Monitoring Windows Events

(without monitoring Logfiles)

Martin Fürstenau, Oce Printing Systems GmbH & Co. KG

martin.fuerstenau@oce.com

OSMC, November 2019

About me

Out of interest

- Senior System Eningeer at Oce Printing Systems Gmbh & Co. KG in Poing near Munich
- 33 years IT, 30 years Unix, 25 years Linux, 15 years Oce, monitoring started with Netsaint.
- Currently maintaining Linux systems, our monitoring landscape … and writing plugins and addons for NagiosIcinga(2)ShinkenNaemonandotherapicompatibleforks.
- Hobbies: Playing the blues (badly) and repairing electrical guitars (much better).

Oce European Data Center - Monitoring

- Datacenter Océ Printing Systems, Poing
  - European Data Center
  - Local Data Center

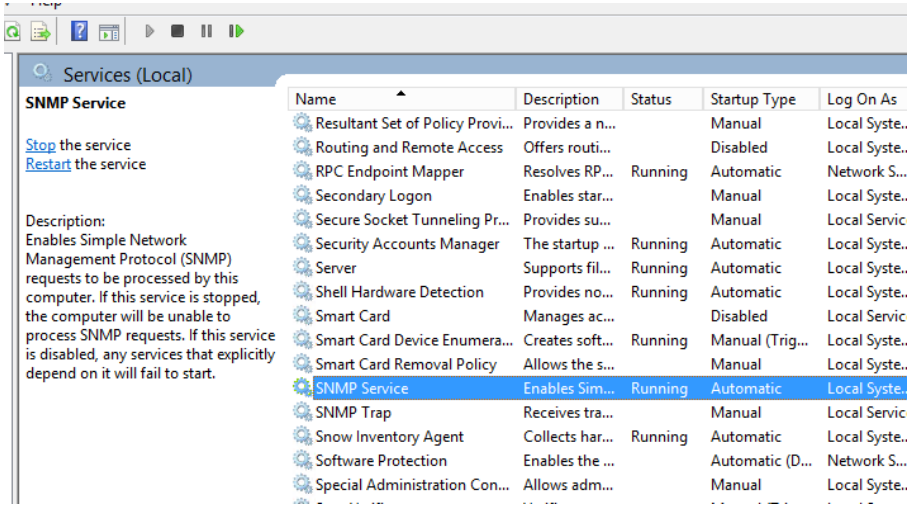
- Our quantity structure
  - 2400 Hosts
    - More than 50 % MS Windows
    - More than 160 network components (Switches, Router,Firewalls)
  - 23500 Services
    - More than ca 50% running on MS Windows
    - Rest is mainly Unix/Linux, SAN, NetApp Filer and network

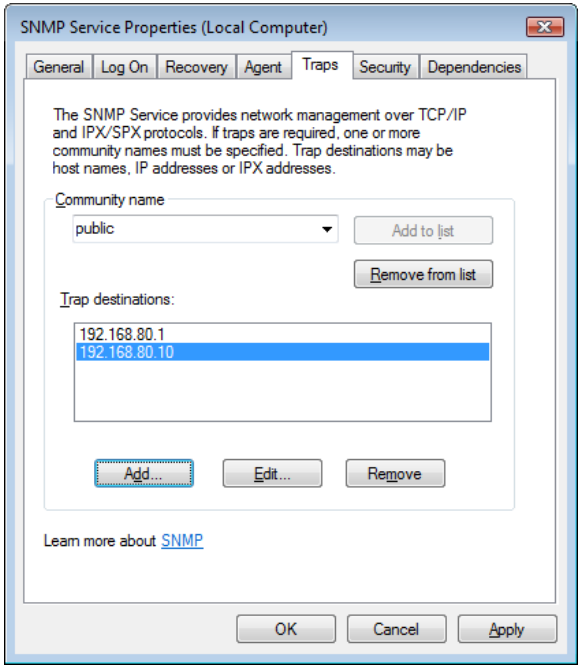
Monitoring Windows Events

- Who needs it?
- And how are you doing it?

