



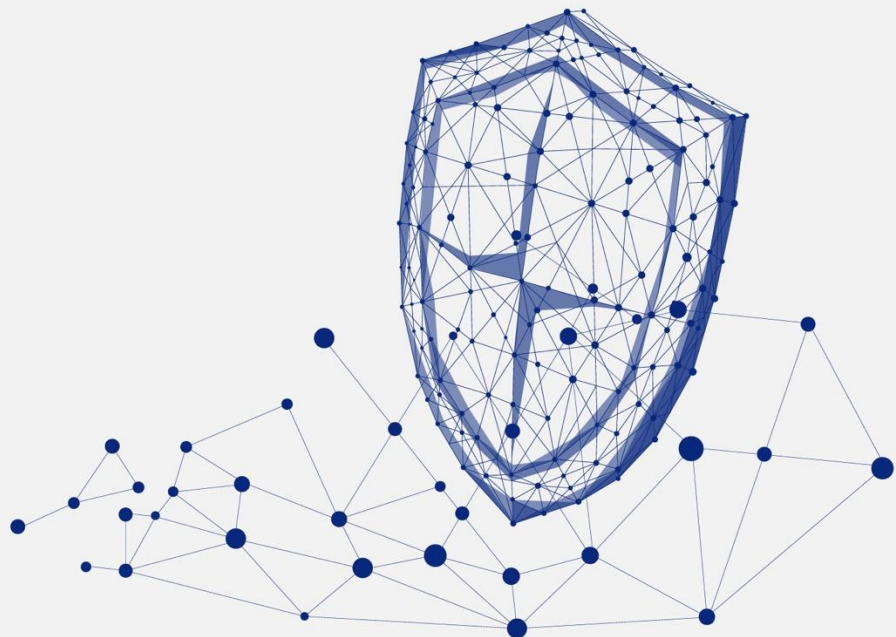
# 明御® 运维审计与风险控制系统

V2.0.8.2.6

## 用户手册

文档版本：01

发布日期：2020-03-26



本文中出现的任何文字描述、文字格式、插图、照片、方法等内容，除另有特别注明，版权均属杭州安恒信息技术股份有限公司（简称“安恒信息”）所有，受到有关产权及版权法保护。任何个人、机构未经安恒信息的书面授权许可，不得以任何方式复制或引用本文的任何片段。

经授权使用本文中内容的单位或个人，应在授权范围内使用，并注明“来源：安恒信息”。违反上述声明者，安恒信息保留追究其法律责任的权利。

除杭州安恒信息技术股份有限公司的商标外，本手册中出现的其他商标、产品标识及商品名称，由各自权利人拥有。

This file is restricted to the personal use of 159\*\*\*\*1510 time: 2020-4-13  
source: bbs.dbappsecurity.com.cn

## 文档说明

产品名称		明御®运维审计与风险控制系统	
适用平台/版本		V2.0.8.2.6	
拟制人	侯汉书（400-文档）	拟制人	吴焱/武朝阳（网关-堡垒机）
发布人	侯汉书（400-文档）	发布人	受控文档

## 修订记录

日期	修订版本	修改记录	修改人
2020-03-26	01	初次发布	詹孝龙（400-文档）

This file is restricted to the personal use of 159\*\*\*\*1510 time: 2020-04-13  
 source: bbs.dbappsecurity.com.cn

# 目录

前言.....	I
一. 快速入门.....	1
1.1 产品简介.....	1
1.2 角色与权限说明.....	2
1.3 登录设备.....	3
1.3.1 通过 CLI 配置.....	3
1.3.2 通过 Web 配置.....	4
1.4 主要业务流程.....	5
二. WEB 配置界面简介.....	6
2.1 使用向导.....	6
2.2 个人信息.....	7
2.3 工具下载.....	9
三. 控制板.....	10
3.1 资源统计.....	10
3.2 运维统计.....	10
3.2.1 系统状态.....	11
四. 部门.....	12
4.1 新建部门.....	12
4.2 安全码管理.....	12
4.3 删除部门.....	13
五. 用户.....	14
5.1 用户管理.....	14
5.1.1 新建用户.....	14
5.1.2 导入用户.....	15
5.1.3 用户配置.....	16
5.1.4 SSH 公钥管理.....	17
5.1.5 查看已授权主机.....	18

5.1.6 查看已授权应用.....	18
5.2 用户组管理.....	18
5.3 动态令牌管理.....	19
5.4 USBKEY 管理.....	20
5.4.1 签发管理员 USBKEY.....	20
5.4.2 签发用户 USBKEY .....	21
5.5 第三方 USBKEY.....	21
<b>六. 资产.....</b>	<b>24</b>
6.1 主机管理 .....	24
6.1.1 新建主机.....	24
6.1.2 导入主机 .....	26
6.1.3 编辑主机 .....	27
6.2 混合云管理.....	29
6.2.1 对私有云资源进行管理 .....	29
6.2.2 对公有云资源进行管理.....	31
6.3 共享帐户管理.....	32
6.4 主机组管理.....	33
6.5 帐户组管理.....	34
6.6 应用管理 .....	35
6.7 应用组管理.....	37
<b>七. 授权.....</b>	<b>39</b>
7.1 运维规则 .....	39
7.1.1 新建运维规则 .....	39
7.1.2 编辑运维规则 .....	40
7.2 审批规则 .....	44
7.3 未授权登录审核 .....	46
<b>八. 审计.....</b>	<b>47</b>
8.1 会话审计 .....	47

8.2 审计规则 .....	49
<b>九. 工单 .....</b>	<b>51</b>
9.1 创建工单 .....	51
9.2 工单审批 .....	52
<b>十. 运维 .....</b>	<b>53</b>
10.1 主机运维 .....	53
10.1.1 全局配置 .....	53
10.1.2 主机运维 .....	55
10.1.3 应用运维 .....	59
10.2 实时监控 .....	60
10.3 命令审批 .....	61
10.4 运维审批 .....	62
10.5 运维报表 .....	62
10.5.1 查看运维报表 .....	62
10.5.2 导出报表 .....	63
10.5.3 报表自动发送 .....	63
<b>十一. 任务 .....</b>	<b>65</b>
11.1 改密计划 .....	65
11.2 自动运维 .....	67
<b>十二. 系统管理 .....</b>	<b>70</b>
12.1 网络配置 .....	70
12.1.1 基础设置 .....	70
12.1.2 Web 配置 .....	71
12.1.3 HA 配置 .....	72
12.1.4 静态路由 .....	73
12.1.5 SNMP 配置 .....	74
12.1.6 集群配置 .....	74
12.1.7 IP 源防护 .....	75

12.2 VPN 管理 .....	76
12.3 认证管理 .....	77
12.3.1 安全配置.....	77
12.3.2 远程认证 .....	79
12.3.3 双因子认证.....	80
12.3.4 第三方 HTTP 平台认证.....	82
12.4 系统配置 .....	84
12.4.1 运维配置.....	84
12.4.2 告警配置 .....	86
12.4.3 语言和界面 .....	88
12.4.4 功能设置 .....	89
12.4.5 SSH KEY 配置 .....	91
12.4.6 改密脚本 .....	92
12.5 存储管理 .....	92
12.5.1 数据归档.....	92
12.5.2 日志备份 .....	94
12.5.3 磁盘管理 .....	94
12.6 操作日志 .....	95
12.7 系统报表 .....	96
12.8 本机维护 .....	97
12.8.1 系统管理.....	97
12.8.2 系统升级 .....	98
12.8.3 许可证 .....	99
12.8.4 资源使用率.....	99
12.8.5 系统备份 .....	100
12.8.6 系统同步推送/接收 .....	102
12.8.7 调试日志 .....	103
12.8.8 网络诊断工具.....	104

12.8.9 系统诊断工具.....	105
12.8.10 系统警报 .....	106
12.8.11 控制台 SSH 公钥.....	106

This file is restricted to the personal use of 159\*\*\*\*1510 time: 2020-04-13  
source: bbs.dbappsecurity.com.cn

感谢您选择安恒信息的网络安全产品。本手册对安恒信息明御®运维审计与风险控制系统（以下简称“DAS-USM”）的使用与配置做了详细的介绍，包括快速入门、Web 配置界面简介、控制板、部门、用户、资产、混合云管理、授权、审计、运维、任务、系统管理等。

手册所提供的内容仅具备一般性的指导意义，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号、配置文件不同等原因，手册中所提供的内容与用户使用的实际设备界面可能不一致，请以用户设备界面的实际信息为准，手册中不再针对前述情况造成的差异一一说明。

出于功能介绍及配置示例的需要，手册中可能会使用 IP 地址、网址、域名等。如无特殊说明上述内容均为示意，不指代任何实际意义。

## 预期读者

本文档主要适用于使用 DAS-USM 系统的用户，超级管理员、部门管理员、运维管理员、审计管理员、运维员、审计员、系统管理员和密码管理员。不同角色的用户所具有的的权限不同，请以实际情况为准。本文假设读者对以下领域的知识有一定了解：





- ◆ UDP、TCP/IP、SNMP 等基础网络通讯协议
- ◆ 数据库、服务器、路由器、交换机等常见设备（系统）的基本工作原理和配置、操作
- ◆ 堡垒机及网络安全运维工具的基本工作原理

## 格式约定

本手册内容格式约定如下：

内容	说明
提示	有助于理解内容的提示或说明信息，或需要特别注意的事项和重要信息。
黑体字	WebUI 界面上的菜单或标签页，例如，“在导航栏中选择‘系统监控>系统状态’，查看接口状态标签”。
< >	WebUI 界面上的按钮名称、复选框名称、文本框名称、选项名称等。例如，“改变 MTU 值，选中<手动>按钮，然后在文本框中输入合适的值”。
>	介绍 WebUI 的操作步骤时，用于隔离点击对象（菜单项、子菜单、按钮以及链接等），例如，“通过‘安全防护>网络层攻击防护>Flood 攻击防御>目的 IP 防御’菜单打开显示页面，点击<新建>按钮”。

本手册图标格式约定如下：

内容	说明
	提示，操作小窍门，方便用户解决问题。
	说明，对正文内容的补充和说明。
	注意，提醒操作中的注意事项，不当的操作可能会导致设备损坏或数据丢失。
	警告，该图表后的内容需引起格外重视，否则可能导致人身伤害。

## 获得帮助

请访问安恒社区 <https://bbs.dbappsecurity.com.cn/> 获取更多文档。

使用过程中如遇到任何问题，请致电服务热线 400-6059-110。

### 联系信息

地址：浙江省杭州市滨江区西兴街道联慧街 188 号安恒大厦

邮编：310052

电话：0571-88380999

传真：0571-28863666

官网：<http://www.dbappsecurity.com.cn/>

邮箱：[400-doc@dbappsecurity.com.cn](mailto:400-doc@dbappsecurity.com.cn)

# 一. 快速入门

## 1.1 产品简介

DAS-USM 是一款统一安全管理与审计产品，分为硬件版和云上版两种。两种版本的功能基本相同，用户可根据需要进行购买。产品集身份认证（Authentication）、帐户管理（Account）、控制权限（Authorization）、日志审计（Audit）功能于一体。支持多种字符终端协议、文件传输协议、图形终端协议、远程应用协议的安全监控与历史查询，具备全方位运维风险控制能力，可满足各类法律法规（如等级保护、赛班斯法案 SOX、PCI、企业内控管理、分级保护、ISO/IEC 27001 等）对运维审计的要求。

DAS-USM 支持的主要功能请参见下表。

功能	描述
<b>认证&amp;授权</b>	
双因子认证	<ul style="list-style-type: none"> <li>◆ 内置手机 APP 认证（谷歌动态口令验证）、OTP 动态令牌、USBkey 双因素认证引擎。</li> <li>◆ 提供短信认证、AD、LDAP、RADIUS 认证接口。</li> <li>◆ 支持多种认证方式组合。</li> </ul>
权限管理	系统预置多种用户角色：超级管理员、部门管理员、运维管理员、审计管理员、运维员、审计员、系统管理员和密码管理员。每种用户角色的权限均不同。
集中授权	梳理用户与主机之间关系，提供一对一、一对多、多对一、多对多的灵活授权模式。
单点登录	托管主机的帐户和密码，运维人员直接点击<登录>即可成功自动登录到目标主机中进行运维操作，无需输入主机的帐户和密码。
自动学习	运维人员通过 DAS-USM 成功登录目标主机后即可自动录入主机信息，减轻管理员配置主机信息、用户与主机关系的工作量。
<b>运维&amp;审计</b>	
运维协议支持	<ul style="list-style-type: none"> <li>◆ 支持管理 Linux/Unix 服务器、Windows 服务器、网络设备（如思科/H3C/华为等）、文件服务器、web 系统、数据库服务器、虚拟服务器、远程管理服务器等。</li> <li>◆ 兼容 Xshell、XFTP、SecureCRT、MSTSC、VNC Viewer、Putty、WinSCP、FlashFXP、SecureFX、OpenSSH 等多种客户端工具。</li> </ul>
统一审计	<ul style="list-style-type: none"> <li>◆ 对所有操作进行详细记录，提供综合查询；审计日志可在线或离线播放，自动备份归档。</li> <li>◆ 审计内容包括图形、字符、文件、应用、SQL 语句等会话及应用会话。</li> </ul>
浏览器客户端运维	<ul style="list-style-type: none"> <li>◆ 基于 H5 技术实现浏览器客户端运维，无需安装本地工具，直接通过浏览器打开运维界面。</li> <li>◆ 支持通过 SSH、Telnet、Rlogin、RDP、VNC 协议的 web 客户端运维。</li> </ul>
文件传输审计	<ul style="list-style-type: none"> <li>◆ 记录所有操作会话，包括在线监控、实时阻断、日志回放、起止时间、来源用户、来源 IP、目标设备、协议/应用类型、命令记录、操作内容。</li> <li>◆ 完整备份传输文件，为上传恶意文件、拖库、窃取数据等危险行为提供查询依据。</li> </ul>

功能	描述
自动运维	实现自动化的运维任务并将执行结果通知相关人员。
资产管理	支持主机、主机组、混合云、账号、账号组、应用等多种资产类型。
命令控制	集中命令控制基于不同主机、不同用户设置不同的命令控制策略，包括命令阻断、命令黑名单、命令白名单、命令审核四种动作。
工单流程	操作人员向管理员申请需要访问的设备，选择条件包括设备 IP、设备帐户、运维有效期、备注事由等，运维工单以邮件方式通知管理员。
<b>其他</b>	
系统自审	对系统自身变化信息进行审计，形成系统分析报表。
产品联动	与同品牌数据库审计系统进行联动，将通过 SSH/RDP 等加密方式操作数据库的行为整合到数据库审计中，实现数据库行为的统一集中查询、展示、审计分析。
冗余架构	<ul style="list-style-type: none"> <li>◆ 硬件采用 CF 卡和机械硬盘“双存储架构”。</li> <li>◆ 结合端口聚合技术、RAID 技术和 HA 技术，实现三重冗余备份的高可用架构。</li> </ul>
API 接口	<ul style="list-style-type: none"> <li>◆ 提供用户、资产、授权的增删改查等 API 接口。</li> <li>◆ 允许第三方平台调用 API 接口，实现用户、资产、权限自动同步。</li> </ul>

## 1.2 角色与权限说明

不同角色的用户具有的权限请参见下表（“√”表示支持，“-”表示不支持）。

	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
部门管理	√	√	-	-	-	-	-	-
安全码管理	√	√	√	√	-	-	-	-
用户管理	√	√	√	-	√	-	-	-
用户组管理	√	√	√	-	-	-	-	-
动态令牌	√	√	√	-	√	-	-	-
USBKEY 管理	√	√	√	-	√	-	-	-
资产管理	√	√	√	-	-	-	-	-
授权管理(运维规则审批、工单审批)	√	√	√	-	-	-	-	-
会话审计	√	√	-	-	√	-	基于审计规则	-
审计规则管理	√	√	-	-	√	-	-	-
主机运维	√	√	√	√	√	√	√	√
实时监控	√	√	√	-	-	-	-	-
任务计划	√	√	√	-	-	-	-	-
系统管理	√	-	-	-	-	-	-	√

## 1.3 登录设备

设备安装上架并连接网线、电源后，超级管理员需登录设备进行功能配置。DAS-USM 支持本地与远程两种配置方法，分别通过 CLI 和 Web 方式进行配置。CLI 支持 Console、Telnet、SSH 等主流通信管理协议。



云上版本仅支持 Web 方式配置。

设备出厂时设置的默认管理口地址 172.16.1.2/24，默认的管理员用户名为 admin，密码为 1q2w3e，登录后请及时修改密码。

### 1.3.1 通过 CLI 配置

请参见以下步骤搭建 DAS-USM 的 Console 口配置环境：

- 步骤1. 请自备配置线缆，将配置线缆的 USB 插头与 PC 的 USB 接口相连。
- 步骤2. 将配置线缆的 RJ-45 插头与设备的 Console 口相连。
- 步骤3. 在 PC 上运行终端仿真程序（如 PuTTY、SecureCRT 等），并按如下表所示设置参数。

参数	数值
波特率	115200 bit/s
数据位	8
奇偶校验	无
停止位	1
数据流控制	无

- 步骤4. 打开电源开关，设备会进行自检并且自动进行初始化配置。如果系统启动成功，会出现以下登录提示。

```

USM0200C1/v2.0.8.2.6 2019-12-03 09:58:32
明御运维审计与风险控制系统控制台

用户名 : admin
密码 : █
    
```

- 步骤5. 在登录提示后输入默认用户名并按回车键，之后输入默认密码并按回车键，此后便可登录系统的 CLI 配置界面。

## 1.3.2 通过 Web 配置



本文仅以硬件版举例说明，云上版需保证配置 PC 和 DAS-USM 路由可达即可。

管理员可登录到设备的 Web 管理平台进行配置。具体方法如下：

**步骤1.** 将 PC 的 IP 地址设置为与 172.16.1.2/24 同网段的 IP 地址，并用网线将 PC 和设备的以太网接口连接起来。

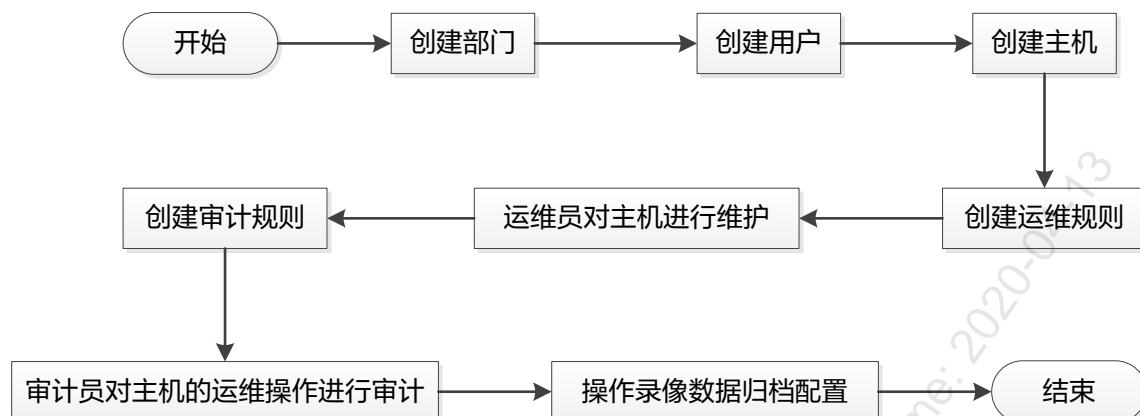
**步骤2.** 在 PC 的浏览器（推荐使用 Chrome 69 及以上版本或者 IE 11 及以上版本浏览器）地址栏中输入“https://172.16.1.2”并按回车键，进入 Web 管理平台登录页面。



**步骤3.** 输入默认用户名、密码，点击<登录>登录到设备的 Web 管理平台主界面。

## 1.4 主要业务流程

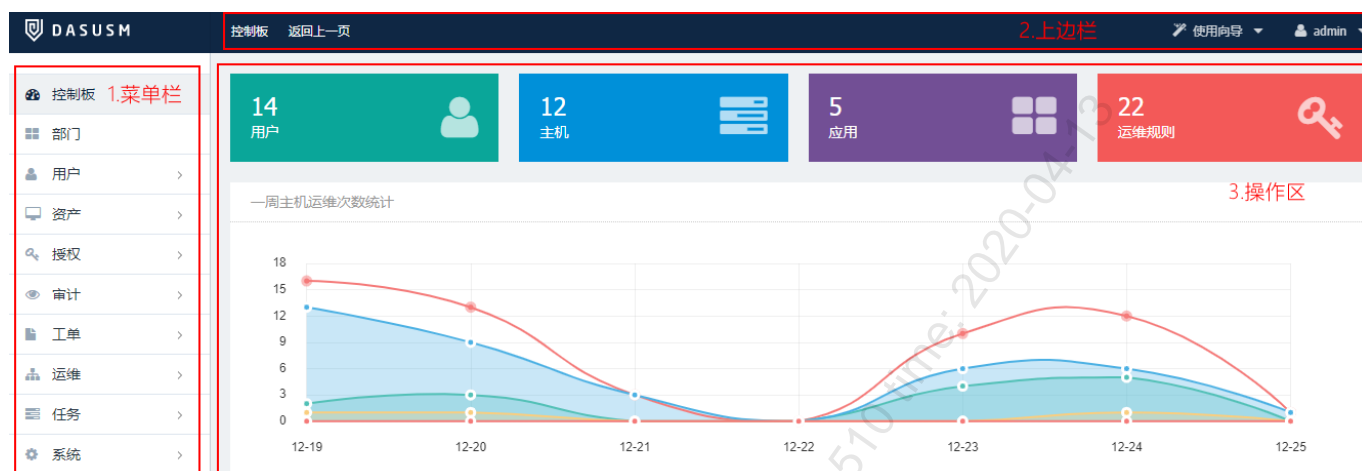
系统的主要业务流程如下图所示。



- 1.创建部门：超级管理员或部门管理员创建部门。详情请参见[新建部门](#)。
- 2.创建用户：创建系统用户，包括运维员等。详情请参见[新建用户](#)。
- 3.创建主机：将主机添加至系统后，系统才能对主机的运维进行审计。详情请参见[主机管理](#)。
- 4.创建运维规则：授权运维员可以登录主机进行运维。详情请参见[运维规则](#)。
- 5.运维员对主机进行维护：运维员通过系统登录主机并对主机进行维护。详情请参见[主机运维](#)。
- 6.创建审计规则：审计管理员创建审计规则，赋予审计员审计主机的权限。详情请参见[审计规则](#)。
- 7.审计员对主机的运维操作进行审计：审计员进行会话审计。详情请参见[会话审计](#)。
- 8.操作录像数据归档配置：对会话录像进行归档。详情请参见[数据归档](#)。

## 二. Web 配置界面简介

设备 Web 配置页面包含三个部分：1.菜单栏；2.上边栏；3.操作区，如下图所示。



### 2.1 使用向导

超级管理员和部门管理员可通过<使用向导>功能，快速配置系统业务。



步骤1. 创建用户，即在 DAS-USM 上新增用户及其登录密码，更多信息请参见[新建用户](#)。

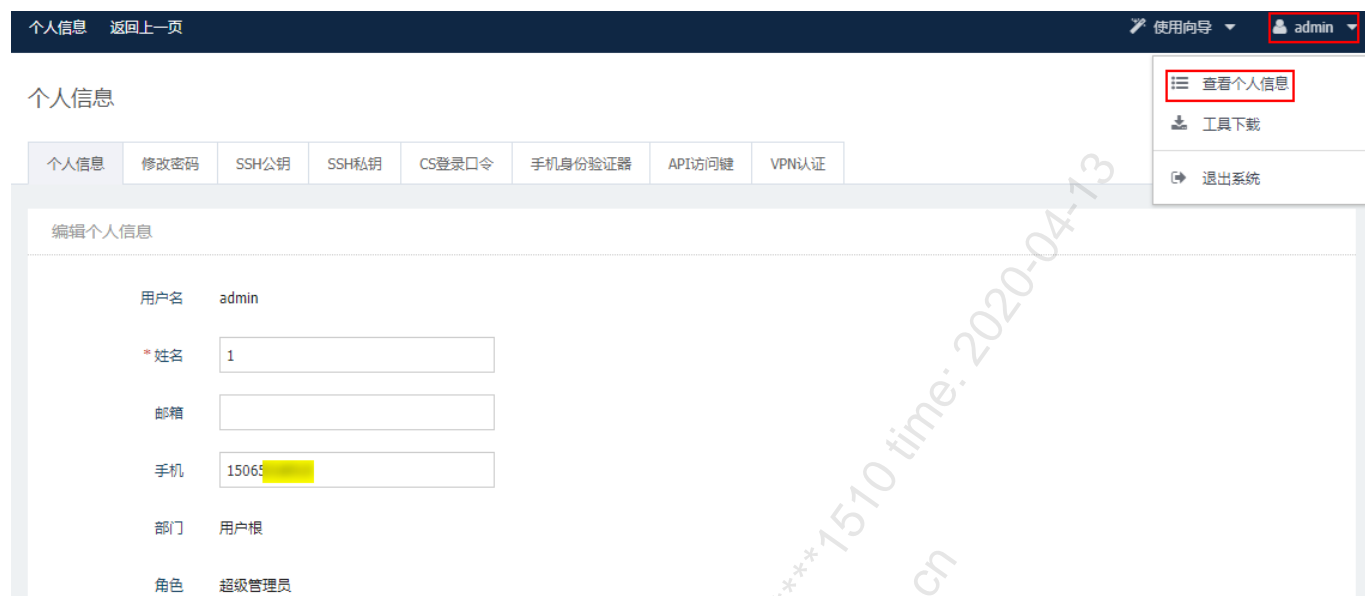
步骤2. 创建主机，即用户所要运维的设备，更多信息请参见[新建主机](#)。

步骤3. 创建运维规则，即绑定用户与主机之间的授权关系，更多信息请参见[新建运维规则](#)。

步骤4. 数据归档配置，即会话的录像进行管理，更多信息请参见[存储管理](#)。

## 2.2 个人信息

在上边栏点击当前用户名，从下拉菜单选择<查看个人信息>进入个人信息页面。



用户可在该页面执行以下操作。

操作选项	说明
编辑个人信息	查看当前登录用户身份的详细信息，编辑其中部分选项。
修改密码	修改当前用户的登录密码。
SSH 公钥	添加或编辑 SSH 公钥。SSH 公钥用于支持用户通过 SSH 协议连接 DAS-USM。更多信息请参考 <a href="#">用户管理</a> 的 SSH 公钥管理部分。
SSH 私钥	添加或替换 SSH 私钥。SSH 私钥用于使用 SSH 协议登录主机。
CS 登录口令	设置 CS 登录口令。CS 登录口令用于通过 FTP、Oracle 客户端、RDP 网关登录。
手机身份验证器	手机身份验证器用于支持用户通过手机 APP 口令的方式登录到设备。 可通过以下步骤完成手机 APP 验证设置：

1. 在个人信息页面的手机身份验证器标签页下，下载适用的验证器程序并安装到手机。



2. 点击<设置验证器>或<重置验证器>。



3. 在手机上打开验证器程序，扫描 DAS-USM 所示二维码，根据提示完成操作。

操作选项	说明
API 访问键	<p>勾选复选框启用 API 访问键。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。</p> <p>API 访问键是系统 API 服务的认证凭据，API 通过 AccessToken 来验证请求发送者的身份，AccessToken 根据用户账号进行区分，每个账号提供的 AccessToken 拥有对该账号下资源的完全权限。</p> <p>用户以个人身份发送请求时，需要首先在发送的请求 Headers 中添加 AccessToken 字段，并设置有效访问键值；系统收到请求后，会通过 AccessToken 找到对应的用户，以同样的方法提取验证码，如果计算出的验证码与一致，即认为该请求是有效的；否则，系统将拒绝处理请求，并返回 HTTP 403 错误。</p>
VPN 认证	<p>查看 VPN 的服务状态及认证方式，管理个人 SSL 证书。DAS-USM 内置 SSL VPN 功能，实现远程运维的安全接入，堡垒机与 VPN 功能的二合一可以降低用户的拥有成本。有关 VPN 配置的更多信息，请参见 <a href="#">VPN 管理</a>。</p>

## 2.3 工具下载

在上边栏点击当前用户名，从下拉菜单选择<工具下载>进入工具下载页面，根据需要下载运维及审计中的常用工具。

The screenshot shows the '工具下载' (Tools Download) page in the DAS-USM interface. The page title is '工具下载 返回上一页'. The left sidebar contains navigation options: 控制版, 用户, 资产, 授权, 审计, 工单, 运维, 任务, 系统. The main content area is titled '工具下载' and includes a notice: '如果需要购买授权, 需要用户自行购买'. Below this, there is a section for '运维及审计工具' (Operation and Audit Tools) with the following table:

名称	下载
单点登录器 运维登录必备工具	本地下载
应用加载器 应用中心IE菜单自动代理必备工具	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
VPN客户端 VPN连接必备工具	本地下载
Adobe AIR 离线播放器运行环境 (推荐版本 4.0)	官方网站
Flash Player 12 Flash播放器, 页面上传/下载按钮, 播放审计会话的依赖插件 (推荐版本 Flash Player 12.0.0.77)	官方网站

At the bottom of the page, there is a '浏览器' (Browser) section.

