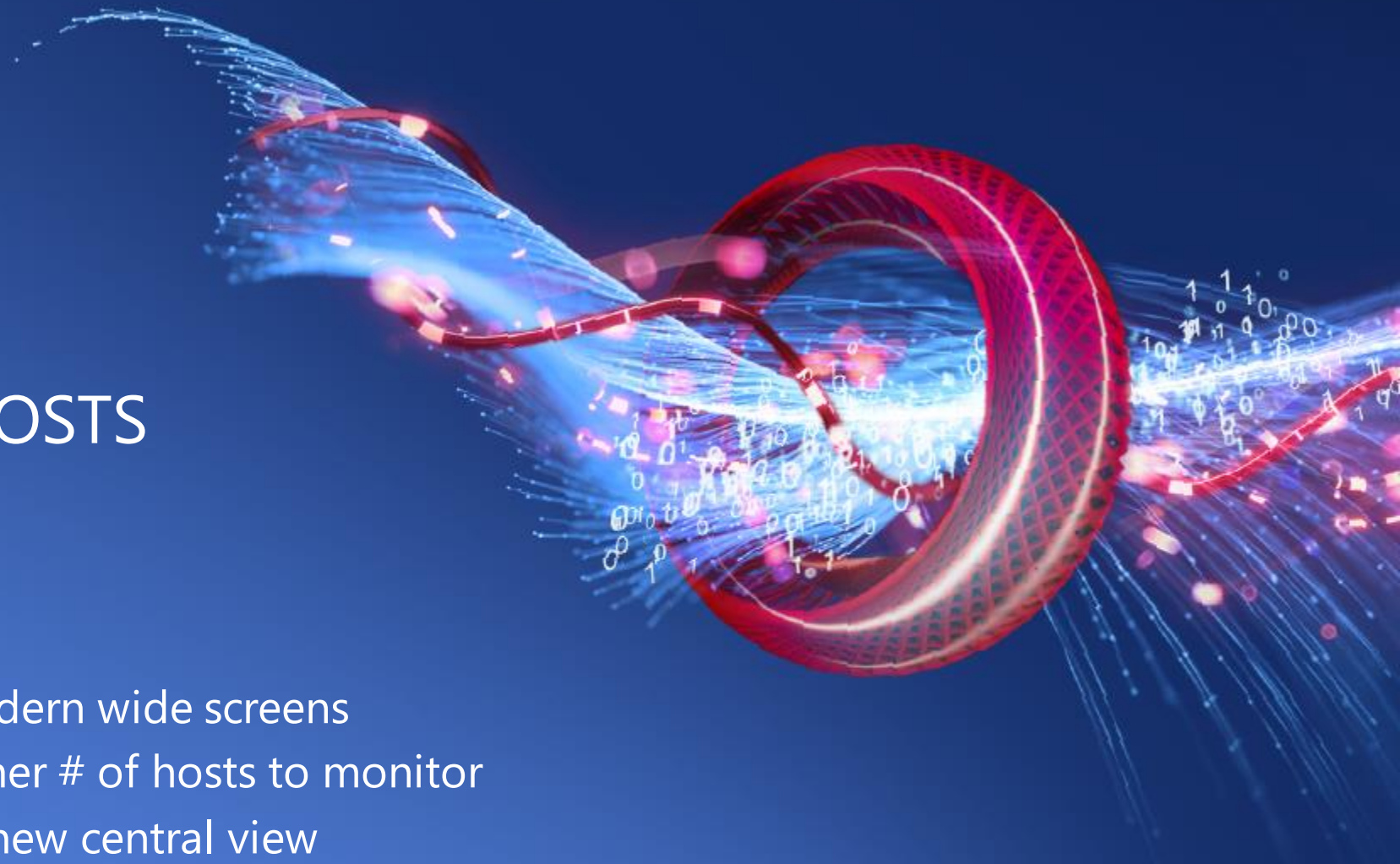
ZABBIX 5.0

(MY PERSONAL...) KEY FEATURES IN DETAIL

Christian Anton, secadm GmbH
Christian.Anton@secadm.de

SECADM
SECURE FOR SURE

01

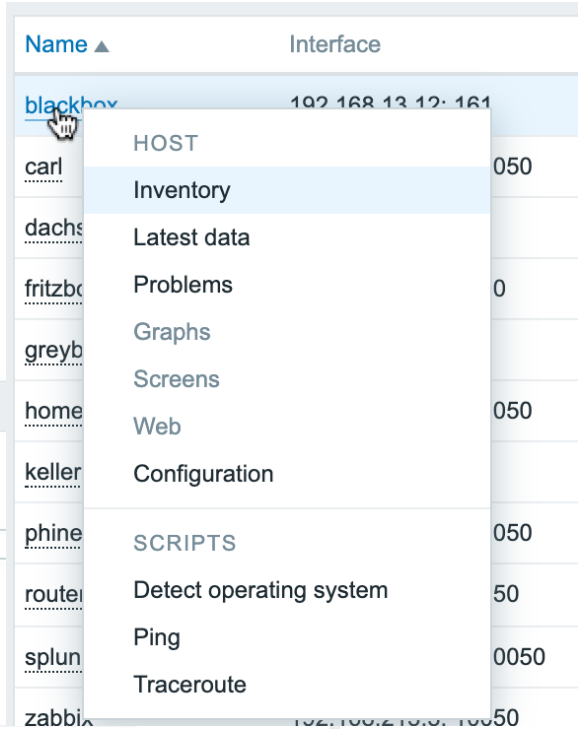


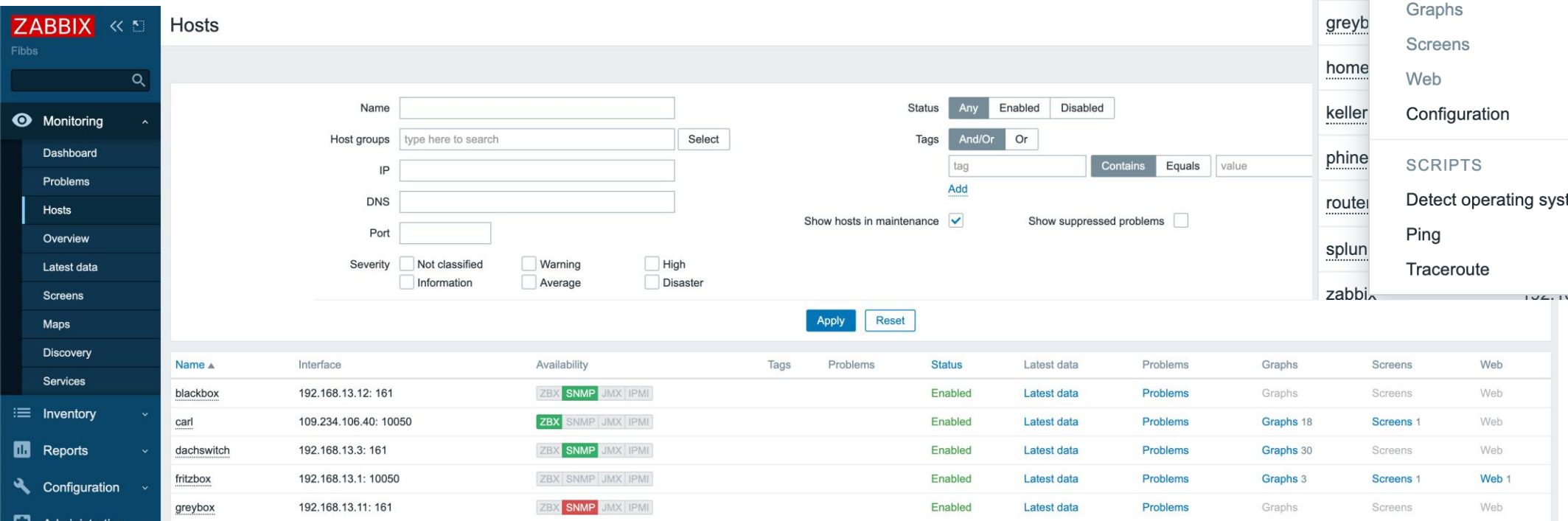
MONITORING → HOSTS AND THE NEW GUI

- New menu respecting modern wide screens
- Changes for handling higher # of hosts to monitor
- Monitoring → Hosts as a new central view
- Minor improvements

LIST OF MONITORED DEVICES
WHERE AM I AND WHAT IS THERE TO SEE?

