



护网行动ESPC培训

绿盟科技版权所有

产品支持部 李倩



CONTENTS 目录 >>>

- 01 ESPC工作原理介绍
- 02 设备管理功能介绍
- 03 日志、报表功能介绍
- 04 告警平台功能介绍



01

ESPC工作原理介绍

▶▶ **ESPCV7是（绿盟企业安全中心）**一款Linux产品，它是绿盟科技安全产品的统一管理平台。

功能：设备管理、日志报表、告警平台、策略管理、资产管理、用户管理、系统管理、级联功能等。



功能模块介绍



服务器配置要求

	性能规格	小数据低配	小数据推荐	大数据低配	大数据高配
硬件规格	CPU	I7 系列 4核心 8线程	E5 系列 8核心 16线程	E5 系列 12核心 24线程	E5 系列 16核心 32线程
	内存	16G	32G以上	48G	64G以上
	硬盘 (可用空间)	500G及以上	1T及以上	2T及以上	4T及以上
部署	部署模式	小数据	小数据	大数据	大数据
	数据库	<u>postgresql</u>	<u>postgresql</u>	<u>postgresql+hive</u>	<u>postgresql+hive</u>

建议使用的浏览器：Chrome 最新版、Firefox 最新版、IE 11



大数据和小数据处理对比

- 大数据处理模式：设备的安全日志是存储HDFS，其它数据包括审计日志、用户信息和模块的运行数据仍然存储在postgres中。
- 小数据处理模式：所有数据存储在postgres中。

