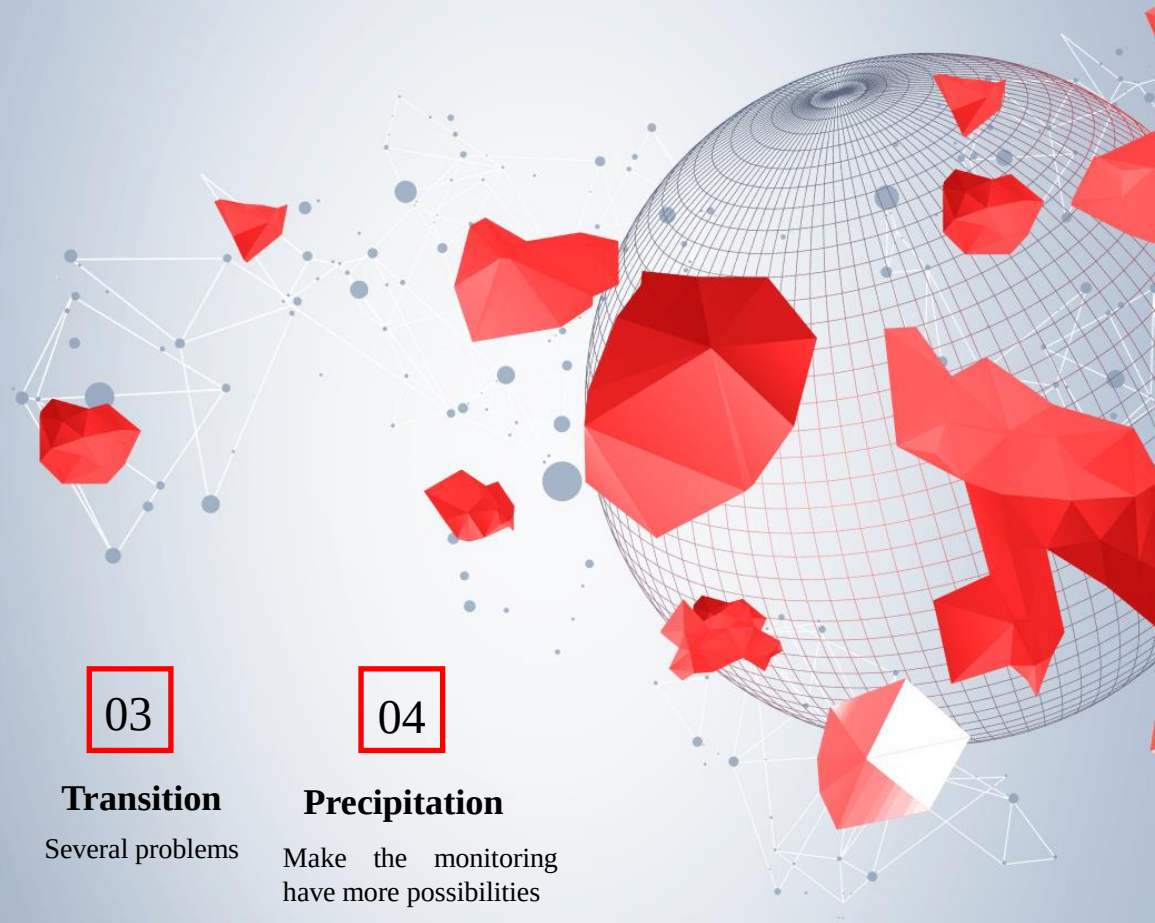
ZABBIX SUMMIT ONLINE /2020

MONITORING EVOLUTION FOR CLOUD NATIVE ENVIRONMENTS

Wang Manxue

Technical manager, China Mobile Online Service Co., Ltd, China

CONTENT



01

Background

Centralized maintenance throughout the country and the biggest over the world

02

Way out

Choose open source

03

Transition

Several problems

04

Precipitation

Make the monitoring have more possibilities

01

BACKGROUND

——CENTRALIZED MAINTENANCE THROUGHOUT THE COUNTRY AND THE BIGGEST OVER THE WORLD

Respond to the challenge actively

operation challenge

Huge amount of users

- There are 900 million users and more than 100 million WeChat fans. The monthly service is more than 100 million times; followers of Weibo are 30.38 million (be the first of the industry); there are more than 50 million users for 10086 APP.
- Ten thousand servers

High requirement

Have high requirement and provide telecom-level service

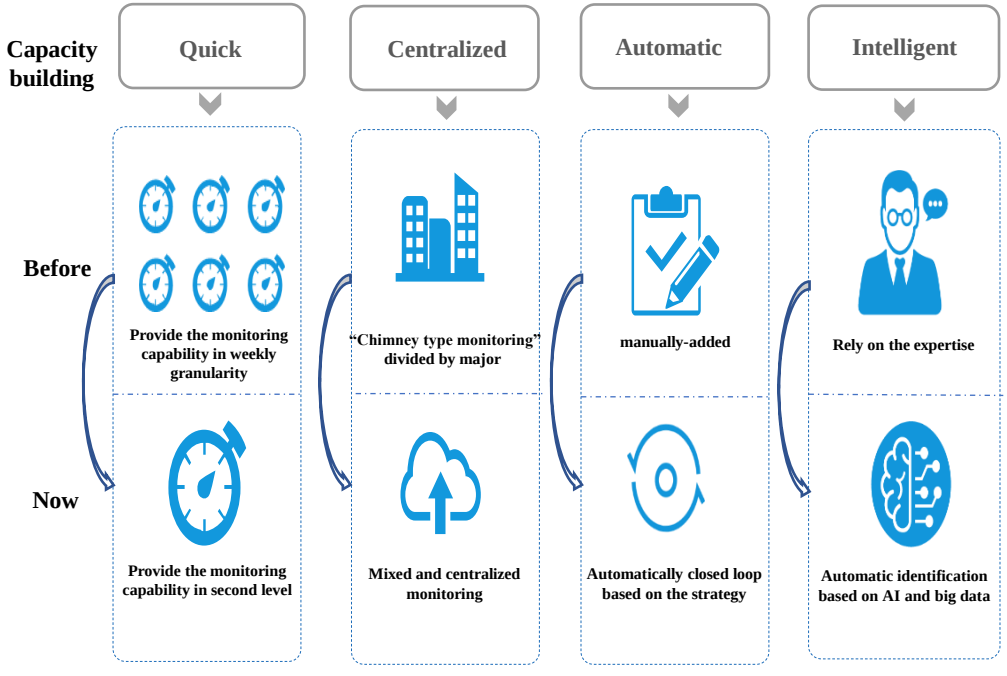
- 99.999% reliability
- 7* 24 guarantee

Hard

The business changes fast and the operation environment is complicated

- Pop up online for 120 times daily and deal with 500 work orders daily
- New technology: Microservice/cloud computing/ container …

