How to proceed when 1 000 call agents tell you: ’My Computer is slow‘

Tobias Oetiker <tobi@oetiker.ch>

22nd Large Installation System Administration Conference

1 Overview

boot up

- users blame IT performance
- stop watch and heisenbugs
- sysinternals tools
- autoit and winspy
- sorry, no quick fix
- but we can monitor it

2 Implementation

design goals

- passive monitoring from users perspective
- let users give their input
- minimal impact
- simple setup and update
- central data store

three tools

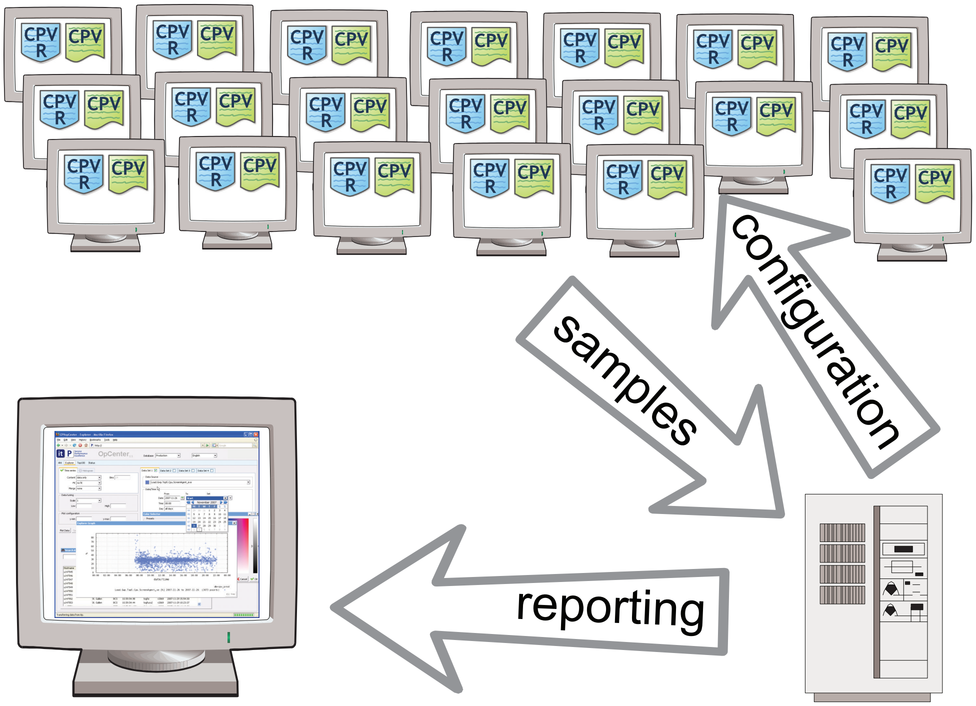
- CPV monitor: observe the system
- CPV reporter: easy problem reporting
- CPV explorer: view the results

cpv monitor and perl/CPAN

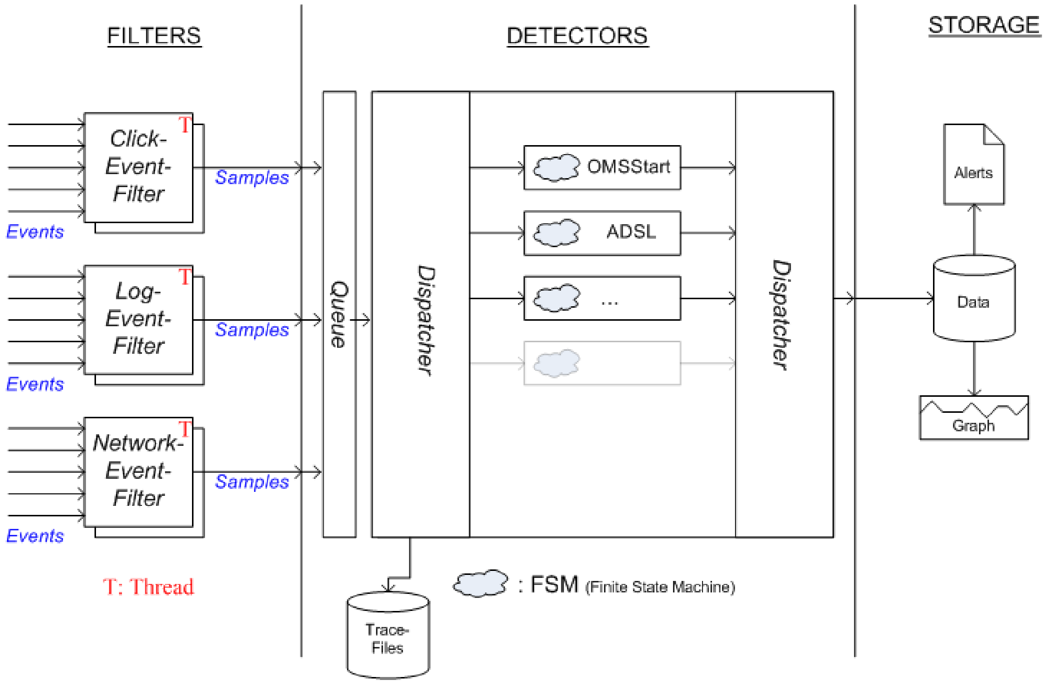
Look it’s perl honey!

