
东软 NetEye 统一身份管理系统 统（NABH） V3.7

故障排查手册

Neusoft

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
1.1	文档目的	1
1.2	读者对象	1
1.3	约定	1
2	NABH 排障流程	2
2.1	网络故障排除	3
2.1.1	NABH 网络指示灯	3
2.1.2	PING NABH.....	3
2.2	配置故障排除	4
2.2.1	访问 NABH 问题	4
2.2.2	用户认证失败.....	4
2.2.3	访问内容不正常	5
2.3	运维操作故障排除	6
2.3.1	Telnet/SSH 协议运维故障排除.....	6
2.3.2	FTP/SFTP 协议运维操作故障排除.....	8
2.3.3	RDP/VNC/Xwindows 协议运维操作故障排除	10
2.4	告警功能排障	12
2.4.1	告警.....	12
2.4.2	告警邮件.....	13
3	FAQ	14

1 前言

1.1 文档目的

本文档编写目的是针对 NABH 上可能出现的现象，快速定位，并解决问题。

1.2 读者对象

本文档适用于 NABH 系统管理员，NABH 运维管理员。

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。

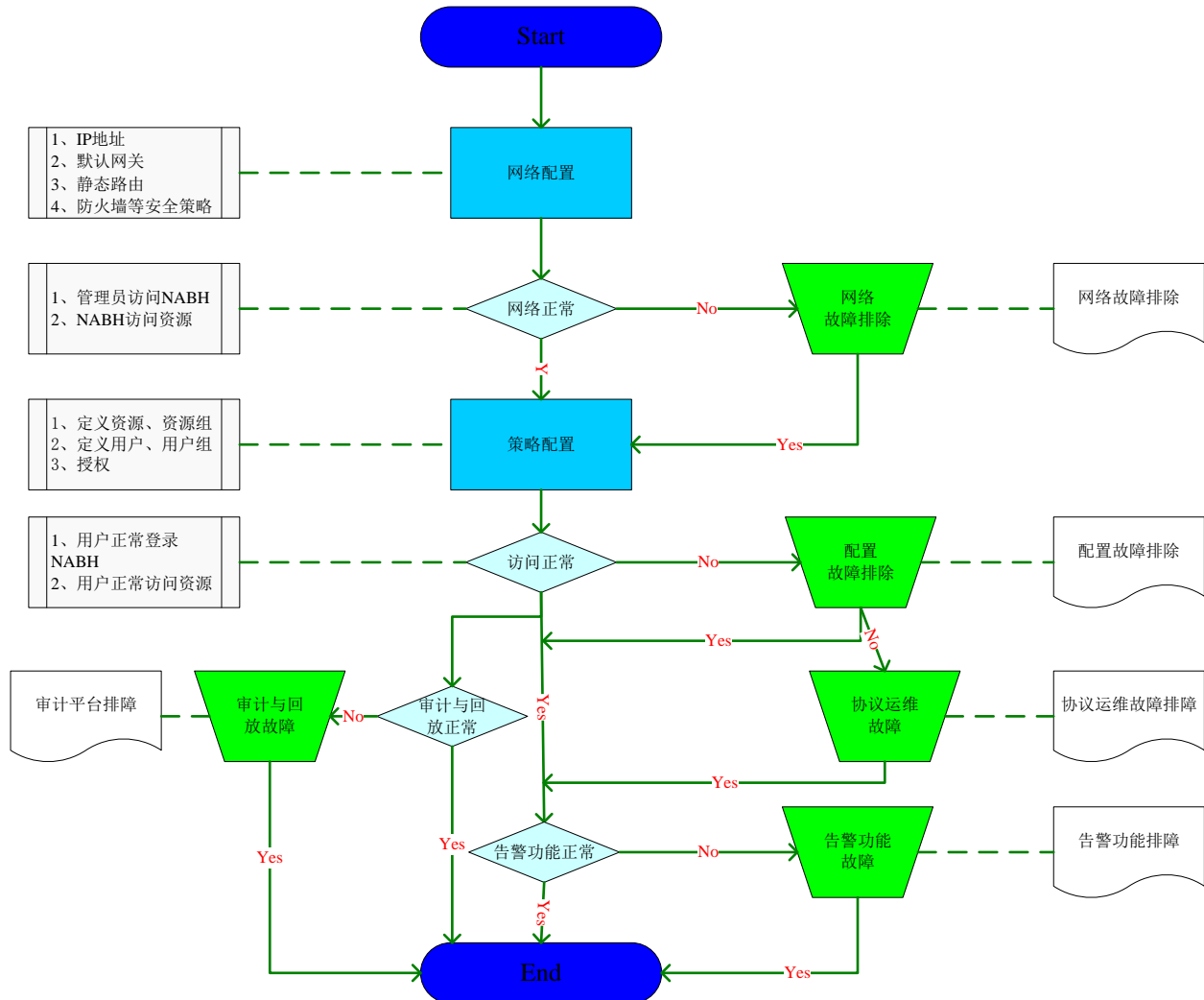
RDP: Remote Desktop Protocol, 远程桌面协议，RDP 专门为运行在服务器上的、基于 Windows 的应用程序提供网络连接上的远程显示和输入功能。Windows NT Server 4.0 支持 RDP 4.0，而 Windows 2000 终端服务使用的是 RDP 5.0。但是这两个版本是完全兼容的。我们常使用 Windows Terminal 终端连接远程服务器时就使用该协议。

Windows Terminal: Windows 远程访问终端，采用微软的 RDP 协议，文档中简称 WT 协议。

SSO: Single Sign-On, 单点登录功能实现用户登录一次 NABH，再次访问所需资源时无需再次输入系统本身的用户与密码。

2 NABH 排障流程

东软 NetEye 统一身份管理系统 NABH 配置和故障排除流程图如下图所示：



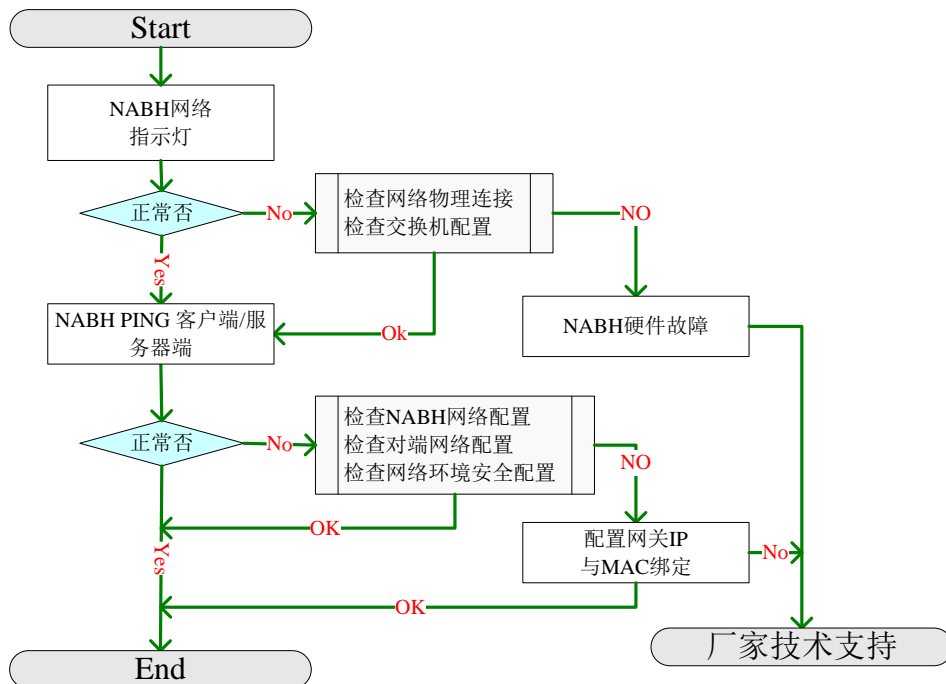
说明：

整个配置工作(深蓝色表示)从开始到结束包括两大部分：网络配置、策略配置。网络配置涉及 NABH 的 IP 地址、默认网关、静态路由和接入网络环境下的防火墙等安全策略的配置；策略配置包括系统配置、定义设备、定义用户、授权和告警配置。在配置完成后，正常情况运维用户可以正常登录 NABH、正常访问设备和审计员能正常审计和回放等。

本流程涉及的不正常情况(浅蓝色表示)包括：网络不正常、运维用户访问不正常、告警功能不正常、审计与回放不正常等。

本流程涉及的排障过程(绿色表示)包括：网络故障排除、配置故障排除、单个代理故障、告警功能故障和审计与回放故障。每类故障对应一个故障排除方法。

2.1 网络故障排除



2.1.1 NABH 网络指示灯

NABH 网络指示灯有两种：前面板指示灯和网口指示灯。前面板指示灯是在有网络流量时有闪烁（A 型机为绿灯、E 型机为黄灯）；网口灯针对交换机接口速率不同颜色不同：10M 时不亮、100M 为绿色、1000M 为橙色。

