东软 NetEye 统一身份管理系统（NABH）

维护手册

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

本手册是 NABH 的维护手册，主要介绍了系统初始化，以及管理员的维护工作。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 约定

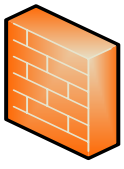
NABH，该产品中文名称为东软 NetEye 统一身份管理系统，英文简称为 NABH。

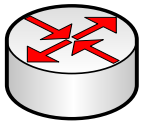
RDP：Remote Desktop Protocol,远程桌面协议，RDP 专门为运行在服务器上的、基于 Windows 的应用程序提供网络连接上的远程显示和输入功能。Windows NT Server 4.0 支持 RDP 4.0，而 Windows 2000 终端服务使用的是 RDP 5.0。但是这两个版本是完全兼容的。我们常使用 Windows Terminal 终端连接远程服务器时就使用该协议。

***SSO*: single Sign-On，单点登录功能。实现用户访问所需资源时无需输入后台设备的用户与密码即可登录系统。

Portal：统一门户登录运维。

另外，本文档中涉及到的网络拓扑图中图标说明如下：

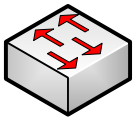

防火墙


路由器


服务器


内部运维人员

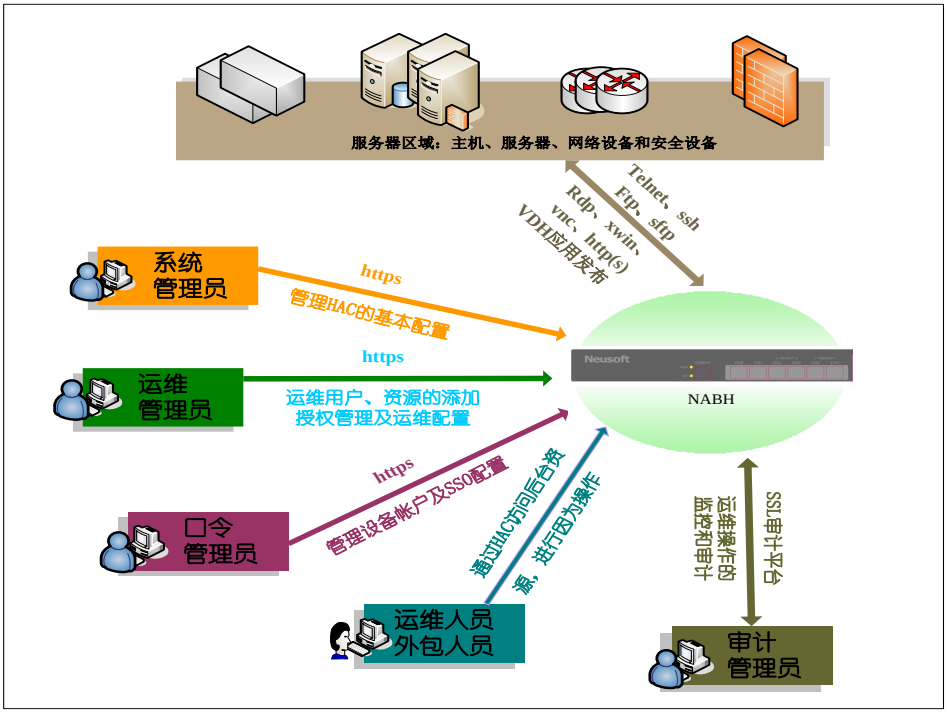

厂商技术支持或外包人员


交换机

2. 产品简介

2.1 系统组成

NABH 系统的组成如下图：



为了保证 NABH 管理安全和只有可信用户才能对后台资源进行运维，NABH 引入两大类用户：NABH 管理员和运维人员。

运维人员是对后台资源进行运维的人员。

NABH 管理员是对 NABH 进行操作，以实现对 NABH 管理、配置及完成审计功能的人员。系统默认四种角色：系统管理员、运维管理员、口令管理员和审计员。系统管理员是对 NABH 设备进行配置和管理人员；运维管理员是配置 NABH，建立运维人员帐户、保护资源及授权等；口令管理员是对后台设备服务器进行配置、管理和维护服务器等；审计员是对运维人员的操作进行审计和 NABH 管理员对 NABH 进行操作的审计。

系统管理员、运维管理员和口令管理员通过 HTTPS 方式访问 NABH 进行操作和配置。

审计员通过 NABH 审计平台软件实施审计。

2.2 工作要求

由于 NABH 实施审计条件是所有对被保护资源的运维流量均需要流经 NABH，所以保证 NABH 工作正常应具备以下要求：

■ 当 NABH 为单臂部署模式时，为了让运维人员访问被保护资源的流量流经 NABH，需要在交换机或安全设备上配置安全策略如访问控制列表，确保运维人员不能直接访问被保护资源，只有 NABH 能访问被保护资源。

■ NABH 能访问保护资源。如果 NABH 到保护资源之间设置了安全策略，需根据所用协议端口开放相关端口。开放端口根据运维协议和保护资源服务端口而定，具体情况如下：

- 采用 Telnet 协议运维：需开放 NABH 到保护资源的 23 端口（23 端口为保护资源 Telnet 服务端口，如果修改请根据实际进行修改，下同）。
- 采用 SSH、SFTP 协议运维：需开放 NABH 到保护资源的 22 端口。
- 采用 FTP 协议运维：需开放 NABH 到保护资源的 21 端口、20 端口和 1024 以上端口（若 FTP 采用主动模式，则只需开放 21、20 端口；若采用被动模式，则需开放 21、1024 以上端口）。
- 采用 RDP 协议运维：需开放 NABH 到保护资源的 3389 端口。
- 采用 XWIN 协议运维：需开放 NABH 到保护资源的 UDP177 端口和 6000 以上端口。
- 采用 VNC 协议运维：需开放 NABH 到保护资源的 5900 以上端口（根据 VNC 服务器的定义，一般为 5900 以上端口）。
- 采用 HTTP 协议运维：需开放 NABH 到保护资源的相应端口。
- 采用 HTTPS 协议运维：需开放 NABH 到保护资源的相应端口。

■ 运维人员能访问 NABH。如果运维人员和 NABH 之间设置安全策略，需根据所用协议端口开放相关端口。具体情况如下：

- 开放 443 端口，目的是运维人员可自行修改密码、查看可访问资源以及进行 RDP、XWIN、VNC 协议运维。
- 采用 Telnet 协议运维：需开放运维终端到 NABH 的 23 端口。
- 采用 SSH、SFTP 协议运维：需开放运维终端到 NABH 的 22 端口。
- 采用 FTP 协议运维：需开放运维终端到 NABH 的 21 端口和 4096 以上端口（4096 以上端口是由 NABH 的工作机制决定的）。
- 采用 RDP 协议运维：需开放运维终端到 NABH 的 3389 和 443 端口。

- 采用 XWIN 协议运维：需开放运维终端到 NABH 的 7000 端口和 443 端口。
- 采用 VNC 协议运维：需开放运维终端到 NABH 的 5900 端口和 443 端口。
- 采用 HTTP、HTTPS 协议运维：需开放 NABH 到保护资源的 7000 和 443 端口。

■ 采用 VDH 进行运维，需开放如下端口：

- 运维终端到 NABH：443、3389、8005 端口；
- NABH 到 VDH 服务器：3389、3390 端口；
- VDH 服务器到保护资源：开放相应端口（该端口是由 VDH 服务器上发布的应用决定的，如发布 http 服务，则需开放 80 端口）

■ 系统管理员、运维管理员终端能访问 NABH，开放端口为 443。

■ 审计员终端能访问 NABH，开放端口为 8001、8004。

■ 审计员终端访问日志备份服务器，进行日志的离线回放，若日志是使用 FTP 协议备份的，需开放 21、1024 以上端口；若是使用 SFTP 协议备份的，需开放 22 端口。

■ NABH 到日志备份服务器，若使用 FTP 协议备份需开放端口：21、1024 以上（采用被动模式）；若使用 SFTP 协议备份，需开放 22 端口。

■ NABH 到发送邮件服务器，需开放相关端口。

■ 总控系统

■ 使用 RDP、XWIN、VNC 协议运维时，客户端操作系统支持 Windows 2000/XP/2003/Vista，浏览器推荐使用支持 IE6、IE7、IE8。

■ 审计平台客户端支持 Windows XP/2003/Vista/7 操作系统。

2.3 浏览器设置

在浏览器中需增加对 NABH 地址的信任（浏览器的安全级别最高支持“中-高”），以及允许 ActiveX 控件的运行。

3. 设备说明

3.1 工作状态

当 NABH 正常加电后，通过面板上各指示灯的状态，可以判断设备的运行情况，其指示灯状态说明见下表：

指示灯名称	指示灯工作状态描述	备注
电源灯	加电后，蓝色	
硬盘灯	黄色（闪烁）或熄灭	启动和读写数据时闪烁，其他情况下处于熄灭状态
网口灯	蓝色（闪烁）或熄灭	网络接通且有数据流量后，该灯为绿色闪烁状态，无数据流量时处于熄灭状态。

3.2 出厂配置

3.2.1 IP 地址

接口名称	IP/Subnet	备注
外网口	192.168.1.100/255.255.255.0	可管理、可提供运维访问服务
内网口	192.168.123.1/255.255.255.0	可管理、可提供运维访问服务
热备口	1.1.1.1/255.255.255.0	可管理
扩展口	空	可管理、可提供运维访问服务

3.2.2 用户名、口令

用户名	口令	管理方式	备注
admin	neteye	WebUI 方式，即 HTTPS	系统内置用户，不可删除，可修改密码。（注意区分大小写）
admin	neteye	Console	系统内置用户，专用于 Console 管理，不可删除，可修改密码。