Respond actively

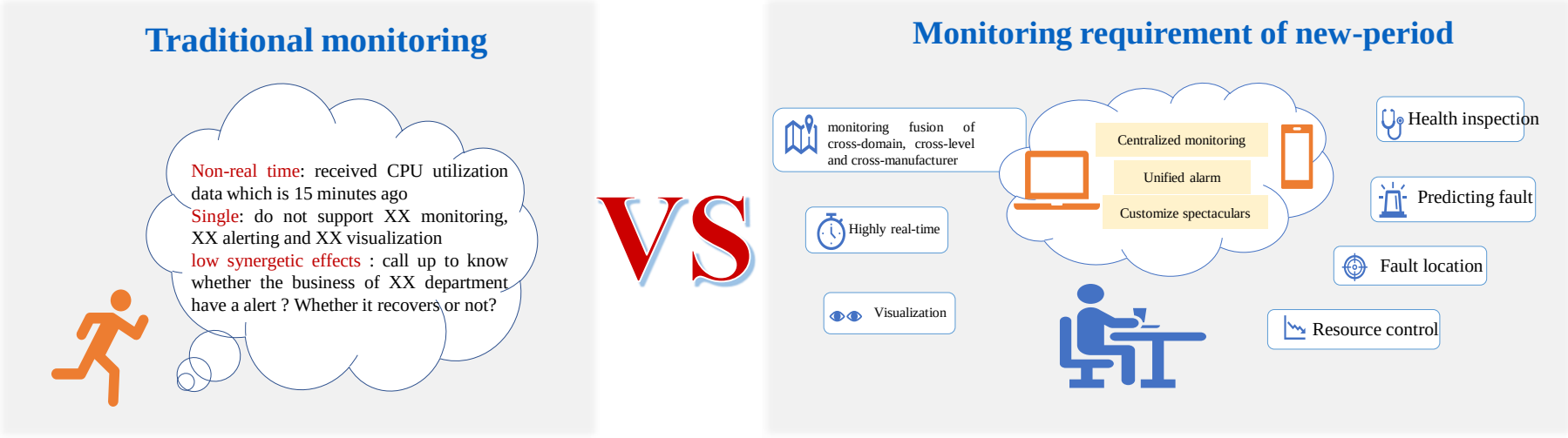


02

WAYOUT
——CHOOSE OPEN SOURCE

- EMBRACE OPEN SOURCE
- UNIFY THE MONITORING PLATFORM
- BRIEF SUMMARY

Embrace open source



Embrace open source and stand on the shoulder of giants-Zabbix

Rapid implementation: utilize the mature capacity of Zabbix and finish the capacity building of monitoring system rapidly in 1 month

Full coverage: the official templates of Zabbix and the templates from community can realize the monitoring coverage of multi-operation system and mainstream middleware rapidly

Real-time stability: Zibbix is very mature, and it can realize second-level data collection; there is no fault online in 3 years

Visualized dashboard: nice combination of Zabbix and Grafana , making abundant visualized dashboards rapidly

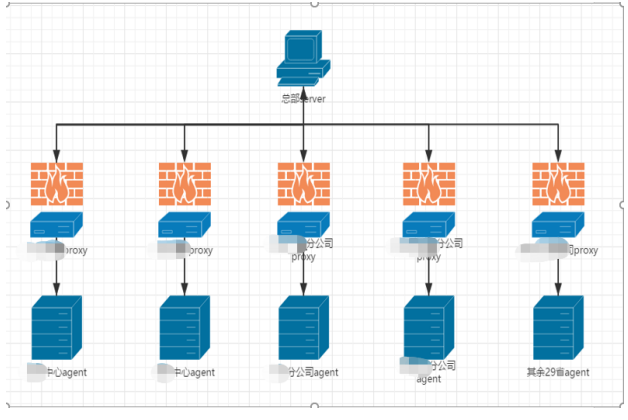
High efficiency and low cost: Zabbix's resource consumption is very low. The main consumption is that the database needs physical hardware support, which takes less resources than Prometheus

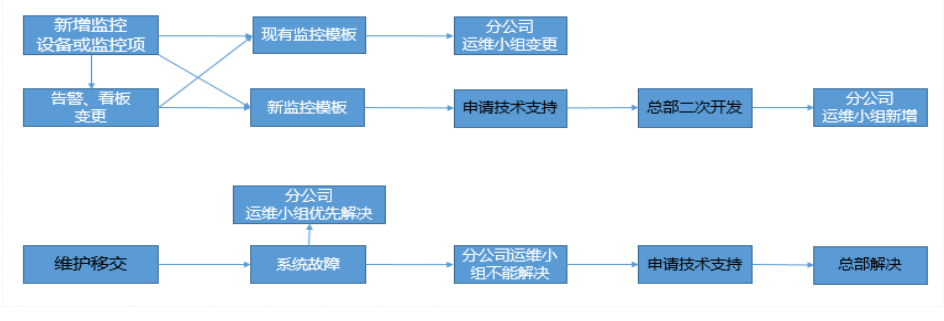
Unify the monitoring platform: centralized construction, unified control and standardized edge node

In order to establish the monitoring ability more quickly and control the system quality more comprehensively, we adopted the construction mode of centralized building, unified management, and standardized accessibility for all our branches.

Network centralization:

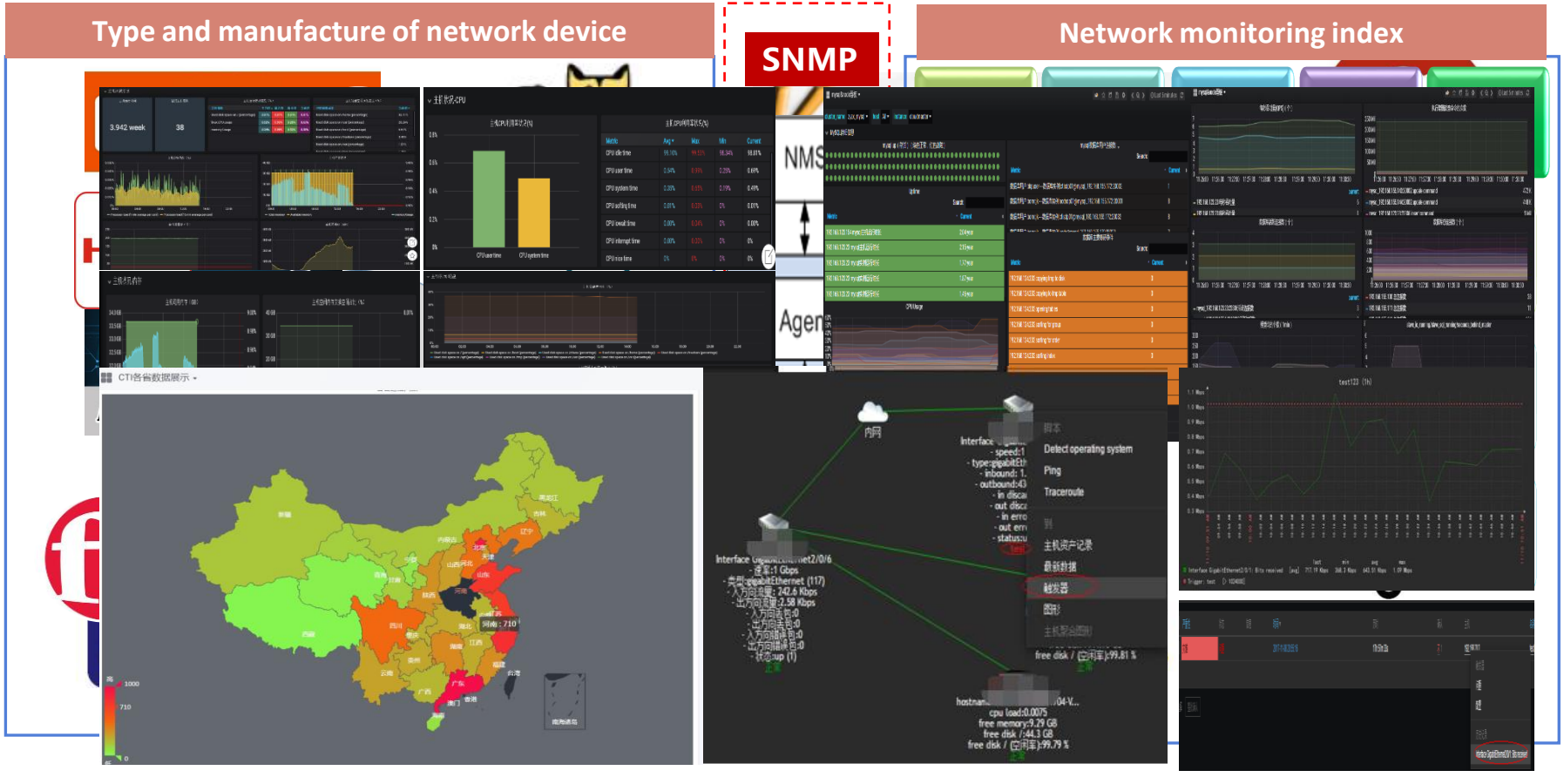
- *The headquarter takes charge of the construction of monitoring capability, standardization of the edge node and the collection, analysis, expression and notification of all the monitoring data.*
- *The branch provides resource maintain and manage the monitoring resource by following the standardized and packaged monitoring templates.*





Summaries: extensive, abundant, various and flexible

The dashboards can be made flexibly and the allocation can be finished in min-level. The diagram is shown in diversified: Line chart, bar chart, pie chart, area chart and topology,etc.



Summaries: within half a year

10000 Hosts	**2 million** Monitoring items	**900 000** Triggers	**300 000** Alerts
84 Proxies	**400+** DashBoard	**545** Users	**1.3K** Actions

Summaries: Zabbix System Optimization

Database

CPU/memory/IO

Connection

(Maximum number of connections, timeout duration)

Data consistency

Suggest adopting database SSD hard disk

Host parameter

Kernel parameter

TCP protocol stack parameter

Semaphore/IO（Zabbix do not release signal set when fails to start）

WEB

Nginx parameter

Php parameter

php.ini：max_input_vars（influence template application and a lot of hosts fail）

Zabbix

Configure the number of startup modules and processes according to specific requirements

