

# 明御<sup>®</sup>运维审计与风险控制系统

## 用户手册

(适用于 V2.0.8.1.7 及以上版本)



杭州安恒信息技术股份有限公司

二〇二〇年六月

# 目录

1 登录系统 .....	8
2 控制板 .....	11
2.1 用户和资产 .....	11
2.2 一周运维次数统计 .....	11
2.3 一周用户运维 .....	11
2.4 一周主机运维 .....	12
2.5 实时监控 .....	12
2.6 今日新增会话 .....	12
2.7 最近运维记录 .....	13
2.8 系统运行状态 .....	13
2.9 许可证信息 .....	13
3 部门 .....	14
3.1 部门管理 .....	14
3.1.1 新建部门 .....	14
3.1.2 删除部门 .....	15
3.1.3 安全码管理 .....	15
4 用户 .....	17
4.1 用户管理 .....	17
4.1.1 新建用户 .....	17
4.1.2 用户角色 .....	18
4.1.3 导入用户 .....	19
4.1.4 导出用户 .....	21
4.1.5 删除用户 .....	21
4.1.6 锁定用户 .....	21
4.1.7 解锁用户 .....	21
4.1.8 搜索用户 .....	22
4.1.9 编辑用户 .....	22
4.1.10 用户配置 .....	23
4.1.11 SSH 公钥管理 .....	24
4.1.12 查看已授权的主机 .....	26
4.1.13 查看已授权应用 .....	26
4.1.14 API 访问 key 设置 .....	26
4.1.15 手机身份验证器 .....	27
4.2 用户组管理 .....	29

4.2.1 新建用户组 .....	29
4.2.2 删除用户组 .....	30
4.2.3 搜索用户组 .....	30
4.2.4 修改用户组名称 .....	30
4.2.5 用户组添加成员 .....	31
4.3 动态令牌 .....	32
4.3.2 导入令牌 .....	32
4.3.3 绑定用户 .....	33
4.3.4 禁用令牌 .....	34
4.3.5 挂失令牌 .....	34
4.3.6 启用令牌 .....	34
4.3.7 解除绑定 .....	35
4.3.8 删除令牌 .....	35
4.3.9 搜索令牌 .....	35
4.4 USBKEY .....	35
4.4.2 签发管理员 USBKEY .....	36
4.4.3 签发用户 USBKEY .....	36
4.4.4 吊销 USBKEY .....	37
<b>5 资产 .....</b>	<b>38</b>
5.1 主机管理 .....	38
5.1.1 新建主机 .....	38
5.1.2 主机账户选项说明 .....	42
5.1.3 导入主机 .....	46
5.1.4 导出主机 .....	48
5.1.5 删除主机 .....	48
5.1.6 禁用主机 .....	48
5.1.7 启用主机 .....	48
5.1.8 搜索主机 .....	48
5.1.9 编辑主机 .....	48
5.2 混合云管理 .....	53
5.2.1 新建局域网 .....	54
5.2.2 新建代理服务器 .....	54
5.2.3 添加主机 .....	55
5.2.4 新建公有云账户 .....	56
5.3 共享账户 .....	57
5.3.1 新建共享账户 .....	57

5.3.2 关联主机 .....	59
5.4 帐户组管理 .....	60
5.4.1 新建帐户组 .....	60
5.4.2 编辑账户组 .....	61
5.4.3 删除帐户组 .....	61
5.4.4 搜索帐户组 .....	61
5.5 应用管理 .....	62
5.5.1 添加应用服务器 .....	62
5.5.2 添加应用 .....	62
5.5.3 添加 IE 代填应用 .....	64
5.5.4 添加数据库类应用 .....	64
5.5.5 删除应用 .....	65
5.5.6 搜索应用 .....	65
5.5.7 编辑应用 .....	65
5.5.8 导出应用 .....	65
<b>6 授权 .....</b>	<b>67</b>
6.1 运维授权 .....	67
6.1.2 新建运维授权 .....	67
6.1.3 编辑运维规则 .....	69
6.1.4 删除、禁用或启用运维规则 .....	72
6.1.5 审批配置 .....	72
6.1.6 查看运维规则 .....	73
6.2 未授权登录审核 .....	73
6.2.1 授权审核条目 .....	73
6.2.2 删除审核条目 .....	74
6.2.3 搜索审核条目 .....	74
<b>7 审计 .....</b>	<b>74</b>
7.1 会话审计 .....	74
7.1.1 查看所有会话 .....	74
7.1.2 搜索审计会话 .....	76
7.1.3 查看应用会话 .....	77
7.1.4 搜索应用会话 .....	78
7.1.5 查询事件 .....	78
7.1.6 搜索事件 .....	79
7.2 审计规则 .....	79
7.2.2 添加审计规则 .....	80

<b>8 工单</b> .....	<b>81</b>
8.1 新建工单 .....	81
8.2 工单审批 .....	83
<b>9 运维</b> .....	<b>83</b>
9.1 工具下载 .....	83
9.1.1 单点登录器 .....	83
9.1.2 IE 代填工具 .....	84
9.1.3 USBKEY 控件(IE) .....	84
9.1.4 离线播放器与 Adobe AIR .....	84
9.1.5 Flash Player .....	84
9.1.6 字符客户端 .....	85
9.1.7 图形客户端 .....	85
9.1.8 文件传输客户端 .....	85
9.2 主机运维 .....	85
9.2.1 单点登录配置 .....	85
9.2.2 全局配置 .....	87
9.2.3 主机登录 .....	90
9.2.4 快速搜索 .....	91
9.2.5 查看主机 .....	91
9.2.6 重复 IP 合并 .....	91
9.2.7 未授权登录 .....	92
9.3 实时监控 .....	93
9.3.1 实时监控 .....	93
9.4 命令审批 .....	94
9.5 运维审批 .....	96
9.6 运维报表 .....	99
9.6.1 按时间范围查看 .....	99
9.6.2 导出报表 .....	99
9.6.3 报表自动发送 .....	100
<b>10 任务</b> .....	<b>100</b>
10.1 改密计划 .....	100
10.1.1 新建改密计划 .....	101
10.1.2 编辑改密任务 .....	103
10.2 自动运维 .....	104
10.2.1 新建自动运维 .....	105
10.2.2 自动运维命令列表 .....	106

10.2.3 编辑自动运维 .....	106
<b>11 系统 .....</b>	<b>108</b>
11.1 认证管理 .....	108
11.1.1 安全配置 .....	108
11.1.2 远程认证 .....	109
11.1.3 双因子认证 .....	113
11.1.4 第三方 HTTP 平台认证 .....	114
11.2 网络配置 .....	116
11.2.1 网络配置 .....	116
11.2.2 Web 设置 .....	121
11.2.3 HA 配置 .....	122
11.2.4 静态路由 .....	126
11.2.5 SNMP 配置 .....	126
11.2.6 集群管理 .....	128
11.2.7 IP 源防护 .....	130
11.3 系统配置 .....	133
11.3.1 运维配置 .....	133
11.3.2 告警配置 .....	135
11.3.3 语言和界面配置 .....	137
11.3.4 功能设置 .....	138
11.3.5 SSHKEY 配置 .....	140
11.3.1 改密脚本设置 .....	141
11.4 存储管理 .....	144
11.4.1 数据归档 .....	144
11.4.2 日志备份 .....	145
11.4.3 磁盘管理 .....	146
11.5 操作日志 .....	147
11.6 系统报表 .....	148
11.6.1 按小时查看 .....	149
11.6.2 按天查看 .....	149
11.6.3 按周查看 .....	150
11.6.4 按月查看 .....	150
11.6.5 导出报表 .....	151
11.7 本机维护 .....	151
11.7.1 系统管理 .....	151
11.7.2 升级管理 .....	152

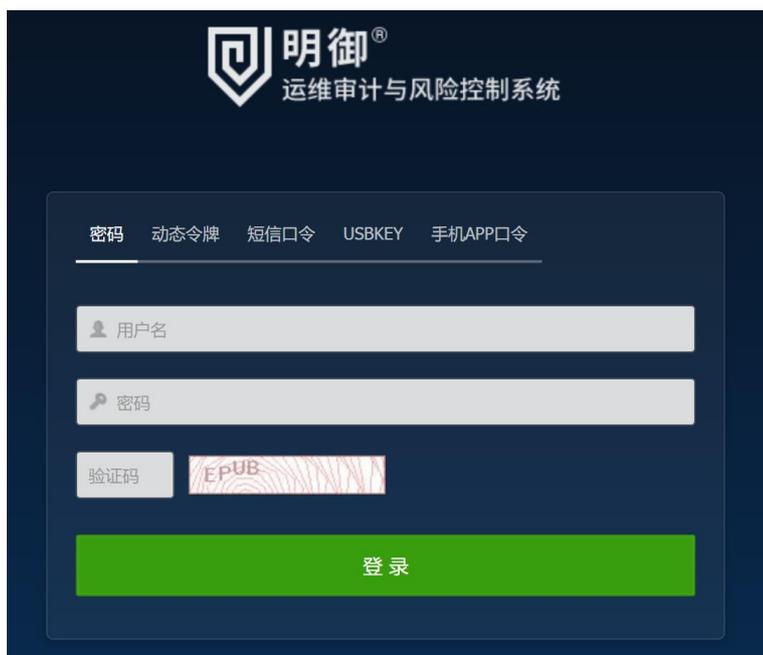
11.7.3 许可证 .....	153
11.7.4 资源监视 .....	154
11.7.5 系统备份 .....	155
11.7.6 系统同步推送 .....	157
11.7.7 系统同步接收 .....	158
11.7.8 调试日志 .....	158
11.7.9 网络诊断工具 .....	159
11.7.10 系统诊断工具 .....	161
11.7.11 系统警报 .....	162
11.7.1 控制台 SSH 公钥 .....	162

# 1 登录系统

通过 WEB 方式管理系统。

- (1) 在浏览器中输入 `https://系统管理 IP`，进入登录窗口。
- (2) 在登录窗口中输入用户名、密码、验证码，（初始密码：123456）

图1-1 登录框示意图



- (3) 单击<登录>后即可进入管理首页。

图1-2 系统首页示意图

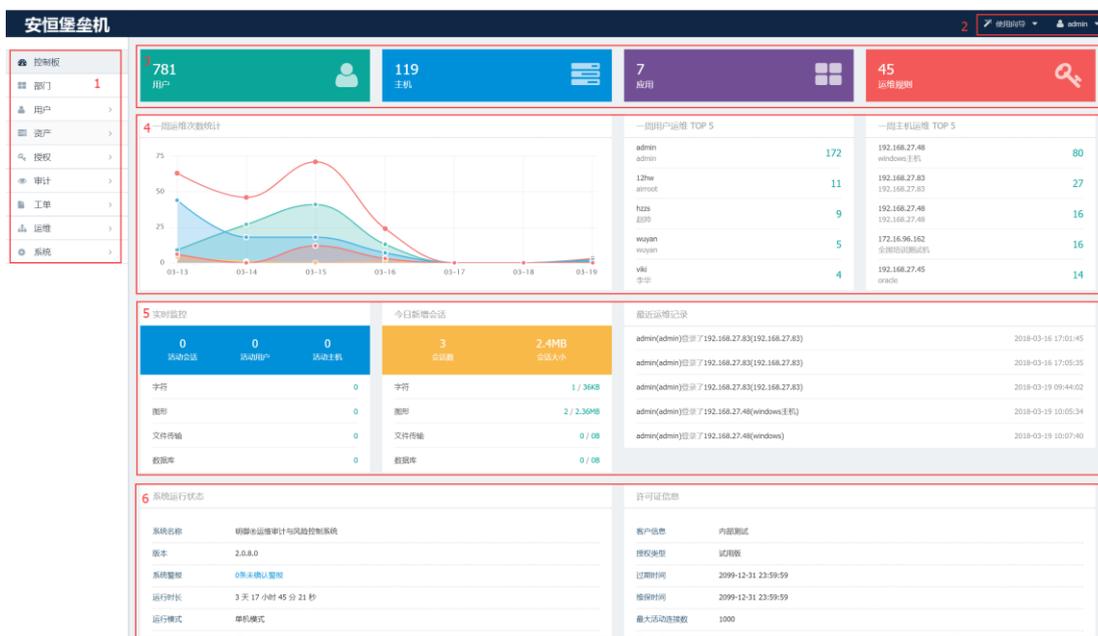


图1-3 用户菜单示意图



表1-1 系统首页说明

区域编号	区域页面介绍
①	显示系统的功能菜单项：控制板、部门、用户、资产、授权、审计、工单、运维和系统
②	使用向导、用户功能菜单项
③	从左往右分别是本用户管理下的用户数量、主机数量、应用数量和运维授权关系数量
④	从左往右依次为一周运维次数统计、一周运维次数用户排名和一周运维次数主机排名。
⑤	从左往右依次为实时监控统计、新增会话记录和最近运维记录。

⑥

从左往右依次为系统运行状态（设备名称、产品描述、软硬件版本等）和许可证信息（授权类型、过期时间、最大活动连接数等）

## 2 控制板

控制板用于显示系统的常用功能、系统运行状态、最近运维会话、系统许可信息等。

### 2.1 用户和资产

显示了能够管理的用户数量、主机数量、应用数量和授权关系数量。单击图标可进入对应的管理界面。

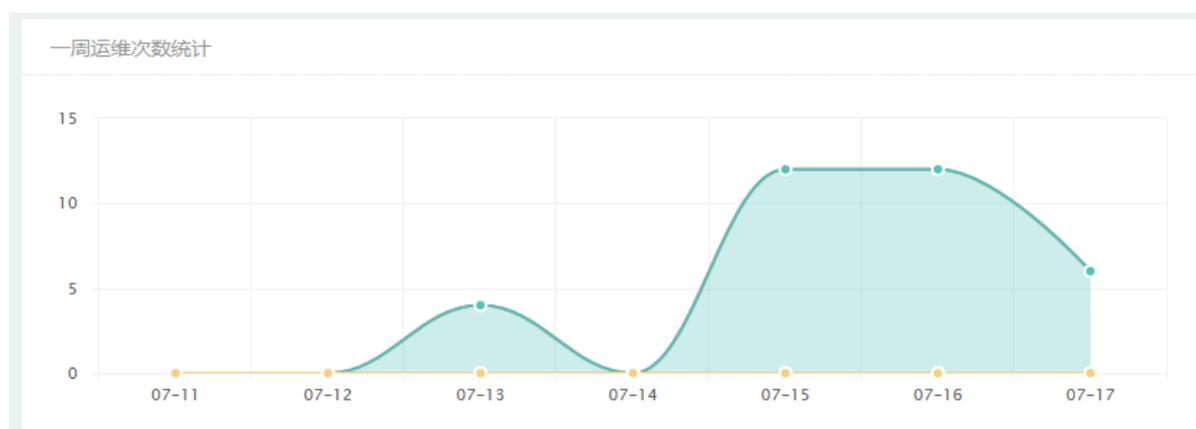
图2-1 用户和资产数量示意图



### 2.2 一周运维次数统计

根据会话类型统计出一周的运维次数。

图2-2 一周运维次数示意图



### 2.3 一周用户运维

根据一周运维次数对用户进行排名。

图2-3 一周用户运维示意图

一周用户运维 TOP 5	
yunwei operator	30
lqz lqz	3

## 2.4 一周主机运维

根据一周运维次数对主机进行排名。

图2-4 一周主机运维示意图

一周主机运维 TOP 5	
10.11.200.10 server	15
192.168.50.139	11
10.11.200.7 fileservr	3
10.11.33.99 rdpservr	2
192.168.50.139 192.168.50.139	1

## 2.5 实时监控

显示当前活动的会话数量和活动的用户数量。

## 2.6 今日新增会话

显示今天产生的运维会话数量。

## 2.7 最近运维记录

显示最近五条具体运维记录。

## 2.8 系统运行状态

系统运行状态显示内容。

图 2-5 系统运行状态显示示意图

系统名称	明御®运维审计与风险控制系统
版本	2.0.8.0
系统警报	0条未确认警报
运行时长	3 天 17 小时 45 分 21 秒
运行模式	单机模式
持有VIP	否
集群模式	主节点

表1-2 系统运行状态显示说明

显示内容	内容描述
系统名称	系统名称
版本号	显示产品的软件版本号
运行时长	显示系统运行的时间是多久
系统报警	由运维审计系统自身产生的报警信息，如CPU、内存等使用率过高产生的报警信息
本地认证	是否开启
远程认证	是否开启
运行模式	是单机模式，还是双机主备模式
持有VIP	是否有虚拟IP地址
集群模式	节点类型

## 2.9 许可证信息

许可证信息包括授权类型、过期时间、最大活动连接数和最大主机数。

图2-5 许可证信息显示示意图

### 许可证信息

授权类型	正式版
过期时间	2099-12-31 00:00:00
最大活动连接数	10000
最大主机数	10000

## 3 部门

明御®运维审计与风险控制系統引入了部门（类似组织结构）的概念，以达到数据隔离的目的。可以隔离用户、主机、授权、审计，并由部门管理员统一管理。

### 3.1 部门管理

部门主要有以下功能：作为容器，包含资产、用户、用户组和子部门；隔离数据，本部门管理员无法看到本部门以外的数据。

#### 3.1.1 新建部门

步骤1 进入[部门]管理界面，单击<新建部门>。

图3-1 部门管理界面



步骤2 选择<上级部门>，填写新建部门的名称。

图3-2 新建部门示意图

## 新建部门

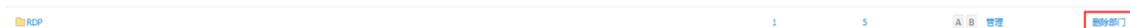


步骤3 单击<创建部门>，新部门建立完毕，可在部门管理界面查看该部门。

### 3.1.2 删除部门

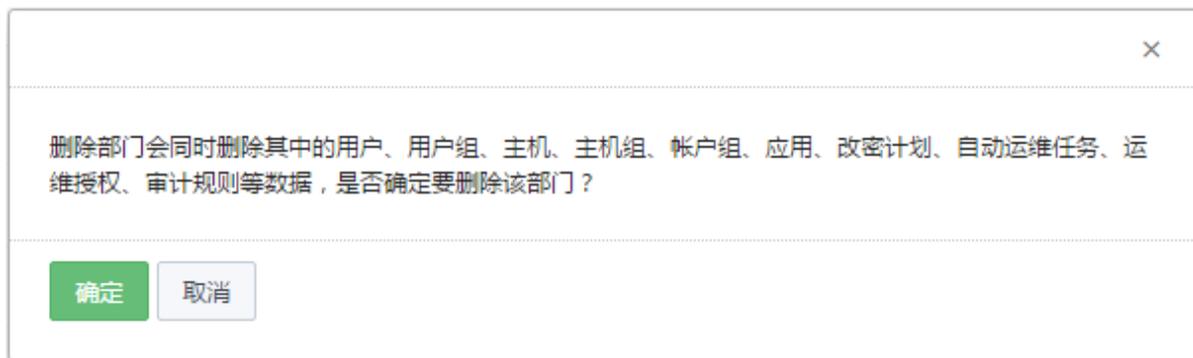
步骤1 在部门列表右方单击<删除部门>。

图3-3 删除部门按钮示意图



步骤2 单击<删除部门>后，提示是否要删除部门及相关数据？

图3-4 删除部门警示示意图



步骤3 单击<确定>后即可成功删除。

### 3.1.3 安全码管理

安全码是部门导出主机密码文件的 zip 包加密密码，分为两部分。运维管理员可以设置安全码前半段(KeyA)，密码管理员可以设置安全码后半段(KeyB)，超级管理员和部门管理员可以对安全码的两部分都进行设置。

图3-5 安全码管理界面

安全码是部门导出主机密码文件的zip包加密密码，分为两部分。运维管理员可以设置安全码前半段(KeyA)，密码管理员可以设置安全码后半段(KeyB)。

例：KeyA设置为 123，KeyB设置为 456，安全码为 123456

例：KeyA设置为 123，KeyB未设置，安全码为 123

例：KeyA未设置，KeyB设置为 456，安全码为 456

---

部门：lqz-department

---

KeyA	已设置   <a href="#">发送到我的邮箱</a>   <a href="#">清除</a>
KeyB	已设置   <a href="#">发送到我的邮箱</a>   <a href="#">清除</a>
更改时间	2016-01-18 16:09:44

---

更改KeyA

KeyA   显示 1-100个数字、英文字母和符号

[保存更改](#)

---

更改KeyB

KeyB   显示 1-100个数字、英文字母和符号

[保存更改](#)

# 4 用户

用户是用于管理运维审计系统的用户成员、部门、用户组、认证方式等功能模块。

## 4.1 用户管理

用户管理用于管理用户成员的创建、编辑、导入、导出等功能。

### 4.1.1 新建用户

步骤1 进入[用户/用户管理]页面。

图4-1 用户管理页面示意图



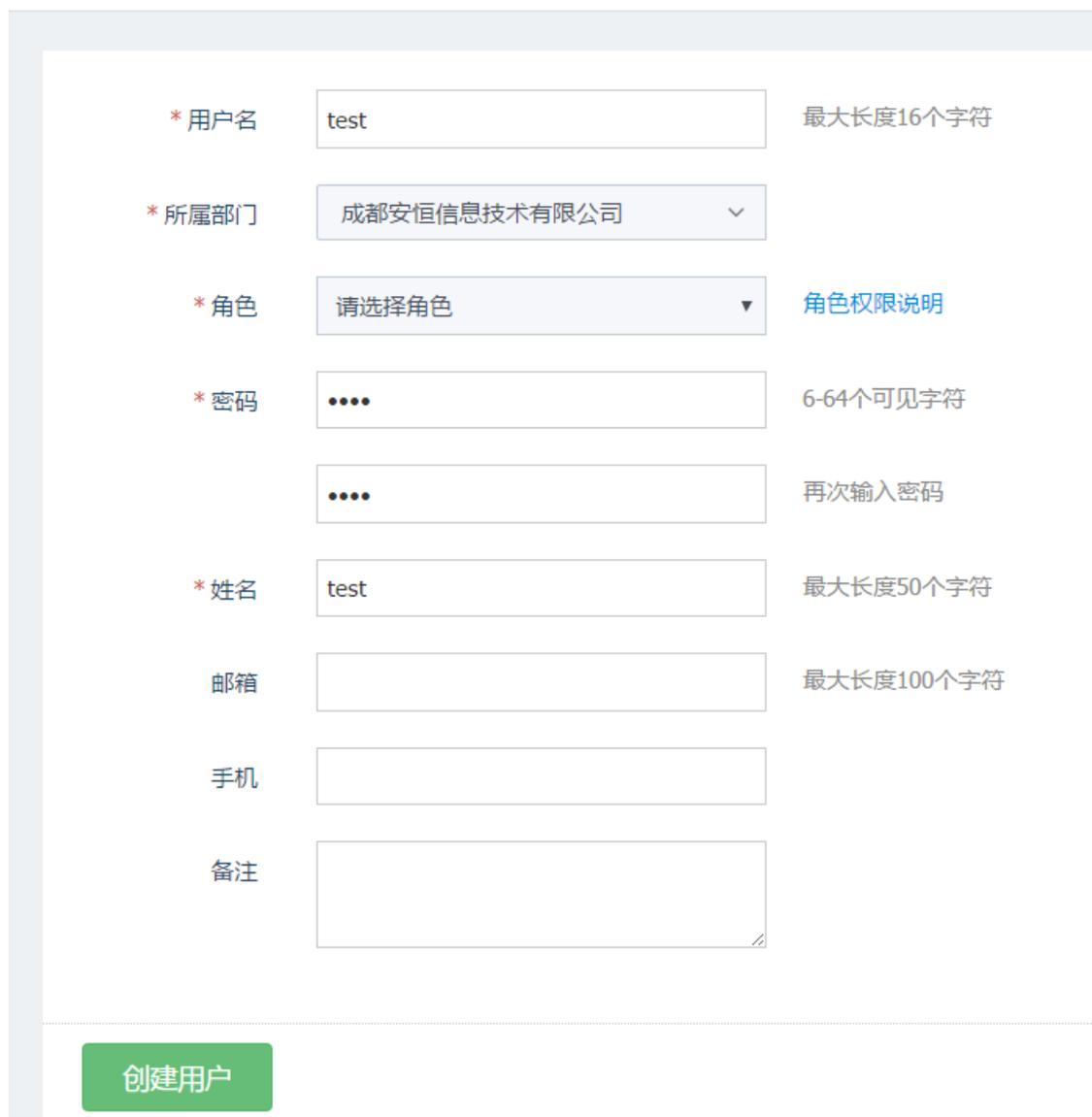
步骤2 单击<新建用户>，进入配置页面。



标红星部分是必填项，填写信息时，请按照要求填写。

图4-2 新建用户示意图

## 新建用户



\* 用户名: test 最大长度16个字符

\* 所属部门: 成都安恒信息技术有限公司

\* 角色: 请选择角色 [角色权限说明](#)

\* 密码: 6-64个可见字符

再次输入密码

\* 姓名: test 最大长度50个字符

邮箱: 最大长度100个字符

手机

备注

**创建用户**

步骤3 单击<保存更改 >后即可成功。

图4-3 创建用户完成提示示意图



步骤4 单击图 4-3 中的用户名称可继续编辑用户相关信息。

### 4.1.2 用户角色

用户角色包括部门管理员、运维管理员、审计管理员、系统管理员、密码管理员、运维员和审计员。

进入[用户/用户管理/新建用户]页面，可以查看用户角色的权限功能范围。  
用户角色的权限是固定的，无法修改。

图4-4 用户角色权限示意图

	超级管理员	部门管理员	运维管理员	密码管理员	审计管理员	运维员	审计员	系统管理员
<b>部门管理</b> 部门添加、删除、编辑	●	●						
<b>安全管理</b> 设置部门安全码	●	●	●	●				
<b>用户管理</b> 用户增加、删除、编辑	●	●	●		●			
<b>用户组管理</b> 用户组增加、删除、编辑	●	●	●					
<b>动态令牌</b> 管理动态令牌	●	●	●		●			
<b>USBKEY</b> 管理USBKEY	●	●	●		●			
<b>资产管理</b> 管理资产	●	●	●					
<b>授权管理</b> 管理运维规则、审批工单	●	●	●					
<b>会话审计</b> 查看、清除、下载历史会话	●	●			●		● 需要审计规则允许	
<b>审计规则</b> 管理审计规则	●	●			●			
<b>主机运维</b> 主机运维、应用运维、创建工单、查看运维报告	●	●	●	●	●	●	●	●
<b>实时监控</b> 管理、审批在线会话	●	●	●					
<b>系统管理</b> 系统配置、操作日志、系统报表、数据维护、系统维护	●							●

### 4.1.3 导入用户

步骤1 进入[用户/用户管理]页面。

步骤2 单击<更多操作>，显示“导入用户”。

图4-5 导入用户按钮示意图



步骤3 单击<导入用户>后进入“导入用户”页面。

图4-6 导入用户页面示意图

## 导入用户

请上传本由本系统导出的文件。或 [下载模板文件](#)，根据文件内提供的格式填写完成后上传到本系统。

上传文件 📁 上传文件

认证方式 本地认证 ▼

其他选项  覆盖已有用户

导入用户

步骤4 单击<下载模板文件>下载后并解压，在用户表格中编辑用户信息。

图4-7 用户导入表格模板示意图

	A	B	C	D	E	F	G
1	# 用户名必填，认证模式为本地认证时密码也必填，其他字段可以不填，样例数据如下所示：						
2	#用户名	密码	部门	角色	姓名	邮箱	手机
3	auditor	1qsd3eef	部门1	审计员	姓名1	auditor@xxx.com	13111111111
4	operator	1w2sddfdd	部门2	运维员	姓名2	operator@xxx.com	13111111112

说明

第一列为用户名（必填项）、第二列为密码（必填项）、第三列为部门（必填项）、第四列为角色（必填项）、第五列为姓名（可选项）、第六列为邮箱（可选项）、第七列为电话号码（可选项）。

步骤5 单击<上传文件>上传用户表。

步骤6 单击<导入用户>后即可导入成功。

#### 4.1.4 导出用户

步骤1 进入[用户/用户管理]页面。

步骤2 用户列表右下角单击<导出用户>后即可查看用户表信息。

#### 4.1.5 删除用户

步骤1 在用户列表中勾选需要删除的用户。

步骤2 单击“删除”按钮即可。

#### 4.1.6 锁定用户

步骤1 在用户列表中单击需要锁定的用户；

步骤2 在用户配置页面勾选“禁用这个用户”，或是在用户列表页面勾选相应的用户后单击锁定即可。

图4-8 锁定用户示意图



#### 4.1.7 解锁用户

步骤1 在用户配置页面取消“禁用这个用户”选项即可解锁，或是在用户列表界面勾选相应的用户，单击解锁按钮。

图4-9 锁定按钮

## 用户管理



### 4.1.8 搜索用户

步骤1 在图 4-1 中搜索框中输入用户名关键字，回车后即可成功过滤出用户列表，也可通过不同的部门和用户角色进行过滤。

### 4.1.9 编辑用户

- 步骤1 进入[用户/用户管理]页面。
- 步骤2 单击用户名，进入编辑页面。
- 步骤3 单击<基本信息>，进入基本信息页面。

图4-10 编辑用户基本信息页面示意图

## 用户信息

基本信息	用户配置	SSH公钥	已授权主机	已授权应用
* 用户名	test			
* 所属部门	用户根			
* 角色	运维员			<a href="#">角色权限说明</a>
* 认证模式	本地认证			
* 密码	<input type="password"/>			6-64个可见字符
	<input type="password"/>			再次输入密码
* 姓名	test			最大长度50个字符
邮箱	<input type="text"/>			最大长度100个字符
手机	<input type="text"/>			
备注	<input type="text"/>			

[保存更改](#)

步骤4 单击<保存更改>即可修改成功。

### 4.1.10 用户配置

步骤1 单击<用户配置>后进入配置页面。

图4-11 用户配置页面示意图

用户信息

基本信息   
  用户配置   
  SSH公钥   
  已授权主机   
  已授权应用

状态  锁定这个用户

认证方式  密码  
 密码和手机APP口令  
 密码和动态令牌  
 密码和USBKEY  
 密码和短信口令

手机APP验证器 未设置

登录IP范围 (黑名单) 不允许以下IP

IP列表

填写点分十进制格式的IPv4地址或IP段，每行只填写一个IP或者一段IP，IP段的起始IP和结束IP之间用“-”隔开。若需填写注释信息，该行请以“#”开头。例：192.168.0.1 或 192.168.0.1 - 192.168.0.255

有效期  -

登录时间限制

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
周一	允许																							
周二	允许																							
周三	允许																							
周四	允许																							
周五	允许																							
周六	允许																							
周日	允许																							