NABH 网络接口有三个：内网、外网和 HA 口。在单臂模式下只接外网口；串联模式下内网口接服务器端，外网口接运维区。

检查网络物理连接包括检查网线问题、连接问题及接交换机的位置。

检查交换机配置包括查看交换机对应 NABH 口的状态、速率问题、双工模式等。

2.1.2 PING NABH

PING NABH 是保证终端到 NABH 网络层是否通。

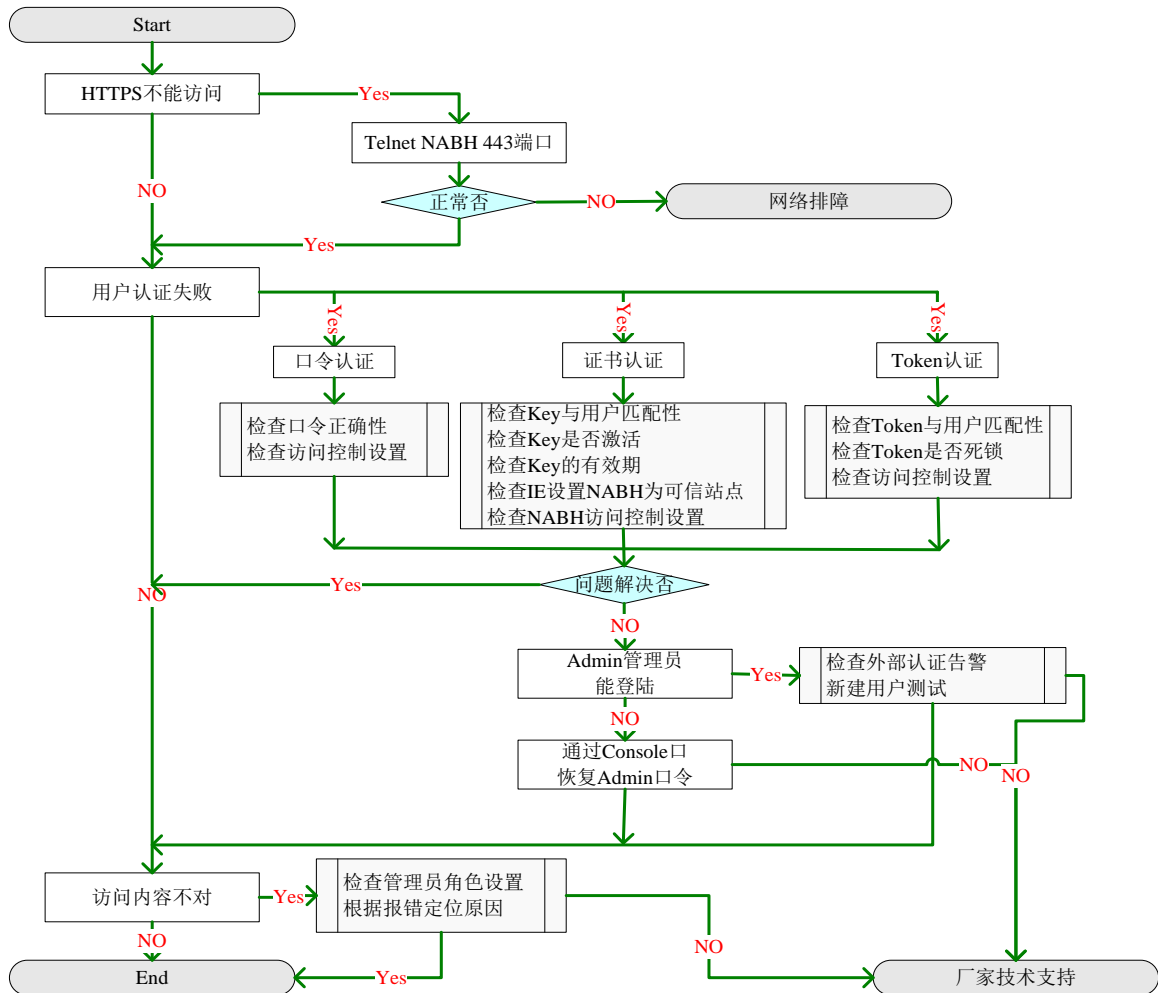
NABH 网络配置包括 IP 地址、默认网关等。检查 NABH 网络配置是确认其正确配置，可以通过 IE 登录 NABH 或通过 NABH console 进行查看。

检查终端（包括运维客户端和保护资源）网络配置是保证终端配置的正确性，可通过测试其到 NABH 的网关是否通来判断。

检查网络环境安全配置是确保终端到 NABH 的网络通路中是否存在安全设置而导致网络

不通。

2.2 配置故障排除



2.2.1 访问 NABH 问题

1、检查 NABH 的 WEB 服务是否正常

通过 Telnet NABH 443 可以看出 NABH 的 WEB 服务是否开启，如果开启应该能访问。

2、检查网络故障

通过网络故障排除可以定位是否是网络问题。如果不是网络问题，说明 NABH 的 WEB 服务没有正常启动，重启 NABH 看是否问题解决，如果没有，报厂家技术支持。

2.2.2 用户认证失败

1、根据用户认证方式检查相关配置

- 根据流程图中方法进行检查，排除相应问题；
- 检查是否所有管理员是否都不能通过认证。

2、Admin 是否能通过认证

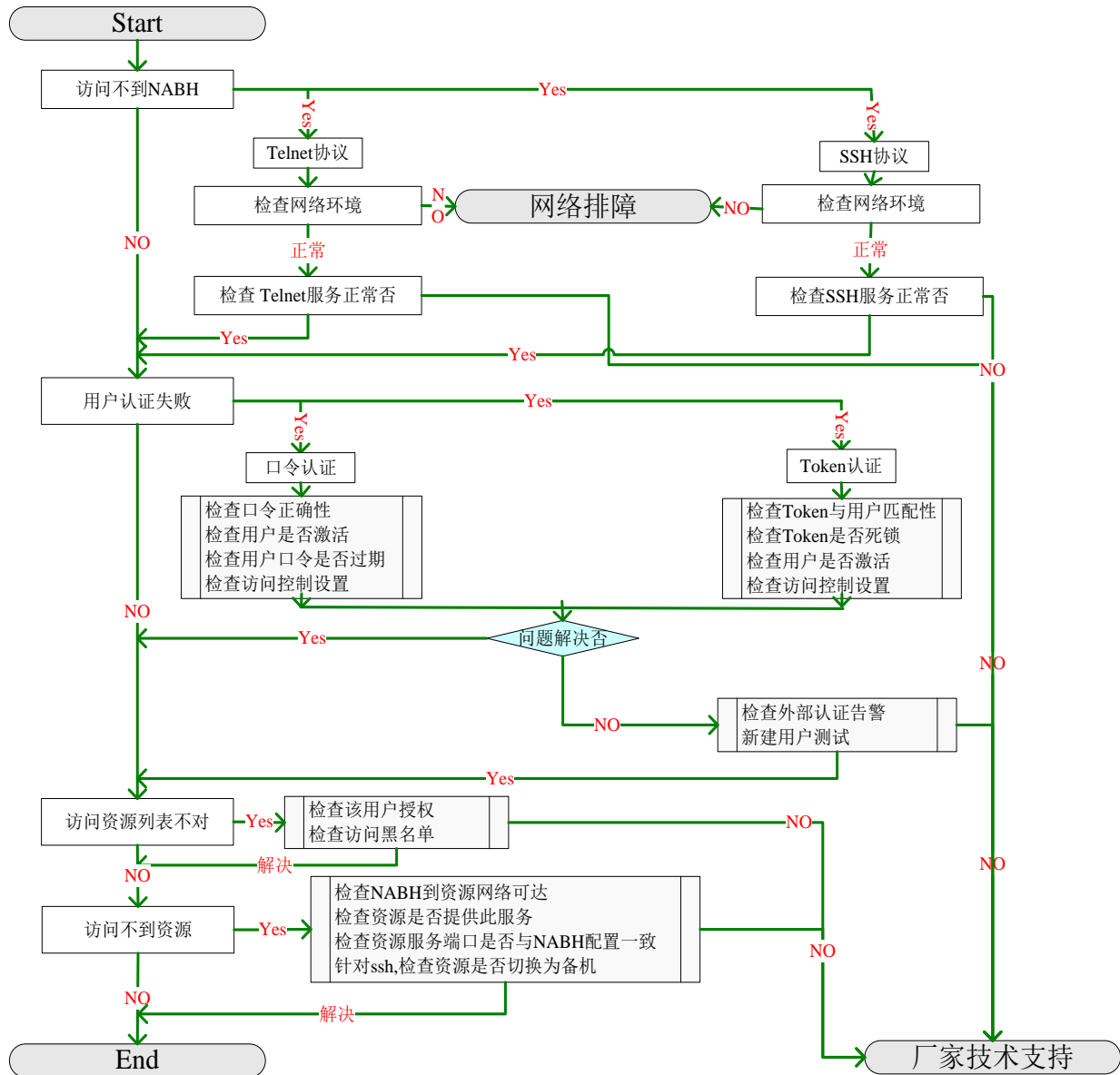
- Admin 认证为口令认证，如果能通过认证，说明 NABH 系统认证工作正常。此时，一般情况是外部认证系统的问题，尤其是其他所有管理员不能通过认证，应检查认证系统的报错信息来定位故障；
- Admin 口令可以通过 Console 口重置口令；
- Admin 认证通过，可新建一个管理员来测试新建管理员是否能正常认证。

