



Webinar

Why monitoring is important?

all our microphones are muted

ask your questions in Q&A, not in the Chat

use Chat for discussion, networking or applause



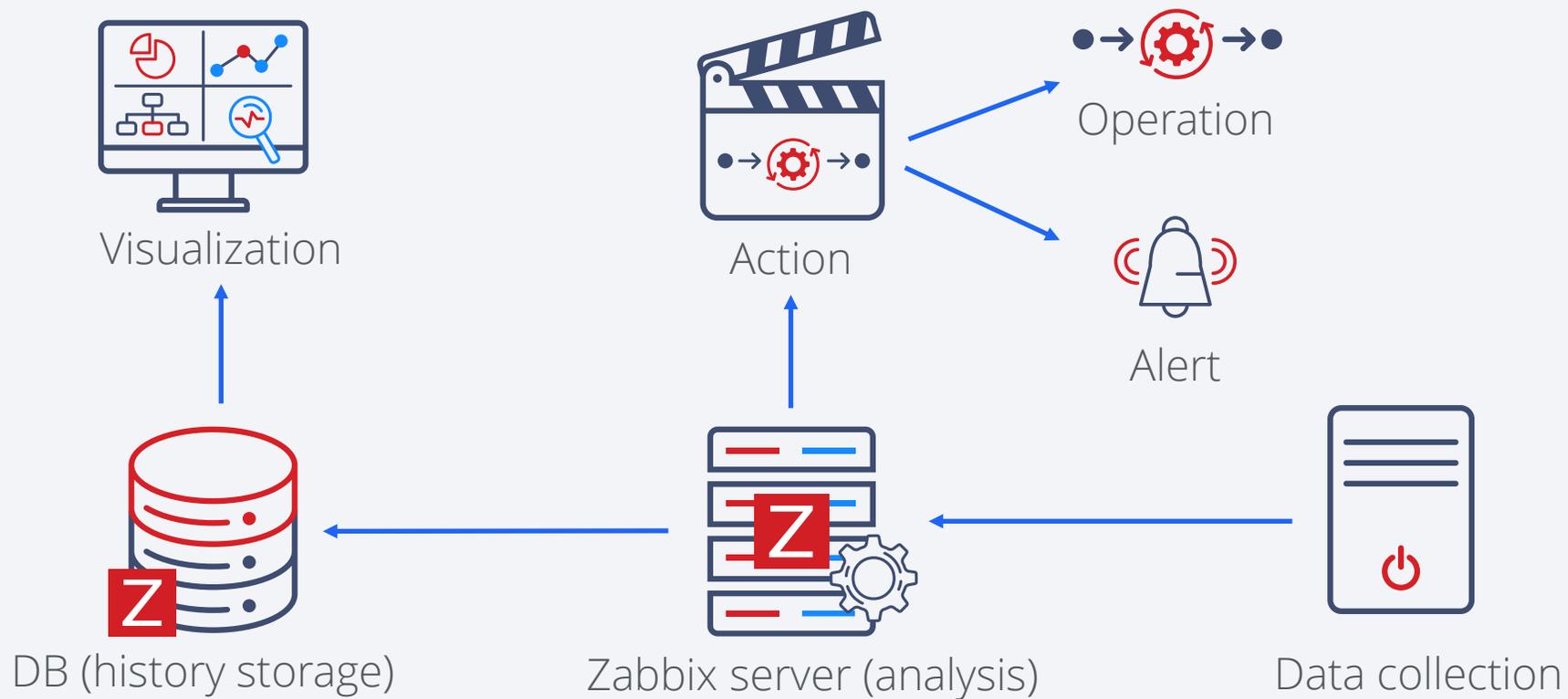
1

What is monitoring

Why You Need Monitoring

What is monitoring?

Monitoring – is a process of data collection, aggregation and analysis for better system characteristic and behavior understanding

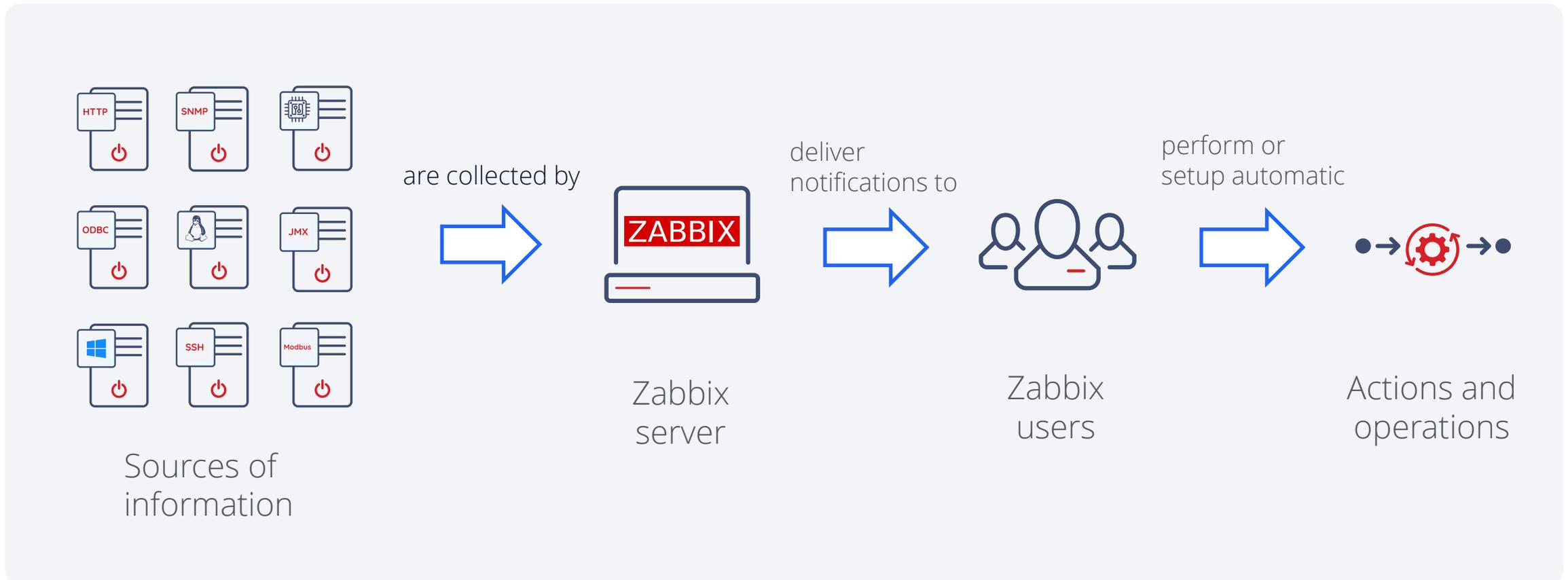


Why You Need Monitoring

Goal of monitoring

... take a right decision based on most current and complete situation overview!