允许     禁止

步骤2 设置用户锁定状态、登录 IP 黑白名单和登录时间限制。

步骤3 单击保存更改即可。

### 4.1.11 SSH 公钥管理

步骤1 单击<SSH 公钥>后进入配置页面。

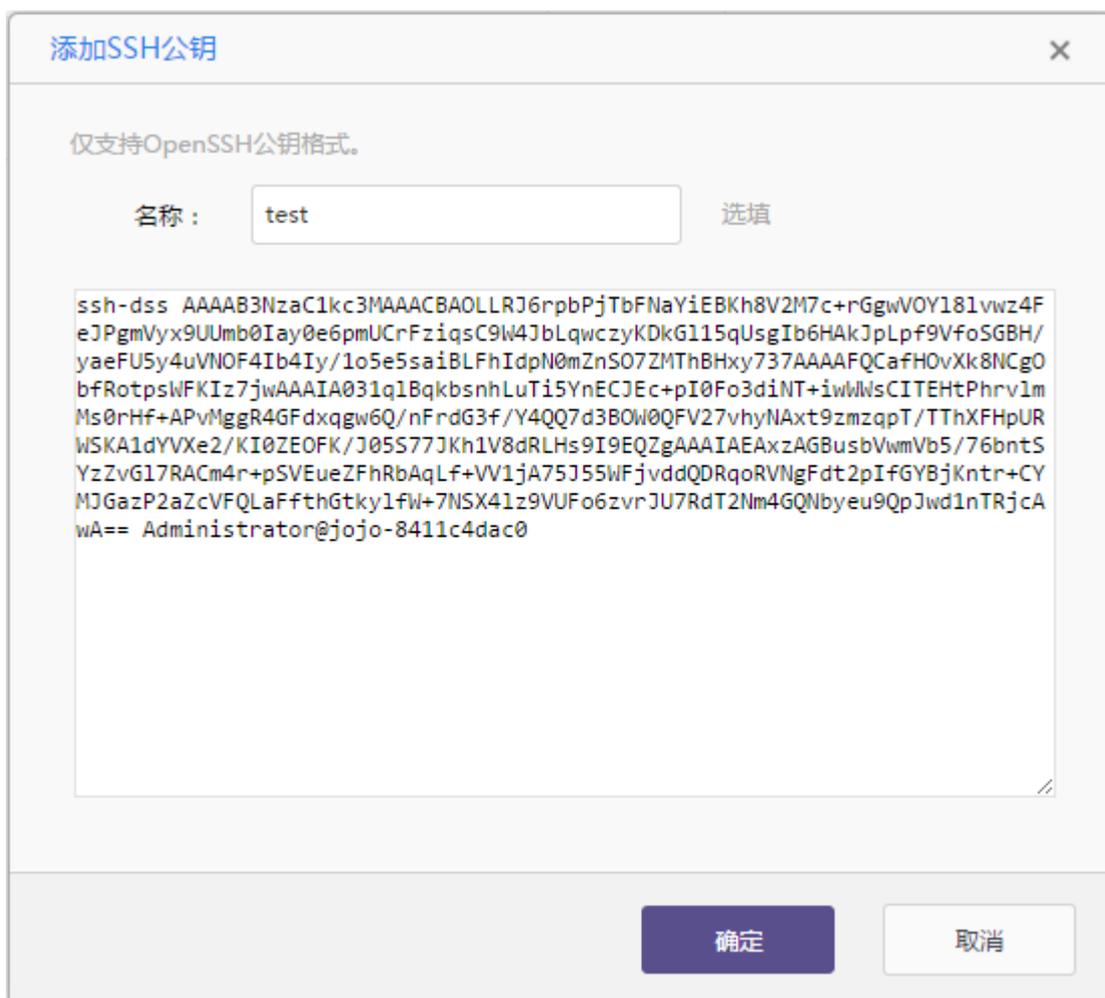
图4-12 用户 SSH 公钥管理页面示意图

用户信息



步骤2 单击<添加 SSH 公钥>后，弹出配置窗口。添加公钥名称和公钥内容。

图4-13 SSH 公钥添加页面示意图



步骤3 单击<确定>后即可添加成功并返回配置页面。

### 4.1.12 查看已授权的主机

步骤1 单击<已授权主机>可查看该已授权给该用户的所有主机。

图4-14 已授权主机列表

用户信息

基本信息 用户配置 SSH公钥 已授权主机 已授权应用

按运维规则过滤

搜索主机名/主机IP

主机	主机组	主机帐户
10.11.0.222 10.11.0.222	运维测试组	[RDP] root
10.11.32.221 应用中心	运维测试组	[RDP] administrator
10.11.32.30 CentOS	运维测试组	[SSH] hh
10.11.32.50 win2012-RD	运维测试组	[RDP] hh.com/administrator
10.11.32.60 SQL_server	运维测试组	[SQL Server] sa
10.11.32.60 SQLServer2008	运维测试组	[SQL Server] sa
10.11.33.66 10.11.33.66		[SFTP] hex
10.11.33.99 win10	运维测试组	[RDP] root

### 4.1.13 查看已授权应用

步骤1 单击<已授权应用>可查看该已授权给该用户的所有应用。

图4-15 已授权应用列表

用户信息

基本信息 用户配置 SSH公钥 已授权主机 已授权应用

按运维规则过滤

搜索应用名称

应用名称
ie

### 4.1.14 API 访问 key 设置

API 访问键主要用于设置二次开发时，调用本系统 API 所需要的 token。

API 访问键是本系统 API 服务的认证凭据，API 通过 AccessToken 来验证某个请求发送者的身份，AccessToken 根据用户账号有所区分，每个账号提供的 AccessToken 拥有对拥有的资源有完全的权限。

当用户想以个人身份发送请求时，需要首先将发送的请求 Headers 添加 AccessToken 字段，并设置有效访问键值；系统收到请求以后，会通过 AccessToken 找到对应的用户，以同样的方法提取验证码，如果计算出来的验证码和提供的一样即认为该请求是有效的；否则，系统将拒绝处理这次请求，并返回 HTTP 403 错误。

步骤1 进入用户信息个人页面的 API 模块。

图4-16 API 访问键设置页面

### 个人信息

个人信息	修改密码	SSH公钥	SSH私钥	CS登录口令	手机身份验证器	API访问键
------	------	-------	-------	--------	---------	--------

API访问键是访问本系统开放API的唯一凭据，请妥善保管。使用API访问键请参阅产品文档。

状态  启用

API访问键  [重置](#)

创建时间 2018-01-08 14:43:14

步骤2 勾选“启用”，如果记得之前设置的访问键，则跳转到步骤 4。

步骤3 如果忘记之前设置的访问键，则单击<重置>，记住设置的键。

步骤4 单击保存。



API访问键的使用请参考《明御®运维审计与风险控制系统用户手册二次开发API》。

#### 4.1.15 手机身份验证器

如果用户选择手机 APP 口令方法登录，需要输入手机身份验证器所提供的动态口令。

图4-17 登录界面



步骤1 进入用户个人信息页面中手机身份验证器模块。

图4-18 手机 APP 口令验证界面



步骤2 根据提示信息，下载身份验证器到手机。

步骤3 单击设置验证器，在手机上根据页面提示操作即可。

图4-19 手机 APP 验证设置界面



## 4.2 用户组管理

用户组概念的引入主要是为了将用户打包，实现批量授权的功能。用户组管理模块用于对用户组的创建、编辑、删除以及添加用户成员等功能。

### 4.2.1 新建用户组

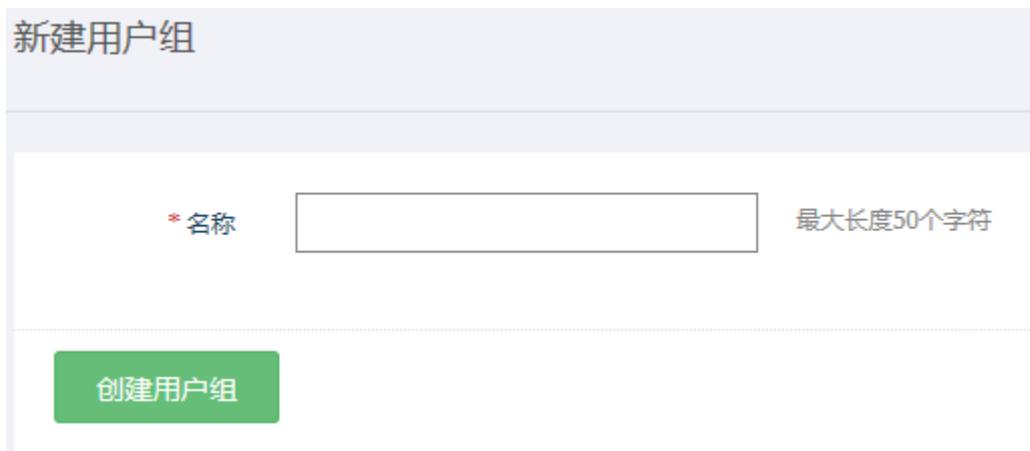
步骤1 进入[用户/用户组管理]页面。

图4-20 用户组管理页面示意图

用户组管理			+ 新建用户组
<input type="checkbox"/> 删除	首页	上一页	1 / 1
	下一页	末页	
搜索用户组	按部门过滤		
用户组名称	所属部门	成员数	
<input type="checkbox"/> kqyonghuzu	kqz部	0	
<input type="checkbox"/> kqz用户组	用户组	1	
<input type="checkbox"/> 运维操作员组	运维操作员组	1	
<input type="checkbox"/> 运维测试	运维测试	2	
<input type="checkbox"/> 部门堡垒机	部门堡垒机	1	

步骤2 单击<新建用户组>后，进入配置页面：填写用户组名称。

图4-21 新建用户组页面示意图



新建用户组

\* 名称  最大长度50个字符

创建用户组

步骤3 单击<创建用户组>后，页面会提示创建用户组成功。

图4-22 用户组创建成功提示

用户组 test 已创建

步骤4 单击用户组名称可进入编辑页面，添加、删除用户组成员。

#### 4.2.2 删除用户组

步骤1 进入[用户/用户组管理]页面中。

步骤2 勾选需要删除的用户组。

步骤3 单击“删除”按钮后即可删除成功。

#### 4.2.3 搜索用户组

与搜索用户方法相同。

#### 4.2.4 修改用户组名称

步骤1 进入用户组管理界面，单击列表中的某个用户组，进入用户组信息页面。

图4-23 用户组信息页面



用户组信息 liqaz

用户组成员 修改用户组名称

删除 添加成员

搜索用户组/姓名 Q 按角色过滤 按部门过滤

用户	角色	部门
<input type="checkbox"/> yi qi	运维管理员	l-de
<input type="checkbox"/> zhong qi	运维管理员	l-de

首页 上一页 1/1 下一页 末页

步骤2 单击[修改用户组名称]，进入名称编辑页面。

图4-24 用户组名称编辑页面

用户组信息 llqqzz

用户组成员 修改用户组名称

部门 l-de

\* 名称  最大长度50个字符

保存更改

步骤3 单击[保存更改]。

#### 4.2.5 用户组添加成员

步骤1 在用户组配置页面单击<用户组成员>后，进入配置页面。

图4-25 用户组添加成员管理页面示意图

用户组信息 llqq用户组

用户组成员 修改用户组名称

移除

首页 上一页 1/1 下一页 末页

搜索用户名/姓名

按角色过滤 按部门过滤

用户	角色	部门
<input type="checkbox"/> llqzadmin llqzadmin	部门管理员	llqz部

步骤2 单击<添加成员>，弹出用户列表。勾选需要添加的用户

图4-26 用户添加成员列表示意图

选择用户 ×

添加

首页 上一页 1 / 1 下一页 末页

	搜索用户名/姓名	按部门过滤	按角色过滤
<input type="checkbox"/>	admin	用户根	超级管理员
<input type="checkbox"/>	hehe hehe	运维测试	部门管理员
<input type="checkbox"/>	lqyunwei lqyunwei	lqz部	运维员
<input type="checkbox"/>	openctm openctm	openctm	部门管理员
<input type="checkbox"/>	operator operator	用户根	部门管理员
<input type="checkbox"/>	test test	lqz部	运维员
<input type="checkbox"/>	xlx_operator adf	运维操作员组	运维员
<input type="checkbox"/>	zheng1_dept zhengxx	部门-郑xx	部门管理员
<input type="checkbox"/>	zheng1_dept_2 zhengxx	部门-堡垒机	运维员

步骤3 单击<添加>后即可添加成功并自动返回配置页面。

## 4.3 动态令牌

动态令牌用于用户采用动态密码认证方式登录运维审计系统的令牌管理。

图4-27 动态令牌硬件示意图



### 4.3.2 导入令牌

步骤1 进入[用户/动态令牌]页面中。

图4-28 动态令牌管理页面示意图

动态令牌 <span style="float: right;">导入令牌</span>					
<input type="checkbox"/> 删除    移动到 ▾    禁用    挂失    应用    解除绑定		首页    上一页    1/1 ▾    下一页    末页			
搜索序列号 <input type="text"/> 搜索用户 <input type="text"/>		按部门过滤 ▾	请选择状态 ▾		
序列号	绑定给用户	令牌所属部门	状态	失效时间	操作
<input type="checkbox"/> 2600400344881		部门-部xx	已禁用	2019-06-09 13:57:00	操作 ▾
<input type="checkbox"/> 2600400344882		部门-部xx	已禁用	2019-06-09 13:57:00	操作 ▾
<input type="checkbox"/> 2600400344883		部门-部xx	已禁用	2019-06-09 13:57:00	操作 ▾
<input type="checkbox"/> 2600400344884		部门-部xx	已禁用	2019-06-09 13:57:00	操作 ▾
<input type="checkbox"/> 2600400344885		部门-部xx	已禁用	2019-06-09 13:57:00	操作 ▾
<input type="checkbox"/> 2600400344886		用户根	已禁用	2019-06-09 13:57:00	操作 ▾
<input type="checkbox"/> 2600400344887		用户根	已禁用	2019-06-09 13:57:00	操作 ▾
<input type="checkbox"/> 2600400344888	kzyunwei kzyunwei	kz部	已启用	2019-06-09 13:57:00	操作 ▾

步骤2 单击<导入令牌>，在弹出的打开文件对话框中选择要导入的动态令牌种子文件进行导入。



种子文件需要向动态令牌供应商申请。

### 4.3.3 绑定用户

步骤1 进入[用户/动态令牌]页面中。

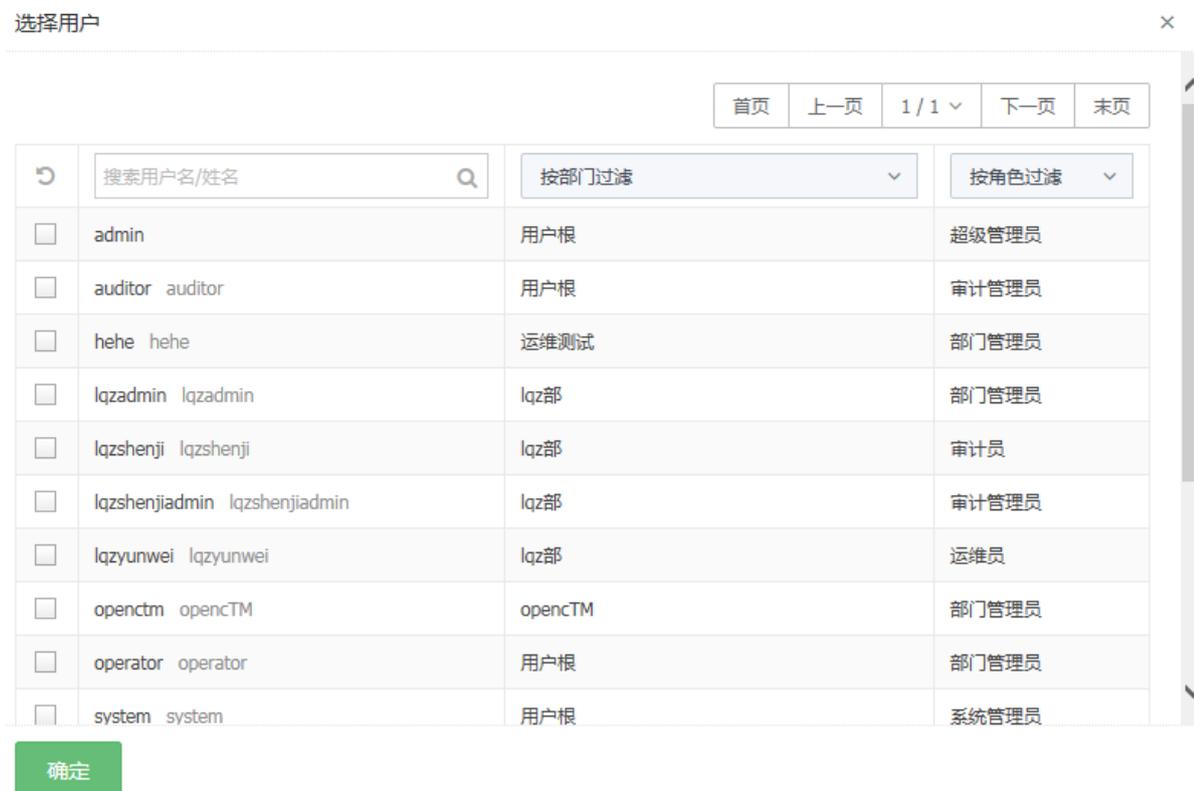
步骤2 单击<操作>后，展示操作列表。

图4-29 操作功能列表示意图



步骤3 单击<绑定>后，弹出用户列表。

图4-30 绑定用户列表示意图



步骤4 选择某个用户，单击确定即可实现绑定。。

#### 4.3.4 禁用令牌

步骤1 进入[用户/动态令牌]页面中。

步骤2 勾选需要禁用的令牌。

步骤3 单击<禁用>后，即可将该令牌变为禁用状态。

#### 4.3.5 挂失令牌

步骤1 进入[用户/动态令牌]页面中。

步骤2 勾选需要挂失的令牌。

步骤3 单击<挂失>后，即可将该令牌变为挂失状态。

#### 4.3.6 启用令牌

步骤1 进入[用户/动态令牌]页面中。

步骤2 勾选需要启用的令牌。

步骤3 单击<启用>后，即可将该令牌变为启用状态。

### 4.3.7 解除绑定

- 步骤1 进入[用户/动态令牌]页面中。
- 步骤2 勾选需要解绑的令牌。
- 步骤3 单击<解除绑定>后，即可解除该令牌与用户之间的关系。

### 4.3.8 删除令牌

- 步骤1 进入[用户/动态令牌]页面中。
- 步骤2 勾选需要删除的令牌。

图4-31 删除动态令牌页面示意图



- 步骤3 单击<>后，即可将该令牌删除。

### 4.3.9 搜索令牌

- 步骤1 进入[用户/动态令牌]页面中。
- 步骤2 可按用户名或动态令牌序列号进行搜索，也可根据部门和令牌状态（禁用、启用、挂失等状态）进行过滤。
- 步骤3 单击<搜索>即可过滤出令牌信息。

## 4.4 USBKEY

USBKEY 用于用户采用 USBKEY 认证方式登录运维审计系统的 USBKEY 管理。

图4-32 USBKEY 硬件示意图



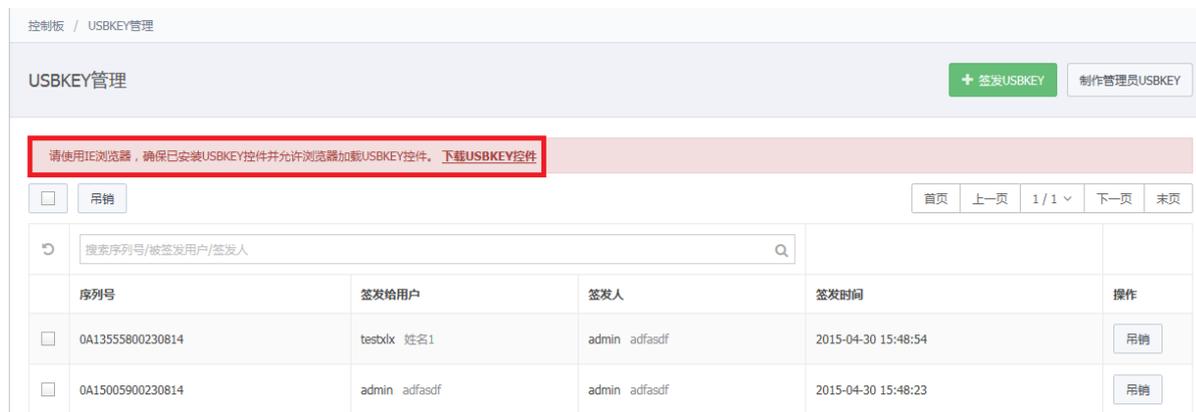
USBKEY仅支持IE浏览器使用！请先签发管理员USBKEY，再签发其他用户USBKEY。

## 4.4.2 签发管理员 USBKEY

步骤1 使用 IE 浏览器登录到运维审计系统。

步骤2 进入[用户/USBKEY/管理员 USBKEY]页面。

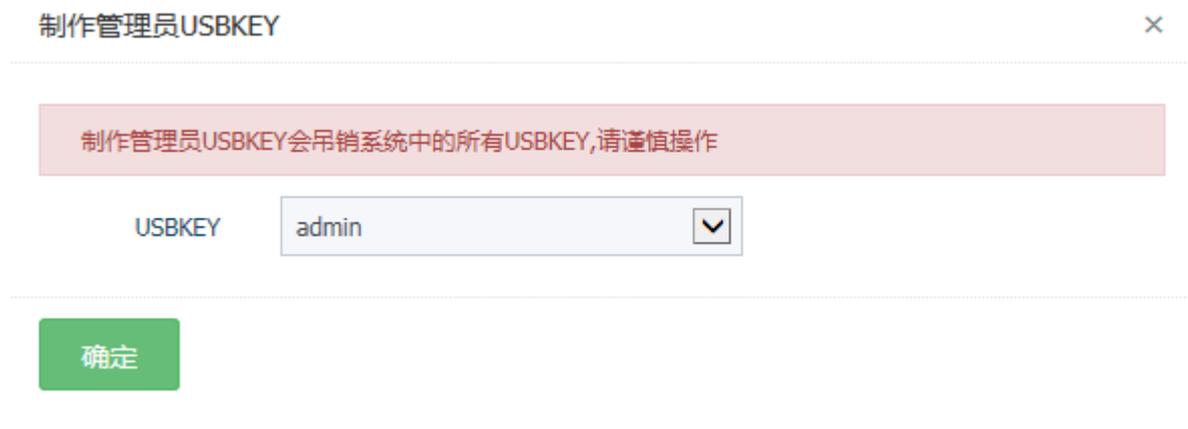
图4-33 USBKEY 管理页面示意图



步骤3 在本地 PC 上插上管理员 USBKEY。

步骤4 单击<制作管理员 USBKEY>后，弹出签发管理员 USBKEY 窗口。选择管理员。

图4-34 签发管理员 USBKEY 示意图



步骤5 单击<确定>后即可签发成功。

## 4.4.3 签发用户 USBKEY

步骤1 使用 IE 浏览器登录到运维审计系统。

步骤2 进入[用户/USBKEY/用户 USBKEY]页面。

步骤3 在本地 PC 上插上用户 USBKEY 和管理员 USBKEY。

步骤4 单击<签发 USBKEY>，弹出签发 USBKEY 窗口。选择好需要被签发的用户。

图4-35 签发用户 USBKEY 示意图

### 签发USBKEY

签发人USBKEY  ▼

被签发USBKEY  ▼

签发给用户 
选择用户

确定

步骤5 单击<确定>后即可签发成功。

#### 4.4.4 吊销 USBKEY

步骤1 使用 IE 浏览器登录到运维审计系统。

步骤2 进入[用户/USBKEY]页面，勾选需要吊销的 USBKEY。

步骤3 单击<吊销>后即可。

# 5 资产

资产是用于管理目标主机的 IP、协议、帐户、密码、应用发布等功能模块。

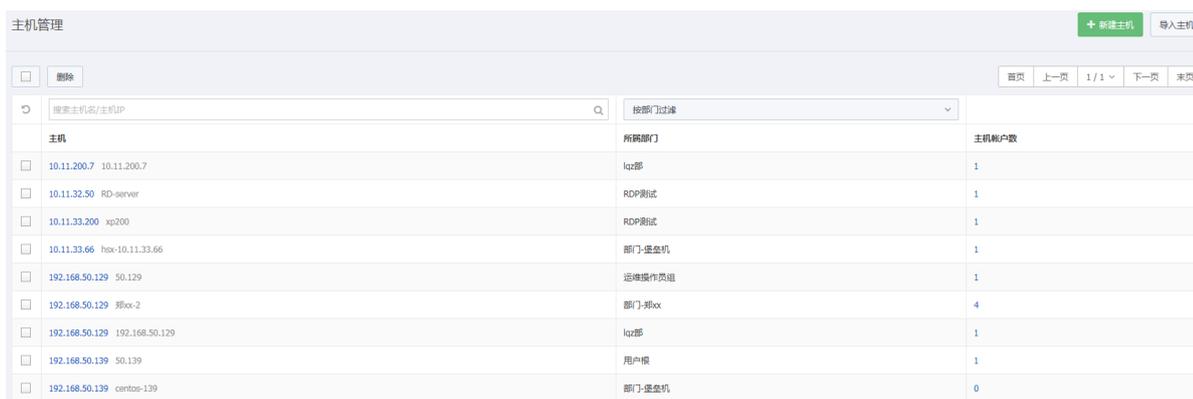
## 5.1 主机管理

主机管理用于管理目标主机的 IP、名称、协议、策略、添加、导入、导出、编辑等功能。

### 5.1.1 新建主机

步骤1 进入[资产/主机管理]页面。

图5-1 主机管理页面示意图



主机	所属部门	主机帐户数
10.11.200.7 10.11.200.7	lqz部	1
10.11.32.50 RD-server	RDP测试	1
10.11.33.200 xp200	RDP测试	1
10.11.33.66 hxx-10.11.33.66	部门-堡垒机	1
192.168.50.129 50.129	运维操作员组	1
192.168.50.129 邦oo-2	部门-邦oo	4
192.168.50.129 192.168.50.129	lqz部	1
192.168.50.139 50.139	用户组	1
192.168.50.139 centos-139	部门-堡垒机	0

步骤2 单击<新建主机>，进入新建主机配置页面。填写主机 IP、主机名称、所属部门、所属网络等。

图5-2 添加主机页面示意图



新建主机

\* 所属部门: 安恒信息

\* 主机网络: Default Network

\* 主机IP:  支持IPv4地址和域名格式, 例: 192.168.50.1 或者 www.example.com

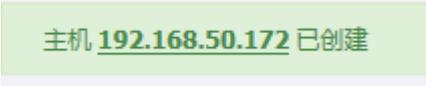
主机名称:  最大长度50个字符

备注:

创建主机

步骤3 单击<创建主机>后提示成功添加主机。

图5-3 添加主机成功显示示意图



主机 [192.168.50.172](#) 已创建

步骤4 单击图 5-3 中的 IP，进入相关页面，可编辑主机基本信息，主机配置信息和主机账户信息。。

图5-4 主机编辑页面

主机配置

基本信息 | 主机配置 | 主机帐户 | 共享帐户

主机配置

- 状态
  - 禁用这台主机
- 会话选项
  - 开启会话二次审批
  - 开启会话备注
  - 开启历史会话审计
  - 开启实时会话监控
- RDP选项
  - 启用键盘记录
  - 允许打印机/驱动器映射
  - 允许使用剪贴板下载
  - 允许使用剪贴板上传
- SSH选项
  - 允许X11转发
  - 允许打开SFTP通道
  - 允许请求exec
  - 禁止文件上传
  - 禁止重命名
  - 禁止目录创建
  - 禁止目录删除
- FTP选项
  - 禁止文件上传
  - 禁止文件下载
  - 禁止文件删除
  - 禁止重命名
  - 禁止目录创建
  - 禁止目录删除
- 文件审计
  - 生成文件SHA1
  - 保存文件
    - 保存下载文件
    - 保存上传文件
    - 启用文件压缩
    - 不保存超过  KB 的文件
    - 单个会话保存的文件超过  MB 时停止保存

保存更改

 提示

主机配置选项与运维规则中协议控制都是相同的选项内容。当运维规则中的协议控制为启用状态

时，系统将忽略主机配置选项，否则系统将采用主机配置选项。

步骤5 单击<主机帐户/添加主机账户>，弹出新建主机帐户配置窗口；选择协议、登录模式、帐户和密码是否代填、验证是否连通。

图5-5 新建主机帐户页面示意图



步骤6 单击<共享帐户/关联共享账户>，弹出可以关联的共享账户列表（可选）。

图5-6 关联共享帐户页面示意图



复选框	名称	登录名	协议	认证类型
<input type="checkbox"/>	root	root	SSH	密码

步骤7 选择所要关联的共享账户，并单击”添加”按钮。

图5-7 添加关联共享帐户页面示意图



提示

步骤 6 和步骤 7 为可选项，有需要关联共享账户可关联，如无需要，可不配置

### 5.1.2 主机账户选项说明

表1-3 RDP 主机帐户选项说明

选项	描述
协议	SYSDEF代表运维人员可以选择任意协议对主机进行运维。
登录模式	自动登录和手工登录。
自动登录	将正确的主机账号和密码录入运维审计系统，运维人员以后就不需要输入帐户和密码即可成功登录到目标主机进行运维操作。
手动登录	无需设置主机的帐户和密码，留空即可；运维人员登录目标主机时需要输入主机的帐户和密码才能登录成功。
验证	如需验证主机的帐户和密码是否正确，请单击“验证”，提示“验证成功”代表帐户和密码正确；提示“验证失败”代表帐户或密码错误；提示“验证超时”代表网络或协议不通。

表1-4 ORACLE 主机选项说明

选项	描述
协议	SYSDEF代表运维人员可以选择任意协议对主机进行运维。
登录模式	自动登录和手工登录。
自动登录	将正确的主机账号和密码录入运维审计系统，运维人员以后就不需要输入帐户和密码即可成功登录到目标主机进行运维操作。
手动登录	无需设置主机的帐户和密码，留空即可；运维人员登录目标主机时需要输入主机的帐户和密码

	才能登录成功。
数据库	主机账户中的数据库。
登陆属性	SERVICENAME和SID。
验证	如需验证主机的账户和密码是否正确，请单击“验证”，提示“验证成功”代表帐户和密码正确；提示“验证失败”代表帐户或密码错误；提示“验证超时”代表网络或协议不通。

表1-5 SSH 主机帐户选项说明

选项	描述
协议	SYSDEF代表运维人员可以选择任意协议对主机进行运维。
登录模式	自动登录、自动登录(二次登录)和手工登录。
自动登录	将正确的主机账号和密码录入运维审计系统，运维人员以后就不需要输入帐户和密码即可成功登录到目标主机进行运维操作。
自动登录(二次登录)	用于管理2种帐户自动跳转登录，如交换机既有远程帐户又有enable命令；如果需要自动登录到enable权限下，就必须采用这种登录模式。
手动登录	无需设置主机的账户和密码，留空即可；运维人员登录目标主机时需要输入主机的帐户和密码才能登录成功。
验证	如需验证主机的账户和密码是否正确，请单击“验证”，提示“验证成功”代表帐户和密码正确；提示“验证失败”代表帐户或密码错误；提示“验证超时”代表网络或协议不通。

表1-6 TELNET 主机帐户选项说明

选项	描述
协议	SYSDEF代表运维人员可以选择任意协议对主机进行运维。
登录模式	自动登录、自动登录(二次登录)和手工登录。
自动登录	将正确的主机账号和密码录入运维审计系统，运维人员以后就不需要输入帐户和密码即可成功登录到目标主机进行运维操作。
自动登录(二次登录)	用于管理2种帐户自动跳转登录，如交换机既有远程帐户又有enable命令；如果需要自动登录到enable权限下，就必须采用这种登录模式。
手动登录	无需设置主机的账户和密码，留空即可；运维人员登录目标主机时需要输入主机的帐户和密码才能登录成功。
验证	如需验证主机的账户和密码是否正确，请单击“验证”，提示“验证成功”代表帐户和密码正确；提示“验证失败”代表帐户或密码错误；提示“验证超时”代表网络或协议不通。

表1-7 FTP 主机帐户选项说明

选项	描述
协议	SYSDEF代表运维人员可以选择任意协议对主机进行运维。
登录模式	自动登录和手工登录。
自动登录	将正确的主机账号和密码录入运维审计系统,运维人员以后就不需要输入帐户和密码即可成功登录到目标主机进行运维操作。
手动登录	无需设置主机的账户和密码,留空即可;运维人员登录目标主机时需要输入主机的帐户和密码才能登录成功。
验证	如需验证主机的账户和密码是否正确,请单击“验证”,提示“验证成功”代表帐户和密码正确;提示“验证失败”代表帐户或密码错误;提示“验证超时”代表网络或协议不通。

表1-8 SFTP 主机帐户选项说明

选项	描述
协议	SYSDEF代表运维人员可以选择任意协议对主机进行运维。
登录模式	自动登录和手工登录。
自动登录	将正确的主机账号和密码录入运维审计系统,运维人员以后就不需要输入帐户和密码即可成功登录到目标主机进行运维操作。
手动登录	无需设置主机的账户和密码,留空即可;运维人员登录目标主机时需要输入主机的帐户和密码才能登录成功。
验证	如需验证主机的账户和密码是否正确,请单击“验证”,提示“验证成功”代表帐户和密码正确;提示“验证失败”代表帐户或密码错误;提示“验证超时”代表网络或协议不通。

表1-9 VNC 主机帐户选项说明

选项	描述
协议	SYSDEF代表运维人员可以选择任意协议对主机进行运维。
登录模式	自动登录和手工登录。
自动登录	将正确的主机账号(X:帐户名)和密码录入运维审计系统,运维人员以后就不需要输入帐户和密码即可成功登录到目标主机进行运维操作。
手动登录	须设置帐户名称X:root(X表示桌面号,从0开始)、密码留空即可;运维人员登录目标主机时需要输入VNC主机的密码才能登录成功。

X:root	<p>表示VNC的帐户。如果VNC服务器只启用了5900端口，那就是0:root；如果VNC服务器同时启用了8个桌面号（即5901-5908），那就是1:root-8:root。</p> <p>如果主机是unix类平台，则帐户名称的格式为X:帐户名（X表示桌面号，从0开始）。</p> <p>如果主机是windows平台，则帐户名称的格式为X:root（X表示桌面号，从0开始），目前仅支持VNC服务端的“VNC password”模式。</p> <p>“X”是为了实现VNC服务会启动多个桌面，且用户之间互不干扰地使用各自的桌面；所以VNC服务使用的端口号与桌面号相关，VNC服务使用的端口从5900开始，例如桌面号是“:1”，则使用的端口是5901；桌面号是“:2”，则使用的端口是5902，依次类推；基于Java的VNC客户程序Web服务端从5800开始，它也与桌面号相关。</p>
验证	<p>如需验证主机的帐户和密码是否正确，请单击“验证”，提示“验证成功”代表帐户和密码正确；提示“验证失败”代表帐户或密码错误；提示“验证超时”代表网络或协议不通。</p>