3.2.3 Console 配置

Console 方式一般是设备在紧急情况或恢复出厂配置时使用，可进行如下工作：

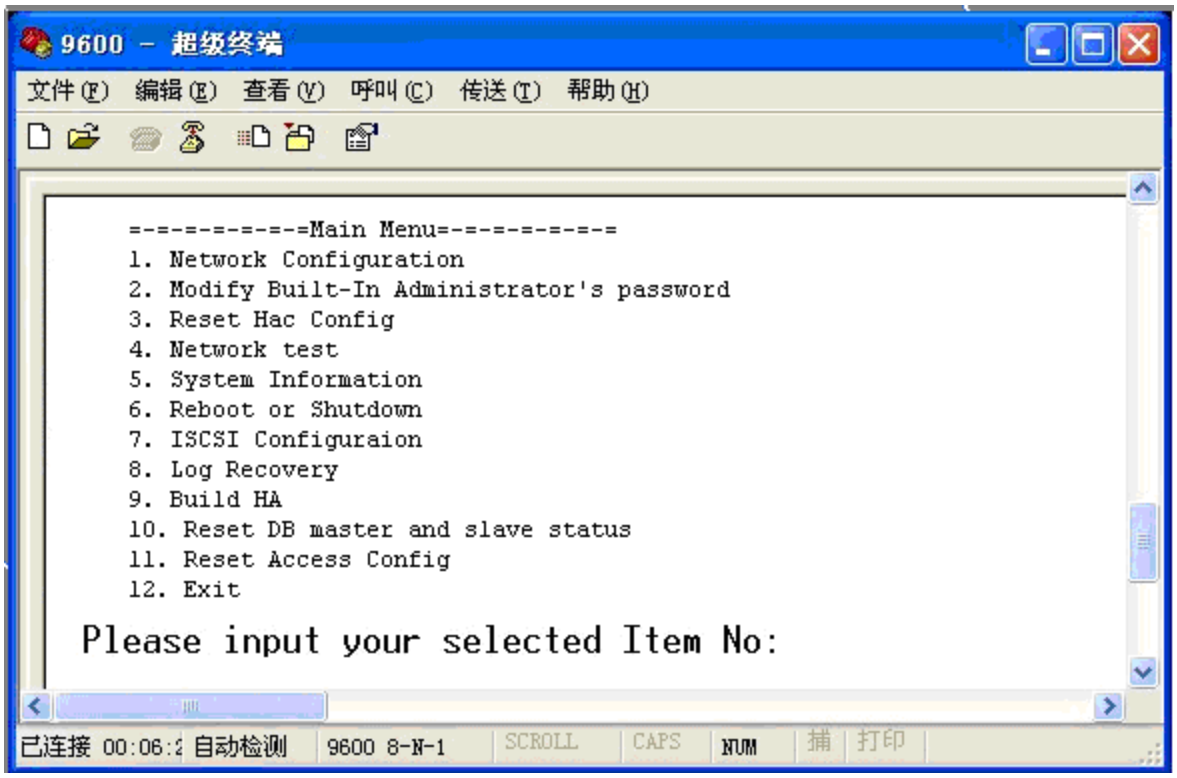
1) 配置网络（内外网地址以及网关）；
2) 修改默认用户 admin 的密码；
3) 恢复出厂（慎用）
4) 测试网络
5) 查看系统信息
6) 重启或关机
7) 外接存储配置
8) 日志恢复
9) 搭建双机
10) 重置数据库状态
11) 清除地址访问控制
12) 退出

注意：使用 Console 口恢复出厂和定义接口 IP 地址后，一定要重启 NABH，否则设置不会生效或者影响其他功能。

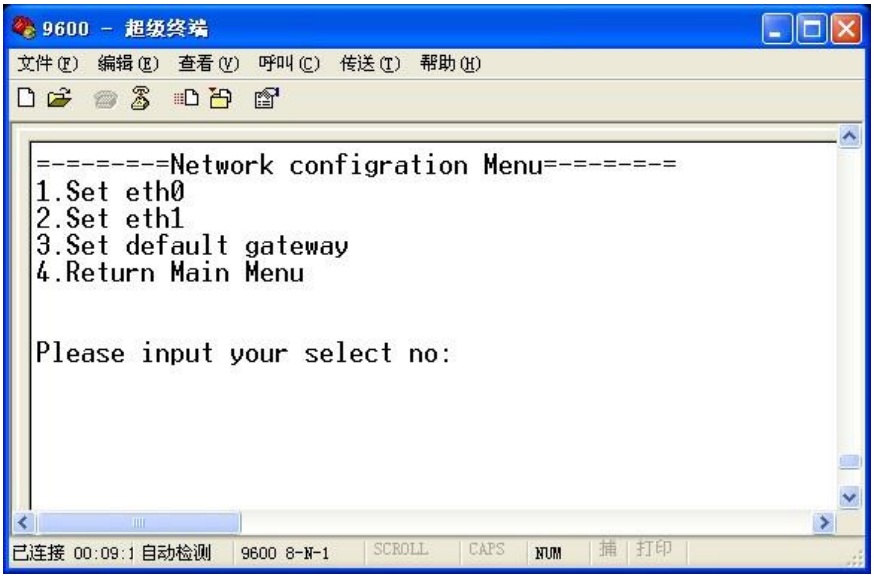
那么，这里 Console 初始化工作主要是修改接口 IP 地址，方法如下：

1) 使用串口线（9 针、公口）连接 NABH 串口；
2) 打开 Windows 自带的超级终端或其他终端仿真软件，设置为：9600，8，0，1 通信参数，如下图：

3） 点击“确定”，出现登录界面，用户名： nabhadmin 密码： ******，回车进入 NABH Console 界面，如下图：



4） 选择 1 选项，修改网口 IP（eth0—外网口，eth1—内网口），出现下图：



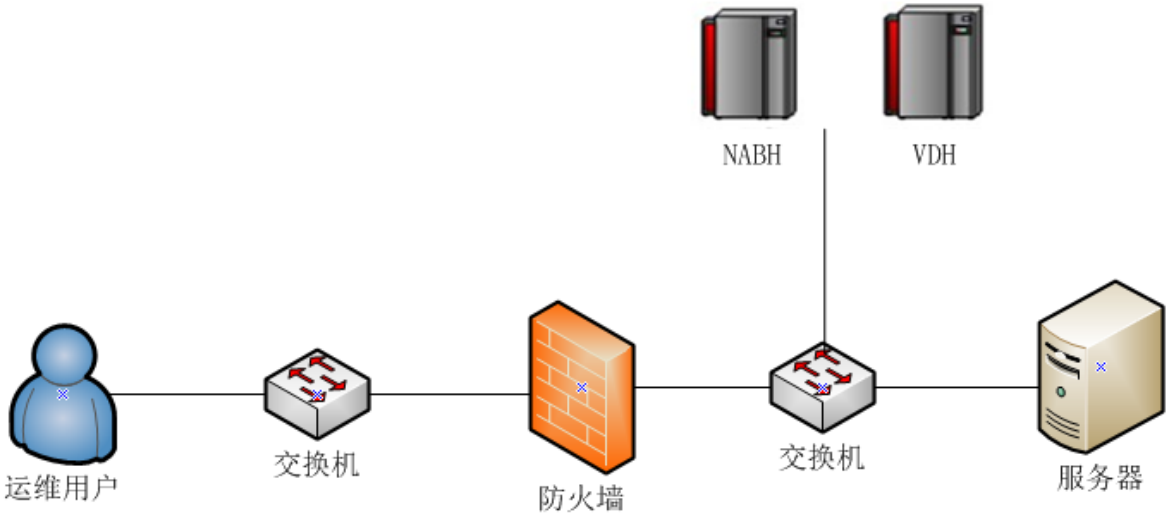
5） 根据实际的 IP 结构，修改 NABH 接口 IP。

4. 准备工作

4.1 确定部署模式

在正式安装配置 NABH 之前，需要确定 NABH 的部署模式，即 NABH 部署为单臂模式还是串联模式。

这一工作决定了 NABH 在网络中的工作位置，同时决定了 NABH 部署是否影响网络结构的变化等。单臂模式拓扑图如下图：



4.2 确定 IP 结构

确定 IP 结构是配置 NABH 最基本的工作，具体内容为：

1） 确定 NABH 的 IP 地址、网关地址；

2） 确定被审计的核心服务器的 IP 地址；

3） 确定 NABH 达到被审计核心服务器、运维终端的路由，保证双向路由可达。

4.3 确定管理员

确定哪些用户为 NABH 系统的管理员，哪些拥有系统管理、运维管理、口令管理以及审计的权限。

5. 初始化配置

初始化配置的主要内容为：设置 NABH IP 地址、网关。

可以采用两种方式：

1） Console 方式：COM 参数为：9600，8，0，1，具体操作见 3.2.3 Console 章节。

2） WebUI 方式管理：登录 https://192.168.1.100；

以下对 GUI 的网络配置方法做详细描述：

5.1 网络配置

设置 NABH IP 地址具体步骤为：

1） 将本地 PC 机的 IP 修改为与 NABH 外网口 IP（192.168.1.100/24）同一网段中的地址；

2） 用直通网线连接 NABH 外网口；

3） NABH 加电开机。

4） 待 NABH 启动完成后，用 IE 浏览器访问：https://192.168.1.100；

5） 访问过程中出现证书安全警告等信息，选择“是”，继续操作，则进入 NABH 管理登录界面：

6） 登录名：admin 密码：****** （注意应勾选口令认证，系统默认登录方式为口令认证），点击“登录”进入 NABH 界面；

7） 选择“系统管理\网络配置”，点击外网口的“编辑”，将外网口 IP 修改为用户规划的 IP，如：192.168.1.1/255.255.255.0，然后“保存”即可。由于 IP 即时生效，网络会中断；

8） 将本地 PC 机的 IP 修改为新网段内的 IP 地址，如：192.168.1.14/255.255.255.0，重新按照上述步骤登录（记住：此时 NABH 登录地址为修改后的新 IP 地址）；

9） 同理按照上述操作将内网口地址、网关地址、DNS 地址修改或添加上。

网络设置是设备正常工作运行最基本的配置工作，主要配置内容为：

- 外、内网口地址
- 热备口地址：此网口在双机热备时，要进行配置。具体配置见“双机热备”相关章节。
- 扩展网口：根据实际网口数量自动控制 NABH 页面扩展网口数量
- 默认网关
- 首选 DNS
- 备选 DNS

若为单臂部署模式时，仅设置缺省网关即可；若为串联方式时，一般需要添加相应达到核心服务器、运维终端的路由。

5.2 配置路由

实际网络环境中，如果还需要配置静态路由，则参考此章节。

步骤如下：

1） 选择“系统管理\网络配置”，点击“静态路由表”，出现如下配置界面：

2） 点击“添加”按钮，添加一条静态路由，如下界面：

- 类型：net、host，分别表示添加的路由是一个网段路由或主机路由；
- 目标网段/目标主机：输入目标网络地址或目标主机地址；

- 掩码：即与目标网段/目标主机相对应的掩码；
- 网关：即下一跳地址。

点击“添加”即可完成该路由的添加。

如，添加一条到达 10.10.1.0/255.255.255.0 的路由，下一跳地址为：172.16.6.254，配置如下图，点击“添加”完成静态路由表的添加：

3） 点击“查看核心路由表”，可以查看目前设备中当前配置的路由，如下图：

目标网段/目标主机	掩码	网关	网卡	标志
10.10.1.0	255.255.255.0	10.10.1.254	eth0	UG
10.10.1.0	255.255.255.0	0.0.0.0	eth0	U
1.1.1.0	255.255.255.0	0.0.0.0	eth2	U
192.168.123.0	255.255.255.0	0.0.0.0	eth1	U
169.254.0.0	255.255.0.0	0.0.0.0	eth2	U
0.0.0.0	0.0.0.0	10.10.1.254	eth0	UG