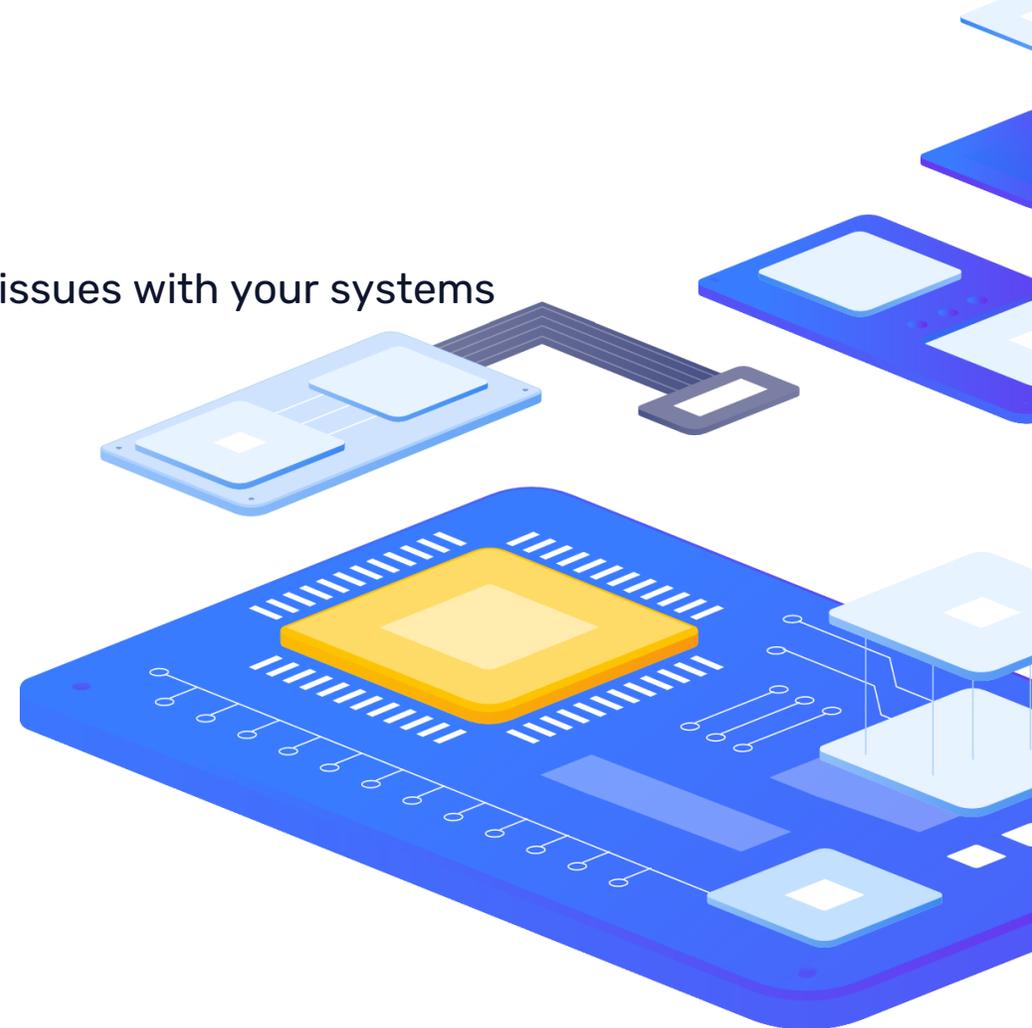
Users perform actions based on situation themselves or setup Zabbix automatic actions or operations to act on their behalf



Why You Need Monitoring

Why monitoring is Important?

- › You have a full hardware and software control over your equipment
- › Incident prevention helps to reduce security risks
- › Early problem detection and notification helps to eliminate possible issues with your systems
- › Optimize your environment and reduce costs



Why You Need Monitoring

Hardware and software control : Use cases

- ▶ The RAM usage for the latest application version is too high. What is a reason?
- ▶ The network is stalling each time I use it for big file transfer
- ▶ My database is slow, so my applications start to suffer
- ▶ What is average free space left on hard disks for several workstations? Can I be notified when it reaches 10GB left?

Why You Need Monitoring

Eliminate security risks : use cases

- › I want to get an alert each time a network connection with a remote server disappears
- › I want to be notified each time a server chassis box is opened
- › I want to get a list of failed login attempts at the end of a day
- › I want to get information about modified files on a server
- › I want to get notification about SSL certificates properties used in our environment

Why You Need Monitoring

Early problem detection : use cases

- ▶ The number of application users is growing. How are we doing with that fact?
- ▶ Where is a bottleneck in our network?
- ▶ Why our storage is busy each Friday at the end of the day?
- ▶ Were there any intrusions to our networking equipment this year?

Why You Need Monitoring

Costs reduction and optimization : use cases

- ▶ Do we really need that much memory on server, or we could cut a half?
- ▶ We bought 100 licenses for our VPN, what is a maximum number that has been used?
- ▶ What workstations are being actively used throughout the year?
- ▶ Can we make one operator work with many monitoring sites remotely?

Why You Need Monitoring

How does it work?

First step – data collection

- › Data is collected by special software agents or collected directly (agentless collection)

Second step – data storage

- › Data is being stored in the supported database

Third step – data analysis

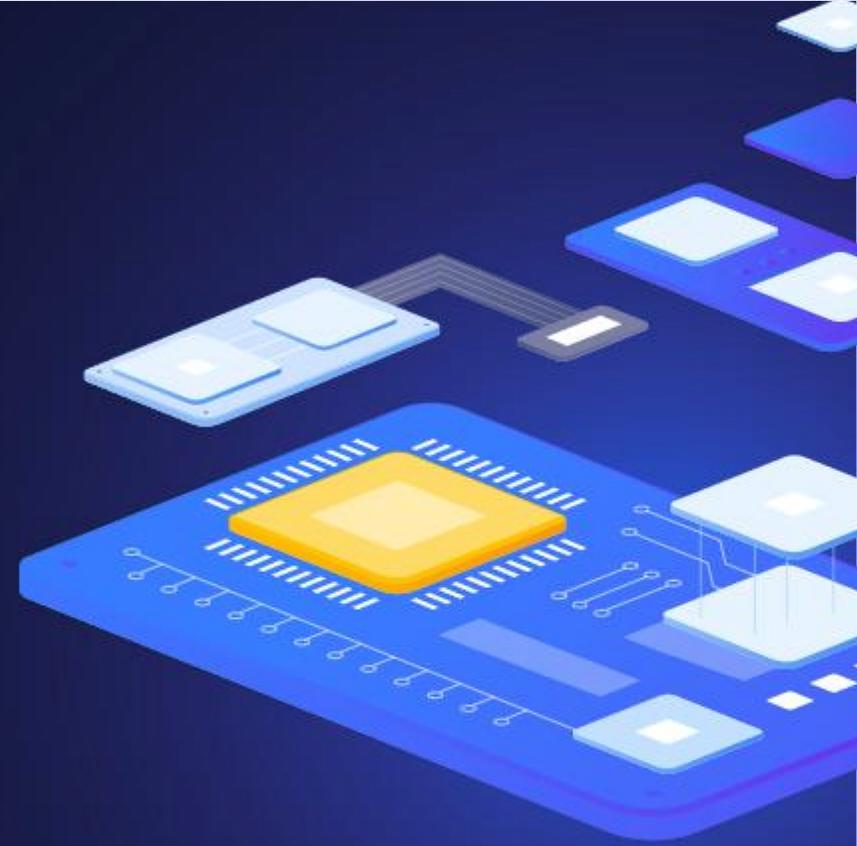
- › Define thresholds and constraints for metrics

Forth step – notifications and actions

- › Perform user notification or conduct actions according to predefined set of operations

2

Data collection

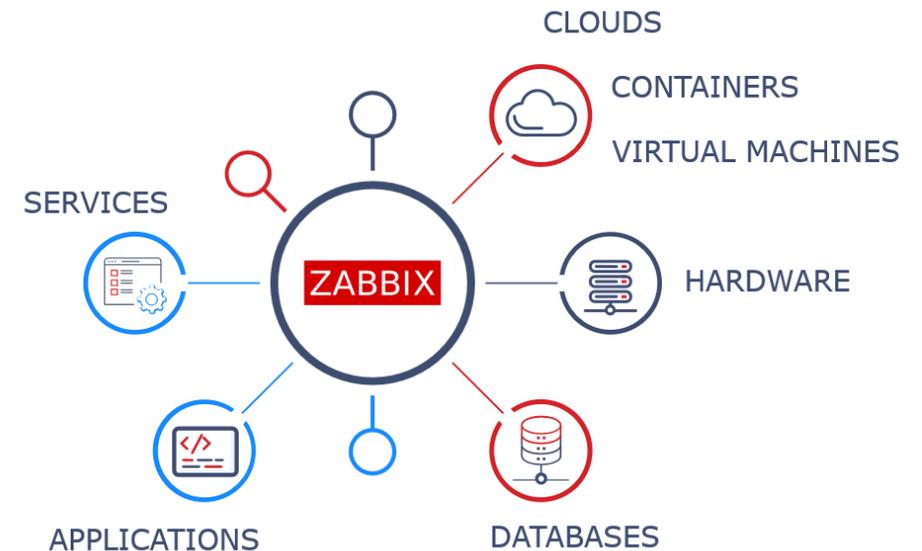


Why You Need Monitoring

Data collection

- ▶ Data can be collected with special software (Zabbix agent) to reach data, that cannot be sent by device itself (like OS metrics, database and other)
- ▶ Some data can be collected with agentless method (SNMP, TCP/UDP checks, JMX, so on)
- ▶ Zabbix can receive certain data issued by side devices or applications (SNMP traps, HTTP traps and so on)

All these methods enrich you with various collection methods for various cases.