表1-10 SQL SERVER 主机账户说明

选项	描述
协议	SYSDEF代表运维人员可以选择任意协议对主机进行运维。
登录模式	自动登录和手工登录。
自动登录	将正确的主机账号和密码录入运维审计系统，运维人员以后就不需要输入帐户和密码即可成功登录到目标主机进行运维操作。
手动登录	无需设置主机的帐户和密码，留空即可；运维人员登录目标主机时需要输入主机的帐户和密码才能登录成功。
验证	如需验证主机的帐户和密码是否正确，请单击“验证”，提示“验证成功”代表帐户和密码正确；提示“验证失败”代表帐户或密码错误；提示“验证超时”代表网络或协议不通。

表1-11 MYSQL 主机账户说明

选项	描述
协议	SYSDEF代表运维人员可以选择任意协议对主机进行运维。
登录模式	自动登录和手工登录。
自动登录	将正确的主机账号和密码录入运维审计系统，运维人员以后就不需要输入帐户和密码即可成功登录到目标主机进行运维操作。
手动登录	无需设置主机的帐户和密码，留空即可；运维人员登录目标主机时需要输入主机的帐户和密码才能登录成功。
验证	如需验证主机的帐户和密码是否正确，请单击“验证”，提示“验证成功”代表帐户和密码正确；提示“验证失败”代表帐户或密码错误；提示“验证超时”代表网络或协议不通。

表1-12 RLOGIN 主机账户说明

选项	描述
协议	SYSDEF代表运维人员可以选择任意协议对主机进行运维。
登录模式	自动登录和手工登录。
自动登录	将正确的主机账号和密码录入运维审计系统, 运维人员以后就不需要输入帐户和密码即可成功登录到目标主机进行运维操作。
手动登录	无需设置主机的账户和密码, 留空即可; 运维人员登录目标主机时需要输入主机的帐户和密码才能登录成功。
验证	如需验证主机的账户和密码是否正确, 请单击“验证”, 提示“验证成功”代表帐户和密码正确; 提示“验证失败”代表帐户或密码错误; 提示“验证超时”代表网络或协议不通。

表1-13 DB2 主机选项说明

选项	描述
协议	SYSDEF代表运维人员可以选择任意协议对主机进行运维。
登录模式	自动登录和手工登录。
自动登录	将正确的主机账号和密码录入运维审计系统, 运维人员以后就不需要输入帐户和密码即可成功登录到目标主机进行运维操作。
手动登录	须设置帐户名称50000:X (50000表示主机DB2协议默认端口号, X表示账户), 密码留空即可; 运维人员登录目标主机时需要输入正确的主机密码才能登录成功。
资产列表	主机账户中的数据库资产。资产列表中最多可填写3个参数, 每个参数长度不超过8字节, 用分号 ‘;’ 隔开
验证	如需验证主机的账户和密码是否正确, 请单击“验证”, 提示“验证成功”代表帐户和密码正确; 提示“验证失败”代表帐户或密码错误; 提示“验证超时”代表网络或协议不通。

### 5.1.3 导入主机

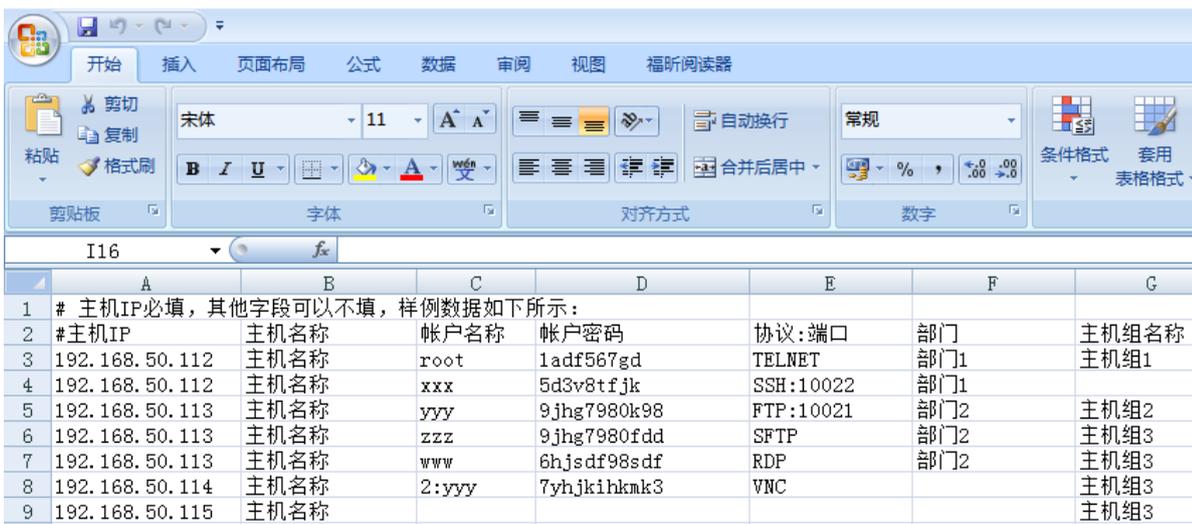
步骤1 进入[资产/主机管理]页面中, 在主机列表右下方单击[导入主机], 进入导入主机页面。

图5-8 导入主机页面示意图



步骤2 单击<下载模板文件>将文件下载至本地并解压，编辑并保存好文件中的主机表格。

图5-9 主机表格文件示意图



	A	B	C	D	E	F	G
1	#	# 主机IP必填，其他字段可以不填，样例数据如下所示：					
2	#主机IP	主机名称	帐户名称	帐户密码	协议:端口	部门	主机组名称
3	192.168.50.112	主机名称	root	1adf567gd	TELNET	部门1	主机组1
4	192.168.50.112	主机名称	xxx	5d3v8tfjk	SSH:10022	部门1	
5	192.168.50.113	主机名称	yyy	9jhg7980k98	FTP:10021	部门2	主机组2
6	192.168.50.113	主机名称	zzz	9jhg7980fdd	SFTP	部门2	主机组3
7	192.168.50.113	主机名称	www	6hjsdf98sdf	RDP	部门2	主机组3
8	192.168.50.114	主机名称	2:yyy	7yhjkihkmk3	VNC		主机组3
9	192.168.50.115	主机名称					主机组3

 说明

第一列为主机IP（必填项）、第二列为主机名称、第三列为账户名称，第四列为账户密码，第五列为协议及端口号，第六列为部门，第七列为主机组名称。网络协议的格式为“协议:端口号”（中间用英文的冒号隔开），如“SSH:22”；如果存在多个协议及端口号，就如“TELNET:23,FTP:21”（中间用英文的逗号隔开）。

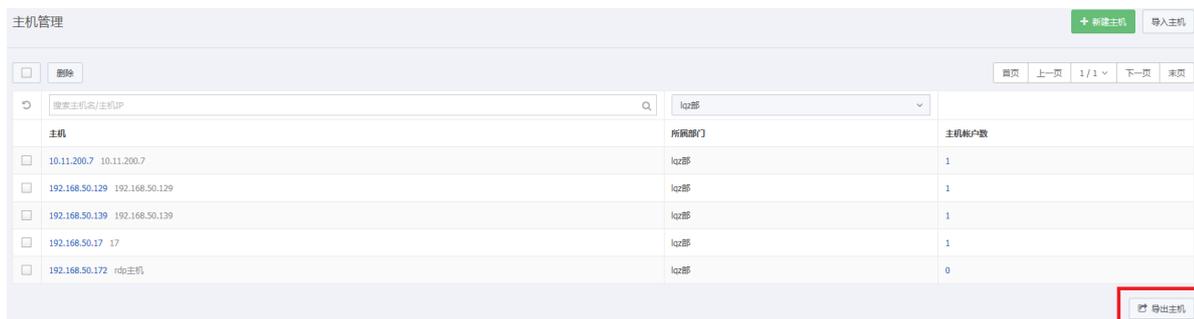
步骤3 单击<上传文件>后，在弹出的打开文件对话框中选择要导入的主机文件进行导入。

步骤4 单击<导入主机>后即可导入成功。

### 5.1.4 导出主机

步骤1 进入[资产/主机管理]页面中，单击页面右下角的<导出主机>即可完成导出。

图5-10 主机管理页面示意图



### 5.1.5 删除主机

步骤1 进入[资产/主机管理]页面中。勾选需要删除的主机。

步骤2 单击删除即可删除成功。

### 5.1.6 禁用主机

步骤1 进入[资产/主机管理]页面中。单击需要禁用的主机，进入主机编辑页面。

步骤2 在<主机配置>中勾选“禁用这台主机”，单击“保存更改”即可。

### 5.1.7 启用主机

步骤1 进入[资产/主机管理]页面中。单击需要启用的主机，进入主机编辑页面。

步骤2 在<主机配置>中不再勾选“禁用这台主机”，单击“保存更改”即可。

### 5.1.8 搜索主机

搜索主机与搜索用户的方法类似，可通过主机 IP 或主机名称进行搜索，也可根据部门进行过滤。

### 5.1.9 编辑主机

步骤1 进入[资产/主机管理]页面中。

步骤2 单击主机的 IP 地址，进入编辑页面。

图5-11 主机编辑页面示意图

## 主机信息

基本信息
主机配置
主机帐户

### 主机信息

所属部门

主机IP\*

主机名称

备注

保存更改

### 协议端口配置

RDP

SSH

TELNET

VNC

SFTP

FTP

SQL Server

MySQL

Oracle

Rlogin

保存更改

步骤3 在基本信息中编辑主机信息即协议端口，编辑完成单击“保存更改”。

步骤4 单击“主机配置”，进行详细配置。

图5-12 主机详细配置示意图



表1-14 主机配置选项说明

选项	功能	解释
会话选项	开启会话二次审批	表示需要对该主机进行审核后方可登录。
	开启会话备注	表示需要写明登录主机的原因或目的才可登录。

	开启历史会话审计	表示对运维会话进行审计。
	开启实时会话监控	表示管理员可以对主机进行实时监控。
	开启命令审批	表示对linux/unix类的主机执行某些命令时，需要得到管理员同意后才可执行成功。
RDP选项	启用键盘记录	表示记录RDP主机的键盘符操作记录。
	允许打印机/驱动器映射	在运维RDP主机时，可以映射本地打印和本地磁盘。
	允许使用剪切板	表示运维RDP主机时，可以使用复制-粘贴功能。
SSH选项	允许X11转发	表示在运维时可以通过SSH方式转发X11协议。
	允许打开SFTP通道	表示在运维时可以使用SSH的客户工具直接打开SFTP协议。
	允许请求exec	表示可以直接使用exec指令。
	禁止文件上传	表示可以禁止通过sftp、scp、rsync命令进行文件上传
	禁止重命名	表示可以禁止通过sftp进行重命名操作
	禁止目录创建	表示可以禁止通过sftp进行目录创建操作
	禁止目录删除	表示可以禁止通过sftp进行目录删除操作
FTP选项	禁止文件上传	表示禁止通过FTP登录后进行上传文件操作
	禁止文件下载	表示禁止通过FTP登录后进行下载文件操作
	禁止文件删除	表示禁止通过FTP登录后进行删除文件操作
	禁止重命名	表示禁止通过FTP登录后进行重命名操作
	禁止目录上传	表示禁止通过FTP登录后进行删除文件操作
	禁止目录下载	表示禁止通过FTP登录后进行删除文件操作
文件传输	生成文件sha1签名	表示可以对SFTP/FTP传输的文件进行sha1签名，确保文件的唯一性与不重复。
	保存文件	表示可以对SFTP/FTP传输的文件进行保存在运维审计系统中。
	保存下载文件	表示可以保存下载的文件。
	保存上传文件	表示可以保存上传的文件。
	启用文件压缩	表示可以对传输的文件进行压缩。
	不保存超过多少KB的文件	表示可以根据单个文件的大小进行保存。
	单个会话保存的文件总大小超过多少MB时停止保存	表示可以控制单个会话保存的文件大小。

- 步骤5 编辑完成后单击“保存更改”。
- 步骤6 单击<主机账户>进入账户编辑页面。
- 步骤7 单击需要编辑的账户名称，在弹出的选项卡中进行编辑。

图5-13 主机账户编辑对话框

新建主机帐户
×

---

协议	SFTP	▼
登录模式	自动登录	▼
帐户类型	普通帐户	▼
主机帐户	lqz	×
<input type="checkbox"/> 特权帐户 <input type="checkbox"/> 使用特权帐户改密		
密码		验证

---

创建主机帐户

 提示

账户类型分为普通账户和特殊账户，普通账户是非匿名的，特殊账户是匿名的。

<特权账户>被勾选后表明该账户是一个特权账户，拥有改密权限。

<使用特权账户改密>被勾选后，系统会自动寻找具有改密权限的特权账户进行改密计划。

具体可参照《自动改密配置举例》。

- 步骤8 编辑完成后单击<保存>即可。

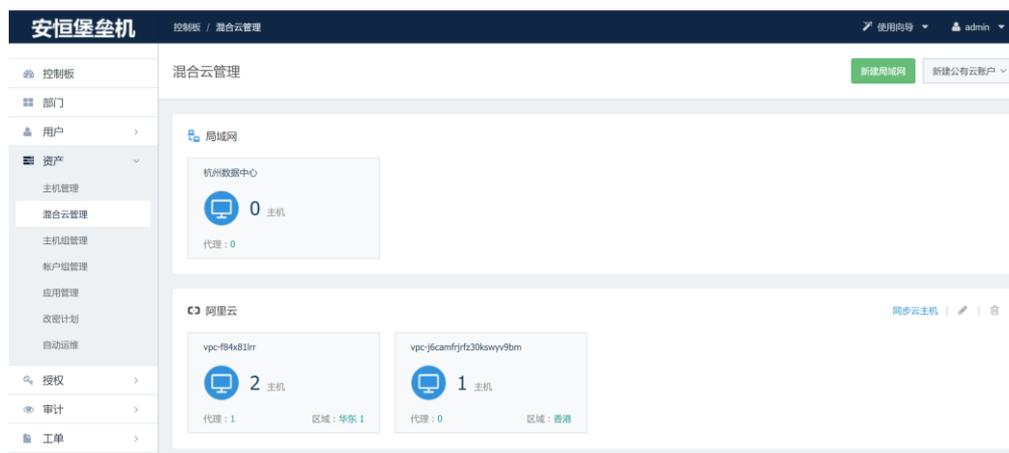
## 5.2 混合云管理

混合云管理是用于对不同数据中心，云上服务器使用代理服务器运维的模式。

## 5.2.1 新建局域网

步骤1 进入[资产/混合云管理]页面中。

图5-14 混合云管理页面示意图



步骤2 单击<新建局域网>进入配置页面，编辑局域网名称。

图5-15 新建局域网示意图



步骤3 单击<创建局域网 >，系统会提示主机网络创建成功。

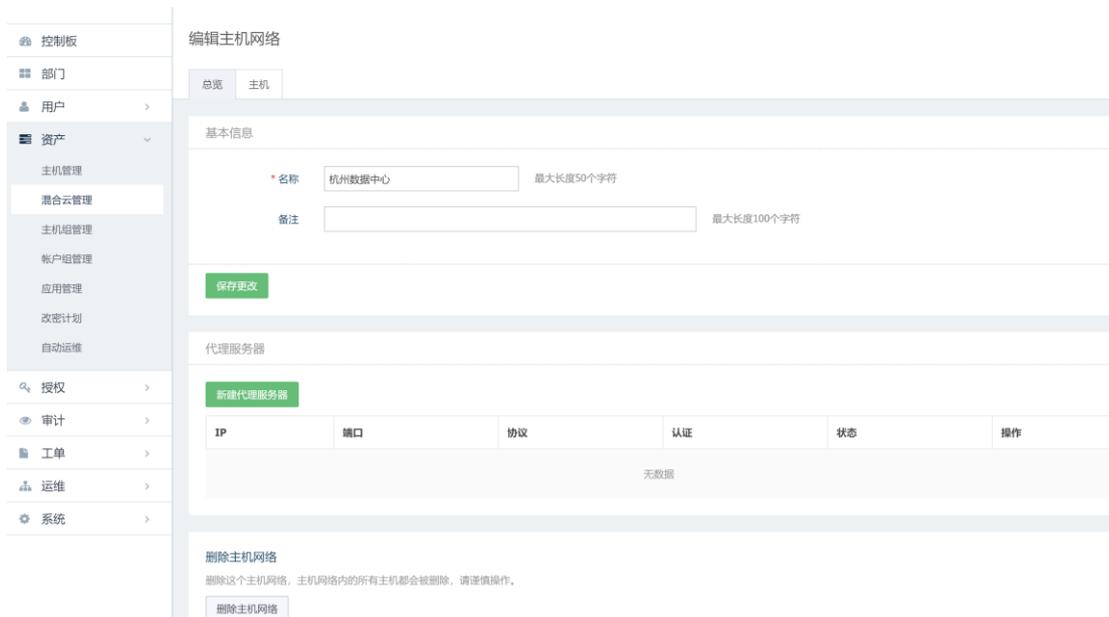
图5-16 局域网创建成功提示



## 5.2.2 新建代理服务器

步骤1 进入[资产/混合云管理]页面中，单击进入某个局域网

图5-17 编辑主机网络示意图



步骤2 单击<新建代理服务器>进入配置页面，编辑代理协议、服务器地址、端口、用户名及密码。

图5-18 编辑代理服务器示意图



步骤3 单击<新建代理服务器>，系统会提示代理服务器创建成功。

图5-19 代理服务器创建成功提示



### 5.2.3 添加主机

步骤1 进入[资产/混合云管理]页面中，单击进入某个局域网，选择<主机>标签。

图5-20 添加主机界面示意图



步骤2 单击<添加主机>，编辑主机 IP，主机名称，所属部分等信息

图5-21 添加主机信息界面示意图

新建主机



步骤3 单击<创建主机>，系统会提示主机创建成功

## 5.2.4 新建公有云账户

目前支持添加阿里云账号下的服务器。

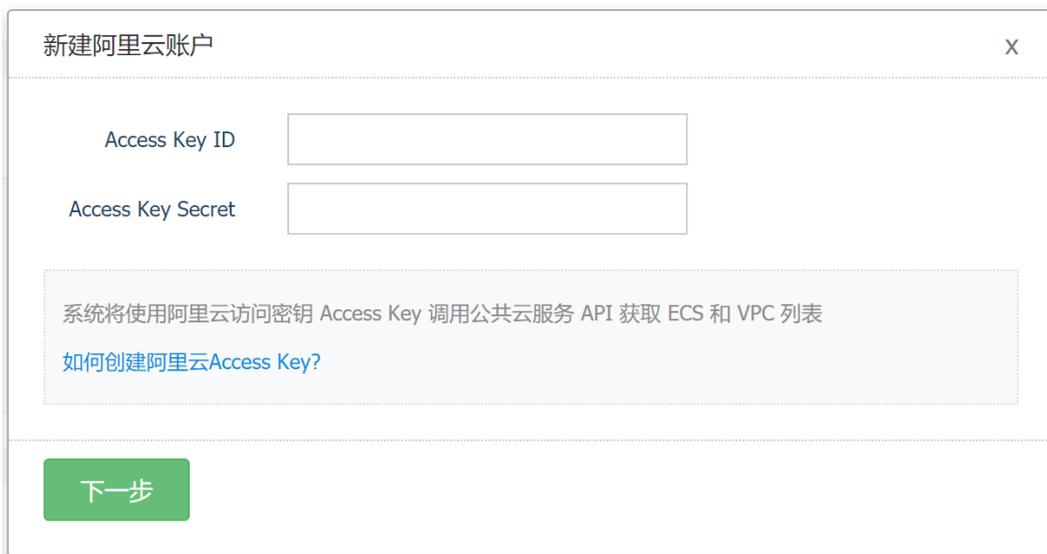
步骤1 进入[资产/混合云管理]页面中，单击<新建公有云账户><阿里云>。

图5-22 阿里云账号添加



步骤2 添加阿里云 Access Key

图5-23 Access Key 添加



步骤3 单击<下一步>，完成阿里云服务器添加导入

图5-24 阿里云服务器添加示意图



步骤4 代理服务器配置与局域网操作步骤相同

## 5.3 共享账户

共享账户是当多个主机的管理帐户的登录名、密码/密钥相同时，通过关联共享帐户可以节约配置时间。

### 5.3.1 新建共享账户

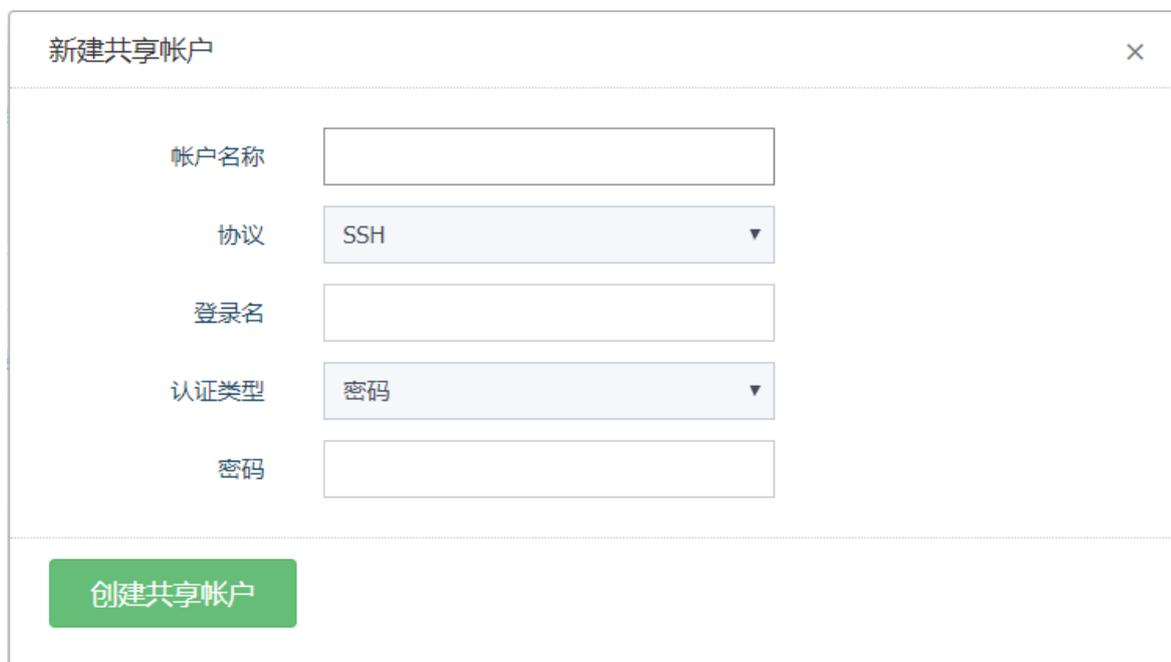
步骤1 进入[资产/共享账户]页面中。

图5-25 共享账户页面示意图



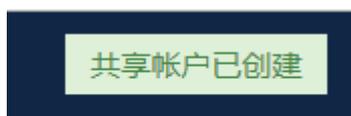
步骤2 单击<新建共享账户>进入配置页面，编辑共享账户信息。

图5-26 新建共享账户示意图



步骤3 单击<创建共享账户 >，系统会提示共享账户已创建。

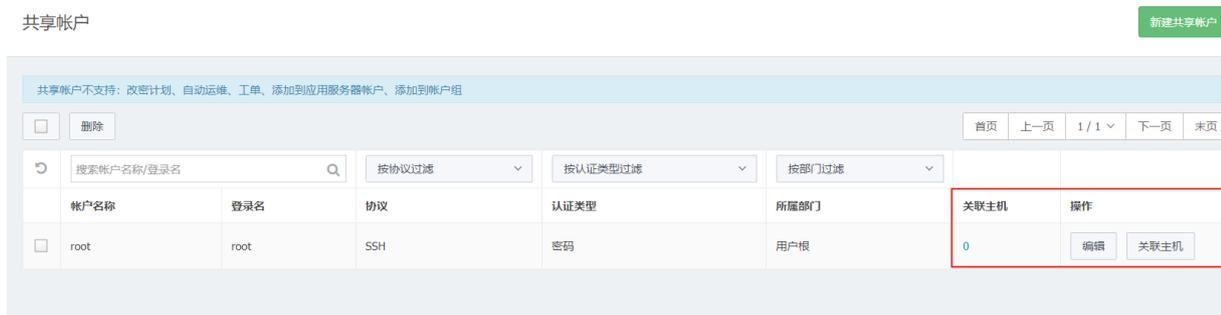
图5-27 共享账户创建成功提示



## 5.3.2 关联主机

步骤1 进入[资产/共享账户]页面中，单击共享账户设置关联主机

图5-28 共享账户示意图



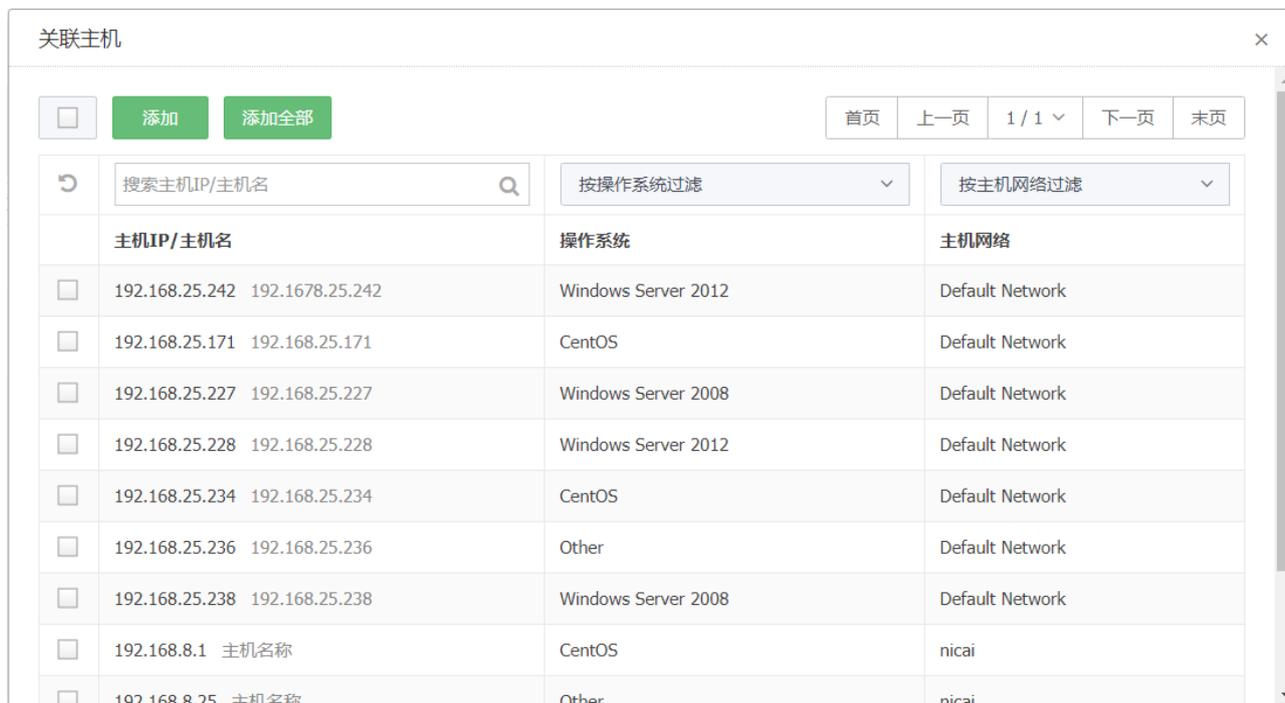
步骤2 单击<关联主机>进入关联页面。

图5-29 关联主机示意图



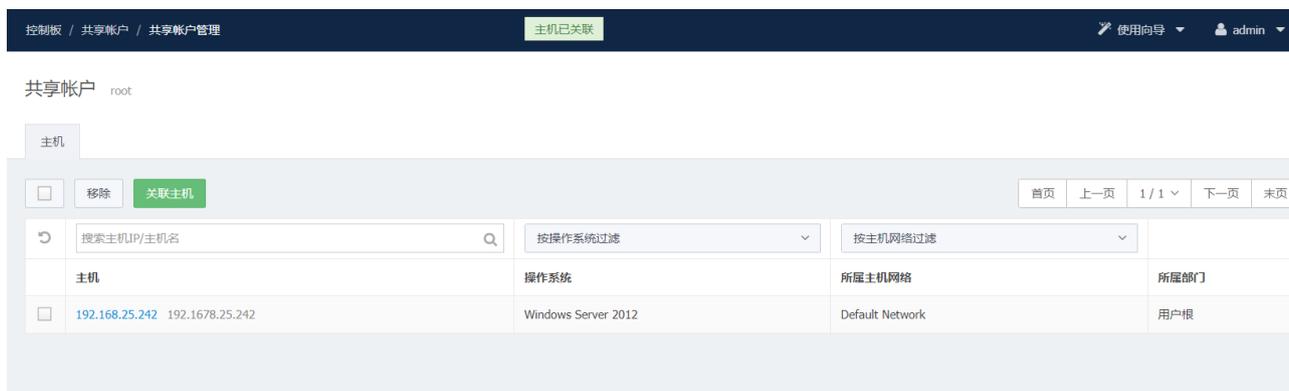
步骤3 单击<关联主机>，选择所要关联的主机。

图5-30 添加关联账户



步骤4 在选择主机后，系统会提示主机已关联。

图5-31 关联主机界面示意图



步骤5 共享账户页面查看关联账户

图5-32 共享账户界面示意图



## 5.4 帐户组管理

帐户组用于对主机帐户的分组，方便在授权的时候进行账户批量授权。

### 5.4.1 新建帐户组

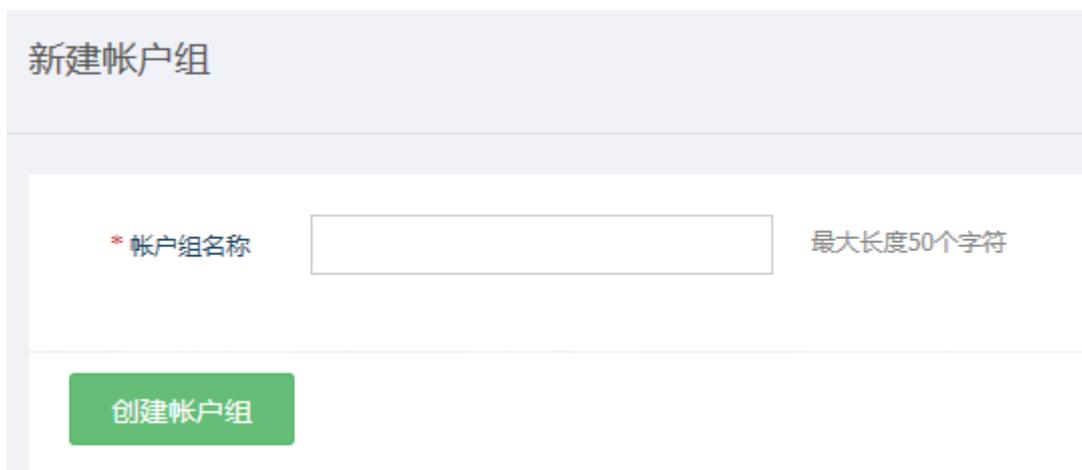
步骤1 进入[资产/帐户管理]页面中。

图5-33 帐户组管理页面示意图



步骤2 单击<新建帐户组>进入配置页面，编辑帐户组名称。

图5-34 新建帐户组示意图



新建帐户组

\* 帐户组名称  最大长度50个字符

创建帐户组

步骤3 单击<创建账户组 >，系统会提示账户组创建成功。

图5-35 账户组创建成功提示

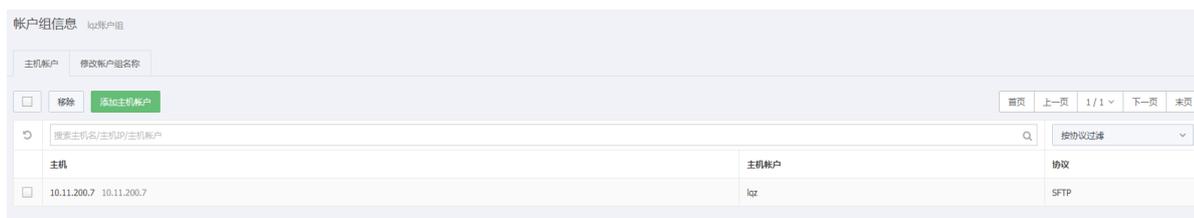


步骤4 单击账户组名称，进入账户组编辑页面，参照 5.2.2 进行编辑即可。

### 5.4.2 编辑账户组

步骤1 在<资产/账户组管理>页面中单击需要编辑的账户组名称，进入账户组编辑页面。

图5-36 账户组编辑页面



帐户组信息 kqz帐户组

主机账户 修改帐户组名称

删除 添加主机账户

搜索主机名/主机IP/主机账户

主机	主机账户	协议
<input type="checkbox"/> 10.11.200.7 10.11.200.7	kqz	SFTP

分页: 首页 上一页 1/1 下一页 末页

步骤2 在<主机账户>选项页面添加或删除账户组成员。

步骤3 在<修改账户组名称>选项页面可编辑账户组名，完成后单击<保存更改>即可。

### 5.4.3 删除帐户组

步骤1 进入[资产/账户管理]页面中，勾选需要删除的主机帐户组。

步骤2 单击<删除>即可将帐户组删除掉。

### 5.4.4 搜索帐户组

与搜索用户方法相似，可以通过账户组名称进行搜索，也可以通过部门进行过滤。

## 5.5 应用管理

用于兼容 windows server 2008 的 remoteAPP 的应用发布管理。

### 5.5.1 添加应用服务器

步骤1 进入[资产/应用管理]页面

图5-37 应用托管管理页面示意图

应用列表	应用服务器																																																							
<table border="1"> <thead> <tr> <th>应用图标</th> <th>名称</th> <th>运行参数</th> <th>应用服务器帐户</th> <th>操作</th> </tr> </thead> <tbody> <tr> <td></td> <td>DASUSM</td> <td></td> <td>qa@win2008</td> <td>编辑 复制</td> </tr> <tr> <td></td> <td>IE</td> <td></td> <td>qa@win2008</td> <td>编辑 复制</td> </tr> <tr> <td></td> <td>Mozilla Firefox</td> <td></td> <td>qa@win2008</td> <td>编辑 复制</td> </tr> <tr> <td></td> <td>Windows PowerShell</td> <td></td> <td>HH.COM\administrator@RD-server</td> <td>编辑 复制</td> </tr> <tr> <td></td> <td>fgdf</td> <td></td> <td>HH.COM\administrator@RD-server</td> <td>编辑 复制</td> </tr> <tr> <td></td> <td>web信息</td> <td></td> <td></td> <td>编辑 复制</td> </tr> <tr> <td></td> <td>写字板</td> <td></td> <td>HH.COM\administrator@RD-server</td> <td>编辑 复制</td> </tr> <tr> <td></td> <td>画图</td> <td></td> <td>qa@win2008</td> <td>编辑 复制</td> </tr> <tr> <td></td> <td>画图</td> <td></td> <td>HH.COM\administrator@RD-server</td> <td>编辑 复制</td> </tr> <tr> <td></td> <td>计算器</td> <td></td> <td>qa@win2008</td> <td>编辑 复制</td> </tr> </tbody> </table>	应用图标	名称	运行参数	应用服务器帐户	操作		DASUSM		qa@win2008	编辑 复制		IE		qa@win2008	编辑 复制		Mozilla Firefox		qa@win2008	编辑 复制		Windows PowerShell		HH.COM\administrator@RD-server	编辑 复制		fgdf		HH.COM\administrator@RD-server	编辑 复制		web信息			编辑 复制		写字板		HH.COM\administrator@RD-server	编辑 复制		画图		qa@win2008	编辑 复制		画图		HH.COM\administrator@RD-server	编辑 复制		计算器		qa@win2008	编辑 复制	
应用图标	名称	运行参数	应用服务器帐户	操作																																																				
	DASUSM		qa@win2008	编辑 复制																																																				
	IE		qa@win2008	编辑 复制																																																				
	Mozilla Firefox		qa@win2008	编辑 复制																																																				
	Windows PowerShell		HH.COM\administrator@RD-server	编辑 复制																																																				
	fgdf		HH.COM\administrator@RD-server	编辑 复制																																																				
	web信息			编辑 复制																																																				
	写字板		HH.COM\administrator@RD-server	编辑 复制																																																				
	画图		qa@win2008	编辑 复制																																																				
	画图		HH.COM\administrator@RD-server	编辑 复制																																																				
	计算器		qa@win2008	编辑 复制																																																				