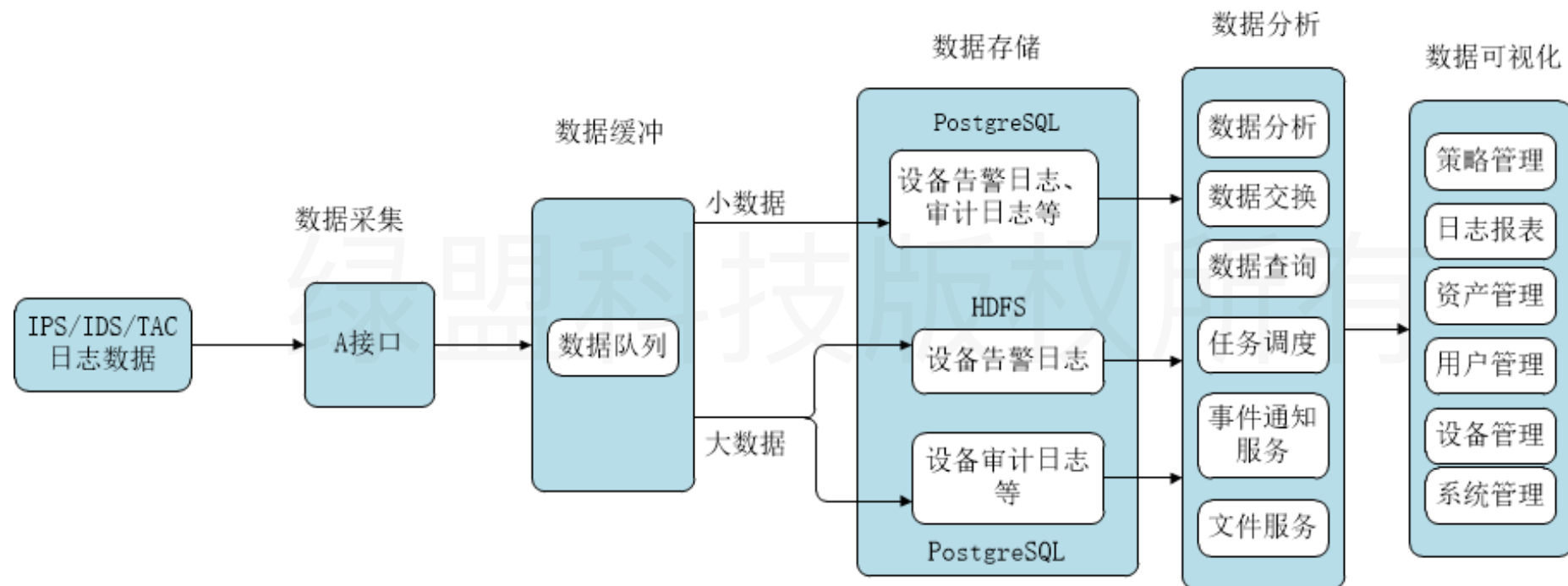
10.5.16.20

数据接入	数据存储	数据处理	应用容器	基础服务	☐
Kafka ●	Redis ●	小数据处理 ●	应用进程管理器 ●	HTTP服务器 ●	☐
NPAI-V2 ●	postgreSql ●			业务服务器 ●	
NPAI-V3 ●	存储服务 ●			业务组件 ●	
	注册中心 ●				

10.5.16.17

数据接入	数据存储	数据处理	应用容器	基础服务	☐
Kafka ●	HDFS ●	Hive ●	应用进程管理器 ●	HTTP服务器 ●	☐
NPAI-V2 ●	Redis ●	Spark ●		业务服务器 ●	
NPAI-V3 ●	postgreSql ●	大数据处理 ●		业务组件 ●	
	存储服务 ●	小数据处理 ●			
	注册中心 ●				

数据处理流程





02

设备管理功能介绍

设备联动

第一步：设备上添加ESPC的地址

适用于NIPS/NIDS V5.0R06F10、
TACV2.0R01F00SP01等新A接口设备

NIPS

云数据中心

本地IP地址 192.168.255.209

绿盟云安全中心(ESPP)

espp.api.nsfocus.com 启动

企业安全中心(ESPC)

服务端IP	10.5.16.20	端口	443	<input checked="" type="checkbox"/> 启动	✓ 已连接
服务端IP	10.5.16.17	端口	443	<input checked="" type="checkbox"/> 启动	正在连接
服务端IP		端口	443	<input type="checkbox"/> 启动	
服务端IP		端口	443	<input type="checkbox"/> 启动	

大数据安全分析(BSA)

服务端IP	10.5.16.12	文件端口	5050	安全日志(JSON)端口	50
服务端IP		文件端口	5050	安全日志(JSON)端口	50
服务端IP		文件端口	5050	安全日志(JSON)端口	50
服务端IP		文件端口	5050	安全日志(JSON)端口	50

点击**确定**生效

适用于NIPS/NIDS V5.6.7-5.6.9等老A
接口设备

NIPS

安全中心

基本配置

本地IP地址 192.168.255.33

绿盟云安全中心地址 espp.api.nsfocus.com 启动

绿盟企业安全中心地址1 10.5.16.20 启动 ✓ 已连接

绿盟企业安全中心地址2 启动

绿盟企业安全中心地址3 启动

绿盟企业安全中心地址4 启动

确定

高级选项 ▶

其他配置

接口版本 1.1.3.59107

重启引擎生效



设备联动

第二步：稍后，发现ESPC上注册成功

The screenshot displays the ESPP/ESPC management interface. At the top, there's a navigation bar with 'ESPC 设备管理' and a search filter for '设备名称、设备IP'. Below this, there are summary cards for '全部 (1)' and 'IPS (1)', each showing 1 green and 0 red device icons. A table lists the devices, with one entry 'IPS:192.168.255.209' highlighted in red and marked as '最新'. A notification bell icon with a '2' badge is visible in the bottom right of the main area. The '消息中心' (Message Center) at the bottom shows two messages: '设备注册成功(IPS: 192.168.255.209)' and '同步设备信息成功(IPS:192.168.255.209)', both highlighted in red. On the right, the 'NIPS' configuration page is partially visible, showing settings for '企业安全中心(ESPC)' with two active service IP addresses (10.5.16.20 and 10.5.16.17) on port 443, both marked as '已连接'.

设备名称	设备IP	类型
IPS:192.168.255.209 最新	192.168.255.209	IPS

消息	内容
设备消息	设备注册成功(IPS: 192.168.255.209)
设备消息	同步设备信息成功(IPS:192.168.255.209)

设备列表展示内容

- **最新**：设备刚接入，执行修改设备基本信息，查看了证书信息、启用、禁用等操作后，“最新”标签消失
- **升级**：升级包管理中下载了该设备可升级的升级包

The screenshot displays the ESPC (Endpoint Security Platform Controller) interface for device management. The main content area shows the details for a device with IP 192.168.255.209. The interface is divided into two main sections: '设备基本信息' (Device Basic Information) and '设备版本信息' (Device Version Information).