标志说明：U—直连路由，UG—静态路由等。

5.3 DNS 配置

NABH 提供的 DNS 功能支持域名解析，如果需要考虑使用邮件报警功能时需要配置相应 DNS，包含首选 DNS 和备选 DNS，配置如下：

说明：“全局配置”项中的“NTP 配置”和 “邮件服务器”配置为域名格式时，必须设置 DNS，如果直接配置为 IP 形式则无需设置 DNS。

5.4 PING 功能

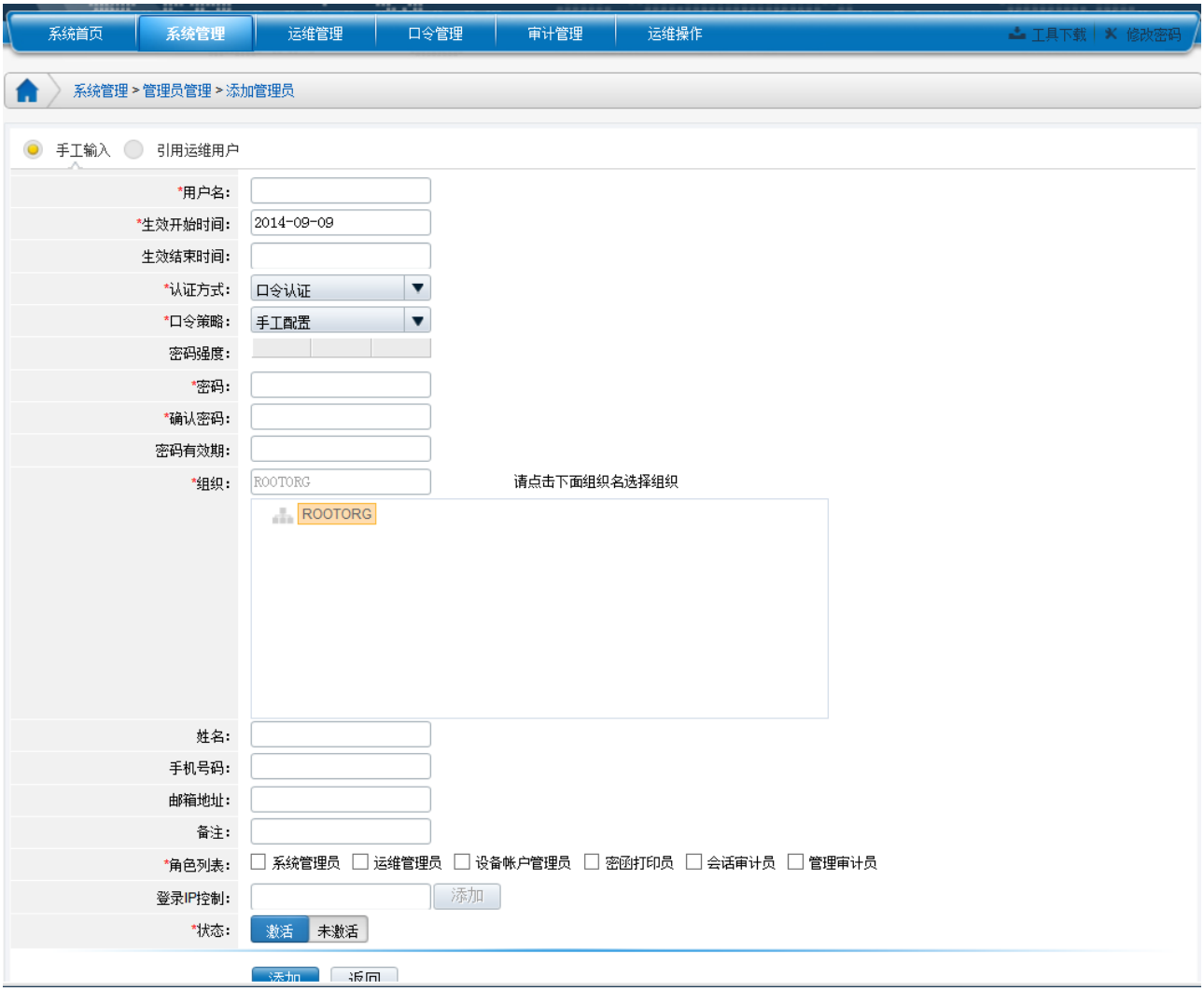
NABH 提供的 ping 功能，可对网络的连通状况进行简单的测试。

NABH 的初始管理员帐户为

admin（超级管理员），该帐户拥有基本的系统管理功能，可配置网络、管理员初始化、重置密码等工作。在系统使用过程中，需要按实际情况另行创建管理员。本章节将讲述管理员的创建过程。

5.5 配置管理员

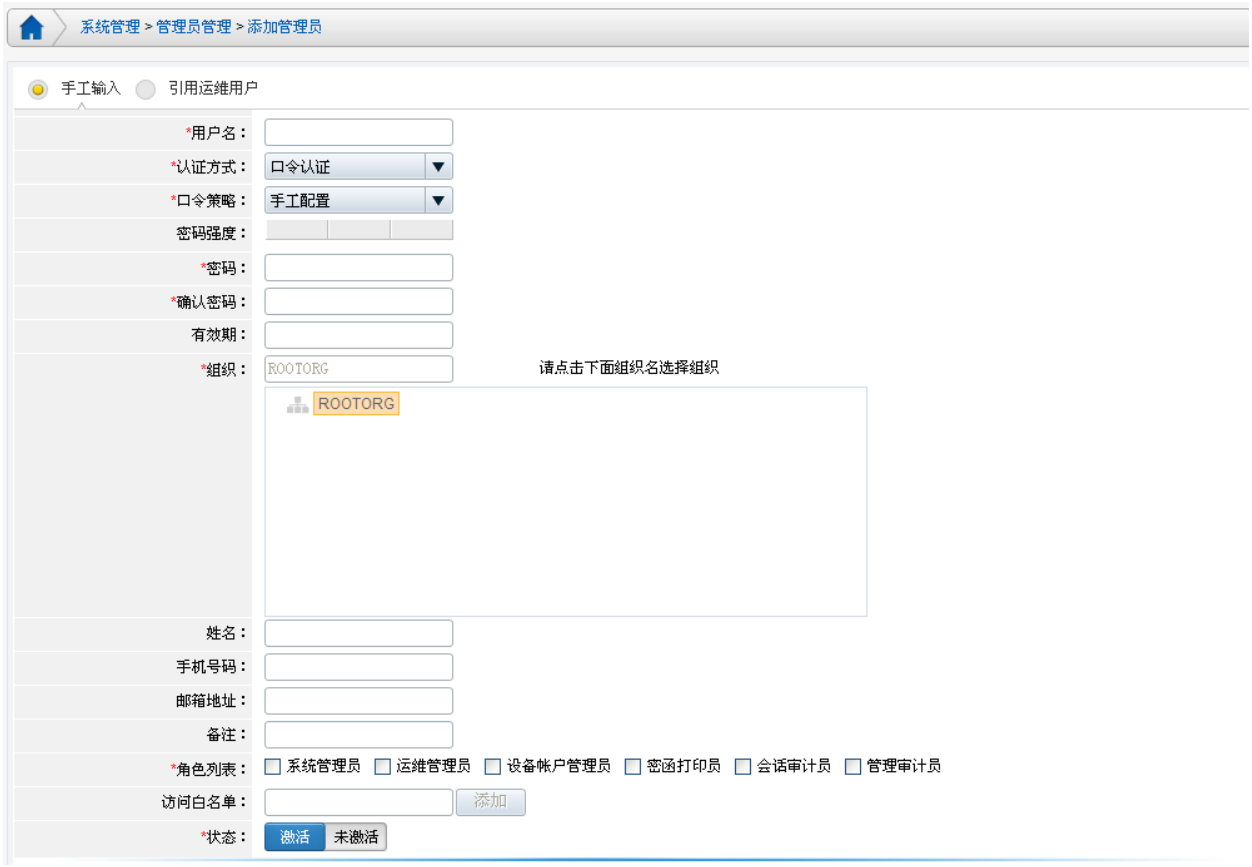
选择“系统管理/管理员管理”，点击“添加”按钮，进入添加管理员界面，如下图：



添加管理员有两种方式，分别为手工输入和引用运维用户。

- 手工输入：用户自行创建一个新的管理员；
- 引用运维用户：在已有运维用户中选择一个或若干个运维用户，将其赋予管理员权限。

进入添加管理员界面后，选中“手工输入”，界面如下：



用户名：输入用户名称；[必选项]

