日本国内における
よくある問い合わせと対応
(令和Ver.)

ZABBIX 2019
Conference
JAPAN

Kazuhiro Mizutani
ZABBIX Support Engineer

#ZabConfJp2019

Agenda

1. CVE-2019-15132
2. CVE-2019-17382
3. グラフプレビュー表示不具合
4. ログファイルの読み直し
5. トリガーが正しく検知されない

CVE-2019-15132

CVE-2019-15132

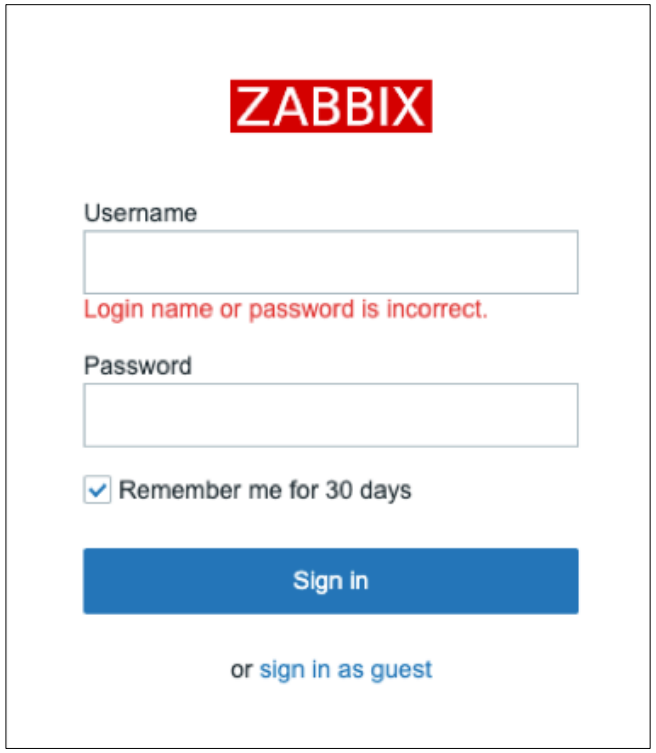
- Zabbix Webインターフェース、または、Zabbix APIでのログイン操作の際、存在するユーザー名でパスワードを繰り返し(5回)間違えると「Account is blocked for 30 seconds.」と表示され、ユーザー名が存在することを確認できてしまう。

- CVE-2019-15132　　：https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15132
- JVNDB-2019-008547：https://jvndb.jvn.jp/ja/contents/2019/JVNDB-2019-008547.html

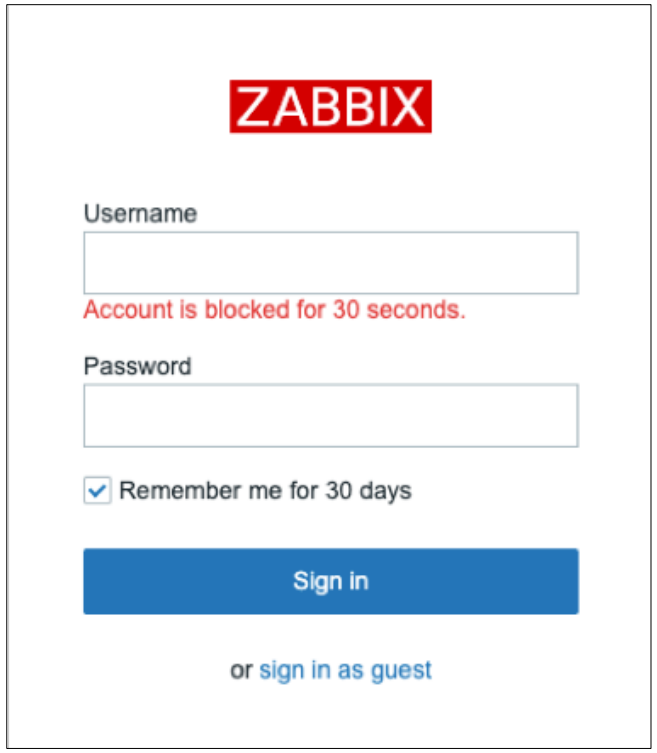
CVE-2019-15132

- Zabbix Webインターフェース

1～4回目



5回目

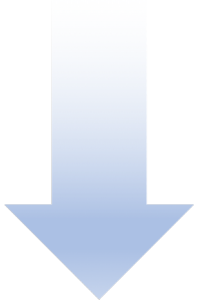


CVE-2019-15132

- Zabbix API (user.login method)

