

# Tips and Tricks on using useful features of Zabbix in large scale environments



2023/10/06-07

**NTT Com Engineering Corporation**



The background of the slide is a photograph of a long, brightly lit server room aisle. On both sides are rows of server racks with perforated metal doors. The floor is covered with metal grates. A semi-transparent blue rounded rectangle is centered over the image, containing the title text.

# Self introduction



Who am I.

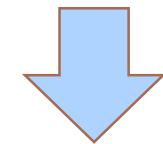
## Takashi Fukushima



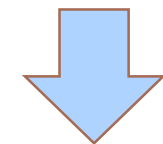
I have been engaged in activities related to Zabbix and monitoring systems with Zabbix as the core for over 15 years, including consulting, custom development, support, and training.



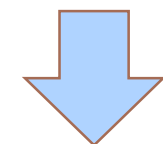
Joined company(2009)



from 2017



from 2021



from 2023



**Now**



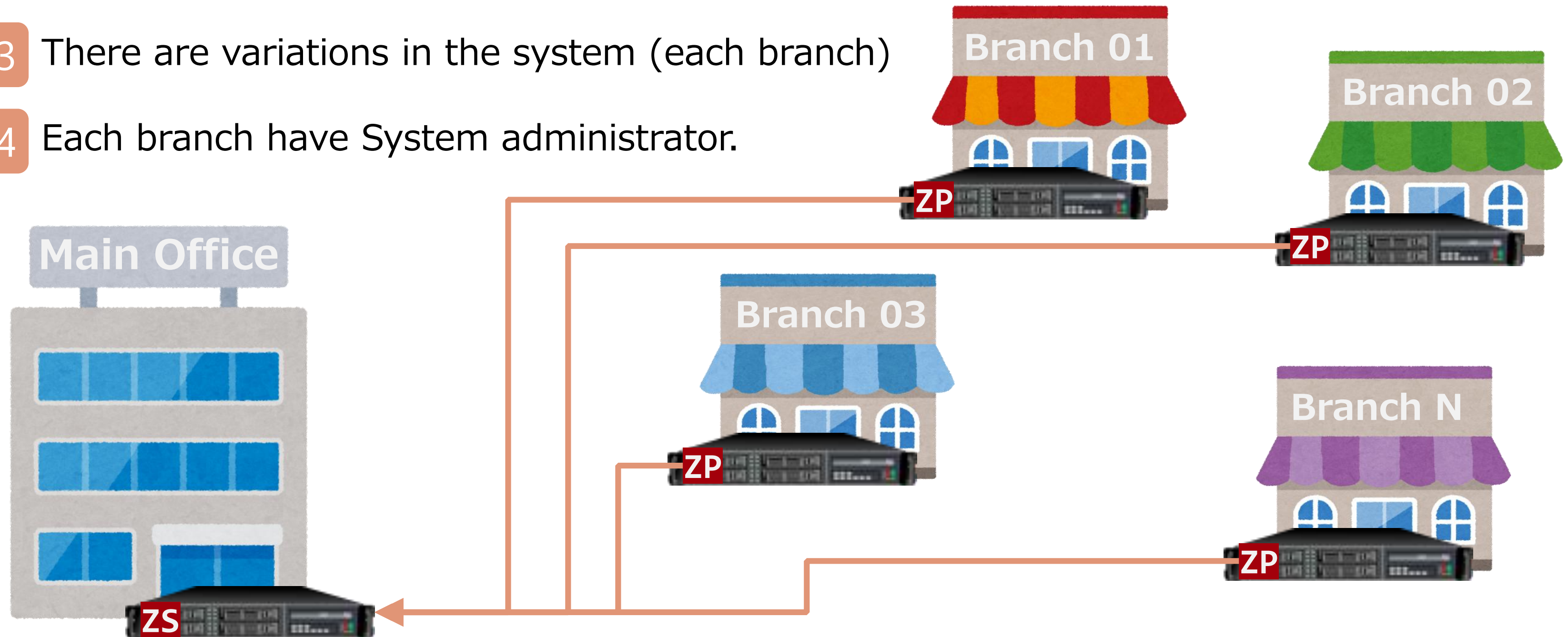
The background is a photograph of a long, brightly lit server room aisle. On both sides are rows of server racks with perforated metal doors. The floor is covered with metal grates. A semi-transparent blue rounded rectangle is centered over the image, containing the text 'Case study' in white.

# Case study



Company-A had the following requirements:

- No. 01 Many branches (and systems)
- No. 02 Monitoring is centralized at the main office  
-> Receive requests from System administrator of each branch
- No. 03 There are variations in the system (each branch)
- No. 04 Each branch have System administrator.



## The additional requirements.

**Ex. 01** Detected PROBLEM will be integrated with a ticket management system and managed within that system.

\* Zabbix will only data collection and fault detection.  
Web interface will not be used for reference.

**Ex. 02** Targets servers and network devices.

**Ex. 03** The system should not only support automate registration but also automate updates.  
However, Rollback if update fails

## The additional requirements.

**Ex. 04** Easily set up multiple log monitors and process monitors.

**Ex. 05** Maintenance settings individually depending on the type of log message.

**Ex. 06** Automatically close PROBLEM events in log monitoring.  
(because the event specifications have changed since Zabbix 4.0)

This Zabbix has the following mechanism.

- Mechanism. 01 Automatic registration.
- Mechanism. 02 Automatic close PROBLEM events.
- Mechanism. 03 Flexible maintenance settings.



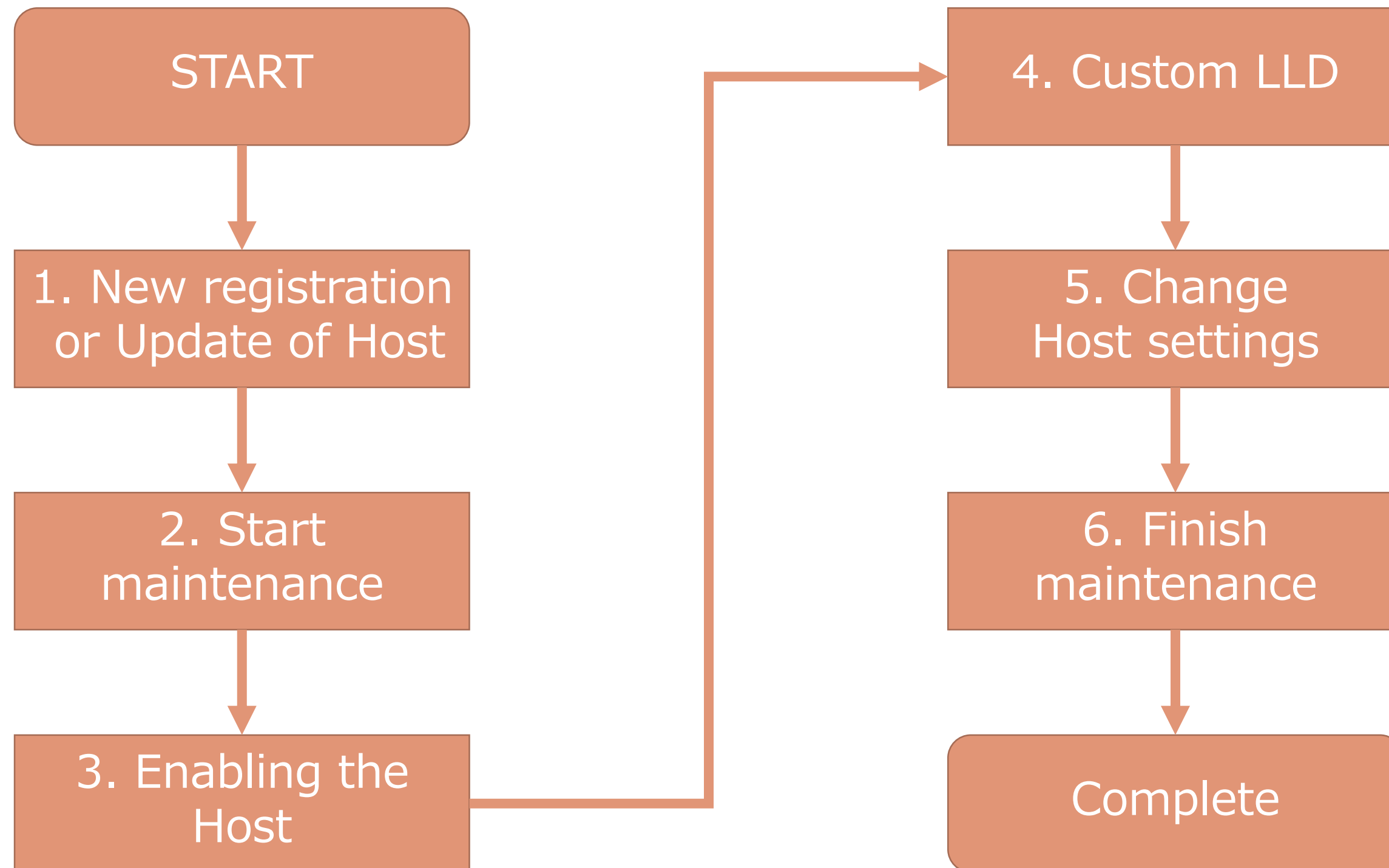


# About the automatic registration mechanism



# About the automatic registration mechanism

The new registration of monitoring settings is carried out in the following 6 steps