- AutoIt
- `use Win32::GuiTest;`
- `use Win32::API;`
- `use Win32::OLE;`
- `use Win32::GUI;`
- `use FSA::Rules;`
- `use threads;`

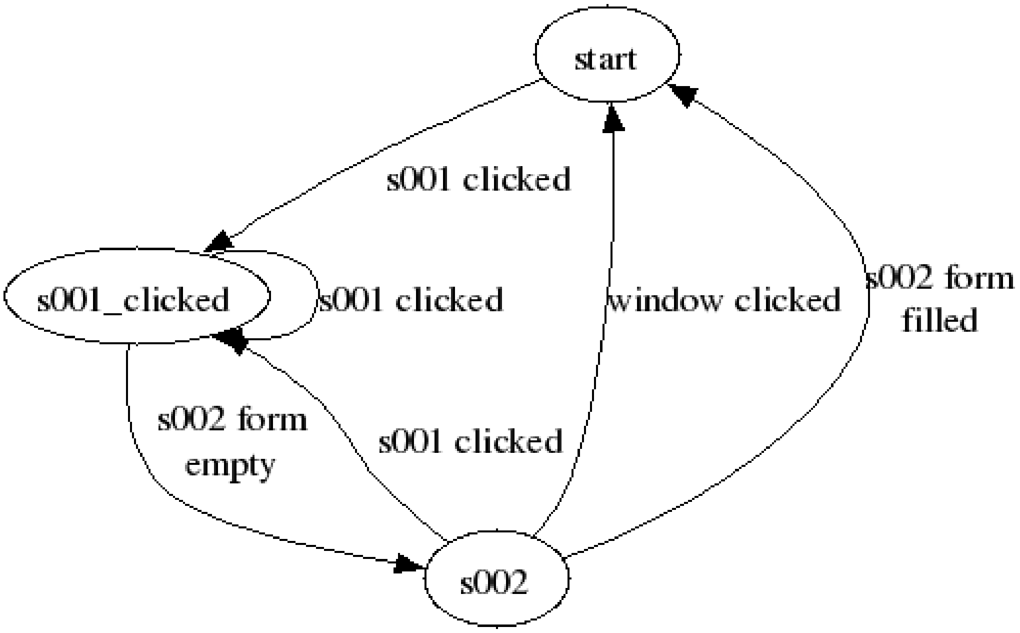
cpv system overview



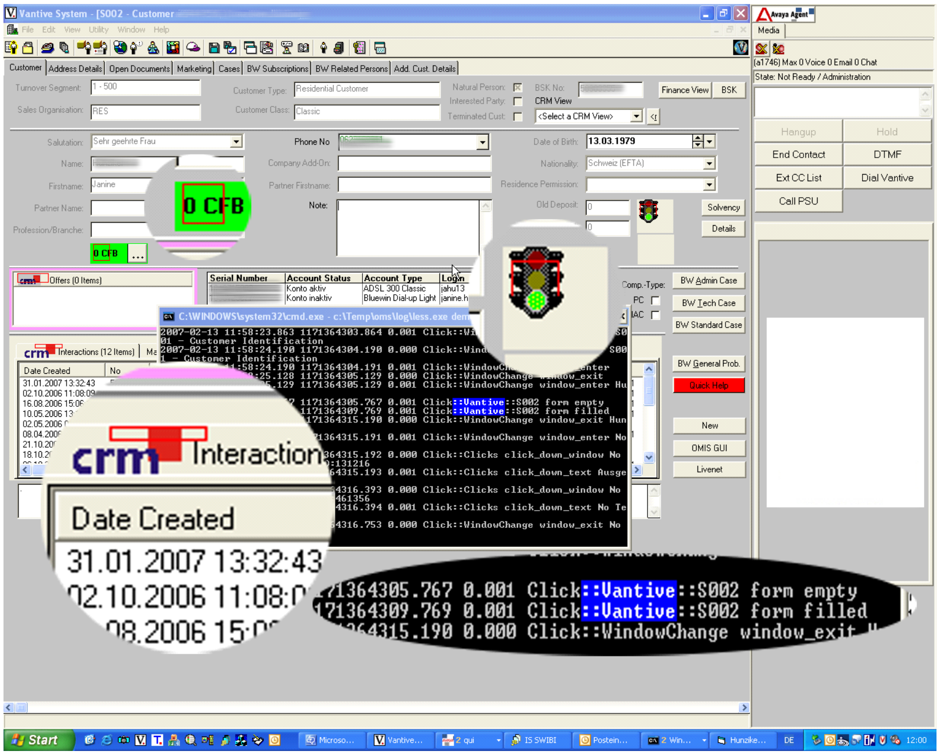
cpv monitor structure



lesson #1: fsm are cool



lesson #1: seemingly simple



(a1746) Max 0 Voice 0 Email 0 Chat
State: Not Ready / Administration

Turnover Segment: 1 - 500
Sales Organisation: RES
Customer Type: Residential Customer
Customer Class: Classic
Natural Person: ☒
Interested Party: □
Terminated Cust: □
BSK No: [redacted]
CRM View <Select a CRM View>

Salutation: Sehr geehrte Frau
