Zabbix and Elastic

Elastic as history storage back-end

ZabConf BeNeLux 01-02-2019
$ whoami

gecos: Robert Hoekstra
jobtitle: Linux and Zabbix Consultant
Org: Xifeo ICT
Special1: Zabbix Certified Professional (6+ yrs)
Special2: Red Hat Certified Architect (9+ yrs)
Why This Topic

• Unfamiliar with Elastic
• Intrigued by the support for it since 3.4
• Experimenting
• Sharing my experiences so far
Elastic Content

• Current Database Back-End Setup
• About Elastic
• Zabbix and Elastic as History Back-End
• Current Install - Migrate or Not
• How to set up
• What’s Next
• Questions
Current Database Back-End Setup

- Structured databases, they do have their limits
  - History Housekeeping needed, or
  - Partitioning

- Typically a single server storing and servicing the data
  - Scales vertically (more CPU / Memory)

- Replication / back-up must be arranged for HA/DR
  - Often relying on 3rd party solutions like VM- or volume snapshots

- Database needs tweaking to increase performance/efficiency
About Elastic

• NoSQL
• Unstructured data store
• JSON RESTful API
• Scalable – Distributed by nature
  • Hardware fault tolerant because of replication
  • No single node to query
• Free, but with limitations
  • Mainly concerning security (RBAC, Auditing, Alerting) and some more advanced features like Machine Learning
Zabbix and Elastic as History Back-End

- Separate config database (still SQL based)
  - Easier to back-up
  - Holds information about all your hosts/items, just no historical information

- No housekeeping for history
  - History does not get purged by Zabbix
  - Just delete – date based – indices to purge

- Scalable history back-end
  - Just add nodes to Elastic cluster

- Not to be confused with Zabbix MONITORING content in Elastic !!
Current Install - Migrate or Not

• Only one history back-end possible per item type
• Either
  • Drop history and start new, in Elastic
  • Migrate data from DB to Elastic
    • Possible with some scripting – not out-of-the-box
• You need scale to gain performance in Elastic (no numbers, sorry)
• Querying history needs knowledge of data, but is possible
  • Itemid and data is in Elastic, meaning of id is in SQL database
How to set up - Preparations

• Read documentation 😊
• Install, like ‘yum install elasticsearch’
• Define mappings and possibly templates
  • Found in database/elasticsearch/elasticsearch.map
  • Templates for automatic index creation – date based
• Make sure SELinux and Firewall are configured to allow communications
• Watch log files to find any errors that need fixing to get it working
How to set up - Zabbix Server

- **zabbix_server.conf**

```plaintext
### Option: HistoryStorageURL
# History storage HTTP[S] URL.
# Mandatory: no
# Default: HistoryStorageURL=
HistoryStorageURL=http://localhost:9200

### Option: HistoryStorageTypes
# Comma separated list of value types to be sent to the history storage.
# Mandatory: no
# Default: HistoryStorageTypes=uint,dbl,str,log,text
HistoryStorageTypes=uint,dbl,str,log,text

### Option: HistoryStorageDateIndex
# Enable preprocessing of history values in history storage to store values in different indices based on date.
# 0 - disable
# 1 - enable
# Mandatory: no
# Default: HistoryStorageDateIndex=0
HistoryStorageDateIndex=0
```
How to set up - Zabbix Web Front-end

- `zabbix.conf.php`

```php
// Zabbix GUI configuration file.
global $DB, $HISTORY;

// Elasticsearch url (can be string if same url is used for all types).
$HISTORY['url'] = 'http://localhost:9200';
//--$HISTORY['url'] = [
  //  'uint' => 'http://localhost:9200',
  //  'dbl' => 'http://localhost:9200',
  //  'str' => 'http://localhost:9200',
  //  'log' => 'http://localhost:9200',
  //  'text' => 'http://localhost:9200'
//--];
// Value types stored in Elasticsearch.
$HISTORY['types'] = ['uint', 'dbl', 'str', 'log', 'text'];
```
## How to set up – Verify Functionality

- curl http://localhost:9200/_cat/indices?v

```bash
> curl http://localhost:9200/_cat/indices?v

<table>
<thead>
<tr>
<th>health</th>
<th>status</th>
<th>index</th>
<th>uuid</th>
<th>pri</th>
<th>rep</th>
<th>docs.count</th>
<th>docs.deleted</th>
<th>store.size</th>
<th>pri.store.size</th>
</tr>
</thead>
<tbody>
<tr>
<td>yellow</td>
<td>open</td>
<td>text</td>
<td>8VPXpHQiR7qHd8IoGfVMzw</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1.2kb</td>
<td>1.2kb</td>
</tr>
<tr>
<td>green</td>
<td>.kibana_1</td>
<td>opXGk7kITGe2GXoT3RTxyQ</td>
<td>1</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>15.9kb</td>
<td>15.9kb</td>
<td></td>
</tr>
<tr>
<td>yellow</td>
<td>open</td>
<td>str</td>
<td>zmaLR_xjQVifqVQwrRywhw</td>
<td>5</td>
<td>1</td>
<td>588</td>
<td>0</td>
<td>195.5kb</td>
<td>195.5kb</td>
</tr>
<tr>
<td>yellow</td>
<td>open</td>
<td>log</td>
<td>9Xqw7TEzToy73Xr2Fwr5yg</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1.2kb</td>
<td>1.2kb</td>
</tr>
<tr>
<td>yellow</td>
<td>open</td>
<td>dbl</td>
<td>f_raSFa9R1mcDSxL-A3FgA</td>
<td>5</td>
<td>1</td>
<td>340954</td>
<td>0</td>
<td>34.5mb</td>
<td>34.5mb</td>
</tr>
<tr>
<td>green</td>
<td>.kibana_2</td>
<td>IRnARzGiRhoe9Z2APsRz7w</td>
<td>1</td>
<td>0</td>
<td>7</td>
<td>0</td>
<td>19.2kb</td>
<td>19.2kb</td>
<td></td>
</tr>
<tr>
<td>green</td>
<td>.tasks</td>
<td>wxaCdVVSkiMC3iliNeuEw</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>6.2kb</td>
<td>6.2kb</td>
<td></td>
</tr>
<tr>
<td>yellow</td>
<td>open</td>
<td>uint</td>
<td>UUM_R80qRm6aN4zv0sJbMg</td>
<td>5</td>
<td>1</td>
<td>144666</td>
<td>0</td>
<td>14.1mb</td>
<td>14.1mb</td>
</tr>
</tbody>
</table>
```
What’s Next – My Personal Observations

• Still experimental – too soon to jump into it for production?
• What other uses for having history in Elastic?
• Difficult – for me – to find real use case
Questions?

Thank you, now it’s time for lunch . . .