思福迪
运维安全管理系统
使用指南
（管理人员）

杭州思福迪信息技术有限公司

目录

1. 概述

思福迪运维安全管理系统为云服务器的运维提供完整的权限控制和审计回放服务。思福迪运维安全管理系统基于账号（Account）、认证（Authentication）、授权（Authorization）、审计（Audit）的AAAA统一管理方案，通过身份管理、授权管理、双因子认证、实时会话监控与切断、审计录像回放、高危指令查询等功能，增强运维管理的安全性。

思福迪运维安全管理系统符合各类法令法规的要求，包括等级保护、银监会、证监会、PCI安全标准委员会、企业内控管理等相关政策规定要求。

本指南主要针对各类云平台的统一运维管理系统使用进行指导说明。

2. 环境确认

2.1 管理账号

在使用思福迪运维安全管理系统之前，请确认你已经找思福迪运维安全管理系统部署的管理员拿到了超级管理员的账号和初始密码：

角色	账号及权限说明
超级管理员	超级管理员账号:admin 初始密码：safetybase 使用超级管理员能够进行系统的任何操作，包括设置、添加资产、审计等操作。
系统管理员	系统管理员由超级管理员手工创建，只能对系统管理进行配置，不能进行审计操作。
审计管理员	审计管理员由超级管理员手工创建，只能对用户管理、会话审计和审计规则及实时监控，不能对系统进行配置。
密码管理员	密码管理员由超级管理员手工创建，可对密码进行托管、修改、录入等操作。
运维人员	运维人员由管理员手工创建，只能对有权限的主机进行运维操作，不能对系统进行配置，也不能对审计信息进行查询操作。

操作步骤：

1. 打开Chrome浏览器。
2. 在地址栏中，输入https://思福迪运维安全管理系统的访问地址，按回车键（Enter），进入系统登录页面。
3. 在思福迪运维安全管理系统登录页面，输入用户名、密码及验证码。
4. 单击**登录**。

注意：第一次**登陆**系统时，建议修改默认密码。

2.2 工具下载

在进行服务端配置前，先下载安装思福迪运维安全管理系统的插件。本小节将介绍软件下载的方法（安装步骤省略）。

操作步骤：

1. 打开Chrome浏览器。
2. 在地址栏中，输入https://思福迪运维安全管理系统的访问地址，按回车键（Enter），进入系统登录页面。
3. 使用admin账号登陆统一运维管理系统页面，然后点击左侧的“系统管理”，在右侧选择“软件管理”，如下图所示：

4. 在相关下载页面，下载并安装“BhostClient”插件，如下图所示：

- BHostClient:运维及配置插件（运维用户必须安装：**建议运维用户将软件安装在D盘**，如果没有D盘的安装在C:\Program\Files路径下）；
- **密码查看器：**查看下载的密码文件时需要安装；

- BHostReplay:用于播放离线的审计录像【**管理员角色建议安装这个版本的客户端**，如果您之前已经安装了**BHostClient客户端**，需要**先卸载**再安装BHostReplay】。

5. 管理员也可以上传指定的运维工具到相关下载中，如Putty、Xshell、Winscp、CRT等运维软件。

   注意：BhostReplay客户端是包含BHostClient的，**管理员角色**查看录像回放及运维时，**只需要安装BHostReplay**就可以了。

3. 服务端配置

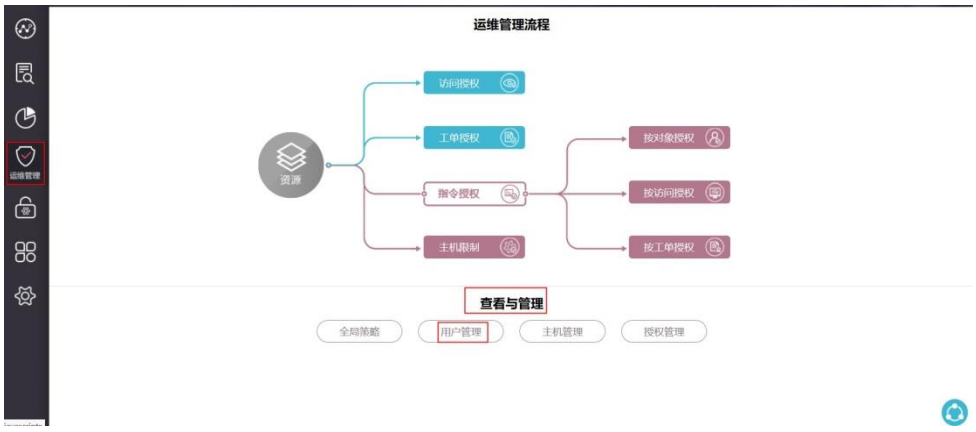
思福迪运维安全管理系统支持手工添加和自动导入主机资产及用户信息，管理员人员可以根据需要参考3.1-3.2的手工添加或参考3.3-3.4的说明进行用户和资产的自动导入。

3.1 手工添加用户组并添加用户

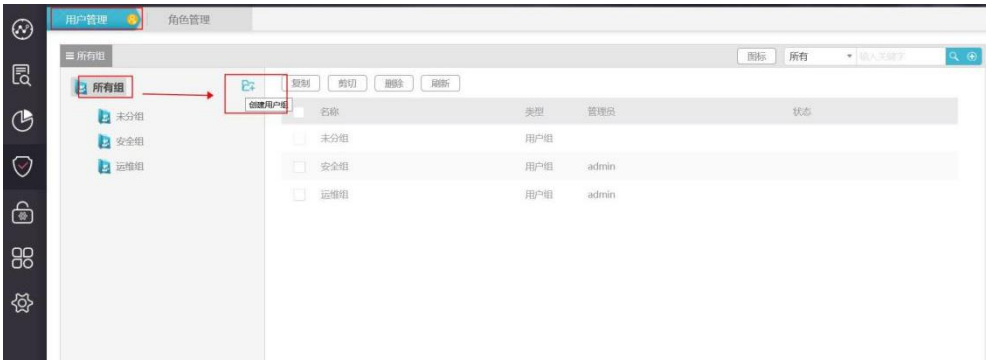
操作步骤：

1. 使用系统管理员*#admin#*登录思福迪运维安全管理系统。

2. 点击左侧的“运维管理”选项，在右侧的“查看与管理”页面中单击“用户管理”如下图所示：



3. 在弹出的“用户管理”页面中，点击“所有组”右侧的“创建用户组”按钮，在弹出的创建用户组页面中输入组名称，组的描述，点击保存按钮，如下图所示：



4. 在用户管理中点击创建的用户组名称，选择右上角的“创建用户”选项，在弹出的创建用户页面，填写相关的信息（比如账号名、姓名、

密码、工号、邮箱等），并选择角色，运维人员一般选择“运维用户角色”其它用户角色，管理员用户可自定义配置，具体如下图所示：

新建用户参数说明：

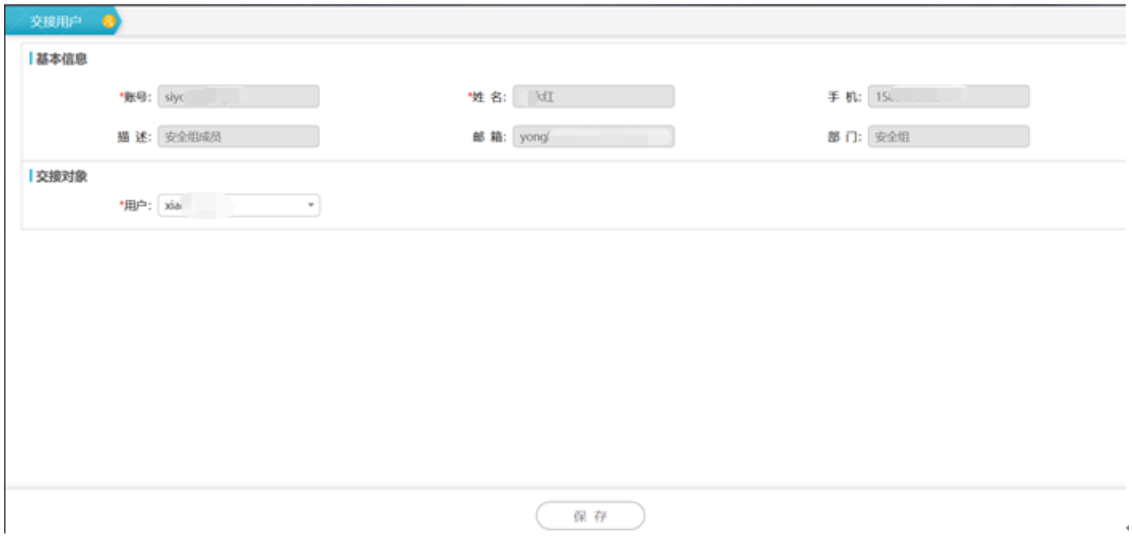
参数	说明
启用	是否启用该用户，勾选后该用户才可以使用。
账号	添加的用户名。
姓名	显示的用户名称。
描述	用户的描述。

认证方式	可选择多因子认证或单用户名密码验证选项。 设置密码：用户第一次登陆不需要修改密码。可直接使用管理员设置的密码登陆。（不建议） 初始密码：用户第一次登陆，强制用户更改密码。（建议选该项）
初始密码	设置用户登陆的密码。
工号	用户的工号（非必填项）
部门	用户所属的部门。
手机	用户的手机号。
邮箱	用户的邮箱信息。
操作	默认为角色定义，可自己选择用户的角色。 角色继承：无须选择权限。
角色	只有选择了角色定义才能手工选择用户的角色信息，一般选择运维用户。
扩展选项	用户登陆安全配置【如果勾选了**唯一登陆**，当前用户只能同时在1台终端上运维】。
访问授权	用户授权策略选择，可以后面自定义。
用户组	可选择用户所属的组，同一个用户可以属于多个不同的组下面。

5. 用户添加成功后，【可按步骤1-4的方式，添加其它用户信息】，具体如下图所示：

6. **用户修改说明：**可以对添加的用户进行：复制、剪切、粘贴、删除、移除等操作。如下图所示：

- **复制：**可从A用户组中选中一个用户，在B用户组中粘贴，从而实现A用户同时属于A用户组和B用户组（也可以通过编辑用户属性-在用户组中勾选多个用户组实现）；
- **剪切：**可从A用户组中选中一个用户，剪切到B用户组中去粘贴，从而实现将属于A用户组的用户移动到B用户组中去。
- **粘贴：**将复制或剪切的用户，复制或移动到其它指定的用户组中。
- **删除：**将选中的用户删除，左侧所有用户组中将不存在该用户。
- **移除：**将选中的用户从当前用户组中移除，其它用户组若还有该用户则不会被移除。
- **交接：**若某用户A临时请假，可在请假前将账号权限交接给用户 B，如下图所示：