2.2.3 访问内容不正常

- 1、检查管理员角色设置，确保角色分配正确；
- 2、根据界面报错信息定位故障原因；
- 3、厂商技术支持。

2.3 运维操作故障排除

2.3.1 Telnet/SSH 协议运维故障排除



2.3.1.1 访问不到 NABH

1、检查网络环境

检查方法与网络故障排除相同。

2、检查 NABH 服务

通过 telnet 相关服务端口检查 NABH 相关服务是否启动。

如果配置为安全模式的 Telnet，则用 Telnet NABH_ip 22 的方式进行检查。

注：NABH 如果配置为安全模式的 Telnet，需采用 SSH 客户端访问 NABH。

2.3.1.2 用户认证失败

与管理员管理故障排除类似。需要注意运维用户两个特性：用户是否激活和口令有效期的问题。

2.3.1.3 访问设备列表不对

1、检查该用户的授权

检查该用户是否有访问此设备的权限和授权规则等。

2.3.1.4 访问不到资源

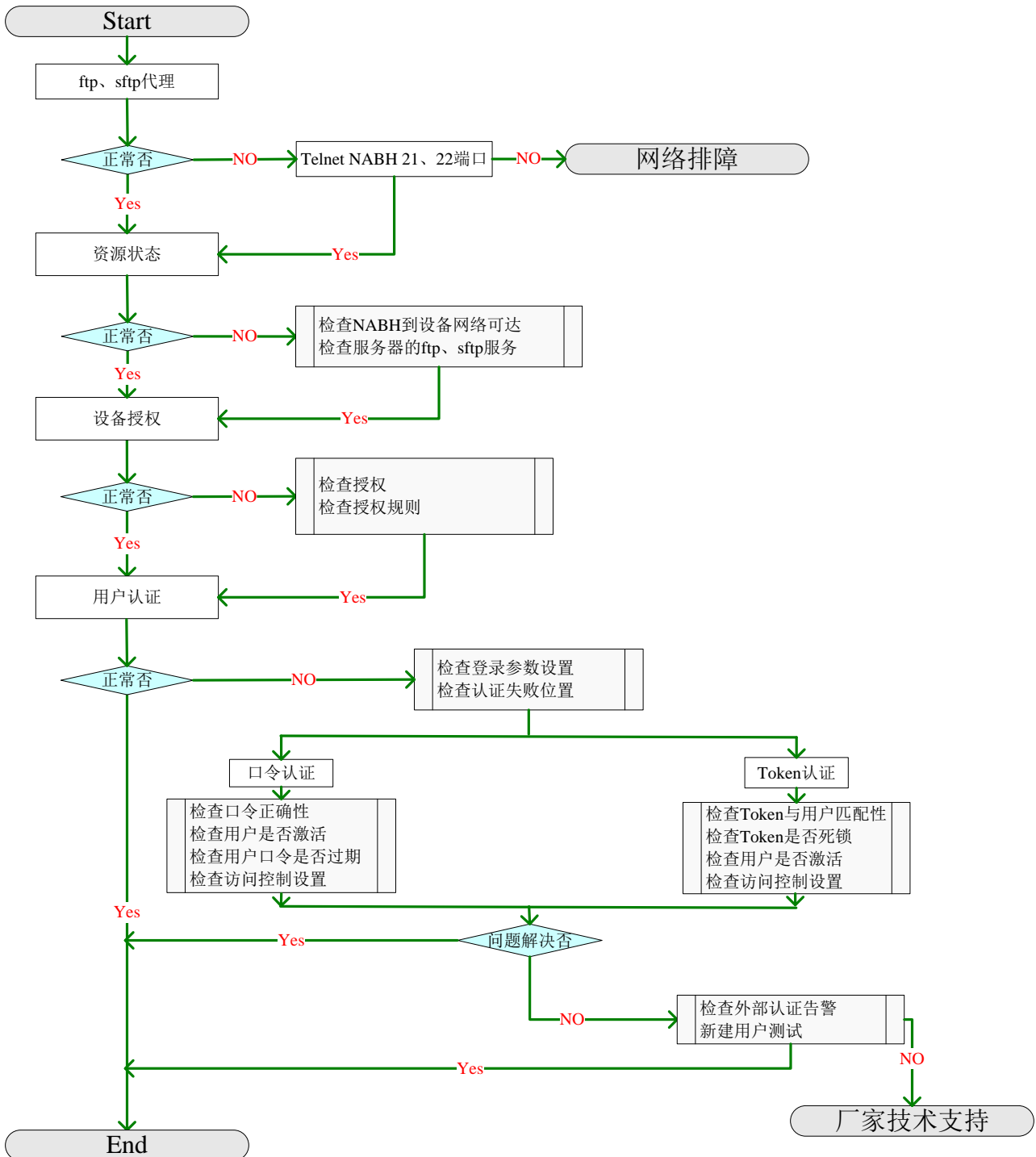
1、检查 NABH 到资源的网络是否可达

- NABH 到资源的网络可达包括网络层可达和端口层可达；
- 网络层可达可通过 NABH ping 资源或资源 ping NABH 的方式检查；
- 端口层可达可查看网络设备和安全设备上是否对此端口进行了限制，也可通过 NABH telnet 资源相关端口进行测试。

2、检查资源是否提供此服务

3、检查资源服务端口是否与 NABH 配置的协议端口一致

2.3.2 FTP/SFTP 协议运维操作故障排除



2.3.2.1 FTP、SFTP 代理

通过 telnet NABH 21 或 22 端口，来检查 NABH 的 FTP 或 SFTP 代理是否正常。

2.3.2.2 设备状态

- 检查 NABH 到运维服务器是否网络可达；
- 检查 FTP 或 SFTP 服务是否正常开启，以及该服务的相关配置。

2.3.2.3 设备授权

- 检查运维用户是否有此 FTP 或 SFTP 协议的授权；
- 检查授权规则是否对此运维用户有限制；

2.3.2.4 用户认证

- 检查在 FTP 或 SFTP 登录时参数设置是否正确，正确的参数设置应为：

用户名：NABH_user#host_user#资源名，如：fox#root#win2003_ftp，其中 fox 为运维帐号，root 为 ftp 服务器帐号，win2003_ftp 为 ftp 资源名。

密码：NABH_pwd#host_pwd。

- 检查 FTP 认证失败的位置

■ 在登录时若提示为：

```
> USER fox#lim#win2003_ftp
< 331 Please specify the password.
> PASS <password>
i Control connection closed normally. 或
```

```
User (172.16.2.103:(none)): fox#lim#win2003_ftp
331 Please specify the password.
Password:
Connection closed by remote host.
```

，则表明是在 NABH 认证时失败。

败。

■ 若提示为：

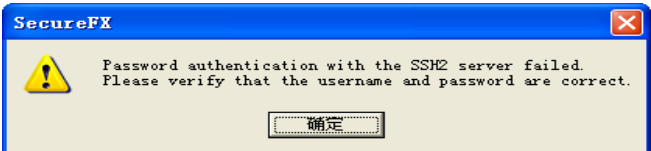
```
< 331 Please specify the password.
> PASS <password>
< 530 Not logged in. 或
```

```
331 Please specify the password.
Password:
530 Not logged in.
```

则表明是在 ftp 服务器认证时失败。

- 检查 SFTP 认证失败的位置

■ 在登录时若提示为：



(SecureFX 为

例) 或 `Permission denied, please try again.` 则表明是在 NABH 认证时失败。

■ 若提示为：

```
i State Change: SSH_STATE_USERAUTH->SSH_STATE_CONNECTION
i State Change: SSH_STATE_CONNECTION->SSH_STATE_DISCONNECTING
i State Change: SSH_STATE_DISCONNECTING->SSH_STATE_CLOSING
i State Change: SSH_STATE_CLOSING->SSH_STATE_CLOSED
i Connected for 22 seconds, 1260 bytes sent, 2173 bytes received
```

