行之有效的企业运维管理工具解决方案

黑龙江省电力调度实业公司

付鑫

目录

大事件

2015.02 ——14岁少年发现天河一号超算集群可被登录控制漏洞，其办公环境WiFi无需密码即可连接，且服务器上将近一半用户均存在弱口令。

2014.02 ——PPS&爱奇艺发生内网渗透。事件起因是某员工操作不当，在源码托管上设置未授权访问，导致内网信息在公网上可以任意访问。

2014.01——中国境内发生DNS解析服务故障，导致百度等多家网站长达几个小时无法访问。据分析，疑是GreatFirewall管理员的误操作导致。

2013.06——京沪等地工商银行网点及电子渠道瘫痪50分钟，工行官方回应称是系统升级导致。

2012.04——证券公司、后台被入侵、40万股民信息泄漏。事件起因是第三方运维人员窃取大量客户信息，并利用这些信息牟取私利。

2011.04——韩国四大银行之一的农协银行出现持续3天以上的网络瘫痪。事故起因于第三方代运维人员对银行核心系统下达了一条rm.dd命令。

IT运维现状

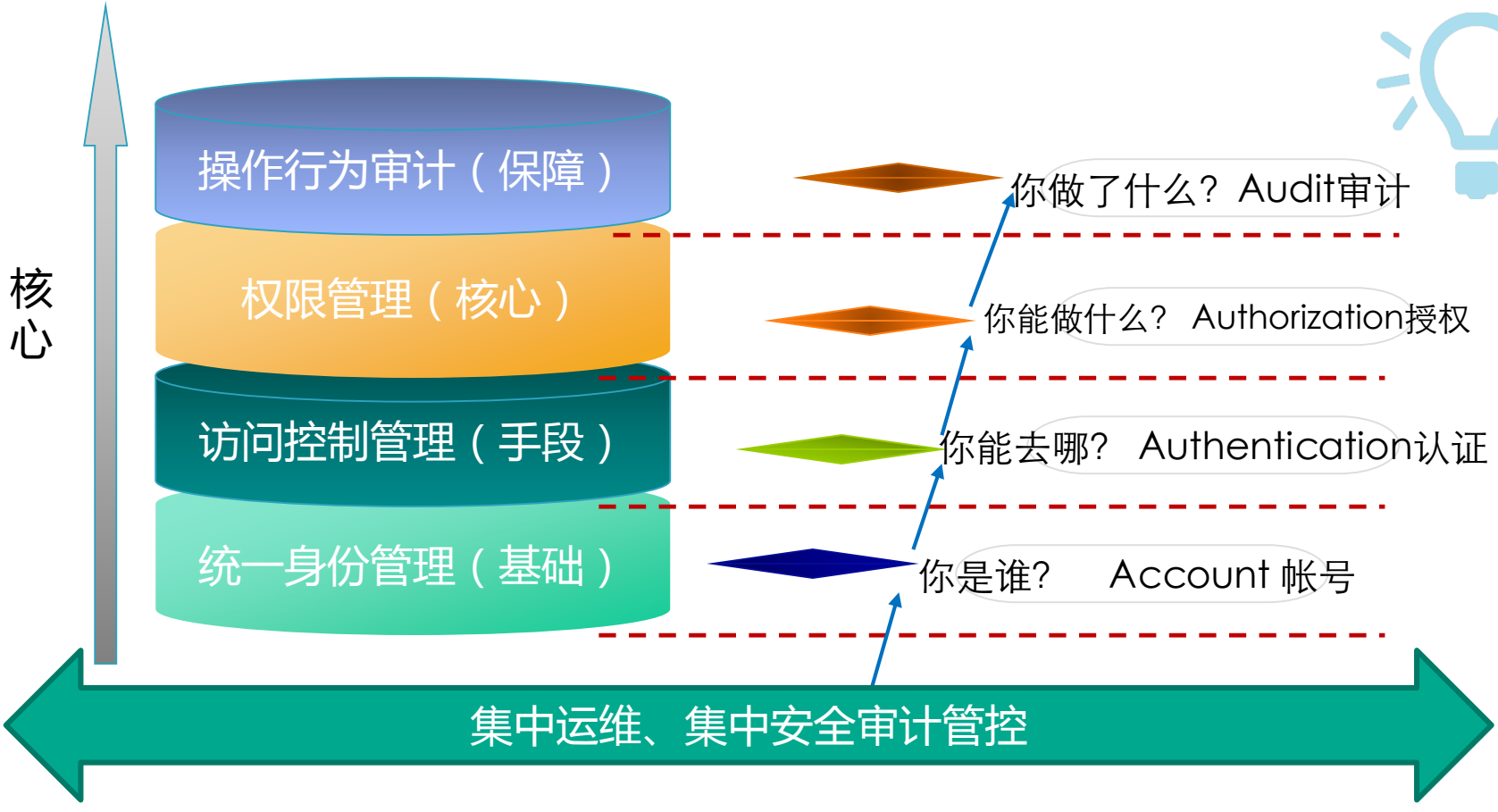
- ✓ 公司规模大
- ✓ 业务数据量大，需求变动频率大
- ✓ 业务涉及地域广大
- ✓ 设备资源规模大
- ✓ 系统重要性提升，压力大
- ✓ 运维方式和手段相对落后

