东软 NetEye 统一身份管理系统（NABH）

快速使用手册

沈阳东软系统集成工程有限公司

2014 年 8 月

版权声明

本手册中涉及的任何文字叙述、文档格式、插图、照片、方法、过程等所有内容的版权属于沈阳东软系统集成工程有限公司所有。未经沈阳东软系统集成工程有限公司许可，不得擅自拷贝、传播、复制、泄露或复写本文档的全部或部分内容。本手册中的信息受中国知识产权法和国际公约保护。

版权所有，翻版必究©

目　录

1. 前言

1.1 阅读说明

本文档为东软 NetEye 统一身份管理系统的快速配置手册。文档中的管理员拥有运维管理、口令管理的权限（不包含审计权限）。其中，**黑色粗体为强调的内容。**红色字体表示特别要注意的事项。

1.2 适用版本

本手册，适用于 3.7 发布版。

1.3 使用环境

NABH 的管理员使用 WEB 登录方式作为用户界面。可以使用 Microsoft Internet Explore 或以其为内核的其他浏览器，因部分控件的兼容问题，如果您使用的是 IE 8 版本以上浏览器，请在兼容模式下进行运行。

2. 准备工作

2.1确定访问的服务器

该内容是准备工作的重点，主要是确定核心服务器提供何种类型的运维协议供运维终端访问，即确定运维终端使用 Telnet、SSH、FTP、SFTP、RDP、XWIN、VNC、VDH、HTTP 和 HTTPS 的哪些协议去访问核心服务器进行日常运行维护操作。

2.2确定用户

即确定运维人员的用户名、授权信息（主要是指某运维人员可以通过哪些协议访问哪些核心服务器或网络设备）。

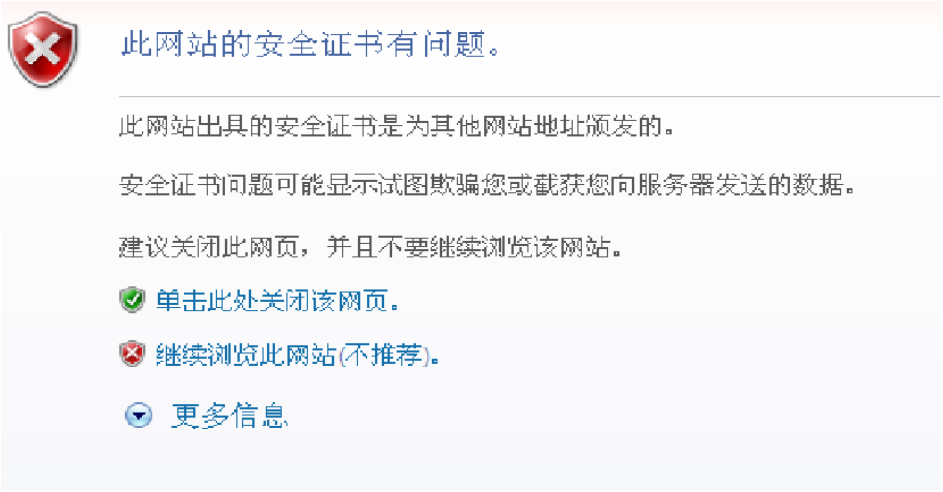
3. 首次登陆

3.1 用户名、密码

此处请联系管理员，确定认证方式等

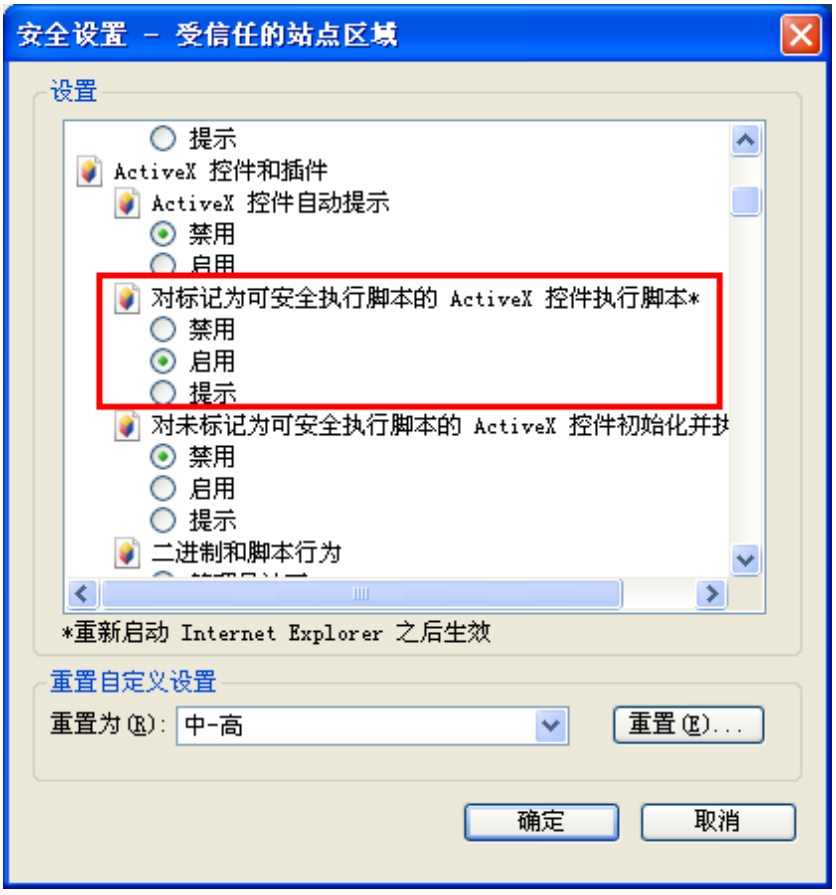
3.2 浏览器设置

用 IE 浏览器访问：https://192.168.1.100；访问过程中，如果是 IE7/8，会出现证书安全警告等信息：



选择“继续浏览此网站”，进入登陆页面。

浏览器中 “工具/Internet 选项/安全”，找到“对标记为可安全执行脚本的 ActiveX 控件执行脚本”，保证该选项为“启用”状态。浏览器的安全级别最高支持“中-高”。



用户登录，如果是令牌模式的管理员，或证书认证的管理员，请不勾选“口令认证”。 以

下以口令认证的管理员登录为例进行说明：

以下是登录成功首页：

首页内容为：当前日期、上次登录时间及登录 IP、最近 10 次操作记录。操作记录包含操作时间、操作的客户 IP、操作功能模块以及操作内容。为了安全性考虑，建议静态口令用户登录后，点击页面右上角“修改密码”，对密码进行更新。

4. 管理员操作步骤

由 admin 创建管理员后，后续的 NABH 的一切管理工作则可交由管理员进行管理。包括配置用户、设备、授权、运维规则以及告警等。本章节将依次对这些功能做介绍，用户可按照本文的顺序进行配置。

4.1 配置用户

用户是 NABH 系统的核心，也是运维的基础。“运维管理\用户管理”中，可以对运维用户进行添加、删除、编辑、授权的管理功能，提供用户的批量导入、导出功能。

添加用户有三种方式：

- 手工创建：用户自行创建一个新的用户；
- 批量导入：使用 excel 模板批量导入；
- 引用管理员：在已有的管理员中选择一个或若干个管理员，将其赋予运维用户的权限。

手工创建用户：

进入添加用户界面，选中“手工输入”，如下图：

各个配置项的基本配置可参考“添加管理员”章节。此处仅讲述与管理员的区别：

用户级别：此功能与双人复核功能相关（**S 版中此功能项无效果**），默认为 3 级；

用户组：可快捷的选择用户组；

用户也可以使用“引用管理员”的方式添加运维用户，即为管理员赋予运维用户的权限。

批量导入：

批量导入需要使用 NABH 的模板，在此基础上进行用户编辑。

注：模板中的各表头字段不可删、减、更改；

导入模板中“口令认证”的用户，明文“密码”不能超过 16 位；

方法如下：

- 先新增一两个用户（可作为样例）；
- 点击“用户导出”按钮，导出一个模板。

导出模板如下：

	A	B	C	D
1	用户名	姓名	密码	认证方式
2	111	123	3D4F2BF07DC1BE38B20CD6E46949A1071F9D0E3D	口令认证
3	test2	托尔斯泰	3D4F2BF07DC1BE38B20CD6E46949A1071F9D0E3D	口令认证
4	liuxf1		DB36FAE6C45F2C61E558829BE2227B388CC14DAE	口令认证
5	liu1		6C400B71D81A5759CCCADC2D5C095F6BA596CB9E	口令认证
6	zhangyk1	张永康	46720008E733325475BD0C7AFC8D3AD24607A93E	口令认证
7	meng2	蒙	3D4F2BF07DC1BE38B20CD6E46949A1071F9D0E3D	口令认证
8	liuxf2	刘旋风	3D4F2BF07DC1BE38B20CD6E46949A1071F9D0E3D	口令认证

