ENGLISH

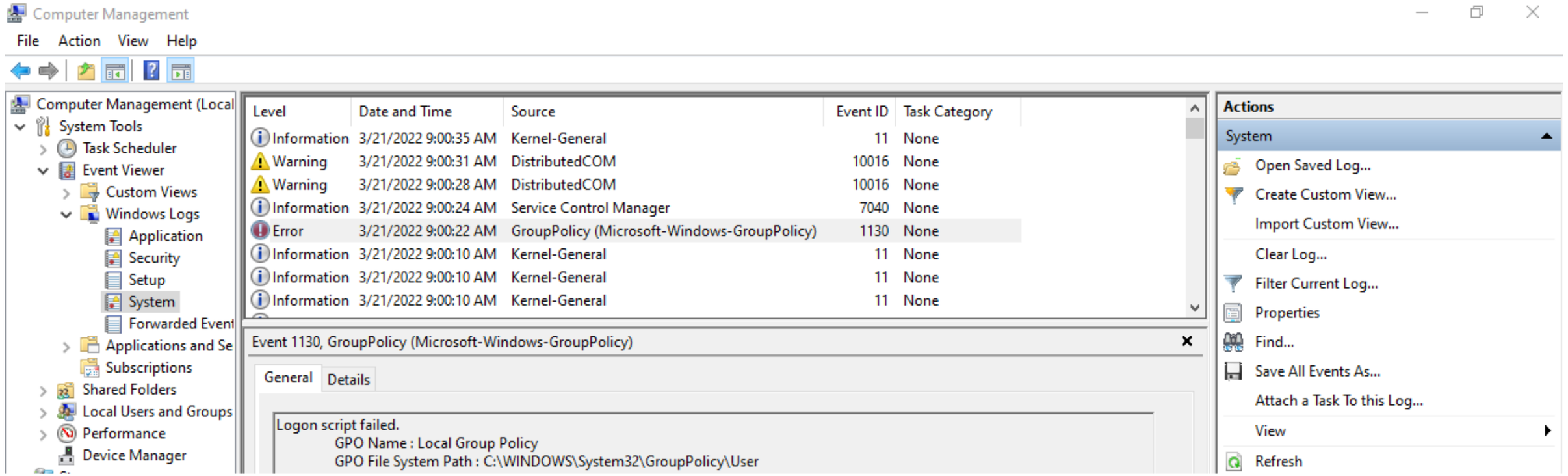
ZABBIX MEETUP ONLINE '22

Eventlog monitoring

Aigars Kadiķis
Technical Support Engineer
Zabbix

WHY EVENT LOG MONITORING

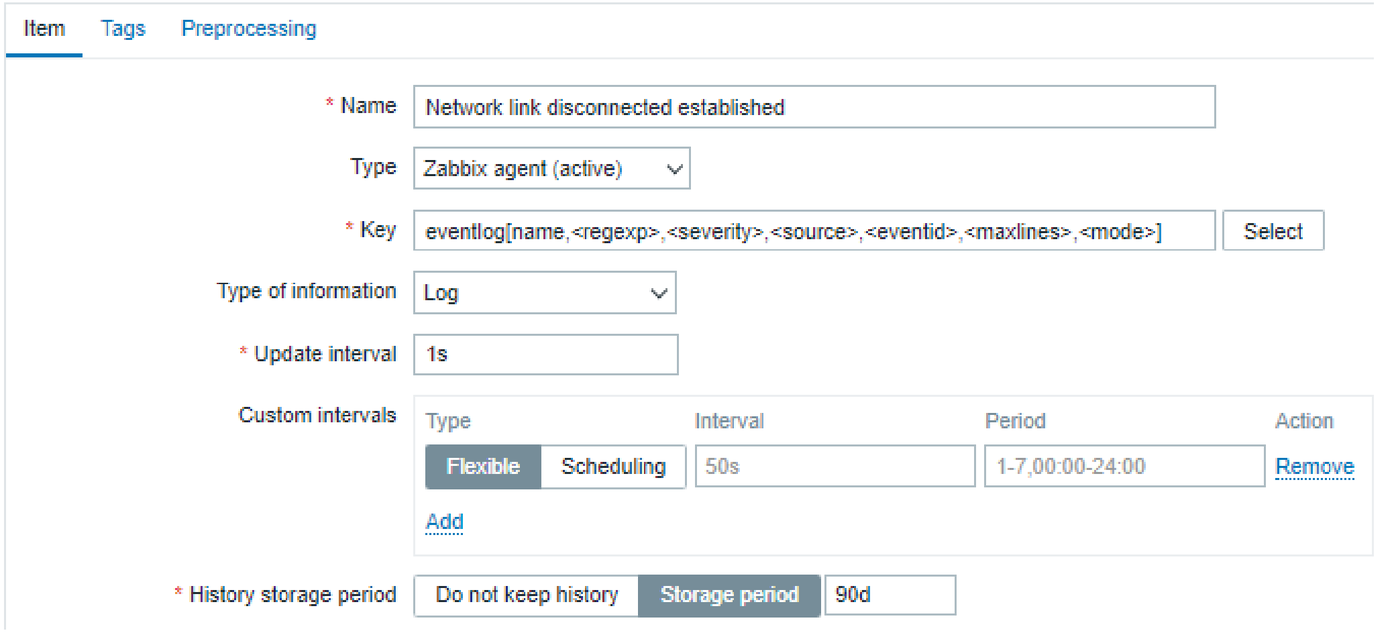
- Capture events by Source, Eventid, Severity
- Most of the applications writes into Windows eventlog
- Can analyze in retrospect



