

2024



SMARTEAGLE
慧鹰

自动化运维作业平台

——场景驱动，开创智能、高效运维自动化

常州慧鹰信息科技有限公司



1

关于慧鹰

2

产品介绍

3

场景案例

4

产品价值

目录

Contents

Part.

1

关于慧鹰

常州慧鹰信息科技有限公司是一家专业从事运维管理软件的研发、销售、咨询和服务的一体化高新技术软件企业，致力于为用户提供全面优质的运维产品及整体解决方案。



SMARTEAGLE
慧鹰

1. 关于慧鹰

公司定位

- 慧鹰充分了解目前运维行业的现状，通过不断的自我创新，倾力打造了一系列运维产品，包括：IT智能运维软件，IT服务管理平台，物联网监控平台，运维开发平台。目前产品广泛涉足于金融、医疗、政府、企业等多个行业。

公司团队

- 公司具有完备的销售团队，全国多点布局；
- 公司研发团队来自IBM、HP、ORACLE、腾讯等各大国内顶尖厂商；
- 公司具有一大批经验丰富的运维工程师，致力于帮用户解决日常运维问题。

公司理念

- 公司秉承“以用户需求为导向，以用户满意为宗旨”的经营理念，积极自主研发创新，极力构造良好运维生态，做到“人人都是运维工程师”！



Part.

2

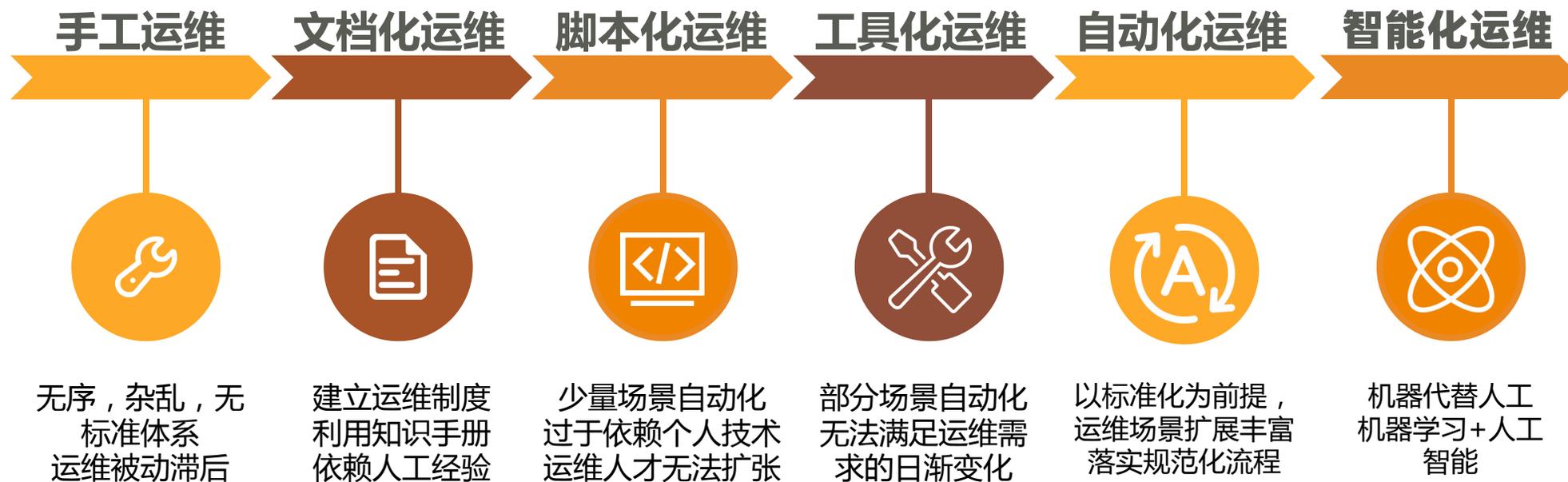
产品介绍

慧鹰SAOP (SmartEagle Automated Operation Platform) 是常州慧鹰最新研发的一代高效自动化运维平台。以ITIL理念为核心指导，通过需求场景化驱动，打造智能运维操作中心，实现运维的闭环管理、精益管理、战略管理。