## 三. 控制板

控制板用于展示系统的资源统计、运维统计及系统状态三类信息。

### 3.1 资源统计

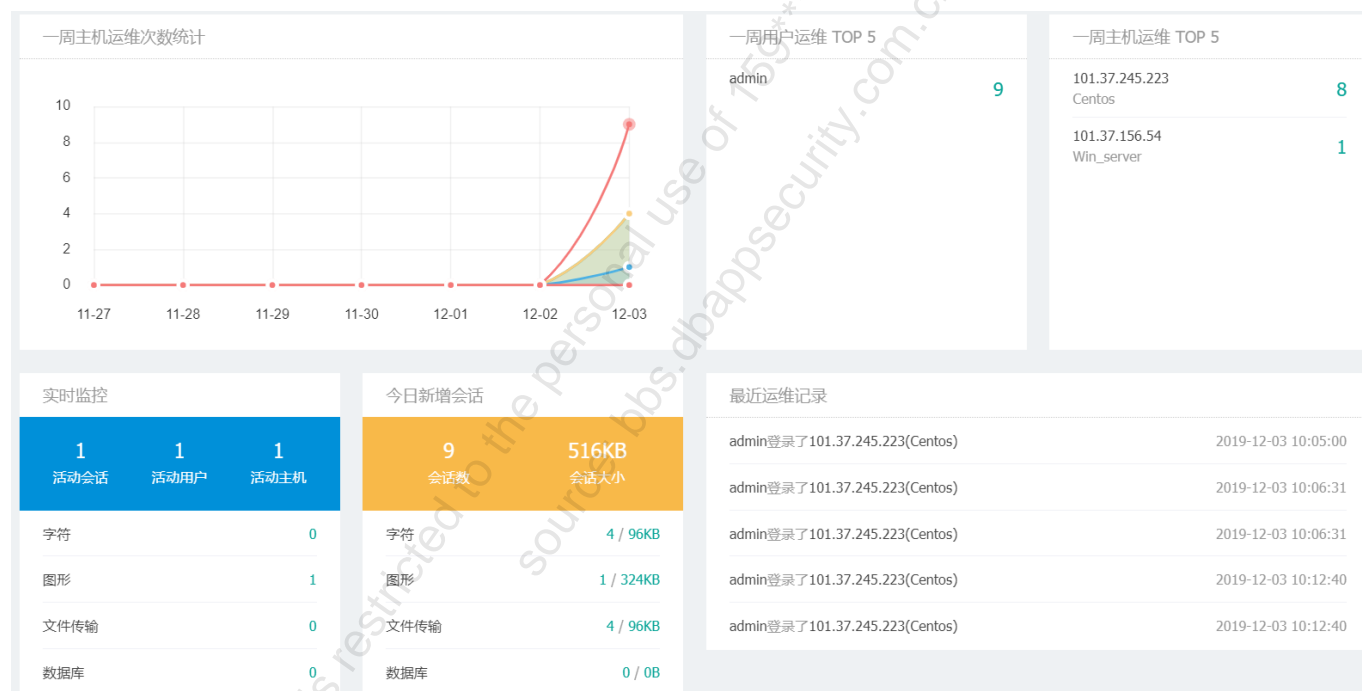
资源统计展示了系统的用户、主机、应用和运维规则数量。



点击上述区域跳转到对应功能的配置页面，更多信息请参见[用户管理](#)，[主机管理](#)，[应用管理](#)和[运维规则](#)。

### 3.2 运维统计

展示最近一周运维情况统计、实时监控、新增会话等信息。



DAS-USM 支持对字符、图形、文件传输和数据库四类运维会话进行统计，有关运维配置的更多信息，请参见[主机运维](#)。

各会话类型说明如下。

会话类型	说明
字符	运维 SSH、Telnet、Rlogin 字符类协议的会话。
图形	运维 RDP、VNC 图形类协议的会话。
文件传输	运维 SFTP、FTP 文件类协议的会话。
数据库	运维 Oracle、MySQL、SQL Server、DB2 数据库协议的会话。

### 3.2.1 系统状态

系统状态部分展示设备自身的版本信息、运行状态及许可证信息。

系统运行状态		许可证信息	
系统名称	明御®运维审计与风险控制系统	客户信息	内部测试
版本	2.0.8.2.6	授权类型	试用版
系统警报	14条未确认警报	过期时间	2099-12-31 23:59:59
运行时长	2 天 20 小时 50 分 51 秒	维保时间	2099-12-31 23:59:59
运行模式	单机模式	最大VPN连接数	200
持有虚拟IP	否	最大运维连接数	4000
		最大主机数	10000

在<系统警报>后点击<\*条未确认警报>跳转到系统警报页面查看详细信息，更多信息请参见[系统报警](#)。

许可证是授权给用户的 DAS-USM 功能使用许可，包括授权的使用类型、时间段、性能规格等。可联系安恒信息客服人员获取许可证文件，在系统菜单栏选择“[系统>本机维护>许可证](#)”导入许可证文件，更多信息请参见[许可证](#)。

This file is restricted to the personal use of 159\*\*\*\*@\*\*\*\*.cn  
source: bbs.dbappsecurity.com.cn  
2020-04-13

## 四. 部门

在 DAS-USM 中，部门是一种虚拟组织结构，用于将用户、主机等资源划分到不同的逻辑分区。每个部门都可以包含资产、用户、用户组和子部门，由部门管理员统一管理。不同部门之间的数据和权限相互隔离，部门管理员无法查看或管理本部门之外的数据。

### 4.1 新建部门

步骤1. 在系统菜单栏点击<部门>进入部门管理页面，点击<新建部门>。



步骤2. 选择部门所属的上级部门并输入部门名称，点击<创建部门>完成创建。



创建成功后新建部门将加入到部门管理列表，点击部门名称前 ▶ 图标展开查看选中部门下的子部门，及各级子部门中的用户和资产信息；点击用户数和资产数列下的数字跳转到用户管理和主机管理页面查看用户和资产，更多信息请参见[用户管理](#)和[主机管理](#)。

### 4.2 安全码管理

安全码是部门导出主机密码文件 zip 包的加密密码，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前后两部分进行设置。安全码机制可以防止管理员权限过于集中，通过分权机制保障密码文件的安全性。关于密码文件导出的详细信息，请参见[改密计划](#)。

步骤1. 在系统菜单栏点击<部门>进入部门管理页面，在部门列表的安全码列下点击<管理>。

部门

系统部门树形结构只支持5级且系统部门数目的上限为500，当前登录用户所在部门为第1级

部门	用户数	资产数	安全码
用户根	22	13	A B 管理
123	1	1	A B 管理
456	0	0	A B 管理
信息科	2	1	A B 管理
外包公司	1	0	A B 管理

步骤2. 在安全码页面设置 KeyA,点击<保存更改>, 设置 KeyB, 点击<保存更改>。

更改KeyA

\* KeyA   显示 1-32个数字、英文字母和符号

---

更改KeyB

\* KeyB   显示 1-32个数字、英文字母和符号

安全码设置完成后，可选择将 KeyA 和 KeyB 发送至指定邮箱，有关邮箱配置的更多信息，请参见[告警配置](#)。

## 4.3 删除部门

超级管理员可删除除用户根之外的所有部门，部门管理员可删除本部门下的子部门。



删除部门会同时删除其中的用户、用户组、主机、主机组、帐户组、应用、改密计划、自动运维任务、运维授权、审计规则等数据，请谨慎操作。

步骤1. 点击<删除部门>。

部门

系统部门树形结构只支持5级且系统部门数目的上限为500，当前登录用户所在部门为第1级

部门	用户数	资产数	安全码	
用户根	22	13	A B 管理	
123	1	1	A B 管理	删除部门
456	0	0	A B 管理	删除部门
信息科	2	1	A B 管理	删除部门
IT支持	0	0	A B 管理	删除部门

步骤2. 在弹出的对话框中点击<确定>即可删除部门。

# 五. 用户

在 DAS-USM 中，用户必须隶属于某一部门，超级管理员或者部门管理员给用户指定角色，这样用户便具备相应的权限，可在系统中对指定资源进行管理。

## 5.1 用户管理

### 5.1.1 新建用户

**步骤1.** 在菜单栏点击“用户>用户管理”进入用户管理页面，在用户管理页面右上角点击<新建用户>。



**步骤2.** 在新建用户页面，输入用户名，选择所属部门，输入密码并确认密码，选择用户所在部门、用户角色、认证模式完成创建。

\* 用户名  最大长度16个字符

\* 所属部门

\* 角色  [角色权限说明](#)

\* 认证模式

\* 密码  [密码强度说明](#)

\* 确认密码  再次输入密码

\* 姓名  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

部分配置项说明请参见下表。

配置项	说明
用户名	最大长度为 16 字符。
角色	系统内置 8 种角色，角色权限说明可点击<角色权限说明>进行查看。
认证模式	选择认证模式： <ul style="list-style-type: none"> <li>◆ 本地认证：通过密码对用户进行认证。</li> <li>◆ Radius：通过远程 Radius 服务器对用户进行认证。</li> </ul> 有关 Radius 服务器配置的更多信息，请参考 <a href="#">认证管理</a> 的远程认证部分。
密码	密码长度为 6~64 字符。

创建成功后新建用户将加入到用户管理列表，点击用户名进入用户基本信息页面，在基本信息页面可以修改用户部门、角色、密码等信息。

## 5.1.2 导入用户

新建用户的效率较低，可使用导入用户的方法批量创建用户。操作方法如下：

**步骤1.** 在用户管理页面单击<导入用户>。



**步骤2.** 在导入用户页面单击<下载模板文件>，将模板文件下载至本地。



**步骤3.** 在本地编辑好模板文件并保存。单击<上传文件>图标上传编辑好的模板文件，选择认证模式，并选择是否覆盖已有同名用户，单击<导入用户>。详细配置请参见下表。

配置项	说明
认证模式	设置用户登录时的认证方式，包括： <ul style="list-style-type: none"> <li>◆ 本地认证：用户登录时在本地进行认证的认证方式，即用户的账户和密码信息存储在</li> </ul>

配置项	说明
	<p>DAS-USM 系统中，用户登录时与用户输入的账户和密码进行比对。</p> <ul style="list-style-type: none"> <li>◆ AD：通过远程 AD 服务器对用户进行认证。通过 AD 认证的用户会自动同步至系统，无需管理员手动创建用户。</li> <li>◆ LDAP：通过远程 LDAP 服务器对用户进行认证。通过 LDAP 认证的用户会自动同步至系统，无需管理员手动创建用户。</li> <li>◆ Radius：通过远程 Radius 服务器对用户进行认证。</li> </ul> <p>有关 AD、LDAP、Radius 服务器配置的更多信息，请参考<a href="#">认证管理</a>。</p>
覆盖已有同名用户	若勾选该选项，当系统中存在与导入文件同名的用户，则系统中已经存在的同名用户信息将被导入文件中的同名用户信息替换。

### 5.1.3 用户配置

在系统菜单栏点击“[用户](#)”>[用户管理](#)”进入用户管理页面，点击用户名进入用户基本信息页面，点击[用户配置](#)进入用户配置页面。设置用户锁定状态、认证方式、VPN 接入配置、登录 IP 黑白名单和登录时间限制，点击[保存更改](#)即可。

#### 用户信息



The screenshot shows the 'User Configuration' tab in the system interface. It includes the following settings:

- 状态 (Status):**  锁定这个用户 (Lock this user)
- 认证方式 (Authentication Method):**
  - 密码 (Password)
  - 密码和手机APP口令 (Password and mobile app code)
  - 密码和动态令牌 (Password and dynamic token)
  - 密码和USBKEY (Password and USBKEY)
  - 密码和短信口令 (Password and SMS code)
  - 第三方USBKEY (Third-party USBKEY)
- 手机APP验证器 (Mobile App Verifier):** 未设置 (Not set)
- VPN远程拨入 (VPN Remote Access):**  允许 (Allow)
- 登录IP范围 (Login IP Range):** (黑名单) 不允许以下IP (Blacklist) Do not allow the following IP
- IP列表 (IP List):** 10.10.1.2, 192.168.0.2

详细配置请参见下表。

配置项	说明
锁定这个用户	用户被锁定后将无法登录系统，解除锁定后即可登录系统。
认证方式	用户登录时的认证方式。
手机 APP 验证器	显示手机 APP 验证器的状态。更多信息请参见 <a href="#">个人信息</a> 的手机身份验证器设置。

配置项	说明
VPN 远程拨入	设置是否允许用户通过 VPN 远程登录到系统。有关 VPN 配置的更多信息，请参见 <a href="#">VPN 管理</a> 。
登录 IP 范围	设置用户可以登录的 IP 地址范围，当选择黑名单时，指定的 IP 地址范围不能登录系统；当选择白名单时，仅允许指定的 IP 地址可以登录系统。
有效期	用户的有效期。只有在有效期内用户才能登录系统。
登录时间限制	指定允许登录的时间段。

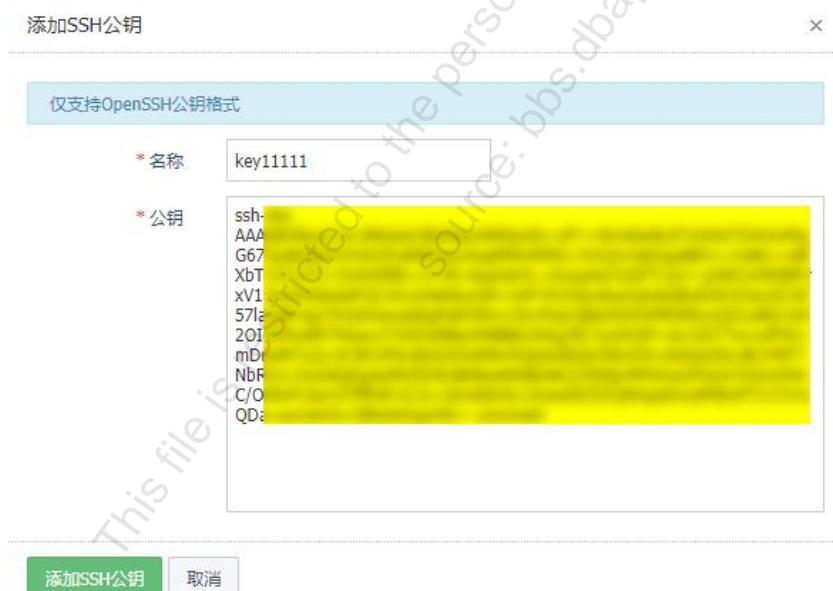
## 5.1.4 SSH 公钥管理

当用户使用 SSH 协议登录系统时，需要配置 SSH 公钥。

**步骤1.** 在用户信息页面，点击<SSH 公钥>进入用户 SSH 公钥配置页面。点击<添加 SSH 公钥>。



**步骤2.** 弹出添加 SSH 公钥对话框，设置公钥名称和公钥内容。点击<添加 SSH 公钥>即可。



## 5.1.5 查看已授权主机

在用户信息页面，点击<已授权主机>进入已授权主机页面，查看对此用户已授权的主机。

用户信息

按运维规则过滤			
每页显示20条数据			
<a href="#">首页</a> <a href="#">上一页</a> <span>1 / 1</span> <a href="#">下一页</a> <a href="#">末页</a>			
主机	主机网络	主机组	主机帐户
1.1.1.1 交换机	Default Network	信息科	[SSH] <span style="background-color: yellow;">[REDACTED]</span>
10.20.176.13 test	Default Network		[RDP] <span style="background-color: yellow;">[REDACTED]</span>
10.20.176.21 linux演示机	Default Network		[SSH] <span style="background-color: yellow;">[REDACTED]</span>

## 5.1.6 查看已授权应用

在用户信息页面，点击<已授权主机>进入已授权应用页面，查看对此用户已授权的应用。

用户信息

按运维规则过滤	
每页显示20条数据	
<a href="#">首页</a> <a href="#">上一页</a> <span>1 / 1</span> <a href="#">下一页</a> <a href="#">末页</a>	
应用名称	
 shujuku	
 test	

## 5.2 用户组管理

为了方便用户管理，可以将用户划分到不同的用户组，实现批量授权功能。

新建用户组并添加用户的操作方法如下：

**步骤1.** 在系统菜单栏点击“用户>用户组管理”进入用户组管理页面，点击<新建用户组>。

用户组管理

[+ 新建用户组](#)

用于对用户进行分组管理、集中授权		
每页显示20条数据		
<a href="#">首页</a> <a href="#">上一页</a> <span>1 / 1</span> <a href="#">下一页</a> <a href="#">末页</a>		
用户组名称	所属部门	成员数
<input type="checkbox"/> 1234	123	0

步骤2. 弹出新建用户组窗口，选择部门，设置名称，点击<创建用户组>。

新建用户组



新建用户组窗口包含以下元素：

- \* 部门：下拉菜单，当前选择“用户根”
- \* 名称：输入框，当前输入“运维组”，右侧标注“最大长度50个字符”
- 底部有一个绿色的“创建用户组”按钮

步骤3. 在创建完成提示页面或用户组列表页面点击新建用户组名称跳转到用户组信息页面。

用户组信息 运维组



用户组信息页面包含以下元素：

- 顶部有“用户组成员”和“修改用户组名称”两个选项卡
- 操作栏包含“移除”、“添加成员”按钮，以及“已选: 0/0(全部选择/取消选择)”
- 右侧有分页控件：每页显示20条数据，首页，上一页，0/0，下一页，末页
- 搜索框：搜索用户名/姓名
- 过滤器：按角色过滤、按认证模式过滤、按部门过滤
- 表格列头：用户、角色、认证模式、部门
- 表格内容：显示“无数据”

步骤4. 点击<添加成员>，在选择用户对话框中勾选用户并点击<添加>将用户添加到用户组。

选择用户



选择用户对话框包含以下元素：

- 顶部有“添加”按钮，以及“已选: 3/22(全部选择/取消选择)”
- 右侧有分页控件：每页显示20条数据，首页，上一页，1/2，下一页，末页
- 搜索框：搜索用户名/姓名
- 过滤器：按角色过滤、按认证模式过滤、按部门过滤
- 表格列头：用户、角色、认证模式、部门
- 表格内容：显示多条用户记录，其中部分记录被选中（勾选框打勾）

已添加的用户将会显示在用户组成员列表中，勾选用户，点击<移除>将选中的用户从当前用户组中移除。关于用户配置的信息，请参见[用户管理](#)。

## 5.3 动态令牌管理

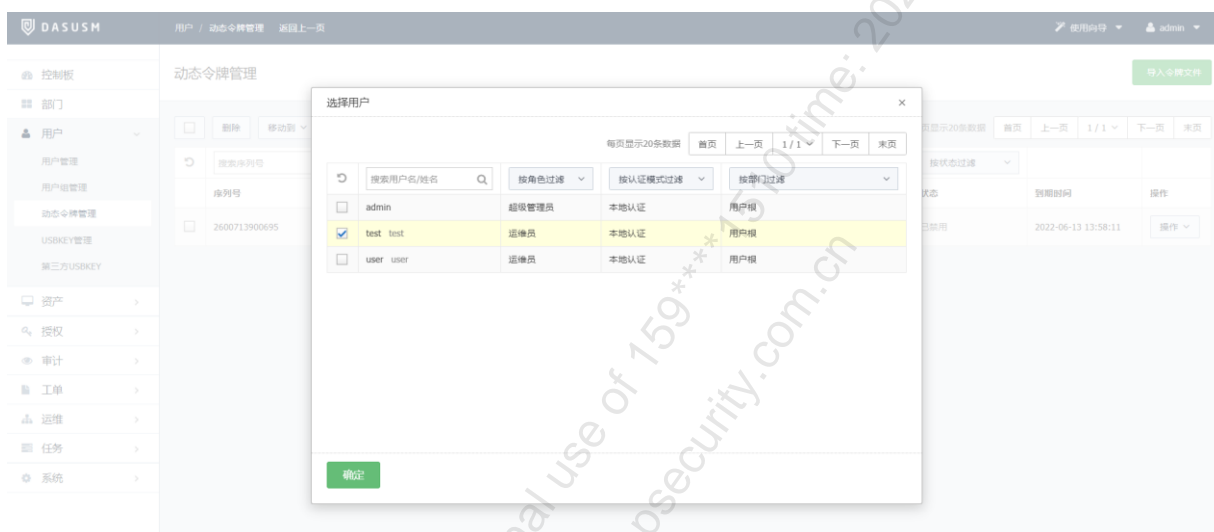
动态令牌管理是指对用户通过动态令牌登录系统进行管理。包括令牌绑定用户、禁用令牌、挂失令牌等。

步骤1. 在系统菜单栏点击“用户>动态令牌管理”进入动态令牌管理页面。点击页面右上角的<导入令牌文件>，

选择令牌文件并上传，完成令牌文件导入。



**步骤2.** 令牌文件导入完成后，点击令牌文件右侧的“操作▶绑定用户”，选择用户绑定动态令牌。绑定完成后，该用户即可使用对应的动态令牌登录系统。



当动态令牌被禁用/挂失时，用户不能再使用该动态令牌登录系统。直到管理员重新启用令牌后，用户才可使用该令牌登录系统。当动态令牌与用户之间解除绑定后，用户不能再使用该动态令牌登录系统，直到管理员重新将动态令牌与用户绑定后，用户才可使用该令牌登录系统。

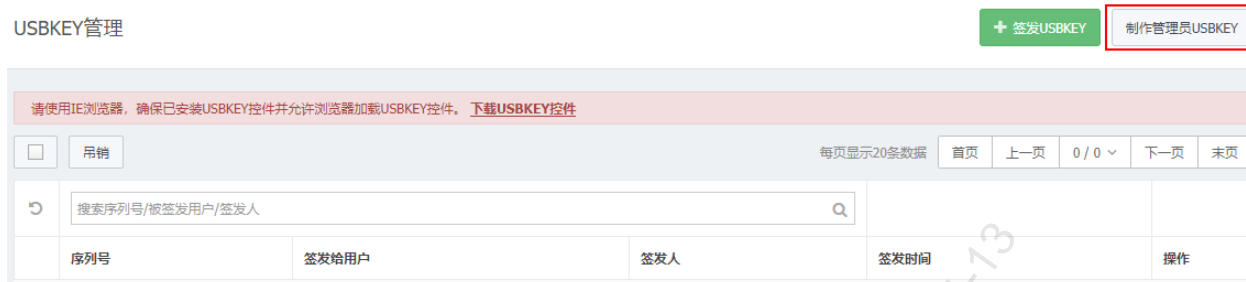
## 5.4 USBKEY 管理

DAS-USM 支持使用 USBKEY 方式对登录用户进行认证。拥有管理权限的用户可签发管理员 USBKEY，之后通过管理员 USBKEY 签发用户 USBKEY。签发完成后，管理员或普通用户在登录到 DAS-USM 时必须插入对应的 USBKEY 才可以完成认证。

### 5.4.1 签发管理员 USBKEY

**步骤1.** 使用 IE 浏览器访问系统，确保本地 PC 已安装 USBKEY 控件并允许 IE 浏览器加载 USBKEY 控件，

在系统菜单栏点击“用户>USBKEY 管理”进入 USBKEY 管理页面。



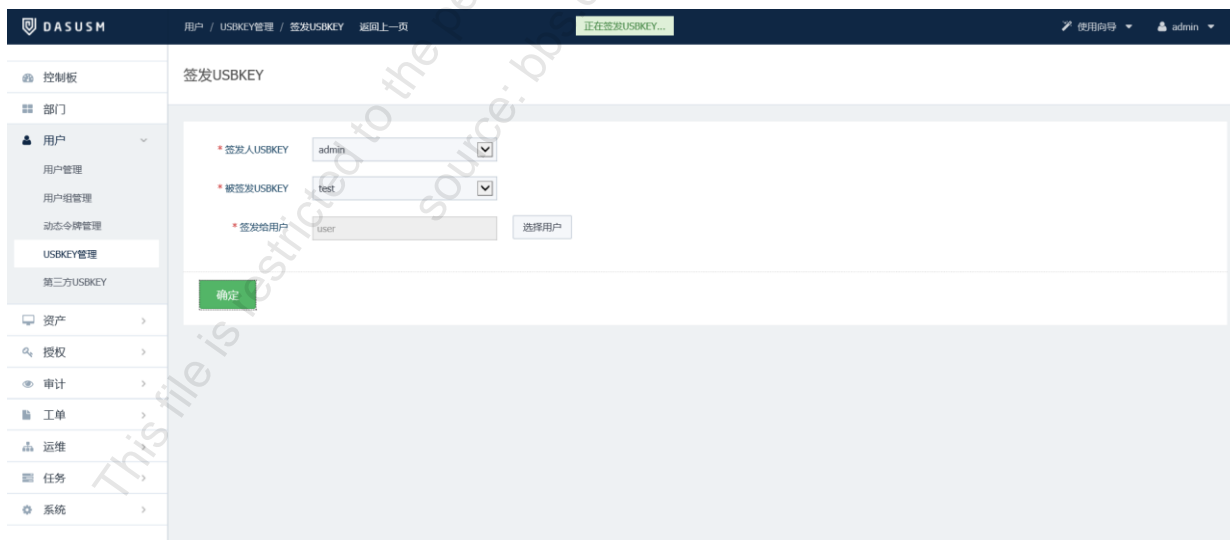
步骤2. 在本地 PC 上插入管理员 USBKEY 后，点击页面右上角<制作管理员 USBKEY>，弹出签发管理员 USBKEY 窗口，选择管理员并点击<确定>，等待管理员 USBKEY 制作完成。

