

乐维自动化管理系统

使用手册

一、概述

1、平台简介

乐维自动化管理系统是面向网络、安全设备及对应服务器的高效自动化运维及巡检平台。

乐维自动化管理系统能够将标准运维操作快速简易地实现整合和自动化，对全网中不同厂商的网络设备、安全设备、服务器进行集中的自动化配置和健康巡检管理，控制不当变更，规避人工错误风险，降低运维成本。此外，NC能够使企业的 IT 策略和相应要求自动化强制实施，并提供快速的智能化巡检检查能力，健全企业高可用性和网络环境安全性。

本产品采用了先进的 B/S 架构，利用可维护的脚本驱动包的方式来实现 IT 设施配置自动化，抽象了实际设备操作的底层实现，让工程师能够在更上层上请求和下发命令。本系统具有优秀的兼容性和扩展性，可以通过编写新的设备模型(xml/xsd)、驱动脚本(perl)，实现对新设备、新版本的良好支持；同时，通过升级原有的模型和驱动，可以扩展设备的管理深度，增加新的自动化操作功能。

本软件能对分布广泛的多厂商设备进行自动化的配置变更、配置管理、健康检查以及跟踪和控制，从而实现最大的运维收益。

乐维自动化管理系统提供标准 webservice 接口，易与第三方工单流程系统、网管系统或合规系统集成，从而实现完整的 IT 生命周期工作流自动化。

2、三员权限

乐维自动化管理目前支持 web 管理，是最直观的管理方式，并提供最全面的功能管理界面，建议用户使用 Chrom 浏览器。

2.1 web 用户

乐维自动化管理在 web 管理界面下有三类用户：

2.1.1 系统管理员

负责系统日常运行维护，包括资产设备的配置备份（定期或不定期）、巡检（定期或不定期）、合规（定期或不定期），进行系统功能、实时性能监控和必要的状态检查，能够在系统中断、运行瘫痪的情况下，及时排除相应故障，避免或尽可能降低系统损失，且负责系统用户的创建和维护，以及解锁因尝试登陆失败锁定的用户。

2.1.2 安全保密管理员

主要负责系统的安全保密管理工作，包括对用户账号权限管理和对系统所产生日志的审查分析，是整个系统安全方面的主要责任人，应由既具备技术能力又熟知安全保密管理要求的工作人员担任。包括设置页面的超时时间、登陆最多尝试次数、用户密码最小长度及密码更新周期，角色权限管理以及给新建用户设置初始化密码和分配角色。

2.1.3 审计员

安全审计员主要负责对系统管理员、安全保密管理员的操作行为进行审计跟踪分析和监督检查，及时发现违规行为，并定期向系统安全保密管理机构汇报相关情况。包括审计查看登录日志、设备操作日志及平台操作日志。

2.2 web 页面登录

步骤 1：确定客户端主机已正常联网。打开浏览器谷歌，用 HTTPS 方式连接乐维自动化管理系统的 IP 地址，例如：https://<ip>:<port>，系统默认使用 8080 端口。



步骤 2：在如图所示的登录界面中，输入用户名和密码，单击【确认】。

提示：系统默认三次密码错误即锁定登录，可以通过登录安全保密管理员或系统管理员进行解锁。如果系统管理员和安全保密管理员均被锁定，请联系厂商。

如出现如图下图所示界面，是由于系统的 SSL 证书失效导致，请联系服务商进行 SSL 证书更新；也可以按如下指示继续操作完成登录（不推荐）。单击【高级】，选择【继续前往 IP（不安全）】，接受乐维自动化管理系统证书加密的通道。



二、功能介绍

2.1 首页

在输入正确的账号和密码文本后点击“登录”按钮，进入运维平台首页面，如图所示：



首页的导航栏由业务、网络、资产、配置、合规、巡检、监控、告警、任务、知识、系统、审计等 12 个部分组成。

首页主要以图形报表展示了：受控资产、在线资产、备份状态、配置状态、合规资产、合规检查项、不合规设备、不合规检查项、巡检资产、巡检检查项、不健康设备、不健康检查项等 12 项内容，便于提供资产管理参考数据。

2.2 业务

以业务视角管理资产和展示相关信息，包括业务自身的管理，业务与资产的关联归属管理，和从业务维度的统计分析。

2.2.1 业务信息

创建业务列表，以业务形式添加受控资产。自定义业务名称，划分所属业务的受控资产。

业务统计 业务信息			
名称	描述	所有者	设备数量
☒ 缺省业务	系统默认缺省的业务名称	系统管理员,TEST,TEST副本,TEST副本副本...	18
☐ 测试	测试		8
☐ 新发现资产	新发现资产缺省归属的业务	系统管理员	0

在业务信息页面中可以新建业务、编辑业务、删除业务。具体操作如下：

2.2.1.1 新建业务

在业务信息页点击  图标，进入新建业务界面，可以为新建的业务命名，添加业务描述。新建的业务可以设置为父业务，也可以指定一个父业务成为其子业务。当取消勾选 **设为父业务：** ☐ 时，可以为其添加已录入系统的资产设备。如勾选 **设为父业务：** ☒，保存后可以在资产模块中为该业务添加设备资产。

业务名：

描述：

指定父业务：

设为父业务：☐

添加设备：

设备预览：

序号	IP地址	设备名称	重名	业务名	操作
暂无数据					

2.2.1.2 编辑业务

在业务信息列表中勾选任意业务，点击  图标，即可进入编辑业务界面。在此处可以修改业务名称、描述信息、重新指定父业务以及增减业务中的设备。

业务名：

缺省业务

描述：

系统默认缺省的业务名称

指定父业务：

请选择

设为父业务：

☐

添加设备：

设备预览：

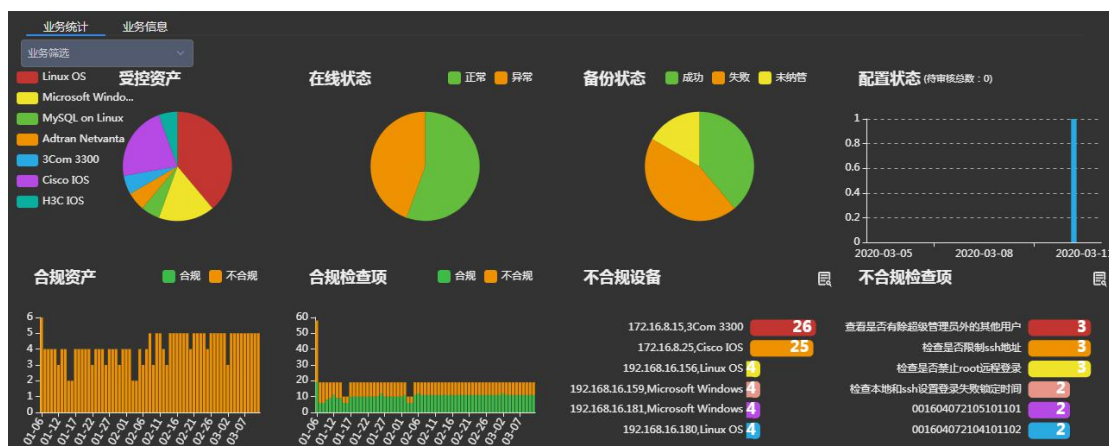
序号	IP地址	设备名称	驱动	业务名	操作
1	192.168.16.180	CA-test	Linux OS	缺省业务	删除
2	192.168.16.181	WIN-E01103M886M	Microsoft Windows	缺省业务	删除
3	192.168.16.158	localhost.localdomain	Linux OS	缺省业务	删除
4	192.168.16.13	-	Linux OS	缺省业务	删除

2.2.1.3 删除业务

在业务信息列表中勾选任意业务，点击  图标，即可删除业务。由于删除业务可能会影响使用该业务的用户，因此操作需慎重。

2.2.2 业务统计

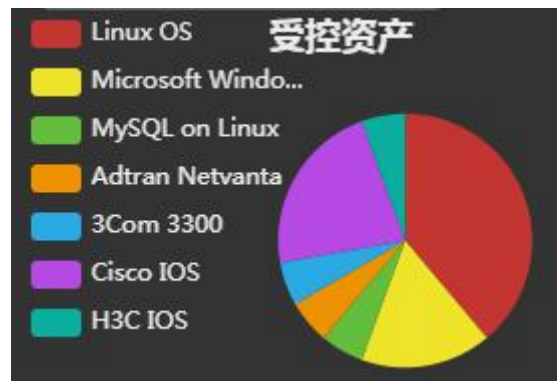
业务统计以图的形式直观展示当前所选的业务的状态，包括受控资产类型，在线状态，合规资产，合规检查项，备份状态，配置状态，不合规设备，不合规检查项，巡检资产，巡检检查项，不健康设备，不健康项。



2.2.2.1 受控资产

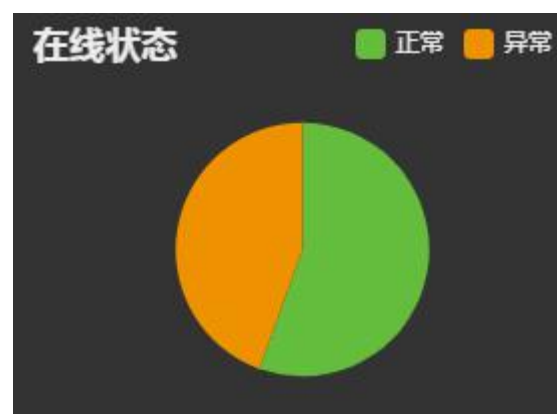
受控资产指的是当前纳管的资产，包括导入的资产和发现的资产。

受控资产图表可以清晰的展示该业务的受控资产类型，及占总数量的百分比，如图所示：



2.2.2.2 在线状态

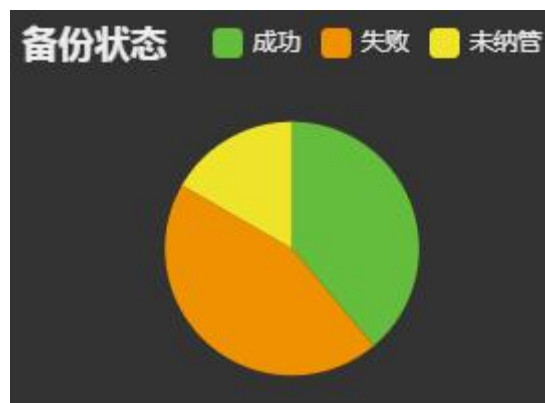
在线状态图表示当前该业务中的受控资产的 ping 连通的状态。直观显示当前业务在线和不在线的比率，双击图表中的“正常/异常”，以列表形式展现具体是哪些受控资产的在线状态，如图所示：



2.2.2.3 备份状态

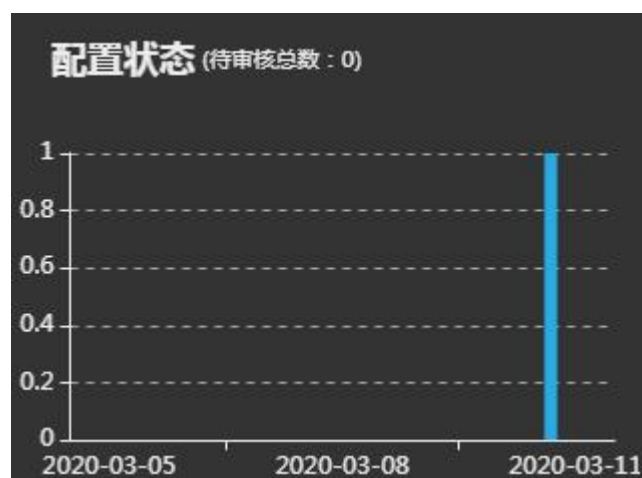
备份状态指受控资产的备份情况。文中的备份指平台执行相关命令获得当前系统的信息。如网络设备，可执行备份，获取当前正在运行的配置信息。

