东软 NetEye 统一身份管理系统（NABH）

高级配置手册

沈阳东软系统集成工程有限公司

2014 年 8 月

版权声明

目　录

1. 前言

1.1 阅读说明

本文档为运维安全审计系统的高级功能说明手册。主要是对组织单位、双人复核、事件通知、帐户导出、设备托管功能做描述。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 3.7PE 发布版，用于说明 NABH 的高级功能。

1.3 使用环境

NABH 的运维管理员使用 WEB 登录方式作为用户界面。NABH 的运维管理员，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 浏览器，请在兼容模式下进行运行。

2. 组织单位

NABH 映射自然组织架构，遵从同级间不可随意跨越管理，低级服从高级组织管理的原则，实现了设备和用户独立管理，也可集中做审计。可支持纵向多达七级，横向 255 的组织架构。

组织单位功能包括组织单位的新增、编辑、详情和删除。组织单位功能界面如下：

系统默认根组织名称为“ROOTORG”。

点击“新增”按钮，进入添加组织界面，如下图：

组织名：输入组织名称；[必选项]

备注：主要是作为描述该组织的附加注释信息；[可选项]

可以通过对组织单位的编辑来修改组织单位的信息，除了根组织之外的其他级别的组织单位均可以删除，删除时要注意只有组织单位无下属组织、用户、设备时才能删除成功。

点击“详情”按钮，进入组织信息界面，如下图：

组织信息可以查看该组织单位中所包含的管理员、用户、用户组、设备、设备组。搜索功能支持模糊搜索。

以下面的组织结构为例，进行事例说明（以下的管理指配置和审计）。

网络中心、开发中心、运维部为三个独立的部门，上级领导部门为信息中心。三个部门相互独立，网络中心的管理员只能对本部门的用户、设备、管理员、授权做管理，其他部门（开发中心、运维部对网络中心来讲是不可见，同时上级信息中心的所有用户、设备也不可见），其他两个部门也同理。但信息中心（上级）则可对本部门以及下面三个部门的所有资源可见，可管。

对非根组织管理员屏蔽“全局配置”、“日志维护”、“系统维护”、“应用发布”、“运维配置”、“统一主机帐户”、“口令管理配置”、“设备帐户管理”中的“SSO 配置”。

3. 双人复核

双人复核是指运维用户在实际的运维过程中，需要第二人进行确认，否则不能放行。复核人还可实时监控活动会话。

总体来说，双人复核需遵循以下的几条规则：

- 可设置登录和告警两种情况需要复核；
- 用户可设置 0-5 级（低-高）；
- 高级用户可复核低级用户（第 5 级用户无需被复核）；
- 最高级用户无需复核；
- 仅 ssh 和 telnet 协议的 Portal 运维支持双人复核功能。

3.1 复核配置项配置

进入“运维管理/运维配置”，配置项中有“复核等待时间”、“ 复核权限级别”、“强制复核级别”三项，如下图所示：

复核等待时间取值范围：1~2147483647，单位为秒；[默认 120s]

复核权限级别取值范围：0~5；[默认级别为 3]

强制复核级别取值范围：0~4；[默认级别为 3]

下面以强制复核级别为例，点击“编辑”：

输入修改的值，此处为 1，点击“保存”，即完成修改。

此时，级别小于等于 1 的用户运维文本协议时必须复核才能登录。

3.2 用户级别设置

进入“运维管理/用户管理”，添加/编辑用户时，增加“用户级别”配置项，以下以添加用户为例：

用户级别设置完成点击“添加”用户添加。用户级别可以被编辑。

通过“用户导入”方式添加的用户，用户级别默认为 0。

3.2 复核事例

前提假设：

强制复核级别为 1，复核权限级别为 1，复核等待时间为 60 秒。

test0 用户级别为 0、test1 用户级别为 1、test2 用户级别为 2、test3 用户级别为 3、test4 用户级别为 4、test5 用户级别为 5。

即：

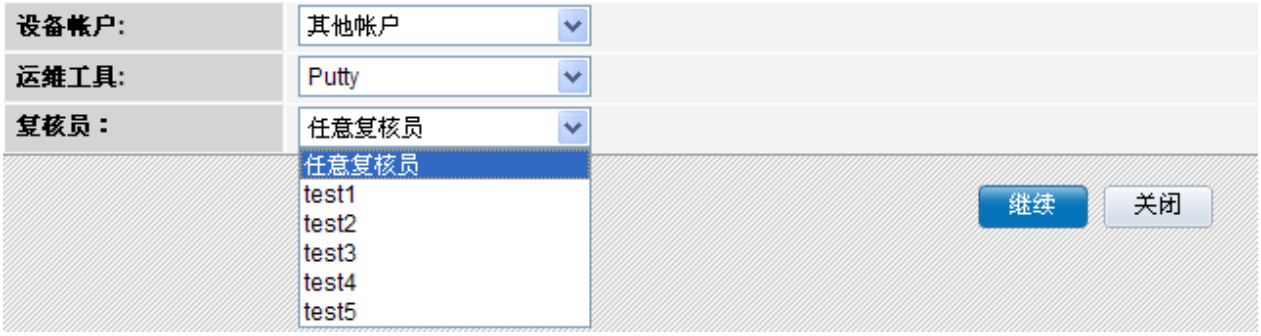
- test0、test1 登录访问文本协议是必须被复核，test2、test3、test4 登录时可选择复核或不符合，test5 登录时不需复核，因为没有级别比它高的用户能复核它；
- test1、test2、test3、test4、test5 具有复核权限。
- 会话超过 60 秒不复核自动退出。

3.2.1 用户登录复核

3.2.1.1 需强制复核用户登录

以 test0 使用“其他帐户”运维 SSH 协议为例。

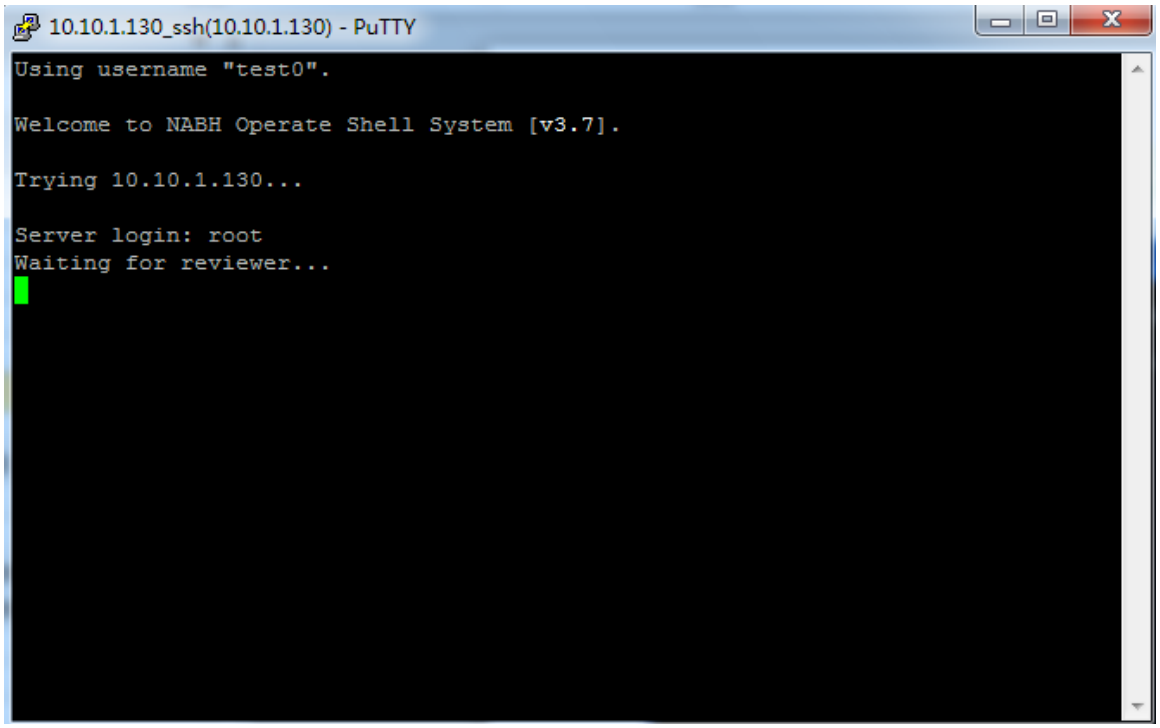
test0 是强制复核用户，必须进行复核才能登录，复核员下拉列表中显示的用户必须具有复核权限且级别大于 test0 的运维用户，“任意复核员”包含下拉列表中所有用户。如下图所示：



