

ZABBIX 2020
Conference
CHINA

演讲主题

安信证券监控平台的设计和实现

演讲嘉宾

李俊平 监控平台负责人 安信证券股份有限公司



01

背景



监控 VS “北斗”

“北斗” 监控平台，想到什么？

- 整体性
监控的集中与统一
- 准确性
监控要控制失真，减少误报漏报
- 扩展兼容性
监控架构应具有良好的扩展兼容性，能快速吸纳更多新工具
- 持续性
监控平台的持续优化



安信证券“北斗”监控平台

背景

既有传统应用也有互联网应用，系统部署方式有：集中部署、分布式部署、容器化部署、云上部署

数据库种类多样，各类关系型数据库、NoSQL数据库都存在



自研系统与外部系统异构并存，各系统还有关联关系，但技术栈、标准化程度不一样

较多系统部署于Windows操作系统，比例接近50%

背景

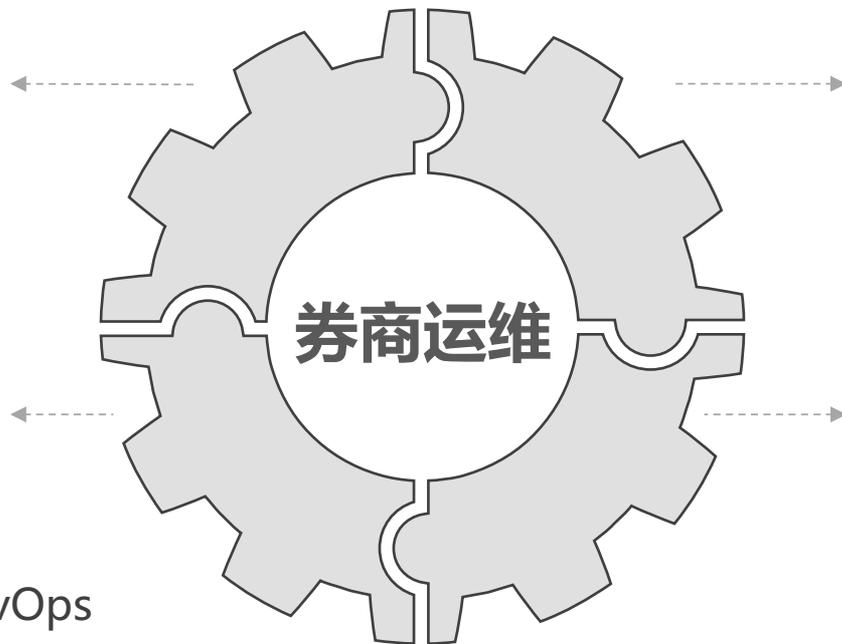
业务连续性、系统稳定性、安全性要求高

系统RTO、RPO期望趋
近于0

双态运维并存

稳态：核心业务，ITIL

敏态：非核心业务，DevOps



事前预防

海恩法则：任何事故的发生之前一定有很多个征兆

墨菲定律：可能发生的一定会发生

强监管

对于核心业务，RTO：
5min，RPO：30s

超过需要上报监管

无监控、不运维

背景