直观显示当前业务受控资产的备份状况，同时点击进备份失败的区域会跳转到相应页面，以列表形式显示备份失败的受控资产，点击>，可展开查看备份失败的具体原因，如图所示：



2.2.2.4 配置状态

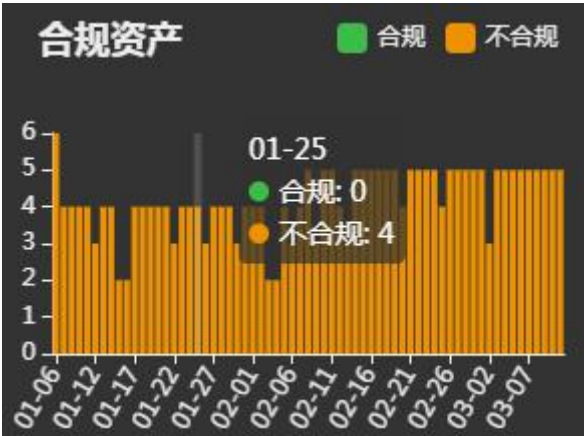
配置状态指备份获得的配置信息的状态，以柱状图的形式显示近一周备份后配置新增、待审核、审核通过、审核拒绝数量，点击可以看到日期当天具体的受控资产配置状态，如图所示：



2.2.2.5 合规资产

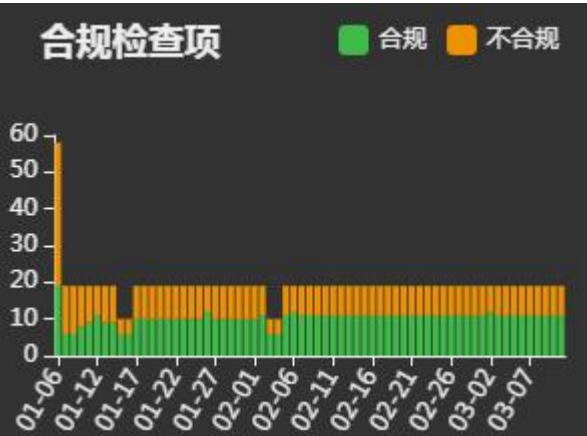
合规资产从资产维度统计该业务内执行合规检查的情况。

合规指对当前资产检查是否符合等保规定。以柱状图的形式直观展示近一个月的合规检查的资产，如图所示：



2.2.2.6 合规检查项

合规检查项是从检查项维度统计合规检查中符合规定和不符合的情况。直观展示近一个月合规结果中合规项和不合规项的总数，如图所示：



2.2.2.7 不合规设备

不合规设备指重点关注在合规检查中，出现不合规项的资产。

缺省显示前 6 个不合规项最多设备，包括设备 ip，设备类型以及不合规的数量，点击可以看到该设备的具体不合规检查项；全部的不合规设备可通过统计图右上角的数据列表查看。如图所示：



2.2.2.8 不合规检查项

不合规检查项是重点关注合规检查后出现的不合规项。

缺省显示前 6 个不合规项最多的具体不合规的检查项名字，点击可看到是哪个设备的不合规项；全部的不合规项可通过统计图右上角的数据列表查看。

如图所示：



2.2.2.9 巡检资产

巡检资产是从资产维度统计业务内资产的健康情况。显示近一个月进行巡检的受控资产健康不健康的变化情况，点击可看见具体的受控资产的巡检情况。

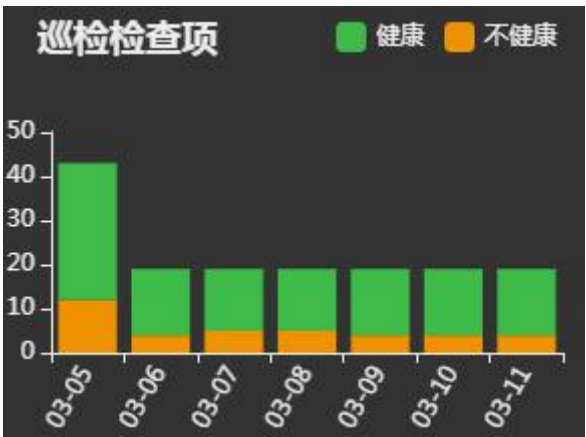
如图所示：



2.2.2.10 巡检检查项

巡检检查项是指巡检任务的所有检查项的统计。

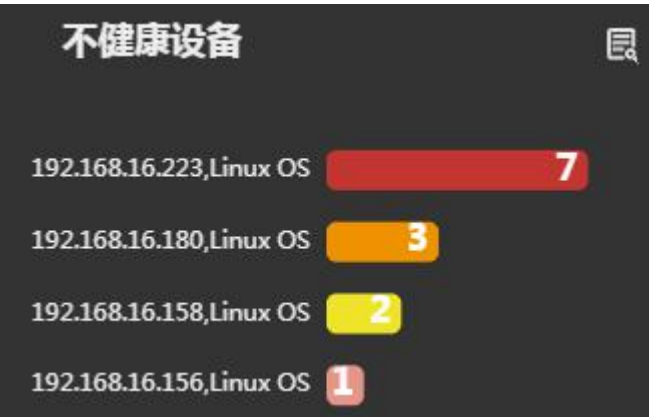
显示最近一个月进行巡检的内容的健康和不健康的巡检项的变化情况，点击可看见是哪些巡检项，以及是具体哪个巡检任务。如图所示：



2.2.2.11 不健康设备

巡检过程中，出现检查项异常的设备均为不健康设备。

显示不健康项最多的 3 台设备的 ip，设备型号，以及巡检不健康项的数目，
点击可以看到具体的不健康项，如图所示：



2.2.2.12 不健康项

巡检过程中出现的异常结果即为不健康项。

显示巡检中出现次数最多的具体的不健康的巡检项，点击可看到具体的受
控资产的不健康巡检项。如图所示：

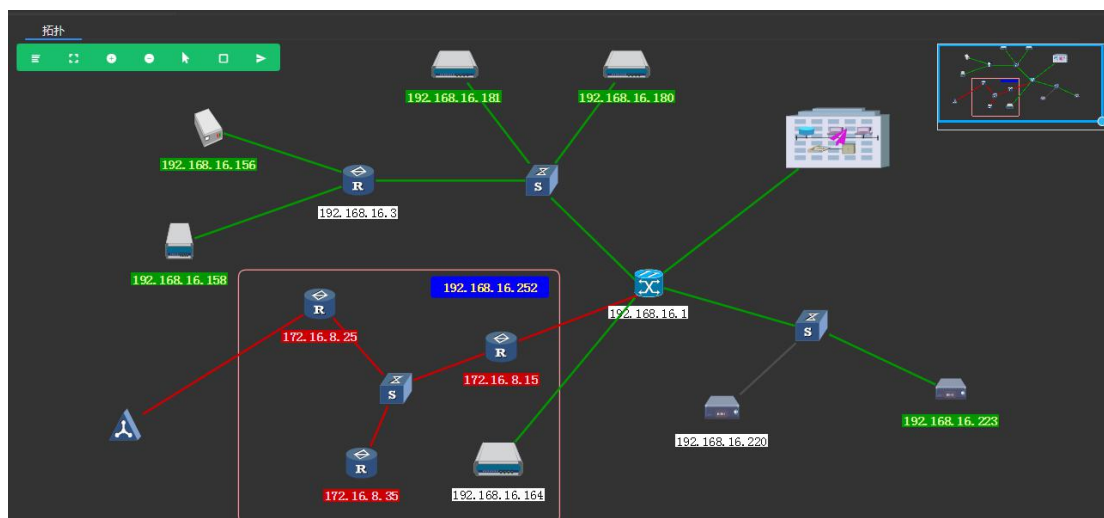


2.3 网络

2.3.1 拓扑

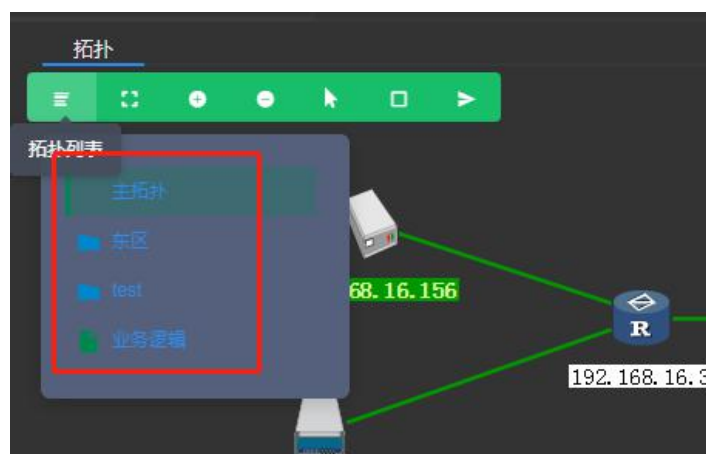
拓扑是指当前的网络结构及连接关系。

可以绘制拓扑图，直观显示设备互连关系，显示设备当前在线状态。



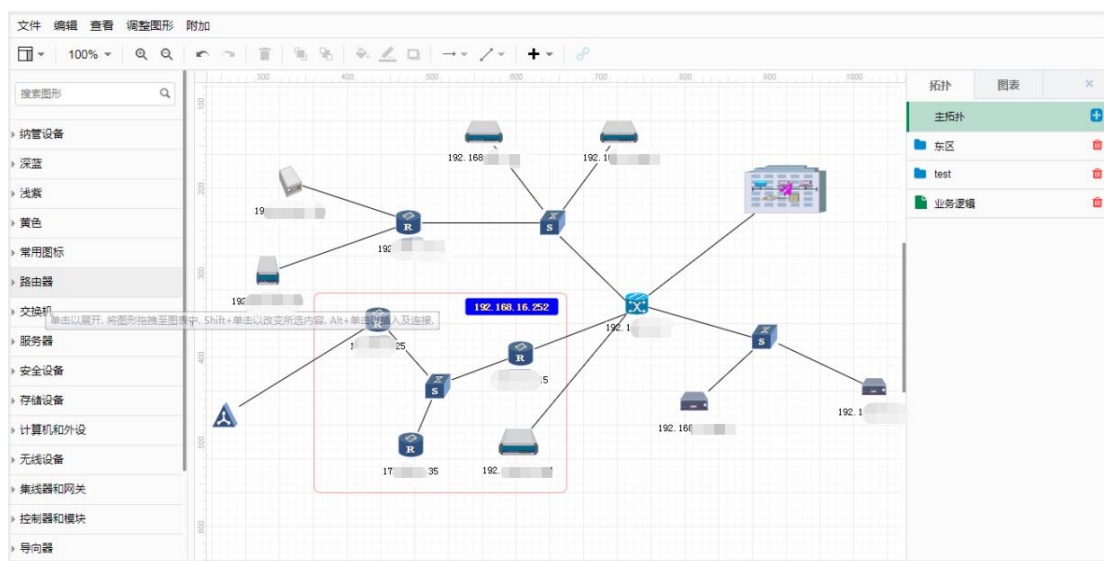
2.3.1.1 拓扑列表

拓扑列表是用来展示已经绘制完成的拓扑图，用户可以通过拓扑列表完成对当前展示内容的切换。



2.3.1.2 拓扑绘制

点击  按钮进入拓扑编辑器页面。



用户可以从左侧图形列表中选择对应设备、建筑、连线等图形完成拓扑图的绘制。右侧拓扑列表可以完成拓扑图新增、编辑、删除等操作。

2.4 资产

2.4.1 资产台账

资产台账左侧以树状形状显示资产类型，右侧列表形式展开该类型的资产。

资产台账用于用户上传记录资产信息。

2.4.1.1 资产类型

资产类型是帮助用户在平台中构建资产台账。

可以帮助用户区分资产，构建父子类型资产类型，父类型可以实现层级管理，子类型则更针对资产层面的管理，可将资产具体到点的位置。

推荐划分资产类型如下：



提示：资产类型可以根据公司的实际资产表情况添加，名称均可自定义

点击资产类型右侧的管理，可以进行添加资产类型。



点击  即可新建资产类型，父类型可根据资产类型的具体情况选择。

添加资产类型

名称

父类型

请选择

描述

取消

保存

选中已创建好的资产类型，点击右上角按钮编辑资产类型，可以修改该资产类型的具体名称。

编辑资产类型

名称

云计算系统

父类型

请选择

描述

取消

保存

选中已创建好的资产类型，点击右上角资产属性按钮，可以对该资产进行自定义资产属性。点击上下箭头可以调整属性的顺序。

基础信息网络 - 资产属性

名称	类型	显示	必填	描述
资产编号	文本	☒	☐	-
重要程度	选择框	☒	☐	-
机密性	文本	☐	☐	-
完整性	文本	☐	☐	-
可用性	文本	☐	☐	-
联系人	文本	☐	☐	-
安全级别	选择框	☒	☐	-
地理位置	文本	☒	☐	-
描述	文本	☒	☐	-
质保期	时限	☒	☐	-

