cybertrust

Zabbix ログ解析方法

2018/2/14

サイバートラスト株式会社
Linux/OSS事業部
技術統括部
花島タケシ

Zabbix ログ解析方法

サイバートラスト株式会社
Linux/OSS事業部
技術統括部
花島 タケシ

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(当社ブログも執筆)
  - ときどき新規機能追加もしたりします
    - 4.0へ向けての機能紹介等(ブログ)
    - 社内向のドキュメント

Zabbixって?

- Zabbixについて多くの方が勘違いしています!

Zabbixは

- 監視に失敗したことを詳細に調査できるツールではありません。

なぜか? というと

- 詳細の99%がログに出力されません!

当社への問い合わせも結構ありますが…

無理なものは無理です!

では、どんなものなのでしょう?

- (失敗も含めて)監視により得られたデータからどうするか?を決める(考える)ためのツールです。

でも…

- 解析とかバグ調査とかできないと困るよね～

なにはともあれ

- DebugLevel=4のログを取得しないと始まりません。

DebugLevel=4の設定方法

- zabbix_server.conf, zabbix_agentd.conf, zabbix_proxy.conf に設定する。

これだと全部のプロセスに影響が出てしまいます。

局所的にDebugLevel=4で取得するには?

- MIRACLE ZBX 2.2までは?

サービス起動後、設定ファイルにDebugLevel=4と記述して下記を実行

kill -HUP <PID>

各サービスのPIDはログから判断する。

注意) Windowsではできません。

設定を戻すことを忘れないようにしましょう。

/sbin/service zabbix_server reload とすると、サービスを再起動することなく、DebugLevelを変更できます。

ログからPIDの判別

```
30449:20180208:121535.686 Starting Zabbix Server. Zabbix 2.2.17-4 (revision 65977).
...
30449:20180208:121535.686 using configuration file: /etc/zabbix/zabbix_server.conf
30449:20180208:121535.716 current database version (mandatory/optional): 02020000/02020001
30449:20180208:121535.716 required mandatory version: 02020000
30453:20180208:121535.783 server #2 started [db watchdog #1]
30452:20180208:121535.783 server #1 started [configuration syncer #1]
30460:20180208:121535.785 server #9 started [trapper #1]
30463:20180208:121535.795 server #10 started [trapper #2]
30464:20180208:121535.796 server #11 started [trapper #3]
30465:20180208:121535.796 server #12 started [trapper #4]
30469:20180208:121535.814 server #13 started [trapper #5]
30471:20180208:121535.820 server #15 started [alerter #1]
30470:20180208:121535.885 server #14 started [icmp pinger #1]
30474:20180208:121536.627 server #16 started [housekeeper #1]
30475:20180208:121536.632 server #17 started [timer #1]
30476:20180208:121536.632 server #18 started [http poller #1]
30478:20180208:121536.648 server #20 started [history syncer #1]
30479:20180208:121537.557 server #21 started [history syncer #2]
30482:20180208:121538.525 server #22 started [history syncer #3]
```

ログからPIDの判別(その2)

cybertrust

```
$ ps ax|grep zabbix_server
29343 ?      S      0:00 /usr/sbin/zabbix_server -c /etc/zabbix/zabbix_server.conf
29348 ?      S      0:53 /usr/sbin/zabbix_server: configuration syncer [synced configuration in 0.005622 sec,
idle 60 sec]
29349 ?      S      0:05 /usr/sbin/zabbix_server: alerter #1 [sent 0, failed 0 alerts, idle 51.232104 sec during
53.320830 sec]
29350 ?      S      0:00 /usr/sbin/zabbix_server: alerter #2 [sent 0, failed 0 alerts, idle 27.074403 sec during
30.558192 sec]
29351 ?      S      0:00 /usr/sbin/zabbix_server: alerter #3 [sent 0, failed 0 alerts, idle 12.399095 sec during
14.518400 sec]
29352 ?      S      0:19 /usr/sbin/zabbix_server: housekeeper [deleted 0 hist/trends, 0 items/triggers, 0
events, 0 sessions, 0 alarms, 0 audit items in 0.038855 sec, idle for 1 hour(s)]
29353 ?      S      0:31 /usr/sbin/zabbix_server: timer #1 [processed 1 triggers, 0 events in 0.000566 sec, 0
maintenances in 0.000496 sec, idle 29 sec]
29354 ?      S      0:27 /usr/sbin/zabbix_server: http poller #1 [got 0 values in 0.000609 sec, idle 5 sec]
29355 ?      S      0:27 /usr/sbin/zabbix_server: discoverer #1 [processed 0 rules in 0.000671 sec, idle 60
sec]
29356 ?      S      1:03 /usr/sbin/zabbix_server: history syncer #1 [synced 0 items in 0.000001 sec, idle 1
sec]
```

MIRACLE ZBX 3.0からは?