1～4回目

```
$ curl -d '{"auth":null, "method":"user.login", "id":1, "params":{"user":"Admin", "password":"xxxxx"}, "jsonrpc":"2.0"}' -H "Content-Type: application/json-rpc" http://127.0.0.1/zabbix/api_jsonrpc.php
{"jsonrpc":"2.0","error":{"code":-32500,"message":"Application error.","data":"Login name or password is incorrect."},"id":1}
```



5回目

```
$ curl -d '{"auth":null, "method":"user.login", "id":1, "params":{"user":"Admin", "password":"xxxxx"}, "jsonrpc":"2.0"}' -H "Content-Type: application/json-rpc" http://127.0.0.1/zabbix/api_jsonrpc.php
{"jsonrpc":"2.0","error":{"code":-32500,"message":"Application error.","data":"Account is blocked for 30 seconds."},"id":1}
```

CVE-2019-15132

- [ZBX-5842]　：https://support.zabbix.com/browse/ZBX-5842
  - Status: REOPENED

- [ZBX-16532]　：https://support.zabbix.com/browse/ZBX-16532
  - Status: CLOSED (Closed as duplicate of ZBX-5842.)

緊急度が高いものではないと判断しており、
対応については検討中

CVE-2019-15132

- 運用での対応
  - アクセス可能なIPアドレスを制限する
  - パスワードを強固にする
  - パスワードを使いまわさない

CVE-2019-17382

CVE-2019-17382

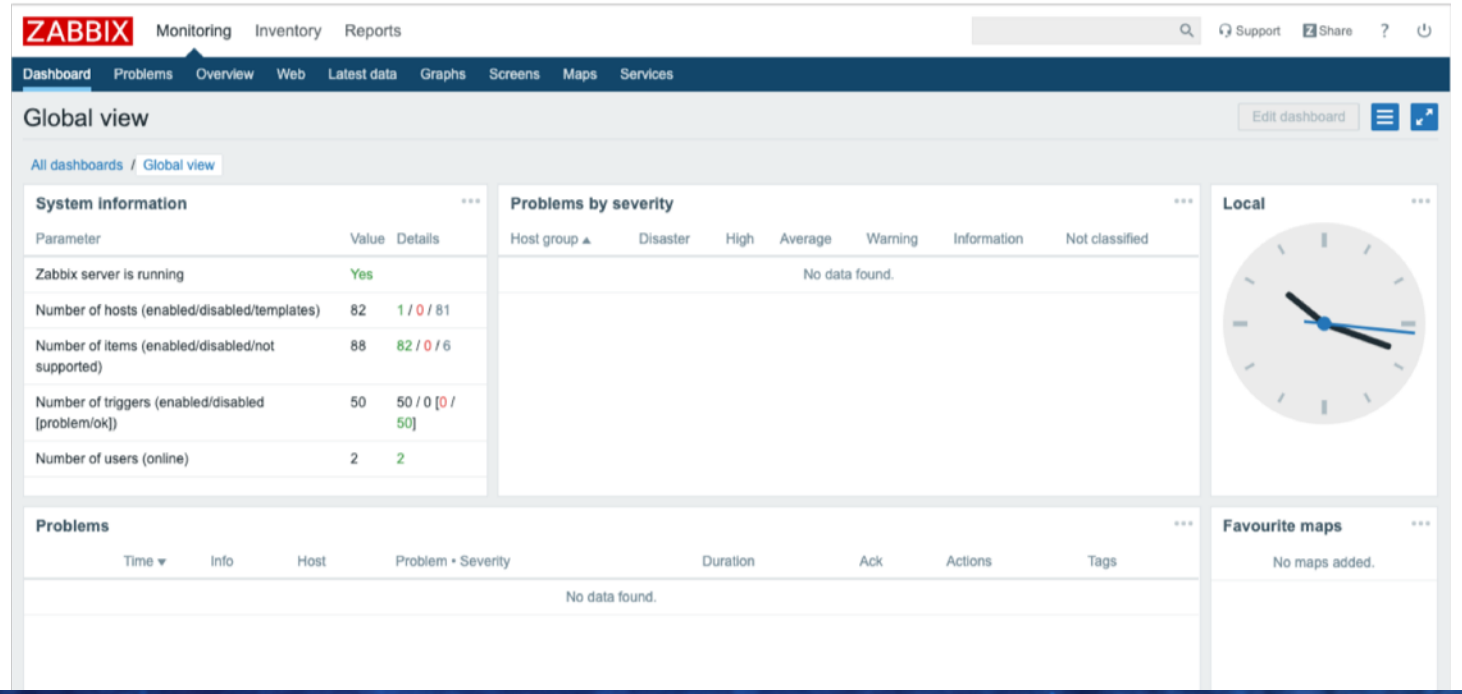
- 「http://xxx.xxx.xxx.xxx/zabbix/zabbix.php?action=dashboard.view&dashboardid=1」にアクセスすると、ログインページをバイパスしてダッシュボードにアクセスし、ユーザー名/パスワード無しでダッシュボード、スクリーン、マップを作成することができてしまう。

