MIRACLE ZBX / Zabbixトラブル事例あるある集
未修正の不具合や最新バージョンの機能＋
サポートに最近寄せられたホットな話題をご紹介！

Zabbix 4.0へ向けての新機能

ミラクル・リナックス株式会社
応用技術部
花島タケシ
2017年8月30日

自己紹介

- MIRACLE ZBXサポート担当
  - Zabbixソースコード調査
  - ドキュメント作成

サポート業務の紹介(1)

- 御客様の問い合わせに対する調査
  - ソースコード調査が基本

サポート業務の紹介(2)

- 数年来、業務形態の改善を行っています
  - 人員育成とか言えないこと
  - リリースされたソースコードの調査
    - LTS、ポイントリリースの両方
    - 社内用のドキュメント作成
  - 毎日SVN上のコミットも調査
    - 開発動向の調査
    - バックポートが必要であるものを抽出

新機能調査のソース

- Web上のリリースノート
  - https://www.zabbix.com/rn3.2.0
  - …
  - https://www.zabbix.com/rn3.4.0
- 3.2、3.4のドキュメント
  - https://www.zabbix.com/documentation/3.2/manual/introduction/whatsnew320
  - …
  - https://www.zabbix.com/documentation/3.4/manual/introduction/whatsnew340
- ソースコード中のChangeLogファイル

新機能調査のソース

- 一番有効なソースはソースコード

3.2.xのドキュメント

- 社外秘です

Zabbix-3.2.xにおける新規追加機能の調査報告書

本報告書は、3.2.xにおける新規追加機能を調査しまとめたものである。特に、Zabbix LLCがリリース毎に告示しているWebページを元から追加機能を抽出し、彼らが解説しているページとソースコード、及びバイナリの動作を検証し、作成を行った。
ただし、Webフロントエンドの追加部分やAPIについては調査を省略している。

3.4.xのドキュメント

- 社外秘です

Zabbix-3.4.xにおける新規追加機能の調査報告書

本報告書は、3.4.xにおける新規追加機能を調査しまとめたものである。特に、Zabbix LLCがリリース毎に告示しているWebページを元から追加機能を抽出し、彼らが解説しているページとソースコード、及びバイナリの動作を検証し、作成を行った。
ただし、Webフロントエンドの追加部分やAPIについては調査を省略している。

3.4.xのドキュメントの中

- 社外秘です

Webフロントエンド、APIに追加された部分については割愛する。

ソースコード調査からは、Alert ManagerプロセスとAlerterプロセスの通信は、珍しくDBを介さず、Unixソケット通信によって行われる。

以下がAlert Managerプロセスのメインループである。

```
src/zabbix_server/alerter/alert_manager.c
   for (;;)
   {
            time_now = zbx_time();
            now = time_now;

            DBへの接続確認
            プロセスタイトルの処理
            zbx_handle_log();
            DBを参照しアラートキューの更新(1秒おき)
            DBを参照しWatchdogアラートの更新(CacheUpdateFrequencyか15分の小さい方おき)
            DBが落ちている場合、その旨をアラートする(前回送信から15分経過している場合)

            /* アラートキューのチェックを行い、Alerterプロセスへ処理指示を送信 */
            while (SUCCEED == am_check_queue(&manager, now))
            {
                     if (NULL == (alerter = zbx_queue_ptr_pop(&manager.free_alerters)))
                              break;

                     if (FAIL == am_process_alert(&manager, alerter, am_pop_alert(&manager)))
                              zbx_queue_ptr_push(&manager.free_alerters, alerter);
            }
```

フロントエンドについて

- 3.2, 3.4でWebフロントエンドの印象は変わっていません

- 今までの経緯だと、x.0では変更されている
  - 4.0では…

3.2.xでの新機能(1)

- イベントタグの導入
  →3.4.0もチェック

  - トリガー設定画面にて
  - あるトリガー由来のイベントを区別可能
  - タグ中に{ITEM.VALUE}と{ITEM.LASTVALUE}マクロが使用可能
  - 正常時にクローズするイベントがタグで選択可能
  - タグによるイベント相関関係を作成可能

3.2.xでの新機能(2)

- 障害の手動クローズ
  これ自体は大したことはなかった

  - Task Managerプロセスの導入
  - 3.4.xで…

3.2.xでの新機能(3)

- バーストするログへの対策
  処理限界量を超えた出力を何秒間まで許容するか？というオプション

  - log[], logrt[]キーにmaxdelayオプション
  - 3.4.xでさらに!
  - log.count[], logrt.count[]キーも導入された
  - 大量生成されるイベントを抑えるためのもの
    - 生成される大量のイベントを処理する側は？
      - 3.0.xでEscalatorプロセスのマルチ化
      - 3.4.xで…