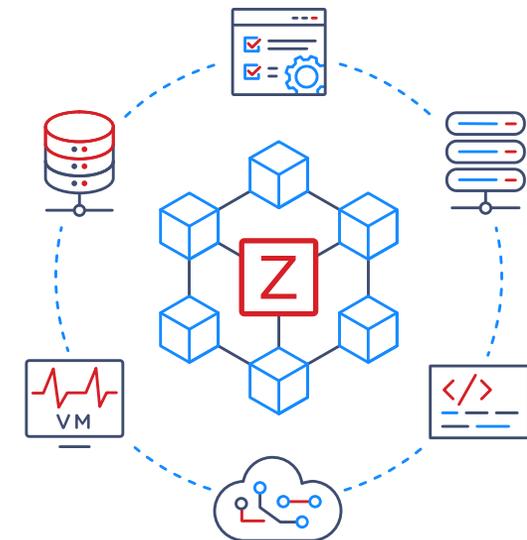


Why You Need Monitoring

Data collection : sources

Sources of data open multiple ways of data collection:

- ▶ SNMP, HTTP, Simple checks, ICMP (ping), etc.
- ▶ JMX
- ▶ Active agent (when agent 'pushes' data to Zabbix server)
- ▶ Passive agent (when Zabbix server collects data from Zabbix agents)
- ▶ Trap receivers: SNMP trap, HTTP trap, Zabbix trapper
- ▶ User parameters and scripting support



Why You Need Monitoring

Data collection : custom monitoring

- ▶ UserParameter in Zabbix Agent and Zabbix Agent 2 – user-defined data collection.
- ▶ Sometimes you may want to run an agent check that does not come predefined with Zabbix.
- ▶ You can define your own way of data collection (script or command set) and collect data that way.

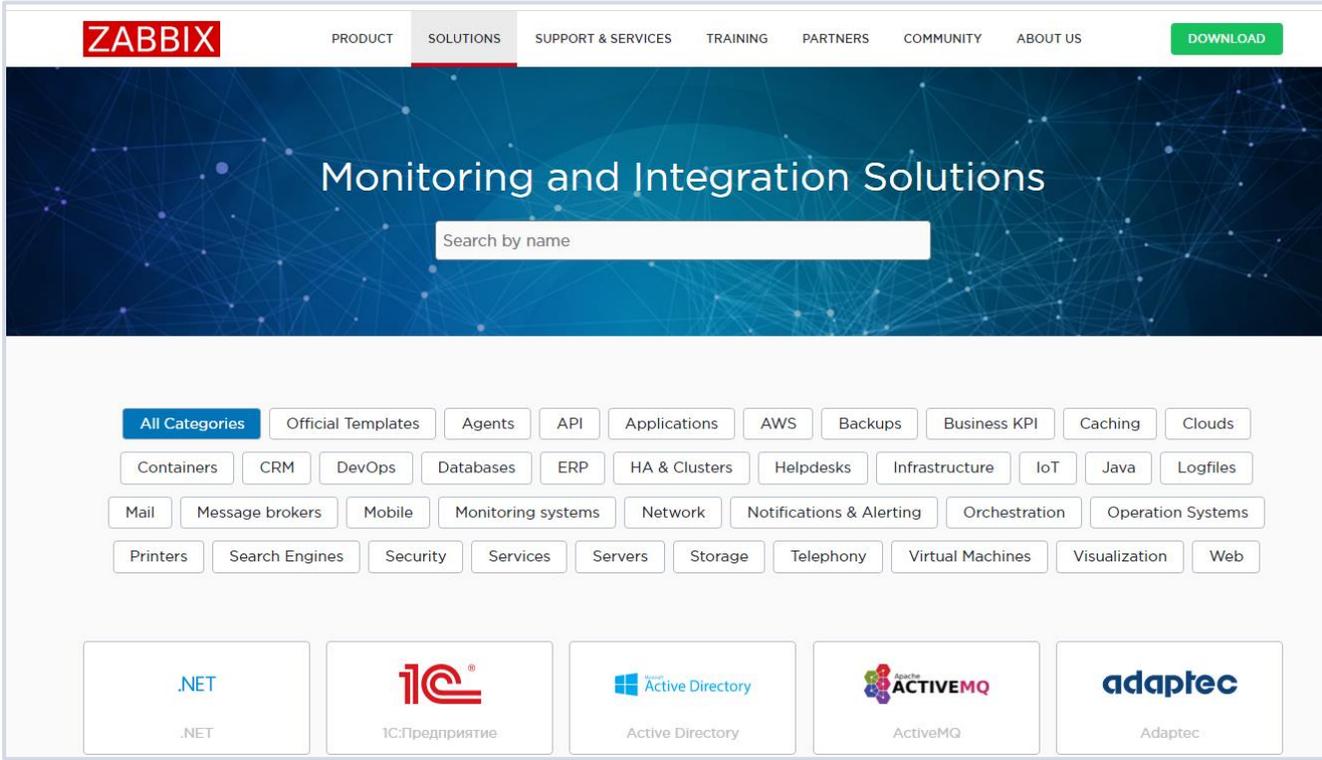


- ▶ Zabbix provides a set of utilities for pushing data to Zabbix server and retrieving data from Zabbix Agents.

Why You Need Monitoring

Data collection : custom monitoring

- ▶ To speed up monitoring system deployment and to group monitored objects by type and data collection approach you may use templates – a presets of items, triggers and corresponding data presentation primitives, provided to you by Zabbix Integration Team and Zabbix Community.



The screenshot displays the Zabbix website's 'SOLUTIONS' page. The header includes the ZABBIX logo and navigation links: PRODUCT, SOLUTIONS (active), SUPPORT & SERVICES, TRAINING, PARTNERS, COMMUNITY, and ABOUT US. A green DOWNLOAD button is also present. The main content area features a dark blue background with a network diagram and the text 'Monitoring and Integration Solutions'. Below this is a search bar labeled 'Search by name'. A grid of category buttons follows, including: All Categories, Official Templates, Agents, API, Applications, AWS, Backups, Business KPI, Caching, Clouds, Containers, CRM, DevOps, Databases, ERP, HA & Clusters, Helpdesks, Infrastructure, IoT, Java, Logfiles, Mail, Message brokers, Mobile, Monitoring systems, Network, Notifications & Alerting, Orchestration, Operation Systems, Printers, Search Engines, Security, Services, Servers, Storage, Telephony, Virtual Machines, Visualization, and Web. At the bottom, there are five integration partner logos: .NET, 1С:Предприятие, Active Directory, ActiveMQ, and Adaptec.

