

# Cause & Symptoms



Business **Centric**

# Life 's upgrade



Life **LTS** is now installed

# The context

Modern IT environments are very complex, where alerts can become overwhelming.

Systems can generate thousands of events, many of which are symptoms of a root cause.

IT teams often struggle to identify which alerts are actual causes and which are downstream symptoms, leading to longer resolution times and potential service disruptions.

"Cause and Symptoms" is Zabbix's answer to this challenge.

# Feature Overview

Introduced with Zabbix 6.4.

The primary goal of "**Cause and Symptoms**" is to reclassify specific problems as "symptom problems" of the "cause problem"

✓ *Alert Noise Reduction*

✓ *Improved resolution times*

# Feature Overview

## How It Works:

- **Data collection and trigger definition:** Zabbix collects continuously data from various sources within the IT infrastructure.
- **Cause:** The primary source of the problem that needs immediate attention.
- **Symptoms:** Secondary alerts triggered by the root cause but not the actual issue.

# How to use it

## Step 1/3

<input type="checkbox"/>	Time ▼	Severity	Recovery time	Status	Info	Host	Problem	Duration	Update	Actions	Tags
<input type="checkbox"/>	01:29:36 PM	Average		PROBLEM		<a href="#">Web server</a>	<a href="#">Failed to fetch status page</a>	27s	<a href="#">Update</a>		
<input type="checkbox"/>	01:29:34 PM	Average		PROBLEM		<a href="#">Web server</a>	<a href="#">Interface eno1: Link down</a>	29s	<a href="#">Update</a>		
<input type="checkbox"/>	01:29:05 PM	Average		PROBLEM		<a href="#">Web server</a>	<a href="#">Service is down</a>	58s	<a href="#">Update</a>		

Displaying 3 of 3 found

Some alerts are present in the **Problem view**

# How to use it

## Step 2/3

The screenshot illustrates the process of marking a problem as a symptom. It shows two instances of the problem management interface. In the top instance, three problems are listed, with the 'Service is down' problem selected. In the bottom instance, the same three problems are shown, but the 'Service is down' problem is now marked as a 'PROBLEM'. A context menu is open over the 'Service is down' problem, with the option 'Mark selected as symptoms' highlighted.

Time	Severity	Recovery time	Status	Info	Host	Problem	Duration	Update	Actions	Tags
01:29:36 PM	Average				Web server	Failed to fetch status page	27s	Update		
01:29:34 PM	Average				Web server	Interface eno1: Link down	29s	Update		
01:29:05 PM	Average				Web server	Service is down	58s	Update		

Time	Severity	Recovery time	Status	Info	Host	Problem	Duration	Update	Actions	Tags
01:29:36 PM	Average		PROBLEM		Web server	Failed to fetch status page	27s	Update		
01:29:34 PM	Average		PROBLEM		Web server	Interface eno1: Link down	29s	Update		
01:29:05 PM	Average		PROBLEM		Web server	Service is down	58s	Update		

Context menu for 'Service is down':

- VIEW
  - Problems
  - History
- CONFIGURATION
  - Trigger
  - Items
- PROBLEM
  - Mark as cause
  - Mark selected as symptoms

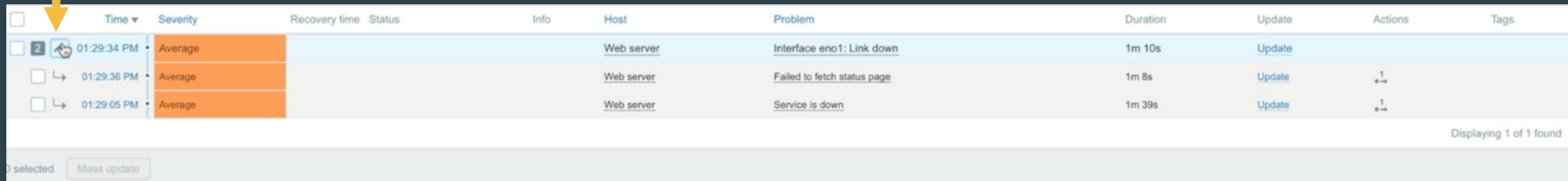
# How to use it

## Step 3/3



<input type="checkbox"/>	Time ▾	Severity	Recovery time	Status	Info	Host	Problem	Duration	Update	Actions	Tags
<input type="checkbox"/>	2 01:29:34 PM	Average		PROBLEM		Web server	Interface eno1: Link down	1m 10s	<a href="#">Update</a>		

0 selected [Mass update](#) Displaying 1 of 1 found



<input type="checkbox"/>	Time ▾	Severity	Recovery time	Status	Info	Host	Problem	Duration	Update	Actions	Tags
<input type="checkbox"/>	2 01:29:34 PM	Average				Web server	Interface eno1: Link down	1m 10s	<a href="#">Update</a>		
<input type="checkbox"/>	↳ 01:29:36 PM	Average				Web server	Failed to fetch status page	1m 8s	<a href="#">Update</a>	1	
<input type="checkbox"/>	↳ 01:29:05 PM	Average				Web server	Service is down	1m 39s	<a href="#">Update</a>	1	