设备基本信息 (Device Basic Information):

设备 IP	192.168.255.209	设备名称	IPS:192.168.255.209
设备状态	正常	设备端口	443
设备类型	IPS	NAT IP	
设备 HASH	B90A-39EF-44CF-EE0C	硬件 HASH	B90A-39EF-44CF-EE0C
当前版本	5.6.10	出厂版本	V5.6R10F
A 接口版本	3.0.0.27248	是否虚拟设备	否
最近升级时间	2015-12-03 16:04:22	安装时间	
ESPC 可配置数目	4	ESPC 配置列表	10.5.16.20, 10.5.16.17
备注			

设备版本信息 (Device Version Information):

系统规则	V5.6R10F13059
固件	V5.6R10F00
引擎	V5.6R10F00SP00
病毒特征库	V5.6R10F25094

The interface also includes a sidebar with navigation options: 设备管理 (Device Management), 全局策略 (Global Policy), 升级包管理 (Upgrade Package Management), and 配置备份 (Configuration Backup). A '添加设备' (Add Device) button is located in the top right corner. A red box highlights the '操作' (Operations) menu on the right side of the device details table, which contains options for '配置设备' (Configure Device).

配置设备网络、路由、DNS等

设备名称	设备IP	类型	当前版本	内存	CPU	流量	状态	操作
TAC:192.168.255.39 升级	192.168.255.39	TAC	2.0.1	3%	22%	676bps/0bps	正常	配置设备
IPS:192.168.255.209 升级	192.168.255.209	IPS	5.6.10	76%	15%	9.8Kbps/0bps	正常	配置设备

ESPC 绿盟企业安全中心

设备列表 设备名称: IPS:192.168.255.209 返回上级

[网络配置](#) [路由配置](#) [DNS 配置](#) [系统服务配置](#) [升级策略配置](#) [配置备份](#) [设备告警](#) 应用配置

接口名称	工作模式	接口类型	IPV4 地址	IPV4 子网掩码	IPV4 网关	传输速率 (Mbps)	操作
M	全双工	管理口	192.168.255.209	255.255.255.0	192.168.255.54	1000	
G1/1	自动	采集口	0.0.0.0	0.0.0.0	0.0.0.0	0	
G1/2	自动	采集口	0.0.0.0	0.0.0.0	0.0.0.0	0	
G1/3	自动	采集口	192.168.1.2	255.255.255.0	192.168.1.1	0	

设备告警（针对单台设备）

功能介绍：若开启该功能，则当设备的CPU、内存、磁盘等达到阈值时便会发出告警。告警方式可选，可配置邮件告警或声音告警。

The screenshot displays a web-based network management interface. On the left, a sidebar menu includes '设备管理' (Device Management), '设备列表' (Device List), '设备拓扑' (Device Topology), and '设备状态' (Device Status). The main content area is titled '设备列表' (Device List) and shows a table of devices. The selected device is '设备名称: IPS:192.168.17.76' with a status of '正常' (Normal). A '配置设备' (Configure Device) button is highlighted in red in the top right corner of the table. Below the table, a configuration panel for the selected device is shown. The '设备告警' (Device Alert) tab is selected and highlighted in red. The '单设备是否启用' (Enable for single device) toggle switch is turned 'ON' and is also highlighted in red. Under the '离线告警配置' (Offline Alert Configuration) section, the '告警方式' (Alert Method) is set to '声音' (Sound). Under the 'CPU 告警配置' (CPU Alert Configuration) section, the 'CPU 告警' (CPU Alert) is set to '关闭' (Off), the '告警阈值' (Alert Threshold) is set to 95%, and the '告警方式' (Alert Method) is set to '声音' (Sound).