- ✓ 信息设备多，品牌多，版本多
- ✓ 信通管理层次多
- ✓ 业务系统多
- ✓ 运维操作多
- ✓ 业界新技术多
- ✓ 运维工具多
- ✓ 人员角色多

- **高权限操作风险不透明**
- **违规操作导致敏感信息泄露**
- **误操作导致服务异常甚至宕机**
- **交叉异构、帐号共享**

- **操作风险不可控**
- **黑客盗用帐号实施恶意攻击**
- **无法有效监管操作、必要取证/举证**

信息运维审计？


核心
操作行为审计（保障）
权限管理（核心）
访问控制管理（手段）
统一身份管理（基础）
你做了什么？Audit审计
你能做什么？ Authorization授权
你能去哪？ Authentication认证
你是谁？ Account 帐号
集中运维、集中安全审计管控

我们新的需求

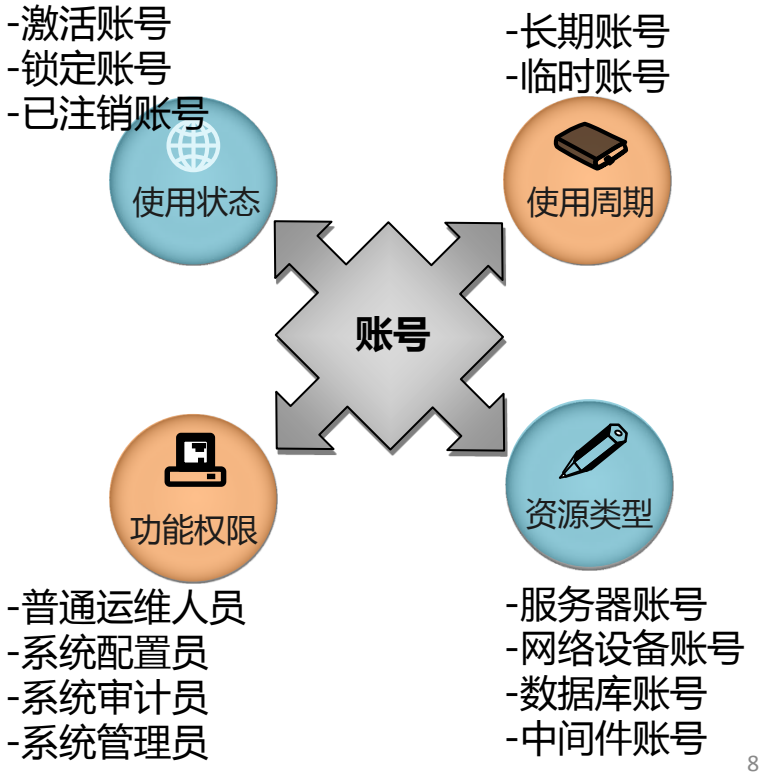
区别于传统单一式的堡垒机的运维审计产品，我们需要的是一个面向服务面向性能的集中的运维管控平台。

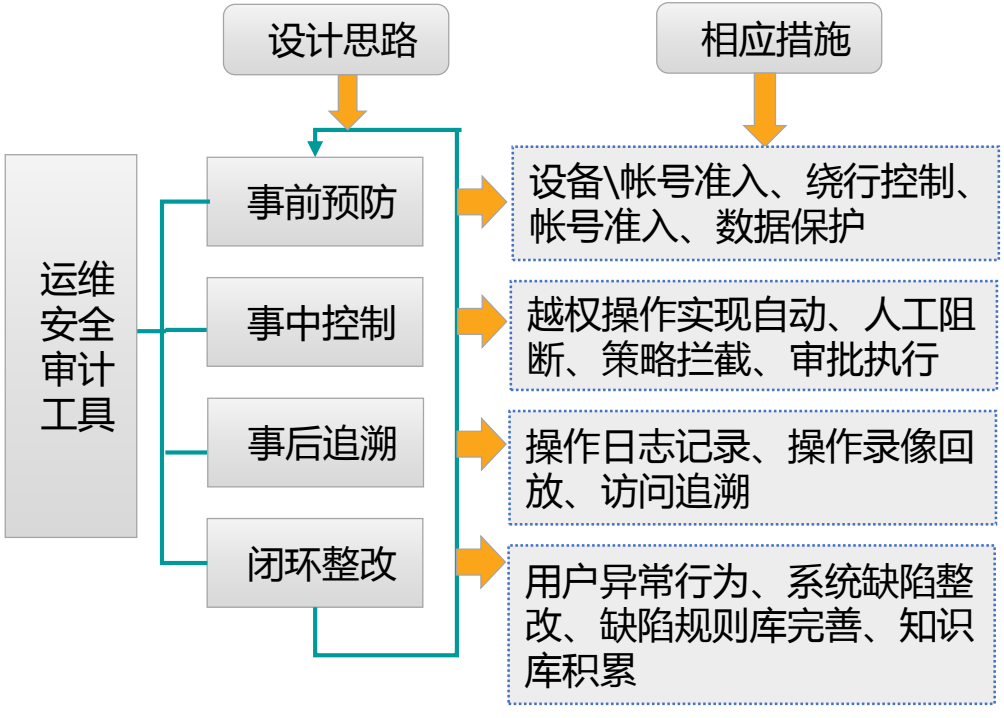
1. 拥有集中的运维操作管控平台。
2. 拥有强大丰富的管理能力。
3. 实现资源全覆盖。
4. 实现集中细粒度的账号权限管理。
5. 实现全过程运维行为审计。
6. 可以灵活接入各种主流运维工具。
7. 云环境智能运维审计。
8. 基于海量数据的运维分析和日志搜索。
9. 具备高可靠的自身安全性。
10. 达到一站式管理。
11. 实现方便灵活的可扩展性。
12. 为自动化运维做底层支撑。

