SANGFOR BVT 用户手册

深信服智安全
SANGFOR SECURITY

地址:深圳市南山区学苑大道1001号南山智园A1栋
咨询热线：400-806-6868 | 服务热线：400-630-6430 | 邮箱: market@sangfor.com.cn | 网址：www.sangfor.com.cn

目录

技术支持说明

为了让您在安装，调试、配置、维护和学习 SANGFOR 设备时，能及时、快速、有效的获得技术支持服务，我们建议您：

1. 参考快速安装手册图文指导，帮助你快速的完成部署、安装 SANGFOR 设备。如果快速安装手册不能满足您的需要，您可以到深信服社区或官网获取电子版的完整版用户手册或者其他技术资料，以便您获得更详尽的信息。

2. 致电您的产品销售商（合同签约商），寻求技术支持。为了更快速地响应您的服务要求和保证服务质量，您所在地的 SANGFOR 的产品销售商配备有经过厂家认证的技术工程师，会向您提供快捷的电话咨询、远程调试及必要的上门技术服务。

3. 在不紧急的情况下，您可以访问深信服社区，寻求技术问题的解决方案和办法。

4. 致电深信服科技技术服务中心，确认最适合您的服务方式和服务提供方，技术服务中心会在您的技术问题得到解决后，帮助您获得有效的服务信息和服务途径，以便您在后续的产品使用和维护中最有效的享受技术支持服务，及时、有效的解决产品使用中的问题。

用户支持邮箱：support@sangfor.com.cn

技术支持热线电话：400-630-6430（手机、固话均可拨打）

深信服社区：bbs.sangfor.com.cn

深信服科技服务商及服务有效期查询：

http://bbs.sangfor.com.cn/plugin.php?id=service:query

公司网址：www.sangfor.com.cn

返修查询，在线咨询，欢迎您关注深信服科技官方技术服务微信：

声明

深信服科技股份有限公司（以下简称为深信服科技、SANGFOR）。

SANGFOR 及图标为深信服科技股份有限公司的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系请联系深信服科技股份有限公司技术服务部。

前言

本手册仅介绍 BVT 设备安装部署的配置指导和最基本使用方法，如需要更详细配置介绍，请登录深信服社区下载详细电子版用户手册。深信服社区访问地址：http://bbs.sangfor.com.cn。

本手册以深信服 BVT-1000-E640 为例进行说明。各型号产品硬件规格存在一定差异， 但是设备配置以及基本使用方法一致，本手册适用于所有型号的 BVT 设备。

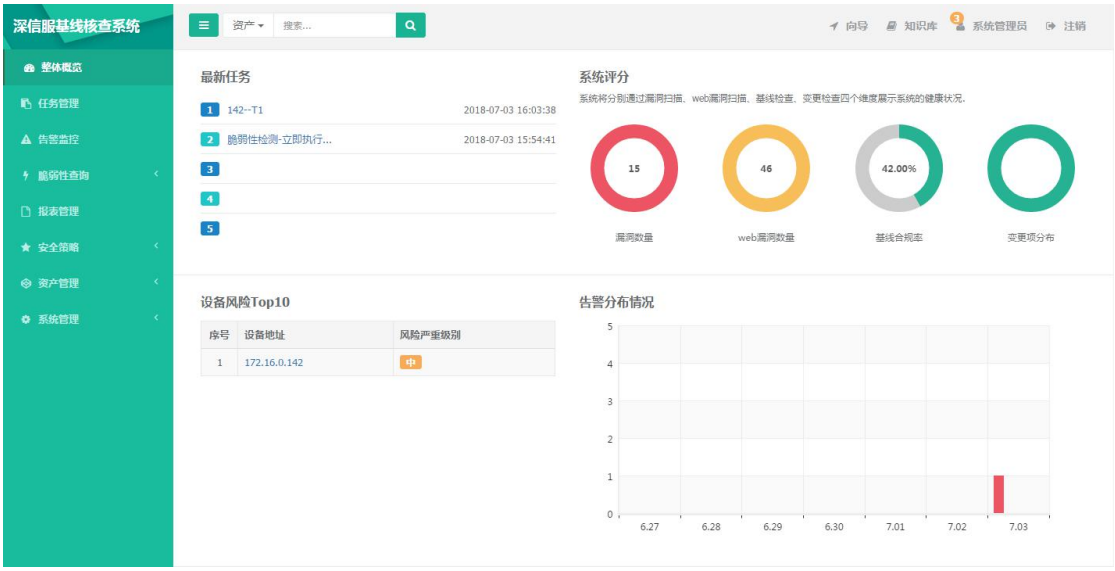
第 1 章 BVT 系列硬件设备的配置

快速配置

1.设备登录

业务控制台说明

用户对系统的绝大部分操作主要通过业务控制台完成。通过业务控制台可以对系统的具体业务模块进行设置、安全内容进行查看，主要包含授权更新、检查策略设置、资产管理、告警策略配置、脆弱性查询等等；



使用 WEB 方式登录

操作步骤：

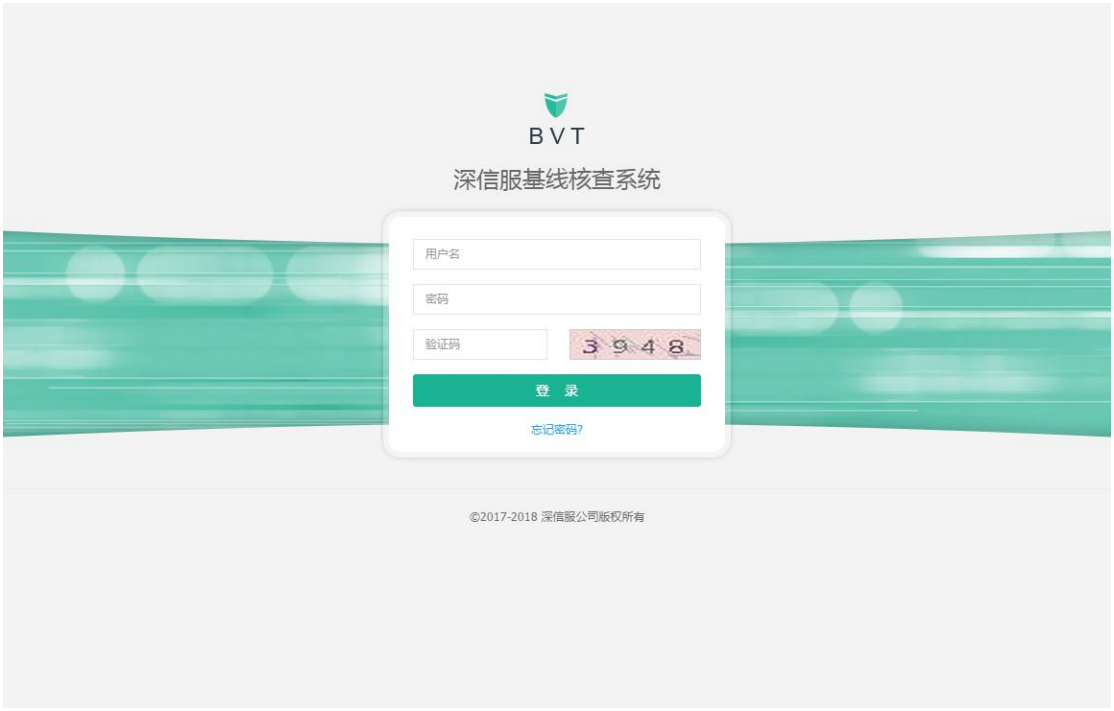
1、用网线连接安装软件时设定 IP 的物理网口（假设安装时为服务器的第一块网卡设定 ip 地址为 192.168. 0.100）。

2、确保管理计算机的 ip 地址与服务器同网段，这里设置为 192.168.0.2，子网掩码为 255.255.255.0；

3、在电脑上打开浏览器（建议使用 IE11、Chrome、Firefox 其中一种）

地址栏输入 https://192.168.0.100

默认用户名：admin　　默认密码：admin　（首次登录需要修改密码）



管理控制台说明

通过管理控制台可以对系统的自身系统运行状态等进行设置，包含网络管理、系统工具(ping工具等)、日期时间设置、数据备份删除设置、系统恢复出厂设置、业务平台密码重置设置、系统关闭及重启；

使用 WEB 方式登录

操作步骤：

1、用网线连接安装软件时设定 IP 的物理网口（假设安装时为服务器的第一块网卡设定 ip 地址为 192.168.0.100）。

2、确保管理计算机的 ip 地址与服务器同网段，这里设置为 192.168.0.2，子网掩码为 255.255.255.0;

3、在电脑上打开浏览器（建议使用 IE11、Chrome、Firefox 其中一种）

地址栏输入 https://192.168.0.100:8082

默认用户名：admin　　默认密码：admin（首次登录需要修改密码）

2.业务系统配置

业务系统配置步骤简介

1、资产口令（必配）

在系统上首先设置需要检查设备的登录帐号口令

2、安全策略告警配置（必配）

将检查结果与系统内置安全策略相匹配比对，如果符合安全策略,将以告警的形式在实时监控模块呈现给用户，用户可以对告警进行相关的处理。该项配置主要包含以下内容

（1）启用系统内置告警策略库；

（2）根据实际用户需求，手工增加策略（按需配置）；

（3）对安全策略产生的告警进行处理

3、基线检查策略参数修改（选配）

对于不同要求的检查，可以对基线检查策略进行参数调整，以达到不同的检查要求

4、　创建检查任务（必配）

2.1.资产管理配置

2.1.1.简介

功能简介

1、资产管理便于设备对当前设备进行识别及管理：

资产不是必须配置的，通过创建检查任务，也可以对非资产进行检查

资产可以通过资产发现或者手工创建

2、 资产管理支持批量资产导入导出，同时支持按视图对资产进行分类（资产分组）

2.1.2.典型配置

单台资产添加

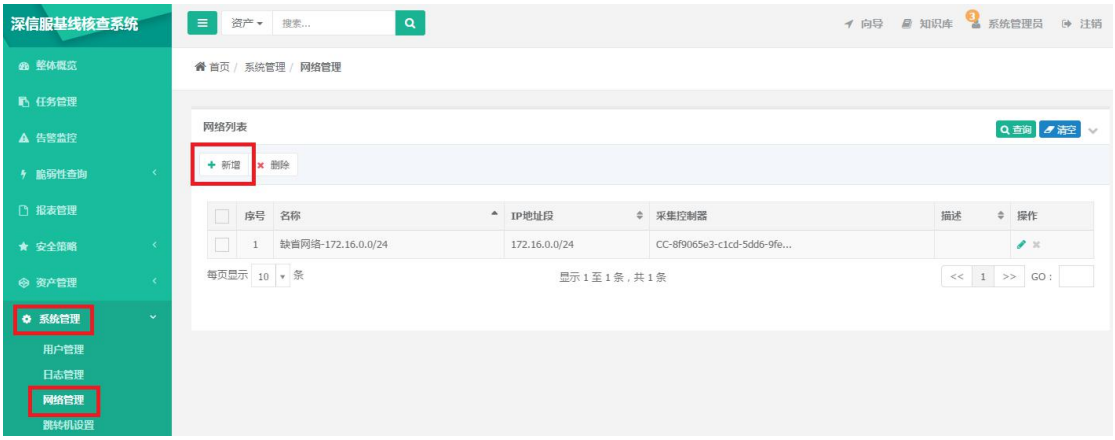
场景：添加 1 台 windows server2008 服务器，ip 地址为 5.5.5.5

具体配置

WEB 登录业务控制台：https://192.168.0.100（根据实际设定的 ip 地址进行登录）默认用户名：admin，密码 admin

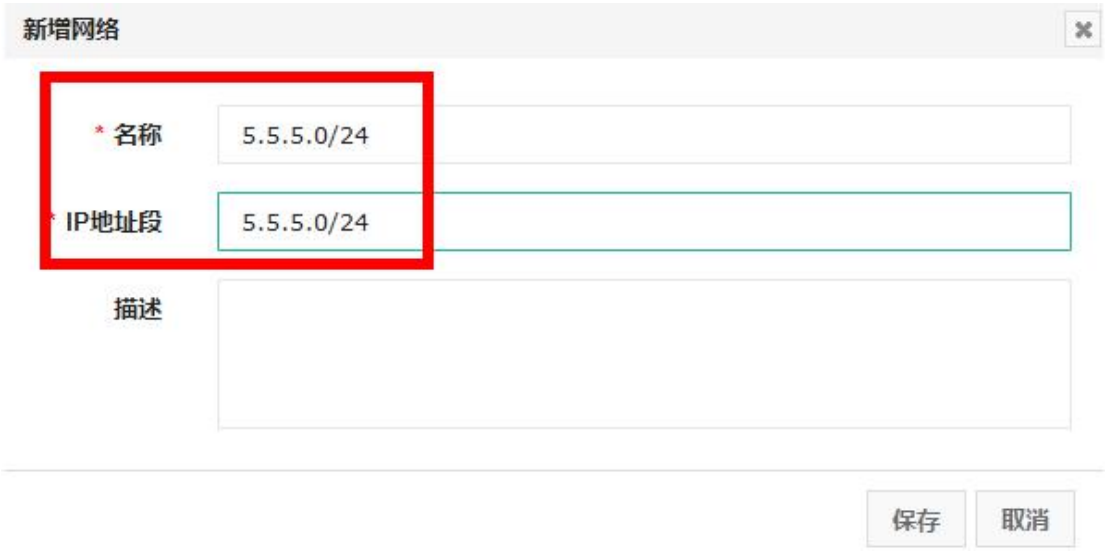
（1）增加 ip 地址段

选择 资产管理->网络管理->IP 地址段，点击新增



增加 5.5.5.0/24 网段，如下图配置

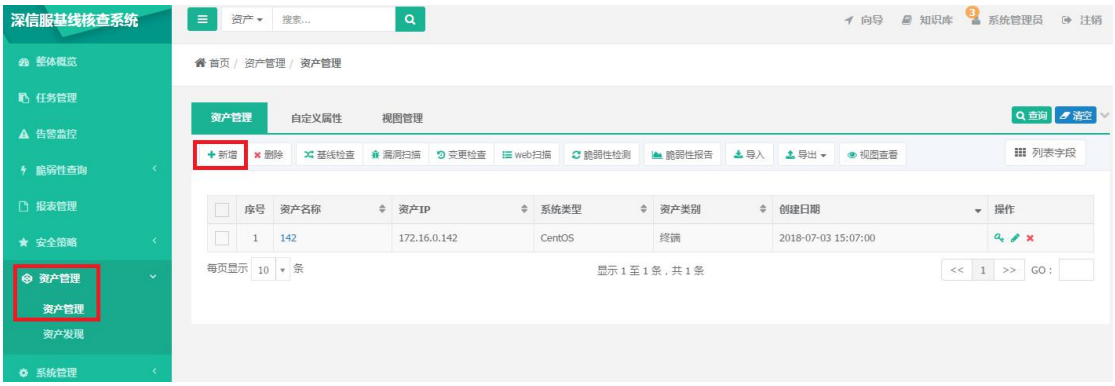
地址:深圳市南山区学苑大道1001号南山智园A1栋
咨询热线：400-806-6868 | 服务热线：400-630-6430 | 邮箱: market@sangfor.com.cn | 网址：www.sangfor.com.cn