## 5.4.2 签发用户 USBKEY

步骤1. 制作好管理员 USBKEY 后，在本地 PC 上插入用户 USBKEY 和管理员 USBKEY，点击页面右上角 <签发 USBKEY>。



步骤2. 进入签发 USBKEY 页面。选择签发人 USBKEY、被签发 USBKEY 以及签发用户，点击<确定>。



等待用户 USBKEY 签发完成后，即可使用 USBKEY 认证方式登录系统。

## 5.5 第三方 USBKEY

使用第三方 USBKEY 认证方式登录系统，需要先在双因子认证配置中配置第三方 USBKEY 认证方式。操作方法如下：

步骤1. 在系统菜单栏点击“系统>认证管理>双因子认证”进入双因子认证配置页面。在<双因子认证>中勾选开启第三方 USBKEY。



步骤2. 在<第三方 USBKEY 通用配置>中，将状态设置为开启，上传证书链后点击<保存更改>。

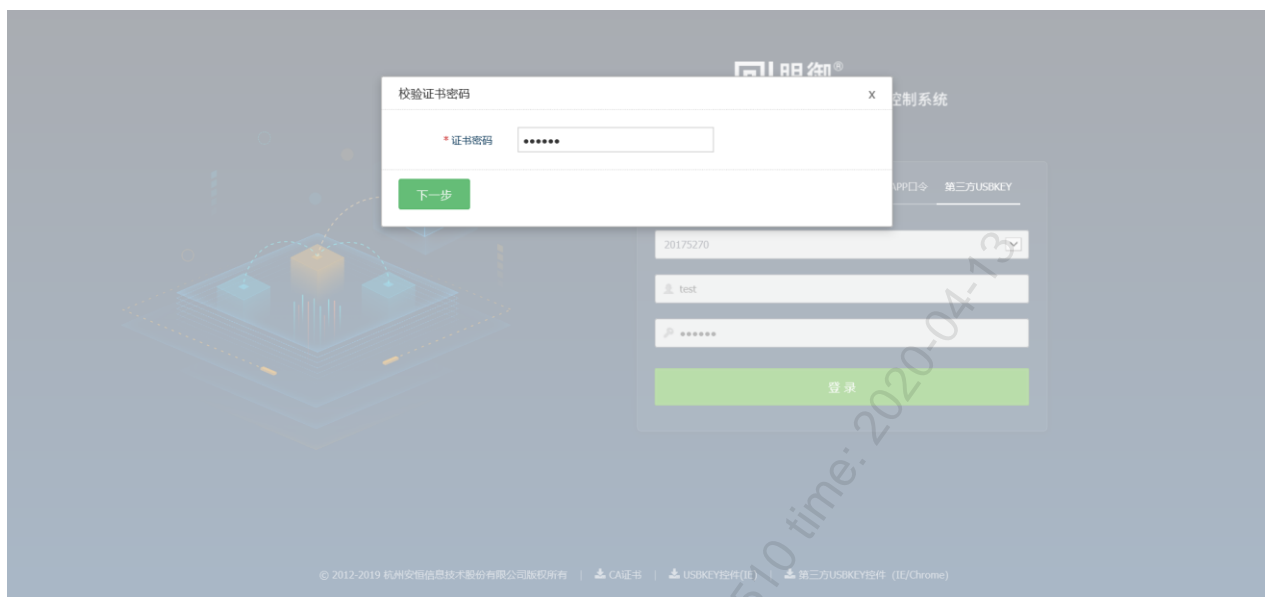


步骤3. 在登录页面右下角点击<第三方 USBKEY 控件 (IE/Chrome)>下载第三方 USBKEY 控件（使用IE/Chrome 浏览器）并安装在本地 PC 中。



步骤4. 将第三方 USBKEY 插入本地 PC，使用 IE/Chrome 浏览器登录 DAS-USM，选择第三方 USBKEY 认证方式登录。浏览器识别第三方 USBKEY 后，输入用户名、密码以及第三方 USBKEY 校验证书密

码登录系统。



首次使用第三方 USBKEY 硬件登录会自动绑定帐户，且无法用此 USBKEY 硬件登录其他帐户。解绑后才可使用此 USBKEY 硬件登录其他帐户。

This file is restricted to the personal use of 159\*\*\*@\*\*\*.cn  
source: bbs.dbappsecurity.com.cn

# 六. 资产

本文中所述的资产包括接入 DAS-USM 的主机及主机中的账户、应用等。超级管理员、部门管理员和运维管理员可对权限内的资产进行管理。

## 6.1 主机管理

主机管理包括新建主机、编辑主机、禁用主机、删除主机等。

### 6.1.1 新建主机

**步骤1.** 在系统菜单栏点击“**资产>主机管理**”进入主机管理页面。点击页面右上角的<新建主机>。



**步骤2.** 选择主机所属部门、主机网络、操作系统、主机组、主机编码，填写主机 IP、主机名等信息。点击<创建主机>完成主机添加。



部分参数的详细配置请参见下表。

配置项	说明
主机网络	配置主机所属的网络。点击<新建>可创建局域网。更多信息请参考 <a href="#">混合云管理</a> 。
主机 IP	支持 IPv4、IPv6 和域名格式。
主机编码	设置主机编码的格式，与被管理主机上的编码设置保持一致： <ul style="list-style-type: none"> <li>◆ UTF-8：是针对 Unicode 的一种可变长度字符编码。</li> <li>◆ GB18030：全称《信息技术 中文编码字符集》，是中华人民共和国国家标准所规定的变长多字节字符集。</li> </ul>

步骤3. 主机创建成功后，点击成功提示中的<创建主机帐户>，进入主机帐户页面。

主机192.168.50.172已创建，前往 [编辑主机信息](#) 或者 [创建主机帐户](#) (创建主机帐户以便授权、运维)

步骤4. 点击<添加主机帐户>。

主机信息



The screenshot shows a web interface with tabs for 'Basic Information', 'Host Configuration', 'Host Accounts', 'Shared Accounts', and 'Privileged Users'. The 'Host Accounts' tab is active. A table with columns 'Username', 'Protocol', 'Password', 'SSH Private Key', and 'Login Mode' is visible, but it contains no data. A green button labeled 'Add Host Account' is highlighted with a red box.

步骤5. 在新建主机帐户窗口选择协议、登录模式、帐户类型，填写登录名和密码，点击<创建主机帐户>完成主机帐户添加。



The screenshot shows the 'New Host Account' form. It includes dropdown menus for 'Protocol' (SSH), 'Login Mode' (Automatic Login), and 'Account Type' (Normal Account). There is a text input for 'Username' (root) and a password input field with a 'Verify' button. A green 'Create Host Account' button is at the bottom.

详细配置请参见下表。

配置项	说明
协议	设置用户登录时使用的协议，包括：SYSDEF、Telnet、SSH、FTP、SFTP、RDP、VNC、SQL Server、MySQL、Oracle、DB2 和 Rlogin。
登录模式	<p>设置主机的登录模式：自动登录、手动登录和自动登录（二次登录）。</p> <ul style="list-style-type: none"> <li>◆ 自动登录：将正确的主机帐号密码托管到 DAS-USM，运维时 DAS-USM 自动代填密码。</li> <li>◆ 手动登录：在运维时需要用户输入正确的主机帐号密码才可登录成功。</li> <li>◆ 自动登录（二次登录）：只支持 SSH 和 Telnet 协议，用于管理两个帐户自动跳转登录。如交换机既有远程帐户又有 enable 命令特权账户，若需要自动登录到 enable 命令特权账户，则必须采取自动登录（二次登录）模式。</li> </ul>

配置项	说明
账户类型	包括普通账户和交换机特权命令帐户两种类型。
登录名	主机帐户登录名。
密码	主机帐户密码。

## 6.1.2 导入主机

手动逐个新建主机的效率较低，可使用导入主机的方法批量创建主机。操作方法如下：

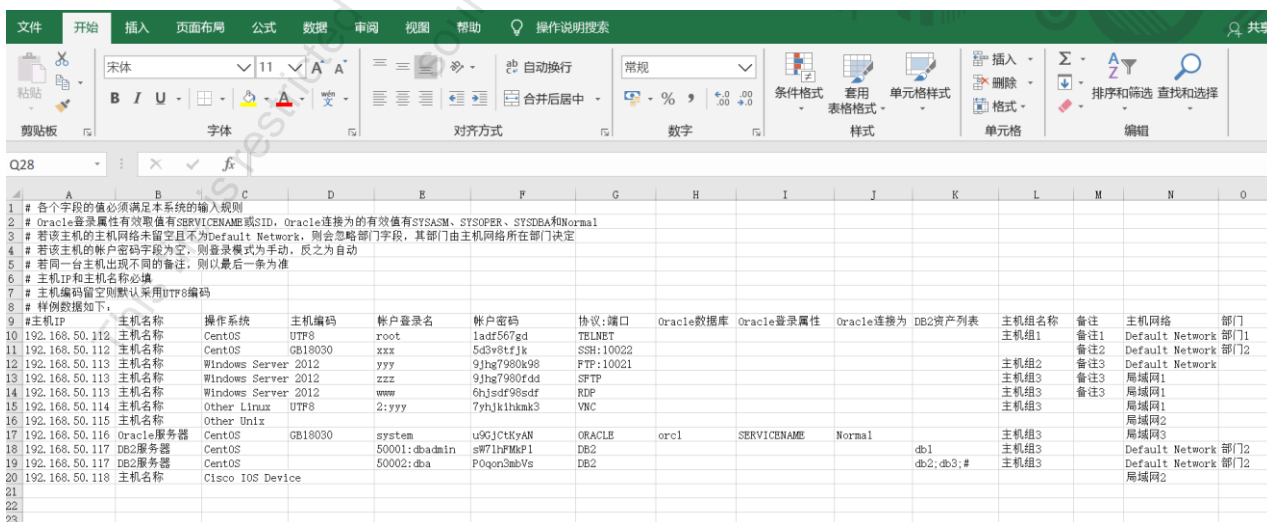
步骤1. 在主机管理页面点击右上角的<导入主机>，进入导入主机页面。



步骤2. 点击<下载模板文件>，将模板文件保存至本地。



步骤3. 根据模板格式添加主机及主机账户，修改模板文件后保存文件。



步骤4. 在导入主机页面点击<上传文件>，选择编辑好的模板文件并上传，上传完成后点击<导入主机>。完成批量添加主机及主机帐户。

## 6.1.3 编辑主机

创建主机后可对主机信息进行修改：

**步骤1.** 在系统菜单栏点击“**资产>主机管理**”进入主机管理页面。点击主机 IP 进入主机基本信息页面。在基本信息页面中可修改主机网络、操作系统、主机 IP、主机名称以及主机编码等信息。

主机信息

所属部门	测试	
* 所属主机网络	<div style="border: 1px solid #ccc; padding: 2px;">Default Network ▼</div>	根据网络位置对主机进行分组管理，可改变主机所在的网络或 <a href="#">新建</a>
* 操作系统	<div style="border: 1px solid #ccc; padding: 2px;">CentOS ▼</div>	
* 主机IP	<input style="width: 100%;" type="text" value="10.20.176.21"/>	
* 主机名称	<input style="width: 100%;" type="text" value="10.20.176.21"/>	
* 主机编码	<div style="border: 1px solid #ccc; padding: 2px;">UTF-8 ▼</div>	
备注	<input style="width: 100%; height: 30px;" type="text"/>	

保存更改

**步骤2.** 点击<主机配置>进入主机配置页面。可配置主机协议控制等选项。

主机信息

基本信息
主机配置
主机帐户
共享帐户
已授权用户

主机配置

状态	<input type="checkbox"/> 禁用这台主机
会话选项	<input type="checkbox"/> 开启会话二次审批
	<input type="checkbox"/> 开启会话备注
	<input checked="" type="checkbox"/> 开启历史会话审计
	<input checked="" type="checkbox"/> 开启实时会话监控
RDP选项	<input type="checkbox"/> 启用键盘记录
	<input checked="" type="checkbox"/> 允许打印机/驱动器映射
	<input checked="" type="checkbox"/> 允许使用剪贴板下载
	<input checked="" type="checkbox"/> 允许使用剪贴板上传
SSH选项	<input checked="" type="checkbox"/> 允许X11转发

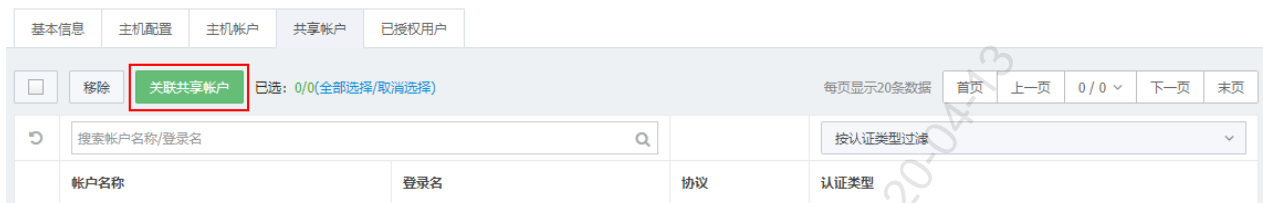
详细配置请参见下表。

选项	功能	解释
会话选项	开启会话二次审批	需要对该主机进行审核后方可登录。
	开启会话备注	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	对运维会话进行审计。
	开启实时会话监控	管理员可以对主机进行实时监控。
RDP 选项	启用键盘记录	记录 RDP 主机的键盘符操作记录。
	允许打印机/驱动器映射	运维 RDP 主机时，可以映射本地打印和本地磁盘。
	允许使用剪切板下载	运维 RDP 主机时，可以使用复制-粘贴功能从主机下载。
	允许使用剪贴板上传	运维 RDP 主机时，可以使用复制-粘贴功能上传至主机。
SSH 选项	允许 X11 转发	运维时可以通过 SSH 方式转发 X11 协议。
	允许打开 SFTP 通道	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	可以直接使用 exec 指令。
SFTP/SCP/ZMODEM 传输控制	禁止文件上传	运维时禁止通过 SFTP/SCP/ZMODEM 方式上传文件。
	禁止文件下载	运维时禁止通过 SFTP/SCP/ZMODEM 方下载文件。
	禁止文件删除	运维 SFTP 主机时禁止删除文件。
	禁止重命名	运维 SFTP 主机时禁止重命名。
	禁止目录创建	运维 SFTP 主机时禁止创建目录。
	禁止目录删除	运维 SFTP 主机时禁止删除目录。
FTP 选项	禁止文件上传	运维 FTP 主机时禁止上传文件。
	禁止文件下载	运维 FTP 主机时禁止下载文件。
	禁止文件删除	运维 FTP 主机时禁止删除文件。
	禁止重命名	运维 FTP 主机时禁止重命名。
	禁止目录创建	运维 FTP 主机时禁止创建目录。
	禁止目录删除	运维 FTP 主机时禁止删除目录。
文件审计	生成文件 SHA1	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	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	可以保存下载的文件。
	保存上传文件	可以保存上传的文件。
	启用文件压缩	可以对传输的文件进行压缩。
	不保存超过*KB 的文件	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*MB 时停止保存	可以控制单个会话保存的文件大小。

步骤3. 点击<主机帐户>进入主机帐户页面。点击帐户名编辑主机帐户信息。点击<添加主机帐户>添加主机帐户。

步骤4. 点击<共享帐户>进入共享帐户（关于共享账户的详细信息，请参见共享帐户管理）页面，点击<关联共享帐户>。

主机信息



步骤5. 在弹出的对话框中勾选需要关联的共享帐户，点击<添加>。

关联共享帐户



步骤6. 点击<已授权用户>进入主机已授权用户页面，可查看已授权此主机的用户。

已授权用户



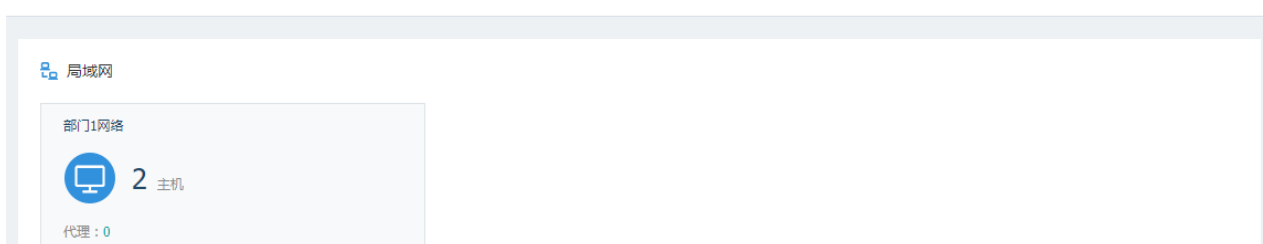
## 6.2 混合云管理

混合云管理是指对私有云和公有云（目前仅支持阿里云和亚马逊云）的资源进行统一管理。


### 6.2.1 对私有云资源进行管理

步骤1. 在系统菜单栏点击“资产>混合云管理”进入混合云管理页面。点击页面右上方<新建局域网>。

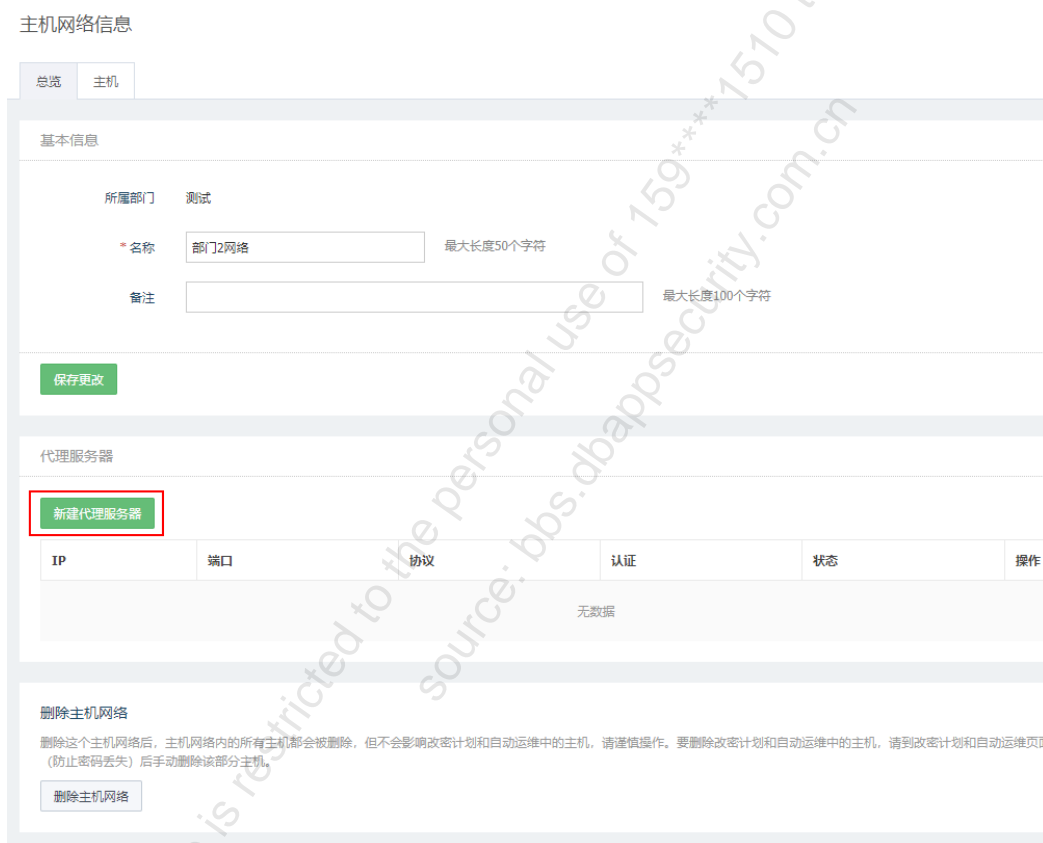
混合云管理



步骤2. 选择局域网所属部门，填写局域网名称，点击<创建局域网>，完成局域网创建。



步骤3. 点击局域网名称进入主机网络信息页面。在总览页面中可以修改主机网络名称和备注、为主机网络添加代理服务器、删除主机网络。



步骤4. 在主机网络信息页面中，点击<主机>标签，点击<新建主机>可新建主机至局域网，点击<移入主机>可将系统中已有主机移入局域网。



步骤5. 在主机网络信息页面中，点击<总览>页签。点击<新建代理服务器>，选择代理协议，填写代理服务器IP、端口、用户名密码等信息，为主机网络添加代理服务器。

新建代理服务器
✕

---

\* 代理协议

\* 服务器地址

\* 端口

\* 认证

\* 用户名

密码  没有密码请留空

异常 (连接超时)

## 6.2.2 对公有云资源进行管理

目前仅支持阿里云和亚马逊云。

步骤1. 在系统菜单栏点击“资产>混合云管理”进入混合云管理页面。点击页面右上角“新建公有云账户>阿里云”。

混合云管理

---

局域网

部门1网络

0 主机

代理: 0

部门2网络

2 主机

代理: 1

阿里云  
亚马逊云

步骤2. 输入 Access Key ID 和 Access Key Secret，点击<下一步>，等待云上主机同步完成。

新建阿里云账户
✕

---

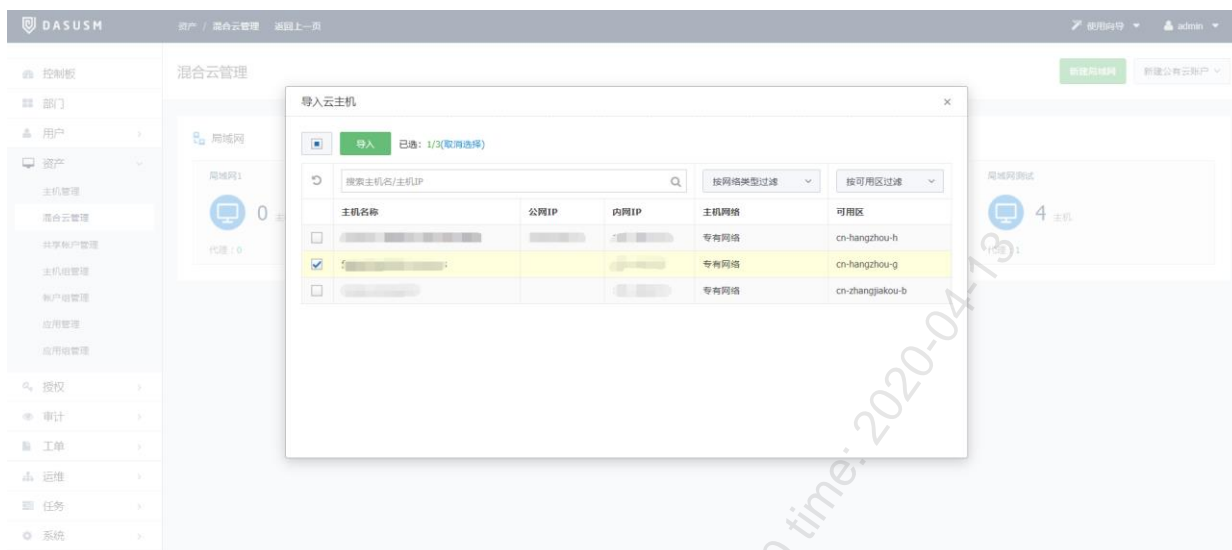
\* Access Key ID

\* Access Key Secret

系统将使用阿里云访问密钥 Access Key 调用公共云服务 API 获取 ECS 和 VPC 列表

[如何创建阿里云Access Key?](#)

步骤3. 同步完成后，选择需要导入的阿里云主机，点击<导入>，将阿里云账号下的主机添加到系统中。



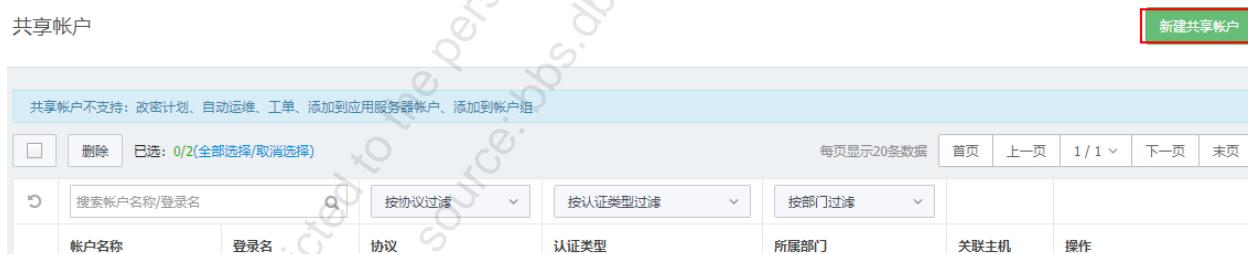
为公有云主机设置代理服务器的方法与私有云主机的操作方法相同，不再赘述。

对亚马逊云资源的管理方法与对阿里云资源管理的方法相同，不再赘述。

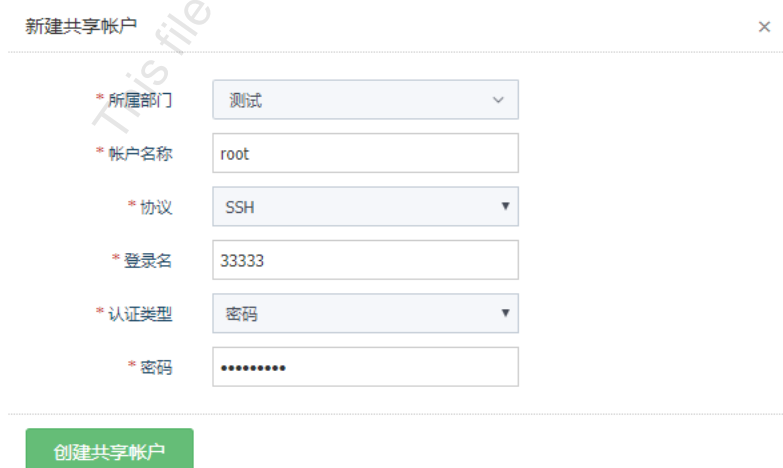
## 6.3 共享帐户管理

具有权限的用户可使用共享账户登录共享账户关联的多个主机，可减少为主机创建账户的工作量。创建共享账户并关联主机的操作方法如下：

步骤1. 在系统菜单栏点击“资产>共享帐户管理”进入共享帐户管理页面。点击右上方<新建共享帐户>。



步骤2. 选择共享帐户所属部门、协议、认证类型，填写帐户名、登录名，填写密码/密钥，点击<创建共享帐户>完成共享账户添加。



部分参数的详细配置请参见下表。

配置项	说明
协议	账户登录系统使用的协议，包括 Telnet、SSH、FTP、SFTP、RDP、VNC 和 Rlogin。
认证类型	当使用 SSH 协议时，可选择密码和密钥；使用其他协议时仅可选择密码。