0 selected [Mass update](#) Displaying 1 of 1 found

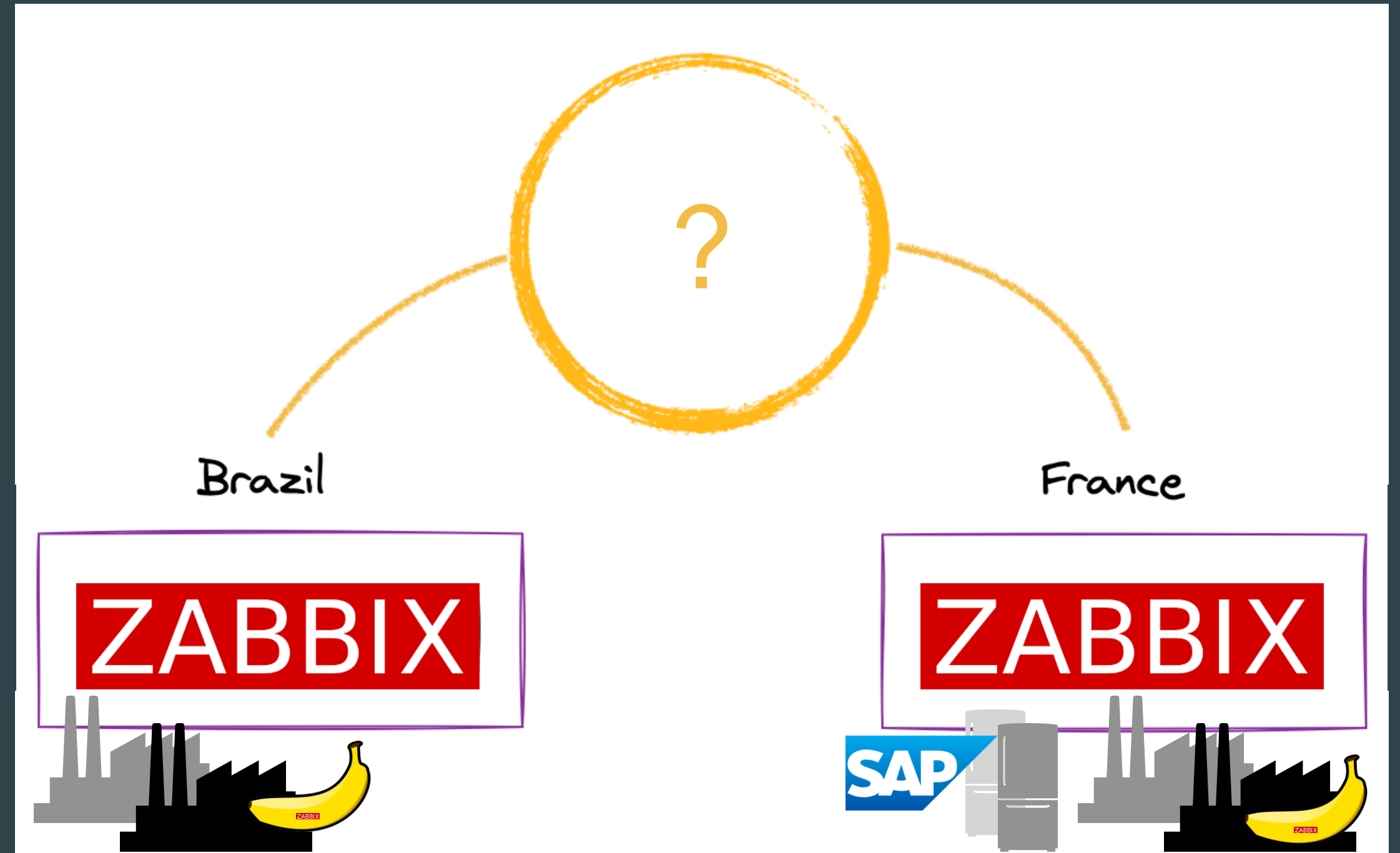
**Too much manual work** to do in order to classify causes and symptoms