认证方式：包括口令认证、AD 域认证、LDAP 认证、Radius 认证、令牌认证和证书认证六种认证方式，默认为口令认证；

下面以添加口令认证为例：

当认证方式为口令认证时，页面如上图所示，有口令策略、密码强度、密码、确认密码等项需要设置。

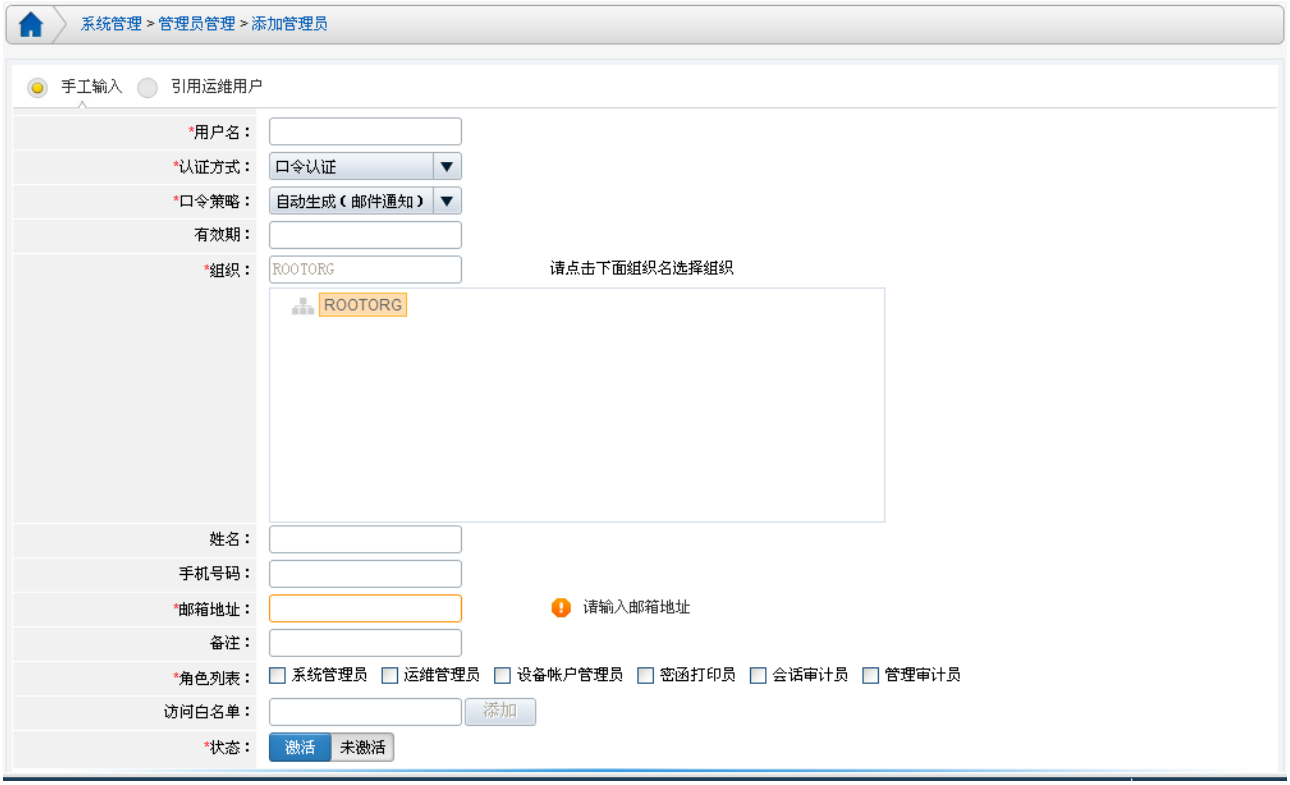
口令策略：包括手工配置口令和自动生成（邮件通知）口令；

手工配置密码可以直接在下面的密码、确认密码框中输入用户密码；

密码强度：系统会根据密码强度规则自动检测用户输入密码的安全强度，密码强度的设置由“系统管理/全局配置/口令复杂度”决定。

密码/确认密码：不限字符，但不能设置空格键；[必选项]

自动生成密码，要求“邮箱地址”为必填项，系统生成的密码发到该邮箱地址中。页面显示如下：



可以用“引用运维用户”的方式添加管理员，即为运维用户赋予管理员的权限。

有效期：可自定义密码的有效期；0或不填，表示没有有效期；

姓名：输入对应登录名的真实姓名，不限字符；[选填项]

手机号码：即管理员的手机号码；[可选项]

邮箱地址：即管理员的邮箱地址，当管理员的配置信息有变更时，系统会通过邮件方式通知管理员；[可选项]

备注：主要是作为描述该用户的附加注释信息；[可选项]

角色列表：为新增的管理员分配角色；[必选项] NABH 中角色划分为 5 个独立部分：

“系统管理员”拥有系统管理导航栏中对应的所有功能；

“运维管理员”拥有运维管理导航栏中对应的所有功能；

“设备帐户管理员”拥有“口令管理”导航栏中对应的的所有功能；

“密函打印员”可登陆密函打印客户端进行密函打印申请；

“会话审计员”拥有（B/S 审计）“审计管理”中与会话相关的所有功能；

“管理审计员”拥有（B/S 审计）“审计管理”中管理审计的功能；

以上角色可多选；

访问白名单：此处设置管理员能在某 IP 地址，或某地址段内登录。支持多个地址。

状态：激活或未激活。未激活则不可使用该帐户登录。

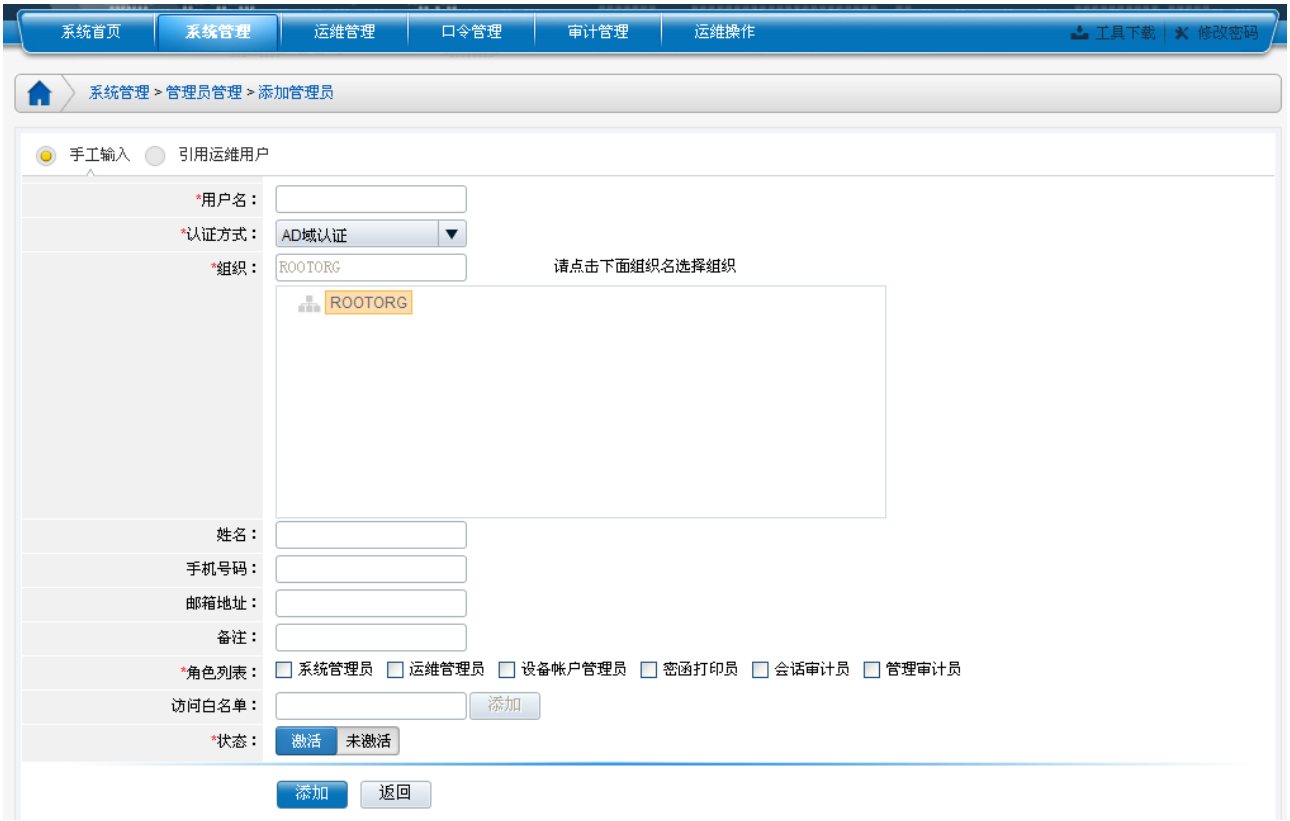
其他认证管理员

✓ 创建 AD 域认证、LDAP 认证、Radius 认证管理员：

为了能使这三类认证方式的管理员能正常使用，首先要配置外部认证，具体见 3.2.3 章节。

下面以 AD 域认证方式管理员为例，其他两种类似：

进入“系统管理/管理员管理/添加管理员”，



各个配置项规则同口令认证管理员。

✓ 创建令牌认证管理员

为了能使令牌认证的管理员正常使用，要使用到动态令牌，具体使用参见《东软 NetEye 统一身份管理系统（NABH）动态令牌使用手册》。

✓ 创建证书认证管理员

为了能使证书认证的管理员正常使用，需要使用到飞天 key，具体参见《东软 NetEye 统一身份管理系统（NABH）飞天 key 使用手册》。

进入“系统管理/管理员管理/添加管理员”，

其中证书 CN 为必填项，并要对证书的有效期进行设置，其他设置同口令认证。

6. 外部认证

NABH 的外部认证支持 LDAP 认证、AD 域认证、Radius 认证和令牌认证。第三方认证既可支持管理员，又可支持运维用户。选择“系统管理/外部认证”，点击“添加”即可进行认证服务器的配置。NABH 支持 RSA 的双机，因此列表中有两个 Radius 服务器。

LDAP 服务器：

添加 LDAP 认证服务器，

服务器名：可任意定义；（必填项）

IP 地址：LDAP 认证服务器的 IP 地址；（必填项）

端口：LDAP 服务器的服务端口；（必填项）

管理员 DN：即 LDAP 认证服务器管理员的 DN；

管理员密码：即 LDAP 认证服务器管理员的密码；

查询基准 DN、合法用户对象类型、用户名字段名称、用户认证字段名称：根据 LDAP 认证服务器的参数进行配置；（必填项）

帐户同步策略：帐户同步操作是将 LDAP 认证服务器上指定查询基准 DN 下的帐户同步到 NABH 用户列表。同步策略是指在进行帐户同步时，对 NABH 上存在而 LDAP 服务器上不存在的 LDAP 认证帐户所采取的动作策略。包括：

1） 不执行任何操作：对这样的帐户不采取任何动作；

2） 设置帐户为未激活：将这样的帐户设置为未激活状态；

3） 删除此帐户：删除这样的帐户；

帐户自动同步：即是否启用帐户自动同步；

同步周期：设置帐户自动同步的时间周期；

激活状态：可选择是否激活服务器；（必填项）

建议：在配置完 LDAP 服务器后，进行一次帐户同步操作。

AD 域服务器

添加 AD 域认证服务器：

服务器名：该 AD 域的域名；（必填项）

IP 地址：AD 域服务器的 IP 地址；（必填项）

端口：AD 域服务器的服务端口，一般默认是 389；（必填项）

激活状态：可选择是否激活服务器；（必填项）

管理员：即 AD 域服务器的管理员名称

管理员 DN：即 AD 认证服务器管理员的 DN；

帐户同步策略：帐户同步操作是将 AD 认证服务器上指定查询基准 DN 下的帐户同步到 NABH 用户列表中。同步策略是指在进行帐户同步时，对 NABH 上存在而 AD 服务器上不存在的 AD 认证帐户所采取的动作策略。包括：

