



# 抗“疫”有情，网安联信创生态在线沙龙伴你行！

抗“疫”公益系列活动之二十（二）

## 浅话信创环境下的运维安全



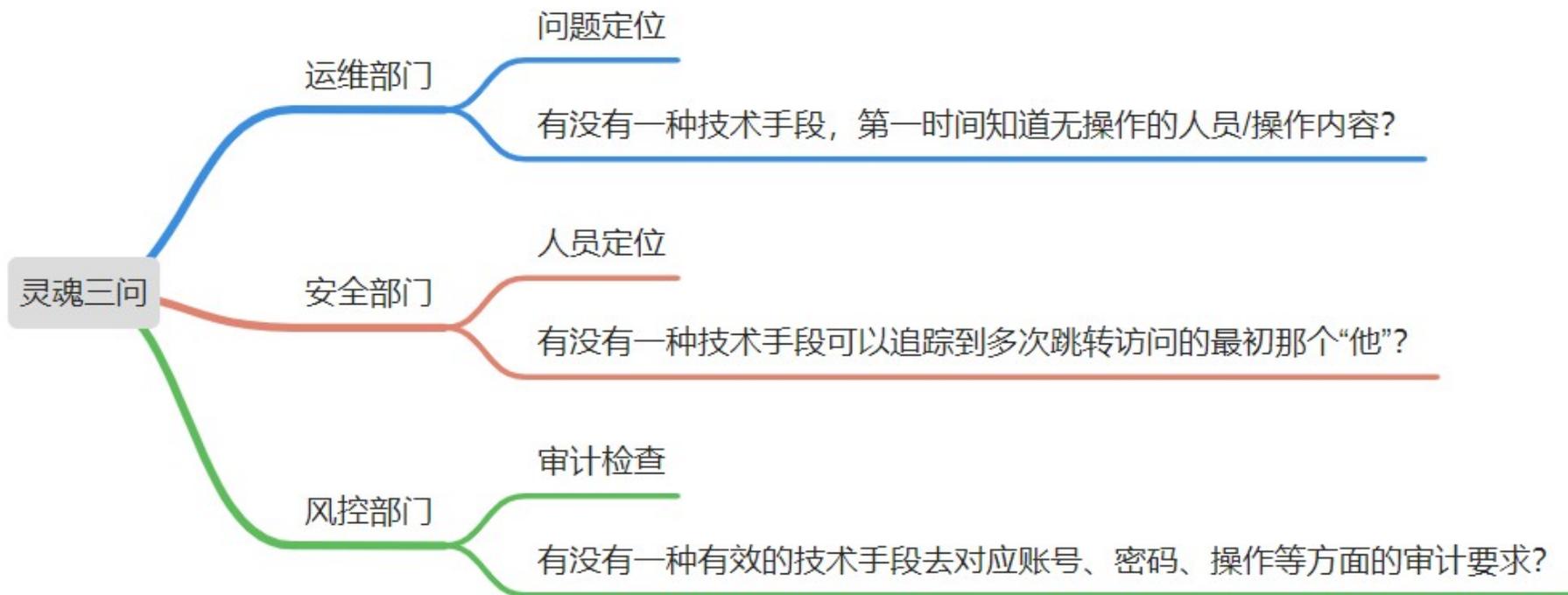
王霄



日期：2020.03



北京圣博润高新技术股份有限公司





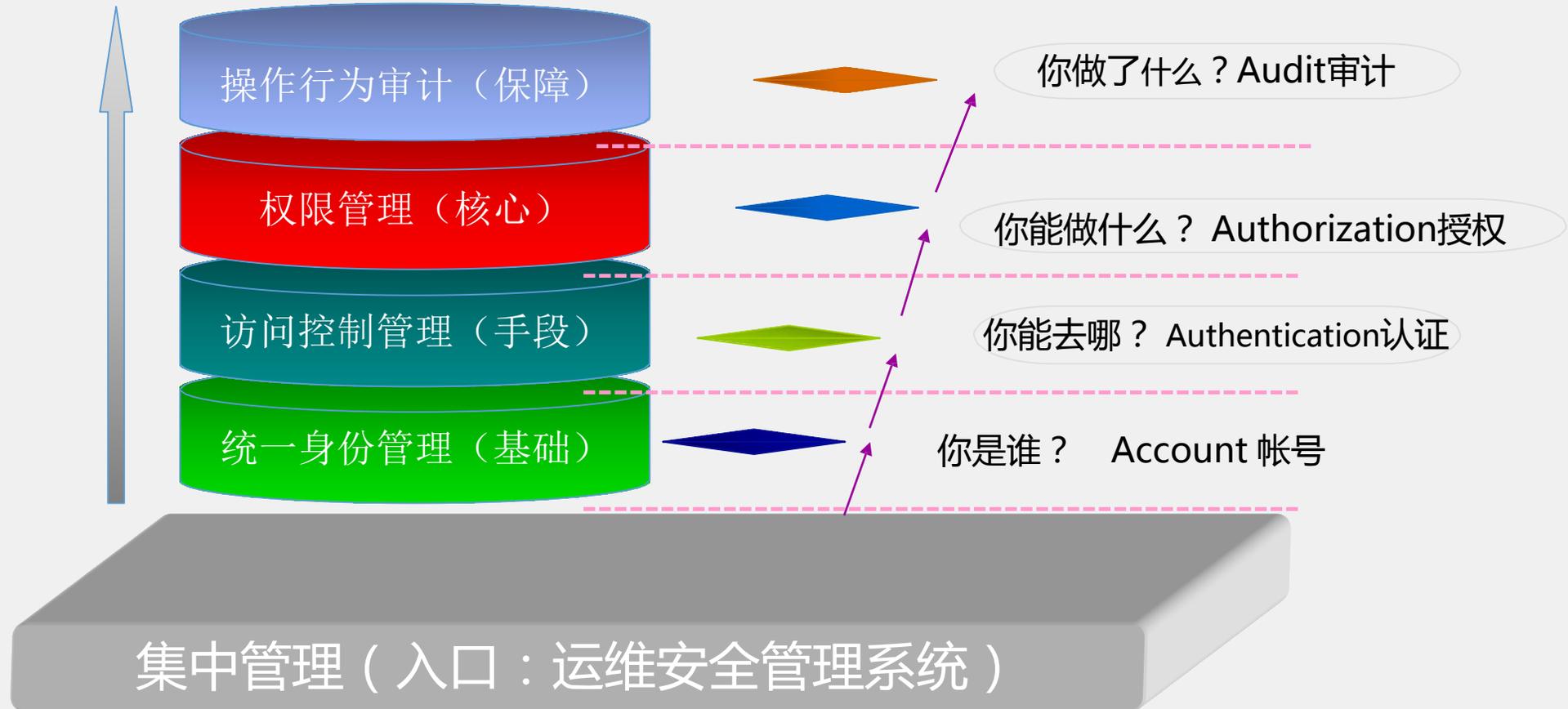
# 运维安全产品起源-解决实践



抗“疫”公益系列活动之二十（二）·



- 最终技术解法基于4A安全思想模型的技术框架





# 运维安全产品起源-发展历程





# 运维安全产品-技术现状

## 管理资源类型

服务器 ( Windows/Linux/Unix )

网络设备 ( 交换机/路由器 )

安全设备 ( 防火墙/IDS/IPS等 )

数据库 ( ORACLE/SQLserver/MYSQL/DB2/Informix/SYBASE )