- CVE-2019-17382　　：https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17382
- JVNDB-2019-010760：https://jvndb.jvn.jp/ja/contents/2019/JVNDB-2019-010760.html

CVE-2019-17382

- 「dashboardid=1」はデフォルトダッシュボード「Global view」
- 「Global view」の共有のタイプのデフォルト設定は「公開」
- 「guest」ユーザーはダッシュボード「Global view」へアクセスすることが可能

- ただし、権限がないため、監視データの閲覧は不可



CVE-2019-17382

- [ZBX-16789] ：https://support.zabbix.com/browse/ZBX-16789
  - Status: CLOSED

- [ZBX-16765] ：https://support.zabbix.com/browse/ZBX-16765
  - Status: CLOSED

意図している動作(仕様)であり、
セキュリティの問題ではありません

CVE-2019-17382

- 「Global view」へのアクセスを許可しない方法(1)
  - ユーザーグループ「Guests」のステータスを無効にする

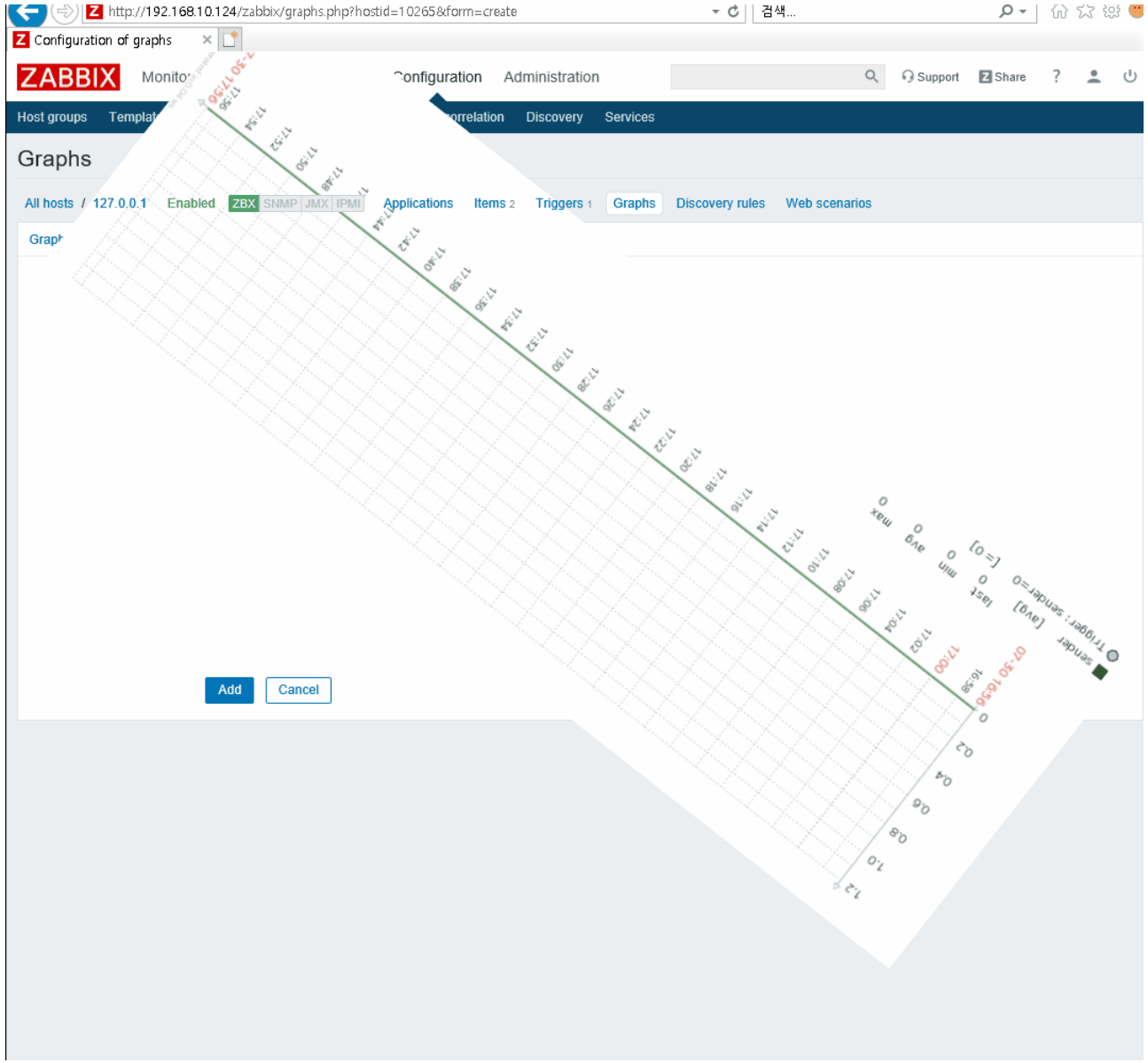
CVE-2019-17382

- 「Global view」へのアクセスを許可しない方法(2)
  - 「Global view」の共有のタイプを「非公開」にする

グラフプレビュー表示不具合

グラフプレビュー表示不具合