Using SNMP traps for Monitoring Windows Events

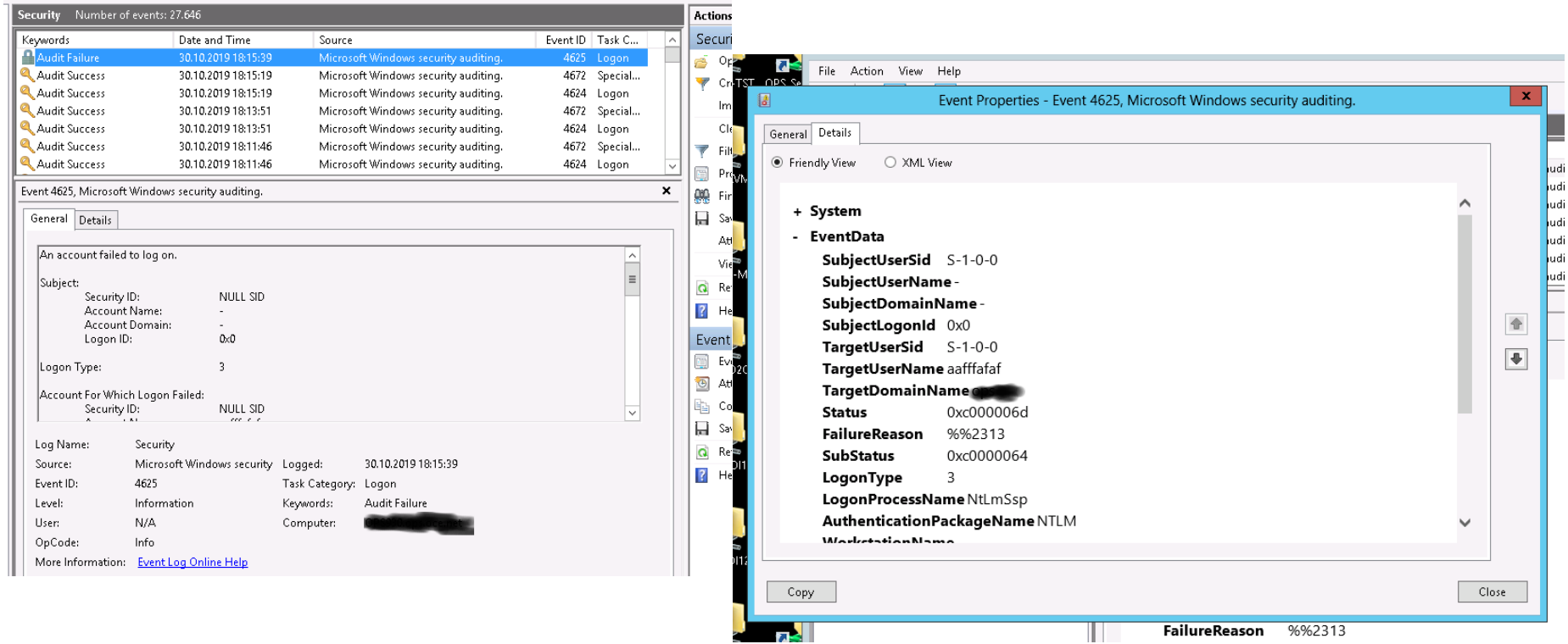
Setting up Windows - Modify your SNMP Configuration