Forbid auto discovery, adopt script to call API

Forbid housekeeper and Enable database table partitioning

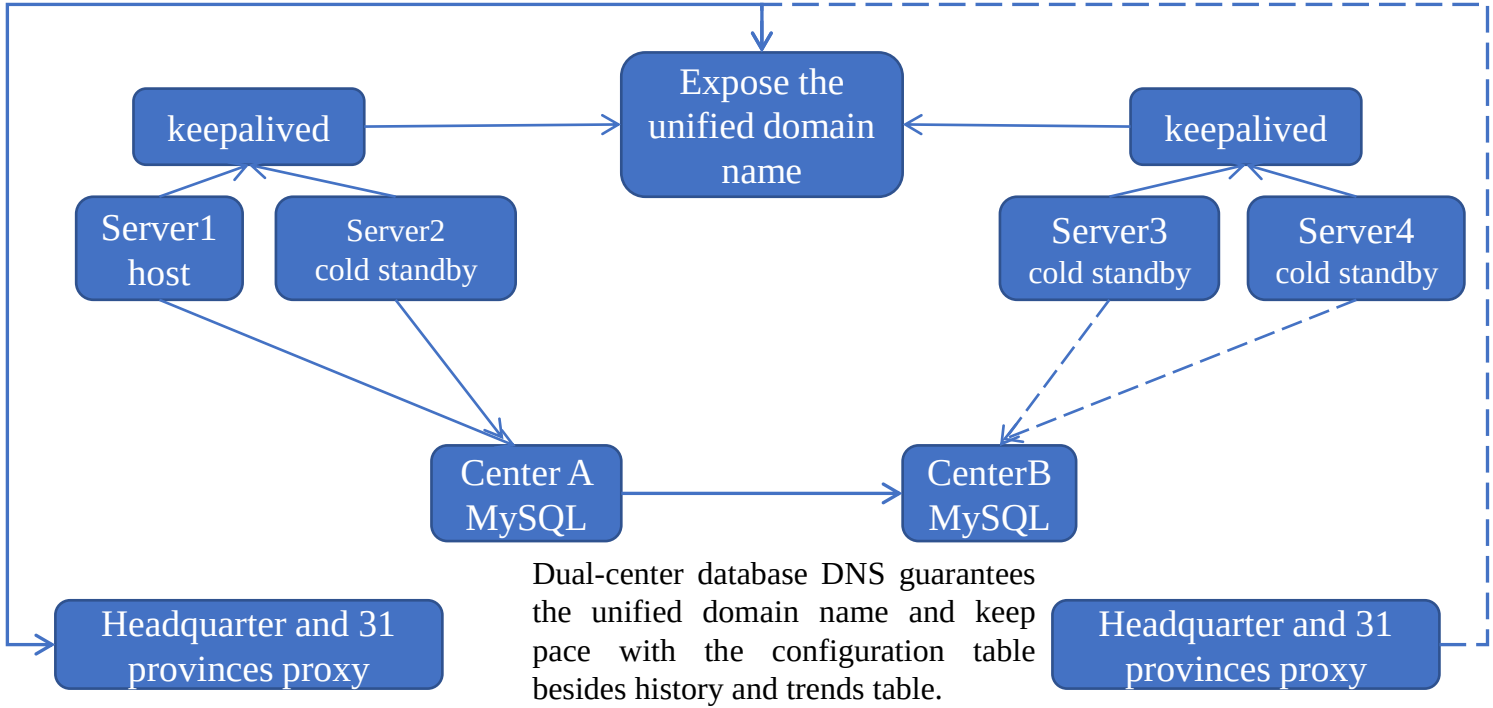
Forbid server connecting agent directly

Configuration parameter optimizaion

defines.inc.php：QUEUE_DETAIL_ITEM_COUNT（define the queue search limitation of the monitoring item and influence the display of information queue）

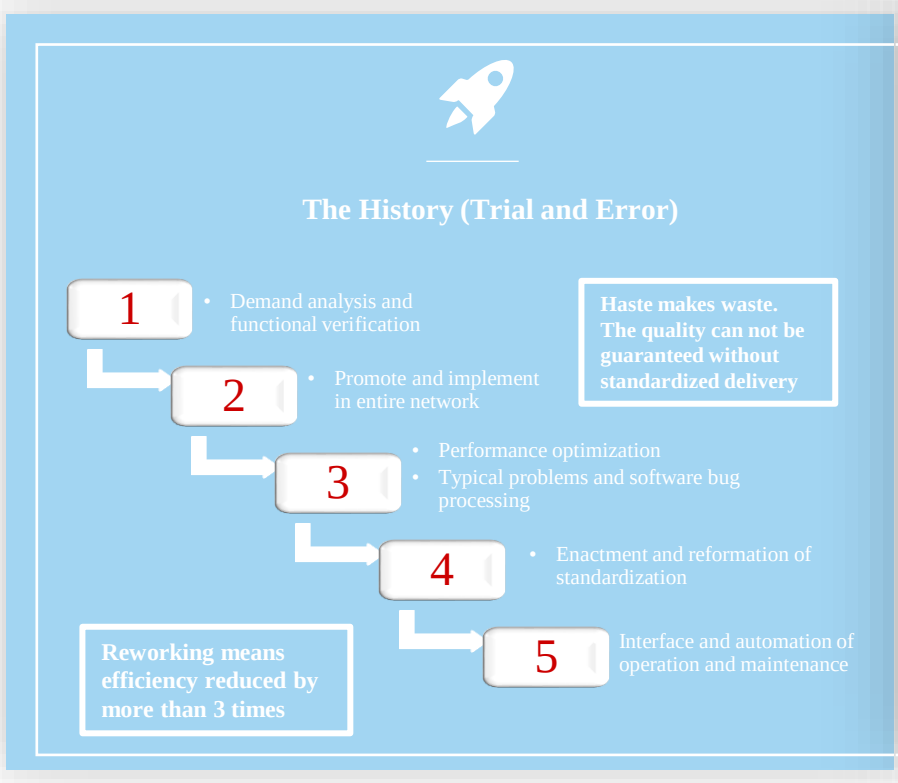
Summaries: dual-center, high-availability solution for Zabbix

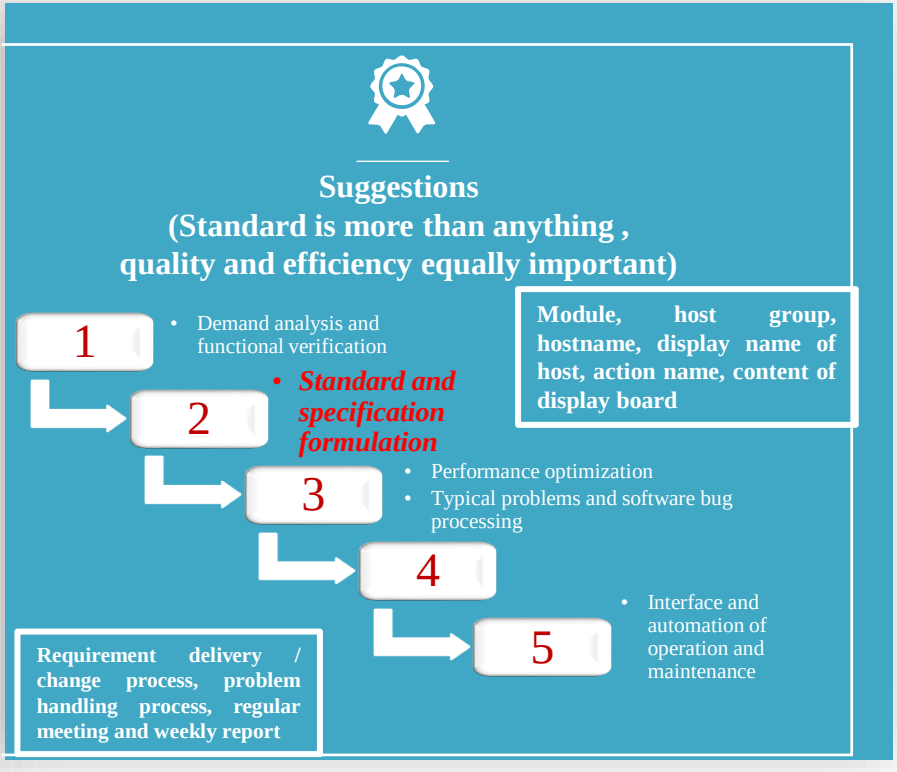
Deploy Zabbix system by A/B dual-center, provide service by exposing the unified domain name, and develop the capability that corresponding proxy switch server with one-click. When the North-Center fault occurs, the server service can be switched by fast switch ZABBIX server domain name resolution. And switch all the proxy server by the automated scripts with the one-click . In case of fault occurs, it can ensure the quick recovery of one key monitoring service within 10 minutes.



Dual-center database DNS guarantees the unified domain name and keep pace with the configuration table besides history and trends table.