ホストにグラフを作成または変更を行おうとした際に、プレビュータブを開くとグラフが回転してしまうのですが...


http://192.168.10.124/zabbix/graphs.php?hostid=10265&form=create
Configuration of graphs
ZABBIX
Configuration
Administration
Support
Share
Host groups
Discovery
Services
Graphs
All hosts / 127.0.0.1
Enabled
ZBX SNMP JMX IPMI
Applications
Items 2
Triggers 1
Graphs
Discovery rules
Web scenarios
Add
Cancel

グラフプレビュー表示不具合

- 再現方法
  - 環境
    - Zabbix 4.0.13未満
    - Internet Explorer 11 (11.615.17763.0)

  - 手順
    1. 「設定」→「テンプレート」or「ホスト」→「グラフ」をクリックします。
    2. 設定を変更できるグラフを選択します。
    3. 「プレビュー」タブに移動し、「グラフ」タブに戻ります。
    4. 「トリガーの表示」設定を変更します。
    5. 「プレビュー」タブに移動します。

グラフプレビュー表示不具合

- [ZBX-16435]　：https://support.zabbix.com/browse/ZBX-16435
- 修正バージョン：Zabbx 4.0.13, 4.2.7, 4.4.0

ログファイルの読み直し

ログファイルの読み直し

ログの読み直しが発生しました...