● 周期规律

天



周



系统的并发在线人数与业务量，开市期间达到峰值，其它时间段稳定

背景-平台建设



理想

- 标准化
- 自动化
- 平台化
- 智能化



现实

- 需求变化
- 并行建设
- 场景覆盖
- 持续演进

02

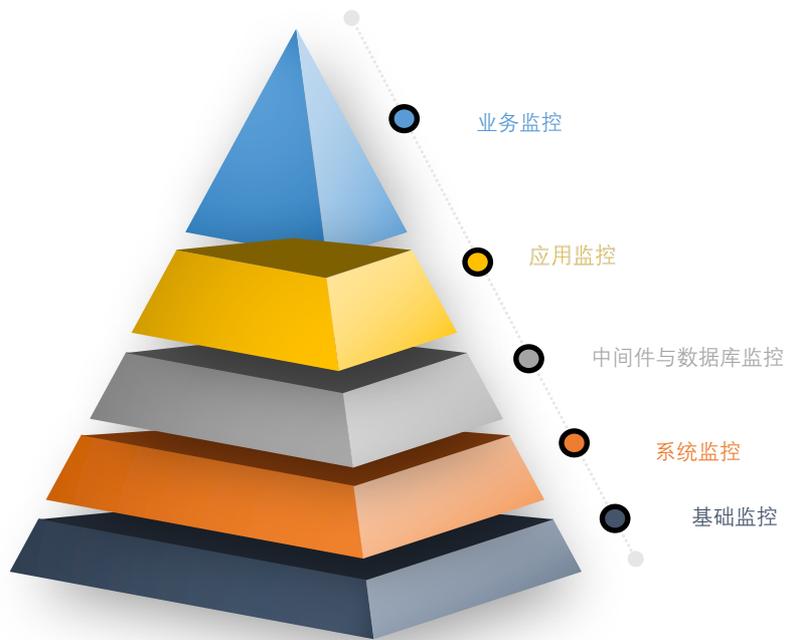
演进



监控平台（阶段一）

Tivoli统一监控系统

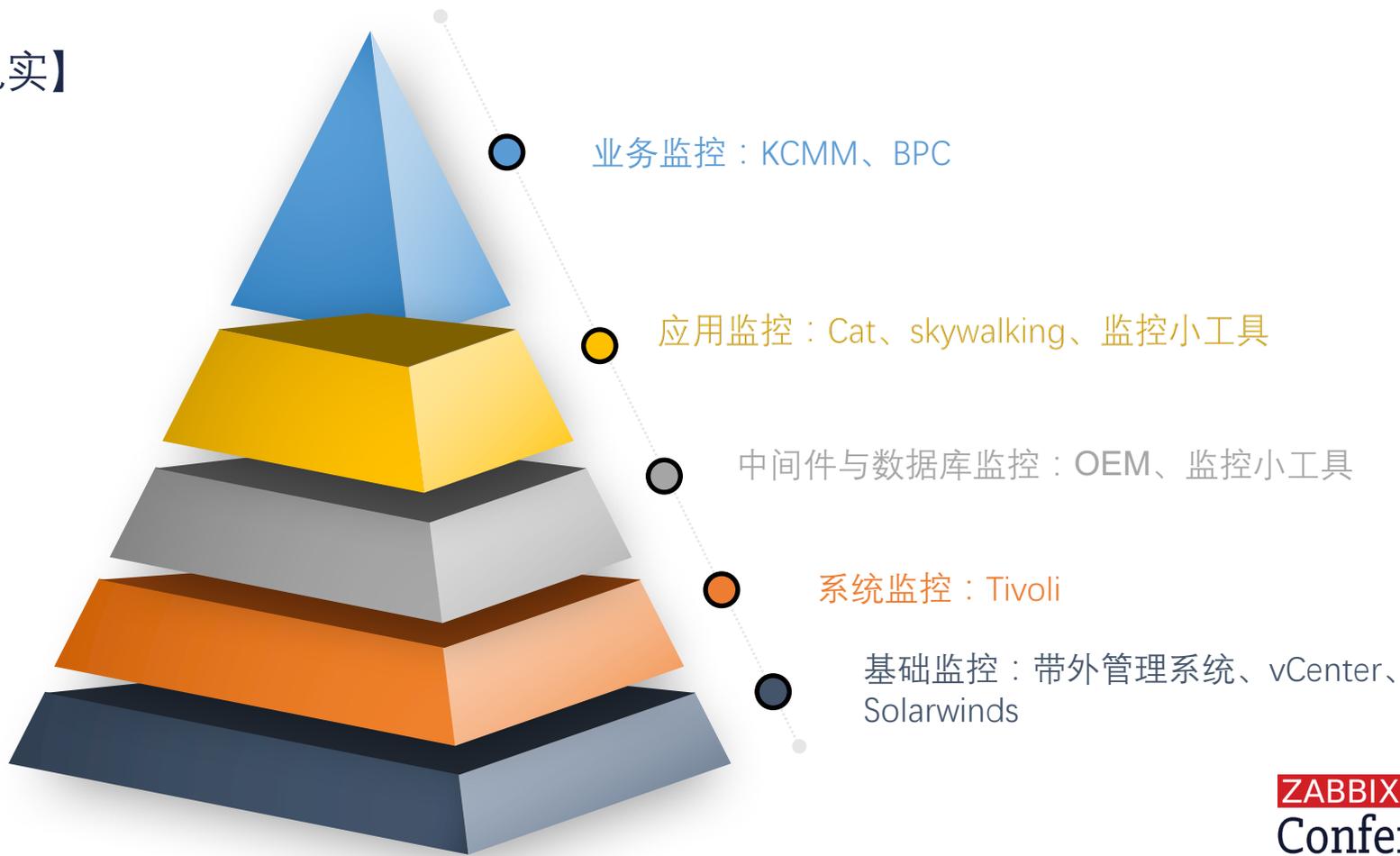
- 技术成熟的商用产品
- 集成性、可扩展性较强
- 支持：
 - 主机系统的监控
 - 数据库的监控
 - 应用的监控
 - 网络的监控
 - ...



【理想】支持各层级的监控

监控平台（阶段一）

【现实】



监控平台（演进一）

分析

- 各专业监控工具变化快，提升监控深度
- 架构厚重，无法适应快速发展的IT环境
- 重基础架构，轻业务应用
- 异常告警强，性能分析弱

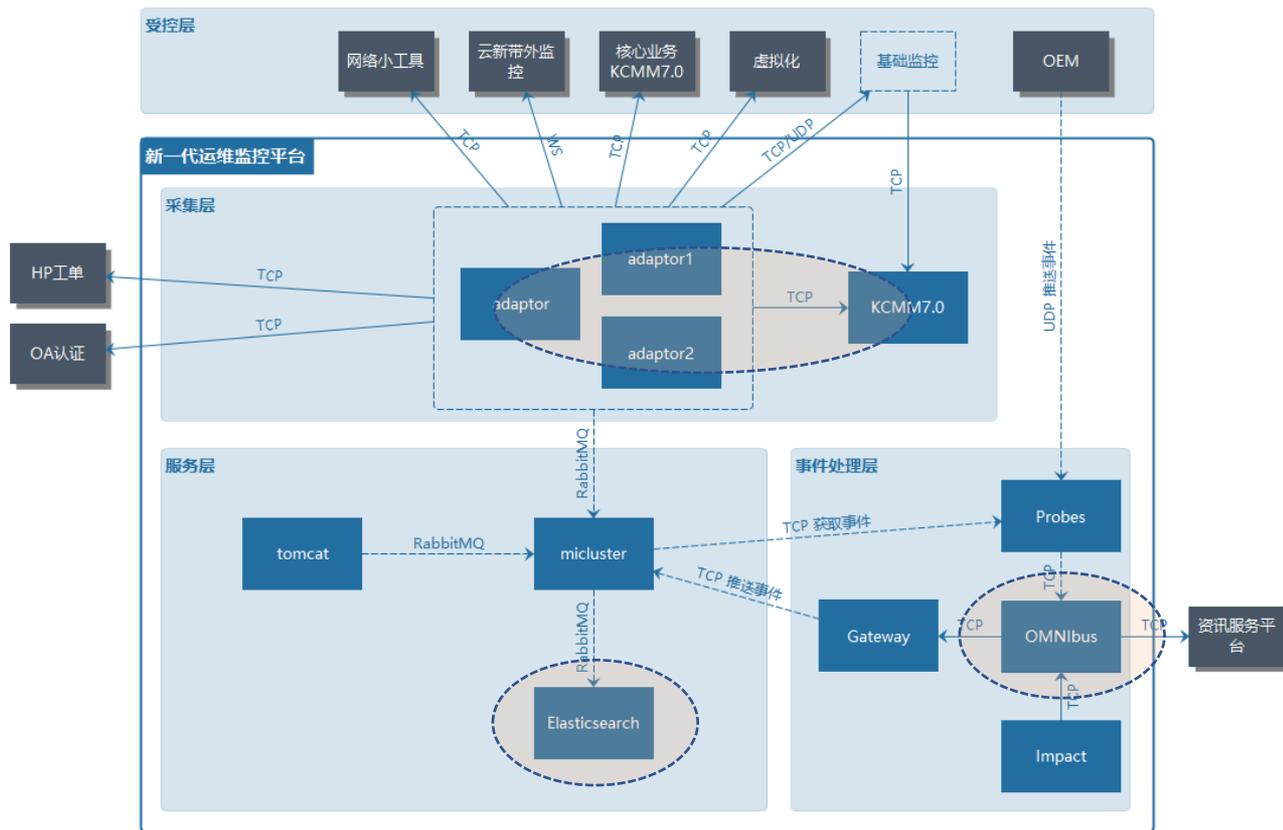


解决思路

- 新平台以模块化方式构架，模块间松耦合
- 保留核心的事件处理引擎，与新旧专业监控工具进行集成
- 升级UI，全面使用HTML5，提供更具现代感的仪表盘和大屏展示
- 以业务监控工具集成、集中日志分析两个方向逐步提高业务应用监控的比重