(SecureFX 为

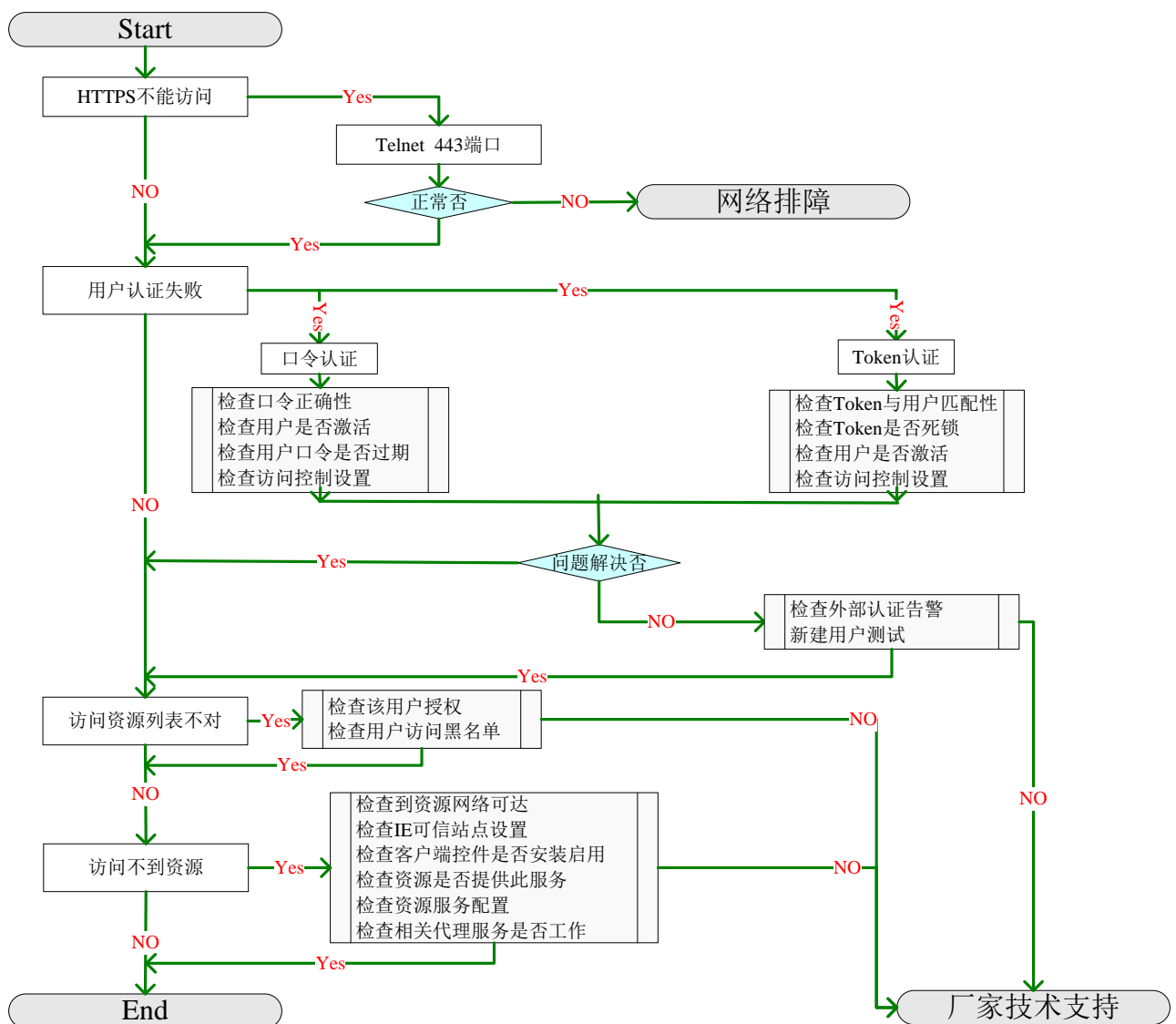
例) 或长时间连接不上, 最后提示 `Connection closed`, 则表明是在 sftp 服务器认证时失败。

➤ 检查 NABH 的认证方式

根据流程图中方法进行检查, 排除相应问题。

如果问题没有解决, 报厂家技术支持。

2.3.3 RDP/VNC/Xwindows 协议运维操作故障排除



2.3.3.1 用户认证失败

需要注意运维用户两个特性：用户是否激活和口令有效期的问题。

2.3.3.2 访问设备列表不对

1、检查该用户的授权

检查该用户是否有访问此资源的权限和授权条件等。

2、检查 NABH 的访问黑名单

检查该用户访问相关资源进入黑名单。

2.3.3.3 访问不到设备

根据排障流程中 6 项进行检查，基本能排除相应问题。如果解决不了，需咨询厂家技术支持。

1、检查 NABH 到资源网络可达

- NABH 到资源的网络可达包括网络层可达和端口层可达；
- 网络层可达可通过 NABH ping 资源或资源 ping NABH 的方式检查；
- 端口层可达可查看网络设备和安全设备上是否对此端口进行了限制，也可通过 NABH telnet 资源相关端口进行测试。