若用户选择“任意复核员”，则 test1、test2、test3、test4、test5 都有可以对该会话登录进行复核，其中一个人对会话复核后，其他人不能再对会话做复核。

若用户选择其中一个复核员如 test4 作为复核员，则只有 test4 能对会话进行复核。

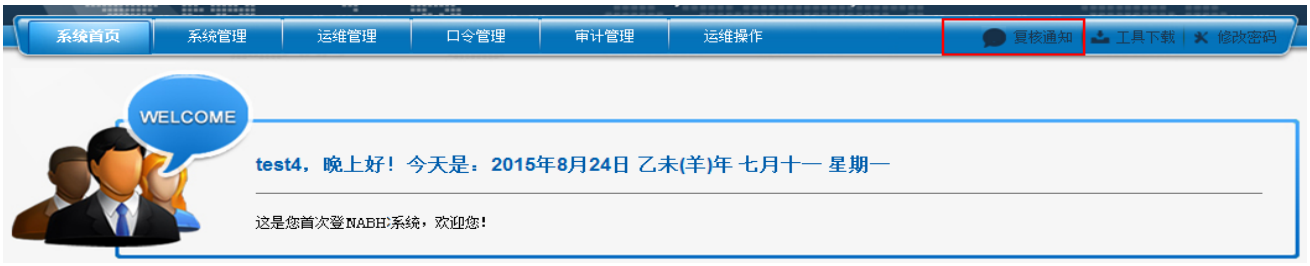
选择复核员如 test4 后运维界面显示为等待状态，如下图所示：



注：若点击“快速执行”，默认的复核员为全部复核员。

复核员在页面右上角可以看到闪烁的复核通知图标，复核员在 60s 内对会话进行复核，登录 HAC，如下图：

若复核员在 60s 内没有对会话进行复核，则会话提示超时退出。

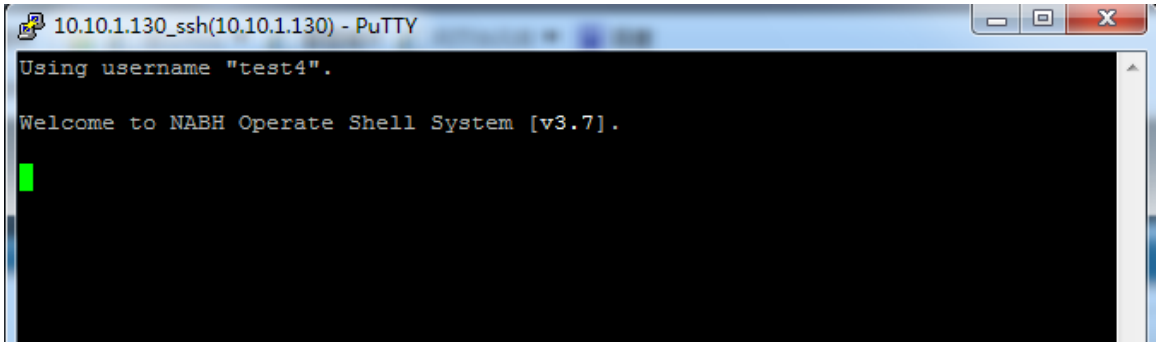


点击“复核通知”图标，弹出需要复核会话的列表窗口，显示需要复核的文本/图形会话信息，如下图。

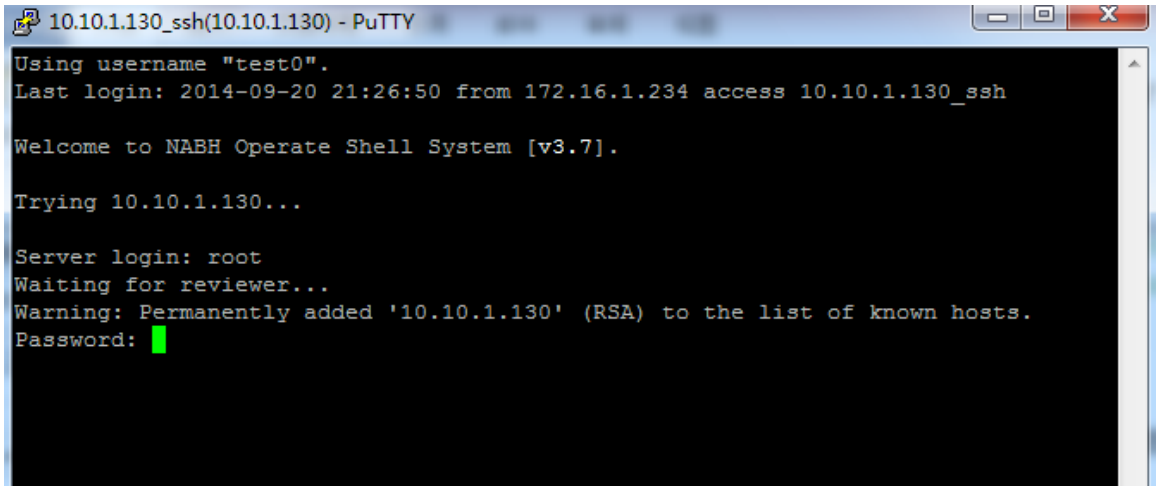
点击“复核”，会转到会话复核页面，如下图：

也可直接点击“运维操作—双人复核”，进行双人复核页面：

点击“复核”，弹出如下会话界面。



运维用户 test0 可输入服务器密码后开始进行会话：

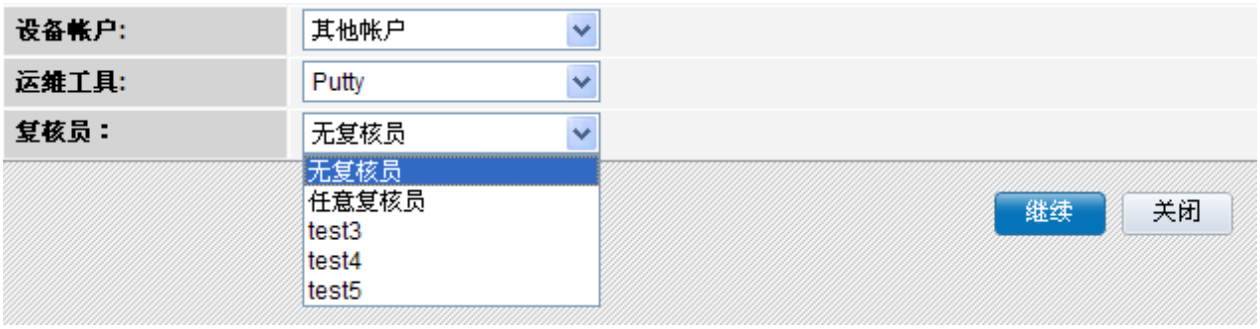


若运维用户使用分配帐户进行运维，复核员复核后无需再输入密码即可登录服务器进行操作。

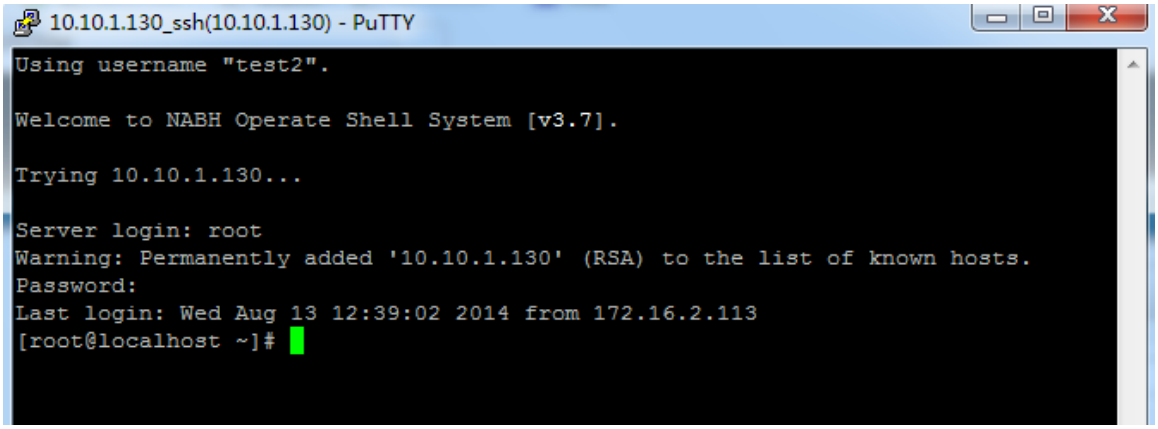
3.2.1.2 可选复核用户登录

以 test2 使用“其他帐户”运维 SSH 协议为例。

test2 为可选复核用户，运维时可选某个复核员、任意复核员和无复核员，复核员下拉列表用户必须具有复核权限且级别大于 test2 的运维用户，“任意复核员”包含下拉列表中所有用户。