目录

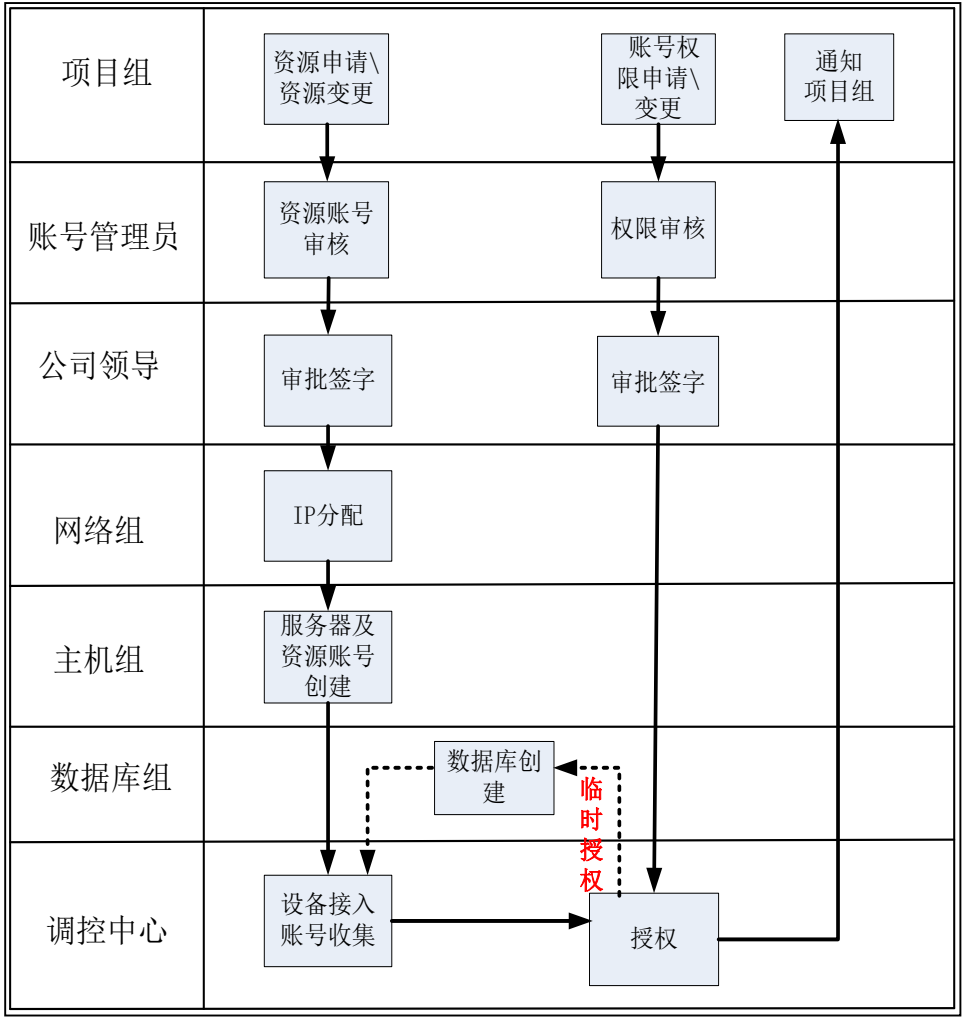
基础篇-思路

基于应用虚拟化实现对服务器、数据库、中间件、网络设备、安全设备等多种IT资源的集中账号权限管理、运维审计管理，能够对用户的运维操作行为进行全面记录和细粒度权限控制、支持自动化、人工运维，实现运维工作全过程可控、可视、可分析、可追溯，使操作落实到人。





基础篇-工程中心（建设）



流程描述

- 项目组资源申请前，应与主机、网络组等沟通协调，了解本地实际情况，合理填报需求。
- 项目组填写资源申请单，需规划好资源用途（从账号规划oracle、weblogic等）方便主机组创建。
- 资源变更需填写资源变更审批单。
- 资源创建配置IP后，申请运维管理中心账号权限，接入资源。
- 项目组人员通过运维管理中心系统进行业务系统部署、日常运维等操作。
- 设备、人员3月未登入将自动变为孤岛资产、闲置用户。