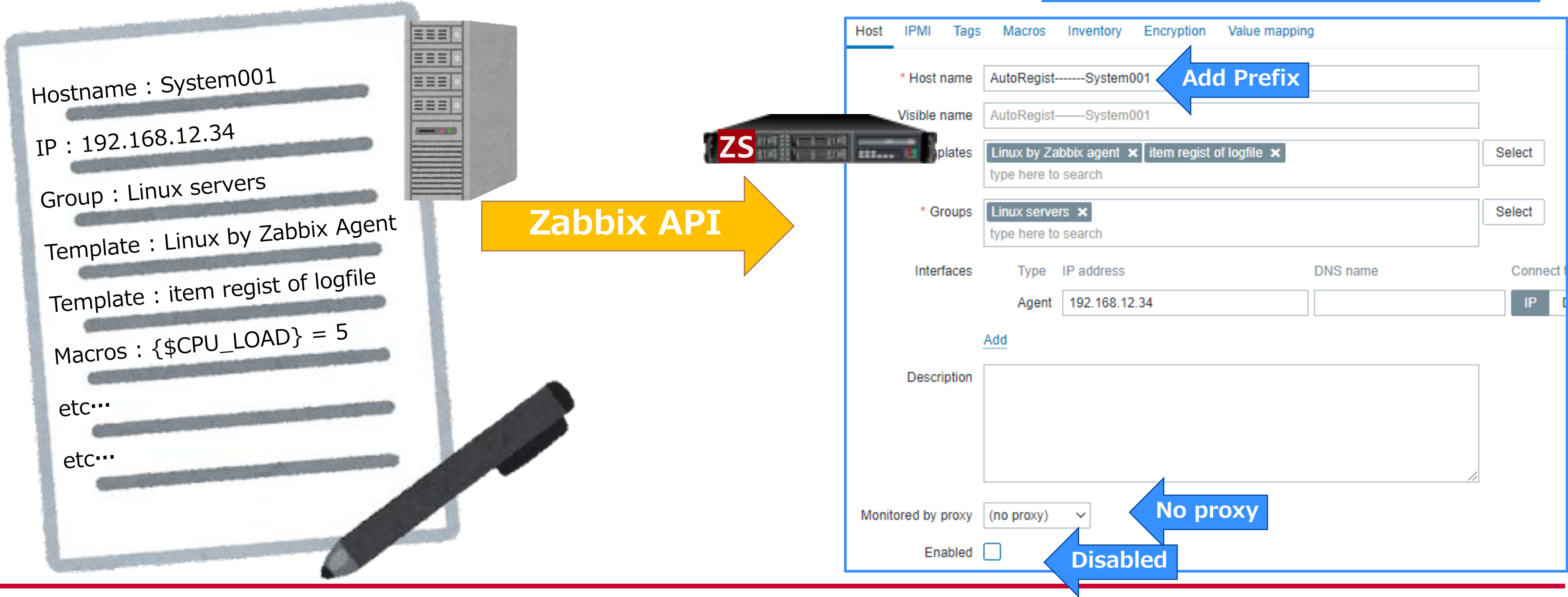


# About the automatic registration mechanism

STEP 01

New registration or Update of Host

Create a host in Zabbix via Zabbix API  
using host information extracted from CMDB via API.





# About the automatic registration mechanism

## STEP 02 Start maintenance

Perform maintenance settings for the host registered in STEP 01.

Periods
Hosts and groups

\* Name
[AutoAdd] from 20210927144302

Maintenance type

With data collection

No data collection

\* Active since
2021-09-27 14:43

\* Active till
2038-01-18 23:59

Description

Add Cancel

With data collection

Periods
Hosts and groups

\* At least one host group or host must be selected.

Host groups

Linux servers ✕

type here to search

Select

Hosts

type here to search

Select

Tags

And/Or Or

State Contains Equals Registering Remove

Add

The host registered in Step 1 will be targeted.

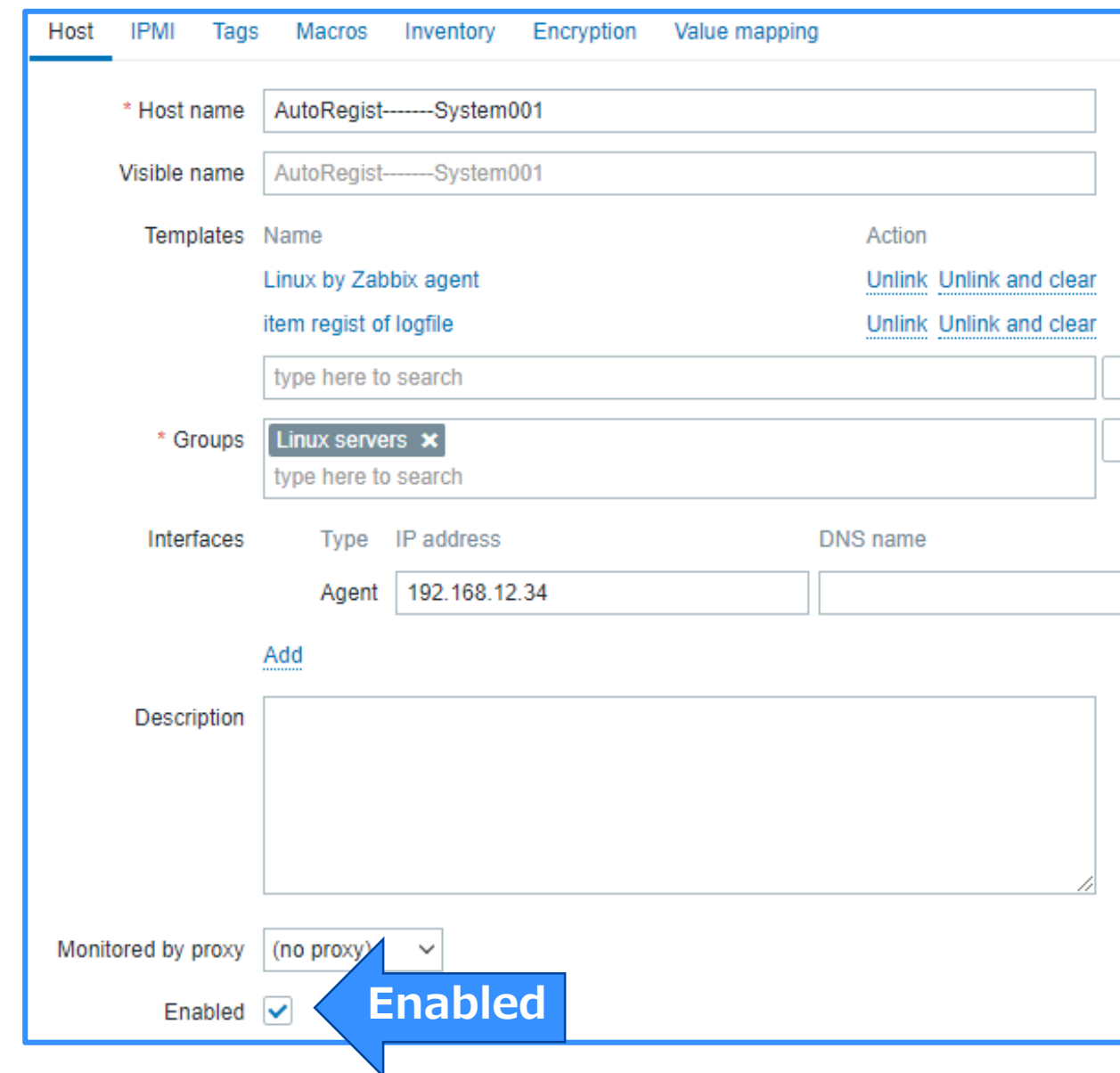
**Stop processing for 1 minute.**  
**( Ensure that the maintenance status is active. )**



# About the automatic registration mechanism

## STEP 03 Enabling the Host

Enable the host registered in STEP 01  
and run config\_cache\_reload on the Zabbix server.



The screenshot shows the Zabbix web interface for configuring a host. The 'Host' tab is selected. The host name is 'AutoRegist-----System001'. The visible name is also 'AutoRegist-----System001'. Under 'Templates', there are two entries: 'Linux by Zabbix agent' and 'item regist of logfile'. The 'Groups' section shows 'Linux servers' selected. The 'Interfaces' section shows an 'Agent' interface with IP address '192.168.12.34'. The 'Description' field is empty. At the bottom, the 'Monitored by proxy' dropdown is set to '(no proxy)'. The 'Enabled' checkbox is checked, and a blue arrow points to it with the word 'Enabled'.

Set a wait time of 1-minute ( CacheUpdateFrequency seconds ) again.



# About the automatic registration mechanism

## STEP 04 Custom LLD

Send CSV data to the server  
using zabbix\_sender.