监控平台（阶段二）

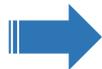
- 采集：adaptor、KCMM
- 事件处理：OMNibus
- 存储：Elasticsearch
- 集成：
 - 带外监控
 - vCenter
 - OEM
 - 网络工具
 - 自研工具
 - 扩展支持更多第三方工具



监控平台（演进二）

分析

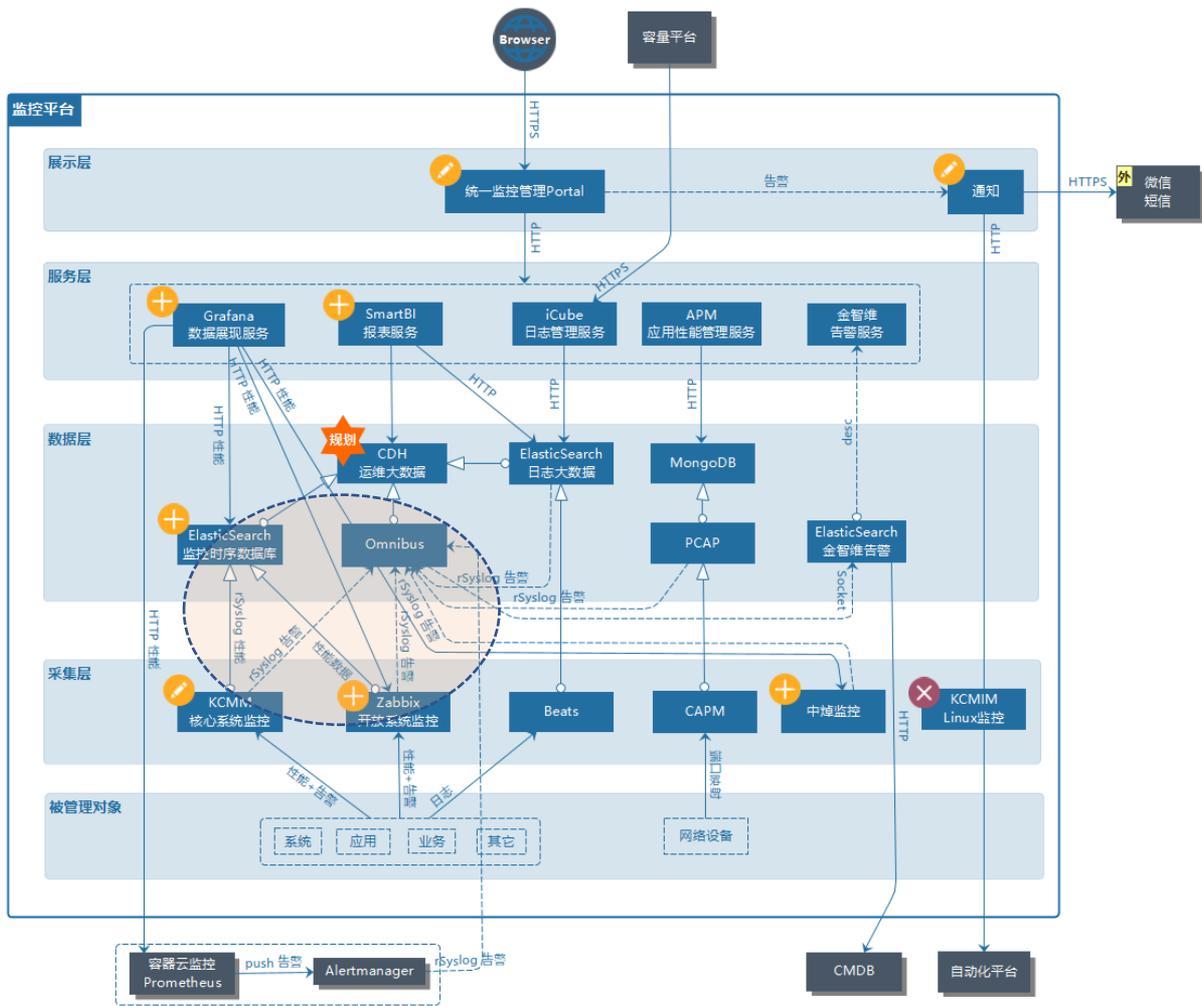
- 与运维场景没有紧密结合
- 告警和性能关联性不强
- 监控策略定义固定模板，复杂的监控场景需要二次开发
- 性能展现内容自助性不高
- 缺乏统一的资源配置信息



解决思路

- 建立统一监控Portal，形成运维门户
- 从用户的角度出发，将监控做为运维工作的抓手
- 以告警为切入点，监控与日志大数据、性能分析、拓扑可视化联动
- 实用原则，引入多个开源模块，快速提供自助化服务
- 资源配置信息从CMDB同步

监控平台 (阶段三)

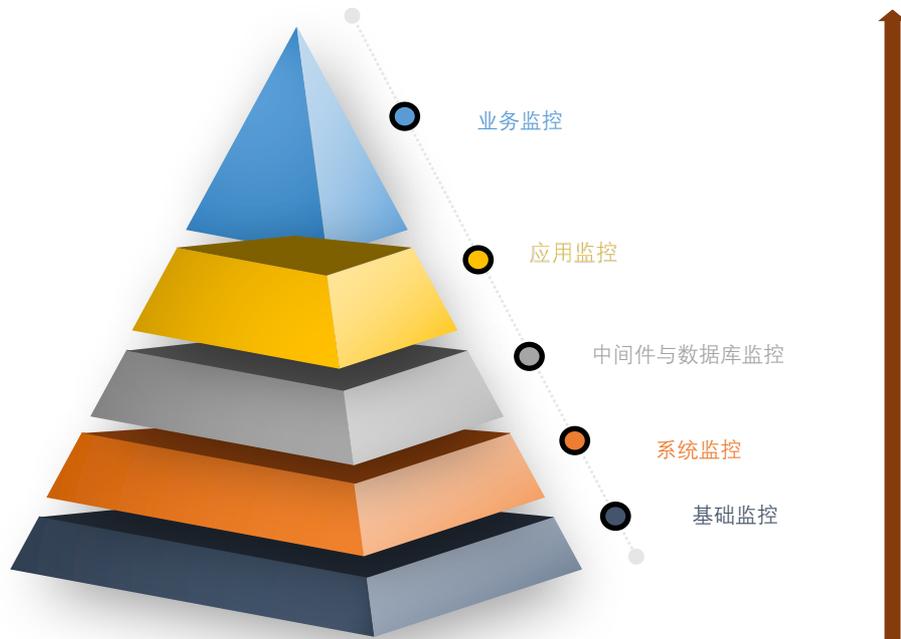


- 展示
 - 统一Portal
 - Grafana
- 采集
 - Zabbix
 - KCMIM
 - Prometheus
- 事件处理：OMNIBUS
- 存储
 - Elasticsearch
 - Hadoop
- 集成
 - 日志大数据
 - 拓扑可视化
 - 业务监控工具
 - ...
- 协同
 - 自动化平台
 - CMDB **ZABBIX** 2020

