

Zabbix 3.0でどう 変わるか

2016年2月26日
ZABBIX-JP 田中 敦

自己紹介

▶ 氏名

▶ 田中 敦 (たなか あつし)

▶ Twitter: @atanka7

▶ 所属

▶ ZABBIX-JP (統合監視ツールZabbixの日本のコミュニティ)

▶ 役職

▶ 副代表

▶ 主な活動

▶ ZABBIX-JPのサイト (<http://www.zabbix.jp/>) で情報発信と
問い合わせ対応

▶ ZabbixのUIなどの日本語翻訳

今日のアジェンダ

- ▶ はじめに
- ▶ Zabbixとは？
- ▶ Zabbix 3.0の新機能と改善点
- ▶ Zabbix 3.0利用時の注意点
- ▶ Zabbix 3.0の応用
- ▶ まとめ

はじめに

はじめに

- ▶ Zabbix 3.0がようやくリリース！
(2016/02/16)
- ▶ Zabbix 3.0で改善された点や新機能を生かすことで、どのような運用ができるようになるかを紹介する。

Zabbixとは？

Zabbixとは

- ▶ オープンソースの統合監視ツール
- ▶ ヨーロッパにあるラトビアという国でZabbix LLCという会社が開発
- ▶ 初期バージョンがリリースされて約10年経過
- ▶ 監視用エージェントを各サーバにインストールして監視
- ▶ UNIX、Linux、Windowsなどの各OSに対応したエージェントあり
- ▶ エージェントがなくても、SNMP、ssh、telnet、IPMI、JMXなどでも監視可
- ▶ 監視の設定はWebブラウザからできる
- ▶ 監視設定にはテンプレートという監視設定パターンをまとめておくと、新しい監視対象のサーバが追加されたら紐づけするだけで監視開始
- ▶ 監視のために取得した各種データは、グラフ化して傾向を把握しやすい
- ▶ 障害検知時に、メールやメッセージを送るだけでなく、独自のスクリプトを実行可能
- ▶ マルチテナントの機能を利用して、同じZabbixサーバ上で利用者を分離可能
- ▶ などなどなどなどなどなどなど...

Zabbixの画面イメージ

8

The image displays a screenshot of the Zabbix web interface in Mozilla Firefox. The interface is divided into several panels:

- Dashboard (ダッシュボード):** Shows navigation links for monitoring data, inventory, reports, and settings. It includes a sidebar with options for adding graphs, screens, and maps.
- Network Map (ネットワークマップ):** Displays a map of Japan with a highlighted region labeled "福岡 正常" (Fukuoka Normal).
- Trigger Status (トリガーのステータス):** A table showing 26 triggers. The first few are in a warning state (yellow), while others are normal (green).
- CPU Load (カスタムグラフ):** A line graph showing processor load over time. The legend indicates: Processor load (1 min average) in green, Processor load (5 min average) in blue, and Processor load (15 min average) in red.
- Disk Space Usage (カスタムグラフ):** A pie chart titled "tkyweb01: Disk space usage / (1h)". The legend shows: Total disk space on / [平均] in red (17.11 GB, 100%) and Free disk space on / [平均] in green (15 GB, 87.70%).

The footer of the interface includes "Zabbix 2.4.6 Copyright 2001-2015 by Zabbix SIA" and "ユーザー 'Admin' でログイン".

Zabbix 3.0の画面イメージ

9

ZABBIX 監視データ インベントリ レポート 設定 管理

ダッシュボード 概要 Web 最新データ トリガー イベント グラフ スクリーン マップ ディスカバリ ITサービス

ダッシュボード

お気に入りのグラフ
グラフが追加されていません。
グラフ

お気に入りのスクリーン
スクリーンが追加されていません。
スクリーン スライドショー

お気に入りのマップ
マップが追加されていません。
マップ

Zabbixサーバーの状態

パラメータ	値	詳細
Zabbixサーバーの起動	はい	localhost:10051
ホスト数 (有効無効テンプレート)	40	2 / 0 / 38
アイテム数 (有効無効取得不可)	107	102 / 0 / 5
トリガー数 (有効無効 [障害/正常])	61	61 / 0 [0 / 61]
ユーザー数 (オンライン)	2	1
1秒あたりの監視項目数 (Zabbixサーバーの要求パフォーマンス)	1.37	

更新時刻: 17:33:41

システムステータス

ホストグループ	致命的な障害	重度の障害	軽度の障害	警告	情報	未分類
Linux servers	0	0	0	0	0	0
Zabbix servers	0	0	0	0	0	0