步骤3. 点击共享帐户右侧的<关联主机>，进入共享帐户关联主机页面，点击<关联主机>。

共享帐户 新建共享帐户

共享帐户不支持：改密计划、自动运维、工单、添加到应用服务器帐户、添加到帐户组

删除 已选: 0/3(全部选择/取消选择) 每页显示20条数据 首页 上一页 1/1 下一页 末页

搜索帐户名称/登录名 按协议过滤 按认证类型过滤 按部门过滤

帐户名称	登录名	协议	认证类型	所属部门	关联主机	操作
<input type="checkbox"/> 13444	12434	SSH	密码	测试	2	编辑 <b>关联主机</b>
<input type="checkbox"/> root	33333	SSH	密码	测试	0	编辑 关联主机
<input type="checkbox"/> root1	44433	SSH	密码	测试	1	编辑 关联主机

步骤4. 点击<关联主机>。

共享帐户信息 13444

主机

移除 **关联主机** 已选: 0/2(全部选择/取消选择) 每页显示20条数据 首页 上一页 1/1 下一页 末页

搜索主机IP/主机名 按操作系统过滤 按主机编码过滤 按主机网络过滤

主机	操作系统	主机编码	所属主机网络	所属部门
<input type="checkbox"/> 10.20.176.21 10.20.176.21	CentOS	UTF-8	部门2网络	测试
<input type="checkbox"/> 192.168.0.3 数据库服务器	CentOS	UTF-8	部门2网络	测试

步骤5. 在弹出的对话框中勾选主机，点击<添加>即可添加关联主机。

关联主机 ×

**添加** 已选: 2/2(全部选择/取消选择) 每页显示20条数据 首页 上一页 1/1 下一页 末页

搜索主机IP/主机名 按操作系统过滤 按主机编码过滤 按主机网络过滤

<input checked="" type="checkbox"/> 10.20.176.21 10.20.176.21	CentOS	UTF-8	部门2网络
<input checked="" type="checkbox"/> 192.168.0.3 数据库服务器	CentOS	UTF-8	部门2网络

## 6.4 主机组管理

对主机进行分组，便于批量对主机进行设置，减少配置工作量。创建主机组并添加主机的方法如下：

步骤1. 在系统菜单栏点击“资产>主机组管理”进入主机组管理页，点击<新建主机组>。



步骤2. 选择主机组所在部门，填写主机组名称，点击<创建主机组>，完成主机组创建。



步骤3. 点击主机组名称，进入主机组成员页面，点击<添加主机>。



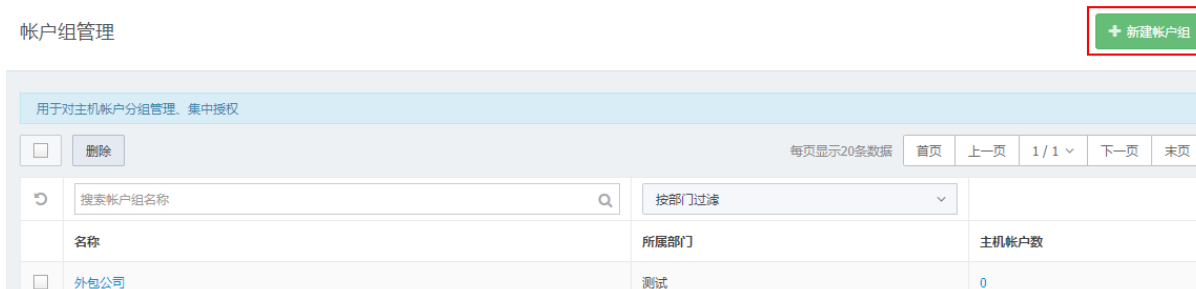
步骤4. 在弹出的对话框中勾选主机，点击<添加>即可将主机添加到主机组中。



## 6.5 帐户组管理

为账户分组，便于对账户进行批量设置。创建账户组并添加账户的操作方法如下：

步骤1. 在系统菜单栏点击“资产>帐户组管理”进入帐户组管理页面，点击<新建帐户组>。



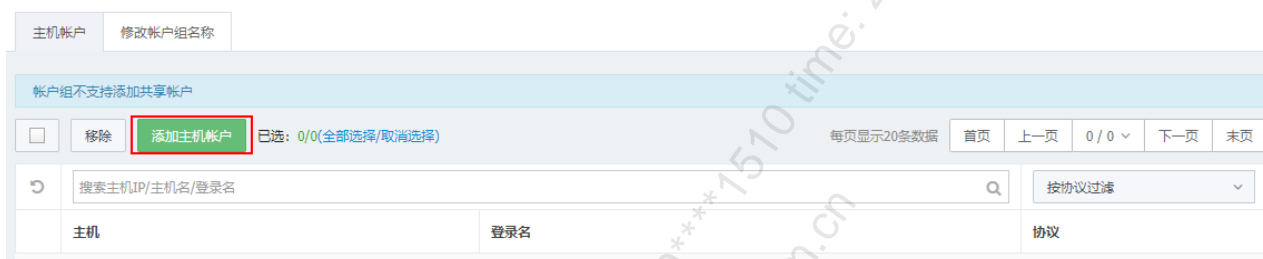
步骤2. 在弹出的对话框中选择帐户组所在部门，填写帐户组名称，点击<创建帐户组>，完成帐户组创建。

新建帐户组



步骤3. 点击帐户组名称，进入帐户组信息页面管理帐户组成员。点击<添加主机帐户>。

帐户组信息 重要账户



步骤4. 在弹出的对话框中勾选主机账户，点击<添加>即可为账户组添加账户。

选择主机帐户



主机	登录名	协议
10.20.176.21	root	SSH
192.168.0.3 数据库服务器	[EMPTY]	SSH
192.168.0.3 数据库服务器	root	SSH

## 6.6 应用管理

创建应用前需添加应用服务器，并将应用加载器安装至应用服务器。操作方法如下：

步骤1. 在系统菜单栏点击“资产>应用管理”进入应用列表页，点击<应用服务器>页签进入应用服务器管理页面，点击<添加应用服务器>。

应用管理



步骤2. 勾选主机，点击<确定>。

选择主机 ×

每页显示20条数据 首页 上一页 1 / 1 下一页 末页

搜索主机IP/主机名	按操作系统过滤	按主机编码过滤	按主机网络过滤	按部门过滤
<input type="checkbox"/>	10.20.176.21 10.20.176.21	CentOS	UTF-8	部门2网络 测试
<input checked="" type="checkbox"/>	192.168.0.3 数据库服务器	CentOS	UTF-8	部门2网络 测试

确定

步骤3. 在应用管理页面点右上角的<新建应用>。

应用管理 + 新建应用

应用列表 应用服务器

步骤4. 选择应用服务器帐户、应用类型，填写应用路径等信息，点击<创建应用>。

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  应用服务器帐户不包括共享帐户

\* 应用名称

\* 应用类型


\* 应用路径  例: C:\oracle\product\10.2.0\client\_1\BIN\sqlplusw.exe

数据库IP

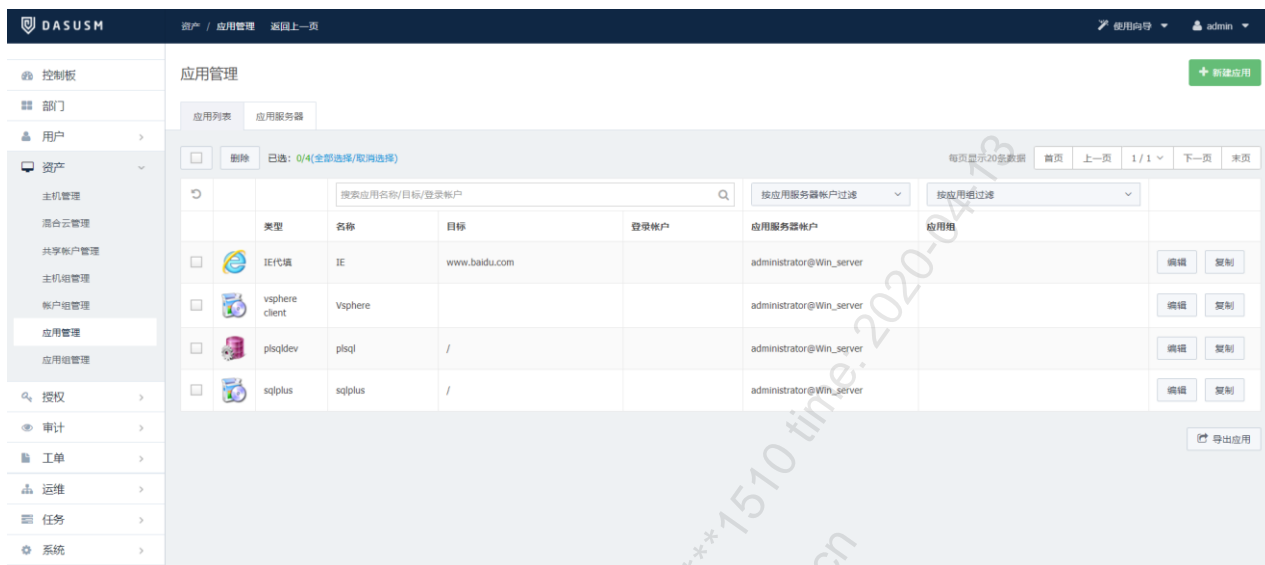
数据库名

数据库帐户

数据库密码

图标 

**步骤5.** 进入应用列表页，可查看创建好的应用。点击应用右侧的<编辑>修改应用信息。点击应用右侧的<复制>复制应用。勾选需要删除的应用，点击<删除>即可删除应用。点击列表右下方<导出应用>可将应用导出至文件以进行查看。



## 6.7 应用组管理

将应用分组便于对应用进行批量设置，减少配置工作量。创建应用组并添加应用的操作方法如下：

**步骤1.** 在系统菜单栏点击“资产>应用组管理”进入应用组管理页，点击<新建应用组>。

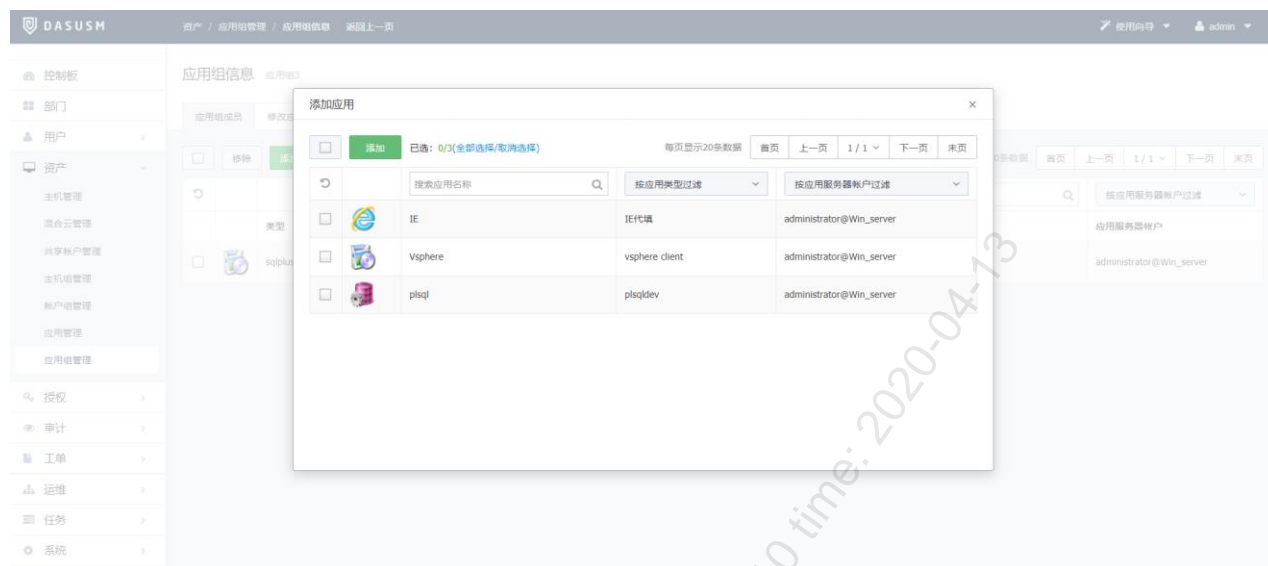


**步骤2.** 选择应用组所在部门，填写应用组名称，点击<创建应用组>，完成应用组创建。



**步骤3.** 点击应用组名称进入应用组信息页面。在应用组信息页面可以管理应用组成员。点击<添加应用>，在

弹出的对话框中勾选应用，点击<添加>。



# 七. 授权

在 DAS-USM 中，授权管理包括运维授权和策略管理两部分内容：运维授权是指将指定主机帐户的运维权限赋予指定用户，策略管理是对主机的访问策略进行管理。

## 7.1 运维规则

运维授权关系类型主要有：

- ◆ 帐户组授权给用户组
- ◆ 单个主机帐户授权给用户组
- ◆ 被托管的应用授权给用户组
- ◆ 主机组授权给用户组
- ◆ 应用组授权给用户组
- ◆ 帐户组授权给单个用户
- ◆ 单个主机帐户授权给单个用户
- ◆ 被托管的应用授权给单个用户
- ◆ 主机组授权给单个用户
- ◆ 应用组授权给单个用户

### 7.1.1 新建运维规则

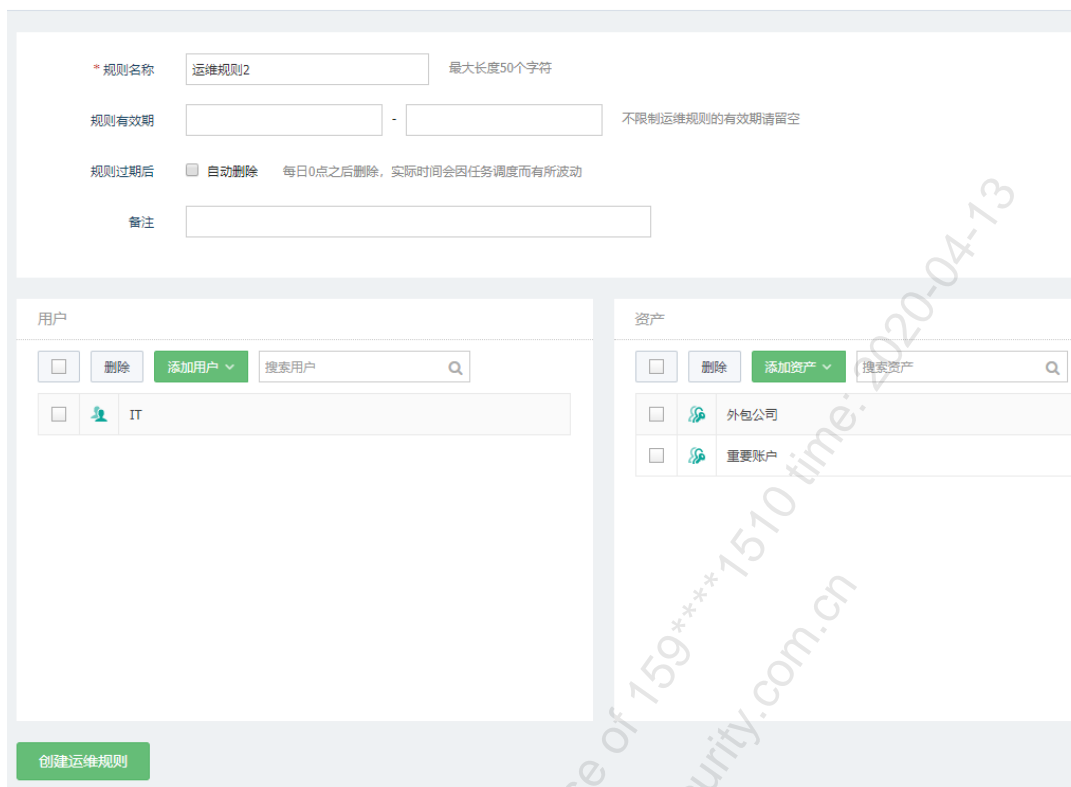
**步骤1.** 在系统菜单栏点击“授权>运维规则”进入运维规则页面。点击右上角<新建运维规则>。



**步骤2.** 进入新建运维规则页面。填写运维规则名称、有效期等信息，设置用户与资产的对应关系（将资产的运

维权限赋予给用户)，点击<创建运维规则>，完成运维规则创建。

新建运维规则



部分配置项的说明请参见下表。

配置项	说明
用户	设置资产由哪些用户进行运维操作，包括用户和用户组。
资产	设置用户可以运维的资产，包括账户、账户组、主机组、应用和应用组。

## 7.1.2 编辑运维规则

创建运维规则后，可修改运维规则。操作方法如下：

**步骤1.** 在系统菜单栏点击“**授权>运维规则**”进入运维规则页面，点击运维规则名称或者点击运维规则右侧

“操作>编辑规则”进入运维规则总览页面，修改运维规则名称、规则有效期等信息，单击<保存更改>。

#### 编辑运维规则



步骤2. 点击<用户/资产>页签进入运维规则用户/资产页面，修改运维规则中的用户、资产间的授权关系，单击<保存更改>。

#### 编辑运维规则



详细配置请参见下表。

配置项	说明
添加用户/用户组	<ul style="list-style-type: none"> <li>◆ 点击“添加用户&gt;添加用户”，在弹出的对话框中勾选用户，点击&lt;添加&gt;。</li> <li>◆ 点击“添加用户&gt;添加用户组”，在弹出的对话框中勾选用户组，点击&lt;添加&gt;。</li> </ul>
删除用户/用户组	勾选用户/用户组，点击<删除>。
添加资产	点击<添加资产>，在下拉菜单中选择<添加资产账户>/<添加账户组>/<添加主机组>/<添加应用>/<添加应用组>，可添加资产账户/账户组/主机组/应用/应用组等资产。
删除资产	勾选资产，点击<删除>。

步骤3. 点击<登录限制>进入运维规则登录限制配置页面，勾选<启用登录限制>，设置源 IP 的黑/白名单列表及登录时段限制，点击<保存更改>。

编辑运维规则

总览
用户/资产
登录限制
命令控制
协议控制

状态  启用登录限制

来源IP限制模式 (黑名单) 不允许以下IP

IP列表

192.168.0.3

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

登录时段限制

	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	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许
周二	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许
周三	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许
周四	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许
周五	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许
周六	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许
周日	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许	允许

允许  禁止

保存更改

步骤4. 点击<命令控制>进入运维规则命令控制配置页面，勾选<启用命令控制>，设置命令阻断，命令审批和

命令黑/白名单，点击<保存更改>。

编辑运维规则

总览
用户/资产
登录限制
命令控制
协议控制

状态  启用命令控制

命令控制功能仅针对Linux命令行进行适配，可能无法适应网络设备命令行中缩写、省略部分，不适合在交换机等网络设备上使用

命令匹配优先级按：阻断会话 -> 需要审批 -> 黑白名单的顺序进行依次匹配

填写命令以行为单位，每一行为一个命令单元(命令+参数)，命令和参数为模糊匹配(支持通配符?\*[])

例1：匹配config命令：请填写config到相应的列表中，若要匹配以en开头的命令，请填写en\*

例2：匹配ps命令及auxef中任意一个参数：请填写ps \*a\* \*u\* \*x\* \*e\* \*f\*到相应的列表中，参数匹配与顺序无关

以下命令会阻断会话

以下命令需要审批

(黑名单) 不允许执行以下命令

telnet

保存更改

步骤5. 点击<协议控制>进入运维规则协议控制页面，勾选勾选<启用协议控制>，配置相关选项，点击<保存更改>。协议控制中的选项控制效果与主机配置中的选项控制效果相同。未启用运维规则协议控制时，

系统默认使用主机配置中的协议控制，请参考编辑主机的[步骤 2](#)。

### 编辑运维规则

总览
用户/资产
登录限制
命令控制
协议控制

状态  启用协议控制 开启后，协议控制由运维规则中的决定，主机配置中的协议控制将失效

---

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

## 7.2 审批规则

审批规则是指对命令审批和运维二次审批设置审批规则，即对主机或运维规则指定审批员。

创建审批规则的操作方法如下：

**步骤1.** 在系统菜单栏点击“[授权](#)”>[审批规则](#)”进入审批规则页面。点击<[新建审批规则](#)>。

+ 新建审批规则

每页显示20条数据
首页
上一页
1 / 1
下一页
末页

按审批类型过滤

名称	审批员	审批对象	审批类型
111	1	0	1
			命令审批

步骤2. 填写审批规则名称，选择审批类型、审批员、审批对象后点击<创建审批规则>。

### 新建审批规则

详细配置请参见下表。

配置项	说明
审批类型	<ul style="list-style-type: none"> <li>◆ 命令审批：运维规则中开启命令控制时，可设置命令审批类型的审批规则，指定命令审批人。若该运维规则未指定审批人，则默认命令审批人为运维的资产所在部门及其上级部门的运维管理员和部门管理员。</li> <li>◆ 运维二次审批：协议控制中开启会话二次审批时，需要审批人审批通过后运维员方可登录运维。运维二次审批类型可为运维规则或主机指定会话二次审批的审批人。若未在审批规则中指定会话二次审批员，则默认审批员为运维的资产所在部门及其上级部门的运维管理员和部门管理员。</li> </ul>
审批员	设置审批员。
审批对象	审批员要审批的运维规则。

步骤3. 进入审批规则页面，点击审批规则名称/审批员/审批对象，进入审批规则编辑页面，可修改审批规则名

称、审批类型、审批员、审批对象等信息。勾选审批规则，点击<删除>即可删除审批规则。

审批规则

+ 新建审批规则

审批规则			
名称	审批员	审批对象	审批类型
<input type="checkbox"/> 规则1	1	0  1	命令审批

## 7.3 未授权登录审核

未授权登录审核是指对用户登录未授权主机的操作进行审核。审核通过后，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。未授权登录审核的操作方法如下：

在系统菜单栏点击“**授权>未授权登录审核**”进入未授权登录审核页面。勾选未授权条目，点击<授权>，即可自动创建相应的授权关系。

状态	用户	主机	端口	协议	登录名	最近登录时间	授权时间	授权人
<input type="checkbox"/> 已授权	admin	10.0.83.83	22	SSH	root	2019-12-05 10:34:21	2019-12-05 10:35:11	admin
<input type="checkbox"/> 未授权	admin	10.0.83.56	22	SSH	root	2019-12-05 10:34:00		

# 八. 审计

审计是指审计员对运维员的主机运维操作记录进行审计，可查看运维员的操作行为记录，作为事件追溯和事故分析的依据。

## 8.1 会话审计

会话审计用于记录运维员对主机操作过程的会话日志。审计员可通过会话审计定位故障及追溯故障根源。会话审计支持在线播放以及下载后离线播放两种查看方式。

会话审计支持通过时间段、主机网络、来源 IP、协议类型等条件进行筛选；支持通过执行过的命令进行全局检索，并定点跳转到命令所在的会话及时间回放会话。会话审计专注于事后审计，主要用于对已经结束的会话进行录像回放或命令检索。

会话审计的操作方法如下：

**步骤1.** 在系统菜单栏点击“**审计>会话审计**”进入会话审计页面。在所有会话页面可以查看字符、图形、文件传输、应用类型的会话日志。

会话审计

所有会话 应用会话 事件查询

可查看所有通过系统建立的完整会话

协议 全部 时间 [ ] - [ ]

搜索 展开更多搜索条件

类型	主机IP/主机名	协议/登录名	姓名/用户名	来源IP	开始时间/结束时间	会话时长/会话大小	主机网络	部门	操作
SHELL	10.20.176.21 10.20.176.21	SSH root	wangshuo wang	10.14.0.62	2019-12-27 13:08:55 2019-12-27 13:13:43	4分48秒 24KB	Default Network	测试	播放 下载 <b>详情</b>

**步骤2.** 点击会话右方的<详情>，查看详细的会话信息。

会话详情

会话ID	30aff3165e0591e70000001603000026		
时长	4分48秒	大小	24KB
开始时间	2019-12-27 13:08:55	结束时间	2019-12-27 13:13:43
用户	wang	来源IP	10.14.0.62
来源端口	51920		
主机名称	10.20.176.21	主机IP	10.20.176.21
登录名	root	协议	SSH
主机端口	22		
主机网络	Default Network		
会话备注			

**步骤3.** 在工具下载页面中下载离线播放器并安装到本地 PC 中。在会话审计页面点击会话右方的<下载>或者在会话详情对话框中点击<下载>，即可下载会话文件到本地，通过离线播放器播放。

**步骤4.** 在会话审计页面点击会话右方的<播放>或者在会话详情对话框中点击<播放>，即可通过 web 方式在线播放审计会话。使用 web 方式在线播放审计会话，需要在本地 PC 中安装 Flash Player，并在浏览器中启用 Flash Player。



查看应用会话的操作方法如下：

**步骤1.** 在会话审计页面点击<应用会话>进入应用会话页面。在应用会话页面可以查看应用的会话日志。

会话审计

所有会话 **应用会话** 事件查询

可查看所有通过应用发布建立的完整会话

应用名称  时间  -

应用	主机IP/主机名	协议/登录名	姓名/用户名	来源IP	开始时间/结束时间	会话时长/会话大小	操作
zzzz	10.20.176.13 应用发布服务器	RDP administrator	test1	10.14.0.47	2019-12-21 11:08:19 2019-12-21 11:09:05	46 秒 388KB	<input type="button" value="播放"/> <input type="button" value="下载"/> <input type="button" value="详情"/>

**步骤2.** 查看应用会话详情、在线/离线播放应用会话方式与其他类型会话相同。

查询事件的操作方法如下：

**步骤1.** 在会话审计页面点击<事件查询>进入事件查询页面。在事件查询页面可以选择类型和时间，点击<搜索>

事件查询相关事件的会话。点击事件右方的<播放>，即可通过 web 方式播放事件的记录。

会话审计

所有会话
应用会话
事件查询

可搜索会话中的关键事件并定位到相应完整会话

类型 所有类型
时间  -

搜索
导出搜索结果
展开更多搜索条件

时间	主机	用户	类型	内容	会话操作
2019-12-31 12:58:26	10.20.176.13	admin	上传保存	ocr.txt	<span style="border: 1px solid #ccc; padding: 2px 5px;">播放</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">详情</span>

步骤2. 点击<导出搜索结果>，设置起始偏移量和导出总条目数，点击<导出>，即可将过滤后的事件导出到本地 Excel 文件中查看。

导出事件列表
×

根据页面的搜索条件导出事件数据，可以指定从搜索结果的第几条数据（起始偏移量）开始导出，以及导出的总条目数，总条目数不能大于10000条。

起始偏移量

大于等于1的整数，默认值1

导出总条目数

有效值1-10000，默认值1000

导出

## 8.2 审计规则

审计规则是创建审计员与资产之间的对应关系，赋予审计员审计资产的权限。

创建审计规则的操作方法如下：

步骤1. 在系统菜单栏点击“**审计>审计规则**”进入审计规则页面，点击<新建审计规则>。

+ 新建审计规则

删除
每页显示20条数据
首页
上一页
1 / 1
下一页
末页

	名称	审计员	资产
<input type="checkbox"/>	123	0	0 0 0

步骤2. 填写审计规则名称，添加审计员和审计资产，点击<创建审计规则>。

新建审计规则

审计规则

\* 名称

用户

删除

<input type="checkbox"/>		admin 1
--------------------------	--	---------

主机

删除

<input type="checkbox"/>		10.20.176.21	10.20.176.21
<input type="checkbox"/>		192.168.0.3	数据库服务器