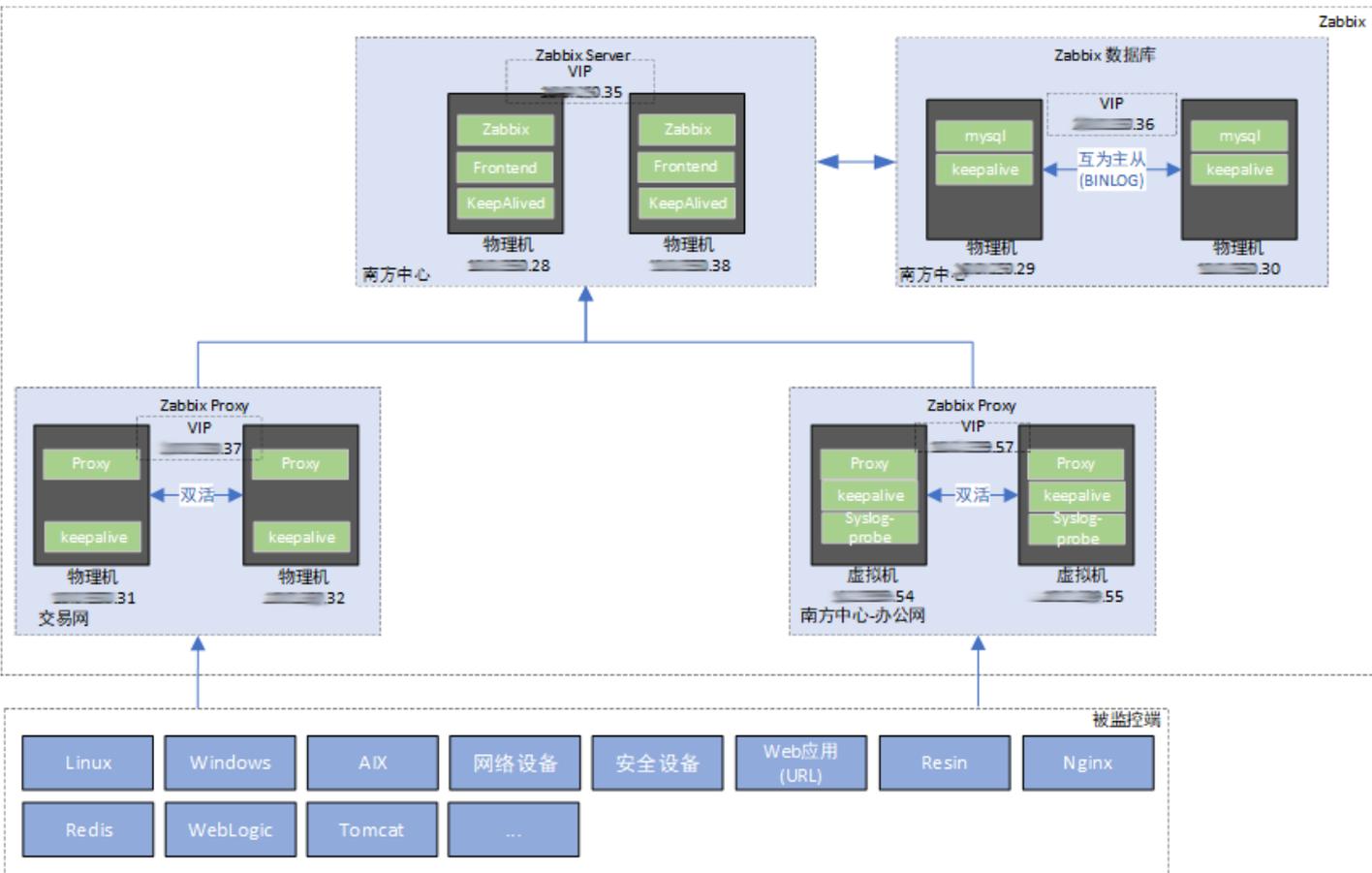
监控平台（阶段三）

Zabbix作用

- 用于通用领域的监控，从基础监控到业务监控各层级的监控
- 扩展兼容性强，适合统一监控集成，将分步骤替换零星的监控工具
 - 增量：统一Zabbix监控
 - 存量：逐步迁移
- 监控模板丰富，监控需求可以快速实现
 - 安全设备监控：IPS、WAF
 - 中间件监控：Nginx、Redis、Tomcat、Resin