步骤2 单击上图中的<应用服务器>选项，进入应用服务器管理页面。

图5-38 应用服务器管理页面

主机	应用	主机帐号	操作
RD-server [10.11.32.50]	5	1	删除
centos-149 [192.168.50.149]	1	3	删除
win2008 [192.168.50.246]	5	2	删除

步骤3 在应用服务器管理页面中可添加或删除应用服务器。

### 5.5.2 添加应用

步骤1 进入[资产/应用管理]页面中。

步骤2 单击<新建应用/新建应用>进入配置页面。选择应用服务器的帐户、填写相关参数、更改图标，在应用类型中可以选择不同类型的應用。

图5-39 添加应用示意图

新建应用

要使用此功能，请先将 [应用加载器](#) 安装到应用服务器，并部署为一个RemoteApp应用程序

应用服务器帐户

应用名称

应用类型

---

应用路径  例：C:\Windows\System32\cmd.exe

运行参数

目标地址  替换运行参数中的%Target

登录帐户  替换运行参数中的%Username

登录密码  替换运行参数中的>Password

图标 

步骤3 单击<创建应用>即可。

图5-40 应用类型示意图

- IE代填
- Oracle工具**
  - sqlplus
  - sqlplusw
  - plsqldev
  - toad
- SQLserver工具**
  - SQL server management studio
  - sqlcmd
- MySQL工具**
  - mysql
  - MySQLAdministrator
  - MySQLQueryBrowser
- 虚拟化工具**
  - vsphere client
- 自定义**

 提示

应用服务器配置详情请参见《应用服务器（RemoteApp）配置手册》。

### 5.5.3 添加 IE 代填应用

步骤1 单击<新建应用>，应用类型选择“IE 代填”，然后编辑：应用名称、应用服务器的 IP、应用服务器的帐户、目标 URL、目标帐户和密码。

图5-41 添加 IE 代填应用示意图

#### 新建应用

要使用此功能，请先将 [应用加载器](#) 安装到应用服务器，并部署为一个RemoteApp应用程序

应用服务器帐户	<input type="text" value="qa@win2008"/>	<input type="button" value="v"/>
应用名称	<input type="text"/>	
应用类型	<input type="text" value="IE代填"/>	
-----		
目标地址	<input type="text"/>	
登录帐户	<input type="text"/>	目标地址的登录帐户
登录密码	<input type="text"/>	目标地址的登录密码
-----		
<input type="button" value="创建应用"/>		

步骤2 单击<创建应用>即可新建成功。

### 5.5.4 添加数据库类应用

步骤1 单击<新建应用>，在应用类型中选择数据库类应用，进入新建数据库应用页面填写应用名称、数据库的 IP、数据库名称，数据库帐户、数据库密码。

图5-42 新建应用页面示意图

### 新建应用

要使用此功能，请先将 [应用加载器](#) 安装到应用服务器，并部署为一个RemoteApp应用程序

应用服务器帐户:

应用名称:

应用类型:

应用路径:  例: C:\oracle\product\10.1.0\client\_1\BIN\sqlplus.exe

数据库IP:

数据库名:

数据库帐户:

数据库密码:

图标: 

步骤2 单击<创建应用>即可新建成功。

### 5.5.5 删除应用

步骤1 进入[资产/应用托管]页面中，勾选需要删除的应用。

步骤2 单击<删除>即可删除成功。

### 5.5.6 搜索应用

与用户搜索类似，可以通过应用名称进行搜索，也可以根据应用服务器账户进行过滤。

### 5.5.7 编辑应用

步骤1 单击需要编辑的应用条目后面的<编辑按钮>，进入配置页面。编辑应用名称、应用服务器、URL、帐户、密码等。

步骤2 单击<保存更改 >后即可修改成功。

### 5.5.8 导出应用

步骤1 单击应用主界面右下方的<导出应用>按钮。

图5-43 导出应用示意图

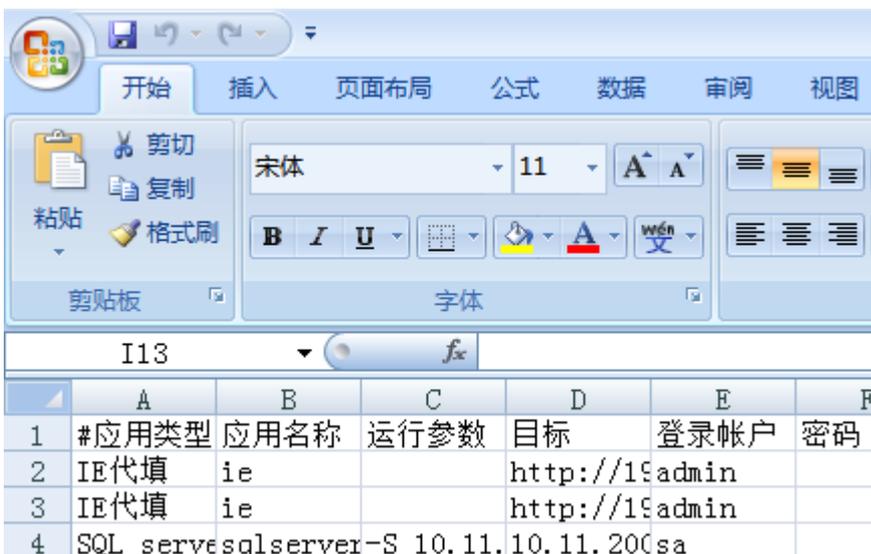


步骤2 在弹出的导出应用对话框中填写压缩文件密码，并单击导出应用按钮即可。

图5-44 导出应用对话框



图5-45 应用导出表格文件示意图



# 6 授权

明御®运维审计与风险控制系统（DAS-USM）的授权管理包括运维授权和策略管理两部分内容。运维授权是指将某部分主机账户的运维权限赋予某部分用户。策略管理是对主机的访问策略管理。

## 6.1 运维授权

6.1.1 运维授权关系类型主要有：

- (1) 账户组授权给用户组；
- (2) 单个主机账户授权给用户组；
- (3) 被托管的应用授权给用户组；
- (4) 账户组授权给单个用户；
- (5) 单个主机账户授权给单个用户；
- (6) 被托管的应用授权给单个用户；

单击<授权/运维授权>进入运维授权主界面。

图6-1 运维授权主页面



### 6.1.2 新建运维授权

以下以“基于用户授权主机账户”为例：

步骤1 进入[授权/运维规则]页面中，单击<新建运维规则>按钮，进入新建运维授权页面。

图6-2 新建运维规则页面

新建运维规则

\* 规则名称  最大长度50个字符

规则有效期  -  不限制运维规则的有效期请留空

备注

---

用户

删除

请添加用户

资产

删除

请添加资产

步骤2 在“新建运维规则”中，单击<添加用户/用户>进入选择用户列表页面。

图6-3 选择用户页面

选择用户

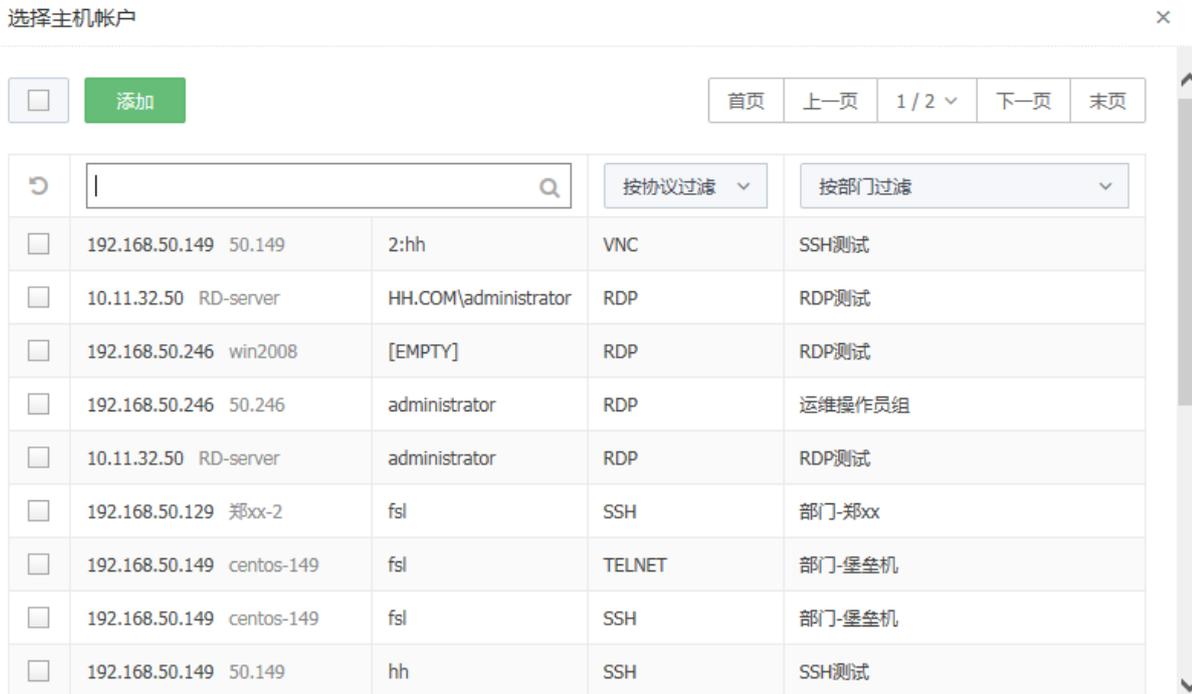
添加

首页 上一页 1 / 1 下一页 末页

<input type="checkbox"/>	admin	用户根	超级管理员
<input type="checkbox"/>	hehe hehe	运维测试	部门管理员
<input type="checkbox"/>	lqzadmin lqzadmin	lqz部	部门管理员
<input type="checkbox"/>	lqzyunwei lqzyunwei	lqz部	运维员
<input type="checkbox"/>	opencm opencTM	opencTM	部门管理员
<input type="checkbox"/>	operator operator	用户根	部门管理员
<input type="checkbox"/>	test test	lqz部	运维员
<input type="checkbox"/>	xlx_operator adf	运维操作员组	运维员
<input type="checkbox"/>	zheng1_dept zhengxx	部门-郑xx	部门管理员

步骤3 在“新建运维规则”中，单击<添加资产/主机账户>进入选择主机账户列表页面。

图6-4 选择主机账户页面



步骤4 选择好用户和资产之后，可以单击<创建运维规则>即可授权成功。

步骤5 也可以在运维规则中，设置有效期、备注、策略。

图6-5 授权有效期示意图

规则有效期  -  不限制运维规则的有效期请留空

备注

步骤6 配置完成后单击<创建运维授权>按钮即可。

### 6.1.3 编辑运维规则

步骤1 在“运维规则”页面中，编辑相应的规则。

图6-6 编辑规则页面示意图

总览 用户/资产 登录限制 命令控制 协议控制

\* 规则名称  最大长度50个字符

规则有效期  -  不限制运维规则的有效期限请留空

备注

状态  禁用这条运维规则

步骤2 可以修改“用户”与“资产”之间的关系。

图6-7 用户/资产编辑页面

总览 用户/资产 登录限制 命令控制 协议控制

用户

删除

<input type="checkbox"/>	用户	operator
--------------------------	----	----------

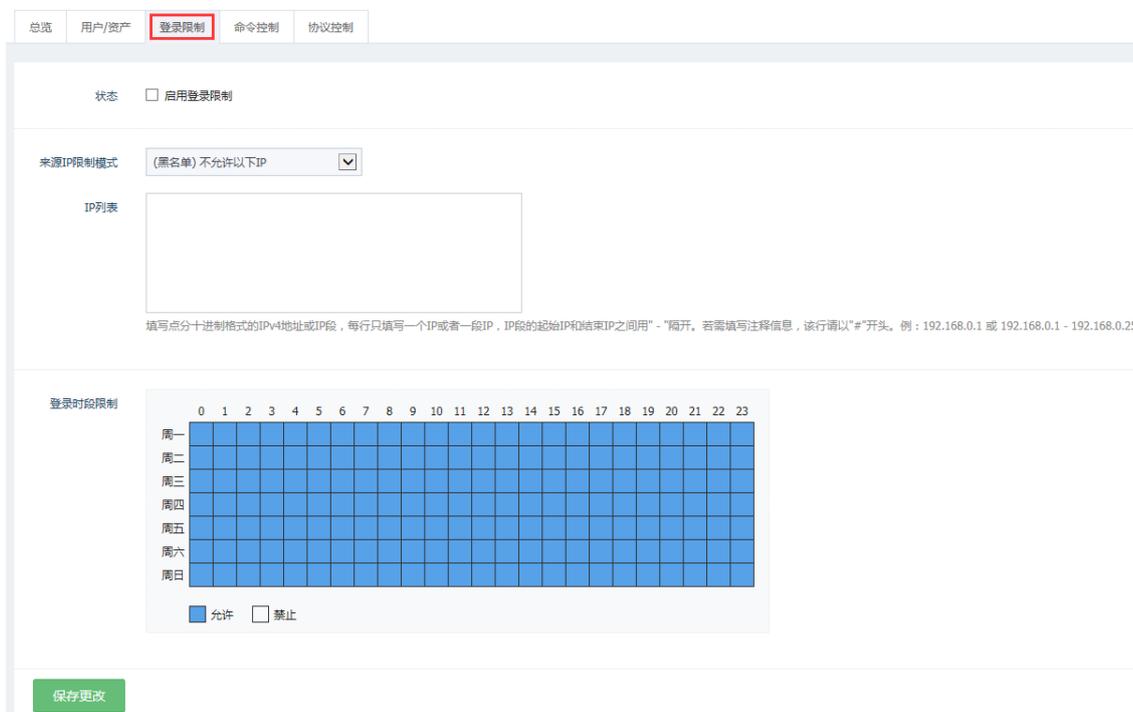
资产

删除

<input type="checkbox"/>	帐户	[SQL Server] sa@10.11.32.60
<input type="checkbox"/>	帐户	[SQL Server] sa@10.11.32.60

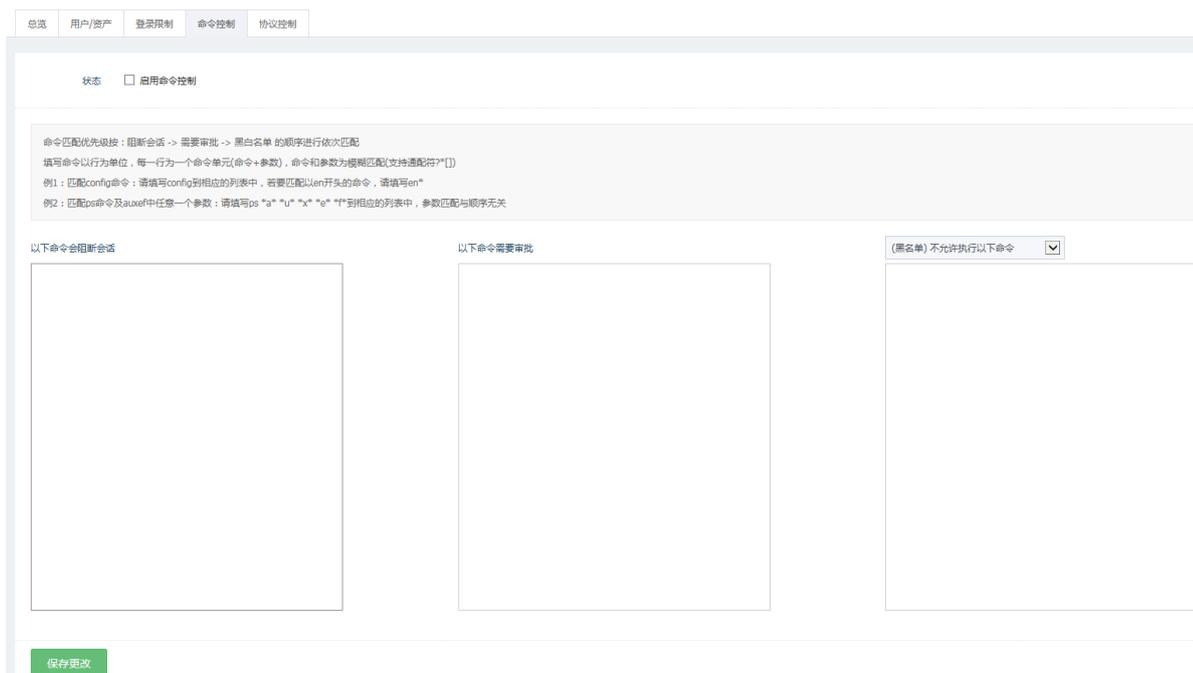
步骤3 在登录限制页面中，可编辑源 IP 的黑白名单列表及登录时段限制。

图6-8 登录限制编辑界面



步骤4 在“命令控制”页面中，可以启用命令控制、命令阻断，命令审批和命令黑白名单功能。

图6-9 命令控制编辑界面



步骤5 在“协议控制”页面中，可以配置各个协议会话中的相关控制选项。

图6-10 协议控制页面

状态  启用协议控制

---

会话选项

- 开启会话二次审批
- 开启会话备注
- 开启历史会话审计
- 开启实时会话监控

RDP选项

- 启用键盘记录
- 允许打印机/驱动器映射
- 允许使用剪贴板下载
- 允许使用剪贴板上传

SSH选项

- 允许X11转发
- 允许打开SFTP通道
- 允许请求exec
- 禁止文件上传
- 禁止文件下载
- 禁止文件删除
- 禁止重命名
- 禁止目录创建
- 禁止目录删除

FTP选项

- 禁止文件上传
- 禁止文件下载
- 禁止文件删除
- 禁止重命名
- 禁止目录创建
- 禁止目录删除

文件审计

- 生成文件SHA1
- 保存文件

- 保存下载文件
- 保存上传文件
- 启用文件压缩
- 不保存超过  KB 的文件
- 单个会话保存的文件超过  MB 时停止保存

保存更改

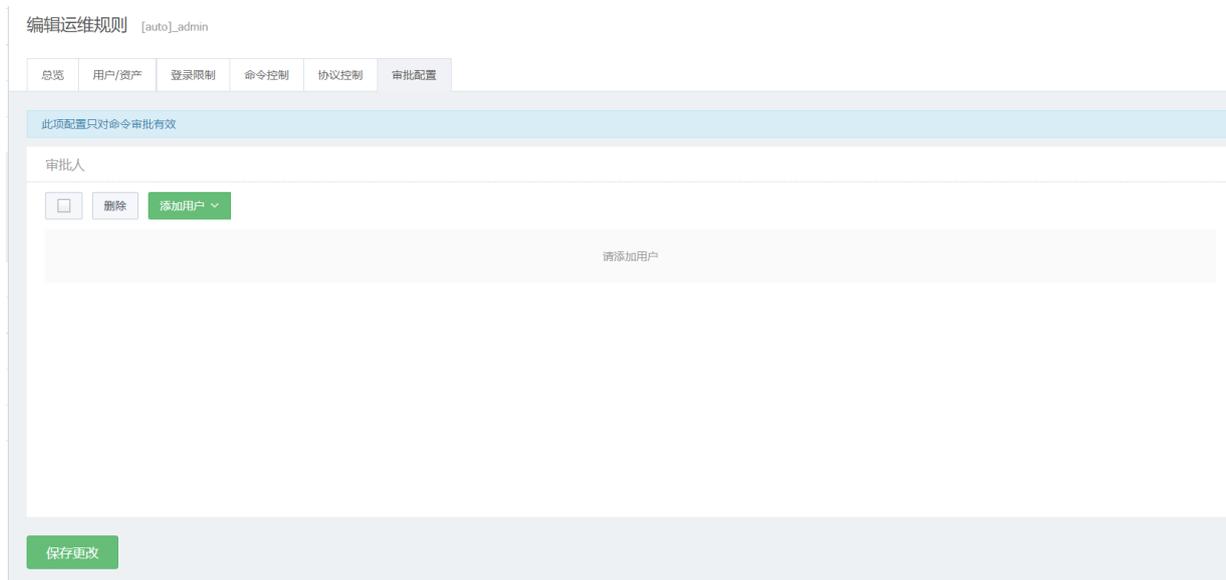
### 6.1.4 删除、禁用或启用运维规则

在运维授权主界面勾选相应的运维规则，可以单击<删除>、<禁用>或 <启用>即可。

### 6.1.5 审批配置

在编辑运维规则界面，设置某用户对该运维规则审计配置，此项配置只对命令审批有效。

图6-11 协议控制页面



### 6.1.6 查看运维规则

为了快速定位授权关系，明御®运维审计与风险控制系统（DAS-USM）提供了按用户名、主机账户、账户组和应用进行模糊搜索的功能，同时还提供了按用户类型、资产类型、IP 范围限制和部门进行过滤的功能，方便用户快速查找授权关系。

## 6.2 未授权登录审核

未授权审核是指对那些未授权主机-用户关系对进行授权与否的操作，授权后，该主机将在对应用户的主机运维列表中显示，该用户运维该主机时无需再输入主机信息。

### 6.2.1 授权审核条目

所谓授权审核，是指对未授权登录的用户-主机关系进行审核，决定授权与否。

步骤1 进入[授权/授权审核]页面。

未授权登录审核

状态	用户	主机	协议	主机账户	最近登录时间	授权时间	授权人
<input type="checkbox"/> 未授权	hehe hehe	10.11.0.222	RDP	root	2016-05-23 11:14:40		
<input type="checkbox"/> 已授权	openctm openctm	10.11.32.30	FTP	hh	2016-05-23 11:08:18	2016-05-23 11:10:31	bbq
<input type="checkbox"/> 已授权	MSQOperator MSQOperator	10.11.32.60	RDP	administrator	2016-05-23 10:57:23	2016-05-23 10:57:34	admin
<input type="checkbox"/> 已授权	MSQOperator MSQOperator	10.11.32.60	SQL Server	sa	2016-05-23 10:55:27	2016-05-23 10:56:08	admin
<input type="checkbox"/> 未授权	openctm	10.11.32.30	FTP	hh	2016-05-23 10:49:05		
<input type="checkbox"/> 未授权	openctm	10.11.33.200	RDP	openctm	2016-05-23 10:34:20		
<input type="checkbox"/> 未授权	admin	10.11.33.99	RDP	root	2016-05-23 10:13:52		
<input type="checkbox"/> 未授权	admin	10.11.32.30	SFTP	root	2016-05-23 10:11:59		
<input type="checkbox"/> 未授权	admin	10.11.32.30	TELNET	hh	2016-05-23 10:09:01		
<input type="checkbox"/> 未授权	openctm	10.11.33.66	SFTP	hax	2016-05-23 10:04:09		
<input type="checkbox"/> 未授权	openctm	10.11.33.99	SSH	openctm	2016-05-23 10:03:39		
<input type="checkbox"/> 未授权	openctm	10.11.33.99	FTP	hax	2016-05-23 10:01:39		
<input type="checkbox"/> 未授权	openctm	192.168.50.246	VNC		2016-05-23 09:56:36		
<input type="checkbox"/> 未授权	openctm	10.11.33.99	SSH	openctm	2016-05-23 09:53:03		

步骤2 勾选相应的未授权条目，单击<授权>按钮即可。

## 6.2.2 删除审核条目

勾选相应条目，单击<删除>按钮即可。

## 6.2.3 搜索审核条目

可以输入主机名、用户名或主机账户进行模糊搜索，也可以根据协议和授权状态进行过滤。

# 7 审计

审计用于审计运维人员对主机的访问操作的日志。

## 7.1 会话审计

会话审计用于记录运维人员对主机操作过程的会话日志。

### 7.1.1 查看所有会话

步骤1 进入[审计/会话审计]页面。可以查看到字符、图形、文件、应用类型的会话审计日志。

图7-1 所有会话页面示意图

类型	主机	协议/主机帐号	用户/来源IP	起始时间	会话时长/会话大小	部门	操作
图形	10.11.32.50 RD-server	RDP administrator	hehe 192.168.50.246	2015-07-01 16:43:41 2015-07-01 16:44:15	34秒 569KB	RDP测试	播放 下载 详情
字符	192.168.50.139 50.139	SSH huanghai	hehe 192.168.50.246	2015-07-01 16:42:40 2015-07-01 16:42:57	17秒 12KB	SSH测试	播放 下载 详情
图形	10.11.32.50 RD-server	RDP administrator	hehe 10.11.32.217	2015-07-01 16:31:11 2015-07-01 16:32:05	54秒 703KB	RDP测试	播放 下载 详情
图形	10.11.32.50 RD-server	RDP administrator	hehe 192.168.50.246	2015-07-01 16:26:42 2015-07-01 16:26:58	16秒 364KB	RDP测试	播放 下载 详情
图形	192.168.50.191 vista	RDP suku	hehe 10.11.32.217	2015-07-01 16:16:30 2015-07-01 16:20:43	4分13秒 4.33MB	RDP测试	播放 下载 详情
图形	10.11.32.50 RD-server	RDP HH.COM\administrator	hehe 192.168.50.203	2015-07-01 16:15:24 2015-07-01 16:15:24	0秒 52KB	RDP测试	播放 下载 详情
图形	192.168.50.191 vista	RDP suku	hehe 192.168.50.203	2015-07-01 16:14:38 2015-07-01 16:14:58	20秒 539KB	RDP测试	播放 下载 详情
图形	192.168.50.190 windows7.1	RDP ga	hehe 192.168.50.203	2015-07-01 16:09:07 2015-07-01 16:09:26	19秒 1.03MB	RDP测试	播放 下载 详情
图形	10.11.33.200 xp200	RDP root	hehe 192.168.50.203	2015-07-01 16:08:46 2015-07-01 16:08:59	13秒 181KB	RDP测试	播放 下载 详情
图形	10.11.32.50 RD-server	RDP HH.COM\administrator	hehe 192.168.50.203	2015-07-01 16:04:18 2015-07-01 16:04:19	1秒 57KB	RDP测试	播放 下载 详情

步骤2 单击会话审计页面中的<详情>后弹出相应会话详情。可以查看到详细的会话信息。

图7-2 会话详情示意图

会话详情			
会话ID	caaa10ee5593a83d000000292f00000f		
时长	34秒	大小	569KB
开始时间	2015-07-01 16:43:41	结束时间	2015-07-01 16:44:15
用户	hehe	来源IP	192.168.50.246
来源MAC	00:50:56:8F:00:04	来源端口	50430
主机名称	RD-server	主机IP	10.11.32.50
主机帐户	administrator	协议	RDP
主机MAC	F4:EA:67:87:03:E7	主机端口	3389
会话备注			
审批人	-	操作	播放 下载

步骤3 单击关闭按钮后即可返回管理页面。

步骤4 单击会话审计页面中的<下载>后，即可下载会话文件，可通过离线播放器查看。



说明

“离线播放器”，请参在工具下载页面中下载安装至本地使用。

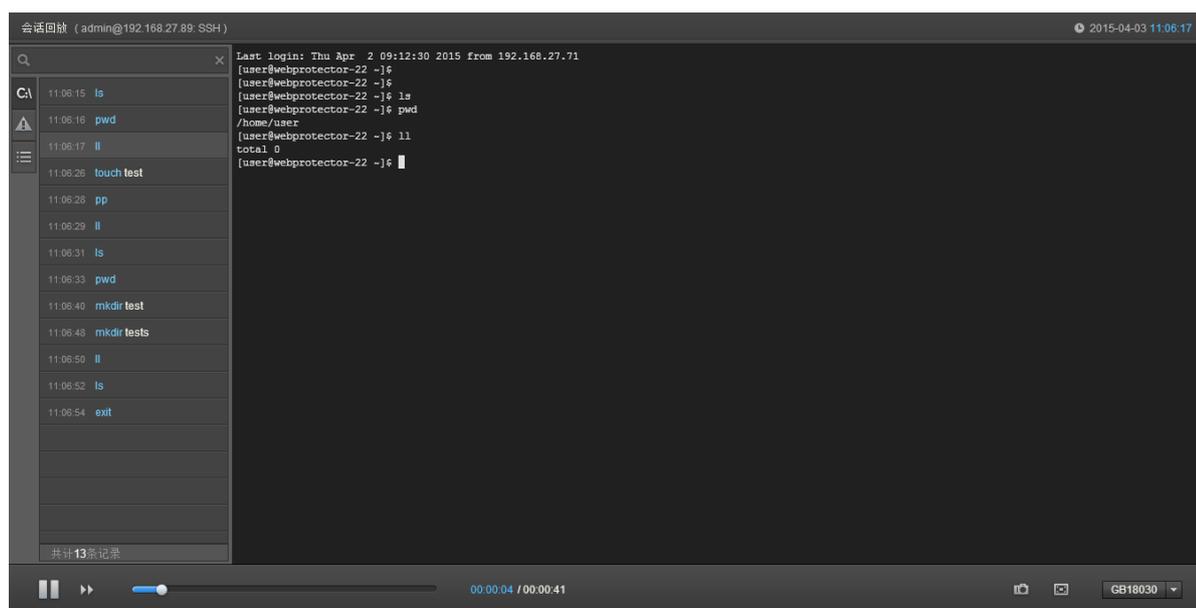
步骤5 单击会话审计页面中的<播放>后，即可通过 web 方式查看会话审计。可以查看日志回放、命令记录、搜索等。