Windows服务器



UNIX服务器



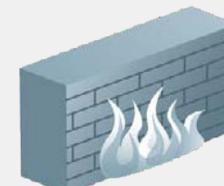
Linux服务器



交换机



路由器



防火墙



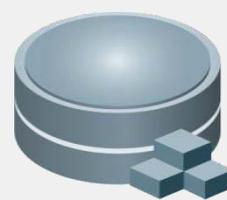
Informix数据库



Oracle数据库



SQL数据库



其他数据库

可以实现

集中认证

统一授权

单点登陆

访问控制

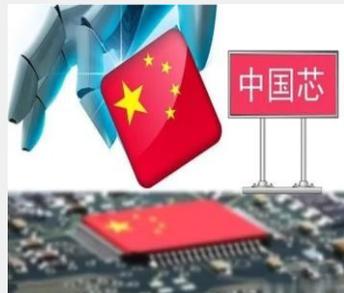
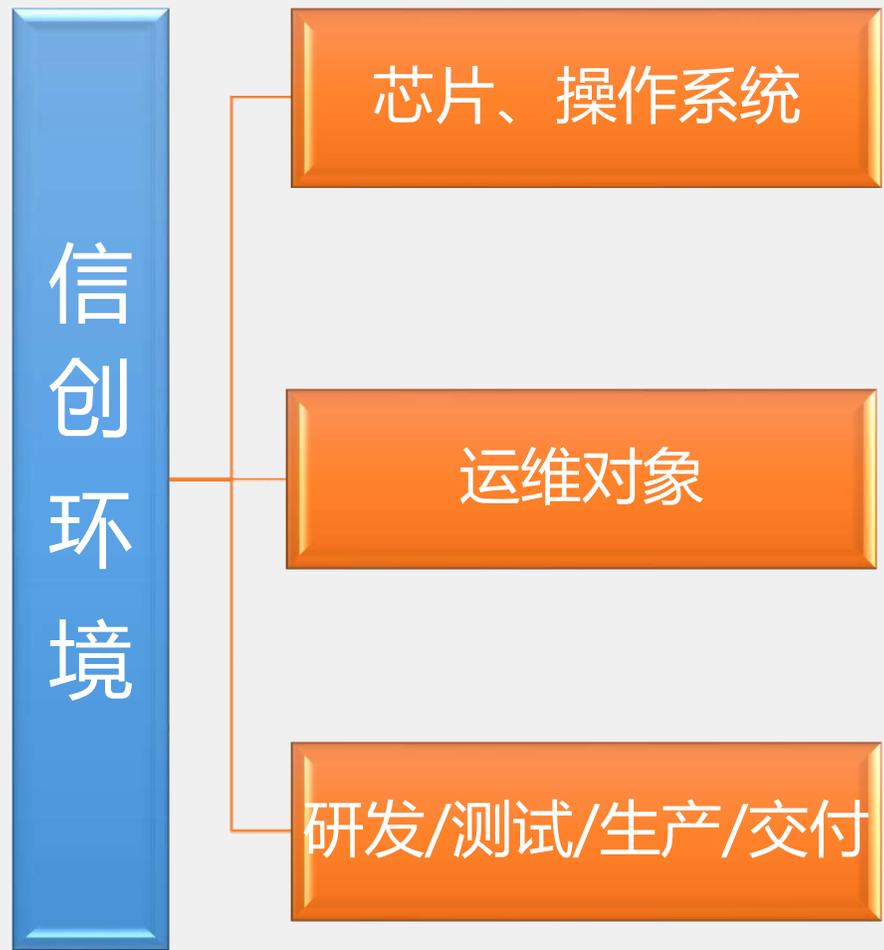
操作审计



图形终端运维审计	字符终端运维审计	数据库运维审计	文件传输操作审计	应用终端操作审计
RDP	Telnet	Oracle	FTP	AS400
X11	SSH	DB2	SFTP	HTTP
VNC		SQL Server	RDP磁盘通道	HTTPS
		Sybase	剪贴板	其他应用终端
		Informix		



# 信创环境下-对运维安全产品的要求



抗“疫”公益系列活动之二十（二）·



# 信创安全功能要求-运维用户管理

产品具备运维用户创建、属性设置；在限制管理IP功能基础上额外加测mac地址限制。

内控管理平台 - Mozilla Firefox

https://172.16.30.10/fort/

圣博润

安全管理员(安全操作员) | [fort1] | 个人信息维护 | 帮助 | 退出

首页 运维管理 流程控制 计划任务

组织定义 用户 资源 授权 规则定义

基本信息 角色信息

用户账号: test1 \* 只能输入数字、字母、下划线、小数点、中划线!

