

ENGLISH



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

The screenshot shows the Windows Event Viewer application. The left pane displays the 'System' log under 'Windows Logs'. The main pane shows a list of events with the following columns: Level, Date and Time, Source, Event ID, and Task Category. The event with ID 1130 is selected, and its details are shown in the bottom pane.

Level	Date and Time	Source	Event ID	Task Category
Information	3/21/2022 9:00:35 AM	Kernel-General	11	None
Warning	3/21/2022 9:00:31 AM	DistributedCOM	10016	None
Warning	3/21/2022 9:00:28 AM	DistributedCOM	10016	None
Information	3/21/2022 9:00:24 AM	Service Control Manager	7040	None
Error	3/21/2022 9:00:22 AM	GroupPolicy (Microsoft-Windows-GroupPolicy)	1130	None
Information	3/21/2022 9:00:10 AM	Kernel-General	11	None
Information	3/21/2022 9:00:10 AM	Kernel-General	11	None
Information	3/21/2022 9:00:10 AM	Kernel-General	11	None

Event 1130, GroupPolicy (Microsoft-Windows-GroupPolicy)

General Details

Logon script failed.
GPO Name : Local Group Policy
GPO File System Path : C:\WINDOWS\System32\GroupPolicy\User

Actions

- System
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this Log...
- View
- Refresh

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»

The screenshot shows the Zabbix configuration interface for an item. The tabs 'Item', 'Tags', and 'Preprocessing' are visible at the top. The configuration fields are as follows:

- Name:** Network link disconnected established
- Type:** Zabbix agent (active)
- Key:** eventlog[name,<regexp>,<severity>,<source>,<eventid>,<maxlines>,<mode>] (with a 'Select' button)
- Type of information:** Log
- Update interval:** 1s
- Custom intervals:** A table with columns for Type, Interval, Period, and Action.

Type	Interval	Period	Action
Flexible Scheduling	50s	1-7,00:00-24:00	Remove

An 'Add' link is located below the table.
- History storage period:** Do not keep history (selected), Storage period, 90d

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:

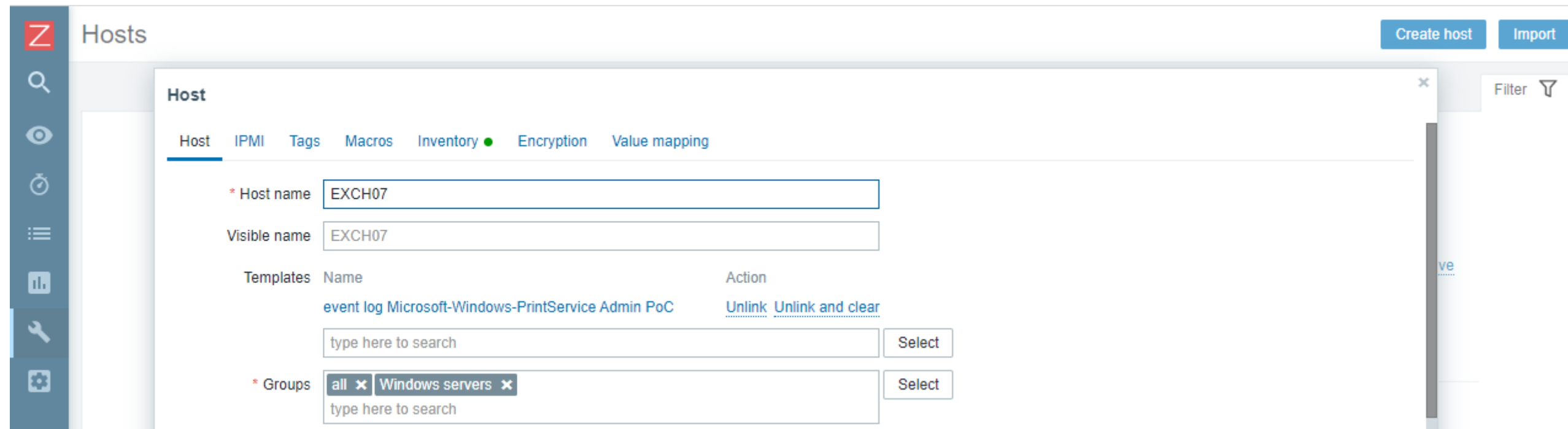
```
c:\zabbix\zabbix_agent2.exe -c c:\zabbix\zabbix_agent2.conf -install
```

