Migration to Zabbix
By Erik Skytte, DBC, Denmark

DBC: http://www.dbc.dk/english/about_dbc
Erik: http://www.linkedin.com/pub/erik-skytte/20/a77/444
Zabbix IRC/Forum: eskytte
DBC’s main task is to develop and maintain the bibliographic and IT-infrastructure in Danish libraries by:

- Producing the **Danish National Bibliography** and user oriented cataloging
- Developing and maintaining **Dan*Bib** as Union Catalog for public, educational and academic libraries as part of an automated ILL
- Developing and maintaining **library.dk** as the common access for citizens to Danish publications and Danish library holdings.
- DBC’s IT systems are based on **open source** and service oriented architecture ... E.g **https://github.com/ding2/ding2**

- Monitored installation:
  - ~ 500 devices (Linux, Windows, SAN, Network, Xen, VMware, environment ...)
  - Huge base of in-house developed applications (some very old)
  - Zabbix agents versions from 1.1.4 -> 2.0.x, Zabbix Server 2.0.5
  - Newer applications and services based on Java, Drupal, Solr, Postgress ...
  - Huge demand for application monitoring
  - No proxies (so far)
Before Zabbix

- **Hobbit / Xymon** - Infrastructure and web monitoring
- **MRTG** - Trending for network devices
- **Munin** - Detailed Linux trending (subgroup of servers)
- **Lots of “plugins”**
- **UserParameter=netstat.active, munin-run netstat | grep active | cut -f2 -d” "**
- **CA Unicenter syslog tool** – SMS to operations
Zabbix deployment

• Hobbit (and other tools) running in parallel - No big bang
  – Easy to compare alarms and state of both systems

• One to one copy of ~ 70 % of triggers and items
• Linux: Good overview because of central config files
• Windows: More work because of decentralized config files

• Lower the amount of high triggers - from old monitoring system
  – Too many and too often high alerts

• Trigger severities: Information, Warning, High,
  – Few Disaster triggers for major problems (e.g. SAN)
Zabbix extensions

• Because Hobbit did manage most of the infrastructure ...

• Zabbix startup project focused on:
  – Application and main systems monitoring
  – Trending
  – Solution of main prod problems:
    • “Zabbix Trading - Attack Productions Problems”
    • http://www.zabbix.com/conf2012_agenda.php

• Infrastructure monitor extension
  – VMware, SAN, firewalls, syslog ...
Zabbix deployment

• Implementation path: not linear
  – And not from bottom to top
  – More top to bottom ...

• Driven by many factors but main ones were:
  – Problems with system
  – Importance of system
  – Active Persons

• Zabbix love:
  – The easy way to put data into Zabbix !!!
  – Userparameters
  – Zabbix_sender
  – Perf counter
Design

- **Important**: Agreement on common system / applications relationships and terms in firm
- Everyone is talking the same language and share common understanding of application hierarchy and dependencies
- DBC: defined in ITIL Group
- **CMDB** or **List** with Main and sub systems:

<table>
<thead>
<tr>
<th>Main System</th>
<th>Sub System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Server</td>
</tr>
<tr>
<td></td>
<td>Network</td>
</tr>
<tr>
<td></td>
<td>SAN</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>Business System X</td>
<td>Webserver</td>
</tr>
<tr>
<td></td>
<td>Middelware</td>
</tr>
<tr>
<td></td>
<td>Backend</td>
</tr>
</tbody>
</table>
Design

• System / application names used in Zabbix from CMDB:
  • Groups (for all main systems)
  • Screen names (drill down menus)
  • Maps (main systems)
  • Template names (easy search)
  • Item names / graphs (lasted data)
  • Item descriptions (service desk integration)
  • Trigger names (trigger list)
  • Trigger descriptions (service desk and SMS)
  • Host names (logical host used for some systems)
Design

• Screen names:
  – Drill down menus

• Search functions
  – Find templates etc.