注意：绝大多数情况下【所属网络】请务必选择缺省网络，否则将造成其他功能模块解析异常

（2）增加具体资产

点击 资产管理->资产管理->新增



如下图进行配置：

注意：红*为必填项

资产名称：根据实际网络、设备自定义取名

系统类型：选择 windows 2008

ip 地址段：选择已有的 5.5.5.0;如果是新增的 ip 地址段，可以直接点击后面的+号

资产类别：此处选择服务器
资产 ip：此处填写需要增加资产的实际 ip

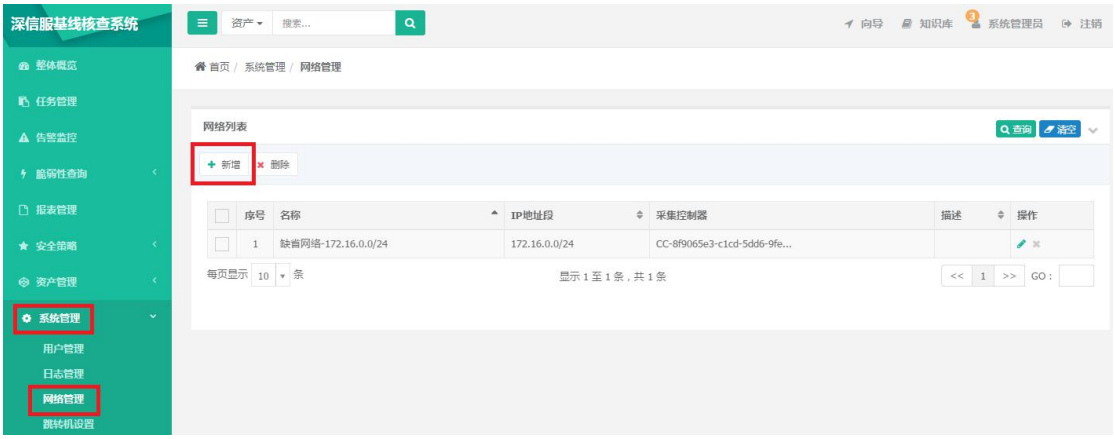
通过“查询“，按钮可以快速的查询当前已添加的资产

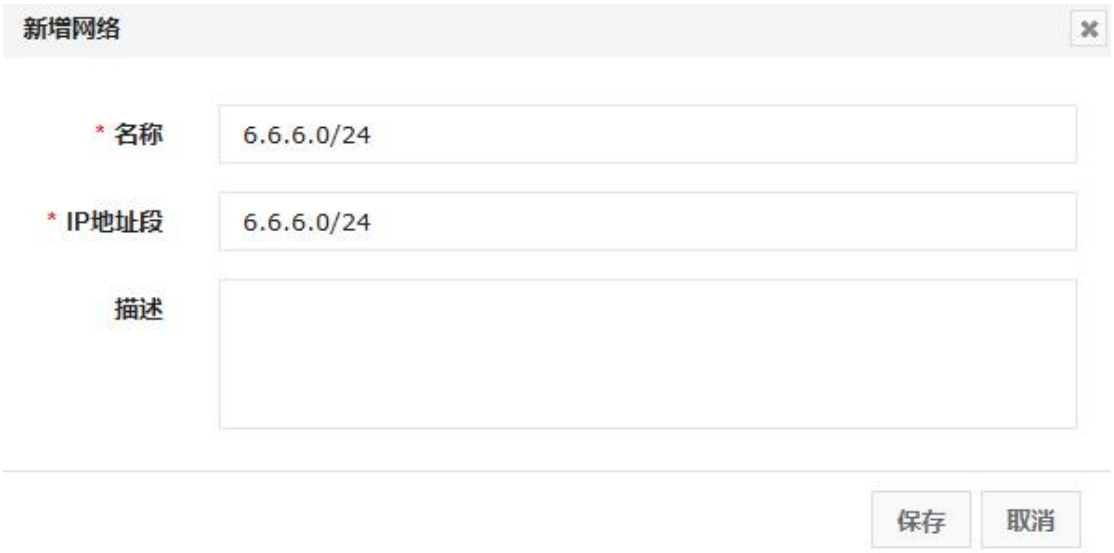
资产批量导入

场景：批量导入 6.6.6.1-6.6.6.10 这十台设备

注意：BTV 系统仅支持 csv 格式的文件导入，文件大小不能超过 5M；

（1）增加 6.6.6.0/24ip 地址段





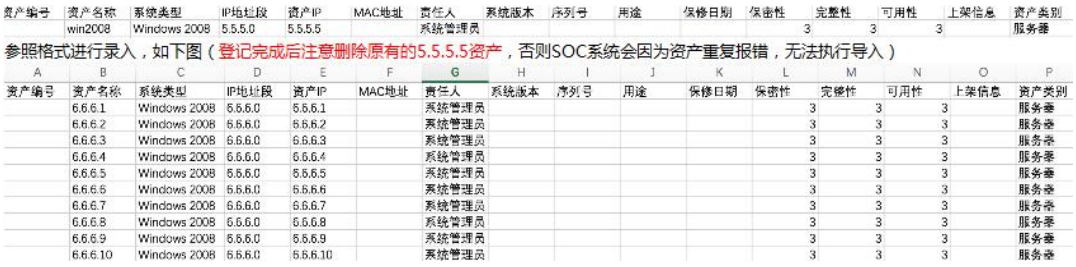
注意：通常情况下【所属网络】请务必选择缺省网络，否则将造成其他功能模块解析异常

（2）建议操作：从导出某一台设备的文件，作为模版；此处以设备 5.5.5.5 为例

选中主机 5.5.5.5,并选择导出为 csv 文件

（3）打开本地保存的 csv 文件（导出文件名为“资产列表.csv”），参照 5.5.5.5 资产格式，根据实际情况录入 6.6.6.1-6.6.6.10 这十台设备；

5.5.5.5 资产导出 csv 格式，如下图



参照格式进行录入，如下图（登记完成后注意删除原有的 5.5.5.5 资产，否则系统会因为资产重复报错，无法执行导入）

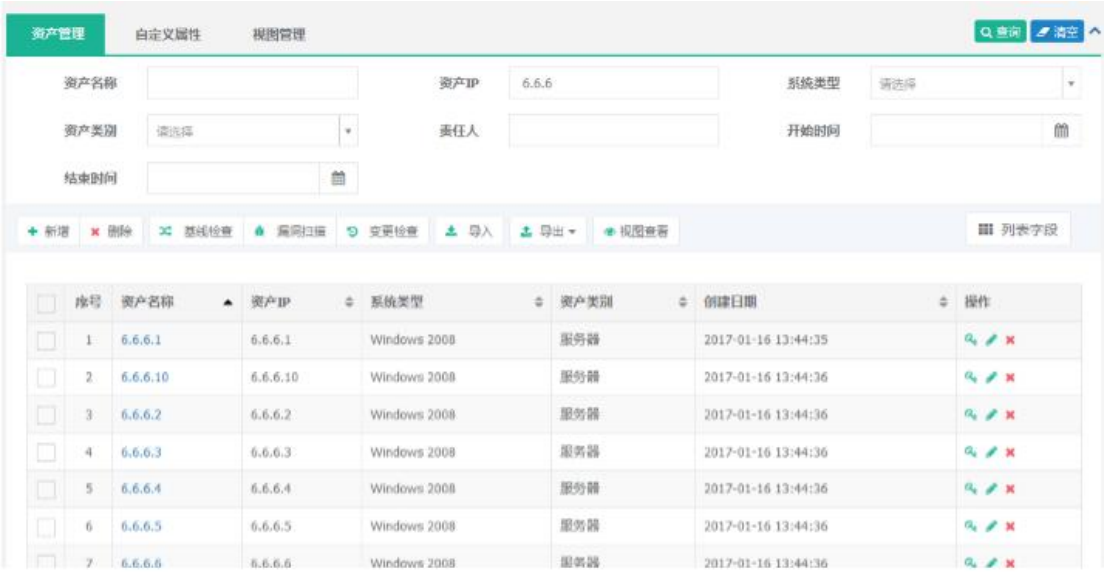
注意：请确保 ip 地址段 6.6.6.0 已经事前添加，否则将报错；

（4）选择本地文件在系统上进行导入

（4）查看导入后的资产

导入成功，将会在页面右下角提示导入成功

查看新导入的 10 台资产



视图（分组）配置

场景：将增加的 10 台 6.6.6.1-6.6.6.10，以及 5.5.5.5 增加组别信息

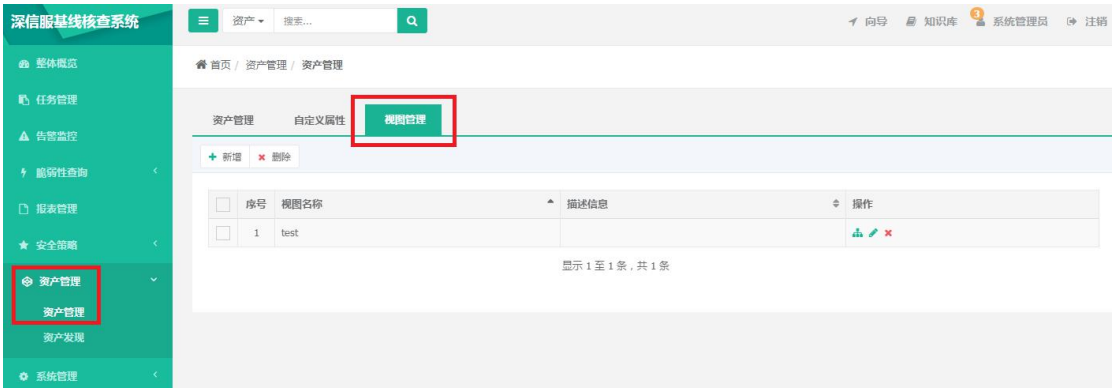
- 6.6.6.1-6.6.6.10：

  父组【test】， 子组【6 网段】

- 5.5.5.5: 父组【test】， 子组【5 网段】

（1）添加父组：test

选择 资产管理-> 资产管理 -> 视图管理，点击 新增，如下图



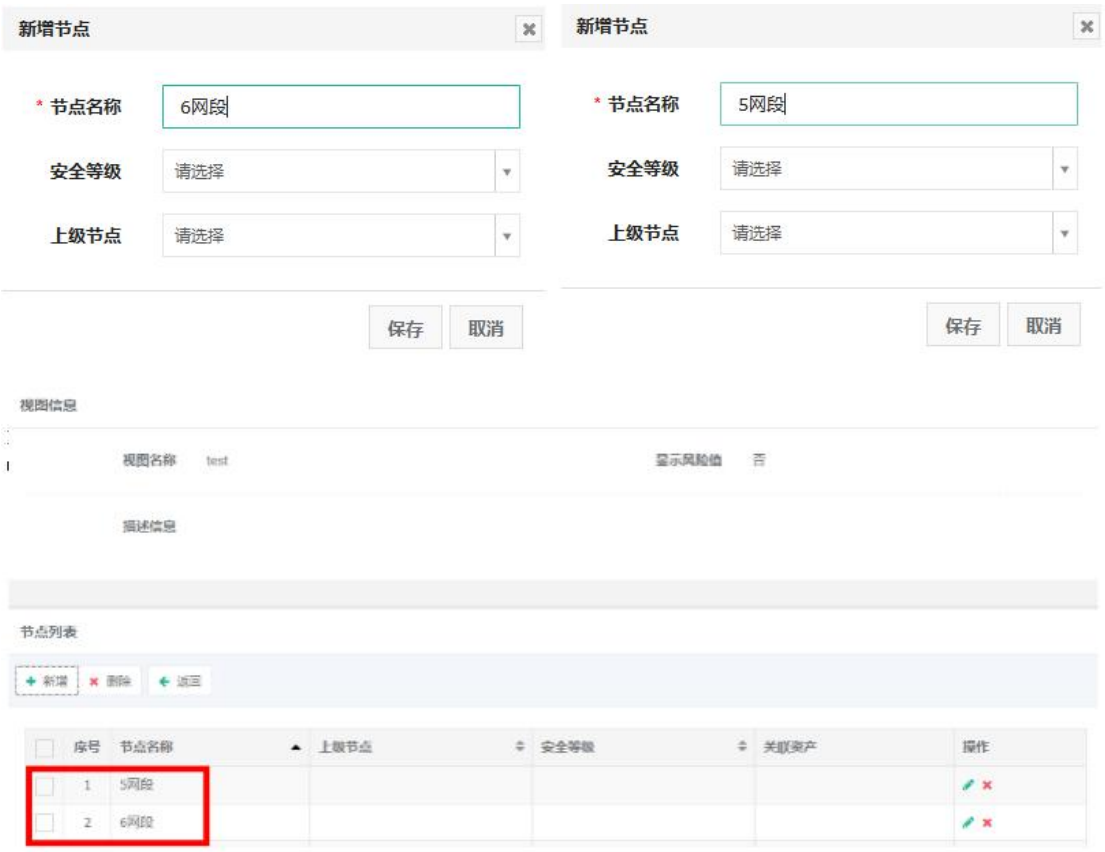
新增 test 父组，如下图

（2）添加子组 6 网段和 5 网段

点击 节点管理

点击 新增

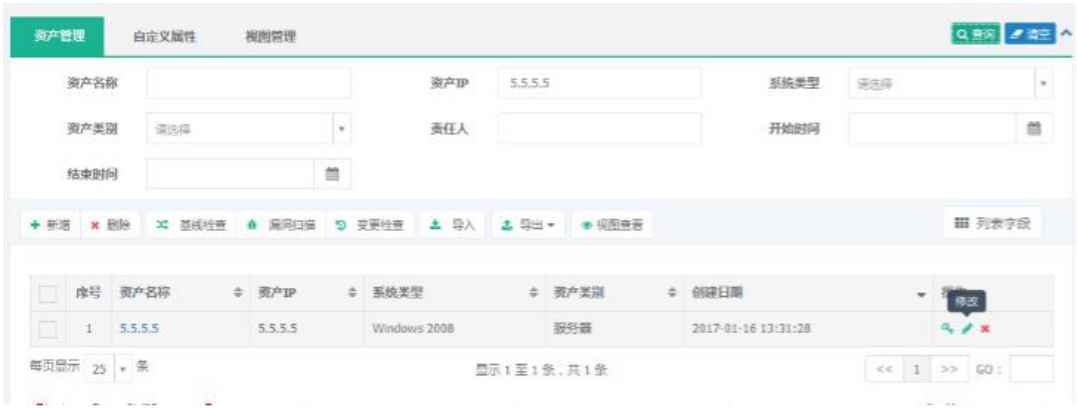
增加 6 网段和 5 网段



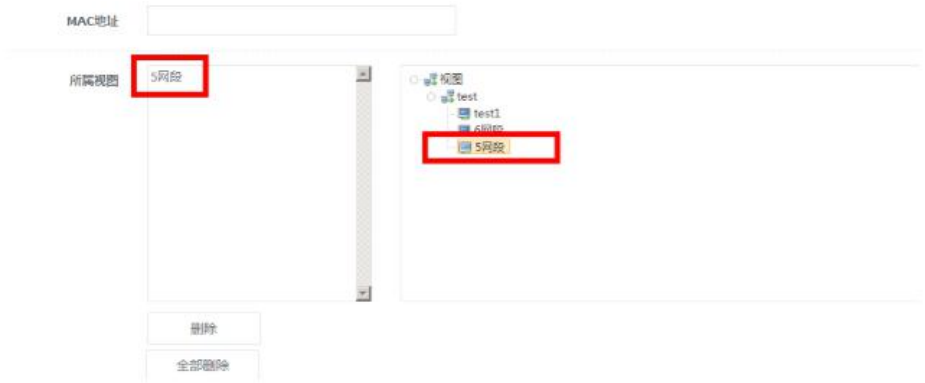
（3）将资产划入相应分组

将 5.5.5.5 划入 5 网段

在 资产管理-> 资产管理-> 资产管理,选中 5.5.5.5 资产，进行修改



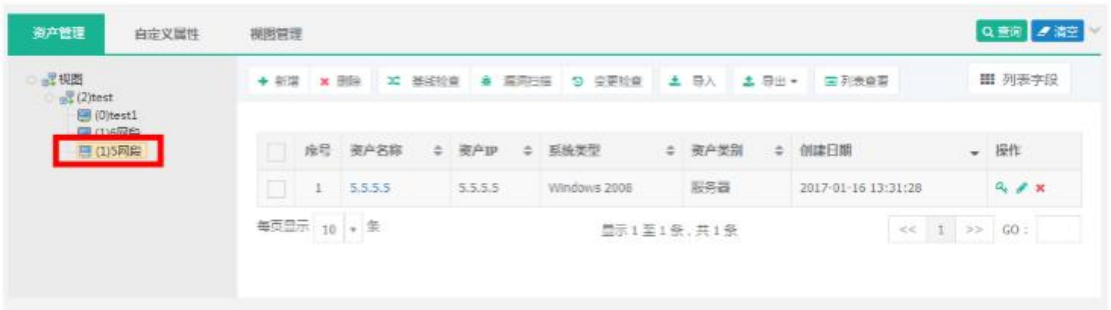
在所属视图中选中 5 网段，并保存



同理将 10 台 6 网络设备加入【6 网段】

（4）点击 资产管理->资产管理->视图查看，可以查看当前已经建立的分组

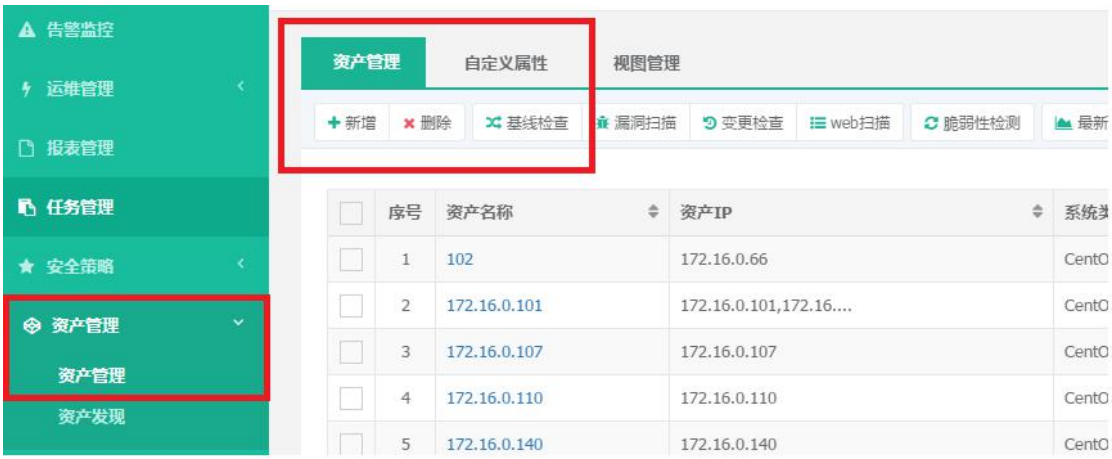
按分组查看



2.1.3. 网站资产管理

2.1.3.1.新增网站资产

进入“资产管理”->“资产管理”->“资产管理”页面，点击“新增”按钮



2.1.3.2.输入网站信息点击保存

操作（认证配置、URL 探测、修改、删除）
URL 探测：探测出该站点下所有 URL 地址
URL 探测->立即探测->查看列表

2.1.3.3.认证配置

可对网站资产认证配置进行启用停用、删除、认证检测。

2.1.4 自定义资产添加

自定义厂商、产品、系统类型（非默认自带）资产添加
场景：
添加一台防火墙：
ip 地址：192.168.1.123
厂商：A 厂商
产品：B 产品
系统型号：C 系统
具体配置