SMARTEAGLE
慧鹰

2.1 运维的发展各个阶段



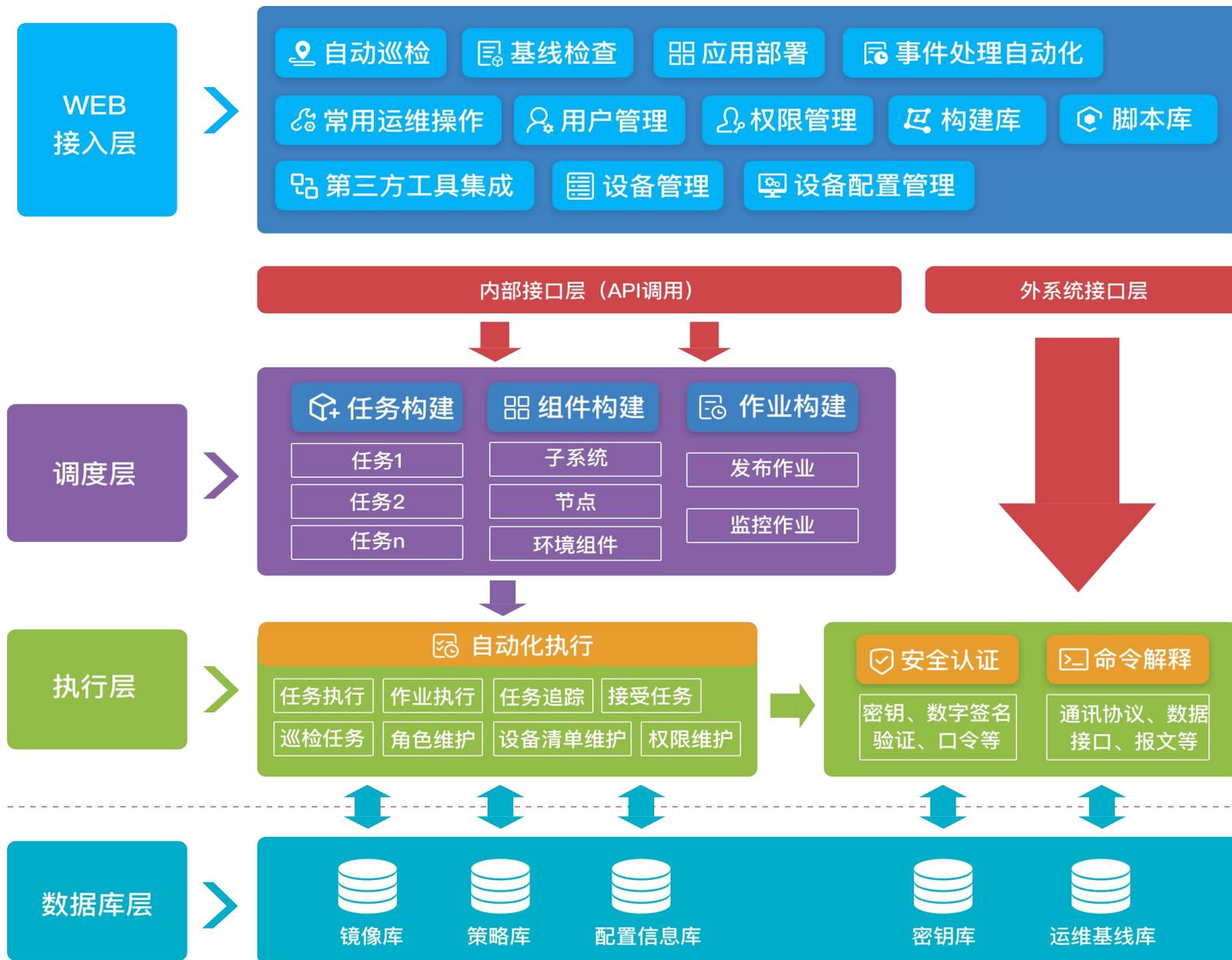
2.2 为什么需要自动化



2.2 为什么需要自动化



2.3 产品介绍 — 功能架构



2.3 产品介绍 — 集成架构



2.4 产品介绍 — 功能介绍

自动化巡检

收集生产环境中设备的日常运行状态数据并根据预设巡检策略分析其健康情况

合规基线核查

基于运维基线，自动执行合规检查，并根据检查结果给出合规整改建议或执行强制合规

应用部署管理

实现应用投产阶段的裸机安装及投产后的软件和补丁分发管理
应用自动化部署配置，建立标准化的安装介质库和部署策略库



事件处理自动化

结合企业流程，自动化执行运维事件处理作业。通过自动化的调度提升效率并减少人工失误，保证业务的正常运行

维护操作自动化

固化例行维护操作，通过一键启停的应用控制，简化人工操作并有效利用维护期窗口以及实现快速的灾备切换

配置收集自动化

自动收集生产环境操作系统、数据库、中间件和网络设备的配置信息，自动跟踪配置变更并向运维人员反馈

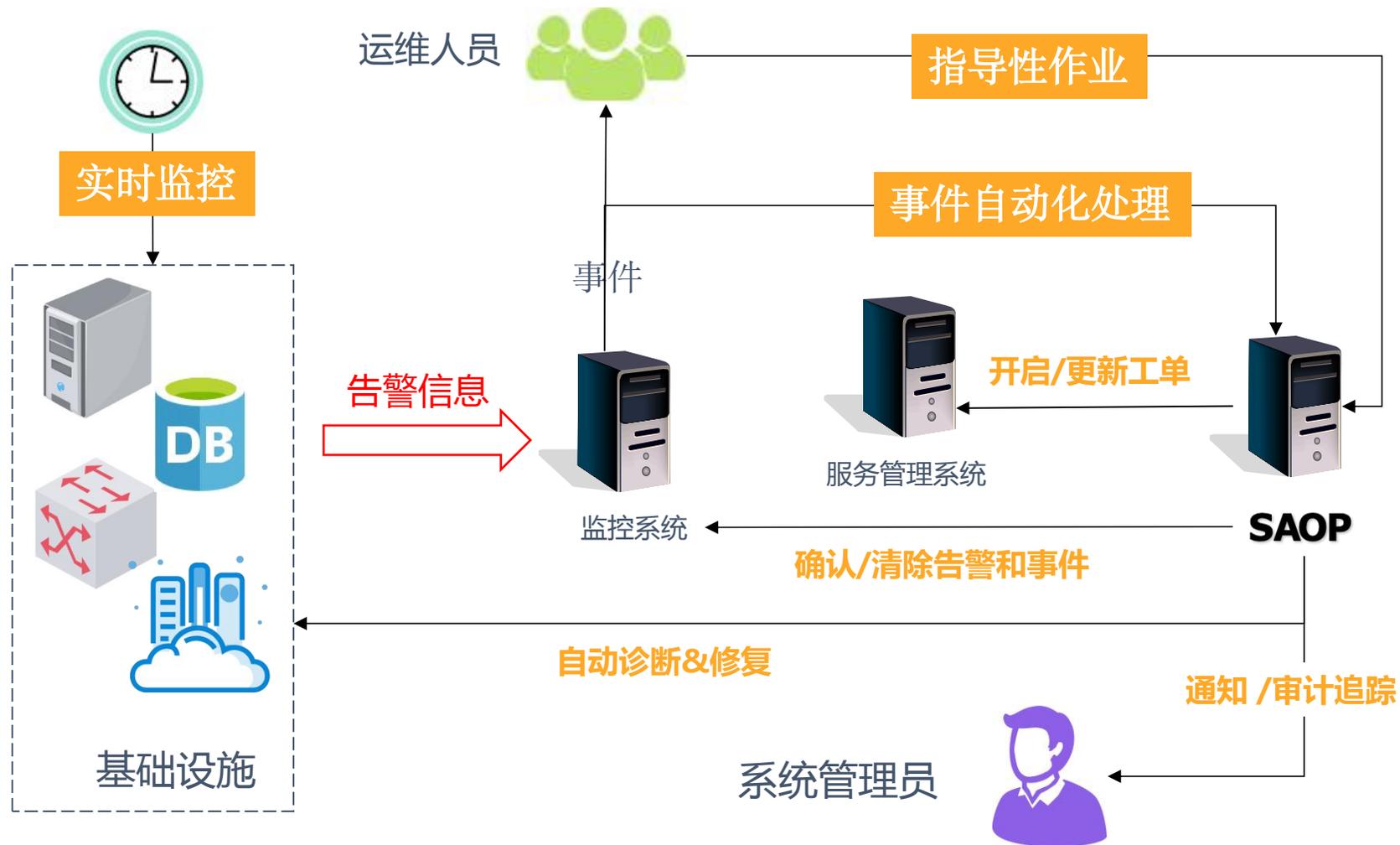
2.4.1 功能介绍-事件处理自动化

日常运维事件的处理流程自动化:

- 网络连通性问题
- 网络端口流量异常
- 性能数据超限 (CPU、内存)
- 进程/服务挂起
- 存储容量瓶颈
- 数据库问题
- 应用系统自动故障排除

日常运维变更操作自动化:

- 与CMDB集成, 实现配置变更操作
 - 系统口令的定时更新
 - 基础设施健康检查与自动修复
 - 合规基线检查并且自动修正
- 忙时额外资源自动分配, 负载均衡