监控平台（阶段三）

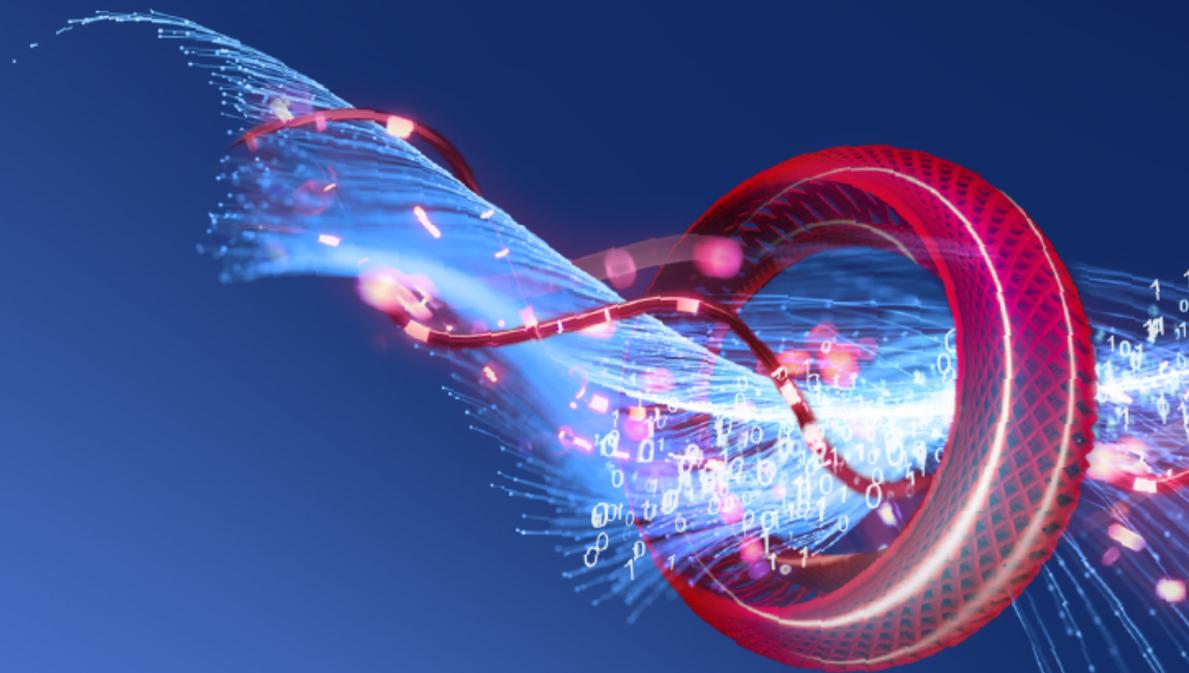


Zabbix架构

- 高可用架构设计
- 分布式组件部署
- 数据库容灾要求

03

实现



监控平台展示

运维工作的抓手：

- 监控首页
 - 默认
 - 自定义
- 活动告警



The active alerts page shows a list of alerts with the following columns: 告警ID, 告警时间, 级别, 资源名称, IP, 告警内容, 业务系统, 响应, 责任人, 来源.

告警ID	告警时间	级别	资源名称	IP	告警内容	业务系统	响应	责任人	来源
224780	2020-09-03 10:47:28	主要	NMS-SZV-JY18	10.7	[OS Windows] NMS-SZV-JY18 服务 Service 'TrustedInsta...	手机证券系统			Zabbix平台
224689	2020-09-03 10:22:46	主要	SIQZ-DG-MID0...	10.0	[OS Windows] SIQZ-DG-MID055 服务 Service 'TrustedIn...	手机证券系统			Zabbix平台
224349	2020-09-03 10:03:06	警告	sjzq-dg-swfb174	10.0	【254功能业务数据 displayonline_config.ini】SIQZ-SZ-...	手机证券系统			中储管理系统
224348	2020-09-03 10:02:57	警告	sjzq-dg-swfb174	10.0	【接入每个IP每秒处理数监控 sc_ip_dealcount_config.ini...	手机证券系统			中储管理系统
224347	2020-09-03 10:02:56	警告	sjzq-dg-swfb174	10.0	【功能导入库: sc_action_info_config.ini】SIQZ-SZ-SW11...	手机证券系统			中储管理系统
224592	2020-09-03 10:02:24	警告	sjzq-dg-swfb174	10.0	【服务监控脚本: sc_dbmiddleware_config.ini】SIQZ-SZ-...	手机证券系统			中储管理系统
224538	2020-09-03 09:48:28	次要	SIQZ-DX-JY43	10.0	[OS Windows] 10.130.43 物理磁盘平均每秒处理列小...	手机证券系统			Zabbix平台
224343	2020-09-03 09:31:38	警告	sjzq-dg-swfb174	10.0	【服务监控脚本: sc_dbmiddleware_config.ini】SIQZ-SZ-...	手机证券系统			中储管理系统
224345	2020-09-03 09:00:15	主要	SIQZ-DGV-JY148	10.0	[OS Windows] SIQZ-DGV-JY148 服务 Service 'wuaserv...	手机证券系统			Zabbix平台
195543	2020-09-03 09:00:06	警告	SIQZ-DG-HQ36	10.0	SIQZ-DG-HQ36,7779.股票【300088】的行情数据解析失...	手机证券系统			中储管理系统
224342	2020-09-03 09:00:02	警告	SIQZ-DG-HQ52	10.0	SIQZ-DG-HQ52,7779.股票【300088】的行情数据解析失...	手机证券系统			中储管理系统
224341	2020-09-03 09:00:01	警告	SIQZ-DG-HQ53	10.0	SIQZ-DG-HQ53,7779.股票【600570】的行情数据解析失...	手机证券系统			中储管理系统
224019	2020-09-03 08:01:49	主要	SIQZ-DGV-JY149	10.0	[OS Windows] SIQZ-DGV-JY149 服务 Service 'wuaserv...	手机证券系统			Zabbix平台
224007	2020-09-03 08:01:00	次要	SIQZ-DX-JY43	10.7	[OS Windows] SIQZ-DX-JY43 物理磁盘平均每秒处理列...	手机证券系统			Zabbix平台



监控平台展示

运维场景：

以告警为切入点

- 查看日志
- 查看性能
- 查看拓扑

The screenshot displays the Zabbix monitoring platform interface. On the left is a dark sidebar with navigation options: 安信证券 (Anxin Securities), 首页 (Home), 管理首页 (Management Home), 运维首页 (Operations Home), 告警中心 (Alert Center), 性能中心 (Performance Center), 管理中心 (Management Center), 日志中心 (Log Center), 综合报表 (Comprehensive Reports), and 系统管理 (System Management). The main area shows a dashboard with several widgets: 活动告警 (Active Alerts), 操作系统 (Operating System), 数据库 (Database), 业务系统 (Business System), and 网络监控 (Network Monitoring). Below these is a table of alerts. The selected alert (ID 224606) is highlighted in blue, and a red box highlights the '查看日志' (View Log), '查看性能' (View Performance), and '查看拓扑' (View Topology) links in the alert details. The alert content is: SQLException告警20200903 10:12:31 [TID:2782.64737.159909915133241...]. The table columns include: 告警ID, 告警时间, 级别, 资源名称, IP, 告警内容, 业务系统, 响应, 责任人, and 来源.