说明

Web方式查看会话审计，须在本地安装flash player才可播放。如果未安装flash player，请工具下载页面中下载安装至本地使用。

图7-3 会话审计在线播放示意图



步骤6 查看完之后，关闭 web 页面即可。

## 7.1.2 搜索审计会话

步骤1 进入[审计/会话审计/所有会话]页面中。

步骤2 单击<展开更多搜索条件>。可组合条件搜索。

图7-4 会话审计搜索条件示意图

协议  时间  -   
 部门   
 主机   
 主机帐户   
 用户   
 来源IP   
 备注

步骤3 单击<搜索>后即可搜索成功。

### 7.1.3 查看应用会话

步骤1 进入[审计/会话审计/应用会话]页面。可以查看到应用的名称、来源信息、操作时长等。

图7-5 应用会话页面示意图

应用	主机	主机帐户	用户	起始时间	会话时长/会话大小	操作
Windows PowerShell	RD-server 10.11.32.50	administrator RDP	hehe 10.11.33.200	2015-07-01 10:51:35 2015-07-01 10:52:22	47秒 217KB	<a href="#">播放</a> <a href="#">下载</a> <a href="#">详情</a>
浏览器	win2008 192.168.50.246	qa RDP	hehe 10.11.33.200	2015-07-01 10:51:07 2015-07-01 10:52:36	1分29秒 3.02MB	<a href="#">播放</a> <a href="#">下载</a> <a href="#">详情</a>
IE	win2008 192.168.50.246	qa RDP	hehe 10.11.33.200	2015-07-01 10:49:22 2015-07-01 10:51:22	2分0秒 2.87MB	<a href="#">播放</a> <a href="#">下载</a> <a href="#">详情</a>
IE	win2008 192.168.50.246	qa RDP	hehe 10.11.33.99	2015-06-30 11:44:01 2015-06-30 11:45:48	1分47秒 1.76MB	<a href="#">播放</a> <a href="#">下载</a> <a href="#">详情</a>
IE	win2008 192.168.50.246	qa RDP	hehe 10.11.33.99	2015-06-29 17:35:30 2015-06-29 17:37:02	1分32秒 2MB	<a href="#">播放</a> <a href="#">下载</a> <a href="#">详情</a>
IE	win2008 192.168.50.246	qa RDP	hehe 10.11.33.99	2015-06-29 17:33:39 2015-06-29 17:35:31	1分52秒 4.58MB	<a href="#">播放</a> <a href="#">下载</a> <a href="#">详情</a>
计算器	RD-server 10.11.32.50	administrator RDP	hehe 10.11.32.217	2015-06-29 12:49:57 2015-06-29 12:52:20	2分23秒 263KB	<a href="#">播放</a> <a href="#">下载</a> <a href="#">详情</a>
浏览器	win2008 192.168.50.246	qa RDP	hehe 10.11.32.217	2015-06-29 12:49:48 2015-06-29 12:52:30	2分43秒 2.5MB	<a href="#">播放</a> <a href="#">下载</a> <a href="#">详情</a>

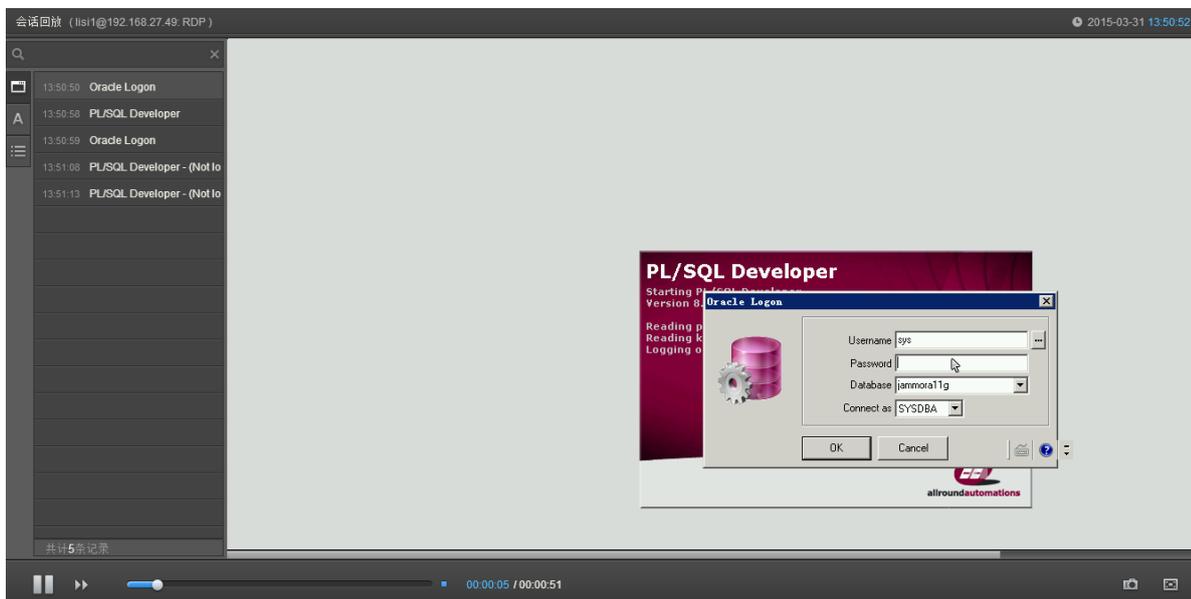
步骤2 单击应用会话页面中的<详情>后，弹出会话详情。可以查看到详细的会话信息。

步骤3 单击关闭按钮后即可返回管理页面。

步骤4 单击应用会话页面中的<下载>后，即可下载会话文件，可通过离线播放器查看。

步骤5 单击会话审计页面中的<播放>后，即可通过 web 方式查看会话审计。可以查看日志回放、文字记录、搜索等。

图7-6 在线查看审计日志示意图



步骤6 查看完之后，关闭 web 页面即可。

### 7.1.4 搜索应用会话

步骤1 进入[审计/会话审计/应用会话]页面中，其余操作与搜索所有会话相同。

### 7.1.5 查询事件

步骤1 进入[审计/会话审计/事件查询]页面中。

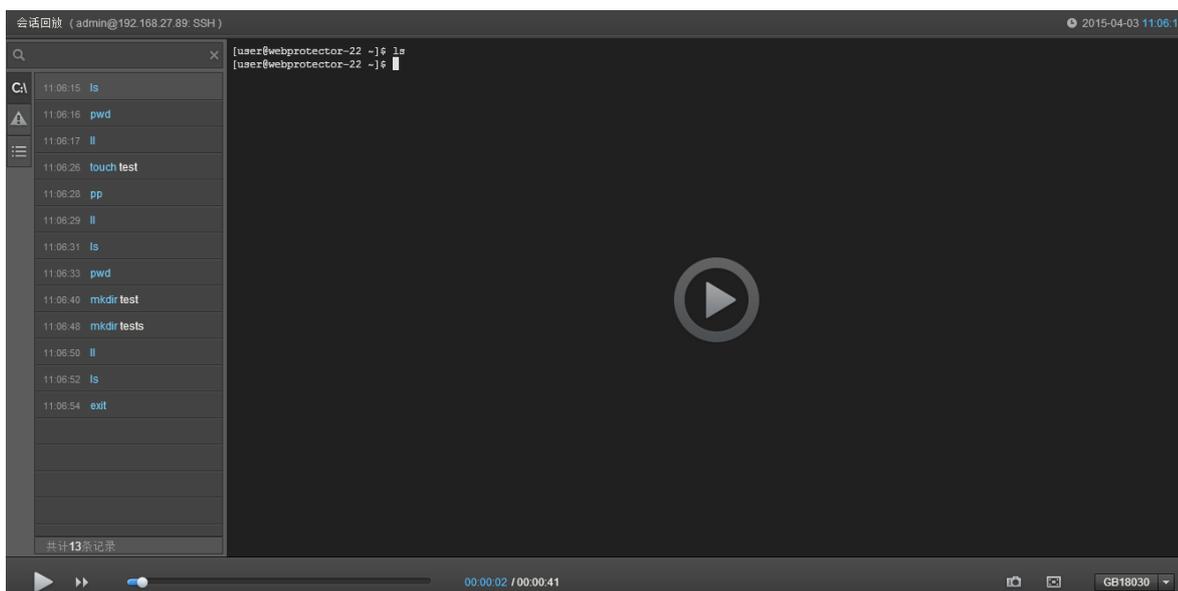
图7-7 时间查询页面示意图

会话审计					
所有会话 应用会话 事件查询					
类型: 所有类型 时间: [ ] - [ ]					
[搜索] [展开更多搜索条件]					
时间	主机	用户	类型	内容	会话操作
2015-07-01 09:10:47	192.168.50.191	hehe	上传文件	Mtscc6.0.6001.18000.zip	详情 播放
2015-07-01 09:11:31	192.168.50.191	hehe	上传保存	ocr.txt	详情 播放
2015-07-01 09:37:12	192.168.50.241	hehe	图形文字	会话审计 -WindowsInternetExplorer	详情 播放
2015-07-01 09:37:13	192.168.50.241	hehe	图形文字	会话审计 -WindowsInternetExplorer	详情 播放
2015-07-01 09:37:21	192.168.50.241	hehe	图形文字	会话审计 -WindowsInternetExplorer	详情 播放
2015-07-01 09:37:28	192.168.50.241	hehe	上传保存	ocr.txt	详情 播放
2015-07-01 09:40:10	192.168.50.191	hehe	上传保存	ocr.txt	详情 播放
2015-07-01 09:41:46	10.11.0.222	hehe	上传文件	keyboard.txt	详情 播放
2015-07-01 09:41:46	10.11.0.222	hehe	上传文件	ocr.txt	详情 播放
2015-07-01 10:01:44	192.168.50.139	hehe	字符命令	[huangha@centos139 ~]\$ ls	详情 播放
2015-07-01 10:02:17	192.168.50.139	hehe	字符命令	[huangha@centos139 ~]\$ ls	详情 播放

步骤2 单击<详情>, 弹出窗口。可以查看会话的详细信息。

步骤3 单击<播放>即可通过 web 方式开始播放会话审计。

图7-8 在线播放审计日志示意图



步骤4 查看完之后, 关闭 web 页面即可。

### 7.1.6 搜索事件

步骤1 进入[审计/会话审计/事件查询]页面中。

步骤2 单击<展开更多搜索条件>按钮。可组合条件搜索。

图7-9 搜索条件示意图



## 7.2 审计规则

审计规则是创建审计员与主机之间的对应关系, 代表某审计员具有审计某主机的权限。进入[审计/审计规则]页面。

图7-10 审计规则管理页面

审计规则			+ 新建审计规则
<input type="checkbox"/> 删除			首页 上一页 1/1 下一页 末页
<input type="text" value="搜索审计规则名称"/>	<input type="text" value="搜索审计员"/>	<input type="text" value="搜索主机"/>	
名称	审计员	主机	
<input type="checkbox"/> 2015-06-20	2	20	
<input type="checkbox"/> 2015-06-20	2	20	
<input type="checkbox"/> dddd	2	2	

### 7.2.2 添加审计规则

步骤1 在审计规则主页面单击“新建审计规则”进入相关页面。

图7-11 新建审计规则页面

#### 新建审计规则

创建审计规则是创建 审计员 与 主机 之间的对应关系，代表左边列表中的审计员有权审计右边列表中的主机。

审计规则

名称

审计员

删除 添加审计员

主机

删除 添加主机

步骤2 添加审计员，在弹出的对话框中选择审计员进行添加。

图7-12 添加审计员对话框

选择用户 ×

添加
 
 首页 上一页 1/1 下一页 末页

按部门过滤

<input type="checkbox"/>	lqzshenji lqzshenji	lqz部	审计员
--------------------------	---------------------	------	-----

步骤3 添加被审计的主机，在弹出的对话框中选择主机进行添加。

图7-13 添加主机对话框



步骤4 最后单击<创建审计规则>即可完成创建。



说明  
审计规则作用的用户对象的角色只能是审计员。

## 8 工单

### 8.1 新建工单

步骤1 进入[工单/我的工单]页面。

图8-1 我的工单列表示意图



步骤2 单击<新建工单>，进入新建工单页面。

图8-2 新建工单页面

新建工单

申请资产

其他选项

授权有效期  -

备注

步骤3 单击<选择资产>，选择主机账户或应用。

图8-3 资产选择对话框

选择主机帐户 ×

<input type="checkbox"/>	10.11.32.30 10.11.32.30		FTP	BBQ
<input type="checkbox"/>	192.168.50.149 50.149	2:hh	VNC	运维测试部
<input type="checkbox"/>	10.11.33.99 Windows10	admin	RDP	RDP
<input type="checkbox"/>	10.11.32.60 Windows2008	administrator	RDP	RDP
<input type="checkbox"/>	192.168.50.150 Windows2012	administrator	RDP	RDP
<input type="checkbox"/>	192.168.50.246 win2008-server	administrator	RDP	运维测试部

步骤4 单击<添加>后，在“我的工单”页面会显示添加的主机，此时工单处于待审批的状态。

图8-4 工单条目

工单号	备注	申请时间/审批时间	状态	详情
5			待审批	详情
4		2016-06-20 10:31:27	已取消	详情

步骤5 勾选相应的工单条目，单击“取消”可取消新建的工单申请。

## 8.2 工单审批

步骤1 进入[工单/工单审批]页面

图8-5 工单审批页面

工单审批

工单号	申请人	所属部门	申请时间/审批时间	状态	详情
5	admin aaaadddd	用户组	2016-06-20 10:32:20	待审批	详情
4	admin aaaadddd	用户组	2016-06-20 10:31:10 2016-06-20 10:31:27	已取消	详情
2	OT 运维员	用户组	2016-06-01 10:28:19 2016-06-01 10:28:42	已批准	详情

步骤2 勾选工单申请条目，单击<批准>，此时申请人可以在<运维>界面登录申请的主机。

# 9 运维

运维用于运维人员登录主机时的功能管理。

## 9.1 工具下载

工具下载用于运维人员在登录主机前的下载需要用到的运维工具。

### 9.1.1 单点登录器

步骤1 单击页面右上方用户菜单中的<工具下载>下载页面。

步骤2 下载“单点登录器”并安装在本地。



单点登录器是用于web方式调用运维客户端工具时，须安装的登录工具。

### 9.1.2 IE 代填工具

- 步骤1 进入[运维/工具下载]页面中。
  - 步骤2 下载“IE 代填工具”。
  - 步骤3 上传至应用服务器中，并安装好。
- 



IE代填工具用于发布IE代填应用时的辅助工具。

---

### 9.1.3 USBKEY 控件(IE)

- 步骤1 进入[运维/工具下载]页面中。
  - 步骤2 下载“USBKEY 控件”并安装在本地。
- 



USBKEY控件用于运维审计系统启用USBKEY认证方式时的登录工具。

---

### 9.1.4 离线播放器与 Adobe AIR

- 步骤1 进入[运维/工具下载]页面中。
  - 步骤2 下载“离线播放器”与“Adobe ATR”，并安装在本地。
- 



离线播放器与Adobe ATR是用于会话审计里的日志导出后进行离线查看的工具。

---

### 9.1.5 Flash Player

- 步骤1 进入[运维/工具下载]页面中。
  - 步骤2 下载“Flash Player”，并安装在本地。
- 



Flash Player用于通过web方式查看会话审计的日志。

---

### 9.1.6 字符客户端

步骤1 进入[运维/工具下载]页面中。

步骤2 下载支持 SSH 和 telnet 协议的客户端工具，并安装在本地。

---



客户端工具用于连接SSH、telnet协议的主机

---

### 9.1.7 图形客户端

步骤1 进入[运维/工具下载]页面中。

步骤2 下载支持 RDP 和 VNC 协议的客户端工具，并安装在本地。

---



图形客户端工具用于连接windows服务器、VNC服务器

---

### 9.1.8 文件传输客户端

步骤1 进入[运维/工具下载]页面中。

步骤2 下载支持 SFTP 和 FTP 协议的客户端工具，并安装在本地。

---



文件传输客户端工具用于连接SFTP/FTP服务器。

---

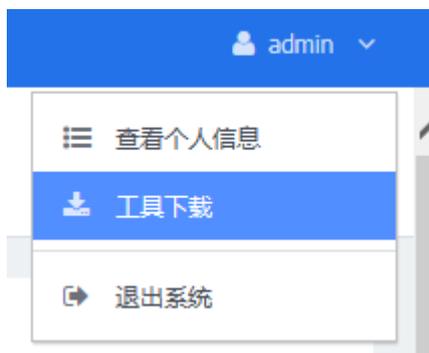
## 9.2 主机运维

主机运维用于运维人员登录主机的 web 页面。

### 9.2.1 单点登录配置

步骤1 在系统页面的右上角单击用户名，在下拉菜单中单击<工具下载>进入工具下载页面。

图9-1 用户下拉菜单



步骤2 选择单点登录器，进行下载。

图9-2 工具下载页面

### 工具下载

运维及审计工具	
名称	下载
 <b>单点登录器</b> 运维登录必备工具	本地下载
 应用加载器 应用中心IE表单自动代填必备工具	本地下载
 USBKEY控件 (IE) USBKEY必备工具	本地下载
 离线播放器 播放下载到本地的会话数据	本地下载
 Adobe AIR 4.0 离线播放器运行环境	本地下载 MD5:66214913c51c9f7589e8fe3bcf66b05f
 Flash Player 12 Flash播放器	本地下载 (IE浏览器版本) MD5:b165fd256a586cdcc2237b6f03e5a8bd 本地下载 (其他浏览器版本) MD5:16a84718fb300915e3c7ca7ea271eddc

步骤3 安装单点登录器。

步骤4 配置各协议的单点登录所用客户端。

图9-3 单点登录配置示意图



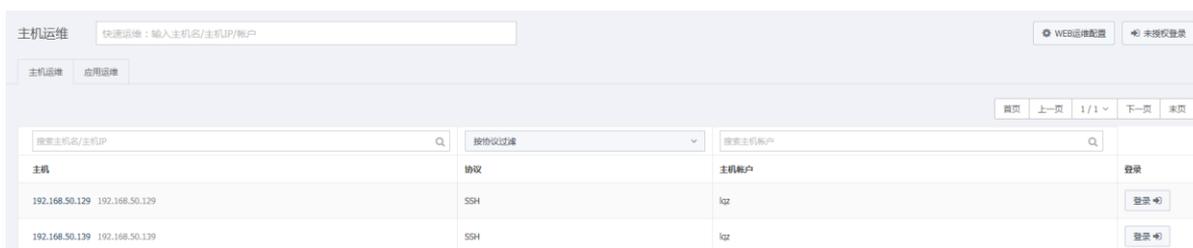
步骤5 配置完成后退出即可。

## 9.2.2 全局配置

### 1. 配置 RDP 参数

步骤1 进入[运维/主机运维]页面。

图9-4 主机运维页面示意图



步骤2 单击右上角<WEB 运维配置>，默认进入 RDP 配置页面。设置分辨率、连接模式、本地设备和资源、本地驱动。

图9-5 WEB 运维配置页面示意图



步骤3 单击<应用>即可生效。

## 2. 配置 SSH 参数

步骤1 单击<SSH>，进入配置页面。选择客户端程序、终端类型、编码格式。

图9-6 全局登录配置页面示意图

Web运维配置
×

RDP	客户端程序	PutTY <input type="button" value="v"/>
SSH	终端类型	默认 <input type="button" value="v"/>
TELNET	编码	默认 <input type="button" value="v"/>
FTP	请确认您已经安装了所选客户端程序	
SFTP		
VNC		
SQL Server		

步骤2 单击<应用>后，即可生效。

### 3. 配置 telnet 参数

步骤1 单击<TELNET>，进入配置页面。

图9-7 全局登录配置页面示意图



步骤2 单击<应用>后生效。

#### 4. 配置 FTP 参数

步骤1 单击<FTP>，进入配置页面。

步骤2 选择对应的客户端程序。

步骤3 单击<确定>后生效。

#### 5. 配置 SFTP 参数

与 FTP 参数配置类似。

#### 6. 配置 VNC 参数

与 FTP 参数配置类似。

#### 7. 配置 SQLSERVER 参数

与 FTP 参数配置类似。

### 9.2.3 主机登录

在主机运维列表中，单击相应主机条目的<登录>，会自动弹出配置好的客户端，登录主机进行操作。

## 9.2.4 快速搜索

步骤1 进入[运维/主机运维]页面。

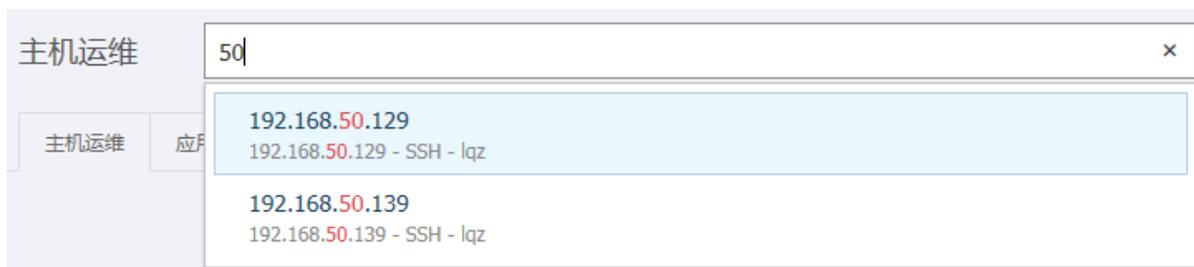
图9-8 主机运维搜索框示意图

主机运维

输入主机IP/主机名/帐户名

步骤2 在搜索框中输入主机 IP/主机名/账户名、或关键信息，系统会自动过滤出与目标主机有关的信息。

图9-9 主机搜索成功示意图



步骤3 单击需要登录的目标主机及帐户后，即可成功登录。

## 9.2.5 查看主机

通过主机名称或主机 IP 实现模糊搜索，也可通过主机协议进行过滤，以此达到快速定位的目的。

## 9.2.6 重复 IP 合并

主机运维中的重复 IP 合并即将相应主机 IP 地址的不同主机账户全部整合在相应主机 IP 地址下，方便查看。

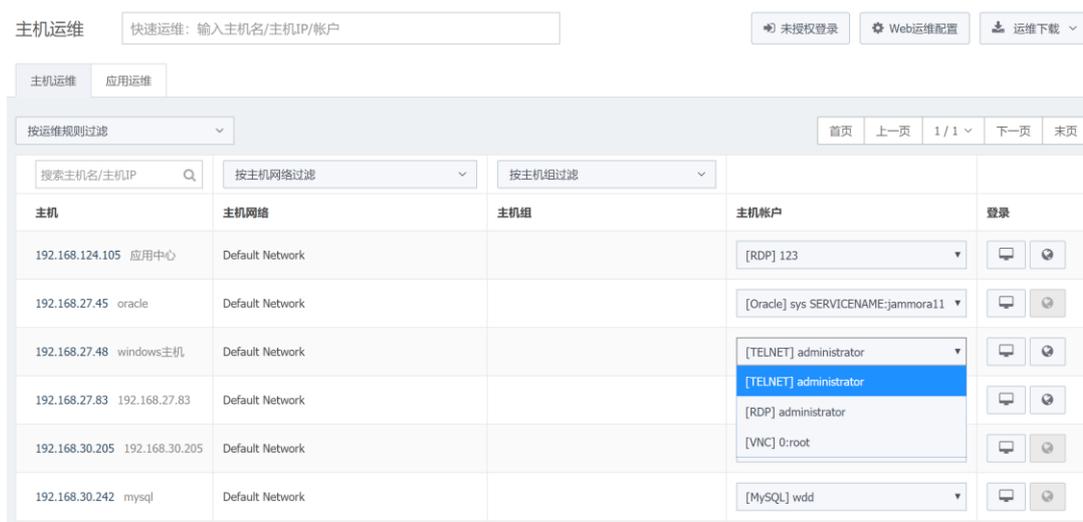
步骤1 单击<运维>下的<主机运维>

图9-10 打开主机运维界面



步骤2 单击主机 IP 地址对应的<主机帐户>即可查看

图9-11 重复 IP 合并示意图

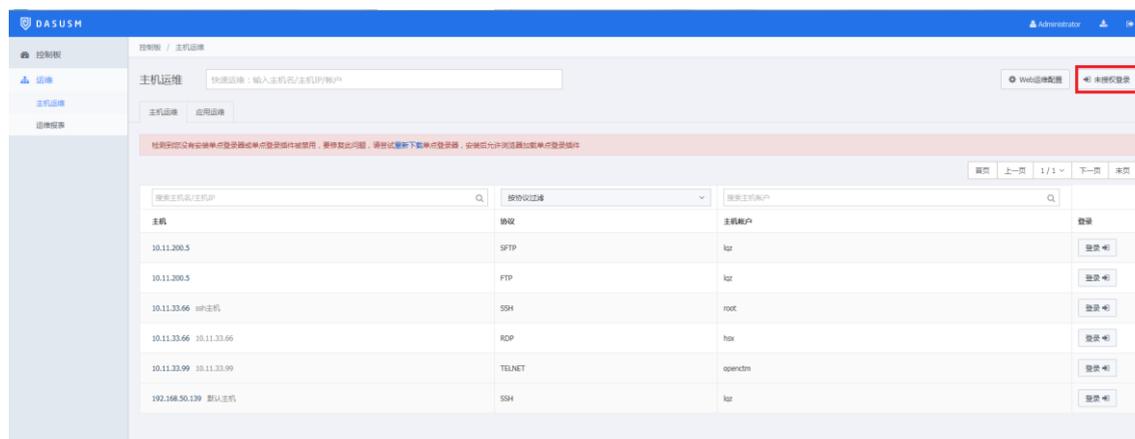


### 9.2.7 未授权登录

当运维人员想访问某主机并且知道该主机的 IP、账户和密码，但该主机没有被授权，没有在运维列表中显示，这时，可以采用未授权的方式。

步骤1 在运维主界面单击<未授权登录>按钮。

图9-12 未授权登录按钮示意图



步骤2 在登录对话框中输入 IP、端口号、协议、账户名、密码，即可登录。

图9-13 未授权登录对话框



## 9.3 实时监控

在线会话用于管理正在运维主机的会话，进行命令审批或会话阻断等操作。

### 9.3.1 实时监控

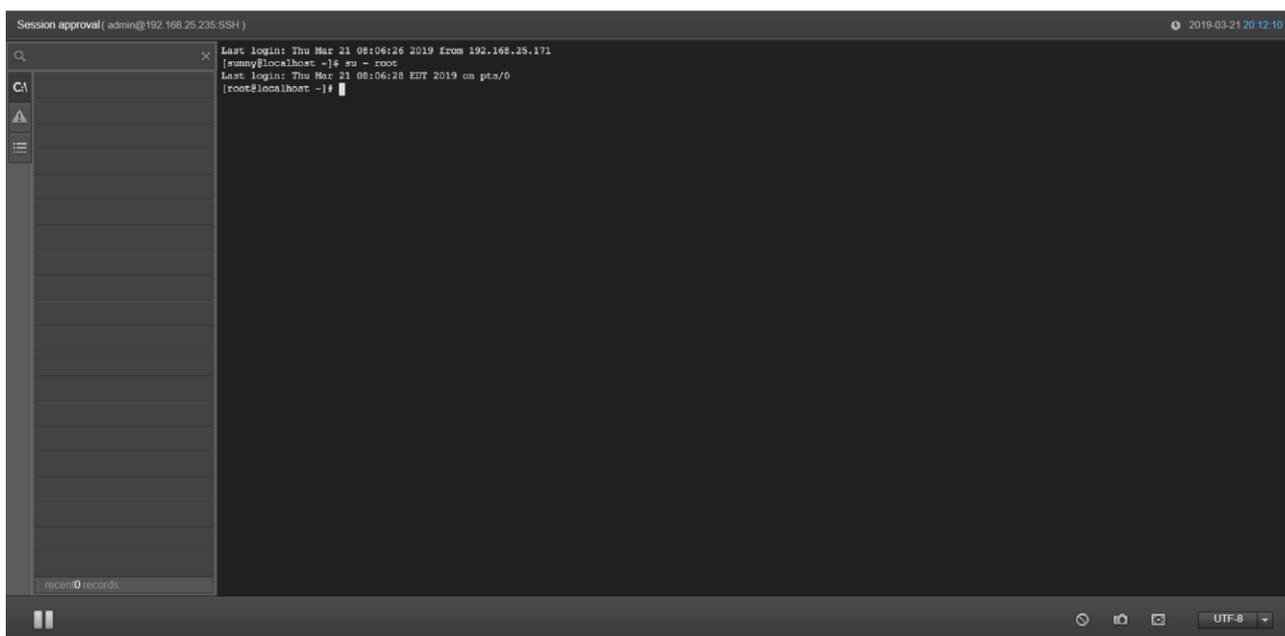
步骤1 进入[运维/在线会话]页面。如果有主机正在运维的会话，就会在页面中显示。

图9-14 在线会话页面

类型	主机	协议/主机帐户	用户/来源IP	开始时间/时长	操作
<input type="checkbox"/> 字符	192.168.50.129 192.168.50.129	SSH kqz	kqyunwei 10.11.200.10	2015-07-02 10:19:37 41秒	<input type="button" value="播放"/> <input type="button" value="详情"/>

步骤2 单击<播放>后，进入运维窗口监控页面，可以实时查看运维会话的操作情况，

图9-15 图 9-11 实时监控对话框



## 2. 阻断会话

步骤1 勾选要阻断的会话

步骤2 单击<阻断会话>按钮即可。

## 9.4 命令审批

运维员进行运维时，若输入了需要审批的命令，需要审批人进行审批后方可操作。

方案一：

步骤1 在<运维/命令审批>主界面查看需要审批的命令。

图9-16 命令审批界面示意图



步骤2 勾选状态为“待审批”的命令，单击“允许”或“拒绝”。

图9-17 命令审批对话框



方案二：

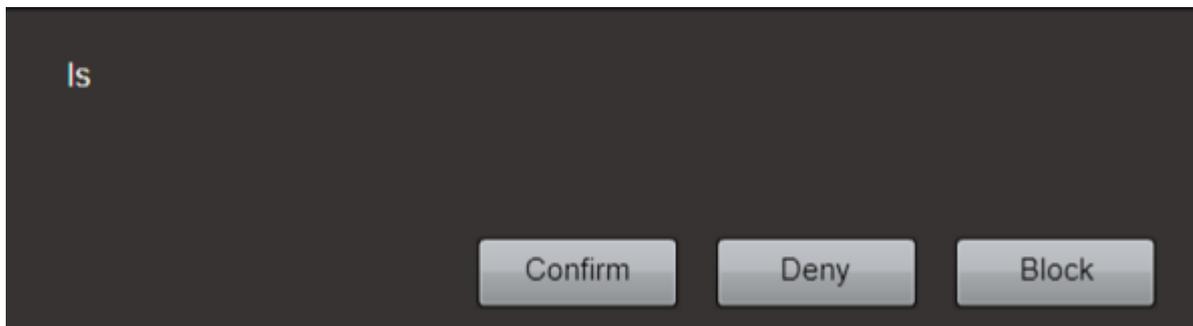
步骤1 在<运维/实时监控/需要命令审批>界面查看需要审批的会话。

图9-18 需要命令审批界面示意图



步骤2 选择需要审批的会话，单击“播放”按钮，监控页面会弹出命令审批对话框，根据实际需求进行处理。

图9-19 命令审批对话框



## 9.5 运维审批

运维审批即二次审批，对于设置了二次审批的主机，即使经过授权，运维人员也不能直接登录成功，系统会自动生成运维申请，由上层管理人员审批通过之后，才能运维。

步骤1 设置二次审批。

在<资产/主机管理>页面中单击需要设置的主机，在配置界面中勾选开启<会话二次审批>并保存。

图9-20 主机配置示意图

## 主机配置

基本信息

主机配置

主机帐户

### 主机配置

---

状态  禁用这台主机

会话选项

- 开启会话二次审批
- 开启会话备注
- 开启历史会话审计
- 开启实时会话监控

RDP选项

- 启用键盘记录
- 允许打印机/驱动器映射
- 允许使用剪贴板

SSH选项

- 允许X11转发
- 允许隧道转发
- 允许打开SFTP通道
- 允许请求exec

文件传输

- 生成文件SHA1
- 保存文件

- 保存下载文件
- 保存上传文件
- 启用文件压缩
- 不保存超过   的文件
- 单个会话保存的文件超过   时停止保存

## 步骤2 运维申请

运维人员在运维页面登录设置过“二次审批”的主机时，系统会提示“运维申请已创建，等待批准”。在<运维/运维审批/我申请的>页面可以查看到主机的审批情况。

图9-21 运维申请示意图

主机	主机账户	备注	申请时间	审批结果
192.168.50.139 192.168.50.139	kgz SSH		2015-07-13 09:22:39	待审批
192.168.50.139 192.168.50.139	kgz SSH		2015-07-13 09:23:36	待审批
192.168.50.139 192.168.50.139	kgz SSH		2015-07-09 13:49:53	已拒绝
192.168.50.139 192.168.50.139	kgz SSH		2015-07-09 13:48:41	登录
192.168.50.139 192.168.50.139	kgz SSH		2015-07-13 09:04:04	已登录