ACTIVE CHECKS ONLY

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

```
Hostname=EXCH07
```

- ✓ Must match the configuration for the Host object:



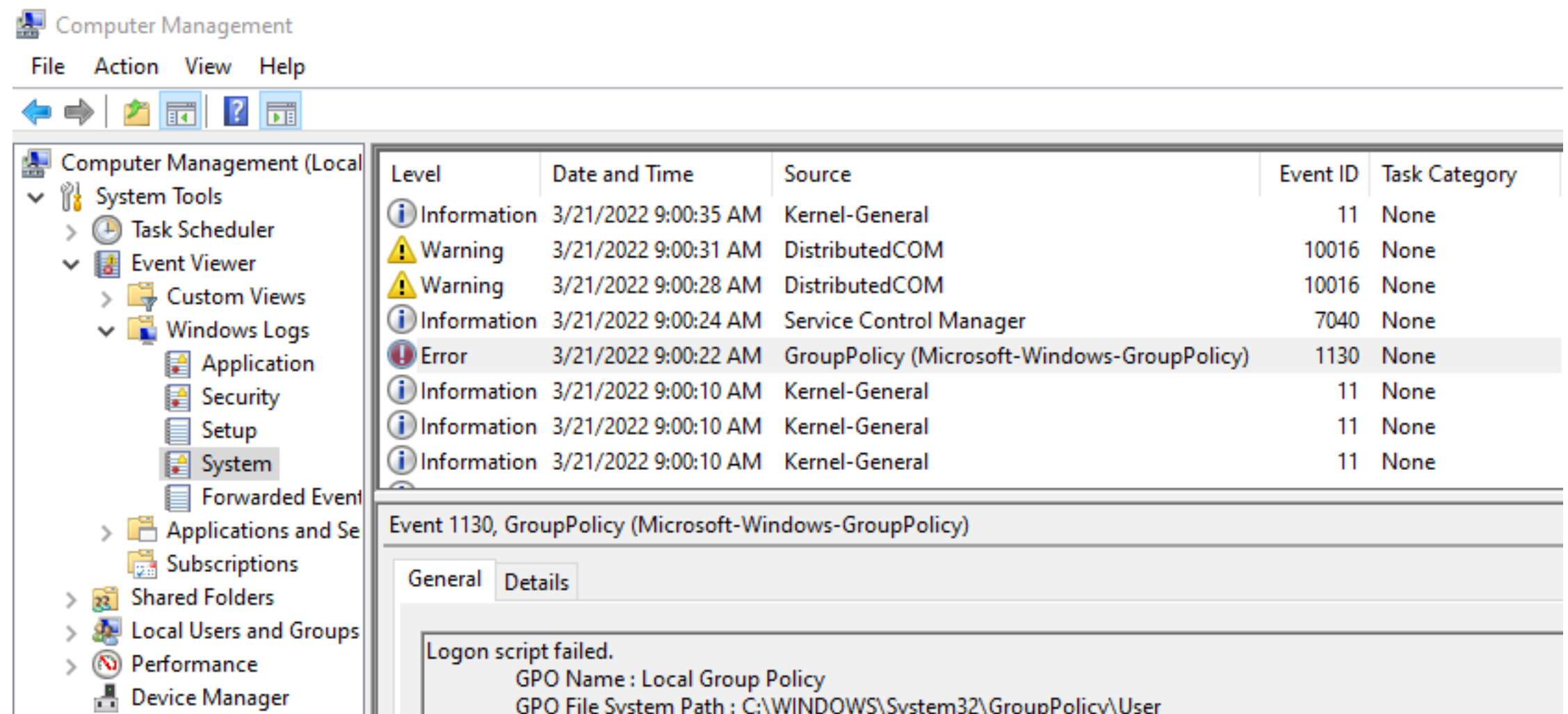
- ✓ Make sure no "Cannot send list of active checks" lines are listed in zabbix_server.log:

```
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,<regex>,<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 << [icon]

ZBX-5CG5525BYB: Warning Error

View as Values [v] As plain text [icon]

< Zoom out > 2022-03-23 10:15:54 – 2022-03-23 11:15:54 [clock] Filter [funnel]

Timestamp	Local time	Source	Severity	Event ID	Value
2022-03-23 10:16:11	2021-09-02 21:19:45	Service Control Manager	Error	7034	The Razer Central Service service terminated unexpectedly. It has done this 1 time(s).
2022-03-23 10:16:11	2021-09-02 21:19:08	Microsoft-Windows-DistributedCOM	Warning	10016	The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID Windows.SecurityCenter.WscDataProtection and APPID Unavailable to the user NT AUTHORITY\SYSTEM SID (S-1-5-18) from address LocalHost (Using LRPC) running in the application container Unavailable SID (Unavailable). This security permission can be modified using the Component Services administrative tool.
2022-03-23 10:16:11	2021-09-02 21:17:26	Microsoft-Windows-DistributedCOM	Warning	10016	The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {2593F8B9-4EAF-457C-B68A-50F6B8EA6B54} and APPID {15C20B67-12E7-4BB6-92BB-7AFF07997402} to the user AKADIKIS-840-G2\aigars SID (S-1-5-21-341453538-698488186-381249278-1001) from address LocalHost (Using LRPC) running in the application container Unavailable SID (Unavailable). This security permission can be modified using the Component Services administrative tool.

ZABBIX

WINDOWS EVENTLOG MONITORING

MONITORING APPROACHES

APPROACH 1 – EASY

- ✓ Detect entries by eventid
- ✓ Will timeout automatically

The screenshot shows the Zabbix configuration interface for a trigger. The main table lists the trigger configuration:

Wizard	Name	Triggers	Key	Interval	History	Trends	Type	Applications	Status	Info
<input type="checkbox"/>	...	Application Error 1000	Triggers 1	eventlog["Application", "Error", "Application Error", "^1000\$", ,]	1s	90d	Zabbix agent (active)	Event Log Application Error	Enabled	

A tooltip is displayed over the trigger, showing the following details:

Severity	Name	Expression	Status
Average	Application Error "{ITEM.VALUE}"	{eventid1000:eventlog["Application", "Error", "Application Error", "^1000\$", ,]}.nodata(3m)=0	Enabled