- Zabbix標準の機能(Runtime Control)で行える。
  サービス起動後、-R log_level_increaseを実行する。
  デーモンに引数付シグナルが送られる。

```
$ /usr/sbin/zabbix_server --help
…
  -R --runtime-control runtime-option   Perform administrative functions
…
        log_level_increase=target  Increase log level, affects all processes if
                                   target is not specified
        log_level_decrease=target  Decrease log level, affects all processes if
                                   target is not specified

        Log level control targets:
        pid                Process identifier
        process-type             All processes of specified type (e.g., poller)
        process-type,N           Process type and number (e.g., poller,3)
```

デバッグログを取得しても…

- 色々なプロセスのログがごちゃごちゃしてて解析が難しいです!

  当社でプロセスごとにログを切り分けるツールを配布中!
  https://www.miraclelinux.com/tech-blog/ff5adp

デバッグログを取得しても…

cybertrust

```
2273:20180213:123132.288 In zbx_preprocess_item_value()
2273:20180213:123132.288 End of zbx_preprocess_item_value()
2273:20180213:123132.288 In zbx_ipc_socket_write()
2273:20180213:123132.288 End of zbx_ipc_socket_write():SUCCEED
2273:20180213:123132.288 End of get_values():1
2273:20180213:123132.288 __zbx_zbx_setproctitle() title:'poller #5 [got 1 values in 0.000434 sec, idle 1
sec]'
2298:20180213:123132.288 End of zbx_ipc_service_recv():1
2298:20180213:123132.288 In preprocessor_add_request()
2298:20180213:123132.288 In preprocessor_sync_configuration()
2298:20180213:123132.288 In DCconfig_get_preprocessable_items()
2298:20180213:123132.288 End of DCconfig_get_preprocessable_items() items:40
2298:20180213:123132.288 End of preprocessor_sync_configuration() item config size: 40, history cache
size: 3
2298:20180213:123132.288 In preprocessor_enqueue() itemid: 23252
2298:20180213:123132.288 In preprocessor_enqueue_dependent() itemid: 23252
2298:20180213:123132.288 End of preprocessor_enqueue_dependent()
2298:20180213:123132.288 End of preprocessor_enqueue()
```

デバッグログを取得した後は

- 現象とログをつき合わせる。
- ソースコードと照らし合わせる。
  - DebugLevel=4のログは、ほとんどが関数の出入りが記される。
  - src/zabbix_server 以下はプロセスごとにディレクトリが分かれている。
    - $ ls src/zabbix_server/

```
Makefile.am  actions.h  dbsyncer  events.c   httppoller  pinger       scripts.c  server.c      trapper
Makefile.in  alerter    discoverer events.h   operations.c poller      scripts.h  snmptrapper   vmware
actions.c    dbconfig   escalator  housekeeper operations.h proxypoller selfmontimer          watchdog
```

使用しているのはZabbixだけど…

- 問題解決には他の知識も必要です。
  - OS
    - プロセスはどう動く?
    - TCP/IP, UDP通信はどのように?
  - DB
    - ロックとは?
  - ライブラリ
    - net-snmp
    - libcurl
  - 正規表現

DebugLevel=4の問題点

- 当然ファイルへの出力が増えます(容量の問題)。
- OS I/Oが増えます(CPUの問題)。
  - 解析する上で避けようがありません。

出力される問題は以前解決しようとした。

→ 通常のログファイルとは別に、専用のストレージに書き出す機能

いや、ちょっと待て！

- それ本当に障害なの？
  - まずはマニュアルを読みましょう。
  - Zabbix LLCのマニュアルには大抵書かれています。
  - 下記はちょっと…

https://www.zabbix.com/documentation/3.0/manual/config/triggers

Trigger status (the expression) is recalculated every time Zabbix server receives a new value that is part of the expression.

If time-based functions (**nodata()**, **date()**, **dayofmonth()**, **dayofweek()**, **time()**, **now()**) are used in the expression, the trigger is recalculated every 30 seconds by a Zabbix *timer* process. If both time-based and non-time-based functions are used in an expression, it is recalculated when a new value is received **and** every 30 seconds.

ここから余談です。

よくある問い合わせ(1)

- ログが大量出力された。アラートを止めたい。
  - Zabbix標準の機能ではできません!
    データベースを直接操作する。
  - 4.0では特定のアラートを全て破棄する機能を開発しました。
  - 3.0にも実装しようかな～

よくある問い合わせ(2)

- logrt[]キーに設定したログの読み返しが発生した。
  - 大体の原因は正規表現の誤りです。
    - 設定によりロックファイルを読み込みます。
  - サイズが変更されずmtimeだけが変更されたときも該当します。

cybertrust

信頼とともに

ソフトバンク・テクノロジーグループ

ソフトバンク・テクノロジー

エムソリューションズ

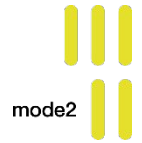
フォントワークス

環

サイバートラスト

アソラテック

リデン



モードツー

公開