This file is restricted to the personal use of 159\*\*\*\*1510 time: 2020-04-13  
 source: bbs.dbappsecurity.com.cn

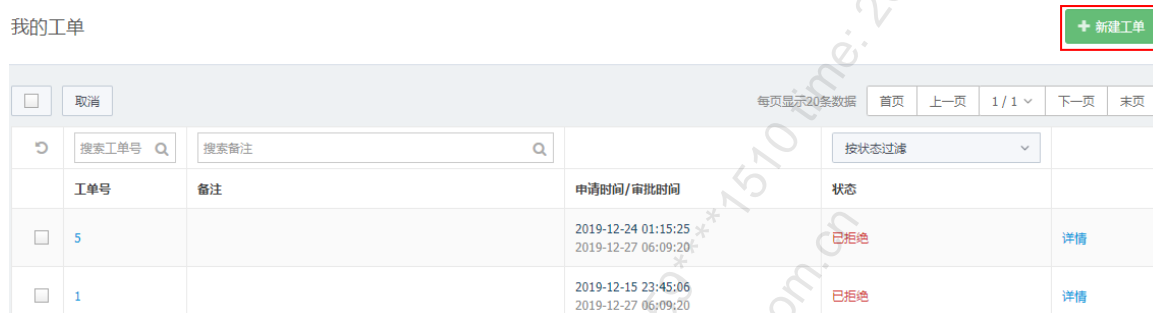
# 九. 工单

当运维人员需要运维授权关系以外的主机，且管理员并没有开启未授权登录时，运维人员可以通过工单向管理员申请运维这些资产。管理员批准工单后系统将自动创建工单中的授权关系。

## 9.1 创建工单

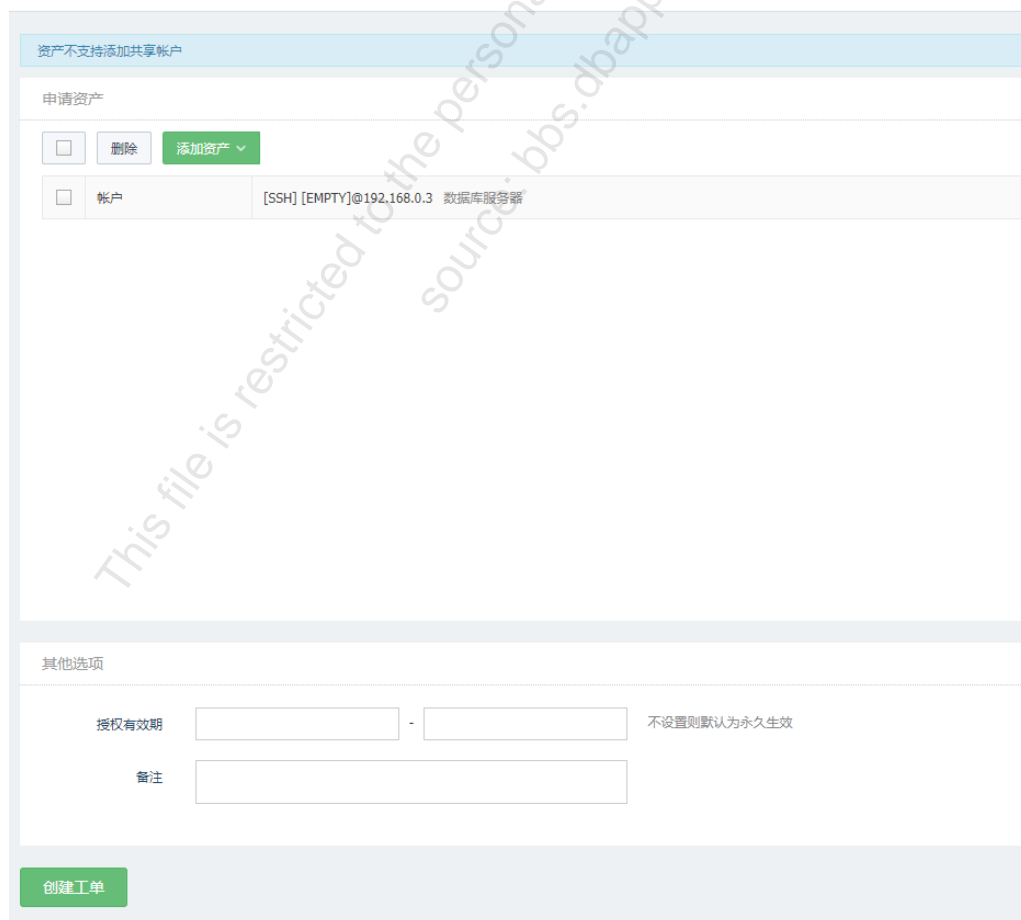
创建工单的操作方法如下：

**步骤1.** 在系统菜单栏点击“**工单**”进入我的工单页面，点击**新建工单**。

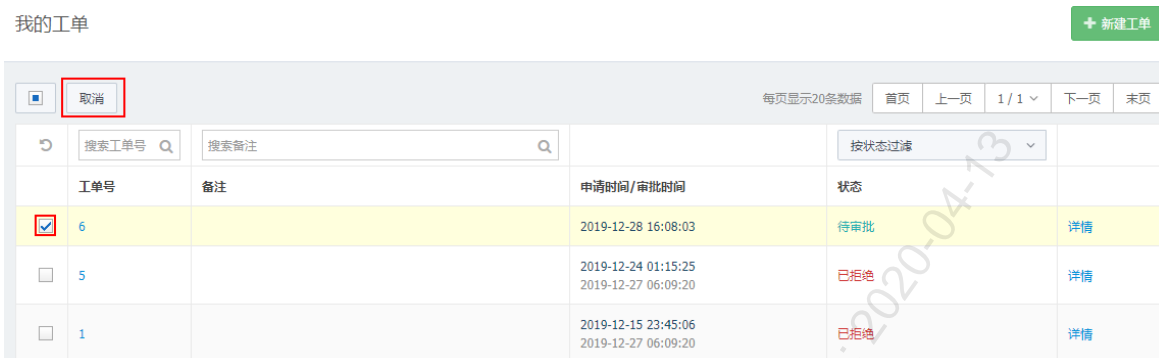


**步骤2.** 进入新建工单页面，点击**添加资产**添加主机账户>或**添加资产**添加应用>，选择要申请的资产并添加，设置授权有效期（可选），点击**创建工单**完成工单申请。

新建工单



**步骤3.** 进入我的工单页面，对于处于“待审批”状态的工单，可以点击工单号或工单右方的<详情>进入工单信息页面修改工单信息，修改完成后点击<保存更改>完成工单信息修改。勾选处于待审批状态的工单，点击<取消>即可取消工单申请。



对于处于“已批准”或“已拒绝”状态的工单，点击工单号或工单右方的<详情>进入工单信息页面查看工单详细信息。

运维员创建完工单后，本部门及上级部门的部门管理员和运维管理委员会收到邮件提醒。邮件提醒的前提条件为：

- ◆ 管理员在个人信息中填写了邮箱。
- ◆ 在“系统>系统配置>告警配置”页，已经完成了邮件配置并可以正常发送测试邮件。

## 9.2 工单审批

运维员申请工单后，管理员对工单进行审批，审批通过后运维员才能运维工单中申请的资产。

审批工单的操作方法如下：

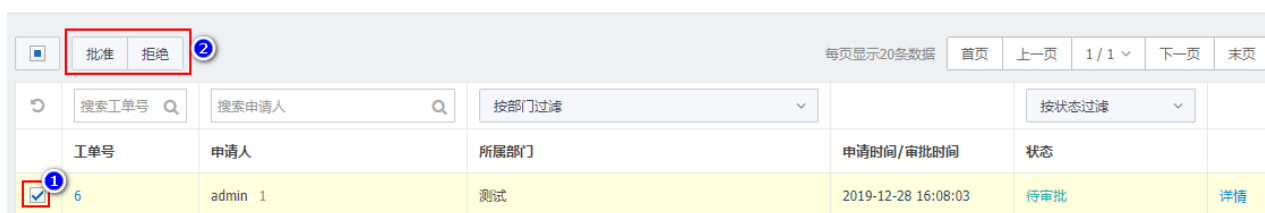
**步骤1.** 在系统菜单栏点击“工单>工单审批”进入工单审批页面。点击工单号或工单右方<详情>可进入工单信息页面查看工单详细信息，对于状态为“待审批”的工单，管理员可以修改工单的资产和授权有效期后再审批。

工单审批



**步骤2.** 进入工单审批页面，勾选需要审批的工单，点击<批准>同意此工单；点击<拒绝>拒绝此工单。

工单审批



# 十. 运维

运维是指运维员登录主机进行维护操作。

## 10.1 主机运维

### 10.1.1 全局配置

在进行主机运维前需要进行全局配置（即 Web 运维配置），操作方法如下：

**步骤1.** 在系统菜单栏点击“**运维>主机运维**”进入主机运维页面，点击<Web 运维配置>。



**步骤2.** 进入 Web 运维配置对话框，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、本地驱动器，点击<保存>即可。



步骤3. 点击<SSH&TELNET&Rlogin>，选择客户端程序、终端类型、编码格式点击<保存>即可。



步骤4. 点击<FTP>，进入 FTP 运维配置页，选择对应的客户端程序，点击<保存>即可。



步骤5. SFTP、VNC、SQL Server、Mysql、DB2 配置与 FTP 配置类似，参考 FTP 配置即可。

步骤6. 点击<Oracle>, 选择对应的客户端程序, 填写配置文件路径, 点击<保存>即可。

Web运维配置
×

RDP	* 客户端程序	<div style="border: 1px solid #ccc; padding: 2px;">PLSQL</div>
SSH & TELNET & Rlogin		<p>请确认您已经安装了所选客户端程序</p>
	配置文件路径	<div style="border: 1px solid #ccc; height: 20px;"></div>
FTP		<p>配置文件tnsnames.ora绝对路径, 如 G:11.2.0\dbhome_1\NETWORK\ADMIN\tnsnames.ora</p>
SFTP		<p>1. 为空白时, 仍可登录, 但客户端不显示目标信息, 且plsql和sqlplus将使用servicename属性进行登录, toad将使用sid属性进行登录</p>
VNC		<p>2. 不为空白时, 需保证当前pc系统用户对配置文件有修改权限。客户端将显示目标信息, 且客户端将根据堡垒保存的账户信息决定使用sid或servicename进行登录</p>
SQL Server		
MySQL		
Oracle		
DB2		

保存

保存配置将会打开运维审计系统, 若您已默认打开, 请忽略此提示

步骤7. 点击<DB2>, 选择对应的客户端程序, 点击<保存>即可。

Web运维配置
×

RDP	* 客户端程序	<div style="border: 1px solid #ccc; padding: 2px;">db2cmd</div>
SSH & TELNET & Rlogin		<p>请确认您已经安装了所选客户端程序</p>
FTP		<p>db2cmd客户端既可以连接实例也可以连接数据库。 QuestCentral客户端无法连接实例, 只能连接数据库。</p>
SFTP		
VNC		
SQL Server		
MySQL		
Oracle		
DB2		

保存

保存配置将会打开运维审计系统, 若您已默认打开, 请忽略此提示

## 10.1.2 主机运维

主机运维支持 B/S 运维、C/S 运维和 H5 运维三种运维方式。

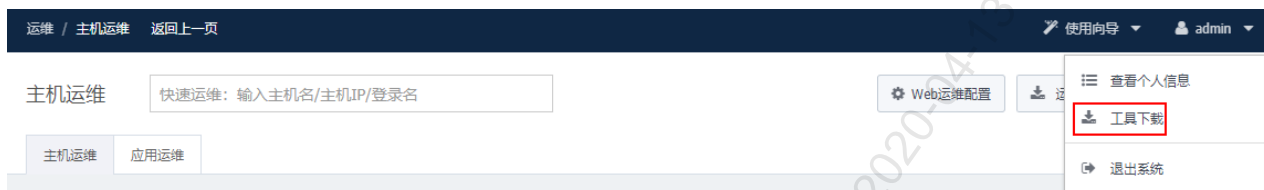
- ◆ B/S 运维支持 SSH、Telnet、Rlogin、FTP、SFTP、VNC、RDP、Oracle、SQL Server、MySQL、DB2 协议。
- ◆ C/S 运维支持 SSH、Telnet、Rlogin、FTP、SFTP、RDP、Oracle 协议。
- ◆ H5 运维支持 SSH、Telnet、Rlogin、VNC、RDP 协议。

进行主机运维前，需要做好以下准备工作：

- ◆ 管理员创建相应用户和资产的运维规则。
- ◆ 下载运维工具。

下载运维工具的操作方法如下：

**步骤1.** 在上边栏点击当前用户名，从下拉菜单选择<工具下载>进入工具下载页面。



**步骤2.** 点击工具右侧的<本地下载>，下载相应工具的安装包到本地。或点击<官方网站>到相应工具的官方网站获取安装包。各工具的用途请参见下表。

名称	说明
单点登录器	单点登录器是使用 Web 方式调用运维客户端时使用的登录工具。
应用加载器	应用中心 IE 表单自动代填必备工具。
USBKEY 控件 (IE)	USBKEY 控件用于系统启用 USBKEY 认证方式时的登录工具。
离线播放器	与 Adobe ATR 一起安装，用于会话审计里的日志导出后进行离线查看。
VPN 客户端	VPN 客户端用于运维审计系统 VPN 连接工具。
Adobe AIR	离线播放器运行环境。
Flash Player 12	Flash 播放器，页面上传/下载按钮、播放审计会话的依赖插件。
Chrome	谷歌浏览器。
FileZilla	用于连接 SFTP/FTP 服务器。
WinSCP	用于连接 SFTP/FTP 服务器。
PuTTY	用于连接 SSH、telnet、Rlogin 协议服务器。
Mstsc	用于连接 RDP 协议服务器。
RealVNC	用于连接 VNC 协议服务器。
SecureFX	用于连接 SFTP/FTP 服务器。
SecureCRT	用于连接 SSH、telnet、Rlogin 协议服务器。
Xshell	用于连接 SSH、telnet、Rlogin 协议服务器。

### ◆ B/S 运维:

步骤1. 在系统菜单栏点击“**运维>主机运维**”进入主机运维页面。



步骤2. 点击资产列表<登录>列中  的图标，自动调用 Web 运维配置中配置的 SSH 客户端登入服务器。



### ◆ H5 运维:

步骤1. 在系统菜单栏点击“**运维>主机运维**”进入主机运维页面。

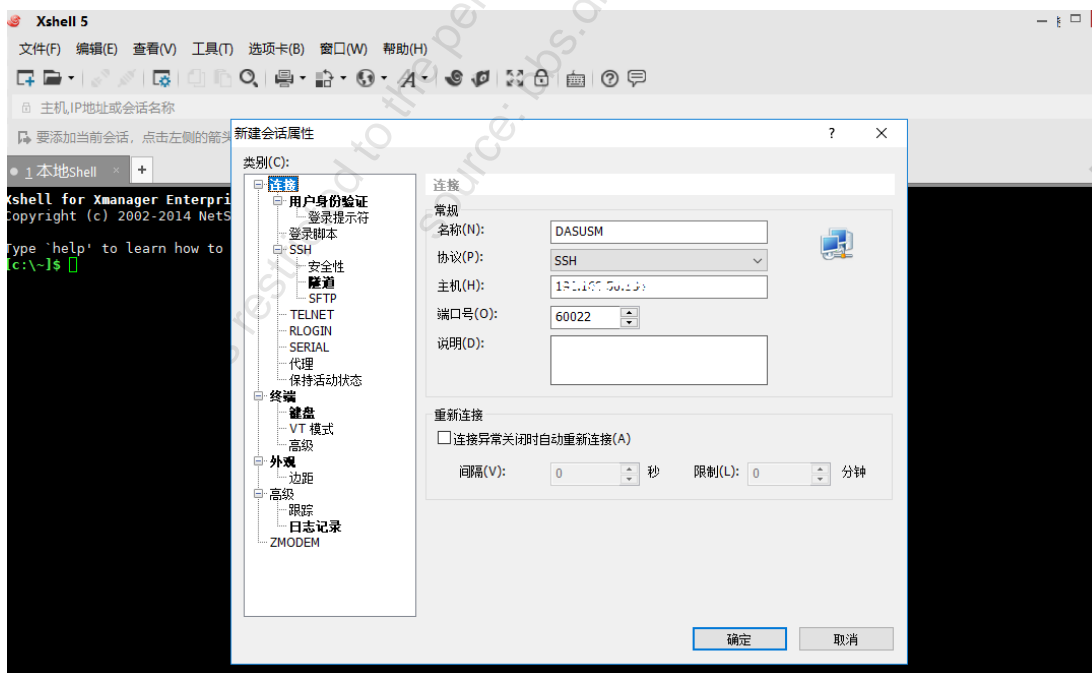
步骤2. 在资产列表中点击<登录>列中的  图标，通过 H5 客户端登入服务器。



SSH、Telnet、Rlogin 协议的 H5 运维仅支持 Edge、Firefox 34+、Chrome 31+浏览器。

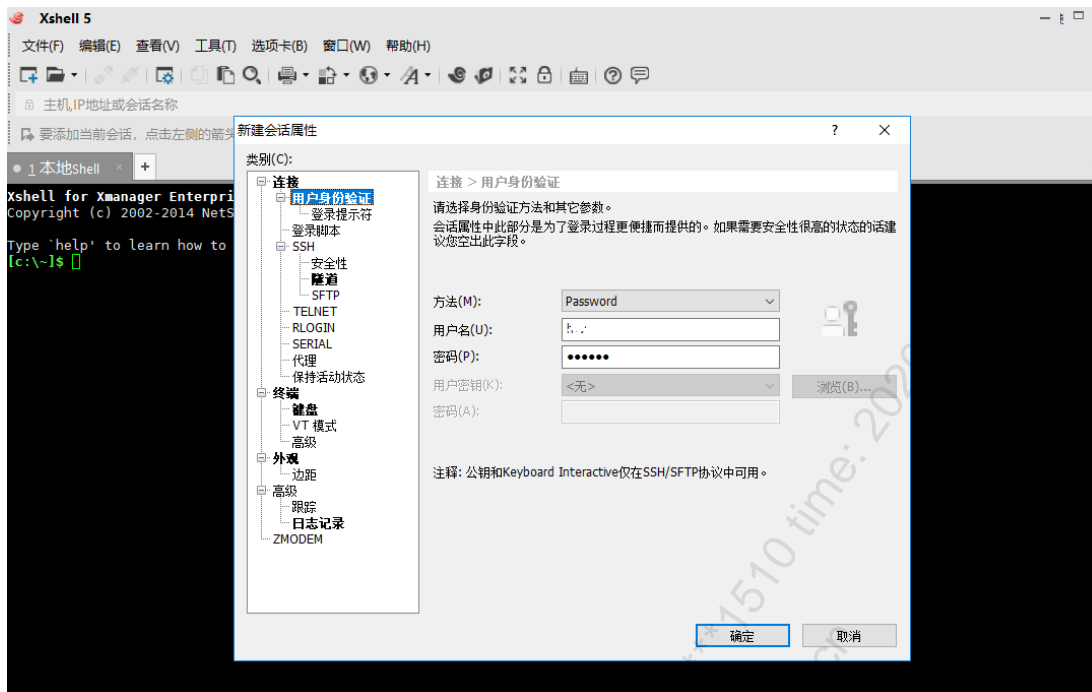
◆ C/S 运维（以 Xshell 工具为例）：

步骤1. 打开 Xshell 工具，在连接设置中输入 DAS-USM 的 IP 和 SSH 协议端口号（SSH 端口号可在“系统>网络配置”页面查看，默认为 60022）。

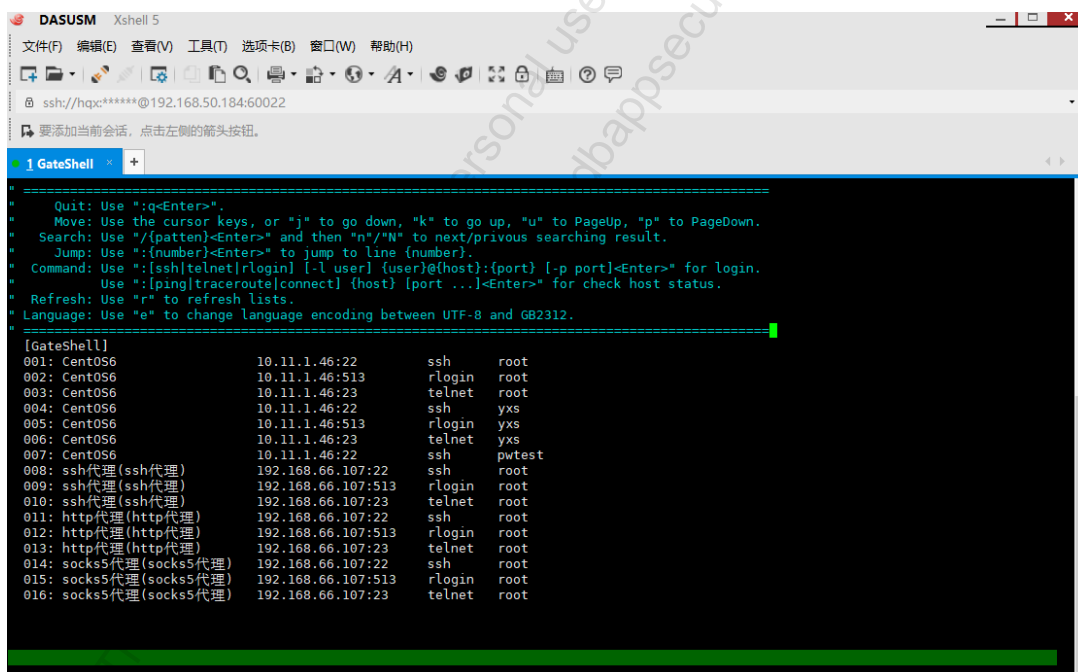


步骤2. 在用户身份验证设置中选择 Password 方式登录，输入 DAS-USM 的用户名和密码。或选择 Public Key 方式登录，选择对应的私钥，使用 Public Key 方式登录需要在 DAS-USM 的个人信息中配置用

户 SSH 公钥。



步骤3. 点击<确定>，连接 DAS-USM。成功登录系统后，进入资产选择界面，通过键盘的上、下箭头选择想要运维的服务器主机，按回车键即可登录目标服务器主机进行运维。

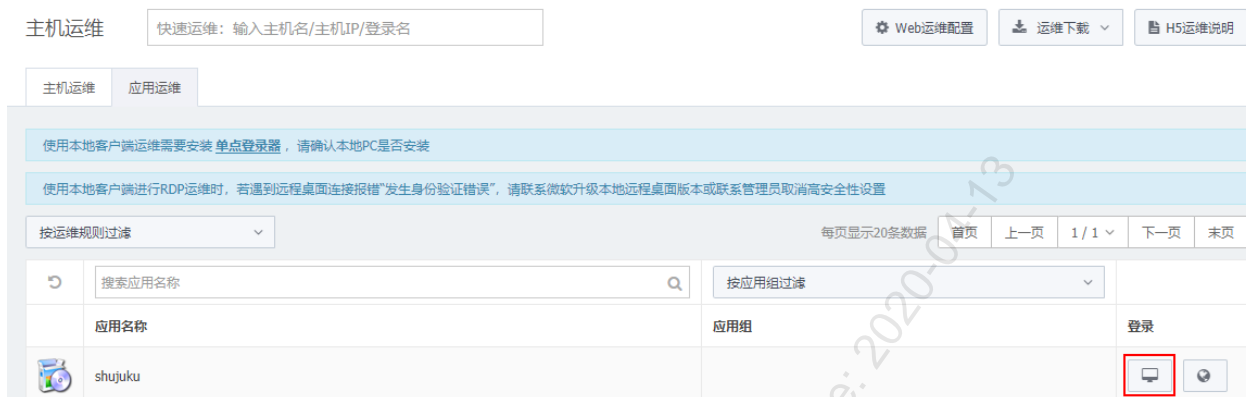


### 10.1.3 应用运维

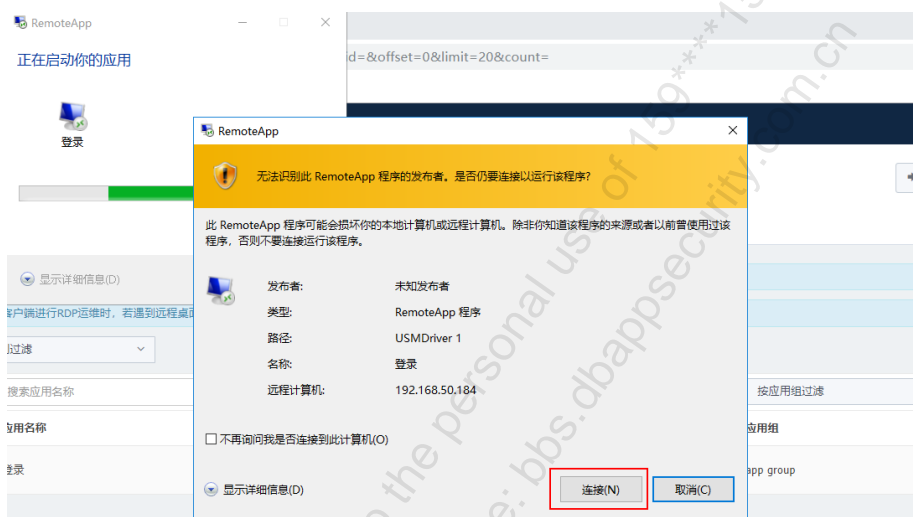
应用运维支持 B/S 和 H5 两种方式运维。

### ◆ B/S 运维:

步骤1. 在系统菜单栏点击“**运维>主机运维**”进入主机运维页面，点击<应用运维>进入应用运维页面。



步骤2. 在应用列表中点击<登录>列中的 图标，自动调用 RemoteApp 程序发起连接，点击<连接>，连接远程应用服务器运维。



### ◆ H5 运维

在应用运维页面，在应用列表中点击<登录>列中的 图标，通过 H5 客户端登入应用服务器进行应用运维。

## 10.2 实时监控

实时监控用于管理正在运维的主机的会话，进行命令审批或会话阻断等操作。操作方法如下：

在系统菜单栏点击“**运维>实时监控**”进入实时监控页面。点击<所有会话>页签，可查看当前正在运维的会话。点击<需要命令审批>页签，可查看当前正在运维且需要命令审批的会话。勾选会话后点击<阻断会话>可将正