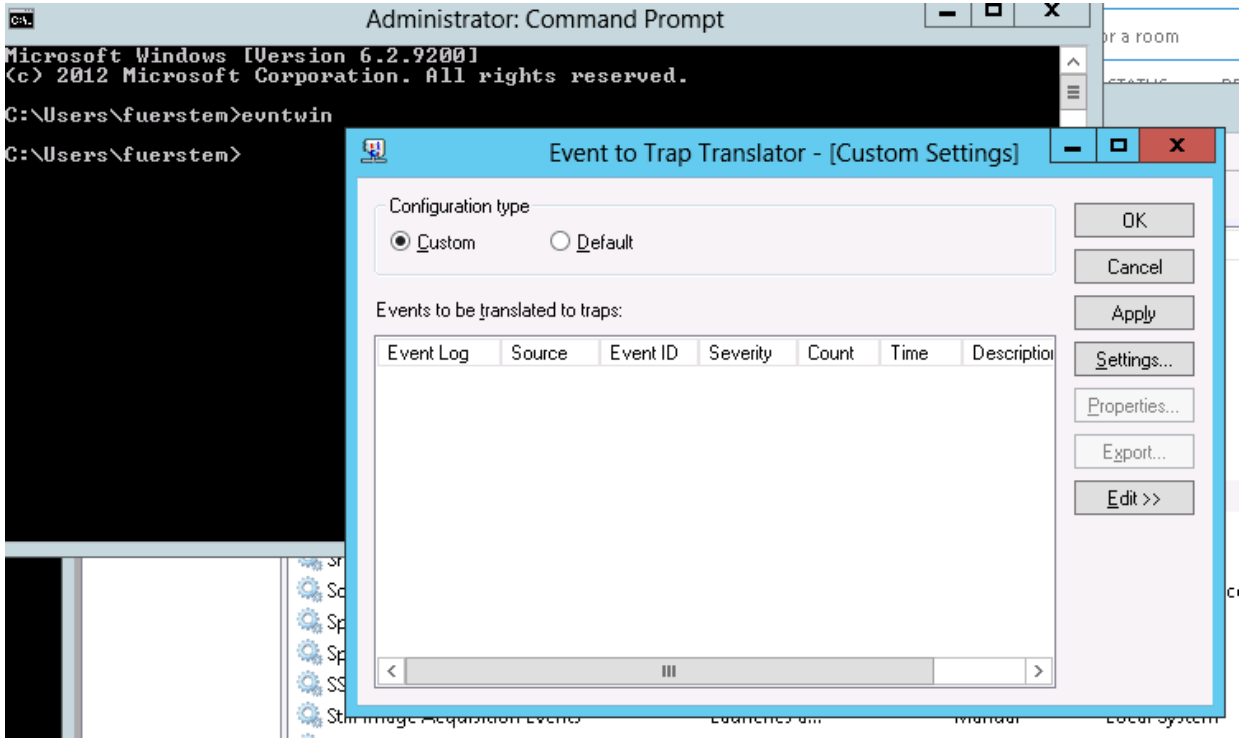
Using SNMP traps for Monitoring Windows Events

An event from the Windows log



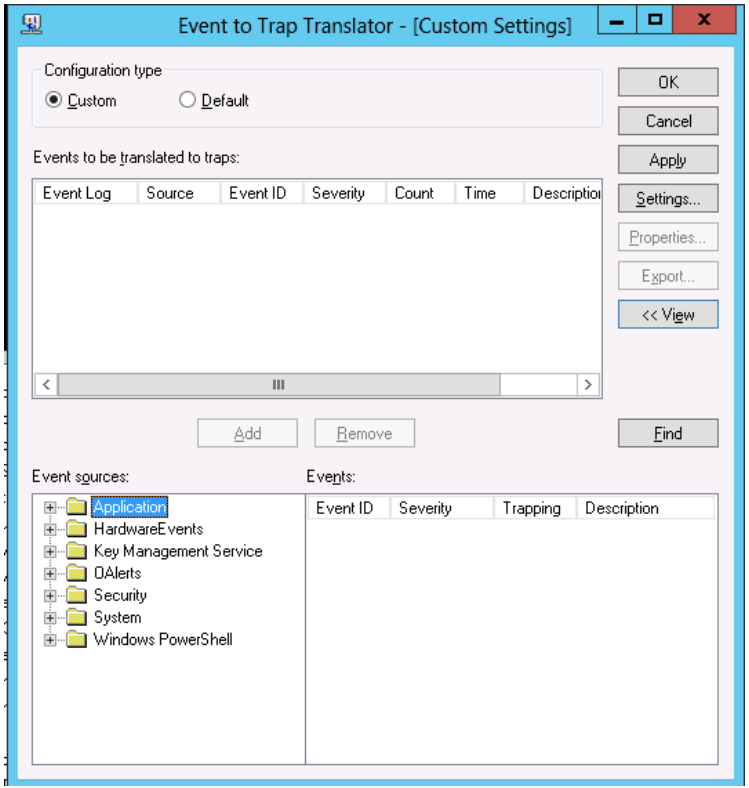
Using SNMP traps for Monitoring Windows Events