提示

对于已批准的运维申请，对应主机会显示“登录”字样，单击该字样，可以运维对应的主机。

## 步骤3 运维批准

步骤4 上级管理员在<运维/运维审批/我申请的/运维批准>页面可以看见下级运维员的运维申请，勾选相应的运维申请条目，并单击<批准>，在弹出的运维审批对话框中填写运维有效期，即可完成运维批准。

图9-22 运维批准示意图

申请人	主机	主机账户	申请时间/审批时间	审批结果/过期时间	备注
operator operator	10.11.32.60 SQLServer2005	SQL Server sa	2016-05-11 17:32:12	待审批	
operator operator	10.11.32.60 SQLServer2005	SQL Server sa	2016-05-11 17:32:18	已批准 已过期	
operator operator	10.11.32.60 SQLServer2005	SQL Server sa	2016-05-11 17:32:17	已批准 已过期	

图9-23 运维有效期配置示意图

**审批有效期** ✕

---

审批有效期  天 有效值1-365。设置运维批准在几天内有效

---

## 9.6 运维报表

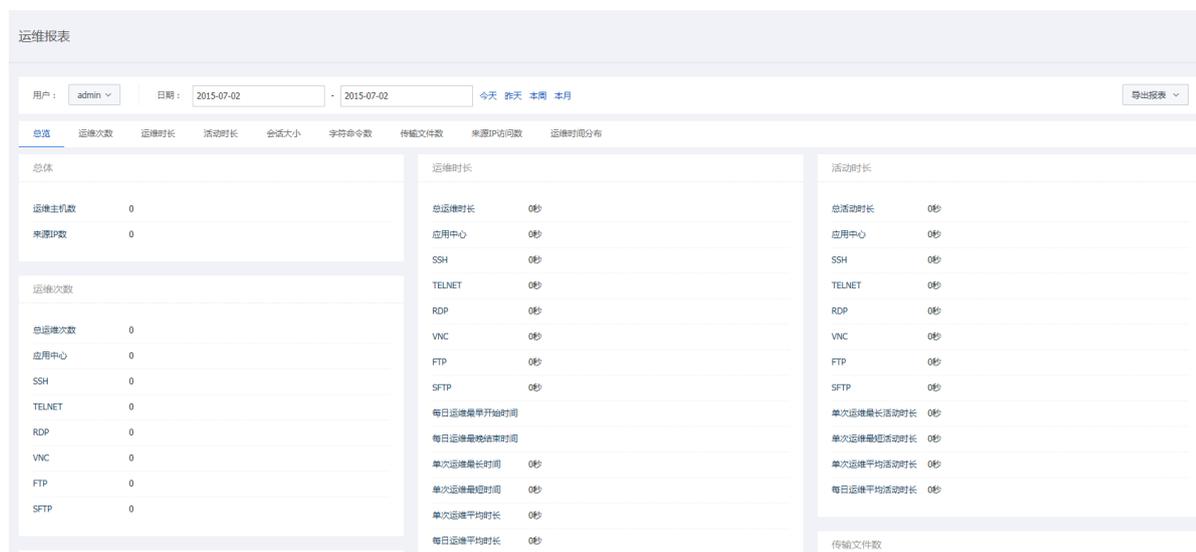
运维报表用于统计当前用户的运维信息报表。

### 9.6.1 按时间范围查看

步骤1 进入[运维/运维报表]页面。可以设置时间范围，选择查看今天、昨天、本周、本月的报表。

步骤2 选择用户后即可查看到该用户的数据报表。

图9-24 查看运维报表示意图



### 9.6.2 导出报表

步骤1 进入[运维/运维报表]页面。

图9-25 运维报表导出页面示意图



步骤2 单击<导出报表>，列出导出的格式。

图9-26 运维报表导出格式示意图



步骤3 单击导出的格式后，即可将统计的报表导出并查看。

### 9.6.3 报表自动发送

在运维报表页面右上角单击<报表自动发送>，在弹出的对话框中设置状态，发送周期以及文件格式。

图9-27 报表自动发送设置对话框



## 10 任务

任务用于运维人员自动改密和自动运维的功能管理。

### 10.1 改密计划

5.4.1 通过明御®运维审计与风险控制系统（DAS-USM）的改密计划功能，可以实现 SSH 协议帐户、telnet 协议、rdp 协议帐户的密码托管。使用密码托管，可以对 ssh 帐户、telnet 帐户、rdp 帐户完成一次性自动改密及定时周期改密任务。

单击“资产”->“改密计划”进入改密计划主界面。

图10-1 改密计划管理页面



## 10.1.2 新建改密计划

步骤1 单击<新建改密计划>按钮，进入改密计划设置界面。

图10-2 新建改密计划

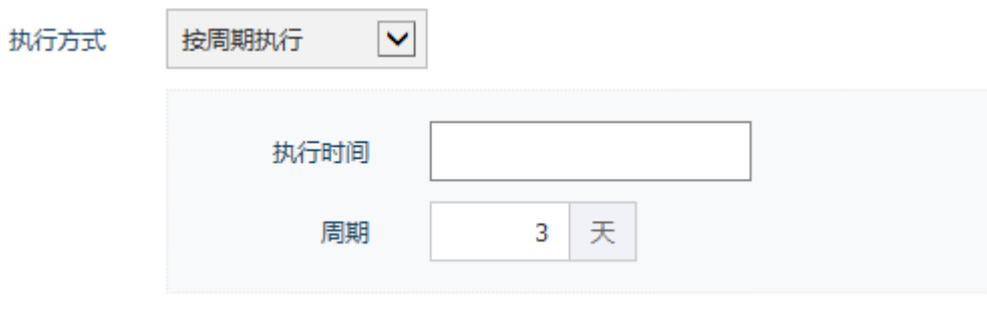


### (1) 任务名称

改密任务名称。

### (2) 执行方式

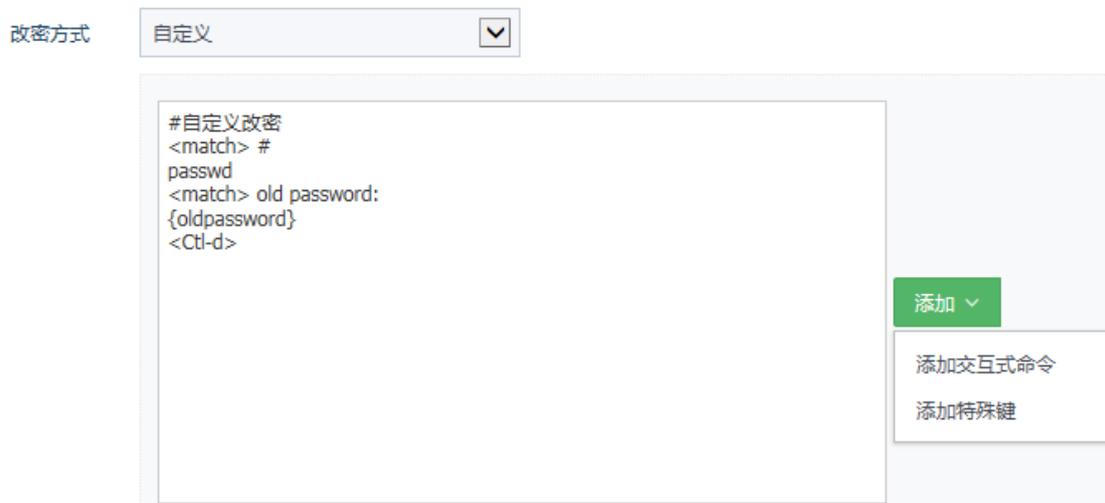
执行方式有手动执行，定时执行和周期执行三种，定时执行需要填写改密任务执行的具体时间，周期执行除了填写执行时间外还必须填写执行周期。



### (3) 改密方式

改密方式的引入是为了根据具体改密主机类型（linux 或 windows）下进行改密。改密方式有主动探测、自定义和改密脚本三种。

图10-3 改密方式示意图

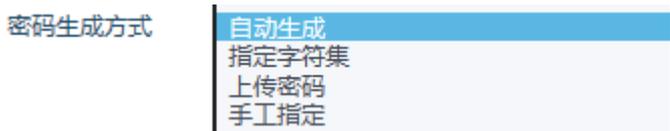


主动探测是指在不知道改密主机类型的情况下，通过探测以确定主机类型来进行改密。

自定义改密是指在知道主机类型的情况下，定义脚本命令来进行改密。脚本语法可以点击帮助进行查看。改密脚本也是在已知主机类型的情况下使用，一个改密脚本可以绑定多个改密计划，当多个改密计划使用同样的脚本进行改密时，可以采用改密脚本的方式。改密脚本可在系统> > 系统配置 > 改密脚本页进行编辑。详细操作参见改密脚本

#### (4) 密码生成方式

改密计划中新密码的计算方式。密码生成方式有自动生成，指定字符集，上传密码和手工指定四种。



#### (5) 发送模式

改密的相关内容，如原密码，改密后的密码等信息可以发送给相关人员。发送方式主要有不发送，邮件发送，ftp 方式发送以及 sftp 方式发送四种。如果需要发送，则需设置发送目标信息。

图10-4 邮件发送模式配置示意图



图10-5 FTP 发送模式配置示意图

发送模式 FTP

服务器地址  IP地址或域名

端口

用户名

密码

路径  相对路径，并确保用户具有此路径的写入权限

文件加密   显示密码 结果文件将被压缩成zip格式，可以选择是否将zip文件加密，密码长度1-64位，留空为不加密。

发送选项  改密前发送密码  发送失败不改密

图10-6 SFTP 发送模式配置示意图

发送模式 SFTP

服务器地址  IP地址或域名

端口

用户名

密码

路径  相对路径，并确保用户具有此路径的写入权限

文件加密   显示密码 结果文件将被压缩成zip格式，可以选择是否将zip文件加密，密码长度1-64位，留空为不加密。

发送选项  改密前发送密码  发送失败不改密

### 10.1.3 编辑改密任务

在改密计划主界面单击相应的改密计划名称，进入编辑页面。

步骤1 修改基本信息。

图10-7 改密任务基本信息

计划信息 lqzchangePASS

基本信息 托管帐户

计划名称

执行方式

改密方式

密码生成方式

密码复杂度  数字  小写字母  大写字母  其他字符

密码长度  有效值6-32

一致性  每次执行任务所有帐户生成相同密码

发送模式

创建人 admin

创建时间 2015-06-25 13:53:20

修改时间

## 步骤2 修改托管账户

在编辑页面单击“托管账户”，进入改密账户编辑页面，可以在该页面添加、编辑、删除主机账户。

图10-8 改密任务托管账户

计划信息 lqzchangePASS

基本信息 托管帐户

搜索主机IP/主机帐户/协议  请选择状态

主机IP	主机帐户	协议	状态	最后修改时间	关联帐户	操作
<input type="checkbox"/> 10.11.200.5	lqz	FTP			0	<input type="button" value="操作"/>

首页 上一页 1/1 下一页 末页

## 10.2 自动运维

明御®运维审计与风险控制系统（DAS-USM）支持自动运维操作。即由系统代替运维人员进行流程化的运

维操作。自动运维支持普通命令，交互式命令以及特殊键。其中交互式命令有特定的语法支持，参照<自动运维配置文件说明>。

### 10.2.1 新建自动运维

在自动运维主页面单击“新建自动运维任务”，对应页面中填写运维信息，单击“创建任务”即可。

图10-9 新建自动运维

#### 新建自动运维任务

#### 任务信息

任务名称

执行方式

手动执行
▼

发送模式

不发送
▼

#### 命令列表

命令列表

添加
▼

帮助

```
#自动运维
```

创建任务

## 10.2.2 自动运维命令列表

自动运维命令列表有固定的命令格式，在命令列表界面单击<帮助>即可查看说明。

图10-10 自动运维帮助示意图

### 自动运维配置文件说明

添加注释请以“#”开头,支持以“#”开头的全局定义:

```
# login_timeout = sec: 设置登录超时sec秒,超时时间范围1-600秒,默认超时时间30秒
# before_send_read = sec: 发送命令前读取缓冲区sec秒,若缓冲区没有数据立即返回,读取时间范围0-86400秒,0为不读取,默认读取时间1秒
# before_match_wait = sec: 等待上一条命令结果返回,匹配结果前等待sec秒,等待时间范围0.1-86400秒,默认值0.2秒
# match_timeout = sec: 设置正则匹配超时sec秒,匹配成功立即返回,匹配时间范围0.1-86400秒,默认值10秒
# match_error = exit: 设置正则匹配失败后是否退出, exit: 退出, continue: 继续
# prompt = #$@~>: 设置终端提示符,默认为 "# "$ "$" "@" "~" ">" 中任意一个
# newline = \r: 发送命令后回车字符, \r 或 \n 或 \r\n 或 \r\r\n, 默认值\r
# logout = exit: 登出命令,默认为exit
```

支持命令格式:

系统保留字: <sendline>, <send>, <match>, <wait>, <KEY>

<sendline> command parameters: 以<sendline> 命名开头,发送带回车的命令(command)及参数(parameters),默认可以不写<sendline>

<send> command argements: 以<send> 命名开头,发送不带回车的命令(command)及参数(argements)

<wait> sec: 等待sec秒,等待时间范围0-86400秒

<match> reg: 匹配正则表达式reg

例1: 匹配以 "#", "\$", "~", ">", "]" 中任意一个作为提示符结束: <match> (?i).\*[\$~>]]([\s]]+\$

例2: 直接匹配提示符 "#": <match> #

<KEY>: 发送特殊按键,键值不区分大小写,可以指定发送次数

例: 发送10个回车: <Enter 10>

<KEY> 键值: <HOME>, <INSERT>, <DELETE>, <END>, <PAGEUP>, <PAGEDOWN>, <UP>, <DOWN>, <LEFT>, <RIGHT>

<KEY> 键值: <CTL-A> ... <CTL-Z>, <CTL-@> ... <CTL-\_>, <ALT-0> ... <ALT-9>, <ALT-A> ... <ALT-Z>, <ALT-~> ... <ALT-?>

<KEY> 键值: <F1> ... <F12>, <ALT-F1> ... <ALT-F12>, <Space>, <Backspace>, <Tab>, <Enter> : \r, <Newline>: \n, <Esc>, <Pause>

## 10.2.3 编辑自动运维

在自动运维主页面单击相应的自动运维任务名称进入编辑页面，可对任务信息和账户信息进行编辑。在账户信息编辑页面可以进行手工执行、手工停止，导出结果等操作。

图10-11 自动运维列表示意图

自动运维 + 新建自动运维任务

任务列表 全部托管帐户

开始  停止  删除
 首页 上一页 1 / 1 下一页 末页

任务名称	部门	状态	执行方式	帐户数	上次执行时间	
<input type="checkbox"/> 任务2	用户组	已停止	手动执行	0		<a href="#">结果导出</a>
<input type="checkbox"/> 任务1	用户组	已停止	手动执行	0		<a href="#">结果导出</a>
<input type="checkbox"/> xxx	用户组	已停止	手动执行	0		<a href="#">结果导出</a>

# 11 系统

系统用于管理运维审计系统的系统配置、系统报表、系统日志、数据维护和系统维护。

## 11.1 认证管理

### 11.1.1 安全配置

#### 1. 登录配置

步骤1 进入[系统/认证管理/登录配置]界面，编辑登录超时时间，验证码过期时间以及 admin 账户限制。

图11-1 登录配置示意图

登录配置

---

登录超时  分钟 有效值1-43200。当用户超过设定时长无操作时，再次操作需要重新登录。默认30。

验证码  启用验证码

验证码过期时间  秒 有效值15-3600。如果设置为0，则不过期。默认60。

限制  禁止admin从Web登录 使admin帐户只能通过设备串口登录本系统

---

步骤2 单击<保存更改>后即可生效。

#### 2. 用户锁定配置

步骤1 进入[系统/系统配置/安全配置]页面。编辑尝试密码次数、锁定时长、重置计数器。

图11-2 用户锁定配置示意图

用户锁定

---

密码尝试次数  次 有效值0-999。如果设置为0，则不锁定帐户。默认值5。

锁定时长  分钟 有效值0-10080。如果设置为0，则锁定帐户直到管理员解除。默认值30。

重置计数器  分钟 有效值1-10080。登录尝试密码失败之后，将登录尝试失败计数器重置为0次所需要的时间。默认值5。

---

步骤2 单击<保存更改>后即可生效。

### 3. 用户密码配置

步骤1 进入[系统/系统配置/安全配置]页面。配置密码强度、密码使用期限以及是否要求新用户第一次登录时进行强制改密。

图11-3 密码策略配置示意图

用户密码配置

---

密码策略  使用强密码 8-64个可见字符，必须包含以下4项：1.大写字母A-Z；2.小写字母a-z；3.数字0-9；4.非字符符号如@,#,\$。

新用户强制改密 本地认证用户首次登录系统后必须修改密码

密码使用期限  天 有效值0-999。如果设置为0，则密码不过期。默认值0。

---

[保存更改](#)

步骤2 单击<保存更改>后即可生效。

## 11.1.2 远程认证

### 1. 本地认证状态

图11-4 本地认证状态示意图

#### 本地认证

状态

### 2. AD 域远程认证

步骤1 进入[系统/认证管理/远程认证]页面。启用远程认证、选择AD域认证模式，填写服务器地址、端口号、Base DN、域名，填写一个AD服务器中的账户和密码，单击<测试连接>，可以测试与服务器的联通性及该账户是否可用。

图11-5 远程认证配置示意图

远程认证

AD
▼

服务器地址	10.11.32.51
备用服务器地址	
端口	389 <input type="checkbox"/> SSL
Base DN	OU=兽人Group,OU=四大家组,DC=hh,DC=com
域	hh.com
帐号	Administrator
密码	●●●●●●
过滤器	((!(cn=aa*)(cn=a*))) <span style="font-size: small; margin-left: 10px;">例: (&amp;(objectClass=person))</span>

同步选项	<input checked="" type="checkbox"/> 自动同步用户	
用户组	<input type="checkbox"/> 同步用户所在组织单位为用户组 <input type="checkbox"/> 同步AD组为用户组并且同步组内的用户成员	
姓名	givenName	填写远程服务器上表示用户姓名的属性名, 如: fullName, 不保存请留空
邮箱	mail	填写远程服务器上表示用户邮箱的属性名, 如: mail, 不保存请留空
手机	mobile	填写远程服务器上表示用户手机号码的属性名, 如: mobile, 不保存请留空

测试连接
立即同步用户

保存更改

步骤2 同步 AD 用户，可自动同步或进行立即同步，自动同步周期为 30 分钟。

步骤3 单击<保存更改>后即可生效。

### 3. LDAP 远程认证

LDAP 配置与 AD 服务器账户配置类似，启用远程认证、选择 LDAP 认证模式，填写服务器地址、端口号、Base DN、域名，填写一个 LDAP 服务器中的账户和密码，单击<测试连接>，可以测试与服务器的联通性及该账户是否可用。

图11-6 远程认证配置示意图

远程认证 LDAP

服务器地址	<input type="text" value="192.168.50.232"/>	
备用服务器地址	<input type="text"/>	没有备用服务器请留空
端口	<input type="text" value="389"/>	<input type="checkbox"/> SSL
Base DN	<input type="text" value="ou=dev,dc=my-domain,dc=com"/>	
帐号	<input type="text" value="cn=Manager,dc=my-domain,dc=com"/>	
密码	<input type="password" value="....."/>	
过滤器	<input type="text"/>	例：(&(objectClass=person))
登录名属性	<input type="text" value="uid"/>	默认值为uid

同步选项	<input checked="" type="checkbox"/> 自动同步用户	
用户组	<input checked="" type="checkbox"/> 将用户所在组织同步为用户组	
姓名	<input type="text" value="description"/>	填写远程服务器上表示用户姓名的属性名，如：fullName，不保存请留空
邮箱	<input type="text" value="email"/>	填写远程服务器上表示用户邮箱的属性名，如：mail，不保存请留空
手机	<input type="text" value="sdfasdf"/>	填写远程服务器上表示用户手机号码的属性名，如：mobile，不保存请留空

---

#### 4. RADIUS 远程认证

输入远程 RADIUS 服务器的 IP 地址、服务端口号、服务器密码、NAS 识别码，选择验证模式。单击<测试连接>可以测试与服务器连通性。

图11-7 远程认证配置示意图

### 远程认证

状态	开启 <input type="button" value="v"/>
认证模式	RADIUS <input type="button" value="v"/>
服务器地址	<input type="text" value="192.168.50.179"/>
端口	<input type="text" value="1812"/>
密码	<input type="password" value="••••••"/>
NAS识别码	<input type="text" value="192.168.50.179"/>
验证模式	用户名 + 动态口令 + 令牌PIN <input type="button" value="v"/>
<input type="button" value="测试连接"/>	

 **提示**

***RADIUS**验证模式有三种：选择用户名和密码时，使用用户名和密码验证；选择用户名和动态口令时，可以使用用户名、密码或者动态口令验证；选择用户名、令牌PIN和动态口令时，可以使用用户名、密码验证，也可以使用用户名、令牌PIN和动态口令验证。*

### 11.1.3 双因子认证

#### 1. 认证方式配置

图11-8 认证方式配置示意图



#### 2. 短信配置

步骤1 进入[系统/认证管理/双因子认证]页面，进行短信配置。

图11-9 短信配置示意图

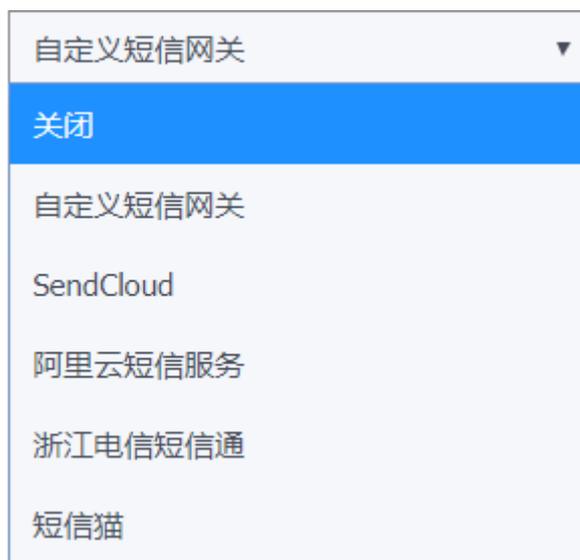


图11-10 短信猫设置示意图

短信配置

短信配置 短信猫

短信模板  短信口令用\$smsToken代替, 留空则采用系统默认模板

测试手机号码

图11-11 自定义短信网关设置示意图

短信配置

短信配置 短信网关

请按照短信网关api填写URL, 手机号码和短信内容分别用\$smsMob和\$smsText代替。  
 GET方式: 填入URL输入框。例如: http://www.sms.com/?uid=username&Key=password&Mobile=\$smsMob&Text=\$smsText  
 POST方式: 分别填入URL和API参数。例如: URL: http://www.sms.com/, API参数: Uid=username&Key=password&Mobile=\$smsMob&Text=\$smsText。如果参数在body中发送, 则以body:开头, 后面跟发送的内容  
 SOAP方式: 分别填入URL和API参数。例如: URL: http://www.sms.com/webservice/sms.php?wsdl, API参数: Submit({"mobile": "\$smsMob", "content": "\$smsText", "account": "0", "password": "0"})

发送方式 POST

URL

API参数

HTTP头部   头部名称与值用英文冒号“:”隔开, 如Content-Type:application/xml, 每一行只填写一个头部信息

短信模板  短信口令用\$smsToken代替, 留空则采用系统默认模板

编码格式 UTF-8

测试手机号码

步骤2 单击<保存更改>后即可生效。

### 11.1.4 第三方 HTTP 平台认证

#### 1. 网易将军令配置

输入认证 URL, HTTP 状态码以及 body 关键字。

图11-12 网易将军令示意图

网易将军令配置

状态 开启

认证URL

参数  参数替换: \$username(用户名), \$password(密码), \$otppwd(动态口令), \$userip(用户源IP)

HTTP状态码  认证成功时服务器返回的HTTP状态码

Body关键字  认证成功时需要同时匹配Body内容的关键字, 不需要匹配则留空。



说明

认证URL中包含了认证所需的用户名、密码等关键字，如：

[https://login.netease.com/api/verifyotp/?username=\\$username&password=\\$password&otpwd=\\$otppwd&product=epayssh&user ip=\\$user ip&usmip=\\$usmip](https://login.netease.com/api/verifyotp/?username=$username&password=$password&otpwd=$otppwd&product=epayssh&user ip=$user ip&usmip=$usmip)

参数替换为：\$username(), \$password(密码), \$otpwd(动态口令), \$user ip(用户源IP), \$systemip(本系统IP)

HTTP状态码表示认证成功时，服务器所返回的状态码。

Body关键字：如果认证成功时需要同时匹配Body内容的关键字，则填写此项，否则留空

## 2. 第三方平台单点登录认证

步骤1 开启该功能。

步骤2 在认证 URL 文本框中输入第三方认证平台的地址。

图11-13 第三方平台单点登录认证配置示意图

第三方平台单点登录认证

状态	<input type="text" value="开启"/>
认证URL	<input type="text" value="https://192.168.50.129/api/routes"/>

认证步骤：

1. 第三方平台发送认证信息到本系统：https://本系统地址/index.php/sso?token=xxx&other=yyy
2. 本系统将接收到的所有认证信息发送回第三方平台：https://第三方平台认证地址?token=xxx&other=yyy
3. 第三方平台返回HTTP状态码200表示认证成功，其他表示认证失败。

## 3. JWT 免登认证配置

在和堡垒机做了 JWT 免登认证时，导入证书，输入用户字段名称，iss 以及 aud。

图11-14 JWT 免登认证示意图

JWT免登认证配置

状态 开启

\* 证书 已配置 | CARoot.pem 已上传

上传证书

PEM证书文件

\* 用户字段名称  JWT中存放用户名的字段名称

iss  留空则不会检查此字段

aud  留空则不会检查此字段

保存更改



说明

具体配置请参考JWT配置文档

## 11.2 网络配置

### 11.2.1 网络配置

#### 1. 接口信息配置

步骤1 填写堡垒机 IP 地址，子网掩码及网关。

图11-15 接口信息配置示意图

接口信息

IP地址	192.168.50.159
子网掩码	255.255.255.0
网关	192.168.50.1

保存更改

步骤2 单击<保存更改>即可。

## 2. DNS 配置

步骤1 进入[系统/网络配置/DNS 信息]界面中。

步骤2 编辑首选 DNS、备选 DNS。

图11-16 DNS 配置示意图

### DNS信息

---

首选DNS	223.5.5.5
备选DNS	223.6.6.6

---

保存更改

步骤3 单击<保存更改>后即可生效。

## 3. 协议端口配置

步骤1 进入[系统/网络配置/协议端口]页面中。

步骤2 修改系统的默认运维端口。

图11-17 协议端口配置示意图

## 协议端口

RDP	63389	<input checked="" type="checkbox"/> 启用
SSH	60022	<input checked="" type="checkbox"/> 启用
TELNET	60023	<input checked="" type="checkbox"/> 启用
VNC	5900	<input checked="" type="checkbox"/> 启用
SFTP	61022	<input checked="" type="checkbox"/> 启用
FTP	60021	<input checked="" type="checkbox"/> 启用
SQL Server	61433	<input checked="" type="checkbox"/> 启用
MySQL	63306	<input checked="" type="checkbox"/> 启用
Oracle	61521	<input checked="" type="checkbox"/> 启用

保存更改

步骤3 支持协议代理开关，要支持某协议，勾选启用框即可。

步骤4 单击<保存更改>后即可生效。

### 4. RD 网关配置

步骤1 进入[系统/网络配置/RD 网关]页面中。

步骤2 在 RD 网关配置界面中可以修改 RD 网关端口。

图11-18 RD 网关配置示意图

RDP网关

---

RDP网关端口

---

[保存更改](#)

### 5. Web 端口配置

步骤1 进入[系统/网络配置/Web 端口]页面中。

步骤2 在 Web 端口配置界面中可以修改系统默认管理端口。

图11-19 Web 端口配置示意图

WEB端口

---

WEB端口

---

[保存更改](#)

步骤3 单击<保存更改>后即可生效。

### 6. 聚合端口配置

步骤1 进入[系统/网络配置/聚合端口信息]页面。

图11-20 聚合端口信息示意图

功能名称	接口名称	连通状态	IP地址	端口配置
业务数据	bond0	✓	192.168.50.159	<a href="#">配置</a>
自定义	bond1	⊗		<a href="#">配置</a>
远程灾备	bond2	⊗		<a href="#">配置</a>

步骤2 选择好一个接口后，单击<配置>，弹出窗口。对业务数据接口进行配置，需配置接口模式。对自定义接口和远程灾备接口进行配置，需配置接口的 IP、掩码、接口模式。

图11-21 业务数据接口配置示意图

bond0 ×

---

模式

0:balance-rr  
 1:active-backup[默认]  
 2:balance-xor  
 3:broadcast  
 4:802.3ad  
 5:balance-tlb  
 6:balance-alb

保存更改

图11-22 自定义接口和远程灾备接口配置示意图

bond2 ×

---

IP地址

子网掩码

模式 1:active-backup[默认] ▼

---

保存更改

步骤3 单击<保存更改>即可生效。

### 7. 物理端口信息

步骤1 进入[系统/网络配置/物理端口信息]页面。

图11-23 物理端口信息示意图

物理端口信息

设备名称	接口名称	速度	连通状态	工作模式	端口配置
admin	eth0	1000Mbps	⊘	bond0	
HA	eth3	1000Mbps	⊘	bond0	<span style="border: 1px solid #ccc; padding: 2px 5px;">配置</span>
P1	eth1	1000Mbps	✔	bond0	<span style="border: 1px solid #ccc; padding: 2px 5px;">配置</span>
P2	eth2	1000Mbps	⊘	bond0	<span style="border: 1px solid #ccc; padding: 2px 5px;">配置</span>

步骤2 选择好一个接口，单击<配置>，将物理接口与逻辑端口绑定。

图11-24 端口配置示意图



## 11.2.2 Web 设置

### 1. Web 设置

步骤1 进入[系统/网络设置/Web 端口]页面中。

步骤2 在 Web 端口配置界面中可以修改系统默认管理端口。

图11-25 Web 端口配置示意图



步骤3 单击<保存更改>后即可生效。

#### 说明

默认未勾选“增强 HTTPS 安全性”，对老版本的系统和低版本的 IE 浏览器兼容性较好，安全性降低。若勾选安全性增强，部分低版本的浏览器无法访问堡垒机。

### 2. Web 证书设置

步骤1 进入[系统/网络设置/Web 设置]页面中。

步骤2 设置 IP 并保存。

图11-26 Web 证书配置示意图

### Web证书配置

---

系统IP

---

保存更改

步骤3 单击<保存更改>后即可生效。



说明

Web 证书配置只有在云堡垒机上才有此功能。

### 11.2.3 HA 配置

步骤1 进入[系统/网络配置/HA 配置]页面。



说明

1. HA配置前提。必须是2台运维审计系统，且是相同的软件版本。
2. 主机和备机的心跳口IP必须是直连或互通。
3. 先配置主机，然后配置备机。
4. 若需要重新配置，需要先回到单机。

图11-27 HA 配置示意图

## HA配置

当前运行模式

单机模式

HA群组验证密钥	963AE14A-7BBA-5043-A50C-3ABEE6EC3672	
HA接口设备	bond0 <input type="button" value="v"/>	
主机HA接口IP	1.1.1.1	
备机HA接口IP	1.1.1.2	
HA口子网掩码	255.255.255.252	
心跳间隔	5 秒	有效值1-300。宕机检测的间隔
宕机切换时间	30 秒	有效值30-3000。无响应多久后进行激活状态切换
服务/虚拟IP	172.16.1.5	HA模式激活时bond0使用此地址提供服务
灾备/虚拟IP	172.16.2.5	HA模式激活时bond2使用此地址提供HA数据
灾备/备份IP	172.16.2.6	通过灾备/虚拟IP向此地址实时同步HA数据

步骤2 先配置主机。1、选择热备模式-主机，选择 HA 接口设备，接口设备需要在网络配置中预先设置。主机 HA 接口 IP 到备机 HA 接口 IP 可连通；填入备机 HA 接口的 IP。2、填入服务/虚拟 IP，HA 激活的一方将在 BOND0 业务数据接口通过此 IP 提供服务；HA 发生切换后，服务/虚拟 IP 会跟随切换。3、填入灾备/虚拟 IP，HA 激活的一方将在 BOND2 灾难备份接口通过此 IP 提供服务；HA 发生切换后，灾备/虚拟 IP 会跟随切换；灾备/虚拟 IP 和灾备/备份 IP 需要在相同网段；不使用远程灾备功能保留默认值。