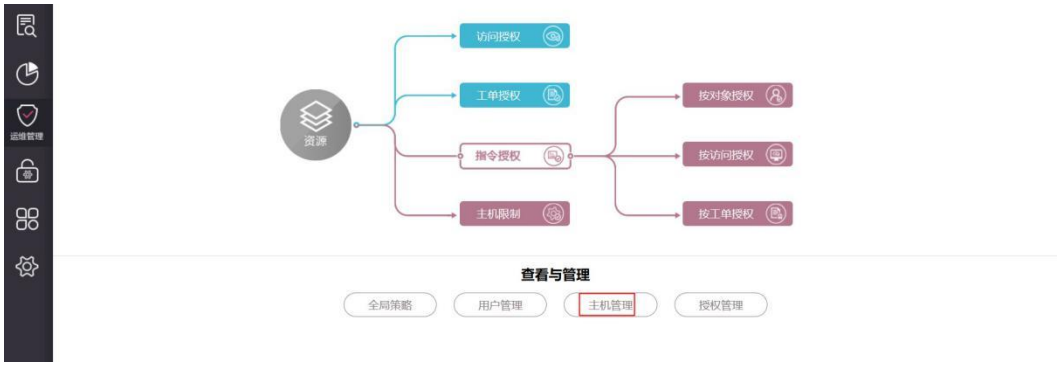


3.2 手工添加主机组并添加主机

操作步骤：

1. 使用系统管理员*#admin#*登录思福迪运维安全管理系统。

2. 点击左侧的“运维管理”选项，在右侧的“查看与管理”页面中单击“主机管理”如下图所示：



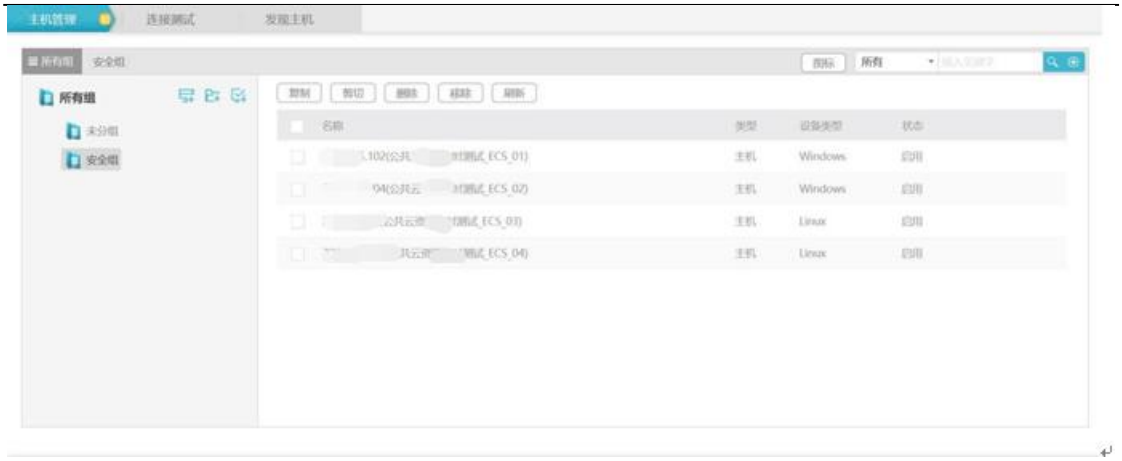
3. 在弹出的“主机管理”页面中，点击“所有组”右侧的“创建主机组”按钮，在弹出的创建主机组页面中输入组名称，组的描述，点击保存按钮，如下图所示：

4. 在主机管理中点击创建的“主机组名称”，选择右上角的“创建主机”选项，在弹出的创建主机页面，填写基本信息（比如主机IP，主机名称，设备类型，设备描述，访问速度，是否是唯一登陆等）；添加服务类型（如RDP, SSH）；添加主机账号（如果需要托管密码可以在这里添加要管理主机的系统管理员账号和密码）具体如下图所示：

上图为添加服务界面，windows主机一般选择RDP，linux主机一般选择SSH，如果要添加SFTP协议，在协议中选择SFTP即可。

上图要勾选“服务”选项【如果在添加协议时同时添加了双协议，这里的可以同时选中两个协议，后面勾选同一账号即可】后，设置管理员账号和密码，如果选择空密码则运维人员在运维时需要手工输入密码，建议托管系统管理员的密码。

5. 主机添加成功后，【可按步骤1-4的方式，添加其它用户信息】，具体如下图所示：



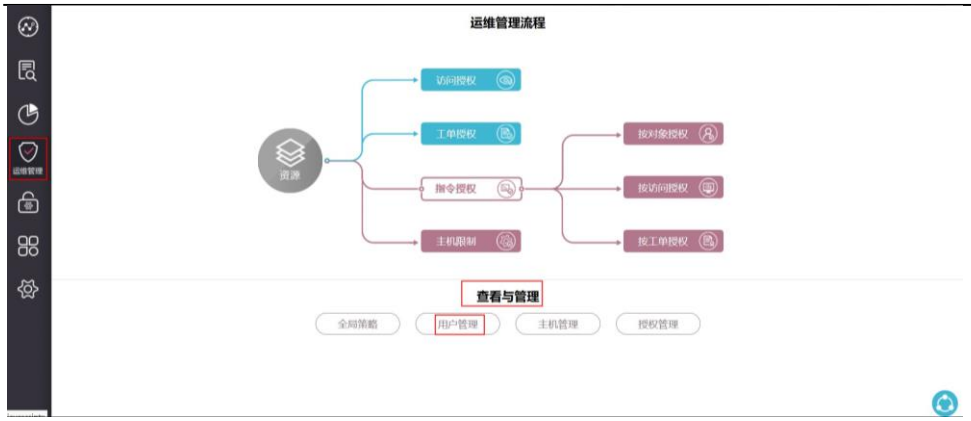
6. **主机修改说明：**可以对添加的主机进行：复制、剪切、粘贴、删除、移除等操作。

- **复制：**可从A主机组中选中一个主机，在B组中粘贴，从而实现A主机同时属于A主机组和B主机组（也可以通过编辑用户属性-在主机组中勾选多个主机组实现）；
- **剪切：**可从A主机组中选中一个主机，剪切到B主机组中去粘贴，从而实现将这台属于A主机组的主机移动到B主机组中去。
- **粘贴：**将复制或剪切的主机，复制或移动到其它指定的主机组中。
- **删除：**将选中的主机删除，左侧所有主机组中将不存在该主机。
- **移除：**将选中的主机从当前主机组中移除，其它主机组若还有该主机则不会被移除。

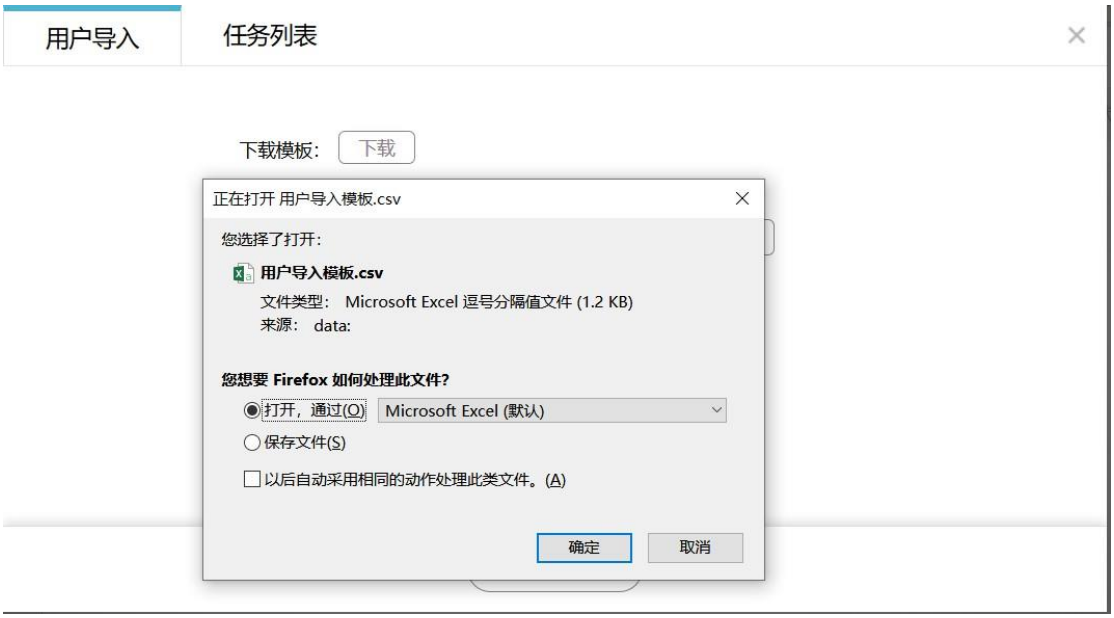
3.3 自动导入用户组和用户

操作步骤：

1. 使用系统管理员*#admin#*登录思福迪运维安全管理系统。
2. 点击左侧的“运维管理”选项，在右侧的“查看与管理”页面中单击“用户管理”如下图所示：



3. 在用户管理页面，单击“导入”按钮，在弹出的“用户导入”对话框里点击“下载模板”后面的“下载”按钮，将用户列表模板下载至本地。如下图所示：



*用户组名称	*组路径	描述	*管理员	用户											
test	/test	test	admin	test											
find	/find	find	admin	find											
*用户账号	*用户姓名	认证方式	*密码	工号	手机	描述	邮箱	部门	*角色	*管理员	第三方认证	唯一登录	失效时间	用户组	是否启用
test	test		12345678			test		test	运维用户	admin		否		/test	是
find	find		12345678			find		find	运维用户	admin		否		/find	是

4. 根据模板规范要求，制作用户资产文件（导入的模板文件支持.csv、.xls两种格式【建议用户使用CSV格式】）。如下图所示：

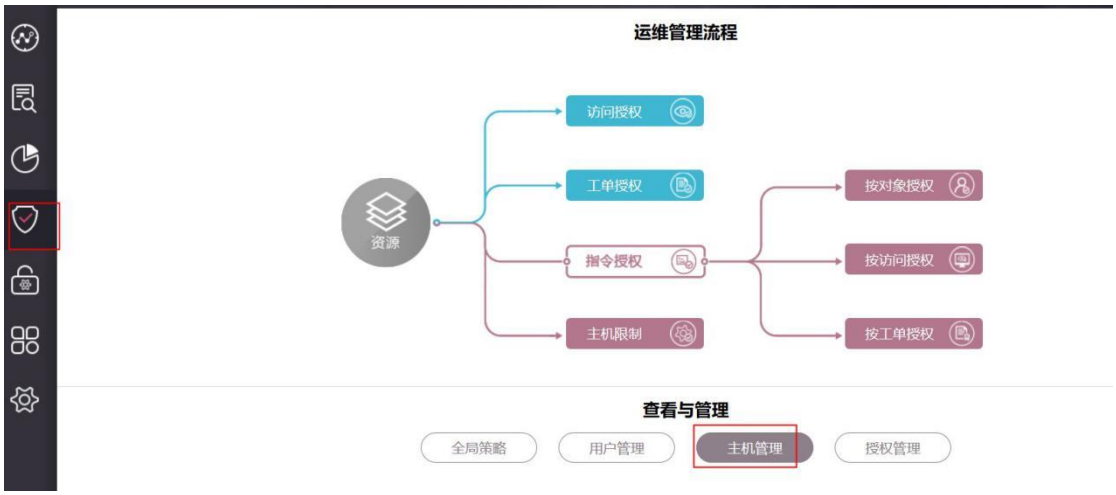
5. 在用户管理页面，选择“所有组” 

，然后选择导入，点击浏览选择本地制作好的用户资产文件，勾选是否覆盖相同账号的用户。单击确认按钮，等待用户导入完成，系统提示本次成功导入用户数量，同时可以在用户管理中查看导入成功的组和用户信息，如下图所示：

