

Practical Zabbix Lessons from Migration and Operations

How we consolidated legacy monitoring and improved operations at scale

Satoru Imai

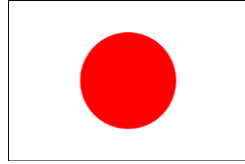
NTT DOCOMO BUSINESS ENGINEERING Corporation, Japan

Agenda

- ◆ Introduction
- ◆ 1. Migration from Nagios and Cacti to Zabbix
- ◆ 2. Two Event Correlation Cases
 - ◆ 2.1 Duplicate RSS alert suppression
 - ◆ 2.2 SNMP trap recovery
- ◆ Summary and Future Vision

About Me

- Name: **Satoru Imai**
- From: **Tokyo, Japan**
- Position: Monitoring Operations Team Lead
- **Zabbix user for 7 years**



NTT DOCOMO BUSINESS ENGINEERING

Our Role in the NTT Group

NTT Group
Global telecom & ICT group

NTT DOCOMO
Integrated ICT Business

NTT DOCOMO BUSINESS
Enterprise ICT solutions

NTT DOCOMO BUSINESS ENGINEERING

Scale at a Glance

344K
Staff

0.3%
of Japan's
population

2,100
Staff

≈€259M
Revenue

System operations for NTT DOCOMO BUSINESS



Largest listed companies in Japan by consolidated workforce
#1 Toyota Motor
#2 NTT Group

My Role

I lead monitoring operations for large-scale customer systems.

What I Do

- **Migrate legacy monitoring tools**
Consolidate Nagios and Cacti on a shared Zabbix platform
- **Operate and improve our Zabbix environment**
- **Connect monitoring with ITSM**
ServiceNow
- **Automate operations**
Ansible, Ticketing, and recovery

Current Zabbix Scale

Version
7.0

Hosts
39,000

Templates
856

Items
155,000

Triggers
59,000

NVPS
1,200

Automation Workflow

Zabbix



ServiceNow



Ansible

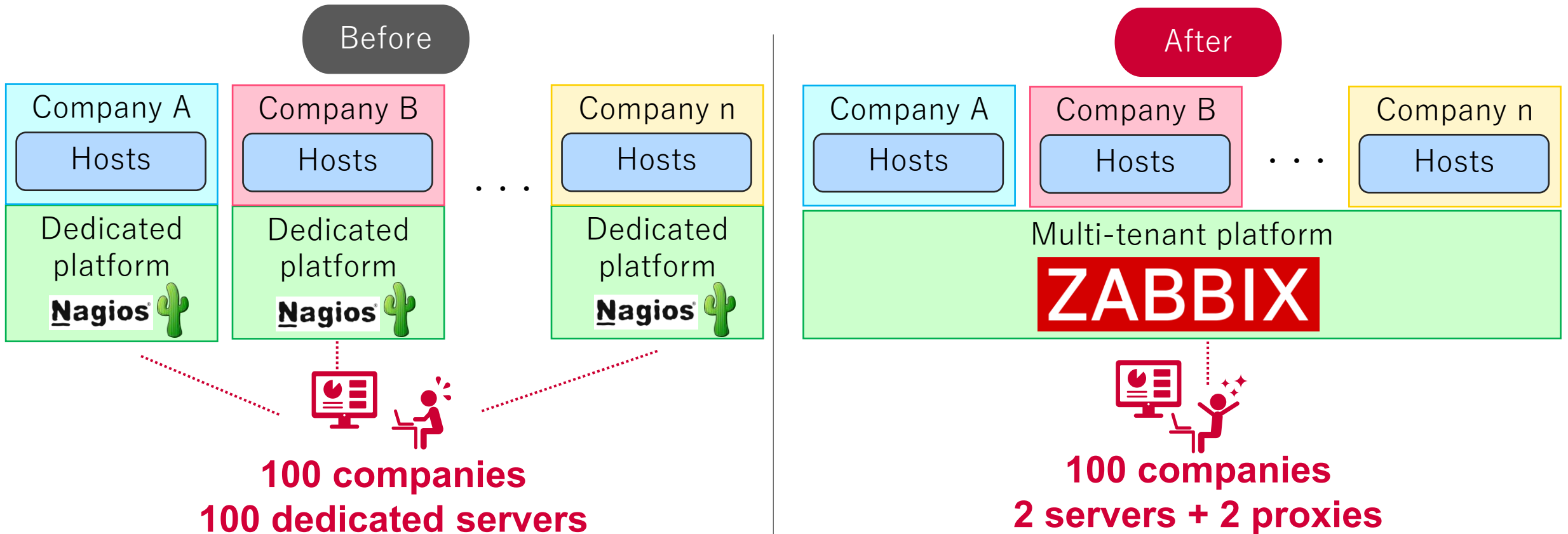
This workflow reduces manual work from detection through ticketing and recovery.