Why You Need Monitoring

Data collection : visualization

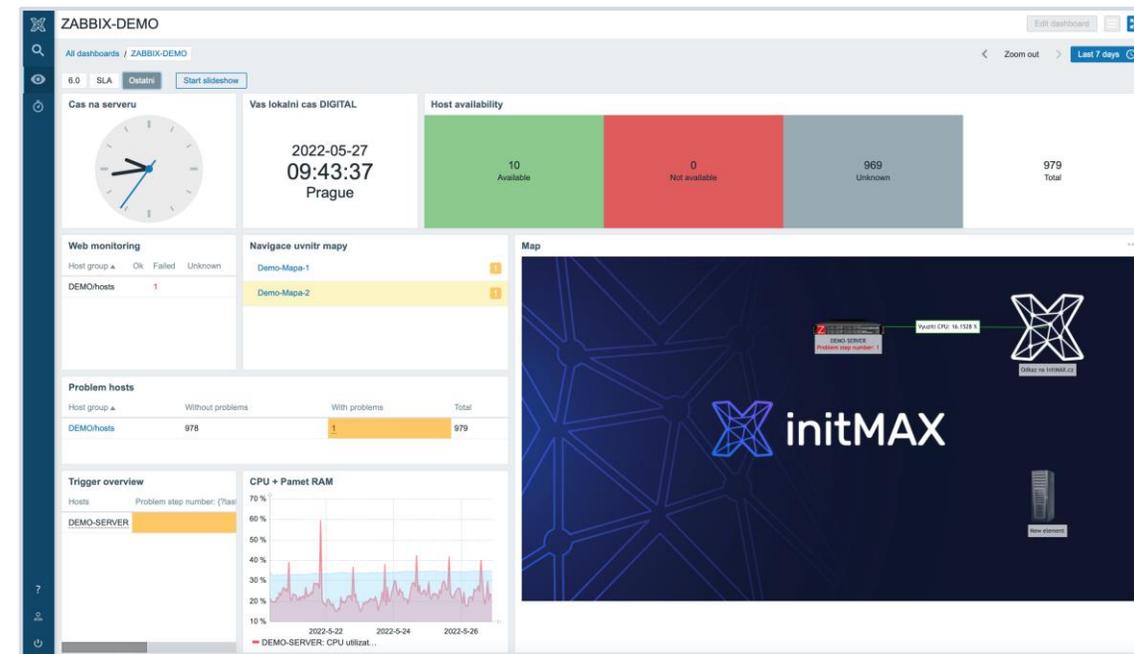
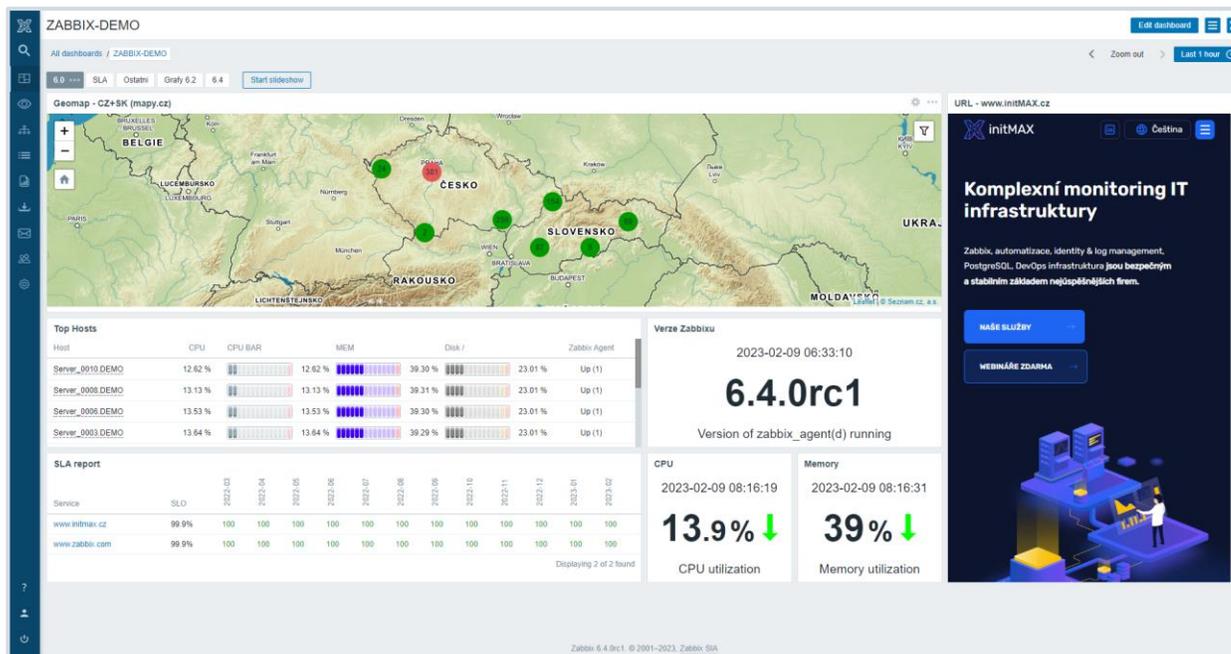
Zabbix can display the collected data in many possible ways.

User can define widget-based dashboards displaying relevant information:

- › Large selection of many different widgets
- › Simple drag and drop placement and scaling of widgets
- › Each widget is highly customizable to fit your needs
- › Display metrics, problems, infrastructure and geo maps on your dashboards
- › Display your current business service SLA information on your dashboards
- › You can access your metrics, problems, reports and maps with a click of a button.

Why You Need Monitoring

Data collection : visualization



Why You Need Monitoring

Data collection : visualization : network maps

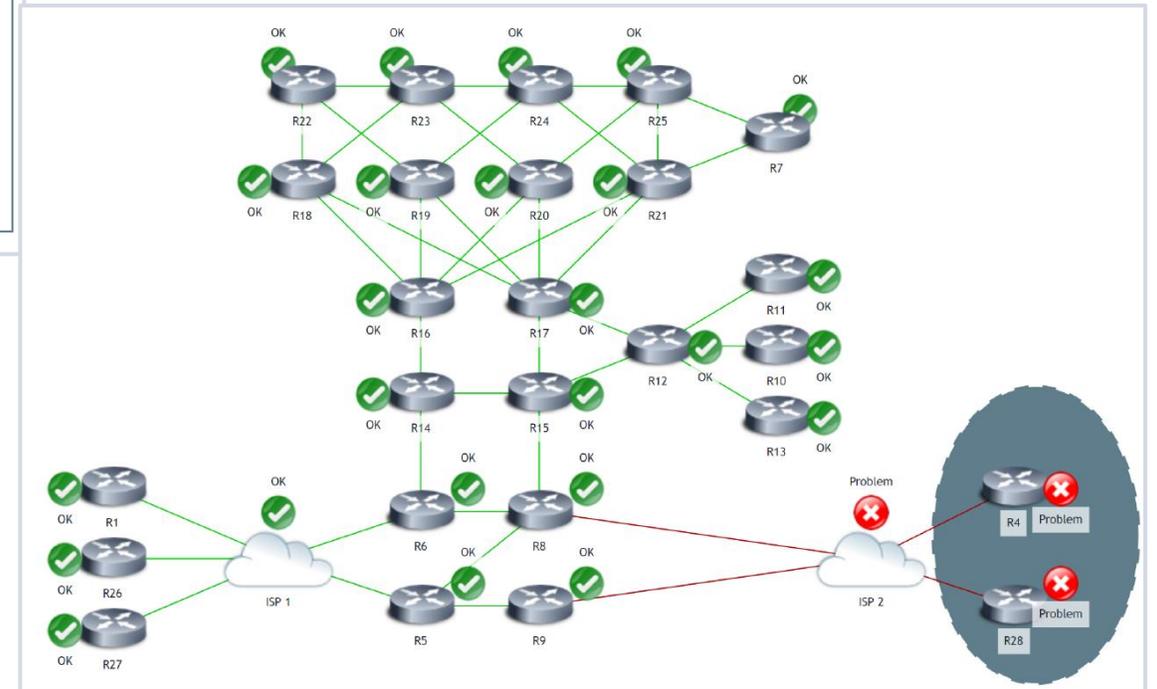
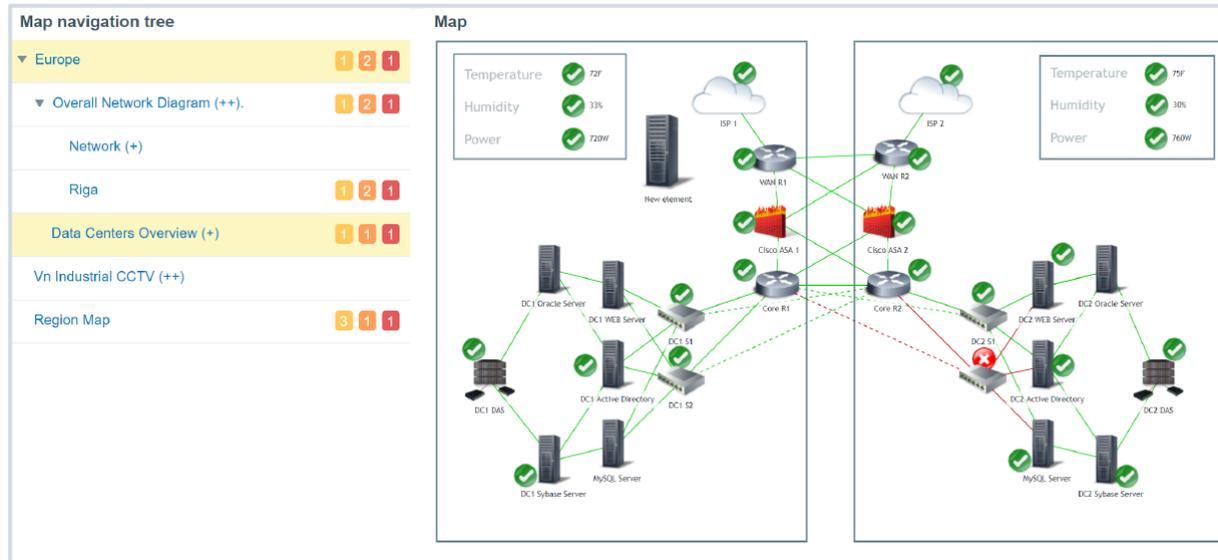
You can present status of your infrastructure on maps.