# Ba-na-na time



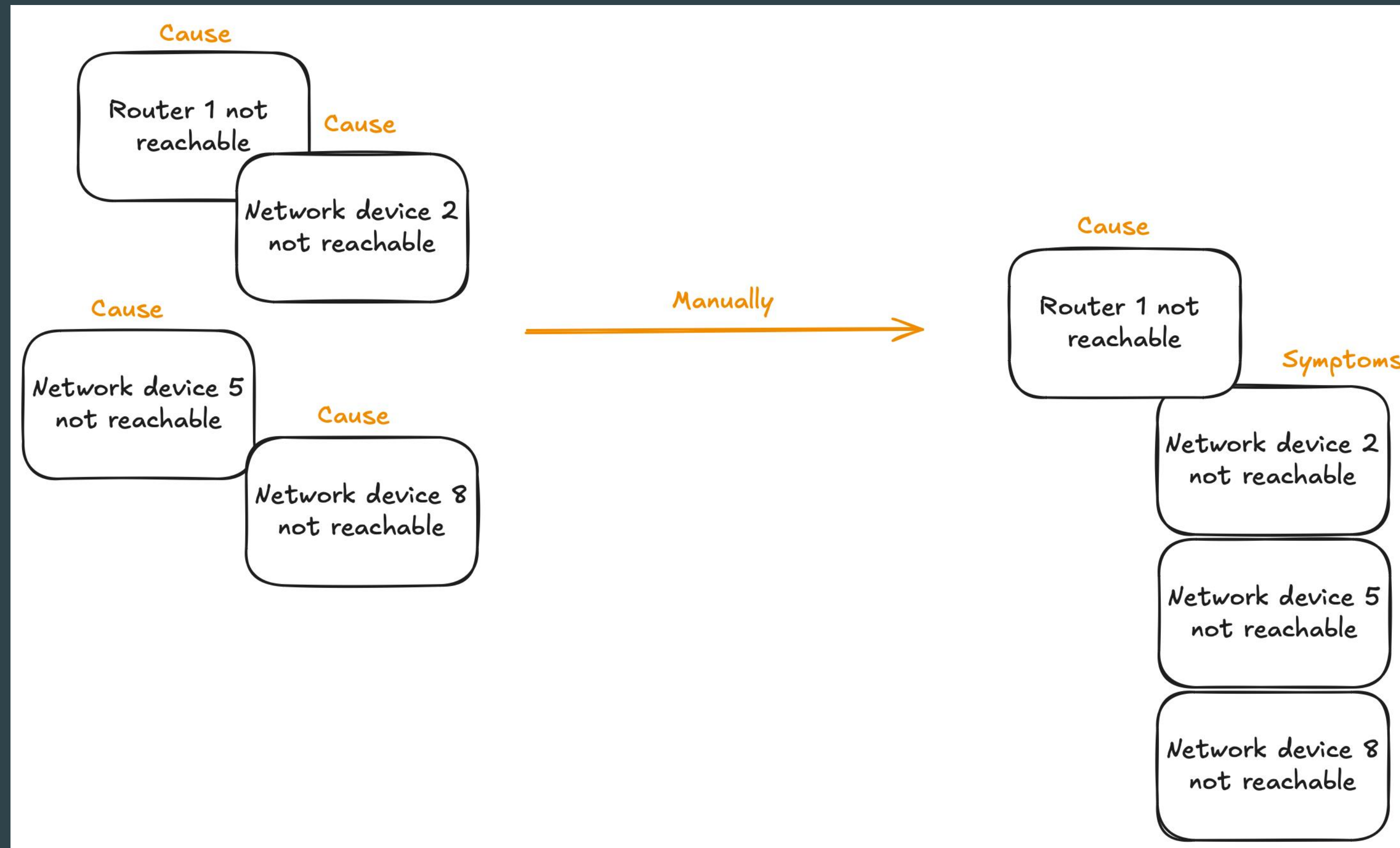
# Case study : the "Banana factory"



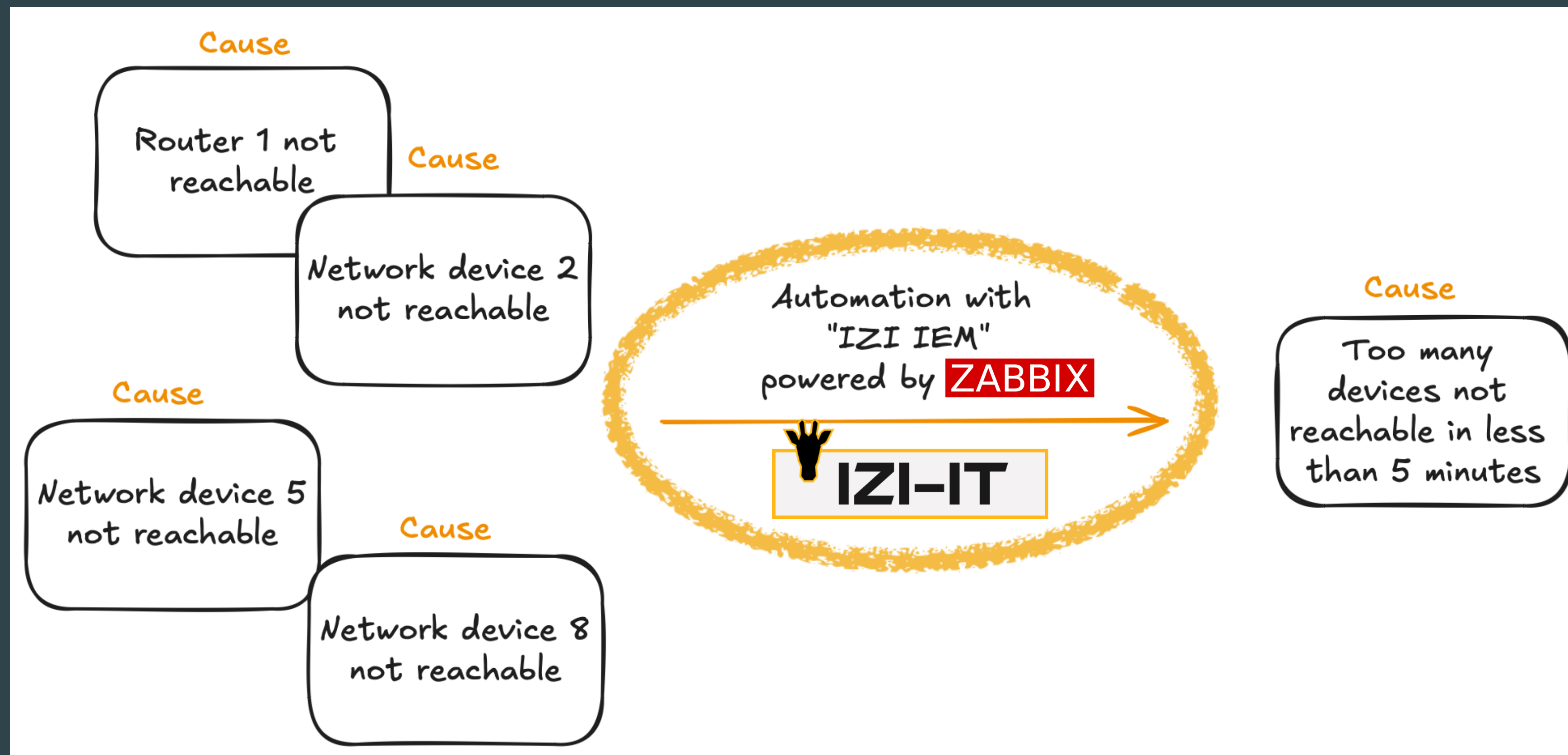
Separate Zabbix instance for the same Banana factory

