How to Debug Common Agent Issues

Volker Fröhlich

12 Sep 2015, Zabbix Conference

Who am I?

- Volker Fröhlich (volter)
- Geizhals Preisvergleich Internet Services AG (`http://geizhals.at`)
- Action simulator, Zabbix blog, various frontend patches
- Fedora packager, Openstreetmap contributor

Goals of this talk

- Item unsupported, odd values, ...
- It is useful to understand the inner workings
- How to figure out what's wrong – efficiently!

Overview

Modes & Protocols

Passive agent

- Server/proxy connects to agent (TCP 10050)
- Wire protocol
- One connection per item retrieval
- Remote commands

Active agent

- Agent connects to server/proxy (TCP 10051)
- JSON protocol
- Configuration is requested
- Auto-registration
- Can buffer and submit multiple values
- Some items only work in this mode

Modes & Protocols II

Sender/Trapper

- Connects to proxy/server (TCP 10051)
- Single value or in bulk
- Timestamped data

Processes

- 1 Main
- 1 Collector
- x Passive workers
- 1 Active worker

Configuration files

- Server, ServerActive
- Hostname, HostnameItem
- UserParameter, Modules
- Include

Frontend level gotchas

- Configuration cache delay, Discovery rule interval, deactivated prototypes
- Confused something (host/template), non-audited changes (ZBX-2815, ZBX-4842)
- Datatype wrong (delta as speed/s)
- Macros
- Quoting, escaping, passing arguments

System level gotchas

- Not restarted
- Wrong configuration file (symlink, agent/agentd)
- Firewall (local or anywhere)
- Permissions
- SELinux/grsecurity/apparmor
- sudo
- Proxies
- Timeouts Active/Passive

What if it's something else?

Have you tried turning it off and on again?

- Read error messages and know where to find them
- Logging/Syslog

Debug level <= 3 (Information)

IPC issues, worker start, problems hostname/hostnameitem, No active checks on server, can not retrieve some JSON key (agent protocol), active check x is not supported, Collector issues

Debug level 4 (Debug)

Which Zabbix function is running and when it finishes, exactly what is sent, what is received; Collector details

- Read the source code – src/libs/zbxsysinfo/
- Sniff, trace, understand/speak the protocols

A list of useful tools

- zabbix_get (zabbix_agentd)
- ps/pgrep
- strace/truss/dtruss
- ltrace/dtrace
- ausearch
- syslog
- netstat/ss
- ip/route/traceroute
- tcpdump/Wireshark
- getent/nslookup/dig/host
- netcat/socat/telnet

strace and ltrace

strace -f -p <pid1> [-p <pid2>]

```
[pid 18178] getpeername(6,  <unfinished ...>
[pid 18178] <... getpeername resumed> {sa_family=AF_INET, sin_port=htons(48881),
    sin_addr=inet_addr("127.0.0.1")}, [16]) = 0
[pid 18178] alarm(7)                        = 0
[pid 18178] read(6, "ZBXD\1", 5)            = 5
[pid 18178] read(6, "\v\0\0\0\0\0\0\0", 8) = 8
[pid 18178] read(6, "agent.ping\n", 2047) = 11
```

ltrace -f -p <pid1> [-p <pid2>]

```
getpeername(6, 0x7ffca5381ce0, 0x7ffca5381ca4, 0x7ffca5385fdf) = 0
strchr("127.0.0.1", ',')                                      = nil
getaddrinfo("127.0.0.1", nil, 0x7ffca5381cb0, 0x7ffca5381ca8) = 0
freeaddrinfo(0xa1b0a0)                                        = <void>
alarm(7)                                                      = 0
read(6, "ZBXD\001", 5)                                        = 5
read(6, "\v", 8)                                              = 8
read(6, "agent.ping\n", 2047)                                 = 11
alarm(0)                                                      = 7
strlen("agent.ping\n")                                        = 11
```

tcpdump

tcpdump -i lo -nn port 10050

```
00:20:34.065579 IP 127.0.0.1.49134 > 127.0.0.1.10050: Flags [S], seq 640796155
00:20:34.065599 IP 127.0.0.1.10050 > 127.0.0.1.49134: Flags [S.], seq 2538515492
00:20:34.065612 IP 127.0.0.1.49134 > 127.0.0.1.10050: Flags [.], ack 1

00:20:34.065636 IP 127.0.0.1.49134 > 127.0.0.1.10050: Flags [P.], seq 1:6
00:20:34.065644 IP 127.0.0.1.10050 > 127.0.0.1.49134: Flags [.], ack 6
00:20:34.065670 IP 127.0.0.1.10050 > 127.0.0.1.49134: Flags [.], ack 14
00:20:34.065687 IP 127.0.0.1.49134 > 127.0.0.1.10050: Flags [P.], seq 14:25, ack 1
...
```

DNS

- PTR record
- res_init(), getaddrinfo()/getnameinfo()

```
getent ahosts <name or ip_address>
```

- IPv6 (gai.conf)
- Empty hosts file (localhost)
- dnsmasq, nscd, bind, dnscache, ...