Preprocessing 1 LLD macros 5 Filters Overrides

LLD macro	JSONPath
{#ENCODING}	\$.encode
{#FILE}	\$.file
{#MSG.ID}	\$.msgid
{#OPTIONS}	\$.options
{#REGEXP}	\$.regexp

[Add](#)

Discovery rule Preprocessing 1 LLD macros 5 Filters Overrides

\* Name

Type

\* Key

\* Keep lost resources period

Allowed hosts

Preprocessing 1 LLD macros 5 Filters Overrides

Preprocessing steps

Name
1: CSV to JSON

[Add](#)

Convert to JSON

Trigger prototype Tags Dependencies

\* Name

Operational data

Severity

\* Expression

[Expression constructor](#)

OK event generation

PROBLEM event generation mode

Allow manual close ☒

URL

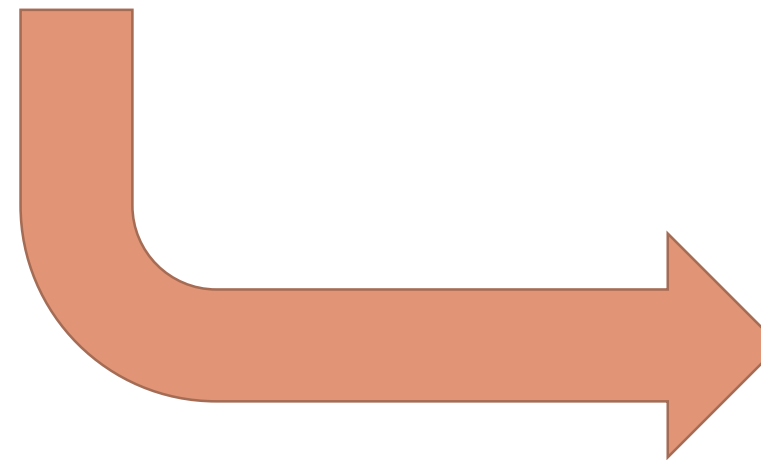


# About the automatic registration mechanism

## STEP 04 Custom LLD

```
zabbix_sender -z 127.0.0.1 -s 'dummy' -k log.discovery -o
'file,regexp,encode,options,interval,period,msgid
/var/log/messages,error,utf8,mtime_noread,1s,7d,001
/var/log/httpd/error.log,(Started|Stopped),utf8,,1s,10d,002
/var/log/zabbix/zabbix_agent2.log,(Starting | stopped.),utf8,,1s,3d,003'
```

CSV to JSON  
&  
LLD macros



```
{
  "{#FILE}": "/var/log/messages",
  "{#REGEXP}": "error",
  "{#ENCODING}": "utf8",
  "{#OPTIONS}": "mtime_noread",
  "{#MSG.ID}": "001"
},
{
  "{#FILE}": "/var/log/httpd/error.log",
  "{#REGEXP}": "(Started|Stopped)",
  "{#ENCODING}": "utf8",
  "{#OPTIONS}": "",
  "{#MSG.ID}": "002"
},
{
  "{#FILE}": "/var/log/zabbix/zabbix_agent2.log",
  "{#REGEXP}": "(Starting | stopped.)",
  "{#ENCODING}": "utf8",
  "{#OPTIONS}": "",
  "{#MSG.ID}": "003"
}
}
```

Various types of monitoring items can be easily generated.



# About the automatic registration mechanism

STEP 05

## Change Host settings

Change the “Monitored by proxy” settings on each host to the appropriate settings.

Host

IPMI

Tags

Macros

Inventory

Encryption

Value mapping

\* Host name

AutoRegist-----System001

Visible name

AutoRegist-----System001

Templates

Name	Action
Linux by Zabbix agent	<a href="#">Unlink</a> <a href="#">Unlink and clear</a>
item regist of logfile	<a href="#">Unlink</a> <a href="#">Unlink and clear</a>

type here to search

Se

\* Groups

Linux servers

type here to search

Se

Interfaces

Type	IP address	DNS name
Agent	192.168.12.34	

Add

Description

Monitored by proxy

Proxy001

Modify

Enabled

☒



# About the automatic registration mechanism

## STEP 06 Finish maintenance

The maintenance settings are removed using the Zabbix API, and monitoring is started.

Any hosts that experienced failures in the previous steps  
 “newly registered hosts” are deleted as part of the rollback process.  
 The prefix is removed from newly registered hosts, reverting them to their appropriate names.

[Periods](#)
[Hosts and groups](#)

\* Name

[AutoAdd] from 20210927144302

Maintenance type

With data collection

No data collection

\* Active since

2021-09-27 14:43

\* Active till


2038-01-18 23:59

Description

Update

Clone

Delete


Delete Maintenance setting

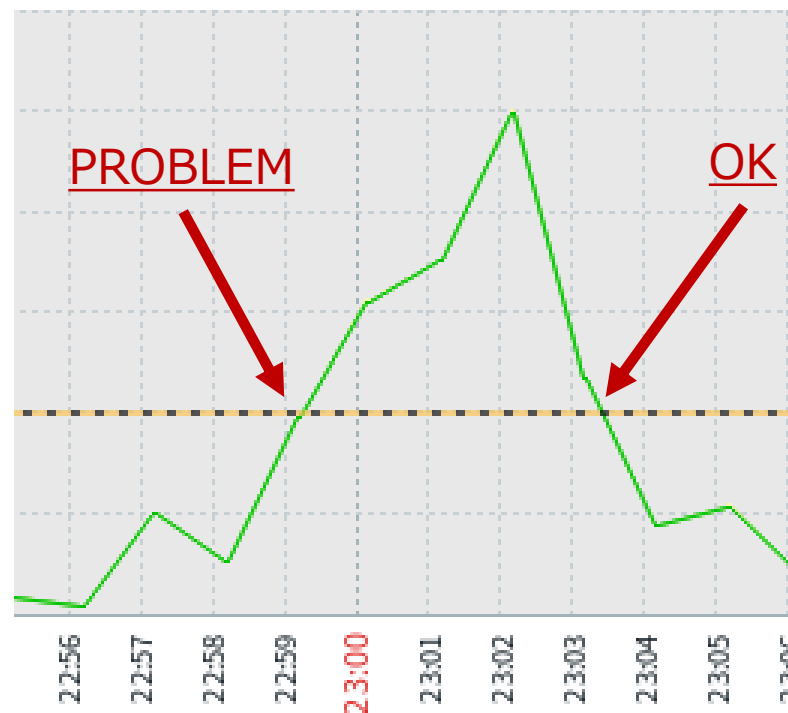


# About the automatic close **PROBLEM** events



# Two types of PROBLEM that Zabbix detects.

Type 1: PROBLEM and OK are always paired.



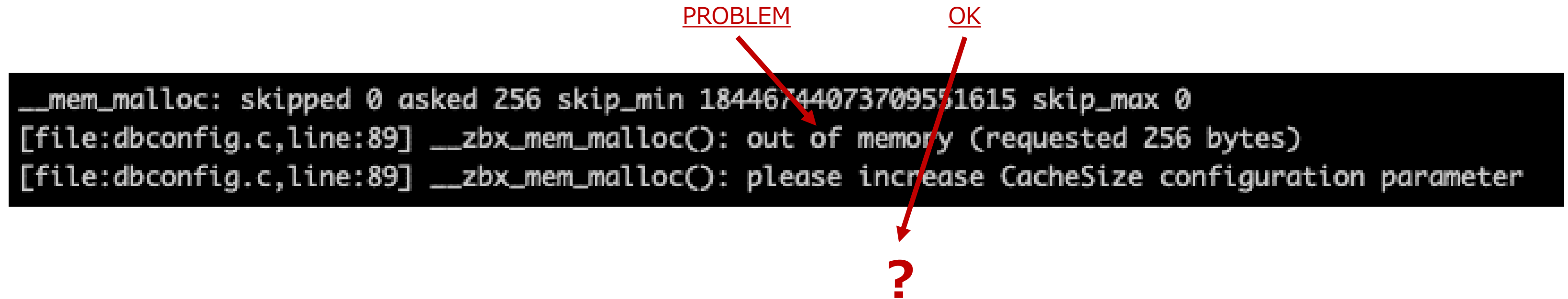
For example: Resource monitoring

We call this “**stateful monitoring**”.



# Two types of PROBLEM that Zabbix detects.

Type 2: PROBLEM and OK do not necessarily pair.



```

__mem_malloc: skipped 0 asked 256 skip_min 18446744073709551615 skip_max 0
[file:dbconfig.c,line:89] __zbx_mem_malloc(): out of memory (requested 256 bytes)
[file:dbconfig.c,line:89] __zbx_mem_malloc(): please increase CacheSize configuration parameter
  
```

?

For example: snmptrap, log monitoring

We call this “**stateless monitoring**”.



# About automatic close PROBLEM events

Add a special tag to “Stateless monitoring”.

☐

Severity

Value

Name ▲

☐

Average

OK

item regist for log-key: Error log of /var/log/httpd/error.log [ pattern:(Started|Stopped) value:{\$ITEM.VALUE}

☐

Average

OK

item regist for log-key: Error log of /var/log/messages [ pattern:error value:{\$ITEM.VALUE} ]

☐

Average

OK

item regist for log-key: Error log of /var/log/zabbix/zabbix\_agent2.log [ pattern:(Starting | stopped.) value:

Omission

Tags

MSGID: 002

TriggerType: Stateless

MSGID: 001

TriggerType: Stateless

MSGID: 003

TriggerType: Stateless

Special Tag

Be executed if PROBLEM-event has a special tag

\* Name

Automatic close PROBLEM events

Conditions

Label

Name

B

Value of tag *TriggerType* equals *Stateless*

Add

Media type

Message templates

Options

\* Name

Automatic close PROBLEM events

Type

Script ▼

\* Script name

auto\_close.sh

Script parameters

Parameter

Action

{ALERT.MESSAGE}

Remove

Add

Script uses Zabbix API’s “event.acknowledge” method and {EVENT.ID} macro to close the event.