DEPENDENCIES

- Zabbix agent or Zabbix agent 2 is required
- Type «Zabbix agent (active)» must be used. Pushing information to server
- Must reach TCP 10051 on central Zabbix server (or Zabbix proxy)
- Type of information: «Log»
- More frequent checks up to «1s»
- Minimal permissions:

  User group «Event Log Readers»



HOW TO INSTALL ZABBIX AGENT

- MSI install:

```
SET INSTALLFOLDER=C:\Program Files\Zabbix Agent 2
msiexec /l*v log.txt /i "%~dp0zabbix_agent2-6.0.0-windows-amd64-openssl.msi" /qb^
 LOGTYPE=file^
 LOGFILE="%INSTALLFOLDER%\zabbix_agent2.log"^
 SERVER=10.1.10.99^
 SERVERACTIVE=10.1.10.99 ^
 HOSTNAME=%computername%.contoso.lan^
 ENABLEPATH=1^
 INSTALLFOLDER="%INSTALLFOLDER%"
```

- Manual install:

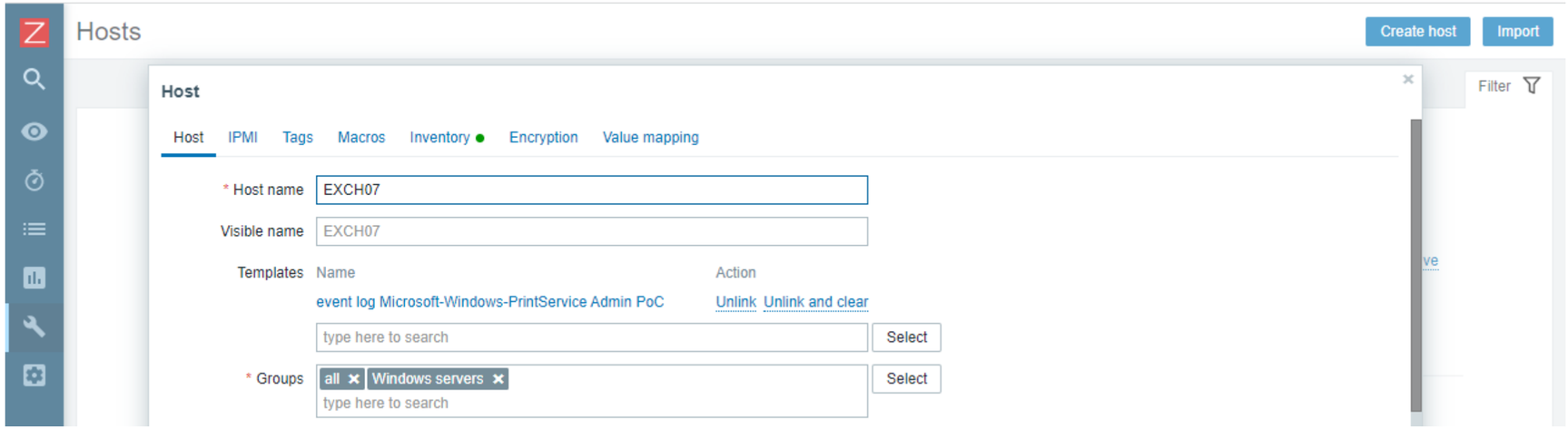
```
c:\zabbix\zabbix_agent2.exe -c c:\zabbix\zabbix_agent2.conf -install
```

ACTIVE CHECKS ONLY

- Zabbix agent configuration (C:\zabbix\zabbix_agentd.conf):

```
Hostname=EXCH07
```

- Must match the configuration for the Host object:



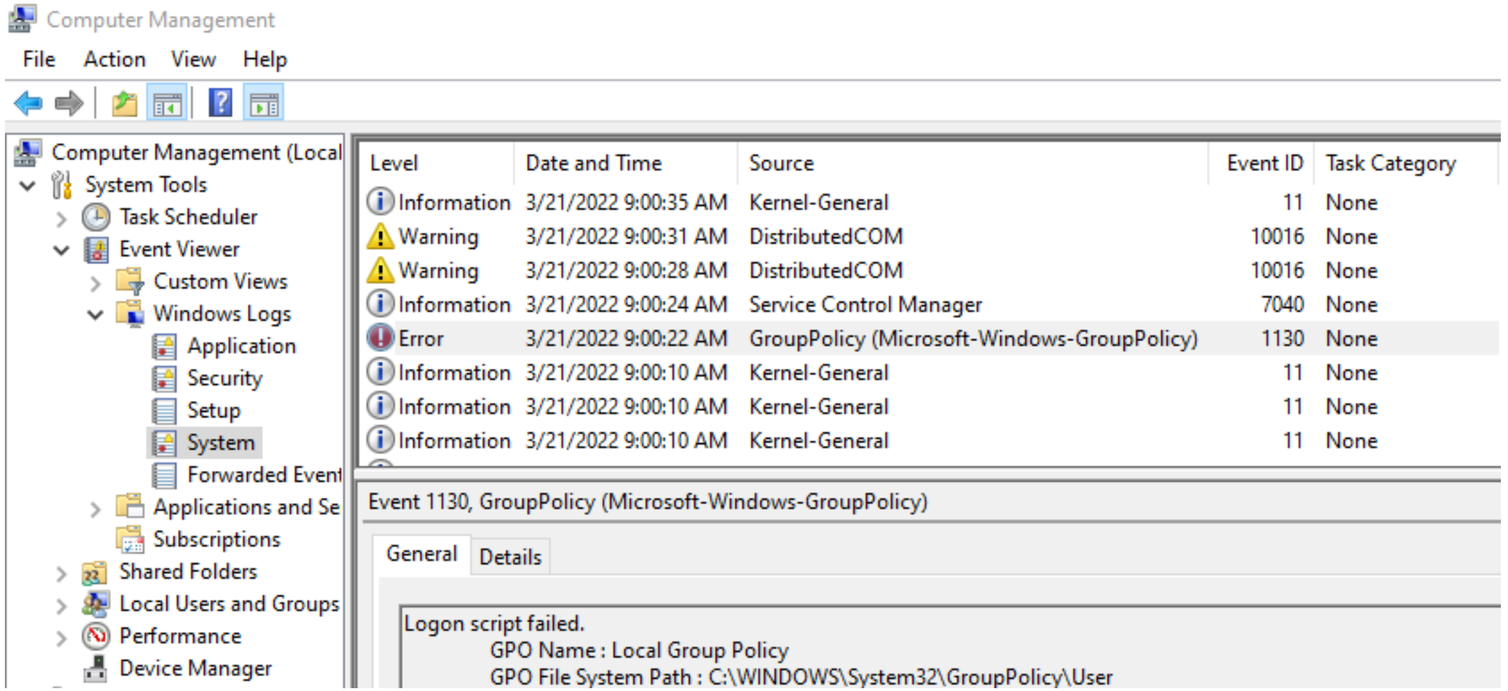
- Make sure no “Cannot send list of active checks” lines are listed in zabbix_server.log:

```
grep "cannot send list of active checks" /var/log/zabbix/zabbix_server.lo
1167209:20220323:093445.245 cannot send list of active checks to "10.1.17.46": host [EXCH07]
not found
```

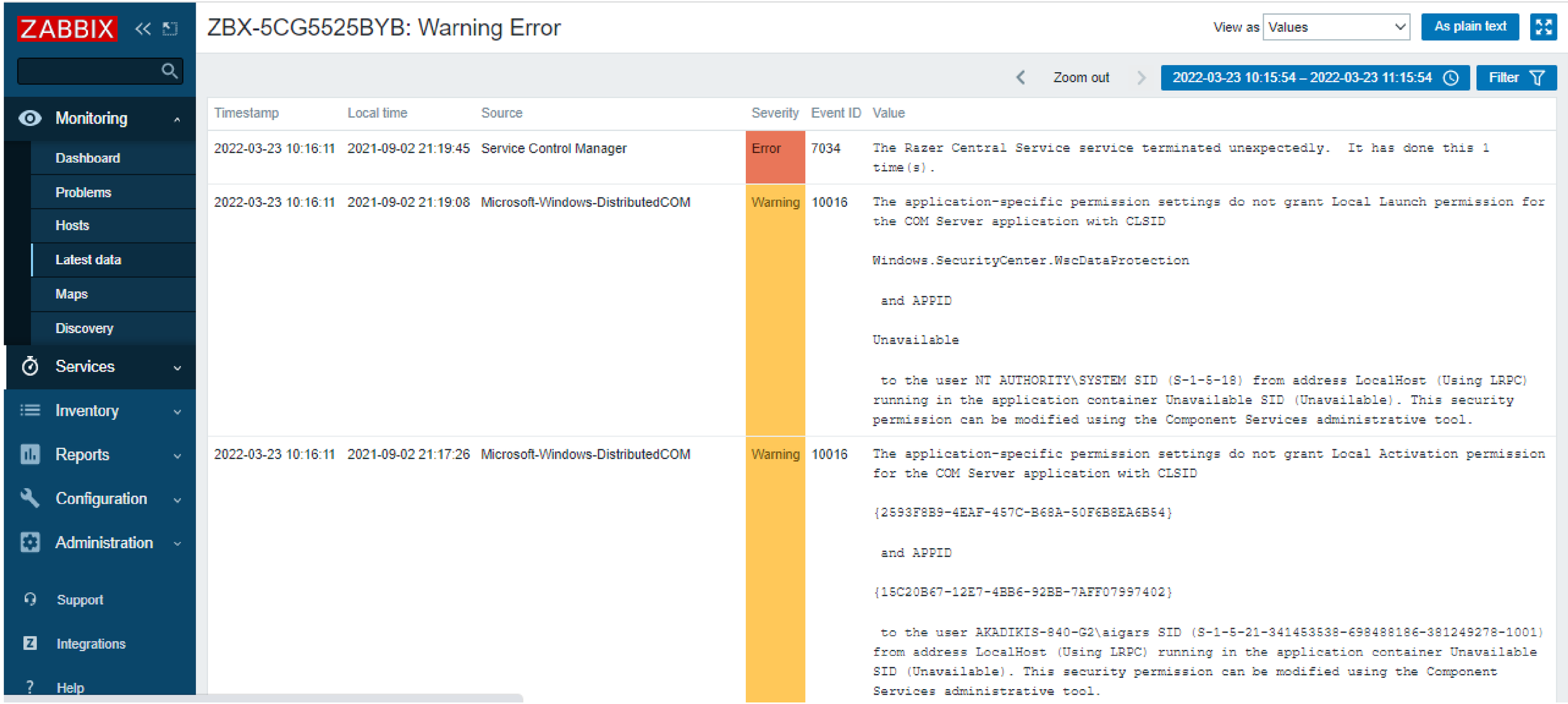
DEDICATED ITEM KEY

eventlog[name,<regexp>,<severity>,<source>,<eventid>,<maxlines>,<mode>]