2、检查 IE 可信站点设置

IE 调用远程桌面连接需要运行控件，为了安全可将 NABH 设置可信站点，并对 IE 安全选项进行相关配置。

3、检查客户端控件是否安装与启动

客户端需要安装 Microsoft Rdp Client Control ActiveX 控件并处在启用状态。

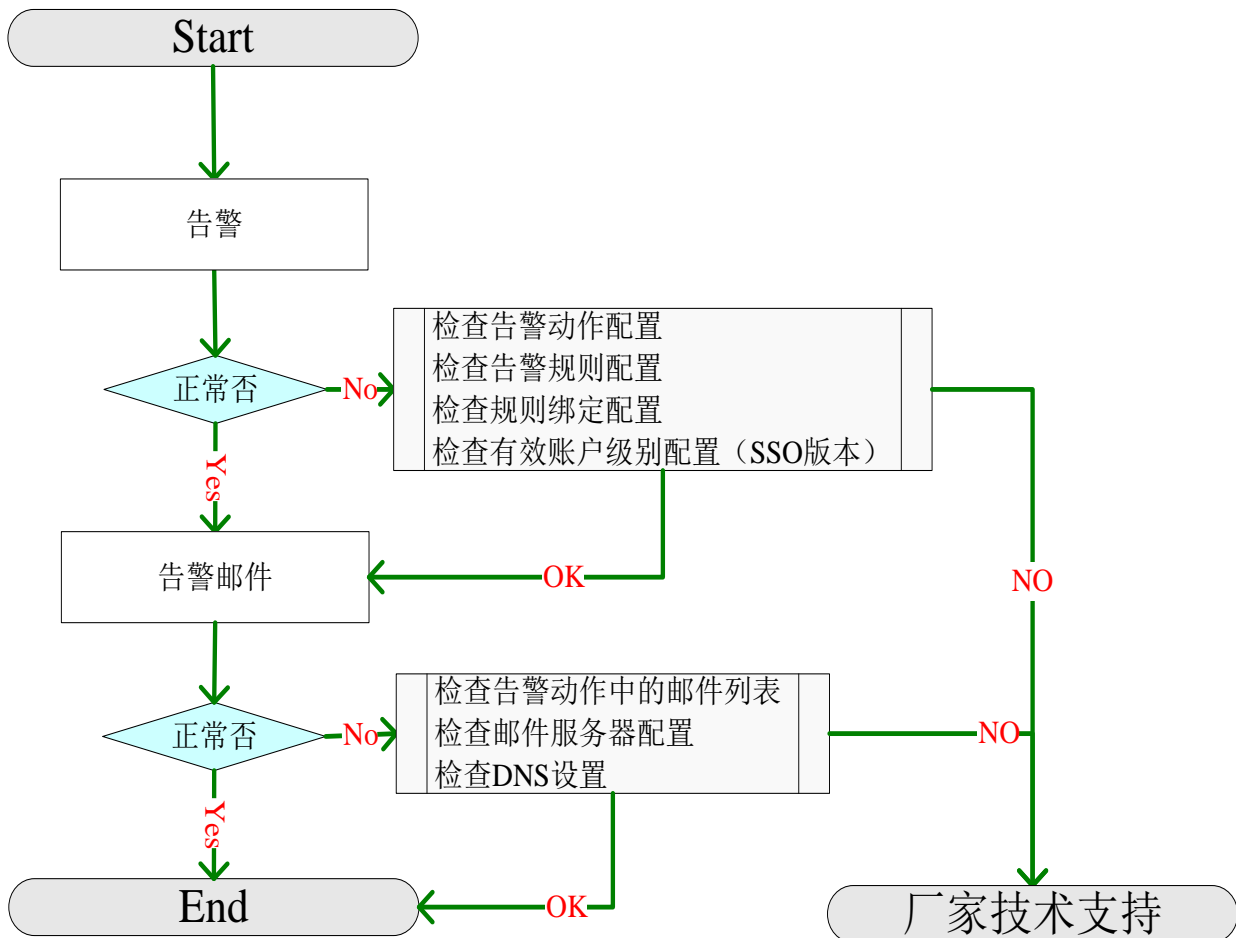
4、检查设备是否提供此服务

5、检查设备服务配置

由于设备服务配置限制可能会引起无法连接，可通过标准客户端直接访问资源的方式来验证设备服务配置是否存在相关限制等。

6、检查 NABH 相关代理服务是否工作

2.4 告警功能排障



2.4.1 告警

首先要保证告警配置正确。

- 检查告警动作配置。包括：告警声音、是否阻断、告警邮件地址列表。

若设置命令阻断动作，则命令不会被执行，并提示阻断信息、发出告警；否则命令被执行，且向审计平台发出告警。

告警邮件列表是在发生告警时，将告警信息以邮件的方式通知管理员。

- 检查告警规则配置。包括：阻断提示信息、告警动作、是否启用、适用协议、匹配命令。

阻断提示信息是在执行阻断动作时，运维客户端上提示的信息。

适用协议包括：SSH/Telnet、FTP、SFTP，必须保证其与运维协议一致。

匹配命令定义了此规则所适用的操作命令。

- 检查规则绑定配置。包括：授权规则、有效账户级别。

2.4.2 告警邮件

发生命令告警时，可将告警详细信息以邮件方式通知用户。需保证邮件的相关配置正确。

- 检查告警动作中的邮件列表，保证其邮件地址为有效地址。
- 检查邮件服务器配置。检查 DNS 设置，保证 DNS 地址为有效地址，使其能解析到邮件服务器地址。

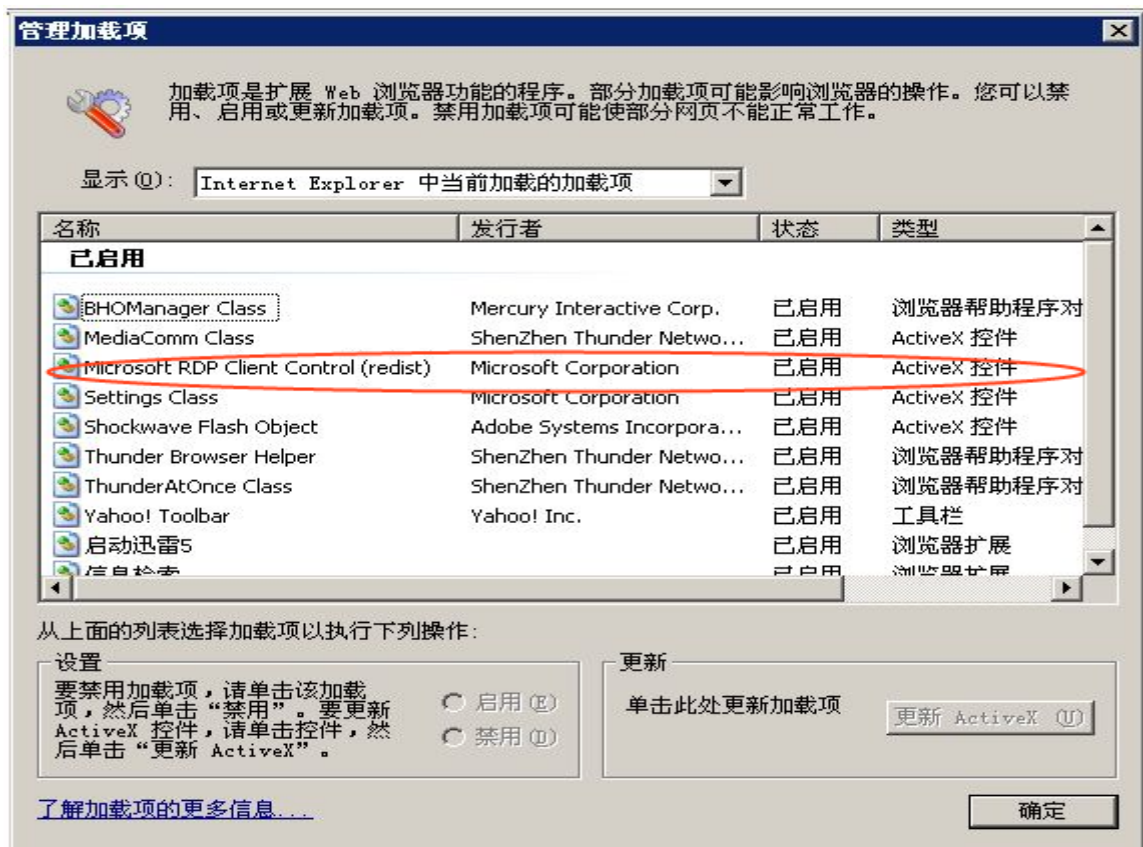
3 FAQ

1、RDP、Xwindows、VNC 某一项服务无法正常访问？

答：从以下几个方面进行排查。

1) IE 相关设置

- RDP、Xwindows、VNC 服务是通过 IE 浏览器进行访问。目前其他类型的浏览器不支持。
- 服务需要 IE 启用”Microsoft Rdp Client Control”ActiveX 控件。通过 IE 工具->管理加载项，查看是否加载此控件，并且属于启用状态。

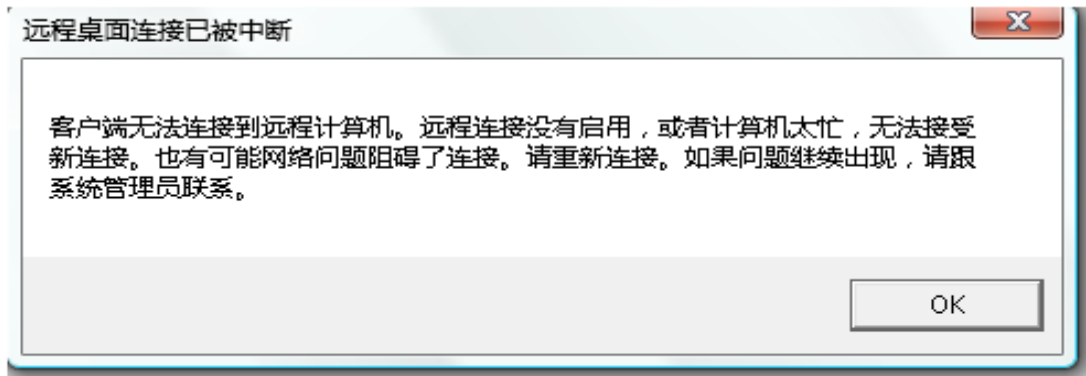


通过 IE 浏览器访问 NABH 运维页面的过程中，浏览器会自动从 NABH 中下载此控件并加载它。

- 由于微软最近的更新导致部分用户 rdp 控件无法使用，解决方法为为客户端应用相应版本的补丁。补丁应用参见如下 web 页面：<http://support.microsoft.com/kb/958470>

2) NABH 代理问题和保护资源是否启动相关服务

访问过程中出现如下界面：



首先，检查 NABH 相关服务是否可用。用客户端直接连接到 NABH 外网口，telnet 相关端口，（RDP 端口：3389，VNC 端口：5900，Xwindows 端口：7000），如果连接成功，说明该服务可用。