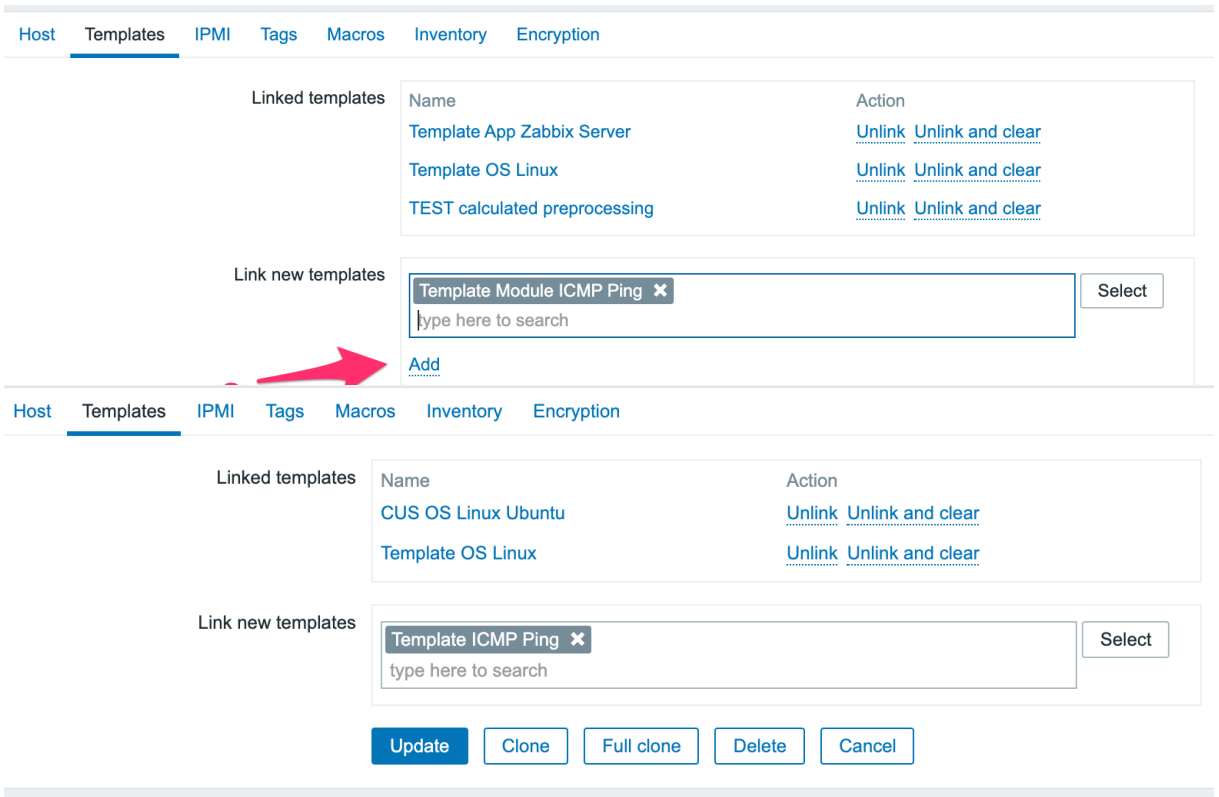
- Long desired feature
- Overview of non-admins / visibility of Host Availability
- For admins: easier to get from viewing to setting things up and back

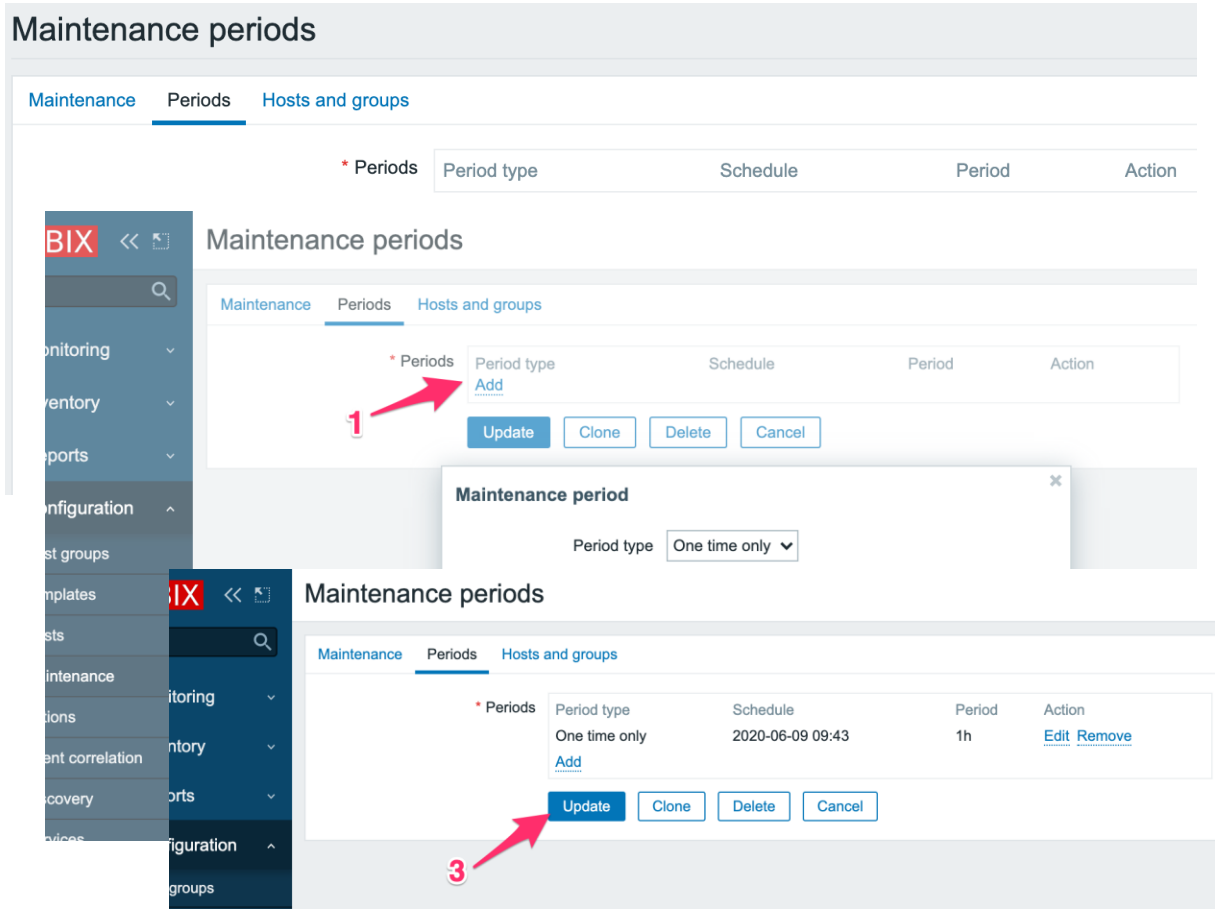




SECADM
SECURE FOR SURE

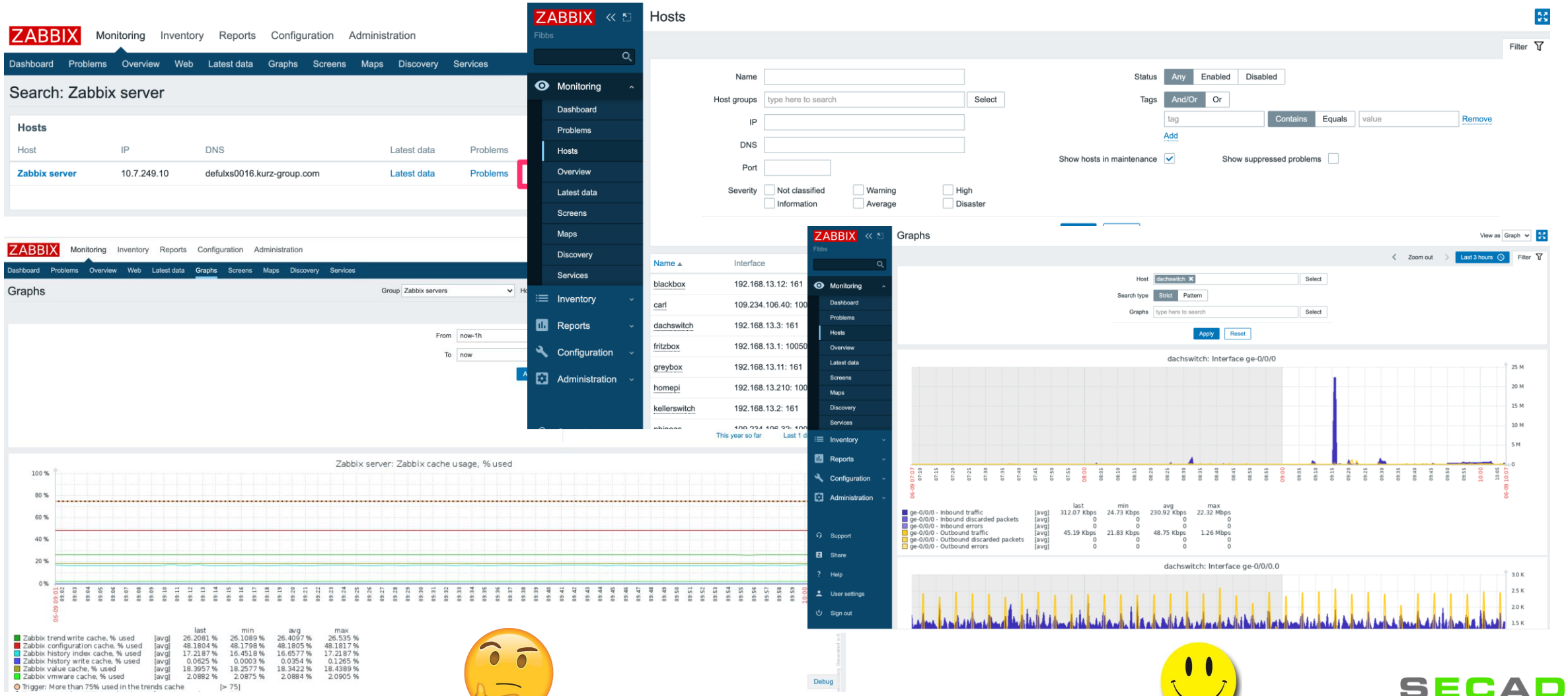
BETTER ADDING OF ELEMENTS TO OBJECTS
NO MORE «ADD, ADD, UPDATE»...