Experience


The History (Trial and Error)
1
Demand analysis and functional verification
2
Promote and implement in entire network
3
Performance optimization
Typical problems and software bug processing
4
Enactment and reformation of standardization
5
Interface and automation of operation and maintenance
Haste makes waste. The quality can not be guaranteed without standardized delivery
Reworking means efficiency reduced by more than 3 times


Suggestions
(Standard is more than anything , quality and efficiency equally important)
1
Demand analysis and functional verification
2
Standard and specification formulation
3
Performance optimization
Typical problems and software bug processing
4
5
Interface and automation of operation and maintenance
Module, host group, hostname, display name of host, action name, content of display board
Requirement delivery / change process, problem handling process, regular meeting and weekly report

03

TRANSITION
——SEVERAL PROBLEMS

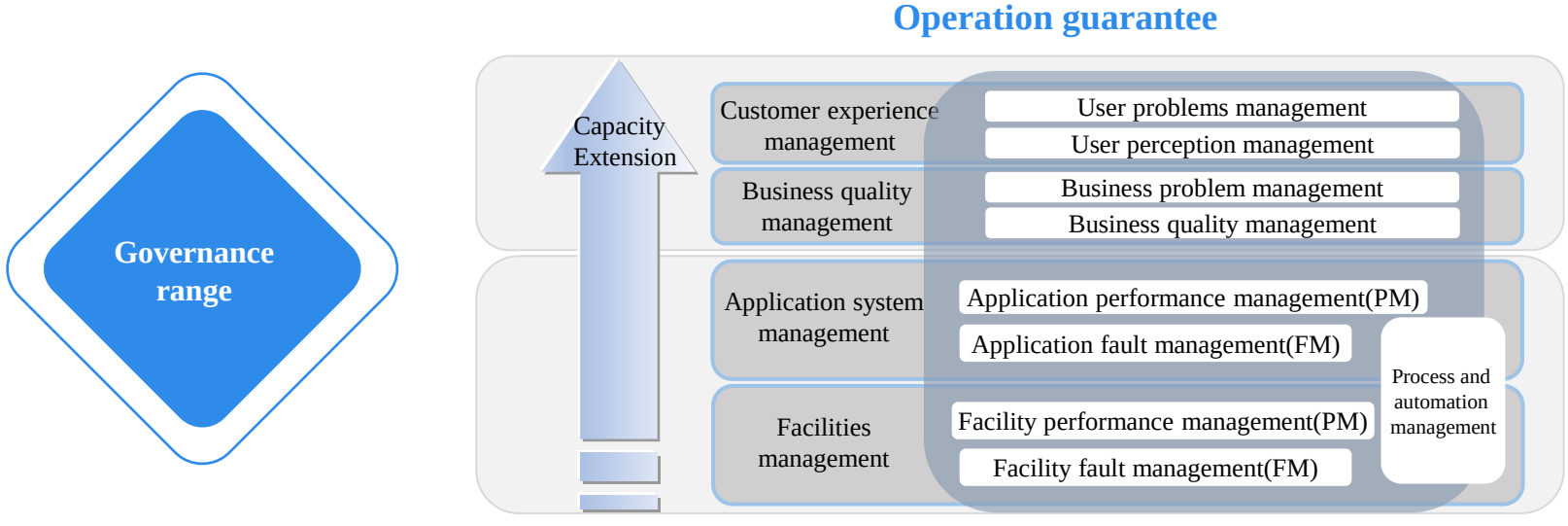
Q1: WE DIDN’T GET ANY NOTIFICATION WHEN OUR SERVICES WERE DOWN WHILE WE COLLECTING 2 MILLION METRICS?

Q2: IS THERE ANY VALUE IN USING MASSIVE LOGS

BRIEF SUMMARY

Q1: we didn’t get any notification when our services were down while we collecting 2 million metrics?

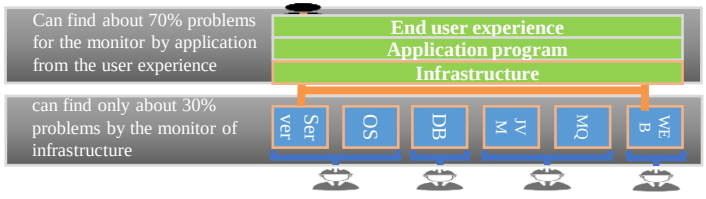
- Take the business quality and customer experience at the core and the target should be manageable, visualized and measurable.
- Network centralized construction, centralized control and standardized access of edge node.
- Software monitoring + hardware monitoring, unify, fusion and fluxion of operation data, construct multi-level measurement system.
- Based on the user experience, establish full link monitoring from end to end; link alert, complaint pre-warning and customer service as whole closed—loop system.



Business and application quality is perceivable, which is the core of monitoring

On the basis of strengthening the monitoring of basic settings, the application performance monitoring and service quality monitoring capabilities are supplemented to ensure the business stability and customer perception.

Application performance management



Application performance monitoring connects front-end with back-end service and user network environment to achieve end-to-end full link and code level monitoring.

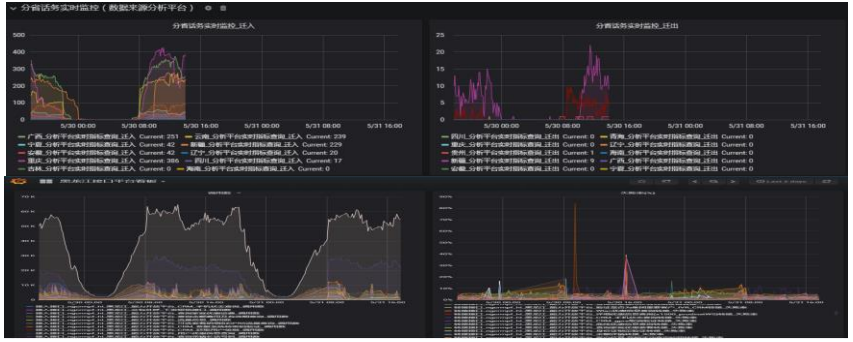
User experience rating → **Front-end interactive experience** → **Network slicing** → **application topology** → **Code location & tracking**