推荐构建的资产属性为：

系统管理软件/平台名称、所在设备名称、版本、主要功能、IP 地址、重要程度、联系人、地理位置、资产编号、描述、质保期、可用性、机密性、完整性、安全级别。

提示：父类型创建的资产属性可被子类型继承，子类型可选择是否继承父类型的属性

选中某一资产类型，点击右上角的  删除按钮，即可删除该资产类型，如果该资产类型下有具体的资产，则无法删除，只能删除空的资产类型。

2.4.1.2 资产列表

添加好资产属性后，可以在资产台账处看见。如图所示：

■	状态	ID	系统管理 软件/平台 名称	所在设备 名称	版本	主要功能	IP地址	重要程度	联系人	地理位置	资产编号	描述	质保期	可用性	机密性	完整性	安全级别	操作
■	>	27	Exsi	192.16...	-	管理、...	192.16...	非常重要	-	-	-	-	-	-	-	-	-	
■	>	28	esxi5	192.16...	5	管理、...	192.16...	非常重要	-	-	-	-	-	-	-	-	-	

资产列表是以列表的形式展现资产信息，如 excel 表，可以建左侧的资产类型当做表名。右侧的资产列表当做表内容，则属性为表中每一列的表头。帮助用户容易理解和使用资产台账。

添加资产：点击右上角的  按钮，填写属性信息，可以添加一条资产。

系统管理软件或平台 - 资产添加

系统管理软件/平台名称		所在设备名称	
版本		主要功能	
IP地址		重要程度	请选择
联系人		地理位置	
资产编号		描述	
质保期		可用性	请选择
机密性	请选择	完整性	请选择
安全级别	请选择		

附件

上传附件

取消 保存

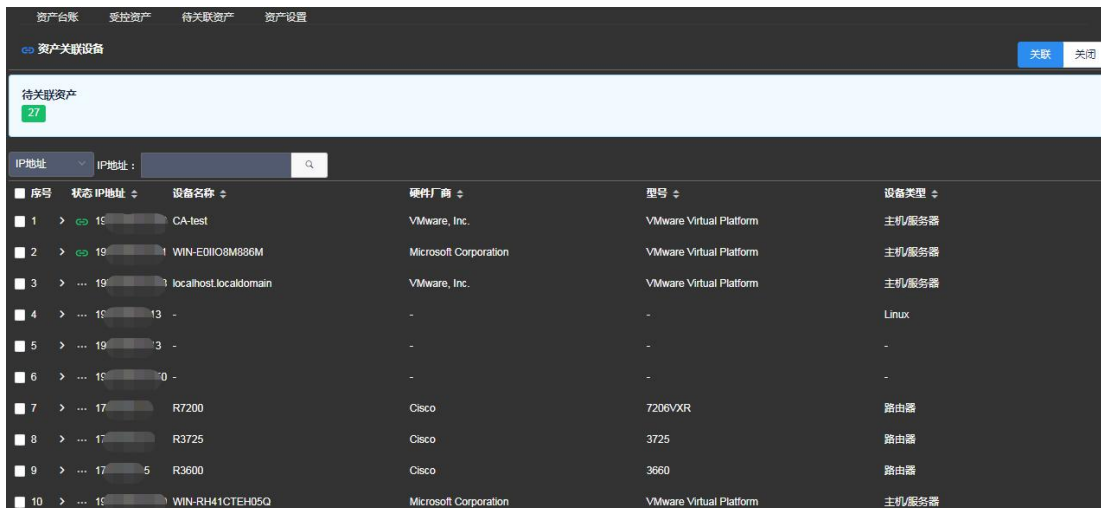
资产导入：点击右上角云符号，可以看到资产模板下载，资产导入，资产导出功能。



点击资产模板下载，可以下载创建好的资产模板，填写对应的资产信息，可以通过资产导入功能批量导入资产条数。通过使用资产导出功能，可以导出已导入的资产信息。



关联资产：主要是为了将资产信息和资产相互联系。用户在查看资产台账时直接可以查看到该条资产信息是对应的哪个资产便于用户使用。选中一条资产，点击右上角  按钮关联资产，可以和受控资产进行关联，弹出的页面，选择要关联的设备，点击右上角的关联即可将资产与设备进行关联。



查看资产信息及关联的资产：点击资产列表的  按钮，即可看到该条资产的所有属性信息和已关联的受控资产的 ip 和类型。



2.4.2 受控资产

受控资产左侧是业务列表，右侧是业务内包含的受控资产

受控资产显示当前业务纳管的所有资产信息。其中缺省业务包含所有的受控资产，其他的业务则各包含其含有的资产。新增的资产未划分业务则默认为缺省业务，方便用户在业务添加资产时可以从缺省业务中查询到未指定业务的资产。

序号	状态	IP地址	设备名称	硬件厂商	型号	设备类型	描述	操作
1	...	10.6	-	-	-	-	-	[Icons]
2	...	172.15	R7200	Cisco	7206VXR	路由器	模拟111	[Icons]
3	...	172.25	R3725	Cisco	3725	路由器	模拟2	[Icons]
4	...	172.25	R3600	Cisco	3660	路由器	模拟3	[Icons]
5	...	192.3	-	-	-	-	神道数据库	[Icons]
6	...	192.3	-	-	-	Linux	-	[Icons]
7	...	192.5	-	-	-	-	-	[Icons]
8	...	192.6	-	-	-	-	-	[Icons]
9	...	192.14	localhost.localdomain	VMware, Inc.	VMware Virtual Platf...	主机/服务器	-	[Icons]
10	...	192.2	-	-	-	-	-	[Icons]

点击业务列表右侧管理可跳转到业务信息处修改业务信息。

2.4.2.1 添加设备

点击右侧  按钮，填写添加设备信息，完成后，点击下一步，填写账号口令信息，缺省可不填。填写完毕后点击保存，可以保存该资产信息，也可以点击下一步，选择是否立即执行备份后保存即可。

添加资产

1 添加设备 2 账户口令 3 协议端口 4 执行备份

< 上一步 下一步 >

IP地址: [Input Field]

描述: [Input Field]

驱动: Cisco IOS

所属管理网络: Default

业务 1: 请选择业务 [Dropdown] 删除

+ 添加业务

取消 保存

2.4.2.2 批量导入资产

点击右上角的  资产导入按钮，可下载资产模板，填写信息。填写完成后，点击“请选择文件”即可上传 excel 表，批量导入 excel 表中的资产信息。



2.4.2.3 资产信息修改

选中一条具体的资产，可在操作出修改设备描述信息，关联资产，修改账户口令，修改协议端口，删除设备。



2.4.2.4 资产信息导出

选中一条或多条具体的资产，点击右上角  导出资产属性信息，可导出设备的资产信息。

2.4.2.5 资产删除

选中一条或多条资产，点击右上角  删除功能，即可删除选中的资产

2.4.2.6 创建外部链接

点击右上角  按钮编辑外部链接，可新建外部链接，直接在浏览器中打开指定的 URL 页面。

外部链接功能主要是帮助用户可以快速跳转到相关设备 web 管理页面，直接登录管理。

2.4.3 待关联资产

待关联资产显示是业务中所有未关联资产台账的资产，帮助用户了解目前系统中存在哪些设备未和已添加的资产台账信息进行关联。

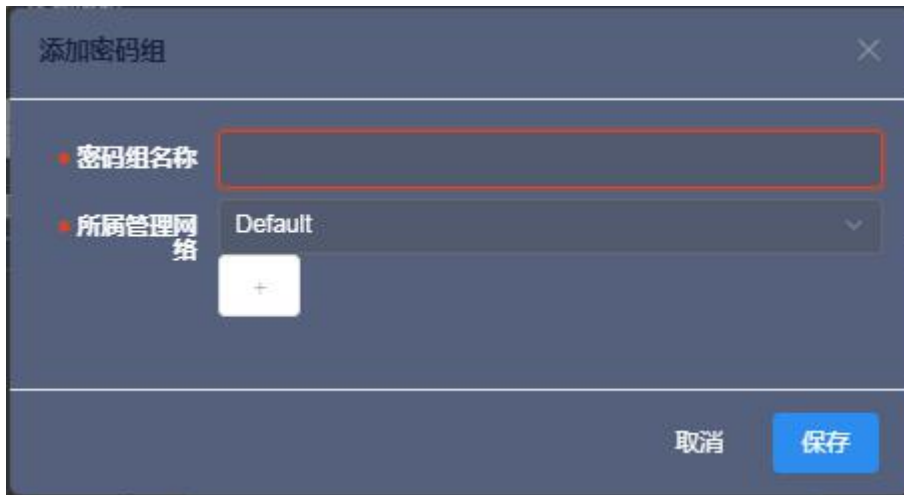
待关联资产页面相关功能与受控资产功能一致，详细可参考受控资产。

2.4.4 资产设置

2.4.4.1 缺省密码

平台通过 ssh，snmp，ftp 连接设备，需要知道设备的用户名密码等相关信息。用户如果为单个在设备处添加密码，则可以在此为设备添加帐号信息。

密码组定义一批拥有相同密码规则的设备。点击密码组右侧  按钮，填写密码组名称，保存后，在密码口令处填写相关的账户口令，此处依旧缺省可不填。设备地址处添加设备的 ip，CIDR，范围或者掩码，添加的设备必须是使用这个密码组的密码。点击保存即可生效。



The image shows a dialog box titled "添加密码组" (Add Password Group). It contains two main fields: "密码组名称" (Password Group Name) with an empty text input field, and "所属管理网络" (Belonging Management Network) with a dropdown menu showing "Default" and a "+" button below it. At the bottom right, there are two buttons: "取消" (Cancel) and "保存" (Save).