- name – Application, Security, Setup, System
- <regex> - seek for specific log message
- <severity> - can be “Critical”, “Error”, “Warning”, “Information”
- <eventid> - Event ID
- <maxlines> - 20 by default
- <mode> - can start from now by using “skip” argument



DATA IN ZABBIX



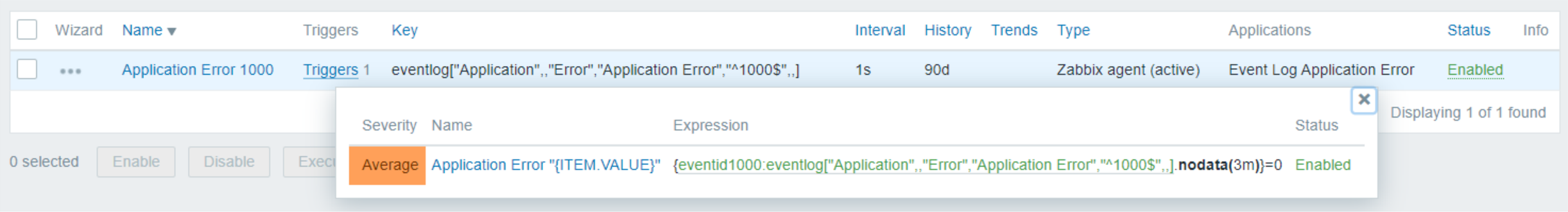
ZABBIX

WINDOWS EVENTLOG MONITORING

MONITORING APPROACHES

APPROACH 1 – EASY

- Detect entries by eventid
- Will timeout automatically



Pros:

- Very easy to setup. Find the Event ID and configure it

Cons:

- Not suitable when 50+ event IDs collected per one server

  CPU usage will increase for the client

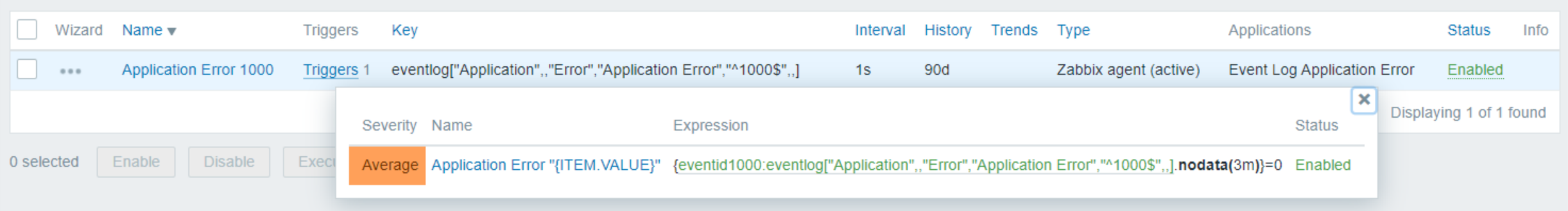
APPROACH 1 – EASY

- Syntax of <eventid>:

^1000$ required to match only «1000» but not match «10000» or «11000»

^ - beginning of string

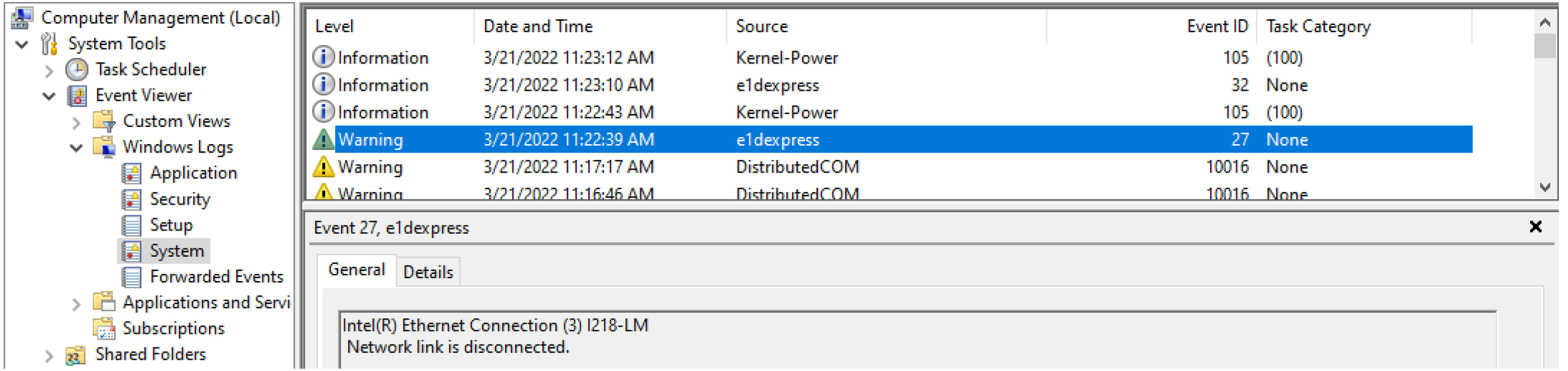
$ - end of string



APPROACH 2 – KNOW PROBLEM ID & RECOVERY ID

- Networ link is disconnected.