2.4.1

事件处理自动化-作业编排

<input type="checkbox"/>	名称	标签	资产数目	执行周期	执行时间	执行状态
<input type="checkbox"/>	Linux基线检查作业	linux centos 基线	1	手动	20秒	未运行
<input type="checkbox"/>	nginx服务健康度检查	信息收集	1	手动	32秒	未运行
<input type="checkbox"/>	Linux进程检测及修复作业	进程检测 进程修复 事件处理	2	手动	1分07秒	未运行
<input type="checkbox"/>	网络端口异常流量检测通知	流量检测 事件通知	3	手动	25秒	未运行
<input type="checkbox"/>	网络连通性问题通知	连通性 事件通知	3	手动	23秒	未运行
<input type="checkbox"/>	性能数据超限 (CPU、内存) 停止进程作业	性能 CPU 内存 停止进程	3	手动	16秒	未运行
<input type="checkbox"/>	进程/服务挂起作业	服务 进程 挂起	2	手动	33秒	未运行
<input type="checkbox"/>	存储容量瓶颈事件通知作业	存储容量 事件通知	1	手动	9秒	未运行
<input type="checkbox"/>	监控系统自动故障排除作业	故障排除 应用系统	3	手动	46秒	未运行

运维作业 / 作业编辑

* 作业名称: Linux进程检测及修复作业

作业标签: 进程检测,进程修复,事件处理

所属分组: 事件处理

* 执行周期: 手动 单次 日 周 月 年

选择资产

全部资产 0/1

cemm 演示机

已选择的资产 0/2

k8s-master1

组件平台

过程编排

<input type="checkbox"/>	步骤	模块/作业名称	过程类型	操作
<input type="checkbox"/>	1	创建工作目录	模块	删除
<input type="checkbox"/>	2	分发Linux进程检测脚本	模块	删除
<input type="checkbox"/>	3	分发Linux进程异常修复脚本	模块	删除
<input type="checkbox"/>	4	执行进程健康检查脚本	模块	删除
<input type="checkbox"/>	5	进程健康检查结果分析	模块	删除
<input type="checkbox"/>	6	执行异常进程问题修复脚本	模块	删除
<input type="checkbox"/>	7	进程健康性检查复查	模块	删除

+

事件处理自动化-收益分析

- A 最小化用户干预，自动修复日常运维故障
- B 自动执行健康检查、合规检查等诊断任务
- C 减少手工操作，增强操作跟踪与合规审计能力
- D 自动处理事件工单，落实ITIL最佳实践



15+

内置15个自动化作业，用以处理运维告警事件，自定义扩展作业



500+

某行业客户生产环境，每周处理500次以上的自动化作业任务



70%

一年的数据统计，自动化处理70%的基础设施告警



80%

运维故障平均修复时间（MTTR）提升了80%

2.4.2 功能介绍-自动化巡检

巡检任务详情

* 名称: 数据中心机房巡检任务 10/255

巡检方式: 自动巡检

周期类型: 每天 每周 每月 自定义

* 周期配置: 周三 1 点 0 分
周日 2 点 0 分

收件人: cgy sdw

描述:

审核人: 请选择审核人

状态:

[更新](#) [删除](#) [返回](#)

[+ 新增巡检任务](#)

- 数据中心机房巡检任务
- 规则数: 5
- 方式: 手动
- 类型: 每周
- 状态: 已启用

巡检规则详情

* 任务: 数据中心机房巡检任务

* 名称: 服务器异常巡检 7/255

等级: 普通 重要

* 对象类型: Windows

对象范围: 所有 部分

* 对象列表:

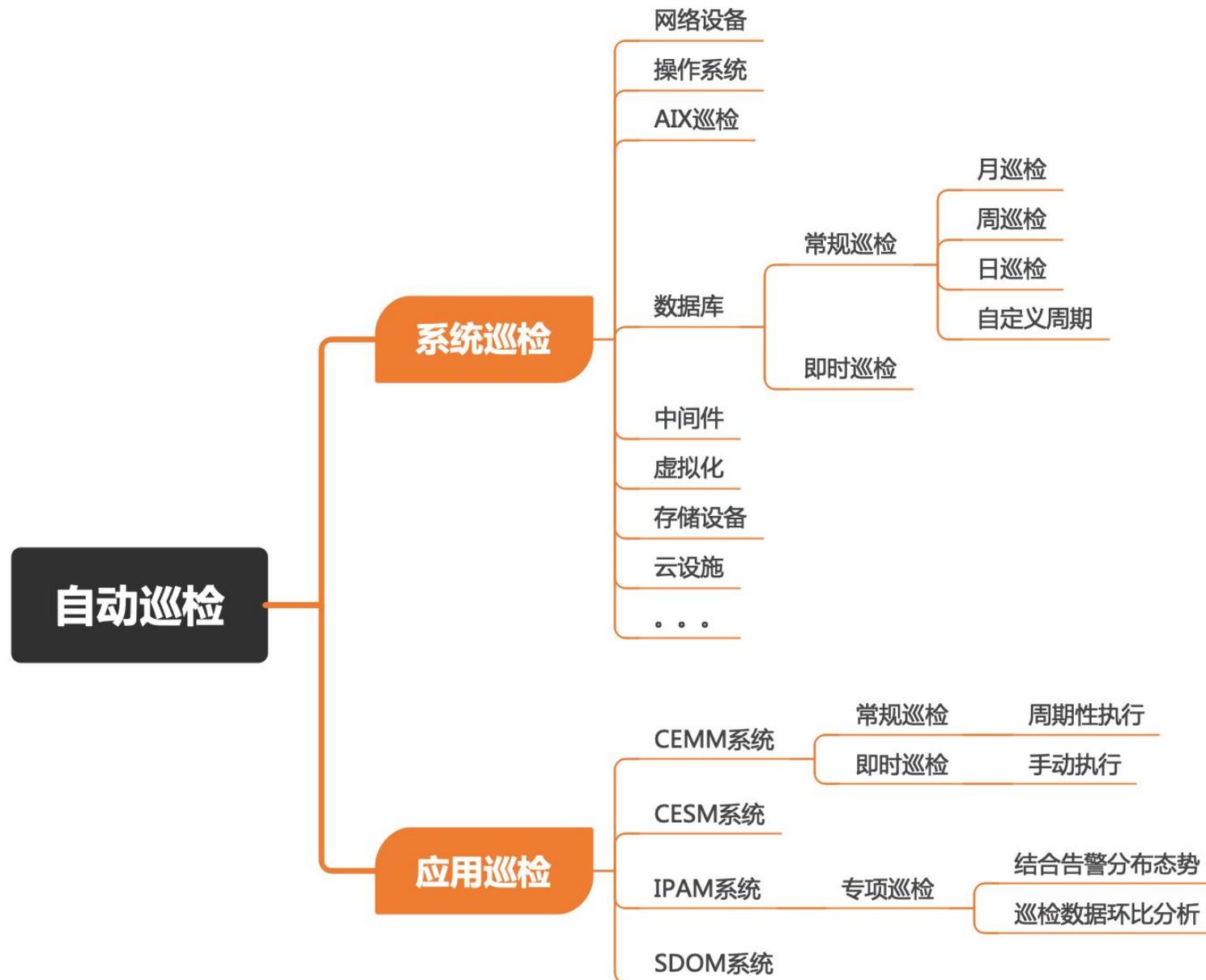
名称	等级	对象数	指标数	对比规则
服务器CPU负载异常巡检	普通	1	1	解析巡检规则异常范围失败
服务器内存负载异常巡检	普通	1	1	解析巡检规则异常范围失败
服务器磁盘使用率异常巡检	普通	1	1	解析巡检规则异常范围失败
网络设备CPU负载异常巡检	普通	1	1	解析巡检规则异常范围失败
网络设备内存负载异常巡检	普通	1	1	解析巡检规则异常范围失败