ログファイルの読み直し

- ログファイルの読み直しが発生する原因
  - Zabbixエージェントのバージョンが低い(Zabbixのバグ)
  - logrtキーのパラメータ(正規表現)が正しくない
  - 非対応のローテーション方式のログファイルを監視している
  - **mtimeのみ更新されるログファイルを監視している**

ログファイルの読み直し

- [ZBX-7098]　：https://support.zabbix.com/browse/ZBX-7098
- 修正バージョン：Zabbx 2.0.13, 2.2.4
- ログローテーション時のログファイルの読み直し改善のために、ログ監視のファイル追跡処理を改善。
- この修正により、ログファイルに「**mtimeのみが更新され、ファイルサイズに変更がない**」場合にログファイルを先頭から読み直す処理が追加。
  ※ログファイルに新規に行が追記された場合は必ずmtimeとファイルサイズが更新されることを前提に、この状態はログファイルが期待しない状態になっていると想定。

※Zabbix Enterpriseサポートご契約者様向けナレッジベース [KB-649] https://enterprise.zabbix.co.jp/knowledgebase/649

ログファイルの読み直し

- Linuxのファイルシステムではmtimeとファイルサイズが厳密には同時に更新されず、僅かな時間差でmtimeが先に更新されることが判明。
- 以下の処理順となった場合、Zabbixエージェントがログファイルの状態を確認した際にログファイルの先頭から読み直してしまう事象を確認された。
    1. アプリケーションがログファイルを追記する
    2. Linuxカーネルがファイルのmtimeを更新する
    3. Zabbixエージェントがログファイルを読む
    4. Linuxカーネルがファイルサイズを更新する

※Zabbix Enterpriseサポートご契約者様向けナレッジベース [KB-4308] https://enterprise.zabbix.co.jp/knowledgebase/4308

ログファイルの読み直し

- [ZBX-9290]　：https://support.zabbix.com/browse/ZBX-9290
- 修正バージョン：Zabbx 2.0.15, 2.2.10
- ログの読み直し処理を改善し、mtimeが異なりファイルサイズが同一の場合は、時間を置いてファイルのステータスを再チェックする。
  - 再チェックでmtimeが異なりファイルサイズが増加している場合は、ログファイルを追記分から読み込む。
  - 再チェックでmtimeが異なりファイルサイズが同一の場合は、別ファイルとしてファイルを先頭から読み込む。

※Zabbix Enterpriseサポートご契約者様向けナレッジベース [KB-4308] https://enterprise.zabbix.co.jp/knowledgebase/4308

ログファイルの読み直し

- [ZBX-9290]　：https://support.zabbix.com/browse/ZBX-9290
- 修正バージョン：Zabbx 2.0.15, 2.2.10
- 1回目のチェックでファイルサイズに変更がなく、mtimeのみが更新されたログファイルを検知した場合、zabbix_agentd.logに以下のメッセージを出力します。

the modification time of log file xxx has been updated without changing its size, try checking again later

※Zabbix Enterpriseサポートご契約者様向けナレッジベース [KB-4308] https://enterprise.zabbix.co.jp/knowledgebase/4308

ログファイルの読み直し

- [ZBX-9290]　：https://support.zabbix.com/browse/ZBX-9290
- 修正バージョン：Zabbx 2.0.15, 2.2.10
- 2回目のチェックでファイルサイズに変更がなく、mtimeのみが更新されたログファイルを検知した場合、zabbix_agentd.logに以下のメッセージを出力し、別ファイルとして先頭からログファイルを読み込みます。

after changing modification time the size of log file xxx still has not been updated, consider it to be a new file

※Zabbix Enterpriseサポートご契約者様向けナレッジベース [KB-4308] https://enterprise.zabbix.co.jp/knowledgebase/4308