test2 选择“无复核员”时，可以直接输入设备帐户名及密码进行运维。如下图：



若运维用户 test2 使用分配帐户进行运维，选择“无复核员”后不用输入用户名密码即可登录进行操作。

选项“全部复核员”或某个复核员，运维过程与强制复核用户类似。

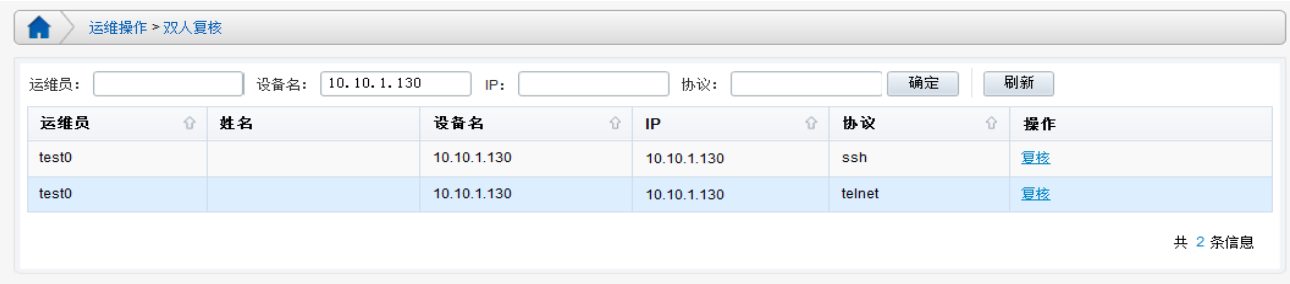
当运维用户通过“快速执行”方式 SSO 运维文本协议时，强制复核用户复核员默认选择“全部复核员”，其他用户复核员默认选择“无复核员”。