共 5 条 20条/页 < 1 > 前往 1 页

0/255

✔ 巡检模板、巡检规则、巡检指标一体化设计

2.4.2 自动化巡检-巡检任务树



立即巡检

巡检信息

巡检任务: 安全设备巡检
 开始时间: 2020-12-01 11:10:00
 上次巡检时间: 2020-11-21 15:30:30
 结束时间:

巡检过程信息

- SIEM服务器: 18 高危操作数, 电源状态
- 导流设备: 46% 内存使用率, 端口状态
- IPS系统服务器: 00% 丢包率, 0% 包转发率
- WAF服务器: 65% CPU使用率, 48% 内存使用率
- AD系统服务器: 服务状态, 18 登录失败次数

巡检看板

巡检报表 报表日期: 2020年4月15日

巡检信息

巡检任务: 机房巡检 巡检历时: 15秒
 巡检时间: 2020-04-15 10:58:02 上次巡检时间: 2020-04-14 09:25:16

巡检统计

健康度: 90分 巡检对象数: 25 异常对象数: 2
 巡检指标数: 120 异常指标数: 12

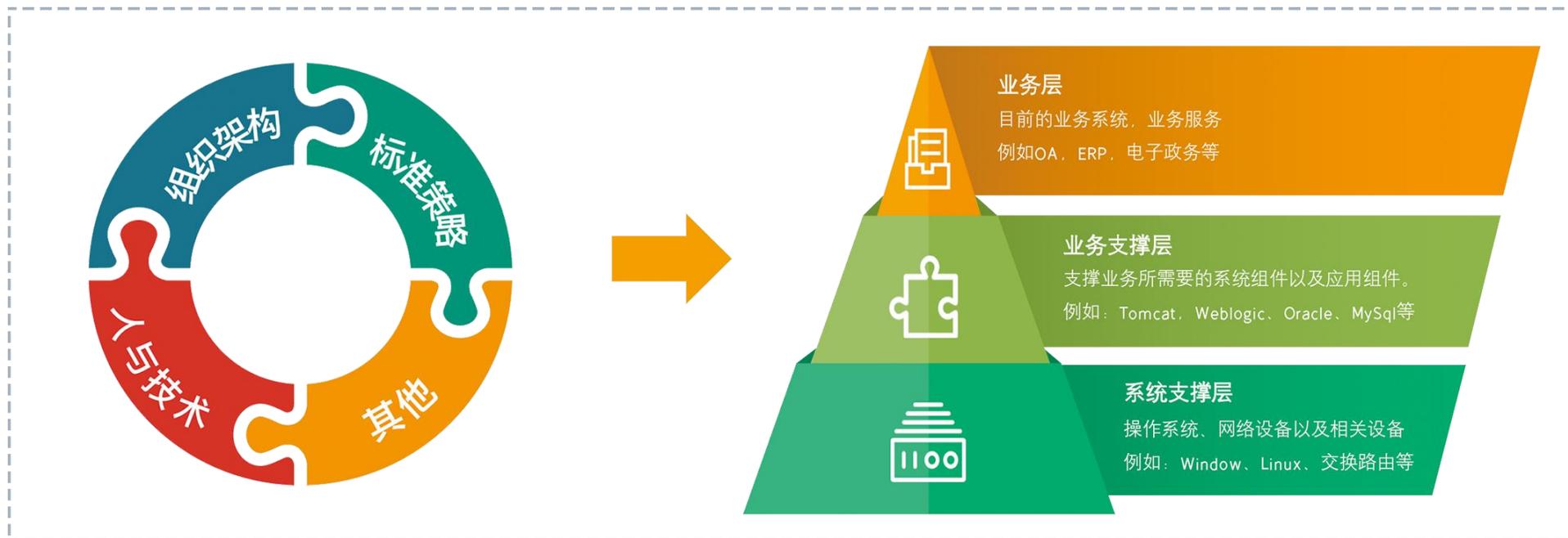
巡检详情

设备类型	设备名称	指标	异常范围	显示值	状态
Windows服务器	日志服务器	CPU平均负载	>=80%	7.67%	正常
Windows服务器	日志服务器	物理内存平均负载	>=70%	46.84%	正常
Windows服务器	日志服务器	磁盘平均使用率	>=80%	44.2%	正常
Windows服务器	SPA服务器	CPU平均负载	>=80%	0%	正常
Windows服务器	SPA服务器	物理内存平均负载	>=70%	23.21%	正常
Windows服务器	SPA服务器	磁盘平均使用率	>=80%	54.9%	正常
Linux服务器	OA服务器	CPU平均负载	>=80%	16.5%	正常
Linux服务器	OA服务器	内存平均负载	>=80%	87.62%	异常
Linux服务器	Synology_	CPU平均负载	>=80%	1.5%	正常
Linux服务器	Synology_	内存平均负载	>=80%	33.97%	正常
Huawei交换机	核心交换机	CPU平均负载	>=80%	31.2%	正常
Huawei交换机	核心交换机	内存平均负载	>=80%	12.5%	正常
Huawei交换机	研发部接入点	CPU平均负载	>=80%	26.5%	正常
Huawei交换机	研发部接入点	内存平均负载	>=80%	30.1%	正常
Huawei交换机	运营部接入点	CPU平均负载	>=80%	14.2%	正常
Huawei交换机	运营部接入点	内存平均负载	>=80%	25.9%	正常
Huawei交换机	运营部接入点	内存平均负载	>=80%	10.1%	正常
Huawei交换机	市场部接入点	CPU平均负载	>=80%	6.55%	正常