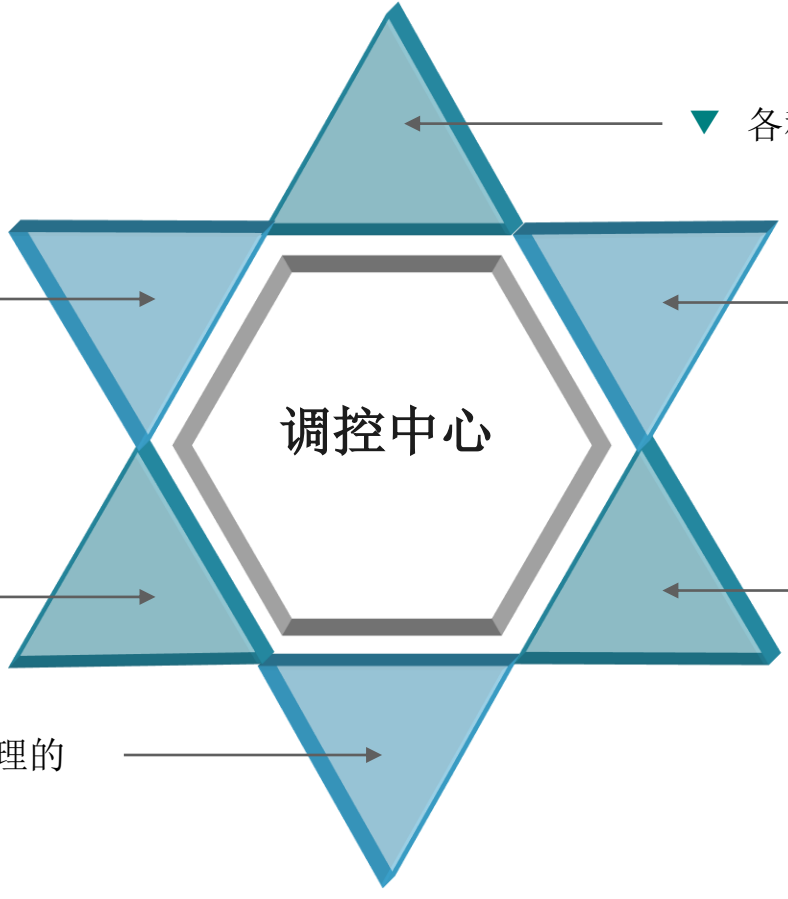
项目实施、建转运、运维深度管控，厂商实施所有内容可控。

基础篇-运检中心

- 虚拟的应用发布平台
- 单点登录，根据访问控制中定义好的从帐号信息，系统自动填写用户名密码

□业务系统部署 □日常巡检 □检修 □升级扩容 □优化 □应急 □运维统计分析

基础篇-调控中心



- 各种资源的调控。
- 账号权限授权许可。
- 敏感信息授权许可。
- 对各种信息通信资源的状态、性能和故障告警信息进行监控。
- 对运维管理中心策略配置，修改密码。
- 负责信通运维检修工作的实时管控，发现异常操作，可远程中断。对运维检修内容限定。
- 负责信通系统应急处理的指挥协调

基础篇-审计管理员

1、审计无盲点：捕获所有的本地和远程操作会话
- 本地登录会话
- 所有远程会话协议，如：Citrix XenApp/XenDesktop, Microsoft Terminal Service, VDI, VMWare View, Remote Desktop，Symantec PCAnywhere，ssh等
- 支持所有虚拟化和云计算平台

2、提高审计效率：直观、简洁的审计方式，极大提高审计效率

3、加大审计深度、扩大审计范围：
- 颗粒度审计，可以按照用户、服务器、文件名、目录名、Windows窗口信息、动作行为
- 不依赖日志，没有日志的应用也可以审计
- 审计深度远远大于日志，可以审计应用中所有操作过程

4、强大灵活的审计策略：能够根据用户、组、应用、服务器制定不同的审计策略

5、身份确认技术
- 保证被审计对象的身份唯一性
- 即使用Administrator进行操作，也能保证审计对象的准确性

基础篇-审计管理员

6、企业级架构设计
- 自动负载均衡，不需要额外购买负载均衡设备
- 应用服务器可以动态加入
- 低数据存储量
- 较小的客户端对CPU的使用率

7、强大的检索功能
- 支持按用户名、服务器、应用、文件、目录、窗口信息等进行检索，迅速定位审计点

8、可与网管系统整合实现报警
- 详细的数据，全面覆盖，对非法或高危操作进行及时发现并加以告警和控制
- 提供邮件、SMS等 实时安全告警

9、在线审计
- 可在线重影会话，实时监控运维操作

10、审计内容可回放
- 可以回放运维操作

11、操作行为分析
- 可以根据运维人员的日常操作做行为分析

基础篇-功能

事前控制

- 认证机制
- 权限管理
- 单点登录

过程监督

- 指令黑白名单
- 敏感指令金库
- 在线审计

事后追溯

- 操作回放
- 绕行审计
- 日志分析

基础篇-功能

统计分析

行为追溯

主动告警

事前预防（授权）

操作模板库/策略配置

指令黑白名单

资源授权

事中控制（监控）

实时监控

现场（远程）授权

操作阻断

事后审计（审计）

审计分析

审计回放

行为追溯

异常事件提醒

用户登录分析

异常登录告警

审计监控提醒

业务操作分析

权限平台审记管理

业务系统审计管理

操作行为追溯

异常授权告警

访问轨迹记录

辅助功能

集成管理

自审计功能

应急管理

....