更新時刻: 17:33:40

最新20件の障害

ホスト	問題	最新の変更	経過時間	情報	コメントあり	アクション
データがありません。						

0件中0件の障害が表示されています 更新時刻: 17:33:41

Web監視

ホストグループ	正常	失敗	不明
データがありません。			

更新時刻: 17:33:41

ホストステータス

ホストグループ	障害なし	障害あり	合計
Linux servers	1	0	1
Zabbix servers	1	0	1

更新時刻: 17:33:41

Zabbix 3.0の新機能と 改善点

Zabbix 3.0の新機能と改善点（1）

- ▶ 通信暗号化と認証
- ▶ アイテム取得間隔の柔軟化
- ▶ マップやスクリーンの共有

Zabbix 3.0の新機能と改善点（2）

12

- ▶ 予測関数
- ▶ SMTP認証
- ▶ ログから数値取得

通信暗号化と認証

- ▶ ZabbixサーバーとZabbixエージェント間、ZabbixサーバーとZabbixプロキシ間など、各コンポーネントの間の通信の暗号化が可能になった。
- ▶ 暗号化方式としては、PSKと証明書の2つの方法を利用することができる。
- ▶ 証明書を利用すれば、正しい証明書を持たない監視対象を勝手につないでしまうことを防ぐことができるので、第三者が不正なアイテムの値をZabbixサーバーに送りつけることを回避することができる。

通信暗号化と認証 (PSK) その1

14

- ▶ PSK (Pre-Shared Key) では、事前に暗号化通信のための鍵を共有しておいて、それを利用して通信の暗号化を行う。
- ▶ 構成例
 - ▶ 共有鍵の生成
 - ▶ `$ psktool -u user1 -p passwd.psk`
 - ▶ 生成されたファイルの頭の「user1:」を削除したファイル `zabbix_agentd.psk` を作成
 - ▶ `zabbix_agentd.conf` への設定

```
TLSCConnect=psk
TLSCAccept=psk
TLSPSKIdentity=user1
TLSPSKFile=/etc/zabbix/cert/zabbix_agentd.psk
```

通信暗号化と認証 (PSK) その2

15

- ▶ Webインターフェース上でホストの暗号化設定
 - ▶ PSKを選択
 - ▶ PSKアイデンティティとして、psktoolで指定したユーザー名を指定し、psktoolで生成されたファイルの「user1:」よりも後ろの部分をPSKに指定

The screenshot shows a web interface for configuring a host named 'LinuxDemo'. The '暗号化' (Encryption) tab is selected. Under 'ホストへの接続' (Connection to host), the 'PSK' option is selected. Under 'ホストからの接続' (Connection from host), the 'PSK' checkbox is checked. The 'PSKアイデンティティ' (PSK Identity) field contains 'user1', and the 'PSK' field contains a long alphanumeric string: '2e404b787f085c1ffd3f50efada9e2ccdc4aaa38b5f3f3eb09c7e876781d47a08b674f7d4b9178c'. At the bottom, there are buttons for '更新' (Update), '複製' (Copy), 'すべて複製' (Copy all), '削除' (Delete), and 'キャンセル' (Cancel).

アイテム取得タイミングの柔軟化

- ▶ アイテムの値取得の間隔を柔軟に設定することができるようになった。
- ▶ これを利用することで、特定の時刻にアイテムの値を取得したり、営業日かつ指定した時刻にアイテムの値を取得することができる。
- ▶ 日付や時刻を指定できるパラメータとしては、日付（1-31）、曜日（1-7 = 月曜日-日曜日）、時（0-23）、分（0-59）、秒（0-59）があり、これらを組み合わせて指定できる。

取得タイミングの設定箇所

17

監視データ インベントリ レポート 設定 管理

ホストグループ テンプレート **ホスト** メンテナンス アクション スクリーン スライドショー マップ ディスカバリ ITサービス

アイテム

すべてのホスト / Zabbix server 有効 ZBX SNMP JMX IPMI アプリケーション 11 アイテム 75 トリガー 46 グラフ 13 ディスカバリールール 2 Webシナリオ

名前

タイプ Zabbixエージェント

キー 選択

ホストインターフェース 127.0.0.1:10050

データ型 数値 (整数)

データの形式 10進数

単位

乗数を使用 1

更新間隔(秒)