3.2.xでの新機能(4)

- vm.vmemory.size[]キー
  - Windows用
  - 仮想メモリ監視の改善
  - 今までの監視キー(vm.memory.size[])はいまいちだった

3.2.xでの新機能(5)

- その他代表的なもの
  - それぞれの障害イベントに対する独立したエスカレーション
  - マクロの値のカスタマイズ
    - マクロ関数 regsub(), iregsub()
    - {ITEM.VALUE}と{ITEM.LASTVALUE}に可能
  - ヒステレシストリガー式の簡素化
  - Webシナリオのエクスポート/インポート
  - 取得不可アイテムに対するnodata()関数
  - 正常イベントへ障害対応コメント入力ができなくなった

3.2.xでの新機能(6)

- その他代表的なもの(その2)
  - count()トリガー関数に第三引数
    - regexpとiregexp
  - VMware監視でデータセンター名の追加
    - vmware.hv.datacenter.name, vmware.vm.datacenter.name

3.4.xでの新機能(1)

- マップ
  - 新しい要素
  - ヴェクトルレンダリング
  - スクリーンとマップのフルクローン
  - エディタの操作性の向上
  - トリガーマップエレメント上で複数のトリガー

3.4.xでの新機能(2)

- 正規表現をPCREに統一
  - さようなら POSIX拡張正規表現
  - Webフロントエンドのテストは既にPCRE
  - grep -P でテスト可能
  - . と * の用法は間違えずに！

3.4.xでの新機能(3)

- プロキシ経由でのリモートコマンド
  - Task Managerプロセス経由で実行
  - Zabbixサーバプロセスの実装も変更

3.4.xでの新機能(4)

- 障害対応済みを通知(アクション実行)
  - Task Managerプロセス経由
  - 3.2.xで正常イベントに対しては障害対応入力が不可

3.4.xでの新機能(5)

- アラート処理の並列化
  - Alert Managerプロセスの導入
  - Alert ManagerプロセスとAlerterプロセスの通信は、UNIXソケット通信
    - IPCの実装が整備された
    - 他にも…
  - バーストログに対する対策かな～と
  - ちょっとアルゴリズム的に怪しい感じも
    - ZBXNEXT-3782

3.4.xでの新機能(6)

- IPMI監視の効率化
  - IPMI Managerプロセスの導入
  - IPMI ManagerプロセスとIPMI Pollerプロセスの通信は、UNIXソケット通信
  - IPMI Pollerプロセスの対象を固定するように

3.4.xでの新機能(7)

- 監視データ保存前に変換処理
  - Preprocessing ManagerプロセスとPreprocessing Workerプロセスの導入
  - Preprocessing ManagerプロセスとPreprocessing Workerプロセスの通信は、UNIXソケット通信
  - 今までも*差分*、*差分/時間*は可能であった
  - これらを導入したことによりBulk監視も導入された
    - XML, JSON, CVS等をパーズして...
  - これについてはまだ調査不十分です

3.4.xでの新機能(8)

- イベントタグへホスト関連マクロとインターフェイスマクロの追加
  - 3.2.0で追加されたイベントタグ
    - {ITEM.VALUE}と{ITEM.LASTVALUE}だけだった
  - 3.4.0で下記が追加された
    - {HOST.ID}, {HOST,HOST}, {HOST.NAME}
    - {HOST.DNS}, {HOST,IP}, {HOST.PORT}, {HOST.ID}

3.4.xでの改善点(9)

- その他代表的なもの
  - JMX監視のエンドポイント
    - 今まではほぼ固定。監視できない対象も多数。
  - JMX監視用のLLDアイテム
    - jmx.discoveryo[]キーが実装された
    - 今まではガワだけ
  - ディレクトリサイズ監視アイテム
    - vfs.dir.size[]キー
  - MaxLinesPerSecondパラメータの効果(4→10)
    - 3.2.0の修正(maxdelay引数)との兼ね合いも
  - ホストインターフェイス探索用LLDアイテム
    - zabbix[host,discovery,interfaces]

