





BDS-A

CPU

" "

3









1 WEB BDS IP

https://192.168.0.100:8082

admin

ruijie123

2 " ">" "

3

- 账号口令管理
- 网络管理
- 系统工具
- 日期时间管理
- 数据备份
- 数据删除
- 系统恢复**
- 重置平台初始口令
- 系统停止和重启
- 系统信息

## 系统恢复

! 系统恢复至出厂设置，相应的生产数据将被清除，如硬件配置有变化，原license将不可用，请重新申请license!

系统恢复



1

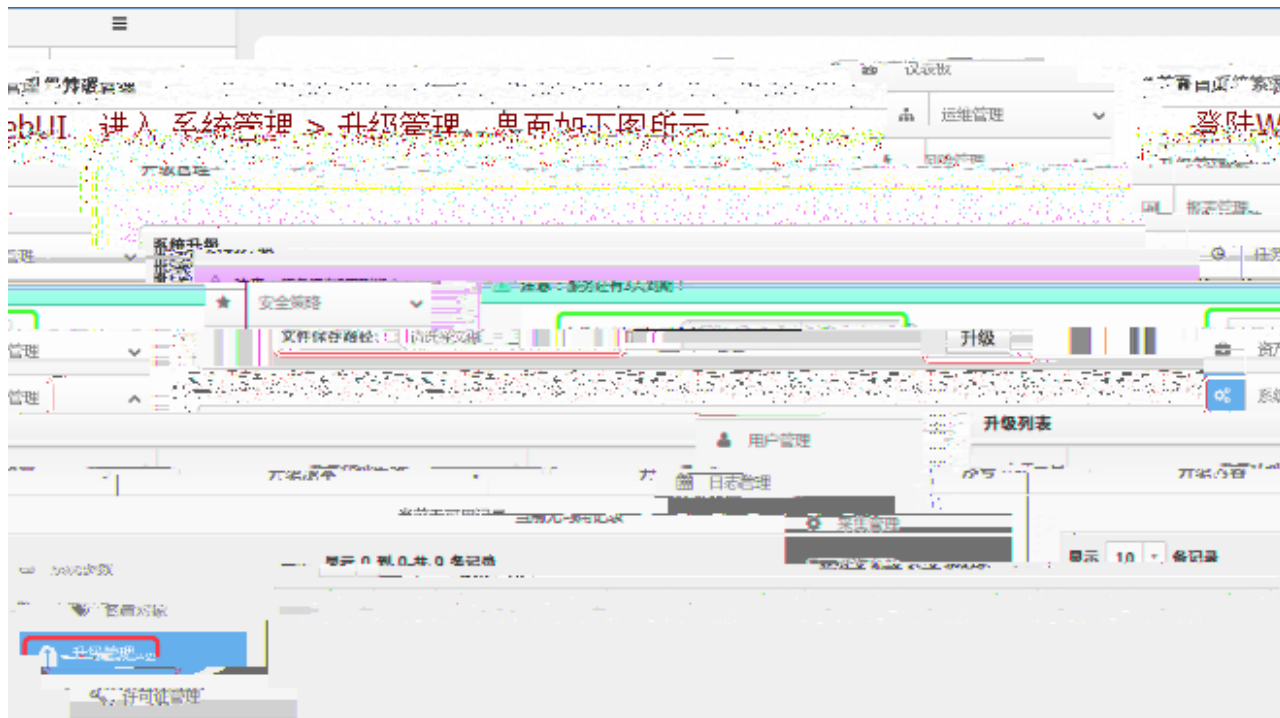
license

2

3

4

MD5







Unknown

1

Unknown

导出

序号	名称	类型	子类	严重级别	设备IP	时间
1	Unknown	其它	其它	信息	172.16.32.12	2016-11-15 06:47:40
2	Unknown	其它	其它	信息	172.16.32.12	2016-11-15 06:47:40
3	Unknown	其它	其它	信息	172.16.32.12	2016-11-15 06:47:40

事件显示为Unknown



导出Unknown的日志:

名称	类型	子类	严重级别	设备IP	时间	序号
Unknown	其它	其它	信息	172.16.32.12	2016-11-15 06:47:40	1
Unknown	其它	其它	信息	172.16.32.12	2016-11-15 06:47:40	2

将研发提供的标准化脚本, 通过"安全策略">"事件策略">"导入"

标准移 过滤

标准化策略列表

策略名称 应用系统

显示 10 条记录

common\_coll

The screenshot displays the Ruijie network management interface. At the top, a table lists several events. The first event is highlighted, and a red box around the '详细信息' (Details) button is connected by a red arrow to the text '点击查看详细信息' (Click to view details). Below the table, a detailed view of a collector is shown. A red box highlights the '采集器名称: comm\_coll' (Collector Name: comm\_coll) field, with a red arrow pointing to the text '显示为comm\_coll,说明没有正确匹配采集器' (Displayed as comm\_coll, indicating that no collector was correctly matched). The collector address is listed as 192.168.100.134.