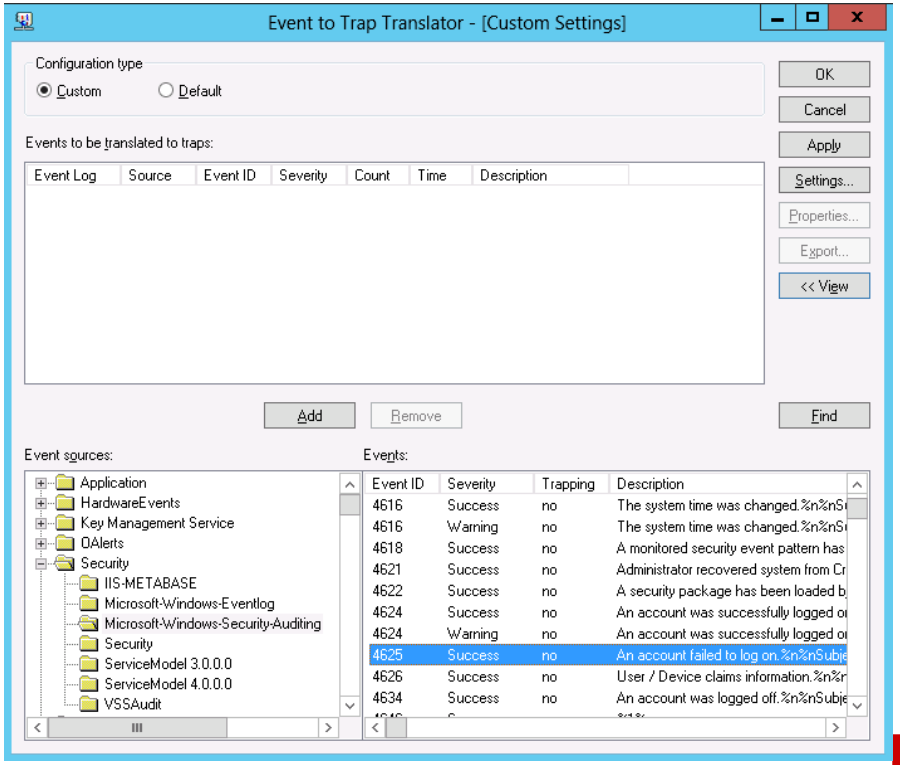
Setting up Windows - Mapping events to traps evntwin and evntcmd



Using SNMP traps for Monitoring Windows Events

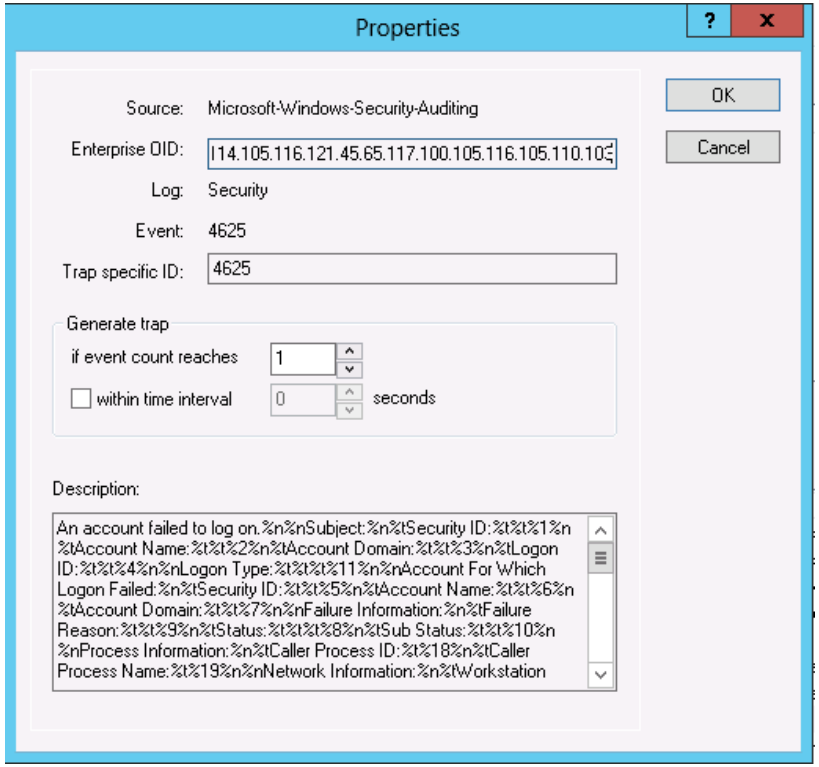
Setting up Windows - Mapping events to traps evntwin and evntcmd