To view in a single pane of glass the status of our services

# Real world alarms



# How do we enhance?



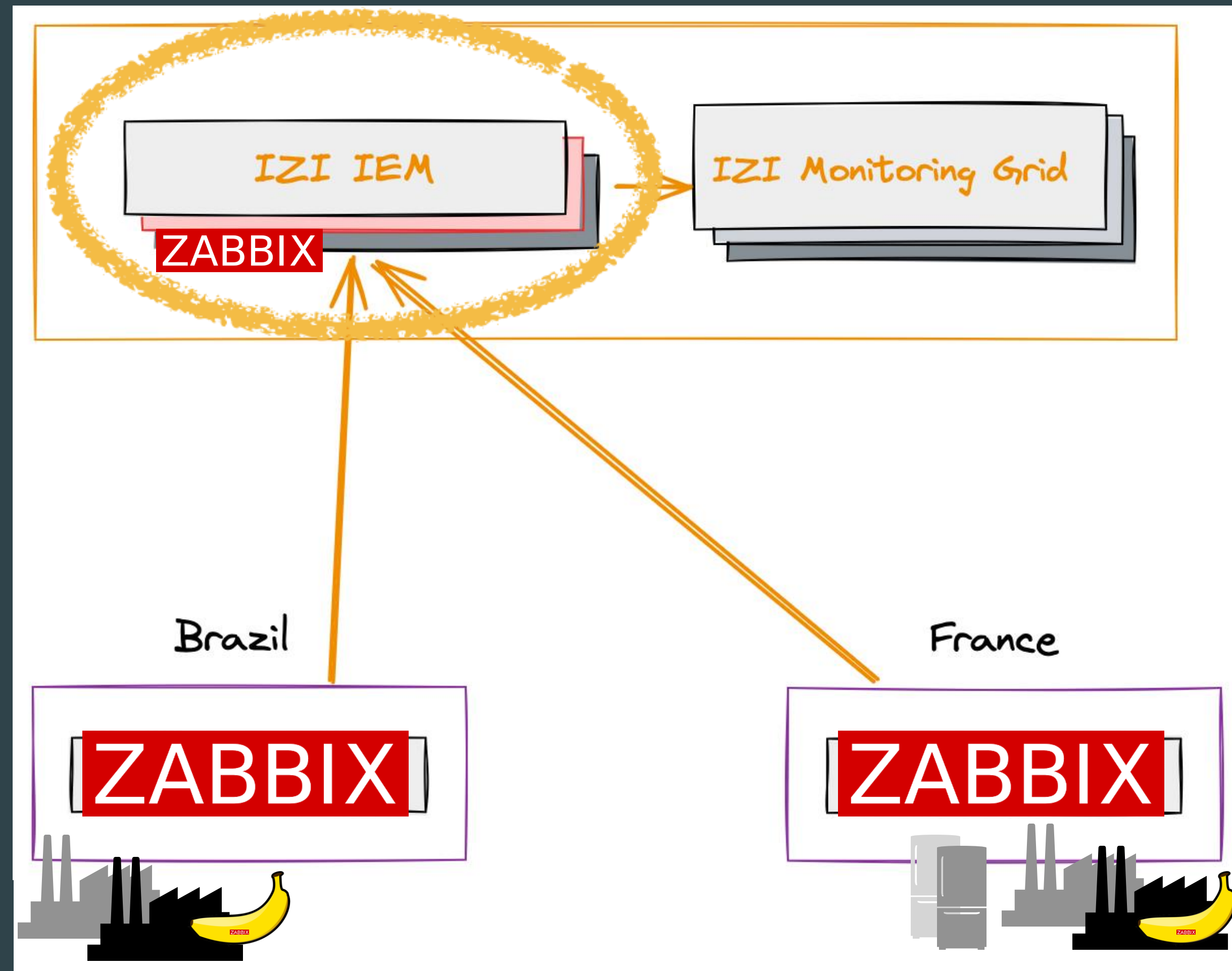
# Usage of "Cause & Symptoms" functionality w

<input type="checkbox"/>	Time ▾	Severity	Info	Host	Problem	Duration	Update	Actions	Tags
<input type="checkbox"/>	19:35:33	Average		<a href="#">Server B</a>	<a href="#">Linux: Zabbix agent is not available</a>	14s	<a href="#">Update</a>	4 →	<a href="#">component: system</a> <a href="#">scope: availability</a>
<input type="checkbox"/>	19:35:28	High		<a href="#">Network device 2</a>	<a href="#">Network device 2 is not available</a>	19s	<a href="#">Update</a>	4 →	<a href="#">component: availability</a> <a href="#">device: network</a>
<input type="checkbox"/>	19:35:24	High		<a href="#">Network device 10</a>	<a href="#">Network device 10 is not available</a>	23s	<a href="#">Update</a>	4 →	<a href="#">component: availability</a> <a href="#">device: network</a>
<input type="checkbox"/>	19:35:18	High		<a href="#">Network device 12</a>	<a href="#">Network device 12 is not available</a>	29s	<a href="#">Update</a>	4 →	<a href="#">component: availability</a> <a href="#">device: network</a>
<input type="checkbox"/>	19:35:08	Average		<a href="#">Server C</a>	<a href="#">Linux: Zabbix agent is not available</a>	39s	<a href="#">Update</a>	4 →	<a href="#">component: system</a> <a href="#">scope: availability</a>
<input type="checkbox"/>	19:35:04	Average		<a href="#">Server A</a>	<a href="#">Linux: Zabbix agent is not available</a>	43s	<a href="#">Update</a>	4 →	<a href="#">component: system</a> <a href="#">scope: availability</a>