Name: [redacted]
Firstname: Janine
Partner Name:
Profession/Branche:
0 CFB
Phone No [redacted]
Company Add-On:
Partner Firstname:
Note:
Date of Birth: 13.03.1979
Nationality: Schweiz (EFTA)
Residence Permission:
Old Deposit: 0
0
Comp.-Type:
PC □
IAC □

Offers (0 Items)

Serial Number	Account Status	Account Type	Login
[redacted]	Konto aktiv	ADSL 300 Classic	jahu13
[redacted]	Konto inaktiv	Bluewin Dial-up Light	janine.h

crm Interactions (12 Items)

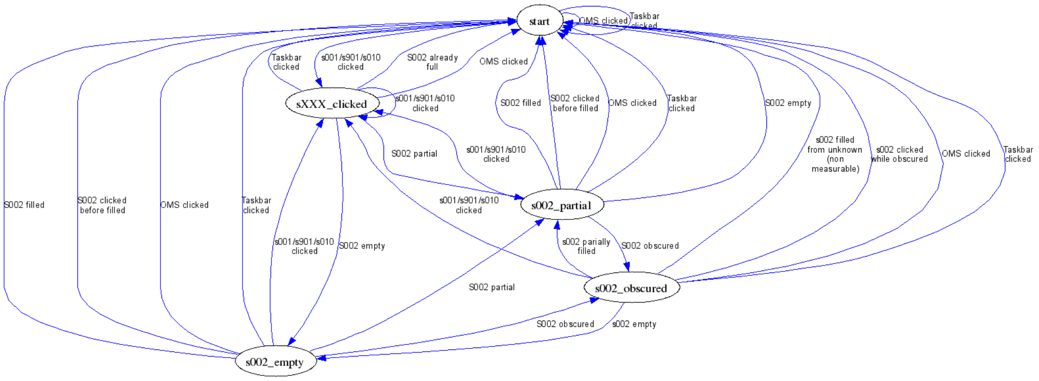
Date Created	No
31.01.2007 13:32:43	
02.10.2006 11:08:09	
16.08.2006 15:06	
10.05.2006 13:	
02.05.2006	
08.04.2006	
21.10.20	
18.10.2	