3.2.2 运维告警复核

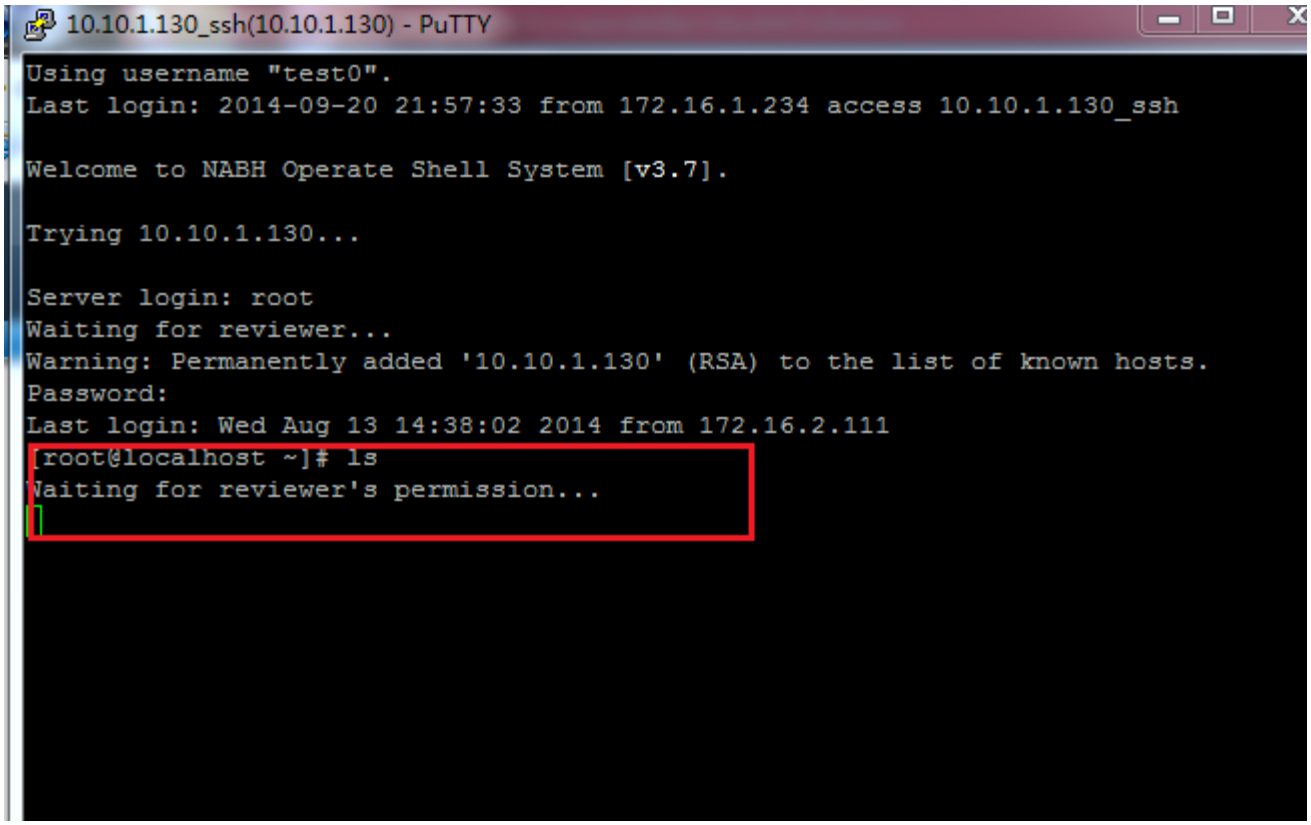
选择“运维操作/双人复核”，进入双人复核页面，如下图：

检索方式：运维员、设备名、设备 IP、协议，可按方式对复核会话进行检索。

下面以 IP 地址“10.10.1.130”模糊检索为例：

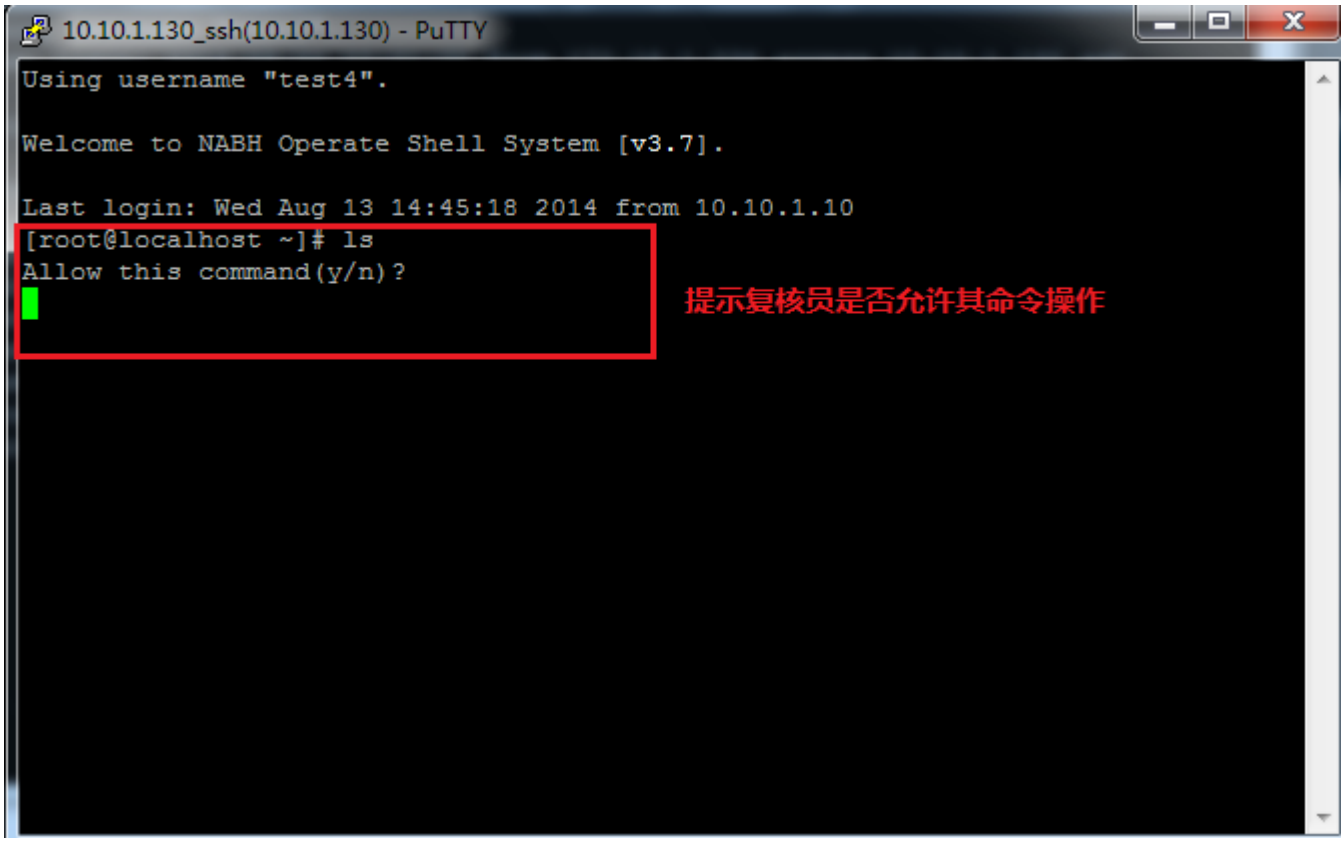


点击“复核”，进入复核窗口，当运维会话输入阻断命令，如：ls，则提示等待复核员的批准，如图所示：



图表 1会话终端

同时，复核员会收到是否允许运维人员执行当前命令的提示，



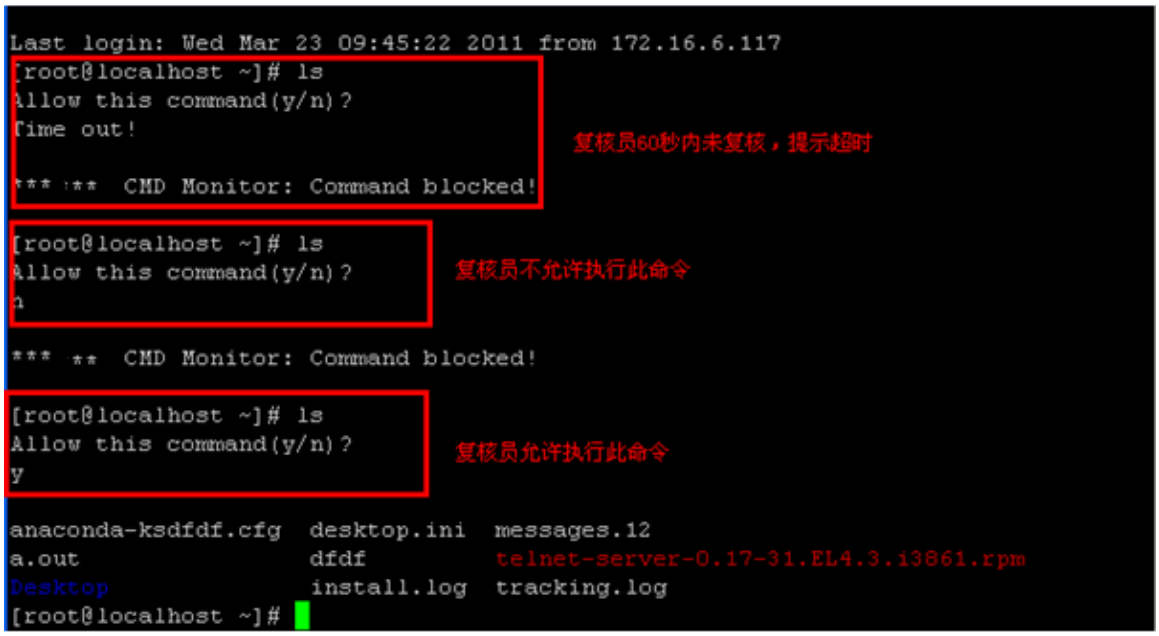
图表 2复核终端

- 若复核员输入“y”，则表示允许执行该命令，运维会话端显示复核结果并执行命令，同

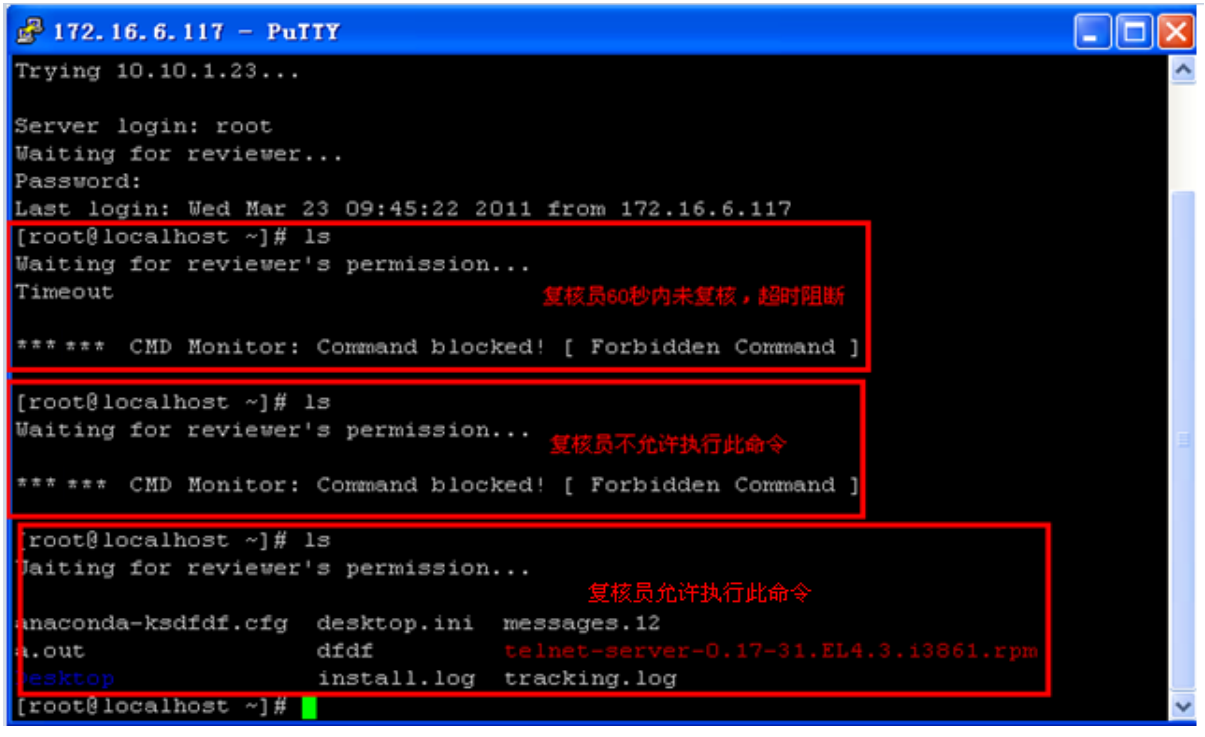
时复核端显示命令执行结果；

- 若复核员输入“n”，则表示阻断命令，运维会话端显示复核结果，并告警阻断。同时复核端显示阻断结果；
- 若复核员在超过 60 秒的时间内仍未做出复核操作，则运维会话端阻断当前命令，同时复核端显示阻断结果。

具体页面可参见下图所示：



图表 3 复核终端



图表 4 会话终端

当运维会话结束时，复核也结束。复核员结束复核会话不会影响运维操作，复核员可对会话进行多次复核操作，但所有复核操作只能是同一复核员。

4. 事件通知

事件通知功能可以将 NABH 上发生的事件以邮件或短信（需定制）的方式通知任何管理员：

添加事件通知对象：

姓名：事件通知接收者的姓名，可任意填写

通知方式：邮件通知

邮件地址：接收者的邮件地址

备注：备注信息，可选项

事件选择：可选择需要通知管理员的事件。主要分为：系统访问事件、配置管理事件、运维操作事件、运维审计事件和系统维护事件五大模块事件。您可以根据实际工作需要，定制不同的事件通知。