1. Migration from Nagios and Cacti to Zabbix



Case Study on the Zabbix Website

Migrating Nagios and Cacti to a Shared Zabbix Platform



Key Result

100 → 4 servers

Less hardware • lower cost • standardized rules

User Group Permissions Keep Customer Access Separate



Challenge

Multiple customers share one platform.



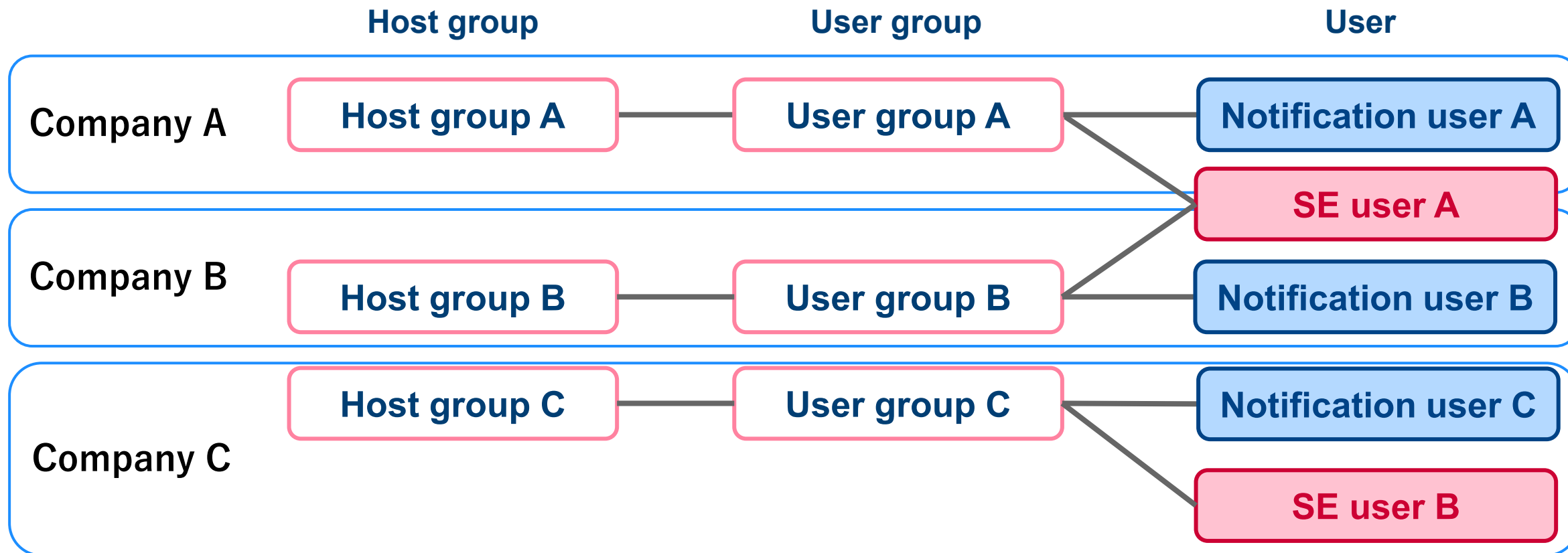
Our Approach

Separate host groups by customer



Result

Separate customer data on the shared platform



Keeping the Same Maximum Detection Time



Challenge

Legacy tools used different check intervals.