4) 不执行任何操作：对这样的帐户不采取任何动作；

5) 设置帐户为未激活：将这样的帐户设置为未激活状态；

6) 删除此帐户：删除这样的帐户；

帐户自动同步：即是否启用帐户自动同步；

同步周期：设置帐户自动同步的时间周期；

激活状态：可选择是否激活服务器；（必填项）

建议：在配置完 AD 域服务器后，进行一次帐户同步操作。

Radius 服务器

添加 Radius 服务器：

IP 地址：Radius 服务器的 IP 地址；（必填项）

端口：Radius 服务器的服务端口，默认用 1812；（必填项）

共享密钥：服务器上面所设置的密钥，即 Secret 值；（必填项）

激活状态：可以选择是否激活服务器。（必填项）

7. 全局配置

7.1 基本配置

配置项	描述	当前值	操作
系统时间	配置当前系统日期和时间。	2013-07-10 10:47:21	编辑
NTP配置	自动与NTP时间服务器同步系统时间（同步后系统时间不可编辑）。	关闭	编辑
口令复杂度	设置管理员、普通用户口令复杂度。	低级	编辑
提示修改密码的提前天数	开始提醒密码将要到期的天数，以所填数值为准。	7	编辑
强制修改密码的提前天数	密码到期前强制修改密码的天数，以密码到期时间往前推算。	0	编辑
强制修改密码的延后天数	密码到期后强制修改密码的天数，以密码到期时间往后推算。	0	编辑
容量告警	设置日志存储空间不足时告警，单位为G。	未设置	编辑
页面超时	配置页面空闲超时时间，单位为分钟。	100	编辑
每页最大记录数	设置数据信息每页最大行数。	10	编辑
审计服务端口	设置审计服务端监听端口。	8001	编辑
邮件服务器	配置邮件服务器参数。	smtp.qiye.163.com	编辑
调试服务	开启SSH调试服务（端口222），在紧急情况下便于系统维护和排障。默认为关闭。	启用	编辑
SNMP服务	开启此服务可获取HAC系统设备信息。	禁用	编辑
SNMP团体名	设置SNMP访问团体名。	public	编辑

- ***系统时间***：设备 NABH 设备系统时间，格式为：YYYY-MM-DD HH:MM:SS，全部为数字，高位补零。默认为系统硬件时钟时间。如：2010-03-02 11:20:35；
- ***NTP 配置***：不编辑此选项，则系统时间可以手动设置；编辑此选项后，将在下方文本输入框，输入 NTP 地址，保存后则以 NTP 服务器的时间为准，系统时间一项则置为灰色，不允许手动修改；
- ***口令复杂度***：用来控制 NABH 管理员密码和运维用户密码的复杂度，分为低、中、高三种，密码为 6-16 位；
  - ✓ 低级：复杂度无要求，密码默认为 6 位；
  - ✓ 中级：需要至少包含字母、数字和特殊字符中的两种，密码默认为 7 位；
  - ✓ 高级：需要包含字母、数字和特殊字符，密码默认为 8 位；
- ***提示修改密码的提前天数***：用户密码到期的前 X 天起，用户登录时提示密码会到期，默认是 7 天；如下例

- ***强制修改密码的提前天数***：用户密码到期的前 M 天要求修改密码，用户可跳过，默认是 0 天；

- ***强制修改密码的延后天数***：用户密码到期后，还可以继续使用原密码 X 天，但也要求修改密码，默认是 0 天；
- ***容量告警***：设置告警阀值，当日志区剩余容量到达设定数值时，单位为 G。当达到告警的数值时，系统管理员登录配置平台后，将会在当前窗口弹出醒目的告警消息；

- ***页面超时***：页面空闲超时时间，以分为单位，如果 GUI 登录的空闲时间超过了设定的时间，将退出至登录界面。
- ***每页最大记录数***：设置 NABH 配置页面中，每页最多显示的信息条目数量，默认为 10 条；
- ***审计服务端口***：该端口是审计平台的登录端口，用户可以自定义，默认是 8001；
- ***邮件服务器***：配置邮件服务器功能。设置发送邮件服务器，格式如：smtp.163.com；然后添加用户名和密码即可完成，如果需要身份验证，请勾选“发送身份验证”，通过点击“测试”来查看邮箱是否可用，测试成功后，会有成功提示，并且测试邮箱将收到一封测试邮件。
- ***调试服务***：设置是否开启 SSH 调试服务（端口 222），在紧急情况下便于系统维护和排障。默认为关闭。
- ***SNMP 服务***：开启此服务可获取 NABH 系统设备信息。默认关闭。
- ***SNMP 团体名***：可以设置 SNMP 访问团体名。
- ***双重认证***：配置双重认证的方式。如下图所示：

添加双重认证：勾选任意两种认证方式，点击“添加”，添加完需要的认证方式后，点击“确定”按钮，则添加对应的双重认证类型；添加管理员/用户时，“认证类型”列表中出现对应的认证类型可供选择。

删除双重认证：点击已添加的双重认证类型，则去掉复选框的勾选状态，点击“确定”，则删除对应的双重认证类型。若已存在对应类型的用户，则无法删除此认证类型。

三方运维方式时，双重认证方式登陆，需注意：1、两个密码之间采用#分割，并且密码中不能含有#号；2、密码输入顺序，与添加的“双重认证”组成顺序一致，如“口令+内置令牌”，三方运维时，密码输入方式为：口令+内置令牌。

-

7.2CA 证书

用户可自行配置 NABH 的 CA 证书，CA 证书模块中，包含三个功能：

- ***证书查看***。可查看 NABH 的 CA 根证书；

- ***证书导入***。可将已经存在的证书文件和证书私钥文件直接导入 NABH 中；
- ***颁发证书***。NABH 可自定义颁发 CA 证书。

证书查看：

可查看 CA 根证书的相关内容。

证书导入：

- ***证书文件***：点击“浏览”按钮，将弹出文件选择对话框，用来导入证书文件。
- ***证书私钥文件***：点击“浏览”按钮，将弹出文件选择对话框，用来导入证书私钥文件。
- ***证书私钥加密***：勾选此选项，则出现新的一行，要求输入证书私钥的口令。

颁发证书：

NABH 可自定义颁发 CA 证书，其中公用名、邮箱地址和证书有效期是必填项。

7.3 服务器证书

用户可自行配置 NABH 的 SSL 证书。服务器证书模块中，共包含四个功能：

- ***证书导入***。可将已经存在的证书文件和证书私钥文件直接导入 NABH 中；
- ***创建证书申请***。可通过 NABH 创建证书申请；
- ***完成证书申请***。使用创建的证书申请，在可信的 CA 中申请证书后，导入到 NABH 中；
- ***自签发证书***。NABH 可自定义签发服务器证书。

证书导入：

证书文件：点击“浏览”按钮，将弹出文件选择对话框，用来导入证书文件。

证书私钥文件：点击“浏览”按钮，将弹出文件选择对话框，用来导入证书私钥文件。

证书私钥加密：勾选此选项，则出现新的一行，要求输入证书私钥的口令。

创建证书申请：

填写证书申请的各项参数。其中公用名和邮箱地址是必填项。

完成证书申请：

使用创建的证书申请，在可信的 CA 中签发证书后，导入到 NABH 中。

自签发证书：

导入和自签发证书后，需重启后生效。

7.4SYSLOG 外发

添加外发服务器，点击“添加”：

服务器地址：即接收系统日志的服务器；

端口：日志服务器在接收系统日志时使用的端口；

协议类型：发送系统日志时使用的协议，包括 TCP 和 UDP 两种；

日志类型：操作系统日志——即 Linux 系统日志

NABH 日志——NABH 应用系统的日志；

日志级别：需要发送的日志的级别，包括：通知消息、警告消息、错误消息、紧急情况。

注：可添加多个 syslog 外发服务器。

7.5 地址控制

通过地址控制模块的设置，可按照 IP 地址、地址段（IP/Mask）和 MAC 地址三种方式控制对 NABH 的允许访问或禁止访问（管理以及运维）。此功能仅赋予根系统管理员。

具体实现页面如下：

功能状态：

开启，则地址控制列表中的策略均可生效；

关闭，则地址控制列表中的策略均不生效；

默认访问策略：

允许，则地址控制列表以外的其他主机允许访问 NABH；

禁止，则其他主机禁止访问 NABH。当“功能状态”开启后才允许选择“禁止”状态；

快速查找：可通过输入 IP、网段、MAC 地址进行模糊检索；

7.5.1 添加地址控制策略

点击页面“添加”按钮，则弹出如图所示的界面：

类型：包含 IP、网段（格式如：172.16.2.0/255.255.255.255、172.16.2.0/22）、MAC 三种类型；

地址：根据选择的类型，输入对应的地址；

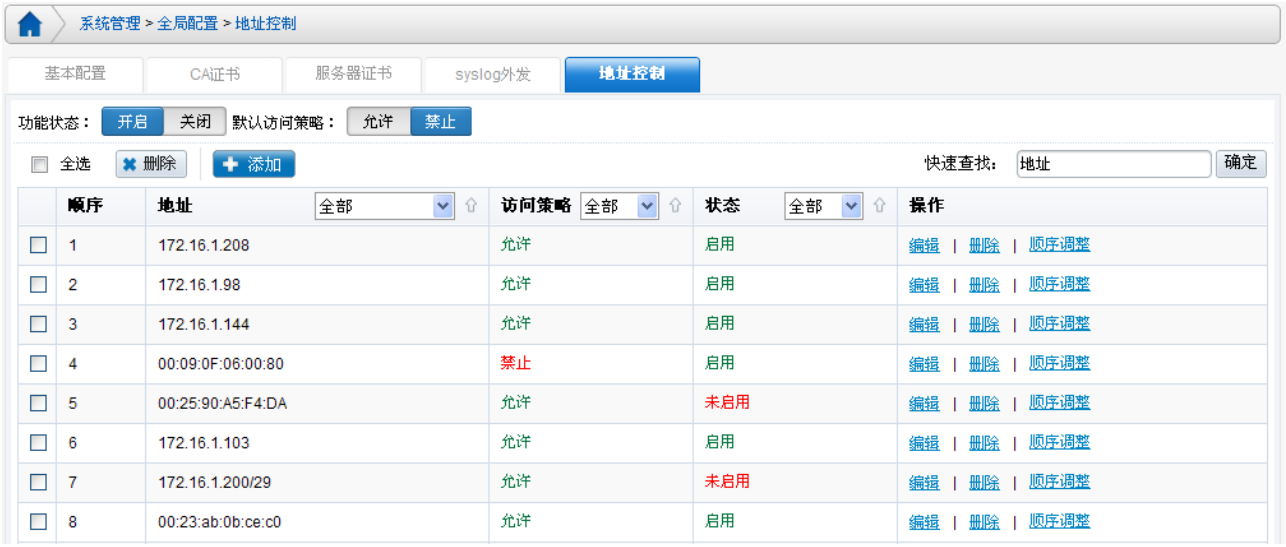
访问策略：定义输入地址对 NABH 的访问策略，允许或禁止；

是否启用：启用，则此地址控制策略生效；禁止：则此地址控制策略不生效；

顺序：末尾，则此策略添加到最尾端；顶部，则此控制策略添加到第一条；自定义，则可自定义此策略的顺序号；

注：地址访问策略按照“顺序”号小的优先生效。如：同一主机存在多种不同的控制策略，“顺序”号小的生效。

添加后的地址访问控制页面，列表显示如图所示：



7.5.2 编辑地址控制策略

点击列表中的“编辑”按钮，显示页面如图所示，可对策略的地址、访问策略和状态进行编辑。

通过列表中的“顺序调整”编辑此策略的“顺序”号，可对编辑的策略向前或者向后调整位置，如图所示：

如上图所示，“顺序”号为 2 的策略调整到 4 后，则原来的顺序号 3、4 向前顺移一位，变为 2、3，其他的策略顺序号不变。对应的地址策略根据移位后的顺序号进行过滤。