用户列表中，不对用户密码做导出。

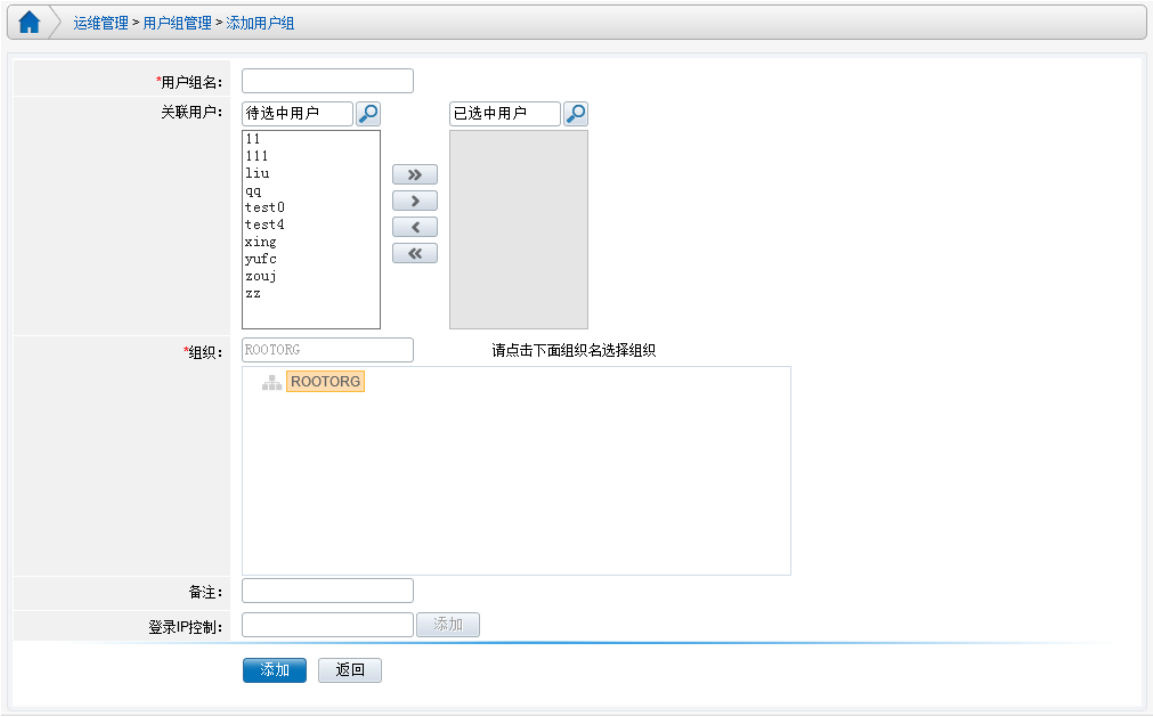
导入的列表中如果输入密码，可导入，如果密码字段为空，则导入后状态置为“未激活”。

当导入的 Excel 表中与已有用户重名时，采用覆盖更新方式处理。

4.2 配置用户组

用户组是将用户进行分组管理，从而方便的实现批量授权。一个用户可隶属于多用户组。

选择“运维管理/用户组管理”，点击“添加”，出现如下界面：



在“待选中用户”中将所要添加的用户右移至“已选中用户”，即可完成用户组的添加。

4.3 配置设备

用户配置好后，接下来需要对设备做配置。与用户一样，可单个添加、可分组管理，可批量导入、导出。设备，此处指核心运维服务器，也可指各种网络设备。

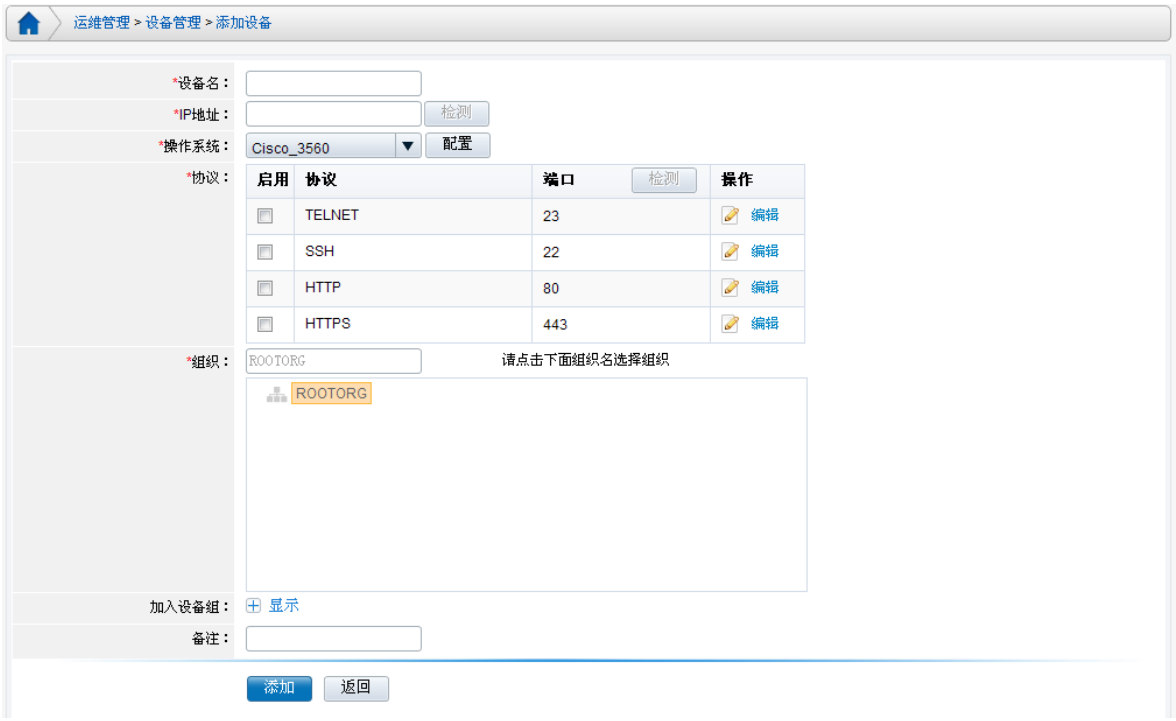
进入“运维管理/设备管理”界面：

- 可通过快速查找对设备进行过滤
- 可通过高级搜索（设备组、操作系统、协议、IP）对设备进行过滤

- 可针对设备名、操作系统、IP 地址对设备进行排序
- 可添加、编辑、删除设备
- 可通过设备导入、导出批量添加设备
  - ***设备导入***：即以 Excel 的形式导入设备配置列表。导出列表包括：设备名、操作系统、IP 地址、资源列表等信息；
  - ***设备导出***：即以 Excel 的形式导出设备配置列表。导入列表包括：设备名、操作系统、IP 地址、资源列表等信息。

添加设备

进入“运维管理/设备管理”后点击“添加”，进入设备添加界面：



设备名：定义设备名称；[必选项]

IP 地址：输入服务器 IP 地址；[必选项]

检测： 用于检查该设备与 NABH 是否联通。

操作系统：从下拉框中选择该设备对应的操作系统；[必选项]

注：若操作系统列表不能满足您实际应用的需求，请进行“配置”添加操作系统，参见后续“添加操作系统”小节

协议：选择远程访问设备时使用的协议；[必填项]

端口检测：用于检查该设备端口是否联通

加入设备组：可以将要添加的设备放置到设备组中

备注：可选项

添加设备，如定义一台 Redhad_AS4：10.10.1.29，协议为：telnet，此时可检测协议端口是否联通，如下图：

可在协议对应的操作中编辑该协议的端口：

- 其中 telnet 协议是否支持中文，如下；

点击“保存”完成添加。之后可做编辑、删除、授权操作。

批量导入设备

用户可以使用“设备导入”功能进行设备的批量导入。方法如下：

点击页面上方的“设备导出”按钮，导出一个 excel 表

该表格中有准备好的数据格式，按照该表格的格式，可以添加大量的设备，之后利用“设备导入”功能，将该表导入到 NABH 即可完成设备的批量添加。

当导入的 Excel 表中存在和已有设备或 IP 重名的设备时，采用**覆盖**的方式处理。

4.4 配置 OS 协议

NABH 为每个操作系统默认配置了常用的协议，如 Cisco-3560 默认配置有 TELNET、SSH、HTTP、HTTPS 四种协议，Windows 设备默认配置有 FTP、RDP、HTTP、HTTPS 四种协议等，其他 Linux 设备也有默认的协议。如果实际应用中，可能会出现协议不够用的情况，可