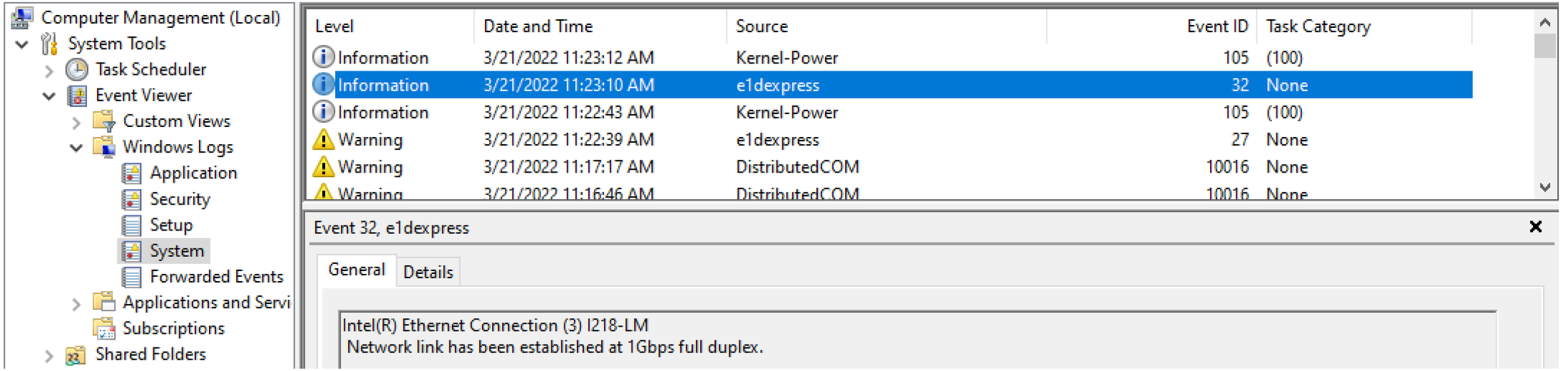
  Source: e1dexpress; Event ID: 27



APPROACH 2 – KNOW PROBLEM ID & RECOVERY ID

- Network link has been established at 1Gbps full duplex.

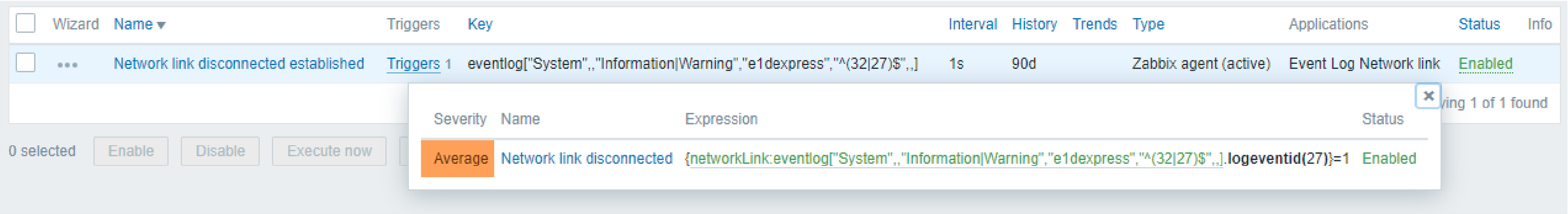
  Source: e1dexpress; Event ID: 32



APPROACH 2 – KNOW PROBLEM ID & RECOVERY ID

Implementation:

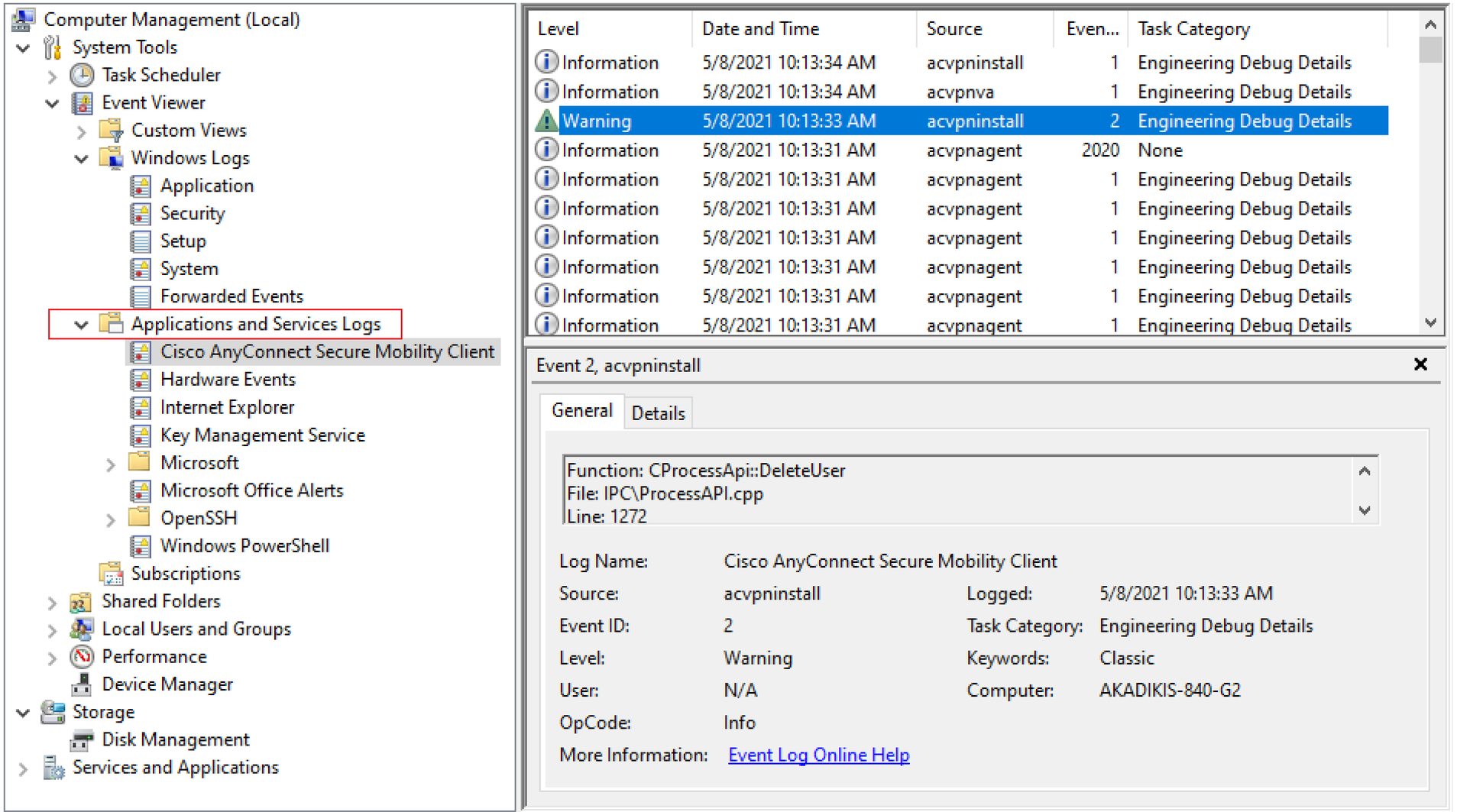
- Item collects both «categories» : 32 and 27
- Event is genereted when «27» arrives. Automatically closes when «another» event comes.



- ^(32|27)$ required to match only «32» or «27». NOT match «3232», «3200», «327», ..

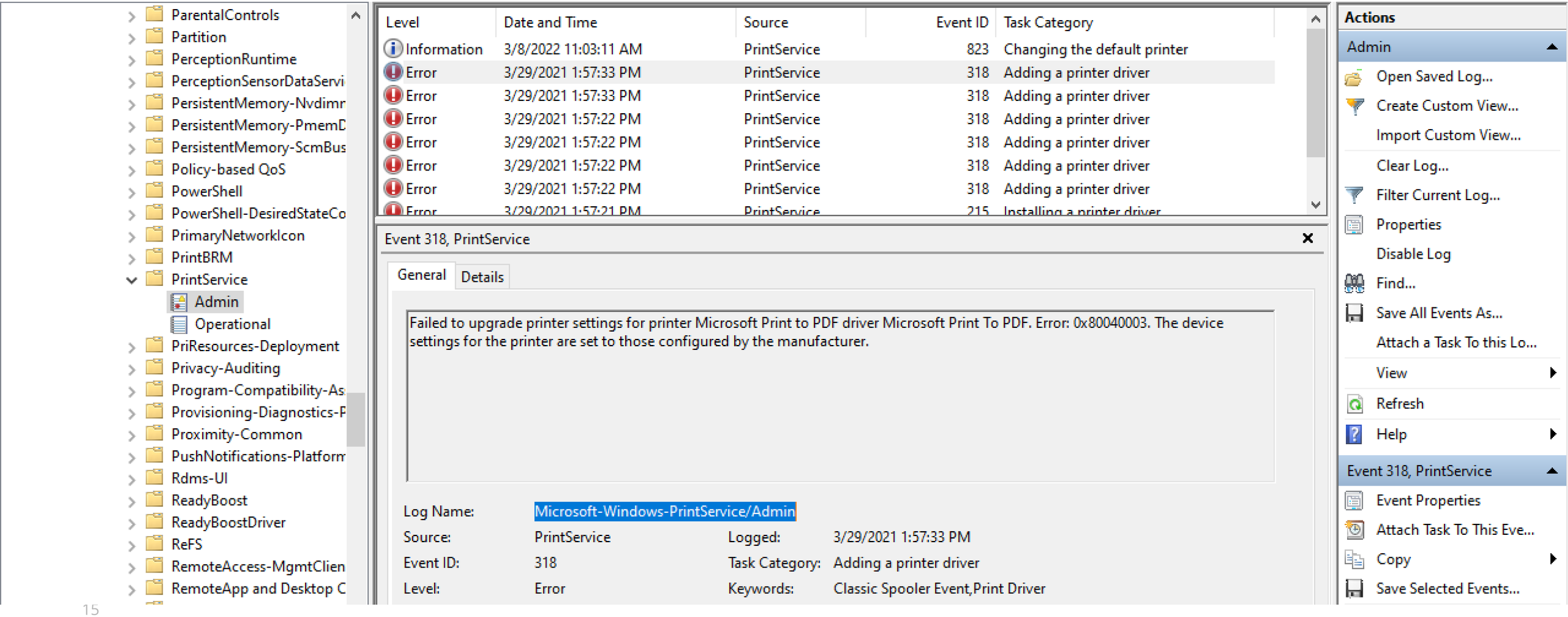
APPROACH 3 – COLLECT EVERYTHING FROM ONE SOURCE

