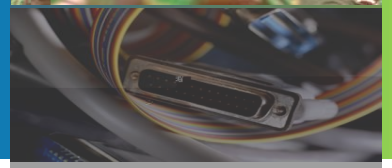
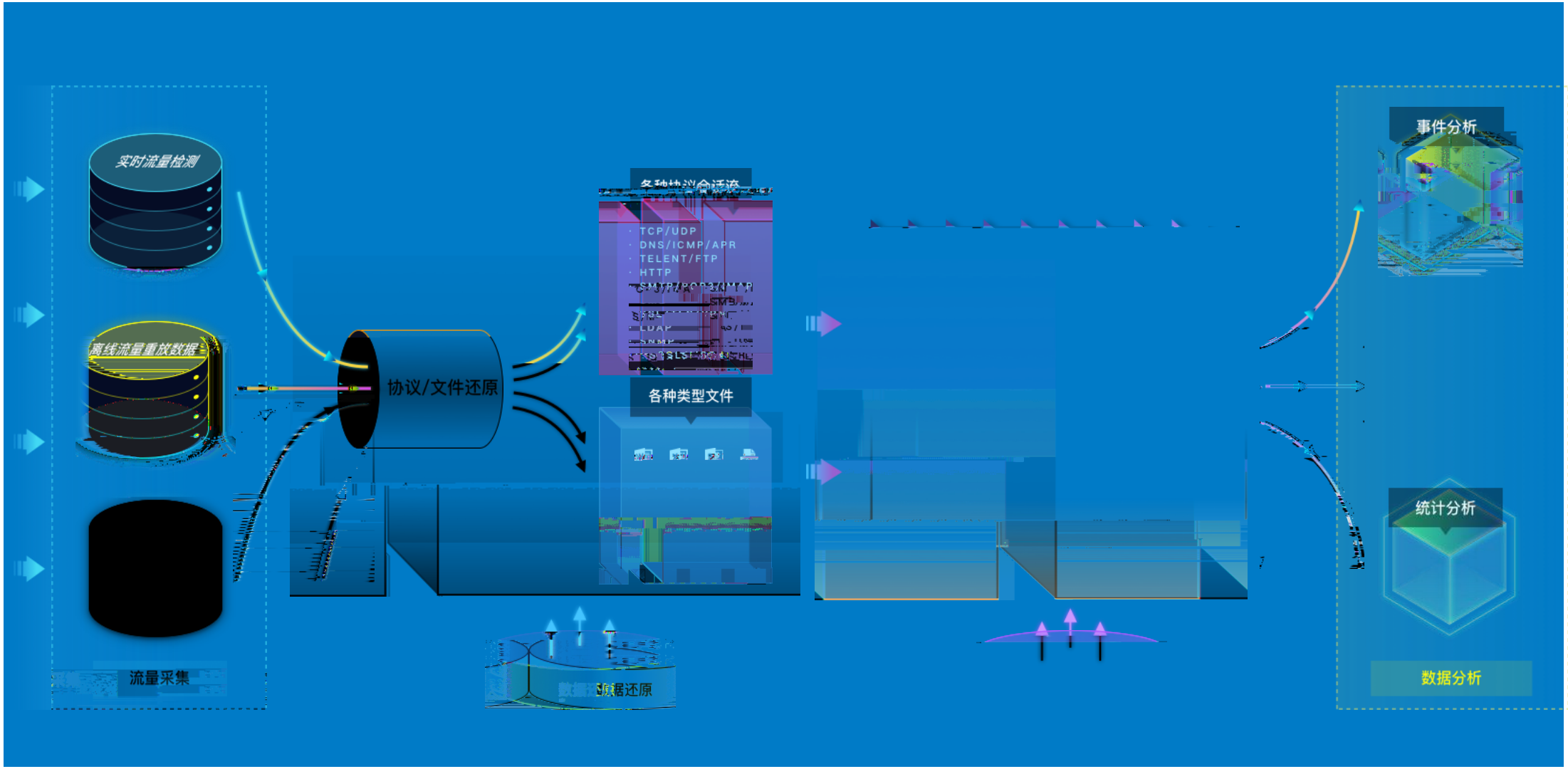
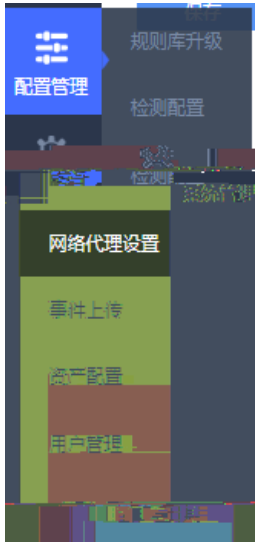