ログファイルの読み直し

- log, logrtキーを利用してログ監視を行っており、「**エージェントがログファイルを読んだタイミングで、2回連続mtimeのみ更新され、ファイルサイズが変わらない**」場合にログファイルの読み直しが発生する。
- 同じログファイルであるにも関わらず、上記の問題が発生する場合の対応、回避策は以下の通りとなります。
  - ログを出力しているアプリケーションでmtimeのみ更新するログの出力が行われている場合は、アプリケーション側でログ出力方法を改善する。
  - ログ監視アイテムの監視間隔が短い場合は、監視間隔を長くする。
  - カスタマーポータル版Zabbixエージェント(※利用にはZabbix Enterpriseサポート契約が必要となります)を利用する。

※Zabbix Enterpriseサポートご契約者様向けナレッジベース [KB-11947] https://enterprise.zabbix.co.jp/knowledgebase/11947

ログファイルの読み直し

- カスタマーポータル版Zabbixエージェント
  - Zabbix Enterpriseサポート契約ユーザー向けに提供
  - 公式リポジトリ版より対応OSが多い
  - マイナーバージョンで影響頻度が高い不具合に対する対処パッチの先行取り込み
  - **日本独自の修正**
    - ✓日本でよく利用されているアプリケーションで問題報告が多いため、「mtimeのみ変更された場合にログを読み直す」動作を行わないように修正 (Zabbix 3.0.29, 4.0.10以降)
  - その他、パッケージ作成に関わる修正

トリガーが正しく検知されない

トリガーが正しく検知されない

- [ZBX-12957] ：https://support.zabbix.com/browse/ZBX-12957
- 修正バージョン：Zabbix 4.0.0
- Zabbix 3.4以前のZabbixサーバおよびZabbixプロキシは、時刻付きの監視データが送信されてきた場合に監視データの時刻調整を行う機能を有しています。
  Zabbix 4.0以降は時刻調整を行わなくなり、監視対象のOSの時刻が正しくない場合に期待通りに動作しない場合があります。

※Zabbix Enterpriseサポートご契約者様向けナレッジベース [KB-11041] https://enterprise.zabbix.co.jp/knowledgebase/11041

トリガーが正しく検知されない

- [ZBX-12957] ：https://support.zabbix.com/browse/ZBX-12957
- 修正バージョン：Zabbix 4.0.0
- Zabbix 3.4以前の動作
  - Zabbixは以下の通信を行う際に監視データ自体とは別に送信元のOSの時刻情報を含めてデータを送信しており、 Zabbixサーバまたは Zabbixプロキシでは時刻を差を調整してトリガー評価やデータベースへの保存を行います。
    - Zabbixエージェント(アクティブチェック) → ZabbixサーバまたはZabbixプロキシ
    - zabbix_senderコマンド → ZabbixサーバまたはZabbixプロキシ
    - Zabbixプロキシ → Zabbixサーバ

※Zabbix Enterpriseサポートご契約者様向けナレッジベース [KB-11041] https://enterprise.zabbix.co.jp/knowledgebase/11041

トリガーが正しく検知されない

- [ZBX-12957]　：https://support.zabbix.com/browse/ZBX-12957
- 修正バージョン：Zabbix 4.0.0
- Zabbix 4.0以降では下記の理由から時刻調整処理を行わないように変更されています。
  - Zabbixサーバ側で受信処理タイムラグが発生するとnsレベルで本来出力された時系列順と異なった順番となり、正しくトリガーの判定が行われない場合があった。
  - Zabbixプロキシを利用している場合に、Zabbixプロキシ受信時とZabbixサーバ受信時の2回の時刻調整が行われるために、監視データの時刻に関連して想定しない問題が発生する場合があった。

※Zabbix Enterpriseサポートご契約者様向けナレッジベース [KB-11041] https://enterprise.zabbix.co.jp/knowledgebase/11041

トリガーが正しく検知されない

- Zabbixエージェントの時刻がZabbixサーバの時刻よりも秒単位で進んでいる場合、かつ、 ValueCache上に該当アイテム情報が存在しない場合※、データがValueCacheに展開されず、過去のデータが参照される場合がある。