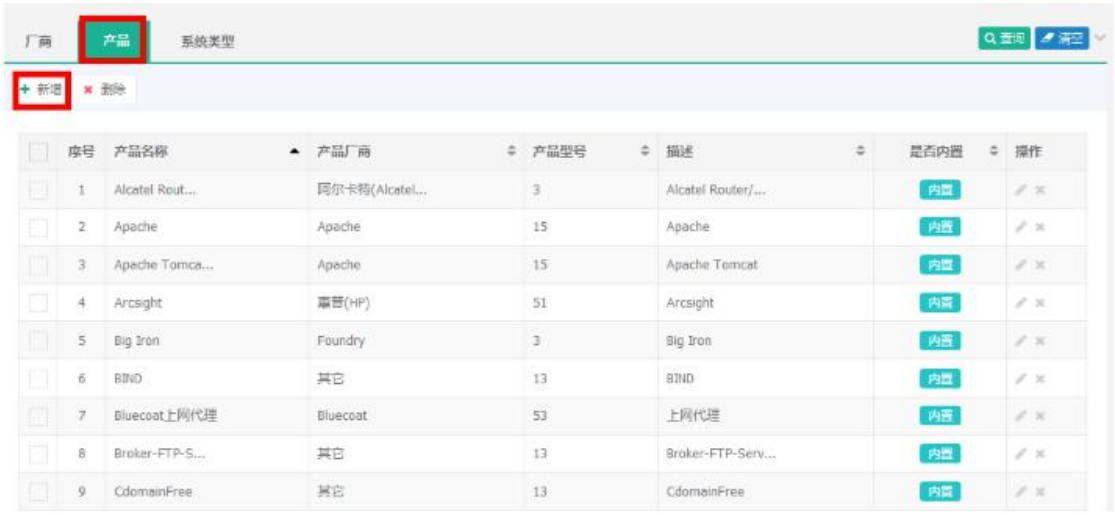
（1）添加厂商

点击 系统管理-内置对象-厂商-新增

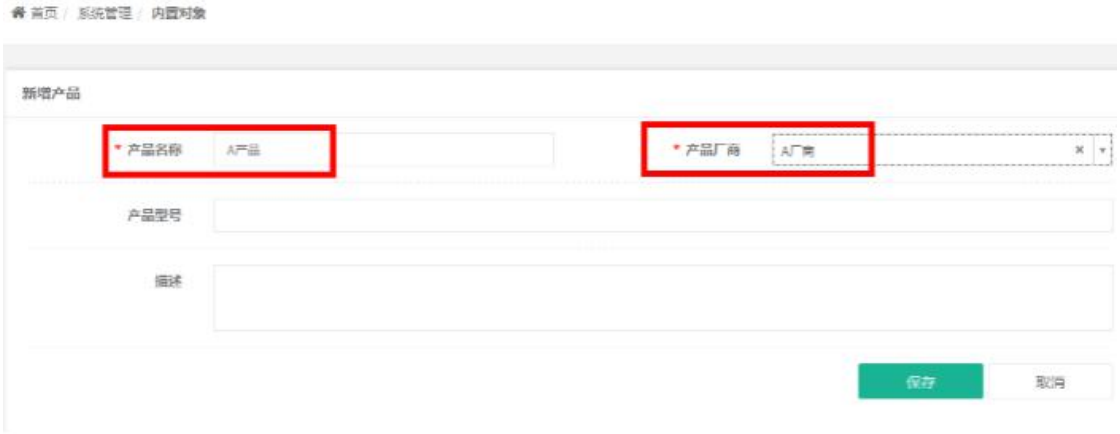
如下图进行配置

（2）增加产品

点击 系统管理-内置对象-产品-新增

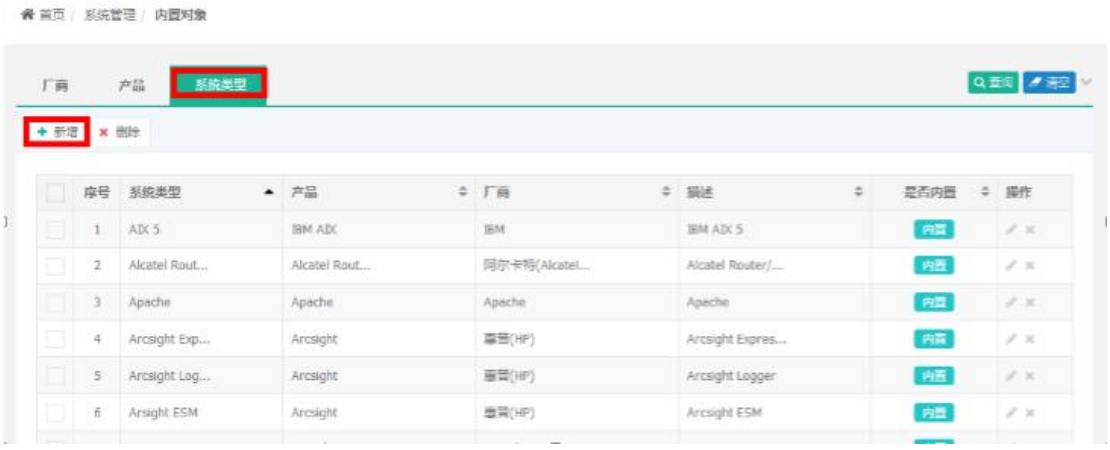


如下图 进行配置，产品厂商选择刚建立的【A 厂商】

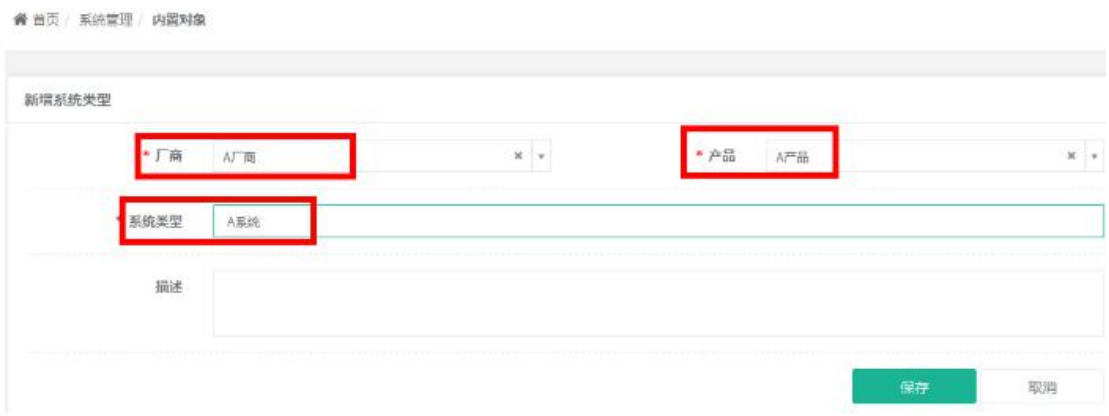


（3）增加系统类型

点击 系统管理-内置对象-系统类型-新增



如下图 进行配置，产品厂商选择刚建立的【A 厂商】，产品选择刚建立的【A 产品】



（4）添加资产，调用新建的【A 系统】
点击资产管理-资产管理-资产管理-新增

参照下图配置，系统类型选择刚建立的【A 系统】，即可完成自定义资产的调用

2.2.告警策略配置（必配）

2.2.1.告警策略说明

功能简介：

所谓告警是指用户特别需要关注的安全问题，这些问题来源于高危漏洞、安全基线违规问题等。

告警管理中包括了如下功能：

1、告警监控：监控系统内存在的各种告警；用户可以通过定义过滤器以监控需要特别关注的告警信息；用户也可以根据个人需求，设置告警的提示音、界面显示方式等；

2、告警处理：处理监控列表中相关告警；针对告警，用户可以清除、确认（不能确定是否需要处理）；

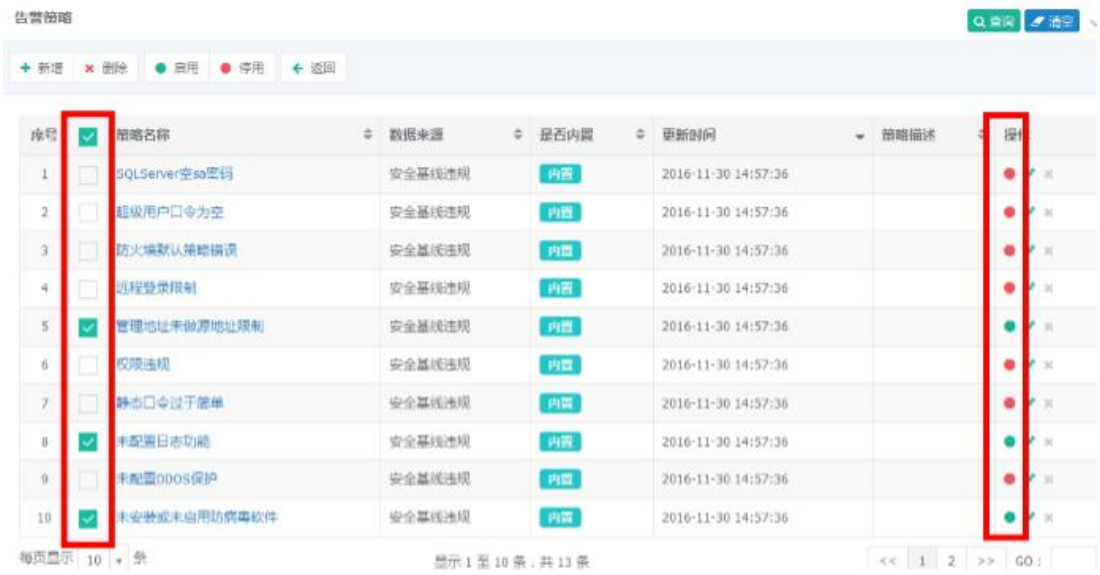
3、策略定义：用户可以定义各类告警产生的策略（系统内置了部分策略）；在告警策略中可以设定对于安全数据的筛选条件以及命中后产生何种响应；响应包括包含发送邮件、发送 Syslog 或 SNMP Trap、执行外部程序或脚本等。

2.2.2.具体配置（必配）

启用默认告警策略（必配）

点击"告警监控"- >"设置告警策略"

勾选绿色状态灯的规则，点击启用；需注意全部勾选启用；



查看策略状态：已启用

配置手工策略（按需配置）

点击新增按钮

根据数据来源，配置相应的过滤器，如配置安全基线违规严重级别大于等于高级的

响应方式选择“产生告警”，配置告警名称和严重级别

点击“保存”按钮

注：漏洞和变更的告警策略参照上面方法介绍。

2.3.检查策略配置（选配）

2.3.1.基线策略配置

介绍：

系统内置默认基线检查策略，不可修改，可以根据不同检查的要求，对各类基线检查项进行自定义，选择需要检查的项，调整检查参数，以满足各类检查的要求。

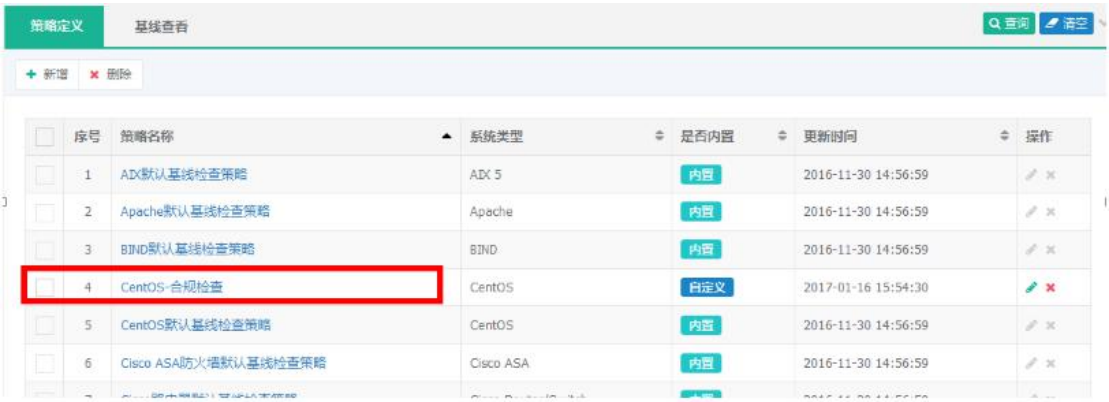
典型配置：

1、进入“安全策略”->“安全基线检查”->“策略定义”页面，点击“新增”按钮

2、输入策略名称，选择系统类型

地址:深圳市南山区学苑大道1001号南山智园A1栋
咨询热线：400-806-6868 | 服务热线：400-630-6430 | 邮箱: market@sangfor.com.cn | 网址：www.sangfor.com.cn

3、点击“保存”按钮



4、创建任务的时候，选择此策略

2.3.2 变更策略配置

介绍：

系统内置默认变更检查策略，不可修改，可以根据不同检查的要求，对各类检查项进行自定义，新增需要检查的项，调整检查参数，以满足各类检查的要求。

配置项的相关说明：

1、配置项类型包括：文件、目录、端口、进程、注册表、启动项。如果设备类型为网络设备或者安全设备，只有一个类型：自定义。

2、配置项严重级别：信息、低级、中级、高级、严重。

3、Unix、Linux 的文件、目录属性包括：文件访问许可、属主用户、属主组、分配的区块、修改时间戳、iNode 数量、link 数量、文件类型、访问时间戳、iNode 创建和修改的时间戳。

4、Windows 的目录属性包括：归档标记、隐藏标记、临时标记、目录标记、最近写时间、NTFS 压缩标记、NTFS GSID、NTFS SACL、安全描述符大小、可变的数据流数目、只读标记、离线标记、系统标记、最近访问时间、创建时间、MS-DOS 8.3 名称、NTFS OSID、NTFS DACL、安全描述控制符。