设备名称	状态	操作
设备名称: IPS:192.168.17.76	正常	配置设备
	正常	配置设备

网络配置 | 路由配置 | DNS 配置 | 系统服务配置 | 升级策略配置 | 配置备份 | 设备告警

单设备是否启用 ON

离线告警配置

告警方式 邮件 声音

CPU 告警配置

CPU 告警 开启 关闭

告警阈值 95 %

告警方式 邮件 声音



设备历史状态查询

- 可以展示设备CPU状态历史趋势、内存状态历史趋势、磁盘状态历史趋势、CF卡状态历史趋势、流量状态历史趋势

The screenshot displays a web interface for device management. On the left is a sidebar menu with options: 设备管理 (Device Management), 全局策略 (Global Policy), 升级包管理 (Upgrade Package Management), 配置备份 (Configuration Backup), and 云平台管理 (Cloud Platform Management). The main content area is titled '设备状态' (Device Status) and includes a search box with the IP address '192.168.17.76'. Below the search box are two date pickers: '开始' (Start) set to '2019-04-02 04:12:00' and '截止' (End) set to '2019-05-10 16:10:02'. A green '查询' (Query) button is positioned below the date pickers. Underneath, there is a section for 'CPU 状态历史趋势' (CPU State Historical Trend) which contains a line graph. The graph shows a red line with two data points, indicating a downward trend in CPU state over time. The y-axis is labeled with values 8 and 10.

开始	截止
2019-04-02 04:12:00	2019-05-10 16:10:02

查询

CPU 状态历史趋势

时间	状态值
2019-04-02 04:12:00	~9.5
2019-05-10 16:10:02	~8.0

▶▶ 全局策略-设备升级（针对所有设备）

- 只检查不下载：检查到有新的升级包时，会通知用户。
- 检查并下载：检查到有新的升级包时，会将升级包下载到ESPC服务器，并通知用户。
- 下载并升级：检查到有新的升级包时，会将升级包下载到ESPC服务器，并自动升级安全设备。

The screenshot shows the ESPC Device Management interface. The top navigation bar includes 'ESPC' and '设备管理'. The left sidebar contains '设备管理', '全局策略', '升级包管理', and '配置备份'. The main content area is titled '全局策略' and features a sub-menu with '系统配置', '设备升级' (highlighted with a red box), '配置备份', and '设备审核'. The '设备升级' section includes the following settings:

- 自动升级: 开启 关闭
- 升级方式: 只检查不下载 检查并下载 下载并升级
- * 升级站点:
- 更新时间:
- 使用代理: 否 是

A green '保存' (Save) button is located at the bottom of the configuration area.

全局策略-告警（针对所有设备）

The screenshot displays the ESPC (绿盟企业安全中心) configuration interface. The main header shows 'ESPC 设备管理' and '绿盟企业安全中心'. The left sidebar contains navigation options: '设备管理', '全局策略' (highlighted with a red box), '升级包管理', '配置备份', and '云平台管理'. The main content area is titled '设备列表' and shows the device name '设备名称: IPS:192.168.255.209'. A '返回上级' button is located in the top right corner. Below the device name, there are tabs for '网络配置', '路由配置', 'DNS 配置', '系统服务配置', '升级策略配置', '配置备份', and '设备告警' (highlighted with a red box). The '设备告警' section includes a toggle switch for '单设备是否启用' (ON), which is also highlighted with a red box. Below this, there are configuration sections for '离线告警配置' and 'CPU 告警配置'. The '离线告警配置' section shows '告警方式' with radio buttons for '邮件' and '声音'. The 'CPU 告警配置' section shows 'CPU 告警' with radio buttons for '开启' and '关闭', and a '告警阈值' slider set to 95%. At the bottom, there is a '告警方式' section with radio buttons for '邮件' and '声音' (checked), and an '应用配置' button.



03

日志、报表功能介绍

日志查询功能说明

- 日志类型依据联动的设备不同，展示的也不同。
- 日志查询拥有“高级查询”功能，可选择动作、危险程度等，也可根据事件的名称、源目的IP等进行查询。
- 日志显示的表格列支持自定义，可任意选择查看哪几项，最多支持同时查看6项内容。
- 表格列的右上方有“日志导出”功能，支持将日志以excel格式导出，最多导出10W条。
- 表格列的下方有获取日志总数按钮，点击可获取日志总数。

绿盟科技版权所有



日志查询

ESPC 绿盟企业安全中心

入侵防护事件

开始 2017-06-18 15:19:37 截止 2017-06-18 16:19:37 查询 高级查询

基础检索

上报设备 192.168.255.134, ... (8)