一旦有相关事件产生，则会接收到相应的邮件通知。内容如下：

你好，NABH事件消息通知：

用户"yufc"退出WEB系统。

== 该邮件由【NABH运维安全审计系统】自动产生并发送 ==

5. 设备帐户导出

进入“口令管理/设备帐户管理”界面，点击“帐户导出”按钮，可以导出全部主机或者指定主机的帐号信息，导出的数据以 xls 表格形式展现。

◆ 全部主机帐户导出：

◆ 指定主机帐户导出：

6. 设备帐户托管

当设备帐户的密码更新周期设置不为 0 时，启用密码托管功能。

启用密码托管功能时，密码更改一次，以后根据设置的时间周期，定期自动修改该帐户的密码。密码更新周期用户可自定义，只要满足“0-999 之间的整数”即可。

对于不同操作系统的设备，对应的托管规则不一致，分为 Linux 或类 Unix 设备（如 Redhat_AS4）、Windows 设备以及网络设备（Cisco、Fortigate、H3C、NetScreen、Topsec）。

1）Linux 或类 Unix 设备托管前提：对应操作系统的 SSO 配置要正确。

- 普通帐户可直接托管（无需添加管理员）；
- 特权帐户：不能托管；

2）Windows 设备托管前提：开启 Windows 设备帐户开关（口令管理\口令管理配置\托管验证）。

3）网络设备支持匿名帐户[null]登录，当设备设置为匿名帐户登录时，不能添加普通帐户。其帐户托管具体规则为：

- 具有管理权限的管理员帐户：可直接托管，匿名帐户[null]不能托管；
- 特权帐户：需存在具有管理权限的管理员帐户；
- 普通帐户：需具有特权帐户。

注：FTP 帐户、VNC 帐户、VDH 帐户以及匿名帐户[null]不能被托管。

启用密码托管，以 Linux 设备 10.10.1.23 的帐户 test 为例，设置密码有效期为 15 天：

保存后，帐户 test 的密码托管显示为“是”，至此完成 test 的设备帐户托管。


Neusoft
东软 NetEye 统一身份管控系统
用户：yufc
安全退出
系统首页
系统管理
运维管理
口令管理
审计管理
运维操作
工具下载
修改密码
口令管理 > 设备帐户管理
密码重置
SSO配置
保管箱管理
全选
删除
添加
帐户获取
帐户导出
帐户有效性检查
设备：
全部设备
查找
帐户名
设备名
IP
帐户类型
密码托管
密码更新周期
登录方式
帐户有效性
状态
操作
admini... 10.10.1.61 10.10.1.61 普通 否 永久有效 口令 激活 编辑 | 删除 | 日志
fox 10.10.1.61 10.10.1.61 FTP 否 永久有效 口令 激活 编辑 | 删除 | 日志
liu 172.16.1.2... 172.16.1.215 普通 否 永久有效 口令 激活 编辑 | 删除 | 日志
root 10.10.1.130 10.10.1.130 普通 否 永久有效 口令 激活 编辑 | 删除 | 日志
sulli 172.16.1.1... 172.16.1.124 普通 否 永久有效 口令 有效 激活 编辑 | 删除 | 日志
test 172.16.1.2... 172.16.1.241 普通 是 15天 口令 激活 编辑 | 删除 | 日志
u913 10.10.1.130 10.10.1.130 普通 是 1天 口令 激活 编辑 | 删除 | 日志
u914 10.10.1.130 10.10.1.130 普通 否 永久有效 口令 激活 编辑 | 删除 | 日志
zouj 10.10.1.130 10.10.1.130 普通 否 永久有效 口令 激活 编辑 | 删除 | 日志

7. 设备帐户密码重置

可以通过密码重置功能对设备帐户的密码进行统一管理，方法如下：

1）点击页面上方的“密码重置”：

2）进入“密码重置”页面，此页面展示的是所有可做重置的设备帐户；

在页面上的主要功能

- ***展现方式：***选择设备帐户的展现方式；
- ***帐户名/IP 地址检索：***对帐户名或 IP 地址进行检索；

- ***帐户名/IP 地址：***勾选需要重置的设备帐户；
- ***密码规则：***“默认”为 NABH 自动生成的 16 位随机密码，“自定义”为用户自己设置的密码；（注意此处自定义密码需符合服务器的密码复杂度设置，否则会失败）

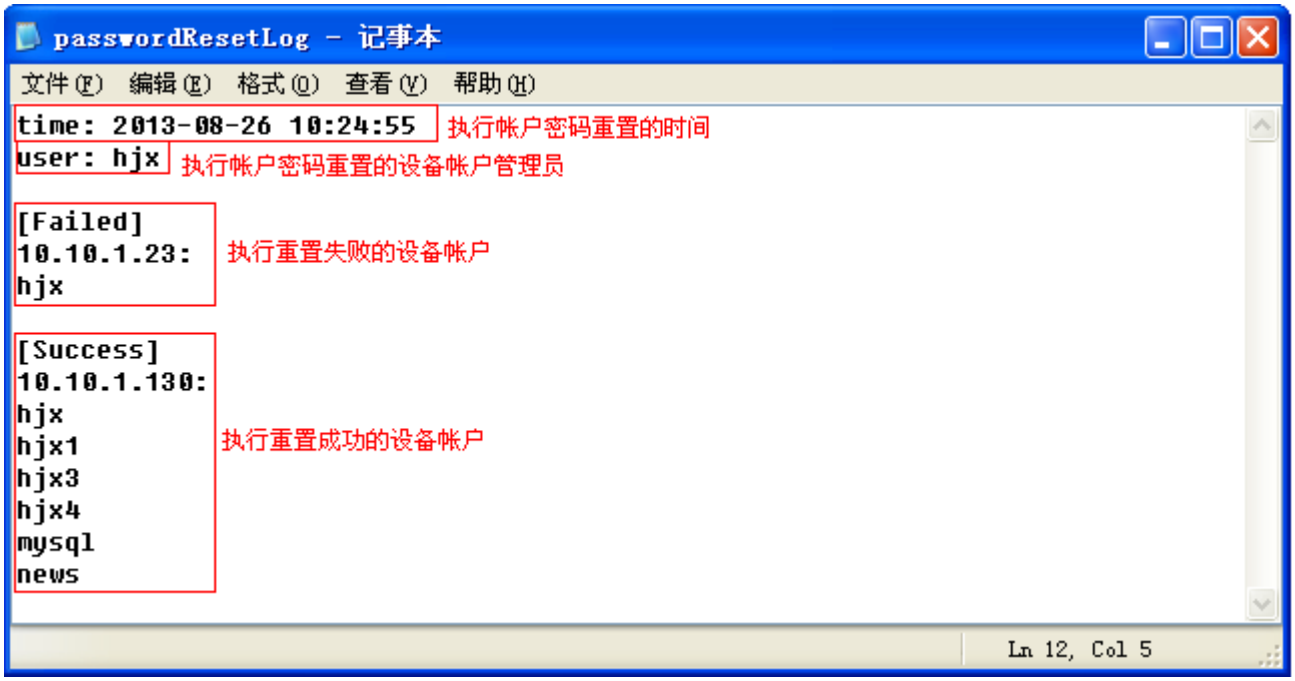
3）选择完帐户后，点击确定即可，即可重置密码；

注：统一设备帐户的隶属设备不能进行密码重置。

4）执行设备帐户密码重置后，密码重置页面增加“日志下载”图标。可通过“日志下载”功能对密码重置的结果进行查看。日志格式为 txt 文件，记录上次一次设备帐户密码重置的结果，具体如下图所示：