Additional UI elements include a '0 selected' indicator, 'Enable', 'Disable', and 'Execute' buttons, and a 'Displaying 1 of 1 found' message.

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

The screenshot shows the Zabbix monitoring interface. At the top, there is a table listing triggers. The first trigger is 'Application Error 1000', which is enabled. Below this, a modal window displays the details of the selected trigger. The modal window has a table with the following data:

Severity	Name	Expression	Status
Average	Application Error "{ITEM.VALUE}"	{eventid1000:eventlog["Application",,"Error","Application Error","^1000\$",,]}.nodata(3m)=0	Enabled

At the bottom of the modal window, it says 'Displaying 1 of 1 found'. The main interface also shows buttons for 'Enable', 'Disable', and 'Execute'.

APPROACH 2 – KNOW PROBLEM ID & RECOVERY ID

✓ Network link is disconnected.

Source: **e1dexpress**; Event ID: **27**

The screenshot shows the Windows Event Viewer interface. On the left, the navigation pane is expanded to 'Windows Logs' > 'System'. The main pane displays a list of events with the following columns: Level, Date and Time, Source, Event ID, and Task Category. The event with ID 27 from source e1dexpress is highlighted in blue. Below the list, the details pane for 'Event 27, e1dexpress' is open, showing the 'General' tab with the message: 'Intel(R) Ethernet Connection (3) I218-LM Network link is disconnected.'

Level	Date and Time	Source	Event ID	Task Category
Information	3/21/2022 11:23:12 AM	Kernel-Power	105	(100)
Information	3/21/2022 11:23:10 AM	e1dexpress	32	None
Information	3/21/2022 11:22:43 AM	Kernel-Power	105	(100)
Warning	3/21/2022 11:22:39 AM	e1dexpress	27	None
Warning	3/21/2022 11:17:17 AM	DistributedCOM	10016	None
Warning	3/21/2022 11:16:46 AM	DistributedCOM	10016	None

Event 27, e1dexpress

General Details

Intel(R) Ethernet Connection (3) I218-LM
Network link is disconnected.

APPROACH 2 – KNOW **PROBLEM ID** & **RECOVERY ID**

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

Source: **e1dexpress**; Event ID: **32**

The screenshot shows the Windows Event Viewer interface. On the left, the navigation pane is expanded to 'System' under 'Windows Logs'. The main pane displays a list of events with the following columns: Level, Date and Time, Source, Event ID, and Task Category. The event with ID 32 from source e1dexpress is highlighted in blue. Below the list, the details pane for 'Event 32, e1dexpress' is open, showing the 'General' tab with the message: 'Intel(R) Ethernet Connection (3) I218-LM Network link has been established at 1Gbps full duplex.'