SECADM
SECURE FOR SURE

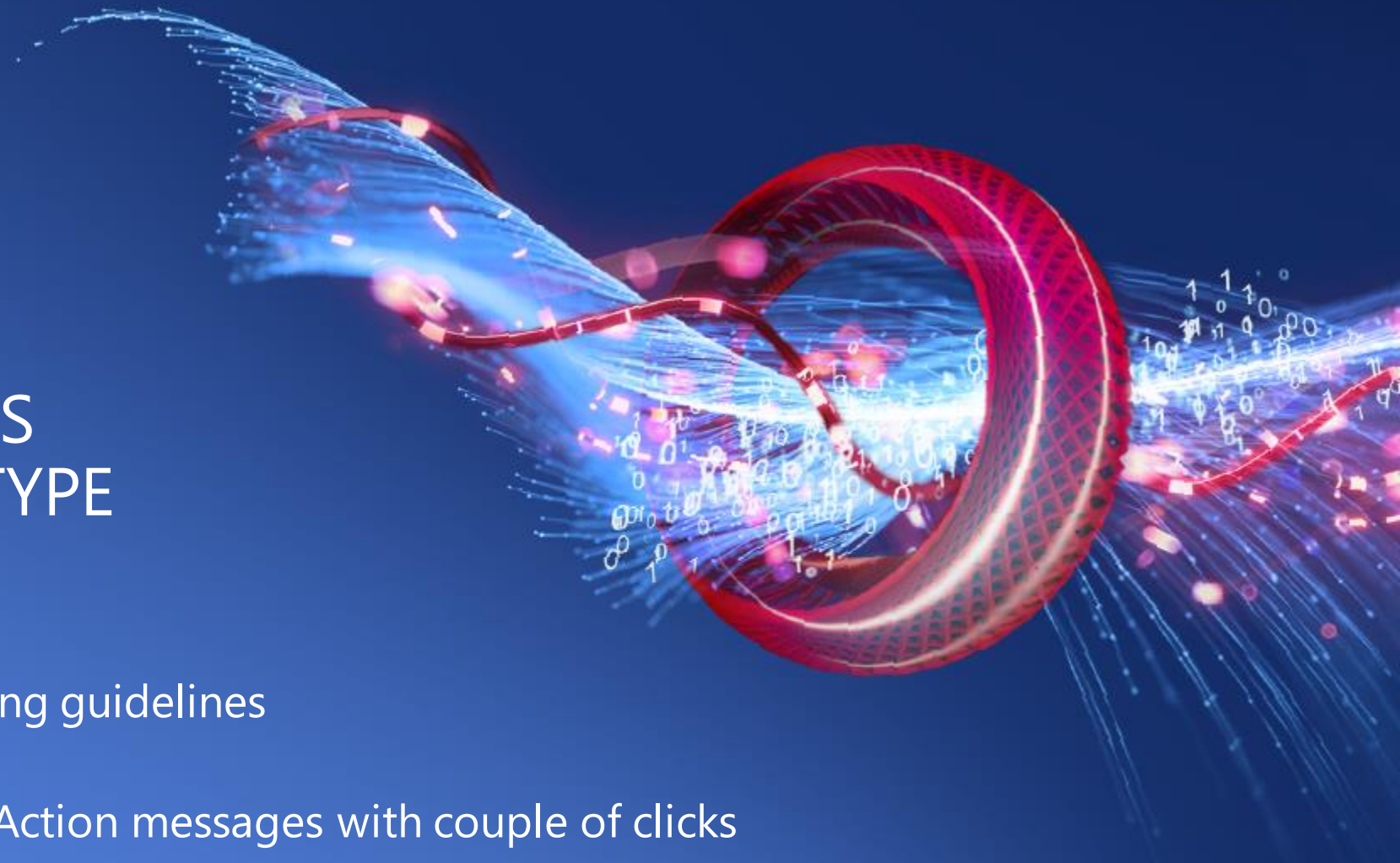
MONITORING → HOSTS → GRAPHS
DIRECT ACCESS TO ALL GRAPHS FOR ONE HOST



SECADM
SECURE FOR SURE

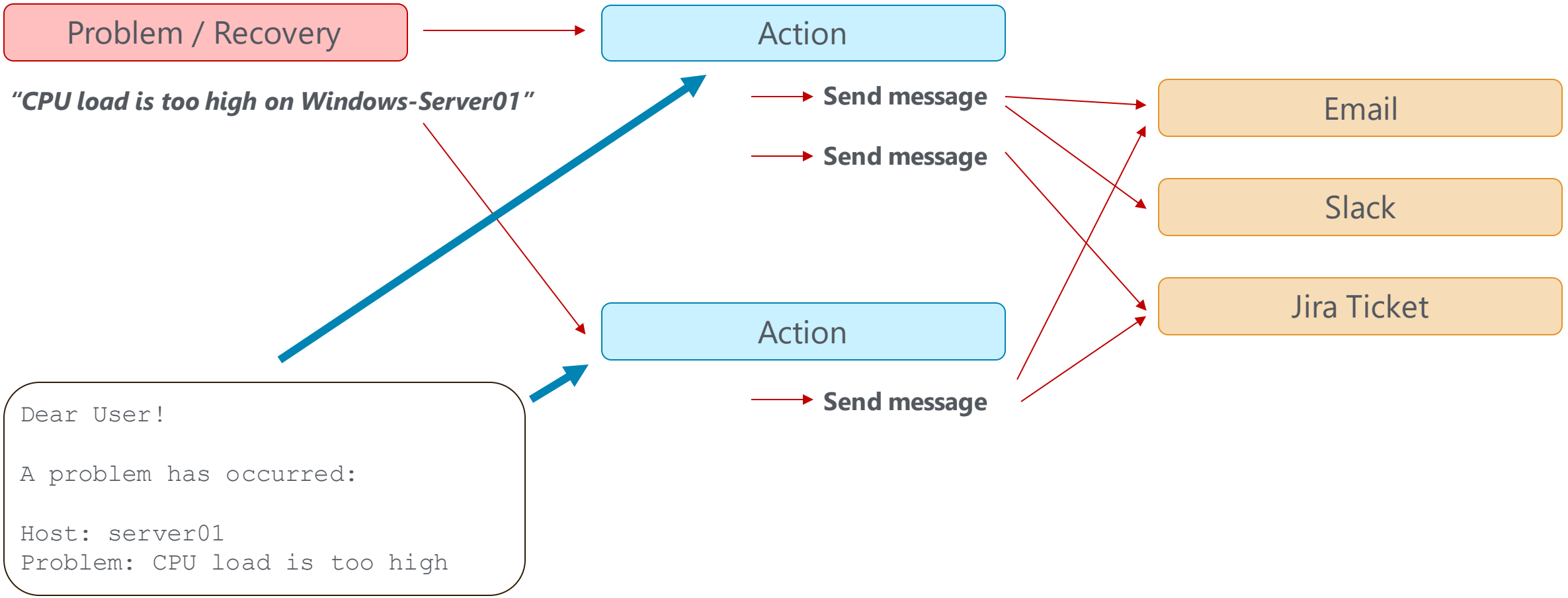
02

DEFAULT MESSAGES FOR EACH MEDIA TYPE

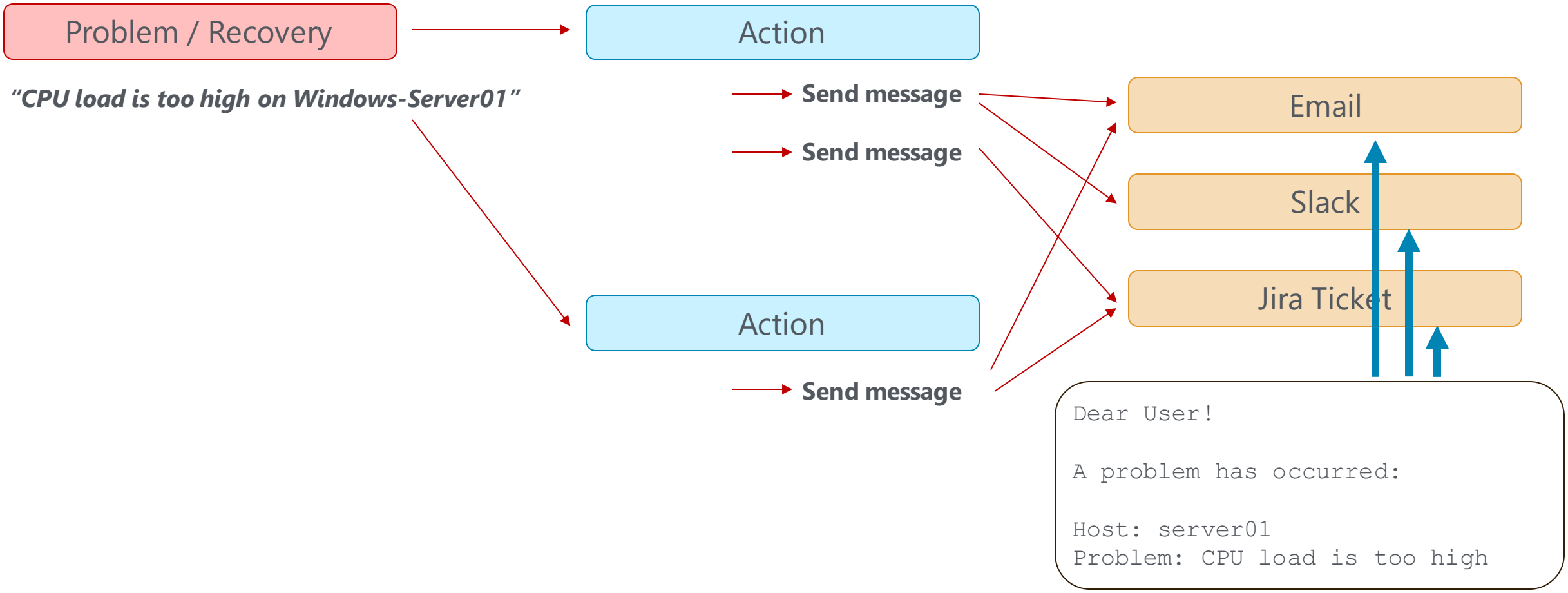


- Easier to manage messaging guidelines
- Perform mass changes in Action messages with couple of clicks
- Simplify configuration of Actions

ACTION WORKFLOW
HOW DO YOU GET YOUR NOTIFICATION?