如果 NABH 服务可用，请检查：

- 真实服务器是否提供服务。

如果 NABH 服务不可用，请检查以下内容：

- 检查系统日志区是否已经没有可用空间。日志空间已满会导致相关进程无法写日志而关闭。请对日志进行备份，并删除已备份的日志。

最后，重新启动 NABH，如仍不能使用，请联系沈阳东软系统集成工程有限公司技术支持。

3) 网络问题

- 检查客户端到 NABH 的网络是否正常。
- 检查 NABH 到真实服务器网络是否正常。
- 检查防火墙是否配置了相关策略。

2、IE 安全级别已经设置，但是加载项中仍看不到”Microsoft Rdp Client Control”ActiveX 控件

答：该问题的原因是：情况默认， Windows XP Service Pack 3 (SP 3)禁用 ActiveX 控件。

解决办法：

1) 请删除下面的注册表项中：

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{7584C670-2274-4EFB-B00B-D6AABA6D3850}
```

删除此项后，需重启 IE。

可参考<http://support.microsoft.com/default.aspx/kb/951607>

2) 手动加载 ActiveX 控件

- 使用 IE 下载控件 https://NABH_ip/msrdp.cab, 并将其解压(包含两个文件: msrdp.ini 和 msrdp.ocx)
- 在“开始->运行”中运行命令: regsvr32 解压文件绝对目录\msrdp.ocx, 如:
regsvr32 c:\msrdp\msrdp.ocx

3、Windows 主机如何开启远程桌面服务?

答: 不同操作系统的 windows 主机, 开启远程桌面的方法各有不同

- 对于 Windows XP 和 2003 server 主机, 需在“我的电脑->属性->远程”中, 将远程桌面服务打开
- 对于 Windows 2000 server 主机, 需安装终端服务组件
开始 -> 设置 -> 控制面板 -> 添加/删除程序 -> 添加/删除 Windows 组件 -> 选中“终端服务” -> 详细信息 -> 勾选“启用终端服务”-> 确定
注意安装组件时, 需用到系统光盘。
- 对于 Windows 2000 professional 主机, 系统不支持远程桌面服务, 需通过第三方的远程桌面软件, 如 VNC 和 PanyWhere 来实现远程桌面服务。

4、在 RDP 访问时, 鼠标移动速度较慢?

答: 该问题的原因是默认的 RDP 协议的刷新频率是 100ms, 相当于 10Hz。所以鼠标移动速度较慢。

可以添加注册表键值来解决这个问题: 在 HKEY_CURRENT_USER \Software \Microsoft \Terminal Server Client 中新建两个 dword 值, 名称分别为: Min Send Interval 和 Min Send Interval 5, 他们的值都为 10, 也就是 10ms 刷新一次。

5、在 RDP 访问时, 远程桌面窗口有条格出现?

答: 该问题出现过的运维环境是 winXP professional 版本 2002 service pack3;