第 1 页

✔ 智能化巡检，自定义巡检任务，异常指标实时提醒，巡检综合评分，巡检报表即刻导出

2.4.3 功能介绍-合规基线核查



安全基线体系

01

- 建立一套当前时间或一段时间内的“理想化综合基线指标”即“**基线体系**”
- 通过一些手段对组织现有的安全指标进行分析,通过对比“理想化的基线指标”，形成一套差距分析结论
- 结合差距分析结论,针对差距进行实时监测、确认、跟踪或者预警,提出改进建议方案

安全基线理念

02

- 传统思路对设备、产品进行配置核查：零乱、混乱
- 面向业务平台整体进行核查，评估整个业务平台的配置安全性
- 建立原则要符合设备特性、适应系统特性，最终目的为业务服务

Linux基线检测

数据库基线检测

Tomcat基线检测

名称 筛选 重置

基线项分类	基线项	说明	结果	操作
访问控制	账号分配检查	用户账号分配检查，避免共享账号存在 1、系统需按照实际用户分配账号； 2、避免不同用户间共享账号，避免用户账号和服务器间通信使用的账号共享。	通过	
访问控制	多余账户锁定策略	应锁定与设备运行、维护等工作无关的账号。	不通过	自定义操作 执行操作

1、限制具备超级管理员权限的用户远程登

✔ 系统内置通用的基线检测库，用户也可以自行扩展不同对象的检测基线

* 作业名称

作业标签

所属分组

* 执行周期 手动 单次 日 周 月 年

选择资产

全部资产 0/2

- cemm 演示机
- k8s-master1

已选择的资产 0/1

- 组件平台

< >

<input type="checkbox"/>	名称
<input type="checkbox"/>	分发文件并输出
<input type="checkbox"/>	Linux基线检查作业
<input type="checkbox"/>	nginx服务健康度检查

共 3 条 <

过程编排	步骤	模块/作业名称	过程类型	操作
<input type="checkbox"/>	1	创建工作目录	模块	删除
<input type="checkbox"/>	2	分发基线检查脚本	模块	删除
<input type="checkbox"/>	3	输出工作目录内容	模块	删除
<input type="checkbox"/>	4	执行基线检查	模块	删除

2021-07-06 05:46:19

cemm 演示机 : 192.168.1.83

开始时间: 2021-07-06 05:46:19

创建工作目录: 执行完成 执行成功

执行结果:

执行成功

开始时间: 2021-07-06 05:46:19 - 结束时间: 2021-07-06 05:46:22

分发基线检查脚本: 执行完成 执行成功

执行结果:

执行成功

开始时间: 2021-07-06 05:46:22 - 结束时间: 2021-07-06 05:46:24

输出工作目录内容: 执行完成 执行成功

执行结果:

```

总用量 4
drwxr-xr-x 2 root root 32 7月 6 13:46 .
drwxr-xr-x 18 root root 237 7月 6 13:46 ..
-rw-r--r-- 1 root root 2512 7月 6 13:46 common-baseline.sh

```

开始时间: 2021-07-06 05:46:24 - 结束时间: 2021-07-06 05:46:25

执行基线检查: 执行完成 执行成功

执行结果:

```

baseline
1 密码必须符合复杂性要求 系统口令策略 用于检查密码是否符合复杂性的要求 高 1 字母大小写
1 密码最长使用期限 系统口令策略 用于检查密码的最长使用期限 高 0 3天
1 密码必须符合复杂性要求 安全审计 用于检查密码是否符合复杂性的要求 高 1 字母大小写
1 密码最长使用期限 安全审计 用于检查密码的最长使用期限 高 1 13位
1 密码最长使用期限 巡检策略 用于检查密码的最长使用期限 高 0 3天

```

2.4.4 功能介绍-应用部署

常用应用发布作业:

- 自动部署与补丁分布管理
- 软件/补丁安装和回退
- 应用补丁安装, 包括: 数据库、中间件以及第三方开发应用的补丁
- 操作系统补丁安装升级
- Prod环境、SIT环境、UAT环境的初始化、回退以及复位
- 应用库镜像创建以及软件版本校验
- 与应用发布流程平台集成

支持应用发布模板

- 将常用的发布流程固化下来, 实现发布过程的重用
- 实现发布流程和目标服务器的解耦、绑定多个目标服务器实现负载均衡场景的并发发布

根据软件开发指导, 支持自定义部署作业编排



2.4.4 应用部署-作业执行

* 资产名称

* IP地址

* SSH端口 ☰ 作业模块 / 插件编辑

访问类型 用户名/密码 SSH Key

* 模块名称

* 访问用户 * 英文名称

<input type="checkbox"/>	名称	标签	资产数目	执行周期	执行时间	执行状态	所属分组	状态	最近一次执行时间	操作
<input type="checkbox"/>	Elasticsearch7.0的Docker容器集群搭建	Elasticsearch Docker 容器	1	手动	7分23秒	未运行	应用部署	<input checked="" type="checkbox"/>	2021-03-02 12:70	执行历史 立即执行 删除
<input type="checkbox"/>	Oracle 11g搭建	oracle 数据库	1	手动	12分45秒	未运行	应用部署	<input checked="" type="checkbox"/>	2021-03-14 13:00	执行历史 立即执行 删除
<input type="checkbox"/>	CEMM系统搭建	cemm 运维监控	1	手动	6分20秒	未运行	应用部署	<input checked="" type="checkbox"/>	2021-03-24 09:52	执行历史 立即执行 删除
<input type="checkbox"/>	CEMM 投产环境回滚	cemm 环境回滚	1	手动	3分08秒	未运行	应用部署	<input checked="" type="checkbox"/>	2021-03-28 12:45	执行历史 立即执行 删除
<input type="checkbox"/>	CEMM 补丁分发以及升级	cemm 补丁 升级	2	手动	8分06秒	未运行	应用部署	<input checked="" type="checkbox"/>	2021-03-30 14:50	执行历史 立即执行 删除

状态

状态

取消

确定

2.4.4 应用部署-功能价值

提高应用质量

- ✓ 模型化应用部署生命周期，减少错误
- ✓ 应用部署回滚，最小化服务宕机时间



标准化流程

- ✓ 实现“研发→测试→生产”规范路径发布
- ✓ 集成应用生命周期管理流程，减少缺陷和延迟



应用发布流水化

- ✓ 自动化部署，减少手工操作，缩短部署时间
- ✓ 标准化流程固化重复操作，全程审计跟踪



2.4.5 功能介绍-配置收集自动化



信息采集

硬件信息：CPU、内存、磁盘...；
标准操作系统软件/补丁信息；
操作系统信息：操作系统类型, 具体OS版本等信息；
数据库信息、中间件基本信息；
网络拓扑、虚拟化环境结构信息；