Business quality monitoring

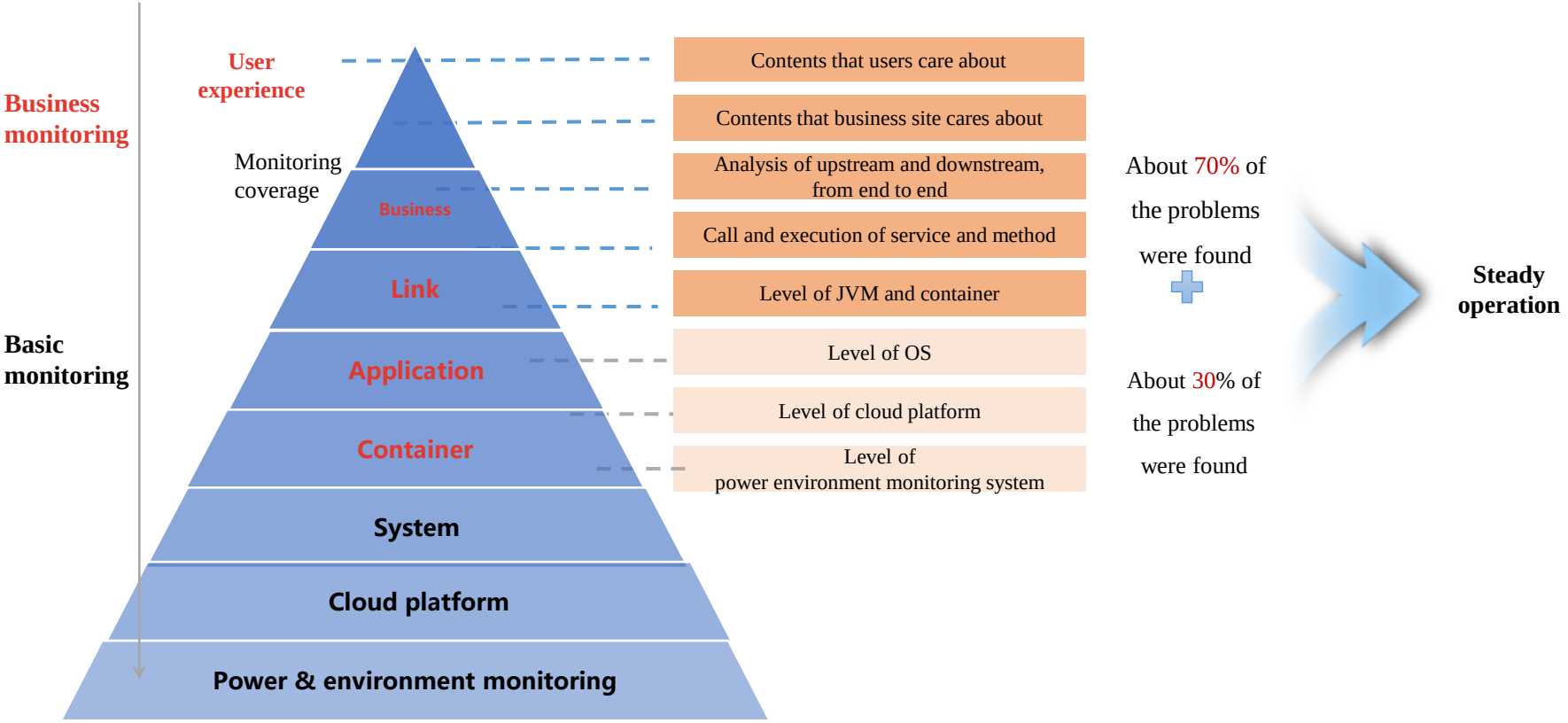
Sorting out the core function modules of business system → Sort out the core monitoring indicators of functional modules → Extraction method and effectiveness of evaluation monitoring indicators → Produce monitoring dashboard

Refer to Google SRE 5 gold metrics

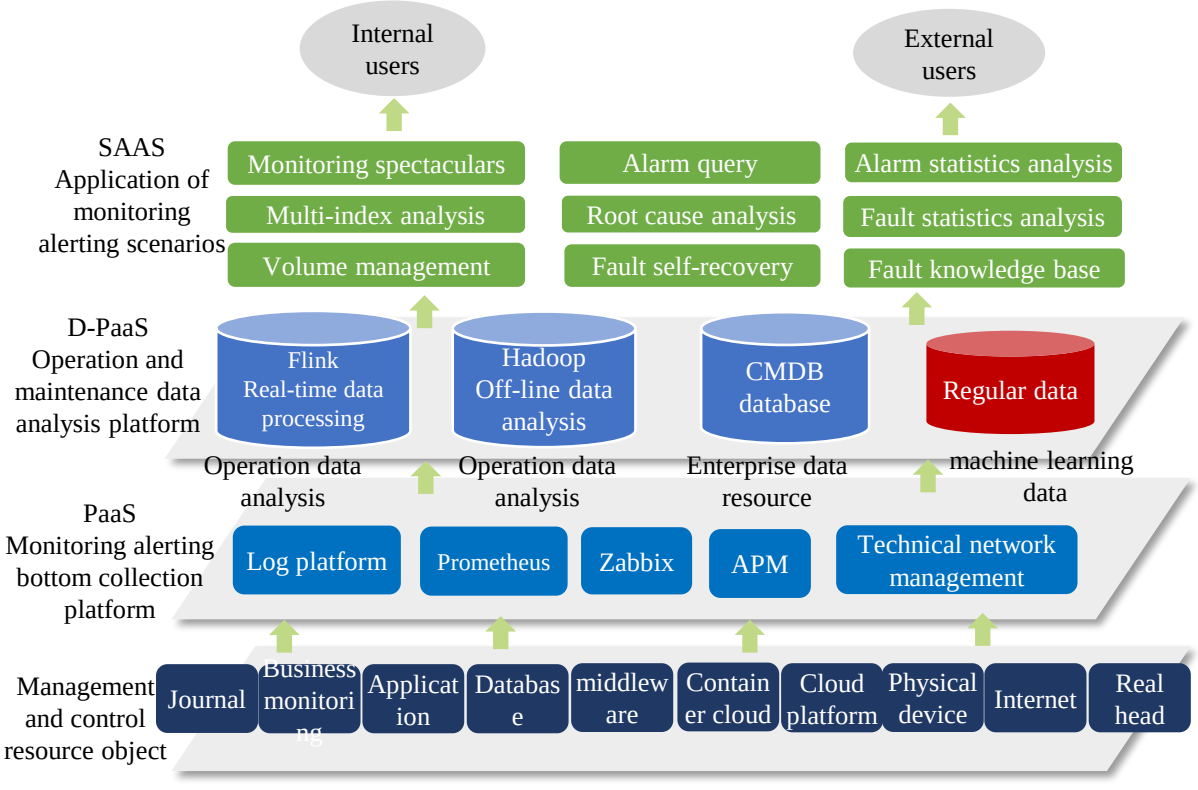
1. Rate: request rate, the number of requests per second.
2. Error: error rate, which is the number of errors per second.
3. Latency: response time, including queue / wait time, in milliseconds.
4. Saturation: the degree of overload, which is related to the resource utilization rate, and can also be directly measured by queue depth.
5. Utilization: the busy level of a resource or system, usually expressed as 0% to 100%.