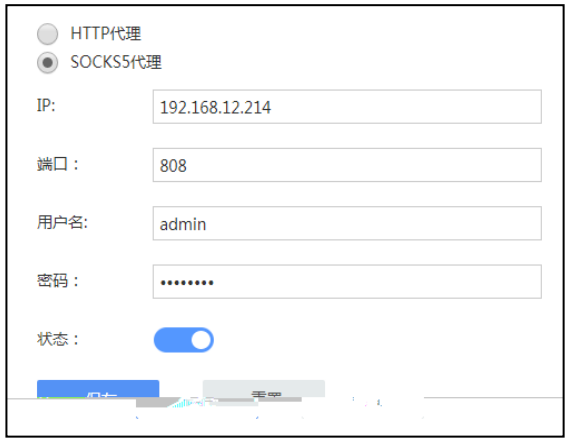
Contents

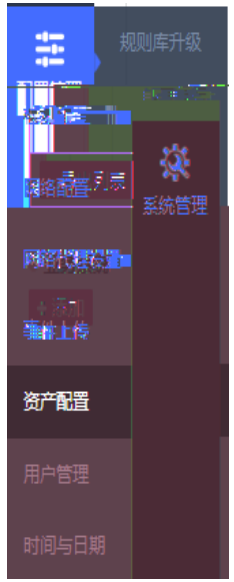

实时流量检测
离线流量重放数据
流量采集
协议/文件还原
· TCP/UDP
· DNS/ICMP/APR
· TELENT/FTP
· HTTP
各种类型文件
数据还原
事件分析
统计分析
数据分析