2.4.4.2 缺省协议

平台使用协议连接设备时部分设备为安全性考虑修改了协议的默认端口。管理者可以使用缺省协议，设置某些设备的协议端口。如某些设备的 ssh 端口改为 1527，不是默认的 22 端口，可以在这新建协议组后修改协议的端口，设备地址处填写修改的 ip,CIDR，范围或掩码，点击保存即可生效。



协议项	设备地址
协议	端口 1527

2.4.4.3 在线监测策略

主要是为了定期获取当前设备的 ping 状态。

获取资产连通状态

所有触发器以服务器时间为准, 基于GMT+08:00时区时间

开始时间

2020-03-10 13:06

☐ 一次
 ☐ 周期性的
 ☐ 每天
 ☐ 每周
 ☐ 每月
 ☒ Cron表达式

* 表达式 [秒 分 时 天 月 周 年 (由空格分割)]

0 */10 * * * *

* (通配符)任何值
 , 附加值
 - 范围
 ? 只可用在天或周中表示不指定特殊的值

结束时间

选择日期和时间

保存

内置了获取资产连通状态和定期清理历史数据，可以修改这两个任务的执行时间，也可以停止/恢复这两个任务。

所属计划			
计划名	状态	下次执行时间	操作
获取资产连通状态	执行中	2020-03-12 13:50:00	⌂
定期清理历史数据	执行中	2020-03-13 00:00:00	⌂

2.4.4.4 配置备份策略

平台中的备份指的是远程登录设备后从设备中查询到相关设备信息保存在平台的数据库中，如 Linux 设备可以备份 ip，mac，cpu，内存等信息。

点击右上角的  按钮，可以添加备份任务。弹出的页面填写任务名称，设置任务组，选中需要备份的设备后保存。

● 基本信息

任务名称

任务组

健康巡检

任务描述



保存后，设置任务的执行时间，在触发器设置中填写名称及设置执行时间，填写完毕后保存即可在左侧的触发器列表看到已设置好的触发器。点击关闭即可关闭弹出的页面。

回到配置备份策略处即可看到已经添加了的备份任务。

序号	计划名称	修改时间	状态	下次执行时间	剩余次数	描述	操作
1	ces	2020-03-04 14:30:16		-	-	-	修改 删除

选中任务后，可对任务进行修改时间，停止任务执行，恢复任务，执行任务，删除任务等相关操作，也可在操作出，点击修改，对任务的设备进行增加、删除。

2.4.4.5 资产发现策略

平台启动资产发现后，当网内新增资产时，资产发现策略可以帮助用户在建网内发现资产并添加到受控资产中。

可选择网络范围，自定义 ip 范围或者以受控资产为种子，设置计划任务事件，周期性的对设置的网络范围进行 ping 扫描和 snmp，共同发现网内是否有新增资产。

发现新资产

状态 无计划

下次执行时间 无

操作

网络范围 ☐ 自定义 ☒ 以受控资产为种子

开始时间

☐ 一次 ☒ 周期性的 ☐ 每天 ☐ 每周 ☐ 每月 ☐ Cron表达式

重复运行, 每 天

保存策略 0 42 14 *1 * ? * [TYPE=DAILY]

结束时间

保存

2.5 配置

左侧是业务列表信息，右侧是业务涵盖的设备资产信息

配置主要用来存放平台自动备份的配置，并可用于配置备份、查看配置、配置比对、配置导出等操作。

2.5.1 配置备份

配置备份模块可以查看当前设备下的历史备份信息，以及对未备份的设备进行备份。

选择一台或多台设备，点击右上角的  备份按钮，弹出的页面点击确定，会创建单次备份任务，在弹出的页面，点击 ，即可执行备份任务，修改触发器时间保存后可设置为计划任务，定期执行备份任务。



触发器设置

所有触发器以服务时间为准, 基于GMT+08:00时区时间

名称

开始时间 2020-03-12 15:01

☐ 一次 ☐ 周期性的 ☒ 每天 ☐ 每周 ☐ 每月 ☐ Cron表达式

重复运行, 每 天

保存值 0 1 15 * * ? * [TYPE=DAILY]

结束时间

保存

备份的数据均存在数据库中，window 和 linux 备份的数据可定制修改，网络设备主要备份了当前的运行配置和保存的配置。

选中设备后，点击右上角的 导出配置按钮，设置时间范围，配置文件选项，保存方式选项，点击确定后，在弹出的页面点击立即运行，即可导出选中的设备的备份配置信息，帮助运维人员使用。

● 时间范围选择：（配置文件的备份时间） ☒ 最后一次 ☐ 所有时间 ☐ 时间范围	● 配置文件选项 ☒ 所有配置 ☐ 启动配置 ☐ 运行配置	● 保存方式选项 ☒ 以备份日期为主目录 ☐ 以设备为主目录
--	--	--

点击  可以展开该设备备份详情，可以看到设备的历史备份信息，设置基线后，可点击“查看变更内容”，查看此次备份的详情。

序号	计划名	所属组	下次执行时间	操作
暂无数据				
☐	序号	配置备份时间	状态	查看变更内容
☐	1	2020-01-06 16:47:33	待审核	查看变更内容
☐	2	2019-12-27 15:56:32	首次备份 基线	查看变更内容

在弹出的页面查看到时间日期，设备 ip，备份文件名，以及与基线对比的差异详情，差异的具体内容。可在变更审核处提出审核意见及是否同意此次变更

点击  展开该设备的备份详情，可选择时间跨度不一样，且不是基线的两次备份信息进行配置比对，帮助运维人员进行差异发现。

配置比对

192.168.16.158 /tmp/monitor 2019-12-27 15:56:32 基线

192.168.16.158 /tmp/monitor 2019-12-27 15:56:32 基线

↑ ↓ ↺ 自动换行

无差异

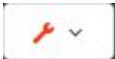
```
1 bash /tmp/monitor.sh
2 cpuInfo: {}
3 [5.9 us, 5.9 sy, 0.0 mi, 88.2 id,]
4 {}
5 cpuInfo: {}
6 5.9
7 {}
8 cpuSys: {}
9 us, 5.9
10 {}
11 cpuFree: {}
12 sy, 0.0 mi, 88.2
13 {}
14 memInfo: {}
15 [Mem : 1012440 total, 369148 free, 129216 used,]
16 [Swap: 2097148 total, 2097148 free, 0 used. 596300]
17 {}
18 memUsed: {}
19 awk: cmd. line:1: (FILENAME= FNR=1) fatal: division by zero attempted
20 {}
21 swapInfo: {}
22 [Swap: 2097148 total, 2097148 free, 0 used. 596300]
23 {}
24 swapUsed: {}
```

```
1 bash /tmp/monitor.sh
2 cpuInfo: {}
3 [5.9 us, 5.9 sy, 0.0 mi, 88.2 id,]
4 {}
5 cpuInfo: {}
6 5.9
7 {}
8 cpuSys: {}
9 us, 5.9
10 {}
11 cpuFree: {}
12 sy, 0.0 mi, 88.2
13 {}
14 memInfo: {}
15 [Mem : 1012440 total, 369148 free, 129216 used,]
16 [Swap: 2097148 total, 2097148 free, 0 used. 596300]
17 {}
18 memUsed: {}
19 awk: cmd. line:1: (FILENAME= FNR=1) fatal: division by zero attempted
20 {}
21 swapInfo: {}
22 [Swap: 2097148 total, 2097148 free, 0 used. 596300]
23 {}
24 swapUsed: {}
```

2.5.2 配置变更

变更功能模块可通过配置文件下发、图形化变更和命令行模式三种方式对设备直接下发信息，可直接查看到返回的结果。

在设备列表选择设备，点击右上角的  按钮，一些便捷的脚本工具，如安装监控探针均可在此看到。

在设备列表出选择设备，点击右上角的  配置变更按钮，选择相应执行方式，对选中的设备进行配置变更。



2.5.2.1 配置文件下发

选中设备，点击右上角【配置文件下发】，弹出的页面，输入目标配置和上传的配置文件之后点击【保存】按钮。下一步选择立即执行或制定计划执行。

2.5.2.2 图形化变更

选中设备，点击右上角【图形化变更】，弹出的页面选择工具脚本后，点击保存，在弹出的页面选择“立即执行”或者制定计划执行

2.5.2.3 命令行模式

选中设备，点击右上角【配置变更】按钮，选择【命令行模式】，弹出的页面输入下发的命令之后点击【保存】按钮。下一步选择立即执行或制定计划执行。

2.6 合规

2.6.1 合规评估

合规评估可针对被乐维自动化管理系统纳管的所有设备进行配置合规检查，点击列表中的设备之后，点击右上角的  合规检查按钮，在弹出的页面写上检查标准，描述，收件人信息后保存。下一步选择立即执行或制定计划执行。

合规检查

检查标准

选择合规标准

备注描述

添加备注描述

收件人

请输入收件人邮箱

使用逗号分隔多个电子邮件地址.

取消

保存

立即运行

任务组 合规检查

任务类型 Compliance Inspect

触发器设置

所有触发器以服务时间为准, 基于GMT+08:00时区时间

名称

运营商标准

开始时间

2020-03-12 17:05

一次

周期性的

每天

每周

每月

Cron表达式

重复运行, 每 1 天

保存值 0 5 17 *? * [TYPE=DAILY]

结束时间

保存

关闭

执行结束后，可以查看所有执行设备的合规结果。针对不合规设备可以提示告知不合规项，选中不合规项，点击右上角的查看详情 按钮，可查看具体的不合规原因，方便管理员进行检查。

详细结果

序号	策略名称	策略描述	期望结果	检查结果	操作
1	应用telnet登录	应用telnet登录	关闭		查看源配置
2	HTTPS服务	HTTPS服务	开启		查看源配置
3	是否开启Console登录	是否开启Console登录	开启		查看源配置
4	是否设置console登录命令	是否设置console登录命令	开启		查看源配置
5	空闲时间超过多长时间注销账户口令，不应超过十分钟	空闲时间超过多长时间注销账户口令，不应超过十分钟。	开启		查看源配置
6	认证超时时间，不应超过2分钟	认证超时时间，不应超过2分钟。	开启		查看源配置
7	是否限制telnet远程管理IP	是否限制telnet远程管理IP	开启		查看源配置
8	是否限制SSH远程管理IP	是否限制SSH远程管理IP	开启		查看源配置
9	SNMP是否开启	SNMP是否开启	开启		查看源配置
10	SNMP团体名加密	SNMP团体名加密	开启		查看源配置

2.6.2 合规策略

合规策略为不同设备不同型号执行不同巡检任务的策略集合，点击右上角 按钮，可以创建策略组，填写策略组名称、描述信息，标准分类，设备驱动，点击保存即创建策略组。

编辑策略组

策略组名称

策略组描述

标准分类

设备驱动

取消

保存

目前合规策略中的具体策略均为内置策略。

序号	标准分类名称		操作
1	等级保护		
序号	策略组名称	策略组描述	
1	华为防火墙	华为 USG5500	
2	天融信防火墙	天融信防火墙	
3	网神防火墙	网神防火墙	
4	网御防火墙	网御防火墙	

2.6.3 合规结果

合规结果模块以设备维度可以看到某个设备进行合规检查的历史检查记录。

点击设备列表中的  按钮即可看到该设备的历史检查记录，点击可查看具体的合规项。弹出的页面点击右侧的查看源配置，即可查合规成功/失败的具体信息。

2	>	172.16.1.1	R7200	3Com 3300	Cisco	7206VXR	模拟111
3	▼	172.16.1.2	R3725	Cisco IOS	Cisco	3725	模拟2
序号	类型	名称	任务组	开始时间	任务耗时	执行人员	状态
1	☑	Compliance_Check_1578...	合规检查	2020-01-06 14:49:51	18分3秒	admin	成功

2.6.4 合规报告

合规报告模块以任务维度记录合规检查的结果。默认按最近时间执行的合规检查任务顺序依次显示。

在“合规报告”页面可以对一定时间内执行的合规任务进行统计展示，统计图下方是对应时间段内的任务列表，合规检查列表上方可根据任务名称、任务组和执行人员进行筛选，例如选择时间单元为“一个月”，点击右边  按钮，即可将近一个月的执行过的任务在下方列表显示。选中一条任务，点击右上角查看，可查看该任务的执行结果。点击右上角查看任务定义，可以查看该任务对应的任务计划中的详细信息。点击右上角取消任务执行，可将执行中的任务中断执行。选中某一个任务之后，点击右上角 word，可以下载报告，报告类型有合规检查报告，合规检查不合规报告，合规检查完整报告，合规评估报告（汇总版），合规异常报告（汇总版），可勾选进行下载。

合规任务	任务名称	包含	值	自定义	开始时间	结束时间	搜索
序号	类型	名称	任务组	开始时间	任务耗时	执行人员	状态
1	☒	Compliance_Check_1584002158...	合规检查	2020-03-12 16:37:04	0秒	admin	
2	☒	Compliance_Check_1578291864...	合规检查	2020-03-12 08:00:00	11秒	admin	
3	☒	Compliance_Check_1578292147...	合规检查	2020-03-12 07:07:00	4分20秒	admin	
4	☒	Compliance_Check_1578292559...	合规检查	2020-03-12 06:07:00	31秒	admin	
5	☒	Compliance_Check_1578291864...	合规检查	2020-03-11 08:00:00	11秒	admin	
6	☒	Compliance_Check_1578292147...	合规检查	2020-03-11 07:07:00	4分20秒	admin	
7	☒	Compliance_Check_1578292559...	合规检查	2020-03-11 06:07:00	31秒	admin	
8	☒	Compliance_Check_1578291864...	合规检查	2020-03-10 08:00:00	12秒	admin	
9	☒	Compliance_Check_1578292147...	合规检查	2020-03-10 07:07:00	4分20秒	admin	
10	☒	Compliance_Check_1578292559...	合规检查	2020-03-10 06:07:00	36秒	admin	