5、Windows 的文件属性包括：比目录属性多一个“文件大小”。

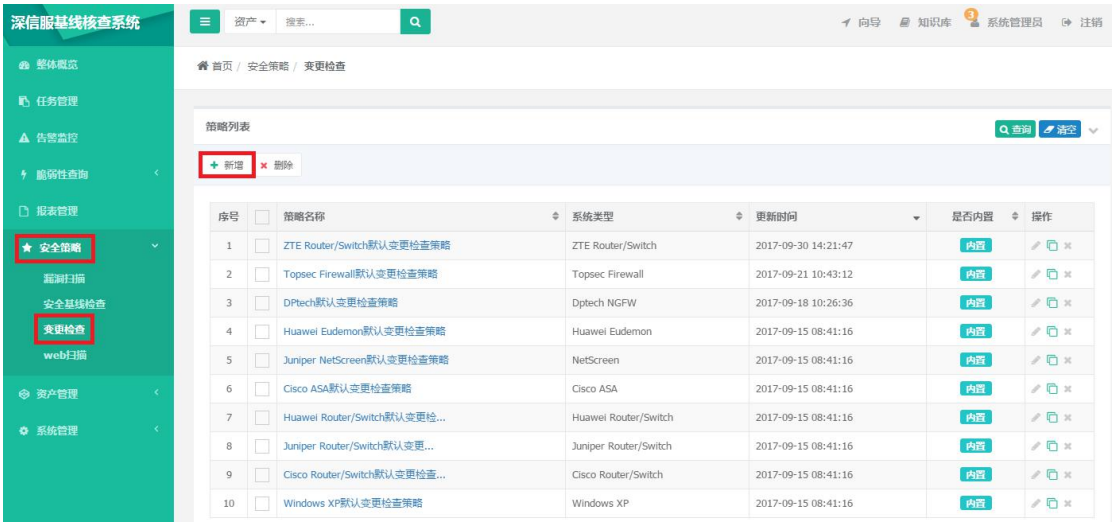
6、Windows 的注册表键属性包括：注册类型：键或值、属主用户、属主组、DACL、SACL、Class 名称、Subkey 数量、Subkey 名称和最多长度、Class 名称最大长度、值数量、值名称最大长度、key 值最大长度、安全描述控制符、key 的安全描述符大小、最近写时间。

7、端口、进程、启动项可以配置白名单。

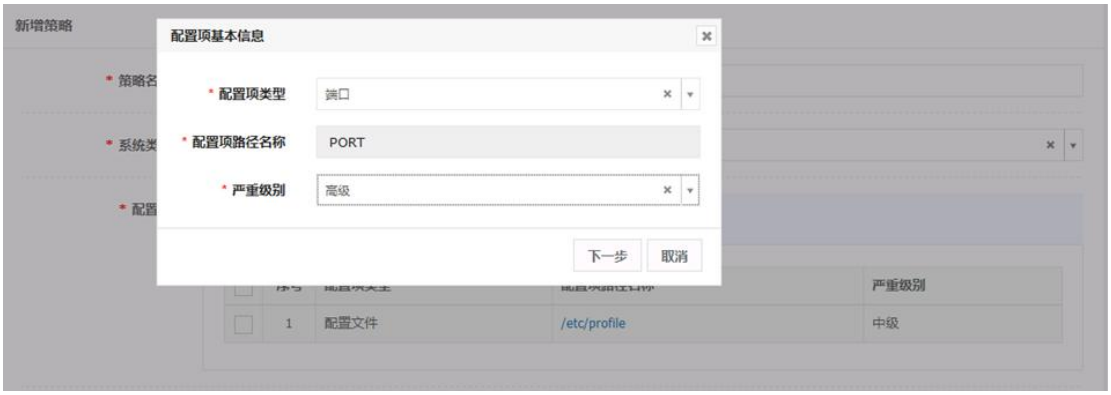
8、网络设备、安全设备的检查项只有自定义，并且要根据不同类型的设备，强制只能使用获取配置的命令，不能输入其他任意命令，具体命令见上面完整性检查策略表里的描述，比如思科路由器默认为 show running-config。可以输入此命令后面的子项，如：show running-config system。

二、典型配置：

1、进入“安全策略”->“变更检查”页面，点击“新增”按钮



2、选择系统类型、输入策略名称、描述、选择需进行变更检查的配置项并定义严重级别等，如：配置项类型为端口，严重级别为高级



3、点击下一步，配置端口白名单

4、添加其他需要检查的内容，点击保存按钮

5、也可以通过复制的方法，在内置策略的基础上修改检查项，创建一个新的策略

填写策略名称

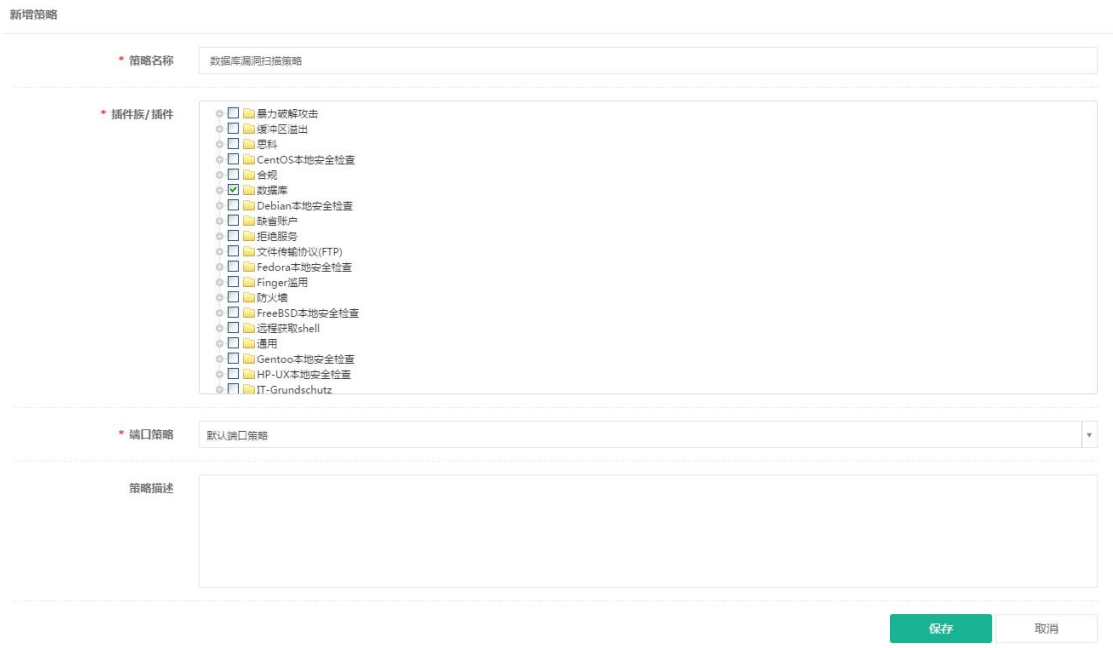
在复制出来的新策略上进行修改即可。

2.3.3.漏洞扫描策略

系统内置默认漏洞扫描策略，不可修改，可以根据不同扫描的要求，对漏洞扫描进行自定义，选择需要扫描的插件族，以满足漏洞扫描的要求。

1. 进入“安全策略”->“漏洞扫描”->“策略定义”页面，点击“新增”按钮

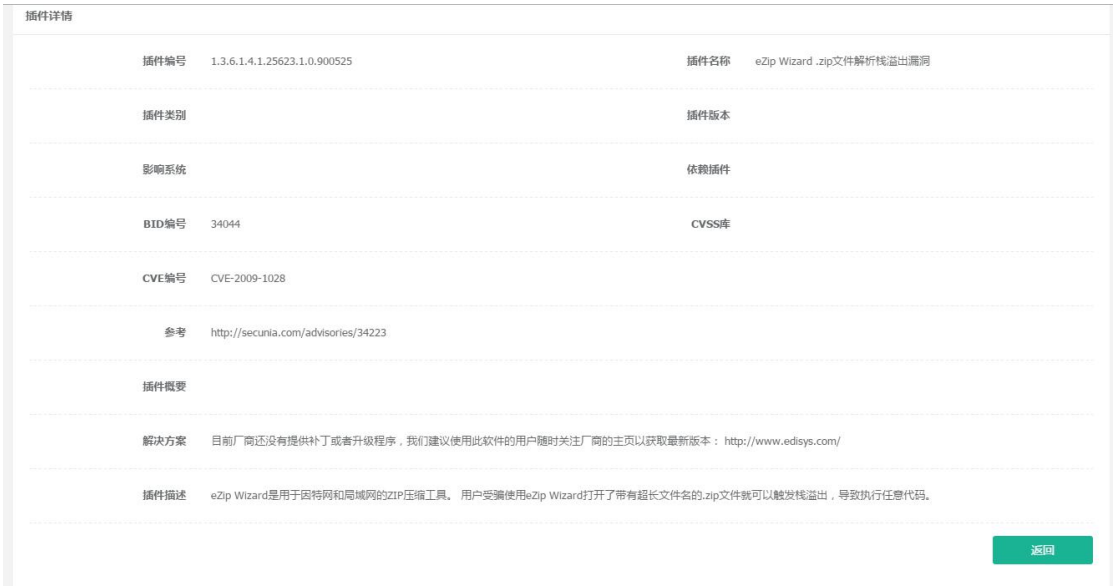
2. 输入策略名称，选择插件族、端口策略。



3、 点击“保存”按钮

4、 创建任务的时候，选择此策略

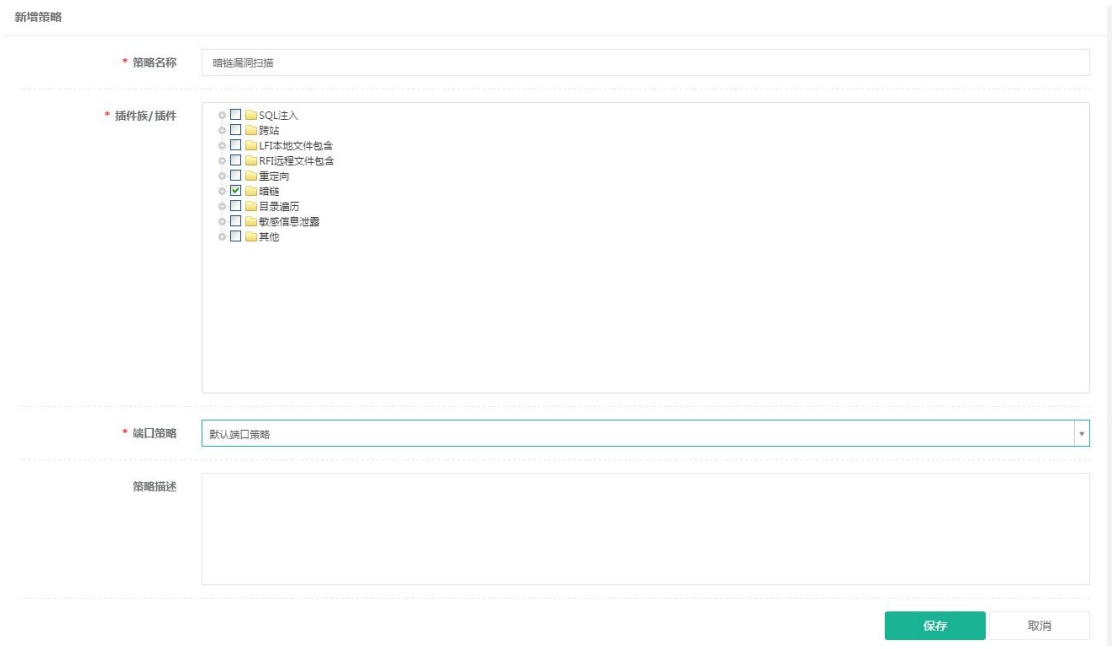
5、 查看漏洞扫描插件



2.3.4.Web 扫描策略

1、进入“安全策略”->“web 扫描”->“策略定义”页面，点击“新增”按钮

2、输入策略名称，选择插件族、端口策略。



3、点击“保存”按钮

4、站点发现策略定义新增

2.4.任务管理（必配）

2.4.1.简介

功能简介

任务管理为合一任务，可以创建漏扫、基线、变更，web 扫描四合一任务，也可以是单独任务；

在任务里选择收集对象（以 IP 为对象，可以是单个 IP 或是个 IP 地址段）、检查策略、任务调度方式（定时、手动、立即执行、一次运行）、描述等。

当输入 ip 地址或地址段时，会首先进行设备发现，再进行后续任务配置，如果 ip 段范围比较大，发现的时间会略长，推荐选择资产进行检查，如图：

2.4.2.基线检查任务

典型配置

点击"任务管理"页面新增按钮

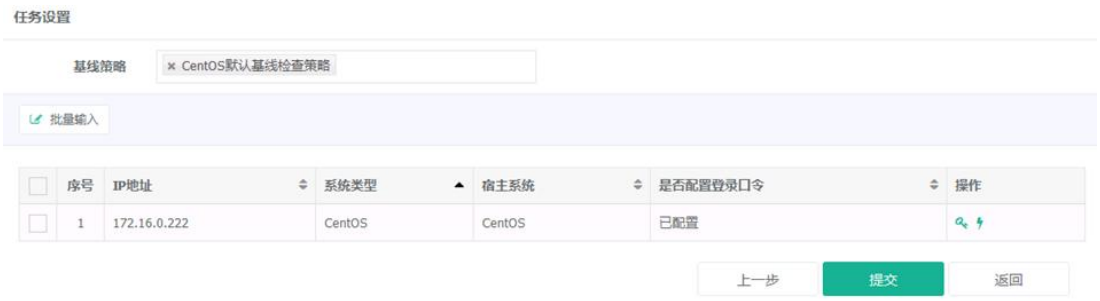
1. 任务新增：用户输入任务名称、收集对象（以 IP 为对象，可以是单个 IP 或是个 IP 地址段）、检查策略、任务调度方式（定时、手动、立即执行、一次运行）、描述等。

如下图所示：

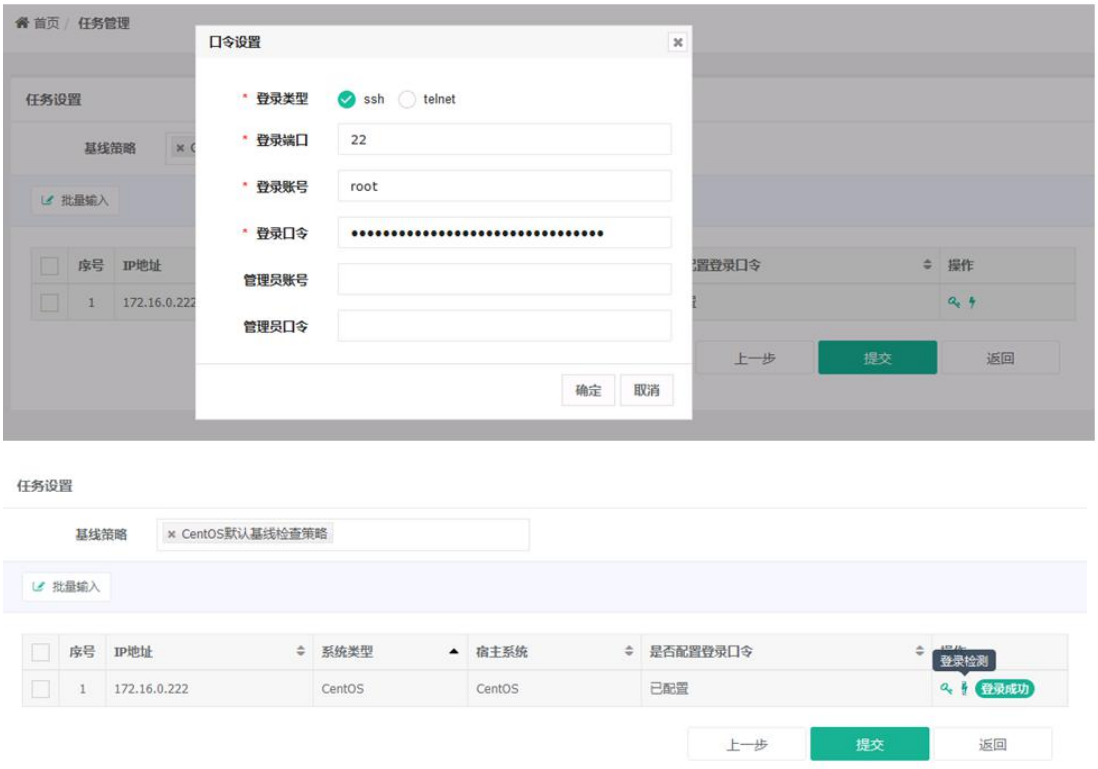
当输入 ip 地址或地址段时，会首先进行设备发现，再进行后续任务配置，如果 ip 段范围比较大，发现的时间会略长，推荐选择资产进行检查，如图：