配置管理

快照方式保存设备配置与变化历史；
配置的比对、跟踪、备份和恢复；
非授权配置变更，出发告警通知；
定时同步基础信息，出现偏差，给出对比报表；



自动执行

自动执行重复性的配置管理任务，批量配置海量设备；
支持计划配置，对常规任务进行调度；
集成运维服务管理系统的自动变更审批机制流程；

2.4.6 配置收集自动化-作业编排

<input type="checkbox"/>	名称	标签	资产数目	执行周期	执行时间
<input type="checkbox"/>	Linux操作系统信息收集	信息采集	3	手动	19秒
<input type="checkbox"/>	iptables防火墙信息收集	iptables 防火墙 信息采集	3	手动	16秒
<input type="checkbox"/>	华为 S628-PWR网络配置信息恢复	华为 网络设备	1	手动	35秒
<input type="checkbox"/>	oracle 11g数据库信息收集	oracle 数据库	1	手动	13秒
<input type="checkbox"/>	elasticsearch7.0信息收集	elasticsearch 数据库	2	手动	9秒
<input type="checkbox"/>	nginx集群信息收集	nginx 集群 负载均衡	3	手动	16秒

运维作业 / 作业编辑

* 作业名称 华为 S628-PWR网络配置信息恢复

作业标签 华为,网络设备

所属分组 信息收集

* 执行周期 **手动** 单次 日 周 月 年

选择资产 全部资产 0/3

- cemm 演示机
- k8s-master1
- 组件平台



已选择的资产 0/1

- 华为 S628-PWR

过程编排

<input type="checkbox"/>	步骤	模块/作业名称	过程类型	操作
<input type="checkbox"/>	1	创建工作目录	模块	删除
<input type="checkbox"/>	2	分发网络设备配置校验脚本	模块	删除
<input type="checkbox"/>	3	加载标准配置备份基线	模块	删除
<input type="checkbox"/>	4	执行配置校验脚本	模块	删除
<input type="checkbox"/>	5	配置校验结果分析	模块	删除
<input type="checkbox"/>	6	配置信息回滚	模块	删除
<input type="checkbox"/>	7	校验并配置标准基线	模块	删除

+

删除

删除

删除

删除

删除

删除



补丁管理

支持用户自定义的补丁策略
与原厂商补丁库集成

- 自动下载补丁和元数据
 - 集成微软基线安全分析器
- 灵活的、智能的补丁安装



密钥管理

发现网络中的SSH系统，枚举用户及私钥以及查看组织中密钥与用户的对应关系

批量执行密码的重置与更新操作

强制化策略生成密码，支持密码、授权导出

创建SSH密钥对以及自动定期更换密钥对



标准化构建

物理机、虚拟机的灵活模板或原生OS安装

统一构建配置规范、软件平台、应用版本

<input type="checkbox"/>	名称	标签	资产数目
<input type="checkbox"/>	Linux用户名/密码批量配置	用户 密码	3
<input type="checkbox"/>	Linux iptables防火墙配置	防火墙 iptables	3
<input type="checkbox"/>	Linux SSH 密钥生成及拷贝	SSH 拷贝 密钥	3
<input type="checkbox"/>	CentOS系统日志归档	centos 日志 归档	3
<input type="checkbox"/>	Log4j日志漏洞修复	log4j 漏洞修复	3

运维作业 / 作业编辑

* 作业名称

作业标签

所属分组

* 执行周期 手动 单次 日 周 月 年

选择资产

全部资产 0/0

无数据

已选择的资产 0/3

- cemm 演示机
- k8s-master1
- 组件平台

过程编排

<input type="checkbox"/>	步骤	模块/作业名称	过程类型	操作
<input type="checkbox"/>	1	创建工作目录	模块	删除
<input type="checkbox"/>	2	分发用户名/密码格式化文件	模块	删除
<input type="checkbox"/>	3	解析用户名/密码描述文件	模块	删除
<input type="checkbox"/>	4	创建/更新用户并设置密码	模块	删除
<input type="checkbox"/>	5	用户赋权	模块	删除

+

近一次执行时间	操作
21-03-03 12:00	执行历史 立即执行 删除
21-03-04 13:00	执行历史 立即执行 删除
21-03-08 13:52	执行历史 立即执行 删除
21-03-10 14:30	执行历史 立即执行 删除
21-03-20 16:23	执行历史 立即执行 删除

Part.