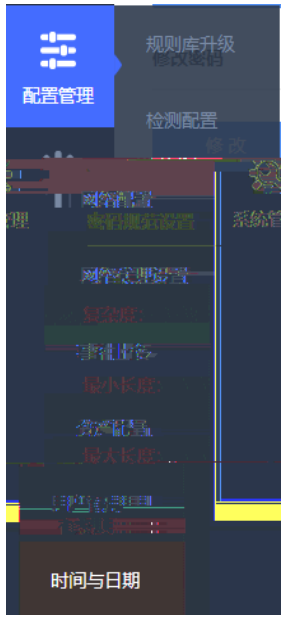
Contents


配置管理
规则库升级
检测配置
网络代理设置
事件上传


HTTP代理
SOCKS5代理
IP:
192.168.12.214
端口：
8080
状态：
保存
重置


HTTP代理
SOCKS5代理
IP:
192.168.12.214
端口：
808
用户名:
admin
密码：
状态：

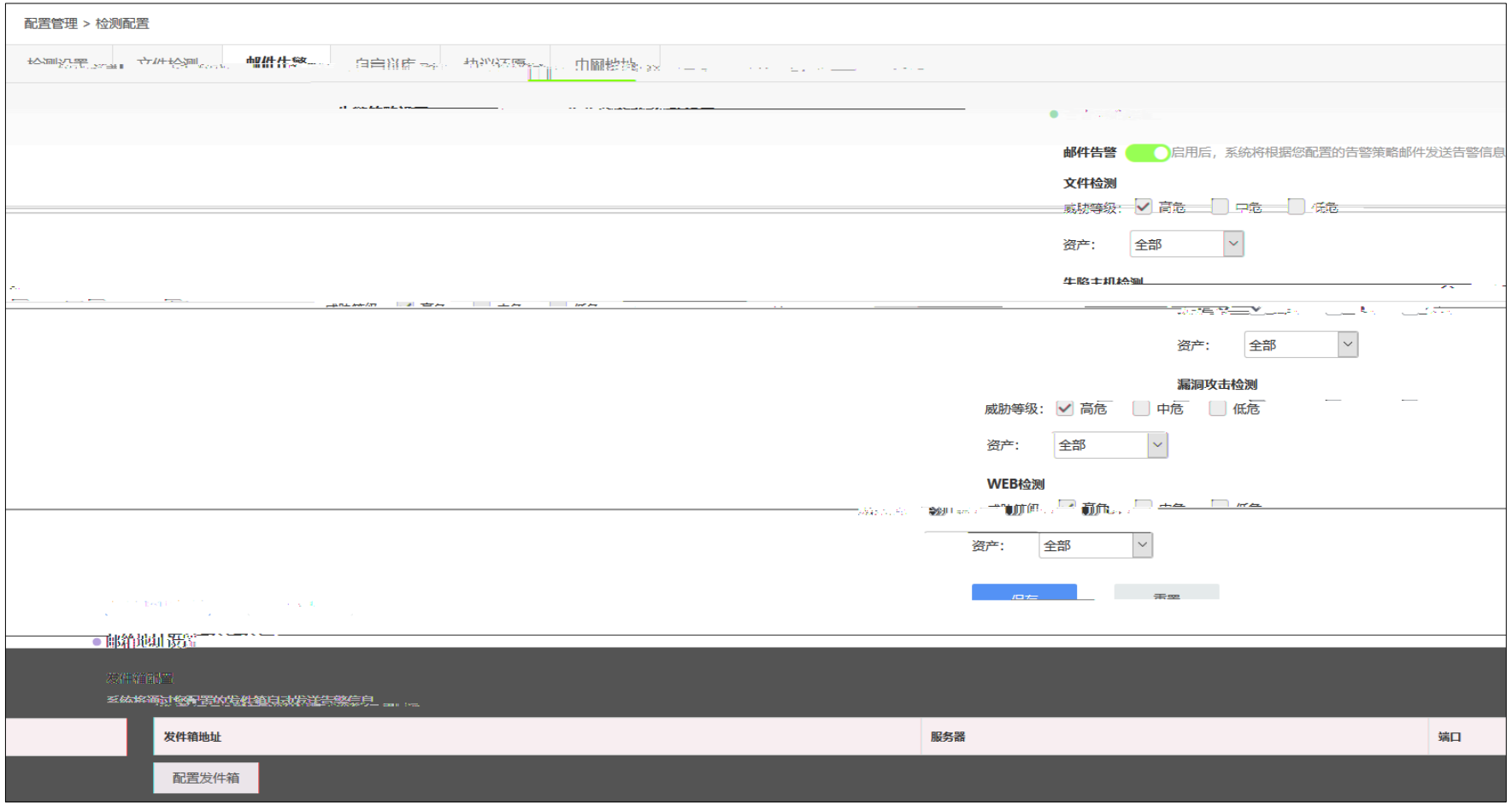

规则库升级
系统管理
资产配置
用户管理
时间与日期


配置管理
规则库升级
检测配置
时间与日期


系统信息 > 时间与日期
服务器时
设置
日期与时间
月
21日
15
44
2018年
设置
置
NTP服务设
添加
输入新增IP
操作
NTP Server
时间同步


规则库升级
配置管理
序号


配置管理 > 检测配置
检测设置
文件检测
邮件告警
自定义库
协议还原
内网地址
基础配置
检测类型设置
检测特征设置
自定义YARA检测规则
添加
搜索规则名称
规则名称
[+] test
继续添加
批量下载
批量删除