在运维的会话阻断。

实时监控

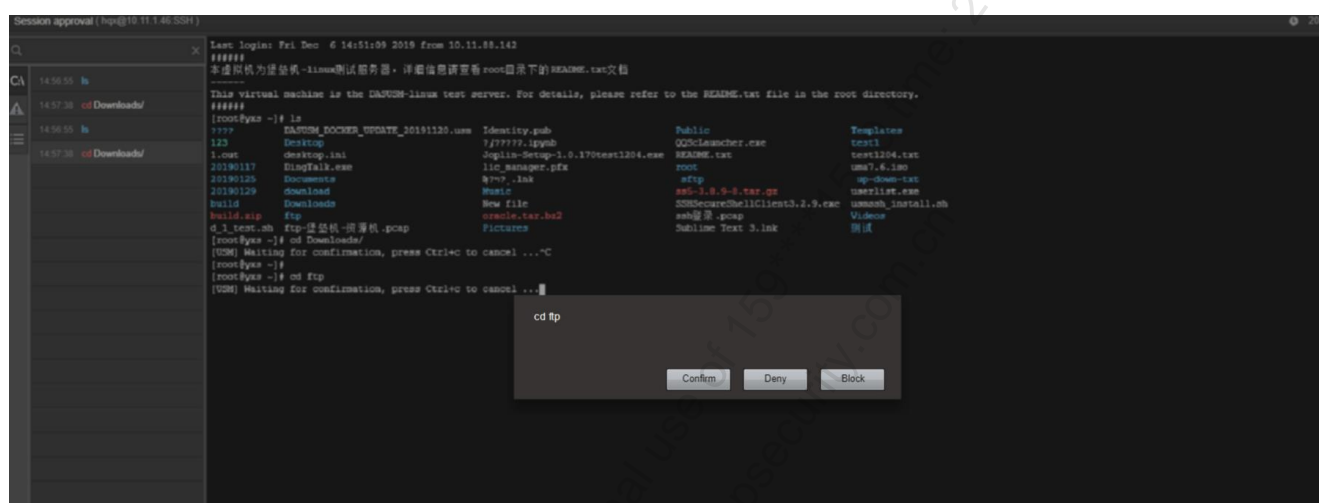
所有会话 1 需要命令审批 0

阻断会话 2

每页显示20条数据 首页 上一页 1/1 下一页 末页

类型	主机IP/主机名	协议/登录名	用户名/来源IP	开始时间/时长	操作
<input checked="" type="checkbox"/> SHELL	10.20.176.21 linux演示机	SSH root	admin 10.11.46.140	2019-12-30 09:50:11 31分48秒	播放 详情

在会话列表中点击<操作>列中的<播放>可查看会话内容。对于需要命令审批的会话，可在播放页面对命令操作进行审批。



## 10.3 命令审批

当运维员申请执行需要审批的命令时，管理员/命令审批人可对命令进行审批。命令审批的操作方法如下：在系统菜单栏点击“**运维**>命令审批”进入命令审批页面。勾选状态为“待审批”的条目，点击<允许>批准执行该命令；点击<拒绝>不允许执行该命令。

命令审批

每页显示20条数据 首页 上一页 1/1 下一页 末页

主机IP/主机名	协议/登录名	用户名/来源IP	命令	申请时间/审批时间	审批人	状态
10.11.1.46 CentOS6	TELNET root	hqx 10.10.200.31	cd test1	2019-12-06 15:31:56		待审批
10.11.1.46 CentOS6	TELNET root	hqx 10.10.200.31	cd test1	2019-12-06 14:57:55 2019-12-06 15:31:30	admin	已拒绝
10.11.1.46 CentOS6	SSH root	hqx 10.10.200.31	cd ftp	2019-12-06 14:57:44 2019-12-06 15:31:39	admin	已允许
10.11.1.46 CentOS6	SSH root	hqx 10.10.200.31	cd Downloads/	2019-12-06 14:57:00		已取消
10.11.1.46 CentOS6	Rlogin root	wusj_op 10.10.200.41	ls	2019-12-04 14:08:28		已取消
10.11.1.46 CentOS6	Rlogin root	wusj_op 10.10.200.41	ls	2019-12-04 14:08:06		已取消
10.11.1.46 CentOS6	Rlogin root	wusj_op 10.10.200.41	ls	2019-12-04 14:06:08 2019-12-04 14:07:01	wusj	已允许
10.11.1.46 CentOS6	TELNET root	wusj_op 10.10.200.41	ls	2019-12-04 14:04:10		已取消
10.11.1.46 CentOS6	SSH root	wusj_op 10.10.200.41	ls	2019-12-04 11:47:35		已取消

## 10.4 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，运维员也不能直接登录主机，系统会自动生成运维申请，由上层管理人员审批通过之后，运维员才能运维该主机。

运维审批的操作方法如下：

在系统菜单栏点击“**运维>运维审批**”进入运维审批页面，勾选状态为“待审批”的条目，点击<批准>并设置审批有效期，允许此次运维；或点击<拒绝>，不允许此次运维；点击<删除>可将运维申请从列表中删除。



在系统菜单栏点击“**运维>运维审批**”进入运维审批页面，点击<我的申请>进入我的申请页面。在本页面申请人可查看运维申请的审批情况。审批通过后，申请人可在此页面点击<本地客户端登录>或<H5 客户端登录>登录资产进行运维。



## 10.5 运维报表

运维报表用于统计当前用户的运维信息。

### 10.5.1 查看运维报表

在系统菜单栏点击“**运维>运维报表**”进入运维报表页面。选择用户及日期（今天、昨天、本周、本月）即可

查看到该用户相应时间段内的运维数据报表。

运维报表 报表自动发送

运维报表均以用户维度生成

用户: tets 日期: 2019-12-30 - 2019-12-30 今天 昨天 本周 本月 导出报表 ▾

[总览](#)
[运维次数](#)
[运维时长](#)
[活动时长](#)
[会话大小](#)
[字符命令数](#)
[传输文件数](#)
[来源IP访问数](#)
[运维时间分布](#)

总体	运维时长	活动时长
运维主机数 0	总运维时长 0 秒	总活动时长 0 秒
来源IP数 0	应用中心 0 秒	应用中心 0 秒
	SSH 0 秒	SSH 0 秒
	TELNET 0 秒	TELNET 0 秒
	RDP 0 秒	RDP 0 秒
	VNC 0 秒	VNC 0 秒
	FTP 0 秒	FTP 0 秒
	SFTP 0 秒	SFTP 0 秒

## 10.5.2 导出报表

点击<导出报表>，选择导出文件格式（DOC、PDF 和 HTML），可将报表数据导出至本地文件进行查看。

运维报表 报表自动发送

运维报表均以用户维度生成

用户: tets 日期: 2019-12-30 - 2019-12-30 今天 昨天 本周 本月 导出报表 ▾

[总览](#)
[运维次数](#)
[运维时长](#)
[活动时长](#)
[会话大小](#)
[字符命令数](#)
[传输文件数](#)
[来源IP访问数](#)
[运维时间分布](#)

导出DOC  
导出PDF  
导出HTML

## 10.5.3 报表自动发送

可设置将运维报表自动以邮件形式发送给本部门的部门管理员和审计管理员。操作方法如下：

**步骤1.** 点击<报表自动发送>。

运维报表 报表自动发送

运维报表均以用户维度生成

用户: tets 日期: 2019-12-30 - 2019-12-30 今天 昨天 本周 本月 导出报表 ▾

步骤2. 将状态设置为开启，选择发送周期和文件格式，点击<确定>。

报表自动发送 ×

---

如果开启了报表自动发送，在每个周期开始时，系统将会自动生成上一周期的运维报表，并以邮件形式发送给本部门的部门管理员和审计管理员。

状态	<input type="text" value="开启"/>
发送周期	<input checked="" type="checkbox"/> 每日 每日00:00发送
	<input checked="" type="checkbox"/> 每周 每周一00:00发送
	<input checked="" type="checkbox"/> 每月 每月一日00:00发送
文件格式	<input type="text" value="DOC"/>

This file is restricted to the personal use of 159\*\*\*\*1510 time: 2020-04-13  
source: bbs.dbappsecurity.com.cn

# 十一. 任务

系统提供自动化的任务功能，减轻用户的手工配置工作量。任务包括改密计划和自动运维两个功能。

## 11.1 改密计划

通过 DAS-USM 的改密计划功能，可以实现 SSH 协议帐户、Telnet 协议账户、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。

创建改密计划的的操作方法如下：

**步骤1.** 在系统菜单栏点击“**任务>改密计划**”进入计划列表页面，点击<**新建改密计划**>。

改密计划 + 新建改密计划

计划列表 全部托管帐户

开始  停止  删除
 每页显示20条数据 首页 上一页 1 / 1 下一页 末页

计划名称	部门	状态	执行方式	帐户数	上次执行时间	
<input type="checkbox"/> ewqewqe	用户根	已完成	手动执行	1	2019-12-27 07:04:20	密码导出
<input type="checkbox"/> test改密	用户根	已完成	定时执行	1	2019-12-17 17:50:54	密码导出
<input type="checkbox"/> asfkha	用户根	已停止	手动执行	1		密码导出
<input type="checkbox"/> eee	用户根	已停止	手动执行	1		密码导出

**步骤2.** 进入新建改密计划页面，填写计划名称，选择执行方式、改密方式、密码生成方式、密码发送方式，点击<**创建任务**>。

新建改密计划

\* 计划名称

\* 执行方式

\* 改密方式

\* 密码生成方式

\* 生成方式

密码复杂度  数字  小写字母  大写字母  其他字符 若全部均未勾选，则会在全部字符中随机生成，不会特定的包含某种字符

不包含字符集  生成的密码不会包含此集合中的字符

\* 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

在出现密码修改失败后，为防止密码丢失，该帐户下一次成功改密前仍会使用上一次准备的密码进行修改，此时将会出现同一任务密码不一致的情况。

\* 密码发送方式

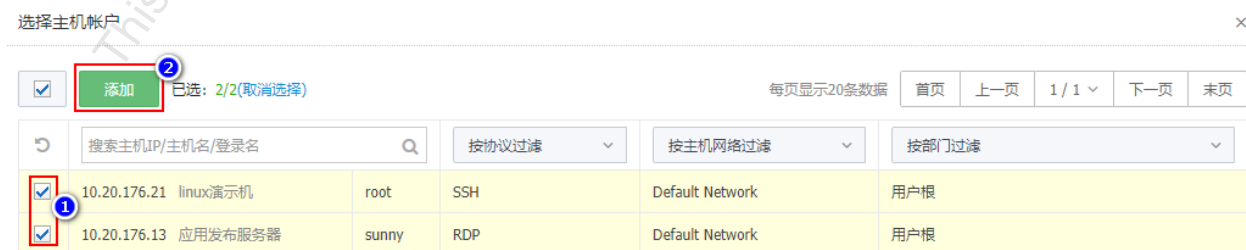
详细配置请参见下表。

配置项	说明
执行方式	支持手动执行、定时执行和定期执行。
改密方式	支持以下三种方式： <ul style="list-style-type: none"> <li>◆ 主动探测：在改密主机类型未知的情况下，通过探测确定主机类型进行改密。</li> <li>◆ 自定义：在已知主机类型的情况下，定义脚本命令来进行改密。了解脚本语法请点击&lt;帮助&gt;。</li> <li>◆ 改密脚本：改密脚本适用于多个计划中的托管帐户全部为同类系统中的帐户时，需要通过脚本改密的情况。改密脚本在“系统&gt;系统配置&gt;改密脚本”页面进行设置。</li> </ul>
密码生成方式	支持以下三种方式： <ul style="list-style-type: none"> <li>◆ 自动生成</li> <li>◆ 上传密码</li> <li>◆ 手工指定</li> </ul>
密码发送方式	支持以下四种方式： <ul style="list-style-type: none"> <li>◆ 不发送。</li> <li>◆ 邮件：以邮件形式发送至用户的邮箱。</li> <li>◆ FTP：发送至FTP服务器，可指定发送的文件路径，默认为用户账户根目录（例如 Windows 系统为 C:\Users\****，“****”为具体的用户名）。</li> <li>◆ SFTP：发送至 SFTP 服务器，可指定发送的文件路径，默认为用户账户根目录（例如 Windows 系统为 C:\Users\****，“****”为具体的用户名）。</li> </ul>

步骤3. 任务创建成功后将自动跳转到计划信息托管账户页面，点击<添加主机账户>。



步骤4. 在弹出的对话框勾选主机账户，点击<添加>。



进入计划列表页面，点击计划名称，进入编辑计划基本信息页面，可以修改计划名称、执行方式、密码生成方式和密码发送方式。

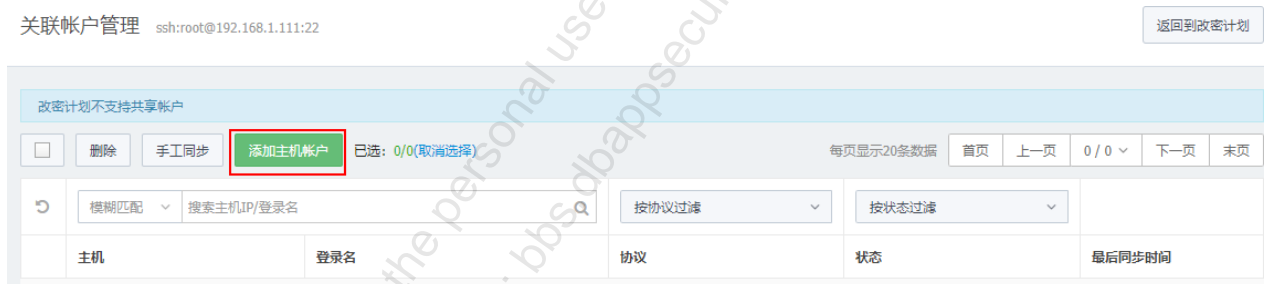
点击<托管账户>进入托管账户列表页面，可以添加、删除托管主机帐户。

DAS-USM 中托管了同一资产不同协议的同一帐户时，若其中一个协议帐户执行了改密，为使该帐户下的其他协议可以正常运维，需要将改密后的密码同步到该帐户下的所有协议中。操作方法如下：

**步骤1.** 在托管账户页面，点击托管帐户后的“操作>管理关联账户”。



**步骤2.** 进入关联帐户管理页，点击<添加主机帐户>。



**步骤3.** 在弹出对话框中，勾选主机账户，点击<添加>即可。

## 11.2 自动运维

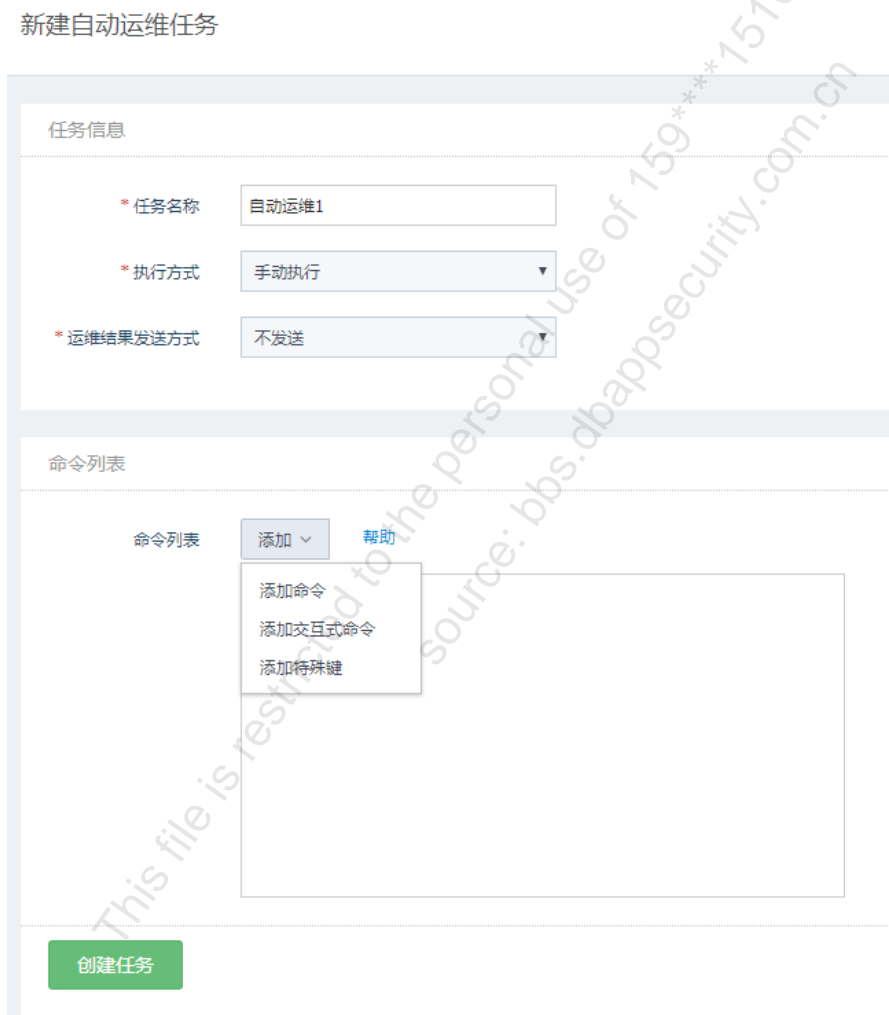
DAS-USM 支持自动运维操作，即由系统代替运维员进行自动化的运维操作。自动运维支持普通命令、交互式命令以及特殊键。

创建自动运维的操作方法如下：

**步骤1.** 在系统菜单栏点击“**任务>自动运维**”进入任务列表页面，点击<**新建自动运维任务**>。



**步骤2.** 进入新建自动运维任务页面。填写任务名称，选择执行方式、运维结果发送方式，添加运维命令，点击<**创建任务**>。

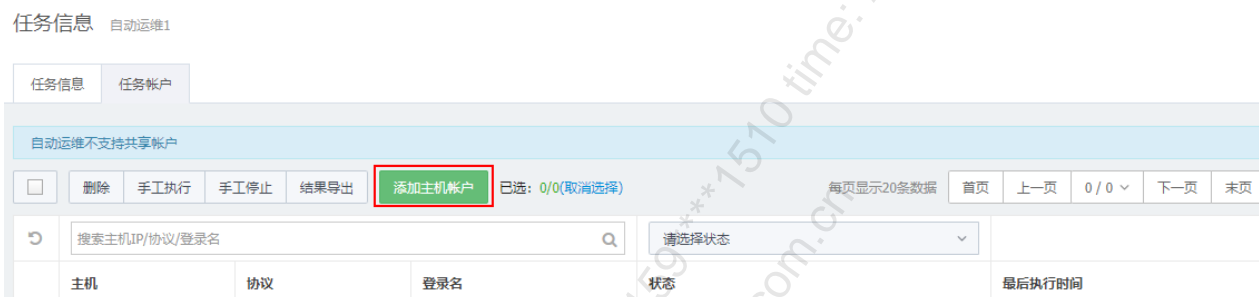


详细配置请参见下表。

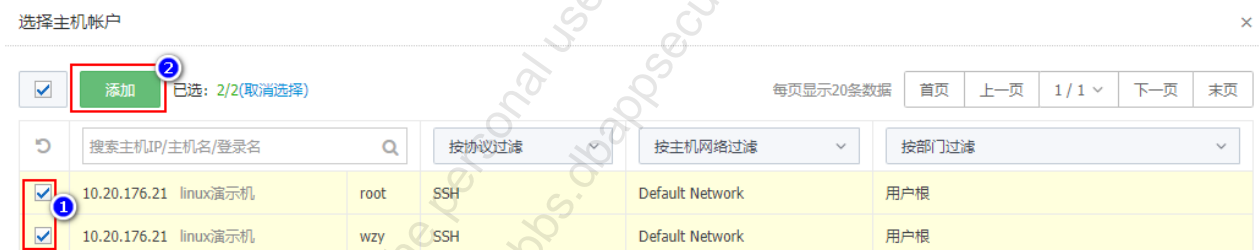
配置项	说明
执行方式	包括手动执行、定时执行和定期执行三种。
运维结果发送方式	包括以下四种方式：

配置项	说明
	<ul style="list-style-type: none"> <li>◆ 不发送。</li> <li>◆ 邮件：以邮件形式发送至用户的邮箱。</li> <li>◆ FTP：发送至 FTP 服务器，可指定发送的文件路径，默认为用户账户根目录（例如 Windows 系统为 C:\Users\****，**** 为具体的用户名）。</li> <li>◆ SFTP：发送至 SFTP 服务器，可指定发送文件路径，默认为用户账户根目录（例如 Windows 系统为 C:\Users\****，**** 为具体的用户名）。</li> </ul>
命令列表	支持命令、交互式命令和特殊键三种方式。关于命令列表的格式说明，请点击<帮助>进行查看。

步骤3. 任务创建成功后将自动跳转到任务信息任务账户页，点击<添加主机账户>。



步骤4. 勾选主机账户，点击<添加>。



## 十二. 系统管理

系统管理用于对 DAS-USM 进行系统配置，包括网络配置、VPN 管理、认证管理、系统配置、存储管理、操作日志、系统报表和本机维护。

### 12.1 网络配置

#### 12.1.1 基础设置

在系统菜单栏点击“**系统>网络配置**”进入网络配置页面，在网络配置页面可以配置 IPv4/6 接口信息、DNS 信息、协议端口信息、RDP 网关、TLS 安全性、聚合端口信息（仅硬件版支持）、物理端口信息（仅硬件版支持）以及查看业务数据流量统计（仅硬件版支持）。

配置相关信息后，点击<**保存更改**>即可保存配置成功。

网络配置

网络配置 Web配置 HA配置 静态路由 SNMP 集群配置 IP源防护

DNS信息

首选DNS

备选DNS

**保存更改**

---

协议端口

\* RDP   启用

\* SSH   启用

\* VNC   启用

\* FTP   启用

\* SQL Server   启用

\* MySQL   启用

\* Oracle   启用

\* DB2   启用

**保存更改**

---

RDP网关

\* RDP网关端口   启用

**保存更改**

---

TLS安全性配置

\* 高安全性  启用

开启后，ftps、rdg、rdp协议将只支持TLS1.2，禁止3DES和SHA1

**保存更改**

接口信息

设备名称	接口名称	速度	连通状态	IP地址	子网掩码	工作模式	接口配置
eth0	eth0		✓	10.20.176.20	255.255.255.0	single	<b>配置</b>

## 12.1.2 Web 配置

Web 配置是指对用户登录系统 Web 管理平台进行设置，包括登录时使用的端口、Web 证书配置等，以提高用户访问系统 Web 管理平台的安全性。

在系统菜单栏点击“**系统**»**网络配置**”进入网络配置页面，点击<**Web 配置**>页签进入 Web 配置页面。在 Web 配置页面可以配置 Web 设置、Web 证书配置、自定义 Web 证书，每一项配置完成后需要点击<**保存更改**>方可生效。

### 网络配置

网络配置	Web配置	HA配置	静态路由	SNMP	集群配置	IP源防护
Web设置						
* Web端口	<input type="text" value="443"/>					
安全性	<input type="checkbox"/> 增强HTTPS安全性 勾选后会使得部分低版本浏览器无法访问系统, 比如Windows XP系统的IE8及以下版本					
<b>保存更改</b>						
Web证书配置						
系统IP	<input type="text"/>					
	留空则清除证书配置					
<b>保存更改</b>						
自定义Web证书						
状态	未上传					
证书主题						
* 证书	<input type="button" value="上传文件"/> 仅支持PEM、DER格式证书					
* 私钥	<input type="button" value="上传文件"/> 仅支持RSA算法密钥					
加密口令	<input type="text"/> 没有加密口令请留空					
证书链	<input type="button" value="上传文件"/> (可选项) 包含多个PEM证书的文件					
<b>保存更改</b>						

详细配置请参见下表。

配置项	说明
Web 端口	访问 DAS-USM Web 管理平台所使用的端口号。
安全性	如勾选<增强 HTTPS 安全性>，部分低版本浏览器将无法访问系统，如 Windows XP 系统的 IE8 及以下版本。
系统 IP	证书服务器的 IP，留空则清除证书配置。
证书	仅支持 PEM、DER 格式证书。
私钥	仅支持 RSA 算法密钥。

### 12.1.3 HA 配置

HA (High Availability, 高可用性) 能够在通信线路或设备发生故障时提供备用方案，防止由于单个产品故障或链路故障导致网络中断，保证网络服务的连续性。实现 HA 功能需要部署两台同一型号的 DAS-USM 设备，并且选择同样的接口作为 HA 接口，先配置 HA 主机后配置 HA 备机。

**步骤1.** 在系统菜单栏点击“系统>网络配置”进入网络配置页面，点击<HA 配置>页签进入 HA 配置页面。选择当前运行模式为“热备模式-HA 主机”，选择数据同步接口，填写对端接口 IP (HA 备机接口 IP)、服务/虚拟 IP、子网掩码，设置心跳间隔 (仅硬件版支持)、宕机切换时间，设置 VRRP\_ID (仅云上版支持)，配置完成后点击<保存更改>，系统将自动重启切换为 HA 主机。

#### 网络配置

网络配置
Web配置
HA配置
静态路由
SNMP
集群配置
IP源防护

HA配置

\* 当前运行模式 热备模式-HA主机 状态说明

\* HA群组验证密钥 E6ED4AC11F47318EA4494B99D8013357

\* 数据同步接口 eth0

\* 本机接口IP 10.20.176.20

\* 对端接口IP 10.0.0.3

\* VRRP\_ID 64 1-254以内的整数，并确保与网络中的其他设备不冲突

\* 宕机切换时间 30 秒 30-300以内的整数

\* 业务接口设备 eth0

\* 服务/虚拟IP 192.168.1.10

\* 子网掩码 255.255.255.0

保存更改

**步骤2.** HA 主机切换完成后，将另一台 DAS-USM 配置为 HA 备机，选择当前运行模式为“**热备模式-HA 备机**”，选择数据同步接口，填写对端接口 IP（HA 主机 IP），将 HA 主机的 HA 群组验证密钥复制到 HA 备机的 HA 群组验证密钥中，点击<**保存更改**>，系统将自动重启切换为 HA 备机。重启完成后，等待数据同步完成。

#### 网络配置



## 12.1.4 静态路由

当 DAS-USM 存在多个路由出口时，需配置静态路由，以方便运维员通过 DAS-USM 登录不同路由出口的目标主机。



当 DAS-USM 仅有一个路由出口时，不能创建静态路由规则。

在系统菜单栏点击“**系统>网络配置**”进入网络配置页面，点击标签<**静态路由**>进入静态路由配置页面。选择出口设备，输入目的地址、子网掩码、下一跳网关，点击<**创建路由规则**>完成路由规则创建。点击规则后的<**删除**>即可删除相应的路由规则。

#### 网络配置



## 12.1.5 SNMP 配置

DAS-USM 支持通过 SNMP 协议对设备进行远程监控。SNMP 是简单网络管理协议 (Simple Network Management Protocol) 的简称, 是标准 IP 网络管理协议, 支持目前主流的网络管理系统, 用于监测网络上的设备是否有存在异常情况。

在系统菜单栏点击“系统>网络配置”进入网络配置页面, 点击标签<SNMP>进入 SNMP 配置页面。选择状态为开启, 设置系统标识、物理位置和联系方式, 点击<保存更改>进行 SNMP 全局设置; 选择 SNMP 版本、设置用户名、选择认证协议, 设置认证 key (6~64 位), 选择加密协议, 设置加密 key (6~64 位), 点击<创建社团>创建只读社团。此处设置应与 SNMP 网管软件设置保持一致。

### 网络配置



The screenshot shows the 'SNMP Configuration' interface with two main sections: 'SNMP配置' and '新建只读社团'.