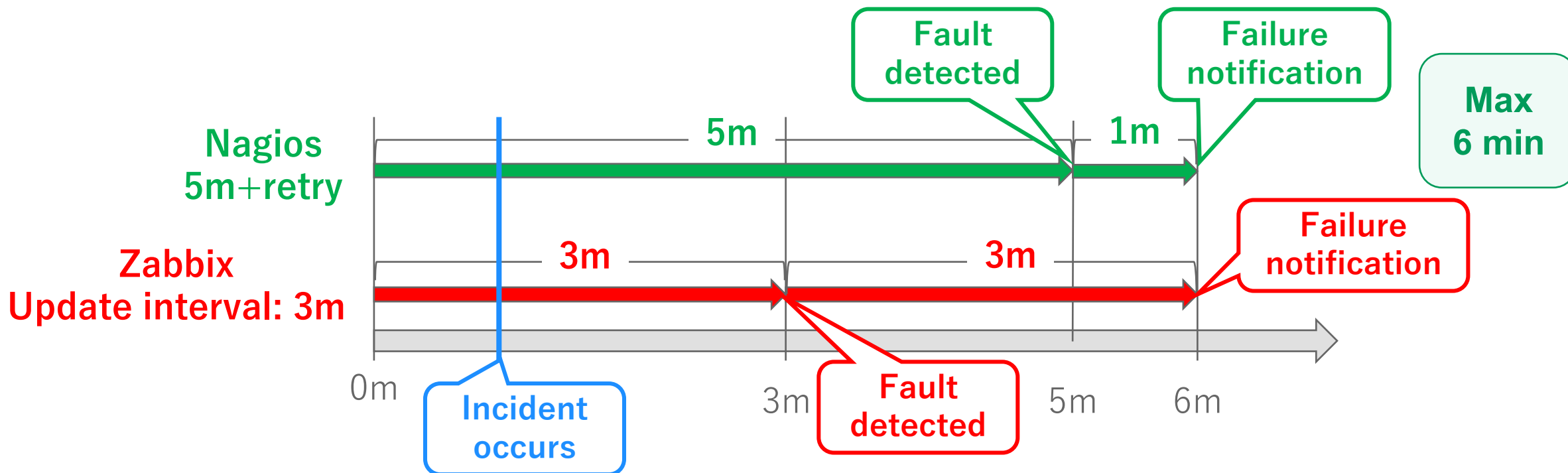
Our Approach

Match Zabbix maximum detection time to Nagios, including retries



Result

Maximum detection time preserved.



Five-Minute Log Notifications with an External Check



Challenge

Original Nagios alert cycle



Our Approach

Replicated the behavior using a custom external check.



Result

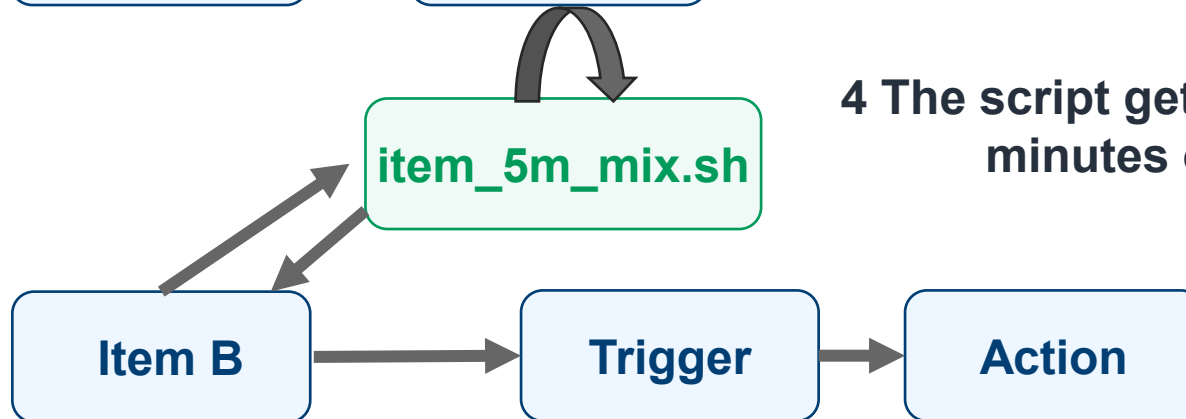
Legacy alerting preserved

1 Capture logs in real-time



2 Store log data in the history.

3 external check every 5 minutes



4 The script gets the last five minutes of data.

5 The trigger creates the alert

Customer Acceptance During Migration



Challenge

customer
acceptance



Our Approach

Explained Zabbix benefits:
HA, maintenance periods,
and standardization.