Level	Date and Time	Source	Event ID	Task Category
Information	3/21/2022 11:23:12 AM	Kernel-Power	105	(100)
Information	3/21/2022 11:23:10 AM	e1dexpress	32	None
Information	3/21/2022 11:22:43 AM	Kernel-Power	105	(100)
Warning	3/21/2022 11:22:39 AM	e1dexpress	27	None
Warning	3/21/2022 11:17:17 AM	DistributedCOM	10016	None
Warning	3/21/2022 11:16:46 AM	DistributedCOM	10016	None

Event 32, e1dexpress

General Details

Intel(R) Ethernet Connection (3) I218-LM
Network link has been established at 1Gbps full duplex.

APPROACH 2 – KNOW PROBLEM ID & RECOVERY ID

Implementation:

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

The screenshot shows the Zabbix configuration interface for a trigger. The main table lists the trigger with the following details:

Wizard	Name	Triggers	Key	Interval	History	Trends	Type	Applications	Status	Info
<input type="checkbox"/>	Network link disconnected established	1	eventlog["System",,"Information Warning",,"e1dexpress",,"^(32 27)\$",,]	1s	90d		Zabbix agent (active)	Event Log Network link	Enabled	

An expanded view of the trigger configuration is shown below:

Severity	Name	Expression	Status
Average	Network link disconnected	{networkLink:eventlog["System",,"Information Warning",,"e1dexpress",,"^(32 27)\$",,].logeventid(27)}=1	Enabled

- ✔ $^(32|27)\$$ 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:

The screenshot shows the Windows Event Viewer interface. The left pane displays the tree view of system logs, with 'Applications and Services Logs' highlighted. The right pane shows a list of events with the following columns: Level, Date and Time, Source, Even..., and Task Category. A warning event from 'acvpinstall' is selected. Below the list, the details for 'Event 2, acvpinstall' are displayed, including the function 'CProcessApi::DeleteUser' and various event metadata.

Level	Date and Time	Source	Even...	Task Category
Information	5/8/2021 10:13:34 AM	acvpinstall	1	Engineering Debug Details
Information	5/8/2021 10:13:34 AM	acvpnva	1	Engineering Debug Details
Warning	5/8/2021 10:13:33 AM	acvpinstall	2	Engineering Debug Details
Information	5/8/2021 10:13:31 AM	acvpnagent	2020	None
Information	5/8/2021 10:13:31 AM	acvpnagent	1	Engineering Debug Details
Information	5/8/2021 10:13:31 AM	acvpnagent	1	Engineering Debug Details
Information	5/8/2021 10:13:31 AM	acvpnagent	1	Engineering Debug Details
Information	5/8/2021 10:13:31 AM	acvpnagent	1	Engineering Debug Details
Information	5/8/2021 10:13:31 AM	acvpnagent	1	Engineering Debug Details
Information	5/8/2021 10:13:31 AM	acvpnagent	1	Engineering Debug Details