告警ID	告警时间	级别	资源名称	IP	告警内容	业务系统	响应	责任人	来源
224632	2020-10-12:37	严重	YZT-dgv-APP26	10.0.0.0	SQLException告警20200903 10:12:31 [TID:2782.64737.159909915133241...	聚安一站通系统			日志平台
224606	2020-10-06:07	严重	wsjq-dg-mid31	10.0.0.0	告警日志 [SEND][101][Client]116.16.30.111 89EDDF81002 89DF1...	安翼网上交易...			日志平台
224349	2020-10-03:06	警告	sjzq-dg-swf174	10.0.0.0	告警性能 [displayonline_config.ini] SJZQ-SZ-SWJ174.displayo...	手机证券系统			中坤管理系统
224348	2020-10-02:57	警告	sjzq-dg-swf174	10.0.0.0	告警性能 [安翼部署架构图 onfig.ini] SJZQ-SZ-SWJ...	手机证券系统			中坤管理系统
224347	2020-10-02:56	警告	sjzq-dg-swf174	10.0.0.0	告警性能 [功能号入库: sc_action_info_config.ini] SJZQ-SZ-SWJ174:1497.服务异...	手机证券系统			中坤管理系统
224592	2020-10-02:24	警告	sjzq-dg-swf174	10.0.0.0	【服务器监控脚本: sc_dbmiddleware_config.ini】 SJZQ-SZ-SWJ174.dbmid...	手机证券系统			中坤管理系统
224538	2020-09-46:28	次要	SJZQ-DX-JY43	10.1.1.1	[OS Windows] 10.1.30.43 物理磁盘平均每秒处理队列小于2	手机证券系统			Zabbix平台
224343	2020-09-31:38	警告	sjzq-dg-swf174	10.0.0.0	【服务器监控脚本: sc_dbmiddleware_config.ini】 SJZQ-SZ-SWJ174.dbmid...	手机证券系统			中坤管理系统
224345	2020-09-30:05	主要	SJZQ-DGV-JY148	10.0.0.0	[OS Windows] SJZQ-DGV-JY148 服务 Service 'wuaserv' (Windows Updat...	手机证券系统			Zabbix平台
195543	2020-09-30:06	警告	SJZQ-DG-HQ36	10.0.0.0	SJZQ-DG-HQ36,7779,股票【300088】的行情数据解析失败	手机证券系统			中坤管理系统
224342	2020-09-30:02	警告	SJZQ-DG-HQ52	10.0.0.0	SJZQ-DG-HQ52,7779,股票【300088】的行情数据解析失败	手机证券系统			中坤管理系统
224341	2020-09-30:01	警告	SJZQ-DG-HQ53	10.0.0.0	SJZQ-DG-HQ53,7779,股票【600570】的行情数据解析失败	手机证券系统			中坤管理系统
224324	2020-08-53:52	次要	O32-DGV-JY4	10.0.0.0	金证PBoem到期提示超过阈值,数值为20200903系统OEM到期提醒: #012 [...]	恒生投资管理...			KCMM核心
224306	2020-08-51:05	严重	YZT-dgv-APP26	10.0.0.0	访问数据库异常2020-09-03T00:50:55.655Z	聚安一站通系统			日志平台

告警ID	告警时间	关闭时间	级别	报警名称	IP	告警内容	业务系统	责任人	关联人	来源
225340	2020-09-03 13:31:53	2020-09-03 13:35:55	高危	WSJY-ZJM-20	10.1.	[OS Windows] 10.1.18.23 物理磁盘C:\中程序大小>0.05	交易		AutoRestore	Zabbix平台
225348	2020-09-03 13:31:24	2020-09-03 13:35:25	主要	WSJY-DGV-TD...	10.0.	[OS Windows] WSJY-DGV-TDXTP 服务 Service "TrustedInstaller" (Windows Modules Installer...	交易		AutoRestore	Zabbix平台
225344	2020-09-03 13:31:03	2020-09-03 13:35:00	主要	WSJY-DGV-TD...	10.0.	[OS Windows] WSJY-DGV-TDXT2 服务 Service "TrustedInstaller" (Windows Modules Installer...	交易		AutoRestore	Zabbix平台
225341	2020-09-03 13:30:45	2020-09-03 13:34:50	主要	WSJY-G-TC81		[OS Windows] WSJY-G-TC81 服务 Service "TrustedInstaller" (Windows Modules Installer) 未启动。	交易		AutoRestore	Zabbix平台

问题分析

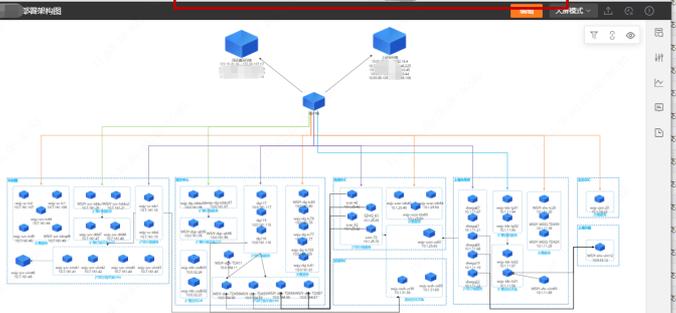
```

时间          原始日志
-----
2020-09-03T13:43:25.062+0800
{
  "dimensions": {
    "hostname": "wsjy-dg-tc81",
    "appprogramname": "微软服务器命令处理TC50",
    "appsystem": "tdpcc"
  },
  "measure": {
    "normalfields": {
      "timestamp": "2020-09-03T05:43:31.731Z",
      "nodeTime": "2020-09-03T13:43:33.480+0800",
      "collectTime": "2020-09-03T05:43:25.062Z",
      "collector": "10.0.161.81"
    }
  }
}

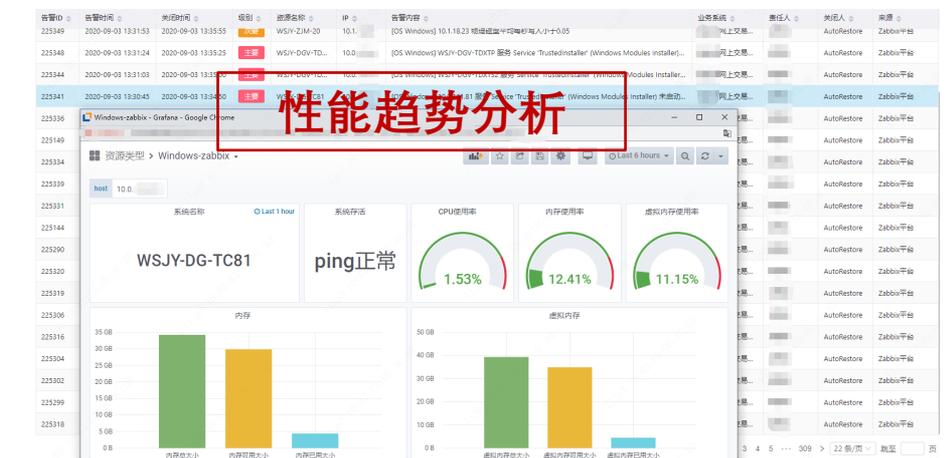
2020-09-03T13:43:19.007[00001E50]-Recv---[ANSWERS:[ANS_MSG_HDR:
["MSG_CODE":"0","MSG_TEXT":"查询该用户的工作任务成功","MSG_LEVEL":"RES
ULT_NUM":"2","MSG_ID":"","PACKAGE_FLAG":"0","DATA_ROWS":"0","BPM_ID
WS":"0","RUN_TIMES":"9","MSG_TRACE":"","ANS_COMM_DATA":["BPM_DA
TA":{"CONFIG":{}}]]]
  
