンスサマリー/パフォーマンス詳細/メトリクスエクスプローラーの指標名 | Unit | Description | 備考 | メトリクス収集条件 | 最小サポートエージェントバージョン |
|---------------------|--|--------|-------------|----|-----------|-------------------|
| name_50 | GPU Name | string | 該当GPUのモデル名を | | | 2.9.3 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|--------|---|--------------------------------|--|-----------------------------------|
| | | | 表す値です。ドライバ
ーバージョンまたは収
集経路によって表示文
字列が若干異なる場合
があります。 | | | |
| model_family | GPU Model
Family | string | ドライバーバージョ
ン、ファームウェア、
収集経路によって異な
る表示となりうるGPU
モデル名を、A100、
H100、L40Sなどの代
表的なファミリー名に
正規化した値です。モ
デル別の集計、フィル
タリング、比較分析を
一貫して実行するた
めの識別子として使用
します。 | | | 2.9.7 |
| gpu_count | GPU Count | string | サーバーで認識され
ているPhysical GPUの
数を表す値です。全
GPU平均値、合計量、
比率指標を解釈する
際の基準となります。 | | | 2.9.3 |
| gpu_utilization | GPU Utilization | % | サーバー内の個別GPU
活用率の平均値です。
Physical GPU環境で
は一般的なGPU Util値 | 搭載
Physical
GPUのAVG
値 | MIG有効環境
では、
nvidia-dcgm
serviceまた | 2.9.6 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|------|--|-------------------------|--------------------------|-----------------------------------|
| | | | を意味し、MIG環境では個別インスタンスのGR Engine Active値を代表GPU使用率として活用できます。サーバー全体のGPUの全般的な活用水準を示す指標です。 | | はnv-hostengineプロセスの起動が必須 | |
| enc_util_206 | Encoder Util | % | サーバー内の個別GPUのエンコーダー（Encoder）エンジン活用率の平均値です。動画エンコード作業がGPUでどの程度使用されているかを示します。値が高いほどNVENCファミリーエンジンの使用比率が高いことを意味します。 | 搭載
Physical GPUのAVG値 | | 2.9.3 |
| dec_util_207 | Decoder Util | % | サーバー内の個別GPUのデコーダー（Decoder）エンジン活用率の平均値です。動画デコード作業がGPUでどの程度使用されているかを示します。値が高いほどNVDECファミリーエンジンの使用比率が高 | 搭載
Physical GPUのAVG値 | | 2.9.3 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|-----------------------|--|------|--|-------------------------|---|-----------------------------------|
| | | | いことを意味します。 | | | |
| gr_engine_active_1001 | GR Engine Active Util | % | サーバー内の個別GPUのGraphics/Compute Engine活性比率の平均値です。MIGインスタンス環境では、そのインスタンスのGPU使用率を代表的に解釈できる指標として活用します。 | 搭載
Physical GPUのAVG値 | nvidia-dcgm serviceまたはnv-hostengineプロセスの起動が必須 | 2.9.3 |
| sm_active_1002 | SM Active Util | % | サーバー内の個別GPUのSM（Streaming Multiprocessor）活性比率の平均値です。実際の演算処理に使用されたSMリソースの一般的な使用水準を示します。 | 搭載
Physical GPUのAVG値 | nvidia-dcgm serviceまたはnv-hostengineプロセスの起動が必須 | 2.9.3 |
| sm_occupancy_1003 | SM Occupancy | % | サーバー内の個別GPUのSM Occupancyの平均値です。アクティブワープがSMにどの程度充填されているかを示し、単純な活性率とは異なりSMリソース活用密度を表します。 | 搭載
Physical GPUのAVG値 | nvidia-dcgm serviceまたはnv-hostengineプロセスの起動が必須 | 2.9.3 |
| tensor_active_ | Tensor Core Util | % | サーバー内の個別GPU | 搭載 | nvidia-dcgm | 2.9.3 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|----------------------|--|------|--|--------------------------------|--|-----------------------------------|
| 1004 | | | のTensor Core活性比
率の平均値です。AI/
ディープラーニング演
算のようにTensor
Coreを使用するワー
クロードの比率を把握
する際に役立ちます。 | Physical
GPUのAVG
値 | serviceまた
はnv-
hostengine
プロセスの起
動が必須 | |
| fp64_active_10
06 | FP64 Compute
Util | % | サーバー内の個別GPU
のFP64演算活性比率
の平均値です。倍精度
(double precision)
演算負荷水準を示しま
す。 | 搭載
Physical
GPUのAVG
値 | nvidia-dcgm
serviceまた
はnv-
hostengine
プロセスの起
動が必須 | 2.9.3 |
| fp32_active_10
07 | FP32 Compute
Util | % | サーバー内の個別GPU
のFP32演算活性比率
の平均値です。単精度
(single precision)
演算負荷水準を示しま
す。 | 搭載
Physical
GPUのAVG
値 | nvidia-dcgm
serviceまた
はnv-
hostengine
プロセスの起
動が必須 | 2.9.3 |
| fp16_active_10
08 | FP16 Compute
Util | % | サーバー内の個別GPU
のFP16演算活性比率
の平均値です。半精度
(half precision) 演
算負荷水準を示し、AI
推論/学習ワークロー
ドで重要になる場合が
あります。 | 搭載
Physical
GPUのAVG
値 | nvidia-dcgm
serviceまた
はnv-
hostengine
プロセスの起
動が必須 | 2.9.3 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|----------------------|--|------|---|--------------------------------|---|-----------------------------------|
| memory_copy_util_204 | Memory Copy Util | % | サーバー内の個別GPUのメモリコピーエンジン活用率の平均値です。GPUメモリとGPU内部演算領域間のデータ移動、Host ↔ Deviceコピー、Device ↔ Deviceコピーなどのメモリコピーやデータ移動経路がどの程度使用されているかを示す指標です。値が高いほど、GPU演算自体よりデータ移動負荷が大きいか、メモリコピー作業がボトルネックになる可能性があります。この値はメモリ容量使用率ではなく、メモリコピー/転送エンジンの活動水準として解釈する必要があります。 | 搭載
Physical
GPUのAVG
値 | | 2.9.3 |
| dram_active_1005 | DRAM Active Util | % | サーバー内の個別GPUのDRAM活性比率の平均値です。GPU DRAMメモリサブシステムがアクティブ状態だった比率を示します。GPUメモリ帯域幅がどの程 | 搭載
Physical
GPUのAVG
値 | nvidia-dcgm serviceまたはnv-hostengineプロセスの起動が必須 | 2.9.3 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|------|--|--------------------------------|---------------|-----------------------------------|
| | | | 度活発に使用されているかを示す指標で、メモリ読み取り/書き込み要求が多いか、メモリアクセス中心のワークロードで高くなる傾向があります。高い値が継続する場合、演算性能よりGPUメモリ帯域幅がボトルネックになっている状況かもしれません。この値はFB Memory Usedのようなメモリ使用容量ではなく、GPU DRAMが実際にどの程度バジーに動作したかを示す活性度指標です。 | | | |
| fb_total_250 | FB Total Memory | MiB | サーバー内の個別GPUのFB（Frame Buffer）全体メモリ容量を合計した値です。サーバー全体のGPUメモリ総量を示します。 | 搭載
Physical
GPUの
SUM値 | | 2.9.3 |
| fb_free_251 | FB Free Memory | MiB | サーバー内の個別GPUのFB空きメモリ容量を合計した値です。サーバー全体で利用可能なGPUメモリ総量を示 | 搭載
Physical
GPUの
SUM値 | | 2.9.3 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|------|--|--------------------------------|---------------|-----------------------------------|
| | | | します。 | | | |
| fb_used_252 | FB Used
Memory | MiB | サーバー内の個別GPU
のFB使用メモリ容量
を合計した値です。サ
ーバー全体のGPUメモ
リ使用総量を示しま
す。 | 搭載
Physical
GPUの
SUM値 | | 2.9.3 |
| fb_resv_253 | FB Reserved
Memory | MiB | サーバー内の個別GPU
のFB予約メモリ容量
を合計した値です。シ
ステム/ドライバー/フ
ァームウェアなどによ
って予約されたGPUメ
モリ総量を示します。 | 搭載
Physical
GPUの
SUM値 | | 2.9.3 |
| fb_USDP_254 | FB Memory
Usage | % | サーバー全体のFBメ
モリ使用率を示す指標
です。個別GPUのメモ
リ使用率を単純平均せ
ず、FB Used合計 / FB
Total合計 * 100で再計
算した値です。 | 搭載
Physical
GPUのAVG
値 | | 2.9.3 |
| bar1_total_90 | BAR1 Total
Memory | MiB | サーバー内の個別GPU
のBAR1全体容量を合
計した値です。BAR1
はホストがGPUメモリ
にアクセスするために
使用するメモリマッピ | 搭載
Physical
GPUの
SUM値 | | 2.9.3 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------------------|--|-------|--|--------------------------------|---------------|-----------------------------------|
| | | | ング領域で、サーバー
全体のBAR1総量を示
します。 | | | |
| bar1_used_92 | BAR1 Used
Memory | MiB | サーバー内の個別GPU
のBAR1使用量を合計
した値です。サーバー
全体で現在使用中の
BAR1メモリ総量を示
します。 | 搭載
Physical
GPUの
SUM値 | | 2.9.3 |
| bar1_free_93 | BAR1 Free
Memory | MiB | サーバー内の個別GPU
のBAR1空き容量を合
計した値です。サーバ
ー全体で利用可能な
BAR1総量を示しま
す。 | 搭載
Physical
GPUの
SUM値 | | 2.9.3 |
| bar1_usdp | BAR1 Memory
Usage | % | サーバー全体のBAR1
使用率を示す指標で
す。個別GPUの比率を
単純平均せず、BAR1
Used合計 / BAR1
Total合計 * 100で再計
算した値です。 | 搭載
Physical
GPUのAVG
値 | | 2.9.3 |
| ecc_sbe_aggre
gate_total_312 | ECC SBE Total | count | サーバー内の個別GPU
のECC Single Bit Error
累積カウンタを合計
した値です。サーバー
全体で累積された単一 | 搭載
Physical
GPUの
SUM値 | | 2.9.3 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------------------|--|-------|--|--------------------------------|---------------|-----------------------------------|
| | | | ビットECCエラーの総
量を示します。 | | | |
| ecc_dbe_aggre
gate_total_313 | ECC DBE Total | count | サーバー内の個別GPU
のECC Double Bit
Error累積カウンター
を合計した値です。サ
ーバー全体で累積され
た二重ビットECCエラ
ーの総量を示します。 | 搭載
Physical
GPUの
SUM値 | | 2.9.3 |
| ecc_sbe_aggre
gate_delta_312 | ECC SBE Delta | count | 収集区間中にサーバー
内の個別GPUのECC
Single Bit Error増加
分を合計した値です。直
近の区間で新たに発生
した単一ビットECCエ
ラー量を示します。 | 搭載
Physical
GPUの
SUM値 | | 2.9.16 |
| ecc_dbe_aggre
gate_delta_313 | ECC DBE Delta | count | 収集区間中にサーバー
内の個別GPUのECC
Double Bit Error増加
分を合計した値です。
直近の区間で新たに発
生した二重ビットECC
エラー量を示します。 | 搭載
Physical
GPUの
SUM値 | | 2.9.16 |
| gpu_temp_150 | GPU
Temperature | °C | サーバー内の個別GPU
温度の最大値を示す指
標です。サーバー全体
のGPUの中で最も高い | 搭載
Physical
GPUのMAX
値 | | 2.9.10 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|-----------------------------|--|------|--|-------------------------|---------------|-----------------------------------|
| | | | 温度を代表し、特定GPUの過熱の有無を素早く識別するために使用します。 | | | |
| memTemp_140 | GPU Memory Temperature | °C | サーバー内の個別GPUメモリ温度の最大値を示す指標です。一般的にHBMまたはGDDRメモリ基準の温度で、メモリの発熱状態や冷却異常の有無を確認する際に使用します。メモリ集約型ワークロードではGPUコア温度より先に上昇することがあるため、合わせて確認することをお勧めします。 | 搭載
Physical GPUのMAX値 | | 2.9.16 |
| power_usage_155 | Power Usage | watt | サーバー内の個別GPUの電力使用量を合計した値です。サーバー全体のGPUが消費している総電力をワット（W）単位で示します。 | 搭載
Physical GPUのSUM値 | | 2.9.3 |
| energy_cumulative_daily_kwh | Energy Cumulative | kWh | 当日00時を基準に累積されたサーバー全体GPUのエネルギー使用 | 搭載
Physical GPUの | | 2.9.16 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|------|--|--------------------------------|---------------|-----------------------------------|
| | | | 量を示す指標です。
NVIDIAドライバ/DCGMなどを通じて収集したpowerUsage値を収集周期単位で積算して計算した参考用推定値で、別途の電力計測器で測定した正確な電力量とは差異がある場合があります。GPU別の電力使用推移と日次使用パターンを参考にする用途で活用します。 | SUM値 | | |
| fan_speed_191 | Fan Speed | % | サーバー内の個別GPUのファン速度の平均値です。ファンが存在するGPUモデルで冷却装置の動作水準を示します。 | 搭載
Physical
GPUのAVG
値 | | 2.9.3 |
| sm_clock_100 | SM Clock | MHz | サーバー内の個別GPUのSMクロックの平均値です。演算ユニットが動作中の平均コアクロック水準を示します。 | 搭載
Physical
GPUのAVG
値 | | 2.9.3 |
| memory_clock_101 | Memory Clock | MHz | サーバー内の個別GPUのメモリクロックの平 | 搭載
Physical | | 2.9.3 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|------------------------|--|-------------|--|--------------------------------|--|-----------------------------------|
| | | | 均値です。GPUメモリ
の動作速度水準を示し
ます。 | GPUのAVG
値 | | |
| video_clock_10
2 | Video Clock | MHz | サーバー内の個別GPU
のビデオエンジンクロ
ックの平均値です。映
像処理関連エンジンの
動作速度水準を示しま
す。 | 搭載
Physical
GPUのAVG
値 | | 2.9.3 |
| pcie_tx_bytes_
1009 | PCIE TX | bytes/
s | サーバー内の個別GPU
のPCIE送信処理量を
合計した値です。GPU
からホストまたは外部
へ転送されたPCIEデ
ータ総量をbytes/s単
位で示します。 | 搭載
Physical
GPUの
SUM値 | nvidia-dcgm
serviceまた
はnv-
hostengine
プロセスの起
動が必須 | 2.9.3 |
| pcie_rx_bytes_
1010 | PCIE RX | bytes/
s | サーバー内の個別GPU
のPCIE受信処理量を
合計した値です。GPU
がホストまたは外部か
ら受信したPCIEデー
タ総量をbytes/s単位
で示します。 | 搭載
Physical
GPUの
SUM値 | nvidia-dcgm
serviceまた
はnv-
hostengine
プロセスの起
動が必須 | 2.9.3 |
| pcie_tx_rx_byt
es | PCIE Total | bytes/
s | サーバー内の個別GPU
のPCIE送受信処理量
を合計した値です。
PCIE TX + PCIE RXに | 搭載
Physical
GPUの
SUM値 | nvidia-dcgm
serviceまた
はnv-
hostengine | 2.9.16 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|--------------------------|--|---------|---|-------------------------|--|-----------------------------------|
| | | | 該当するサーバー全体のPCIeデータ移動総量です。 | | プロセスの起動が必須 | |
| nvlink_tx_bytes_1011 | NVLink TX | bytes/s | サーバー内の個別GPUのNVLink送信処理量を合計した値です。GPU間でNVLinkを通じて転送されたデータ総量をbytes/s単位で示します。 | 搭載
Physical GPUのSUM値 | nvidia-dcgm serviceまたはnv-hostengine プロセスの起動が必須 | 2.9.3 |
| nvlink_rx_bytes_1012 | NVLink RX | bytes/s | サーバー内の個別GPUのNVLink受信処理量を合計した値です。GPU間でNVLinkを通じて受信されたデータ総量をbytes/s単位で示します。 | 搭載
Physical GPUのSUM値 | nvidia-dcgm serviceまたはnv-hostengine プロセスの起動が必須 | 2.9.3 |
| nvlink_tx_rx_bytes | NVLink Total | bytes/s | サーバー内の個別GPUのNVLink送受信処理量を合計した値です。NVLink TX + NVLink RXに該当するサーバー全体のGPU間通信総量です。 | 搭載
Physical GPUのSUM値 | nvidia-dcgm serviceまたはnv-hostengine プロセスの起動が必須 | 2.9.16 |
| power_violation_rate_240 | Power Violation Rate | % | サーバー内の個別GPUの中で電力制限（power cap）違反比 | 搭載
Physical GPUのMAX | | 2.9.16 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|--|--|------|---|--------------------------------|---------------|-----------------------------------|
| | | | 率が最も高い値を代表
として示す指標です。
電力制約によりパフ
ォーマンス制限が発生
しているGPUがあるかど
うかを素早く識別する
ために使用します。 | 値 | | |
| thermal_violati
on_rate_241 | Thermal
Violation Rate | % | サーバー内の個別GPU
の中で熱制約
(thermal limit) 違
反比率が最も高い値を
代表として示す指標で
す。過熱によるパフ
ォーマンス制限の有無を
素早く識別するために
使用します。 | 搭載
Physical
GPUのMAX
値 | | 2.9.16 |
| low_util_violati
on_rate_244 | Low Util
Violation Rate | % | サーバー内の個別GPU
の中で低活用 (low
utilization) 関連違反
比率が最も高い値を代
表として示す指標で
す。設定された低活用
条件に該当するGPUが
あるかどうかを確認す
るために使用します。 | 搭載
Physical
GPUのMAX
値 | | 2.9.16 |
| board_limit_vi
olation_rate_2
43 | Board Limit
Violation Rate | % | サーバー内の個別GPU
の中でボード全体のハ
ードウェア限界 | 搭載
Physical
GPUのMAX | | 2.9.16 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|--------------------------------|--|------|--|--------------------------------|---------------|-----------------------------------|
| | | | (board limit) 関連
違反比率が最も高い値
を代表として示す指標
です。電源部・ボード
設計限界などボードレ
ベルの制約が最も多く
かかっているGPUを識
別する際に使用しま
す。 | 値 | | |
| sync_boost_violation_rate_242 | Sync Boost Violation Rate | % | サーバー内の個別GPU
の中で同期ブースト
(sync boost) 関連違
反比率が最も高い値を
代表として示す指標で
す。複数GPUの動作速
度を合わせるための制
約に最も大きく影響を
受けているGPUを識別
する際に使用します。 | 搭載
Physical
GPUのMAX
値 | | 2.9.16 |
| reliability_violation_rate_245 | Reliability Violation Rate | % | サーバー内の個別GPU
の中で信頼性
(reliability) 保護関
連違反比率が最も高い
値を代表として示す指
標です。安定性とハー
ドウェア保護のための
制約に最も大きく影響
を受けているGPUを識
別する際に使用しま | 搭載
Physical
GPUのMAX
値 | | 2.9.16 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|------------------------|--|------|---|-------------------------|---------------|-----------------------------------|
| | | | す。 | | | |
| power_violation_240 | Power Violation | ns | 収集区間中にサーバー内の個別GPUが電力制限（power cap）制約状態にあった時間を合計した値です。単位はns（ナノ秒）で、サーバー全体で電力制約によりパフォーマンス制限が発生した時間を総量の観点で示します。 | 搭載
Physical GPUのSUM値 | | 2.9.16 |
| thermal_violation_241 | Thermal Violation | ns | 収集区間中にサーバー内の個別GPUが熱制限（thermal limit）制約状態にあった時間を合計した値です。単位はns（ナノ秒）で、サーバー全体で過熱によりパフォーマンス制限が発生した時間を総量の観点で示します。 | 搭載
Physical GPUのSUM値 | | 2.9.16 |
| low_util_violation_244 | Low Util Violation | ns | 収集区間中にサーバー内の個別GPUが低活用関連制約状態にあった時間を合計した値です。単位はns（ナノ秒）で、サーバー全体で低活用条件違反状態 | 搭載
Physical GPUのSUM値 | | 2.9.16 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------------|--|------|--|-------------------------|---------------|-----------------------------------|
| | | | がどの程度継続したかを総量の観点で示します。 | | | |
| board_limit_violation_243 | Board Limit Violation | ns | 収集区間中にサーバー内の個別GPUがボード限界（board limit）制約状態にあった時間を合計した値です。単位はns（ナノ秒）で、電源部・ボード設計限界などボードレベルの制約が最も多くかかっているGPUを識別する際に使用します。 | 搭載
Physical GPUのSUM値 | | 2.9.16 |
| sync_boost_violation_242 | Sync Boost Violation | ns | 収集区間中にサーバー内の個別GPUがsync boost関連制約状態にあった時間を合計した値です。単位はns（ナノ秒）で、複数GPUの動作速度を合わせるための制約に最も大きく影響を受けているGPUを識別する際に使用します。 | 搭載
Physical GPUのSUM値 | | 2.9.16 |
| reliability_violation_245 | Reliability Violation | ns | 収集区間中にサーバー内の個別GPUが信頼性（reliability）保護制 | 搭載
Physical GPUの | | 2.9.16 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマリー/パフォーマンス詳細/メトリクスエクスプローラーの指標名 | Unit | Description | 備考 | メトリクス収集条件 | 最小サポートエージェントバージョン |
|---------------------|--|--------|--|------|-----------|-------------------|
| | | | 約状態にあった時間を合計した値です。単位はns（ナノ秒）で、安定性とハードウェア保護のための制約に最も大きく影響を受けているGPUを識別する際に使用します。 | SUM値 | | |
| response_time_out | Response Timeout | string | 一定時間NVMLを通じたデータ収集が行われない場合、この値をFalseとして記録します。 | | | 2.9.19 |

infra_gpu_id

サーバーに搭載された個別GPU 1台単位のパフォーマンス/状態情報を収集するカテゴリです。GPU別のutilization、SM/DRAM/Tensor/FP演算使用率、メモリ容量/使用量、温度、電力、クロック、PCIe/NVLink、ECC、violation状態などを提供します。特定GPUの過熱、電力制限、メモリ不足、インターコネクットのボトルネックを確認する際に使用します。

- 収集対象をPhysical / MIGに区分する基準：ボード/カード全体のハードウェア状態を代表する指標かどうかに応じて、Physicalのみ収集すれば十分な対象はPhysical指標のみを収集します。
- DCP（Datacenter Profiling）指標の収集には、nvidia-dcgmサービス（またはnv-hostengineプロセス）が起動している必要があります。
- Agent 2.9.16以上のバージョンでnvidiaiv2.collector=trueを設定すると、接続可能なNVML、DCGM Libraryを通じてメトリクスデータを自動的に収集します。（nvidia-smiまたはdcgmiクエリは使用しません。）
- デフォルト収集周期：30s