※前回の該当データへのアクセスから24時間が経過している場合、または、Zabbixサーバの再起動を行なっている場合

トリガーが正しく検知されない

- 本問題による影響
  - トリガーが正しく検知されない
    - 過去のデータを参照してしまうため、トリガー条件式が真にならず、障害イベントが生成されない
  - マクロが正しく展開されない
    - 過去のデータを参照し、{ITEM.VALUE}等のマクロが過去のデータとして展開されてしまう

トリガーが正しく検知されない

- [ZBX-16754] ：https://support.zabbix.com/browse/ZBX-16754
- 修正バージョン：Zabbx 4.0.14, 4.2.8, 4.4.1

Zabbix/src/libs/zbxdbcache/valuecache.c

```
1891 1891      if (0 != item->db_cached_from && range_start >= item->db_cached_from)
1892 1892          return SUCCEED;
1893 1893
1894 1894      /* find if the cache should be updated to cover the required range */
1895 1895      if (NULL != item->tail)
1896 1896      {
1897 1897          /* we need to get item values before the first cached value, but not including it */
1898 1898          range_end = item->tail->slots[item->tail->first_value].timestamp.sec - 1;
1899 1899      }
1900 1900      else
1901      -          range_end = time(NULL);
     1901 +          range_end = ZBX_JAN_2038;
1902 1902
1903 1903      /* update cache if necessary */
1904 1904      if (range_start < range_end)
```

Zabbix/include/common.h

```
1056 #define ZBX_JAN_2038        2145916800
```

2145916800 = 2038/01/01 00:00:00 (UTC)

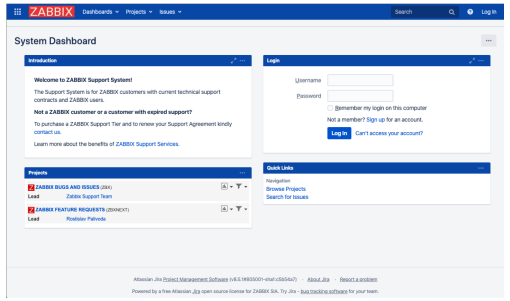
$(2^{31} - 1)$ = 2147483647 = 2038/01/19 03:14:07 (UTC)

ValueCacheへのデータの展開を現在時刻迄ではなく、
ZBX_JAN_2038(2038/01/01 00:00:00 (UTC))迄に変更

おわりに

おわりに

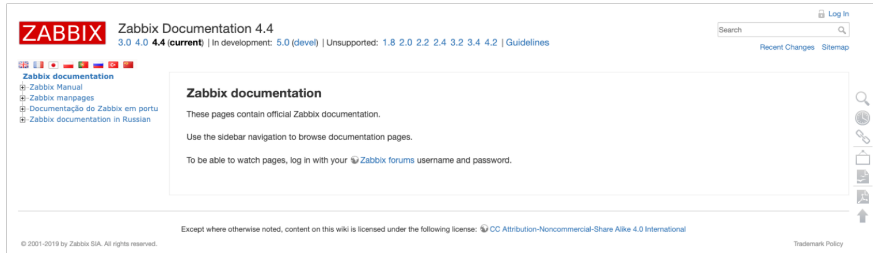
- Bug Ticket System
  https://support.zabbix.com/