用户名称: test1 \* 只能输入数字、字母、汉字、小数点、中划线!

开始时间: [ ]

结束时间: [ ]

所属部门: ROOT部门 \*

口令: [ ] \*

手机: [ ]

电子邮箱: [ ]

通信地址: [ ]

登录时修改: [ ]

确认口令: [ ] \*

座机: [ ]

高级选项 >>

访问时间规则: 请选择

访问权限: 无

认证方式: 用户名+口令(默认方式)

mac地址: 请输入允许登录的mac地址,若有多个,请用“,”隔开,最多存储4个  
注: mac地址只能输入数字、字母。

访问地址规则: 请选择

保存 返回

抗“疫”公益系列活动之二十(二)



# 安全功能要求-运维对象管理

## 运维对象管理：创建、运维账户口令设置、改密等

浏览器地址: https://172.16.30.200/fort/

页面标题: 内控管理平台 - Mozilla Firefox

用户: 安全管理员(安全操作员) | [fort1] | 个人信息维护 | 帮助 | 退出

导航: 首页 | 运维管理 | 流程控制 | 计划任务

当前页面: 口令计划

- 口令计划
- 口令修改计划 ✓
- 口令备份计划
- 口令备份FTP

### 编辑口令修改计划

计划名称:  \* 只能输入数字、字母、汉字、下划线、中划线

---

#### 基本信息

所属部门:

执行方式: 一次性执行

执行时间:  \*

口令设置: 手动指定固定口令

口令设置:  口令确认:

发送方式: 邮件发送

密码包接收人: [+添加](#)

解密密钥接收人: [+添加](#)

#### 资源

资源/地址:  [Q检索](#) [刷新](#) [+添加资源](#) [删除资源](#)

<input type="checkbox"/>	资源	地址	设备类型	所属部门
资源组 <a href="#">+添加资源组</a>				

#### 资源账号

资源/地址:  账号:  [Q检索](#) [刷新](#) [+添加资源-账号](#) [删除资源-账号](#)

<input type="checkbox"/>	账号	资源	地址	设备类型	所属部门
--------------------------	----	----	----	------	------





# 安全功能要求-访问控制

可根据主体、客体、管理方式、操作命令、操作时间等设置访问控制策略

内控管理平台 - Mozilla Firefox

https://172.16.30.200/fort/

安全管理员(安全操作员) | [fort1] | 个人信息维护 | 帮助 | 退出

首页 运维管理 流程控制 计划任务

组织定义 用户 资源 授权 规则定义

规则定义

- 命令规则
- 时间规则 ✓
- 地址规则
- 资源时间规则

### 编辑时间规则

名称:  \* 只能输入数字、字母、汉字、下划线、中划线, 不能大于32位

部门:  \*

启动日:  \*

终止日:  \*

状态类型: 禁止使用

时间设置: 设置方式: 每星期

星期(可多选): 周一, 周二, 周三, 周四, 周五

小时(可多选): 00, 01, 02, 03, 04, 05

(使用【Ctrl】+【鼠标左键】进行多选或取消选中)

描述:





# 安全功能要求-操作审计-运维审计

对运维用户的操作进行审计，生成审计记录，包括操作时间、运维用户、源地址、运维对象、管理方式、操作内容、操作结果等，审计日志存储周期不小于6个月。

The screenshot shows a web browser window with the URL <https://172.16.30.200/fort/>. The page title is "内控管理平台 - Mozilla Firefox". The interface is for the "圣博润" (SBR-info) system. The main content area is titled "审计留存配置" (Audit Retention Configuration). Under the "空间腾退" (Space Reclamation) section, there is a label "当硬盘使用到达总硬盘数：" (When disk usage reaches total disk capacity:). A dropdown menu is set to "70%", with a red warning message: "时候 此处的百分比必须比告警配置中硬盘告警百分比大" (Time: This percentage must be larger than the disk alert percentage in the alert configuration). Below this, there are four radio button options:

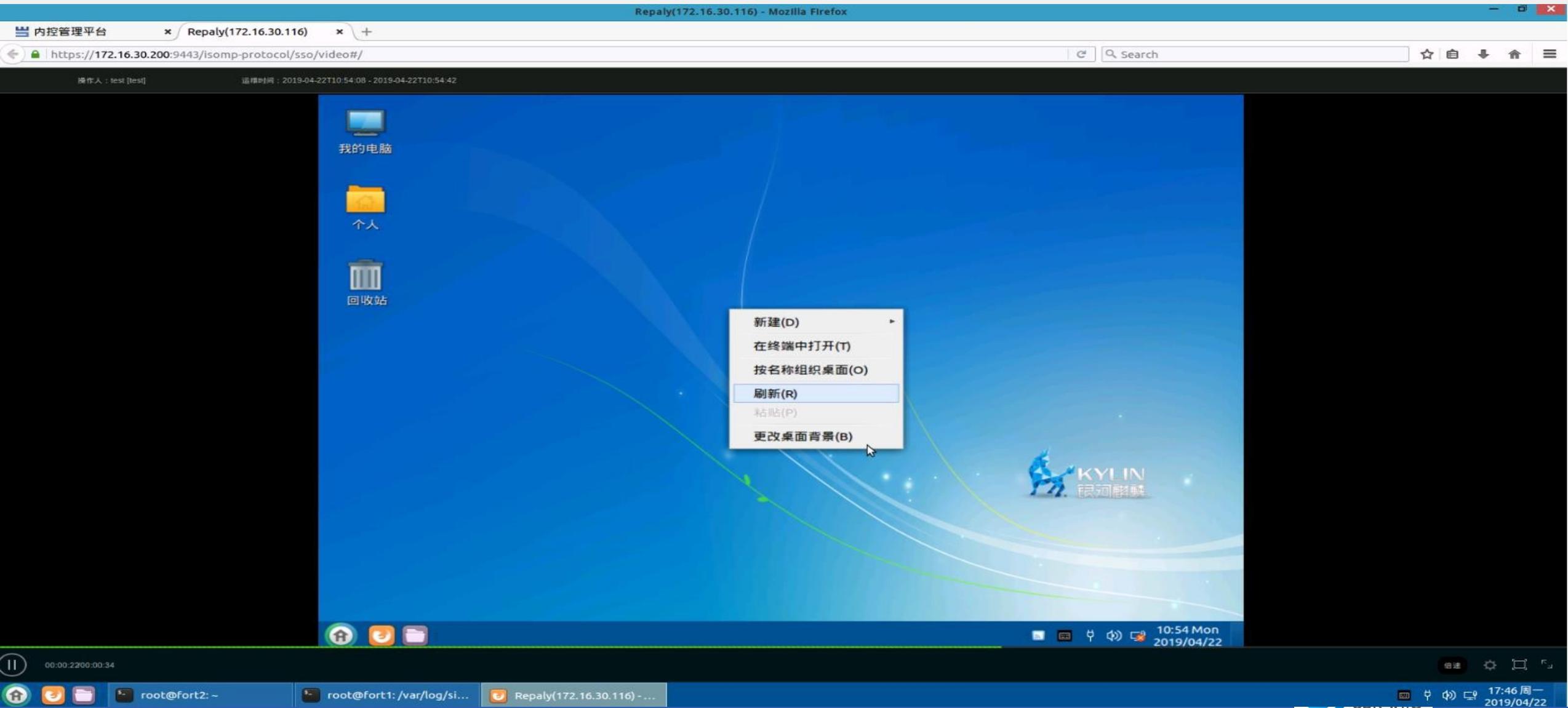
- 不再生成新记录的运维审计文件 (Do not generate new maintenance audit records)
- 删除最早一个月的运维审计文件 (Delete the earliest maintenance audit files of one month)
- 删除最早一天的运维审计文件 (Delete the earliest maintenance audit files of one day)
- 删除最早一个会话的运维审计文件 (Delete the earliest maintenance audit files of one session)

At the bottom right of the page, there is a button labeled "保存" (Save). The footer contains the text "抗“疫”公益系列活动之二十(二)" (Anti-Epidemic Public Welfare Series Activity No. 20(2)).