Monitoring layer in cloud architecture



Construction of an open, independent and self-controllable alerting monitoring monitoring system



"1 platform, 4 systems and 3 capabilities"

automatic operation system

One platform- monitoring alerting platform

Four systems

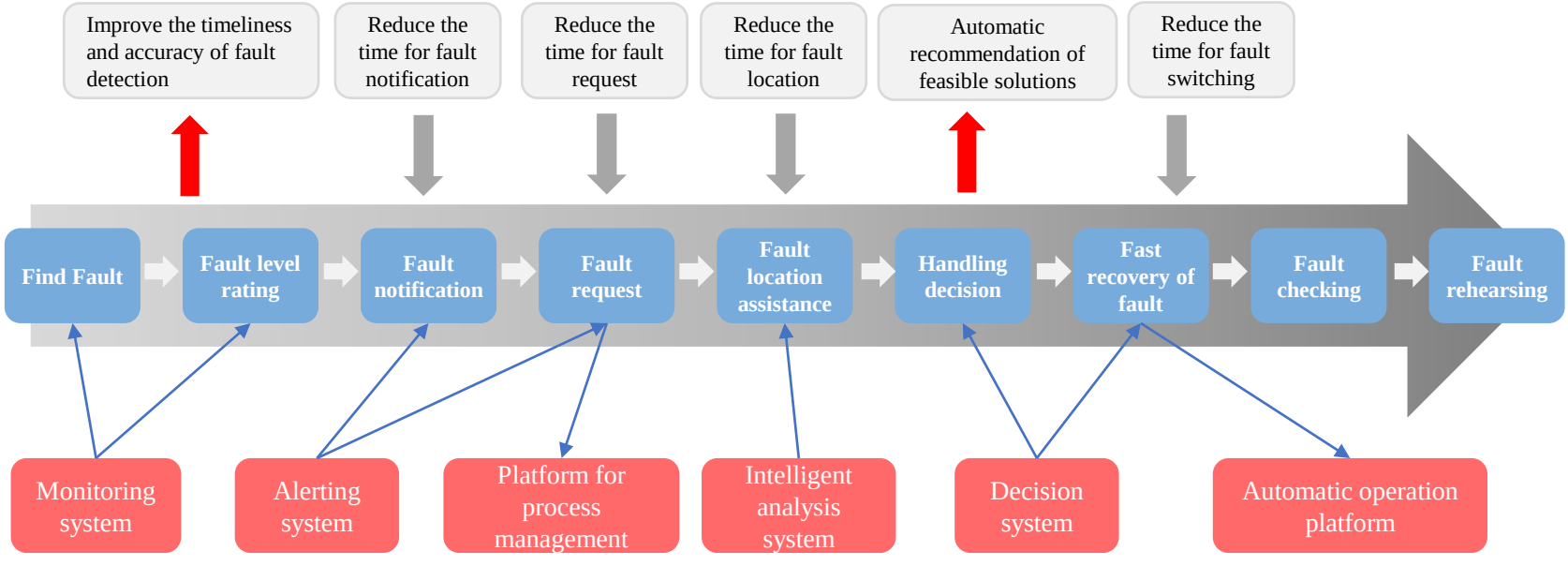
- Link system of four in one: control, monitor, manage and operation
- Support system of decision analysis: handling the daily faults basing on big data analysis and artificial intelligence algorithm
- Develop operation and cooperation system: construct high-efficient organization and cooperation system and open operation capability
- Evolution system of operation service: the operation service can be measured with 360 degrees

3 capabilities

- Automation capabilities: implement with high efficiency and improve the efficiency of personnel
- Data capability: operating state is transparent and can optimize digital drive system
- Intelligent capability: utilize artificial intelligent algorithm to assist operation to make decision and analyze

Realize automatic and intelligent operation scenarios from end to end

Realize the automatic handling of fault operation from end to end through the basic capability construction of the platform and combining the rules, algorithm, workflow engine and fault tree to improve the efficiency and quality of operation work.



04

PRECIPITATION ——MAKE THE MONITORING HAVE MORE POSSIBILITIES

- AUTOMATIC ACCELERATION
- DATA EMPOWERING

1. Automatic acceleration

Pain points

- Large enterprises have much basic resource, extensive business, frequent online change and huge monitoring configuration task
- Monitoring addition can not be completed immediately and needs frequent adjustment, and the repeated workload is large
- The use barrier of open source tools is high. There is no user-friendly web page for most of it and it can be used flexibly after training
- The workers are all over the country; the basic resource has been to 10 000 level; the business change is frequent; it is difficult for unified management

Solutions

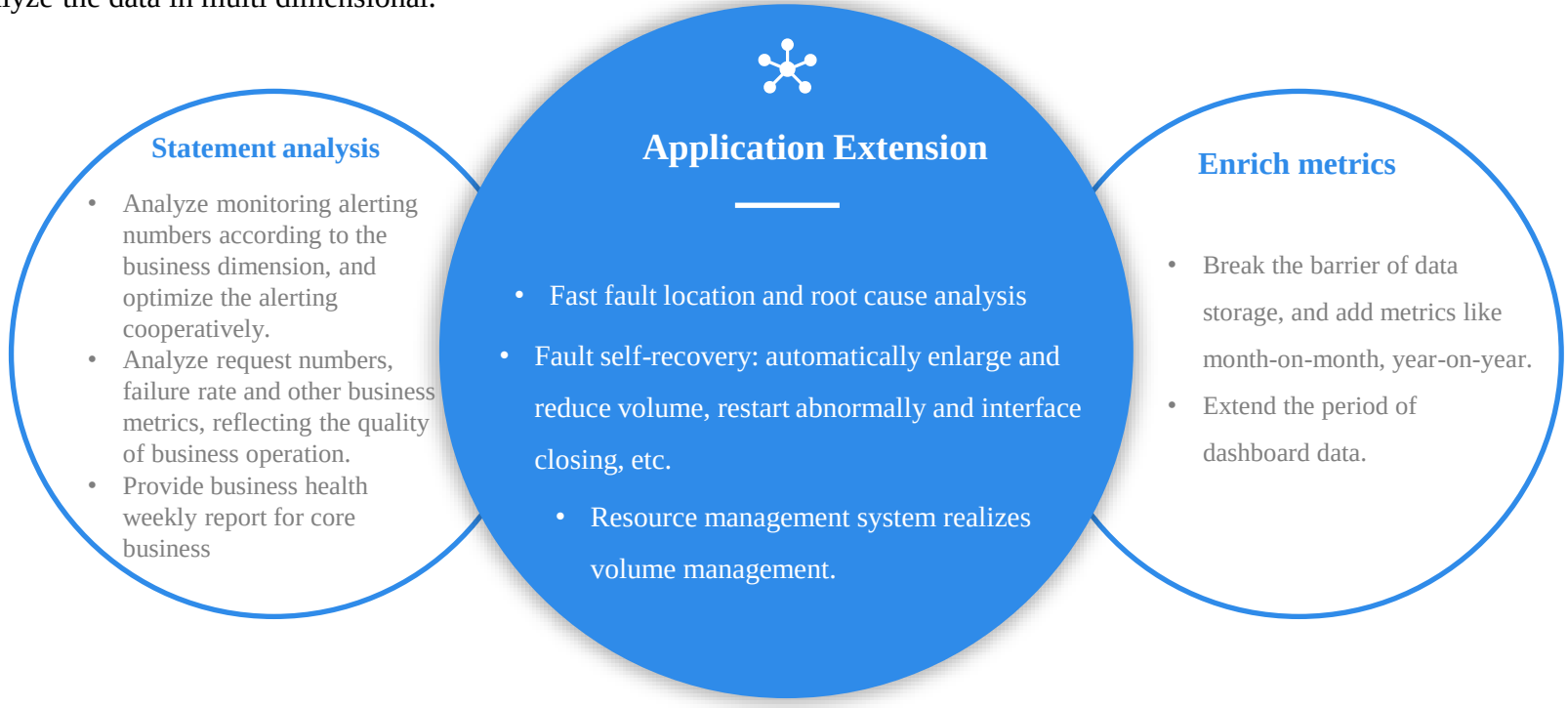
1. Standardization, streamlining and modularity of monitoring capability
2. Second development, automation
3. Interface of configuration, Interface of data expression