The background of the slide is a photograph of a long, brightly lit server room aisle. On both sides are rows of white server racks with perforated doors. The floor is covered with metal grates. A semi-transparent blue rounded rectangle is centered over the image, containing the title text.

# About the flexible maintenance settings



# About the flexible maintenance settings

Add the special tag "Message ID Number".

<input type="checkbox"/>	Severity	Value	Name ▲
<input type="checkbox"/>	Average	OK	item regist for log-key: Error log of /var/log/httpd/error.log [ pattern:(Started Stopped) value:{\$ITEM.VALUE}
<input type="checkbox"/>	Average	OK	item regist for log-key: Error log of /var/log/messages [ pattern:error value:{\$ITEM.VALUE} ]
<input type="checkbox"/>	Average	OK	item regist for log-key: Error log of /var/log/zabbix/zabbix_agent2.log [ pattern:(Starting   stopped.) value:

Omission

Tags	
MSGID: 002	TriggerType: Stateless
MSGID: 001	TriggerType: Stateless
MSGID: 003	TriggerType: Stateless

Special Tag

Special tags are defined by csv data to be set using LLD macros.

Trigger tags

Inherited and trigger tags

Name	Value	Action
MSGID	{#MSG.ID}	<a href="#">Remove</a>
TriggerType	Stateless	<a href="#">Remove</a>

Add

Trigger tags

Inherited and trigger tags

Name	Value	Action
MSGID	002	<a href="#">Remove</a>
TriggerType	Stateless	<a href="#">Remove</a>

Add

Special tags are defined for each type of log message detected.

# About the flexible maintenance settings

Perform tag-maintenance settings for special tags.

\* At least one host group or host must be selected.

Host groups

all hosts ✕

type here to search

Select

Hosts

type here to search

Select

Tags

And/Or Or

MSGID

Contains Equals

002

Remove

MSGID


Contains Equals

007

Remove

Add

Messages to unmonitor



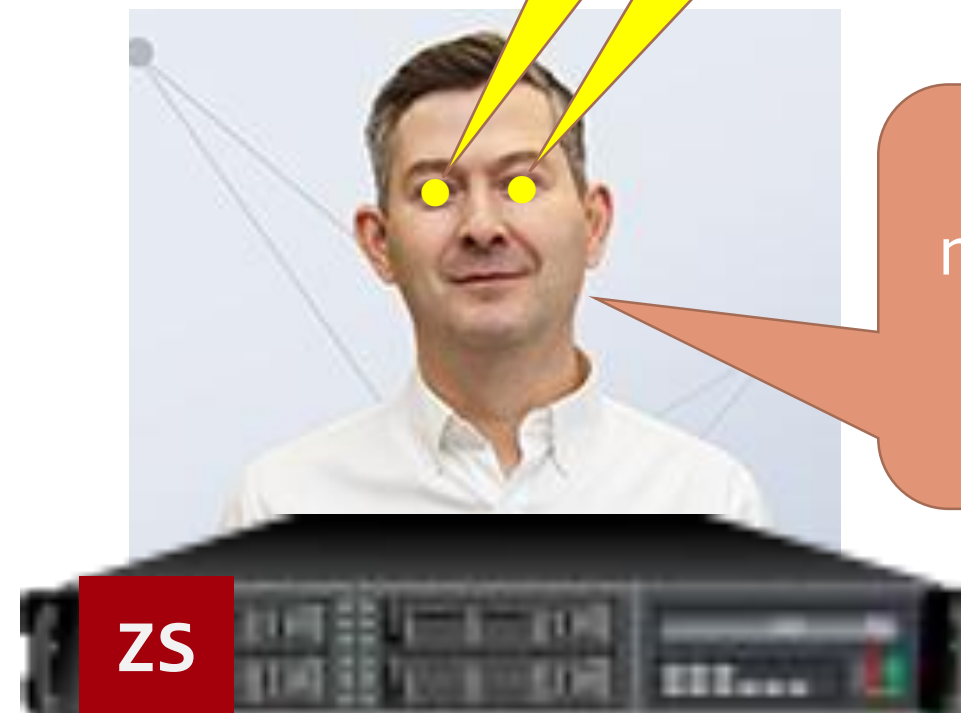
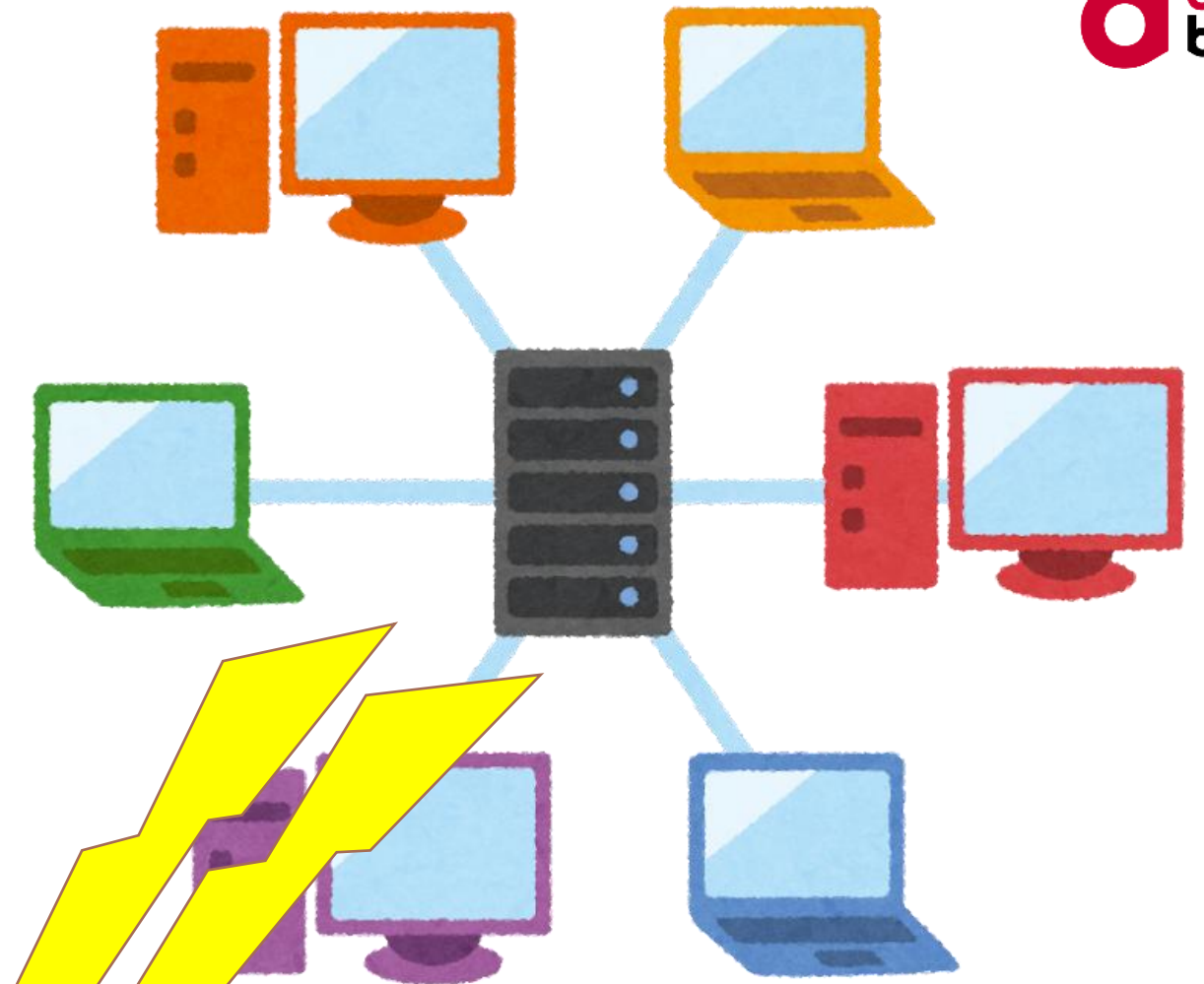
Allows to perform maintenance of log monitoring on a **message-type basis**.



Everyone at Company-A was happy.



Employee of company A



My Zabbix is always  
monitoring over your servers.

Ha-ha!!



