

Zabbix 入門セミナー

～ゼロから始めるサーバ監視～

SRA OSS合同会社

OSS 事業本部 技術部 基盤技術グループ

- 監視について
- Zabbix の概要
- Zabbix の基本的な操作

- ☑ 村中 拓磨 (ムラナカ タクマ)
- ☑ SRA OSS合同会社 OSS 事業本部 基盤技術グループ
- ☑ Zabbix 認定スペシャリスト

職務

- ☑ Zabbix を中心とした OSS のテクニカルサポートや構築を担当

監視について

- 本来稼働しているはずのサービスに障害が発生したとき

監視をしていない場合

- どのサーバ・サービスが原因になっているか特定する時間がかかる
- 障害が発生していることに気づかない可能性も

結果として顧客にまで影響が及ぶことも

監視をしている場合

- 障害発生の原因特定が容易
- 障害の発生をリアルタイムで確認できる

障害発生時の迅速な対応が可能かつ日頃の監視によって未然に防げることも

なにを監視する？

- サーバリソース（メモリや CPU の使用率など）
 - ネットワーク（機器に対して疎通が取れるか、ダウンしていないか）
 - アプリケーション（プロセスが稼動しているか）
 - Web ページ（Web ページが表示されるか、画面遷移できるか）
 - ログ（サーバやアプリケーションにエラーが発生していないか）
- etc.

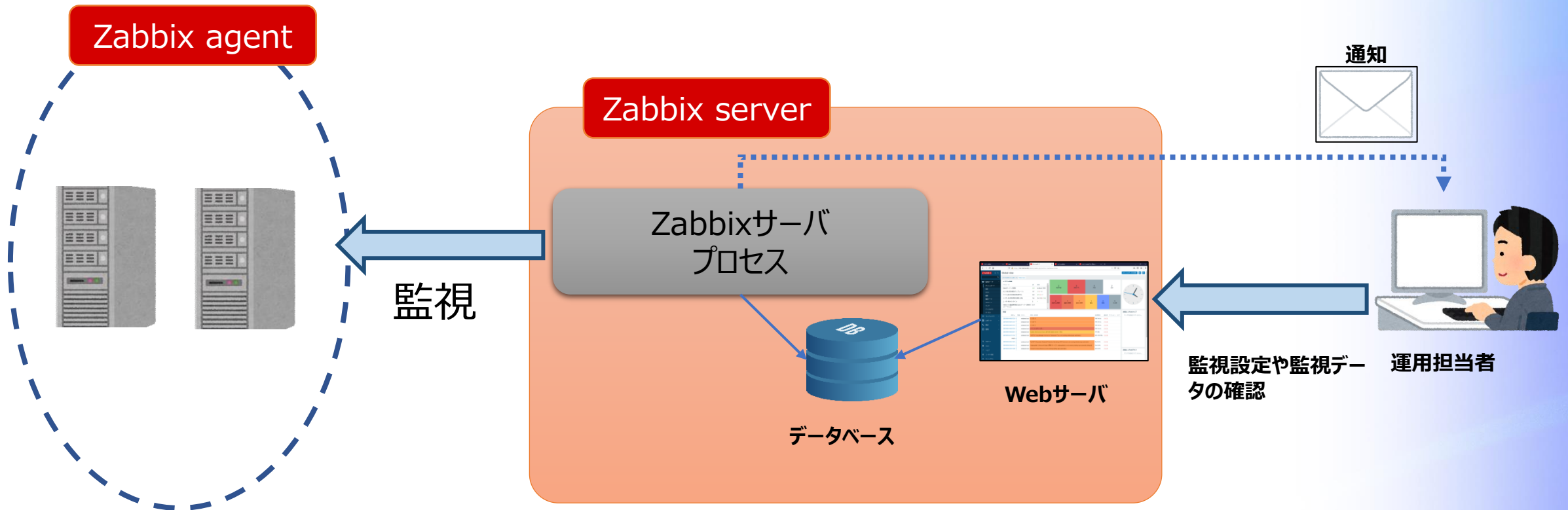
Zabbix の概要

- ネットワーク上の機器やサービスを監視して、異常があれば、通知してくれるオープンソースの統合監視ソフトウェア
- 最新版は、Zabbix6.4 (2023/3 リリース)
- 2004 年バージョン 1.0 がリリース