更新間隔カスタマイズ

タイプ	更新間隔	期間	アクション
例外設定	定期設定	<input type="text" value="50"/>	<input type="text" value="1-7,00:00-24:00"/>

[追加](#) [削除](#)

ホスト保存期間(日)

トレンド保存期間(日)

保存時の計算 なし

アイテム取得タイミングの例

- ▶ 毎時、同じ分の時に複数のアイテムの値を取得する。
 - ▶ 毎時0分と30分に取得実施 ⇒ m0,30
 - ▶ 毎時10分毎に取得実施 ⇒ m/10
- ▶ 毎日、同じ時間にアイテムの値を取得する。
 - ▶ 毎日9時に取得実施 ⇒ h9
- ▶ 営業日のサービス時間帯のみアイテムの値を取得する。
 - ▶ 月曜日から金曜日まで9時から18時までに10分間隔で取得実施
⇒ wd1-5h9-18m/10

マップやスクリーンの共有

- ▶ マップ、スクリーン、スライドショーを管理者ではなくても作成して共有できるようになったので、Zabbixの各ユーザーの見たい形にカスタマイズできるようになった。
- ▶ これによって、マップやスクリーン、スライドショーの作成を、Zabbixサーバーの管理者に依頼して作成してもらわなくても、各自が自分の見たいものを見やすい形でスクリーンなどを作成できるようになる。
- ▶ 作成したマップやスクリーンは共有するユーザーやユーザーグループを指定して共有できるので、同じシステムやサービスの関係者間で共有して利用することができる。

マップの共有設定

20

ネットワークマップ

マップ 共有

タイプ 非公開 公開

共有するユーザーグループ ユーザーグループ
[追加](#)

共有するユーザー ユーザー 権限
[追加](#)

[追加](#) [キャンセル](#)

ネットワークマップ

マップ 共有

タイプ 非公開 公開

共有するユーザーグループ ユーザーグループ 権限 アクション
会計システム管理者 [読込専用](#) [読書可能](#) [削除](#)
[追加](#)

共有するユーザー ユーザー 権限 アクション
[追加](#)

[追加](#) [キャンセル](#)

予測関数

- ▶ トリガーの関数として予測関数が追加されたので、指定した時間後にどういう値になるか、指定した値に達するのがいつになるのかをトリガーで判断できるようになった。
- ▶ `forecast()`
 - ▶ 引数で指定した条件（近似関数、算定元とする時間範囲、経過時間）に対して、どのくらいの値になるかを返却する関数。
- ▶ `timeleft()`
 - ▶ 引数で指定した条件（近似関数、算定元とする時間範囲、アイテムの値）に対して、あとどれくらいの時間がかかるかを返却する関数。

- ▶ デフォルトで用意されているメール送信用のメディアに、SMTP認証の機能が追加された。
- ▶ これによって、障害発生時のメール送信を行う際、SMTPサーバーでの認証が必要となるような環境でも、標準のメール送信用のメディアに対する設定を追加するだけで利用できるようになった。
- ▶ SMTP認証を必要としていなくても、メール送信用のポート番号も指定できるようになったので、SMTPサーバーのポート番号を変更しているような環境でも標準のメール送信用のメディアで対応できるようになった。

Emailの設定画面

23

ZABBIX 監視データ インベントリ レポート 設定 管理

一般設定 プロキシ 認証 ユーザーグループ ユーザー **メディアタイプ** スクリプト

メディアタイプ

名前

タイプ

SMTPサーバー

SMTPサーバーポート番号

SMTP helo

送信元メールアドレス

接続セキュリティ なし STARTTLS SSL/TLS

認証 なし パスワード

有効

ログから数値取得

- ▶ Zabbix 2.2からアイテムキーのlog[]を使用して、正規表現を指定することで文字列を切り出すことができていたが、log[]の値は、データ型として「ログ」でしか保存できなかった。
- ▶ Zabbix 3.0からは、その切り出した文字列を数値としても保存できるようになったため、ログファイルに出力される行から数値の部分を切り出して、その値を数値として監視したりグラフ化したりすることができるようになった。

数値取得例

25

- ▶ ログファイルにサーバールームの気温が出力されているような環境にて。

- ▶ ログフォーマット

```
2016/02/24 13:42:24 Center: 1, Rack: 2-4, Temp: 27.5 degree
2016/02/24 13:47:24 Center: 1, Rack: 2-4, Temp: 28.4 degree
2016/02/24 13:52:24 Center: 1, Rack: 2-4, Temp: 27.9 degree
```