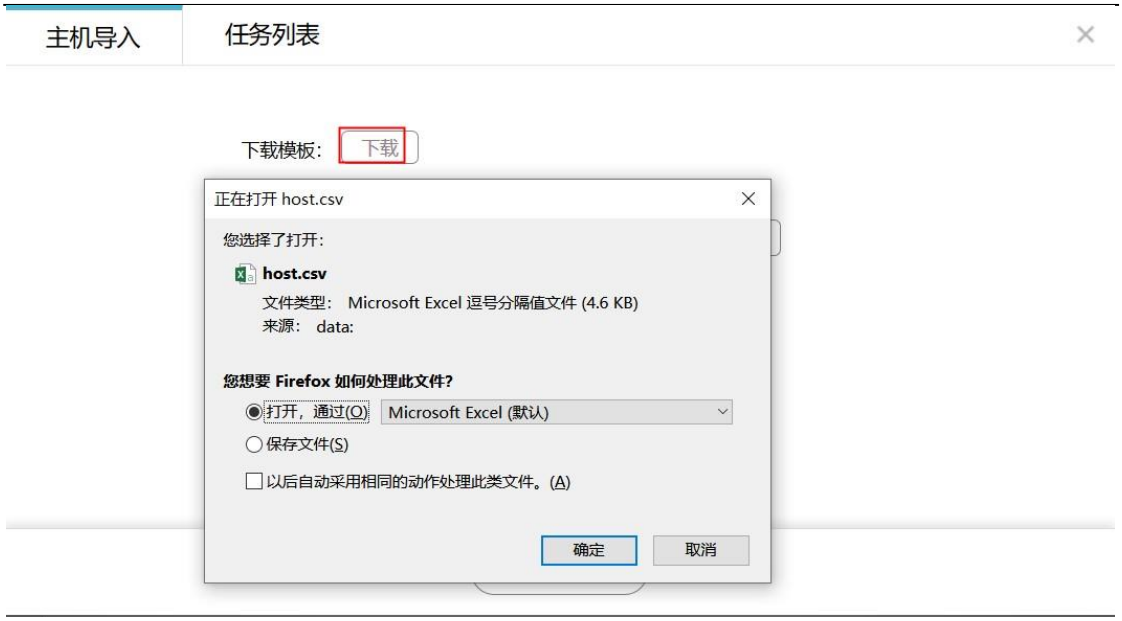
3.4 自动导入主机资产和主机组

操作步骤：

1. 使用系统管理员#admin#登录思福迪运维安全管理系统。
2. 点击左侧的“运维管理”选项，在右侧的“查看与管理”页面中单击“主机管理”如下图所示：



3. 在主机管理页面，单击“导入”按钮，在弹出的“主机导入”对话框里点击“下载模板”后面的“下载”按钮，将主机列表模板下载至本地。如下图所示：



4. 根据模板规范要求，制作主机资产文件（导入的模板文件支持.csv、.xls两种格式【建议用户使用CSV格式】）。如下图所示：

*协议名称	*端口	描述																			
RDP	3389																				
SSH	22																				
*AD域名称	*服务器IP（多个IP用,分隔）																				
*密钥名称	*类型	密码	*内容																		
*设备类型	*类型	账号切换	切换密码	描述	*服务名称	*协议.端口	是否隐藏														
Windows	Windows				RDP	RDP:3389	否														
Linux	Linux	su	Password:		SSH	SSH:22	否														
*主机组/未分组	描述	主机																			
/test	test组资源	220.4.65.1	220.4.68.188																		
*主机IP	*主机名	*设备类型	描述	访问速度	唯一登录	主机组	*协议.端口	连接参数	应用发布	跳转来源	跳转来源	跳转来源	跳转命令	命令提示	账号切换	切换密码	登录密码	登录名提	登陆成功	换行符	*账号	AD域	密
220.4.65.1	测试_ECS	Windows		正常	否	/test,	RDP:3389,	RDP:3389"",												LF,	administrator		
220.4.68.1	测试_ECS	Linux		正常	否	/test,	SSH:22,	SSH:22"",							su,	Password:,				LF,	root		

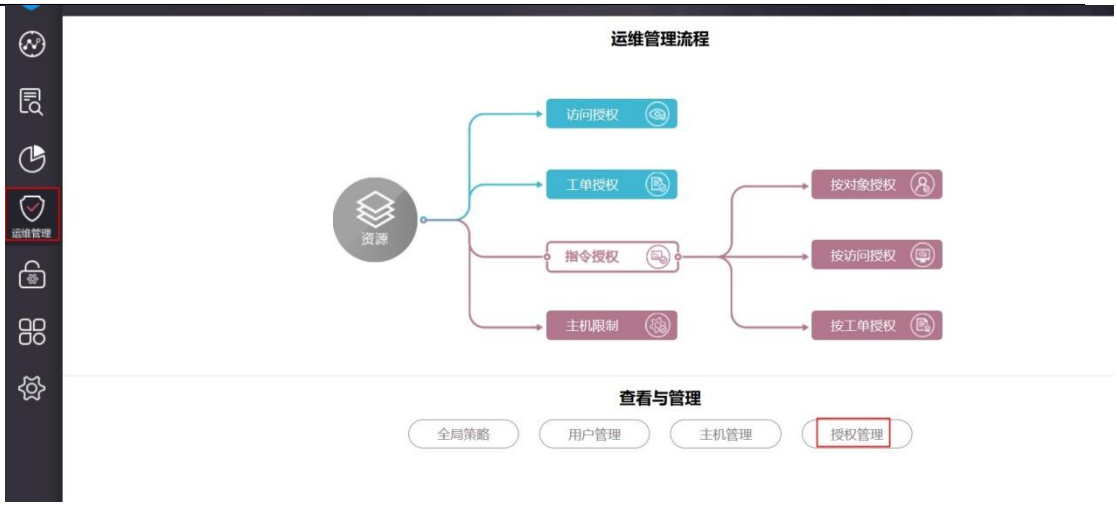
5. 在主机管理页面，选择“所有组”，然后选择导入，点击浏览选择本地制作好的主机资产文件，勾选是否覆盖相同IP的主机。单击确认按钮，等待主机导入完成，系统提示本次成功导入主机数量，同时可以在主机管理中查看导入成功的组和主机信息，如下图所示：

3.5 添加管理授权策略

操作步骤：

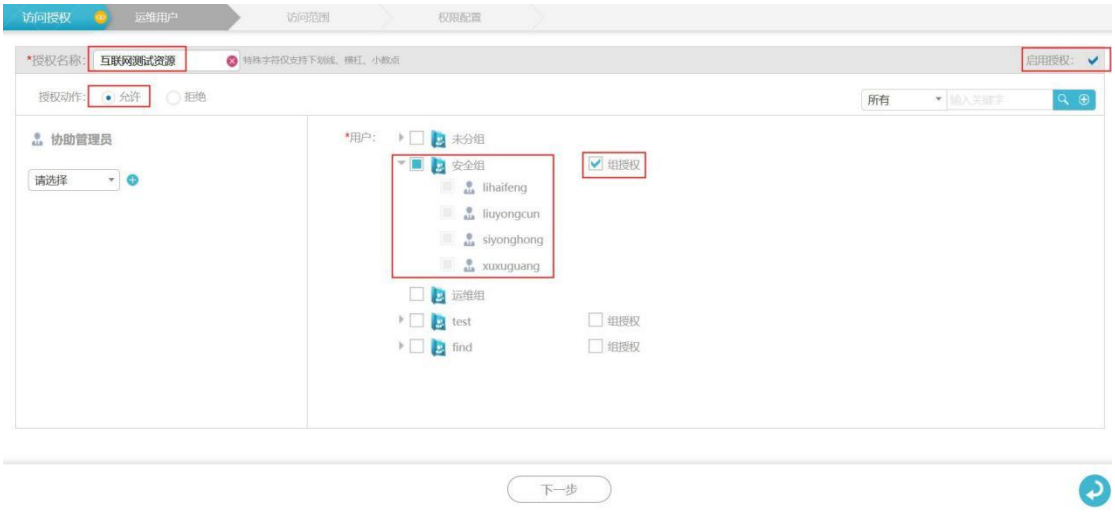
1. 使用系统管理员#admin#账号登录思福迪运维安全管理系统。

2. 定位到“运维管理”选项，在右侧的“查看与管理”页面中单击“授权管理”，**如下图所示：**



3. 在授权管理页面，点击创建按钮，如下图所示：

4. 在“访问授权”页面的“运维用户”配置中输入授权名称-选择授权动作-选择授权的用户名-勾选组授权【组授权适用于批量授权，若没有勾选该选项，后续添加到该组的用户需要管理员单独授权】，点击下一步按钮，如下图所示：



5. 在“访问授权”页面的“访问范围”配置中-选择授权的主机组或主机-勾选组

授权【组授权适用于批量授权，若没有勾选该选项，后续添加到该组的主机资产需要管理员单独授权】，点击下一步按钮，如下图所示：

6. 在“访问授权”页面的“权限配置”中-配置要授权的操作，如剪切板、磁盘、上传、下载等操作，同时也可以设置相应的策略生效时间、客户端运维地址限制等配置，如下图所示：

7. 点击保存即完成授权策略的配置，如下图所示：

注意：用户可根据实际的需求进行分级授权管理配置，在使用分级授权管理时，建议步骤4-5中不要勾选组授权。

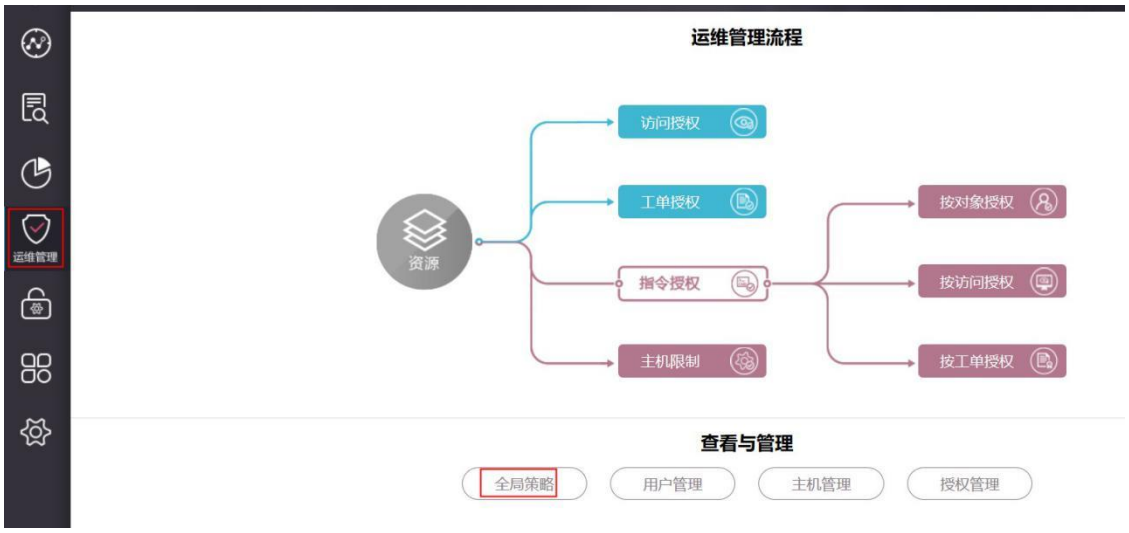
4. 高级功能配置

4.1 全局策略配置

操作步骤：

1. 使用系统管理员#admin#账号登录思福迪运维安全管理系统。

2. **定位到**“运维管理”选项，在右侧的“查看与管理”页面中单击“全局策略”，**如下图所示：**



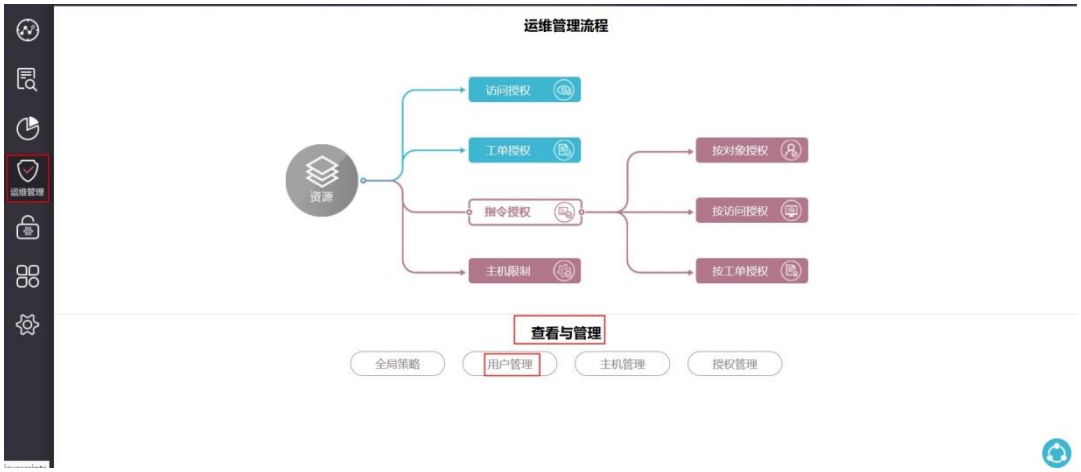
3. 在全局策略配置页面，可以配置安全策略及运维策略，配置完成后，点击保存按钮即可，具体如下图所示：