At present, self-service monitoring can realize all kinds of self-service monitoring, including adding, deleting, modifying and checking, covering 85% of the company's monitoring needs. only two engineers can maintain the whole monitoring system to chieve followings:

1. Add the basic monitoring items of host resource application process with one-click,
2. addition, deletion and modification of alerting contact,
3. query of monitoring coverage with one-click,
4. regular inspection of Zabbix, etc.

2. Data empowering

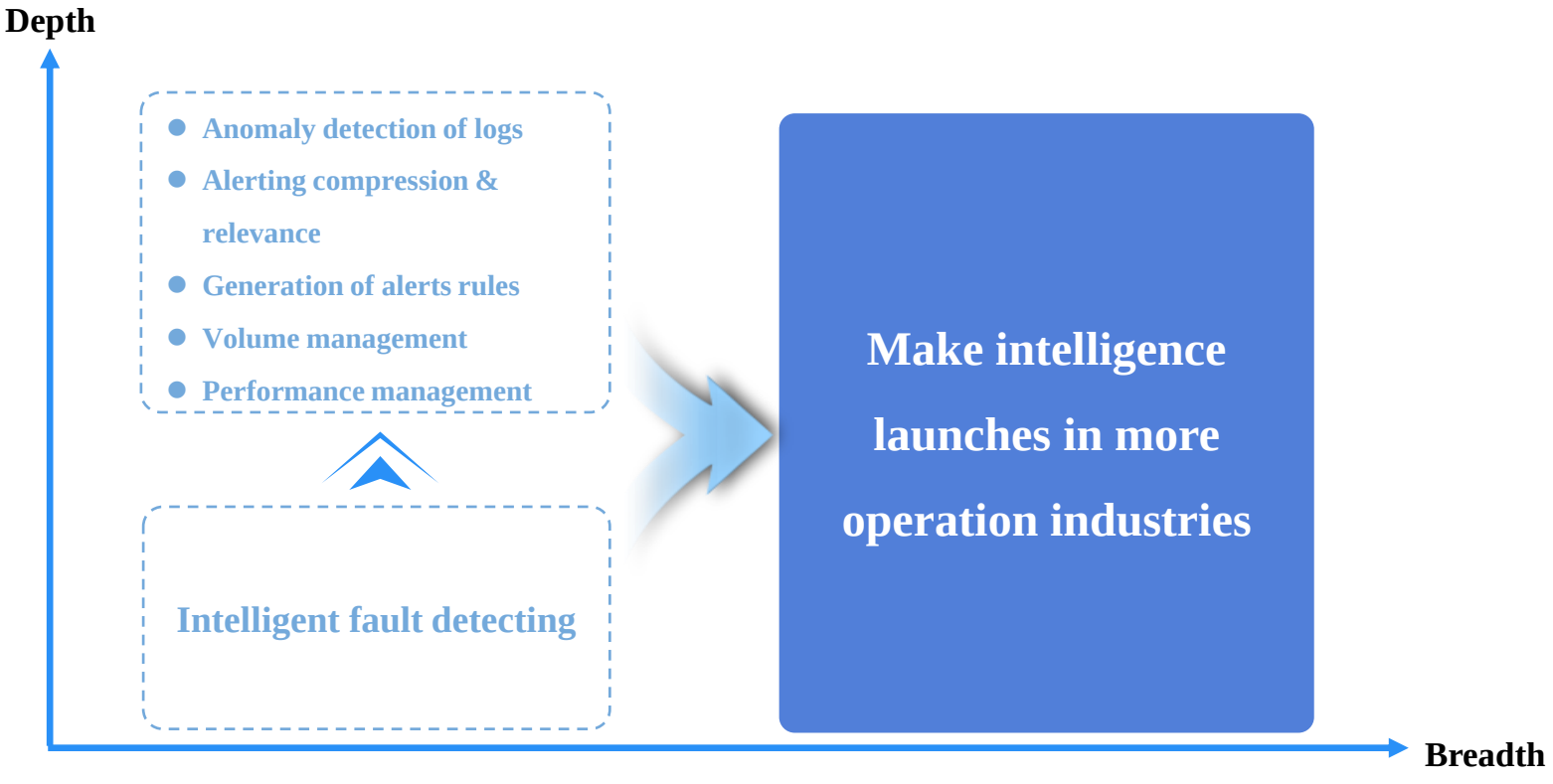
Extract Zabbix, Prometheus, alerting platform, log platform, CMDB and other data to load on the big data analysis platform and to analyze the data in multi dimensional.



Current figures

1 000 000 **Hosts**	26 060 000 **Monitoring items**	**780 000** **Triggers**	1 980 000 **Alerting**
60 billion **Logs**	**1700+** **DashBoard**	975 **Users**	**84** **Proxies**

Future


Depth
Anomaly detection of logs
Alerting compression & relevance
Generation of alerts rules
Volume management
Performance management
Intelligent fault detecting
Make intelligence launches in more operation industries
Breadth

Thank you!