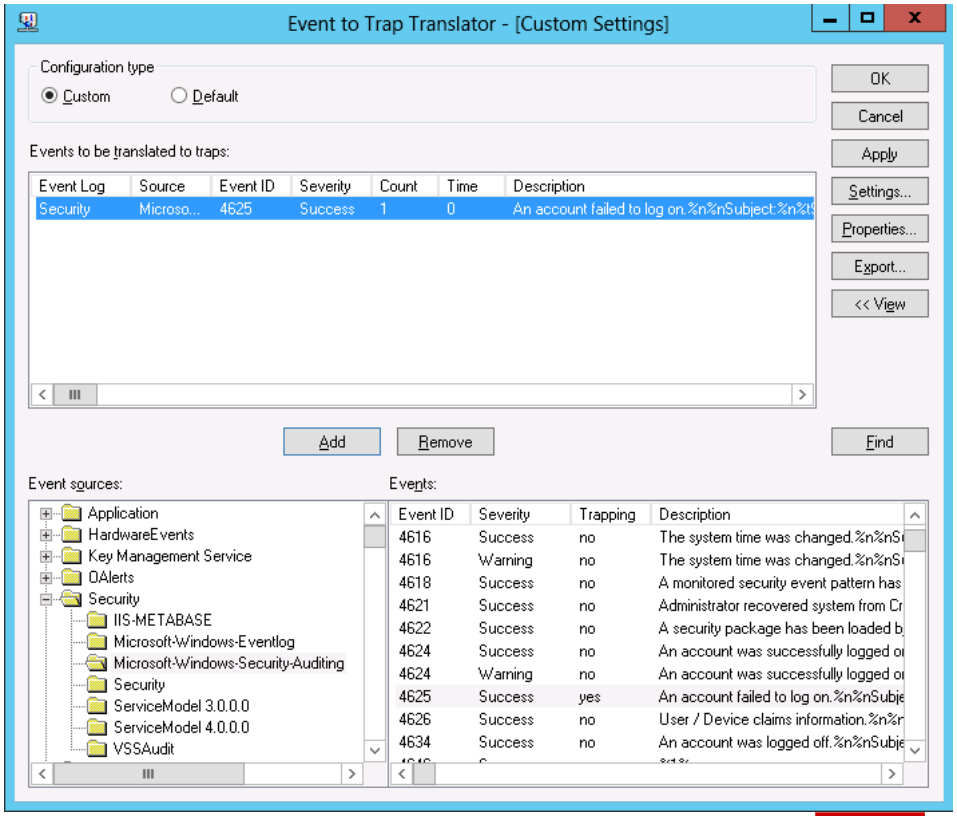




Using SNMP traps for Monitoring Windows Events

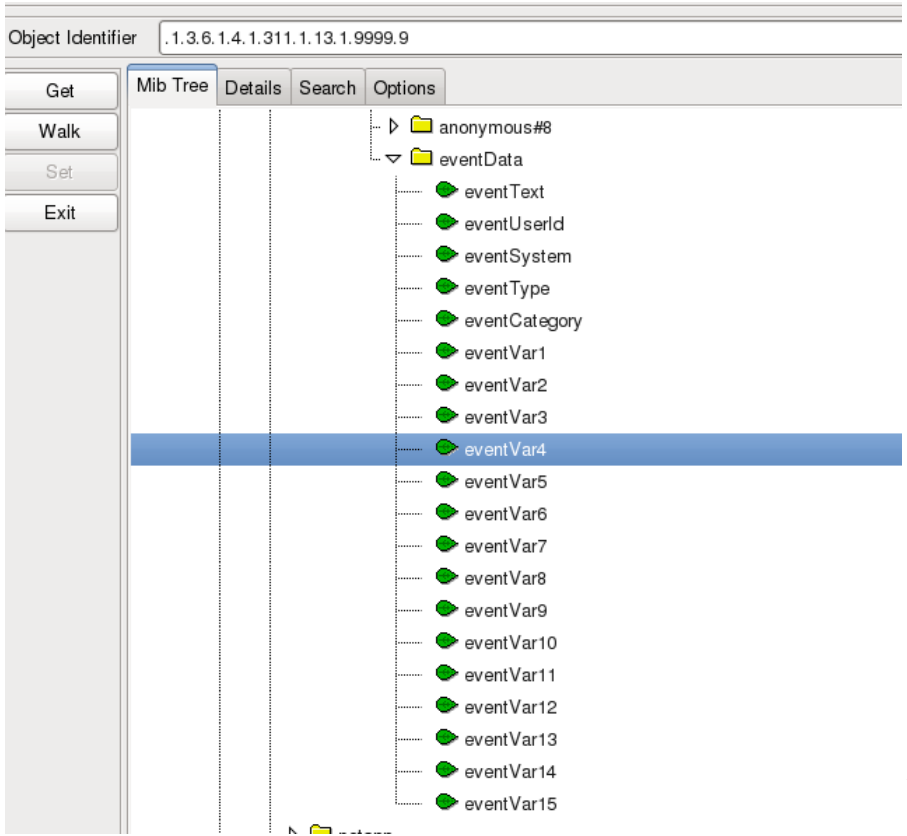
Setting up Windows - Mapping events to traps evntwin and evntcmd





Using SNMP traps for Monitoring Windows Events On the Linux side - a MIB to convert for snmptt ?