通过配置来新增。**此配置为可选项。**

下面以 Windows 设备为例，要新增 VNC 协议来做介绍：

选择“运维管理/设备管理”，进入添加或编辑设备界面，在该页面点击操作系统后面的“配置”，进入到操作系统配置页：

通过编辑进行操作系统配置，完成添加当前操作系统中不包含的协议，点击“保存”即可。

4.5 添加操作系统

当现有操作系统类型不满足客户需求时，可通过进入“运维管理/设备管理/添加设备/配置”中的“添加”来增加操作系统。**此配置为可选项。**

下面以增加 H3C 操作系统为例：

系统名称：编辑操作系统时不可修改，添操作系统时可通过下拉列表选择 H3C 操作系统；

系统版本：操作系统对应的版本；[选填项]

权限提升：具有权限提升的操作系统，可勾选此项，此处选择启用：

提升命令：填写权限提升的命令，如：Cisco 为 en，H3C 为 su，linux 类只支持 su

- 注意：提升权限的完整命令为：enable 和 super。但是在实际应用中，通常使用简写。Linux 操作系统只支持 su，不支持 su 带参数。

- 如果在这里填写 en、su，那么在实际应用过程中，en/ena/enable、su/super 等命令都可匹配为权限提升。

提升口令符：填写当输入“权限提升命令”后，操作系统出现的固定提示符，如：Password：

- 注意：应根据实际的情况，确认权限提升口令符中的“：”后，是否需要添加一个空格。

协议：选择操作系统开放的协议；

服务协议包括：TELNET、FTP、SFTP、SSH、RDP、XWIN、VNC、HTTP、HTTPS、VDH 应用协议；[必选项]

点击“保存”完成编辑。

4.6 配置设备组

“设备组”将设备进行分组管理，将具有相同共性的设备归类，方便批量授权。选择“运维管理/设备组管理”，页面如下：

1）设备组添加，点击上图中“添加”：

添加时，提供按设备名、IP 地址过滤查询的功能，方便管理员添加。

设备组名：[必填项]

备注：对资源组的描述说明。

设备列表：可选择的设备。

点击“添加”完成设备组添加。

2）设备组编辑，点击设备组管理界面“操作”中的“编辑”，即可对设备组信息进行编辑。

3）设备组删除，在“运维管理/设备组管理”，勾选所要删除的设备组前面的复选框，点击“删除”或者直接点击“操作”中的“删除”按钮即可完成设备组的删除。

4）设备组授权：点击设备组管理界面“操作”中的“授权”按钮，可进入到“运维管理/授权管理/授权规则”，可查看该设备组的授权信息。

4.7 配置访问规则

NABH 系统默认存在一个名为 *ANY* 的所有权限访问规则。规则是用于定义用户访问后台设备的要求，主要是对会话时间、会话长度、地点、会话类型做限制。如无需限制，则选择 ANY 即可。**此配置为可选项。**

若用户想要自定义访问规则，可阅读以下章节，否则可跳过。

添加规则的具体配置步骤如下：

1) 选择“运维管理\授权管理\授权规则”，显示如下：

➢ 可针对规则名、客户 IP 对列表进行排序

2) 点击 “添加”按钮，出现如下配置页面：

规则名：可任意填写；[必填项]

访问日期区间：用于设置访问该资源的具体时间，包含以下几个方面：

年/月/日：限制可访问该资源组的年、月、日，不填为不限制；[可选项]

周：限制可访问该资源的一周中的某天，如周一~周日（以 1~7 表示），不填为不限制；[可选项]

时间：限制可访问该资源的一天中的时间段，格式为：hh:mm-hh:mm，如：13:00-23:59，不填为不限制； [可选项]

会话时间：限制可访问该资源持续会话时间，以分为单位，只能为数字范围为：1-9999，不填为不限制；[可选项]

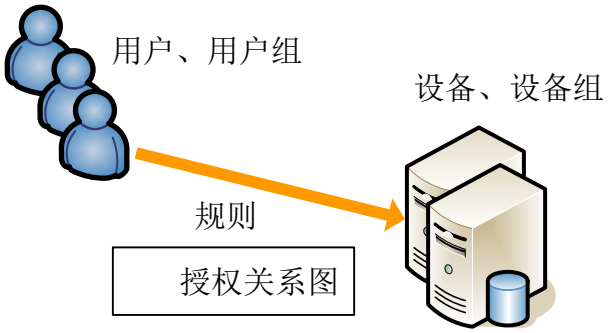
客户 IP：限制可访问该资源的 IP 地址，不填为不限制。[可选项]

3) 点击“添加”即可完成访问规则设置。

用户和设备配置完毕后，就可以开始做授权绑定了。授权管理定义了用户、用户组可以访问的设备、设备组，并且指定了对应的授权规则和访问规则。选择“运维管理/授权管理”，页面如下：

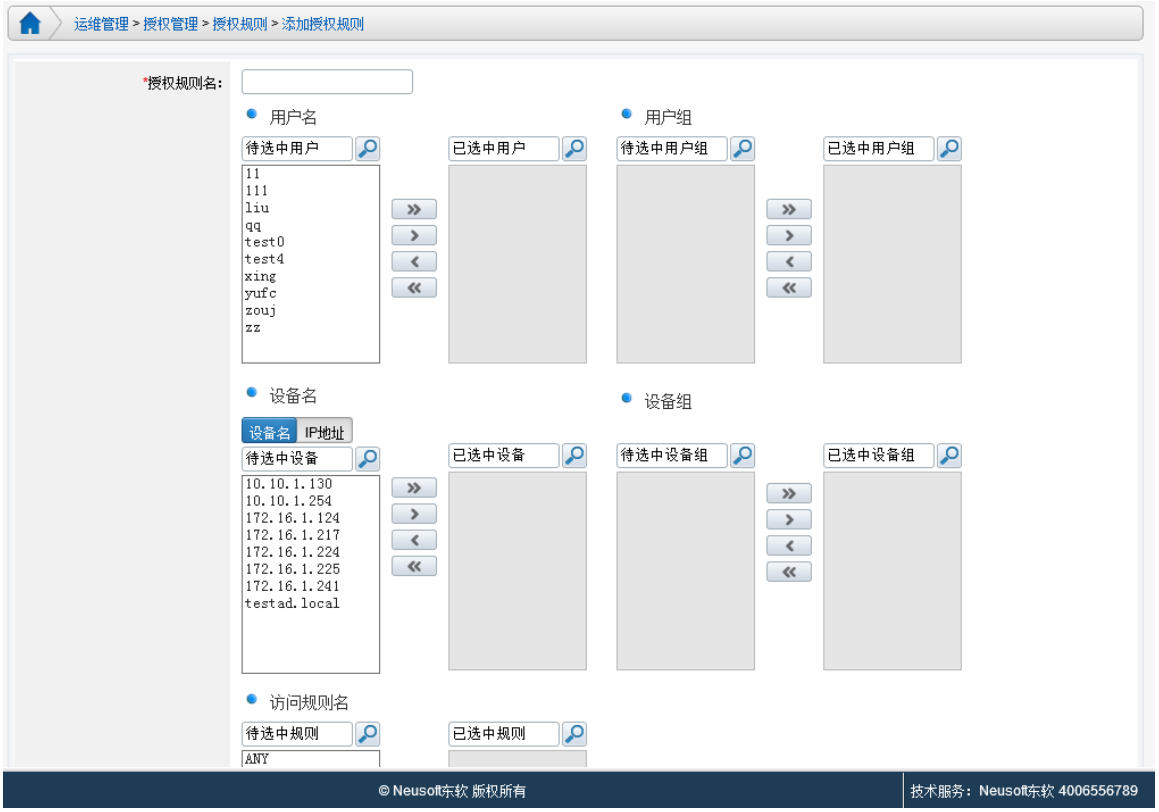
4.8 配置授权

在前面的章节，已经对用户、用户组、设备、设备组的创建一一做了讲述。接下来，则介绍授权这一重要章节。



通过创建授权规则，将用户/组与设备/组，以及规则三者进行绑定，从而实现运维。对相同设备、设备组有相同规则的运维，均可通过一条授权解决。

1）选择“运维管理/授权管理/授权规则”，点击“添加”：



授权规则名：定义授权规则的名称；

用户名、用户组：此两选项为并集关系，可单选也可多选；

设备名、设备组：同上，此两选项也为并集关系，可单选也可多选；

访问规则名：访问规则名；

配置完授权后，用户就有了后台设备的访问权限。另外，用户、设备界面也存在授权入口，方便用户快速配置。

4.9 配置设备帐户

前一节中完成了授权，用户就可以通过 NABH 访问后台设备了，但还需要自己输入用户名和密码。如果需要 NABH 完成自动登录的功能，则还需为每个用户配置相应的设备帐户。

具体步骤如下，以 linux 设备 10.10.1.23（Redhat_AS4）设备的管理帐户 root 以及网络设备 10.10.1.254（H3C）的匿名帐户[null]为例：