4.2 多因子认证配置

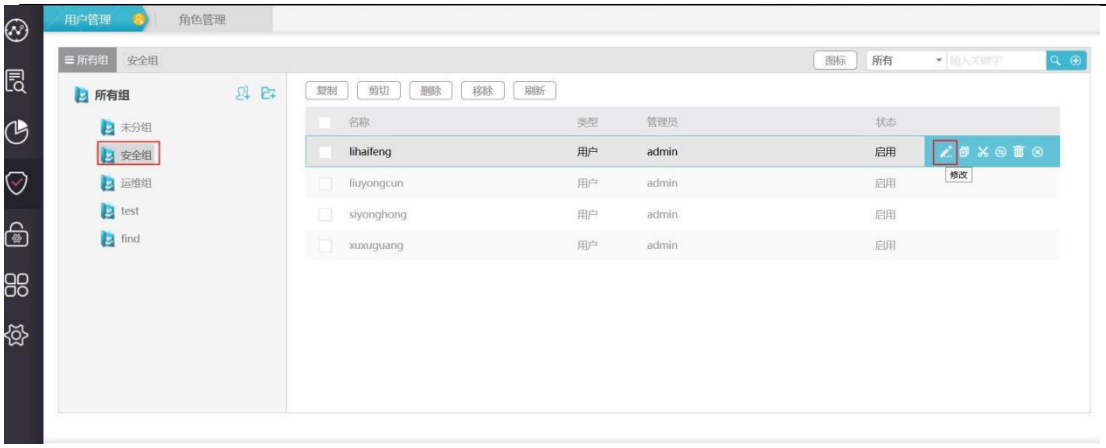
操作步骤：

1. 使用系统管理员*#admin#*登录思福迪运维安全管理系统。

2. 点击左侧的“运维管理”选项，在右侧的“查看与管理”页面中单击“用户管理”如下图所示：



3. 在所有组中选择组-选择右侧用户的修改选项，如下图所示：



4. 在编辑用户界面中，将认证方式修改为“需要的认证方式”，点击保存即可，如下图所示：

使用TOTP认证之后，需要点击下面的“重置TOTP”按钮，然后使用谷歌认证器扫描二维码进行绑定和验证，如下图所示：

说明：这里如果管理设置为本地认证+TOTP认证选项，运维用户在使用本地密码+TOTP（谷歌认证器）登陆堡垒机时，密码格式为：用户密码+TOTP的动态验证码【先输用户密码然后紧接着输入谷歌认证器生成的动态码即可】。

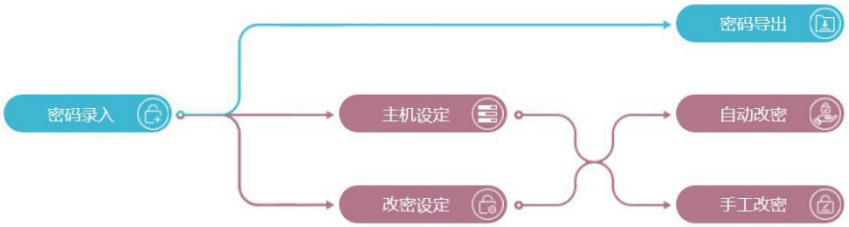
4.3 批量修改密码配置

思福迪运维安全管理系统的密码管理功能，支持单个手动、自动批量修改主机账号的密码，管理员也可以根据系统设置的任务计划实现密码的批量修改计划。同时批量修改密码任务对运维用户无感知。

要使用批量修改密码配置，需要准备如下环境：

- **邮件服务器或FTP服务器：**用于接收和发送密码配置；
- **管理员邮件地址配置：**配置admin的邮箱地址；
- **改密设定配置：**配置接收者及管理员密码；密码管理的使用流程，如下图所示：

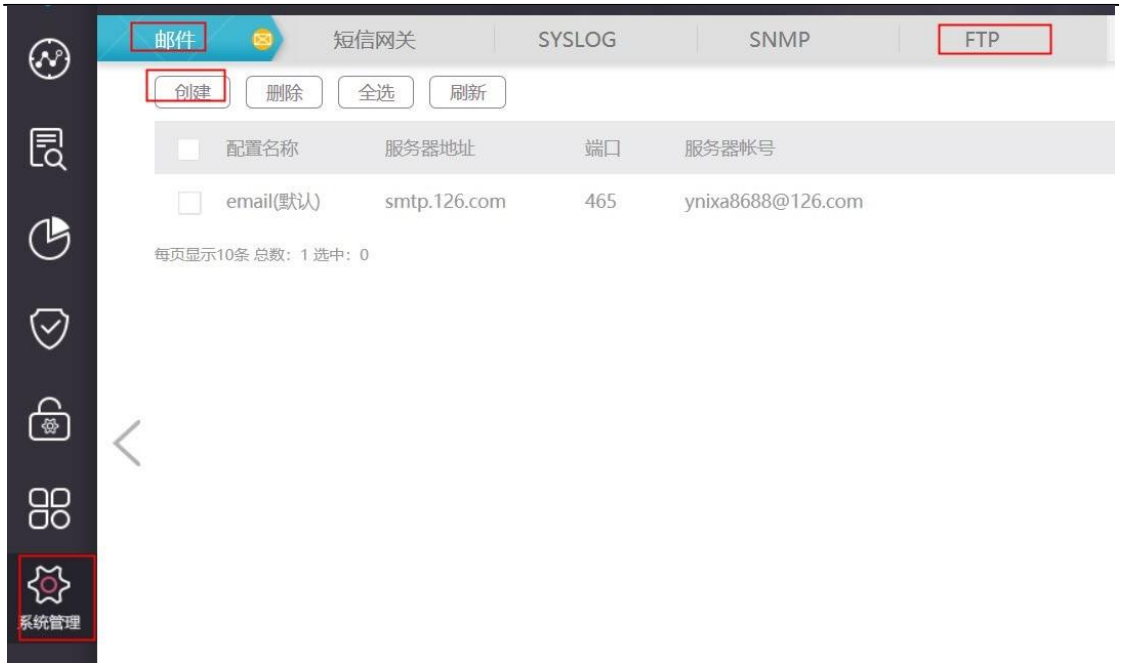
密码管理流程



- **密码录入**:可录入主机账号密码/密钥;
- **密码导入**:可将主机账号的密码下载或发送给指定管理员;
- **密码导出**：可将主机账号的密码导出【下载后的密码通过“密码查看工具”-输入**改密设定中的密码+管理员密码**查看】;
- **主机设定**:可设定运维主机的改密方式;
- **改密码设定**:可配置改密策略与发送方式;
- **自动改密**:可配置自动改密计划;
- **手工改密**:可选择主机账号进行手工改密;
- **全局策略**:可配置审批规则;
- **历史清单**:可查看改密的历史清单。

操作步骤：

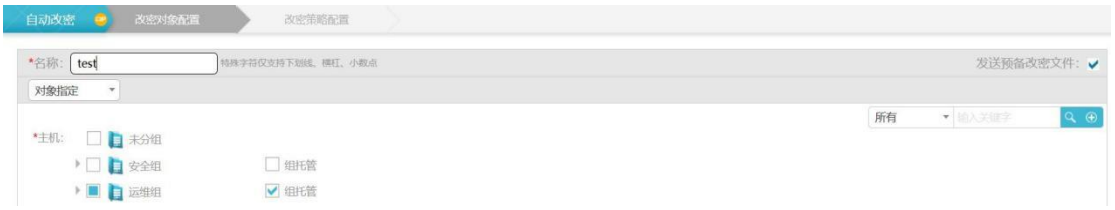
1. 设备邮件服务器或FTP的配置，点击“系统管理”-“输出配置”-邮件或FTP选项—创建邮件或FTP接收者，如下图【这里以邮件服务器为例】所示：



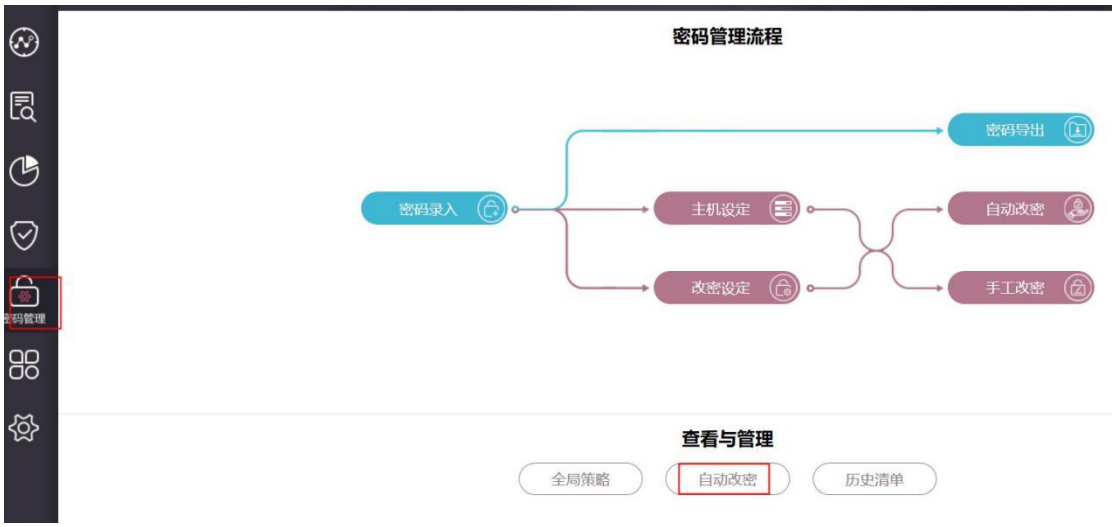
2. 设置管理员账号的邮箱地址，点击右上角的管理员admin账号头像，进入配置页面，如下图所示：

3. 点击密码管理流程中的”改密码设定”，配置改密码设置的接收人，如下图所示：

4. 选择密码流程中的自动改密，在自动改密设置中设置名称-选择需要修改密码的主机-选择改密的主机账号-配置改密码策略等，具体如下图所示：

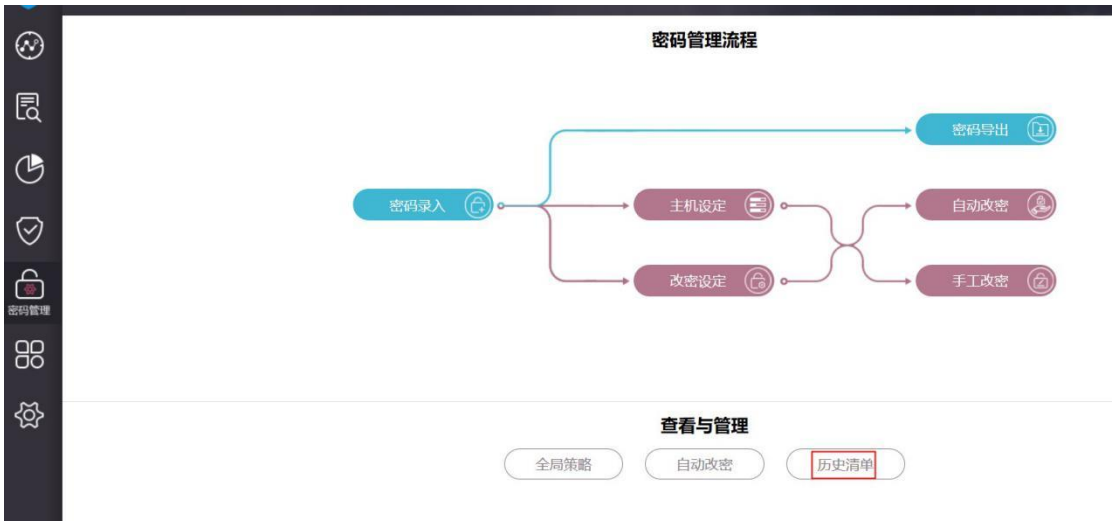


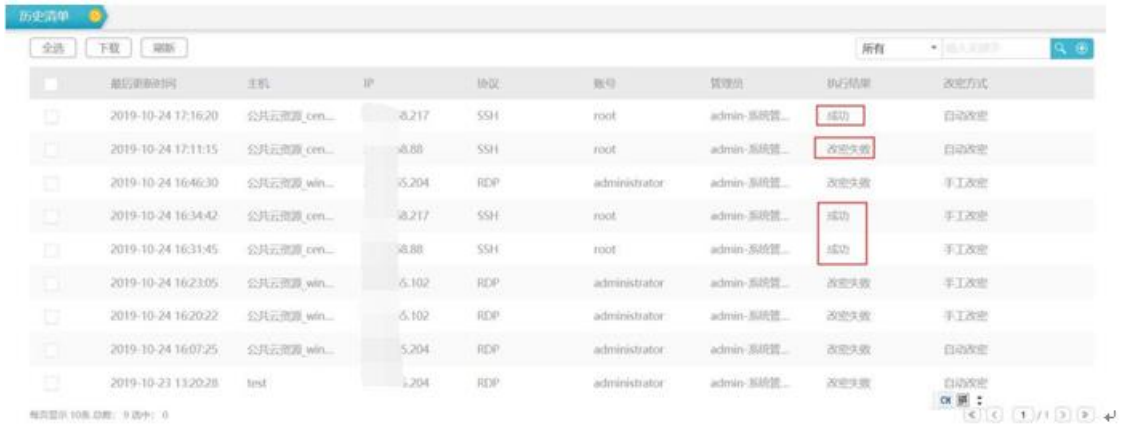
5. 配置完自动改密策略后，系统会根据配置的自动改密策略执行对主机的密码修改操作，可以在“密码管理”-“查看与管理”-“自动改密”中查看任务的执行状态，如下图所示：