远程桌面客户端版本: 6.0.6001.18000; 是因为缺少系统补丁。可以安装 WindowsXP-KB969084-x86-chs.exe 解决此问题。

6、Telnet、SSH、FTP、SFTP 中某个协议不能访问?

答: 从以下情况进行检查。

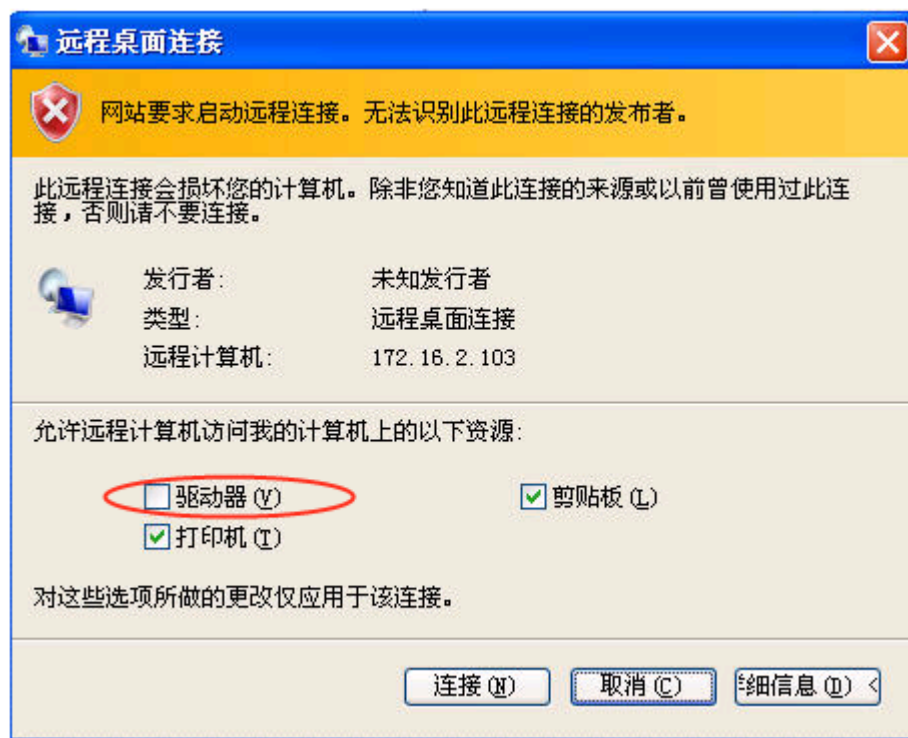
- 1) 检查客户端到 NABH 的网络是否正常;
- 2) 检查防火墙是否配置了相关策略;

- 3) 检查设备是否提供服务;
- 4) Telnet 检查 NABH 相关服务是否可用。(ftp 端口: 21, ssh 端口: 22, sftp 端口: 22, telnet 端口: 23)
- 5) 检查系统日志区是否已经没有可用空间。日志空间已满会导致相关进程无法写日志而关闭。请对日志进行备份, 并删除已经备份过的日志。

最后, 重新启动 NABH, 如仍不能使用, 请联系沈阳东软系统集成工程有限公司技术支持。

7、在 RDP 运维页面中勾选磁盘映射选项, 登录后发现本地磁盘没有映射到远程主机?

答: 如果在执行 rdp 登录操作时会弹出以下页面, 而用户没有勾选驱动器选项, 则会导致本地磁盘驱动器没有映射。



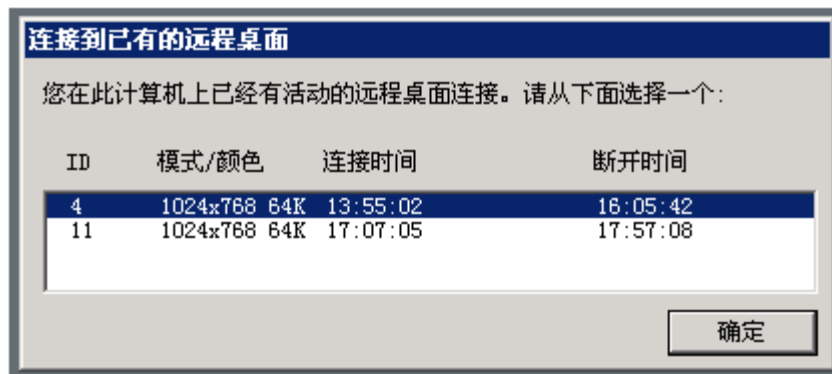
注: 通常客户端在登录的时候不需要再次勾选。此情况的产生是因为 RDP 对驱动器映射的提示与客户端程序版本和安全设置有关系, 属于安全保护。

如果勾选以上的选项后, 仍然不能完成此功能, 则请联系服务器管理员, 开启服务器允许映射磁盘驱动器的功能。

8、在使用 RDP 访问保护资源后, 通过非注销的方式退出, 若用此用户名再次登录时, 不能进入原连接的会话?

答: Windows server 具有为同一个用户提供多个会话的功能, 采用某些版本的客户端进行

登录的时候可以显示让用户选择需要登录的会话，如下图所示。



如果客户端不能提供这个功能，请在服务器终端服务配置中设置“限制每个用户使用一个会话”。

9、 Windows telnet 服务不能设置采用自动登录的方式？

答：NABH V3.7 版本只支持类 Unix 系统的 Telnet 自动登录。

10、 管理员在自动登录管理->设备账户管理页面中，设置 RDP 自动登录帐号时，始终提示用户名密码错误？

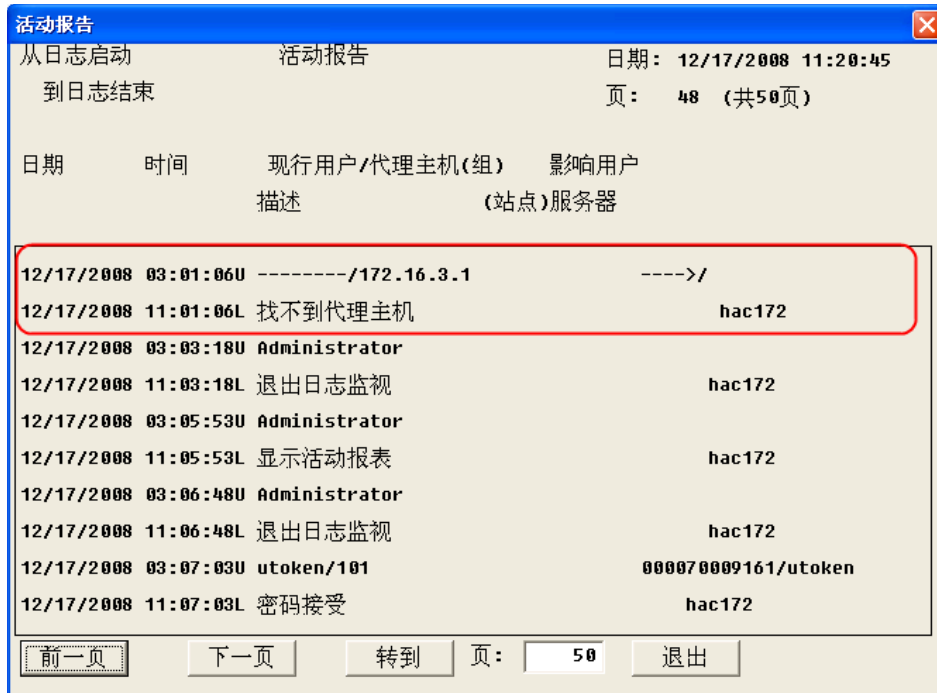
答：请将资源的服务器类型更改为 Windows。

11、 采用令牌认证方式进行登录，提示用户名密码无效？

答：请按以下步骤检查：

首先在安盟服务器进行本地身份验证，如果能通过，请登录安盟服务器，查看 token 服务器的活动日志。

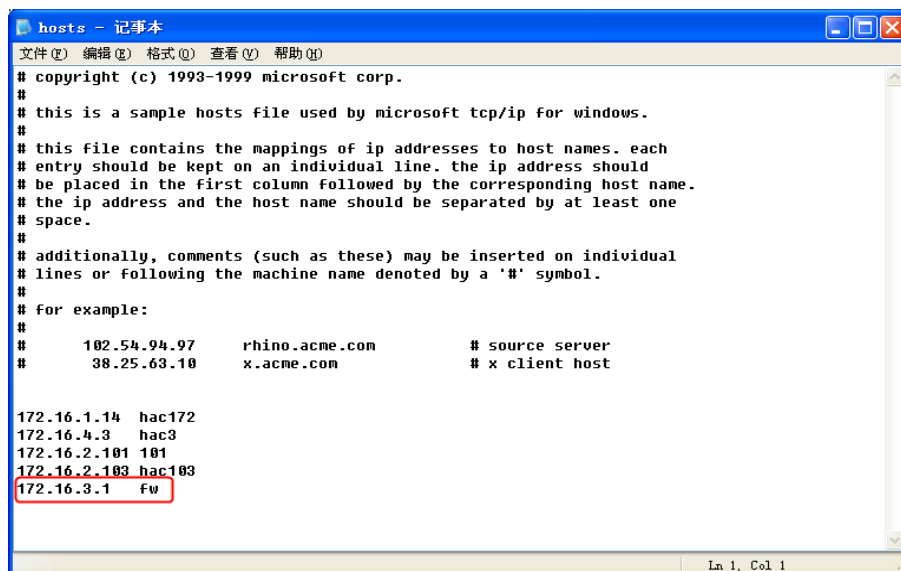
- 如果活动日志提示为：



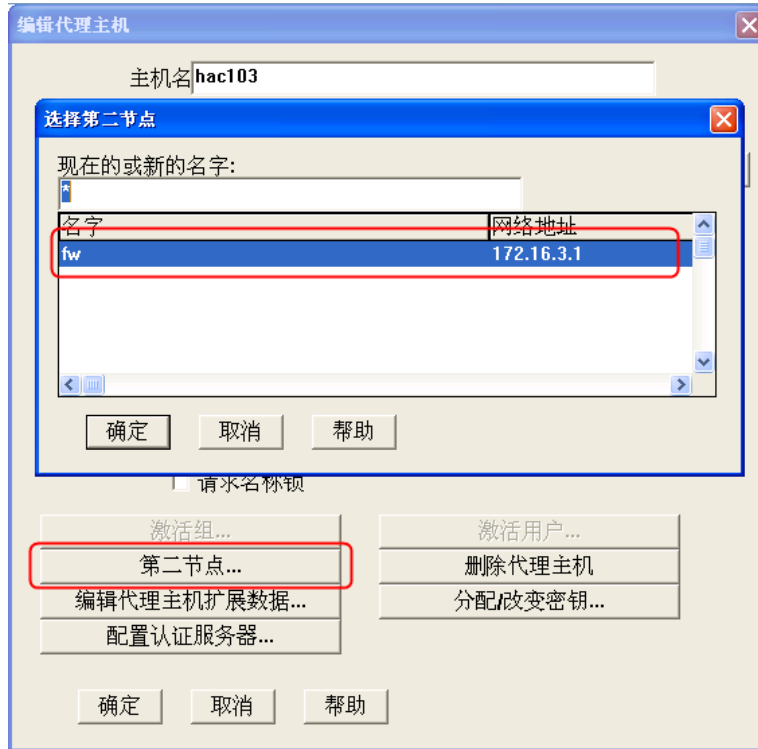
日志提示找不到代理主机，而 172.16.3.1 为防火墙地址，经查看是由于在防火墙上设置了 NAT 策略。解决方法有两种：

- 1) 在防火墙上取消 NAT 即可,建议将 token 认证服务器与 NABH 部署在同一网段。
- 2) 添加 UNIX 代理主机的第二节点。

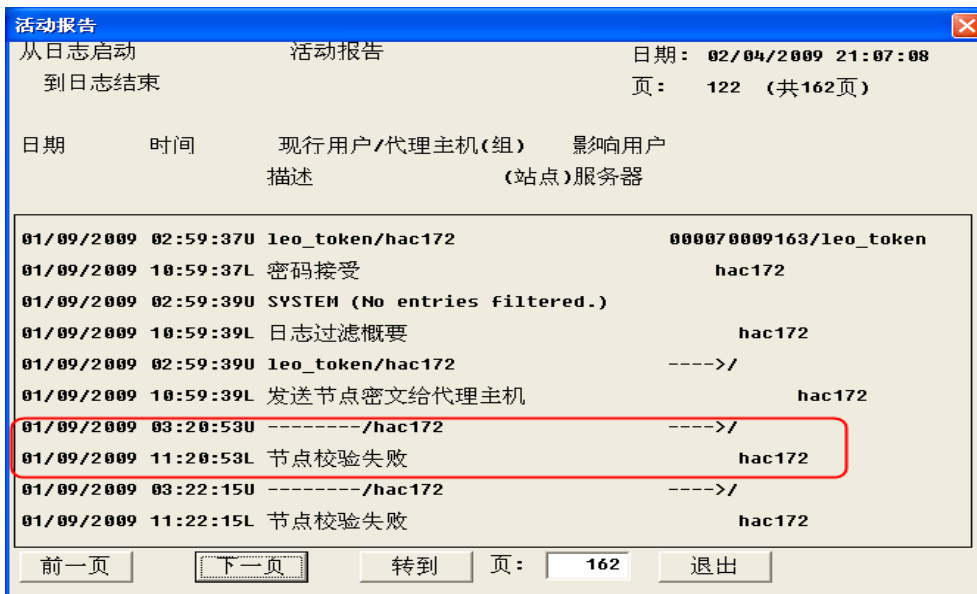
首先，编辑认证服务器本地的 hosts 文件，添加防火墙的地址。如图：



