Zabbix – Distribution system and Time Base Correlation

Modules and extensions for Zabbix from S&T Slovakia

Marek Konečný, 17.6.2018
Agenda

1. Distribution system
2. Time Base Correlation
1| Distribution system
Remote Zabbix agent and Zabbix proxy management:

- Restart Zabbix agent and Zabbix proxy
- Zabbix proxy update
- Zabbix Agent and Zabbix proxy status identification
- View the contents of Zabbix agent configuration files
- Listing Zabbix agent distribution directory

Zabbix agent configuration repositories

Distribution of Zabbix agent configuration files, monitoring scripts, and binary files
Unlimited repositories

The repository can be located on any server (Zabbix server, Zabbix proxy, dedicated server ...)

There is no need to create a new account on the monitored server

There is no need to open any port to the monitored server (except Zabbix agent port)

There is no SSH connection to the monitored server

Distribution system uses Zabbix agents on monitored servers only

The distribution system is designed for heterogeneous environments – HPUX, Solaris, AIX, Linux, MS Windows

Distribution system tools collect information about monitored servers using the Zabbix DB Zabbix API

Each monitored server has its own repository directory with all configuration files, scripts and binaries

rsync is used to synchronize the contents of distribution directories

Distribution system tools work with separate servers and clusters
Repository

[root@zabbix34sdemo]# tree -d
.
|-- zabbix_distribution
|   |
|   |-- clusters
|   |   `-- zabbix34cdemo.snt.sk
|   
|   `-- servers
|       `-- zabbix34a1demo.snt.sk
|           `-- zabbix34cdemo.snt.sk -> /usr/lib/zabbix/zabbix_distribution/clusters/zabbix34cdemo.snt.sk/
|           `-- zabbix34a2demo.snt.sk
|                   `-- zabbix34cdemo.snt.sk -> /usr/lib/zabbix/zabbix_distribution/clusters/zabbix34cdemo.snt.sk/
|                   `-- zabbix34pdemo.snt.sk

|-- zabbix_tools

Monitored server

[root@zabbix34a1demo]# tree -d
.
|-- zabbix_instrumentation
|   |
|   `-- zabbix34cdemo.snt.sk
Administrator tools

```
zabbix_agent_conf.pl  view the contents of Zabbix agent configuration files on monitored servers
zabbix_agent_deploy.pl deploying distribution directory contents to monitored servers
zabbix_agent_distrib_dir.pl view the contents of distribution directories on monitored servers
zabbix_agent_restart.pl Zabbix agent restart
zabbix_agent_status.pl Zabbix agent activity status
zabbix_agent_stop.pl  Zabbix agent stop

zabbix_cluster_deploy.pl deploying distribution directory contents to monitored clusters
zabbix_cluster_restart.pl Zabbix agents restart on monitored clusters

zabbix_proxy_restart.pl Zabbix proxy restart
zabbix_proxy_start.pl Zabbix proxy start
zabbix_proxy_status.pl Zabbix proxy status
zabbix_proxy_stop.pl  Zabbix proxy stop
zabbix_proxy_update.pl Zabbix proxy update
```

The tools are located on the repository servers
The use of the tools is very simple - they have only one argument (server or cluster name)
It is very easy to create additional tools with our supplied perl module
S&T also supplies additional tools as part of its modules and extensions (eg TBC)
2| Time Base Correlation
Processing SNMP traps, specific log files, directories with log files, and log files with multiline record type
The content of the processed directories may vary over time and it is possible to select log files using a regular expression identifying their name
The content of the files is processed by Event correlation service
The correlation engine is configurable and allows to reduce the stream of records processed by Zabbix agent or Zabbix proxy
TBC processing takes place on servers with Zabbix agent or Zabbix proxy
Linux and Unix OS are supported
Architecture – specific log file processing
Architecture – directory processing
Architecture – SNMP trap processing
Examples of processed log files and directories

/var/log/demo/

|-- demo3.log
|   |-- directory
|       |-- test1.log
|       |-- test10.log
|       |-- test17.log
|       |-- test18.log
|       |-- test19.log
|       |-- test2.log
|       |-- test20.log
|       |-- test22.log
|       |-- test3.log
|       |-- test4.log
|       |-- test5.log
|       |-- test6.log
|       |-- test7.log
|       |-- test8.log
|       `-- test9.log

|-- directory
|   |-- test1.log
|   `-- test9.log

|-- directory_ml
|   |-- test1.log
|   `-- test3.log

/var/log/zabbix/tbc

|-- TBC_demo3.log
|   |-- TBC_directory.log
|   |-- TBC_directory_ml.log
|   `-- directory.log

|-- directory.log
|   |-- directory_ml.log

Zabbix agent
## Logmerger and EC Service

### Logmerger singl line and multi line (sl/ml)

- Perl scripts created by S&T
- Cyclically Started by Zabbix agent - one instance per directory
- Processing the source log:
  - always from the beginning
  - from the beginning for the first entry only
  - from the first entry point
- Event storm protection Storm
- Number of processed lines per cycle
- Directory definition
- Initial line identifications with regular expressions (ml)
- Defining the linking string (ml)
- Maximum output line length (ml)
- Defining the output file
- Self monitoring – processing error log files