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 対象 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|--------|--|------------------|---------------|-----------------------------------|
| index | GPU Index | string | サーバー内のGPUを識別するためのインデックス値で、OSまたはドライバーが認識したGPUの順番を意味します。 | Physical,
MIG | | 2.9.3 |
| name_50 | GPU Name | string | 該当GPUのモデル名を表す値です。ドライバーバージョンまたは収集経路によって表示文字列が若干異なる場合があります。 | Physical,
MIG | | 2.9.3 |
| uuid_54 | GPU UUID | string | 該当GPUの固有識別子（UUID）です。再起動やデバイス順序の変更に関係なく、GPUを安定して識別する際に使用します。 | Physical,
MIG | | 2.9.3 |
| gpuType | GPU Type | string | 該当GPUのTypeをPhysicalとMIGで表示します。 | Physical,
MIG | | 2.9.3 |
| modelFamily | GPU Model Family | string | 該当GPUモデルを代表する上位モデル群の値を示します。ドライバーバージョンや収集経路によって同一のGPUでもモデル名が若干異 | Physical,
MIG | | 2.9.7 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 対象 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|------|---|------------------|---|-----------------------------------|
| | | | なる場合があるため、A100、H100、L4などの共通基準の単純化されたモデル名に正規化して提供します。同一ファミリーのGPUを一貫して分類・集計・比較する際に使用します。 | | | |
| gpuUtilization | GPU Utilization | % | 該当GPUの活用率を意味します。Physical GPU環境では一般的なGPU Util値を意味し、MIG環境ではGR Engine Active値を代表GPU使用率として解釈できます。 | Physical,
MIG | MIG有効環境では、nvidia-dcgm serviceまたはnv-hostengineプロセスの起動が必須 | 2.9.6 |
| encUtil_206 | Encoder Util | % | 該当GPUのエンコーダー（Encoder）エンジン活用率を示します。値が高いほどNVENCファミリーエンジンの使用比率が高いことを意味します。 | Physical | | 2.9.3 |
| decUtil_207 | Decoder Util | % | 該当GPUのデコーダー（Decoder）エンジン活用率を示します。値が高いほどNVDECフ | Physical | | 2.9.3 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 対象 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|------|--|---------------|--|-----------------------------------|
| | | | ファミリーエンジンの使用比率が高いことを意味します。 | | | |
| grEngineActive_1001 | GR Engine Active Util | % | 該当GPUのGraphics/Compute Engine活性比率を示します。MIG インスタンス環境では、そのインスタンスのGPU使用率を代表的に解釈できる指標として活用します。 | Physical, MIG | nvidia-dcgm serviceまたはnv-hostengine プロセスの起動が必須 | 2.9.3 |
| smActive_1002 | SM Active Util | % | 該当GPUのSM (Streaming Multiprocessor) 活性比率を示します。実際の演算処理に使用されたSMリソースの全般的な使用水準を示します。 | Physical, MIG | nvidia-dcgm serviceまたはnv-hostengine プロセスの起動が必須 | 2.9.3 |
| smOccupancy_1003 | SM Occupancy | % | 該当GPUのSM Occupancyを示します。アクティブワーブがSMにどの程度充填されているかを示し、単純な活性率よりSMリソース活用密度をより正確に表します。 | Physical, MIG | nvidia-dcgm serviceまたはnv-hostengine プロセスの起動が必須 | 2.9.3 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 対象 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|------|---|---------------|--|-----------------------------------|
| tensorActive_1004 | Tensor Core Util | % | 該当GPUのTensor Core活性比率を示します。AI/ディープラーニング演算のようにTensor Coreを使用するワークロードの比率を把握する際に役立ちます。 | Physical, MIG | nvidia-dcgm serviceまたはnv-hostengine プロセスの起動が必須 | 2.9.3 |
| fp64Active_1006 | FP64 Compute Util | % | 該当GPUのFP64演算活性比率を示します。倍精度（double precision）演算負荷水準を示します。 | Physical, MIG | nvidia-dcgm serviceまたはnv-hostengine プロセスの起動が必須 | 2.9.3 |
| fp32Active_1007 | FP32 Compute Util | % | 該当GPUのFP32演算活性比率を示します。単精度（single precision）演算負荷水準を示します。 | Physical, MIG | nvidia-dcgm serviceまたはnv-hostengine プロセスの起動が必須 | 2.9.3 |
| fp16Active_1008 | FP16 Compute Util | % | 該当GPUのFP16演算活性比率を示します。半精度（half precision）演算負荷水準を示し、AI推論/学習ワークロードで重要になる場合があります。 | Physical, MIG | nvidia-dcgm serviceまたはnv-hostengine プロセスの起動が必須 | 2.9.3 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 対象 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|------|--|---------------|---|-----------------------------------|
| memoryCopyUtil_204 | Memory Copy Util | % | 該当GPUのメモリコピーエンジンの使用率を示します。GPUメモリとGPU内部演算領域間のデータ移動、Host ↔ Deviceコピー、Device ↔ Deviceコピーなどのメモリコピーやデータ移動経路がどの程度使用されているかを示す指標です。値が高いほど、GPU演算自体よりデータ移動負荷が大きいか、メモリコピー作業がボトルネックになる可能性があります。この値はメモリ容量使用率ではなく、メモリコピー/転送エンジンの活動水準として解釈する必要があります。MIG有効のPhysical GPUはデータを収集できません。 | Physical | | 2.9.3 |
| dramActive_1005 | DRAM Active Util | % | 該当GPU DRAMメモリサブシステムがアクティブ状態だった比率を示します。GPUメモリ帯域幅がどの程度活発に使用されているかを | Physical, MIG | nvidia-dcgm serviceまたはnv-hostengineプロセスの起動が必須 | 2.9.3 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 対象 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|------|---|---------------|---------------|-----------------------------------|
| | | | 示す指標で、メモリ読み取り/書き込み要求が多いか、メモリアクセス中心のワークロードで高くなる傾向があります。高い値が継続する場合、演算性能よりGPUメモリ帯域幅がボトルネックになっている状況かもしれません。この値はFB Memory Usedのようなメモリ使用容量ではなく、GPU DRAMが実際にどの程度バジーに動作したかを示す活性度指標です。 | | | |
| fbTotal_250 | FB Total Memory | MiB | 該当GPUのFB（Frame Buffer）全体メモリ容量を示します。 | Physical, MIG | | 2.9.3 |
| fbFree_251 | FB Free Memory | MiB | 該当GPUのFB空きメモリ容量を示します。現在利用可能なGPUメモリ量を意味します。 | Physical, MIG | | 2.9.3 |
| fbUsed_252 | FB Used Memory | MiB | 該当GPUのFB使用メモリ容量を示します。現在実際に占有されて | Physical, MIG | | 2.9.3 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 対象 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|------|--|---------------|---------------|-----------------------------------|
| | | | いるGPUメモリ量を意味します。 | | | |
| fbResv_253 | FB Reserved Memory | MiB | 該当GPUのFB予約メモリ容量を示します。システム/ドライバ/ファームウェアなどによって予約されたGPUメモリ領域です。 | Physical, MIG | | 2.9.3 |
| fbUsdp_254 | FB Memory Usage | % | 該当GPUのFBメモリ使用率を示す指標です。FB Used / FB Total * 100で計算します。 | Physical, MIG | | 2.9.3 |
| bar1Total_90 | BAR1 Total Memory | MiB | 該当GPUのBAR1全体容量を示します。BAR1はホストがGPUメモリにアクセスするために使用するメモリマッピング領域です。 | Physical, MIG | | 2.9.3 |
| bar1Used_92 | BAR1 Used Memory | MiB | 該当GPUで現在使用中のBAR1メモリ容量を示します。 | Physical, MIG | | 2.9.3 |
| bar1Free_93 | BAR1 Free Memory | MiB | 該当GPUで利用可能なBAR1空き容量を示します。 | Physical, MIG | | 2.9.3 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 対象 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|--------------------------|--|-------|---|---------------|---------------|-----------------------------------|
| bar1Usdp | BAR1 Memory Usage | % | 該当GPUのBAR1使用率を示す指標です。BAR1 Used / BAR1 Total * 100で計算します。 | Physical, MIG | | 2.9.3 |
| eccSbeAggregateTotal_312 | ECC SBE Total | count | 該当GPUで累積されたECC Single Bit Errorの総数を示します。累積カウンタのため、継続的な傾向観察が重要です。 | Physical | | 2.9.3 |
| eccDbeAggregateTotal_313 | ECC DBE Total | count | 該当GPUで累積されたECC Double Bit Errorの総数を示します。二重ビットエラーは単一ビットエラーよりも深刻な状況を意味します。 | Physical | | 2.9.3 |
| eccSbeAggregateDelta_312 | ECC SBE Delta | count | 直近の収集区間中に新たに増加したECC Single Bit Errorの数を示します。その区間の新規単一ビットエラー発生量を確認する際に使用します。 | Physical | | 2.9.16 |
| eccDbeAggregateDelta_313 | ECC DBE Delta | count | 直近の収集区間中に新たに増加したECC | Physical | | 2.9.16 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 対象 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|------|---|----------|---------------|-----------------------------------|
| | | | Double Bit Errorの数を示します。その区間の新規二重ビットエラー発生量を確認する際に使用します。 | | | |
| gpuTemp_150 | GPU
Temperature | °C | 該当GPUの現在温度を示します。個別GPU基準の過熱の有無を判断する代表的な指標です。 | Physical | | 2.9.3 |
| memTemp_140 | GPU Memory
Temperature | °C | 該当GPUメモリの現在温度を示します。一般的にHBMまたはGDDRメモリ基準の温度で、メモリの発熱状態や冷却異常の有無を確認する際に使用します。メモリ集約型ワークロードではGPUコア温度より先に上昇することがあるため、合わせて確認することをお勧めします。 | Physical | | 2.9.16 |
| powerUsage_155 | Power Usage | watt | 該当GPUが現在消費している電力をワット（W）単位で示します。 | Physical | | 2.9.3 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 対象 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|-----------------------|--|------|--|----------|---------------|-----------------------------------|
| powerRate | Power Rate | % | 該当GPUの電力使用率を示します。電力使用量 / 電力上限 * 100として解釈し、電力上限に対してどの水準まで使用しているかを示します。 | Physical | | 2.9.3 |
| energyCumulativeDaily | Energy Cumulative | kWh | 当日00時を基準に累積計算した該当GPUの日次エネルギー使用量です。NVIDIAドライバー/DCGMなどを通じて収集したpowerUsage値を収集周期単位で積算して計算した参考用推定値で、別途の電力計測器で測定した正確な電力量とは差異がある場合があります。GPU別の電力使用推移と日次使用パターンを参考にする用途で活用します。 | Physical | | 2.9.16 |
| pstate_190 | Performance State | P | 該当GPUの現在のパフォーマンス状態（P-state）を示す値です。数字が低いほど高いパフォーマンス状態を意味し、P0が最も | Physical | | 2.9.3 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 対象 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|------|---|----------|---------------|-----------------------------------|
| | | | 高いパフォーマンス状態です。値の範囲は通常P0からP15で、実際の保存時にはプレフィックスPを除いた数字のみを使用します。例えばP0は0、P2は2として保存されます。 | | | |
| fanSpeed_191 | Fan Speed | % | 該当GPUファンの現在速度をパーセンテージで示します。ファンが存在するモデルで冷却装置の動作水準を示します。 | Physical | | 2.9.3 |
| smClock_100 | SM Clock | MHz | 該当GPUのSMクロックをMHz単位で示します。演算ユニットが動作中のコアクロック水準を示します。 | Physical | | 2.9.3 |
| memoryClock_101 | Memory Clock | MHz | 該当GPUのメモリクロックをMHz単位で示します。GPUメモリの動作速度を示します。 | Physical | | 2.9.3 |
| videoClock_102 | Video Clock | MHz | 該当GPUのビデオエンジンクロックをMHz単位で示します。映像処理関連エンジンの動作 | Physical | | 2.9.3 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 対象 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|---------|---|----------|---|-----------------------------------|
| | | | 速度水準を示します。 | | | |
| pcieTxBytes_1009 | PCIE TX | bytes/s | 該当GPUからPCIeを通じて外部へ転送されたデータ処理量をbytes/s単位で示します。 | Physical | nvidia-dcgm serviceまたはnv-hostengineプロセスの起動が必須 | 2.9.3 |
| pcieRxBytes_1010 | PCIE RX | bytes/s | 該当GPUがPCIeを通じて外部から受信したデータ処理量をbytes/s単位で示します。 | Physical | nvidia-dcgm serviceまたはnv-hostengineプロセスの起動が必須 | 2.9.3 |
| pcieTxRxBytes | PCIE Total | bytes/s | 該当GPUのPCIe送受信処理量の合計をbytes/s単位で示します。PCIE TX + PCIE RXに該当します。 | Physical | nvidia-dcgm serviceまたはnv-hostengineプロセスの起動が必須 | 2.9.16 |
| nvlinkTxBytes_1011 | NVLink TX | bytes/s | 該当GPUからNVLinkを通じて他のGPUへ転送されたデータ処理量をbytes/s単位で示します。 | Physical | nvidia-dcgm serviceまたはnv-hostengineプロセスの起動が必須 | 2.9.3 |
| nvlinkRxBytes_ | NVLink RX | bytes/ | 該当GPUがNVLinkを | Physical | nvidia-dcgm | 2.9.3 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 対象 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|--------------------------|--|---------|--|----------|---|-----------------------------------|
| 1012 | | s | 通じて他のGPUから受信したデータ処理量をbytes/s単位で示します。 | | serviceまたはnv-hostengineプロセスの起動が必須 | |
| nvlinkTxRxBytes | NVLink Total | bytes/s | 該当GPUのNVLink送受信処理量の合計をbytes/s単位で示します。NVLink TX + NVLink RXに該当します。 | Physical | nvidia-dcgm serviceまたはnv-hostengineプロセスの起動が必須 | 2.9.16 |
| powerViolationRate_240 | Power Violation Rate | % | 該当GPUが電力制限（power cap）制約状態にあった比率を示す指標です。電力制限によりパフォーマンス制限がどの程度発生したかを示します。 | Physical | | 2.9.16 |
| thermalViolationRate_241 | Thermal Violation Rate | % | 該当GPUが熱制限（thermal limit）制約状態にあった比率を示す指標です。過熱によりパフォーマンス制限がどの程度発生したかを示します。 | Physical | | 2.9.16 |
| lowUtilViolationRate_244 | Low Util Violation Rate | % | 該当GPUが低活用（low utilization）関 | Physical | | 2.9.16 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 対象 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|------------------------------|--|------|---|----------|---------------|-----------------------------------|
| | | | 連制約状態にあった比率を示す指標です。設定された低活用条件に該当する状態がどの程度発生したかを示します。 | | | |
| boardLimitViolationRate_243 | Board Limit Violation Rate | % | 該当GPUがボード全体のハードウェア限界（board limit）関連制約状態にあった比率を示す指標です。電源部・ボード設計限界などボードレベルの制約によりパフォーマンス制限がどの程度発生したかを示します。 | Physical | | 2.9.16 |
| syncBoostViolationRate_242 | Sync Boost Violation Rate | % | 該当GPUが同期ブースト（sync boost）関連制約状態にあった比率を示す指標です。複数GPUの動作速度を合わせるための制約によりパフォーマンス制限がどの程度発生したかを示します。 | Physical | | 2.9.16 |
| reliabilityViolationRate_245 | Reliability Violation Rate | % | 該当GPUが信頼性（reliability）保護関連制約状態にあった比 | Physical | | 2.9.16 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 対象 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|--------------------------|--|------|--|----------|---------------|-----------------------------------|
| | | | 率を示す指標です。安定性とハードウェア保護のための制約によりパフォーマンス制限がどの程度発生したかを示します。 | | | |
| powerViolation
_240 | Power Violation | ns | 収集区間中に該当GPUが電力制限（power cap）制約状態にあった時間を示す値です。単位はns（ナノ秒）で、電力制限によりパフォーマンス制限が発生した時間を示します。 | Physical | | 2.9.16 |
| thermalViolatio
n_241 | Thermal Violation | ns | 収集区間中に該当GPUが熱制限（thermal limit）制約状態にあった時間を示す値です。単位はns（ナノ秒）で、過熱によりパフォーマンス制限が発生した時間を示します。 | Physical | | 2.9.16 |
| lowUtilViolatio
n_244 | Low Util Violation | ns | 収集区間中に該当GPUが低活用関連制約状態にあった時間を示す値です。単位はns（ナノ | Physical | | 2.9.16 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 対象 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|------------------------------|--|------|---|----------|---------------|-----------------------------------|
| | | | 秒) で、低活用条件違
反状態がどの程度継続
したかを示します。 | | | |
| boardLimitViol
ation_243 | Board Limit
Violation | ns | 収集区間中に該当GPU
がボード全体のハード
ウェア限界 (board
limit) 関連制約状態
にあった時間を示す値
です。単位はns (ナノ
秒) で、ボードレベル
の制約によりパフォー
マンス制限が発生した
時間を示します。 | Physical | | 2.9.16 |
| syncBoostViola
tion_242 | Sync Boost
Violation | ns | 収集区間中に該当GPU
が同期ブースト
(sync boost) 関連制
約状態にあった時間を
示す値です。単位は
ns (ナノ秒) で、複数
GPUの動作速度を合わ
せるための制約により
パフォーマンス制限が
発生した時間を示しま
す。 | Physical | | 2.9.16 |
| reliabilityViolat
ion_245 | Reliability
Violation | ns | 収集区間中に該当GPU
が信頼性
(reliability) 保護制
約状態にあった時間を | Physical | | 2.9.16 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 対象 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|------|---|----|---------------|-----------------------------------|
| | | | 示す値です。単位は
ns（ナノ秒）で、安定
性とハードウェア保護
のための制約によりパ
フォーマンス制限が発
生した時間を示しま
す。 | | | |

infra_gpu_process

GPUを使用する個別プロセス単位のGPUおよびシステムリソース使用情報を収集するカテゴリです。GPU index/UUID、PID、process name/type、SM使用率、memory controller使用率、encoder/decoder使用率、FB memory使用量、保護メモリ（CCPM）などを提供します。またCPU使用率、RSSメモリ、process I/O情報も合わせて提供し、GPUリソース使用原因だけでなくCPU・メモリ・I/Oボトルネックの可能性まで、プロセスの観点から分析できます。

- Agent 2.9.16以降、nvidiaiv2.collector=trueを設定するとMIG環境でプロセスとMIGの対応関係を確認できます。
- デフォルト収集周期：30s

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|--------|--|--------------------------|---------------|-----------------------------------|
| index | GPU Index | string | このプロセスが実行されているGPUのindex値を意味します。サーバー内でGPUを区別す | Agent 2.9.16以上：MIGに割り当てら | | 2.9.3 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|--------|---|-----------------------|---------------|-----------------------------------|
| | | | るための順番として使
用します。 | れたプロセ
ス情報を確
認可能 | | |
| uuid | GPU UUID | string | このプロセスが実行さ
れているGPUのUUID
を意味します。GPUの
固有識別子で、index
と異なりデバイス順序
の変更に関係なくGPU
を安定して識別する際
に使用します。 | | | 2.9.3 |
| pid | Process ID | string | GPUを使用中のプロセ
スのPID（Process
ID）を意味します。 | | | 2.9.3 |
| process_name | Process
Command | string | GPUを使用するプロセ
スの名前を意味しま
す。例えばpython、
cuda_program、Xorg
などが表示される場合
があります。 | | | 2.9.3 |
| process_type | Process Type | string | 実行中のGPUプロセス
のタイプを意味しま
す。CはComputeプロ
セス（CUDA、AI/演算
作業）、GはGraphics
プロセス（GUI、レン
ダリング、ディスプレ | | | 2.9.3 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|--------|---|----|---------------|-----------------------------------|
| | | | イアクセラレーショ
ン) を意味します。環
境によって両方のタイ
プが共存する場合があ
ります。 | | | |
| owner | Owner | string | このプロセスを実行し
たユーザーアカウント
(user) を示す値で
す。 | | | 2.9.16 |
| args | Arguments | string | このプロセスの実行
arguments (コマンド
ライン引数) を示す値
です。 | | | 2.9.16 |
| stime | StartTime | string | このプロセスの開始時
刻をepoch time基準
で示した値です。 | | | 2.9.16 |
| gpu_utilization | GPU Utilization | % | このプロセスが収集時
点でバインドされてい
るGPUデバイス全体の
GPU Utilizationを表
示します。この値はプ
ロセス別に直接測定し
たGPU使用率ではな
く、そのプロセスが接
続されているGPU全体
の使用率をプロセス情
報と合わせて示す値で | | | 2.9.16 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|------|---|----|---------------|-----------------------------------|
| | | | す。そのため、同一GPUを使用する複数のプロセスには同一または類似した値が表示される場合があります、この値だけで個別プロセスがGPU使用率にどの程度寄与したかを判断してはいけません。 | | | |
| sm_util | SM Util | % | このプロセスがGPUのSM（Streaming Multiprocessor）演算リソースをどの程度使用しているかを示す比率です。実際の演算処理に使用されたGPUコアリソースの活用水準を示し、値が高いほどそのプロセスがGPU演算リソースを強く使用していることを意味します。ただし、この値はプロセス観点のSM使用率であり、GPUデバイス全体を基準に測定されるSM Active Util（%）とは測定基準が異なる場合があります。そのため、特定プロセスのSM Utilが | | | 2.9.3 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|-------------------------|--|------|--|----|---------------|-----------------------------------|
| | | | 高くても、GPU全体の
観察区間のアイドル時
間、カーネル間ギャッ
プ、他のプロセスとの
スケジューリング、
MIG/Time-slicingの影
響などによって、GPU
のSM Active Utilはよ
り低くまたは異なる値
を示す場合があります。
(MIG Instanceを
使用するプロセスの場
合、ドライバーおよび
モニタリングインター
フェイスの提供範囲の
制限により、プロセス
別のSM Util値が収集
されないか、画面に表
示されない場合があります。) | | | |
| mem_controlle
r_util | Memory
Controller Util | % | このプロセスがGPUメ
モリコントローラーを
どの程度使用している
かを示す比率です。
VRAMの容量をどの程
度占有しているかでは
なく、GPUメモリへの
読み取り/書き込みお
よびデータ移動要求が
どの程度活発だったか | | | 2.9.15 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|------|--|----|---------------|-----------------------------------|
| | | | <p>を示す指標です。値が
高いほど、そのプロセ
スがメモリ帯域幅また
はメモリアクセス経路
を多く使用している可
能性があります。ただ
し、この値はプロセス
観点のメモリコントロ
ーラー使用率であり、
GPUデバイス全体を基
準に測定される</p> <p>Memory Copy
Util (%) または
DRAM Active
Util (%) とは意味が
異なります。Memory
Copy UtilはGPU全体
のメモリコピー/転送
エンジン使用率に近
く、DRAM Active Util
はGPU DRAMが観察区
間中に読み取り/書き
込み要求でアクティブ
状態だった比率に近い
です。（MIG Instance
を使用するプロセスの
場合、ドライバーおよ
びモニタリングインタ
ーフェイスの提供範囲
の制限により、プロセ
ス別のSM Util値が収</p> | | | |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|------|--|----|---------------|-----------------------------------|
| | | | 集されないか、画面に
表示されない場合があ
ります。) | | | |
| enc_util | Encoder Util | % | このプロセスがGPUエ
ンコーダー
(Encoder) エンジン
をどの程度使用してい
るかを示す比率です。
主に動画エンコード、
ストリーミング、映像
保存/圧縮作業で増加
します。 | | | 2.9.3 |
| dec_util | Decoder Util | % | このプロセスがGPUデ
コーダー (Decoder)
エンジンをどの程度使
用しているかを示す比
率です。主に圧縮され
た動画ストリームのデ
コード、再生、映像分
析前処理過程で増加し
ます。 | | | 2.9.3 |
| fb_used | FB Used | MiB | このプロセスが使用中
のFrame Buffer (GPU
メモリ) のサイズを示
します。単位はMiB
で、このプロセスが占
有しているVRAM使用
量として解釈できま | | | 2.9.3 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|---------|---|----|---------------|-----------------------------------|
| | | | す。 | | | |
| ccpm | CCPM | MiB | このプロセスが使用中のConfidential Computing Protected Memoryの使用量を示します。単位はMiBで、NVIDIA H100のようにConfidential ComputingをサポートするGPUで活用できます。この機能をサポートしないGPUでは0と表示される場合があります。 | | | 2.9.3 |
| cpu | CPU | % | このプロセスが使用した全体CPU使用率を意味します。 | | | 2.9.15 |
| rss | RSS | Byte | このプロセスのRSS (Resident Set Size) 値で、現在システムメモリに読み込まれているメモリのサイズを意味します。 | | | 2.9.15 |
| total_char_io | Process IO Total | Bytes/s | このプロセスが毎秒発生させる全体Characterに基づくI/O (char I/O) 処理量 | | | 2.9.15 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/パフォーマンス
詳細/メトリクスエク
スプローラーの指標
名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ートエー
ジェント
バージョ
ン |
|---------------------|--|------|---|----|---------------|-----------------------------------|
| | | | を意味します。ディス
クだけでなく、パイ
プ、ターミナル、バッ
ファ、キャッシュ層へ
のI/Oも含まれる場合
があるため、実際の物
理ディスクI/Oより大
きくなる場合があります。 | | | |

infra_gpu_xid

NVIDIAドライバーが `/var/log/messages` に記録した `NVRM: Xid` ログを解析してGPU障害/イベント履歴を収集するカテゴリです。Xid Code、GPU Index、PCI Bus ID、関連PID/プロセス名、原文メッセージを提供し、GPUエラーの発生時点、対象GPU、関連プロセス、エラー種別を追跡する際に使用します。Xidは単純なアプリケーションエラーからドライバー・ハードウェア・PCIeの問題まで多様な原因を含む場合があるため、コードの意味と発生頻度、GPU状態指標、システムログを併せて分析することが重要です。

- Agent 2.9.19以上からサポートします。
- 基本収集周期: 60s

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/詳細/メトリク
スエクスプローラー
指標名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ート
Agent
Version |
|---------------------|--|--------|----------------------------|----|---------------|--------------------------------|
| index | GPU Index | string | Xidイベントが発生し
たGPUのインデックス | | | 2.9.19 |

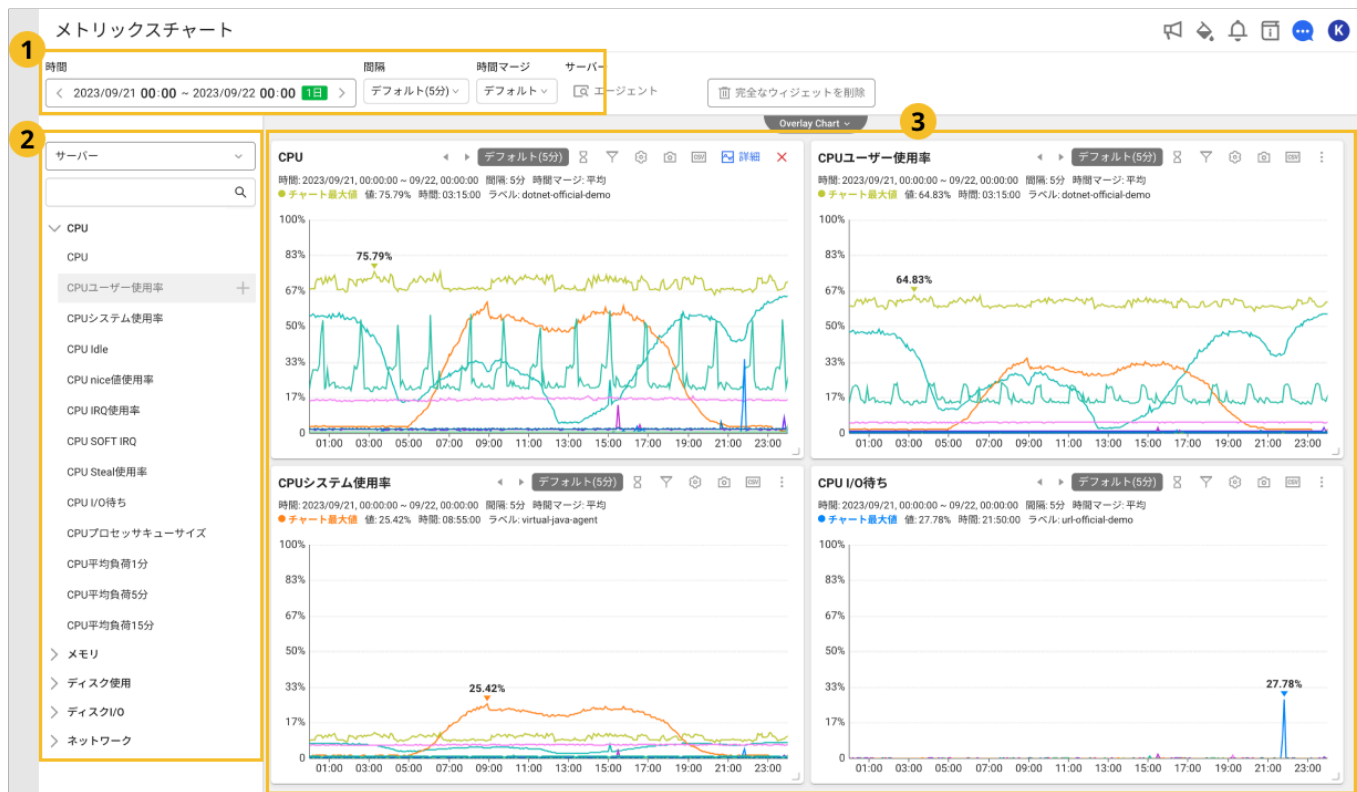
| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/詳細/メトリク
スエクスプローラー
指標名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ート
Agent
Version |
|---------------------|--|--------|---|----|---------------|--------------------------------|
| | | | です。サーバー内のGPUデバイスを識別するための番号で、nvidia-smiに表示されるGPU Indexとマッチングして障害が発生したGPUを確認する際に使用します。 | | | |
| pcieBusId | PCI Bus ID | string | Xidイベントが発生したGPUのPCI Bus IDです。GPU Indexが変更される可能性がある環境で物理GPUを識別するための補助識別子として使用でき、同一サーバー内のGPUデバイス位置を確認する際に参照します。 | | | 2.9.19 |
| agentTimestamp | Agent Timestamp | string | /var/log/messagesに記録された実際のイベント発生時刻です。 | | | 2.9.19 |
| xidCode | XID Code | string | NVIDIAドライバーから報告されたXidエラーコードです。GPUドライバー、ハードウェア、PCIe、メモリ、アプリケーションエラーなど多様なGPU異常状態を区別するコード | | | 2.9.19 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/詳細/メトリク
スエクスプローラー
指標名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ート
Agent
Version |
|---------------------|--|--------|--|----|---------------|--------------------------------|
| | | | で、コード別の意味を
基準に障害原因分析と
RMA (Return
Merchandise
Authorization) の要
否を判断する際に活用
します。 | | | |
| pid | PID | string | Xidログに含まれるプ
ロセスIDです。特定の
プロセス実行中にGPU
エラーが発生した場
合、原因プロセスを追
跡するために使用しま
す。ログにPID情報が
ない場合やドライバー
/ハードウェアレベル
で発生したイベントの
場合は値がないことが
あります。 | | | 2.9.19 |
| taskName | Task Name | string | Xid発生時にNVIDIAド
ライバーが記録した
Task Nameです。
Linuxの/
proc/{pid}/commまた
はスレッド別/
proc/{pid}/task/{tid}/
commの値に該当する
短い名前、実行コマ
ンド全体 (cmdline)
を意味するものではあ | | | 2.9.19 |

| Field
カテゴリフィールド名 | Title
パフォーマンスサマ
リー/詳細/メトリク
スエクスプローラー
指標名 | Unit | Description | 備考 | メトリクス収
集条件 | 最小サポ
ート
Agent
Version |
|---------------------|--|--------|---|----|---------------|--------------------------------|
| | | | りません。マルチスレ
ッドアプリケーション
では同一PIDでも、エ
ラーが記録されたタス
クによってpython3、
pt_nccl_watchdogのよ
うに異なる名前が表示
されることがあります。
したがって、実際の
アプリケーションを
識別する際はPID、
GPU PCIアドレス、
GPU UUID、cmdline
情報と併せて解釈する
ことをお勧めします。 | | | |
| message | Message | string | /var/log/messagesか
ら解析したNVRM: Xid
ログの詳細メッセージ
です。Xidコードのほ
かに、GPU UUID、
PCI情報、チャネル情
報、プロセス情報、エ
ラー詳細文などが含ま
れる場合があります、障害
原因分析時に原文確認
用として使用します。 | | | 2.9.19 |

メトリクスチャート

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

時間選択

最大カウント

カテゴリ

2023/08/17 08:04 ~ 2023/08/17 09:04 1時

100

app_counter

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

検索 CSV

| | 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。

Logモニタリング

ログは、アプリケーションやシステムで発生するイベントやメッセージを記録するファイルです。異常を特定してシステムの劣化を防いだり、発生したトラブルの原因を確認する場合は、ログを確認することが重要です。

最近のITサービス構築環境は、MSA（マイクロサービスアーキテクチャ）やKubernetesベースへと移行が進んでおり、管理対象が増加しています。一般的なログモニタリングでは、サーバーに接続して `tail` コマンドやエディタを使ってログを確認します。しかし、個別のサーバーに逐一接続するような単純な方法では対応が困難です。では、数百～数千台のサーバーから発生するログを、どのようにして確認すればよいのでしょうか？

WhaTapログモニタリングサービスを使用すると、数多くのログを簡単に管理できます。

❗ Linuxの `tail` コマンドは、時間の経過とともにコンテンツを追加するログを確認するためによく使用されます。

主な機能

- 中央統合管理

WhaTapは、大量のログを中央で一元管理します。個別のサーバーにアクセスしなくても、中央からログを確認できるため、利便性に優れています。

- すべてのログを収集

ログを選別して収集する場合、重要なデータが欠落する可能性があります。WhaTapはすべてのログを収集し、収集されたログは **ライブテール** でリアルタイムに確認できます。

- 可視性確保

WhaTapのさまざまなチャートからログを確認できます。これにより、エラーや問題に関する情報へのアクセス性が向上し、障害の早期検知が可能になります。

- 柔軟な容量管理

個別のサーバーにログを保存する場合、ログによってファイルシステムの容量が過剰に占有される問題が発生する可能性があります。WhaTapを利用してログを中央に集約すれば、各サーバーでログファイルを保持する必要はなく、中央に保存されたログデータの保持期間のみを管理すれば済みます。

- 複数の分析的視点

障害の状況を把握し予測するためには、さまざまな観点からログを分析する必要があります。WhaTapでは、特定のタグを含むログ件数の推移を確認したり、フィルターを適用して分析したりすることができます。よく使うパターンはチャートとして保存し、いつでも呼び出して確認できます。

- パターン通知

障害のパターンをアラートとして設定することで、問題を予防したり迅速に把握したりすることができます。

WhaTapでは、個別のログに特定のキーワードが含まれている場合に通知を受け取る **リアルタイムログアラート** と、特定のタグを含むログ件数の推移を基準に通知を受け取る **複合ログアラート** を提供しています。

ログ分析

ライブテール

ライブテールメニューでは、リアルタイムで収集されたログを `tail` コマンドのように画面上で流れる形式で確認できます。

① 詳しくは、[ライブテール](#) のドキュメントを参照してください。

ログトレンド

ログトレンドメニューでは、収集されたすべてのログ、または特定のタグを含むログの件数推移を確認できます。ログの発生件数は障害の発生および解消のタイミングと密接に関連しているため、ログ件数の推移を通じて障害の原因を分析し、対応のスピードを向上させることができます。

① 詳しくは、[ログトレンド](#) のドキュメントを参照してください。

ログの検索

ログ検索メニューでは、収集されたすべてのログ、または特定のタグを含むログを照会できます。特定の時間帯やサーバーで発生したログをタグを基準にして検索・確認することができます。隣接ログ機能を使用すれば、特定のError

やException発生の前後に記録されたログをあわせて確認し、原因分析に活用できます。

① 詳しくは、[ログ検索](#) のドキュメントを参照してください。

ログエクスプローラー

ログエクスプローラー メニューを使用すると、ログデータを迅速に検索、フィルタリング、分析できます。フィールド構造を把握し、クエリベースのフィルタリングによって必要なログを効率的に検索し、その結果をデータとして可視化することができます。ログエクスプローラー機能は、Luceneインデックスを基盤として動作します。

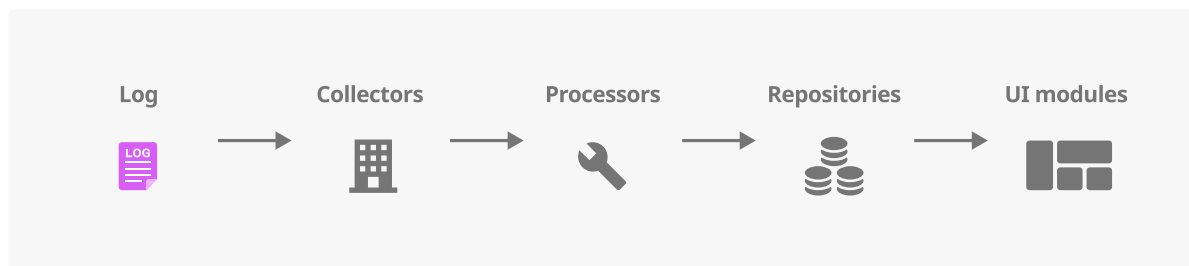
① 詳しくは、[ログエクスプローラー](#) のドキュメントを参照してください。

ログモニタリングを適用する

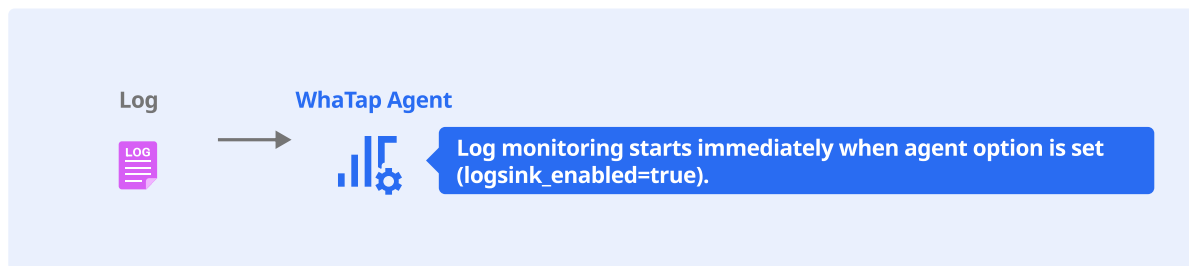
WhaTapログモニタリングサービスを利用するための基本的な使用方法について説明します。WhaTapログモニタリングは、追加のエージェントを構成やログのパーサを適用する必要はありません。簡単な設定で迅速に起動できます。