动作 允许 阻断 旁路阻断 隔离

危险程度 低风险 中风险 高风险

流行程度 高 中 低

攻击手段 拒绝服务攻击 获取权限攻击 信息收集行为 可疑网络活动
 网络操作监控

服务类型 www CGI FTP TELNET

事件检索

事件名称

协议摘要

日志导出

出全部 (Excel)

动作
允许

手动报表

- 支持IPS/IDS、SAS、NF、SAS-H、WAF 手动报表生成（报表模板内置，不支持自定义）
- 生成的报表在报表任务列表中查看和下载

The screenshot displays the ESPC (绿盟企业) web interface. The top navigation bar includes the ESPC logo and the NSFOCUS brand. The main content area is titled "入侵防护报表" (Intrusion Protection Report) and shows a report for the period "2017-06-17 17:55:40 ~ 2017-06-18 17:55:40". A sidebar on the left contains navigation options: "报表管理", "报表任务", "周期任务", and "过滤条件".

A file dialog box is open in the foreground, titled "正在打开 入侵防护报表.zip". The dialog shows the file "入侵防护报表.zip" with a size of 339 KB and a source of "https://10.5.16.19". The user is prompted to choose how to handle the file, with "保存文件(S)" (Save file) selected. The save location is "C:\Users\nsfocus\Desktop".

On the right side of the interface, there is a vertical menu with a red box highlighting the "报表" (Reports) section. Below this menu, a table is partially visible, showing columns for "攻击手段" (Attack Method) and "事件次数" (Event Count).

攻击手段	事件次数
拒绝服务攻击	0

周期报表

- 支持IPS/IDS、SAS、NF、SAS-H、WAF 周期报表生成
- 周期报表每执行一次生成一个子任务，每次执行的报表结果在子任务列表中查看和下载

ESPC 绿盟企业安全中心

周期任务

【入侵防护报表】的子任务列表

返回上级

批量删除

<input type="checkbox"/>	任务名称	检索时间	执行状态	执行时间	操作
<input type="checkbox"/>	入侵防护报表	开始时间：2017-06-17 15:47:00 结束时间：2017-06-18 15:47:00	✓ 运行成功	开始时间：2017-06-18 15:47:00 结束时间：2017-06-18 15:47:05 总耗时：5秒	删除任务 查看在线报表 下载HTML报表 下载WORD报表 下载PDF报表
<input type="checkbox"/>	入侵防护报表	开始时间：2017-06-16 15:47:00 结束时间：2017-06-17 15:47:00	✓ 运行成功	开始时间：2017-06-17 15:47:00 结束时间：2017-06-17 15:47:05 总耗时：5秒	删除任务 查看在线报表 下载HTML报表 下载WORD报表 下载PDF报表

许可协议 | 文档下载 | 关于 | 绿盟科技版权所有©2016

▶▶ 报表过滤

- 将常用报表内容过滤条件保存成过滤器，生成手动报表/周期报表时直接引用

The screenshot shows the ESPC (绿盟企业安全中心) interface. The top navigation bar includes the logo 'ESPC 绿盟企业安全中心' and icons for home, edit, notifications (1), and user profile. The left sidebar contains menu items: '报表管理', '报表任务' (highlighted with a red box), '周期任务', and '过滤条件'. The main content area shows a configuration form for a report task. It includes fields for '开始时间' (Start Time) and '结束时间' (End Time), both set to 2017-06-17 18:42:35. Below these is a modal window titled '从已保存的过滤器中选择' (Select from saved filters). The modal contains a table with the following data:

	名称	创建时间	描述
<input checked="" type="radio"/>	111	2017-06-18 18:41:12	
<input type="radio"/>	test	2017-06-18 18:15:59	

Below the table is a pagination control showing '1' of 1 pages. At the bottom right of the modal, the '确定' (Confirm) button is highlighted with a red box, and the '取消' (Cancel) button is also visible. Below the modal, there are radio button options for '动作' (Action) and '危险程度' (Risk Level):

- 动作: 允许, 阻断, 旁路阻断, 隔离
- 危险程度: 高风险, 中风险, 低风险

At the bottom of the page, there is a footer with the text: '许可协议 | 文档下载 | 关于 | 绿盟科技版权所有©2016'. A small JavaScript error message 'javascript:void(0);' is visible in the bottom left corner.