3

场景案例

基于场景驱动的ATOP，具体能做什么？

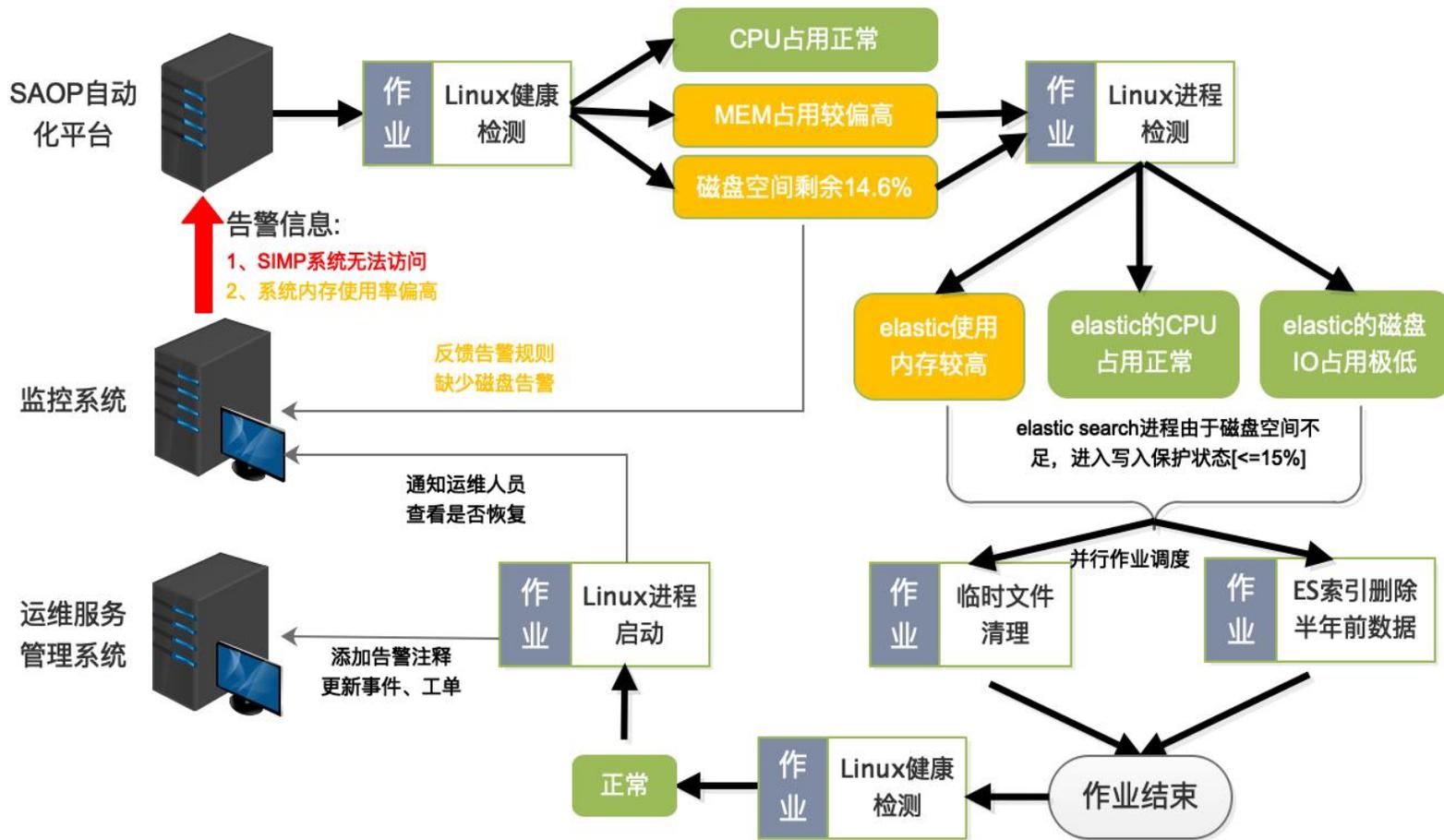


SMARTEAGLE
慧鹰

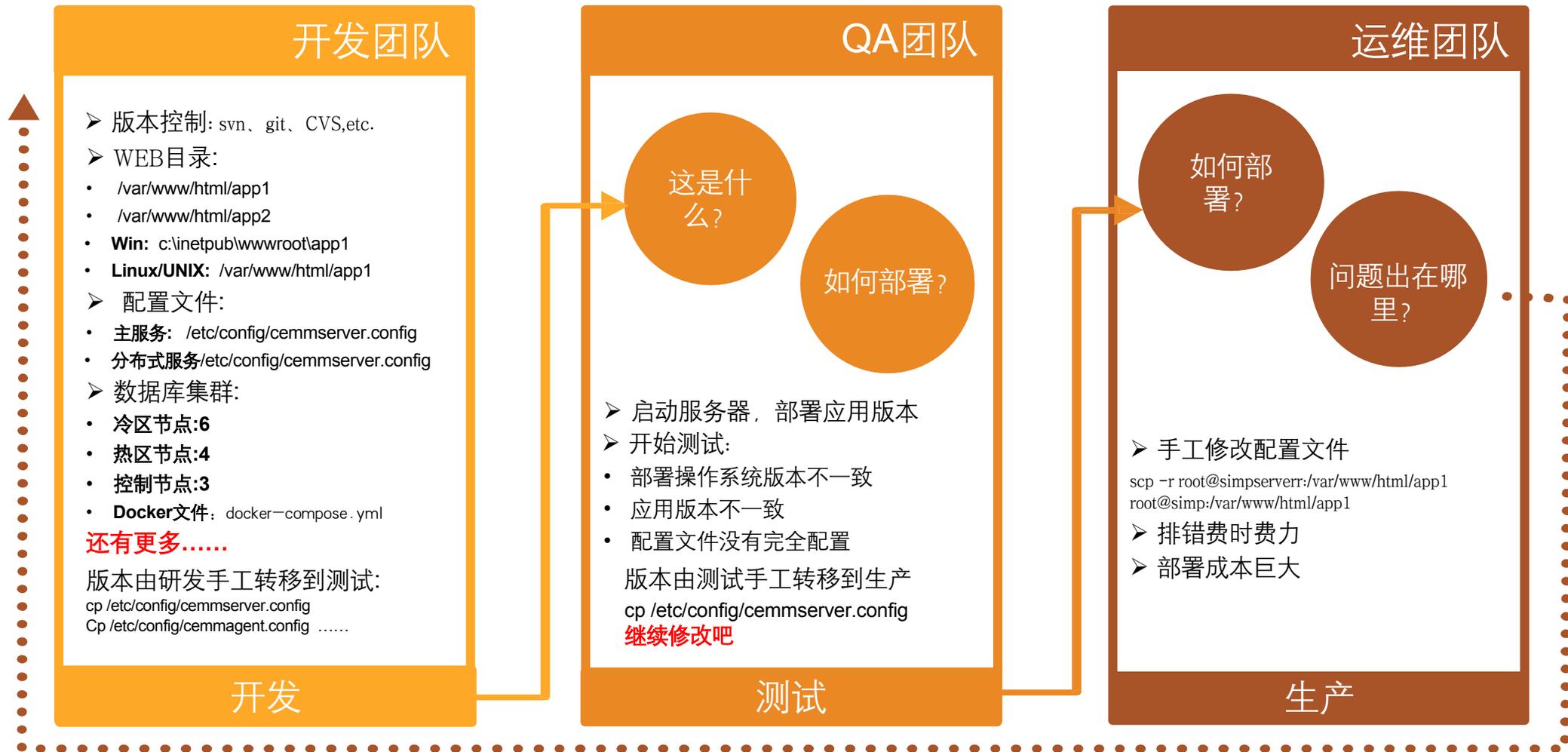
作业描述：自动化运维作业中，纳入事件处理自动化以及设备健康性检查，帮助用户更为精准的处理日常运维故障

执行流程：

1. 监控系统发生告警，业务系统处理中断，进程执行处于假死状态
2. 运维人员启动ATOP健康检查流程验证、分析原因并发现进程对于数据写入处于保护状态，根本原因是核心服务器磁盘空间非常低
3. SAOP执行自动化流程：
 - 执行清理磁盘操作
 - 检查进程中IO写情况
 - IO写入偏慢，业务进程卡死
 - 重启启动业务进程
 - 重新检查进程状态，恢复OK
 - 通知运维人员查看告警恢复事件
 - 更新服务管理系统的自动化事件，自动在事件增加告警注释，并关闭事件工单



作业描述：开发团队、QA团队、运维团队。面对生产交付过程，该如何处理？运维人员该如何减压？
相互独立的团队、大量的手工作业，



3.2 应用发布管理-解决应用部署的难题

第一步：应用建模

- 通过Layer(层)将需要部署在一起的 Artifacts(构件)进行整合;
- 部署的Artifacts(构件)支持是二进制编译产物、压缩文件、图片、配置文件或脚本等;
- 应用模型将一些列的特定版本的 Artifacts(构件)整合为一个完整包进行部署;
- 同一应用模型支持部署到多个不同的环境中;

第二步：环境建模

- 支持构建环境的架构和配置信息，包括环境中所需的资源及其相关信息
- 构成环境的资源可以是物理机器、虚拟机或云资源;
- 精确追踪每个环境中所部署的构件清单;