<input type="checkbox"/>	Time ▾	Severity	Info	Host	Problem	Duration	Update	Actions	Tags
<input checked="" type="checkbox"/>	6 ^ 19:36:00	Information		<a href="#">IZI IEM</a>	<a href="#">Too many unavailable device detected in less than 5 minutes</a>	51s	<a href="#">Update</a>	4 →	<a href="#">component: business</a>
<input type="checkbox"/>	↳ 19:35:58	High		<a href="#">Network device 8</a>	<a href="#">Network device 8 is not available</a>	53s	<a href="#">Update</a>	5 →	<a href="#">component: availability</a> <a href="#">device: network</a>
<input type="checkbox"/>	↳ 19:35:54	High		<a href="#">Network device 5</a>	<a href="#">Network device 5 is not available</a>	57s	<a href="#">Update</a>	5 →	<a href="#">component: availability</a> <a href="#">device: network</a>
<input type="checkbox"/>	↳ 19:35:49	High		<a href="#">Router device 1</a>	<a href="#">Router device 1 is not available</a>	1m 2s	<a href="#">Update</a>	5 →	<a href="#">component: availability</a> <a href="#">device: network</a>
<input type="checkbox"/>	↳ 19:35:28	High		<a href="#">Network device 2</a>	<a href="#">Network device 2 is not available</a>	1m 23s	<a href="#">Update</a>	5 →	<a href="#">component: availability</a> <a href="#">device: network</a>
<input type="checkbox"/>	↳ 19:35:24	High		<a href="#">Network device 10</a>	<a href="#">Network device 10 is not available</a>	1m 27s	<a href="#">Update</a>	5 →	<a href="#">component: availability</a> <a href="#">device: network</a>
<input type="checkbox"/>	↳ 19:35:18	High		<a href="#">Network device 12</a>	<a href="#">Network device 12 is not available</a>	1m 33s	<a href="#">Update</a>	5 →	<a href="#">component: availability</a> <a href="#">device: network</a>
<input type="checkbox"/>	19:35:33	Average		<a href="#">Server B</a>	<a href="#">Linux: Zabbix agent is not available</a>	1m 18s	<a href="#">Update</a>	4 →	<a href="#">component: system</a> <a href="#">scope: availability</a>
<input type="checkbox"/>	19:35:08	Average		<a href="#">Server C</a>	<a href="#">Linux: Zabbix agent is not available</a>	1m 43s	<a href="#">Update</a>	4 →	<a href="#">component: system</a> <a href="#">scope: availability</a>
<input type="checkbox"/>	19:35:04	Average		<a href="#">Server A</a>	<a href="#">Linux: Zabbix agent is not available</a>	1m 47s	<a href="#">Update</a>	4 →	<a href="#">component: system</a> <a href="#">scope: availability</a>

# IZI I.E.M.

IZI IEM (IZI Intelligent Event Management) is a business rule manager based on Zabbix.



# IZI I.E.M. Interface

## Rules definition

IZI IEM Rules Zabbix IZI Monitoring Grid admin Logout

### IEM Rule Generator

Alert Name:

Over (Time Period):

Occurrences:

Content to match:

Operator:

Content to match:

Occurrences:

Operator:

Tags (optional):

IZI IEM Rules Zabbix IZI Monitoring Grid admin Logout

### Defined Rules

Name	Rules	Status
Too many failed login attempt detected in less than 5 minutes		Active <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Deactivate"/>
Too many unauthorized access error detected in less than 5 minutes		Active <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Deactivate"/>
Too many unavailable device detected in less than 5 minutes		Active <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Deactivate"/>
Too much Error 500 detected in less than 5 minutes		Active <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Deactivate"/>

# IZI I.E.M. processing...

<input type="checkbox"/>	Time ▾	Severity	Info	Host	Problem	Duration	Update	Actions	Tags
<input type="checkbox"/>	19:35:33	Average		Server B	Linux: Zabbix agent is not available	14s	<a href="#">Update</a>	4 →	component: system scope: availability
<input type="checkbox"/>	19:35:28	High		Network device 2	Network device 2 is not available	19s	<a href="#">Update</a>	4 →	component: availability device: network
<input type="checkbox"/>	19:35:24	High		Network device 10	Network device 10 is not available	23s	<a href="#">Update</a>	4 →	component: availability device: network
<input type="checkbox"/>	19:35:18	High		Network device 12	Network device 12 is not available	29s	<a href="#">Update</a>	4 →	component: availability device: network
<input type="checkbox"/>	19:35:08	Average		Server C	Linux: Zabbix agent is not available	39s	<a href="#">Update</a>	4 →	component: system scope: availability
<input type="checkbox"/>	19:35:04	Average		Server A	Linux: Zabbix agent is not available	43s	<a href="#">Update</a>	4 →	component: system scope: availability