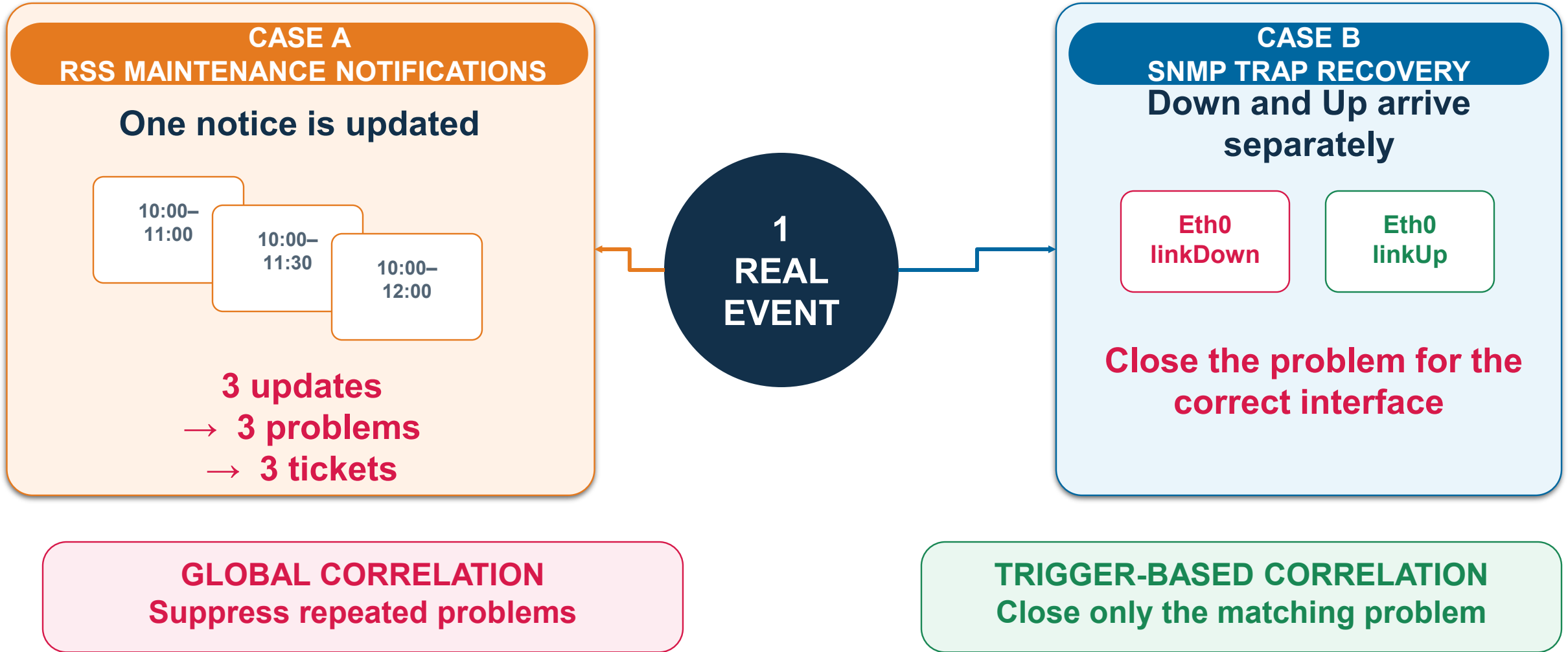
Result

Customers understood
the value and accepted
the change.

Capability	Before (Nagios / Cacti)	After (Zabbix)
 Maintenance	Manual setup	Maintenance periods
 Graphs	Original graph style	Nagios-like graph style
 Email notifications	Different by source	Zabbix only
 System redundancy	Single server	Redundant servers
 Log filtering	Monitoring agent or equipment	Zabbix server
 Recovery	Not linked	Problem and OK events are linked

2. Two Event Correlation Cases

Operational Cases That Required Event Correlation



Two Event Correlation Mechanisms

GLOBAL EVENT CORRELATION

- 1 SCOPE**
Across trigger events
- 2 MATCH**
Match event-tag conditions
- 3 RESULT**
Suppress a repeated new problem

Ex. RSS duplicate suppression

TRIGGER-BASED CORRELATION

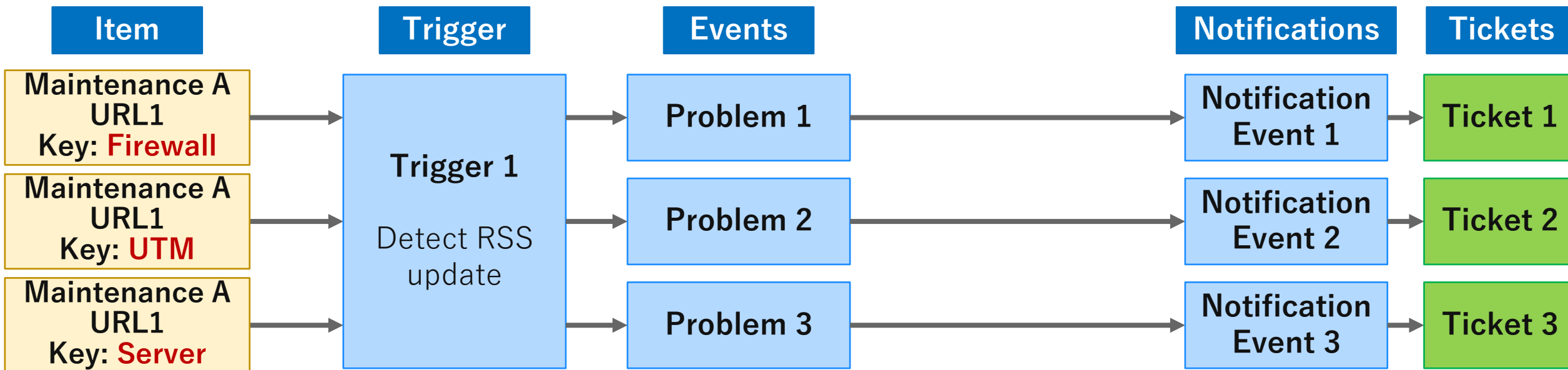
- 1 SCOPE**
Inside one trigger
- 2 MATCH**
Match tag values
- 3 RESULT**
Close the correct open problem

Ex. SNMP Trap recovery

Choose by event behavior, not by the monitoring source

2-1: Duplicate RSS alert suppression

We monitor RSS maintenance with Zabbix.
Sometimes, one maintenance notice contains several keywords.