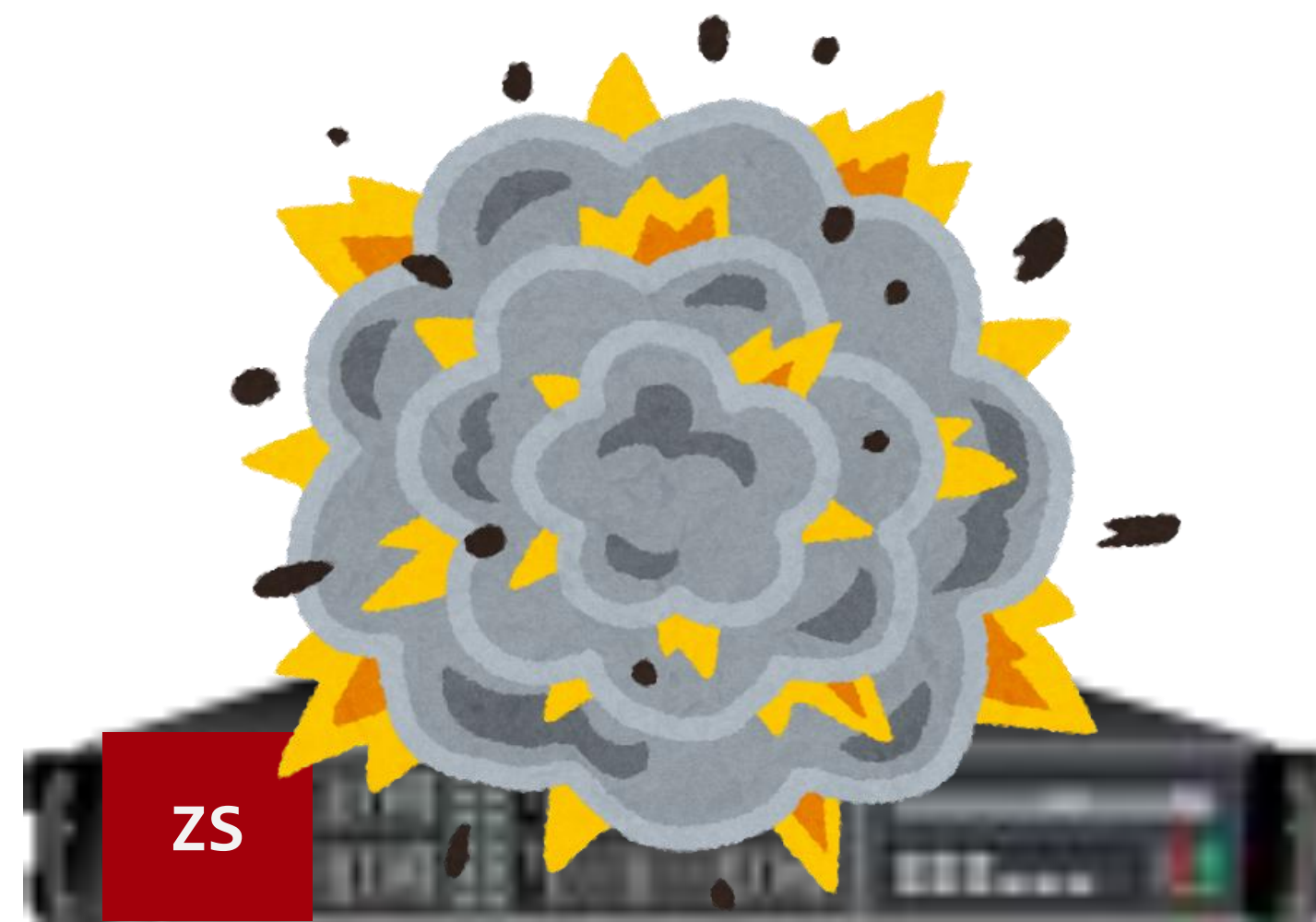
# Troubleshooting case 01



# Troubleshooting example. case 1



Error occurs  
in automatic registration mechanism





# The cause of this trouble is very simple

Sent a very large amount of data.

```
[root@tr060 ~]# zabbix_sender -z 127.0.0.1 -s 'dummy' -k log.discovery -o 'file,regexp,encode,options,msgid,
/var/log/me, error,utf8,mtime_noread,001
/var/log/ht x a, Size of data part of csv : About 322KB
/var/log/zabbix-agent2.log,(Started|Stopped),utf8,,003'
Response from "127.0.0.1:10051": "processed: 1; failed: 0; total: 1; seconds spent: 0.000108"
sent: 1; skipped: 0; total: 1
```

The problem occurred because within the program, zabbix\_sender was being executed through the shell, which Fails with "Argument list too long" error due to ARG\_MAX limit

As a legendary trainer, that's nothing special to me.

```
[zabbix@Stagingserver ~]$ xargs --show-limits
Your environment variables take up 2016 bytes
POSIX upper limit on argument length (this system): 2617376
POSIX smallest allowable upper limit on argument length (all systems): 4096
Maximum length of command we could actually use: 2615360
Size of command buffer we are actually using: 131072
```

Argument list limit

Trainer  
10th Anniversary  
Polo Shirt



# There are other things to keep in mind.

Please read the Zabbix manual carefully.

## Data limits for return values

There is no limit for low-level discovery rule JSON data if it is received directly by Zabbix server. This is because the return values are processed without being stored in a database.

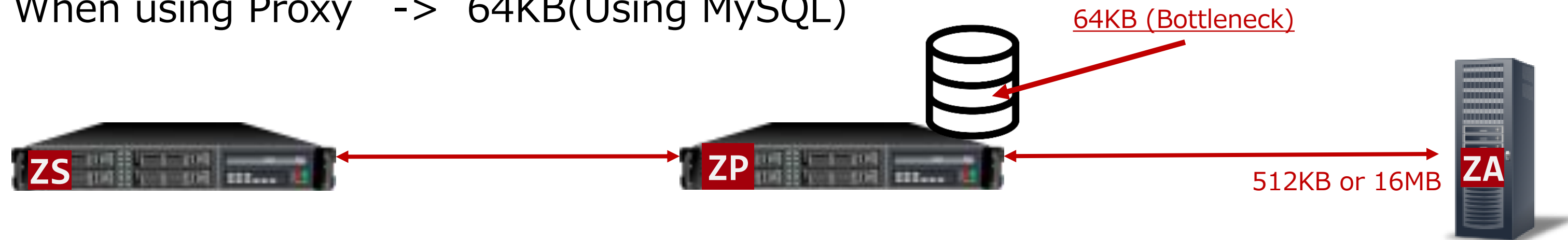
There is also no limit for custom low-level discovery rules. However, if custom low-level discovery rule data is retrieved using a user parameter, the user parameter return value limit applies.

If data has to go through Zabbix proxy, it has to store this data in the database. In such a case, database limits apply.

[https://www.zabbix.com/documentation/6.0/en/manual/discovery/low\\_level\\_discovery/notes#data-limits-for-return-values](https://www.zabbix.com/documentation/6.0/en/manual/discovery/low_level_discovery/notes#data-limits-for-return-values)

UserParameters -> 512KB(up to Zabbix 5.0) or 16MB(Zabbix6.0 or later)

When using Proxy -> 64KB(Using MySQL)





# Troubleshooting case 02

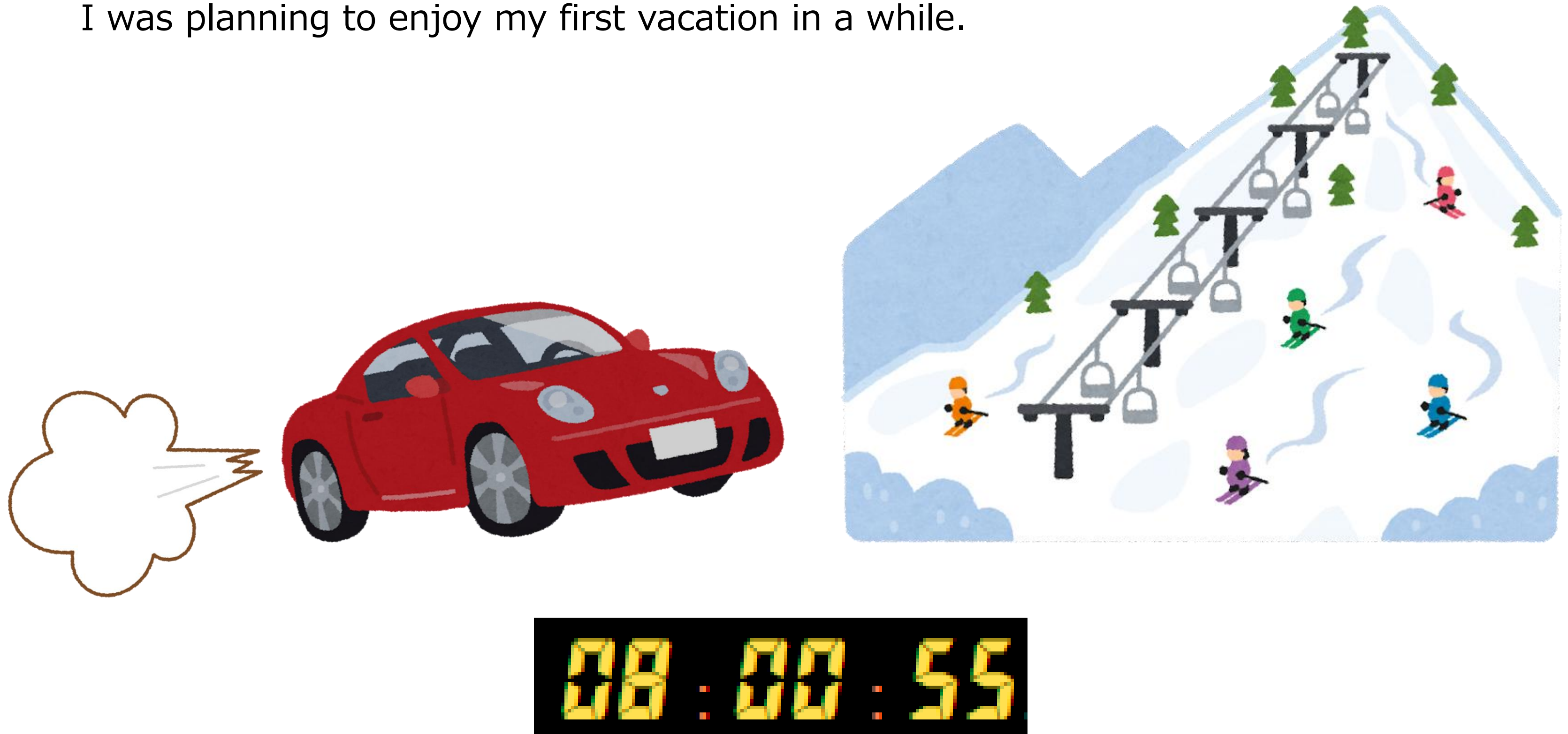






# Troubleshooting example. Part 2

I was planning to enjoy my first vacation in a while.