C:\WINDOWS\system32\cmd.exe - c:\Temp\oms\log\less.exe dem

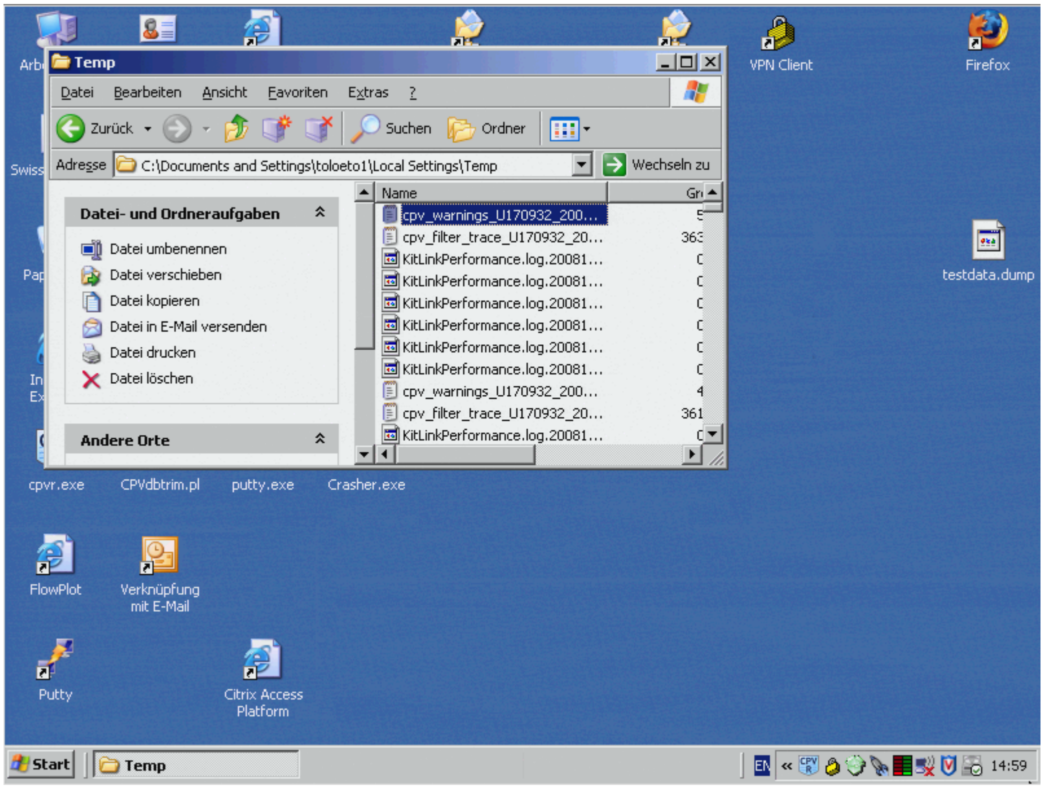
```
2007-02-13 11:58:23.863 1171364303.864 0.001 Click::Wi                   S0
01 - Customer Identification
2007-02-13 11:58:24.190 1171364304.190 0.000 Click::Wind                 S00
1 - Customer Identification
         1:58:24.190 1171364304.191 0.001 Click::WindowCh          _enter
          :25.128 1171364305.129 0.000 Click::WindowChange window_exit
          5.129 1171364305.129 0.001 Click::WindowChange window_enter Hu

          7 1171364305.767 0.001 Click::Vantive::S002 form empty
            1171364309.769 0.001 Click::Vantive::S002 form filled
             1171364315.190 0.000 Click::WindowChange window_exit Hun

              71364315.191 0.001 Click::WindowChange window_enter No

              364315.192 0.000 Click::Clicks click_down_window No
              ):131216
              64315.193 0.001 Click::Clicks click_down_text Ausge

              4316.393 0.000 Click::Clicks click_down_window No
              461356
              4316.394 0.001 Click::Clicks click_down_text No Te

              4316.753 0.000 Click::WindowChange window_exit No
```

```
171364305.767 0.001 Click::Vantive::S002 form empty
171364309.769 0.001 Click::Vantive::S002 form filled
  364315.190 0.000 Click::WindowChange window_exit H
```