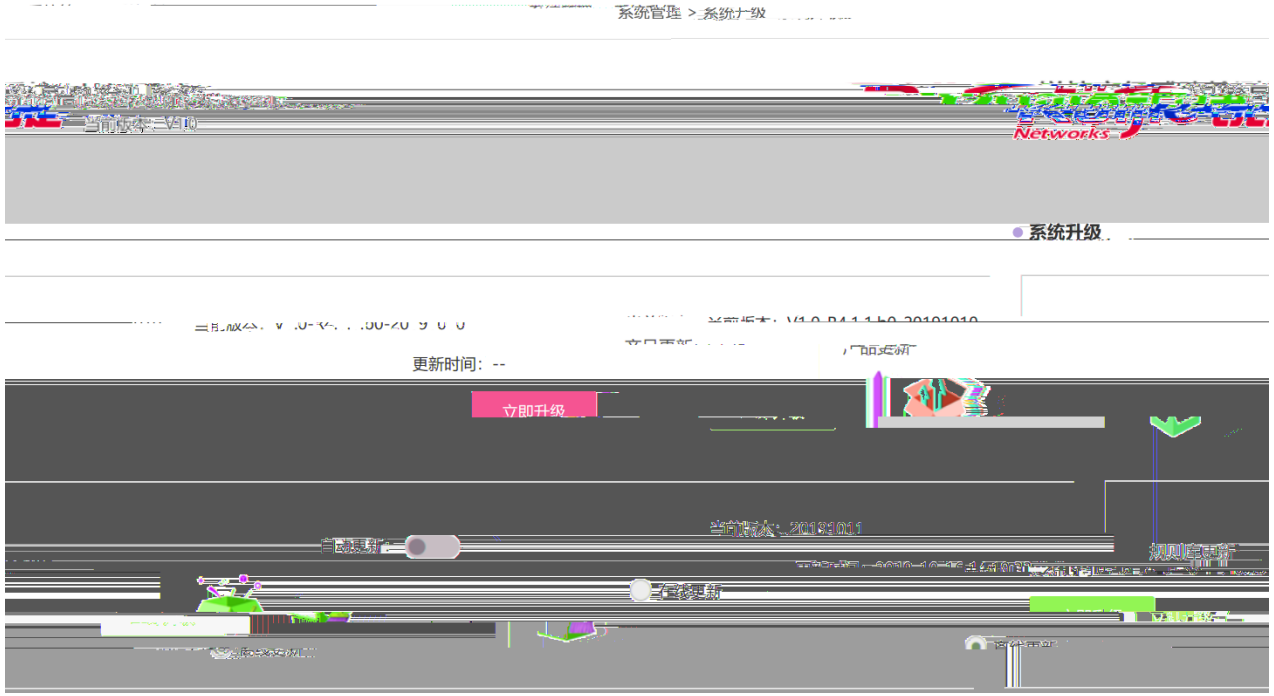

配置管理 > 检测配置
邮件告警
启用后，系统将根据您配置的告警策略邮件发送告警信息
文件检测
威胁等级：
高危
中危
低危
资产：
全部
漏洞攻击检测
威胁等级：
高危
中危
低危
资产：
全部
WEB检测
资产：
全部
发件箱配置
发件箱地址
服务器
端口
配置发件箱


检测设置
文件检测
邮件告警
自定义库
协议还原
内网地址
黑名单
黑IP
黑域名
黑URL
黑流量特征
黑文件HASH
还没有添加黑IP 点击添加
白名单
白IP
白域名
白文件HASH
还没有添加白IP
系统规则库
暂无被停用规则