04

告警平台功能介绍

绿盟科技版权所有



事件告警配置

ESPC v7.0R00F03版本新增告警平台模块，支持针对部分告警事件进行邮件通知。具体配置方法如下：

告警中心

告警配置

告警监控

启用

* 规则名称 test-低

* 统计时间 请选择检查点

通知方式

告警级别

* 规则描述

* 统计规则

* 发生次数

* 过滤条件

危险程度

事件名称

目的 MAC

源 MAC

目的地址

流行程度

目的端口

VLAN ID

事件次数

攻击手段

动作

源地址

服务类型

规则编号

源端口

网络接口

协议摘要

操作符	检查条件	操作
=	低风险	

添加检查点

告警配置-说明

➤ **统计规则**：分为计数和求和两种；

统计规则选择计数时：

指的是对匹配上规则的事件进行计数。比如：若配置的是统计规则编号为10000的日志在30分钟内发生了K次就告警，进行匹配时是当有一条规则编号为10000的日志发生一次就计数一次，最后将30分钟内该事件发生的次数进行求和M。若最后 $M \geq K$ ，则就产生告警，若 $M < K$ 则不告警。

统计规则选择求和时：

指的是对匹配上规则的事件的求和字段进行求和，统计其阈值。比如：若配置的是统计规则编号为10000的日志在30分钟内危险程度阈值超过K时就告警，进行匹配时是当有一条规则编号为10000的日志发生一次统计其危险程度的值一次（比如高：3中：2低1），若30分钟内该事件的危险程度，高危险的发生了A次/中危险的发生了B次/低危险的发生了C次。则在这30分钟内，该事件危险程度的总统计值为 $M=3A+2B+C$ 。若最后 $M \geq K$ ，则就产生告警，若 $M < K$ 则不告警。

➤ **过滤条件**：对日志事件的一些过滤条件，最多可以建5条，这些过滤条件之间是与的关系，即需要同时满足这些过滤条件。

求和时统计字段对应的数值

类型	字段	数值
入侵防护日志	<u>gr_pop</u> (流程度)	1-高; 2-中; 3-低; 4-其他
	<u>gr_type</u> (攻击手段)	16-拒绝服务攻击; 32-获取权限攻击; 48-信息收集行为; 64-可疑网络活动; 80-网络操作监控
	action(动作)	1-允许; 2-阻断; 3-旁路阻断; 4-隔离
	<u>gr_danger</u> (危险程度)	1-高风险; 2-中风险; 3-低风险
	<u>gr_service</u> (服务类型)	1-www; 2-CGI; 3-FTP; 4-TELNE; 5-POP; 6-NETBIOS; 7-SSH; 8-SMTP; 9-IMAP; 10-DNS; 11-TFTP; 12-FINGER; 13-KERBEROS; 14-LINUXCONF; 15-LDAP; 16-SUNRPC; 18-RSH; 19-RLOGIN; 20-SQL; 21-LPD; 22-IRC; 23-



告警监控

可查看产生的实时告警及全部告警。

告警中心	告警监控		
告警配置			
告警监控			
实时告警	全部告警		
告警名称	告警级别	发生时间	告警描述
test-低	低	2019-04-06 14:08:19	test
test-低	低	2019-04-06 14:05:19	test
test-低	低	2019-04-06 14:02:19	test
test-低	低	2019-04-06 13:59:19	test
test-低	低	2019-04-06 13:56:19	test
test-低	低	2019-04-06 13:53:19	test
test-低	低	2019-04-06 13:50:18	test
test-低	低	2019-04-06 13:47:18	test

▶▶ 告警平台-注意事项

- ▶ 使用邮件告警前需要配置邮件告警服务器
- ▶ 告警监控分为实时监控和历史监控。实时监控可以对最近2小时告警进行查看。历史监控是对所有告警进行查看。
- ▶ 当新建多个告警规则时，各个规则之间是相互独立的关系。

绿盟科技版权所有



谢谢！

绿盟科技版权所有