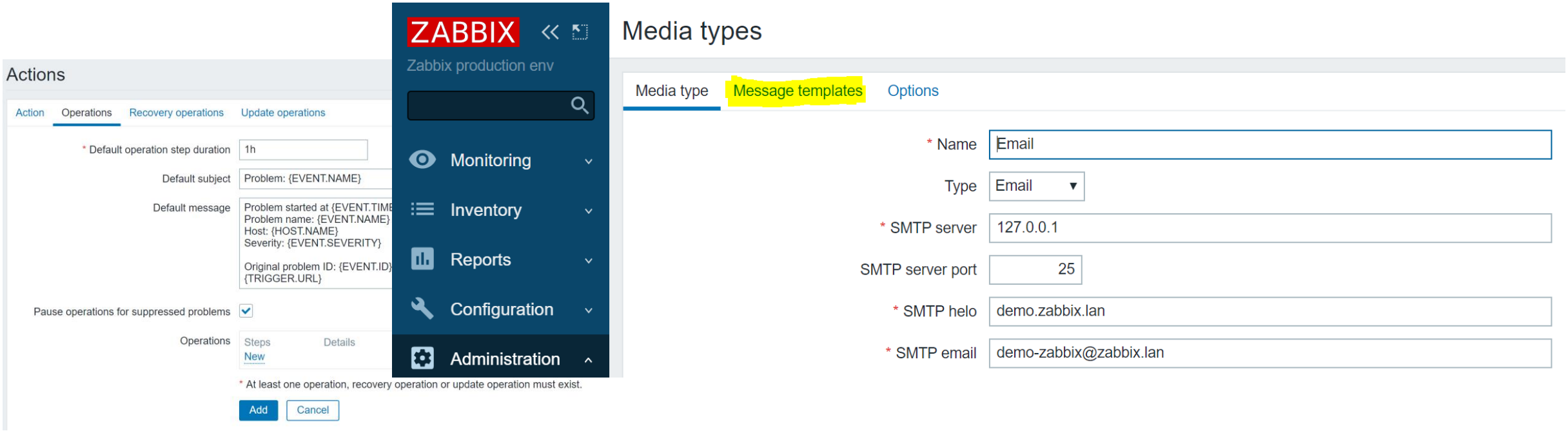


ACTION WORKFLOW
HOW DO YOU GET YOUR NOTIFICATION?



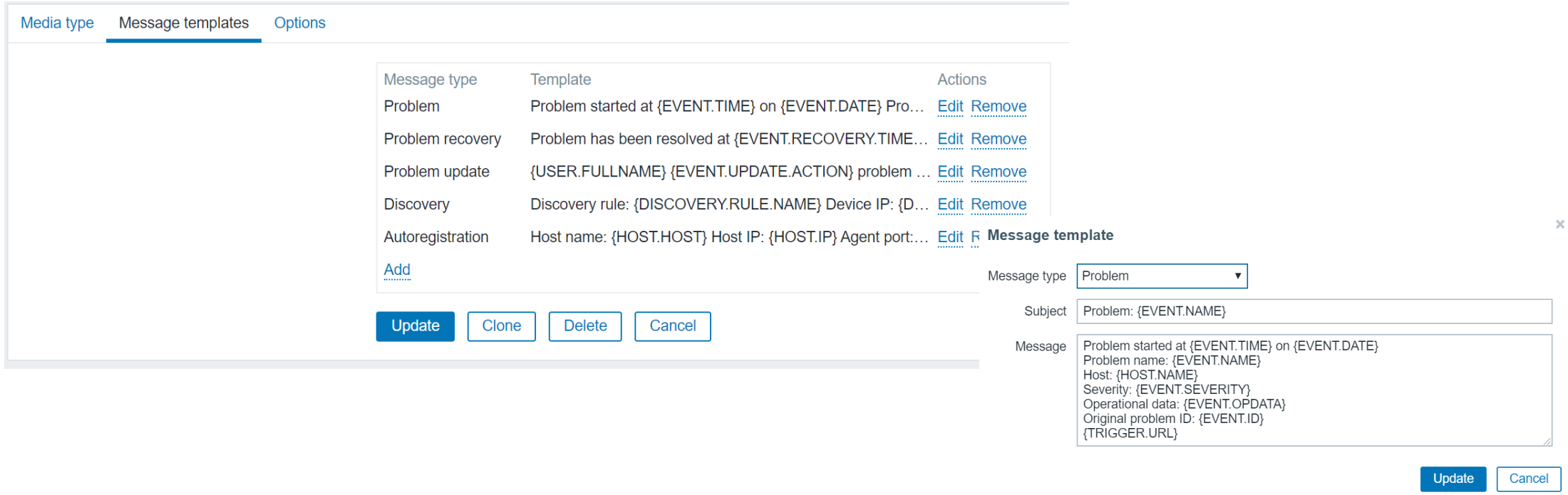
DEFAULT MESSAGES
FOR EACH MEDIA TYPE

- More flexible configuration of complex notification scenarios with less effort
- Manage high amount of actions with a wide variety of media types
- Transferable between Zabbix installations (NEW: **import/export** media types!!!)



DEFAULT MESSAGES
FOR EACH MEDIA TYPE

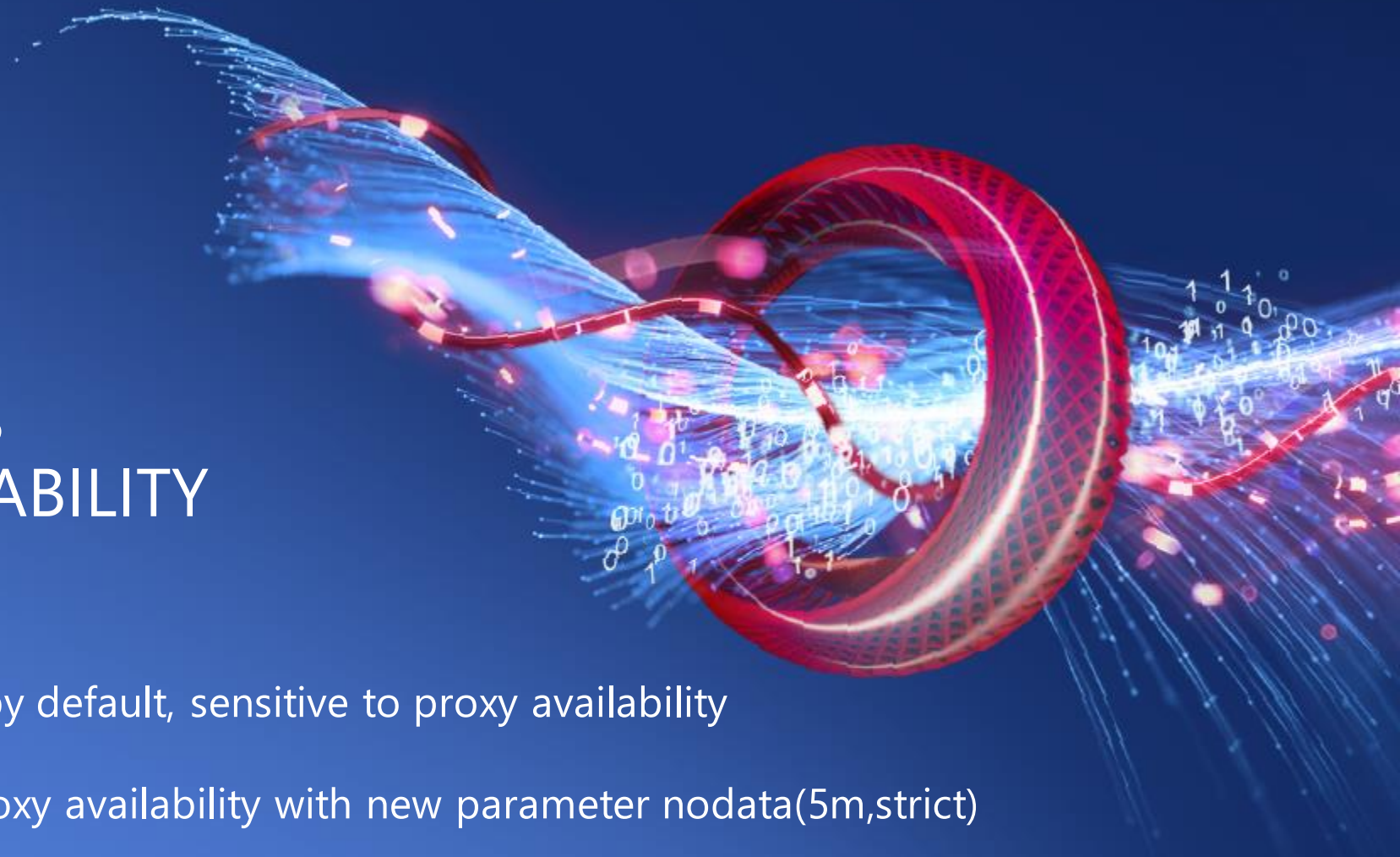
- Define standard messaging for Media type
- Define standard messaging for every state of a problem
- If needed – **override on Action level**



SECADM
SECURE FOR SURE

03

NODATA TRIGGERS AND PROXY AVAILABILITY



- nodata() triggers are now, by default, sensitive to proxy availability
- Turn off sensitiveness to proxy availability with new parameter nodata(5m,strict)
- Avoid massive event storms and other issues because of single proxy