用户管理

认证管理

设备管理

密码管理

工作票操作票

敏感数据管理

应用管理

报表管理

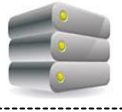
业务操作

用户授权

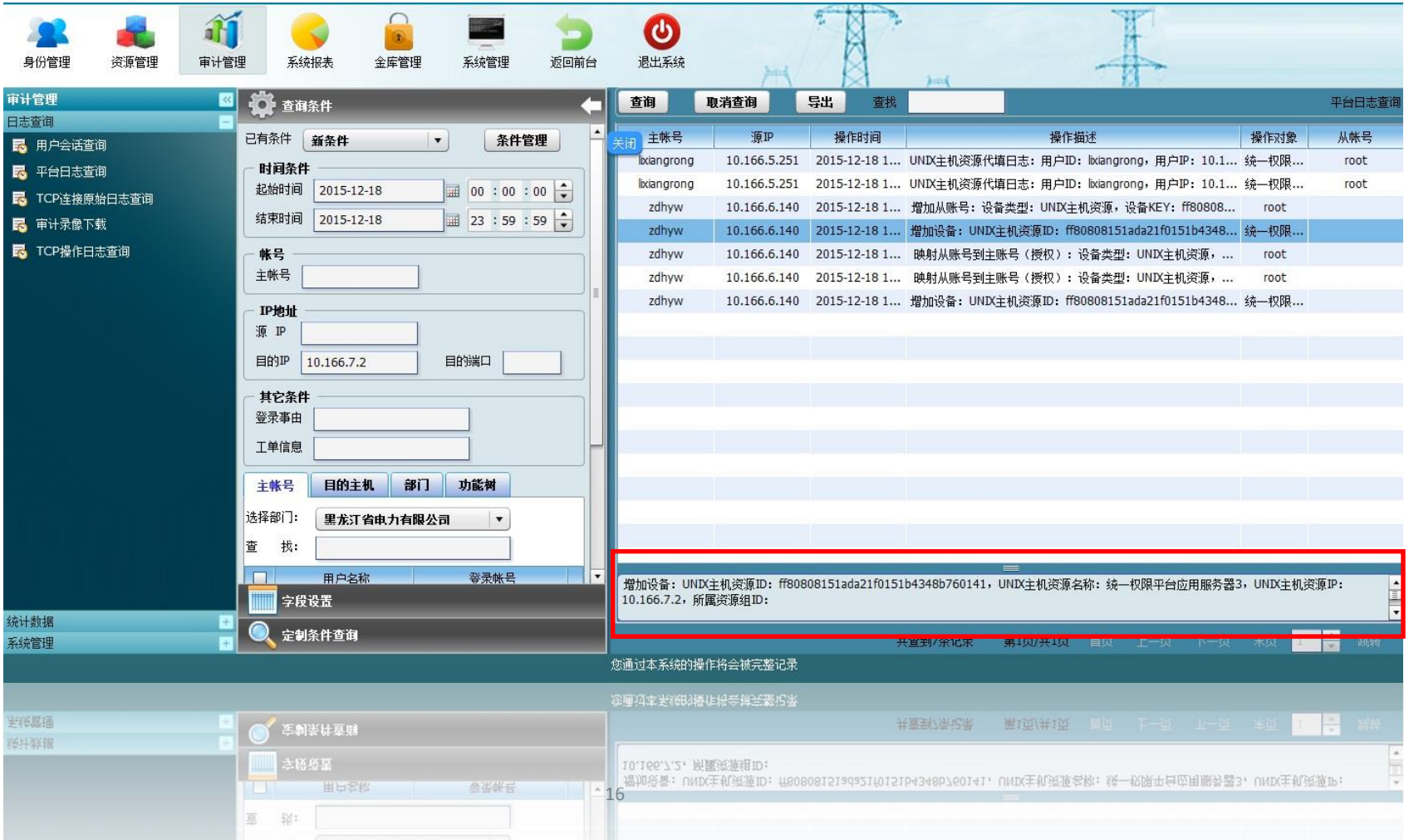
用户登录

访问轨迹

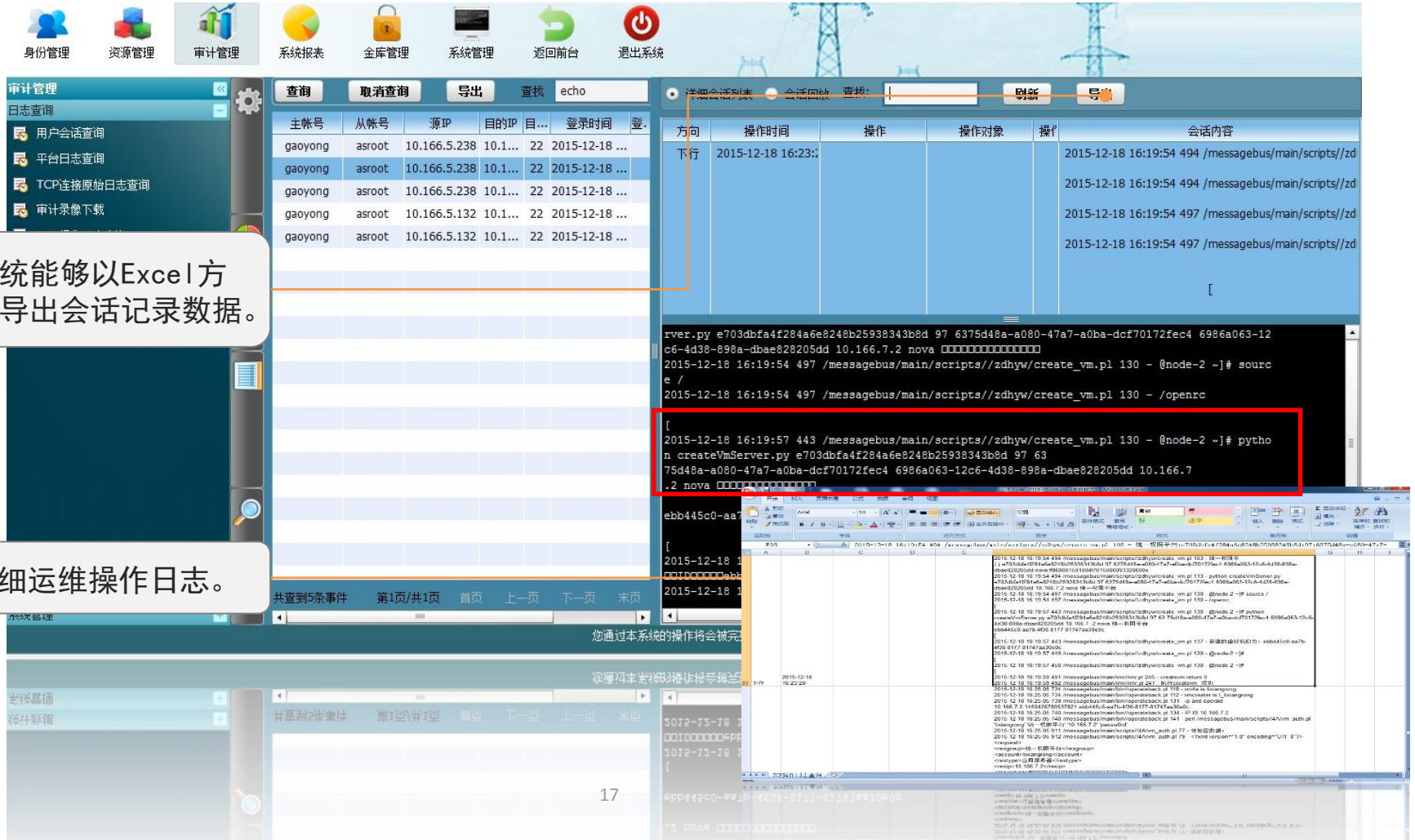
主机、数据库
网络设备、安全设备、
应用系统