lesson #1: complexity trap



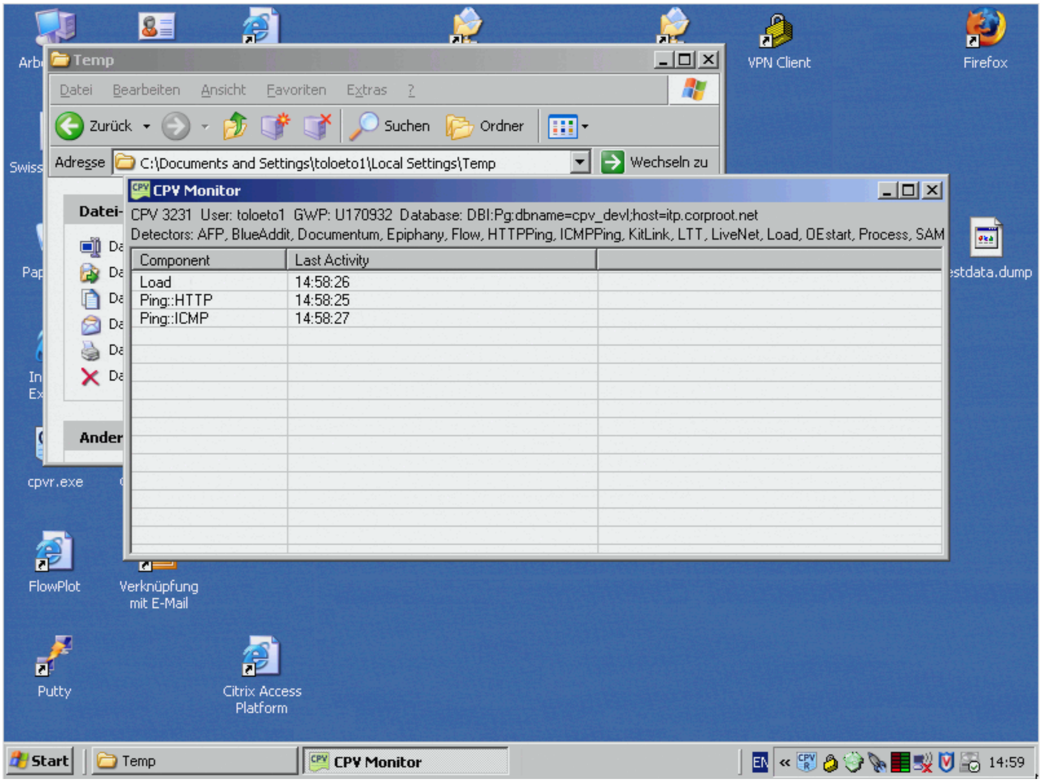
cpv monitor



C:\Documents and Settings\toloeto1\Local Settings\Temp

Name	Gr
cpv_warnings_U170932_200…	5
cpv_filter_trace_U170932_20…	363
KitLinkPerformance.log.20081…	0
KitLinkPerformance.log.20081…	0
KitLinkPerformance.log.20081…	0
KitLinkPerformance.log.20081…	0
KitLinkPerformance.log.20081…	0
KitLinkPerformance.log.20081…	0
cpv_warnings_U170932_200…	4
cpv_filter_trace_U170932_20…	361
KitLinkPerformance.log.20081…	0