# Troubleshooting example. Part 2



Zabbix server was down!!



Company-A's Zabbix server



## What problem occurred.



NVPS decreased by 1/10.



Error message on Zabbix web interface.



Nodata function for hosts monitored directly from Zabbix Server is experiencing issues.

Finally, the HistoryIndexCache became full and the Zabbix Server process was down.

Restarting the Zabbix Server and database did not resolve the issue.



# What problem occurred.

These are the processes we focused on.

	(busy rate)
Configuration syncer	100%
Task manager	<b>90%</b>
Timer	50%
Trapper	95%
ipmp manager	95%
icmp pinger	95%
Unreachable poller	80%

We initially thought that the auto-close mechanism might be the cause.  
Because process “task manager” seemed very busy. (near 100%)

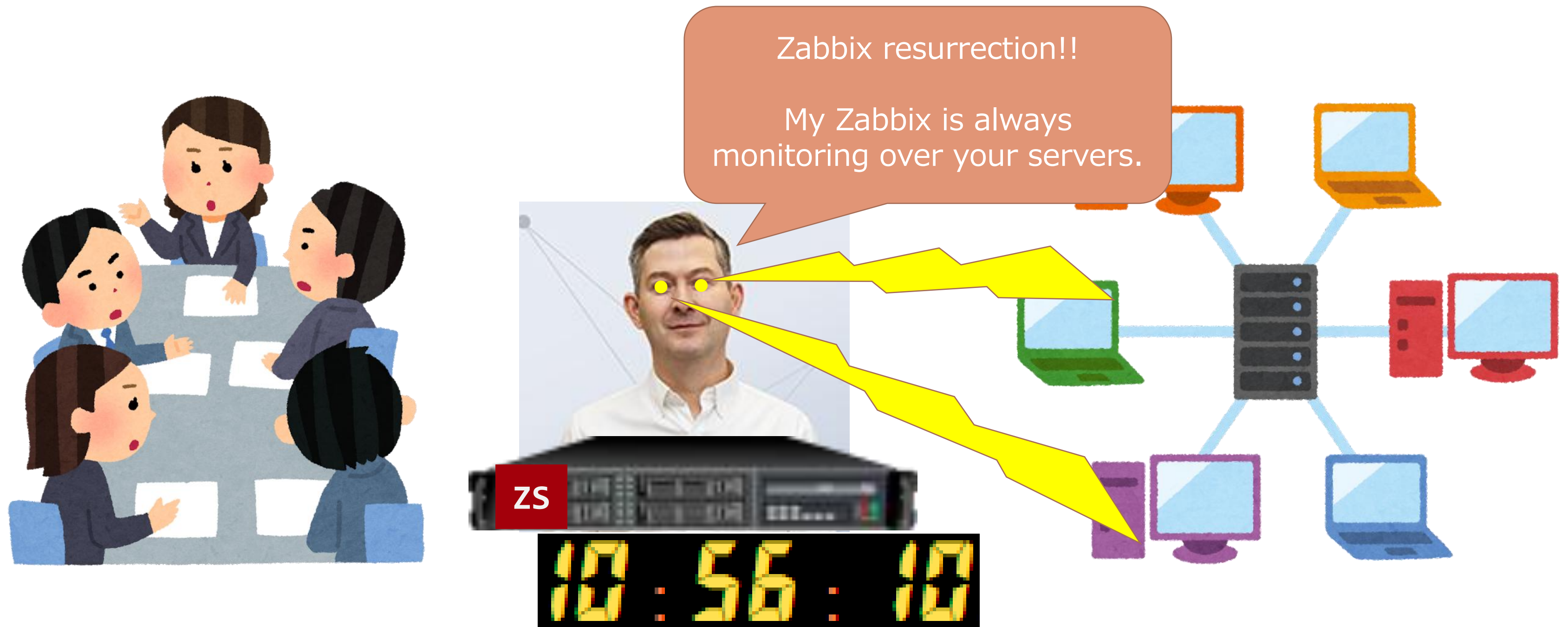
Proposed to stop the mechanism of “Automatic close PROBLEM events”.



# Propose temporary measures.

We proposed to stop the “automatic close PROBLEM events” mechanism.

The problem issue ended while Company-A was discussing whether to accept the proposal.



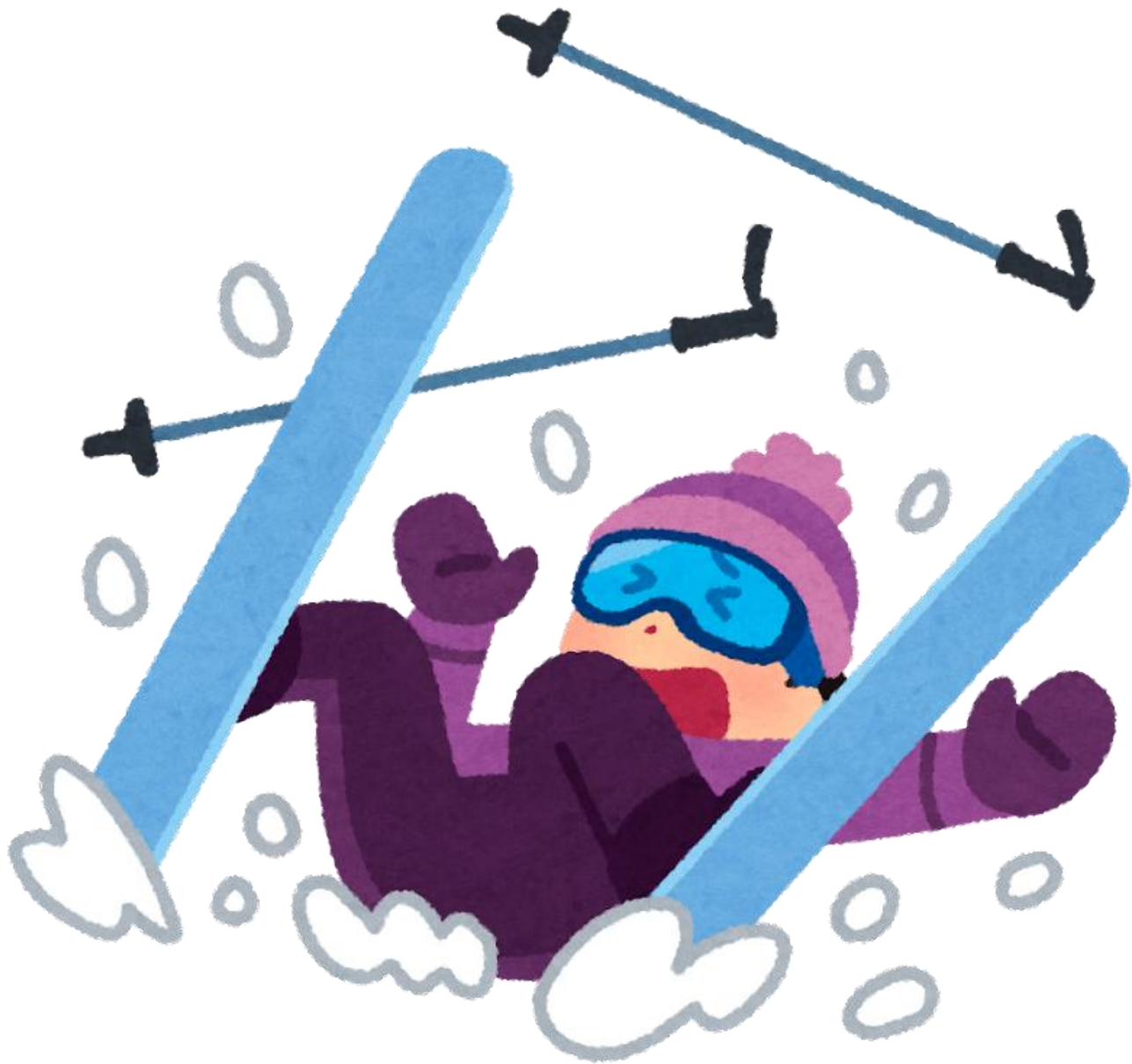


# Case being settled

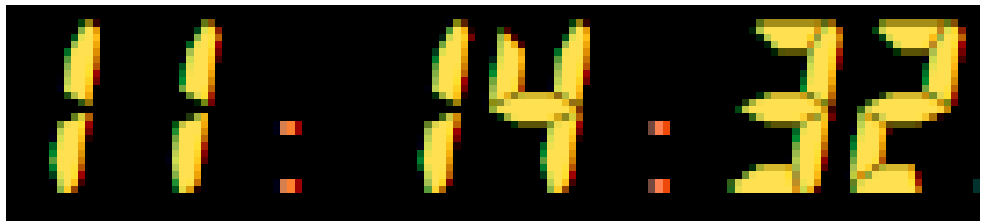
I enjoyed skiing.