User may display statuses of his elements together with real time data to get a detailed overview of your infrastructure on a Zabbix map:

- › Ability to display any data in real time on your maps
- › Easy drag-and-drop map element deployment
- › Clone and modify existing maps
- › Execute scripts within your infrastructure from the map screen
- › Create multi-level maps with submaps
- › Context-based interaction with map elements
- › Create linkages between map elements
- › Create nested maps - change the scope of your current view with a click of a button

Why You Need Monitoring

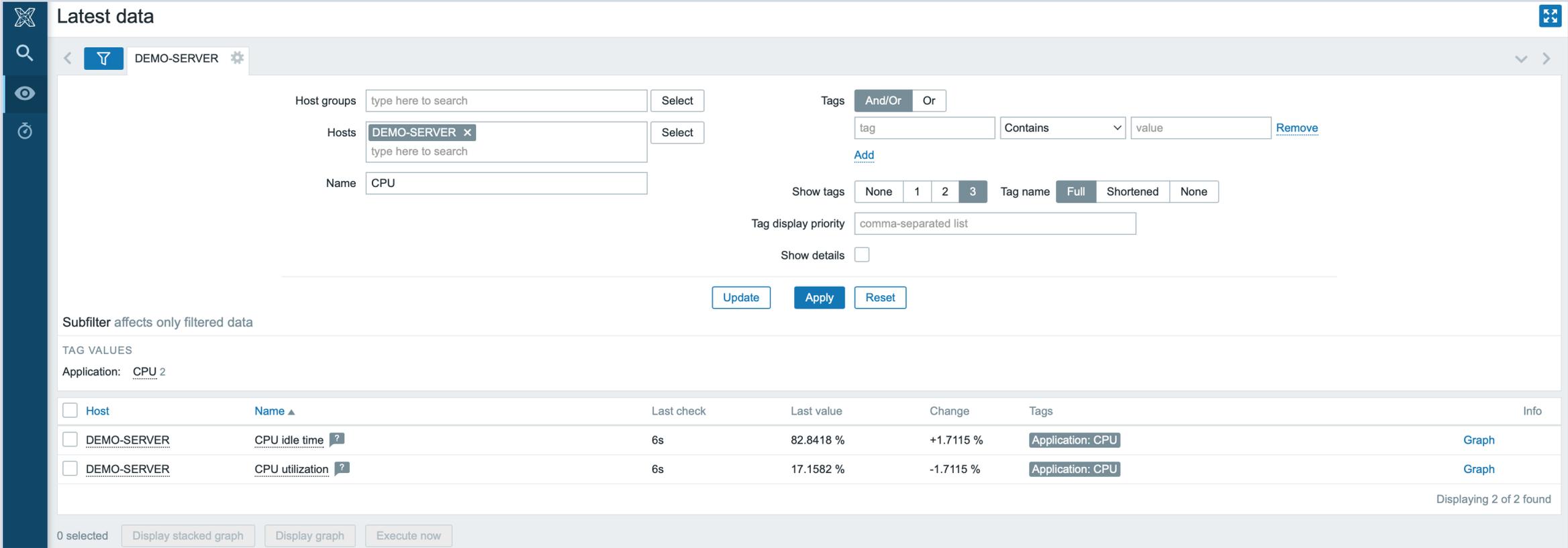
Network maps example



Why You Need Monitoring

Data collection : data display

You may view and filter data inside Zabbix as soon as it is received by server:



The screenshot shows the Zabbix 'Latest data' interface for a host named 'DEMO-SERVER'. The interface includes a sidebar with navigation icons, a search bar, and a filter section. The filter section has fields for 'Host groups', 'Hosts' (with 'DEMO-SERVER' selected), and 'Name' (with 'CPU' entered). There are also options for 'Tags' (And/Or, Or), 'Show tags' (None, 1, 2, 3), 'Tag name' (Full, Shortened, None), and 'Tag display priority' (comma-separated list). A 'Show details' checkbox is also present. Below the filter section are 'Update', 'Apply', and 'Reset' buttons. A note states 'Subfilter affects only filtered data'. The main area displays 'TAG VALUES' for 'Application: CPU 2'. A table shows two data points for 'DEMO-SERVER': 'CPU idle time' and 'CPU utilization'. The table has columns for Host, Name, Last check, Last value, Change, Tags, and Info. At the bottom, there are buttons for '0 selected', 'Display stacked graph', 'Display graph', and 'Execute now'. The status 'Displaying 2 of 2 found' is shown at the bottom right.

Latest data

DEMO-SERVER

Host groups: type here to search [Select]

Hosts: DEMO-SERVER x [Select]
type here to search

Name: CPU

Tags: And/Or Or
tag [Contains] value [Remove]
Add

Show tags: None 1 2 3 Tag name: Full Shortened None

Tag display priority: comma-separated list

Show details:

[Update] [Apply] [Reset]

Subfilter affects only filtered data

TAG VALUES

Application: CPU 2

<input type="checkbox"/> Host	Name ▲	Last check	Last value	Change	Tags	Info
<input type="checkbox"/> DEMO-SERVER	CPU idle time ?	6s	82.8418 %	+1.7115 %	Application: CPU	Graph
<input type="checkbox"/> DEMO-SERVER	CPU utilization ?	6s	17.1582 %	-1.7115 %	Application: CPU	Graph

0 selected [Display stacked graph] [Display graph] [Execute now]

Displaying 2 of 2 found

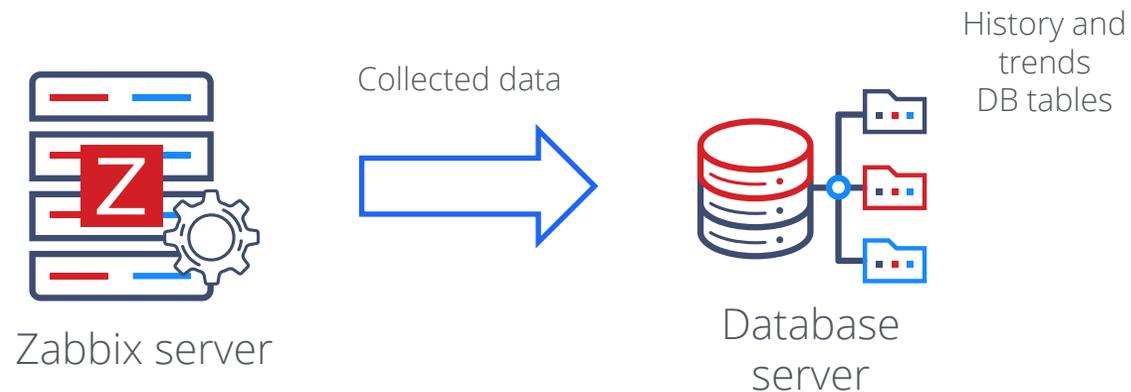
Why You Need Monitoring

Database storage

Zabbix Server stores all collected data in a central database according to its data type and purpose.