```

告警ID	告警时间	关闭时间	级别	报警名称	IP	告警内容	业务系统	责任人	关联人	来源
225340	2020-09-03 13:31:53	2020-09-03 13:35:55	高危	WSJY-ZJM-20	10.1.	[OS Windows] 10.1.18.23 物理磁盘C:\中程序大小>0.05	交易		AutoRestore	Zabbix平台
225348	2020-09-03 13:31:24	2020-09-03 13:35:25	主要	WSJY-DGV-TD...	10.0.	[OS Windows] WSJY-DGV-TDXTP 服务 Service "TrustedInstaller" (Windows Modules Installer...	交易		AutoRestore	Zabbix平台
225344	2020-09-03 13:31:03	2020-09-03 13:35:00	主要	WSJY-DGV-TD...	10.0.	[OS Windows] WSJY-DGV-TDXT2 服务 Service "TrustedInstaller" (Windows Modules Installer...	交易		AutoRestore	Zabbix平台
225341	2020-09-03 13:30:45	2020-09-03 13:34:50	主要	WSJY-G-TC81		[OS Windows] WSJY-G-TC81 服务 Service "TrustedInstaller" (Windows Modules Installer) 未启动。	交易		AutoRestore	Zabbix平台

关联影响分析



系统巡检



性能趋势分析

Global view

All dashboards / Global view

System information

Parameter	Value	Details
Zabbix server is running	Yes	10051
Number of hosts (enabled/disabled/templates)	414	288 / 0 / 126
Number of items (enabled/disabled/not supported)	106846	93972 / 225 / 12649
Number of triggers (enabled/disabled (problem/vok))	25667	25495 / 72 [1231 / 24284]
Number of users (online)	3	1
Required server performance, new values per second		

Problems by severity

Host group	Disaster	High	Average	Warning	Information	Not classified
Celuetuoguan/VOS		20	40			
Discovered hosts	7	390	817			
Linux	6	22	5			
Mcafee IPS Group				6		
MID/Nginx		12				
MID/Redis	1					
MID/Tomcat	4		4			

Local

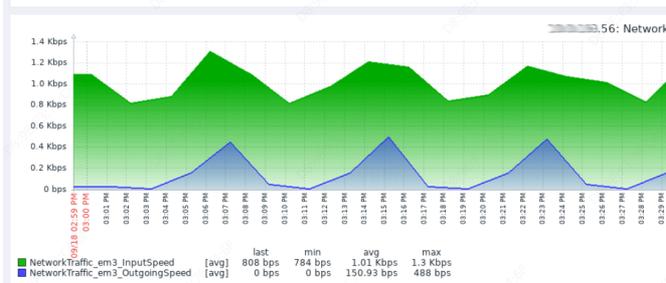
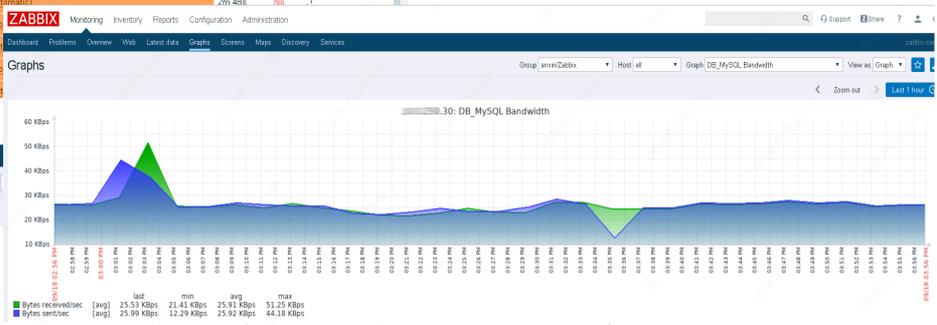
Zabbix原生监控数据展示, Dashboard和Graph