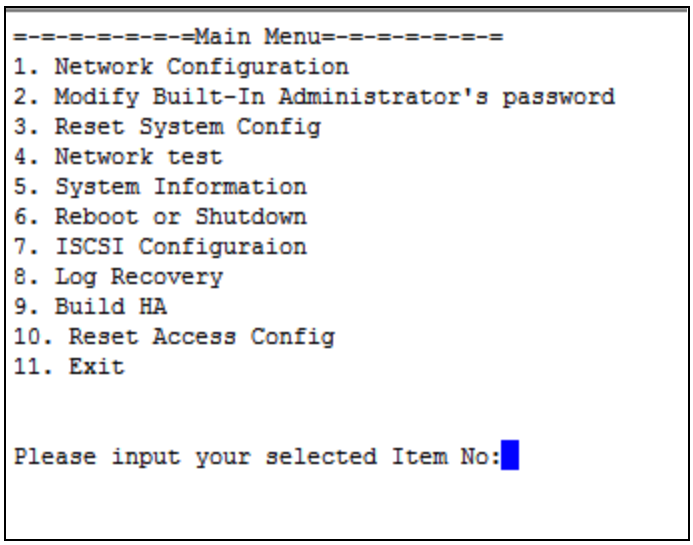
7.5.3 删除地址控制策略

点击列表中的“删除”按钮，进行删除操作；也可选择多条记录，进行批量删除操作，如图所示：

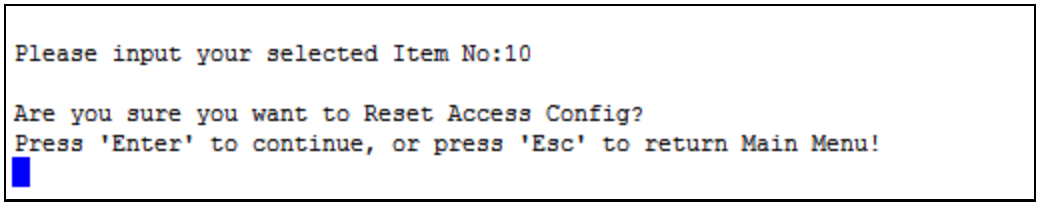
7.5.4 清除地址控制策略

当访问控制策略配置误操作，可通过 Console 做应急处理，见如下。

1、打开 console 口，具体操作见 3.2.3 节，界面如图所示：



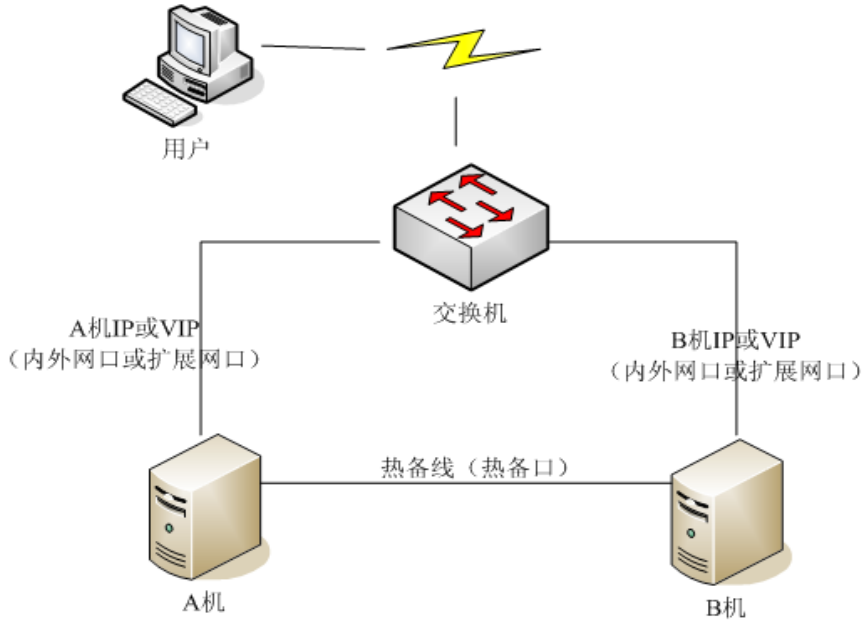
2、选择第 10 项，则弹出如图所示界面：



3、执行“回车”，则可完成清除地址控制策略功能。

8. 双机热备

“双机热备”是 NABH 提供设备高可用性，保障业务连续运行的一个重要功能。双机环境的部署由厂商技术人员来完成，具体网络结构图如下所示：



具体搭建方式参考相关文档，以下仅对功能做简单描述：

“系统管理\双机热备”，点击“双机配置”，出现如下界面：

双机热备状态：设备双机热备的开关；

监听网口：即双机热备切换监听的网口；可监听一个，也可同时监听内、外网口，或扩展网口；

热备对端 IP：即用于检查设备健康状态而发送心跳信号的 HA 网口的对端设备热备网口 IP 地址；热备 IP 地址大（例如：1.1.1.2）的为主机，地址小（例如：1.1.1.1）的为备机；

网卡 IP：指定一个内、外或者扩展网卡的 IP；

VIP 地址：可对指定网卡 IP 添加一个虚 IP，要求与指定网卡属于同一网段；

注：搭建双机时，需要保证防火墙上开放对 NABH 主、备机的实 IP 地址、虚 IP 到服务器端的访问；

双机热备的状态有四种：Active、Standby、Failure、Init。分别表示：主机工作状态，备机等待状态，双机状态错误、初始化（通常设备为重启状态）。

以下是双机热备状态下，主机工作的图例：

9. 日志维护

NABH 安全审计系统随着日积月累的运维，硬盘上会存储着大量的日志文件，硬盘的可用空间将会越来越小，以及面临硬件的老化问题，所以有必要对日志文件进行备份、转移。系统提供了日志维护功能，可以进行日志备份，包括：日志自动和手动备份。日志维护包括日志状态、日志备份、日志文件删除 3 项内容。

建议用户做定期备份，以及日志文件删除。尤其是当硬盘空间显示即将占满时，需做日志文件删除，否则有可能会导致无法登录、运维的情况。

9.1 日志备份

9.1.1 服务器配置

要进行日志备份，必须设置备份配置，进入到“系统管理/日志维护”，点击“日志备份”标签，点击“服务器配置”进入服务器配置页面，如下图：

服务器类型：支持 FTP 和 SFTP 两种协议；

IP 地址：外部 FTP 或 SFTP 服务器 IP 地址；

端口: 根据服务器类型，设置对应的端口；

用户名：FTP 或 SFTP 服务器的用户名；

密码：FTP 或 SFTP 服务器的用户密码；

上传目录：即 FTP 或 SFTP 服务器设置的授权目录（可读写权限）；

备份周期：即备份启动的周期，可以月、周、日进行；

备份时间：即备份启动的时刻，精确到小时；

自动备份：是否启动自动备份功能。

设置好备份参数后，点击“保存”即可生效。

9.1.2 日志备份

日志备份显示所有手动备份、自动备份的信息，并可以按照时间范围进行手动备份。

日志备份信息内容包括：

类型：说明该信息是手动备份、自动备份；

日志服务器：说明日志备份的服务器地址；

日志服务器目录：说明日志备份的具体目录；

备份操作时间：说明备份操作的开始结束时间；

备份区间：说明备份日志的时间范围；

状态：说明该操作的状态，如备份成功。

手动备份可以设置备份的时间段：开始日期和结束日期。如果需要对 2013 年 1 月 1 日的日志进行备份，设置时间段 2013-01-01 到 2013-01-01，点击“执行”即执行手动备份。