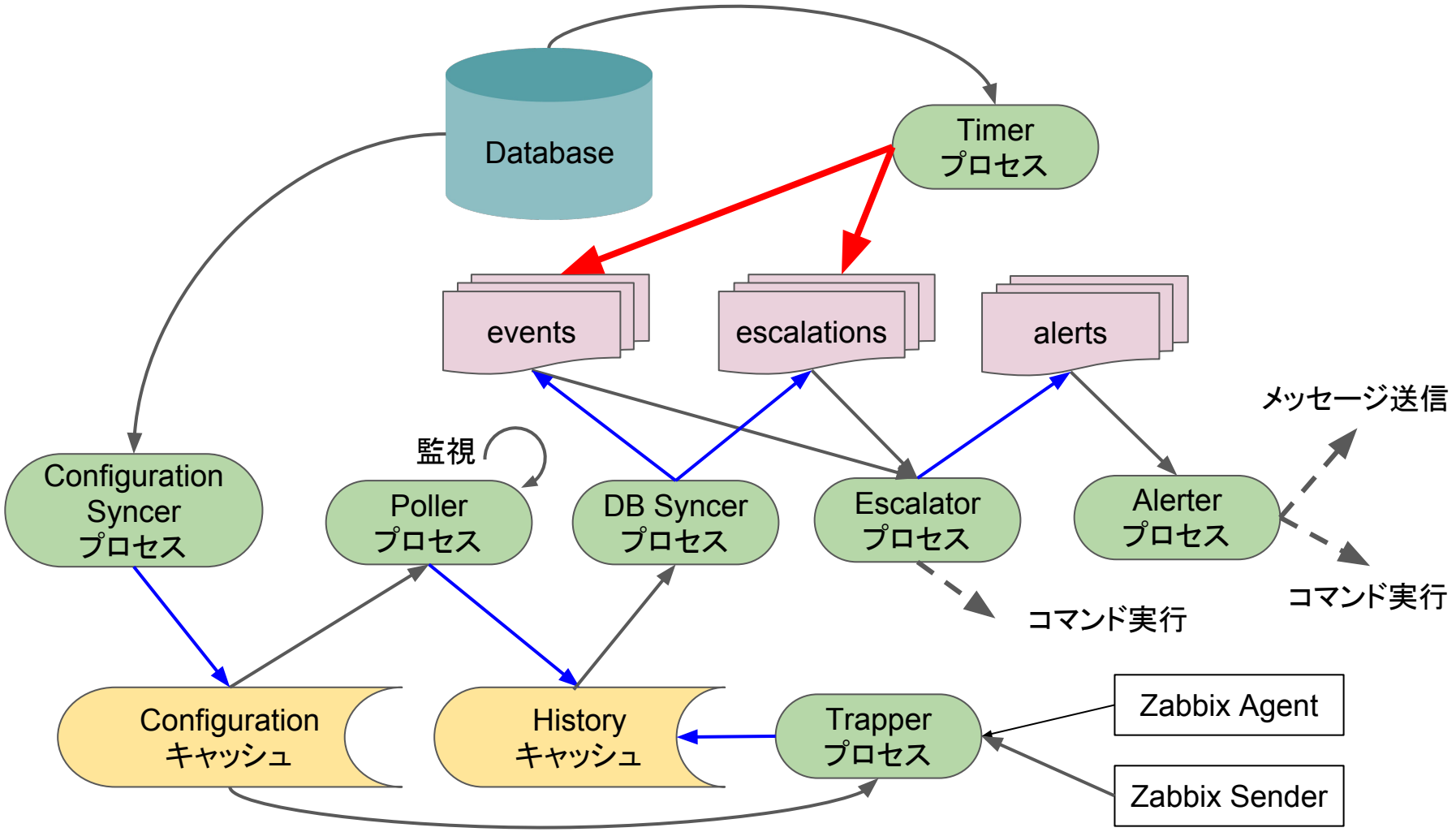
3.4.xでの改善点(10)

- その他代表的なもの(その2)
  - Web監視でURLエンコードとプニュコード
  - CIDRサブネットマスク表記のサポート
    - エージェントのServerパラメータ
  - IE9とIE10はサポートされなくなりました

Task Managerプロセスって？

- 3.2.0から導入
- 現在の処理はこちら
  - 手動クローズした障害の後処理
  - リモートコマンドの実行
  - 障害対応済みを通知
- 通常監視とは独立したプロセス
- taskテーブルをポーリングして適宜処理

監視プロセスの連携



プロセス間通信の改善？

- 今まではプロセス間で直接通信することはなかった
  - DBを介していました
    - DBのパフォーマンスが重要！
    - 仮想マシンで…
- UNIXソケットによる通信の整備
  - 現在は3つ(Alerter, IPMI, Preprocessor)
  - 今後のバージョンで増えることはある？
    - おそらく既存プロセスの仕組みは変えないかと

質問タイム

【お問い合わせ先】
info@miraclelinux.com
http://www.miraclelinux.com