1）选择“口令管理/设备帐户管理”：

2）在“设备”下拉列表中选中所要添加帐户的设备名 ；

3）点击“添加”按钮，则进入添加设备帐户界面；

帐户类型：包括普通帐户、管理帐户、特权帐户、FTP 帐户、VNC 帐户和 VDH 应用帐户，用户根据实际选择帐户类型；

注：

- 仅网络设备和 Linux 或类 Unix 设备：支持特权帐户；
- 网络设备的特权帐户可托管；
- Linux 或类 Unix 设备的特权帐户不能托管；
- 特权帐户不校验帐户密码；
- 管理帐户不添加，即可托管普通帐户

帐户级别：默认为 1 级，与告警功能相关，具体用法见本文 4.12 章

密码更新周期：帐户托管设置密码周期；[可选填]

SSH 密钥登录：是否启用 SSH 密钥登录功能，仅适用开启 SSH 服务的设备；[可选项]

登录私钥：上传 SSH 密钥登录的私钥；[可选项]

关联用户：此处关联的用户，则可使用该帐户自动登录；

关联用户组：此处关联的用户组中的所有用户，都可使用该帐户自动登录；

帐户状态：设置帐户激活或未激活，激活时可用；

点击“保存”完成添加。

对于网络设备，如：10.10.1.254，在“设备”下拉列表中选中所要添加帐户的设备名，可按上例所说的设备帐户进行添加匿名设备帐户。以下介绍匿名设备帐户的添加，进入添加页面，可以看到“匿名帐户”勾选框：

勾选“匿名帐户”，并填入密码：

点击“保存”完成添加。

注：NABH 所支持的网络设备包括以下操作系统：Cisco、Fortigate、H3C、NetScreen、Topsec。

4.10 SSO 配置

SSO 配置在设备帐户的托管方面，起到非常关键的作用，通过配置文件，可以实现自动登录，帐户的更新托管。NABH 系统默认出厂时，配置了常用的操作系统文件，因操作系统，尤其是 Linux 各版本或多或少存在些特殊设置，所以当出现帐户添加失败，托管不成功的错误等，就要检查此部分配置文件是否与实际相符。**此配置为可选项。**

选择“口令管理/设备帐户管理”，

点击 SSO 配置，进入以下页面：

默认模板可覆盖大部分托管改密操作，对于部分特殊的帐户，如：提示符不同等。可采用手动追加配置，以“;”作为分隔符。

配置内容时，也可自动获取配置信息。前提：需要安装 portal 客户端。自动配置获取方法如下：

点击“配置获取”，弹出提示如图所示：

设备名称：根据操作系统类型，过滤“设备管理”添加的对应类型设备；

设备 IP：根据选择的“设备名称”显示对应的 IP 地址；

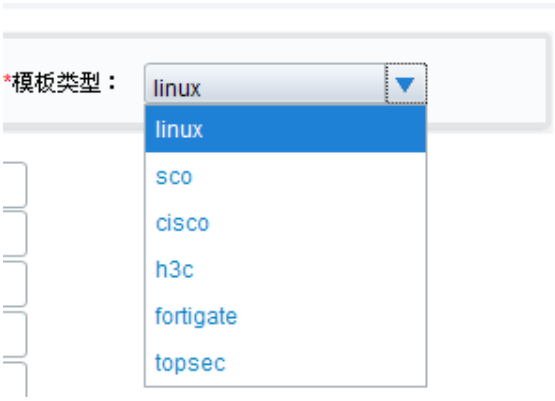
协议：根据选择的“设备名称”过滤协议。包含 ssh 或 telnet 协议；

点击“确认”按钮，则弹出 putty 运维窗口，模拟执行用户登录和改密操作，根据登陆和改密的过程，系统自动获取对应的 SSO 托管登陆配置信息。具体过程，见下列示例说明。

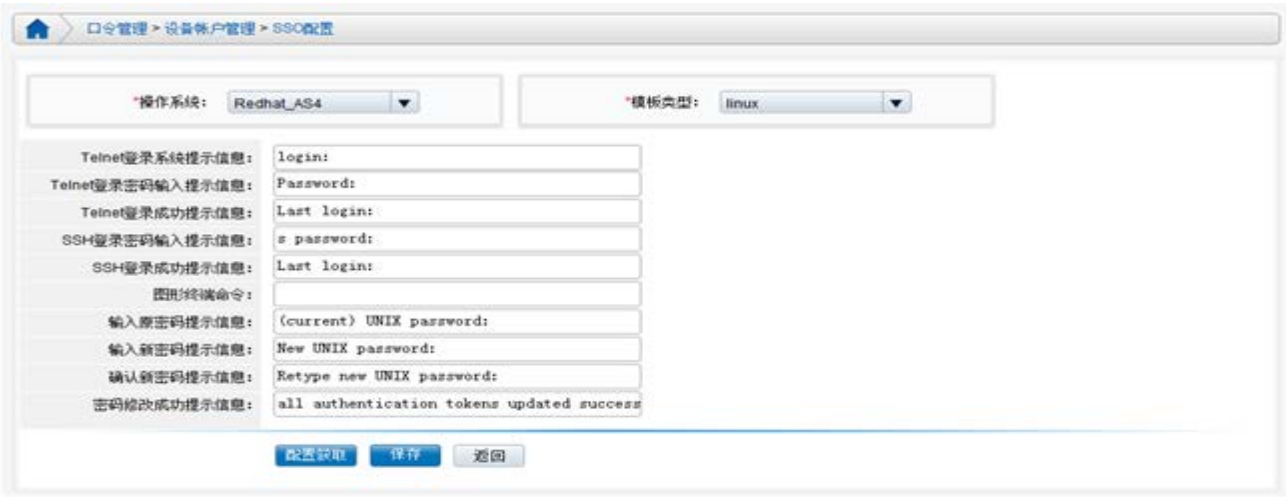
说明：putty 窗口模拟用户登陆和改密的操作必须一次成功，出现操作错误，非一次成功时，请退出重新执行模拟操作后再保存。