Event 2, acvpinstall

General Details

Function: CProcessApi::DeleteUser
File: IPC\ProcessAPI.cpp
Line: 1272

Log Name: Cisco AnyConnect Secure Mobility Client
Source: acvpinstall Logged: 5/8/2021 10:13:33 AM
Event ID: 2 Task Category: Engineering Debug Details
Level: Warning Keywords: Classic
User: N/A Computer: AKADIKIS-840-G2
OpCode: Info
More Information: [Event Log Online Help](#)

APPROACH 3 – COLLECT EVERYTHING FROM ONE SOURCE

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

The screenshot displays the Windows Event Viewer interface. On the left, a tree view shows the hierarchy of system logs, with 'PrintService' expanded to show 'Admin' and 'Operational' sub-logs. The main pane shows a list of events from the 'PrintService' log. The selected event (ID 318) is highlighted, and its details are shown in a separate pane below. The 'Log Name' field in the details pane is highlighted in blue, indicating it is selected for copying.

Level	Date and Time	Source	Event ID	Task Category
Information	3/8/2022 11:03:11 AM	PrintService	823	Changing the default printer
Error	3/29/2021 1:57:33 PM	PrintService	318	Adding a printer driver
Error	3/29/2021 1:57:33 PM	PrintService	318	Adding a printer driver
Error	3/29/2021 1:57:22 PM	PrintService	318	Adding a printer driver
Error	3/29/2021 1:57:22 PM	PrintService	318	Adding a printer driver
Error	3/29/2021 1:57:22 PM	PrintService	318	Adding a printer driver
Error	3/29/2021 1:57:22 PM	PrintService	318	Adding a printer driver
Error	3/29/2021 1:57:21 PM	PrintService	215	Installing a printer driver

Event 318, PrintService

General Details

Failed to upgrade printer settings for printer Microsoft Print to PDF driver Microsoft Print To PDF. Error: 0x80040003. The device settings for the printer are set to those configured by the manufacturer.

Log Name: **Microsoft-Windows-PrintService/Admin**

Source: PrintService Logged: 3/29/2021 1:57:33 PM

Event ID: 318 Task Category: Adding a printer driver

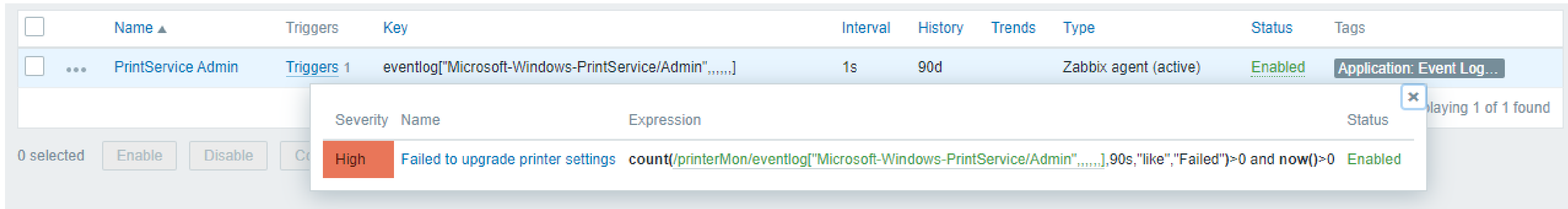
Level: Error Keywords: Classic Spooler Event,Print Driver

Actions

- Admin
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Disable Log
- Find...
- Save All Events As...
- Attach a Task To this Lo...
- View
- Refresh
- Help
- Event 318, PrintService
- Event Properties
- Attach Task To This Eve...
- Copy
- Save Selected Events...

APPROACH 3 – COLLECT EVERYTHING FROM ONE SOURCE

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



The screenshot shows the Zabbix configuration interface. A table lists triggers for the 'PrintService Admin' host. A tooltip is displayed over one of the triggers, showing its details.