• Trigger names:
  – Address receiver group
  – Quick overview/relation
  – Win: log: Error message
  – Linux: TCP port: Email service down
  – Win: Service: “Citrix XML”: Stopped (6)
  – WebServices: openxid.addi.dk: Error
  – Danbib: Netpunkt: Targed process down
  – ORS: 10 tasks in error state
Design

• Item names
  – Grouping of latest data
  – (Linux OS template)

• Template names (hierarchy)

<table>
<thead>
<tr>
<th>3 Memcache</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 MySQL Template</td>
</tr>
<tr>
<td>3 Netstat TCP Template</td>
</tr>
<tr>
<td>3 Oracle Template</td>
</tr>
<tr>
<td>4 ADHL</td>
</tr>
<tr>
<td>4 Artesis Openscan17 tracelog</td>
</tr>
<tr>
<td>4 Artesis Openscan20 tracelog</td>
</tr>
<tr>
<td>4 Artesis Opensearch2.1 tracelog</td>
</tr>
<tr>
<td>4 Artesis Opensearch11 tracelog</td>
</tr>
<tr>
<td>4 Artesis Opensearch20 tracelog</td>
</tr>
<tr>
<td>4 Basis yaz-client tests</td>
</tr>
</tbody>
</table>

| Disk: Used space on /usr/local in % |
| Disk: Used space on /var in %       |
| Host uptime (in sec)                |
| Host: Agent ping (TCP)              |
| Host: Agent version                 |
| Host: information - uname            |
| Host: Ping                           |
| Log: linux log                       |
| Memory: Available                    |
| Memory: Buffers                      |
| Memory: Cached                       |
| Memory: Total                        |
| Net: Traffic in eth0                 |
| Net: Traffic out eth0                |
| Port: Email/SMTP service is running  |
| Port: SSH service is running         |
| Process: cron is running             |
Service desk integration

• **Action message:**

%SUMMARY={HOST.NAME}: {TRIGGER.NAME}
%FROM_USERID=zabbix@dbc.dk
%DEVICE={HOST.NAME}
%TYPE=I
%PRIORITY=1 - Høj
%ZEXTERNALSYSTEMTICKET={EVENT.DATE}-{TRIGGER.ID}
%
{ITEM.DESCRIPTION}
%DESCRIPTION={HOST.NAME}:{TRIGGER.NAME}
%
{TRIGGER.COMMENT}
Starttid: {EVENT.DATE} {EVENT.TIME}
Alarm indhold: {ITEM.VALUE}

• **Item description:**

%AFFECTED_SERVICE=Danbib *(Main system)*
%AFFECTEDCOMPONENT=Netpunkt *(Sub system)*
Service desk integration

- General Action for service desk mails and SMS to people “on call”
  - Goal: Reduce amount of actions

<table>
<thead>
<tr>
<th>Conditions</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance status not in &quot;maintenance&quot;</td>
<td>Send message to user groups: Vagt</td>
</tr>
<tr>
<td>Trigger value = &quot;PROBLEM&quot;</td>
<td>Send message to users: servicedesk</td>
</tr>
<tr>
<td>Trigger name like &quot;(vagt)&quot;</td>
<td></td>
</tr>
<tr>
<td>Host group &lt;&gt; &quot;Sandkasse&quot;</td>
<td></td>
</tr>
</tbody>
</table>

Trigger split:
“Business”
“Technical”

- CA Unicenter Service Desk:

<table>
<thead>
<tr>
<th>Requester</th>
<th>Affected End User</th>
<th>Hoved Produkt</th>
<th>Komponent</th>
<th>Incident Area</th>
<th>Status</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>zabbix</td>
<td></td>
<td>Danbib</td>
<td></td>
<td>Netpunkt</td>
<td>Closed</td>
<td>1 - Høj</td>
</tr>
</tbody>
</table>

  Details:
  - Reported By: zabbix
  - Assignee: Skytte, Erik
  - Group: IT-Infra
  - Summary: host: Danbib: Netpunkt: Nep targetd process not running (vagt)
  - Description: host: Danbib: Netpunkt: Nep targetd process not running (vagt)
    Frontend process for Netpunkt system. Restart process!
    Starttid: 2013.05.22 13:31:40
    Alarm indhold: 5
    http://zabbix/zabbix/events.php?triggerid=20246