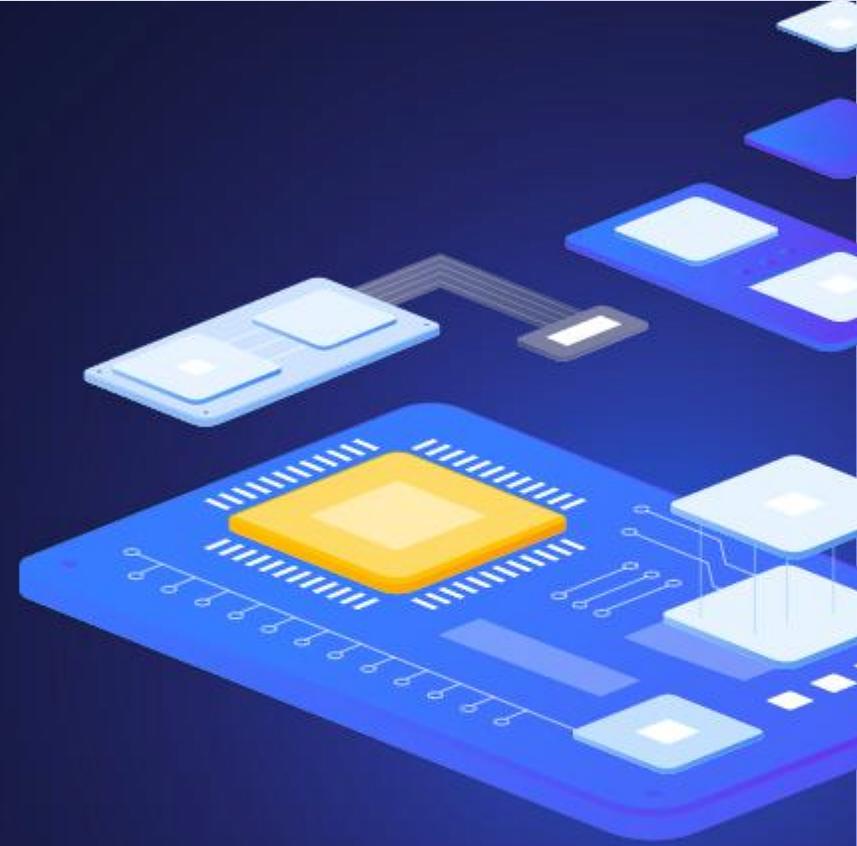
Two types of stored data based on purpose:

- ▶ History – every value collected by system at specified times (big and slow to process, but precise)
- ▶ Trends – each hour Zabbix calculates minimum, maximum, average (for an hour) and count of values and writes it to the separate tables. This speeds up the workflow with interface and some specific functions.



3

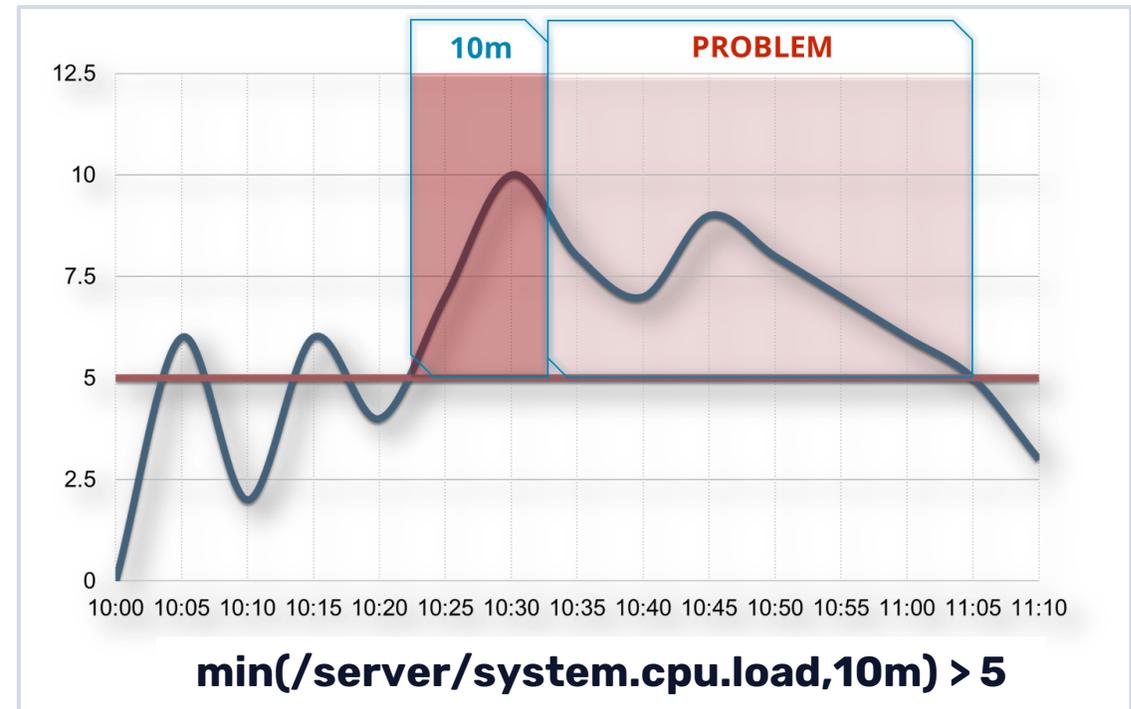
Data analysis



Why You Need Monitoring

Data analysis : trigger expressions

- ▶ It is useless just to store data in monitoring system without its analysis.
- ▶ Zabbix supports triggers – logical expressions that are evaluated each time we receive a new value.
- ▶ If logical expression is evaluated to TRUE – it means we have a PROBLEM and Zabbix will notify a user about that situation or perform other predefined action(s).



Why You Need Monitoring

Data analysis : trigger severities

Define trigger severity levels based on importance level. Since not all triggers carry the same level of importance, one of six severity levels can be assigned to a trigger. The severity level then is applied to the visual representation of triggers and can be used to finetune the reaction to problem events.

Severities are used for:

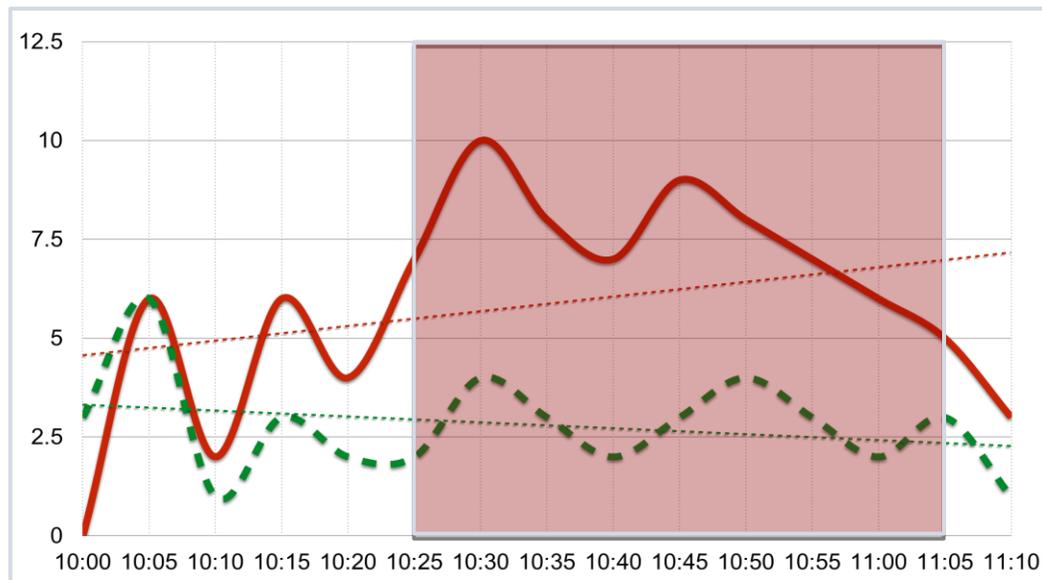
- › Visual representation of triggers
- › Audio in global alarms
- › Choosing notification channel (high severity - SMS, other - email)

Not classified
Information
Warning
Average
High
Disaster

Why You Need Monitoring

Data analysis : anomalies detection

With help of Zabbix trigger expressions we can even go back in history and check for anomalies – database data is used for that check.