- Yes (EVNTAGENT-MIB.mib)
- NO (EVNTAGENT-MIB.mib)



Using SNMP traps for Monitoring Windows Events
On the Linux side - snmptt -snmpttunknown.log

```
Tue Oct 29 18:25:04 2019: Unknown trap (.1.3.6.1.4.1.311.1.13.1.35.77.105.99.114.111.115.111.102.116.45.87.105.110.100.111.119.115.45.83.101.99.117.114.105.116.121.45.65.117.100.105.116.105.110.103.0.4625) received from server_xxxxx at:
Value 0: server_xxxxx
Value 1: 192.168.2.3
Value 2: 18:15:17:56.53
Value 3: .1.3.6.1.4.1.311.1.13.1.35.77.105.99.114.111.115.111.102.116.45.87.105.110.100.111.119.115.45.83.101.99.117.114.105.116.121.45.65.117.100.105.116.105.110.103.0.4625
Value 4: 10.53.12.30
Value 5: public
Value 6: .1.3.6.1.4.1.311.1.13.1.35.77.105.99.114.111.115.111.102.116.45.87.105.110.100.111.119.115.45.83.101.99.117.114.105.116.121.45.65.117.100.105.116.105.110.103
Value 7:
Value 8:
Value 9:
Value 10:
Ent Value 0: .1.3.6.1.4.1.311.1.13.1.9999.1.0=An account failed to log on. <cr> Subject:<cr>    Security ID:           S-1-0-0<cr>    Account Name:          -<cr>   Account Domain:        -<cr>   Logon ID:              0x0<cr> <cr>
Ent Value 1: .1.3.6.1.4.1.311.1.13.1.9999.2.0=Unknown
Ent Value 2: .1.3.6.1.4.1.311.1.13.1.9999.3.0=server_xxxxx.mydomain
Ent Value 3: .1.3.6.1.4.1.311.1.13.1.9999.4.0=16
Ent Value 4: .1.3.6.1.4.1.311.1.13.1.9999.5.0=12544
Ent Value 5: .1.3.6.1.4.1.311.1.13.1.9999.6.0=S-1-0-0
Ent Value 6: .1.3.6.1.4.1.311.1.13.1.9999.7.0=-
Ent Value 7: .1.3.6.1.4.1.311.1.13.1.9999.8.0=-
Ent Value 8: .1.3.6.1.4.1.311.1.13.1.9999.9.0=0x0
Ent Value 9: .1.3.6.1.4.1.311.1.13.1.9999.10.0=S-1-0-0
Ent Value 10: .1.3.6.1.4.1.311.1.13.1.9999.11.0=aafffafaf
Ent Value 11: .1.3.6.1.4.1.311.1.13.1.9999.12.0=ops
Ent Value 12: .1.3.6.1.4.1.311.1.13.1.9999.13.0=0xc000006d
Ent Value 13: .1.3.6.1.4.1.311.1.13.1.9999.14.0=Unknown user name or bad password.
Ent Value 14: .1.3.6.1.4.1.311.1.13.1.9999.15.0=0xc0000064
Ent Value 15: .1.3.6.1.4.1.311.1.13.1.9999.16.0=3
Ent Value 16: .1.3.6.1.4.1.311.1.13.1.9999.17.0=NtLmSsp
Ent Value 17: .1.3.6.1.4.1.311.1.13.1.9999.18.0=NTLM
Ent Value 18: .1.3.6.1.4.1.311.1.13.1.9999.19.0=
Ent Value 19: .1.3.6.1.4.1.311.1.13.1.9999.20.0=-
Ent Value 20: .1.3.6.1.4.1.311.1.13.1.9999.21.0=-
Ent Value 21: .1.3.6.1.4.1.311.1.13.1.9999.22.0=0
Ent Value 22: .1.3.6.1.4.1.311.1.13.1.9999.23.0=0x0
Ent Value 23: .1.3.6.1.4.1.311.1.13.1.9999.24.0=-
Ent Value 24: .1.3.6.1.4.1.311.1.13.1.9999.25.0=-
Ent Value 25: .1.3.6.1.4.1.311.1.13.1.9999.26.0=-
```