2.7 巡检

2.7.1 巡检检查

巡检检查可针对被乐维自动化管理系统纳管的所有设备进行巡检检查，巡检只要是查看该设备是否符合设定的预期结果，从而判断当前巡检的内容是否健康不健康。

点击列表中的设备之后，点击右上角的  健康巡检按钮，在弹出框中输入检查标准和收件人，保存后在弹出的界面中选择立即执行或者任务执行。

健康巡检

检查标准

常规巡检

备注描述

添加备注描述

收件人

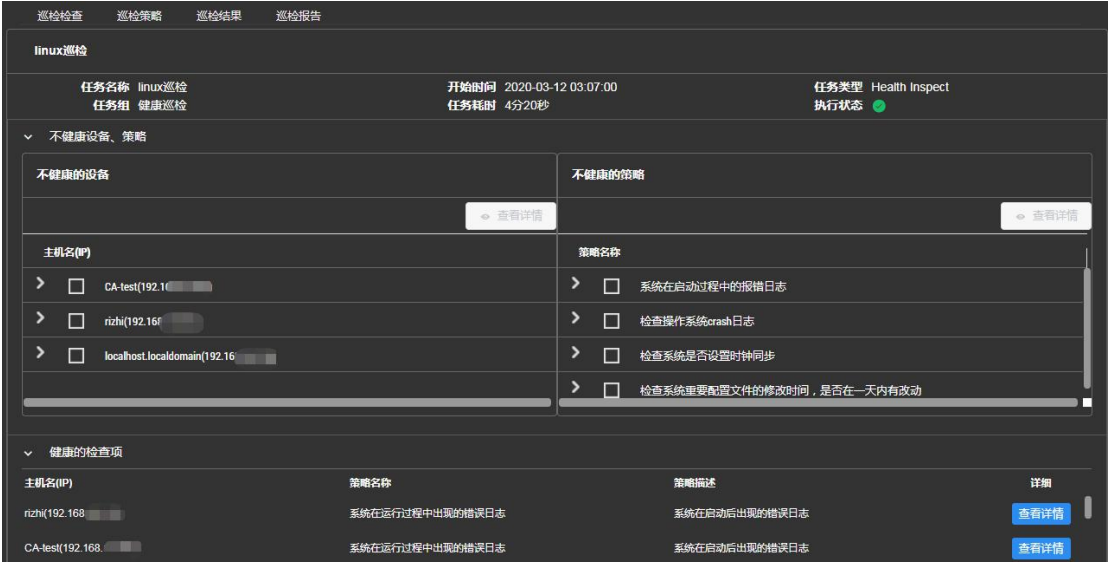
请输入收件人邮箱

使用逗号分隔多个电子邮件地址。

取消

保存

执行结束之后，可以查看所有执行设备的巡检结果。针对不健康的设备可以提示告知不健康项，选中不健康项，点击右上角的查看详情按钮可显示不健康项的结果原因，方便管理员进行检查。



2.7.2 巡检策略

巡检策略为不同设备不同型号执行不同巡检任务的策略集合，所有的巡检策略中的脚本命令均可以在被巡检的设备中执行。

页面以列表形式显示当前所有的巡检策略。

常规巡检			
序号	策略组名称	策略组描述	操作
1	天融信防火墙巡检	天融信防火墙巡检	  
2	启明防火墙巡检	启明防火墙巡检	  
3	网御防火墙巡检	网御防火墙巡检项	  
4	RedHat Linux主机巡检	RedHat Linux主机巡检	  
5	AIX_UNIX 主机巡检	AIX_UNIX 主机巡检	  
6	HP_UNIX 主机巡检	HP_UNIX 主机巡检	  
7	配置检查	华为交换机的巡检项	  
8	1	1	  
9	11	12	  

点击页面右上角的  按钮添加策略组，在跳转的页面填写策略组名称，策略组描述，标准分类，设备驱动，即可创建一个新的策略组。

其中具体含义为：

策略组名称：这个填写的主要是添加的一类策略的名称，比如都是关于 linux 的，即可写为 linux 巡检；

策略组描述：这个填写的主要是描述信息，可自己填写；

标准分类：标准分类主要在此创建，下拉有已经创建好的，点击+号，可以自定义标准分类名称；

设备驱动：主要选择，该策略组中的巡检脚本可以在那种设备上执行，如策略组为 linux 巡检，策略都是关于 linux 相关脚本，驱动选择 linux OS 即可；

选中一个策略组，点击右侧的编辑组信息，即可修改组的信息。点击查看组内策略，即可查看该策略中的所有策略。点击删除，即可以删除这个策略组；

查看策略组内容				添加策略
策略组名：linux健康巡检 设备厂商：红帽		检查标准：主机巡检 设置类型：Redhat Linux		
策略名称	策略描述	最后修改时间	操作	
系统在运行过程中出现的错误日志	系统在启动后出现的错误日志	2019-07-16 15:59:05	编辑	删除 启用
系统启动过程中报错日志	系统在启动过程中的报错日志	2019-04-19 13:59:05	编辑	删除 启用
安全异常访问登录日志	用户登录、网络连接等安全相关的报错日志	2019-07-16 16:03:06	编辑	删除 启用
用户登录失败的尝试日志	检查是否存在登录失败的用户分析原因	2019-04-19 14:00:07	编辑	删除 启用
计划任务报错日志	检查计划任务中出现的失败日志	2019-07-16 16:08:16	编辑	删除 启用
邮件报错日志	检查发送的邮件中是否有错误、失败的日志	2019-07-16 16:11:13	编辑	删除 启用
重启间隔	查系统重启、关机信息与实际操作是否相符	2019-07-16 15:21:44	编辑	删除 启用
重要配置文件	检查系统重要配置文件的修改时间，是否在一天内有改动	2019-04-22 15:39:35	编辑	删除 启用
僵尸进程	检查系统是否存在僵尸进程	2019-07-16 15:28:48	编辑	删除 启用
crash日志	检查操作系统crash日志	2019-04-19 14:02:35	编辑	删除 启用
时钟同步	检查系统是否设置时钟同步	2019-09-30 17:33:35	编辑	删除 启用

双击或者点击右侧的查看组内策略，均可以进入添加巡检策略页面。点击右上角的添加策略，填写策略名称，描述自定义，诊断脚本主要写该巡检策略的监测脚本。Linux 的诊断脚本均为 shell 脚本，命令可在 linux 设备执行，即可放入诊断脚本中；

Windows 的诊断脚本为 powershell 脚本，命令可以 windows 的 powershell 执行即可。交换机的诊断脚本只要为具体的命令，可在设备上执行即可。shell 的巡检脚本示例如下：

```
V_RHEL_HEA_NTPSERV1="ntp";

Server_IP1="192.168.54.4";Server_IP2="192.168.54.5";Server_IP3="192.168.54.6";

NTPSET1=`/usr/sbin/ntpq -p 2>/dev/null`; NTPSET2=`ls /usr/sbin/ntpdate
2>/dev/null`; NTPSERV=` crontab -l |grep $V_RHEL_HEA_NTPSERV1 | grep -E
"$Server_IP1|$Server_IP2|$Server_IP3"`; Resultcmd=`echo "$NTPSERV" |awk '{print
$6,$7}`;if [[ "$NTPSET1" != "" ]] || [[ "$NTPSET2" != "" ]]; then if [[ "$NTPSERV" != "" ]];
then echo -e "Check ntp is @@OK@@,\n ${NTPSERV} \nrunning the command
";echo $Resultcmd;echo "result is " ; $Resultcmd; else echo -e "Check ntp is
@@False@@"; fi; else echo "Check ntp is @@False@@, Not configured NTP
service."; fi; echo

"*****
*****";
```

一句话形式的脚本，也可以分段，不过在 Linux 上，写成一句话形式的方便执行该脚本必须在 Linux 设备上，可执行，可以看见具体的执行结果。

填写完毕后，点击下一步，在页面中填写匹配数据块开始与结束为止，设置规则条件，用来判断执行结果是否为健康不健康。其中，在数据块处设置输出结果匹配那一块内容，规则条件是对 shell 脚本结果值的匹配，@@value@@为固定格式不可修改，其次，最后的 echo ” *****” 是数据块

结束段落的匹配，改好之后保存即可。包含关系代表规则条件被匹配到是健康的，不包含关系代表规则条件被匹配到时不健康的，均可勾选正则。

点击下一步，根据巡检内容是否设置统计规则，点击开启统计，选中设置好的统计方式，即可在统计报表中生成统计图。

点击下一步告警规则，可以在告警信息处，告警规则组填写组名，告警规则名选择具体的告警规则，即可与告警处的告警规则进行关联。点击保存。就可以完成巡检规则的创建。

点击巡检策略右侧的编辑，即可对已完成的巡检规则进行修改，包括巡检脚本。点击删除即可删除巡检策略，点击启用按钮，即可选择该巡检组巡检时是否启用该条巡检策略。

提示：基于 linux 的数据库，为了方便命令连接数据库，执行命令时会先创建临时变量，如果执行目前现有的数据库巡检策略，需先在设备上执行生成临时变量。新增数据库巡检策略，只要 linux 上可执行，均可放入诊断脚本中，下面为数据库的临时变量。

PGSQL 临时变量：

export PGHOST=127.0.0.1

export PGPORT=端口

export PGDATABASE=数据库名称

export PGUSER=postgres 数据库用户名

export PGDATA=`ps -ef|grep postgres|grep -v grep|grep '\-D'|awk

'{print \\${NF}}'|grep "/"`

export PGHOME= "/opt/bjca3" 数据库目录

export PATH=\$PGHOME/pgsql/bin:\$PGHOME/bin:\$PATH:.

```
export
```

```
LD_LIBRARY_PATH=$PGHOMELib:/lib64:/usr/lib64:/usr/local/lib64:/lib:/
```

```
usr/lib:/usr/local/lib:$LD_LIBRARY_PATH
```

MongoDB 临时变量:

```
export username=$username;
```

```
export password=$password;
```

```
export port=$port;
```

```
export dbname=$dbname;
```

```
export mongopath=`find / -name mongo 2>/dev/null|head -1`;
```

2.7.3 巡检结果

巡检结果以设备维度记录列表中的设备历史执行巡检任务的结果。

在设备列表页面，点击, 即可看到该设备的历史检查记录，可看到任务名称，执行时间，任务耗时及执行的状态。

11	▼	192.168.16.156	rizhi	Linux OS	VMware, Inc.	VMware Virtual Platform	日志服务器
序号	类型	名称	任务组	开始时间	任务耗时	执行人员	状态
1	①	linux巡检	健康巡检	2020-03-12 03:07:00	4分20秒	admin	
2	①	linux巡检	健康巡检	2020-03-11 03:07:00	4分21秒	admin	
3	①	linux巡检	健康巡检	2020-03-10 03:07:00	4分20秒	admin	
4	①	linux巡检	健康巡检	2020-03-09 03:07:00	4分20秒	admin	
5	①	linux巡检	健康巡检	2020-03-08 03:07:00	4分20秒	admin	

点击任务组名称，即可进入任务结果的页面，查看健康不健康巡检项，点击查看详情，即可看到结果的详情。

详细结果

序号	策略名称	策略描述	期望结果	检查结果	操作
1	系统在运行过程中出现的错误日志	系统在启动后出现的错误日志	否		查看源配置
2	系统启动过程中报错日志	系统在启动过程中的报错日志	否		查看源配置
3	安全异常访问登录日志	用户登录、网络连接等安全相关的报错日志	否		查看源配置
4	用户登录失败的尝试日志	检查是否存在登录失败的用户分析原因	否		查看源配置
5	计划任务报错日志	检查计划任务中出现的失败日志	否		查看源配置
6	邮件报错日志	检查发送的邮件中是否有错误、失败的日志	否		查看源配置
7	重启间隔	查系统重启、关机信息与实际操作是否相符	间隔在30分钟之内为正常		查看源配置
8	重要配置文件	检查系统重要配置文件的修改时间，是否在一天内有改动	没有重要配置文件在一天内有改动		查看源配置
9	僵尸进程	检查系统是否存在僵尸进程	是		查看源配置
10	crash日志	检查操作系统crash日志	否		查看源配置