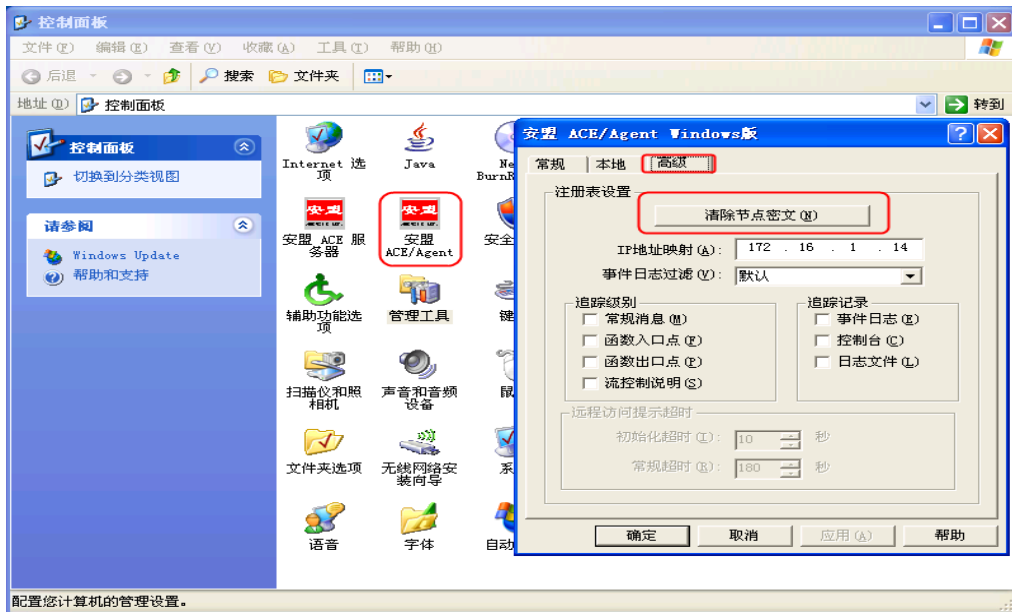
然后，编辑代理主机，添加第二节点；



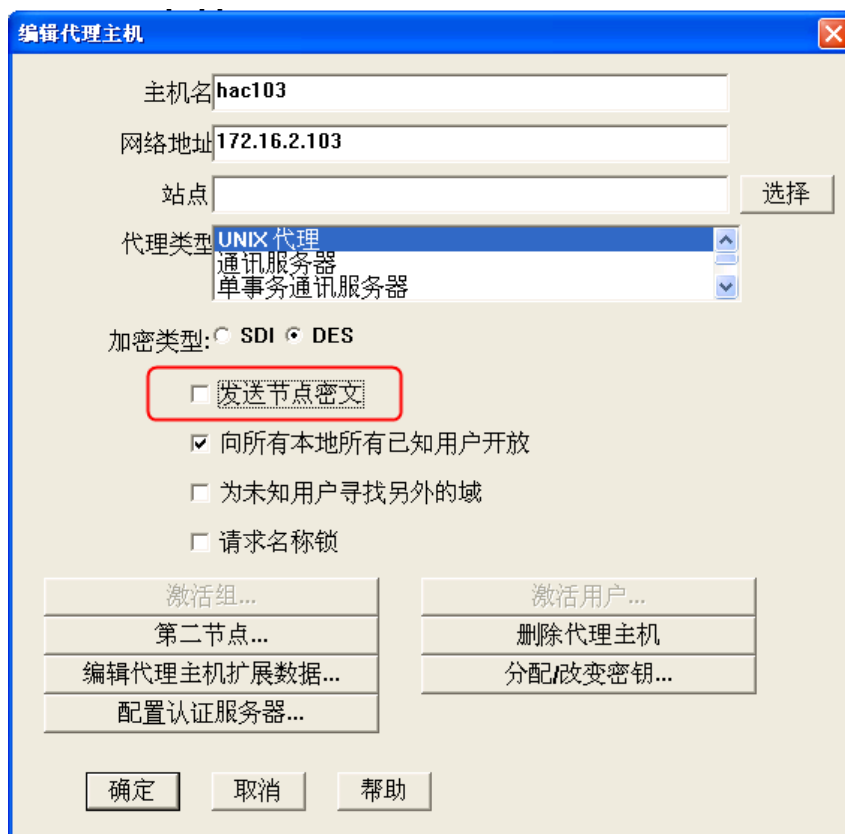
➤ 如果活动日志提示为：

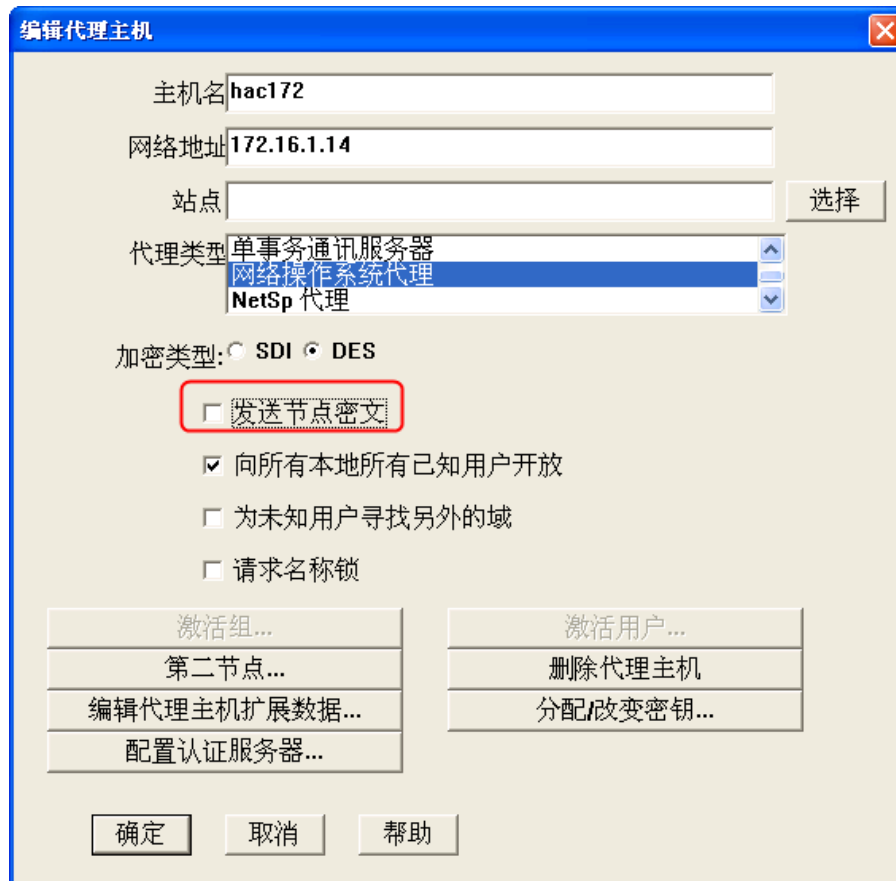


则需在认证服务器的控制面板中，打开“安盟 ACE/Agent”，清除节点密文，如下图：



并且在“编辑代理主机”处，将“UNIX 代理主机”和“网络操作系统代理主机”的“发送节点密文”选项取消勾选，如图：





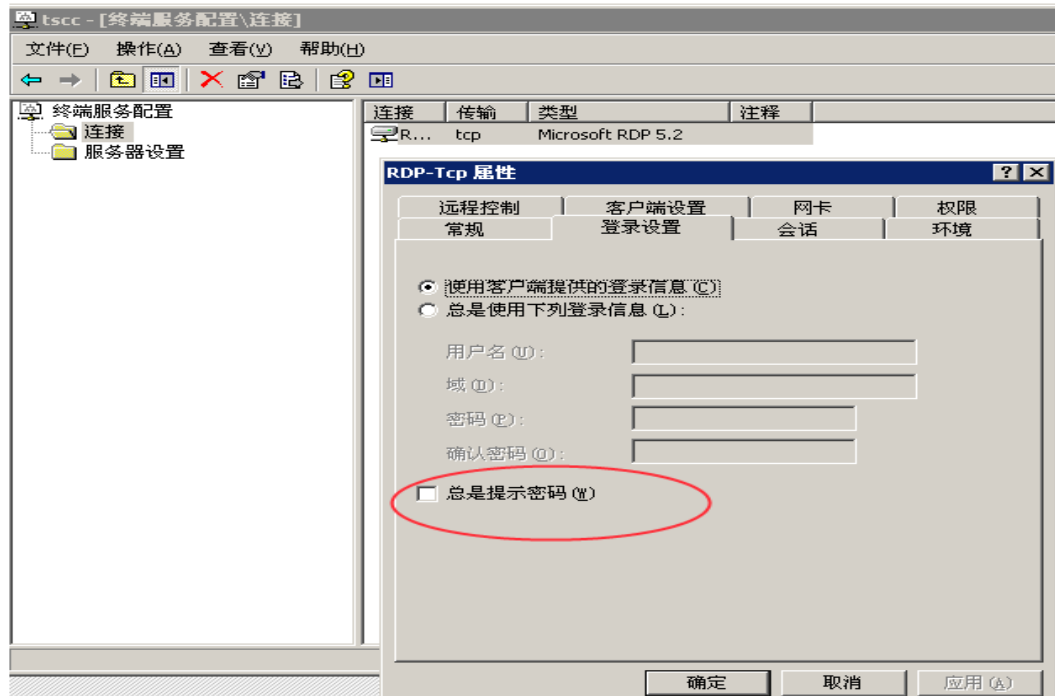
12、 新增一台与以前相同类型的服务器，添加账户时，一直提示账户名密码验证失败？

答：服务器类型虽然一样，但是由于命令提示符和欢迎信息等可以自定义，sso 的配置文件可能和原有服务器不一致。登录 sso 配置页面检查操作系统类型信息是否和新增服务器一致。如果不一致，增加新的操作系统模板，将服务器的相关信息录入。

13、 Windows Server RDP 自动登录始终不成功，需要手动输入密码才能登录？

答：需从两个方面进行检查：

- 1) 由于 RDP 的自动登录配置时不对账户进行密码校验，请登陆 NABH，对此资源重新输入正确的用户名和密码。
- 2) 检查 Windows Server 上的终端服务器配置,是否选中了"总是提示密码"选项。请在开始-程序-管理工具-终端服务配置-左侧树状列表中的“连接”，双击右侧“RDP-Tcp”项，查看登录设置-总是提示密码选项框是否勾选。如果勾选，取消即可。



14、 真实服务器原有地址不变更的情况下，主机进行了更换、主机 SSH 版本变更、或主备机切换后，不能通过 NABH 进行 ssh 和 sftp 登录访问？

答：为了保证运维的安全，防止中间人攻击，NABH 对主机更改的机器的密钥不做主动更改。遇到此情况需要将 NABH 重新启动。

15、 已经配置了邮件告警服务器，为什么没有收到告警邮件？

答：请从以下两方面进行排查：

- 1) NABH 到邮件服务器的网络是否畅通。
- 2) 登录配置管理平台 系统信息->网络设置页面，查看是否配置了正确的 DNS。

NABH 默认没有配置 DNS 服务器地址。如果没有，请添加正确的 DNS 服务器地址。

16、 运维操作有时出现异常中断？

答：NABH 是采用代理技术实现数据的转发的，一般情况不会出现上述情况。以下情况会引起异常中断：

- 网络环境问题，当出现网络中断时会出现运维操作异常中断；
- 资源服务端设置超时机制，当空闲时间超过一定时间会出现；
- 针对某些协议，如 RDP 等，由于设置允许的客户端数，当超过此数时会出现中断；
- 运维操作日志大于 4G 时，NABH 会自动中断；
- 在授权规则中设置会话时长，当到达此时间时会自动中断。

17、 使用 Telnet 协议运维 SCO 服务器时，命令阻断不成功？

答：由于用户的 `unix/linux` 主机上设置非常自由，NABH 不可能针对它做各种适应，而阻断功能必须要目标主机配合，NABH 通过发送 `Ctrl-C` 来阻断命令行，可以通过修改服务器的 `/etc/profile` 或其它登录后的自动执行脚本，添加一行命令 `stty intr ^C` 即可。