**SNMP配置:**

- \* 状态: 开启
- \* 系统标识: DASUSM
- \* 物理位置: TestLocation
- \* 联系方式: admin@test.com
- 保存更改

**新建只读社团:**

- \* SNMP版本: v3
- \* 用户名: 333344
- \* 认证协议: SHA
- \* 认证key: [masked] 强度说明
- \* 加密协议: AES
- \* 加密key: [masked] 强度说明
- 创建社团

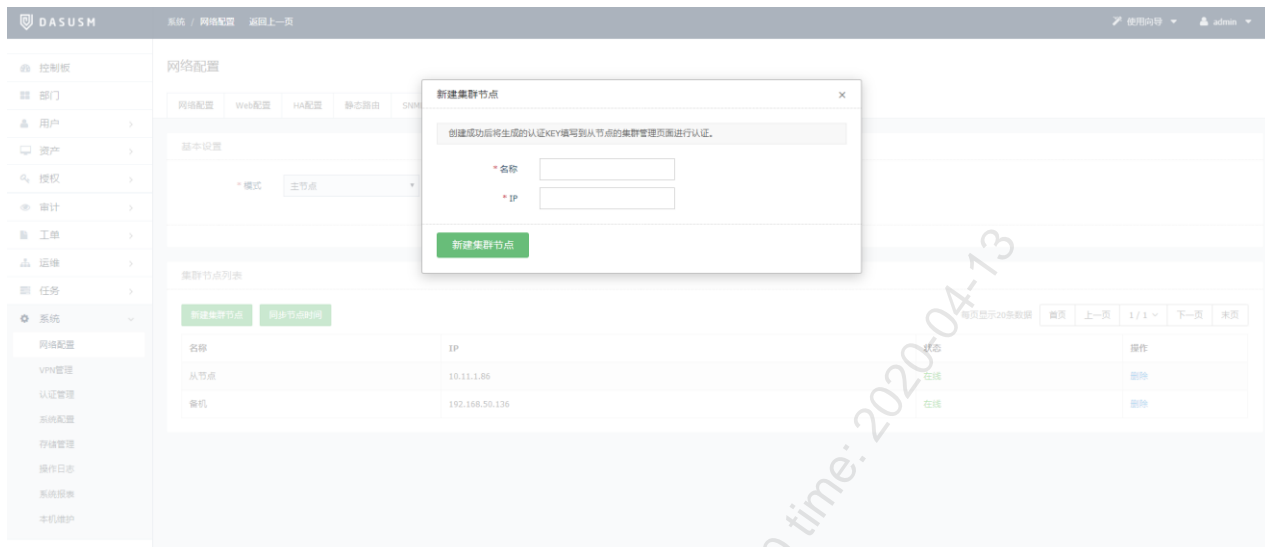
## 12.1.6 集群配置

DAS-USM 支持集群模式部署, 多台堡垒机组成集群提供更高业务处理性能及可靠性。在系统菜单栏点击“系统>网络配置”进入网络配置页面, 点击<集群配置>页签进入集群配置页面。对于云上版 DAS-USM, 集群功能需要配合 HA 功能使用, 集群主节点为 HA 主机, 单机只能设置为集群从节点。

设置主、从节点的操作方法如下:

**步骤1.** 在基本配置中选择模式为“主节点”, 点击<保存更改>。点击<新建集群节点>, 填写从节点名称和 IP,

点击<新建集群节点>，将生成的认证 KEY 复制备份。



步骤2. 在从节点集群配置页面，选择模式为“从节点”，填写主节点 IP 和新建集群节点时备份的认证 KEY，点击<保存更改>。

### 网络配置



## 12.1.7 IP 源防护

可设置黑名单模式或白名单模式对源 IP 进行防护，当设置为黑名单模式时，黑名单 IP 列表中的 IP 无法访问系统；当设置为白名单模式时，仅允许白名单列表中的 IP 访问系统。操作方法如下：

在系统菜单栏点击“系统>网络配置”进入网络配置页面，点击<IP 源防护>页签进入 IP 源防护配置页面。选择防护模式为黑/白名单模式，点击<添加黑名单 IP>/<添加白名单 IP>，填写黑/白名单 IP 后，点击<添加到 IP

列表>，点击<保存更改>。

### 网络配置

网络配置
Web配置
HA配置
静态路由
SNMP
集群配置
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 添加黑名单IP

	IP	地址段
<input type="checkbox"/>	192.6.3.3	192.6.3.3-192.6.3.3

## 12.2 VPN 管理

DAS-USM 内置 SSL VPN 功能，实现远程运维的安全接入。可通过以下步骤在设备上开启 VPN 功能：

**步骤1.** 在系统菜单栏点击“**系统>VPN 管理**”进入 VPN 管理基本配置页面。设置 VPN 状态为开启，填写 VPN IP 地址池、选择认证方式、设置 TCP 端口、UDP 端口等信息，点击<保存更改>。

### VPN管理

基本配置
活动会话

基本配置

\* 状态 开启

服务状态 正常

\* VPN IP地址池 192.168.0.0/24

1. 请确保该地址池不与堡垒机主机IP，热备模式备机IP，集群模式集群节点IP，用户网络网段及服务器网络网段冲突  
2. 尽量使用私有网络地址，例如10.1.1.0/24

\* 认证方式

密码

不支持中文用户名登录

\* TCP端口

60443

\* UDP端口

60443

启用 启用UDP传输后可增加传输效率

\* MTU手动探测

1420

启用 当出现VPN连接正常，但是某些数据流量不通的情况时，可尝试开启mtu手动探测，并改小mtu值。

\* 免登跳转  允许用户VPN登录后免登跳转至WEB页面

保存更改
重启服务

**步骤2.** 点击<活动会话>页签进入活动会话页面，可查看通过 VPN 运维的活动会话。

## 12.3 认证管理

### 12.3.1 安全配置

在 DAS-USM 的安全配置页面可以配置系统的登录安全性、用户名策略、用户密码策略等。操作方法如下：

**步骤1.** 在系统菜单栏点击“系统>认证管理”进入安全配置页面。在<登录配置>项中编辑登录超时时间，选择是否启用验证码，是否允许用户多地同时登录，是否禁止 admin 从 Web 登录，点击<保存更改>。

认证管理



**步骤2.** 在<用户锁定>项中，设置密码尝试次数、锁定时长和重置计数器，点击<保存更改>。

用户锁定



配置项说明请参见下表。

配置项	说明
密码尝试次数	允许用户尝试密码的次数，如果输入密码错误的次数达到设置值后，用户账号将被锁定，在锁定时长内不能登录系统。取值范围 0~999，设置为 0 表示不限制用户尝试密码的次数。
锁定时长	用户账号被锁定的时长，达到锁定时长后，用户可重新登录系统。取值范围 0~10080，设置为 0 表示账户被锁定后需要管理员手动进行解锁。
重置计数器	重置尝试密码次数的时间间隔。取值范围 1~10080。设置为 5 分钟，表示：当输入密码错误的次数小于密码尝试次数时，间隔 5 分钟后再尝试输入密码，此时用户输入密码的次数重新从 1 开始。

步骤3. 在<用户名策略配置>项，编辑用户名字符黑名单（创建的用户名不能包含用户名字符黑名单，例如当设置用户名黑名单为 dd 时，则用户名不能设置为\*dd\*，“\*”表示任意字符串），点击<保存更改>。

用户名策略配置

用户名字符黑名单

```
srre
dddgg
dd
```

对用户名所包含的字符串进行检查，每行只算一个字符或者字符串

保存更改

步骤4. 设置用户密码配置策略，点击<保存更改>。

用户密码策略配置

长度  -  有效值6-64

复杂度  数字  小写字母  大写字母  其他字符 密码中必须出现的字符种类。

相关度

用户名  密码不得与用户名相同

密码不得与用户名逆序相同

历史密码  个 改密时检查的历史密码个数，有效值为0-5；为0时，则不检查历史密码

密码使用限制  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。

密码过期前警告时间  天 密码过期前多少天进行提醒。如果设置为0，则不提醒。

保存更改

部分配置说明请参见下表。

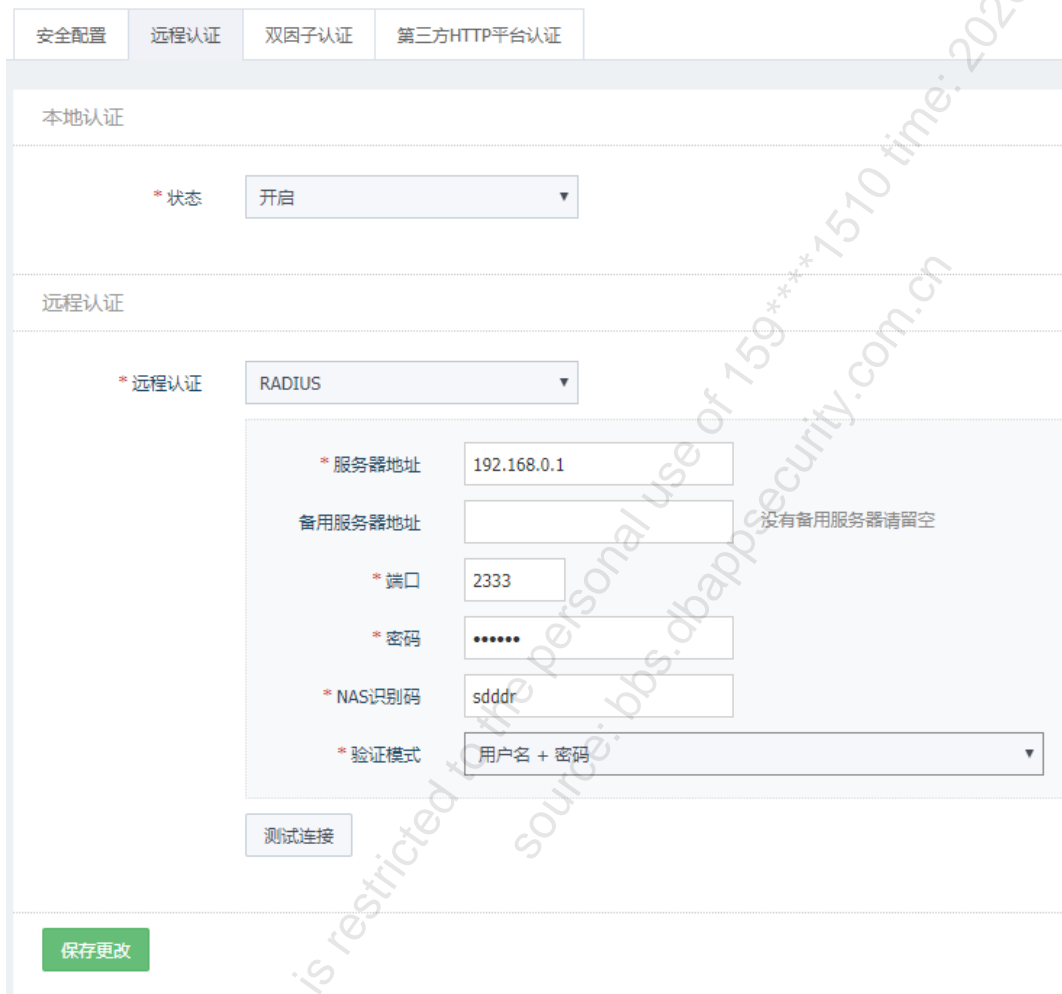
配置项	说明
长度	密码长度，取值范围 6~64 字符。
复杂度	密码中必须出现的字符，包括数字、大写字母、小写字母和其他字符。
密码使用期限	取值范围 0~999，设置为 0 表示密码不过期。
密码过期前警告时间	设置密码过期前多少天，系统提醒用户修改密码。设置为 0，表示不提醒。

## 12.3.2 远程认证

远程认证是指当用户登录系统时，调用远程服务器对用户账户信息进行认证，认证通过后方可登录系统。远程认证的配置方法如下：

在系统菜单栏点击“系统>认证管理”进入安全配置页面，选择**远程认证**页签进入远程认证配置页面。在本地认证项中设置是否开启本地认证。在远程认证项中设置远程认证模式，填写远程认证服务器信息，填写完成后点击<保存更改>。

### 认证管理



详细配置请参见下表。

配置项	说明
远程认证	<p>设置远程认证的类型，包括 LDAP、AD 和 RADIUS 三种。关闭表示不启用远程认证。</p> <ul style="list-style-type: none"> <li>● LDAP 是轻量目录访问协议（Lightweight Directory Access Protocol）的缩写，是互联网上目录服务的通用访问协议。LDAP 服务可以有效解决众多网络服务的用户账户问题，LDAP 服务器是用于查询和更新 LDAP 目录的服务器，包括用户账号目录。</li> <li>● AD 是活动目录（Active Directory）的缩写，用于在 Windows 服务器集中管理所有 Windows 账户、登录密码及权限。AD 服务器可实现集中的安全管理和统一的安全策略。</li> </ul>

配置项	说明
	<ul style="list-style-type: none"> <li>RADIUS 是远程认证拨号用户服务（Remote Authentication Dial In User Service）的缩写，广泛应用于小区宽带上网、IP 电话、移动电话预付费、无线网络接入等业务。RADIUS 服务器负责接收用户的连接请求、认证用户，然后向请求方返回所有必要的配置信息。</li> </ul>
<b>Radius</b>	
服务器地址	远程认证服务器的 IP。
端口	远程认证服务器的端口。
密码	远程认证服务器的密码。
NAS 识别码	网络访问服务器识别码，认证服务器配置文件中 nastype 字段内容。
验证模式	进行远程认证时的模式，包括：用户名+密码、用户名+动态口令、用户名+动态口令+令牌 PIN 三种。
<b>AD</b>	
服务器地址	AD 域控服务器的地址，可为 IP 地址或域名。
端口	AD 域控服务器的端口。
Base DN	AD 域控服务器的根节点，即 AD 服务器收到认证请求时目录查询的起始点。
域	AD 域控服务器的域名称。
账号	AD 域控服务器的账户。
密码	AD 域控服务器账户对应的密码。
过滤器	过滤条件，符合过滤条件的用户将被同步至 DAS-USM。
<b>LDAP</b>	
服务器地址	LDAP 域控服务器的地址，可为 IP 地址或者域名。
端口	LDAP 域控服务器的端口。
Base DN	LDAP 域控服务器的根节点，即 LDAP 服务器收到认证请求时目录查询的起始点。
账号	LDAP 域控服务器的账号。
密码	LDAP 域控服务器账号对应的密码。
过滤器	过滤条件，符合过滤条件的用户将会被同步至 DAS-USM。
登录名属性	LDAP 用户登录名的属性，例如 uid、sn 等。



当认证模式选择 LDAP 或者 AD 时，保存更改后，点击<立即同步用户>会将配置信息立即同步至用户。如果选择了<自动同步用户>，则系统将在 5 小时内将配置信息同步至用户。

### 12.3.3 双因子认证

双因子认证是指用户登录 DAS-USM 时，除了需要密码认证成功之外还需要其他一种因子（如短信口令）认

证成功后才可成功登录 DAS-USM。

**步骤1.** 在系统菜单栏点击“**系统>认证管理**”进入安全配置页面，选择**双因子认证**页签进入双因子认证配置页面。勾选需要启用的认证方式，点击<**保存更改**>。

#### 认证管理



勾选<**短信口令**>后，需要进行短信配置；勾选<**第三方 USBKEY**>后，需进行第三方 USBKEY 通用配置。

**步骤2.** 设置短信配置，选择状态，编辑相关信息（具体配置参数请咨询选中的短信服务提供商），点击<**保存更改**>。

#### 短信配置

步骤3. 配置第三方 USBKEY 通用配置，配置完成后，需要点击<保存更改>。

第三方USBKEY通用配置

---

已支持厂家：北京数字认证股份有限公司

\* 状态 开启

可信任证书链

状态 未配置

更改配置 上传证书链

由多个PEM证书文件压缩生成的zip文件

吊销列表

\* 检查方式 不检查

保存更改

步骤4. 设置吉大正元配置，需要关闭北京数字认证股份有限公司的认证，配置完成后需要点击<保存更改>。

吉大正元配置

---

\* 状态 开启

\* 认证服务器地址 192.168.0.3

\* 端口 2334

\* 应用标识 SDDRTTTT

保存更改

### 12.3.4 第三方 HTTP 平台认证

第三方 HTTP 平台认证是指通过网易将军令或其他第三方平台认证登录 DAS-USM。

步骤1. 在系统菜单栏点击“系统>认证管理”进入安全配置页面，选择**第三方 HTTP 平台认证**页签进入第三方 HTTP 平台认证配置页面。

**步骤2. 网易将军令配置。**在网易将军令配置中设置状态为开启，配置相关信息，点击<保存更改>。

网易将军令配置

---

\* 状态

\* 认证URL

\* Product

\* Token

\* 公钥

\* 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。

详细配置请参见下表。

配置项	说明
认证 URL	认证 URL 中包含了认证所需的用户名、密码等关键字。需要以实际情况为准。
Product	网易将军令用于验证的 header 信息中的 product 关键字。
Token	网易将军令用于验证的 header 信息中的 token 关键字。
公钥	网易将军令用于验证的 header 信息中的密钥。
HTTP 状态码	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。

**步骤3. 第三方平台单点登录认证配置。**在第三方平台单点登录认证中设置状态为开启，填写认证 URL，点击<保存更改>。

第三方平台单点登录认证

---

\* 状态

\* 认证URL

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。

步骤4. JWT 免登认证配置。在 JWT 免登认证配置中设置状态为开启，点击<上传证书>上传 PEM 证书文件，填写用户字段名称等信息，点击<保存更改>。

JWT免登认证配置

\* 状态

\* 证书  未配置  
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

步骤5. 江苏意源配置。在江苏意源配置中设置状态为开启，填写认证服务器地址、服务器认证端口、客户端认证端口、应用标识，点击<保存更改>。

江苏意源配置

\* 状态

\* 认证服务器地址

\* 服务端认证端口

\* 客户端认证端口

\* 应用标识

以上第三方 HTTP 平台认证参数，请咨询对应的服务提供商。

## 12.4 系统配置

### 12.4.1 运维配置

#### 12.4.1.1 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，支持 Web 未授权登录及 API 未授权登录。

在系统菜单栏点击“系统>系统配置”进入运维配置页面。在未授权登录项中配置未授权登录选项。

### 系统配置

系统配置

运维配置
  告警配置
  语言和界面
  功能设置
  SSH KEY配置
  改密脚本

运维配置

未授权登录

允许Web未授权登录
  允许API未授权登录

收集未授权登录  
 收集主机帐户和密码  
 自动创建运维规则

此三项不支持无需验证用户名和密码的目标机器，如部分交换机和防火墙

详细配置请参见下表。

配置项	说明
允许 Web 未授权登录	允许未授权的用户通过 Web 方式登录主机。
允许 API 未授权登录	允许未授权的用户通过 API 方式登录主机。
收集未授权登录	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。
收集主机账户和密码	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帐户和密码。
自动创建运维规则	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。

### 12.4.1.2 运维登录配置

在运维登录项中配置运维登录选项。

- 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 不同应用共享的同一会话的审计权限由第一个应用决定，若您有严格细致的审计规则，不建议开启此功能

详细配置请参见下表。

配置项	说明
允许使用用户密码登录主机	允许用户使用 DAS-USM 帐户登录主机，主要适用于用户和帐户同属于 AD/LDAP 的场景。
允许使用 SSH 私钥登录主机	勾选此项后，系统将允许用户无需输入密码，直接使用 SSH 私钥登录主机进行运维。
允许使用 SSH-agent-forwarding 方式登录 SSH 服务器	勾选此项后，系统将支持 SSH-agent-forwarding 特性，适用于 SSH 服务器要求采用 publickey 方式登录的场景。需要在 SSH 登录项中设置 SSH banner。
开启应用会话共享	勾选此项后，不同应用共享的同一会话，审计权限由第一个应用决定。

### 12.4.1.3 SSH 登录配置

在 SSH 登录项中配置 SSH 登录选项。

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  变量名称可自定义
- 发送运维来源IP  变量名称可自定义

- Shell使用命令行方式 便于熟悉使用命令行的用户使用

SSH banner  最大长度64个字符。例如：OpenSSH\_7.6

详细配置请参见下表。

配置项	说明
允许使用公钥登录	勾选此项后，用户可以使用 SSH 公钥登录运维审计系统和目标服务器。
允许使用密码登录	勾选此项后，用户将通过密码登录运维审计系统和目标服务器。
允许发送环境变量	勾选此项后，用户可以选择允许发送运维用户信息和运维来源 IP。
Shell 使用命令行方式	勾选此项后，将通过命令行方式登录系统。
SSH banner	配置此项后方可使用 SSH-agent-forwarding 方式登录 SSH 服务器。

### 12.4.1.4 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。

运维时长限制  空闲时长超过  分钟 时自动断开连接

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、SQL server、Oracle：客户端和服务端均无数据发送时。

## 12.4.2 告警配置

在系统菜单栏点击“系统>系统配置”进入运维配置页面，点击<告警配置>页签进入告警配置页面。

### 12.4.2.1 邮件告警配置

在邮件配置项中配置邮件的地址、端口、账号、密码、收件人邮箱，点击<保存更改>保存邮件配置。点击<发

送测试邮件>可测试邮件是否配置成功。

邮件配置

\* 发送方式

\* 服务器地址

\* 端口   SSL

\* 帐号   匿名发送

\* 收件人  多个收件人用";"隔开

### 12.4.2.2 Syslog 配置

在 Syslog 配置项中填写发送者标识、Syslog 服务器 IP、端口，选择数据格式，点击<保存更改>保存 Syslog 配置。点击<发送测试数据>可测试 Syslog 是否配置成功。

Syslog配置

\* 发送者标识

\* 服务器IP

\* 端口

\* 数据格式  建议使用JSON格式

### 12.4.2.3 告警外送配置

在告警外送配置项中将操作日志状态设置为开启，勾选需要外送的告警等级（包括邮件告警和 Syslog 告警），

点击<保存更改>。

### 告警外送配置

操作日志 开启

邮件告警  低  中低  中  
 中高  高

Syslog告警  低  中低  中  
 中高  高

主机命令  外送到syslog服务器  
发送“事件查询”页面中的主机命令到syslog服务器

保存更改

#### 12.4.2.4 系统资源告警配置

在系统资源告警配置项中设置告警阈值，勾选启用邮件告警，点击<保存更改>。当达到告警阈值时系统将会发送告警邮件。

### 系统资源告警配置

告警阈值

网卡流量达到规格的	80	%	时执行告警
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
配置数据分区使用率达到	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

#### 12.4.3 语言和界面

在系统菜单栏点击“系统>系统配置”进入运维配置页面。选择语言和界面页签进入语言和界面配置页面。在语言设置项中可以设置系统语言。在 Logo 设置项中可以上传自定义 Logo。

系统支持三种界面显示语言：简体中文、繁体中文和英文。启用了允许用户切换界面语言选项时，用户在登录时可以自由选择界面语言。当用户选择的界面语言设置与系统语言设置不一致时，系统外送的各类通知、日志

等文本将仍然使用系统语言设置的语言。

## 系统配置

运维配置	告警配置	语言和界面	功能设置	SSH KEY配置	改密脚本
------	------	-------	------	-----------	------

语言设置

\* 系统语言 简体中文

界面语言  允许用户切换界面语言

启用允许用户切换界面语言选项，用户在登录时可以选择偏好的界面语言。  
当用户选择的界面语言设置与系统语言设置不一致时，系统外送的各类通知、日志等文本将仍然使用系统语言设置。

保存更改

Logo 设置

登录页 Logo 上传图片

图片尺寸：宽度小于等于 300px，高度小于等于 64px；支持的图片格式：png, gif, jpg；图片大小：小于 1MB

顶部 Logo 上传图片

图片尺寸：宽度小于等于 160px，高度小于等于 32px；支持的图片格式：png, gif, jpg；图片大小：小于 1MB

## 12.4.4 功能设置

在系统菜单栏点击“系统>系统配置”进入运维配置页面。选择功能设置页签进入功能设置页面。

### 12.4.4.1 部门管理

开启部门管理后，可以实现用户、资产的层级管理。设置状态为“开启”，点击<保存更改>。

部门管理

适用于需要对系统对象进行分隔管理的场景。系统对象包含用户，资产，授权和审计数据等

开启部门管理后，管理员角色将只能管理本部门及下级部门的系统对象，不能管理上级或同级部门的系统对象

开启部门管理后，每增加一个系统对象，都要设置其所属部门

设置太多层级的部门有可能会引起系统对象难以管理，权限混乱的情形。请合理安排部门层级。

\* 状态 开启

保存更改

## 12.4.4.2 主机导出配置

当设置不导出密码时，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。选择是否导出密码，点击<保存更改>。操作方法如下：

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

## 12.4.4.3 工单配置

关闭工单功能后，运维员无法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。开启工单功能时，勾选<过期自动删除>，运维规则过期后，用户在运维界面将无法看到通过工单生成的过期的运维规则。完成配置后需要点击<保存更改>。

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

## 12.4.4.4 同品牌数据库审计系统 API 访问键设置

API 访问键用于为第三方开发人员提供相应应用接口。设置 API 访问键的操作方法如下：勾选<启用>，点击<重置>重置 API 访问键（可选操作），点击<保存更改>。

同品牌数据库审计系统API访问键配置

API访问键  启用

API访问键 ..... 显示 重置

创建时间 2019-11-28 10:51:08

保存更改

## 12.4.4.5 报表自动统计

开启报表自动统计后，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。

设置状态为“开启”或“关闭”，点击<保存更改>。

### 报表自动统计

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

\* 状态

保存更改

## 12.4.5 SSH KEY 配置

当用户有多个 DAS-USM 时并且需要配合 HAProxy 等负载均衡产品使用，需要将多个 DAS-USM 的 SSH KEY 配置为相同时，才可以正常使用负载均衡功能。

在系统菜单栏点击“系统>系统配置”进入运维配置页面。选择 SSH KEY 配置页签进入 SSH KEY 配置页面。在客户端生成私钥后，点击<上传新 DSA 私钥>或<上传新 RSA 私钥>弹出私钥上传对话框，输入私钥后点击<上传 DSA 私钥>或<上传 RSA 私钥>。

### 系统配置

运维配置	告警配置	语言和界面	功能设置	SSH KEY配置	改密脚本
<p>DSA密钥</p> <p>系统DSA指纹 22:1a:0a: [REDACTED]</p> <p>系统DSA公钥  <pre>ssh-dss zBiDh4MM udixLLaF AAAFQChG Wa8mNSD3 dNNvk+r+ IdFVAKGA ViTdw2AS rDtXhxQ5</pre> </p> <p>上传新DSA私钥</p>					