2.7.4 巡检报告

巡检报告页面以任务维度记录巡检任务的执行结果，其默认顺序按最近执行时间的任务依次排列。

巡检检查 巡检策略 巡检结果 巡检报告

巡检任务

任务名称

包含

值:

自定义

开始时间: 选择日期和时间

结束时间: 选择日期和时间

搜索

序号	类型	名称	任务组	开始时间	任务耗时	执行人员	状态
1	①	linux巡检	健康巡检	2020-03-12 03:07:00	4分20秒	admin	
2	①	windows巡检	健康巡检	2020-03-12 02:07:00	1分16秒	admin	
3	①	linux巡检	健康巡检	2020-03-11 03:07:00	4分21秒	admin	
4	①	windows巡检	健康巡检	2020-03-11 02:07:00	1分12秒	admin	
5	①	linux巡检	健康巡检	2020-03-10 03:07:00	4分20秒	admin	
6	①	windows巡检	健康巡检	2020-03-10 02:07:00	1分17秒	admin	
7	①	linux巡检	健康巡检	2020-03-09 03:07:00	4分20秒	admin	
8	①	windows巡检	健康巡检	2020-03-09 02:07:00	1分11秒	admin	
9	①	linux巡检	健康巡检	2020-03-08 03:07:00	4分20秒	admin	
10	①	windows巡检	健康巡检	2020-03-08 02:07:00	51秒	admin	

在“巡检报告”页面可以对一定时间内执行的巡检任务进行统计展示，统计图下方是对应时间段内的任务列表，巡检列表上方可根据任务名称、任务组和执行人员进行筛选，例如选择时间单元为“一个月”，点击右边

搜索

按钮，即可将近一个月的执行过的任务在下方列表显示。选中一条任务，点击右上角“查看”，可查看该任务的执行结果。点击右上角查看任务定义，可以查看该

任务对应的任务计划中的详细信息。点击右上角取消任务执行，可将执行中的任务中断执行。选中某一任务之后，点击右侧的 word 生成报告按钮，可将该任务的执行结果以报告形式显示出来，可选择下载的报告为常规巡检报告，完整巡检报告，巡检报告（汇总版），巡检项统计报告，巡检异常报告（汇总版），异常巡检报告。

2.8 监控

2.8.1 主机监控

主机监控主要指 Linux/Unix 监控和 Windows 监控。平台需要在被监控的设备上安装监控探针，服务器才会收集监控信息。Linux 监控收集的数据有系统运行时间、CPU、CPU 使用率、内存、内存使用率、根分区使用率、系统负载情况等。Windows 监控收集的数据有系统运行时间、CPU、CPU 使用率、内存、内存使用率等。



选择设备列表中的设备，点击右上角的 **增加探针** 按钮，在弹出的页面的填写参数配置信息，点击测试&保存，可添加监控探针。点击删除探针，即可删除添加了的探针。

点击 **仪表盘配置** 可设置仪表盘。

序号	名称	路径	监控项	描述	匹配设备
1	汇总	/grafana/d/zCMR45VZz/hui-zong	汇总	-	-
2	汇总Test	/grafana/d/3uNGchQZk1/hui-zong-test	汇总	-	-
3	Linux/Unix监控	/grafana/d/gdTEOl_zk/linux-unixjian-kong	1	使用 Node Exporter v0.16 0.17，精简优化重要指标展示。包含：...	☒
4	Windows监控	/grafana/d/woRrCAriz/windowsjian-kong	1	Windows系统监控仪表盘	☒
5	SNMP	/grafana/d/fYi-Qjiv/snmp	2	-	☒

选中设备后，已创建监控仪表盘的设备的右侧，可以看到监控仪表盘，添加对比，修改探针。

仪表盘修改

监控项

请选择

仪表盘

汇总

仪表盘路径

/grafana/d/zCMR45VZz/hui-zong

仪表盘参数

描述

取消

保存

2.8.2 硬件监控

硬件监控指 ipmi 监控，不必要在设备上安装探针，需要设备开启 ipmi。平台可以通过 ipmi 获取到设备的硬件数据，比如硬件温度，风扇速度，传感器状态等。

选择设备列表中的设备，点击右上角的 **增加探针** 按钮，在弹出的页面的填写参数配置信息，点击测试&保存，可添加监控探针。点击删除探针，即可删除添加了的探针。



点击 **仪表盘配置** 按钮可设置仪表盘。

选中设备后，已创建监控仪表盘的设备的右侧，可以看到监控仪表盘，添加对比，修改探针。

2.8.3 网络监控

网络监控主要显示网络设备和安全设备，设备需开启 snmp 团体密码。平台通过 snmp 获取到网络设备数据有系统运行时间，流入流出速率，接口状态等。

选择设备列表中的设备，点击右上角的 **增加探针** 按钮，在弹出的页面的填写参数配置信息，点击测试&保存，可添加监控探针。点击删除探针，即可删除添加了的探针。

点击  按钮可设置仪表盘。

选中设备后，已创建监控仪表盘的设备的右侧，可以看到监控仪表盘，添加对比，修改探针。

2.8.4 应用监控

应用监控主要是 black box 监控信息，获取应用信息数据。

选择设备列表中的设备，点击右上角的  按钮，在弹出的页面的填写参数配置信息，点击测试&保存，可添加监控探针。点击删除探针，即可删除添加了的探针。

点击  按钮可设置仪表盘。

选中设备后，已创建监控仪表盘的设备的右侧，可以看到监控仪表盘，添加对比，修改探针。

2.8.5 综合监控



2.8.6 服务器状态

服务器状态列出的当前监控启动的状态，绿色正常，红色为未启动成功。

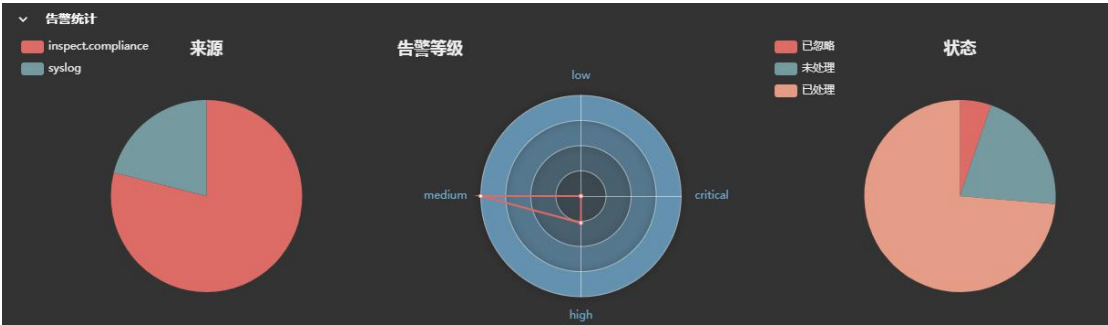
点击右侧的配置，可修改监控的端口等配置。监控服务器的重启。可以重启服务。



2.9 告警

2.9.1 告警信息

告警信息显示的是巡检、合规、监控出现在告警规则中配置的条件不符合预期的告警信息。



告警统计以图表的形式直观显示告警内容，图表为来源，告警等级，状态。

序号	告警名称	告警所属组	来源	资产IP	资产所属组	开始时间	最近发生时间	结束时间	严重等级	操作
1	authpriv	authpriv	syslog	192.168.16.158	Default	2020-03-10 17:35:06	2020-03-10 17:35:06	-	★★★★★	忽略 处理 详情
2	local7	local7	syslog	192.168.16.170	Default	2020-03-09 10:10:11	2020-03-09 13:55:14	-	★★★★★	忽略 处理 详情
3	cron	cron	syslog	192.168.16.158	Default	2020-02-03 03:10:18	2020-03-12 14:51:08	-	★★★★★	忽略 处理 详情
4	syslog	syslog	syslog	192.168.16.158	Default	2020-02-02 19:20:10	2020-03-12 06:14:54	-	★★★★★	忽略 处理 详情
5	密码复杂度	Linux安全检查	inspect.compliance	192.168.16.180	Default	2020-01-14 07:10:05	2020-01-14 07:10:05	2020-01-14 07:10:14	★★★★★	忽略 处理 详情
6	密码复杂度	Linux安全检查	inspect.compliance	192.168.16.156	Default	2020-01-14 07:09:56	2020-01-14 07:09:56	2020-01-14 07:10:09	★★★★★	忽略 处理 详情
7	密码复杂度	Linux安全检查	inspect.compliance	192.168.16.158	Default	2020-01-13 13:40:27	2020-01-13 13:40:27	2020-01-13 13:40:41	★★★★★	忽略 处理 详情
8	检查密码有效期显...	Linux安全检查	inspect.compliance	192.168.16.158	Default	2020-01-11 07:10:36	2020-01-11 07:10:36	2020-02-12 20:32:31	★★★★★	忽略 处理 详情
9	检查密码有效期显...	Linux安全检查	inspect.compliance	192.168.16.180	Default	2020-01-11 07:10:36	2020-01-11 07:10:36	2020-01-11 07:11:03	★★★★★	忽略 处理 详情
10	查看密码长度	Linux安全检查	inspect.compliance	192.168.16.158	Default	2020-01-08 18:35:07	2020-01-08 18:35:07	2020-01-08 18:35:12	★★★★★	忽略 处理 详情

以列表形式显示告警信息，包括告警的时间内容，资产 ip，来源等相关信息，点击右侧忽略，可忽略该条告警。点击处理，可选择脚本，执行治愈任务。点击详情，可以看到具体的告警信息。

2.9.2 告警规则

告警规则是为了配置对合规、巡检、监控的项目与预期不符合的项目的告警。

1 巡检

巡检主要添加巡检的告警的规则。

序号	规则名称	规则组	所属分类	条件表达式	是否自愈	严重等级
1	数据库缓冲命中串	Oracle巡检项	巡检	value<=90	否	★★★★★
2	查询闲置连接数	pgsql巡检项	巡检	value>0	否	★★★★★
3	当前等待队列长度	Mongo巡检项	巡检	value>0	否	★★★★★
4	内存排序比例	Oracle巡检项	巡检	value<=90	否	★★★★★
5	检查排序区	Oracle巡检项	巡检	value>=5	否	★★★★★
6	剩余可用连接数	Mongo巡检项	巡检	value<=1000	否	★★★★★
7	重做日志缓冲区分配额	Oracle巡检项	巡检	value>=1	否	★★★★★
8	日志缓冲区	Oracle巡检项	巡检	value>=1	否	★★★★★
9	内存数据缓冲命中串	Oracle巡检项	巡检	value<=90	否	★★★★★

点击页面右上角，新建告警规则按钮，可以新建告警。在弹出的页面上填写规则名，规则组，设置严重等级，设置是否允许自愈，选择治愈脚本，填写的条件表达式，填写概要模板，详情模板。

+ 添加告警规则

规则名

规则组

Oracle巡检项

所属分类

巡检

严重等级

Medium

允许自愈

条件表达式

如 : value >= 90 up ==0 'foo'.test(value)

概要模板

详情模板

取消

保存

条件表达式在巡检脚本中以@%%value%%@包围了 value 值，在此写入判断规则，如 value<90

选中已添加的规则，点击右上角的修改告警规则，可以对已创建好的告警规则进行修改。点击删除，即可删除该条告警规则。

I 监控

监控主要是 ipmi 的告警规则。

序号	规则名称	规则组	所属分类	条件表达式	持续时间	是否自愈	严重等级
1	掉线	alerts	监控	up == 0	1m	否	★★★★

I 日志

日志统计报表

I 合规

合规主要是关于合规检查不合规项的告警

序号	规则名称	规则组	所属分类	条件表达式	是否自愈	严重等级
1	检查密码有效期是否为90天	Linux安全检查	合规	value != 90	是	★★★★
2	查看密码长度	Linux安全检查	合规	value < 8	是	★★★★
3	本地和ssh远程登录失败...	Linux安全检查	合规	value != 0	否	★★★★
4	密码复杂度	Linux安全检查	合规	value == 0	是	★★★★