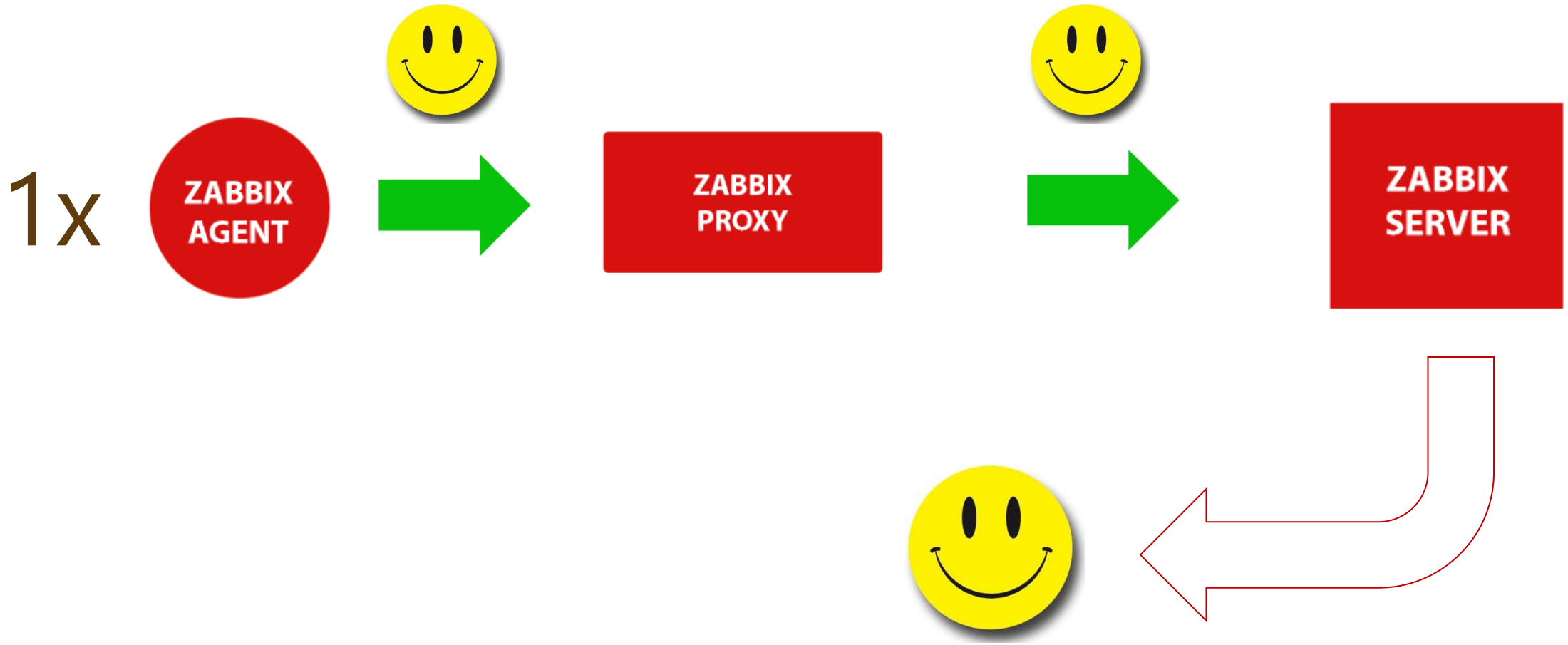
NODATA TRIGGERS
AND PROXY AVAILABILITY BACKGROUND

ZBXNEXT-1891 – Implicit trigger dependency when monitored via proxy (2003)

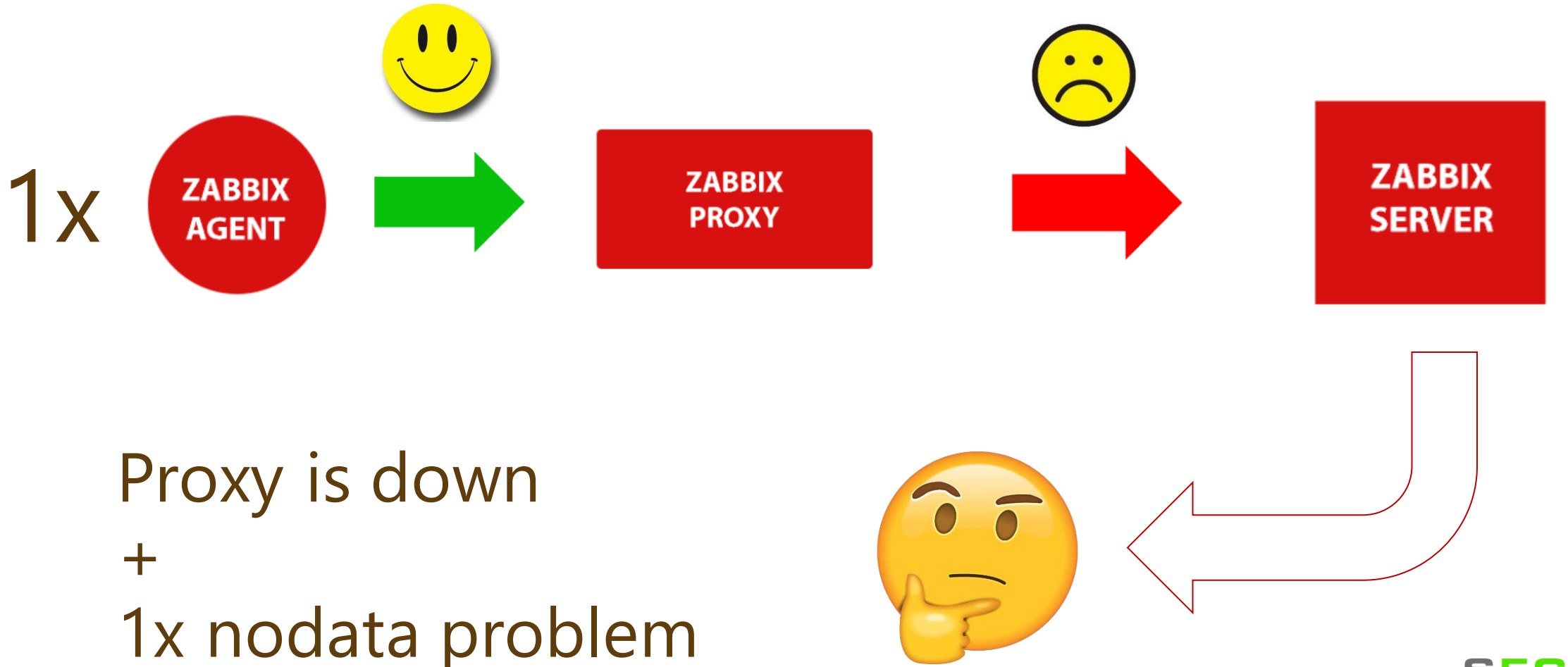
- nodata() trigger function – Checking for no data received
- If host is monitored by proxy, but proxy can't report data to server = no data
- Event and alert storms, other performance issues
- nodata() triggers are used in official Zabbix agent templates
- cheap in calculation

High	OK	Template App Zabbix Agent - active agent: Zabbix agent on is unreachable for 5 minutes	{phineas:agent.ping.**nodata**(5m)}=1