4.10.1 配置模板

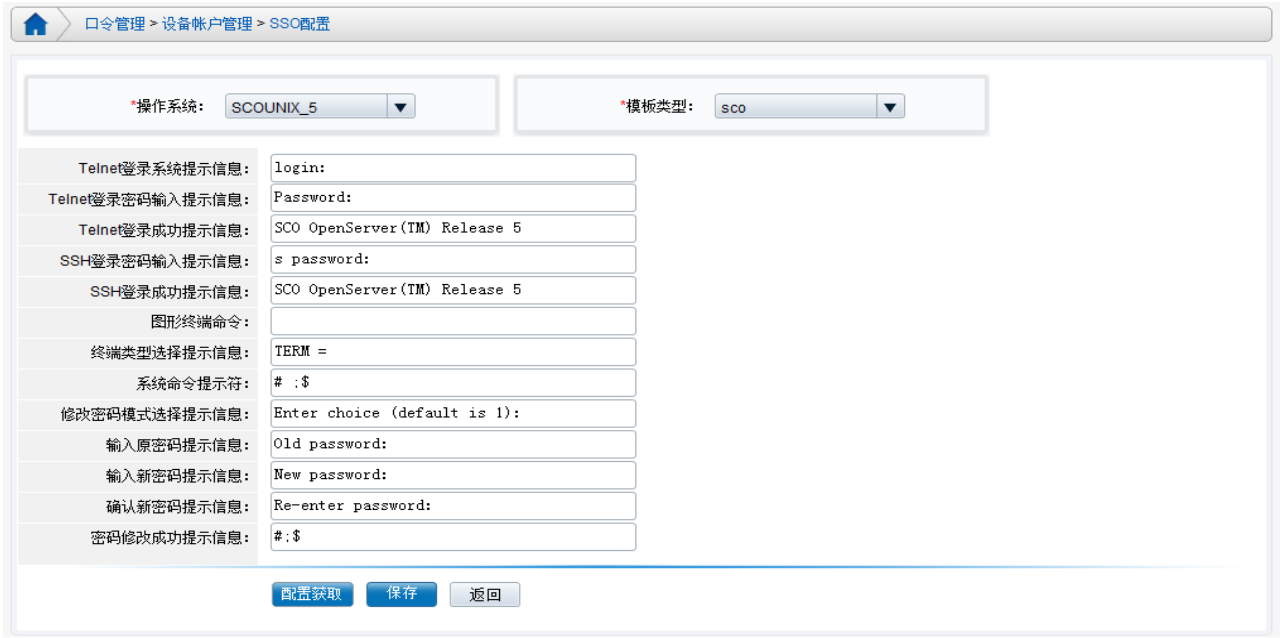
目前有三类模板：Linux、SCO（Unix）、网络设备：



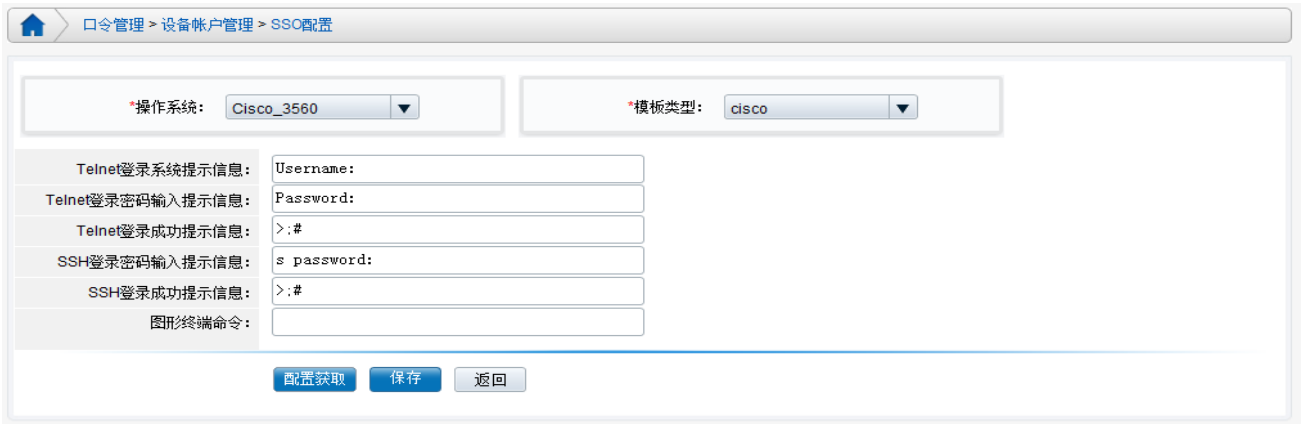
1）linux 模板的配置内容为：



2）sco 模板的配置内容为：



3）网络设备模板的配置内容为：

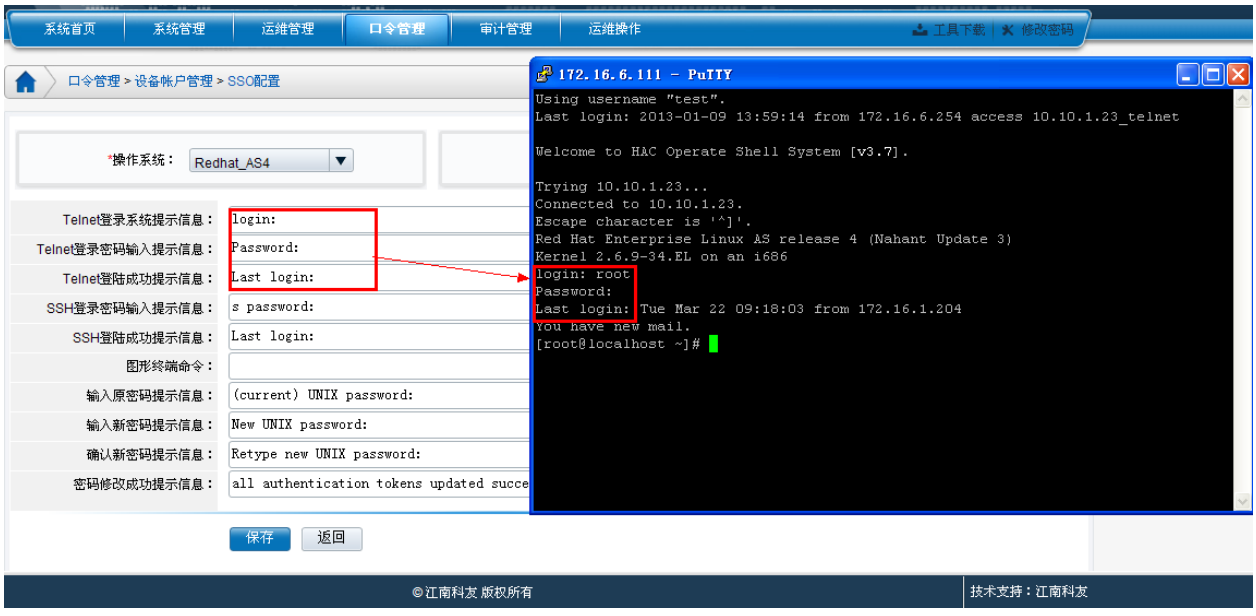


4.10.2 模板配置

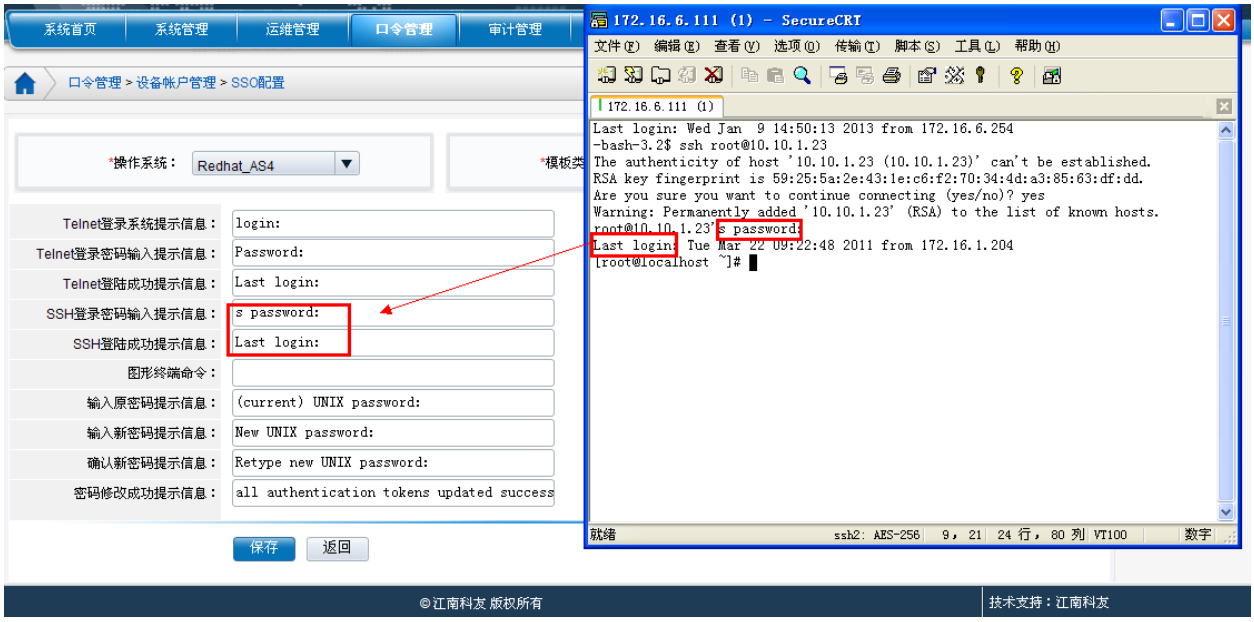
手动配置内容时，首先选择需要配置的操作系统，然后选择模板。当显示的模板符合要求时，再进行配置。存在多种提示符时，以“;”分隔。