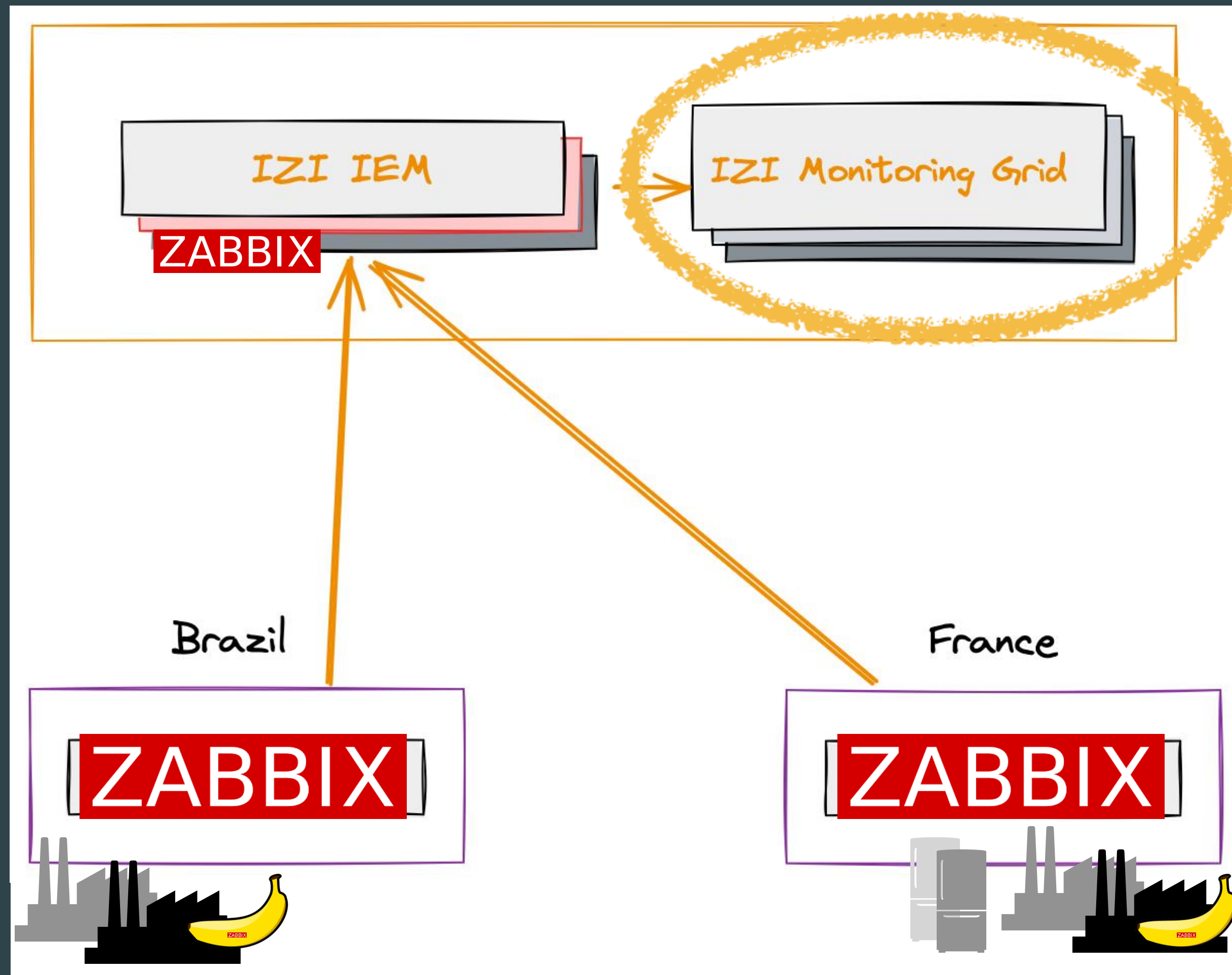
IZI IEM

<input type="checkbox"/>	Time ▾	Severity	Info	Host	Problem	Duration	Update	Actions	Tags
<input type="checkbox"/>	6 ^ 19:36:00	Information		IZI IEM	Too many unavailable device detected in less than 5 minutes	51s	<a href="#">Update</a>	4 →	component: business
<input type="checkbox"/>	↳ 19:35:58	High		Network device 8	Network device 8 is not available	53s	<a href="#">Update</a>	5 →	component: availability device: network
<input type="checkbox"/>	↳ 19:35:54	High		Network device 5	Network device 5 is not available	57s	<a href="#">Update</a>	5 →	component: availability device: network
<input type="checkbox"/>	↳ 19:35:49	High		Router device 1	Router device 1 is not available	1m 2s	<a href="#">Update</a>	5 →	component: availability device: network
<input type="checkbox"/>	↳ 19:35:28	High		Network device 2	Network device 2 is not available	1m 23s	<a href="#">Update</a>	5 →	component: availability device: network
<input type="checkbox"/>	↳ 19:35:24	High		Network device 10	Network device 10 is not available	1m 27s	<a href="#">Update</a>	5 →	component: availability device: network
<input type="checkbox"/>	↳ 19:35:18	High		Network device 12	Network device 12 is not available	1m 33s	<a href="#">Update</a>	5 →	component: availability device: network
<input type="checkbox"/>	19:35:33	Average		Server B	Linux: Zabbix agent is not available	1m 18s	<a href="#">Update</a>	4 →	component: system scope: availability
<input type="checkbox"/>	19:35:08	Average		Server C	Linux: Zabbix agent is not available	1m 43s	<a href="#">Update</a>	4 →	component: system scope: availability
<input type="checkbox"/>	19:35:04	Average		Server A	Linux: Zabbix agent is not available	1m 47s	<a href="#">Update</a>	4 →	component: system scope: availability