**Problems:**

1. Duplicate alerts and tickets
2. Operators must identify duplicates
3. Important alerts may be buried

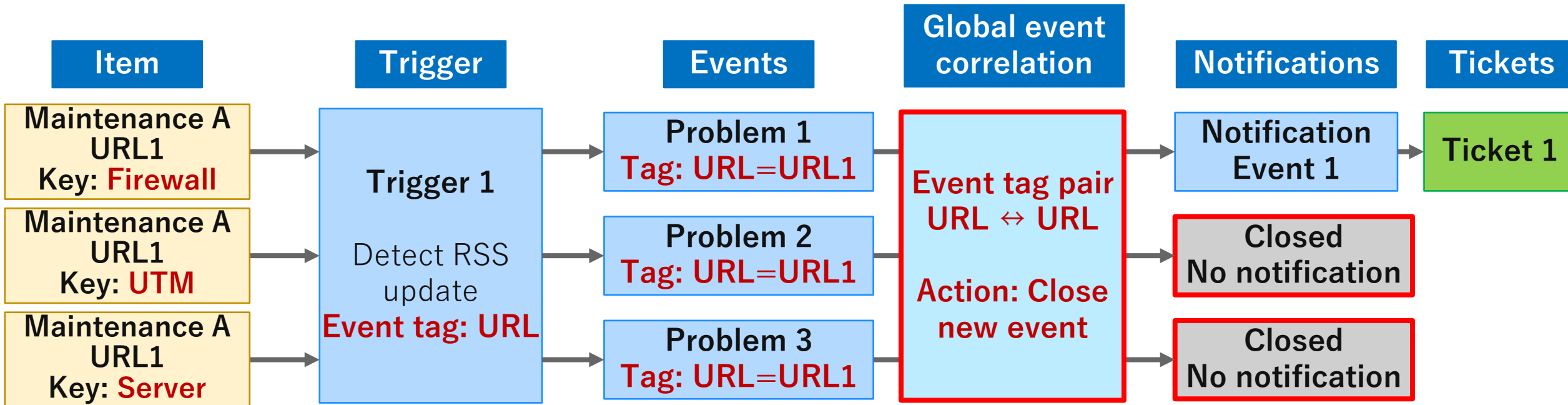
After

Global Event Correlation Closes Duplicate Problems

is

Set the RSS URL as an event tag.

Match the old and new tag values using an Event tag pair condition, then select Close new event.



Improvements:

1. Each maintenance notice creates only one problem notification
2. Duplicate problem events are closed automatically

Other Uses of Global Event Correlation

Use event tags whenever one incident can generate repeated problem events.

Log monitoring

The same error repeats while an incident is active

Tag: error_id

SNMP trap monitoring

The same trap repeats from one device and interface

Tag: host , interface

External service monitoring

The same outage appears across multiple checks

Tag: service , URL

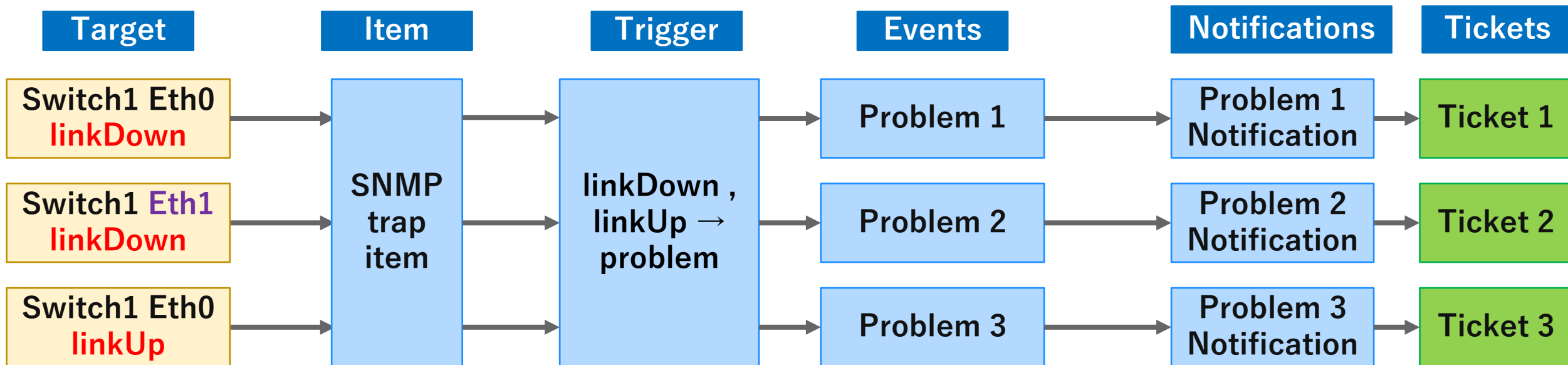
Design tip: use tags that uniquely identify the incident—such as URL, interface, or device.