点击“日志下载”图标，弹出页面如下图：

保存 passwordResetLog.txt 文件，打开保存的日志文件，页面显示如图：



8. 帐户有效性检查

帐户有效性检测可以检测某一时刻设备账户的有效性，并将检测结果在页面展示，如下图所示：

帐户有效性结果：

空：表示未执行有效性检查；

无效：表示检查结果不通过，可能原因：密码不正确、网络不通等。

有效：表示帐户密码正确。

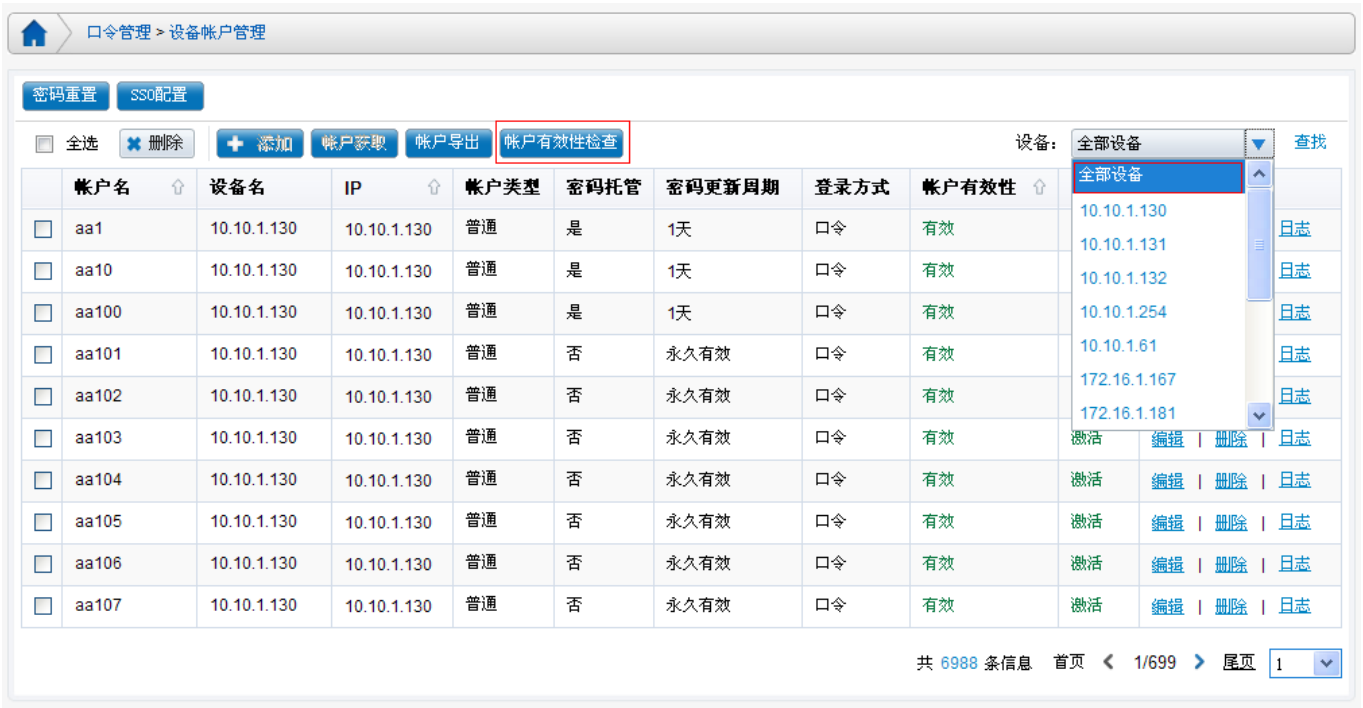
说明：

1、帐户有效性只检查“普通帐户”、“管理帐户”、“FTP 帐户”；

2、对于 windows 帐户，只有开启了“口令管理配置—托管验证”开关，才对其进行检测。

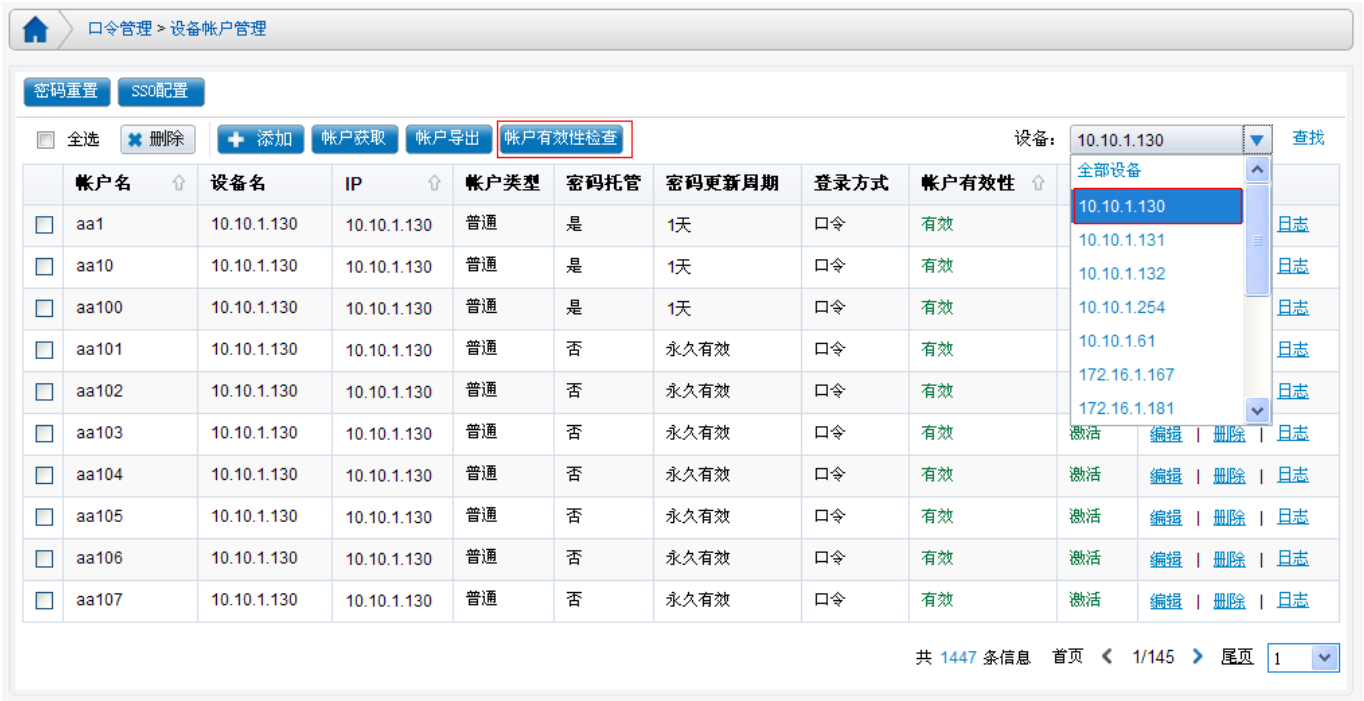
帐户有效性检测提供全部设备、单个设备、全部设备部分帐户、单个设备部分帐户几种检测方式：

1、对全部设备进行检测



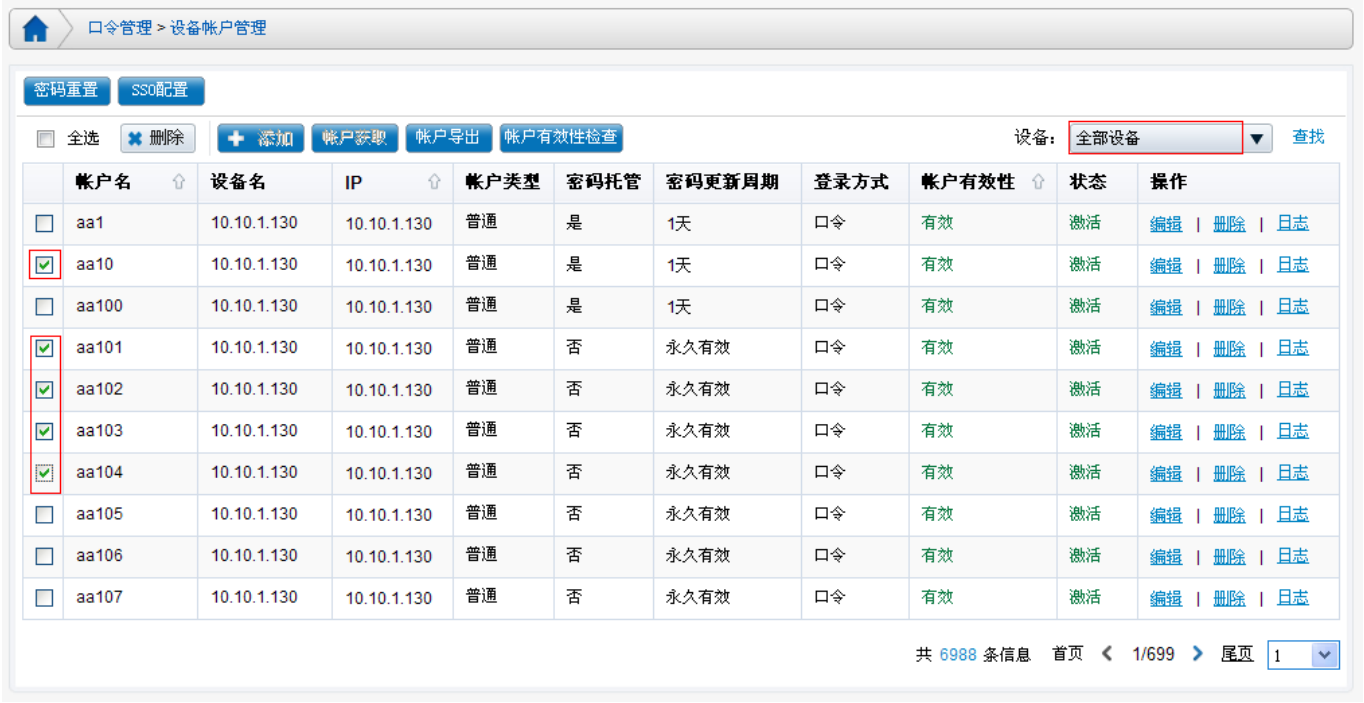
在“口令管理>设备帐户管理”页面，“设备”下拉列表中选择“全部设备”，点击页面上的“帐户有效性检查”，将对全部设备上的所有帐户进行检测。