ログモニタリングの動作原理

Common log integration services



WhaTap log monitoring service



一般的なログ統合サービスは収集機、処理機、ストレージ、UIモジュールで構成されています。段階別設定と構成作業が必要なため、それぞれのモジュールを構築する過程が煩わしく、追加費用が発生します。

WhaTapログモニタリングは簡単に適用できます。既存のモニタリングエージェントがコレクターとして機能するため、エージェントオプションをオンにするだけでログモニタリングを開始できます。

- [Java](#) PHP Python Go Server Kubernetes

- 出力されたファイルからログを読まずに、Javaアプリケーションのログライブラリに渡されるログを直接収集します。
- ログを直接収集するため、ファイルI/Oを引き起こさず、システムに与える性能への影響が非常に低いです。
- トランザクショントレースとログの接続を追跡する特徴を確保し、トレースからログを確認できます。

❗ Javaログのライブラリ

典型的なJavaログライブラリはApache Log4j、Logbackです。

❗ Java Agent2.1.1バージョンから使用できます。

- 既存のエージェントにログ収集機能を追加しました。モニタリングエージェントがログファイルから追加で出力されたログを読み取り読み取り収集する方法を利用します。

❗ PHP Agent2.3.2バージョンから使用できます。

- 既存のエージェントにログ収集機能を追加しました。モニタリングエージェントがログファイルから追加で出力されたログを読み取り読み取り収集する方法を利用します。
- ログにトランザクションIDを出力すると、トランザクショントレースとログの接続追跡性を確保し、トレースからログを確認できます。

❗ Python Agent1.2.2バージョンから使用できます。

- 既存のエージェントにログ収集機能を追加しました。モニタリングエージェントがログファイルから追加で出力されたログを読み取り読み取り収集する方法を利用します。
- 既存のエージェントにログ収集機能を追加しました。モニタリングエージェントがログファイルから追加で出力されたログを読み取り読み取り収集する方法を利用します。

❗ Server Agent2.1.2バージョンから使用できます。

- Kubernetesコンテナにログを収集できます。

- Kubernetesコンテナ内のアプリケーションからログを収集できます。

 Kubernetes Agent 1.1.35バージョンから使用できます。

ログモニタリングを適用する

使用するアプリケーションに応じた適用方法は以下のとおりです。ログモニタリングを適用する前に、[対応バージョン](#)を必ずご確認ください。

1. 対応するエージェントのバージョンを確認し、**アップデート**してください。
2. ログモニタリング**オプション**を設定してください。
3. ログモニタリングを**有効**にしてください。

Java

Javaアプリケーションでログを収集する方法について案内します。

PHP

PHPアプリケーションからログを収集する方法について説明します。

Node.js

Node.jsアプリケーションでログを収集する方法を案内します。

 Python

Pythonアプリケーションからログを収集する方法について説明します。

 Go

Goアプリケーションからログを収集する方法について説明します。

 Server

サーバーアプリケーションからログを収集する方法について説明します。

 Kubernetes

Kubernetesコンテナとコンテナ内部のアプリケーションのログを収集する方法について説明します。

Java

Javaアプリケーションでログを収集するための設定方法を案内します。

エージェントのアップデート

Javaエージェントのバージョン2.1.1以降で利用可能です。アップデート方法については、[次のドキュメント](#)を参照してください。

エージェント設定の確認

ホーム画面 > プロジェクト選択 > ログ > ログ設定

1. WhaTapモニタリングサービスの初期画面でプロジェクトを選択した後、**ログ > ログ設定** メニューに移動してください。
2. **ログモニタリング開始タブの 1. エージェント設定の確認** の案内に従って、エージェント設定を確認してください。

エージェント設定

1. プロジェクトの **管理 > エージェントの設定** メニューをクリックしてください。
2. **オプション作成** の **オプション選択** ドロップダウンリストから **直接入力** をクリックし、`logsink_enabled=true` オプションを入力して **適用** ボタンをクリックして追加してください。
 - キー入力欄に `logsink_enabled` を入力してください。
 - 値入力欄に `true` を入力してください。
3. ログモニタリングを適用するには、アプリケーションを再起動します。

主なオプション

- `hooklog_enabled` `Boolean`

既定値 `false`

Logライブラリをフックして、ログモニタリングを有効化します。

- ① アプリケーションを実行する前に、[whatap.conf](#) オプションを有効にして、その後にログモニタリングの On/Off を `logsink_enabled` 設定で動的に制御できます。アプリケーションを起動する前に `logsink_enabled` オプションを `true` に設定する場合、このオプションを個別に設定しなくてもログモニタリングが可能です。

今後ログモニタリングを活用する可能性がある場合は、事前にこのオプションを設定することをお勧めします。

- **hooklog_custom_methods**

カスタムログを登録します。特定のログフレームワークの内容を収集します。サイトで個別に作成したログモジュールのログを追跡する際に利用してください。

Java

```
package io.home.test;

public class MyLog {
    public void customLog(String log) { ... }
}
```

whatap.conf

```
hooklog_custom_methods=io.home.test.MyLog.customLog
```

- **logsink_enabled** Boolean

既定値 `false`

Logモニタリング機能をOn/Offします。

- ① アプリケーションが起動する前に[whatap.conf](#)に `hooklog_enabled` オプションが設定されている場合、このオプションを使用すると、ログモニタリングのOn/Offを動的に制御することができます。

- **logsink_trace_enabled** Boolean

既定値 false

LogにトランザクションIDを挿入して、トランザクショントレースのログタブの表示有無を指定します。

ログモニタリングの活性化

ホーム画面 > プロジェクト選択 > ログ > ログ設定

ログモニタリングを開始する タブの 2. ログモニタリング機能の活性化 で、WhaTapログモニタリングを有効化または無効化できます。

-  ログモニタリングの有効化：トグルボタンをオンにするとログモニタリングが有効になり、有効化した日から15日間は無料でお試しいただけます。
-  ログモニタリングの無効化：トグルボタンをオフにするとログモニタリングが無効になり、以降ログは保存されません。

ⓘ ログモニタリングの有効化権限

エージェントをインストールした後、プロジェクトに対して編集権限を持つユーザーのみがログモニタリングを有効化できます。権限の詳細については、[次のドキュメント](#)を参照してください。

PHP

PHPアプリケーションでログを収集するための設定方法を案内します。

エージェントのアップデート

PHPエージェント2.3.2バージョンから可能です。アップデート方法は[次の文書](#)を参照してください。

エージェント設定の確認

ホーム画面 > プロジェクト選択 > ログ > ログ設定

1. WhaTapモニタリングサービスの初期画面でプロジェクトを選択した後、**ログ > ログ設定** メニューに移動してください。
2. **ログモニタリングを開始する** タブの **1. エージェント設定の確認** の案内に従って、エージェント設定を確認してください。

設定ファイルパスの確認

ログモニタリングするファイルの**設定ファイルパス**を確認してください。CLI環境または、ウェブで確認することができます。

CLI環境で確認する

```
$ php -i | grep 'Scan'
Scan this dir for additional .ini files => /etc/php8.0.d
```

❗ パスが"(None)"の場合、設定ファイルのパスは*/usr/whatap/php*です。

ウェブで確認する

CLI環境とApache環境でPHPの設定が異なる場合は、Web上で `phpinfo()` 関数の結果を確認してください。

コマンド入力

設定ファイルパスを含むコマンドを入力すると、ログモニタリングが開始されます。

```
export LOGFILES=/some/path/file1,/some/other/file2
echo "whatap.logsink_enabled=true" | sudo tee -a [設定ファイルパス]/whatap.ini
echo "whatap.logsink.files=$LOGFILES" | sudo tee -a [設定ファイルパス]/whatap.ini
```

ログモニタリングの活性化

ホーム画面 > プロジェクト選択 > ログ > ログ設定

ログモニタリングを開始する タブの 2. ログモニタリングの有効化 で、WhaTapのログモニタリングを有効または無効に設定できます。

-  ログモニタリングの有効化：トグルボタンをオンにするとログモニタリングが有効になり、有効化した日から15日間は無料でお試しいただけます。
-  ログモニタリングの無効化：トグルボタンをオフにするとログモニタリングが無効になり、以降ログは保存されません。

ⓘ ログモニタリングの有効化権限

エージェントをインストールした後、プロジェクトに対して編集権限を持つユーザーのみがログモニタリングを有効化できます。権限の詳細については、[次のドキュメント](#)を参照してください。

Node.js

Node.jsアプリケーションでログを収集するための設定方法を案内します。

エージェントのアップデート

Node.jsエージェント0.5.1バージョンから可能です。 アップデート方法は、[次の文書](#)を参照してください。

エージェント設定の確認

ホーム画面 > プロジェクト選択 > ログ > ログ設定

1. Whatapモニタリングサービスの初期画面でプロジェクトを選択した後、**ログ > ログ設定** メニューに移動してください。
2. ログモニタリング開始タブの **1. エージェント設定の確認** の案内に従って、エージェント設定を確認してください。

エージェント設定

1. プロジェクトの **管理 > エージェントの設定** メニューをクリックしてください。
2. オプション作成 の オプション選択 ドロップダウンリストから **直接入力** をクリックし、`logsink_enabled=true` オプションを入力して **適用** ボタンをクリックして追加してください。
 - キー入力欄に `logsink_enabled` を入力してください。
 - 値入力欄に `true` を入力してください。
3. ログモニタリングを適用するには、アプリケーションを再起動します。

主なオプション

- `logsink_enabled` Boolean

既定値 `false`

ログモニタリングの活性化有無を設定します。

- `logsink_trace_txid_enabled` Boolean

既定値 `true`

ログにトランザクションIDを挿入して、トランザクション トレースのログタブの表示有無を指定します。

- `logsink_limit_content_enabled` Boolean

既定値 `true`

ログメッセージの最大サイズの制限有無を設定します。

- `logsink_limit_content_length` Number

既定値 `10,000`

ログメッセージの最大長さを設定します。この値は、`logsink_limit_content_enabled` オプションが `true` に設定された場合にのみ適用されます。

ログモニタリングの活性化

ホーム画面 > プロジェクト選択 > ログ > ログ設定

ログモニタリングを開始するセクションのログモニタリングを有効にするタブのトグルボタンで、WhaTapログモニタリングの有効または無効にできます。

-  ログモニタリングの有効化：トグルボタンをオンにするとログモニタリングが有効になり、有効化した日から15日間は無料でお試しいただけます。
-  ログモニタリングの無効化：トグルボタンをオフにするとログモニタリングが無効になり、以降ログは保存されません。

ⓘ ログモニタリングの有効化権限

エージェントをインストールした後、プロジェクトに対して編集権限を持つユーザーのみがログモニタリングを有効化できます。権限の詳細については、[次のドキュメント](#)を参照してください。

Python

Pythonアプリケーションでログを収集するための設定方法を案内します。

エージェントのアップデート

Pythonエージェント1.2.2バージョン以降で可能です。アップデート方法は[次の文書](#)を参照してください。

エージェント設定の確認

ホーム画面 > プロジェクト選択 > ログ > ログ設定

1. WhaTapモニタリングサービスの初期画面でプロジェクトを選択した後、**ログ > ログ設定** メニューに移動してください。
2. **ログモニタリングを開始する** タブの **1. エージェント設定の確認** の案内に従って、エージェント設定を確認してください。

ログ収集の活性化

設定ファイルパス(**WHATAP_HOME**)を含むコマンドを入力すると、ログ収集がすぐに開始されます。

```
export LOGFILES={ログファイル全体パス},...  
echo "logsink_enabled=true" | sudo tee -a {設定ファイルパス}/whatap.conf  
echo "logsink.files=$LOGFILES" | sudo tee -a {設定ファイルパス}/whatap.conf
```

ログとウェブトランザクションの連動

1.3.6 以降バージョン

1.3.6バージョンから次の方法でトランザクションとログの連動を設定できます。現在、WhaTapはPythonのlogging、loguruライブラリを対応しています。使用するPython Logライブラリに従って**whatap.conf**を構成してください。

- loggingモジュール

logging

```
echo "trace_logging_enabled=true" | sudo tee -a{設定ファイルパス}/whatap.conf
```

- loguruモジュール

loguru

```
echo "trace_loguru_enabled=true" | sudo tee -a{設定ファイルパス}/whatap.conf
```

1.3.6以前バージョン

トランザクションごとに発生したログを個別に照会できるように、ログにトランザクションID `{txid}` を出力します。WhaTapモニタリングでは、PythonのLogRecordに `{txid}` を自動的に注入し、フォーマッタを設定することでログファイルに `{txid}` を出力できるようにします。

```
settings.py
...
LOGGING = {
...
    'formatters': {
        ...
    },
    'handlers': {
        ...
    },
    'loggers': {
        ...
        '{ロガー名}': {
            'handlers': [...],
            ...
        },
    },
}
```

```

}

try:
    import whatap.trace.mod.logging as whatap_logging
    if whatap_logging.logging_injection_processed:
        LOGGING['formatters']['whatap.formatter']={
            '():': 'django.utils.log.ServerFormatter',
            'format': '[{server_time}] -- {{ "@txid" : "{txid}" }} -- {message}',
            'style': '{',
        }
        LOGGING['handlers']['whatap']={
            'level': 'DEBUG',
            'class': 'logging.handlers.RotatingFileHandler',
            'filename': os.path.join(BASE_DIR, 'logs', 'whatap_log.log'),
            'formatter': 'whatap.formatter',
        }
        LOGGING['loggers'][ロガー名]['handlers'].append('whatap')
except:
    pass
...

```

ログモニタリングの活性化

ホーム画面 > プロジェクト選択 > ログ > ログ設定

ログモニタリングを開始する タブの 2. ログモニタリングの有効化 で、WhaTapのログモニタリングを有効または無効に設定できます。

-  ログモニタリングの有効化：トグルボタンをオンにするとログモニタリングが有効になり、有効化した日から15日間は無料でお試しいただけます。
-  ログモニタリングの無効化：トグルボタンをオフにするとログモニタリングが無効になり、以降ログは保存されません。

ⓘ ログモニタリングの有効化権限

エージェントをインストールした後、プロジェクトに対して編集権限を持つユーザーのみがログモニタリングを有効化できます。権限の詳細については、[次のドキュメント](#)を参照してください。

Go

Goアプリケーションでログを収集するための設定方法を案内します。

エージェント設定の確認

ホーム画面 > プロジェクト選択 > ログ > ログ設定

1. Whatapモニタリングサービスの初期画面でプロジェクトを選択した後、**ログ > ログ設定** メニューに移動してください。
2. **ログモニタリングを開始する** タブの **1. エージェント設定の確認** の案内に従って、エージェント設定を確認してください。

ログ収集の活性化

次のコマンドを入力すると、すぐにログの収集が開始されます。

```
export LOGFILES=/some/path/file1,/some/other/file2
echo "logsink_enabled=true" | sudo tee -a /usr/whatap/agent/whatap.conf
echo "logsink.files=$LOGFILES" | sudo tee -a /usr/whatap/agent/whatap.conf
```

ログモニタリングの活性化

ホーム画面 > プロジェクト選択 > ログ > ログ設定

ログモニタリングを開始する タブの **2. ログモニタリングの有効化** で、Whatapのログモニタリングを有効または無効に設定できます。

-  ログモニタリングの有効化：トグルボタンをオンにするとログモニタリングが有効になり、有効化した日から15日間は無料でお試しいただけます。
-  ログモニタリングの無効化：トグルボタンをオフにするとログモニタリングが無効になり、以降ログは保存されません。

ⓘ ログモニタリングの有効化権限

エージェントをインストールした後、プロジェクトに対して**編集権限**を持つユーザーのみがログモニタリングを有効化できます。権限の詳細については、[次のドキュメント](#)を参照してください。

Server

サーバーアプリケーションでログを収集するための設定方法を案内します。

エージェントのアップデート

サーバーエージェントのバージョン2.1.2以降で利用可能です。アップデート方法は [次の文書](#) を参照してください。

エージェント設定の確認

ホーム画面 > プロジェクト選択 > ログ > ログ設定

1. Whatapモニタリングサービスの初期画面でプロジェクトを選択した後、**ログ > ログ設定** メニューに移動してください。
2. ログモニタリングを始めるの1. エージェント設定の確認にある**OS選択**タブで、**Linux (shell) または Windows (PowerShell、管理者権限) **を選択してください。
3. 基本インストールまたはカテゴリ付きインストールを参考にして、エージェント設定を確認してください。

ⓘ 次の設定は、エージェントを再起動する必要があります。

Linux Shell

• 基本インストール

Linux Shell

```
export LOGFILES=/some/path/file1,/some/other/file2
echo "logsink.files=$LOGFILES" | sudo tee -a /usr/whatap/infra/conf/whatap.conf
```

• カテゴリ付きインストール

Linux Shell

```

1  cd /usr/whatap/infra
2  sudo mkdir extension
3
4  cat <{<EOL | sudo tee extension/logsink.conf}> /dev/null
5  [[inputs.logsink]]
6  category = "serverlog"
7  ## ログ発生量統計の別途データとしての送信有無
8  stats_enabled = true
9  ## 対数発生量の統計カテゴリ
10 stats_category = "logsink_stats"
11 ## ログファイルパス(path)にアスタリスク(*)が含まれ、除外するログ非対象ファイル名を設定
12 excludeNames = [ ".gz", ".zip" ]
13 [[inputs.logsink.file]]
14 ## ログファイルの指定時、日付パターン(strftime.org)指定可能
15 path = "/some/path/%Y-%m-%d/.log"
16 disabled = false
17 encoding = "utf-8"
18
19 [[inputs.logsink.file]]
20 path = "/some/other/log"
21 disabled = false
22 encoding = "utf-8"
23
24 [[inputs.logsink.file]]
25 ## 行単位ログで該当キーワードを検索する時、以前のログにマージ
26 nowrap_keywords = ["Caused by:", "Test"]
27
28 [[inputs.logsink.file]]
29 ## プロジェクトコード及びプロジェクトライセンスの入力時、ログを同じリージョンの希望するプロジェクトに転送可能
30 # pcode = プロジェクトコード
31 # license = "プロジェクトライセンス"
32
33 [[inputs.logsink.file]]
34 # whatap_host_ip = "収集サーバーIP1/収集サーバーIP2"
35 # whatap_host_port = 6600
36
37 [[inputs.logsink.file]]

```

```

38 path = "/tmp/mixed.log"
39 disabled = false
40 encoding = "utf-8"
41 ## [{"A":1,"B":2}, {"C":3,"D":4},...] 形態をそれぞれのログに分離できる{"A":1,"B":2} {"C":3,"D":4}
42 multiline_pattern = "simple_json_array"
43 EOL
44
45 sudo service whatap-infra restart

```

Windows Powershell

• 基本インストール

Windows Powershell

```

$LOGFILES="c:\\whatap\\logs\\%Y-%m-%d\\*.log,c:\\whatap\\logs\\*.log"
Add-Content "c:\\Program Files\\WhatapInfra\\whatap.conf" -Value "logsink.files=$LOGFILES"

```

• カテゴリ付きインストール

Windows Powershell

```

1  # 管理者権限が必要
2  New-Item -type "Directory" -Path "C:\\Program Files\\WhatapInfra\\extension"
3
4  $contentToAdd = @"
5  [[inputs.logsink]]
6  category = "serverlog"
7  ## ログ発生量統計の別途データとしての送信有無
8  stats_enabled = true
9  ## 対数発生量の統計カテゴリ
10 stats_category = "logsink_stats"
11 ## ログファイルパス(path)にアスタリスク(*)が含まれ、除外するログの非対象ファイル名を設定
12 excludeNames = [ ".gz", ".zip" ]
13 [[inputs.logsink.file]]
14 ## ログ ファイルの指定時、日付パターン(strftime.org)指定可能
15 path = "c:\\whatap\\logs%Y-%m-%d_.log"
16 disabled = false

```

```

17  encoding = "utf-8"
18
19  [[inputs.logsink.file]]
20  ## 行単位ログで該当キーワードを検索する時、以前のログにマージ
21  nowrap_keywords = ["Caused by:", "Test"]
22
23  [[inputs.logsink.file]]
24  ## プロジェクトコード及びプロジェクトライセンスの入力時、ログを同じリージョンの希望するプロジェクトに転送可
   能
25  # pcode = プロジェクトコード
26  # license = "プロジェクトライセンス"
27
28  [[inputs.logsink.file]]
29  # whatap_host_ip = "収集サーバーIP1/収集サーバーIP2"
30  # whatap_host_port = 6600
31
32  [[inputs.logsink.file]]
33  path = "/tmp/mixed.log"
34  disabled = false
35  encoding = "utf-8"
36  ## [{"A":1,"B":2},{ "C":3,"D":4},...] 形態をそれぞれのログに分離することができる。
37  {"A":1,"B":2} {"C":3,"D":4}
38  multiline_pattern = "simple_json_array"
39
40  "@"
41
42  New-Item -path "C:\Program Files\WhatapInfra\extension" -name "logsink.conf" -type "file" -value $contentToAdd
   -Force
43
44  Restart-Service "Whatap Infra"

```

オプション設定

- `stats_enabled` : 収集ステータスデータの収集有無を設定します。(既定値: `false`)
 - `true` に設定する必要がある、`stats_category` で設定したカテゴリ（`logsink_stats`）に統計データが生成されます。
- `stats_category` : 収集ステータスデータを保存するメトリクスカテゴリを設定します。 `logsink_stats` に設定す

る必要があります。統計データのフィールドは次のとおりです。

保存される統計データフィールド: file checkInterval encoding filepos checkedLocalTime
lastupdatedLocalTime fileSize error firstCheck transferBytes

- **excludeNames** : ログファイルのパス (path) にアスタリスク (*) が含まれている場合、ログ収集対象外のファイル名を設定して除外することができます。カンマ (,) を区切り文字として使用することで、複数の値を設定できます。

Example

```
excludeNames = [ ".gz", ".zip" ]
```

- **nowrap_keywords** : 行単位のログ検索時に、このオプションで指定されたキーワードが検出されると、前のログと結合されます。
- **pcode** : ログを送信する同じリージョンのプロジェクトコードを入力します。
- **license** : ログを送信する同じリージョンのプロジェクトのライセンスコードを入力します。

❗ pcode 、 license オプションの場合、サーバーエージェント2.7.4バージョン以降に対応します。

Windowsイベントログのオプション設定

Windowsイベントログ収集時、次のようにオプションを設定することができます。

```
1 # 管理者権限が必要
2 New-Item -type "Directory" -Path "C:\Program Files\WhatapInfra\extension"
3
4 $contentToAdd = @"
5 [[inputs.win_eventlog]]
6     category = "win_event_log"
7     stats_category = "win_event_log_stats"
8     stats_enabled = true
9     enabled = true
10 [[inputs.win_eventlog.file]]
11     #true | false
12     enabled = true
13     # Application, Security, Setup, System, ForwardedEvents
```

```

14     file = "Application"
15     #1: Information, 2: Warning 3: Error 4: Audit Success 5 Audit Fail
16     #event_type =
17     #event id
18     #event_id =
19     #event source name
20     #source_name = ""
21     #プロジェクトコード及びプロジェクトライセンスの入力時、ログを同じリージョンの希望するプロジェクトに転送可能
22     #pcode = プロジェクトコード
23     #license = "プロジェクトライセンス"
24     #whatap_host_ip = "収集サーバーIP1/収集サーバーIP2"
25     #whatap_host_port = 6600
26
27 "@
28
29 New-Item -path "C:\Program Files\WhatapInfra\extension" -name "win_eventlog.conf" -type "file" -value $contentToAdd
   -Force
30
31 Restart-Service "Whatap Infra"

```

- カテゴリ指定(`category`) 必須
例) `win_event_log`
- 統計カテゴリ指定(`stats_category`) 必須
例) `win_event_log_stats`
- 統計カテゴリOn/Off(`stats_enabled`) 必須
例) `true` または `false`
- 収集機能On/Off(`enabled`) 必須
例) `true` または `false`
- ファイル別収集機能On/Off(`enabled`) 必須
例) `true` または `false`
- ファイル(`file`) 必須

例) Application、Security、Setup、System、Forwarded

- イベントタイプ(event_type) 非必須

例) 1、2、3、4、5

① イベントタイプ

1. Information
2. Warning
3. Error
4. Audit Success
5. Audit Fail

- イベントID(event_id) 非必須
- イベントソース名(source_name) 非必須
- プロジェクトコード(pcode) 非必須
- プロジェクトライセンス(license) 非必須

① エージェント対応バージョン

- ウィンドウイベントログ収集の場合、サーバーエージェント2.5.2バージョン以降に対応します。
- ウィンドウイベントログオプションの中で pcode 、 license オプションの場合、サーバーエージェント2.7.4バージョン以降に対応します。

複数のファイルを指定および分離

複数のファイル指定

複数のログファイルを同じカテゴリに設定するには、各ログファイルのパスを `[[inputs.logsink.file]]` 項目に追加して、`path` 設定により、ファイルパスを指定します。また、`category`、`stats_enabled`、`stats_category` などのオプションを使用して、ログ発生量の統計設定などの付加的な設定が可能です。

/root/test1 および /root/test2 ファイルを同じカテゴリ（serverlog）に指定した例です。

```
[[inputs.logsink]]
  category = "serverlog"
  stats_enabled = true
  stats_category = "logsink_stats"
  excludeNames = [ ".gz", ".zip" ]
```

```
[[inputs.logsink.file]]
  path = "/root/test1"
  disabled = false
  encoding = "utf-8"
```

```
[[inputs.logsink.file]]
  path = "/root/test2"
  disabled = false
  encoding = "utf-8"
```

❗ category、stats_enabled、stats_category、nowrap_keywords などのオプションに関する詳細は、[オプション設定](#) を参照してください。

この例は、**ログTail** メニューで次のように確認できます。

| serverlog | | | |
|-----------|--------|-------------------------|---|
| ▼ | oname | 時刻 | |
| ▼ | APPSVR | 2024-10-11 18:14:30.325 | file /root/test1 pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709
kdjfhakdhgldkjggha;dfghad;fkjggha;dfkjggha;dfgjha;fkghj;fgjh |
| ▼ | APPSVR | 2024-10-11 18:14:30.325 | file /root/test1 pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709
kdjfhakdhgldkjggha;dfghad;fkjggha;dfkjggha;dfgjha;fkghj;fgjh |
| ▼ | APPSVR | 2024-10-11 18:14:30.325 | file /root/test1 pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709
kdjfhakdhgldkjggha;dfghad;fkjggha;dfkjggha;dfgjha;fkghj;fgjh |
| ▼ | APPSVR | 2024-10-11 18:14:30.325 | file /root/test1 pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709
kdjfhakdhgldkjggha;dfghad;fkjggha;dfkjggha;dfgjha;fkghj;fgjh |
| ▼ | APPSVR | 2024-10-11 18:14:30.325 | file /root/test1 pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709
kdjfhakdhgldkjggha;dfghad;fkjggha;dfkjggha;dfgjha;fkghj;fgjh |
| ▼ | APPSVR | 2024-10-11 18:14:30.325 | file /root/test1 pcode 34 oname APPSVR agenttime 1728638069515 oid 1988910709
kdjfhakdhgldkjggha;dfghad;fkjggha;dfkjggha;dfgjha;fkghj;fgjh |
| ▼ | APPSVR | 2024-10-11 18:14:40.326 | file /root/test2 pcode 34 oname APPSVR agenttime 1728638079521 oid 1988910709
sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbvcvmbn.bcmn |

ファイル分離

異なるカテゴリにログファイルを割り当てるには、`logsink{数字}.conf` ファイルをそれぞれ作成し、各ファイルの `category` 項目に異なる値を設定してください。

`logsink.conf` と `logsink1.conf` を使用して、異なるログカテゴリを設定した例です。

logsink.conf

```
# cat logsink.conf
[[inputs.logsink]]
  category = "serverlog1"
  stats_enabled = true
  stats_category = "logsink_stats"
  excludeNames = [ ".gz", ".zip" ]

[[inputs.logsink.file]]
  path = "/root/test1"
  disabled = false
  encoding = "utf-8"
```


logsink1.conf

```
#cat logsink1.conf
[[inputs.logsink]]
  category = "serverlog2"
  stats_enabled = true
  stats_category = "logsink_stats"
  excludeNames = [ ".gz", ".zip" ]

[[inputs.logsink.file]]
  path = "/root/test2"
  disabled = false
  encoding = "utf-8"
```

❗ category、stats_enabled、stats_category、nowrap_keywords などのオプションに関する詳細は、[オプション設定](#)を参照してください。

この例は、ログTailメニューで次のように確認できます。

| ログTail | | 検索 | |
|----------|--------|-------------------------|---|
| All logs | | 検索条件: 入力された文字列を含むログ | |
| ▼ | oname | 時刻 | ログ内容 |
| ▼ | APPSVR | 2024-10-11 18:20:55.084 | file /root/test1 pcode 34 oname APPSVR agenttime 1728638454313 oid 1988910709 category serverlog1
kdjfhakdhgldkjg ha,dfgghad;fkjggha;dfkjggha;dfgjha;fkgjha;fgjh |
| ▼ | APPSVR | 2024-10-11 18:20:55.087 | file /root/test1 pcode 34 oname APPSVR agenttime 1728638454313 oid 1988910709 category serverlog1
kdjfhakdhgldkjg ha,dfgghad;fkjggha;dfkjggha;dfgjha;fkgjha;fgjh |
| ▼ | APPSVR | 2024-10-11 18:21:05.103 | file /root/test2 pcode 34 oname APPSVR agenttime 1728638464315 oid 1988910709 category serverlog2
sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbcvmbn.bcmn |
| ▼ | APPSVR | 2024-10-11 18:21:05.104 | file /root/test2 pcode 34 oname APPSVR agenttime 1728638464315 oid 1988910709 category serverlog2
sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbcvmbn.bcmn |
| ▼ | APPSVR | 2024-10-11 18:21:05.104 | file /root/test2 pcode 34 oname APPSVR agenttime 1728638464315 oid 1988910709 category serverlog2
sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbcvmbn.bcmn |
| ▼ | APPSVR | 2024-10-11 18:21:05.104 | file /root/test2 pcode 34 oname APPSVR agenttime 1728638464315 oid 1988910709 category serverlog2
sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbcvmbn.bcmn |
| ▼ | APPSVR | 2024-10-11 18:21:05.104 | file /root/test2 pcode 34 oname APPSVR agenttime 1728638464315 oid 1988910709 category serverlog2
sadlkfj;kgj'fdnc/mbnv.c,mbn.cvmbn.vc,mnbcvmbn.bcmn |