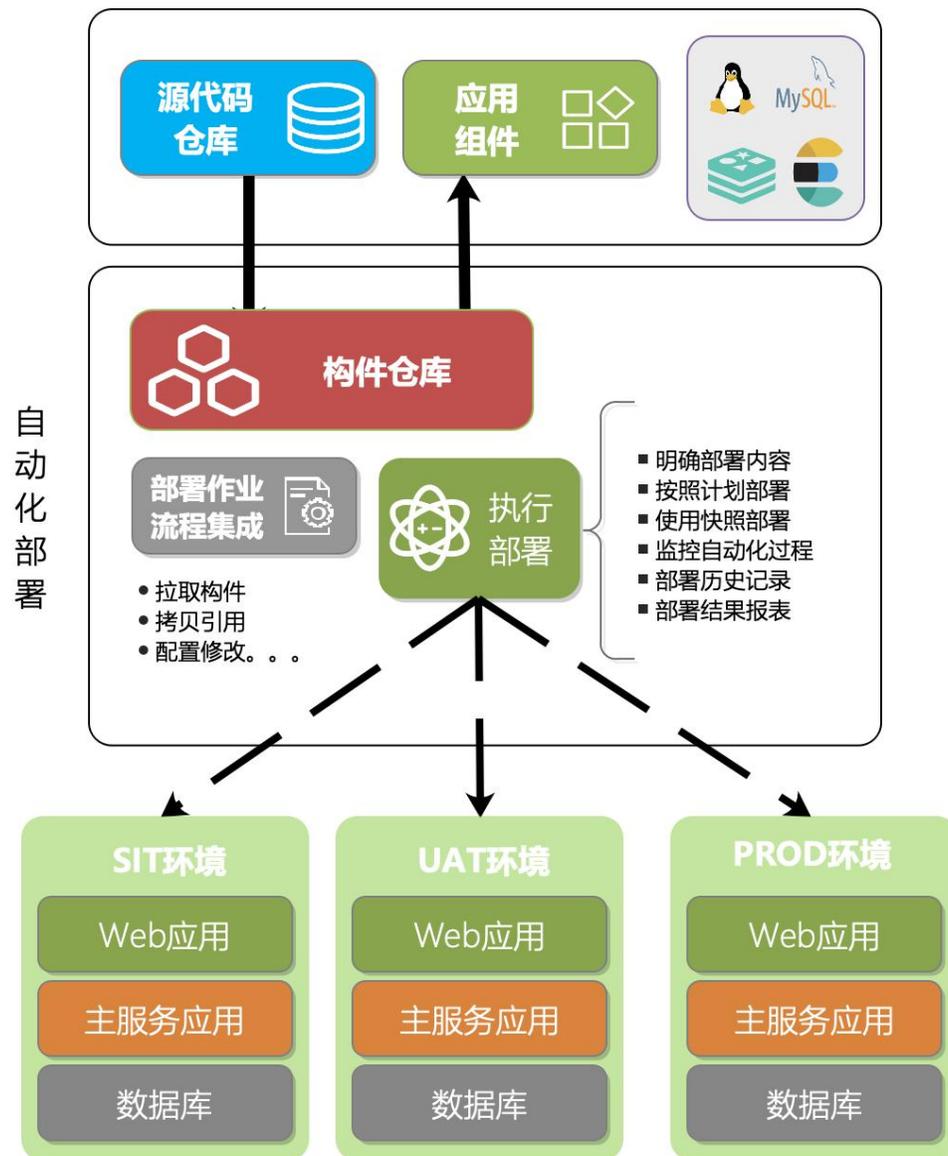
第三步：应用作业制定

- 图形化的应用流程建模过程，支持分支、并行等;
- 可重用的应用部署流程;
- 支持跨不同环境的应用部署;
- 可重用现有部署脚本，对现有过程的冲击较少;
- 提供开箱即用的工具集成接口;

第四步：快照技术部署

- 将组件、流程、环境都可以进行快照固定，以便快速回滚或部署;
- 提供快照间的对比以及当前部署与之前快照的对比;

部署自动化编排+环境构建



Part.

4

产品价值

通过ATOP实现智能自动化运维会带来什么效益呢？



SMARTEAGLE
慧鹰

4. 产品价值

慧鹰ATOP建立了统一运维操作管理平台，实现真正的“运维管控”。

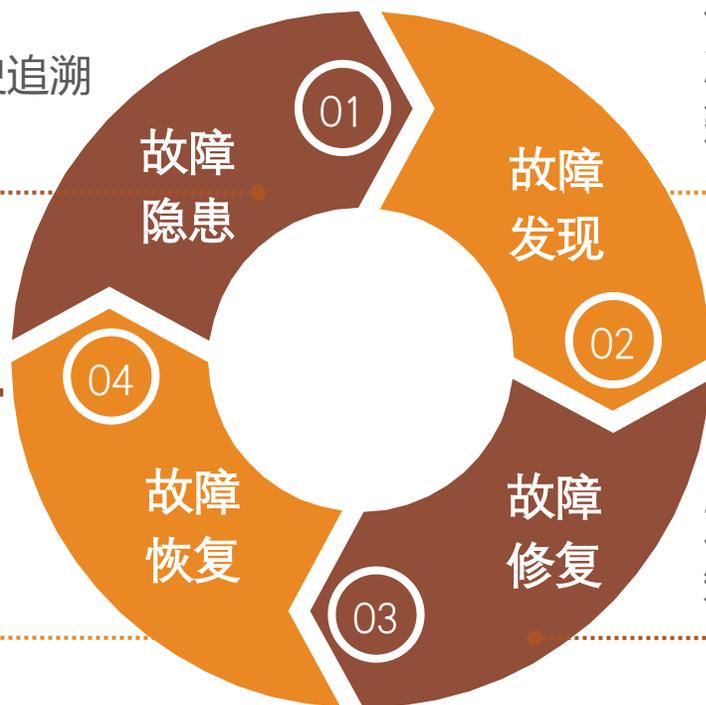
- ✓ 从可用性运维角度，ATOP很好的补充了传统网管系统在故障管理的两大薄弱环节
传统网管主要解决缩短故障发现时间的问题，而在隐患检测、故障修复方面缩手无策。

预防和控制

定期有效的风险性检查
对变更的管理和控制，实现历史追溯
消除隐患及不当配置变更

核查和减负

有效降低告警洪灾效应
减轻运维人员负担，填补人力资源缺口
建立智能的故障分析决策中心



合规和审计

集成有效的合规和审计工具
集中统一管理，落实运维规范
建立并实现真正的运维流程

效率和便捷

自动化的发布和变更
对已知错误的自动修复能力
知识和经验共享，快速定位和排障

2024



SMARTEAGLE
慧鹰

感谢您的观看

THANK YOU FOR YOUR LISTENING