图11-28 主机配置示意图

**HA配置**

当前运行模式: 热备模式-HA主机

HA群组验证密钥	<input style="width: 90%;" type="text" value="228990FD-6E37-516E-B714-EDA4C26ED070"/>	
HA接口设备	<span style="border: 1px solid #ccc; padding: 2px;">bond0</span>	
主机HA接口IP	<input style="width: 90%;" type="text" value="192.168.50.132"/>	
备机HA接口IP	<input style="width: 90%;" type="text" value="192.168.50.138"/>	
HA子网掩码	<input style="width: 90%;" type="text" value="255.255.255.0"/>	
心跳间隔	<input style="width: 40px;" type="text" value="5"/> 秒	有效值1-300。宕机检测的间隔
宕机切换时间	<input style="width: 40px;" type="text" value="30"/> 秒	有效值30-3000。无响应多久后进行激活状态切换

服务/虚拟IP	<input style="width: 90%;" type="text" value="192.168.50.131"/>	HA模式激活时bond0使用此地址提供服务
灾备/虚拟IP	<input style="width: 90%;" type="text" value="172.16.2.5"/>	HA模式激活时bond2使用此地址提供HA数据
灾备/备份IP	<input style="width: 90%;" type="text" value="172.16.2.6"/>	通过灾备/虚拟IP向此地址实时同步HA数据

步骤3 单击<保存更改>，确定后即可生效。

步骤4 配置备机。选择热备模式-备机，将主机上的 HA 群组验证密钥复制-粘贴至备机上，选择 HA 接口设备，接口设备需要在网络配置中预先设置。主机 HA 接口 IP 与备机 HA 接口 IP 与步骤 2 中一致。

图11-29 备机配置示意图

**HA配置**

当前运行模式: 热备模式-HA备机

HA群组验证密钥	<input style="width: 90%;" type="text" value="228990FD-6E37-516E-B714-EDA4C26ED070"/>	
HA接口设备	<span style="border: 1px solid #ccc; padding: 2px;">bond0</span>	
主机HA接口IP	<input style="width: 90%;" type="text" value="192.168.50.132"/>	
备机HA接口IP	<input style="width: 90%;" type="text" value="192.168.50.138"/>	
HA子网掩码	<input style="width: 90%;" type="text" value="255.255.255.0"/>	
心跳间隔	<input style="width: 40px;" type="text" value="5"/> 秒	有效值1-300。宕机检测的间隔
宕机切换时间	<input style="width: 40px;" type="text" value="30"/> 秒	有效值30-3000。无响应多久后进行激活状态切换

步骤5 单击<保存更改>，确定后即可生效。

步骤6 最后访问人员使用服务/虚拟 IP。

图11-30 同步过程示意图

本机状态 (已激活, 持有VIP) : 192.168.50.131	对端状态
数据口IP: 192.168.50.132	数据口IP: 192.168.50.138
HA口IP: 192.168.50.132	HA口IP: 192.168.50.138
连接状态: SyncSource	连接状态: SyncTarget
角色状态: Primary	角色状态: Secondary
数据状态: UpToDate	数据状态: Inconsistent
同步进度: 14.0%	同步进度: 14.0%
磁盘读/写: 1437197/299096	磁盘读/写: 0/1439088
网络收/发: 0/1435936	网络收/发: 1440032/0
CurrentUUID: 0x57C58D7042C36513	CurrentUUID: 0x2939E41718D0B1AE
BitmapUUID: 0x2939E41718D0B1AE	BitmapUUID: 0x0000000000000000
HistoryUUID: 0x0000000000000004	HistoryUUID: 0x0000000000000000
OlderUUID: 0x0000000000000000	OlderUUID: 0x0000000000000000

步骤7 配置远程灾备，可选配置。将第 3 台设备选择热备模式-远程灾备，将主机上的 HA 群组验证密钥复制-粘贴至远程灾备上；灾备/备份 IP 需要在网络配置中预先设置，第 3 台设备配置灾备/备份 IP 所在接口与步骤 2 步骤 4 中主机、备机 bond2 远程灾备口 ip 互通；灾备/虚拟 IP 和灾备/备份 IP 与步骤 2 中填入配置保持一致。

图11-31 远程灾备配置示意图

**HA配置**

---

当前运行模式: 热备模式-远程灾备

HA群组验证密钥:

灾备/虚拟IP:  HA模式激活时bond2使用此地址提供HA数据

灾备/备份IP:  通过灾备/虚拟IP向此地址实时同步HA数据

步骤8 单击<保存更改>，确定后即可生效。

步骤9 异常处理。主机、备机、远程灾备出现无法同步故障或者填入配置有误时，将所有设备状态选择为单机模式，<保存更改>后重新配置 HA 功能。

 **提示**

设备作为备机加入到HA中，备机将丢弃原有配置数据，系统为灾难备机加入到HA中，灾难备机将丢弃原有配置数据。请慎重操作。

## 11.2.4 静态路由

步骤1 进入[系统/网络配置/静态路由]页面。

图11-32 静态路由配置示意图

### 新建路由规则

---

目标地址	
子网掩码	255.255.255.0
下一跳/网关	
出口设备	bond0 <span style="float: right;">▼</span>
Metric	0
备注	

---

创建路由规则

步骤2 在页面中填写。目标地址、掩码、下一跳网关、出口设备等。

步骤3 单击<创建路由规则>后即可提示创建成功，并在列表中显示。

## 11.2.5 SNMP 配置

步骤1 进入[系统/网络配置/SNMP 配置]页面中。

图11-33 SNMP 配置示意图

## SNMP配置

状态	关闭 <input type="button" value="v"/>
系统标识	DASUSM
物理位置	TestLocation <input type="button" value="x"/>
联系方式	admin@test.com

步骤2 单击<添加帐号>，弹出窗口。输入 SNMP 的共同体名称、选择 SNMP 版本、是否限制 IP。

图11-34

图11-35 添加 SNMP 信息示意图

## 新建只读社团

Read community	<input type="text"/>
SNMP版本	v2c <input type="button" value="v"/>
IP限制	<input type="text"/>

步骤3 单击<创建账号>后即可添加成功。

图11-36 SNMP 管理页面示意图

## 社团信息

社团	SNMP版本	IP限制	删除
0	v2c	default	<input type="button" value="删除"/>

步骤4 在<节点信息>区，可以查看 SNMP 输出的 OID 信息。

图11-37 OID 信息显示示意图

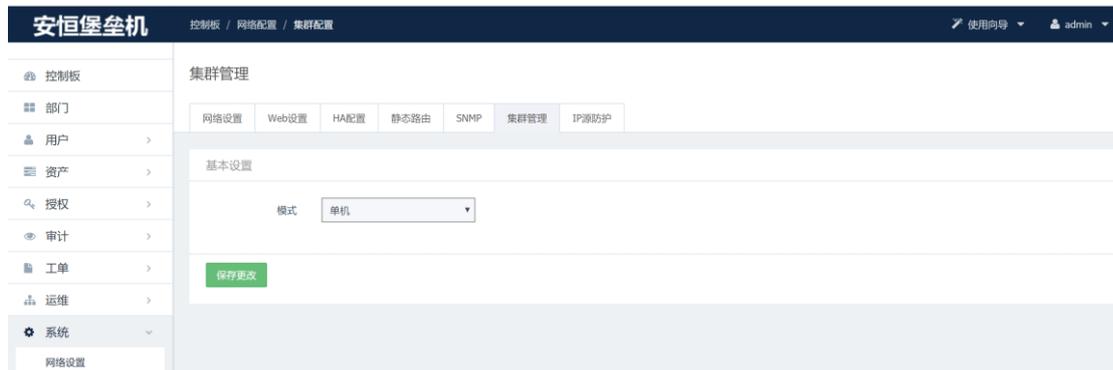
常用节点信息

OID	名称	描述
.1.3.6.1.4.1.2021.4	memory	系统内存信息
.1.3.6.1.4.1.2021.9	dskTable	系统磁盘信息
.1.3.6.1.4.1.2021.10.1.3	laLoad	系统CPU负载
.1.3.6.1.4.1.2021.11	systemStatus	系统CPU信息
.1.3.6.1.2.1.2	interfaces	系统网卡信息
.1.3.6.1.2.1.4	ip	系统IP信息
.1.3.6.1.2.1.6	tcp	系统TCP信息

### 11.2.6 集群管理

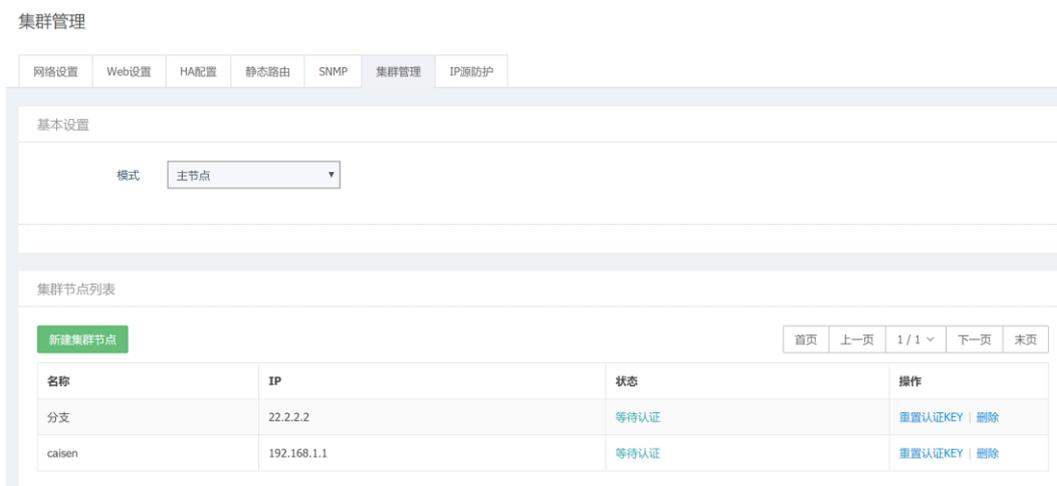
步骤1 单击[系统/网络配置/集群管理]进入集群管理配置界面

图11-38 打开集群管理界面



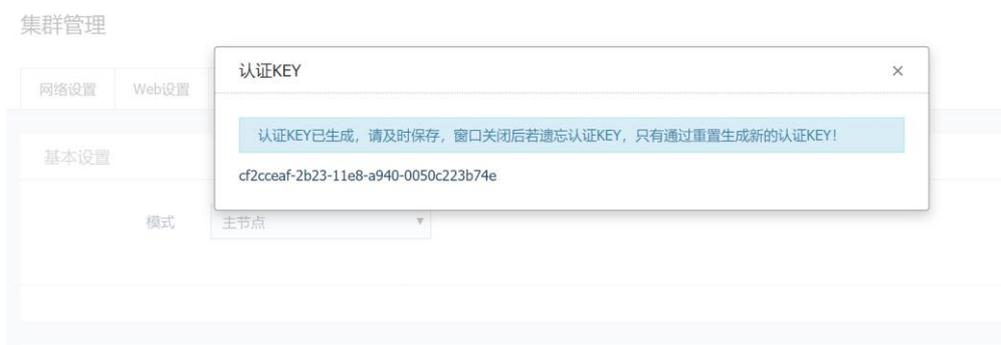
步骤2 <基本设置>中，可将模式设置为<主节点><子节点>，不需要集群时，直接将模式设置为<单击>，单击<保存更改>即可

图11-39 主节点模式界面



步骤3 新建集群节点。填入名称、IP，单击<新建集群节点>即可，复制保存认证 key。

图11-40 新建集群节点



步骤4 在节点设备中，输入主节点 IP，认证 key，打击<保存更改>，完成子节点的配置。

图11-41 从节点配置界面

集群管理

网络设置
Web设置
HA配置
静态路由
SNMP
集群管理
IP源防护

基本设置

模式 从节点

主节点IP 192.168.1.1

认证KEY 49e288e6-2b24-11e8-a940-0050c223b74e

保存更改

### 11.2.7 IP 源防护

IPtables 源防护主要用于对来源地址限制访问堡垒机。当不需要防护时，将防护模式设置为关闭，需要防护时分为两种防护模式，黑名单模式开启时，列入黑名单的 IP 地址将不允许访问堡垒机，白名单模式开启时，只有列入白名单的 IP 地址可以进行访问堡垒机。

步骤1 单击[系统/网络配置/IP 源防护]进入 IP 源防护设置页面。

图11-42 打开 IP 源防护界面

DASUM
控制板 / 系统配置 / IP源防护
admin

- 控制板
- 部门
- 用户
- 资产
- 授权
- 审计
- 工单
- 运维
- 系统
  - 系统配置
  - 系统日志
  - 系统报表
  - 数据维护
  - 系统维护

IP源防护

网络配置
安全配置
运维配置
静态路由
SNMP
告警配置
认证配置
HA配置
SSH KEY配置
界面配置
IP源防护

基本设置

防护模式 白名单模式

保存更改

白名单IP列表

删除
添加白名单IP

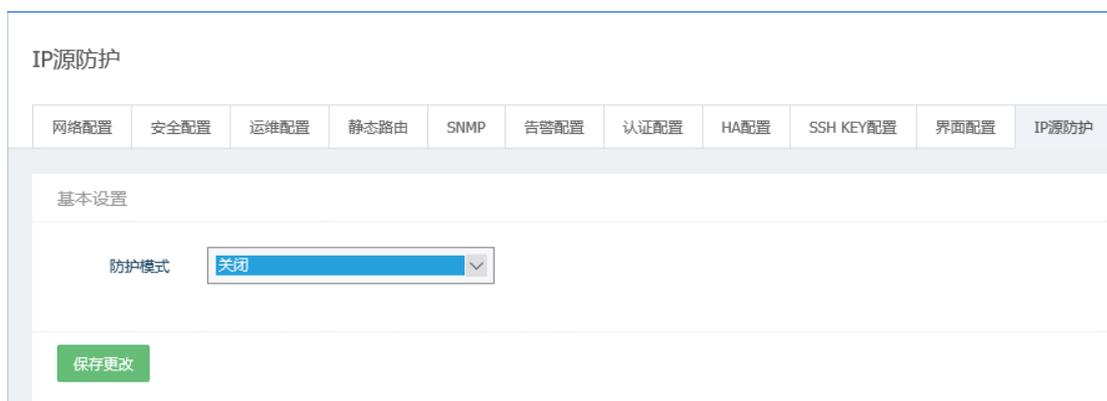
搜索IP/地址/备注

IP	地址段	备注	
<input type="checkbox"/>	10.0.0.1/8	10.0.0.0-10.255.255.255	成都安恒
<input type="checkbox"/>	10.11.0.1/16	10.11.0.0-10.11.255.255	成都研发
<input type="checkbox"/>	192.168.50.0/24	192.168.50.0-192.168.50.255	成都测试
<input type="checkbox"/>	192.168.50.136	192.168.50.136-192.168.50.136	本机

步骤2 <基本设置>中，可将防护模式设置为<关闭><黑名单模式><白名单模式>，不需要防护时，直接将防护模式设置为<关闭>，单击<保存更改>即可。

杭州安恒信息技术股份有限公司

图11-43 关闭模式



IP源防护

网络配置 安全配置 运维配置 静态路由 SNMP 告警配置 认证配置 HA配置 SSH KEY配置 界面配置 IP源防护

基本设置

防护模式 关闭

保存更改

开启<黑名单模式>时,将防护模式设置为<黑名单模式>,在<黑名单 IP 列表>中单击<添加黑名单 IP>,按照表单要求填写 IP 地址和备注,单击<添加到 IP 列表>即可。删除黑名单时,直接单击相应 IP 地址,单击<删除>即可。

图11-44 黑名单模式



IP源防护

网络配置 安全配置 运维配置 静态路由 SNMP 告警配置 认证配置 HA配置 SSH KEY配置 界面配置 IP源防护

基本设置

防护模式 黑名单模式

保存更改

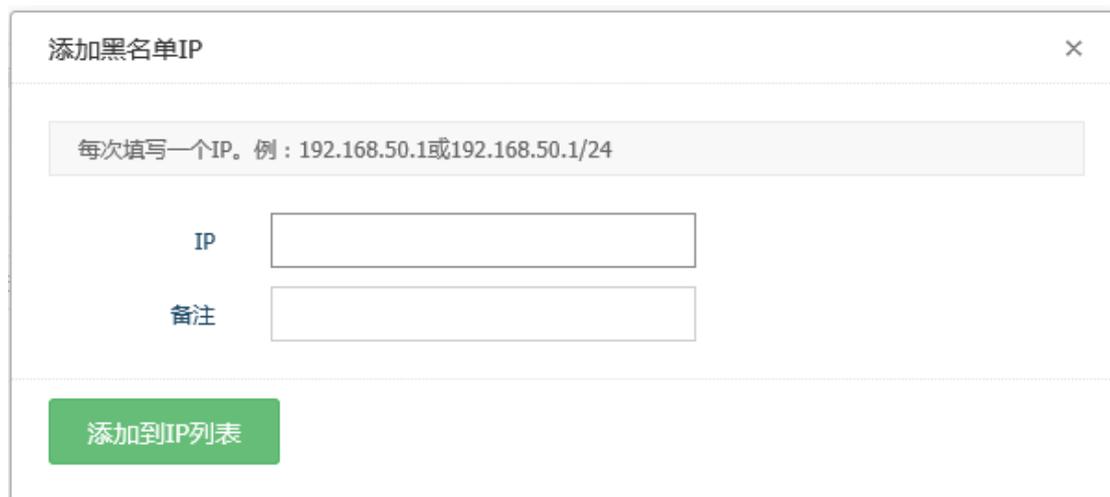
黑名单IP列表

删除

搜索IP/地址/备注

IP	地址段	备注

图11-45 添加黑名单 IP



添加黑名单IP

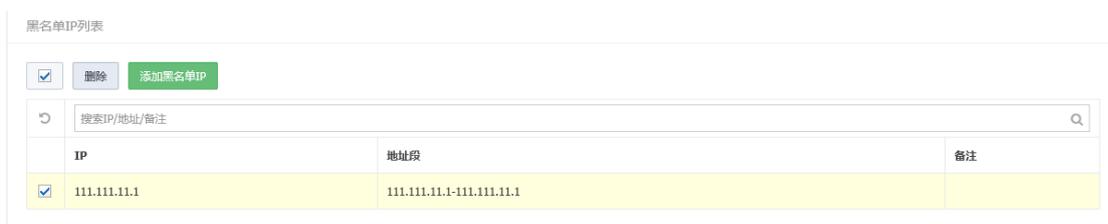
每次填写一个IP。例：192.168.50.1或192.168.50.1/24

IP

备注

添加到IP列表

图11-46 删除黑名单



开启<白名单模式>时，将防护模式设置为<白名单模式>，在<白名单 IP 列表>中单击<添加白名单 IP>，按照表单要求填写 IP 地址和备注，单击<添加到 IP 列表>即可。删除白名单时，直接单击相应 IP 地址，单击<删除>即可。

图11-47 白名单模式

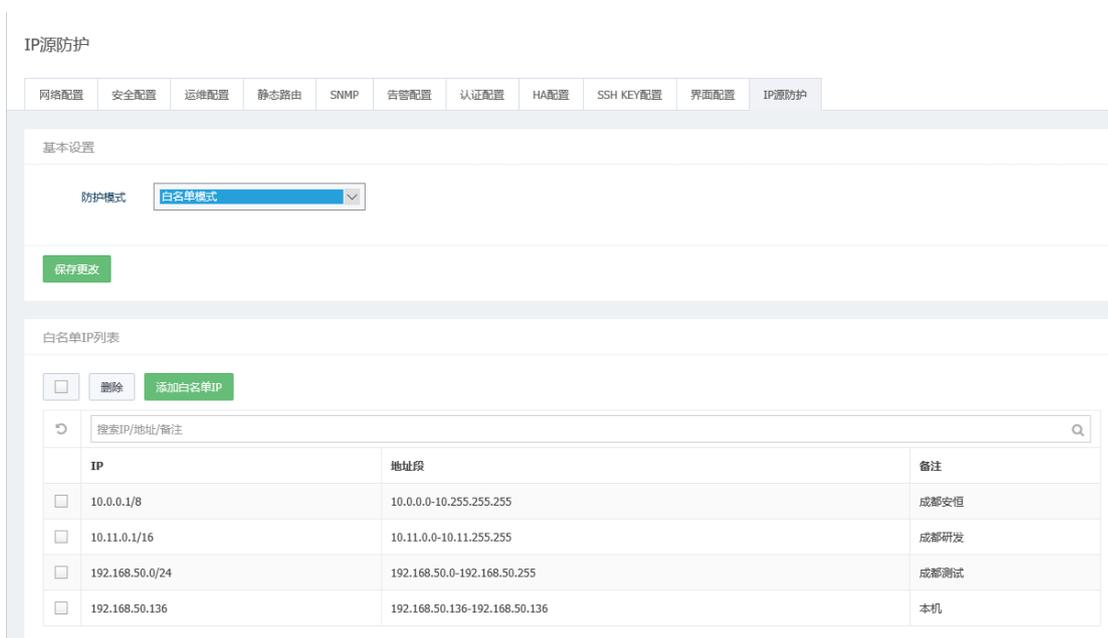


图11-48 添加白名单

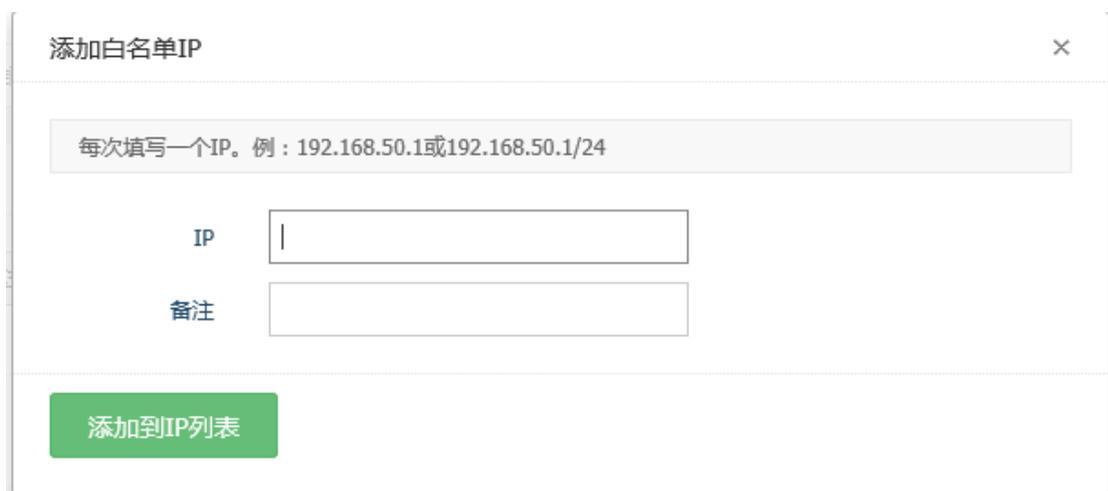


图11-49 删除白名单

白名单IP列表

删除

IP	地址段	备注
<input checked="" type="checkbox"/> 10.0.0.1/8	10.0.0.0-10.255.255.255	成都安恒
<input type="checkbox"/> 10.11.0.1/16	10.11.0.0-10.11.255.255	成都研发
<input type="checkbox"/> 192.168.50.0/24	192.168.50.0-192.168.50.255	成都测试
<input type="checkbox"/> 192.168.50.136	192.168.50.136-192.168.50.136	本机

## 11.3 系统配置

### 11.3.1 运维配置

运维配置包括未授权登录，运维登录和运维时长限制配置。

#### 1. 未授权登录配置

运维授权配置主要是对未授权登录进行相关配置，如下图所示。

图11-50 未授权登录配置示意图

运维配置

**未授权登录**

- 允许未授权登录
  - 收集未授权登录
  - 收集主机帐户的密码
  - 自动创建运维规则

**运维登录**

- 允许使用用户密码登录主机 适用于用户和主机帐户同属于AD/LDAP的场景
- 允许使用用户SSH私钥登录主机
- 允许使用SSH-agent-forwarding方式登录SSH服务器 适用于登录堡垒机和登录SSH服务器使用同样私钥的场景
- 开启应用会话共享

**SSH登录**

- 允许使用公钥登录
- 允许使用密码登录
- 允许发送环境变量
  - 发送运维用户信息 USM\_USERNAME 变量名称可自定义
  - 发送运维来源IP USM\_SOURCEIP 变量名称可自定义
- UsmsHELL使用命令行方式

SSH banner  最大长度64个字符。例如：OPENSHELL\_7.6

**运维时长限制**

- 空闲时长超过  分钟 时自动断开连接

其中“收集授权关系”是指用户进行未授权登录后，系统会自动收集用户和主机的授权对应关系，在<未授权登录审核>页面可以查看。如下图所示。

图11-51 未授权登录审核页面

未授权登录审核

状态	用户	主机	协议	主机账户	最近登录时间	授权时间	授权人
<input type="checkbox"/> 未授权	openctm Steven	10.11.33.66	SSH	openctm	2015-11-09 10:31:02		
<input type="checkbox"/> 未授权	zheng1_dept zhengex	192.168.50.206	SSH	root	2015-11-09 08:52:31		
<input type="checkbox"/> 未授权	zheng1_dept zhengex	192.168.50.129	SSH	fsf	2015-11-09 08:51:46		
<input type="checkbox"/> 未授权	testlx22 dsdfs	192.168.50.139	SSH	xlx	2015-11-06 18:37:48		
<input type="checkbox"/> 未授权	openctm Steven	10.11.0.1	SSH	[EMPTY]	2015-11-06 16:11:34		
<input type="checkbox"/> 未授权	zheng1_dept zhengex	192.168.50.205	SSH	git	2015-11-06 08:51:00		
<input type="checkbox"/> 未授权	admin adfastf	10.11.0.253	TELNET	[EMPTY]	2015-11-05 17:25:32		
<input type="checkbox"/> 未授权	zheng1_dept zhengex	192.168.50.139	SSH	fsf	2015-11-05 17:18:46		
<input type="checkbox"/> 未授权	openctm Steven	10.11.33.88	SSH	openctm	2015-11-05 10:46:15		
<input type="checkbox"/> 未授权	zheng1_dept zhengex	192.168.50.207	SSH	git	2015-11-04 16:13:33		
<input type="checkbox"/> 未授权	zheng1_dept zhengex	192.168.50.129	SSH	jojo	2015-11-04 10:28:00		
<input type="checkbox"/> 未授权	zheng1_dept zhengex	192.168.50.139	SSH	openctm	2015-11-02 11:10:04		
<input type="checkbox"/> 未授权	zheng1_dept zhengex	192.168.50.139	SSH	xlx	2015-11-02 11:09:56		
<input type="checkbox"/> 未授权	zheng1_dept zhengex	192.168.50.139	SSH	root	2015-11-02 11:09:04		
<input type="checkbox"/> 未授权	zheng1_dept zhengex	10.11.33.66	SSH	openctm	2015-10-27 14:04:27		
<input type="checkbox"/> 未授权	zheng1_dept zhengex	192.168.50.205	SSH	wsd	2015-10-27 12:49:24		
<input type="checkbox"/> 未授权	zheng1_dept zhengex	192.168.50.139	SYSDEF	fsf	2015-10-27 09:56:24		

“收集主机账户和密码”是指用户进行未授权登录后，系统会自动收集用户所登录主机的账户和密码。

“自动授权”是指系统检测到未授权登录的事件发生后，会自动创建相应授权关系，不需要管理员进行手动授权。

### 2. 运维登录

“允许使用用户密码登录主机”，是指允许用户使用堡垒账户登录主机。勾选次项后，在运维界面的账户列表中会有相关项，如下图所示，选用[SYSDEF][SELF]账户，即可使用堡垒账户登录主机。主要适用于用户和账户同属于 AD/LDAP 的场景。

图11-52 堡垒账户示意图



“允许使用 SSH-agent-forwarding 方式登录 SSH 服务器”，勾选此项后，堡垒将支持 SSH-agent-forwarding 特性，适用于 SSH 服务器要求采用 publickey 方式登录的场景。

### 3. 修改 SSH 的 banner

由于 openssh 漏洞相对来说比较多，堡垒机实际上只是做协议转发，并未用到 openssh，该功能默认不开启，但 xshell 客户端不能使用 SSH-agent-forwarding 特性，在设置 ssh 的 banner 为 openssh\_x 时，会被漏洞扫描工具扫出漏洞。

### 4. 运维时长限制

当协议连接上的空闲时长超过此限制，网络连接会自动断开。



说明

各协议空闲时长定义如下：

rdp、vnc：客户端无数据发送时。

ftp：命令通道和数据通道均无数据发送时。

ssh、telnet、sftp、mysql、sqlserver、oracle：客户端和服务端均无数据发送时。

### 11.3.2 告警配置

#### 1. 邮件方式告警

步骤1 进入[系统/系统配置/告警配置/邮件配置]页面。配置邮件的地址、端口、账号、密码、收件人邮箱，可测试邮件是否配置成功。

图11-53 邮件配置示意图

#### 邮件配置

发送方式	<input type="text" value="SMTP"/>	<input type="button" value="v"/>
服务器地址	<input type="text" value="mail.dbappsecurity.com.cn"/>	
端口	<input type="text" value="25"/>	<input type="checkbox"/> SSL
帐号	<input type="text" value="root@163.com"/>	<input checked="" type="checkbox"/> 匿名发送
收件人	<input type="text" value="root@163.com"/>	
<input type="button" value="发送测试邮件"/>		

步骤2 单击<保存更改>。启用状态、勾选系统日志告警等级、勾选策略日志告警等级。

图11-54 告警配置示意图

### 操作日志告警

---

状态

邮件告警
 低
  中低
  中
  中高
  高

Syslog告警
 低
  中低
  中
  中高
  高

步骤3 单击<保存更改>后即可生效。

## 2. Syslog 方式告警

步骤1 进入[系统/系统配置/告警配置/syslog 配置]页面。配置发送标识、服务器 IP、端口，可以测试是否连通。

图11-55 syslog 配置示意图

### Syslog配置

---

发送者标识

服务器IP

端口

步骤2 单击<确定>后即可配置成功，并自动返回管理页面。启用状态、勾选系统日志告警等级、勾选策略日志告警等级。

步骤3 单击<保存更改>后即可生效。

### 3. 系统资源告警

步骤1 进入[系统/系统配置/告警配置/系统资源告警配置]页面。配置发送标识、服务器 IP、端口，可以测试是否连通。

系统资源告警包括了：CPU 使用率、内存使用率、系统分区使用率和会话分区使用率达到预设阈值时的告警信息，该阈值可自定义

图11-56 系统资源告警配置示意图

#### 系统资源告警配置

**告警阈值**

CPU使用率达到	95	%	时执行告警
内存使用率达到	95	%	时执行告警
系统分区使用率达到	95	%	时执行告警
会话分区使用率达到	95	%	时执行告警

邮件告警  启用

保存更改

### 11.3.3 语言和界面配置

#### 1. 语言设置

系统支持三种界面显示语言：简体中文、繁体中文和英文。

图11-57 界面语言配置示意图

#### 语言设置

**语言**

简体中文

English

繁體中文

保存更改

#### 2. 系统 logo 设置

系统支持自定义登录界面 logo 和顶部 logo。

图11-58 logo 设置示意图



### 11.3.4 功能设置

#### 1. 部门管理

开启部门管理后，可以实现用户、资产的层级管理。

图11-59 部门管理配置示意图



#### 2. 主机导出配置

密码导出设为否时，导出的文件的密码字段会置空。请根据安全需要进行配置。

图11-60 主机导出配置示意图

### 主机导出配置

---

不导出密码时，导出文件的密码字段会置空

文件在导入时，密码字段为空的帐户会视为手动登录模式，反之为自动登录模式

相同的帐户名，不同的登录模式，视为不同帐户，故在导入时会出现新建帐户，而非修改帐户的情况

密码导出 是 ▼

保存更改

### 3. 工单配置

配置工单功能使用与否。在不需要工单功能的场景中，建议关闭工单功能，否则运维员可通过新建工单浏览系统中所有的主机 IP 地址和主机帐户列表。

图11-61 工单配置示意图

### 工单配置

---

在不需要工单功能的场景中，建议关闭工单功能，否则运维员可通过新建工单浏览系统中所有的主机IP地址和主机帐户列表

状态 开启 ▼

生成的运维规则  过期自动删除

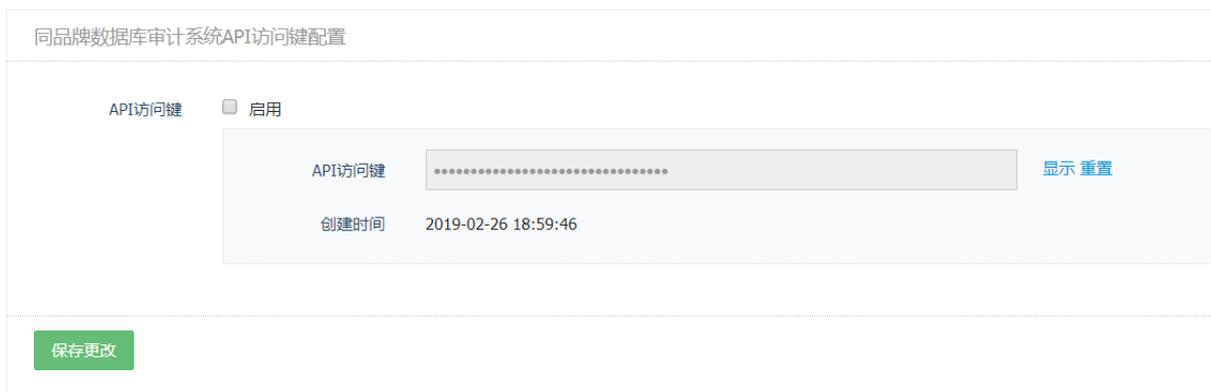
保存更改

#### 提示

勾选了生成的运维规则过期自动删除时，通过工单生成的运维规则在过期后将不会出现在主机运维页。

#### 4. 同品牌数据库审计系统 API 访问键配置

图11-62 同品牌数据库审计系统 API 访问键配置界面



#### 提示

同品牌数据库审计系统 API 访问键是用于为同品牌数据库审计开发人员提供相应应用接口

#### 5. 报表自动统计配置

开报表自动统计后，可以提升报表页面数据加载效率。

开报表自动统计后，系统会在每日 0 点后自动统计前一周期的报表数据，会消耗一定系统 CPU 资源并持续一定时间，请按需设置。。

图11-63 报表自动统计配置示意图



### 11.3.5 SSHKEY 配置

步骤1 在客户端生成私钥

步骤2 单击<上传新 DSA 私钥>或<上传新 RSA 私钥>弹出私钥上传对话框

图11-64 私钥上传对话框



### 11.3.1 改密脚本设置

改密脚本用于改密计划中通过改密脚本方式改密。适用于多个计划中的托管账户全部为同类系统中的账户时，需要通过脚本改密的情况。新增改密脚本完成后，将脚本关联任务操作步骤参见改密计划。