Other networking-related trouble

- Routing (IPv6 again!)

```
ip route get <target_ip_address>
```

- Latency, efficiency (like old HTTP)
- Ephemeral port re-use with Windows hosts

```
Protocol src_ip:src_port dst_ip:src_port
```

- Lost TCP segments

Timing/Timeouts

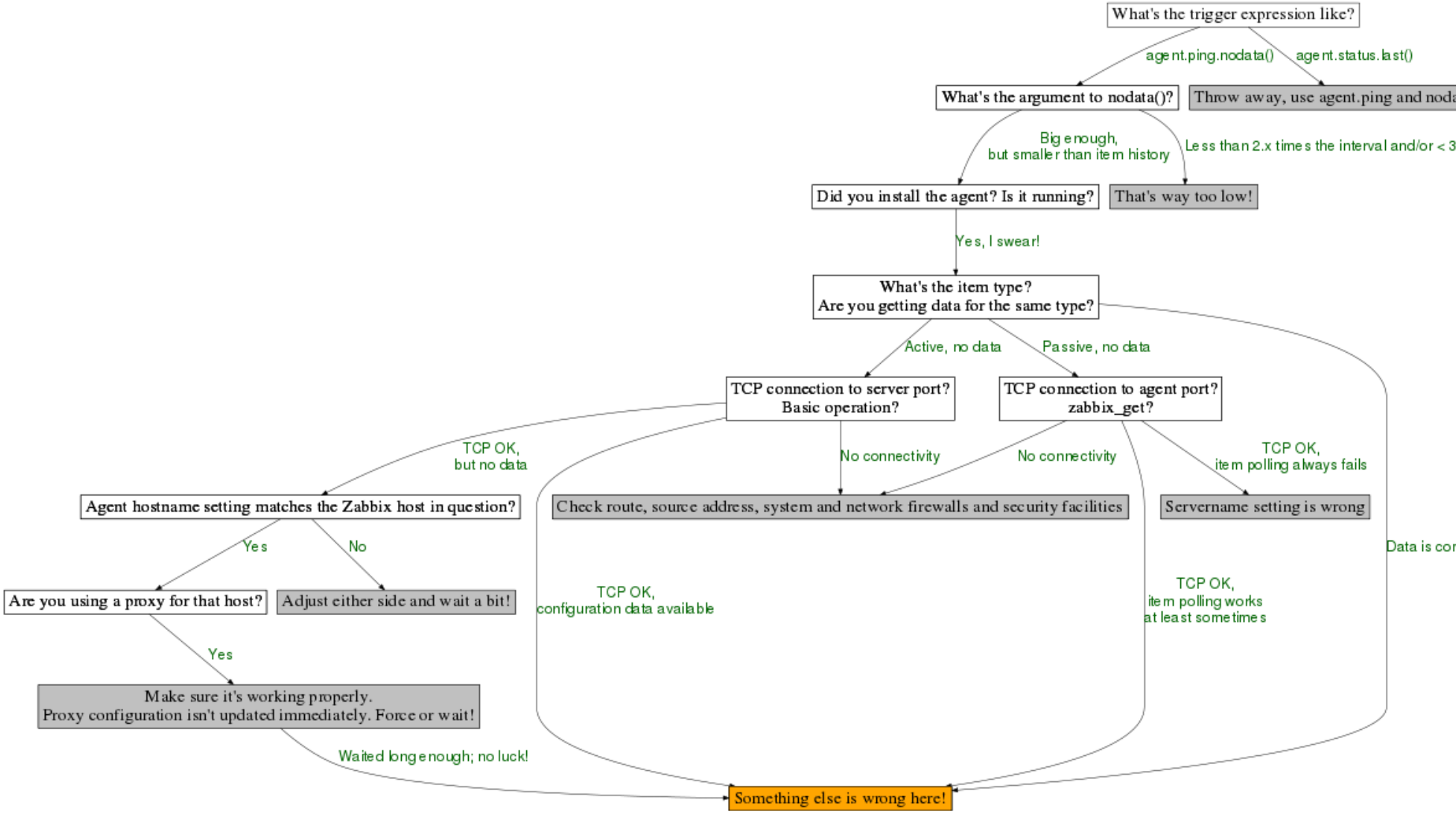
- Which timeout applies and how often? Active, passive?
- Scalability for active checks (ZBXNEXT-691)
- Re-enable unsupported active agent items (ZBXNEXT-2633)
- When are active items scheduled
- Influence of network latency and lossyness
- zabbix_get has a hard-coded timeout! (ZBXNEXT-1468)
- Escaping agent timeouts

Other gotchas

- Environment, shell
- Testing with zabbix_agentd – No collector
- hostnameitem and zabbix_sender (ZBXNEXT-1729)
- Debugging zabbix_sender is only possible on the server/proxy
- Zabbix doesn't care about stderr or the exit code, empty response disables item (ZBXNEXT-2230)
- web.page.* does not use a HTTP client library (ZBXNEXT-1816)
- Order matters when submitting timestamped data with zabbix_sender
- LLD items

"Agent unreachable"

Bottom-up approach



"Agent is responding with a wrong value"

Poking/bisecting approach

- zabbix_get locally –> Value OK
- zabbix_get from server –> Value OK

Maybe a problem with name resolution in the server!

- Log level 4 or tcpdump –> No incoming request
- Ensure general connectivity –> OK

Obviously querying a different host

Contact information and readings

- volter in #zabbix and #zabbix-de on Freenode IRC
- volker.froehlich@geizhals.at

Readings

- `http://blog.zabbix.com/mysterious-zabbix-problems-how-we-debug-them`
- `http://zabbix.org/wiki/Troubleshooting`
- `http://zabbix.org/wiki/Docs/protocols`
- Internetworking with TCP/IP, Vol. 1, Douglas E. Comer