- Zabbix のメジャーバージョンは LTS とポイントリリースの 2 種類がある
- LTS は 1 年半周期で、ポイントリリースは半年周期でリリースされる
- サポート（開発）期間の長さが異なり、ポイントリリースは約半年で期間終了となる
- サポート期間が終了すると、バグ修正や機能改善がされなくなるため LTS バージョンによる構築を推奨

LTS (Long Term Support)
6.0 (2022/2 リリース)
5.0 (2020/5 リリース)

ポイントリリース
6.4 (2023/3 リリース)
6.2 (2022/5 リリース)



Zabbix server

- Linux
- IBM AIX
- FreeBSD
- NetBSD
- OpenBSD
- HP-UX
- Mac OS X
- Solaris

Zabbix agent

- Linux
- IBM AIX
- FreeBSD
- NetBSD
- OpenBSD
- HP-UX
- Mac OS X
- Solaris
- Windows

Zabbix agent2

- Linux
- Windows

監視メトリクス

エージェント監視

リソース監視

- CPU
- メモリ
- ネットワーク
- ファイルシステム

ポート監視

ログ監視

プロセス/サービス 監視

Web 監視

エージェントレス監視

ICMP 監視

DB 監視

SNMP 監視

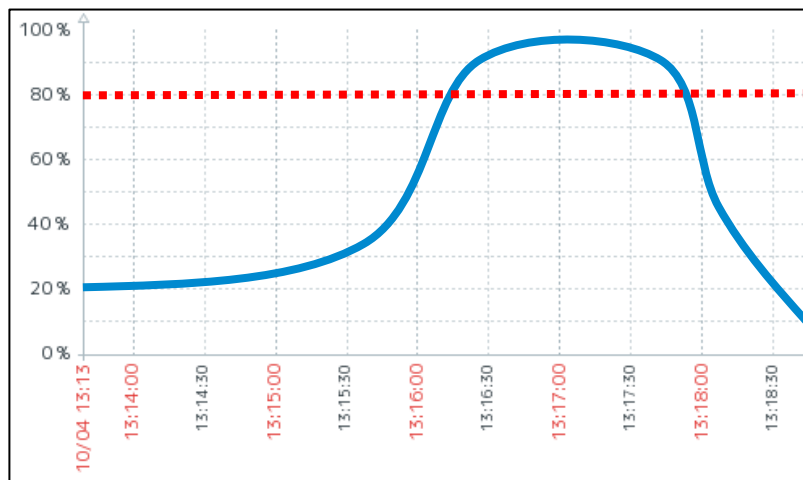
Java 監視

SSH/Telnet 監視

VMware 監視

- アイテムが取得したデータに対して任意の障害の発生条件を作成できる

閾値



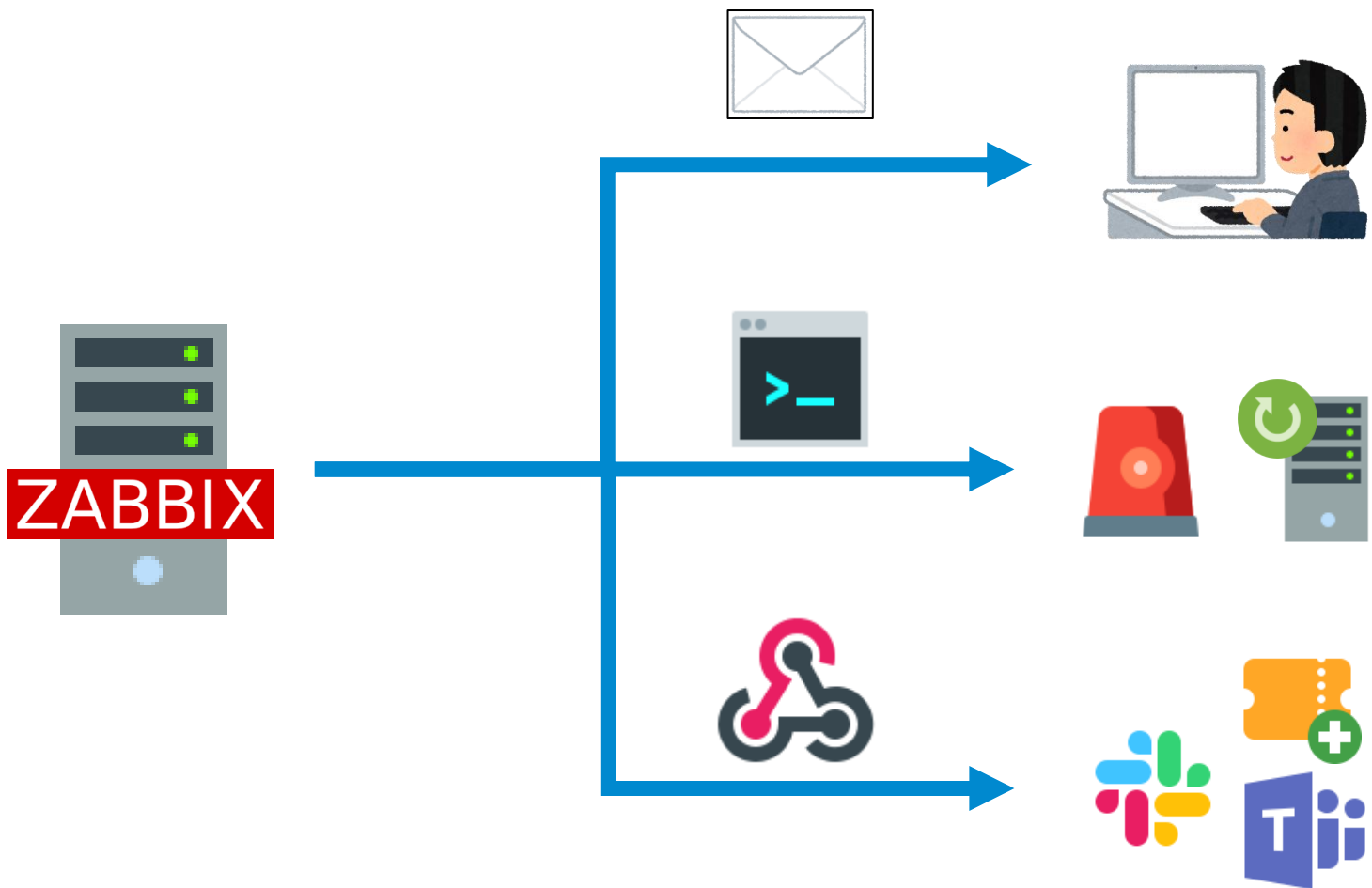
(例)メモリ使用率が 80% を超えたら障害とする

文字列

```
2023 02/14 09:13:25 [INFO] ...  
2023 02/14 09:15:10 [ERROR] ...  
2023 02/14 09:21:47 [INFO] ...
```

(例)アプリケーションのログに「ERROR」が出力されたら
障害とする

障害発生時の通知(アクション)



担当者にメール

HTML メールにも対応

コマンド実行

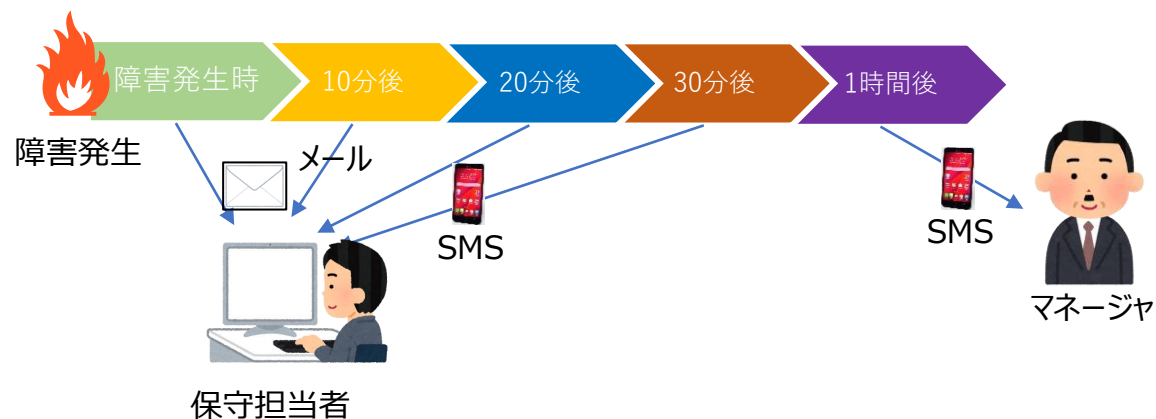
サーバやプロセスの再起動
パトランプの点灯

Webhook

外部アプリとの連携
Slack, Teams, Redmine etc.