Zabbix Conference 2013 - Erik Skytte - DBC
Tie the different areas together

- “There are too many menus in Zabbix ð%#”! ...”
Tie the different areas together

- **DBC Main Screen**
  - Links to all the other Screens, Maps, Graphs and documentation

- **Zabbix as index for Wiki and other IT documentation**
Tie the different areas together

• Navigating in DBC Zabbix:
  – Main DBC screen
  – Dashboard (links)
  – Search function

• Internal Zabbix Workshop focus:
  – Dashboard, Latest data, Events, Screens

• Main screen:
  – Nice overview when major problems occur (lots of triggers)
  – E.g. main SAN problems
Building application screens

• Application Screen – overview ...

[Diagram of network and application screens]
Building application screens

- Add application documentation as background
- Quick application overview
- Quick status over different parts of an application
  - E.g. Frontend, Middleware, Backend

- Added “link” icon
- Added “logical host” – to show general application triggers

- Add applications hosts
- Remember to decolorize the background image
Building application screens

- Use of “headline” and “separator” icons
  - More easy to organize hosts etc.
  - No need to change background
  - Add information in host label (e.g. DNS)

<table>
<thead>
<tr>
<th>AD / DNS</th>
<th>Fil Server</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="AD / DNS servers" /> OK</td>
<td><img src="image2.png" alt="Fil Server" /> OK</td>
</tr>
<tr>
<td><img src="image3.png" alt="Service Desk" /> OK</td>
<td><img src="image4.png" alt="Navision / Ln / SQL" /> OK</td>
</tr>
<tr>
<td><img src="image5.png" alt="Print" /> OK</td>
<td><img src="image6.png" alt="Diverse" /> OK</td>
</tr>
</tbody>
</table>

Win: Log: Error message
Building application screens

- Add technical documentation as backgrounds
  - Quick access to documentation
Building application screens

- Make overview screens – graphs for one or more applications
  - Management love them
Users - different focus and tools

• System admins
  – Most functions and screens

• Developers (important partner!)
  – Application and Service screens and items, java items etc.,

• Support/operators
  – Dashboard, Main Screen, Overview Screens, Service Desk integration

• Application specialists
  – Application and service screens, (Trending), email

• Application / product owners / project managers ...
  – Application screens, reports, email alerts

• Management
  – Overview Screens (when problems), “Traffic lights”, reports, email alerts

• Zabbix not isolated to IT/technical people!
**Special monitoring**

- **Oracle connections**
  - saved over time and sorted in groups
  - (Oracles own tool focuses on real time monitoring)

- Python script reads oracle session file - *listener.log*
Special monitoring

- **Firewall problem**
  - Heavy Packet loss etc.
  - Cisco ASA Mem Blocks 9344
  - SNMP OID: .1.3.6.1.4.1.9.9.147.1.2.2.1.1.4.9344.8

- Item, triggers and SMS actions easy/fast setup
- Problem solved after upgrade of Firewall firmware ...

Zabbix Conference 2013 - Erik Skytte - DBC
Special monitoring

• Syslog / log management
• Windows logging from old Hobbit system
• Linux logging
Miscellaneous

• Host based templates
  – more templates
  – but better overview
  – and management of configuration and changes

• Quick CMDB host information
  – Scripts: /bin/grep - "^\{HOST.HOST\}" /etc/zabbix/hostlist.txt
  
• E.g. output: “Medius projekt VMware Server”
Miscellaneous

• **Future**
  – More application monitoring
  – Web monitoring based on python scripts and selenium
  – …

• **Zabbix tutorials:**
  • [http://www.zbxtutorials.org/](http://www.zbxtutorials.org/)

• **Fun stuff**
  – [http://www.youtube.com/watch?v=RKBs6Sm0uRg](http://www.youtube.com/watch?v=RKBs6Sm0uRg)