2、对单个设备进行检测



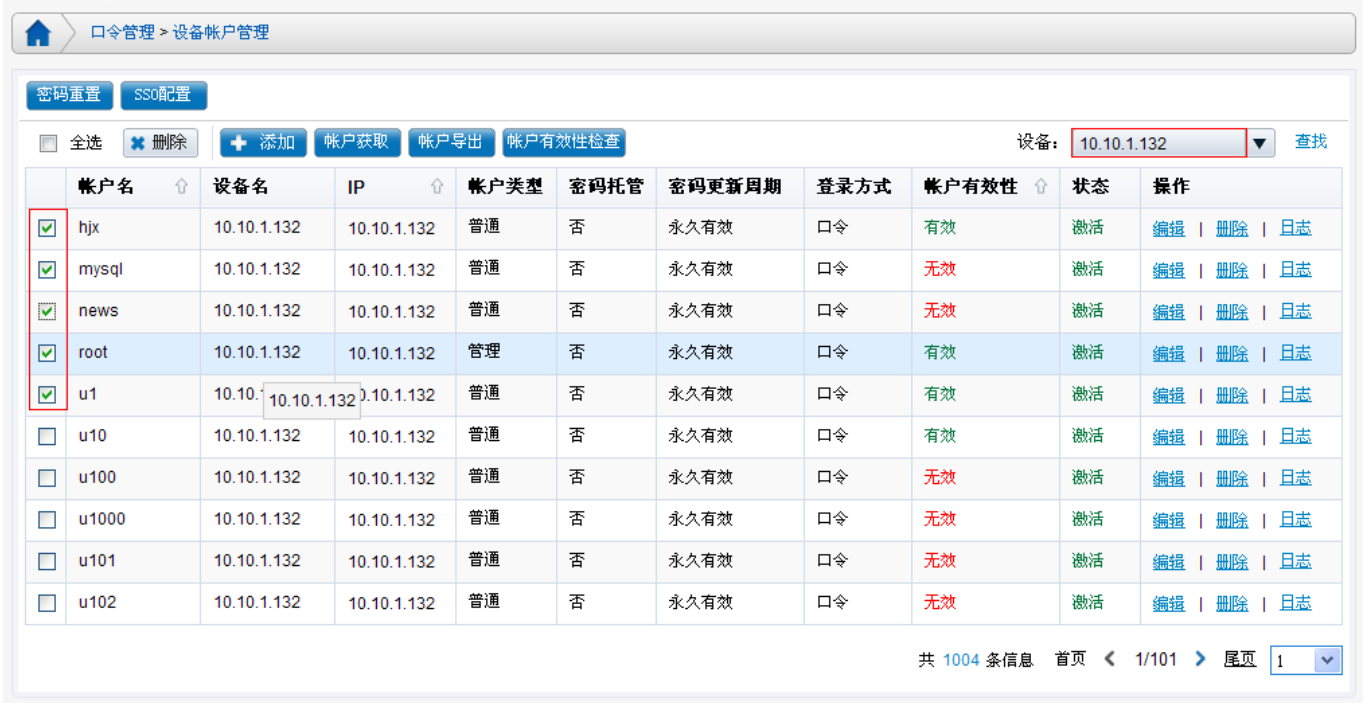
在“口令管理>设备帐户管理”页面，“设备”下拉列表中选择想要检测的设备（此处以10.10.1.130 为例），点击页面上的“帐户有效性检查”，将对指定设备上的所有帐户进行检测。

3、对“全部设备”部分帐户进行检测



可以对全部设备的部分帐户进行检测，方法是在“设备”下拉列表中选择“全部设备”，勾选要检测账户前面的复选框，点击“帐户有效性检测”按钮对选中帐户进行检测。

4、对单个设备部分帐户进行检测



可以对单个设备的部分帐户进行检测，方法是在“设备”下拉列表中选择要检测的设别（如 10.10.1.132），勾选待检测账户前面的复选框，点击“帐户有效性检测”按钮对选中帐