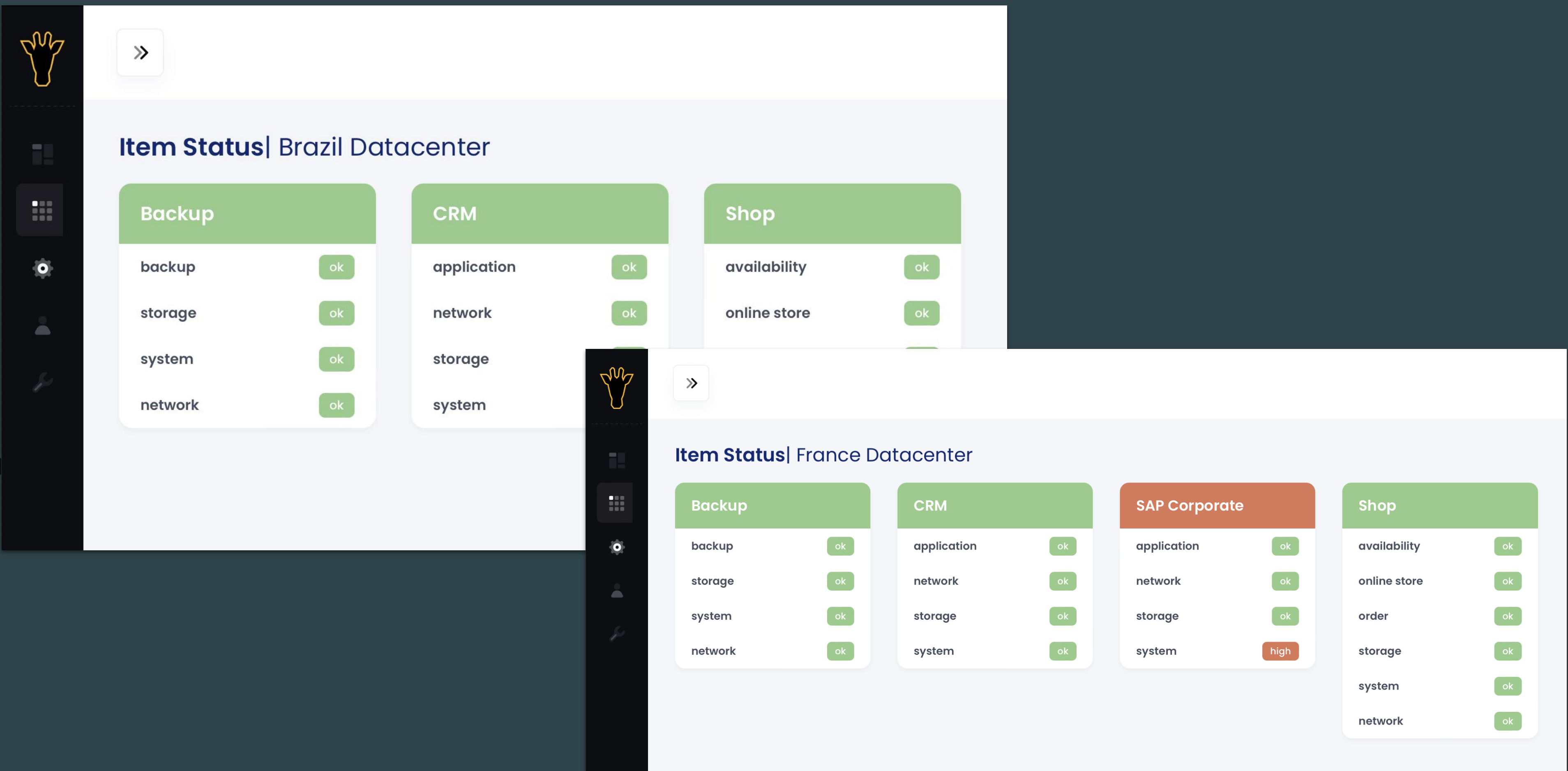
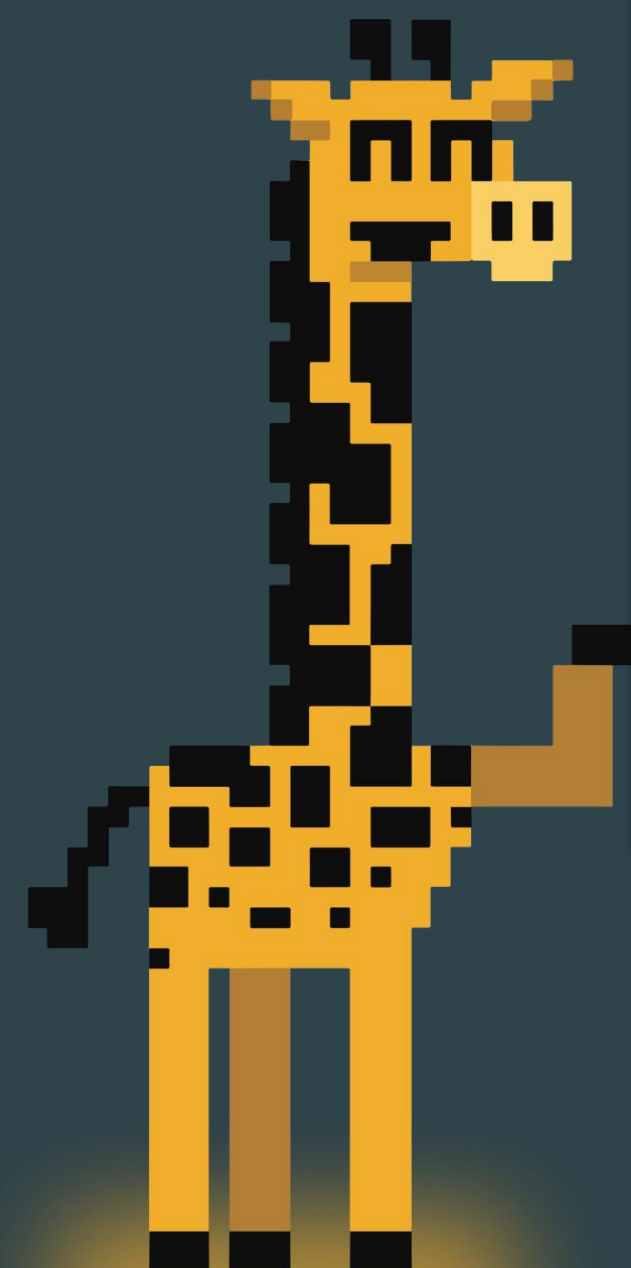