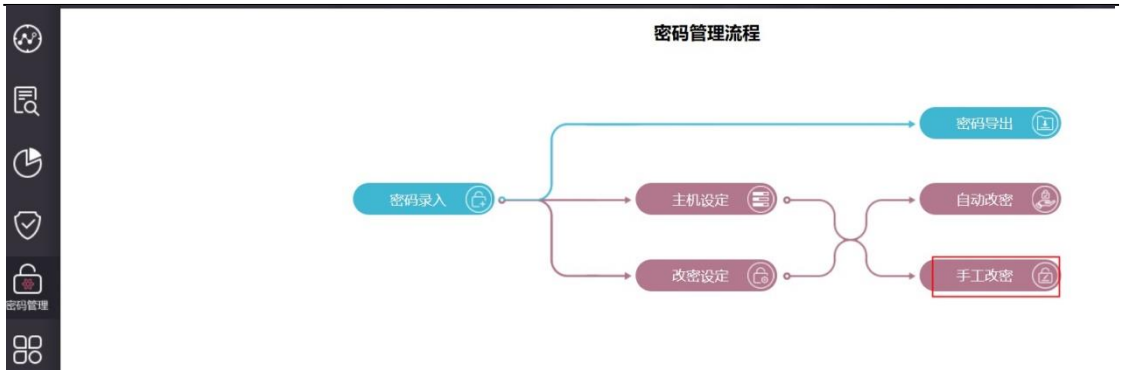
6. 可在右上角的消息  中对改密任务的接收和发送，进行确认，如下图所示：

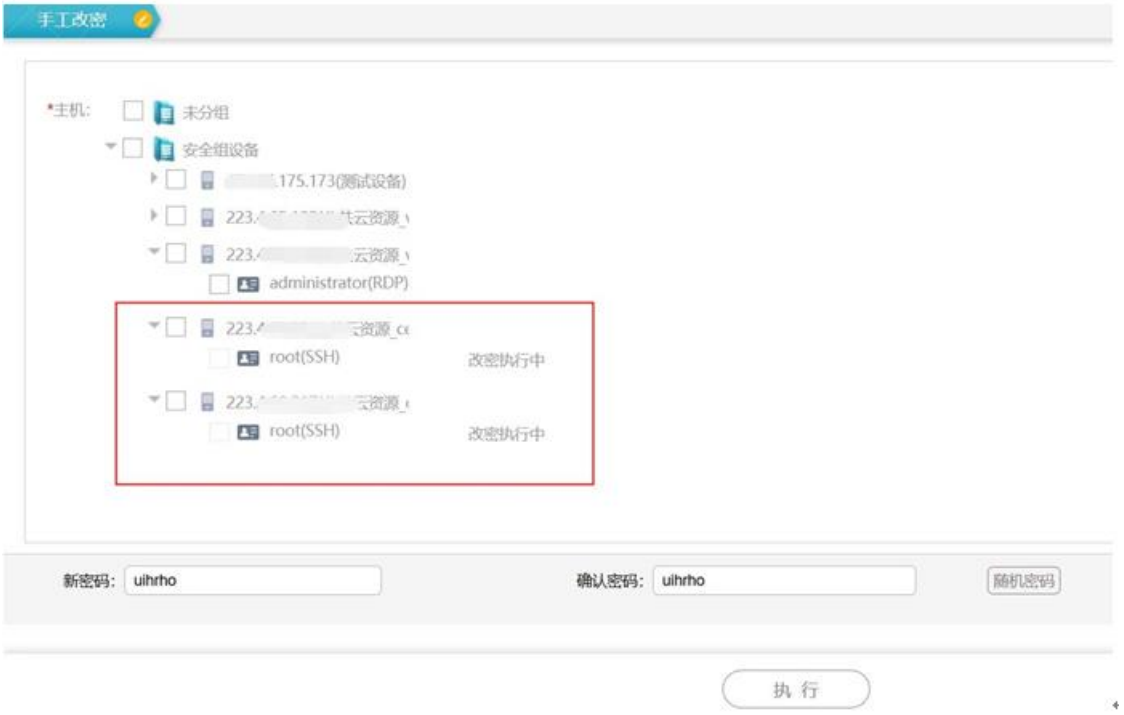
7. 可以在“密码管理”-“查看与管理”-“历史清单”中查看任务历史执行的情况，如下图所示：





8. 管理员也可以通过“密码管理”-“手工改密”批量修改主机的密码，如下图所示：





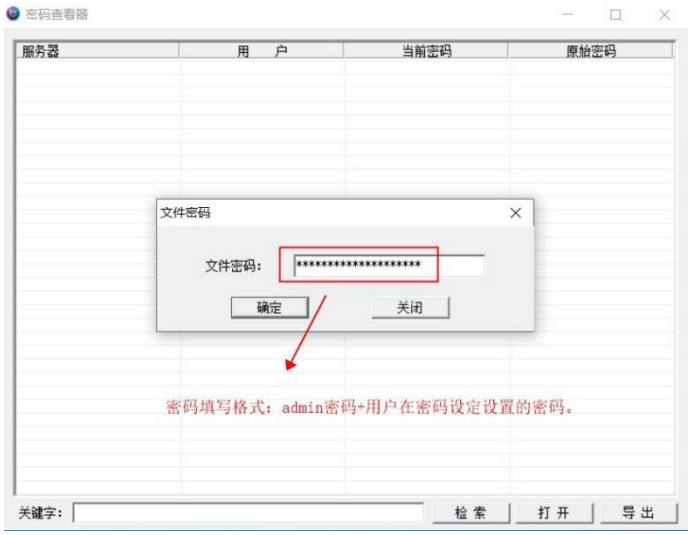
9. 可以在“密码管理”-“查看与管理”-“历史清单”中查看手工改密的执行情况，如下图所示：

说明：管理员可以根据实际情况，结合密码策略进行自动批量修改ecs主机的管理员密码。密码自动修改，堡垒机会自动进行托管，运维用户使用中没有任何影响。

密码查看说明：

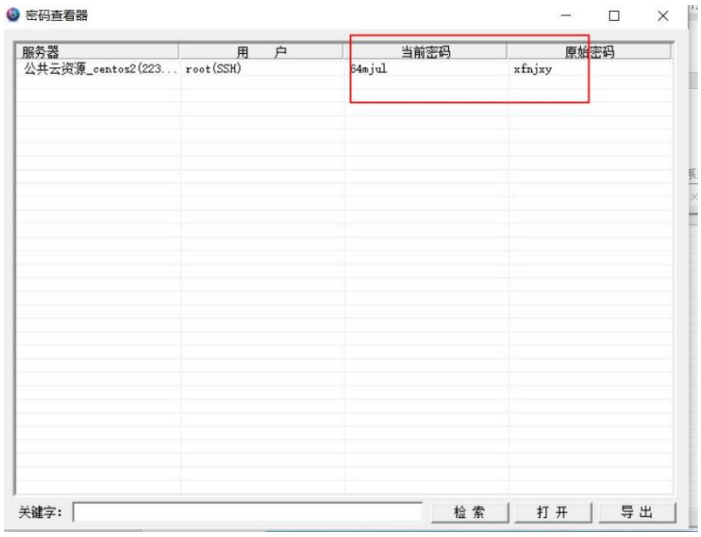
管理员可以在设置的邮箱中，查看自动批量修改的密码配置。如下图所示：

将邮件中的密码文件下载，然后使用“系统管理”-“软件管理“-”密码查看器“软件打开进行查看，如下图所示：



上图中的密码格式：使用admin的密码+用户在“改密设定“中设置的密码，才能查看实际的密码文件【这在前面的参数说明中有提到】。

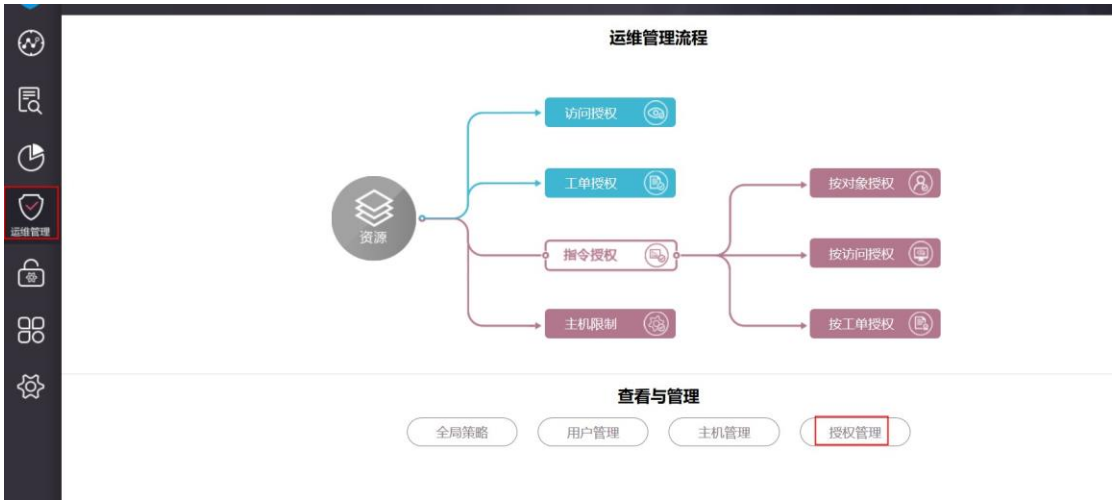
【**强烈建议**：用户在”密码管理“-改密设定”中的密码不要设置成一样的。】



4.4 分权管理配置

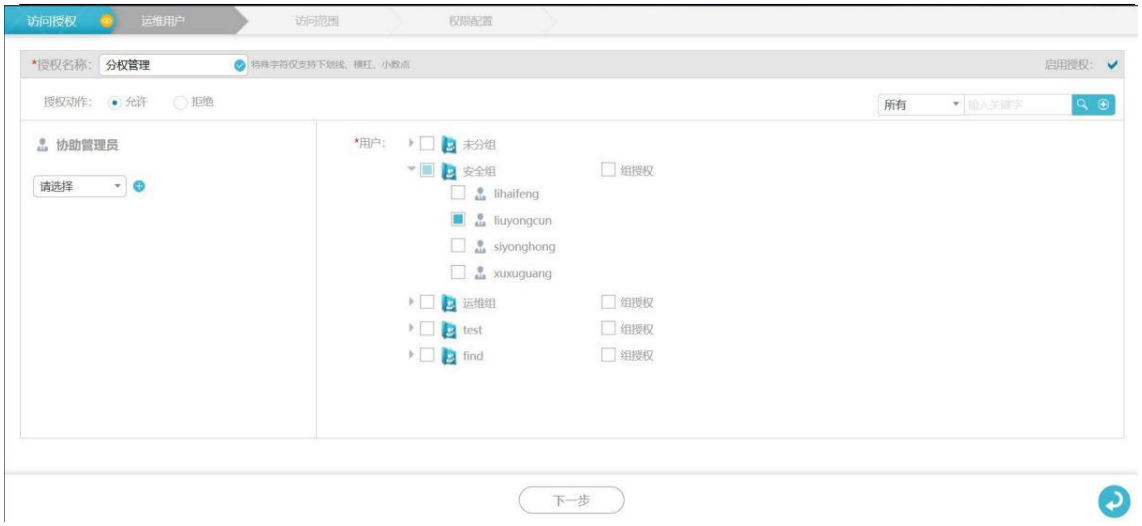
操作步骤：

1. 使用系统管理员#admin#账号登录思福迪运维安全管理系统。
2. **定位到**“运维管理”选项，在右侧的“查看与管理”页面中单击“授权管理”，**如下图所示：**