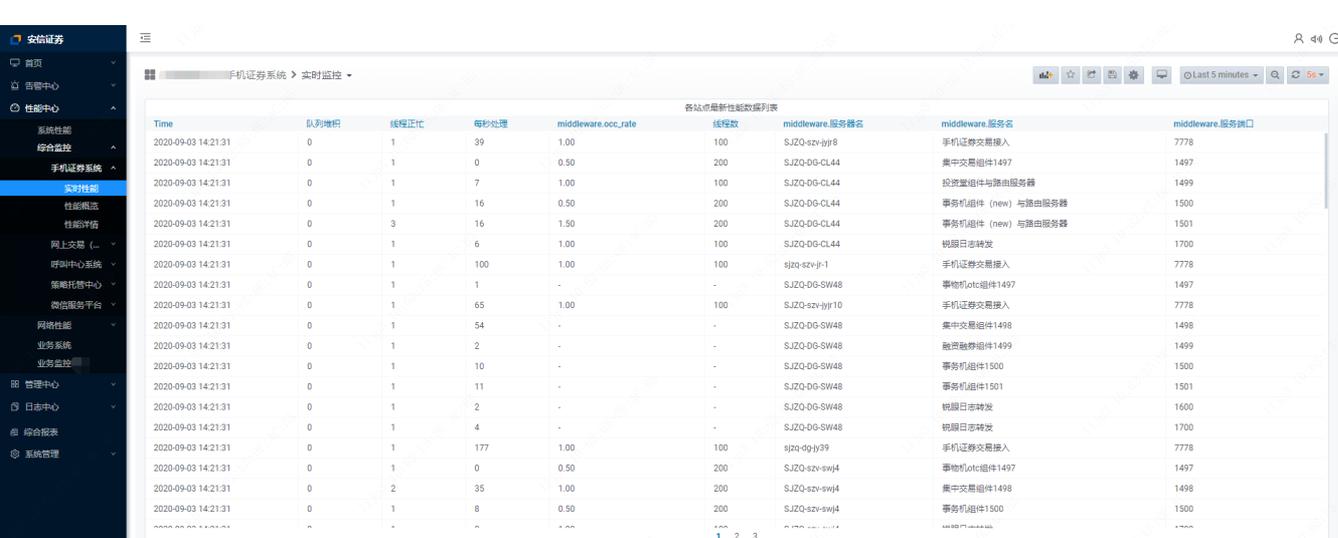
Problems

Time	Info	Host	Problem - Severity	Duration	Ack	Actions	Tags
03:53:27 PM		115	[OS Linux] 115 swap的总交换大小警告: 大于10%	18s	No	1	
03:52:56 PM		24	[OS Windows] 24 服务 Service TrustedInstaller (Windows Modules Installer) 未启动 (startup type automatic)	50s	No	1	
03:52:49 PM		23	[OS Windows] 23 物理磁盘平均每秒写入小于0.05	56s	No	1	
03:52:34 PM		9	[OS Windows] 9 19 服务 Service TrustedInstaller (Windows Modules Installer) 未启动 (startup type automatic)	1m 11s	No	1	
03:51:19 PM		80	[OS Windows] 80 30 服务 Service TrustedInstaller (Windows Modules Installer) 未启动 (startup type automatic)	2m 26s	No	1	
03:51:14 PM		78	[OS Windows] 78 3 服务 Service TrustedInstaller (Windows Modules Installer) 未启动 (startup type automatic)	2m 31s	No	1	
03:50:57 PM		79	[OS Windows] 79 3 服务 Service TrustedInstaller (Windows Modules Installer) 未启动 (startup type automatic)	2m 48s	No	1	
03:50:51 PM		36	[OS Windows] 36 服务 Service TrustedInstaller (Windows Modules Installer) 未启动 (startup type automatic)				
03:50:41 PM		81	[OS Windows] 81 19 服务 Service TrustedInstaller (Windows Modules Installer) 未启动 (startup type automatic)				
03:47:27 PM		8	[OS Windows] 8 19 服务 Service TrustedInstaller (Windows Modules Installer) 未启动 (startup type automatic)				
03:38:43 PM		80	[OS Windows] 80 3 服务 Service TrustedInstaller (Windows Modules Installer) 未启动 (startup type automatic)				

Graphs

Group: Celuetuoguan/VOS | Host:





Zabbix + Grafana:

- 系统监控
- 中间件监控
- 应用监控
- 业务监控



04

展望



展望

安信证券“北斗”监控平台：

- 运维人员：通过监控了解系统状态，掌握系统实时容量情况，以及时发现系统异常，恢复业务连续性，或者提前预防故障，实施部署扩容工作
- 研发人员：通过监控发现系统各服务与应用组件的历史性能趋势，以便实施对应的架构和代码性能优化工作
- 业务人员：通过监控能掌握业务当前的运转情况，客户的实际体验情况如何，并基于相关信息展开针对性的营销活动

运维

传感器



研发

指南针



业务

小助手



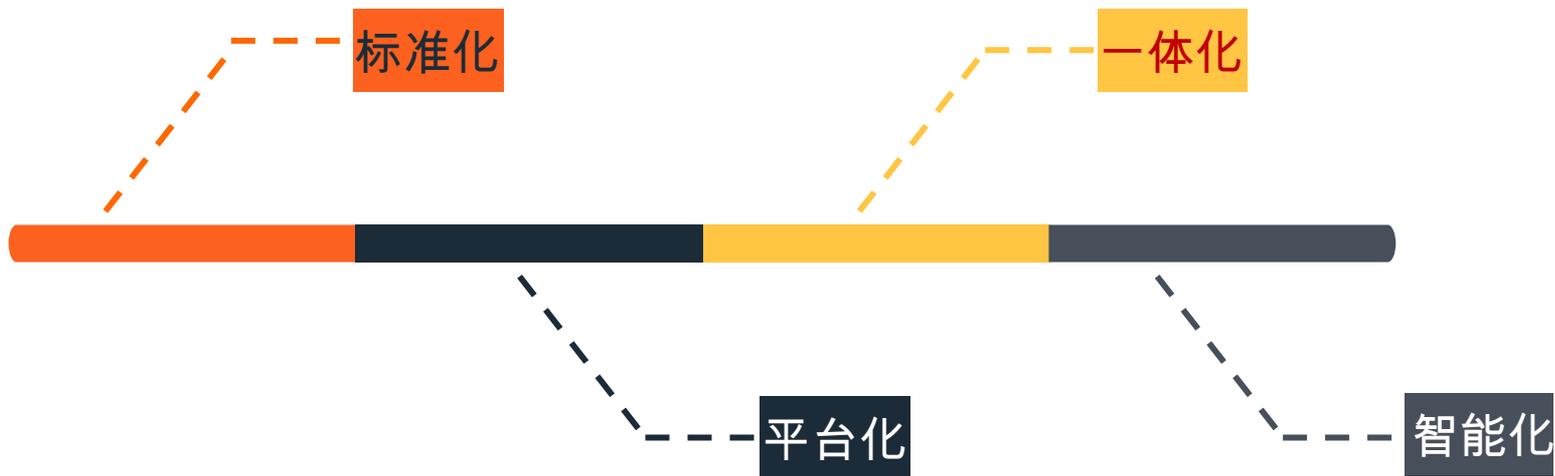
展望

● IT运维平台：“监”、“管”、“控”、“营”四位一体



展望

- 通过监控推进运维工作标准化
- 持续优化监控平台，提供更多自助式服务，为运维赋能
- 运维数据的价值落地与探索



联系我们

Contact us

Zabbix 中国致力于为国内用户提供培训、咨询、以及其他的专业技术支持。也为国内的用户搭建交流学习的平台。



138-1772-0274



china@zabbix.com



www.grandage.cn
www.zabbix.com/cn



上海市徐汇区虹梅路1905号



Zabbix开源社区



Zabbix中国



Zabbix_China



Zabbix_team



Zabbix 开源社区



加入技术交流群

ZABBIX 2020
Conference
CHINA

THANK YOU 😊