cpv monitor monitor

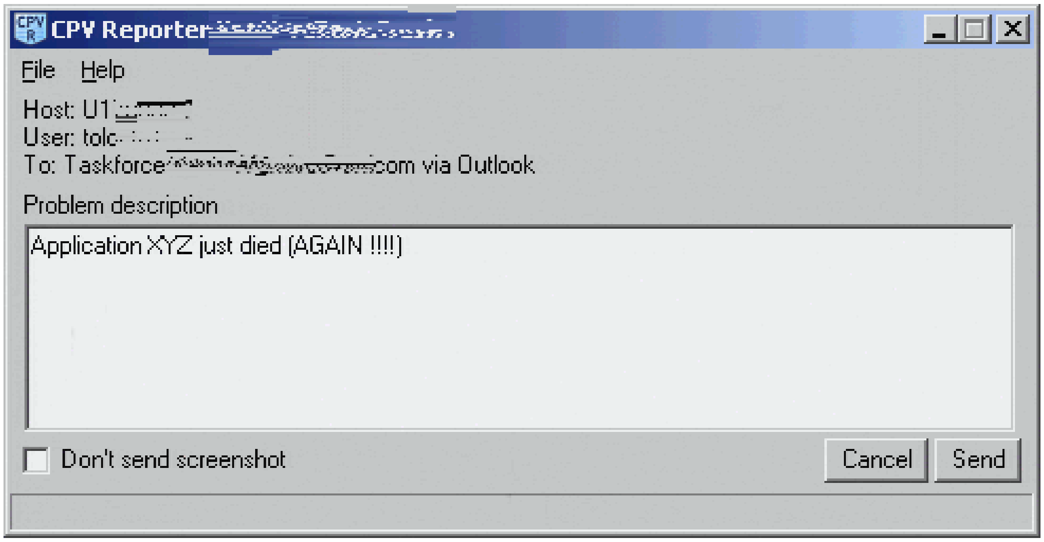


C:\Documents and Settings\toloeto1\Local Settings\Temp

CPV 3231 User: toloeto1 GWP: U170932 Database: DBI:Pg:dbname=cpv_devl;host=itp.corproot.net
Detectors: AFP, BlueAddit, Documentum, Epiphany, Flow, HTTPPing, ICMPPing, KitLink, LTT, LiveNet, Load, OEstart, Process, SAM

Component	Last Activity
Load	14:58:26
Ping::HTTP	14:58:25
Ping::ICMP	14:58:27

cpv reporter



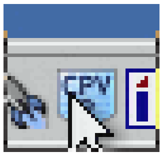
CPV Reporter [redacted]

Host: U1[redacted]
User: tolc[redacted]
To: Taskforce[redacted]com via Outlook

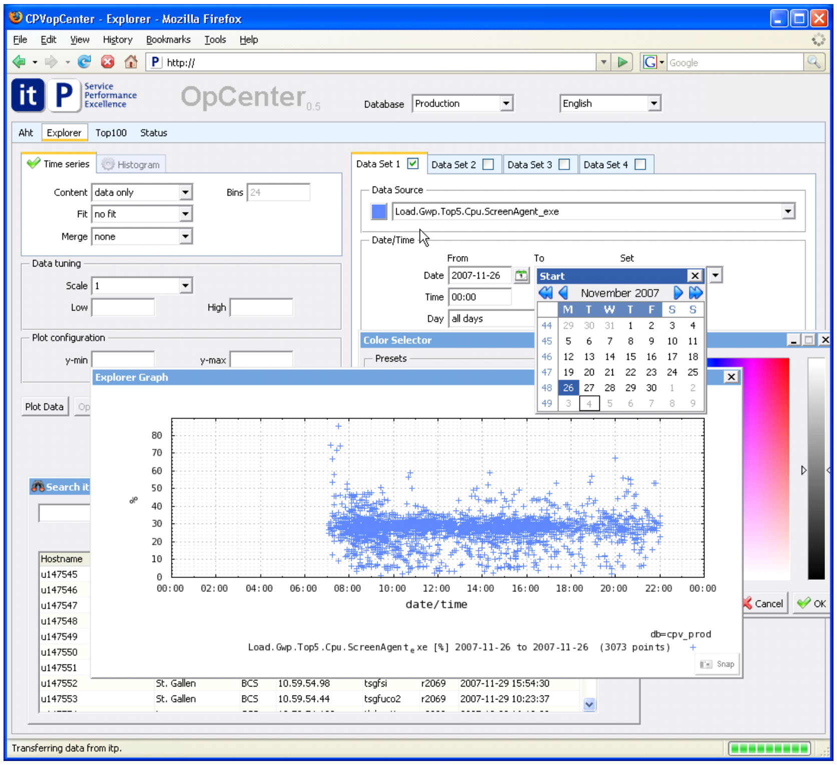
Problem description

Application XYZ just died (AGAIN !!!!)

□ Don't send screenshot



cpv explorer



CPVopCenter - Explorer - Mozilla Firefox

http://

Database: Production
English

Time series

Content: data only
Fit: no fit
Merge: none
Bins: 24

Data tuning
Scale: 1
Low:
High:

Plot configuration
y-min:
y-max:

Data Set 1 ☑ Data Set 2 □ Data Set 3 □ Data Set 4 □

Data Source: Load.Gwp.Top5.Cpu.ScreenAgent_exe

Date/Time

	From	To	Set
Date	2007-11-26		
Time	00:00		
Day	all days		

Start

November 2007

	M	T	W	T	F	S	S
44	29	30	31	1	2	3	4
45	5	6	7	8	9	10	11
46	12	13	14	15	16	17	18
47	19	20	21	22	23	24	25
48	26	27	28	29	30	1	2
49	3	4	5	6	7	8	9

Explorer Graph

db=cpv_prod
Load.Gwp.Top5.Cpu.ScreenAgent$_e$xe [%] 2007-11-26 to 2007-11-26 (3073 points)

Hostname						
u147545						
u147546						
u147547						
u147548						
u147549						
u147550						
u147551						
u147552	St. Gallen	BCS	10.59.54.98	tsgfsi	r2069	2007-11-29 15:54:30
u147553	St. Gallen	BCS	10.59.54.44	tsgfuco2	r2069	2007-11-29 10:23:37

Transferring data from itp.