序号	名称	类型	子类	严重级别	设备IP	时间
1	Unknown	其它	其它	信息	192.168.100.135	2016-12-15 20:18:00
2	Unknown	其它	其它	信息	192.168.100.135	2016-12-15 20:18:00
3	Unknown	其它	其它	信息	192.168.100.135	2016-12-15 20:18:00
4	Unknown	其它	其它	信息	192.168.100.135	2016-12-15 20:18:00
5	Unknown	其它	其它	信息	192.168.100.135	2016-12-15 20:18:00
6	Unknown	其它	其它	信息	192.168.100.135	2016-12-15 20:17:12
7	Unknown	其它	其它	信息	192.168.100.135	2016-12-15 20:17:12

采集器

采集器名称: comm\_coll      采集器地址: 192.168.100.134

采集器网络: 缺省网络

当前事件速率(0eps)

资产

资产列表

需要将该目标设备在此外进行增加资产

资产名称	资产IP	序号
2	电子病例	192.168.100.52
3	LIS	192.168.100.57
192.168.100.131		4
192.168.100.135		5
192.168.100.136		6
		netscreen-131
		PACSLIS
		Centos_19



当前事件速率(0eps)

资产

资产列表

需要将该目标设备在此外进行增加资产

资产名称	资产IP	序号
2	电子病例	192.168.100.52
3	LIS	192.168.100.57
192.168.100.131		4
192.168.100.135		5
192.168.100.136		6
		netscreen-131
		PACSLIS
		Centos_19



Ruijie 大数据安全平台

● 点击“展现模式”后，默认进入总览页面，该页面包含安全评分、漏洞数量top5、工单处理情况、告警类别分布以及安全评分趋势5个模块

安全评分: 93

漏洞数量: 1 亿 391 0万

工单处理: 64 / 43

告警类别分布: 27

查看全网安全概况，点击首页右上角“展现模式”可以进入：

● 点击右上角“实时攻击态势”，进入相应界面；该页主要以中国地图的方式呈现攻击源、攻击集中地等

攻击源: 2016-11-16  
源IP: 115.252.234.127  
源IP: 218.36.53.55

攻击地: 2016-11-16  
攻击地: 115.252.234.127

● 通过“资产安全态势”模块，可以查看资产安全风险的实时变化趋势

● 通过“资产安全态势”模块，可以查看资产安全风险的实时变化趋势

● 通过“资产安全态势”模块，可以查看资产安全风险的实时变化趋势

资产安全态势

资产安全态势

资产安全态势

资产名称	资产ID	操作系统	应用	风险等级	风险值	风险等级	风险值	风险等级	风险值
1 上海东方明珠	17715678	CenOS	nginx	高	97	0	44	中	97
2 上海东方明珠	17715679	Centos	nginx	中	52	0	35	中	45
3 上海东方明珠	17715680	CenOS	nginx	低	0	0	44	中	44
4 上海东方明珠	17715681	Centos	nginx	低	0	0	44	中	44
5 上海东方明珠	17715682	CenOS	nginx	低	0	0	44	中	44
6 上海东方明珠	17715683	Centos	nginx	低	0	0	44	中	44
7 上海东方明珠	17715684	CenOS	nginx	低	0	0	44	中	44
8 上海东方明珠	17715685	Centos	nginx	低	0	0	44	中	44
9 上海东方明珠	17715686	CenOS	nginx	低	0	0	44	中	44
10 上海东方明珠	17715687	Centos	nginx	低	0	0	44	中	44

安全指数



资产风险分布情况

资产风险排行TOP10

告警严重级别分布

告警严重级别分布 (最近24小时)

200

200

今日事件产

[www.ruijie.com.cn](http://www.ruijie.com.cn)

[www.ruijie.com.cn/service.aspx](http://www.ruijie.com.cn/service.aspx)

[bbs.ruijie.com.cn](http://bbs.ruijie.com.cn)

[webchat.ruijie.com.cn](http://webchat.ruijie.com.cn)

4008-111-000