3. 在授权管理页面，点击创建按钮，如下图所示:

4. 在创建“访问授权”的选项中选择，用户、授权的主机、使用权限等，保存即可，如下图所示：



5. 分权管理配置适用于多级厅局单位的场景，比如A包含B，C是B厅局的用户，C只需要授权访问B厅局的资源控制。管理员可根据实际需求灵活定义访问控制的策略，实现分权管理。

5. 日志审计

5.1 实时监控

操作方法：

1. 使用审计管理员#audit#账号【管理员自定义的名字】登录思福迪运维安全管理系统【该用户用管理员定义，并授权给相应的操作人员】。

2. 在实时监控页面能够显示堡垒机的授权信息、运行状态和运维统计数据等，如下图所示：

参数说明：

「|证书」展示堡垒机授权信息；

客户名称：显示为采购/测试用户单位名称；

托管上限：最多可以添加的主机数量；

设备型号：堡垒机的产品型号；

设备类型：显示为供货设备/服务设备

授权起始：堡垒机授权起始时间；

服务期限：即授权起始时间起所提供的维保期限，服务设备状态下为测试/服务使用期限。

「|系统概要」展示堡垒机运行状态信息；

日志：可点击 

进入查看系统日志，系统日志包含了系统运行、系统配置、用户登录、用户配置、用户检索等日志，双击可查看详细的日志信息，具体如下图所示：

「|告警」展示及处理系统告警日志，点击“更多”按钮，可查看详细的数据，如下图所示：

「|时间趋势」展示每小时/天产生运维操作/会话量趋势；小时/天：可点击切换显示两周或当日的运维操作/会话量；

全部/异常：可点击切换显示所有运维操作/会话或异常操作/会话；操作/会话：可点击切换显示运维操作/会话量；

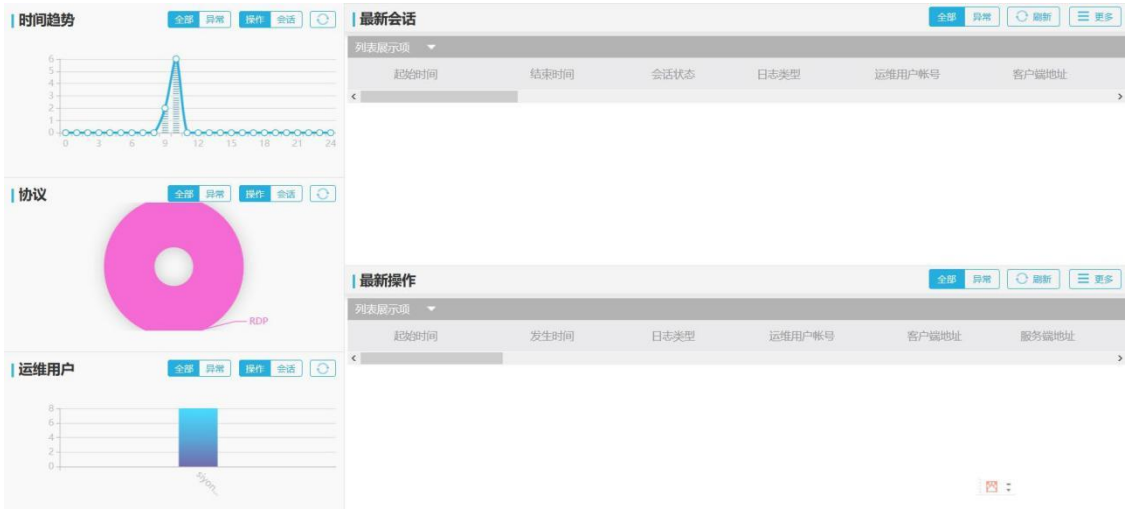
图表展示区：可点击某个时间点查看该时间内运维操作/会话的统计与详细数据，

如图所示：

「服务器」展示运维主机产生的运维操作/会话量统计；

全部/异常：可点击切换显示运维主机产生的运维操作/会话或异常操作/会话；

操作/会话：可点击切换显示运维主机产生的运维操作/会话量；图表展示区：可点击运维主机IP查看该主机运维操作/会话的统计与详细数据，如图所示：

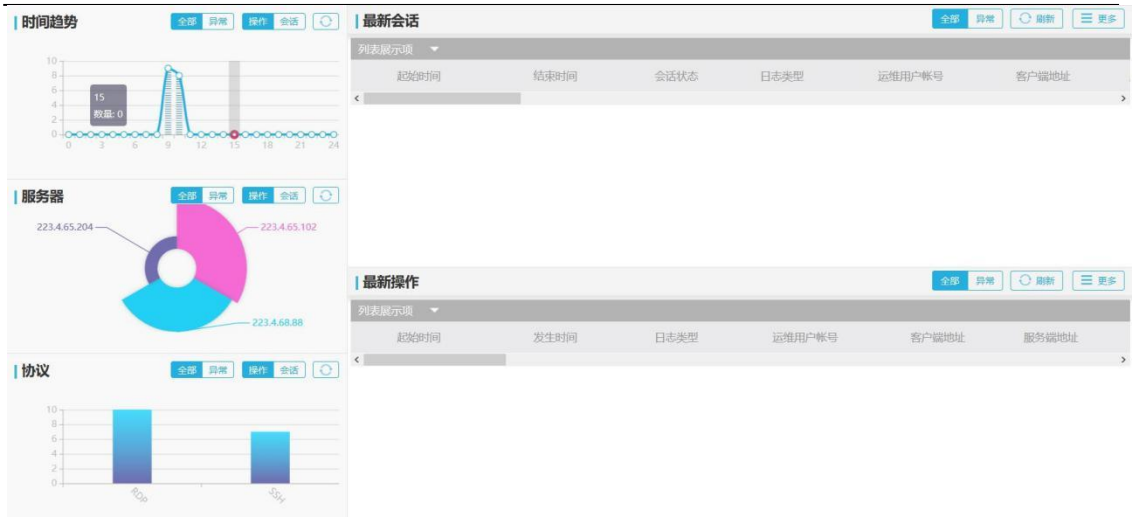


「|运维用户」展示运维用户产生的运维操作/会话量统计；

全部/异常：可点击切换显示运维用户产生的运维操作/会话或异常操作/会话；

操作/会话：可点击切换显示运维用户产生的运维操作/会话量；

图表展示区：可点击运维用户查看该用户运维操作/会话的统计与详细数据，如图所示：



5.2 数据检索

操作方法：

1. 使用审计管理员#audit#账号【管理员自定义的名字】登录思福迪运维安全管理系统【该用户用管理员定义，并授权给相应的操作人员】。
2. 在数据检索页面能够对历史会话/操作及系统日志的内容进行检索，在检索界面,可以添加多个检索条件,如下图所示：

3. 对于检索出来的记录可以进行在线回放、关联分析、下载，下载后的视频回放

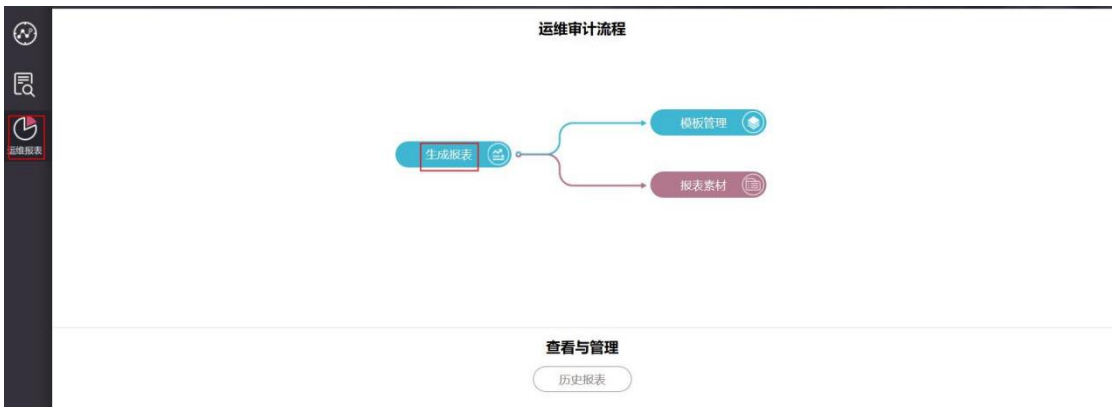
需要安装章节2.4“工具下载”中的BhostReplay软件。

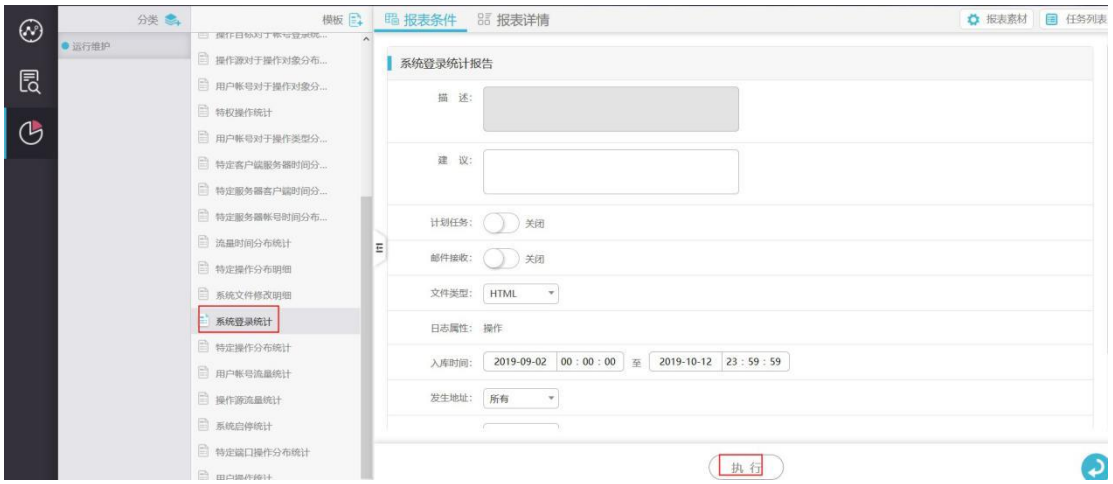
5.3 运维报表

操作方法：

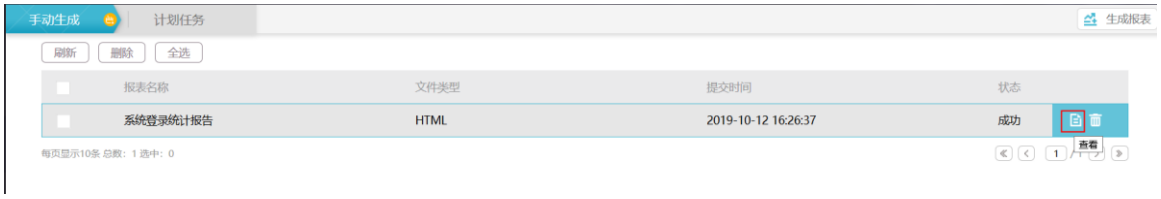
1. 使用审计管理员#audit#账号【管理员自定义的名字】登录思福迪运维安全管理系统【该用户用管理员定义，并授权给相应的操作人员】。