# 安全功能要求-操作审计-审计查阅

允许授权管理员查阅审计记录；报表支持通用格式导出：信创要求wps





# 安全功能要求-告警

## 依据告警策略对违规操作告警

内控管理平台 - Mozilla Firefox

https://172.16.30.200:444/fort/

安全审计员(安全审计员) [fort1] | 个人信息维护 | 帮助 | 退出

审计管理 报表管理

运维审计 配置审计 告警归纳

时间 请选择 请选择 请选择 类型 -请选择- 级别 -请选择-

Q检索

序号	时间	类型	资源/模块	用户	告警摘要	级别	状态	服务器名	告警内容
1	2019-04-22 14:29:17	登录认证失败次数过多	用户登录	test1	用户非法登录	DEBUG	未阅读	fort1	查看详情
2	2019-04-22 14:21:02	执行非法命令	命令黑名单	test	账号test, 命令越权(资源172.16.30.116)	DEBUG	未阅读	fort1	查看详情
3	2019-04-22 14:20:48	执行非法命令	命令黑名单	test	账号test, 命令越权(资源172.16.30.116)	DEBUG	未阅读	fort1	查看详情
4	2019-04-22 11:08:00	执行非法命令	命令黑名单	test	账号test, 命令越权(资源172.16.30.116)	DEBUG	已阅读 (安全审计员于1...	fort1	查看详情
5	2019-04-20 15:46:25	执行非法命令	命令黑名单	test	账号test, 命令越权(资源172.16.30.116)	DEBUG	未阅读	fort1	查看详情
6	2019-04-20 15:46:17	执行非法命令	命令黑名单	test	账号test, 命令越权(资源172.16.30.116)	DEBUG	未阅读	fort1	查看详情
7	2019-04-20 15:46:04	执行非法命令	命令黑名单	test	账号test, 命令越权(资源172.16.30.116)	DEBUG	未阅读	fort1	查看详情
8	2019-04-20 15:46:01	执行非法命令	命令黑名单	test	账号test, 命令越权(资源172.16.30.116)	DEBUG	未阅读	fort1	查看详情
9	2019-04-20 15:40:24	登录认证失败次数过多	用户登录	test	用户非法登录	DEBUG	未阅读	fort1	查看详情
10	2019-04-20 15:32:39	执行非法命令	命令黑名单	test	账号test, 命令越权(资源172.16.30.116)	DEBUG	已阅读 (安全审计员于1...	fort1	查看详情

首页 上一页 下一页 尾页

每页显示 10 条 共 1 页 当前第 1 页 去 1 页 跳转





# 安全功能要求





抱**圣**贤之思 怀**博**学之志 展**润**泽之力

## 专注运维操作领域

- ✓ 堡垒主机产品始于2007年
- ✓ 市场化时间超过10年
- ✓ 堡垒主机市场占有率连续5年第一
- ✓ 专注合规市场

## 专业&成熟

- ✓ 在设备规模超过100,000台的环境中部署
- ✓ 在全国范围超过30个分支节点的环境中部署
- ✓ 在超过8000个字符并发的环境中成功部署
- ✓ 产品最安全，不存在任何中高级安全漏洞

## 产品资质

- ✓ IT产品信息安全认证证书
- ✓ 信息技术产品安全测评证书，级别Eal3+
- ✓ 涉密信息系统产品检测证书
- ✓ AK名录

## 未来方向

- ✓ SAAS堡垒主机，高可靠，高扩展
- ✓ 对资产变化的感知能力，对IP、账号等具备实时发现，定期巡检的能力
- ✓ 适应移动时代的发展需要，由移动运维走向移动管理
- ✓ 自动化风险分析与评估，及时发现与管理风险



**快速服务电话 400-966-2332**  
**周经理 18588659288**



[www.sbr-info.com](http://www.sbr-info.com)

地址：北京市海淀区高梁桥斜街59号院2号楼3层

电话：010-82138088

技术支持热线：800-810-2332 / 400-966-2332

技术支持邮箱：[support@sbr-info.com](mailto:support@sbr-info.com)