ログモニタリングの活性化

ホーム画面 > プロジェクト選択 > ログ > ログ設定

ログモニタリングを開始するセクションのログモニタリングを有効にするタブのトグルボタンで、WhaTapログモニタリングの有効または無効にできます。

-  ログモニタリングの有効化：トグルボタンをオンにするとログモニタリングが有効になり、有効化した日から15日間は無料でお試しいただけます。
-  ログモニタリングの無効化：トグルボタンをオフにするとログモニタリングが無効になり、以降ログは保存されません。

ⓘ ログモニタリングの有効化権限

エージェントをインストールした後、プロジェクトに対して編集権限を持つユーザーのみがログモニタリングを有効化できます。権限の詳細については、[次のドキュメント](#)を参照してください。

Kubernetes

Kubernetesコンテナおよびコンテナ内のアプリケーションのログを収集するための設定方法を案内します。

エージェントのアップデート

Kubernetesエージェント1.1.35バージョン以降で使用可能です。アップデート方法は[次の文書](#)を参照してください。

エージェント設定の確認

ホーム画面 > プロジェクト選択 > ログ > ログ設定

1. WhaTapモニタリングサービスの初期画面でプロジェクトを選択した後、**ログ > ログ設定** メニューに移動してください。
2. **ログモニタリングを開始する** タブの **エージェント設定およびログモニタリングの有効化** にある **1. エージェント設定の確認** の案内を参考にして、エージェント設定を確認してください。

コンテナログ収集の有効化

Kubernetesコンテナでログを収集するには、**1. エージェント設定の確認** で **ログ設定を適用** ボタンをクリックしてください。

コンテナの内部アプリケーションログ収集の有効化

Java 2.1.1、Python 1.2.2以降のバージョンで利用可能です。Kubernetesコンテナ上で実行されるアプリケーションのログを収集するには、以下を参考にしてください。

1. **ログ > ログ設定 > ログモニタリングを開始する** タブに移動してください。
2. **1. エージェント設定の確認** の下部にある  **エージェント設定** ボタンをクリックしてください。
3. **エージェント設定** で、**オプション作成** のオプション選択ドロップダウンリストから **直接入力** をクリックしてください。

4. エージェント設定コマンドのキー `logsink_enabled` と値 `true` を入力欄に入力してください。

```
logsink_enabled=true
```

5. 適用ボタンを選択します。Kubernetesコンテナ内のアプリケーションからログを収集できます。

- ① • Javaアプリケーションのログ収集に関する詳細は、[次のドキュメント](#)を参考にしてください。
- Pythonアプリケーションのログ収集に関する詳細は、[次のドキュメント](#)を参考にしてください。
- Goアプリケーションのログ収集に関する詳細は、[次のドキュメント](#)を参考にしてください。

ログモニタリングの活性化

ホーム画面 > プロジェクト選択 > ログ > ログ設定

ログモニタリングを開始するセクションのログモニタリングを有効にするタブのトグルボタンで、WhaTapログモニタリングの有効または無効にできます。

- ログモニタリングの有効化：トグルボタンをオンにするとログモニタリングが有効になり、有効化した日から15日間は無料でお試しいただけます。
- ログモニタリングの無効化：トグルボタンをオフにするとログモニタリングが無効になり、以降ログは保存されません。

① ログモニタリングの有効化権限

エージェントをインストールした後、プロジェクトに対して編集権限を持つユーザーのみがログモニタリングを有効化できます。権限の詳細については、[次のドキュメント](#)を参照してください。

Kubernetesログモニタリングのカテゴリガイド

Kubernetesに関するさまざまなログを確認できます。WhaTap Kubernetesでは、モニタリングカテゴリを提供しています。

⚠ 設定によって重複したログ内容が保存される場合があるため、重複がないか必ず確認してください。

| カテゴリ | 説明 |
|-----------------|---|
| #K8sEvent | <ul style="list-style-type: none"> Kubernetesで発生したイベントがデフォルトで保存および作成されるログ ユーザー設定に関係なく基本作成 |
| #WhatapEvent | <ul style="list-style-type: none"> WhaTapイベント設定によって発生したイベントが格納されるログ ユーザー設定に関係なく、デフォルトで作成されます |
| containerStdout | <ul style="list-style-type: none"> コンテナ標準出力ログ ユーザー設定時に作成 ノードエージェントに <code>logsink_enabled=true</code> 設定を追加したした場合 |
| AppLog | <ul style="list-style-type: none"> コンテナ内アプリケーションログ ユーザー設定時に作成 アプリケーションエージェントに <code>logsink_enabled=true</code> 設定の追加時 |

containerStdOutログフィルターの設定

ホーム画面 > プロジェクト選択 > 管理 > エージェント設定

Kubernetesログで必要な情報を選別するためのフィルタリングオプションを案内します。フィルタリングにより、許可または除外するログを設定できます。

1. 管理 > エージェント設定 に移動してください。
2. プロジェクトデフォルト タブで、オプション作成 方式から 直接入力 をクリックしてください。



ログネーミングのルール

Kubernetes containerStdOutログはノードの*/var/log/containers/*パスの下位に生成されます。次のようなネーミングルールに従っています。

```
<podName>_<namespace>_<containerName>-<containerId>.log
```

ログフィルターオプション

- **log_filter_enabled** bool

既定値 false

ログフィルターの使用有無を設定します。

- **log_filter_allow_list** list

許可するログの一覧を設定します。フィルタリングの適用時に含める項目を意味します。

- **log_filter_deny_list** list

除外するログの一覧を設定します。フィルタリングの適用時に除外する項目を意味します。

ログフィルター動作

`log_filter_enabled` オプションが有効になっている場合にのみ、ログフィルターが動作します。該当オプションの値が `true` に設定された状態で、`log_filter_allow_list` および `log_filter_deny_list` を通じてログを選択的に収集できます。

ログフィルターはブラックリストベースで動作します。例えば、`log_filter_enabled` 活性化した後 `log_filter_allow_list` オプションに追加する項目を設定しない場合、デフォルトではすべてのコンテナのログ収集がブロックされます。また、ログフィルターはallowルールよりdenyルールの優先順位が高いです。同一の項目がallowとdenyの両方に設定されている場合、denyルールが優先的に適用され、そのログは収集されません。

ログフィルターの例

単一ネームスペースログの収集

- 許容 `log_filter_allow_list` `*_infra_*`

`infra` ネームスペースに存在するすべてのコンテナが収集対象として特定されます。

マルチネームスペースログの収集

- 許容 `log_filter_allow_list` `*_infra_*`、`*_monitoring_*`

`infra`、`monitoring` ネームスペースに存在するすべてのコンテナが収集対象として特定されます。

特定の単語を含むPodを除く

- 許容 `log_filter_allow_list` `*_*_*`
- 除外 `log_filter_deny_list` `*prod*_*_*`

すべてのコンテナが収集対象として特定されますが、`podName` に `prod` が含まれているログは除外されます。

特定の単語を含むPodログの収集

- 許容 `log_filter_allow_list` `*prod*_*_*`

`podName` に `prod` が含まれるPodのログのみが収集されます。

マルチネームスペースログの収集と特定の単語を含むPodを除く

- 許容 `log_filter_allow_list` `*_infra_*`、`*_monitoring_*`
- 除外 `log_filter_deny_list` `*prod*_**`

`infra`、`monitoring` ネームスペースのログが収集され、`podName` に `prod` が含まれているログは除外されます。

コンテナ名内の特定の単語で始まるコンテナログを除外

- 許容 `log_filter_allow_list` `*_*_db-*`

すべてのネームスペースで `containerName` が `db` で始まるコンテナのログは除外されます。

ライブテール

ⓘ ログ参照権限がない場合は、そのメニューにアクセスできません。

ホーム画面 > プロジェクト選択 > ログ > ログTail

ログTail メニューでは、サーバーコンソールに接続せずに、ログデータストリームをモニタリング画面上で直接確認できます。複雑で大量のログも、フィルター と ハイライト 機能を活用して絞り込み、素早く把握できます。ログデータの取得周期は2秒です。

主な用語は次のとおりです。

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

ⓘ ログテーブルカラムの端をドラッグしてカラムの幅を修正できます。

エージェントオプション

エージェントオプションが設定されている場合、ログレベルを収集し、各ログの左側に色付きの縦線が次のように表示されます。

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

❗ エージェントのオプション設定

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

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

1 フィルター領域

フィルター適用

フィルターを適用すると、入力した条件に合ったログをフィルタリングします。複数のフィルターを入力できます。フィルターのタグが同じ場合、OR(||)、そうでない場合はAND(&&)が適用されます。

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

❗ ガイドUI

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



検索キー、オペレーター、検索値の入力

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

- 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

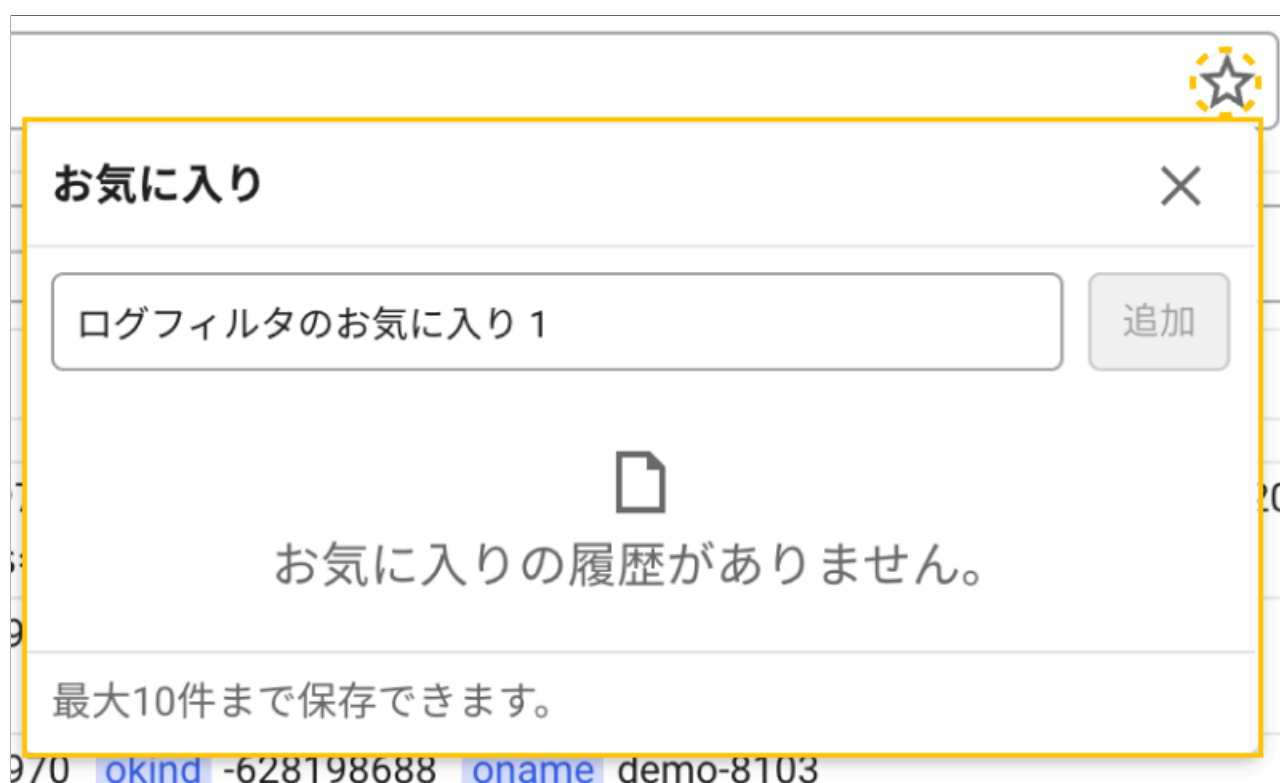
入力フィールドにテキストを入力し、Enter または Tab キーを押すか、入力欄下のガイド UI で推奨値をクリックまたは矢印キーで選択して追加できます。

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 == ote-account 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

カテゴリー

AppLog

フィルター

content

+=select*

×

フィルターを入力してから「Enter」キーを押して追加します。

content == +=select*

act

🔍

⏸

🔄

📄

⚙

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

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

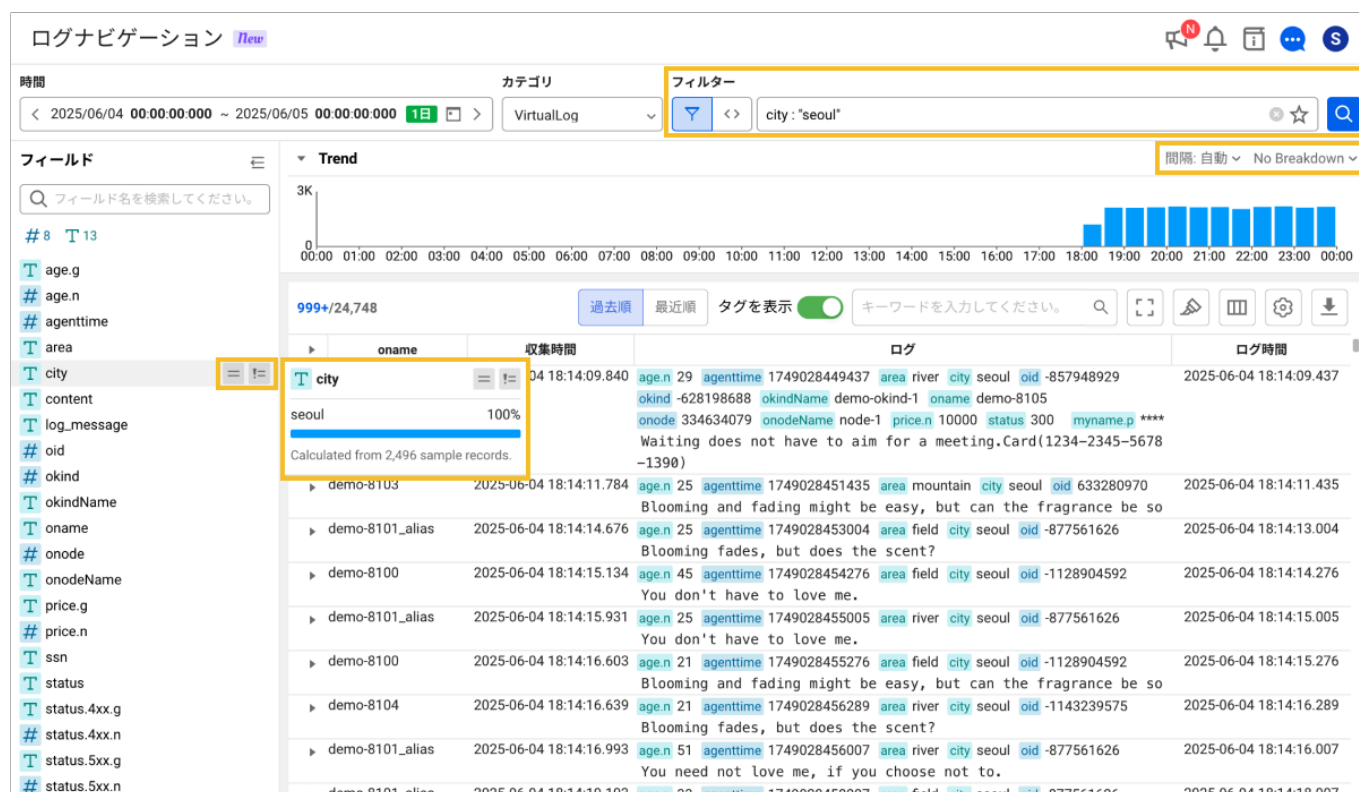
ⓘ ログ参照権限がない場合は、そのメニューにアクセスできません。

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
 - `^ / v` アイコン: 行の移動
 - `Cmd + F` (Mac) / `Ctrl + F` (Windows): キーワード検索

複数キーワード条件

複数キーワードでハイライトする場合は、次のように作成します。

| 入力文字列 | 説明 | 結果 |
|--------------------------------|---|-----------------|
| <code>a b c</code> | 各キーワードをスペースで区切ります。 | a, b, c |
| <code>"Whatap is good."</code> | キーワードにスペースを含める場合は、 <code>"</code> または <code>"</code> で囲みます。 | Whatap is good. |

| 入力文字列 | 説明 | 結果 |
|---------------------|--|------------------|
| "Whatap\\ is good." | ""で囲まれたキーワードに、\を含める場合は、\\と入力する必要があります。 | Whatap\ is good. |

ハイライトカラー設定

ハイライトするキーワードおよび色を設定できます。

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

カラム設定

 ボタンをクリックして、カラムを追加したり順序を設定することができます。

カラム追加

カラム追加：タグを選択して、テーブルにカラムを追加できます。

 ログカラムの選択を解除すると、**ログ表示詳細設定**を確認できません。必ず1つ以上のカラムを選択します。

カラム順序設定

カラム設定でカラムを追加すると、**表示項目**に該当カラムが追加されます。希望するカラムをドラッグして、カラムの順序を変更してください。

ログ表示詳細設定

⚙ ボタンをクリックして、ログの表示を詳細に設定します。デフォルトでは **content**、**タグ** の両方がチェックされており、両方の項目が表示されます。

- **content**と**タグ**のいずれかを必ず選択してください。
- **タグ管理**リストにタグを追加すると、追加した順にログのタグが表示されます。タグの順序はドラッグで変更できます。追加したタグを無効にすると、無効にしたタグはログのタグに表示されません。
- チェックが解除された項目は、テーブルに表示されません。次のように**タグ**を解除する場合、テーブルからログの**タグ**は表示されません。

log table contents remove tag sc

ⓘ カラムおよびログ表示設定の適用範囲

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

ログファイルのダウンロード

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

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

WhaTap log search query 文法

👍 これは、WhaTapログエクスプローラーで使えるWhaTapログ検索クエリ構文に関するドキュメントです。

1. Equal

- `field : value`

2. Not

- `not field : value`

3. Wildcard (`String` タイプのフィールドのみ使用可能、検索値の前後に `"` は不)

- `field : val*`

4. Exist

- `field : *`

5. Range (`Number` タイプのフィールドのみ使用可能)

- `<`, `>`, `<=`, `>=` が使用可能
- 例: `field < 30 and field >= 10`

6. Combining Multiple Queries

- AND 例: `field < 30 and field >= 10`
- OR 例: `field < 30 or field >= 10`

7. Grouping

- 例: `(field < 30 or field >= 10) and other : 70`

8. Escaping Special Characters

- Luceneでエスケープが必要な特殊文字一覧: `&` `&` `|` `|` `!` `(` `)` `{` `}` `^` `"` `~` `*` `?` `:` `\` `/`
- 文字の前に `\` を付けてエスケープする
- 例: `(1+1):2` を検索するには `\(1\+1\)\:2`

検索インデックスフィールドタイプ

サポートされるフィールドタイプは `Number` と `String` の2種類のみです。

- `Number` : Long、double、floatタイプの数値値
 - 使用例 : `field : "value"`
- `String` : メール本文のような全文テキスト
 - 使用例 : `field : value`
- `Boolean` : True または False
 - `field : true` または `field : false` の形式で使します

ログトレンド

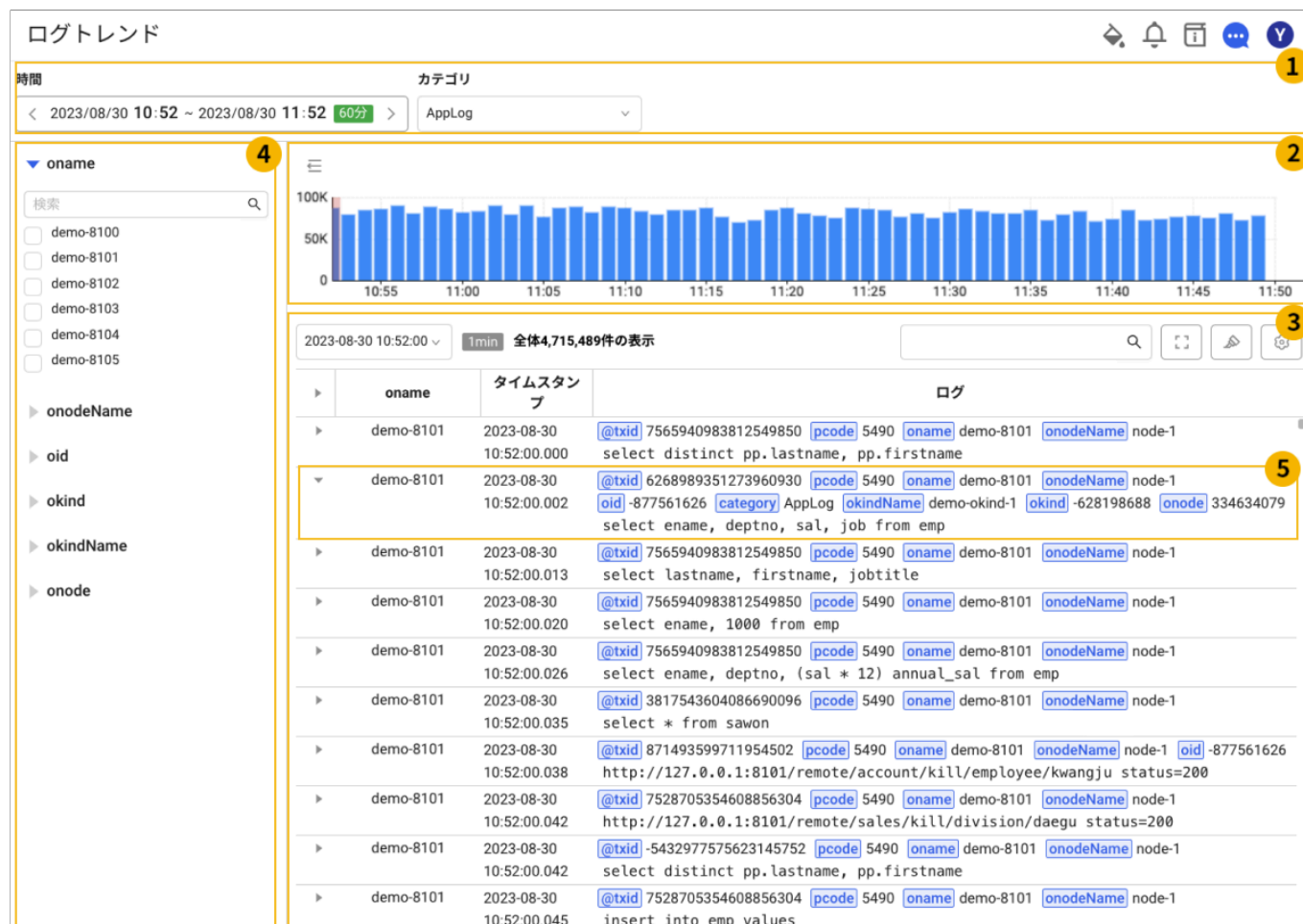
ⓘ ログ参照権限がない場合は、そのメニューにアクセスできません。

ホーム画面 > プロジェクト選択 > ログ > ログトレンド

ログトレンドでは、タイプ別に分類されたログの発生件数の推移を通じて、特定エラータイプの発生パターンを確認し、時間別の詳細ログデータを確認できます。ハイライト機能により、目的のログをすばやく識別できます。カテゴリ別に収集されたログの推移を照会できます。

主な用語は次のとおりです。

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



データ参照

- 下部までスクロールすると、次のデータを表示します。
- 1で検索するログデータの時間と収集単位としてカテゴリを指定します。
- カテゴリを変更すると、選択されたカテゴリに対応するログを表示します。2バーチャートと3ログテーブルで確認できます。
- 2棒グラフのバーをクリックすると、バーの時間範囲に対応するログを検索します。
- 3ログテーブルの左上から照会されたログの総数を確認できます。
- 3 ログテーブル上段の右の「全画面」アイコンを選択すると、ログと収集時間を全画面で確認できます。
- 4 サイドメニューからタグでフィルタリングすることでログを確認できます。検索キーは最大2つまで選択でき、

検索値は複数選択できます。

- エージェントオプションが設定されている場合、ログレベルを収集し、各ログの左側に色付きの縦線が次のように表示されます。

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

❗ エージェントのオプション設定

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

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

- ❗ ログテーブルカラムの端をドラッグしてカラムの幅を修正できます。

個人情報の照会

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

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

ログContentの確認

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

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

ハイライト設定

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

コンテンツハイライト

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

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

複数キーワード条件

複数キーワードでハイライトする場合は、次のように作成します。

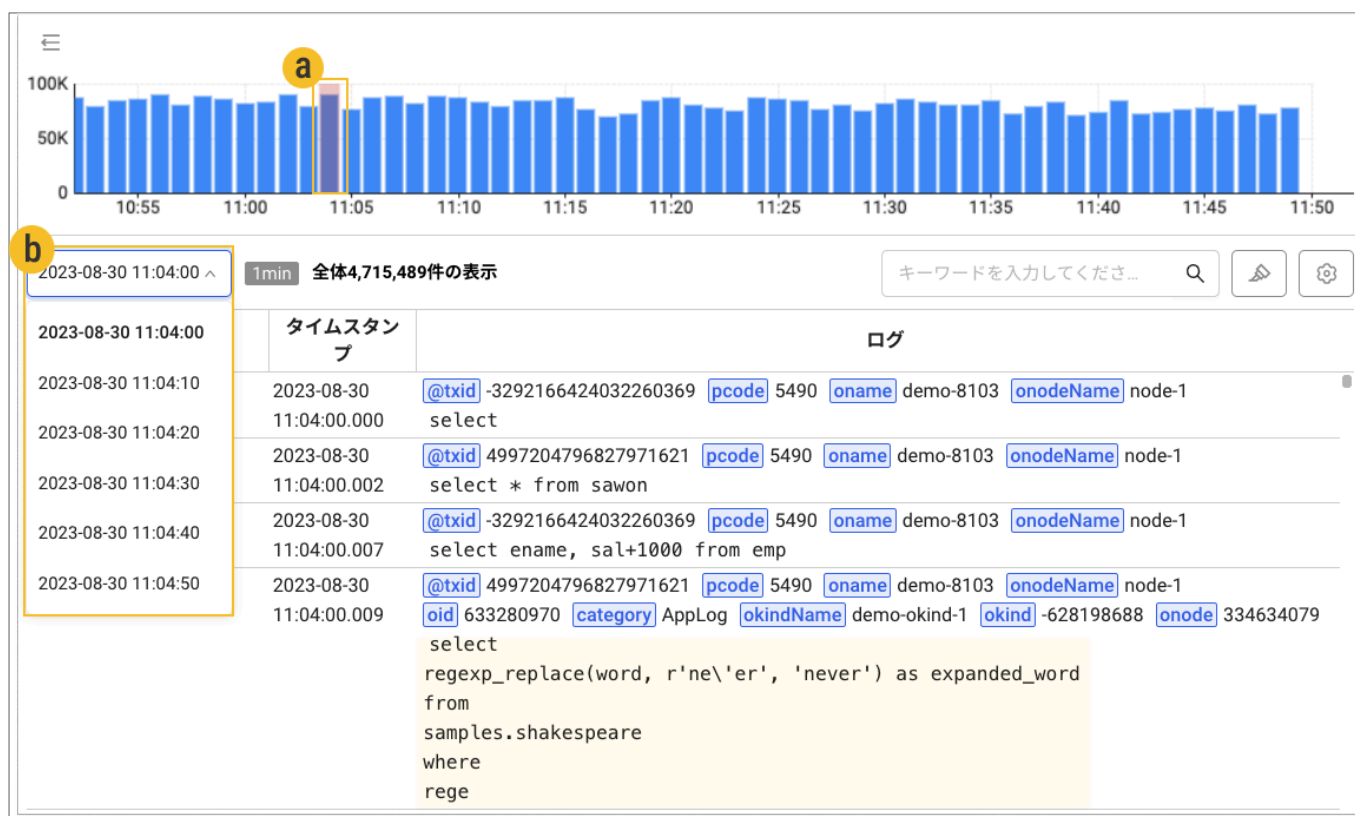
| 入力文字列 | 説明 | 結果 |
|---------------------|--|-------------------|
| a b c | 各キーワードをスペースで区切ります。 | a, b, c |
| "Whatap is good." | キーワードにスペースを含める場合は、" または "" で囲みます。 | Whatap is good. |
| "Whatap\\ is good." | ""で囲まれたキーワードに、\ を含める場合は、\\ と入力する必要があります。 | Whatap\\ is good. |

ハイライトカラー設定

ハイライトするキーワードおよび色を設定できます。

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

ログをチャートで検索



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

テーブル設定

カラム設定

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

- ・ **カラム追加**

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

- ・ **カラム順序設定**

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

ログ表示詳細設定

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

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

ログテーブルコンテンツタグ非表示

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

ⓘ カラムおよびログ表示設定の適用範囲

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

ログファイルのダウンロード

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

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

ログの検索

❗ ログ参照権限がない場合は、そのメニューにアクセスできません。

ホーム画面 > プロジェクト選択 > ログ > ログ検索

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

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

主な用語は次のとおりです。

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

1 ログ検索

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

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

category == AppLog

2

AppLog (4,404,050)

AppStdErr (438)

AppStdOut (19,489)

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

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

4

データ参照

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

| | | | | | | | |
|---|-------|------|---------------|-----------|-----------|--|-----------------------|
| 2023-12-18 14:31:02.563 | INFO | 2277 | 1702877462042 | 778873916 | AppLog | io.home.test.logback02starter.base.web.LogbackControllerGreeting | |
| INFO log in our greeting method. | | | | | | | |
| 2023-12-18 14:31:02.563 | WARN | 2277 | 1702877462043 | 778873916 | AppLog | io.home.test.logback02starter.base.web.LogbackControllerError | http-nio-19090-exec-2 |
| io.home.test.logback02starter.base.errors.exception.ApiException: [2284] 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: [2284] 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: [2284] 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: [2284] 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: [2284] 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。