基础篇-工程中心-应用案例-openstack创建虚拟机



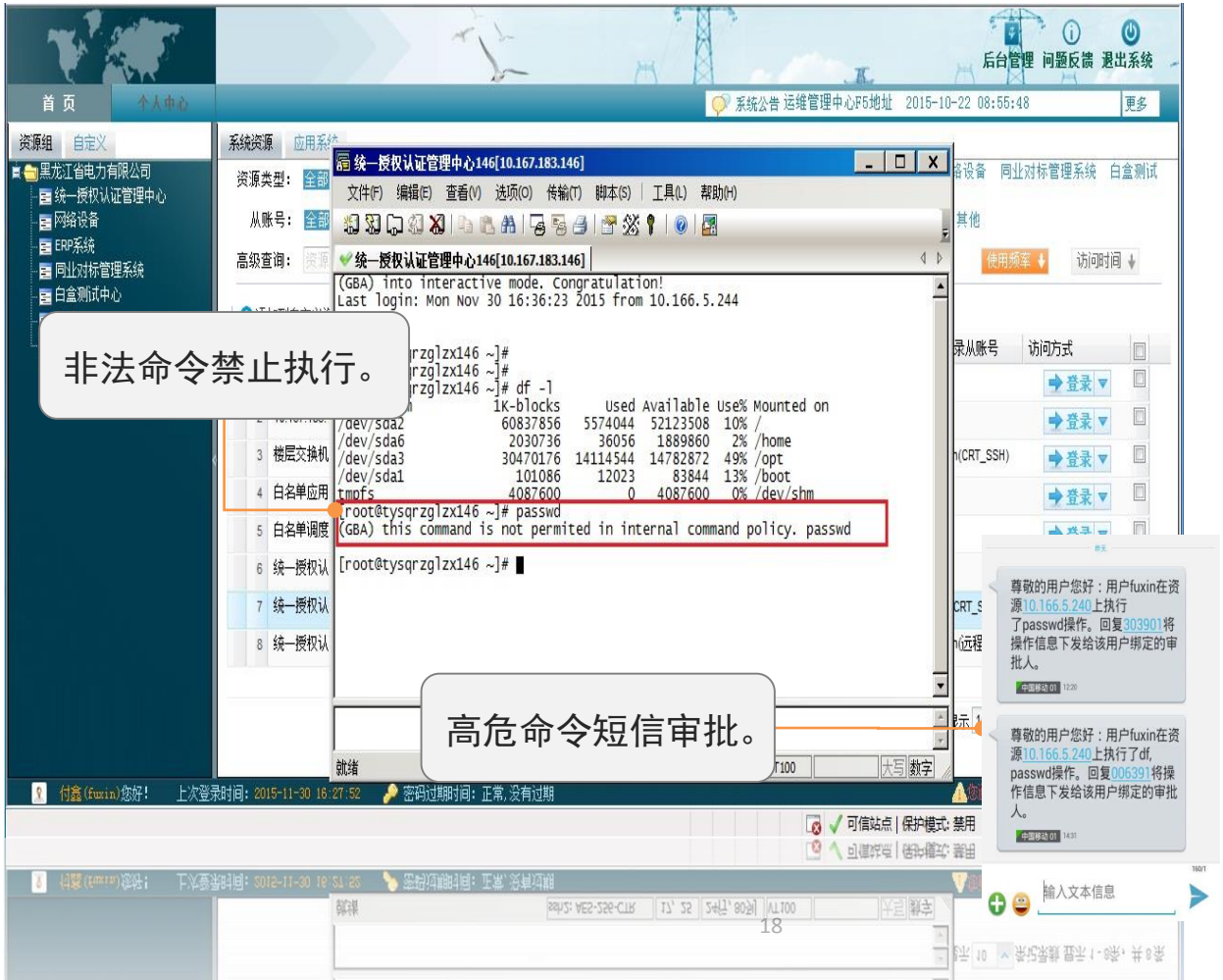
基础篇-工程中心-应用案例-openstack创建虚拟机



系统能够以Excel方式导出会话记录数据。

详细运维操作日志。

基础篇-调控中心-应用案例-事前防范



➢敏感指令黑白名单：

管理员在后台设置禁止使用或允许使用的黑白名，黑白名单与授权进行绑定，确保了不同权限管理员的不同设备操作权限。