- 通知のエスカレーションが可能

(例)障害発生から 10 分おきに継続して保守担当者へメール通知、
障害発生から 1 時間経過しても復旧しない場合は
マネージャに SMS 通知



用語	説明
ホスト	監視対象となるサーバやデバイス。 IP アドレスや DNS 名を設定する。
アイテム	ホストに対する監視項目。 CPU 使用率、メモリ使用率など 1 アイテムにつき 1 項目。
トリガー	アイテムが取得したデータに対する障害の発生条件の設定。
イベント	トリガーが閾値を超えた/下回った場合に内部生成される 障害/復旧のインシデント履歴。
アクション	イベント生成時に実行される、障害通知（メール）や コマンド実行などの設定。

- アイテム、トリガーなどがテンプレート化でき、複数のホストに同じ監視設定をするときにテンプレートを利用すると効率的
- Zabbix をインストールするとデフォルトで様々な機器やサービスのテンプレートが搭載されているため、自ら監視設定を作成せずとも監視を始められる

標準テンプレート一例

AWS

Cisco

Microsoft

VMware

F5

etc.

特定のグラフや障害の発生数、地理マップ、Zabbix server の情報など
 様々なデータを一元的に表示可能

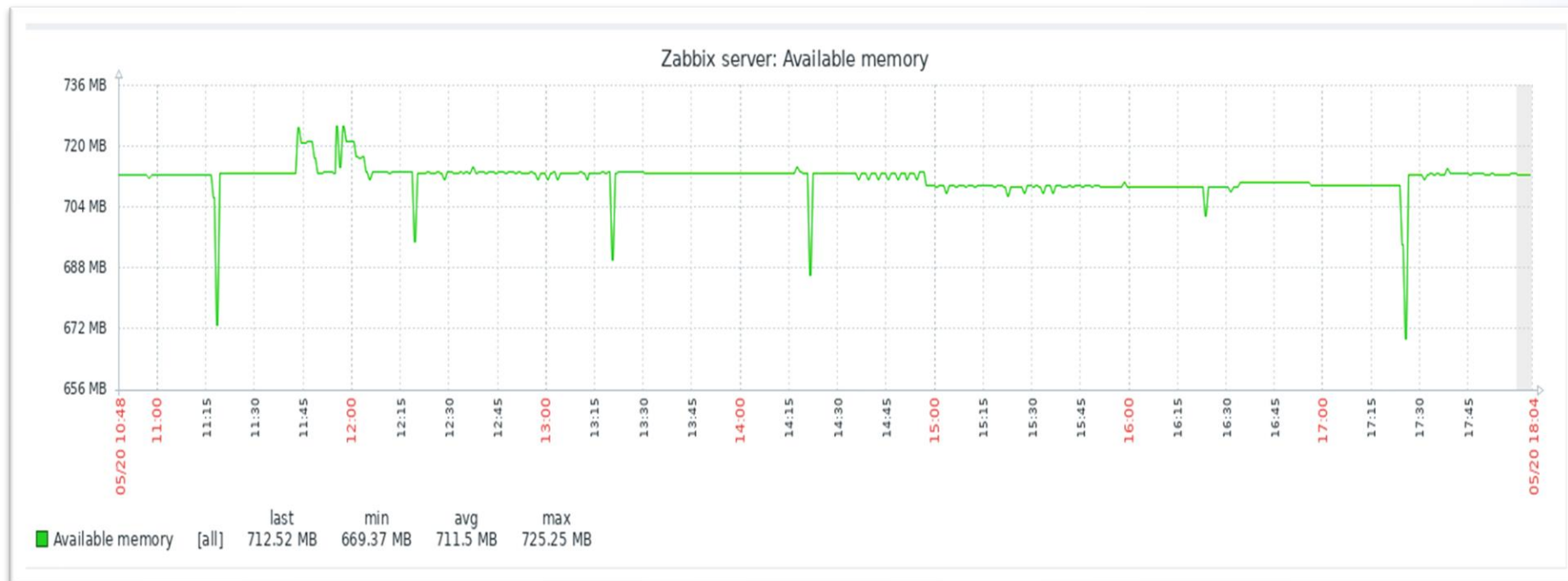


定期的な統計情報の PDF レポートの送信

- ダッシュボードを定期レポートとしてメール送信可能
- 日次、週次、月次の定期レポート送信をスケジュール可能



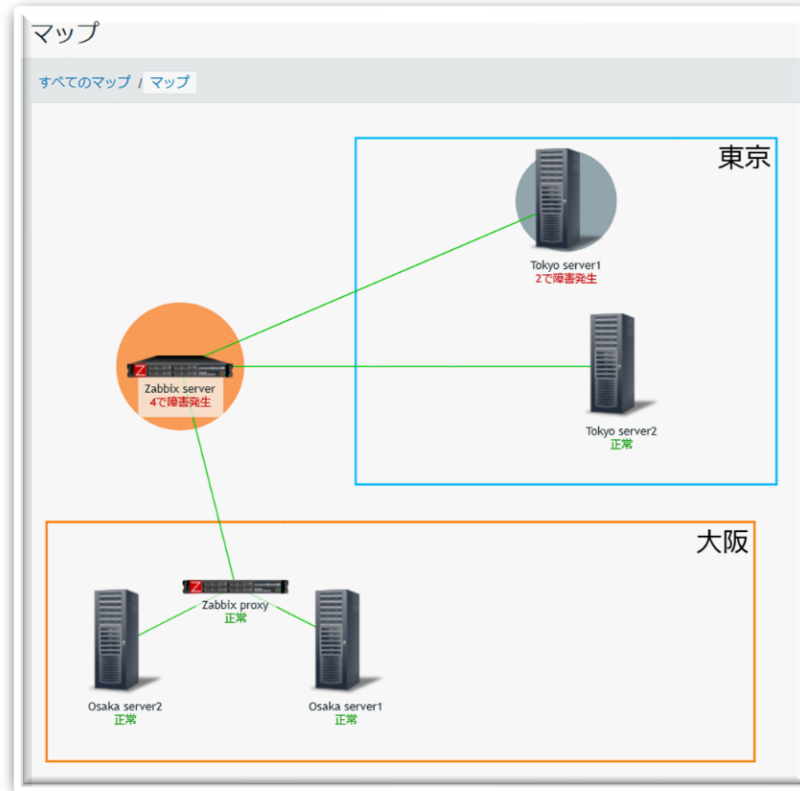
- アイテムが取得したデータを自動的にグラフ表示してくれる
- 表示範囲の指定も柔軟にできる
- 長期間の表示も可能でデータの推移・傾向を把握できる



- 「監視データ」→「障害」
- 過去の障害履歴や対応の履歴（対応コメントなど）を確認できる

時間	深刻度	復旧時刻	ステータス	情報	ホスト	障害	継続期間	確認済	アクション	タグ
18:29:00	軽度の障害	18:31:21	解決済		Linux sever3	Linux server3と疎通が取れません	2m 21s	はい	1	
18:28:32	情報		障害		Zabbix server	Host information was changed on Zabbix server	3m 47s	いいえ		Application: General Application: OS