3 Thinking big

thinking BIG

wants

- $\sim$ 1500 clients in the call-center
- dynamic configuration
- individual profiles

infrastructure

data store : PostgreSQL

configuration : Apache, CPVservice.cgi

analysis : Apache, Qooxdoo, CPVjson.cgi, Gnuplot

4 Observability

observation tools

- GetWindowText and friends
- Reading log files
- Windows WMI (Load, Processes)
- Active Probing (Ping, HTTP)
- HTTPAnalyzer ($$$) for http(s)
- Full Custom Probes

5 It is a learning experience

lesson #2: finding outlook errors

- outlook modal popup send button does not work
- GetAsyncKeyState: Although the least significant bit of the return value indicates whether the key has been pressed since the last query, due to the pre-emptive multitasking nature of Windows, another application can call GetAsyncKeyState and receive the “recently pressed” bit instead of your application. **The behavior of the least significant bit** of the return value is retained strictly for compatibility with 16-bit Windows applications (which are non-preemptive) and **should not be relied upon**.

-
  ```
  GetClassName(WindowFromPoint(GetCursorPos()))
  eq 'MsoCommandBar';
  ```

lesson #3: WMGetText

- GetWindowText or WMGetText
- Application becomes real busy with WMGetText
- stay with GetWindowText

lesson #4: server issues

- 2008-10-27: 1,459 devices sent 2,417,807 samples
- 4 Core / 32-bit / 4 GB ram
- 40 days of data   100,000,000 samples
- index does not fit in ram
- too much data for processing

lesson #5: index compaction

- function based index
- hours since 2007 is good for 7 years with 2 byte
- 2 byte for metric id
- 2 byte for workstation id
- two WHERE conditions

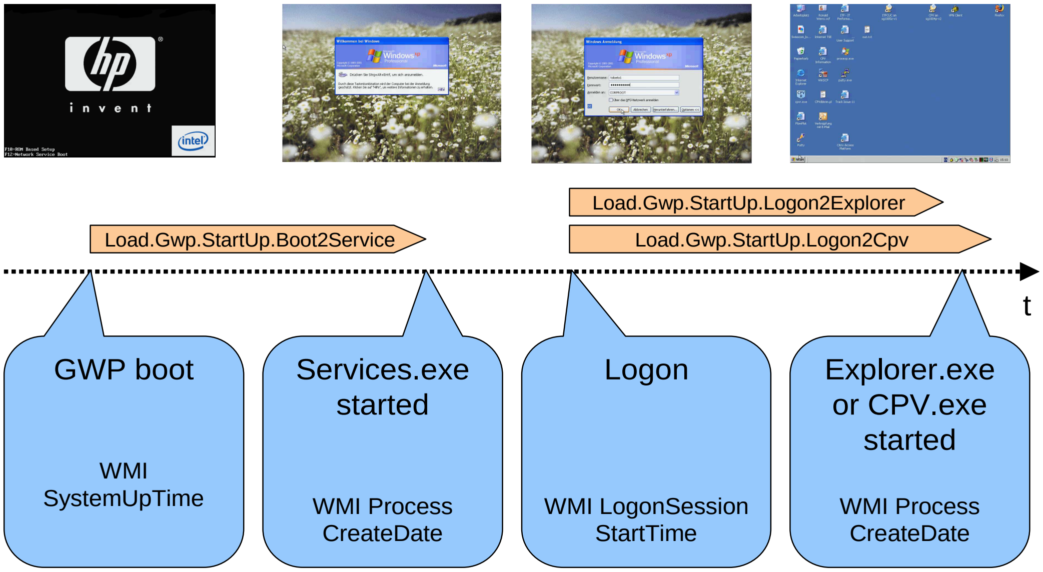
lesson #6: random data reduction

- too much data for statistics
- how to get $12\,\%$ of the samples?
- add 2 byte random value to each sample
- select all sample with $\mathrm{rand} < \mathrm{maxrand}\frac{12}{100}$

lesson #7: threaded perl

- works very well on win32
- full copy — lots of memory
- save require modules after creating the thread
- only thread where really necessary

lesson #8: measuring boot and logon time


Load.Gwp.StartUp.Logon2Explorer
Load.Gwp.StartUp.Boot2Service
Load.Gwp.StartUp.Logon2Cpv
t
GWP boot
WMI SystemUpTime
Services.exe started
WMI Process CreateDate
Logon
WMI LogonSession StartTime
Explorer.exe or CPV.exe started
WMI Process CreateDate