NODATA TRIGGERS
LET'S VISUALIZE

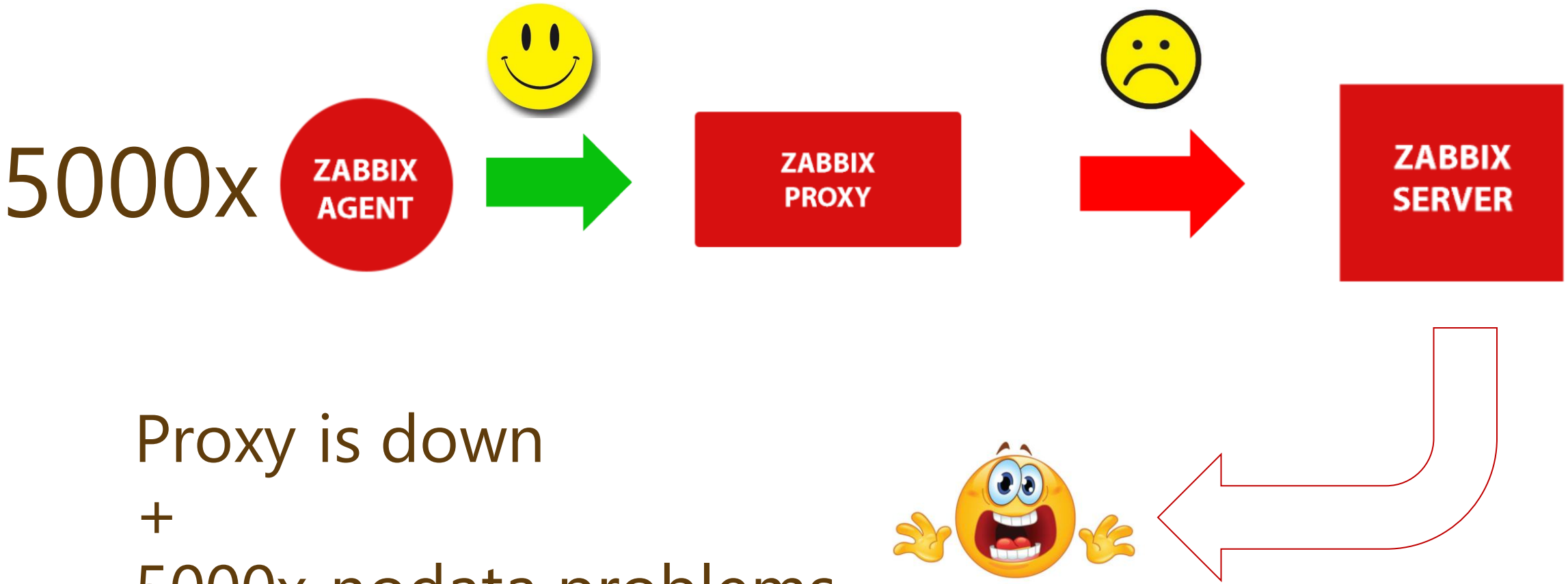


NODATA TRIGGERS
LET'S VISUALIZE



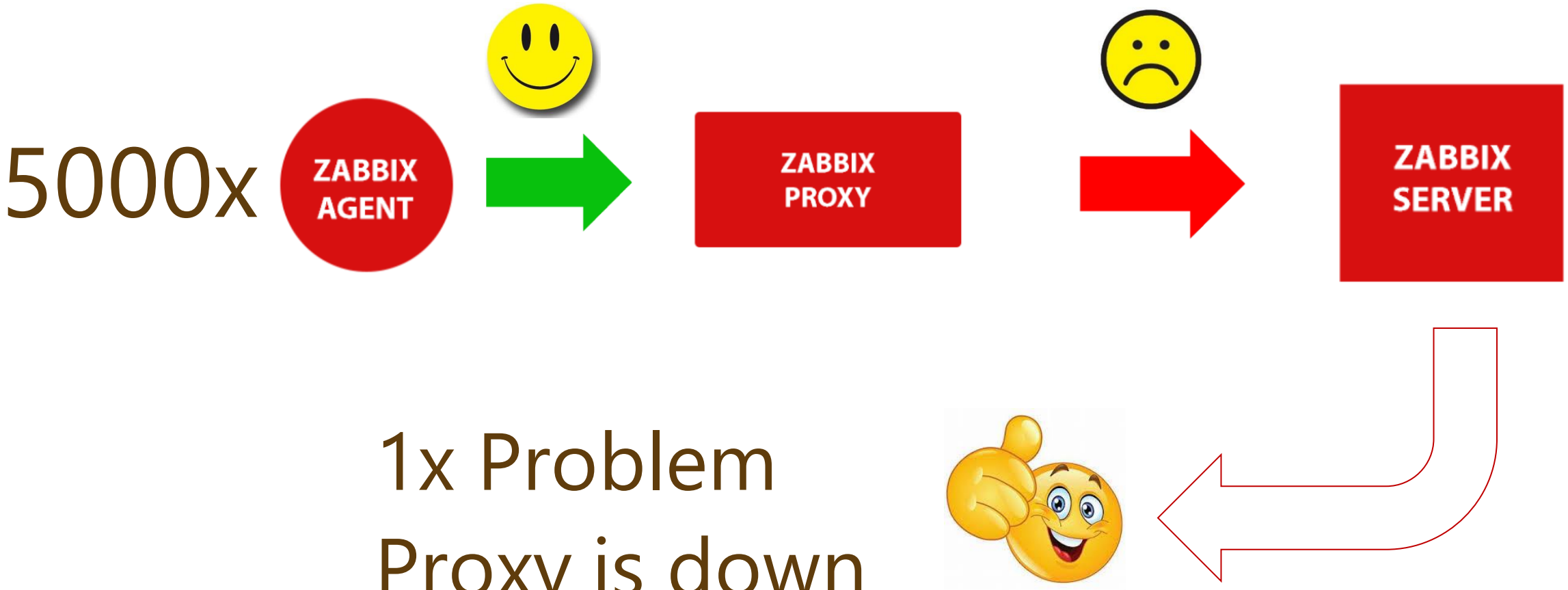
Proxy is down
+
1x nodata problem

NODATA TRIGGERS
LET'S VISUALIZE



Proxy is down
+
5000x nodata problems

NODATA TRIGGERS
LET'S VISUALIZE – 5.0



NODATA TRIGGERS
FINAL NOTES

- Much easier than setting up global event correlation and Trigger dependencies
- Out of the box functionality, just works as expected without any further setup
- What if I **don't** want to respect proxy availability? `nodata(5,strict)` !

04

LLD OVERRIDES

- Exception handling for specific Item and Trigger prototypes in LLD rules

LLD OVERRIDES
AND HOW THEY DIFFER FROM LLD FILTERS

LLD filters define whether an **entity** is being discovered or not

- Example: do not discover file systems with type «swap» or «proc»

LLD overrides define exceptions for **specific prototypes** based on content of LLD macros

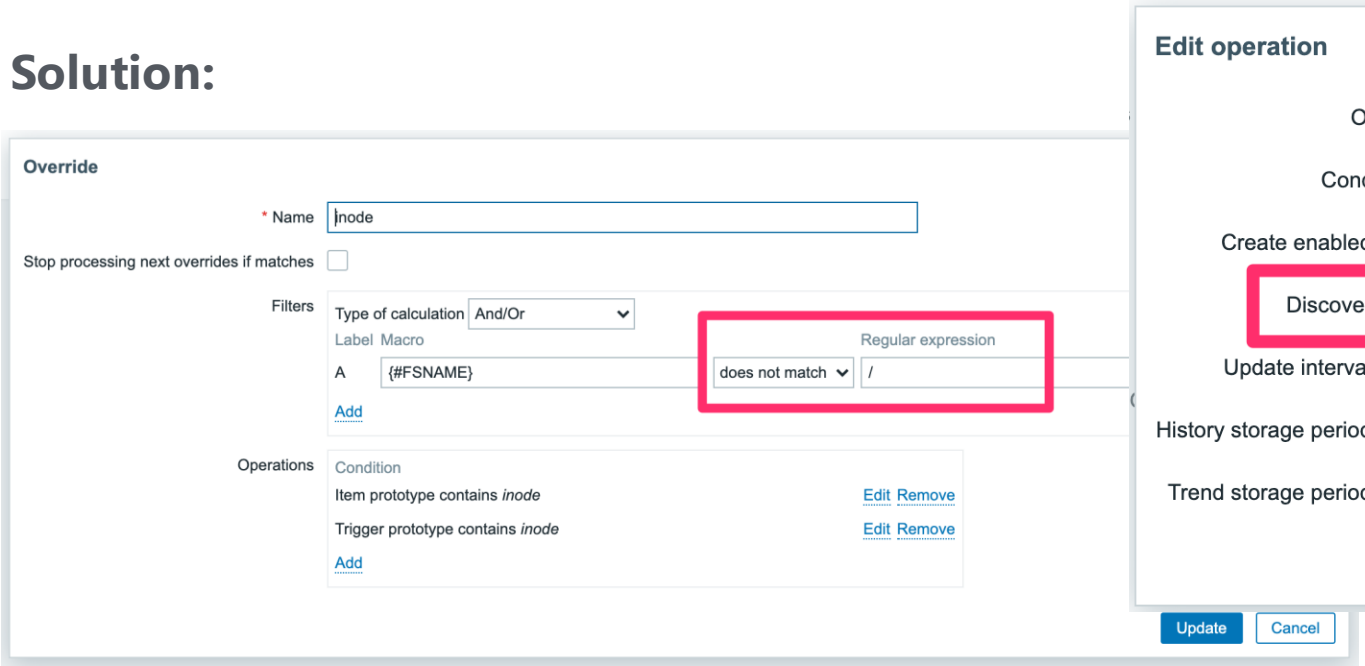
- Example: set a different severity for a trigger on a root file system
- Example: do not add Trigger/Item for the entity in certain circumstances
- Example: set specific update interval / storage period for item

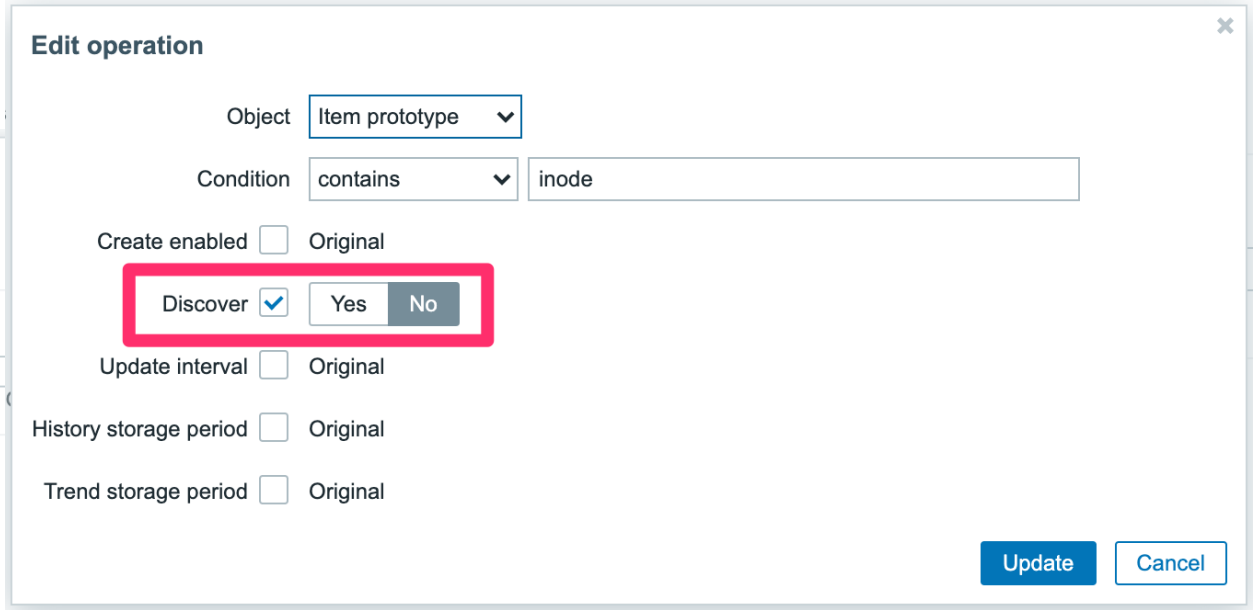
LLD OVERRIDES USE CASE:
ONE FILE SYSTEM LLD FOR BOTH WINDOWS AND LINUX

Problem:

- Windows does NOT support Inode monitoring: `vfs.fs.inode(fsname, <mode>)`

Solution:





05

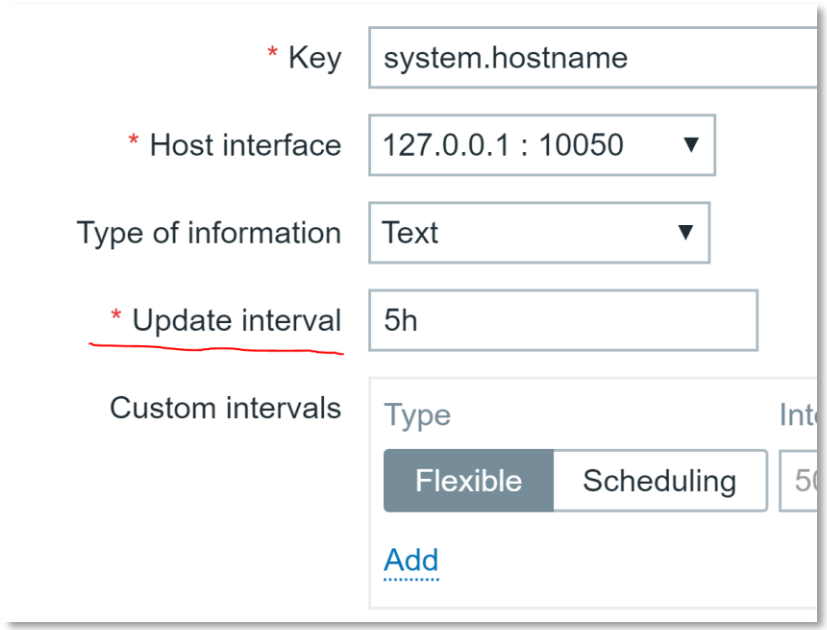
TEST ITEM FROM USER INTERFACE

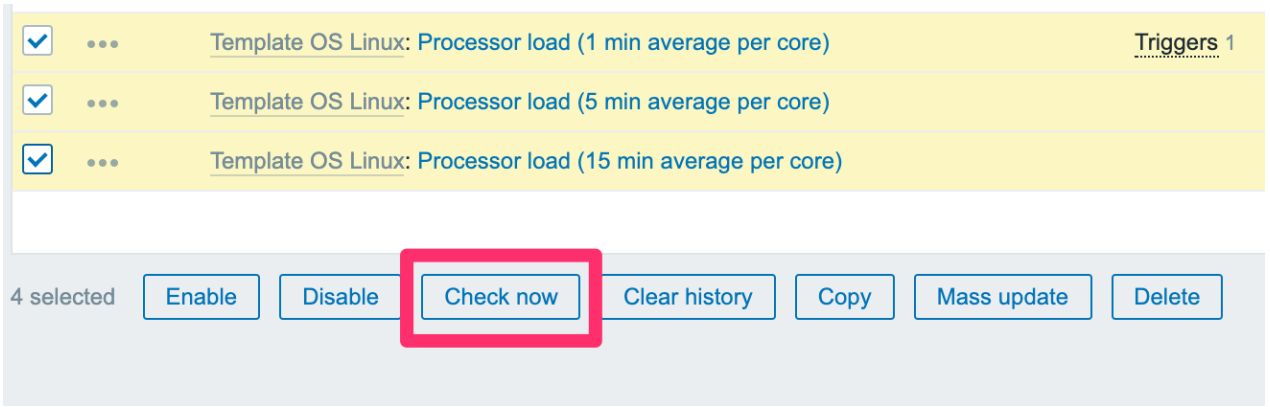
- In previous versions it was difficult to tell if a newly-configured item was configured correctly or not.
- Now it is possible to test item from UI even before saving it, and get a real value in return.
- And even test all pre-processing steps

TEST ITEM
WHAT WE DID BEFORE?

```
[root@meetup tmp]# zabbix_get -s 127.0.0.1 -k system.hostname
meetup
[root@meetup tmp]#
[root@meetup tmp]#
[root@meetup tmp]# zabbix_agentd -t system.hostname
system.hostname                                [s|meetup]
[root@meetup tmp]#
```

- Simply wait for next update interval cycle
- zabbix_agentd -t < item_key >
- zabbix_get -s <host> -k <key>
- In Zabbix 4.0, «Check now» aka «Execute Now» has been added for passive items





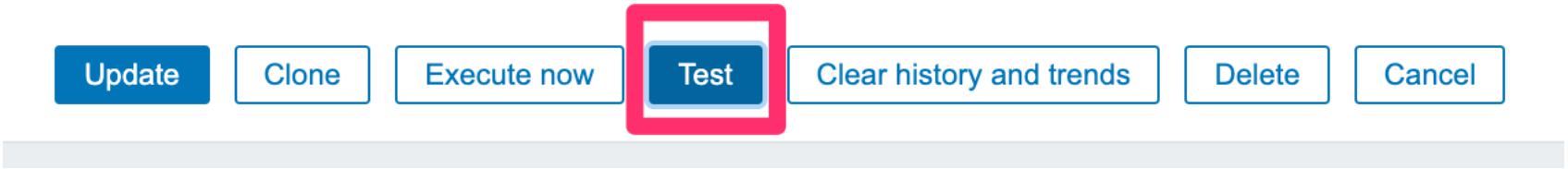
SECADM
SECURE FOR SURE

TEST ITEM
PROBLEMS

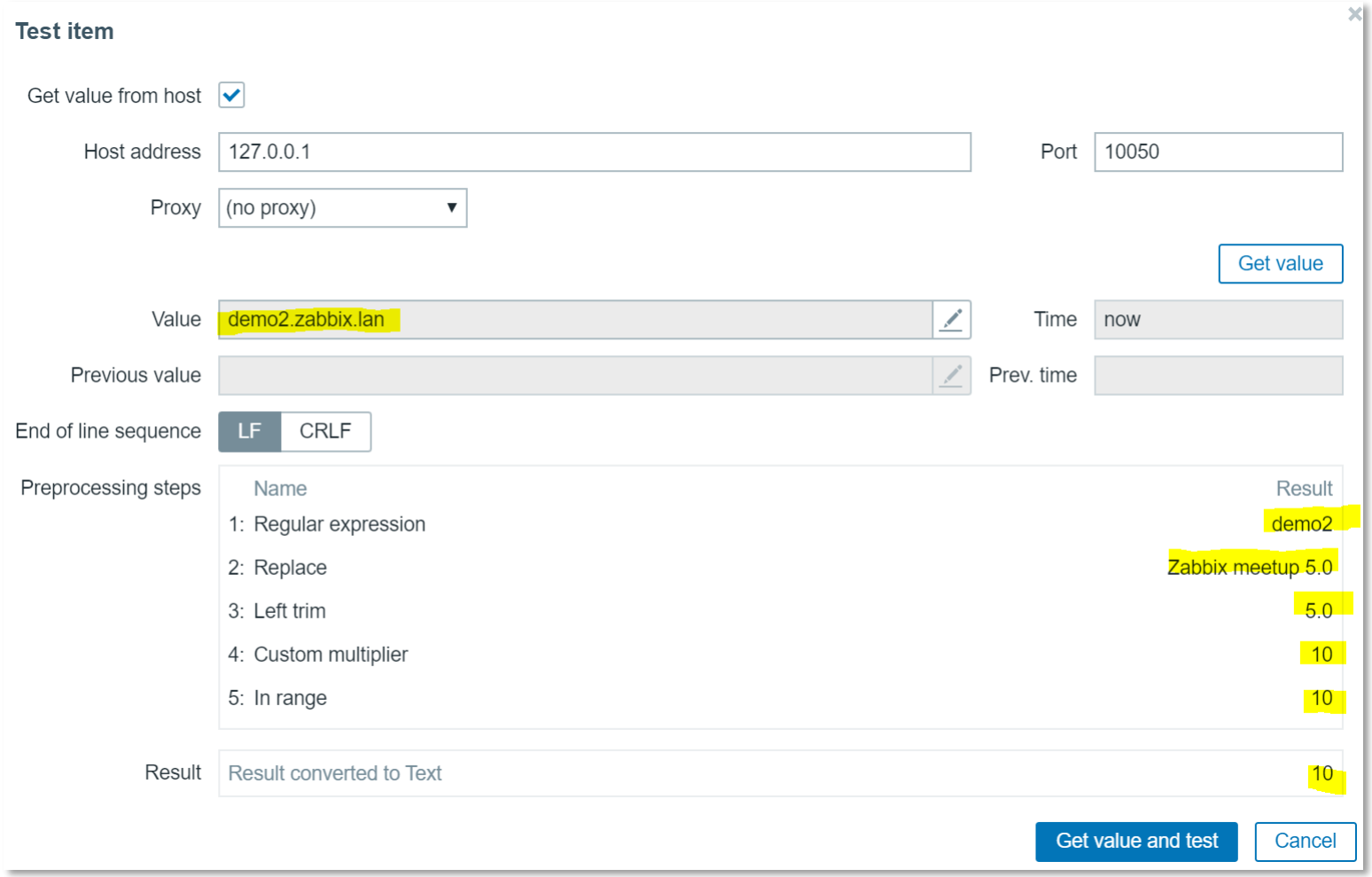
- Waiting is not an option!
- «Check Now» is only available on host level (not templates)
- «Check Now» is executed by the server (Configuration cache, …)
- Zabbix_agentd and zabbix-get don’t respect pre-processing
- Dependent Items…?