ideal



reality

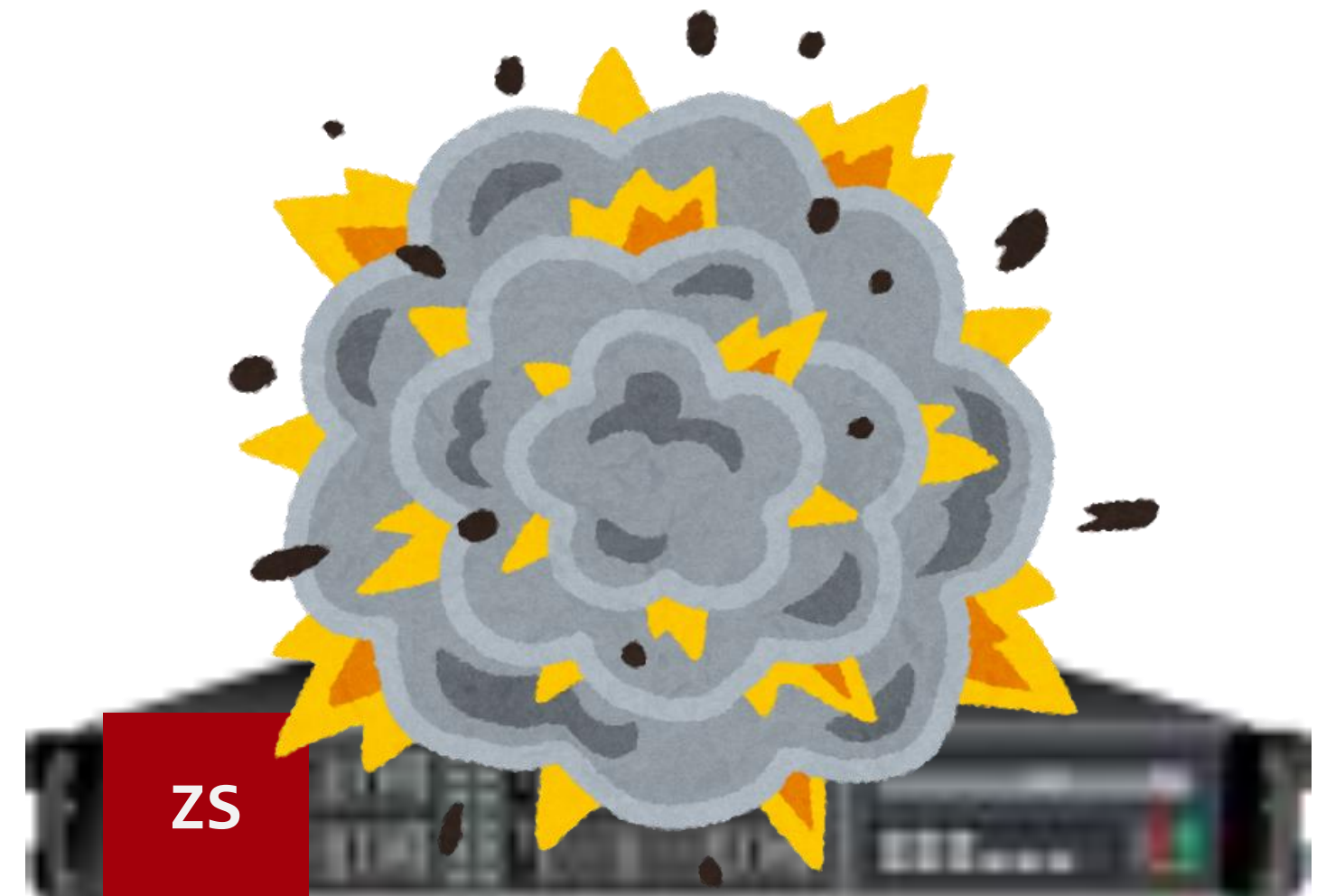




Problem occurred again.



Zabbix server was down again.



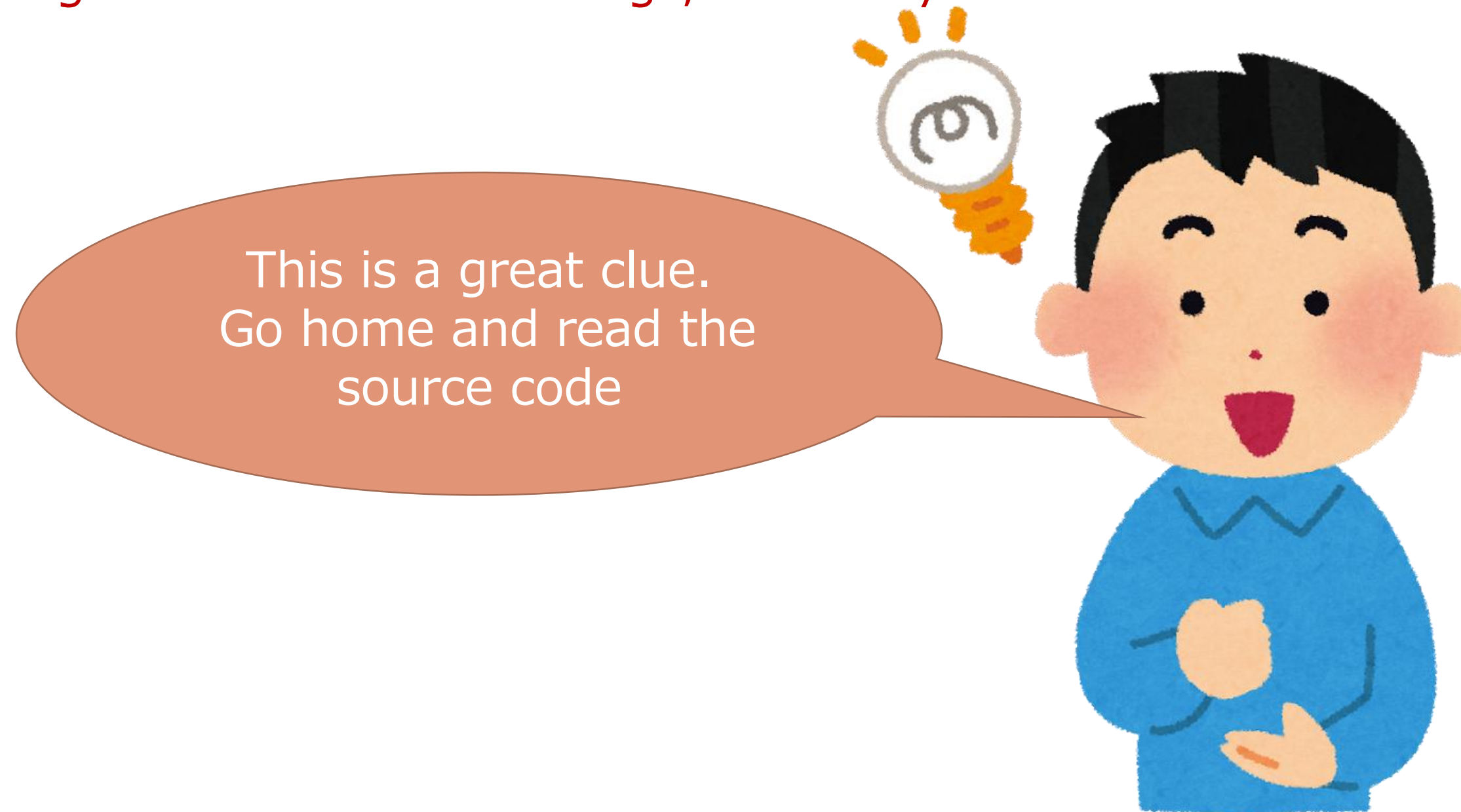
15 : 25 : 29



# New clues

Over 1,000 maintenance settings were in effect when the trouble occurred.

After disabling all maintenance settings, Zabbix system recovered.





but .....

My BOSS said.

Please read the source code now.

The only acceptable answers  
for me are 'Yes' or 'OK.'