Explore «Applications and Services Logs» registry:



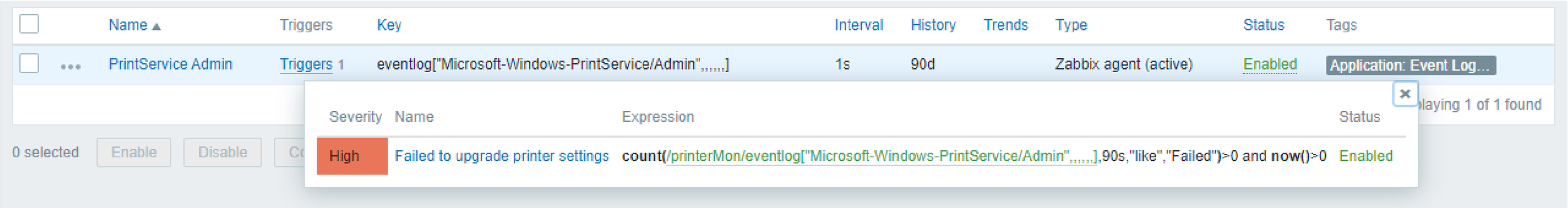
APPROACH 3 – COLLECT EVERYTHING FROM ONE SOURCE

Find the application you want to monitor. Copy the «Log Name» to clipboard:



APPROACH 3 – COLLECT EVERYTHING FROM ONE SOURCE

- Send all lines to Zabbix
- Aggregate triggers on-the-fly



Pros:

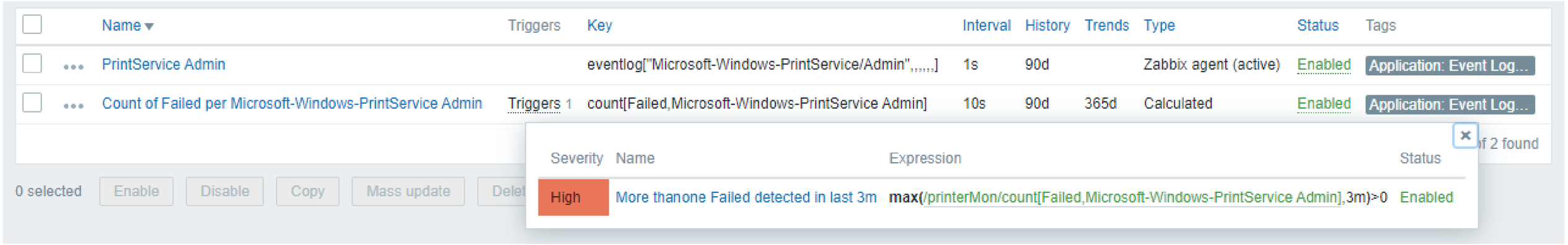
- Events has been classified into categories
- No dublicate reads from the perspective of agent

Cons:

- More storage/memory requirements for Zabbix server

APPROACH 4 – PRODUCE GRAPHS FOR HITS

- Send all lines to Zabbix
- Create calculated items to match patterns. Produce integer numbers



Pros:

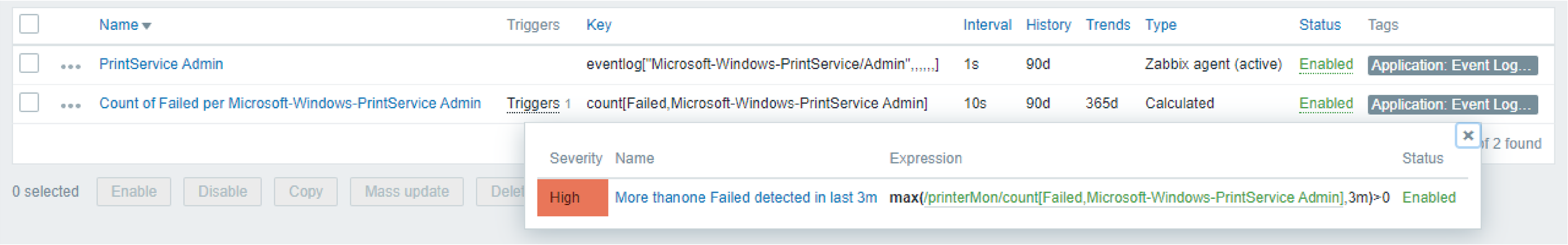
- Graphs available
- No dublicate reads from the perspective of agent