备份内容包含：当前配置、数据库中的运维会话及日志。

（注意：手动备份是增量备份，备份结束时间必须不大于前天）

9.2 日志文件删除

对已经做过备份的日志文件，NABH 提供删除功能。

日志删除信息包括：

类型：说明该信息是手动备份、自动备份；

日志文件备份操作时间：说明备份操作的开始结束时间；

备份区间：说明备份日志的时间范围；

操作：说明该操作的状态。

日志文件删除后，审计员可进行离线回放（非本地回放）。

9.3 日志状态

此处用户可以清楚的了解到与日志备份、日志删除等相关的状态，包括是否手动备份成功、自动备份是否成功、某段时间的日志文件被删除等。

日志状态信息如下：

9.4 备份恢复

9.4.1 配置恢复

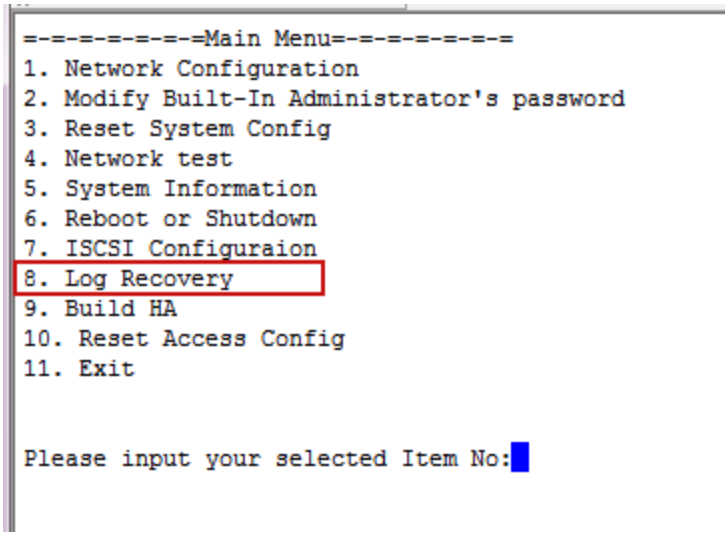
9.1.2 节中自动备份的配置文件可通过以下方式进行配置恢复。

“系统管理—系统维护—系统备份”页面，执行配置备份恢复操作，默认“保护密钥”为 UnionHAC。

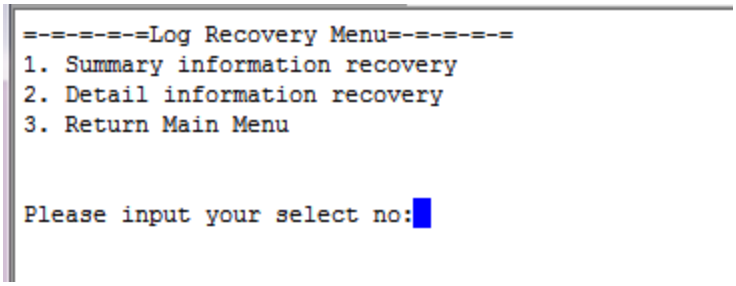
9.4.2 日志恢复

进行日志恢复前，应确保日志备份服务器正确配置，并且“上传目录”指向对应的日志备份目录，备份服务器与 NABH 之间网络畅通。

通过 3.2.3 配置进入 Console 口，可以看到：



输入 8，可以进行日志恢复操作：

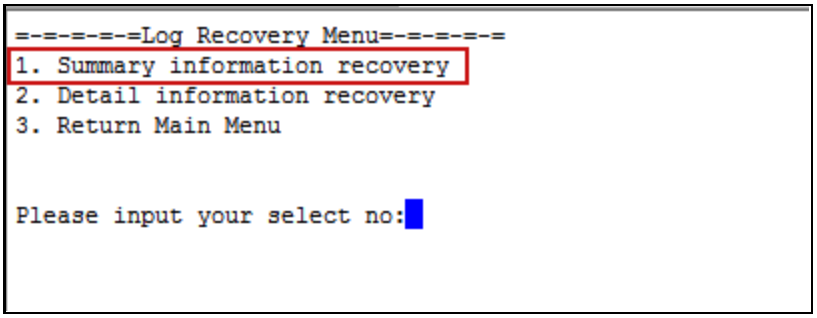


其中：

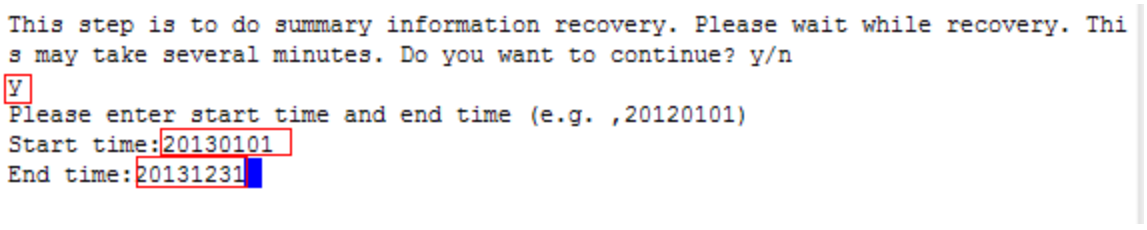
- 第一项：概要信息恢复，包含数据库会话及会话日志。恢复后可查看运维的会话，并进行回放；
- 第二项：会话详细信息恢复。恢复后可查看会话的详细信息，并进行上下行检索。
- 第三项：退出上一页面。

9.4.2.1 概要信息恢复

进行概要信息恢复后，可查看运维的会话，并进行回放。具体操作如下：选择 1，如图所示：



选择是否需要进行恢复，如输入：y，并输入需要恢复概要信息的时间：



直到“Press any key to continue”完成：

```
This step is to do summary information recovery. Please wait while recovery. Thi
s may take several minutes. Do you want to continue? y/n
y
Please enter start time and end time (e.g. ,20120101)
Start time:20130101
End time:20131231
Connected to 10.10.1.63 (10.10.1.63).
220 (vsFTPd 2.0.5)
331 Please specify the password.
230 Login successful.
200 Switching to Binary mode.
Local directory now /usr/local/keyou/Log/log_tmp
output to local-file: /usr/local/keyou/Log/log_tmp/2013.txt? 227 Entering Passiv
e Mode (10,10,1,63,138,30)
150 Here comes the directory listing.
226 Directory send OK.
?Invalid command
221 Goodbye.
Finish
Press any key to continue...
```

若缺少恢复文件，会有相应引导信息：

```
This step is to do summary information recovery. Please wait while recovery. This may take several
 minutes. Do you want to continue? y/n
y
Please enter start time and end time (e.g. ,20120101)
Start time:20140101
End time:20140101
Connected to 10.10.1.63 (10.10.1.63).
220 (vsFTPd 2.0.5)
331 Please specify the password.
230 Login successful.
200 Switching to Binary mode.
Local directory now /usr/local/keyou/Log/log_tmp
output to local-file: /usr/local/keyou/Log/log_tmp/2014.txt? 227 Entering Passive Mode (10,10,1,63
,142,18)
150 Here comes the directory listing.
226 Directory send OK.
?Invalid command
221 Goodbye.
ls: /usr/local/keyou/Log/log_session/usr/local/keyou/Log/log_tmp_file: No such file or directory
Finish
Press any key to continue...
```

完成上述恢复操作后，可查看运维的会话，并进行回放。

9.4.2.2 会话详细信息恢复

根据实际需要，可对会话的详细信息进行恢复操作。恢复后，可查看会话的详细信息，并进行上下行检索。

具体操作如下：输入 2，如图所示：

```
=-=-=-=-=Log Recovery Menu=-=-=-=-=
1. Summary information recovery
2. Detail information recovery
3. Return Main Menu


Please input your select no:
```

选择是否需要进行恢复，如输入：y，并输入需要恢复详细日志的时间：

```
This step is to do detail information recovery. Please make sure summary information has been reco
veried. This may take several minutes. Do you want to continue?y/n
y
Please enter start time and end time (e.g. ,20120101)
Start time:20130101
End time:20131231
```

直到“Press any key to continue”完成：

```
This step is to do detail information recovery. Please make sure summary informa
tion has been recoveried. This may take several minutes. Do you want to continue
?y/n
y
Please enter start time and end time (e.g. ,20120101)
Start time:20120101
End time:20131231
/usr/local/keyou/Log/2013/0803/ssh.B1FCA79A1FC65924.hlog
Press any key to continue...
```

若没有在输入时间段的详细信息，则不显示内容：

```
This step is to do detail information recovery. Please make sure summary information has been reco
veried. This may take several minutes. Do you want to continue?y/n
y
Please enter start time and end time (e.g. ,20120101)
Start time:20110101
End time:20110101
Press any key to continue...
```

10. 系统维护

系统维护包括：重新激活、系统重启、系统备份、升级管理、缓存维护功能。

10.1 重新激活

“系统激活”是 NABH 授权 License 导入部分。具体 License 包含如下几个方面：

- ***授权有效期***;
- ***授权主机数***（即被审计的核心服务器数量）;
- ***授权用户数***（即运维用户的数量）;
- ***授权模块***（SSO，VDH）
- ***授权协议数***（包含 TELNET、FTP、SSH、RDP、SFTP、VNC、XWIN、HTTP、HTTPS 等协议）。

NABH 提供了灵活的授权方式，可以根据上述五项的任意组合。

设备默认出厂时未授权，需要根据客户购买 License 后，再导入沈阳东软系统集成工程有限公司授权的激活文件，设备方可使用和生效。

客户在购买 License 时，需要提供如下图示中要求的内容：

用户名：客户用户名；

公司名：客户的公司名称。

沈阳东软系统集成工程有限公司会根据客户的上述信息，结合“注册码（设备内部唯一标识码）”，生成许可文件，用于激活设备。

10.2 系统重启

可以对 NABH 机器实现远程关机或重新启动：

选择关机或重新启动，点击“确定”完成操作。

10.3 系统备份

系统备份步骤：

1） 选择：“系统备份”，出现如下界面：

2） 输入保护密钥后，点击“确定”，即可进行配置的备份。

3) 点击下载位置，将该文件保存在本地，完成配置备份。

恢复配置文件步骤：

1) 选择：“恢复”，出现如下界面：

2) 点击浏览，定位到保存好的配置文件；输入保护密钥（该密钥就是在配置备份时输入的密钥），点击“确定”即可完成恢复。

注意：配置恢复操作，会将以前的配置覆盖掉，该过程需要重新启动设备。

10.4 升级管理

“升级管理”主要显示 NABH 版本补丁升级记录，升级记录页面如下图：

补丁升级页面如下图：

通过浏览选择系统升级文件，并将该文件上传。上传完升级文件后，必须重启设备，使升级文件生效。

10.5 缓存维护

缓存维护，主要用于清除 http(https)运维过程中所产生的临时文件，当 http(s)运行的文件系统被破坏，导致不可运维时，使用此功能。

11. 应用发布

在此设置 VDH 的相关信息，可以添加、删除 VDH，配置应用协议。进入“运维管理/应用发布”，界面如下

- *VDH 名称：*填写 VDH 的名称，可随意填写；[必填项]
- *IP 地址：*填写 VDH 的 IP 地址；[必填项]
- *应用配置：*配置应用协议。