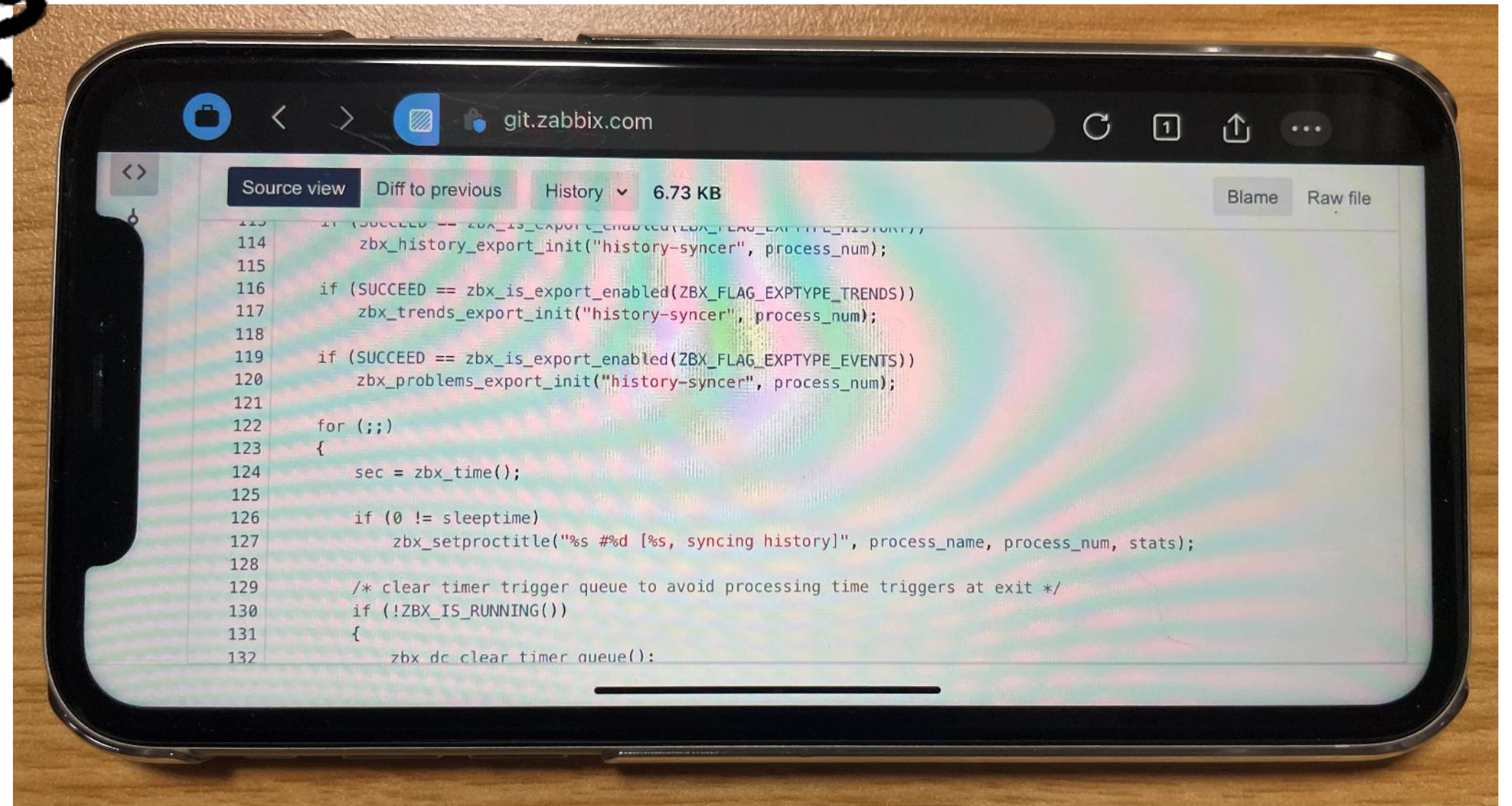


My BIG BOSS

15 : 39 : 48



# Decipher source code on iPhone.





# Found the specifications

**Spec 01** HistorySyncer is checking if tags match.

**Spec 02** Tagged maintenance needs to check whether the tag matches for **every PROBLEM event**.  
- P ... Number of events generated.

**Spec 03** Every time an event is generated, an  $M*N*O$  check is performed.  
- M ... Number of Tags attached to the event.  
- N ... Number of Tags attached to the maintenance settings.  
- O ... Number of active maintenance settings.

Therefore, **the number of operations is the product of  $M * N * O * P$ .**

\* reference data ( Company-A ):

- Sometimes, PROBLEM events were occurring in **large numbers**.
- Each event has 2 tags.
- Each maintenance setting has 2 tags.

but, a lot of tag-value (about 50)

- Always, **500 over** active maintenance settings. ( max:1500 over )



# Permanent countermeasure plan.

Merge similar strings and reduce the total number of maintenance settings.

Host groups **all hosts** ✕  
type here to search

Hosts type here to search

Tags

And/Or Or

MSGID	Contains	Equals	002	R
MSGID	Contains	Equals	007	R

[Add](#)

Host groups **all hosts** ✕  
type here to search

Hosts type here to search

Tags

And/Or Or

MSGID	Contains	Equals	009	R
MSGID	Contains	Equals	025	R

[Add](#)

Host groups **Windows servers** ✕  
type here to search

Hosts type here to search

Tags

And/Or Or

MSGID	Contains	Equals	002	R
MSGID	Contains	Equals	007	R
MSGID	Contains	Equals	009	R
MSGID	Contains	Equals	025	R

[Add](#)

Reducing the number of target hosts

Merge

16 : 36 : 43



Things aren't going according to planned.





Zabbix is a very versatile and deep tool.

## Legendary trainer



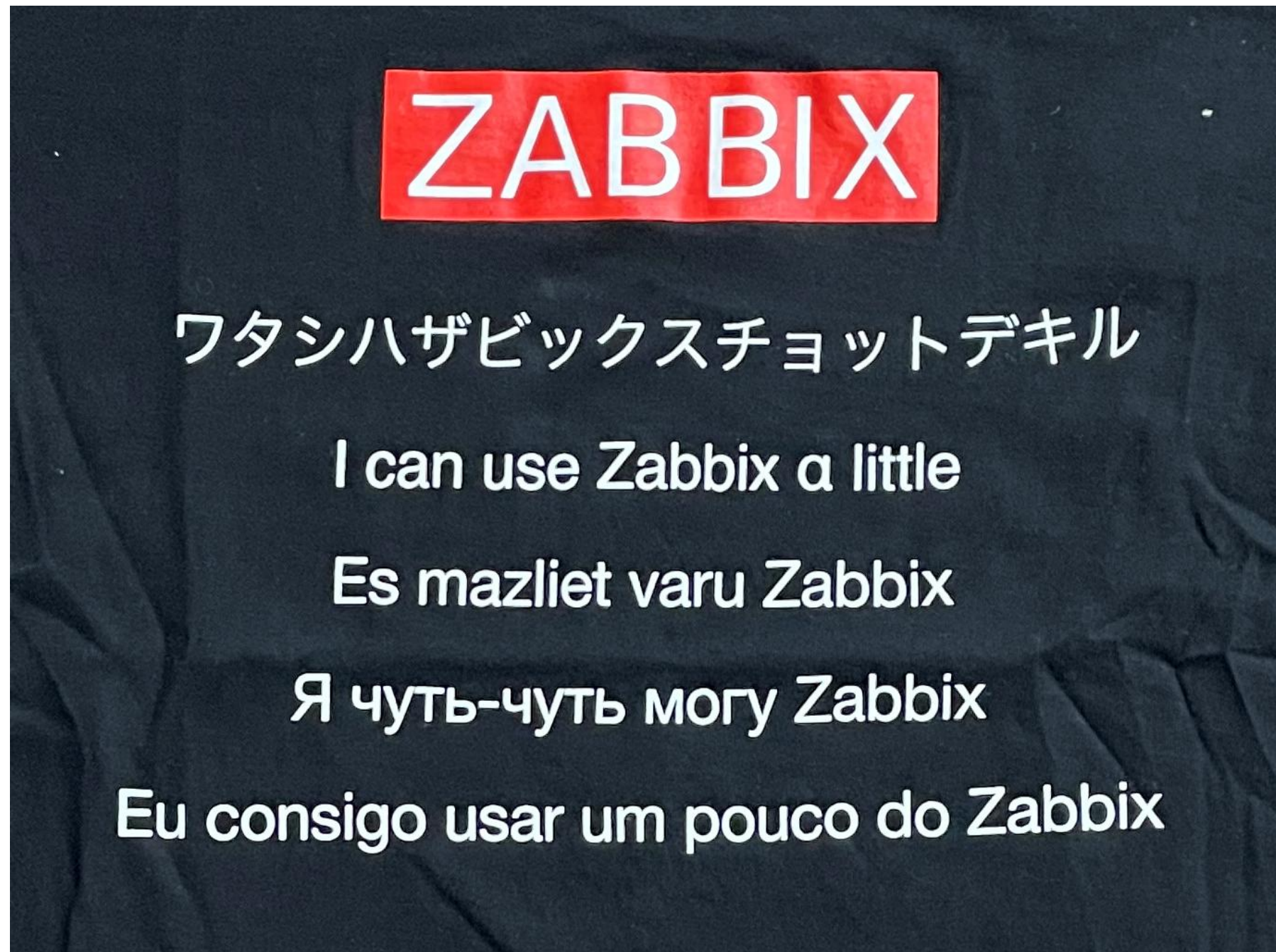
## “ザビックスチョットデキル” trainer



The meaning of 'ザビックスチョットダケデキル' is 'I can use Zabbix a little. '



Do you want this T-shirt ?



This T-shirt sold by a Zabbix Japan LLC

For inquiries, please contact Zabbix **Japan staff.**



The background is a photograph of a long, brightly lit server room aisle. On both sides are rows of server racks with perforated metal doors. The floor is covered with metal grates. A semi-transparent blue rounded rectangle is centered over the image, containing the word 'Summary' in white text.

# Summary



**No.01** Custom LLD is a powerful and useful feature with great potential,  
but it should be used with a good understanding of Zabbix's specifications.

---

**No.02** Tag-level maintenance is a handy feature that allows  
for flexible maintenance settings,  
but excessive use tag-maintenance will increase the system load.

---

**No.03** If you want to enjoy skiing, better not to bring your smartphone.

---





Thank you for your attention.