2. 在运维报表页面能根据已配置的报表即时/定期生成报表，如下图所示：





3. 生成指定的报表后，可在运维报表—查看与管理—历史报表中查看生成的报表文件，点击”查看”按钮，即可查看，如下图所示：



6. 最佳实践

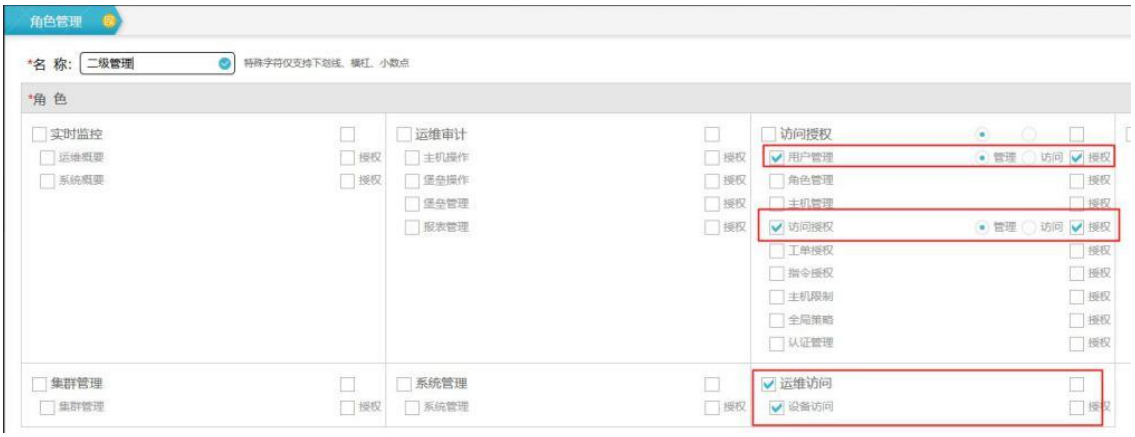
6.1 分级管理用户

适用场景：组织分级管理，允许上级查看和管理下级的运维用户，下级单位只能管理自己的运维用户。【适用多层的组织结构，申请1台堡垒机可能管理多个层次资源】

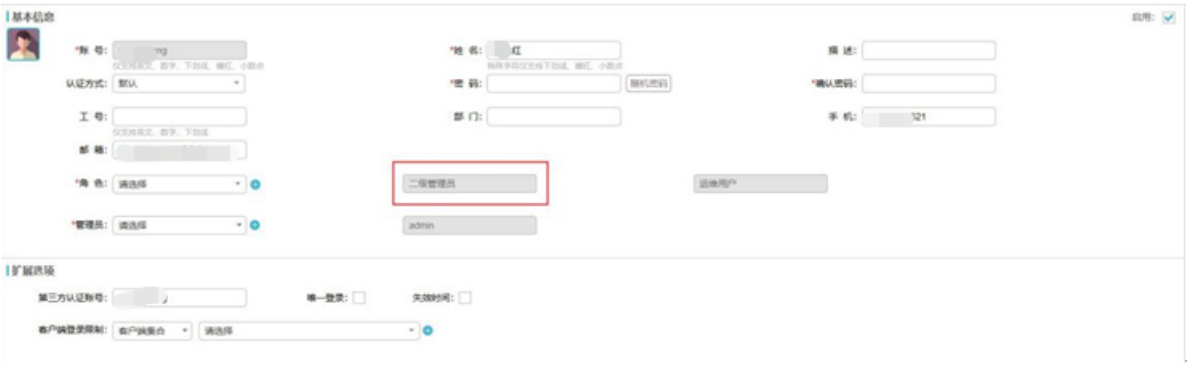
具体的操作步骤如下：

1. 使用admin账号登陆“思福迪运维安全管理系统”，依次点击左侧的“运维管理”-用户管理-选择“所有组”然后新建一个管理组命名为“二级管理员”，如下图所示：

2. 选择“角色管理”-“创建”新建一个二级管理员角色，勾选“访问授权”下面的用户管理、访问授权、运维访问等选项，点击保存按钮。



3. 点击“用户管理”-“二级管理员员”-添加一个用户，然后角色选择二级管理员，点击保存按钮，如下图所示：



4. 然后点击“所有组”-在右侧的窗口中选择要管理的组，选择修改选项，在“管理员处“添加新建的二级管理员用户，点击保存按钮，如下图所示：

5. 我们也可以选择这个组织下的某个用户的管理员为二级管理员的用户，添加之后二级管理员就可以用该组织下的用户进行编辑、删除等操作了。

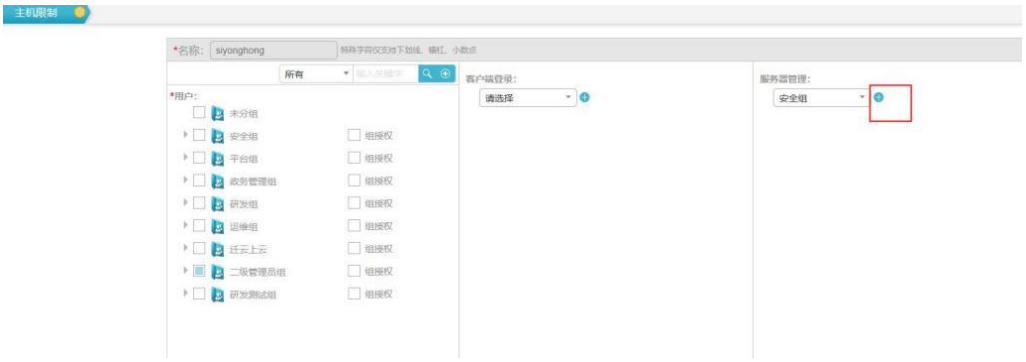
6.2 分级管理主机

适用场景：二级组织分组管理，允许上级组织查看和管理下级组织的主机资源，下级单位只能管理自己的主机资源。

具体的操作步骤如下：

1. 使用admin登陆“思福迪运维安全管理系统”，依次点击“运维管理”-用户管理-角色管理，添加主机管理的角色，勾选内容如下图所示：

2. 然后依次点击“运维管理”-查看与管理下面的“授权管理”-主机限制选项，点击“创建”按钮，创建一个主机限制，名称自己定义，二级管理员可以选择自己创建的二级管理员用户，在服务器管理处点击+号，创建一个主机访问的授权组，勾选该用户可以管理的主机组，如下图所示：



3. 配置完成后，点击保存，然后在创建的主机限制中选择自己新建的主机授权集合，即可完成配置。

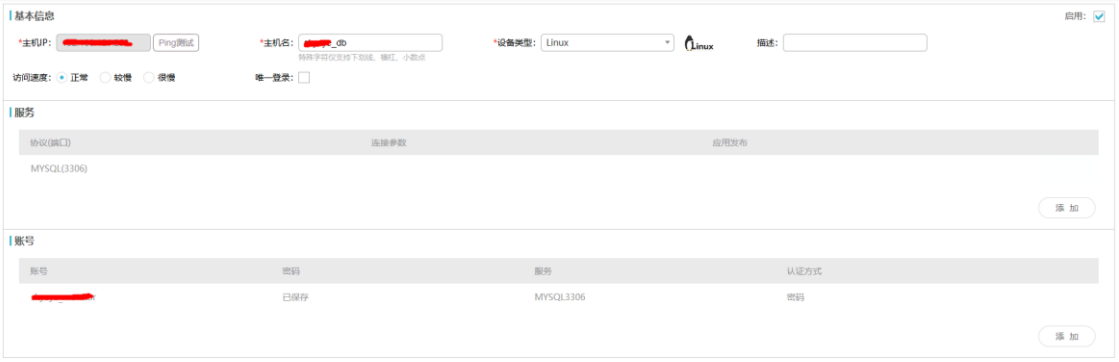
6.3 堡垒机管理Mysql数据库

适用场景：运维人员通过堡垒机使用本地的Navicat软件管理Mysql数据库。

操作步骤：

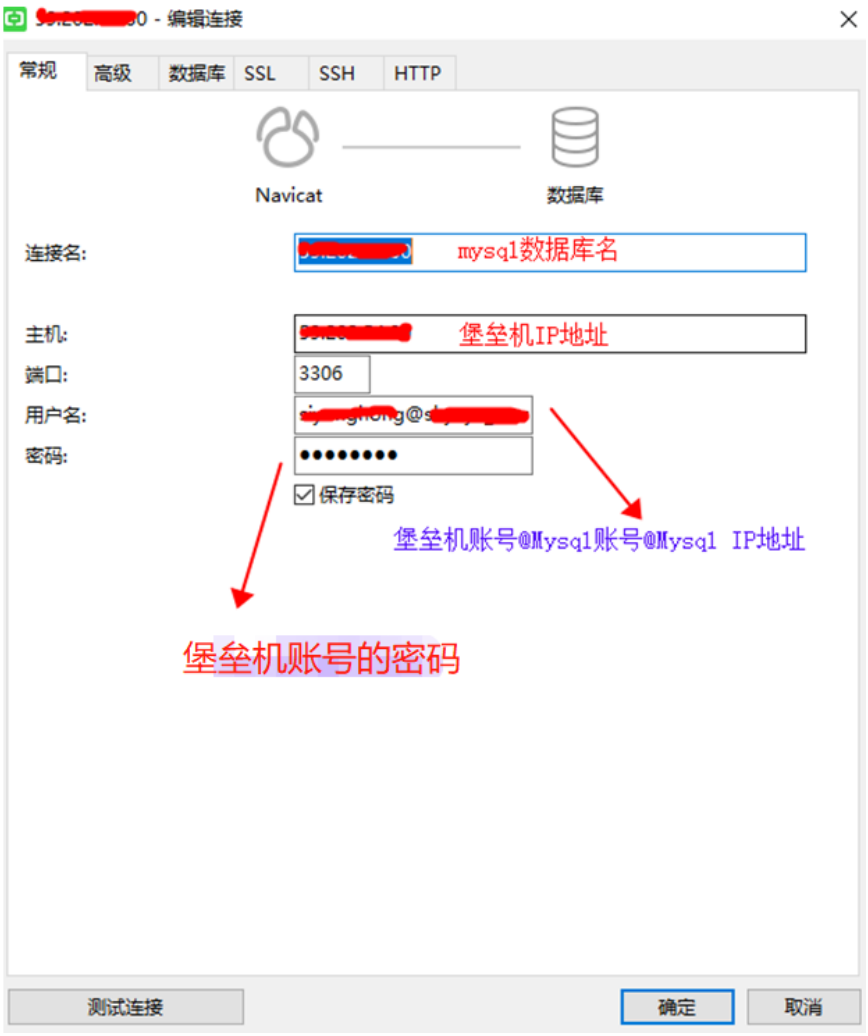
1. 在安全组的配置中，添加堡垒机的入站规则，允许,入方向，TCP3306的安全组规则，如下图所示：

2. 在使用admin账号登陆堡垒机，在主机管理中添加RDSForMysql的主机资产，配置信息（mysql的IP地址、服务里选MYSQL、配置MYSQL的账号【这里一定要在账号中托管Mysql的登陆账号密码，否则可能导致连接失败】），如下图所示：



3. 在控制台中添加堡垒机的IP地址白名单，允许堡垒机访问 Mysql的数据库；

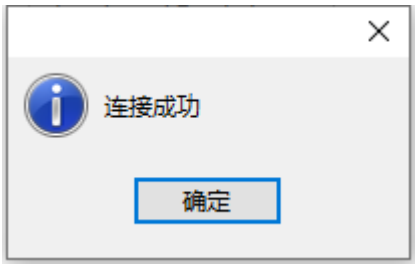
4. 运维端打开Navicat的客户端，配置如下的连接属性（连接名、主机、端口、用户名、密码）如下图所示：



- 连接名：可以填写Mysql数据库的名称，用户自定义；
- 主机：这里填写堡垒机的IP地址；
- 端口：Mysql数据库的默认端口为3306；

- 用户名：这里填写格式堡垒机运维账号@Mysql数据库用户名@Mysql数据库IP地址,比如运维账号为zhangsan，数据库用户名为root，数据库Ip地址为192.168.1.100，这里填写的格式为shangsan@root@192.168.1.100
- 密码：这里填写的密码为堡垒机账号的密码。

5. 配置完成后，点击测试连接，会提示连接成功的信息，如下图所示：



6. 配置完成后运维用户就可以直接使用本地的Navicat软件来管理 Mysql数据库了。

6.4 堡垒机管理SQLServer数据库

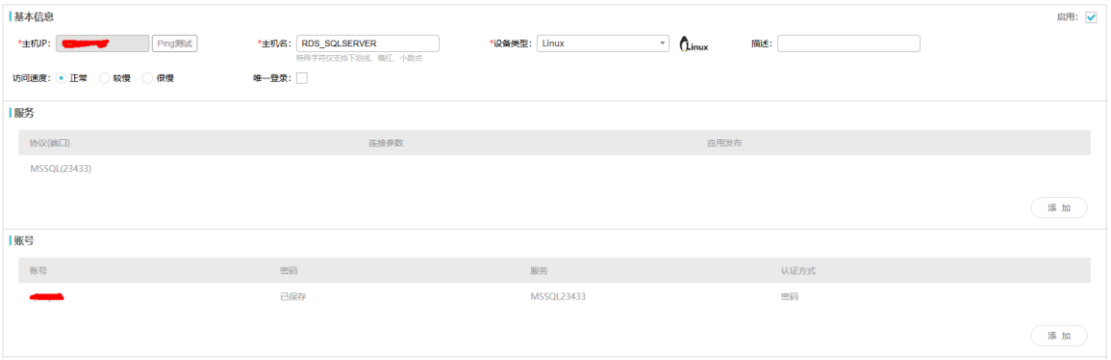
适用场景：运维人员通过堡垒机使用本地的Navicat软件管理SQLServer数据库。