① ガイドUI

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



検索キー、オペレーター、検索値の入力

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

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

フィルタータグ追加

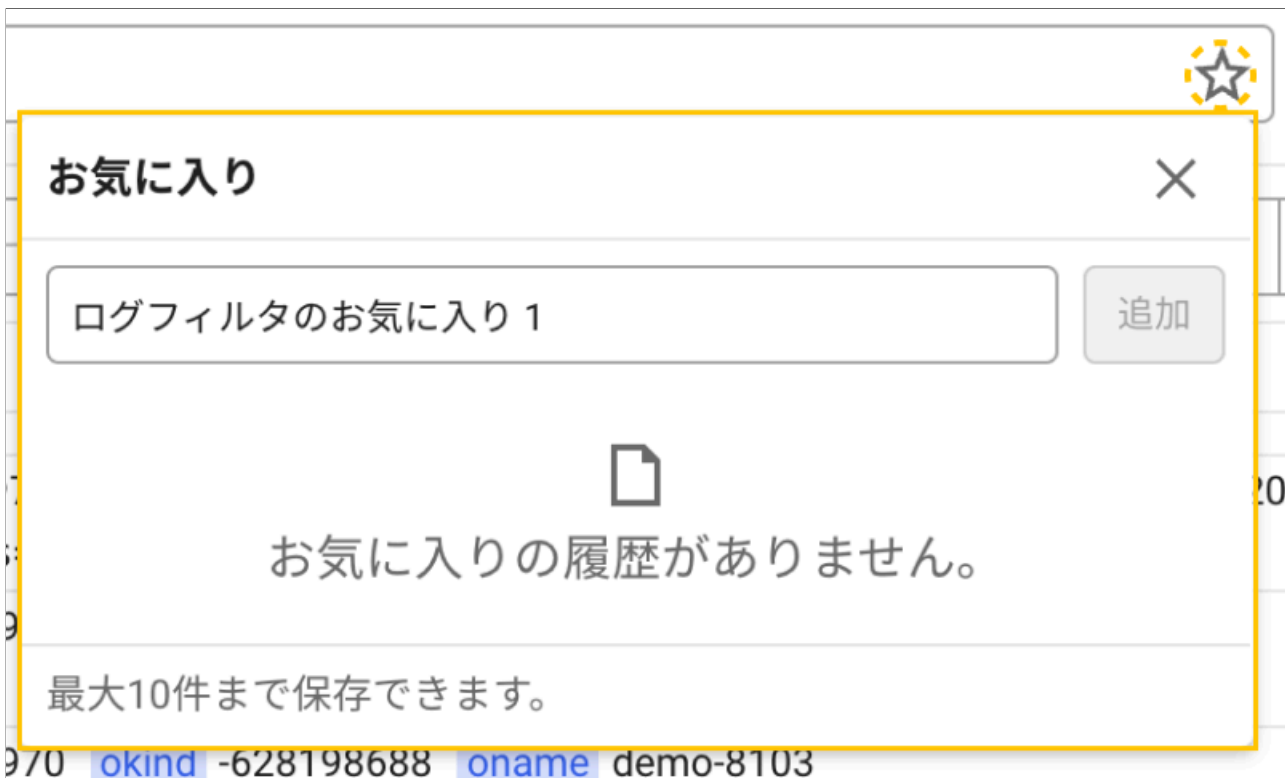
入力フィールドにテキストを入力し、Enter または Tab キーを押すか、入力欄下のガイド UI で推奨値をクリックまたは矢印キーで選択して追加できます。

フィルタータグの削除

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

フィルターのお気に入り

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



フィルター適用の例外状況

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

構文解析されていないキーワードのフィルター適用

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

フィルター ⓘ

🔍 content == *select* ✕

フィルターを入力してから「Enter」キーを押して追加

✕

content == *select*

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

ログ検索

時間: 2024/01/15 14:50 ~ 2024/01/15 15:50 6000

フィルター: category == ApplLog && oid == 397157872 && content != "select"

category == ApplLog && oid == 397157872 && content != "select"

全体の41,513件の内、10,500件を照会し、検索された結果は9999+件です。

AppLog (41,513)

controller debug_point status
exception filename host ip
java_class key level log_source
loggername method namespace
oid okind okindName name
referer region responseTime
send_pack_count service status
status_4xx status_success
status_nxx targetPcode task
taskPoolActiveCount
task_delayedTime threadName
type uri

AppStdErr (2,355)

AppStdOut (56,731)

AppStdIn (56,731)

ログをもっと照会しますか？
ログパーサーを追加することで、追加の照会なしで検索ができます。
ログパーサーの設定 追加照会

- ① 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 X

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

| 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 |
|-------------------------------|----------------------------|---------------------------------------|
| <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か、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> |
| <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。

- ❗ ・ 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

ホーム画面 > プロジェクト選択 > ログ > ログ設定

ログ設定 の上部タブからログモニタリングを設定できます。 エージェント設定の確認、ログモニタリングの有効化設定、ログデータの保持期間および照会パスワードの設定、ログパーサーの登録、クイックインデックスの設定、個人情報のマスキング管理などを行うことができます。

！ 権限

- ・ **ログモニタリング機能の活性化** を使用するには、**プロジェクト修正** 権限が必要です。
- ・ **ログエディター** 権限があれば、**ログモニタリング機能の活性化** のほか、**ログ設定** メニューを編集できます。

ログモニタリングを開始する

ログモニタリングの開始 ログフィルター設定 ログプライマリパーサ設定 ログセカンダリパーサの設定 高速インデックス設定 ログ長期保存統計 個人情報の非属別化

エージェントの設定とログモニタリング活性化 料金プラン表示

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

▼ 1. エージェント設定の確認

Javaアプリケーションからログを収集するには、次の点を確認してください。
1. エージェントバージョンを確認して、必要だったらアップデートしてください。（v2.1.1以降のバージョンから可能）
2. エージェント設定 > オプション作成 > オプション選択 > 直接入力 > 下のエージェント設定コマンドを入力してください。
3. 再起動してください。

エージェント設定

logsink_enabled=true コピー

▶ 2. ログモニタリング機能の活性化

ログモニタリングデータの設定 初期化 保存

ログ照会パスワード ☐ ログ照会の際にパスワードを入力するようにするには、オンにしてください。

ログ保存期間(初期値) 最小1日から最大40日まで入力できます。

ログ使用量

| カテゴリ | データ保存期間 | 累積ログ数(保存期間基準) | 平均ログ数(日) | ログ数(前日) | 予想ログ数(1週間) | 予想ログ数(1月間) |
|------------|---------|---------------|-------------|-------------|---------------|---------------|
| Total | | 3,523,236,480 | 234,882,433 | 124,084,216 | 1,644,177,010 | 7,046,472,900 |
| AppLog | 15日 | 3,494,072,628 | 232,938,175 | 123,070,829 | 1,630,567,225 | 6,988,145,250 |
| AppStdErr | 15日 | 338,233 | 22,548 | 12,222 | 157,836 | 676,440 |
| AppStdOut | 15日 | 13,911,268 | 927,417 | 483,168 | 6,491,919 | 27,822,510 |
| VirtualLog | 15日 | 14,914,351 | 994,290 | 517,997 | 6,960,030 | 29,828,700 |

1. ログ > ログ設定 の ログモニタリングの開始 タブをクリックしてください。
2. ⓘ ガイド表示アイコンと 料金プラン表示ボタンを選択すると、案内画面に移動します。

エージェント設定とログモニタリングの有効化

- ① 領域でエージェント設定を確認し、ログモニタリングの有効化または無効化を設定できます。

エージェントの設定確認

ログモニタリングを開始するために、エージェントのバージョンと設定情報を確認してください。1. エージェント設定の確認 の案内に従って進めてください。

- アプリケーションモニタリング

アプリケーション別の適用方法については、[Java](#)、[PHP](#)、[Node.js](#)、[Python](#)、[Go](#) のドキュメントを参照してください。

- サーバーモニタリング

サーバーモニタリングの適用方法については、[Server](#) ドキュメントを参照してください。指示に従って [whatap.conf](#) にログモニタリング対象ファイルの設定を追加します。

- Kubernetesモニタリング

Kubernetesモニタリングの適用方法については、[Kubernetes](#) ドキュメントを参照してください。

ログモニタリングの有効化

ログモニタリングを有効化または無効化できます。2. ログモニタリング機能の活性化 でログモニタリングの有効／無効を設定してください。

-  ログモニタリングの有効化：トグルボタンをオンにするとログモニタリングが有効になり、有効化した日から15日間は無料でお試しいただけます。
-  ログモニタリングの無効化：トグルボタンをオフにするとログモニタリングが無効になり、以降ログは保存されません。

ログモニタリングのデータ設定

2 領域でログ使用量が確認できます。またログ保存期間とログ照会パスワード設定を変更できます。

ログ参照パスワード

セキュリティを強化するため、**ログ照会パスワード**を設定してください。ログ検索パスワードの指定はオプションです。ログ検索パスワードを使用中の場合は、ログ画面に入るときは必ずパスワードを入力します。

❗ パスワードを忘れた場合

ログ編集権限を持つユーザーは、**ログ設定** で新しいパスワードに変更できます。

ログ保存期間

共通に適用する基本(default) データ保持期間です。

- 最小1日から最大40日まで入力できます。未指定の場合、既定値は1日です。ログ保存期間の選択オプションの他に、ユーザーが希望する期間を入力できます。
- **ログ使用量**一覧で別に設定しない場合、このログデータの保存期間がデフォルトで適用されます。**ログ使用量** リストでカテゴリごとのデータ保持期間を設定し、**初期化** ボタンをクリックすると、デフォルトのデータ保持期間に初期化されます。

ログ使用量

ログ使用量一覧でカテゴリ別のログデータの保存期間を指定できます。ログ数は、当該期間中に蓄積されたログの件数を意味します。例えば、**日間ログ数**は、1日にたまったログ件数、**予想ログ数**は、データ保持日に今日のログ数を掛けたログ件数を意味します。

ログデータの保存期間を次のように指定できます。期間指定により、古いデータを削除してスペースを確保できます。

- **トライアルプロジェクト**
データ保存期間として1日、2日、3日を選択できます。
- **有料プロジェクト**

データの保存期間として1日、2日、3日、4日、5日、6日、7日、10日、30日、40日が選択できます。

- **保存量基準課金**

データの保存期間によってコストが異なります。

例、1日平均200万ログ件数が蓄積され、データ保存期間を3日に指定した場合、平均600万ログ件数が収集サーバーに保持され、課金の対象となります。

ログフィルター設定

ログフィルター設定は、ユーザーが指定したフィルター条件に一致するログのみを保存する機能です。必要なログだけを保存することでコストを削減できます。

ⓘ 権限

ログ編集権限を持つユーザーのみ設定できます。

ログフィルター設定の追加

新しいフィルター設定を追加する方法です。ログフィルターを設定する際は、フィルター名、ライブテール表示有無、カテゴリ、フィルター条件が必須入力項目です。

保存しないログであっても、ライブテール表示有無トグルを有効にするとライブテールで確認できます。

ⓘ カテゴリごとに設定できるフィルターは1つのみです。

1. ログ > ログ設定 > ログフィルター設定 タブに移動します。
2. + 追加 ボタンをクリックして新しいフィルター設定を作成します。
3. ログフィルター設定追加で フィルター名、ライブテール表示有無、カテゴリ、フィルター条件 を入力します。
 - フィルター名: フィルターを識別する名前
 - ライブテール表示有無: 保存の有無に関係なくライブテールに表示するかを選択
 - カテゴリ: フィルターを適用するログカテゴリ (複数選択可能)
 - フィルター条件: フィルターに保存するログの条件

ⓘ フィルター条件の詳細については [WhaTap log search query 構文](#) を参照してください。

- 例
 - 含む: `oid:123`
 - oid が 123 のログだけを収集します。
 - 含まない: `not oid:123`
 - oid が 123 ではない ログだけを収集します。
 - すべて含む: フィルター条件を未入力
 - すべて含まない: `not content:*`

4. 追加 ボタンをクリックすると、登録結果プレビューで各フィルター設定を確認・修正できます。

5. 確認が完了したら、適用 ボタンをクリックしてログフィルター設定を保存します。

シミュレーション

入力したカテゴリとフィルター条件でログを事前に検索し、ログフィルターを適用する前に結果を確認できます。

シミュレーション ボタンをクリックすると、フィルターが適用された **ログ検索** 画面が表示されます。

ログフィルター設定の修正

登録済みのログフィルターは編集アイコンをクリックして修正できます。

ログフィルター設定修正 画面では既存の値が表示され、必要な項目を変更して適用できます。

 ログフィルターを修正する際、選択できるカテゴリは1つのみです。

ログフィルター設定の削除

登録したフィルターは削除アイコンをクリックして削除できます。削除後は必ず **保存** ボタンをクリックしてください。

❗ 変更を保存しないとフィルターは削除されません。

ログフィルター設定のJSONインポート/エクスポート

ログフィルター設定はJSON形式でインポート/エクスポートできます。
他のプロジェクトに同じログフィルターを適用したい場合に便利です。

JSONエクスポート

1. 画面右上の **JSON**  をクリックします。
2. **JSONエクスポート** ウィンドウが開いたら、**エクスポート** ボタンをクリックします。
3. ログフィルター設定がJSONファイルとしてダウンロードされます。

JSONインポート

1. 画面右上の  をクリックします。
2. インポートするJSONファイルを選択します。
3. **JSONインポート** ウィンドウで **リストに追加** または **上書き** を選択してログフィルター設定をインポートします。
4. **保存** ボタンをクリックして変更を反映します。

バリデーション条件

設定を保存する際のバリデーションは次の通りです。

- **type:** **GENERAL** のみサポート
- **category:** 必須、**string** タイプのみサポート
- **condition**
 - **language:** **jsonDsl** , **lucene** のみサポート
 - **description:** 無効なフィルター条件は保存できません

- **showLiveTail:** `boolean` タイプのみサポート
- **name:** 必須、`string` タイプのみサポート

ログパーシング

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)?|[Ee]rr?(?:or)?|ERR?(?:OR)?|[Cc]rit?(?:ical)?|CRIT?(?:ICAL)?|[Ff]atal|FATAL|[Ss]evere|SEVERE|EMERG(?:ENCY)?|[Ee]merg(?:ency)?)`
- name: `DATA`
 - regular expression: `.*`

GROK parsing pattern

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

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

ンは、複雑で長い正規表現を簡単に適用できる機能を提供します。

Tag extraction

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

(?<SEMANTIC>REGX) 活用の例

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

Unparsed area

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

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

semantic replace

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

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

サンプルログパースキーワード別にマッチングされる正規表現

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

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

正規表現の基本文法

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



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

このようにパージ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
```

上記の内容でパージングすると、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。

448

❗ GROKパーサの注意事項

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

GROK追加パターンの選択

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

追加パターンカテゴリのドロップダウン

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

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

カテゴリ別パターンタイプ一覧

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

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

活用例

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

Sample log

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

GROK parsing pattern

```
%{CATALINA8_LOG}
```

Tag extraction

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

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

パターン詳細表示

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

パターン詳細表示

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

各パターン項目で次の機能を使用できます。

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

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

シミュレーションサンプルログの保存

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

JSONパーサ

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

JSONを適用する

ログ設定 > ログプライマリパーサ設定

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

Example

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

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

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

×

パーサ シミュレーション

ガイド表示

パターン

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

Prefix

-

Postfix

-

Ignore

url

ログ

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

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

シミュレーション

シミュレーション結果 成功しました。

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

性能測定の結果 成功しました。

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

パターン適用

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

7. パターン適用後、カテゴリとログ検出条件、パターンを入力します。

453

×

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

454



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

JSONフォーマット活用例

Sample log

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

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

Tag extraction

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

JSONフォーマットを一部構成する時の活用例

Some JSON format sample log

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

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

Tag extraction

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

ログ高速インデックス設定

高速インデックス設定

ログ設定メニューの上段から高速インデックス設定タブを選択します。大量のログを収集すると、ログ検索性能が低下する場合があります。よく使う検索条件は、インデックス(index)で生成すると、ログ検索がより速くなります。設定項目は次のとおりです。

| 設定値 | 必須の有無 | 説明 |
|---------------|-------|--------------------------|
| カテゴリ | 必須 | 高速インデックスを設定するカテゴリ |
| 検索キー | 必須 | 高速インデックスを設定する検索キー |
| 大文字と小文字を区別しない | オプション | 大文字と小文字の区別するかどうか |
| ルール | 必須 | * を少なくとも 1 つ以上を含める必要あり |
| 活性化有無 | 必須 | 活性化または非活性化の設定(既定値 true) |

ログ長期保管統計設定

ログ長期保存統計の設定

ログ設定メニューの上段からログ長期保存統計タブを選択します。ログデータは、非常に大容量のため、長期間保存することは難しいです。したがって、ログ統計データの設定機能を使用して特定の条件を満たすログデータが5分ごとに何件収集されたかに関する情報を保存できます。長期間にあたって、実際のログデータが削除されても、条件を満たすログがどれだけ収集されているかの推移は確認できます。

ログ長期保存統計の追加

×

ログ長期保存統計 追加

統計キー*

統計キーを入力してください。

データ保存期間
(ディスク使用量)

15日 (約 3 MB) ▾

カテゴリ*

カテゴリを選択してください。

ログ検出条件*

まず、カテゴリを選択してください。 ▾

まず、カテゴリを選択してください。

除外 ☐

大小文字を区別する ☒

+ 追加する

追加

ログ長期保存統計タブで + 追加する ボタンを選択するとログ長期保存統計 追加画面が表示されます。 + 追加する ボタンでルールを追加したり、作成したルールを**-**アイコンで削除できます。

設定項目

| フィールド | 説明 |
|-----------|--|
| カテゴリ | ルールが適用されるカテゴリです。 |
| 統計キー(key) | ルールを満たすログが発生した場合、保存するキーとして同じキーを重複で設定できません。 |
| ログ検出条件 | ログ統計データを生成する条件です。この条件を満たすログがどのくらい収集されたかで統計データを生成します。 |
| 除外 | 除外をチェックすると、入力した条件を満たさない値で統計データを作成します。 |
| 大小文字を区別する | 入力したログ検出条件の値に対して大文字と小文字の区別有無を指定します。 |
| 活性化有無 | 活性化または非活性化の設定(既定値 true) |

例

次のように設定を追加した場合、収集されたログのうち、statusが 200 , 300 のログを対象にTotalCountのキーで統計データを作成します。

| ログ長期保存統計 指定した条件を満たすログがどれ程収集されたかの統計データが生成できます。  | | | | | + 追加する | 保存 |
|---|------------|-----------------|-------------------|-------------------------------------|---|---|
| カテゴリ | 統計キー | ログ検出条件 | データ保存期間 (ディスク使用量) | 活性化 | | |
| AppLog | TotalCount | status 200, 300 | 15日 (約 3 MB) | ☒ |  |  |

データ参照

1. 統合Flexボードのウィジェットテンプレートでログ長期保存統計を検索し、ウィジェットを作成します。



ウィジェットテンプレート

⇒ 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

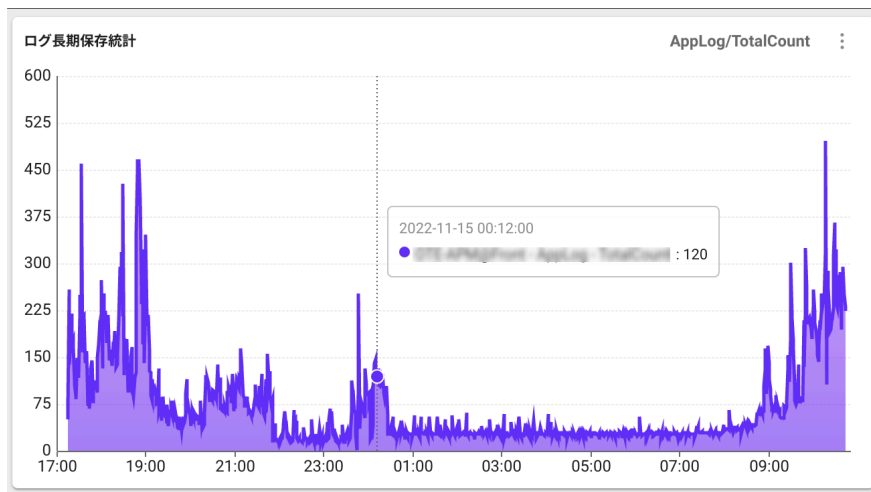
キャンセル 適用

ⓘ 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。



ログ個人情報非識別化設定

個人情報の非識別化

個人情報の非識別化ではログデータ内の個人情報をマスキング処理したり、安全な値に置換できます。

- 暗号化の保存：指定された機密な情報は暗号化され、データベースに保存されます。
- マスキング処理：ログ画面に表示される時、機密な情報は基本的にマスキング(*******)処理されて表示されます。
- 置換処理：機密な情報をユーザーが指定した安全な値に変更します。

個人情報の分類

一般的に個人情報として分類する項目は次のとおりです。一般の個人情報以外にも機密な情報として処理すべき項目があれば**個人情報の非識別化機能**を通じて、ログ内で必要な項目をマスキング処理または置換処理してください。

- 個人識別番号
- パスポート番号
- 運転免許証番号
- 外国人登録番号
- クレジットカード番号
- 銀行口座番号
- 生体情報

要求権限

非識別化された個人情報はマスキング処理されて表示されます。 **ログの個人情報照会権限**が付与されたユーザーのみ **個人情報の表示** トグルを通じて元のデータを確認できます。非識別化の対象検索キーの追加及び修正は、**ログ編集権限**が必要です。

❗ ログの個人情報照会権限及びログ編集権限の詳細は[次の文書](#)を確認してください。

個人情報の非識別化設定

新規のログデータにマスキング処理を適用して機密な情報を保護できます。

ログ設定

ログモニタリングの開始 ログプライマリパーサ設定 ログセカンダリーパーサの設定

個人情報の非識別化 個人情報が含まれた検索キーを追加すると、当該データを暗号化して保存し、マスキングします。

活性化 ☒ カテゴリ AppLog @txid agenttime @mt

ログ個人情報の非識別化チェック 以前に積み重ねられたログを非識別化します。

時間 < 2025/01/21 16:48 ~ 2025/01/21 17:48 1時 >

カテゴリ カテゴリを選択してください。

個人情報項目

個人情報パターン

置換を適用するかどうか ☒

置換値 ①

点検開始 チェックを中止

× 個人情報の非識別化 追加

カテゴリ *

カテゴリを選択してください。

検索キー *

暗号化保存およびマスキング処理する検索キーを選択します。

暗号化する検索キーを入力してください。

追加

1. 個人情報の非識別化タブで追加するボタンを選択します。
2. 右側の個人情報の非識別化 追加画面でカテゴリを選択し、マスキング処理する検索キーを入力します。
3. 追加ボタンをクリックして設定を追加します。
4. 個人情報の非識別化一覧で非識別化項目を確認した後、右上の保存ボタンを押して現在の設定を保存してください。

| 個人情報の非識別化 個人情報が含まれた検索キーを追加すると、当該データを暗号化して保存し、マスキングします。 | | | | + 追加する | 保存 |
|--|------------|-----------|-------|--------|----|
| 活性化 | カテゴリ | 検索キー | 修正 | | |
| ☐ | VirtualLog | agen | 削除 編集 | | |
| ☒ | VirtualLog | status | 削除 編集 | | |
| ☒ | AppLog | agenttime | 削除 編集 | | |

- 非識別化処理された検索キーの場合、ログコンテンツ内の **検索キー.pii** 形式で出力されます。

- 個人情報の非識別化一覧内の活性化カラムで非識別化項目を  活性化にできます。
- 個人情報の非識別化一覧内の編集カラムで  修正及び  除去できます。

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

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

個人情報の表示

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

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

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

例: **status.pii** 例 *******

ログの個人情報の非識別化点検

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

❗ できません。

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

対象キー指定による置換

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

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

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

ログ個人情報の非識別チェック

収集されてあるログを非識別化します。

[✓ チェック履歴の確認](#)

時間

< 2025/03/21 12:26 ~ 2025/03/21 13:26 1時 >

カテゴリ

VirtualLog

個人情報項目

個人識別番号

個人情報パターン

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

置換の適用有無

☐

置換値

*****_*****

チェック開始

チェック中止

カテゴリ

VirtualLog

検索開始時刻

2025/03/21 12:26

検索終了時刻

2025/03/21 13:26

個人情報項目

個人識別番号

個人情報パターン

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

置換値

*****_*****

パターンのマッチング結果

0 ☒ 結果の確認

チェック作業の開始時刻

2025/03/21 13:28

チェック作業の終了時刻

2025/03/21 13:28

置換の適用有無

No

チェック作業の結果

SUCCESS

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

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

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

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

6. 条件を入力した後、**チェック開始**ボタンを選択します。

❗ 点検中の場合はいつでも**チェック中止**ボタンで点検過程を中止できます。

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

個人情報の非識別チェックの開始
×

選択した個人情報パターンに一致する値を置き換えます。

❗ 置き換え後はデータの復元ができません。

置き換えが必要な場合は "**置き換え**" を直接入力してください。

置き換え

キャンセル

確認

8. 点検作業の完了後、例の画像のように右側から**チェック作業の結果**を確認できます。
 - **カテゴリ**：点検されたカテゴリ情報を表示します。
 - **検索開始時刻**及び**検索終了時刻**：点検が実行された時間範囲を表示します。
 - **個人情報項目**：点検された個人情報の項目を表示します。

- **個人情報パターン**：使用された正規表現式のパターンを表示します。
- **置換値**：適用された置換値を表示します。
- **パターンのマッチング結果**：識別された個人情報の数を表示します。**結果の確認**をクリックするとサンプルログを確認できます。
- **チェック作業の結果**：個人情報が識別された結果を表示します。

SUCCESS (点検成功)、FAILED (点検失敗)、STOP (点検中止)、TIMED_OUT (時間超過による点検終了)

チェック履歴の確認

ログ個人情報の非識別化点検を行った後、過去に行われた点検結果を照会するには、上段右側で**チェック履歴の確認**ボタンをクリックします。置き換え履歴、点検時点、適用された個人情報項目などを追跡できます。また**チェック履歴の確認**画面の上段右側の  **CSV** ボタンをクリックすると_CSV_ファイル形式でそのリスト情報をダウンロードできます。

| チェック履歴の確認   | | | | | |
|--|---------------|------------------|------------------|---------|-----------|
| <div> <div> < 2025/03/25 08:17 ~ 2025/03/25 09:17 1時  > </div> <div> 個人情報項目  </div> <div>  </div> <div>  CSV </div> </div> | | | | | |
| | パターンのマッチング... | チェック作業の開始時刻 | チェック作業の終了時刻 | 置換の適用有無 | チェック作業の結果 |
| *** | 0 | 2025/03/25 09:16 | 2025/03/25 09:16 | No | SUCCESS |
| *** | 0 | 2025/03/25 09:16 | 2025/03/25 09:16 | No | SUCCESS |
| *** | 0 | 2025/03/25 09:16 | 2025/03/25 09:16 | No | SUCCESS |

個人情報のパターン

既存のログデータから個人情報を識別する際に使用される正規表現式のパターンの例は以下の通りです。

| 個人情報のパターン | 個人情報の例 | 正規表現式パターン | 置換される値 |
|-----------|-----------------|---|--------------------|
| 個人識別番号 | 123456-1234567 | (?<!w)d{2}(0[1-9] 1[0-2])([0-2][0-9] 3[0-1])-[1-4]d{6}(?!w) | *****_
***** |
| パスポート番号 | M1234567 | ([MSRODTC][0-9]{7}\b) | ***** |
| 運転免許証番号 | 01-23-456789-00 | (?<!w)d{2}-d{2}-d{6}-d{2}(?!w) | **_**_
*****_** |
| 外国人登録 | 987654-1234567 | (?<!w)d{6}-?[5-8]d{6}(?!w) | *****_
***** |

| 個人情報のパターン | 個人情報の例 | 正規表現パターン | 置換される値 |
|------------|---------------------|--|-------------------------|
| 番号 | | | |
| クレジットカード番号 | 1234-5678-9012-3456 | (?<!w)d{4}-d{4}-d{4}-d{4}(?!w) | ****_****_
****_**** |
| 携帯電話番号 | 010-1234-5678 | (?<!w)(+82-?1[016789]-?d{3,4}-?d{4} 01[016789]-?d{3,4}-?d{4})(?!w) | ***_****_
**** |
| メールアドレス | example@domain.com | ([a-zA-Z0-9][a-zA-Z0-9._%+~]*@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,}) | ***@***.*** |

| 個人情報のパターン | 個人情報の例 | 正規表現式パターン | 置換される値 |
|-----------|------------------|---------------------------|---------------------------------------|
| 銀行口座番号 | 123456-01-654321 | (?<!w)d{6}-d{2}-d{6}(?!w) | <div>*****_**_</div> <div>*****</div> |
| 事業者登録番号 | 111-11-01111 | (?<!w)d{3}-d{2}-d{5}(?!w) | <div>***_**_</div> <div>*****</div> |
| 法人登録番号 | 111111-1111111 | (?<!w)d{6}-?d{7}(?!w) | <div>*****_</div> <div>*****</div> |

ログ設定のインポート/エクスポート

ログ設定のインポート・エクスポート

パーサ設定、高速インデックス設定、フィルター設定の内容をJSONファイル形式で保存し、他のプロジェクトからJSONファイルをインポートして適用できます。プロジェクトごとに何度も繰り返し設定を作成する手間を減らします。

1. 1つのプロジェクトにパーサ設定、高速インデックス設定、フィルター設定を追加します。
2. 各設定タブで画面右上に**JSON**  ボタンを選択します。
3. **JSONエクスポート**画面が表示されると、画面右上にある**抽出**ボタンを選択します。
4. JSON設定ファイルがユーザーPCに保存されます。
5. 他のプロジェクトに移動してから、**ログ** > **ログ設定**メニューに移動してください。
6. まず、JSON設定ファイルをエクスポートした設定タブを選択し、 ボタンを選択します。
7. ファイル選択画面が表示されたら、ユーザーのPCに保存したJSON設定ファイルを選択します。
8. **JSONインポート**画面が表示されたら、設定内容を確認し、**リストに追加する**または**上書き**ボタンを選択します。
9. 画面右上の**保存**ボタンを選択します。

 JSON設定ファイルをインポートして、**保存**ボタンを選択しないと、インポートされた設定は保存されません。

警告アラート

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

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

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

主な機能

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

権限

イベントを追加または設定するには、**アラート設定権限** が必要です。

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

📌 参考資料

詳細については、[メンバー権限](#) を参照してください。

イベント設定

ホーム画面 > プロジェクト選択 >  **アラート通知** > **イベント設定**

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

メトリクス

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

リアルタイムログ

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

複合ログ

ログの内容を基準に警告通知を発生させる複合ログイベントを設定します。

ホーム画面 > プロジェクト選択 >  **アラート通知** > **イベント設定**

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

メトリクス

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

リアルタイムログ

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

複合ログ

ログの内容を基準に警告通知を発生させる複合ログイベントを設定します。

参考

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

共通機能

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

- **JSON 一括編集**: すべてのイベント条件を JSON 形式で一括編集できます。
- **JSON 一括ダウンロード**: 現在登録されているイベント条件を JSON ファイルとして保存できます。
- **Excel 一括ダウンロード**: イベント一覧を Excel ファイルとしてダウンロードし、外部レポートやバックアップに活用できます。

JSON 一括編集

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

❗ 上書き後は、以前のイベント設定に戻すことはできません。

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



JSON データ構造



```

{
  "productType": "{productType}",
  "platform": "{platform}",
  "events": {
    "HITMAP": {
      ...
    },
    "LOG_REALTIME": [
      {...}
    ],

```