2-2: SNMP trap recovery

We are receiving SNMP traps for network device interface monitoring.

linkDown and linkUp traps were handled as separate events.

Operators identified the matching interface and closed the problem manually.

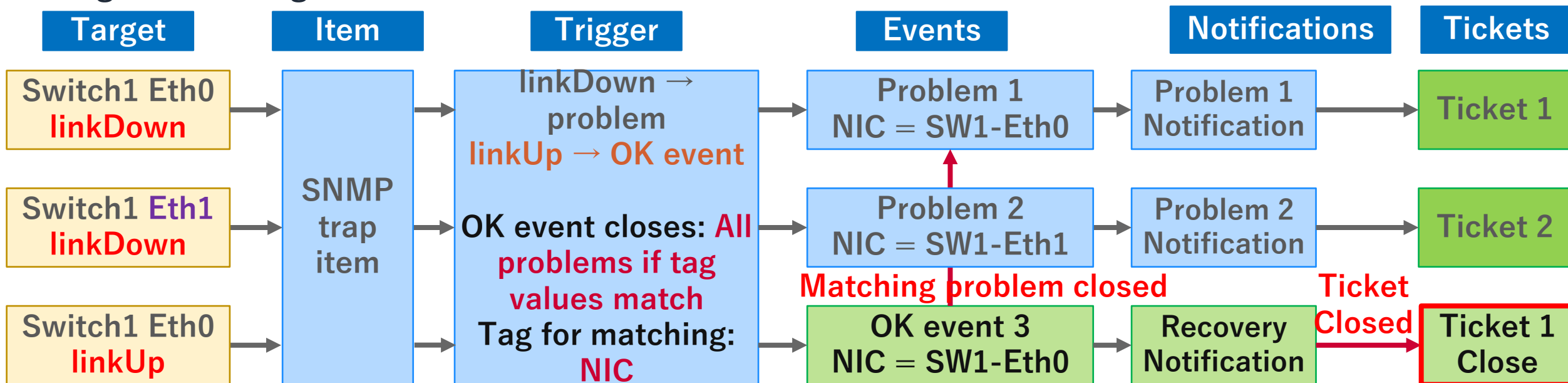


Problems:

1. Operators match linkDown and linkUp manually
2. Multiple interfaces slow identification
3. Recovery traps create extra tickets

With these settings, an OK event closes only the problems that share its tag value.

- PROBLEM event generation mode: Multiple
- OK event closes: All problems if tag values match
- Tag for matching: NIC



Improvements:

1. linkUp closes only the problem with the matching NIC tag
2. The recovery notification closes the related ServiceNow ticket