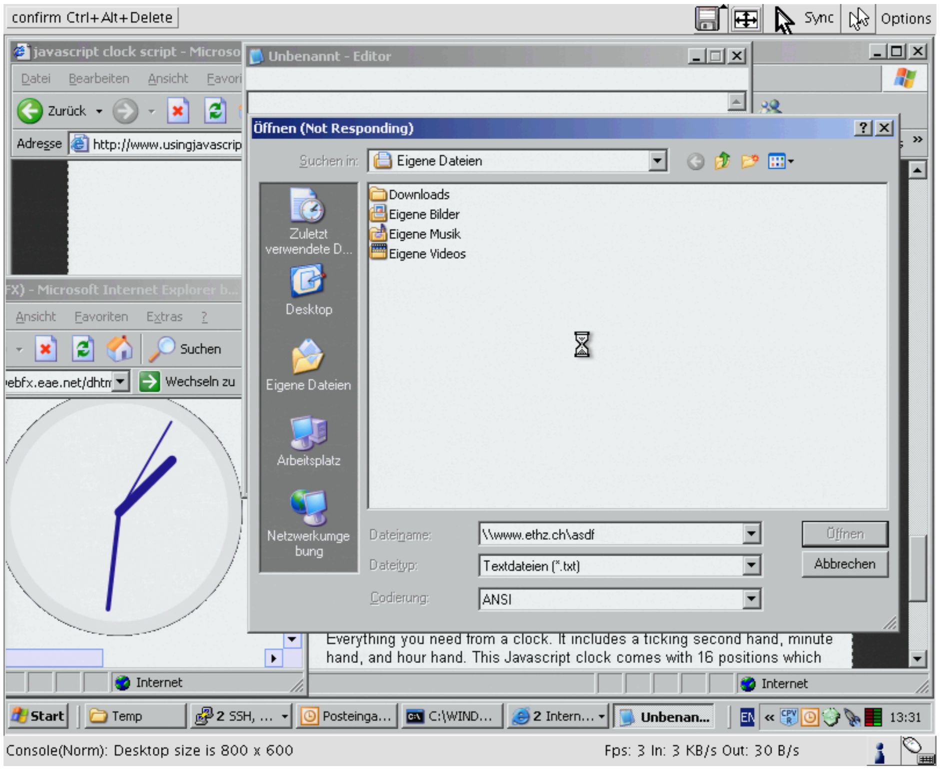
lesson #9: detecting crashes

- no wait but process handle
- no signals only exit codes
- 0xC0000005 - segfault
- 0x00000103 - still running
- `TerminateProcess` can define exit code

Implementation

- find active window
- attach process handle
- poll for exit code

lesson #10: application hangs - symptoms



Öffnen (Not Responding)

Suchen in: Eigene Dateien

Dateiname: \\www.ethz.ch\asdf

Dateityp: Textdateien (*.txt)

Codierung: ANSI

Everything you need from a clock. It includes a ticking second hand, minute hand, and hour hand. This Javascript clock comes with 16 positions which

Console(Norm): Desktop size is 800 x 600

Fps: 3 In: 3 KB/s Out: 30 B/s

lesson #10: application hangs - detection

- dead apps don’t process messages
- explorer fakes responsiveness

Implementation

- find active window
- window ping: SendMessage `WM_NULL`
- wait until the window is back

6 Impact

positive

- CPV reporter - being part of the solution
- CPV explorer - data accessibility
- case: CRM crash detection
- ongoing: webapp monitoring
- structured problem solving
- closed feedback loop
- SLA benchmarks

challenge

- CPV drama triangle - victim / rescuer
- who is begin observed
- mapping the human ways
- side effects
- high observability assumptions

7 Future Work

future work

- DLL injection
- webapps, webapps, webapps
- dealing with the data

Tobi Oetiker <tobi@oetiker.ch> OETIKER+PARTNER AG

Commercial Contact: Claus Henning Simon <ClausHenning.Simon@swisscom.com>
Swisscom IT Services AG