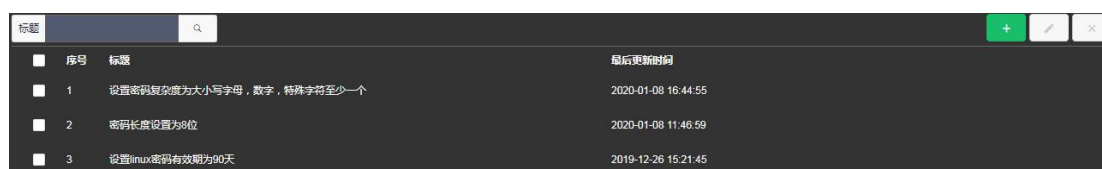
点击页面右上角，新建告警规则，可以新建告警。在弹出的页面上填写规则名，规则组，设置严重等级，设置是否允许自愈，选择治愈脚本，填写的条件表达式，填写概要模板，详情模板

条件表达式在巡检脚本中以@%%value%%@包围了 value 值，在此写入判断规则，如 value<90

选中已添加的规则，点击右上角的修改告警规则，可以对已创建好的告警规则进行修改。点击删除，即可删除该条告警规则。

2.9.3 治愈规则

治愈规则主要是治愈脚本，可在设备上执行治愈脚本，成功执行后可以添加到治愈规则中。



标题	标题	最后更新时间
1	设置密码复杂度为大小写字母，数字，特殊字符至少一个	2020-01-08 16:44:55
2	密码长度设置为8位	2020-01-08 11:46:59
3	设置linux密码有效期为90天	2019-12-26 15:21:45

点击添加，创建规则名称，脚本内容处可以填写治愈的脚本或命令，点击保存后即创建成功。



编辑治愈规则

规则名称: 设置密码复杂度为大小写字母，数字，特殊字符至少一个

脚本内容: `sed -i 's/password.*require.*password.*require.*pam_pwquality.so try_first_pass local_users_only retry=3 authok_type= minlen=8 ucredit=-1 lcredit=-1 dcredit=-1 /etc/pam.d/system-auth, echo -e "Password complexity has been set at least one upper and lower case letter, number, special character" ;`

取消 保存

2.9.4 治愈记录

主要记录已执行治愈规则的告警信息。包括已执行操作，执行时间，执行人，资产 IP，资产所属组，详情。点击详情下的告警详情可以查看到该条治愈是来自那条告警规则。点击治愈详情，可以看懂治愈结果。

序号	已执行操作	执行时间	执行人	资产IP	资产所属组	详情
1	执行治愈规则:设置linux密码有效期...	2020-01-07 10:12:03	admin	192.168.16.156	Default	告警详情 治愈详情
2	执行治愈规则:设置linux密码有效期...	2020-01-08 11:42:17	system	192.168.16.180	Default	告警详情 治愈详情
3	执行治愈规则:设置linux密码有效期...	2020-01-11 07:11:04	system	192.168.16.156	Default	告警详情 治愈详情
4	执行治愈规则:密码长度设置为8位	2020-01-07 17:15:29	admin	192.168.16.158	Default	告警详情 治愈详情
5	执行治愈规则:密码长度设置为8位	2020-01-08 11:51:34	system	192.168.16.158	Default	告警详情 治愈详情
6	执行治愈规则:密码长度设置为8位	2020-01-08 11:42:28	system	192.168.16.180	Default	告警详情 治愈详情
7	执行治愈规则:密码长度设置为8位	2020-01-09 07:10:52	system	192.168.16.156	Default	告警详情 治愈详情
8	执行治愈规则:密码长度设置为8位	2020-01-08 13:48:32	system	192.168.16.158	Default	告警详情 治愈详情
9	执行治愈规则:密码长度设置为8位	2020-01-08 17:02:17	system	192.168.16.158	Default	告警详情 治愈详情
10	执行治愈规则:密码长度设置为8位	2020-01-08 18:35:12	system	192.168.16.158	Default	告警详情 治愈详情

2.10 任务

每次备份、合规、巡检时都会生成任务，而这些任务均可以在任务模块中查询到。

2.10.1 单次任务

单次任务是每次创建任务之后就会创建单次任务。

单次任务 周期任务 任务结果 🔍 🏠 ⏸ 🔄 ▶ ✖									
序号	任务类型	任务名称	任务组	修改时间	状态	下次执行时间	剩余次数	描述	操作
1	①	Health_Check_15840...	健康巡检	2020-03-12 17:23:14	📅	-	-	xad	修改 历史查询
2	☑	Compliance_Check_...	合规检查	2020-03-12 16:35:50	📅	-	-	-	修改 历史查询
3	☑	Compliance_Check_...	合规检查	2020-03-12 16:34:33	📅	-	-	xad	修改 历史查询
4	☑	Compliance_Check_...	合规检查	2020-03-09 17:19:34	📅	-	-	-	修改 历史查询
5	①	业务统计页面测试2	健康巡检	2020-03-05 11:21:22	📅	-	-	主机巡检——linux	修改 历史查询
6	①	业务子页面测试	健康巡检	2020-03-05 11:18:46	📅	-	-	常规巡检——linux	修改 历史查询
7	🔍	ces	健康巡检	2020-03-04 14:30:16	📅	-	-	-	修改 历史查询
8	🔍	测试备份	备份	2020-03-04 09:24:51	📅	-	-	-	修改 历史查询
9	🔍	测试配置回滚	健康巡检	2020-03-03 10:22:21	📅	-	-	-	修改 历史查询
10	●	测试	工具	2020-03-01 21:19:41	📅	-	-	测试	修改 历史查询

点击右上角的工具，可以创建备份、合规、巡检等任务。



选中任务，点击任务计划与执行，可设置任务触发器执行时间，改为周期任务，或者直接点击立即执行。



选中任务，点击右上角的暂停任务，可停止任务的执行，点击右上角的恢复任务，可以使停止的任务重新执行，点击执行任务，可以使任务直接执行。点击删除，可以删除该条任务。

2.10.2 周期任务

周期任务是所有的定期执行的任务。

单次任务 周期任务 任务结果									
序号	任务类型	任务名称	任务组	修改时间	状态	下次执行时间	剩余次数	描述	操作
1	测试任务	测试任务	健康巡检	2020-03-04 09:21:51	📅	2020-03-16 09:47:00	-	测试	修改 历史查询
2	①	linux巡检	健康巡检	2020-03-01 21:24:48	📅	2020-03-13 03:07:00	-	-	修改 历史查询
3	①	windows巡检	健康巡检	2020-01-07 11:00:33	📅	2020-03-13 02:07:00	-	-	修改 历史查询
4	☑	Compliance_Check_...	合规检查	2020-01-06 14:49:40	📅	2020-03-13 08:00:00	-	cisco 路由器	修改 历史查询
5	☑	Compliance_Check_...	合规检查	2020-01-06 14:48:51	📅	2020-03-13 07:07:00	-	linux	修改 历史查询
6	☑	Compliance_Check_...	合规检查	2020-01-06 14:35:59	📅	2020-03-13 06:07:00	-	windows	修改 历史查询

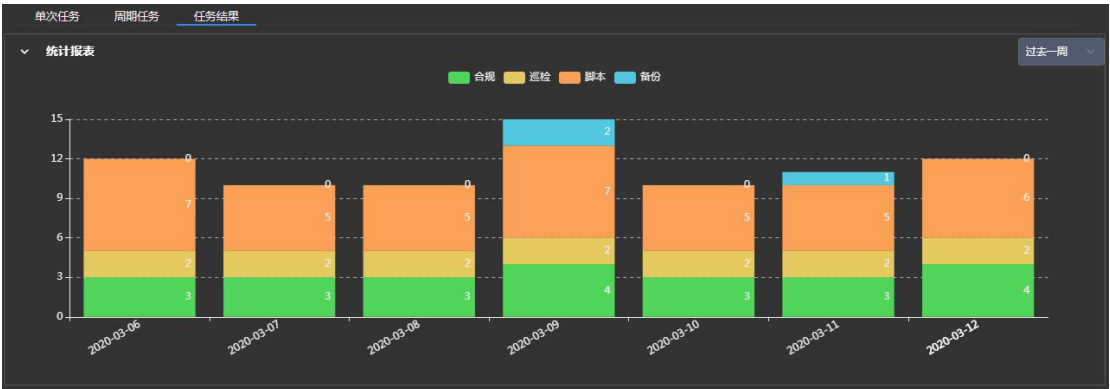
点击右上角的工具，可以创建备份、合规、巡检等任务。

选中任务，点击任务计划与执行，可设置任务触发器执行时间，改为周期任务，或者直接点击立即执行。

选中任务，点击右上角的暂停任务，可停止任务的执行，点击右上角的恢复任务，可以使停止的任务重新执行，点击执行任务，可以使任务直接执行。点击删除，可以删除该条任务。

2.10.3 任务结果

任务结果可以看到所有的任务的执行结果。



柱状图显示直观显示近期任务变换情况。

全部	任务名称	包含	值	自定义	开始时间	选择日期和时间	结束时间	选择日期和时间	搜索
序号	类型	名称	任务组	开始时间	任务耗时	执行人员	状态		
1	合规检查	Compliance_Check_1584002158...	合规检查	2020-03-12 16:37:04	0秒	admin	成功		
2	查看系统信息 (Run now ID2318)	_interactive		2020-03-12 14:43:13	10秒	admin	失败		
3	合规检查	Compliance_Check_1578291864...	合规检查	2020-03-12 08:00:00	11秒	admin	成功		
4	Compliance_ScriptTool_172.16.8...	_interactive		2020-03-12 08:00:02	6秒	admin	失败		
5	Compliance_ScriptTool_172.16.8...	_interactive		2020-03-12 08:00:01	7秒	admin	失败		
6	合规检查	Compliance_Check_1578292147...	合规检查	2020-03-12 07:07:00	4分20秒	admin	成功		
7	Compliance_ScriptTool_192.168...	_interactive		2020-03-12 07:07:00	4分18秒	admin	失败		
8	合规检查	Compliance_Check_1578292559...	合规检查	2020-03-12 06:07:00	31秒	admin	成功		
9	linux巡检	健康巡检		2020-03-12 03:07:00	4分20秒	admin	成功		
10	Inspect_ScriptTool_192.168.16.1...	_interactive		2020-03-12 03:07:00	4分20秒	admin	失败		

在“任务报表”页面可以对一定时间内执行的各种任务进行统计展示，统计图下方是对应时间段内的任务列表，任务列表上方可根据任务名称、任务组和执行人员进行筛选，例如选择时间单元为“一个月”，点击右边【搜索】按钮，即可将近一个月的执行过的任务在下方列表显示。选中一条任务，点击右

上角可查看该任务的执行结果。点击右上角查看任务定义，可以查看该任务对应的任务计划中的详细信息。点击右上角取消任务执行，可将执行中的任务中断执行。

2.11 知识

知识模块设置了可用于参考的相关知识，也可自行创建经验分享文档供使用人员参考。

2.11.1 设备配置

设备配置可以在配置变更-工具->command runner 中直接使用此命令知识库中的条目。



以列表形式显示当前的知识库内置的知识

网络设备中已内置 Cisco、H3C、Huawei 等相关知识命令。可以在当前的页面点击右上角添加知识库，弹出来的页面上，填写名称、标签、缠上、适配版本、排他版本、描述、以及命令，即可创建一条知识。