For example: if load average today exceeds average load of the same hour yesterday for at least 2 times – we have a problem!

`avg(/server/system.cpu.load,1h) / avg(/server/system.cpu.load,1h:now-1d) > 2`

Why You Need Monitoring

Data analysis : machine learning

Defining problem thresholds manually is not always an efficient approach. In dynamic environments where the baseline values can periodically change it is important to automatically calculate a reference point against which the problem threshold will be calculated.

Zabbix Baseline monitoring enables you to do just that:

- ▶ Detect anomalies based on analysis of history data in real-time
- ▶ Get powerful insights using baseline monitoring



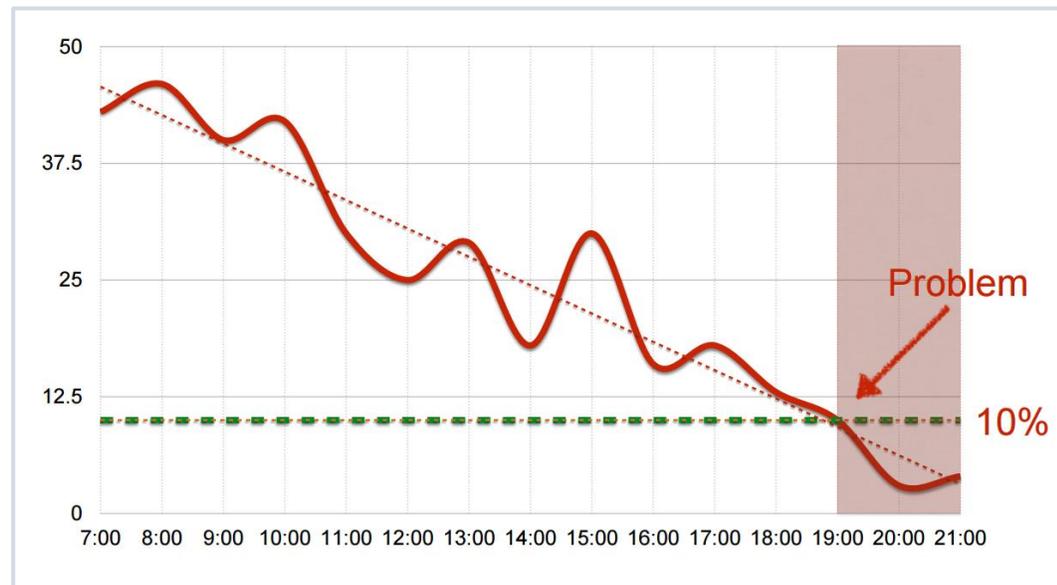
Why You Need Monitoring

Data analysis : a little of magic : forecasts

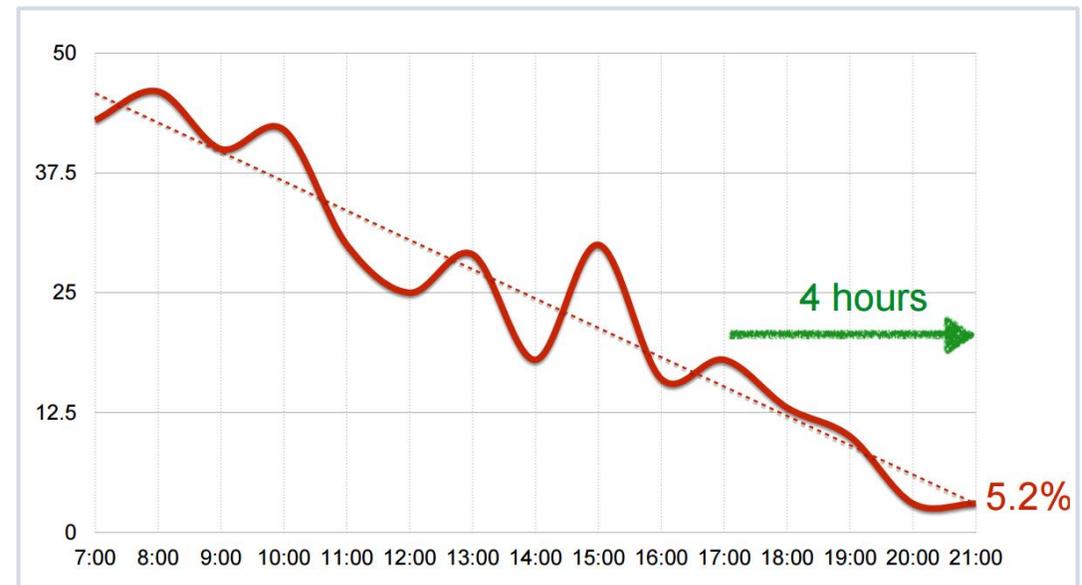
We can foresee the future by analyzing what had happened before in history (no magic, sorry – only statistics).

► We can:

Predict **time**
(when we hit a certain value?)



Predict **value**
(what value is going to be after certain period of time?)



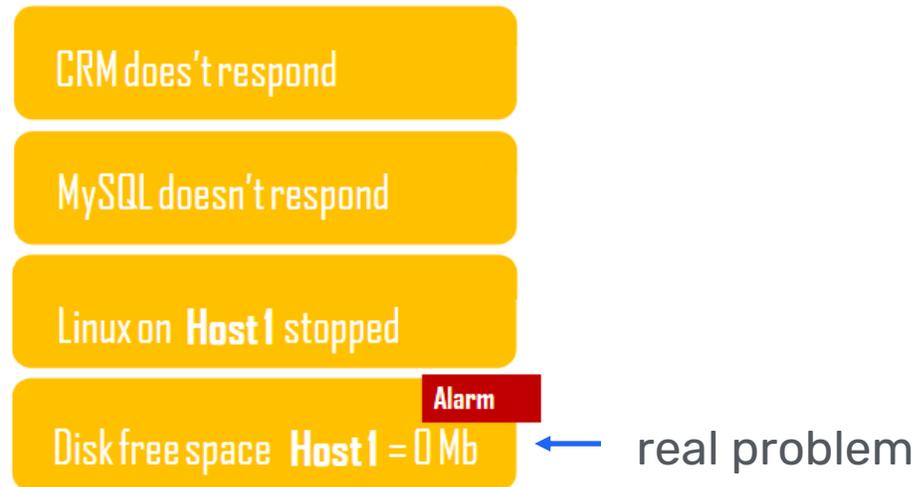
Why You Need Monitoring

Data analysis : emphasize important problems

With help of trigger dependencies, you can define multi-level trigger structure and have only important notifications that are relevant to current situation.

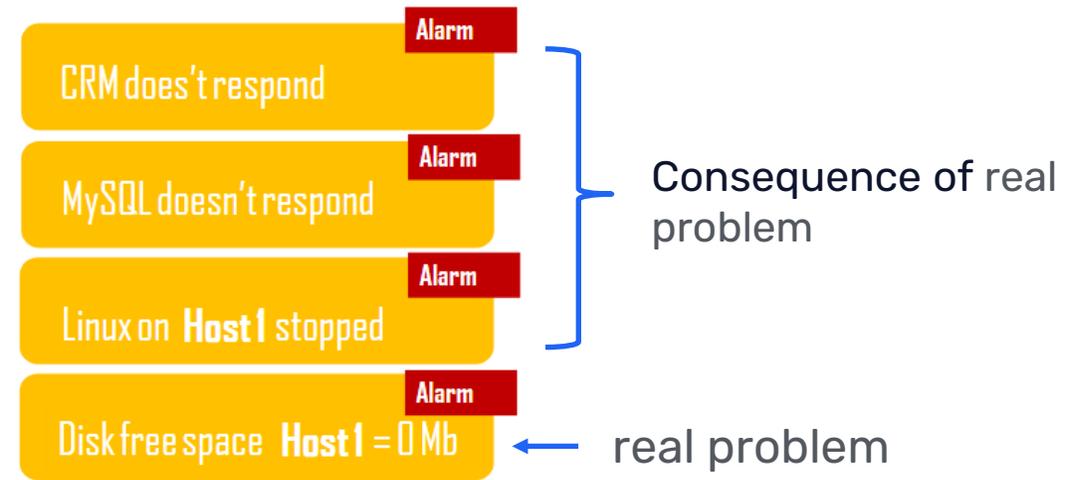
Example 1:

HostN problem list with dependencies



Example 2:

HostN problem list without dependencies



Why You Need Monitoring

Data analysis : business level monitoring

You can define services and create service trees to perform impact analysis:

- › Define and monitor business service SLA levels
- › Simulate an outage to see business-level impact
- › Multiple service status calculation algorithms
- › Define service weights for custom service status calculation
- › Calculate your business service availability based on service weights or number and percentage of unavailable child services



4

Notification and Automatization



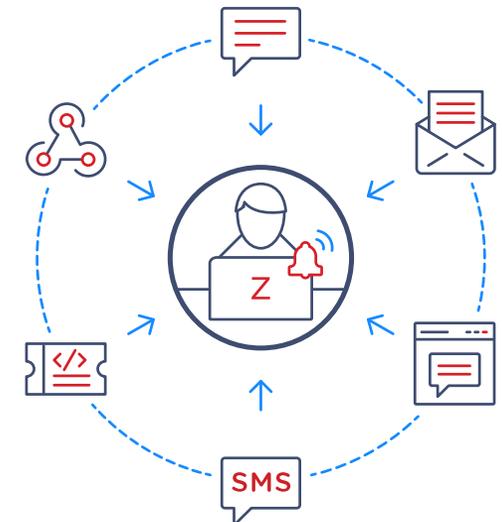
Why You Need Monitoring

Notifications and actions

You may use multiple messaging channels to notify the responsible person or people about the different kinds of events occurring in your environment:

- ▶ Alerting systems: VictorOPS, Opsgenie, Pagerduty, SIGNAL4, and more
- ▶ Email
- ▶ SMS for reliable alerts using USB modems
- ▶ Online SMS gateways
- ▶ Communication platforms: Slack, MS Teams, Telegram, Express.ms, Rocket.chat, and more
- ▶ Webhooks for integration with external messaging, ITSM or ticketing systems

Zabbix user may define different messages for different messaging channels. You can either utilize the default message templates or create and customize your own message template.

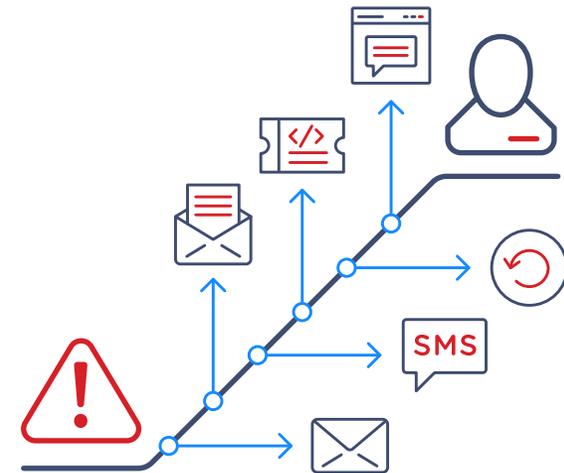


Why You Need Monitoring

Notifications : escalations

You can escalate the notification for faster resolution: from simple notifications and escalations to different users, to delayed notifications and automatic issue remediation:

- › Immediately inform users about new problems
- › Proactively execute remote scripts
- › Repeat notifications until problem is resolved
- › Delay notifications and remote commands
- › Escalate problems to other user groups
- › Different escalation paths for acknowledged and unacknowledged problems
- › Send a recovery message to all of the involved parties
- › Unlimited number of escalation steps



Why You Need Monitoring

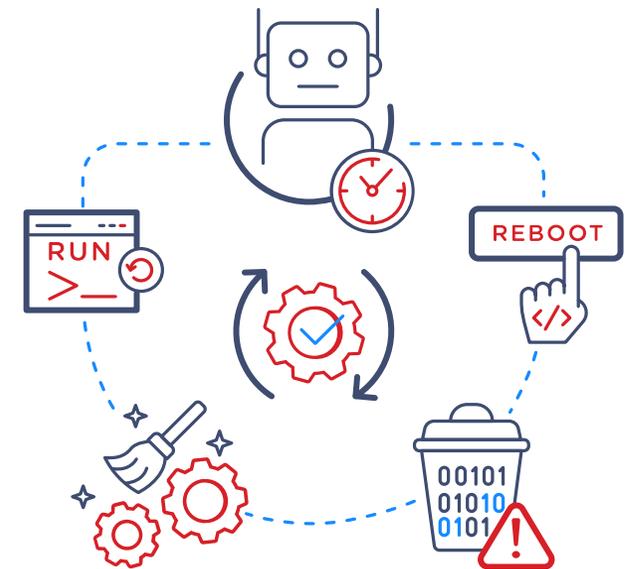
Auto-remediation

With Zabbix you can not only receive a notification about a problem but also automatically resolve it.

A remediation script or command can be executed to attempt and resolve the issue.

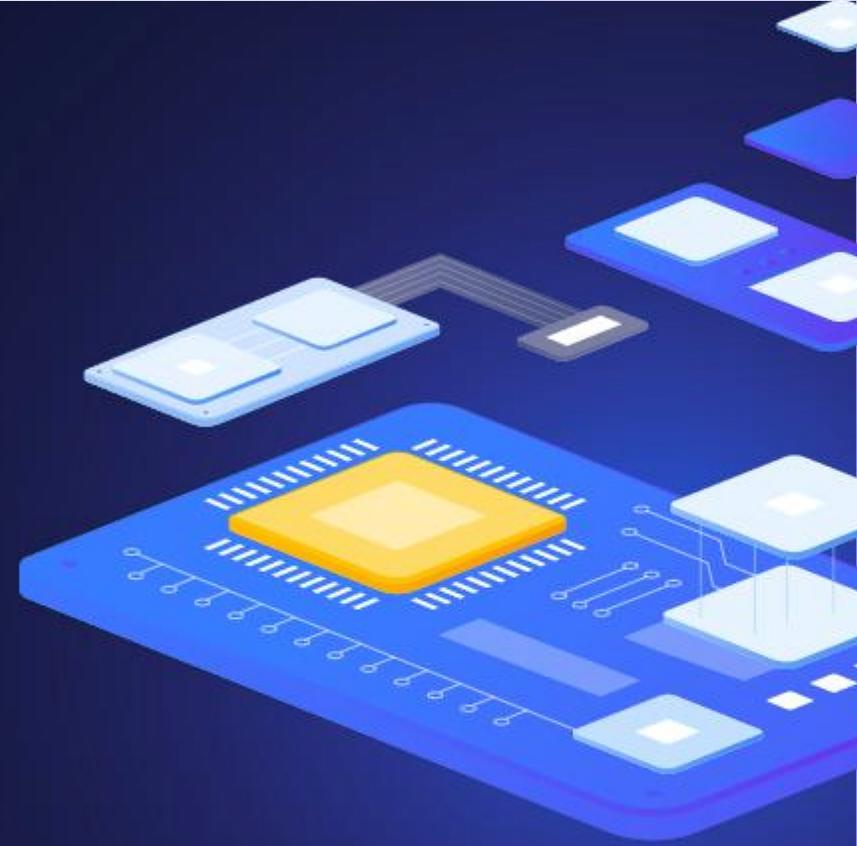
Execute a remediation script to:

- › Restart a service
- › Manage your cloud resources
- › Perform automatic resource rescaling
- › Executing any other custom logic





Questions?



Why You Need Monitoring

CONTACT US:

Phone:



+420 800 244 442

Web:



<https://www.initmax.cz>

Email:



tomas.hermanek@initmax.cz

LinkedIn:



<https://www.linkedin.com/company/initmax>

Twitter:



<https://twitter.com/initmax>

Tomáš Heřmánek:



+420 732 447 184