发现结果包含自动发现的检查对象和选择的资产对象等。

此时，可以新增检查对象，然后勾选需要检查的，进行下一步配置选择检查策略。



配置检查所需的账号口令，进行登录检测：



点击提交，任务创建完成。

2. 任务删除：在列表中选择需要进行删除的一个或多个任务；点击删除功能进行删除，删除前提示用户是否删除该任务，另如任务正在执行也可以删除；删除成功，在列表界面中看不到该任务相关信息，该任务之前完成的安全基线检查将参与统计，系统不提供查看删除后查看任务对应产生的报告功能。

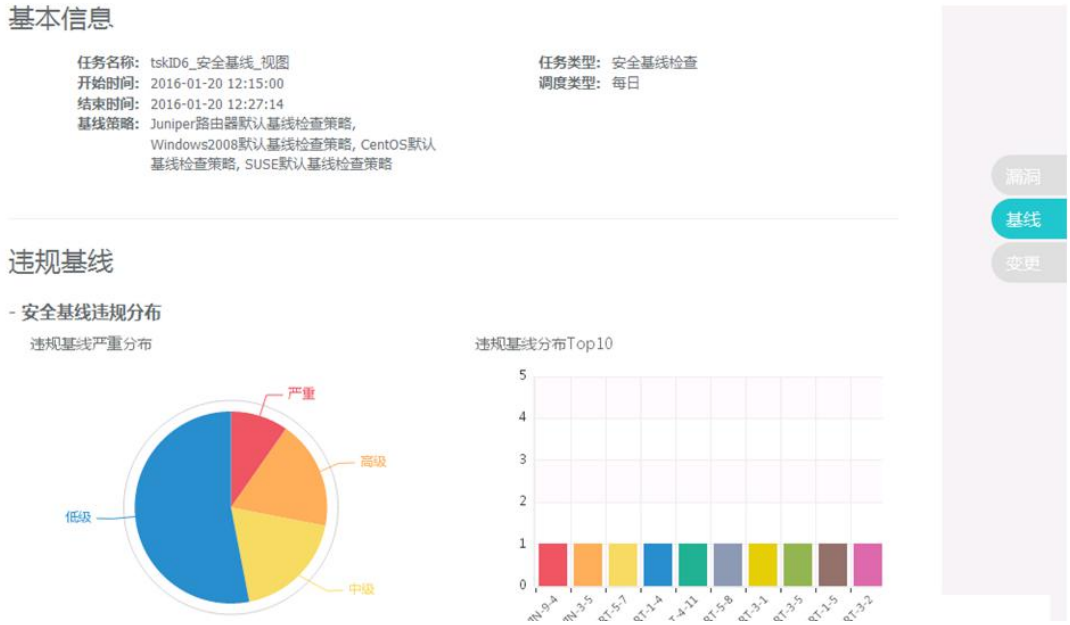
3. 停止调度：对于周期型任务可以停止调度。如下图所示：

4. 恢复调度：对于已经被停止调度的任务，用户可以选择恢复调度。

序号	任务名称	任务类型	调度类型	任务状态	创建时间	最近开始时间	操作
11	test_161	安全基线检查、变更检查	手动	已完成	2016-01-19 15:14:34	2016-01-19 15:54:07	
12	tskID25_变更_视图	变更检查	手动	已完成	2016-01-19 15:00:51	2016-01-19 15:01:50	
13	tskID7_漏扫_视图	漏洞扫描	一次运行	已完成	2016-01-19 13:34:28	2016-01-19 13:45:00	
14	tskID6_安全基线_视图	安全基线检查	每日	已完成	2016-01-19 11:19:45	2016-01-20 12:15:00	
15	tskID5_漏扫_视图	漏洞扫描	一次运行	已完成	2016-01-19 11:18:33	2016-01-19 12:00:00	
16	变更检查-立即执行-20160...	变更检查	立即执行	已完成	2016-01-18 17:23:57	2016-01-18 17:23:57	
17	漏洞扫描-立即执行-20160...	漏洞扫描	立即执行	已完成	2016-01-18 17:23:51	2016-01-18 17:23:51	
18	安全基线检查-立即执行-201...	安全基线检查	立即执行	已完成	2016-01-18 17:23:43	2016-01-18 17:23:43	

任务执行结果

5. 报告查看：选择某一任务，可查看该任务历史报告、详细报告情况，详细内容包括：任务基本信息（包括任务名称、开始时间、结束时间、任务类型、检查策略）、基线违规严重级别分布图、主机列表（包括主机 IP 地址、任务执行状态、符合、不符合、基线类型）、产生违规主机的详细信息（包括基线名称、基线编号、严重级别、发现时间、描述、解决方案等）。如下图所示：



6. 报告导出：在任务列表中进入详细报告功能，在详细报告页面中可导出报告，支持 Word、PDF 等格式。

7. 报告对比：点击一个任务，在报告列表中选择 2 个报告；报告内容包括任务名称、任务类型、两次报告的生成时间对比、两次报告的基线数量对比（按照总数）、两次报告的基线合规率对比、两次任务中发现相同的和不同的基线。

2.4.3.变更检查任务

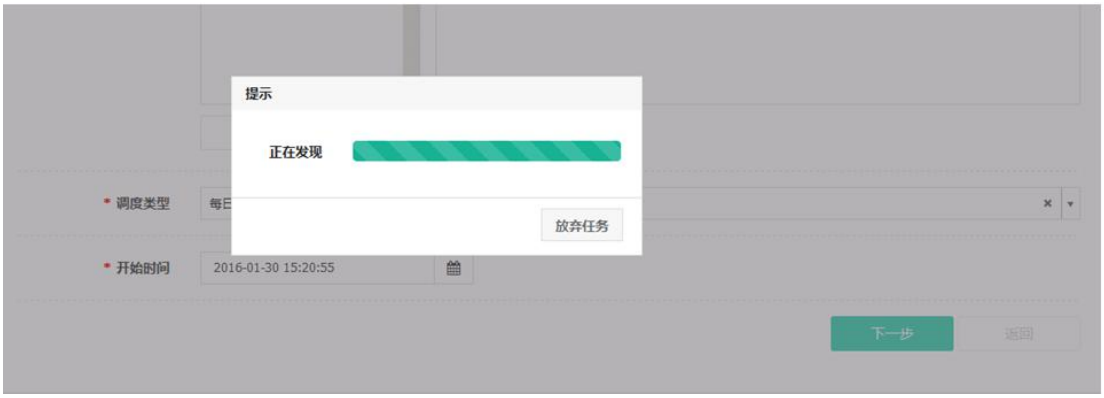
典型配置

点击"任务管理"页面新增按钮

1、任务新增：用户输入任务名称、收集对象（以 IP 为对象，可以是单个 IP 或是个 IP 地址段）、检查策略、任务调度方式（定时、手动、立即执行、一次运行）、描述等。

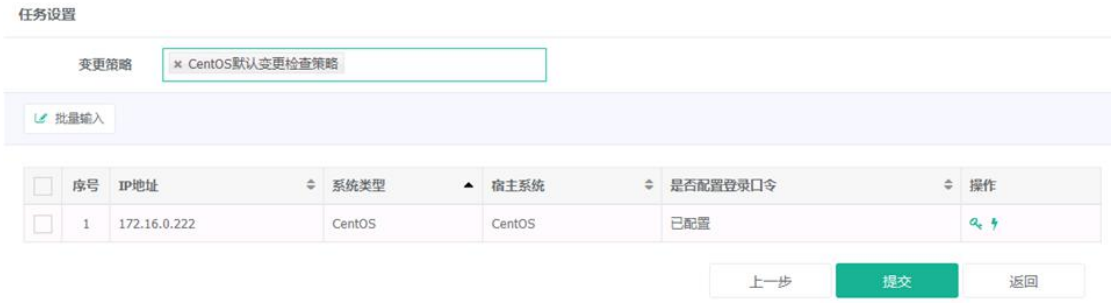
如下图所示：

当输入 ip 地址或地址段时，会首先进行设备发现，再进行后续任务配置，如果 ip 段范围比较大，发现的时间会略长，推荐选择资产进行检查，如图：

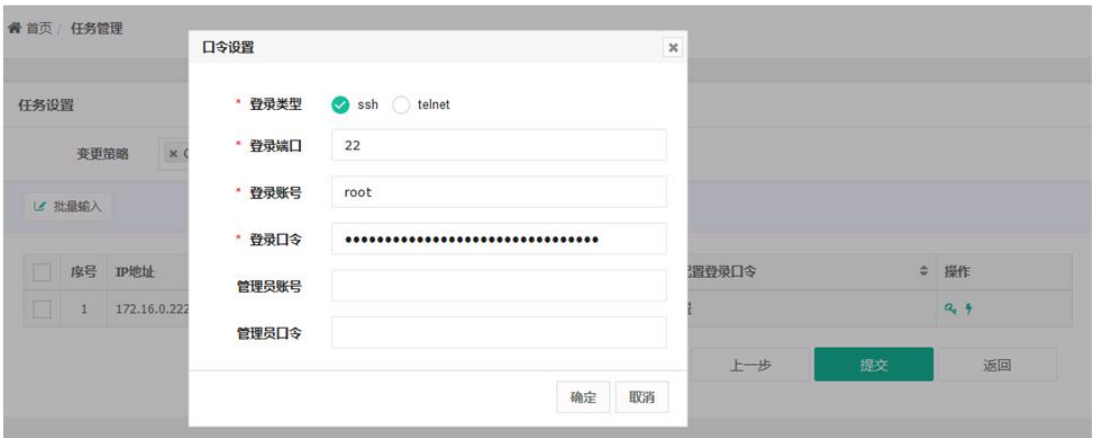


发现结果包含自动发现的检查对象和选择的资产对象等。

此时，可以新增和修改检查对象，然后勾选需要检查的，进行下一步配置选择检查策略。



配置检查所需的账号口令，进行登录检测：



点击提交，任务创建完成。

2、任务删除：在列表中选择需要进行删除的一个或多个任务；点击删除功能进行删除，删除前提示用户是否删除该任务，另如任务正在执行也可以删除；删除成功，在列表界面中看不到该任务相关信息，该任务之前完成的安全基线检查将参与统计，系统不提供查看删除后查看任务对应产生的报告功能。

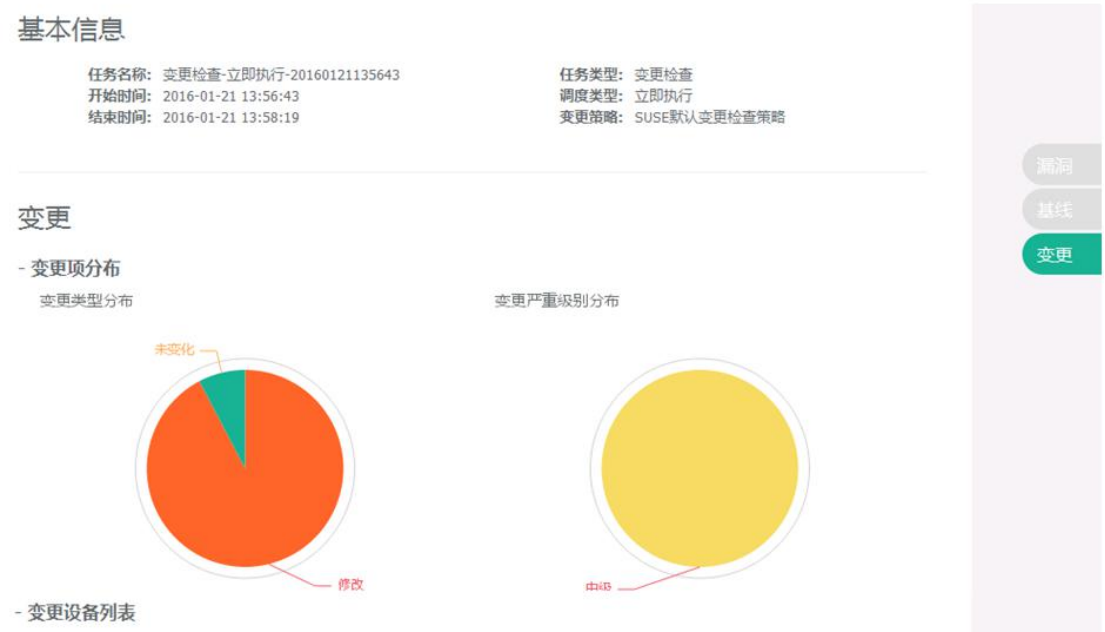
3、停止调度：对于周期型任务可以停止调度。如下图所示

4、恢复调度：对于已经被停止调度的任务，用户可以选择恢复调度。

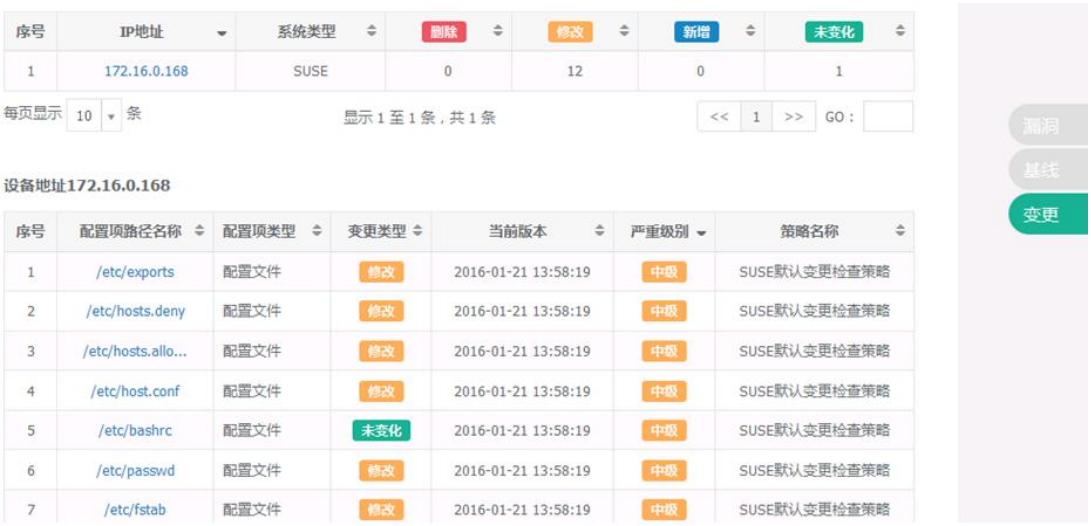
序号	任务名称	任务类型	调度类型	任务状态	创建时间	最近开始时间	操作
11	test_161	安全基线检查、变更检查	手动	已完成	2016-01-19 15:14:34	2016-01-19 15:54:07	
12	tskID25_变更_视图	变更检查	手动	已完成	2016-01-19 15:00:51	2016-01-19 15:01:50	
13	tskID7_漏扫_视图	漏洞扫描	一次运行	已完成	2016-01-19 13:34:28	2016-01-19 13:45:00	
14	tskID6_安全基线_视图	安全基线检查	每日	已完成	2016-01-19 11:19:45	2016-01-20 12:15:00	
15	tskID5_漏扫_视图	漏洞扫描	一次运行	已完成	2016-01-19 11:18:33	2016-01-19 12:00:00	
16	变更检查-立即执行-20160...	变更检查	立即执行	已完成	2016-01-18 17:23:57	2016-01-18 17:23:57	
17	漏洞扫描-立即执行-20160...	漏洞扫描	立即执行	已完成	2016-01-18 17:23:51	2016-01-18 17:23:51	
18	安全基线检查-立即执行-201...	安全基线检查	立即执行	已完成	2016-01-18 17:23:43	2016-01-18 17:23:43	

任务执行结果

5、报告查看：选择某一任务，可查看该任务历史报告、详细报告情况，详细内容包括：任务基本信息（包括任务名称、开始时间、结束时间、任务类型、检查策略）、变更项、严重级别分布图、主机列表（包括主机 IP 地址、系统类型、各种状态的数量）、主机的详细信息（包括配置项名称、配置项类型、变更类型、当前版本、严重级别、策略名称）。如下图所示：



地址:深圳市南山区学苑大道1001号南山智园A1栋
咨询热线：400-806-6868 | 服务热线：400-630-6430 | 邮箱: market@sangfor.com.cn | 网址：www.sangfor.com.cn