户进行检测。

注意：

1、页面上方的“全选”复选框，仅对当前页生效。勾选“全选”复选框，仅对所选设备**当前页**的设备帐户进行检测。

2、仅支持当前页多选，不支持跨页多选。即勾选某一页上的设备帐户，翻页后上次勾选的帐户自动无效，帐户有效性检测时不予检测。

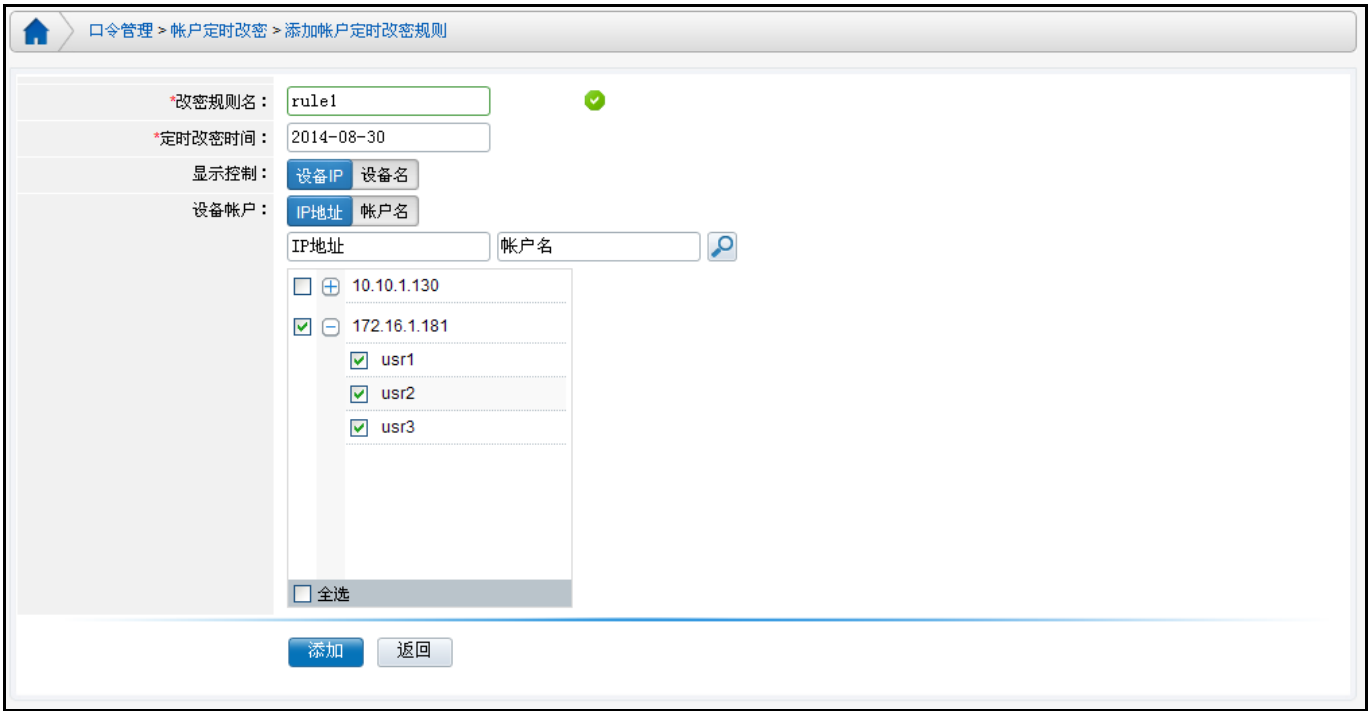
9. 帐户定制改密

帐户定时改密功能可在某个指定日期同时对多个托管帐户进行改密。只能对托管帐户进行定时改密，且统一账户隶属帐户不能设置定时改密。

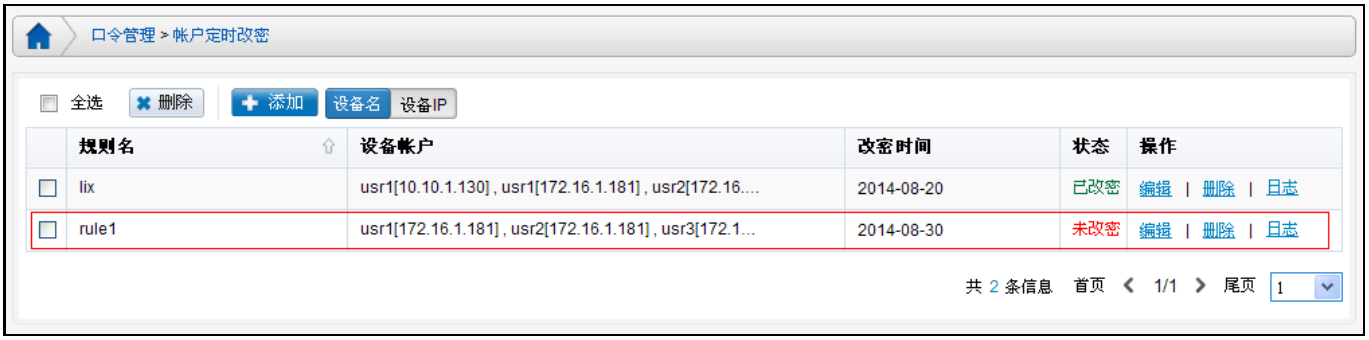
定时改密由定时改密规则进行管理，在定时改密规则中设定改密时间和改密帐户，方法如下：

进入“口令管理>帐户定时改密”页面，点击页面上的“添加”按钮：

在“添加帐户定时改密规则”页面，设定规则名、定时改密时间及要定时改密的设备帐户。



点击页面上的“添加”按钮，添加该规则。在“口令管理->帐户定时改密”页面，可看到刚刚添加的规则，刚添加的规则改密状态为未改密。

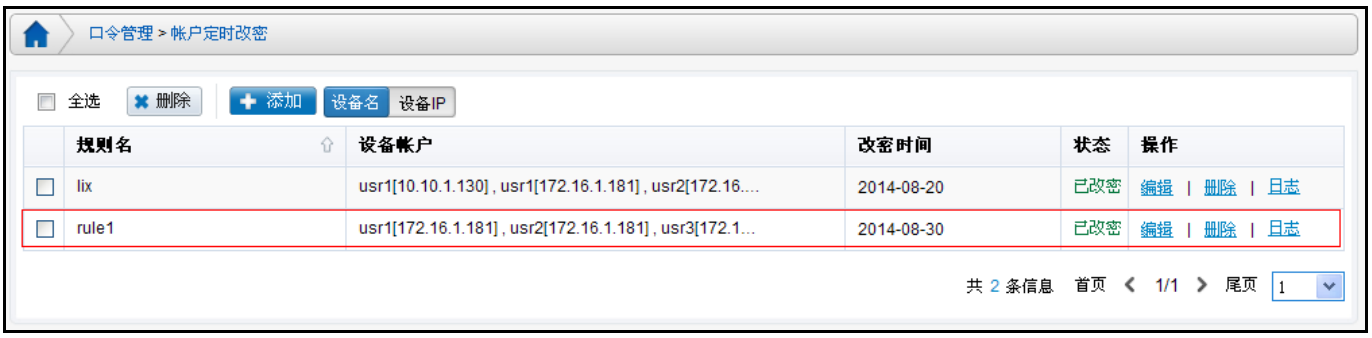


编辑：可编辑定时改密规则；

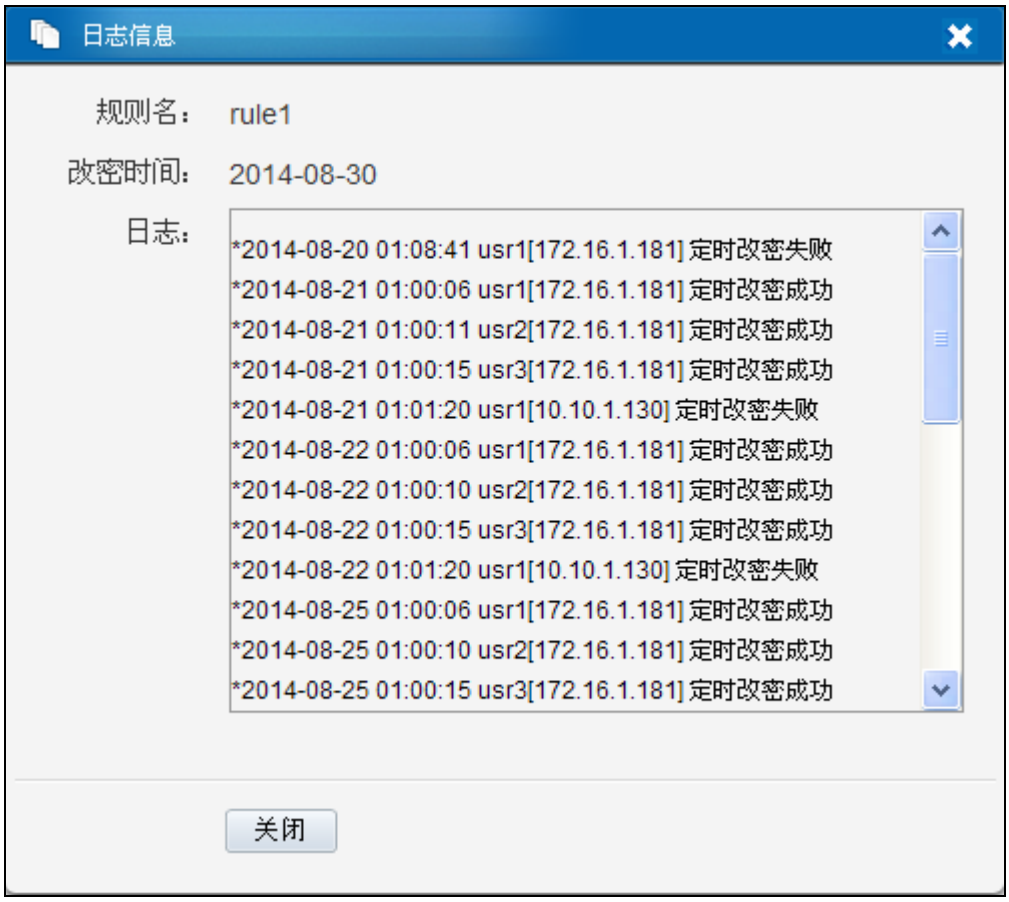
删除：可删除定时改密规则；

日志：记录历史改密信息；

当一条规则到定时改密时间改密后，帐户定时改密页面该规则“状态”显示为“已改密”，如图所示：



点击“日志”按钮，可查看该规则下所有帐户历史改密记录，如图所示：



定时改密规则说明：

1) 凌晨 1 点，会对定时改密帐户进行改密操作；

2) 托管改密时间早于定时改密时间，先托管改密；到定时改密时间后再定时改密。

3) 托管时间晚于定时改密时间，先按定时改密时间改密。

4) 托管时间等于定时改密时间，按定时改密时间改密，等到下次托管到期再托管改密。