➢调控指令审批功能：

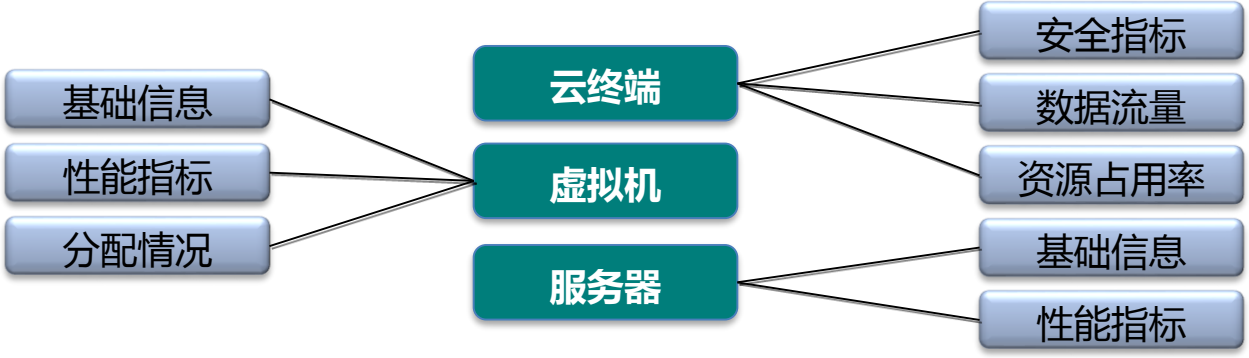
调控人员可以了解实际操作内容，也可以在操作的过程中对相关命令进行审批。

目录

进阶篇-信息运维监控

可以实时监控到服务器的各项指标

与日志分析系统、告警系统、漏扫系统等联动，可以监测运维过程中包括服务器的运行情况、资源情况、性能情况等关键指标数据。从可用性、健康度、繁忙度三个维度评价业务整体运行现状。