Name	Triggers	Key	Interval	History	Trends	Type	Status	Tags
PrintService Admin	Triggers 1	eventlog["Microsoft-Windows-PrintService/Admin",,,,,,]	1s	90d		Zabbix agent (active)	Enabled	Application: Event Log...

Severity	Name	Expression	Status
High	Failed to upgrade printer settings	count(/printerMon/eventlog["Microsoft-Windows-PrintService/Admin",,,,,,],90s,"like","Failed")>0 and now()>0	Enabled

Pros:

- ✓ Events has been classified into categories
- ✓ No duplicate 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

The screenshot displays the Zabbix monitoring interface. At the top, there is a table of items with columns: Name, Triggers, Key, Interval, History, Trends, Type, Status, and Tags. Two items are visible:

Name	Triggers	Key	Interval	History	Trends	Type	Status	Tags
PrintService Admin		eventlog["Microsoft-Windows-PrintService/Admin",.....]	1s	90d		Zabbix agent (active)	Enabled	Application: Event Log...
Count of Failed per Microsoft-Windows-PrintService Admin	Triggers 1	count[Failed,Microsoft-Windows-PrintService Admin]	10s	90d	365d	Calculated	Enabled	Application: Event Log...

Below the table, there are buttons for "0 selected", "Enable", "Disable", "Copy", "Mass update", and "Delete". A modal window is open, showing a trigger configuration table:

Severity	Name	Expression	Status
High	More thanone Failed detected in last 3m	max(/printerMon/count[Failed,Microsoft-Windows-PrintService Admin],3m)>0	Enabled

Pros:

- ✓ Graphs available
- ✓ No duplicate 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:

Name	Triggers	Key	Interval	History	Trends	Type	Status	Tags
PrintService Admin		eventlog["Microsoft-Windows-PrintService/Admin",.....]	1s	90d		Zabbix agent (active)	Enabled	Application: Event Log...
Count of Failed per Microsoft-Windows-PrintService Admin	Triggers 1	count[Failed,Microsoft-Windows-PrintService Admin]	10s	90d	365d	Calculated	Enabled	Application: Event Log...

0 selected Enable Disable Copy Mass update Delete

Severity	Name	Expression	Status
High	More than one Failed detected in last 3m	<code>max(/printerMon/count[Failed,Microsoft-Windows-PrintService Admin],3m)>0</code>	Enabled

of 2 found

Item Tags 1 Preprocessing

* Name

Type

* Key

Type of information

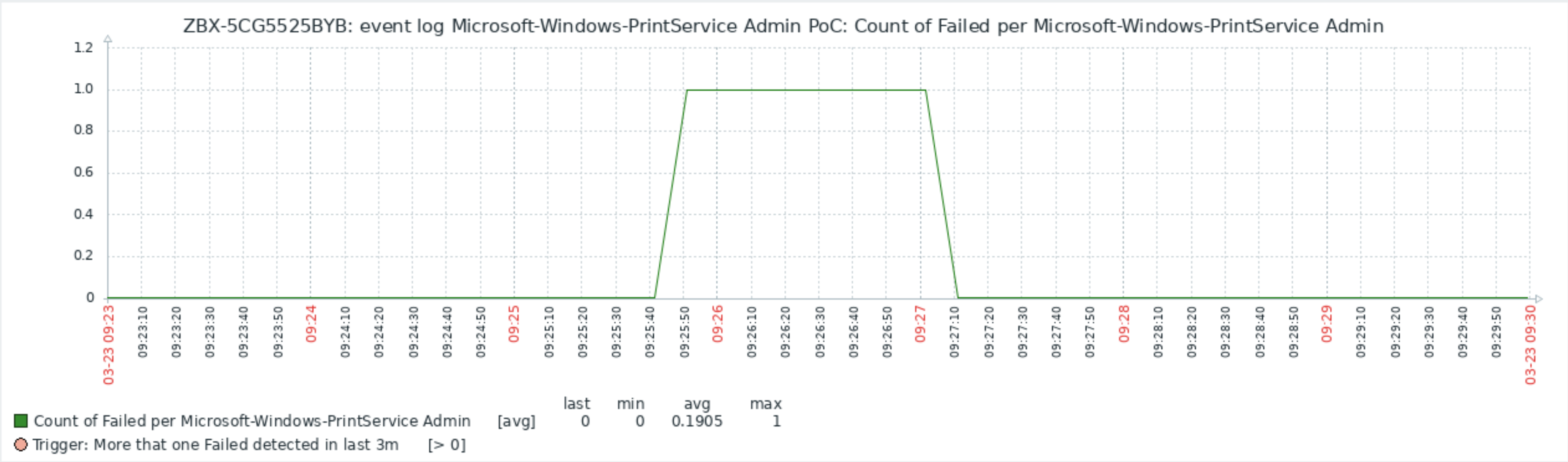
* Formula

Units

* Update interval

APPROACH 4 - PRODUCE **GRAPHS** FOR HITS

Graph:



ZABBIX

QUESTIONS?

AIGARS KADIKIS
TECHNICAL SUPPORT ENGINEER

ZABBIX

ZABBIX

THANK YOU!

AIGARS KADIKIS
TECHNICAL SUPPORT ENGINEER

ZABBIX