Using SNMP traps for Monitoring Windows Events
On the Linux side - a 1st configuration for snmptt

```
EVENT LoginDenied .1.3.6.1.4.1.311.1.13.1.35.77.105.99.114.111.115.111.102.116.45.87.105.110.100.111.119.115.45.83.101.99.117.114.105.116.121.45.65.117.100.105.116.105.110.103.0.4625 "Status Events" Normal
FORMAT FooFooFoo $*
SDESC
Get the traps from the event system
Variables:
EDESC
```

```
Tue Oct 29 18:36:17 2019
.1.3.6.1.4.1.311.1.13.1.35.77.105.99.114.111.115.111.102.116.45.87.105.110.100.111.119.115.45.83.101.99.117.114.105.116.121.45.65.117.100.105.116.105.110.103.0.4625
Normal "Status Events"server_xxxxx - FooFooFoo An account failed to log on. <cr> Subject:<cr>   Security ID:            S-1-0-0<cr>     Account Name:
-<cr>   Account Domain:         -<cr>   Logon ID:               0x0<cr> <cr> Logon Type:                        3<cr> <cr> Account For Which Logon Failed:<cr>
Security ID:          S-1-0-0<cr>     Account Name:           aafffafaf<cr>   Account Domain:         ops<cr> <cr> Failure Information:<cr>   Failure Reason:
Unknown user name or bad password.<cr> <cr>     Status:                 0xc000006d<cr>  Sub Status:             0xc0000064<cr> <cr> Process Information:<cr>
Caller Process ID:      0x0<cr>         Caller Process Name:    -<cr> <cr> Network Information:<cr>     Workstation Name:       <cr>    Source Network Address:
-<cr>   Source Port:           -<cr> <cr> Detailed Authentication Information:<cr>     Logon Process:          NtLmSsp <cr>    Authentication Package: NTLM<cr>
Transited Services:     -<cr>   Package Name (NTLM only):       -<cr>   Key Length:               0<cr> <cr> This event is generated when a logon request fails. It is
generated on the computer where access was attempted.<cr> <cr> The Subject fields indicate the account on the local system which requested the logon. This is most
commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.<cr> <cr> The Logon Type field indicates the kind of logon
that was requested. The most common types are 2 (interactive) and 3 (network).<cr> <cr> The Process Information fields indicate which account and process on the
system requested the logon.<cr> <cr> The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and
may be left blank in some cases.<cr> <cr> The authentication information fields provide detailed information about this specific logon request.<cr>     - Transited
services indicate which intermediate services have participated in this logon request.<cr>      - Package name indicates which sub-protocol was used among the NTLM
protocols.<cr>  - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.<cr>  Unknown,server_xxxxx.ops.oce.net
16 12544 S-1-0-0 - - 0x0 S-1-0-0 aafffafaf ops 0xc000006d Unknown user name or bad password.  0xc0000064 3 NtLmSsp  NTLM  - - 0 0x0 - - -
```

Using SNMP traps for Monitoring Windows Events
On the Linux side - a 2nd configuration for snmptt

```
EVENT LoginDenied  .1.3.6.1.4.1.311.1.13.1.35.77.105.99.114…….
EXEC /root/work.duck/wintrap/duck "$1" "$2" "$3" "$4" "$5" "$6" "$7" "$8" "$9"
FORMAT FooFooFoo $*
SDESC
Get the traps from the event system
Variables:
EDESC
```

```
#!/bin/bash

echo  >> /root/work.duck/wintrap/duck.log
echo  >> /root/work.duck/wintrap/duck.log
echo  >> /root/work.duck/wintrap/duck.log
echo "1: $1" >> /root/work.duck/wintrap/duck.log
echo "2: $2" >> /root/work.duck/wintrap/duck.log
echo "3: $3" >> /root/work.duck/wintrap/duck.log
echo "4: $4" >> /root/work.duck/wintrap/duck.log
echo "5: $5" >> /root/work.duck/wintrap/duck.log
echo "6: $6" >> /root/work.duck/wintrap/duck.log
echo "7: $7" >> /root/work.duck/wintrap/duck.log
echo "8: $8" >> /root/work.duck/wintrap/duck.log
echo "9: $9" >> /root/work.duck/wintrap/duck.log
```

océ
A CANON COMPANY

Using SNMP traps for Monitoring Windows Events
On the Linux side - a 2nd configuration for snmptt

```
1: An account failed to log on. <cr> Subject:<cr>       Security ID:           S-1-0-0<cr>     Account Name:
2: Unknown
3: server_xxxxx.mydomain
4: 16
5: 12544
6: S-1-0-0
7: -
8: -
9: 0x0
```