11.1 VDH 添加、删除

1）添加 VDH，输入 VDH 名称和 IP，点击后面的“添加”按钮完成添加：

VDH 添加成功：

2）删除 VDH，点击右侧操作下面的“删除”，或勾选 VDH 后点击上面的删除键，完成删除操作。

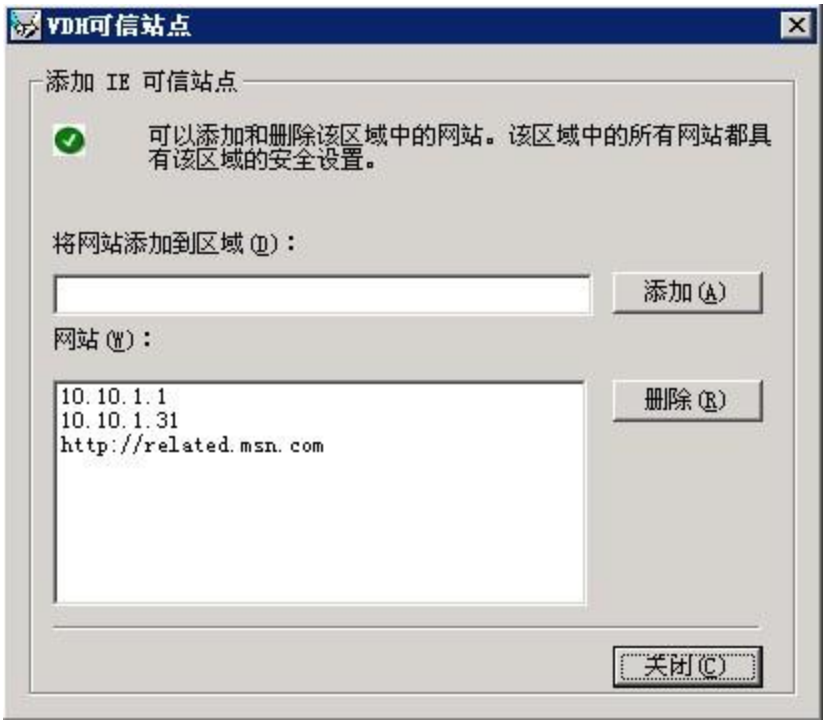
11.2 VDH 监控

可通过“VDH 监控”，来监控 VDH 服务器的性能状态。点击操作下面的“监控”，如下图;

- ***任务管理器：***可查看相关的应用程序、进程等。同：Windows 任务管理器；
- ***计算机管理：***可对 VDH 主机进行管理；

- ***事件查看器：***可审核系统事件和存放系统、安全及应用程序日志；
- ***性能：***可查看 VDH 主机性能；
- ***网络配置：***可查看及修改网络配置：

- ***信任站点：***可添加信任站点：



- ***关于：***可以查看 VDH 的版本：

11.3 VDH 应用安装

VDH 的应用，必须在操作台进行安装，具体步骤和注意事项请参见《东软 NetEye 统一身份管理系统（NABH）_应用发布配置手册》

11.4 VDH 应用管理

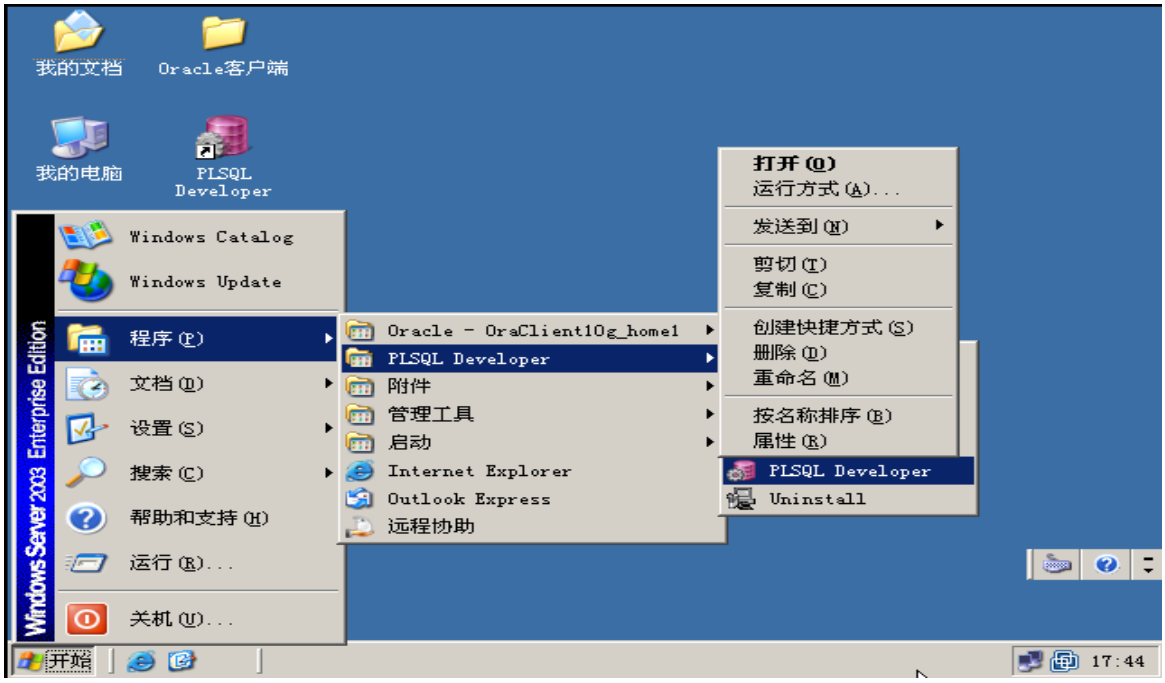
对 VDH 应用协议进行配置，可添加、编辑、删除应用协议。进入“运维管理/应用发布”，点击右侧“VDH 应用管理”，页面如下：

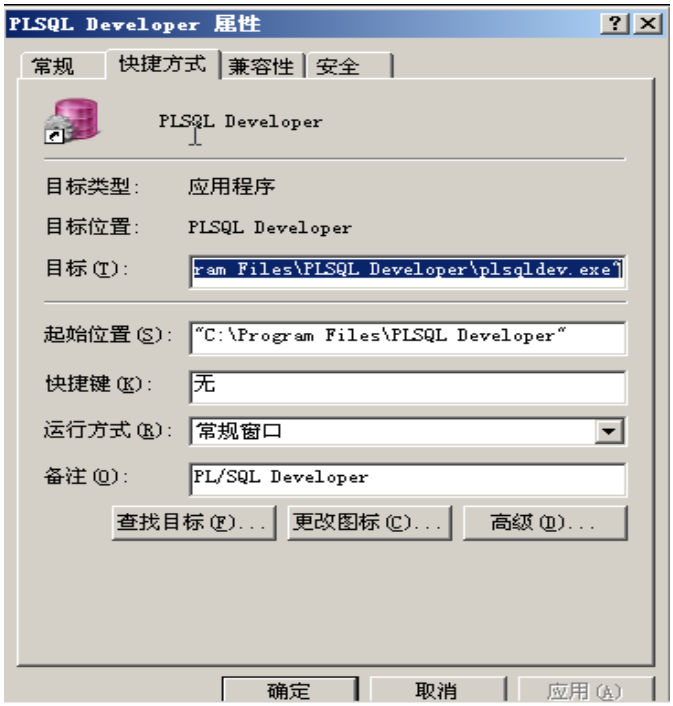
添加应用协议，点击“添加”进入添加页面：

- ***协议名称：***填写协议名称，由字母、数字、下划线、中杠线、点组成，此名称用于资源管理中显示的协议名[必填项]；
- ***权限设置：***可设置为普通用户、超级用户（不推荐使用）；
- ***代理转发：***勾选此代理则采用数据库代理方式审计，支持 Oracle、Informix、DB2 三种数据库类型，勾选此项审计平台可审计数据库详细信息。
- ***程序名称：***填写应用程序名称，此名称是在用户进行运维时桌面显示的图标名称；[必填项]
- ***程序路径：***应用程序在 VDH 主机上的安装路径，目前所有的应用程序必须安装在 C:\Program Files 或 C:\Windows 目录下。

下面以 PLSQL 为例，

PLSQL 应用程序的路径，从开始菜单/程序/PLSQL Developer/PLSQL Developer/右键属性：





快捷方式中的“目标”，便是 PLSQL 应用程序的路径。

添加 PLSQL 协议：

- ***自启动：***设置定义的程序是否运维用户在登录 vdh 时，能自动启动；（“我的电脑”不允许设置为自动启动）
- ***启动参数：***即该应用启动时，运行的参数。

  点击“保存”完成添加。

添加完成，可在资源管理中添加该应用的资源，进入“运维管理/资源管理/操作系统配置”。可添加 PLSQL 协议。

运维用户在运维时的效果为：

1） 点击“运维”进行运维，如下图

填写完数据库名，即可以 SSO 运维 VDH 应用。

12. 运维配置

“运维配置”提供运维的相关设置，包括帐户锁定、托管登录、RDP 设置、telnet 设置、双人复核相关设置（S 版无此功能）等。进入“运维管理/运维配置”，页面如下：

配置项	描述	当前值	操作
托管登录	在托管设备帐户运维时，可允许用户自行输入登录名和密码登录设备。	启用	编辑
变更工单	运维时要求输入工单号及变更事由。	禁用	编辑
Telnet设置	设置采用前端SSH方式登录后台Telnet服务器。	禁用	编辑
Imperva数据库审计	设置是否应用Imperva数据库审计功能。	禁用	编辑
复核等待时间	设置等待复核员操作的命令阻塞最大时限。	120	编辑
复核权限级别	设置复核员的用户级别。	3	编辑
强制复核级别	设置操作必须经过复核的用户级别。	3	编辑

帐户锁定：为了防止用户帐户密码被暴力破解，所设置的登录次数限制。默认值为 5 次，如果超过设置值，该帐户将被锁定，变成未激活状态。死锁次数设置为零，表示不启用此功能（死锁次数对认证方式为令牌认证的运维账户不起作用）；

托管登录：可控制运维用户是否可以自行输入后台核心服务器的的设备帐户和密码，登录后台服务器，默认禁用；

Telnet 设置：设置 telnet 运维时，客户端到 NABH 段是否为加密协议，即 SSH。默认关闭。

复核等待时间：范围 1~2147483647，单位为秒，默认 120 秒；指在命令复核时，复核员 120 秒内无操作，则会置超时处理，命令会被阻断；

复核权限级别：指用户级别为 3，以及以上的用户拥有复核的权限；默认级别为 3；

强制复核级别：默认级别为 3。指 3 级以及以下的用户运维登录和告警必须被复核。

S 版中无复核部分，详细实例请参看《东软 NetEye 统一身份管理系统（NABH）高级配置手册》

13. RDP 配置

RDP 设置：RDP 运维过程中磁盘映射、剪贴板和 Console 控制设置：

- ***磁盘映射：***勾选此项后，运维用户在 RDP 运维过程中有磁盘映射的权限；
- ***RDP 剪贴板：***勾选此项后，运维用户在 RDP 运维过程中可使用本地的剪贴板；
- ***RDP 登录 Console：***勾选此项后，运维用户在 RDP 运维时可使用 Console 方式登录 RDP 服务器；

14. 口令管理配置

托管通知：实现当帐户密码被更改时，系统会自动发送邮件到指定的邮箱。

- 接收人邮箱：填写密码变更时要通知的管理员的邮箱地址；
- 邮件主题：填写邮件主题；

设为启用时有效，点击“保存”完成设置。