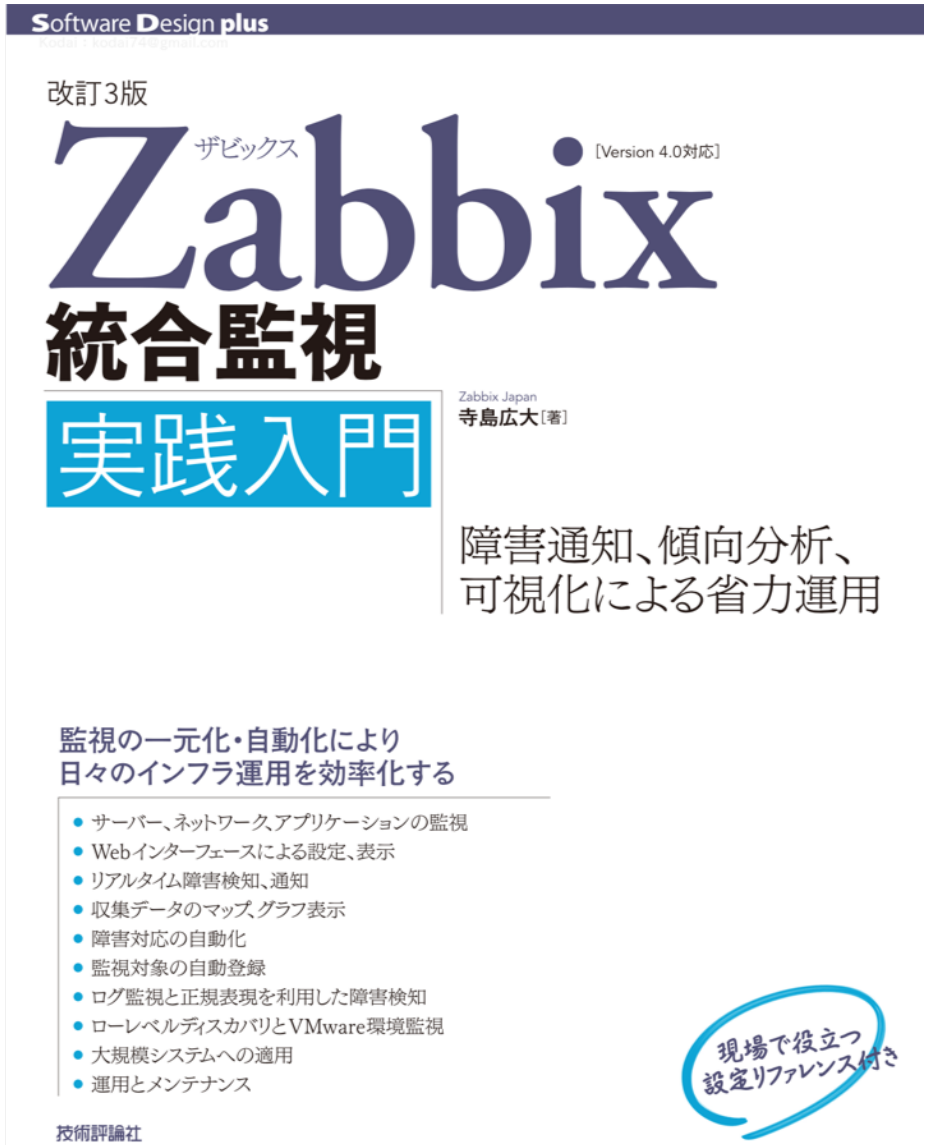
- Zabbix Enterprise カスタマーポータル
  https://enterprise.zabbix.co.jp

  ※カスタマーポータル版インストールパッケージのダウンロード、ナレッジベースの閲覧等には
  Zabbix Enterpriseサポート契約が必要となります。

- Zabbix documentation
  https://www.zabbix.com/documentation



おわりに


Software Design plus
改訂3版
ザビックス
Zabbix
[Version 4.0対応]
統合監視
実践入門
Zabbix Japan
寺島広大[著]
障害通知、傾向分析、
可視化による省力運用
監視の一元化・自動化により
日々のインフラ運用を効率化する
サーバー、ネットワーク、アプリケーションの監視
Webインターフェースによる設定、表示
リアルタイム障害検知、通知
収集データのマップ、グラフ表示
障害対応の自動化
監視対象の自動登録
ログ監視と正規表現を利用した障害検知
ローレベルディスカバリとVMware環境監視
大規模システムへの適用
運用とメンテナンス
現場で役立つ
設定リファレンス付き
技術評論社

THANK YOU

ZABBIX 2019
Conference
JAPAN

#ZabConfJp2019