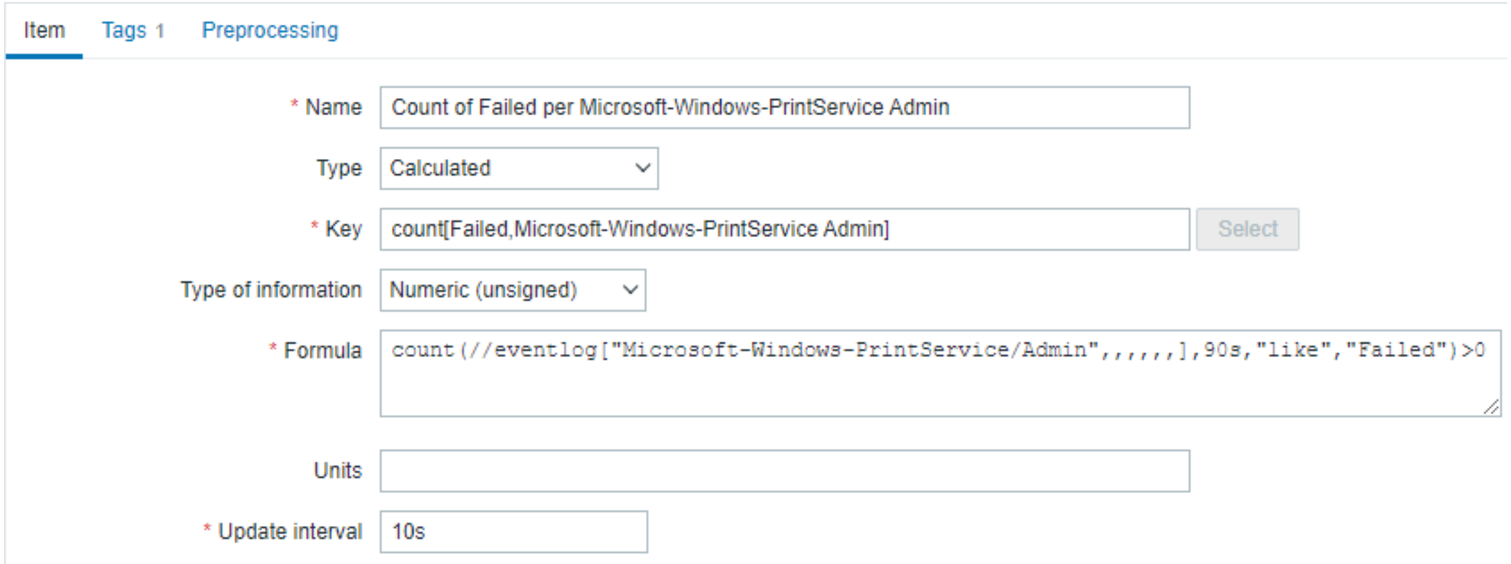
Cons:

- More storage/memory requirements for Zabbix server
- Cannot browse event records straight away from problems page

APPROACH 4 – PRODUCE GRAPHS FOR HITS

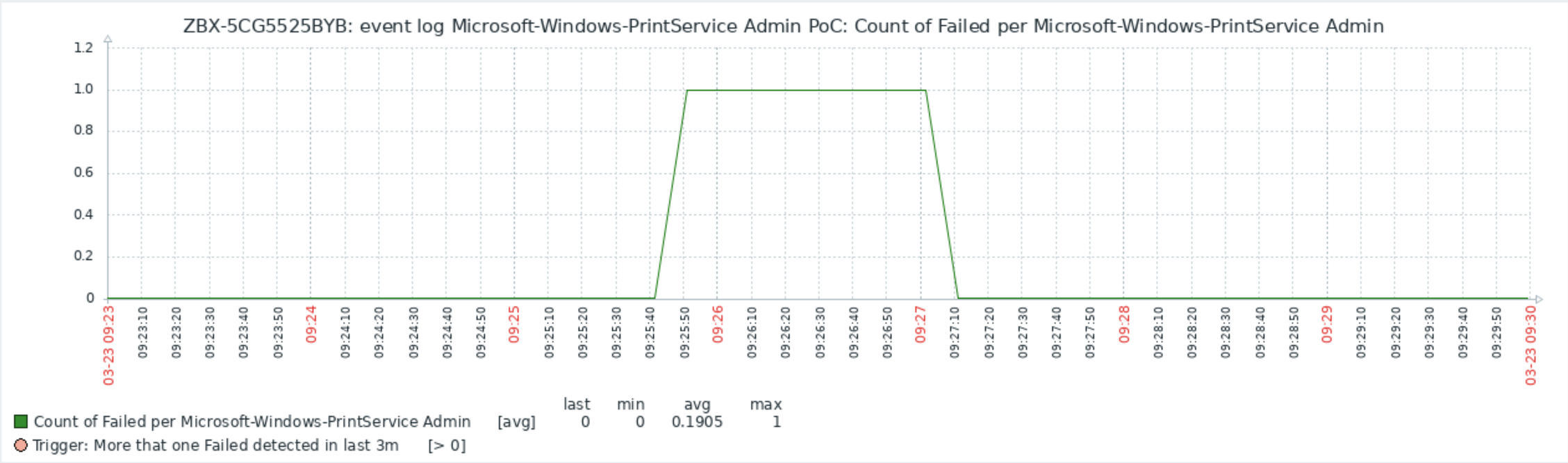
Calculated item counts a pattern «Failed» for the central item:





APPROACH 4 – PRODUCE GRAPHS FOR HITS

Graph:



ZABBIX

QUESTIONS?

AIGARS KADIKIS
TECHNICAL SUPPORT ENGINEER
ZABBIX

ZABBIX

THANK YOU!

AIGARS KADIKIS
TECHNICAL SUPPORT ENGINEER
ZABBIX