```

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

```

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

| ! | JSON フィールド | 説明 |
|---|------------|-----|
| | L ANOMALY | 異常値 |

JSON 一括ダウンロード

画面上部の [JSON 一括ダウンロード] ボタンをクリックします。

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

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

Excel 一括ダウンロード

画面上部の [Excel 一括ダウンロード] ボタンをクリックします。

メトリクス

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

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

基本オプション

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

表 | メトリクスイベント一覧構成

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

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

イベント設定

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

イベント追加

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

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

テンプレート選択

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

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

イベント条件定義

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

指標設定

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

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

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

❗ カテゴリや指標が不明な場合は、メトリクス照会を活用してください。

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

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

メトリクス検索

All 13件 / 全 149件

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

< 1 > 50件 / ページ

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

❗ イベントレベルの動作

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

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

4. 選択したイベントレベルのフィールド、演算子、値を入力します。

a. + 追加 をクリックすると条件を追加できます。

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

b. - をクリックすると、その条件が削除されます。

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

発生回数

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

1. 発生頻度を選択します。

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

2. 発生回数を入力します。

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

一時停止

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

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

❗ 解消通知が有効な場合

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

解消通知

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

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

イベント動作時間

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

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

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

シミュレーション

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

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

シミュレーション開始

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

シミュレーション結果の理解

1. 時系列データ

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

2. レベル別発生状況

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

3. 対象別詳細情報

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

4. ピーク区間の特定

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

🟢 シミュレーション活用のヒント

• 複数時間帯でのシミュレーション

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



- 実際の障害期間を含める

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

- 対象フィルタリングの追加

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

- しきい値を段階的に調整

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

イベント対象選択

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

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

対象選択

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

- **選択入力** 直接入力

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

監視対象のタグ、演算子、値を直接入力してください。

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


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

❗ 入力方法を変更すると、作成中の内容は初期化されます。

基本情報および通知設定

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

イベント有効化

設定した条件を満たした際にイベントを発生させるかどうかを設定します。

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

イベント名

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

メッセージ

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

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

- 変数の使用例

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

イベント受信

イベント通知を受信するメンバーを指定します。

- 全体受信** タグ選択受信

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

指定したタグを持つプロジェクトメンバーに通知が送信されます。

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

ⓘ 受信タグ

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

イベント修正／削除

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

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

イベント共有

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

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

エクスポート

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

インポート

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

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

JSON 形式で編集する

1. 画面右上の [JSON ] ボタンをクリックします。

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

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

JSON error

JSON データ構造

```
{
  "version": 2,
  "eventId": "zcef7s7f27rum1",
  "enabled": true,
  "stateful": false,
  "title": "Active Transaction",
  "message": "Active Transaction = ${active_tx_count}",
  "category": "app_counter",
  "alertLabel": [
    "oid"
  ],
  "repeatCount": 1,
  "repeatDuration": 0,
  "silent": 300000,
  "receiver": [],
  "timeTag": [],
  "selectString": "",
  "conditions": [
    {
      "level": 20,
      "enabled": true,
      "rule": "active_tx_count > 100"
    }
  ],
  "createTime": 1763632674345,
  "lastModifiedTime": 1763632674347,
  "lastModifiedUser": "support@whatap.io",
  "basic": true,
  "metaId": "java004",
}
```

```

"selectCondition": {
  "oid": [
    "-1010758404",
    "-250906941"
  ]
}
}

```

表 | JSON データ構造

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

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

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

付録

発生条件・対象選択ガイド

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

レベル動作ガイド

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

1. 優先順位に基づくイベント発生

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

例

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

2. レベル上昇

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

例

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

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

3. レベル下降

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

例

設定:

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

シナリオ:

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

4. 動作フロー

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

メトリクス値: 60% → 75% → 92% → 85% → 60%

状態: 正常 Warning Critical Warning 正常

 (発生) (発生) (維持) (解消)

 Warning

 (維持)

- ① 進行中状態を持つイベントは、条件が満たされている間は継続して有効となり、条件が解除されるまで維持されます。

条件設定ガイド

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

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

`${}` 使用例:

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

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

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

1. 比較演算子

数値比較

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

文字列比較

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

2. 算術演算子

- 基本的な算術演算

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

- 括弧による優先順位の制御

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

- 負の値の表現

```
cpu > -100
```

3. 論理演算子

- AND 演算 (&&)

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

- OR 演算 (||)

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

- 複合論理演算

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

4. パターンマッチング演算子

- LIKE 演算子

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

- NOT LIKE 演算子

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

5. 組み込み関数

- Null チェック関数

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

- 集計関数

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

- 数学関数

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

- 文字列関数

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

- 条件関数

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

形式

```
if(条件, true値, false値)
```

例

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

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

形式

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

例

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

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

形式

```
in(値, 候補値1, 候補値2, ..., 候補値N)
```

例

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

❗ 記述時の注意事項

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

リアルタイムログイベント

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

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

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

基本オプション

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

表 | リアルタイムログイベント一覧構成

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

| 項目 | 説明 |
|---|---|
| イベント発生一時停止 | <p>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</p> <ul style="list-style-type: none"> - 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 | <p>イベントが適用される対象の条件</p> <ul style="list-style-type: none"> - 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 |
|  | <p>イベントの有効化状態</p> <ul style="list-style-type: none"> - 有効: 条件を満たすとイベント発生 - 無効: イベントが動作せず、条件をチェックしない |

イベント設定

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

リアルタイムログイベントの追加

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

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

✔ 変数使用ルール

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

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

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

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

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

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

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

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

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

イベントの編集/削除

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

イベントの共有

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

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

エクスポート

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

インポート

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

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

JSON 形式で編集する

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

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

JSON error

付録

発生条件・対象選択ガイド

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

レベル動作ガイド

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

1. 優先順位に基づくイベント発生

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

例

設定:

- Warning: CPU > 70%

- Critical: CPU > 90%

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

2. レベル上昇

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

例

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

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

3. レベル下降

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

例

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

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

4. 動作フロー

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

メトリクス値: 60% → 75% → 92% → 85% → 60%

状態: 正常 Warning Critical Warning 正常

 (発生) (発生) (維持) (解消)

 Warning

 (維持)

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 | <p>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</p> <ul style="list-style-type: none"> - 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 | <p>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</p> <ul style="list-style-type: none"> - 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 |
|  | <p>イベントの有効化状態</p> <ul style="list-style-type: none"> - 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: level:ERROR） |
| 分母フィルター | 比率計算の分母となるログ条件（例: level:*） |
| イベント発行条件 | 比率（%） {演算子} {閾値}（例: rate > 10） |

- 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: host） |
| イベント発行条件 | ユニーク値数 {演算子} {閾値}（例: cardinality > 100） |

- **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: response_time.n） |
| 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

通知設定

ホーム > プロジェクト選択 >  アラート通知 > 通知設定

ユーザー別アラート受信設定

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

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

通知手段の設定

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

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

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

メール通知

メール通知は、会員登録時に入力したメールアドレス宛に送信されます。

SMS通知

SMSで通知を受信できます。

 SMS通知機能は、有料プロジェクトでのみ利用できます。

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

✔ 登録した電話番号の変更および削除

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

WhatsApp通知

WhatsAppを通じて通知を受信できます。

ⓘ WhatsApp通知機能は、有料プロジェクトでのみ利用できます。

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

モバイル通知

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

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

繰り返し通知（エスカレーション）設定

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

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

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

イベント受信タグ

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

イベント受信タグの追加・編集・削除

 イベントに **適用中のイベント受信タグ** は削除できません。

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

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

イベント受信タグを解除する

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

受信タグ未設定のアラートを受信する

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

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

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

イベント受信モードの選択

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

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

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

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

通知受信言語の選択

ユーザーが受信するアラート通知の言語を選択できます。

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

曜日・時間別通知設定

ユーザーごとに、曜日および時間帯別の通知受信可否を設定できます。

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

サードパーティプラグイン

外部アプリケーションを通じて警告アラートを受信できます。

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

JSON、Opsgenie、PagerDuty、LINE、ilert

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

表 | サードパーティプラグイン一覧

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

サードパーティプラグインの追加

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

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

サードパーティプラグイン通知の追加方法

Slack

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

Telegram

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

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



① 使用可能なコマンド一覧

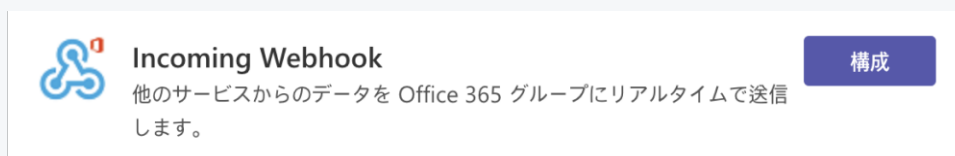
- `/help` : コマンド一覧を表示
- `/license` : 通知を受信するプロジェクトのアクセスキーを入力
- `/remove` : 通知を受信しないプロジェクトコードを入力
- `/list` : 現在通知を受信しているプロジェクトコードを表示

Teams

- 通知を受信したいチャンネルの **コネクタ** に移動します。



2. Webhook を追加し、[構成] ボタンをクリックします。



3. Webhook 名を入力し、[作成] ボタンをクリックします。



Incoming Webhook

フィードバックの送信

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

* が付いているフィールドは必須です

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

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

イメージをアップロードします。



既定のイメージ

作成

キャンセル

4. 生成された Webhook URL をコピーします。

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

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



URL は最新です。

完了

削除

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

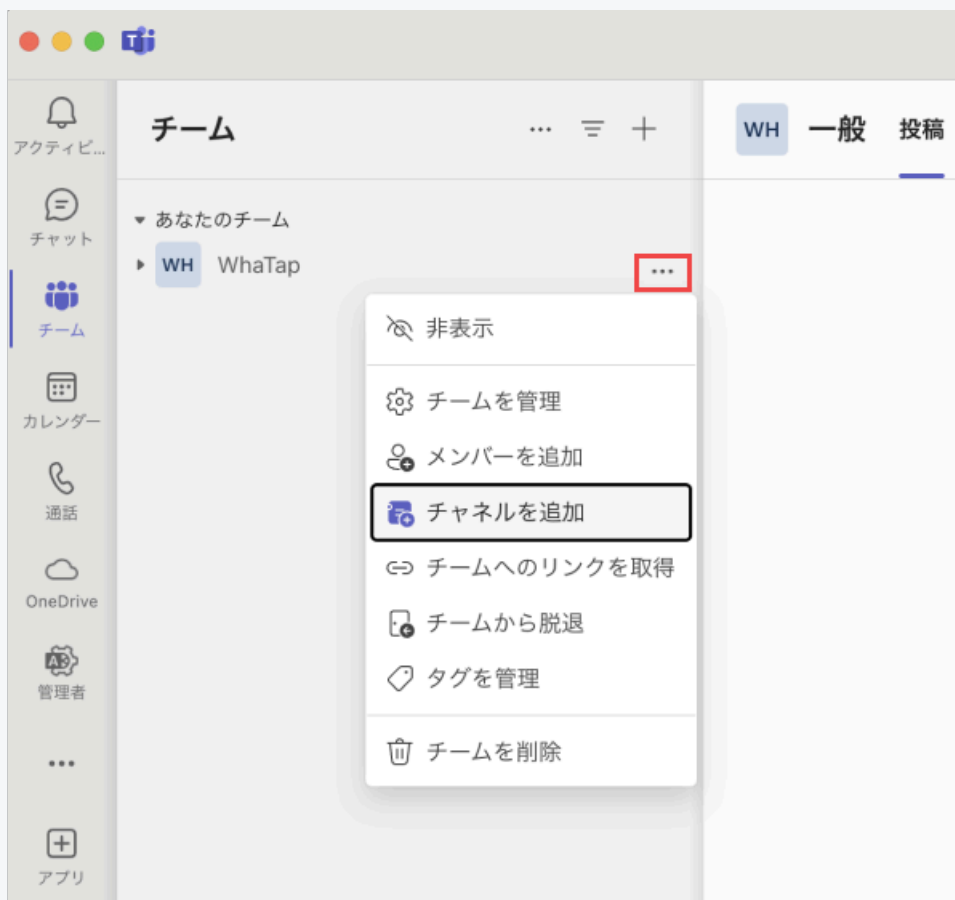
6. [登録] ボタンをクリックします。



Teams Workflows

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

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



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



チャンネルの作成

チャンネル名 *

WhaTapのイベントチャンネル

説明

他のユーザーが、適切なチャンネルを見つけられるように説明を入力します

チャンネルの種類を選択する * ⓘ

選択

☒ 標準
チームの全員がアクセスできます。

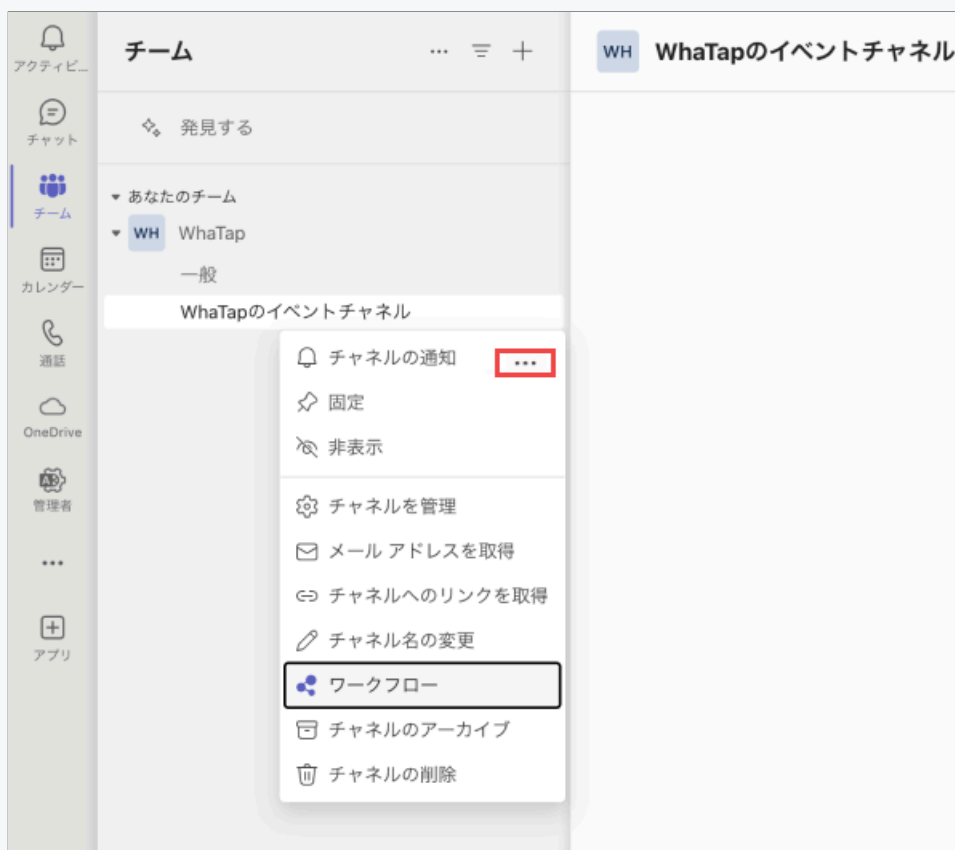
☐ 共有
組織内または組織外の人またはチームがアクセスできます。

☐ プライベート
チームの特定のユーザーがアクセスできます。

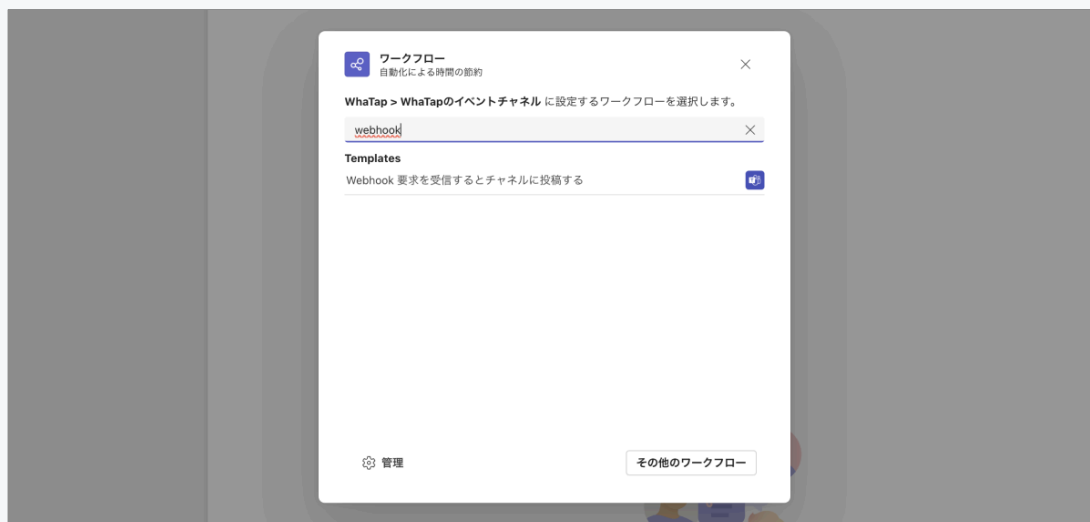
キャンセル 作成

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

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



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



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



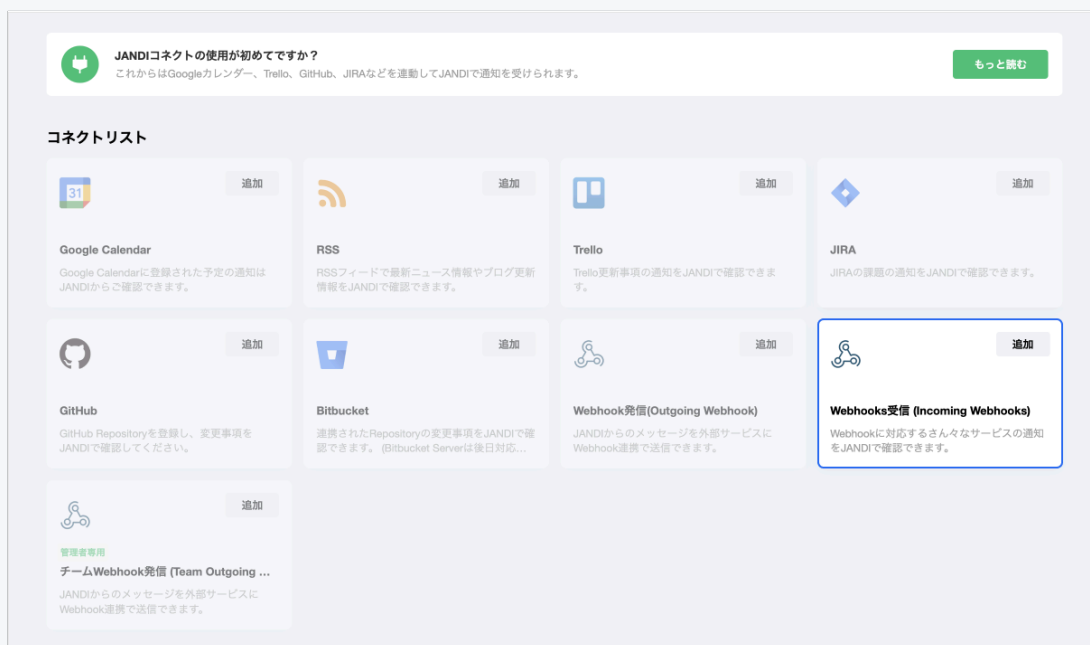
8. WhaTap モニタリングサービスの **サードパーティプラグインの追加** 画面に戻り、Teams **Workflows** タブ下部の **Channel Name** と **Webhook URL** に値を入力します。
9. [登録] ボタンをクリックします。

Jandi





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



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



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



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



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

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



インテグレーション

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

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

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

← インテグレーション

ワットテスト

基本情報

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

クリップボードにコピーする

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

Webhook



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

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

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

Webhook JSON



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

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

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

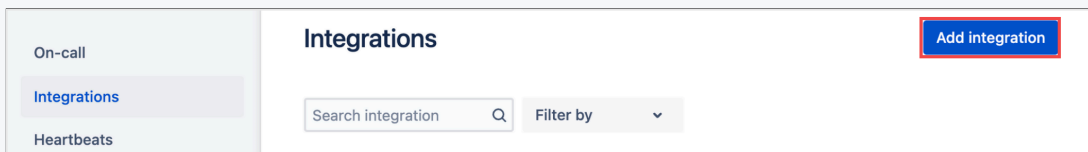
2. **Webhook Name** と **Webhook URL** の項目を入力してください。
3. ヘッダー値を追加するには、**ユーザーヘッダー値の追加** の + 追加 をクリックし、key と value を入力してください。
4. [登録] ボタンをクリックしてください。

Opsgenie

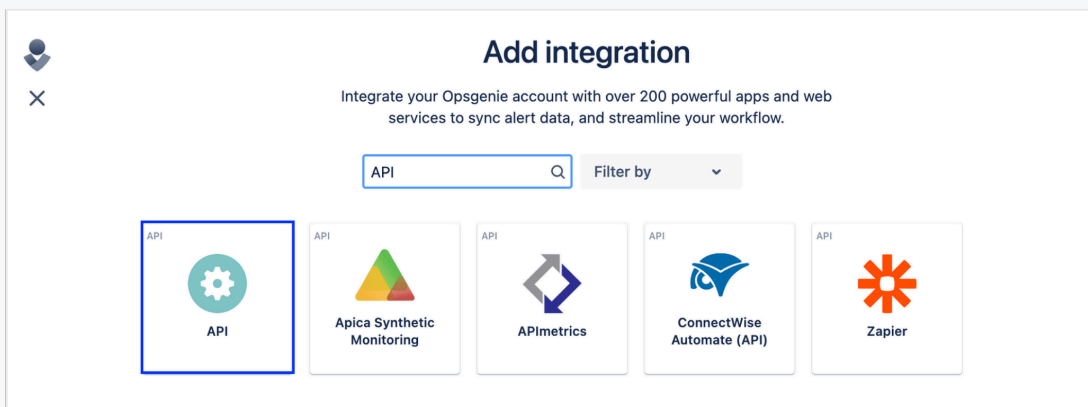




1. **Teams** メニューで、アラートを受信するチームを選択してください。
2. **Integration** メニューに移動し、[Add Integration] ボタンをクリックしてください。



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



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



Forwarding rules
Your on-call schedule

ON-CALL
Global policies
All schedules
All escalations

CONNECTED APPS
Atlassian products

INTEGRATIONS
Integrations
Heartbeats
Slack
GitLab

Settings

Name:

Assigned to Team: ?

API Key: ?

Read Access: ?
☒

Create and Update Access: ?
☒

Delete Access: ?
☒

Restrict Configuration Access: ?
☐

Enabled: ?
☒

Suppress Notifications: ?
☐

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

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



PagerDuty



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



PagerDuty

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

PagerDuty

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

PagerDuty

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

PagerDuty

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

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

LINE



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

LINE 3rd パーティプラグイン追加

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

コマンド

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



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

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

使用例

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



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

ilert



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



Finish setup] ボタンをクリックして設定を完了します。

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

大量アラート発生の防止

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

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



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

イベント通知フォーマット

共通アラートテンプレート

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

- プロダクトタイプ: アプリケーション、データベース、Kubernetes
- イベントタイプ: アプリケーションアラート、データベースアラート、メトリクスアラート
- イベントチャンネル: 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 | "zf3uoj0fv4v7" |

イベントタイプ別対応フィールド

ⓘ 特定のイベントタイプでのみサポートされるフィールドです。該当しないイベントタイプの場合、値が存在しないことがあります。

| フィールド名 | タイプ | イベント種別 | 説明 | 例 |
|-----------|--------|--------|--------|---------------|
| eventRule | String | 基本、メト | イベント発生 | "memory ≥ 80" |

| フィールド名 | タイプ | イベント種別 | 説明 | 例 |
|-------------|--------|----------|--------|--|
| | | リクス | ルール | |
| field | String | リアルタイムログ | ログ検索キー | "content" |
| keyword | String | リアルタイムログ | ログ検索値 | "Error" |
| logCategory | String | リアルタイムログ | ログカテゴリ | "AppLog" |
| logContent | String | リアルタイムログ | ログ内容 | "00:00000:00009:2025/04/06 23:03:52.55 server Error: 1601, Severity: 17, State: 3\n00:00000:00009:2025/04/06 23:03:52.55 server There are not enough 'user connections' available to start a new process." |

対象フィールド

| フィールド名 | タイプ | 説明 | 例 |
|--------|--------|----------------|-----------------|
| Oid | Number | エージェントの一意識別子 | -98765432 |
| Oname | String | エージェント名 | "web-server-01" |
| Okind | Number | エージェント種別の一意識別子 | 867318026 |

| フィールド名 | タイプ | 説明 | 例 |
|-----------|--------|-----------------|---------------------|
| OkindName | String | エージェント種別名 | "web-server" |
| Onode | Number | エージェントノードの一意識別子 | 334634079 |
| OnodeName | String | エージェントノード名 | "production-node-1" |

イベント固有値フィールド

| フィールド名 | タイプ | 説明 | 例 |
|--------|--------|------------|---------------------------|
| Id | Number | イベントの一意識別子 | 5768121 |
| UUID | String | イベント固有識別子 | "550e8400-e29b-41d4-a716" |

状態／フラグフィールド

| フィールド名 | タイプ | 説明 | 例 |
|-------------|---------|----------------|-------------|
| Stateful | Boolean | 状態ベースイベントかどうか | true, false |
| Disabled | Boolean | 無効化されたイベントかどうか | true, false |
| Escalation | Boolean | エスカレーション有無 | true, false |
| SystemEvent | Boolean | システムイベントかどうか | true, false |

検索タイプ別クエリ構文

① 検索の基本構文については、[WhaTap ログ検索クエリ構文](#) ドキュメントを参照してください。

1. キーワード検索

「Database Connection」という文字列を含むイベント

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

2. 複数値検索

指定した複数の値のうち、いずれかを含むイベントを検索します。

```
title: Database Connection
```

現在のイベントレベルが Info または Warning のイベント

```
level: info warning
```

3. パターン検索

ワイルドカードを使用してパターン検索ができます。

名前パターンで特定のエージェントで発生したイベントを検索

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

タイトルが Connection で終わるイベントを検索

```
title: *Connection
```

4. 複合条件検索

複数の条件を組み合わせて、より正確に検索できます。

レベルが Critical で、タイトルに Database を含むイベント

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

特定のエージェントにおける Warning または Critical のイベント

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

5. OR 条件検索

複数の条件のうち、**いずれか一つでも満たす**イベントを検索します。

タイトルまたはメッセージに特定のキーワードを含むイベント

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

6. 除外条件

特定の条件を除外して検索できます。

Info レベルを除いたすべてのイベント