选中一条知识命令，即可在弹出的页面查看到相关的命令。

选中一条知识命令，点击右上角的编辑，即可对该条命令进行编辑。点击右上角的删除即可删除该条知识命令。

提示： 知识库一层一层结构可在名称上填写 A_B_C ，以下划线区分一级二级标题。

2.11.2 巡检策略

巡检策略显示当前内置的标准分类和策略组。点击可查看具体的巡检脚本命令。添加删除方式可参考巡检-巡检策略。

序号	标准分类名称		
1	▼ 常规巡检		
序号	策略组名称	策略组描述	操作
1	天融信防火墙巡检	天融信防火墙巡检	  
2	启明防火墙巡检	启明防火墙巡检	  
3	网御防火墙巡检	网御防火墙巡检项	  
4	RedHat Linux主机巡检	RedHat Linux主机巡检	  
5	AIX_UNIX 主机巡检	AIX_UNIX 主机巡检	  
6	HP_UNIX 主机巡检	HP_UNIX 主机巡检	  
7	配置检查	华为交换机的巡检项	  

2.11.3 合规策略

合规策略中等级保护内置了当前等保的检查策略。可新建自定义合规标准，方便检查。

1	▼ 等级保护		
序号	策略组名称	策略组描述	操作
1	华为防火墙	华为 USG5500	  
2	天融信防火墙	天融信防火墙	  
3	网神防火墙	网神防火墙	  
4	网御防火墙	网御防火墙	  
5	山石防火墙	山石防火墙	  
6	华为路由器	华为路由器	  
7	思科路由器	思科路由器	  

2.11.4 协作论坛

点击右上角“创建”按钮，选择普通文档或 Markdown，填写相对应的内容，并可上传相应的附件文档，保存后可由其他人进行查阅，并可添加评论与作者进行讨论，优化经验文档。

2.12 系统

用户可以在系统模块设置关于系统使用，用户，角色权限，调试，邮箱等。也可以查看服务器的状态。

2.12.1 系统设置

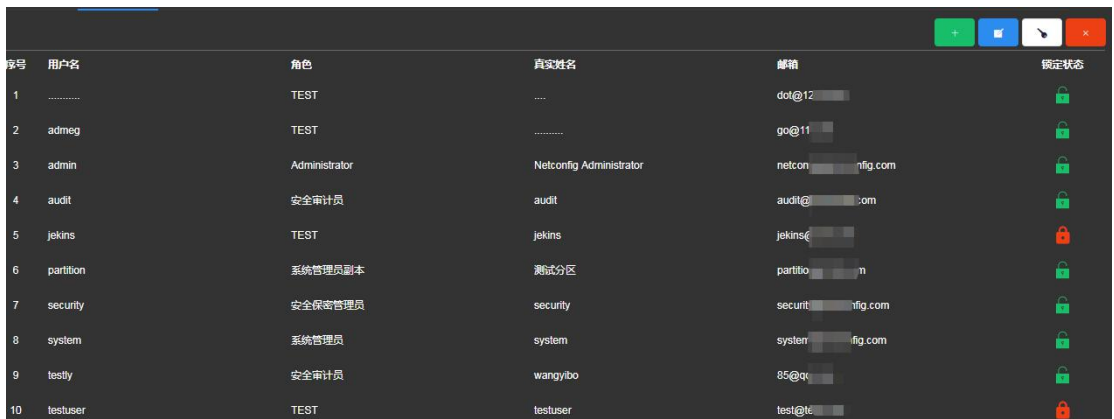
用于设置系统的密码更新周期、密码最小长度、登录最多尝试次数、页面超时时间。可在页面直接进行修改，修改完成后点击右上角的保存即可。



密码更新周期(天)	7
密码最小长度	8
登录最多尝试次数	3
页面超时时间(分)	10

2.12.2 用户管理

以列表形式显示当前创建的所有用户，包括角色，真实姓名等信息。



序号	用户名	角色	真实姓名	邮箱	锁定状态
1	-----	TEST	----	dol@12	
2	admeg	TEST	-----	go@11	
3	admin	Administrator	Netconfig Administrator	netcon	
4	audit	安全审计员	audit	audit@	
5	jenkins	TEST	jenkins	jenkins@	
6	partition	系统管理员副本	测试分区	partitio	
7	security	安全保密管理员	security	securit	
8	system	系统管理员	system	system	
9	testly	安全审计员	wangyibo	85@q	
10	testuser	TEST	testuser	test@te	

点击右上角新建用户，在弹出的页面填写相关信息，点击保存即创建的新的用户。

选中用户，点击右上角的编辑用户，可以对用户信息进行编辑。用户锁定或修改密码，可以点击右上角的解锁用户/修改密码，对用户解锁和重新修改用户的密码。点击右上角的删除用户，可以删除用户。

2.12.3 角色管理

以列表形式显示当前创建的角色。



序号	角色	描述	操作
1	系统管理员	-	  
2	安全保密管理员	-	  
3	安全审计员	-	  
4	系统管理员副本	系统管理员创建的副本角色	  
5	TEST	-	  
6	TEST副本	TEST创建的副本角色	  
7	TEST副本副本	TEST副本创建的副本角色	  
8	TEST副本副本副本	TEST副本副本创建的副本角色	  
9	TEST副本副本副本副本	TEST副本副本副本创建的副本角色	  

点击右上角的添加角色，可以创建新的角色。在弹出的页面勾选角色权限，业务，点击确定后即可创建一条新的角色、

选中角色后，点击操作的创建副本，在弹出的页面修改角色名称，描述信息，可以创建一条和母本权限一样的新的角色。点击编辑，可修改该角色的权限，业务范围。点击删除用户，可以删除该条用户。

2.12.4 日志设置

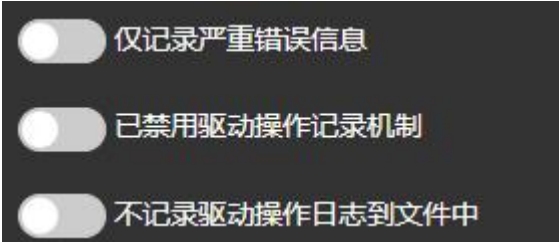
日志设置可以看到当前的存储空间总大小 MB，可用空间大小 MB，日志已用空间大小 MB，日志已用空间百分比%，日志存储空间大小 MB，日志存储空间将满告警，日志已满处理，处理方式有两种，备份并清理数据，直接清除数据。时间为 360 天之前或 180 天之前，可在页面上直接修改。



2.12.5 调试设置

调试可开启仅记录严重错误信息，已禁用驱动操作记录机制，不记录驱动操作日志到文件中。开启这些写配置项用于对驱动进行调试和诊断。由于可能会引起性能上的问题，建议只在调试和诊断时启动这些项。

管理员想查看备份/合规/巡检的过程时，可开启仅记录严重错误信息和不记录驱动操作日志到文件中，可以在后台 osgi-config\scratch\logs 看到具体的日志文件。



2.12.6 邮箱设置

邮箱设置可以设置系统邮箱，可作为电子邮件的发送地址，可以直接修改默认的邮箱信息，点击右上角的保存即可保存邮箱信息，点击测试，可像邮箱发送测试邮件

发信服务器设置(带“为必填项)		测试邮件	
服务器:	smtp.126.com	发件人:	netconfig@126.com
端口:	25	使用安全链接 (SSL):	☐
发件人:	Netconfig	收件人:	netconfig@126.com
账号:	netconfig@126.com	邮件内容:	测试邮件: 标题: 测试邮件 内容: 恭喜您, 如果您收到此邮件则代表运维平台后台邮件发信服务器设置正确!

2.12.7 通知规则

通知规则用于设定哪些事件发生后以什么样的方式进行告警。

查询：	规则名称	包含	值：	搜索					
序号	规则名称	规则描述	通知方式	业务	状态	创建者	最后修改者	创建时间	修改时间
1	Notification	System Notification	对话框	(共享)	启用	system	-	2020-03-10 13:07:00	2020-03-10 13:07:00
2	AlarmSendMailNotific...	Alarm mail notification	电子邮件	(共享)	启用	system	-	2020-03-10 13:07:00	2020-03-10 13:07:00

点击页面右上角的新增，可以新增通知规则。在弹出的页面中填写规则名称，规则描述，事件类型可下拉栏选择，通知方式可以设置为发送电子邮件告警，发送短信通知，页面弹出提示框等，状态是否启动，优先级，生效时间等填写完毕后保存即生成一条通知规则。

选中规则，点击右上角的编辑，可对规则信息进行编辑。点击右上角的删除，可删除创建的通知规则。

2.12.8 加载 license

使用该平台需要获得授权的 license。当前证书信息可以显示当前的 license 的信息包括版权信息，支持最大设备数，有效期。上传新的证书，可以更新目前过期/未过期的证书信息。

2.12.9 服务器状态

服务器状态统计

以折线图、柱状图显示当前服务器性能，包偶 cpu、内存、硬盘。

服务器参数信息

列表形式显示系统属性值和线程。

服务器日志

服务器启动后的运行日志，最下为最新日志。

2.13 审计

审计模块主要用于记录日志。

2.13.1 登录日志

审计用户登录、退出系统的情况，可根据用户名、ip、时间范围、搜到登录日志，也可以导出登录日志。

序号	状态	用户名	角色	IP地址	登录时间	退出时间	描述
1	🔒	admin	Administrator	192.168.16.144	2020-03-12 18:19:30	2020-03-12 18:29:46	Normal logout!
2	🔓	admin	Administrator	114.246.192.144	2020-03-12 16:56:45	-	Normal login!
3	🔒	admin	Administrator	114.246.192.144	2020-03-12 16:45:37	2020-03-12 16:55:58	Normal logout!
4	🔒	admin	Administrator	114.246.192.144	2020-03-12 16:20:22	2020-03-12 16:56:37	Normal logout!
5	🔒	admin	Administrator	114.246.192.144	2020-03-12 16:01:15	2020-03-12 16:12:06	Normal logout!
6	🔒	admin	Administrator	114.246.192.144	2020-03-12 14:11:46	2020-03-12 14:57:55	Normal logout!
7	🔒	admin	Administrator	114.246.192.144	2020-03-12 13:13:48	2020-03-12 14:11:32	Normal logout!
8	🔒	admin	Administrator	114.246.192.144	2020-03-12 11:44:44	2020-03-12 12:13:00	Normal logout!
9	🔒	admin	Administrator	114.246.192.144	2020-03-12 11:31:52	2020-03-12 11:44:29	Normal logout!
10	🔒	admin	Administrator	114.246.192.144	2020-03-12 10:44:19	2020-03-12 11:30:02	Normal logout!

2.13.2 设备操作日志

记录任务期间与设备交互时的日志，如备份任务，工具任务中的修改配置类。可根据任务名称、时间搜索。

序号	设备	任务名称	任务组	任务类型	开始时间	结束时间	执行人员	会话日志
1	10.63.0.1	查看系统信息 (Run now ID...)_interactive	Script Tool Job	Script Tool Job	2020-03-12 14:43:13	2020-03-12 14:43:23	admin	查看日志
2	192.168.16.144	查看系统信息 (Run now ID...)_interactive	Script Tool Job	Script Tool Job	2020-03-12 14:43:13	2020-03-12 14:43:17	admin	查看日志
3	172.16.8.25	Compliance_ScriptTool_17..._interactive	Script Tool Job	Script Tool Job	2020-03-12 08:00:02	2020-03-12 08:00:08	admin	查看日志
4	172.16.8.35	Compliance_ScriptTool_17..._interactive	Script Tool Job	Script Tool Job	2020-03-12 08:00:02	2020-03-12 08:00:07	admin	查看日志
5	192.168.16.13	Compliance_ScriptTool_19..._interactive	Script Tool Job	Script Tool Job	2020-03-12 07:07:00	2020-03-12 07:11:18	admin	查看日志
6	192.168.16.13	Inspect_ScriptTool_192.16..._interactive	Script Tool Job	Script Tool Job	2020-03-12 03:07:00	2020-03-12 03:11:20	admin	查看日志
7	192.168.16.144	Inspect_ScriptTool_192.16..._interactive	Script Tool Job	Script Tool Job	2020-03-12 03:07:00	2020-03-12 03:07:11	admin	查看日志