图11-65 改密脚本配置示意图



步骤1 新建改密脚本，单击“新建改密脚本”按钮

图11-66 新建改密脚本配置示意图

创建改密脚本

脚本名称

脚本命令

添加交互式命令 添加特殊键 帮助

#改密脚本

创建

步骤2 编辑脚本名称以及脚本命令，单击“创建”按钮

图11-67 编辑改密脚本配置示意图



步骤3 查看改密脚本

图11-68 编辑改密脚本配置示意图



密码导出设为否时，导出的文件的密码字段会置空。请根据安全需要进行配置。

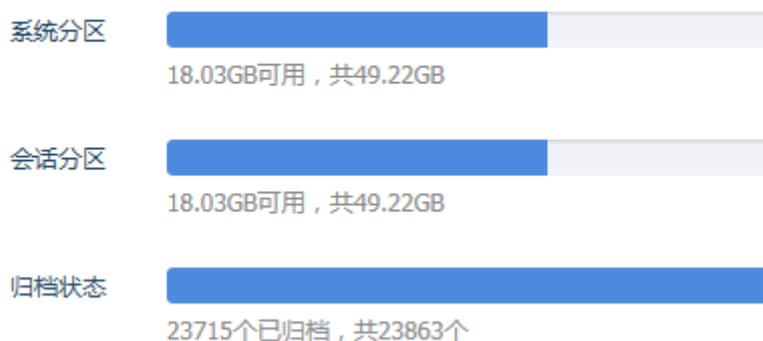
## 11.4 存储管理

### 11.4.1 数据归档

#### 1. 磁盘数据状态

图11-69 磁盘数据状态示意图

#### 磁盘数据状态



#### 2. 录像归档

可以开启或关闭录像归档功能，并且支持以 ftp 或 sftp 方式将归档数据发送到目标服务器。

图11-70 录像归档配置示意图

录像归档配置界面包含以下配置项：

- 状态**：下拉菜单，当前选择“开启”。
- 时段**：输入框显示“20 - 23”，右侧说明为“每天进行录像归档的时段，有效值0-23”。
- 速度限制**：输入框显示“0”，右侧说明为“限定录像归档时的传输速度，有效值0-100，如果设置为0，则不限制传输速度”。
- 传输模式**：下拉菜单，当前选择“FTP”。
- 服务器地址**：输入框显示“10.11.33.99”。
- 端口**：输入框显示“21”。
- 用户名**：输入框显示“hsx”。
- 密码**：输入框显示“\*\*\*\*\*”。
- 路径**：输入框显示“129归档”，右侧说明为“绝对路径或相对路径，并确保用户具有此路径的写入权限”。
- 测试用户**：按钮。
- 保存更改**：绿色按钮。

#### 3. 自动删除

可以设置自动删除多少天之前的数据。

图11-71 自动删除设置示意图

自动删除

---

自动删除  自动删除  天 前的录像

当会话分区可用空间不足  GB 时删除最早的录像  
默认值15GB。请勿轻易修改此值

删除选项  只删除已归档的录像

---

**保存更改**

#### 4. 手工删除

可根据数据类型和日期进行删除，如下图所示。

图11-72 手工删除示意图

手动删除

---

删除数据前请确保数据已经备份

选择日期  此日期之前的数据将被删除

删除内容  操作日志

系统警报

录像  只删除已归档的录像

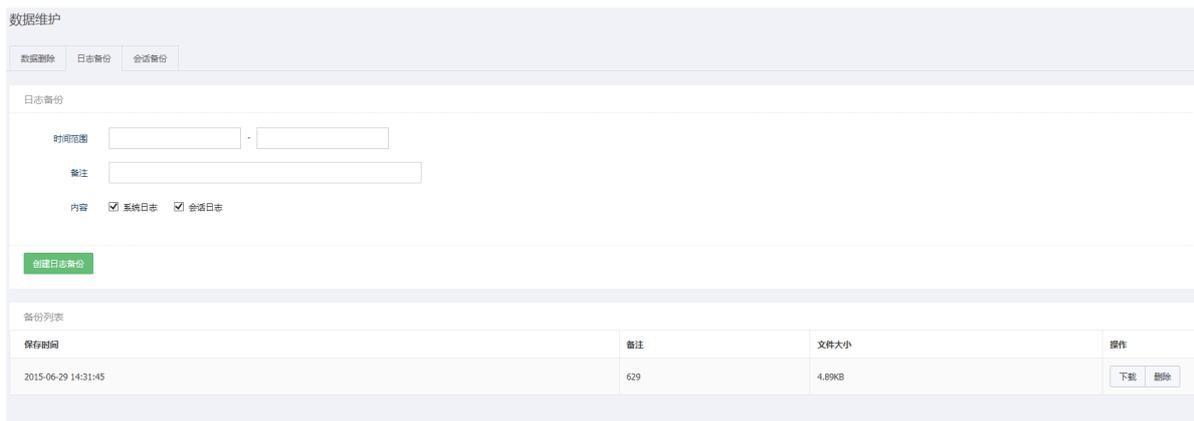
---

**删除数据**

#### 11.4.2 日志备份

步骤1 进入[系统/存储管理/日志备份]页面。选择好时间范围，编辑备注、选择好导出的内容。

图11-73 日志备份管理页面示意图



步骤2 单击<创建日志备份>即可生成备份文件。

步骤3 在备份列表单击<下载>按钮后即可将文件下载至本地查看。

### 11.4.3 磁盘管理

步骤1 进入[系统/系统维护/磁盘管理]页面。

图11-74 磁盘管理页面示意图



步骤2 单击<刷新磁盘信息>即可查看磁盘的最新状态。

步骤3 单击<磁盘检测>即可查看磁盘是否运行正常。

步骤4 单击<磁盘同步>即可将 raid 环境的下磁盘进行数据同步。

## 11.5 操作日志

步骤1 在[系统/操作日志]页面中，可搜索或导出日志。

图11-75 操作日志示意图

操作日志

操作日志 操作日志配置

时间  -

重要性

日志类型

操作结果

用户

来源IP

日志内容

重要性	时间	日志类型	日志内容	用户	来源IP	结果
中	2016-10-08 13:56:10	运维日志	监控会话: 74fd4f05788a6900000000003000005	admin	10.11.80.80	成功
低	2016-10-08 13:55:53	登录日志	登录系统	admin	192.168.50.129	成功
高	2016-10-08 13:53:40	维护日志	下载日志备份文件: log_20160802_20160803_20160803_57a15f97d99c0.zip	admin	10.11.200.40	成功
低	2016-10-08 13:42:50	登录日志	登录系统	admin	192.168.50.129	成功
中	2016-10-08 13:40:31	审计日志	会话会话: 33d55285788d5900000000003000005	admin	10.11.80.80	成功

步骤2 单击<操作日志配置>可对系统各类日志的重要性进行配置。

图11-76 操作日志配置示意图

操作日志
操作日志配置

操作日志配置

登录日志
▼

重要性	默认重要性	日志描述
低 ▼	低	登录系统
低 ▼	低	退出系统
中低 ▼	中低	登录系统, 未知系统错误
中低 ▼	中低	登录系统, 用户不存在
中低 ▼	中低	登录系统, 有效期之外登录
中低 ▼	中低	登录系统, 用户被锁定
中低 ▼	中低	登录系统, 密码错误
中低 ▼	中低	登录系统, 本地认证被禁用
中低 ▼	中低	登录系统, 远程认证被禁用
中低 ▼	中低	登录系统, 认证模式不匹配
中低 ▼	中低	登录系统, 从禁止的IP地址登录
中低 ▼	中低	登录系统, 禁止admin从Web登录
中低 ▼	中低	登录系统, 在禁止的时间段登录
中低 ▼	中低	登录系统, 连接远程认证服务器失败
中低 ▼	中低	登录系统, 认证方式未启用

保存更改

恢复默认设置

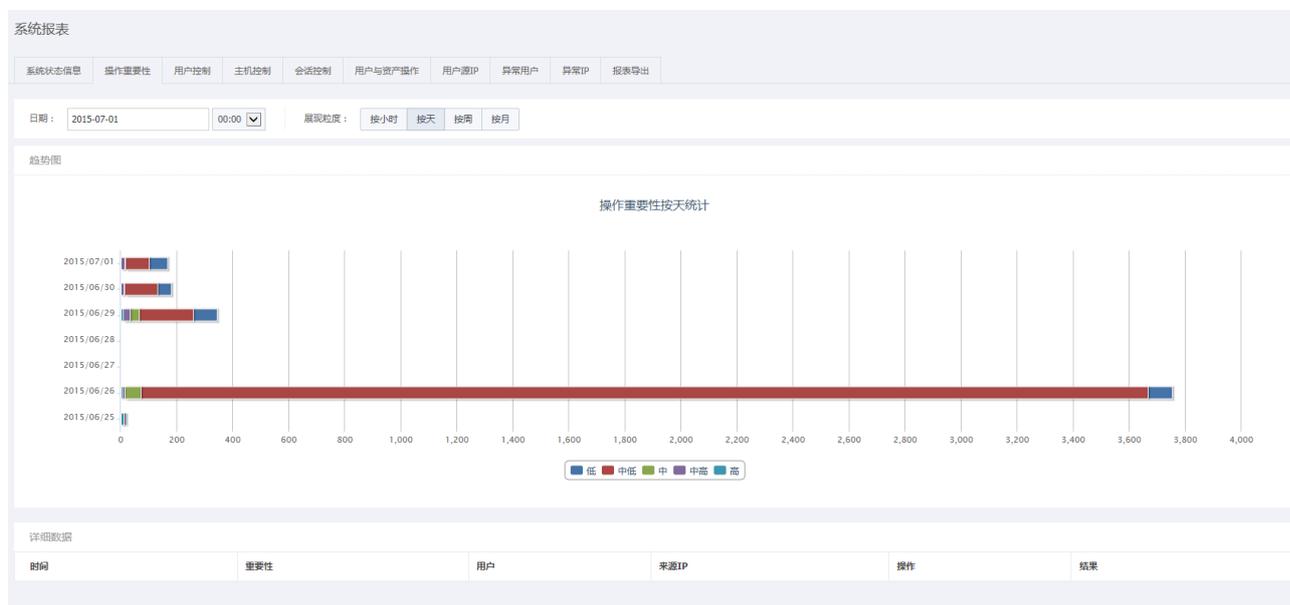
## 11.6 系统报表

系统报表是用于统计运维审计系统的日志报表。

## 11.6.1 按小时查看

步骤1 进入[系统/系统报表]页面。以“操作重要性”为例。

图11-77 系统报表示意图



步骤2 单击<按小时查看>，且设置好时间及小时。



说明

按小时查看表示查看此前近7个小时的报表信息。例如选择的是4月3日00:00，那统计的是4月2日18:00-4月3日00:00的数据。

步骤3 单击<确定>后即可查看统计的报表。

## 11.6.2 按天查看

步骤1 进入[系统/系统报表]页面。以“操作重要性”为例。

步骤2 单击<按天查看>，并且选择好日期。

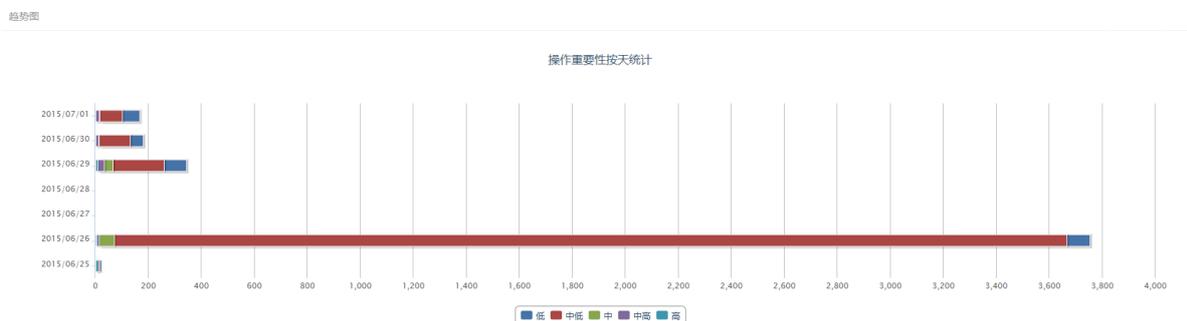


说明

按天查看表示查看此前近7天的报表信息。例如选择的是4月3日，那统计的是3月28日-4月3日的的数据。

步骤3 单击<确定>后即可查看到统计报表。

图11-78 系统报表示意图



### 11.6.3 按周查看

步骤1 进入[系统/系统报表]页面。以“操作重要性”为例。

步骤2 单击<按周查看>，并选择好日期。

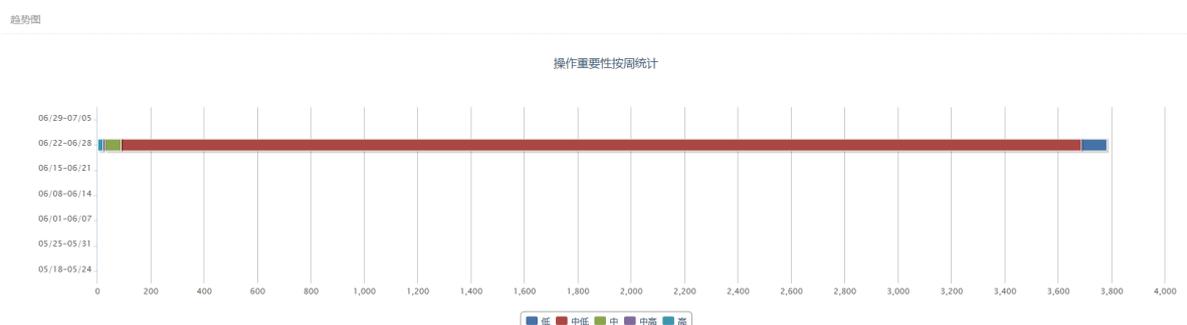


说明

按周查看表示查看此前近7周的报表信息。例如选择的是4月3日，那统计的是2月16日-4月5日的  
数据。

步骤3 单击<确定>后即可查看统计的报表。

图11-79 系统报表示意图



### 11.6.4 按月查看

步骤1 进入[系统/系统报表]页面。以“操作重要性”为例。

步骤2 单击<按月查看>，并选择好日期。

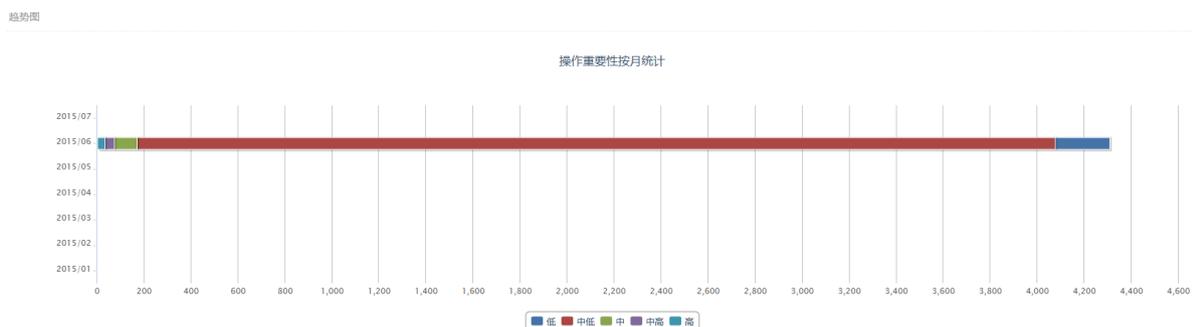


说明

按月查看表示查看此前近7个月的报表信息。例如选择的是2015年4月3日，那统计的是2014年10月-2015年4月的数据。

步骤3 单击<确定>后即可查看到统计的报表。

图11-80 系统报表示意图



### 11.6.5 导出报表

步骤1 进入[系统/系统报表]页面。

步骤2 单击<报表导出>进入配置页面。选择好周期、时间、文件格式。

图11-81 导出系统报表示意图



步骤3 单击<导出系统报表>后即可导出报表并查看。

## 11.7 本机维护

### 11.7.1 系统管理

步骤1 进入[系统/本机维护/系统管理]页面，同步浏览器时间或 ntp 时间服务器时间。

图11-82 系统时间页面示意图



步骤2 在[系统/本机维护/系统工具]页面中，可重启或关闭设备，以及恢复出厂设置。

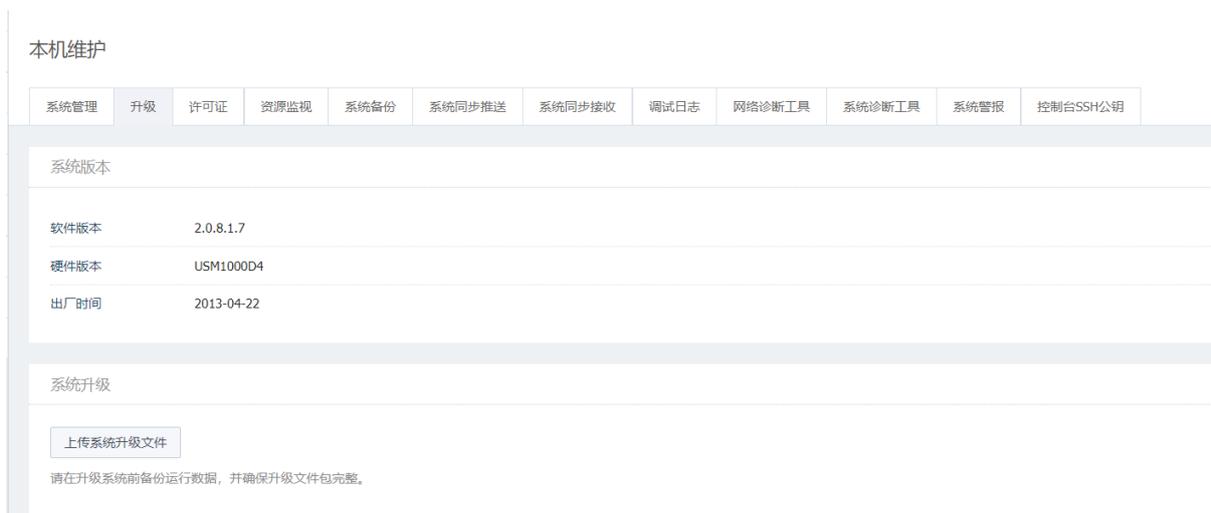
图11-83 系统工具相关配置



### 11.7.2 升级管理

步骤1 进入[系统/本机维护/升级]页面，在系统版本下可以查看本机的版本及出厂时间。

图11-84 系统升级页面示意图



步骤2 在系统升级下单击上传系统升级文件，选择升级文件上传。

图11-85 系统升级相关配置



### 11.7.3 许可证

在[系统/本机维护/许可证]页面中可进行许可证申请文件的生成，许可证文件的导入和备份。

图11-86 许可证管理界面



- 步骤1 单击<生成系统认证文件>, 可生成许可证申请文件, 用该文件向相关人员申请许可证文件。
- 步骤2 单击<备份许可证>, 可将当前许可证文件导出到本地保存。
- 步骤3 拿到新的许可证文件后, 单击<导入许可证>, 可将已申请的许可证文件从本地上传到系统。

### 11.7.4 资源监视

在[系统/本机维护/资源监视]页面中, 可查看系统资源状态, 如 cpu 使用率、内存使用率、网络情况等。

图11-87 资源监视界面



## 11.7.5 系统备份

### 1. 手动备份

步骤1 进入[系统/本机维护/系统备份]页面，编辑备注。

图11-88 系统配置手动备份页面示意图

### 系统配置手动备份

---

备注

---

创建系统配置备份

步骤2 单击<创建系统配置备份>后备份列表中即可产生备份信息。

### 2. 自动备份

步骤1 在自动备份区填写备份周期，备份保留数目。

图11-89 系统配置自动备份示意图

系统配置自动备份

---

状态

周期   有效值1-60

保留   有效值1-180，当自动备份数量超过此限制时会自动删除最早备份

下次执行时间

上次执行时间 2015-07-02 00:00:25

---

步骤2 设置信息填写完成后，单击<保存更改>即可。

### 3. 备份下载

步骤1 进入[系统/本机维护/系统备份/备份列表]页面。

步骤2 单击<下载>后即可下载备份文件至本地。

### 4. 备份还原

步骤1 进入[系统/本机维护/系统备份/备份列表]页面。

步骤2 单击<还原>后即可将备份的文件恢复还原至系统中。

### 5. 上传还原

步骤1 进入[系统/本机维护/系统备份/系统配置还原]页面。

图11-90 系统配置还原示意图

系统配置还原

---

请在还原系统配置前先进系统配置备份，并确保上传的备份文件完整。

单击<上传系统配置文件>后即可将系统配置备份的文件恢复还原至系统中。

## 11.7.6 系统同步推送

开启系统配置推送，系统将按照设定的推送周期向目标设备推送本设备的系统配置。

步骤1 开启推送功能，设置推送周期和推送密钥。

图11-91 系统配置推送示意图

系统配置推送

---

状态

推送周期  分钟

推送密钥  [显示](#) [重置](#)

密钥创建时间 2016-01-21 15:30:38

---

[保存更改](#)



提示

单击上图的重置即可设置推送密钥，推送设备上设置的推送密钥，在接收设备设置接收配置时会用到。

步骤2 添加推送目标，即接收设备。

添加推送目标

---

名称

目标IP

Web端口

---

[添加目标](#)

步骤3 查看推送目标。

步骤4 可以在目标列表中进行手动推送系统配置，也可删除推送目标。

图11-92 推送目标列表

推送目标列表

名称	目标IP	Web端口	上次推送时间	推送结果	
138	192.168.50.138	443			<input type="button" value="手动推送"/> <input type="button" value="删除"/>

### 11.7.7 系统同步接收

步骤1 在接收设备上设置源设备（即推送设备）的密钥，开启接收功能即可接收推送设备推送的系统配置。

图11-93 系统配置接收示意图

系统配置接收

状态

关闭 ▼

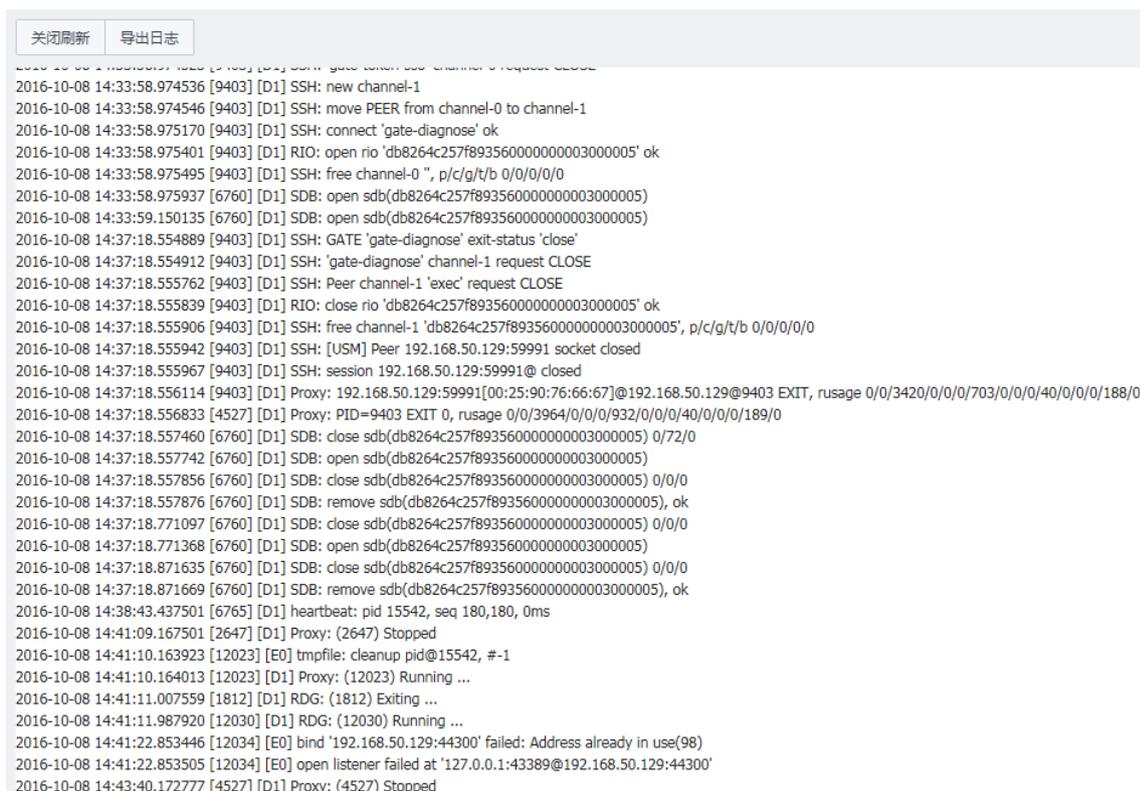
源设备密钥显示

保存更改

### 11.7.8 调试日志

步骤1 进入[系统/本机维护/调试日志]页面。

图11-94 调试日志页面示意图



步骤2 单击<关闭刷新>即可暂停调试日志的更新。

步骤3 单击<导出日志>即可将调试日志导出查看。

## 11.7.9 网络诊断工具

### 1. 连通性检测

步骤1 进入[系统/系统维护/网络诊断/连通性检测]页面。可以检测主机的 IP 或端口是否连通、路由是否可达、TCP 端口、UDP 端口。

图11-95 连通性检测功能示意图

## 连通性检测

类型	PING <input type="button" value="v"/>
主机地址	10.11.200.10
<input type="button" value="执行测试"/>	
<pre> PING 10.11.200.10 (10.11.200.10) 56(84) bytes of data.  64 bytes from 10.11.200.10: icmp_seq=1 ttl=63 time=0.499 ms  64 bytes from 10.11.200.10: icmp_seq=2 ttl=63 time=0.435 ms  64 bytes from 10.11.200.10: icmp_seq=3 ttl=63 time=0.429 ms  64 bytes from 10.11.200.10: icmp_seq=4 ttl=63 time=0.449 ms  --- 10.11.200.10 ping statistics ---  4 packets transmitted, 4 received, 0% packet loss, time 3000ms  rtt min/avg/max/mdev = 0.429/0.453/0.499/0.027 ms           </pre>	

步骤2 单击<执行>后即可自动检测出主机的是否连通。

### 2. TCPDump 抓包

步骤1 进入[系统/系统维护/网络诊断/TCPDump 抓包]页面。设置抓包的 IP 或端口，抓包的数量。

图11-96 TCPDump 抓包功能示意图

## TCPDUMP抓包

主机IP	<input type="text"/>
端口	<input type="text"/> 1-65535之间的有效端口号
包数量	<input type="text" value="5000"/> 内置的TCPDump每次可以抓取最多5000个数据包
<input type="button" value="开始"/> <input type="button" value="停止"/>	

步骤2 单击<开始>后即可开始抓包。

步骤3 单击<停止>后即可停止抓包，并在右侧显示<下载>按钮。

图11-97 TCPDump 抓包功能示意图

主机IP  ✕

端口  1-65535之间的有效端口号

包数量  内置的TCPDump每次可以抓取最多5000个数据包

步骤4 单击<下载>按钮即可将文件下载至本地，使用 wireshark 软件查看。

步骤5 单击<删除>按钮可将抓包文件删除

### 11.7.10 系统诊断工具

在[系统/本机维护/系统诊断工具]页面中可查看系统各设备信息和前十个进程。

图11-98 系统诊断示意图



## 11.7.11 系统警报

步骤1 进入[系统/系统维护/系统警报]页面。

图11-99 系统警报页面示意图

时间	警报内容	确认时间	确认者
<input type="checkbox"/> 2016-10-08 15:50:02	内存负载超过 1%		
<input type="checkbox"/> 2016-10-08 15:50:02	CPU负载超过 1%		
<input type="checkbox"/> 2016-10-08 15:45:01	内存负载超过 1%		
<input type="checkbox"/> 2016-10-08 15:40:01	内存负载超过 1%		
<input type="checkbox"/> 2016-10-08 15:40:01	CPU负载超过 1%		

步骤2 单击<确认警报>后，表示已经处理了警报日志。

## 11.7.1 控制台 SSH 公钥

控制台 SSH 公钥适用于此刻需要登录堡垒机控制台但此时无法连接设备串口时的场景。

重置控制台 SSH 公钥会自动重新生成一对 SSH 密钥，系统会保存公钥并显示私钥的内容，但不会保存私钥，请妥善保管好私钥。

步骤1 进入[系统/系统维护/控制台 SSH 公钥]页面。

图11-100 控制台 SSH 公钥页面示意图

本机维护

系统管理 升级 许可证 资源监视 系统备份 系统同步推送 系统同步接收 调试日志 网络诊断工具 系统诊断工具 系统警报 控制台SSH公钥

控制台SSH公钥

指纹 21:fe:b7:70:fc:a5:21:5a:71:e9:54:d3:7c:4b:4c:ca

控制台SSH公钥

```
ssh-dss AAAAB3NzaC1kc3MAAACBAN1ioT1ysju+m3VCn8ZQ8n1e0um8VOLIrnXV5i0
dAkx3RHylQ85FYFFHreUFeQF/165ULn91TPAuAA06MzyBzXH4G2dmu1zsciqAedAmd
z3j8HSrOBx171KgEVnoK3blygaMr-b9vn/LyWMTNCD/aIkY5rYZWQHk1e1TOJLzD5A
AAAFQDqQC86fY0dkuGjcxU0HKQZaySWQAAAIEA1OZ/HUyVhoRyS2NYxL+Ju1eQntdz
zLEdP0p6D7CoP1yKsIXwJYAn8sKuN6tg8YCNP9b1Z9jfP55htz4Hdx8Y2uVNT1pB7I
W2aD195Y5oDq6fMOcxRDUpf/G/juLD0jFzFGmq7w1WwFvYWuHddPOF4yUdbZ61VQgMO
x9K5fGyZIAAACBALdzUe3kpm5x4k5F1hf+AJn1V9xBZJA0RCP4wuhqyhFAMJwG7Ww9
dY5ZLzFEcdDQ/o1n8nb6N8ghwYQysrcy+Y1EG7B1S7f18jxu/L7omP7TN26wQ55bt
yZ1Wro7hVdxcK2Au0rNoGoHJA6U38PFRRCav/Lqm56AFqK0pra8N comment
```

重置控制台SSH公钥

步骤2 单击重置控制台 SSH 公钥，在弹出的提示框中单击“确定”。

图11-101 控制台 SSH 公钥页面示意图

重置控制台SSH公钥会自动重新生成一对SSH密钥，系统会保存公钥并显示私钥的内容，但不会保存私钥，请妥善保管好私钥。是否确定要重置控制台SSH公钥？