## 12.4.6 改密脚本

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](#)。

新建改密脚本的操作方法如下：

**步骤1.** 在系统菜单栏点击“**系统>系统配置**”进入运维配置页面。点击<改密脚本>进入改密脚本页面，点击<新建改密脚本>。



**步骤2.** 在创建改密脚本弹窗中填写脚本名称和脚本命令（关于脚本命令的说明可点击<帮助>进行查看），点击<创建>完成改密脚本创建。



## 12.5 存储管理

### 12.5.1 数据归档

数据归档是指对会话的录像进行归档，并对归档文件设置自动删除规则。操作方法如下：

**步骤1.** 在系统菜单栏点击“**系统>存储管理**”进入数据归档页面。在数据盘使用状态项中可以查看详细的数据

## 盘分区使用状态。

### 存储管理



**步骤2.** 在录像归档项中可以开启录像归档功能，将会话文件保存到远程归档服务器中。设置录像归档的状态为“开启”，选择传输模式，设置归档时段、传输速度限制、归档服务器地址、端口、用户名密码和归档路径，点击<保存更改>保存录像归档配置。

### 录像归档

\* 状态: 开启 录像归档开启时将审计数据转储到存储服务器，关闭时录像存储在本设备上

\* 时段:  -  每天进行录像归档的时段，有效值0-23

\* 速度限制:  MB/s 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: FTP

\* 服务器地址:

\* 端口:

\* 用户名:

\* 密码:

\* 路径:  相对路径，例如填写：/test（对应的绝对路径为：文件服务器配置路径/test）；请确保用户具有此路径的写入权限

步骤3. 在自动删除项中设置自动删除条件，点击<保存更改>，可以自动清理系统数据盘空间。

自动删除

---

自动删除  自动删除  天 前的录像 有效值1-9999，自动删除历史审计数据，节省系统空间

当会话分区可用空间不足  GB 时删除最早的录像  
有效值1-999999，默认值15，请勿轻易修改此值

删除选项  只删除已归档的录像

---

## 12.5.2 日志备份

在系统菜单栏点击“系统>存储管理”进入数据归档页面。选择日志备份页签进入日志备份页面。选择需要备份的时间范围和备份内容，点击<创建日志备份>。

存储管理

数据归档 日志备份

---

日志备份

时间范围  -

备注

内容  操作日志  会话日志

---

在备份列表中可查看创建的日志备份，点击<操作>列中的<下载>可将备份下载到本地文件中查看。点击<操作>列中的<删除>可以删除日志备份。

备份列表

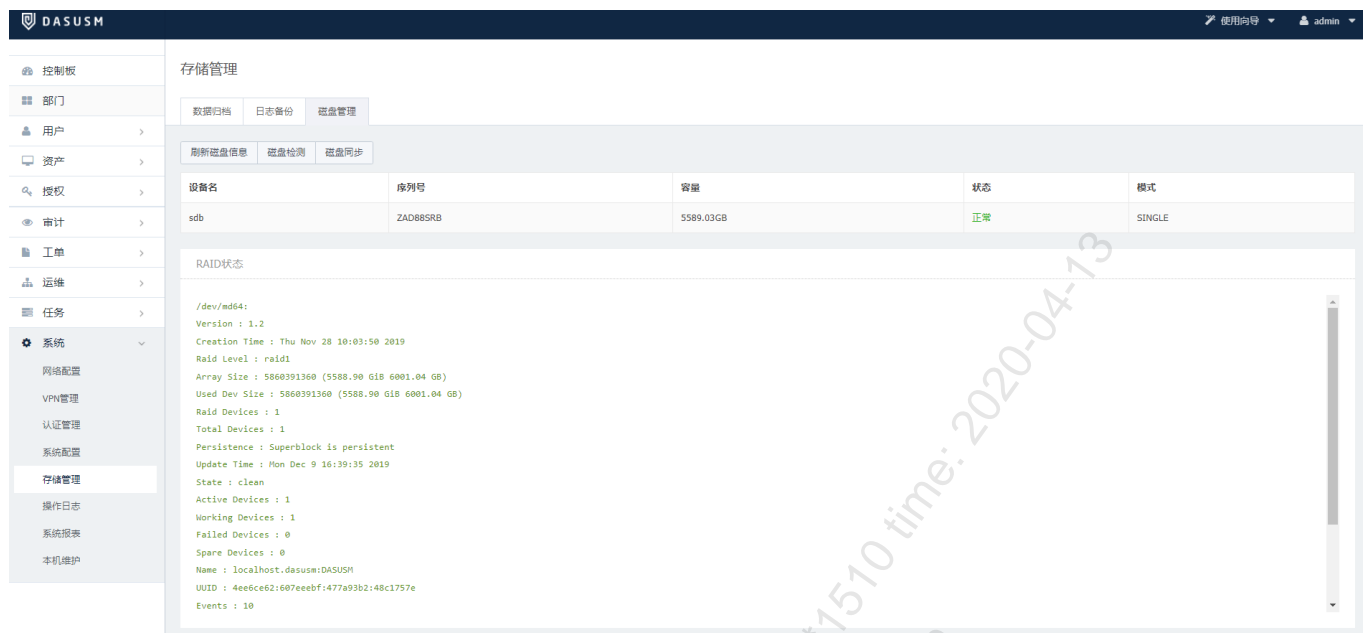
保存时间	备注	文件大小	操作
2019-12-30 20:12:28	2019-12-11_2019-12-19	9.79KB	<input type="button" value="下载"/> <input type="button" value="删除"/>

## 12.5.3 磁盘管理

磁盘管理功能仅适用于硬件版。

在系统菜单栏点击“系统>存储管理”进入数据归档页面。选择磁盘管理页签进入磁盘管理页面。点击<磁盘检

测>可以检测系统磁盘信息。点击<磁盘同步>可以同步系统磁盘信息。



## 12.6 操作日志

在系统菜单栏点击“系统>操作日志”进入操作日志页面，设置时间，点击<展开更多搜索条件>可设置其他搜索条件，点击<搜索>可查询搜索结果。点击<导出日志>可将日志文件导出至本地。

操作日志



点击<操作日志配置>页签进入操作日志配置页面，选择日志类型，设置重要性，点击<保存更改>。点击<恢复

默认设置>可恢复默认配置。

操作日志

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
中	中	串口登录
中	中	串口退出
低	低	用户认证
中低	中低	登录系统, 用户VPN认证未启用
中	中	VPN登录连接
中	中	VPN免登WEB

保存更改
恢复默认设置

## 12.7 系统报表

系统报表是用于统计系统的状态及操作记录（包括系统状态信息、操作重要性、用户控制、主机控制、会话控制、用户与资产操作、用户源 IP、异常用户和异常 IP）。

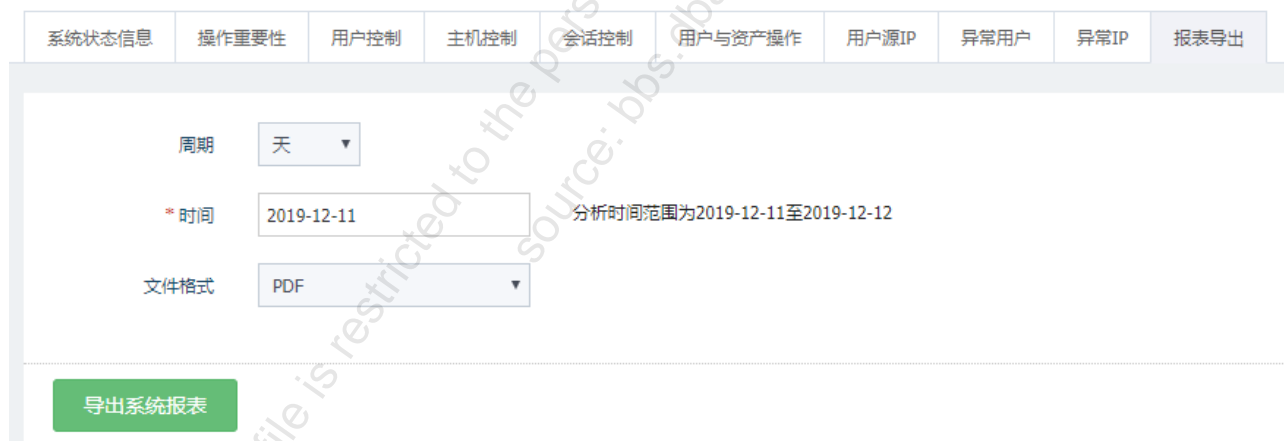
在系统菜单栏点击“系统>系统报表”进入系统报表页面。选择按小时/按天/按周/按月查看系统报表各项数据。

### 系统报表



点击<报表导出>页签进入报表导出页面，选择报表分析时间范围和导出文件格式，点击<导出系统报表>，将系统数据报表导出至本地进行查看。

### 系统报表



The form is used for exporting system reports. It includes the following fields and options:

- 周期 (Period):** 天 (Day)
- \* 时间 (Time):** 2019-12-11. 分析时间范围为2019-12-11至2019-12-12
- 文件格式 (File Format):** PDF

A green button labeled "导出系统报表" (Export System Report) is located at the bottom of the form.

## 12.8 本机维护

本机维护是指对系统进行维护管理，主要包括系统管理、系统升级、许可证管理、系统备份等。

### 12.8.1 系统管理

**步骤1.** 在系统菜单栏点击“系统>本机维护”进入系统管理页面，在系统时间项中设置时间服务器，勾选<自动同步>可自动同步时间服务器的时间；点击<同步服务器时间>可同步时间服务器的时间；点击<同步

浏览器时间>可同步浏览器时间。

本机维护



步骤2. 在系统工具项中，点击<重启设备>，在弹出的对话框中点击<确定>可以重启设备；点击<关闭设备>，在弹出的对话框中点击<确定>可关闭设备；点击<恢复出厂设置>，在弹出的对话框中点击<确定>可恢复设备的出厂设置。

## 12.8.2 系统升级

步骤1. 在系统菜单栏点击“系统>本机维护”进入系统管理页面，点击<系统升级>页签进入系统升级页面。点击<上传系统升级文件>，选择系统升级文件并上传。

本机维护



步骤2. 上传完成后点击<开始升级>进行系统升级，若暂时不需要升级，可点击<取消本次升级操作>。

系统升级

开始升级

文件上传已完成，点击按钮开始升级。

冷补丁及版本升级会重启服务，将造成短暂的业务中断，耗时约2-8分钟。

如果暂时不需要升级，可以[取消本次升级操作](#)

### 12.8.3 许可证

只有取得合法的许可证文件并导入系统后，才能正常使用产品的功能。许可证到期后，需要导出系统认证文件，并与产品服务人员联系以获取新的许可证。操作方法如下：

步骤1. 在系统菜单栏点击“系统>本机维护”进入系统管理页面，点击<许可证>页签进入许可证管理页面。点击<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。

许可证管理

申请许可证

如需申请许可证，请导出系统认证文件，并与相关人员联系。

生成系统认证文件

步骤2. 点击<备份许可证>，可将当前许可证文件导出到本地保存。

备份许可证

当得到有效许可证文件之后，将原有的许可证导出到本地备份保存。

备份许可证

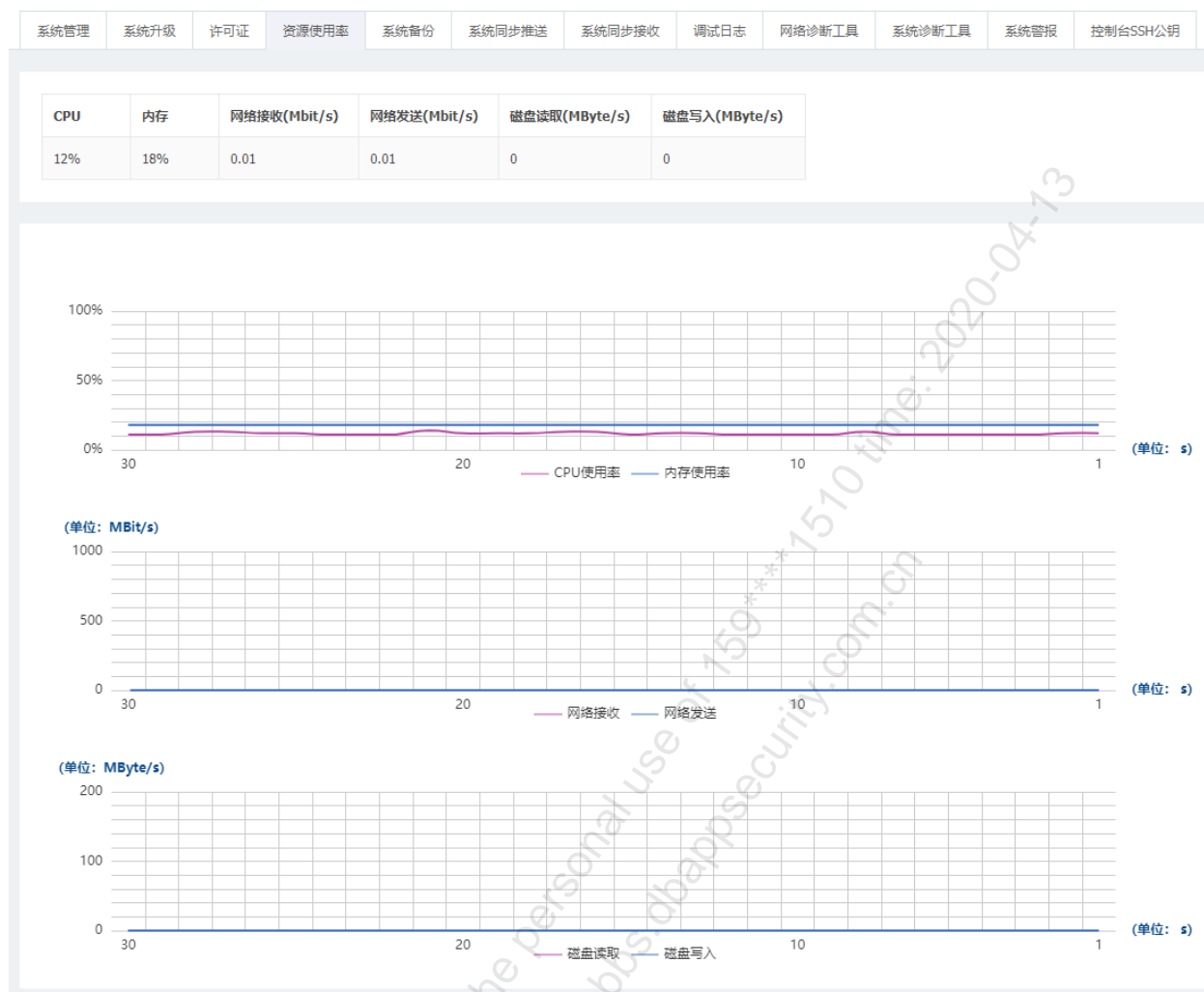
步骤3. 获取新的许可证文件后，点击<上传许可证>，可将已申请的许可证文件从本地上传到系统。上传完成后点击<导入许可证>，将新的许可证导入到系统中。

### 12.8.4 资源使用率

在系统菜单栏点击“系统>本机维护”进入系统管理页面，点击<资源使用率>页签进入资源使用率页面。可查

看系统资源状态，如 CPU 使用率、内存使用率、网络速率、磁盘读写速率等。

本机维护



## 12.8.5 系统备份

系统备份功能可在系统配置出错或者系统配置数据丢失时，对系统配置进行还原，减少系统配置工作量。

**步骤1.** 在系统菜单栏点击“系统>本机维护”进入系统管理页面，点击<系统备份>页签进入系统备份页面。

**步骤2.** 在系统配置自动备份区设置状态为开启，填写备份周期、备份保留数目。设置下次执行时间（建议设置

为业务量较低的时间点), 点击<保存更改>, 系统将会按照设置的时间及周期自动创建备份文件。

#### 系统配置自动备份

\* 状态

\* 周期  天 有效值1-60

\* 保留自动备份数  有效值1-30, 当自动备份数量超过此限制时会自动删除最早自动备份文件

\* 下次执行时间

上次执行时间 2019-12-31 00:06:47

保存更改

步骤3. 在系统配置手动备份项中填写备份备注, 点击<创建系统配置备份>可手动创建系统配置备份文件。

#### 系统配置手动备份

手动备份数目上限30, 当前数目: 2

备注

创建系统配置备份

步骤4. 在备份列表中可以点击<下载>将备份文件下载到本地。点击<还原>, 在弹出的对话框中点击<确定>可将系统还原至当前备份文件中的配置。点击<删除>, 在弹出的对话框中点击<确定>可以删除备份文件。

#### 备份列表

每页显示20条数据   1 / 1

创建时间	按备份类型过滤	创建人	备注	文件大小	操作
2019-12-31 10:29:52	手动备份	admin		36.32KB	<input type="button" value="还原"/> <input type="button" value="下载"/> <input type="button" value="删除"/>
2019-12-31 10:29:45	手动备份	admin		36.29KB	<input type="button" value="还原"/> <input type="button" value="下载"/> <input type="button" value="删除"/>
2019-12-31 00:06:47	自动备份	[system]		36.28KB	<input type="button" value="还原"/> <input type="button" value="下载"/> <input type="button" value="删除"/>

此外, 您还可以通过手动上传系统配置文件还原系统配置。操作方法如下:

步骤1. 在系统配置上传还原项中点击<上传系统配置文件>, 选择文件并上传。

#### 系统配置上传还原

上传系统配置文件

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。



请在还原系统配置前备份系统的当前配置，并确保上传的备份文件完整。

**步骤2.** 上传完成后点击<还原系统配置>即可将系统还原至上传的配置文件中的配置。若不需要还原此配置，点击<取消还原>即可取消系统配置还原操作。

#### 系统配置上传还原

还原系统配置

文件上传已完成，点击按钮进行还原。

若想重新上传，请先 [取消还原](#)

请在还原系统配置前先进行系统配置备份，并确保上传的备份文件完整。

## 12.8.6 系统同步推送/接收

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.** 在推送系统配置的 DAS-USM 系统菜单栏点击“系统>本机维护”进入系统管理页面，点击<系统同步推送>页签进入系统同步推送页面。将状态设置为开启，设置推送周期，点击<重置>设置推送密码，点击<保存更改>。

### 本机维护

系统管理	系统升级	许可证	资源使用率	系统备份	系统同步推送	系统同步接收	调试日志	网
<p>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。 增加目标设备IP之后，需要在目标设备的系统配置接收选项里填写本设备的推送密钥。</p>								
<p>系统配置推送</p>								
* 状态	<input type="text" value="开启"/>							
* 推送周期	<input type="text" value="3"/> 分钟							
推送密钥	<input type="password" value="....."/>							<a href="#">显示</a> <a href="#">重置</a>
密钥创建时间	2019-12-31 10:46:32							
<p><a href="#">保存更改</a></p>								

**步骤2.** 编辑目标 IP 和 Web 端口，点击<添加目标>可添加推送目标。在推送目标列表中点击<手动推送>可以

手动推送系统配置。

#### 添加推送目标

名称	<input type="text"/>
* 目标IP	<input type="text" value="192.168.0.3"/>
* Web端口	<input type="text" value="3333"/>

添加目标

步骤3. 在接收系统配置的 DAS-USM 系统菜单栏点击“系统>本机维护”进入系统管理页面，点击<系统同步接收>页签进入系统同步接收页面。设置状态为开启，将源设备系统同步推送页面的密钥填写到接收设备中，点击<保存更改>即可接收推荐的系统配置。

#### 本机维护

系统管理	系统升级	许可证	资源使用率	系统备份	系统同步推送	系统同步接收	调试日志
------	------	-----	-------	------	--------	--------	------

开启系统配置接收，系统将允许其他设备向本设备推送系统配置。  
需要设置源设备的推送密钥。

#### 系统配置接收

* 状态	<input type="text" value="开启"/>
* 源设备密钥	<input type="text" value="....."/> <a href="#">显示</a>

保存更改

### 12.8.7 调试日志

在系统菜单栏点击“系统>本机维护”进入系统管理页面，点击<调试日志>页签进入调试日志页面，可查看系统调试日志信息。点击<关闭刷新>可关闭调试日志的刷新。点击<导出日志>可将调试日志导出到本地文件中

查看。

本机维护

系统管理	系统升级	许可证	资源使用率	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
------	------	-----	-------	------	--------	--------	------	--------	--------

关闭刷新 导出日志

```

2019-12-31 09:21:09.838173 [28240] [D1] SSH: drain client buffer 0/0, flush peer ioqueue 0/0
2019-12-31 09:21:09.838470 [28240] [D1] RIO: close rio '171e5e5f5e0aa27600000002030000005' ok
2019-12-31 09:21:09.838559 [28240] [D1] SSH: detach channel-1 from bridge-0 'linux演示机_10.20.176.21:22'
2019-12-31 09:21:09.838577 [28240] [D1] SSH: free channel-1 '171e5e5f5e0aa27600000002030000005', iostat rP/wC 8/8 rC/wP 237/288, sP/sC 0/0 qP/qC 0/0
2019-12-31 09:21:09.838605 [28240] [D1] SSH: Client channel-3 'subsystem' request CLOSE
2019-12-31 09:21:09.838615 [28240] [D1] SSH: drain client buffer 0/0, flush peer ioqueue 0/0
2019-12-31 09:21:09.838713 [28240] [D1] SSH: Peer channel-3 request EOF
2019-12-31 09:21:09.838737 [28240] [D1] SSH: drain peer buffer 0/0, flush client ioqueue 0/0
2019-12-31 09:21:09.838766 [28240] [D1] SSH: [USM] Peer 127.0.0.1:50468 socket closed
    
```

## 12.8.8 网络诊断工具

在系统菜单栏点击“系统>本机维护”进入系统管理页面，点击<网络诊断工具>页签进入网络诊断工具页面。

### 12.8.8.1 连通性检测

在连通性检测项中可以检测主机的 IP 或端口是否连通、路由是否可达、TCP 端口、UDP 端口是否正常。本文以 PING 类型举例说明。

选择类型为 PING，设置主机地址，点击<执行测试>即可查看测试结果。

本机维护

系统管理	系统升级	许可证	资源使用率	系统备份	系统同步推送	系统同步接收	调试
------	------	-----	-------	------	--------	--------	----

连通性检测

\* 类型

\* 主机地址

```

PING 192.168.0.3 (192.168.0.3) 56(84) bytes of data.
--- 192.168.0.3 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 12999ms
    
```

### 12.8.8.2 TCPDUMP 抓包

在 TCPDUMP 抓包项中填写抓包主机 IP、端口、包数量，选择监听端口，点击<开始>开始抓包。点击<停止>后即可停止抓包，并在右侧显示<下载>按钮和<删除>按钮。点击<下载>按钮即可将文件下载至本地，使用

Wireshark 软件查看，点击<删除>按钮可将抓包文件删除。

#### TCPDUMP抓包

主机IP

端口  1-65535之间的有效端口号

监听接口

包数量  内置的TCPDump每次可以抓取最多5000个数据包

## 12.8.9 系统诊断工具

在系统菜单栏点击“系统>本机维护”进入系统管理页面，点击<系统诊断工具>页签进入系统诊断工具页面，选择系统诊断信息类型（包括综合信息、系统负载、内核信息等）即可查看相应类型的诊断信息。

#### 本机维护

系统管理	系统升级	许可证	资源使用率	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
------	------	-----	-------	------	--------	--------	------	--------	--------

系统诊断

综合信息

```

loadavg: 0.15 0.15 0.21 1/512 30721

MemTotal: 8009412 kB
MemFree: 6304668 kB
MemAvailable: 6318664 kB
Buffers: 0 kB
Cached: 232736 kB

nr_free_pages 1576167
nr_alloc_batch 1042
nr_inactive_anon 2737
nr_active_anon 315504
nr_inactive_file 32034

Personalities :
unused devices: <none>

No bonding informations.

```

点击<下载诊断日志>即可将诊断日志下载至本地。

```

综合信息
-----
loadavg: 0.15 0.15 0.21 1/512 30721

MemTotal: 8009412 kB
MemFree: 6304668 kB
MemAvailable: 6318664 kB
Buffers: 0 kB
Cached: 232736 kB

nr_free_pages 1576167
nr_alloc_batch 1042
nr_inactive_anon 2737
nr_active_anon 315504
nr_inactive_file 32034

Personalities :
unused devices: <none>

No bonding infomations.
    
```

下载诊断日志

## 12.8.10 系统警报

在系统菜单栏点击“系统>本机维护”进入系统管理页面，点击<系统警报>页签进入系统警报页面。勾选告警日志，点击<确认警报>确认警报日志；勾选告警日志，点击<导出系统告警日志>，可将系统警报日志导出到本地查看。

本机维护

系统管理	系统升级	许可证	资源使用率	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															
<div style="display: flex; justify-content: space-between; align-items: center;"> <div> <input checked="" type="checkbox"/> 确认警报                     <span style="margin-left: 20px;">导出系统告警日志</span> </div> <div>                         每页显示20条数据                         <span style="margin-left: 10px;">首页</span> <span style="margin-left: 10px;">上一页</span> <span style="margin-left: 10px;">1/3</span> <span style="margin-left: 10px;">下一页</span> <span style="margin-left: 10px;">末页</span> </div> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30px;"></th> <th style="width: 30%;">时间</th> <th style="width: 35%;">警报内容</th> <th style="width: 15%;">确认时间</th> <th style="width: 10%;">确认者</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>2019-12-27 00:00:09</td> <td>许可证 非正式</td> <td></td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>2019-12-26 00:00:12</td> <td>许可证 非正式</td> <td></td> <td></td> </tr> </tbody> </table>													时间	警报内容	确认时间	确认者	<input checked="" type="checkbox"/>	2019-12-27 00:00:09	许可证 非正式			<input checked="" type="checkbox"/>	2019-12-26 00:00:12	许可证 非正式		
	时间	警报内容	确认时间	确认者																						
<input checked="" type="checkbox"/>	2019-12-27 00:00:09	许可证 非正式																								
<input checked="" type="checkbox"/>	2019-12-26 00:00:12	许可证 非正式																								

## 12.8.11 控制台 SSH 公钥

控制台 SSH 公钥用于支持维护人员登录 DAS-USM 后台收集支持维护所需信息。生成控制台 SSH 公钥时系统会保存公钥并显示私钥的内容，但不会保存私钥，维护人员需妥善保管好私钥。若不慎遗失私钥，请及时重置或清除控制台 SSH 公钥。

在系统菜单栏点击“系统>本机维护”进入系统管理页面，点击<控制台 SSH 公钥>进入控制台 SSH 公钥页面。点击<重置控制台 SSH 公钥>，在弹出的对话框中点击<确定>可重置控制台 SSH 公钥；点击<清除控制

台 SSH 公钥>，在弹出的对话框中点击<确定>可清除控制台 SSH 公钥。

本机维护

系统管理	系统升级	许可证	资源使用率	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 93:91: [REDACTED]

控制台SSH公钥

```
ssh-dss
G67Qu8j
yS1zTZ+
AAAFQCo
1ewaAKg
Jz8NscM
3xMIkr9
AN0BJAK
eeItt3S
```

[REDACTED]

重置控制台SSH公钥    清除控制台SSH公钥

This file is restricted to the personal use of 159\*\*\*\*1510 time: 2020-04-13  
 source: bbs.dbappsecurity.com.cn