18:28:27	情報		障害		Zabbix server	Hostname was changed on Zabbix server	3m 52s	いいえ		Application: General Application: OS
18:26:04	軽度の障害	18:32:04	解決済		linux server2	CPU使用率が70%を超えました	6m	はい	1	

- 「監視データ」→「マップ」
- 任意のマップを作成することが可能で、インフラの構成やどのサーバで障害発生しているのかを把握しやすくなる



Zabbix は自動的にネットワークをスキャンして、検出されたデバイスを監視対象として追加することが可能

- 複数のネットワークインターフェースを持つデバイスの検出
- IP アドレス範囲を指定したネットワークスキャン
- 検出されなくなったデバイスの非監視対象可

Zabbix の操作 ～ホスト、アイテム、 トリガー作成～

ダウンロードページに OS、使用する DB、Webサーバに応じたインストール手順が記載されています。

<https://www.zabbix.com/jp/download>

今回は監視マネージャとなるサーバには [Zabbix 6.0 インストール](#) 内の手順をもとに Zabbix server6.0, PostgreSQL14, Apache をインストール
監視対象のサーバには Zabbix agent6.0 のみインストール

監視マネージャサーバ

OS: RHEL8

Zabbix server6.0

DB: PostgreSQL14

Web サーバ: Apache



監視

監視対象サーバ

OS: RHEL8

IPアドレス: 192.168.44.32

Zabbix agent6.0

今回は以下の流れで監視対象のサーバの CPU 使用率を監視して、40% を上回ったら障害とするような設定を行います。

1. ホスト作成
2. アイテム作成
3. トリガー作成

1. ホスト作成

- 「設定」→「ホスト」→「ホストの作成」

監視対象のサーバのホスト名、
ホストが所属するグループ、
サーバの IP アドレスを入力

ホスト名: Linux server

グループ: Linux servers

インターフェース:

タイプ: エージェント

IP: 192.168.44.32

新しいホストの作成

ホスト IPMI タグ マクロ インベントリ 暗号化 値のマッピング

ホスト名 Linux server

表示名 Linux server

テンプレート 検索文字列を入力

グループ Linux servers

検索文字列を入力

インターフェース	タイプ	IPアドレス
	エージェント	192.168.44.32

追加

説明

プロキシによる監視 (プロキシなし) ▾

有効

2. アイテム作成

- 「設定」→「ホスト」→「Linux server」→「アイテム」→「アイテムの作成」

サーバの CPU 使用率を取得するアイテムを作成

名前: CPU使用率

タイプ: Zabbixエージェント

キー: system.cpu.util

データ型: 数値(浮動小数)

監視間隔: 10s

アイテム

すべてのホスト / Linux sever 有効 ZBX アイテム1 トリガー グラフ ディスカバリールール Webシナリオ

アイテム タグ 保存前処理

* 名前 CPU使用率

タイプ Zabbixエージェント

* キー system.cpu.util 選択

データ型 数値(浮動小数)

* ホストインターフェース 192.168.44.32:10050

単位

* 監視間隔 10s

3. トリガー作成

- 「設定」→「ホスト」→「Linux server」→「トリガー」→「トリガーの作成」

CPU 使用率が 40% を超えたら
障害とするトリガーを作成

名前: CPU使用率が40%を超えました

深刻度: 警告

条件式:

`last(/Linux server/system.cpu.util)>40`



トリガー

すべてのホスト / Linux sever 有効 ZBX アイテム 1 トリガー-1 グラフ ディスカバリールール Webシナリオ

トリガー タグ 依存関係

* 名前 CPU使用率が40%を超えました

イベント名 CPU使用率が40%を超えました

運用データ

深刻度 未分類 情報 警告 軽度の障害 重度の障害 致命的な障害

* 条件式 `last(/Linux sever/system.cpu.util)>40` 追加

条件式ビルダー

- 監視対象サーバに SSH ログインをして以下のコマンドを実行

yes > /dev/null (障害発生確認後「Ctrl + C」で停止)

必ず自身の検証サーバなど本番として稼働していないサーバで実行してください！

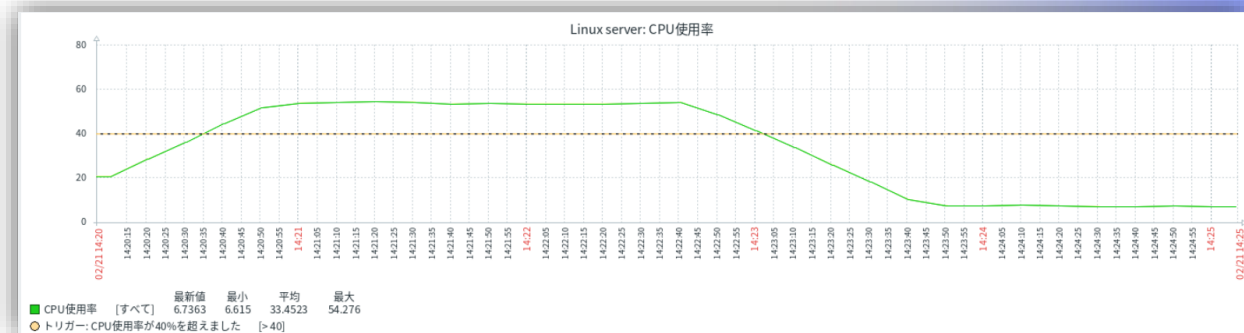
障害

< 🔍

時間	深刻度	復旧時刻	ステータス	情報	ホスト	障害
14:20:41	<input type="checkbox"/>		警告	障害	Linux server	CPU使用率が40%を超えました

0 選択 一括更新

「監視データ」→「障害」



「監視データ」→「最新データ」→「CPU使用率の「グラフ」」

- SRA OSS LLC Youtube チャンネル
<https://www.youtube.com/c/sraoss-official>
- SRA OSS Tech Blog
<https://www.sraoss.co.jp/tech-blog/>
 - [第 1 回 Zabbix を動かしてみよう](#)
 - [第 2 回 Zabbix のさまざまな監視機能を試してみよう](#)
 - [第 3 回 Zabbix API 入門](#)
 - [Zabbix 6.0 インストール](#)

ご清聴ありがとうございました。