- ▶ 正規表現

- ▶ "Temp: ([0-9]+ | [0-9]+¥.[0-9]*) degree"

- ▶ アイテムのキー

- ▶ log[/tmp/sample.log,"Temp: ([0-9]+ | [0-9]+¥.[0-9]*) degree",,,,¥1]

その他の新機能と改善点

- ▶ メディアスクリプトの起動オプションカスタマイズ
- ▶ マクロの適用範囲確認
- ▶ trendのAPI提供
- ▶ ホスト登録時のインベントリモードの初期設定
- ▶ SNMPでのLLD時のOID複数化
- ▶ ハウスキーパー処理の手動実行
- ▶ 値のマッピングのインポート/エクスポートに対応
- ▶ Windowsのnet.if.*の計算元カウンタの64bit対応
- ▶ 各種デーモンをフォアグラウンドで実行可

Zabbix 2.2から2.4での主な新機能と改善

27

- ▶ LLDのマルチフィルタ
- ▶ アドホックグラフ
- ▶ SNMP bulk処理のホスト単位での設定
- ▶ Web監視でリクエストヘッダのカスタマイズ
- ▶ トリガー条件式記述方法の変更

Zabbix 3.0利用時の注意 点

システム要件

▶ 重要な変更点

- ▶ PHP 5.4以降 (PHP 7.0以降は未対応)
- ▶ libcurl 7.20.0以降(SMTP認証を利用する場合)
- ▶ gnutls 3.1.18以降(他の暗号化方式を選択することで回避可)
- ▶ openssl 1.0.1以降(他の暗号化方式を選択することで回避可)

各OSの対応状況

- ▶ RHEL 6/CentOS 6 - △
 - ▶ 標準のライブラリではSMTP認証の機能が利用不可
 - ▶ 初期のバージョンではopensslのバージョンが古い(1.0.0)ので、古いopensslでは暗号化通信利用不可
 - ▶ OSを最新の状態に更新し、通信暗号化にはopensslを選択、PHPはSCLなどを利用

- ▶ RHEL 7/CentOS 7 - ◎
 - ▶ OSを最新の状態に更新しておくこと
 - ▶ RHEL/CentOS 7.1.1503では、trousersというパッケージに問題があり、gnutlsとmysqlclientを同時に利用するプログラムが起動できない問題があった

- ▶ 各コンポーネント間の通信暗号化を利用するのであれば、`configure`時に以下の3つのうち1つオプションの追加が必要
 - ▶ `--with-openssl`
 - ▶ `--with-gnutls`
 - ▶ `--with-mbedtls`

メディアスクリプト呼び出し方法変更

32

- ▶ アクションから呼び出すメディアスクリプトの引数を自由に設定できるようになった
- ▶ 以前のメディアスクリプトをそのまま呼び出すときには引数の追加が必要

- ▶ {ALERT.SENDTO}
- ▶ {ALERT.SUBJECT}
- ▶ {ALERT.MESSAGE}

メディアタイプ

名前	<input type="text" value="メール送信"/>								
タイプ	スクリプト <input type="button" value="▼"/>								
スクリプト名	<input type="text" value="sendmessage_smtp_php/sendmessage_smtp_php.sh"/>								
スクリプトパラメータ	<table><thead><tr><th>パラメータ</th><th>アクション</th></tr></thead><tbody><tr><td><input data-bbox="1753 991 2339 1033" type="text" value="{ALERT.SENDTO}"/></td><td><input type="button" value="削除"/></td></tr><tr><td><input data-bbox="1753 1062 2339 1105" type="text" value="{ALERT.SUBJECT}"/></td><td><input type="button" value="削除"/></td></tr><tr><td><input data-bbox="1753 1133 2339 1176" type="text" value="{ALERT.MESSAGE}"/></td><td><input type="button" value="削除"/></td></tr></tbody></table>	パラメータ	アクション	<input data-bbox="1753 991 2339 1033" type="text" value="{ALERT.SENDTO}"/>	<input type="button" value="削除"/>	<input data-bbox="1753 1062 2339 1105" type="text" value="{ALERT.SUBJECT}"/>	<input type="button" value="削除"/>	<input data-bbox="1753 1133 2339 1176" type="text" value="{ALERT.MESSAGE}"/>	<input type="button" value="削除"/>
パラメータ	アクション								
<input data-bbox="1753 991 2339 1033" type="text" value="{ALERT.SENDTO}"/>	<input type="button" value="削除"/>								
<input data-bbox="1753 1062 2339 1105" type="text" value="{ALERT.SUBJECT}"/>	<input type="button" value="削除"/>								
<input data-bbox="1753 1133 2339 1176" type="text" value="{ALERT.MESSAGE}"/>	<input type="button" value="削除"/>								
	<input type="button" value="追加"/>								
有効	<input checked="" type="checkbox"/>								
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>									