Using SNMP traps for Monitoring Windows Events
On the Linux side - a 3rd configuration for snmptt

```
EVENT LoginDenied  .1.3.6.1.4.1.311.1.13.1.35.77.105….
FORMAT FooFooFoo $*
EXEC /root/work.duck/wintrap/log_wintrap --logfile=/root/work.duck/wintrap/duck.log --
eventText="$1" --eventUserId="$2" --eventSystem="$3" --eventType="$4" --eventCategory="$5"
--eventVar1="$6" --eventVar2="$7" --eventVar3="$8" --eventVar4="$9" --eventVar5="$10" --
eventVar6="$11" --eventVar7="$12" --eventVar8="$13" --eventVar9="$14" --eventVar10="$15" --
eventVar11="$16" --eventVar12="$17" --eventVar13="$18" --eventVar14="$19" --eventVar15="$20"
SDESC
Get the traps from the event system
Variables:
EDESC
```

Using SNMP traps for Monitoring Windows Events
On the Linux side - a 3rd logfile for snmptt

```
eventSystem: server_xxxxxxx
eventText: An account failed to log on.
 Subject:
        Security ID:            S-1-0-0
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

 Logon Type:                    3

 Account For Which Logon Failed:
        Security ID:            S-1-0-0
        Account Name:           aafffafaf
        Account Domain:         ops

 Failure Information:
        Failure Reason:         Unknown user name or bad password.

        Status:                 0xc000006d
        Sub Status:             0xc0000064

 Process Information:
        Caller Process ID:      0x0
        Caller Process Name:    -

 Network Information:
        Workstation Name:
        Source Network Address: -
        Source Port:            -

 Detailed Authentication Information:
        Logon Process:          NtLmSsp
        Authentication Package: NTLM
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0

 This event is generated when a logon request fails. It is generated on the computer where access was attempted.

 The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server

 The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).

 The Process Information fields indicate which account and process on the system requested the logon.

 The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left

 The authentication information fields provide detailed information about this specific logon request.
        - Transited services indicate which intermediate services have participated in this logon request.
        - Package name indicates which sub-protocol was used among the NTLM protocols.
        - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

eventType: 16
eventUserId: Unknown
eventVar1: S-1-0-0
eventVar2: -
eventVar3: -
eventVar4: 0x0
eventVar5: S-1-0-0
eventVar6: aafffafaf
eventVar7: ops
eventVar8: 0xc000006d
eventVar9: Unknown user name or bad password.
eventVar10: 0xc0000064
eventVar11: 3
```

How to proceed

wintrap2mon

- Will contain filter for each variable
- Should handle most events
- Should be expandable by adding filters from files
- Option to write all variables to logfile

Resources

- http://www.snmptt.org
- https://docs.microsoft.com/en-us/windows/win32/snmp/about-snmp
- https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/evntcmd
- https://wiki.opennms.org/wiki/Windows_Event_Log_Traps
- https://support.microsoft.com/de-de/help/324263/how-to-configure-the-simple-network-management-protocol-snmp-service-i
- https://documentation.commvault.com/commvault/v11_sp5/article?p=features/alerts/setup_alerts_snmp_trap.htm

Resources

- http://www.snmptt.org
- https://docs.microsoft.com/en-us/windows/win32/snmp/about-snmp
- https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/evntcmd
- https://wiki.opennms.org/wiki/Windows_Event_Log_Traps
- https://support.microsoft.com/de-de/help/324263/how-to-configure-the-simple-network-management-protocol-snmp-service-i
- https://documentation.commvault.com/commvault/v11_sp5/article?p=features/alerts/setup_alerts_snmp_trap.htm

Thank you for you patience with an old man

and

let’s have a drink now

(and a second, and a third and a……)


océ
A CANON COMPANY