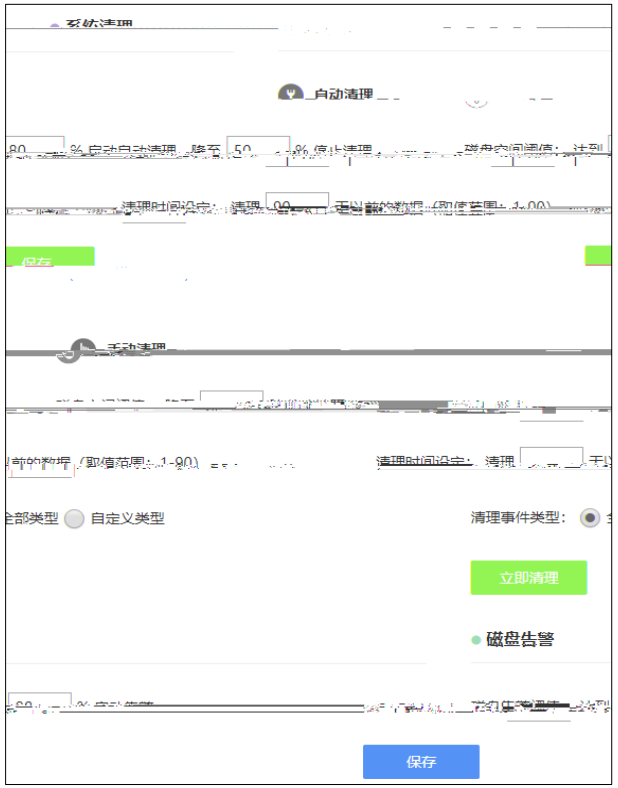

配置管理 > 检测配置
1M
保存
重置

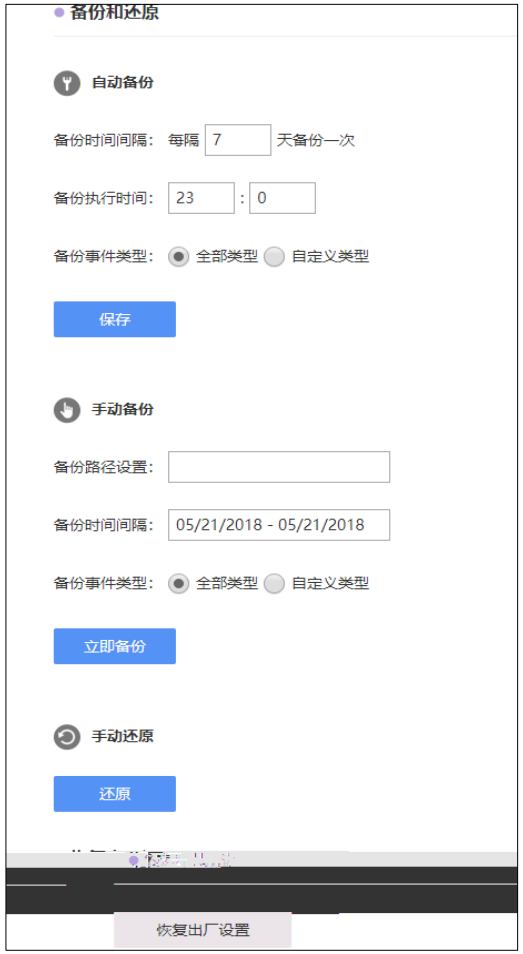

配置管理 > 检测配置
内网地址列表
10.0.0.0/8
IP/掩码
172.16.0.0/12
IP/掩码
192.168.0.0/16
IP/掩码

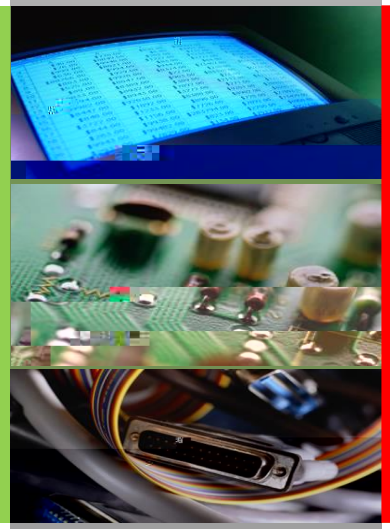

异常行为设置
系统升级
隐蔽信道
系统管理
系统维护
设备日志
异常协议
License信息
异常心跳

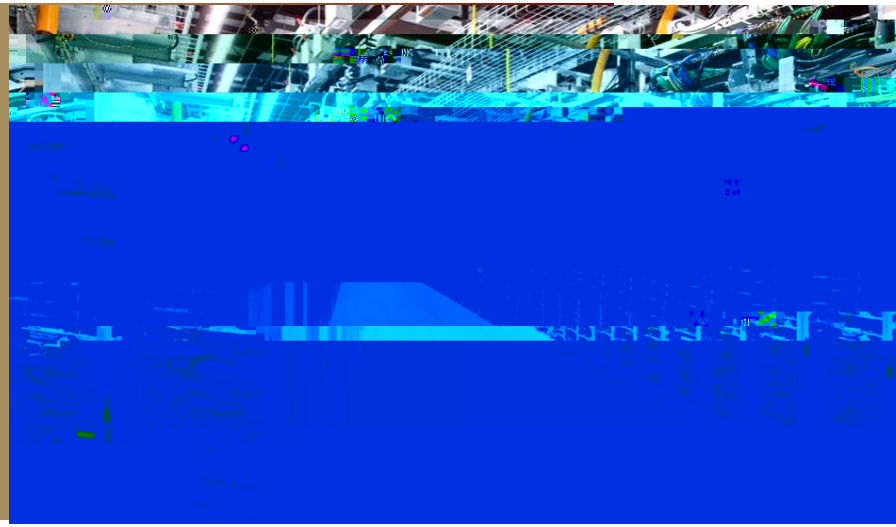

系统管理 > 系统升级
Networks
系统升级
更新时间：--
立即升级


系统升级
系统管理


自动清理
保存
手动清理
清理事件类型：
立即清理
磁盘告警
保存


备份和还原
自动备份
备份时间间隔： 每隔 7 天备份一次
备份执行时间： 23 : 0
备份事件类型： 全部类型 自定义类型
保存
手动备份
备份路径设置：
备份时间间隔： 05/21/2018 - 05/21/2018
备份事件类型： 全部类型 自定义类型
立即备份
手动还原
还原
恢复出厂设置





Ruijie Networks Certification Center

Addr: 29 A 11 100036

university.ruijie.com.cn