Summary and Future Vision

Why the Migration Mattered



Operational load

×100

Maintenance repeated
for every server



Availability & quality

1

Single-server risk
and uneven rules



Scale & cost



Rack, power, backup
and refresh costs

Consolidation removed repeated work and made quality easier to standardize

What We Achieved

MIGRATION

100
servers



4
servers

Shared templates • common rules •
lower infrastructure cost

OPERATIONS

1

ticket per incident

NIC

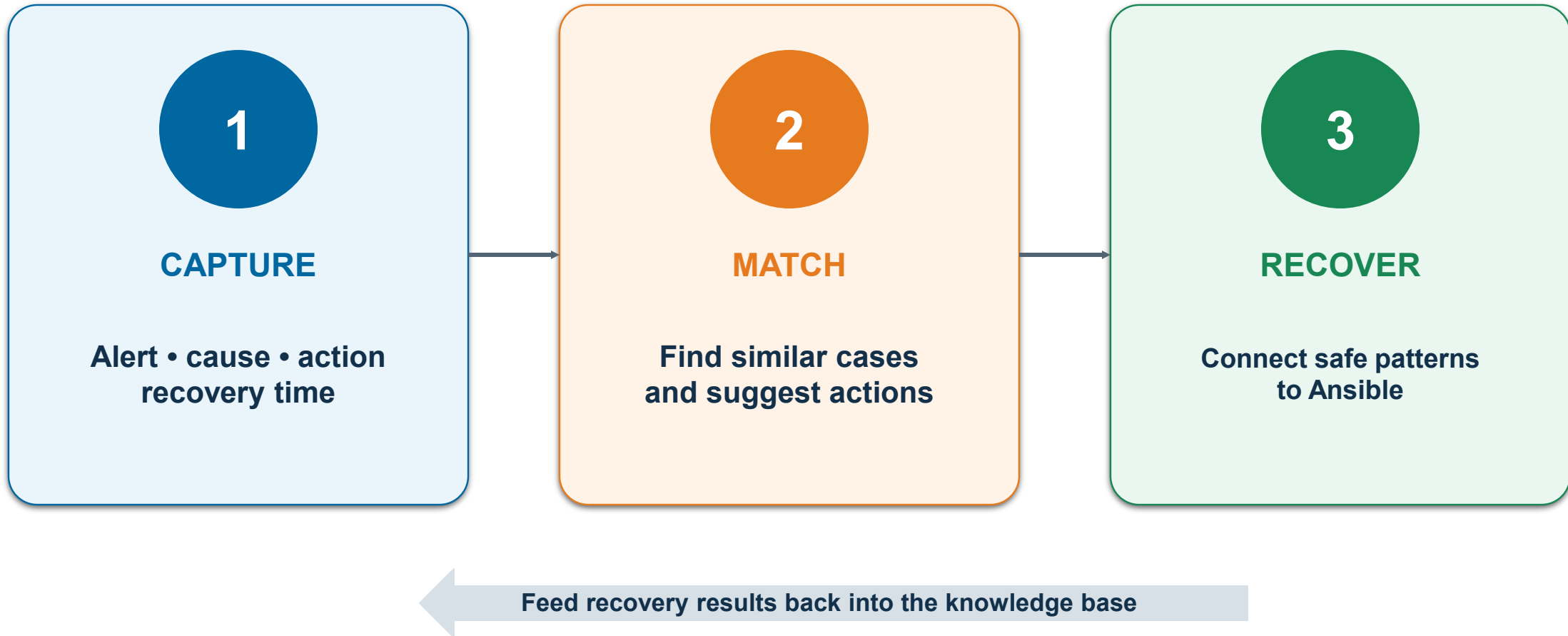
automatic matching

No duplicate RSS tickets • no manual
SNMP recovery matching

Same monitoring coverage — less repeated work

Future Vision: Using Past Experience for Faster Recovery

Reuse operational knowledge from more than 100 customer environments



Visit Our Booth

Explore
**sponsor
booths** and
connect
with fellow
attendees.



Thank you



Satoru Imai
NTT DOCOMO BUSINESS ENGINEERING

Appendix

A detailed introduction to the settings

Item

Item Tags 1 Preprocessing 1

* Name RSS_fic_japan-east

Type External check

* Key RSS_Checker.sh[https://status.sdpf.ntt.com/rss/ja/fic/japan-east/,Test_RSS,rss_fic_] Select

Type of information Text

Host interface 127.0.0.1:10050

* Update interval 0

Custom intervals

Type

Flexible Scheduling

Interval m/5

Period Action

Remove

Processing flow

1. Every five minutes, retrieve RSS updates.
2. Send the RSS data with zabbix_sender.
3. Receive it in a Zabbix trapper item.

Item

Item Tags 1 Preprocessing

* Name RSS_trapper_fic_japan-east

Type Zabbix trapper

* Key rss_fic_japan-east Select

Type of information Text

A detailed introduction to the settings

Trigger

Tags

Name	Value
rss_url	{{ITEM.VALUE}.regsub("^.*?(https?:[/[^\]+).*\$", "\1")}}

Trigger

Tags 1

Dependencies

* Name

RSS_fic_japan-east 【Maintenance】

Event name

RSS_fic_japan-east 【Maintenance】

Operational data

Severity

未分類

情報

警告

軽度の障害

重度の障害

致命的な障害

* Problem expression

find(/Test_RSS/rss_fic_japan-east,, "iregexp", "@RSS_Maintenance")=1

Flow

4. Generate a problem event and set the RSS URL as an event tag
5. Match old/new values with Event tag pair and run Close new event

Event correction

* Name

RSS Duplicate Suppression

* Conditions

Label Name

A

Value of old event tag rss_url equals value of new event tag rss_url

Remove

Add

Description

Operations

☐ Close old events

☒ Close new event

* At least one operation must be selected.