运行监测

监测与业务系统关联相应的中间件、数据库、服务器、网络设备等资源在运维过程中的操作。监测非法外连。

中间件　数据库　服务器　网络

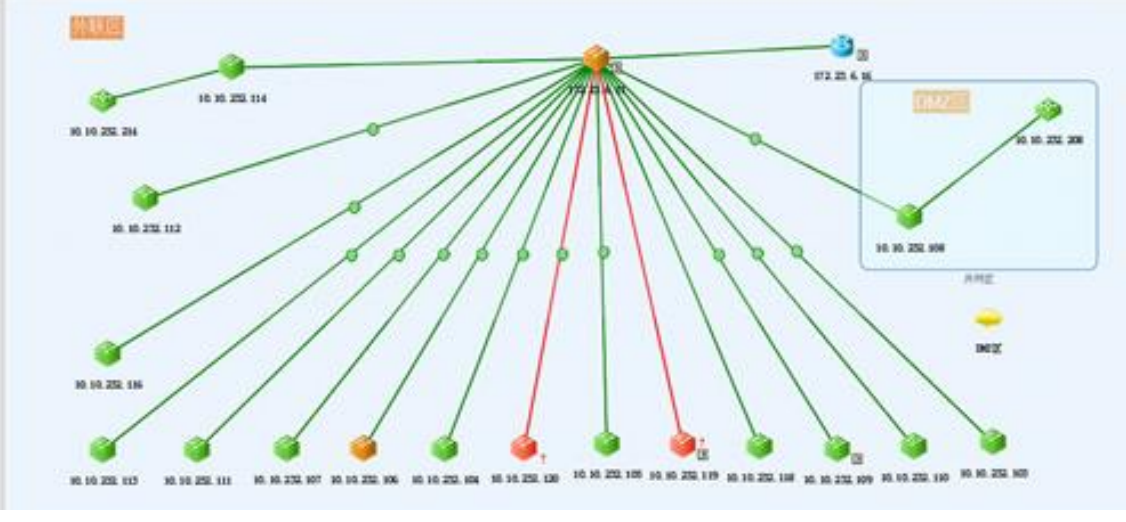
告警管理

通过灵活配置告警类别、严重级别、告警阀值生成告警规则，系统依据配置的告警规则提供包括短信、邮件、即时通讯等多种方式的告警服务功能，通过告警管理降低IT管理人员的管理被动性。

进阶篇-运行方式管理

1、依据现有的服务器账号密码、交换机流量、日志信息，自动构建图形化的业务拓扑、网络资源拓扑，生成服务器的运行方式，直观的反映业务包含的IT资源及其之间的关系，一目了然定位故障点。

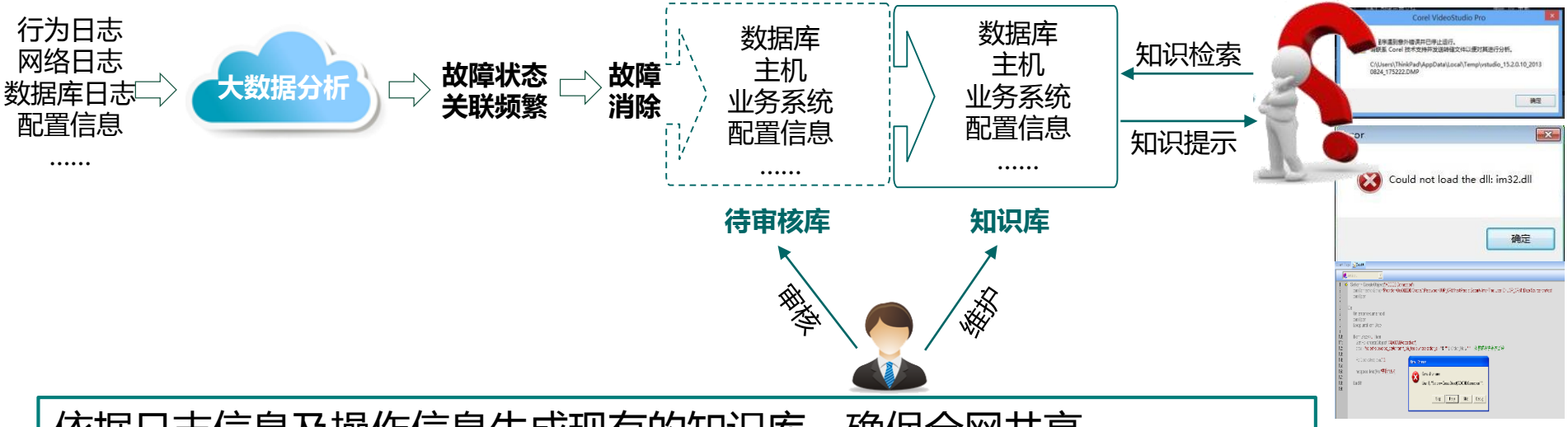
2、根据运维操作频率，定位孤岛资产。



进阶篇-知识库管理

大数据分析-知识收集

将大数据分析得到的频发故障状态关联，通过运维管理中心回放运维操作、配置比对，经验证后确实能够消除故障的结果纳入到知识库。



依据日志信息及操作信息生成现有的知识库，确保全网共享

目录

后记-技术发展和应用

先进技术提升运维水平

自动工具提升运维能力

- 适应信息通信技术发展，不仅成功应对新技术带来的运维变化与挑战，而且不断应用新技术提升运维自动化
- 快速迭代开发、持续部署，完善审计，建设统一运维平台，开展精准化权限，标准化基础设施，虚拟化运维应用工具，自动化工具、移动化操控工作、智能化分析、智慧机器人，从而实现全业务细粒度监视、全过程审计、全数据在线分析

谢谢!