TEST ITEM
5.0

- Works on **host** and **template** level (by entering a valid IP and port to connect to for testing)
- Can be used **before** an item is actually saved in configuration
- Gives **instant** feedback
- Runs through and visualizes the whole **preprocessing** chain and outputs of all steps
- Can test items located on hosts behind **Proxy**
- Also works for **calculated** and **aggregated** items
- Allows substitution of **macro values** (NEW: secret macros)



TEST ITEM
5.0



06

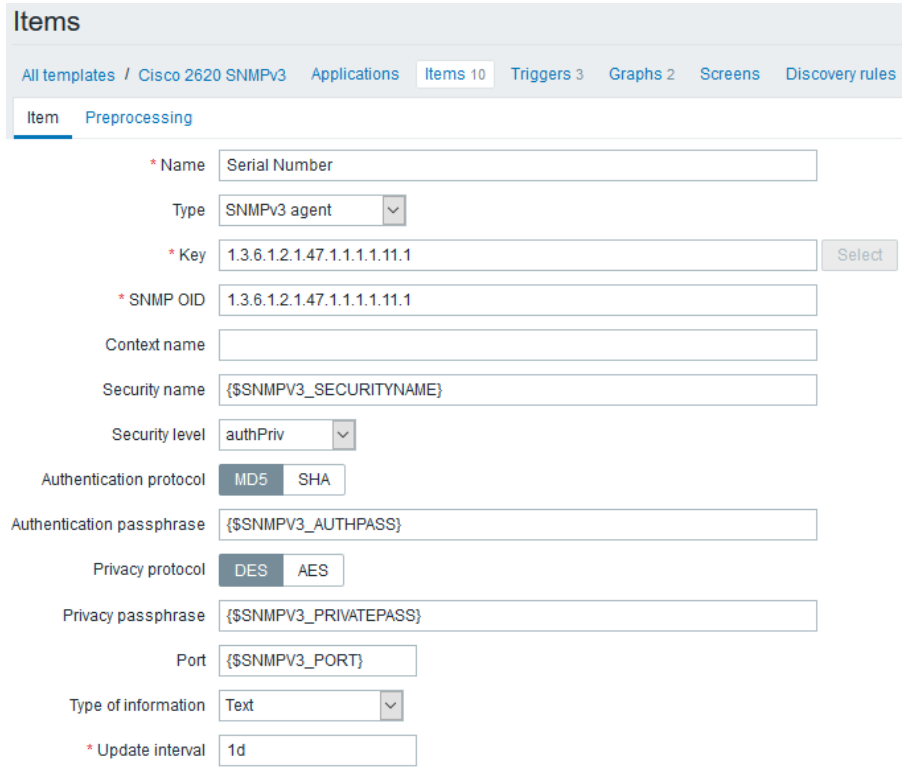
SNMP CREDENTIALS AT HOST INTERFACE LEVEL

- SNMP connection related settings where they should be
- Simplify configuration: make templates unique and transportable
- SNMPv1, SNMPv2, SNMPv3 => SNMP Agent

SNMP CREDENTIALS
AT HOST INTERFACE LEVEL

- Complexity of authentication parameters
- Simple human mistakes – typos
- In case of many items, chance to make mistake increases
- One mistake in Item prototype can affect whole host

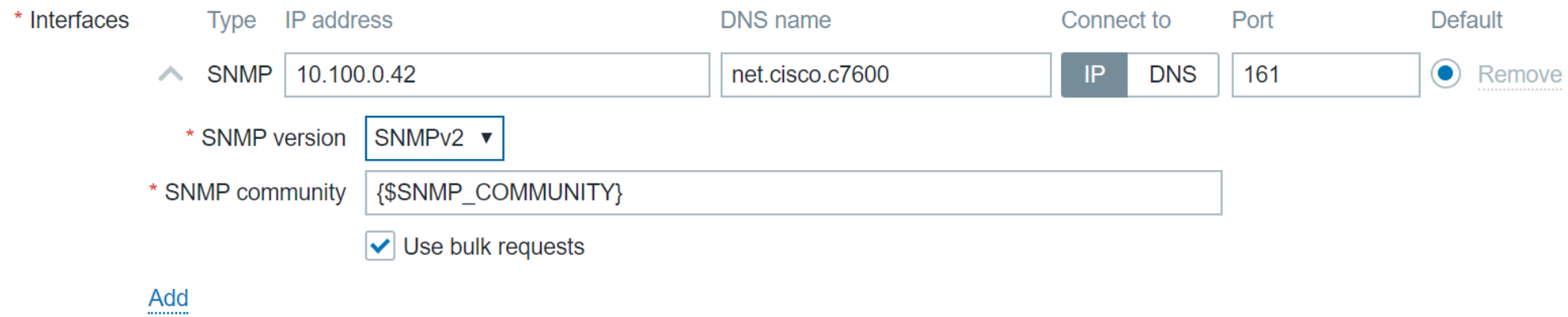
* Name	Hardware serial number
Type	SNMPv3 agent
* Key	system.hw.serialnumber (Select)
* SNMP OID	1.3.6.1.2.1.47.1.1.1.1.11.1
Context name	zAbbIxMonitorIng
Security name	letsM0n1t0rzabb1x
Security level	authNoPriv
Authentication protocol	MD5 / SHA
Authentication passphrase	z318$2@sjwe#*21AAa



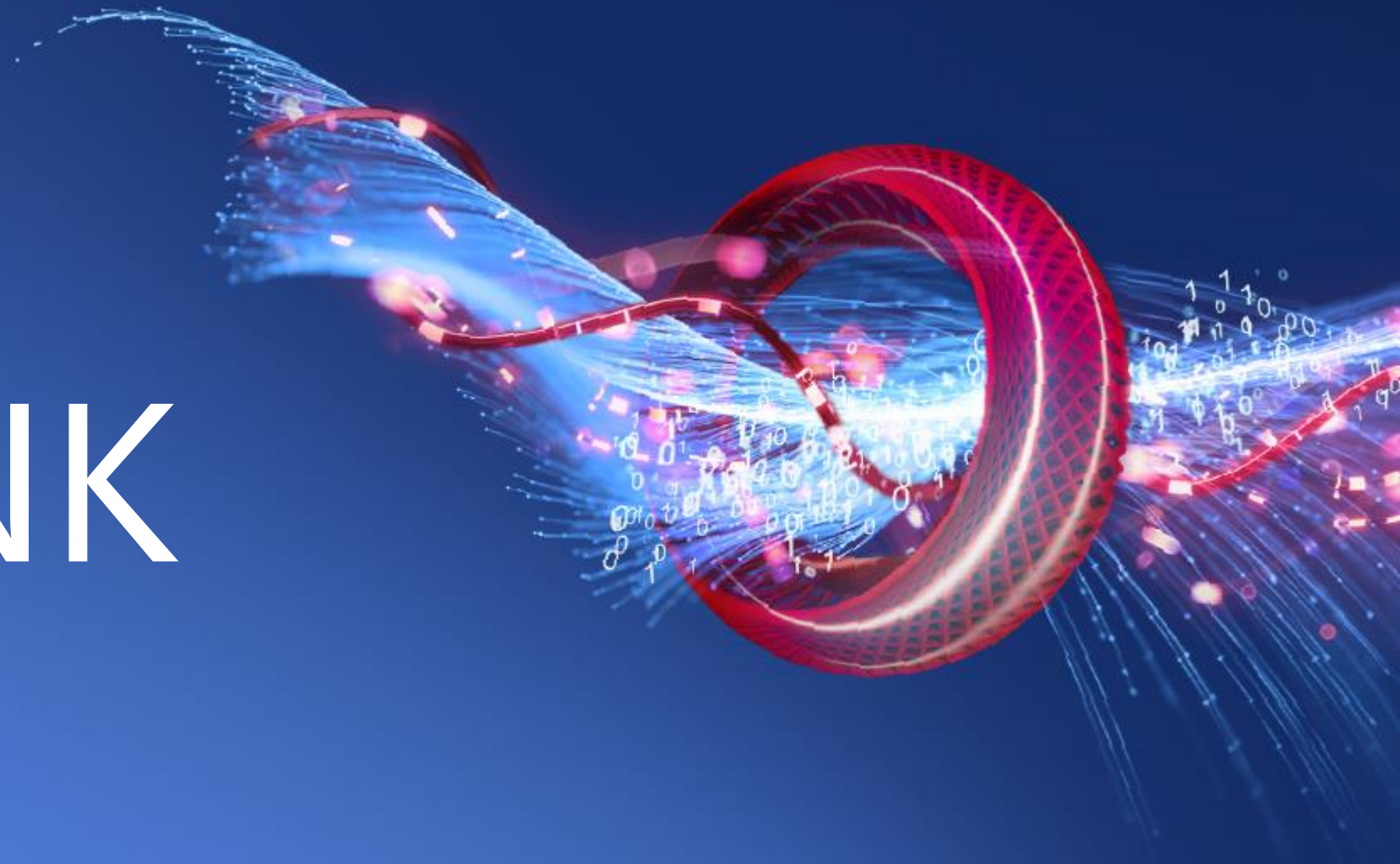
SECADM
SECURE FOR SURE

SNMP CREDENTIALS
AT HOST INTERFACE LEVEL

- Instead of suggesting to «be careful!» minimize possibilities to make mistake
- snmpv1, snmpv2, snmpv3 replaced with SNMP Agent
- All configuration is done on interface level
- All items inherit settings from chosen interface



THANK YOU!



SECADM
SECURE FOR SURE