序号	IP地址	系统类型	删除	修改	新增	未变化
1	172.16.0.168	SUSE	0	12	0	1

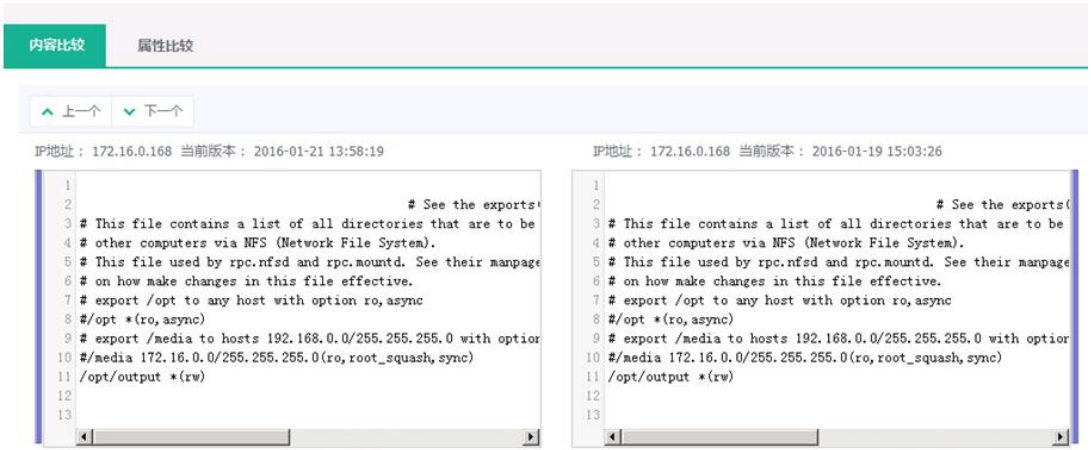
每页显示 10 条　显示 1 至 1 条，共 1 条　<< 1 >> GO：

漏洞　基线　变更

设备地址172.16.0.168

序号	配置项路径名称	配置项类型	变更类型	当前版本	严重级别	策略名称
1	/etc/exports	配置文件	修改	2016-01-21 13:58:19	中级	SUSE默认变更检查策略
2	/etc/hosts.deny	配置文件	修改	2016-01-21 13:58:19	中级	SUSE默认变更检查策略
3	/etc/hosts.allo...	配置文件	修改	2016-01-21 13:58:19	中级	SUSE默认变更检查策略
4	/etc/host.conf	配置文件	修改	2016-01-21 13:58:19	中级	SUSE默认变更检查策略
5	/etc/bashrc	配置文件	未变化	2016-01-21 13:58:19	中级	SUSE默认变更检查策略
6	/etc/passwd	配置文件	修改	2016-01-21 13:58:19	中级	SUSE默认变更检查策略
7	/etc/fstab	配置文件	修改	2016-01-21 13:58:19	中级	SUSE默认变更检查策略

点击变更类型为修改的可以查看当前版本与基线版本的对比情况：



6、报告导出：在任务列表中进入详细报告功能，在详细报告页面中可导出报告，支持 Word、PDF 等格式。

7、报告对比：点击一个任务，在报告列表中选择 2 个报告；报告内容包括任务名称、任务类型、两次报告的生成时间对比、两次报告的变更情况对比。

2.4.4.漏扫任务

典型配置

点击"任务管理"页面新增按钮

1、任务新建：用户输入任务相关属性；如扫描对象选择为 IP 地址段则可支持 IPv4 地址段、一个或多个独立的 IPv4 地址或 IPv6 地址；任务执行的参数包括调度方式（一次还是周期）、周期类型（天、周、月）。如下图所示：

2、任务删除：用户可以在任务列表中删除一个或多个任务（正在执行的任务也可以删除）。
3、停止调度：对于周期型任务可以停止调度，这里停止调度的含义是今后不再进行调度，但如果用户需要继续其任务的调度，则可以使用“启用”功能（即恢复调度）。如下图所示：

4、启用（恢复调度）：对于已经被停止调度的任务，用户可以选择恢复调度。如下图所示：

正在执行的任务

可以查看任务进度，如下图所示：

地址:深圳市南山区学苑大道1001号南山智园A1栋
咨询热线：400-806-6868 | 服务热线：400-630-6430 | 邮箱: market@sangfor.com.cn | 网址：www.sangfor.com.cn

任务执行结果

5、报告查看：在任务报告列表中选择一个报告，点击查看详细；报告可以另存为 PDF、Word、Excel、HTML 等格式。如下图所示：

- 漏洞插件族分类统计列表

序号	插件族/插件	严重	高级	中级	低级	信息	总计
1	服务探测	0	0	0	11	15	26
2	通用	0	2	4	8	10	24
3	产品探测	0	0	0	0	17	17
4	Windows系统	0	4	2	4	6	16
5	Web应用程序滥用	0	0	0	1	12	13
6	Windows:微软公告	0	10	0	0	0	10
7	端口扫描	0	0	0	0	3	3
8	General	0	0	0	0	2	2

- 漏洞CVE年份分类统计列表

6、报告删除：用户可以删除历次任务的一个或多个任务执行报告。

7、报告对比：用户可以选择一个任务的两次报告进行比对，比对的内容有：任务名称、对象范围、任务类型、两次报告的生成时间对比、两次报告的漏洞数量对比（按照 总数、严重级别）、两次任务中发现相同和不同的漏洞；比对结果可以导出为 PDF、Word 等格式。

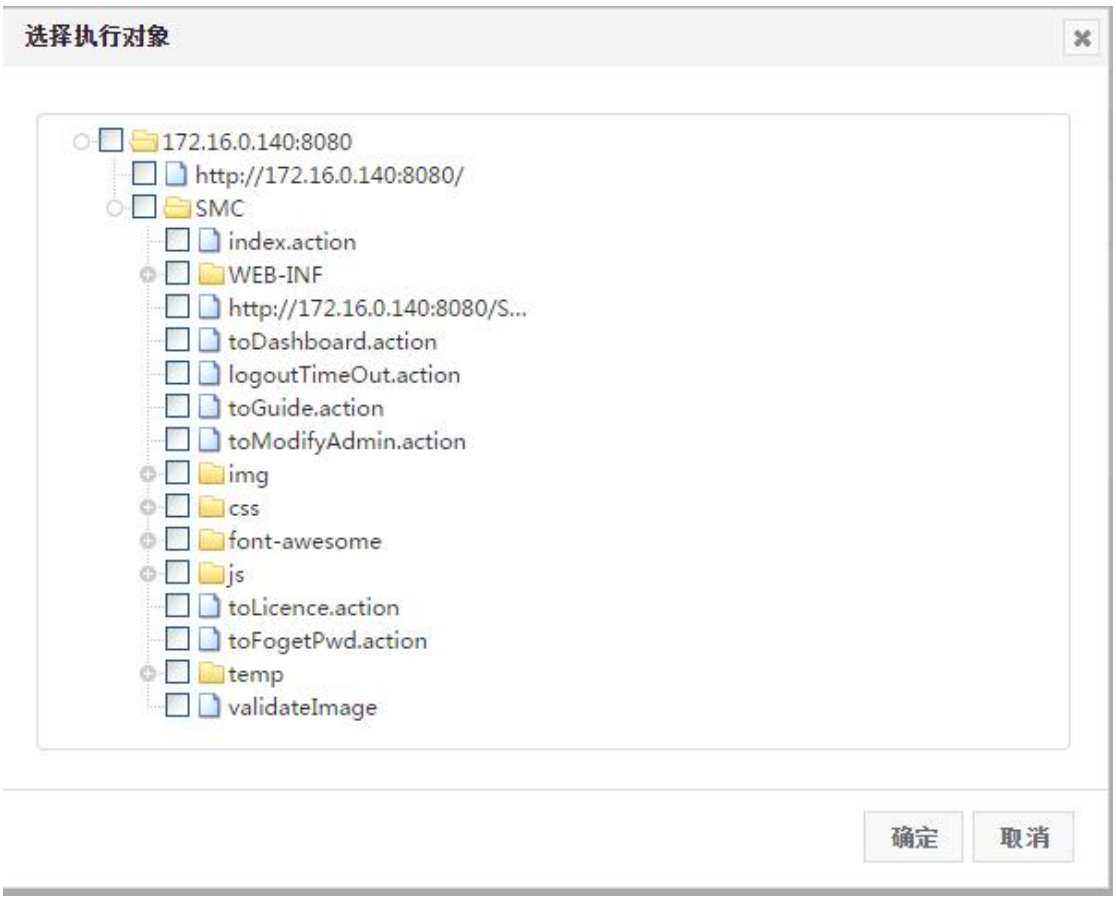
2.4.5.web 任务

点击"任务管理"页面新增按钮

1.任务新建：用户输入任务相关属性；手动输入 url 地址或者带有网站的资产，任务执行的参数包括扫描策略，爬网功能（1.0 和 2.0），任务执行的参数包括调度方式（一次还是周期）、周期类型（天、周、月）。如下图所示：

下一步

可在选择任务对象时点击查看列表按钮选择 URL



用户选择网站资产进行 web 漏洞扫描

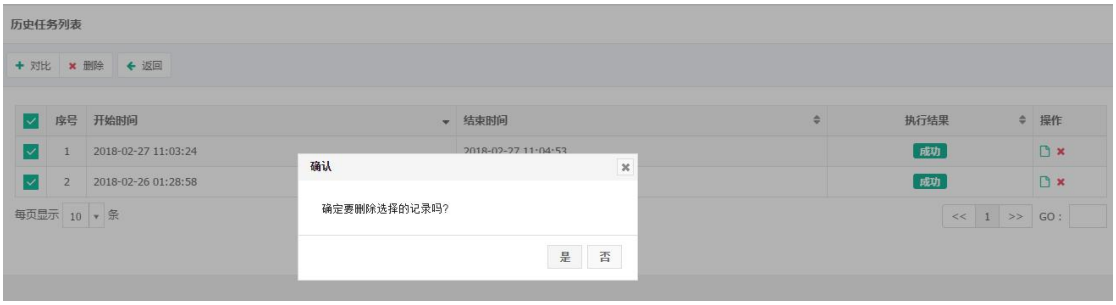
2. 任务删除：用户可以在任务列表中删除一个或多个任务（正在执行的任务也可以删除）。

3.停止调度：对于周期型任务可以停止调度，这里停止调度的含义是今后不再进行调度，但如果用户需要继续其任务的调度，则可以使用“启用”功能（即恢复调度）。如下图所示：

任务执行结果

5. 报告查看：在任务报告列表中选择一个报告，点击查看详细；报告可以另存为 PDF、Word、HTML 等格式。如下图所示：

5. 报告删除：用户可以删除历次任务的一个或多个任务执行报告。



6.报告对比：用户可以选择一个任务的两次报告进行比对，

地址:深圳市南山区学苑大道1001号南山智园A1栋
咨询热线：400-806-6868 | 服务热线：400-630-6430 | 邮箱: market@sangfor.com.cn | 网址：www.sangfor.com.cn

2.5.离线任务配置（选配）

当某些设备网络不可达时，基线检查和变更检查提供离线脚本。

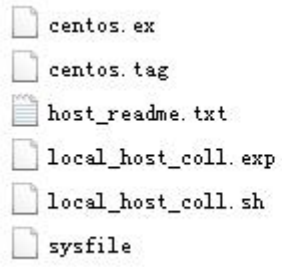
典型配置

1、点击"任务管理"页面离线按钮

通过下载相关系统类型的采集脚本：

2、上传到相关设备上执行脚本，

将下载到的离线检查脚本，上传至目标设备，解压，如 CentOS 解压后为



打开 host_readme.txt 查看脚本执行方法，执行命令后获取采集结果 result.txt，将刚才解压的目录（含 result.txt），打包成新的 zip 文件，导入离线报告。

3、导入成功后即可在任务列表里查看离线任务。

2.6.安全仪表板查看

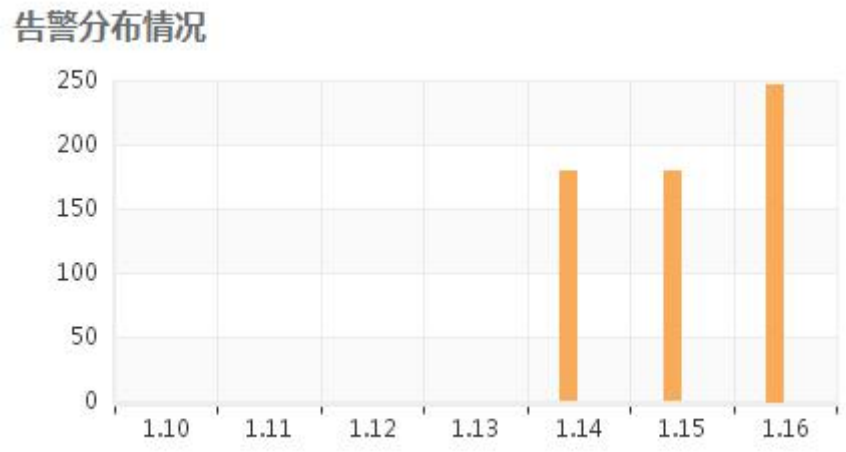
安全事件仪表板查看

仪表板默认包含：最新任务、告警分布情况、系统评分、漏洞分布情况、违规基线分布、变更项分布、设备风险 TOP10、趋势图等。

1、最新任务：列出了最近执行的 5 次任务

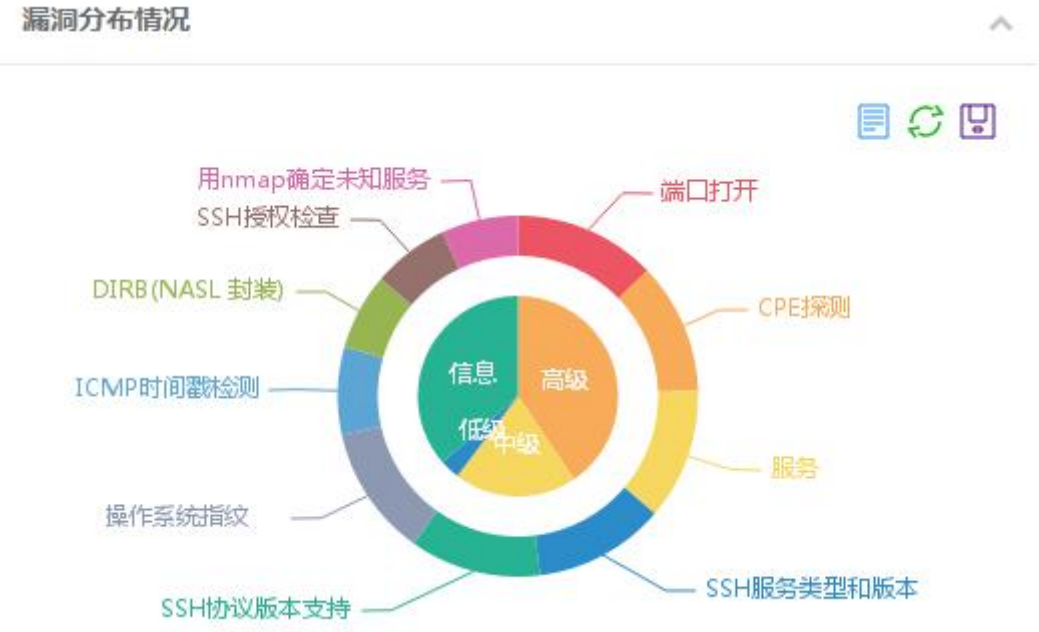
2、告警分布情况：最近 7 天的告警数量

地址:深圳市南山区学苑大道1001号南山智园A1栋
咨询热线：400-806-6868 | 服务热线：400-630-6430 | 邮箱: market@sangfor.com.cn | 网址：www.sangfor.com.cn