```
not level: info
```

リアルタイムアラート

リアルタイムアラート機能は、イベント設定で設定したイベントが発生した際に、ポップアップ形式で表示されます。イベント発生と同時に通知を受け取ることで、問題を迅速に把握し、対応することができます。また、すでに発生した通知や見逃した通知の履歴を確認することで、リアルタイム対応が難しかった状況を把握し、解決に役立てることができます。

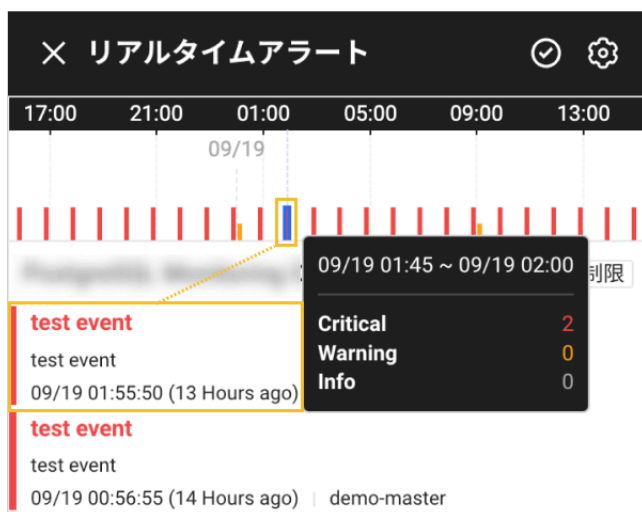
リアルタイムアラートを確認する

リアルタイムアラートは、画面右上にポップアップとして表示されます。通知が発生した時刻、タイトル、メッセージを確認できます。

- 個別の通知を閉じるには、メッセージ右上の ✕ ボタンをクリックしてください。
- 画面に表示されているすべてのポップアップ通知を閉じるには、**すべての通知を閉じる** をクリックしてください。

通知履歴を確認する

1. プロジェクトを選択して表示される画面の最上部にある 🔔 をクリックしてください。
2. リアルタイムアラート ウィンドウが表示されます。
 - 現在のプロジェクトについて、直近24時間以内の通知を最大100件まで確認できます。
 - 個別のイベント項目を選択すると、関連するメニューに移動します。
 - リアルタイムアラート ウィンドウ内の時間別チャートで任意の時間帯を選択すると、該当するイベント項目に移動します。



- すべての通知履歴を確認するには、**全体の通知履歴** ボタンをクリックしてください。**アラート通知 > イベント履歴** メニューに移動します。

❗ リアルタイムアラート の一覧が空の場合、**全体の通知履歴** ボタンが表示されます。受信タグ未設定の通知を受け取る オプションを無効にしてください。

イベントを一括で解消する

リアルタイムアラート の一覧から、進行中のすべてのイベントを一括で解消できます。

イベント解消が完了するまでに、約30秒～1分程度かかる場合があります。

- イベント一括処理** 機能を使用すると、現在進行中のイベントに対する解消通知が大量に発生する可能性があります。
- イベント一括処理** 機能を使用した後でも、イベントルールが有効であり、データが引き続きしきい値を超えている場合、イベントは再度発生することがあります。
- イベント解消通知は、**アラート通知 > イベント設定** メニューでイベントを編集し、**イベントが解消されたときに追加通知** または **解消通知** オプションを無効にすることで停止できます。

使用方法:

1. プロジェクトを選択して表示される画面上部の  をクリックします。
2. リアルタイムアラート ウィンドウが表示されたら、右上の  をクリックします。
3. リアルタイムアラートリストの進行中イベントを一括で解消します。 というメッセージが表示されたら、解消 ボタンをクリックします。

リアルタイムアラートを設定する

1. プロジェクトを選択して表示される画面上部の  をクリックします。
2. リアルタイムアラート ウィンドウが表示されたら、右上の  をクリックします。
3. リアルタイムアラート設定画面で各項目を設定します。
 - ポップアップ通知: リアルタイムアラート ウィンドウが閉じている状態でも、ポップアップ形式で通知を表示します。
 - 解消済みイベントを表示: リアルタイムアラート 一覧に解消済みイベントも含めて表示します。
 - 通知音の試聴: ブラウザで再生される通知音を事前に確認できます。Critical または Warning の横にある  をクリックしてください。音が再生されない場合は、ブラウザの設定をご確認ください。

システムイベント

WhaTap モニタリングは、プラットフォーム全体で自動的に検知・生成される共通イベントを提供します。本ドキュメントでは、システムによって発生するイベントの種類、発生条件、および対応方法について説明します。

EVENT_BLOCKED_BY_SYSTEM

プロジェクト内で短時間に過剰な数のイベントが発生した場合、WhaTap システムがこれを検知し、イベントの発生を一時的にブロックします。イベントがブロックされると、システムは次のメッセージをユーザーに通知します。このイベントが発生した場合は、イベント設定内容を確認し、必要に応じて調整してください。

 **Critical**



イベントメッセージ

Excessive events detected, event blocked for stability. name: server agent

| | |
|----------|--------------------------------|
| プロジェクト番号 | 8 |
| プロジェクト名 | new server |
| 対象 | server agent |
| イベント名 | EVENT_BLOCKED_BY_SYSTEM |
| イベント日時 | (GMT+0900) 2024-11-18 18:03:18 |

WhaTapにログイン

new serverプロジェクトのserver agentから過度なイベントが検知されたため、イベント発生が遮断されます。server agentから一定期間の間にイベントが発生しなくなると、遮断が自動で解除されます。

ブロック基準

イベントは次の基準に基づいてブロックされます。

1. エージェント単位のブロック

1つのエージェントで **1分以内に10件** のイベントが発生した場合、そのエージェントから発生する以降のイベントはブロックされます。

2. 複数エージェントによる全体ブロック

条件 **1** によりイベントがブロックされたエージェントが **1分以内に3件以上** 発生した場合、プロジェクト全体のイベントがブロックされます。

3. プロジェクト単位のブロック

1つのプロジェクトで **1分以内に100件** のイベントが発生した場合、プロジェクト全体のイベントがブロックされます。

ブロック解除方法

システムによってイベントがブロックされた場合、対象のエージェントまたはプロジェクトで **1分間** イベントが発生しない状態を維持する必要があります。

- ・ **アラート通知 > イベント設定** メニューから設定されているすべてのイベントを無効化してください。 **イベント設定** を見直し、過剰なイベントが発生しないように閾値を調整する必要があります。
- ・ イベントを設定する前に、**シミュレーション** 機能を活用してイベント発生回数を事前に予測できます。

실험실

사용자에게 새로운 기능 또는 실험적인 기능을 제공합니다. 사이드 메뉴의  실험실 또는 **사이트맵**을 통해 접근할 수 있습니다. 제품에 따라 제공하는 기능이 다를 수 있습니다.

✔ 사이트맵으로 실험실 메뉴 접근하기

사이드 메뉴에서  실험실이 보이지 않는다면  **사이트맵**으로 접근할 수 있습니다.

1. 전체 화면 왼쪽 아래에  **사이트맵** 아이콘을 클릭하세요.
2. **사이트맵** 창의 오른쪽 아래에 **실험실** 섹션에서 원하는 메뉴를 선택하세요.

⚠ 주의

실험실의 기능은 현재 개발 중인 베타 버전으로 예기치 않은 오류가 발생할 수 있습니다.

해당 기능 사용 시 주의가 필요합니다. 중요한 데이터나 운영 환경에서 사용을 권장하지 않습니다. 피드백이나 문제점이 발생하면 지원팀(support@whatap.io)으로 문의하시기 바랍니다.

MXQL 데이터 조회

MXQL은 와탭의 성능 데이터(메트릭스)를 유연하게 조회하기 위한 쿼리 언어입니다. 하나의 프로젝트에 포함된 여러 에이전트에서 수집한 메트릭스들을 종합적으로 조회하고 활용하기 위해서 사용합니다. **MXQL**에 대한 자세한 내용은 [다음 문서](#)를 참고하세요.

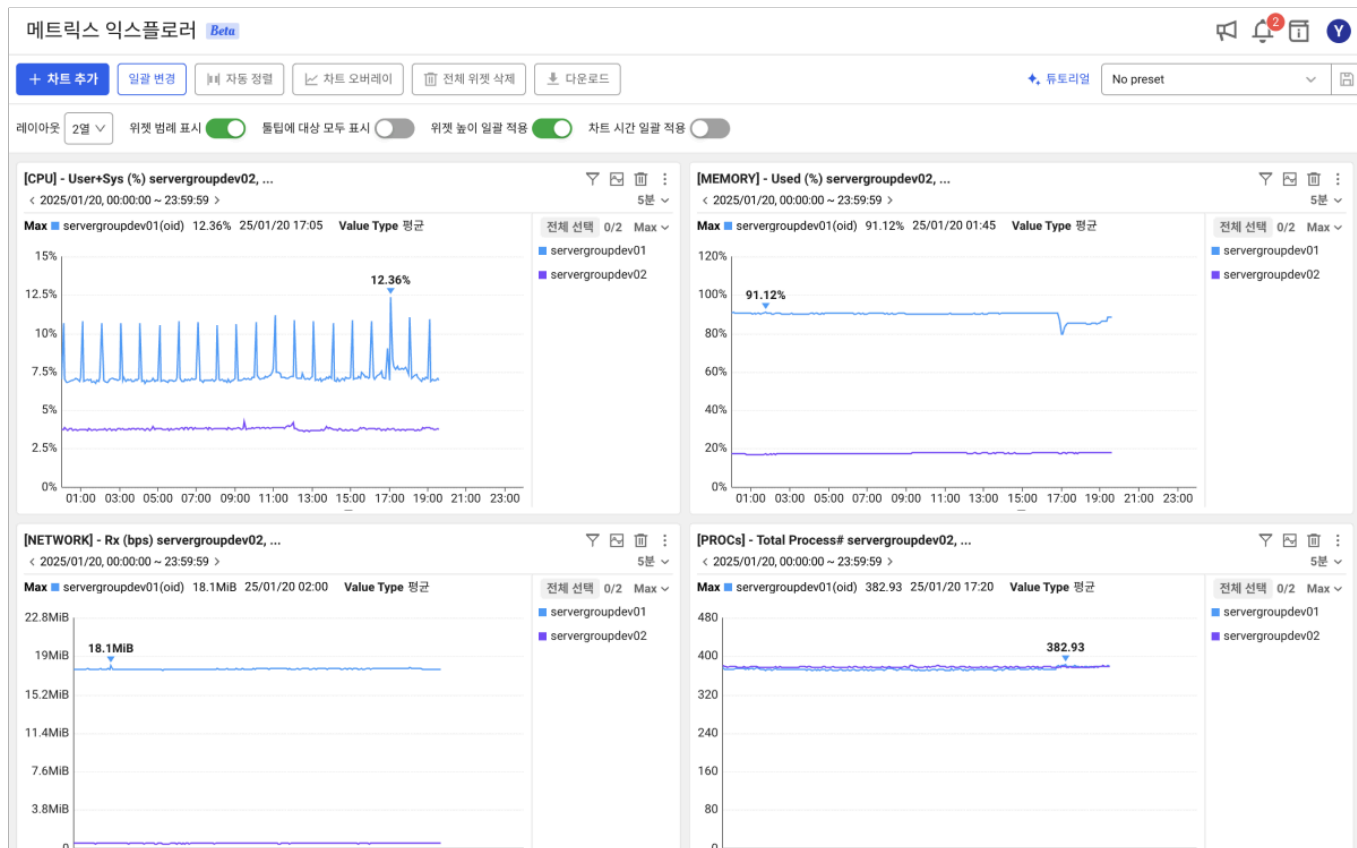
알림 메시지

프로젝트 멤버에게 메일 또는 서드 파티 플러그인을 통해 전달하는 경고 알림 메시지를 수정할 수 있는 사용자 정의 기능을 제공합니다. 자세한 내용은 [다음 문서](#)를 참고하세요.

메트릭스 익스플로러

홈 화면 > 프로젝트 선택 > 실험실 > 메트릭스 익스플로러 Beta

메트릭스 익스플로러 Beta 메뉴는 모니터링 대상으로부터 수집한 데이터를 시계열 차트로 시각화하여 제공합니다. 이를 통해 사용자는 시스템 성능을 효과적으로 모니터링하고 이상 징후를 빠르게 식별하여 문제 해결에 필요한 인사이트를 얻을 수 있습니다.



- 다양한 지표를 시계열 차트를 통해서 시각적으로 확인할 수 있으며, 장애 발생 시점의 여러 지표를 한번에 분석할 수 있습니다.
- 특정 시간 범위를 선택하여 과거 데이터를 조회하고, 해당 기간 동안의 성능을 분석할 수 있습니다.
- 특정 시간대나 조건에 맞는 데이터를 필터링하여 보다 정확한 분석을 수행할 수 있습니다.
- 사용자는 원하는 차트를 화면에 배치하고 레이아웃을 자유롭게 조정할 수 있습니다.
- 사용자가 원하는 지표들을 배치하고 프리셋으로 저장하여 필요 시 불러올 수 있습니다.

차트 위젯 추가하기

대시보드에 지표를 위젯으로 추가하려면 화면 왼쪽 상단의 **차트 추가** 버튼을 선택하세요.

조회 시간 설정하기

시간에서 지표를 조회할 날짜와 시간을 설정하세요.

대상 선택하기

프로젝트에 포함된 에이전트 중 원하는 대상을 선택하세요. 개별 에이전트를 선택하거나 에이전트 설정을 통해 분류한 그룹 단위로 선택할 수 있습니다.

대상

전체

에이전트

종류별

서버별

대상 검색

Q

전체 선택

0/9

전체 접기

↺

▼ Project

▼ demo-okind-0

demo-8104

demo-8102

demo-8100

▼ demo-okind-1

demo-8103

demo-8105

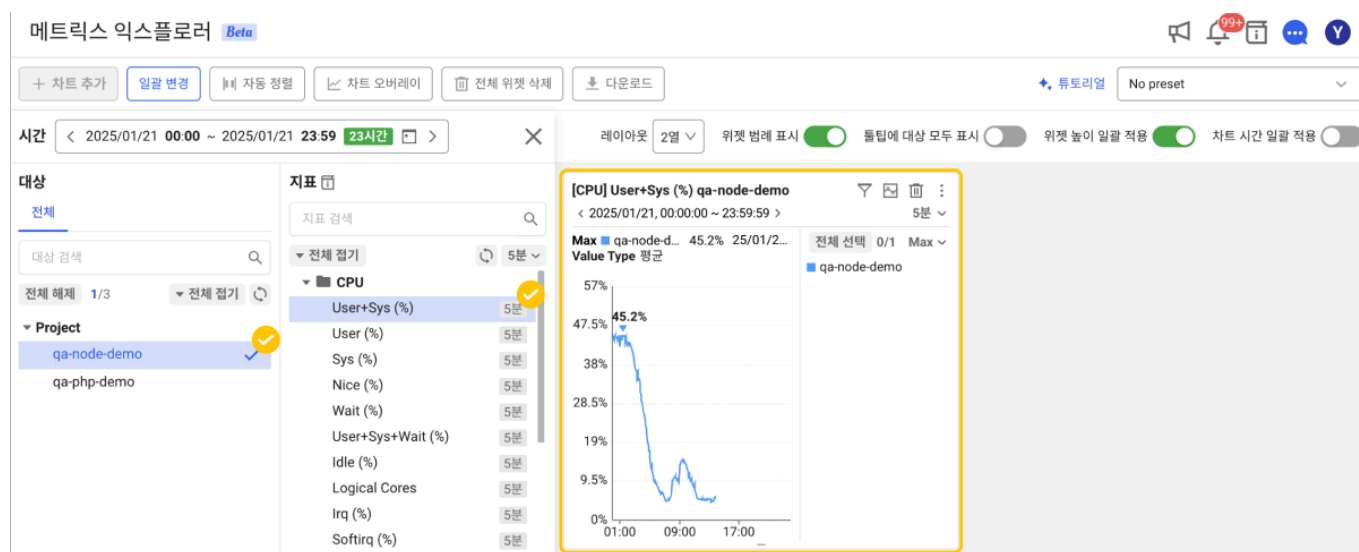
demo-8101

- **에이전트:** 개별 에이전트를 선택하거나 모두 선택할 수 있습니다.
- **종류별:** 에이전트 설정에서 `whatap.okind` 로 분류된 그룹 단위로 에이전트를 모니터링합니다.
- **서버별:** 에이전트 설정에서 `whatap.onode` 로 분류된 그룹 단위로 에이전트를 모니터링합니다.

- ❗ • 설정한 시간과 날짜에 따라 선택할 수 있는 대상이 변경될 수 있습니다.
- 에이전트 목록에서 마우스 클릭해 대상을 선택하거나 해제할 수 있습니다. Shift 키를 이용해 여러 개의 에이전트를 한번에 선택할 수도 있습니다.
- **전체 선택** 또는 **전체 해제** 버튼을 선택하면 관련 하위 대상들을 한번에 선택 또는 해제할 수 있습니다.
- 원하는 에이전트가 목록에 표시되지 않는다면 **새로고침** 버튼을 선택하세요.
- **전체 접기** 또는 **전체 펼치기** 버튼을 선택해 그룹 단위로 목록을 감추거나 펼칠 수 있습니다.

지표 선택하기

모니터링할 대상 에이전트를 선택한 후 **지표** 패널에 선택할 수 있는 목록이 표시됩니다. 목록에서 원하는 지표를 선택하세요.



선택한 지표에 해당하는 차트 위젯이 오른쪽의 대시보드에 배치됩니다. 다른 지표를 추가로 선택해 차트 위젯을 추가할 수 있습니다. 차트 영역을 확대해 넓게 보려면 **시간** 옵션 오른쪽의 × 버튼을 선택하세요. **대상**과 **지표** 패널이 사라지고 차트 영역만 화면에 표시됩니다.

- ❗ • **지표 검색** 입력란에 문자열을 입력하면 원하는 지표를 빠르게 검색할 수 있습니다.
- 지표의 카테고리 및 필드 이름을 기준으로 검색할 수 있습니다. 카테고리 및 필드에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.
- **전체 접기** 또는 **전체 펼치기** 버튼을 선택해 카테고리 단위로 지표 목록을 감추거나 펼칠 수 있습니다.

- ❗ • 원하는 지표 항목이 목록에 표시되지 않는다면 **새로고침** 버튼을 선택하세요.

NUMA Node 지표

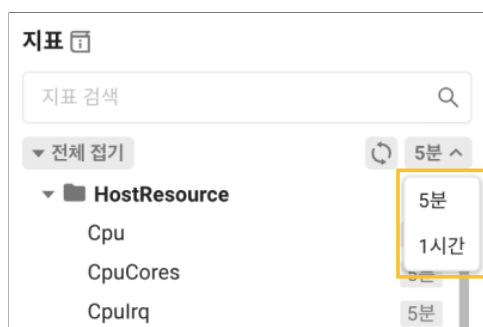
지표 목록에 **NUMA Node** 카테고리를 추가했습니다. NUMA 노드별 CPU 사용률, 메모리 사용량, 노드 간 메모리 접근 비율 등을 조회할 수 있습니다. 노드별 지표를 비교하면 특정 노드에 부하가 쏠렸는지, 원격 노드 메모리 접근이 과도한지 확인할 수 있습니다.

차트 범례는 다음과 같이 표시합니다.

| Item | Description |
|----------------|--|
| NUMA Node 카테고리 | Node 0 형태로 노드 번호 표시 |
| CPU Core 카테고리 | Core cpu1 (Node 0) 형태로 코어 이름과 소속 노드를 함께 표시 |

CPU Core 범례의 노드 표기는 NUMA 연결 정보를 수집한 Linux 환경에서만 나타납니다. 정보가 없는 코어와 Windows·Unix 환경에서는 Core cpu1 형태를 유지합니다.

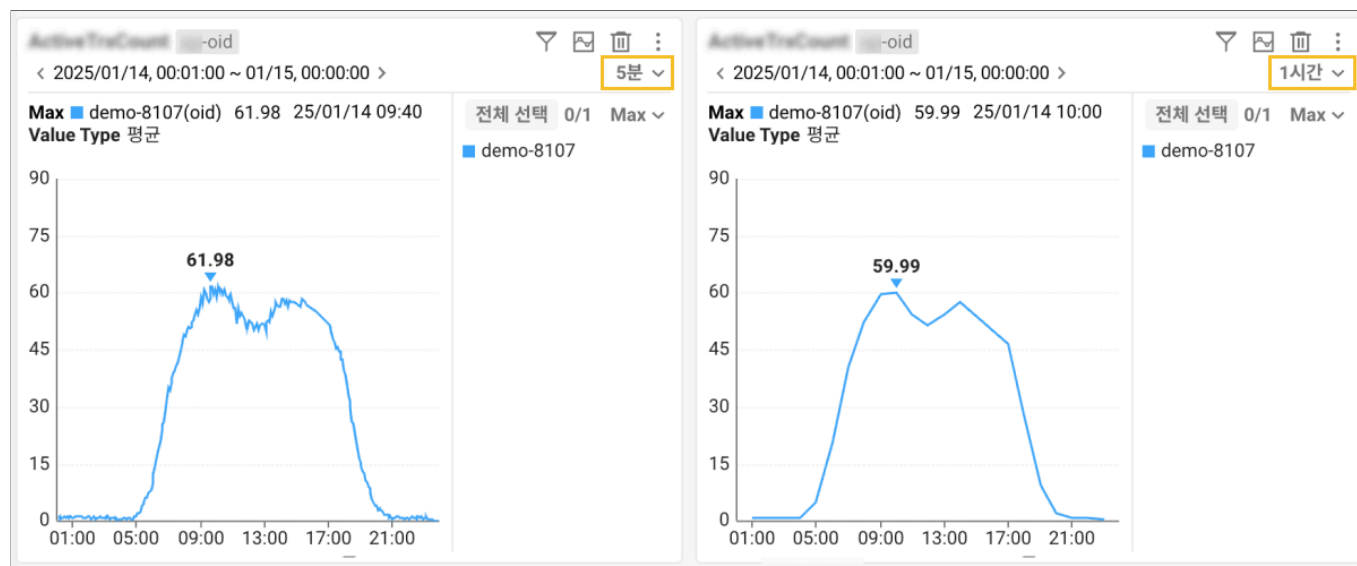
인터벌 설정하기



차트마다 인터벌을 설정할 수 있어 데이터의 집계 단위를 조정하여 다양한 시간 간격의 데이터를 시각화할 수 있습니다. **지표** 패널의 오른쪽 상단에 ⌚ 버튼을 선택하면 인터벌 옵션을 선택할 수 있습니다.

지표마다 기본 설정된 인터벌 시간이 다르며 조회 시간 범위에 따라 인터벌 시간이 변경됩니다.

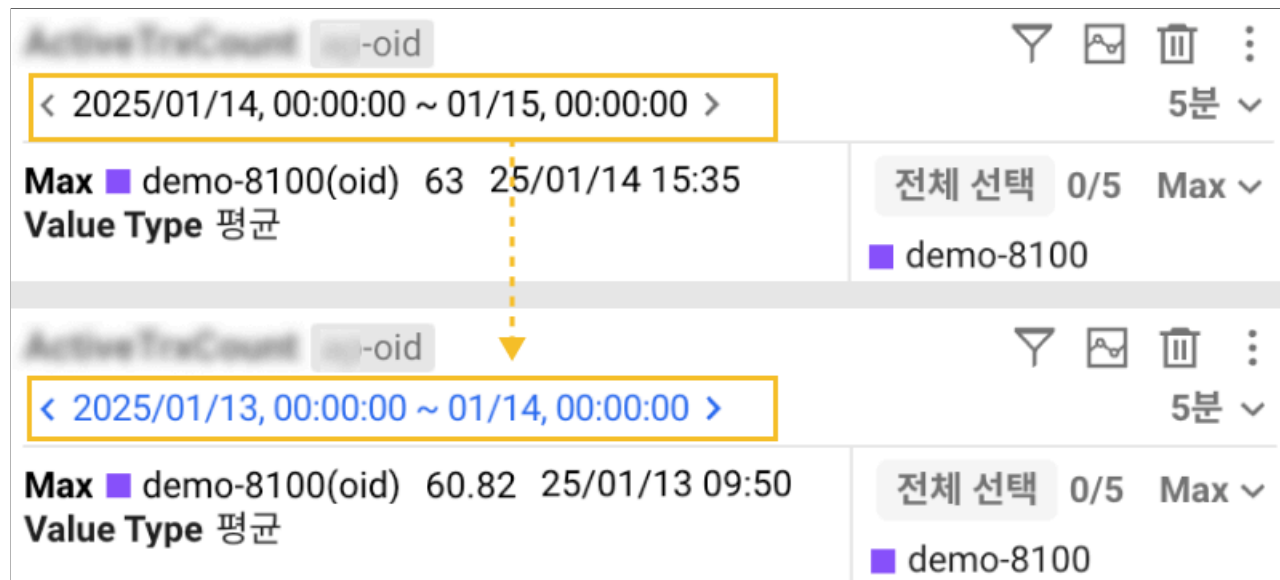
예를 들어, **5분** 인터벌은 5분 단위의 평균 값을 표시하고, **1시간** 인터벌은 1시간 단위의 평균 값을 표시합니다.



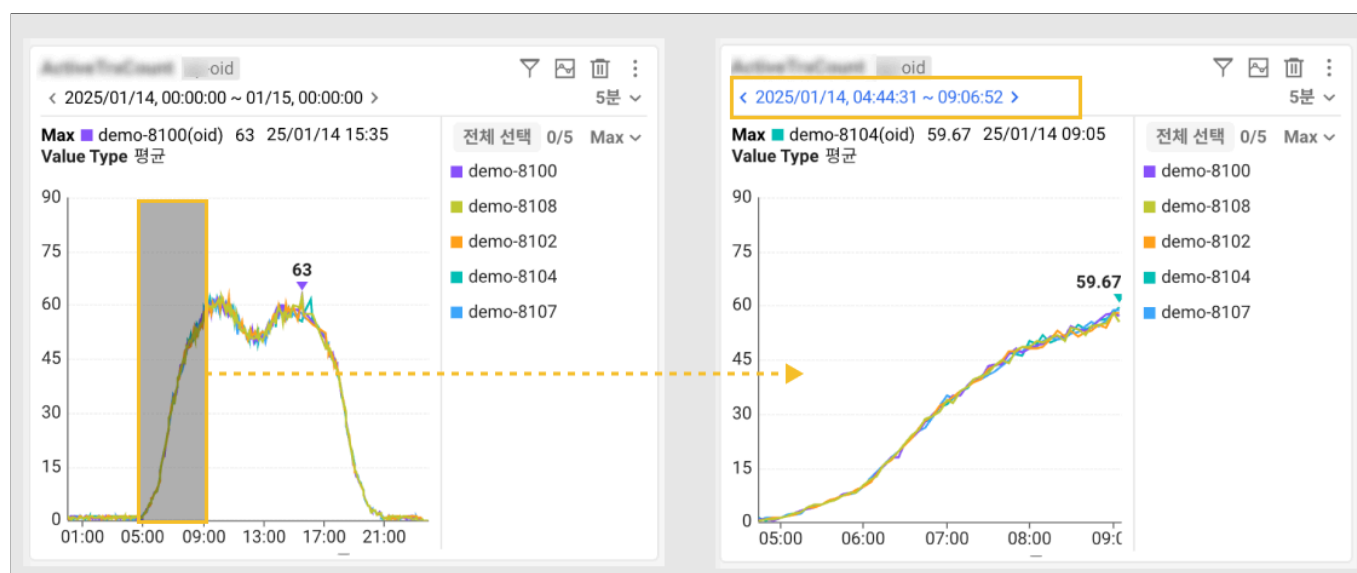
- ✓ 인터벌 옵션을 조정하여 짧은 시간 간격의 세부 데이터부터 긴 시간 간격의 전체 추세까지 다양한 관점에서 데이터를 분석할 수 있습니다.

조회 시간 변경하기

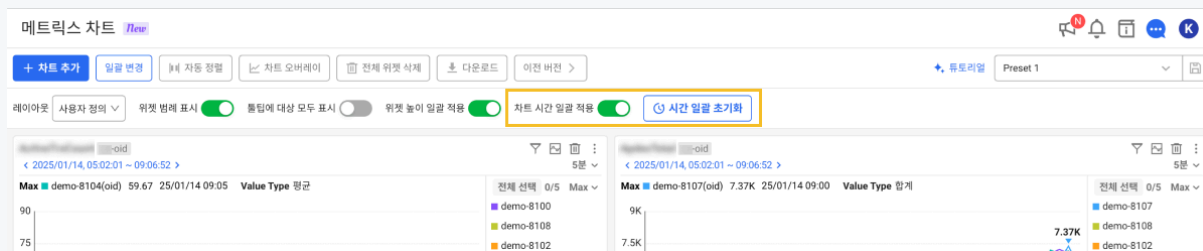
개별 위젯의 차트 조회 시간 범위를 변경하려면 위젯 상단의 < 또는 > 버튼을 선택하세요. 시간 변경 범위는 시간 옵션에 설정된 시간 기준과 같습니다. 예를 들어, 시간 옵션에서 1일로 설정되어 있을 때, < 또는 > 버튼을 선택하면 시간을 1일 단위로 변경할 수 있습니다.



또는 차트의 특정 영역을 드래그하면, 드래그한 범위만큼 시간을 변경해 조회할 수도 있습니다.



- ✓ 화면 상단에 **차트 시간 일괄 적용** 옵션을 활성화한 상태에서 개별 위젯의 시간을 변경하면 모든 위젯의 시간을 변경할 수 있습니다.



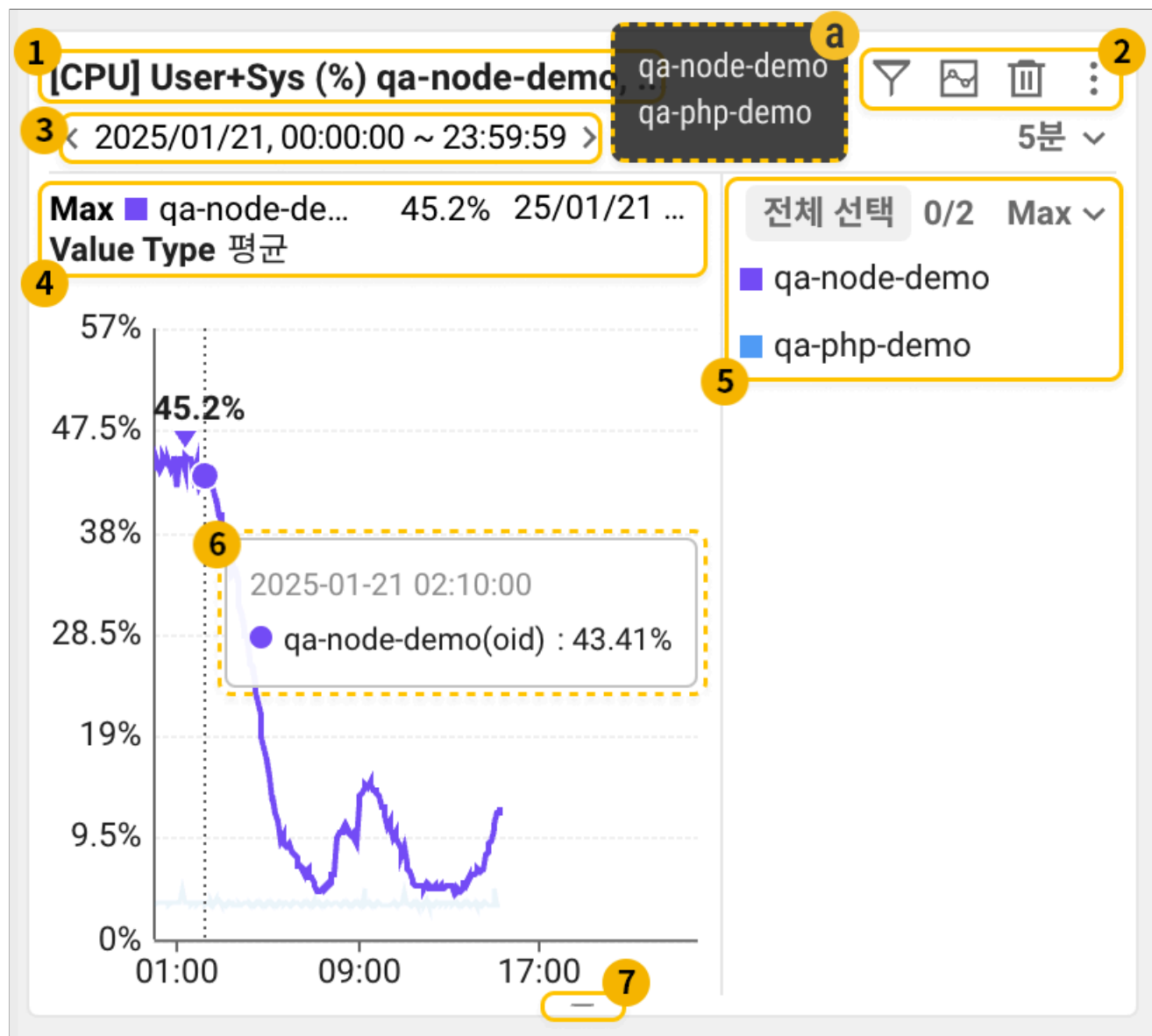