以 Redhat_AS4 系统为例

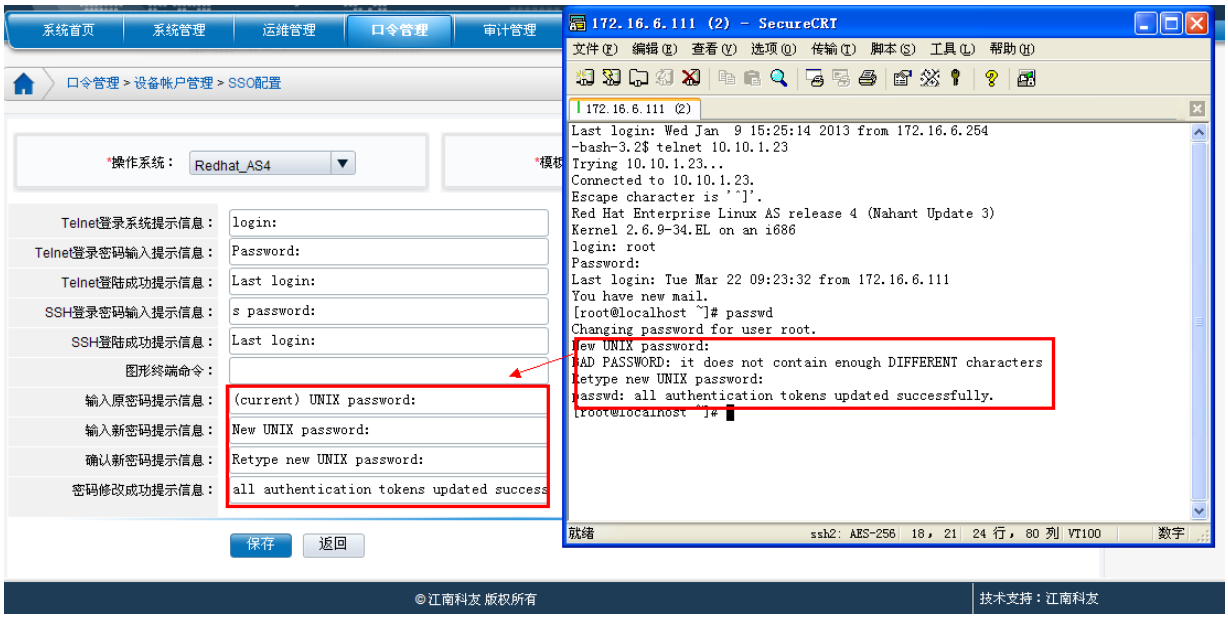
- telnet 登录配置，如下图：



- SSH 登录配置，如下图：



- 修改密码配置，如下图：
  - 该部分的配置是根据系统的普通用户修改自身密码来填写，而非 root 帐号的修改密码。



图形终端命令：指的是 xwin 协议自动登录时，启动的应用程序，比如 xterm，或 firefox 等。

4.10.3 配置获取

手动配置模板，存在困难时，可运用“配置获取”功能，采用模拟用户登录和改密操作后，自动获取对应的 SSO 配置信息。

注：模拟用户登录和改密操作必须一次执行成功，否则，请重新获取配置再保存。

以 Redhat_AS4 系统为例，如下图：

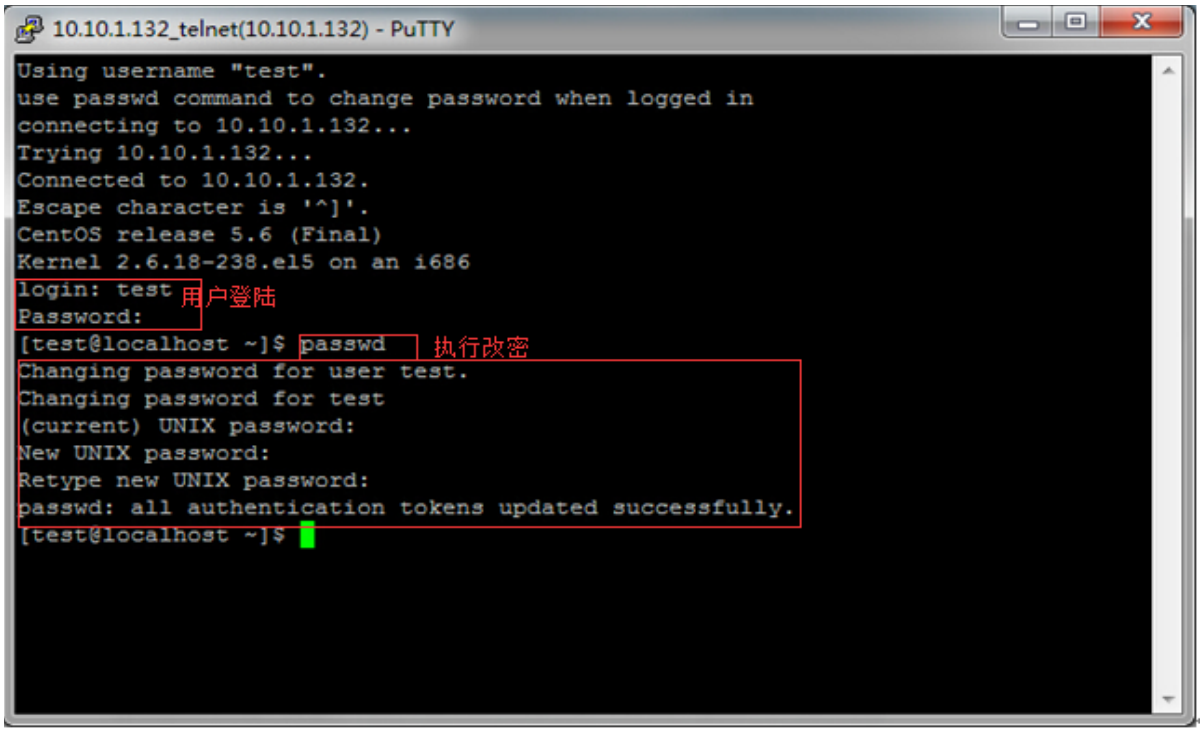
首先，添加需要获取 SSO 配置信息的设备，操作系统选择 Redhat_AS4，协议列表包含 telnet 和 ssh 协议。

进入“口令管理--设备帐户管理--SSO 配置”页面：

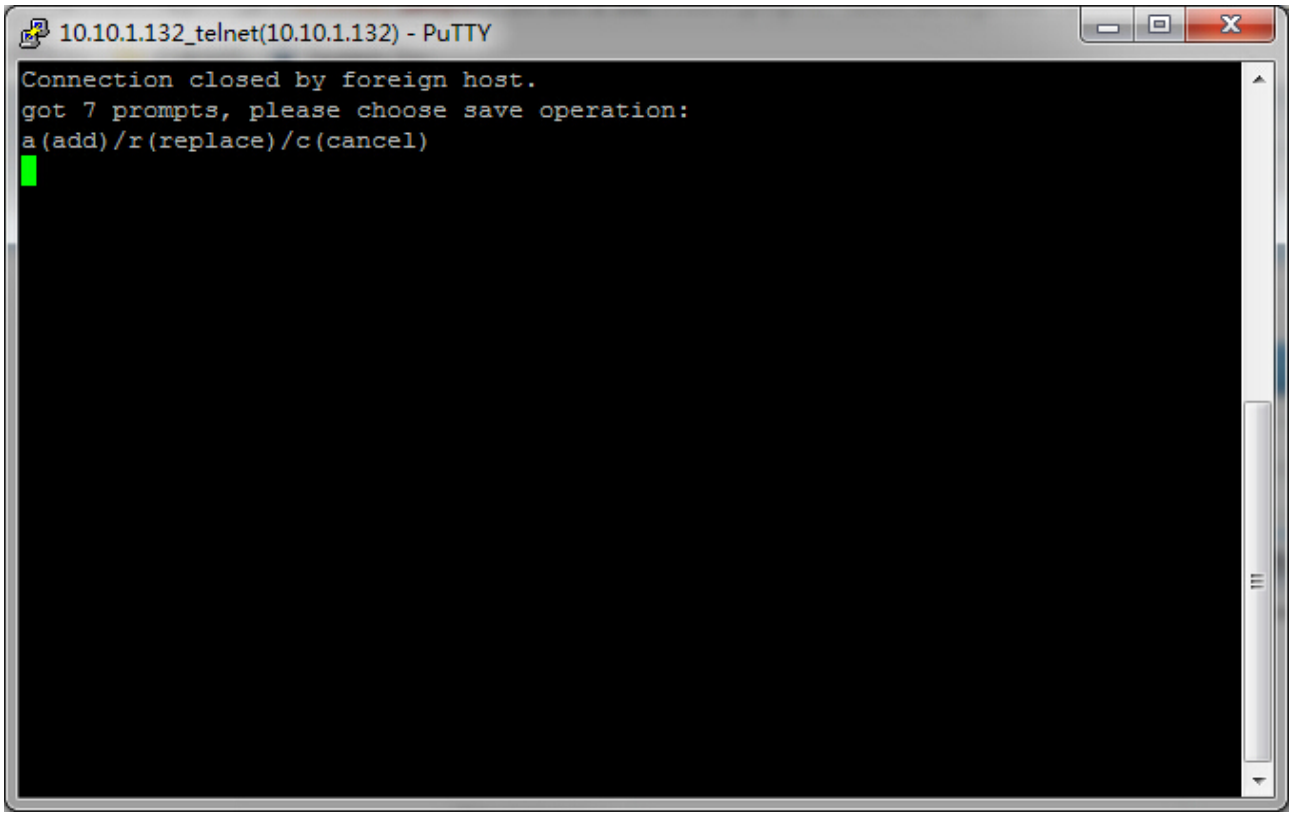
- 获取 telnet 登录配置，如下图：

选择操作系统为 Redhat_AS4，对应模板为 linux，点击“配置获取”按钮，弹出“配置向导”框，在“设备名称”下拉菜单中选择对应的设备，在协议下拉菜单中选择对应的协议 telnet：