非推奨のAPI削除

- ▶ 非推奨であったAPIが3.0で削除された

- ▶ ZBXNEXT-2724 : Remove the deprecated API features from 3.0

<https://support.zabbix.com/browse/ZBXNEXT-2724>

- ▶ 例 : (一部)

- ▶ action.exists、 host.exists、 host.getobjects、 item.exists、 item.getobjectsなど

Zabbix 3.0の応用

応用例 1 : 遠隔地監視

- ▶ Zabbix 3.0よりも前のバージョンの場合、遠隔地の監視を行う際には、やり取りするデータは暗号化せずに平文のままインターネット上でやりとりされていた。
- ▶ データの漏えいを防ぐためには、別途、通信を暗号化するものと組み合わせてインターネット上に流れるデータを暗号化する必要があった。
- ▶ Zabbix 3.0では、標準で通信を暗号化できるようになったので、別途、特別なものを用意して環境構築を行う必要がなくなった。

応用例 2 : 運用担当者ごとに画面カスタマイズ

- ▶ Zabbix 3.0よりも前のバージョンでは、マップやスクリーンを編集できるのは、「Zabbix特権管理者」か「Zabbix管理者」という特殊な権限を持ったユーザーしかできなかった。
- ▶ アクセスできるホストなどをサービス毎に分離して、それぞれのサービスごとに管理者を設けて運用させたくても、マップやスクリーンの作成は、特殊な権限を持った管理者しかできなかった。
- ▶ Zabbix 3.0からは、マップ、スクリーン、スライドショーを各ユーザーが作成し、共有することができるようになったので、各サービスの管理者が、より容易に自分たちにあった監視用の画面を作成できるようになった。

応用例 3 : サービス開始前チェック

- ▶ Zabbix 3.0よりも前のバージョンでは、1日に1回チェックするという指定はできたが、そのチェックを行う時刻を指定できなかった。
- ▶ Zabbix 3.0からは、特定の時刻にアイテムの値を取得することができるようになったので、営業日の毎朝9時にアクセスできる状態であるかをチェックするような設定ができるようになった。
- ▶ ただし、同時刻に多数のアイテムの値取得処理が集中してしまった場合、平行して値取得処理を行うのには限界がある（基本的には、取得するアイテムの種別用のPollerプロセスの数まで）ので、すべてのアイテムを同時に取得できずにキューに溜まってしまう場合があることに注意。

応用例 4 : ログから数値を取得し監視

- ▶ ログファイルに出力された、例えば、処理時間とか温度とかの値を正規表現で切り出して、数値としてグラフ化したり、トリガーで大小比較をすることができるようになった。
- ▶ つまり、既存のシステムで監視したい数値を含むログを出力する機能が用意されていれば、そこから正規表現を指定して切り出すことで、数値として監視し、グラフ化できるようになった。

まとめ

Zabbix 3.0によって

- ▶ 各コンポーネント間の通信を暗号化できるようになったので、通信の傍受による情報漏えいを標準の機能で防げるようになった。
- ▶ アイテムの値を取得するタイミングを柔軟にカスタマイズできるようになったので、様々な用途に利用できる可能性が高まった。
- ▶ 利用者ごとにカスタマイズできる範囲が広がったので、システム管理者に依存しなくても、よりそれぞれの運用に合わせたマップやスクリーンを作成して監視ができるようになった。

ご参考

- ▶ Zabbix 3.0.0リリースノート
 - ▶ <http://www.zabbix.com/rn3.0.0.php>
- ▶ What's New in Zabbix 3.0
 - ▶ http://www.zabbix.com/jp/whats_new.php
- ▶ Zabbix 3.0 Manual
 - ▶ <https://www.zabbix.com/documentation/3.0/manual>
- ▶ Zabbix 3.0をCentOS 7にインストール
 - ▶ <http://qiita.com/atanaka7/items/294a639effdb804cfdaa>

▶ ご清聴いただきありがとうございました。

✓ 本資料内で利用させて頂いた各プロダクト名やサービス名などは、各社もしくは各団体の商標または登録商標です。