- 조회 시간 범위를 변경한 다음 최근 시간으로 다시 변경하려면  버튼을 선택하세요.

만약 화면 상단에 **차트 시간 일괄 적용** 옵션을 활성화한 상태라면  **시간 일괄 초기화** 버튼이 표시됩니다. 이 버튼을 선택하면 모든 위젯의 시간을 초기화할 수 있습니다.

- ❗ **일괄 변경** 기능을 이용해 전체 위젯의 시간을 변경하고, 모니터링 대상과 인터벌도 수정할 수 있습니다. 자세한 내용은 [다음 문서](#)를 참조하세요.

차트 위젯 상세 안내

차트 위젯에 표시되는 각 항목에 대한 자세한 내용을 확인하세요.



- 1 **차트 위젯 이름:** 차트 위젯 상단에서 선택한 지표 이름, 지표 그룹명, 대상을 표시합니다.
 - a: 마우스 포인터를 위젯 이름 위로 가져가면 모니터링 대상을 확인할 수 있습니다.
- 2 **위젯 옵션:** 차트 위젯의 옵션 메뉴입니다. 자세한 내용은 [다음 문서](#)를 참조하세요. 인터벌 옵션에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.
- 3 **시간:** 차트의 데이터를 조회하는 시간 범위를 표시합니다. < 또는 > 버튼을 선택해 조회 시간 범위를 조정할 수 있습니다.
- 4 **데이터:** 모니터링 대상 중 조회한 데이터의 최댓값(Max)과 데이터 병합 방식(Value Type)을 확인할 수 있습니다.

- **5 범례:** 모니터링 대상을 범례로 표시합니다. 범례 표시에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.
- **6 차트:** 조회한 데이터를 시계열 그래프로 표시합니다. 마우스 포인터를 그래프 위로 가져가면 툴팁을 통해 상세 정보를 확인할 수 있습니다. 차트의 특정 영역을 드래그하면, 드래그한 범위만큼 시간을 변경해 조회할 수 있습니다.
- **7 크기 조절:** 차트 위젯의 가운데 하단 영역을 드래그하면 위젯의 크기를 조절할 수 있습니다.

차트 위젯 옵션 이용하기

차트 위젯의 오른쪽 상단에 위치한 옵션 버튼을 통해 다양한 기능을 이용할 수 있습니다.

▽ 대상 필터링하기

화면에 추가한 차트 위젯에 모니터링 대상을 추가하거나 제외할 수 있습니다.

1. ▾ 버튼을 선택하면 모니터링 대상을 선택할 수 있는 팝업 메뉴가 나타납니다.



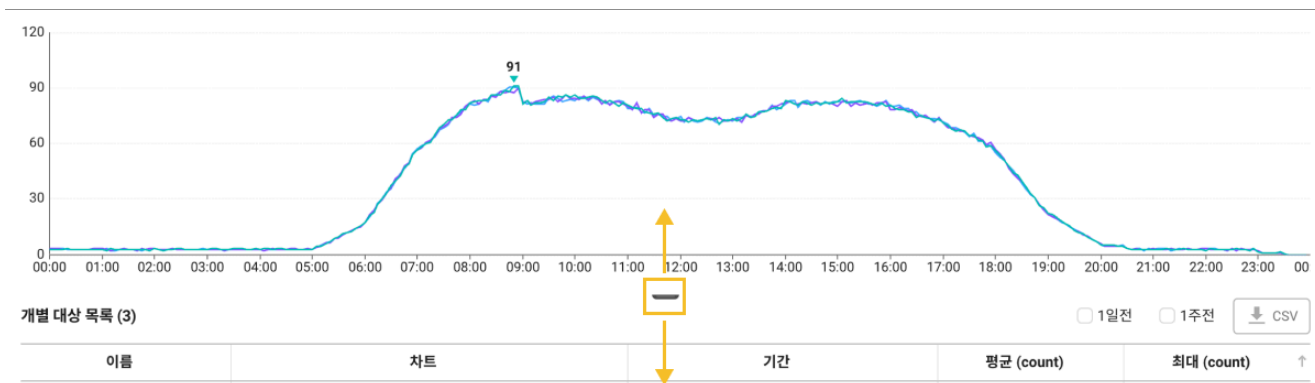
2. 화면의 안내에 따라 원하는 대상을 선택하세요.
3. 적용 버튼을 선택하세요.

상세 조회하기

차트의 데이터를 더 넓은 화면에서 자세한 정보를 확인하려면  버튼을 선택하세요. 상세 조회 창이 나타납니다. 개별 대상에 대한 차트와 평균 및 최대값을 조회할 수 있습니다.



- **1일전:** 하루 전의 데이터와 비교해 확인할 수 있습니다.
- **1주전:** 한 주 전의 데이터와 비교해 확인할 수 있습니다.
- **↓ CSV:** 조회한 데이터를 CSV 형식의 파일로 다운로드할 수 있습니다.
- 그래프 차트 하단의 아이콘을 드래그하면 차트의 크기를 조절할 수 있습니다.

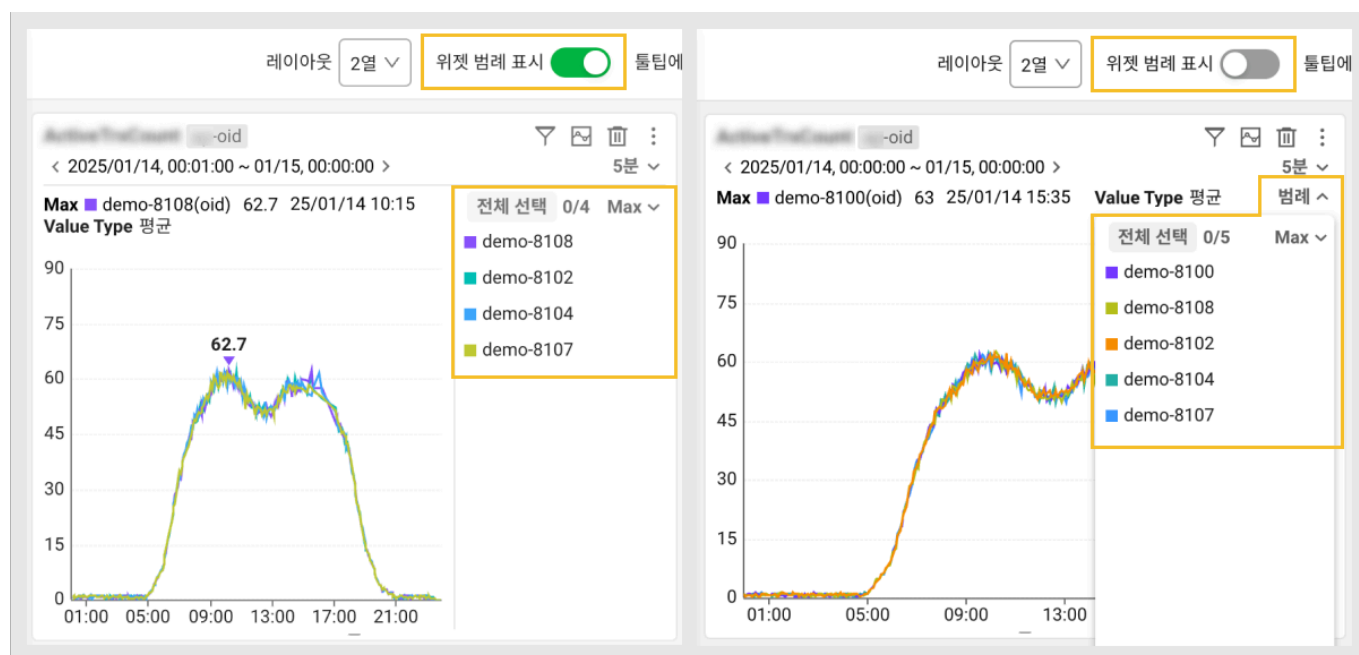


🗑️ 차트 위젯 삭제하기

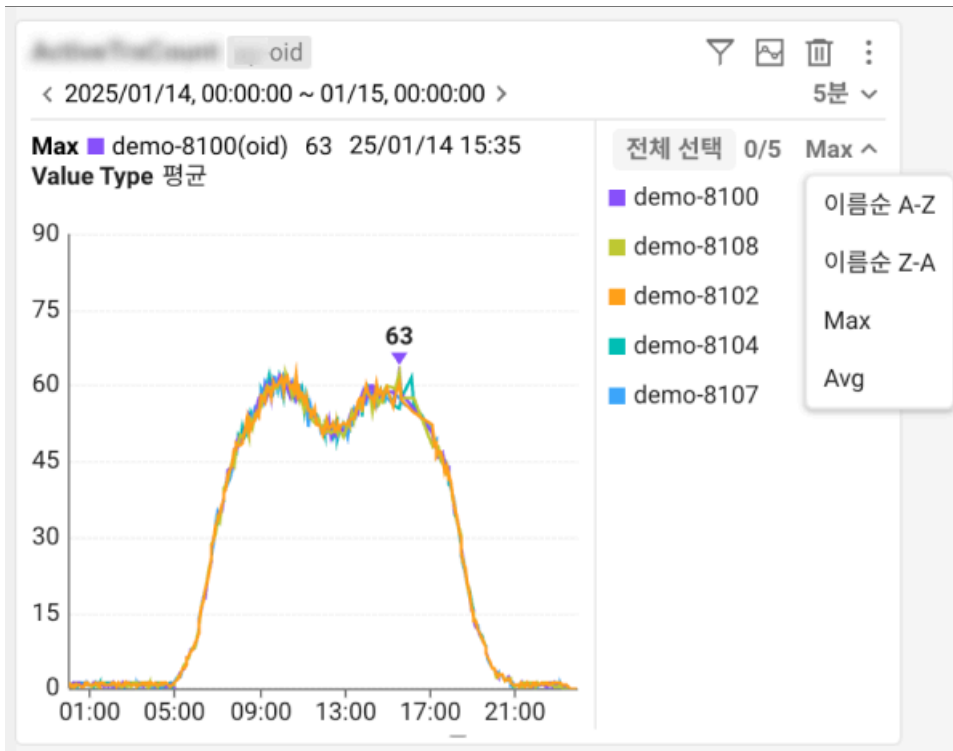
화면에 배치한 차트 위젯을 삭제하려면 🗑️ 버튼을 선택하세요.

범례 활용하기

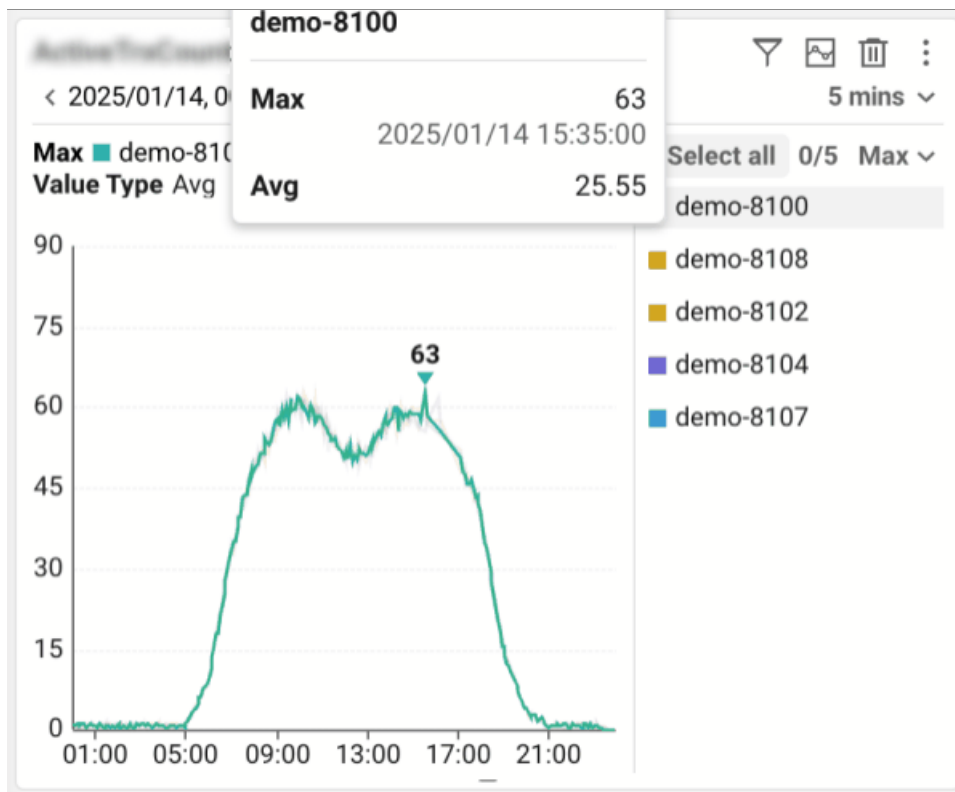
범례를 통해서 차트에 표시되는 모니터링 대상을 확인하고, 원하는 기준으로 정렬하거나 필터링할 수 있습니다. 화면 상단의 **위젯 범례 표시** 옵션을 켜거나 끄면 위젯의 차트 오른쪽에 범례를 표시하거나 숨길 수 있습니다. 옵션을 끈 상태에서는 **범례**를 클릭해 모니터링 대상을 확인하고, 선택할 수 있습니다.



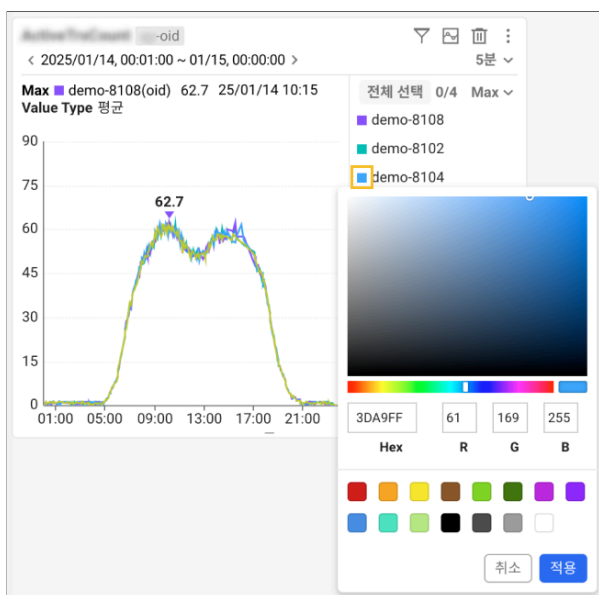
- 전체 선택/전체 해제 버튼을 선택해 모니터링 대상을 선택하거나 해제할 수 있습니다.
- 범례 목록에서는 모니터링 대상을 이름순, 최댓값, 평균값 기준으로 정렬할 수 있습니다.



- 범례 목록에서 각 항목에 마우스를 오버하면 해당 모니터링 대상에 대한 그래프를 강조해서 확인할 수 있고, Max 값이 기록된 특정 시간을 톨팁으로 표시합니다. 또는 범례 목록의 대상을 선택해 필터링할 수도 있습니다.



범례 색상 변경하기

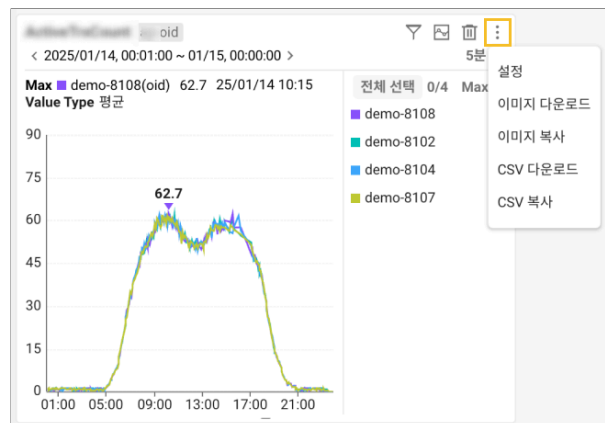


모니터링 대상에 해당하는 그래프의 색상을 변경할 수 있습니다. 범례 목록에서 색상을 변경하려는 대상의 왼쪽에 네모 상자를 선택하세요. 원하는 색상을 선택한 다음 **적용** 버튼을 클릭하세요.

❗ 설정한 색상은 프리셋 기능을 통해서 저장되지 않습니다. 이 기능은 향후 업데이트를 통해 제공할 예정입니다.

추가 옵션 이용하기

차트 위젯 오른쪽 상단에  버튼을 선택하면 다음의 추가 옵션을 이용할 수 있습니다.



• 설정

- **자동 Y축 사용:** 조회한 데이터 범위 내의 Y축의 크기를 자동 조정할 수 있습니다.
- **최대값 표시:** 차트의 그래프 영역에 최대값을 표시할 수 있습니다.
- **이미지 다운로드:** 차트를 이미지 형식의 파일로 다운로드할 수 있습니다.
- **이미지 복사:** 차트를 이미지 형식으로 클립보드에 복사할 수 있습니다.
- **CSV 다운로드:** 차트에서 조회한 데이터를 CSV 형식의 파일로 다운로드할 수 있습니다.
- **CSV 복사:** 차트에서 조회한 데이터를 CSV 형식으로 클립보드에 복사할 수 있습니다.

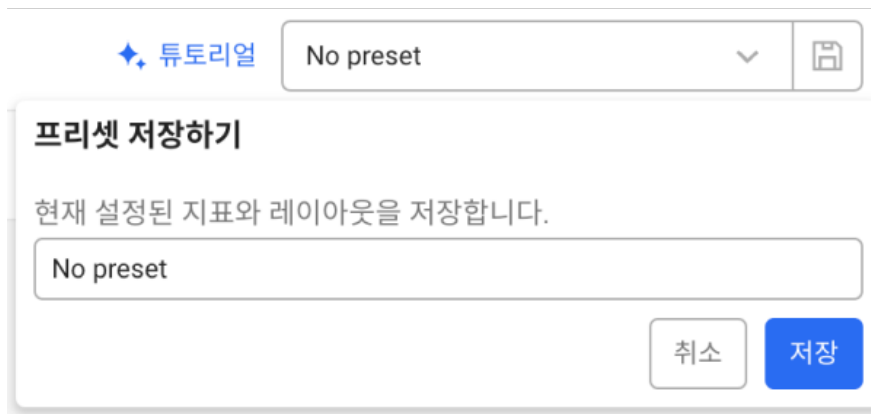
프리셋 설정하기

대시보드에서 사용자가 설정한 위젯의 설정과 레이아웃 상태를 저장하고 불러올 수 있습니다. 위젯의 크기를 조절하고, 원하는 위치에 배치해 새로운 프리셋을 만들 수 있습니다.

❗ **프로젝트 수정** 권한이 있는 멤버만 프리셋을 저장하거나 수정할 수 있습니다. 멤버 권한에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.

새로운 프리셋 만들기

1. 대시보드에서 원하는 형식으로 위젯을 배치해 보세요. 크기를 조절하고 자주 확인하는 위젯만 배치할 수도 있습니다.
2. 화면 오른쪽 위에  버튼을 선택하세요.
3. 새로운 프리셋 이름을 입력하세요.



4. **저장** 버튼을 선택하세요.

프리셋 목록에서 새로 저장한 프리셋을 확인할 수 있습니다.

- ❗
- 새로 만든 프리셋에 변경 사항이 생겼다면 다시 프리셋을 저장해야 합니다.  버튼을 선택한 다음 같은 이름으로 프리셋을 저장하세요. 기존의 프리셋에 변경 사항을 덮어쓰기합니다.
 - 대시보드의 변경 사항을 저장하지 않고 다른 메뉴로 이동하면 변경 사항은 저장되지 않습니다.
 - 프리셋은 프로젝트 단위로 저장되어 다른 사용자와 공유할 수 있습니다.
 - 프리셋에 저장되는 대상은 대시보드의 레이아웃과 대시보드에 배치한 위젯, 위젯에서 수정한 옵션(**대상**, **인터벌**)입니다. 화면 상단의 **시간** 옵션은 저장되지 않습니다.
 - 프리셋을 불러온 다음 위젯의 조회 시간을 변경하려면 **일괄 변경** 기능을 이용하세요. 자세한 내용은 [다음 문서](#)를 참조하세요.

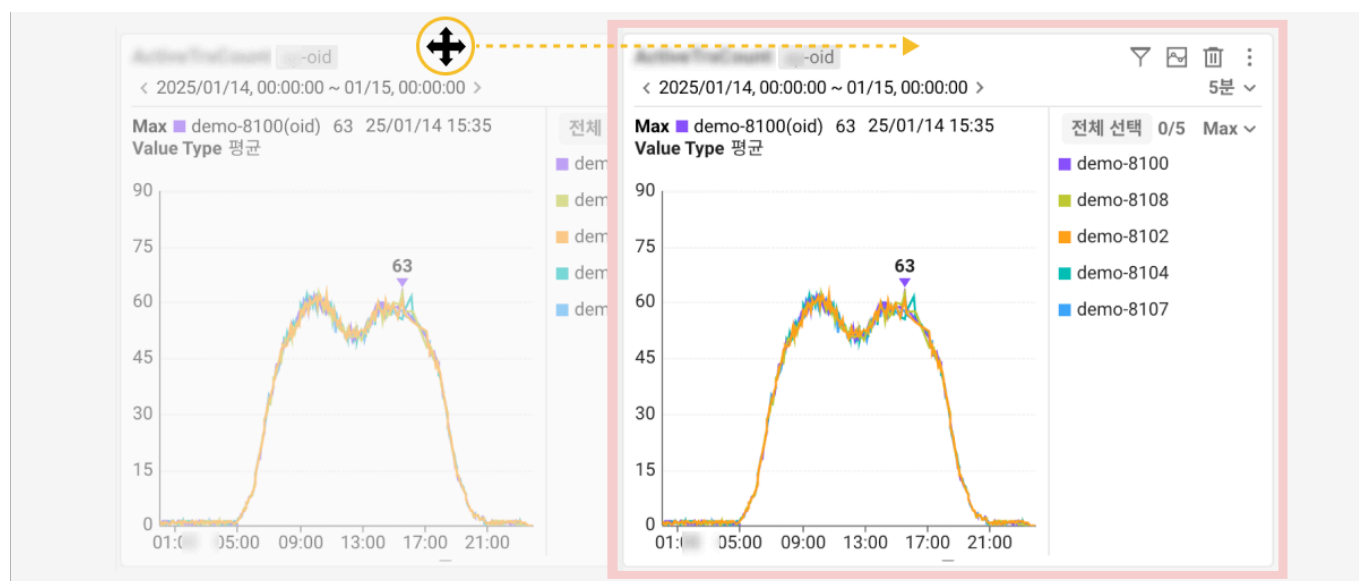
프리셋 삭제하기

사용하지 않는 프리셋이 있다면 프리셋 목록에서 삭제할 수 있습니다. 프리셋 목록에서 삭제하려는 항목의 오른쪽에 ✕ 버튼을 선택하세요.

대시보드 위젯 편집하기

대시보드에 배치한 위젯을 사용자가 원하는 위치에 배치하거나 크기를 조절할 수 있습니다.

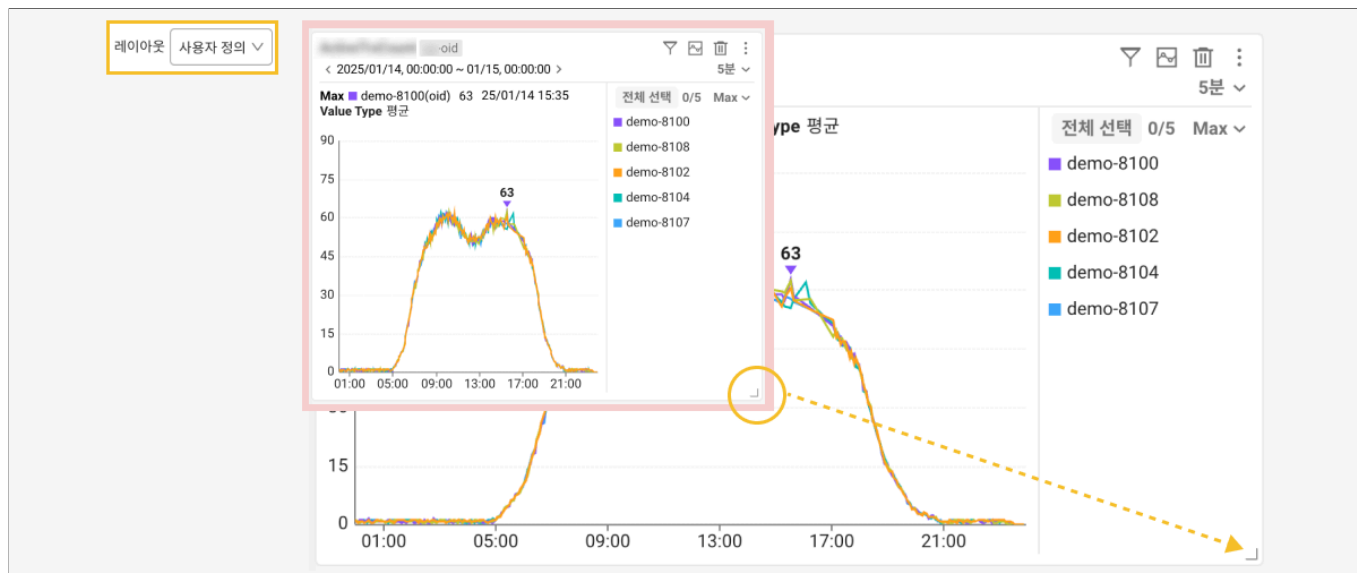
위젯 이동하기



위젯의 상단 부분을 마우스 포인터로 이동하면 + 모양으로 변경됩니다. 이때 마우스로 클릭한 상태로 원하는 위치로 드래그하여 위젯을 이동할 수 있습니다.

위젯 크기 조절하기

대시보드 옵션의 레이아웃이 사용자 정의로 설정되어 있으면 위젯의 크기를 조절할 수 있습니다.



위젯의 오른쪽 아래에  요소를 마우스로 클릭한 상태에서 원하는 크기로 드래그하세요.

ⓘ 레이아웃이 사용자 정의로 설정되어 있지 않다면 위젯의 높이만 조절할 수 있습니다. 위젯 하단 가운데 영역을 마우스로 클릭한 상태로 크기를 조절하세요.

대시보드 옵션 이용하기

화면 상단에 위치한 옵션 메뉴를 이용해 차트 위젯에 적용된 다양한 설정을 한번에 적용할 수 있습니다. 또한 대시보드의 레이아웃을 원하는 형태로 설정할 수도 있습니다.



차트 위젯 옵션 일괄 변경하기

화면에 배치된 차트 위젯에 세부 옵션을 한번에 적용할 수 있는 기능을 제공합니다. 화면 왼쪽 상단에 **일괄 변경** 버튼을 선택하세요. **일괄 변경** 창이 나타나면 원하는 옵션을 설정한 다음 **적용** 버튼을 선택하세요.

일괄 변경

×

시간

<

2025/01/21 00:00 ~ 2025/01/21 23:59

23시간

📅

>

대상

전체

대상 검색

🔍

전체 해제

2/3

▼ 전체 접기

🔄

▼ Project

qa-node-demo

✓

qa-php-demo

✓

인터벌

변경 안함

5분

1시간

적용 위젯

전체 선택

☐ User+Sys (%)

2025/01/21, 00:00:00 ~ 23:59:59

sm-oid

5분

☐ Used (%)

2025/01/21, 00:00:00 ~ 23:59:59

sm-oid

5분

☐ Rx (bps)

2025/01/21, 00:00:00 ~ 23:59:59

sm-oid

5분

☐ Total Thread#

2025/01/21, 00:00:00 ~ 23:59:59

sm-oid

5분

취소

적용

- **시간:** 차트의 데이터 조회 범위를 설정할 수 있습니다.
- **대상:** 모니터링 대상을 선택하세요. 개별 에이전트를 선택하거나 개별 에이전트를 선택하거나 에이전트 설정을 통해 분류한 그룹 단위로 선택할 수 있습니다.
 - **에이전트:** 개별 에이전트를 선택하거나 모두 선택할 수 있습니다.
 - **종류별:** 에이전트 설정에서 `whatap.okind` 로 분류된 그룹 단위로 에이전트를 모니터링합니다.
 - **서버별:** 에이전트 설정에서 `whatap.onode` 로 분류된 그룹 단위로 에이전트를 모니터링합니다.

586

- **인터벌:** 다양한 시간 간격으로 데이터의 집계 단위를 조정할 수 있습니다.
- **적용 위젯:** 변경할 옵션을 적용할 차트 위젯을 선택하세요. 선택한 위젯에 변경한 옵션을 한번에 적용할 수 있습니다.

대시보드 자동 정렬하기

대시보드에 배치한 위젯들의 위치를 자동 정렬하려면 **자동 정렬** 버튼을 선택하세요. 위젯의 너비, 높이가 작은 크기 순으로 위젯의 배치를 자동 정렬합니다. 너비가 같으면 높이가 작은 순으로 정렬합니다.

여러 개의 차트 비교하기

대시보드에 배치한 여러 개의 차트 데이터를 하나의 차트에서 확인할 수 있는 기능입니다. 이 기능을 통해서 동시간대의 여러 지표 정보를 다른 지표와 비교해가며 확인할 수 있습니다. **차트 오버레이** 버튼을 선택하세요. 화면에 오버레이 차트를 배치할 수 있습니다.



- 오버레이 차트 왼쪽 상단에 **건수**를 선택하면 x축 차트의 데이터 기준을 변경할 수 있는 목록이 나타납니다. 원하는 항목을 선택해 차트의 데이터를 비교할 수 있습니다.
-  : 현재 조회 중인 데이터를 기준으로 차트를 이미지 형식의 파일로 다운로드할 수 있습니다.
-  : 현재 조회 중인 데이터를 기준으로 차트를 CSV 형식의 파일로 다운로드할 수 있습니다.
- 오른쪽 섹션에서는 각 지표별 에이전트 목록을 확인할 수 있습니다. 개별 에이전트의 색상은 차트의 그래프 색상과 일치합니다.

배치된 위젯 일괄 삭제하기

대시보드에 배치한 여러 개의 위젯을 한번에 삭제할 수 있습니다. **전체 위젯 삭제** 버튼을 선택하세요. 확인 메시지가 나타나면 **삭제** 버튼을 선택하세요.

CSV 파일로 다운로드하기

대시보드에 배치한 위젯의 데이터를 CSV 형식의 파일로 다운로드할 수 있습니다. **다운로드 > CSV 다운로드**를 선택하세요. 각 시간대별 지표의 데이터를 확인할 수 있습니다.

이미지 파일로 다운로드하기

대시보드에 배치한 모든 위젯을 하나의 이미지 형식의 파일로 다운로드할 수 있습니다. **다운로드 > 이미지 다운로드**를 선택하세요. 대시보드 화면을 그대로 캡처한 이미지를 저장할 수 있습니다.

기타 옵션 이용하기

그 밖의 다음 기타 옵션을 통해 대시보드의 레이아웃을 조정하거나 위젯의 적용된 옵션을 쉽고 간편하게 일괄 설정할 수 있습니다.



- **레이아웃**: 대시보드에서 열의 수, 즉 한 줄에 배치할 수 있는 위젯의 개수를 설정할 수 있습니다. 최대 4열까지 설정할 수 있습니다. **사용자 정의**를 선택하면 열의 수에 상관없이 위젯을 배치할 수 있습니다.

① **사용자 정의**에서는 위젯의 너비와 높이를 자유롭게 조절할 수 있습니다. 다른 옵션을 선택하면 위젯의 높이만 조절할 수 있습니다.

- **위젯 범례 표시**: 옵션을 켜거나 끄면 위젯의 차트 오른쪽에 범례를 표시하거나 숨길 수 있습니다. 옵션을 끈 상태에서는 **범례**를 클릭해 모니터링 대상을 확인하고, 선택할 수 있습니다. 범례 활용에 대한 자세한 내용은 [다음 문서](#)를 참조하세요.
- **툴팁에 대상 모두 표시**: 차트에 마우스 포인터를 가져가면 해당 그래프의 위치에 해당하는 값을 툴팁을 통해 확인할 수 있습니다. 마우스 포인터가 위치한 시간대의 모든 대상의 데이터를 툴팁을 통해서 확인하려면 옵션을 켜세요.
- **위젯 높이 일괄 적용**: 옵션을 켜면 모든 위젯의 높이를 동일하게 설정할 수 있습니다.

- **차트 시간 일괄 적용:** 개별 차트 위젯의 데이터 조회 시간을 변경할 때, 다른 위젯의 차트 시간도 같이 변경하려면 옵션을 켜세요.

튜토리얼 이용하기

화면 오른쪽 상단에 **튜토리얼** 버튼 선택 시 튜토리얼을 사용할 수 있습니다.