点击“确定”之后弹出 putty 工具，模拟设备帐户执行登录和改密操作：



完成后，输入 exit 退出：



选择 a（追加）、r（覆盖）、c（取消），则弹出如下图所示的页面：

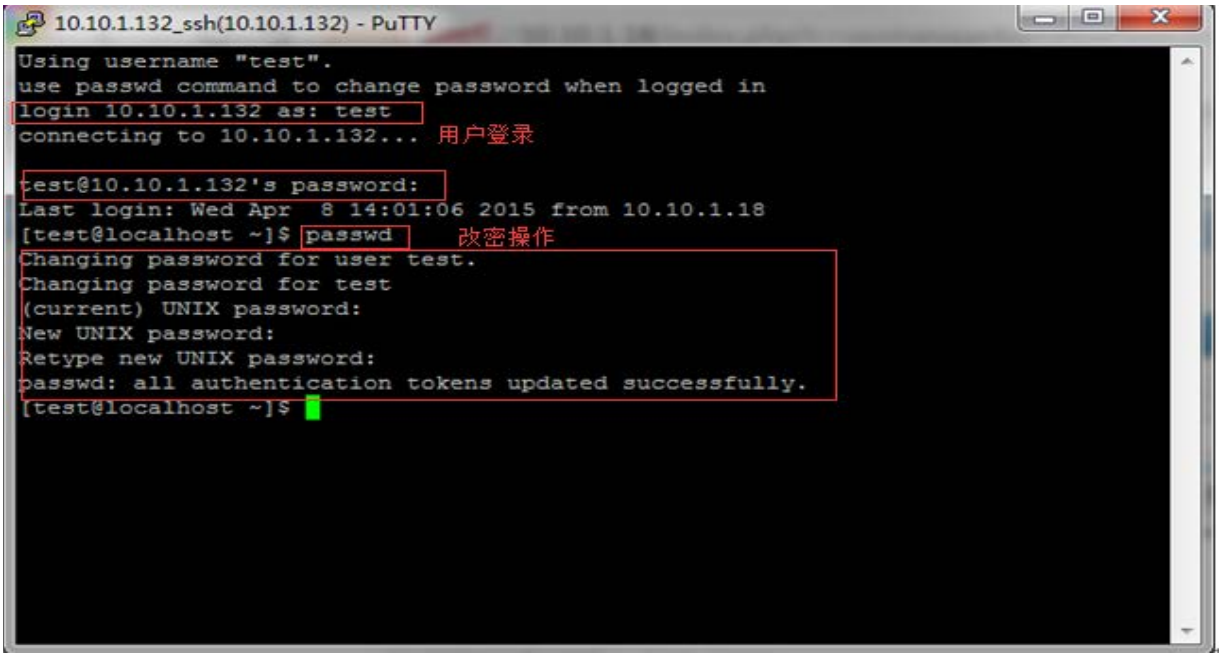
点击“继续配置”，则进入“配置向导”页面，可继续自动获取配置；

点击“配置结束”，则页面自动刷新，展示保存后的配置页面；

点击“保存”按钮，保存对应的 SSO 配置模板。

- SSH 登录配置，如下：

选择 ssh 协议进行配置获取，模拟用户登录并进行改密操作：



选择 a（追加）、r（覆盖）、c（取消），并结束配置，页面展示如图所示：

点击“保存”按钮保存此操作系统对应模板的 SSO 配置。

4.11 配置统一帐户

统一帐户，是根据 NABH 用户反映的现实应用而增加的一种比较特殊的帐户，用于方便、快捷的统一管理相同帐户。

在实际应用中，会有如下情形：一个运维用户负责维护多台服务器，出于方便记忆和管理，这些服务器上的帐户和密码相同。通过统一帐户管理进行帐户、密码的分配，实现了添加一次，则自动匹配所有的符合统一帐户条件的授权，同时，可以做到多台服务器帐户密码同时进行定期更新，大大减轻了口令管理员和运维用户的工作量。**此配置为可选项，可根据实际情况做配置。**

统一帐户的特殊性，添加成功有以下的前提：

1. 管理员已经配置了运维用户对设备的授权；
2. 如果是 Linux 和类 Linux 的帐户，必须满足相同操作系统，相同的登录配置；

具体操作步骤：

选择“口令管理/统一帐户管理”，进入统一帐户管理页面：

- 可添加、编辑、删除设备统一帐户；
- 可查看统一帐户日志；
- 可添加、删除统一帐户的隶属设备；

1）添加设备统一帐户，点击“添加”按钮，进入帐户添加页面

帐户名、密码、确认密码：即服务器的帐户和密码

关联用户：将设备帐户与运维用户关联，若运维用户拥有该设备的授权，则可使用该设备帐户直接运维；（举例选择 test 用户）

关联用户组：将设备帐户与运维用户组关联，若用户组拥有该设备的授权，则可使用该设备帐户直接运维；

SSH 密钥登录：选择是否启用 SSH 密钥登录功能，仅适用开启包含 SSH 协议的设备；

登录私钥：上传 SSH 密钥登录的私钥；

密码更新周期：设置密码定期修改时间。

备注：输入该帐户的备注信息。

状态：只有激活的帐户才能在运维过程被使用。

添加完后，在“设备帐户管理”页面中，也会自动添加该设备帐户。

在设备帐户分配页面中，会自动完成对该运维用户的帐户分配。

2）编辑设备统一帐户，点击主机帐户后面对应操作中的“编辑”，可对帐户信息进行编辑。

3）查看设备帐户日志：

4）设置，设备统一帐户添加完成，检测到用该帐户的设备会在“已选中设备”中显示，可添加，删除已选中设备：

4) 设备统一帐户删除，在您要删除的设备统一帐户前面复选框打钩，点击“删除”即可。

统一帐户添加成功后，在设备帐户界面中也会显示

4.12 告警管理

针对运维过程中可能存在潜在操作风险，NABH 根据用户配置的安全策略实施运维过程中的违规操作检测，对违规操作提供实时告警和阻断，以下对具体配置过程做介绍。**此配置为可选项。**

“告警管理”包含告警规则和命令规则两部分。命令规则指的是配置哪些命令需要做告警处理，告警规则是指明哪些用户、设备需要遵循指定的命令规则。

4.12.1 命令规则

目前 NABH 的命令规则区分为黑名单和白名单两种类型，且仅对文本协议和文件传输协议有效。以下对创建过程做详细介绍：

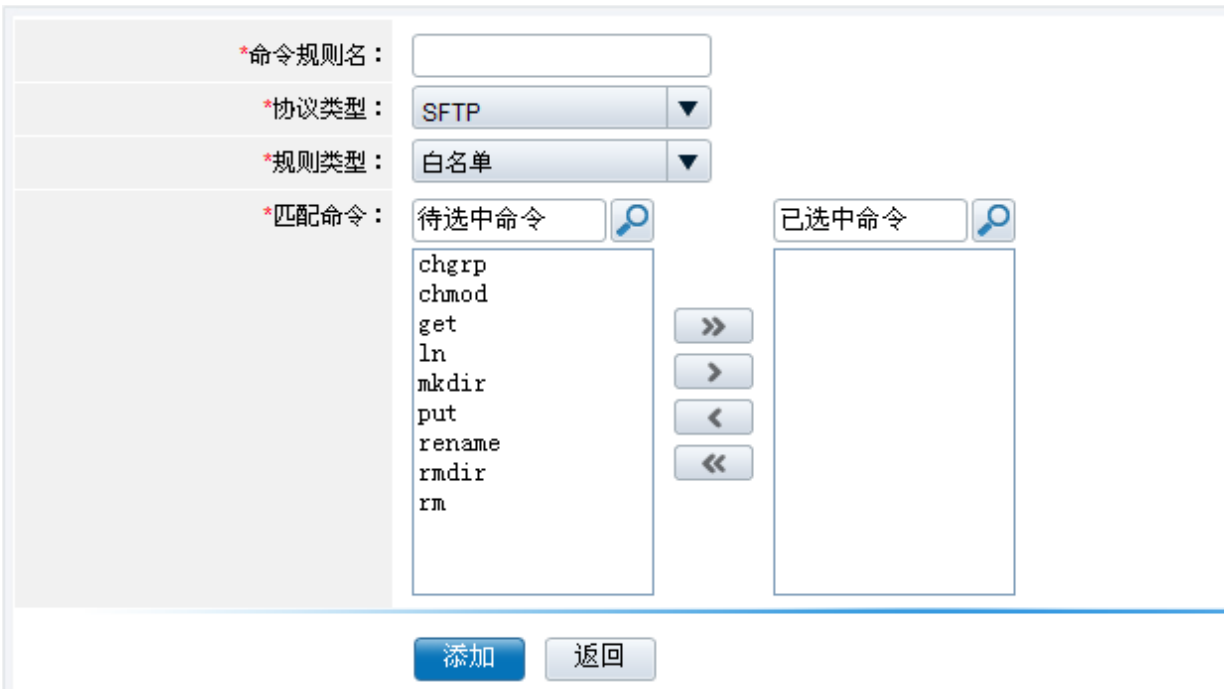
选择“运维管理/告警管理/命令规则”，

点击“添加”，

SSH 和 Telnet 告警配置页面

文本协议 Telnet、SSH 的黑白名单“匹配命令”支持正则表达式，可参考后续的告警样例。

FTP 告警配置页面



SFTP 告警配置页面

命令规则名：自定义[必填项]