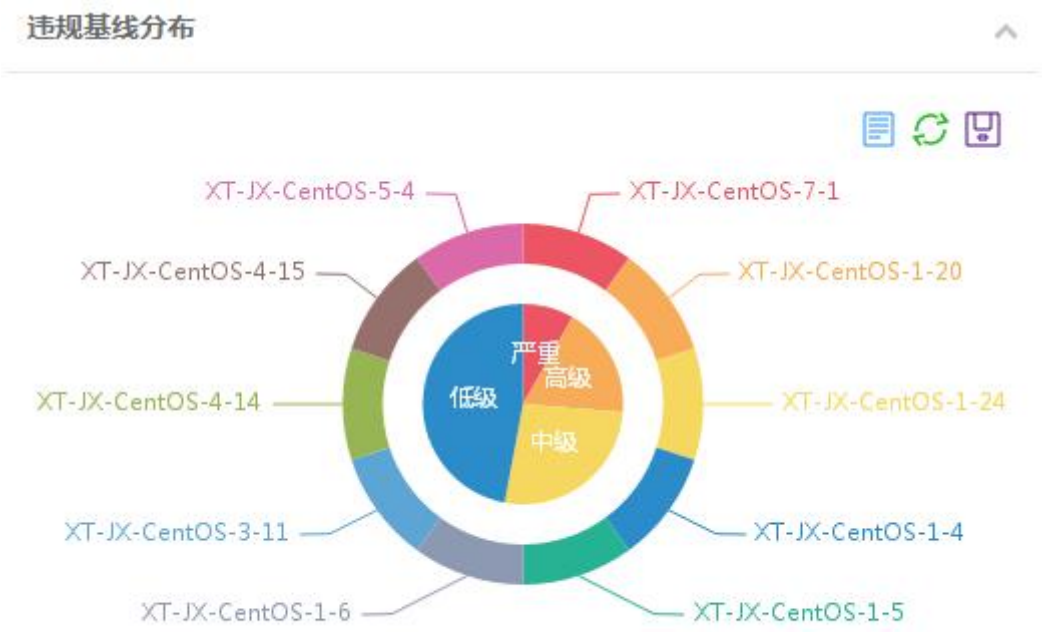
3、系统评分：根据漏洞、基线、变更三个维度展现系统健康状况

4、漏洞分布情况



地址:深圳市南山区学苑大道1001号南山智园A1栋
咨询热线：400-806-6868 | 服务热线：400-630-6430 | 邮箱: market@sangfor.com.cn | 网址：www.sangfor.com.cn

5、违规基线情况



6、变更检查变更项情况

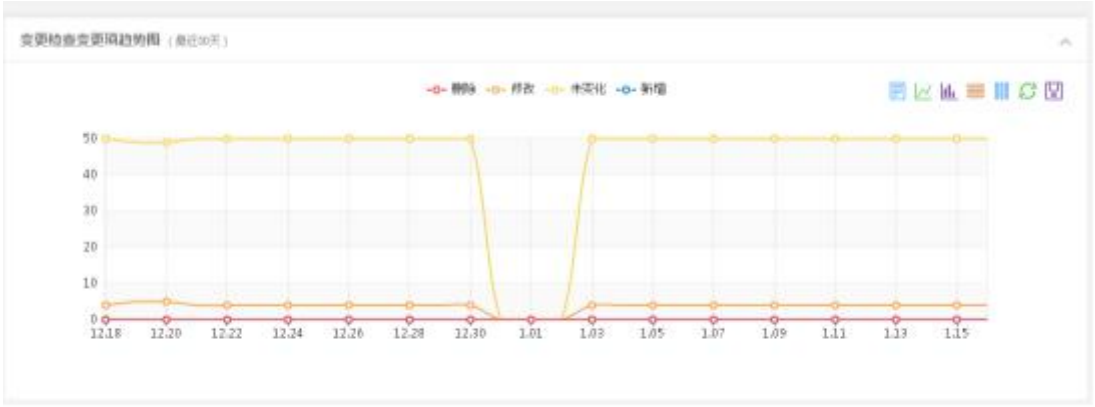
7、设备风险 TOP10

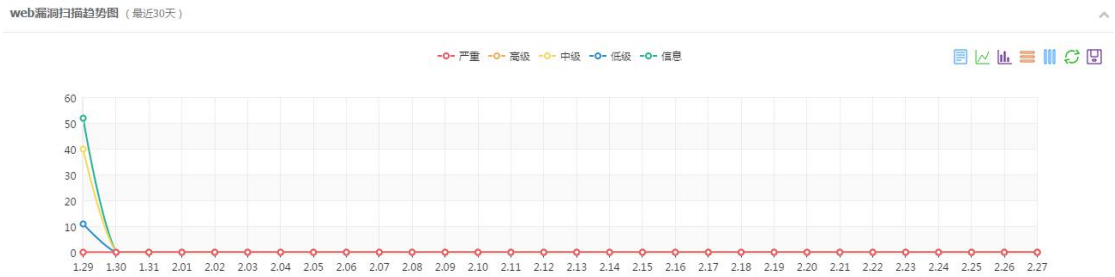
地址:深圳市南山区学苑大道1001号南山智园A1栋
咨询热线：400-806-6868 | 服务热线：400-630-6430 | 邮箱: market@sangfor.com.cn | 网址：www.sangfor.com.cn

设备风险Top10

序号	设备地址	风险严重级别
1	172.16.0.35	中
2	172.16.0.201	中
3	172.16.0.200	中
4	172.16.0.190	中
5	172.16.0.169	中
6	172.16.0.168	中
7	172.16.0.117	中

8、趋势图





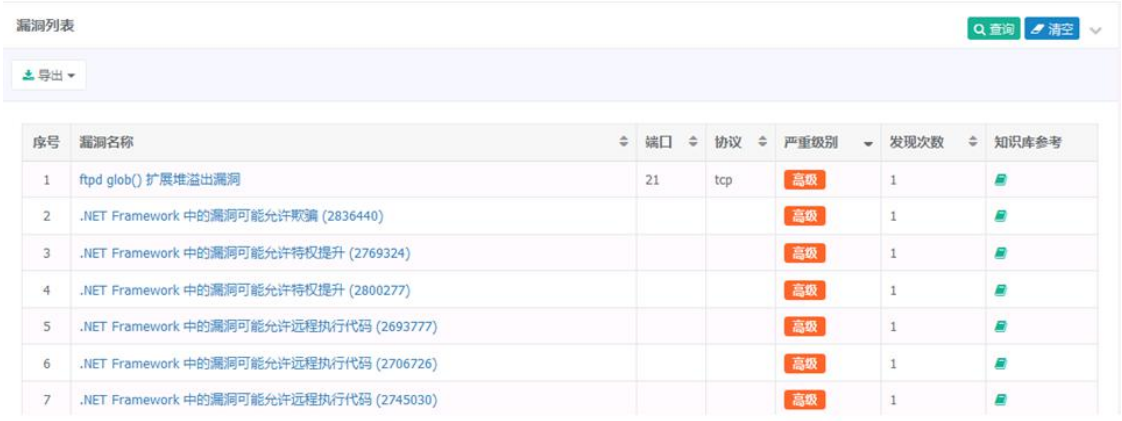
3.脆弱性查询

3.1.漏洞查看

进入“脆弱性查询”->“漏洞”页面

漏洞管理包括如下主要操作：

1、漏洞查看：列表查看登录用户权限范围存在的漏洞，列表中除应显示漏洞的列表属性：



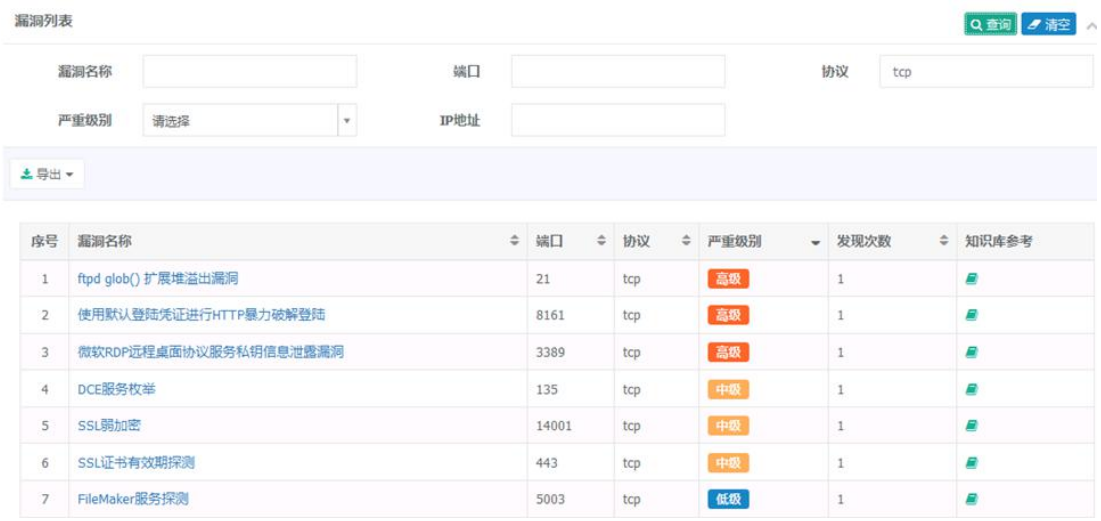
序号	漏洞名称	端口	协议	严重级别	发现次数	知识库参考
1	ftpd glob() 扩展堆溢出漏洞	21	tcp	高级	1	
2	.NET Framework 中的漏洞可能允许欺骗 (2836440)			高级	1	
3	.NET Framework 中的漏洞可能允许特权提升 (2769324)			高级	1	
4	.NET Framework 中的漏洞可能允许特权提升 (2800277)			高级	1	
5	.NET Framework 中的漏洞可能允许远程执行代码 (2693777)			高级	1	
6	.NET Framework 中的漏洞可能允许远程执行代码 (2706726)			高级	1	
7	.NET Framework 中的漏洞可能允许远程执行代码 (2745030)			高级	1	

列表中显示知识库，鼠标移动到知识库参考图标上显示相关参考，如下图所示：

列表中显示发现次数，点击漏洞名称可查看具体哪些 IP 存在此漏洞），如下图所示：

2、漏洞查询：用户可以根据漏洞的相关属性对系统存在的当前漏洞进行查询；查询结果可以导出成报告报告可以另存为 PDF、Word 等格式。

如下图所示：



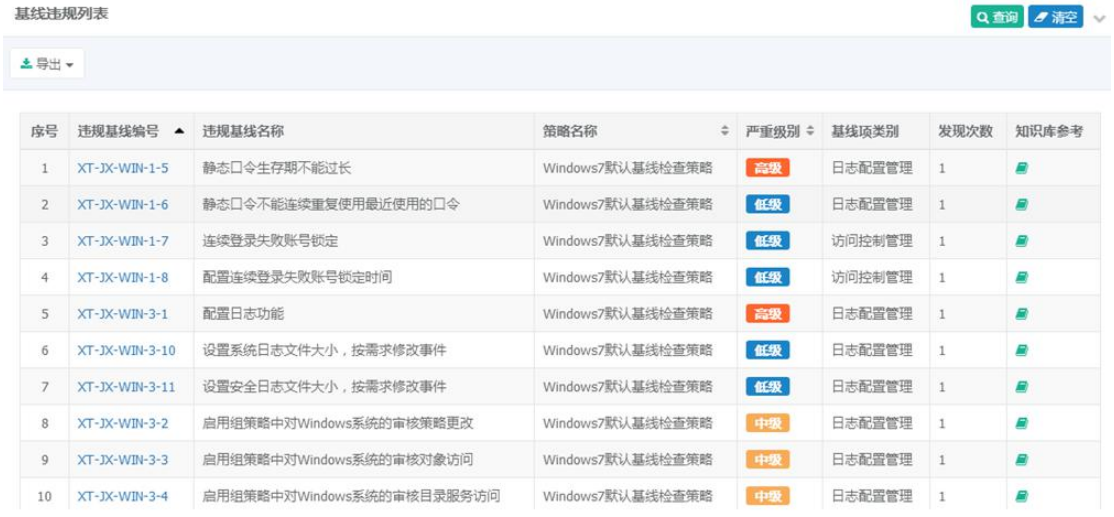
序号	漏洞名称	端口	协议	严重级别	发现次数	知识库参考
1	ftpd glob() 扩展堆溢出漏洞	21	tcp	高级	1	
2	使用默认登陆凭证进行HTTP暴力破解登陆	8161	tcp	高级	1	
3	微软RDP远程桌面协议服务私钥信息泄露漏洞	3389	tcp	高级	1	
4	DCE服务枚举	135	tcp	中级	1	
5	SSL弱加密	14001	tcp	中级	1	
6	SSL证书有效期探测	443	tcp	中级	1	
7	FileMaker服务探测	5003	tcp	低级	1	

3.2.安全基线违规

进入“脆弱性查询”->“安全基线违规”页面

安全基线违规管理的相关操作包括：

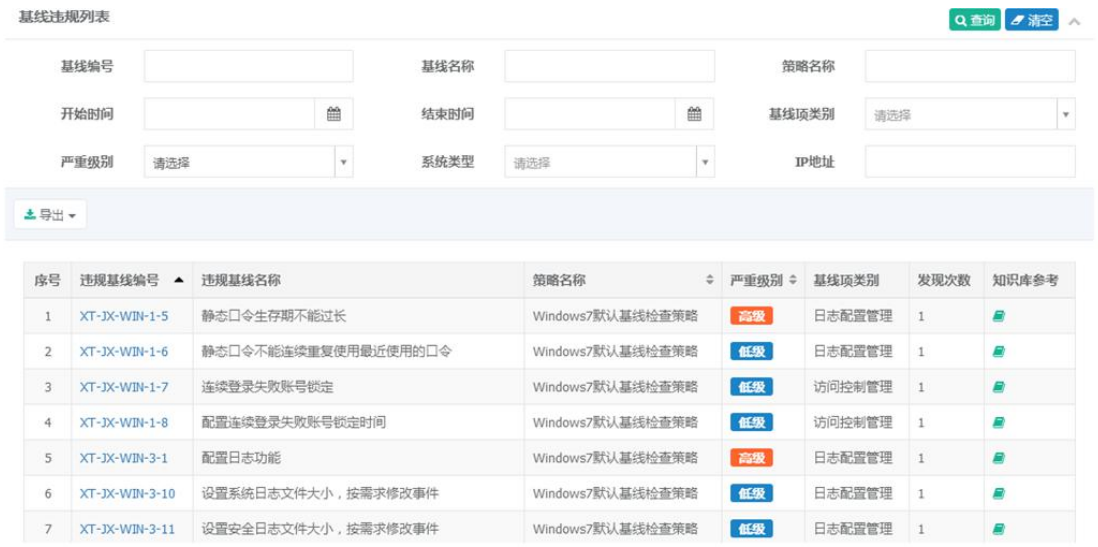
1、违规列表：需显示系统内所有的违规信息情况，以列表方式呈现，列表查看时可以依据某种选中的视图（和用户个人相关），也可不选择任何视图查看；列表内容包括：违规基线名称、违规基线描述、违规对象数。如下图所示：



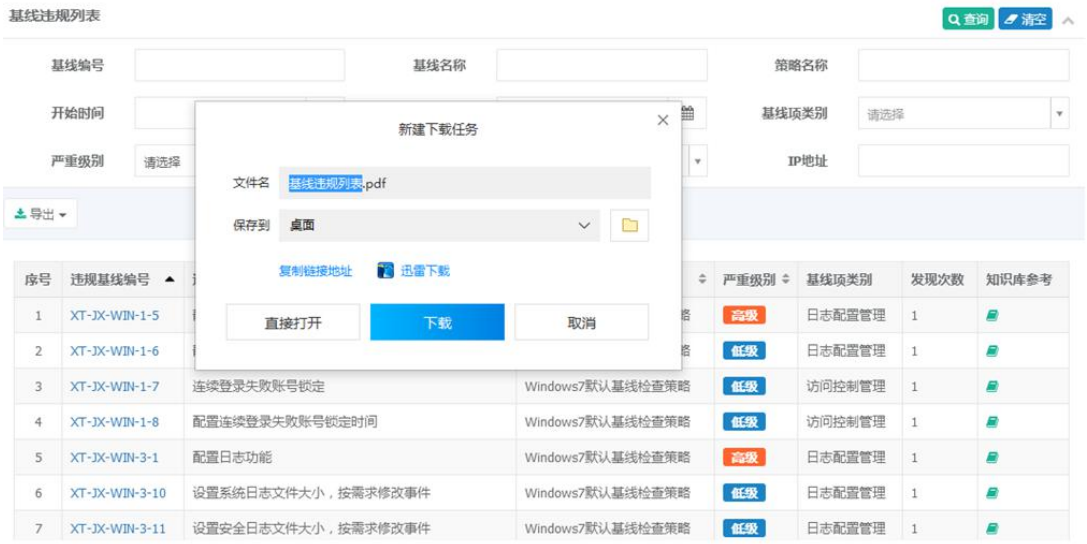
序号	违规基线编号	违规基线名称	策略名称	严重级别	基线项类别	发现次数	知识库参考
1	XT-JX-WIN-1-5	静态口令生存期不能过长	Windows7默认基线检查策略	高级	日志配置管理	1	
2	XT-JX-WIN-1-6	静态口令不能连续重复使用最近使用的口令	Windows7默认基线检查策略	低级	日志配置管理	1	
3	XT-JX-WIN-1-7	连续登录失败账号锁定	Windows7默认基线检查策略	低级	访问控制管理	1	
4	XT-JX-WIN-1-8	配置连续登录失败账号锁定时间	Windows7默认基线检查策略	低级	访问控制管理	1	
5	XT-JX-WIN-3-1	配置日志功能	Windows7默认基线检查策略	高级	日志配置管理	1	
6	XT-JX-WIN-3-10	设置系统日志文件大小，按需求修改事件	Windows7默认基线检查策略	低级	日志配置管理	1	
7	XT-JX-WIN-3-11	设置安全日志文件大小，按需求修改事件	Windows7默认基线检查策略	低级	日志配置管理	1	
8	XT-JX-WIN-3-2	启用组策略中对Windows系统的审核策略更改	Windows7默认基线检查策略	中级	日志配置管理	1	
9	XT-JX-WIN-3-3	启用组策略中对Windows系统的审核对象访问	Windows7默认基线检查策略	中级	日志配置管理	1	
10	XT-JX-WIN-3-4	启用组策略中对Windows系统的审核目录服务访问	Windows7默认基线检查策略	中级	日志配置管理	1	