Enabled

☒

Update

Clone

Delete

Cancel

New condition

Type

Event tag pair

* Old tag name

rss_url

Operator

equals

* New tag name

rss_url

Add

Cancel

A detailed introduction to the settings

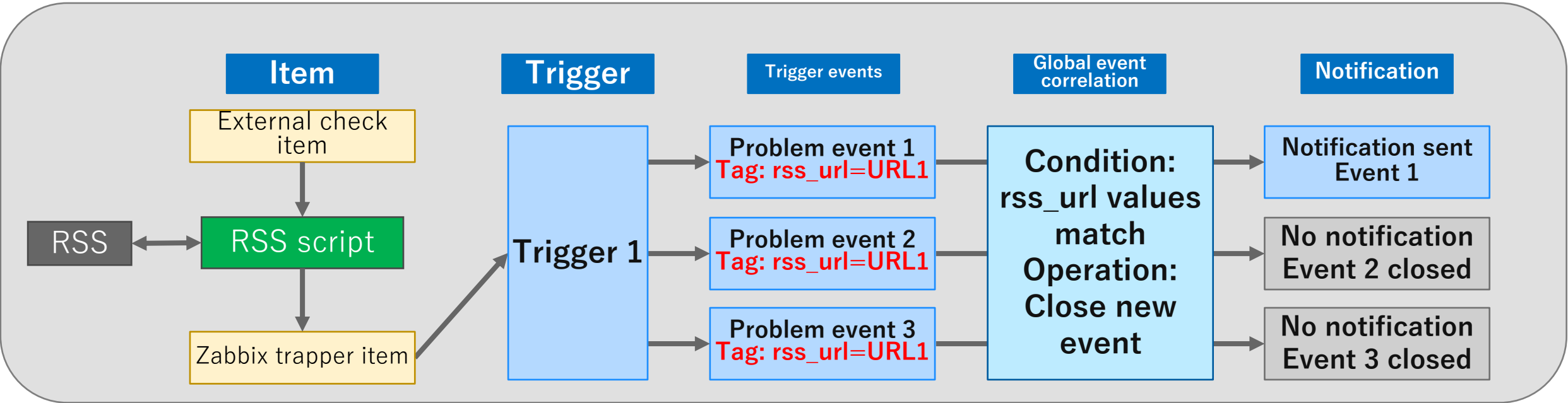
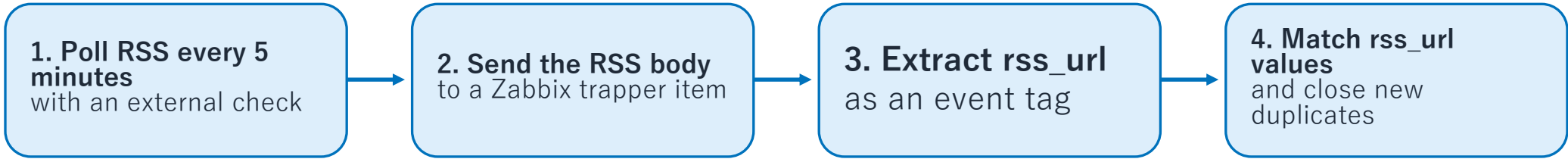
☐	Time ▼	Severity	Recovery time	Status	Info	Host	Problem	Duration	Update	Actions	Tags
☐	09:09:17 PM	重度の障害	09:09:17 PM	RESOLVED		Test_RSS	RSS_fic_japan-east 【Maintenance】	0	Update		Application: RSS rss_url: https://sdpf.ntt...
☐	09:09:15 PM	重度の障害	09:09:15 PM	RESOLVED		Test_RSS	RSS_fic_japan-east 【Maintenance】	0	Update		Application: RSS rss_url: https://sdpf.ntt...
☐	09:09:14 PM	重度の障害		PROBLEM		Test_RSS	RSS_fic_japan-east 【Maintenance】	30s	Update		Application: RSS rss_url: https://sdpf.ntt...

 Test_RSS RSS_fic_japan-east 【Maintenance】

Resolved by event correlation rule "RSS Duplicate Suppression".

Appendix: RSS Alert Suppression Architecture

The RSS workflow combines an external check, a Zabbix trapper item, event tags, and global event correlation.



Appendix: SNMP Trap Items

Receive linkDown and linkUp traps with an SNMP trap item.
Capture unmatched traps with a fallback item for investigation.

Items

All templates / Template SNMP Trap Interface Sta...

Items 2

Triggers 2

Graphs

Dashboards

Discovery rules

Web scenarios

	Name ▲	Triggers	Key	Interval
☐	*** snmptrap (linkDown linkUp)	Triggers 2	snmptrap[linkDown linkUp]	
☐	*** snmptrap.fallback		snmptrap.fallback	

Matching item: snmptrap[regexp]
Receive linkDown / linkUp traps
Evaluate Down / Up in the trigger

Fallback item: snmptrap.fallback
Receive unmatched traps
Use them to improve matching rules

Trigger

Trigger

Tags 1

Dependencies

* Name

Interface {{ITEM.VALUE}.regsub("^(GigabitEthernet[0-9/]+).*\$", "1") is down

Event name

Interface {{ITEM.VALUE}.regsub("^(GigabitEthernet[0-9/]+).*\$", "1") is down

Operational data

Severity

未分類

情報

警告

軽度の障害

重度の障害

致命的な障害

* Problem expression

find(/Template SNMP Trap Interface Status Monitoring/snmptrap[linkDown|linkUp], "like", "linkDown")=1

Expression constructor

Add

OK event generation

Expression

Recovery expression

None

* Recovery expression

find(/Template SNMP Trap Interface Status Monitoring/snmptrap[linkDown|linkUp], "like", "linkUp")=1

Expression constructor

Add

PROBLEM event generation mode

Single

Multiple

OK event closes

All problems

All problems if tag values match

* Tag for matching

interface-tags

© NTT DOCOMO BUSINESS Corporation All Rights Reserved.

33