### EC service

- Perl script – Simple Event Correlator
- Runs as a service
- Correlators - configuration files for each log or directory
- Processing the source log:
  - always from the beginning
  - from the beginning for the first entry
  - from the first entry point
- Defining input and output files
- Self monitoring - defining and processing error log files
S&T supplies three basic correlators for EC:
- Suppress
- Counter
- Timer
Correctors are provided in two modes of operation:
- Source mode
- Condition mode

The concept of correlators and modes is explained in the following slides
It is possible to create a number of filters with chained logical conditions.
The picture presents Counter 3x correlator.
Timer correlator

Zabbix agent

TBC

Timer

Suppressing

Time window

t

Suppressing
Counter correlator - Condition mode example

Counter 3x, 1h

Condition match

Input log
<time stamp> <event>
1 CCOUNTER 3 | 81
2 CCOUNTER 3 | 81
3 CCOUNTER 3 | 31
4 CCOUNTER 3 | 435
5 CCOUNTER 3 | 81
6 CCOUNTER 3 | 56

Output log
<time stamp> <event>
TBC
3 CCOUNTER 3 | 31
6 CCOUNTER 3 | 56
Counter correlator - Source mode example

Counter 3x, 1h

Source match

Input log
<time stamp> <event>
1 SCOUNTER 3 | 81
2 SCOUNTER 3 | 81
3 SCOUNTER 3 | 31
4 SCOUNTER 3 | 435
5 SCOUNTER 3 | 81
6 SCOUNTER 3 | 31
7 SCOUNTER 3 | 31

Output log
<time stamp> <event>
5 SCOUNTER 3 | 81
7 SCOUNTER 3 | 31

TBC

Only one rule for all source variations!
Timer correlator - Condition mode example

**Timer 5s, 30s**

**Condition match**

**Input log**

```
<time stamp> <event>
1 CTIMER 5 | 81
2 CTIMER 5 | 66
3 CTIMER 5 | 31
4 CTIMER 5 | 435
.
.
17 CTIMER 5 | 234
18 CTIMER 5 | 81
```

**Output log**

```
<time stamp> <event>
1 CTIMER 5 | 81
17 CTIMER 5 | 234
```

2s

30s
Timer correlator - Source mode example

**Timer 5s, 30s**

Source match

Input log

<time stamp> <event>

1 STIMER 5 | 81
2 STIMER 5 | 81
3 STIMER 5 | 81
4 STIMER 5 | 81

Only one rule for all source variations!

Output log

<time stamp> <event>

1 STIMER 3 | 81
17 STIMER 3 | 81
Simulation for Counter 3x correlator (Source mode)

1) ./directory is empty

2) creating and filling log files:

```
[root@zabbix34a1demo]# echo "1 SCOUNTER 3 | 85" >> ./directory/test8.log
[root@zabbix34a1demo]# echo "2 SCOUNTER 3 | 83" >> ./directory/test8.log
[root@zabbix34a1demo]# echo "3 SCOUNTER 3 | 82" >> ./directory/test6.log
[root@zabbix34a1demo]# echo "4 SCOUNTER 3 | 83" >> ./directory/test8.log
[root@zabbix34a1demo]# echo "5 SCOUNTER 3 | 83" >> ./directory/test8.log
[root@zabbix34a1demo]# echo "6 SCOUNTER 3 | 81" >> ./directory/test6.log
[root@zabbix34a1demo]# echo "7 SCOUNTER 3 | 82" >> ./directory/test6.log
[root@zabbix34a1demo]# echo "8 SCOUNTER 3 | 82" >> ./directory/test6.log
```

3) Zabbix problems:

Only one correlator, item and trigger is needed for all log files in a directory and all event variations!
Correlation possibilities

Detection of event sequences over time
Time-dependent filtering
Time-dependent validity of correlation rules
Conditional suppression – chaining rules
Generators of synthetic events
Postprocessing events
...

Detection of event sequences over time
Time-dependent filtering
Time-dependent validity of correlation rules
Conditional suppression – chaining rules
Generators of synthetic events
Postprocessing events
...
TBC tools for Distribution system

- `zabbix_agent_deploy.pl` deploying configuration files with correlators to monitored servers
- `zabbix_tbc_start.pl` EC service start
- `zabbix_tbc_status.pl` EC service status check
- `zabbix_tbc_stop.pl` EC service stop
Contact

S&T Slovakia s.r.o.
Mlynské Nivy 71
821 05 Bratislava

t: +421 258 273 111
m: +421 905 618 324
marek.konecny@snt.sk
www.snt.sk
S&T Slovakia s.r.o.
Mlynské Nivy 71
SK-821 05 Bratislava

+421 2 58273 111
www.snt.sk
snt@snt.sk