操作步骤：

1. 在安全组的配置中，添加堡垒机的入站规则，允许,入方向，TCP23433【假设这里的SQLServer数据库端口是23433,用户根据实际 的 sql数据库端口进行配置】的安全组规则，如下图所示：

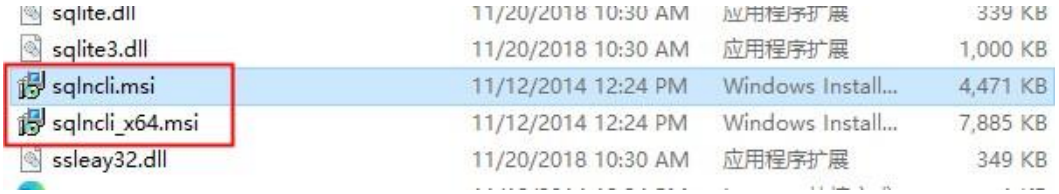
2. 使用admin账号登陆堡垒机，依次点击左侧的“系统管理”-“模块设置”-将MSSQL2008的服务端口改为数据库的端口号，这里的数据库端口号为23433【如果不是这个端口的，根据实际的sql数据库端口填写】，如下图所示：

3. 然后，点击左侧的“运维管理“-在查看与管理下面点击”主机管理“，在主机管理中添加RDSForSQLServer的主机资产，配置信息（RDS的IP地址、服务里选MSSQL、配置MSSQL的账号【这里一定要在账号中托管Mssql的登陆账号密码，否则可能导致连接失败】），如下图所示：

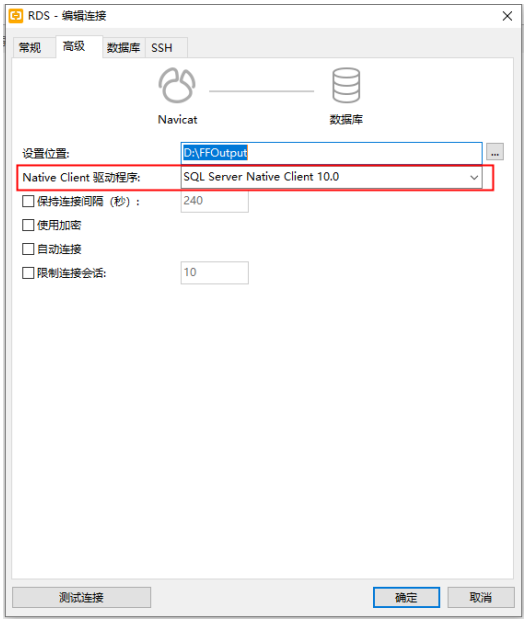


4. 在控制台中添加堡垒机的IP地址白名单，允许堡垒机访问Mssql的数据库；

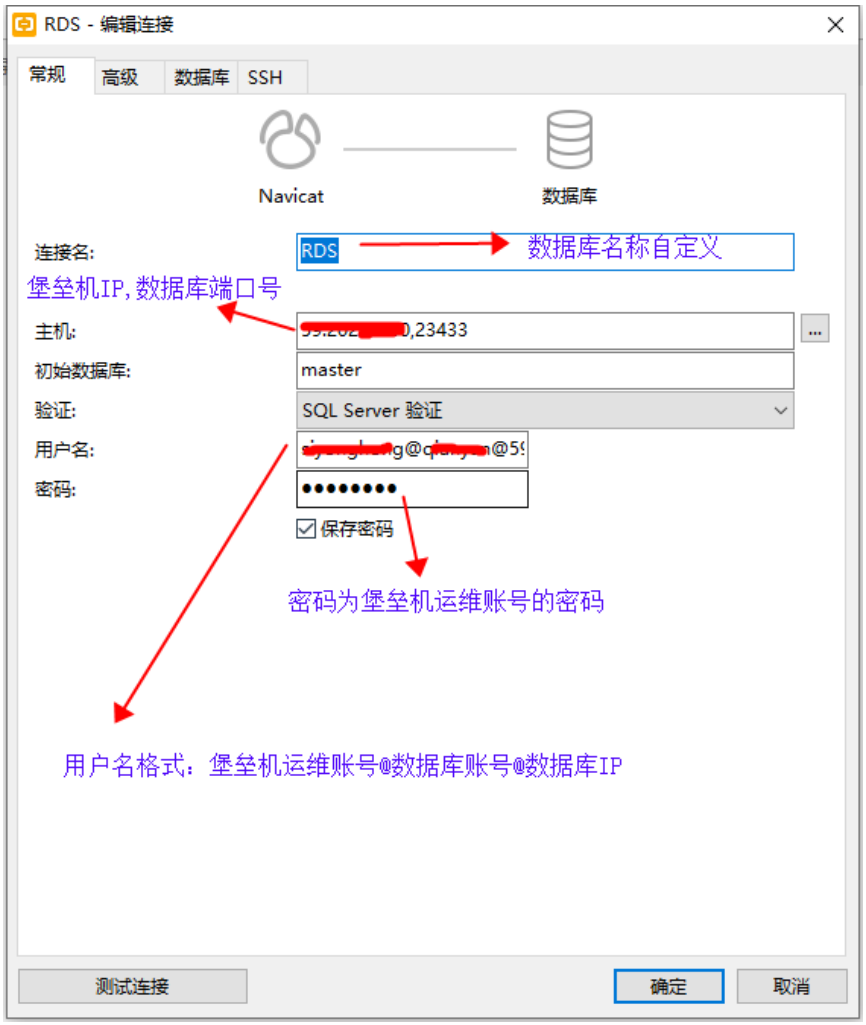
5. 如果您已经安装了Navicat客户端管理工具，需要提前安装C:\ProgramFiles\PremiumSoft\NavicatPremium12目录下的两个文件：sqlncli.msi、sqlncli_x64.msi，如下图所示：



6. 打开Navicat客户端，点击连接“选择SQLServer”，在新建连接中点击高级，配置“设置位置”、“NativeClient驱动程序”，如下图所示：

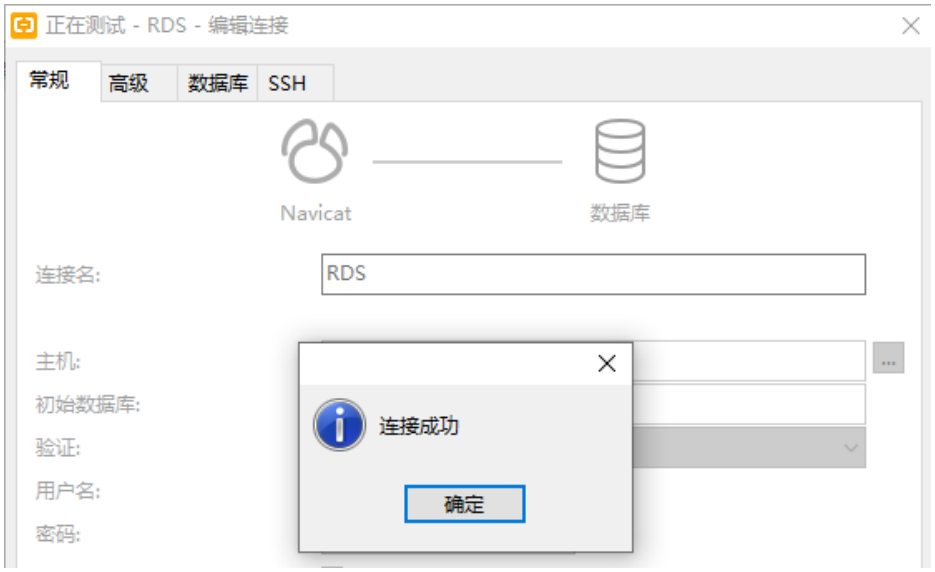


7. 在“常规“选项卡中，配置如下的连接属性（连接名、主机、端口、用户名、密码）如下图所示：



- 连接名：可以填写SQLServer数据库的名称，用户自定义；
- 主机：这里填写堡垒机的IP地址，数据库端口号：
- 初始数据库：默认master即可；
- 用户名：这里填写格式堡垒机运维账号@SQLServer数据库用户名@SQLServer数据库IP地址,比如运维账号为zhangsan，数据库用户名为sa，数据库Ip地址为192.168.1.100，这里填写的格式为shangsan@sa@192.168.1.100
- 密码：这里填写的密码堡垒机运维账号的密码。

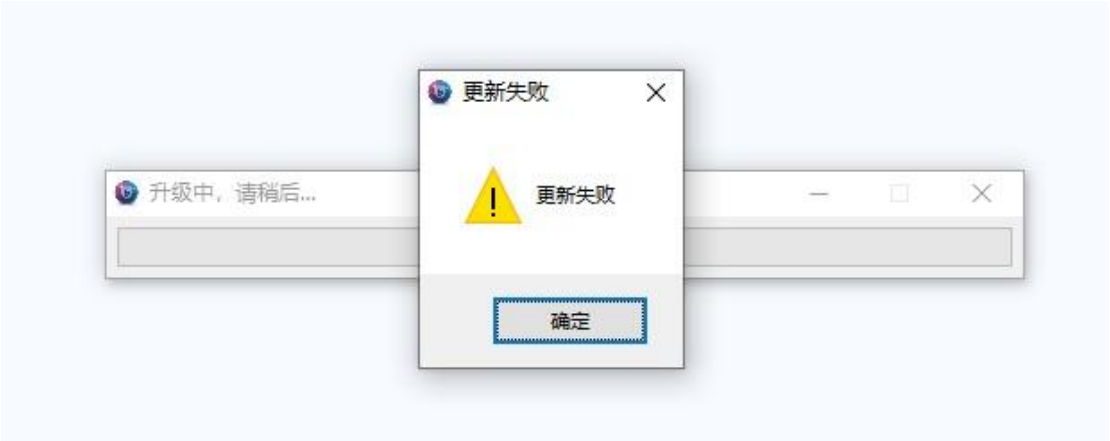
8. 配置完成后，点击测试连接，会提示连接成功的信息，如下图所示：



9. 配置完成后运维用户就可以直接使用本地的Navicat软件来管理SQLServer数据库了。

7. FAQ

Q：使用web方式运维堡垒机时一直提示更新组件，如下图所示：



A:在运维界面点击右上角的相关下载按钮,重新下载BHostClient和BhostReplay，将安装路径指定在D盘（不建议安装要默认路径,如果没有D盘的，建议安装在c:\Program\Files路径下）。

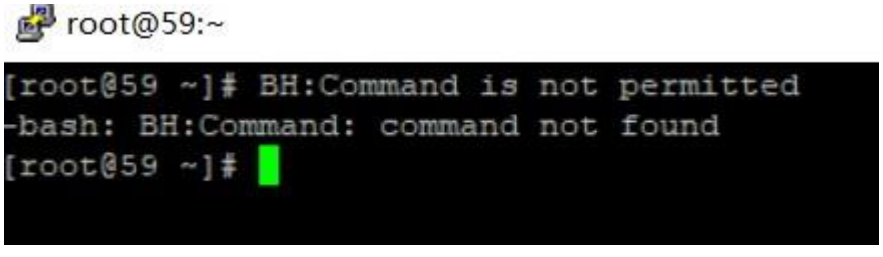
Q：使用堡垒机web访问方式运维时提示下图的报错?

A:请确认堡垒机的入站方向有没有放行8443端口的访问，web访问方式是需要调用H5组件，会用到8443端口。

Q：负载均衡SLB环境结合堡垒机使用时，发现无法正常进行运维？

A:负载均衡SLB环境结合堡垒机监听使用时，需要使用后端服务器的方式配置监听443，8443，5555，3389，222端口，不能使用虚拟服务器组的方式。协议要使用TCP（四层协议）。

Q：运维SSH协议时，使用su - 命令提示报错如下图所示：



A:通过编辑主机里的账号切换命令,将su删除掉即可，如下图所示：