2、违规详细查看：在安全基线违规列表中，选择某个违规信息，可进一步查看该违规的详细信息。包括：基线编号、基线名称、基线配置项类别、基线内容、系统类型、描述、解决方案等。如下图所示：

3、查询：在违规列表中提供查询功能，输入相关查询字段进行查询。如下图所示：



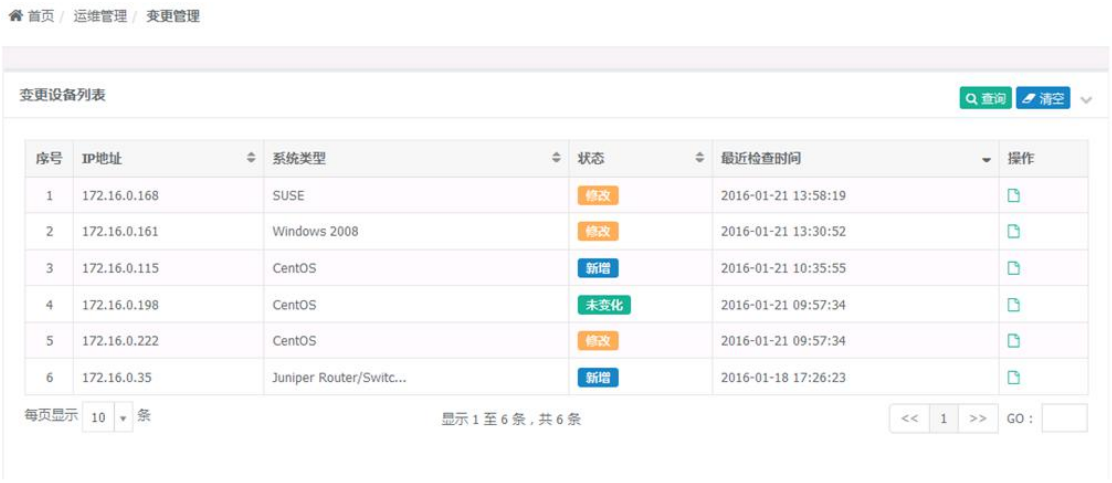
4、导出报表：在违规列表中，点击导出按钮，选择导出的格式类型，支持格式包括 WORD、PDF、HTML 等。如下图所示：



3.3.变更管理

进入“脆弱性查询”->“变更管理”页面

查看设备列表：



查询：

查看检查结果：

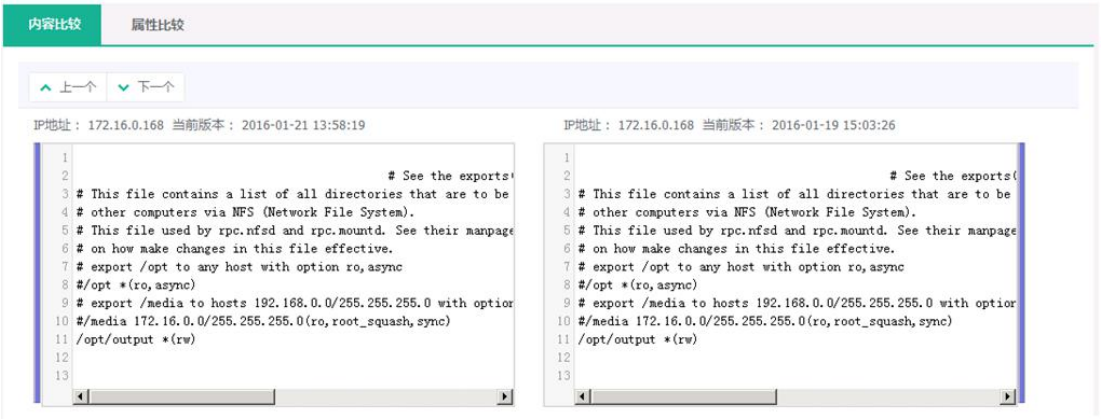
查看最新配置：

将最新配置设为基线，以后以此为基线进行变更比较：

点击配置项名称，查看配置项历史版本：

点击版本名称查看详情：

与当前基线比较：



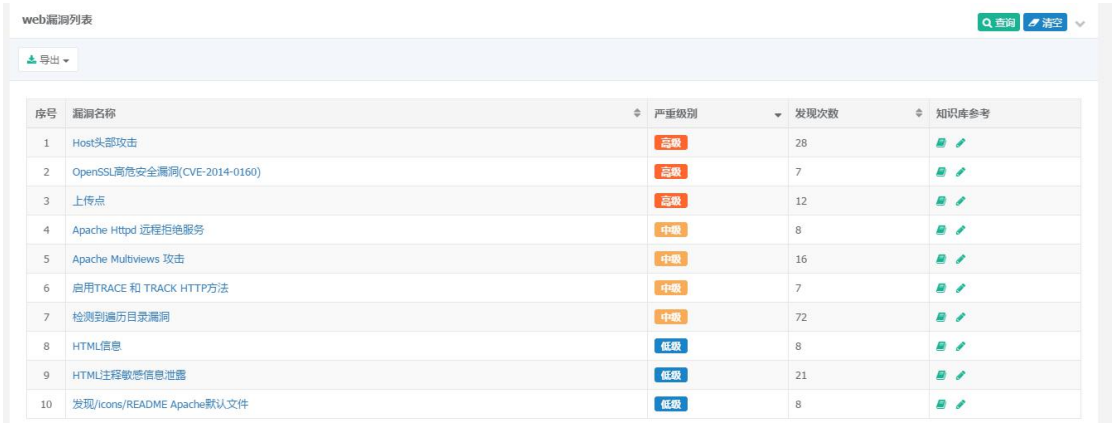
与其他设备的相同基线比较：

3.4web 漏洞查看

进入“脆弱性查询”->“web 漏洞”页面

web 漏洞管理包括如下主要操作：

1.web 漏洞查看：列表查看登录用户权限范围存在的 web 漏洞，列表中除应显示 web 漏洞的列表属性：



列表中显示知识库，鼠标移动到知识库参考图标上显示相关参考，如下图图所示：

列表中显示发现次数，点击 web 漏洞名称可查看具体哪些 url 存在此 web 漏洞），如下图所示：

2、web 漏洞查询：用户可以根据 web 漏洞的相关属性对系统存在的当前 web 漏洞进行查询；查询结果可以导出成报告报告可以另存为 PDF、Word、excel 等格式。

如下图所示：

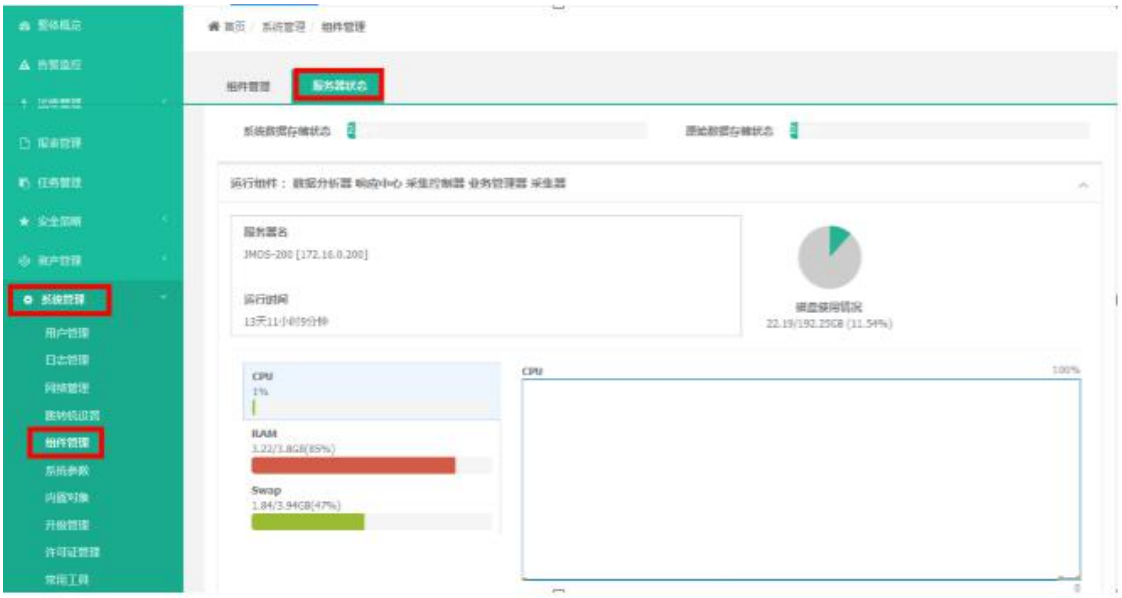
4.实施后设备运行检查

4.1.整体运行状态检查

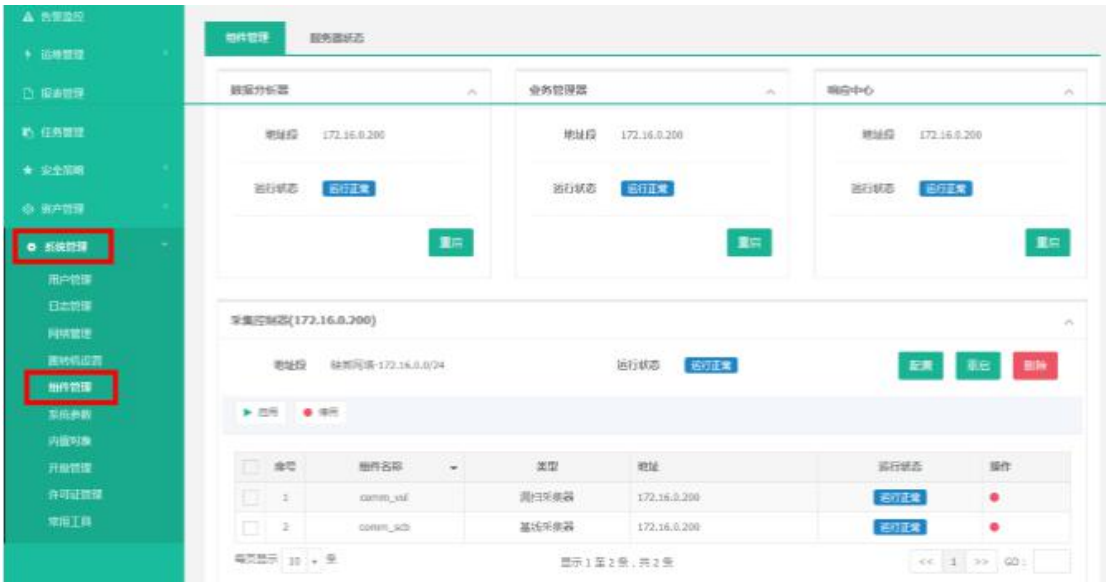
基础检查

操作方法：

1、 在“系统管理”>“组件管理”查看设备运行时间、CPU、内存、硬盘利用率



2、在菜单"采集管理"> "采集器管理"查看采集器运行状态。



注： 如发现有组件运行状态为“异常”，可尝试点击“重启”按钮恢复。

检查标准

1、检查个组件运行是否正常

2、硬盘利用率低于 80%是正常的，高于 80%则系统默认会自动清理硬盘；

3、CPU 和内存稳定运行时不高于 80%是正常的，CPU 或内存达到 80%以上，需要关注：

- 设备是否正在高 EPS（每秒事件量）的情况下接收日志：EPS（每秒事件量）越高，CPU 利用率会越高。

4.2.设备日志检查

基础检查

操作方法：

1、登录管理控制台 WEB 页面

2、点击"系统管理">"日志管理"

这里记录了系统各组件的运行日志，包括异常故障日志。

检查标准

1、检查系统日志里是否有异常日志，系统运行的日志都会在这里显示。

4.3.主要功能使用情况检查

基础检查

操作方法：

1、登录管理控制台 WEB 页面。

2、查看"任务管理"里周期任务是否按时执行。

3、查看“告警监控”里是否按照告警规则产生告警。

4、查看"整体概览" 下各个仪表盘是否有相应的统计报告产生。

检查标准

操作方法：

1、资产管理页面选择一个资产进行快速检查。

2、任务管理页面创建一个手动任务，每天手动执行一次。

3、安全概览下个仪表盘显示正常，统计数据正确。

5.常见问题处理

5.1.配置了资产，却采集不到数据

常见的几种可能如下：

（1）网络不通

解决方法：设备与间互 ping，确认联通性；可以登录硬件管理平台 https://x.x.x.x:8082(x.x.x.x 为具体地址)，默认用户名 admin，默认密码 admin，进行 ping 操作，如下图:

登录硬件管理系统

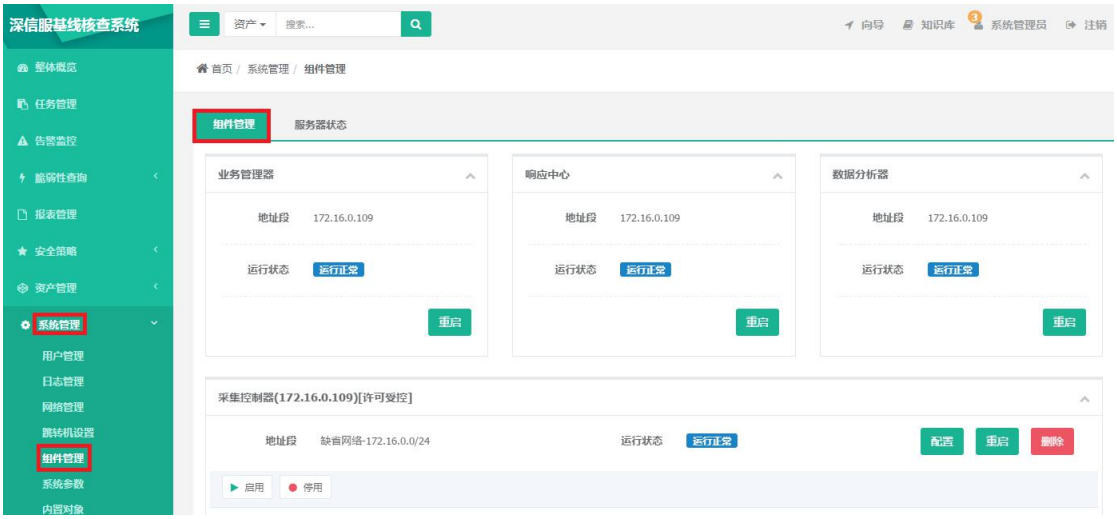
执行 ping 等操作

地址:深圳市南山区学苑大道1001号南山智园A1栋
咨询热线：400-806-6868 | 服务热线：400-630-6430 | 邮箱: market@sangfor.com.cn | 网址：www.sangfor.com.cn

（2）没有将资产所在网段添加到采集控制器里

新增的资产所在网段如果不在默认网段范围内，需要在采集控制器里添加管理的网段

进入“系统设置”->“组件管理”



点击“配置”按钮，添加管理网段

（3） 资产账号口令错误

确认配置的资产帐号口令是否正确

6.漏洞库更新

漏洞库更新频率为月更新，离线升级包形式。

地址:深圳市南山区学苑大道1001号南山智园A1栋
咨询热线：400-806-6868 | 服务热线：400-630-6430 | 邮箱: market@sangfor.com.cn | 网址：www.sangfor.com.cn