协议类型：定义了此规则所适用的协议

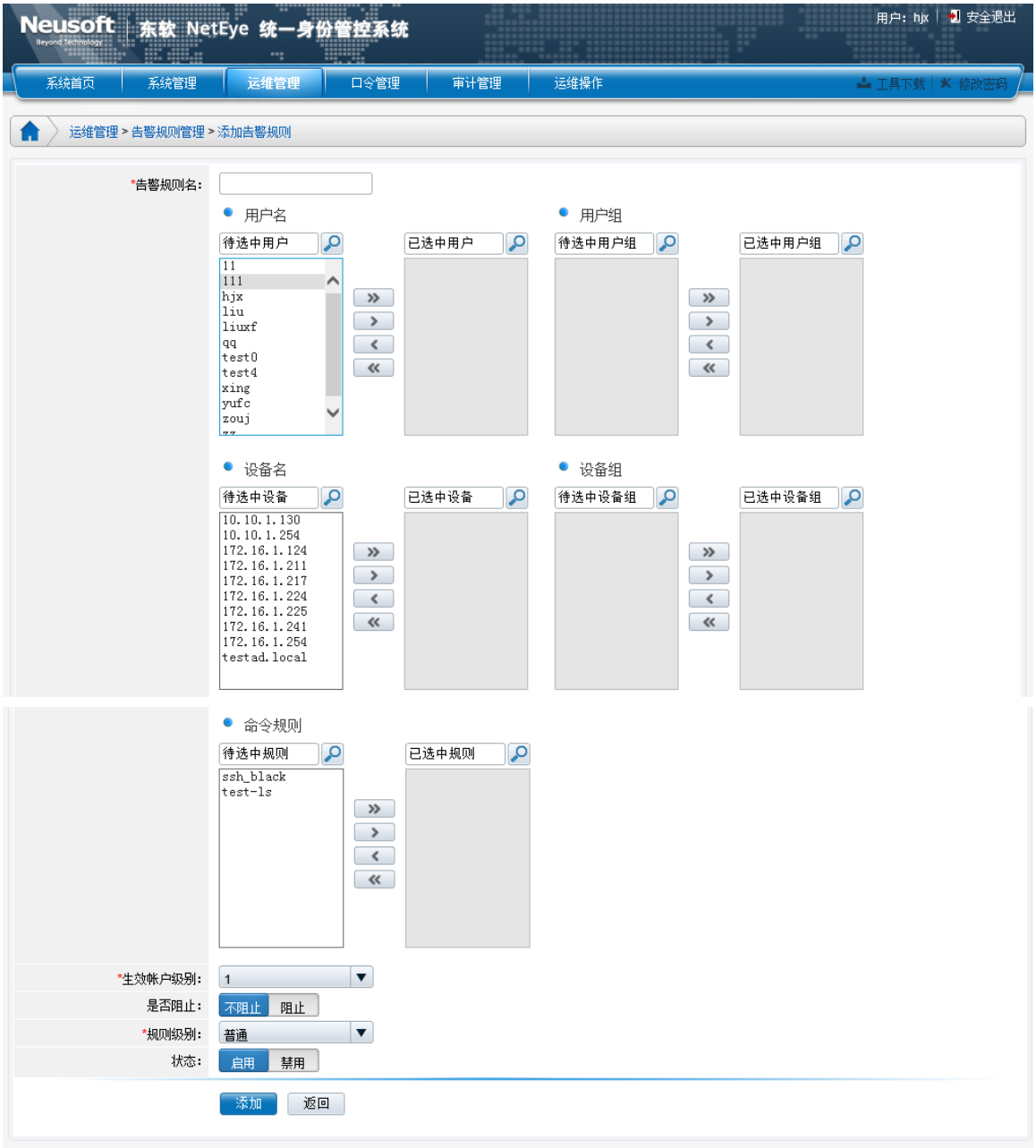
规则类型：黑名单或白名单

匹配命令：定义了此规则所适用的操作命令。

4.12.2 告警规则

选择“运维管理/告警管理/告警规则”，

点击“添加”，



告警规则名：[必填项]

用户名、用户组：可选择的用户或用户组信息；（两者可以选其一，也可以都选择）；

设备名、设备组：可选择的设备或设备组信息；（两者可以选其一，也可以都选择）；

命令规则：命令规则中定义的所有规则；

生效帐户级别：生效帐户级别指的是设备帐户的级别小于或等于设置的级别时，均告警。

规则级别：分为普通、严重、紧急。此级别划分后，不同级别在告警会话在审计平台中将呈现不同的颜色。紧急为大红粗体，严重为红色，普通为淡红色。

4.12.3 告警生效条件

告警能正常使用除了要创建完整的告警、命令规则之外，还与告警规则中的“有效帐户级别”和设备帐户管理中的“帐户级别”有关。

告警遵循以下规则：

1. **黑名单告警绑定级别大于等于设备帐户级别，告警命令有效；**
2. **白名单告警绑定级别小于等于设备帐户级别，告警命令有效；**
3. **未添加设备帐户时，授权关联黑名单，则黑生效；关联白名单，则白生效；同时关联，则黑名单生效；**
4. **黑白名单同时满足告警条件时，白名单不生效，黑名单生效。**

4.12.4 告警样例

黑名单的匹配命令符合 Pcre 正则表达式，可参考以下例子：

- 若要使某命令，如“shutdown”被阻断，其他的都可以放行，可应用黑名单，“匹配命令”设置为“^shutdown\b”；
- 若要使含有 cat 或 vi 或 pwd 任意一条命令出现，就会告警，可应用黑名单，“匹配命令”设置为“^cat\b|^vi\b|^pwd\b”，之间用分隔线|隔开；

白名单的匹配命令不符合标准的 Pcre 正则表达式，参考以下例子：

- 若要使除了某命令，如“cd”，其他的都不能使用，可应用白名单规则，“匹配命令”设置为“cd”；
- 若要使除了 pwd，date，cd 三条命令，其他均不放行，可应用白名单，“匹配命令”设置为“pwd,date,cd”，之间用逗号隔开。

5. 特殊设备配置

5.1 域设备支持

NABH 对于域资源的处理有特殊之处，配置上与其他资源有部分不同。该部分介绍域控制器、域成员以及域帐户在 NABH 上的配置，以下是具体配置过程：

1. 添加域操作系统

- 因域比较特殊，默认配置中无此系统，需要手工配置此操作系统。进入“运维管理/设备管理/操作系统配置”，点击“添加”：

- 选择 rdp 协议后，保存。

2. 添加域控制器

进入“运维管理/设备管理/添加设备”，添加域控制器：

设备名：要求是域控制器的真实名称；[必填项]

操作系统：选择 Domain；

3. 添加域成员

设备名：可自定义，符合设备名要求即可；

操作系统：选择 Domain。

4. 添加域帐户

- 进入“口令管理/设备帐户管理/帐户列表”，给域控制器添加帐户 user：

- 添加完成，返回到“口令管理/设备帐户管理/帐户列表”可查看到域帐户的格式显示为：帐户名+@+域名：

授权，过程同普通授权相同。

5.2 应用发布 VDH

1）应用发布中配置 VDH 和 VDH 应用，见《东软 NetEye 统一身份管理系统（NABH）维护手册》;

2）“设备管理”中添加含有 VDH 应用的设备，具体如下：

选择“运维管理/设备管理”，点击“添加”，点击操作系统后的“配置”进入操作系统配置界面

选择 Windows 操作系统，点击“编辑”，

在协议中找到 VDH 应用，此例为“PLSQL”将其右移至已选中协议中，点击“保存”。返回到设备添加界面，添加相应的设备。

IP 地址：后台服务器的地址；（此例为数据库的地址）

操作系统：选择 Windows 系统

3）授权，同普通帐户；

4）分配设备帐户

VDH 设备的帐户添加，帐户类型要选择“VDH 应用帐户”，自动登录类型目前除了支持 PLSQL、SQLPLUS、SVC、IBM_TS3310、JUNIPER_FW、SANGFOR、SPAM、ARRAY、JUNIPER_IDP、SQLSERVER2005 十类，用户根据自身需要自定义登录类型，具体见《东软

NetEye 统一身份管理系统（NABH）VDH 自登录代填操作手册》。

由于客户端本身或者用户的需求，部分应用发布协议登录需要填写扩展参数：

Spam：扩展参数为空时，默认为管理员登录，扩展参数不为空时使用内部登录，所选邮件域即为扩展参数的内容。

Array、Juniper_idp：扩展参数不填写时，使用 https 打开默认页面，扩展参数为“http”时使用 http 方式打开默认页面。

Sqlserver2005：扩展参数为“sqlserver 服务器 ip/端口号/数据库实例名”，例：“192.168.10.10，1433”、“192.168.10.10，testsql”、“192.168.10.10，1433，testsql”。

5）应用发布运维

选择“运维操作/应用发布”，点击“运维”应用发布协议，

其中扩展参数需填写数据库名称。

点击“继续”，即可以 SSO 运维 VDH 应用。