# IZI Monitoring Grid



IZI Monitoring Grid is a innovative way to visualize your key performance indicators in a single place.

# The technical view



The dashboard displays the following data:

### Item Status | Brazil Datacenter

Category	Item	Status
Backup	backup	ok
	storage	ok
	system	ok
	network	ok
CRM	application	ok
	network	ok
	storage	ok
Shop	availability	ok
	online store	ok

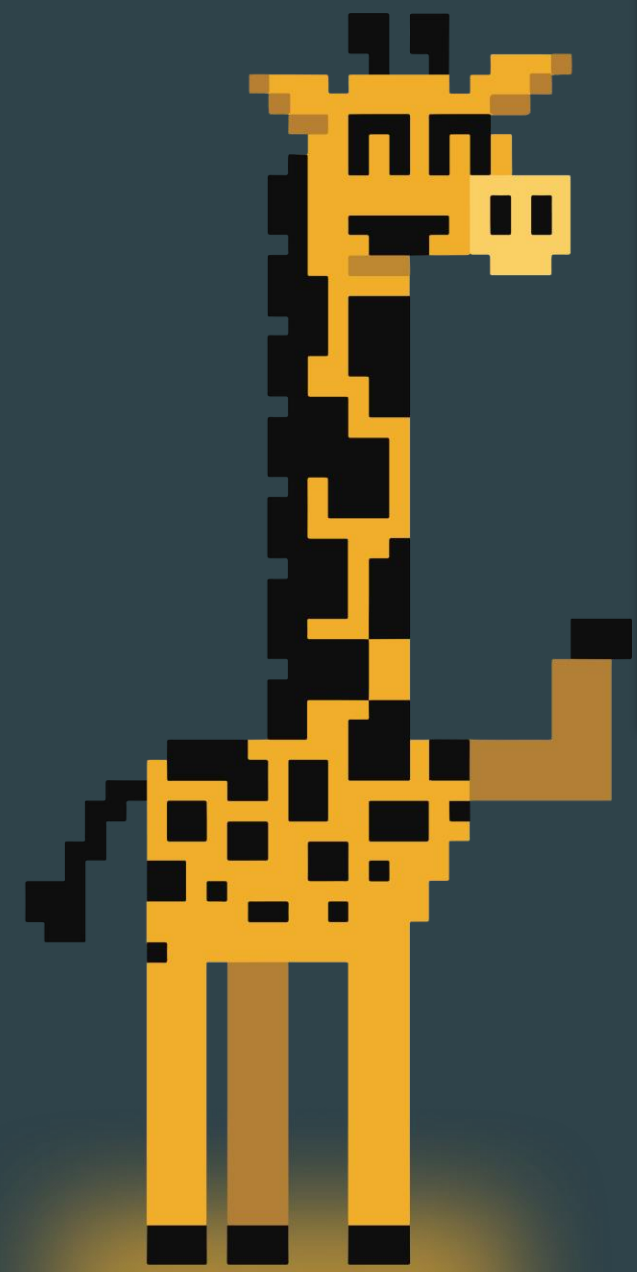
### Item Status | France Datacenter

Category	Item	Status
Backup	backup	ok
	storage	ok
	system	ok
	network	ok
CRM	application	ok
	network	ok
	storage	ok
SAP Corporate	application	ok
	network	ok
	storage	ok
Shop	availability	ok
	online store	ok
	order	ok
	storage	ok
System	system	ok
	network	ok
	system	high

# The technical view



# The business view



## Item Status | Business view

Backup - BV	CRM - BV	SAP Corporate - BV	Security - BV	Shop - BV
availability <span>ok</span>	availability <span>ok</span>	availability <span>ok</span>	availability <span>ok</span>	availability <span>ok</span>
integrity <span>ok</span>	integrity <span>ok</span>	integrity <span>ok</span>	integrity <span>ok</span>	integrity <span>ok</span>
performance <span>average</span>	performance <span>average</span>	performance <span>ok</span>	performance <span>ok</span>	performance <span>average</span>
security <span>ok</span>	security <span>ok</span>	security <span>ok</span>	security <span>ok</span>	security <span>ok</span>

# Conclusion



As we always said, **Small is beautiful!**

Thanks for Zabbix's functionality "**Cause & Symptoms.**"



*Biggest wild banana breeder*

- French-speaking community leader
- Focus to made Zabbix **IZI**-er for you

📧 Steve Destivelle

👉 [contact@izi-it.io](mailto:contact@izi-it.io)